

# ***Installing Windows 2000 Server to run Internet Information Services***

*Third draft (November 2002)*

## **Required:**

- Windows 2000 Server CD
- Windows 2000 Service Pack 3 CD

## **Assumptions:**

- You have appropriate licences entitling you to use the software
- You have backed up ALL your important files to another machine or to removable media. This process destroys ALL information currently on the hard disk of the server.
- You should also make a note of your current network settings (IP address, network mask and gateway), and likewise your video settings.

## **Procedure:**

### **1. Obtaining Windows 2000 Service Pack 3**

If you haven't already got it on CD, you'll need to download it from Microsoft's web site (or ask me to send you a copy). You need to do this on an up-to-date computer (NOT the server itself) from which you can arrange for the downloaded material to be written to CD.

Visit

<http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/sp3lang.asp>

and click the Go button. On the next screen, click the SP3 Network Installation link, and then the Save button to save the Service Pack to a suitable location on your hard disk.

Once the download is complete (it's about 125MB of data), write the file on to a CD-ROM.

### **2. Make sure the server is disconnected from the network.**

### 3. Begin the Windows 2000 Server installation.

Insert the Windows 2000 Server CD into the server and restart the system so that it boots from the CD. (You may need to change the BIOS settings to tell your computer to use the CD instead of the hard disk.) You should see the following message:

“Setup is inspecting your computer’s hardware configuration ...”

followed by a blue information screen. After a couple of minutes, a menu appears. Press <ENTER> to set up Windows 2000 Server.

If you are using a new hard disk, you will see a warning “Setup has determined that your computer’s setup disk is new...”. Press C to continue.

Scroll through the licence agreement and press <F8> to accept.

Delete any existing partitions by highlighting them and pressing D (followed by L to confirm). If you are using a disk that previously contained data, you may see one or warnings during this process.

Using the create option (C), make two new partitions – the first for the operating system and programs (on C:), the second for your data (D:, or whatever the first available drive letter is). C: should be at least 2000MB. (Increase this if you plan to install other programs in addition to Windows and IIS.) Assign whatever space is left to D:.

Highlight the C: partition using the arrow keys and press <ENTER> to continue the installation. Format the partition using the NTFS file system.

File copying now begins, and takes quite a long time (more than ten minutes, depending on the speed of your computer). At the end the computer will reboot: as the computer restarts, **interrupt the system boot process** and change the BIOS settings back to their default, so that your computer again will boot from its hard disk. Then allow booting to continue.

At the Welcome screen, press the Next button to continue (or just wait for it to carry on automatically).

Change the user locale (“your locale”) to English (United Kingdom), the system locale (by clicking the Set default... button) similarly, and also the keyboard layout. Remove the English (United States) keyboard layout from the list of installed input locales. Click NEXT to continue. (You can safely ignore any warning that appears about not being able to remove the current keyboard layout until the next reboot.)

Enter your name (or, perhaps better, the name of your research group or department), and set the organization to “University College London”.

Select Per Seat licensing.

Choose a name for your computer, and enter a password for the local Administrator account. It is VERY IMPORTANT that you choose a strong password: the local administrator has full control of the machine, and can operate it remotely. The password should be at least 8 characters long, a mixture of letters, numbers and punctuation or special characters, and not be a dictionary word or name.

Click NEXT to continue.

Select the components to install as follows, by un-ticking all the items EXCEPT:

- Internet Information Services (IIS)

Double-click this item and un-tick all subcomponents EXCEPT:

- Common files
- FrontPage 2000 Server Extensions (if you need this for your web site)
- Internet Information Services Snap-in
- WorldWide Web Server

Click OK to continue, and then NEXT to set the time, zone etc. Click NEXT again to install the network drivers. Select Typical Settings (the default). The server is NOT a member of any domain. Specify a suitable workgroup name (e.g. that of your project) and click NEXT.

*Temporary screen corruption has been noted at this point on some systems, but the process should continue uninterrupted.*

Make a cup of tea at this point.

When the Setup Wizard has completed its work, remove the CD-ROM from the drive and click the Finish button to restart the computer.

Note that the server is still disconnected from the network at this stage.

#### **4. Configure initial settings.**

Log on to the server quoting the password you chose earlier. The “Configure Your Server” screen appears. Tick the last item to indicate that you will configure the server later by hand. Click NEXT, and un-tick the box that says “Show this screen at startup”. Close the window by clicking the X in the top right corner.

Drag the “Connect to the Internet” icon into the Recycle Bin.

## **5. Install Service Pack 3 from the CD-ROM.**

Insert the Service Pack CD-ROM and view it by double-clicking on My Computer. Depending on how you got the disk, it may contain just one program, or a folder with a number of sub-folders. If the former, simply double-click to run the service pack installation program. If there are folders, navigate to the Update folder, and double-click the Update icon (the one that looks like a dark blue-and-white box in front of a computer screen).

At the Welcome screen of the setup wizard, click NEXT. Confirm you agree to the licence terms, and proceed. As this is a new installation, there is NO NEED to archive files. Press NEXT to continue.

Click the Finish button to reboot your machine. Whilst the system is restarting, connect it to the network.

## **6. Configuring video settings**

Right-click on the desktop, and click the Properties menu item. Click the Settings tab, and select your preferred video settings. A screen area of at least 800x600 is recommended, and a colour palette of at least 256 colours (if available). Reboot if necessary.

## **7. Configuring network settings**

Right-click on My Network Places, and click the Properties menu item. Right-click Local Area Network Connection, and choose Properties.

Un-tick File and Printer Sharing for Microsoft Networks.

Double-click Internet Protocol (TCP/IP). Click and enter the IP address, subnet mask and default gateway that you wrote down before.

Use the following DNS server addresses:

- 144.82.100.41
- 144.82.100.1

Click the Advanced button, then on the WINS tab disable NetBIOS over TCP/IP and click OK. Ignore any warning about empty WINS addresses: continue clicking OK until you are returned to the Network and Dial-up Connections screen.

8. Installation of security patches for Windows issued since Service Pack 3 was released.

Start Internet Explorer. Choose the last option (“... I want to connect through a LAN”), click NEXT, choose “I connect through a LAN”, click NEXT and then remove the tick from the automatic proxy discovery box. Click NEXT again. Do not attempt to set up an Internet mail account at this stage. Click Finish to complete the configuration.

Internet Explorer will now start up. (You may have to click the Try Again button if it thinks you are off-line.)

Go to the windowsupdate web site:

<http://windowsupdate.microsoft.com>

After a short delay, a security warning appears. Click yes to install and run the Windows Update Control. (Repeat as necessary.) Wait whilst a check is made for the latest version of the software. When the Welcome screen appears, click the link to Scan for updates. At least 15 critical updates should be identified.

Click the link to Review and install updates.

Note that some items (e.g. Microsoft Internet Explorer 6 Service Pack 1) need to be installed separately from the rest.

Click the Install Now button to install any exclusive items, following the on-screen prompts. When an exclusive item has been installed, it is usually necessary to reboot the machine.

After rebooting, log in again and go back to the windowsupdate web site. Repeat the above process to find what critical updates remain and to be install them.

Continue the process of rebooting and re-visiting the windowsupdate site until no further exclusive or non-exclusive items are left to install.

(As of mid-November 2002, there was one exclusive item out of 15 critical updates. The process described above required two reboots – one after the installation of Internet Explorer 6 Service Pack 1, the second after the installation of the remaining 14 updates which were downloaded in a single step. The number of updates is likely to change, of course – and can even go down, as Microsoft occasionally releases cumulative patch bundles that roll up several individual patches into one

‘mega-patch’.)

## 9. Configuring automatic updating for critical updates

It is possible to keep a system up-to-date by regularly re-visiting the windowsupdate site and downloading new updates as they appear. However, it’s normally preferable to have this done automatically:

Click Start (at the bottom left of the screen), Settings, Control Panel. Double-click Automatic Updates, and place a tick against the box saying “Keep my computer up to date.”

If you log on to the server as Administrator once a day or more, select “Download the updates automatically and notify me when they are ready to be installed.

**IMPORTANT NOTE:** With this option, you will only be notified of new updates when you log in as Administrator. The updates will not be installed until you confirm that you have seen the notification and are happy to proceed.

If you don’t regularly administer the machine, instead select “Automatically download the updates, and install them on the schedule that I specify.” Choosing a time of 7.00am or thereabouts may be sensible, so that system operation is not affected during normal office hours but allowing you to find out quickly if there is a problem.

Click OK, and close the Control Panel window.

## 10. Setting up time synchronisation.

You can set your computer’s clock by hand, by it’s better to allow it to synchronise its time with one of the college time servers. This ensures that your clock is always accurate and won’t drift.

Click Start (at the bottom left of the screen), Run..., and type  
cmd

in the box. Click the OK button, and you should get a command prompt.

Now type:

```
net time /setsntp:ntp0.ucl.ac.uk
```

```
net start w32time
```

```
exit
```

(The 0 character at the end of ntp0 is the digit zero.)

Now check the service starts automatically:

Back in Windows, right-click My Computer and select Manage. Expand the Services and Applications branch and click to choose Services. Scroll down the list in the right-hand pane, and right-click "Windows Time". Select Properties, and set "Startup type" to automatic. Click OK, then close the Computer Management window.

## 11. Hardening Windows

Click Start, Settings, Control Panel. Double-click Administrative Tools, then Local Security Policy.

Click in the left pane to expand the Account Policies branch. Click to select Password Policy, and in the right pane double-click "Passwords must meet complexity requirements". Enable this function. Similarly set Enforce password history to remember the last 10 passwords. Change the Minimum password length to 7 characters.

Now, in the left hand pane, click Account Lockout Policy, then on the right set the lockout threshold to 3 attempts, and accept the suggested changes to related parameters (lockout period etc.).

Click in the left hand pane to expand the Local Policies branch. Click to select Audit Policy. Audit account logon events for failure. Audit logon events so that failures are audited. Audit policy change for success and failure. Audit privilege use for failure.

Click Security Options. Set the following:

- Additional restrictions for anonymous connections: "No access without explicit anonymous permissions"
- Clear virtual memory pagefile when system shuts down: Enabled
- Do not display last user name in logon screen: Enabled (and remember your username is Administrator!)
- LAN Manager Authentication Level: Send NTLMv2 response only\refuse LM & NTLM
- Number of previous logons to cache: 0
- Restrict CD-ROM access to locally logged-on user only: Enabled
- Restrict floppy access to locally logged-on user only: Enabled
- Shut down system immediately if unable to log security audits: Enabled
- Unsigned driver installation behaviour: Warn but allow installation
- Unsigned non-driver installation behaviour: Warn but allow installation

Close the Local Security Settings window.

Double-click Services. Disable the following services by double-clicking them and setting the startup type to disabled:

- Alerter
- Clipbook
- DHCP Client
- Fax Service
- Indexing Service
- Messenger
- NetMeeting Remote Desktop Sharing
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Registry Service
- Smart Card
- Smart Card Helper
- Telephony
- Telnet

Close the Services window.

Close the Administrative tools window

12. Disable the default administrative shares (C\$, D\$ etc.)

Note: Be very careful following the instructions in this section. Getting it wrong can seriously damage your computer's health!

Click Start, Run. In the box, type

```
regedit
```

and press <ENTER>.

Double-click HKEY\_LOCAL\_MACHINE in the left hand pane. Double-click SYSTEM, and continue to open:

```
CurrentControlSet  
Services  
Lanmanserver  
parameters
```

From the menu, select Edit, New, DWORD Value. Type

AutoShareServer

and press <ENTER> to give a name to this value. Close the window by clicking the X in the top right corner.

### 13. Prepare the second partition (D:) for data and web pages

Right-click My Computer and select Manage. In the left hand pane, click Disk Management. Right-click on the D: partition and select Format. Click the OK button twice and wait for the disk to be formatted.

Close the Computer Management window.

### 14. Configuring Internet Information Server (IIS)

Use Internet Explorer to go to the following page:

<http://www.microsoft.com/windows2000/downloads/recommended/iislockdown>

Click the link to the IIS Lockdown Tool, and then click the Open button. The IIS Lockdown Wizard will run.

After reading the information, click NEXT. Agree to the licence terms and proceed to the Server Template Page.

Click to highlight the “Dynamic Web Server (ASP enabled)” template. On the next screen, make sure there is a tick alongside the option to install the URLScan filter. Continue to click NEXT until the Lockdown Tool has completed its work.

Note: You can safely ignore the warnings that digital signatures are missing from **these** tools. However, if you see similar messages in future when installing software on your server, you should think carefully about how trustworthy the source of your software is before proceeding.

Double-click on My Computer, browse to the D: partition, and create a folder there to hold your web pages.

Now click Start, Programs, Administrative Tools, Internet Services Manager. In the left hand pane,

double-click on the name of your computer. Right-click on the Default Web Site and choose Properties. Click on the Home Directory tab, and use the browse button to select the folder you made on the D: partition in the previous step as your local path. Close the Internet Information Services window.

15. Install and run the Microsoft Baseline Security Analyzer.

As a final check on your settings, you may like to install the Microsoft Baseline Security Analyzer:

Using Internet Explorer, go to

<http://www.microsoft.com/technet/security/tools/Tools/mbsahome.asp>

In the Download Now section, click the link to the tool. When the File Download window appears, click Open to download and install the Baseline Security Analyzer.

Click through the screens of the Setup program accepting all the default values. At the end the Baseline Security Analyzer will start up.

Click the link to Scan a computer, then Start scan. (You may have to resize the window to see the link. It's towards the bottom of the screen.) At the security warning, click Yes to accept the MSSecure XML File.

Don't be surprised to find some warnings, even after all the effort made to secure your system. Some of the tests are not very precise, or particularly useful<sup>[1]</sup>. Nevertheless, reading through all the result details and the suggested ways of correcting any problems can be very educational.

When you have finished looking at the results, close the Baseline Security Analyzer and close any other windows that you opened earlier.

## **16. Miscellaneous**

BIOS settings should be checked to make sure that the system is configured only to boot from the hard disk. If possible (if the BIOS permits it, that is), a password should be set to prevent unauthorized changes to the BIOS configuration.

Make sure you have a regular backup regime. This is simplified if you are consistent about keeping all your data and web pages on a separate partition (D:). There is little need to back up the system files on C: - in the event of a disaster, you would always reinstall these files anyway.

Obtain and use anti-virus software. See

<http://www.ucl.ac.uk/fsecure>

for details. You will need an IS username and password to access this page.

---

[1] A few patches (five at the time of writing) are wrongly identified as being applicable to your system, when in fact they are not. One check warns that the guest account has a weak password; but since this account is disabled by default, arguably the weakness of the password is irrelevant.