Windows Server 2012 R2 Essentials Installation Guide for Small Businesses

Also covers Windows Storage Server 2012 R2 Essentials

Nicholas Rushton, BA Hons.

Callisto Technology And Consultancy Services

11th Edition © 2013-2020

11th Edition Revised. Updated August 2020

Copyright © Nicholas Rushton, 2013-2020

Table of Contents

COMMENTS & REVIEWS FROM OTHER PURCHASERS

You are in good company - thousands of people have used guides from CTACS to help them setup their home and business networks. This is what purchasers of the *Windows Server Essentials Installation Guide for Small Businesses* have written in their reviews:

"Very detailed instructions which allowed me to setup my new server. Something I've never done before."
– Southpaw

"Great book! This led me step by step through setting up my new server. I have very little IT experience and have never worked with servers or networks before. Highly recommended this book to any neophytes like myself. Please do everything exactly as he suggests. The only problems I had was when I did not carefully read his instructions." - WDE

"Outstanding little book. Gets right to the basics to install and use Windows Essentials. Highly recommended." - A COBOL Guy

"If you are a small business IT provider, then you need this book." - King P

*"Setting up my first server and this book is easy to follow, understand, and put into actual practice.
I highly recommend it to anyone setting up their first server."* - CM

"We replaced the Windows Small Business 2003 server at our small church with a new server running Windows Server Essentials. I volunteered to do the migration even though I had very little experience with servers. This e-book was an excellent starting point. I read through it before starting the job and referred back to it many times during the process. It was instrumental in the successful setup of the new server." - Kathleen Z

"Very easy to read and very informative." - MAH

"Excellent book - Just set up a Windows Essentials server using this book with excellent results. Well worth the money." - Earl A

About the Book

Microsoft's Windows Server 2012 R2 Essentials ("*Essentials*") and Windows Storage Server 2012 R2 Essentials ("*Storage Server*") are versions of Windows Server designed for use in small businesses and home offices. Microsoft's definition of a small business is one with up to 25 employees; as over 90% of business employees work in such companies the potential market for Essentials is absolutely huge. This guide has been produced because: (a) Essentials is not supplied with a proper manual; (b) there aren't many books available on Essentials; (c) the books that are available tend to be quite technical with hundreds and hundreds of pages. Such books may be useful as reference works for IT professionals, but can fall short as straightforward guides for simply getting Essentials installed and up as running in the minimum amount of time. In contrast, this book has been written according to the Goldilocks Principle – not too little information, not too much information, but just right! It is based on real world experience and using it, a person with a keen interest and a reasonable amount of IT knowledge should be in a position to install Essentials successfully. Indeed, many hundreds of people have done precisely that using this book.

The book is organized as follows:

Chapter 1 gives an overview of Essentials and describes the components of a network. Chapter 2 describes how to install the Essentials software and get the server up and running and introduces the Essentials User Interface or *Dashboard*. How to create users and shared folders is described in Chapter 3. Connecting devices such as desktops and laptops is the topic of Chapter 4. How to backup the server to cope with problems is important and is covered in Chapter 5, whereas Chapter 6 is about printing. The various techniques for accessing the network remotely are covered comprehensively in Chapter 7, including mobile devices in Chapter 8. Housekeeping and maintenance are covered in Chapter 9. Exercising greater control over the network is covered in Chapter 10, using Group Policy. Microsoft's Office 365 service is a popular addition to Essentials and is discussed in Chapter 11. Finally, Chapter 12 covers a range of miscellaneous and sometimes more advanced topics.

About Windows Server 2012 R2 Essentials

SBS went through several iterations over the years, in line with changes to the main Windows Server product at its core. The earliest versions were based on Windows NT 4.0; they were succeeded in turn by SBS 2000, SBS 2003, SBS 2003 R2 and SBS 2008. With SBS 2011, Microsoft changed tactics; besides the regular SBS 2011 Standard product, they also launched a new version called Windows SBS 2011 Essentials. This stripped out products such as the Exchange email server, on the basis that many small businesses now outsource their email to cloud-based services such as Google's Gmail or Microsoft's own Office 365 offering. Shortly thereafter, the SBS moniker was dropped altogether and Essentials became the main small business offering. This was updated in turn to Windows Server 2012 Essentials, which is now at the R2 version.

Given that *Essentials* no longer includes products such as Exchange, SQL Server and SharePoint, one obvious question is: What differentiates it from Microsoft's regular Windows Server products? The answer is that it is lower cost, has simplified licencing requirements but is restricted to a maximum of 25 users and 50 devices, whereas corporate versions of Windows Server can be expanded to cope with many thousands of users. *Essentials* also features something called the *Dashboard*; this originated in Microsoft's orphaned Windows Home Server line and provides a simplified, easier method of setting up and managing a server. It is this combination of price and simplicity that makes Windows Server 2012 R2 Essentials such a compelling proposition for many small businesses.

About Windows Storage Server 2012 R2 Essentials

Storage Server and *Essentials* are the same basic product and do the same thing; as such 99% of this guide applies equally well to both (any differences are highlighted). The key difference is that *Essentials* is an item of software that can be purchased and then installed on any suitable computer, whereas *Storage*

Server is only available pre-loaded onto a storage appliance or NAS box, such as those manufactured by *Thecus*.

About the Author

The author has worked in IT for over 30 years, on systems of all sizes and types throughout the world, from the largest companies to the smallest. Towards the end of the 1990's Microsoft released a product called Small Business Server ("*SBS*"); this comprised versions of Microsoft's main corporate networking applications (Server, Exchange, IIS, SQL Server) priced and packaged in such a way that it could run on a single file server. Shortly thereafter he became involved with a number of business start-ups and SBS was an ideal fit in many cases. A lot of his professional interest since then has been with small businesses – including running several of his own – giving him a vast amount of experience on small business IT. He currently runs his own independent consultancy.

Problems with the Artwork?

Pictures and illustrations can sometimes be problematic with eBooks. If you would like a free printable PDF file containing all the illustrations, just forward a copy of the email confirmation you received from Amazon when you bought the book to ctacs@outlook.com (please make sure there is no personal financial information in your email).

1. HARDWARE AND INFRASTRUCTURE

1.1 Overview

A typical small network or infrastructure is depicted below. The key components are:

Server - this is the heart of the network, which runs Essentials and upon which the data is stored
Backup device – for example, an external USB drive connected to the server
Internet connection - this may be a separate router or an all-in-one wi-fi router
Switch and Wireless Access Point(s) – to provide expansion in larger networks
Printer(s) – may be networked or plugged into the server with a USB cable
Desktops PCs – running Windows Professional, connected using Ethernet or wirelessly
Laptops, tablets and smartphones – connected wirelessly

Whilst it may not match your own setup exactly, it should be broadly similar. Further information about the components is given underneath the diagram and/or in later sections of the guide.
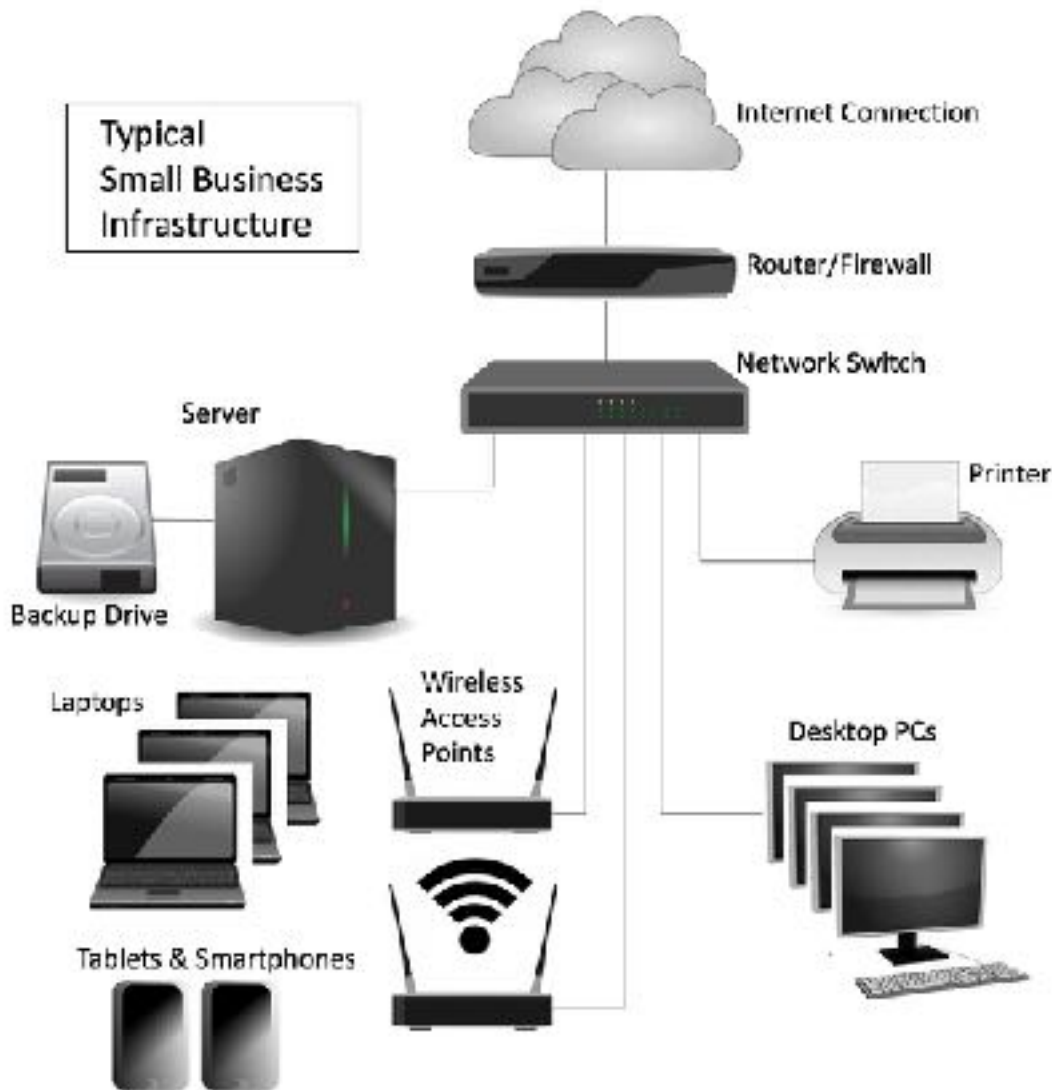

Figure 1: Typical small business infrastructure

1.2 The Server

Essentials requires its own, dedicated file server. A file server is similar to a normal desktop computer but is designed to hold multiple hard disk drives for additional storage and to be more reliable as it is intended to be powered up continuously. The main suppliers of file servers include Dell, HP, Lenovo, Fujitsu and IBM; other brands are available, but you may wish to avoid obscure manufacturers and unbranded machines. File servers are not usually available in retail stores but are obtained from specialist IT dealers or online. If you are learning about *Essentials* and do not happen to have a spare server to hand, you can use virtualization software on most modern computers to run a copy in a closed environment (a good, free product that runs both on PCs and Macs is Oracle's *VirtualBox*).

Choosing a server can be daunting, particularly as it is not something that a small business is likely to buy very often (the typical replacement cycle for a server being around 5 years). Given the specialist nature of the topic, you may wish to seek professional advice if you are not experienced in such matters. The following suggestions are guidelines only to help get you started:

- Spend as much as you can afford.

- In general, memory contributes more than processor power. So, you would usually be better off spending your money on more RAM rather than a marginally faster processor.

- Multiple disk drives are desirable as they enable increased capacity and performance. If you have at least two drives they can be configured to provide redundancy in the event of problems (referred to as *RAID*, this topic is discussed in the next section).

- File servers do not use the regular hard drives found in desktop PCs and laptops. Instead, higher-quality drives with improved performance and increased reliability (improved MTBF or *Mean Time Between Failures*) are preferred. Such drives may have standard SATA interfaces or SAS interfaces (better, but may not be supported in lower-cost servers). Examples of such drives include: Seagate Enterprise Performance; Seagate Enterprise Capacity; WD Gold; WD Re. As might be expected, these hard drives are more expensive than desktop ones.

- Most servers have more than one network adapter. This enables them to share the workload, providing better throughput, or provide redundancy in the event of one failing.

- Some servers have or have the option of redundant power supplies – if one fails then the other one takes over automatically. This is worth having.

- Servers are available in both tower format (similar to desktop PCs) and in horizontal rack format, for mounting in cabinets alongside other equipment such as communications equipment and network switches.

- Often the given base price for a server is for a bare-bones model and hard disk drives, memory and other features may have to be specified separately. Costs can add up – a complete system may be several times the initial headline price, so budget accordingly.

- Consider taking out a maintenance agreement at the time of purchase. These vary in service levels and price and your choice will depend upon your requirements, but generally they provide peace of mind and good value. The key decision point is: How long can you do without the server? It is possible to obtain maintenance agreements that provide an onsite presence within 4 hours.

For a very small business or other organization with less than ten staff, a suitable choice may be a *micro-server*. This is a proper server rather than just a glorified PC, but in a small, low-cost form factor. The genre was largely invented by Hewlett-Packard and their Proliant MicroServer series is very popular. An equivalent model from Dell is the T30

Similar to microservers are the NAS boxes that come pre-loaded with *Storage Server*, such as those manufactured by *Thecus*. These have *Storage Server* loaded on a smallish hard drive or solid state drive (SSD), but it is still necessary to purchase one or more hard drives for data storage as discussed in the following section.

Note that it is not necessary to purchase a monitor, keyboard and mouse for the server, as it can be operated without them (so called *headless operation)*. Borrow them from another machine for the initial installation, as thereafter they are not required.

1.3 Disk Drives and Storage Options

Most desktop and laptop computers have one physical hard disk, configured as a single volume (commonly referred to as "the C: drive"), upon which everything is stored. However, in a server there is usually a need for a greater amount of storage, plus that storage also has to be very reliable. Performance becomes a consideration too, as many people may be accessing the server simultaneously. The way to address these issues is by using multiple hard drives and to configure them in special ways. There is no single one-size-fits-all solution here, as it depends upon the size, requirements and budget of the organization. The options are reviewed below.

Single Drive System

A server in a very small business environment may only have a single physical hard drive. In such a case, it should be divided into two volumes: a volume on which the operating system is installed (the C: drive) and a volume on which the organization's data is stored (the D: drive). The rationale here is that if the operating system ever needs to be re-installed or upgraded, then it can be done without directly affecting the data. The C: volume does not need to be huge – 60GB to 100GB is quite adequate and the remainder of the drive should be partitioned as the D: drive. The major downside to a single drive system is that in the event of it failing then the server will be out of action until it can be replaced, plus the associated risk of data loss is high.

Twin Disk Drives

A very natural solution for Essentials is to have two hard drives in the server, one for the operating system and one for the data. The first one can be quite small; at the time of writing, the smallest readily available drives are 160GB, which is ideal. The second drive, for the data, can be as large as you want. This arrangement gives some performance benefits, as the drives operate independently, sharing the workload, plus the operating system and data are quite separate, which facilitates re-installations and upgrades. However, it still does not address the issue of reliability or protection.

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 etc. The basic idea is to improve reliability and performance by using multiple disks to provide redundancy and share the workload. The most common scenarios in small server systems are RAID 0, RAID 1, RAID 5, RAID 6 and RAID 10.

RAID 0 consists of two identical drives. When a file is written, some data goes on one drive and some goes on the other. As both drives are being written to (or read) simultaneously, throughput is maximised. However, as bits of files are scattered across the two drives, if one drive fails then everything is lost. Also, the speed of disk drives is not necessarily the bottleneck in many servers. For these reasons RAID 0 should be avoided, as it offers no protection at all, but is described here for reasons of consistency.
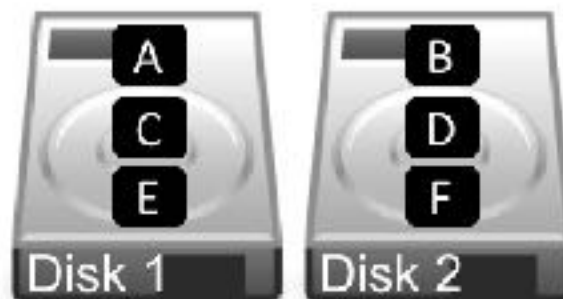

Figure 2: RAID 0 – Data striped across two drives

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 is then synced so it becomes a true copy of the remaining healthy drive in 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 server has two 2TB drives installed then the total amount of usable storage capacity is 2TB rather than 4TB.
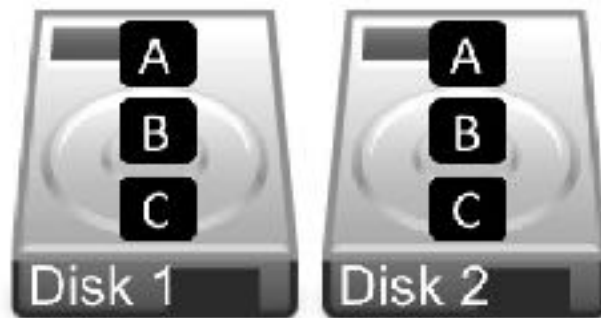
Figure 3: RAID 1 – Data mirrored across two drives

RAID 5 uses at least three but preferably four or more drives. Data is written across all the drives simultaneously, 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 in order to provide resilience, RAID 5 loses only about 25%. For instance, if a server has four 2TB drives installed then the total amount of usable storage capacity is 6TB rather than 8TB.
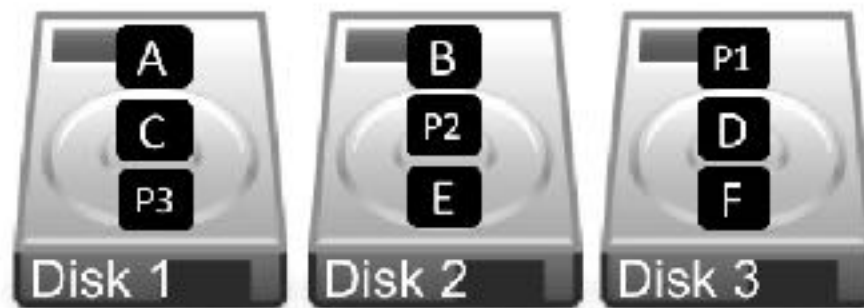
Figure 4: RAID 5 – Multiple drives with parity information

RAID 6 uses at least four but preferably five or more drives. It is similar to RAID 5, but uses two sets of parity information written across the drives. The benefit of this approach is that the system can cope with the simultaneous failure of two drives, thereby making it more resilient than RAID 5, although it loses more capacity in order to provide that resilience. If a server has five 2TB drives installed in a RAID configuration then the total amount of usable storage capacity is 6TB rather than 10TB.
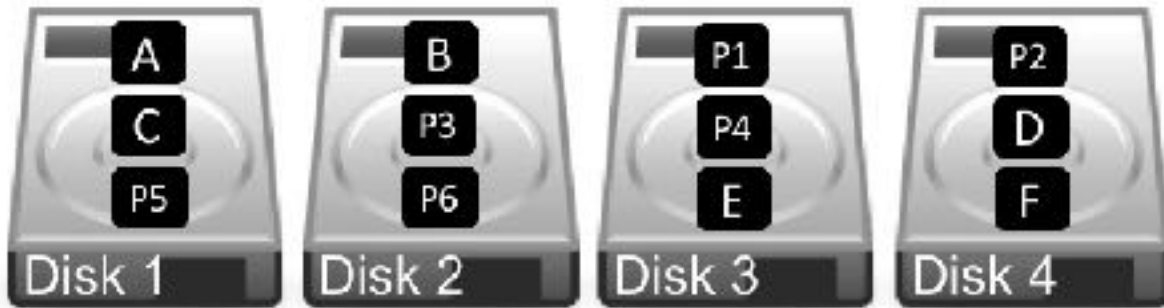
Figure 5: RAID 6 – Multiple drives with double parity information

RAID 10 (also known as RAID 1+0) combines RAID 1 and RAID 0 techniques. Requiring a minimum of four drives, it comprises a pair of RAID 1 mirrored drives, with data being striped across the pair in the way that RAID 0 operates. It thus combines both redundancy and performance, making it of particular interest where high throughput in needed, for instance in demanding applications such as video editing. The amount of available storage is half that of the total drive capacity e.g. a system with four 2TB drives would give 4TB of usable space.
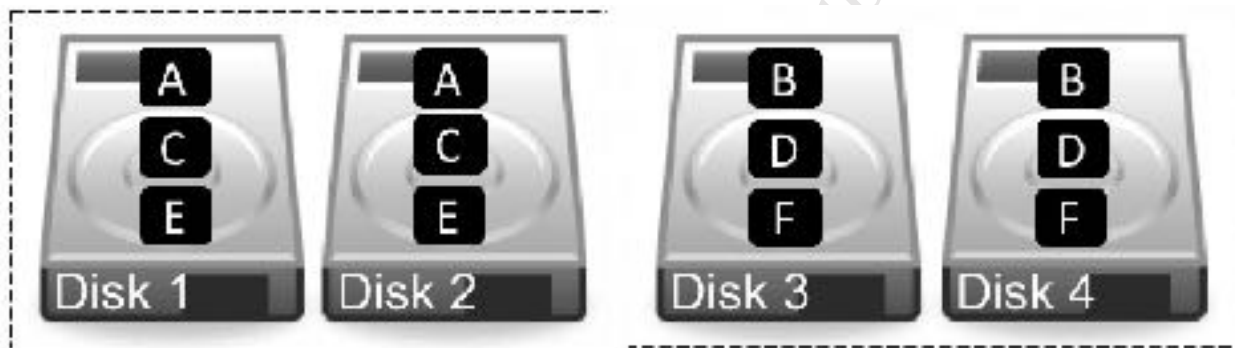

Figure 6: RAID 10 – Simultaneous striping and mirroring

What to do? If you have a server with a single drive then the question of RAID does not arise, although you might want to seriously consider acquiring another drive. If you have a server with two drives, you should probably use RAID 1. If you have a server with three or four drives it should be configured for RAID 5 and if you have five drives, then use RAID 6. The RAID level is usually set using a BIOS option on the server, although some server vendors supply additional software to setup and manage the RAID system. Once set, the RAID level cannot easily be changed, so it is important to think it through and 'get it right'.

It is important to note that RAID systems require a special controller and that these are available in two types. Low-cost servers may have a built-in RAID controller on the motherboard; these are referred to as *software RAID* or embedded *RAID* by manufacturers but are known colloquially as *fake RAID* and are to be avoided as they can be prone to failures and data loss. The weakness is that they use software drivers within Windows so if, for whatever reason, the operating system will not start then the drives may not be visible for repair and recovery purposes. Instead, a separate hardware RAID controller card should be purchased as these offer better performance and reliability.

Special utility software is usually provided by the vendor for configuring the RAID, sometimes at the BIOS level when the server is booted. If this is not the case, then the array may initially appear as a single drive. This utility will also assist in coping with drive failures and a process known as 'rebuilding the RAID', which is where a replacement drive is incorporated into the existing system. Many RAID systems also support the concept of a spare or redundant drive. This is a drive which is not normally used, but in

the event of one drive failing it will automatically switch in and the rebuilding will begin, rather than requiring a manual intervention.

One important thing to note is that a RAID system is **not** a backup system. It can help prevent data loss in the event of problems, but it is still important to make separate provision for backup. For instance, if the server was stolen or the premises went up in flames then the data would be lost regardless of whether and whatever RAID system was used.

Storage Spaces

Storage Spaces is an alternative to RAID and a standard feature in Essentials. It is designed to address three aspects of storage:

Firstly, on a Windows computer each hard drive normally has a separate drive letter to identify it. For instance, the first drive is the C: drive, the second is the D: drive, the third is the E: drive and so on. However, it is more convenient, particularly in a network, if drives can be pooled together to appear as a single large volume. This makes it easier to find things by removing the requirement to know upon which physical drive a particular file or folder is located:

Figure 7: Storage Pool aggregates the hard drives

Secondly, like RAID, Storage Spaces provides a degree of protection against data loss in the event of a drive failing. Multiple copies of files are stored on different drives; if a drive fails then a copy from a different one is automatically used. The failed drive can then be replaced and added back to the storage pool. Finally, the pool can easily be added to in order to provide more storage space, without excessive disruption or reconfiguration. One important thing to note is that the drives can largely be of any type; for instance, external USB hard drives can be connected to the computer and added to the storage pool.

In some respects Storage Spaces is more flexible than RAID, as well as being cheaper to implement. However, performance may not be so high (not necessarily an issue in a small setup).

SSD and 2 ½ inch Drives

Solid State Drives or SSDs offer a significant performance boost over conventional mechanical hard drives or HDDs. Having said that, drive performance is not necessarily a big consideration in small systems as there are other potential bottlenecks, such as network and processor performance. SSDs are expensive compared to HDDs, probably too expensive for general purpose storage in most instances. However, there may be some merit in using a small SSD for the C: drive that holds the operating system.

Most file servers use 3 ½ inch HDDs as these offer the highest capacities and best price-performance among disk drives. Smaller 2 ½ inch drives ("laptop drives") can be an alternative in some scenarios: they

use less power, are quieter and more reliable due to reduced vibration levels. The disadvantages of 2 ½ inch drives are that they are not available in such high capacities and are more expensive. Also, they may need to be mounted in caddies to make them fit into the drive bays on the server.

Types of Hard Drive

File servers do not use the regular hard drives found in desktop PCs and laptops. Instead, higher-quality drives with improved performance and increased reliability (improved MTBF or *Mean Time Between Failures*) are preferred. Such drives may have standard SATA interfaces or SAS interfaces (better, but may not be supported in lower-cost servers). Examples of such drives include: Seagate Enterprise Performance; Seagate Enterprise Capacity; WD Gold; WD Re. As might be expected, these hard drives are more expensive than desktop ones.

Storage Server Systems

Matters are slightly different with a Storage Server system. Here, *Storage Server* is provided pre-loaded on a relatively small hard drive; for instance, with the Thecus W2000 and W4000 it has been loaded on a 64GB SSD that becomes the C: drive. Additional hard drives are then purchased and installed for the data storage. There is no option for RAID, instead Storage Spaces is used to provide resilience.

1.4 Switch and Wireless Access Points

The devices in a network are connected together using Ethernet cabling and wireless access points (WAPs). In a very small business, everything might link back to an all-in-one router or wireless router, whereas in a larger setup there may be a separate router and possibly a separate firewall. Ethernet switches and wire access points may be used to expand the network and provide greater capacity. The following points can be usefully observed:

- Use wired connections whenever possible as performance is 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

1.5 Client Devices

By *client devices*, we mean desktop computers, laptop computers, tablets and smartphones. To connect to an Essentials-based network, the device needs to be running a version of Windows Professional or better, such as *Windows 10 Professional* or *Windows 7 Professional*. Older versions of Windows, such as XP and Vista, which are no longer generally supported by Microsoft, should not be used (although it is technically possible). Best practice is that all desktops and laptops are running the same version of Windows, rather than a mixture of versions.

Client computers running other operating systems, such as Windows Home editions, macOS or Linux, can be connected to Essentials but in a limited, unofficial and unsupported manner and how to do so is covered in this guide.

Devices such as iOS or Android tablets and smartphones can likewise only be connected in a limited fashion.

1.6 IP Considerations

Every device in a network has a unique number within that network to identify it, known as the *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 other purposes and are known as *public IP addresses*. However, a small selection is 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 without risk of duplication and the same numbers are used worldwide millions of times over. The three 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*

Much of the 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 hubs 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 topic.

Devices such as computers and printers do not come with IP addresses already allocated; instead, they have to be configured with a suitable address and 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 PC to *192.168.1.101*, the second to *192.168.1.102*, the third to *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 unmanageable.

With dynamic IP addresses, the numbers are assigned automatically by a DHCP (*Dynamic Host Configuration Protocol*) server and it 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 Essentials detects one of these during the installation it will use it but, if it does not, it can be configured to provide its own DHCP service.

However, it is not really a choice of static or dynamic IP, as you need both. Some devices – servers and routers, for instance, work better with or require static addresses, plus they are often useful for printers. So, the principle is to allocate them static addresses but have the general-purpose computing devices – the desktops, laptops, tablets and smartphones – using dynamic addresses.

Regardless of whether the IP addresses come from a router or are supplied by Essentials itself, it is a good idea to have a scheme to follow. As mentioned above, routers are commonly set to numbers such as *192.168.1.1* or *192.168.1.254*. The server should be set to an adjacent address. Printers and any specialized devices should be close by. The numbers allocated for computers, tablets and smartphones should be a contiguous block of numbers elsewhere, allocated dynamically by the router or other DHCP source. So, for instance, a typical setup might be as follows:

IP Address(es)	Role
192.168.1.1-192.168.1.49	Use for printers and any special devices (static)
192.168.1.50-192.168.1.200	Use for computers, tablets, smartphones (dynamic)
192.168.1.253	Essentials file server (static)
192.168.1.254	Internet router/gateway (static)

One implication of the above is that the network has a maximum of 255 devices in it, although as Essentials is only licensed for 25 users and 50 devices this is unlikely to be an issue. In larger networks, *subnets* are used to expand the size of the network, but we will assume there is only one in use (it is commonly set to *255.255.255.0* in a small network).

Note: there are two 'flavors' of IP: TCP/IPv4 and TCP/IPv6. In this guide we are using the more common IPv4, as most people find it easier to deal with addresses such as 192.168.1.254 rather than something like, say, 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

2. INSTALLATION OF WINDOWS SERVER 2012 R2 ESSENTIALS

2.1 Overview

Setting up an Essentials server consists of several stages. The first one is to install the software and get it to the stage where it can subsequently be configured and customized to reflect the needs of your organization. This typically takes around 60 minutes and is the topic of this chapter.

2.2 Installing Essentials

There are three main techniques by which Essentials can be physically installed onto the server. Read the descriptions and choose the one which is most applicable to you:

Method 1 – Essentials has been supplied on a DVD or USB stick. Go into the BIOS of the server and set it to boot appropriately. Accessing the BIOS varies according to the server brand, but is typically the F2 key on Dell and the F10 key on HP. Insert the DVD or USB stick, connect an Ethernet cable to the server and restart it.

Method 2 – The server manufacturer has supplied a special start-up or management disk. This typically provides driver and RAID support for the server and may do some other configuration work. The usual process is to set the server to boot from CD/DVD as described above. Insert the disk, plug in an Ethernet cable and restart the server. The management software will run – this may take several minutes – but eventually you will be prompted to eject the disk and insert the Essentials DVD. The server may then restart.

Method 3 – Essentials has been purchased pre-loaded on the server. This does not mean that it is ready to use, just that what normally comes on the distribution DVD has already been copied to the server's hard drive so the installation process can run from that. Plug in an Ethernet cable and start the server. This is also the method used in *Storage Server* installations.

Regardless of which method has to be used, after a short while the following screen is displayed. Check the settings, change them if necessary to reflect your country and language, then click **Next**:

On the following screen click the **Install now** button. You may then receive a screen prompting you to enter the product key (i.e. licence key). This can be found on a sticker that comes with the copy of Essentials or may be on the server or other documentation if it came pre-loaded. Then click **Next**. On the subsequent screen tick the box to accept the license terms and click **Next**. On the following screen click the **Custom: Install Windows only (advanced)** box:
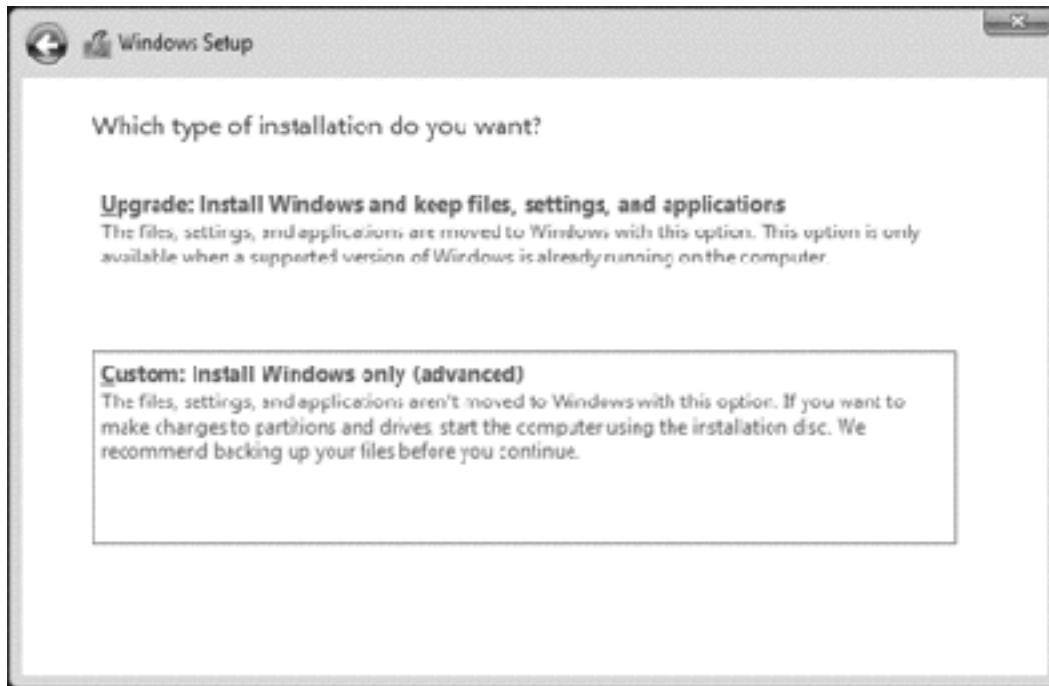

Figure 9: Choose the Custom option

A decision has to be made on where to install Windows i.e. *Essentials* (in the case of *Storage Server* this decision has already been made for you, so you can skip this paragraph). What options appear here will depend on what drives are in the server and how they are configured. On a small system there may only be a single drive. A larger system might have two or more drives. On a RAID system, the drives may appear as a single drive. In this example there are two drives and Windows will be installed on the smaller one with the larger one used for data. Do not try to use the 'System Reserved' partition. The Windows drive needs to be at least 60GB in size but slightly larger is better. **Very important:** make sure the drives/ partitions are formatted before proceeding then click **Next**.
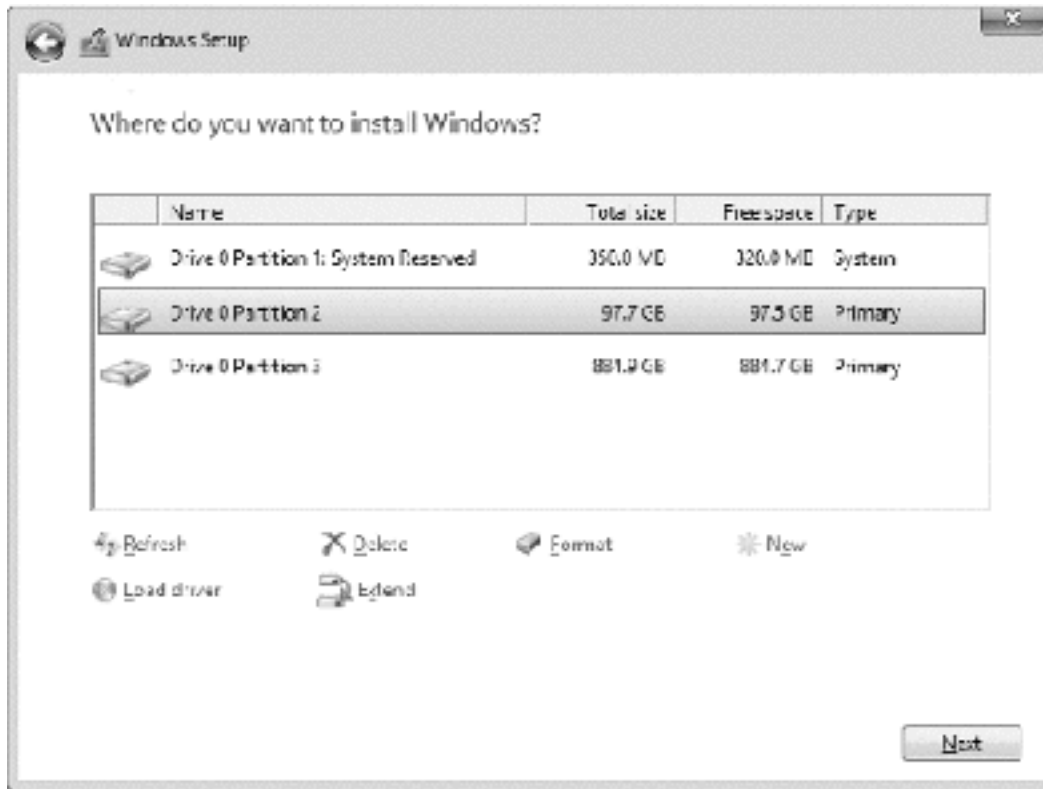
Figure 10: Choose a drive partition

Whilst the next stage runs - which typically takes around 10 minutes - the server will display a progress screen and will restart several times. Eventually the following screen will appear, prompting you to create and confirm a password for the built-in Administrator account. Choose something non-obvious - a random mixture of letters, numbers and punctuation is best - and make a note of it. Then click **Finish**.
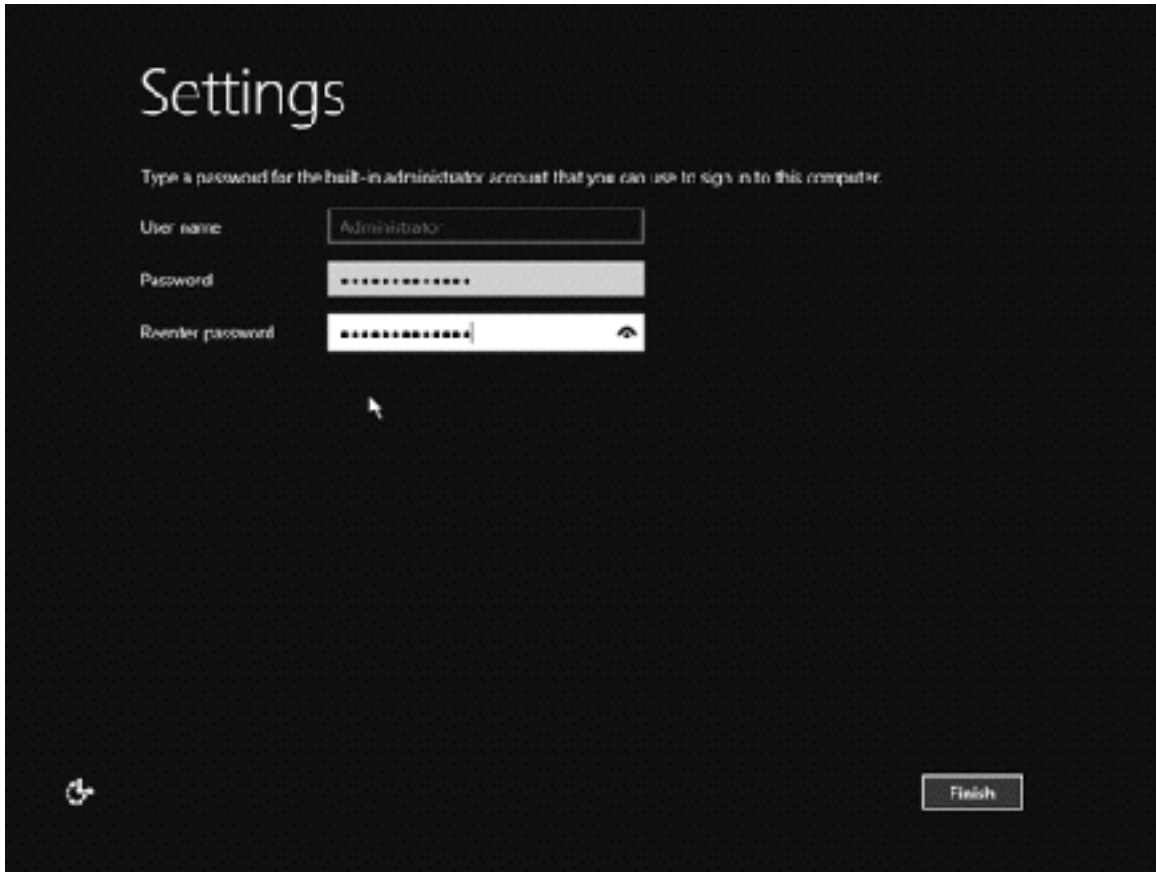
Figure 11: Specify a password for the Administrator

The server will prompt you to press **Ctrl+Alt-Delete** and login - do so as *Administrator*:
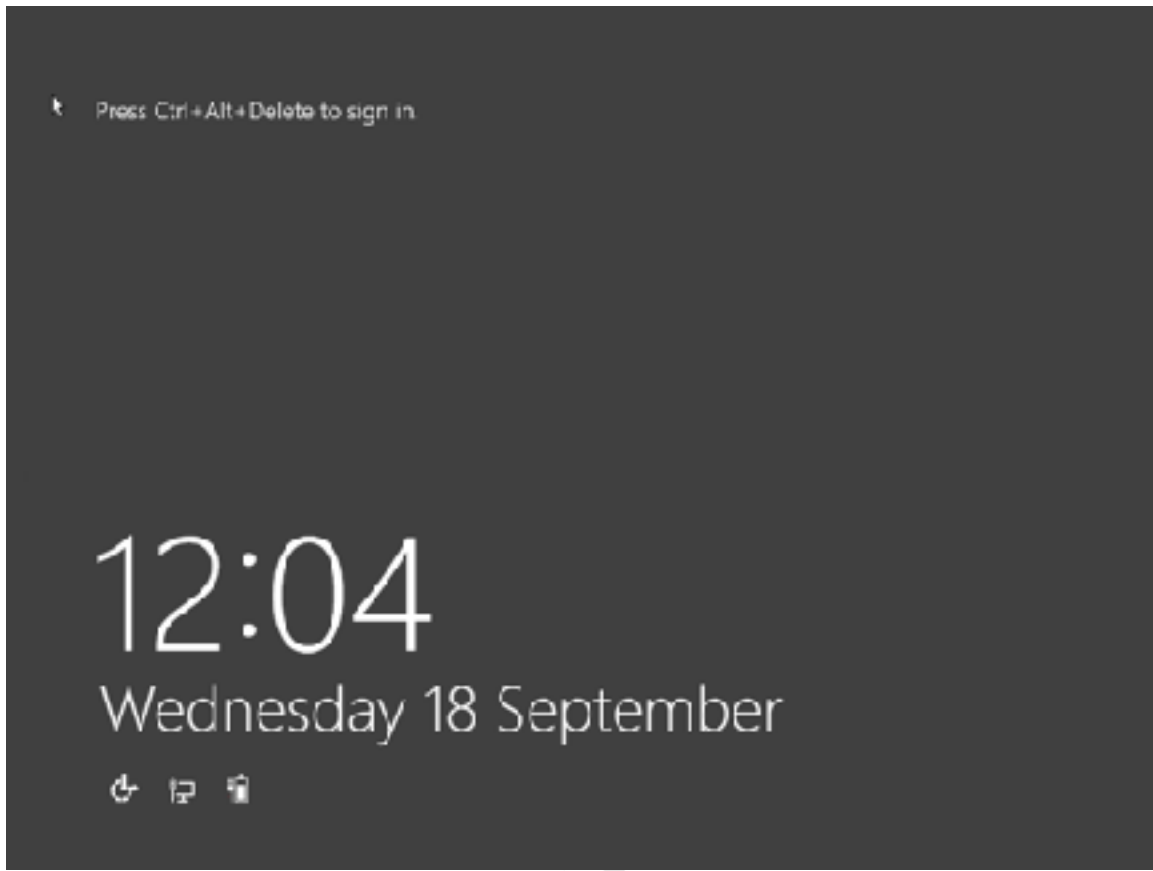
Figure 12: Screen awaiting login

Following the first login, a message is displayed on the right-hand side of the screen asking whether Essentials should look for other devices on the network, including printers. It is important that you choose **Yes**, otherwise Windows will be configured with a public rather than private networking profile and things will not work correctly:
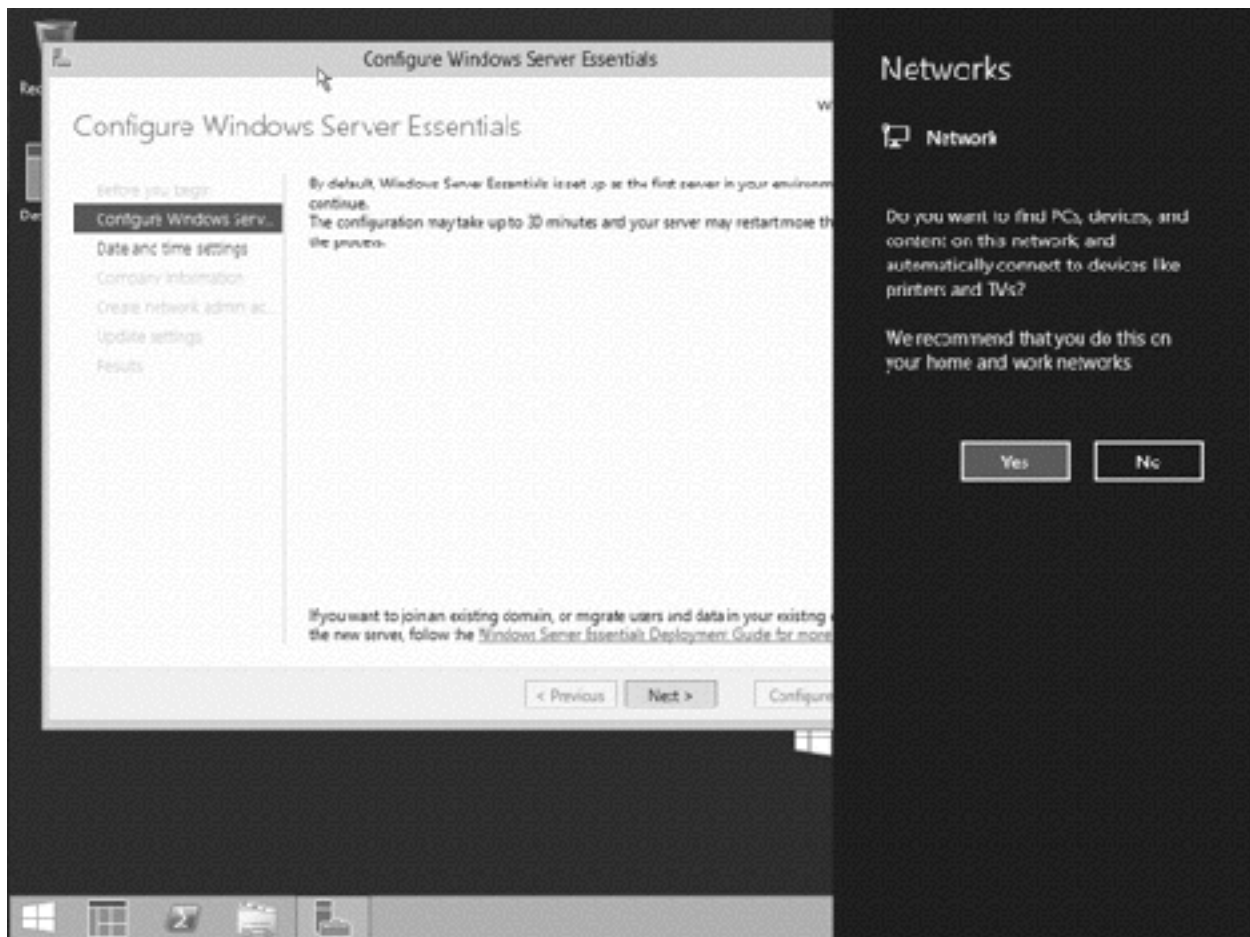
Figure 13: Networks notification screen

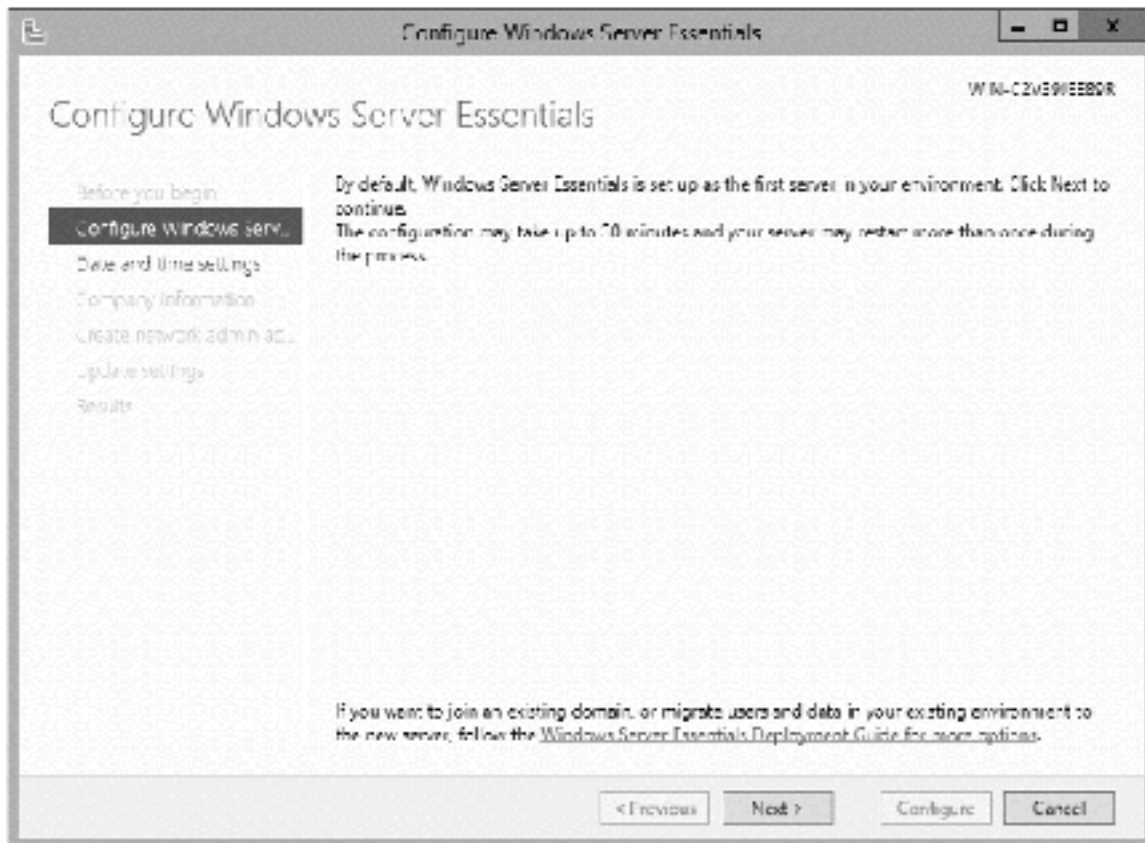After a minute or so the screen will clear to show this panel:

Figure 14: First Configuration screen

However, before continuing the IP address of the network adapter should be changed. Assuming that you have a typical internet router, Essentials will have picked up an IP address from it, but it will be a dynamic address that can change periodically, whereas it really needs to be a fixed IP address. To change it, right-click the **Start** button and choose **Network Connections**. Right-click the network adapter and choose **Properties**. Highlight **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. Change it to use a specific IP address. The address depends upon how the router is configured; typically they use a 198.168.nnn.nnn addressing scheme with the router itself on, say, 192.168.1.1 or 192.168.1.254. The server should be given an adjacent address. In this example, the router is 192.168.1.1 so the server is being set to 192.168.1.2. The Default gateway is the address of the router; the subnet mask should be 255.255.255.0 and the Preferred DNS server set to the address of the router:

Figure 15: Specify the IP address

Make the change, click **OK** and **Close.** Wait about 30 seconds for the adapter to pick-up the new IP address then return to the *Configure Windows Server Essentials* screen and click **Next**. If the date and time are incorrect click **Change system date and time settings** and adjust accordingly. Then click **Next**:
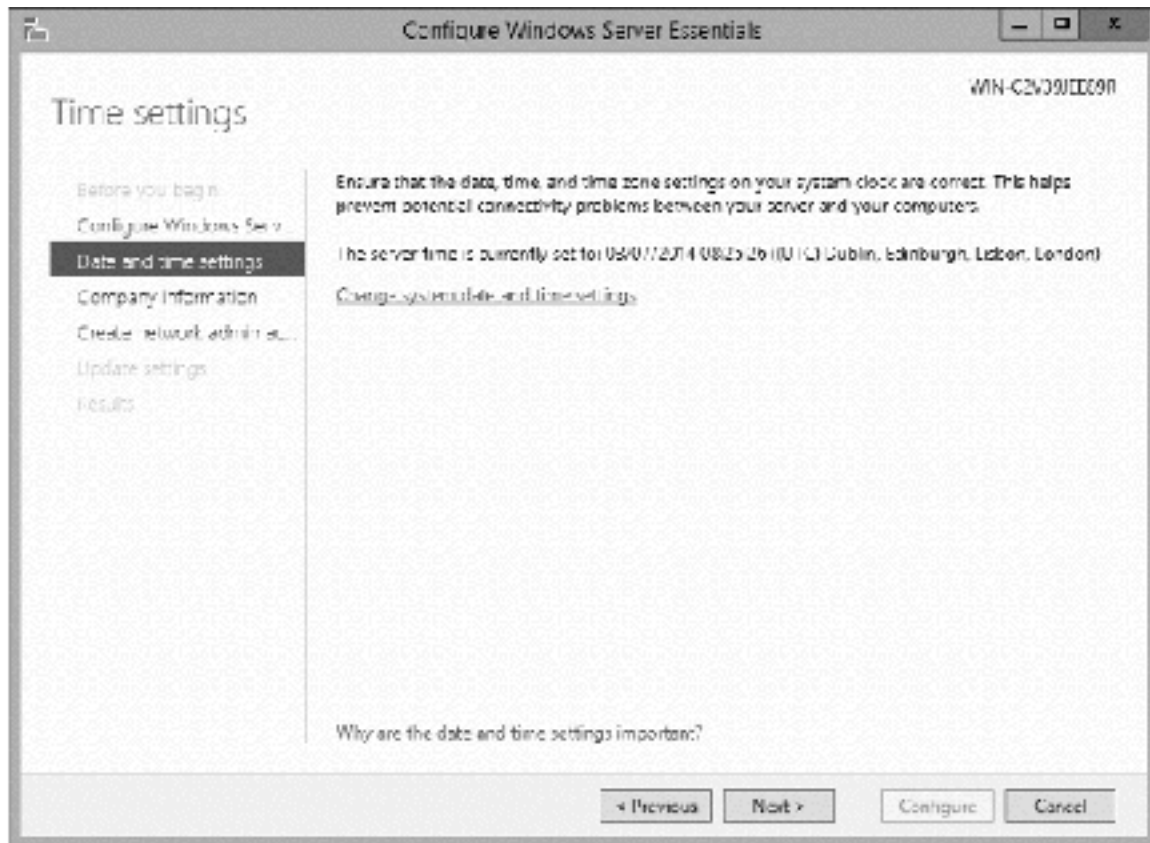
Figure 16: Date and time settings

On the following screen, enter the Company name. In turn, Essentials will propose an *internal domain name* along with a name for the server. If the company name is lengthy then consider abbreviating it. For instance, here we have used *CTACS* rather than *Callisto Technology And Consultancy Services*. Change the Server name to *server* and click **Next** (the name can be just about anything but the examples in this guide assume *server*). Note that none of these fields are case sensitive. Also note that once these details have been specified they cannot subsequently be changed without reinstalling the server, so check carefully before clicking **Next**:
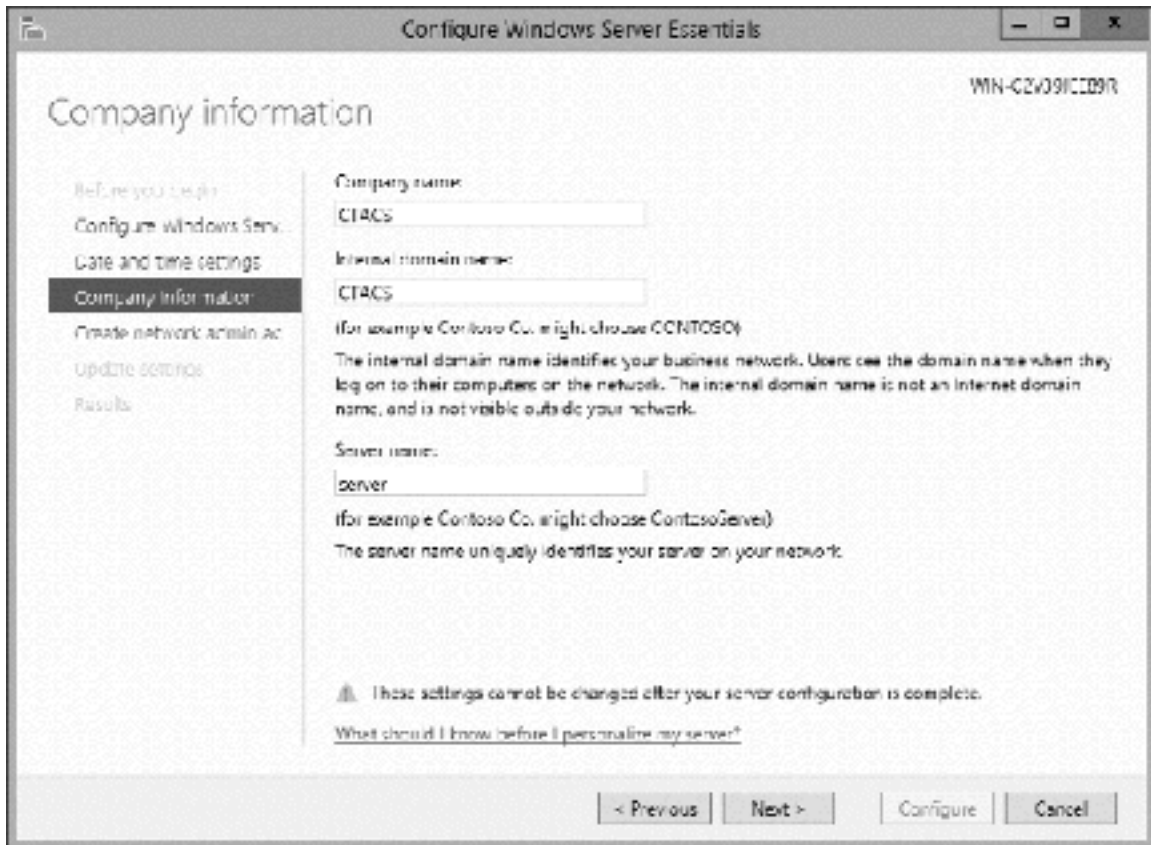
Figure 17: Specify company, domain and server name

The following step is to create an everyday network administrator account. Although there is already an account called *Administrator*, it is considered bad practice to use it unless absolutely necessary; instead, another account for regular administrative work is preferred. A good name for it is *systemadmin*. The password can be the same as the Administrator one, but if it is not then be sure to make a note of it. Click **Next**:
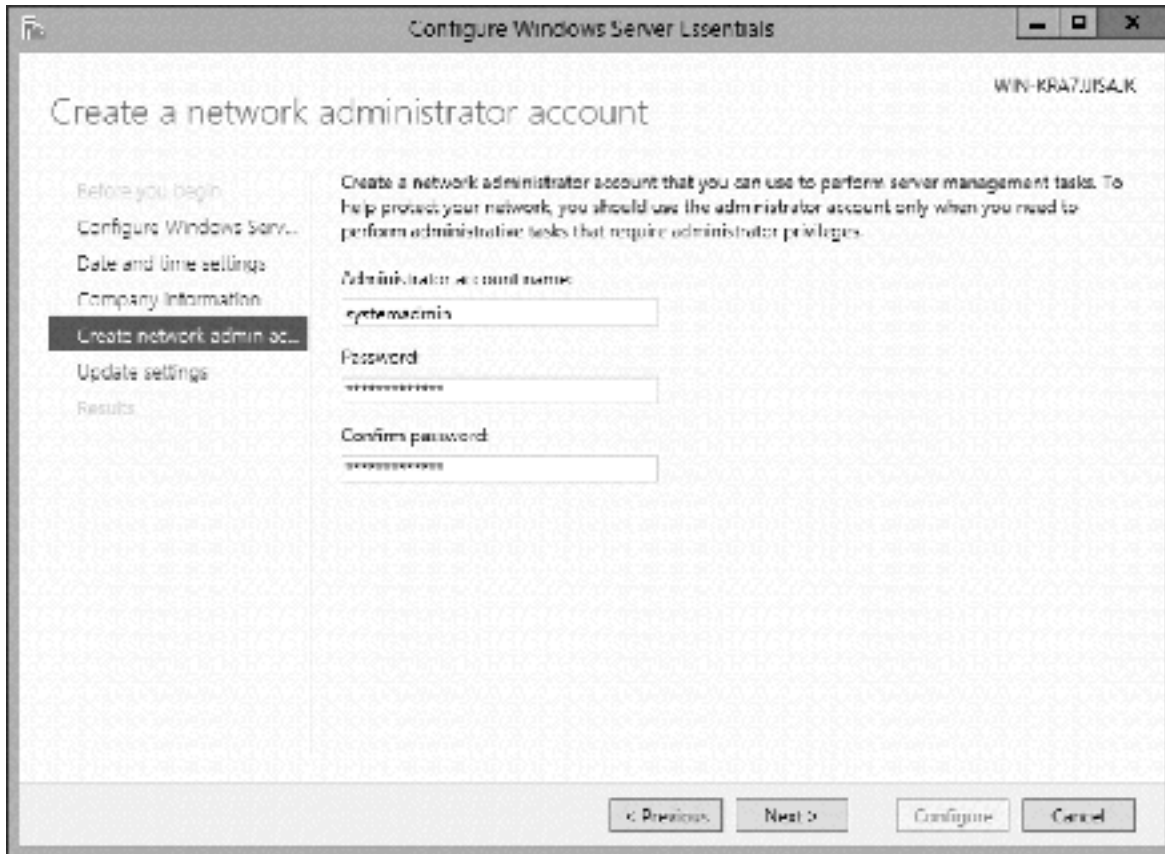
Figure 18: Create a network administrator account

Windows update settings should now be specified. With a server you want total control over the process; you do not want it applying updates and rebooting when it wants to, so set it to **Do not check for updates**. Then click the **Configure** button (note that the Next button may in any case be greyed out):
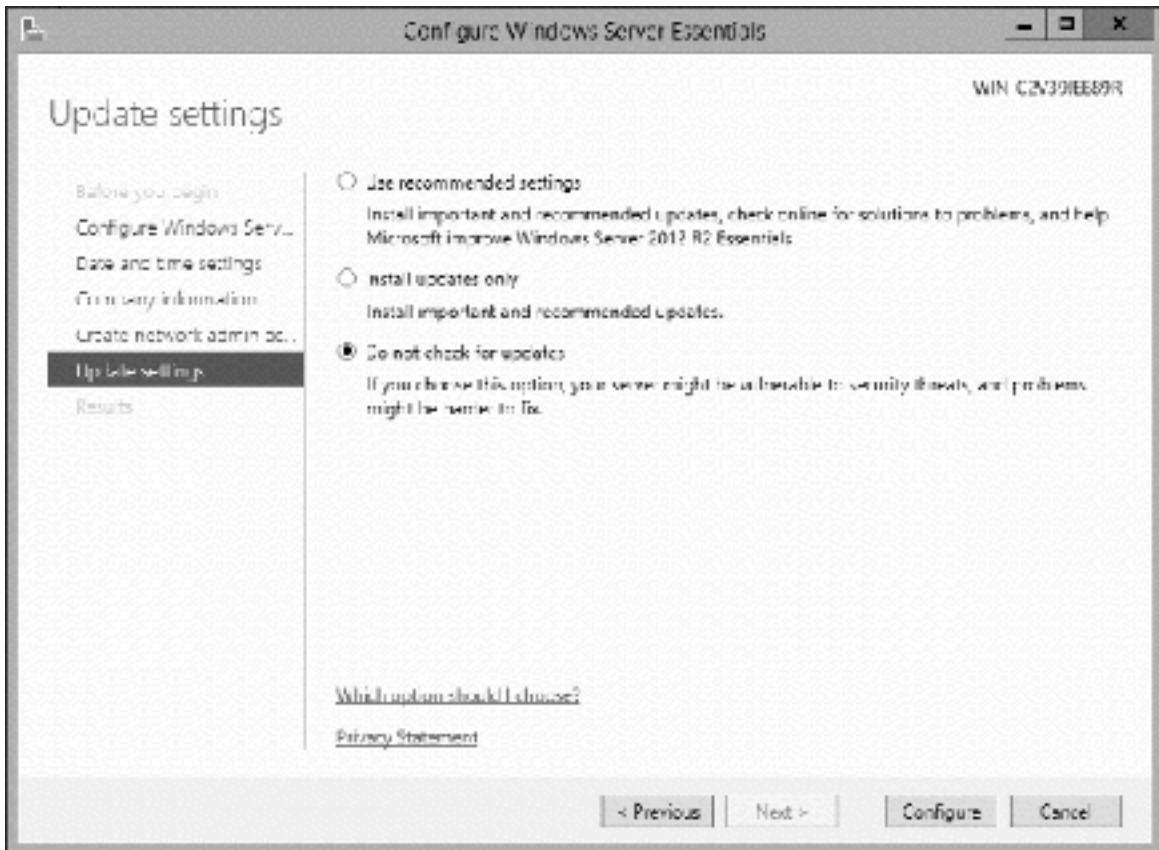
Figure 19: Specify update settings

Essentials will now display the following screen whilst it makes the necessary changes. The server may reboot several times during this stage, which will typically take between 10-30 minutes to complete.
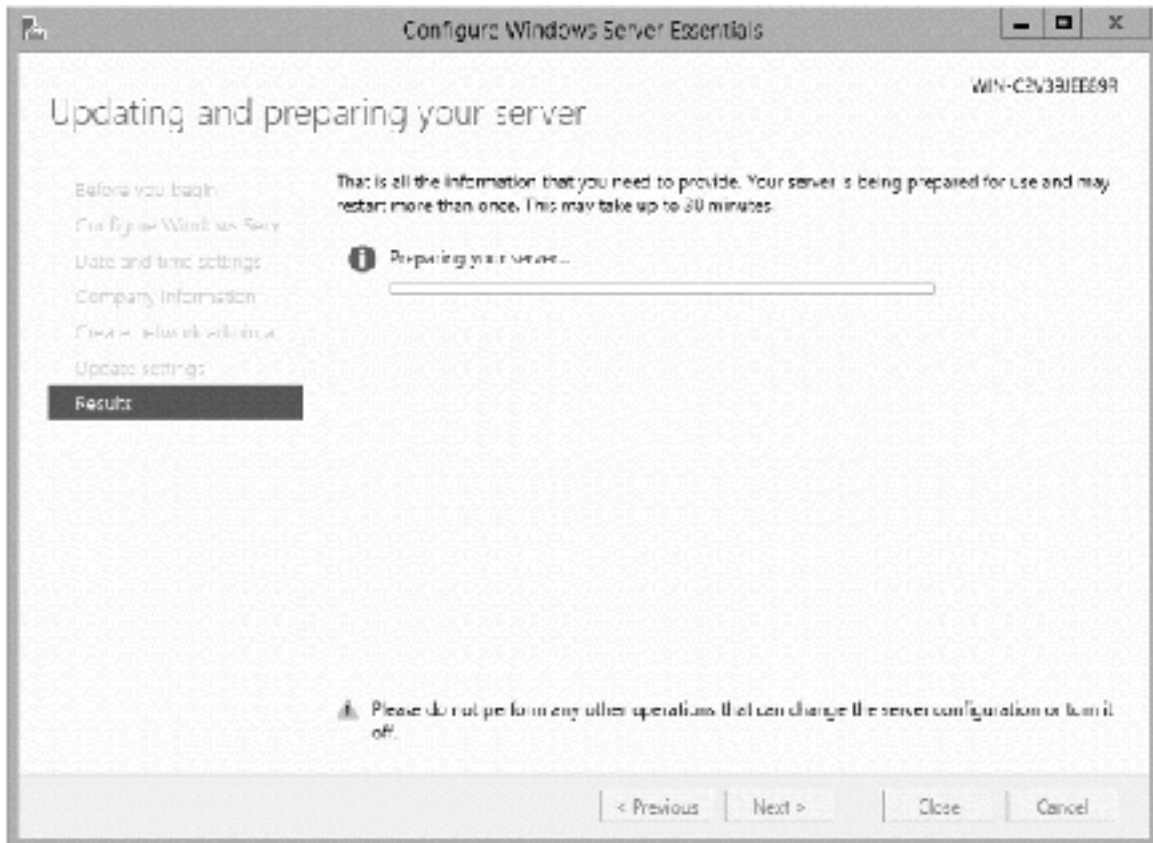
Figure 20: Status screen

When everything has completed the following screen appears. Note that it is not necessary to 'Register with Microsoft online services' so just click **Close** to acknowledge:
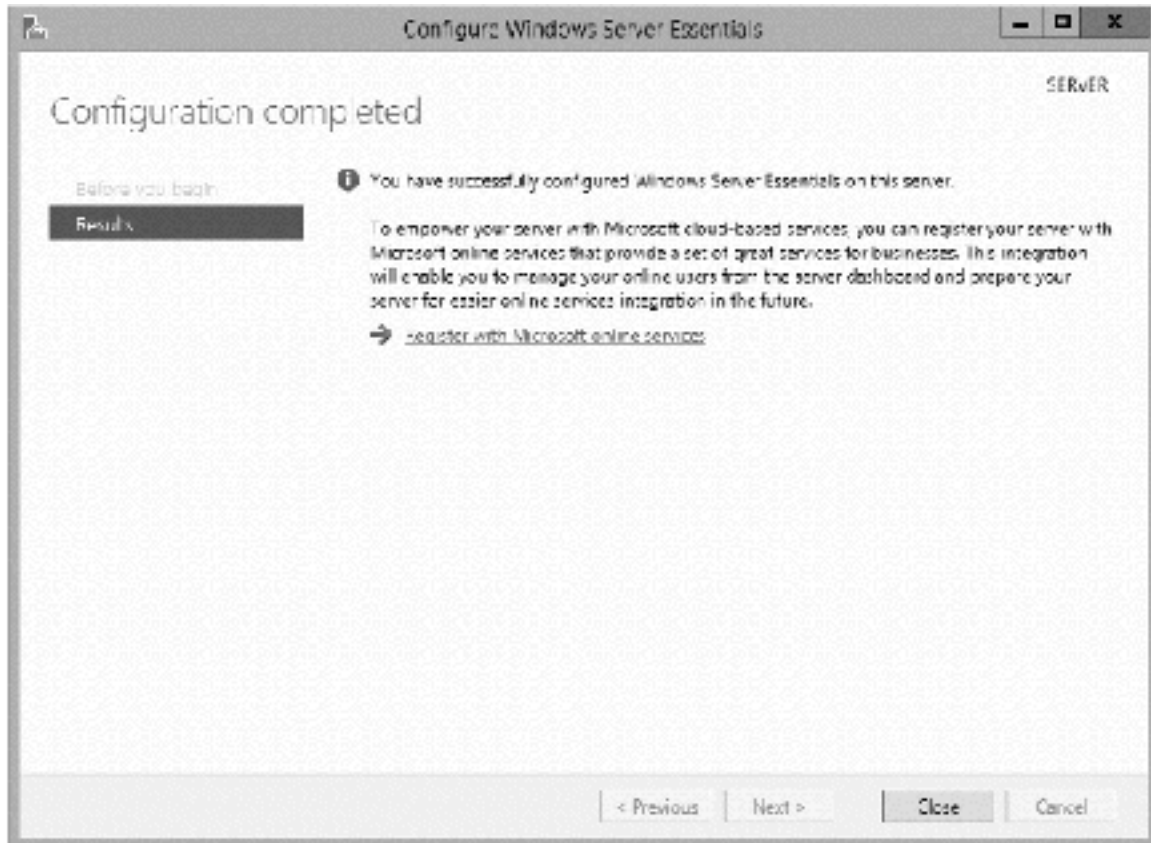
Figure 21: Confirmation screen

Important: As mentioned previously, Essentials assumes that you are using an internet router that provides IP addresses via a built-in DHCP server. If this is **not** the case, then it will now be necessary to install DHCP on the server **before** proceeding further and how to do so is described in <u>12.10 Installing DHCP</u>.

Suggestion: Make a written note of the various server settings and keep it somewhere safe. In particular you should record: Administrator password; the Network Administrator name and password; the server IP address; the internal domain name.

2.3 Managing Essentials – The Five Minute Tour

The key component in configuring and managing *Essentials* is the *Dashboard*. It can be thought of as a sort of shell or front end that sits on top of Windows Server, providing a simplified and friendly interface to the underlying complexity of the operating system. The Dashboard can be launched by double-clicking its icon on the Desktop, which looks like this:

The Dashboard icon can also be found on the Taskbar, as well as on the Start Screen. The Dashboard takes several seconds to load, then appears thus:
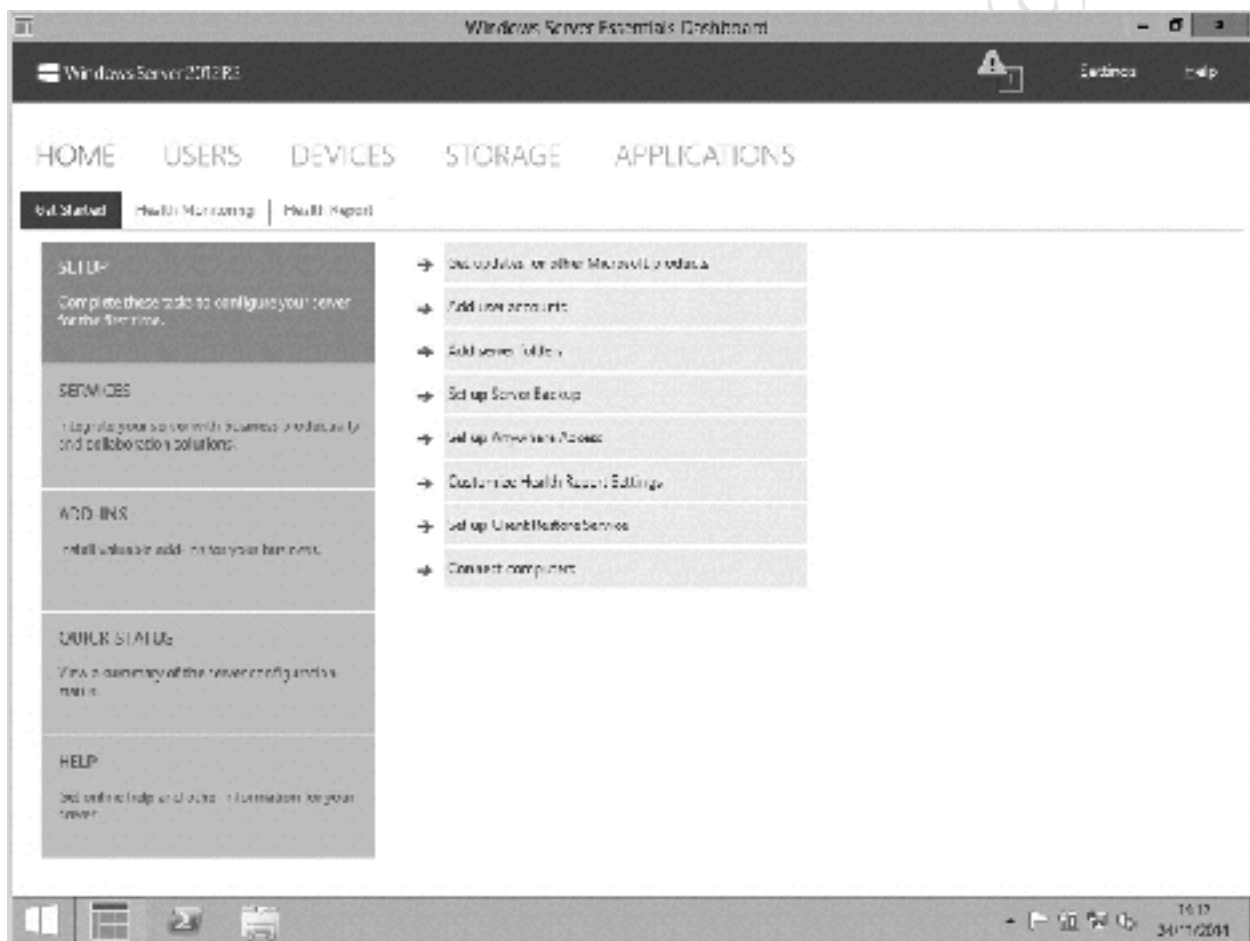

Figure 22: The Dashboard

It is organized into a number of sections: *USERS*, *DEVICES*, *STORAGE* and *APPLICATIONS*. Each of these will display the status and characteristics of that topic and will list a number of clickable tasks pertaining to it. The *HOME* page, displayed above, is structured in a way to help you setup the server using a checklist of tasks to be completed such as *Add user accounts*, *Add server folders* and so on.

At the top of the screen is a status section where any warning or error messages indicated (see picture below). If there are messages, click in the area to expand and then click **See more information**. It is

necessary to make a judgement about the seriousness of any messages. Generally speaking they will be fairly trivial and can safely be ignored, often relating to matters such as automatic updates not being switched on. If the server only has a single disk drive there will be a message saying that the data folders are on the same drive as the operating system, which can also be ignored (unless of course your system is supposed to have more than one drive in it, in which case there is a problem).

Figure 23: Messages on the Dashboard

Although much of Essentials is controlled through the Dashboard, there are several other tools that you will need to be familiar with. Click the **Start** button or press the Start key on the keyboard to display the *Start Screen*:
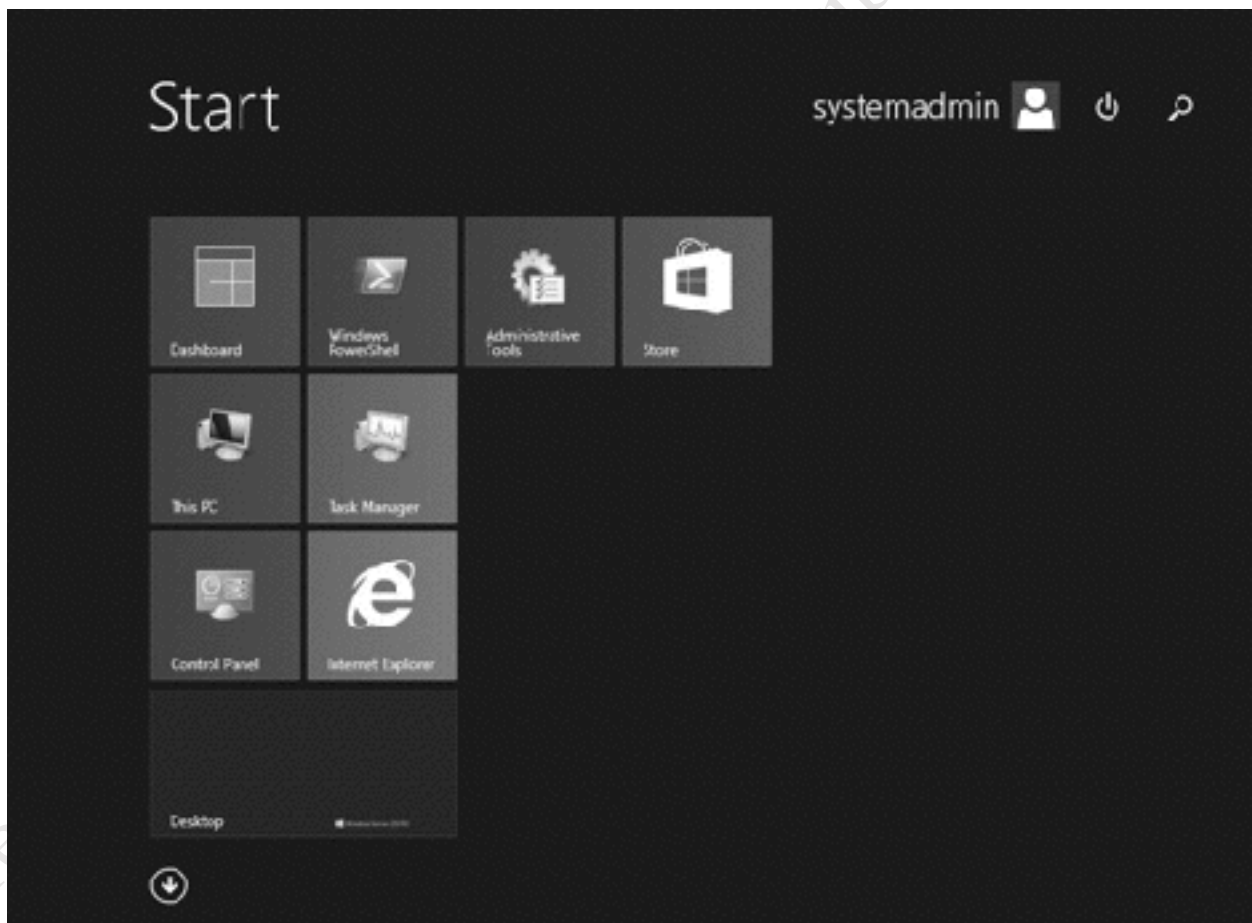
Figure 24: The Start Screen

On the Start Screen are a number of useful tiles:

- *Dashboard* – as discussed above

- *This PC* – displays File Explorer (formerly known as Windows Explorer), used for examining the contents of drives and folders

- *Control Panel* – for managing various aspects of the server, such as Windows Updates and adding printers

- *PC Settings* – the modern alternative and long term replacement to the Control Panel. At present this does not have full functionality so we will only use Control Panel in this guide

- *Windows PowerShell* – an advanced alternative to the Command Prompt ("DOS prompt")

- *Task Manager* – for checking performance and resource utilization

- *Internet Explorer* – for accessing the internet

- *Administrative Tools* – provides access to more advanced aspects of controlling the server

As with Windows 8.1, clicking on the Start Screen's downward arrow will display a list of all applications installed on the server. More experienced users may prefer to work at this level for some tasks. Note that some of the features associated with Windows 8 and Windows 10 (e.g. *Live Tiles*) are not present in Windows Server.

3. USERS AND FOLDERS

3.1 Overview

For users to access the server, accounts have to first be created on it. Note that these accounts are quite separate and unrelated to any that may exist on the computers themselves (i.e. local Windows user accounts) and effectively replace them. Also, folders have to be created in which users can store data. Essentials will have created some folders automatically to get you started; in some instances these will be sufficient but if they are not then additional ones to reflect the particular requirements of the organization can be created.

If you are **not** using Storage Spaces, go to section <u>3.3 Creating User Accounts</u> at this point. If you are using Storage Spaces, continue with section <u>3.2 Setting up Storage Spaces</u> below.

3.2 Setting up Storage Spaces

As described previously, *Storage Spaces* is a feature of Windows Server that allows systems with multiple hard drives to be better utilized and managed. If you are going to use it, it should be setup now before creating any users and folders on the system.

As is often the case with Windows in general, there are several ways of going about something and it is no different in Essentials. The simplest method is from the Dashboard; however, it makes a number of assumptions and largely hides the process of what is going on. This can result in such outcomes as a pair of 2TB drives being added together to create an apparent 16TB mirrored drive, which many people will find very strange indeed. A second method uses *Server Manager*, the standard tool for managing a regular copy of Windows Server, which is not commonly used on an Essentials system but is still available 'under the hood'. It allows complete control over the process, but requires a higher degree of technical knowledge. The third method is available from the Control Panel and offers a good compromise between simplicity and functionality, so this is what we will use (it also happens to be identical to the method used in Windows 8.1 and Windows 10).

In this example, the server had a single hard disk, divided into two partitions. Essentials was installed upon a smallish C: partition and the D: drive was available for data storage. Two further drives, each of 2TB have now been added and Storage Spaces will be used to join them together to create a larger, protected volume. These drives can be internal hard drives, external USB or eSATA drives or any mixture.

First make sure that the new drives are being recognised. Right-click **Start** and choose **Disk Management**. There may be a message about having to initialize the new drives – do so. However, it is not necessary to format them. Then right-click **Start**, choose **Control Panel** and click **Storage Spaces**. Click **Create a new pool and storage space** (if User Access Control is invoked answer **Yes**). A panel listing the available drives is shown:
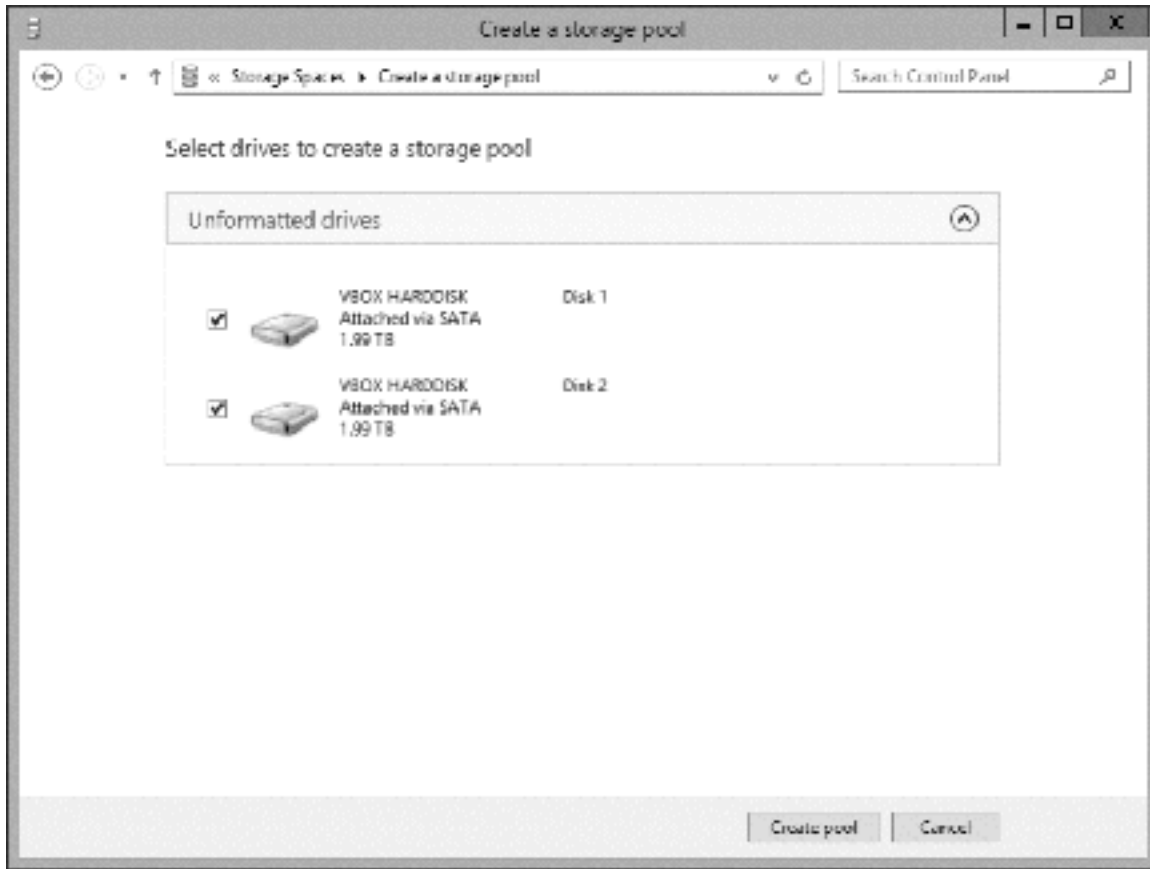
Figure 25: Select the drives to create a storage pool

Tick each drive and click the **Create pool** button. The options which then appear depend upon the number of drives being added. If two drives are being used, the options are:

- *Simple* - in which the drives are aggregated to create a single large volume (sometimes known as JBOD or *Just a Bunch of Disks* in other computing environments)

- *Two-way mirror* – in which data is duplicated on each drive in order to provide redundancy (analogous to RAID 1 in other computing environments)

If three or more drives are being used then two more options become available:

- *Three-way mirror* – in which data is triplicated across the drives to provide greater redundancy

- *Parity* – here data is stored across all the drives. Additional information (known as *parity*) is used by the system, such that data is preserved in the event of a drive failure (analogous to RAID 5 in other computing environments)

The amount of storage space available depends upon the option selected. In our example, we are using a pair of 2TB drives. If these are configured in Simple mode then the total amount of storage is 4TB; if configured in Two-way mirror mode then the amount of available storage is 2TB.

Note that when creating a storage space you can name it and give it a drive designation e.g. F: in this example. This drive designation may replace an existing one plus only applies to the server, not to any connected computers. Click **Create storage space**:
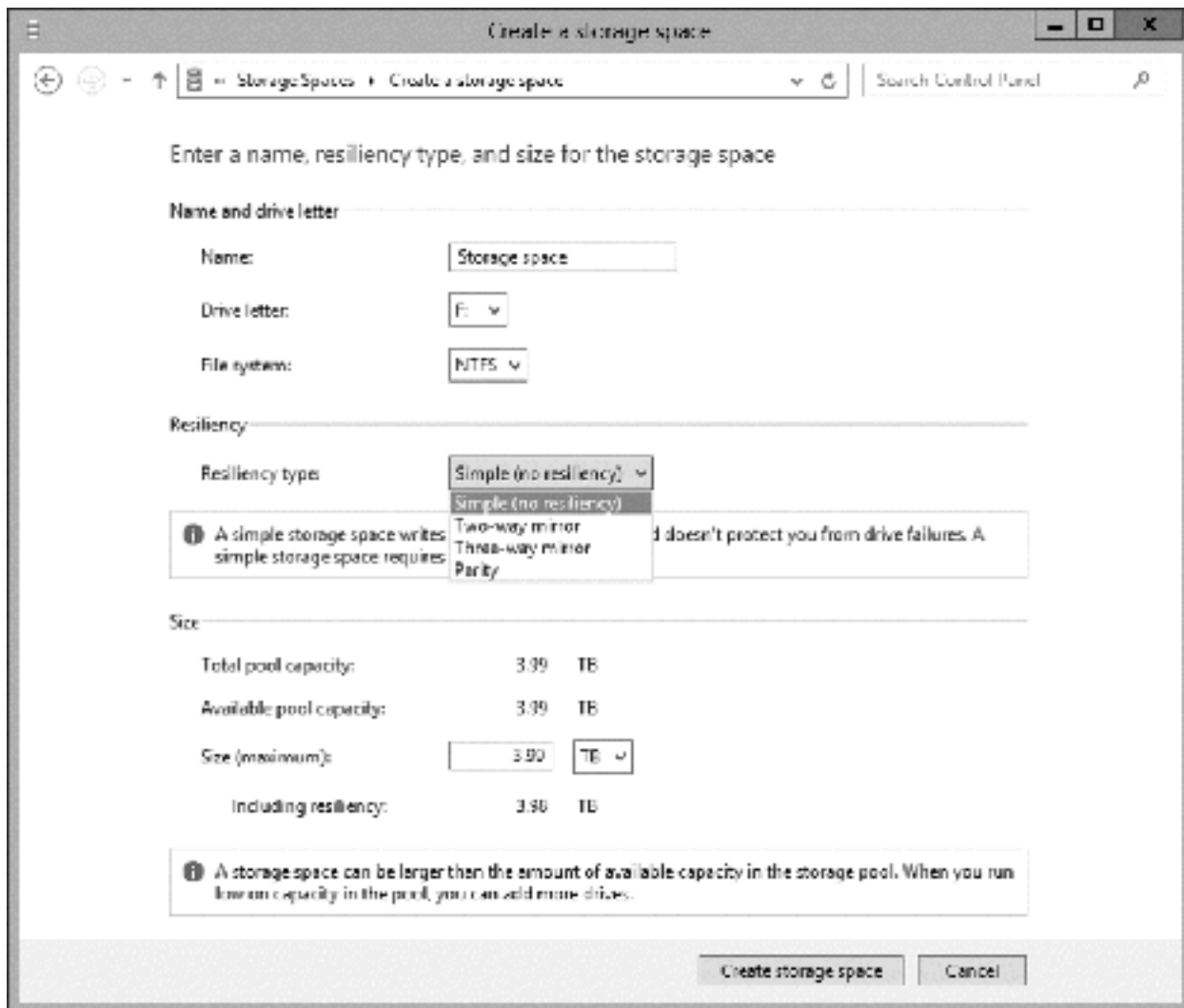
Figure 26: Creating a storage space

After the Storage Space has been created, a summary screen is displayed. The Storage pool can also be managed from this screen:
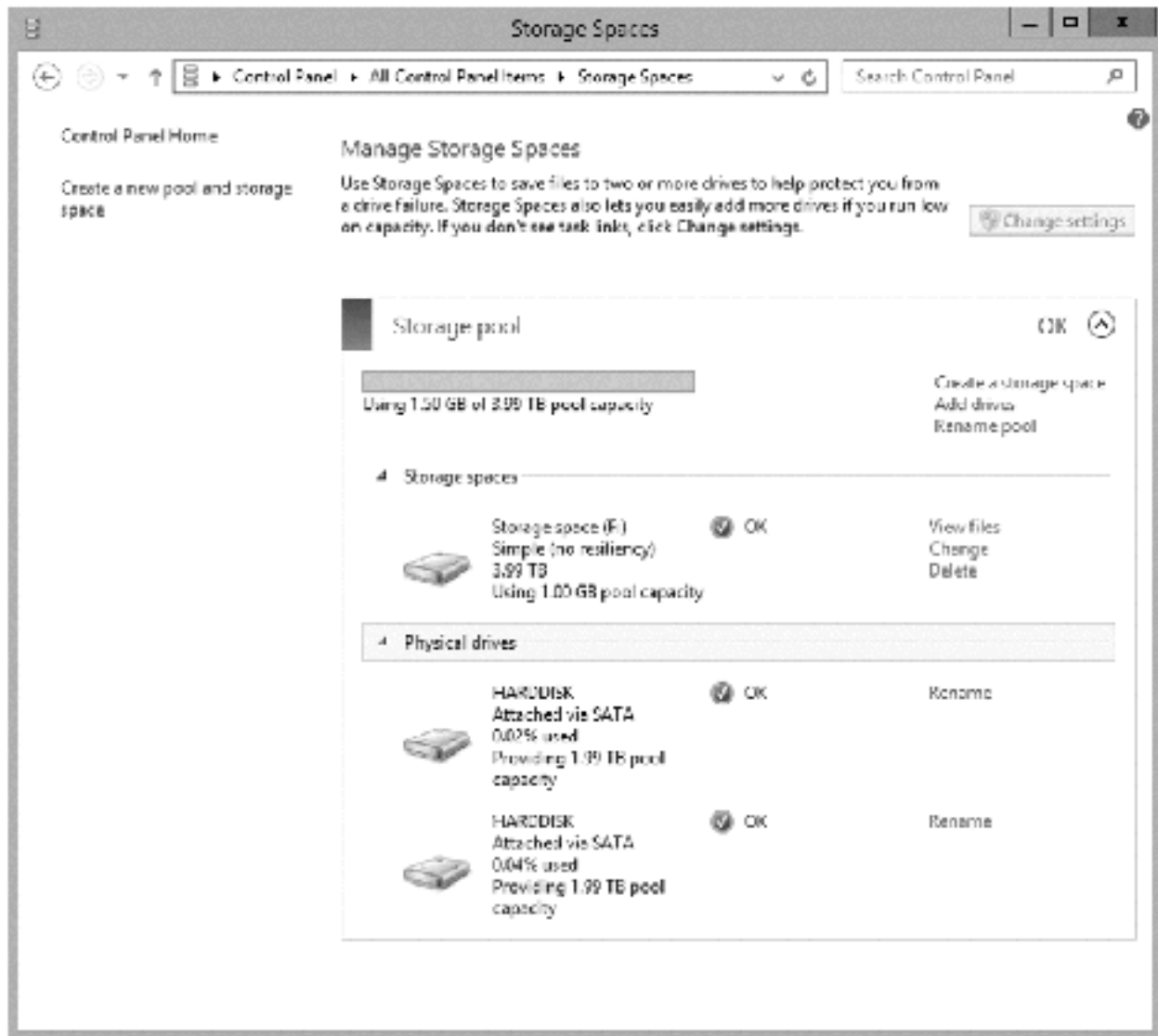
Figure 27: Managing the Storage Pool

During the initial installation, Essentials will have created a number of shared and important system folders. Depending on what volumes were in the server, these will have been placed on the D: or possibly the C: drive; they now need to be moved to the more spacious Storage Pool that we have created, corresponding to F:. Fortunately, there is a built-in function on the Dashboard to make this easy.

Go into the Dashboard and click **STORAGE**. On the STORAGE section, click the **Server Folders** tab. There will be five folders listed. Highlight the first one, then in the right-hand panel click Move the folder to start the *Move a Folder* wizard:
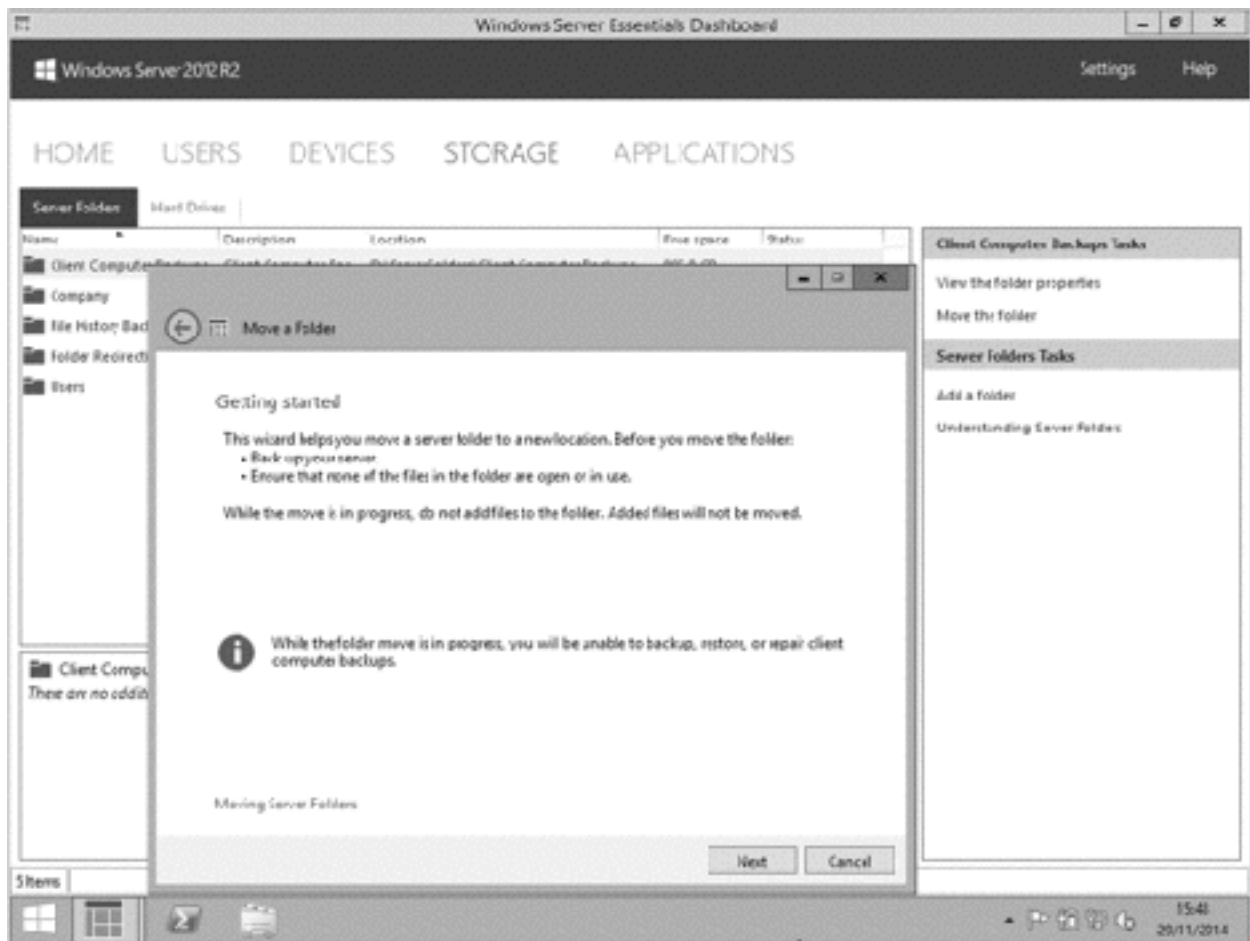
Figure 28: Move a Folder Wizard

Click **Next** on the Wizard. On the resultant panel highlight the new destination for the folder (in our example it is the F: drive) and click **Move folder**:
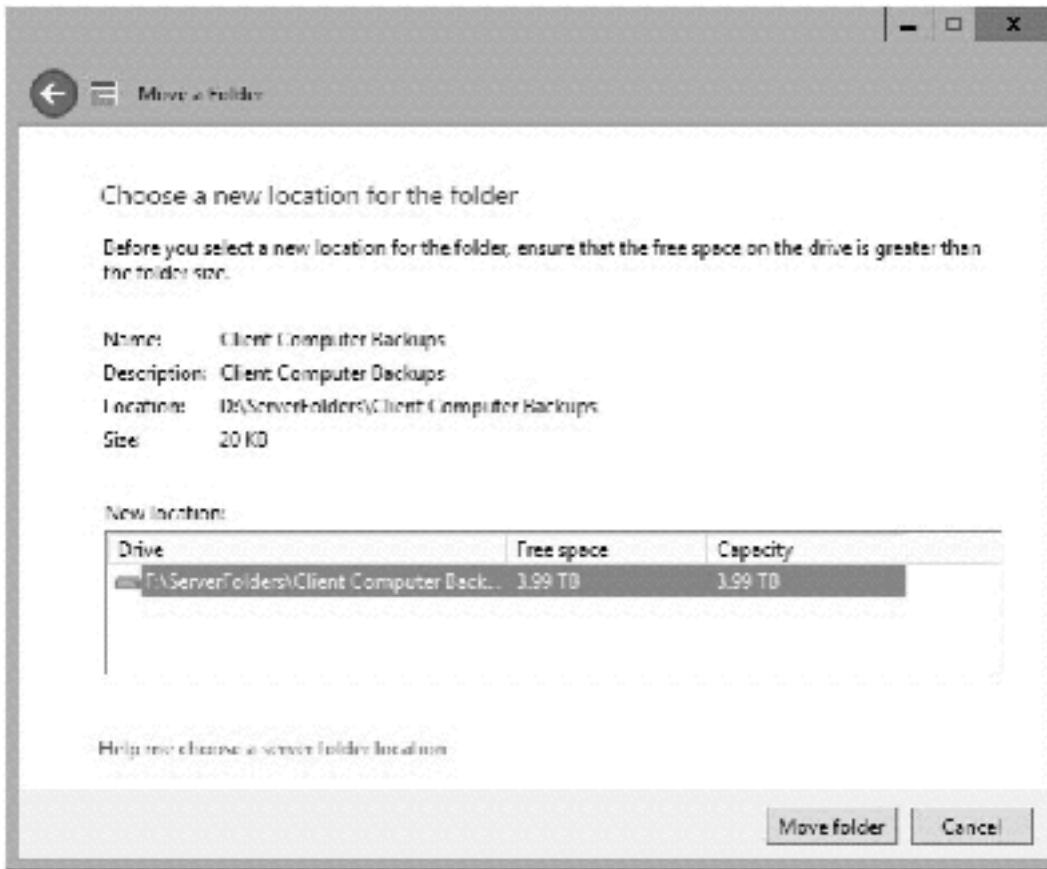
Figure 29: Choose a new location for the folder

Once the folder has been moved – which will only take a few seconds – a message is displayed advising that the *Server Backup Configuration* should be run. As we haven't setup the backup yet this can be ignored by clicking **Close**.

The process should now be repeated to move the *Company*, *File History Backups*, *Folder Redirection* and *Users* folders to the Storage Pool.

3.3 Creating User Accounts

On the server. Launch the Dashboard and click on **USERS** to display the following screen:
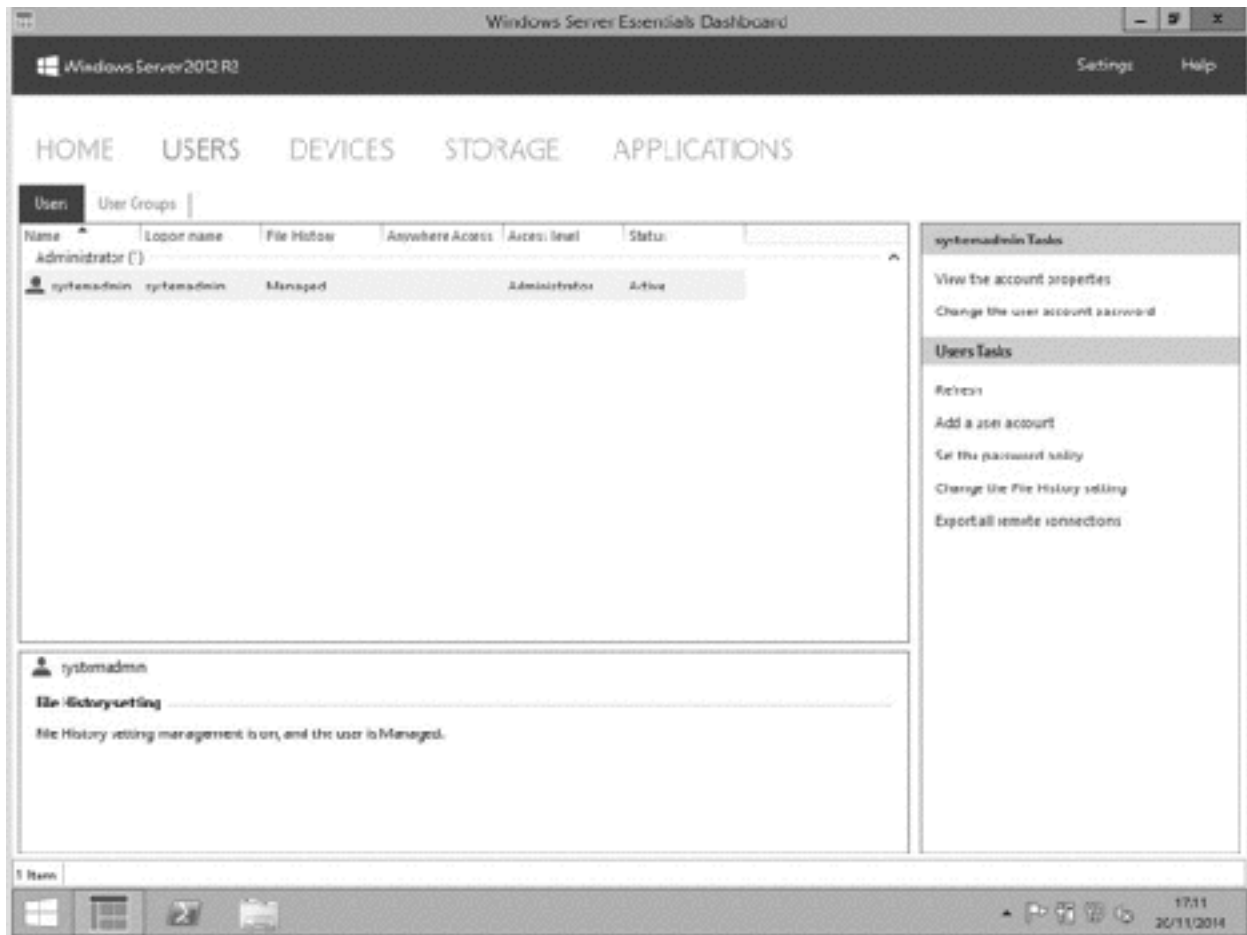
Figure 30: Users tab on the Dashboard

The first thing to do is set the password policy, which means defining how complex (strong) should the logon passwords be for users. Strong passwords provide better security, but can frustrate and slow down users if they are too complicated to remember. Essentials provides four possibilities:

Strong – password has to contain at least 7 characters and be made up from at least 3 of these categories: uppercase letters, numbers and symbols. Example: *Footy98!*

Medium Strong - password has to contain at least 5 characters and be made up from at least 3 of these categories: uppercase letters, lowercase letters, numbers and symbols. Example: *6Goal*

Medium - password must be at least 5 characters but no restriction on what they are. Example: *balls*

Weak - password can be anything except blank. Example: *ko*

It is recommended that strong passwords are use, especially if remote access to the server is to be used. Also note that if Essentials is to be used with Office 365 (covered in Chapter 11. OFFICE 365) then strong passwords are mandatory. On the right-hand panel of the screen – *User Tasks* – click **Set the password policy**. Drag the pointer to the desired setting. Also, consider taking the tick off the **Passwords never expire** option, else the users will be prompted to change their passwords on a regular basis, which often leads to frustration. Then click **Change policy**.
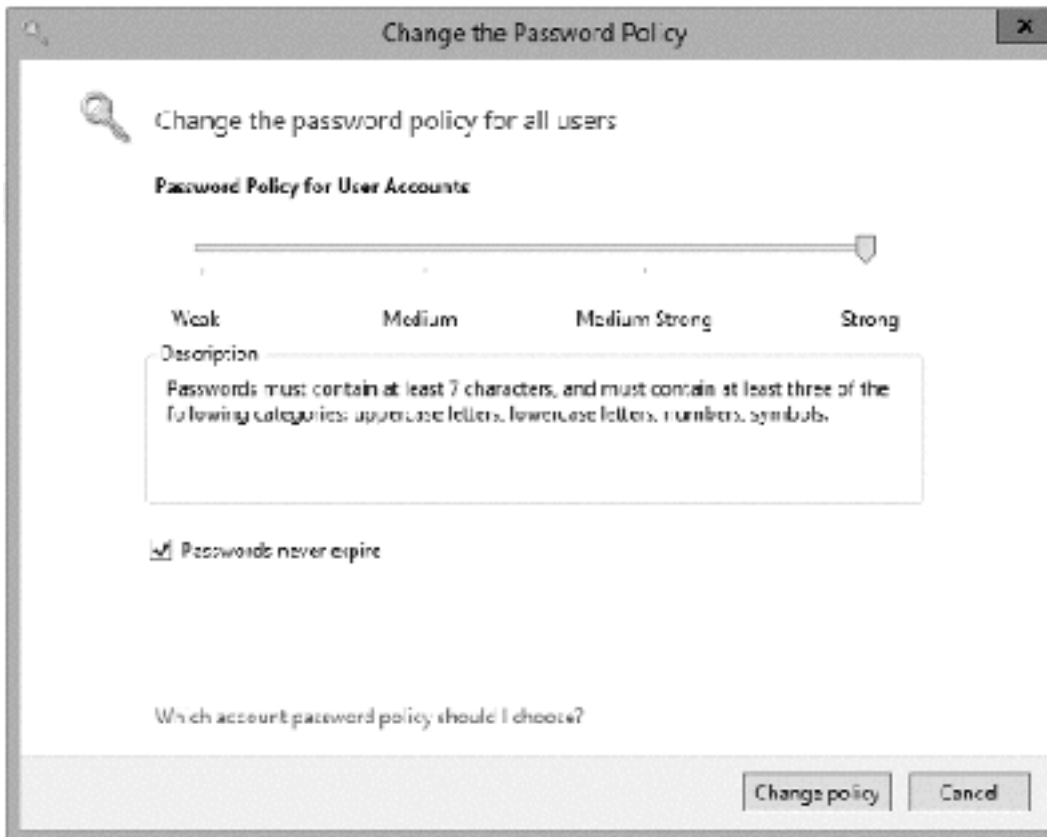
Figure 31: Password policy

The users can now be created. It is suggested that a list of all users is first written down, along with their passwords, and used as a checklist.

Within the User Tasks section, click **Add a user account** to display the following form:

Figure 32: Add a user account

Enter the user's first and last names. Essentials will propose a user account name (i.e. logon name) of the two concatenated together. However, you might want to simplify it and here we have changed the suggested name of *LouiseBookman* to *louiseb*. If you take this approach, be sure to be consistent for all users. Enter a password according to the policy defined above and confirm it. There are two possible levels of access for users: *Standard* or *Administrator*. As we already have an Administrator account, all users should be Standard users. Try to avoid the mistake of making people administrators simply because they are important within the organization – this is about their role on the server, note their role within the organization. Click **Next**.

The subsequent screen specifies what shared folders the user should have access to. This is a bit of a chicken-and-egg situation as we have not created any at this stage. However, there is a built-in folder called *Company* and Essentials is proposing 'Read only' access to it; change it to the more useful 'Read/ Write' and click **Next**.
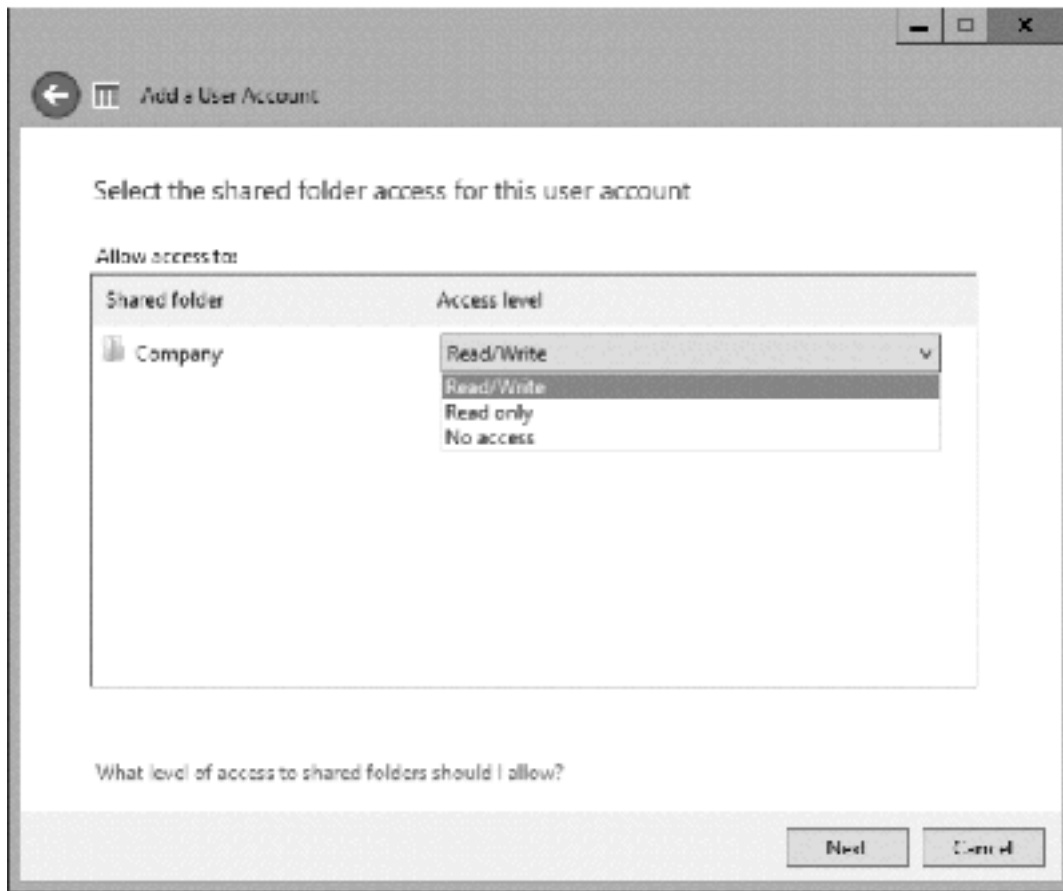
Figure 33: Specify access to folder

The follow-on screen is concerned with remote access i.e. being able to access the server from outside the office over the internet, referred to as *Anywhere Access*. The defaults are fine so just click **Create Account**:
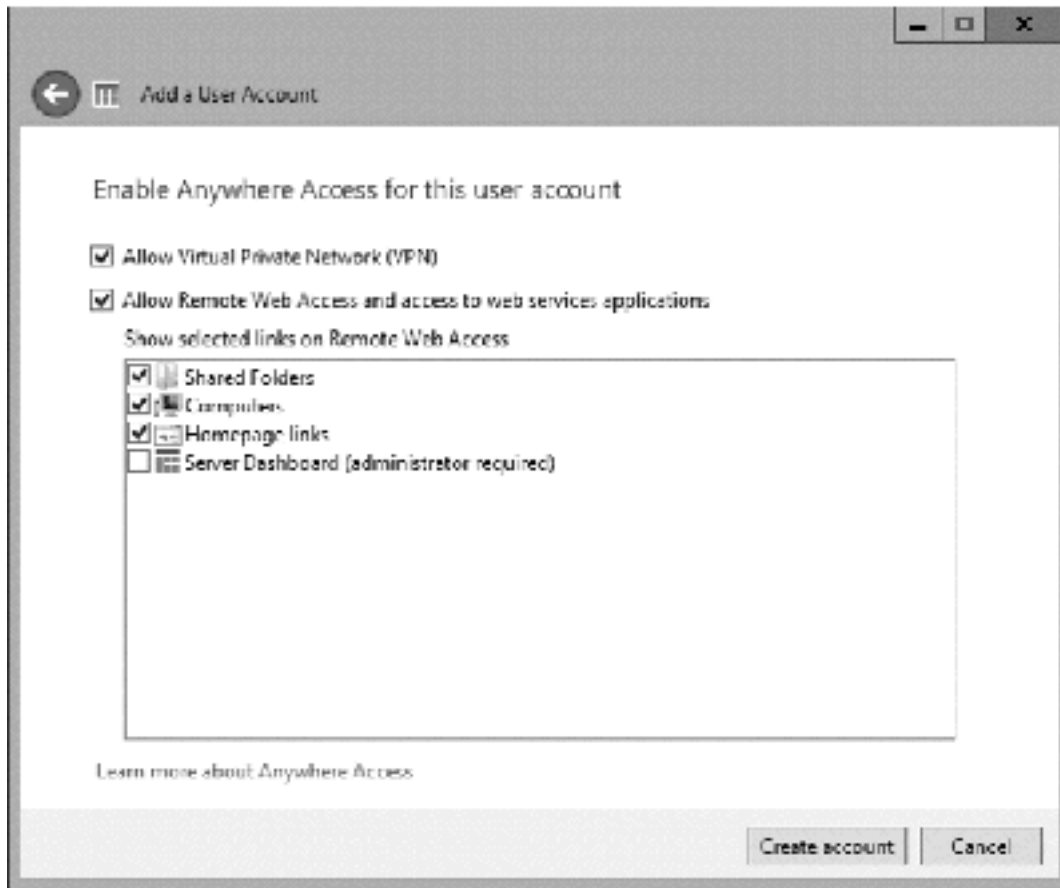
Figure 34: Specify Anywhere Access for user

Essentials will process for a few seconds and then display the confirmation that the user has successfully been created:
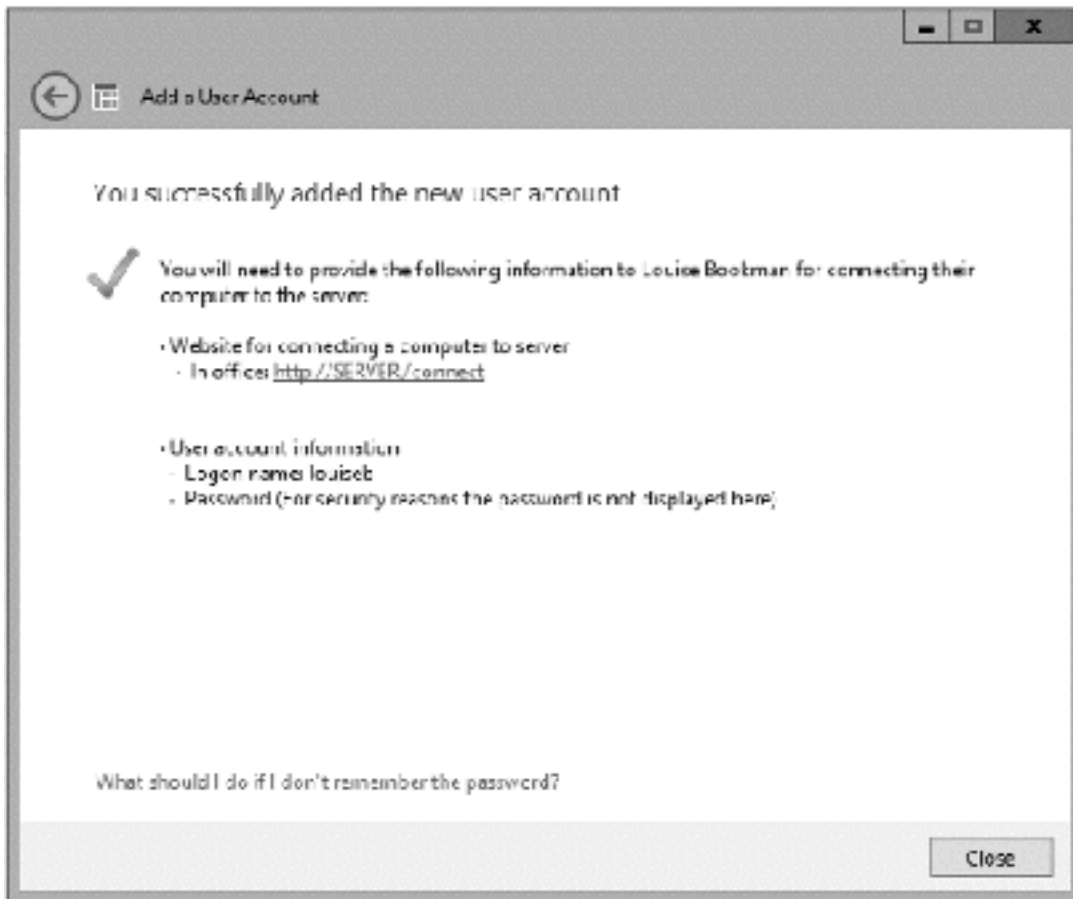
Figure 35: Confirmation of new user account

Check the details then click **Close**. Continue creating all the users in the same way. Essentials allows a maximum of 25 users to be created.

3.4 Managing Users

To change a user's password, go into the Dashboard and click the **USERS** tab. Click the user's name to highlight it. On the right-hand panel click **Change the user account password**. Enter the old and new passwords and click **Change Password**.

To delete a user account, go into the Dashboard and click the **USERS** tab. Click on the user's name to highlight it. On the right-hand panel click **Remove the user account**. Acknowledge the message about the implications of doing so.

To temporarily disable a user – for instance, because they are going on extended leave or because of a disciplinary or security issue - go into the Dashboard and click the **USERS** tab. Click on the user's name to highlight it. On the right-hand panel click **Deactivate the user account**.

3.5 Folder Redirection

Each user has a personal folder ("home folder") on the server, accessible from any computer they login from. However, anything saved in the user's standard *Documents* folder remains in that folder on the machine they created it on, which is not very useful when people are moving around and sharing computers. Ideally, what is required is that the data "follows people around" and Essentials can be configured to do this using a feature called *Folder Redirection*. This is enabled using *Group Policy*. Group Policy is a more advanced feature used in regular versions of Windows Server but Essentials has a wizard to simplify the process for some specific tasks.

Go into the Dashboard and click **DEVICES**. In the Computers Tasks section, click **Implement Group Policy**. The following panel is displayed; simply click **Next**:
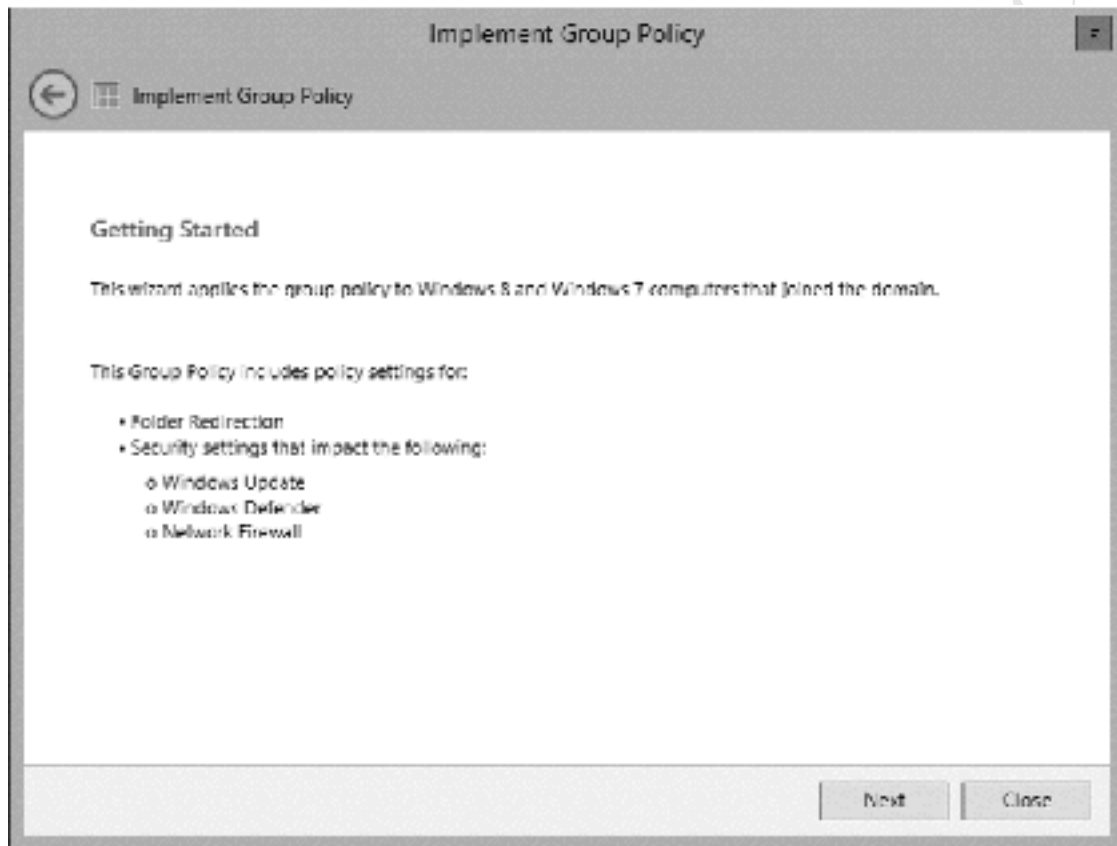

Figure 36: Implement Group Policy

The subsequent screen wants to know which folders should be redirected. Make sure all of them are ticked and click **Next**:
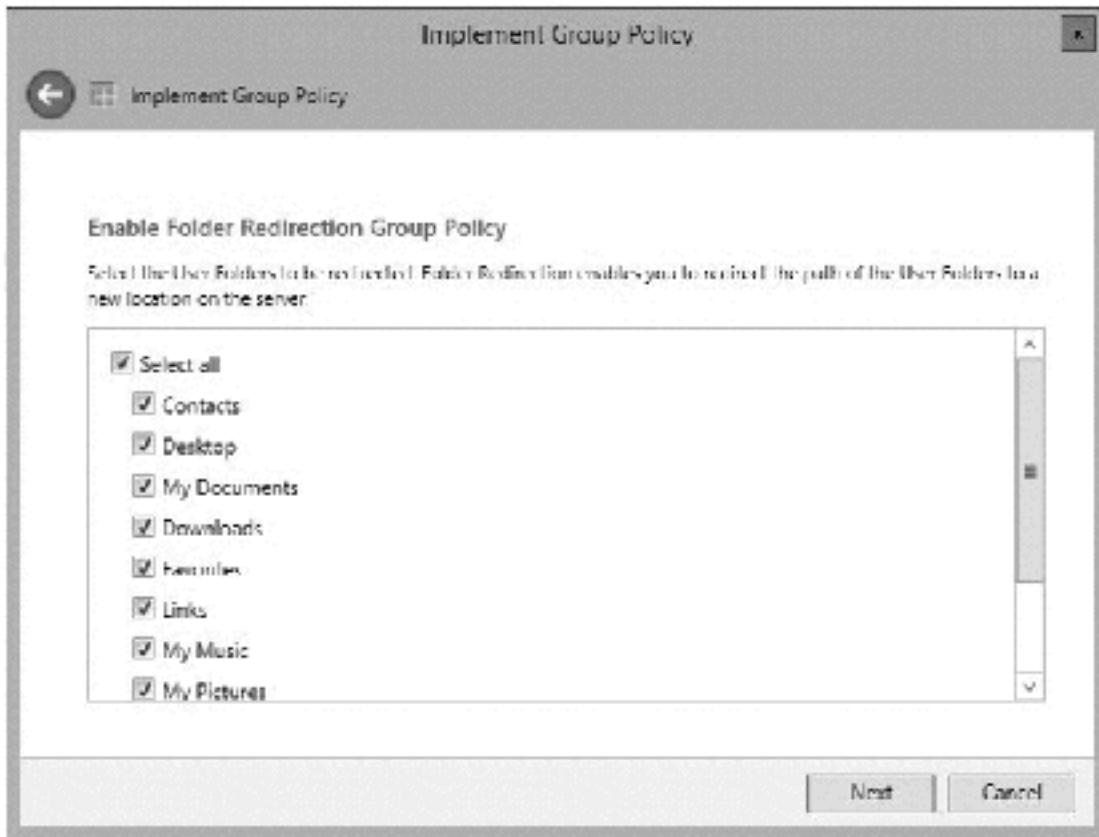
Figure 37: Enable folder redirection Group Policy

Besides redirecting the personal folders, various security policies can also be switched on to force computers to take Windows Updates and so on. If you have a third-party anti-virus program installed e.g. AVG, McAfee, Norton etc., remove the tick from Windows Defender and Network Firewall, else leave everything ticked for maximum protection. However, some people find constant Windows Updates annoying, preferring instead to run them on a manual basis once a month or so. If you prefer this approach, do not tick the Windows Update box. Click **Finish**.
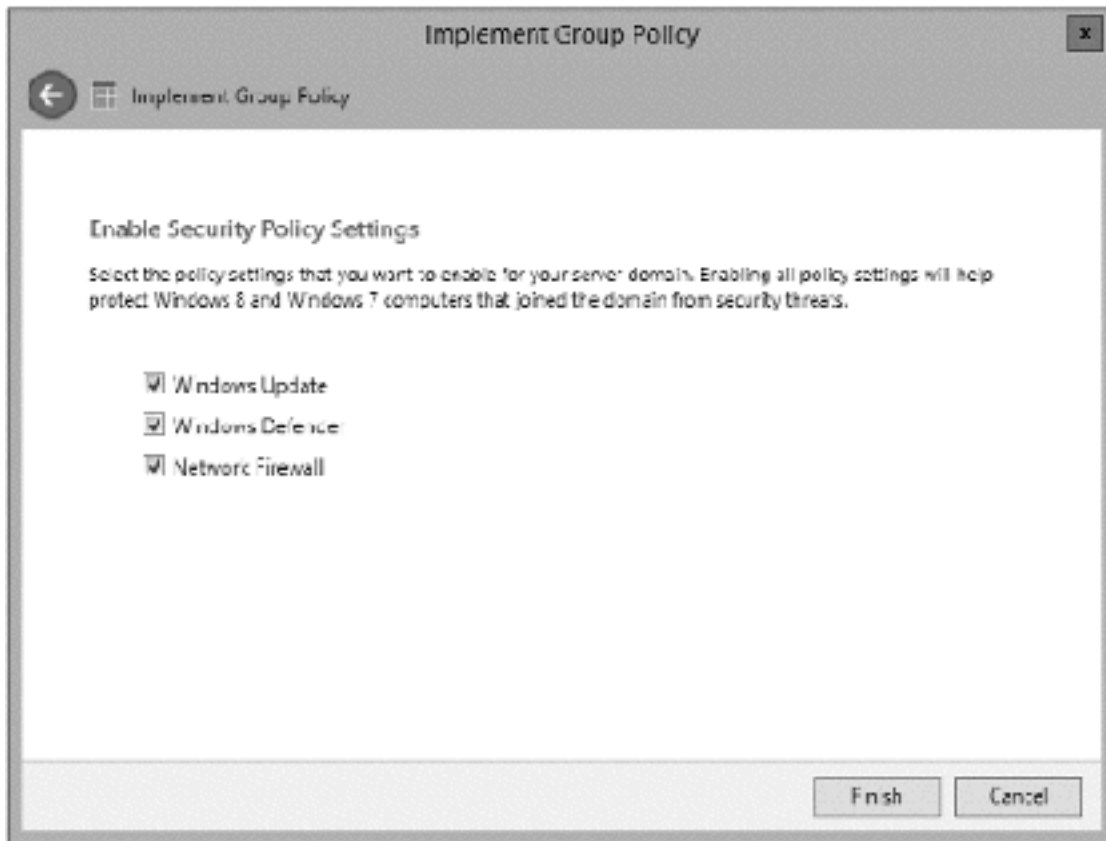
Figure 38: Enable Security Policy Settings

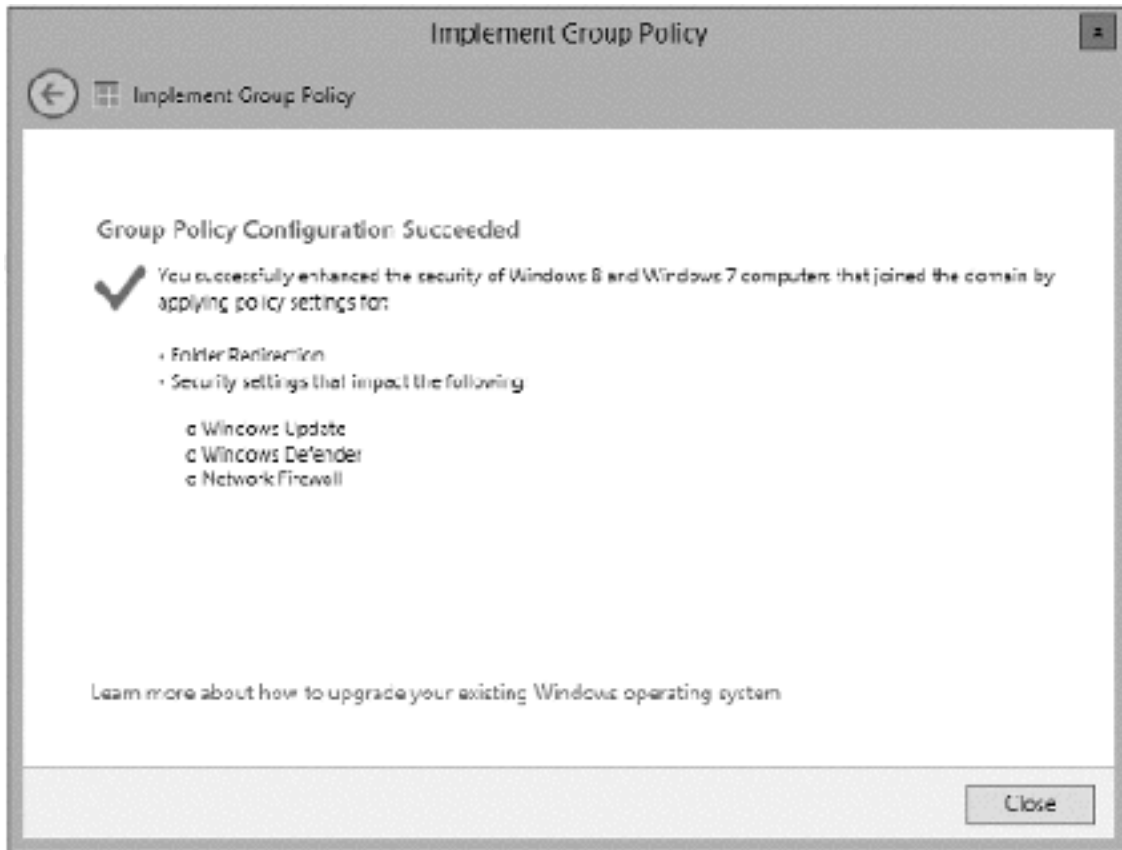After a little while, a confirmation screen is displayed. Click **Close**:

Figure 39: Confirmation screen

It is assumed that you are working through this guide in order, meaning that as yet no computers have been connected to the server as described in Chapter 4. CONNECTING COMPUTERS TO THE SERVER. If this is not the case and you are enabling Group Policy retrospectively, then note that you will have to physically restart the computers in order for them to pick up the new settings.
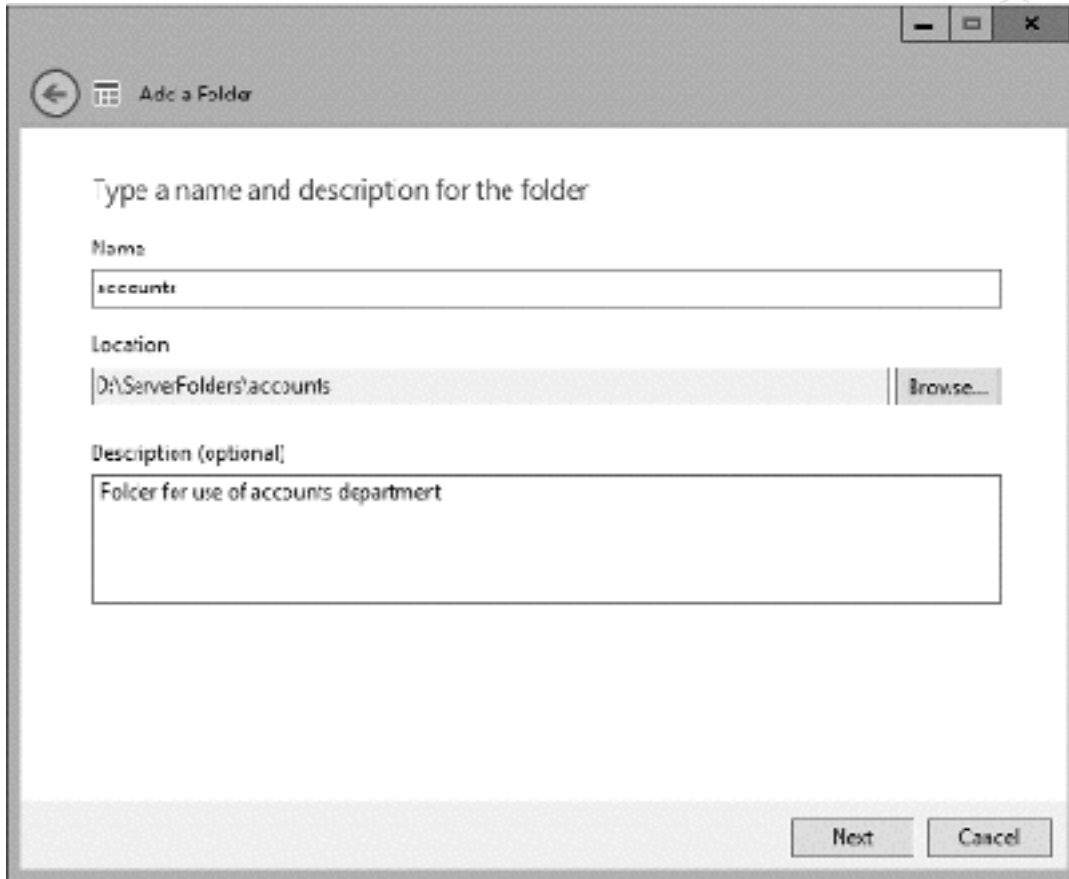
Besides setting up folder redirection, this process also simultaneously enables something called *offline folders*. The effect of this is that if a user has a laptop computer and takes it out of the office, they will still have access to the data in their Documents folder. If they make any changes, the changes will be automatically synchronized to the server when they are back in the office.

One possible consideration is if computers with low-capacity hard drives are being used. For instance, this might be the case if SSD drives are in use, as sometimes these are only of 60-120GB capacity. If users have a lot of data, or if computers are shared by multiple users, it is possible that the drives might quickly run out of space.

3.6 Creating Additional Folders

By default, Essentials provides a shared *Company* folder that everyone has access to, plus a private home folder for each individual user. Any additional sub-folders created inside the *Company* folder will also be available to everyone, but what if you need folders that are to be restricted to certain users only? For instance, there might be a need for a folder for, say, the accounts department that only the accountant and the managing director should have access to.

To do this launch the Dashboard and click **STORAGE**. On the right-hand side under 'Server Folder Tasks' click **Add a Folder**. Enter the name for the folder – let's call it *accounts*. Essentials proposes a location for it, for instance *D:\ServerFolders\Accounts*. Click **Next** to accept this:

Figure 40: Add a folder

The follow-on screen is for setting access; in this example two users will be given full access, whereas the other staff will have none at all. Use the dropdowns to define the access then click **Add Folder**:
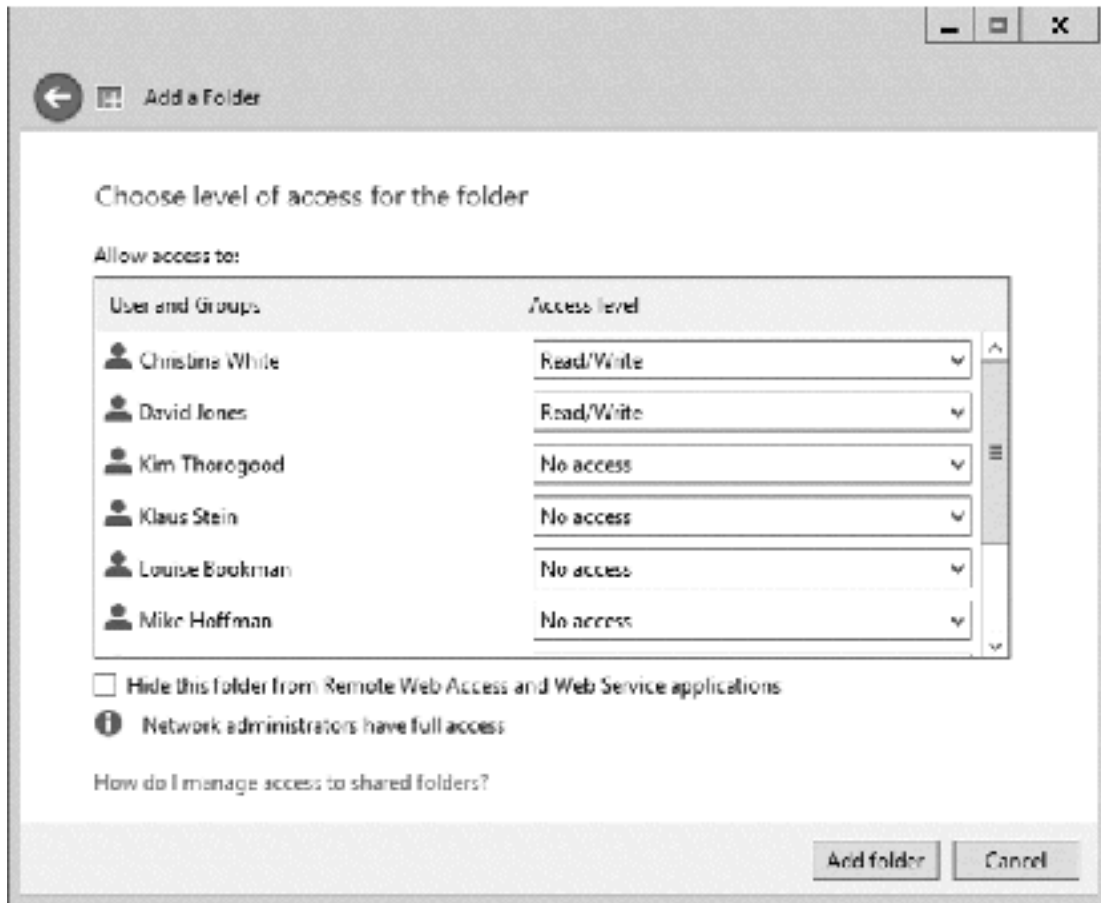
Figure 41: Specify access to folder

Upon completion, a confirmation screen is displayed advising to check the Server Backup Configuration. This is not necessary as we have yet to configure backups and, even if backups had been configured, all the Shared Folders are included in it by default. Just click the **Close** button.

3.7 User Groups

In an organization with a small number of users, specifying who has rights to folders is fairly easy to manage. But if there are more users – up to the maximum of 25 permitted by Essentials – it becomes more time consuming as you might, potentially, have to specify the level of access for up to 25 individual people. Such organizations are usually large enough that they contain departments or teams to carry out the different functions; for instance, there might be several people working in accounts, several in sales, several in marketing and so on.

To support these typical business structures, Essentials features the concept of *groups*. A group consists of a number of users who have something in common within the organization, such as they are all members of the same team. Access rights can be specified for the group, which means they then apply to all members of that group. If a new person joins the team they just have to be defined as a member of the relevant group, at which point they inherit all the relevant access rights.

To create a group, launch the Dashboard, click **USERS** and then click **User Groups** followed by **Add a new user group**. Specify a name to the group and click **Next**. On the subsequent screen, the users are listed down the left-hand side and the members of the group down the right-hand side. Click on a user to select him or her and click the **Add>>** button. To add several at a time, hold down the **Ctrl** key and click the names you want, then click the **Add>>** button. When finished, click **Next**.
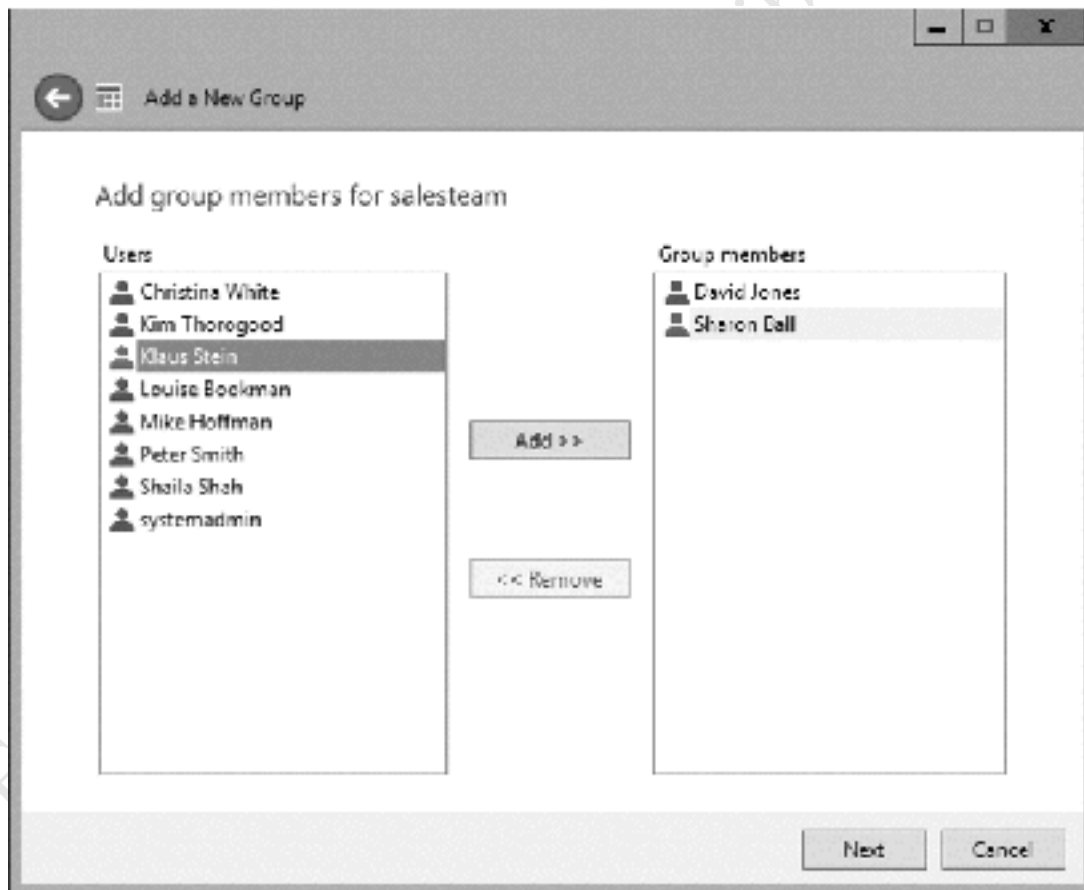

Figure 42: Specifying group members

The follow-on screen allows you to specify which shared folders the group have access to. Choose the appropriate access rights using the dropdowns then Click **Next**. This is followed by the screen that defines

what can be accessed remotely; just click **Create Account**, then close the acknowledgment screen. As can probably be appreciated these screens are substantially the same ones used to create individual users.

Having created our group, let's suppose that we want to create a shared folder just for them. On the Dashboard, click **STORAGE** followed by **Server Folders** then **Add a Folder**. Name the folder (e.g. *sales*) and click **Next**.

The next screen controls the access to the folder, the only difference being that any groups are now listed as well as the remaining individuals who are not members of any groups. Specify the desired access then click **Add folder**.
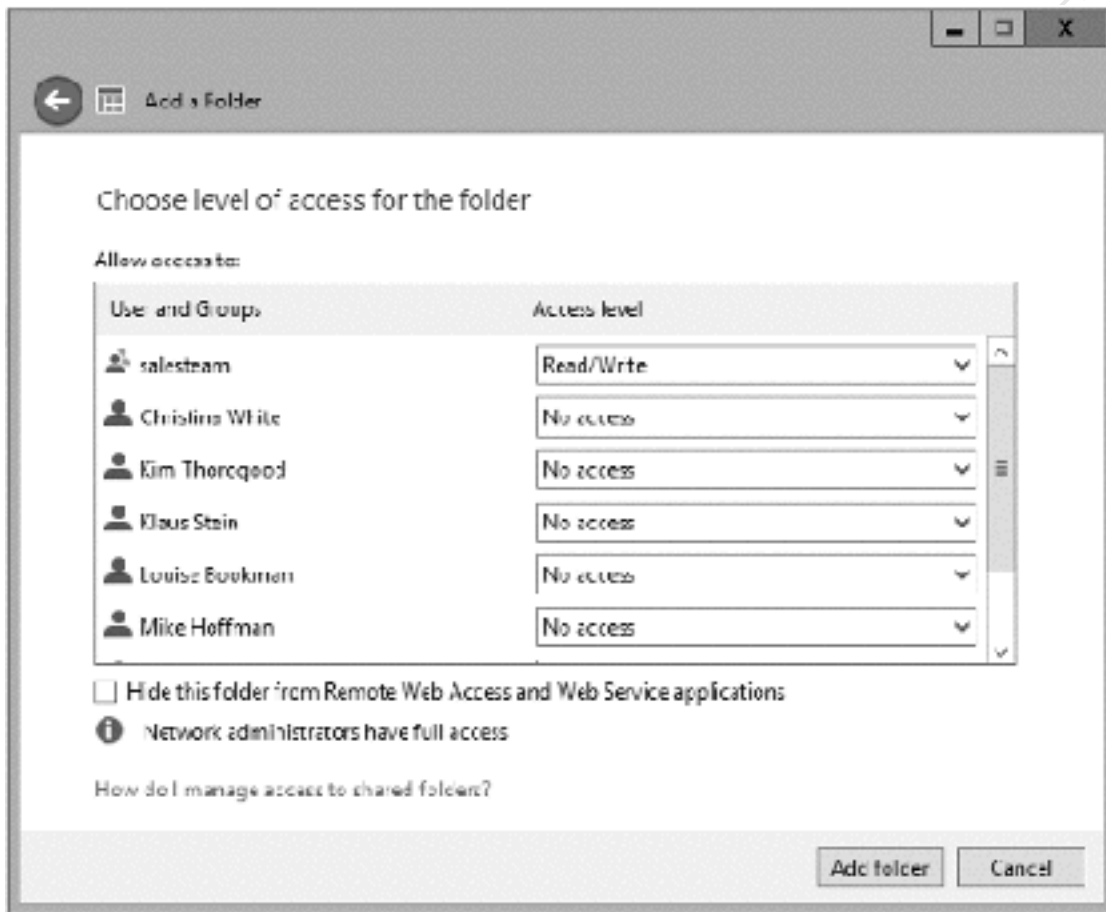

Figure 43: Specifying access to a folder

4. CONNECTING COMPUTERS TO THE SERVER

4.1 Overview

Each computer in the organization now needs to be connected to the server, a process also known to as *adding to the domain*. The key requirements are:

- The computer has to be running a Professional or better version of Windows 7 SP1, Windows 8/8.1 or Windows 10.

- It should have the latest Windows updates applied first (and if you are running Windows 10 first read section 4.4 Adding Windows 10 Computers to the Domain).

- Each computer must have a unique name within the network to identify it. It is best to follow a scheme of some description; this could be as simple as PC01, PC02, PC03 etc., or a scheme that relates to its location or function. To change the name of a Windows computer, go to **Control Panel** > **System** and click **Change settings** in the *Computer name, domain and workgroup* settings section.

- Make sure that the computer is linked to the network and has basic connectivity. It is preferable that it is wired for this stage; if you are working on a wireless laptop, temporarily use an Ethernet cable and plug it in.

- Login to the computer as a local administrator or other user with administrative rights.

Computers using Home or Starter editions of Windows cannot be connected to the domain, nor can those running Windows Vista or Windows XP (although see section 4.6 Connecting Computers with Unsupported Windows Operating Systems for a limited workaround). Apple Macs running OS X 10.6 or later can be connected – see section 4.9 Connecting Macs.

4.2 Using the Windows Server Essentials Connector

A special piece of software – the *Windows Server Essentials Connector* – is used. On the PC to be connected, load Internet Explorer and type *http://server/connect* into the Address box. If the message 'Intranet settings are turned off by default' appears it can be ignored. Click **Download software for Windows**. Click **Run** and confirm any UAC prompts that appear:
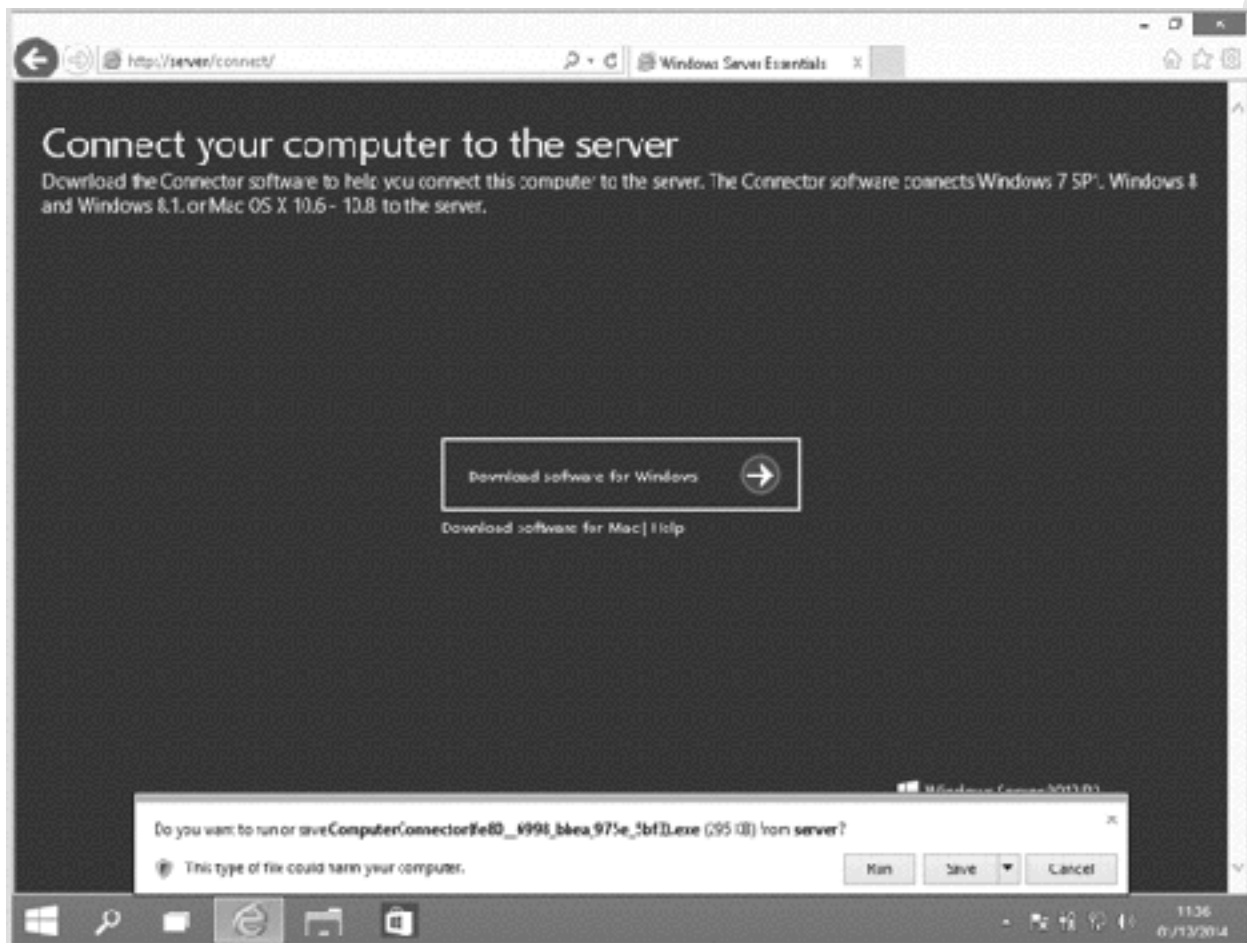

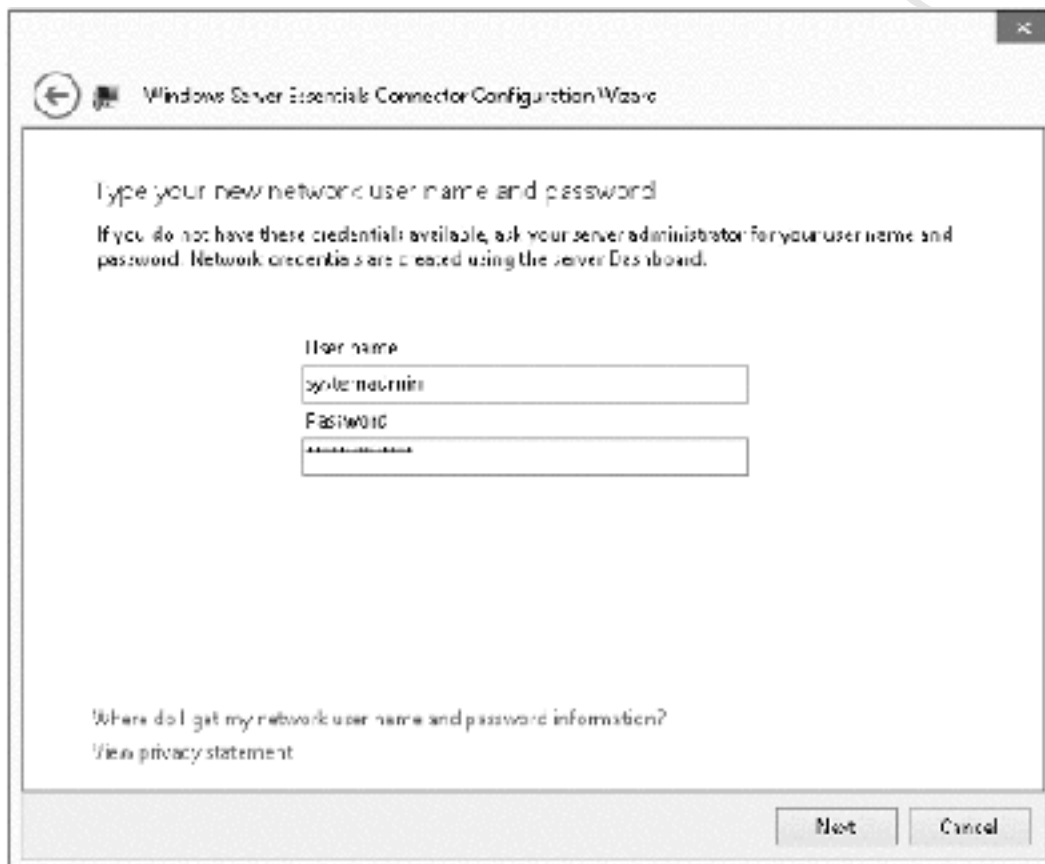*Figure 44: Download the Windows Server Essentials Connector*

Accept the license terms on the first panel and click **Next**. If the computer does not already have Microsoft's *.NET Framework 4.5* software installed it will first download and install it, which may take several minutes. The main installation of the connector software itself could take some time, potentially up to 30 minutes. Once installed, a panel will appear asking you to choose a server to connect to; usually there will only be one of course but you have to choose it anyway. Next the connector software will ask for a user name, but before providing one it is necessary to understand what is going on.

When setting up a network, there are a number of possible scenarios. The first thing to consider is whether particular computers are used individually only e.g. Mary has her own computer, Mike has his own computer and so on, or whether the computers should be viewed as resources that can in theory be used by any member of the team. The second consideration is whether the computers are new, or have already been in use for a while. Many of the questions that follow relate to these matters; if a computer has been used for a while by a particular individual then he or she is probably going to have data on it and there may be a need to preserve that data, either on the computer itself or by migrating it to the network.

If this is the case, then it is strongly advised to backup the data (e.g. to a memory stick or external USB drive) **before** proceeding as there is a chance it will be lost when the computer is connected to the server.

The best situation is where the computers are all new, or can be made as though they are new by reinstalling a fresh copy of Windows on them (for instance, which would be required if they were previously running Home editions of Windows and now need to have Professional editions installed so they can be used with Essentials). All the data should be stored on the network, in the *Company* folder or in the user's individual private folders as appropriate. Ideally there should be no data kept on the computers at all or, if this is unavoidable because there are laptops which go offsite, then the *Folder Redirection* feature described earlier will be particularly beneficial. The philosophy should be that any user can login to any computer, even if some computers are only ever actually used by one user. In the examples below, the answers reflect this scenario.

So, returning to the first screen that the Windows Server Essentials Connector displays, do not use the name of a person who will be using the computer. Instead, enter the details for the network administrator that we created earlier - *systemadmin* - and click **Next**:

Figure 45: Enter user name and password

There will be a warning recommending that a standard user rather than an administrator is being used - this can be ignored by clicking the **No** button. Restart the computer if prompted. After it has restarted, logon as the local admin user, then the following screen eventually appears. It is suggested that the first option – **Set up this computer for myself** – is chosen. Click **Next**:
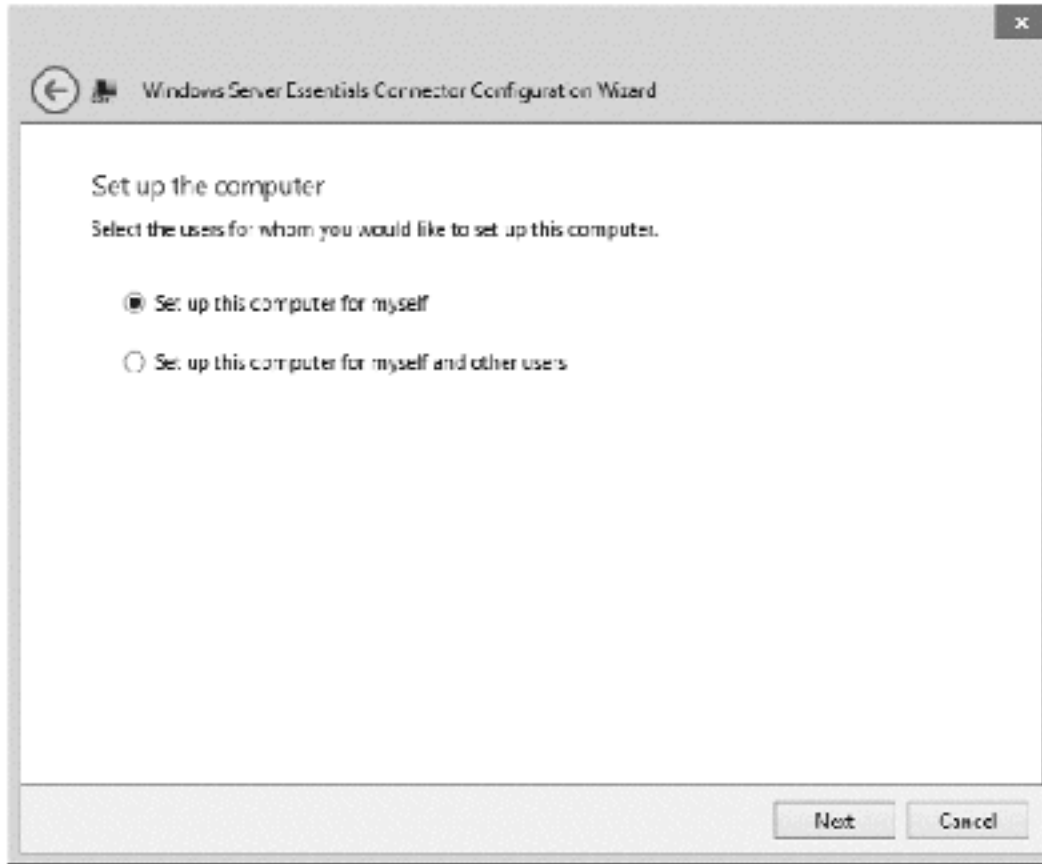
Figure 46: Setup computer screen

With the following screen you can give the computer a meaningful description (e.g. the name of the person who uses it, where it is located, an asset number etc.) then click **Next**:
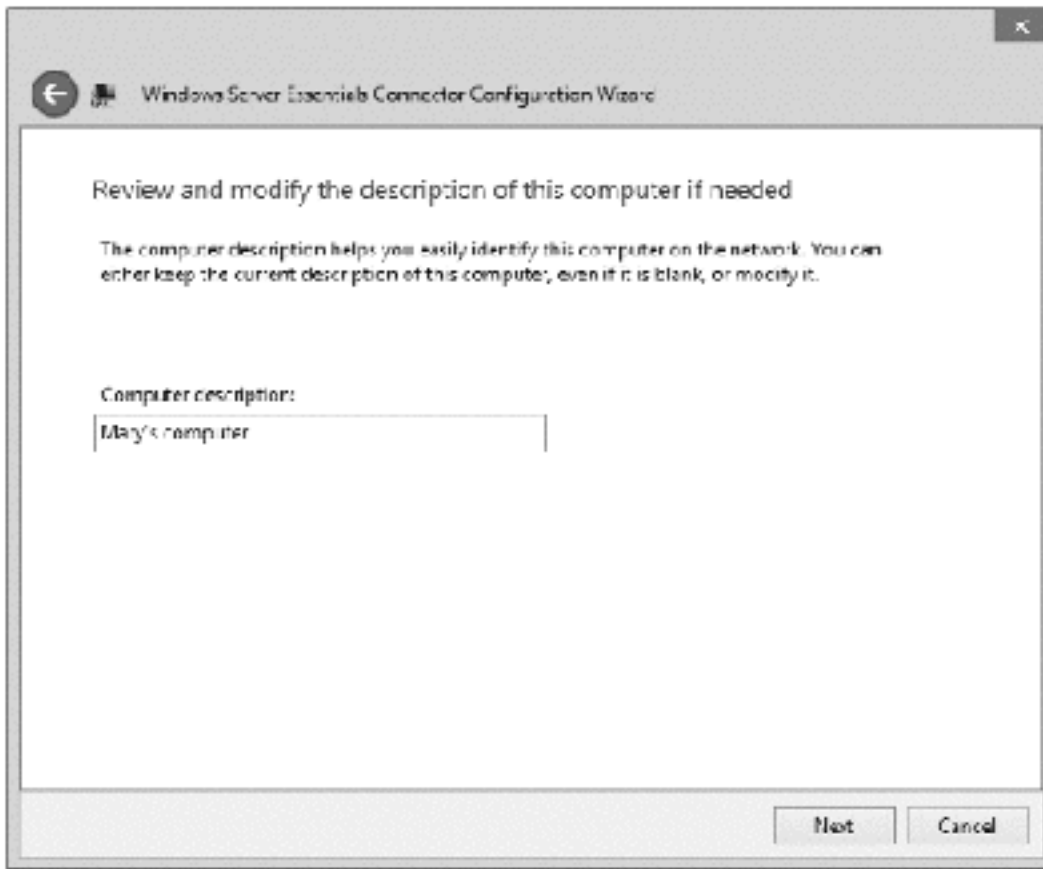
Figure 47: Description for computer

The subsequent screen is about backups. You can choose whether Essentials will 'wake up' a computer to automatically take a backup, or will only do so if the computer is already switched on. As there are quite a few considerations here, some of which are not immediately apparent and are technical in nature, choose **No, only back up this computer if it is turned on** then click **Next**:
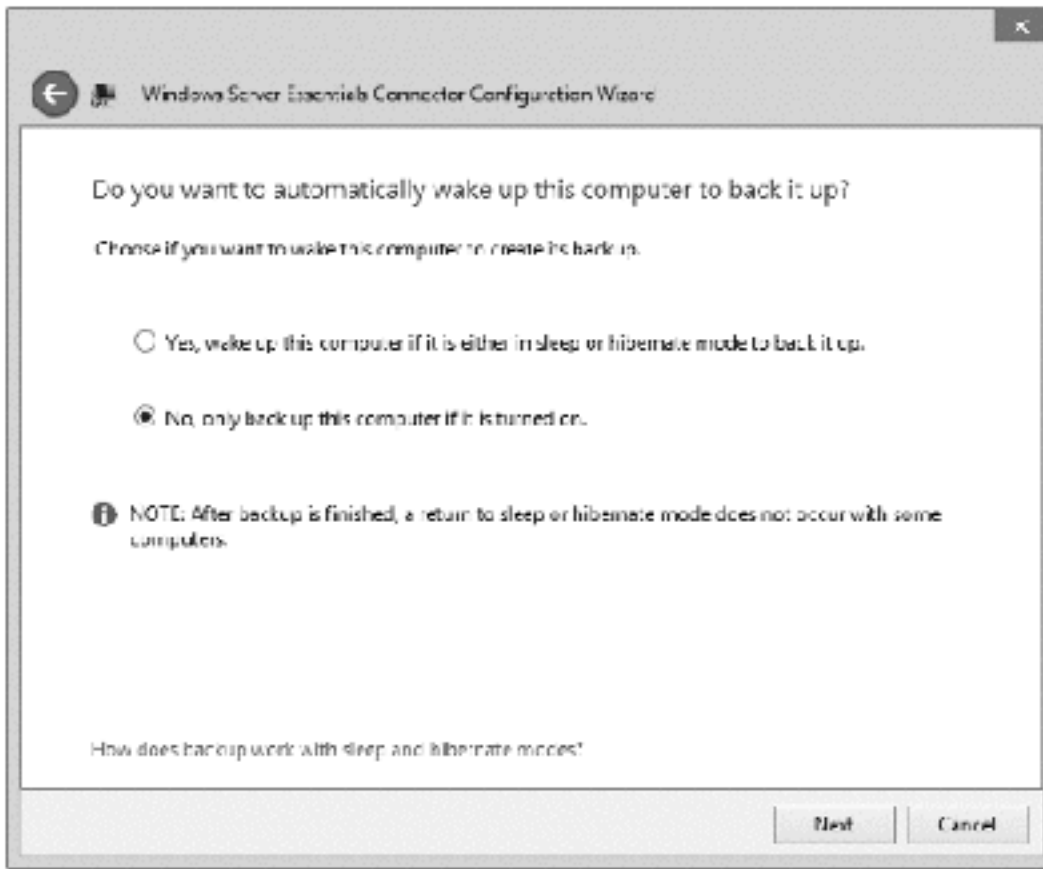
Figure 48: Wake-up computer for backups

When complete, a confirmation screen that the computer has been connected to the server is displayed. Click **Finish**. The computer will logoff; thereafter it can be used by anyone who has been defined as a user on the server.

4.3 Troubleshooting the Windows Server Essentials Connector

If the Windows Server Essentials Connector does not work, you may have a DNS issue. This is quite common in an environment where internet connectivity is provided through an all-in-one router that also provides DHCP and DNS services. The easiest fix for this is to explicitly force the client computers to point to the server for DNS. To do so, go into the network adapter settings for each PC (**Control Panel** > **Network and Sharing Center** > **Change Adapter Settings** in most versions of Windows). Click the **Use the following DNS server addresses** option and for the **Preferred DNS server** specify the IP address of the file server. This will cause DNS lookups to initially go through the server rather than the router.

If you are unable to download the Connector software from the server, try specifying the IP address of the server rather than its name e.g. instead of typing *http://server/connect* try *http://192.168.1.253/connect* (specify whatever IP address you are using).

It may also be the case that an updated version of the Connector software that fixes some problems is available but has not been picked up by the server. Go to the Microsoft website and check if an updated version is available; if it is, download it onto the computers and run it locally.

If the Connector cannot be made to work, use the instructions in section 4.7 Adding a Computer to the Domain without using the Connector.

4.4 Adding Windows 10 Computers to the Domain

At the time of writing, the Windows Server Essentials Connector software as shipped is not fully compatible with computers running Windows 10. The workaround is to manually download update KB2790621 from Microsoft (Google it) onto the PC, which will install the *Windows Server Essentials Connector Configuration Wizard* in the *All Apps* section of the Start Menu. Run the Wizard and you will be prompted to select the server or enter its IP address. On the next panel enter the *Systemadmin* details. Thereafter the installation largely follows the normal process as described in section 4.2 Using the Windows Server Essentials Connector

4.5 Additional Considerations When Connecting Windows 8 Clients

It is strongly recommended that any computers running Windows 8 are first upgraded to Windows 8.1, as it has many improvements over the original release and the upgrade is free from the Windows Store. There are reports of some people having difficulties in upgrading to Windows 8.1, usually to the effect that the upgrade does not appear in the Windows Store. The usual resolution is to ensure that the Windows 8 machine has all possible updates applied first and it is sometimes necessary to run Windows Update several times.

When connecting Windows 8 clients, it is suggested that this is done using the standard version of Internet Explorer run from the Desktop, rather than the full screen 'app' version. Anecdotally, connecting a Windows 8 client sometimes seems to take longer than connecting a Windows 7 client. It is also the case that the first login can take an inordinate amount of time.

Provided the computer is running Windows 8.1, the user has the ability to disable the Start Screen and instead login directly to the Desktop. This is done as follows. Go to the Desktop. Right-click on the **Taskbar** and choose **Properties**. Go to the **Navigation** tab. In the Start Screen section, tick the **When I sign in or close all apps on a screen, go to the desktop instead of Start** box. You may also want to tick the **Show my desktop background on Start** option. Click **OK**, then restart the computer. Note that this setting applies only to the user who actioned it and does not disable the Start Screen for everyone who uses the computer.
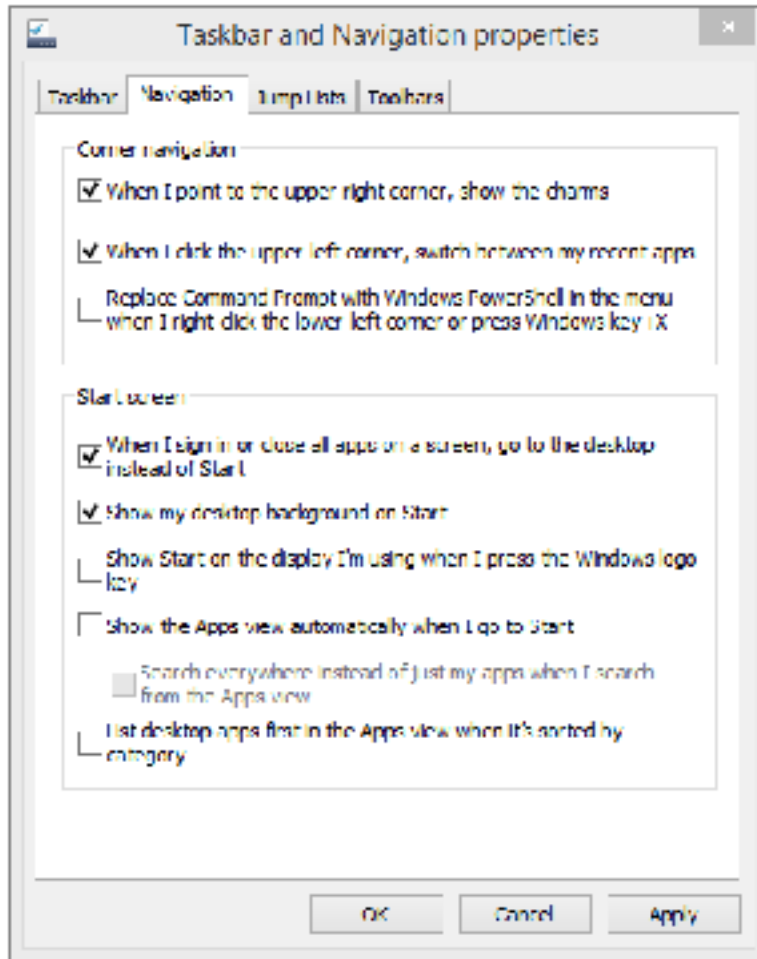
Figure 49: Taskbar and Navigation properties

4.6 Connecting Computers with Unsupported Windows Operating Systems

Officially, only computers running Windows 8, Windows 8.1 or Windows 7 SP1 (or modern versions of Mac OS X) can be connected to an Essentials server. However, it is actually possible to connect computers running unsupported versions of Windows such as Windows XP, Windows Vista or Home Editions of Windows 7 and Windows 8, albeit in a simplified fashion. It is possible to access the shared data folders, but not take advantage of the specific features that Essentials offers in terms of control and backup (technically speaking, unsupported computers can be workgroup members but cannot join the domain).

To connect a computer running an unsupported version of Windows, click **Start** (or right-click **Start** in Windows 8.1 or Windows 10) and choose **Run**. Alternatively, hold down the **Windows key** and the **R key** simultaneously. In the dialog box that appears, type *\\server* or ** followed by the IP address of the server (e.g. *\\192.168.1.251*). The user will be prompted to enter their user name and password; if they are the only person that uses that particular computer tick the **Remember my password** or **Remember my credentials** box:
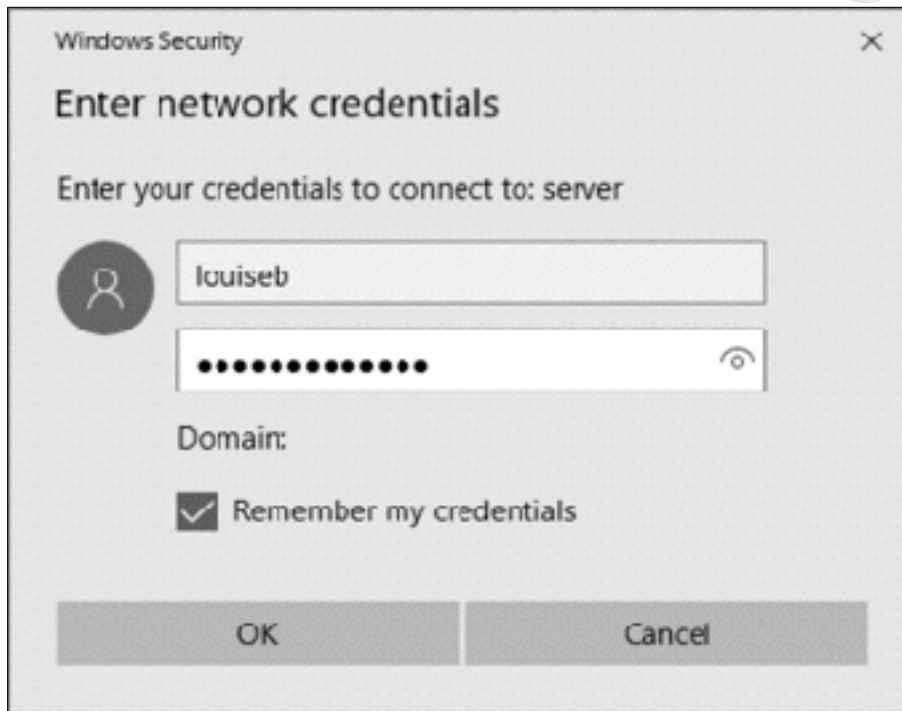

Figure 50: Enter user name and password
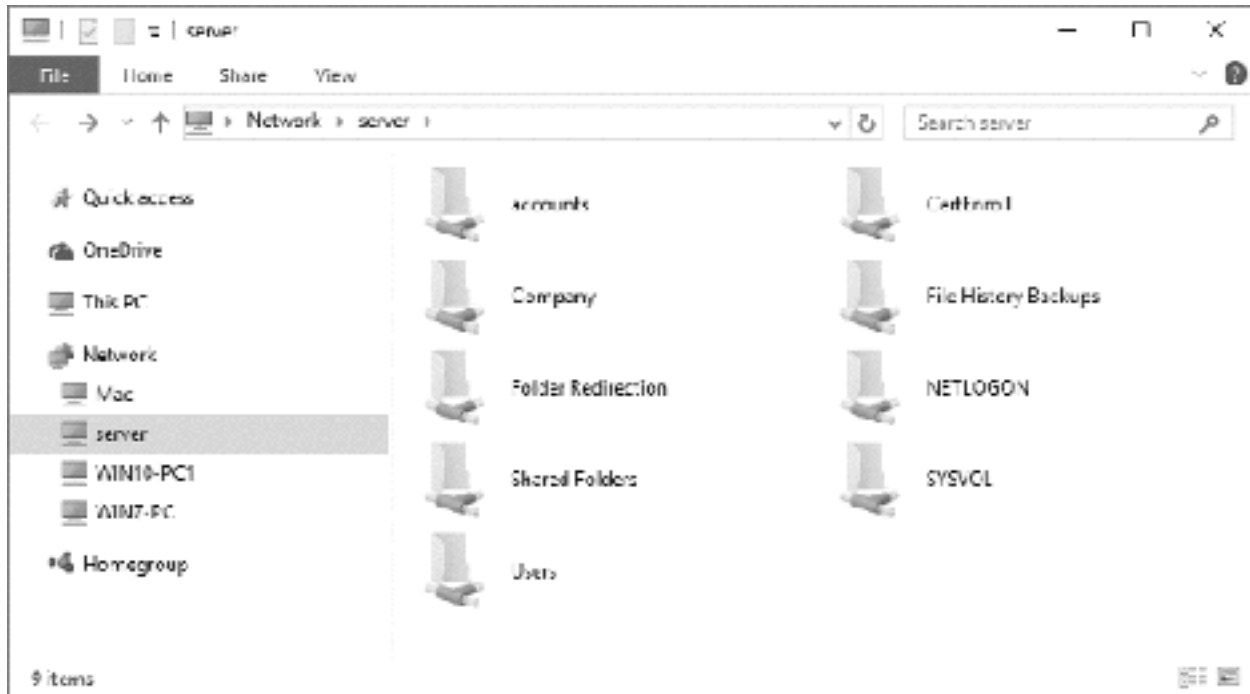
A list of shared folders on the server will be shown:

Figure 51: List of network folders

The user can work with any of the folders to which they have been granted access (for example, the *Company* folder). To access their home folder, double-click the *Users* folder then double-click the folder that has the same name as their user name. Note that although they can see the names of other people's home folders, they will not be able to access them because of security restrictions.

4.7 Adding a Computer to the Domain without using the Connector

It is not strictly necessary to use the Windows Server Essentials Connector software in order to connect a computer. If you have previous experience of setting up Windows Server networks you will probably be aware of the traditional 'Connect to a domain' method and this does still work with Windows Server Essentials. However, it does have some implications, most specifically that the computer will not be known to the Dashboard for management purposes and that the Launchpad and Backup capabilities will not be added to it. Additionally, it will not be possible to access the computer remotely using the Access Anywhere feature discussed in section 7.3 Controlling Anywhere Access for Individual Users. Given that this is case, why would you choose to connect in this way? The answer is that in some rare circumstances the Connector software, for some reason, simply does not work on a particular computer and being able to connect it at all is more important than having full access to the management tools provided by Essentials. Or, you may have purchased Essentials as a lower cost alternative to regular Windows Server and are not concerned about the backup and management features that it offers.

Connecting Windows XP Clients to the domain

- Click the **Start** button, right-click My **Computer** and click **Properties**

- Click the **Computer Name** tab

- Click the **Change** button

- Under the 'Member of' section click **Domain**. Enter the name of the domain followed by a suffix of *.local,* for example, *ctacs.local*.

- You will be prompted to enter the Administrator name and password for the domain

- After a short delay you will receive a 'Welcome to the domain' message

- Follow the instructions to restart the computer

- Check that you can logon as Administrator

Connecting Windows Vista Clients to the domain

- Click the **Start** button, right-click **Computer** then click **Properties**

- Under 'Computer name, domain, and workgroup settings', click **Change settings**. Respond to any security messages generated by UAC.

- 'System Properties' are displayed. Make sure you are on the 'Computer Name' tab

- Click the **Change** button

- Respond to any prompt for an Administrator password or confirmation

- Under 'Member of' click on **Domain**. Enter the name of the domain followed by a suffix of *.local,* for example, *ctacs.local*.

- You will be prompted to enter the Administrator name and password for the domain

- After a short delay you will receive a 'Welcome to the domain' message

- Follow the instructions to restart the computer

- Check that you can logon as Administrator

Connecting Windows 7 Clients to the domain

- Click the **Start** button, right-click **Computer** then click **Properties**

- Under 'Computer name, domain, and workgroup settings', click **Change settings**

- 'System Properties' are displayed. Make sure you are on the 'Computer Name' tab

- Click the **Change** button

- Respond to any prompt for an Administrator password or confirmation

- Under 'Member of' click on **Domain**. Enter the name of the domain followed by a suffix of .*local,* for example, *ctacs.local*.

- You will be prompted to enter the Administrator name and password for the domain

- After a short delay you will receive a 'Welcome to the domain' message

- Follow the instructions to restart the computer

- Check that you can logon as Administrator

Connecting Windows 8.1 Clients to the domain

A couple of considerations apply when using Windows 8. Firstly, when installing or configuring Windows 8, specify that it is to use a local ID rather than a Microsoft ID. Secondly, make sure that it is running Windows 8.1 (a free upgrade from Windows 8 to Windows 8.1 is available through the Windows Store for computers running Windows 8).

- Right-click the **Start** button and choose **System**.

- Under 'Computer name, domain, and workgroup settings', click **Change settings**

- 'System Properties' are displayed. Make sure you are on the 'Computer Name' tab

- Click the **Change** button

- Respond to any prompt for an Administrator password or confirmation

- Under 'Member of' click on **Domain**. Enter the name of the domain followed by a suffix of .*local,* for example, *ctacs.local*.

- You will be prompted to enter the Administrator name and password for the domain

- After a short delay you will receive a 'Welcome to the domain' message

- Follow the instructions to restart the computer

- Check that you can logon as Administrator

Connecting Windows 10 Clients to the domain

There are two methods for connecting a Windows 10 computer to the domain: a 'classic' way which is the same as with earlier versions of Windows, plus a 'modern' way that was introduced with Windows 10. However, there is a potential issue with the latter, as Microsoft have changed it with different releases of Windows 10. For this reason, it is suggested that you use the classic method only and the modern one is

not described here. Note: it is important that the computer should have initially been setup to use a local account rather than a Microsoft account.

- Right-click the **Start** button and choose **System**.

- Under 'Computer name, domain, and workgroup settings', click **Change settings**

- 'System Properties' are displayed. Make sure you are on the 'Computer Name' tab

- Click the **Change** button

- Respond to any prompt for an Administrator password or confirmation

- Under 'Member of' click on **Domain**. Enter the name of the domain followed by a suffix of *.local,* for example, *ctacs.local.*

- You will be prompted to enter the Administrator name and password for the domain

- After a short delay you will receive a 'Welcome to the domain' message

- Follow the instructions to restart the computer

- Check that you can logon as Administrator

4.8 Disabling the Launchpad

The Launchpad is installed when a computer is connected to the server using the Windows Server Essentials Connector and is intended as an easy way for users to do 'networky' type of activities. Specifically:

- It enables a user to backup their computer to the server

- It gives a link to Remote Web Access

- It provides access to the Shared Folders on the server

- It enables the user to run the server Dashboard (provided they have administrative rights)

However, a special way to do these things is not really necessary. For instance, users already have a link to the Shared Folders via an icon on the Desktop and it is not appropriate for an ordinary user to have access to the Dashboard. In previous versions of Essentials the Launchpad was far more prominent, whereas now it has to be specifically invoked by double-clicking on its icon on the Taskbar:
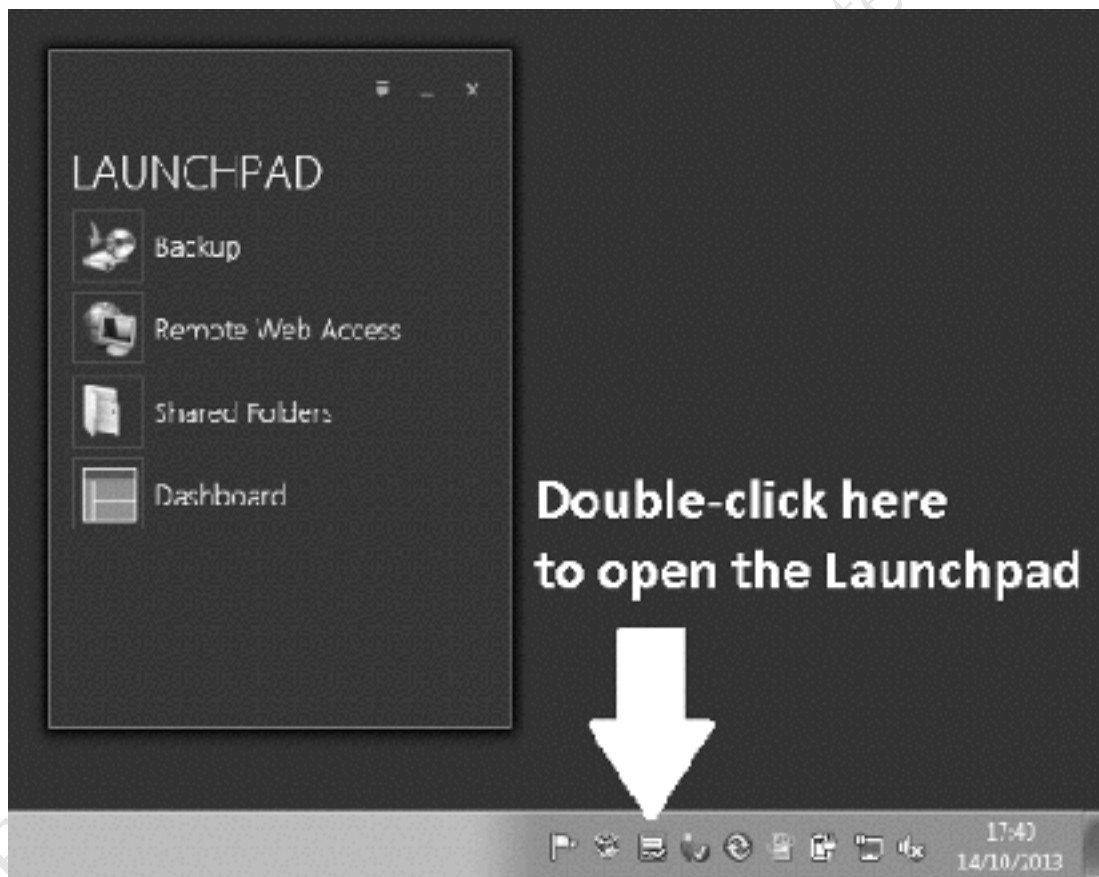
Figure 52: The Launchpad

Accordingly, there is a strong case for disabling the Launchpad altogether and there are several ways of doing so. If the computer is only ever used by one person, click on the downward chevron and choose **Settings**, then remove the tick from **Automatically run the Connector when I sign in to Windows** and click **OK**:
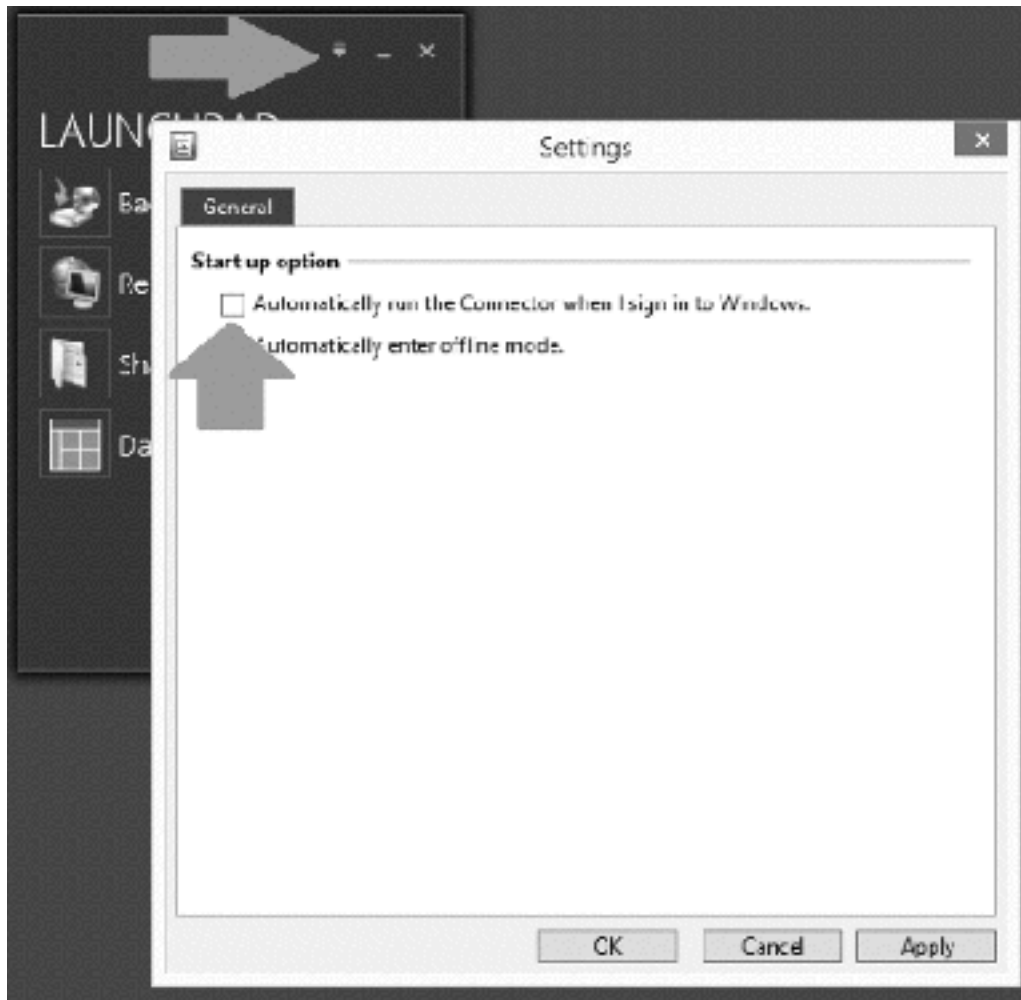
Figure 53: Launchpad Start up option

If the computer is used by multiple people, run **msconfig** (for which you will need administrative rights) and on the **Startup** tab clear the tickbox for the *C:\Windows\System32\Essentials\EssentialsTrayApp.exe* entry. It will then be necessary to restart the computer. However, note that this does not work for Windows 8/8.1.

However, one implication of removing the Launchpad is that it will prevent local backups working (see section 5.5 Configuring Backups for the Computers for information on this topic).

4.9 Connecting Macs

A special piece of software – the *Connector for Mac* – is normally used. This is the Mac analogue to the Windows Server Essentials Connector, but is less capable and not so polished. Officially, only Mac OS X 10.6 – 10.8 are supported, which are relatively old versions of the operating system. On the Mac to be connected, load Safari and enter the IP address of the server followed by the word '*connect*' in the Address box e.g. *http://192.168.1.253/connect*. When the page loads click **Download software for Mac**:
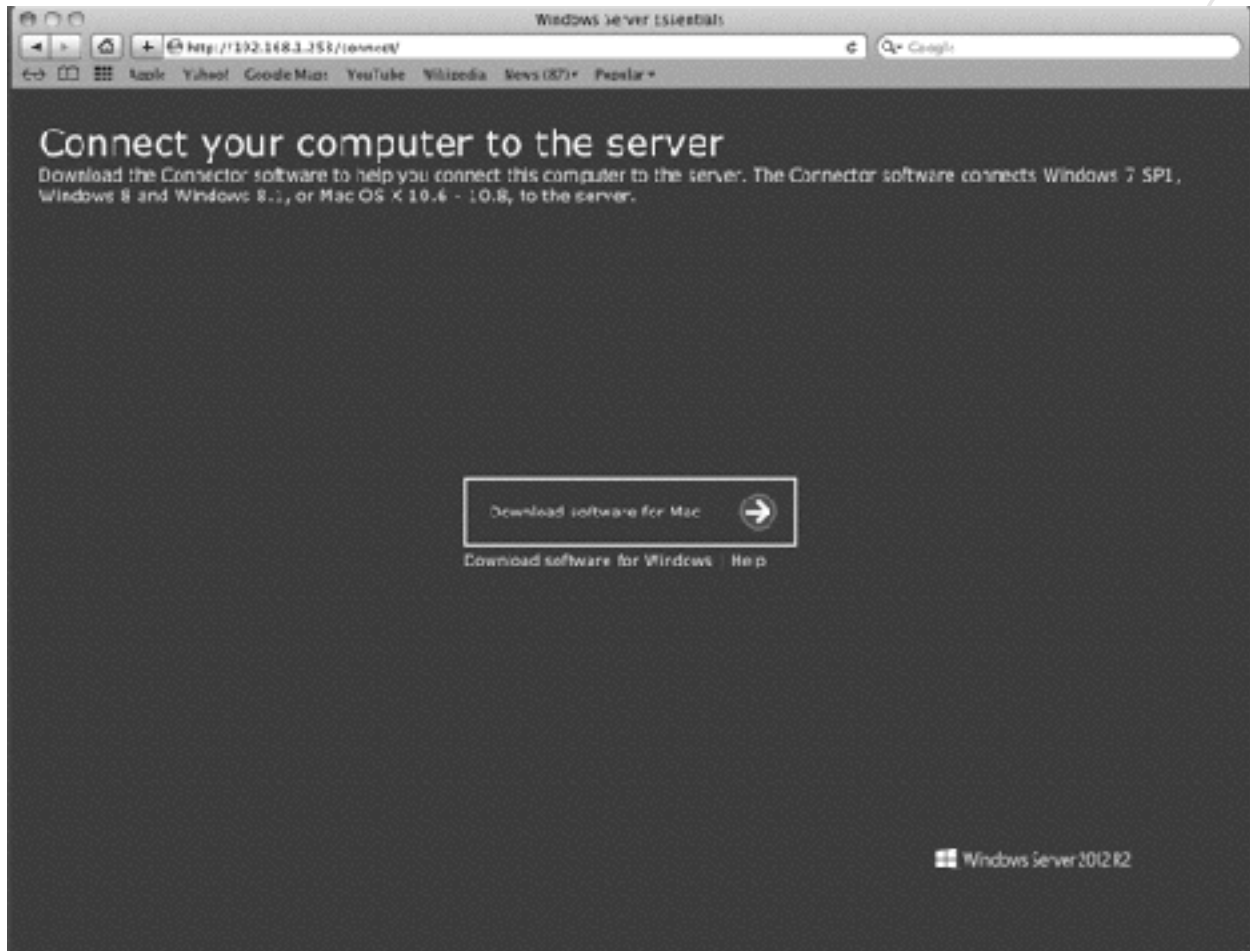
Figure 54: Download the Connector for Mac from the server

Upon completion the Connector software will be in the Downloads section, from where it can be run. You will be prompted to enter the details of a user who has authority to install software on the Mac. The first screen is just an introduction – click the **Continue** button:
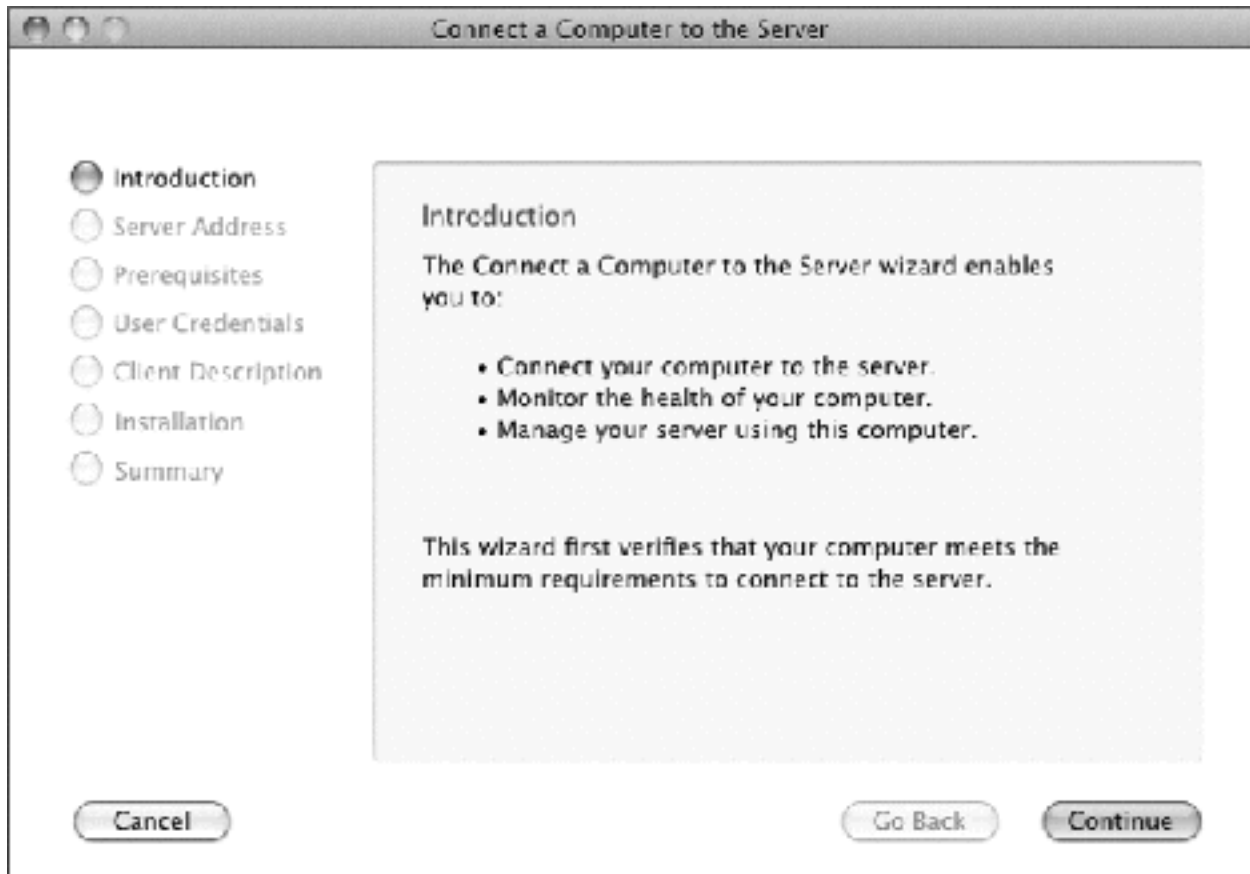
Figure 55: Initial screen of the Connector software

The second screen is ambiguous; rather than enter the name of the server you should enter its IP address then click **Continue**:
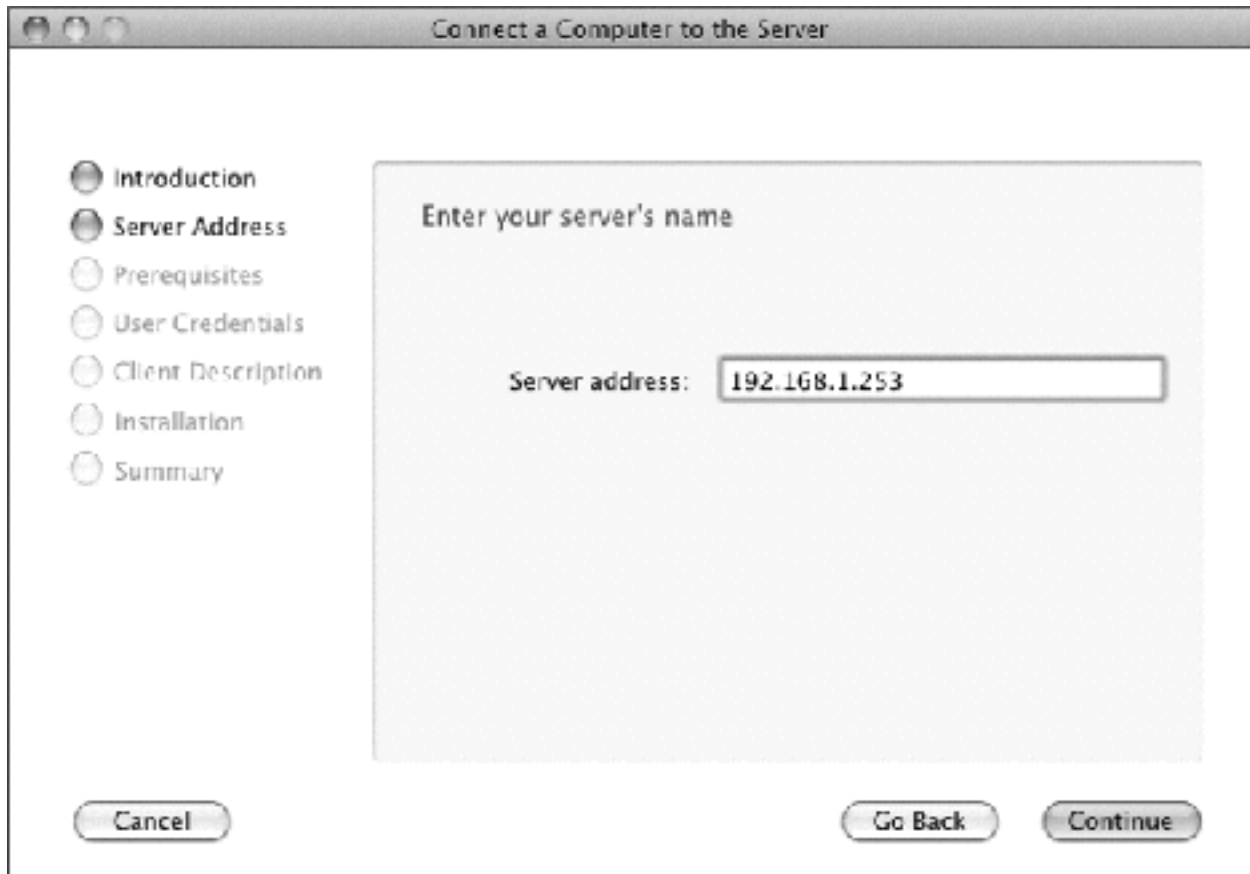
Figure 56: Enter the IP address of the server

The computer needs to have a name. You can use what is suggested or change it to something more meaningful e.g. *davidmac, marymac, louisemac* or *mac1, mac2, mac3* etc. The name should be 15 characters or less and should be letters and numbers only:
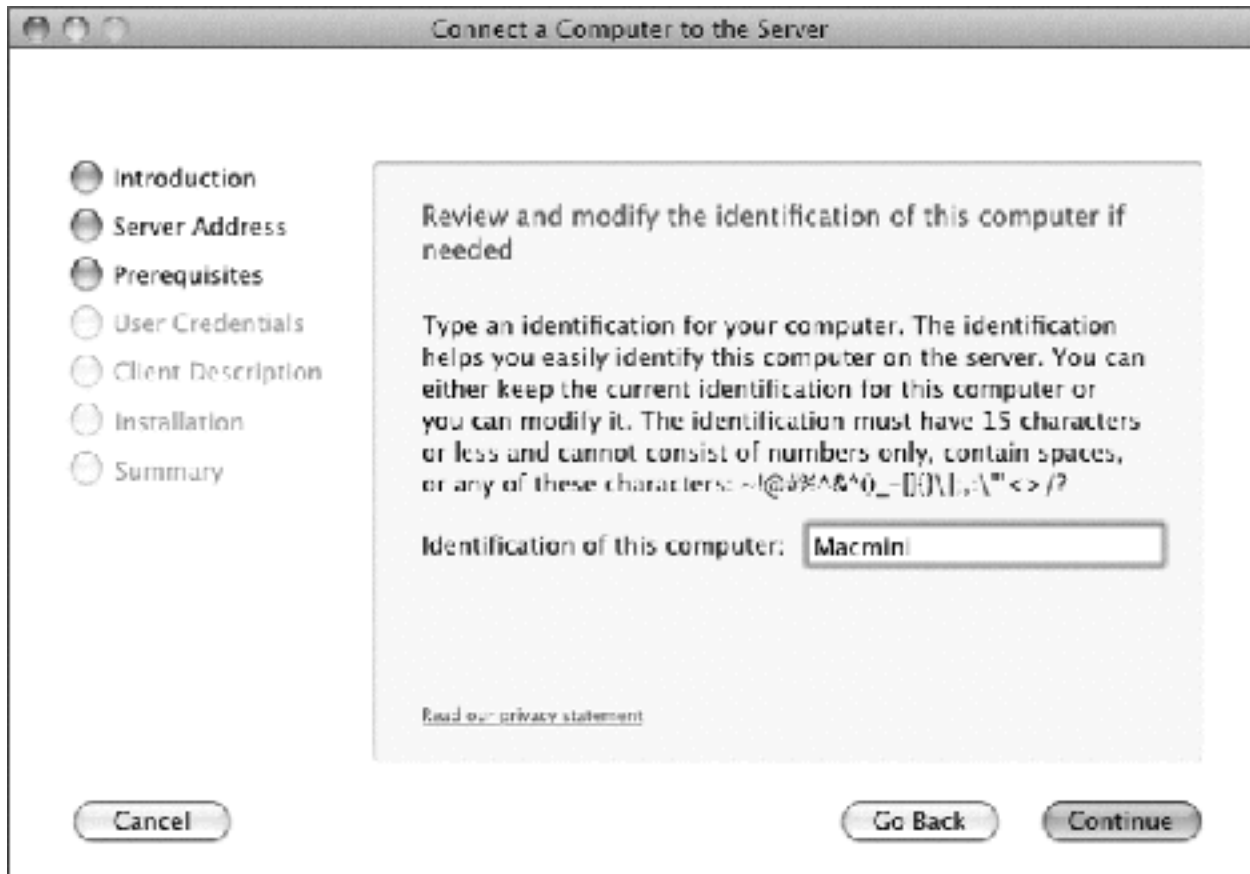
Figure 57: Give the Mac a name

The next screen is another ambiguous one – you should enter the details for the server's *systemadmin* account, not the name of a standard user:

Figure 58: Enter the details for systemadmin

The subsequent screen allows you to set a description for the computer as it will appear on the server. It is suggested that you use the same name you specified a few screens back. Click **Continue**.
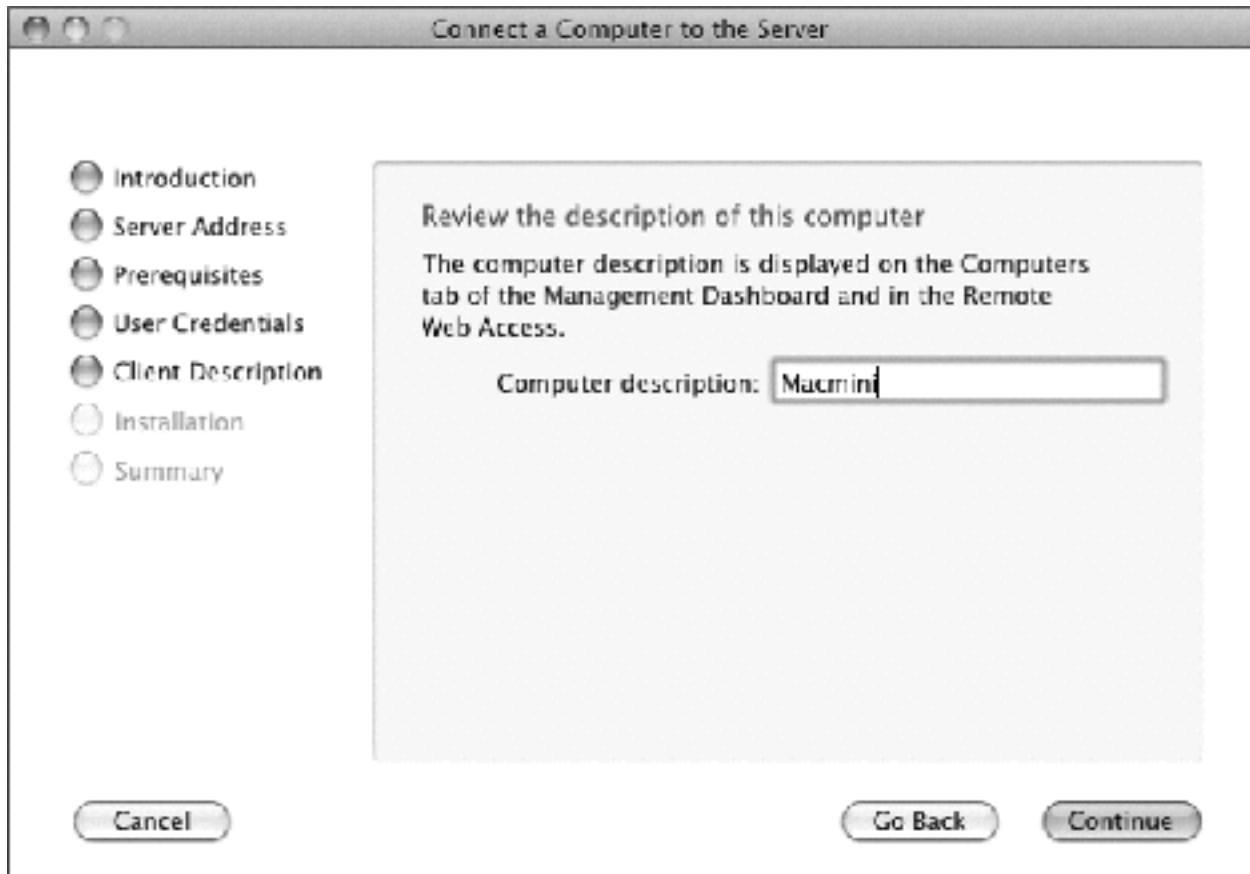
Figure 59: Review the description of the Mac

After a little while you should receive a confirmation screen that the Mac has been connected. It is suggested that you **do not** tick the box to **Automatically start Windows Server Launchpad at startup**. Click **Close**.
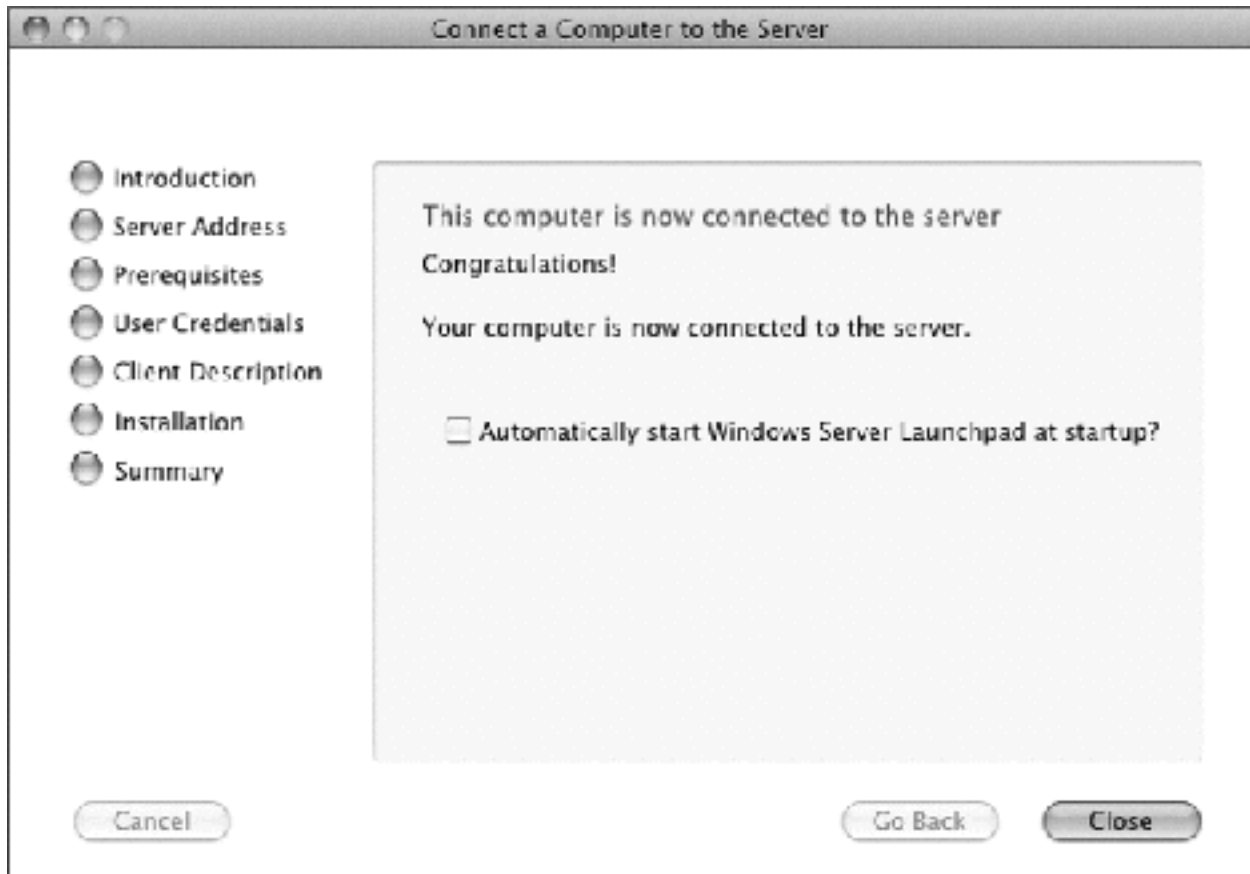
Figure 60: Confirmation that the computer is connected

An icon for the Launchpad will have been placed in the *Applications* folder. You may wish to place it on the Dock for convenience. Upon running the Launchpad, the user has to provide their user details as previously defined on the server (see section 3.3 Creating User Accounts).

Figure 61: Logging in via the Launchpad

There are three options on the Launchpad: *Backup*; *Remote Web Access*; *Shared Folders*. The first option is for backing up the Mac to the server and seems to be generally problematic - it is therefore suggested that Mac users use a Time Capsule or other solution for this task instead. *Remote Web Access* provides access to the server from outside the office – see section 7.4 Using Remote Web Access. The third option is for accessing the server's shared folders and the one most likely to be of interest.
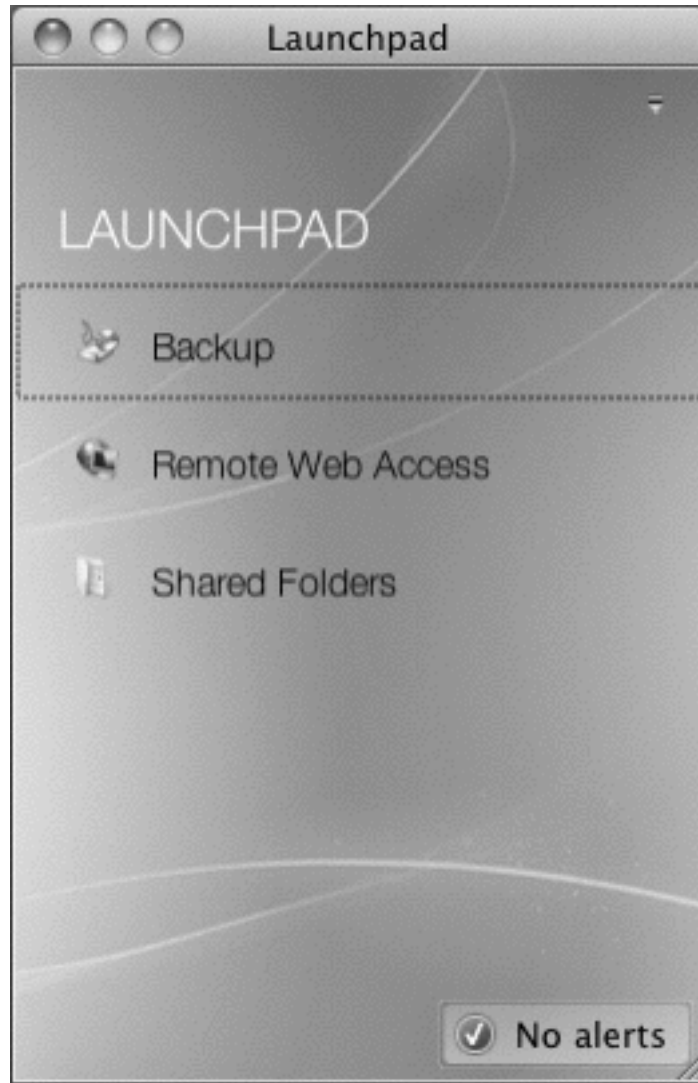
Figure 62: Mac version of the Launchpad

Click on the *Shared Folders* option. Although the user has already logged in via the Launchpad, there may be another prompt to do so again, this time generated by macOS. Enter the user name and password again and optionally tick the **Remember this password in my keychain** box:

Figure 63: Enter the user name and password

A list of available shared folders (*volumes)* is displayed. Choose the volume to mount and click OK; or, to mount multiple volumes in one go, hold down the **Command key** and click on the required folders in turn. Note that all the shared folders on the server are listed, including ones not normally accessed by users:

Figure 64: Select the volume(s) to mount

Having mounted a volume an icon will be placed on the desktop and its contents will be displayed. From here the files and folders can be used in the normal way.

Figure 65: Example of mounted volume

4.10 Alternative Strategies for Connecting Macs

Rather than use the *Connector for Mac* software, an alternative approach is to run Windows on the Mac and access the server using that. The benefit of this is that it provides the full range of features and functionality associated with Essentials – albeit in a Windows environment - rather than just the subset offered by Connector for Mac. There are two ways of going about this:

Method One is to use Apple's Boot Camp utility. This allows a Mac to startup using macOS or Windows as required. There are two limitations: firstly, only one operating system at a time can be used. For instance, if the computer is running Windows and you want to use OS X then it is necessary to restart it. Secondly, only the most recent versions of Windows (8, 8.1 and 10) are supported on modern Macs (although older machines may be able to use Windows 7 with earlier versions of Boot Camp).

Method Two is to use virtualization software. This enables the Mac to operate as normal under OS X but to run a separate copy of Windows in its own self-contained window at the same time, as though it was just another application. This is particularly useful where a user prefers to work predominantly in a Mac environment, but also needs to connect to the Windows server. The copy of Windows can be any version – none of the restrictions imposed by the Boot Camp method apply. One possible downside is that the computer needs sufficient memory (RAM) to run both operating systems simultaneously, say a minimum of 8GB. Virtualization software is available from several sources: a well-regarded commercial program is *Parallels* from the company of the same name, whereas a free alternative is *VirtualBox* from Oracle.

Whichever method is used, a licenced copy of Windows has to be obtained and used for the installation. This needs to be a Professional edition or better.

4.11 Connecting Linux Computers

Microsoft do not provide a version of the Windows Server Essentials Connector for Linux. However, Linux PCs can be connected as Workgroup members, in much the same way as computers running unsupported versions of Windows can as described in section 4.6 Connecting Computers with Unsupported Windows Operating Systems. This is possible because Linux distributions include support for the SMB filing system used by Windows networking; this may be built-in, or can be added by downloading what is commonly described as a Samba client. In this example, we are using the popular Ubuntu Linux distribution.

On the Linux computer, click the **Files** icon, followed by **Connect to Server**. In the resultant dialog box, enter the address of the server preceded by *smb://* e.g. *smb://192.168.1.2* and click **Connect**:
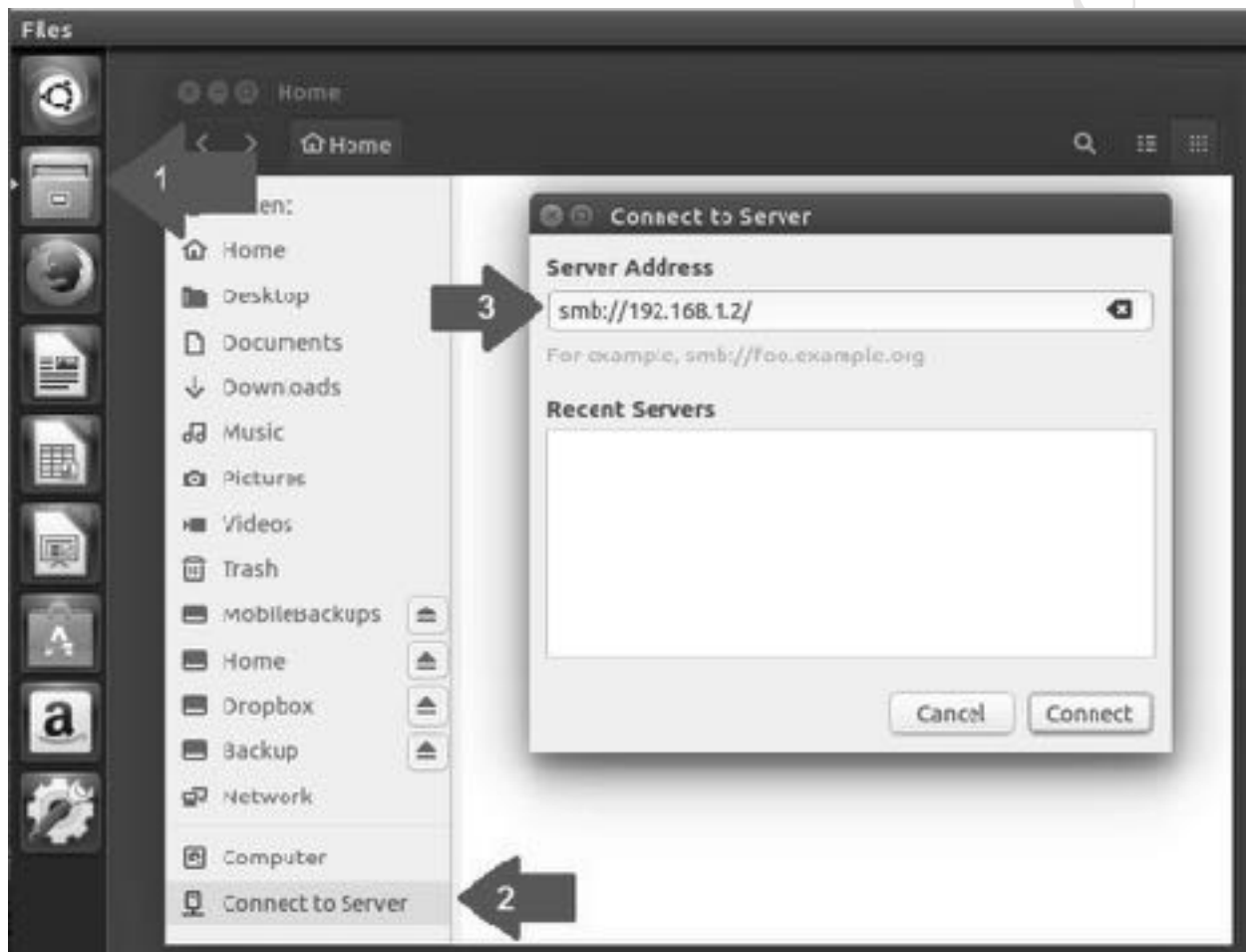
Figure 66: Enter the address of the server

On the resultant panel, enter the user's name and password as defined on the server and click **Connect** (the *Domain* can be ignored):

Figure 67: Enter the user's details

The drives and folders on the server will be listed (note that some system folders may be listed, even though they cannot and should not be accessed). To access a folder, double-click it. You may need to drill-down to find the one you want and you may be prompted to provide the username and password again, in which case do so. The folder will then open and you can use the files in the normal manner.

5. BACKUPS AND RESTORES

5.1 Overview

It is extremely important to backup data on a regular basis, in order to cope with the problems that can arise with computers. Things such as: deleting files by accident; virus infections; data corruption; computer failure; equipment being lost or even stolen. In general, the value of data far outweighs the value of computers; for instance, around half of businesses that have a serious data loss subsequently cease trading within twelve months, plus there may be statutory requirements to retain certain data in some parts of the world. The assumption to follow is that it is a question of *when* rather than *if* data will be lost at some point, which is when the backups will be needed.

The best strategy is to aim for a *3-2-1 solution*, which means: there are at least three copies of the data; they are held in at least two different formats; at least one copy is held offsite, away from the premises. This system of having multiple backups to multiple places ensures that there is always a fall-back in the event of problems. For instance:

The computers in the office are backed up to the server. The server in turn is backed up to a local USB hard drive. Optionally, the server or at least the most important data are backed up to a Cloud-based service. For an extra level of protection, the server could also be backed up to a NAS (network attached storage) device located elsewhere in the premises:
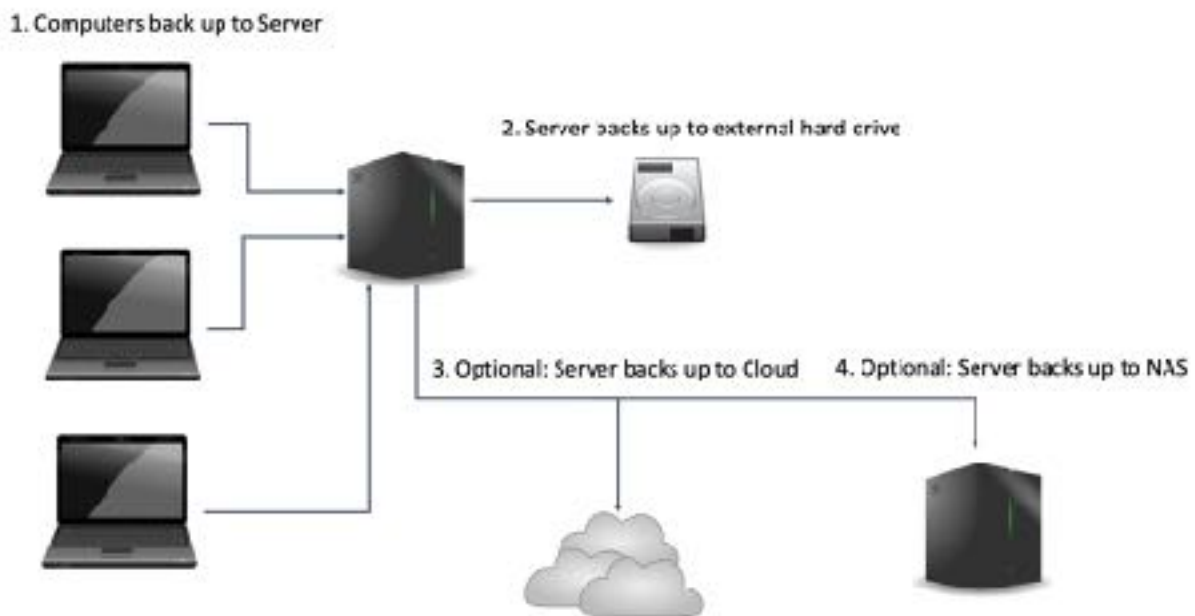
Figure 68: Multi-tiered approach to backups

5.2 Configuring Backups for the Server

The easiest way to backup the server is to use the built-in program in Essentials in conjunction with a plug-in external USB hard drive. The USB drive should be at least equal in capacity to the total amount of storage in the server e.g. if the server has 2TB disc storage then the backup drive should be at least 2TB as well. If the server has USB 3.0 ports then be sure to use an USB 3.0 drive, as the performance will be better.

Connect a suitable USB drive – note that anything already on it will be lost as it is going to be formatted. Launch the Dashboard, choose the **DEVICES** section and in the right-hand panel entitled 'Server Tasks' click **Set up Backup for the Server** to display the following screen, then click **Next**:
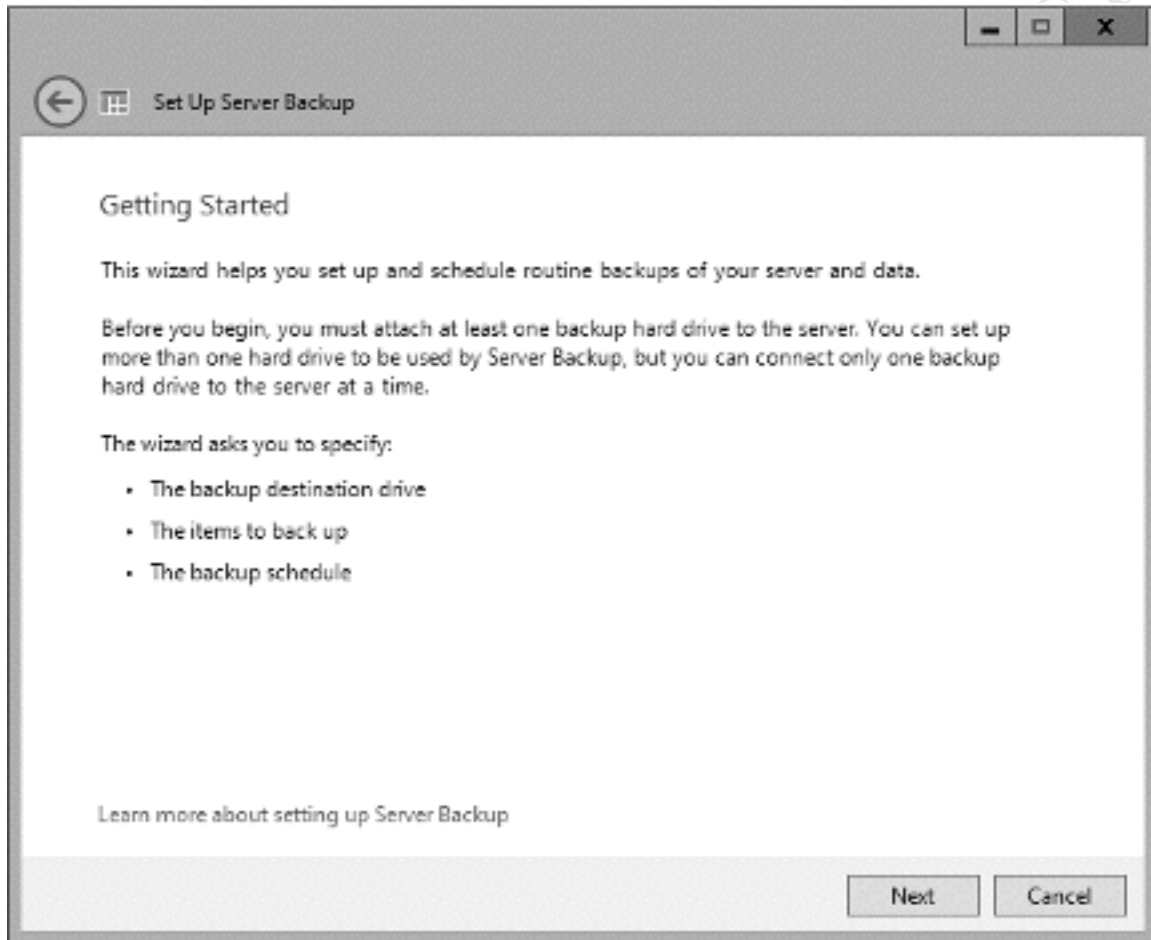
Figure 69: The Backup Wizard

The subsequent screen wants to know which disk drive should be used for holding the backups. If the USB drive does not appear, tick the **Show all drives that can be used as backup drives** box and click **Refresh List**. Once the backup drive has been selected click **Next**.
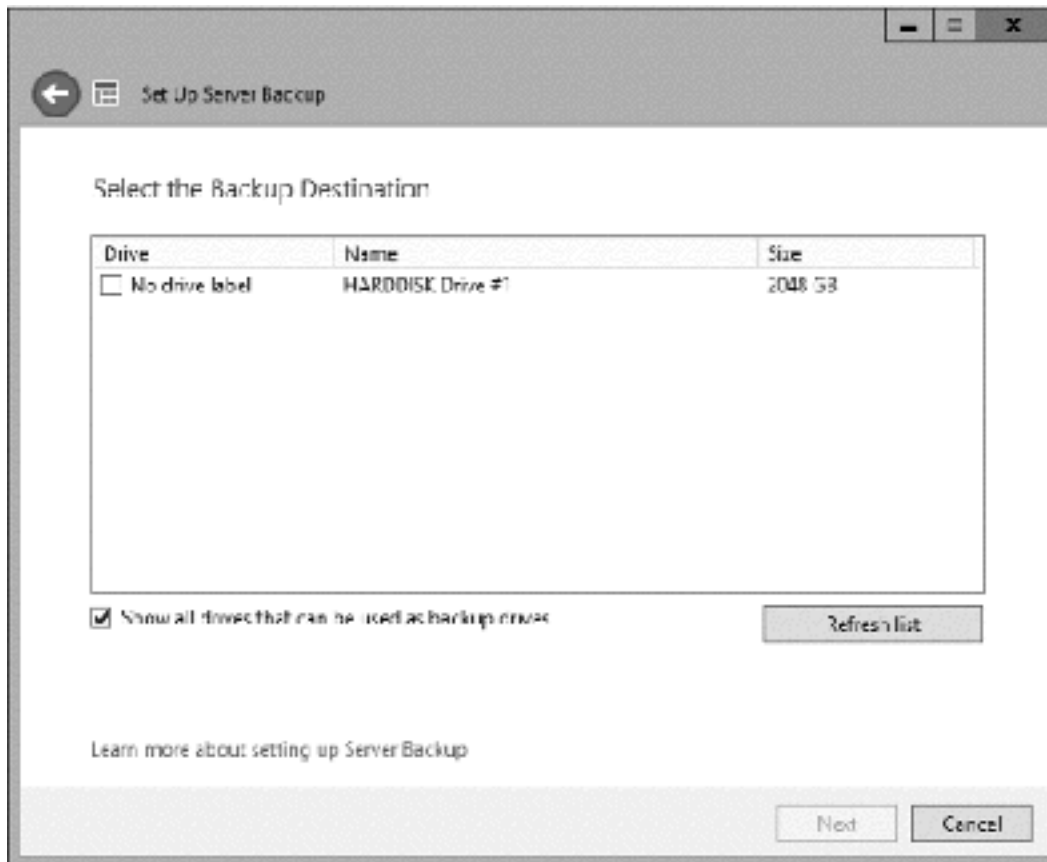
Figure 70: Select the backup destination

A message is displayed warning that the selected backup drive is about to be reformatted. This is fine so click **Yes**.
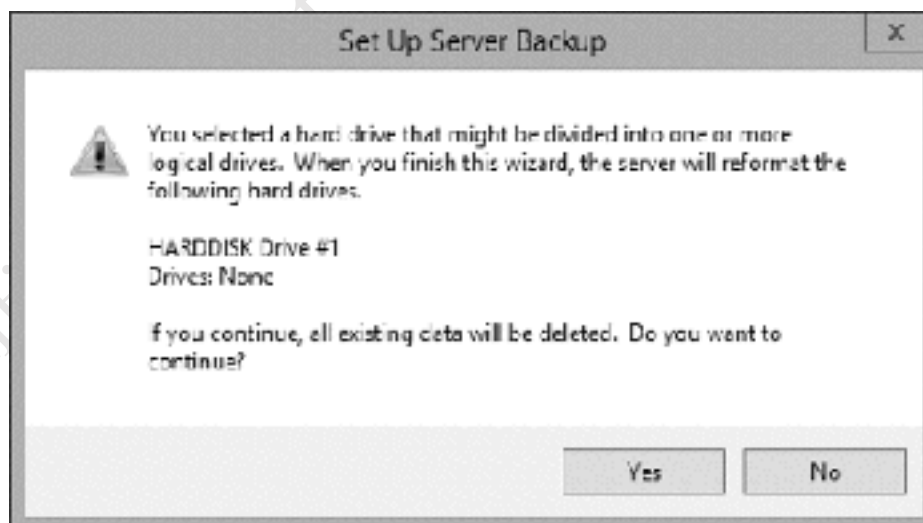
Figure 71: Message about formatting backup drive(s)

The backup drive needs to be labelled. Choose something meaningful like *SERVERBACKUP*:
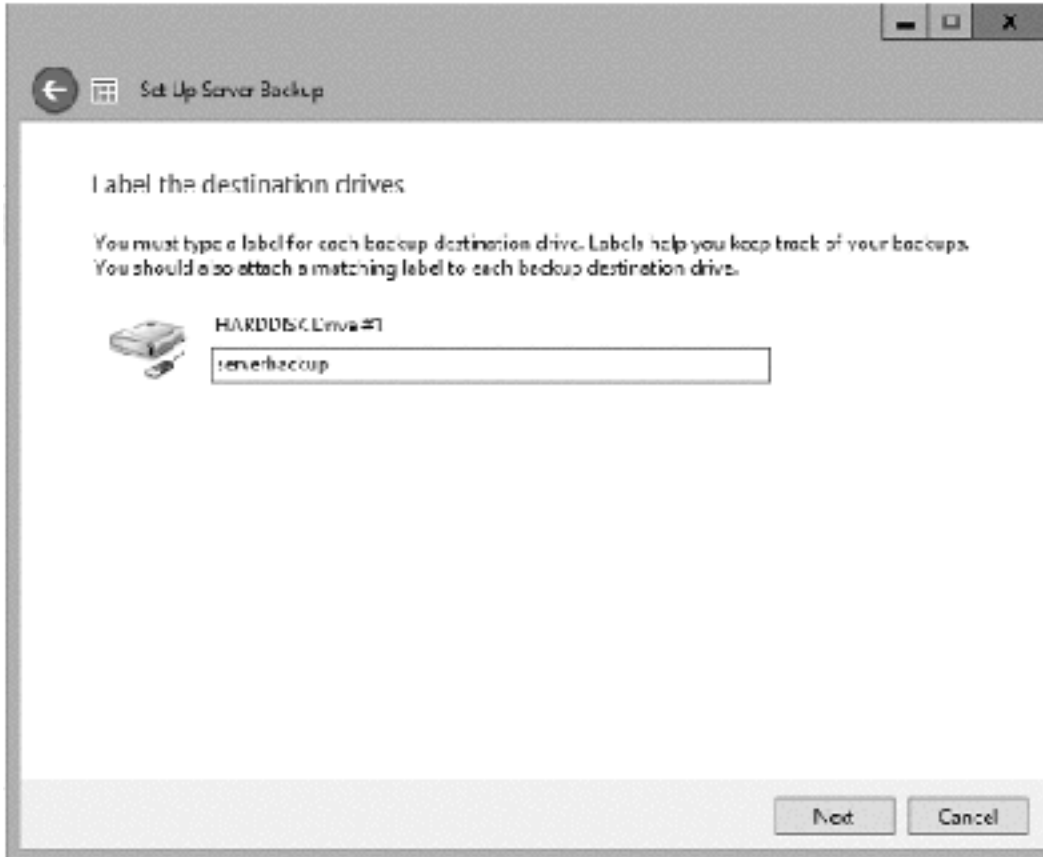
Figure 72: Label the backup drive

On the next screen the backup schedule is specified. The default suggestion of twice a day is possibly overkill in many situations. Instead, click **Custom** and choose a time. The best time to perform a backup is out-of-hours or whenever the business/organization is not operational, as the backup can consume a lot of resources on the server, slowing down normal activities. In this example the backup is set for 1.00am. Click **Next**:
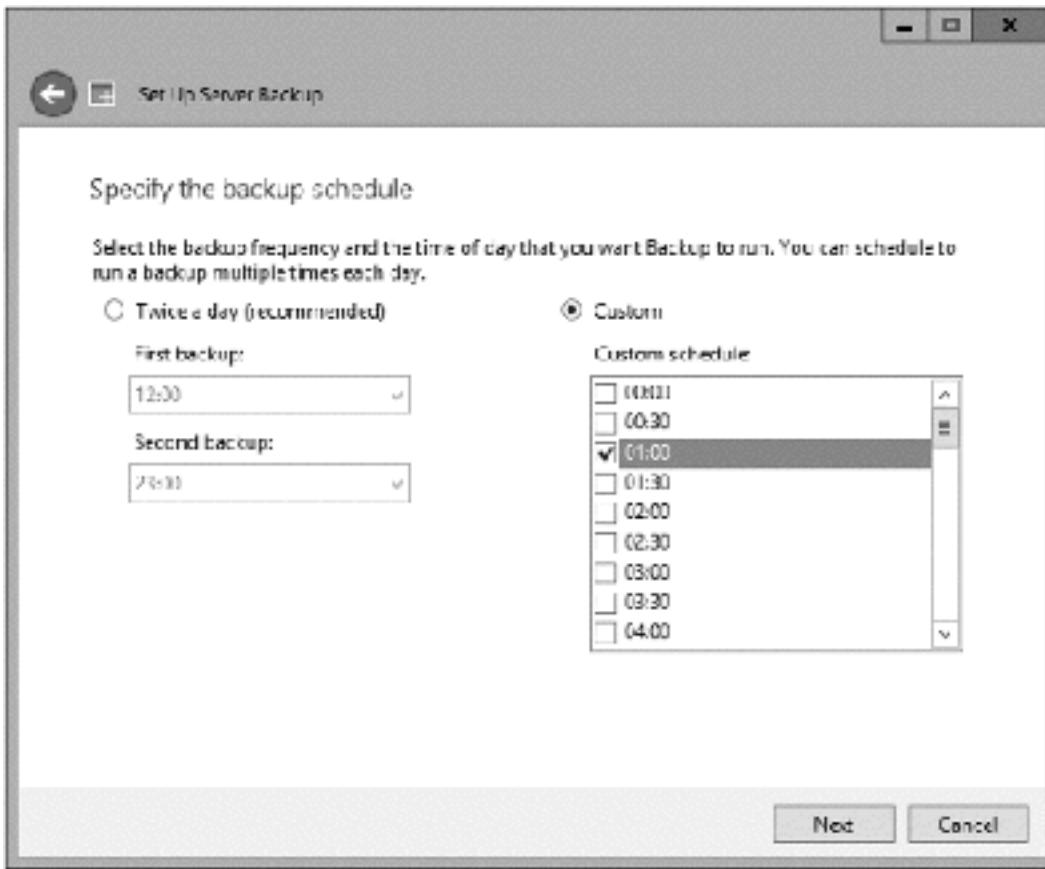
Figure 73: Set the backup schedule

The subsequent screen is for specifying which items need to be backed up. Everything should be ticked; however, make sure that the backup drive itself is not included (it should not be listed, but if it is then make sure it is not selected). Then click **Next**:
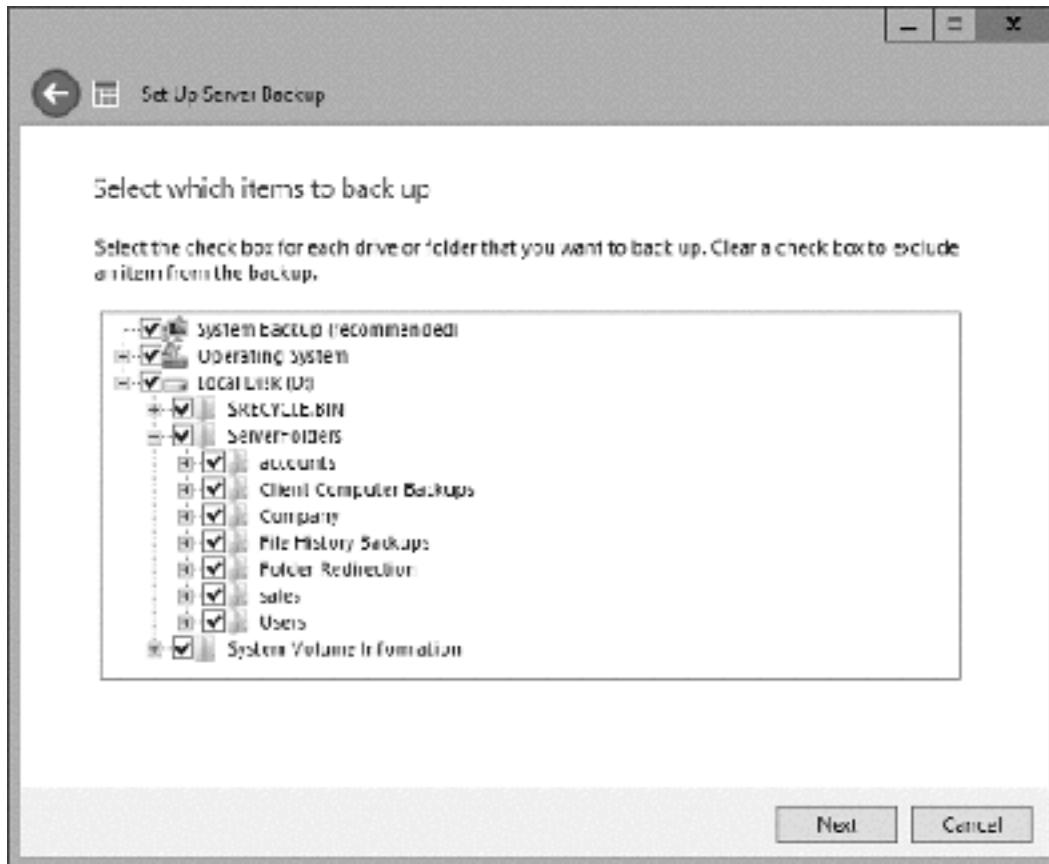
Figure 74: Select the items to backup

A screen to confirm the backup settings is shown. Click on **Apply settings**. The server will process for a short while and then give a final confirmation that the backup has been setup.

The backup job should be checked. As it may not be convenient to wait overnight to check it, run it immediately by going into the Dashboard and clicking the **DEVICES** section. Click on the server and then on the right-hand panel click **Start a backup for the server** followed by **Yes** to the resultant prompt. When the backup is completed - which may potentially be several hours depending on the amount of data - the backup status of the server on the screen will be updated accordingly.

5.3 Recovering Files to the Server

In the event of data loss or there being a need to recover (restore) deleted or older versions of files to the server, the Dashboard is used. Click on the **DEVICES** tab, make sure the server is highlighted, right-click it and choose **Restore files or folders for the server** to start the Restore Wizard. Click **Next** on the first screen. The second screen asks for the location of the Backup location – choose **On this server (SERVER)** followed by **Next**. There is then a choice of whether to **Restore from the most recent backup (recommended)** or **Restore from a backup that I select (advanced)**. The latter is more flexible and in this example we will choose it, causing the following screen to be displayed. Select a backup to be restored using the calendar and time fields, then click **Next**:
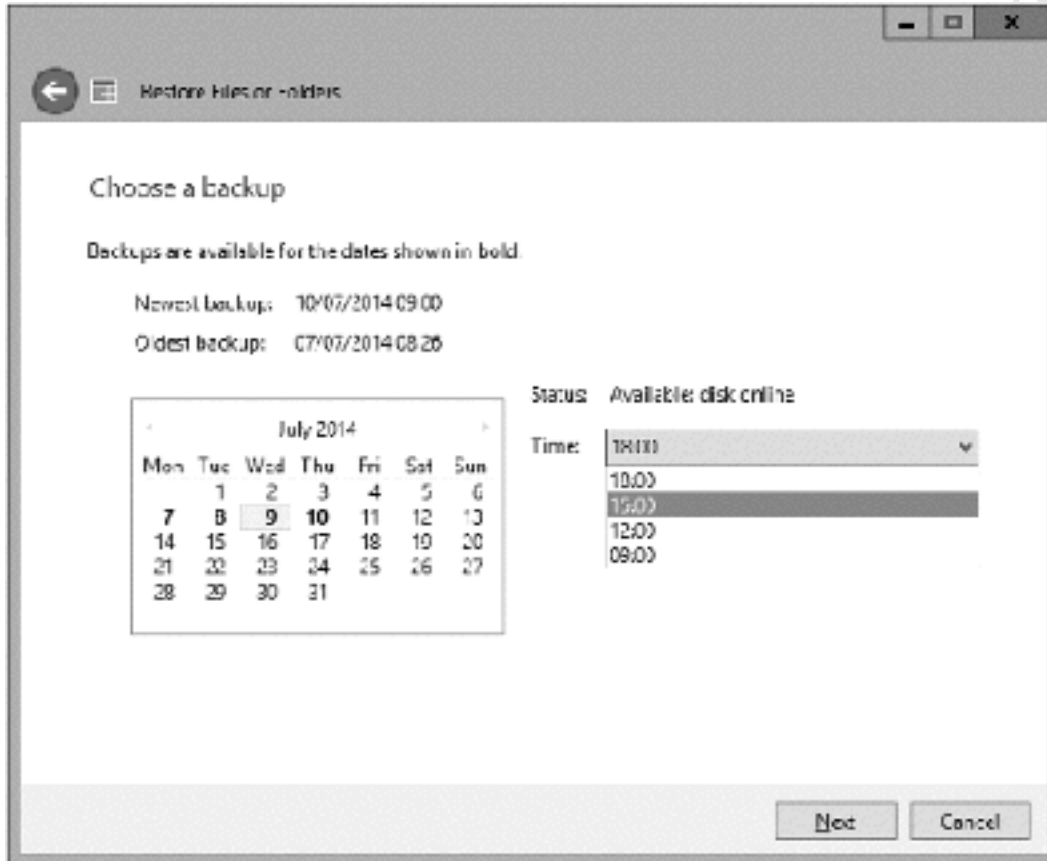
Figure 75: Choosing a backup

On the subsequent screen there is a choice between restoring an entire disk drive or a selection of files and folders; most commonly you would be doing the latter. Choosing it displays a screen where you can drill down to select the items to be restored. Note that by holding the **Ctrl** key down whilst clicking you can select multiple items. Then click **Next** to proceed:
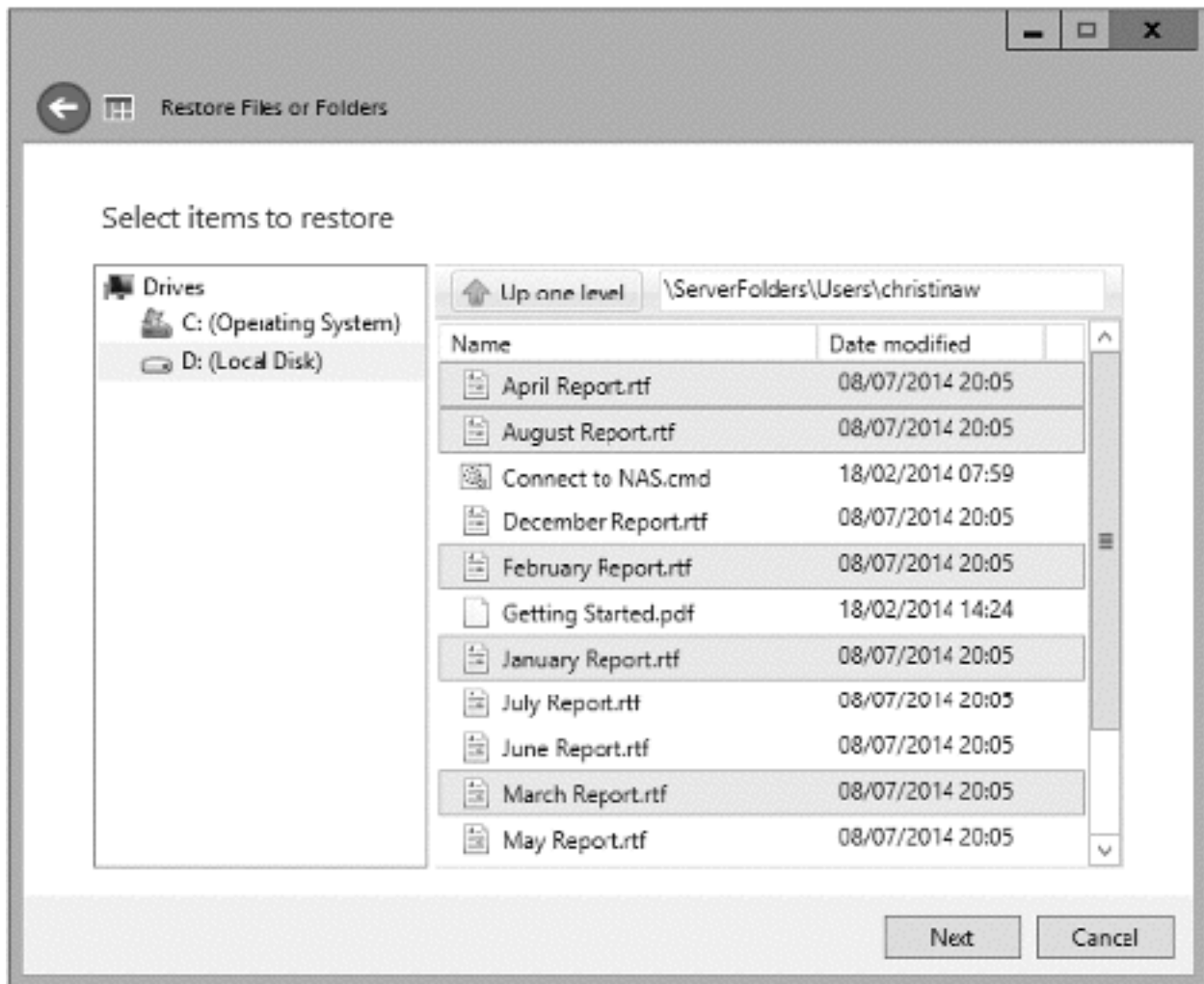
Figure 76: Select the items to restore

The next screen is for specifying the various options when recovering files. Specifically, whether they should be recovered to the original location or to another location, and what to do when duplicates are found. Make a decision and click **Next**:
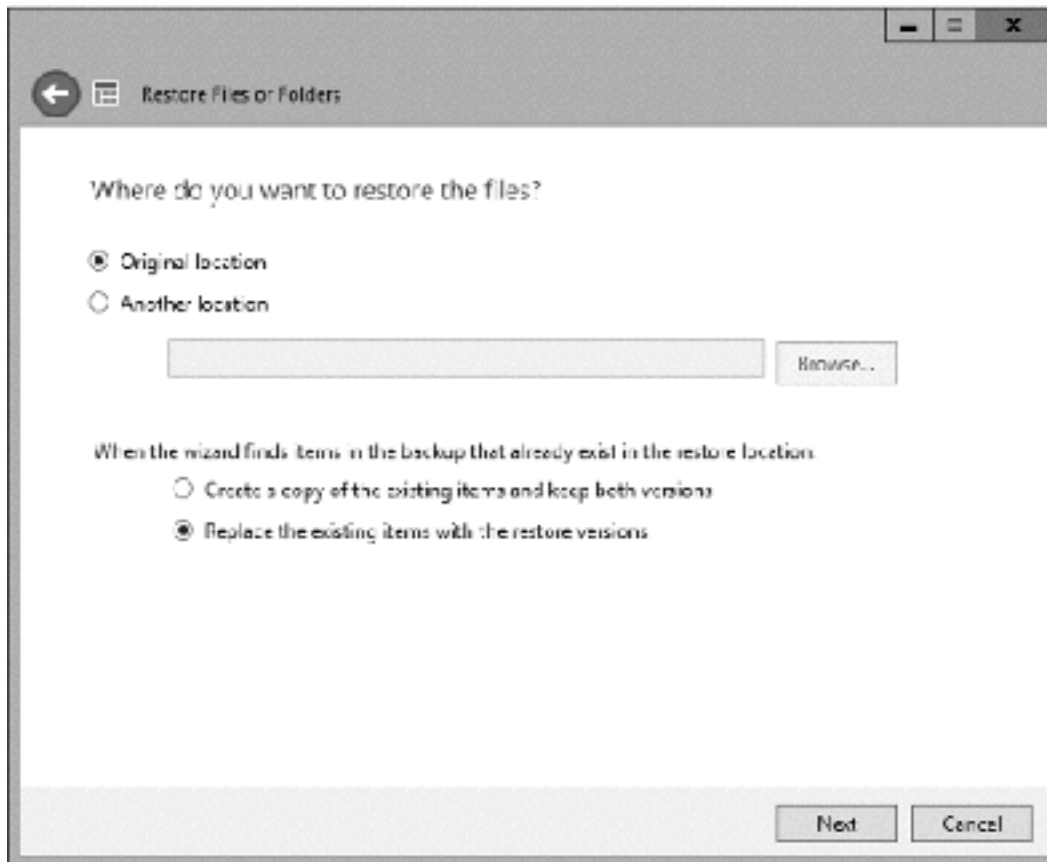
Figure 77: Specify the destination

A confirmation screen is then displayed – click the **Restore Now** button to proceed. The time taken for the recovery of the files depends upon the volume of data. When complete, a screen to that effect will be shown.

5.4 Backing up to a Network Drive

One potential downside of using an USB drive for backups is that it has to be physically located close to the server. In the event of a disaster – for instance, fire, flood or theft – not only might the server be lost but the backup drive might be as well. One way to mitigate against this is to use a network drive for backups, such as a NAS or *Network Attached Storage device*. This gives a lot more flexibility as to where it is located; for instance, it could be in a totally different part of the building. The network drive can be in addition to or in place of an USB backup drive.
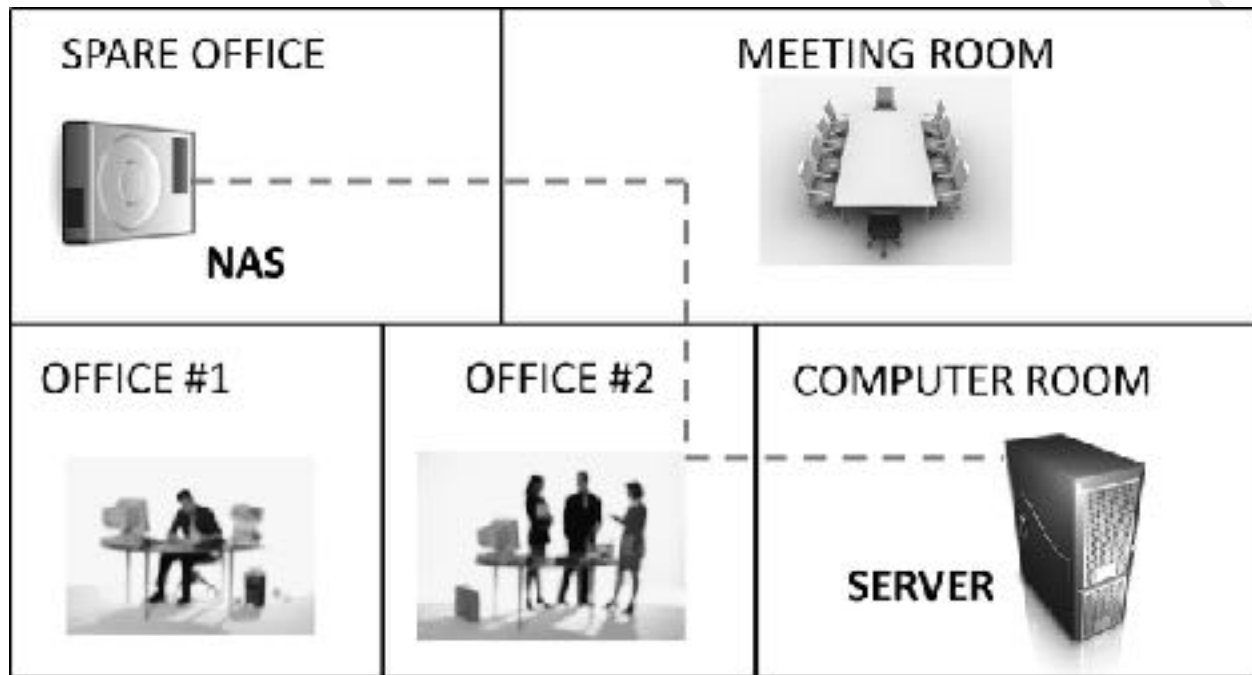
Figure 78: Locate the NAS drive in a separate part of the premises

As there are many different brands of NAS to choose from (e.g. Synology, QNAP, Netgear, Lenovo and so on) the specifics of setting up a particular one will not be covered and the manufacturer's documentation should be referred to. However, the basic principle is that a dedicated shared folder for backups with read/write access should be created on the NAS, along with a dedicated user account.

When we configured the backup to USB in section 5.2 Configuring Backups for the Server, we did so from the Dashboard. However, the Dashboard lacks the flexibility needed to deal with network backups and instead we will need to work directly with the underlying Windows Server backup tool. To access it, go to the Start Screen and click **Administrative Tools**. From there choose **Windows Server Backup** and the following screen will be displayed after a few seconds:
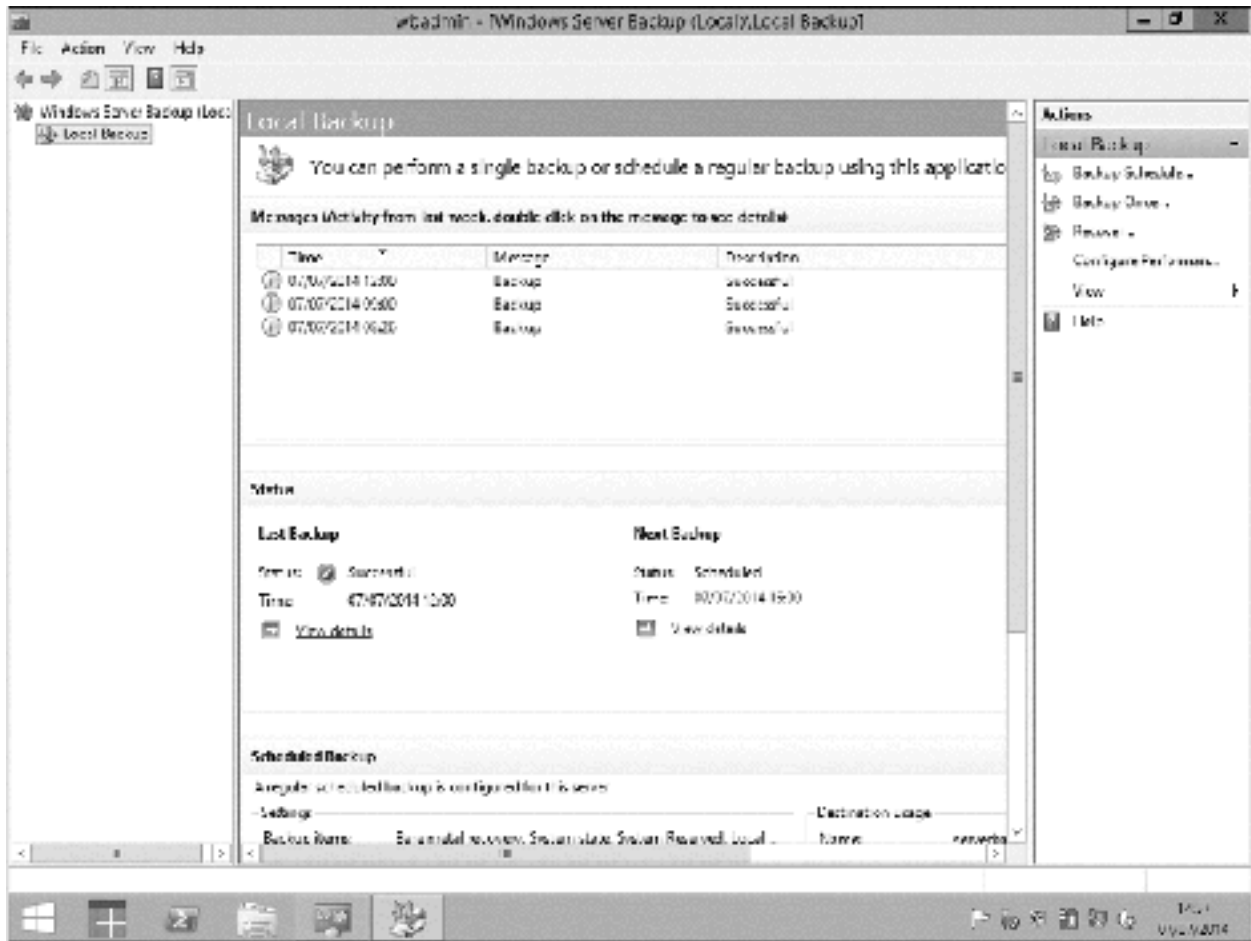
Figure 79: Windows Server Backup screen

In the left-hand panel click **Local Backup**. Then, in the right-hand panel click **Backup Once**. On the screen that appears choose **Different options** then click **Next**:
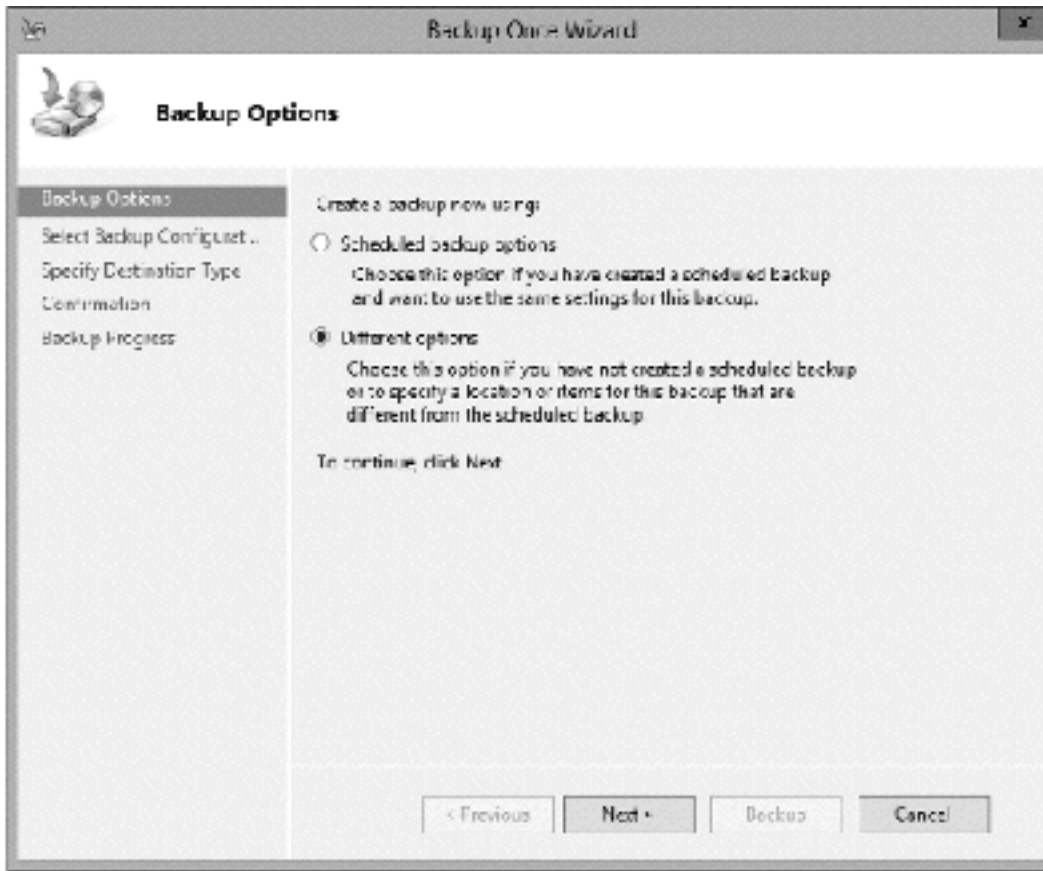
Figure 80: Choose a backup option

The subsequent screen gives a choice between a *Full server (recommended)* or *Custom* backup. Although the former seems a better choice, choose **Custom** as the Full server backup will not work correctly with a networked backup drive. Click **Next**. This screen will appear:
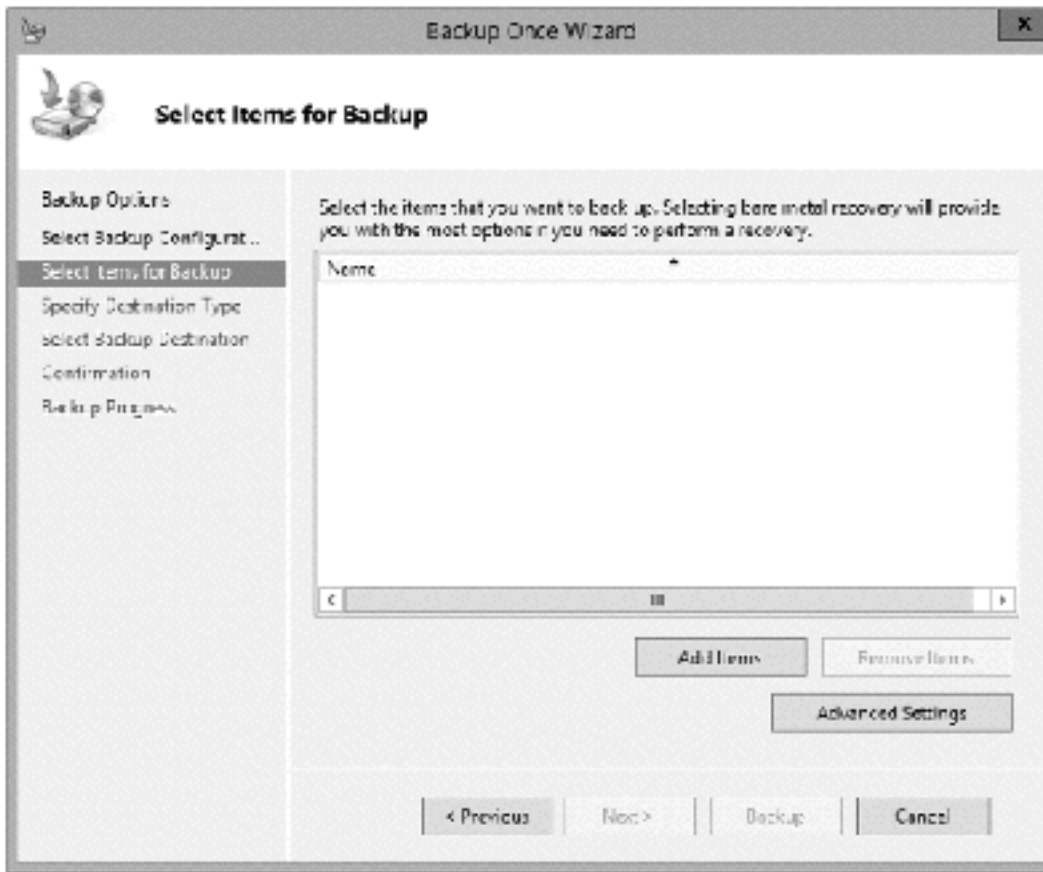
Figure 81: The Backup Once Wizard

Click the **Add Items** button. On the panel, choose the items to be backed up. This would normally be just the disk volume containing the data (in our case, the D: drive). Click **OK**.
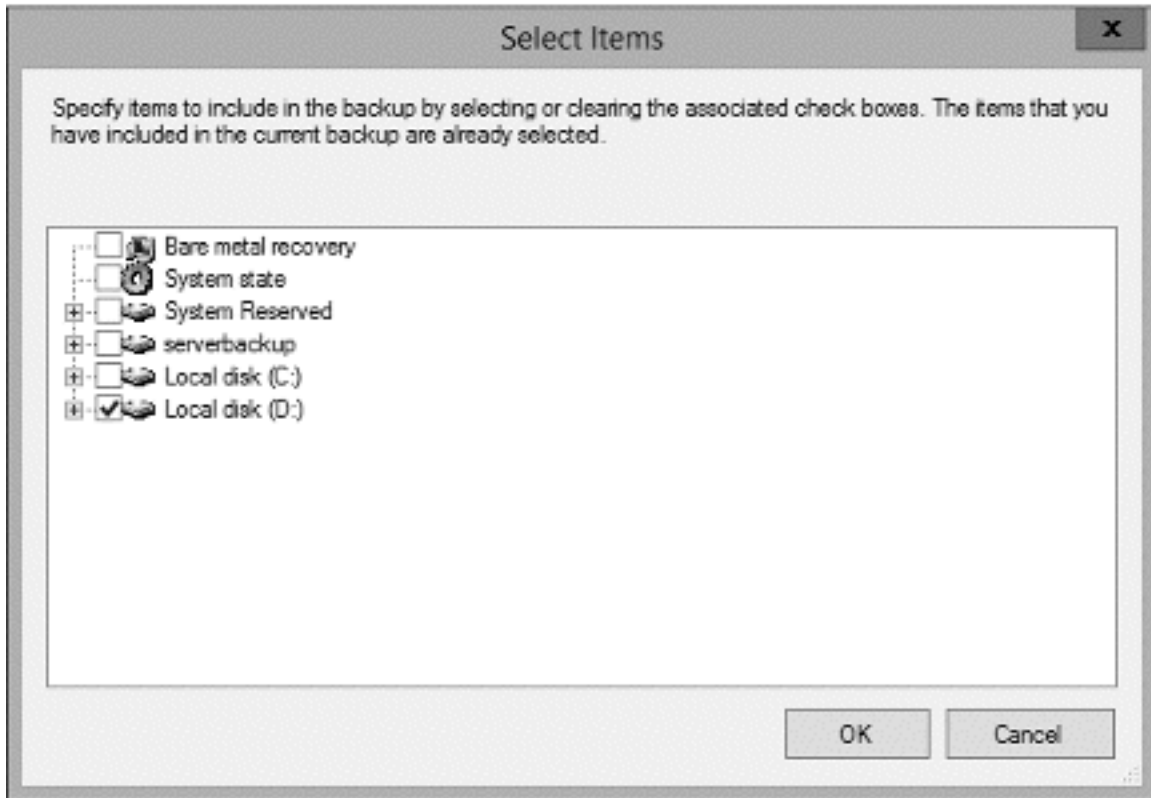
Figure 82: Select items to backup

You will be returned to the previous screen – click **Next**. On the following screen the backup destination type has to be chosen – click **Remote shared folder** and click **Next**. On the screen after that, enter the location of the NAS folder in the form *\\NAS_name\folder_name*. In this example, the NAS is called *backserver* and the backup folder is called *netbackup*, hence *\\backserver\netbackup*. Choose the **Do not inherit** option, click **Next**:
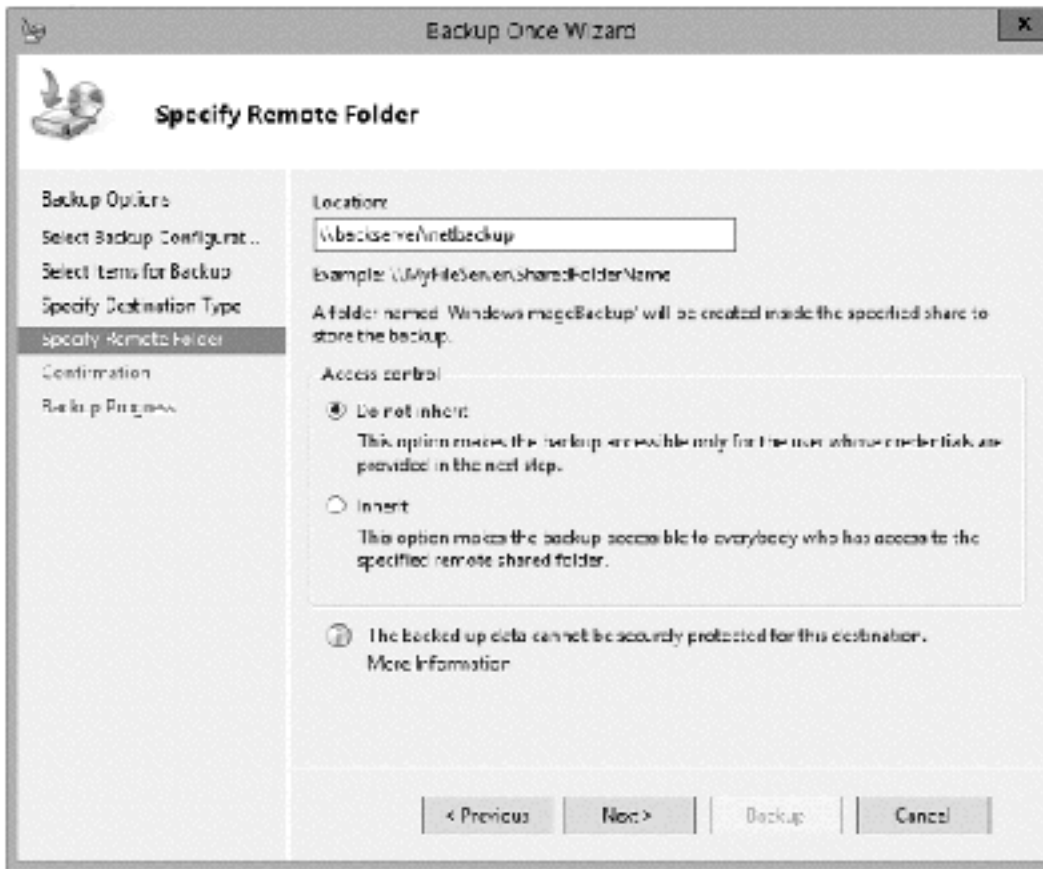
Figure 83: Specify Remote Folder

After a few seconds there will be a prompt to enter a user name and password for the backup – this has to be an account that has been defined on the NAS box, not the Essentials server. Continue, and a confirmation screen will be shown. Click the **Backup** button:
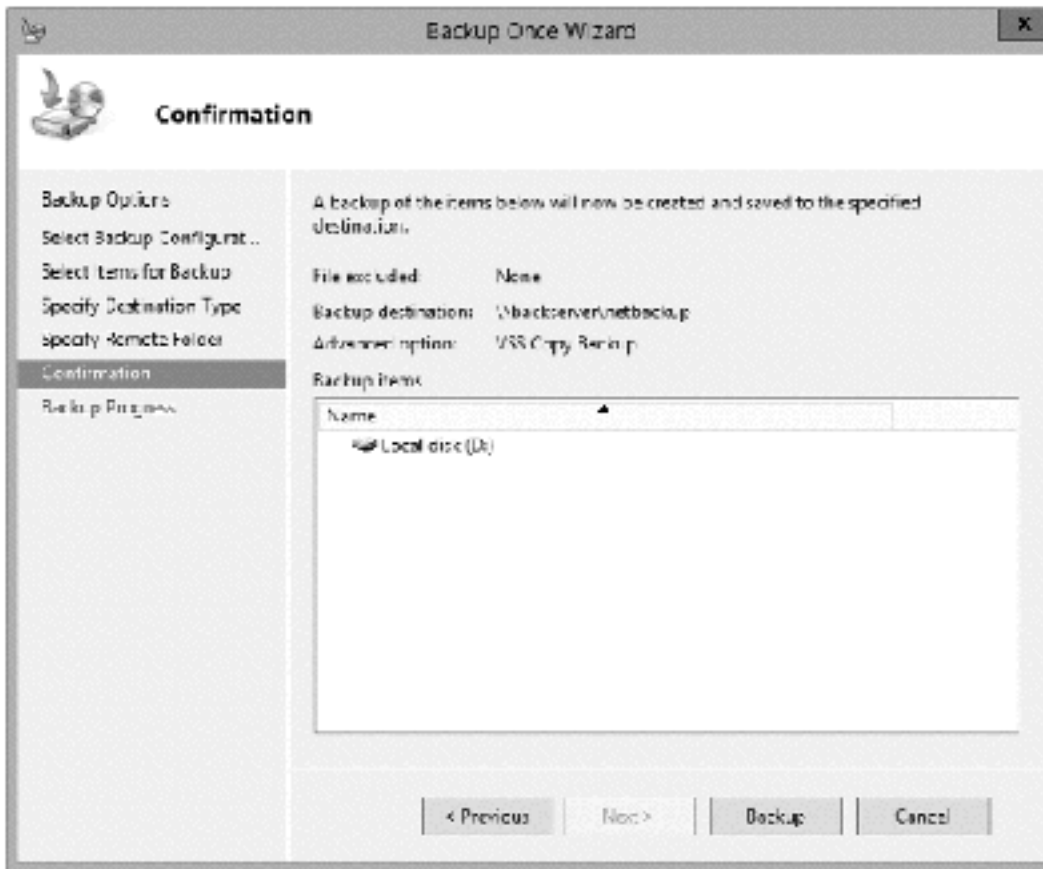
Figure 84: Backup confirmation screen

In this example, the backup to NAS has been run manually and in a way that does not interfere with the scheduled backup to USB. However, if backing up to NAS is to be the main backup it can instead be scheduled as a regular job.

An additional advantage of using NAS devices is that they can be of higher storage capacities than USB drives. For instance, suppose the server had, say, 16TB of data. At the time of writing it is not possible to buy USB drives of this capacity, whereas this amount of storage is readily achievable with a NAS. However, a disadvantage of using a NAS is that whereas an USB drive can hold multiple backups, when used with Windows Server Backup a network drive can only hold a single backup i.e. the most recent one. So, in the event of problems, it is only possible to revert to the last backup rather than a selection of older ones.

5.5 Configuring Backups for the Computers

By default, Essentials will backup any connected computers on a daily basis. It will start doing this shortly after a computer is added to the network for the first time; because of this it is a good idea to use a wired connection when setting up a laptop as a complete first backup could be very slow over a wireless link. These backups generate complete, up-to-date image copies of the workstations, meaning they can be used to restore complete machines as well as just files and folders.

In general, best practice in a network dictates that all data should be stored on the server and data should not be stored locally. However, this does not always happen, particularly with laptops, which may be taken offsite. The use of Folder Redirection as discussed elsewhere in this guide can help with this, as it ensures that the data on laptops is synchronized with the server, but the facility to have laptops fully backed up is very useful.

In the case of desktop computers, it is less clear cut as to whether daily backups are really needed as the machines do not change much if no user data should be stored on them. You might, therefore, wish to turn off the automatic backups. This has to be done for individual computers and to do so, the computer needs to be powered on. It is suggested that a newly connected workstation is first allowed to back itself up completely one time. After it has been connected for a couple of hours, go into the Dashboard on the server and click on the **DEVICES** tab. The computer in question should have a status of 'Successful' against it, meaning it has been backed up. Right-click on the computer name and from the pop-up menu choose **Customize backup for the computer**. A panel will be displayed giving two options – click on **Disable backup for this computer**. A further panel is then displayed, asking whether you want to keep or delete the existing backups: choose **Keep the existing backups for this computer**. A confirmation message is displayed – click **Save Changes**:
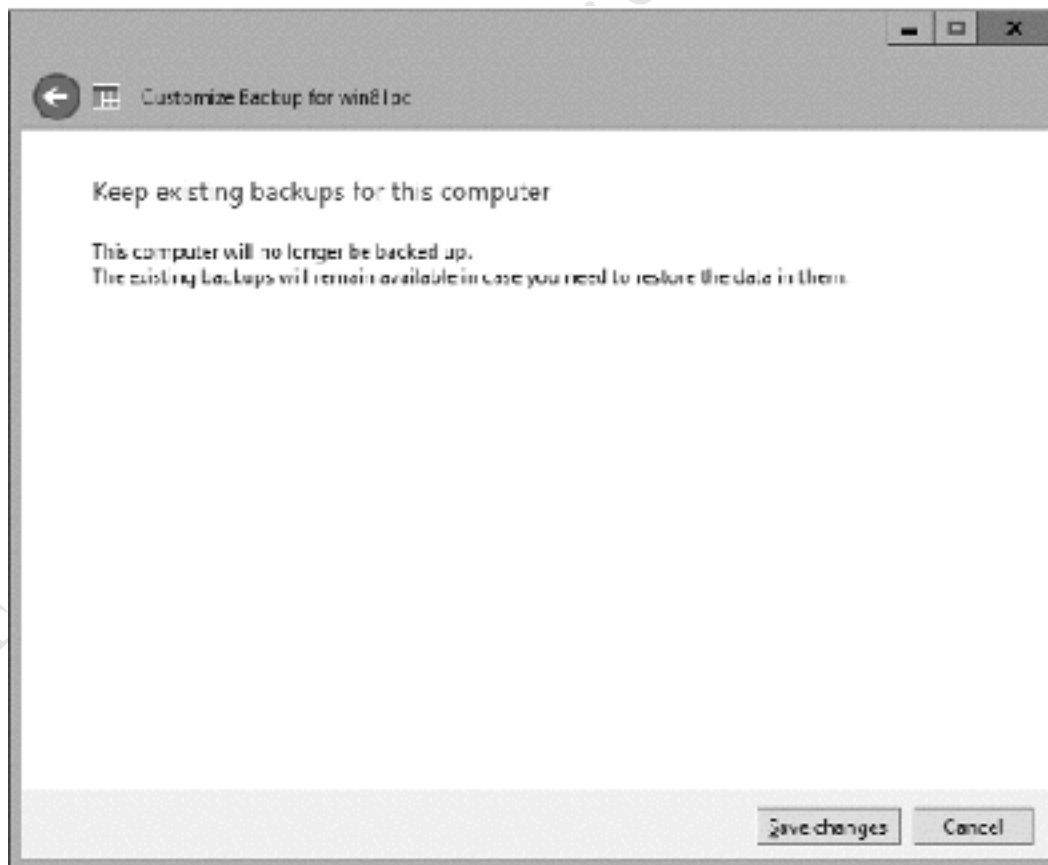

Figure 85: Message about existing backups

No further backups will occur. However, any existing backup(s) will be preserved and can be used for restoring data if necessary.

Changing the Backup Parameters

The time at which computers are backed up and the length of time that backups are retained can be controlled. To do so, launch the Dashboard and click **DEVICES**. Under **Computer Tasks** on the right-hand side of the screen click **Client computer backup tasks** to display this panel:
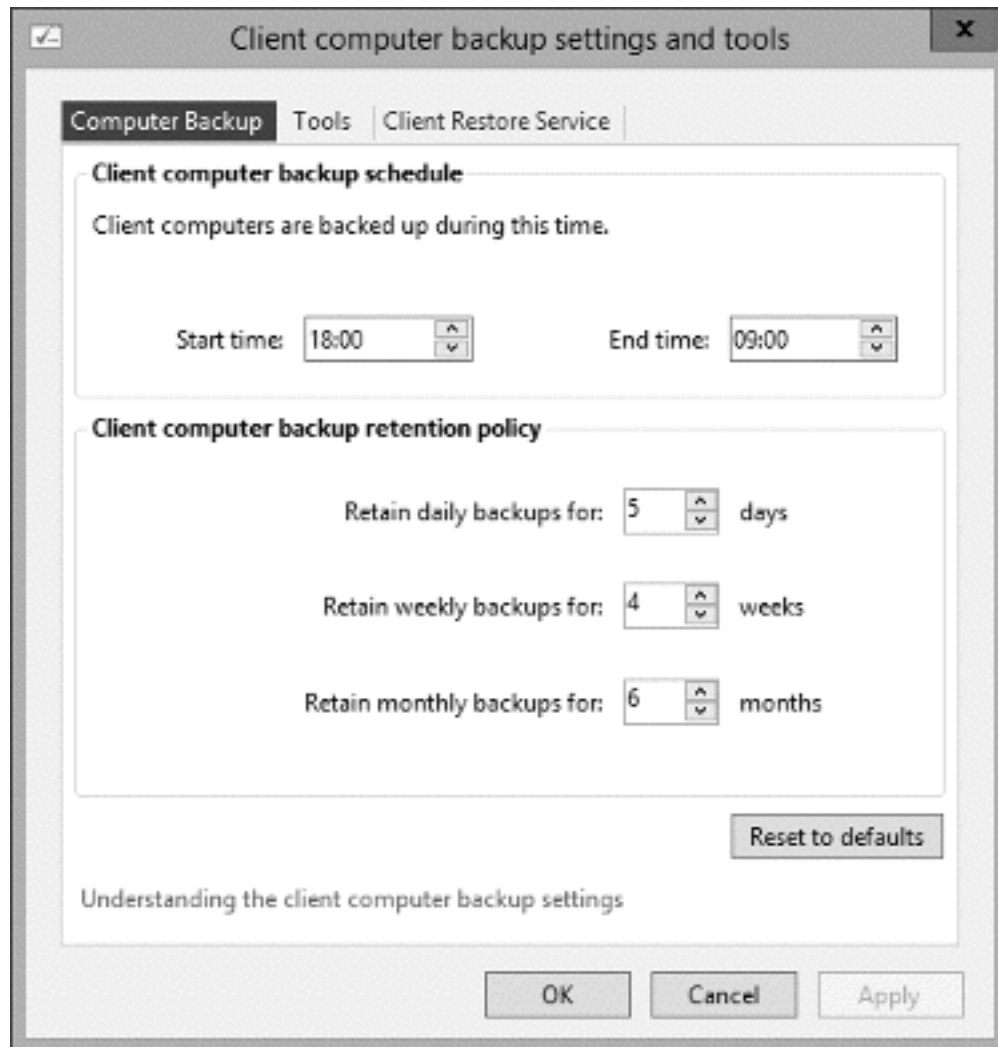

Figure 86: Settings for client computers backups

By default, backups occur between 18:00 and 09:00 hours (6pm to 9am), but this window can be changed if required. The backups themselves are organized into daily, weekly and monthly ones, although this process is largely invisible. If desired the retention periods for the different backups can be adjusted.

Having made any changes to the settings, click **OK**.

5.6 Restoring Data to a Computer

In the event of data loss from a computer, it can be restored from the backup(s) stored on the server. However, the actual process has to be initiated from the computer itself. Go the computer in question, either physically or remotely using the facility described in 12.8 Managing Computers from the Server and login. Note that any user credentials can be used for the computer login. Open the Launchpad and start the Dashboard. Login to the Dashboard as *systemadmin* and click **DEVICES**. Right-click the computer and choose **Restore files or folders for the computer**. A list of available backups is shown; choose one and click **Next**:
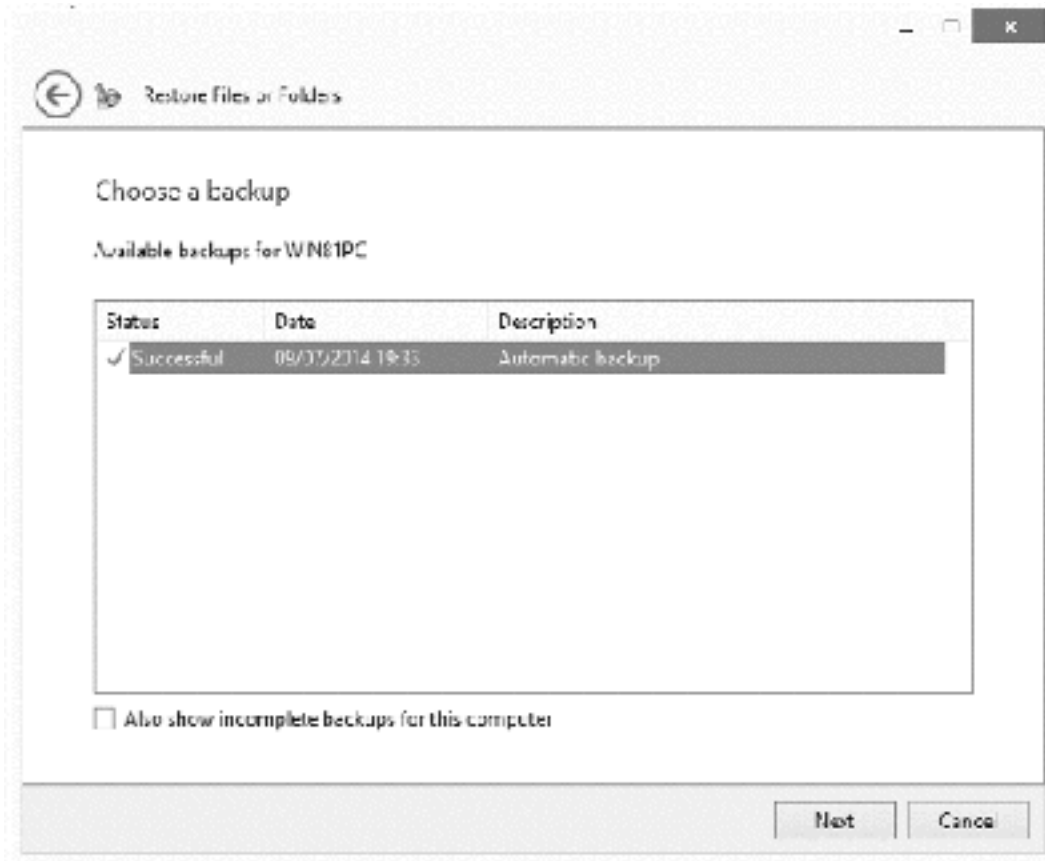
Figure 87: Choose a backup

The backup volume is opened, which may take a little while. From the resultant screen, choose the items to be restored then click **Next**:
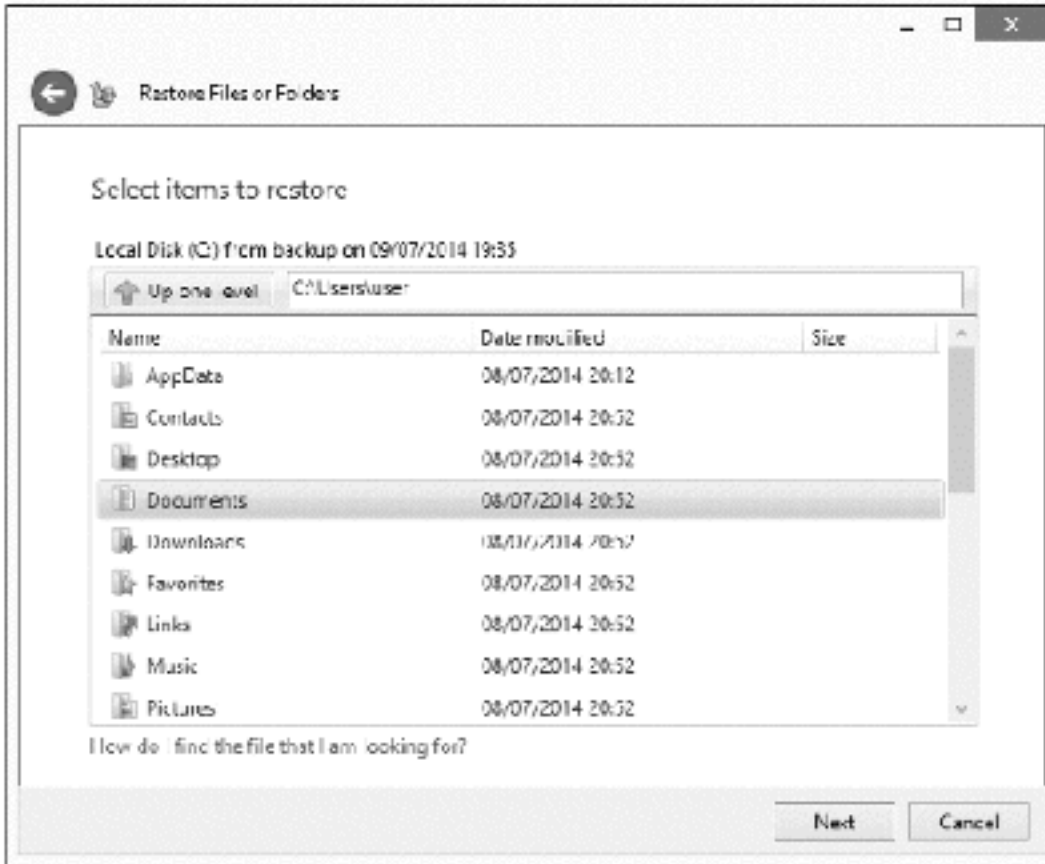
Figure 88: Choose the items to be restored

The subsequent screen allows you to specify where the items will be restored to, for example to their original location. There may be additional requests for authentication – enter the details for the *systemadmin* account. Upon completion a confirmation screen is displayed; at this point you can close down the Dashboard and plus logout from the computer if you have been using the *systemadmin* account.

6. PRINTING

6.1 Overview

One advantage of networking is that it allows printers to be shared, thus potentially saving money as well as physical space. Perhaps surprisingly so, Essentials does not include any particular features to make printer sharing easier than usual. However, there are there are several widely used methods for setting up printers in a networked environment, two of which are discussed in this chapter. Each of them has benefits and disadvantages and there is probably no such thing as 'the best' solution; however, some explanation is given as to when you might take a particular approach.

Before beginning, identify the client operating systems that are in use and download all the appropriate printer drivers from the printer manufacturer's website. In general, there will be a driver that works with 32-bit versions of Windows (usually referred to as x86 or x32) and a driver that works with 64-bit versions of Windows (usually referred to as x64); however, some printers have a single driver for all variants. Some manufacturers offer an additional 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 try to sell you more consumables. 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 fully utilize them.

Next, physically setup the printer and configure it with a fixed IP address consistent with the IP addressing scheme used in the network. Check that the printer is working correctly before beginning the installations on the clients.

Suggestion: a good location to store the printer drivers is the *technical* share, accessible as *server**technical$* by administrative users such as *systemadmin*.

6.2 Networked Printer

Most printers, other than very low cost and old models, have built-in network adaptors, either wired and/ or wireless. This means that they can operate independently of the file server, with the computers talking to them directly. This is the simplest and most effective method for setting up a printer in a small business network. This approach also works very well in a scenario where many different operating systems are in use.

The printer(s) should be physically setup and connected to the network **before** the computers are added to the domain. Then:

- Visit each individual computer and login as a local user with administrative rights. Or, if developing a master disk image that will subsequently be cloned - also referred to as *Ghosting* - work on that image.

- Install the printer through the standard Windows method (**Control Panel** > **Devices and Printers** > **Add Printer**) or by using the manufacturer's provided installation program.

- Specify the printer as being on a TCP/IP port. Provide the fixed IP address of the printer.

- Set the printer as the default printer.

- Change any defaults if necessary e.g. paper size, print quality and so on.

- Remove any superfluous 'virtual' printers if they are not going to be used (e.g. OneNote, fax, XPS)

- Print a test page to verify correct operation

The computers can then be added to the domain. The printer will appear in the list of printers for each user, although they may have to explicitly choose it to make it their default printer.

6.3 Shared Printer via Server

With this method, the printer(s) are installed initially on the server and defined as shared resources; users can then choose to connect to them from their computers if they so wish. This technique has merit where there are multiple printers in use and where the users are technically literate. Also, it allows new printers to be installed retrospectively after the network has already been setup, in contrast with the previous method where the printer(s) are installed before the computers are connected to the domain. However, with this approach the users need to have administrative rights on the domain or at least be given the administrator password. Alternatively, the printer can be installed by the administrator.

The procedure is:

- Install the printer on the server through the standard Windows method (**Control Panel** > **Devices and Printers** > **Add Printer**) or by using the manufacturer's provided installation program.

- Specify the printer as being on a TCP/IP port. Provide the fixed IP address of the printer.

- On the Printer Sharing panel click **Share this printer so that others on your network can find and use it**. Give it a meaningful **Share name** and use the **Location** and **Comment** fields to provide other helpful details. Then click **Next**:
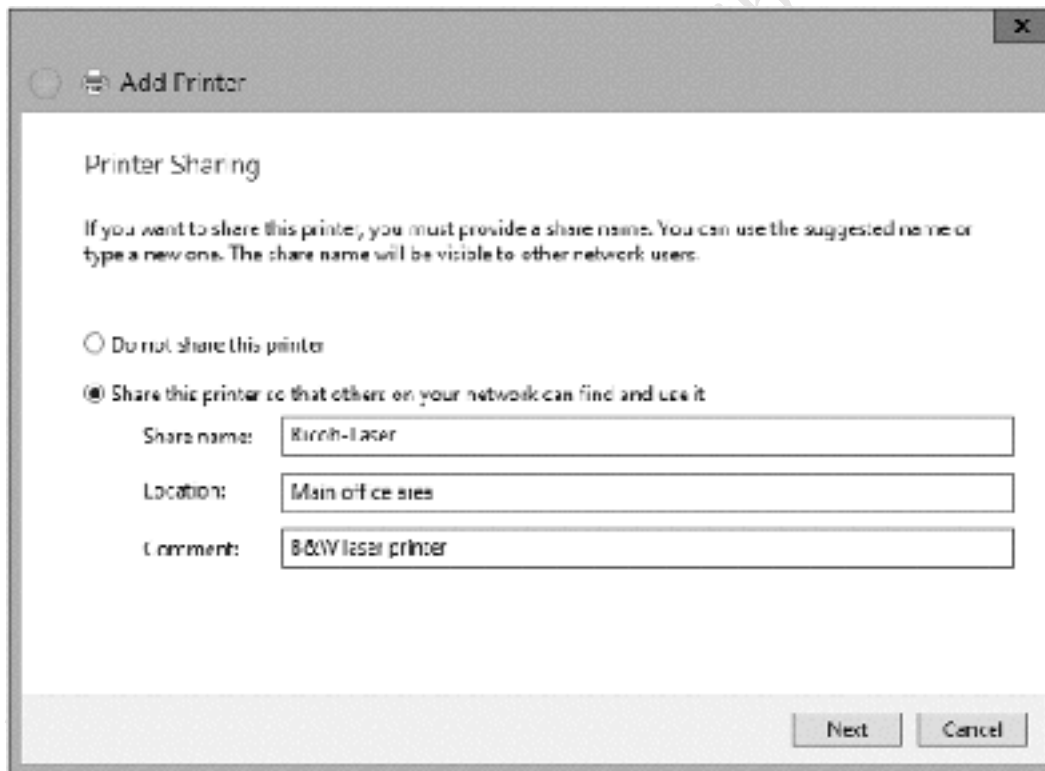
Figure 89: Printer Sharing

Complete the installation and check that it is working by printing a test page. Then, within **Devices and Printers** right-click the printer and choose **Printer Properties**. Click the **Sharing** tab. Make sure that the **List in the directory** box is ticked:
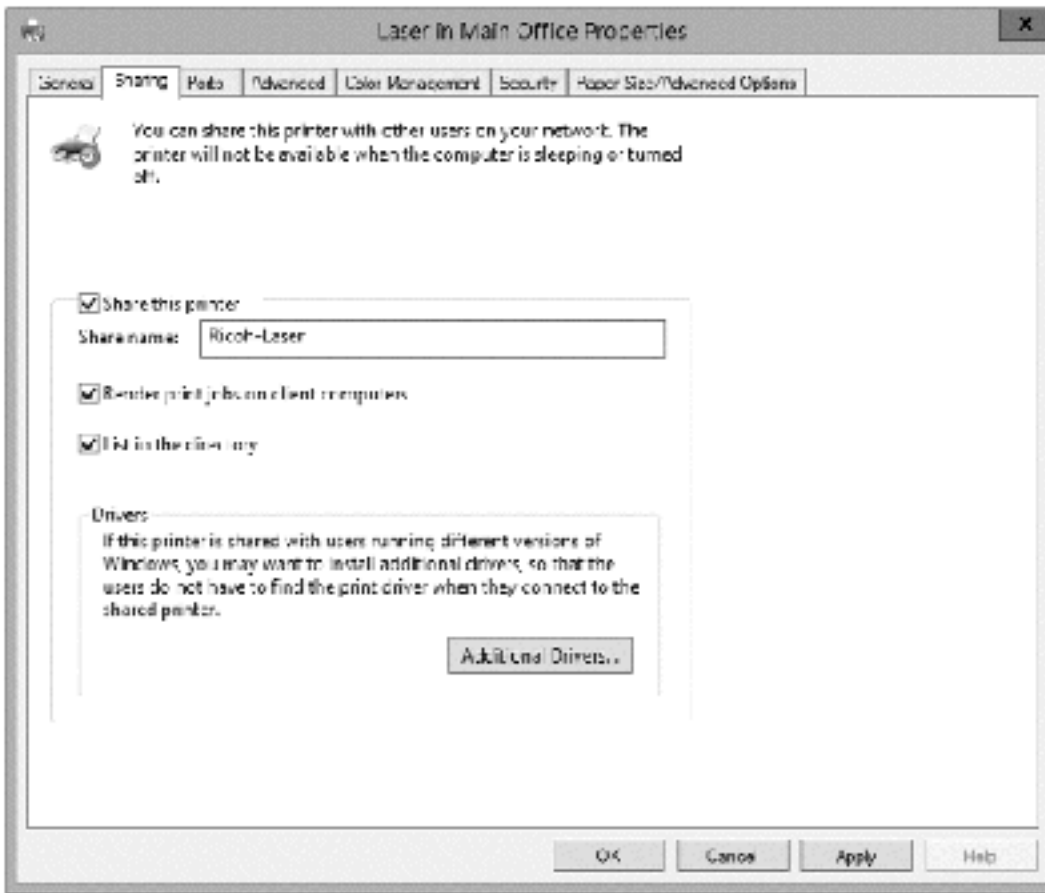
Figure 90: Properties for shared printer

If all the client computers are using 64-bit versions of Windows, then we are complete on the server side. However, if any client computers are using 32-bit versions of Windows then click the **Additional Drivers** button. On the next panel, tick the **x86** box followed by **OK**. Note: this reflects the most common scenario with printers, referred to by Microsoft as *Type 3* printers. With some printers – usually more recent models known as *Type 4* printers – this step is not needed as the drivers will work with all modern versions of Windows regardless of whether they are 32-bit or 64-bit:
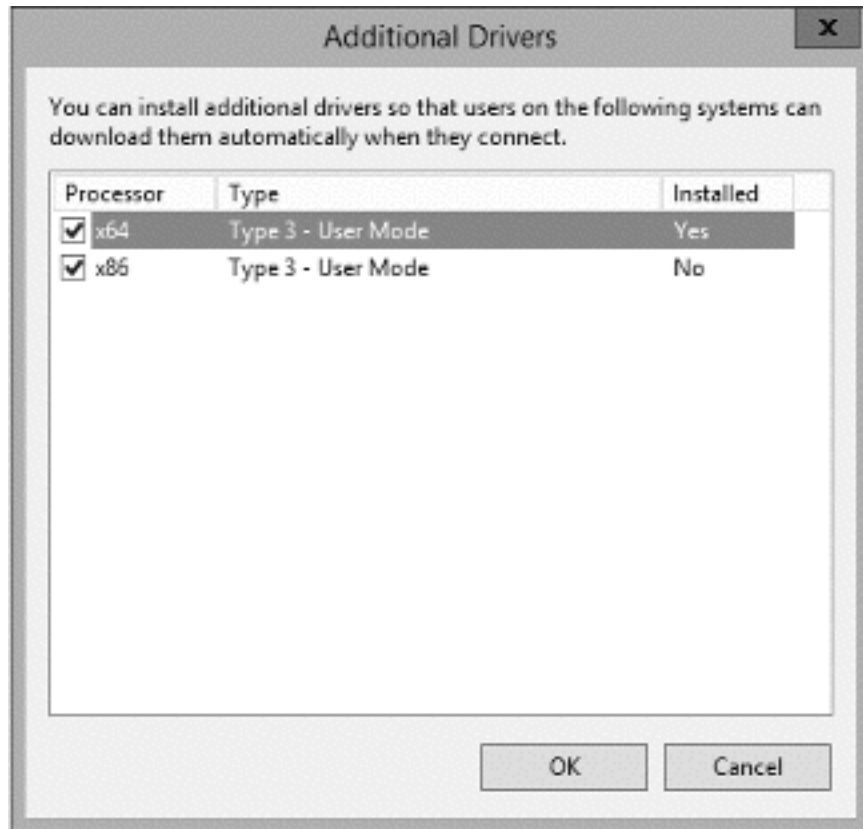
Figure 91: Additional printer drivers

Having clicked **OK**, you will then be prompted to enter the location of the x86 ("32-bit") driver. Follow the screens through then click **Apply** followed by **OK**.

The printer can now be installed on the client computers. To do this, a user must have administrative rights or, when prompted, enter the account details for an administrative user. From **Devices and Printers**, choose **Add Printer**. Choose **Add a network, wireless or Bluetooth printer** and click **Next**:
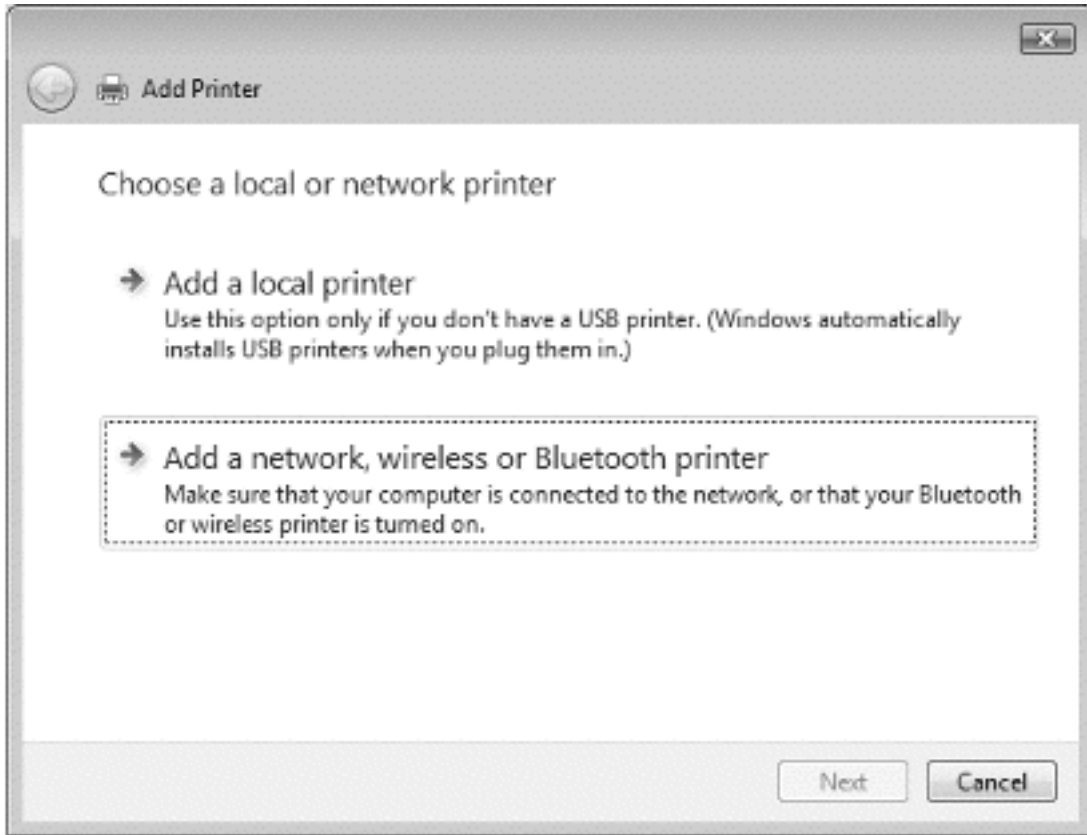
Figure 92: Adding a printer

The shared printer(s) will be listed. Highlight it and click **Next**:
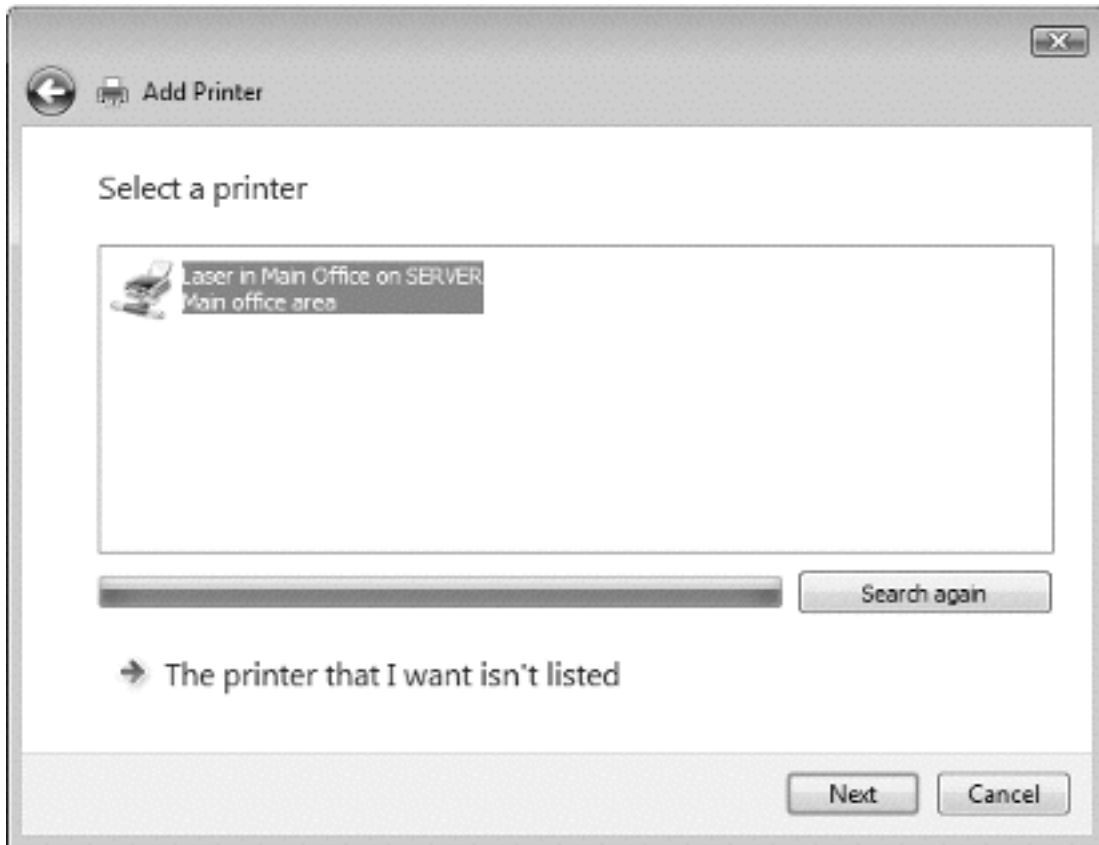
Figure 93: Select a printer

A message about the need to install a printer driver is likely to be displayed. Click **Install driver**:
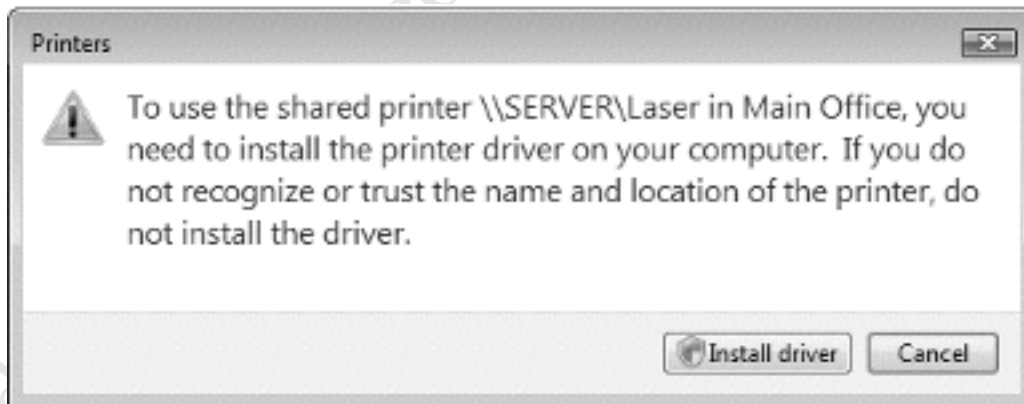
Figure 94: Message about printer driver

If necessary, enter the account details for an Administrator to complete the installation. Once the printer is installed, print a test page to confirm that it is working.

7. REMOTE ACCESS

7.1 Overview

There is often a need to access data and systems from outside the office, for instance by home-based or travelling workers; Essentials features a number of options to enable this, in addition, it is possible to use third party file syncing tools such as Dropbox and Google Drive to provide indirect access. Three options are described here; some, none or all can be used depending upon the requirements of the organization.

7.2 Setting up Anywhere Access

Microsoft use the term *Anywhere Access* to describe the remote access capabilities in Essentials. Configuring remote access can be difficult and time consuming with regular versions of Windows Server; fortunately, Essentials has a step-by-step wizard to make things easier. Go into the Dashboard. At the top right-hand side of the screen, click on **Settings**. On the panel that opens, click **Anywhere Access** to display the following screen then click **Configure:**

Figure 95: First Anywhere Access screen

On the two subsequent screens just click **Next** and you will arrive at this one:
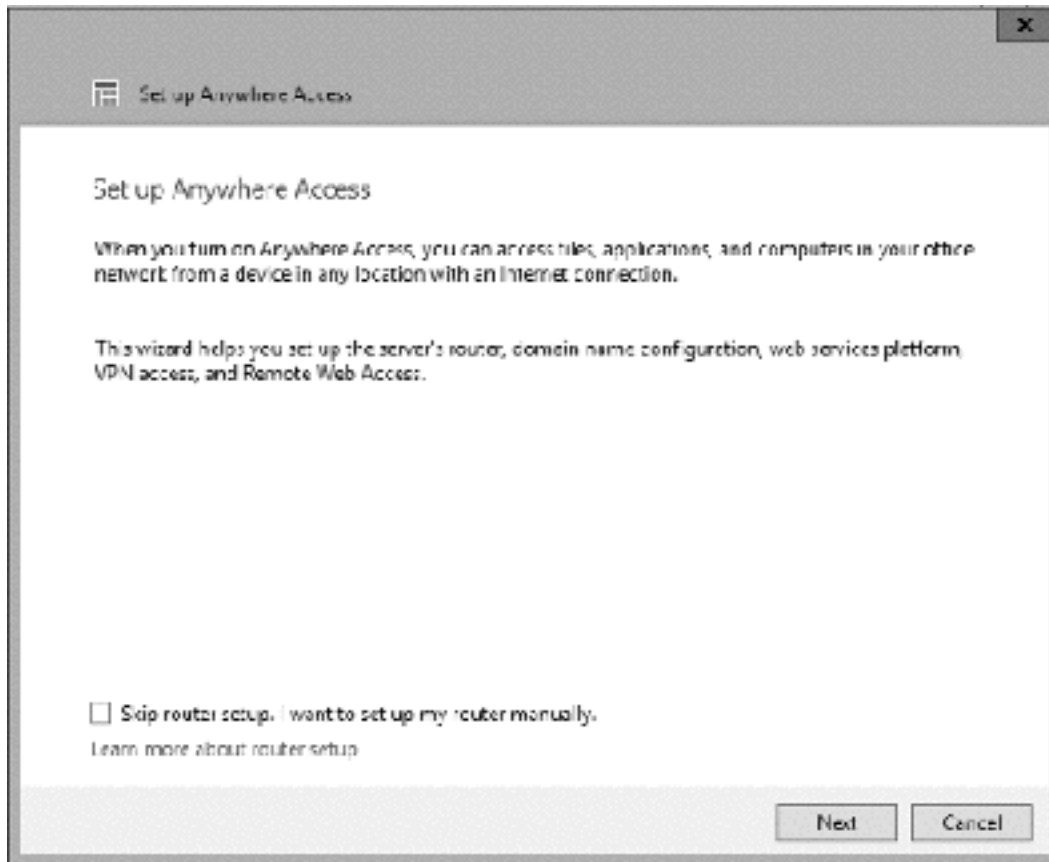
Figure 96: Second Anywhere Access panel

The process starts by asking about a domain. This is not the same as the internal domain name that was chosen when the server was setup; rather this refers to an *external domain name*. Internal domain names are those that are only visible inside the network; in our example, we created an internal domain name of *ctacs.local*. External domain names are those that are visible outside the network i.e. from the internet. Examples of external domain names would be *www.ctacs.co.uk*, *www.apple.com*, *www.microsoft.com* and so on.

You can choose to use an existing domain name that you own and have control over. This option requires you to have an understanding of topics such as SSL Certificates and DNS. If your eyes glaze over at this point or you do not have a suitable domain name or simply prefer not to use it for this purpose you can create a new domain name:
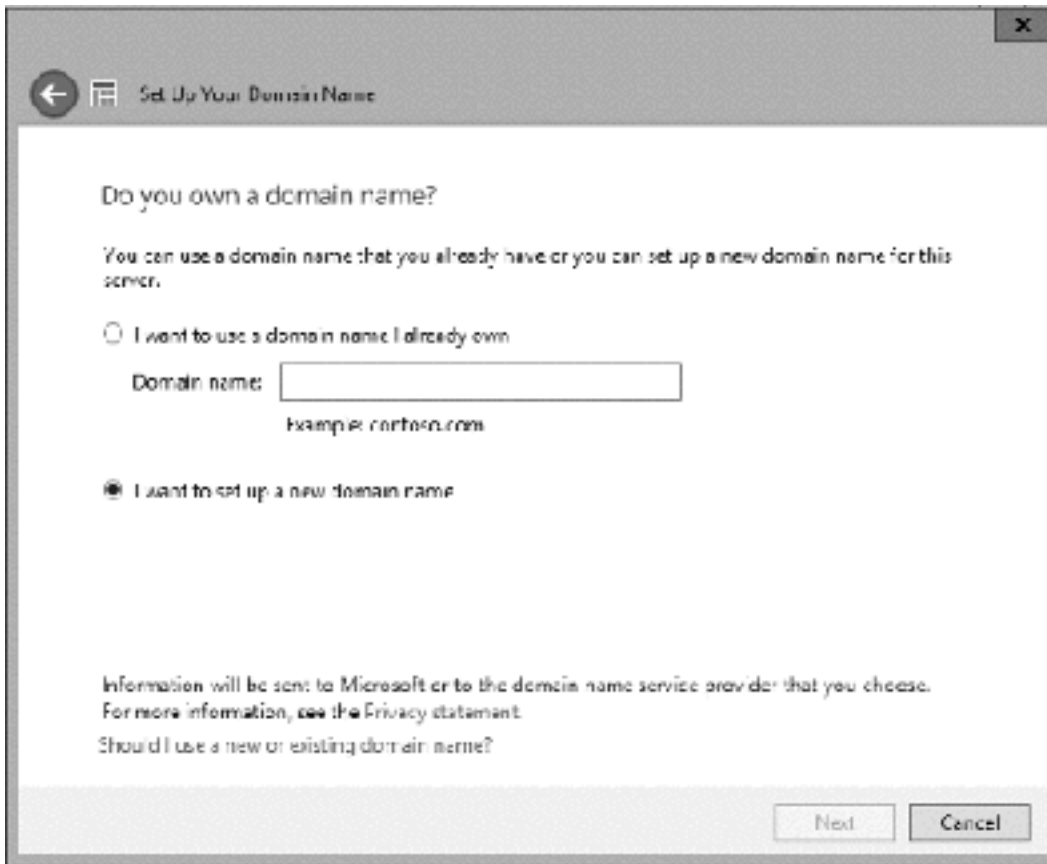
Figure 97: Domain names

If you choose to create a new domain name, the following screen is shown:
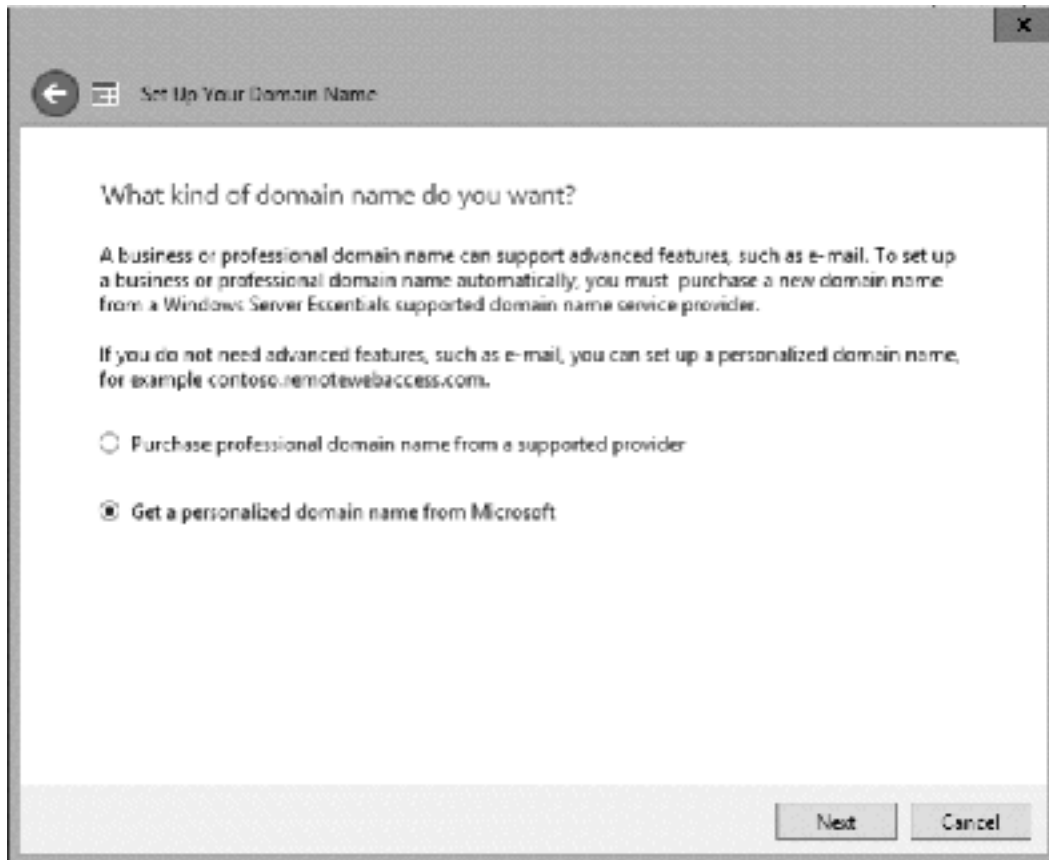
Figure 98: Choose between a professional or personal domain name

You can choose to purchase a *professional domain name*, or use a *personalised domain name* from Microsoft. The differences are as follows:

Professional Domain Name

Price – varies, typically UK £10-20 / US $15-$30 / € 13-25 per annum
Choice of name – anything you wish, subject to it being available e.g. *mycompany.com*
Ownership and control – You

Personalised Domain Name

Price – Free
Choice of name – has to end in remotewebaccess.com e.g. mycompany.remotewebaccess.com
Ownership and control – Microsoft, ultimately

For many organizations, a personalised domain name is absolutely fine and removes any concerns about having to deal with the topic in too much detail. So, it will be assumed that this is what we are using.

If you choose the personalised domain name option, you will need to go online and sign-in with a Microsoft Account name. You may already have one; for instance, you do if you have a Hotmail or Outlook email address. If not, you will need to sign-up for one. Having signed in, you need to accept the Privacy Statement and Agreement. The following panel is displayed:
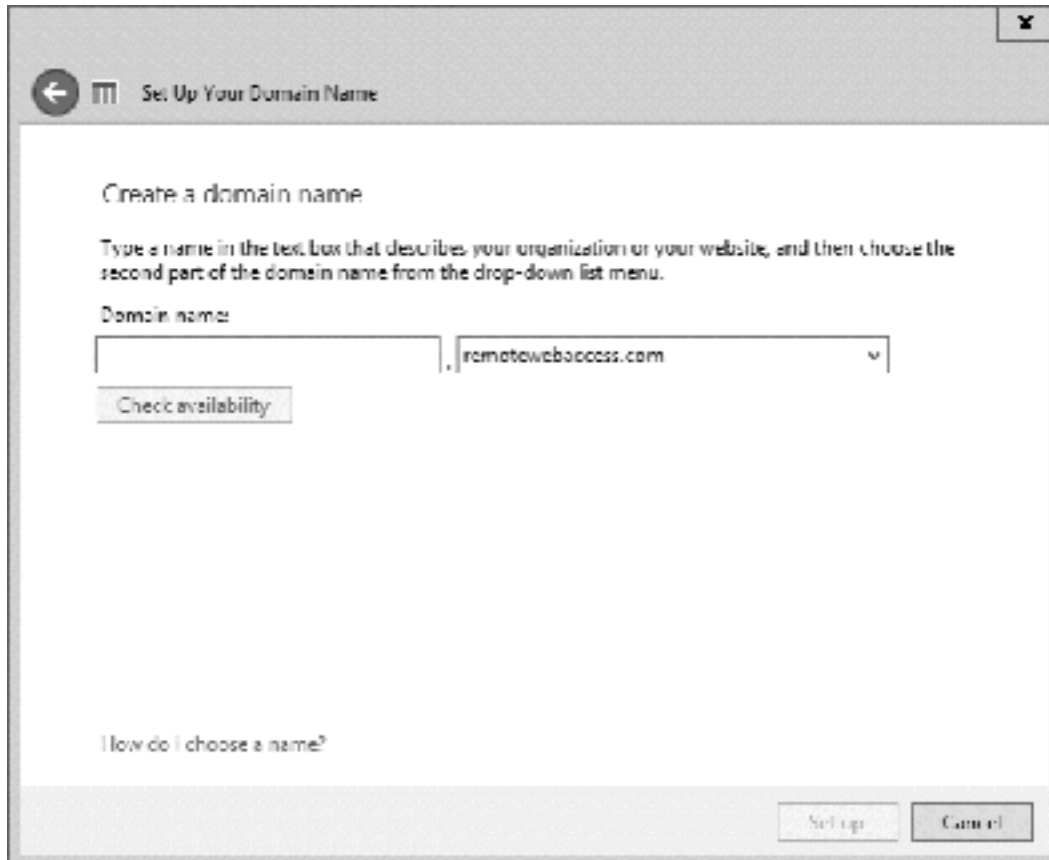
Figure 99: Choose a domain name

You can now choose the first part of the domain name. Type in your choice and click the **Check availability** button. Note that whatever name you decide upon, it will end in *remotewebaccess.com*. So, for instance, if you chose *acmecompany* then the domain name would be *acmecompany.remotewebaccess.com*. If your preferred name is not available then you will have to try for a different one.

Once you have chosen a name and decided to continue, Essentials will think about it for a little while and make some changes to the system. When it has done so, a message confirming that the domain name has been setup on the server will be displayed.

Click **Next** for the following screen. This where you specify what type of access you want and the choices are *Virtual private network (VPN)* and *Remote Web Access*. Unless you have a specific reason not to do so, tick both and click **Next**:
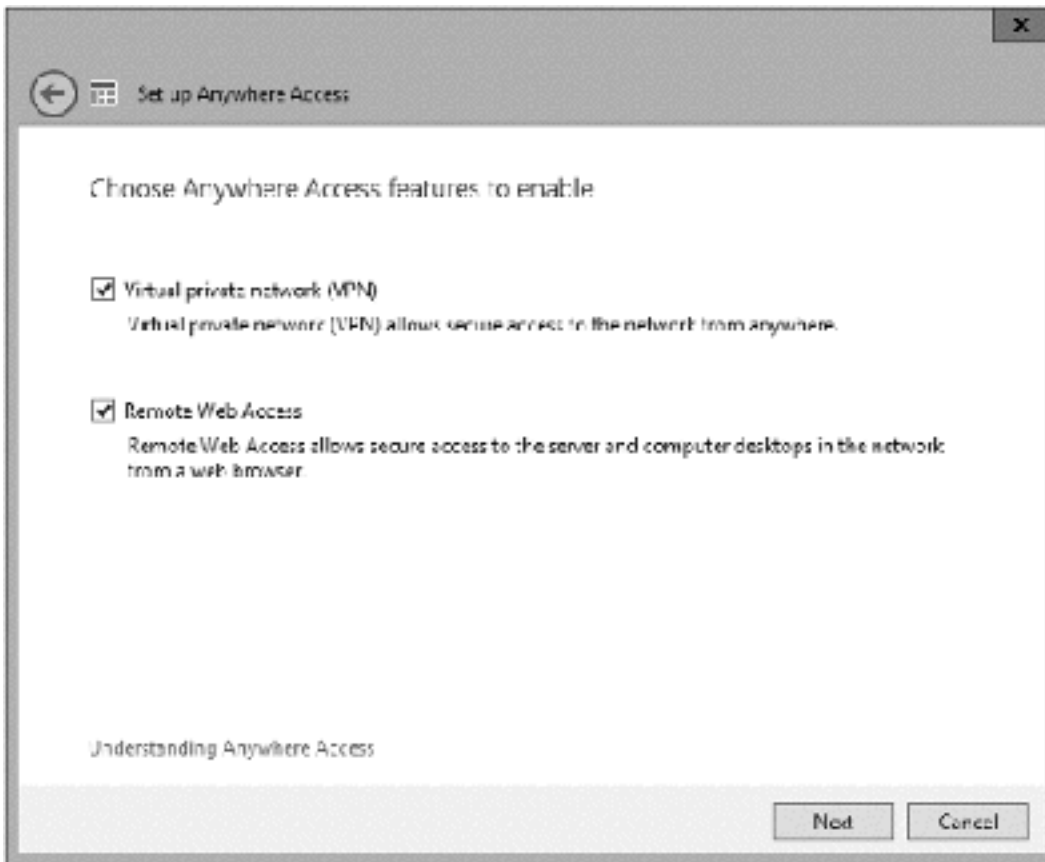
Figure 100: Choose Anywhere Access features

The subsequent screen is for specifying that the existing users and any further ones you create will be granted remote access. If you do not want to do this, you can edit individual users at any point by using the Dashboard:
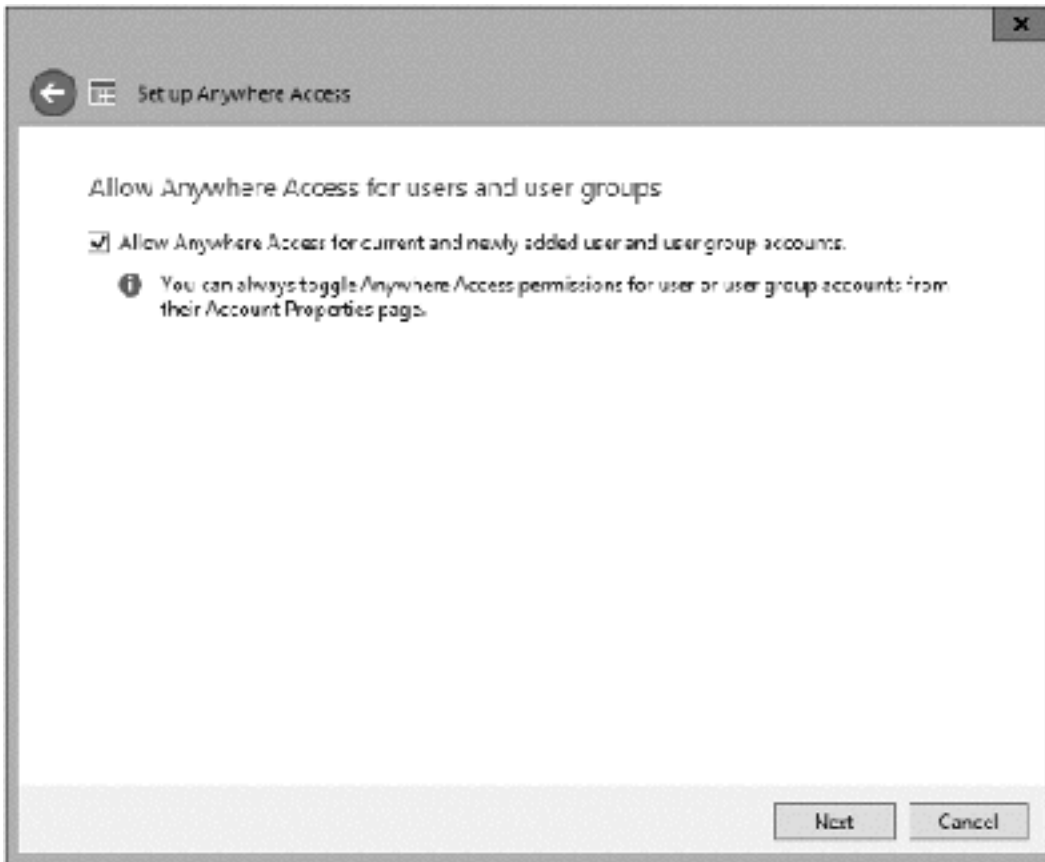
Figure 101: Allow Anywhere Access for users

After a few minutes, Essentials will confirm that everything has been successfully setup. The most common difficulty is that the wizard cannot configure your router, which will happen if the router is a rare or unusual model or if it does not support a feature called *UPnP port forwarding* (an example of a popular router that can cause problems is the Apple AirPort Extreme). In such cases, the router will have to be configured manually. How to do so is really outside the scope of this guide as it depends upon the brand of router; however, instructions for doing so for most routers can be found at the *www.portforward.com* website. From a technical perspective the requirement is to forward ports 80, 443 and 1723 to the internal IP address of the server. Worst case it may be necessary to run the whole process again, but this time look for an option at the beginning that says *Skip router setup. I want to setup my router manually* and tick it.

7.3 Controlling Anywhere Access for Individual Users

The facilities available with Anywhere Access can be customized on a per user basis. To do so, go into the Dashboard and click on **USERS**. Double-click on the user name then click the **Anywhere Access** tab:
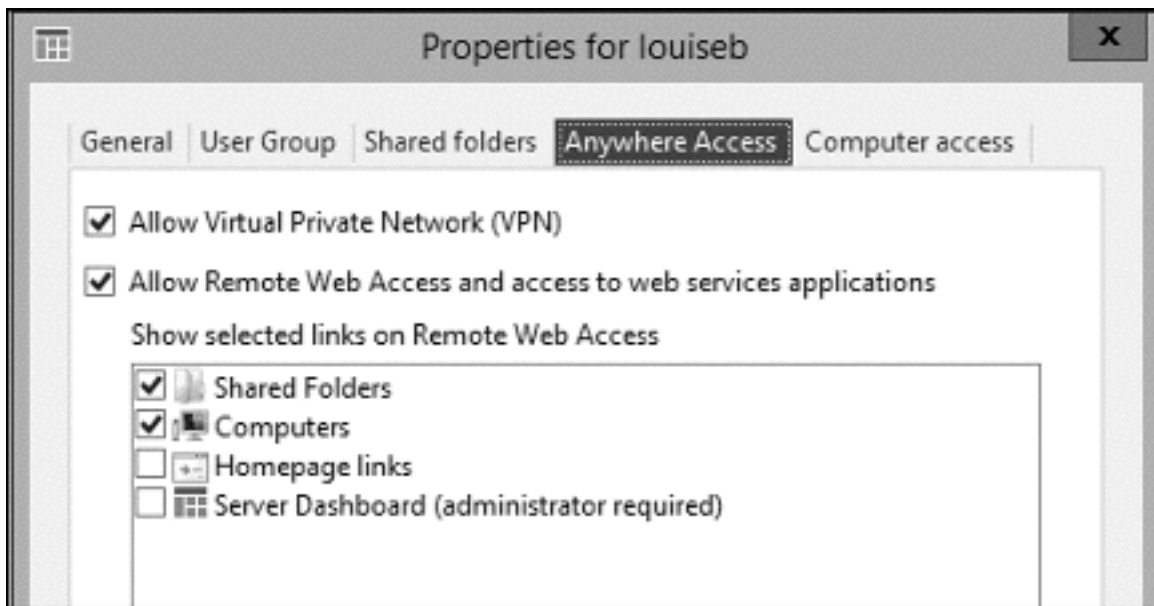
Figure 102: Control Anywhere Access for individual user

There are 6 items that can be controlled:

Virtual Private Network – should be ticked if VPN is to be used
Remote Web Access – has to be ticked for the user to be able to do anything at all
Shared Folders – tick to give access to the shared folders on the server
Computers – allows user to access office computers from outside
Homepage links – not very useful, do not bother to tick
Server Dashboard – only enable this for the administrator(s)

Make any changes then click **Apply**. If the user is to be given remote access to the office computers, you will also need to click on the **Computer Access** tab. This produces the following screen. Note that only computers that have been connected using the *Windows Server Essentials Connector* will be listed.
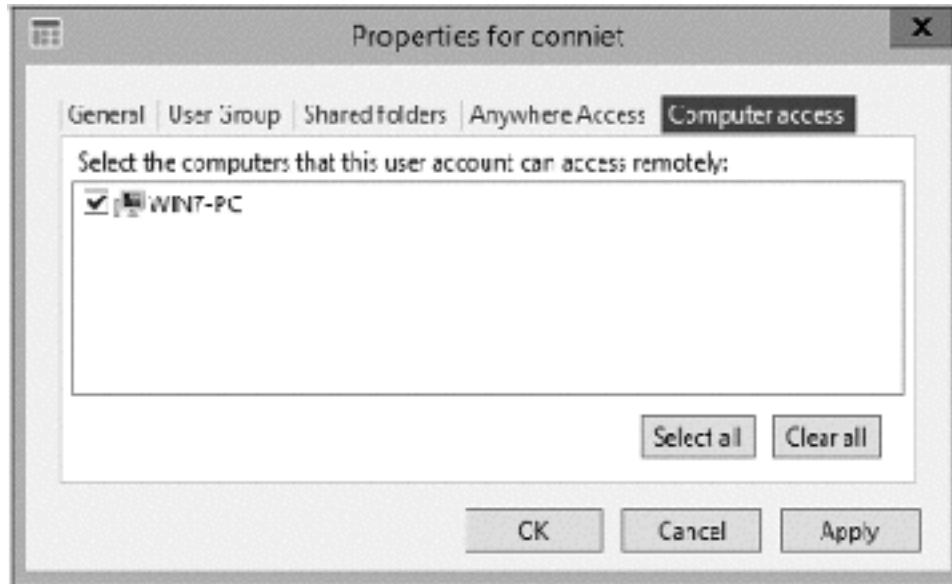
Figure 103: Specify the computers to be used

Tick the computer(s) to which the user is allowed access then click on **Apply**. When finished, click **OK**.

7.4 Using Remote Web Access

The facility that we have just setup – Remote Web Access – enables users to connect to the Essentials server from anywhere in the world using just a browser (e.g. Internet Explorer, Firefox, Chrome, Safari) and without having to install anything or prepare the computer being used in any special way. Just type in the external domain address that you registered e.g. *acmecompany.remotewebaccess.com*, which will cause the following screen to appear after a few seconds. If you are using a browser other than Internet Explorer then you may receive security warnings, but these can safely be acknowledged in this instance. Also note that there may be some minor cosmetic variations in the screens depending upon the browser being used:
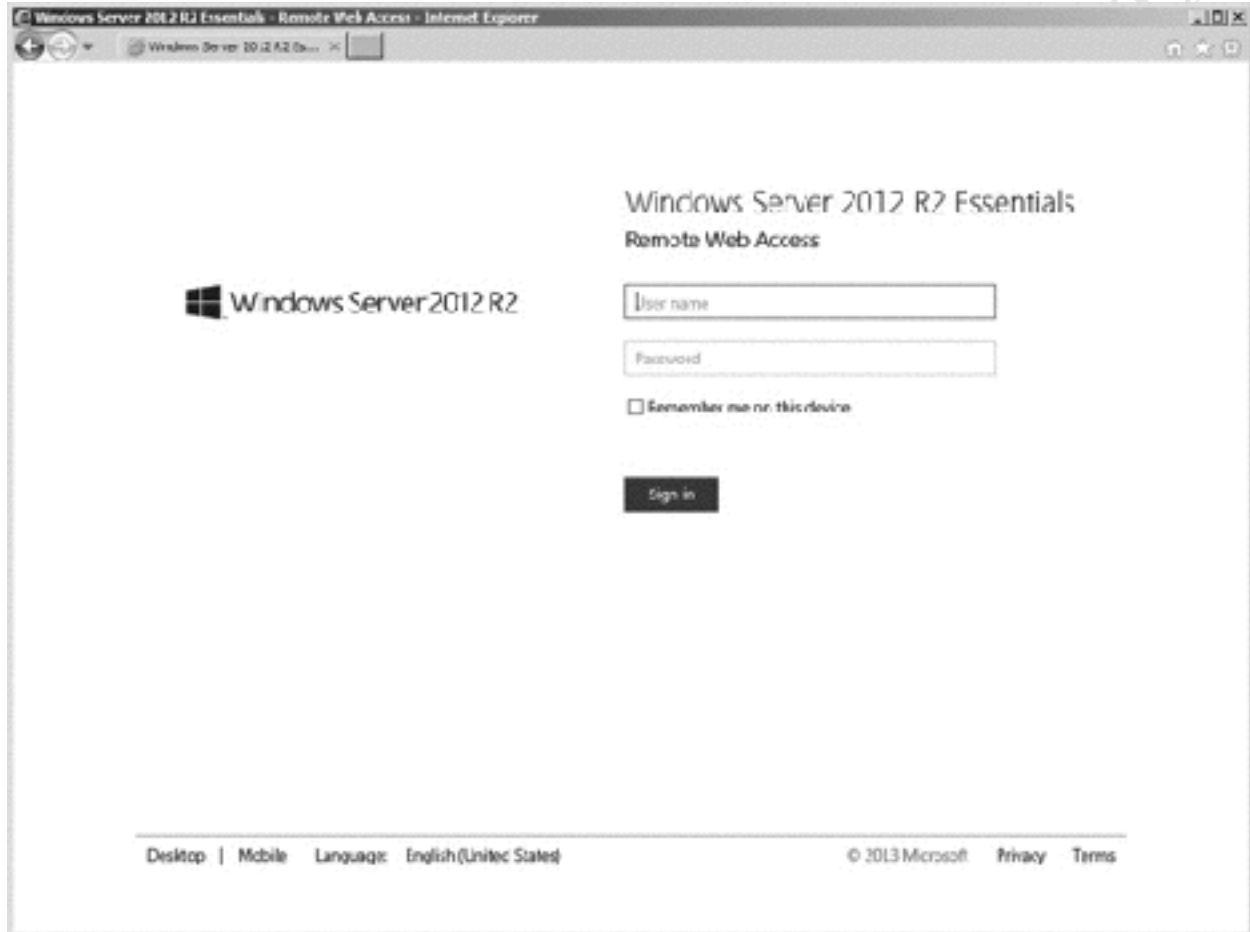
Figure 104: Remote Access login screen

The user now needs to enter their user name and password -   these are the same ones they use with Essentials inside the office. After a few seconds, a screen along the following lines will be displayed. Note that the contents may vary depending upon your particular setup plus it can be customized for individual users (this will be discussed later on). But generally there will be access to the shared folders of the server, along with a list of *Devices*. Devices in this context means any computers located in the office that the user has been given permission for connecting to:
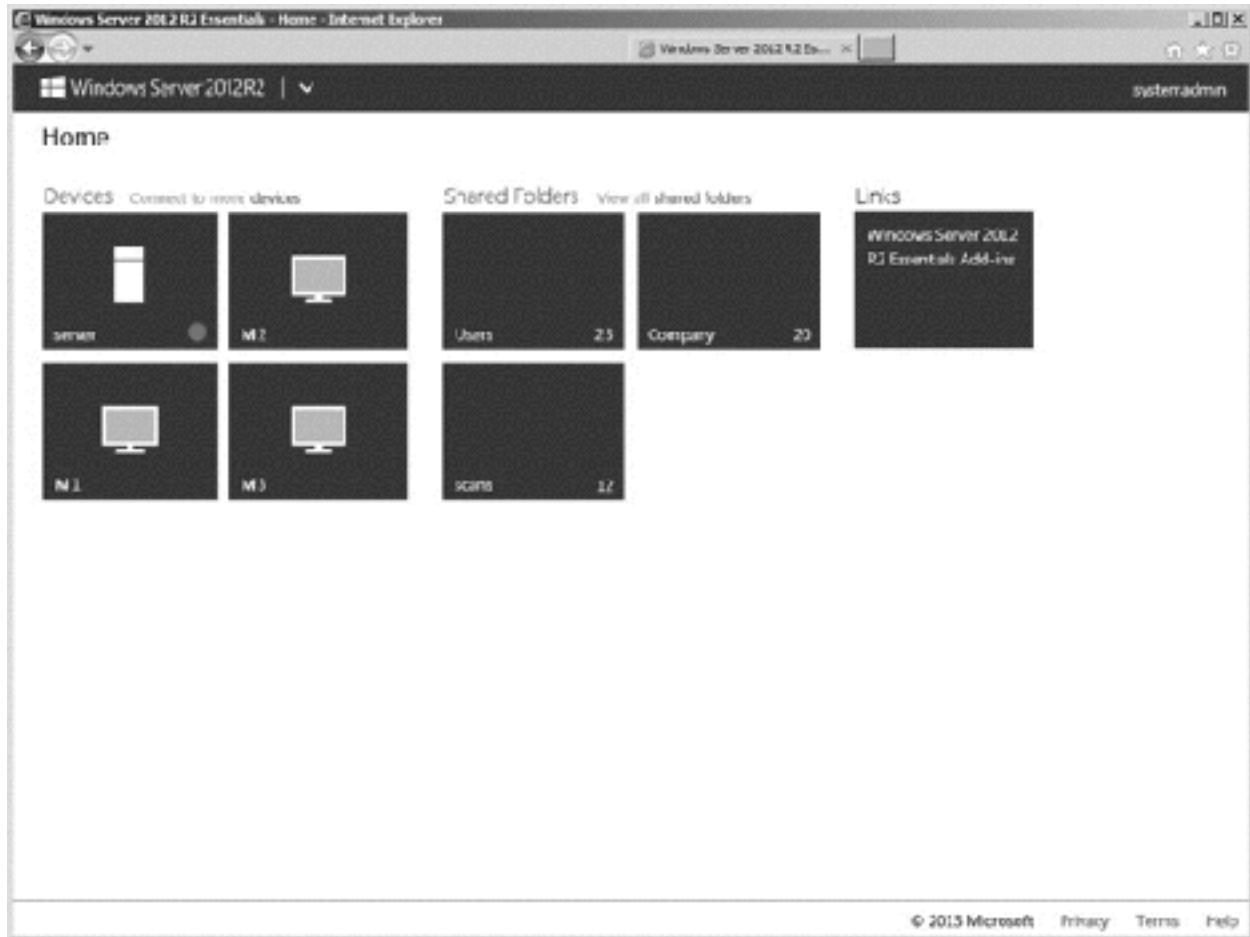
Figure 105: Remote Web Workplace

Clicking on a shared folder causes it to open. Open folders can be viewed as tiles or as a list. Double-clicking on a file allows the user to download it to their local computer, where it can be edited. After it has been edited, or when a new file has been created locally, it can be uploaded back to the server. If you have used the online version of Microsoft's OneDrive the screens will look familiar, as it is based on very similar technology.

The devices (computers) that a user sees depends upon how that user has been configured on the server. A common arrangement is for the user to be given access to their own computer, but you can give access to as many or as few (or none at all) as you wish. When the user clicks on a device, they will be prompted to login to it; usually they will use their standard user name and password. If any messages and warnings are displayed, they can be acknowledged or ignored as appropriate. After a few seconds, they will see their normal computer screen and can use it just as though they were back in the office. However, things may seem a little slower and the mouse may be a bit jerky depending on the speed of the internet connection. Note that the office computer being used has to be left switched on for this to work.

Suggestion: instead of leaving the regular office computers powered on, consider buying one or two computers for remote access use only. These can be located in a locked room or cupboard, or for instance next to the server. They will not need screens or keyboards as they are only ever used remotely.

7.5 Using the VPN (Virtual Private Network)

Note: some governments block VPN access, particularly to computer systems located outside of their territory.

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/kilometres 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 and for some organizations having a VPN is a necessity, which is why Essentials provides the capability. But there are considerations: VPNs can be notoriously difficult to setup, configure and diagnose. For these reasons, many small businesses will be better off using the Remote Web Access described previously and perhaps only use a VPN if it is really needed.

The following section describes how to configure Windows 10 and Windows 7 computers to work with the VPN service, as these are the most popular systems with users of Essentials. VPN clients are also available for other platforms such as Windows Vista, macOS, iPads and Linux.

Click **Start** > **Settings** > **Network & Internet** > **VPN** > **Add a VPN connection** to display the following panel:
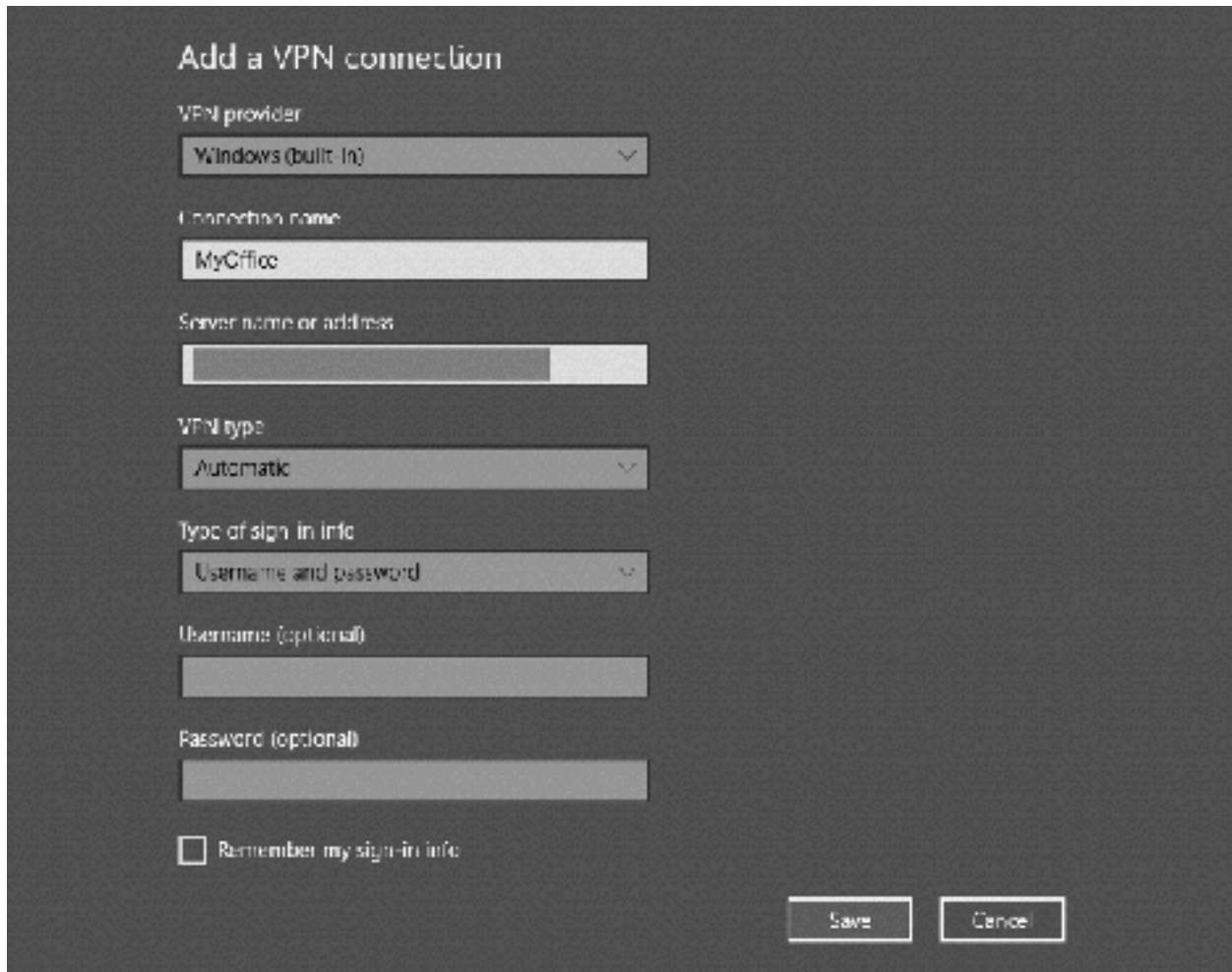
Figure 106: Adding a new VPN connection

Click **VPN provider** and choose *Windows (built-in)*, which will normally be the only option available. Specify a **Connection name** e.g. *MyOffice*. For the **Server name or address** enter the external domain address that you registered earlier. Set the **VPN type** to *Automatic*. The **Type of sign-in info** should be *Username and password*. For security reasons it is suggested that you do not specify what the **Username** and **Password** are and do not tick the **Remember my sign-in info** box. Click **Save** and you will be returned to the main VPN Settings screen.

Now click **Change adapter options**. Right-click the newly created VPN connection – *MyOffice* in our example – and choose **Properties**. Click on 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**.
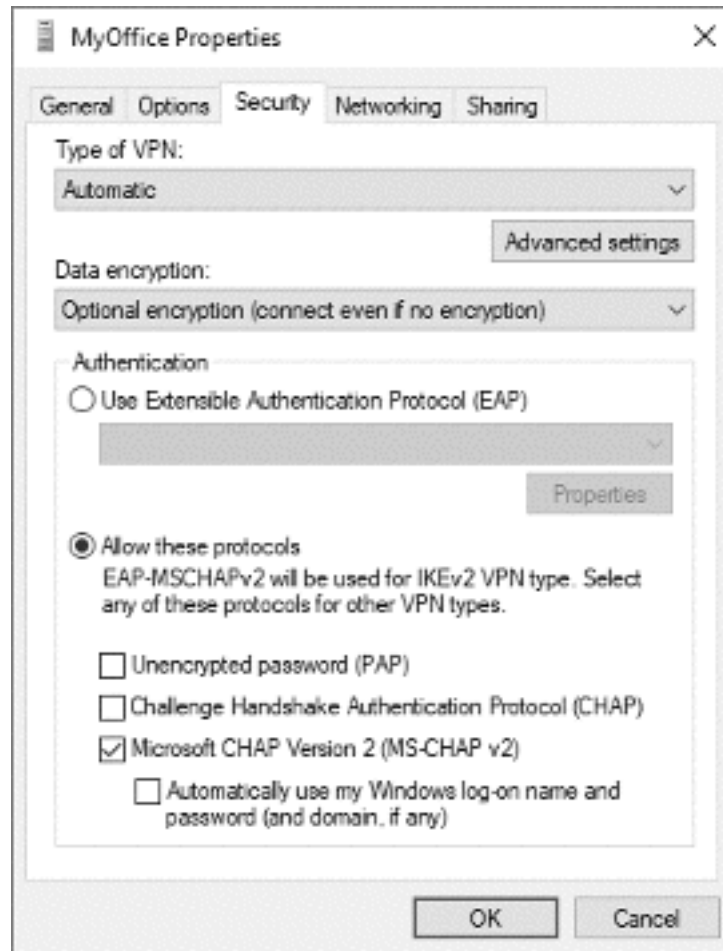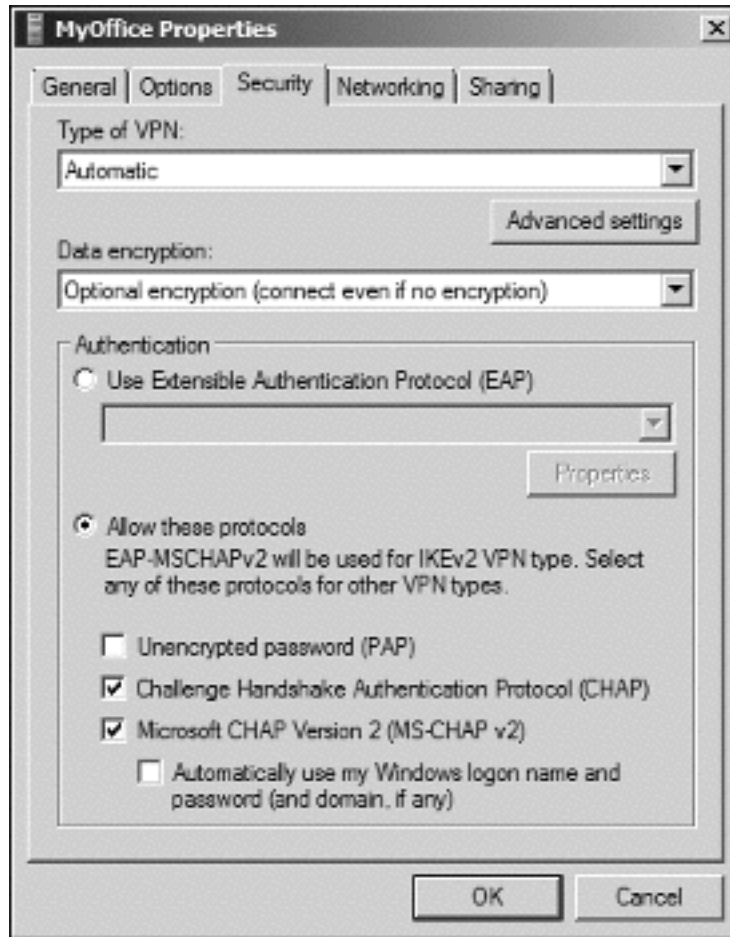
Figure 107: VPN connection properties

Close the Network Connections panel and return to the main VPN Settings screen. Click **MyOffice** and **Connect**. Enter the username and password as defined on the server, followed by **OK**. After a short while, the status will change to *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 using the VPN, click the **Disconnect** button from the VPN Settings screen.

Windows 7 Clients

Go into the **Control Panel** and choose **Network and Sharing Centre**, then click **Setup a new connection or network**. On the panel that pops up choose **Connect to a workplace** followed by **Next**; on the subsequent screen click **Use my Internet connection (VPN)**:
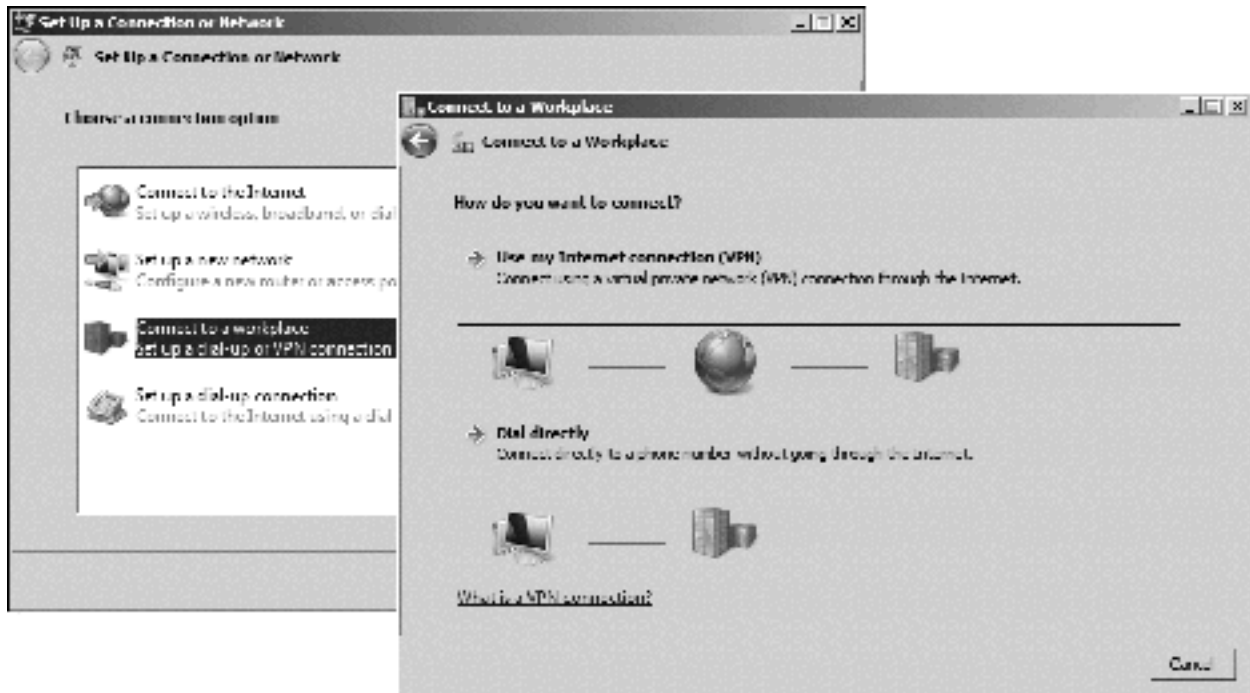
Figure 108: Setup a new connection in Windows 7

On the next panel, specify the external domain address that you registered earlier as the **Internet address**. Specify a **Destination name**, such as *MyOffice*. Tick the **Don't connect now** box and click **Next**:
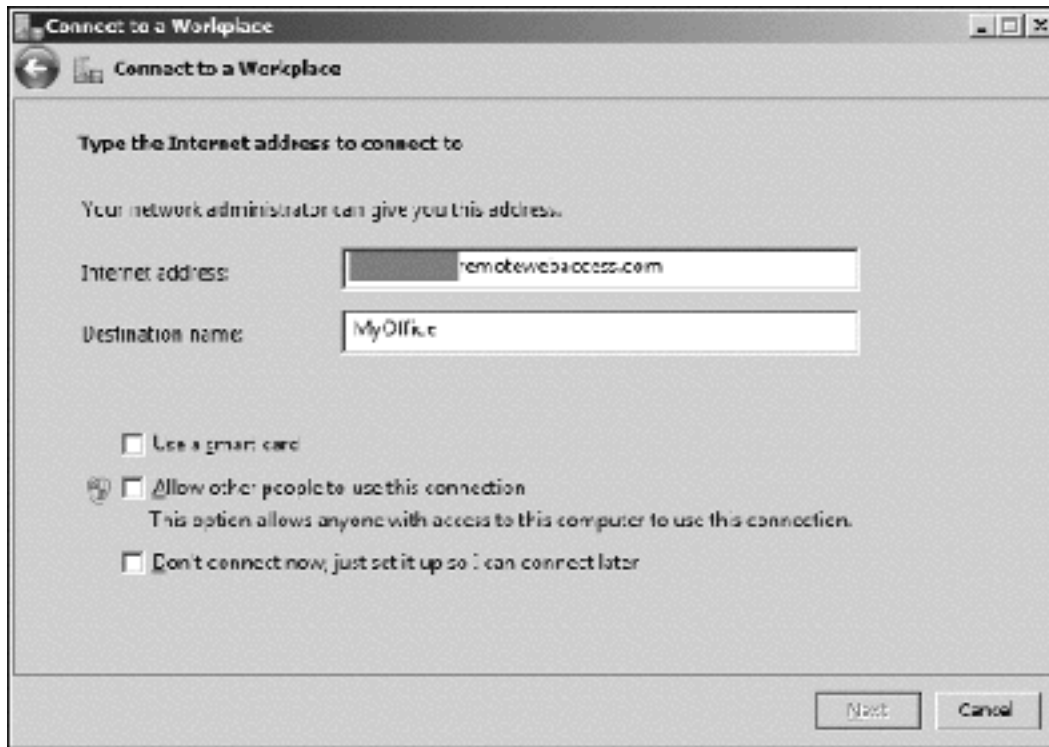
Figure 109: Specify the internet address of the server

On the following screen enter the user name and password (it is not necessary to enter the Domain name):
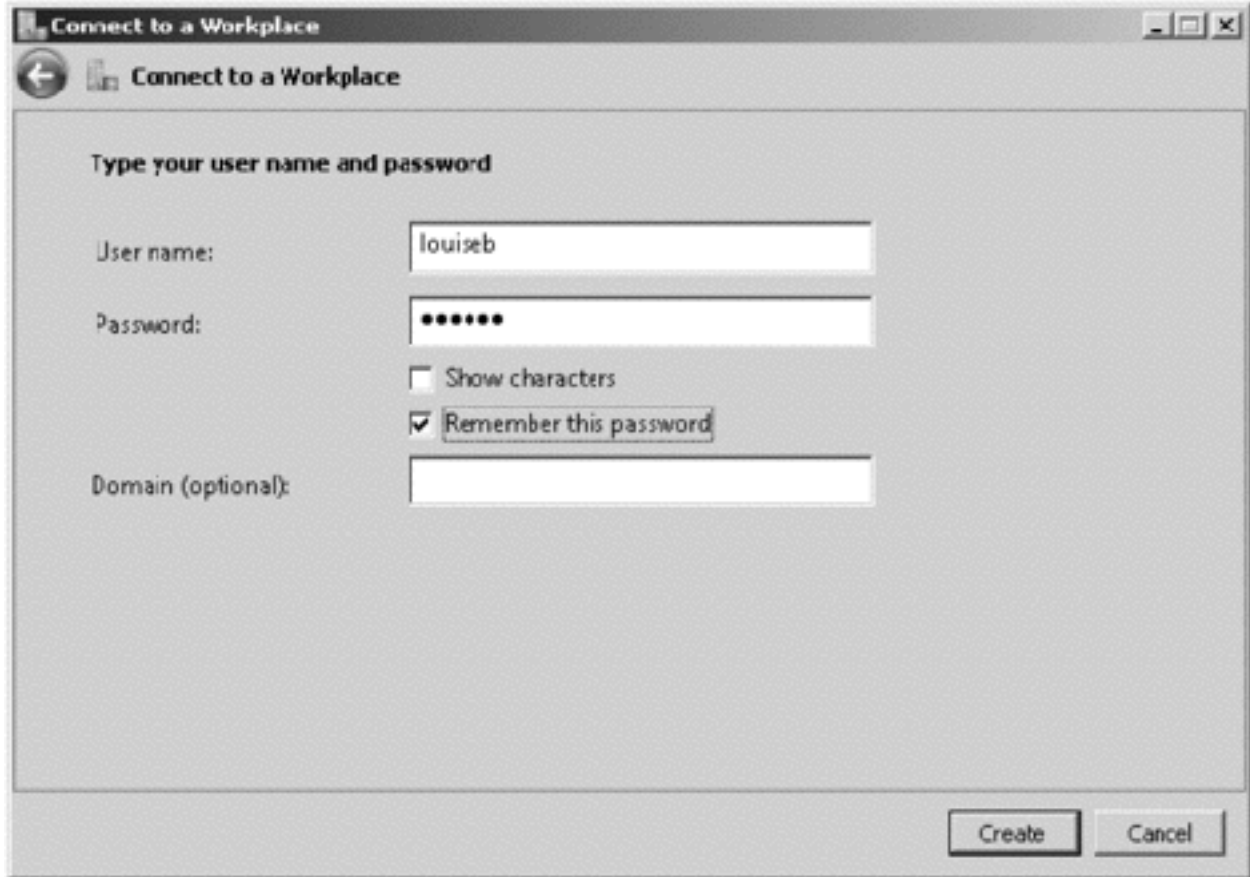
Figure 110: Enter user name and password

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

Returning to the *Network and Sharing Center* screen, click **Change adapter settings**. Right-click the newly created VPN connection – *MyOffice* in our example – and choose **Properties**. Click on 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 111: VPN connection properties

At this point the connection should be tested from outside the premises. Click the network icon on the Taskbar to display a list of available network connections, then click the VPN Connection (*MyOffice* in our example) and the **Connect** button that subsequently appears. A logon panel is shown; enter the user name and password (there is no Domain name) and click **Connect**:
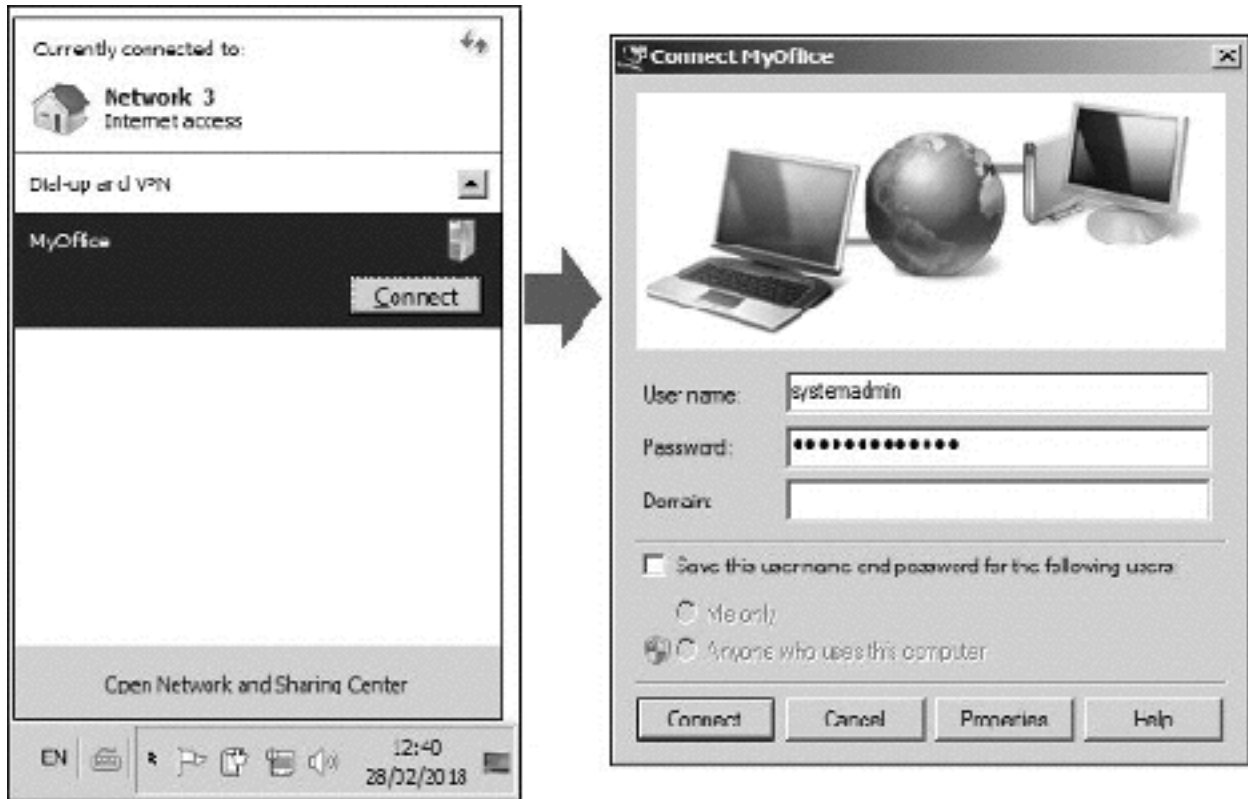
Figure 112: Connecting to the VPN

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, if so choose **Home** or **Work** (they are basically the same thing).

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 ('*MyOffice*') followed by the **Disconnect** button.

7.6. Using Dropbox with Essentials

Essentials has a number of features to enable remote working. However, a simple and popular method that can complement these and provide additional capabilities is Dropbox. Dropbox can provide remote access to data in a simpler method with less effort and on a wider range of devices, plus provide controlled access to selected files for third parties via emailed links. It can also or alternatively be used as a way of backing up data from the server, providing offsite storage to complement the internal backup. Microsoft actually have a direct competitor to Dropbox in the form of OneDrive (formerly SkyDrive), but anecdotally Dropbox seems to work far better on Essentials.

There are five main considerations when using Dropbox with Essentials:

1.   A single Dropbox account has to be used for everyone

2.   The account should have sufficient space. A standard free account only has 2GB of space (plus any additional space gained through referrals). This is unlikely to be enough so consider a paid account; for instance, a Dropbox Pro account provides 1000GB space for $9.99 US equivalent per month

3.   Whether it will be used for additional backups or as a means of providing remote access to data when out of the office

4.   Who has access to it (if used for backups only, then only the server administrator needs access)

5.   Who will be responsible for managing it (usually the person who controls the server administrator account)

Install the Dropbox client on the server. This is best done by downloading it directly from the Dropbox home page. Note: this will be easier if you first disable the Internet Explorer Enhanced Security feature as described in 12.2 Disabling Internet Explorer Enhanced Security. As soon as the installation is complete, click **Advanced settings** as this allows you to specify the Dropbox location. For the location, choose the shared folders location, which is typically *D:\ServerFolders* (although it may be on a different hard drive on your system). Note that Dropbox automatically installs itself as what is called a service, meaning it will start-up automatically each time the server restarts.

Next, launch the Dashboard and go to the **STORAGE** section. Click the **Server Folders** tab. On the right-hand side under 'Server Folder Tasks' click **Add a folder**. Enter a name of *Dropbox* and make sure that it picks up the correct location. As the Dropbox folder already exists, Essentials will use it rather than create a new one. Click **Next**:
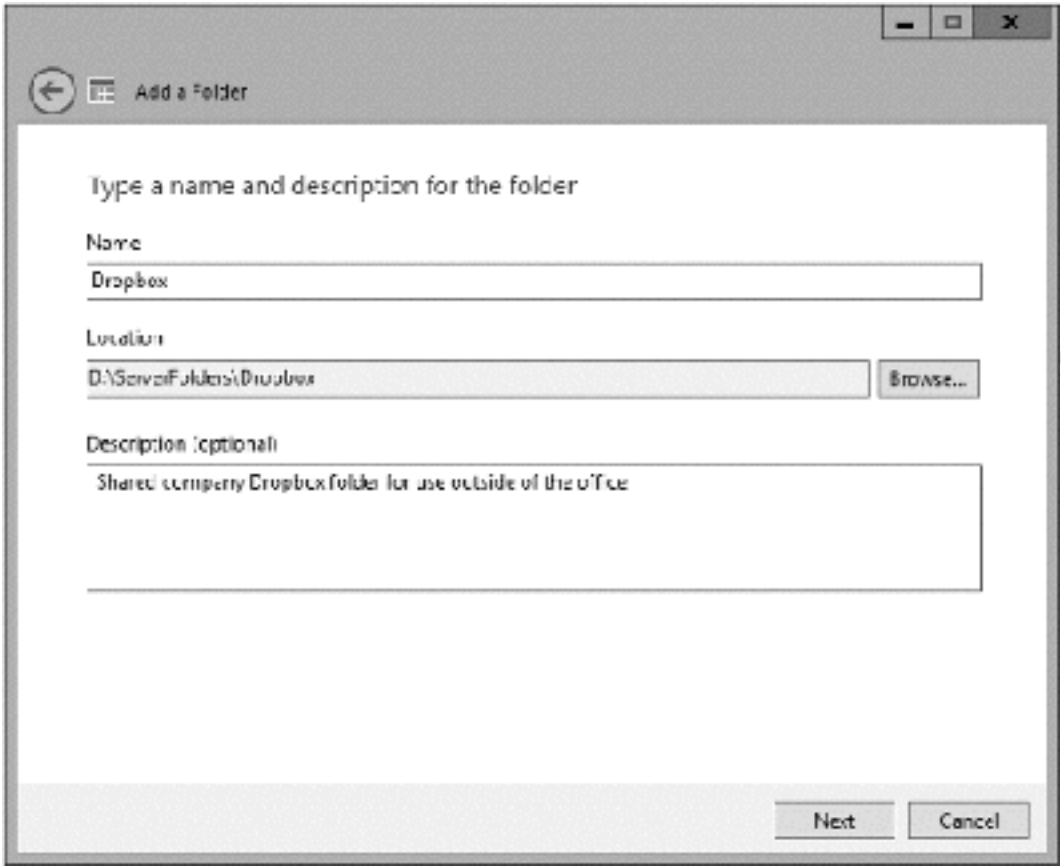
Figure 113: Add a folder for Dropbox

On the following screen, specify who has access to the Dropbox folder. The choices are Read/Write (i.e. full access), Read Only (i.e. retrieve things from Dropbox but not be able to add things) or No access. Then click **Add folder**:
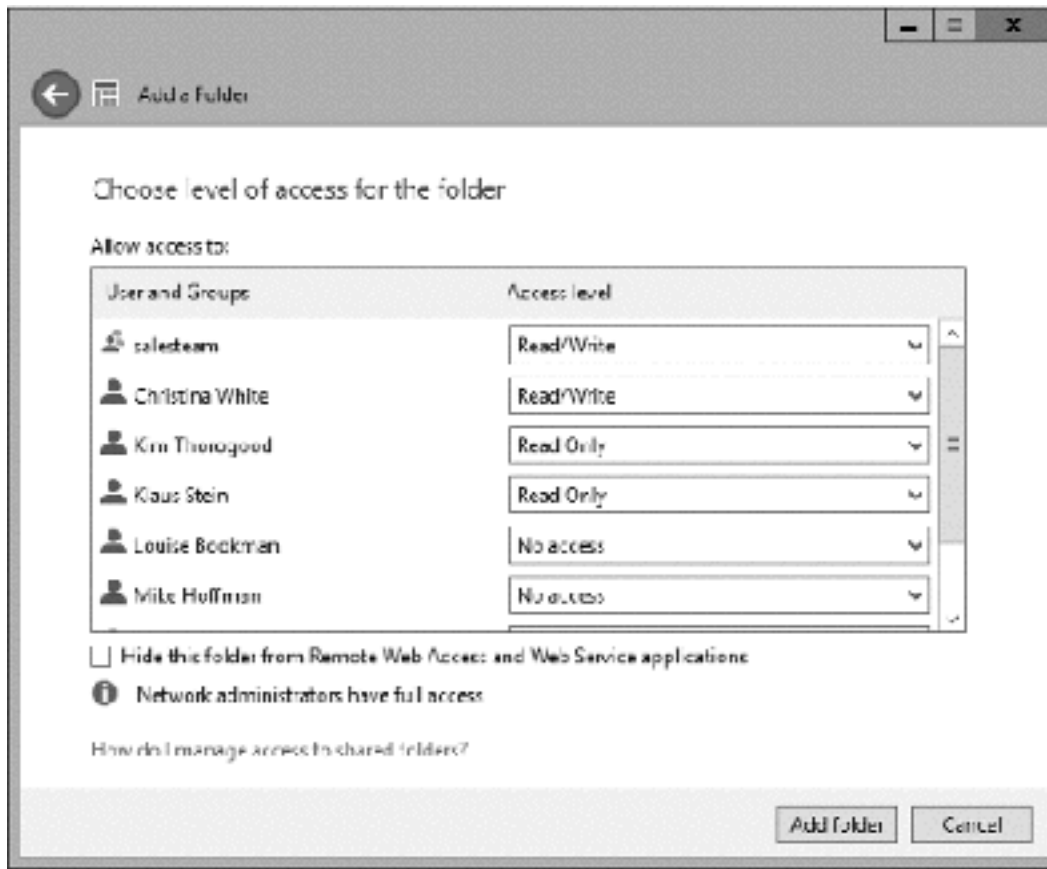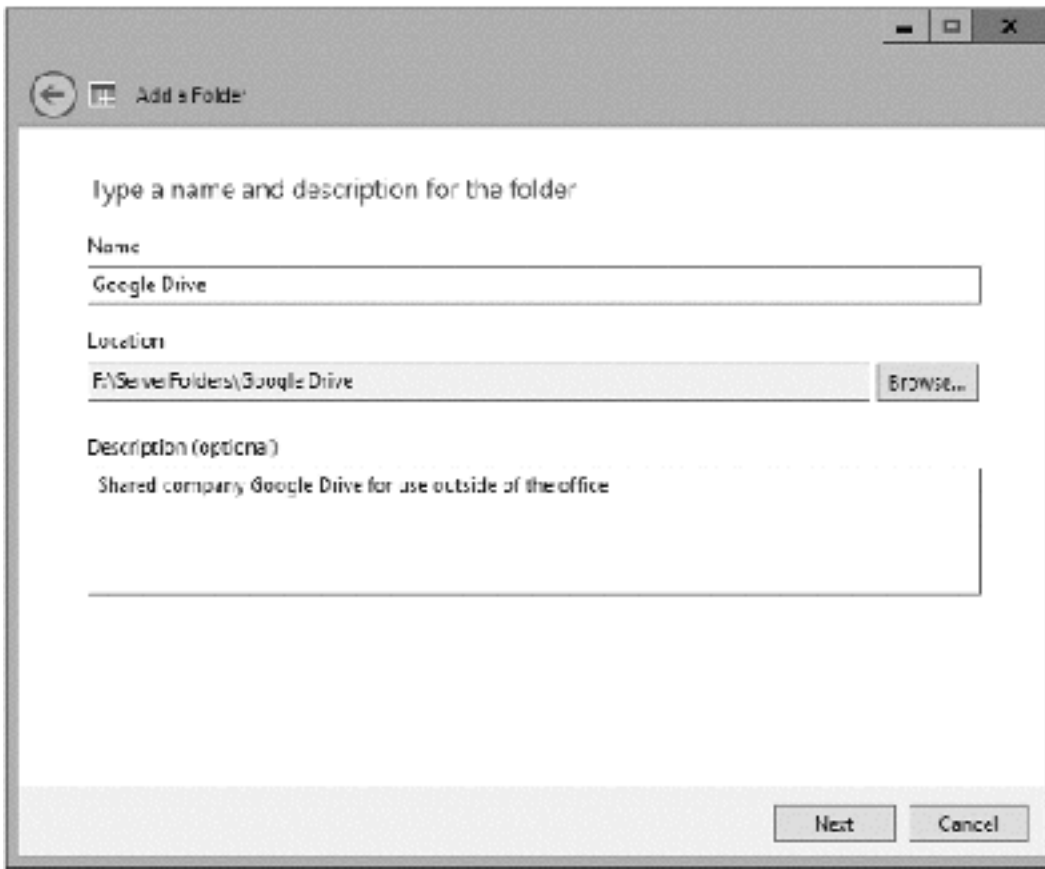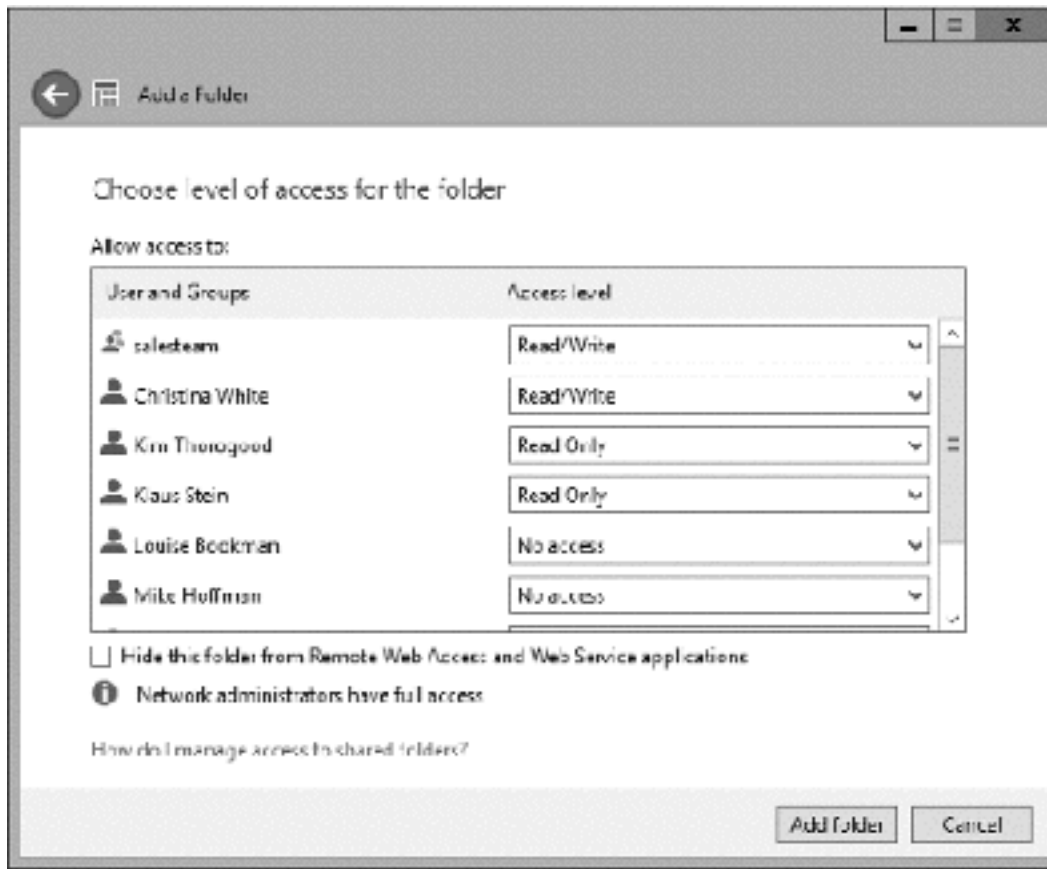
Figure 114: Specify the access level for the users

A confirmation screen is displayed upon completion. It is not actually necessary to check the Server Backup Configuration so just click the **Close** button.

To gain access, the permitted users should now have the Dropbox client installed on the devices they use outside of the office, downloadable from *www.dropbox.com*. It is suggested that the users are not given the password and allowed to install it themselves, so as to reduce the risk of errors or abuse. At the time of writing, Dropbox is available for: Windows, macOS, iPad & iPhone, Android, Windows Phone, Blackberry and selected Linux distributions.

To make files available outside of the office, they simply have to be placed in the *ServerFolders\Dropbox* folder.

One thing to consider is what happens when people leave the organization, as if they have Dropbox installed on a home computer they will continue to have access to whatever is stored on the server's Dropbox folder. In such circumstances it will be necessary for the administrator to change the password of the Dropbox account and advise remaining staff of the new password. Dropbox Pro and Dropbox for Business both have the capability to 'remote wipe' devices and this can be used to remove the organisation's data from the former user's computer.

7.7. Using Google Drive with Essentials

Google Drive provides 15GB free storage; optional paid plans are available to increase this amount. Begin by going to the Google website and downloading and installing the Google Drive client on the server. Note: this will be easier if you first disable the Internet Explorer Enhanced Security feature as described in 12.2 Disabling Internet Explorer Enhanced Security. When you reach Step 4 pause and click on the **Advanced setup** button:
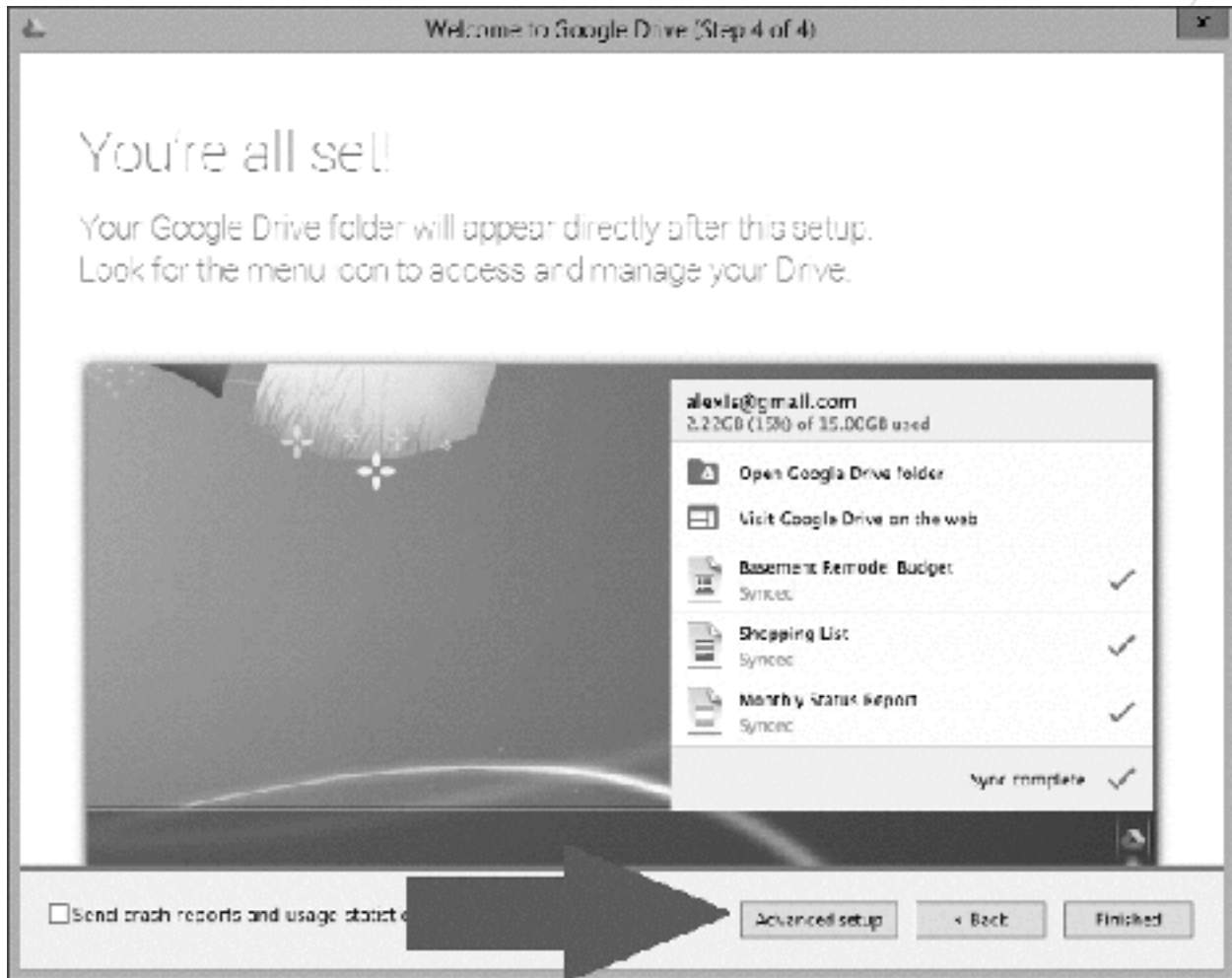
Figure 115: Installing Google Drive

This will display a panel where you can specify the location for Google Drive, which is necessary as the default location is unsuitable for our purposes. Click the **Change** button and navigate to the shared folders location, which is typically *D:\ServerFolders* (although it may be on a different hard drive on your system). Click **Make new folder** and create one called *Google Drive* within *ServerFolders* (it does not actually need to be called *Google Drive* but this makes it obvious what it is). Then click **OK** and **Start Sync**:
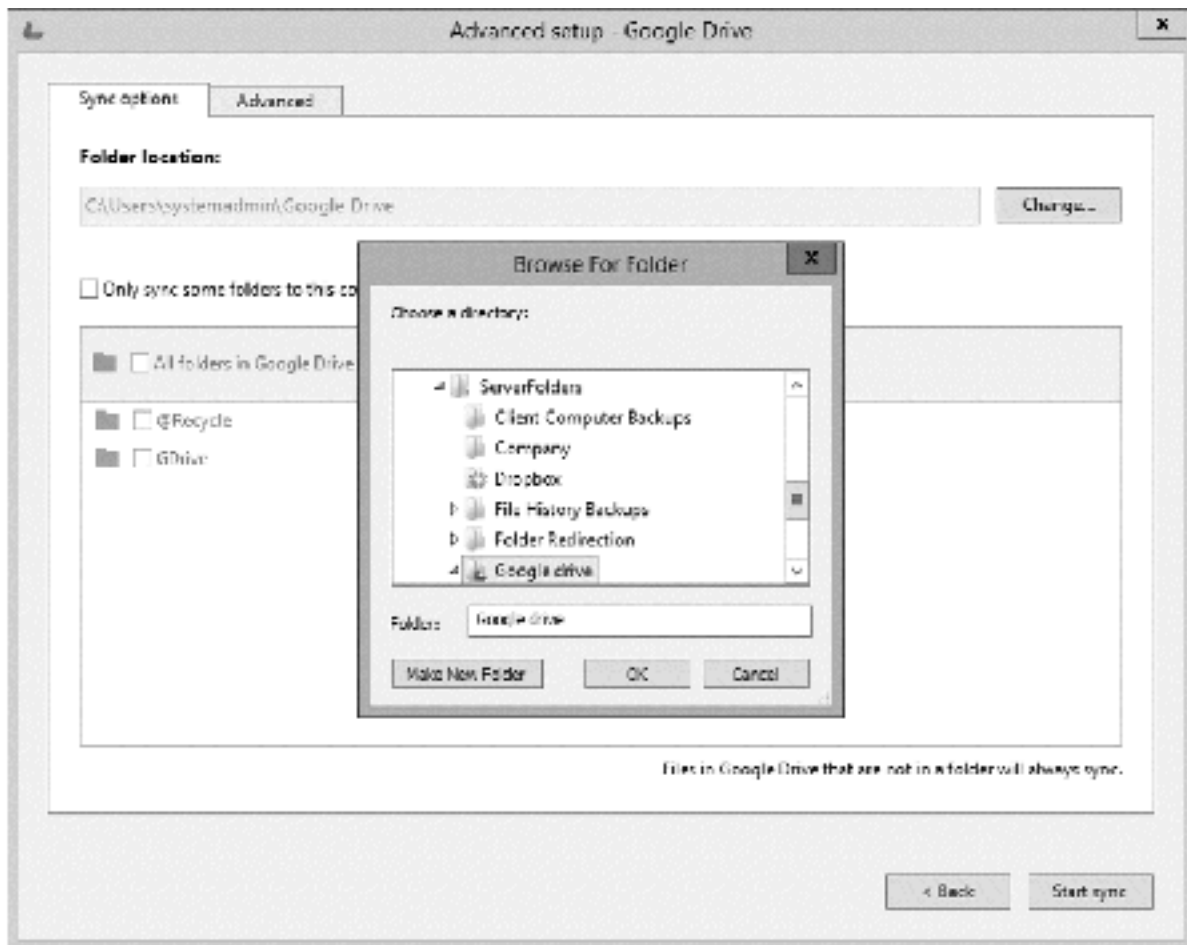
Figure 116: Specifying a folder for Google Drive

Next, launch the Dashboard and go to the **STORAGE** section. Click the **Server Folders** tab. On the right-hand side under 'Server Folder Tasks' click **Add a folder**. Enter a name of *Google Drive* and make sure that it picks up the correct location. As the Google Drive folder already exists, Essentials will use it rather than create a new one. Click **Next**:

Figure 117: Add a folder for Google Drive

On the following screen, specify who has access to the *Google Drive* folder. The choices are Read/Write (i.e. full access), Read Only (i.e. retrieve things from Google Drive but not be able to add things) or No access. Then click **Add folder**:

Figure 118: Specify the access level for the users

A confirmation screen is displayed upon completion. It is not actually necessary to check the Server Backup Configuration so just click the **Close** button.

To gain access, the permitted users should now have the Google Drive client installed on the devices they use outside of the office, downloadable from Google. It is suggested that the users are not given the password and allowed to install it themselves, so as to reduce the risk of errors or abuse. At the time of writing, Google Drive is available for: Windows, Mac OS X, iPad & iPhone and Android.

To make files available outside of the office, they simply have to be placed in the *ServerFolders\Google Drive* folder.

One thing to consider is what happens when people leave the organization, as if they have Google Drive installed on a home computer they will continue to have access to whatever is stored on the server's Google Drive folder. In such circumstances it will be necessary for the administrator to change the password of the Google account and advise the remaining staff of the new password. However, any existing data will remain on the user's computer and the implications of this need to be considered.

8. WORKING WITH MOBILE DEVICES

8.1 Overview

Most portable devices such as iPads, iPhones and Android tablets and cell phones are not able to directly connect to domain-based Windows networks in the sense that a desktop computer or laptop can. However, this does not mean that they cannot access data and be used in a productive manner. A variety of apps and techniques are available to both access data and administer the server and some of the main ones are discussed below.

8.2 Accessing the Server using File Browser

For iOS users, *File Browser* from Stratospherix is a good way of accessing folders and files on the server. It is a commercial product obtainable from the App Store, but is inexpensive and well worth buying. It is not specifically designed for Essentials, rather it is a generic tool for accessing pretty much any computer or NAS. To use, enter the IP address of the server plus a valid user name and password. The user can use any of the folders to which they have been granted access (for example, the *Company* folder). To access their home folder, double-click the *Users* folder then double-click the folder that has the same name as their own user name. Note that they can see the names of other people's home folders, but will not be able to access them because of security restrictions. Files can be viewed, but not edited.
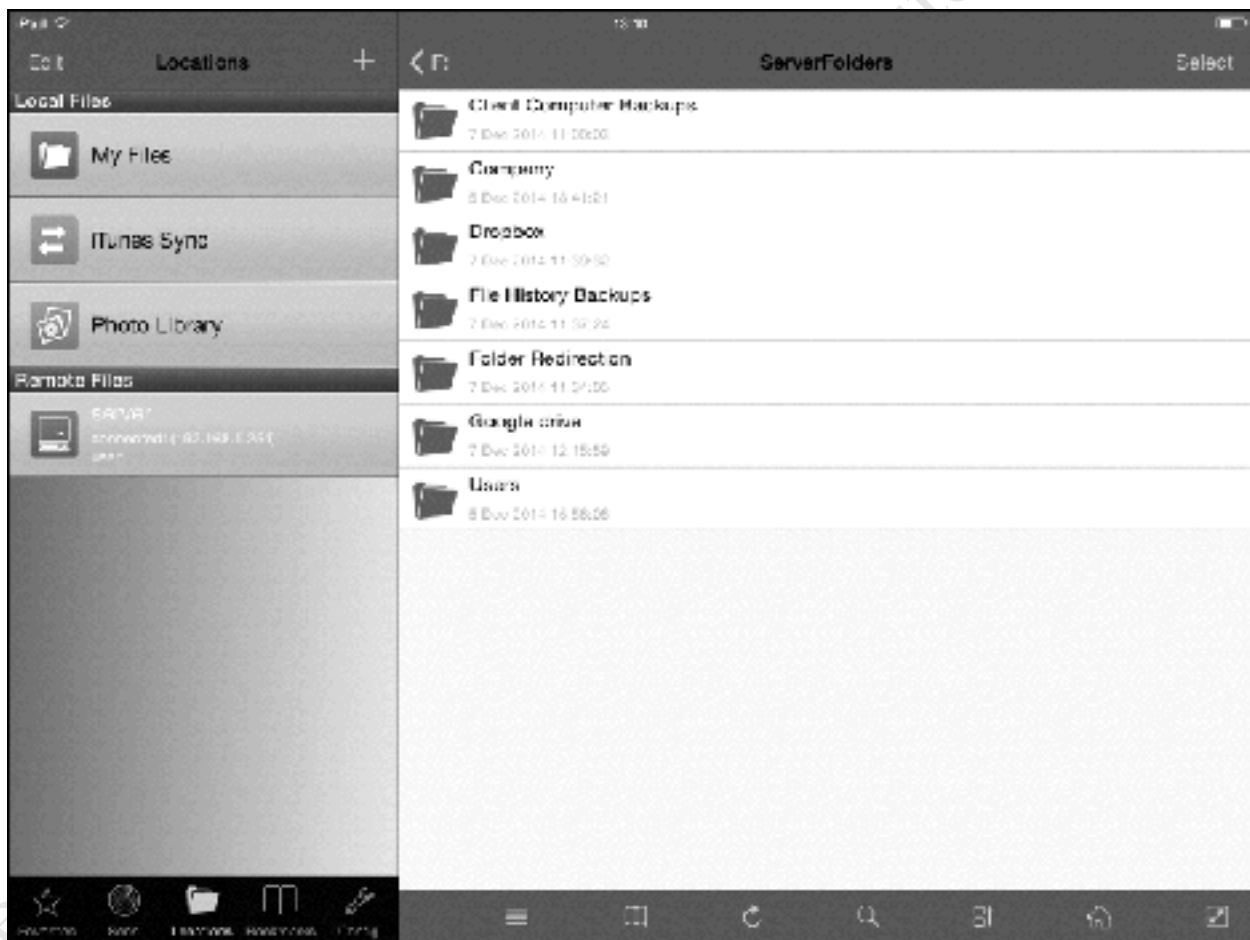
Figure 119: File Browser from Stratospherix running on iPad

8.3 Using Dropbox and Google Drive

Dropbox and Google Drive provide indirect routes to accessing data on the server. They have a number of advantages: firstly, they are available on a wide range of portable devices. Secondly, they require minimal knowledge to get it up and running on the client devices (users can do it themselves, for example). Thirdly, they are free (or rather can be, depending on the amount of storage the organization requires). Installation of Dropbox on Essentials is covered in sections 7.6. Using Dropbox with Essentials and 7.7. Using Google Drive with Essentials.

8.4 My Server App for Windows Phone

My Server is an official app from Microsoft for use with Windows Phone devices, specifically designed for managing Essentials servers. It can be used for managing users, devices and alerts, analogous to a mobile version of the Dashboard. It also provides access to the shared folders, although some people find it fairly rudimentary.

8.5 Microsoft Remote Desktop app for iOS

Microsoft have an official app for iOS that enables the server to be accessed remotely for administrative purposes. It is basically an RDP client, suitable for generic access to any Windows Server i.e. it is not specific to Essentials. It can be downloaded free of charge from the App Store.

Whilst working on a small screen with no keyboard imposes some restrictions, Microsoft have done a good job with this tool. To improve usability, the Remote Desktop app has a virtual keyboard and a screen zoom facility. Pressing down with a finger for a couple of seconds is equivalent to a right-hand button mouse click, which is very useful.
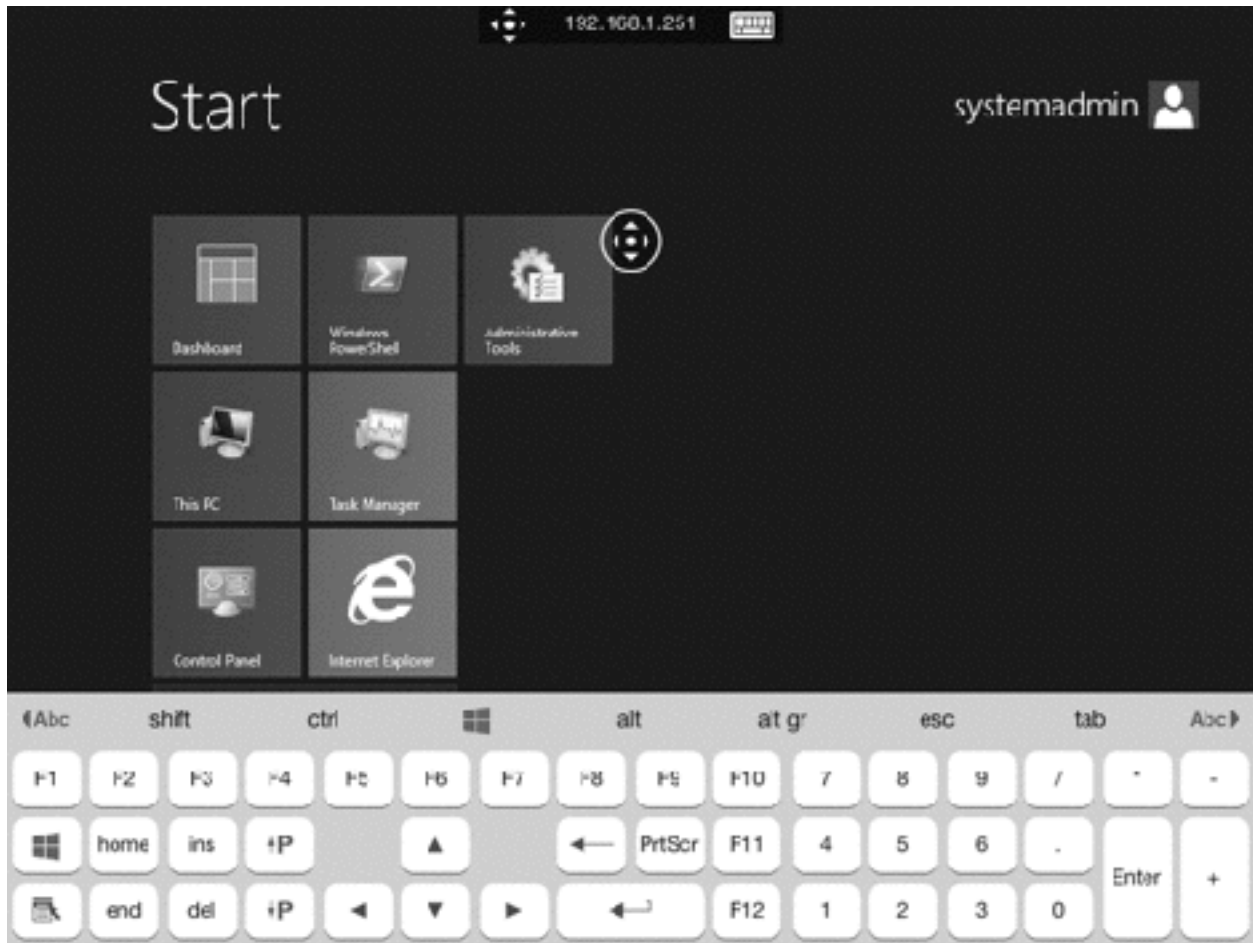
Figure 120: Microsoft Remote Desktop app running on iPad

8.6 Chromebooks

Chromebooks are a popular computing choice for many people and organizations. In essence a Chromebook is a laptop that only runs a browser; the underlying operating system is very minimalist compared to Windows and this means it does not currently understand file servers i.e. it cannot logon to a domain. As such it is only possible to do things that can be done within a browser, but this still gives some possibilities:

- A Chromebook can be used for remote access, as the Remote Web Access service is of course web-based. Using a Chromebook is largely the same as using a regular PC and browser, as described in 7.4 Using Remote Web Access.

- A Chromebook can be used to remotely administer the server. To do so requires RDP client software. There are several available, but one that works quite well is *Chrome RDP* from Fusionlabs.net. This is available from the Chrome Store; it is a commercial application but the license is only US $9.99 (a 7-day trial version is available for those who want to try-before-they-buy).

- If a Cloud-based file sync service such as Dropbox, Google Drive or Box is being used with the server, then it will be possible to access the data from the Chromebook by logging in to the appropriate website. Of these services, Google Drive is possibly the most useful because of the tight integration with Chrome and the ability to edit files using Google Docs.

- To directly access the files and folders of the server in a more conventional manner, *File System for Windows* may be useful. This is a free download from the Chrome store and extends Chrome OS to understand the SMB protocols used in Windows networks.

9. HOUSEKEEPING AND MONITORING THE HEALTH OF THE SYSTEM

9.1 Overview

The Essentials server needs to be checked on a regular basis to ensure that there are no problems. Clearly some types of problem will be immediately apparent, for example if the server is powered down for whatever reason then nobody will be able to use it. But there are plenty of other things that need to be monitored; for instance: Has the backup completed successfully? Is the server running out of storage space? To help with this, Essentials has tabs on the Dashboard to view the status plus generate status reports. These reports can be run manually as required, or can be configured to run automatically on a regular basis and emailed to interested parties (usually meaning the system administrator). Additionally, there are some housekeeping tasks that need to be carried out on an occasional basis.

9.2 Checking the Dashboard

If there are any issues, they will be immediately apparent whenever the Dashboard is open. Issues are indicated by a warning indicator at the top of the screen:
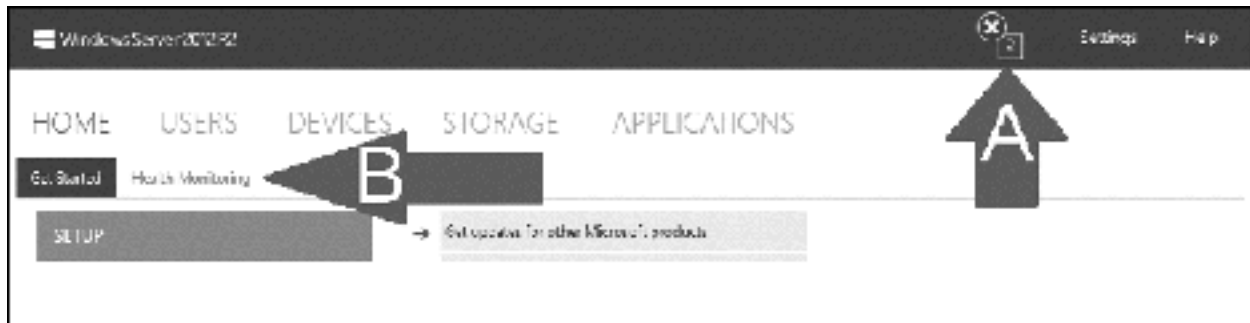
Figure 121: Checking the Dashboard

If the indicator is shown ("A"), click on the tab labelled **Health Monitoring** ("B") to display a supporting screen:
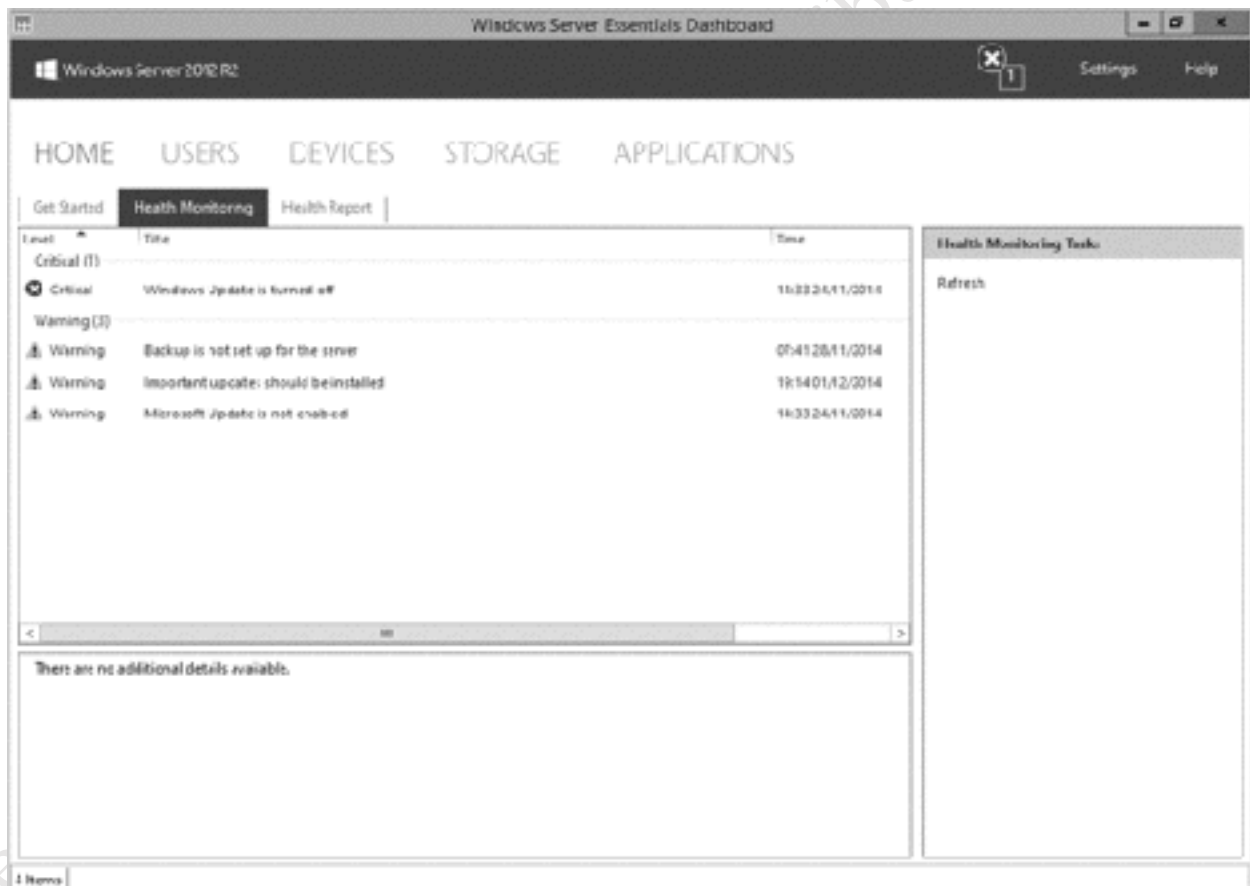
Figure 122: Health Monitoring tab in Dashboard

Alerts may be *Critical* – implying that they should be addressed as soon as possible – or *Warnings*, meaning that they can usefully be addressed but that it is not a matter of urgency. Having said that, some judgement is required as many alerts can be considered as informational only e.g. Windows updates not

being switched on. As an alert is highlighted, a more detailed description and suggested resolution is displayed at the bottom half of the screen.

On the right-hand panel, several options may be given for the highlighted alert, usually to ignore or delete it. However, sometimes a clickable option of **Try to repair** the problem is offered, which can be useful.

The Dashboard also reports on the status of the computers. Click on the **DEVICES** tab and all the computers that have been connected will be listed, along with their status. For instance, in the example below we can see that the computer in question is healthy in all aspects:

Name ▲	Status	Description	Backup status	Update status	Security status	Alerts	Group Policy
Computers (11)							
Win81pc	Online	Mary's computer	Successful	🔔 Up to date	🔔 In compliance	✅ No alerts	Implemented

Figure 123: Health status of a computer

9.3 Generating a Report

To the right of the Health Monitoring tab is the Health Report tab; this is used to generate a comprehensive "all-in-one" report on the status of the Essentials server and any issues. Reports can be run manually when required, or automatically on a scheduled basis.

Click on the **Health Report** tab. In the right-hand panel under Health Report Tasks there will, assuming this is the first time it has been used, be two entries: 'Generate a Health Report' and 'Customise Health Reports settings'. Click **Generate a Health Report**; this will take only a few seconds to run, after which the report will be listed in the upper left-hand panel:

Figure 124: Health Report tab in Dashboard

There will now be additional tasks in the right-hand panel to open or delete the newly generated health report. Make sure the report is highlighted then click **Open the Health Report** to display it in its own window. When it has been read through, it can be closed and kept or deleted as preferred.

9.4 Customizing the Health Report

The health report can provide a lot of information, some of it useful, some of it less so. For instance, it is important to know that the backups are working and how much free storage space is on the hard drives, but the report might also produce information on fairly obscure topics that are sometimes better described as 'theoretical problems', as they do not really affect normal operation. The issue with having too much information is that is becomes difficult to separate the wheat from the chaff; fortunately, it is possible to customize what topics are reported upon.

To do so, the Health Report screen needs to be open. On the right-hand panel a list of tasks is displayed, one of which is 'Customize Health Report Settings'. Click it to display the following screen:
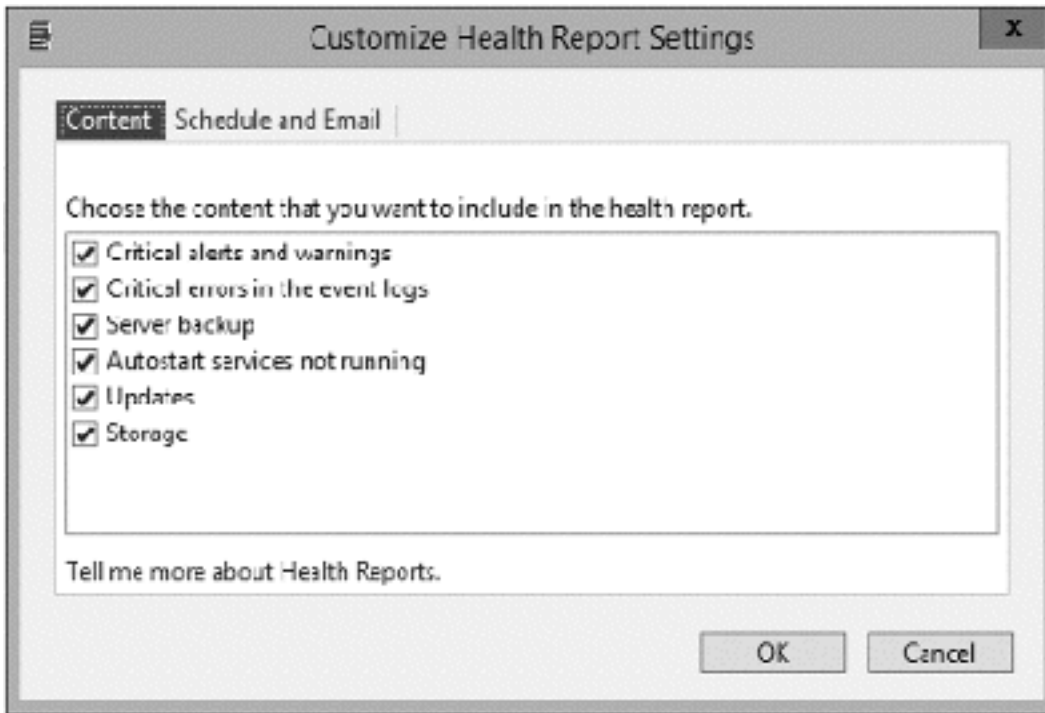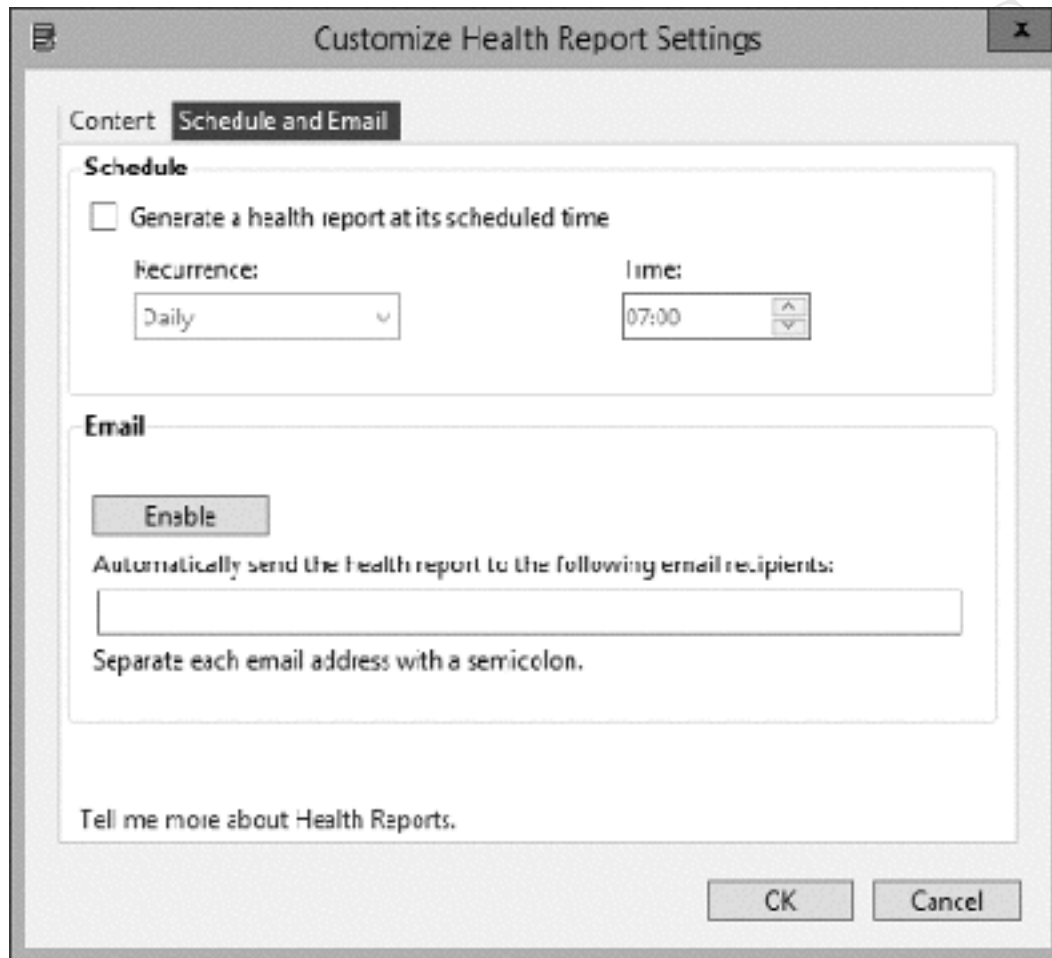
Figure 125: Health Report settings

Remove the ticks from any items that are not of regular interest then click **OK**. If there is ever reason to investigate an apparent problem then it is a matter of seconds to restore the options and generate a more comprehensive report.

9.5 Setting up a Scheduled, Emailed Report

Rather than run a report manually, it might be more convenient to setup a report than runs automatically on a scheduled basis and, optionally, have it emailed to the network administrator or other interested parties. Emailed reports are particularly useful as they do not require physical access to the server, which is a consideration if you are, for example, an IT consultant supporting a customer with Essentials or normally work away from the office.

To schedule a report, open the Health Report screen. On the right-hand panel listing the available tasks click **Customize Health Report Settings**. This is the same screen as in the previous section but this time click the **Schedule and Email** tab to display this screen:

Figure 126: Schedule a Health Report

Click the **Generate a health report at its scheduled time** box. Use the **Recurrence** drop-down to specify a Daily or Hourly schedule (although the latter is overkill for most situations). If choosing the daily option, specify what time of day the report should run. One suggestion is to have it run early in the morning – that way you are prepared for any problems when you arrive at the office. If you choose hourly, it runs every hour on the hour. Click **OK**.

To have the reports emailed, click the **Enable** button in the email section. A panel for email settings is displayed and the following information needs to be entered: who the email is from (which must be an existing email account); the name of the SMTP server; the SMTP port (usually 25 but check first); whether or not the SMTP server requires a secure SSL connection; whether the SMTP server requires

authentication (they usually do); the user name and password of the person sending the email as specified in the first field. Then click **OK**:

Figure 127: Specify email settings

Having hit **OK** you will be returned to the first screen, where you can enter the email addresses of the recipients for the reports. You should include yourself on this list.

9.6 Optimizing the Hard Drives

The hard drives on the server should be optimized (defragmented) on a regular basis to reduce file fragmentation and maximize performance. As with all modern versions of Windows, this can be scheduled to take place automatically.

Display the **Start Screen** and click the icon for **Administrative Tools**. On the resultant list of tools double-click the icon for **Defragment and Optimize Drives** to show the following panel:
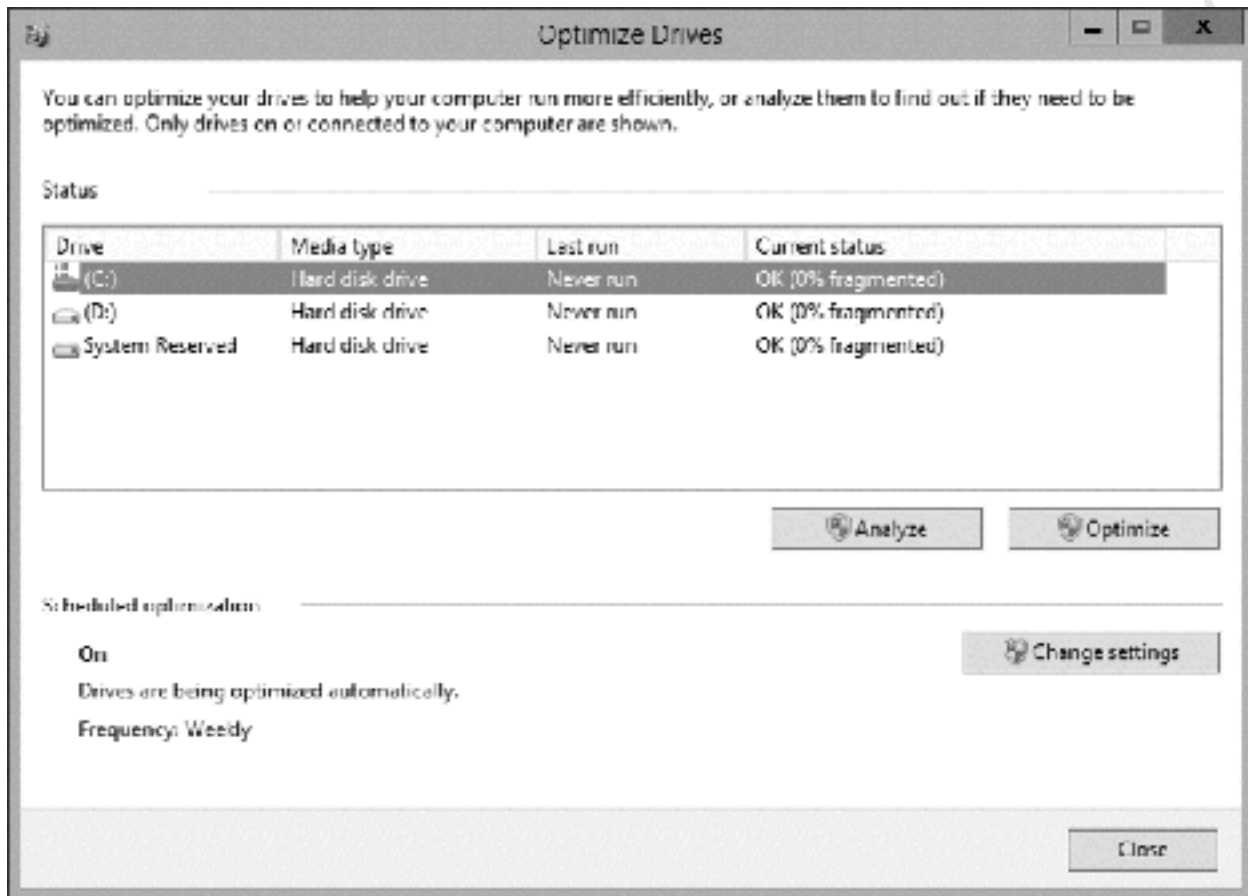
Figure 128: Optimize the hard drives

Towards the bottom left-hand corner it should read that Scheduled optimization is 'On' and that the drives are being optimized automatically on a weekly frequency. If this is not the case, click the **Change settings** button and adjust the settings accordingly.

Important: if the server includes any Solid State Drives (SSD's) then they should never be optimized – it is not necessary and will shorten their lifespan. Turn off scheduled optimization and optimize any conventional hard drives on a manual basis every week or so. This can be done using the panel displayed above: highlight the drive, click **Analyze** to determine its status then click **Optimize** if necessary. Note that Essentials is usually smart enough to identify SSD's itself, but it is worth checking in case it has not correctly done so.

9.7 Applying Windows Updates to the Server

Earlier on in this guide it was suggested that automatic Windows updates are not enabled on the server. The reason for this is to ensure total control over the process and stop the risk of the server rebooting on its own accord after certain updates. However, it is still important to check for and apply regular updates or when Microsoft issues any patches for Essentials. It is suggested that this work is done out of hours so as to avoid any disruption to service, perhaps once a month or so.

To do so, display the Start Screen and choose **Control Panel** (as a matter of general convenience it is suggested that the Control Panel view is switched from Category to Large icons). Click the icon for **Windows Update** and on the resultant panel click **Change settings**. On the next screen, change the setting to **Never check for updates (not recommended)** and click **OK**.
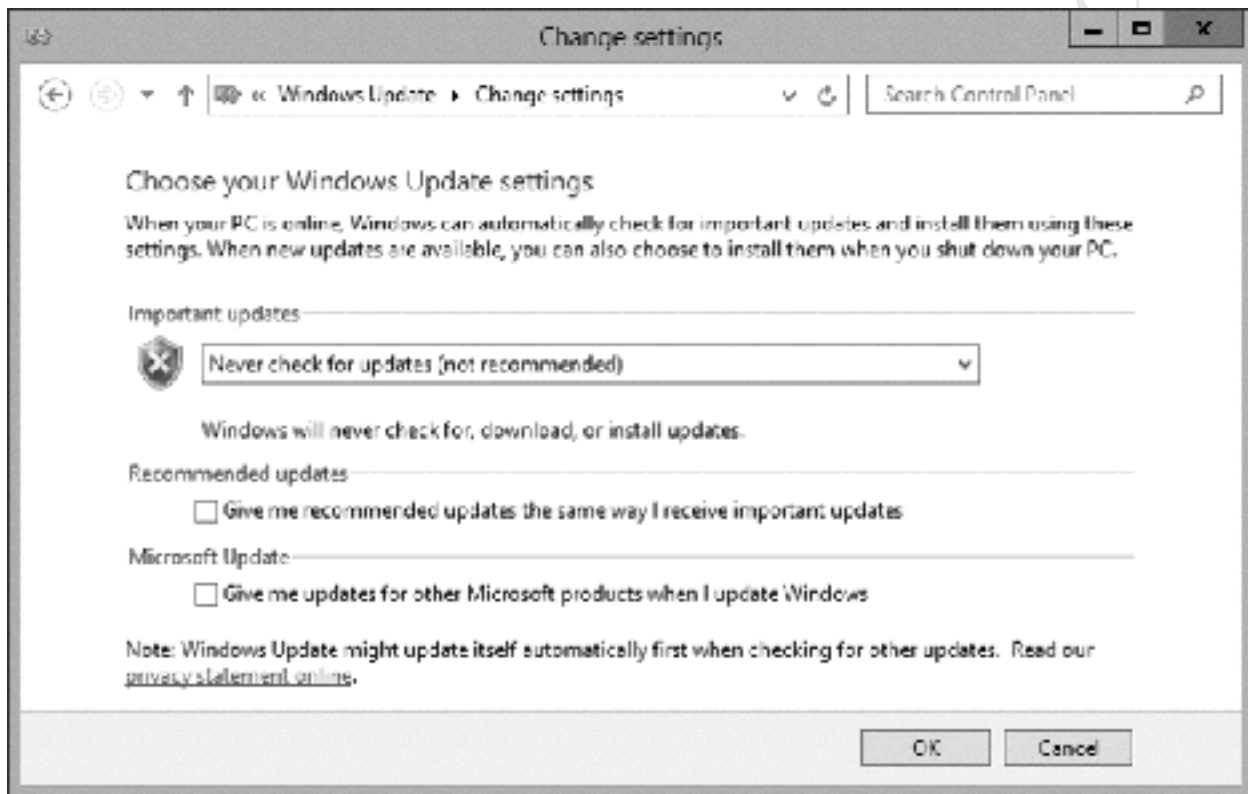
Figure 129: Windows Update settings

The above step is a one-off; from now on, you can simply go into Windows Update and click **Check for Updates** whenever you wish.

9.8 Shutting Down and Restarting the Server

The server is usually left running continuously but there will be occasions when it needs to be restarted (e.g. following updates) or shutdown (e.g. to add hardware). There are two ways of doing so:

Method 1 - From the Start Screen. Press the **Start** button to display the Start Screen. Click on the power icon in the top right-hand corner of the screen and choose **Shut down** or **Restart/Update and restart**:
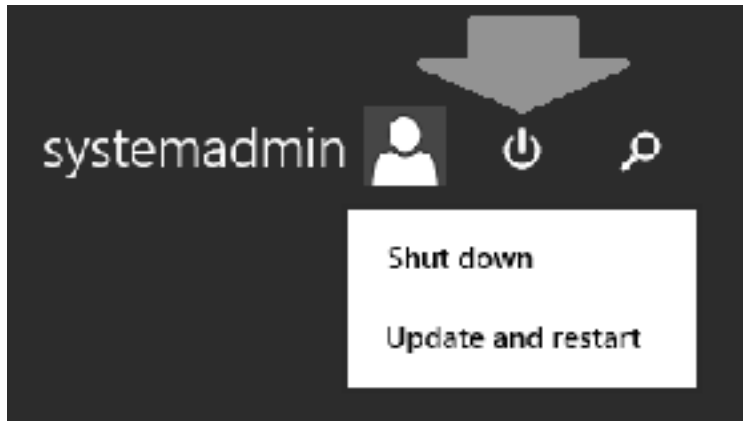
Figure 130: Shutting down from the Start Screen

You will be prompted to enter a reason for shutting down the server – choose one from the drop-down menu and click **Continue**.

Method 2 – From the Start button. Right-click the **Start** button and choose Shutdown or sign out. Choose the desired option from the list. You will be prompted to enter a reason for shutting down the server – choose one from the drop-down menu and click **Continue**.

9.9 Task Manager and Resource Monitor

Task Manager and *Resource Monitor* are built-in tools that can be used to help identify bottlenecks on servers that have performance problems, such as running slowly. Whilst the diagnosis and resolution of problems is a specialist topic that goes outside of the remit of this guide, they do provide useful information that most system administrators will find helpful. For instance, if a bottleneck with the network adapter was identified then it might be an option to add a second and 'team' it as described in 12.11 Multiple Network Adapters (NIC Teaming). Incidentally, *Server Storage* systems are always supplied with dual network adapters.

Many users will be familiar with the Task Manager as it is common to all versions of Windows. To start it, right-click on the **Taskbar** and choose **Task Manager** from the pop-up menu; it may appear as a blank panel, in which case click the **More details** button in the bottom left-hand corner to display the following screen:

Figure 131: Task Manager Processes tab

On this *Processes* tab, Task Manager provides useful information about how busy the server is and how much memory is being used. For instance, if a process is hogging the CPU or memory it can be identified and, if appropriate, terminated.

Clicking on the **Performance** tab provides information in a graphical format for CPU, Memory and Ethernet (i.e. the network connection) and is useful for monitoring what is happening with the server:
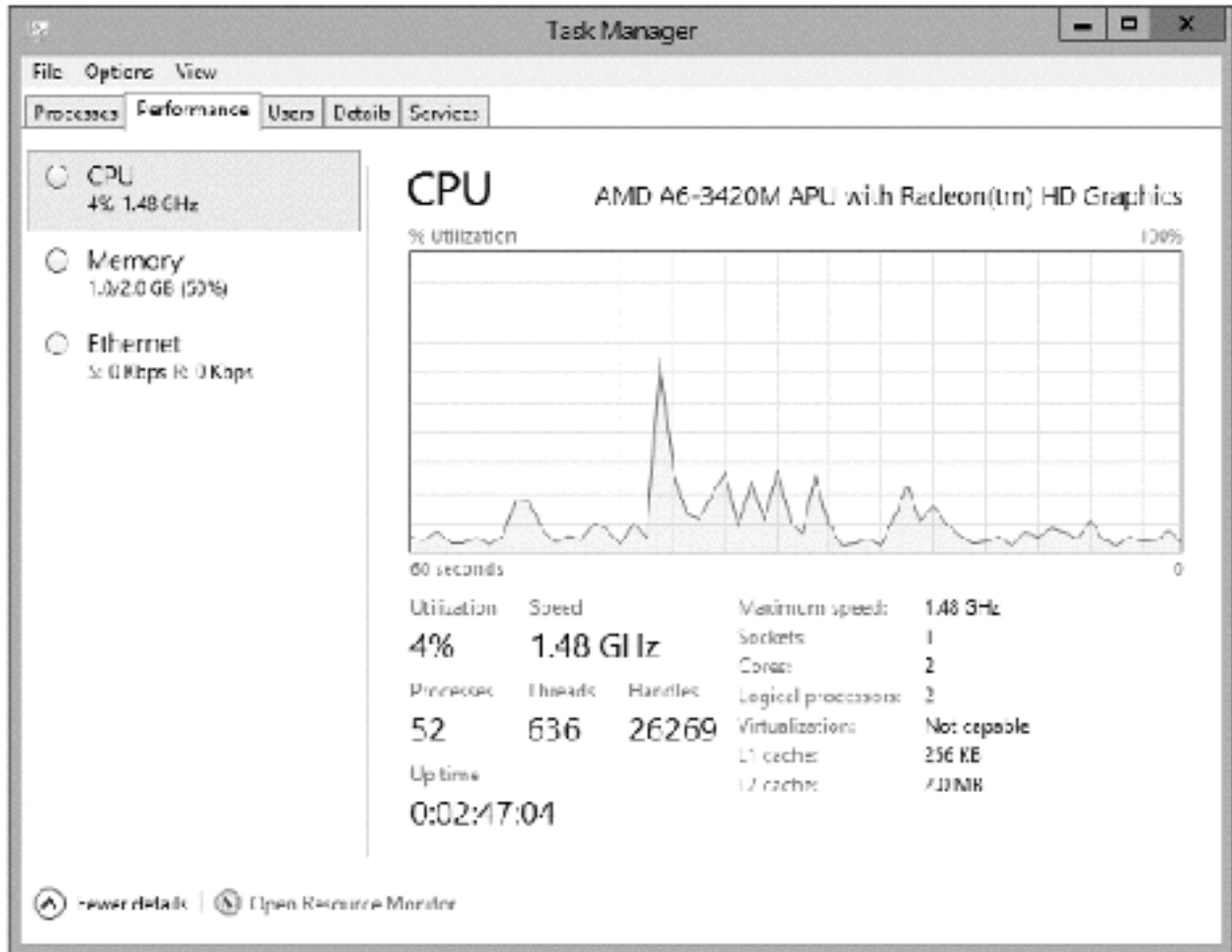
Figure 132: Task Manager Performance tab

More detailed information can be obtained by clicking the **Open Resource Monitor** button in the bottom left-hand corner of the Performance tab screen. This displays the following screen, which can be thought of as the 'Task Manager on steroids'. Resource Monitor can be invoked from Administrative Tools or directly from the Start Screen (when expanded to display all icons):
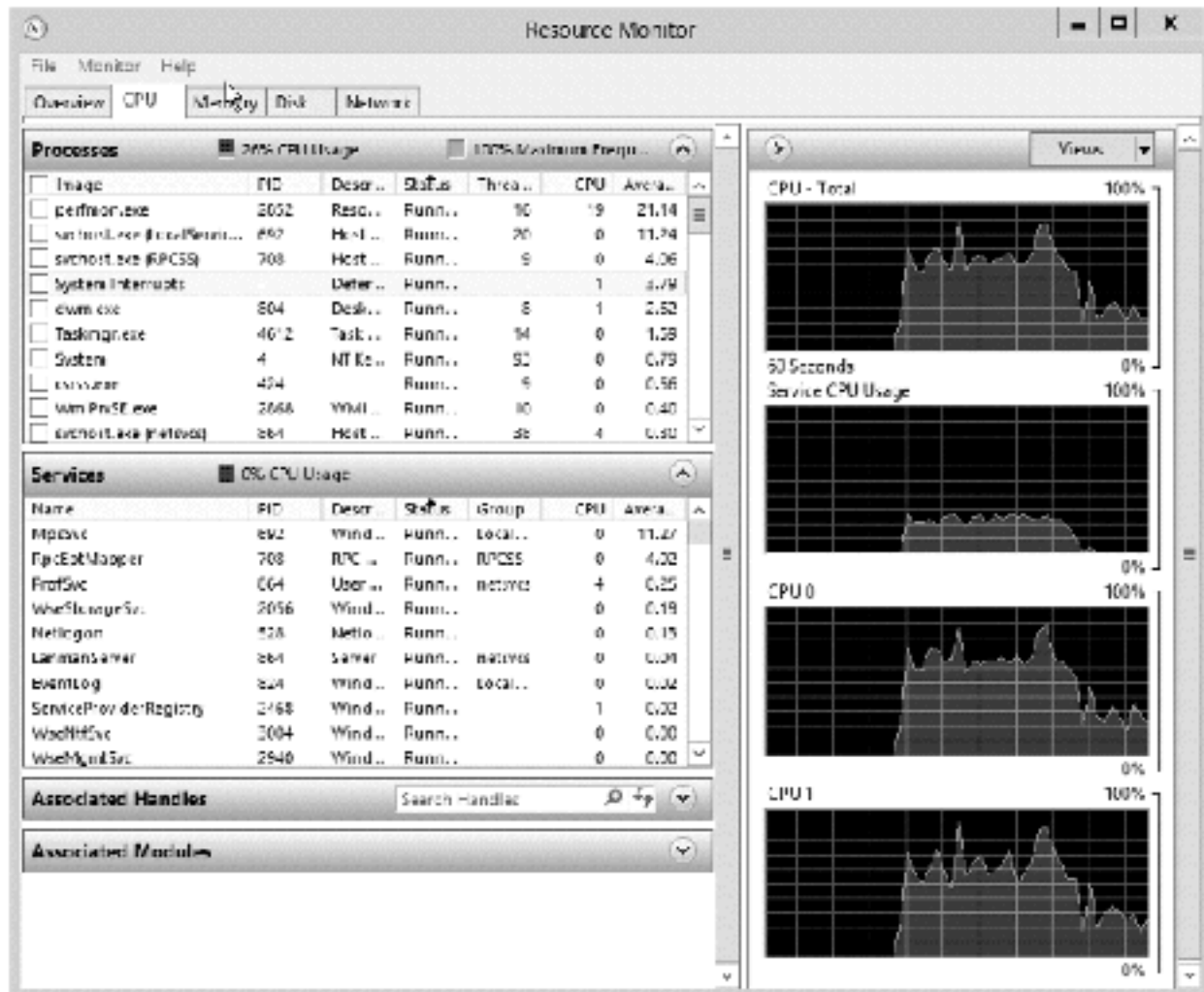
Figure 133: Resource Monitor screen

10. GROUP POLICY

10.1 Overview

This chapter is concerned with making the network more capable, easier to use and more manageable using Group Policy. Earlier on, Group Policy was switched on in order to enable Folder Redirection (see 3.5 Folder Redirection). However, this act of simply 'flicking a switch' hides the powerful, underlying tool. Computers and user accounts have many hundreds of settings that control their behaviour, such as how often passwords need to be changed, what items appear on the Desktop, the default home page within Internet Explorer and much more. Building upon Active Directory, Group Policy enables such things to be defined and then enforced across groups of computers and users, thereby creating a more consistent and controlled environment. To do this it is necessary to go underneath the hood and work directly with more advanced tools, outside of the Essentials Dashboard. This chapter is not intended as an in-depth tutorial about Group Policy, rather it is concerned with simple practical examples of using it.

10.2 Group Policy Management Console

Group policies are created and controlled using the *Group Policy Management* console. It is one of the Administrative Tools and can be accessed in several ways:

- Click the **Administrative Tools** icon on the Start Screen. Double-click the **Group Policy Management** icon

- Right-click the **Start** button, choose **Control Panel** and from there double-click the **Administrative Tools** icon followed by **Group Policy Management**

- In the Server Manager Dashboard, click **Tools** followed by **Group Policy Management**

The console looks like this:
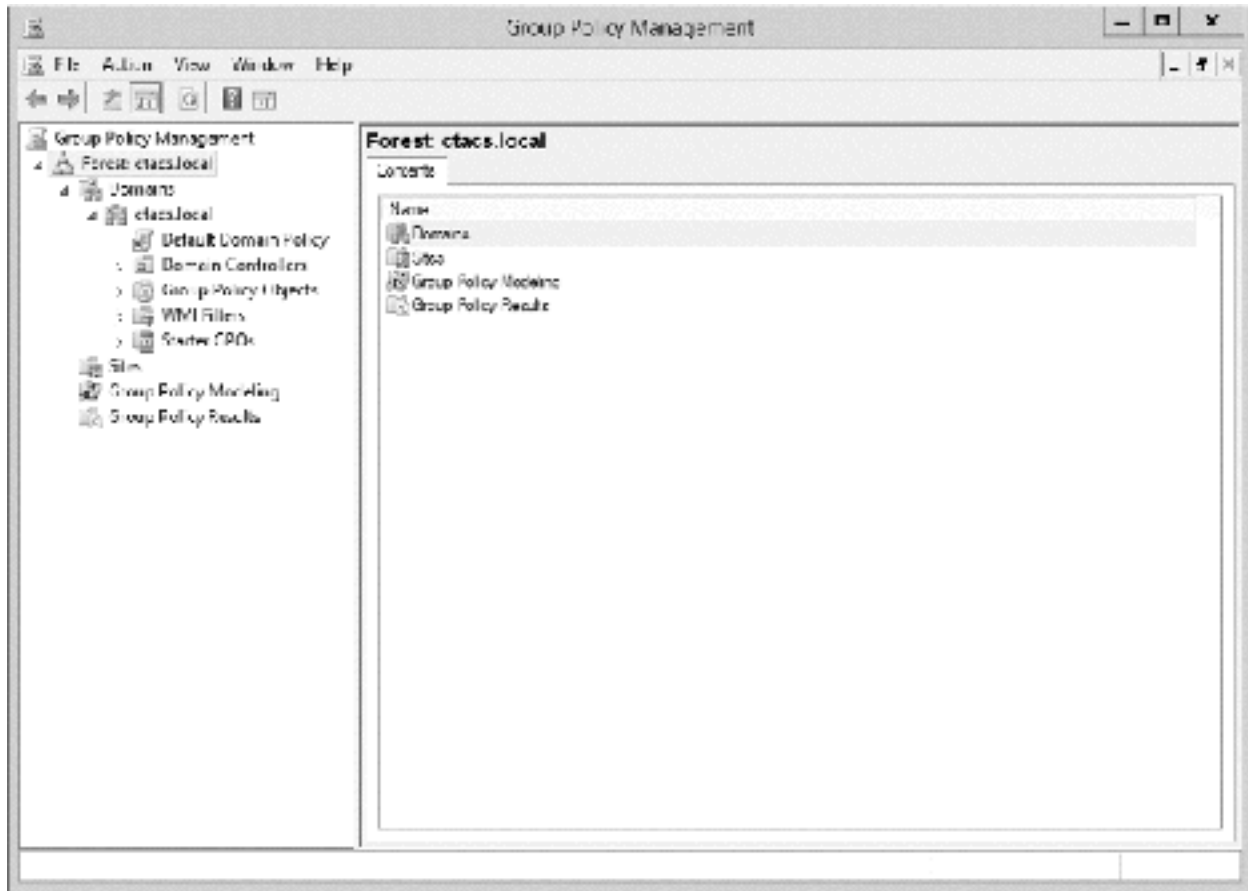
Figure 134: Group Policy Management console

Expand the tree in the left-hand panel to display the overall structure of the domain. The structure can be added to but to keep things simple we will leave things as they are. Notice an entry called *Default Domain Policy*; as the name implies, this covers default settings for the entire network. Any changes to this will therefore apply to all computers or users in the system and our examples will focus on this.

Making a change involves right-clicking an item – such as *Default Domain Policy* – and choosing **Edit**. Policies are created or modified for the *Computer Configuration* or *User Configuration*, the former affecting all computers and the latter affecting all users. There is no mechanism to explicitly save changes, as it is implicit when making modifications. The policies and preferences do not immediately propagate, rather they are applied the next time a client logs in to the network or when a computer starts up. However, it is sometimes possible to expedite matters by bringing up a command prompt ("DOS prompt") on a workstation and typing the command *gpupdate /force*.

One thing to note is that some Group Policy settings are operating system dependent. For instance, some may only be applicable to (say) Windows 8 and 8.1 and not work on (say) Windows 7. However, the majority are applicable to all versions of Windows.

10.3 Defining the Internet Home Page for All Users

Some organizations require that all users have a standard home page within Internet Explorer, such as the company's website or an email system such as Google Mail or Office 365. Group Policy can be used to achieve this.

Launch the **Group Policy Management Console**, which can be done by going to the **Start Screen** and clicking **Administrative Tools** followed by **Group Policy Management**. Expand the tree in the left-hand panel, right-click the entry for *Default Domain Policy* and choose **Edit**. In the new window, expand the tree and drill down to **User Configuration** > **Preferences** > **Control Panel Settings**. Right-click the entry for **Internet Settings** and choose **New**. A pop-up listing the various versions of Internet Explorer is shown; note that most of these are now obsolete and should no longer be in use, also that the current version, Internet Explorer 11 (nor the Edge browser for that matter) is not listed at the time of writing, although it will in fact use the Internet Explorer 10 settings:
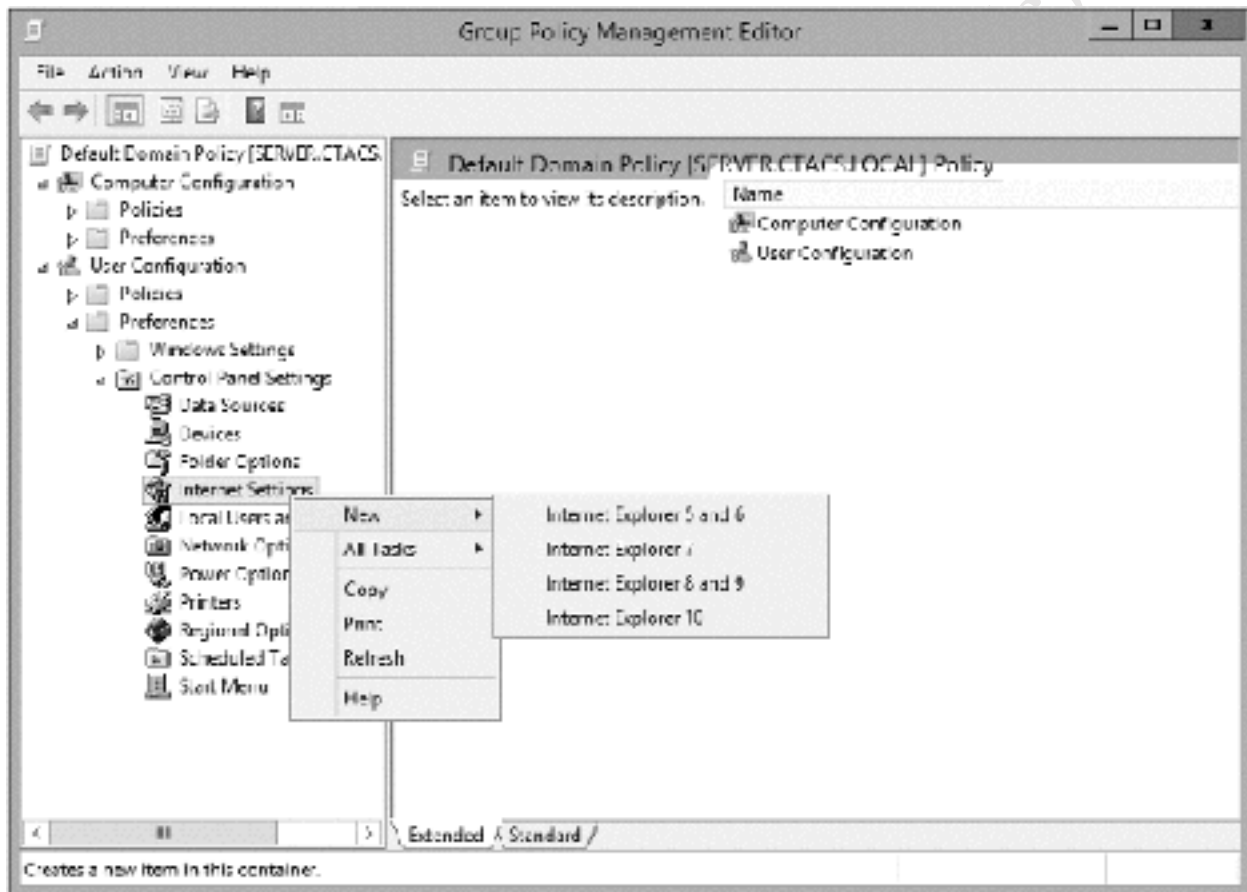
Figure 135: Choose the version of Internet Explorer

On the assumption that the organization is indeed using IE10 or IE11, click **Internet Explorer 10** and the properties box is displayed. Enter the details for the desired standard home page:
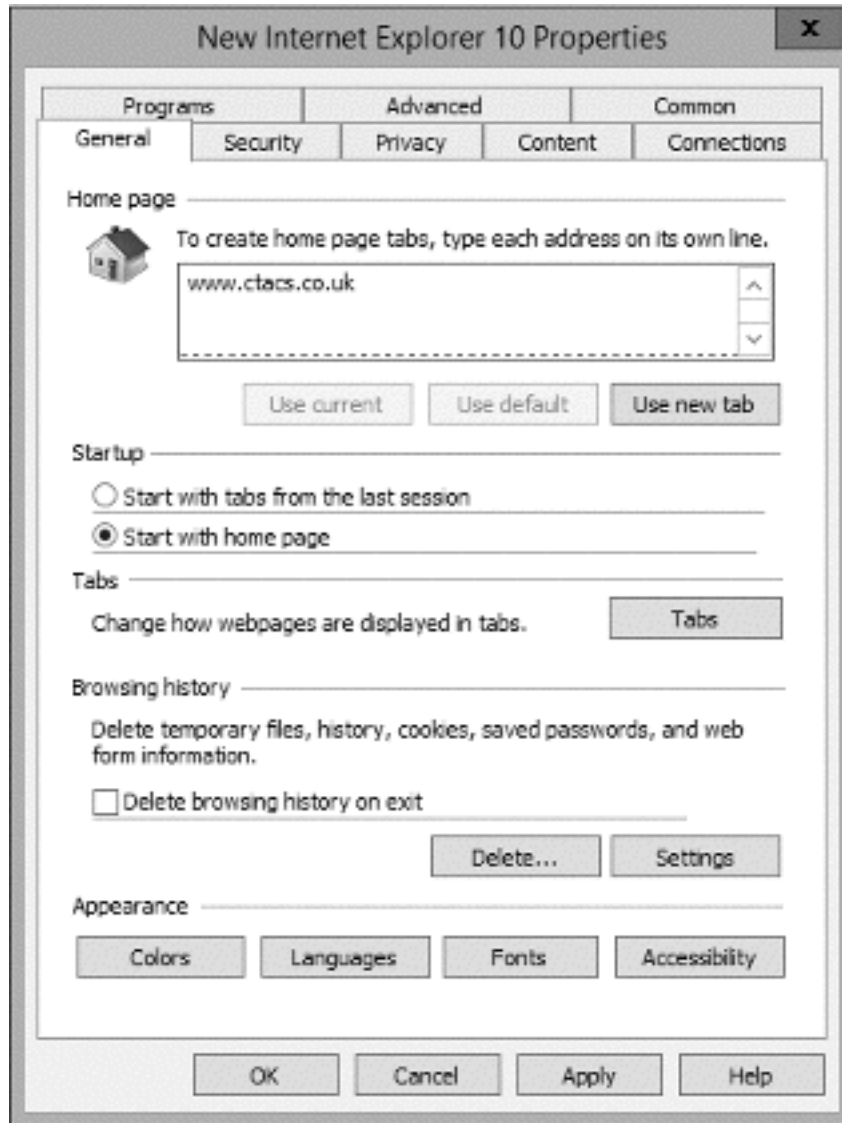
Figure 136: Specify the home page settings

In the 'Home page' section there is a red dotted line – press the **F6** key and it will change to a solid green line. NOTE: This is very important – unless this is done the setting will not apply. Click **OK**.

The effect of this is that all users will now have the specified page as their home page within Internet Explorer.

Other browsers, such as Microsoft Edge, Mozilla Firefox and Google Chrome, are not supported out of the box. They can be managed using *ADMX* files, which are extension files that are imported into Active Directory; for example, Google provide their own ADMX files that allow over 200 settings in Chrome to be managed. As this is a more advanced and specialized use of Group Policy it is not appropriate to cover it in this guide.

10.4 Windows Logon Behaviour

By default, Windows 7 clients and upwards display the name of the last person to use the computer. This can be confusing in an environment in which people share computers, as it necessary for the next person using it to explicitly specify "Logon as other user", which is inconvenient for some people. However, this behaviour can be changed, such that a blank user name and password are always presented to users and this is done through Group Policy.

Launch the **Group Policy Management Console**. Expand the tree in the left-hand panel, right-click the entry for *Default Domain Policy* and choose **Edit**. In the new window, expand the tree and drill down to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**. Go to **Interactive login** and Enable **Do not display last user name**.

10.5 Logon Warning/Security Message

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

On the server, open the Group Policy Management Console. Right-click the *Default Domain Policy* and choose **Edit**. Drill down to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**. Find *Interactive login: Message title for users attempting to logon*. Tick the *Define this policy setting* box, enter the name of the organization and click OK. Then repeat for *Interactive login: Message text for users attempting to log on* and specify the detailed warning or greeting message. Click **OK**.

11. OFFICE 365

11.1 Overview

The predecessor to Essentials – Small Business Server – included Microsoft Exchange and SharePoint to provide email and collaborative website (intranet) facilities respectively. However, running an email system in-house is quite an ambitious task and most small businesses prefer to outsource it these days. There are several ways of going about this but a popular choice is Microsoft's own *Office 365*. Office 365 is a cloud-based subscription service which, depending on the package taken, provides email, the SharePoint collaborative system, online conferencing, a public-facing website and the full Office suite of Word, Excel, PowerPoint and other products. Office 365 is a great choice for Essentials users because it fully integrates with it, allowing easy management of both local and online accounts from the Dashboard. Because Office 365 is a comprehensive product in its own right and has several variants, it is not possible to cover it in detail in a guide of this nature. However, the key aspects of integrating and managing it with Essentials are explored.

It is suggested that the organization has an Office 365 subscription in place **before** trying to integrate it with Essentials and that the organization's email and domain have been transferred across. In one sense, the two are totally separate products, as in many organizations have Office 365 but do not use Essentials and many organizations use the latter but not the former. However, there are a couple of considerations when planning to use both.

Firstly, additional thought needs to be given to user names. It is suggested that the local user name, the Microsoft online services name (the 'Office 365 name') and the email address should all be the same. For instance:

Local user name – louiseb

Microsoft online services name – louiseb@bloggscompany.com

Email address – louiseb@bloggscompany.com

Secondly, when creating local users it is a pre-requisite that strong passwords are used, as Office 365 insists on them (see 3.3 Creating User Accounts for a discussion about password policy).

11.2 Installation

Launch the Dashboard. On the **HOME** page under **Get Started**, go to **Services** and highlight 'Integrate with Microsoft Office 365'. On the right-hand side of the screen, click **Integrate with Microsoft Office 365** to launch the wizard. Assuming that the Office 365 subscription has already been setup as suggested, tick the **I already have a subscription** box and click **Next**:
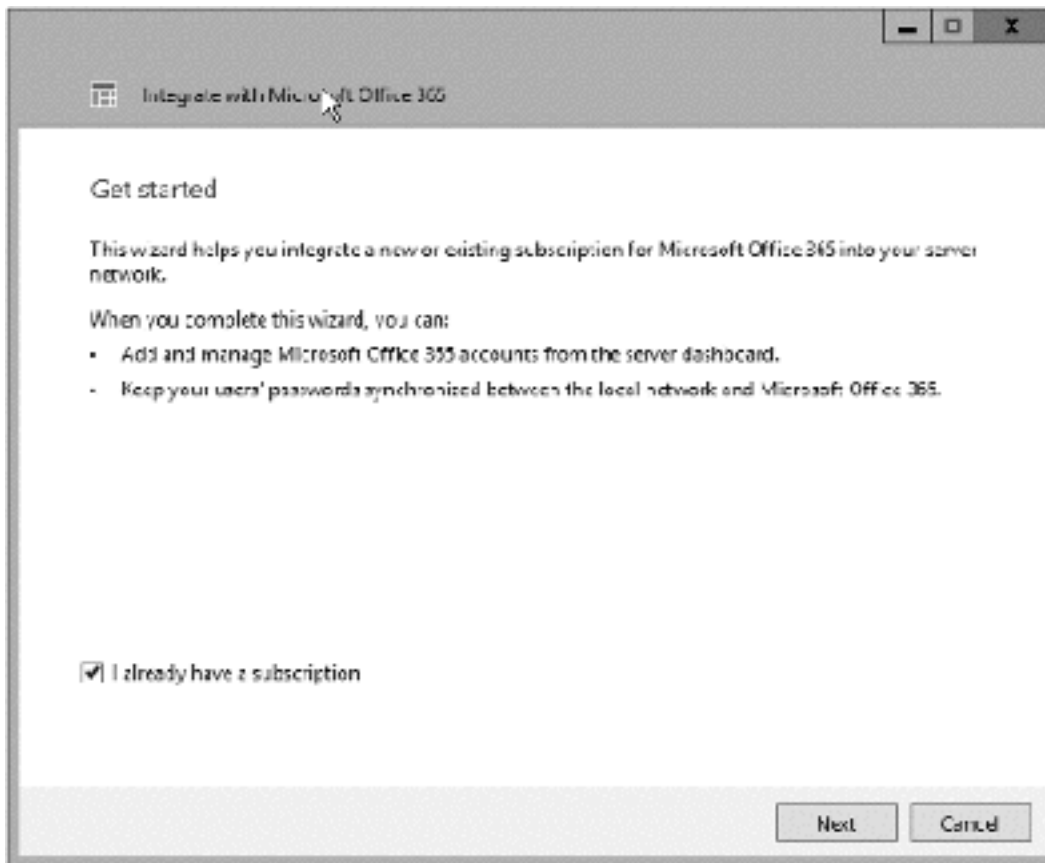
Figure 137: Office 365 Getting Started

Enter the details of the Microsoft account used to manage the Office 365 subscription i.e. the credentials used when signing up for Office 365:
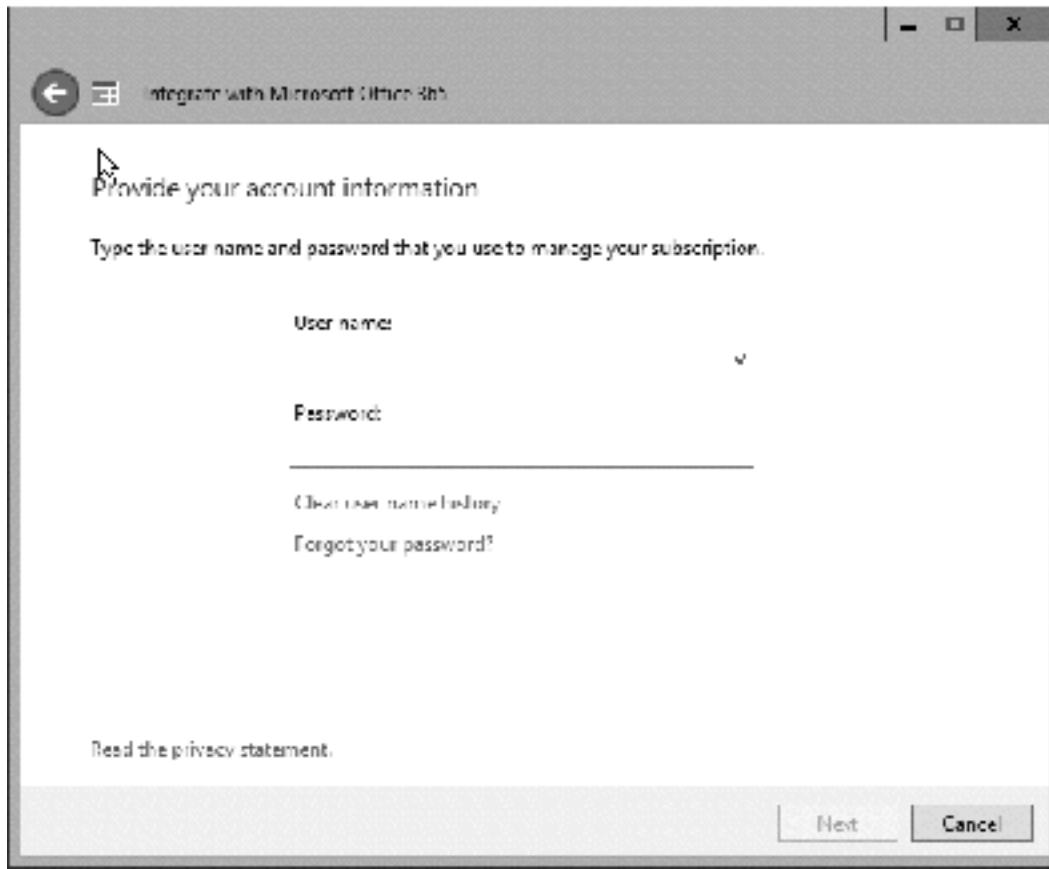
Figure 138: Office 365 account information

A message is displayed advising that the server's password policy will be changed to *Strong*, regardless of the current setting, as this is a pre-requisite for using Microsoft Online Services. Acknowledge the message and click **Next**:
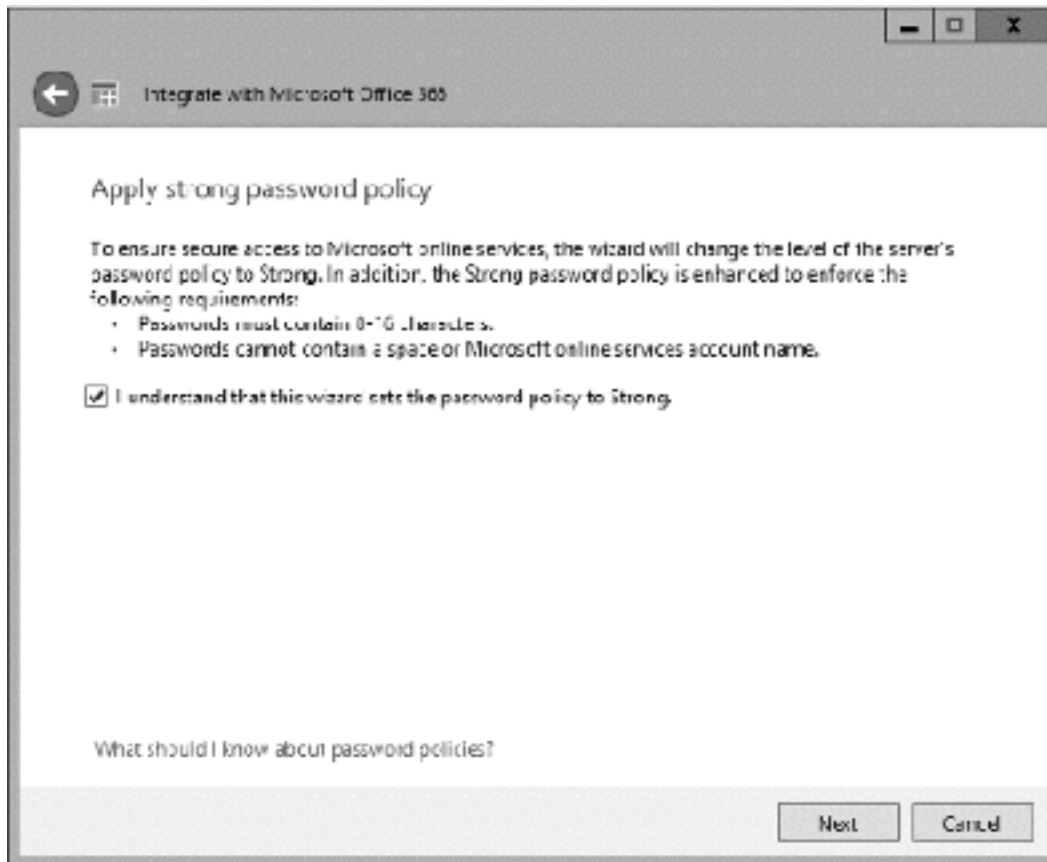
Figure 139: Office 365 – Apply strong password policy

After a short delay a confirmation screen is displayed:

Figure 140: Confirmation screen

The Dashboard has to be restarted to reflect the changes. Click **Restart Dashboard**. After it restarts there will be a new tab for Office 365. Clicking it gives the following display (note that some information has been intentionally obscured for privacy reasons):
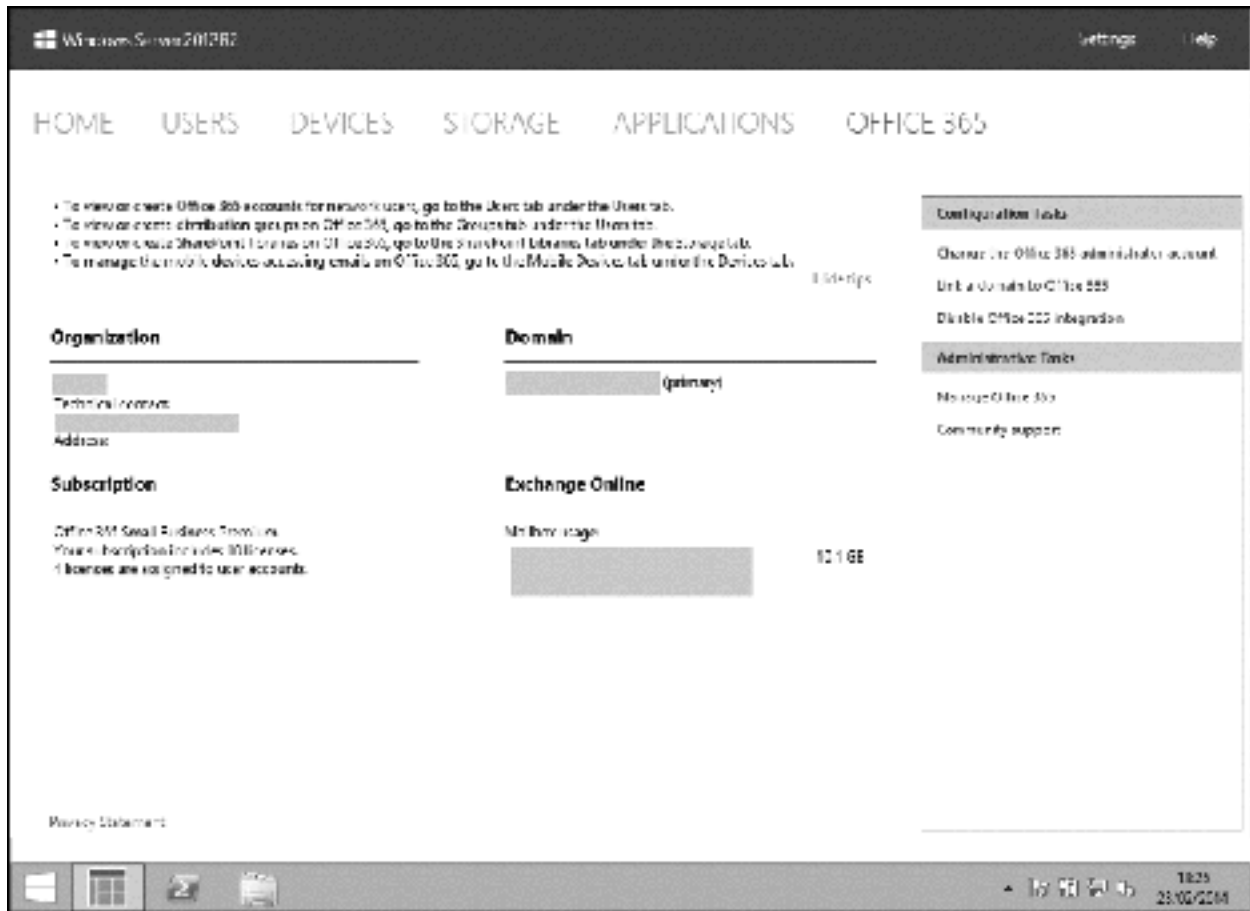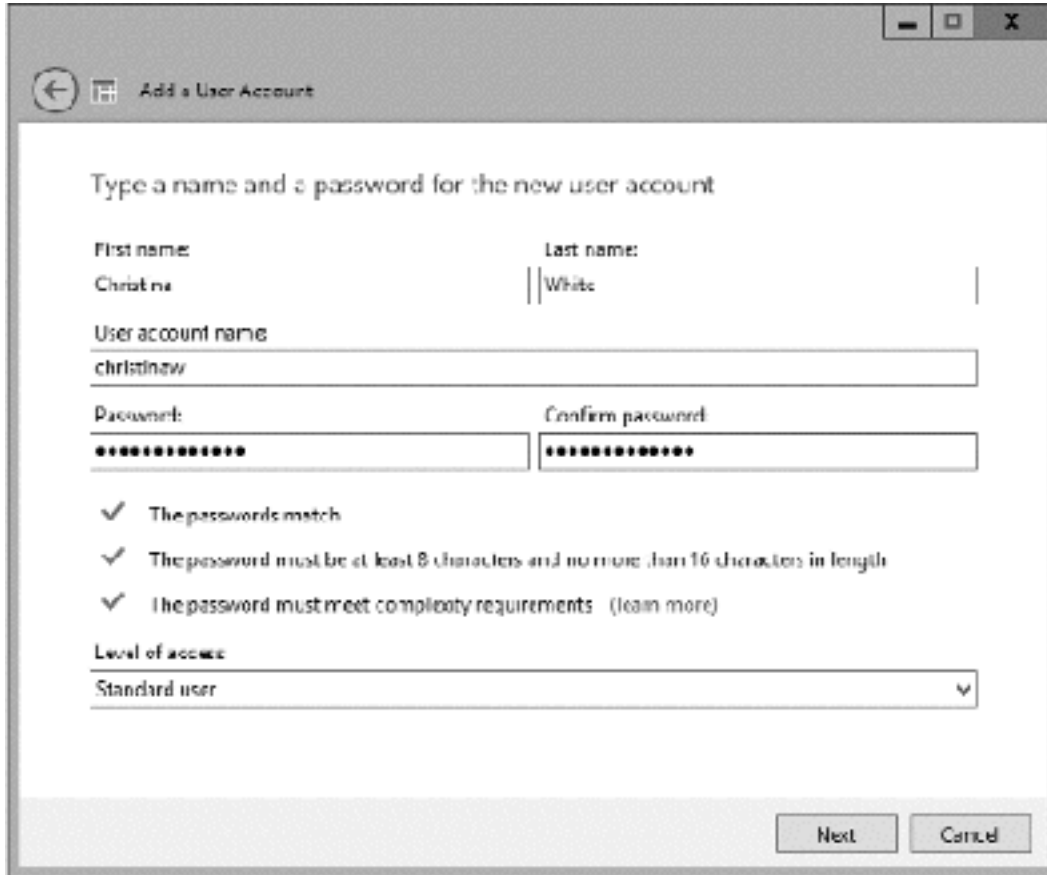
Figure 141: Updated Dashboard incorporating Office 365

This screen is largely a status screen and in itself does not actually do much. For instance, clicking **Manage Office 365** under Administrative Tasks will simply take you to the regular website used for managing Office 365. Instead, the real action is to be found elsewhere, particularly in changes to managing users from the **USERS** tab.

11.3 Creating a New User

The process for creating a new user in Essentials starts off the same as before (see 3.3 Creating User Accounts) although there is now a reminder that the password needs to be strong. Enter the details for the user and click **Next**.

Figure 142: Creating a new user account

However, the next step is different as it relates to the Microsoft Online Services account. The options are: Create a new account; Assign an existing account; Continue without an account. In all likelihood you want to create a new account. Under what conditions would you assign an existing account? An example might be where the organization is based around particular roles such as accounts, sales, enquiries and such. You might choose to assign a particular named individual to a role; in the event that the individual leaves or is replaced then you can assign somebody else without affecting the online account itself.
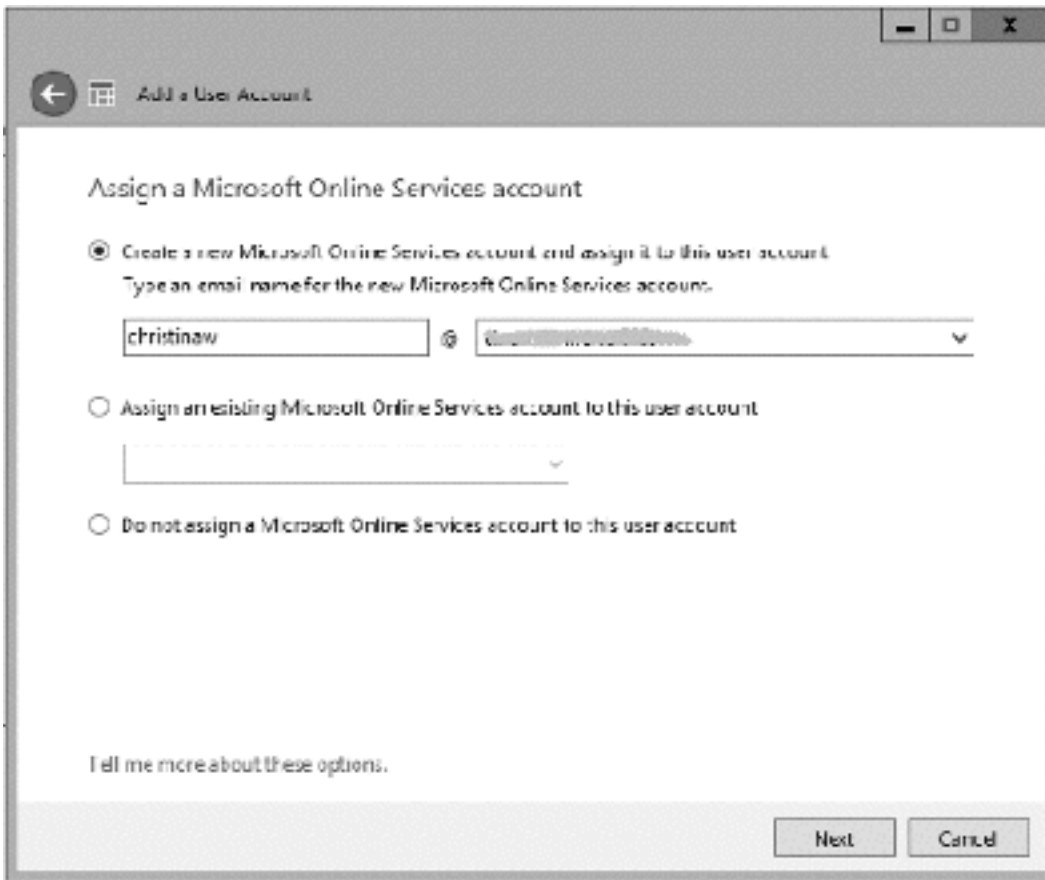
Figure 143: Assign an online account

The next panel is for specifying what online services the user is to have. The answer to this depends upon what level of Office 365 subscription the organization has and what features you wish the individual to have. Choose the appropriate option(s) and click **Next**.
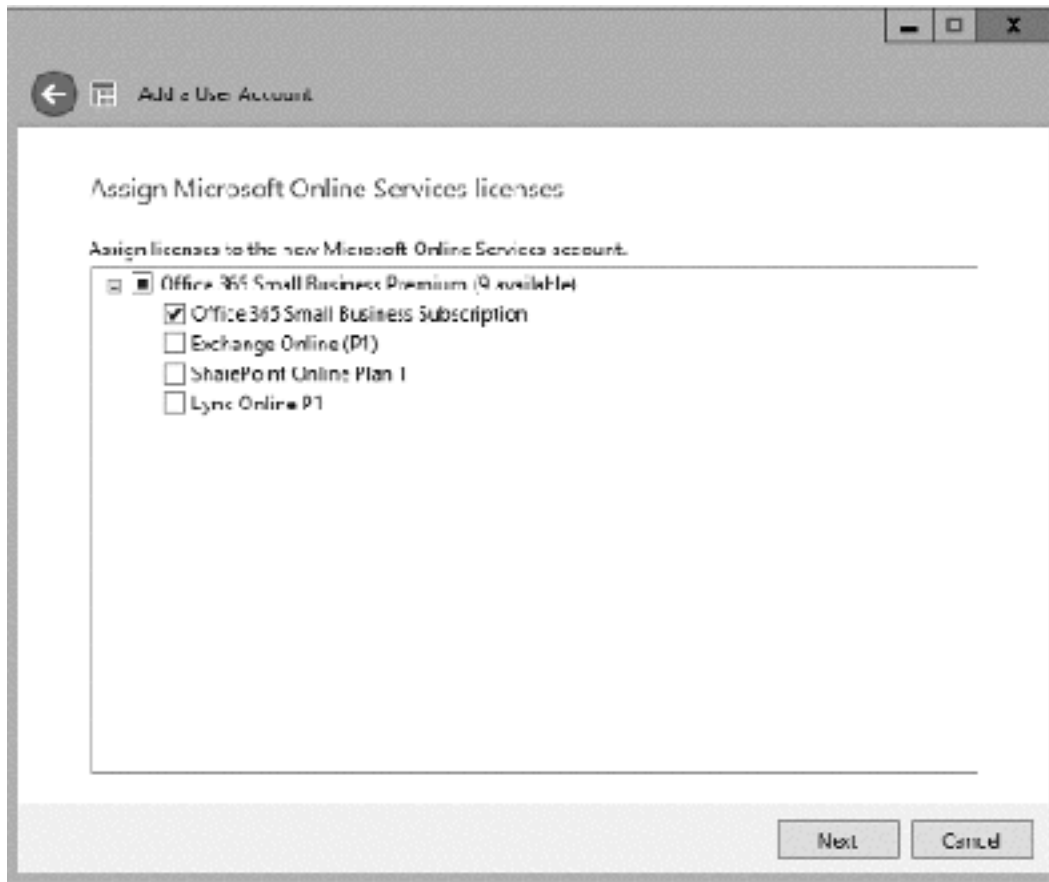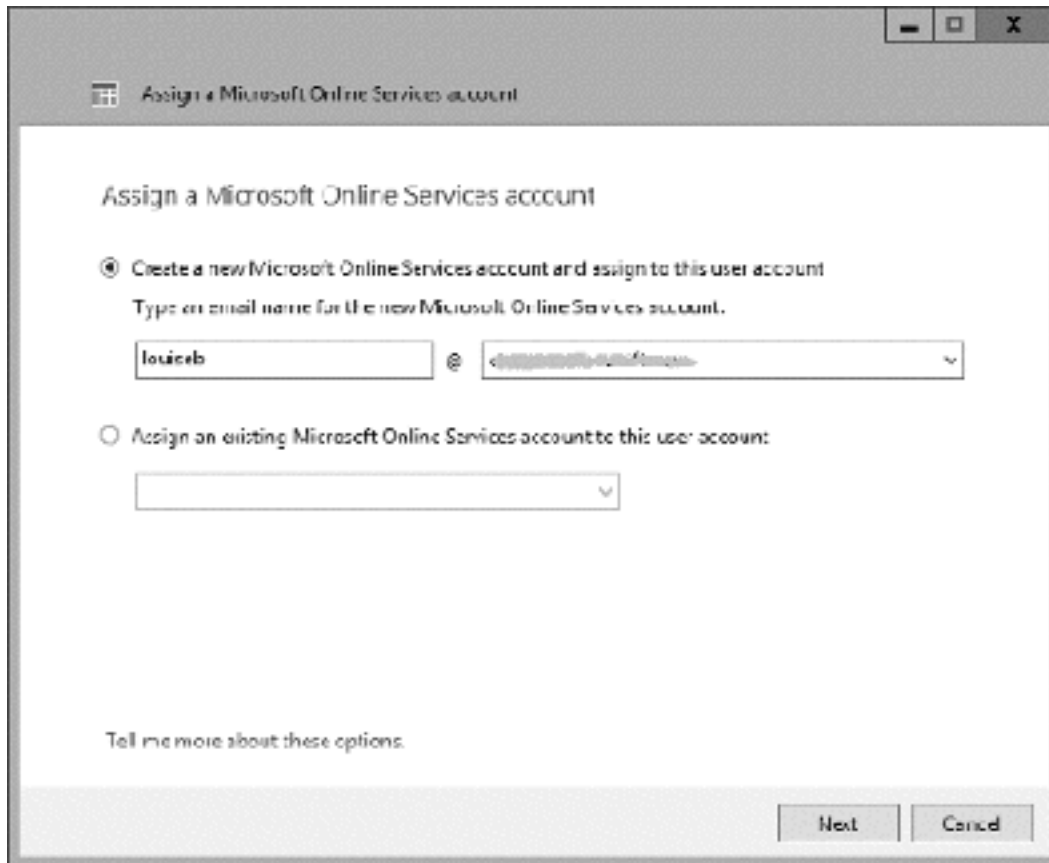
Figure 144: Assign licenses

Thereafter, creation of the user continues in the normal manner, but when complete they will have both a local account and a corresponding online account with Microsoft. Note that the user may be prompted to change their password the first time that they login.

11.4 Assigning an Existing Local Account

There may be a requirement to assign an existing local account to Office 365. For instance, this would need to be done if the organization already had Essentials and subsequently subscribed to Office 365. To do this, launch the Dashboard and click the **USERS** tab. Highlight the user and on the right-hand side of the screen click **Assign a Microsoft online account**. On the resultant panel there is a choice to Create a new Microsoft Online Services account or Assign an existing Microsoft Online Services account:

Figure 145: Assign an existing local user account

On the subsequent screen choose the options that the user will have, which depends upon the organization's subscription package and requirements:
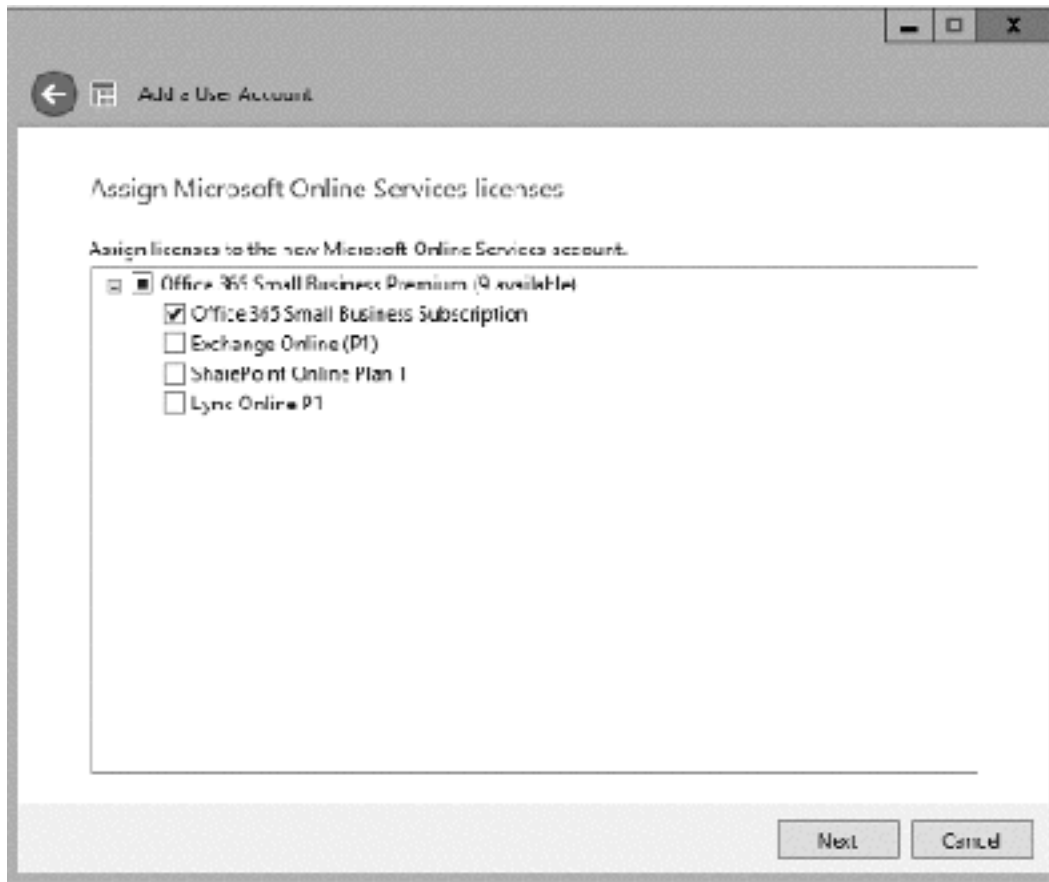
Figure 146: Assign licenses

After a short while a confirmation screen will be displayed. Note that the user may be prompted to change their password the next time they login.
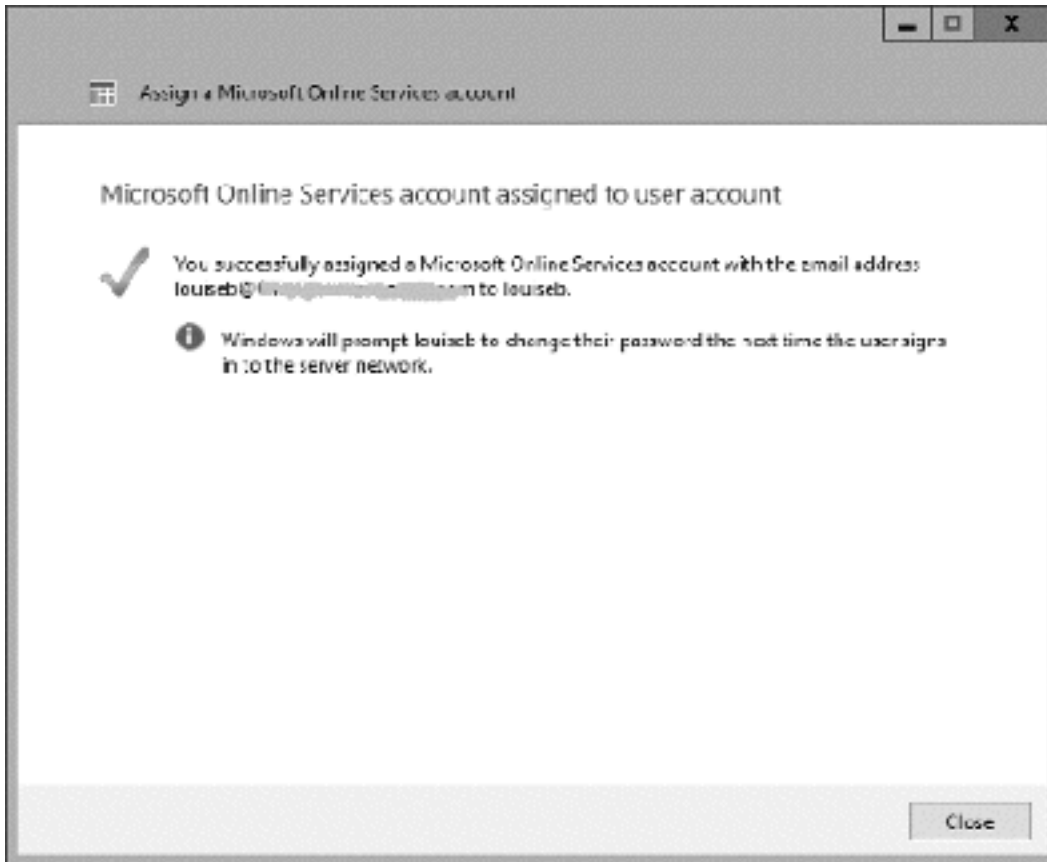
Figure 147: Confirmation panel

11.5 Removing and Blocking an Online Account

To remove a user from online services, highlight the user on the Dashboard. On the right-hand side of the screen click **Unassign a Microsoft Online Account**.

To block a user from online services – which really means to temporarily disable them – double-click on the user's name. Click the **Microsoft online** tab. In the top right-hand corner is a drop-down that controls whether the user is allowed to or blocked from using online services. After making a change click **Apply**.
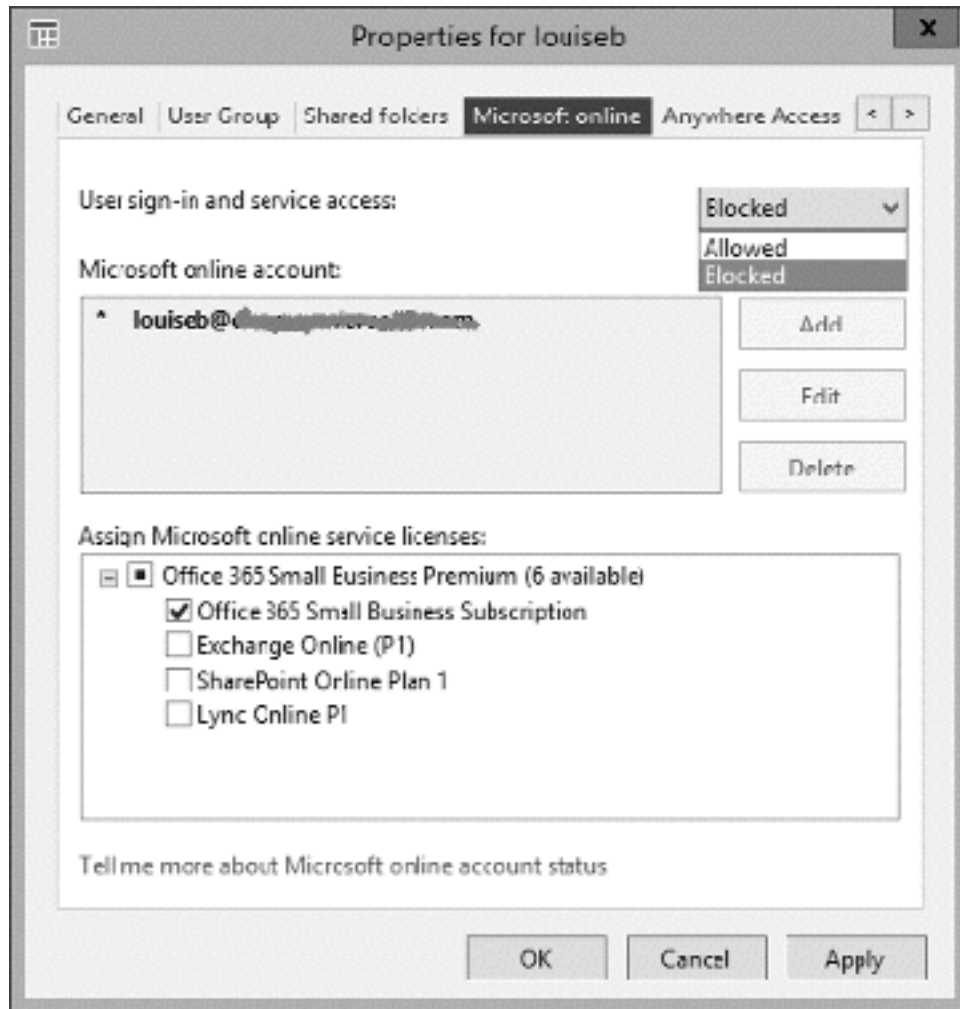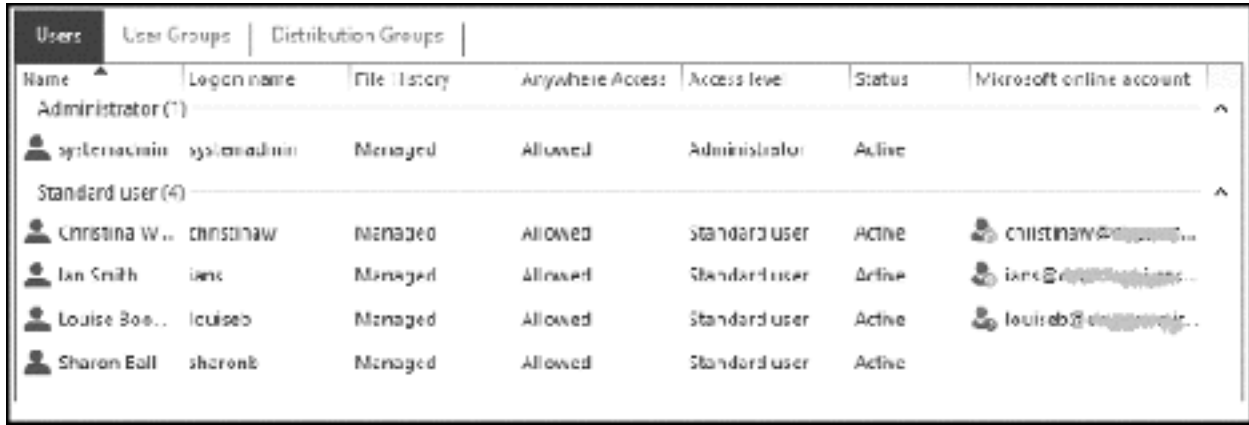
Figure 148: Blocking an account

11.6 Checking Who Has an Online Account

It is easy to see at a glance who has online accounts. In the Dashboard click on the **USERS** page, then click on the Users tab. A new column has been added on the right-hand side, listing details of the corresponding online accounts for the local users:

Name	Logon name	File History	Anywhere Access	Access level	Status	Microsoft online account
Administrator (1)						
systemadmin	systemadmin	Managed	Allowed	Administrator	Active	
Standard user (4)						
Christina W...	christinaw	Managed	Allowed	Standard user	Active	christinaw@...
Ian Smith	ians	Managed	Allowed	Standard user	Active	ians@...
Louise Bos...	louiseb	Managed	Allowed	Standard user	Active	louiseb@...
Sharon Eall	sharonb	Managed	Allowed	Standard user	Active	

Figure 149: Check online account status

To the left of the online account name is a status indicator. If a user is allowed to use online services there is a small blue icon with a green arrow in a circle. If the user is blocked from using online services the icon is grey with a small red indicator.

11.7 Changes to Storage Page in Dashboard

If the subscription to Microsoft Online Services includes SharePoint then the STORAGE page in the Dashboard is also updated. An additional tab is added, called SharePoint Libraries. From here, libraries can be created and managed. Note that several of the options for managing the libraries are nothing more than links to the external website. For more information about what SharePoint is and does go to http://office.microsoft.com/en-us/sharepoint/

Figure 150: SharePoint tab in Dashboard

11.8 Changes to Devices Page in Dashboard

Office 365 subscriptions include support for mobile devices, including many popular tablets and smartphones. Depending on the type of subscription, the capabilities of the device and how it is configured, access to email, calendar, contacts and SharePoint may be available. The DEVICES page in the Dashboard is also updated. An additional tab is added, called (logically enough) Mobile Devices. From here, devices can be monitored and managed.

Figure 151: Devices tab in Dashboard

As mentioned at the beginning of this chapter, Office 365 is a weighty subject in its own right. The purpose here has been to review the integration aspects with Essentials, rather than delve into the rich functionality it offers for online users. Further information about Office 365 can be obtained from the Microsoft website.

12. MISCELLANEOUS TOPICS
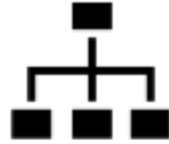
12.1 Overview

This chapter contains a selection of miscellaneous topics which do not fit elsewhere or of a more advanced or less frequently required nature.

12.2 Disabling Internet Explorer Enhanced Security

By default, Internet Explorer will not easily allow you to browse the internet due to a feature called *Internet Explorer Enhanced Security* being enabled. There are solid reasons why general Internet browsing is not a good idea on a server, but not being able to access the Internet from the server makes things difficult in a small network. It is therefore necessary to disable the Enhanced Security feature.

To do so start Server Manager. There are 3 methods for doing so: click on Administrative Tools from the Start Screen or Taskbar (if you have added it to the Taskbar) and select Server Manager; else start PowerShell from the Taskbar, type **servermanager** and press Enter; else press the **Windows key** and **R key** simultaneously, type **servermanager** and press **Enter**.

Server Manager can be thought of as a more capable variant of Dashboard and is used for managing the regular versions of Windows Server 2012 R2. Click **Configure this local server**. A panel displaying the Properties of the server is displayed; approximately half-way down the right-hand side it reads 'IE Enhanced Security Configuration':

Figure 152: Server Manager

Click where it reads **On** and in the window that pops up select **Off** for both **Administrators** and **Users**. Save the changes by clicking **OK**.
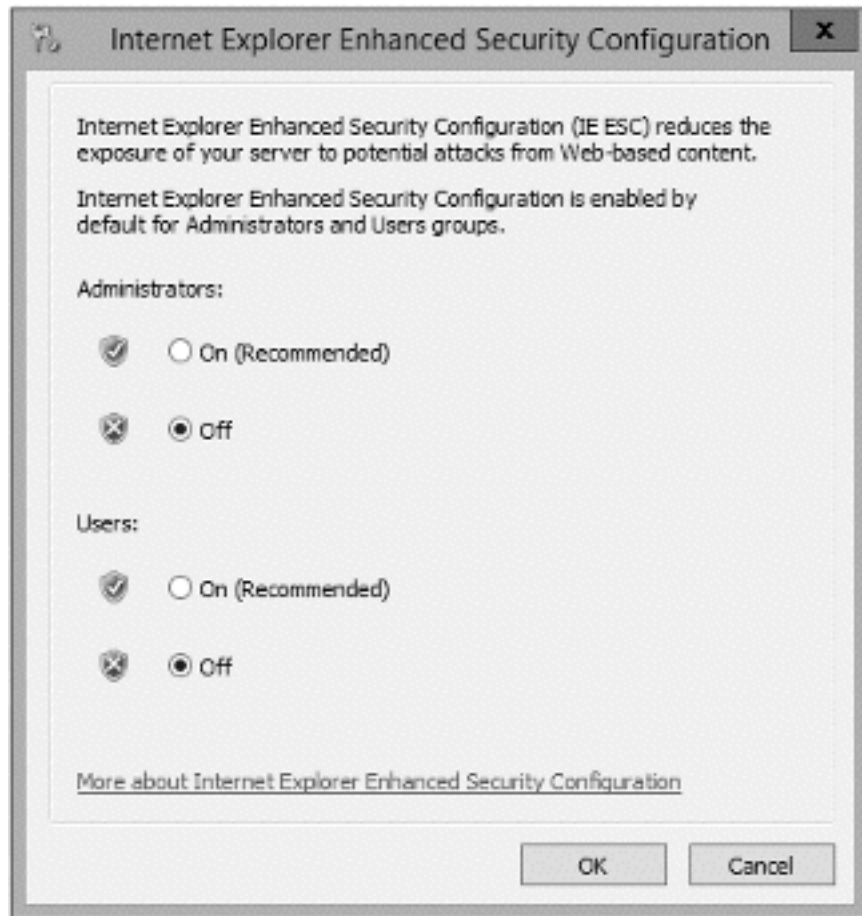
Figure 153: Internet Explorer Enhanced Security Configuration

12.3 Security Software for the Server

Windows computers, including Windows-based servers, require an anti-virus program to help protect them. A variety of free and commercial ones are available; unfortunately, most of the free ones are not compatible with Essentials or are not licensed to run on server systems. Examples of relatively low-cost anti-virus packages that may be suitable include Avira Server Security and AVG File Server Edition.

As there is a choice of third packages available, it is not appropriate to discuss the installation details of a specific one here. However, regardless of whatever else is or is not installed, to provide additional protection a program called *Malwarebytes* can usefully be installed on the server. Malwarebytes is often more effective at identifying and removing malware that may be missed by the regular anti-virus programs. A free version can be downloaded via the www.malwarebytes.org website (be careful not to download the evaluation version or select it during installation).

Malwarebytes should be run on a regular basis. Unfortunately, it is not possible to schedule the free version to do this automatically. The paid version can be scheduled to scan and is well worth considering as it is an inexpensive purchase.
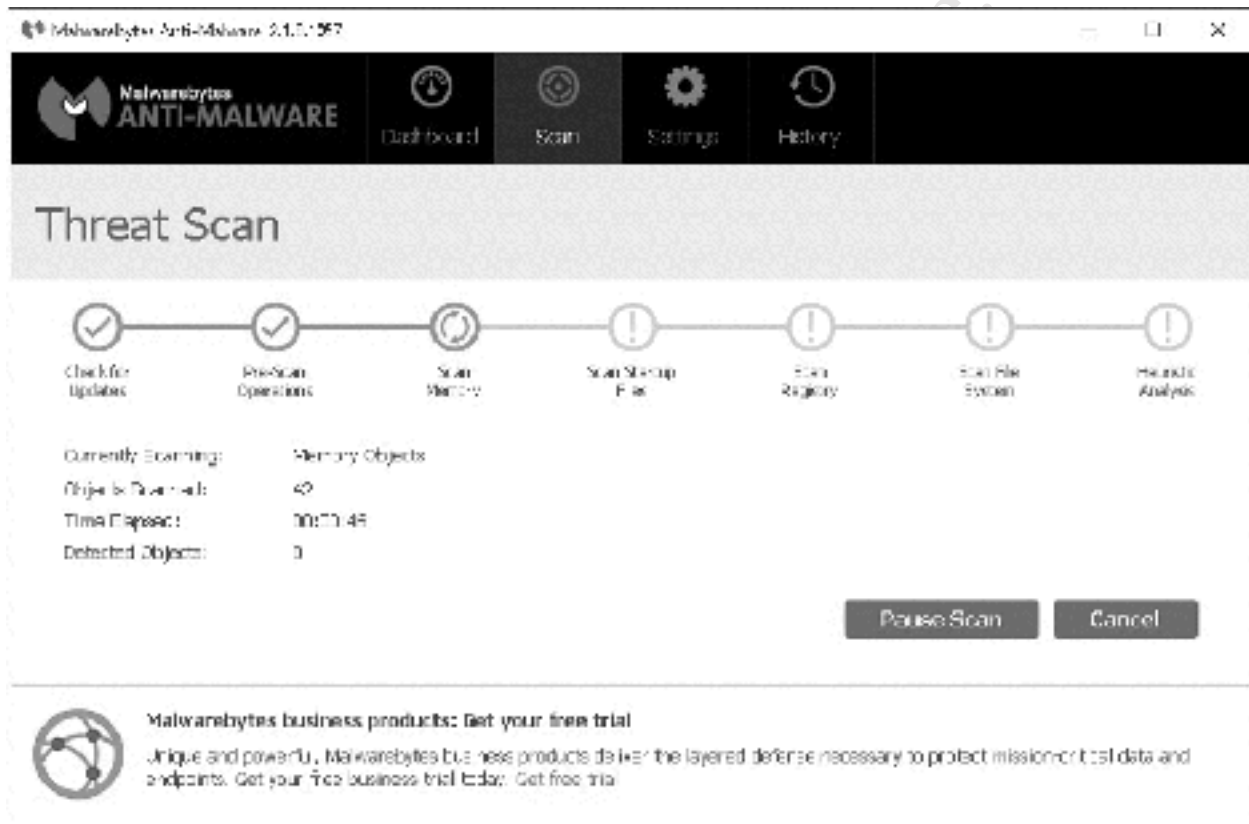

Figure 154: Malwarebytes running

12.4 Customizing the Server Desktop Screen

By default the Desktop screen on the server is relatively bland, showing just the icons for the Dashboard and the Recycle bin. However, it can be customized to make it more useful and informative.

If you don't like the colour of the Desktop, go into **Control Panel** > **Display** > **Change desktop background** and choose a different colour or picture.

Next, go to the Start Screen. Right-click **Administrative Tools** and choose **Pin to Taskbar**. Do the same for the **Control Panel**. This will make it easier to get to them from the Desktop.

Secondly, there is a free utility called *BGInfo* (Background Information) available from Microsoft. The purpose of *bginfo.exe* is to capture and display important system information from the server and display it on the Desktop, making it very useful for diagnostics and such. Examples of data captured include: current user name; computer name; IP address; operating system version. It can be downloaded from https://docs.microsoft.com/en-us/sysinternals/downloads/bginfo

Detailed information on usage can be obtained from the download site but the basic principles are:

- Extract the *bginfo.exe* file from the download. Place it in the Startup folder. This is located at *C:\PrograData\Microsoft\Windows\Start Menu\Programs\Startup*. Note that this is a hidden folder – to display it in File Explorer choose **View** > **Hidden items**.

- Run *bginfo.exe* and customize it to display the desired fields e.g. items such as IP address, amount of free space on the drives, user name and so on. When done click on **File** > **Apply** and **Exit.** Note that this software is not really supported and it can be a bit awkward to work with!

Thereafter, BGInfo will run automatically every time the server starts up. The screenshot below shows an example of a customized Desktop.
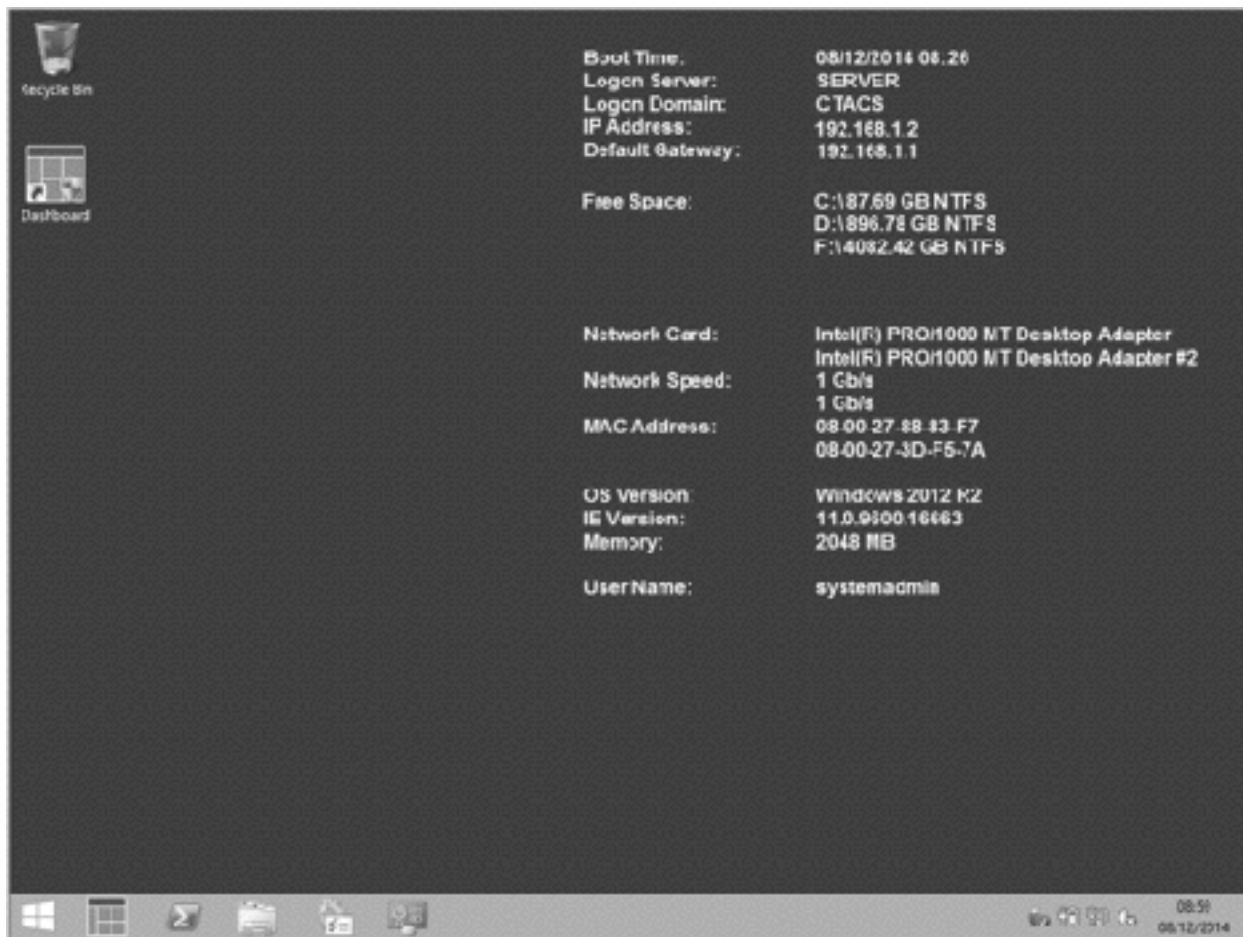
Figure 155: BGInfo

12.5 Headless Operation

When setting up the server a screen, keyboard and mouse are needed. But once the installation is complete, these can be dispensed with and the server operated *headless*. For this reason, it is not worth buying these items; instead, borrow them from another computer or make some other temporary arrangement.

The server can be managed from any other computer in the network using a program called *Remote Desktop Connection*. This program is a standard part of Windows and can be located at **Start** > **All Programs** > **Accessories** in Windows 7 or from the Start Screen in Windows 8 and 8.1.

Upon launching Remote Desktop Connection it will ask for the name of computer to connect to i.e. the server. Type in *server*; alternately, type in its IP address. You will then have to provide login details (*systemadmin* and password), at which point you will be connected to the Essentials server.

When launching Remote Desktop Connection, you may receive the following screen. If so, tick the **Don't ask me again for connections to this computer** box and click **Yes**. It will not be shown again from the computer you are currently using.
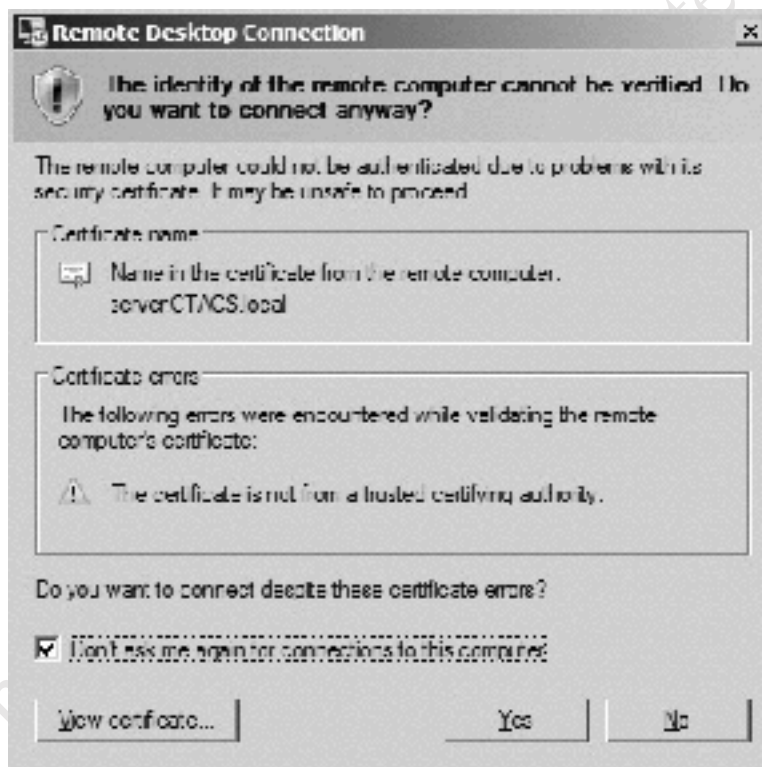

Figure 156: Certificate warning

When you have finished the remote session, be sure to logout and close down the Remote Desktop software.

12.6 Drive Mappings via Login Script

The process of connecting a computer to the network using the Windows Server Essential Connector places links to the server's shared folders on the Desktop. The folders can also be accessed by referring to them using what is referred to as their UNC name e.g. *\\server\company*. However, many users feel more comfortable with drive letters e.g. C:, D:, E: and so on. If this is the case then the shared folders can be mapped to drive letters; there are several ways of doing this but a simple method is via a script (batch) file.

Using Notepad or some other basic text editor, create a file called *logon.cmd* with the following contents:

```
@echo off
: Logon script:
: Map shared company folder and home drive
net use s: \\server\company /persistent:no
net use h: \\server\users\%username% /persistent:no
```

Make sure the file is saved as a plain text type. It should be placed in the following folder on the server…

C:\Windows\sysvol\sysvol\domainname.local\scripts

…where *domainname.local* is the name of the domain. This folder is automatically mapped by the server as a special share called *netlogon*.

Go to the **Control Panel** and choose **Administrative Tools** followed by **Active Directory Users and Computers**. Expand the tree on the left-hand side to display the Users. Tip: click the **Type** column to sort the list – it will make it easier to differentiate the user accounts that you have created from the numerous built-in ones:
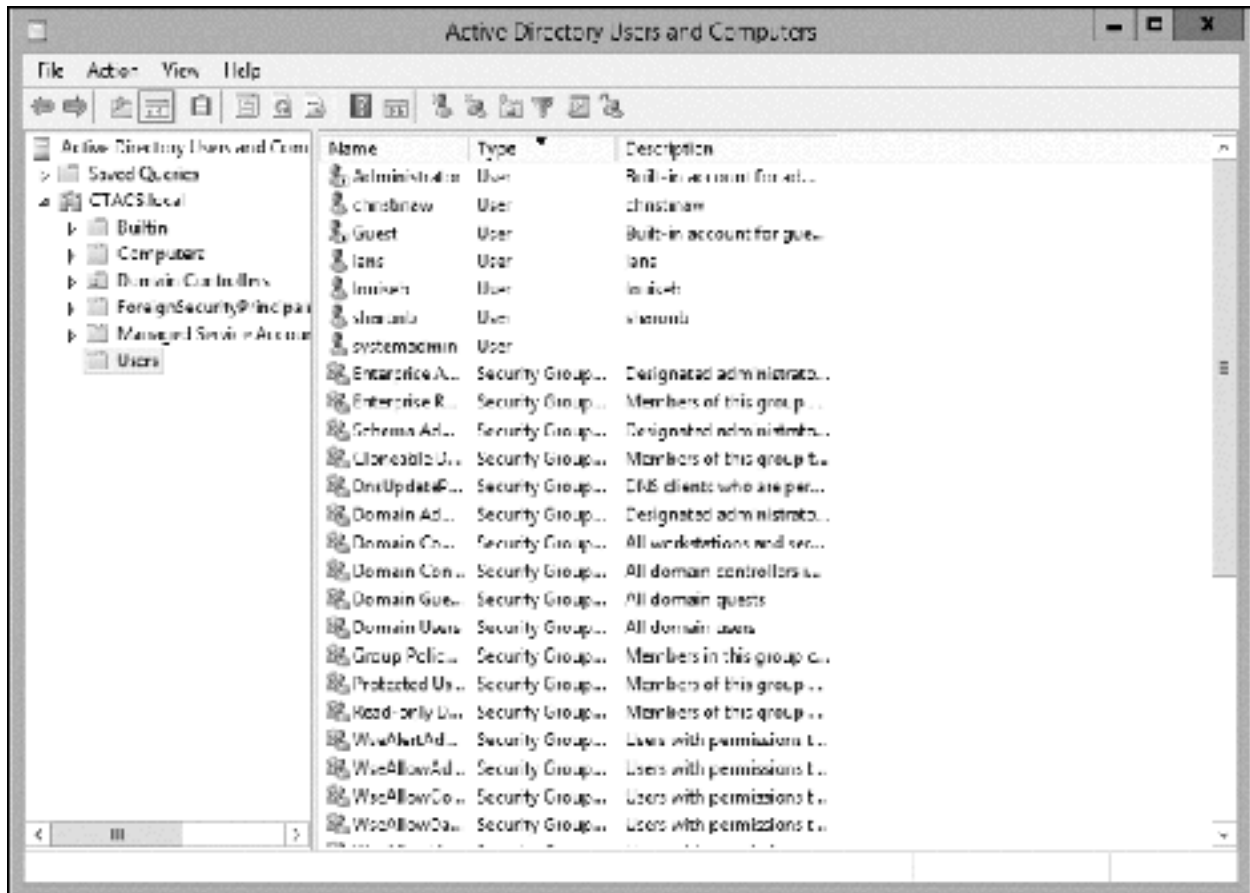
Figure 157: Active Directory & Computers

Double-click on a user name. Click on the **Profile** tab. In the **Logon script** box type *logon.cmd* then click **OK**:
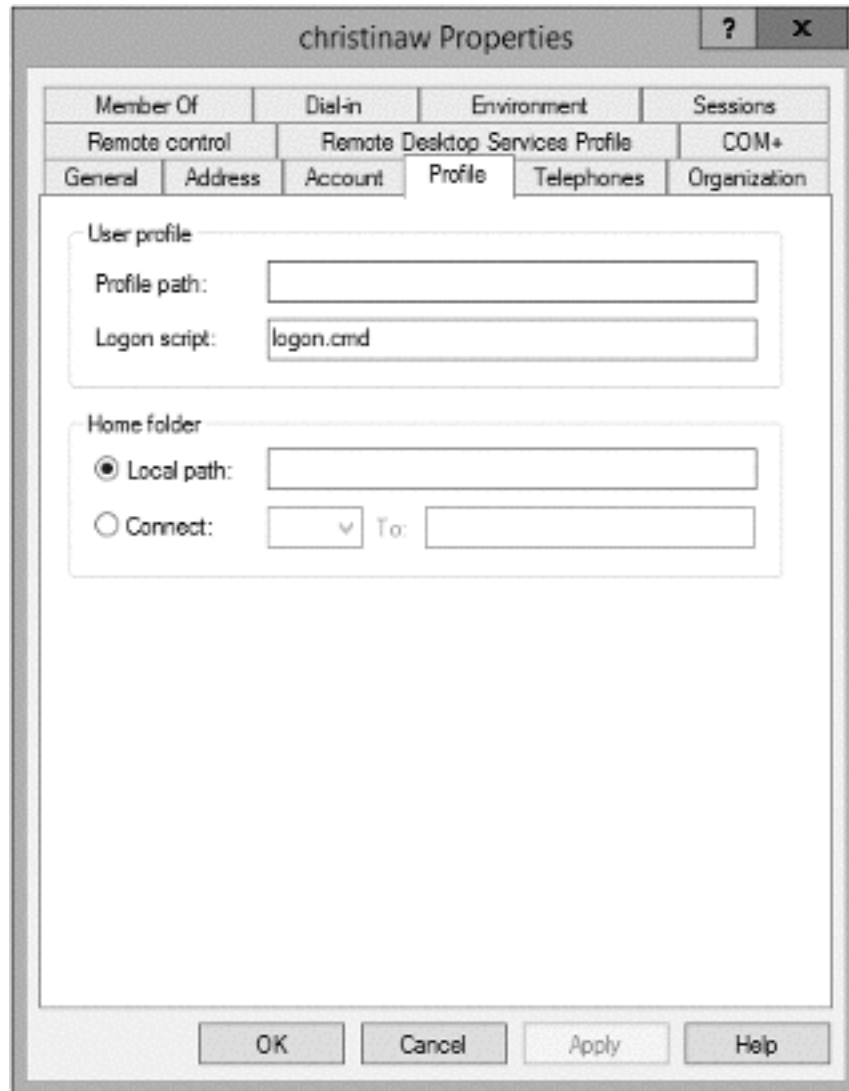
Figure 158: User Properties

Repeat this process for each user. Now, when a user logs on the script will be executed invisibly in the background. The *Company* share will appear as the S: drive and the user's home folder will appear as the H: drive.

12.7 Restore Missing Shortcut to Shared Folders

Each user should have an icon on their Desktop that provides a shortcut to the Shared Folders. If it is missing or accidentally deleted then it can easily be recreated as follows:

Right-click on the Desktop. Choose **New** > **Shortcut**. Where it reads 'Type the location of the item' enter *\\server\shared folders*. Note that there is a space between the words 'shared' and 'folders'. Click **Next**.
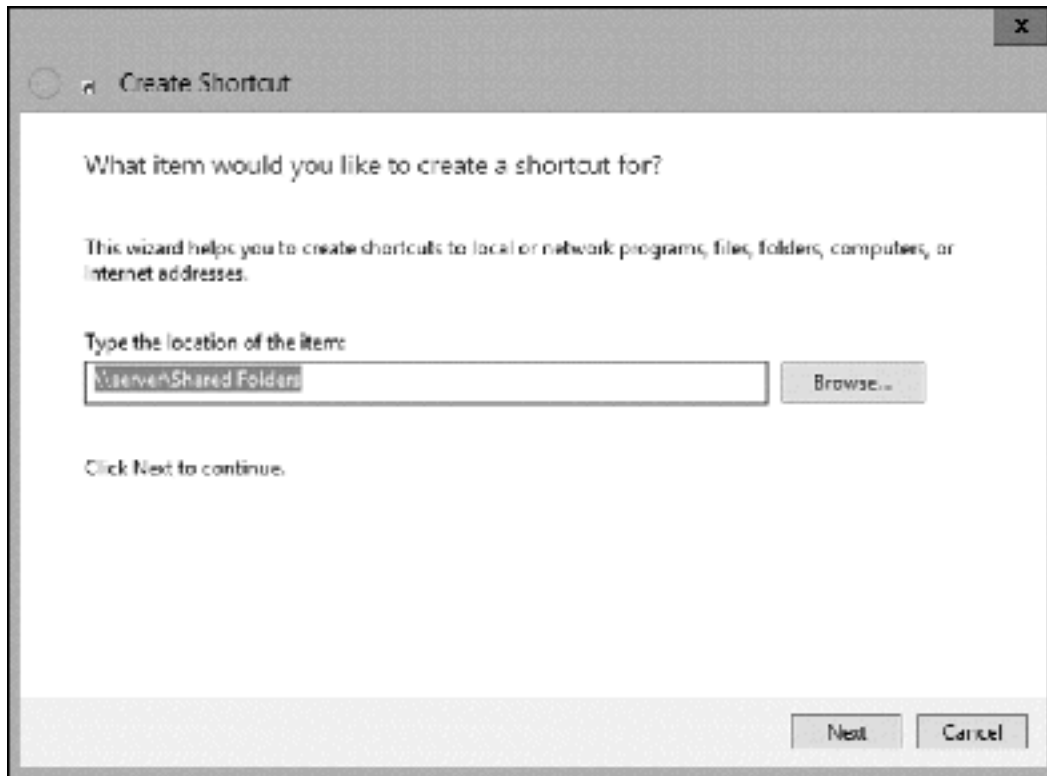
Figure 159: Create a shortcut

On the subsequent screen, type a name for the shortcut e.g. *Shared Folders* then click **Finish**.

12.8 Managing Computers from the Server

Essentials features a remote support capability. Using it, it is possible to connect to computers on the network and take control and manage without having to physically visit them, which is useful for support purposes, installing software and so on.

The computer to be managed needs to be powered on. If so, it will appear in the Dashboard under the **DEVICES** tab. Right-click on it and choose **Remote Desktop to the computer**. A prompt to logon to the computer will appear – normally you would enter the details for *systemadmin*. Note that if a user is already logged in to the computer then they will be logged off to permit the remote support session.

Having logged in, it is just as though you are sitting in front of that computer. When your work is finished, be sure to logoff.

12.9 Windows Server Essentials Media Pack

Add-ins are programs that are specifically designed to work with Essentials to improve functionality or add new capabilities. They run on the server and when installed integrate themselves with the Dashboard, such that they can be managed from it. Add-ins may come from Microsoft themselves or from third parties and may be free or supplied on a commercial basis. To obtain a list of Add-ins available from Microsoft, launch the Dashboard, click **APPLICATIONS** and then click the **Microsoft Pinpoint** tab. Third party Add-ins are usually obtained directly from the suppliers' websites.

A good example of an Add-in is *Windows Server Essentials Media Pack* from Microsoft. This provides media streaming capabilities, enabling the server to stream media such as photos, music and videos to DLNA-compliant clients such as the Xbox, smart TVs, Blu ray players and media streaming devices. Although Essentials is usually pitched as a business product, it is often installed in home-based businesses and sometimes as a home system. Plus of course some businesses are media based and require streaming capabilities.

Download and install the *Windows Server Essentials Media Pack* from Microsoft's website (Google it to find it). The installation will run for several minutes. After completion launch the **Dashboard**, click on **Settings** and a new entry called *Media* will have appeared – click it to display the following:
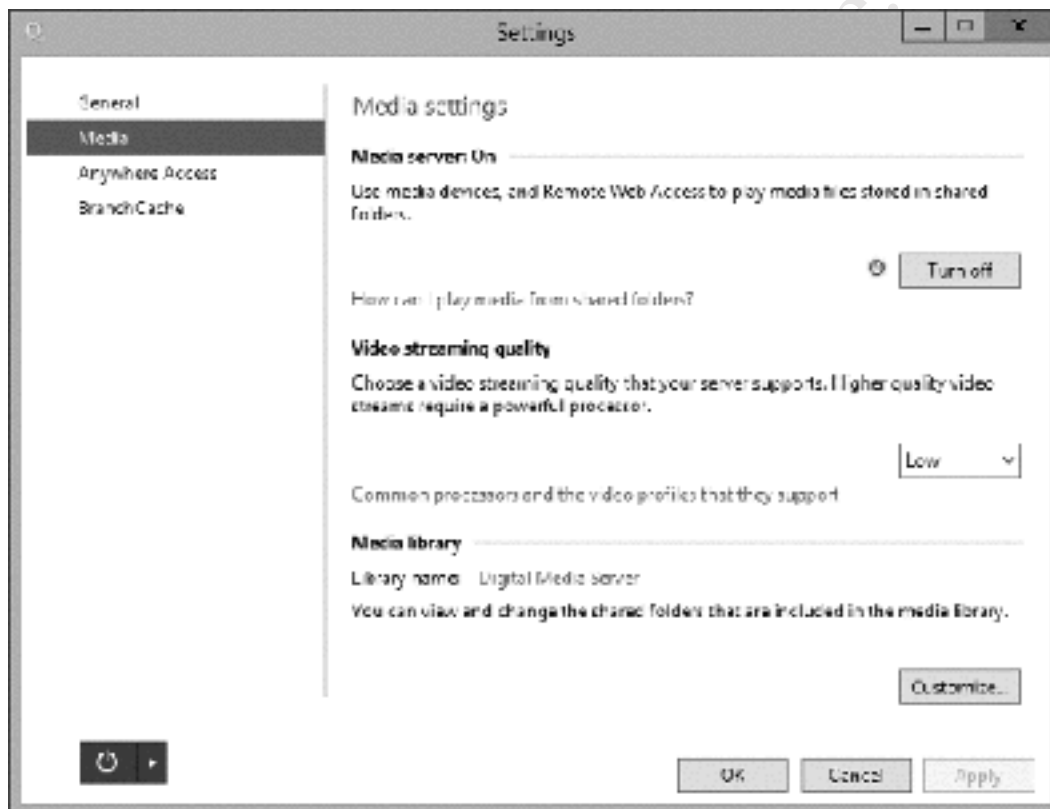

Figure 160: Media Settings

There are three settings. The first one is a simple switch to turn streaming on or off. The second one – *Video streaming quality* – is a dropdown that controls the quality of the video. This is a matter of experimentation and, as might be expected, higher quality video streaming requires a more powerful server.

The third setting – *Media library* – controls the media folders. During installation, three new shared folders will have been created: *Music*, *Pictures* and *Videos*, all located inside *ServerFolders*. By default these are shared and used for holding media; using this panel it is possible to exclude them from media

usage and/or specify additional folders. Unless you have specific requirements, it is suggested you simply use the default settings:
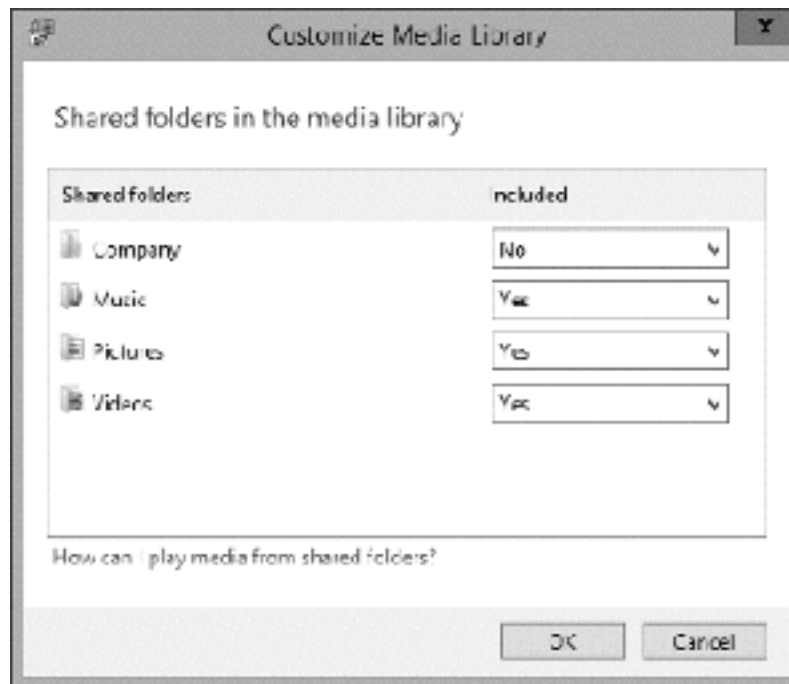

Figure 161: Customize the Media Library

The next step is to populate the folders by copying files in the appropriate formats into each of the folders. For instance, JPEG/JPGs into *Pictures*, MP3's into *Music* and MP4's into *Videos*. Having done so you should be able to connect your DLNA client to the server. As DLNA devices vary somewhat there is no single method for doing so. Some clients, for instance Windows PCs, will simply see the media server within Windows Explorer/File Explorer. Double-click the server and the computer's default media player should open – you should then be able to access photo, music and videos (in the case of Windows Media Player the server will be listed underneath the Other Libraries section):
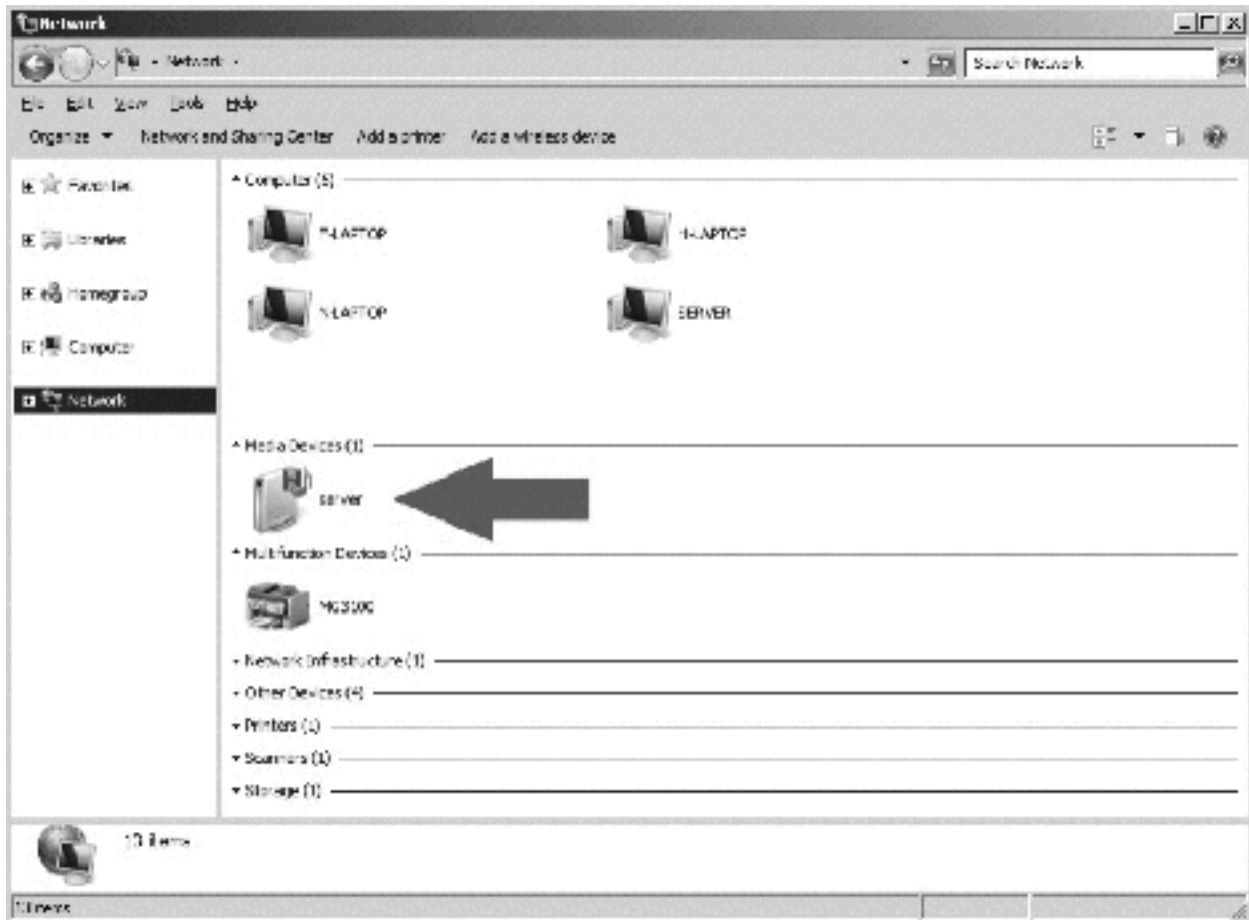
Figure 162: How Windows 'sees' the media server

On other devices it may be necessary to explicitly go into network settings or there may be an option to search for media servers - refer to the manufacturer's instructions or website for details.

12.10 Installing DHCP

Essentials assumes that IP addresses are provided by an all-in-one internet router or hub; accordingly, it does not run a DHCP service by default and it has to be manually installed if such a router is not being used. This is done using the instructions below; unfortunately, it does necessitate "going under the hood" to use the more complicated tools of Windows server.

Bring up a command prompt and enter *servermanager* to display this screen:
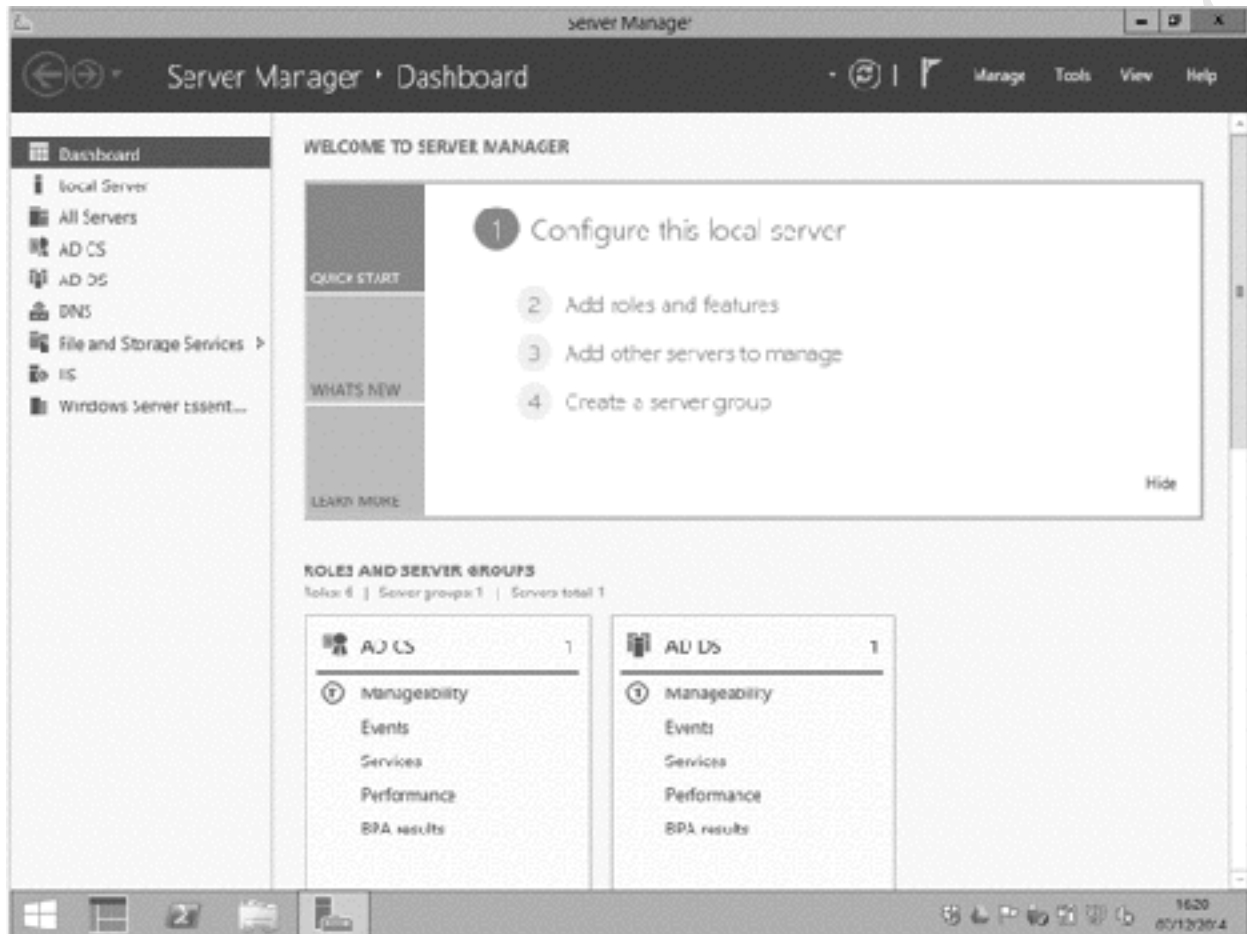
Figure 163: Server Manager screen

Click **Manage**. Choose **Add roles and features**. Click **Next** on the *Add Roles and Features Wizard* and on the resultant screen choose **Role-based or feature-based installation** followed by **Next**. On the next screen make sure the server is highlighted and click **Next**. On the list of possible features click **DHCP Server**. A message will appear asking if additional (required) features should be added. Make sure that the **Include management tools (if applicable)** box is ticked and click the **Add Features** button:
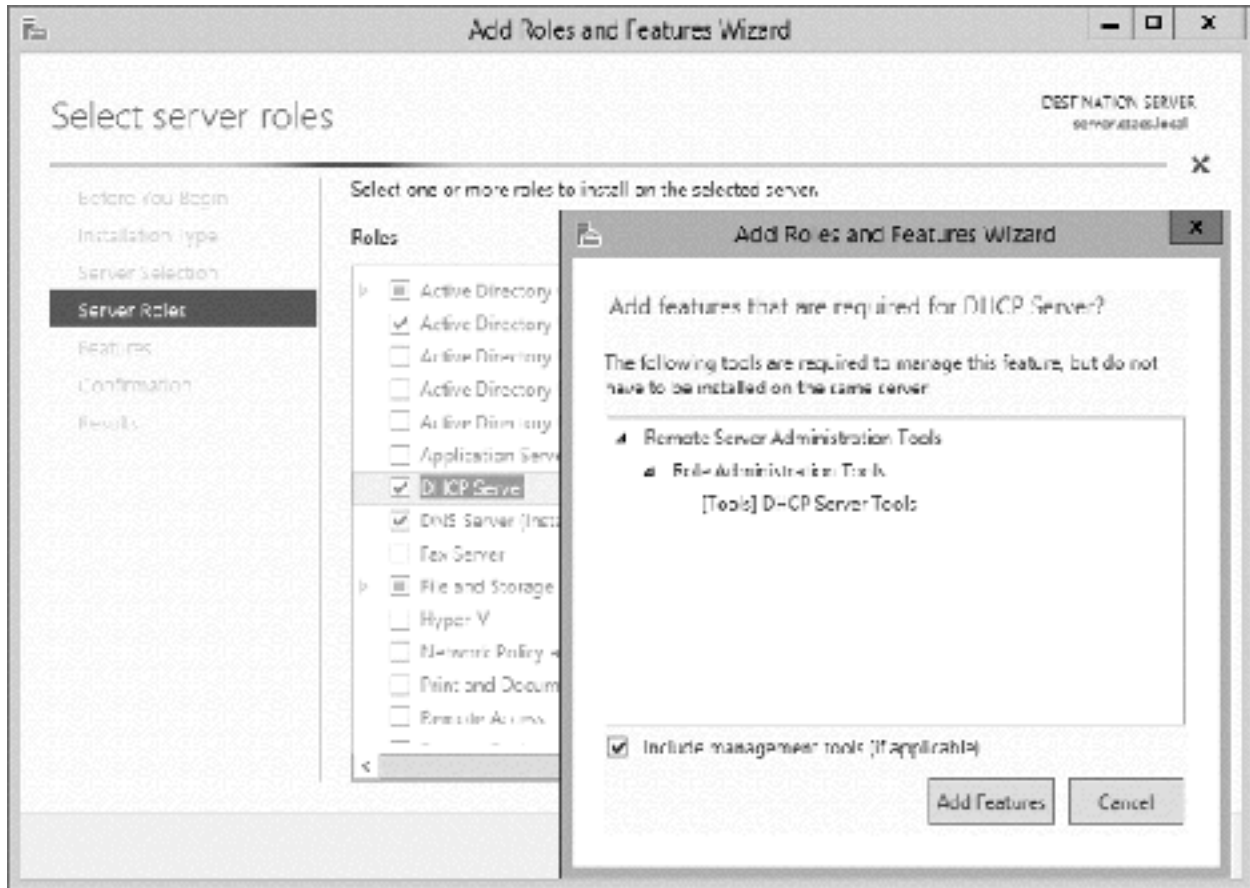
Figure 164: Choose DHCP Server

Carry on clicking **Next** on each subsequent screen. Eventually a confirmation screen is displayed; tick the **Restart the destination server automatically if required** box followed by **Yes** to the message:
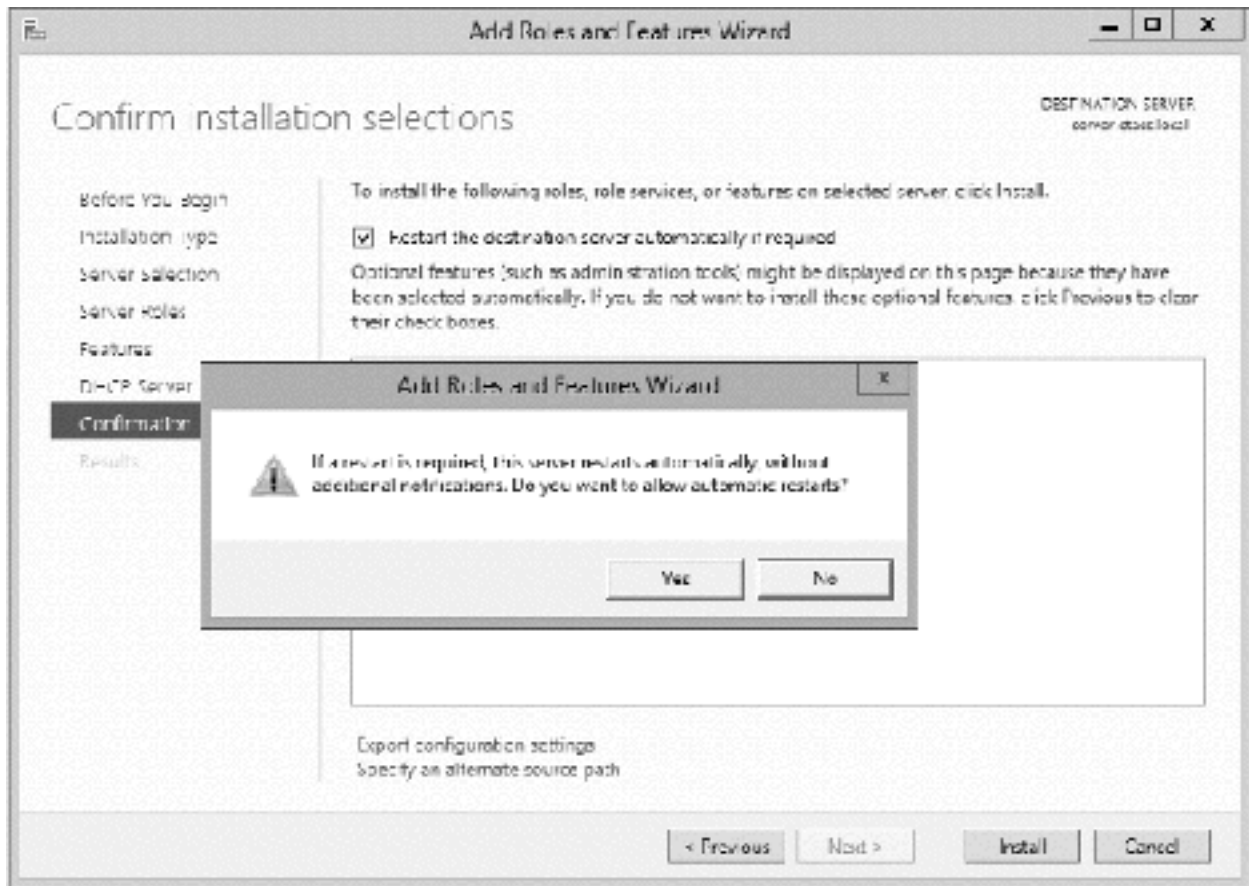
Figure 165: Reminder about automatic restarts

Finally click the **Install** button. Whilst the process is running, which may take several minutes, a progress screen is shown; when complete, click **Close**:
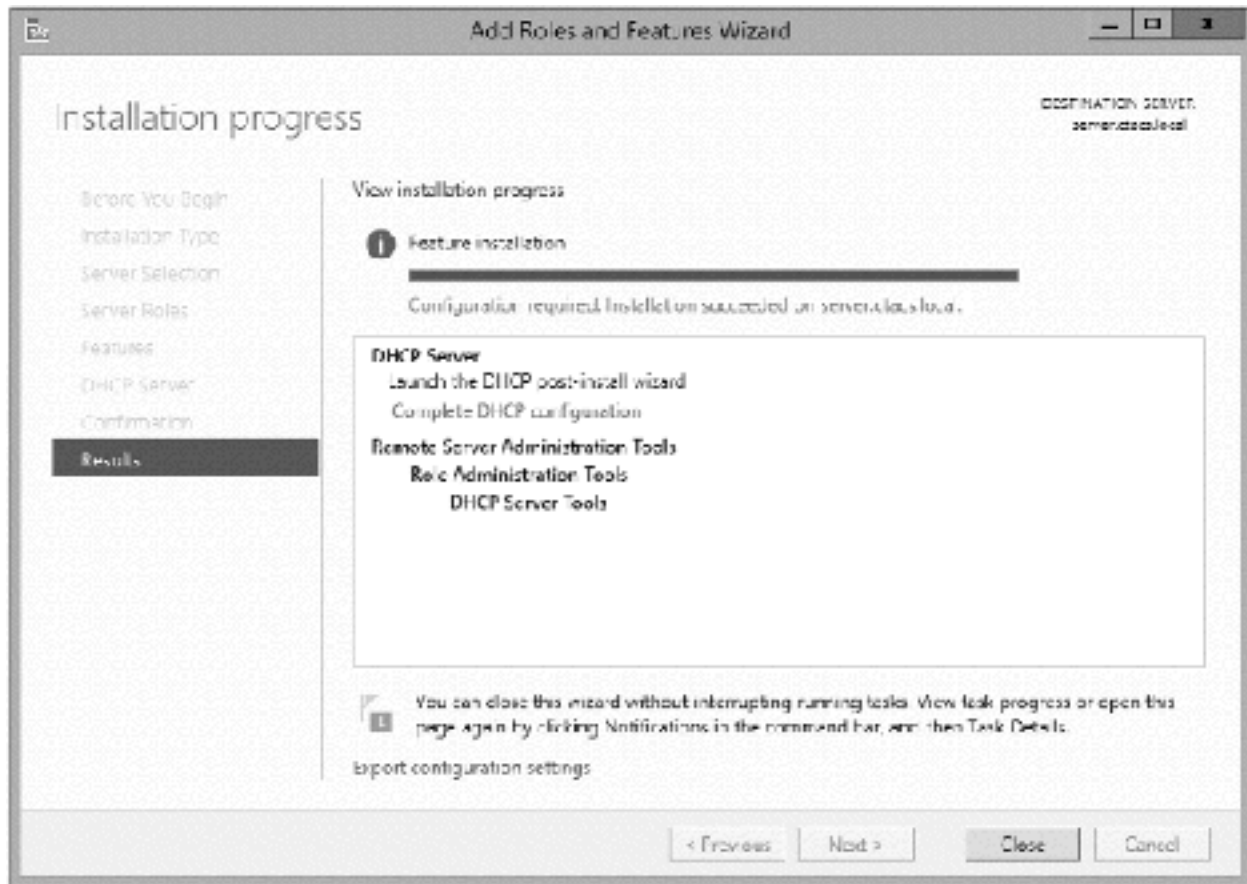
Figure 166: Installation progress screen

Restart the server at this point. When the server comes back up, run System Manager again. There will an entry for DHCP in the left-hand panel – click on it. There is a warning message that configuration work is required; work through the message until a hyperlink entitled **Complete DHCP configuration** is displayed then click on it:
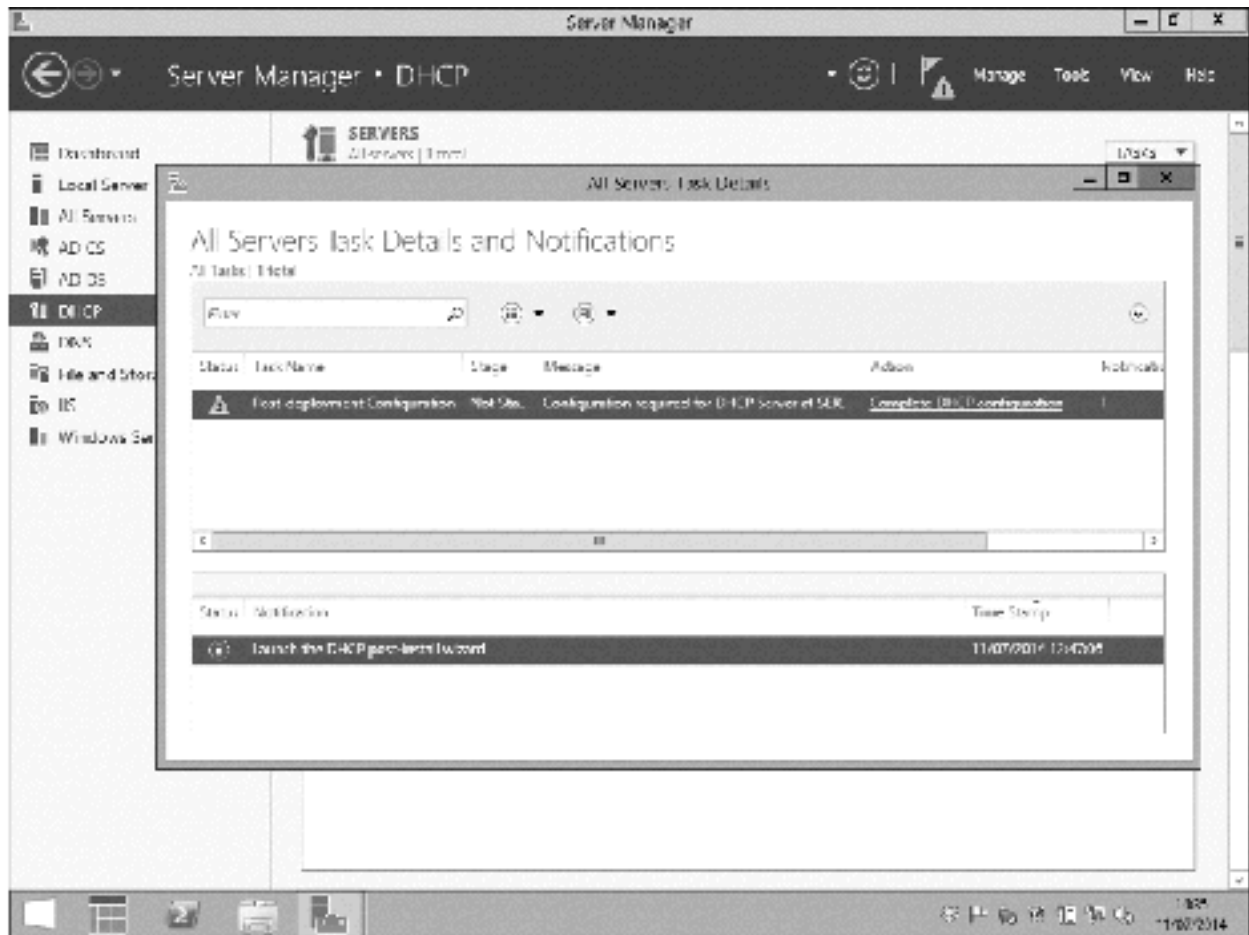
Figure 167: Message about further configuration

The *DHCP Post-Install configuration* wizard appears. Click **Next** to show the following:
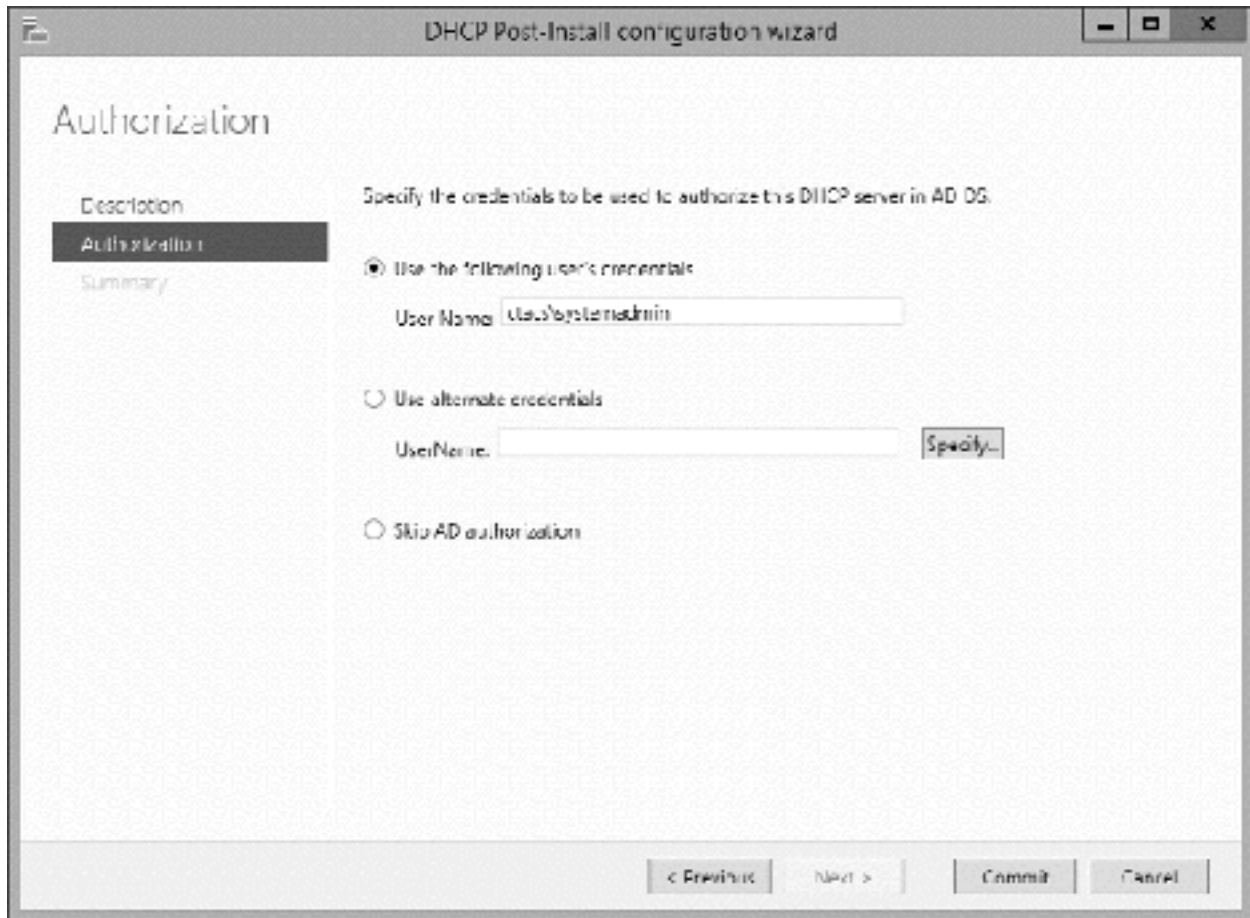
Figure 168: Post-Install configuration wizard

The existing user credentials (*"Systemadmin"*) are fine so just click the **Commit** button. After a few seconds a Summary panel will be shown. Click **Close**.

It is now necessary to configure the IP scope. Click on **Administrative Tools** and choose **DHCP**. Expand the tree down the left-hand side so it appears as follows:

Figure 169: Configure DHCP Server

Right-click on the entry for **IPv4** and choose **New Scope** to bring up the New Scope Wizard. Click **Next** and the following panel is displayed. Give it a suitable name e.g. *workstations* and a description, then click the **Next** button:
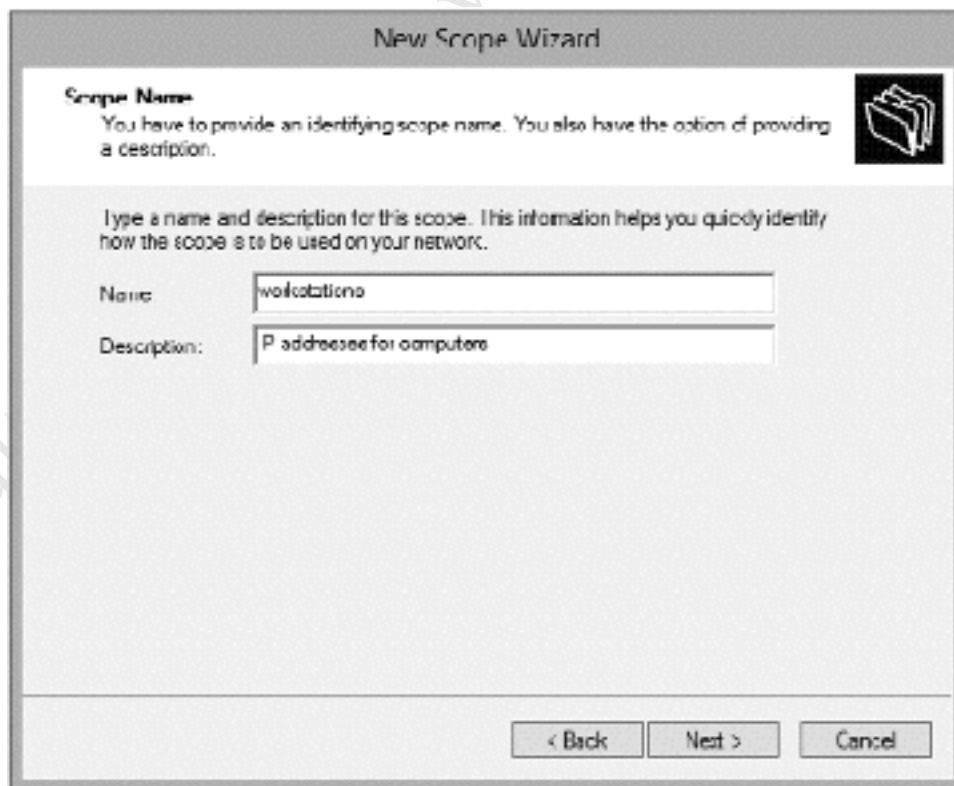
On the subsequent screen enter the addresses as outlined in the earlier section *IP Considerations*. In this example, our server is on 192.168.1.254 and the scope for the workstations will be 192.168.1.100 to 192.168.1.150. Set the **Length** to 24 and the **Subnet mask** will automatically adjust to 255.255.255.0. Then click **Next**:

Figure 171: IP address range for DHCP server

The next panel allows you to specify any exclusions (gaps) in the IP scope. Unless you have very specific requirements (unlikely) just click **Next**.
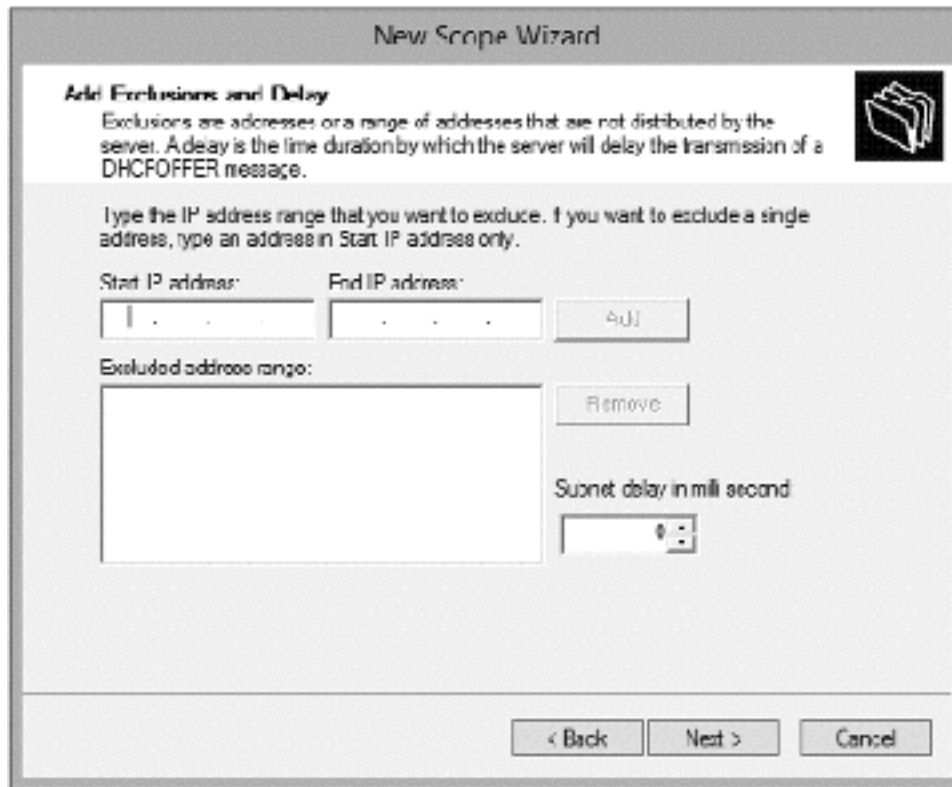
Figure 172: Exclusions and delays

The subsequent screen is for specifying how long a lease will last. The default value of 8 days is inappropriate, so reduce it to one day and click **Next**.
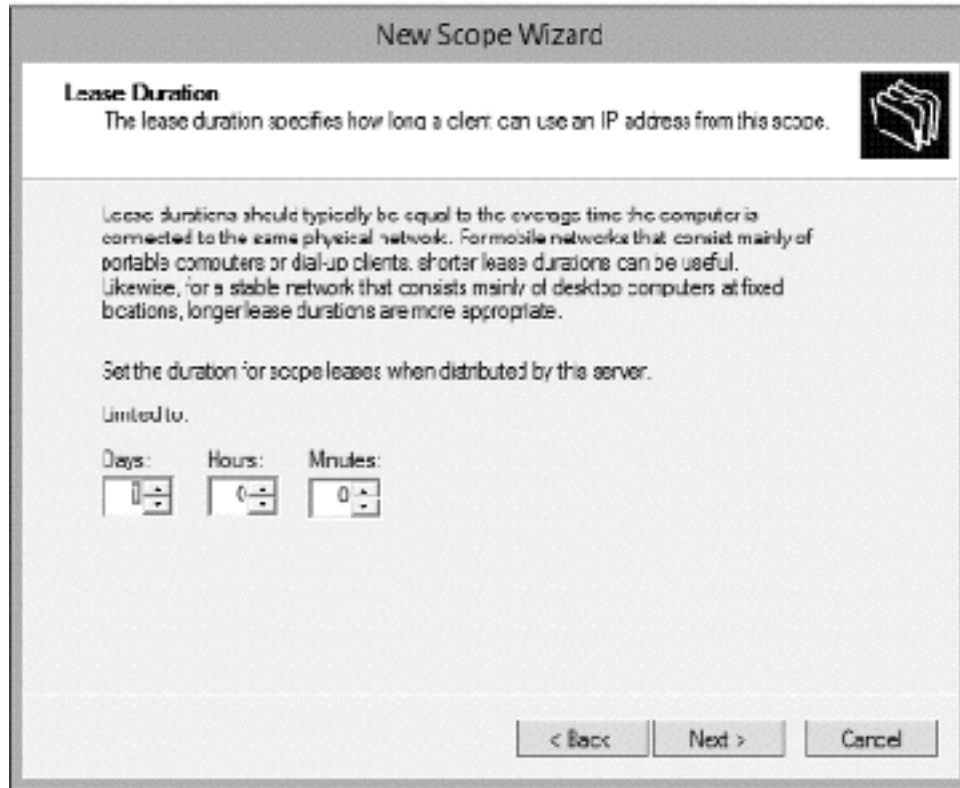
Figure 173: Specify Lease Duration

The following screen is concerned with more sophisticated options. They are of no great importance so choose **No, I will configure these options later** and click **Next**.
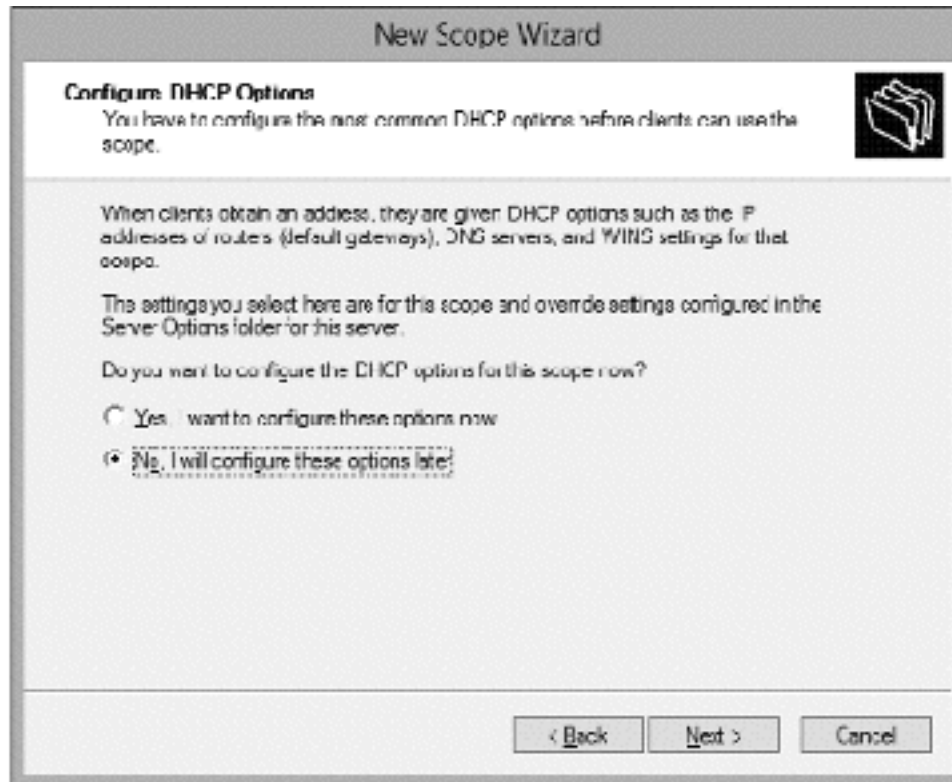
Figure 174: Configure more advanced DHCP options

Upon completion - which is a matter of seconds - a confirmation screen is shown. Click **Finish**.

Figure 175: Completion notice for New Scope Wizard

The scope now has to be activated. Expand the tree on the left-hand side of the DHCP panel. Currently, the entry for IPv4 will have a blue circle with a white exclamation mark on it. Wait 30 seconds then right-click the new scope that we just created and choose **Activate**. The exclamation mark will be replaced by a green circle containing a white tick mark in it; everything should now be working correctly.
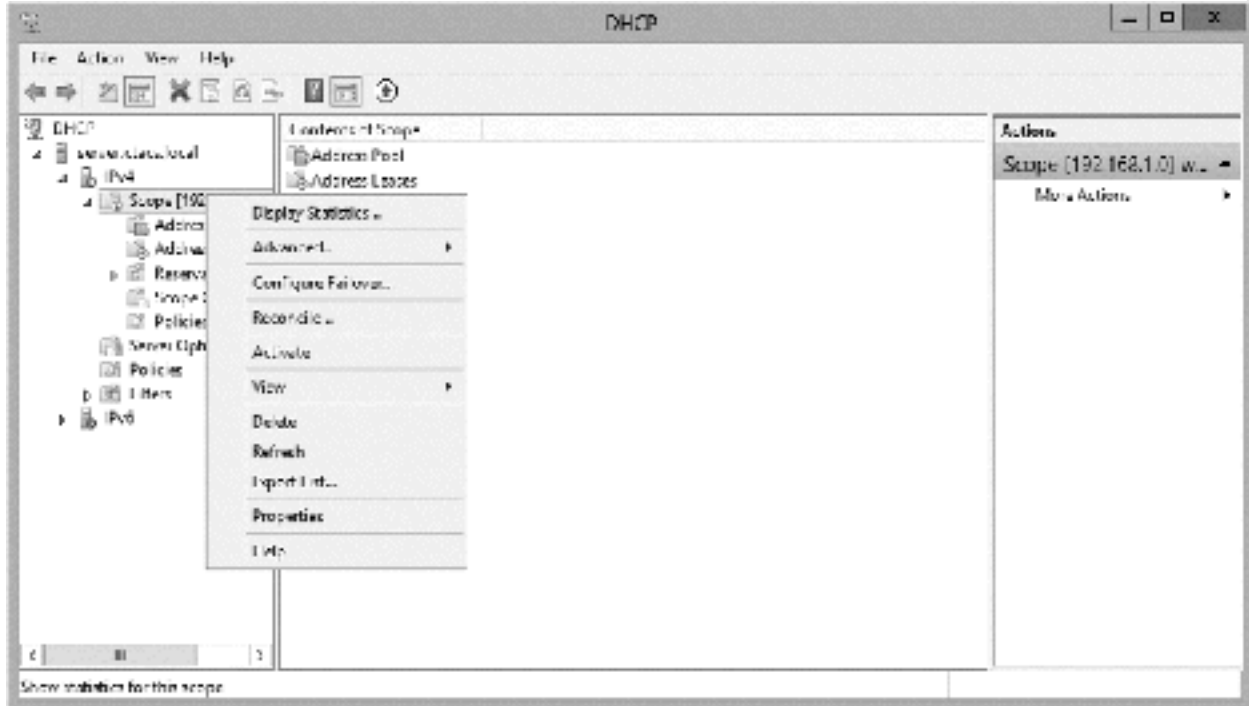

Figure 176: DHCP after configuration

12.11 Multiple Network Adapters (NIC Teaming)

A file server may have more than one network (Ethernet) adapter. In the case of *Storage Server*, there are always two adapters as standard. Multiple adapters can be used together in different ways to improve resilience and/or performance using a technique referred to as *Teaming* or *NIC Teaming* (NIC is short for *Network Interface Card*).

In this example, a second Ethernet adapter has been installed in the server to try and improve network performance. Important: before progressing, make a note of the settings of the first adapter, which was given a fixed IP address in Chapter 2. INSTALLATION OF WINDOWS SERVER 2012 R2 ESSENTIALS, as it may be necessary to re-enter them later on.

On the server, launch Server Manager (bring up a command prompt and enter *servermanager* or go the **Start Screen** and click on **Administrative Tools** and run it from there). Click on **Configure this local server**. In the Properties section look for the NIC Teaming entry. Click where it reads **Disabled** and the following panel is shown:
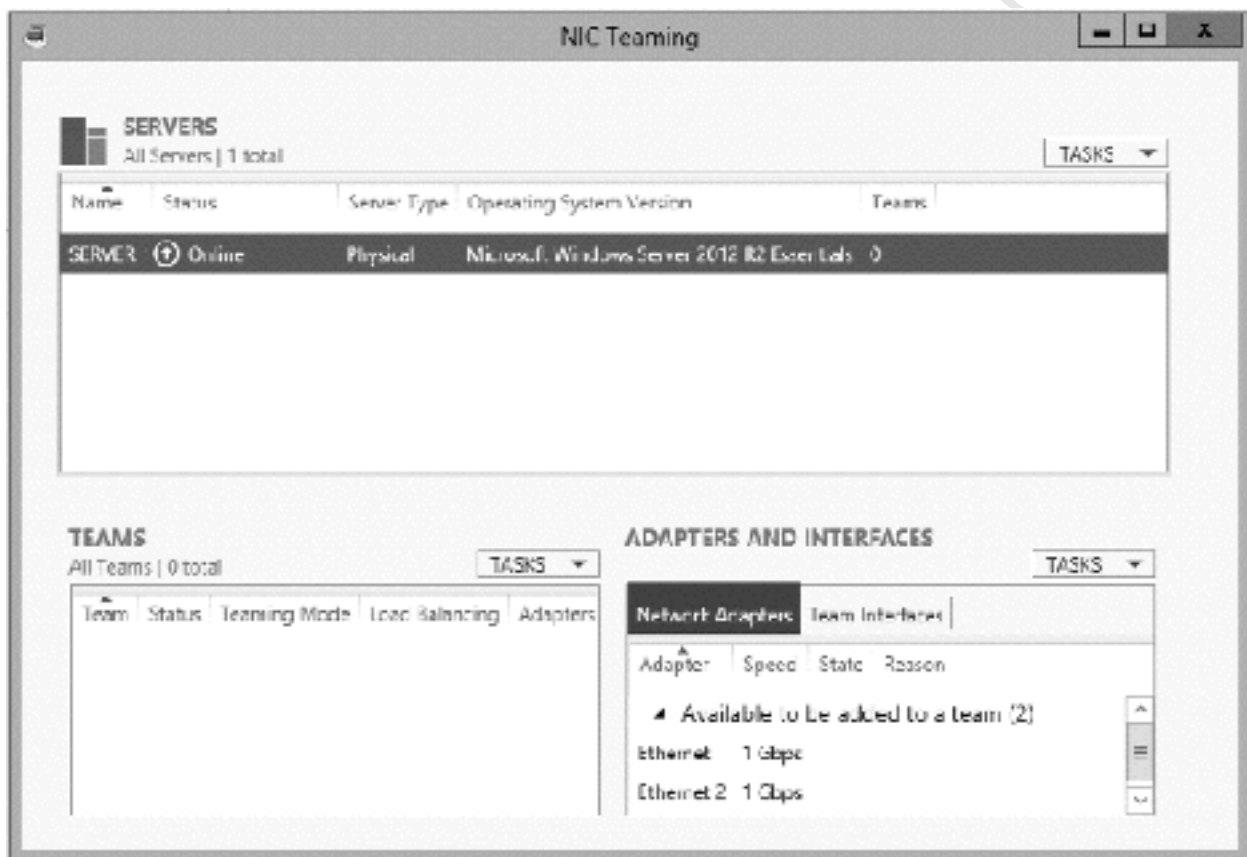

Figure 177: NIC Teaming screen

In the Teams section, click the **TASKS** drop-down and choose **New Team**. On the resultant panel, give the Team a name, tick the boxes for the network adapters and click **OK**. In this example we have called our Team *LAN* and are using two network adapters. The 'Additional properties' entry is for setting more advanced options; for instance, if you wish to configure one of the network adapters as a Standby adapter which will take over if the main one fails:
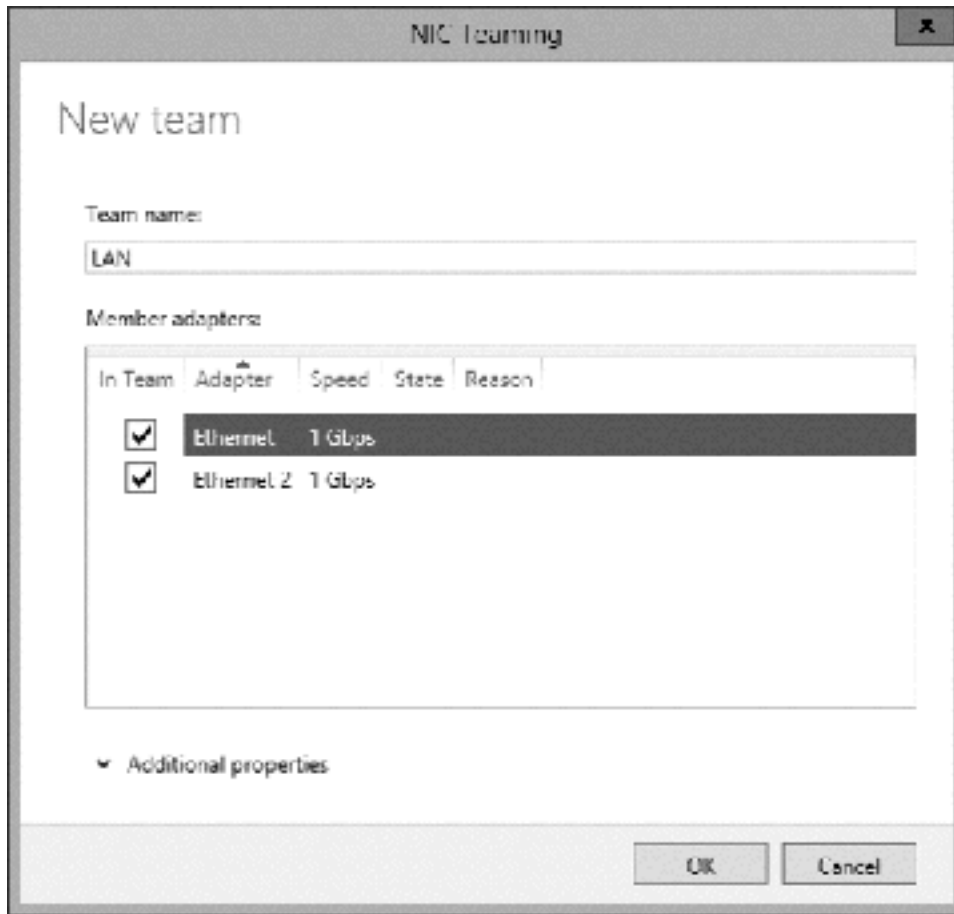
Figure 178: Creating a new team

The server may take a minute or so to adjust, during which time connectivity may be lost and an error status may be displayed on the NIC Teaming screen. When everything is working it should appear so:
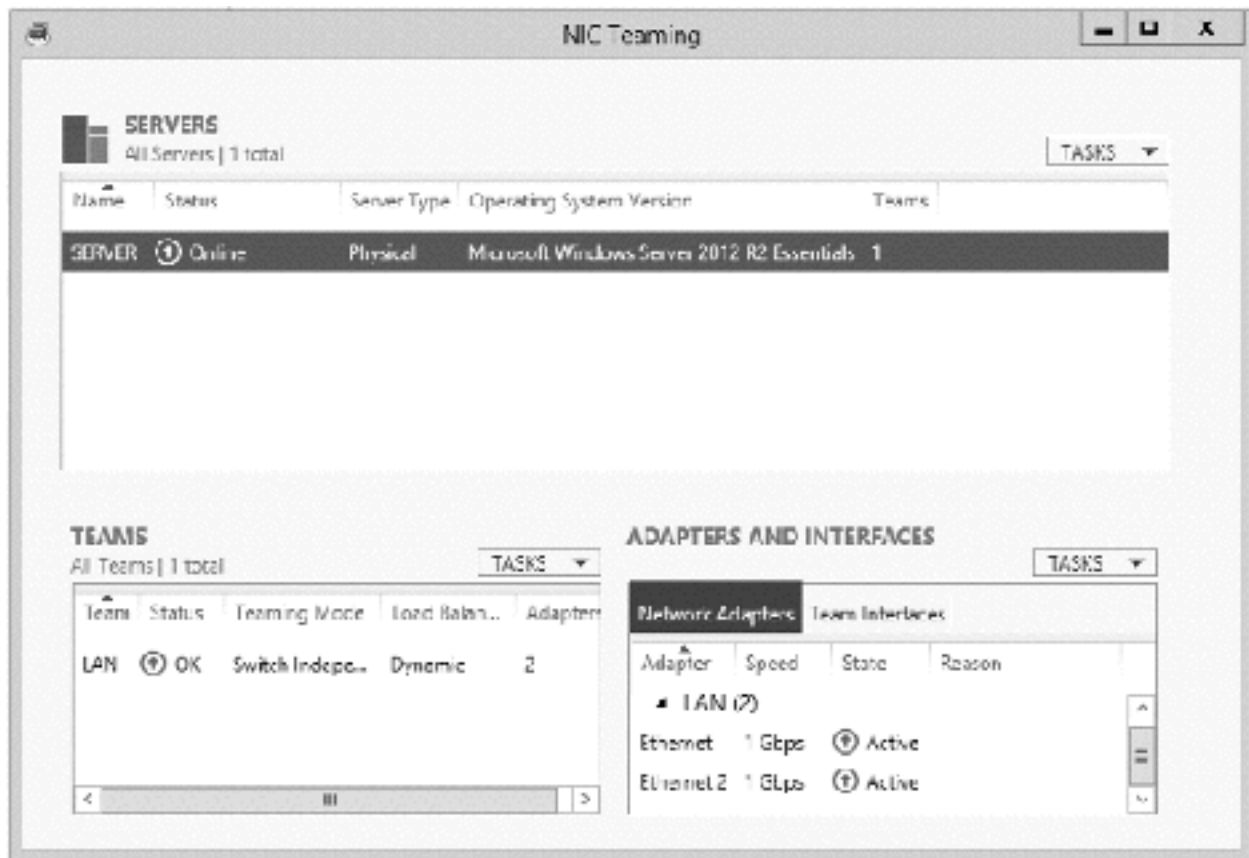
Figure 179: NIC Teaming status

Note that the server's IP address may have changed as a consequence of doing this and it is therefore strongly advised that you immediately check and correct matters if necessary. Returning to the server Properties screen within Server Manager, there should now be an entry underneath NIC Teaming for *LAN* (or whatever you called the Team):
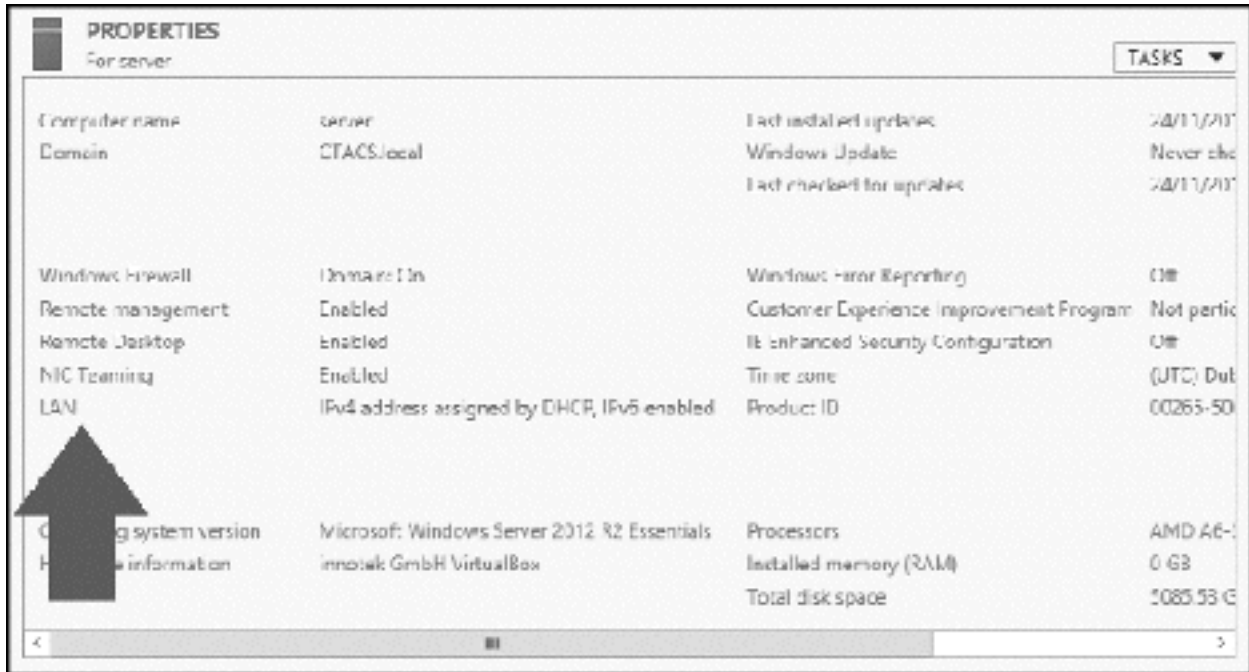
Figure 180: LAN entry in server Properties

Click on the blue writing to the right of *LAN* and it will display the Network Connections:
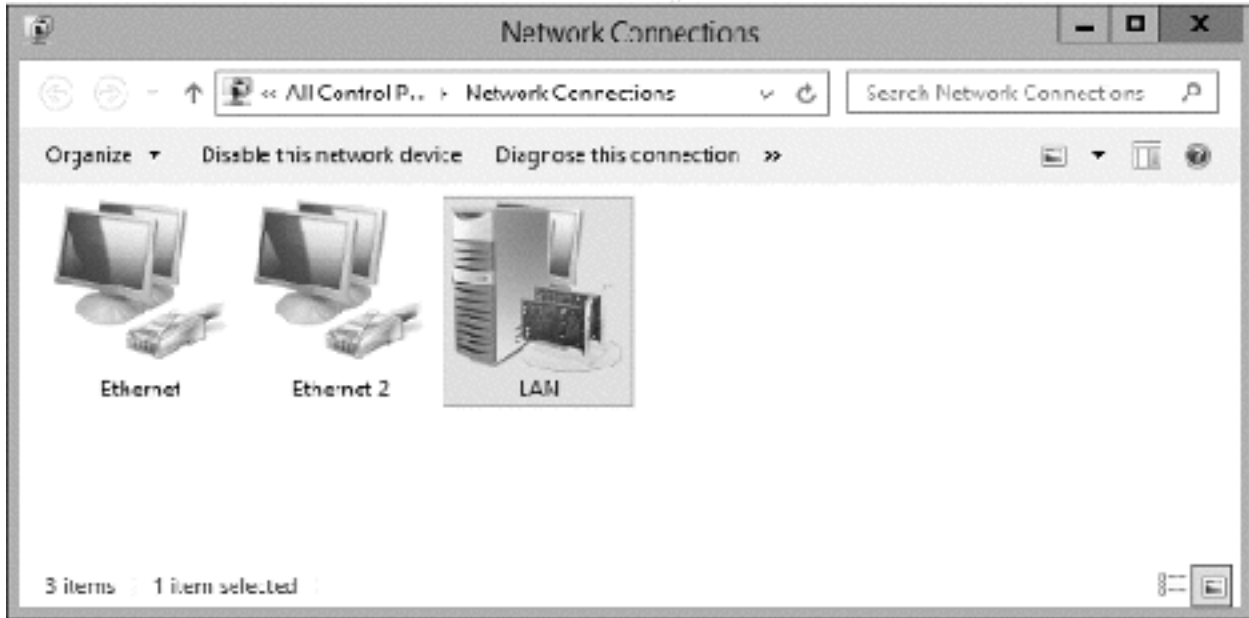

Figure 181: Network Connections

Right-click the entry for *LAN* and choose **Properties**. Highlight **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. Change the entries to be the same as they were before beginning this exercise.

12.12 Installing Windows Server Essentials Experience on Server 2012

Essentials is a member of the wider Windows Server family, which includes editions that can handle hundreds, thousands, even tens of thousands of users. The key technical differentiator between Essentials and its larger siblings is the Windows Server Essentials Dashboard, which provides a simplified and elegant way of setting up and managing features that normally require a great deal of time, effort and knowledge. However, it is possible to add this feature to the standard versions of Windows Server, where it is known as the *Windows Server Essentials Experience*. Why would you wish to do this? One reason is that Essentials is restricted to a maximum of 25 users. If an organization outgrew it they would have to move to a regular version of Windows Server, but they may wish to retain the methods of working and systems management that they are accustomed to. This section describes how to install the Essentials Experience onto regular Windows Server for organizations that are undertaking such an upgrade.

Launch **Server Manager** and click **Manage** followed by **Add Roles and Features**. Choose **Role-based or feature-based installation** and click **Next**. Select the destination server - there may only be one of course - and click **Next**. Tick **Windows Server Essentials Experience** on the subsequent screen, followed by **Next**. A message about the requirement for additional features is displayed – click the **Add Features** button to proceed:
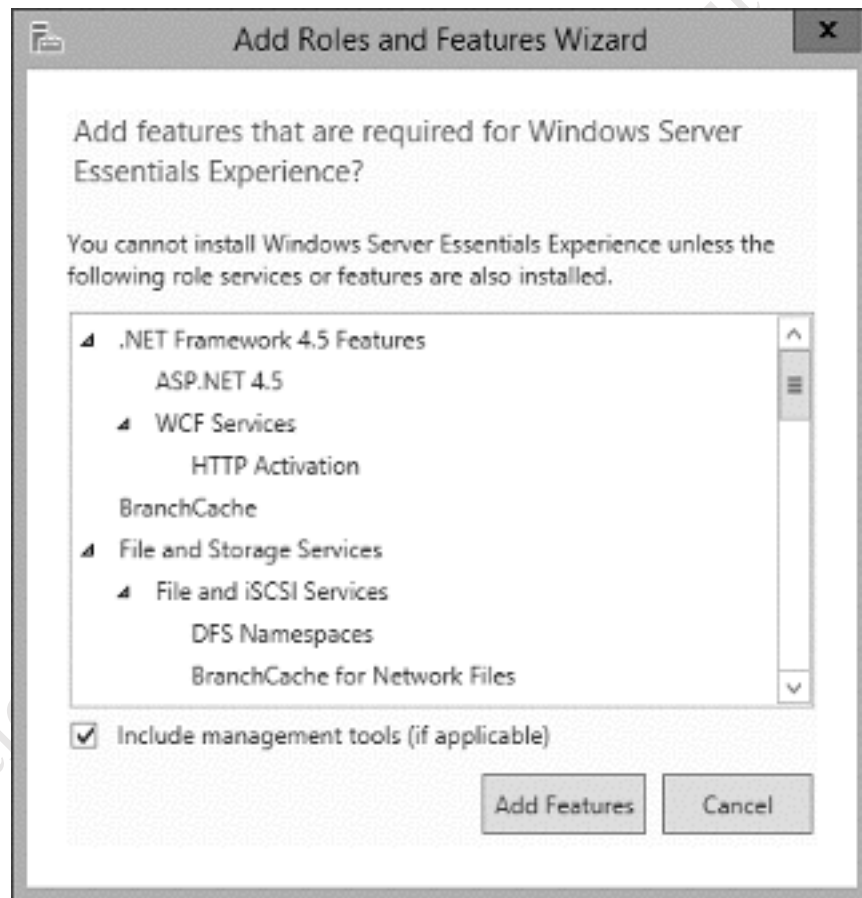

Figure 182: Add Roles and Features Wizard

Click **Next** on the subsequent screens. After a while a screen about the Web Server (IIS) is shown – click **Next** on this, too. A screen to confirm the various options is displayed – tick the **Restart the destination server automatically if required box** then click **Install**.

The installation will run for a number of minutes and the server may restart during this time. When it is completed, login and go to **Server Manager**. On the Dashboard there will be a notification flag to the effect that additional configuration work is required – click the message to start the process. After a short while a screen entitled *Configure Windows Server Essentials* is displayed; click the **Configure** button. The configuration process will then take a further several minutes to complete.

A new icon – simply called *Dashboard* – will have been placed on the Desktop of the server. Note that this is the Dashboard from Windows Server Essentials and quite separate from the regular Windows Server Manager Dashboard. Double-clicking it will display the standard console for managing an Essentials server that has been used throughout this guide. It is suggested that the server is managed totally using the Essentials Dashboard and that the standard tools of Windows Server are not used.