

Server Setup Guide for Primary Schools



Contents

Contents	2
Introduction.....	4
Planning Process	5
Overview, Standards and Conventions	6
Server Hardware and Environment.....	6
Hardware Naming Conventions	6
IP Addressing Scheme	7
User Names and Passwords	8
Pre-Installation Work.....	9
Basic Installation of Windows Server 2008 R2	10
Configuration and Customisation	21
Create Organization Units and Groups.....	21
Change the Password Policy	21
Folder Structure and Shares.....	22
Login Scripts and Drive Mappings	24
Creating Users.....	25
Modify User Details	26
Specifying Proxy Settings Using Group Policy	27
Specifying Home Page Using Group Policy	28
Redirect the 'My Documents' Folder and Enable Offline Working (Optional).....	29
Server: Backups and System Management Tools.....	30
Installation of Windows Server Backup	30
Running Windows Server Backup for the First Time	30
Install Server Management Software.....	33
Install Wireless Management Software	33
Configuring Defragmentation for the Server Hard Disks	34
Enable Shadow Copies	35
Next Steps, Tidying Up and Miscellaneous Activities	36
Disabling Internet Explorer Enhanced Security	36
Install Anti-Virus Software	36
Setup Alternative Administrator Account.....	36
Apply Windows Updates to the Server	36
Activate Windows.....	36
Restore Old Data.....	37

Installing Printers	37
Check Logins	38
Test Remote Desktop	38
Windows 7 Logon Behaviour	38
Logon Warning/Security Message	38
Install Internet Explorer 9 on Server	38
Creating a Master Image	39
Imaging of PCs	40
Connecting a Windows 7 Client to the domain	40
Connecting a Windows XP Client to the domain	41
Connecting a Windows 8 Client to the domain	41
Appendix A: Installation Checklist	42
Appendix C: Creating Mandatory Profiles	45
Appendix D: Installation of Anti-Virus Software	49
Install Admin Server	49
Install Anti-Virus Client on Server	56
Install Anti-Virus Client on Workstations	57
Appendix E: Two Minute Guide to the New Network	60

Document History		
3.0	July 2012	Improvements, updates, rationalisation and re-sequencing of sections
2.0	March 2012	Improvements and amendments following feedback
1.0	January 2012	First issue
0.1	September 2011	Pre-release version for testing

Introduction

This guide describes how to setup a network file server in a typical primary school, suitable for meeting the needs of pupils and teachers. The design is based around the following principles and assumptions:

- The overall design is intended to be consistent and universal and reflects the requirements of the majority of primary schools¹
- There is a single file server with a single domain
- The network operating system is Windows Server 2008 R2
- The clients are Windows 7 Professional or better and/or Windows XP Professional. The use of Windows 8 is discouraged due to the unfamiliarity of the Metro environment in schools
- Each network is treated as though it was a new installation, rather than as a migration² in Microsoft terminology. In other words, an opportunity to start again from scratch. However, any existing data should be preserved and transferred across
- Workstations are specifically imaged/re-imaged for use on the network
- There is a maximum of 255 devices on the network
- Teachers and older pupils have individual logins, younger children use shared logins
- The network provides home folders for individual users along with a number of pre-defined shared folders
- Users are organised into groups e.g. cohorts, pupils, teachers and security and access are based around groups. For instance, the teachers group can use resources that the pupils group cannot
- Control and security are implemented using the standard tools provided by Windows Server (specifically Group Policy and Mandatory profiles) rather than via third party products³
- User applications are not run from the server directly, although they may access shared data on the server and may be installed from master copies stored on the server
- The server has a workable backup system that enables all user data to be recovered in the event of problems, but is not necessarily intended as a speedy disaster recovery solution
- A managed anti-virus solution is installed (AVG Business Edition is recommended)
- This is a curriculum network and it is envisaged that a separate administration network is used for running applications such as SIMS and Finance, as is commonly the case
- The simplest solution to meeting a requirement is used whenever possible and over-engineered and highly technical solutions are avoided
- Through a combination of simple elegant design and by taking a consistent approach, the system is engineered to be easy to understand, maintain and support by IT technicians who are familiar with the general concepts

¹ Examples are based around Hertfordshire and Essex schools; however, it is applicable elsewhere if the appropriate IP addresses and internet connectivity options are specified.

² In a migration, the operating system is upgraded in-situ e.g. from Windows Server 2003 to 2008, or the new and old servers run simultaneously during the build. However, the latter can give rise to DNS and DHCP issues.

³ In a school environment it is normal to control or 'lock down' the Desktop, both to prevent users changing things intentionally or otherwise, but also to provide a customised experience (for instance, by giving each year group their own set of applications). Such control can be provided through a third party program or suite such as RM CC4, RM Ranger or Viglen ClassLink. However, these programs have a number of drawbacks: they cost money; they may interfere with the normal operation of the server and workstation; they may use proprietary, non-standard methods of doing things; they may be incompatible with other widely used software. A decade ago, when most of these suites originated, the native tools in Windows Server were both limited and arcane. However, this is no longer the case and these days Windows Server largely provides everything needed 'out of the box'. Accordingly, we'll be using Group Policy Objects (GPOs) and Mandatory Profiles to control the user experience.

Planning Process

The installation of a new computer network in a school represents a significant investment in time and money for all parties concerned. To ensure success, it is necessary that the implementation is carefully planned and managed. Primary schools do not differ much in their requirements, other than in the numbers of users and computers and, unlike with a business, this is usually a case where 'one size (design) fits all'. By using standard products and procedures, backed up with appropriate project management, a successful outcome can be anticipated.

The first step is to understand any specifics of the school. This can be done through a site survey and by talking with the Head, ICT co-ordinator and the IT technician (if there is one). Specifically, answers to the following questions are required:

- Is this a first or a replacement server?
- Will this be a curriculum network or a hybrid curriculum/administrative network?
- How much existing data does the school have?
- How many workstations does the school have?
- How suitable are the workstations (specifications, operating systems)?
- Are there any other networking devices to be considered (Macintosh, iPads etc.)?
- How suitable is the infrastructure (Gigabit Ethernet? Wireless 11n?)
- Where will the server be located?
- What are the likely timescales?
- Is funding available?

With regards to the last point (funding), clearly the exact cost of the project will have to be determined but ballpark figures can be discussed so as to set expectation. For rough guidance, most school file server installations cost in the order of £5,000-£10,000 depending on scale.

It should be kept in mind that the main objectives are to implement a network that successfully meets the school's needs and is manageable and is profitable to the supplier, both in immediate terms and as part of a longer term business relationship. The objective is not to install a network regardless of practicalities or consequences, or set expectations that cannot realistically be met. For example, if some of the school's existing infrastructure is unsuitable then the cost of upgrading this has to be factored in and, if this is unpalatable to the school, then a hard-headed decision has to be taken as to whether the overall project can be undertaken.

Once the school has signed up for a new network then a project plan should be put together. The purpose of the plan is to define 'who does what and when' plus provide a high level monitoring and control mechanism, so it should therefore be in sufficient detail to do this. Project plans usually comprise a list of activities and tasks, expressed as a checklist or GANTT chart. For simplicity and ease of access it is suggested to use a checklist and a sample one can be found in *Appendix A: Installation Checklist*.

Overview, Standards and Conventions

Server Hardware and Environment

A good vendor for file servers is Dell, partly as the ordering process can be easily managed online. Schools can be categorised as small, medium or large depending on the number of users and an appropriate model of server should be specified accordingly. Server specifications are changed as infrequently as possible so as to maintain consistency, with change usually being driven by Dell having refreshed their product line. For current file server specifications, please see *Appendix B: Server Hardware and Specification*.

After installation, the server will thereafter be operated *headless* using a Remote Desktop connection. Therefore a screen, keyboard and mouse can be 'borrowed' for the installation and there is no requirement to purchase these items for everyday use. Headless operation reduces costs, saves space and energy and discourages teachers from trying to work directly on the server.

The server should ideally be located in a secure location (preferably a locked room) where it cannot be easily accessed by people.

Backup devices and an intelligent uninterruptible power supply (UPS) should be considered mandatory for all installations.

Ideally the school's cabling system will be Gigabit capable. If not, an Ethernet switch with at least one Gigabit port for the server should be used so as to minimise bottlenecks. Wireless networks should be based around simultaneous dual-band access points.

Hardware Naming Conventions

The server should be called *SERVER*.

The domain should be the name of the school with a suffix of *local*. Example: *sunnyside.local*. Schools with long names should be shortened to something more convenient such that they are less than 15 characters e.g. Our Lady of St Paul and Vincent could become *ourlady.local*.

Desktop computers should be named using the format *xxx-location-nn*, where *xxx* is an abbreviation for the school, *location* is a short description of where the computer is located and *nn* is a two digit number to identify the computer.

Example: the school is called Hillside Mixed Juniors. There are 20 desktops in the ICT Suite, named *HMJ-SUITE-01*, *HMJ-SUITE-02*, *HMJ-SUITE-03* etc. Each classroom has two desktops. These are named *HMJ-CLASS3-01*, *HMJ-CLASS3-02* and so on.

Laptop computers should be named using the format *xxx-laptop-nn*, where *xxx* is an abbreviation for the school, *laptop* identifies as a laptop (and hence potentially mobile) computer and *nn* is a two digit number to identify the laptop.

Example: the school is called Our Lady of Mercy. The laptops are named *OLM-LAPTOP-01*, *OLM-LAPTOP-02*, *OLM-LAPTOP-03* and so on.

The computers should be labelled with their designated names.

IP Addressing Scheme

LEA primary schools operate using IP ranges that are not routable on the internet i.e. they use private IP addresses. For example, Hertfordshire schools use a 172.nnn.nnn.nnn scheme, Essex schools use a 10.nnn.nnn.nnn scheme and other counties do similar. A 24-bit subnet (255.255.255.0) should normally be specified.

A further difference between counties is that in Hertfordshire the gateway router is usually located at the top of the scope (e.g. 172.16.24.254) and the server at the bottom (e.g. 172.16.24.1), whereas in Essex it is the other way around (e.g. gateway at 10.41.8.1, server at 10.41.8.254). Accordingly, there is some variation between the two schemes.

IP v4 ('traditional IP') is used rather than IP v6.

The IP scope should be used as follows:

Usage	Hertfordshire – 172.nnn.nnn.nnn
1	Server (fixed IP address)
2..9	Reserved for future usage
10..200	Use for desktops, laptops, tablets. Assign dynamically from DHCP address pool
201..219	Wireless Access Points (WAPs). Use IP reservations
220..239	Printers. Use IP reservations
240..253	Other connectivity or specialised devices ⁴ e.g. Espresso box, NAS etc.
254	Gateway router (fixed IP address)

Usage	Essex – 10.nnn.nnn.nnn
1	Gateway router (fixed IP address)
2..9	Reserved for future usage
10..200	Use for desktops, laptops, tablets. Assign dynamically from DHCP address pool
201..219	Wireless Access Points (WAPs). Use IP reservations
220..239	Printers. Use IP reservations
240..253	Other connectivity or specialised devices e.g. Espresso box, NAS etc.
254	Server (fixed IP address)

If there are existing devices that do not fit within this scheme (e.g. printers with static IP addresses) then their IP addresses should be changed to make them compliant.

The design limitations imposed by this scheme are: 190 concurrent leases for computers; maximum of 20 networked printers; maximum of 20 Wireless Access Points. However, these are more than sufficient for most primary schools.

The DNS servers for Hertfordshire are 172.16.1.50 and 172.16.1.100.

The DNS settings for Essex are 10.34.1.11 and 10.34.1.12.

⁴ Use reserved IP addresses if possible else use static IP addresses

User Names and Passwords

Standards for Administrators

By default, the Administrator password on Windows Server has to comprise a mixture of letters, numbers and at least one special character. Use the convention of **!Unicornmmyy** where *mm* and *yy* represent the month and year the server was installed.

Example: a server installed in October 2013 would have a password of **!Unicorn1013**

The password should be protected (kept secret from the users) in order to protect the integrity of the server. A copy of it should be placed in a sealed envelope and kept in the school safe; it should be explained to the Head that there is no normal reason for them to ever need to use it but it is there for emergencies.

Standards for User Names and Passwords

A graded system is used on the principle that (for example) a 7 year old does not have the same cognitive abilities as an 11 year old or a teacher. Use lower case for all names and passwords.

Group	Login Type	Format	Password	Rationale
Reception Nursery Year 1 Year 2	Group	Simplified variant of group name i.e. "R", "N", "1", "2"	None	Children cannot be expected to type their names or understand the concept of passwords.
Year 3 Year 4	Individual	First name plus initial of surname e.g. katiep, johnd. For duplicates add number as suffix e.g. maryo2. Remove apostrophes and hyphens from names	Common password for entire class e.g. "password". Password cannot be changed.	Introduces concepts of user ID and password. Most children are able to type their own name.
Year 5 Year 6	Individual	First name plus initial of surname e.g. katiep, johnd. For duplicates add number as suffix e.g. maryo2. Remove apostrophes and hyphens from names	Password is the child's first name. Password cannot be changed.	Children are able to type their own name and memorise a personal password.
Staff	Individual	First name plus initial of surname e.g. katiep, johnd. For duplicates add number as suffix e.g. maryo2. Remove apostrophes and hyphens from names	Assign a random password consisting of a word and numbers according to a particular theme. Record the details in Active Directory. e.g. piano45, drums23, etc.	Provides higher level of security than use of first name e.g. prevents unauthorised use by older children who may know the teacher's name

Pre-Installation Work

There are a number of activities that should take place before the installation takes place. These vary depending on whether it is a new installation into a school that has never had a server, or if it is a replacement server for a school that has. Some of these activities can be carried out or organised by the local IT technician or ICT Co-ordinator:

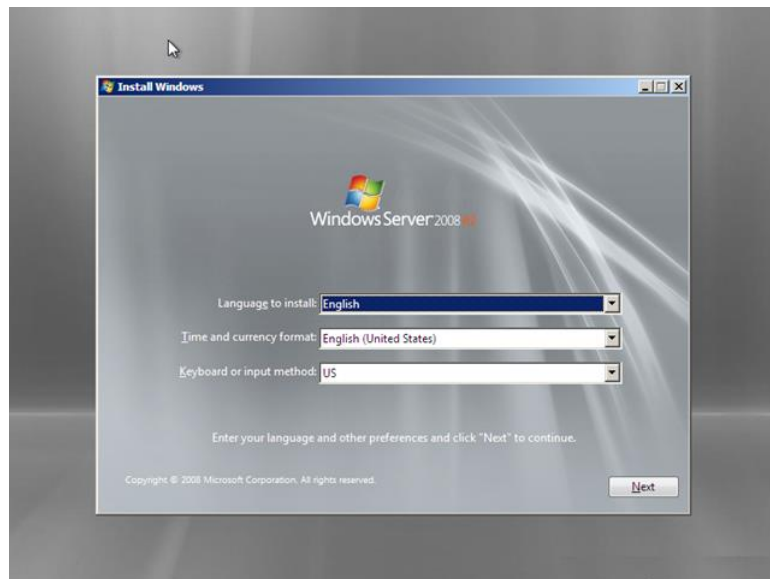
- Equipment ordered, delivered and onsite
- Software ordered. Licence details available
- If site currently has Ranger, arrange for software maintenance/protection to end
- If site currently has Sophos, arrange for annual maintenance to end
- All computers are up-to-date with Windows updates and service packs
- Hardware and printer device drivers obtained for all equipment
- Obtain password details for all existing systems and software⁵
- Application software requirements identified
- Teachers advised as to what is happening and when e.g. any downtime and non-availability of ICT Suite agreed and publicised
- Teachers advised that any documents being stored on the Desktop should be transferred to their home or shared directories
- Archive backup of old server taken. It is suggested that this is done as a simple disc copy to an external USB drive rather than with any proprietary software (e.g. use standard *xcopy* command)
- Virus check of entire school
- List of all current users obtained
- Server updated with latest BIOS, latest RAID firmware and drivers

⁵ If a Microsoft licensing agreement is in place then the serial numbers for Windows, Windows Server and Office may be online. A good idea is to print off the Windows Server serial number and stick it onto the server in lieu of a COA.

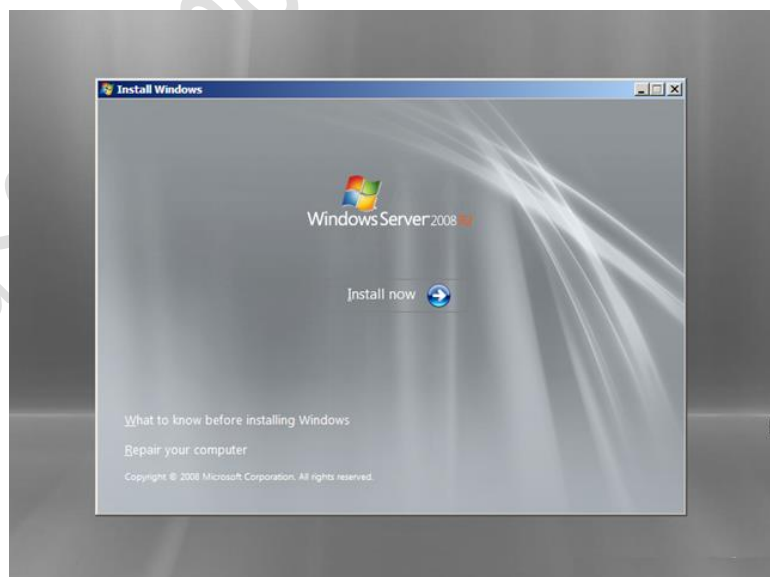
Basic Installation of Windows Server 2008 R2

It is assumed here that the RAID array has been configured as a single large drive and will be partitioned more appropriately later on. Check the BIOS settings on the server and make sure that it is set to boot from the installation media (DVD or USB as appropriate).

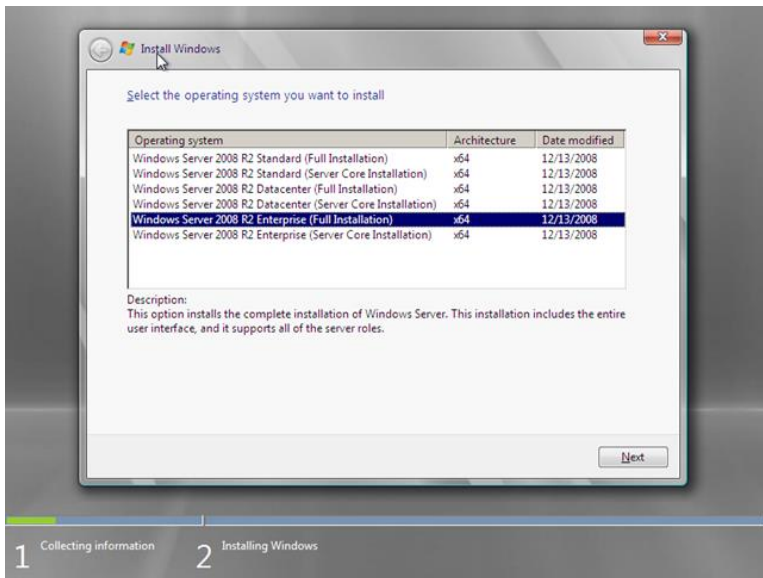
The operating system can be installed in one of two ways. With some servers, it is possible to simply boot from the Windows Server 2008 R2 installation media. However, many server vendors provide an initial setup CD/DVD that provides driver and RAID support etc. This is used to start the server; at some stage this disc is ejected, the Windows Server installation media should be inserted and the normal setup then runs. Regardless of approach, eventually the following screen is displayed:



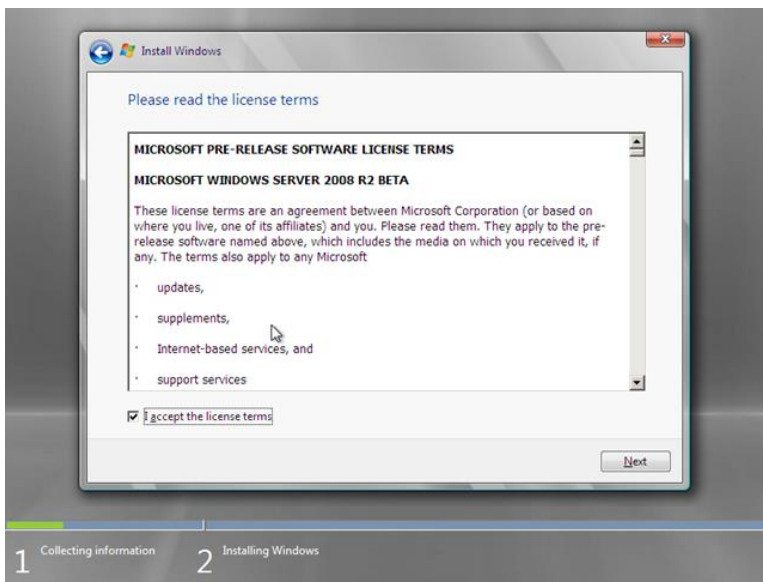
Make sure the language, time and currency format and keyboard input method are set to UK English as they usually default to US settings.



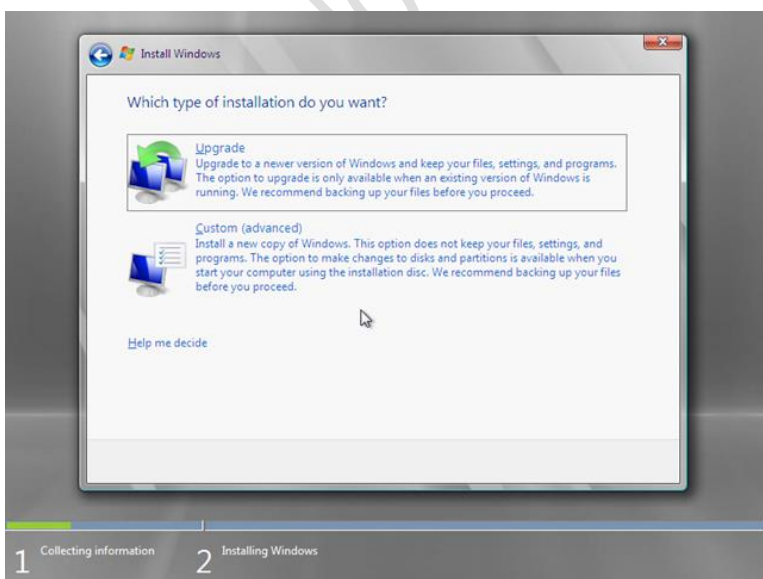
From this screen, click on **Install now**.



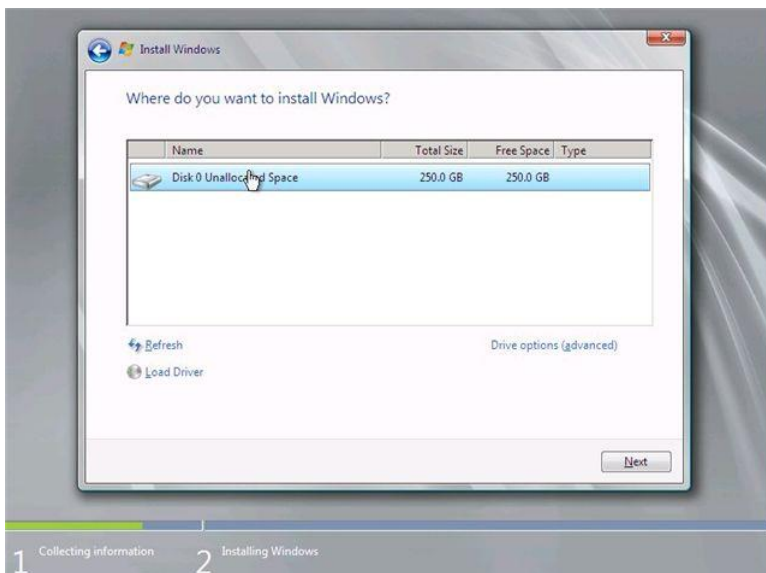
Choose the version that you are going to install – this will almost certainly be **Windows Server 2008 R2 Standard (Full Installation)**



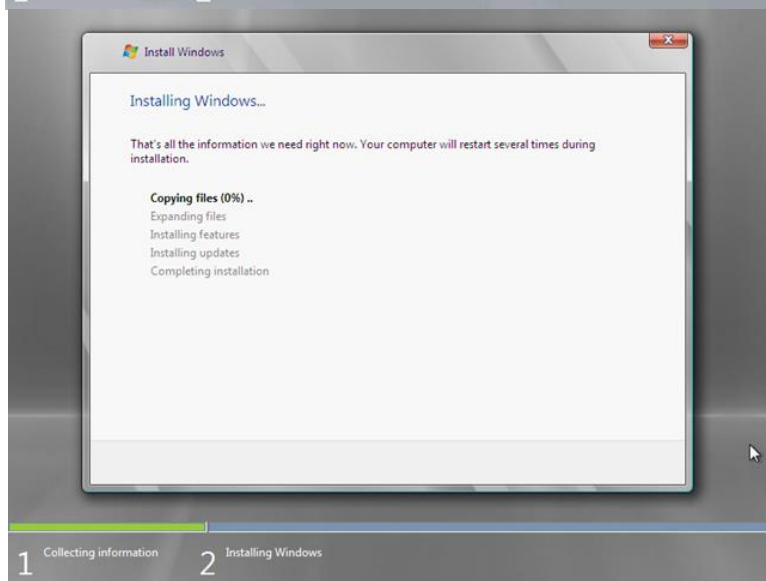
Accept the license terms and click **Next**.



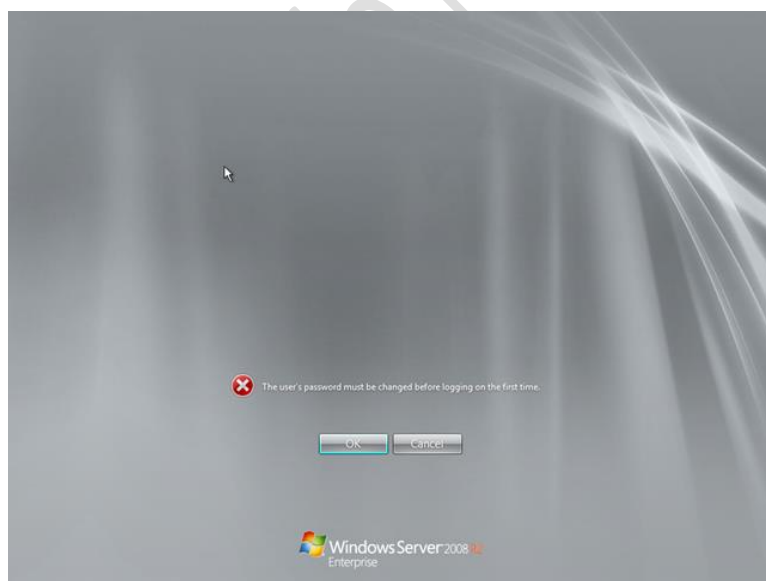
Choose the type of installation. This should be **Custom (advanced)**.



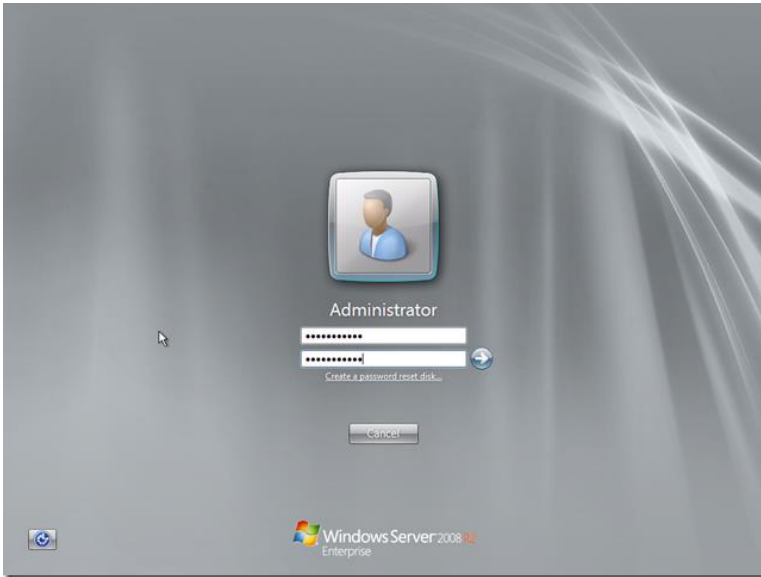
Specify where Windows is to be installed. One disk – corresponding to the RAID array – should be visible. This will install to a single volume, which we will repartition later.



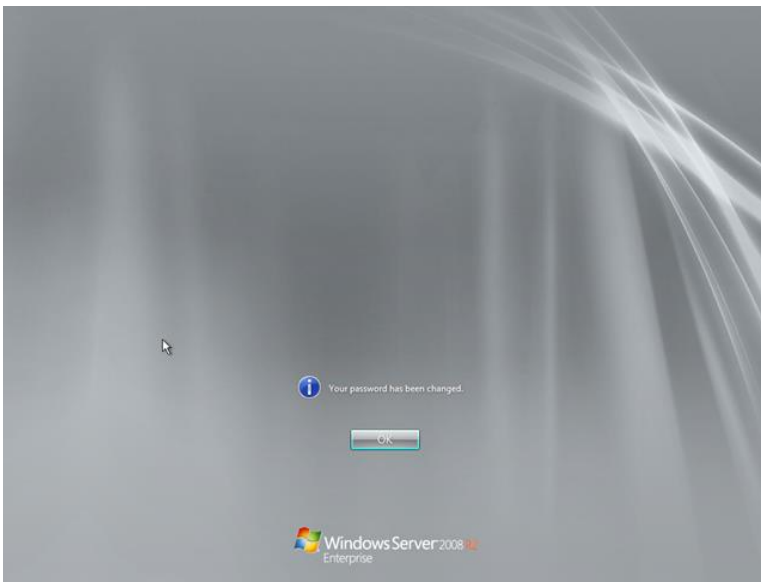
At this point Windows will start installing. This requires no interaction and will complete in 10-30 minutes depending upon the specification of the server.



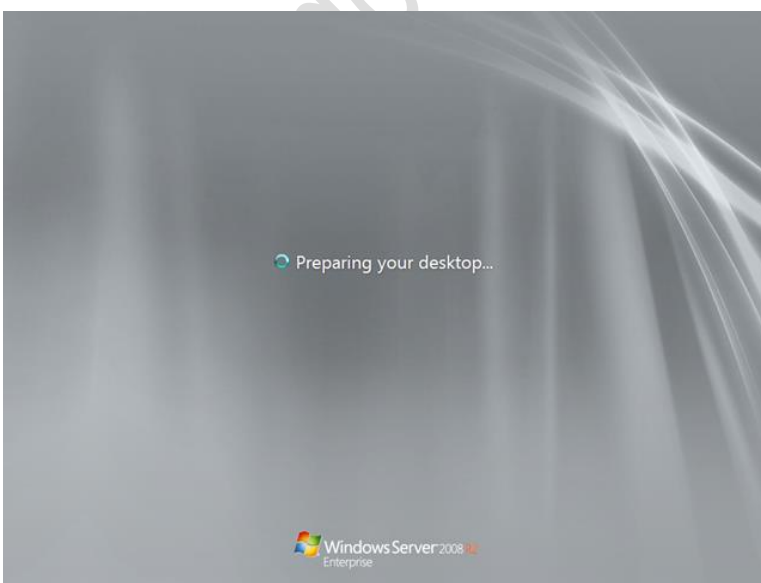
After Windows has installed and rebooted, it will prompt you to change (strictly speaking, set) an Administrator password.



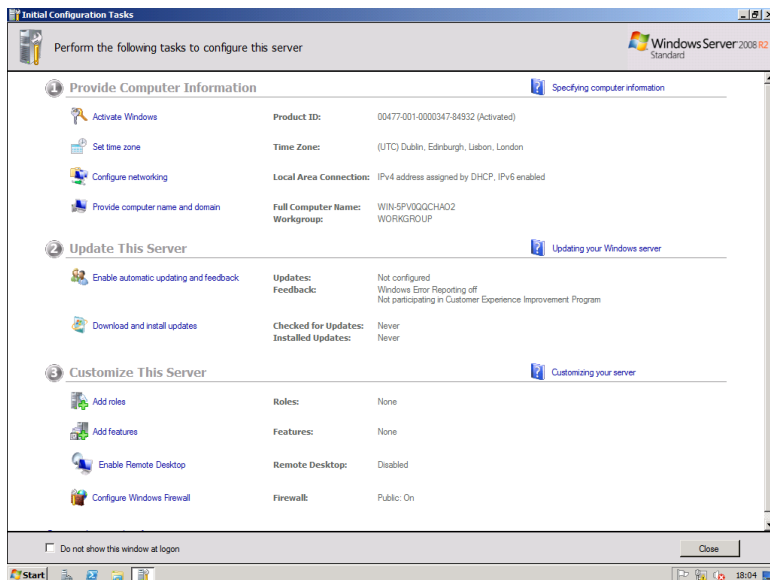
Specify and confirm the Administrator password.



Windows confirms that the password has been changed.



Logging in for the first time...

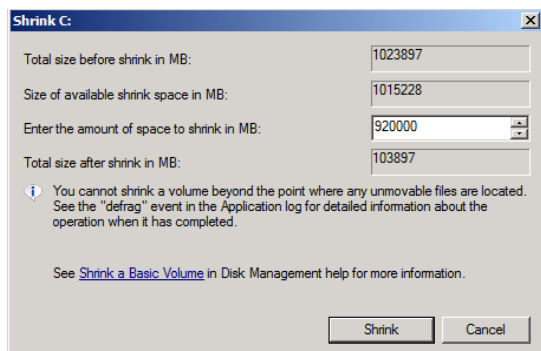


After starting the server, a screen displaying a list of tasks that need to be completed is displayed. This will continued to be shown at start-up until disabled using the tickbox at the bottom of the screen and is a useful memory aid in the early stages. However, for now, just close this screen.

Note that it is not necessary to Activate Windows at this stage or to download updates in case you have to scrap things and start again - wait until things are basically working correctly.

Before proceeding, make sure the previous file server (if there is one) is disconnected from the network.

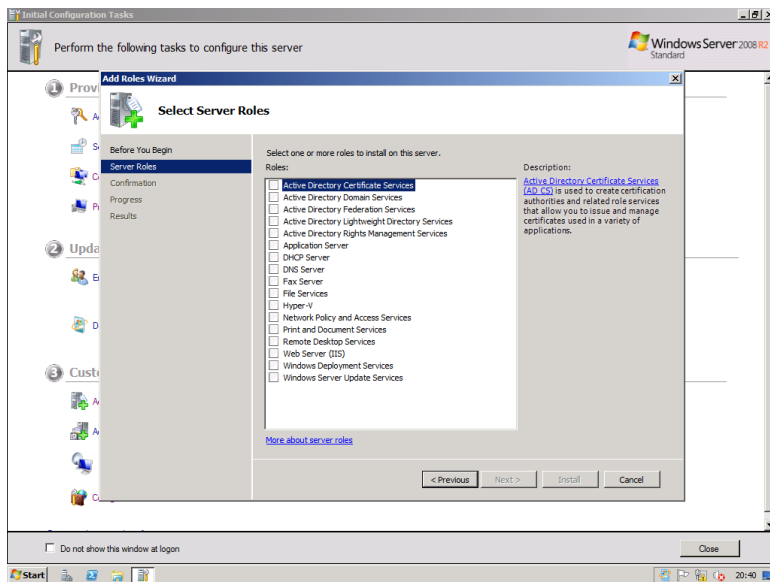
The first step is to **Configure Networking**. Set a suitable address for the server e.g. 10.1.1.254. Specify the gateway e.g. 10.1.1.1 and the DNS settings for the county (e.g. Essex is 10.34.1.11 and 10.34.1.12, Herts is 172.16.1.50 and 172.16.1.100). Use **Start > Control Panel > Internet Properties > Connections** and specify the proxy server (e.g. Essex is *cache.essex.sch.local* and Herts is *wf3.thegrid.org.uk*). Change the name of the computer to *Server* but leave as a Workgroup computer for now. Restart the server.



When the server has restarted, click on **Start** then right-click **Computer** and choose **Manage**. After the console opens expand **Storage** and choose **Disk Management**. Right-click on the C: drive and choose **Shrink Volume**. Adjust the size so that it will be around 100 GB and click **Shrink**. When finished, right-click on the unallocated space and choose **New Simple Volume**. Use the whole of the space, format it to NTFS (Quick Format is sufficient), but do not assign a drive letter.

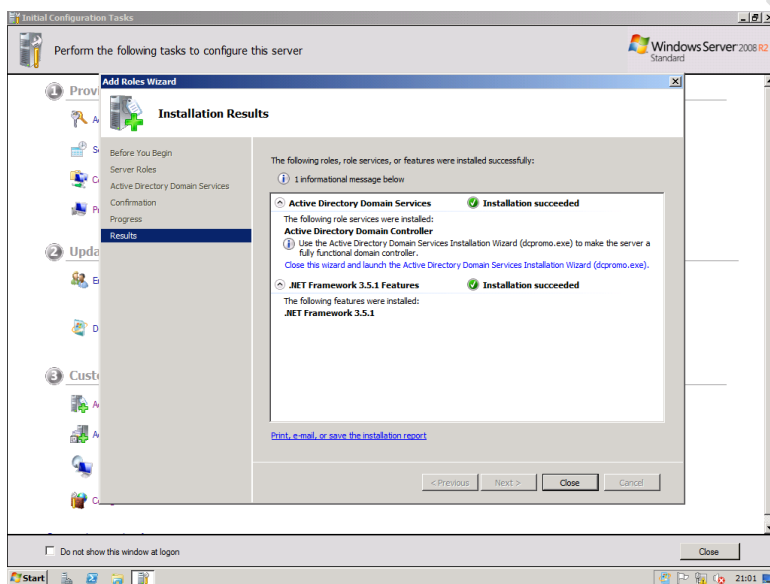
After the volume has been created, change the drive designations such that the DVD drive (if present) becomes **E:** and assign **D:** to the newly created volume. Name it *DATA* and name the C: drive as *SYSTEM*.

Restart the server at this point.

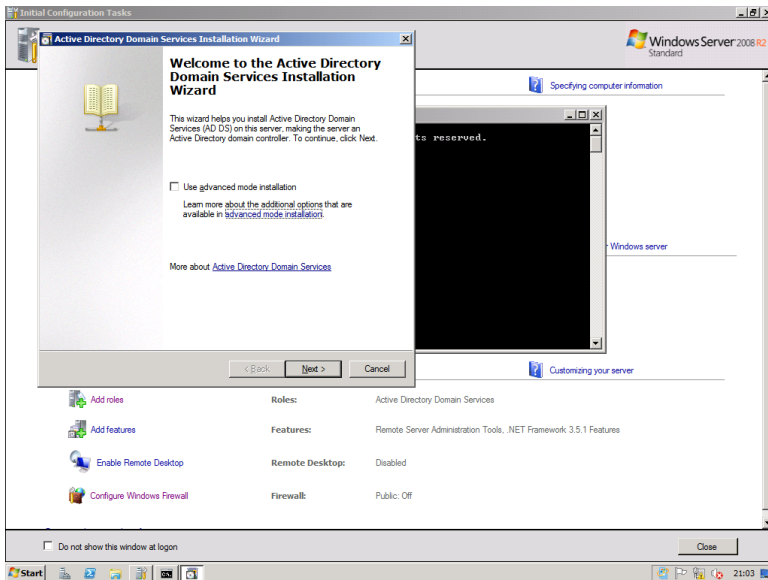


After the restart, under **Customize This Server** choose **Add roles**. Skip the first message screen, then this screen will be displayed.

There are 17 roles listed, but not all are required. Only the following roles need to be setup: Active Directory Domain Services; DHCP Server; DNS Server; File Services. Note that some are associated so, for example, DNS will be installed when Active Directory is setup.

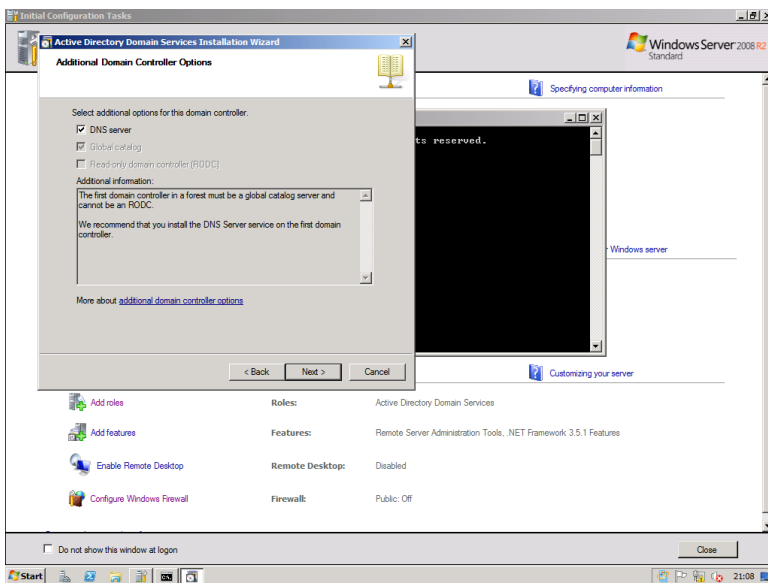


Start by clicking on **Active Directory Domain Services**. You may be prompted to install **.NET Framework 3.5.1 Features**; if so click on **Add Required Features**. On the following screens click on **Next** and then **Next** again, then finally **Install**. After it has done so (which will take several minutes) the screen on the left will be displayed. Click **Close** to continue.

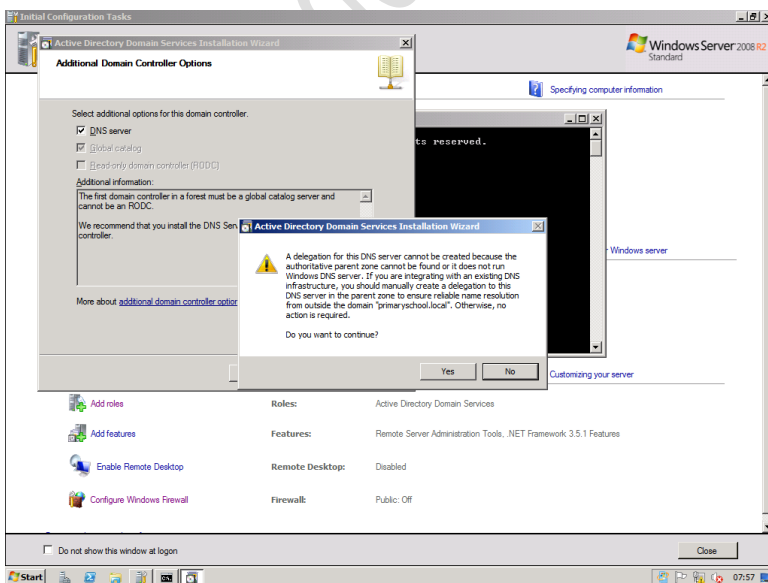


Now bring up a **CMD** prompt, type **DCPROMO** and press **Enter**. The screen to the left is displayed.

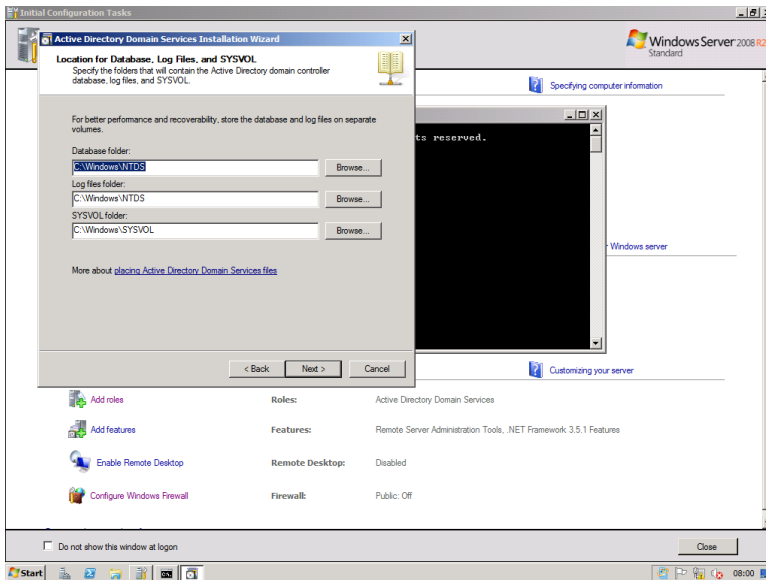
Click on **Next** twice. On the following screen choose **Create a new domain in a new forest** then **Next**. For the name of the domain, use the school name suffixed with *.local* (e.g. *primaryschool.local*) and click **Next**.



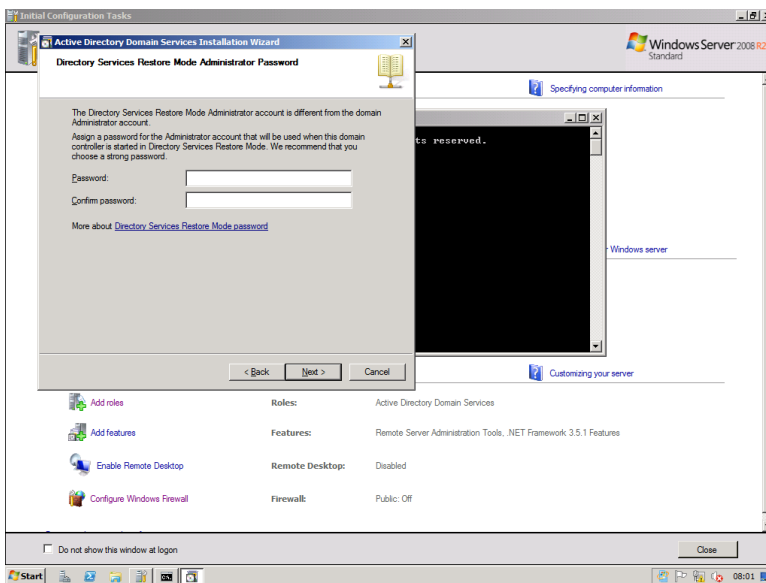
The Forest functional level should be set to **Windows Server 2008 R2**. Then click **Next**. It will think about things for a little while and then tell you the server also needs to be a DNS Server. Click **Next**.



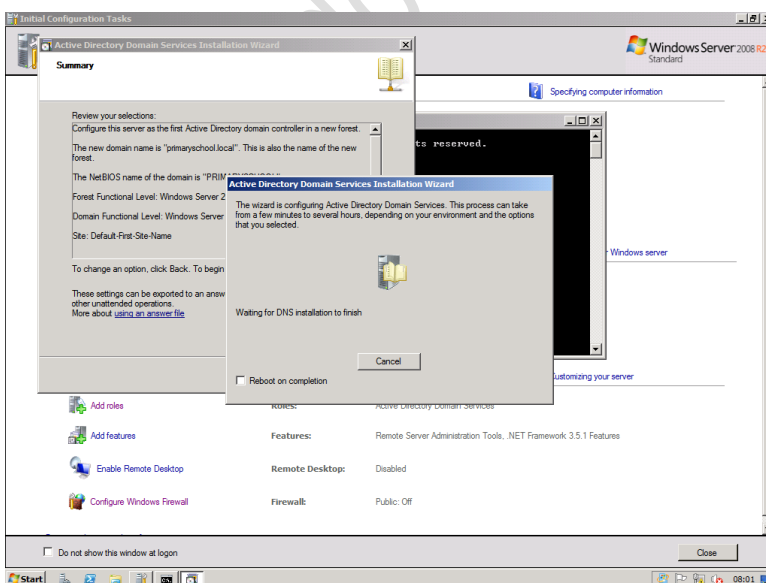
A DNS warning will be displayed - this is okay and can safely be ignored by clicking on **Yes**.



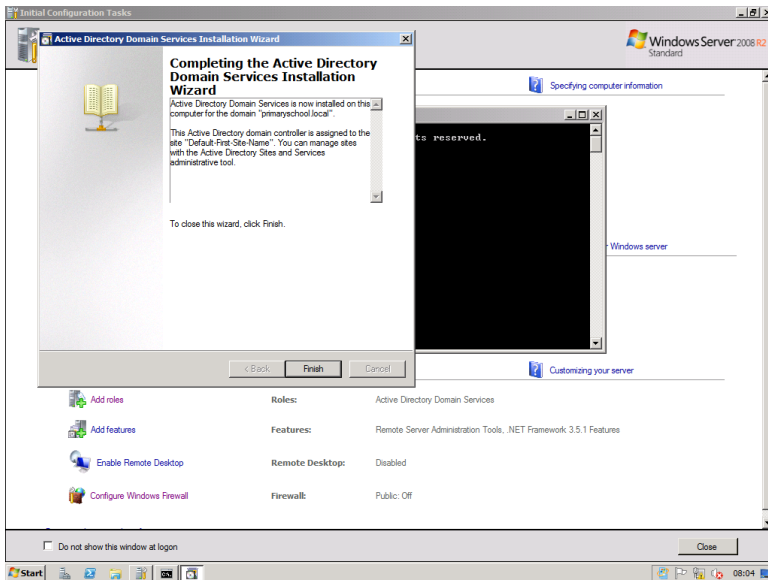
A message about locations for the various AD files is displayed. The defaults on the following screen are fine so just click **Next**.



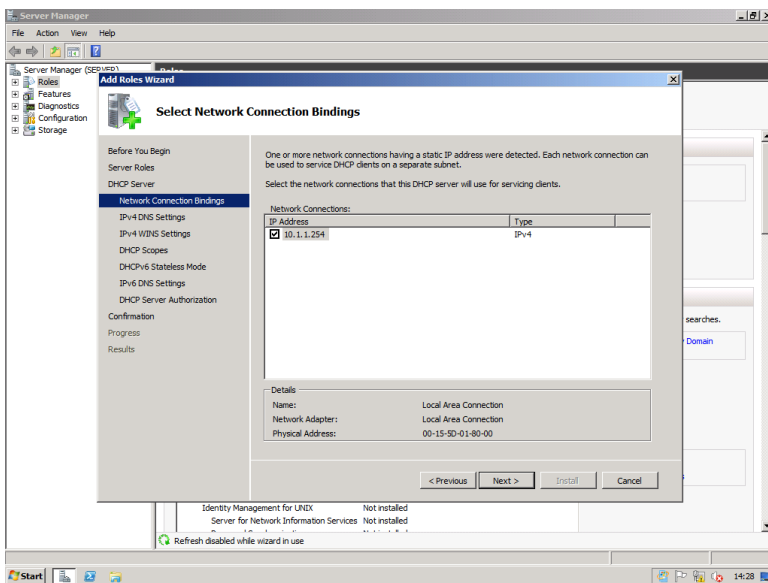
A password for AD is required. Use the same one as the main Administrator password.



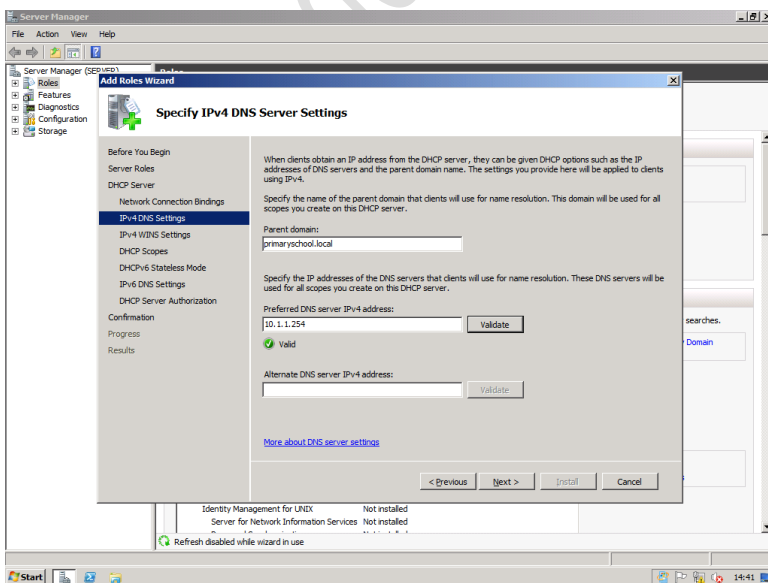
A Summary screen is displayed. Click **Next** to proceed; the system will create the Active Directory schema. This will take several minutes.



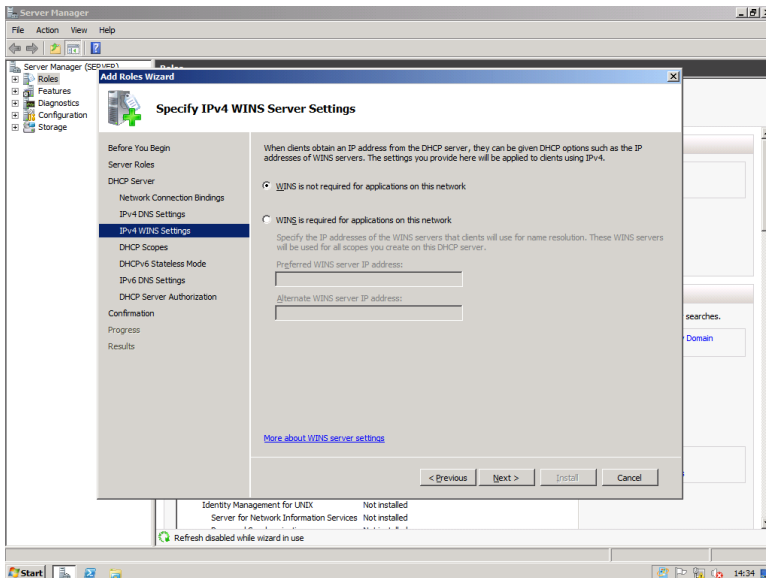
When finished, the screen shown on the left is displayed. Click **Finish** and restart the server.



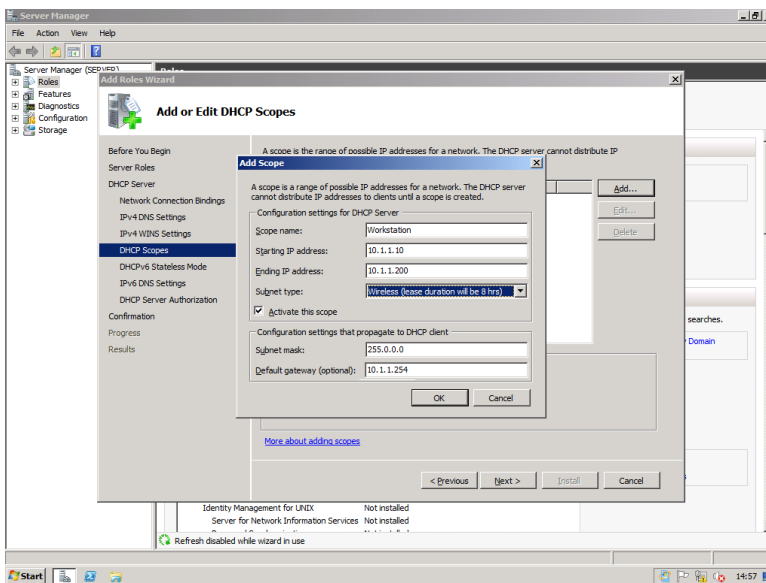
After the server restarts the Task List is once again displayed. Go to **Add Roles** and this time Add **DHCP Server**. Follow through the prompts - confirm that it is picking up the server's network adapter.



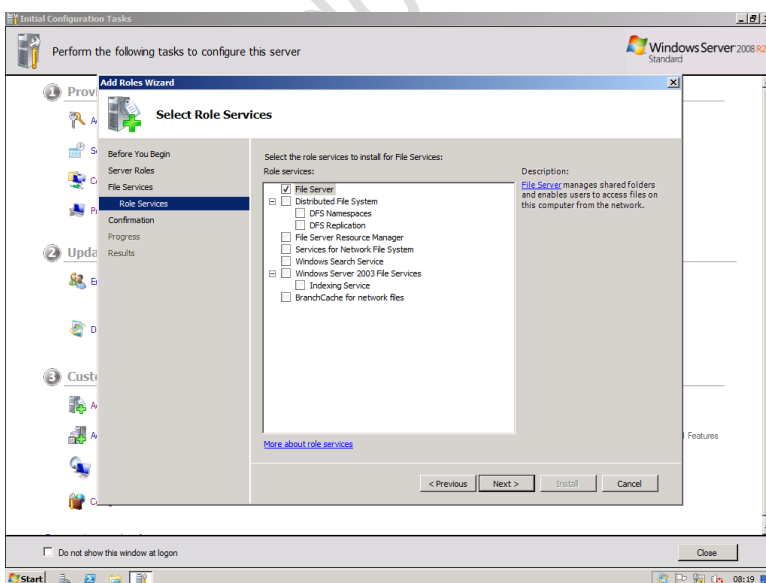
Click **Next**. On the following screen, use the server's IP address for the **Preferred DNS server IPv4 address**. Then click **Next**.



The following screen asks about WINS. WINS is largely archaic and not usually needed so just click **Next**.



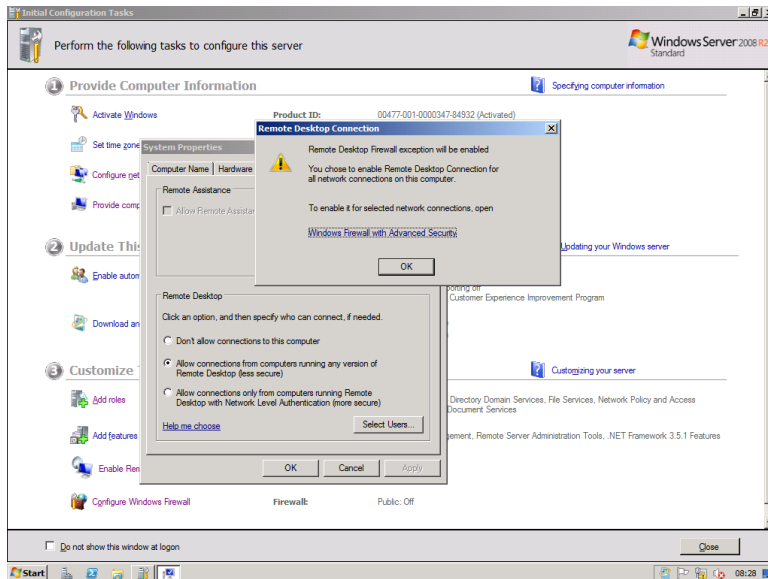
On the next screen specify the IP scope. Click on **Add** to add a scope; give it a name (e.g. *workstations*), specify a start address of **x.x.x.10** and an end address of **x.x.x.200**. Use a Subnet type of **Wireless**, which will give 8 hour leases. Specify a subnet mask of **255.255.255.0**⁶. **IMPORTANT:** Set the **Default gateway (optional)** field to the address of the **router**⁷. Click **Next** on the remaining screens, which relate to IPv6 and which we are not using, then click on the **Install** button.



After the install completes, the Task List is once again displayed. Add **File Services**. Accept all the defaults - the only option needed is **File Server**.

⁶ Note that the default value of 255.0.0.0 is unsuitable and must be changed to 255.255.255.0

⁷ It's not 'optional' at all. Very important to specify else the internet will not work. Use 10.nnn.nnn.1 in Essex schools and 172.nnn.nnn.254 in Herts.



At this point all the roles have been added. The next step is to **Enable Remote Desktop⁸**, which will enable the server to be managed from any workstation. Click **Start**, right-click on **Computer** and choose **Properties**. On the resultant screen, click **Remote Settings**. Choose the **Allow Connections from computers running any version of Remote Desktop** option, acknowledge the message that pops up, then click **OK** again.

Finally, configure the DNS setting. Click on **Administrative Tools > DNS**. In the left-hand panel, right-click on the Server and choose **Properties**. Click on the **Forwarders** tab. Click on the **Edit** button. Check that county DNS addresses (i.e. **10.34.1.11 & 12** for Essex, **172.16.1.50 & 100** for Herts) have been automatically added and correct if this hasn't happened. Also, make sure that the 'Use root hints if no forwarders are available' box is **not** ticked as this will result in excessive network traffic and reduced internet performance.

At this point the basic installation is complete. The server can now be configured and customised.

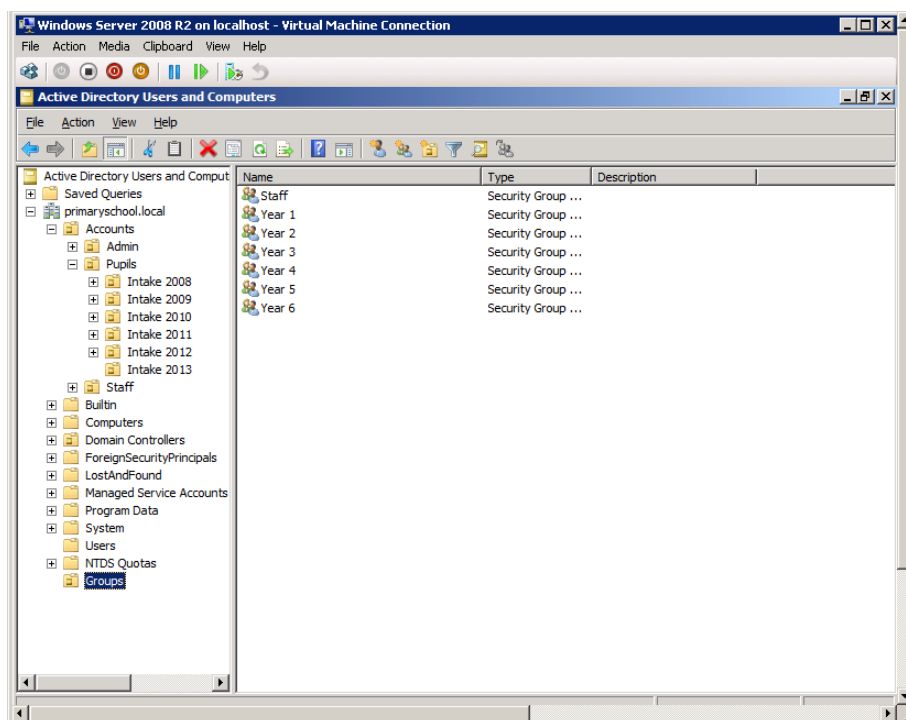
⁸ Note that this **does not** mean adding the remote access role for Terminal Services-type operation by users.

Configuration and Customisation

Create Organization Units and Groups

Use the **Active Directory Users and Computers** tool to create an Organization Unit called **Accounts**. Within it, create three more OUs called **Admin**, **Staff** and **Pupils**. Within Pupils, create a number of OU for the cohorts e.g. **Intake 2010**, **Intake 2011**, **Intake 2012** and so on. These should go back in time enough to cover all the existing children, and also forward by 5 years to cover future years.

Now create an OU actually called **Groups**. Within it, create Groups (that is, Security Groups) called **Staff**, **Year 1**, **Year 2**, **Year 3**, **Year 4**, **Year 5** and **Year 6**⁹. The AD tree should now look like this:



Note that some of these objects may not be fully utilised for now, but rather are defined to partly keep options open for the future.

Change the Password Policy

By default Windows Server 2008 R2 has a password policy of “complex passwords”, which means that passwords have to consist of a mixture of letters, numbers and specials characters. Such passwords are too complicated for children and therefore the policy needs to be changed. To do so, go into the **Group Policy Management Editor**; right-click the Default Domain Policy and choose **Edit**. Drill down to:

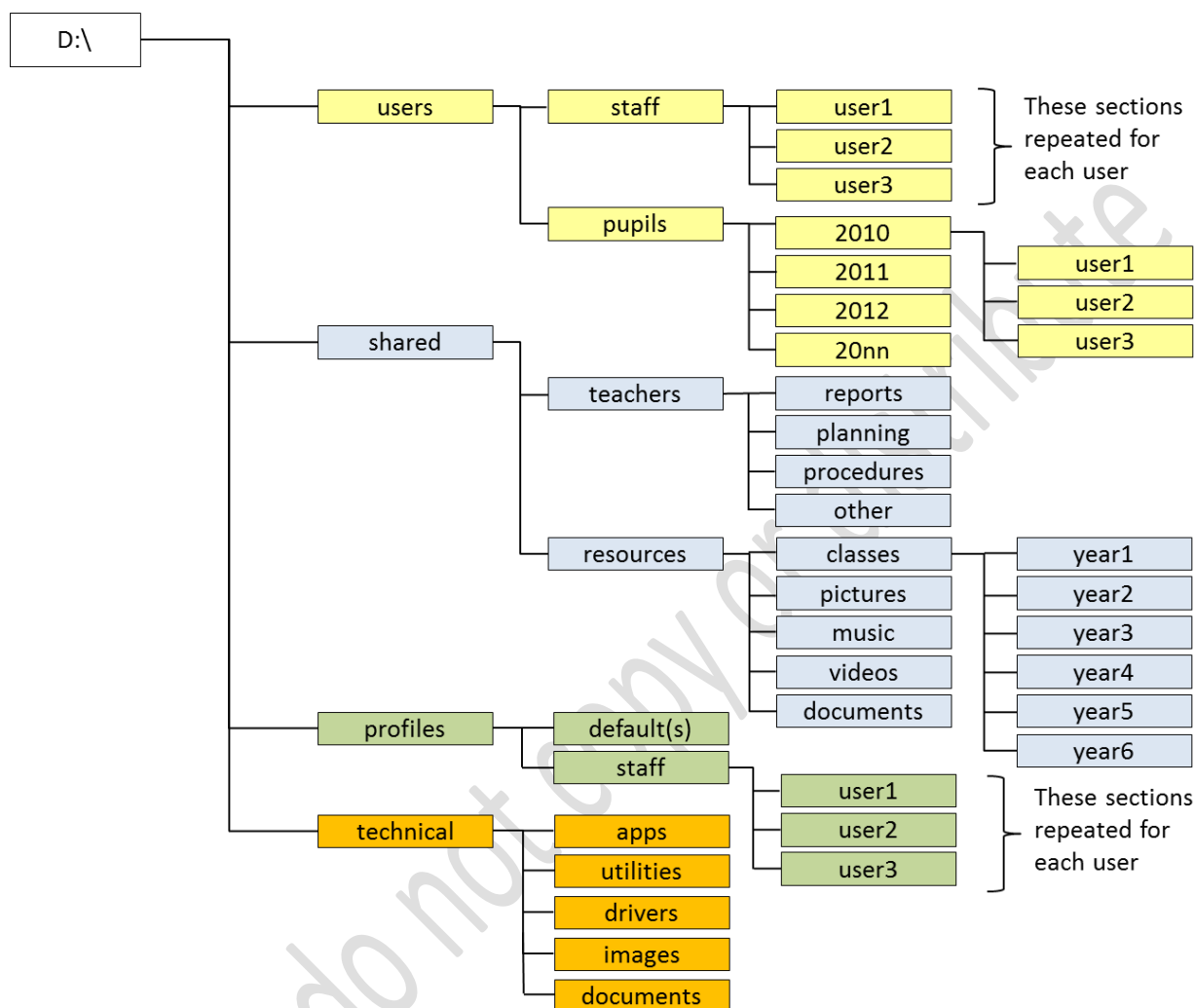
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies>Password Policy

Change *Minimum password length* to 0 characters and *Password must meet complexity requirements* to Disabled. Change *Maximum password age* to 0. Change *Minimum password age* to 0.

⁹ Obviously if there are no infants in the school then there is no need to create Year 1 and Year 2.

Folder Structure and Shares

The basic design principle is that the operating system files are located on one drive (the System drive) and everything else is located on the other drive (the Data drive). On the data drive the following folder structure should be created:



The roles of the folders are as follows:

Folder Name	Purpose
profiles	Top-level folder for user profiles. Staff have their own folders to support roaming profiles, whereas pupils share default folders that contain mandatory profiles.
users	Holds all the individual home folders for the users. These are grouped into staff and pupils.
shared	Holds data that is shared amongst groups of users.
teachers	Shared folder that can be seen by all staff and only by staff. Used for storing planning information, lessons reports and other information that children don't need or shouldn't see.
resources	Contains information to be shared throughout the school, grouped into four main folders. Staff have read-write access to and pupils have read-only access to: pictures, music, videos and documents. A further folder – classes – contains read-write folders for each class and enable teachers to distribute items to their pupils plus provide an area where the children can work on groups projects etc.
technical	Used by ICT technicians only. Consists of apps (master copies of software); utilities (Acrobat, Flash, QuickTime etc.); drivers (sound, video, printers etc.); images (disc images i.e. 'Ghosts'); documents (documentation for the network plus copies of software licences etc.).

The 'Technical' folder should be populated with items that will be of use in managing the network. Create six folders as follows:

Folder Name	Purpose
Apps	Master copies of applications e.g. Office, educational programmes. Anything that will need to be installed on the workstations.
Drivers	Hardware device drivers e.g. printer drivers.
Utilities	Anti-virus software, Acrobat, Flash players and so on.
Images	Disc images of machines created using PING or Ghost.
Updates	Updates and service packs etc.
Documentation	Any information pertaining to the network e.g. licences, lists of machines, records of IP addresses and so on.

Similarly, the 'Teachers' folder should be given some structure:

Folder Name	Purpose
Reports	Repository for term/annual reports of children
Planning	Contains curriculum and planning documents
Procedures	Details of procedures and processes, useful forms and so on
Other	A container for documents that teachers wish to share among themselves

Having created the folder structure, a number of shares need to be setup:

Folder name	Share name	Notes
D:\profiles	profiles\$	Should be a hidden share. Give Full Control to Everyone
D:\users\pupils	pupils	Give Full Control to Everyone
D:\users\staff	staff	Give Full Control to Staff group and Administrators
D:\shared\teachers	teachers	Give Full Control to Staff group and Administrators
D:\shared\resources	resources	Give read access to Everyone Give Change and Read access to Staff Give Full Control to Administrators
D:\technical	technical\$	Should be a hidden share. Give Full Control to Administrators

Shares are made hidden by placing a dollar sign (\$) at the end of the share name. Right-click on the folder and choose **Properties > Sharing**. Click on the **Advanced Sharing** button. On the next panel click the **Share this folder** box. Specify the share name; this will default to the name of the folder but by adding a \$ sign at the end (e.g. *hiddenfolder\$*) it will become a hidden share. Click on Permissions and then **OK** etc. and close the dialogue box.

Optional:

The individual class folders in D:\shared\resources\classes are read-only. However, if the school desires they can be made read-write to enable pupils to update them and collaborate on work.

Login Scripts and Drive Mappings

Login scripts are executed when the user logs on and can be used to map drives. This functionality can be achieved via several means but the simplest method is via a batch file.

Create three batch files, named **pupil.bat**, **teacher.bat** and **admin.bat** (contents shown below). These should be placed in *C:\Windows\sysvol\sysvol\domainname.local\scripts* where *domainname.local* is the name of the domain. This folder is automatically mapped by the server as a share called NETLOGON.

The drive mappings should not be changed from those shown. Also, note that S: is reserved for sites where SIMS may be installed and should therefore never be used.

Batch file for pupils – pupil.bat

```
@echo off
: Pupil logon script
: Updated 11/11/11 by NR
:
: Map shared resources drive
net use r: \\server\resources /persistent:no
```

Batch file for teachers – teacher.bat

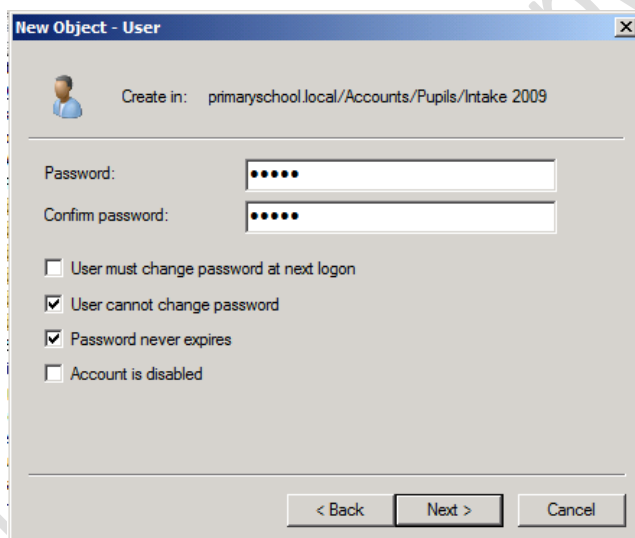
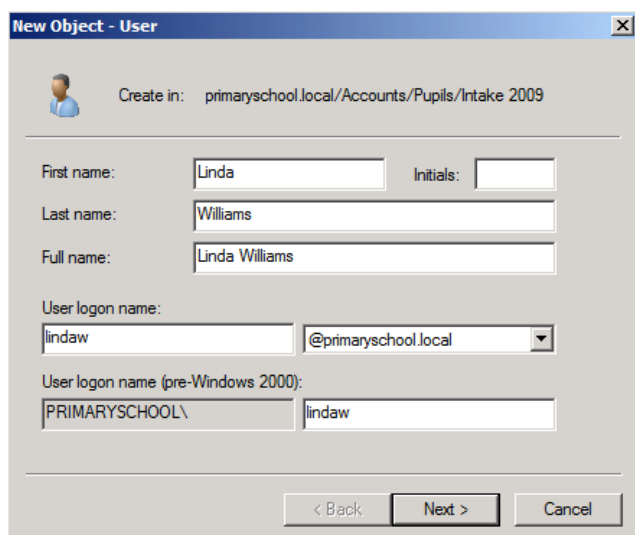
```
@echo off
: Teacher logon script
: Updated 11/11/11 by NR
:
: Map shared resources and teachers drive
net use r: \\server\resources /persistent:no
net use t: \\server\teachers /persistent:no
```

Batch file for Administrators – admin.bat

```
@echo off
: Admin logon script
: Updated 11/11/11 by NR
:
: Map shared resources, teachers and technicians drive
net use r: \\server\resources /persistent:no
net use t: \\server\teachers /persistent:no
net use z: \\server\technical$ /persistent:no
```


Creating Users

Individual users can be created using **Active Directory Users and Computers** or the **Active Directory Administrative Centre**. This document assumes the former, which will be more familiar to anyone accustomed to Windows Server 2003 or other early versions. Make sure the correct Organisation Unit is highlighted on the left-hand side¹⁰ (e.g. Staff) and choose **Action > New > User** from the menu. Complete the details along the following lines and in accordance with the naming standards described elsewhere in this document.



Click **Next** then enter the password characteristics as shown (User cannot change password, Password never expires).

Creating users can be time consuming – allow about an hour per class including the steps in next section. Unsurprisingly, tools are available to bulk-create users. A free one comes with Windows Server; it is called *csvde.exe* and is located in the C:\Windows\System32 folder. The basic principle is that a CSV containing the names of the users and other information is created in Excel – these names can be generated from the school’s SIMS application. Or, if this is a replacement network, a list of user names can be exported from Active Directory on the old system using *csvde.exe*. This CSV is then imported into Active Directory using *csvde.exe*. However, the tool is fairly basic and some work is still required.

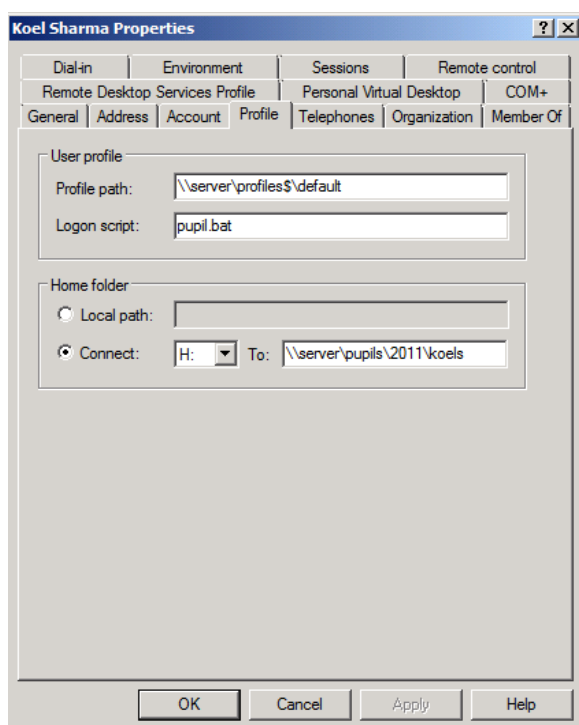
¹⁰ This is simply a convenience to help keep tracks of things. Users can actually be created anywhere and then dragged later into the correct OUs.

Modify User Details

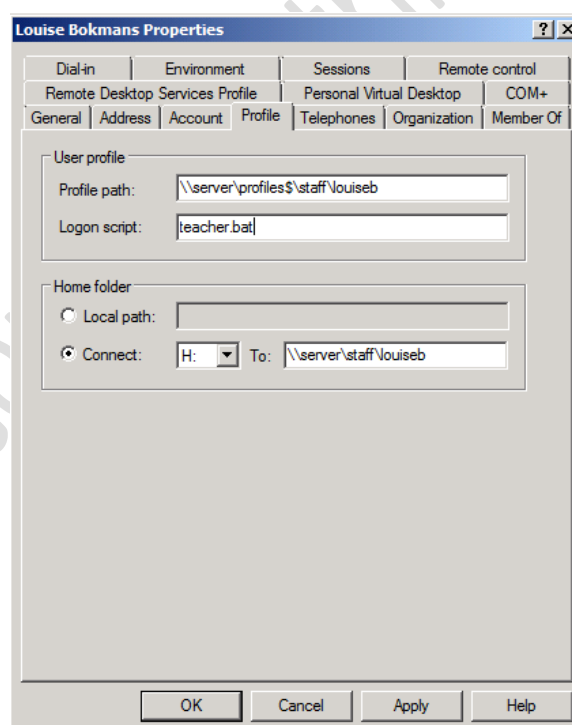
Each user should now be modified to specify the appropriate login script and profile. Use **Start > Administrative Tools > Active Directory Users and Computers**. Bring up the user's details, click on the Profile tab and specify the Login script; for a pupil this should be *pupil.bat*, for a teacher it should be *teacher.bat*, and for an administrator it should be *admin.bat*. Next, specify the home folder by clicking on the **Connect** option. Specify the **H:** drive and give a value of `\\server\staff\username` for a teacher or `\\server\pupils\cohort\username` for a pupil.

Examples: `\\server\staff\louiseb` for a teacher and `\\server\pupils\2011\koels` for a pupil

Specify the Profile path. For pupils, a *Mandatory Profile*¹¹ is used, in which case the Profile path will be `\\server\profiles$\default` or `\\server\profiles$\yearN`. For staff, they should have their own roaming profile, in which case the Profile path will be `\\server\profiles$\staff\staffname` (where *staffname* is the user login name). Information on creating mandatory profiles can be found in Appendix C.



Details for a pupil



Details for a teacher

Then, click on the 'Member Of' tab and assign the correct group membership. Having done this click on **Apply** and **OK**. Note that some characteristics can be applied to multiple users simultaneously e.g. the Logon script and the Profile path. Select the users, right-click and choose **Properties**. It is also suggested that this is used to set the Description field to the name of the year group or teacher.

¹¹ Teachers have conventional roaming profiles, enabling them to have a personalised computing environment that follows them from machine to machine. Students have mandatory profiles, giving them a consistent computing environment regardless of which machine they use. Mandatory profiles have three great advantages for schools when compared with roaming profiles; firstly, pupils cannot make any permanent changes to them as they are effectively 'read only' profiles; secondly, they can be shared, meaning that all users (or a group of users) can be given an identical configuration (desktop, wallpaper, Start Menu and so on). Thirdly, mandatory profiles are usually smaller than roaming profiles, meaning that logon and logoff times are faster, which is of particular benefit in wireless networking environments.

Specifying Proxy Settings Using Group Policy

Computers in primary schools are not usually connected directly to the internet; rather, all internet activity goes through proxy servers operated by or on behalf of the LEA.

The proxy settings for Essex are:

cache.essex.sch.local - ports 8080¹²

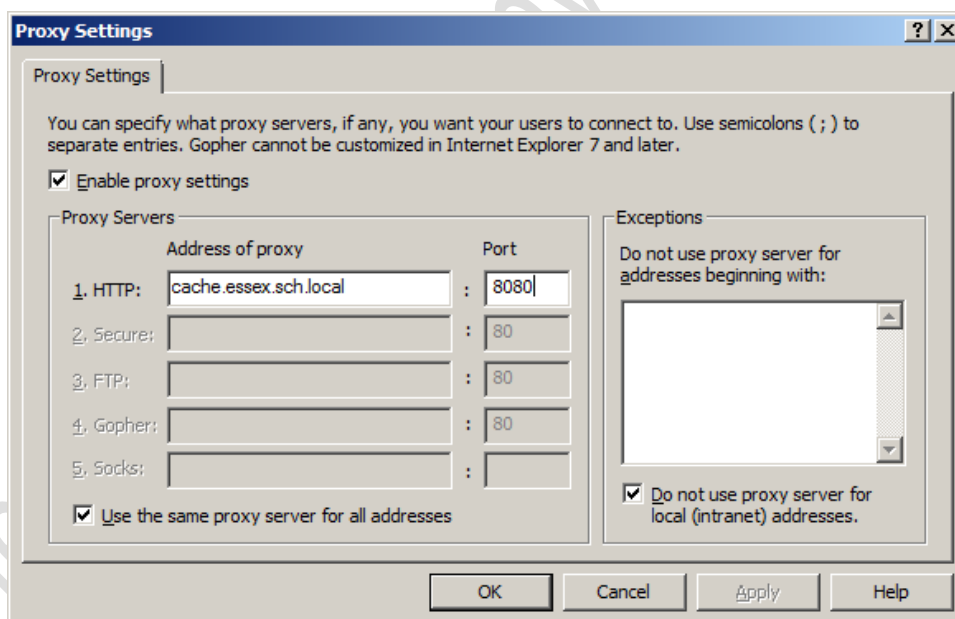
The proxy settings for Herts are:

wf3.thegrid.org.uk - port 80 for HTTP
wf3.thegrid.org.uk - port 80 for Secure
proxy.intra.thegrid.org.uk - port 3128 for FTP

The most effective way to put these settings on the computers is through Group Policy. Click on **Start > Administrative Tools > Group Policy Management**. Right-click the Default Domain Policy and choose **Edit**.

Drill down to: User Configuration > Policies > Windows Settings > Internet Explorer Maintenance > Connection > Proxy Settings

Double-click on **Proxy Settings** to display the following panel, complete it using the values above (this example is for Essex schools) then click on **OK**:



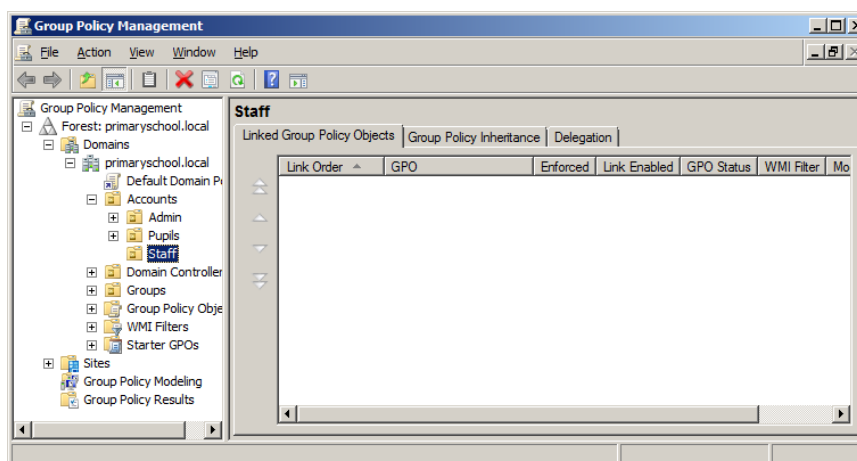
When finished, close down Group Policy.

¹² Port 8080 is normally used. However, teachers may benefit by being on port 8084, which has less filtering.

Specifying Home Page Using Group Policy

Group Policy can be used to specify different settings for Staff and Pupils in many areas relating to access and rights. A fuller discussion is outside the scope of this document; this simple example uses Group Policy to define different home pages for staff and pupils.

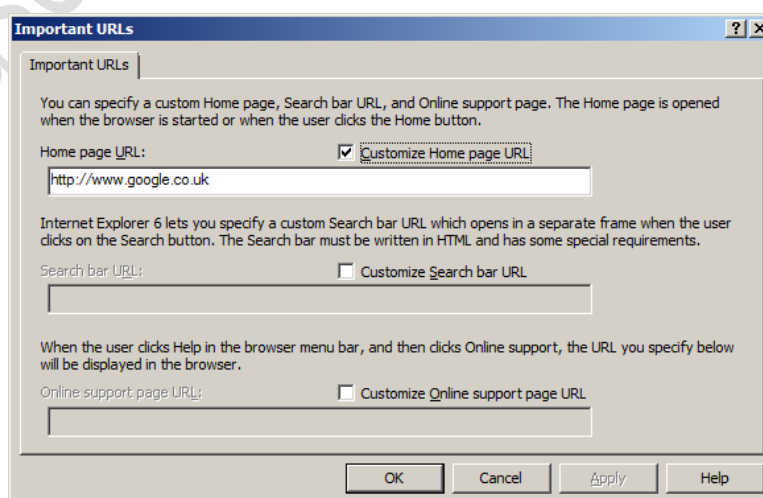
Launch Group Policy Management. Expand the tree to display the Organisational Units created earlier (see below); right-click on Staff and choose **Create a GPO in this domain, and link it here**.



Call the new GPO 'Staff Internet Home Page' and click on OK. Right-click on the new GPO and choose **Edit**. Drill down to: User Configuration > Policies > Windows Settings > Internet Explorer Maintenance > URLs > Important URLs

Specify the Home page URL. Note that the full URL must be specified e.g. <http://www.outlook.com> (this is the home page for the Office 365 email system). Click on OK.

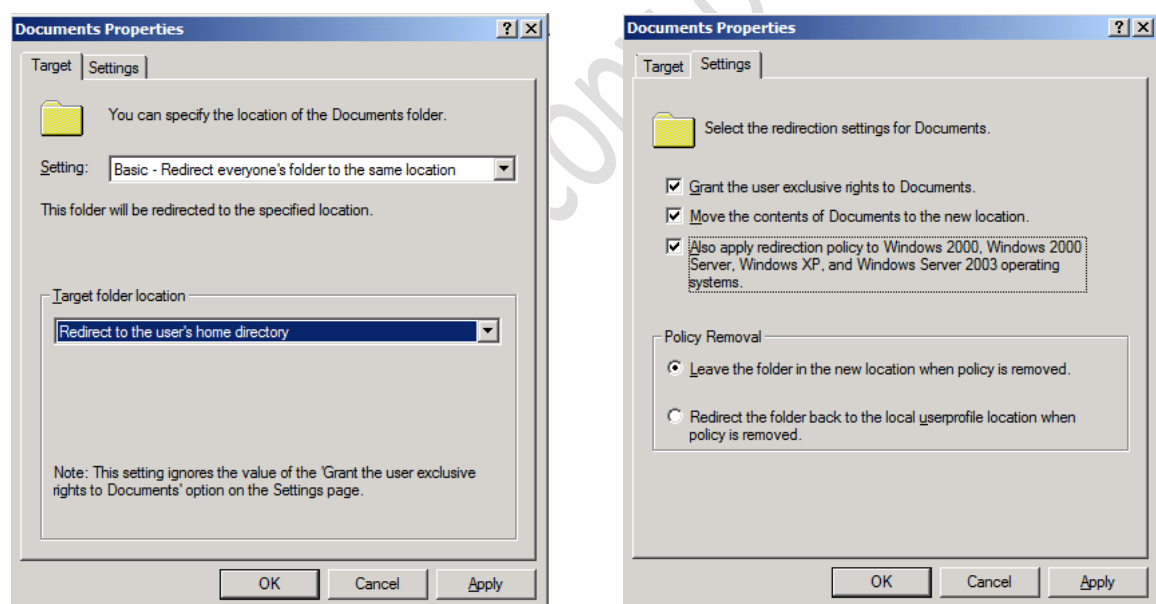
Now basically repeat the steps. This time right-click on Pupils and choose **Create a GPO in this domain, and link it here**. Call the new GPO 'Pupil Internet Home Page' and click on OK. Right-click on the new GPO and choose **Edit**. Drill down to: User Configuration > Policies > Windows Settings > Internet Explorer Maintenance > URLs > Important URLs. Specify the URL of a home page suitable for children e.g. www.google.co.uk (or Espresso is a good choice if the school uses it). Again, remember that the full URL must be specified e.g. <http://www.google.co.uk>. Click on OK.



Redirect the 'My Documents' Folder and Enable Offline Working (Optional)

The purpose of this is to redirect the user's 'My Documents' folder to their home drive (H:). By doing so, any files the user creates will automatically be stored on the network and be available from any computer. The effect of redirecting the home folder also means that offline folders will be enabled for users e.g. staff with laptops will have copies of the files in their home folders available when they are working offsite. However, note that redirection and offline folders frequently have problems associated with them and for this reason this section is optional.

- Launch Group Policy Management
- View the Settings for the Default Domain Policy
- Edit User Configuration
- Expand to *User Configuration\Policies\Windows Settings\Folder Redirection\Documents*
- Right-click the Documents line and choose Properties
- On the Target tab, change the Setting to 'Basic - redirect everyone's folder to the same location' and the Target folder location to 'Redirect to the user's home directory'.
- Click **Apply**, then click on the Settings tab.
- Make sure it looks as shown below. If Windows XP is in use at the site, ensure the box for Windows XP and other earlier operating systems is ticked. Then click on **Apply** and **OK**.
- A warning message may be displayed. This can safely be ignored – just click on **Yes**.



An additional step may be needed for best results and to ensure that Windows 7 clients also work correctly:

- Launch Group Policy Management
- View Settings for the Default Domain Policy
- Expand to *Computer Configuration\Policies\Administrative Templates\Network\Offline Files*
- The setting for *Allow or Disallow use of the Offline Files Feature* should be set to **Enabled**.
- The setting for *Subfolders always available offline* should be set to **Enabled** if Windows XP machines are in use

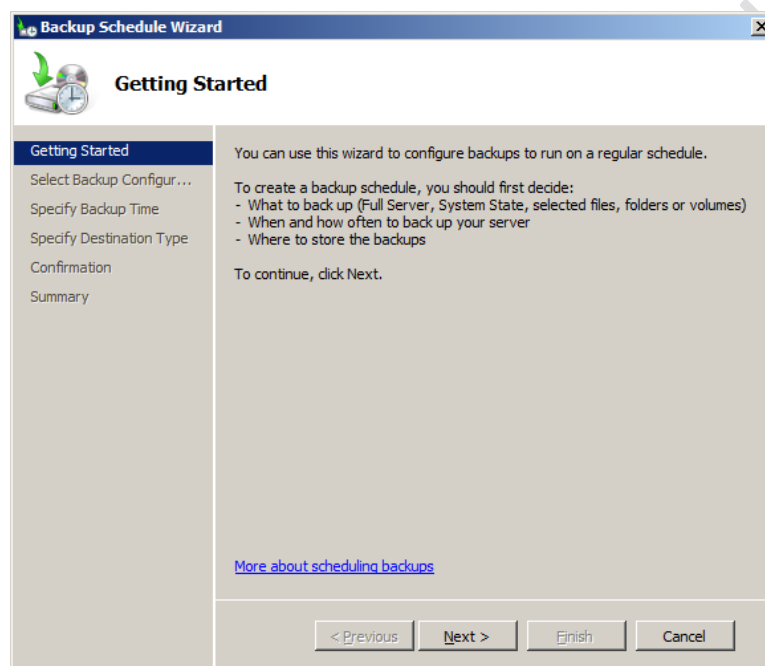
Server: Backups and System Management Tools

Installation of Windows Server Backup

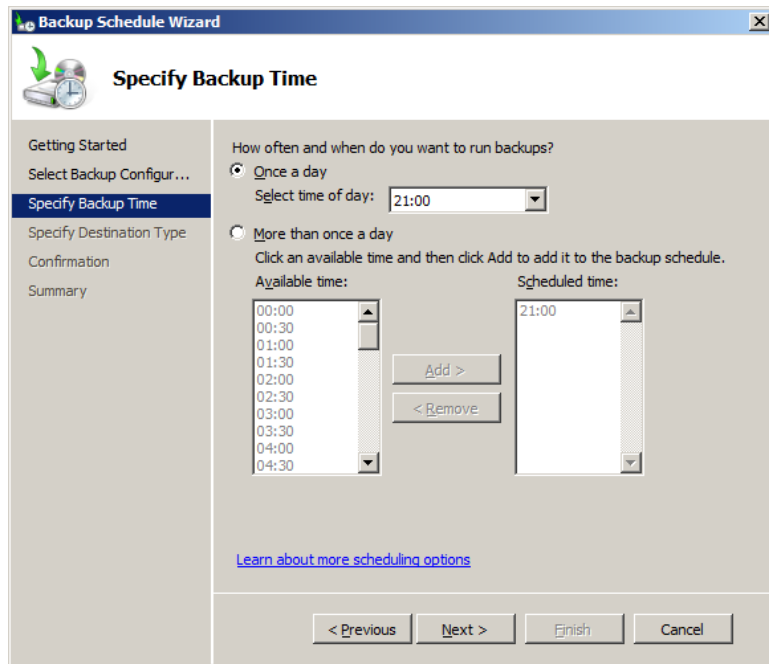
The server is backed up using Windows Server Backup. This is a standard component of Server 2008 R2 but first has to be installed. To do so, use **Start > Administrative Tools > Server Manager**. Click **Add Features** and then select **Windows Server Backup Features**. Follow the instructions.

Running Windows Server Backup for the First Time

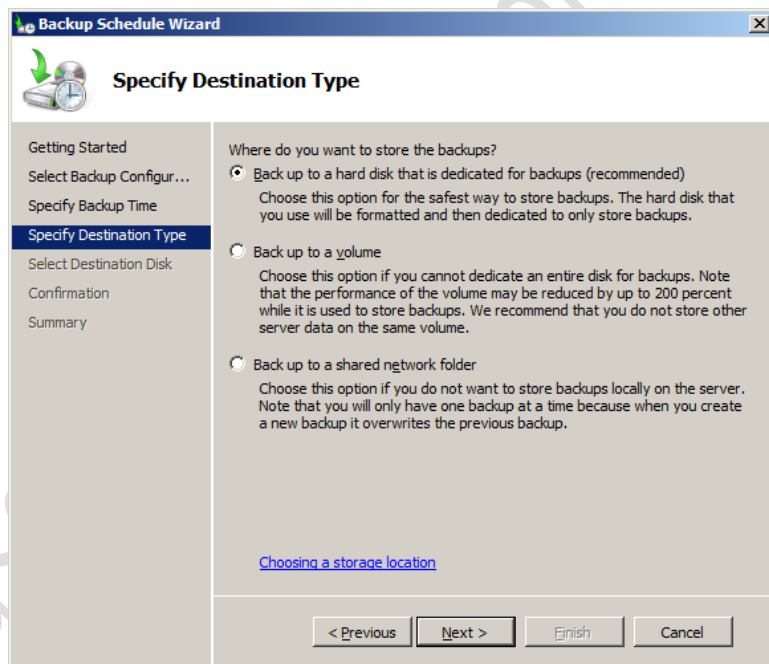
Click on **Start > Administrative Tools > Windows Server Backup**. If it is being run for the first time the following message is displayed: “No backup has been configured for this computer. Use the Backup schedule wizard or the Backup Once Wizard to perform a regular or one-time backup.” Accordingly, click on **Backup Schedule...** on the **Actions** panel and the following screen will be shown:



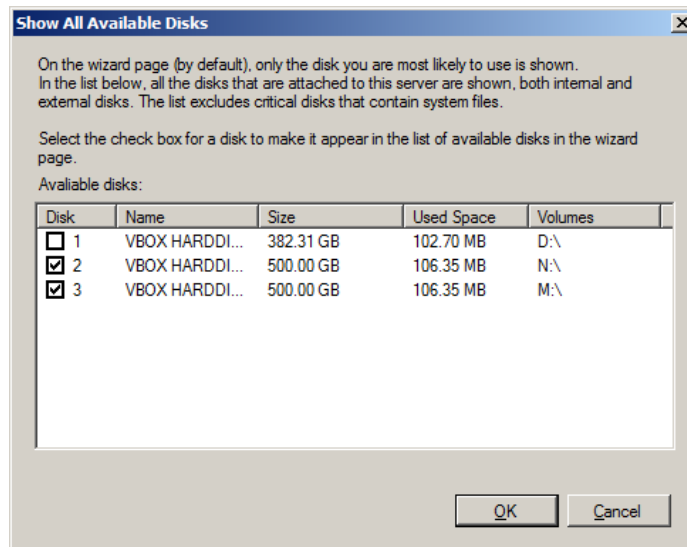
Click on **Next**. The following screen allows you to choose between a ‘Full Server’ or a ‘Custom’. Choose the former and click **Next**. On the next screen the backup time and frequency are shown; the default is 21:00 (9pm) once a day, which is fine so click **Next**:



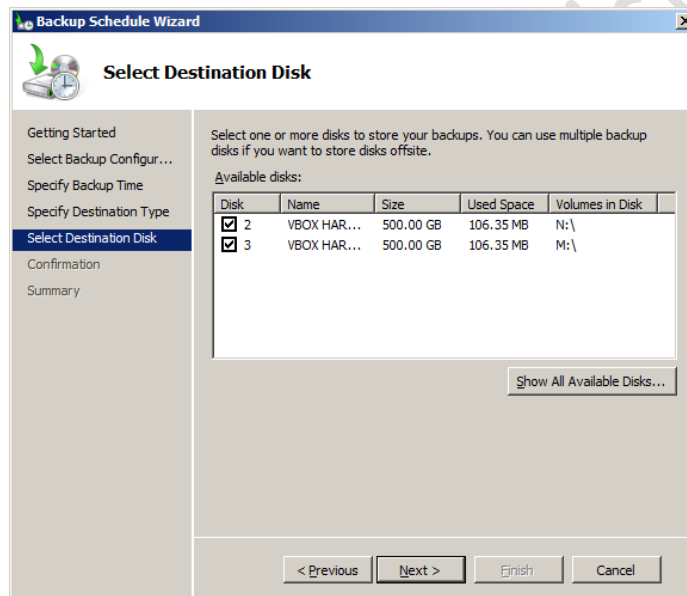
The destination of the backup is specified on the next screen. Usually the first option – backing up to an external hard drive – is used.



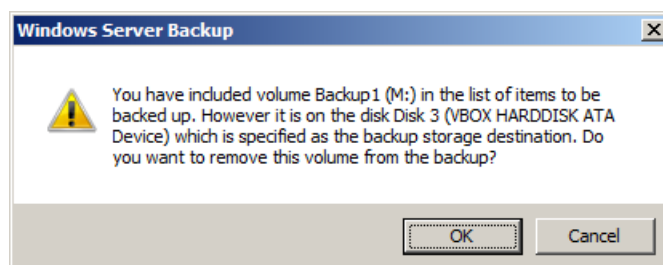
Plug-in the external hard disks, make sure that Windows has recognised them, then click **Next** to show this screen:



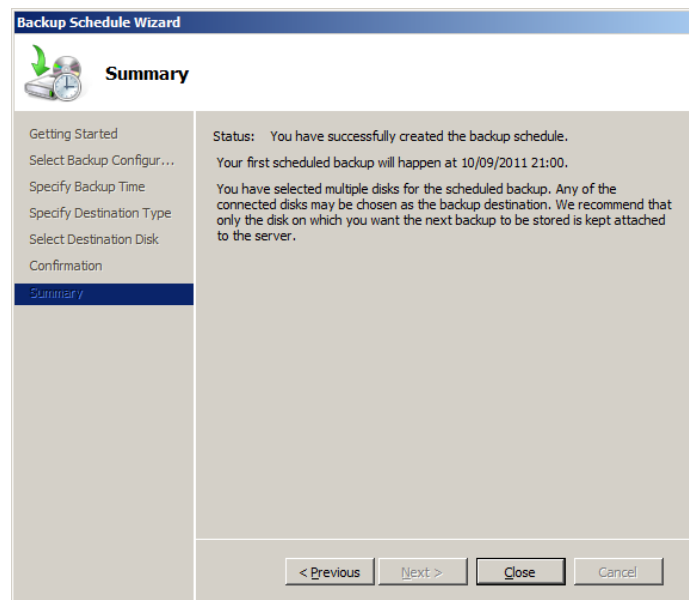
Tick the external drives to be used and click **OK**



Click the disks to be used and then click on **Next**. The backup program might detect that the external drives will be *included* within the backup rather than as backups, which you do not want. If the following message is received click **OK**.



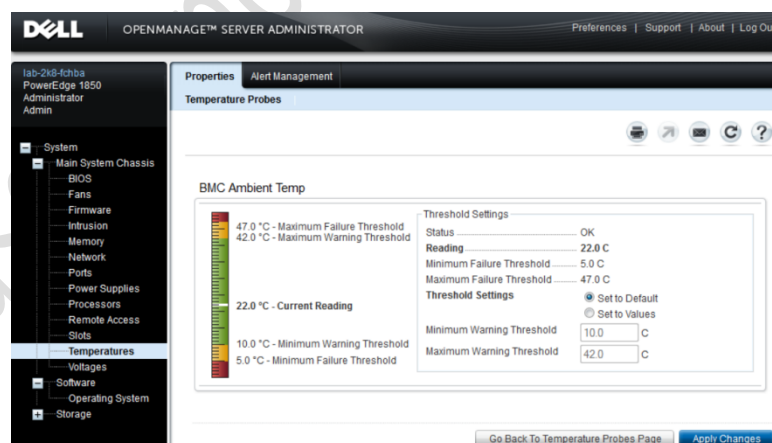
There will be a warning about formatting – note that backup disks use a special file system that is not visible to regular Windows. It is not possible to plug a backup disk into a standard Windows computer and read it like a normal USB drive once it has been formatted for backup purposes. Click on **Yes** then click on **Finish** on the Confirmation screen that follows. The backup drive will be formatted, which may take some time depending on its capacity. Eventually a Summary screen will be displayed:



Note that it doesn't really matter which backup drive is used at any time; the way the backups work mean that any drive will have a complete up-to-date after the backup job has been completed. However, it makes sense to swap the backup drives on a regular basis, daily or weekly depending on local circumstances (that is, availability of a person to swap the drives). The drive that is not in use should be unplugged and kept in a safe location and away from the server.

Install Server Management Software

Most mainstream server suppliers provide some form of management software to help monitor and manage the health of the server hardware e.g. the RAID sub-system, operating temperatures etc. For instance, the Dell software is OpenManage. This should be installed once the main build is complete. If a password is required, use the main Administrator one.



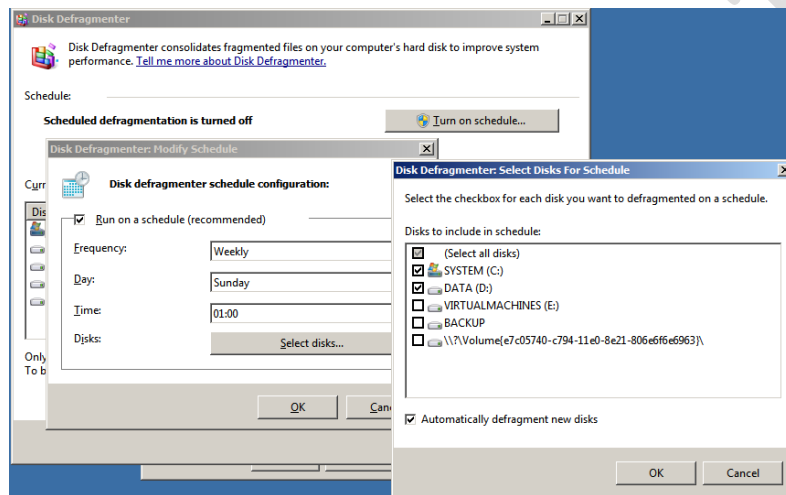
Install Wireless Management Software

Some wireless systems are managed using a web page whereas others require the installation of a utility program (e.g. Apple AirPort, D-Link DWL-3200AP), in which case it can usefully be installed on the server.

Configuring Defragmentation for the Server Hard Disks

To help ensure that they are performing at peak performance, the hard disks on a file server should be defragmented on a regular basis. To do so:

- Click on **Start > Computer**
- Right-click on one of the drives (it doesn't particularly matter which) and choose **Properties**
- Click on the **Tools** tab then click on **Defragment now**
- Click on the **Turn on schedule** button
- A panel pops up – tick the **Run on a scheduled** box. Specify a suitable frequency e.g. weekly on a Sunday at 1.00am
- Click the **Select disks** button. Choose the main disks (usually this will be C: and D:) then click **OK**.
- Close down the dialogue boxes.



Enable Shadow Copies

The Shadow Copies feature of Windows Server 2008, in conjunction with the “Previous Versions” feature in Windows 7, allows for the easy recovery of earlier versions of data files created by users without having to restore from the main backups.

To enable:

Click **Start** > **Administrative Tools** > **Share and Storage Management**

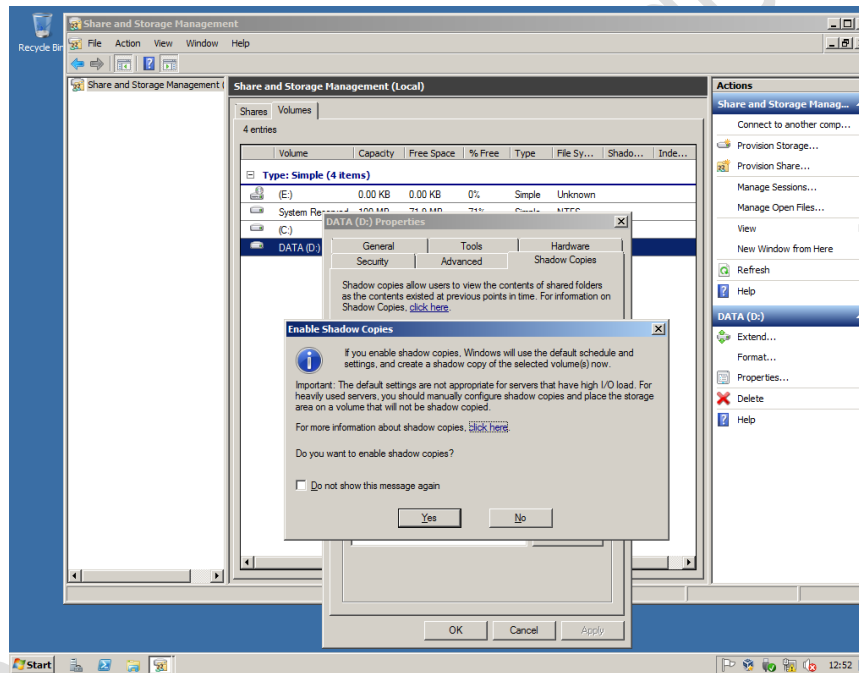
Click on the **Volumes** tab

Right-click on the **D:** drive and choose **Properties** (in fact, you can click any drive)

Click on the **Shadow Copies** tab

Click on **D:** and click **Enable**

A warning message is displayed (see below). Click on **Yes**

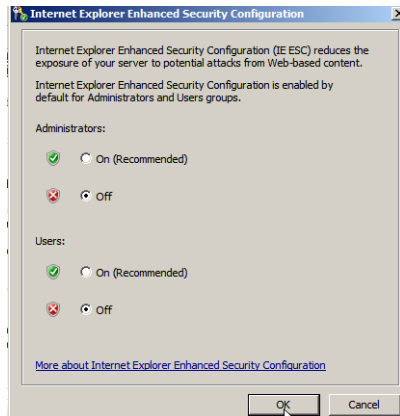


To avoid any performance issues, the default settings should be used. These will cause shadow copies to be taken twice a day, at 7:00am and 12:00pm.

Next Steps, Tidying Up and Miscellaneous Activities

Disabling Internet Explorer Enhanced Security

By default, in Windows Server 2008 Internet Explorer has limited internet connectivity due to a feature called *Internet Explorer Enhanced Security* being enabled. There are good reasons why general Internet browsing is not a good idea on a server, but not being able to access the Internet freely makes things difficult. It is therefore useful to disable Enhanced Security:



Start **Server Manager** by clicking the **Server Manager** icon on the Taskbar, or the **Server Manager** via the **Administrative Tools** menu in the **Start** menu. Now scroll down to **Security Information** within **Server Summary** and click **Configure IE ESC**. In the window that pops up select **Off** for both **Administrators** and **Users**. Save the changes by clicking **OK**.

Install Anti-Virus Software

Anti-virus should be installed on the server at the earliest opportunity, and on the workstations. Instructions on how to do this using AVG Business Edition can be found in Appendix D.

Setup Alternative Administrator Account

For a variety of reasons it is not good practice to use the Administrator account any more than necessary: firstly, in case the account accidentally gets locked or disabled. Secondly, it can be confusing with Windows 7 clients, which prefer to use the local account with that name. Instead, an alternative administrative account should be setup and, once the server has gone live, this is the one that should be normally used. It is recommended to setup an administrative account called *ittechnician* and use it whenever possible. To create it:

- Click on **Start > Administrative Tools > Active Directory Users and Computers**
- Expand tree on left-hand side of screen to show Users
- Right-click on Administrator and choose **Copy**
- Complete the dialogue box. Set the password to the same as Administrator

Apply Windows Updates to the Server

Go into Windows Update (**Start > All Programs > Windows Update**), check for updates and apply them. After the server is fully up-to-date, adjust the settings so that it looks for updates but does not apply them automatically (this is to help avoid surprises and unplanned reboots).

Activate Windows

It is necessary to activate Windows on the server. To do so, click on **Start** then right-click on **Computer** and choose **Properties**. Approximately $\frac{3}{4}$ down the screen is the section to Activate Windows.

Restore Old Data

If there is an existing file server, the important data on it should be identified and copied to an external USB drive. Typically, this will comprise user data, shared information, master copies of software, profiles. Great care should be taken to avoid spreading any viruses from the old system and the following approach is suggested:

- Run a complete anti-virus scan on the old server
- Install Malwarebytes on the old server and run it
- Copy the data to the external USB drive
- Plug the external USB drive into a standalone PC that is known to be 'clean'
- Run an anti-virus scan on the external USB drive
- When satisfied, copy the data onto the new server
- Run a full scan on the new server

The data should be restored according to the new folder structure, not the one from the previous environment. This may necessitate copying the items to a temporary 'Lost and Found' folder and then redistributing it to the proper folders. In the event of any questions or ambiguity, input should be sort from the ICT Co-ordinator.

Note that when the data has come from a server that was running Ranger then some additional effort may be required. Ranger uses non-standard folders for user data, for instance it may have created additional *My Documents* and *My Work* folders, and this is now an opportunity to put things in the correct place.

Installing Printers

In the past it was common to use the server to manage printing. Print jobs would be spooled onto the server, which would then hand them out to the printer(s). In some instances, the printers would be physically connected to the server with a USB or parallel connection. This approach has some advantages in terms of central control, but has two particular disadvantages. Firstly, it creates a workload for the server. Secondly, in an environment that uses multiple workstation operating systems (Windows XP, Windows Vista, Windows 7 32-bit, Windows 7 64-bit), there can be considerable difficulties in ensuring that the right drivers are deployed. Because of these considerations and because most printers are now IP-based, it is recommended that workstation-based printing is used. Using this method the printers are installed locally on each workstation and there is no server involvement as such. The basic technique is:

- Download the appropriate drivers and store them on the server in the *technical* share
- Visit each individual computer, login as an administrator and choose add a printer
- Specify the printer as being on a TCP/IP port. Provide the static IP address of the printer
- When prompted for a driver, point at the technical share on the server
- Set the printer as the default printer
- Change any defaults if necessary (e.g. paper size to A4)
- Remove any superfluous virtual printers (e.g. OneNote, fax, XPS etc.)
- Print a test page to verify correct operation

If this method is used then some effort can be saved by installing the printer as part of the initial disc image(s) for the workstations.

Check Logins

As many user logins as possible should be checked to make sure that they are working correctly. Check that they have correct access to their folders, can get on the Internet and are able to print. Any anomalies should be investigated and resolved.

Test Remote Desktop

During installation, Server 2008 R2 will automatically have configured Remote Desktop. To test, go to any workstation, login and launch Remote Desktop. Verify that you can connect to the server. If the server is to be used headless from now on – recommended – the screen, keyboard and mouse can be removed.

Windows 7 Logon Behaviour

By default, Windows 7 clients display the name of the last person to use the computer. This can be confusing, as it necessary for the next person using it to specify “Logon as other user”, which is a difficult concept, particularly for small children. However, this behaviour can be changed, such that a blank user name and password are presented to users. This is done through Group Policy.

On the server, open Group Policy Editor. Right-click the Default Domain Policy and choose **Edit**. Drill down to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options**. Find **Interactive login** and Enable **'Do not display last user name'**.

Logon Warning/Security Message

Group Policy can be used to specify a message that appears at the logon screen. For instance, the message could state the name of the school (“Primary School Network”) along with an advisory or warning message (“Do you not attempt to use this computer system unless you have been authorised to do so”). There are two entries that need to be set: one for the title and one for the message itself.

On the server, open Group Policy Editor. Right-click the Default Domain Policy and choose **Edit**. Drill down to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options**. Find **Interactive login** and edit **'Message title for users attempting to logon'**. Then, edit **'Message text for users attempting to logon'**.

Install Internet Explorer 9 on Server

If Internet Explorer 9 is used on any workstations, then it should also be installed on the server as the act of doing so will add group policy support for it.

Connecting Clients to the Domain

To connect to the domain the client computer must be running a 'Professional' version of Windows, such as Windows XP Professional, Windows 7 Professional, Windows 7 Enterprise or Windows 7 Ultimate. The following operating systems are not supported: versions prior to Windows XP; home editions of any operating system; Windows Vista; Apple Macintosh; any Linux variants.

The client needs to have had recent Windows updates applied; specific requirements include: NET 4 Framework Client Profile¹³; Service Pack 1 (Windows 7 clients); Service Pack 3 (Windows XP clients); Group Policy Client Side Extensions KB943729 (Windows XP clients).

Based on experience and to minimise problems, the preferred approach is to start afresh and create brand new images for the workstations, thereby ensuring consistency and avoidance of any historical issues. If this is not possible then the existing workstations will first need to be removed from the old domain and then added to the new one. If the previous network was running Ranger then the Ranger client will need to be removed. This can be done by logging in to the old domain from each workstation using the RangerRemove account; if this is problematic e.g. because the old server is not available then follow the instructions at:

<http://johnreid.it/2009/10/27/uninstall-ranger-from-a-computer-without-the-rangerremove-user/>

Creating a Master Image

The first stage is to build a master image for each of the most common type of PCs used by the school. This image typically consists of:

- The operating system e.g. Windows 7 Professional
- The current service pack for the operating system e.g. SP3 in the case of Windows XP
- The latest Windows updates
- Any drivers that might be required (screen, network, sound etc.)
- Internet Explorer 8
- The version of Microsoft Office licensed by the school e.g. Office 2010
- The current service pack for Microsoft Office e.g. SP2 in the case of Office 2007
- Current Flash and Shockwave players
- An agreed selection of the most popular education programs used by the school (for guidance, this is usually no more than about 5 or 6)

The local Administrator password should be set the same as the Administrator's server password. Name the computer as 'changeme'.

The master image should be copied to a portable USB hard disk or large capacity USB memory stick using the free PING¹⁴ utility. A copy of it should be retained on the network in the 'technical' area.

¹³ If this is a teacher or admin PC that will be running SIMS then the full NET 4 client has to be installed.

¹⁴ PING (a recursive acronym meaning 'PING Is Not Ghost') can be downloaded from <http://ping.windowdream.com/>. It can be run from DVD or a bootable USB version can be created using instructions located at <http://ping.windowdream.com/forum/viewtopic.php?f=7&t=7037>

Imaging of PCs

Each PC should be imaged using PING. Typically, this process will take between 10-60 minutes depending on the size of the image and the performance of the media and computer.

After a PC is imaged it can be finalised and added to the domain. This process varies depending on whether the PC is running Windows XP Professional or Windows 7:

Windows XP Professional

- Run **NewSID** utility to generate new SID plus rename the computer
- Add to domain
- Test by logging in as Administrator
- Disable any GUEST or USER account
- Install anti-virus client

Windows 7 Professional

- Generate a new SID: **Start > Run > Sysprep** and run the Sysprep utility
- Set the 'System Cleanup Action' to 'Enter Out-of-Box' Experience (OOBE)' and tick 'Generalize'
- Make sure 'Shutdown option' is set to Reboot
- Run the Sysprep utility (it will take some time to complete)
- After the reboot complete the Country/Time/Keyboard screen
- Accept the EULA
- Rename the computer
- Add to domain
- Test by logging in as Administrator
- Install anti-virus client

Connecting a Windows 7 Client to the domain

- Click the **Start** button, right-click **Computer** and then click **Properties**
- Under 'Computer name, domain, and workgroup settings', click **Change settings**
- 'System Properties' are displayed. Make sure you are on the 'Computer Name' tab
- Click the **Change** button
- If prompted for an Administrator password or confirmation, answer it
- Under 'Member of' click on **Domain**. Enter the name of the domain (that is, the school name as defined on the server). Make sure it is followed by a suffix of *.local*. Click on **OK**.
- You will be prompted to enter the Administrator name and password for the domain
- After a short period (up to a minute) you will receive a 'Welcome to the domain' message
- Restart the computer
- Check that you can logon as Administrator

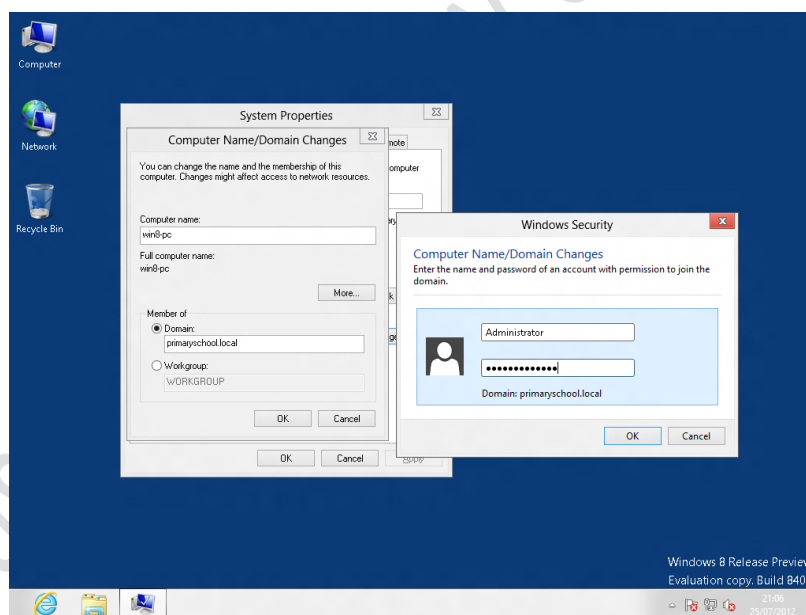
Connecting a Windows XP Client to the domain

- Click the **Start** button, right-click My **Computer** and then click **Properties**
- 'System Properties' are displayed. Make sure you are on the 'Computer Name' tab
- Click the **Change** button
- Under 'Member of' click on **Domain**. Enter the name of the domain (that is, the school name as defined on the server). Make sure it is followed by a suffix of *.local*. Click on **OK**.
- You will be prompted to enter the Administrator name and password for the domain
- After a short period (up to a minute) you will receive a 'Welcome to the domain' message
- Restart the computer
- Check that you can logon as Administrator

Connecting a Windows 8 Client to the domain

Although Windows 8 may not be particularly suitable for use in schools at this time, this section provides some notes on adding a Windows 8 client to the network in case this has to be done.

- When installing Windows 8, specify that it is to use a local ID rather than a Microsoft ID.
- When the computer gets network connectivity for this first time it will ask if it is a Home, Work or Public network. Choose Home or Work (it doesn't matter which).
- Press the **Windows Key + R** simultaneously to produce the Run box. Enter *SYSDM.CPL* and the standard System Properties box will be displayed. Add to the domain in the normal manner.



Note that the network logon screen for Windows 8 is different from that of its predecessors, which may be an issue in a mixed OS environment.

In most regards – with the notable exception of the Metro user interface – Windows 8 behaves much the same as Windows 7. Given the lack of a Start menu, it is suggested that desktop icons are used for providing access to user applications.




Appendix A: Installation Checklist

Ref	Activity	Date due	Who
1	Network design and hardware/software requirements completed		
2	Equipment and software ordered		
3	Equipment and software delivered and available		
4	Build server hardware; update BIOS and firmware		
5	Connect server to UPS and network switch		
6	IP details obtained and domain name decided		
7	Initial install of Windows Server 2008 R2		
8	Partition drives		
9	Add server role: Active Directory Domain Services		
10	Add server role: DHCP Server		
11	Add server role: File Services		
12	Enable Remote Desktop		
13	Configure DNS Settings		
14	Create Organisational Units (OUs) and Groups		
15	Change the password policy		
16	Create shared folders: Shared, Teachers, Technical and Profiles		
17	Create sub-folders within Shared (music, pictures, videos, classes)		
18	Create sub-folders within Teachers folder		
19	Create sub-folders within Technical folder		
20	Create login scripts/batch files		
21	Obtain list of users		
22	Create users		
23	Modify user details: profiles, login scripts, group membership		
24	Specify proxy settings using Group Policy		
25	Specify Internet Home page using Group Policy		
26	Use GPO to redirect home folders & enable offline files		
27	Install Windows Server backup and test		
28	Install server management software		
29	Install wireless management software		
30	Configure defragmentation for server hard disks		
31	Enable shadow copies		
32	Disable Internet Explorer enhanced security		
33	Install anti-virus software on server		
34	Setup alternative administrator account		
35	Apply Windows updates to server		

36	Activate Windows on server		
37	Transfer data from any previous network system		
38	Test logins for users (all teachers plus one pupil for each cohort)		
39	Test access via Remote Desktop		
40	Change Windows 7 logon behaviour		
41	Setup logon warning/security message		
42	Develop disc image(s) for workstations		
43	Image the workstations		
44	Create mandatory profiles		
45	Connect workstations to domain		
46	Populate the Technical folder		
47	Deploy anti-virus to workstations		
48	Printer installations		
49	Remove screen, keyboard and mouse from server		
50	Check for further Windows updates and set to manual check only		
51	Take full backup of server		
52	Communicate user details and passwords to teachers		
53	Arrange training and tuition materials for teachers ¹⁵		
54	Formal handover of network		
55	Arrange onsite presence for 'Go live' day		
56	Analyse issues ("snag list") and arrange resolutions/workarounds		
57	Formal review of network with ICT Co-ordinator & Head		
58	Decommission old server		

¹⁵ Appendix E contains an example of the sort of documentation that should be provided to teachers

Appendix B: Server Hardware Specifications

COMPONENT	Small School (around 30 concurrent users)	Medium School (around 50 concurrent users)	Larger School (around 100 concurrent users)
CPU	Intel Core i3-2100, 2C/4T, 3.10 GHz, 3MB cache	Intel Xeon X3430, 4C, 2.40GHz, 8MB cache	2 x Intel Xeon E5620, 4C, 2.40GHz, 12MB cache
RAM	8GB LV UDIMM	8GB LV UDIMM	16GB, LV UDIMM
HDD	2 x 1000GB SATA 7.2K RPM	4 x 500GB NLSAS 7.2K RPM	4 x 600GB SAS 15K RPM
RAID	PERC H200 C13 – RAID 1 (total storage 1.0TB)	PERC H700 C11 cabled – RAID 5 (total storage 1.5TB)	PERC H700A C10 cabled – RAID 5 (total storage 1.8TB)
DVD	16x DVD-ROM SATA	16x DVD-ROM SATA	16x DVD-ROM SATA
PSU	Built-in	Redundant PSU (2 x PSU)	Redundant PSU (2 x PSU)
NIC	Built-in	Broadcom® NetXtreme II 5709 Dual Port 1GbE NIC	Broadcom® NetXtreme II 5709 Dual Port 1GbE NIC
WARRANTY	3 year Basic Warranty NBD	3 year Basic Warranty NBD	3 year ProSupport and NBD onsite service
EXAMPLE	Dell PowerEdge T110 II (chassis for 4 x HDDs) 	Dell PowerEdge T310 (chassis for 4 x HDDs) 	Dell PowerEdge T410 (chassis for 6 Hot Plug HDDs) 
GUIDE PRICE	£786	£1823	£3707
UPS	APC Smart-UPS 750 LCD (ebuyer 226815) £186	APC Smart-UPS 750 LCD (ebuyer 226815) £186	APC Smart-UPS 1500 LCD (ebuyer 226810) £365
BACKUP	2 x Buffalo 1TB MiniStation portable hard drive (ebuyer 407013) £65 each	2 x Buffalo 2TB DriveStation external hard drive (ebuyer 260790) £93 each	2 x Buffalo 2TB DriveStation external hard drive (ebuyer 255189) £93 each
NOTES	Good value and capable entry level server	Adds better hard disks, better RAID, redundant PSU, dual LAN adaptors	Adds better CPU, more RAM, high performance hot swap disks, enhanced warranty

Servers direct from Dell. Prices are indicative only and exclude VAT. Last updated November 2012.

Appendix C: Creating Mandatory Profiles

Mandatory profiles have three great advantages for schools when compared with roaming profiles; firstly, users cannot make any permanent changes to them as they are effectively 'read only' profiles; secondly, they can be shared, meaning that all users (or a group of users) can be given an identical configuration (desktop, wallpaper, Start Menu etc.). Thirdly, mandatory profiles are smaller than roaming profiles, meaning that logon and logoff times are faster, which is of particularly benefit in wireless environments.

Although creating mandatory profiles under Windows XP was relatively straightforward, Microsoft's official solution for creating them with Windows 7 involves Sysprep and imaging and is rather complicated. This appendix describes a simpler, common process for both operating systems. However, as profiles are different between Windows 7 and Windows XP it is suggested that this process is done twice if both operating systems are used i.e. once on a Windows 7 machine, once on a Windows XP machine.

Step One: Create an Idealised Student Profile

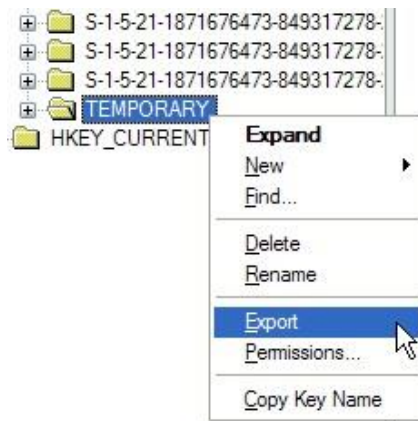
The first stage is to create a "perfect desktop". Ideally this should be done with a freshly imaged machine. It should not yet be part of the domain. Create a new local administrator account called **Student** and login as Student. Install all of the applications and Windows updates. Configure the desktop icons, wallpaper, Start Menu, toolbars, preferences etc. Make sure that any programs that have 'first run' requirements (such as Internet Explorer and Microsoft Office) have been run. Logoff and then logon again with the Student account and test everything. Then reboot and logon with another Administrative account.

Step Two: Configure the Student Profile for use by any user

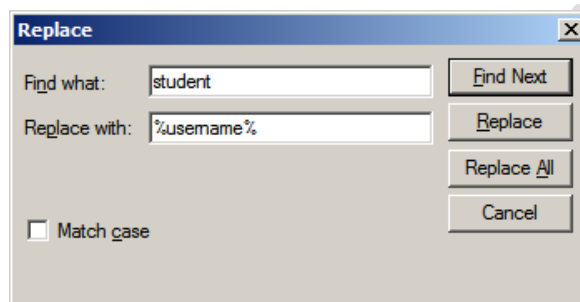
The newly created Student profile will have many hardcoded references to the 'Student' user within it. These have to be replaced with the system variable **%username%**. Then, whenever a user logs on using this modified profile, their name and user specific paths will be substituted automatically for the variable. Without this step the mandatory default user profile will not work properly.

A user profile is really a database of user specific registry settings and hence can be modified using the registry editor. Make sure you are logged on with a different local Administrator account (NOT the Student account):

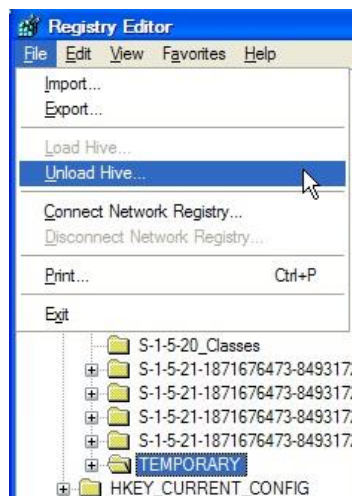
- Use **Control Panel > Folder Options** to 'Show hidden folders, files and drives' and deselect 'Hide protected Operating System Files'
- Open the registry editor by clicking **Start** and entering **regedit** in the Run box
- Click on HKEY USERS
- Choose **File > Load Hive** from the menu
- Navigate to the location of the newly created Student profile and open the *ntuser.dat* file. If using Windows 7 it is located at *C:\Users\Student*; if using Windows XP it is located at *C:\Documents and Settings\Student*. Note: there may be several *ntuser.dat* files. Some judgement is required but generally use the one which is largest and has most recently been modified.
- When the *ntuser.dat* is loaded, it will prompt for a 'Key Name'. Call it *TEMPORARY*.
- Right click on the TEMPORARY item and Export the file. Save it on the desktop with a name of *defaultregistry*



- On the desktop, right-click on the newly created *defaultregistry.reg* file and edit it using Notepad
- Use Edit > Replace and change all occurrences of *student* with *%username%*

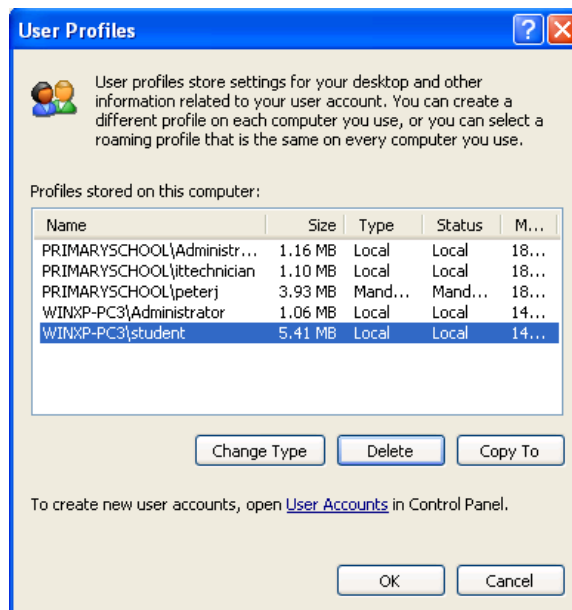


- Save the changes and exit Notepad
- Double-click the *defaultregistry.reg* file on the desktop to re-enter the changed data into the registry. A warning message will be displayed “Are you sure you want to add the information...” – click **Yes**
- Within regedit, choose File > Unload Hive... from the menu. Don’t worry about any warning messages – you do want to do this.
- Then close regedit and reset the viewing settings in Folder options. Also delete the file *defaultregistry* from the desktop.

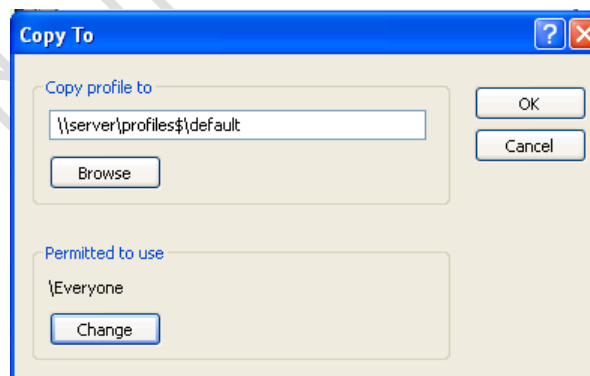


Step Three: Copy the Student Profile to a network share

- If using Windows 7... Click on Start then right-click on Computer and choose **Properties > Advanced system settings > Advanced tab > User Profiles > Settings** button.
- If using Windows XP... Click on Start then right-click on My Computer and choose **Properties > Advanced tab > User Profiles > Settings** button.
- Select the Student Profile as shown below and click the "Copy To" button¹⁶.



- Specify a destination of `\\server\profiles$\default` if working with Windows XP or `\\server\profiles$\default.V2` if working with Windows 7. Set 'Permitted to use' to *Everyone*. Note that you may be prompted to provide login credentials at this point. Click **OK** to copy.



Step Four: Set the default user profile to be a mandatory (read only) profile

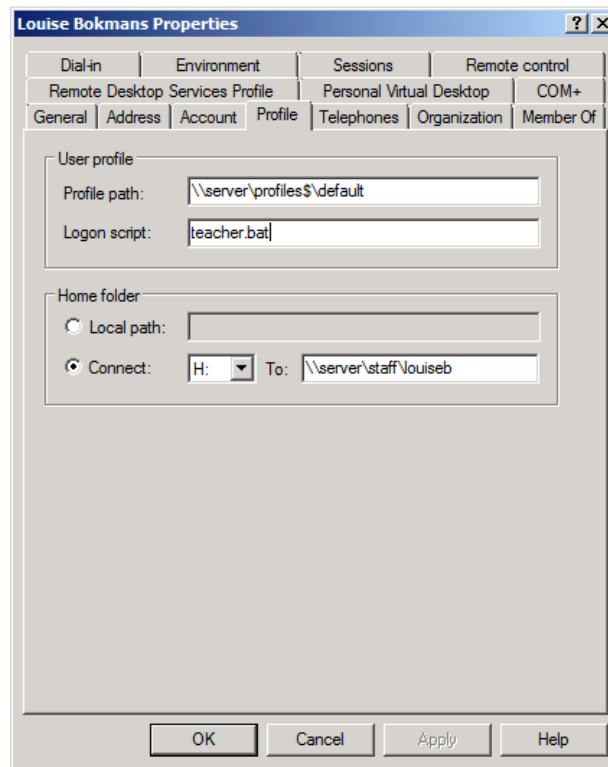
- Open the *default* (or *default.V2*) folder and rename *ntuser.dat* to *ntuser.man*. Note that it may be a hidden file on the server depending on your settings

This turns the modified default user profile into a read-only 'Mandatory Profile'.

¹⁶ Copy button greyed out? Try rebooting the PC. Still greyed out? Download and install a utility called Windows Enabler 1.1 (Google it)

Step Five: Modify Users' details to pick up the Mandatory User Profile on the Server

- Go into **Active Directory Users and Computers**. Right-click on a user and click **Properties** then select the Profile tab.
- Enter a Profile path of `\\server\profiles$\default`
- **Do NOT** put the .V2 extension in the profile path
- Click **OK** to finish



If problems are encountered with this procedure, it is usually down to security permissions so check them carefully.

Using Multiple Mandatory Profiles for Different Year Groups

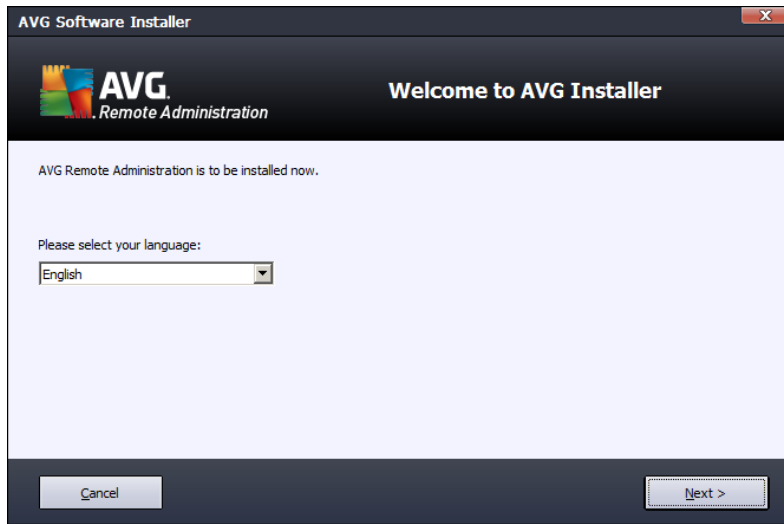
For some schools a single mandatory profile for all pupils is sufficient. However, multiple mandatory profiles can also be used. For example, a particular school might require different Desktops & Start Menus for each year group. This can be achieved by creating separately named mandatory profiles for each year and ensuring that the profile paths are set accordingly for each cohort. A quick way to do this is by making multiple copies of *default* and/or *default.v2*, then renaming them to *year6/year6.v2*, *year5/year5.v2* and so on. Shortcut icons can then simply be dragged into the corresponding Desktop sub-folders for each mandatory profile to customise it. Note that in a mixed XP/Windows 7 environment, different icons may be needed for the v2 profiles as the operating systems usually run applications from different places.

Appendix D: Installation of Anti-Virus Software

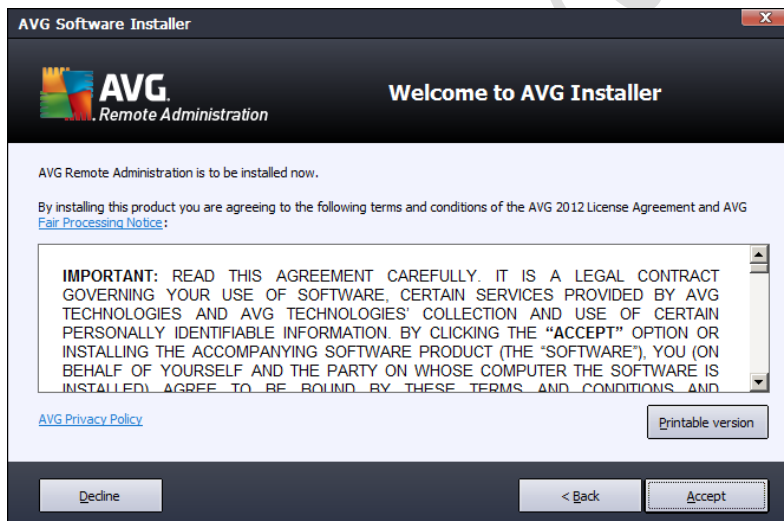
This appendix describes how to install AVG Business Edition anti-virus software on the network. The installation consists of three stages: (i) install the Admin Server component on the file server; (ii) install the anti-virus client on the file server; (iii) install anti-virus clients on the workstations.

Before commencing, check that the file server has internet connectivity and that the AVG serial number(s) are available¹⁷. Download the latest versions of the software from the AVG website at <http://www.avg.com/gb-en/download.prd-avb>.

Install Admin Server

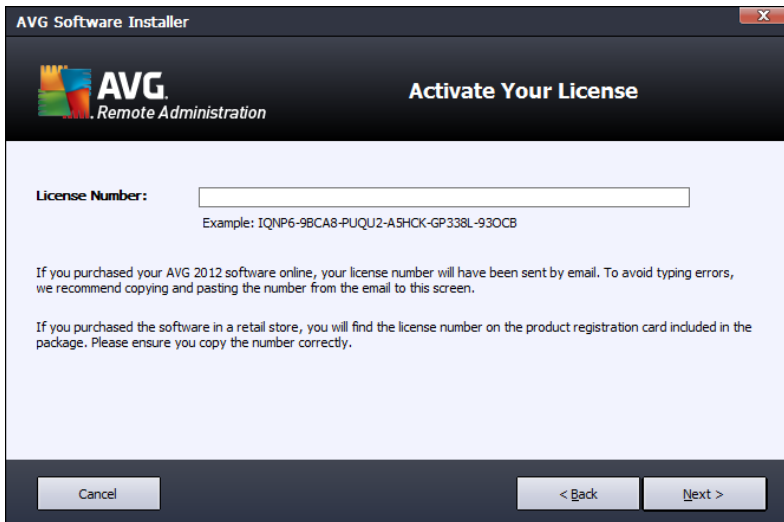


On the file server, run the executable for the Admin Server. Choose **English** and click **Next**.

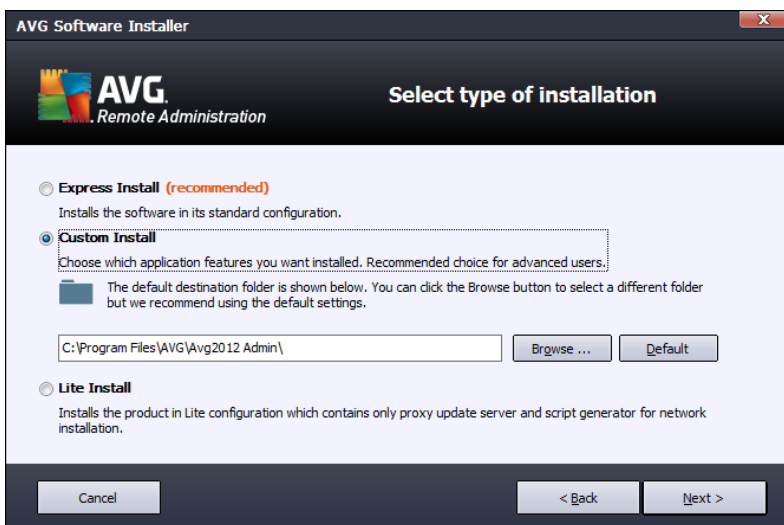


Accept the license agreement.

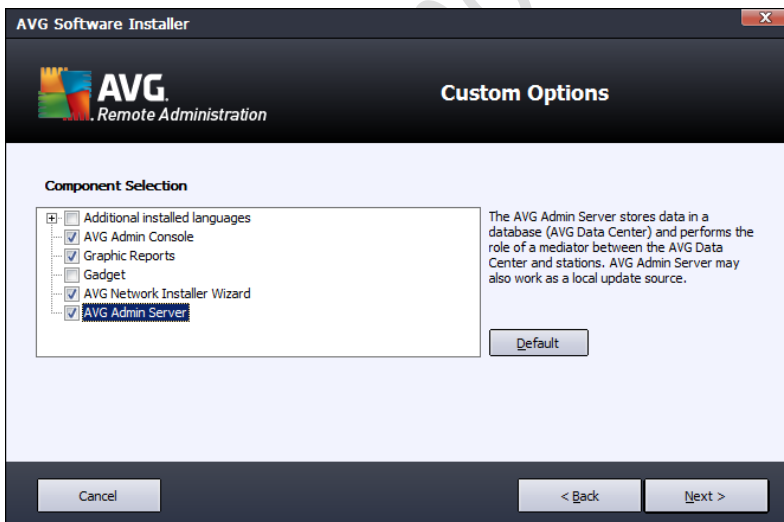
¹⁷ Note. When AVG has been purchased online, they may initially provide what they call a time-limited "sales license". This has to be registered, at which point the proper license number will be provided.



Enter the license number and click **Next**.



Choose **Custom Install** and click **Next**.



The following items need to be selected:

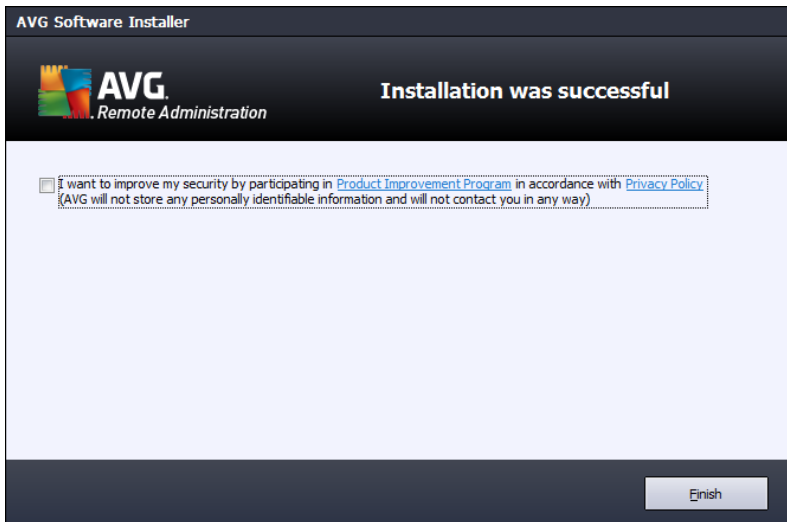
AVG Admin Console

Graphic Reports

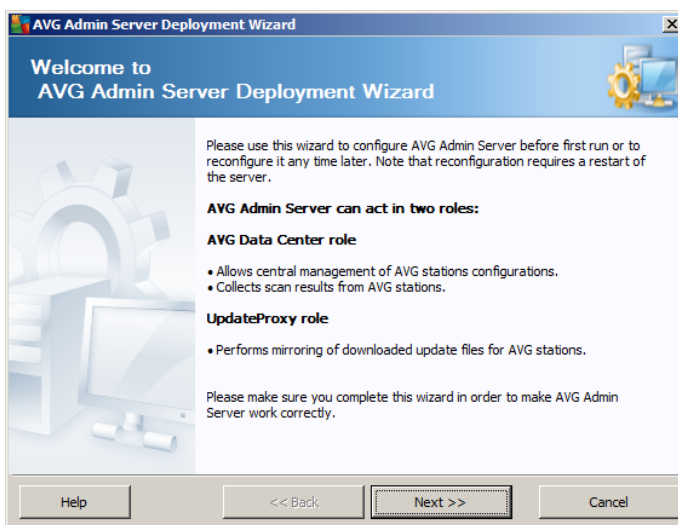
AVG Network Installer Wizard

AVG Admin Server

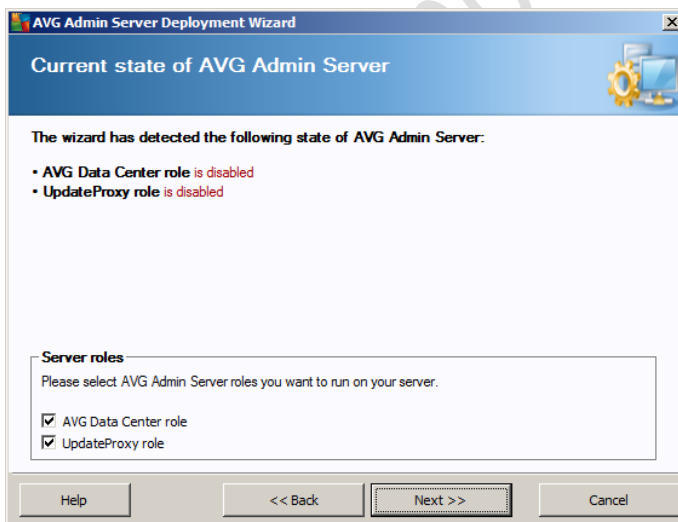
The click **Next**



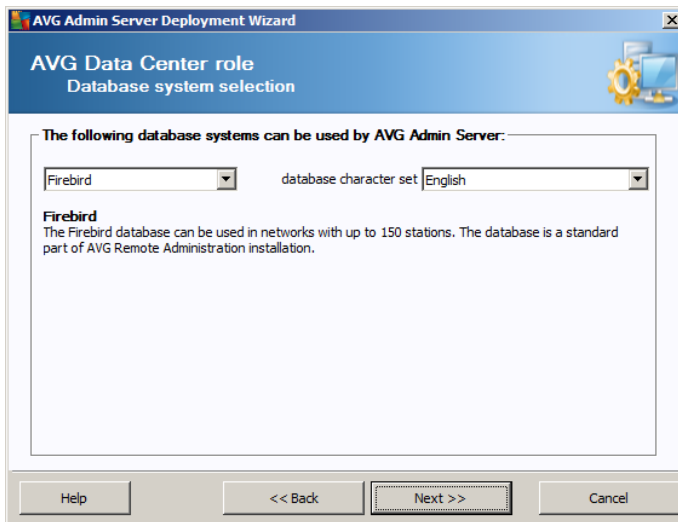
The installation will run for a couple of minutes. When finished, take the tick off this box and click the **Finish** button.



The Admin Server Deployment Wizard should now start. Click **Next**

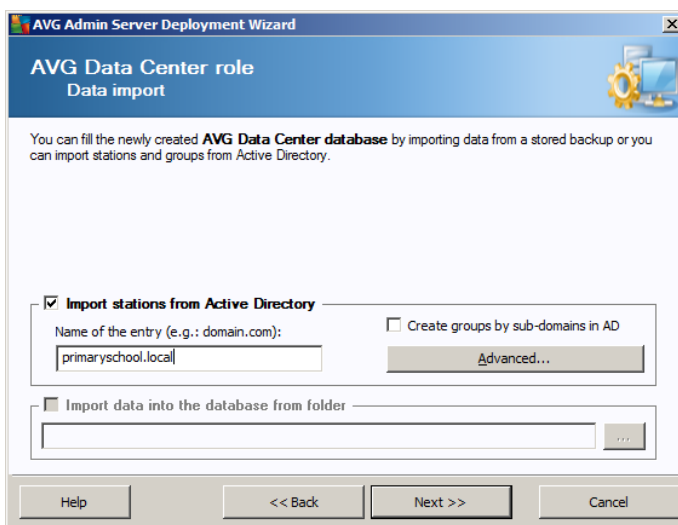


It will state that the AVG Admin Server is currently disabled. Make sure the two boxes are ticked and click **Next**

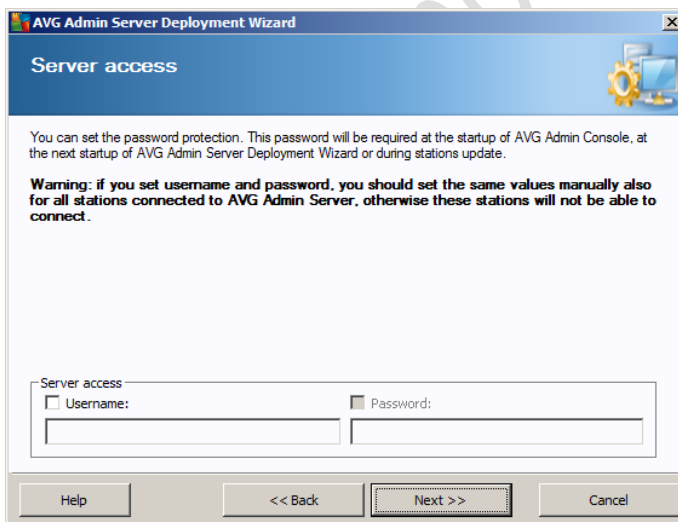


The database system to be used by the Admin Server has to be specified. Choose *Firebird*, which comes with the AVG software, and click **Next**.

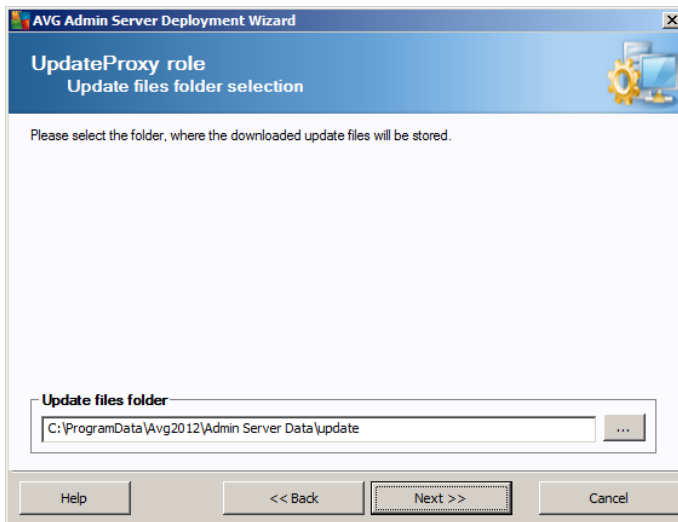
Note: Firebird has a maximum limit of 150 workstations, but this should be sufficient for most primary schools.



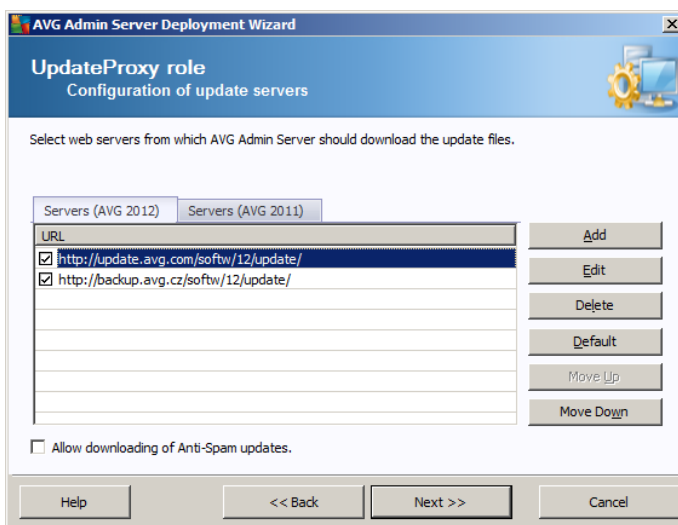
On the following screen it is possible to import a list of workstations from Active Directory. This is optional and only worth doing if all the workstations have already been added to the domain (else just click **Next** to skip). Tick the box and specify the domain name (make sure that it ends in the suffix *.local*).



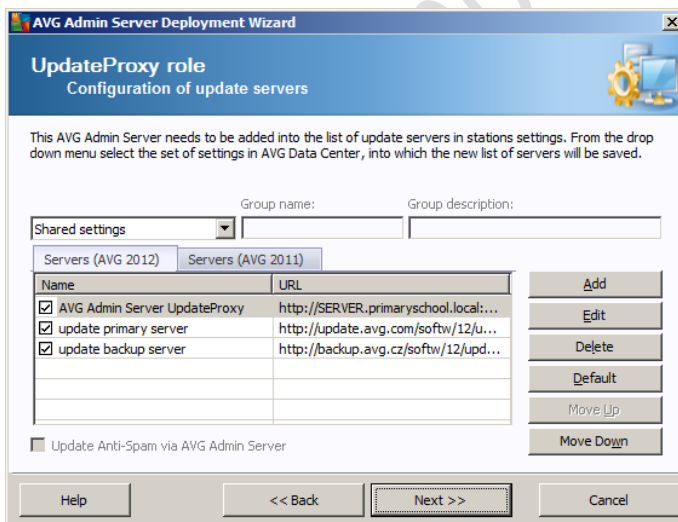
Specifying an additional password simply adds unnecessary complication so ignore this screen and just click **Next**.



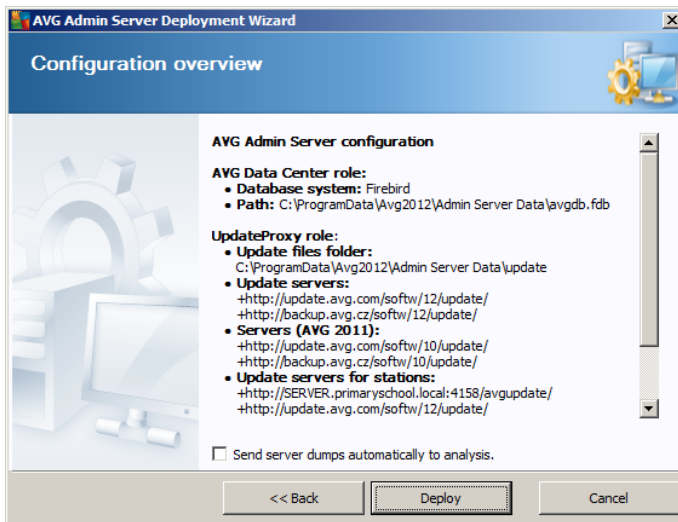
The default value is fine – just click **Next** to continue.



AVG have multiple update servers. The default settings are fine. Take the tick off 'Allow downloading of Anti-Spam updates' (not usually needed). Click **Next**.

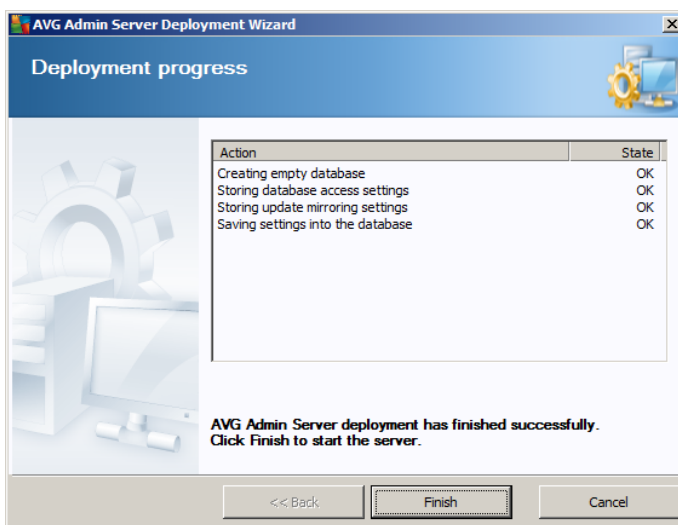


Accept the defaults on the next screen and click **Next**

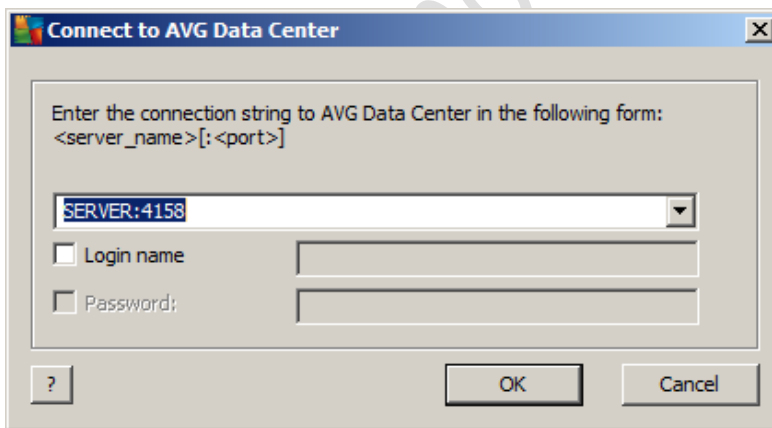


A summary screen is shown.

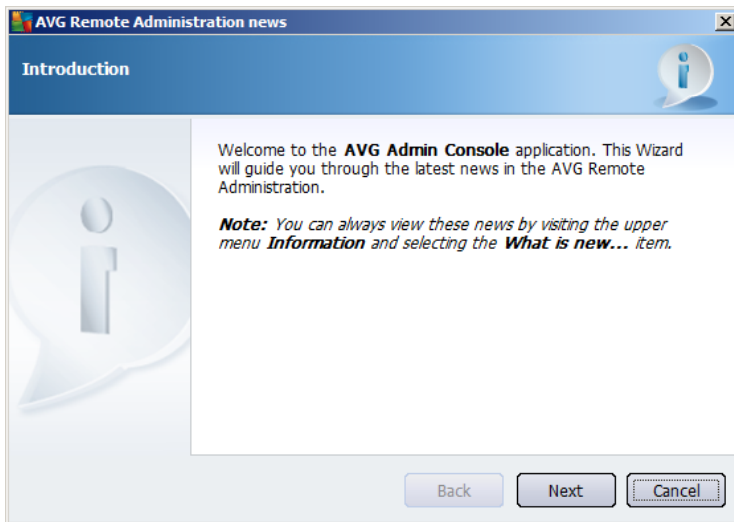
Click **Deploy** to continue.



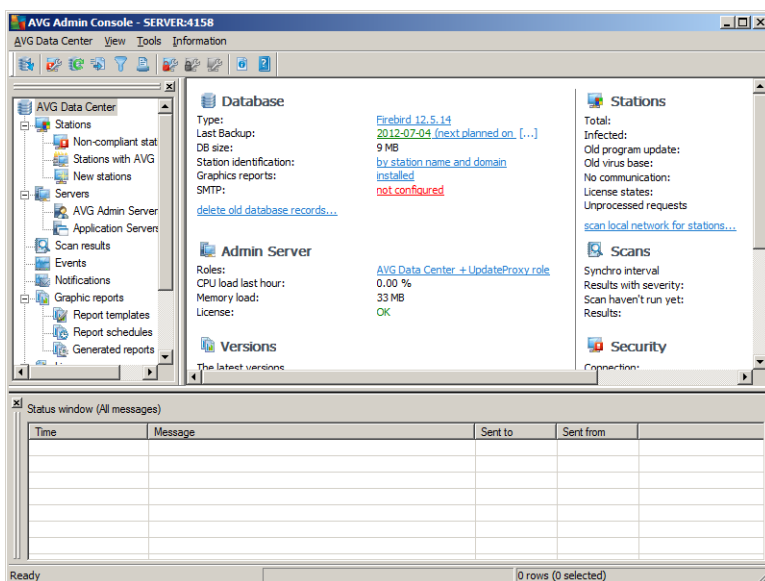
When complete, this screen is displayed. Click **Finish**.



After installation finishes, launch the AVG Admin Console to confirm that it is working properly. The first time it is run, this panel will appear (it should have a value of SERVER:4158). Click on **OK**.



Latest news about the Admin console may be shown. Click **Next** to read it.



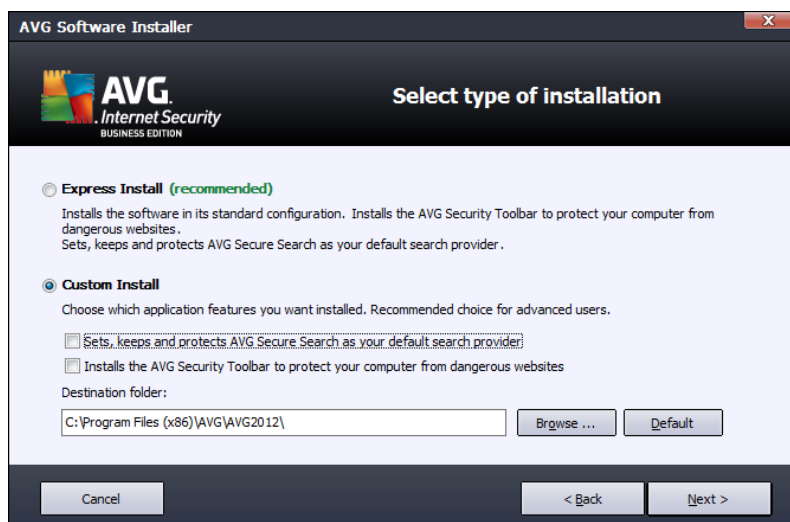
Eventually the Admin Console proper is displayed.

From the main menu click on **Tools > AVG Admin Server Settings**. Click on the **UpdateProxy** tab. On the bottom half of the screen is a section marked **Internet Connection**. Click the **Use Proxy Server** box and check the appropriate details for the county are in place, else specify them¹⁸.

A full discussion of operating the console is outside the scope of this document. However, one useful thing to do is to create sensible groups for the workstations. To do so, right-click on the **Stations** entry on the left-hand panel and click **Create New Group**. Create groups (for example) for ICT Suite desktops, teacher laptops, trolley laptops. After the clients have been installed their entries can be dragged into these groupings for ease of management and to allow customisation if required.

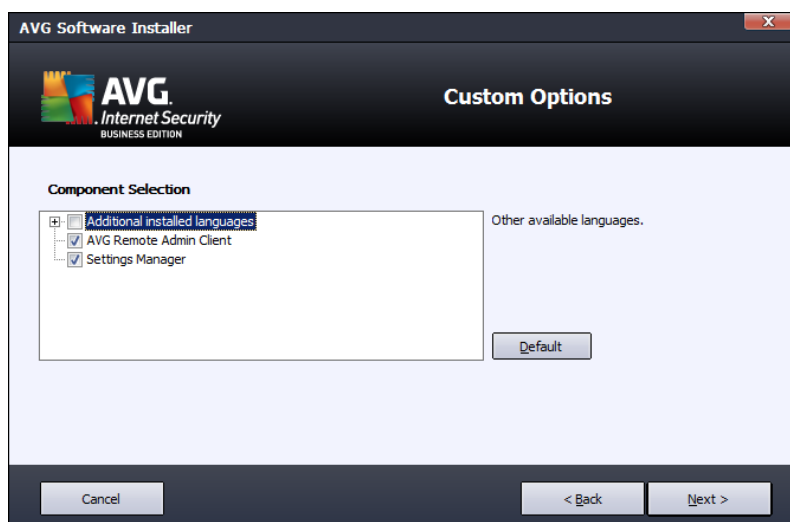
¹⁸ For Herts, a setting of wf3.thegrid.org.uk and port 80 will work.

Install Anti-Virus Client on Server

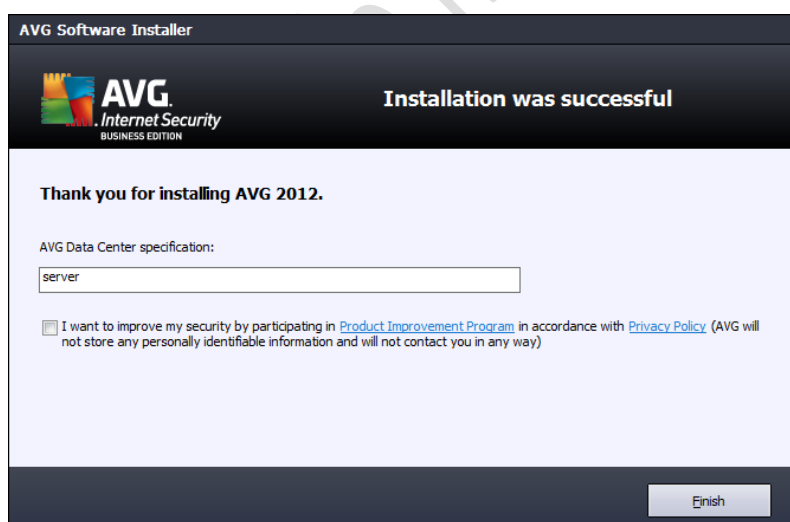


On the file server, run the executable for the Server anti-virus client. The first three screens are the same as per the Admin Console, so just step through them and enter the licence number.

When you reach this screen, choose **Custom Install** and take off all the tickboxes. Then click **Next**.



All options should be ticked, other than *Additional installed languages*. Click **Next**.

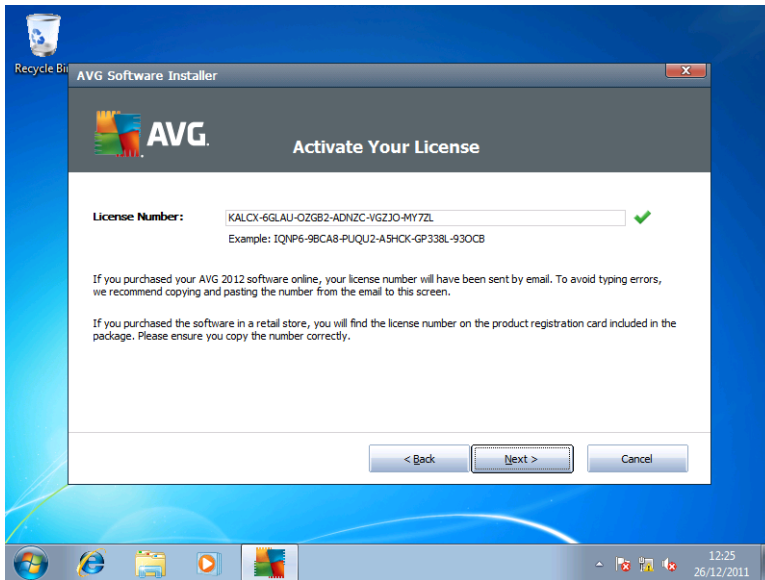


On the final screen, enter a value of 'server', remove the tick-box and click **Finish**. The anti-virus software will now load and update itself. If it does not do so, go into **Advanced Settings > Update > Proxy** and specify the correct proxy server for the county (use the http value e.g. 8084 for Essex, rather than the AVG default of 3128).

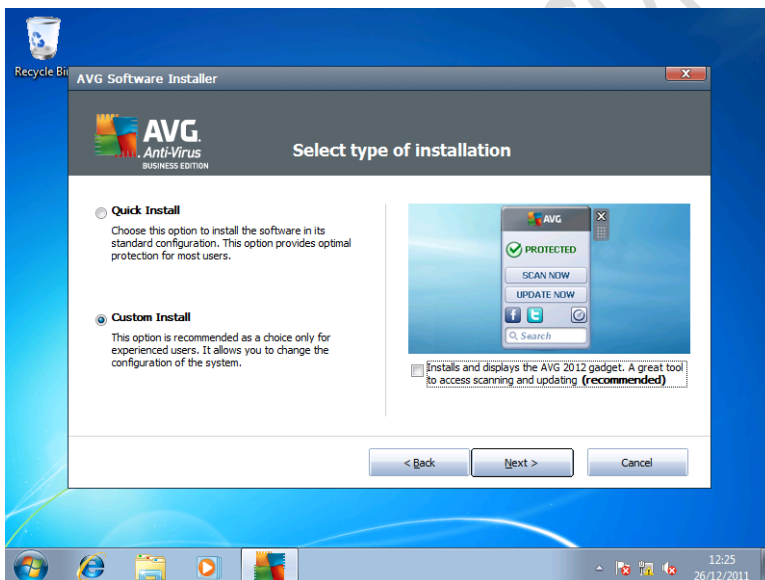
Install Anti-Virus Client on Workstations

The anti-virus client can be deployed in two ways: it can be installed remotely from the server; it can be installed locally on each workstation. Remote installation can be problematic and for this reason it is therefore suggested that the software is installed locally. To facilitate matters, it is suggested that the installation programs are placed in the *Technical* folder, which maps as the Z: drive for system administrators (alternatively, access the \\server\technical\$ share).

NOTE: AVG change these screens on a regular basis so there may be some cosmetic variations from those shown.



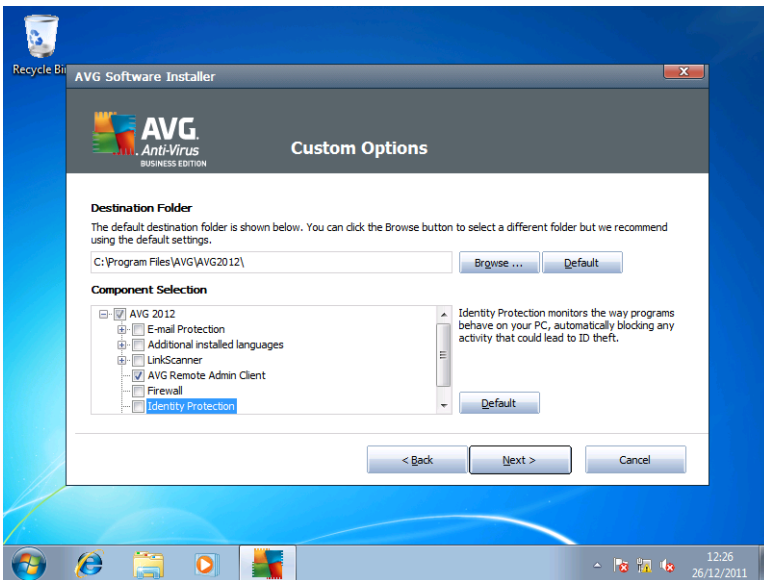
Login to the workstation as an administrator and run the executable for the workstation anti-virus client from the Z: drive. Enter the licence number and click **Next**.



Choose **Custom Install**.

If there is an option to install the 'AVG 2012 gadget' decline to do so.

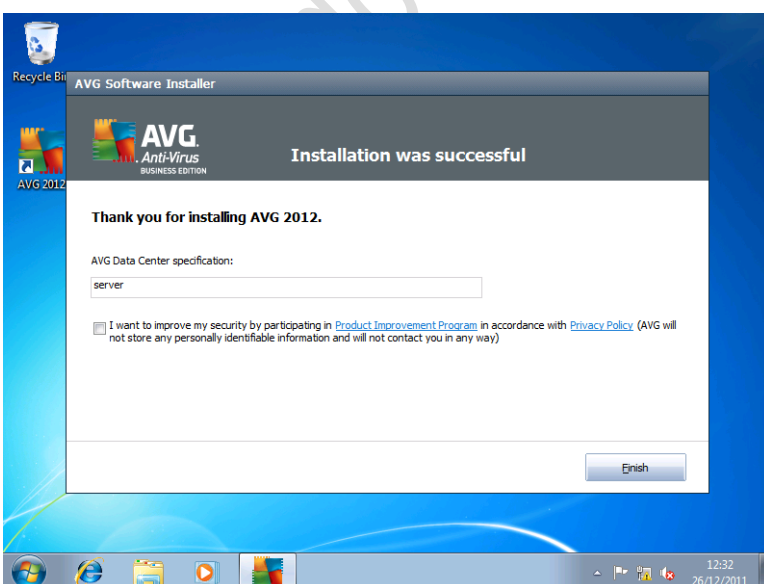
Click **Next**.



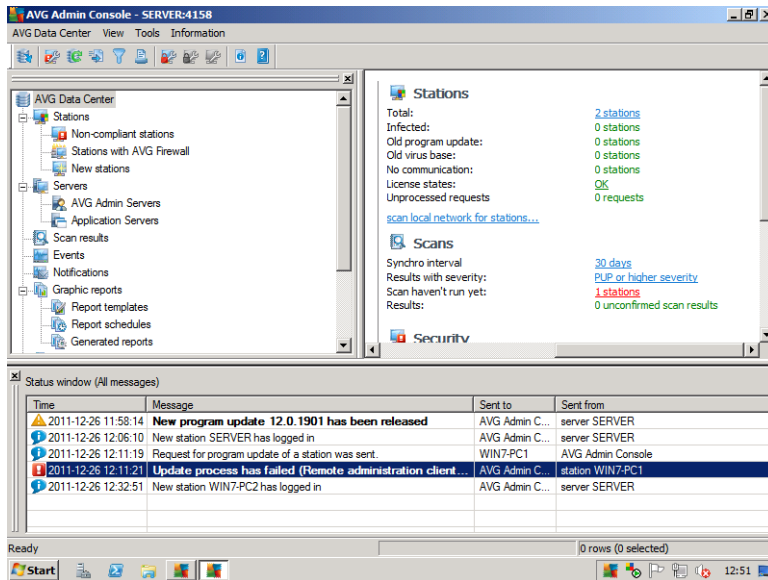
By default AVG installs a lot of optional items. The only component that should be ticked is the *AVG Remote Admin Client*. Click **Next**.



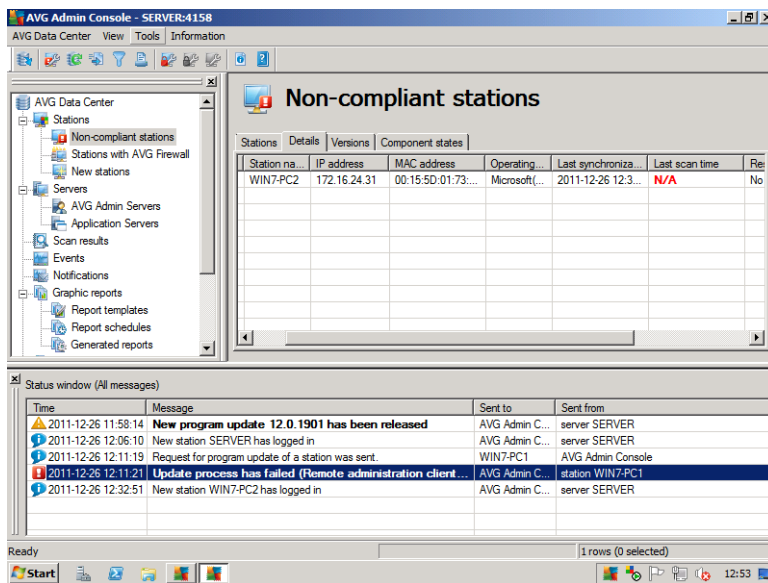
More stuff that is not needed. Make sure that none of these options are ticked, then click **Next** to continue.



On the 'Installation was successful' screen, enter a value of *server* in the 'AVG Data Center specification' field – **this is very important**. Make sure the box is not ticked and click **Finish**. At this point the workstation should connect to the server and update itself.



Shortly thereafter, the workstation should be visible from the AVG Admin Console on the server.



The workstation will appear under 'New stations' or 'Non-compliant stations'. Check its status; if it has failed to update then right-click and force a virus database update. This will usually resolve matters.

Appendix E: Two Minute Guide to the New Network

Your username is _____

Your password is _____

Where should I store my stuff?

The best place to store things is in the **My Documents** folder. Most programs (e.g. Word, PowerPoint) do this automatically. If you do so then your work is automatically backed up to the network and can be accessed from any computer on the network. The worst place to store things is on your Desktop.

Sharing work with colleagues

If you click on **Start > My Computer** you will see that you have three disk drives:

H: is your personal **Home** drive and is a mirror of your **My Documents**. That is, they are one and the same and you can use either for your work.

T: is the **Teachers** drive and is shared with your colleagues. It contains a number of folders already and you can add new ones in whatever way makes sense to you. This drive cannot be accessed by the children.

R: is the **Resources** drive and is visible to everyone, staff and children alike. This acts as a sort of library whereby pictures, music, documents and videos for the entire school can be stored. Teachers are able to put things in the Resources drive, but children can only retrieve them and cannot add to it.

Sharing with pupils

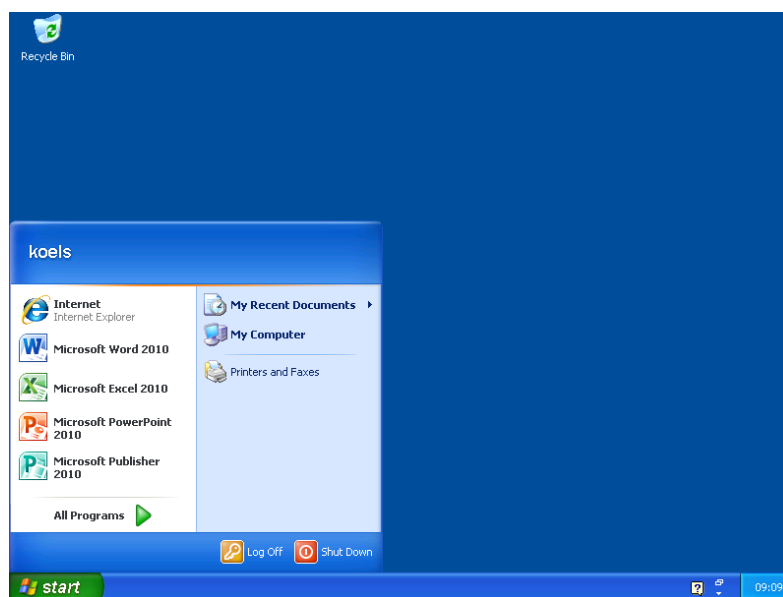
In the Resources drive is a folder for each year group - this can be used to distribute work to your pupils. Example: you have downloaded some useful documents for a lesson with year 6. Save the documents in R:\classes\year6. The children have access to this area and can see them. However, note that they do not have permissions to store things in the class areas.

Secret Tip

If you need to see what work a pupil has created then you would normally need to login as that child. However, there is a secret backdoor that can be used to quickly access any pupil from your own login. Hold down the Windows key (towards the bottom left-hand side of the keyboard – it looks like a flag) and press R. A small box appears; in the box type [\\server\pupils](#) and press Enter. The storage area for the pupils is shown, organised by cohort. Simply open the cohort folder corresponding to the year group.

Pupil Usage

The pupils login using their user ID and password. After a successful login they will be presented with a relatively clean Desktop along the following lines:



The correct way to run a program is by clicking on the **Start** button. The 'bread and butter' programs – Internet, Word, PowerPoint and so on are listed. Other programs can be found by clicking on the **All Programs** option. If desired, icons for other programs can be added to the Desktop (just ask the IT Technician).

The pupils in each year group share a common Desktop. They cannot save documents to it or corrupt it – any changes they make will be forgotten and the next time they login it will be back the way it should be.

The pupils have access to two drives: a Home drive **H:** where they should store their work, and the Resources drive **R:** as described earlier. Once again, the My Documents is a mirror of the H: drive so they don't have to worry about the specifics; when they save things they will go in the right place by default.

Problems?

Setting up a network is an enormous undertaking, such that the potential for some errors and mistakes exists. There has been a lot of testing but there may well be a few teething problems; fortunately these are usually of a minor nature and can easily be rectified. These should be recorded on the attached sheet and brought to the attention of the IT Technician for assessment and resolution.

Snag List compiled by _____

Description	Who is affected?	Category
		Show stopper / Annoyance / Suggestion
		Show stopper / Annoyance / Suggestion
		Show stopper / Annoyance / Suggestion
		Show stopper / Annoyance / Suggestion
		Show stopper / Annoyance / Suggestion
		Show stopper / Annoyance / Suggestion
		Show stopper / Annoyance / Suggestion
		Show stopper / Annoyance / Suggestion