Synology Setup Guide
For Small Businesses

Based on DSM 4.3

Nicholas Rushton, BA Hons.

Callisto Technology And Consultancy Services

Second Edition. This edition was updated on 21st March 2014.

Contents

Introduction

This guide describes how to setup a Network Attached Storage device (NAS) from Synology for use in a small business. NAS systems are particularly suitable for many small businesses, offering a more efficient and affordable alternative to a conventional file server running Windows Server. The vast majority of businesses comprise less than 25 people and, whilst it is possible to setup a NAS to service hundreds or even thousands of users, the focus in this guide is specifically on small businesses and with an emphasis is on things that work and are useful in such an environment. The guide is supported with a growing website at: www.serverinstallationguides.co.uk.

There are numerous vendors of NAS including Synology, Western Digital, Netgear, QNAP, Buffalo, Thecus and others. Among these, Synology stands out for its rich functionality, useful features, flexibility and ease of use. Typically, NAS devices are controlled using web pages, making them clunky to use. However, Synology have a proper operating system with such familiar features as a Desktop and a drag and drop interface, analogous to a normal Windows or Apple Mac computer. It is also possible to install applications to further increase functionality. This operating system – known as *DiskStation Manager* or *DSM* – is accessed using a standard browser from another computer on the network. This guide is based around DSM 4.3.

A Synology NAS solution has the following benefits:

- Provides shared folders and resources plus private areas ('home folders') in which users can store their work
- Provides centralised storage, enabling easier management and backup (as compared to standalone computers or peer-to-peer networks)
- Low cost, cheaper than a conventional file server and with better price performance
- Automatic, regular backup of data
- Remote access, including private cloud (analogous to Dropbox or SkyDrive but of huge capacity and with no ongoing costs)
- NAS devices can be physically small and use little energy, giving low running costs
- NAS devices are reliable and almost maintenance free. Largely immune to viruses, they do not require frequent software updates and have reduced support requirements
- Allows use of Home editions of Windows, enabling purchase of cheaper computers and those from high street retail outlets
- No additional software licensing needed (no need for Client Access Licences or CALs)
- Works equally well with all modern versions of Windows as well as Apple Mac

It is true that NAS solutions tend to offer less control and management facilities than server-based networks, although Synology DSM mitigates some of this. For example, they do not readily allow central management of connected computers and do not allow so-called roaming profiles, whereby users have a personalised computing environment and desktop that follows them from computer to computer. However, in a small business the advantages far outweigh the potential disadvantages, which is why a NAS is often a good solution.

1. Hardware, Software and Infrastructure Considerations

1.1 Choice of DiskStation/RackStation

Currently, Synology offer around 30 different models of their NAS hardware, categorised into four types of user: large scale business; small and medium business; home to business workgroup; home to small office. For a typical small business, a model from the small and medium business or home to business workgroup categories is most likely to be suitable. The models vary according to form factor, number of hard drives that can be used, performance and ultimately price:

Form Factor	DiskStation models (designated with the letters DS) are standalone units designed to sit on top of a cupboard or desk. RackStation models (designated with the letters RS) are designed to be mounted in standard computer cabinets (racks) that take devices that are 19" (48cm) wide. Smaller organisations will typically use a DiskStation but if a cabinet is already in place (perhaps to hold other equipment) then a RackStation may be the better choice.
Number of Hard Drives	Synology NAS units can hold between 1 and 12 hard drives, depending on the model. Having more drives allows more storage capacity. Additionally, the use of more drives permits the use of RAID (discussed below) that can improve resilience and throughput.
Performance	Some DiskStations and RackStations have more powerful processors, hold more memory (RAM) and have multiple network adaptors – these models have a plus sign at the end of the model number (e.g. DS214+). However, it is by no means essential to buy a plus model.

Choosing the right model can be confusing, as there is some overlap between them. By way of example here are some models available at the time of writing (Synology also have their own online guide at: http://www.synology.com/en-uk/support/nas_selector)

DS214+

A good choice for organisations with up to 10 employees

DS1513+

A more capacious unit for organisations with up to 25 employees

RS812+

A rack-mounted unit for organisations with up to 25 employees

Figure 1: A selection of Synology models

1.2 Choice of Hard Drives

DiskStations and RackStations are not usually supplied by the manufacturer with hard drives installed in them. Rather, the idea is that the customer buys the drives separately and installs them (which is very easy to do) else buys a ready-populated unit from a reseller. This approach is better because it offers more options. Synology NAS units are very flexible in terms of the brand and type of hard drives that can be used in them. However, it is not necessarily the case that any drive or combination of drives can be installed; rather, there is a list of supported drives to be found on the Synology website at: http://www.synology.com/en-global/support/compatibility

Hard drives are manufactured in 3.5" and 2.5" form factors; either can be used although some DiskStations/RackStations require adaptor brackets to use the 2.5" ones. The 3.5" drives offer higher capacities and better price performance but 2.5" drives use less power, generate less vibration, are generally quieter in operation and are becoming an increasingly popular choice. It is possible to buy drives that have been specifically optimised for use in NAS, such as the Western Digital Red series or the Seagate NAS line and these are recommended.

Although most of today's hard drives are mechanical, solid state drives based around flash memory ('SSDs') are increasingly being seen in laptop computers and elsewhere and will probably become the norm in all computing devices. At present, they are considerably more expensive than their mechanical counterparts for high-capacity units. The popular ones are supported by Synology DSM; however, the main benefits are reduced power consumption and the absence of noise, rather than any performance improvements in a typical NAS environment.

1.3 RAID

RAID stands for *Redundant Array of Independent (or Inexpensive) Disks*. There are various types of RAID, referred to using a numbering system i.e. RAID 0, RAID 1, RAID 5. The basic idea is to improve reliability and performance by using multiple disks to provide redundancy and share the workload. Synology support many different RAID levels; depending on the model and the physical drives installed, the following RAID levels might be available: JBOD; RAID 0; RAID 1; RAID 5; RAID 5+Spare; RAID 6; RAID 10; SHR (Synology Hybrid RAID, which allows drives of differing capacities to be used). However, despite all these options the three most common scenarios in a small business are RAID 1, RAID 5 and SHR.

RAID 1 consists of two identical drives that mirror each other. So, when a file is saved there are actually two separate but identical copies behind the scenes, one held on each drive, even though you can only see one as the mirroring process itself is invisible. If one of the drives fails, the second one automatically takes over and the system carries on without a blink. At the earliest opportunity the faulty drive should be replaced with a new one; the system then 'syncs' it so it becomes a true copy of the remaining healthy drive (a process known as 'rebuilding the array'). In a RAID 1 system, the total usable storage capacity is half that of the total drive capacity installed; for example, if a DiskStation has two 2TB drives installed then the total amount of usable storage capacity is 2TB rather than 4TB.

RAID 5 uses at least three but preferable four drives. Data is written across all the drives, along with what is known as parity information. The benefit of this is that the system can cope with the failure of any one single drive. RAID 5 is considered to offer a good combination of price, performance and resilience. Whereas a RAID 1 system loses 50% of the total drive capacity, RAID 5 loses only about 25%. For example, if a RackStation has four 2TB drives installed then the total amount of usable storage capacity is 6TB rather than 8TB.

SHR (Synology Hybrid Raid) is a more flexible approach to RAID. Whereas RAID systems require multiple drives of identical capacity, SHR can work with drives of differing capacities. It creates a mixture of usable space plus puts some aside for redundant storage ('protection'). SHR is only really of relevance when there is a mixture of odd-sized drives, which might be the case for instance if you were using a mixture of old and new ones. By way of example, if you had a pair of 2TB drives, a 1TB one and a 500GB one then SHR would give you 3.5TB usable space and use a further 2TB for protection.

In summary, a server with two drive bays should be normally configured as RAID 1 whilst one with four drive bays should normally be configured as RAID 5.

Synology have a web page for calculating the amount of available storage for different RAID configurations at:

http://www.synology.com/en-global/support/RAID_calculator

1.4 Location

The server should be attached to the network via a Gigabit Ethernet connection or two Gigabit Ethernet connections if the particular model supports it. Ideally it should be located out of sight and reach, for instance in a locked room or cupboard as little physical access is needed and it is operated headless i.e. there is no need for a screen or keyboard and mouse.

1.5 UPS

It is strongly recommended that an intelligent UPS (Uninterruptible Power Supply) is used with the NAS. In the event of power problems this will enable the server to continue operating for short periods and to shut it down in an orderly manner if necessary. Most popular brands work with Synology e.g. APC, CyberPower ; a full list of supported UPS's can be found on the Synology website at:

http://www.synology.com/en-global/support/faq/300

1.6 Internet Connection, Hub, Router, Switches

A network has to be connected to the outside world in order to access the internet. Optionally, it can also be used to provide remote access to the network for staff who are working outside the office or travelling – something that Synology is quite good at. Many small businesses and especially micro businesses will have an all-in-one router or wireless router; in turn, this will be connected to a switch and maybe a wireless access point.

Three points to follow here are:

- Use wired connections whenever possible as performance is so much better than wireless
- Wired connections should be at Gigabit speed, wireless connections at 801.11N or better
- Avoid domestic grade equipment. Spending more on professional or prosumer ("professional consumer") routers and switches will give better performance and reliability

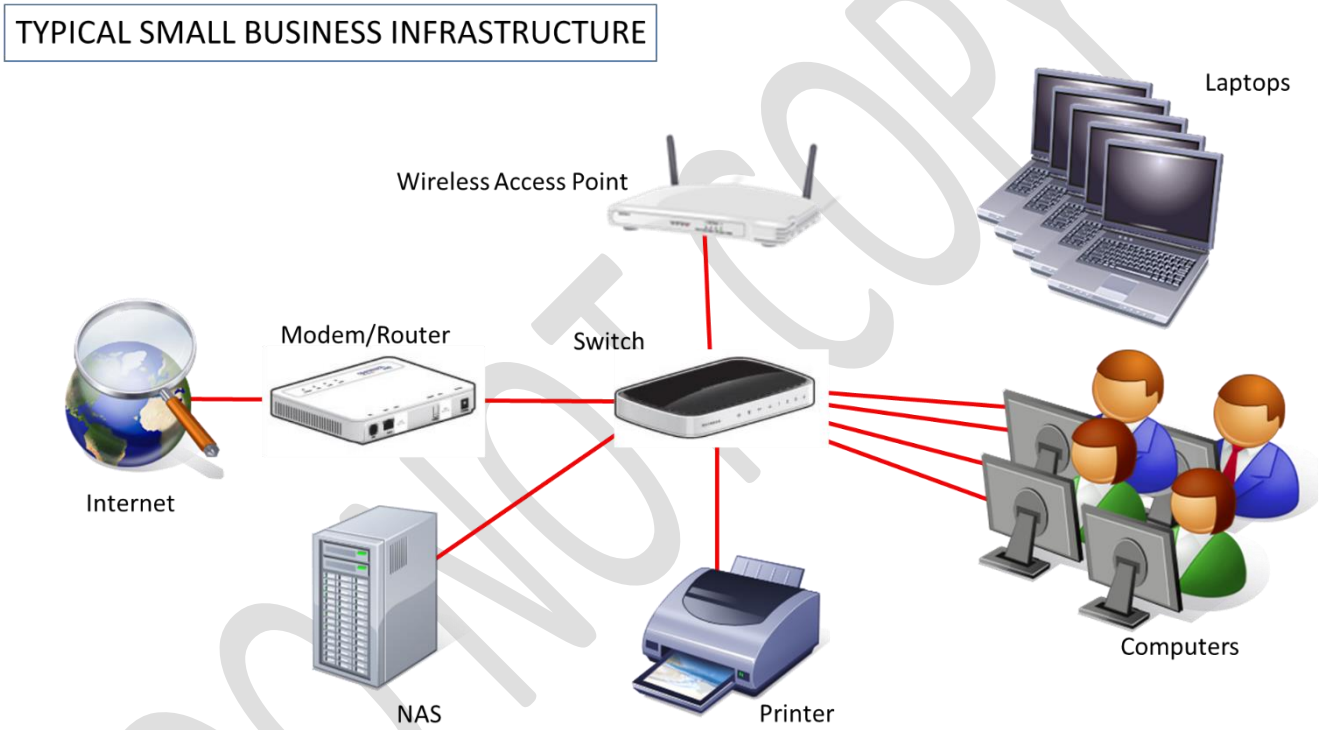

Figure 2: Infrastructure

1.7 Workstations

The client computers can be running any mixture of Windows 7, Windows 8, Windows Vista or Windows XP. Home or Professional versions are equally suitable. Apple Macintosh computers running Mac OS X 10.5 or better can also be connected, as can Linux PCs (but the latter are not specifically discussed in this guide). Devices running iOS, Android and Windows Phone can be connected, but Chromebooks can only be connected in a very limited sense.

Although existing workstations can usually be connected on an "as is" basis, by far and away the best approach is to use this as an opportunity to re-install Windows or re-image them with a clean and up-to-date set of software and drivers. This helps ensure consistency and optimal performance. Tools such as Symantec Ghost or the freeware product PING can be used for imaging multiple machines.

1.8 IP Considerations

Every device on a network has a unique number within that network to identify it, known as its *IP address*. These numbers consist of four sets of digits and take the form *nnn.nnn.nnn.nnn*. Nearly all of the possible numbers are allocated to the internet for websites and such and are known as *public IP addresses*. However, a small selection are available for internal or local area networks; these are known as *private IP addresses* and are invisible to the outside world. As these IP addresses are private they can safely be used by anyone and the exact same numbers are used millions of times over. The three number sequences which are available for private use are:

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

Most equipment intended for use in small businesses and homes tends to be pre-set to use the 192.168.nnn.nnn numbering scheme; for instance, internet routers commonly have an address of 192.168.1.1 or 192.168.1.254 depending on brand. Although these addresses can be changed, there is rarely any need to and it is best not to do so unless one has a good understanding of the subject.

Devices such as computers and printers do not come with IP addresses already allocated; instead, they have to be configured with a suitable address. There are two ways of doing so - you can use *static IP addresses* or *dynamic IP addresses*.

With static IP addresses, it is necessary to visit each device and individually configure it. For instance, you might set the first computer to be 192.168.1.101, the second to be 192.168.1.102, the third to be 192.168.1.103 and so on. You have to be careful to keep track of everything and above all make sure that there are no duplicates. If this sounds like hard work then that's because it is – you might get away with it if there are only a handful of computers but beyond that it rapidly becomes unworkable.

With dynamic IP addresses, the numbers are assigned automatically by a DHCP (Dynamic Host Configuration Protocol) server which keeps track of everything. This is not usually a physical server like a file server, rather it is a piece of software. Most all-in-one routers of the sort used in small businesses and homes have DHCP server software built-in. If DSM detects one of these during installation, it will use it. However, if it does not then DSM can provide its own DHCP service, using a free application that can be downloaded from Synology.

Regardless of whether the IP addresses come from a router or are supplied by DSM, it is a good idea to have a scheme to follow. As mentioned above, routers are commonly set to addresses such as 192.168.1.1 or 192.168.1.254. The server should be set to an adjacent address; printers and any specialised devices should be close by; the numbers allocated for computers should be a contiguous block of numbers elsewhere. So, for instance, a typical setup might be as follows:

IP Address(es)	Role
192.168.1.1	Internet router
192.168.1.2	DiskStation/RackStation
192.168.1.3 - 192.168.1.20	Printers and other special devices
192.168.1.100 - 192.168.1.250	Computers, smartphones, tablets etc.

The gateway router and server should have static IP addresses. Printers, Wireless Access Points and any specialised devices should have static IP addresses or – better still – reserved IP addresses. Workstations and similar devices should have dynamic addresses from DHCP.

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: 150 addresses for general computing devices (PCs, laptops, iPads etc.); maximum of 17 networked printers and other special devices. As we are implementing a relatively small network there should be more than enough capacity.

2. Installation of DSM Operating System

Having physically installed the disk drives into the server and connected it to a power supply and the network, it is necessary to install DiskStation Manager – DSM – the operating system for the DiskStation/RackStation. There are two ways of doing this: with *Web Assistant* or *Synology Assistant* and both are discussed below. Web Assistant works with servers manufactured from 2013 onwards, but will not work with earlier models. In contrast, the Synology Assistant will work with any model. There are some network situations in which Web Assistant doesn't work, in which case you will need to use Synology Assistant as described in section 2.2 Installation using Synology Assistant.

2.1 Installation using Web Assistant

Web Assistant is invoked by typing the following address into the browser on a computer connected to the same network: *find.synology.com*. You can do this from a Windows PC, Mac or iPad. After scanning your network for a few seconds it should find the DiskStation and display the following screen:

Figure 3: Web Assistant, first screen

Click the **Connect** button. On the following screen, click the button on the right-hand side of the screen:

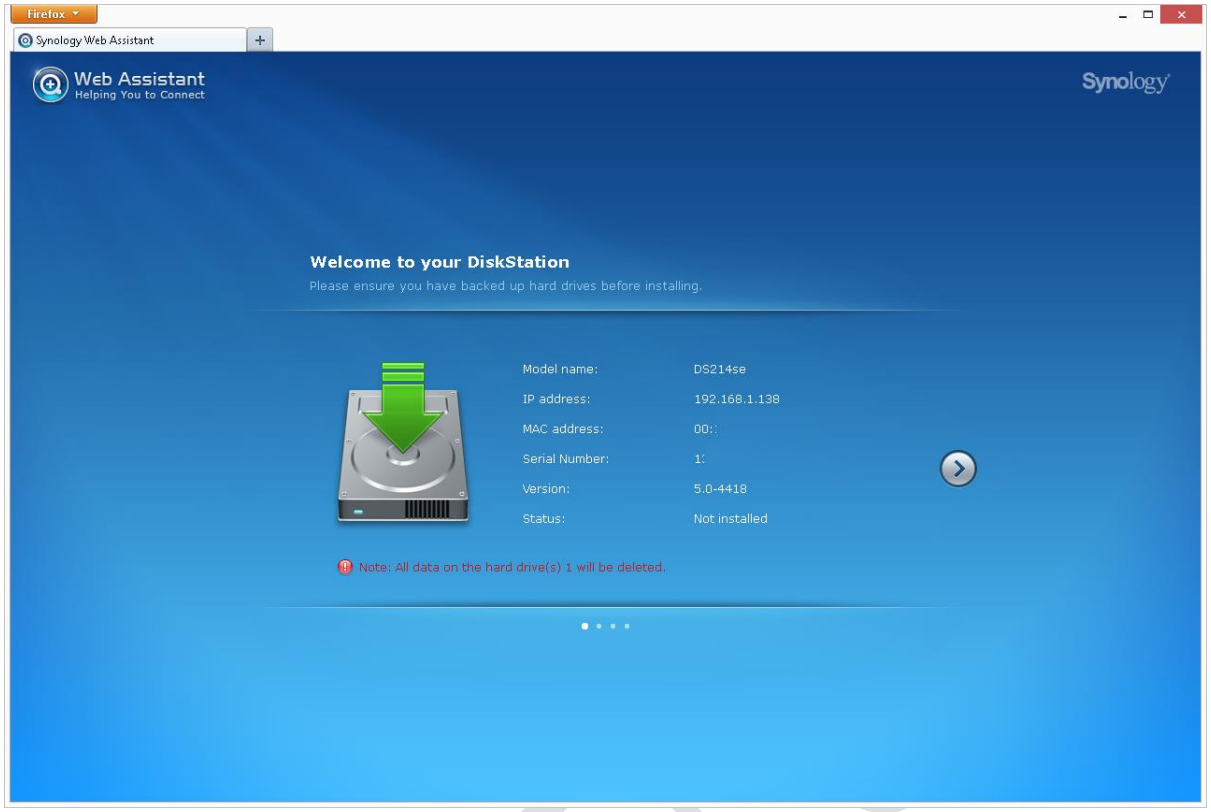

Figure 4: Web Assistant, second screen

The next screen gives a choice of downloading the latest version of DSM from Synology or using a copy that is on the computer or an installation disc. You want the first option. Then click the button on the right-hand side of the screen.

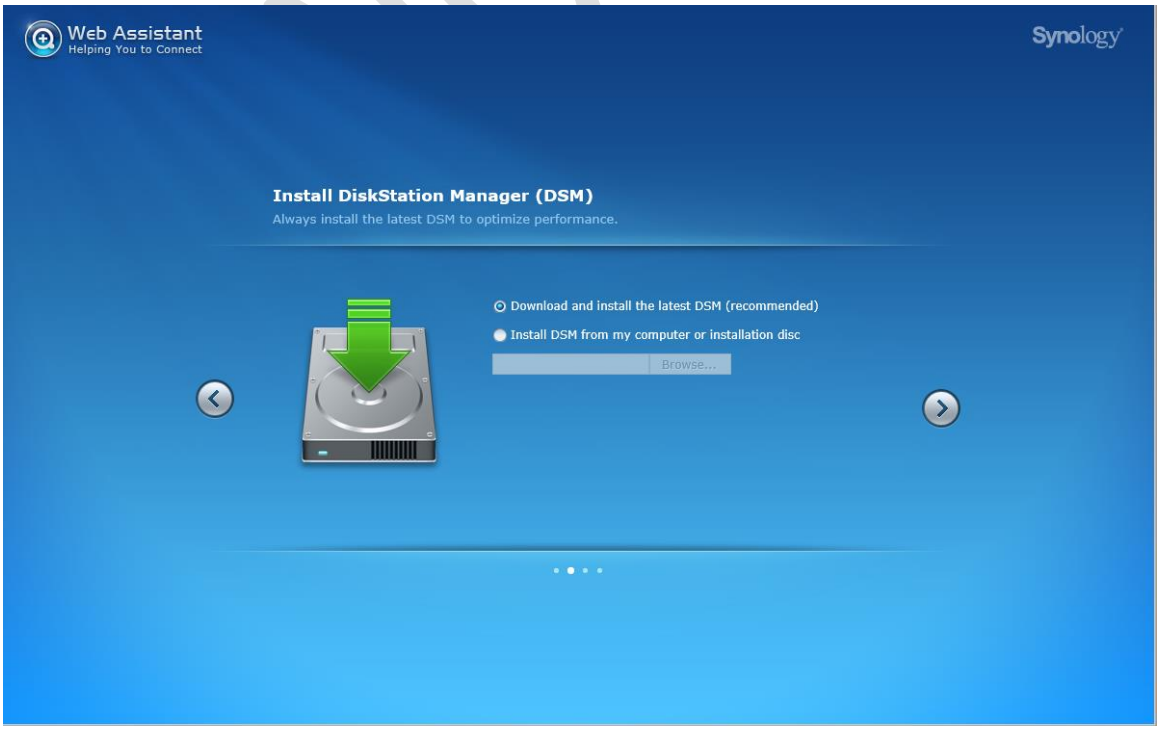

Figure 5: Download or specify DSM

On the subsequent screen enter and confirm a password for the main admin user – choose something non-obvious and make a note of it. You can also give the server a name – it is suggested that you simply call it *server*. Take the tick off the **Create a Synology Hybrid RAID (SHR) volume after installation** and click the **Install Now** button:

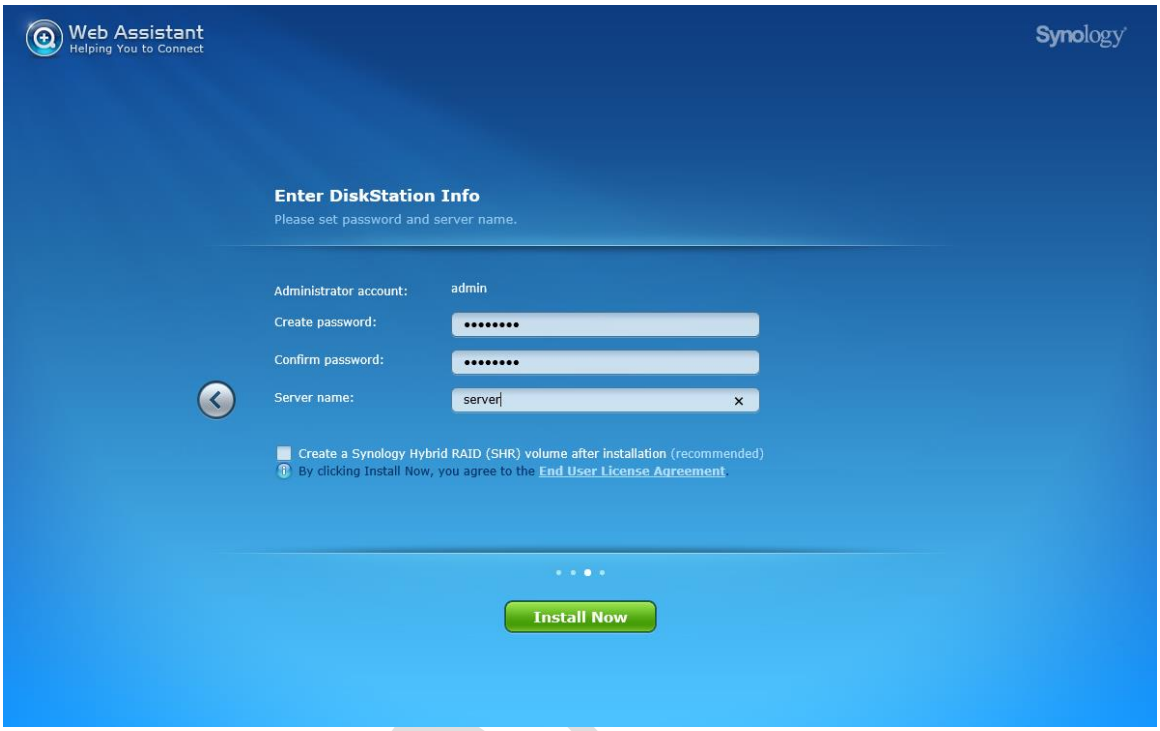

Figure 6: Specify password and server name

A warning message that any data on the disk(s) is about to be destroyed is shown. Acknowledge it by checking the tickbox and clicking **OK**. DSM will then be installed, during which time a status screen is displayed. The time taken for this stage varies but is in the order of ten minutes.

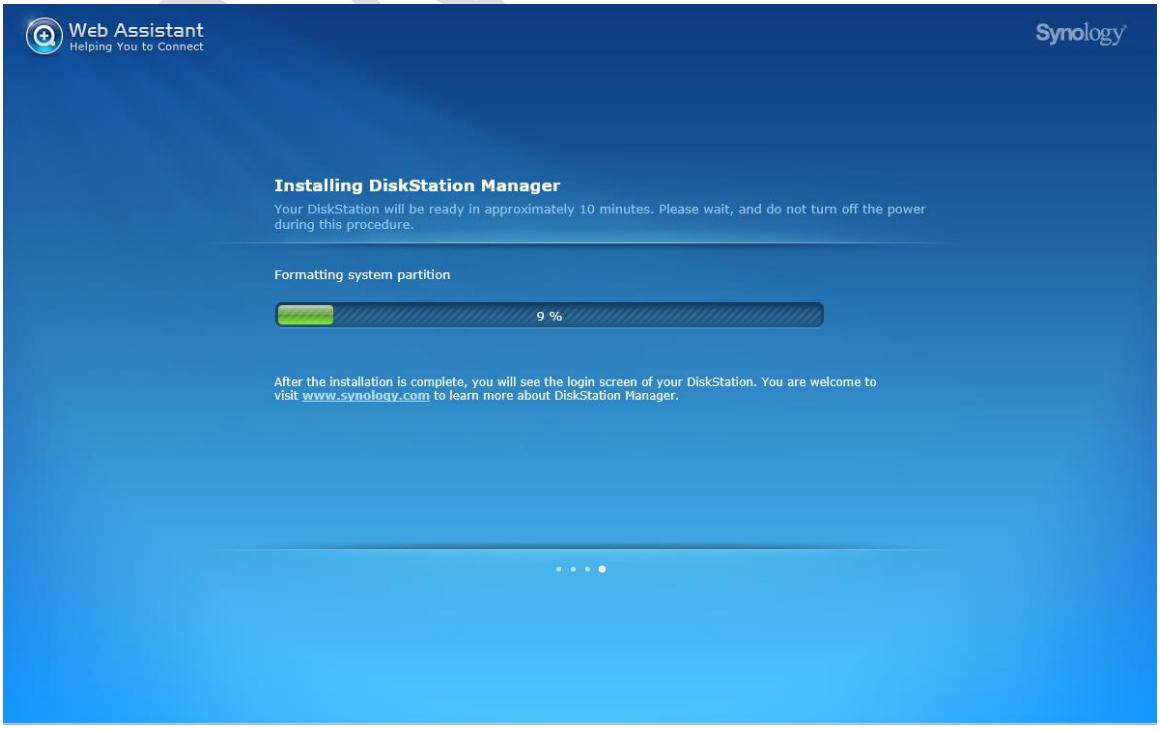

Figure 7: Progress screen

After the installation has finished you will be presented with the DSM login screen. Jump to section 2.3 Logging In For The First Time to continue.

2.2 Installation using Synology Assistant

Download the latest version of the Synology Assistant software from the Synology website – it is available for both Windows and Mac. Install and run it on a computer. If you receive a message from the firewall on your computer, allow access for the Synology Assistant software. After a few seconds it should find the DiskStation or RackStation:

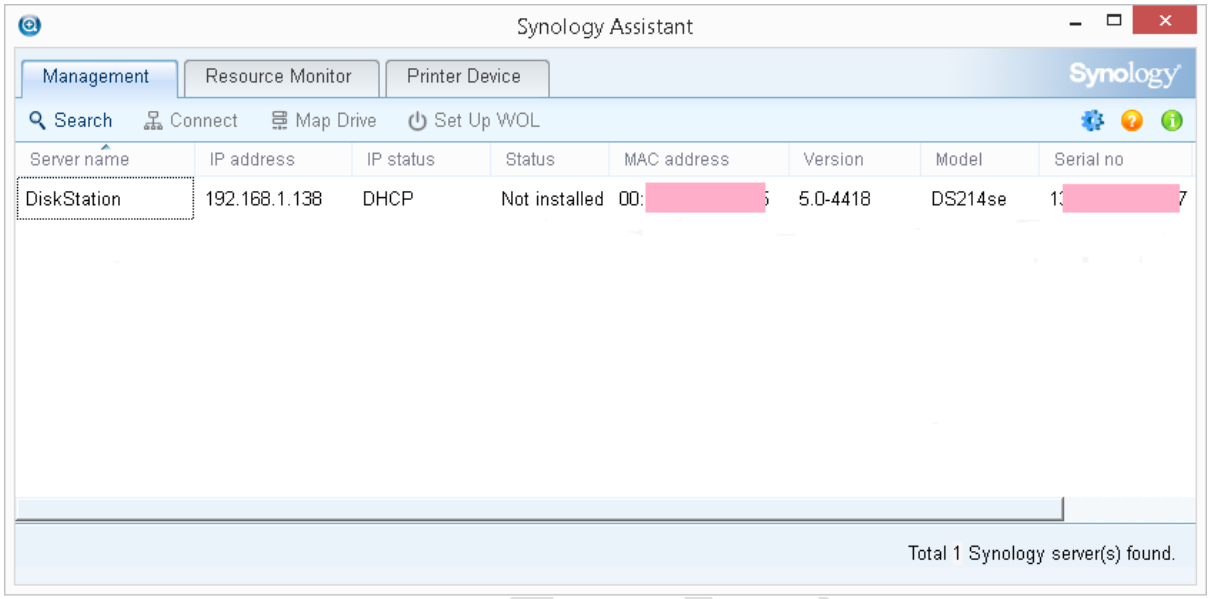

Figure 8: Synology Assistant

Right-click on the DiskStation entry and choose **Install**. As the DSM operating system has not yet been installed it will prompt for a disk image, known as a "PAT file" in Synology parlance. If the DiskStation came with an installation CDROM it will be on that, but in any case it is always best to download the latest one for the appropriate model from the Synology website. Click **Next**.

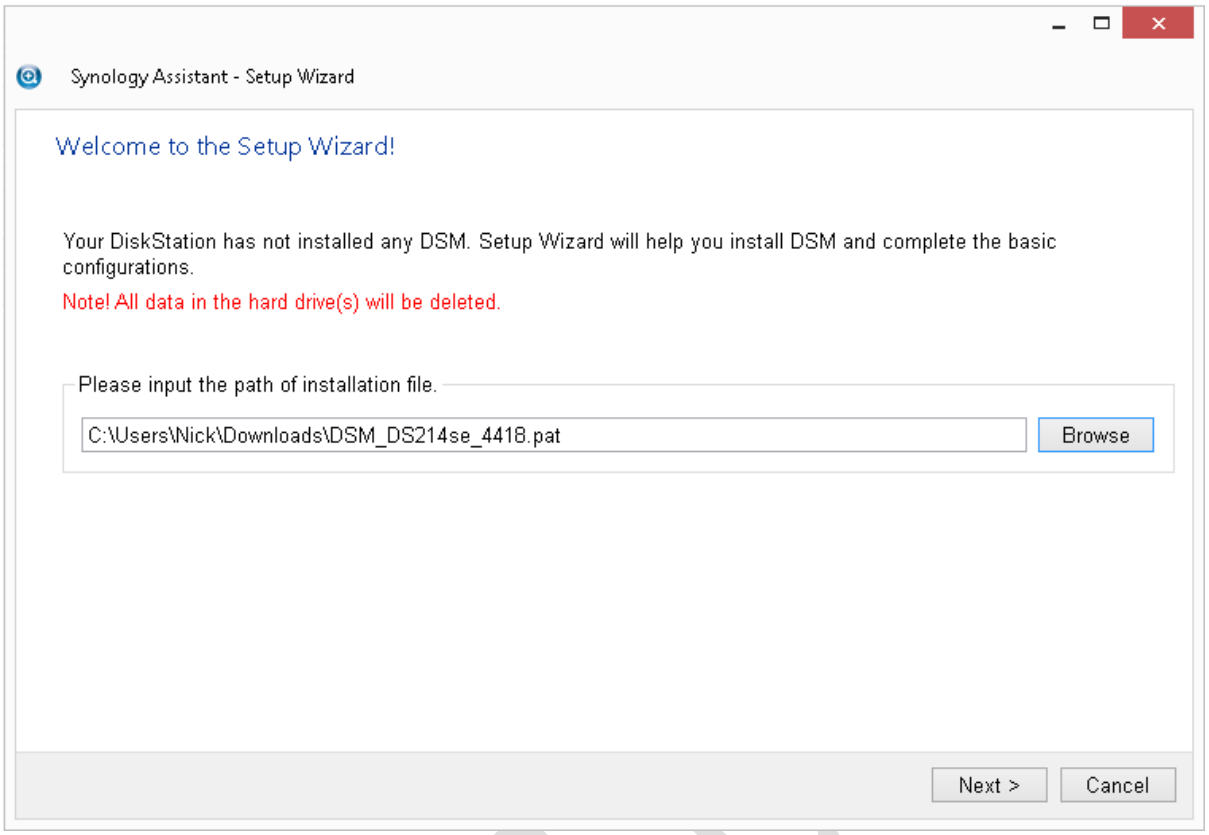

Figure 9: Specify the DSM installation file

You will prompted to enter and confirm a password for the main admin user – choose something non-obvious and make a note of it. You can also give the server a name – it is suggested that you simply call it *server*. Take the tick off the **Create a Synology Hybrid RAID (SHR) volume after installation** option and click **Next**.

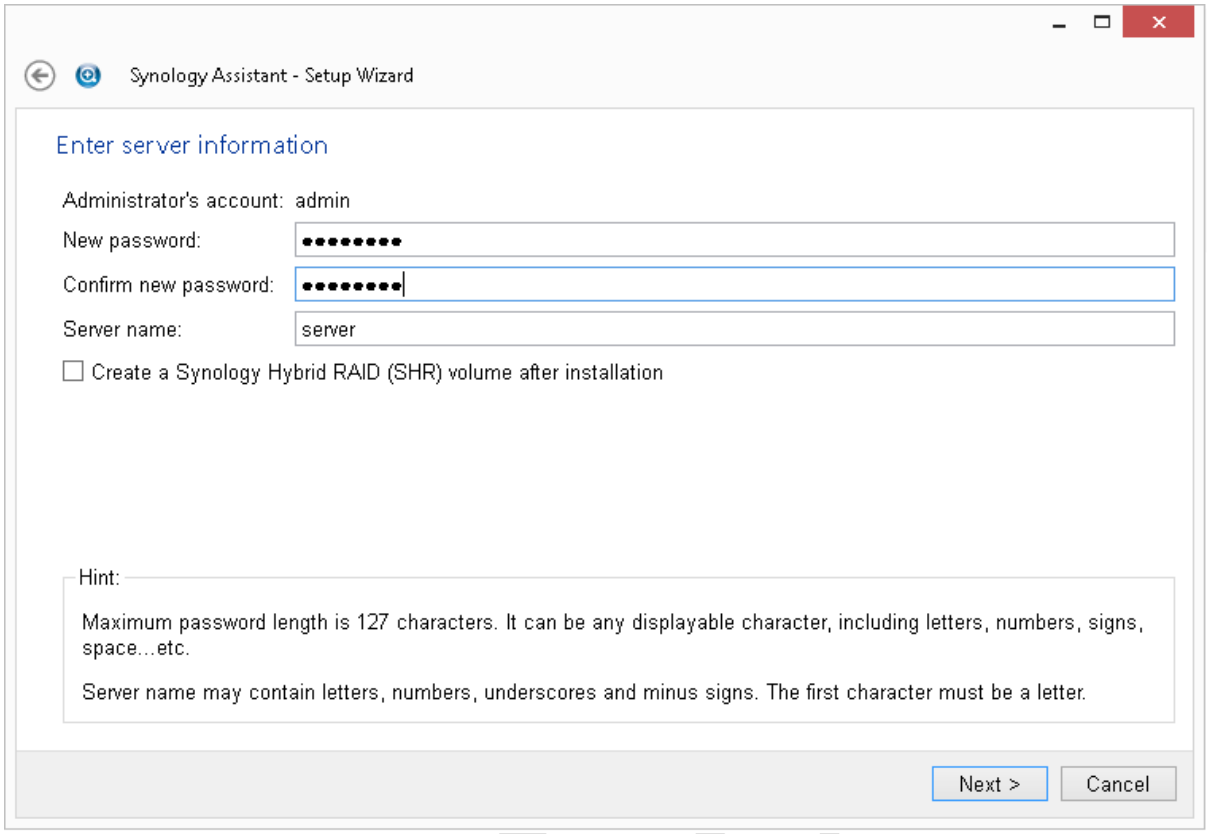

Figure 10: Specify the admin password and server name

The subsequent screen is concerned with the IP address of the server. For now, just accept the **Get network configuration automatically (DHCP)** option and click **Finish**.

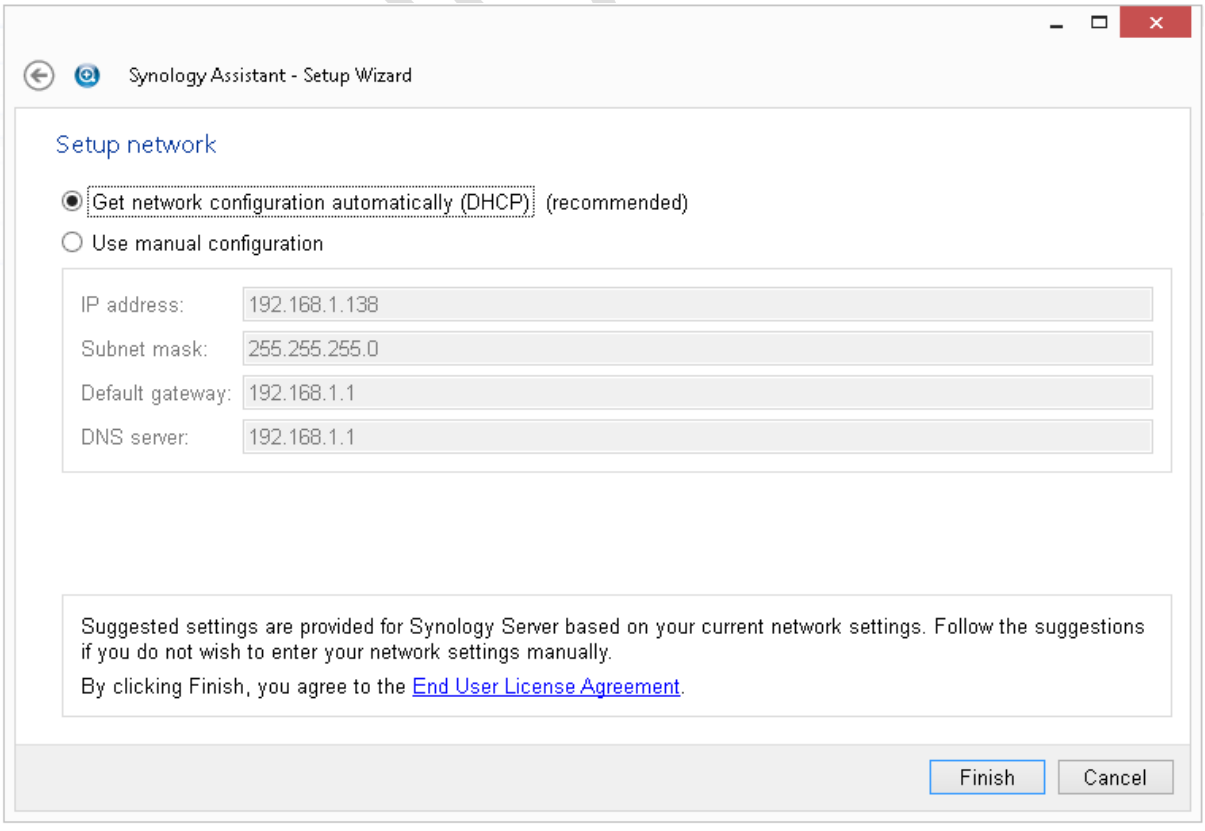

Figure 11: IP address settings

The installation now runs, during which time a progress screen is shown. This stage takes in the order of 10 minutes or so.

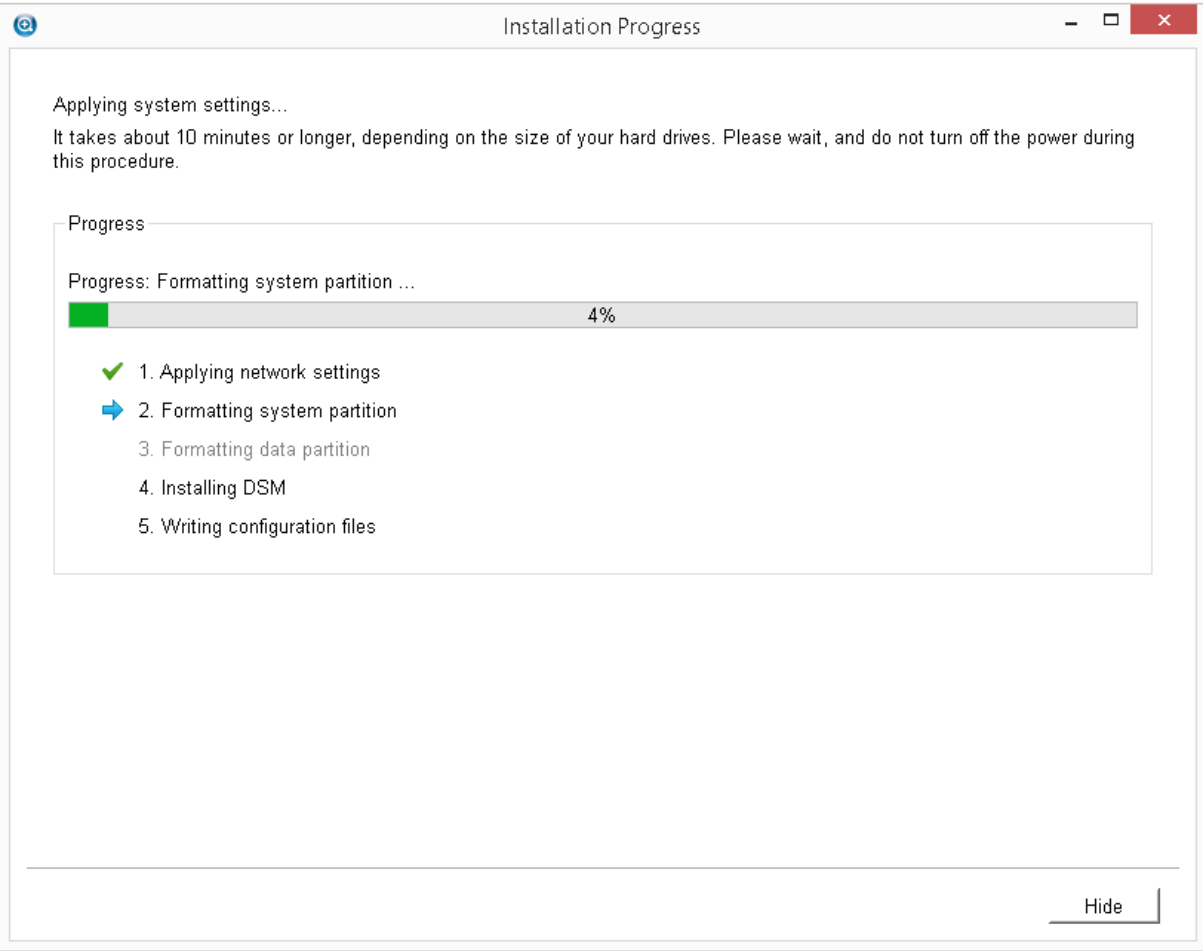

Figure 12: Progress screen

After installation has completed, click on **Close**.

The DiskStation should now be accessible from a computer with a browser on the same network. Load up your preferred browser (e.g. Internet Explorer, Firefox or Chrome) and enter *http:\\server* in the address bar.

2.3 Logging In For the First Time

If the login screen is not being displayed, enter *http://server* in the address bar of the browser:

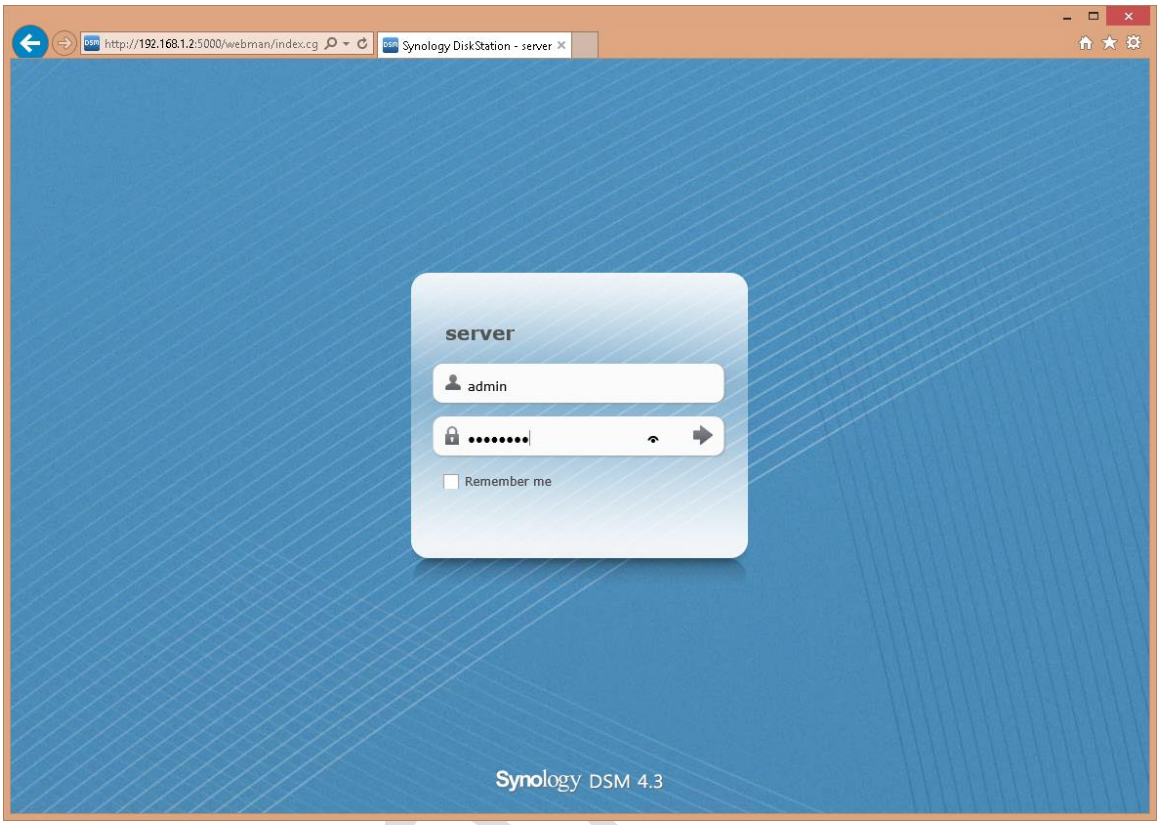

Figure 13: Login screen

Enter a user name of *admin* and the password you defined earlier. Upon logging in for the first time the *DSM Quick Start Wizard* screen is displayed:

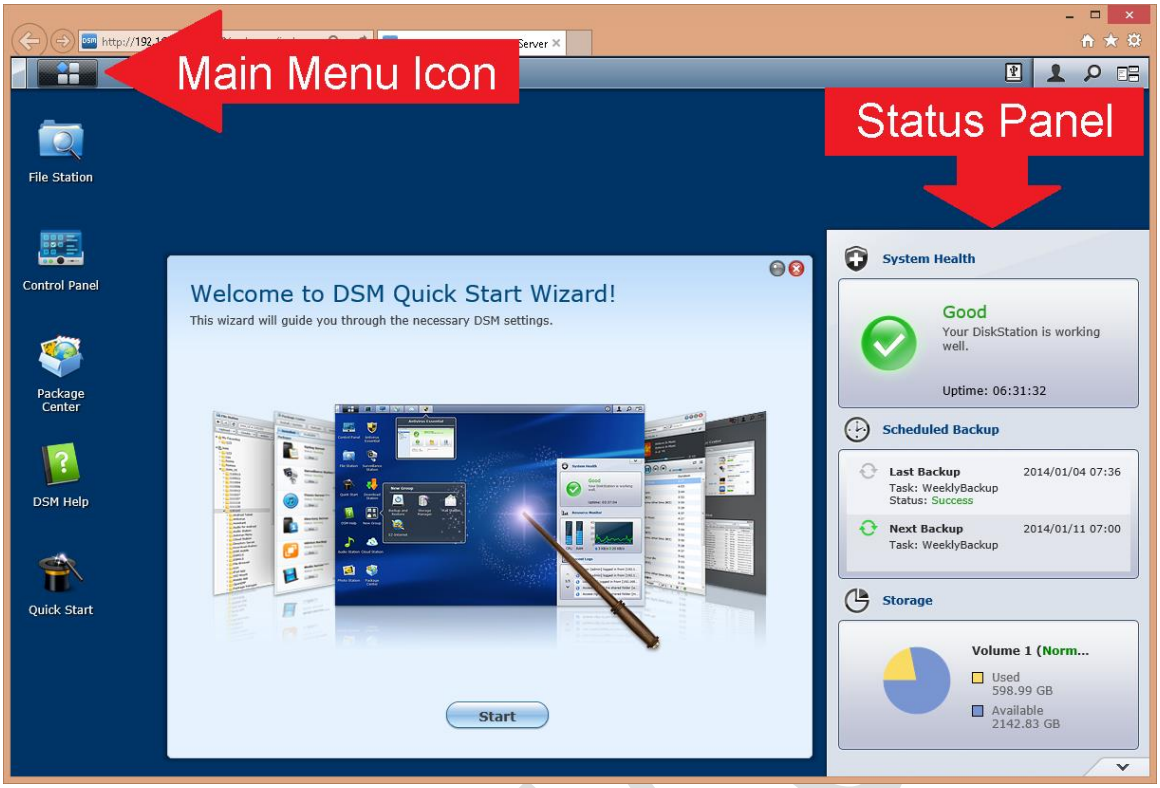

Figure 14: The Desktop

The DSM Quick Start Wizard is designed to help you get things up and running quickly, but lacks the flexibility we need. Close it by clicking on the cross in the top right-hand corner. You will be prompted as to whether you want to see it next time you login – click **No**.

The status panel at the right-hand side of the screen can be customised to display different options. Available options are: System Health; Resource Monitor; Storage; Scheduled Backup; Current Connections; File Change Log; Recent Logs. The first three are particularly useful. Monitoring and reporting are discussed later.

If unfamiliar with DSM, note the location of the Main Menu icon in the top left-hand corner of the screen. Along with the Control Panel icon on the Desktop, it is used in most aspects of configuring and managing the Server.

The first thing to do is to sort out the IP address for the server. During installation the DiskStation received an IP address from DHCP. However, file servers and NAS boxes are better off with fixed addresses so we need to change matters. Click **Control Panel** followed by **Network** then click the **Network Interface** tab.

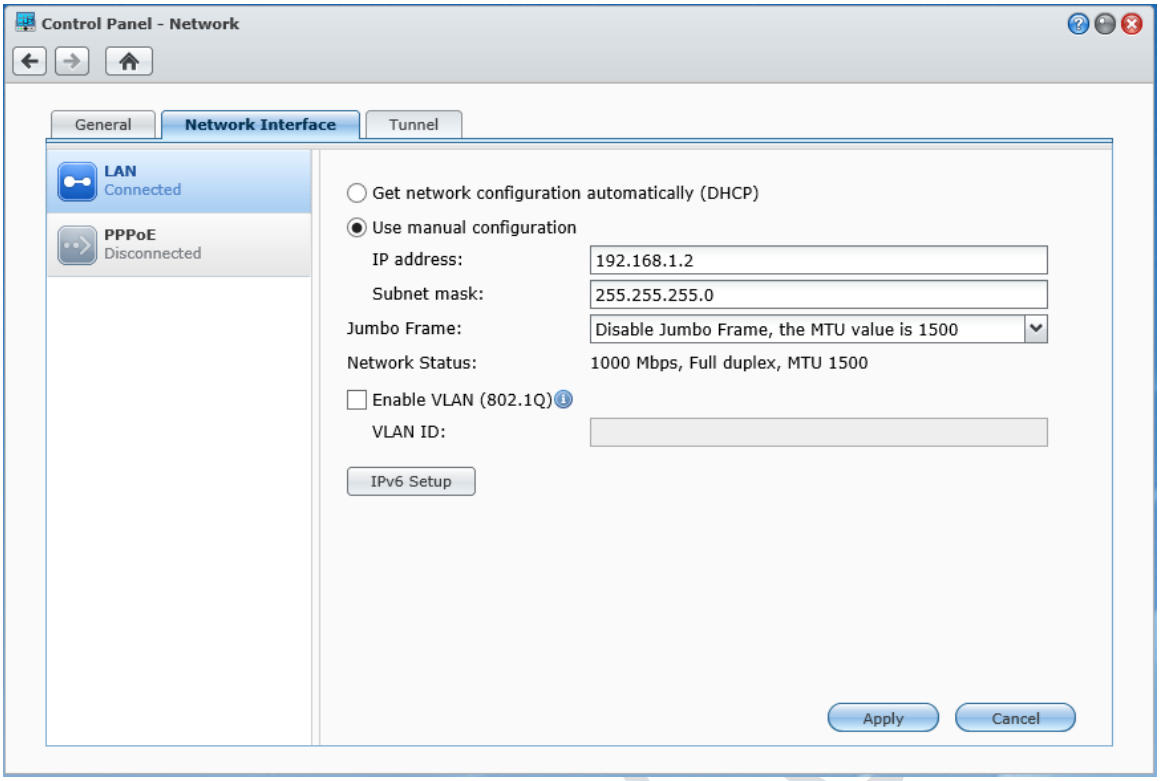

Figure 15: Specify a fixed IP address

Click **Use manual configuration** and specify an IP address that is adjacent to that of the router. In this example the internet router is 192.168.1.1 so we will choose 192.168.1.2. The 'Subnet mask' should be set to 255.255.255.0, then click **Apply**.

2.4 Creating the Disk Volumes

The next thing to do is to setup the disk volumes. Click on the Menu icon and choose **Storage Manager**. This will invoke the **Volume Creation Wizard**; click **Custom** followed by **Next**:

Figure 16: Creating a disk volume

From the next screen choose **Single Volume on RAID** and click **Next**. On the subsequent screen choose all of the drives and click **Next**. There may be a message about all the data on the disks being erased – click **OK** to acknowledge it.

On the screen after that specify the RAID type. The available options and best answer depends upon what hardware is in place, but should be RAID 1 for a small system with a pair of drives or RAID 5 for a system with more than two drives, as discussed earlier. A system with a single drive can only use Basic:

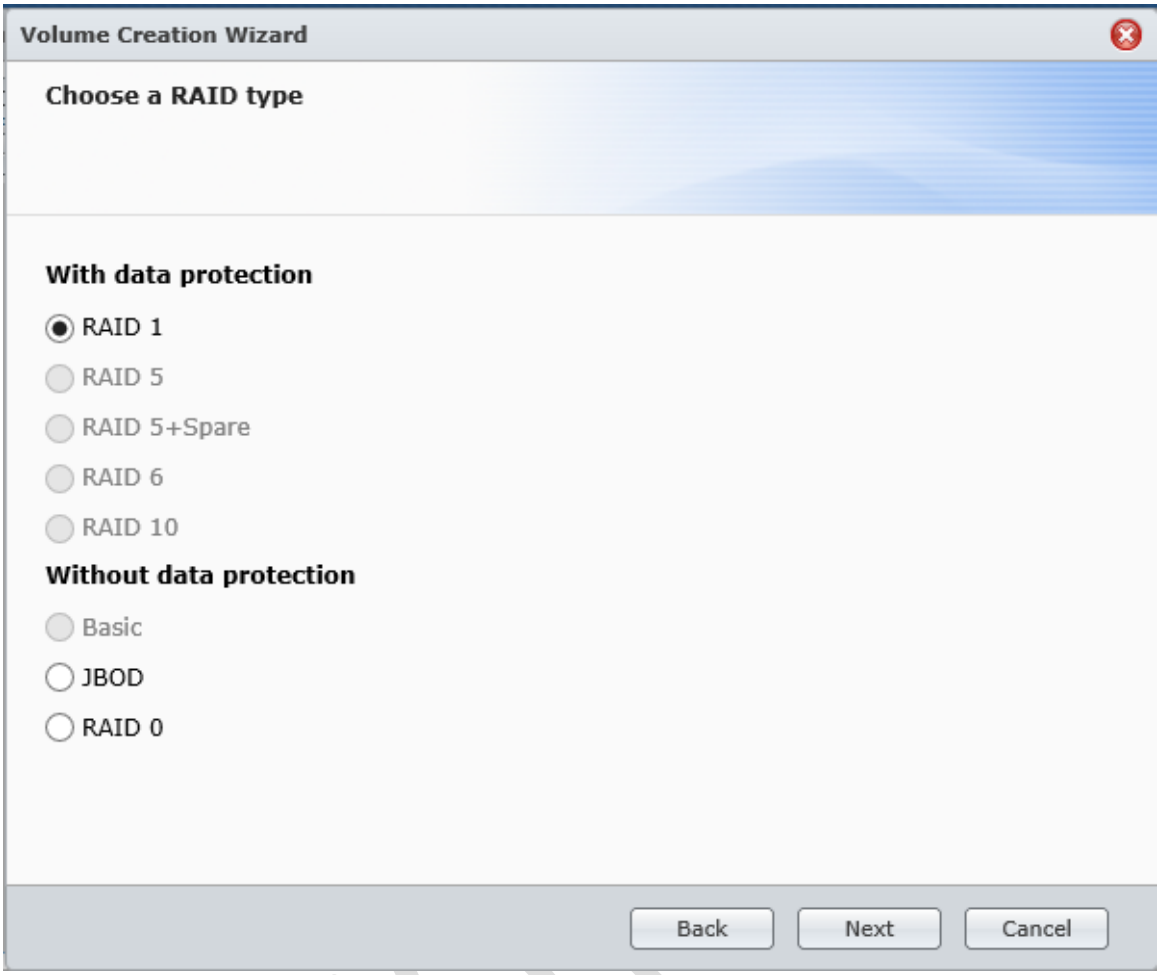

Figure 17: Choose a RAID type

The next screen will suggest a disk check – choose **Yes** and click **Next**, then click **Apply** on the following summary screen. Depending on the options and drives, this process may well take several hours. It may even need to run overnight if there are a lot of high-capacity drives. When the process is completed Storage Manager will display details of the volume and storage:

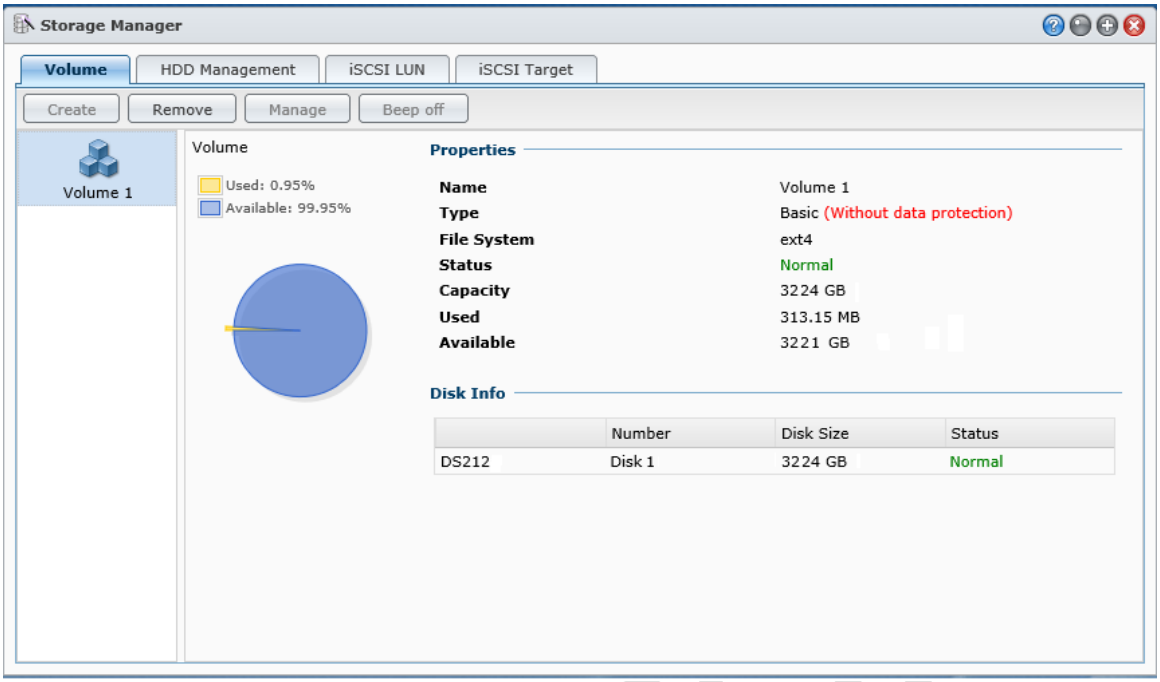

Figure 18: Volume status screen

2.5 Networking Configuration

By default, DSM will have switched on network services for Windows PCs and Apple Macs and setup a workgroup called *Workgroup*. To verify click on **Control Panel** > **Win/Mac/NFS** and check the Windows File Service tab. If Apple Macs are not used then the Mac File service can be disabled from its tab. The NFS Service will be disabled by default (this only needs to be enabled if Linux machines are used, which is not commonly the case in most small businesses).

It is unlikely that a small business will access the internet through a proxy server, but if it does then then the details will need to be entered. To do so, click **Control Panel** > **Network**. On the General tab, click **Connect via a proxy server** and enter the details of the proxy.

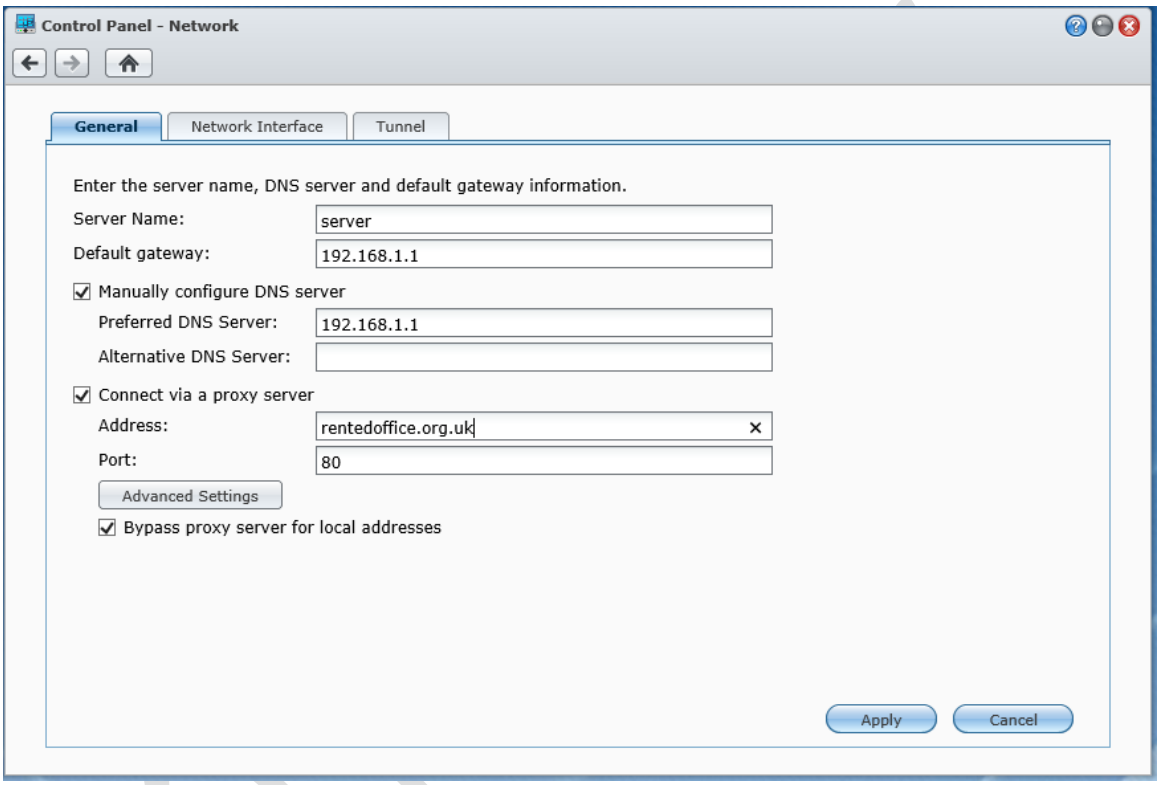

Figure 19: Proxy server settings

2.6 DHCP Considerations

In many small businesses, the router that connects them to the internet will also provide IP addresses for the computers and other devices via dhcp. If so DSM will use it, nothing further needs to be done about IP and you can skip to the next section. However, if this is not the case then the DiskStation/RackStation will need to be configured as a DHCP server, described below:

Click on the **Package Centre** icon and download and install DHCP Server. Once installed, it can be managed from the Main Menu or from the Network entry in Control Panel. Click on the Network Interface tab, then click on the **DHCP Server** button that will have been added to it. There are three tabs for the DHCP Server:

General - This is used to configure DHCP. Make sure the **Enable DHCP Server box** is ticked. The default value for the **Address lease time** of 600 minutes is fine. Enter the address of your **Primary DNS Server** and optionally add the **Secondary DNS Server** address. If you do not know the DNS addresses, login to your router and see what it is picking up. Alternatively, go to https://www.whatsmydns.net/dns/uk for many popular British ISPs or https://www.whatsmydns.net/dns/usa for many popular North American ISPs. There is no need to add a Domain name. Click on **Add** and enter details of the Subnet list i.e. the range of addresses for DHCP. In this example the Start IP address is 192.168.1.100, the End IP address is 192.168.1.250, the Netmask is 255.255.255.0 (it invariably is in small networks) and the Gateway (internet router) is 192.168.1.1. Click on **Apply**.

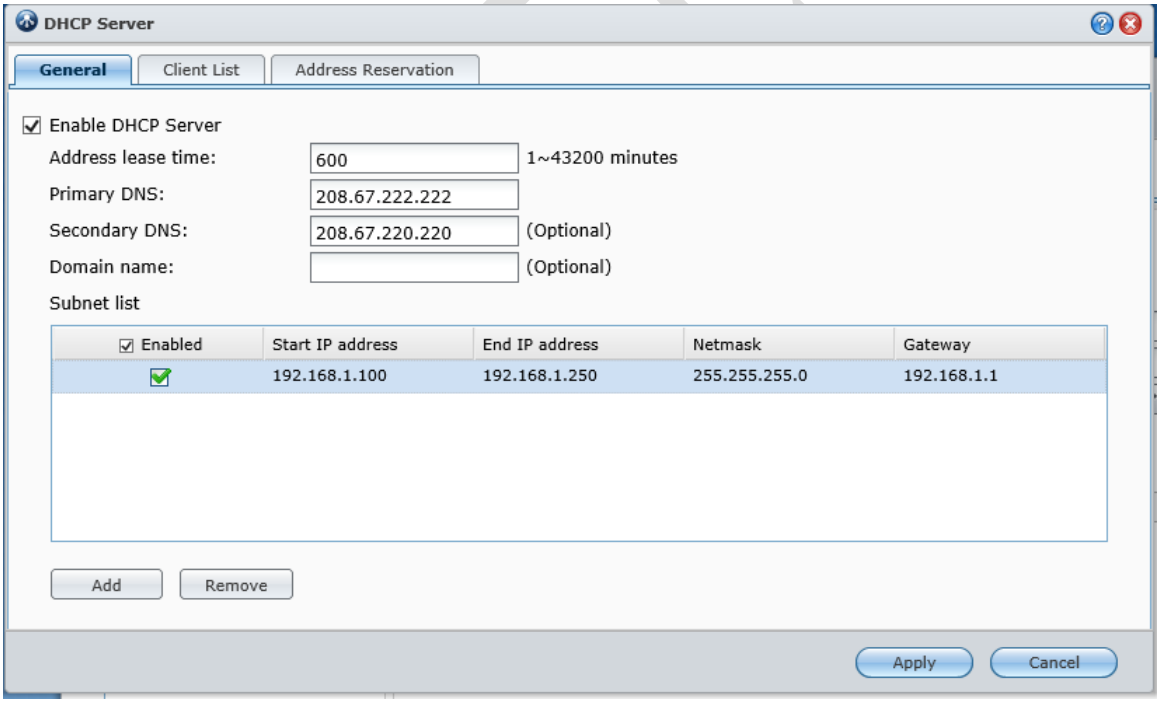

Figure 20: DHCP settings

Client List - This lists the devices which have received leases along with the details of those leases. There is nothing to configure here, it is used for monitoring what is going on.

Address Reservation - This is used for making IP reservations, which is the preferred method for handling devices such as printers and wireless access points.

2.7 Power Management

The DiskStation/RackStation has five options related to power management. Some of these are to do with energy saving and can be used to reduce power consumption and hence save money. To access, go into **Control Panel** and click **Hardware** to display the following panel (note that there are some minor variants in these panels depending upon the model you have):

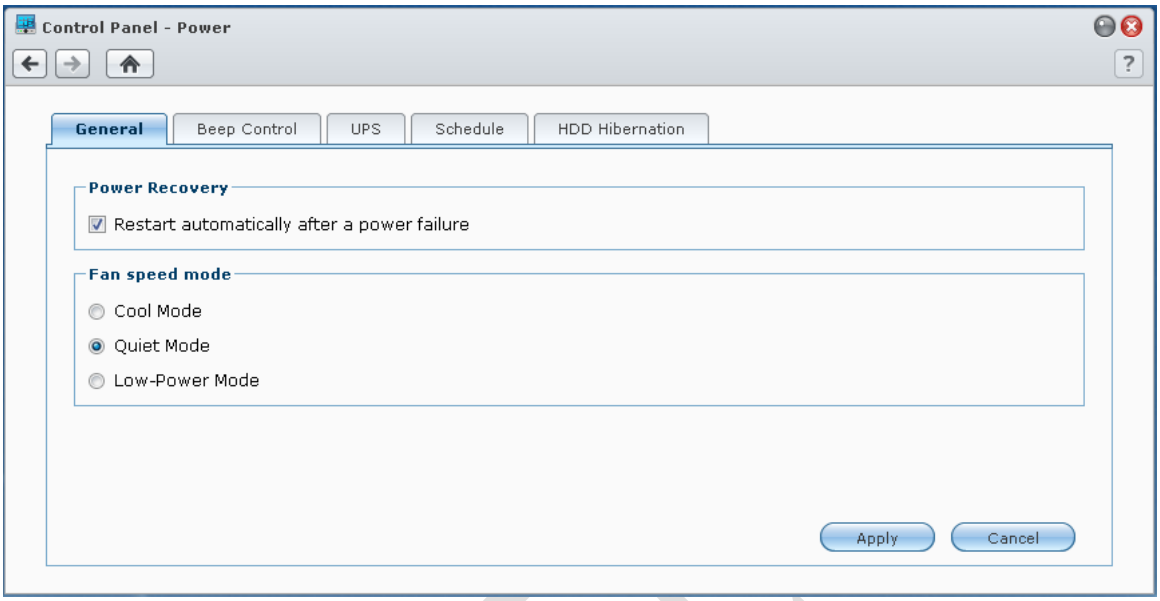

Figure 21: Power Management

General - Under Power Management, tick 'Restart automatically after a power failure'. If the server is located in an area where people are working set the Fan speed mode to 'Quiet Mode', otherwise set to 'Cool Mode'.

Beep Control - In the event of certain error conditions (e.g. fan failure) the Server will make a beeping noise. There are four options – make sure all are ticked.

UPS - The Server should be connected to an UPS (Uninterruptible Power Supply) via an USB cable. Tick the 'Enable UPS Support' box. Leave the 'Network UPS Server IP' blank (as there is unlikely to be one). The 'Time before DiskStation enters Safe Mode' can be left at the default value.

Schedule - Most DiskStation/RackStations can be programmed to power themselves on and off, thus enabling energy usage to be minimised and security to be enhanced. However, note that if this is to be done then it is important to check that it will not be powered down when an activity such as backup or an anti-virus scan is scheduled to take place.

To create a schedule, click the **Create** button on the Schedule tab. Specify whether the event is to Startup or Shutdown and whether it is to run daily, weekly or at weekends (it is also possible to specify particular days of the week). Then click on **OK**. Make sure the task is Enabled (which it will be if it has just been created), and to click **Save**.

In this example, the server is programmed to startup at 6:00am each morning and shutdown at 11:55pm each night:

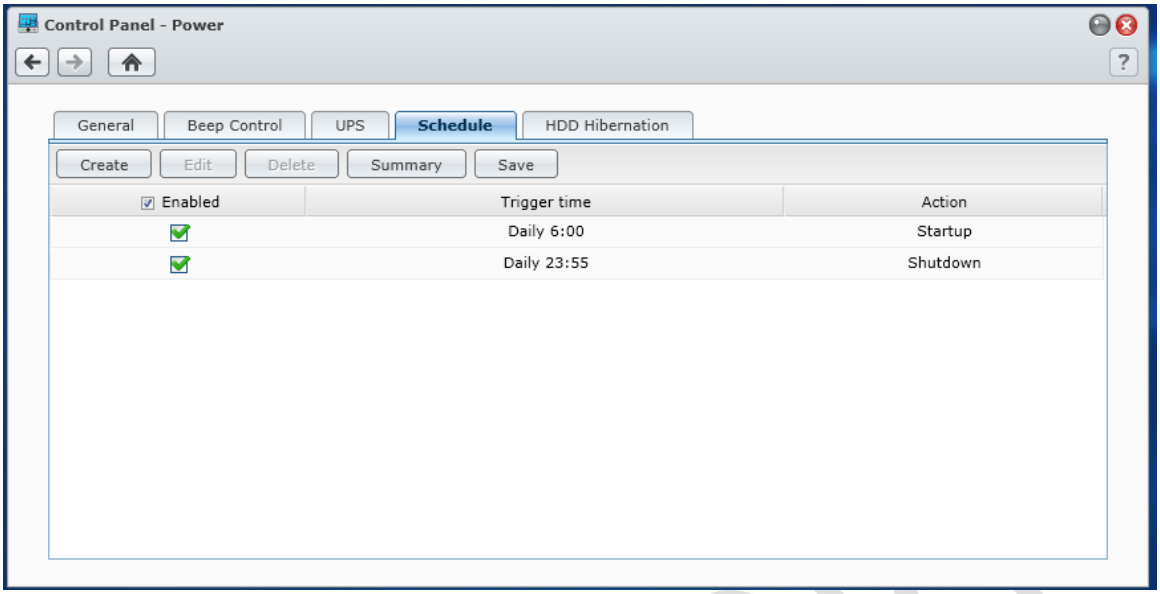

Figure 22: Scheduled startup and shutdown

HDD Hibernation - The hard disk(s) can be programmed to hibernate after a set period. This also saves energy, but may result in a short delay when someone attempts to access the server (typically in the order of about 15 seconds). Power to an external USB hard disk (e.g. a backup unit) can also be managed:

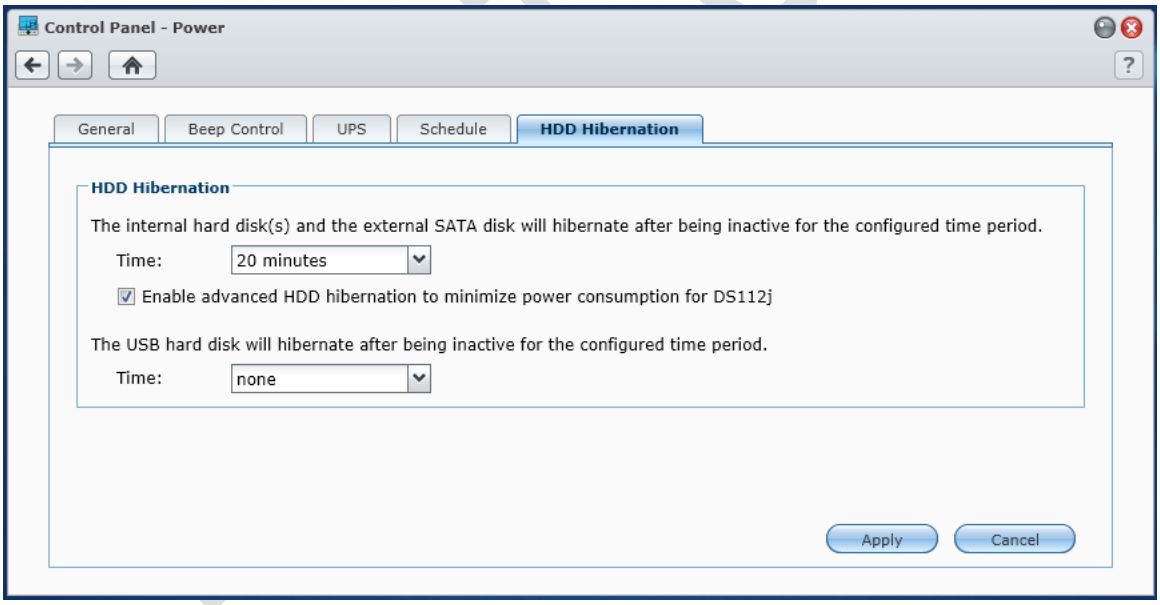

Figure 23: HDD hibernation

3. Folder Structure and Shared Folders

The basic purpose of a network is to provide an environment for users to store and share information. This is done by creating folders on the server, some shared and some private, then defining access rights to control who sees what.

The structure of these folders will depend upon the requirements of the organisation. But a typical arrangement would be:

- A shared, company-wide folder that everyone has access to
- Individual private home folders for each user
- A location to store master copies of programs, drivers, utilities and so on

To create a top level shared folder, choose **Control Panel** > **Shared Folder** and click **Create**. Fill in the detail (most of the fields can actually be left blank) and click **OK**:

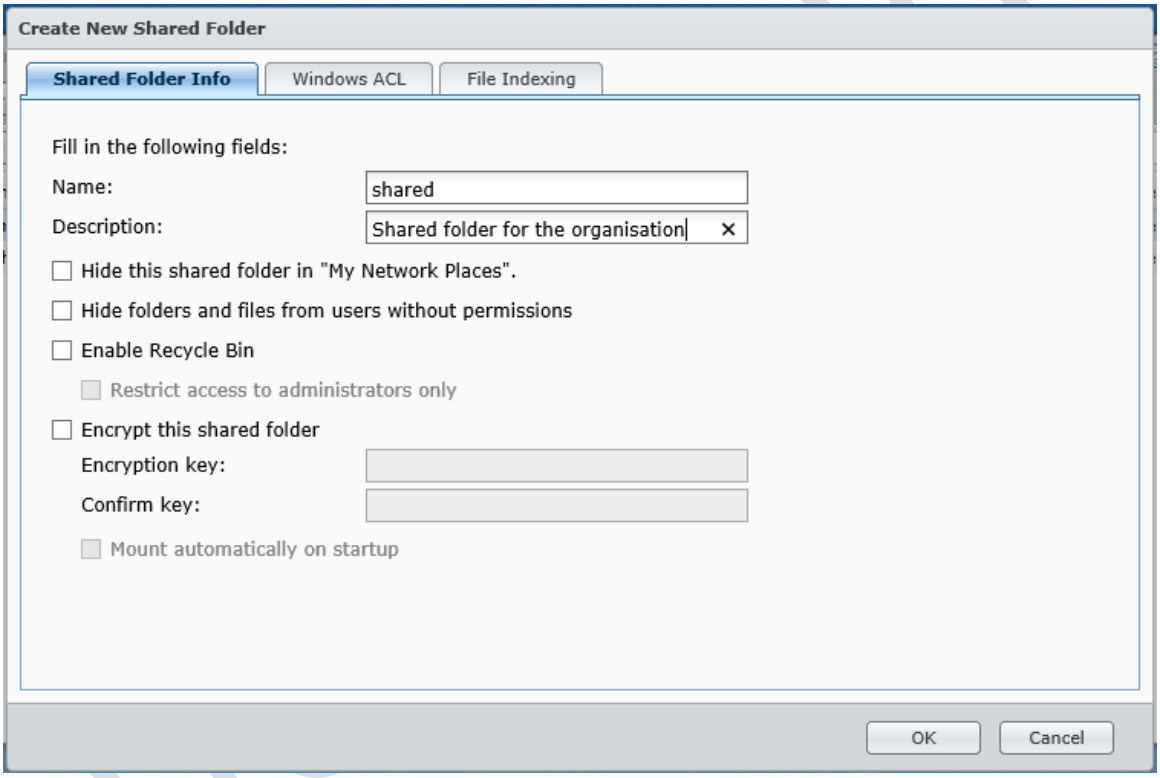

Figure 24: Creating a new shared folder

A second screen, which is concerned with permissions and access, will be displayed. At this point we haven't yet defined the users, so just set it for Read/Write access for *admin* and click **OK** (we will revisit this later when the users have been created).

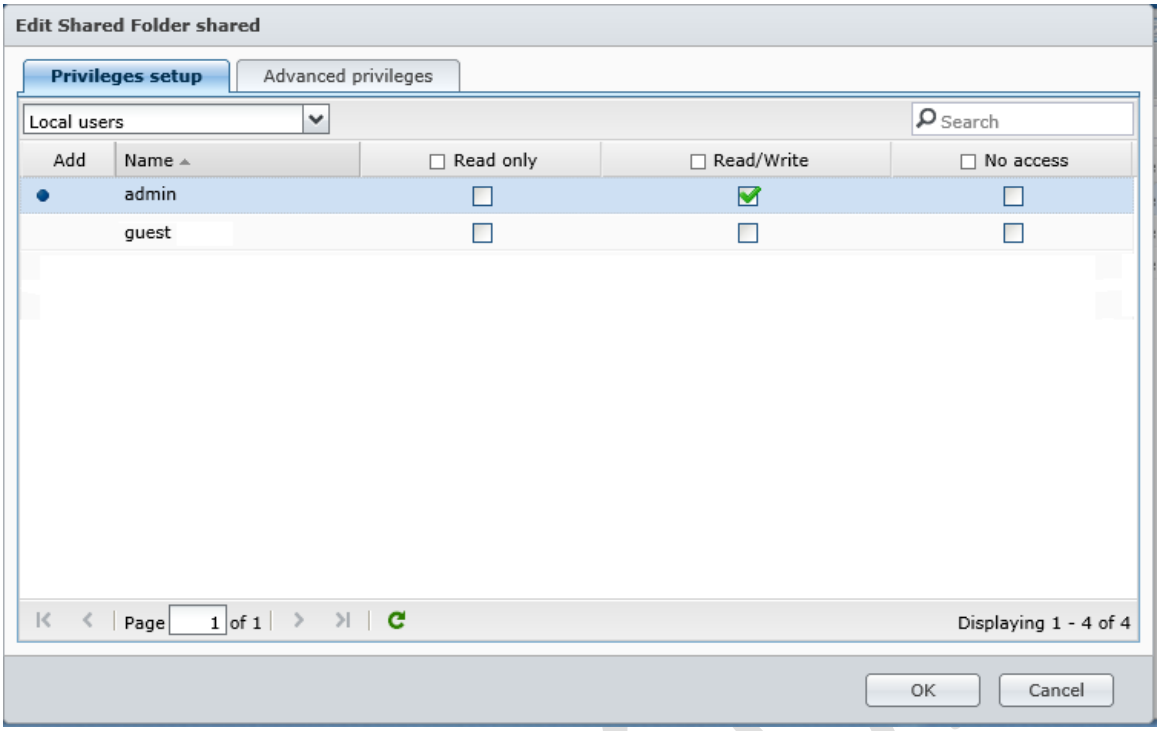

Figure 25: Privileges for shared folder

Create a shared folder called *technical* in the same way, but this time tick the 'Hide this shared folder in My Network Places' and 'Hide folders and files from users without permissions' boxes.

Go to **Control Panel** > **User**. Click the **User Home** button and then tick the **Enable user home service** option. Click **OK**. This will cause home folders to be created automatically for any users that are subsequently defined.

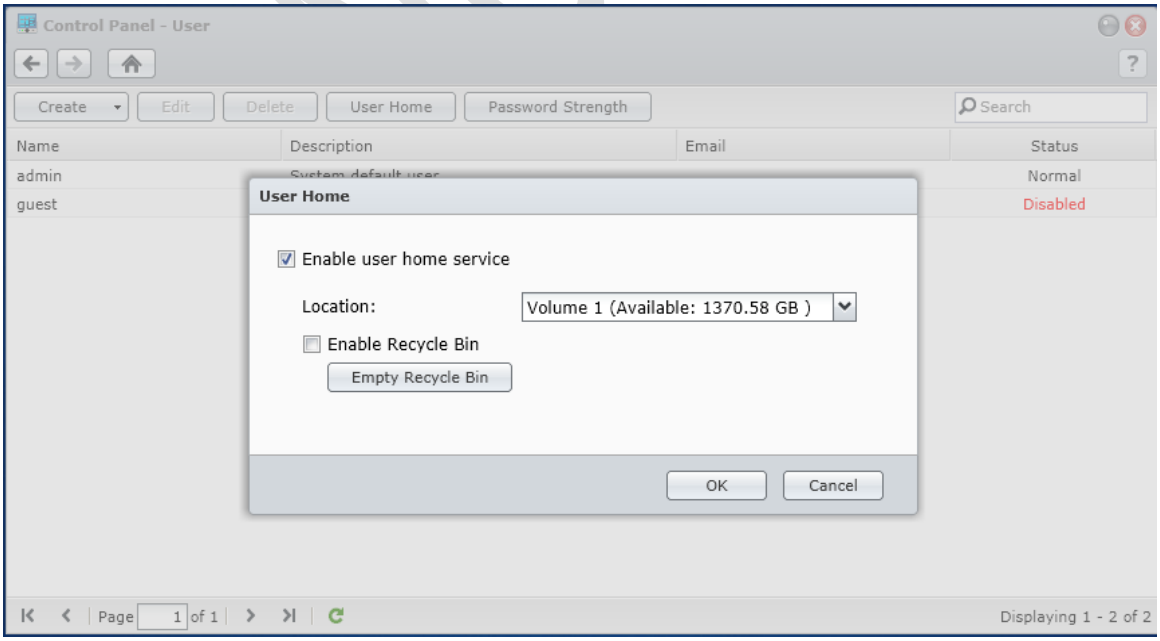

Figure 26: Enable user home service

Having enabled the User home service, go to **Control Panel** and click on **Shared Folder**. Double-click the entry for the *homes* folder; tick the 'Hide this shared folder in My Network Places' box and click **OK**. Then close the Shared Folder screen.

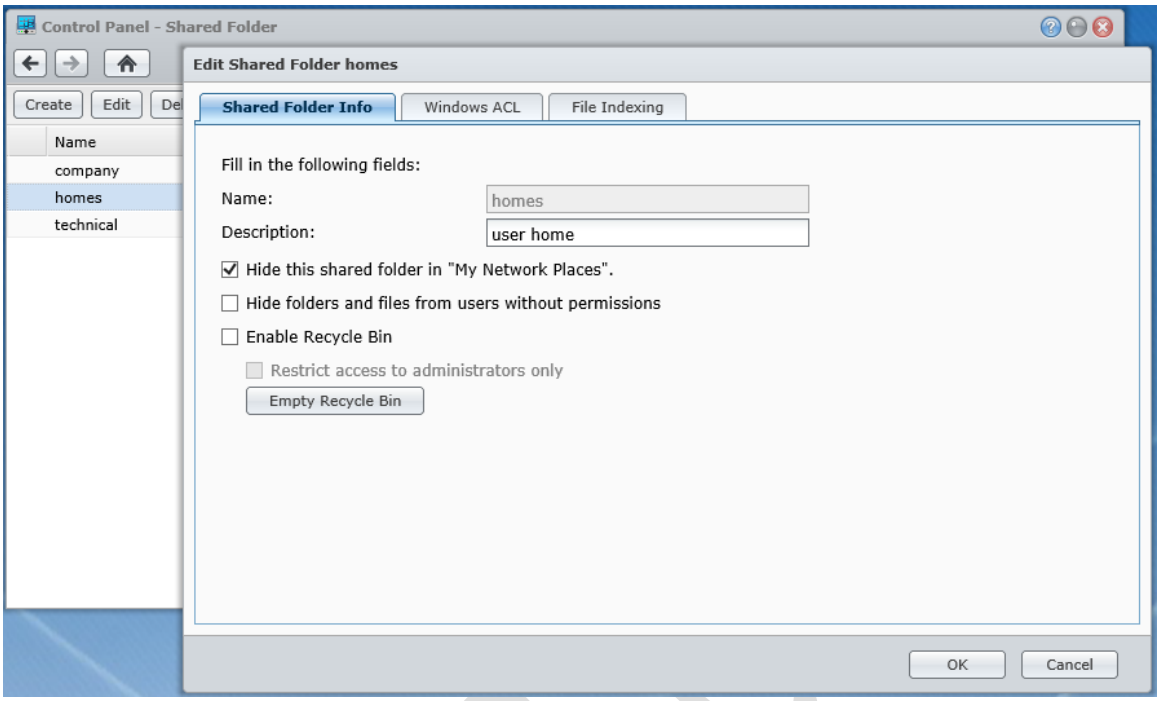

Figure 26: Hide the user home folders

Launch **File Manager**. Click on the *technical* folder. Use the **Create** button to create four sub-folders within it: *software*, *drivers*, *images*, *utilities*. Note that the Create button can define two types of folders: (standard) folders and 'New Shared folders'. We want standard folders.

When completed, the folder structure should look like this within File Station:

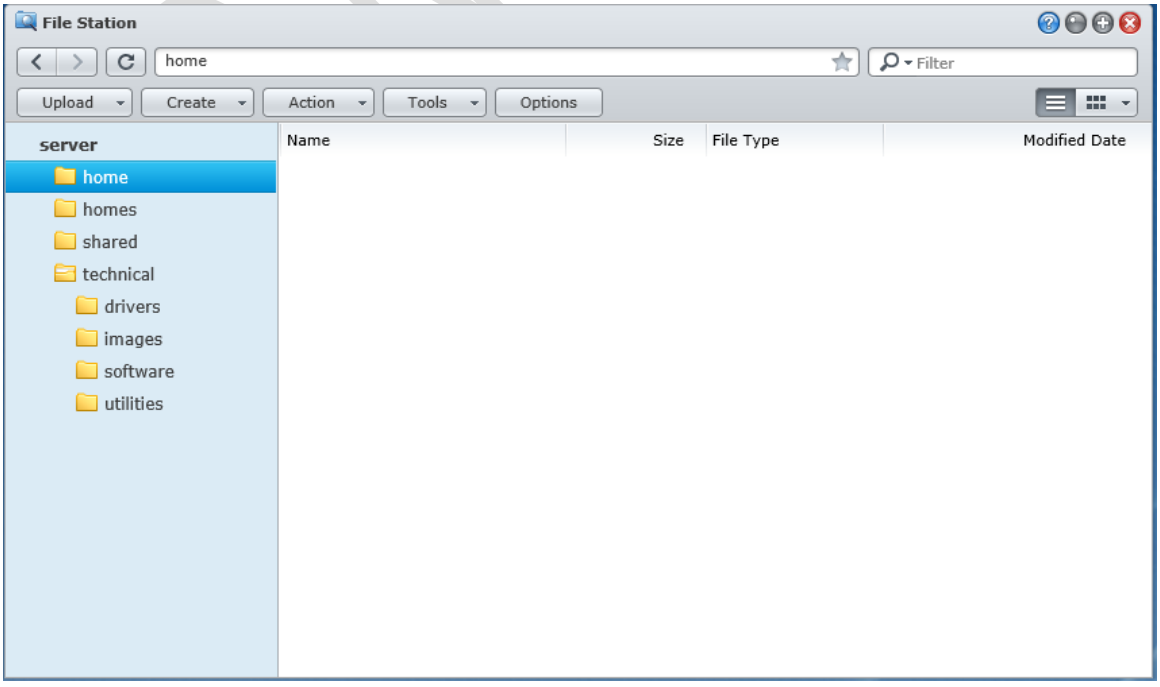

Figure 27: File structure

At this point it should be possible to view the folders from a connected PC by choosing **Start** > **Run** and typing in *server* (it will be necessary to enter the admin id and password for the Server). Note that to view the hidden technical folder it is necessary to type *server**technical*. If this does not work, type in the IP address of the server instead e.g. *192.168.1.2**technical* in our example.

4. Creating Users

At this stage the user accounts should be created on the Server. Whilst the creation of accounts is very straightforward, some thought needs to be given to the naming conventions and methods of working. The reasons for this will become more apparent later but some of the considerations are:

- Are the computers new or existing ones?
- Does each user have their own computer or do they share?
- Is there a requirement for any user to be able to use any computer?
- How many users are there?
- Is it essential to make things as easy and automated as possible or is a small amount of effort from the users acceptable?

As a general point, the more consistency there is then the better things will be. For user names, two common conventions are to use the first name plus the initial of the surname, or the initial of the first name plus the surname, although in some parts of the world other conventions might be more appropriate. In the case of particularly long names and double-barrelled names it might be an idea to abbreviate them. For example:

Name of person	User name
Nick Rushton	nickr
Mary O'Hara	maryoh
Ian Smith	ians
Amber Williams	amberw

Alternatively:

Name of person	User name
Nick Rushton	nrushton
Mary O'Hara	mohara
Ian Smith	ismith
Amber Williams	awilliams

To create a user, launch Control Panel and click the **User** icon. Click on the **Create** button to display the following panel:

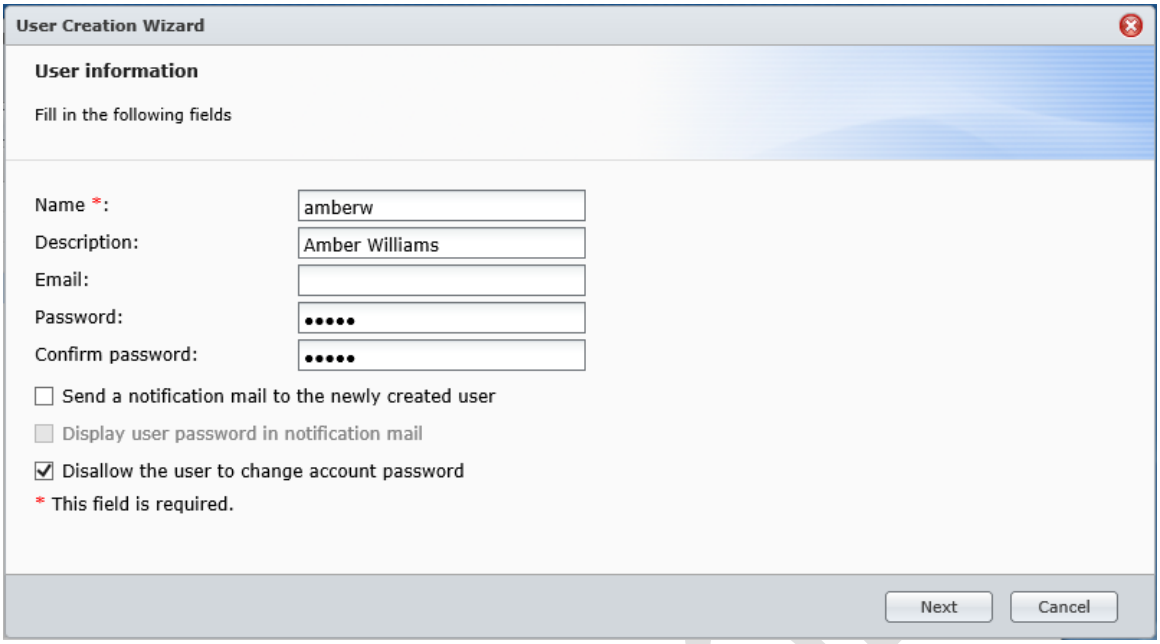

Figure 28: Creating a user

Enter: the user's login name; a description for them (e.g. their full name); a password and its confirmation. Click the 'Disallow the user to change account password' box. It is not necessary to specify the email address or send a notification to the newly created user. Click on **Next**.

On the subsequent screen make sure they are a member of the *users* group then click **Next**.

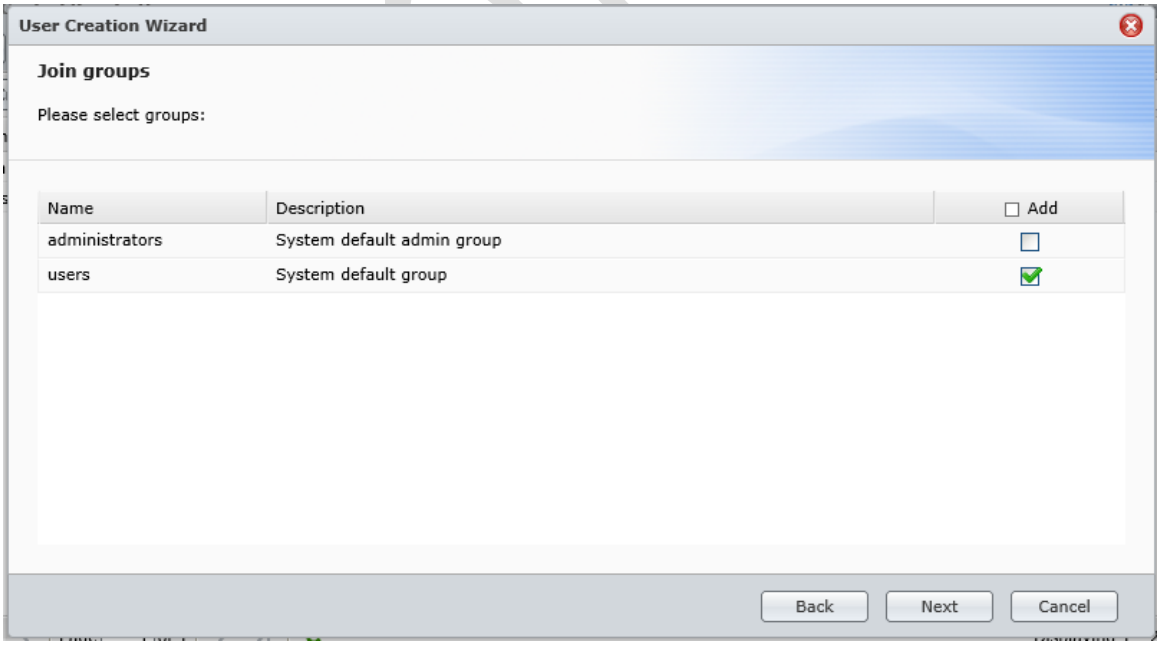

Figure 29: Group membership

The next screen defines what folders the user can use. Give them Read/Write access to the *shared* folder but no access to the homes or technical folders. Click **Next**.

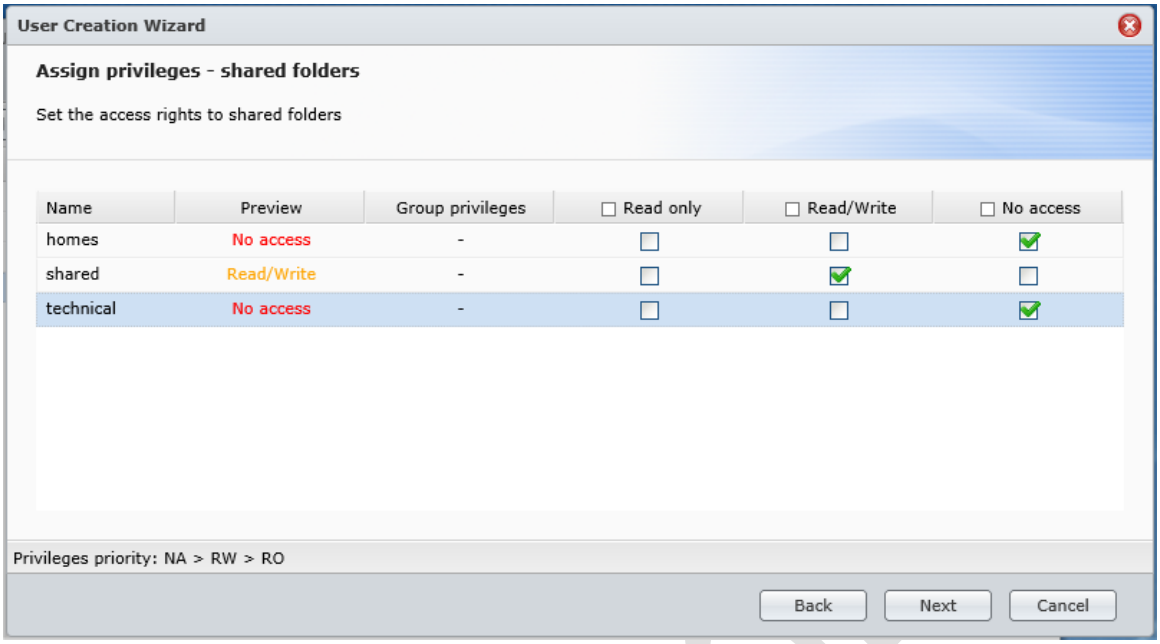

Figure 30: Assign privileges to shared folders

The next screen allows you to define how much storage space the user has. As disk space is cheap these days you may wish to simply ignore this by clicking **Next**. The subsequent screen controls access to some of the DSM applications. FTP is less widely used these days so take the tick off unless you are specifically intending to use it, then click **Next**:

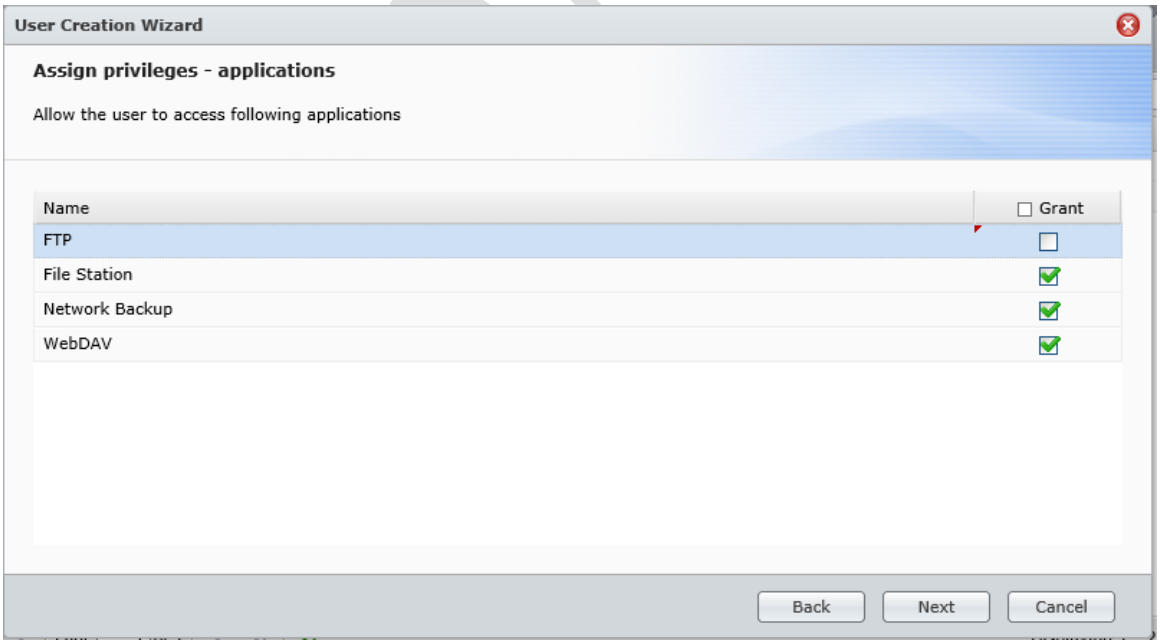

Figure 31: Assign privileges to applications

The next screen is not very useful so just click **Next**:

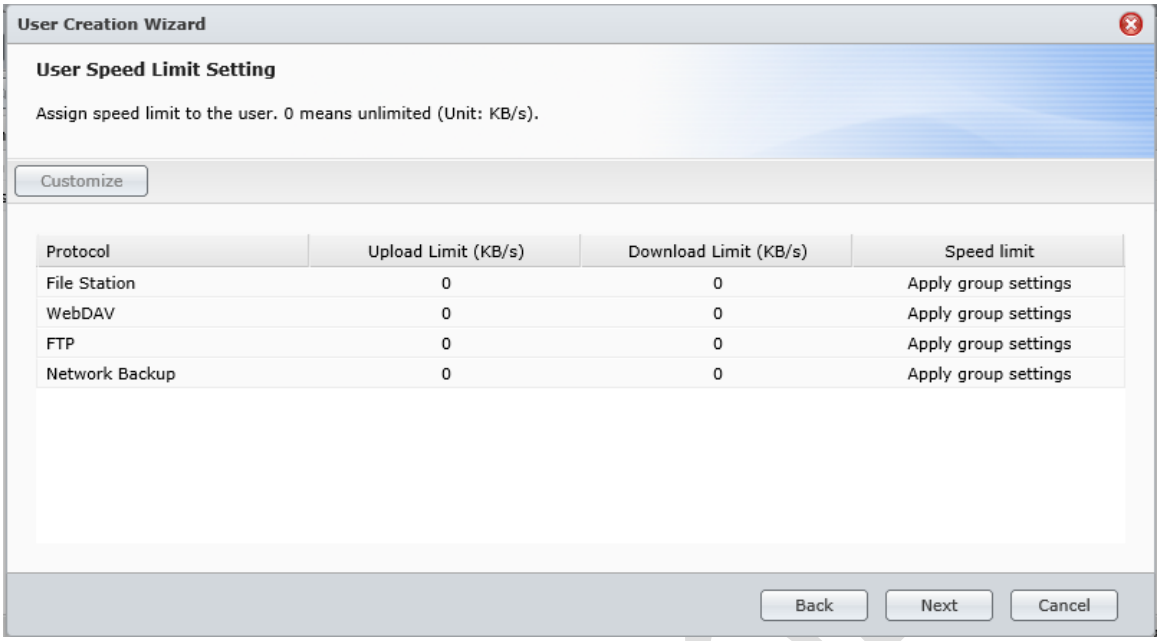

Figure 32: User speed limit setting

Finally a confirmation screen is displayed – click **Apply** to create the user.

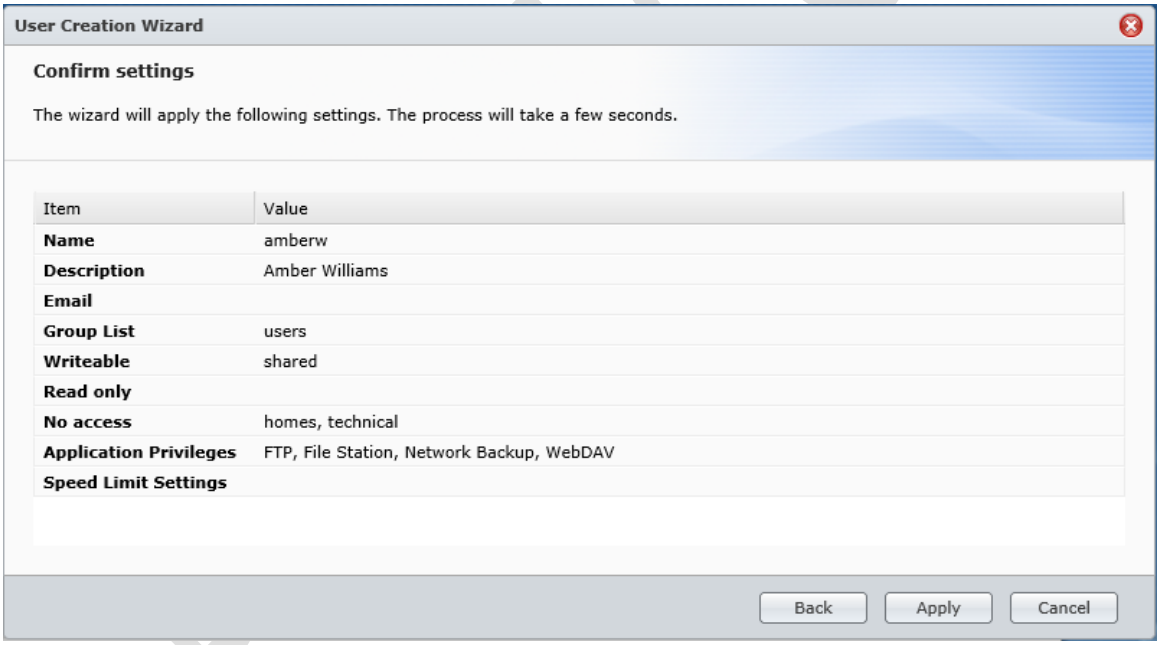

Figure 33: Confirmation screen

Repeat these steps until all of the users have been created.

5. Accessing the Server

There are several methods for accessing the DiskStation. The first is by using a browser, the second is by typing in the name of a shared folder, the third is by mapping the shared folders as disk drives (plus there are three methods of doing this). Each approach has it merits.

5.1 - Using A Browser

This is the most basic method for accessing the DiskStation and works for Windows PCs and Macs. Simply go to any computer on the network, launch a browser such as Firefox, Internet Explorer or Chrome and type in the IP address of the server e.g. 192.168.1.2 or whatever it is. The standard DSM login screen is displayed; the user should enter their name and password and they will be presented with a fairly minimalist Desktop; in essence, all they can access is File Station (unless additional options have been granted to them). File Station can be launched by clicking on its icon, which appears on the Desktop and also in the Main Menu. Within File Station they can see only the folders and files that belong to them or to which they have been granted access, such as their home folder and any shared folders.

To work with a file or folder, right-click it and a pop-up menu will appear with the various available options. Alternatively, click the **Action** button:

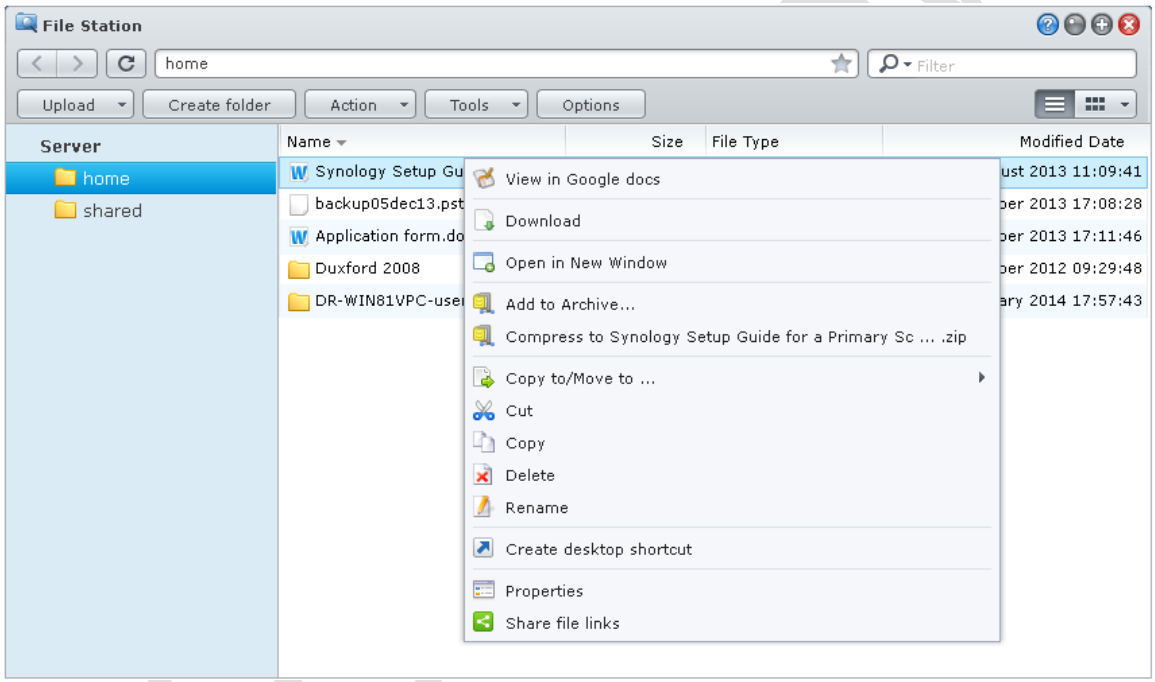

Figure 34: Using File Station

There is an option to view documents, spreadsheets and presentations using Google docs, although there are some restrictions on the maximum size of files that can be viewed in this way. Also note that this is a viewer only and not an editor. If it is required to edit a file, choose the **Download** option to first download it to the local computer. Make the changes to the document using Word, Excel or other preferred application, then use the **Upload** button in File Station to upload the new version back to the server.

Most graphic files and photographs can be viewed by double-clicking on them. From there they can be zoomed and manipulated.

When the user has finished the remote session, they should logout. To this, click on the **Options** icon in the top right-corner of the screen and click **Logout**:

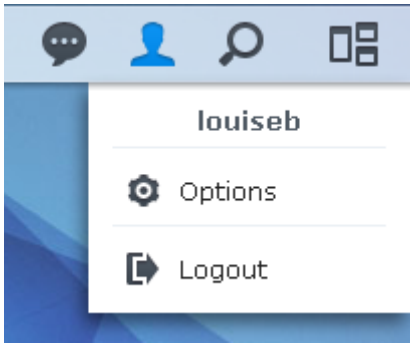

Figure 35: Options icon

5.2 - Accessing A Shared Folder

To access a shared folder from a Windows PC click **Start** then choose **Run** (in the case of Windows 8.1 right-click the **Start** button then choose **Run**). Alternatively, hold down the **Windows key** and press the letter **R**. In the small dialog box that appears, type in the name of the shared folder e.g. *server**shared* and click **OK**.

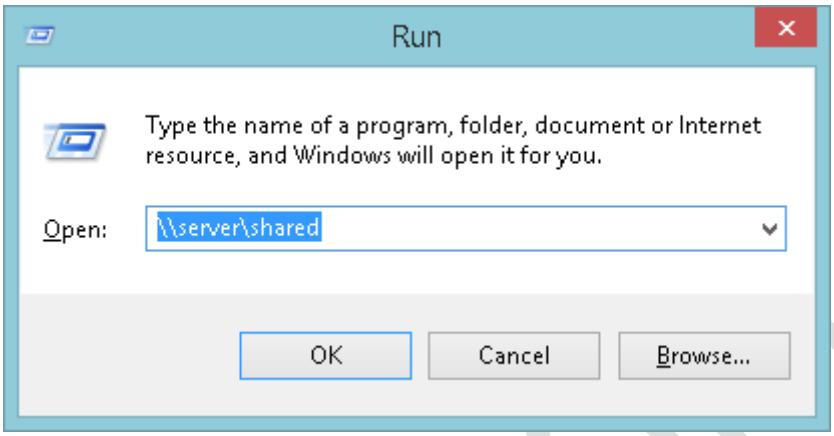

Figure 36: Accessing a shared folder

The contents of the folder will be displayed in Windows Explorer, from where the files can be used in the standard way.

5.3 - Mapping The Drives Manually

Network drives can be mapped using Windows Explorer:

If using Windows 8 or Windows 8.1, open Windows Explorer (which appears on the Taskbar by default). On the menu bar click **Computer** then click the **Map network drive icon** on the ribbon, followed by **Map network drive** on the dropdown.

If using Windows 7, open Windows Explorer, which appears on the Taskbar by default, else click **My Computer** on the **Start** menu. If the menu bar is not displayed, click **Organize** > **Layout** > **Menu bar** to display it. From the Menu bar choose **Tools** > **Map Network Drive**.

If using Windows Vista, run Windows Explorer by clicking **Start** > **All Programs** > **Accessories** > **Windows Explorer**, else click **Computer** on the **Start** menu. If the menu bar is not displayed, click **Organize** > **Layout** > **Menu bar** to display it. From the Menu bar choose **Tools** > **Map Network Drive**.

If using Windows XP, run Windows Explorer by clicking **Start** > **All Programs** > **Accessories** > **Windows Explorer**, else click **My Computer** on the **Start** menu. From the menu bar choose **Tools** > **Map Network Drive**.

On the resultant panel choose a drive letter from the drop-down. For the Folder, click on the **Browse** button and navigate through the network to find the server and the desired folder. Or, simpler still, just type in the name of the folder:

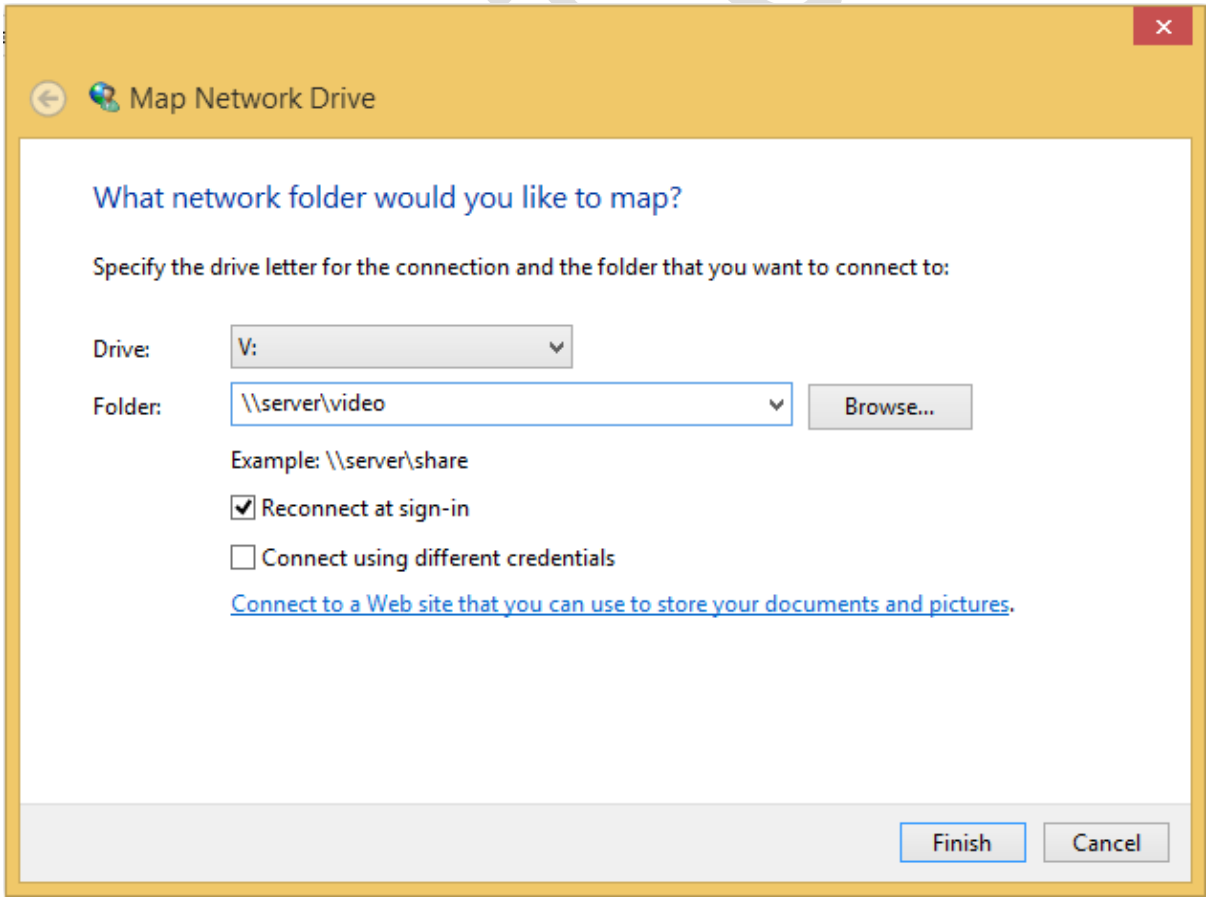

Figure 37: Mapping a drive

If the computer is only ever used by one person tick the **Reconnect at sign-in** box – this will cause Windows to remember the mapping. Then click **Finish**. You will be prompted to enter the user's name and password that were defined earlier on the DiskStation. Again, if the computer is used just by one person tick the **Remember my credentials** box. Then click **OK**.

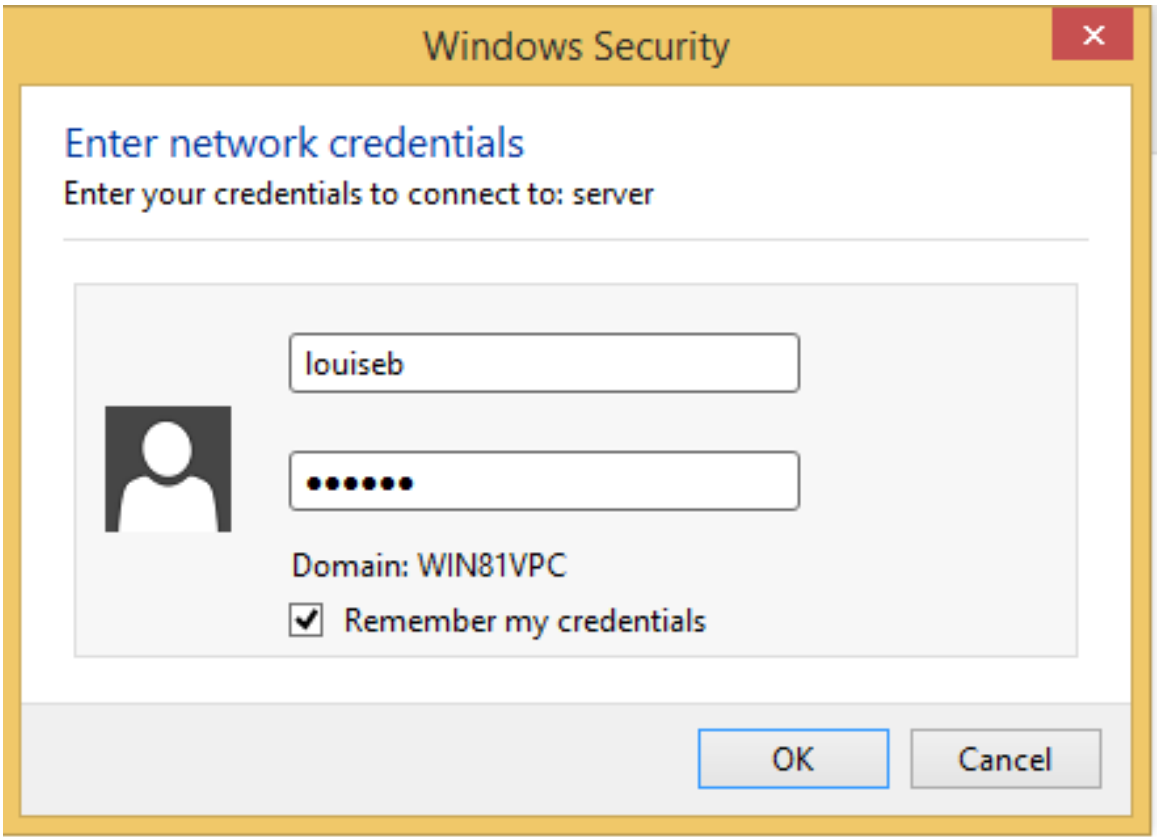

Figure 38: Entering network credentials

Upon a successful connection, the contents of the newly mapped drive will be displayed. The process now needs to be repeated for each folder that the user needs access to.

Note that you can use whatever drive letters you wish, as long as they are not already in use (for instance you cannot use C as that is always in use on a computer). However, using sensible letters makes things easier. For example, map *music* to M, *photo* to P and *video* to V. Here are the suggested mappings:

Drive	Folder
H	\\server\home
M	\\server\music
P	\\server\photo
S	\\server\shared
V	\\server\video

5.4 Using the Synology Assistant

The Synology Assistant is used when initially setting up a DiskStation but is able to do several other things as well, one of which is mapping drives. This is a good solution if each user has their own computer and no other person uses it.

Download and install the Assistant on each computer. If you receive a message from the computer's firewall, grant the Assistant access. An icon will be placed on the computer's desktop – double-click to run it. The following window is displayed:

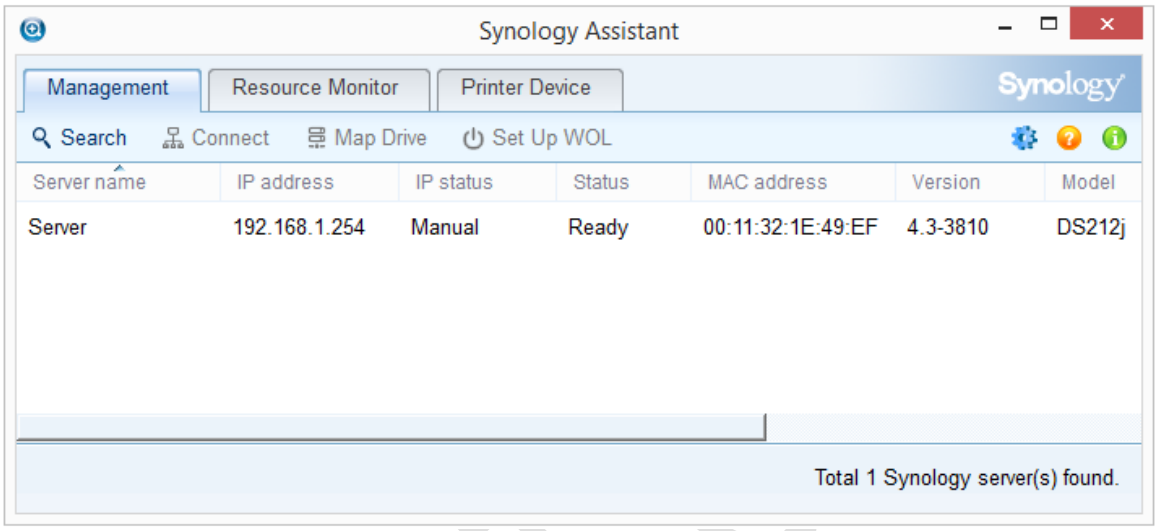

Figure 39: Synology Assistant

The server should be listed, although the Assistant may scan for it for a little while. If it does not appear click the **Search** button; if it still does not appear then there is a problem of some sort e.g. computer not connected to network; server not powered on; firewall needs configuring on computer. Click on the server entry – it will then become possible to click the **Map Drive** button. Do so and you will be prompted to enter logon details. Then click **Next**.

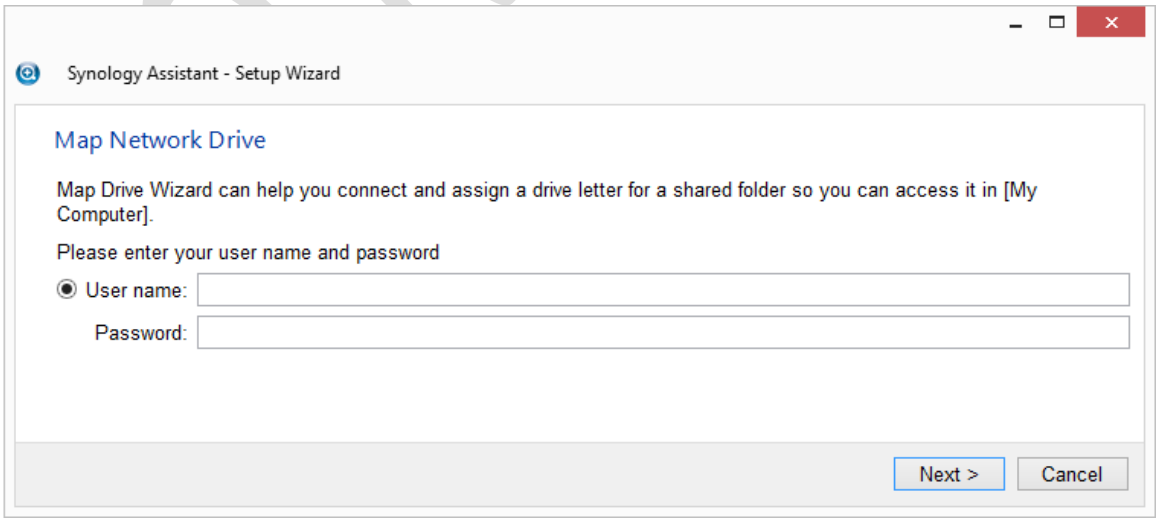

Figure 40: Enter user name and password

The subsequent screen lists the folders to which the user has access:

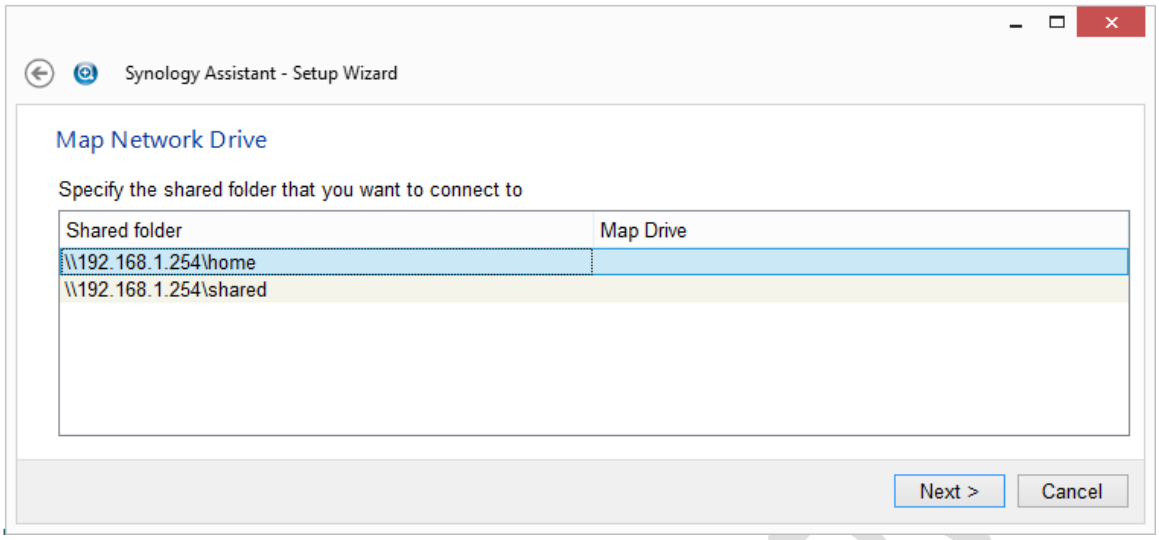

Figure 41: Choose a folder to connect to

Choose a folder and click **Next**. On the following screen choose a drive letter for the folder; the default is Z but you can use any free letter. However, it is suggested that H: is used for the Home drive and S: for the Shared drive. If the computer is only ever used by one person tick the **Reconnect at logon** box then click **Next**.

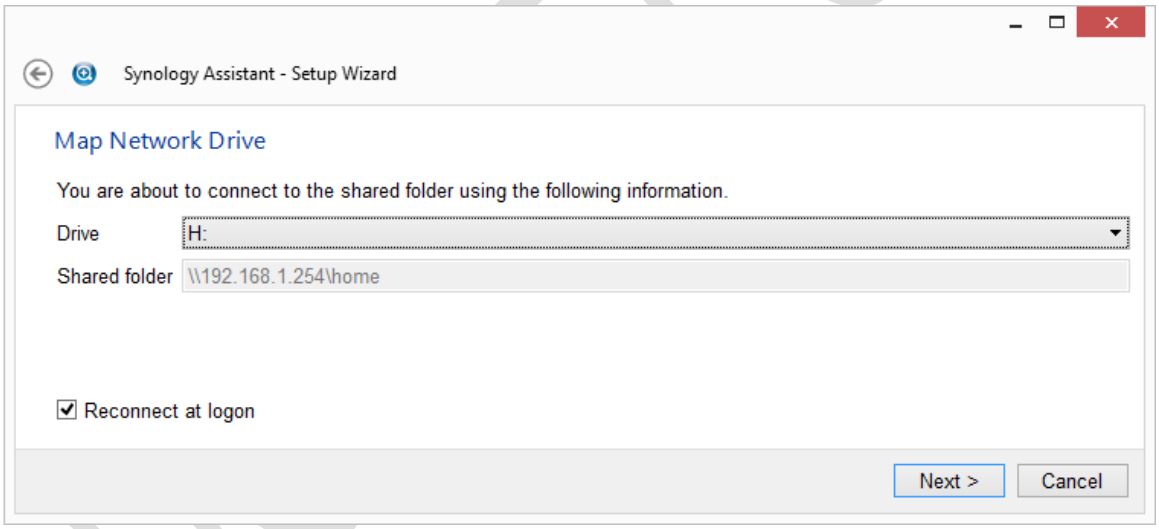

Figure 42: Map the drive

You may receive an additional logon prompt from Windows. Enter the login details, click tick the **Remember my credentials** box if only one person uses the computer and click **OK**.

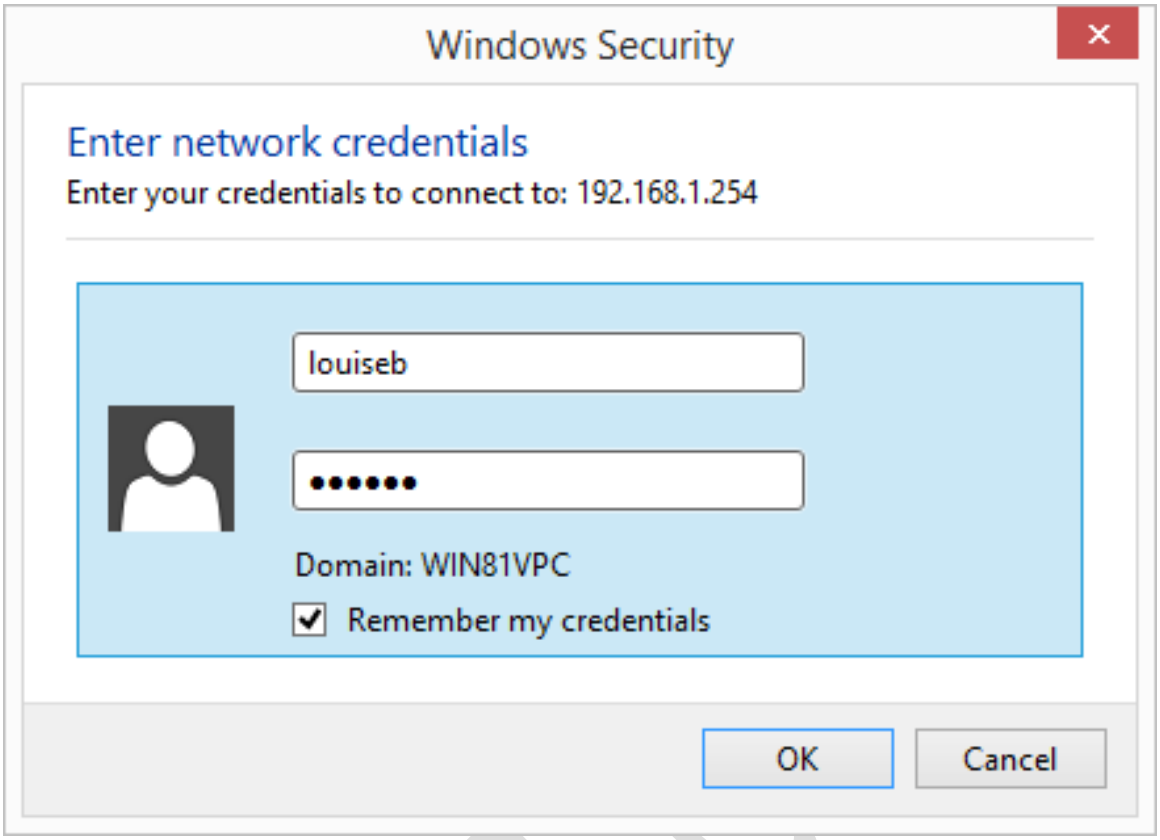

Figure 43: Enter user name and password

The drive will be mapped – click **Finish** on the confirmation screen. Repeat the process as many times as is necessary to provide access to all the required folders. When complete, close the Synology Assistant (in fact, it will continue to run on the Taskbar) and open Windows Explorer to verify that the folders have been mapped to drives, for example:

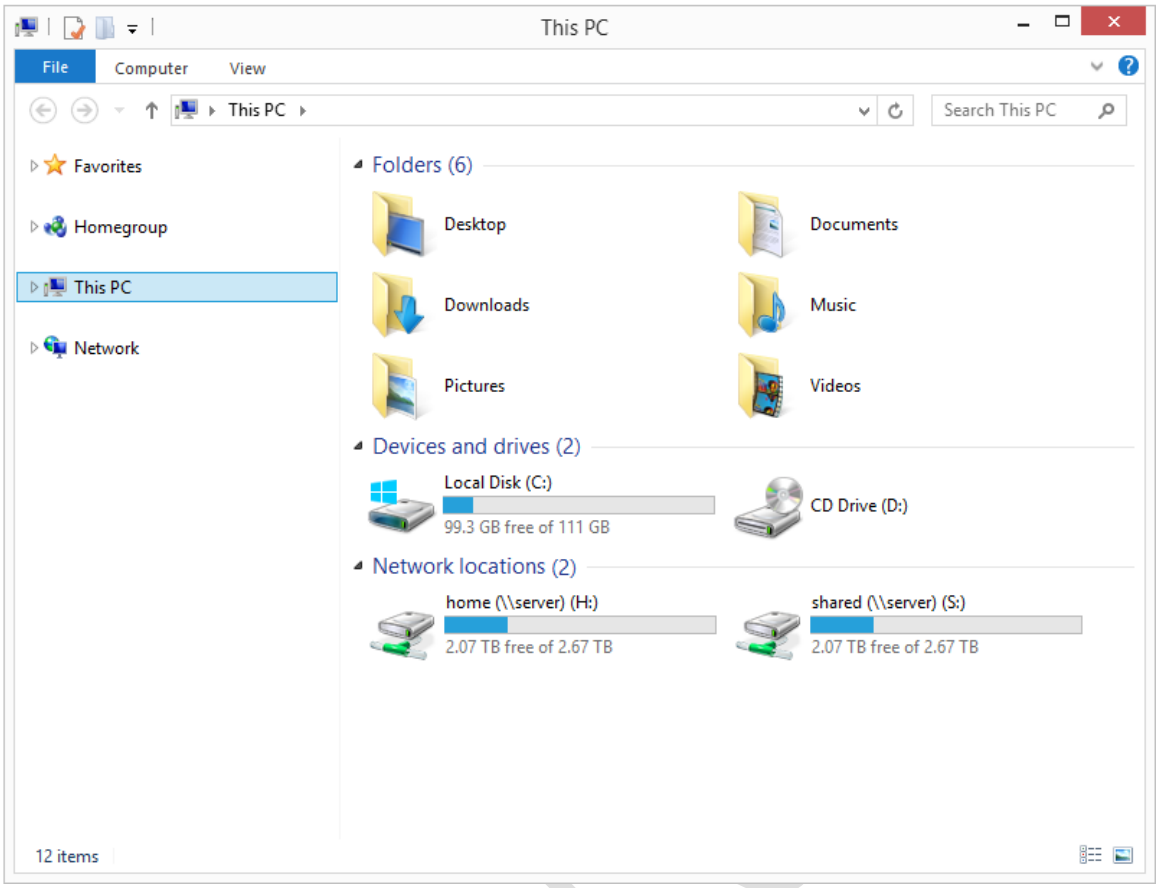

Figure 44: Mapped drives within Windows Explorer

Note that the drive mappings are permanent (assuming the **Reconnect at logon** and **Remember my credentials** boxes were ticked) and hence will survive reboots. It is not necessary to run the Synology Assistant again unless it is ever desired to make changes to the mappings.

5.5 Using a Script/Batch File

Using a batch file works well if people need to share computers, which is often the case in a business environment. Use Notepad or WordPad to create a plain text file called *Connect to NAS.cmd*:

```
@echo off
ping server -n 1 > nul
if errorlevel 1 goto offline
:online
: remove drive mappings if already present
net use * /delete /y > nul
: map the drives
net use s: \\server\shared /persistent:no
net use h: \\server\home /persistent:no
goto end
:
:offline
cls
echo You are not connected to the network.
echo If you are outside the office then this is okay.
echo If you are inside the office then it means there is a problem.
echo Data stored on the network is not currently available.
pause
:end
```

The file should be placed on the Desktop of the computer. After the computer starts up, the user should run it by double-clicking on its icon. A window is displayed prompting for the user name, followed by a prompt for the password:

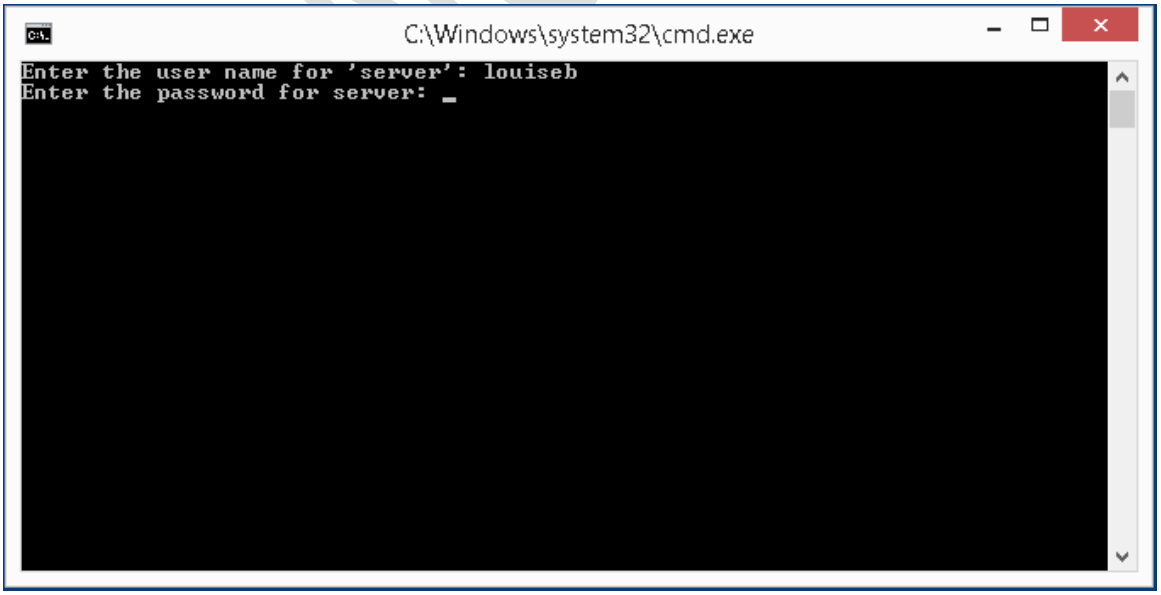

Figure 45: Enter user name and password

After the user has successfully entered their details, the Home (H:) and Shared (S:) drives will be available until the computer is shutdown or they logoff using the Start menu. This can be verified by launching File Explorer (which appears by default on the Taskbar with Windows 7 and Windows 8).

If the server is not available, then rather than mapping the drives a warning message is displayed instead:

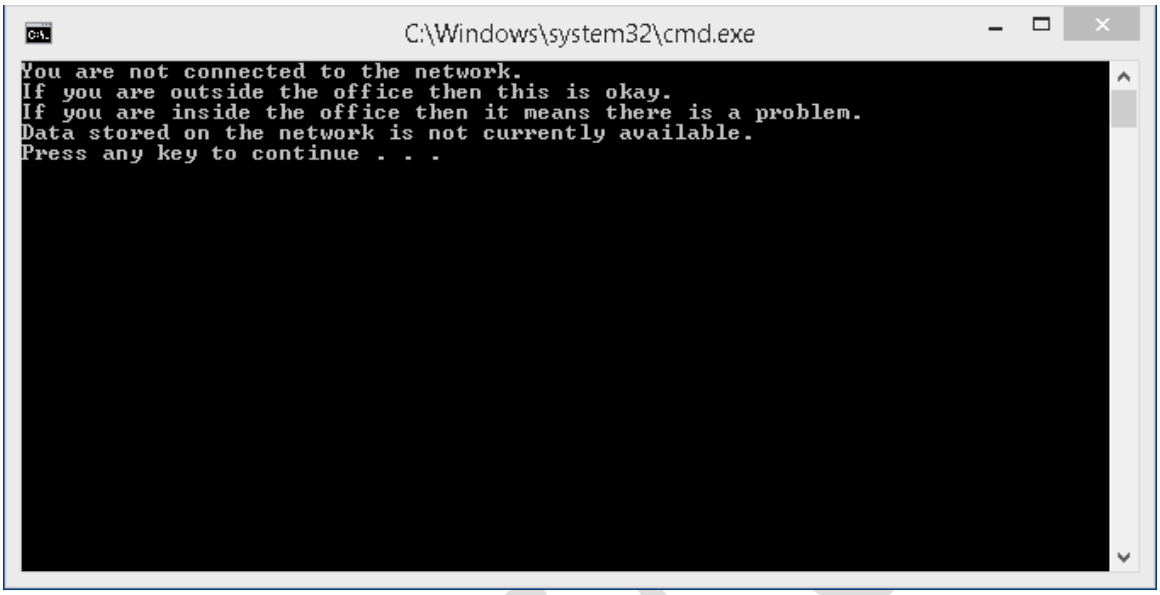

Figure 46: Warning message

It is to be expected that this message will appear if using, say, a laptop computer outside of the office, but if it appears inside the office then it indicates a problem. This could be a connectivity issue on the computer e.g. Ethernet cable unplugged. If everyone in the office is receiving it then it would suggest that the server is powered off or otherwise out of action.

When a particular user has finished with a computer, they should logoff or restart the computer.

Ideally, computers should be setup with only one Windows user defined on them (i.e. a user created via the Control Panel on the computer). If this is not the case, then the *Connect to NAS.cmd* file needs to be placed on the Desktop for each individual user. More efficiently, it can be placed in the following location where it will appear on the Desktop for all users:

Windows XP	C:\Documents and Settings\All Users\Desktop
Windows Vista	C:\Users\Public\Public Desktop
Windows 7	C:\Users\Public\Public Desktop
Windows 8	C:\Users\Public\Public Desktop

Note that the Public Desktop folder is a hidden folder on Windows 8, 7 and Vista and will therefore first need to be made visible before it can be used. To do this, go to **Control Panel** on the computer and choose **Folder Options**. Click on the **View** tab, enable **Show hidden files, folders and drives** and click **OK**.

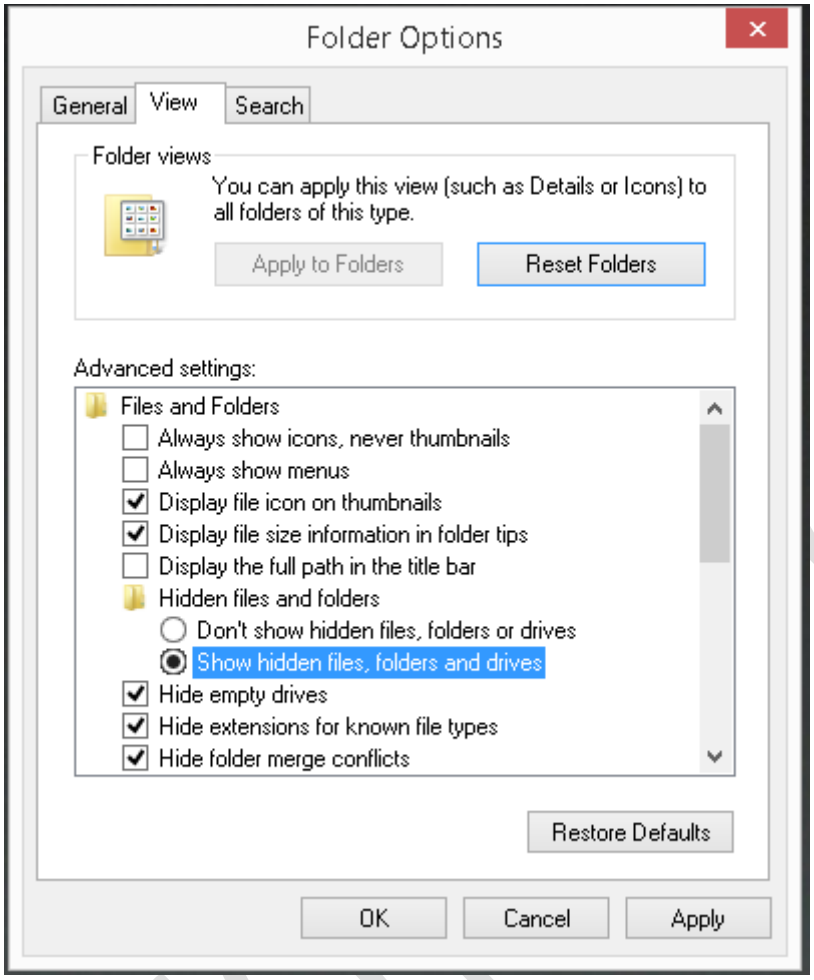

Figure 47: Show hidden files

Copy the *Connect to NAS.cmd* file to the Public Desktop folder, then make the Public Desktop folder hidden again.

Note that *Connect to NAS.cmd* is not very forgiving of errors. If the user enters the wrong logon details there will be a brief error message and the drives will fail to map. The user will need to run the file and try again.

5.6 Connecting an Apple Mac

There are various iterations of the OS X operating system and some subtle differences between them. However, the following technique should work with all versions. Before starting, make sure that the Mac File Service is enabled on the DiskStation. To do this go to **Control Panel** and click the **Win/Mac/NFS** icon. Click on the **Mac File Service** tab then tick the **Enable Mac file service** box. It is not necessary to specify any of the other settings.

On the menu bar of the Mac, click **Go** followed by **Connect to Server**. Alternatively press **Command K**:

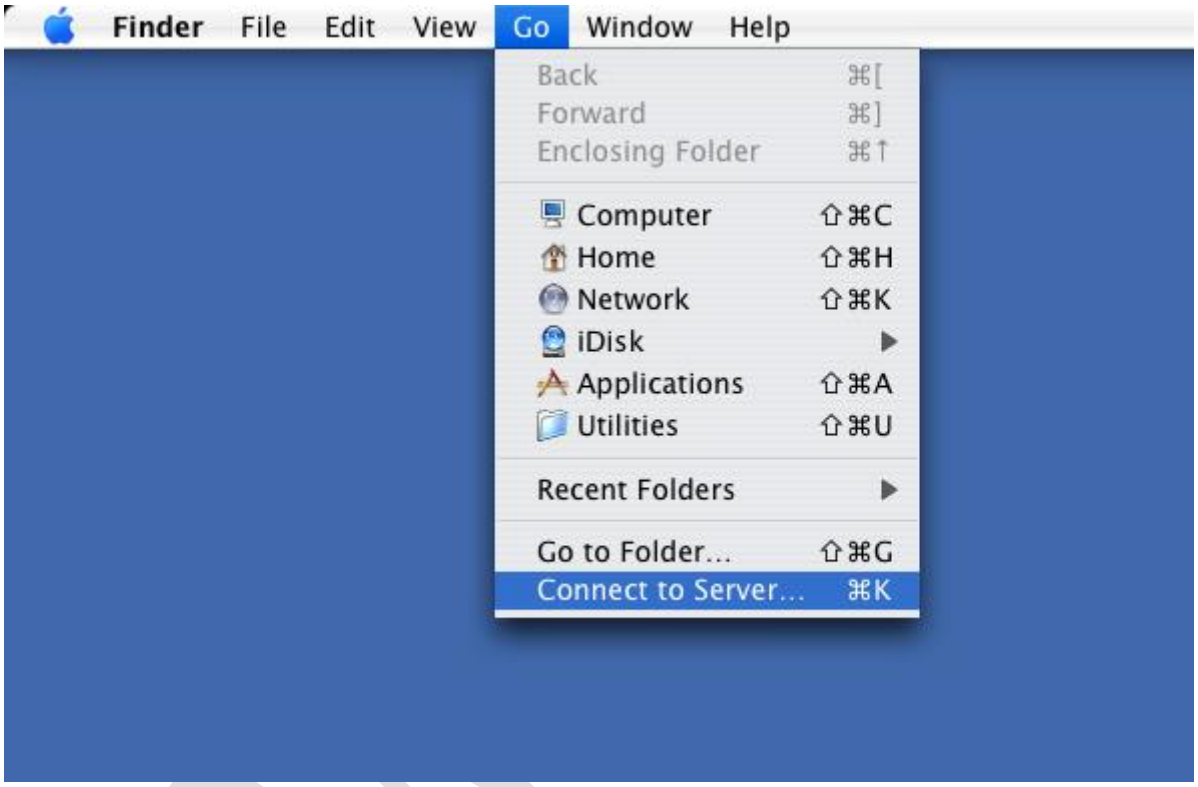

Figure 48: Connect to Server

A dialog box is displayed. Enter the name or IP address of the DiskStation preceded with *afp://*

e.g. *afp://192.168.1.254* or *afp://server*

To add the server to your list of Favorites for future reference click the + button. Then click **Connect**:

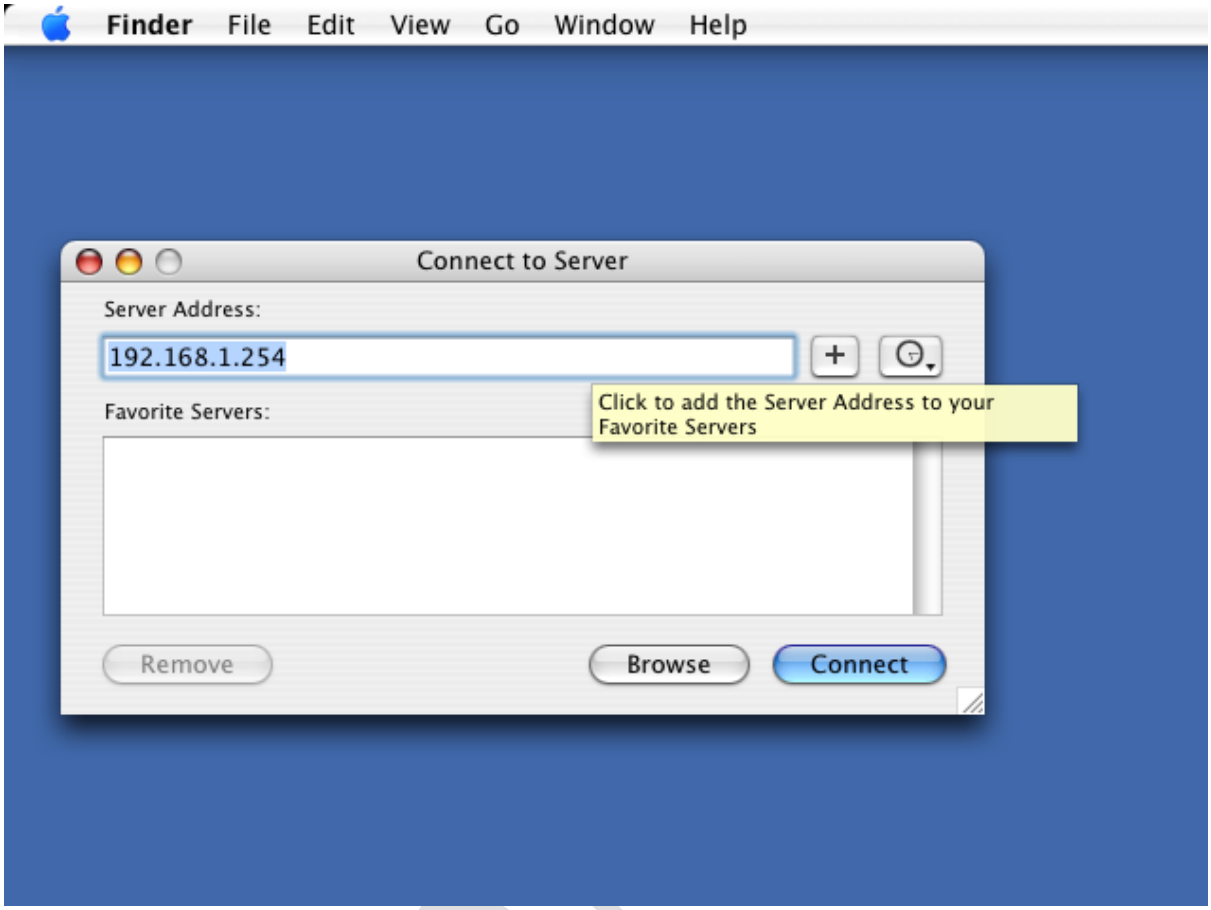

Figure 49: Enter IP address of DiskStation

Specify the user name and password as defined on the DiskStation and click **Connect**:

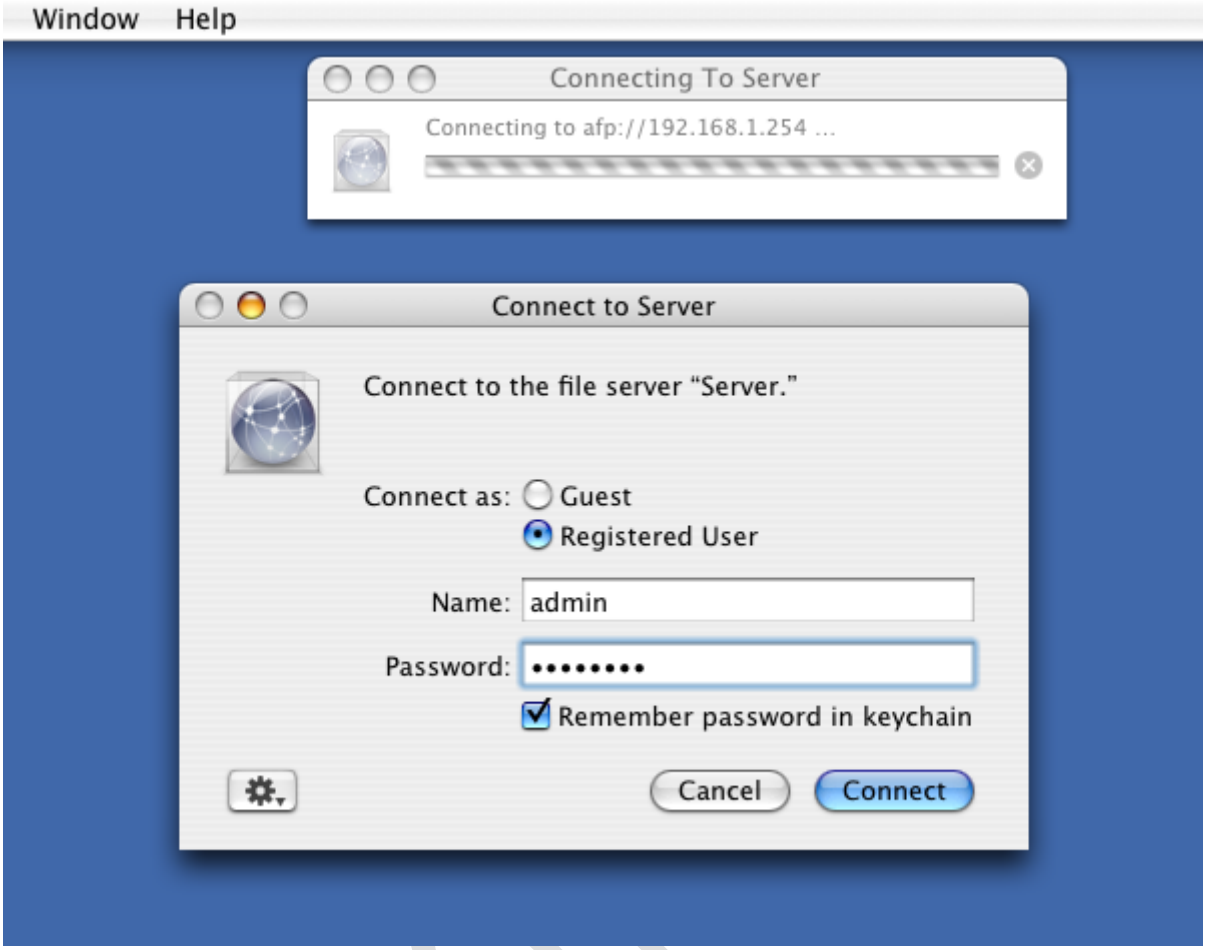

Figure 50: Enter user name and password

A list of shared folders is displayed, referred to as *volumes* in Apple parlance. Choose the volume to mount and click **OK.** Note: to mount multiple volumes in one go, hold down the Command key and click on the required folders:

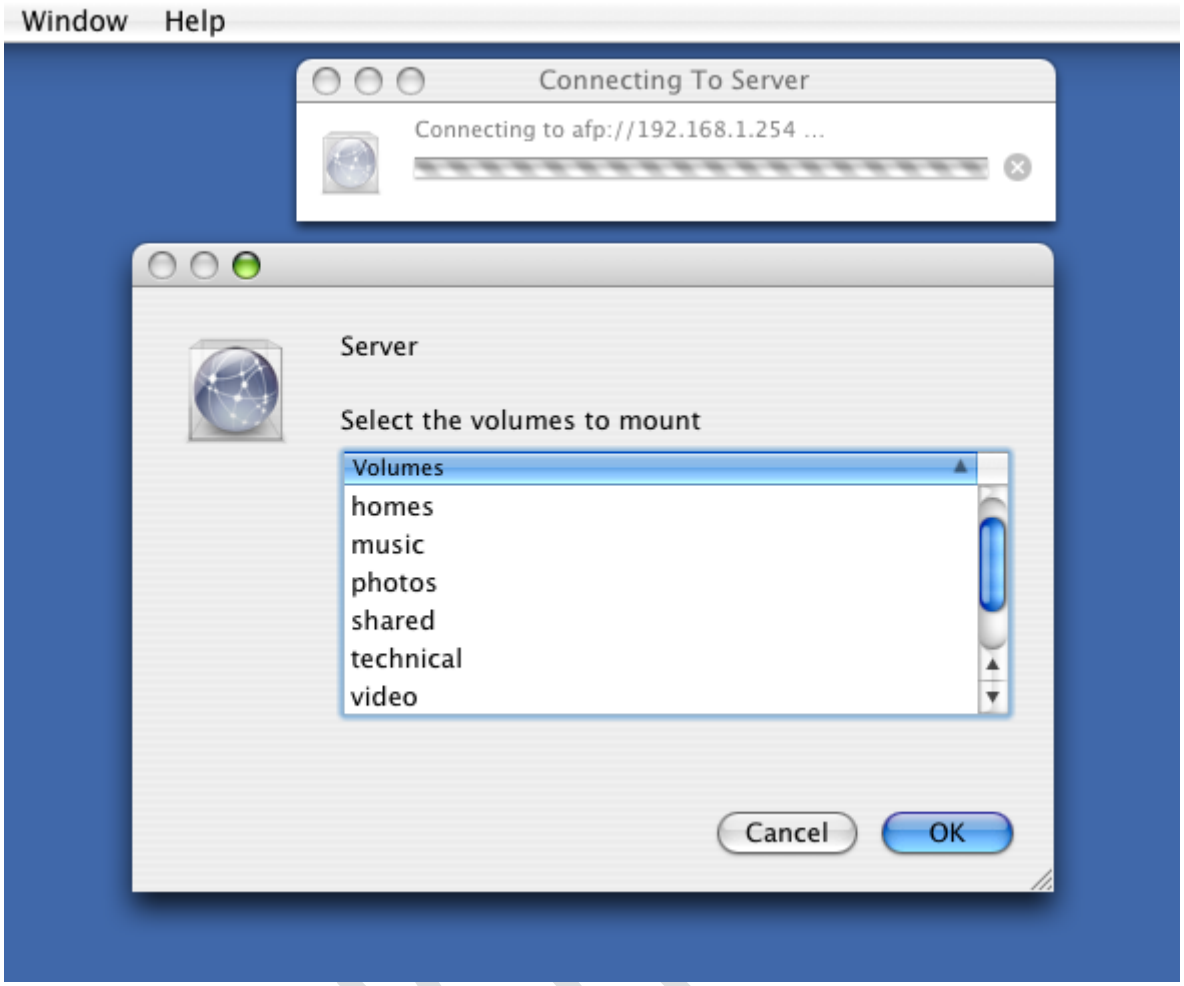

Figure 51: Select the folder(s) to mount

An icon for the folder will appear on the Desktop. Click it to display the contents. It behaves like any standard OS X folder:

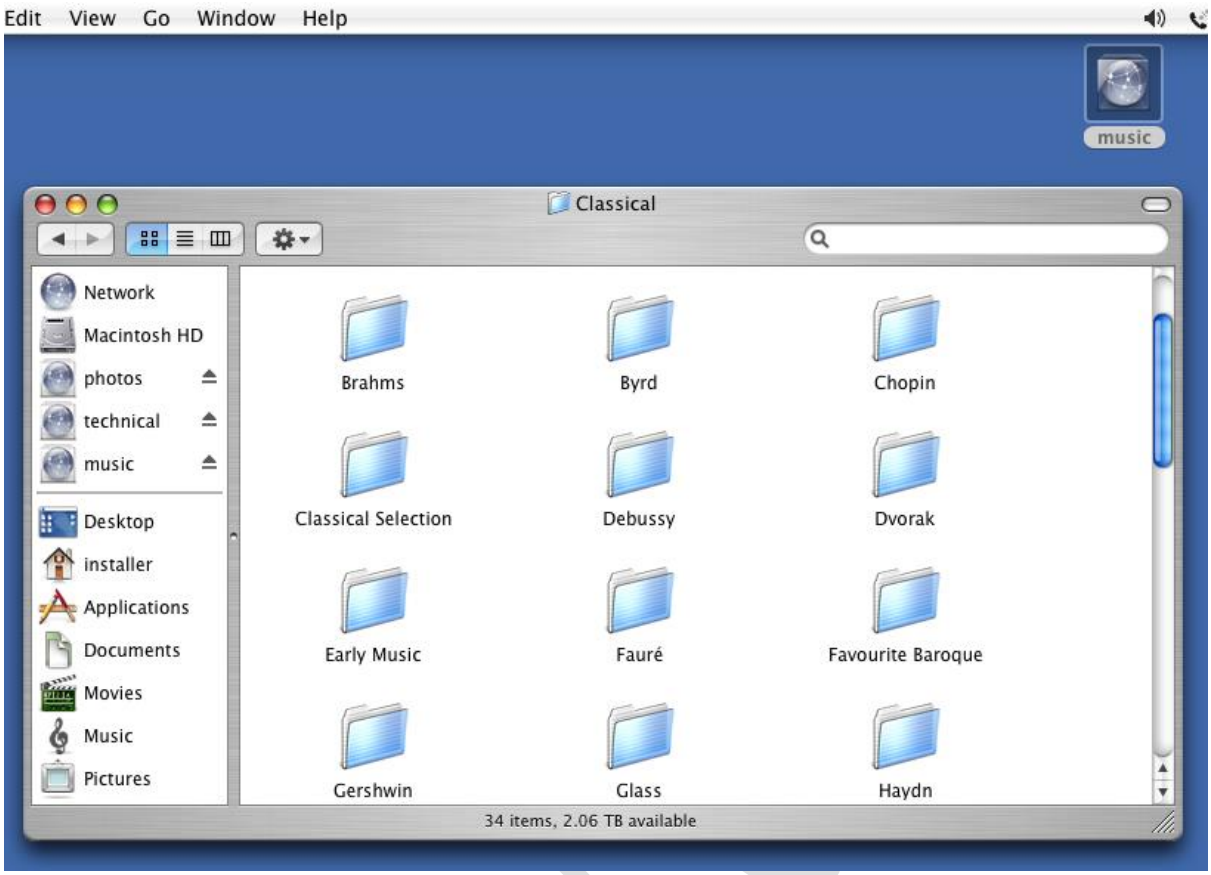

Figure 52: Contents of mounted folder

A slight variation on the above is to click on the Mac's hard drive icon on the Desktop, navigate to the Server (DiskStation), click the Connect button and then login and mount a volume (shared folder):

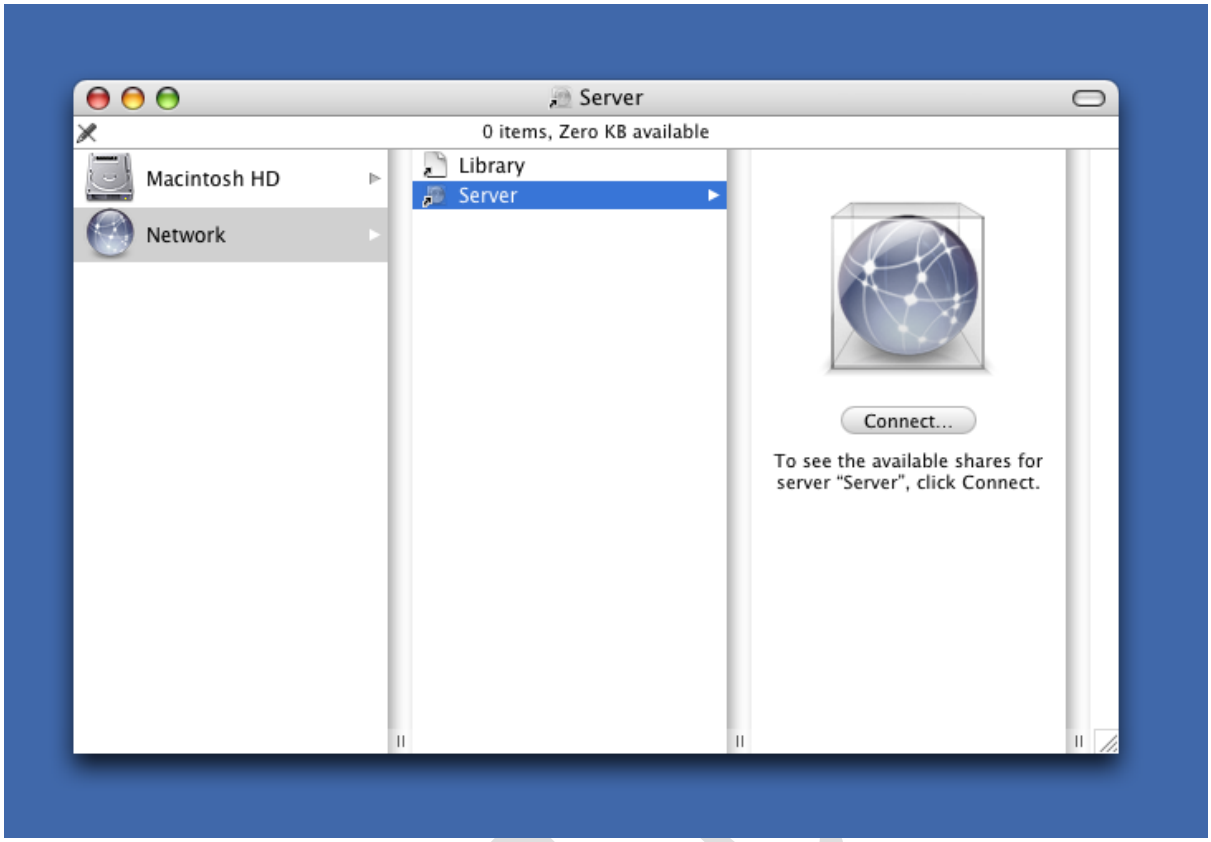

Figure 53: Alternative method of connecting to server

6. Backups

There are several options for backing-up the server: to an external USB drive; to another DiskStation or RackStation; to a Cloud-based service. The first scenario is most likely in a small business and is the one covered here.

6.1 Preparation of External Drives

The backup solution requires at least one but preferably a pair of external USB drives. These should be: USB 3.0 specification (USB 2.0 drives will work but are slower); of sufficient capacity to hold all the data (for example if there is 1TB data then use at least 1TB drives); portable if possible (as they do not require mains power and are more convenient to store). To prepare a drive for backup usage plug it into a spare USB socket - note that on some DiskStations/RackStations not all of the USB sockets are of USB 3.0 specification. Choose **Control Panel** followed by **External Devices**. The drive should appear; highlight it and click **Format**.

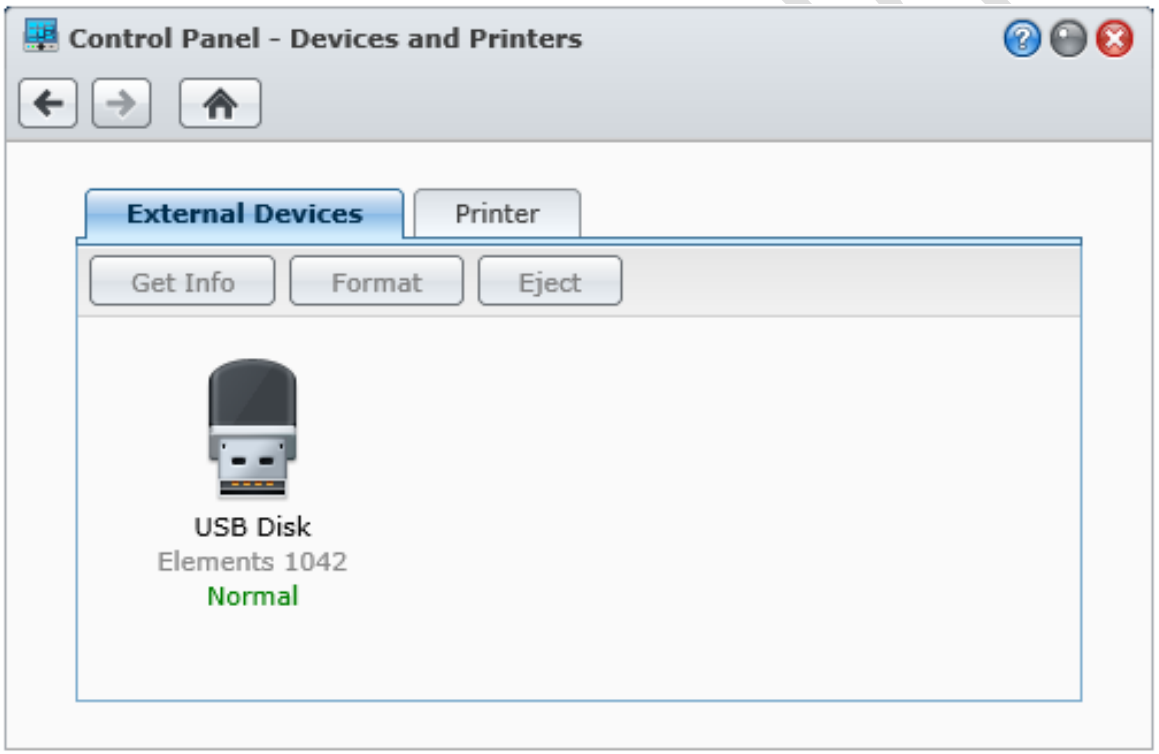

Figure 54: External drive identified

Choose the DSM default file system type of **EXT4** and click **OK** - the formatting may take some time, depending on the capacity of the drive. Note: EXT4 is a Linux file system and not natively understood by Windows machines; should there ever be a need to read a backup drive from a Windows PC it can be done using a free downloadable utility called *Ext2FS* from Paragon Software.

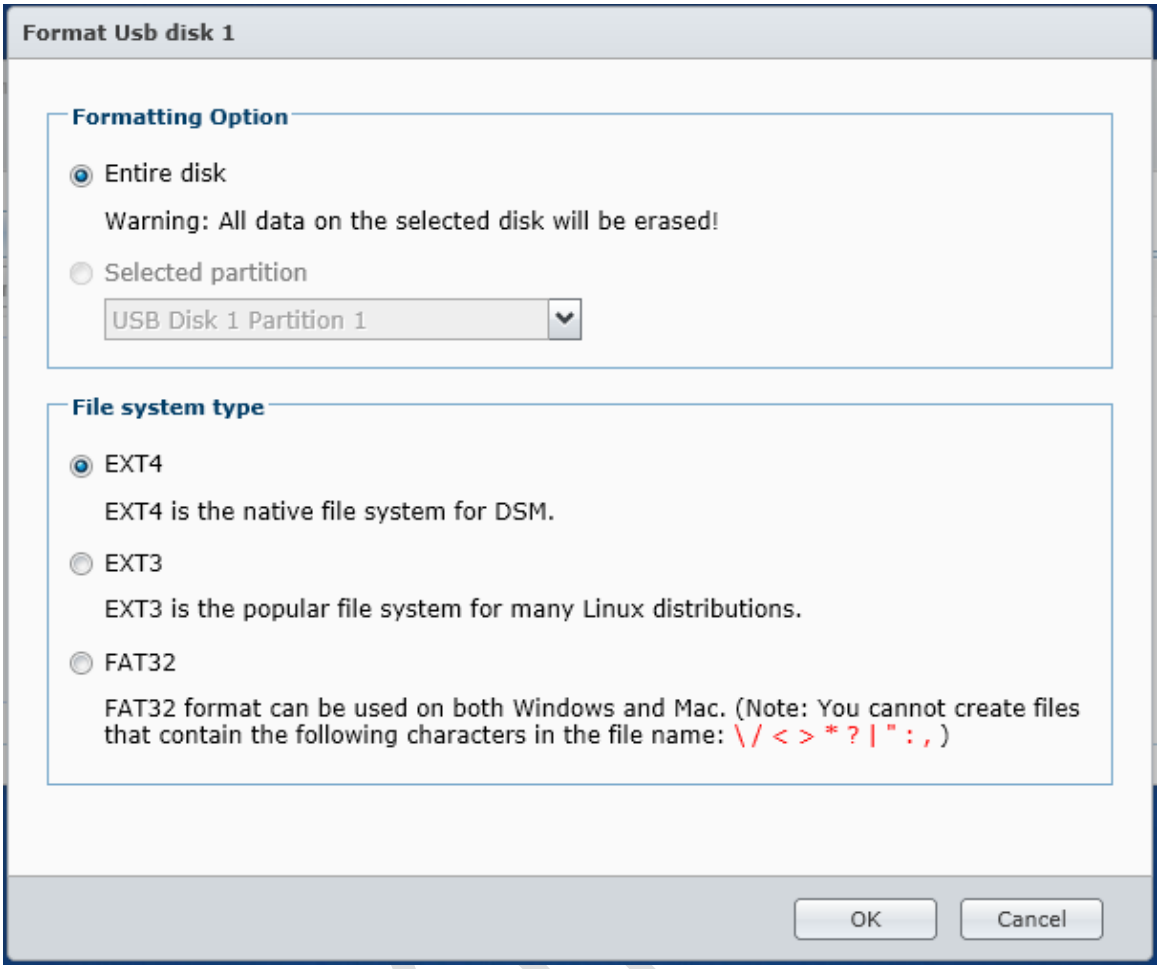

Figure 55: Format external drive

When finished, eject the drive and repeat the process for the second drive if there is one.

From the **Main Menu**, choose **Backup and Restore**. Click **Create** and choose **Data backup task**, which will invoke the Backup Wizard. Give the task a name e.g. *WeeklyBackup*. For the destination type, choose **Local Backup**.

On the next screen, make sure the Destination is the external USB drive, check all the tickboxes and click **Next**:

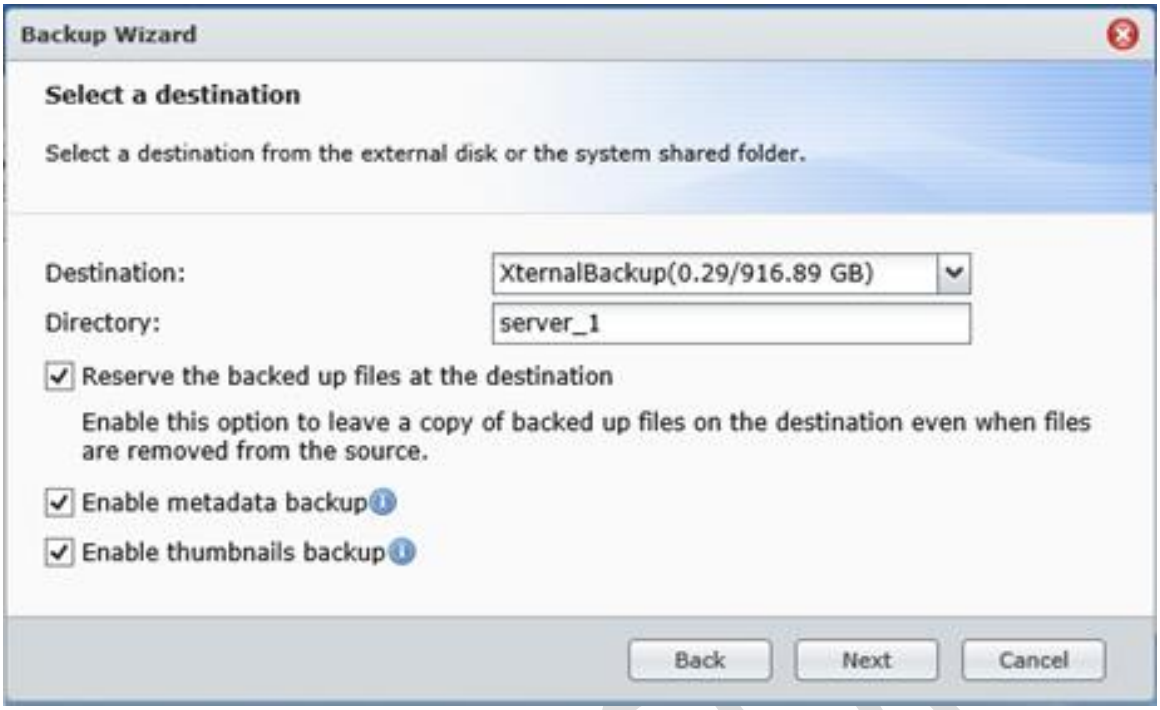

Figure 56: Format the backup drive

Specify the schedule. The backup should be scheduled to run outside of normal working hours. In this example the backup is configured to run at 8:00pm each Friday. Click **Next**:

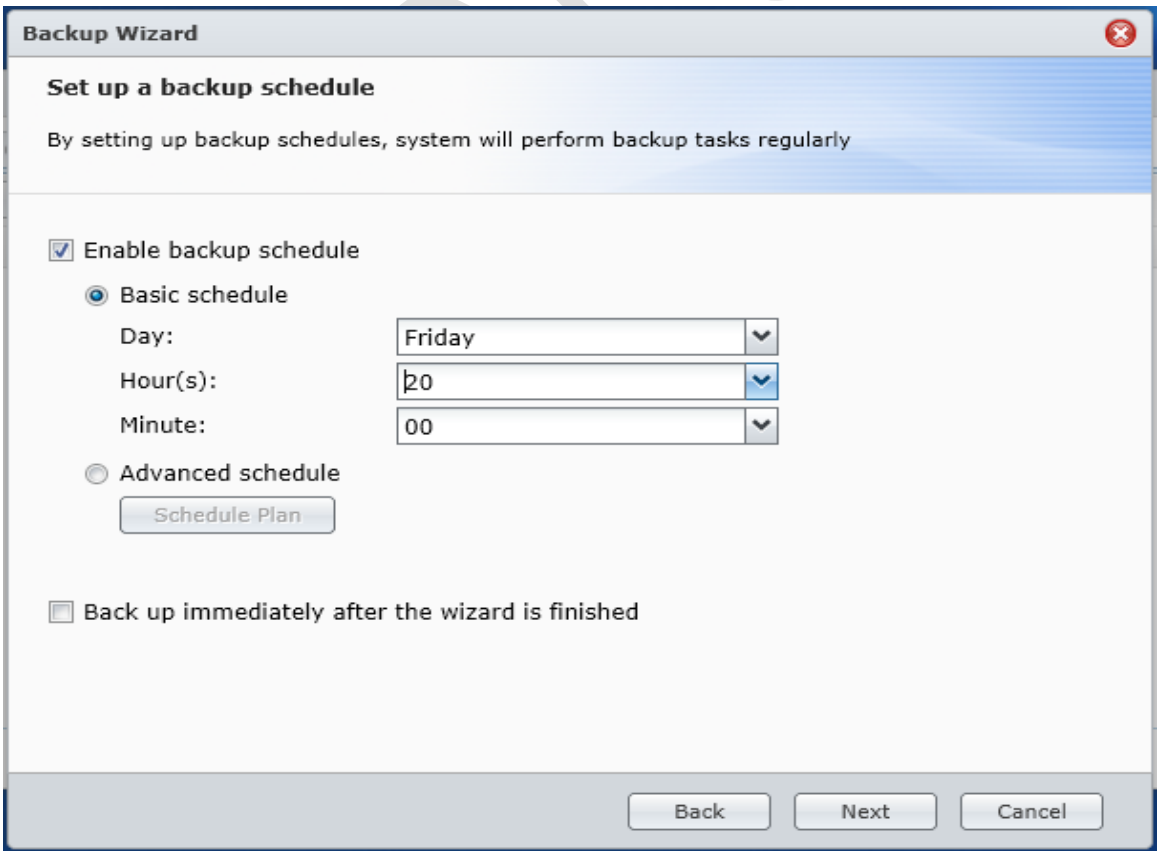

Figure 57: Schedule the backup

A confirmation of the settings is displayed. Click **Apply**:

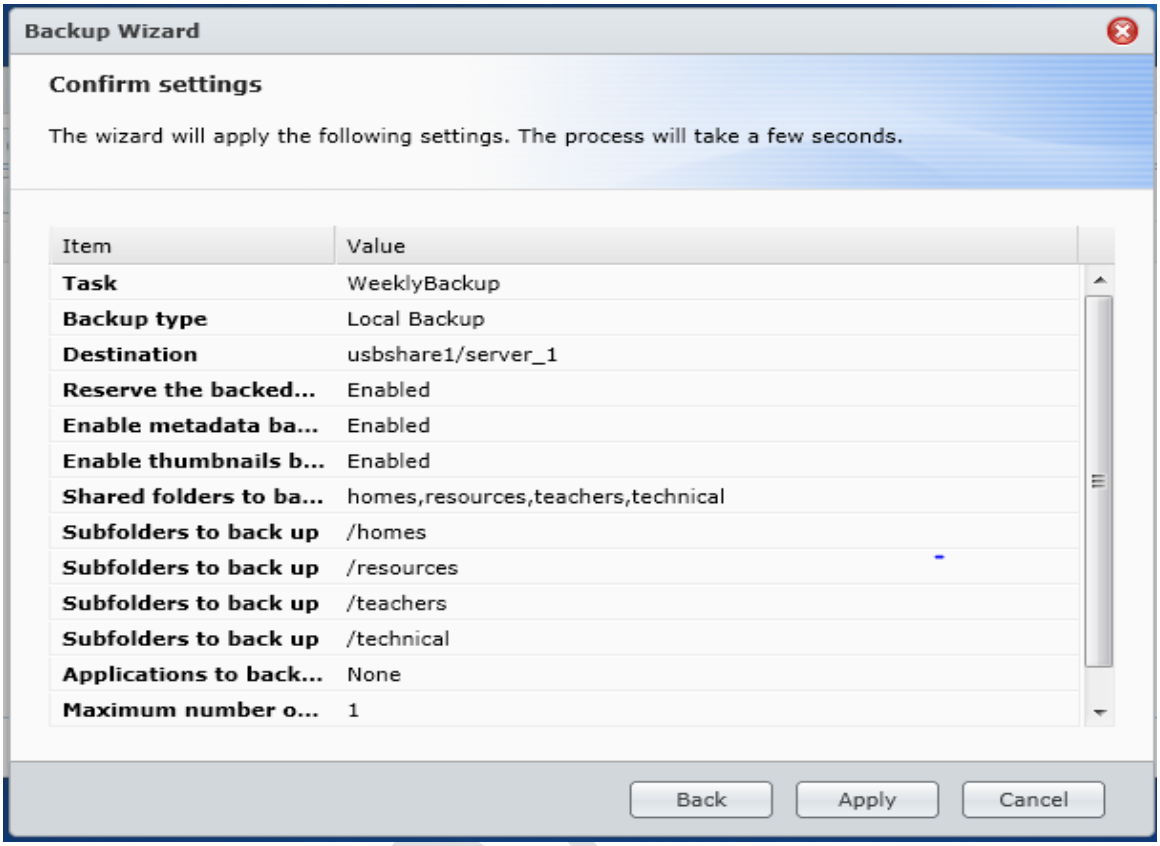

Figure 58: Summary of settings

6.2 Weekly Procedure When Using Two Backup Drives

Each week, following a successful backup, the USB drive should be ejected and replaced with the other one if a pair of drives are being used. It should then be kept in a safe place away from the server until it is re-used the following week. Better still, keep it offsite altogether.

Tip! Although the DiskStation includes a proper Restore function, using the File Station application it is possible to simply drag'n'drop files from the backup device onto the main storage and which may be more convenient in some instances.

6.3 Using Data Replicator to Backup Laptops

If the users have laptops and store data on them rather than on the network, then there is a requirement to be able to backup that data. This can be done using the *Synology Data Replicator 3* program, which can be downloaded from the Synology website. The backups will be stored on the DiskStation.

Install the software on the user's laptop; running it will display the following screen:

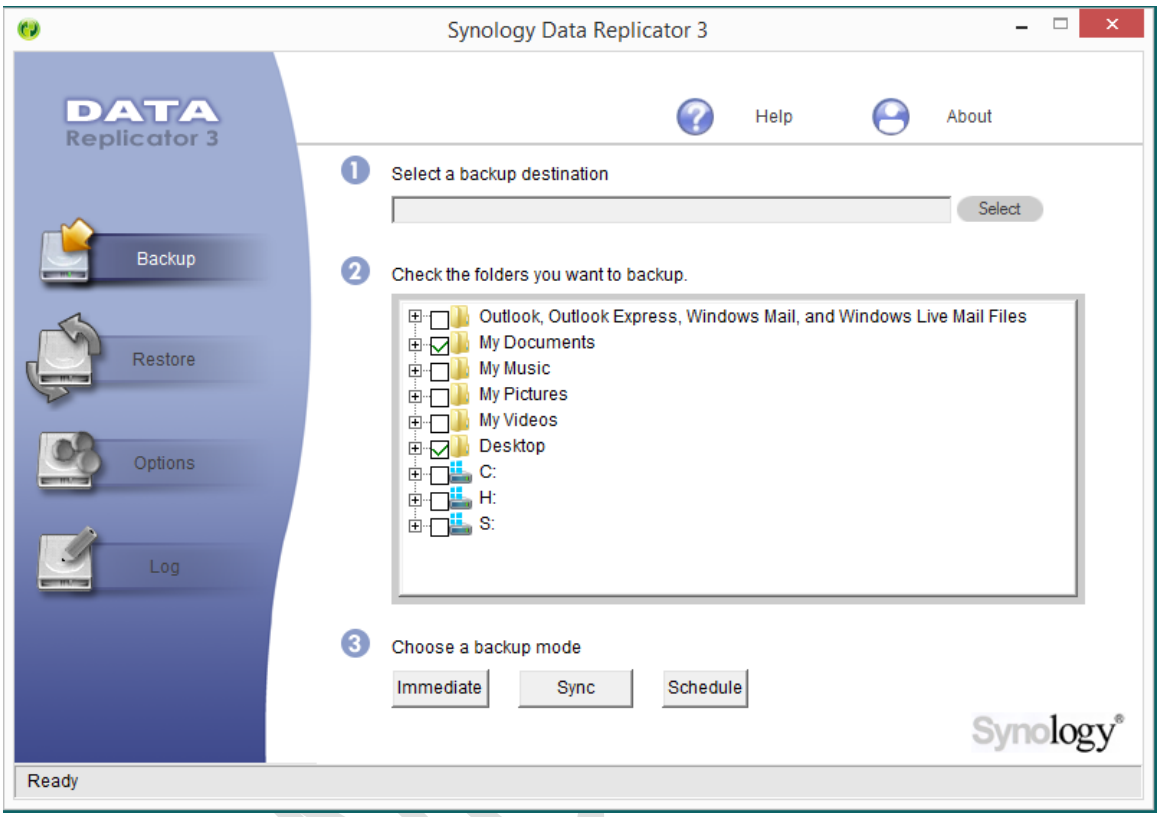

Figure 59: Synology Data Replicator

Firstly, specify a backup destination by clicking the **Select** button. A panel is displayed, giving a choice of 'Synology Server' or 'Other location'. Choose **Synology Server** and click **OK** (if you are running this for the first time you may receive a warning from the computer's firewall - you need to allow access for the Data Replicator application). After a few seconds a screen is displayed listing the server; click on it followed by the **Next** button. On the subsequent panel, specify the user's logon credentials; do not click the 'Auto-connect on Data Replicator 3 startup' box; click **Next**:

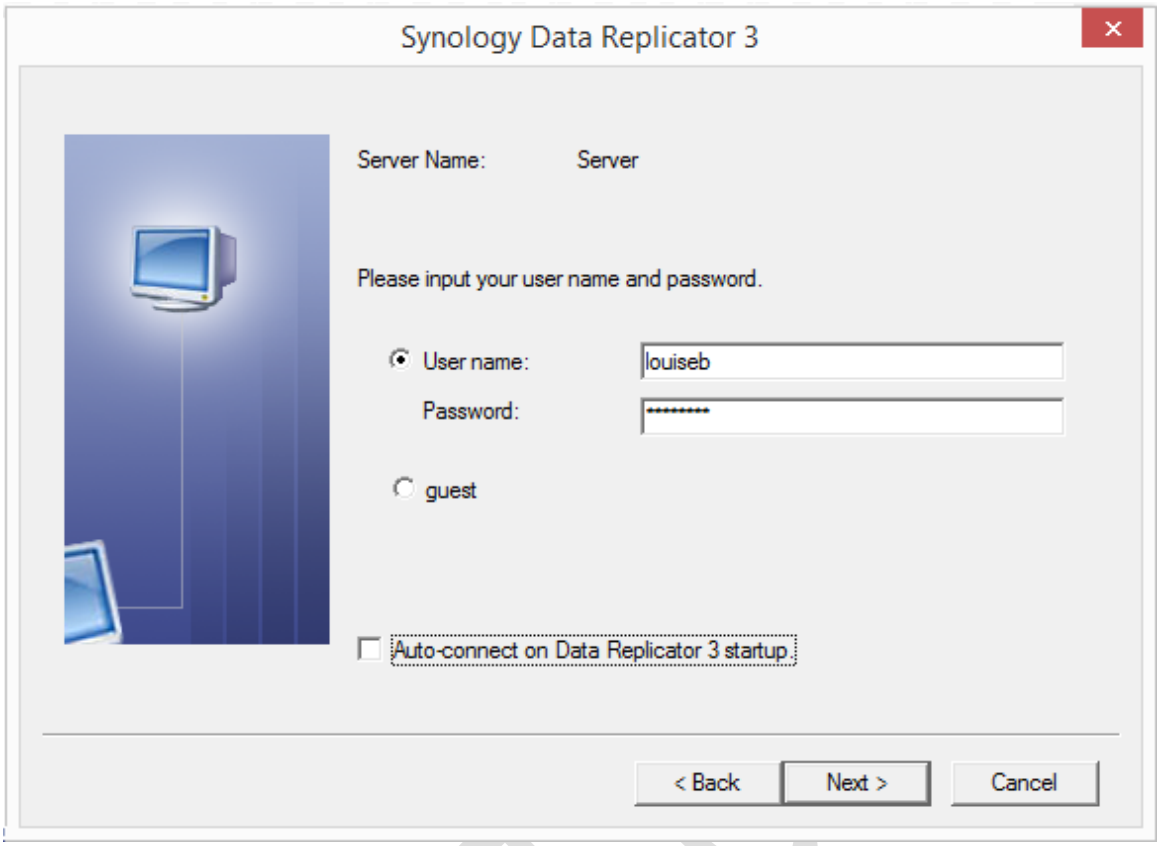

Figure 60: Enter user name and password

On the next screen specify the backup folder (the destination) on the server. Depending on how the system has been configured, there should at least be a choice of *home* and *shared*; always specify **home** as this is private to the user, whereas other folders can be accessed by other users. Click **Finish:**

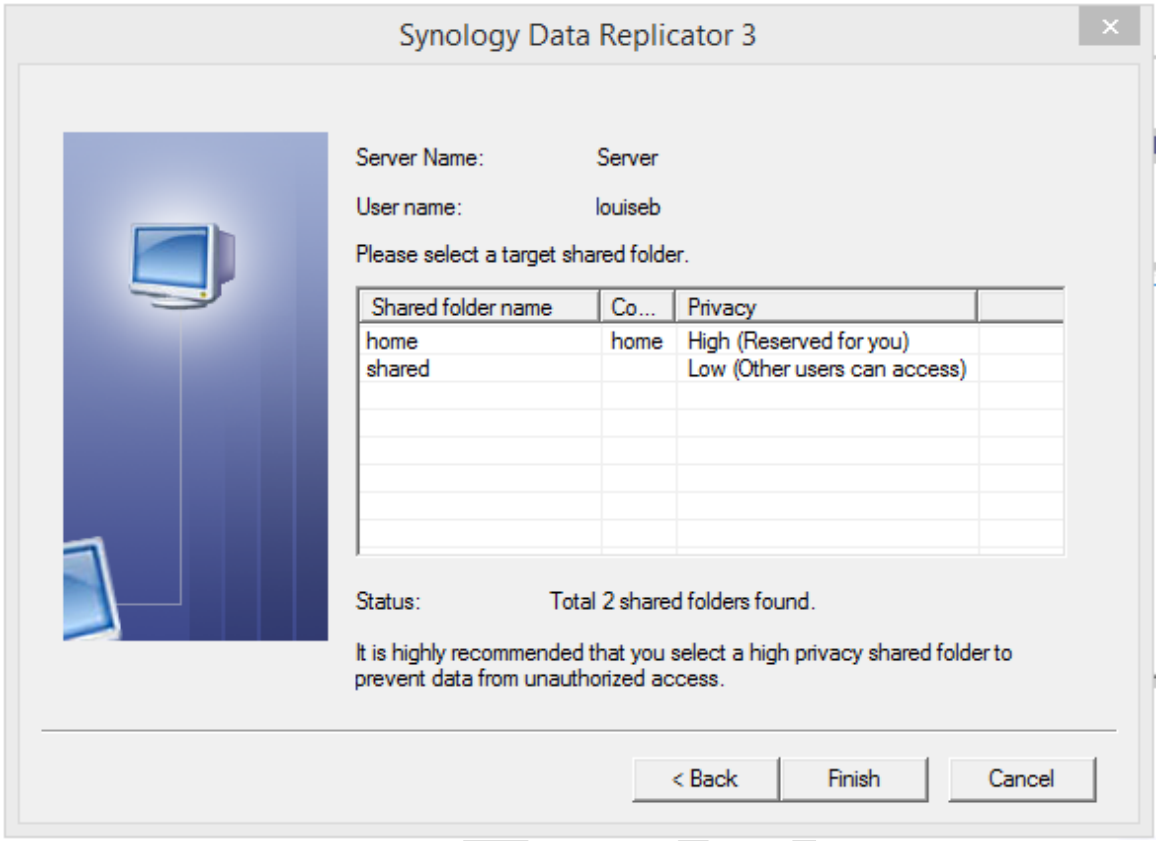

Figure 61: Choose destination for backup

Next specify the folders to be backed up. Usually this will be the My Documents and similar folders; if files are stored on the Desktop (which is bad practice but people do it) tick it. Do not select any complete disk drives and especially not network drives such as H: and S:

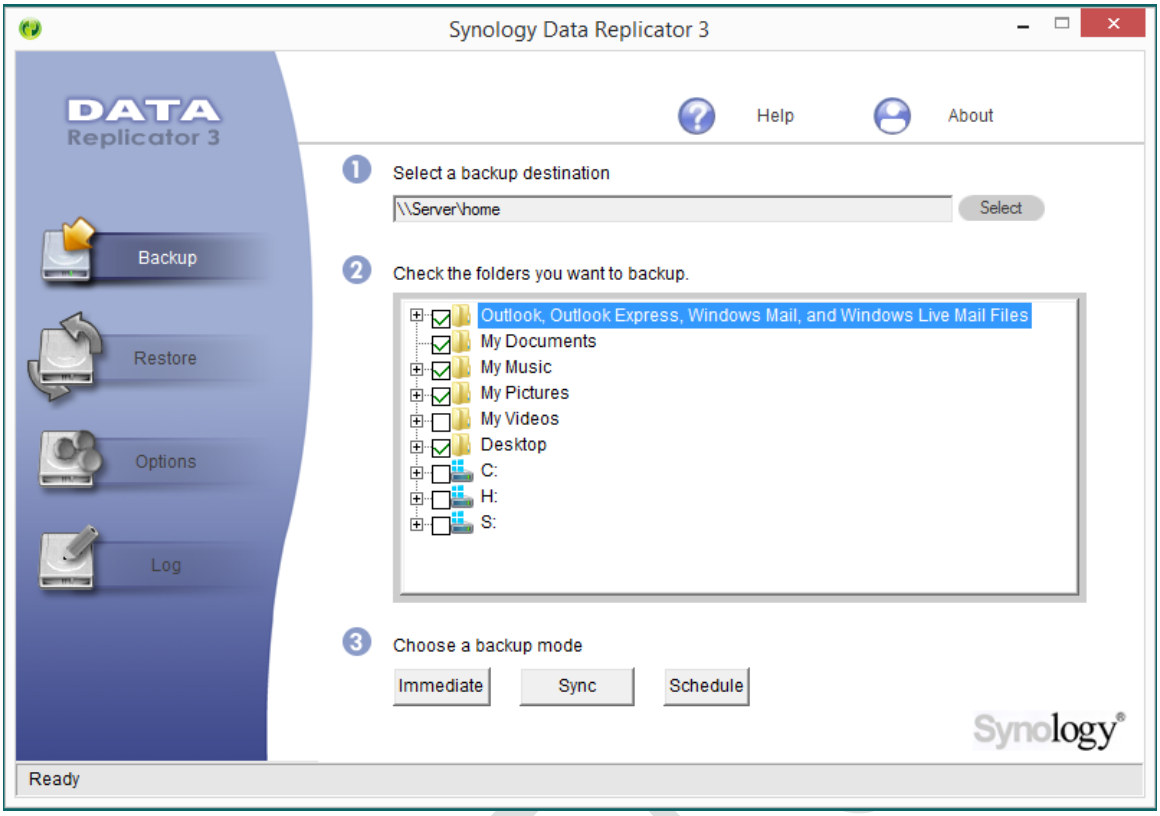

Figure 62: Choose the folders to backup

Then, choose the backup mode:

Immediate – runs the backup now

Sync – causes any changes to automatically be replicated to the DiskStation. This is potentially the most useful option if the laptops stay in the premises all the time. If this mode is chosen, also click **Options** and tick the **Auto-start Data Replicator 3 on Windows Startup** box.

Schedule – allows a backup to be scheduled on a daily, weekly or monthly basis. If this is selected then the password for user needs to be specified.

Note that if the user has a lot of data stored on the laptop the backup may take some time, particularly over a wireless connection (potentially hours). For users with high volumes of data it is suggested that a wired Ethernet connection is used during backups, even if this isn't their usual method of connecting to the network.

The backup folder is stored in the user's home folder - corresponding to the H: drive - and has a name of the form *DR-computername-username* e.g. *DR-laptop4-louiseb*.

Using Data Replicator 3, users can backup and restore their own data as they wish. The data can also be accessed by the administrator on the Server using File Manager. Backups are held in the same file and folder formats as regular files and can be copied and moved about in exactly the same way.

6.4 Use of Time Machine for Mac Users

The server can be specified as a backup destination for use by Time Machine. This is done as follows:

Create a shared folder on the server specifically for this purpose (creating shared folders is described in section 3 - Creating Shared Folders). Give the folder a meaningful name e.g. *macbackup* and give **Read/Write** access to all the Mac users.

Next, go to **Control Panel,** choose **File Services** and click the **Win/Mac/NFS** tab. Scroll down to the Mac section. Make sure the **Enable Mac file service** box is ticked. Underneath it is a drop-down box called **Time Machine** – click on it and choose the backup folder that was just created e.g. *macbackup* in our example. Click the **Apply** button.

To perform a backup go to a Mac and launch Time Machine. Click **Select Disk** and the backup folder ("*macbackup* on *server*" in our example) will be available. Select it and click the **Use Backup Disk** button. It will be necessary to enter the user name and password as defined on the server.

Suggestion: to avoid the server filling up with backups, apply a quota to each Mac user. Go to **Control Panel** and click the **User** icon. Highlight a user name and click the **Edit** button, then click the **Quota** tab. Click the **Enable quota** box and in the Quota box specify a value, such as 500 GB, 1000 GB or whatever is appropriate. Then click **OK**.

7. Printing

One advantage of networking is that it allows printers to be shared, thus potentially saving money as well as physical space. There are three methods for sharing a printer:

USB through DSM	Most USB-only printers can be plugged directly into the Server and DSM handles the sharing
Ethernet or wireless through DSM	The printer is connected to the physical network and DSM handles the sharing
Ethernet or wireless independently	Many modern printers have built-in Ethernet or wireless connections, giving them an existence on the network totally independent of any server or computers

At this stage, only very low cost and very old printers have USB-only connectivity and most people will not want to share such printers. Also, such arrangements are something of a kludge and can be very difficult (meaning time consuming and expensive) to diagnose and fix if they do not work. The second technique is analogous to the way networked printers have traditionally worked; print jobs are first sent to the server, which then feeds them out ("spools them") to the printer. This has some advantages in terms of control in a larger environment with many users and printers, but often requires someone to manage the process and generates an additional workload for the server. However, modern printers are intelligent devices in their own right and can talk directly to computers without a server acting as a middleman. In a small business environment, it is suggested that the third method is used.

The exact method of setting up any particular printer varies, but the following principles can usefully be followed:

- Printers may have wireless and/or wired connections. Wired connections are always preferable, as performance is so much better compared to wireless.
- Configure the printer with a fixed IP address. This should be adjacent to the address of the server and well away from the addresses used by the computers. For instance, in the example in this book the internet gateway is 192.168.1.1 and the server is 192.168.1.2. If two printers were added to the setup then suitable addresses would be 192.168.1.3 and 192.168.1.4
- Download the latest drivers for the printers. Consider storing the drivers in the *technical* folder (accessible as *server**technical* by the admin user) so that they can then be copied to the individual computers, rather than have to download them from the internet each time.
- Printer manufacturers sometimes offer a choice of drivers, for instance a basic one as well as a full-featured one. Use the basic one – the 'full feature' ones sometimes have superfluous features designed to capture marketing information and sell you more cartridges. However, be aware that with some multifunction devices (combined printers/copiers/scanners) not all functions may be available in a networked environment, or may require additional software from the manufacturer to be fully utilised.

8. Working Remotely

The ability to work outside the office whilst still being able to access to the organisation's data is of great importance to most companies. To meet this need Synology offers several different, complementary solutions:

File Station – allows users to login to the Server over the internet and download/upload files from within a browser

Cloud Station – a private version of a cloud service like Dropbox or SkyDrive

VPN or Virtual Private Network – allows users to connect remotely and access folders as though they were in the office

The above solutions are for regular computers. Additionally, Synology also has a selection of apps ("DS apps") to enable access from iOS and Android devices, described in Section 11.

8.1 Setting Up Remote Access

The first step that needs to be taken is to configure the server for remote access. The basic principle here is the same with any such system: ensure that it is connected to the internet; setup port forwarding so that incoming requests are directed to the right place; setup DDNS (Dynamic DNS) so that the system can be located on the internet. DSM includes something called the *Synology EZ-Internet Wizard* that largely automates the whole process and works perfectly for most people in most situations. There is also an even simpler method called *QuickConnect*; however, it has limitations on performance and capacity and for these reasons we will use the EZ-Internet Wizard.

Go to the **Main Menu** and click the **EZ-Internet** icon followed by **Next**:

Figure 63: The EZ-Internet Wizard

The first thing the wizard wants to know is how the server is connected to the Internet. There are three ways of doing so and all are very straightforward to configure. The most common scenario in a small business is that the connection is through a router (also sometimes referred to as a 'hub' or 'internet gateway') so we will assume that to be the case.

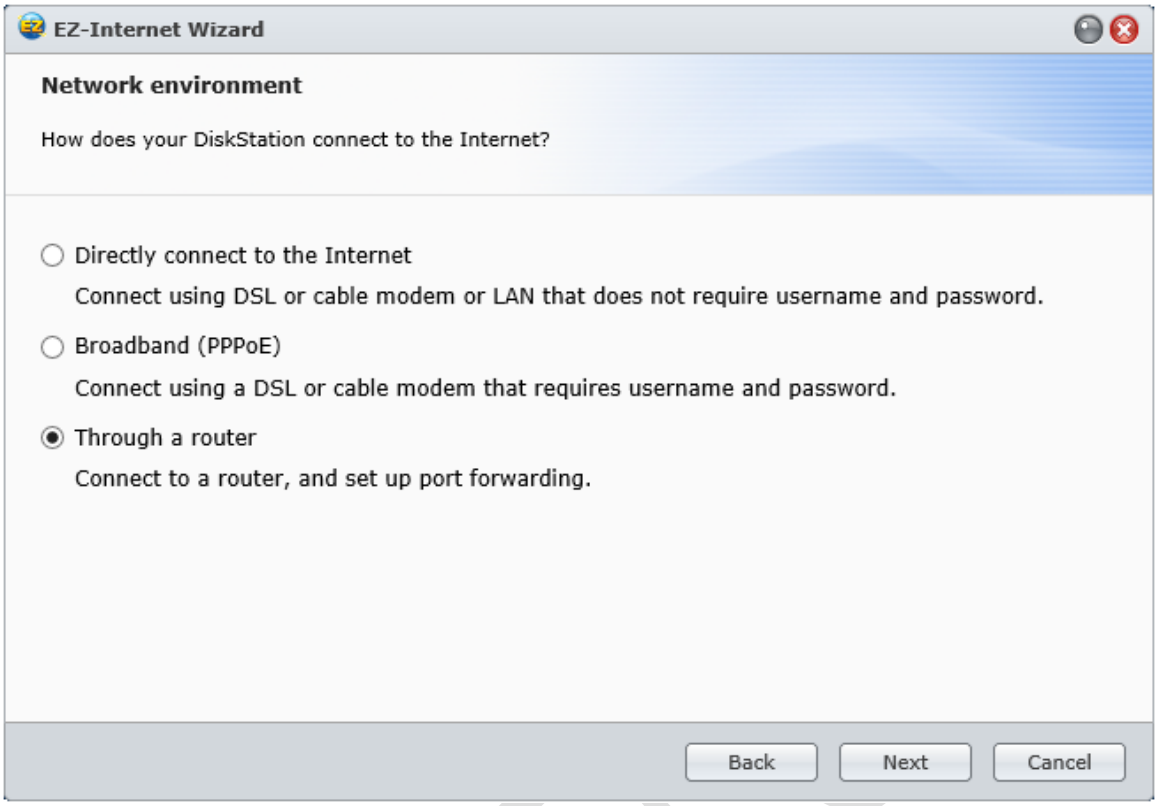

Figure 64: Specify the type of Internet connection

The wizard will now interrogate the router and in most cases should correctly identify it:

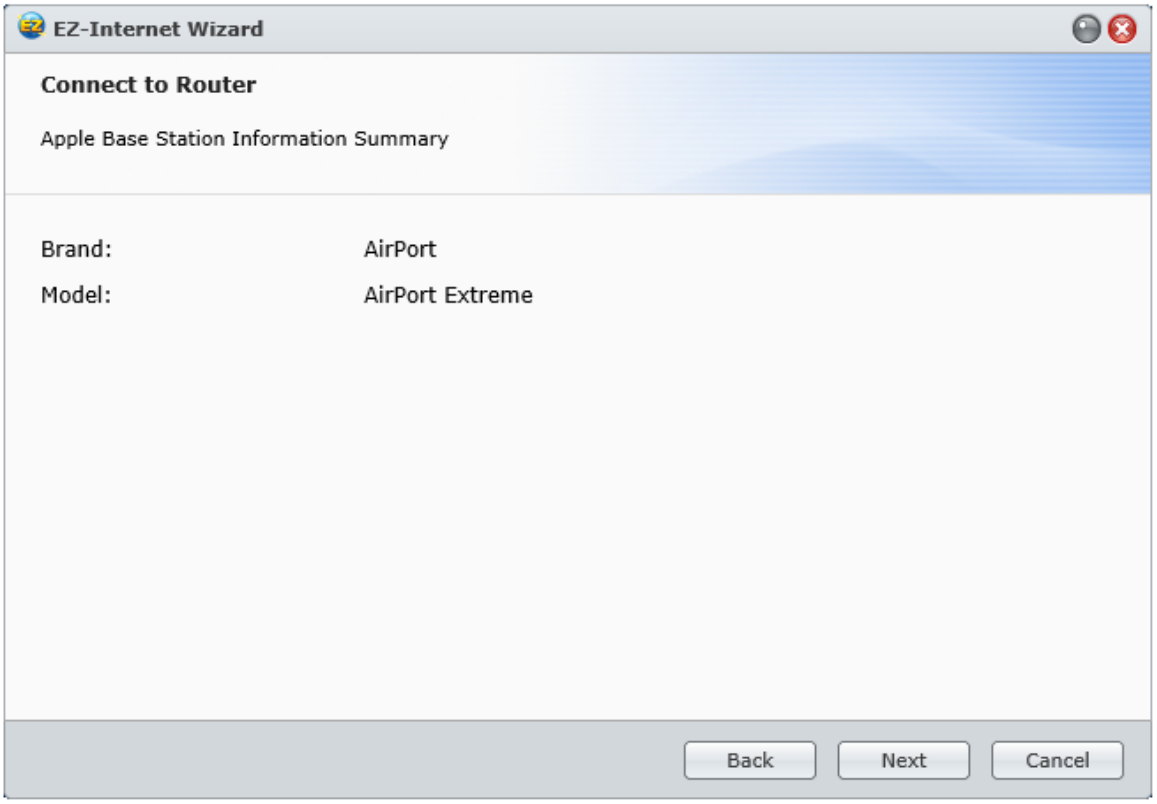

Figure 65: Identification of router

Clicking **Next** will cause the 'Port Forwarding Setup' to run. The purpose here is to specify what types of activity need to be done remotely. Unless you have very specific requirements simply accept the defaults that the wizard is proposing and click **Next**:

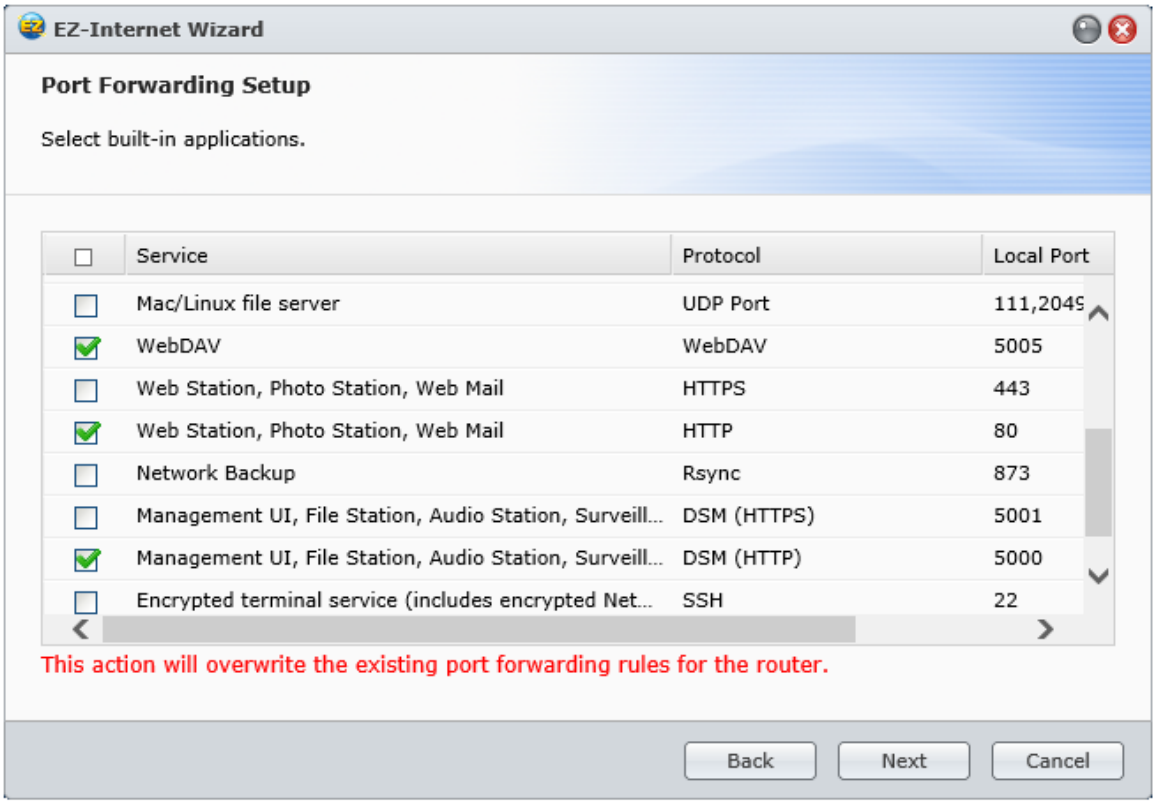

Figure 66: Port forwarding

The next step is concerned with DDNS. It is easy to find a website on the internet – you simply enter its name e.g. *www.ctacs.co.uk*, *www.synology.com* or whatever. But what is the name (hostname) of your server on the internet? The answer is: it doesn't have one; it just has a number (an IP address); you might not be aware of what that number is; that number may be changed from time-to-time by your internet service provider. DDNS services address this by giving you a unique name and automatically updating what goes on behind the scenes if the underlying IP address changes. Numerous organisations provide DDNS services, some on a free basis and others on a commercial basis. Examples of suppliers include No-IP, DynDNS and FreeDNS. Synology also offer free hostnames and signing up for one will be the best option for many small businesses. This process is quick and straightforward.

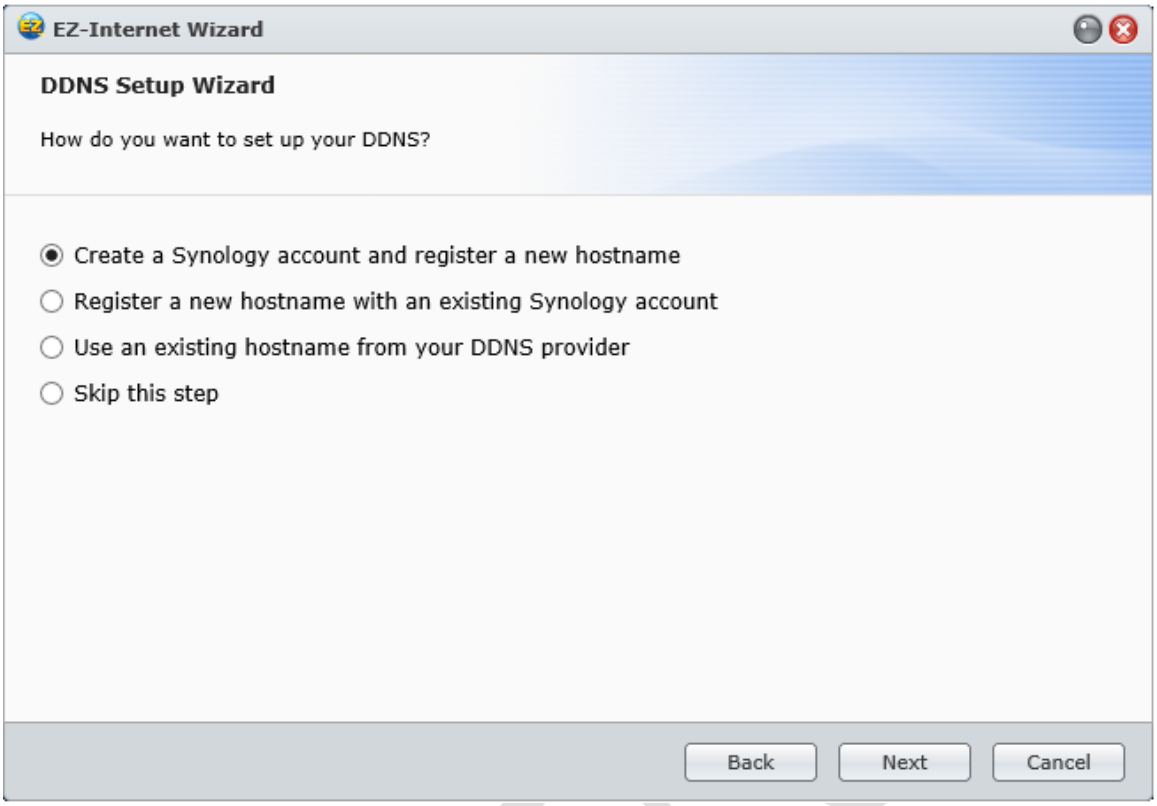

Figure 67: Setting up DDNS

Having created a Synology account and registered a hostname (or entered details of an existing hostname), the wizard continues with a confirmation screen. Just click **Apply** to proceed. Note that in this screenshot the DDNS details have been intentionally obscured:

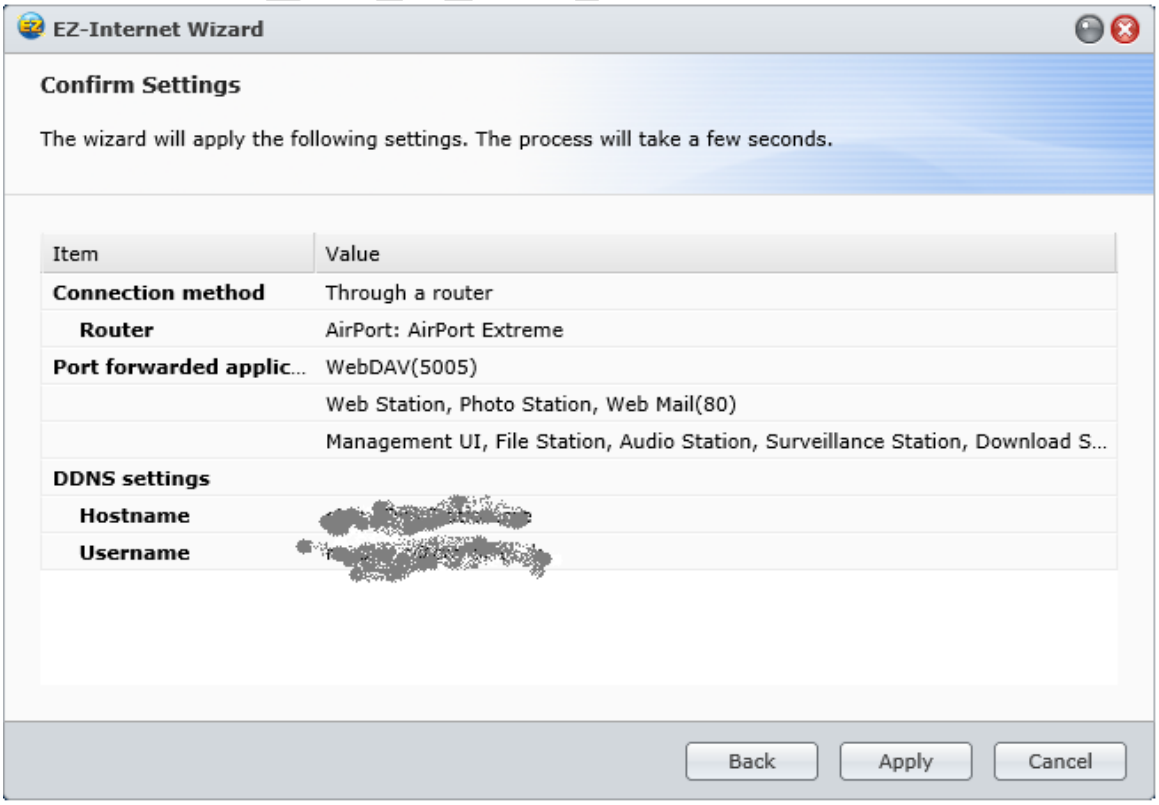

Figure 68: Confirmation of settings

Another screen is displayed – click **Finish**:

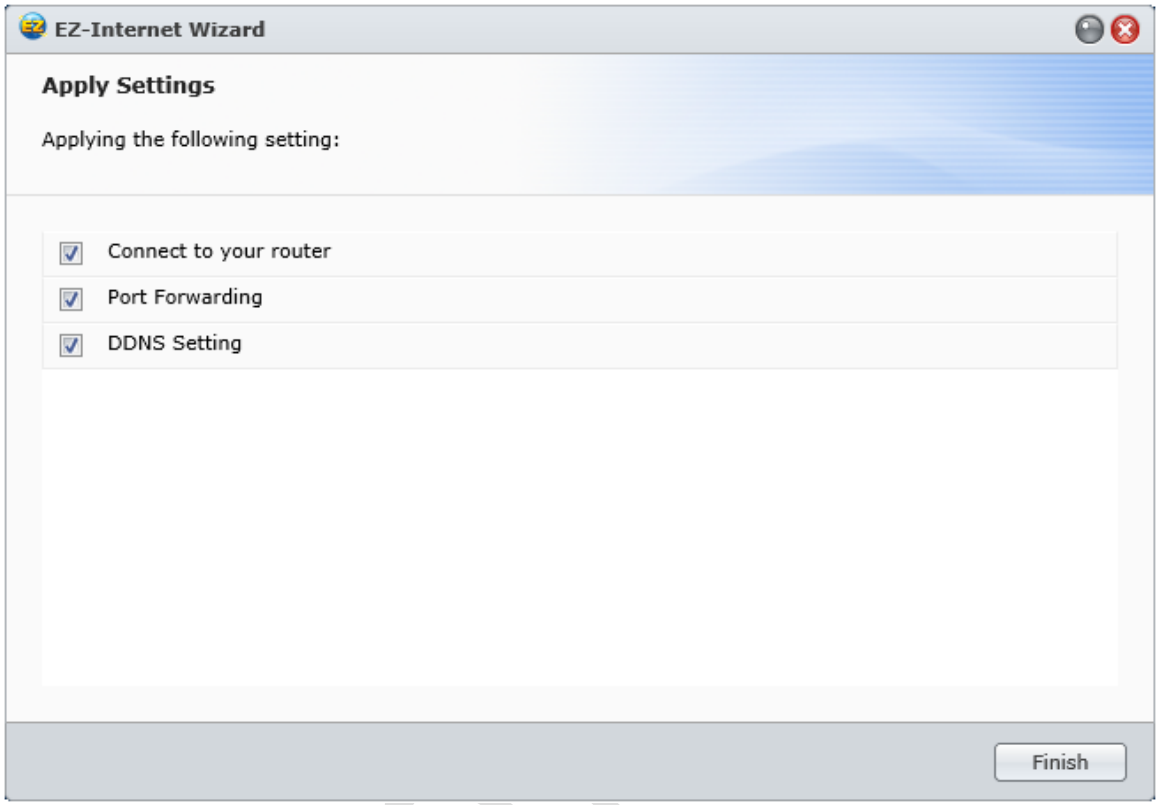

Figure 69: Final screen of EZ-Internet wizard

To test the setup, go to a computer, launch the browser (e.g. Internet Explorer, Firefox) and enter the hostname that you registered e.g. *ourcompany.synology.net* or whatever it is. You should be greeted with the main DSM logon screen after a few seconds. If it cannot be found, don't panic: some older routers have problems as they get confused as to whether the hostname is really internal or external. So, the next step is to check if the server can be accessed from outside the premises; if it can then everything is working.

If things are not working, then the most likely cause is that DSM has been unable to configure the router properly, in which case it will have to be done manually. This consists of forwarding ports 80, 5000 and 5005 to the internal IP address of the server and instructions for doing so with most routers can be found at the *www.portforward.com* website. Additional information on manually configuring remote access can be found on the Synology website at: http://www.synology.com/en-uk/support/tutorials/456#t3

8.2 Using File Station

In order to use File Station remotely, a user must be defined as having rights to do so. When a new user is created they receive appropriate rights by default; conversely, rights can be removed for any users who should not have remote access. This can be checked or changed by going to the **Control Panel** and clicking the **User** icon; select the user from the list and click on the **Applications** tab.

When offsite, a user can access the server from just about any computer with an internet connection – no preparatory work is needed and no software needs to be installed. Enter the registered hostname into the browser's address bar (e.g. *ourcompany.synology.net* or whatever it is) and after a few seconds the normal DSM login screen will be displayed. The user should enter their name and password and they will be presented with a fairly minimalist Desktop; in essence, all they can access is File Station (unless additional options have been granted to them).

File Station can be launched by clicking on its icon, which appears on the Desktop and also in the Main Menu. Within File Station they can only see folders and files that belong to them or to which they have been granted access, such as their home folder and the shared folder we setup.

To work with a file or folder, right-click it and a pop-up menu will appear with the various available options. Alternatively, click the **Action** button:

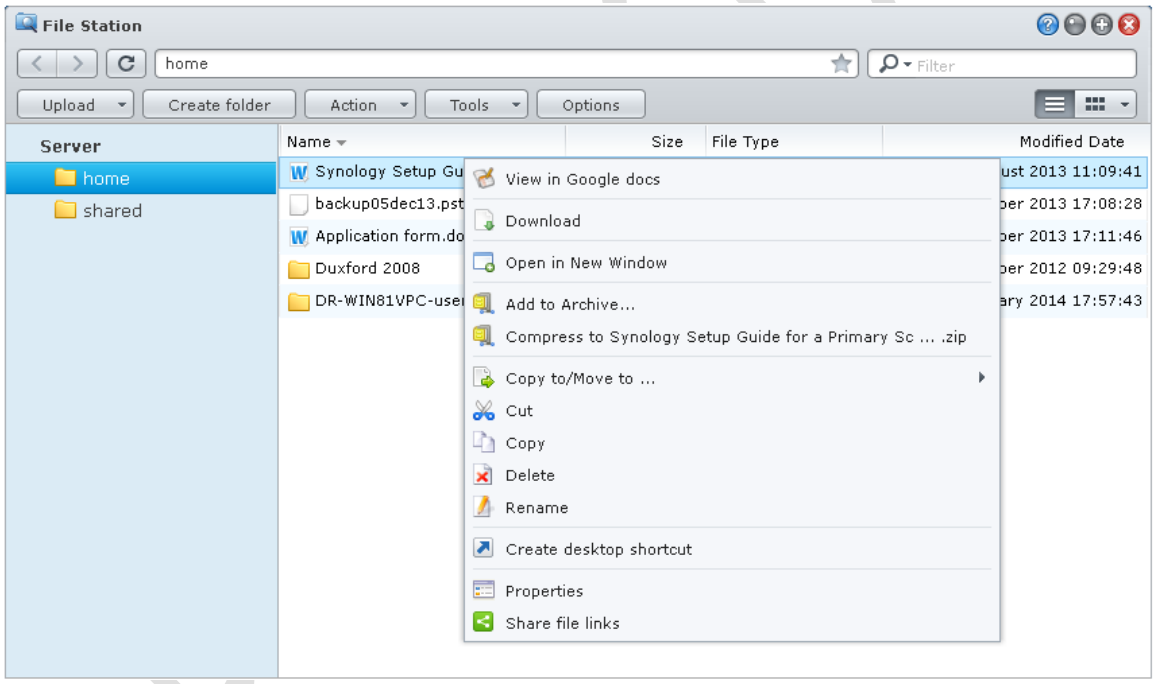

Figure 70: File Station display

There is an option to view documents, spreadsheets and presentations using Google docs, although there are some restrictions on the maximum size of files that can be viewed in this way. Also note that this is a viewer only and not an editor. If it is required to edit a file, choose the **Download** option to first download it to the local computer. Make the changes to the document using Word, Excel or whatever application is used, then use the **Upload** button in File Station to upload the new version back to the server.

Most graphic files and photographs can be viewed by double-clicking on them. From there they can be zoomed etc.

When the user has finished the remote session, they should logout. To this, click on the **Options** icon in the top right-corner of the screen and click **Logout**:

Figure 71: Option to Logout

As an additional safety precaution the browser should then be closed. If this is not the user's normal computer they should clear down the history as well.

8.3 Setting up and Using a VPN

The purpose of a *Virtual Private Network* or VPN is to securely extend a network to users who are offsite, such as home workers or those in a remote office. Think of it as the equivalent of having a very long network cable that reaches out from the office for 10, 100, 1000 miles or more. However, instead of an actual cable the connection goes over the internet, with powerful encryption and other techniques used to maintain security. One advantage of a VPN is that it allows proper access to files and folders for editing, just as if in the office. One caveat: VPNs can be notoriously difficult to setup, configure and diagnose. DSM goes a long way towards making it easy and it usually works, but if it doesn't then be prepared for some pain.

Start off by downloading and installing the VPN Server from the Package Centre. Having done so, open the **Main Menu** and click **VPN Server**:

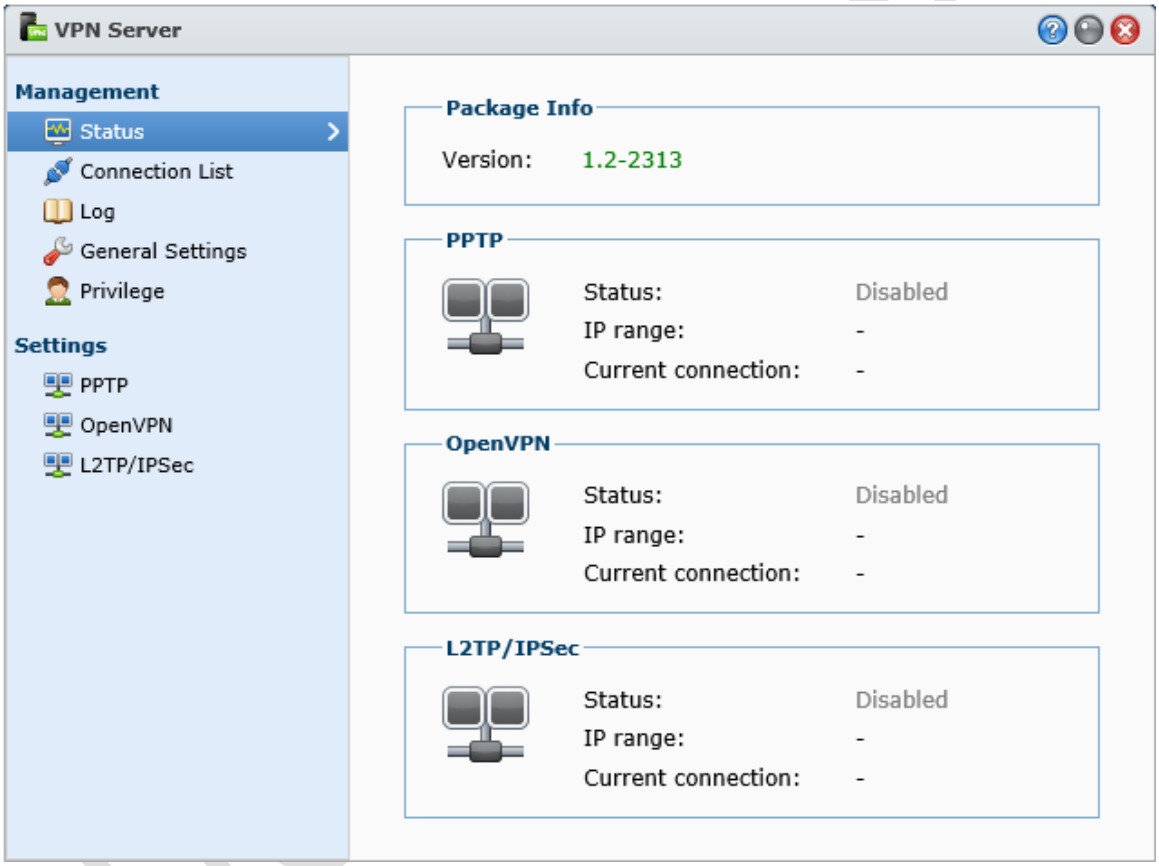

Figure 72: VPN Server main screen

VPNs come in a variety of 'flavours', based around different protocols. The Synology VPN Server supports the popular ones of PPTP, OpenVPN and L2TP/IPSec. These have varying qualities; PPTP is a relatively old one but is widely supported on many different types of clients and will be used here as an example.

Click **PPTP** under the Settings section and on the resultant panel check the **Enable PPTP VPN Server** tickbox. The default settings are fine – the only one that needs particular attention paying to it is the **Dynamic IP address** setting. The key principle here is that the IP range is different from that used within the internal network; so if, for example, the internal network uses the 192.168.nnn.nnn addressing scheme then the VPN should be set to use the 10.nnn.nnn.nnn addressing scheme (or the other way around). Click **Apply**

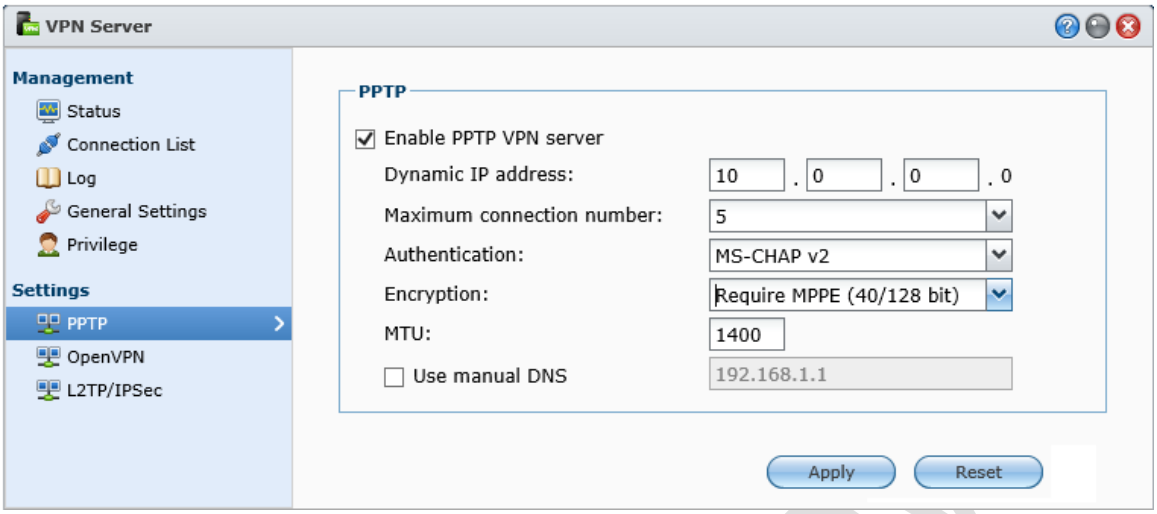

Figure 73: VPN settings

A warning will may be given about port 1723 needing to be open on the router. To do this, choose **Control Panel** > **Router Configuration**. Click the **Create** button. A panel called 'Port Forwarding' is displayed – click **Built-in application** followed by **Next**. On the resultant screen tick the options relating to VPN Server, then click **Apply** followed by **Save**. There may be some warning messages generated but these can be ignored. Click the **Test Connection** button to make sure everything seems okay. If it is, then you can proceed to configure the client computers.

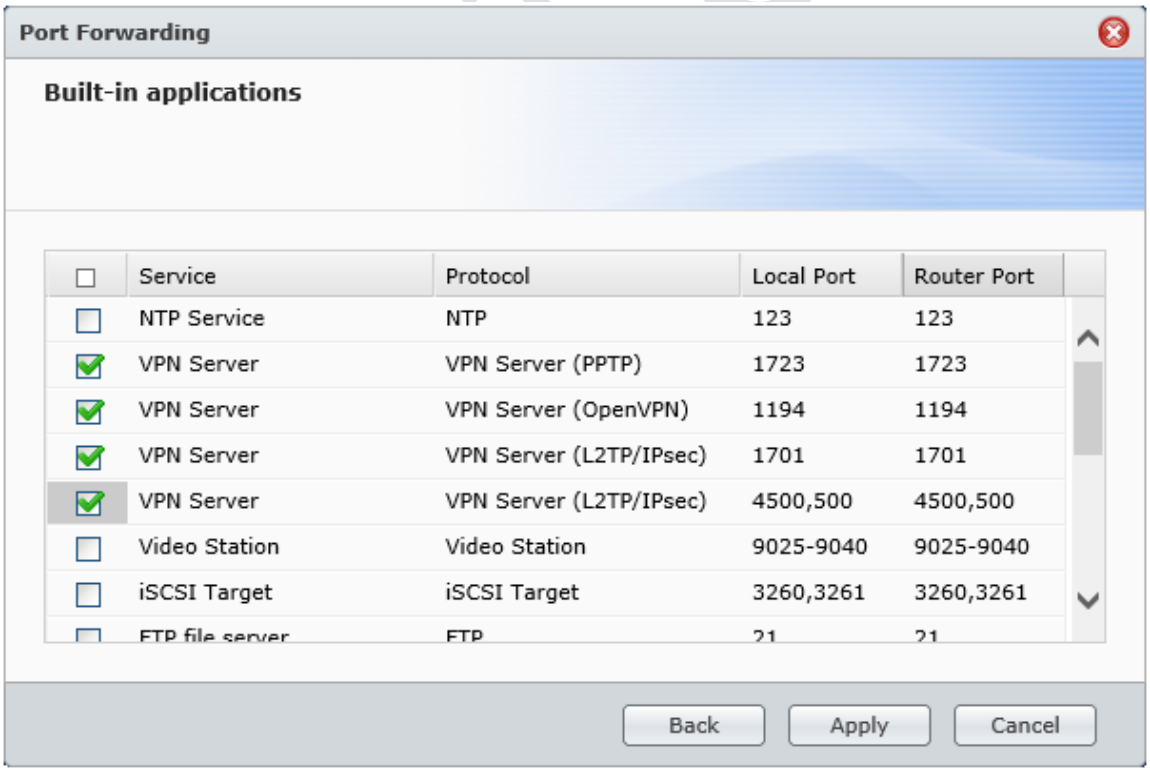

Figure 74: Port forwarding for VPN

8.3.1 Configuring Windows 8 Clients

Go into the **Control Panel** and choose **Network and Sharing Centre**. Click on **Setup a new connection or network**. On the panel that pops up choose **Connect to a workplace** then **Next**:

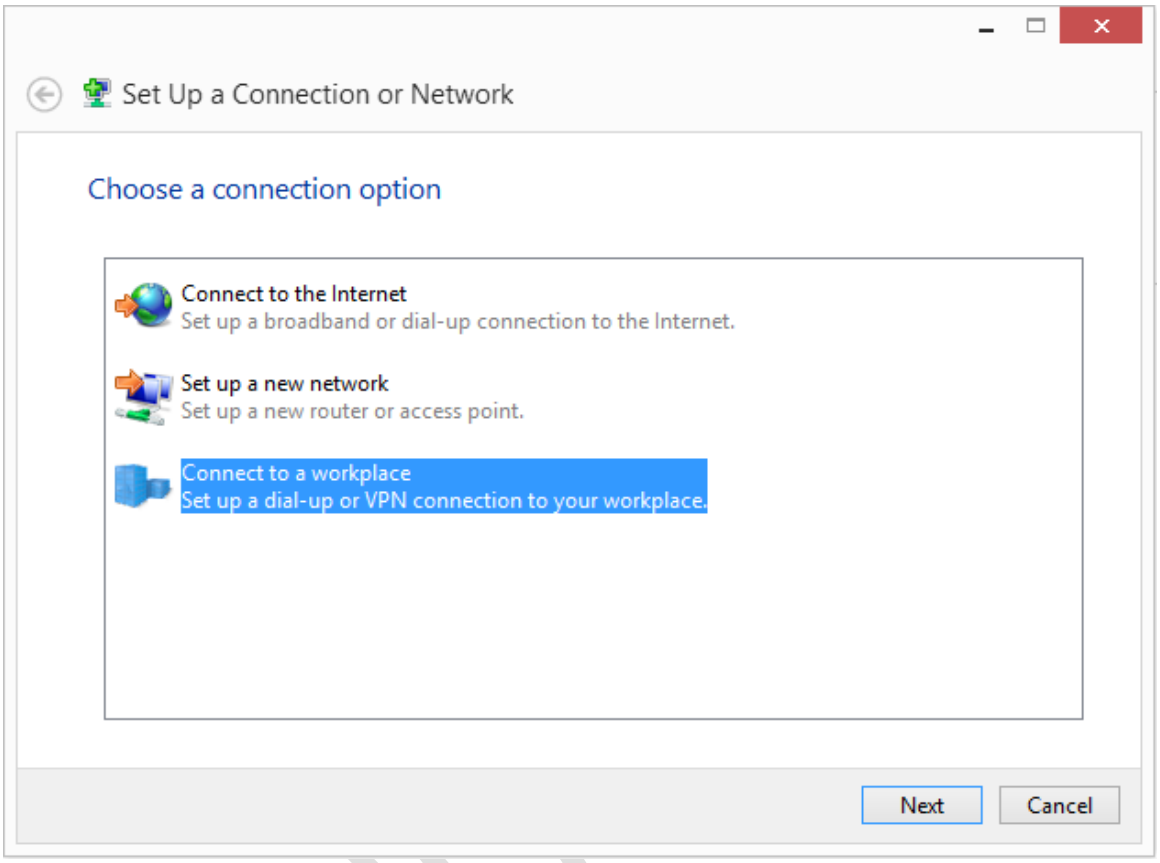

Figure 75: Setup a new connection

On next screen click **Use my Internet connection (VPN)**:

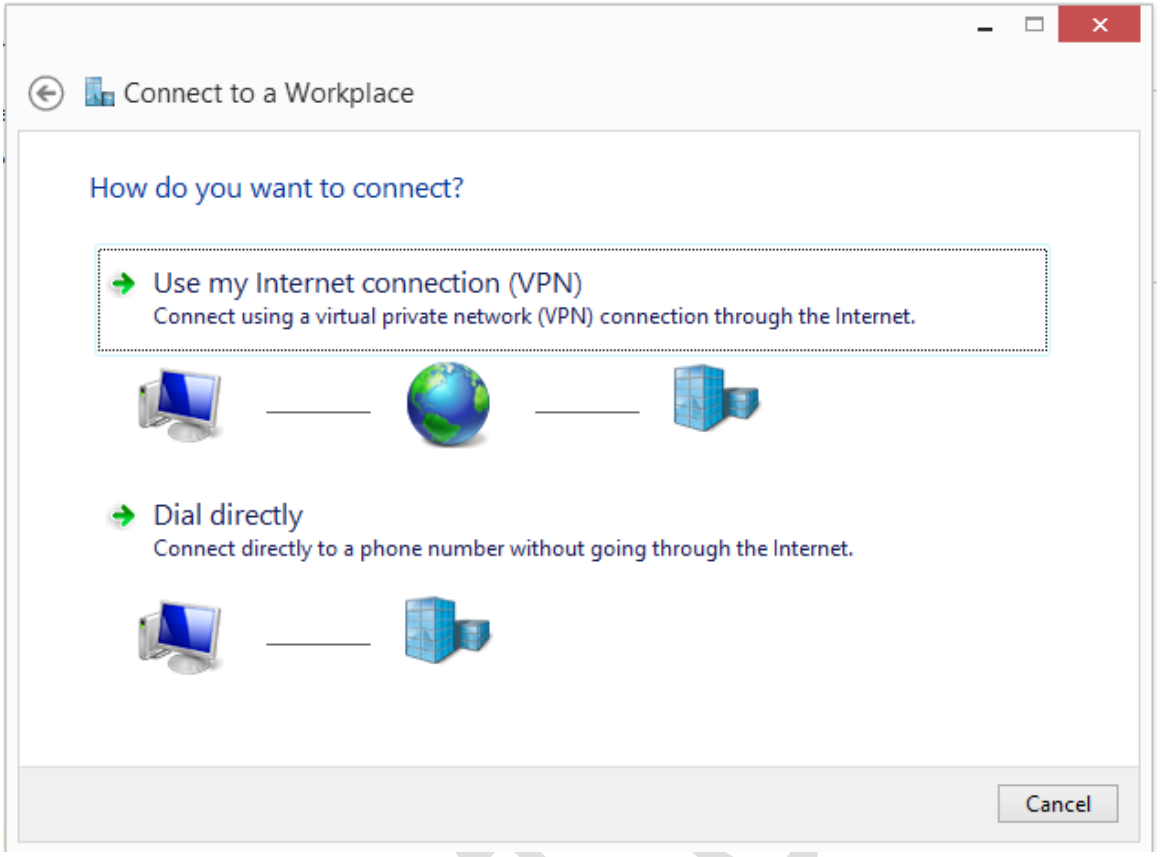

Figure 76: Choose VPN connection

Enter the external domain address (hostname) that you registered earlier and click **Create**:

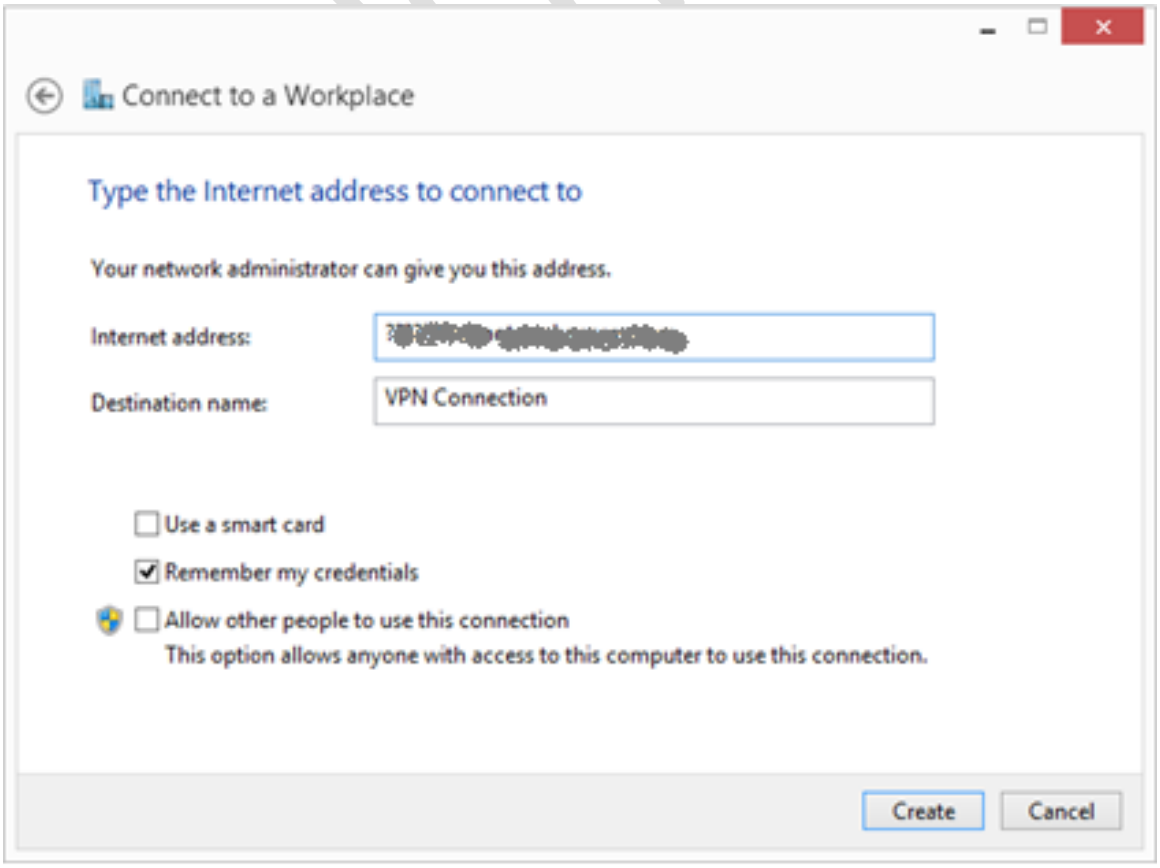

Figure 77: Enter the external address of the DiskStation

After a little while the Networks panel will pop up on the right-hand side of the screen, showing that a VPN connection has been defined:

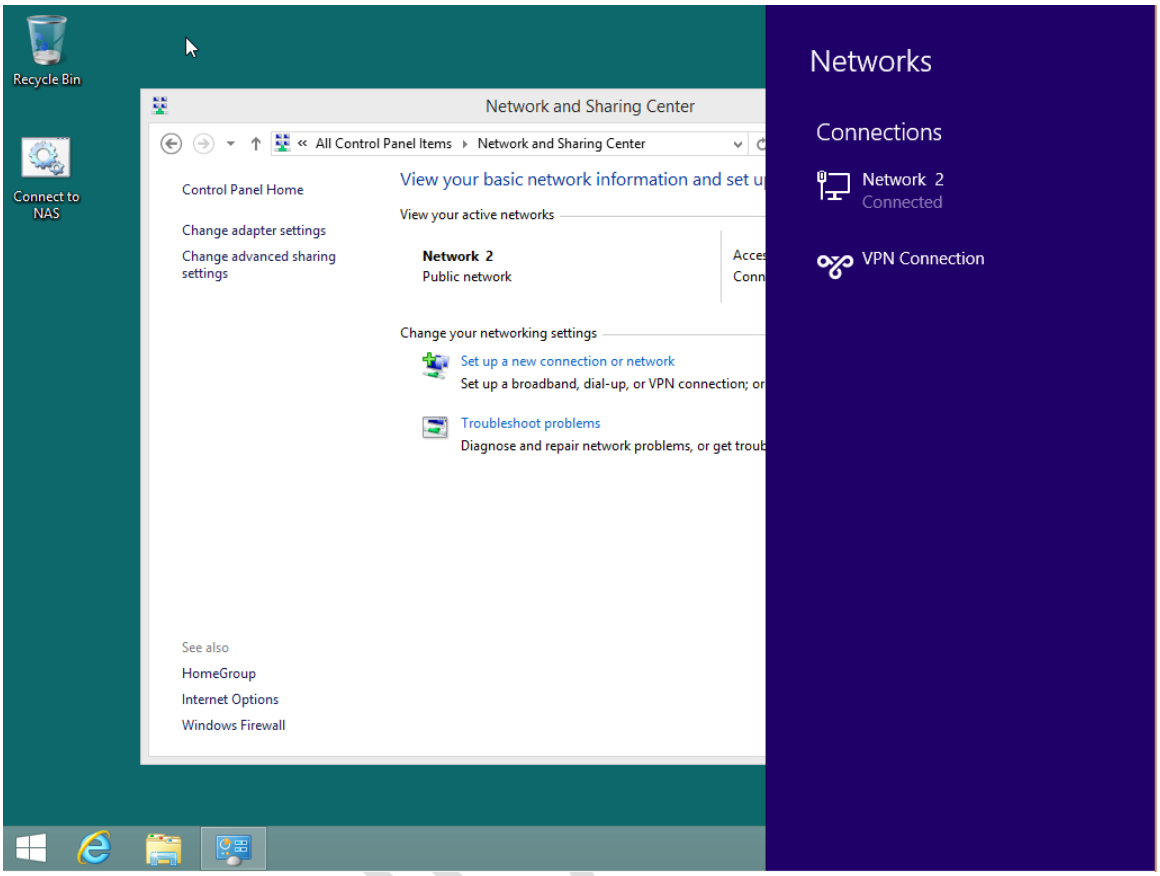

Figure 78: VPN appears in list of connections

Click on the newly created VPN Connection – enter the user name and password and after a few seconds the user will be connected. The next stage is to test the computer (preferably outside of the office!).

The usual way to start the VPN connection is by click the network icon on the Taskbar; the list of available networks will appear on the right-hand side of the screen thus:

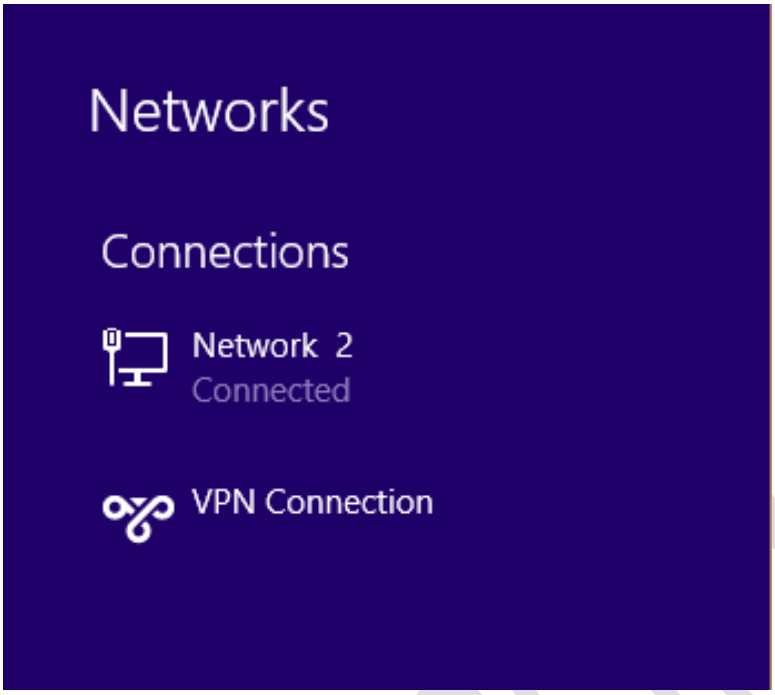

Figure 79: List of connections

Click the VPN Connection and a button labelled **Connect** will appear - click it. You will then be prompted to sign in using the normal network username and password:

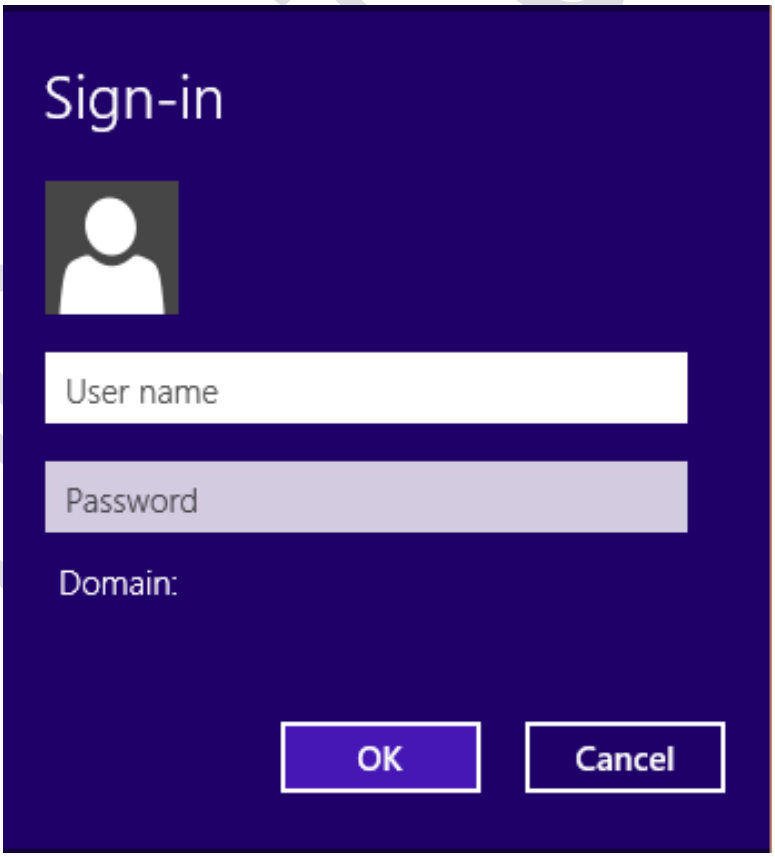

Figure 80: Enter user name and password

A few seconds later you should be connected. You can now access resources on the Server as though you were in the office. For instance, press the **Windows key** and the **R key** simultaneously and in the run box type \\server\company to display and access the shared folder.

When you have finished, click the network icon on the Taskbar to again display the list of network connections on the right-hand side of the screen. This time click the VPN Connection and then click the **Disconnect** button.

8.3.2 Additional Information for Windows 8 Computers

If the VPN connection does not work on Windows 8, try this. Right-click the **Start** button and choose **Network Connections**. The newly created VPN connection should appear alongside the computer's normal network connection(s):

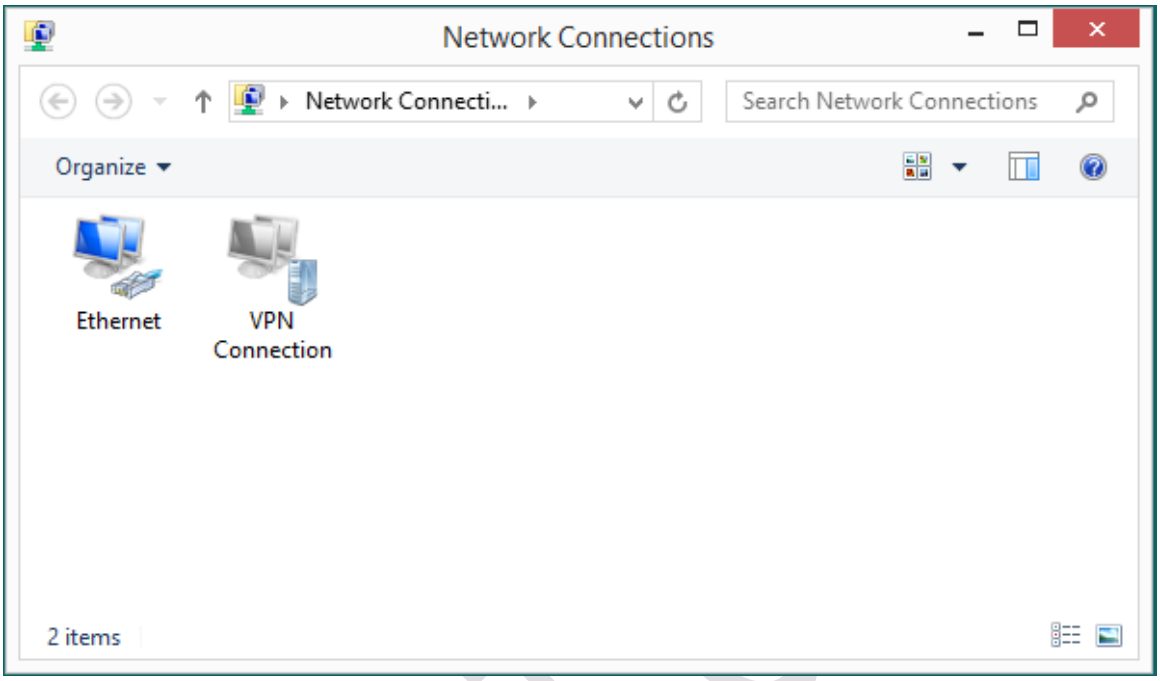

Figure 81: List of network connections

Right-click the newly added VPN Connection and choose **Properties**. Click the **Security** tab. The 'Data encryption' dropdown needs to read **Optional encryption (connect even if no encryption)** and the **Allow these protocols** button should be enabled, such that the panel appears as follows. Then click **OK**.

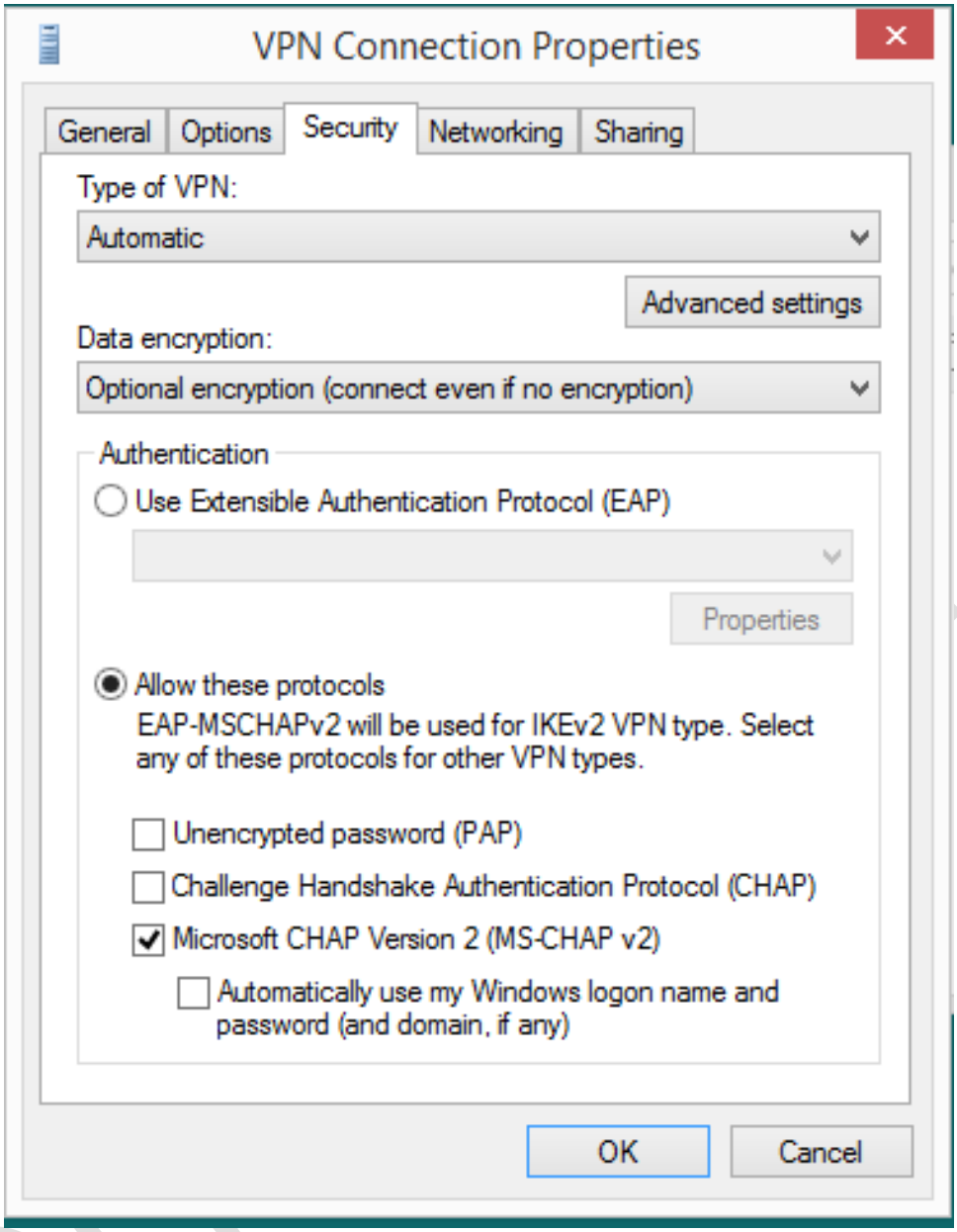

Figure 82: VPN connection properties

8.3.3 Windows 7 Clients

Go into the **Control Panel** and choose **Network and Sharing Centre**. Click on **Setup a new connection or network**. On the panel that pops up choose **Connect to a workplace** then **Next**:

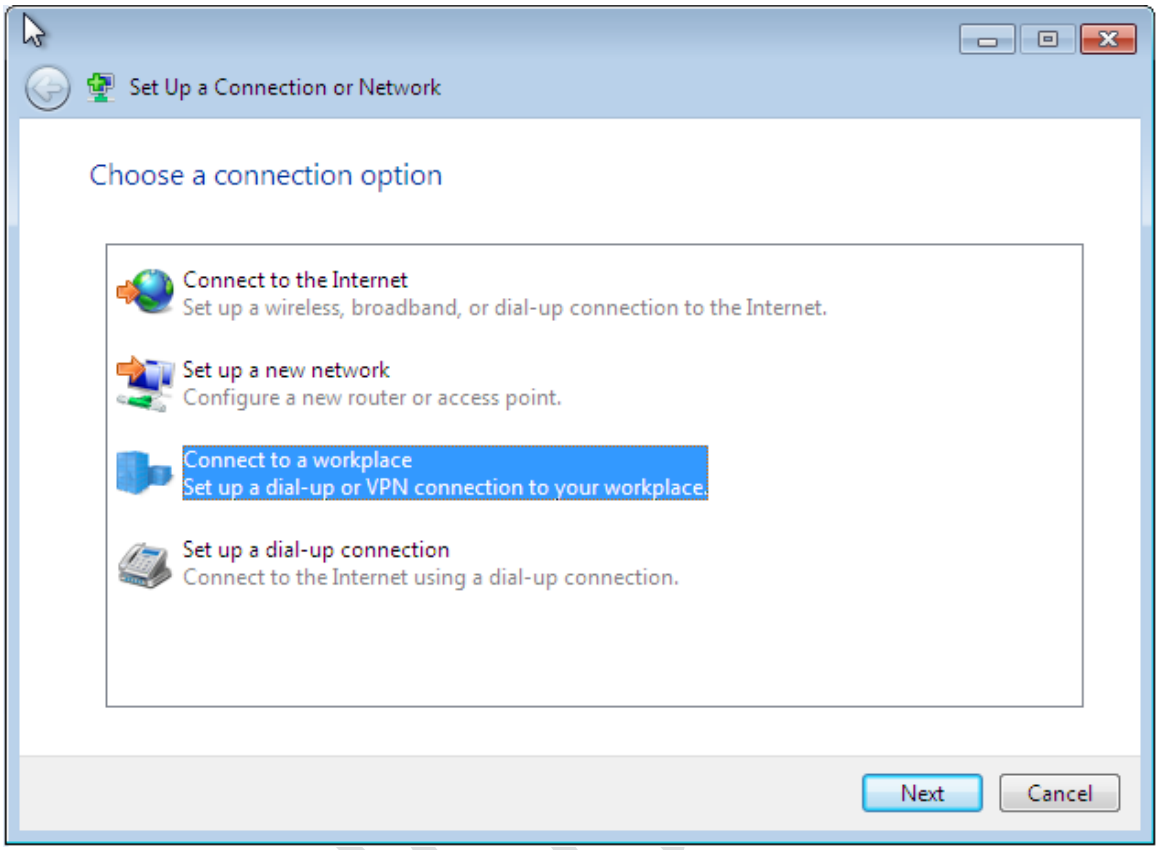

Figure 83: Setup a new network connection

On the next screen click **Use my Internet connection (VPN):**

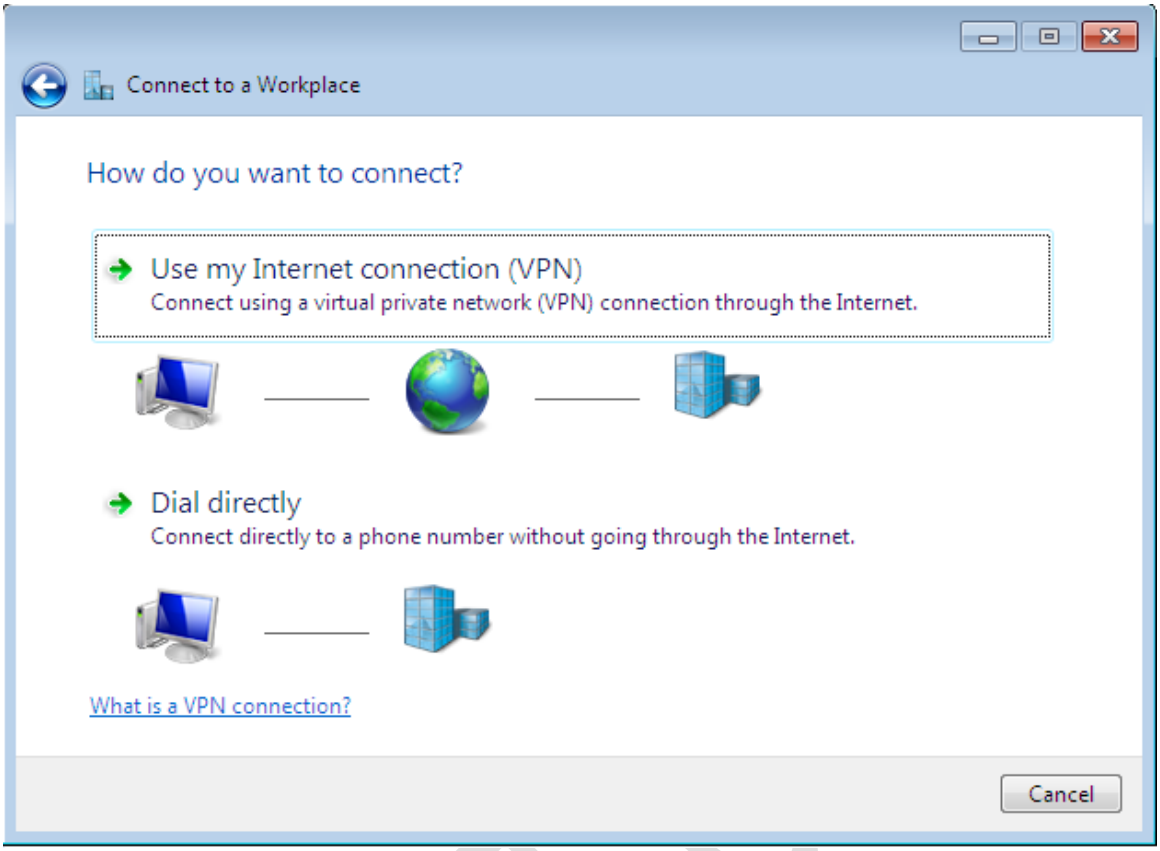

Figure 84: Setup a new VPN connection

Enter the external domain address (hostname) that you registered then click **Next**:

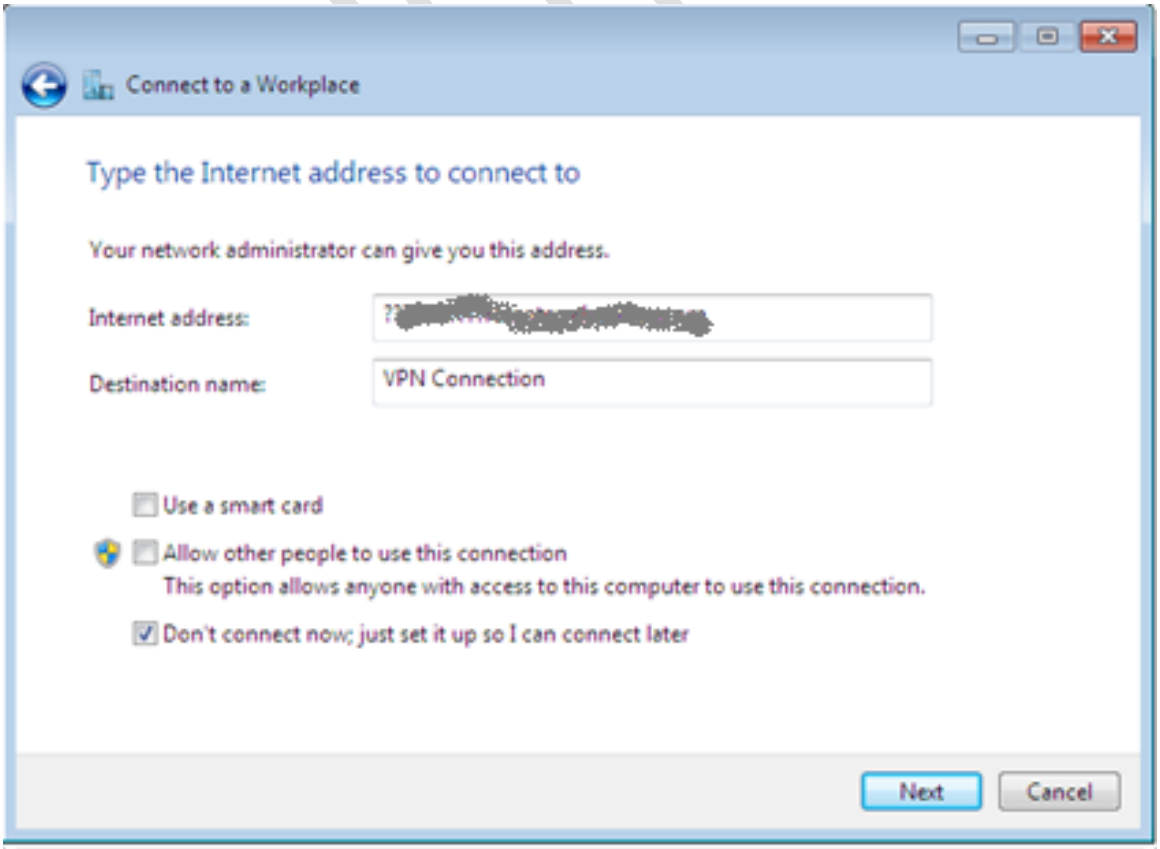

Figure 85: Enter the external address of the DiskStation

On the following screen enter the user name and password (there is no Domain name):

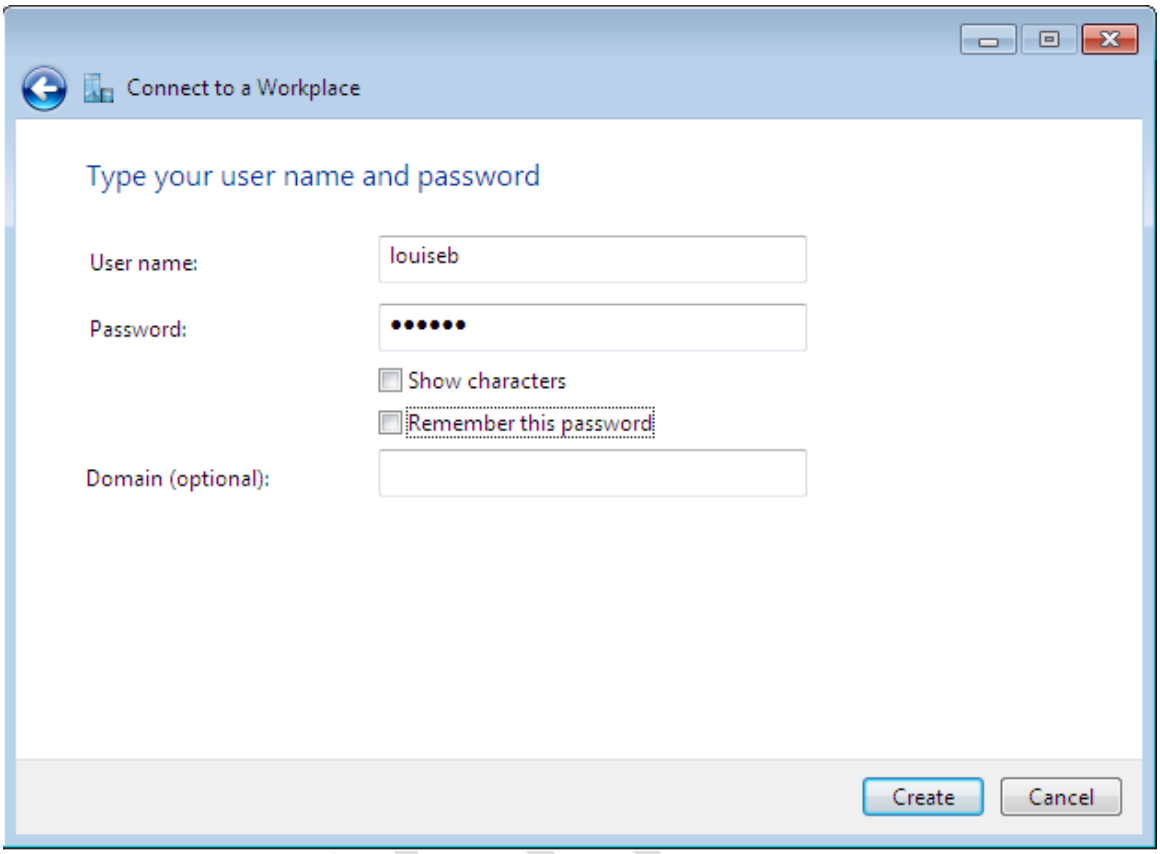

Figure 86: Enter user name and password

Assuming all is well, a few seconds later a confirmation screen will be shown. Click **Close**:

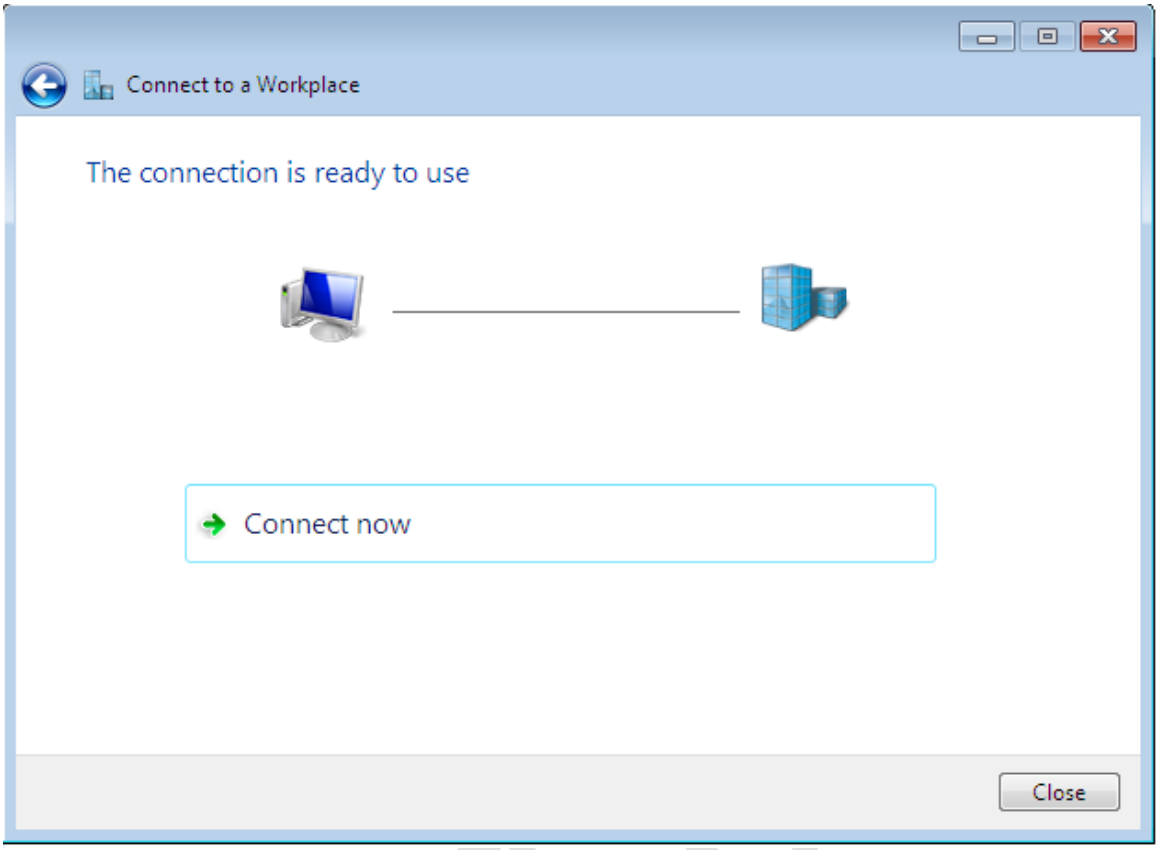

Figure 87: New connection is ready for use

The connection should now be tested from outside the office. Click the network icon on the Taskbar:

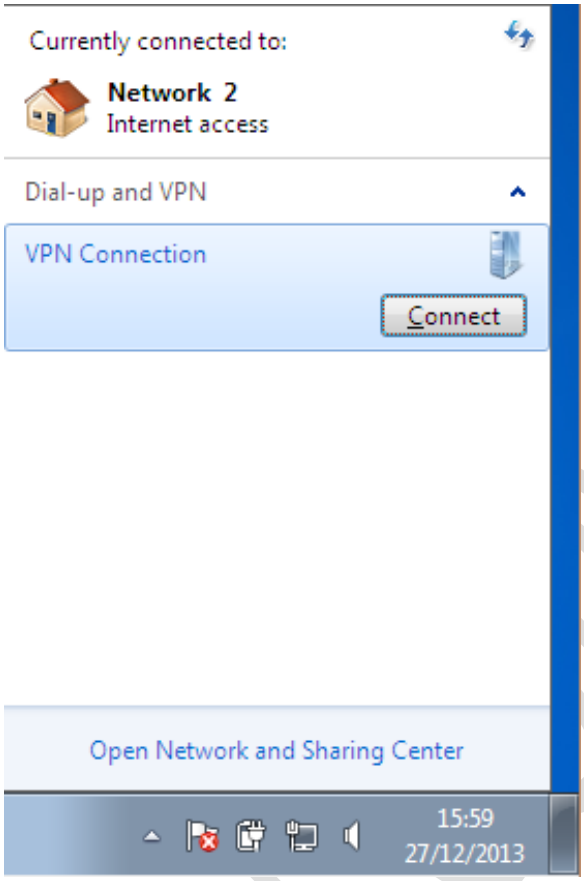

Figure 88: List of connections

A list of available network connections appears in the bottom right-hand corner of the screen. Click the VPN Connection and then the **Connect** button that subsequently appears. A logon panel is shown; enter the user name and password (it is not necessary to enter a Domain name) and click **Connect**:

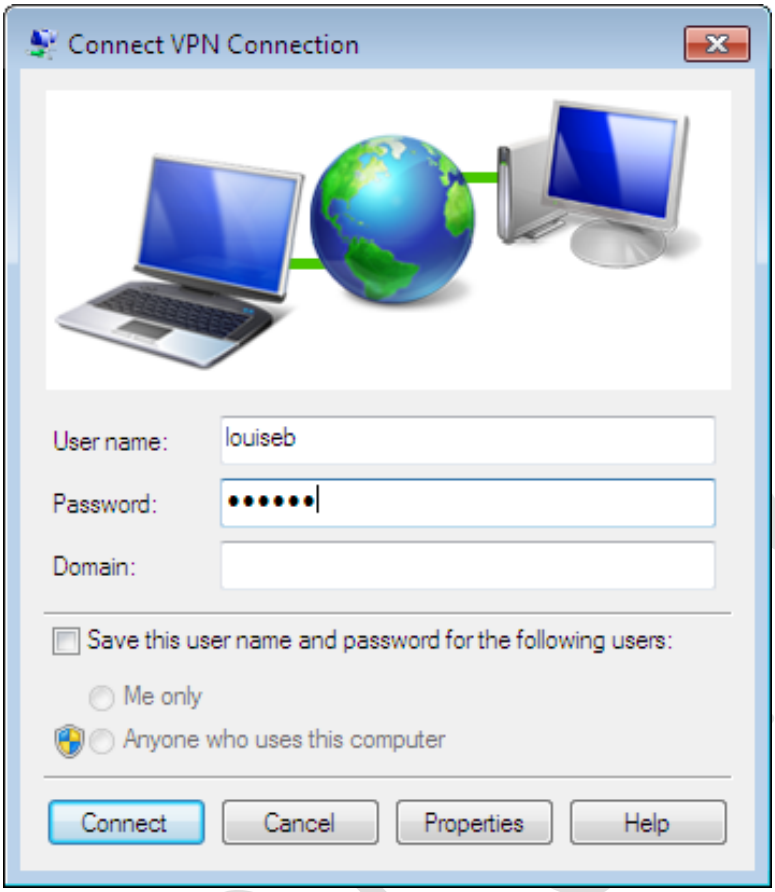

Figure 89: Enter user name and password

A few seconds later you should be connected. The first time you connect you may receive a prompt asking to choose the network location; a choice of Home, Work and Public is given - Choose **Work**.

You can now access resources on the Server as though you were in the office. For instance, press the **Windows key** and the **R key** simultaneously and in the run box type *server**shared* to display and access the shared folder or *server**home* to access the user's home folder.

When you have finished, click the network icon on the Taskbar to again display the list of network connections on the right-hand side of the screen. This time click the VPN Connection and then click the **Disconnect** button.

8.3.4 Verify Connections from the Server

The status of the VPN and the connections in use can be monitored from the server. From the **Main Menu** choose VPN **Server** and click on **Connection List**:

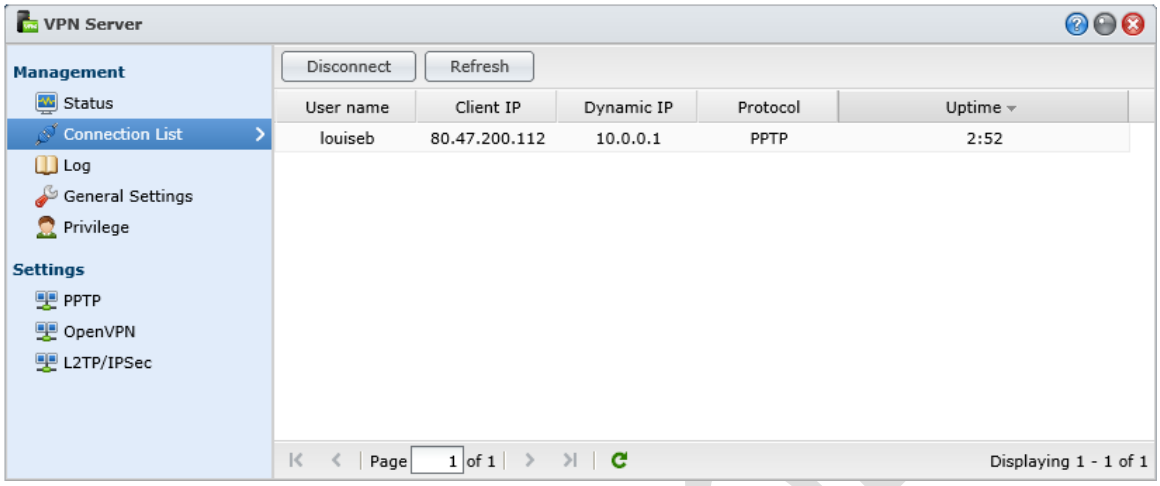

Figure 90: List of active VPN connections

If required, a user can be disconnected from the VPN by highlighting their name and clicking the **Disconnect** button.

8.4 Setting up and Using Cloud Station

Many people will be familiar with cloud-based syncing services such as Dropbox, SkyDrive, Google Drive and so on. The basic idea is simple: somewhere on the internet is a small amount of private space for your usage – think of it as a USB memory stick in the sky. On your computer is a folder corresponding to that space. Anything you put in that folder is automatically copied ('synced') to that space on the internet. If you then install the sync software on another computer it will have a copy of whatever is on the first one. Whenever anything changes on one computer, the change is reflected automatically on the other.

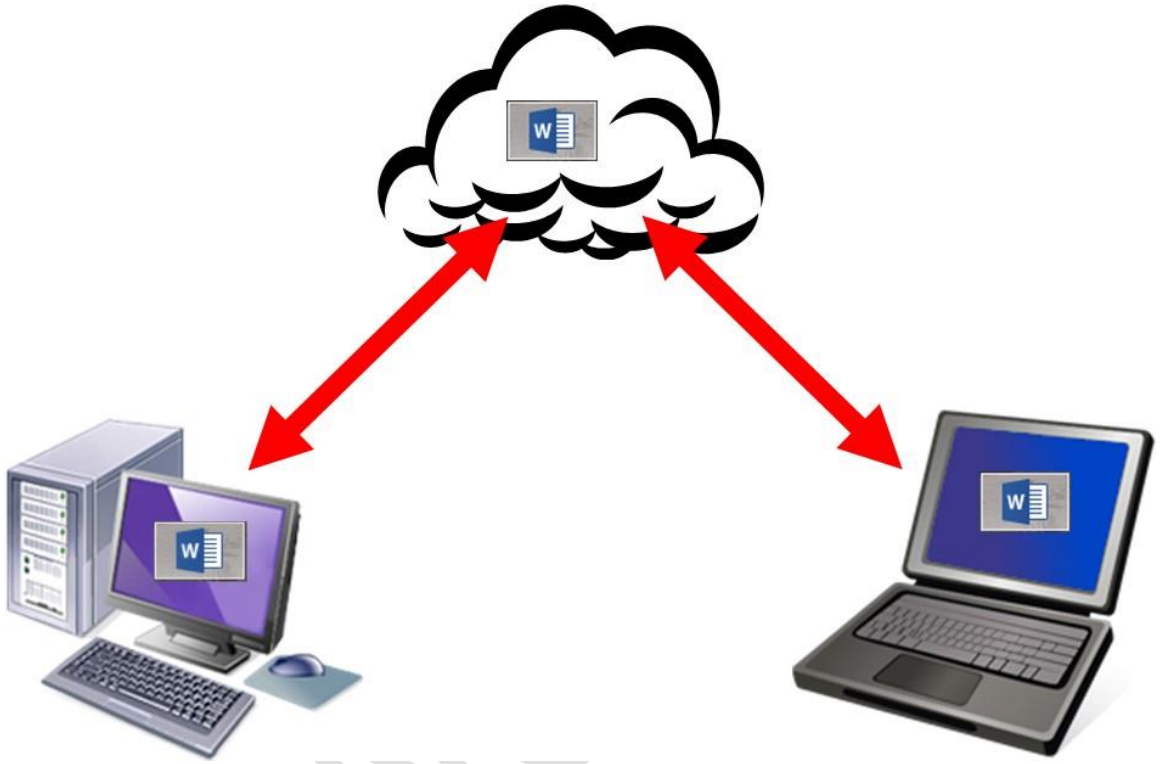

Figure 91: Cloud computing overview

Whilst incredibly useful, these services do have some drawbacks. Firstly, although they give some free space it is not very much and if you need more you have to pay for it e.g. Dropbox gives 2GB free but charges US $119.88 a year for 100GB. Secondly, most services have restrictions on file sizes and how much data you can store on them. Finally, some people are just not comfortable with the idea of their data being held by Microsoft or Google or whoever. Synology's *Cloud Station* gets round all of these issues: it is free to obtain and use; there are no practical restrictions on space and usage; data is stored on your server, meaning everything is under your control. Put simply – Cloud Station is a "private cloud". It is thus particularly suitable for people who work away from the main premises or users who take laptops home.

8.4.1 Installation of Cloud Station on Server

Download and install Cloud Server from the Package Centre. After it has installed launch it from the **Main Menu** by clicking on the **Cloud Station** icon; the following panel is displayed:

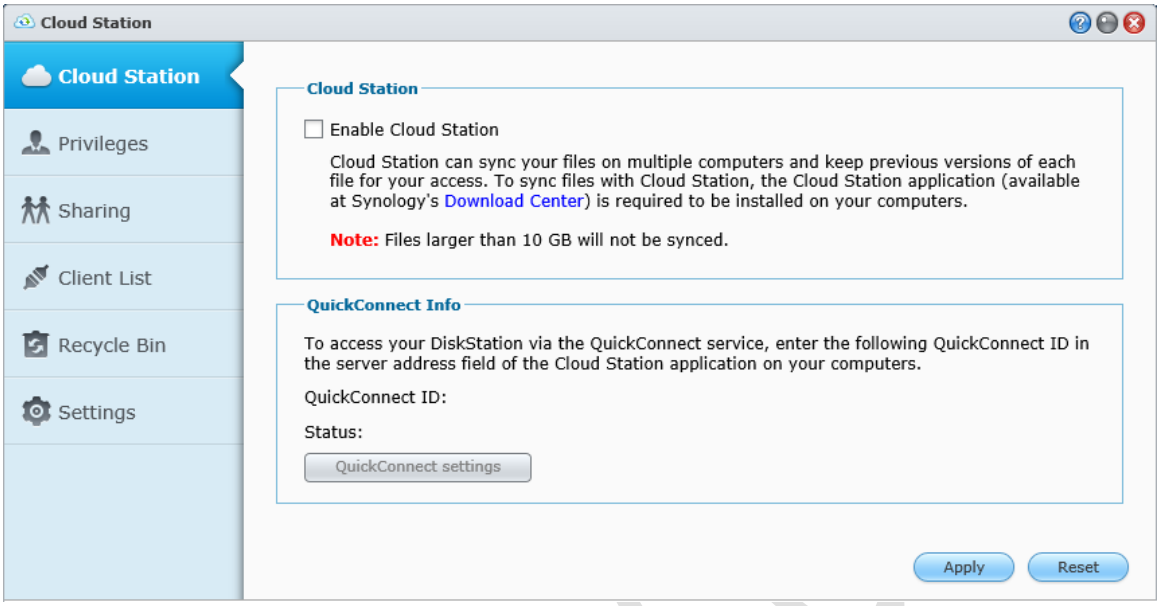

Figure 92: Cloud Station screen

Check the **Enable Cloud Station** tickbox followed by **Apply**. It will then be possible to use the tabs down the left-hand side of the panel (note that there may be a slight delay the very first time that this is done). Click on the **Privileges** tab – this displays the list of users and is where Cloud Station can be enabled for those who are going to use it. Use the tickboxes then click **Save** when finished.

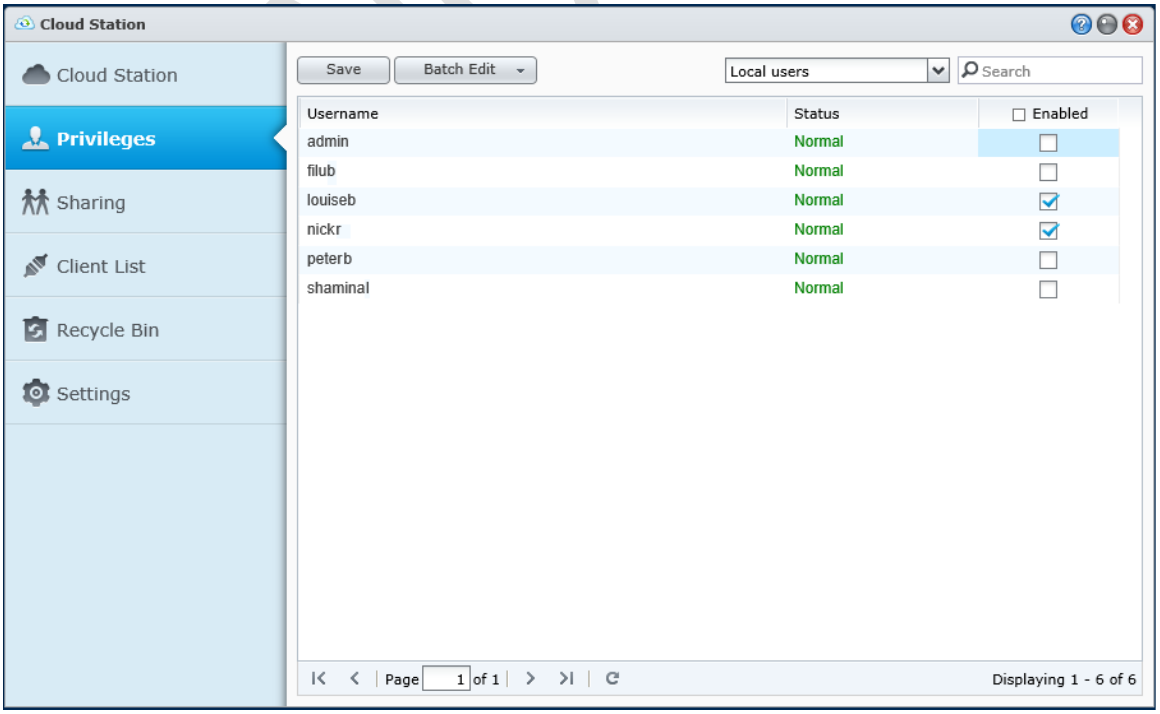

Figure 93: Enable users for Cloud Station

The **Sharing** tab is for specifying which folders will be synced. A list of all shared folders is displayed; place a tickbox against the folder(s) to be shared and click **Save**. Avoid the temptation to share everything – in this example it is just the folder called *shared* that will be synced. Note that users must have full read/write access to any synced folders.

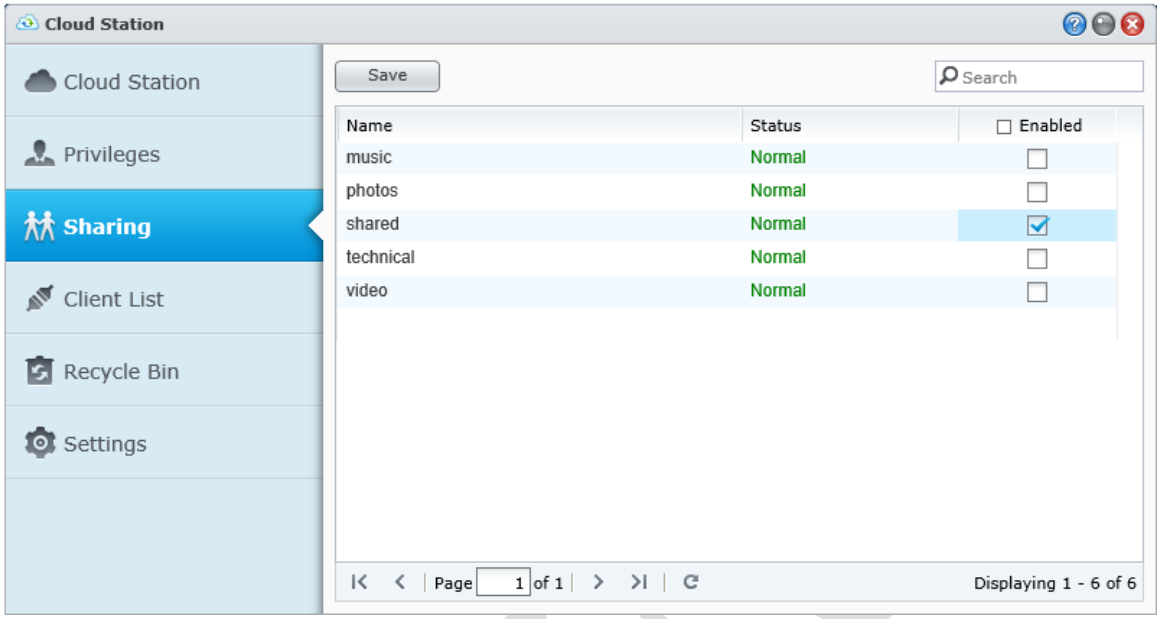

Figure 94: Specify the folders

The Client List tab is used for monitoring who is using the system. The Recycle Bin and Settings tab can be ignored.

Go to the **Control Panel** and click on the **Router Configuration** icon. Click the **Create** button. A panel called 'Port Forwarding' is displayed – click **Built-in application** followed by **Next**. On the resultant screen tick the entry for **Cloud Station** then click **Apply** followed by **Save**. There may be some warning messages generated but these can be ignored. Click the **Test Connection** button to make sure everything seems okay. If it is, then you can proceed to configure the client computers.

8.4.2 Installation of Cloud Station on User Computers

The synchronisation software – the Cloud Station client - has to be installed on a computer in order for it to connect to the server. It is available from the Download section of the Synology website in both Windows and Mac versions; this walkthrough uses the Windows version.

Upon running the Cloud Station client for the first time the following panel is displayed:

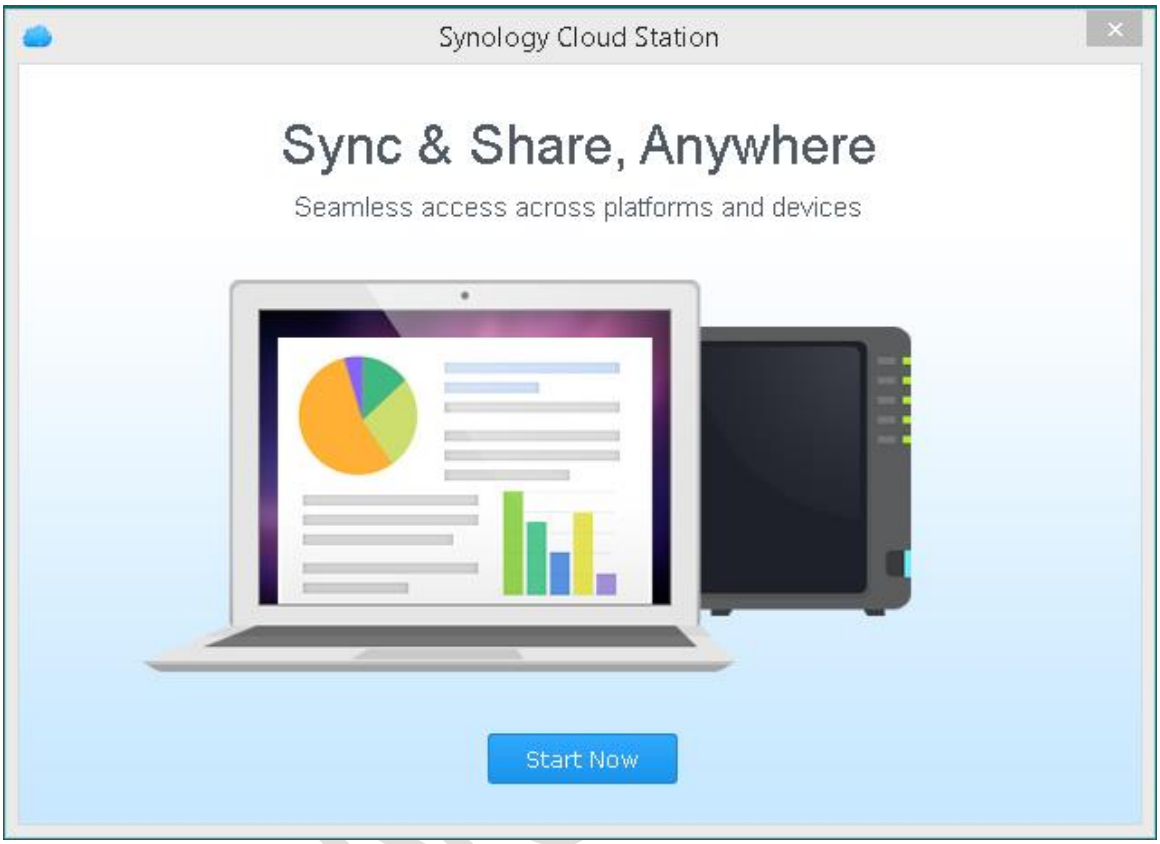

Figure 95: Installation of Cloud Station client

Click **Next**. On the following screen enter the external domain name (hostname) that was previously registered, along with the user name and password, then click **Next**:

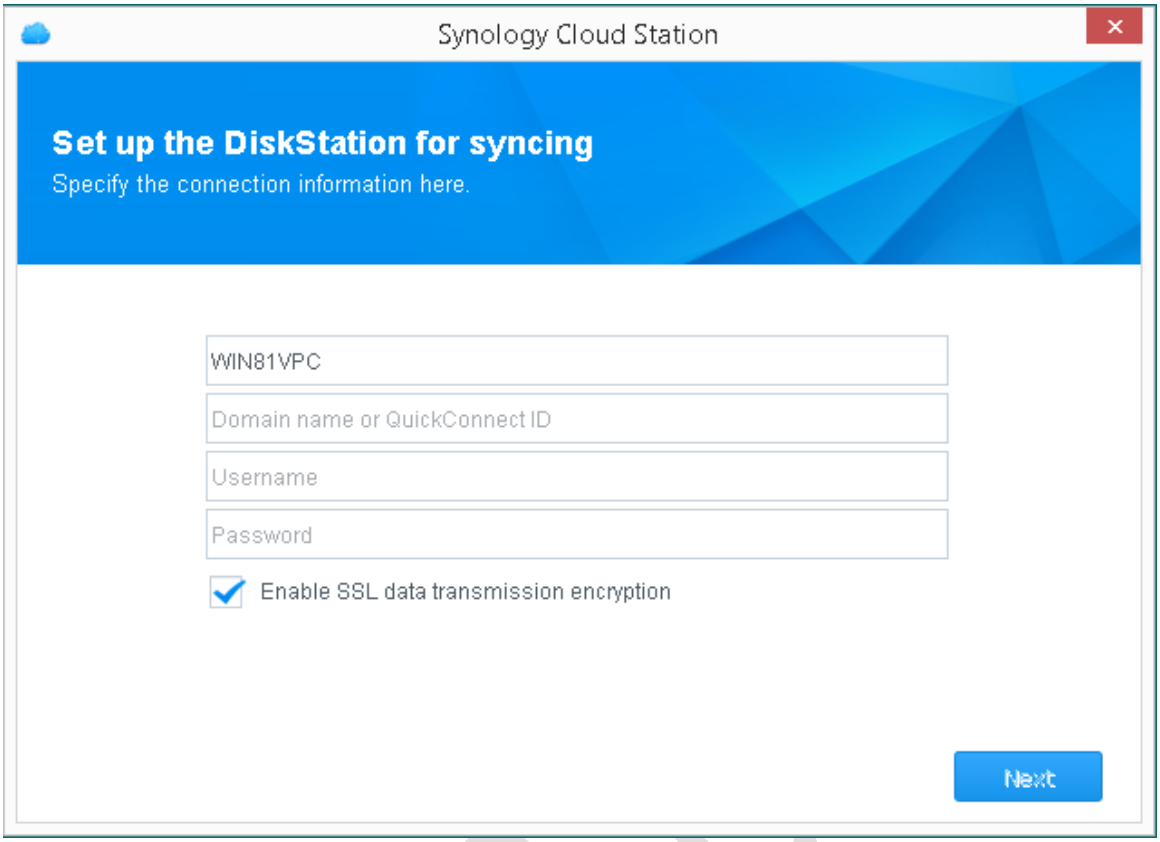

Figure 96: Enter details for Cloud Station

A 'SSL Certificate Warning' message may be displayed. This is fine, so just click the **Proceed Anyway** button. On the subsequent screen you specify the location of the folder to be synced; the defaults are fine so just tick the **Enable** box and click **Next**:

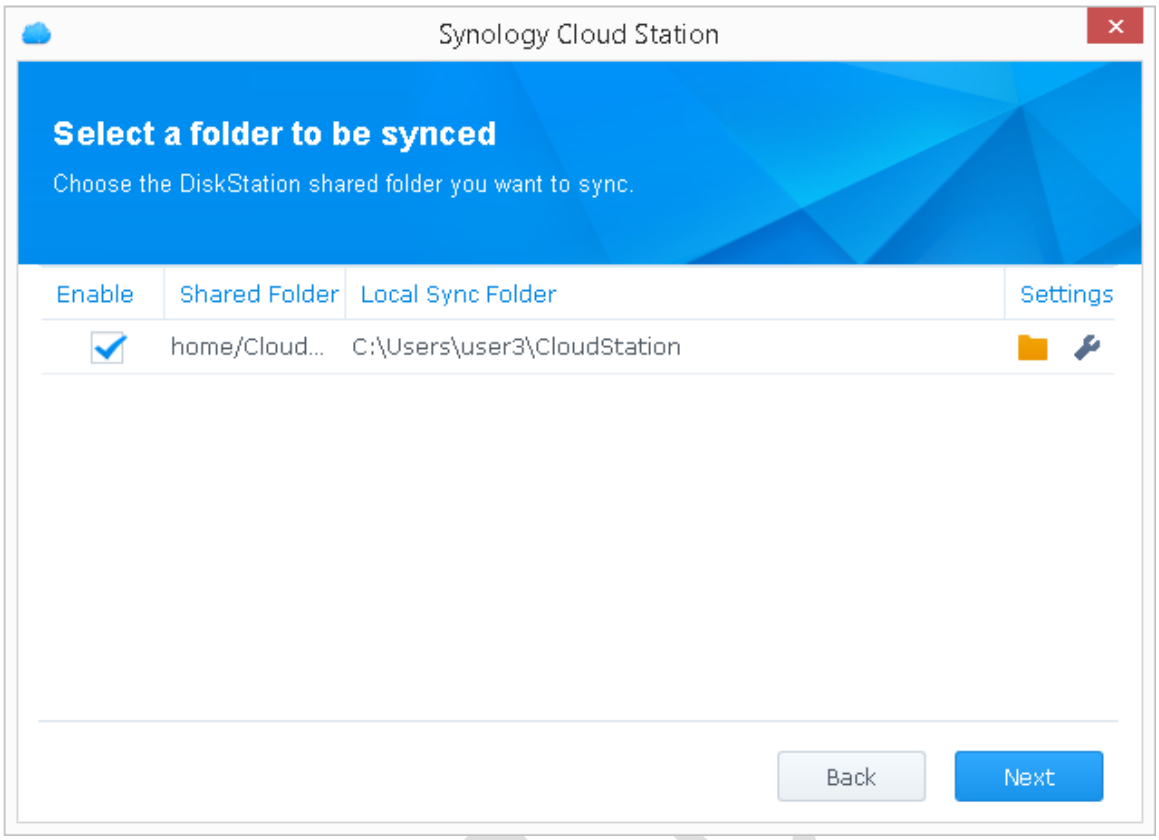

Figure 97: Select a folder to sync

A confirmation screen will be displayed – click **Finish** and the computer will commence syncing in the background. There will be an icon on the right-hand side of the computer's Task Bar that looks like a small cloud; click on it, choose **Settings** and click the **Sharing** tab. Make sure that the available folders are being shared and if any are not then tick the appropriate boxes, followed by **Apply**. This icon can also be used to access the CloudStation and shared folders; click it and choose **Open Cloud Station folder**:

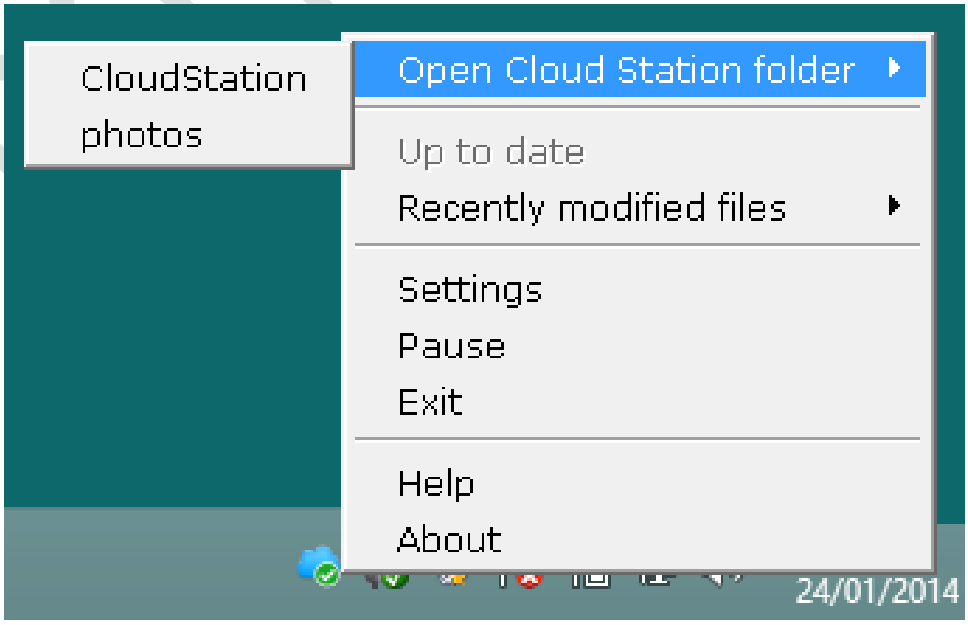

Figure 98: CloudStation utility

The CloudStation folder is actually located in the user's library on the computer, along with Documents, Downloads, Music, Pictures etc. One thing to note is that the Cloud Station folder is **not** the same as the user's home folder on the server. Rather, it is a sub-folder within the home folder.

9. Tidying Up, Miscellaneous and Security Topics

9.1 Anti-Virus Package

The chances of the server becoming infected with a virus are extremely low as it is based on a customised version of Linux and as such is not very susceptible. However, the files being stored on it by Windows computers and other clients may be infected and these are what need to be checked to prevent further distribution. Synology's "Antivirus Essential" is a free download from the Package Center and runs on the Server itself; separate provision needs to be made for the clients (e.g. using Microsoft Security Essentials, AVG, McAfee etc.) as there is no linkage between the two, nor is this intended as a replacement for security on the client workstations.

Having downloaded and installed the anti-virus package, an icon will appear on the Main Menu button. Click on it to display the Console:

Three types of on-demand scan are available and it is pretty self-evident what each does. By default, the latest anti-virus signatures will be downloaded before the scan commences (this behaviour can be changed from the **Settings** option).

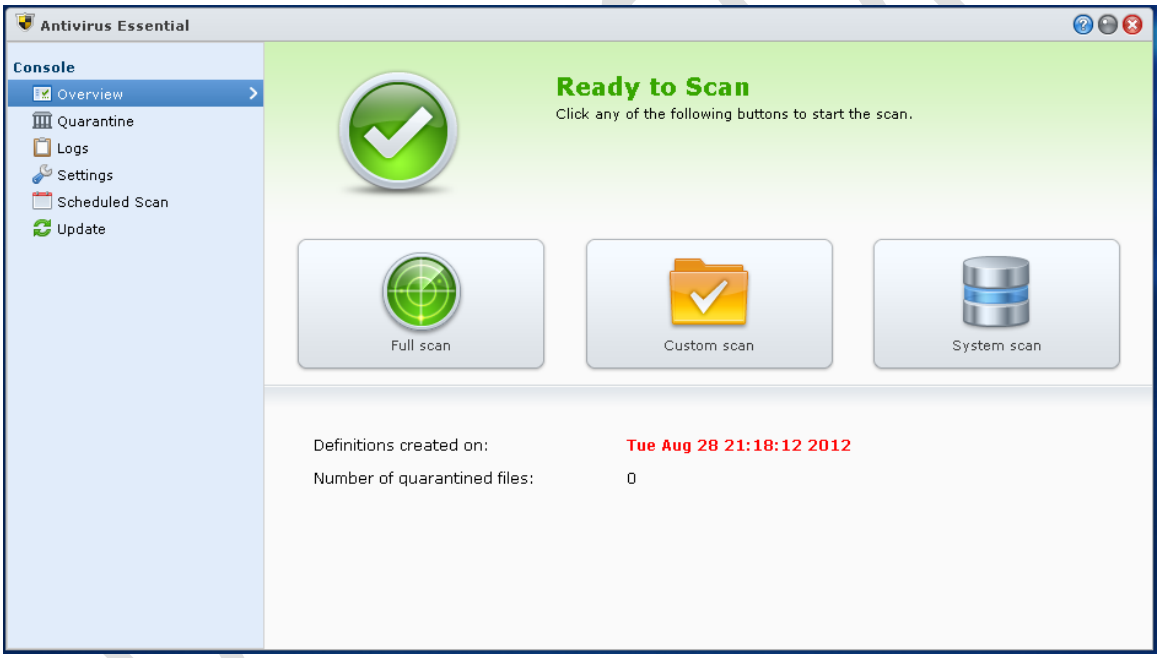

Figure 99: Antivirus Essential

Note that scanning can result in high CPU and memory utilisation and, depending on the amount of data stored, can be time consuming. For this reason, it is best done as a scheduled task out of hours, for instance during the middle of the night or at the weekend. To schedule a scan, click on the **Scheduled Scan** option followed by the **Create** button:

In this example, the DiskStation is set to do a full scan each weekend, starting at 1:30am.

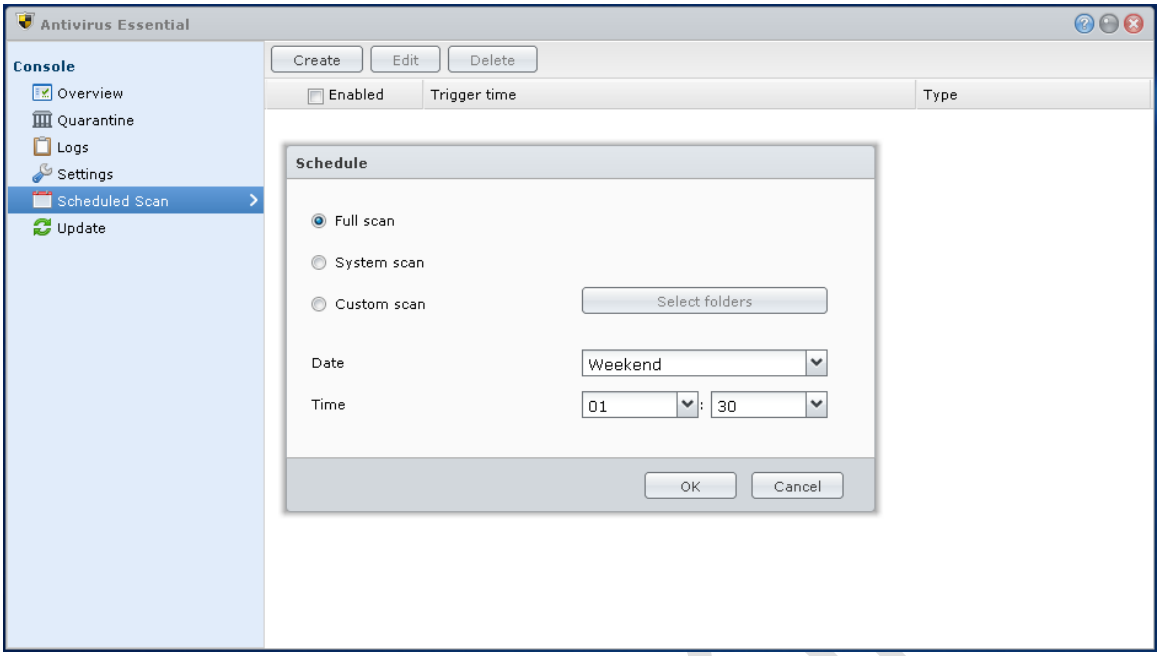

Figure 100: Antivirus Essential

Click on **OK** after setting up and make sure the **Enabled** switch is ticked.

9.2 Populating the Technical Folder

The Technical folder should be populated with items that will be of use in managing the network. To recap, earlier on we created four folders. These should be used as follows:

apps	Master copies of applications e.g. Office, educational programs. 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	Disk images of machines created using PING or Ghost.

9.3 Restore Old Data

Any data from the previous network or computer setup should be restored. 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 'catch all' folder and then redistributing it to the proper folders. Great care should be taken to avoid spreading any viruses from the old environment and the following approach is suggested:

- Copy the data from its original location(s) to an external USB drive of suitable capacity
- Plug the external USB drive into a standalone PC that is known to be clean and virus-free
- Run an anti-virus scan on the external USB drive
- When satisfied, connect the USB drive to the server and copy the data across
- Run a full scan on the servers

9.4 Logoff Shortcut

A desktop icon to logoff the user is a useful addition to a computer. To create one:

Right-click on the Desktop and choose **New** > **Shortcut**.

Type in: *C:\Windows\System32\shutdown.exe /l* and click **Next**
Name the shortcut 'Logoff' and click **Finish**
Right-click the newly created icon and choose **Properties**
Click **Change Icon,** choose a more appropriate icon and click **OK**. For example:

Figure 101: Logoff icon

The Logoff shortcut can usefully be placed on the Desktop next to the one for connecting the computer to the NAS.

9.5 Change Default File Save Location for Microsoft Office

If the computers do not leave the business premises, consider changing the default file save location for Word, Excel, and PowerPoint. Changing it from *My Documents* to *H:* will make life easier for users. The instructions vary depending upon the version of Office but is usually:

File > Options > Save.

9.6 Change DSM Logout Time

Being permanently logged in to DSM is not a good idea from a security perspective. To counter this, users are logged out automatically after a period of inactivity. Whilst this is a good thing, it can be inconvenient when people are working but also being interrupted to deal with other things. The amount of time for automatic logout can be adjusted; to do so, go into **Control Panel** and click the **DSM Settings** icon. On the **Security** tab the Logout timer can be set to any amount from 1 minute to 65535 minutes (about 45 days!). A sensible value might be, say, 30 to 60 minutes. Having made the change, click the **Apply** button.

9.7 Block Suspicious Login Attempts

Sometimes users forget their login details and are unable to access the server. On other occasions, people who are not entitled to use it (for instance, hackers) may attempt to do so, hoping that they can guess a valid username and password. To help reduce the risk of the latter, DSM can be set to lock an account if there are too many incorrect attempts at gaining access. To set this, go to **Control Panel** and click the **Auto Block** icon. On the **General** tab tick the **Enable auto block** box then click **Apply**. The default values of 5 login attempts within 5 minutes are suitable in most situations. It is strongly recommended that this is done.

9.8 Block DoS Attacks

A Denial of Service (DoS) attack is when someone or something on the internet tries to bring down a server or website by constantly bombarding it with traffic, causing it to crash or at least making it so busy responding that it cannot operate properly. There is a facility within DSM that provides some protection: go to **Control Panel** and click the **Firewall and QoS** icon. On the **Security** tab tick the **Enable DoS Protection** box then click **Apply**. It is strongly recommended that this is done.

9.9 Switch off Occasionally Used Services

As the server is connected to the internet, there is always a security risk that it can be attacked by external miscreants and hackers. One way to reduce the risk is to switch off services that are not used or are only used infrequently or under special circumstances. For instance, one particular company has a VPN to allow remote access, but it is only used two or three times a year when the accountant visits the branch office. At all other times of the year, the VPN Server is switched off.

10. Housekeeping and Reporting

The server should be monitored on a regular basis, say once a week or so, to check that there are no problems. Things that can be usefully looked at include:

- Check for DSM Updates (see below)
- Disk space
- Confirmation that the backup has completed successfully
- Logfile generated by anti-virus scan

Monitoring can be done in three, complimentary ways:

- By logging in to the server
- By using the Synology Assistant software
- By setting up automatic notifications
- Using the DS Finder app on a portable device such as an iPad

10.1 Logging in to the Server

Login as the admin user from any computer on the network. On the right-hand of the screen the overall status of the Server should be displayed; if it is not, click on the chevron in the bottom right-hand corner of the screen to display it:

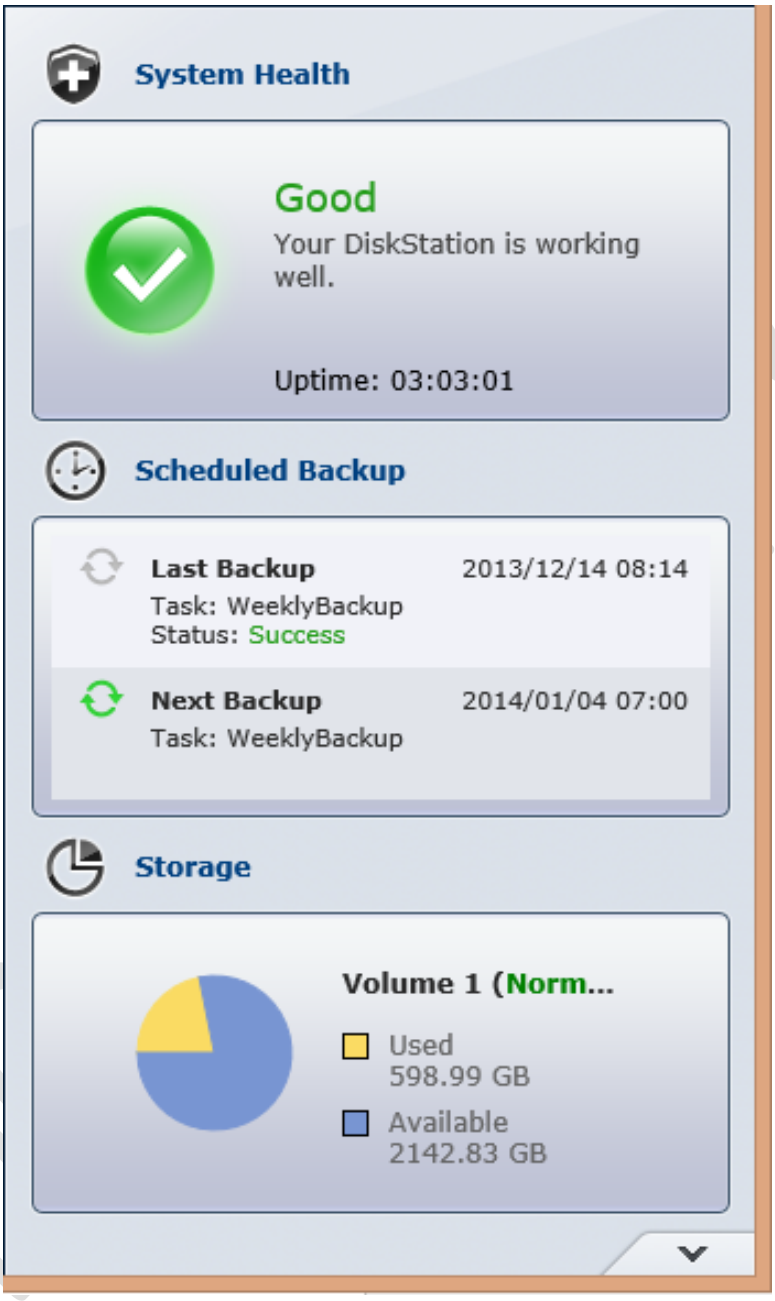

Figure 102: Server status

There are a selection of items that can be displayed and the number that can be shown at once depends upon the resolution of the screen and size of the browser window. To change an item, click on its name and choose another from the pop-up list. A good choice is: System Health; Scheduled Backup; Storage.

10.2 Using the Synology Assistant software

The Synology Assistant software is used when initially setting up a server but can do other things, including monitoring the system. For this reason, you may wish to leave a copy on one computer (for example your computer, if you are the administrator) for this purpose.

Launch Synology Assistant. There are three tabs: Management, Resource Monitor and Printer Device. Click **Resource Monitor**. Click the **Add** icon. A list of servers is displayed (although there would only usually be one of course); select it and click **Next**. On the following panel enter the password for the admin user (note that only the administrator can use this facility) and click **Next**. A confirmation screen is displayed ("Configuration report") – click **Finish**. On the resultant screen click the server and the panel should look as follows:

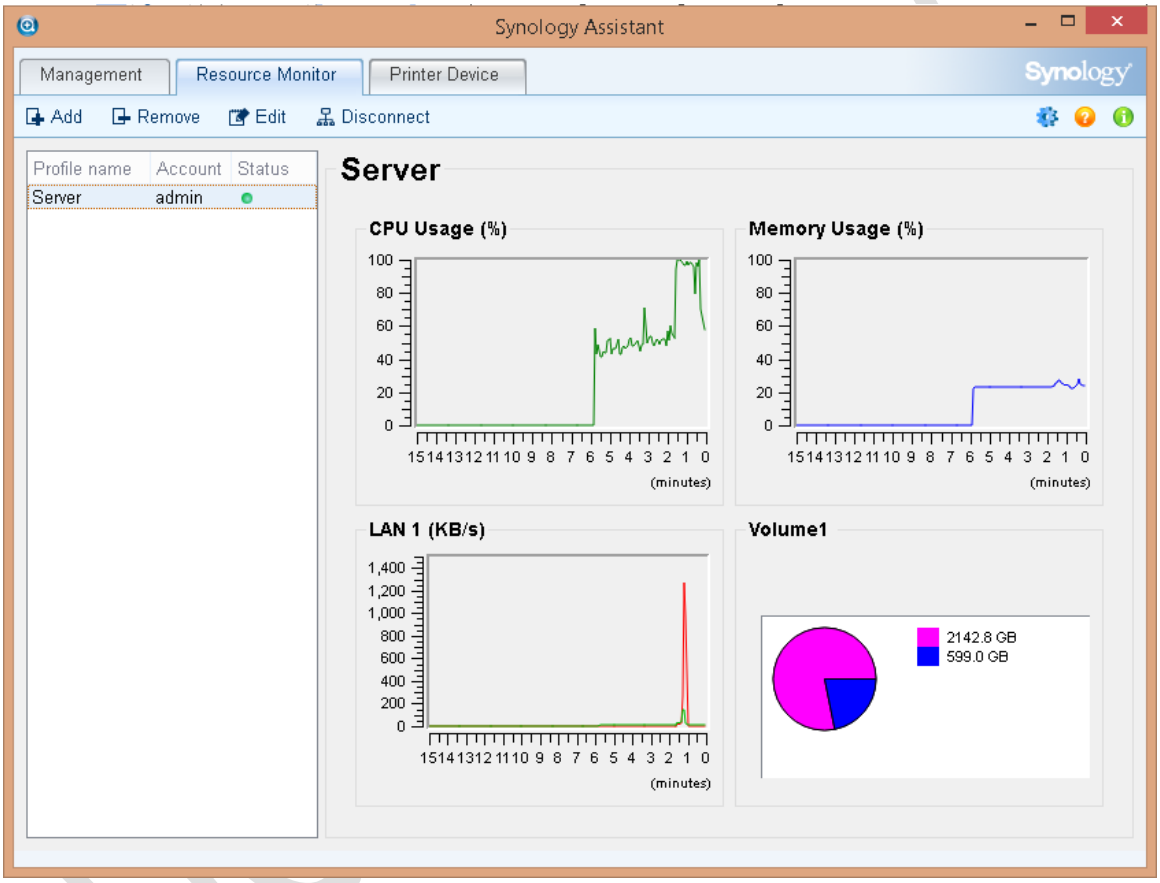

Figure 103: Server status

The information captured by the Synology Assistant is of use in checking the amount of available disk space and the overall performance of the server. It would be typically used, for instance, if users were reporting that the network appears to be running slowly or that file transfers are taking a long time.

10.3 Setting up Automatic Email Notifications

Whilst it is important to check the server on a regular basis, this is not always possible. For instance, the person who looks after the system may not be located in the office. Also, it is better to deal with some problems sooner rather than later. For these reasons, DSM can proactively advise when issues occur using automatic notifications sent by email.

To configure this go into **Control Panel** and click on **Notifications**. There are two tabs on the resultant screen; the General tab is for setting up email details and such and the Advanced tab is for specifying the events that generate notifications.

On the General tab there is a choice of notification by Email, SMS and Push Service (meaning Skype). Any of these can be used and they are not mutually exclusive. SMS (text messaging) uses the commercial Clickatell service and is not covered here. Anecdotally, Skype seems to be problematic, so it is suggested that email is used.

To setup email click on the **Email** icon:

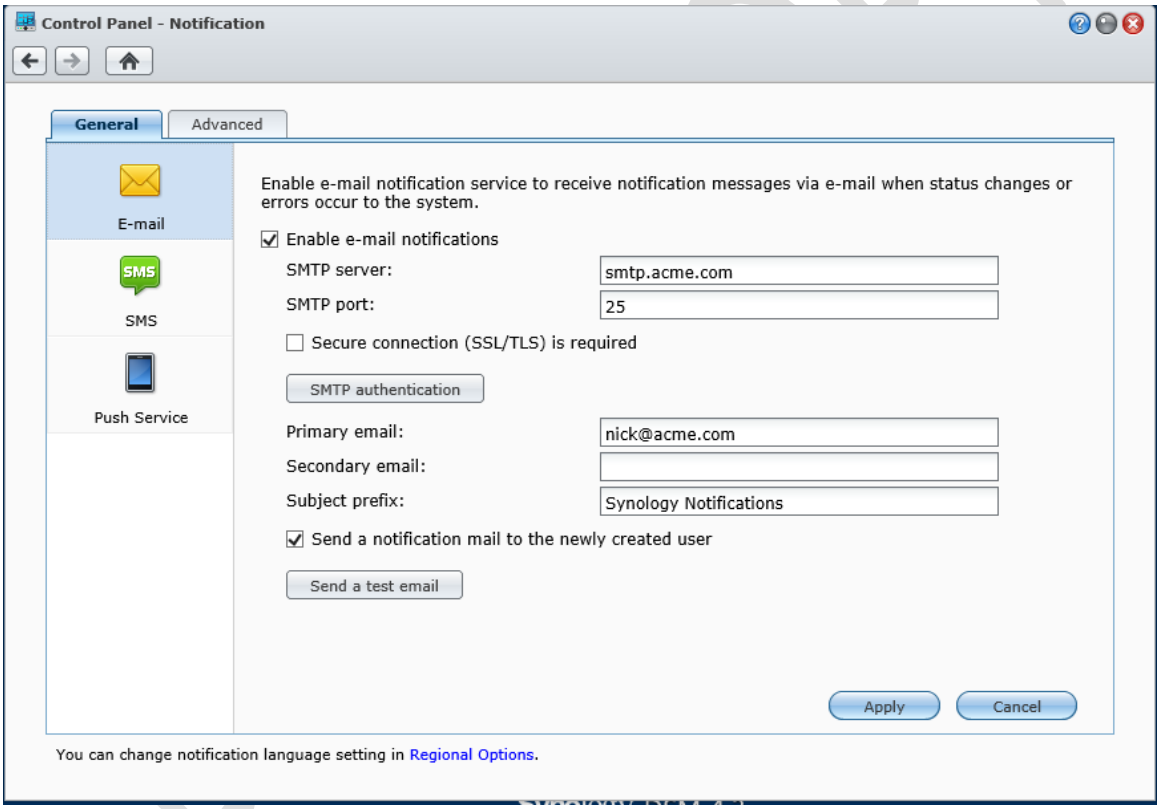

Figure 104: Email settings

A panel for email settings is displayed. Tick the box to enable email notifications. Enter the name of the SMTP server plus the SMTP port (usually 25 but check first). If a secure SSL connection is needed tick the relevant box. If SMTP authentication is required (it usually is) then click the button and enter the email user name and password (this must be for an existing account, such as your own). In the Primary email field enter the email address of the first recipient; if there is another recipient enter their email address in the Secondary email field. Enter the title for the notification emails in the Subject prefix field. To test that everything is working, tick the 'Send a notification to the newly created user' box and click the **Send a test email** button. Then click the **Apply** button.

To specify the events that are reported upon, click the **Advanced** tab to display the following panel:

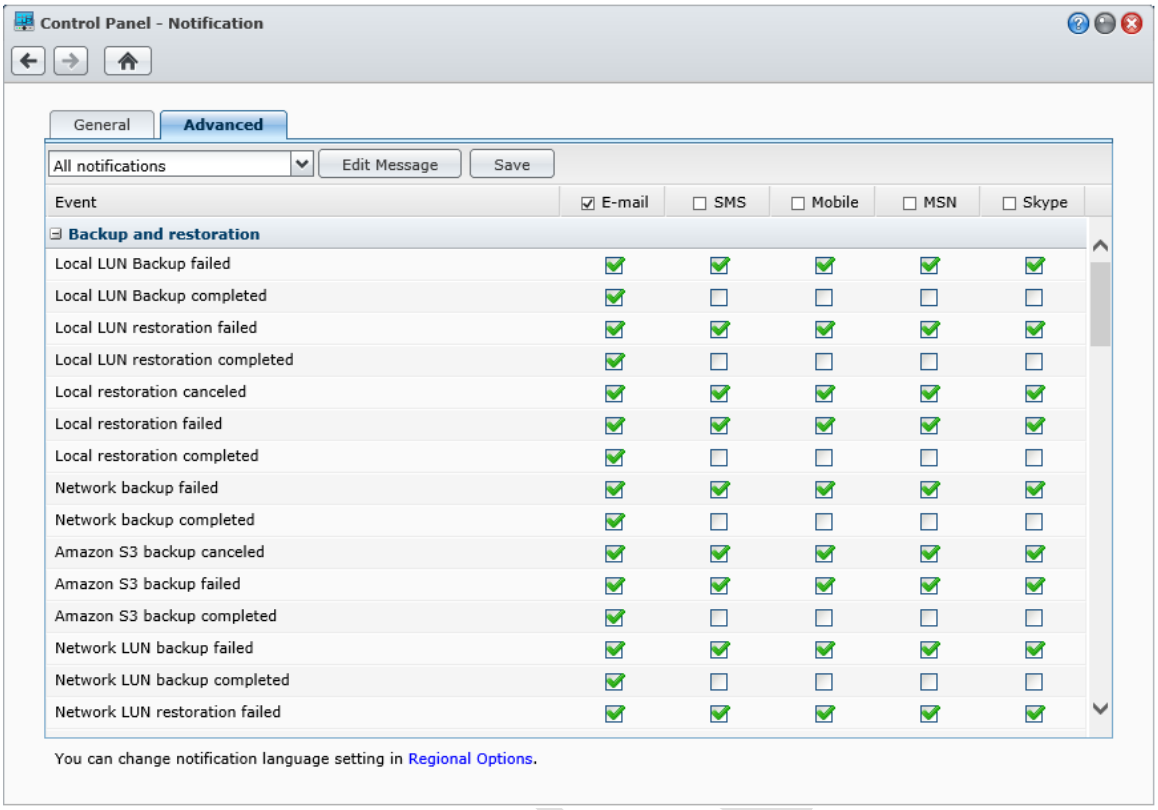

Figure 105: Specify the notification events

There are dozens of different potential notifications that can be generated. However, in a typical small business many of these will be of little relevance. The notifications are grouped into seven categories; towards the top left-hand of the screen is a drop-down box that allows the category to be chosen. Alternatively, leave the drop-down on 'All notifications' and add or remove the tickboxes against the individual items. Make sure that the E-mail box at the top of the screen is ticked before beginning this process. The other columns – SMS, Mobile, MSN and Skype – should be left unticked and if this is done then the individual settings for those columns will be ignored. When finished customising, click the **Save** button.

10.4 Using DS Finder on a Mobile Device

Available for iOS, Android and Windows Phone, *DS Finder* is a comprehensive app for monitoring the status of the DiskStation, including such things as disk space, technical and network information. It can monitor server events and generate email status reports. On the iPad it can be switched to a full screen view within Safari, called DSM Mobile, that allows more comprehensive information and control

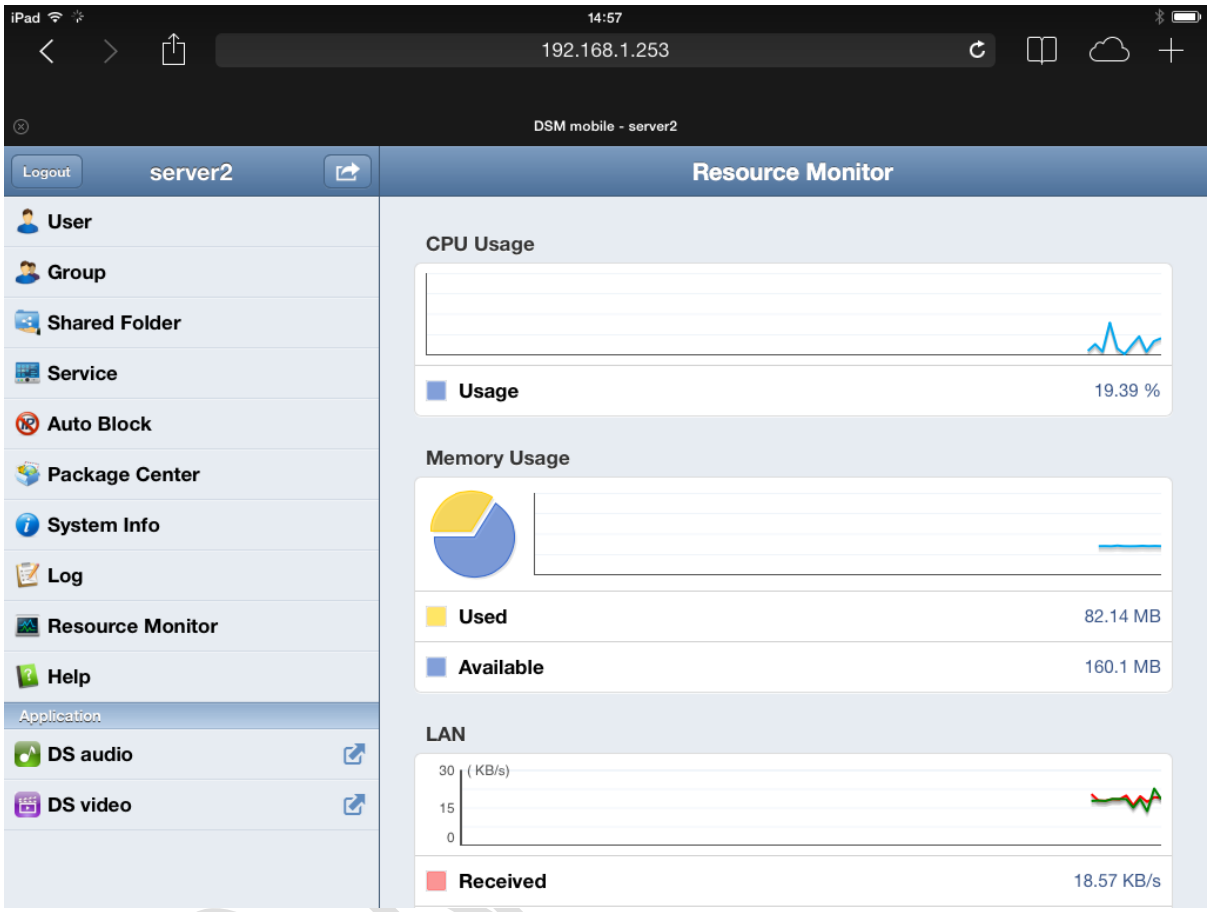

Figure 106: DS Finder on the iPad

10.5 Checking for DSM Updates

The DSM software is updated on a regular basis by Synology. Updates may be major e.g. from DSM 4 to DSM 5, although typically these only occur every couple of years. Significant updates e.g. from DSM 4.2 to DSM 4.3 are more frequent, typically every 6-9 months. Additionally, there are more frequent updates to fix problems and these are made available by Synology in a more frequent manner. DSM can be configured to automatically check for updates; however, it is suggested that it is done manually instead so as to avoid any surprises.

To check for updates, launch **Control Panel** and click the **DSM Update** icon. Make sure that **Check and download update** is not ticked; regardless of this setting, it will still advise if an update is available anyway but not download and install it automatically. To check if an update is of relevance, click on the **What's New** link and/or look at the various Synology forums available on the internet. If the update is required, click the **Download** button. Once the download is complete, the button will change to read **Update Now**. As updates invariably require a reboot of the system it is suggested that they are done outside of normal working hours.

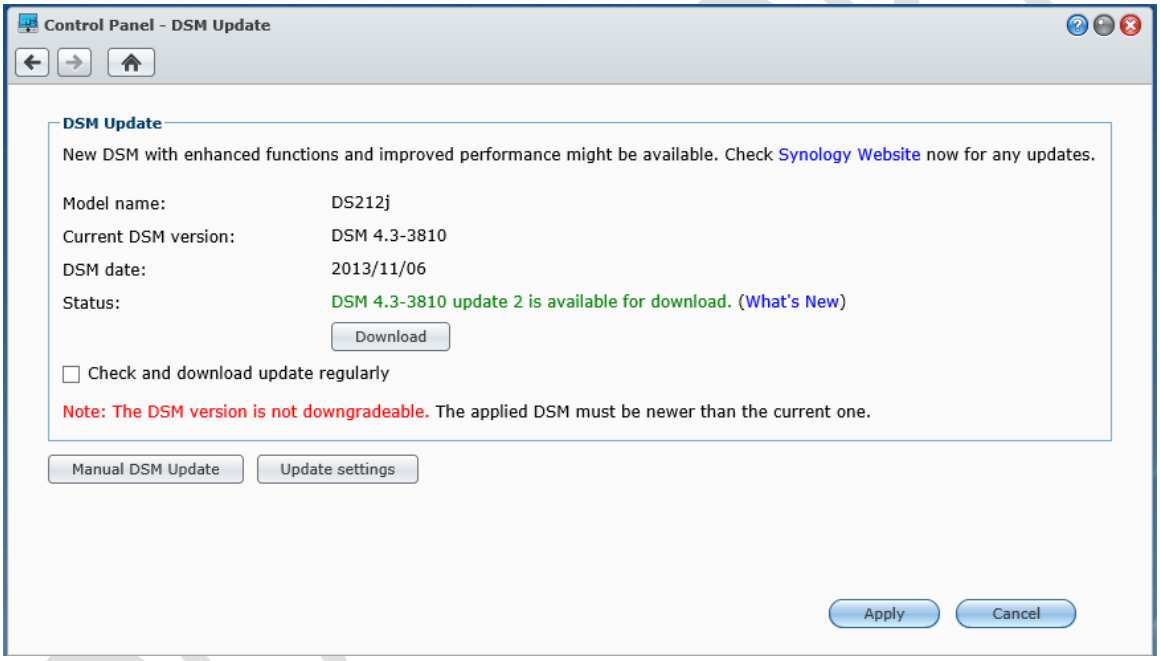

Figure 107: Check for DSM updates

10.6 Scheduled Disk Checks

Click on the **Main Menu** icon. Click on **Storage Manager**. Click on the **HDD Management** tab. Click the **Test Scheduler** button followed by the **Create** button. Give the task a meaningful name (e.g. *Test HDDs*) and select **Quick Test** and **Test all disks**.

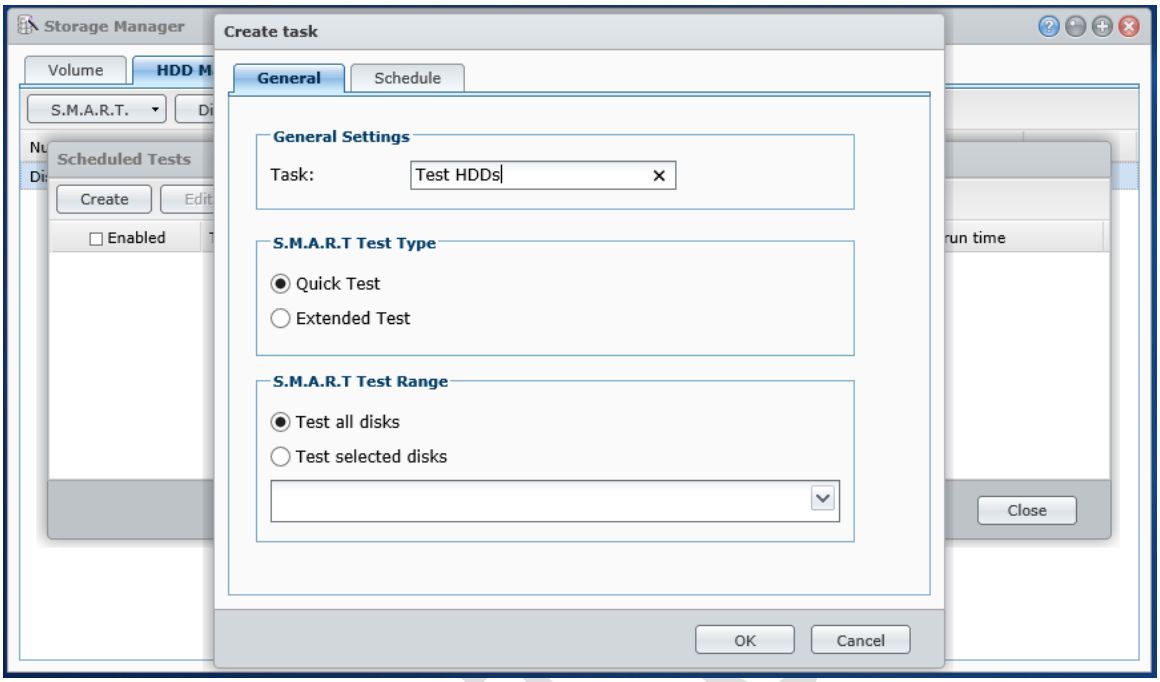

Figure 108: HDD check

Click on the **Schedule** tab. Setup a suitable schedule e.g. run every weekend at 8.00pm, then click **OK**:

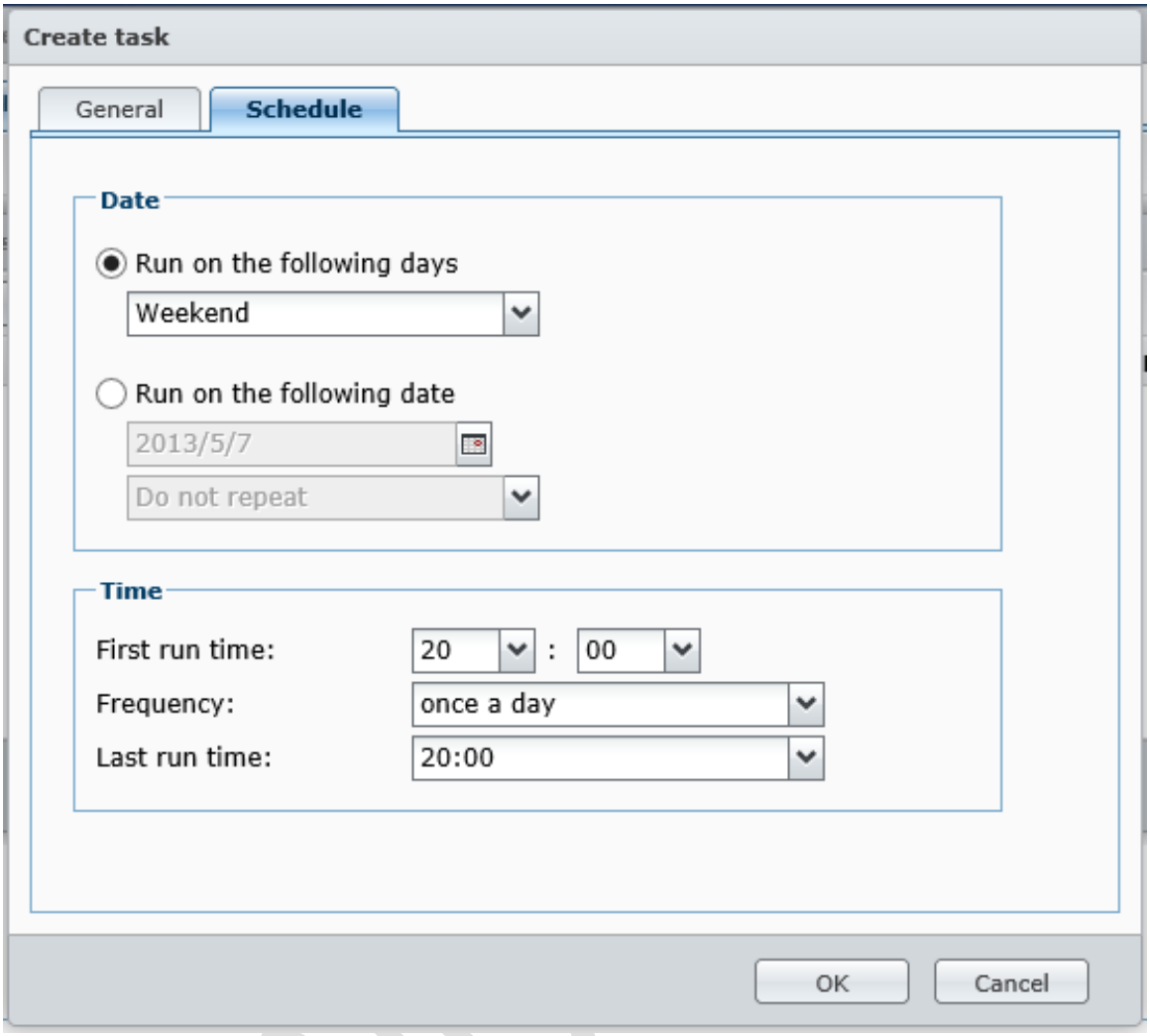

Figure 109: Scheduled HDD check

11. Connecting iPads and Other Mobile Devices

IPads, other tablets and Smartphones are widely used and people expect to be able to use them to access their business data. To this end there are numerous apps available to connect such devices to the Server. Many of these apps are aimed at home users, at people who want to stream music and videos and view photographs. However, there are several apps that provide direct access to the filing system. They cannot easily be used in the same way as a computer with the ability to create and edit documents, mainly because tools such as Microsoft Office are not available on the iPad. However, they can provided read-only access to the files, enabling users to view documents and such.

There are several apps available to do this:

DS File is a free download from Synology. In order to use it, the WebDAV service has to be first enabled on the Server; to do this, launch **Control Panel**, click **WebDAV** and check the **Enable WebDAV** tickbox. After launching DS File, the address of the server and the logon details have to be specified. It is then possible to navigate the filing system and view documents. They can also be downloaded to and from the iPad.

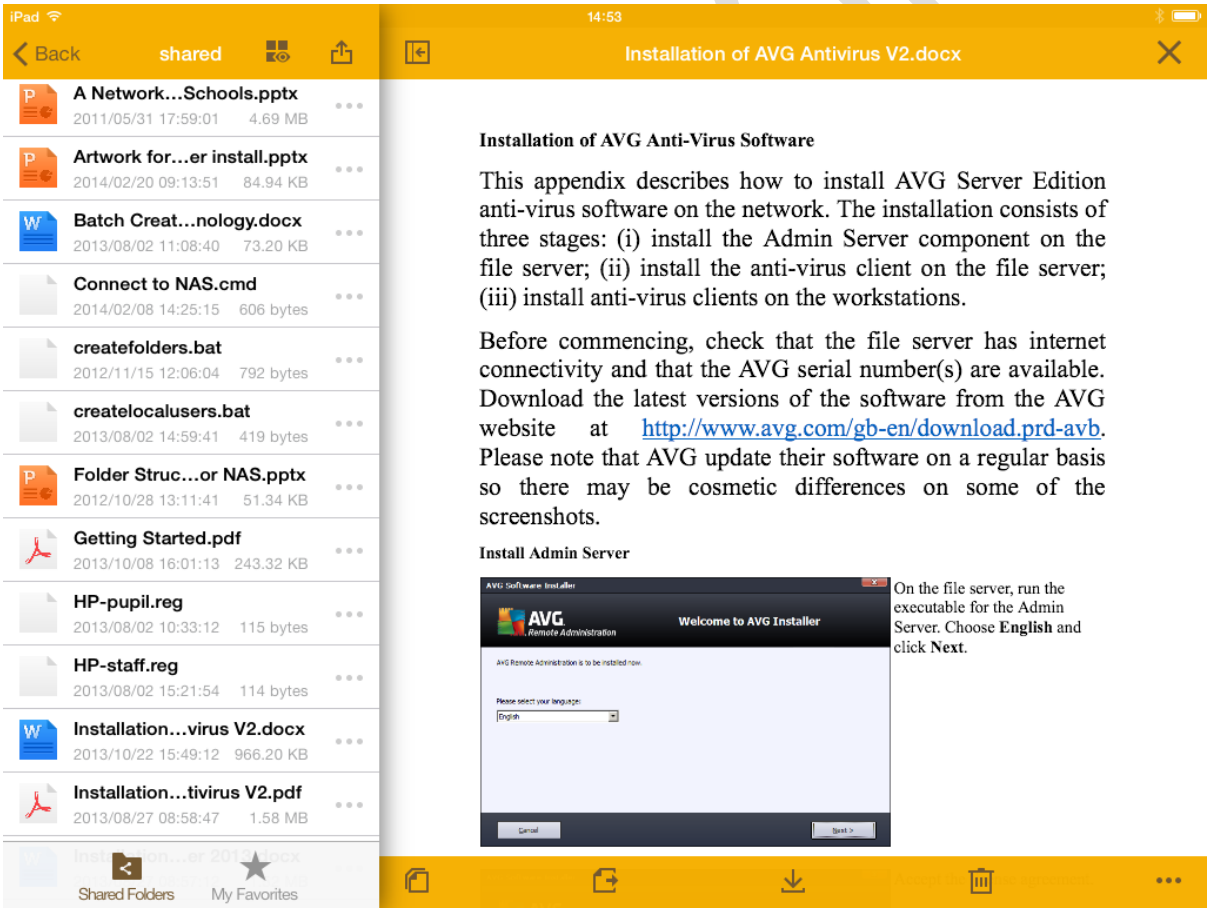

Figure 110: DS File on the iPad

File Browser from Stratospherix is an inexpensive commercial alternative. It is broadly similar but with additional features, plus has the ability to integrate with OneDrive (formerly SkyDrive) and Dropbox.

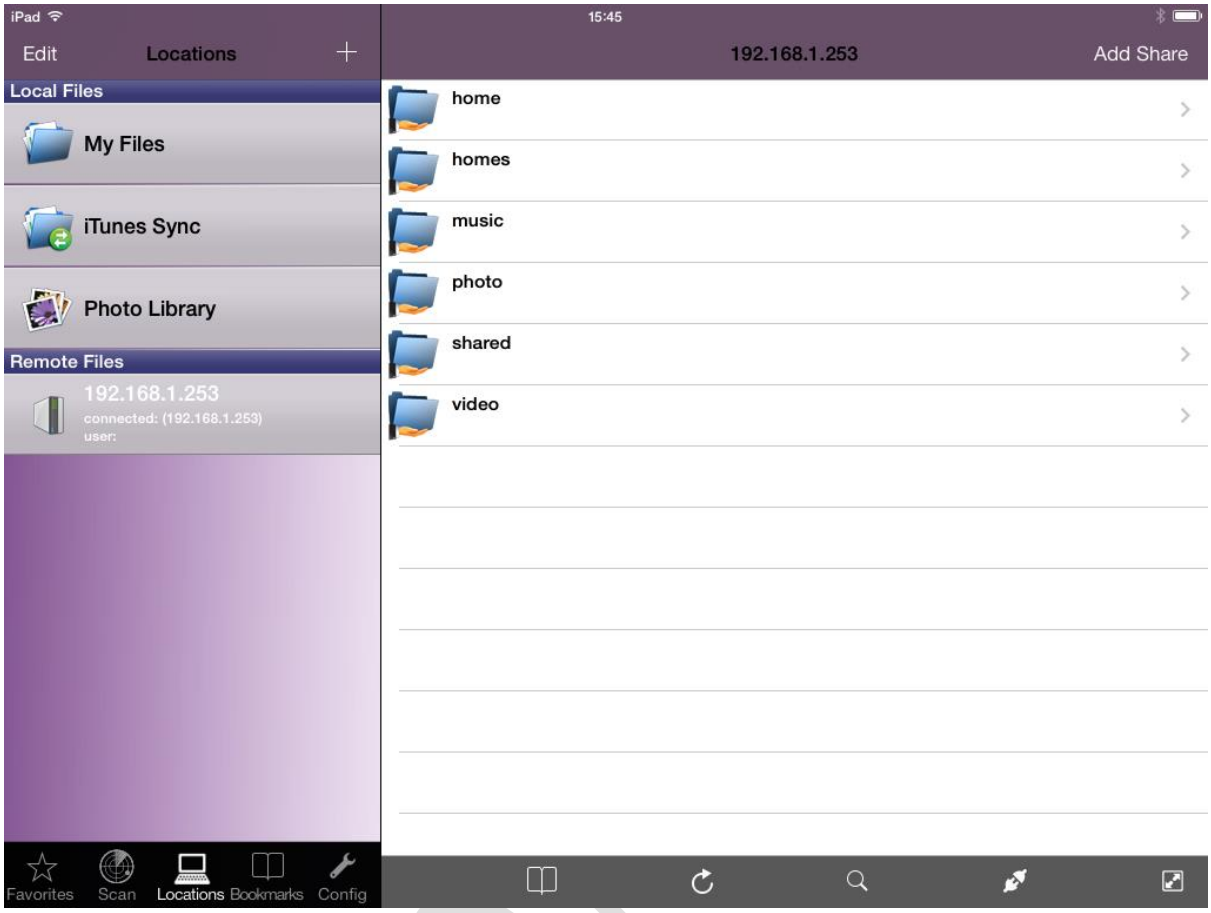

Figure 111: File Browser on the iPad

12. Additional Packages for the DiskStation/RackStation

Whilst the DSM operating system has a huge amount of useful functionality built-in, it is possible to extend it further through the installation of free, optional packages. Some of these have already been discussed – specifically the anti-virus package and Cloud Station – but many others are available. Some of these have been developed by Synology, others have been supplied by third parties.

To review what is available, click on the **Package Center** icon located on the DSM Desktop to display the following screen:

Figure 112: The Package Center

At the time of writing over 50 packages are available, broken down into the five categories of: Backup; Multimedia; Business; Security; Utilities. Some of these address very specific requirements; for instance, the multimedia packages are mainly likely to be of interest to home users wishing to stream video and music. Within the business category, the following ones are available among others and may be of some interest:

Mail Server	Enables an organisation to run its own email system
OpenERP	Includes Sales, CRM, Project Management, Warehouse management, Manufacturing, Accounting and Human Resources
OrangeHRM	A Human Resources management system
osTicket	A ticketing/helpdesk application
SugarCRM	Customer Relationship Management application
Zarafa	An alternative to Microsoft Exchange that provides email, calendaring, collaboration and tasks

Thank you!

We hope that you have found this guide helpful and interesting. Supplementary and supporting information can be found at the following website: www.serverinstallationguides.co.uk

If you have any suggestions or have found areas for improvement, please let us know at enquiry@ctacs.co.uk