Windows Server 2016 Network Installation Guide

Nicholas Rushton, BA Hons.

Callisto Technology And Consultancy Services

Updated July 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 small business networks. This is what purchasers of the *Windows Server Network Installation Guide* have written in their reviews:

*"***** Excellent Book"* – Frank

"Excellent Guide for anyone starting a Home or Small Office Network… A must read for any non-IT professional attempting to setup and maintain a small office or home network. This guide begins with the basic concepts of pre-installation and steps you through to a live server". – Mikmock

"This book is EXCELLENT for setting up a server for a small business environment with a single server. Even with very little knowledge of servers, one can easily get up and running using this step by step guide. This covers all the steps in a logical, clear, and well written sequence, and addresses all the real-life issues one might encounter getting a server up and running". – Paul

"One of the best entry level guides to server installation…As an entry level, step by step, setup guide, Nick Rushton's guides are beautiful". – Bill L

"This is a great, simple introduction to the installation and basic configuration of Windows Server. There's a minimum of introductory / what's new in this release / what's a network kind of filler material - the book pretty much gets straight into step-by-step instructions on how to install and then configure the installation". – Amazon Customer

"Great Guide. To the point with actual steps for completing an installation." - ByJWPon

Introduction

What is this guide and who is it for?

The purpose of this guide is to take the reader through a typical installation of a small Windows Server 2016 network and is written for the following audiences:

- Someone who is new to Windows Server 2016 and installing it for the first time
- Someone setting up Windows Server 2016 in a small business setting
- Someone wishing to learn the basics of Windows Server 2016 and who wants a succinct, practical guide based on real world scenarios

The approach is very much practical and hands on. It should give you a basic understanding of Windows Server and help you setup a network that should meet the needs of a typical small organization such as a business, non-profit, church, school and so on. However, it is not intended as a detailed description of all Window Server's many capabilities or as a reference manual and is not aimed at enterprise installations involving large numbers of servers and techniques such as virtualization. It assumes a reasonable working knowledge of Windows and the basics of networking. It is written in a friendly, "do-it-like-this" style, rather than with undue emphasis on theory and abstract topics.

The book is organized as follows:

Chapter 1 gives an overview of Windows Server and describes the components of a network. Chapter 2 describes how to install the software and get the server up and running. Configuring disk storage and creating shared folders is covered in Chapter 3, whilst Chapter 4 describes how to create and manage users. Connecting devices such as desktops and laptops is the topic of Chapter 5. How to backup the server to cope with problems and recover data is important and is covered in Chapter 6, whereas Chapter 7 is about printing. Exercising greater control over the network is covered in Chapter 8, Group Policy. Remote access to the network via a VPN is covered comprehensively in Chapter 9. Housekeeping and maintenance are covered in Chapter 10. Chapter 11 is about getting started with the Windows Server Essentials Experience. Finally, Chapter 12 covers a range of miscellaneous and some more advanced topics.

About the Author

The author has worked in IT for over 35 years, on systems of all sizes and types throughout the world, from the largest companies to the smallest. A lot of his professional interest in recent years 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 and is the author of numerous networking guides, published through CTACS as eBooks and paperbacks. Other titles include: *Windows Server 2019 Essentials; Windows Server 2019; Windows Server 2016 Essentials; Little Book of macOS Server; Synology NAS Setup Guide; Little Book of Synology; QNAS Setup Guide; Little Book of QNAP QTS; Using Windows 10 as a Server; Little Book of TerraMaster.*

Problems with the Artwork?

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

1. INTRODUCTION

1.1 What is Windows Server 2016?

Windows Server 2016 is a popular version of Microsoft's networking software for organizations of all sizes; with a legacy of more than 20 years, it is a mature, well-established and reliable platform. During that time it has evolved constantly, adding new functionality and capabilities and becoming easier to use and manage. In recent years, much of the focus in information technology has been on *cloud computing*, whereby data and applications are held externally and accessed over the internet. However, many organisations prefer to operate what Microsoft refer to as *on-premises computing*, whereby they own and run their own file server(s). There are several reasons for doing so:

- They wish to retain full ownership of their own data, keeping it fully under their own control. This may be because of security concerns, or a matter of simple preference.
- They may not have access to a sufficiently fast, reliable internet connection.
- The desire to avoid the ongoing subscription charges associated with cloud computing.
- There is a need to use one or more applications that require local processing and storage (for instance, a particular accounting or line-of-business package)

Windows Server is designed to address these requirements. It is available in three different, general purpose editions, plus there are a further three editions for use in more specialized roles. The variants reflect the different markets that Microsoft is targeting with the product and also reflect differences in licensing, capacity and functionality. The general purpose editions are as follows:

Windows Server 2016 Standard – this is the everyday version for business, education and other markets. A small business will typically have one or two physical file servers running Windows Server 2016 Standard. This guide is based around this edition.

Windows Server 2016 Datacenter – this is a higher capacity edition for larger organizations with multiple servers and/or locations and includes extensive support for virtualization and cloud-based computing. Although the basic principles of Windows Server as discussed in this guide are still applicable, the more advanced topics of particular interest to enterprise users are not covered.

Windows Server 2016 Essentials – this edition is for small businesses without in-house support and features a simplified user interface for configuration and management. The information in this guide is most applicable to Windows Server 2016 Standard and users of Essentials would find the CTACS *Windows Server 2016 Essentials Guide for Small Businesses* more relevant than this book.

The specialized editions are not covered in this guide, but for reference they are:

Windows Server 2016 MultiPoint Premium Server – available to academic customers only, this edition enables multiple low-cost workstations (sometimes referred to as 'dumb terminals') to be connected to a single server, providing benefits in terms of cost and manageability.

Windows Storage Server 2016 – enables computer manufacturers to create storage appliances, effectively NAS (network attached storage) devices, that run Windows rather than the more common Unix/Linux variants found in such products.

Microsoft Hyper-V Server 2016 – a hypervisor, used for running virtualized copies of Windows Server, especially cut-down versions known as Nano Servers.

1.2 A Typical Small Network

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

Server - this is the heart of the network, which runs Windows Server 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.

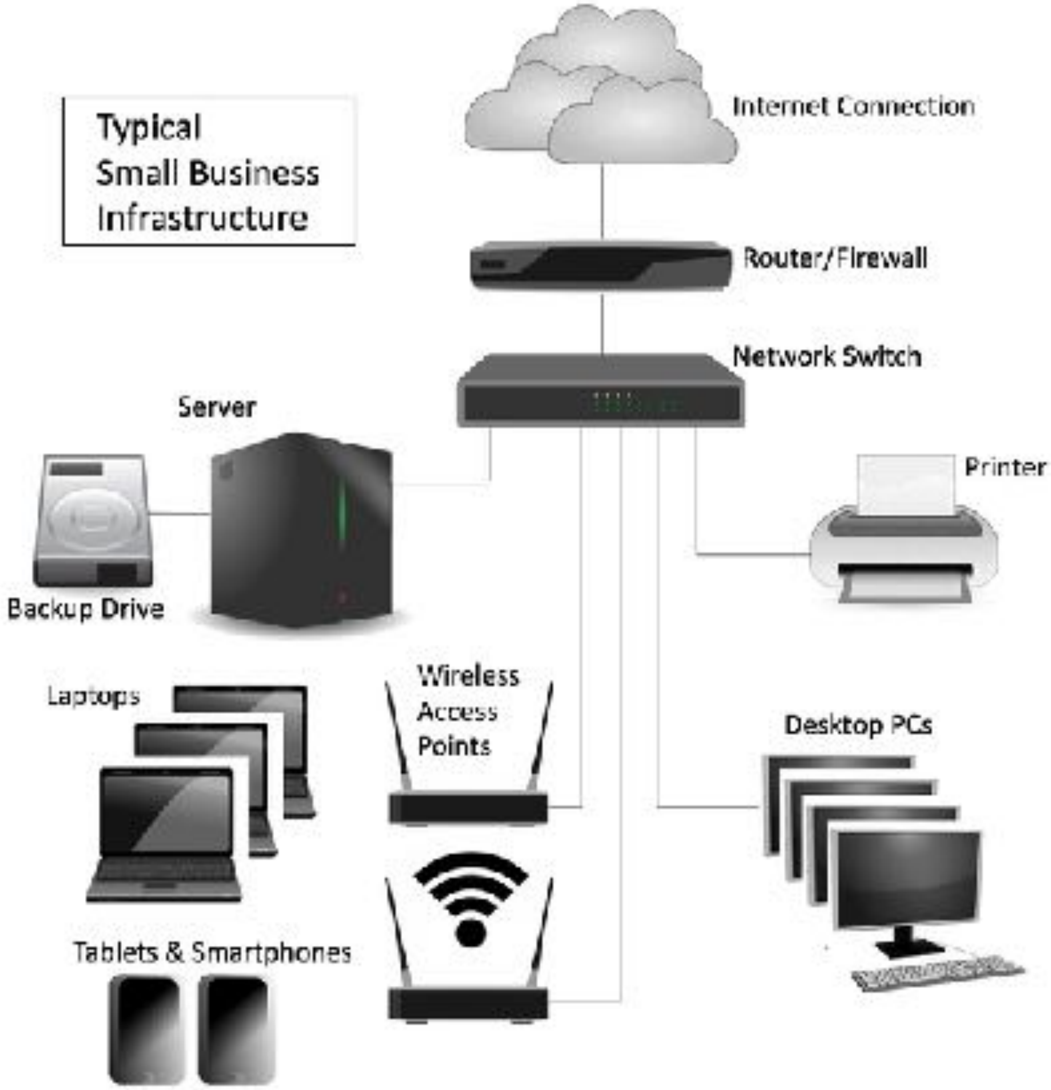


Figure 1: Typical small business infrastructure

1.3 The Server

Windows Server requires its own, dedicated server hardware, which may also be referred to as a *file server*. A server has some similarities to a regular 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 and Fujitsu; other brands are available, but you may wish to avoid obscure manufacturers and unbranded machines. File servers are not usually available in retail computer stores, but are obtained from specialist IT dealers or online. If you are learning about Windows Server 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*). If you do not have a copy of the Windows Server software, you can download a fully-functional but time-limited evaluation copy from Microsoft, which is ideal for learning purposes.

Choosing a server can be daunting, particularly as it is not something that an organization or individual 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 (known 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 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 (typically communications equipment and network switches).
- Often the given base price for a file server is for a bare-bones model and hard disk drives, memory and other features may have to be additionally specified. Costs can add up – be aware that a complete system may be several times the initial headline price and budget accordingly.
- Consider taking out a maintenance agreement at the time of purchase. These vary in service levels and cost and your choice will depend upon your requirements, but they generally provide peace of mind and good value. The key decision point is: How long can you operate 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 still 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 T40. For a slightly larger organization – say up to 25 users or so – a standard entry-level file server is more appropriate. Beyond that, increasingly powerful servers are available that can service hundreds of users. The next stage is to use multiple servers, with the workload spread across them. As mentioned above, there are a number of vendors to choose from. Dell are a popular choice as everything can be conveniently ordered from their website in many countries.

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

1.4 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” and upon which everything is stored. However, in a server there is usually a need for a greater amount of storage, plus that storage also must be very reliable. Performance becomes a consideration too, as many people may be accessing the server simultaneously. The way to address these requirements is by using multiple hard drives and to configure them in special ways. There is no *one-size-fits-all* solution here, as it depends upon the size, requirements and budget of the organization. The main options are reviewed below.

Single Drive System

A server in a very small organization might only have a single physical hard drive, although this is not generally advised as in the event of it failing the server will be out of action until it can be replaced, plus the associated risk of data loss is high. If you are using a server with a single hard drive, you can achieve some benefits of a two-drive system by dividing it into two volumes: one on which the operating system is installed (the C: drive) and one 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, plus it is also easier to manage and backup the data. The C: volume does not need to be huge – 60GB to 120GB is usually adequate and the remainder of the drive should be partitioned as the D: drive.

Twin Disk Drives

A common approach is to have two drives in the server, one for the operating system and one for the data. 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: if the first drive failed, the system would be totally out of action; if the second drive data failed, all the data would be lost and you would be dependent on the integrity of the backup (the topic of backups is covered in 6. BACKUPS AND RESTORES). The first drive can be quite small; at the time of writing, the smallest readily available drives are 120GB SSDs, which are ideal. However, if you plan on installing applications on the server, such as an accounting package or line-of-business application, then you might want something of greater capacity. The second drive, for the data, can be as large as you require or can afford.

RAID

RAID is short 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 and so on. 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 data is written, some goes on to one drive and some goes on to the other. As both drives are being written to or read simultaneously, throughput is maximized. 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 a bottleneck in many network systems. For these reasons RAID 0 should not normally be used.

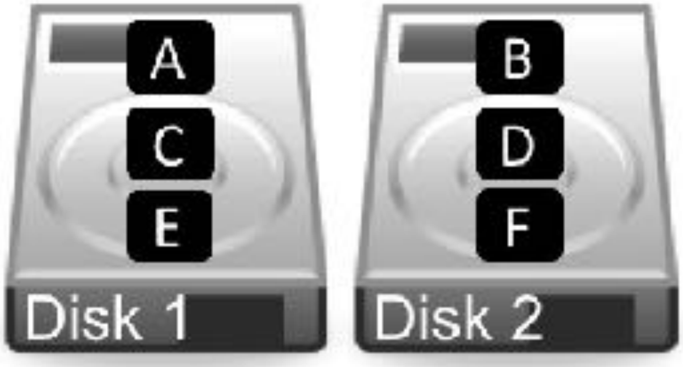


Figure 2: RAID 0 – Data striped across two drives

RAID 1 consists of two identical drives that mirror each other. 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 transparent. If one of the drives fails, the second one automatically takes over and the system carries on without interruption. At the earliest opportunity, the faulty drive should be replaced with a new one; the system is then synchronized 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 instance, if a disk array has two 2TB drives installed then the total amount of usable storage capacity is 2TB rather than 4TB.

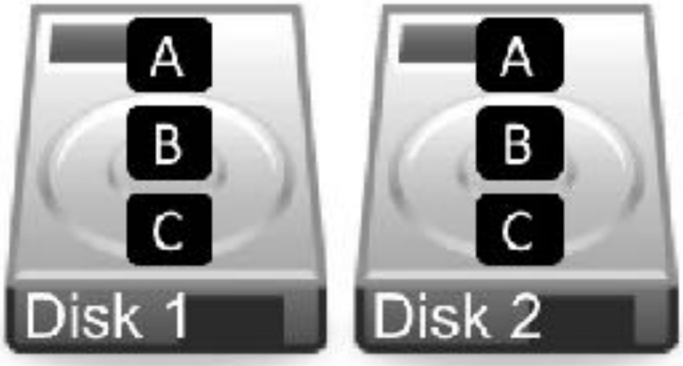


Figure 3: RAID 1 – Data mirrored across two drives

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

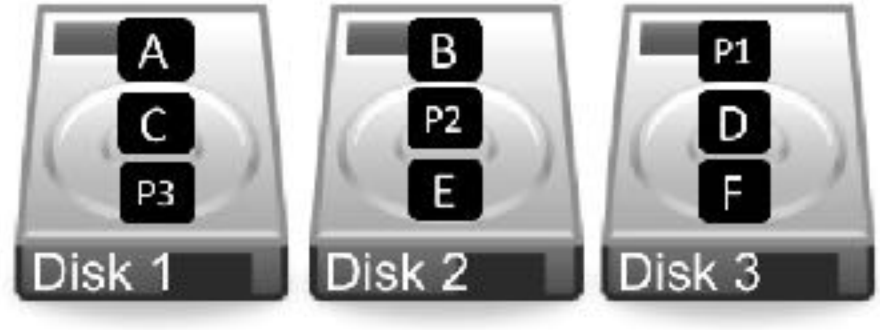


Figure 4: RAID 5 – Multiple drives with parity information

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 of the drives, thereby making it more resilient than RAID 5, but it loses more capacity in providing that resilience. There may also be a performance hit compared with RAID 5, due to the additional parity processing. If a disk array has five 2TB drives installed in a RAID configuration, then the total amount of usable storage capacity is 6TB rather than 10TB.

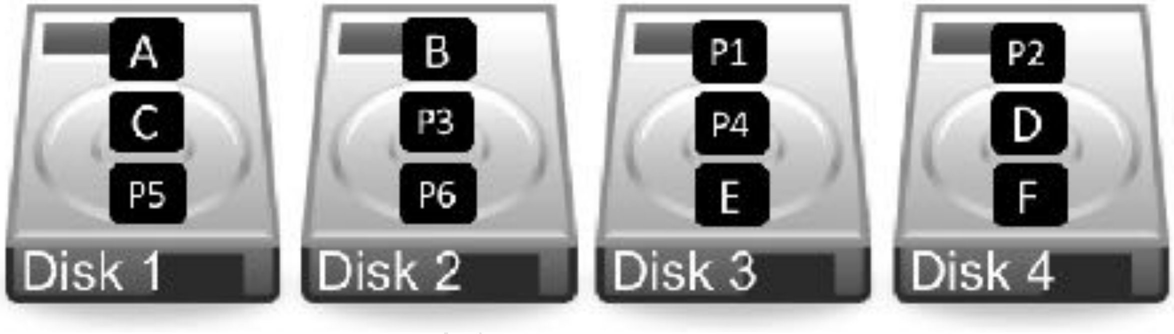


Figure 5: RAID 6 – Multiple drives with double parity information

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.

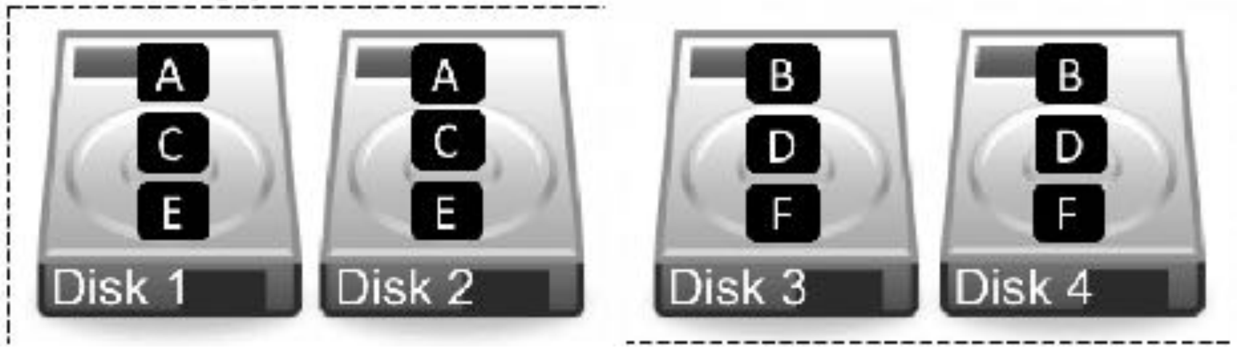


Figure 6: RAID 10 Mirrored and striped drives

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 is a standard feature in Windows Server. It is designed to address three aspects of storage:

Firstly, on a Windows computer each hard drive usually 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 which physical drive or drive letter a file or folder is located upon:

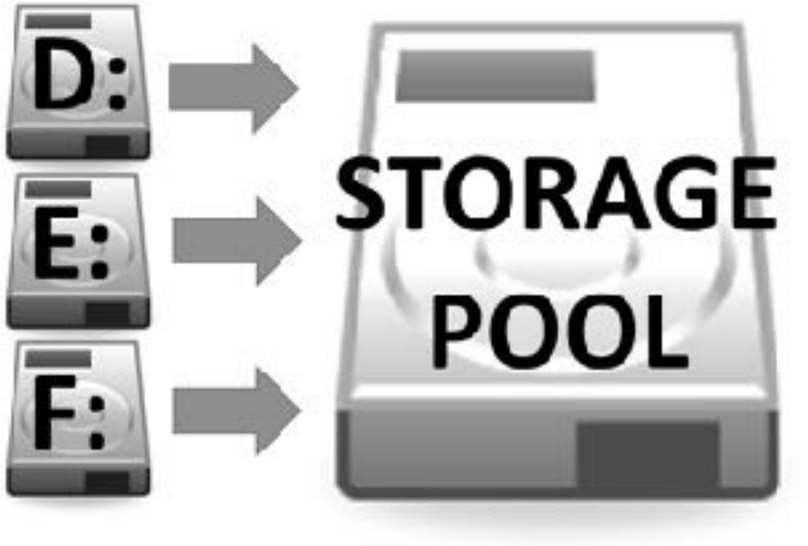


Figure 7: Storage Pool aggregates the hard drives

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. There is a common perception that it is just a low-cost alternative to RAID; in fact, it is an extremely sophisticated feature and with additional capabilities of particular interest to corporate users, although in this example we will stick to the basics as more applicable to a small network.

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.

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 still 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 and 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.

1.5 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 when possible, as performance is better than wireless
- Wired connections should be at least Gigabit speed. 10 Gigabit Ethernet (10GbE) is becoming more affordable and is better for linking the server to network switches and to desktop computers equipped with suitable network cards
- Wireless connections should be to 802.11ac or 802.11n standard
- Avoid domestic grade equipment. Spending more on professional or prosumer ("professional consumer") routers and switches should give better performance and reliability

1.6 Client Devices

By *client devices*, we mean desktop computers, laptop computers, tablets and smartphones. To connect to a Windows Server-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 Windows Server 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.

1.7 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 Windows Server 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 Windows Server 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	Internet router/gateway (static)
192.168.1.2	File server (static)
192.168.1.3-192.168.1.20	Use for printers and any special devices (static)
192.168.1.50-192.168.1.250	Use for computers, tablets, smartphones (dynamic)

One implication of the above is that the network has a maximum of 255 devices in it, although this will be sufficient for a small organization. In larger networks with multiple servers, dozens of printers and maybe thousands of users, a more sophisticated scheme would be required, necessitating the use of *subnets*. This takes it outside the scope of this guide, but a more detailed explanation can be found online at:

https://en.wikipedia.org/wiki/Subnetwork

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.nnn rather than something like, say, 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

2. BASIC INSTALLATION AND CONFIGURATION

2.1 Overview

Setting up a Windows 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 takes around 30-45 minutes and is the topic of this chapter.

2.2 Installing Windows Server

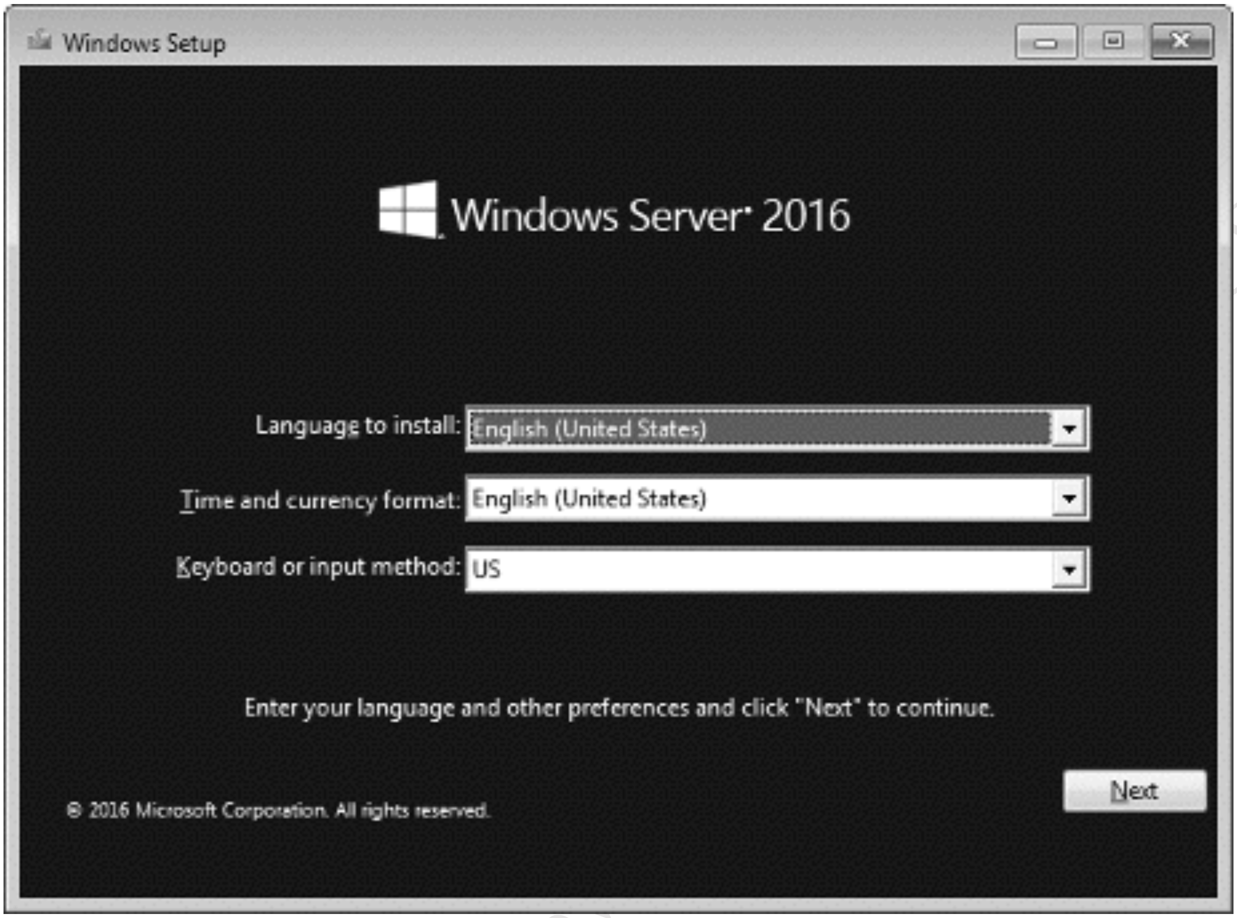
There are several techniques by which Windows Server can be physically installed onto the server. Read the descriptions below and choose the one which is most applicable to you:

Method 1: Windows Server has been supplied on a DVD or USB. Go into the BIOS of the server and set it to boot from DVD or USB as appropriate. Accessing the BIOS varies according to the server brand but is typically the F2 key on Dell and the F10 key on HP, for instance. Insert the DVD, connect an Ethernet cable to the main or only network adapter on 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, connect an Ethernet cable to the main or only network adapter on the server and restart it. The management software will run – this may take several minutes – but eventually you will be prompted to eject the disk and insert the main Windows Server DVD. The server may then restart.

Method 3: Windows Server has been purchased pre-loaded on the server (less common). This does not mean that it is ready to use, just that what normally comes on the distribution DVD or download has already been copied to the server's hard drive, so the installation process can run from that. Connect an Ethernet cable to the main or only network adapter on the server and start it.

Regardless of which method is being used, after a short while the following screen is displayed. Check the regional settings, make any changes as required and click **Next**:



Windows Setup

Windows Server 2016

Language to install: English (United States)

Time and currency format: English (United States)

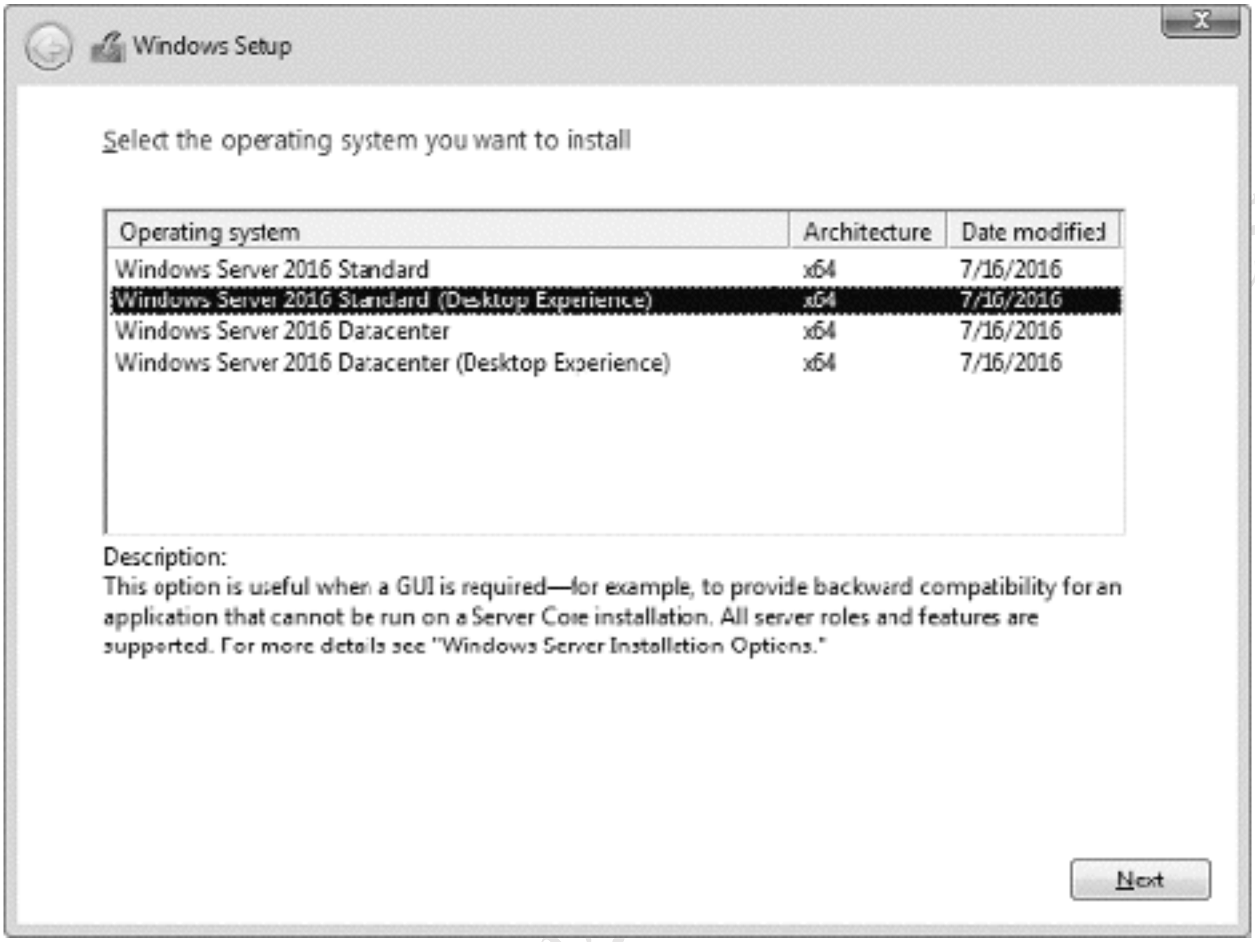
Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

© 2016 Microsoft Corporation. All rights reserved.

Figure 8: Specify regional settings

On the following screen click the **Install now** button. Depending on the edition, you may receive a choice of what to install and if so, you want the option with *Desktop Experience*. With this, Windows Server will look like a regular version of Windows complete with Desktop, icons, Start menu and so on. With the other option the Windows graphical user interface ('GUI') is not installed and the server is more like an appliance or black box; this mode is more suitable for organizations that have many servers, used for specific roles rather than general purpose networking. So, choose **Windows Server 2016 Standard (Desktop Experience)** and click **Next**:



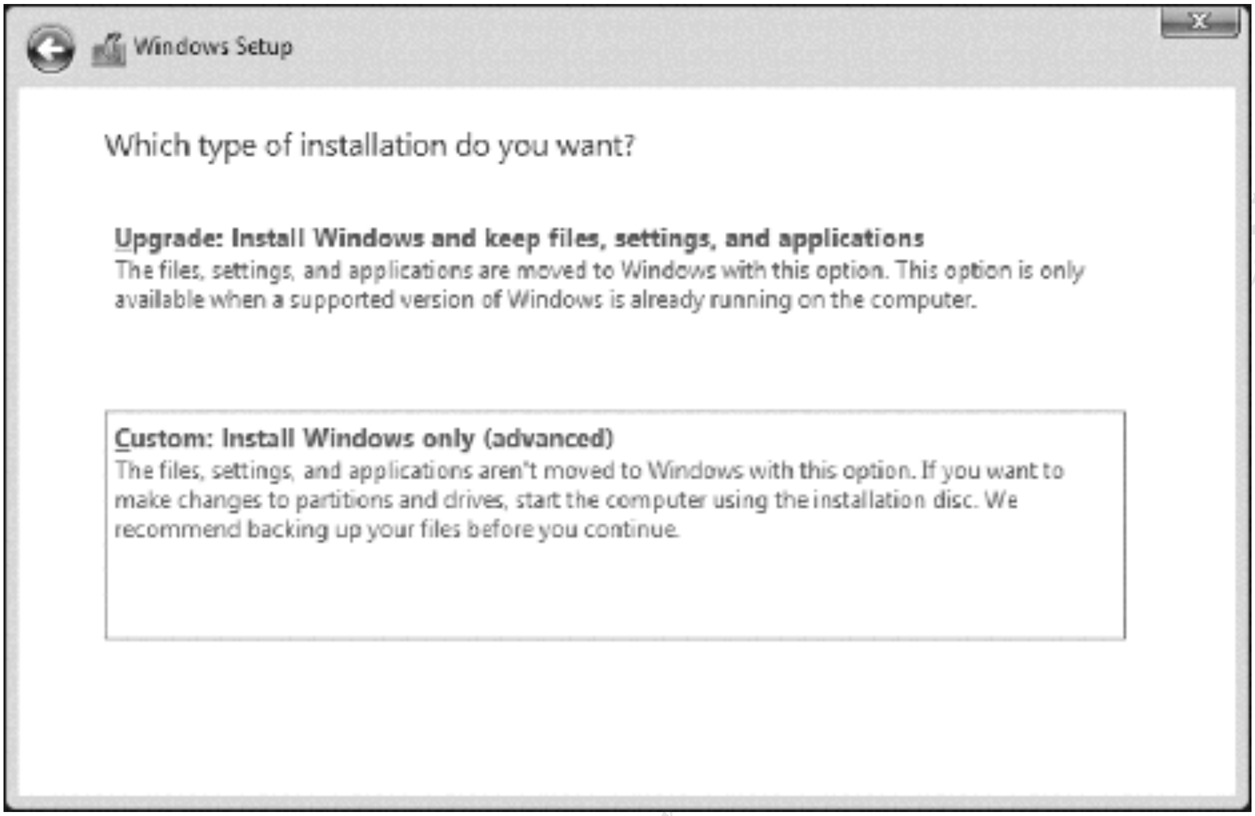
Select the operating system you want to install

Operating system	Architecture	Date modified
Windows Server 2016 Standard	x64	7/16/2016
Windows Server 2016 Standard (Desktop Experience)	x64	7/16/2016
Windows Server 2016 Datacenter	x64	7/16/2016
Windows Server 2016 Datacenter (Desktop Experience)	x64	7/16/2016

Description:
This option is useful when a GUI is required—for example, to provide backward compatibility for an application that cannot be run on a Server Core installation. All server roles and features are supported. For more details see "Windows Server Installation Options."

Figure 9: Select the operating system to install

Tick the **I accept the license terms** box on the following screen and click **Next**. On the subsequent screen choose **Custom: Install Windows only (advanced)**:



Windows Setup

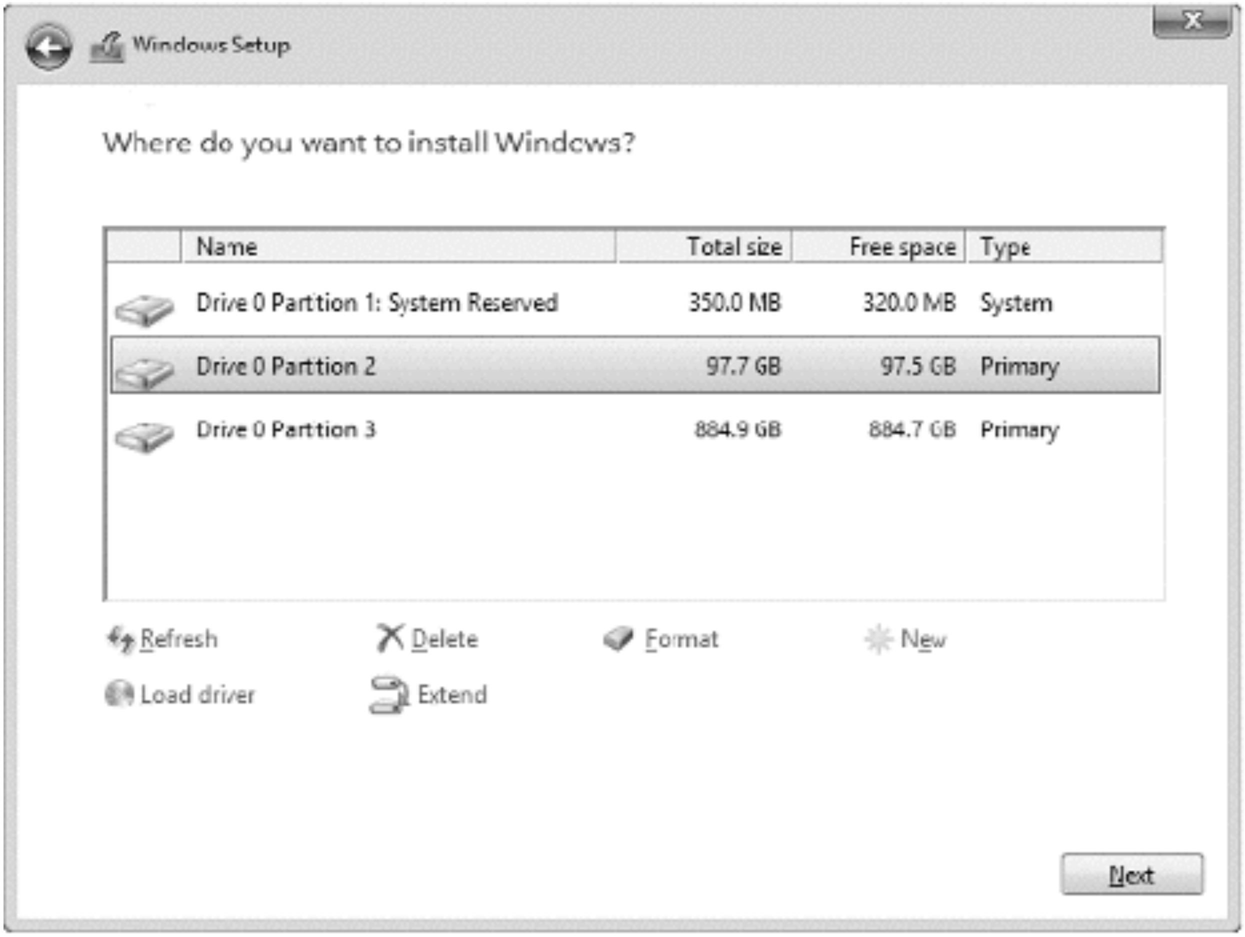
Which type of installation do you want?

Upgrade: Install Windows and keep files, settings, and applications
The files, settings, and applications are moved to Windows with this option. This option is only available when a supported version of Windows is already running on the computer.

Custom: Install Windows only (advanced)
The files, settings, and applications aren't moved to Windows with this option. If you want to make changes to partitions and drives, start the computer using the installation disc. We recommend backing up your files before you continue.

Figure 10: Choose 'Custom Install'

A decision has to be made about where to install Windows Server and the options available will depend on what drives are in the server and how they are configured. On a very small system there may only be one drive. A larger system might have two drives; typically, Windows would be installed on the smaller one and the larger one would be used for data. On a RAID system the drives will appear as a single volume (unless, perhaps, the installation was started from a manufacturer's management CD/DVD as described at the beginning of this chapter). Do not try to use the 'System Reserved' partition. The Windows drive should be at least 60 GB in size but larger is better. In this example, the server has 1 TB storage, divided into one partition of about 100 GB and one of about 900 GB. We will therefore use the former. **Very important:** make sure the drives/partitions are formatted before proceeding, then click **Next**:

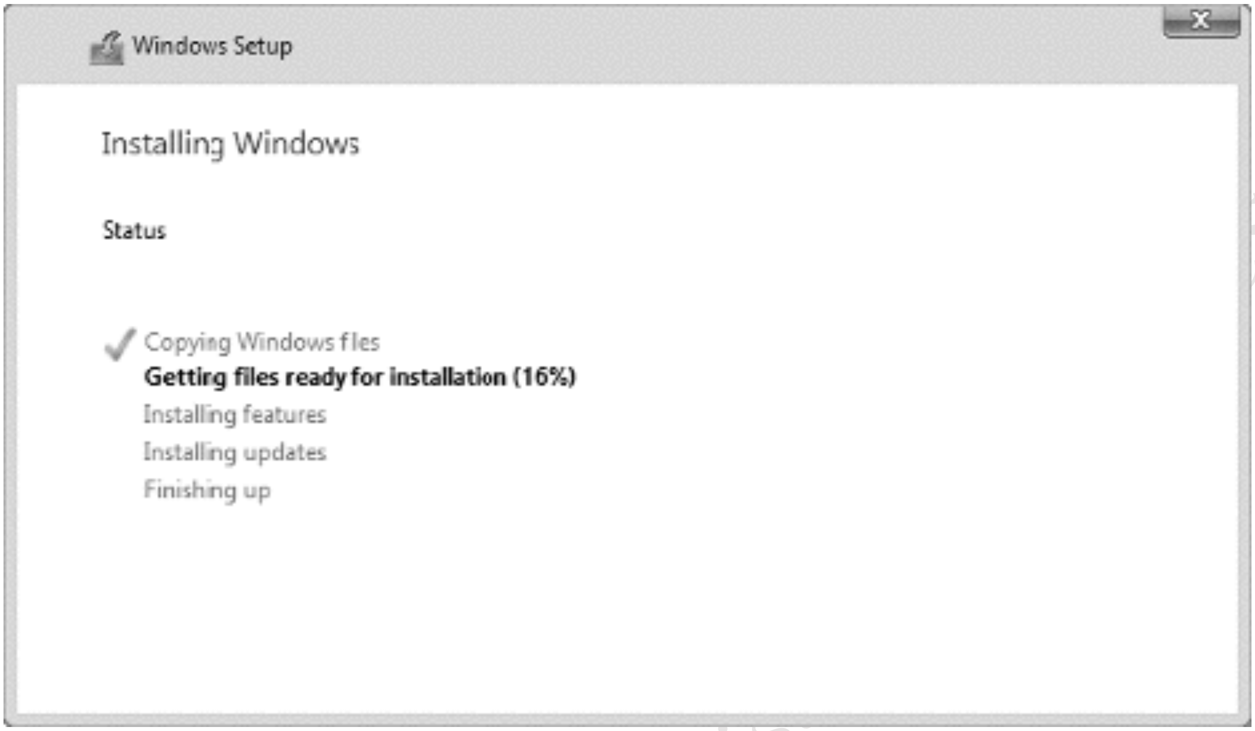


Where do you want to install Windcws?

	Name	Total size	Free space	Type
	Drive 0 Partition 1: System Reserved	350.0 MB	320.0 MB	System
	Drive 0 Partition 2	97.7 GB	97.5 GB	Primary
	Drive 0 Partition 3	884.9 GB	884.7 GB	Primary

Figure 11: Choose the installation partition

The next phase typically runs for around 10-15 minutes, during which the server may restart several times:



Installing Windows

Status

✓ Copying Windows files

Getting files ready for installation (16%)

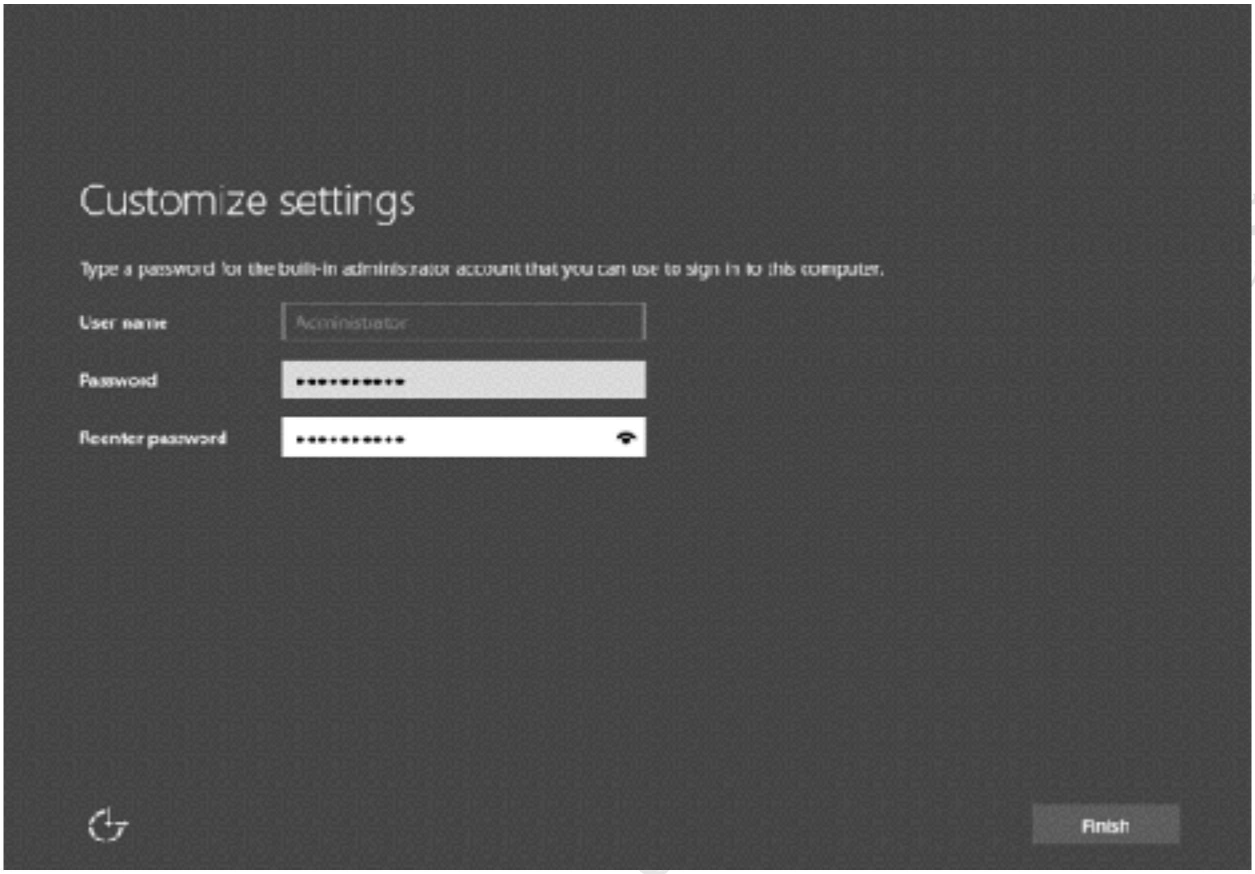
Installing features

Installing updates

Finishing up

Figure 12: Installation progress screen

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**.



Customize settings

Type a password for the built-in administrator account that you can use to sign in to this computer.

User name: Administrator

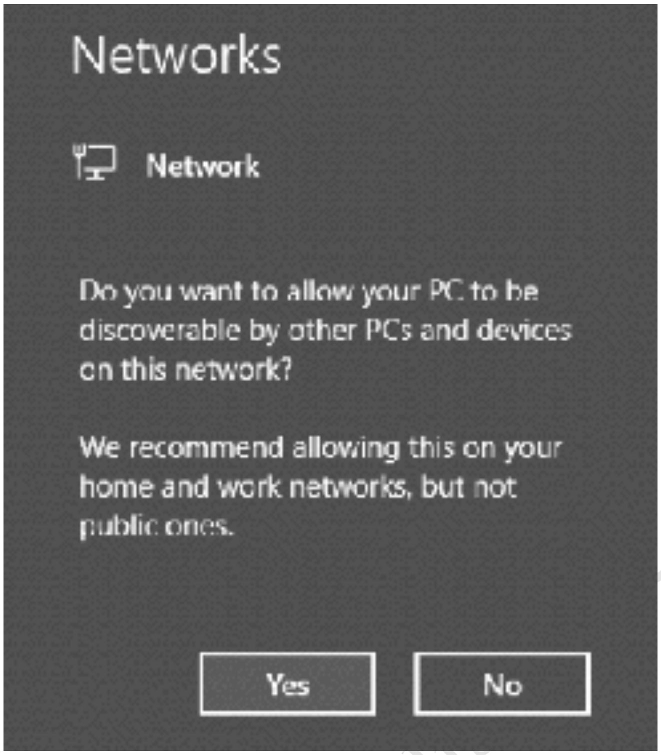
Password: •••••••••••

Reenter password: •••••••••••

Figure 13: Specify a password for Administrator

After several seconds, you will be able to login. Press **Ctrl+Alt-Delete** and enter the password for *Administrator* that you created.

Following the first login, a message is displayed on the right-hand side of the screen asking whether the server 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:



Networks

Network

Do you want to allow your PC to be discoverable by other PCs and devices on this network?

We recommend allowing this on your home and work networks, but not public ones.

Figure 14: Networks notification screen

After a minute or so the screen will clear to show *Server Manager*, which is used for configuring and managing servers. In some respects, it behaves like a web site – notice the backwards and forwards buttons in the top-left hand corner, along with the refresh icon on the right-hand side. If you have used earlier versions of Windows Server then you should try and use Server Manager wherever possible, although the older methods of doing things, for the most part, still work.

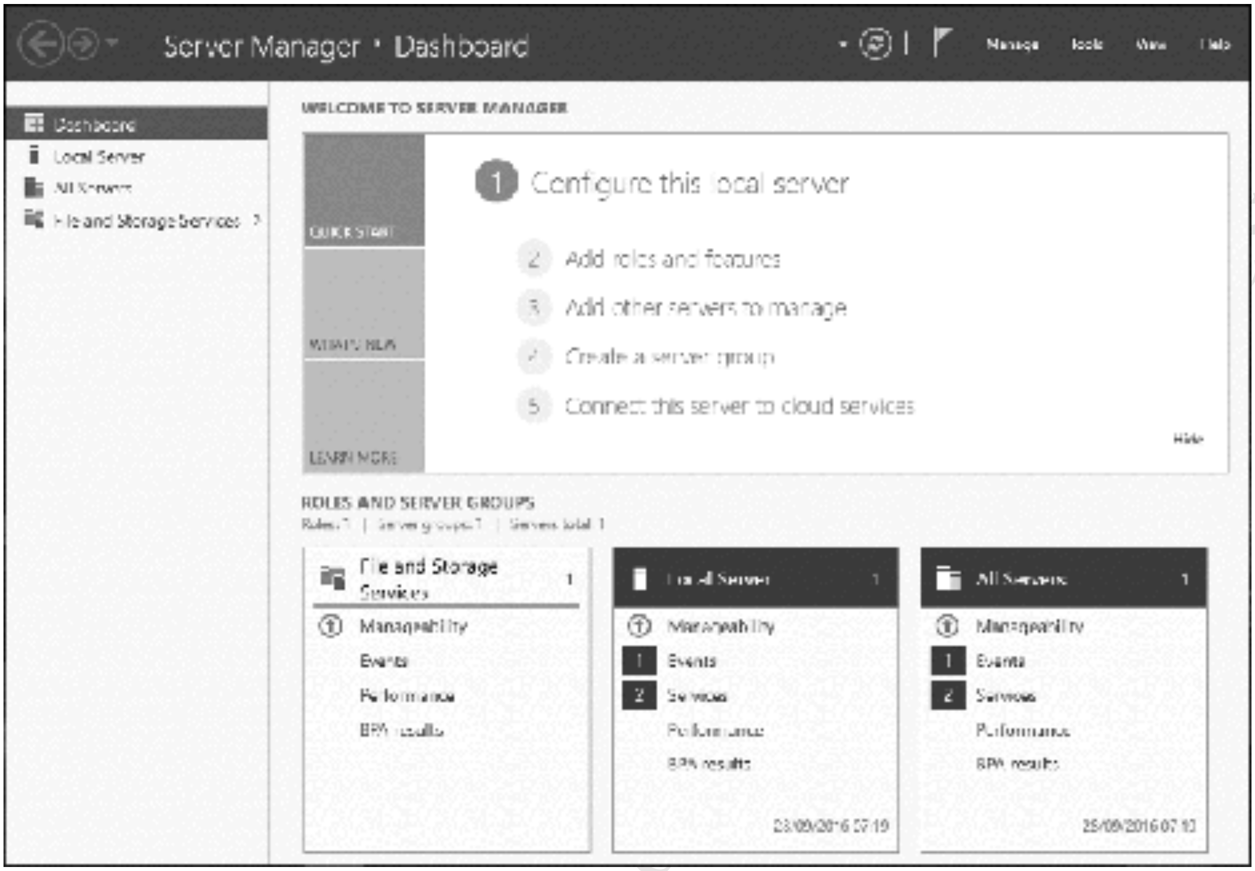


Figure 15: Server Manager Dashboard

The first step is to configure networking. On the left-hand panel, click where it reads **Local Server** and the screen will change thus:

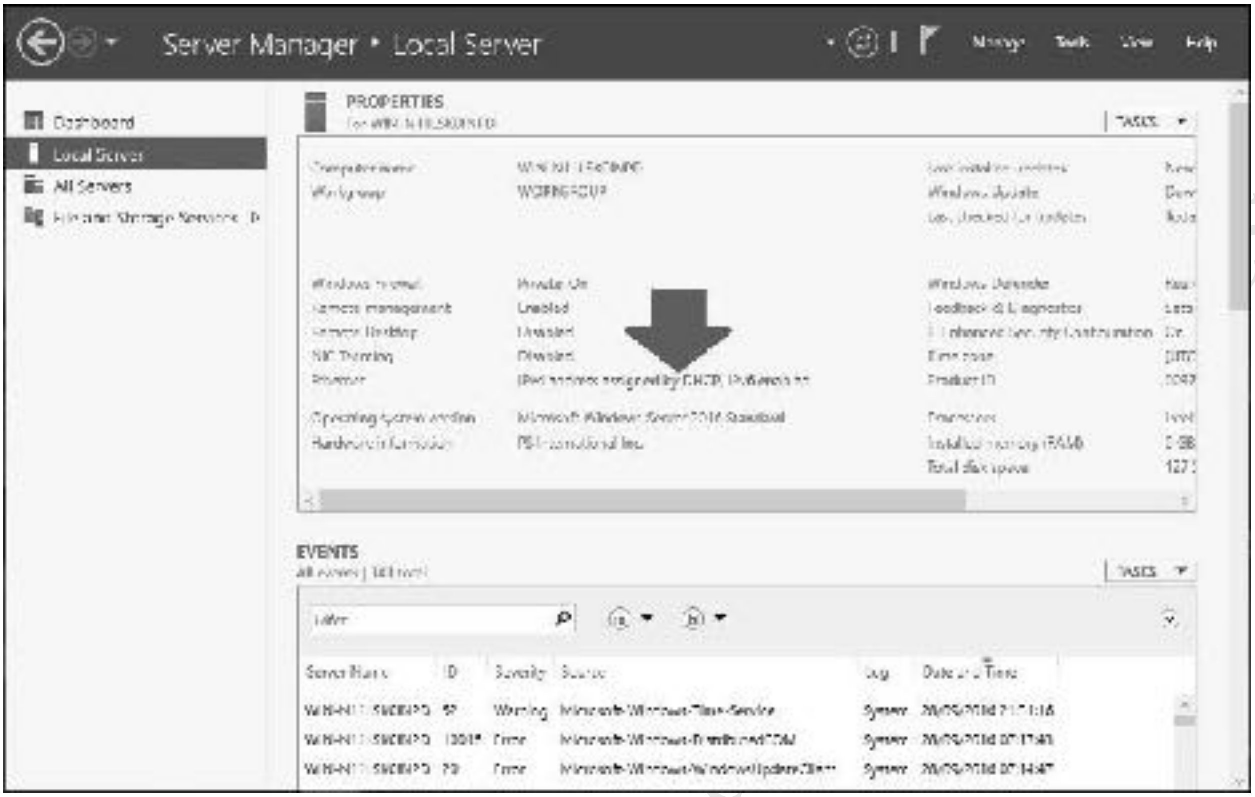
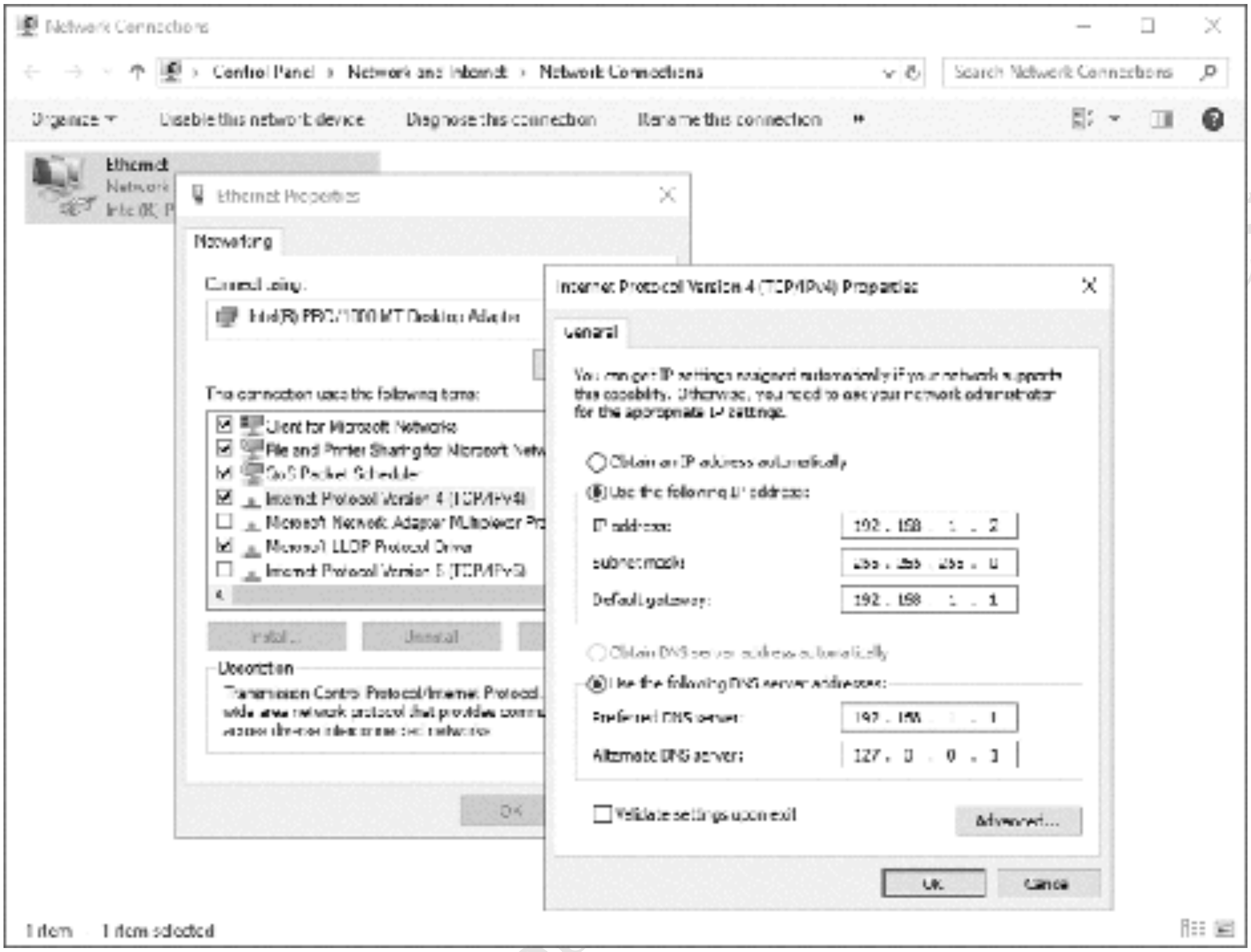


Figure 16: Local Server Properties panel within Server Manager

On the center panel, look for where it says *Ethernet*. Click **IPv4 address assigned by DHCP, IPv6 enabled** and the network adapter(s) will be shown; there may only be one on a small server, but if there is more than one then choose the one that is connected. Further information about using multiple adapters can be found in 12.9 Multiple Network Adapters (NIC Teaming) but it is suggested you do not pursue this until the server is up and running. Right-click the adapter and choose **Properties**. On the resultant panel highlight **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. At present, the adapter will be set to *Obtain an IP address automatically* – change it to *Use the following IP address*. The actual address to use depends upon the IP scheme in use; in our example, we are using a 192.168.nnn.nnn addressing scheme with the router on 192.168.1.1. The server should be given an adjacent address, such as 192.168.1.2. The **Default gateway** is the address of the router; the **Subnet mask** should be 255.255.255.0, the **Preferred DNS server** is the same as the default gateway/router and the **Alternate DNS server** should be 127.0.0.1 (known as the *local loopback address*). Make the changes and click **OK**, followed by **Close** on the subsequent screen:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1

Alternate DNS server: 127 . 0 . 0 . 1

□ Validate settings upon exit

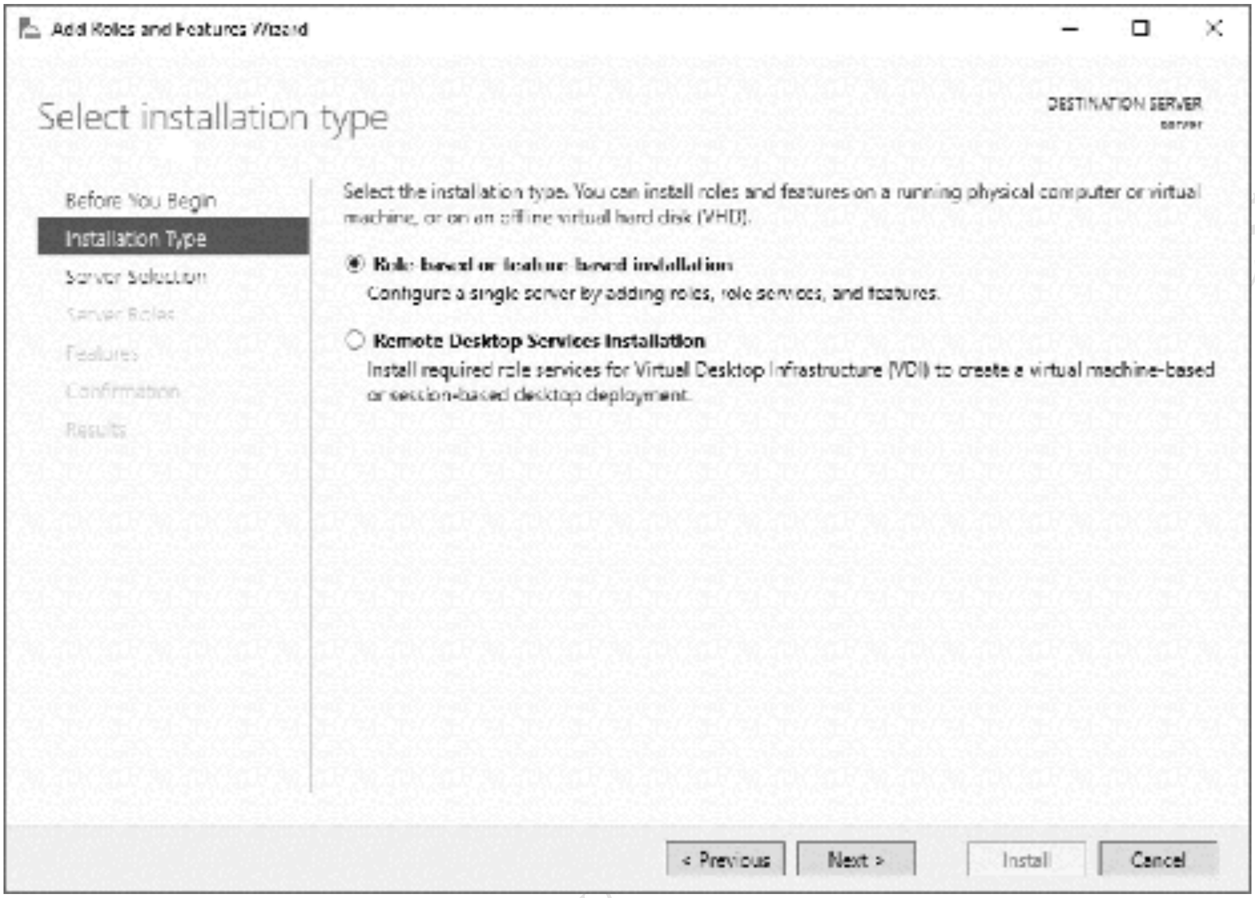
Network Connections
Control Panel › Network and Internet › Network Connections
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
Ethernet
Ethernet Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Desktop Adapter
This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Netw
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Pr
☑ Microsoft LLDP Protocol Driver
□ Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Description
Transmission Control Protocol/Internet Protocol. wide area network protocol that provides comm across diverse interconnected networks.
OK
Advanced...
OK
Cancel
1 item
1 item selected

Figure 17: Specifying the IP address for the server

Close the Network Connections window to return to the main Server Manager (Local server) screen. On the center panel, look for where it reads *Computer name*. Click the value, which will currently be something random (e.g. WIN-AHDU1541FOP) and the *System Properties* panel will be displayed. Click the **Change** button on the **Computer Name** tab and change the C*omputer name* to something more meaningful. In a small network with a single server you can simply call it *server*, but in a larger network there will need to be a convention for naming the servers. This could be along the lines of *server01*, *server02*, *server03* and so on, or could be based on location (*newyork*, *london*, *delhi* etc.) or function (*accounts*, *sales*, *marketing* etc). Click **OK** and there will be a message advising that the server needs to be restarted. Click **OK** followed by **Close** and then click the **Restart Now** button.

After the server has restarted, login as *Administrator* and you will be returned to the Server Manager screen. Before continuing, one optional thing to consider is labelling the disk volumes to reflect their roles. For instance, on a two-drive server the C: drive could be labelled *System* and the D: drive labelled *Data*. To do this, launch *File Explorer*, which has an icon on the Taskbar. Expand *This PC*, right-click each drive in turn and choose **Rename** from the pop-up menu.

Returning to the Server Manager screen, click **Manage** followed by **Add roles and features**. The initial screen lists some pre-requisites but is not important, so tick the **Skip this page by default box** and click **Next**. On the subsequent screen choose **Role-based or feature-based installation** followed by **Next**:



Select installation type

DESTINATION SERVER
server

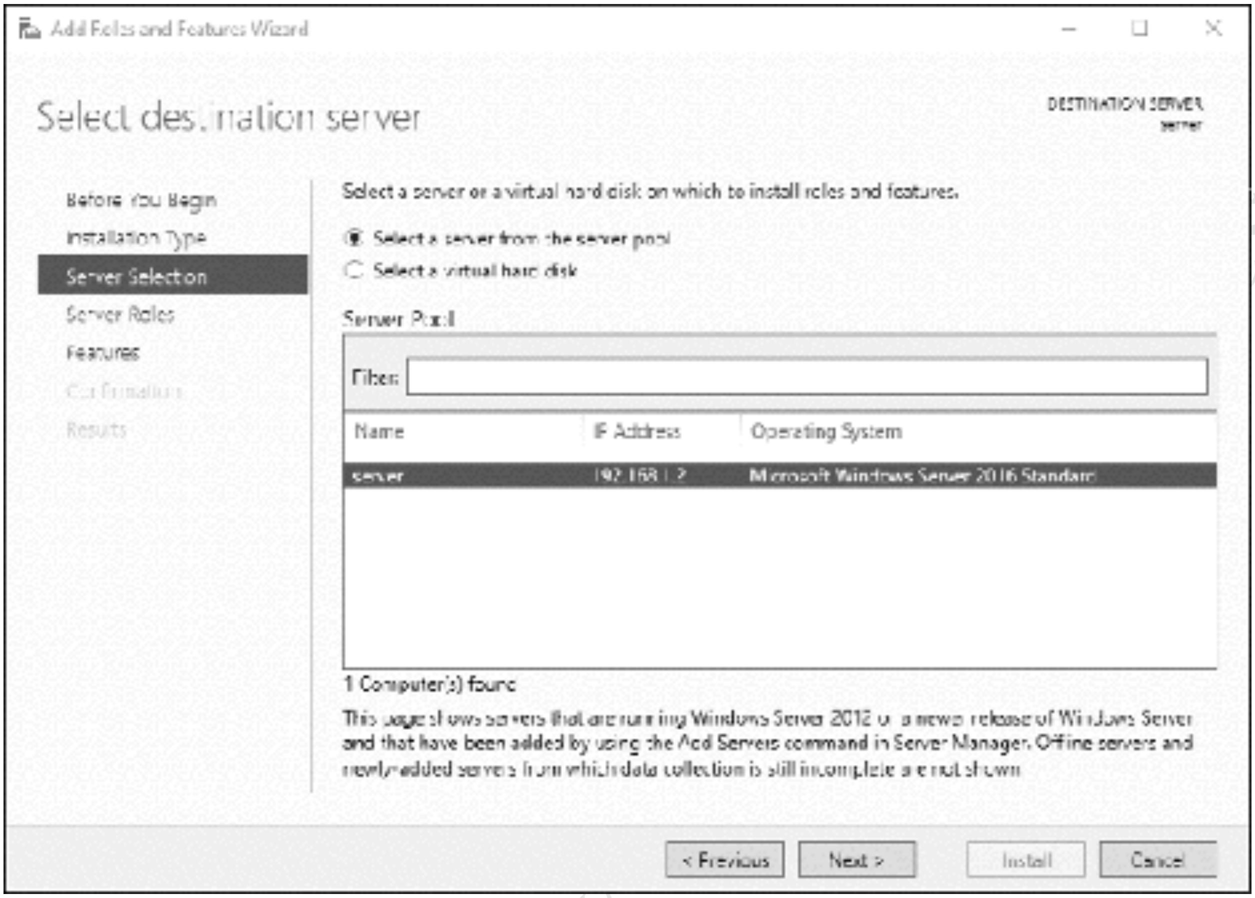
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.

○ Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Figure 18: Add Roles and Features Wizard

On the following screen only one server should be listed - the one you are working on – although in a large organization with existing servers others may also be listed. Click **Next** to continue:



Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool

○ Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
server	192.168.1.2	Microsoft Windows Server 2016 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Figure 19: Select the destination server

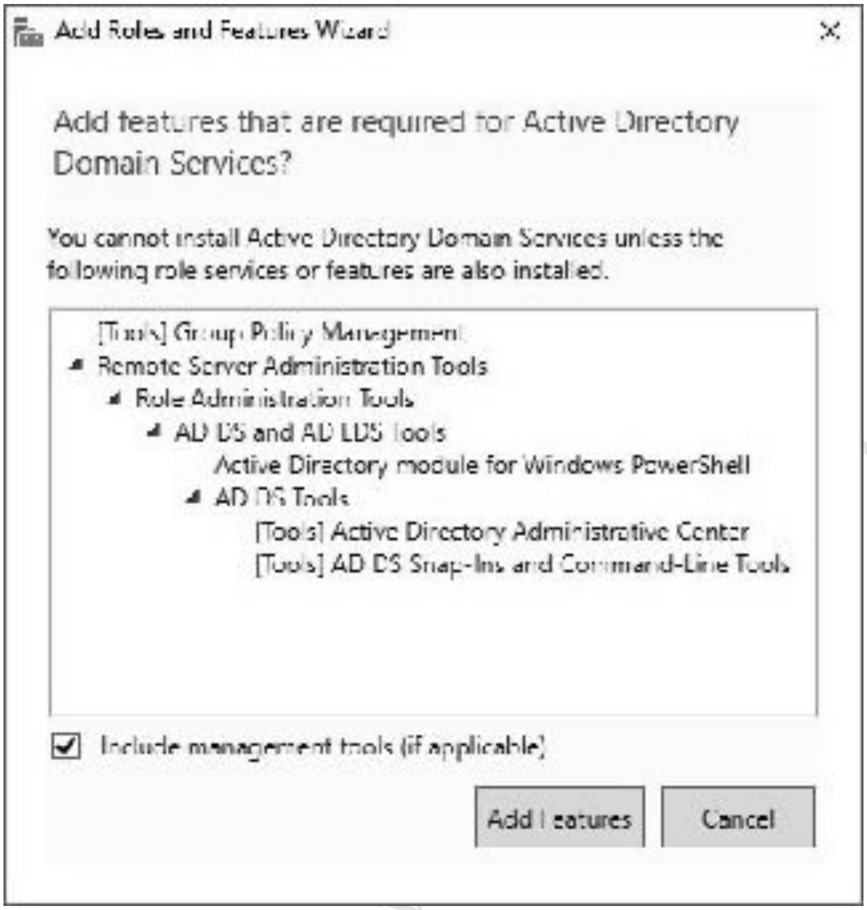
There are over 20 roles listed on the following screen. The ones that should be installed depend upon the role of the server, for instance in a network with multiple servers the different roles can be shared out for reasons of performance and resilience. In our example, there is a single server that will run everything required in a typical installation for a small organization. Accordingly, only the following roles need to be installed: *Active Directory Domain Services*; *DHCP Server*; *DNS Server*; *File and Storage Services* (which will in fact already be installed at this stage). These services do the following things:

Active Directory Domain Services maintains details of all the objects (computers, printers, users and so on) in the network and handles security and logons. For a more detailed explanation look at this article: http://en.wikipedia.org/wiki/Active_Directory.

DHCP Server provides and manages IP addresses for devices on the network. For a more detailed explanation look at this article: https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

DNS Server translates between names - which human beings prefer - and IP numbers - which computers prefer. For a more detailed explanation look at this article: https://en.wikipedia.org/wiki/Domain_Name_System

Start by clicking on **Active Directory Domain Services**. The following panel immediately appears; the defaults are generally fine so just click the **Add Features** button:



Add Roles and Features Wizard

Add features that are required for Active Directory Domain Services?

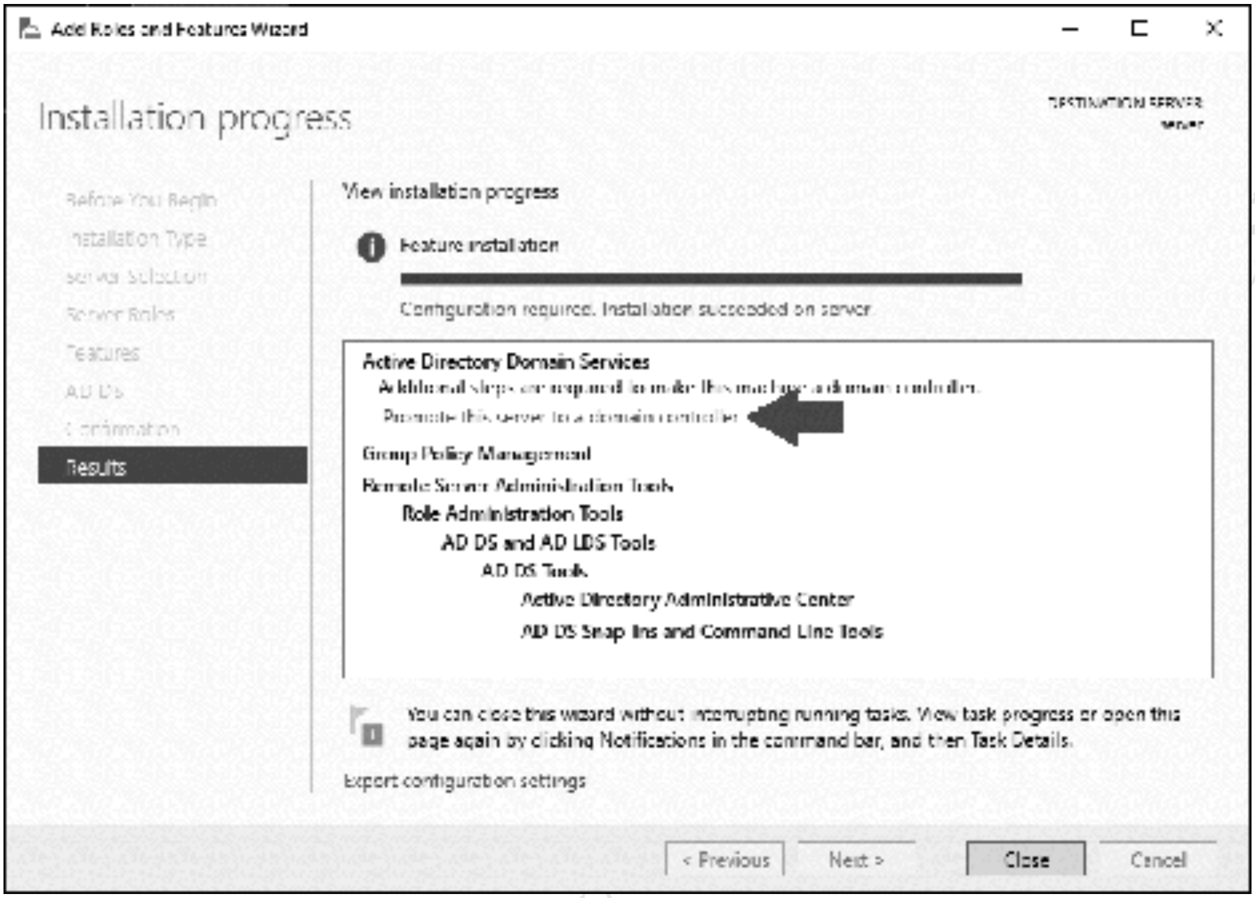
You cannot install Active Directory Domain Services unless the following role services or features are also installed.

```
   [Tools] Group Policy Management
 ◢ Remote Server Administration Tools
     ◢ Role Administration Tools
         ◢ AD DS and AD LDS Tools
             Active Directory module for Windows PowerShell
           ◢ AD DS Tools
                 [Tools] Active Directory Administrative Center
                 [Tools] AD DS Snap-Ins and Command-Line Tools
```

☑ Include management tools (if applicable)

Figure 20: Prompt about adding features

You will be returned to the previous screen – click **Next** and **Next** and **Next.** Tick the **Restart the destination server automatically if required box**, acknowledge the message and click **Install**. It will take several minutes to install Active Directory, during which time an Installation progress screen will be shown. When installation is complete, click **Close**.



View installation progress

Feature installation

Configuration required. Installation succeeded on server.

Active Directory Domain Services

Additional steps are required to make this machine a domain controller.

Promote this server to a domain controller

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

AD DS Tools

Active Directory Administrative Center

AD DS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Figure 21: Installation complete

Having installed Active Directory Domain Services, the next stage is to ‘promote’ the server to be the *Domain Controller*. If you have used earlier versions of Windows Server such as 2003 or 2008 you may be familiar with the *DCPROMO* command, which was once used to do this. This does not exist in recent versions of Windows Server; instead, promotion is done from the Server Manager screen. Looking at Server Manager, there will now be a new entry on the left-hand panel, marked *AD DS*:

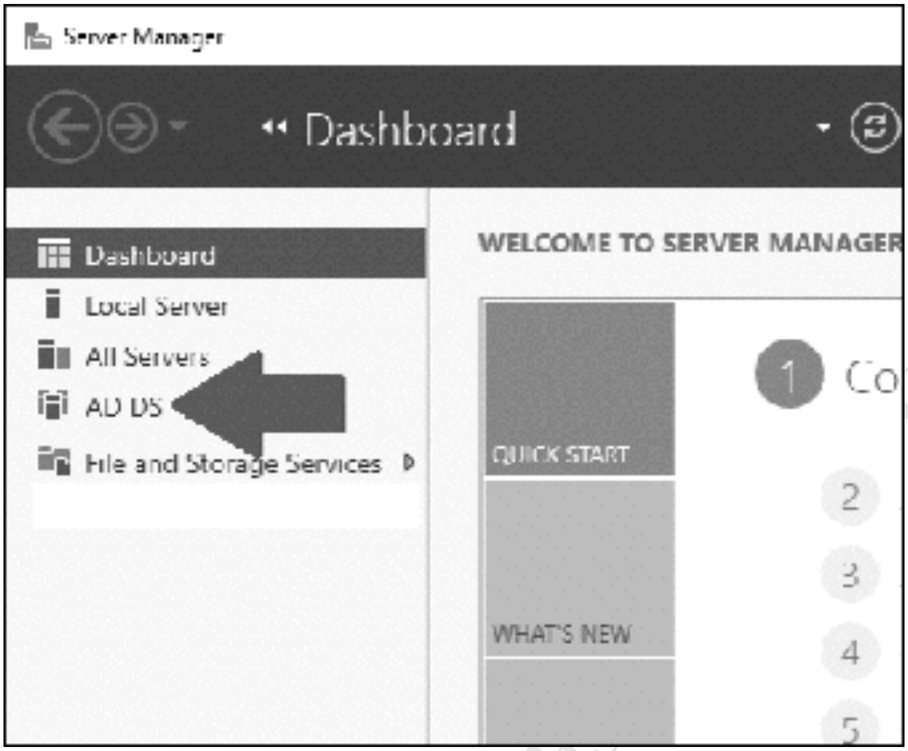
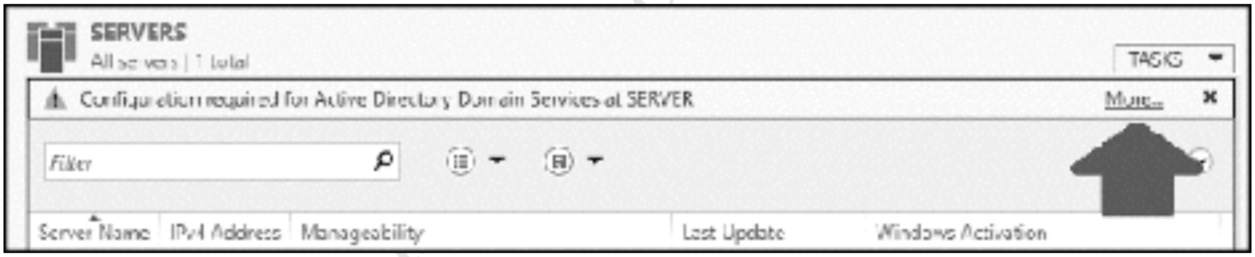


Figure 22: Entry for Active Directory in Server Manager Dashboard

Click on **AD DS**. On the resulting screen is a warning message that further configuration is required:

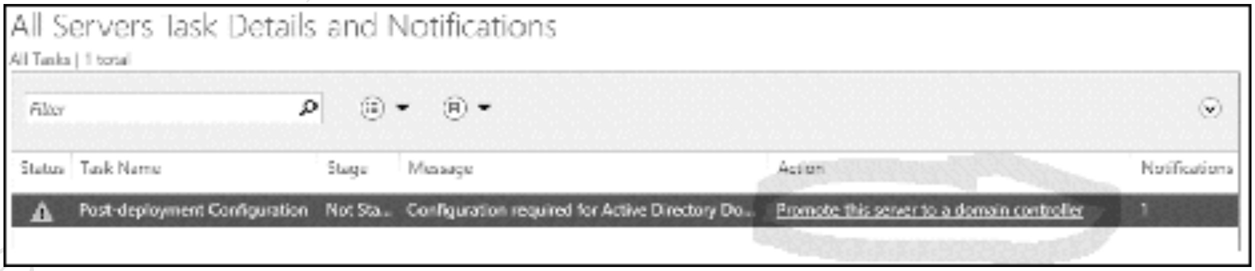


Configuration required for Active Directory Domain Services at SERVER

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation

Figure 23: Message about need for additional configuration

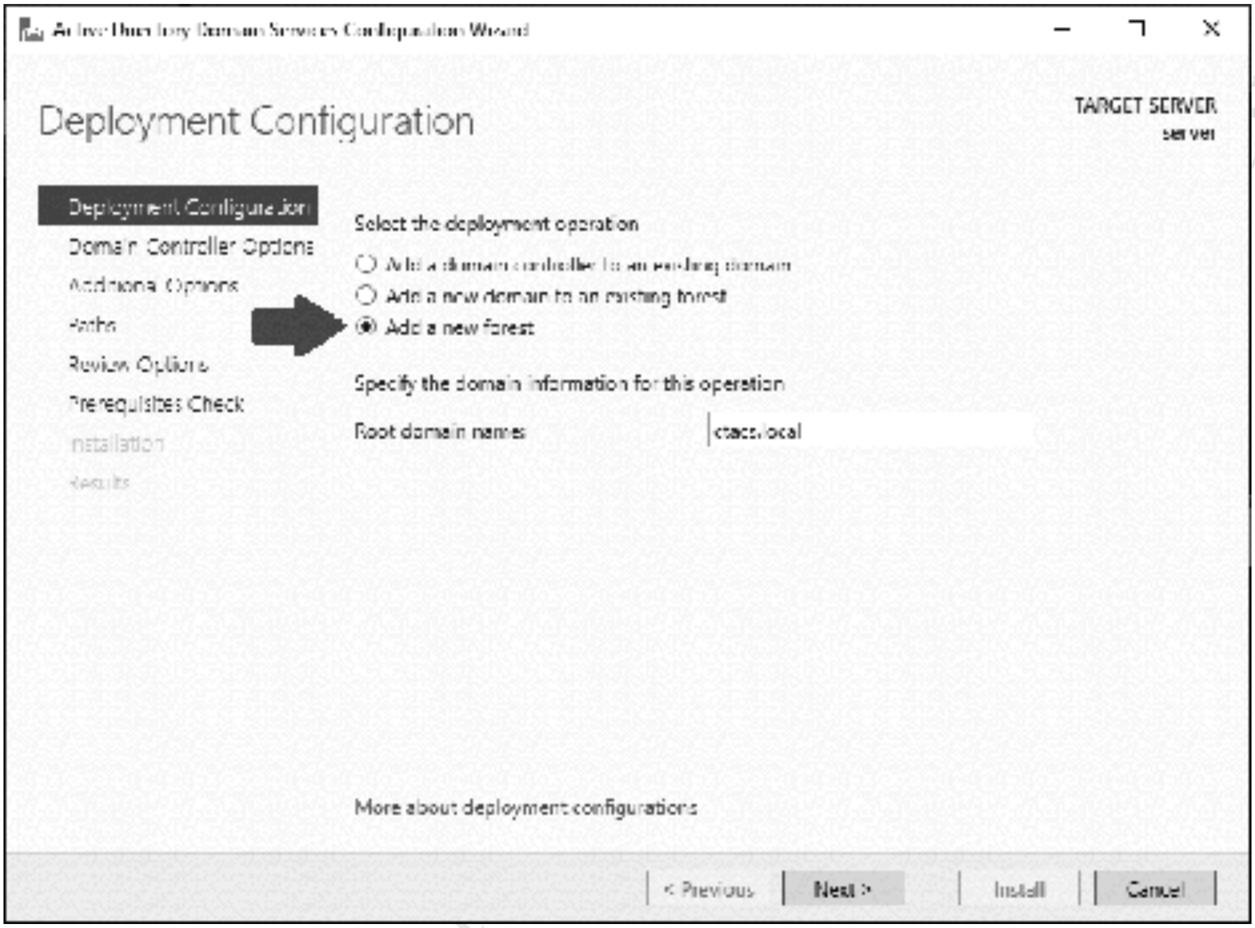
Click where it reads **More…** and an additional panel appears:



Status	Task Name	Stage	Message	Action	Notifications
⚠	Post-deployment Configuration	Not Sta...	Configuration required for Active Directory Do...	Promote this server to a domain controller	1

Figure 24: Promote server to be a domain controller

Click where it reads **Promote this server to a domain controller** and the *Deployment Configuration* panel is displayed. Choose the **Add a new forest** option and specify a **Root domain name**. In large organizations with multiple servers and/or locations, it is common to use the internet domain name prefixed by some other information to identify the separate locations or functions e.g. *london.ctacs.co.uk*, *liverpool.ctacs.co.uk*, *washington.ctacs.co.uk*. In a small organization with a single server the domain name would commonly be the name of the organization with a suffix of *.local* added e.g. *ctacs.local* (people with experience of installing servers may be aware of some debate over the use of *.local* but we will stick with it here). Click **Next**:



Select the deployment operation

○ Add a domain controller to an existing domain

○ Add a new domain to an existing forest

● Add a new forest

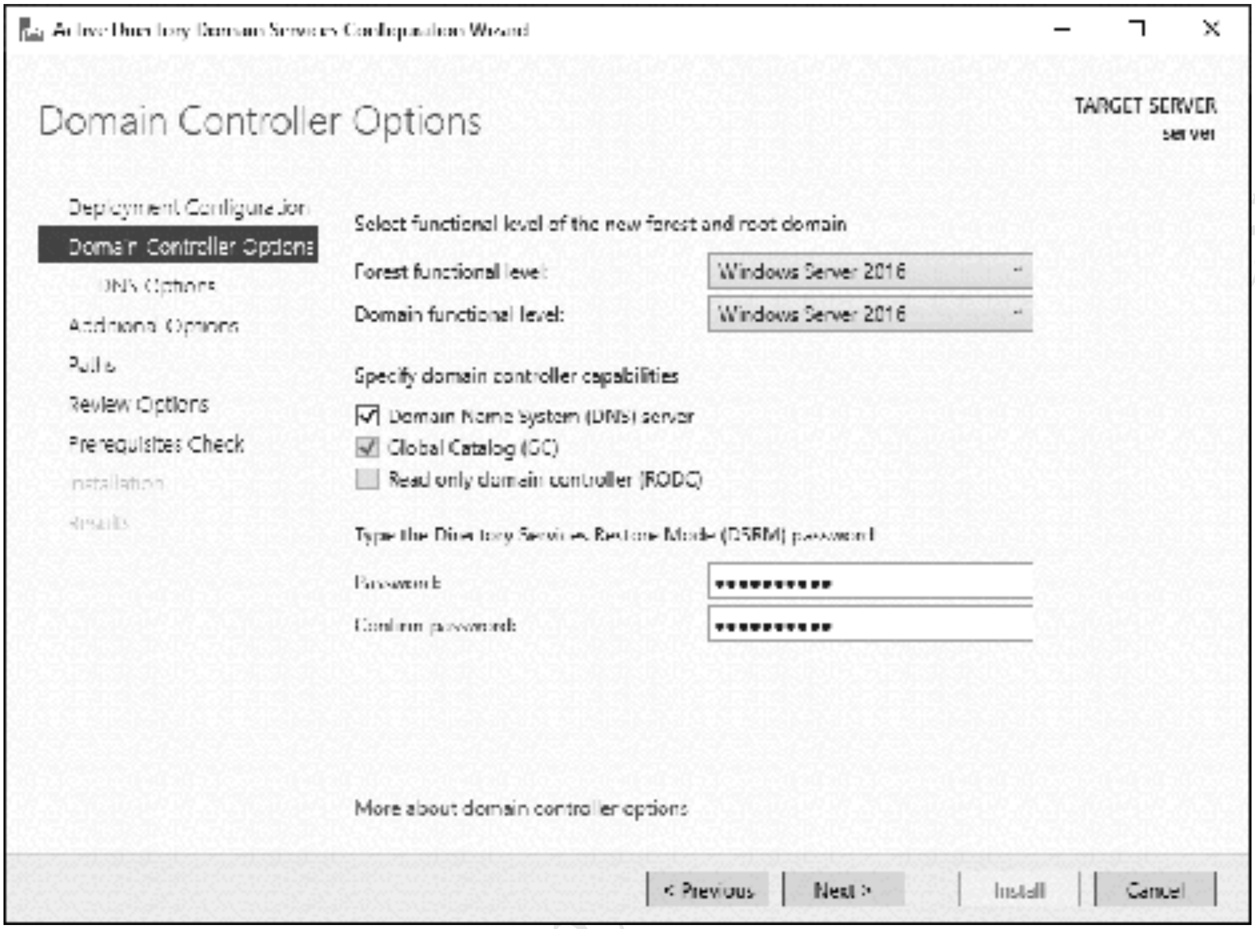
Specify the domain information for this operation

Root domain name: ctacs.local

More about deployment configurations

Figure 25: Specify options for the domain

After a short while the following screen is displayed. The **Forest functional level** and **Domain functional level** should both be set to *Windows Server 2016;* alternative settings are available but would normally only be used if other, older versions of Windows Server were already in place. Leave the **Domain Name System (DNS) server** and **Global Catalog** boxes ticked. A password has to be specified – for convenience, you could use the same one as the Administrator account. Then click **Next**:



Domain Controller Options

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

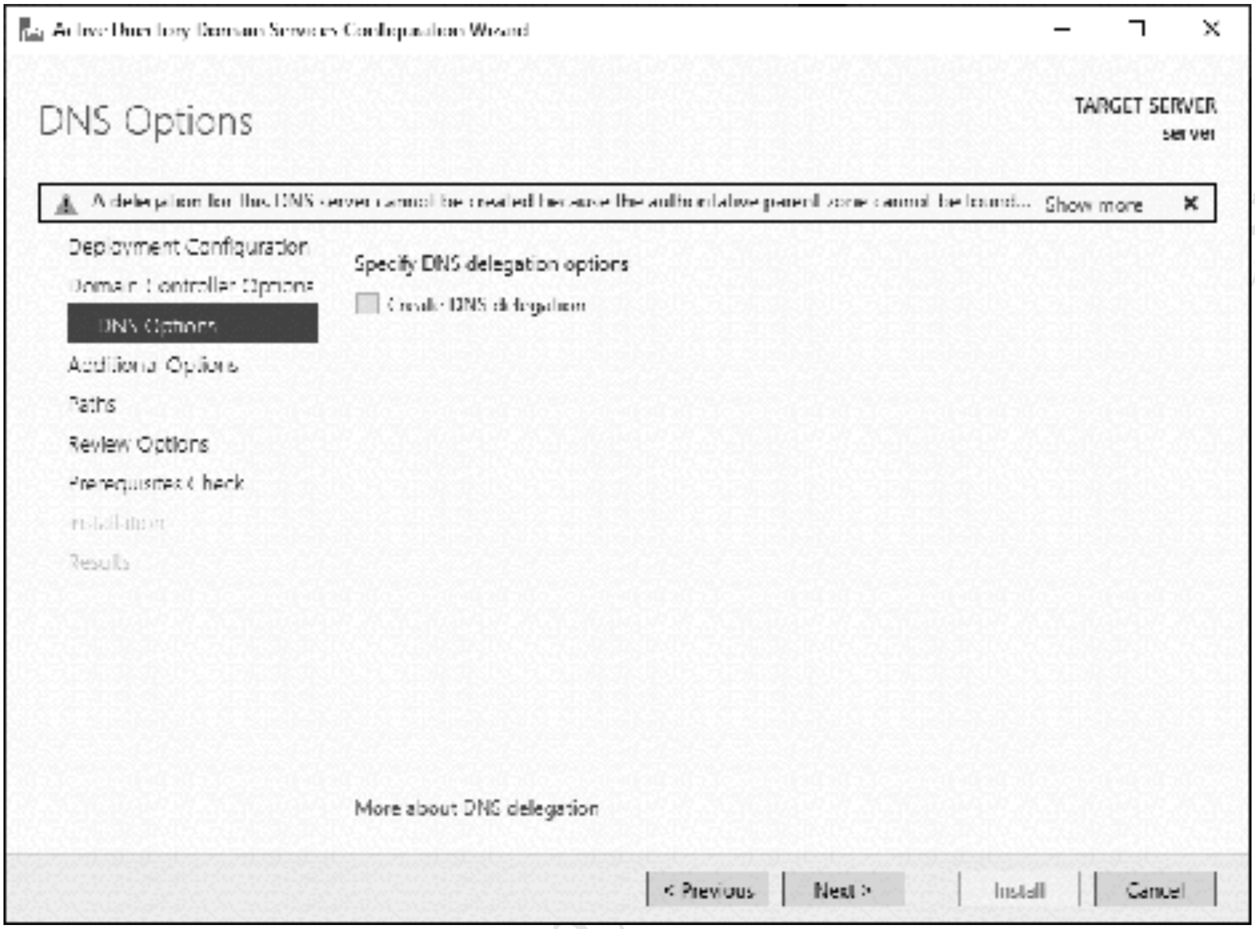
Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●●

More about domain controller options

Figure 26: Options for the domain controller

On the next screen a warning may be displayed relating to DNS; a common cause of this is that you are using an all-in-one internet router that is providing DNS, in which case the message can be ignored for now. Click **Next**:



Active Directory Domain Services Configuration Wizard

DNS Options

TARGET SERVER
server

⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... Show more ✖

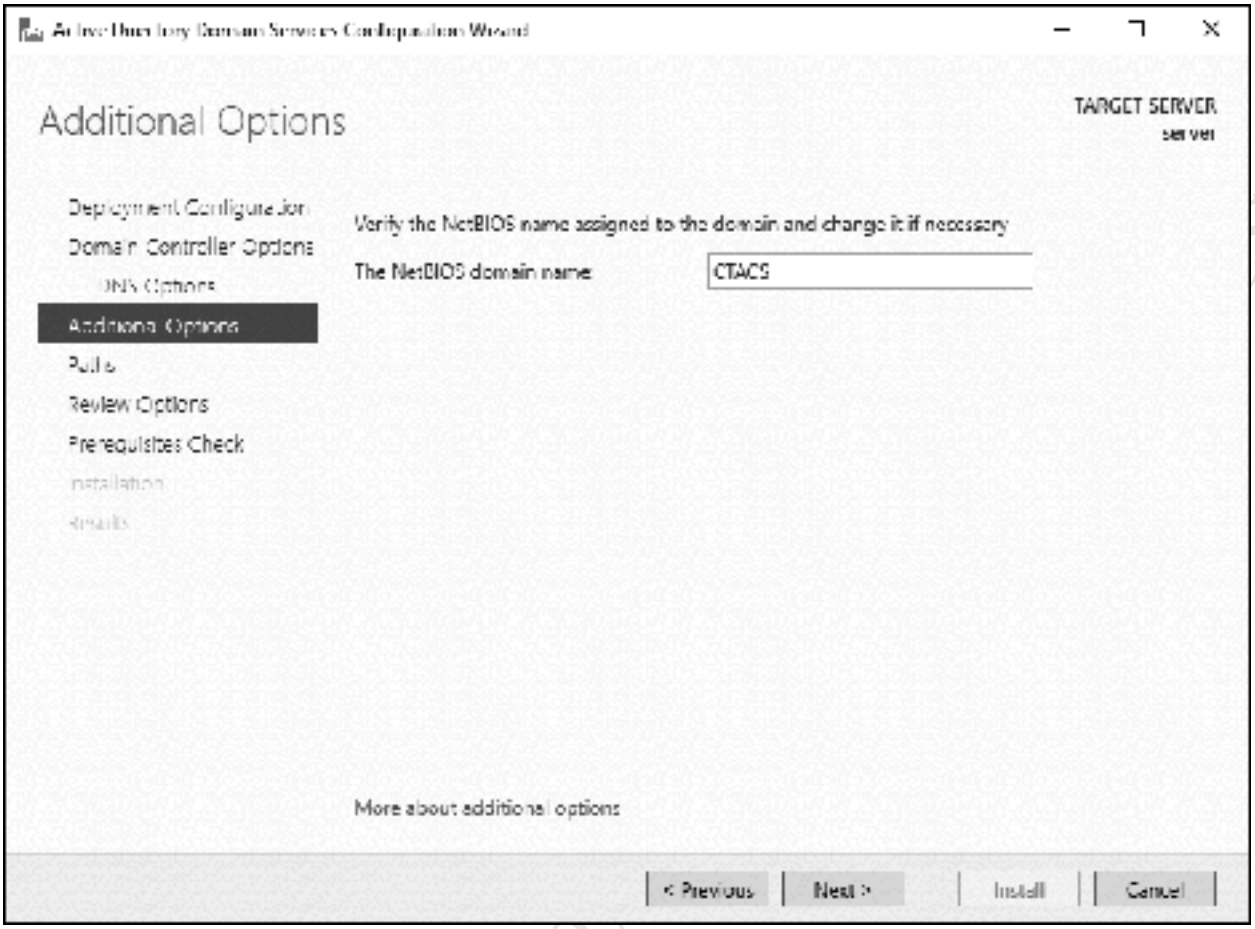
Specify DNS delegation options

□ Create DNS delegation

More about DNS delegation

Figure 27: Message about DNS

The subsequent screen asks you to verify the *NetBIOS* name. This will be the same as the domain name you chose (less the suffix) and usually you just accept it by clicking **Next.** The exception to this would be if it is more than 15 characters in length, in which case you need to abbreviate it:



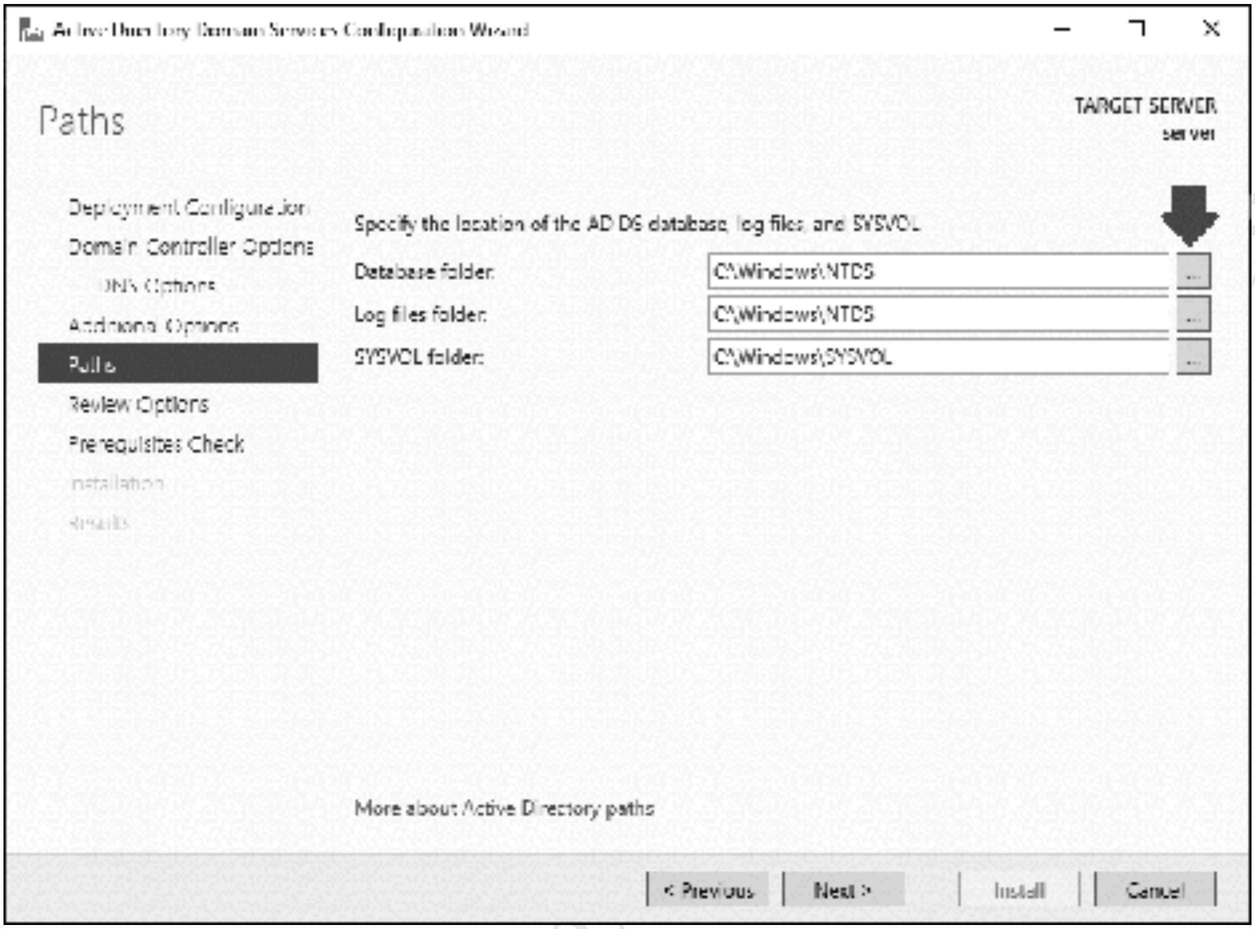
Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: CTACS

More about additional options

Figure 28: NetBIOS domain name

The following screen allows control over the location of the various files and logs associated with Active Directory. On a small system there is no particular need to change this so just click **Next**:



Paths

TARGET SERVER
server

Specify the location of the AD DS database, log files, and SYSVOL

Database folder: C:\Windows\NTDS

Log files folder: C:\Windows\NTDS

SYSVOL folder: C:\Windows\SYSVOL

More about Active Directory paths

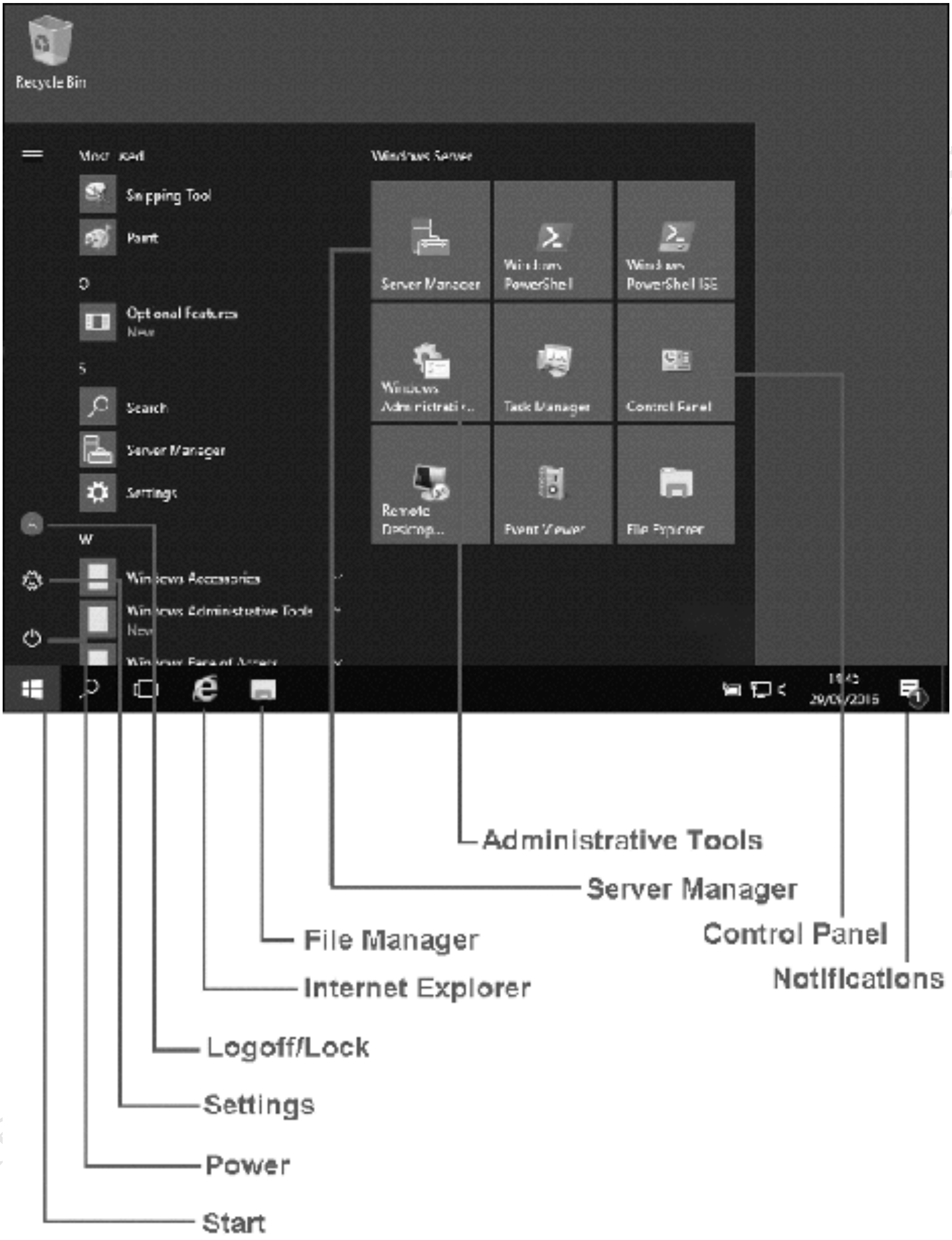
Figure 29: Active Directory paths

The subsequent screen is a summary of the various selections and settings - click **Next**. Windows Server runs a *Prerequisites Check* - this may well generate some warning messages, which can be unsettling, but usually they are just theoretical or obscure issues or can be addressed subsequently and can safely be ignored for now. Provided the last entry in the results list reads *All prerequisite checks passed successfully. Click 'Install' to begin installation* you can go ahead and do so. Click **Install** to begin the installation proper, which will run for several minutes and during which a status screen is displayed and after which the server will restart. Log back in as Administrator.

What needs to be done next depends upon the local infrastructure. If the server is connected to an all-on-one router that provides DHCP services, which is typically the case in a very small network, or is part of an existing network that already includes working servers, then you will shortly be able to continue with the next section 3. STORAGE AND SHARED FOLDERS. However, if this is the *only* server and it is *not* connected through a router that provides DHCP, then it will be necessary to install the DHCP service on the server itself *before* continuing and how to do so is described in 12.8 Installing DHCP.

2.3 Windows Server 2016 User Interface

We have used Server Manager to configure the server, but as can be appreciated, it is an application and not the operating system itself. Windows Server 2016 is essentially the same as the Windows 10 desktop operating system, but with additional features and capabilities for networking, and as such has the same basic user interface. If you close down Server Manager and click the **Start** button (or press the **Start** key on the keyboard) you will be presented with something along the following lines:



F
igure 30: Windows Server 2016 User Interface

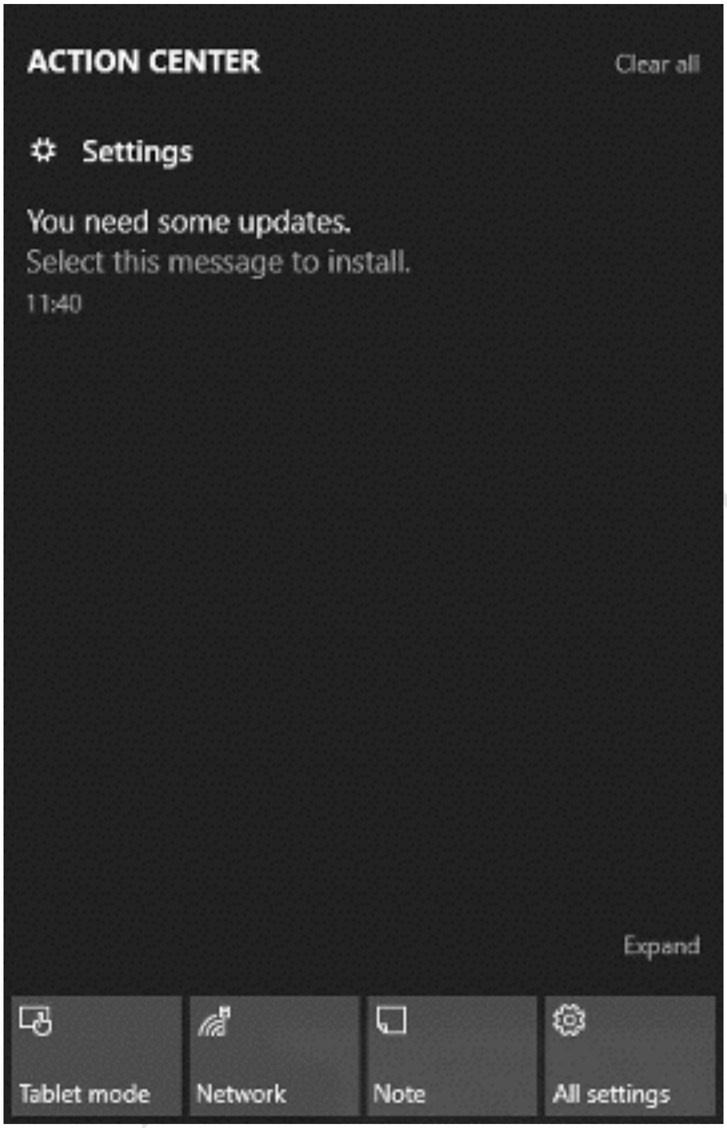
All the programs on the system are available on the Start menu, organized alphabetically. The most frequently used ones will appear at the top of the screen; any new ones which are subsequently installed will be marked as '*New*'. On the right-hand of the Start menu are tiles (icons) for a selection of commonly used items, including: *Server Manager* (which we have already used); *Windows Administrative Tools*, which is a selection of useful tools and which can be viewed as a list or as icons; *Control Panel*, the traditional method of adjusting the settings on a Windows computer.

The Start menu can be customized to reflect your preferences. For instance, it can be resized and made larger or smaller. The individual tiles can be resized, removed, or added to the Taskbar on the bottom of the screen (right-click a tile and choose an option). Additional tiles can be added: right-click on a program from the list on the left-hand side and choose **Pin to Start**.

In the bottom left-hand corner of the Start menu are three small icons. The one at the bottom is *Power* and is used for shutting down or restarting the server, should that ever prove necessary. The middle one – which looks like a cogwheel – is *Settings* (strictly speaking, *Windows Settings*). Settings is the modern version of the Control Panel; it largely duplicates the functionality of the Control Panel and longer term will probably replace it. The top icon is used for logging off from the server or locking the screen and should always be clicked after you have finished working on the server, for security purposes.

On the Taskbar, to the right of the Start button, are four icons. The two most useful ones are *Internet Explorer* and *File Explorer*. One thing to note is that the Edge browser, which is Microsoft's preferred browser for Windows 10, is not present in Windows Server.

On the right-hand side of the Taskbar is the *Notifications* icon; when the system needs to inform you of something a number appears on it, corresponding to the number of messages it has. Clicking the icon will then expand it to show the *Action Center*, where you can read the messages. Many of the messages are actionable and you can click them to make something happen:



Settings

You need some updates.
Select this message to install.
11:40

Figure 31: Notifications/Action Center

One useful thing to know is that right-clicking the Start button brings up a menu of useful shortcuts for managing the system and is generally quicker than working through the Start Menu or Server Manager. For instance, during the installation we intentionally went into Server Manager to change the IP address of the network adaptor; however, a quicker way of doing so is to right-click **Start** and choose **Network Connections**.

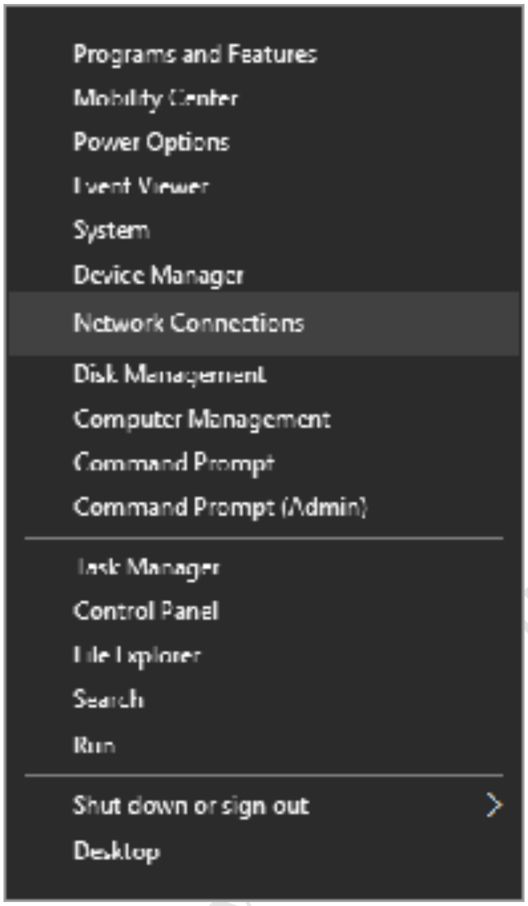


Figure 32: Start button right-click menu

3. STORAGE AND SHARED FOLDERS

3.1 Overview

The main purpose of a network is to provide an environment in which users can store and share information. This is implemented by creating folders on the server, some shared and some private, then defining access rights to control who sees what. The structure of these folders will depend upon the requirements of the organization, but a typical arrangement might be: one or more shared company folders that everyone has access to; folders for the different departments and functions within the business; individual private or 'home' folders for each user (analogous to the Documents folder on a PC). These folders are known as *network shares* or *shared folders*.

In our example we have two volumes, one for the operating system (the C: drive) and one for the data (the D: drive). On the data volume we will create the following structure:

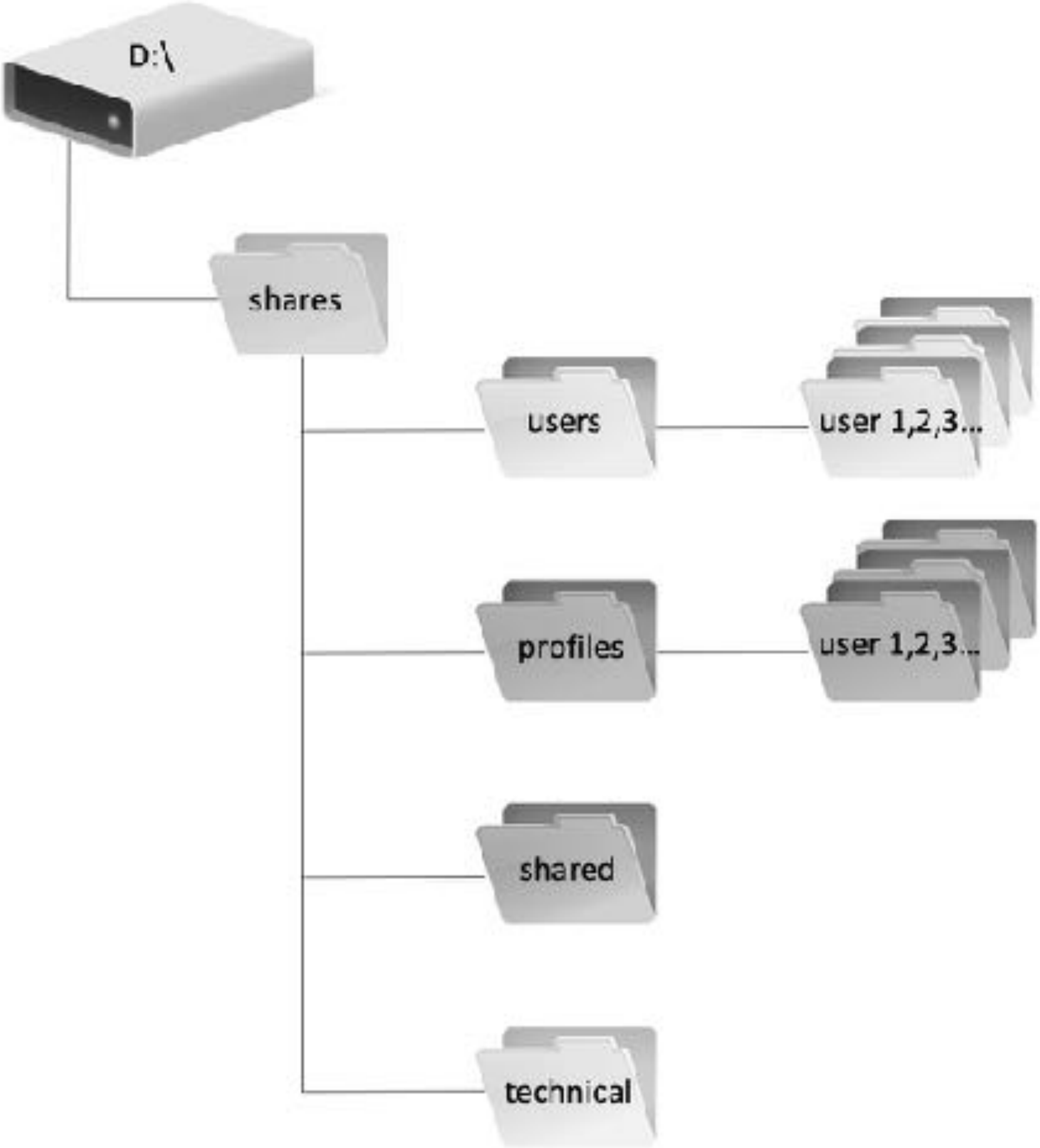


Figure 33: Example folder structure

The folders sit below a top-level one called *shares* that is created automatically. The folders are used as follows:

Users - Holds the individual home folders for users

Profiles - Folder for holding user profiles (the purpose and use of profiles is discussed later)

Shared - Holds data that can be used by everyone in the organization

Technical - For use by the person(s) supporting the system and contains master copies of software, utilities, technical documentation and so on.

You can create as many folders as you require, with whatever names you wish, at whatever point. For instance, you might create additional folders for departments or teams or classes. It is suggested that some thought is given to the structure, to make it logical and sensible. However, you might wish to start using the template above.

Folders are created using Server Manager. If you have worked with earlier versions of Windows Server, such as Windows Server 2003, 2008 or 2012, then you may be pleased to hear that the other, older techniques and tools for creating and managing shares are generally still available and work as expected. However, it is suggested that you do acquaint yourself with the new methods of doing things: even though they may seem unfamiliar at first, they are well thought out and work well.

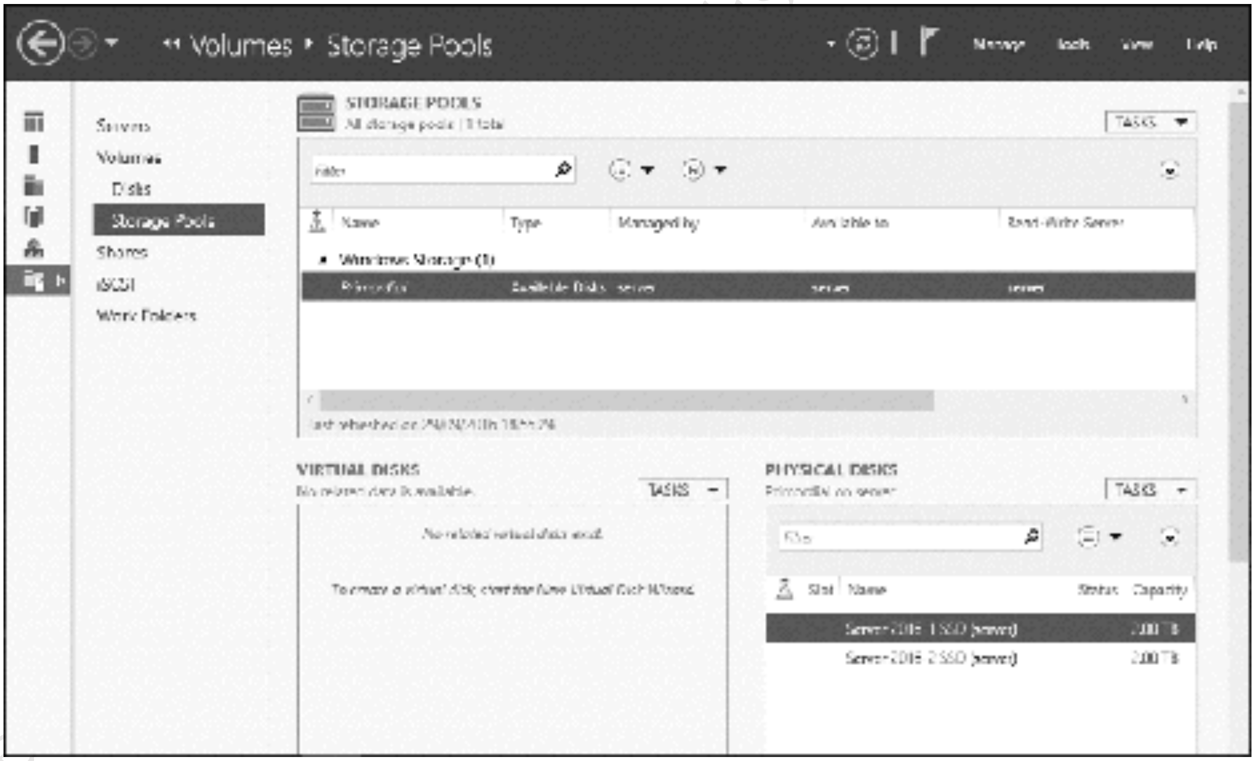
Important: If you are ***not*** *using Storage Spaces, go to section 3.3 Creating a Shared Folder using Server Manager at this point. If you* ***are*** *using Storage Spaces continue with section 3.2 Setting up Storage Spaces below.*

3.2 Setting up Storage Spaces

As introduced earlier on, *Storage Spaces* is a feature of Windows Server that allows systems with multiple hard drives to be better utilized and managed. There is a common perception that it is just a low-cost alternative to RAID; in fact, it is an extremely sophisticated feature and with additional capabilities of particular interest to corporate users, although in this example we will stick to the basics as applicable to a small network. If you are going to use Storage Spaces, it should be setup ***now*** before creating any users and folders on the system.

In this example, the server had a single hard drive, upon which Windows Server had been installed. 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 or external USB, USB-C or eSATA drives.

First make sure that the new drives are being recognized: right-click **Start** and click **Disk Management**. There may be a message about having to initialize the new drives, in which case do so. There will be a choice of MBR (Master Boot Record) and GPT (GUID Partition Table); MBR is an older and more universal system but is restricted to drives of up to 2TB capacity, whereas GPT will work with larger capacity drives but requires that the server has a UEFI BIOS (although all modern servers do so). Make a choice and click **OK**. Having initialized the drives, it is not necessary to format the drives, so quit Disk Management. Next, click **File and Storage Services** from Server Manager. On the left-hand side panel, click **Storage Pools** and the screen should appear as follows, although the specifics will vary depending on your particular system:



STORAGE POOLS
All storage pools | 1 total

Name	Type	Managed by	Available to	Read-Write Server
▪ Windows Storage (1)				
Primordial	Available Disks	server	server	server

Last refreshed on 29/08/2018 15:54:26

VIRTUAL DISKS
No related data is available.

No related virtual disks exist.

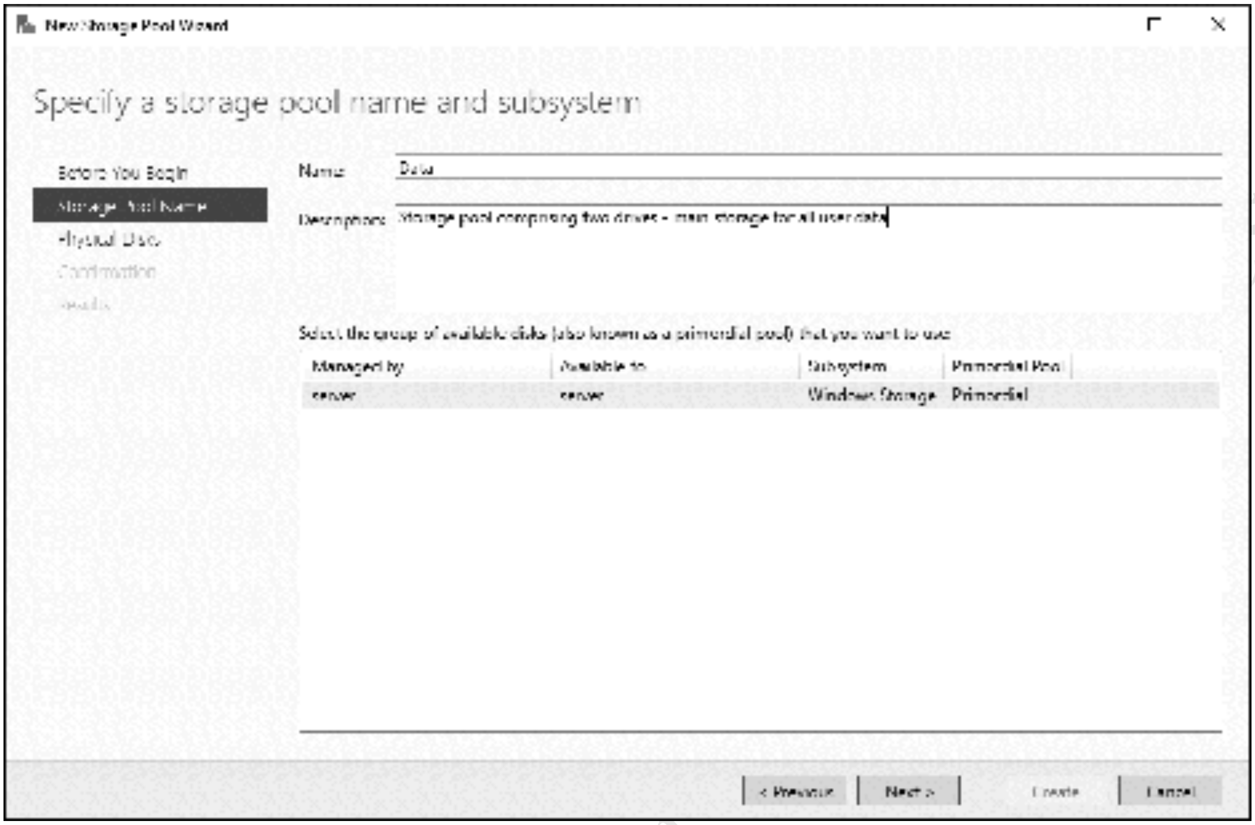
To create a virtual disk, start the New Virtual Disk Wizard.

PHYSICAL DISKS
Primordial on server

Slot	Name	Status	Capacity
	Server-2016 1 SSD (server)		2.00 TB
	Server-2016 2 SSD (server)		2.00 TB

Figure 34: Server Manager Storage Pools

The screen is divided into three main panels: *Storage Pools*, *Virtual Disks* and *Physical Disks*. In the top-right hand corner of each panel is a dropdown labelled *TASKS*; click on TASKS for Storage Pools and select **New Storage Pool** to invoke the *New Storage Pool Wizard*. Click **Next** to display the following panel. Enter a Name (e.g. *Data*), an optional Description and click **Next**:



New Storage Pool Wizard

Specify a storage pool name and subsystem

Name: Data

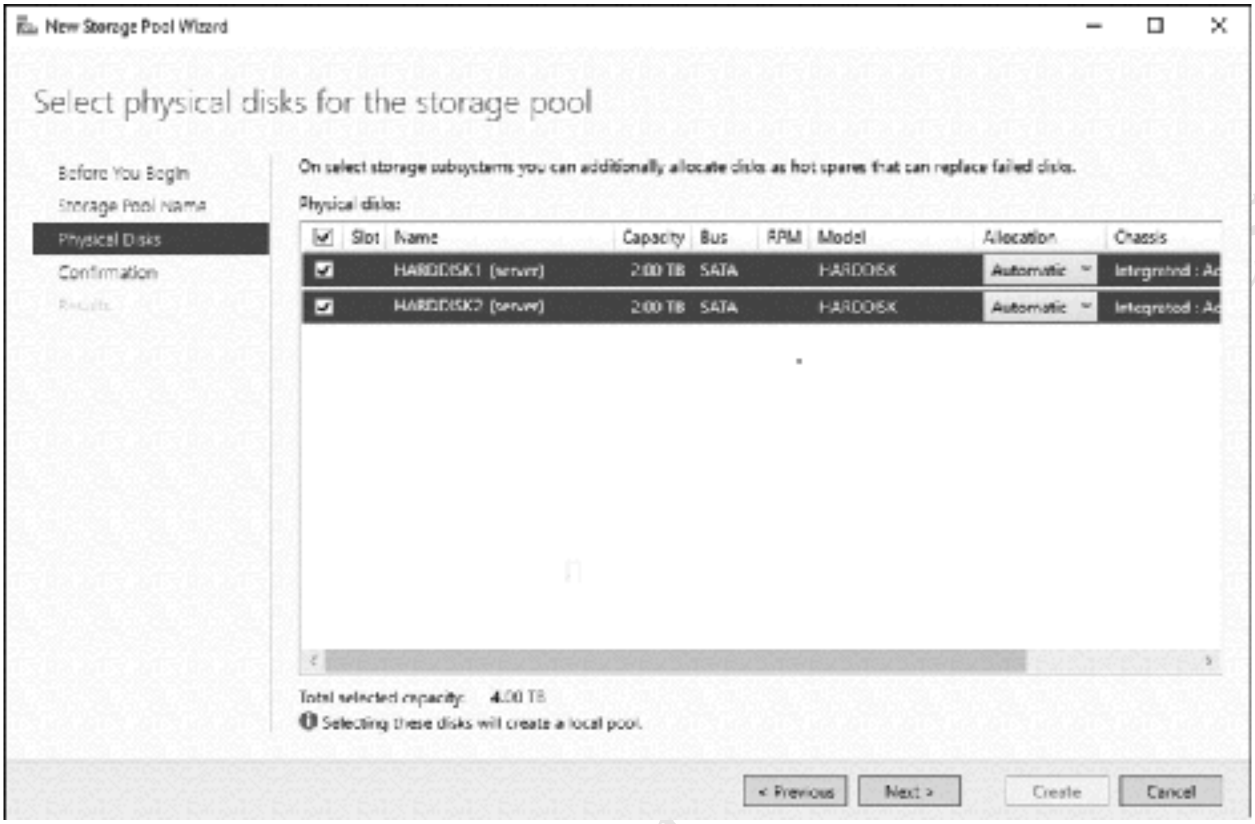
Description: Storage pool comprising two drives – main storage for all user data

Select the group of available disks (also known as a primordial pool) that you want to use:

Managed by	Available to	Subsystem	Primordial Pool
server	server	Windows Storage	Primordial

Figure 35: New Storage Pool Wizard

On the subsequent screen, tick the boxes for each disk to be used in the storage pool, followed by **Next**:



New Storage Pool Wizard

Select physical disks for the storage pool

On select storage subsystems you can additionally allocate disks as hot spares that can replace failed disks.

Physical disks:

☑	Slot	Name	Capacity	Bus	RPM	Model	Allocation	Chassis
☑		HARDDISK1 (server)	2.00 TB	SATA		HARDDISK	Automatic	Integrated : Ac
☑		HARDDISK2 (server)	2.00 TB	SATA		HARDDISK	Automatic	Integrated : Ac

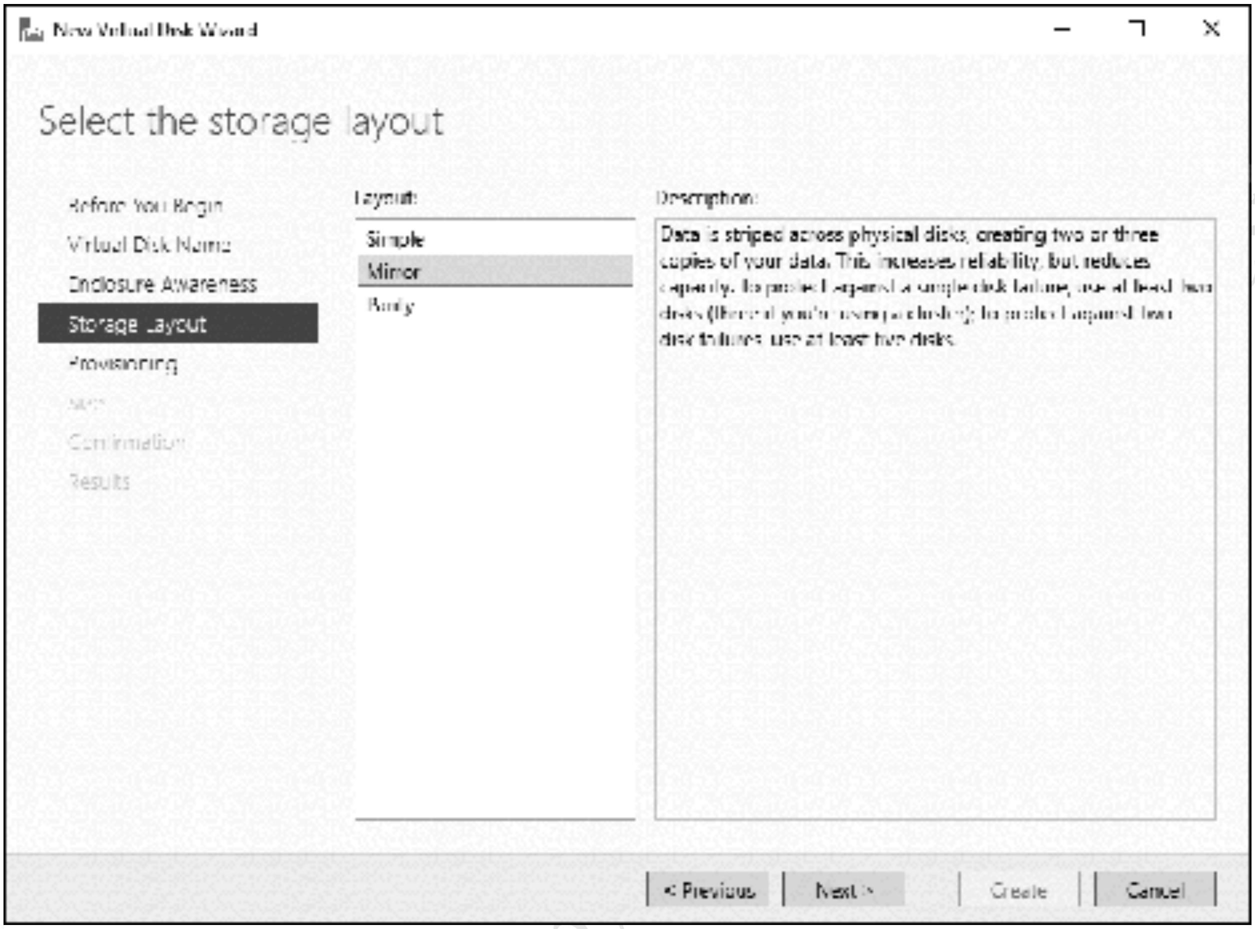
Total selected capacity: 4.00 TB

Selecting these disks will create a local pool.

Figure 36: Select disks for the storage pool

A *Confirm selections* screen will be shown – click the **Create** button. After a short while the *Storage Pool Wizard* will complete – click **Close** to finish.

The next step is to create a *Virtual disk*. From the main Storage Pools screen, in the Virtual Disks section, click TASKS and choose **New Virtual Disk**. Select the storage pool from the pop-up screen and click **OK**. The *New Virtual Disk Wizard* will begin – click **Next** on the first screen. On the subsequent screen, specify the virtual disk name (e.g. '*Data*') and an optional description, then click **Next**. The next screen is about something called *Enclosure resiliency,* which is unlikely to be used on a small system, so just click **Next**. The following screen appears:


New Virtual Disk Wizard

Select the storage layout

Layout:

- Simple
- Mirror
- Parity

Description:

Data is striped across physical disks, creating two or three copies of your data. This increases reliability, but reduces capacity. To protect against a single disk failure, use at least two disks (three if you're using a cluster); to protect against two disk failures, use at least five disks.

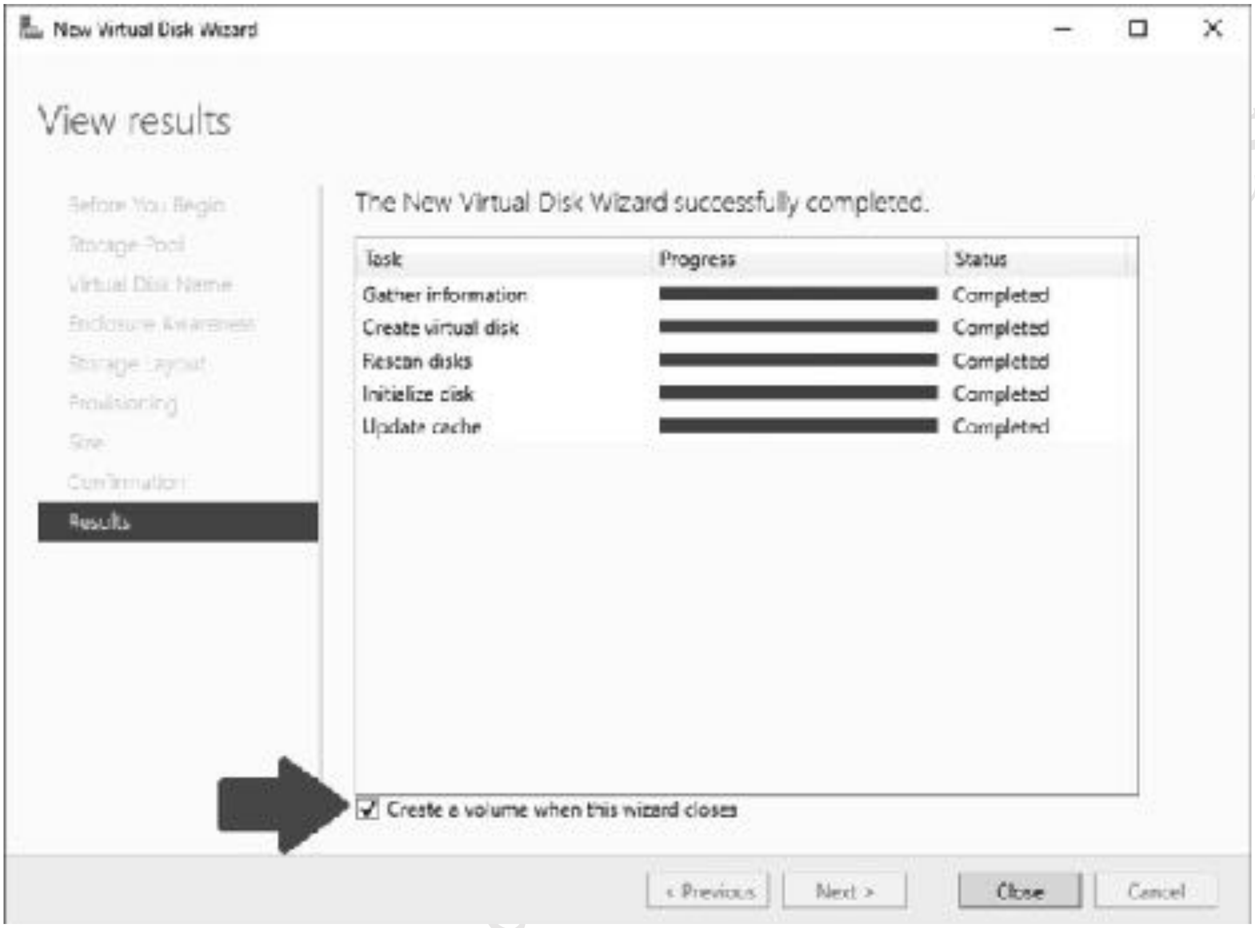
Figure 37: New Virtual Disk Wizard

There are three types of storage layout to choose from:

- *Simple* - in which the drives are aggregated to create a single large volume, analogous to RAID 0 or JBOD (*Just a Bunch of Disks*) in other computing environments
- *Mirror* – in which data is duplicated on each drive in order to provide redundancy, analogous to RAID 1 in other computing environments. Requires at least two physical drives in the underlying Storage Space.
- *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 drive failures, analogous to RAID 5 or RAID 6 in other computing environments. Requires at least three physical drives in the underlying Storage Space.

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. Make a choice depending on your requirements and the number of disks available, then click **Next**.

On the follow-on screen, there is a choice between *Thin* or *Fixed Provisioning*. This defines whether all the disk space is allocated at the beginning ("Fixed") or starts small and grows as required ("Thin"). In a small setup, you would generally choose **Fixed** (Thin Provisioning is of more interest in a larger network with many servers, typically sharing common disk space). On the next screen you can further specify the size of the virtual disk – choose the **Maximum size** option and click **Next**. A *Confirm selections* screen is displayed – click **Create**. After a short while, depending on the options chosen, a completion screen is shown. Note that the **Create a volume when this wizard closes** box should be ticked:



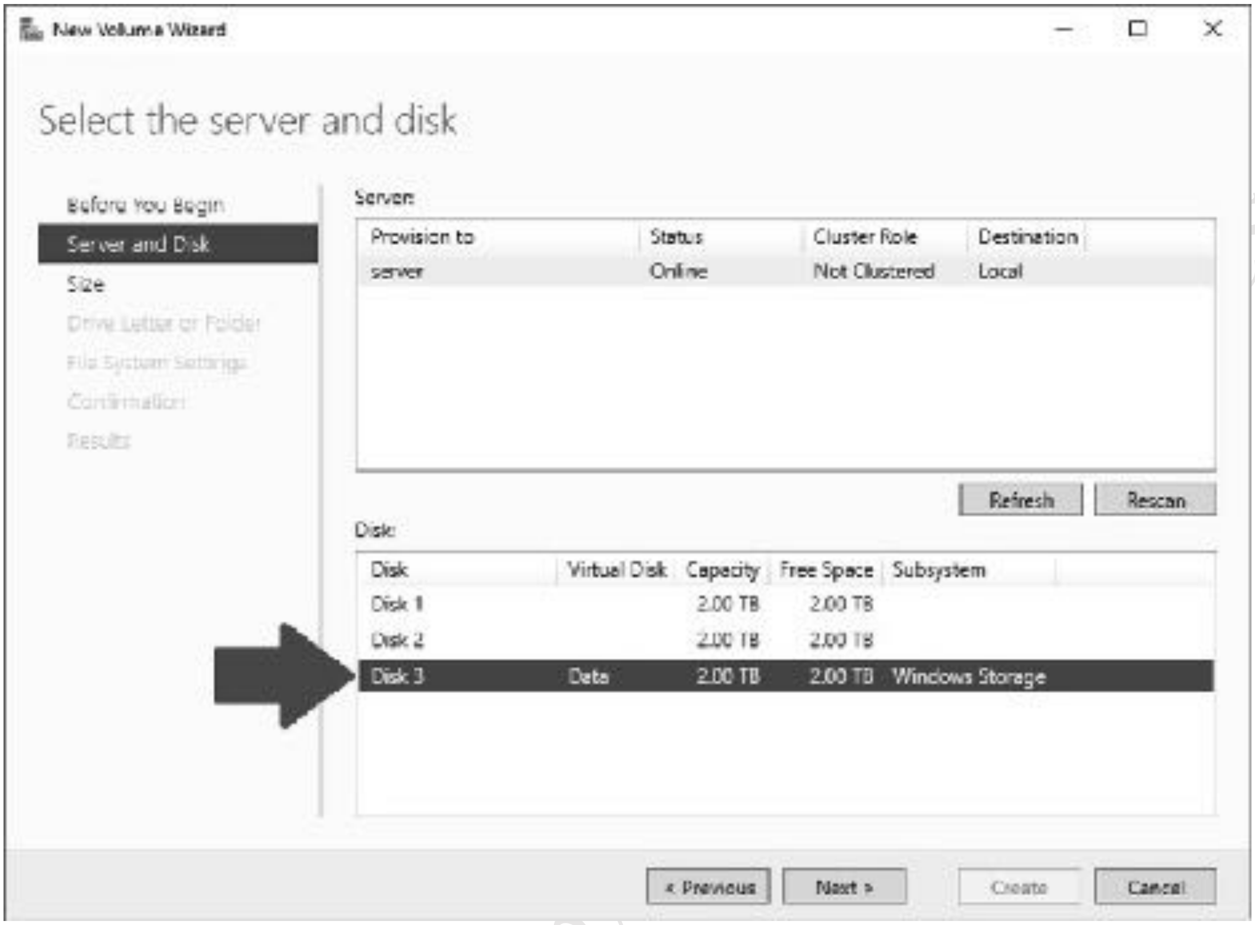
The New Virtual Disk Wizard successfully completed.

Task	Progress	Status
Gather information		Completed
Create virtual disk		Completed
Rescan disks		Completed
Initialize disk		Completed
Update cache		Completed

☑ Create a volume when this wizard closes

Figure 38: Virtual Disk Wizard completion screen

Click **Close** and the *New Volume Wizard* will commence. Click **Next** on the first screen. On the second screen highlight the newly created storage space and click **Next**:



Select the server and disk

Server:

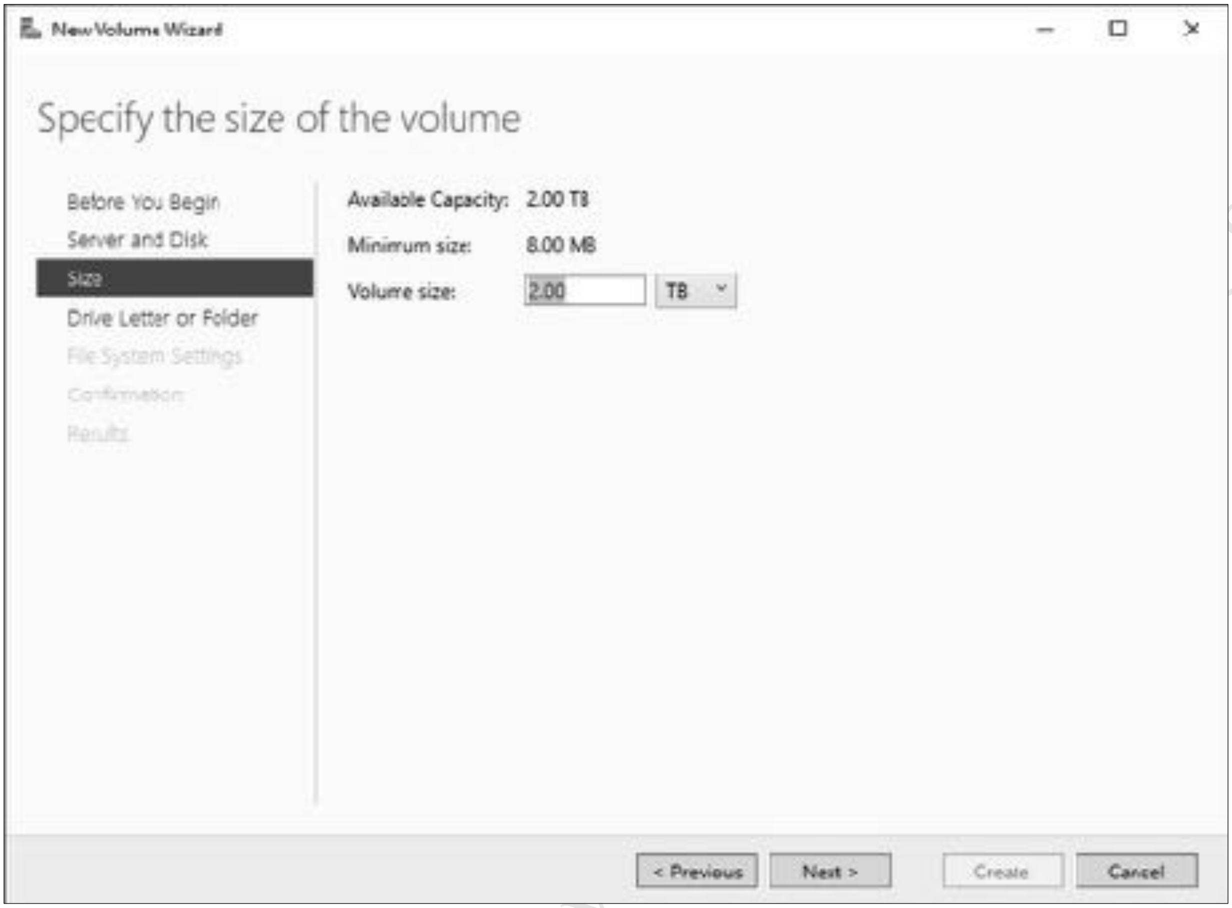
Provision to	Status	Cluster Role	Destination
server	Online	Not Clustered	Local

Disk:

Disk	Virtual Disk	Capacity	Free Space	Subsystem
Disk 1		2.00 TB	2.00 TB	
Disk 2		2.00 TB	2.00 TB	
Disk 3	Data	2.00 TB	2.00 TB	Windows Storage

Figure 39: New Volume Wizard

The size of the volume can now be specified. Unless you have very specific reasons to do otherwise, make it as large as permitted and click **Next**:



Specify the size of the volume

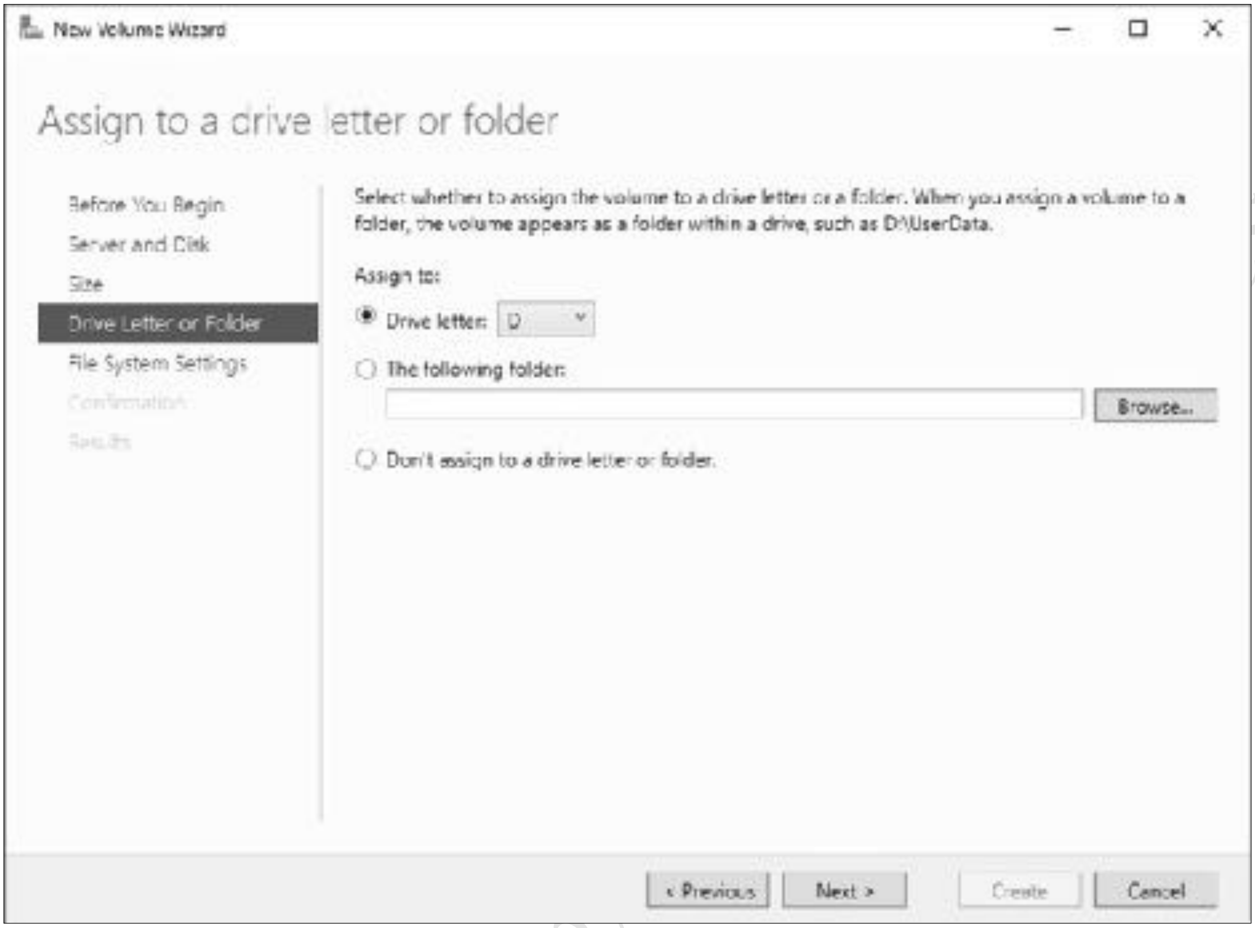
Available Capacity: 2.00 TB

Minimum size: 8.00 MB

Volume size: 2.00 TB

Figure 40: Specify the size of the new volume

On the subsequent screen, assign a free drive letter to the new volume. In this example, we will make it the D: drive. Click **Next**:



Assign to a drive letter or folder

Select whether to assign the volume to a drive letter or a folder. When you assign a volume to a folder, the volume appears as a folder within a drive, such as D:\UserData.

Assign to:

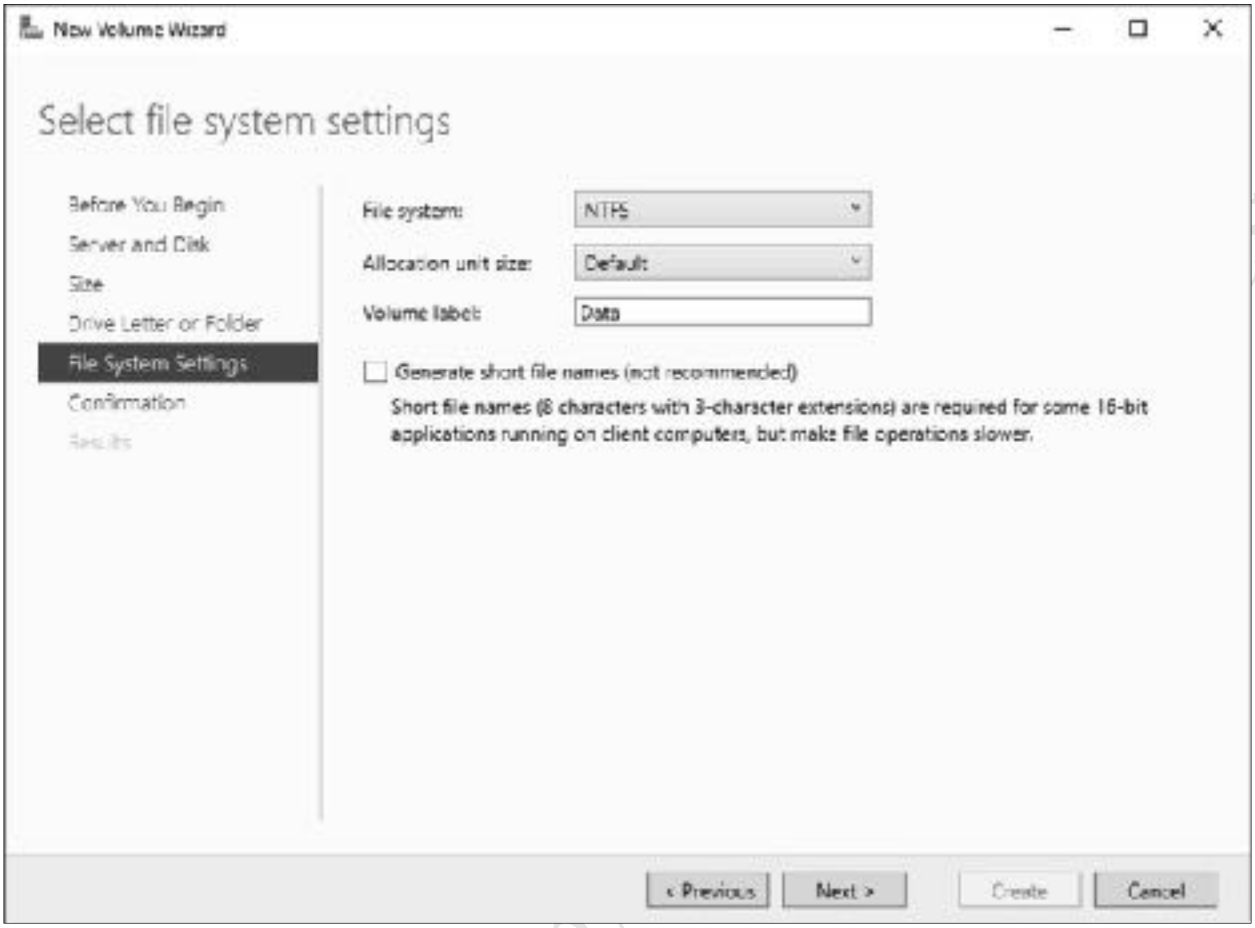
● Drive letter: D

○ The following folder:

○ Don't assign to a drive letter or folder.

Figure 41: Assign a drive letter to the new volume

On the following screen, check the *File System* type - you will usually want NTFS - and assign a *Volume label* e.g. ‘Data’. Click **Next**:



Select file system settings

File system: NTFS

Allocation unit size: Default

Volume label: Data

□ Generate short file names (not recommended)

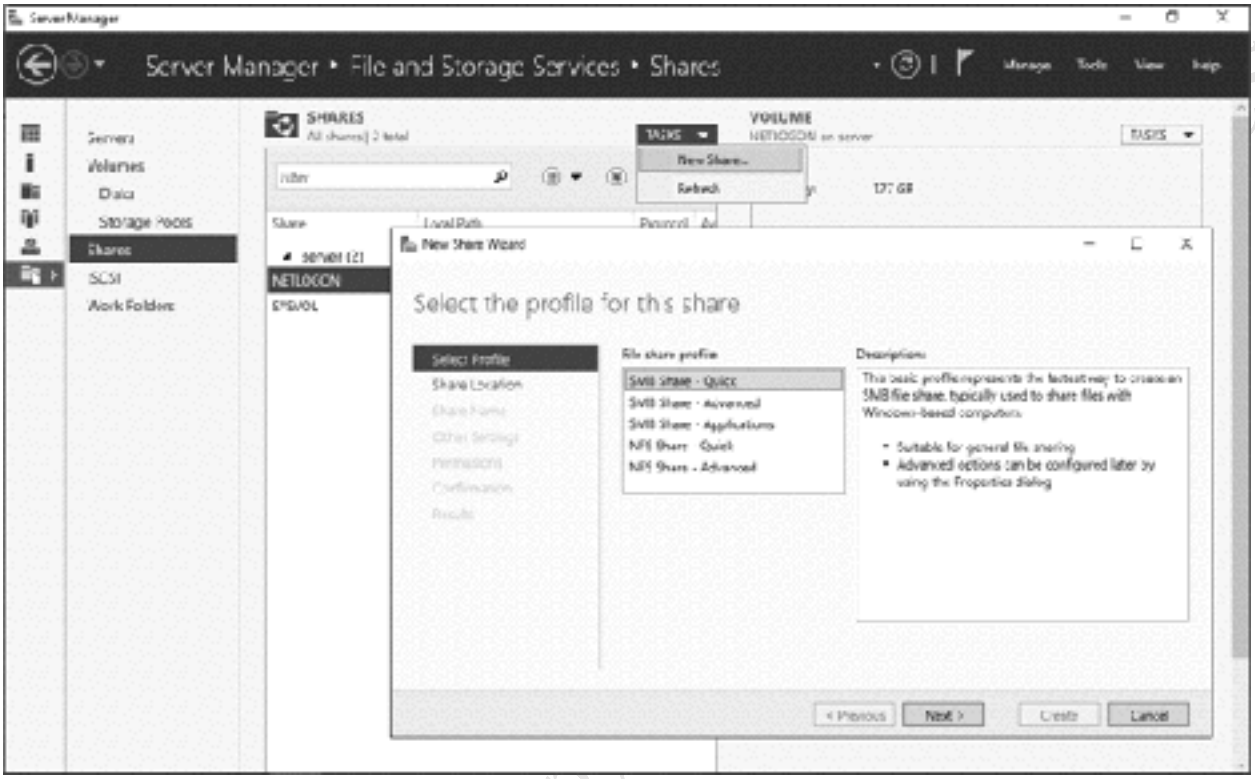
Short file names (8 characters with 3-character extensions) are required for some 16-bit applications running on client computers, but make file operations slower.

Figure 42: Select file system settings

A *Confirm selections* screen is displayed - assuming everything is satisfactory, click **Create**. After a while a completion screen is shown, the time for which depends upon the size of the drives and the options chosen. Click **Close**. The new drive should now be visible in File Explorer.

3.3 Creating a Shared Folder using Server Manager

Go into **Server Manager**. In the left-hand panel click **File and Storage Services** followed by **Shares**. In the **SHARES** section click **TASKS** followed by **New Share** to start the *New Share Wizard*:



Select the profile for this share

This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.

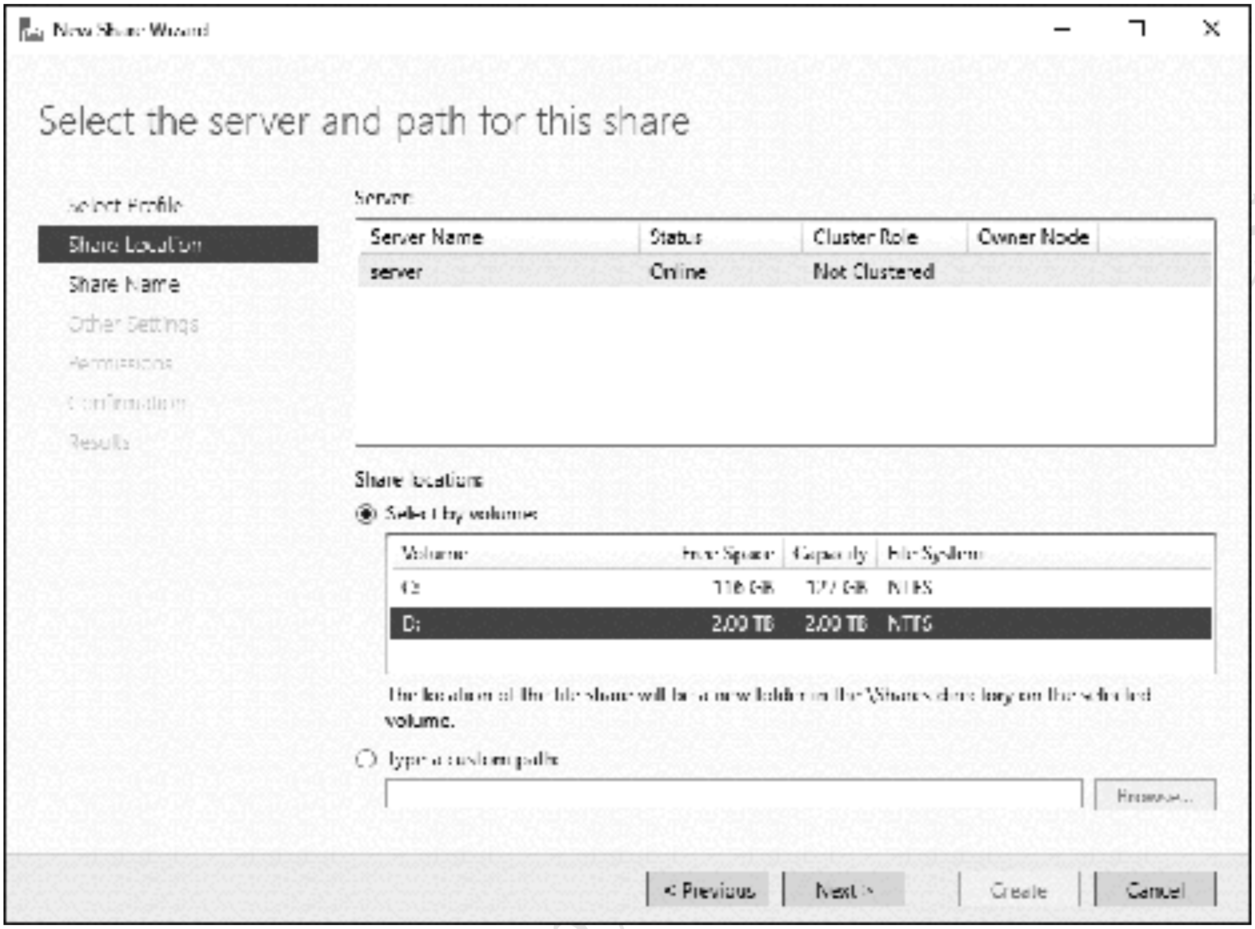
- Suitable for general file sharing
- Advanced options can be configured later by using the Properties dialog

Figure 43: New Share Wizard

There are five types different 'profiles' for shares, in which the terms *SMB* relates to Windows PCs and *NFS* relates to computers running UNIX or Linux variants, although note that most devices, including Linux computers and Macs, also understand SMB:

SMB Share - Quick: the most commonly used option in a small network
SMB Share - Advanced: allows additional features to be specified and controlled
SMB Share - Applications: provides capabilities of relevance to corporate and larger environments
NFS Share - Quick: simple way of creating shares for UNIX/Linux computers
NFS Share - Advanced: additional features for UNIX/Linux computers

Choose **SMB Share – Quick** followed by **Next**. On the resultant panel explicitly specify the volume where the shared folder is to reside if there is more than one to choose from (in this example it is the D: drive) and click **Next**:



New Share Wizard

Select the server and path for this share

- Select Profile
- Share Location
- Share Name
- Other Settings
- Permissions
- Confirmation
- Results

Server:

Server Name	Status	Cluster Role	Owner Node
server	Online	Not Clustered	

Share location:

● Select by volume:

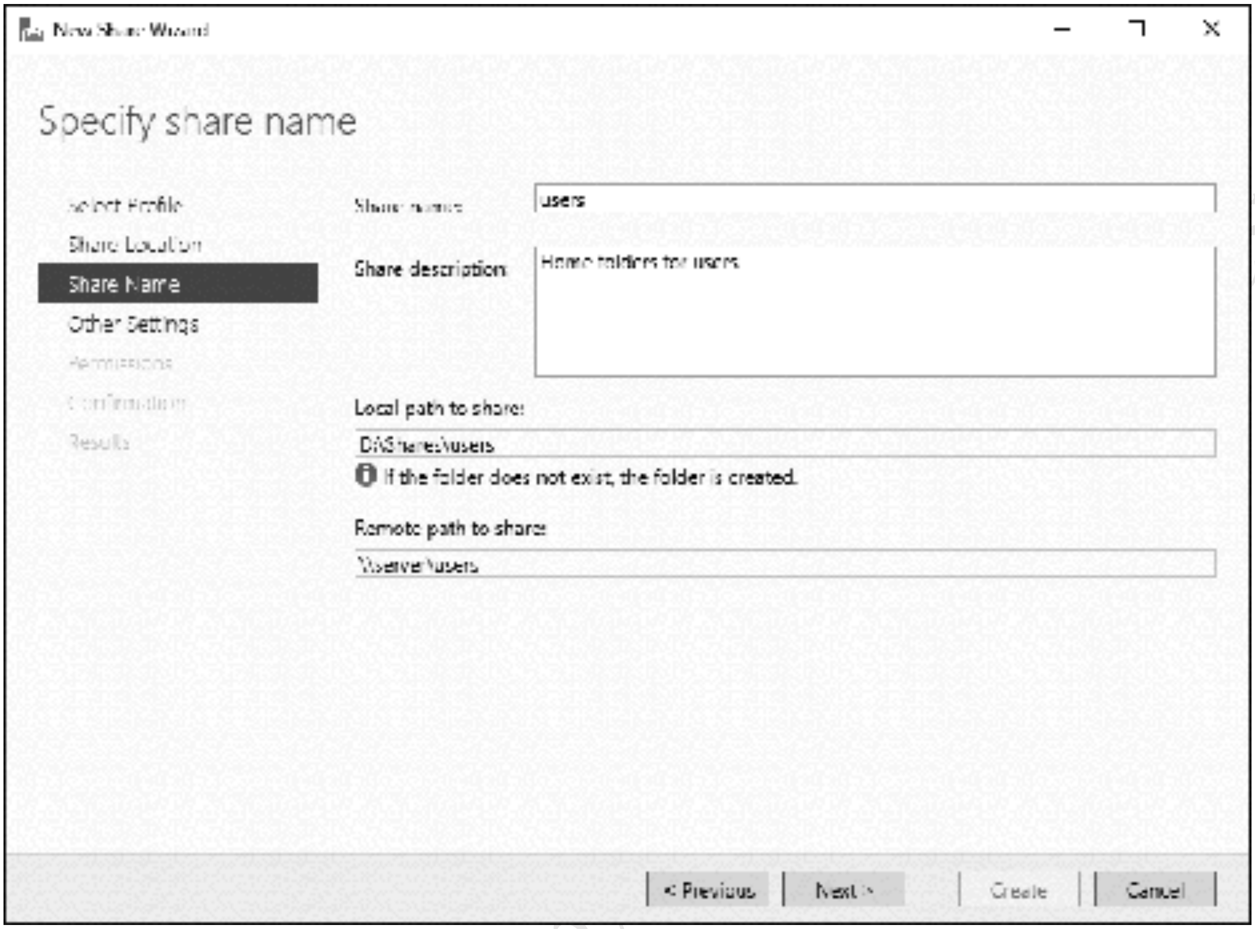
Volume	Free Space	Capacity	File System
C:	118 GB	127 GB	NTFS
D:	2.00 TB	2.00 TB	NTFS

The location of the file share will be a new folder in the \Shares directory on the selected volume.

○ Type a custom path:

Figure 44: Specify the location for the share

On the follow-on screen enter a *Share name* of *users* plus an optional *Share description*. The wizard will fill-in the *Local path to share* as *D:\Shares\users* and the *Remote path to share* as *\\server\users*. Note that all shared folders are below a folder called *Shares*, which the wizard creates automatically. Click **Next**:



Share name: users

Share description: Home folders for users

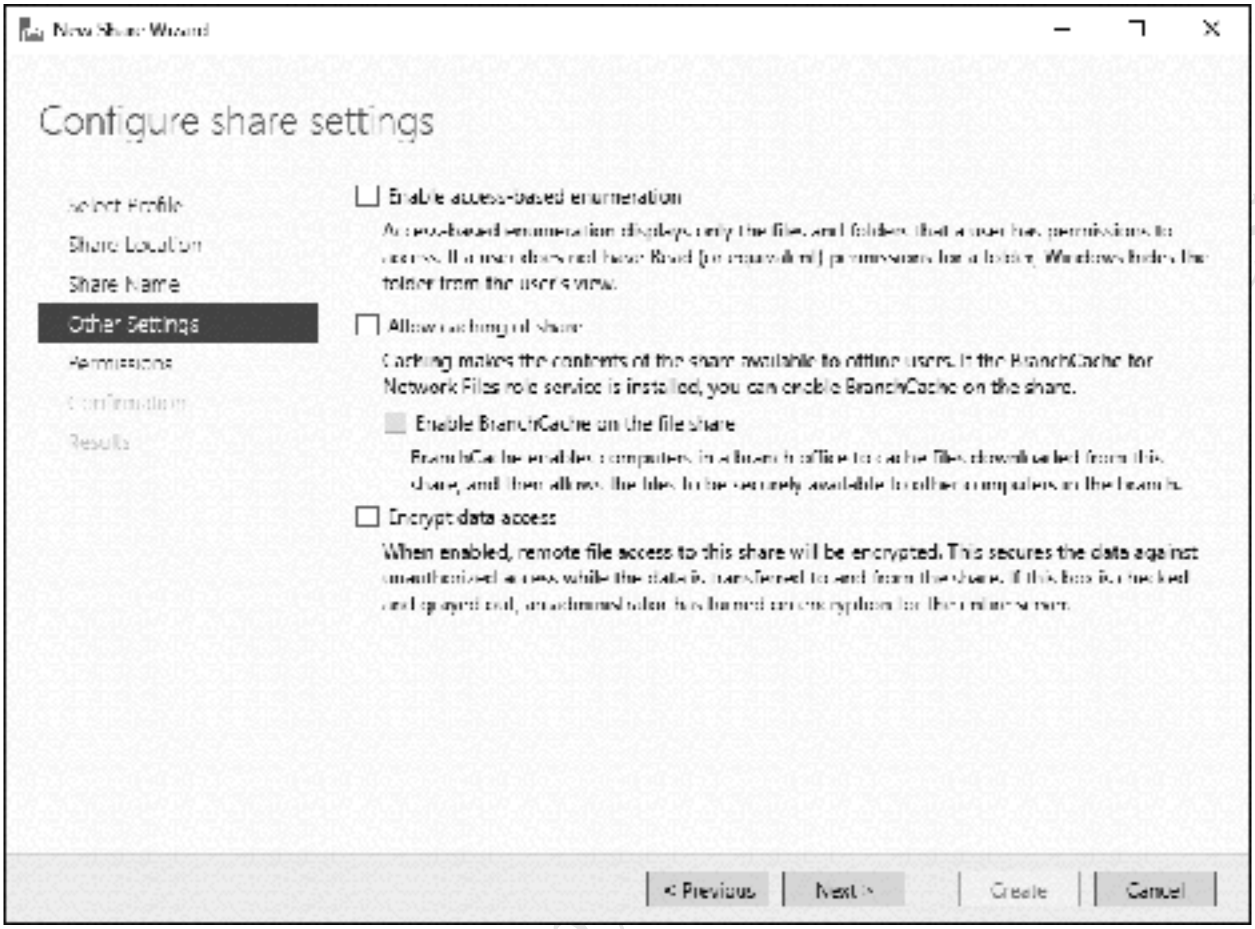
Local path to share:
D:\Shares\users

If the folder does not exist, the folder is created.

Remote path to share:
\\server\users

Figure 45: Specify the share name

On the next screen you would commonly leave all the boxes unticked. Click **Next**:



Configure share settings

□ Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

□ Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

□ Enable BranchCache on the file share

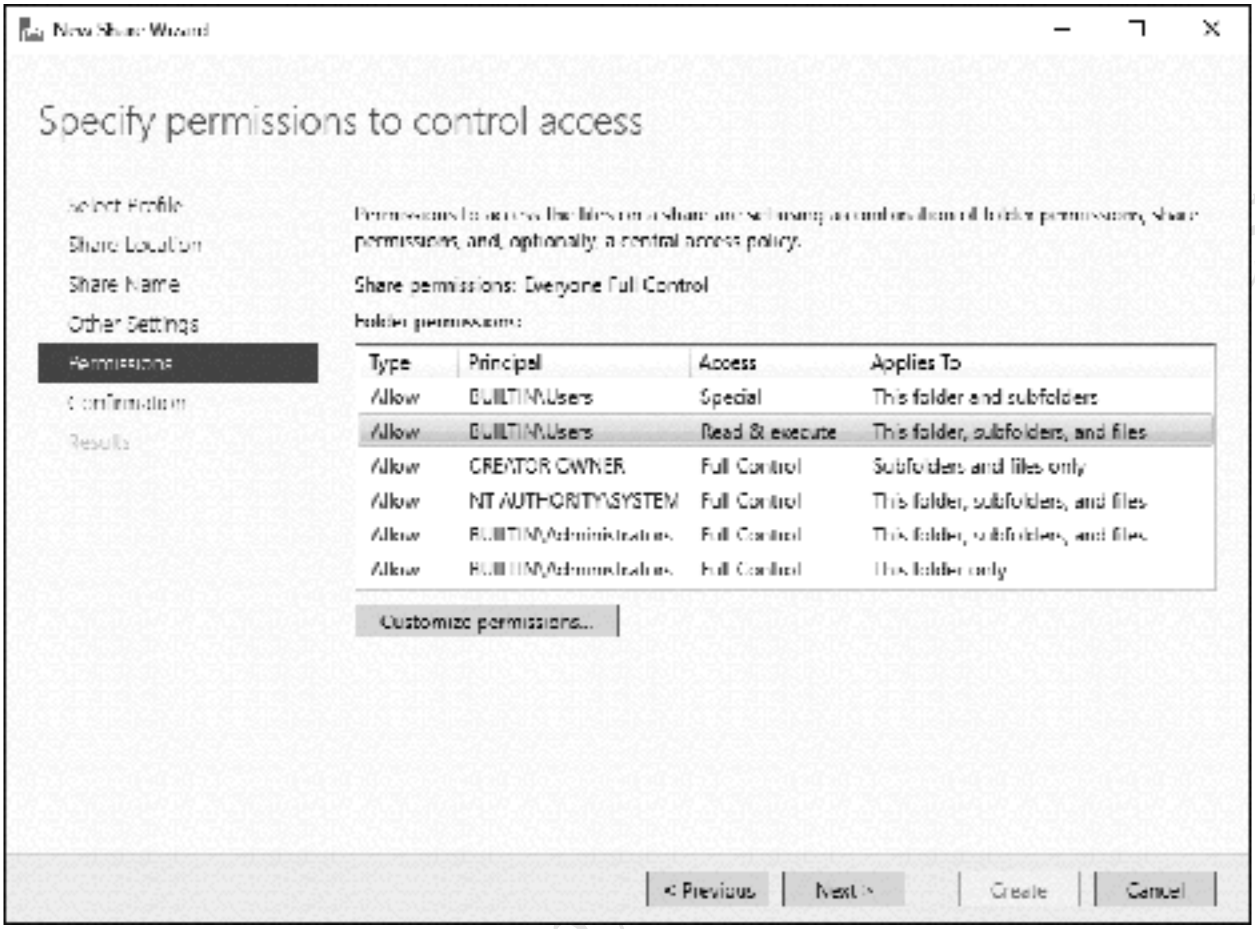
BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

□ Encrypt data access

When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

Figure 46: Configure share settings

The next screen defines permissions to control access. The default is that all users have complete control over this folder, which is fine for our purposes so just click **Next**:



Specify permissions to control access

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execute	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder only

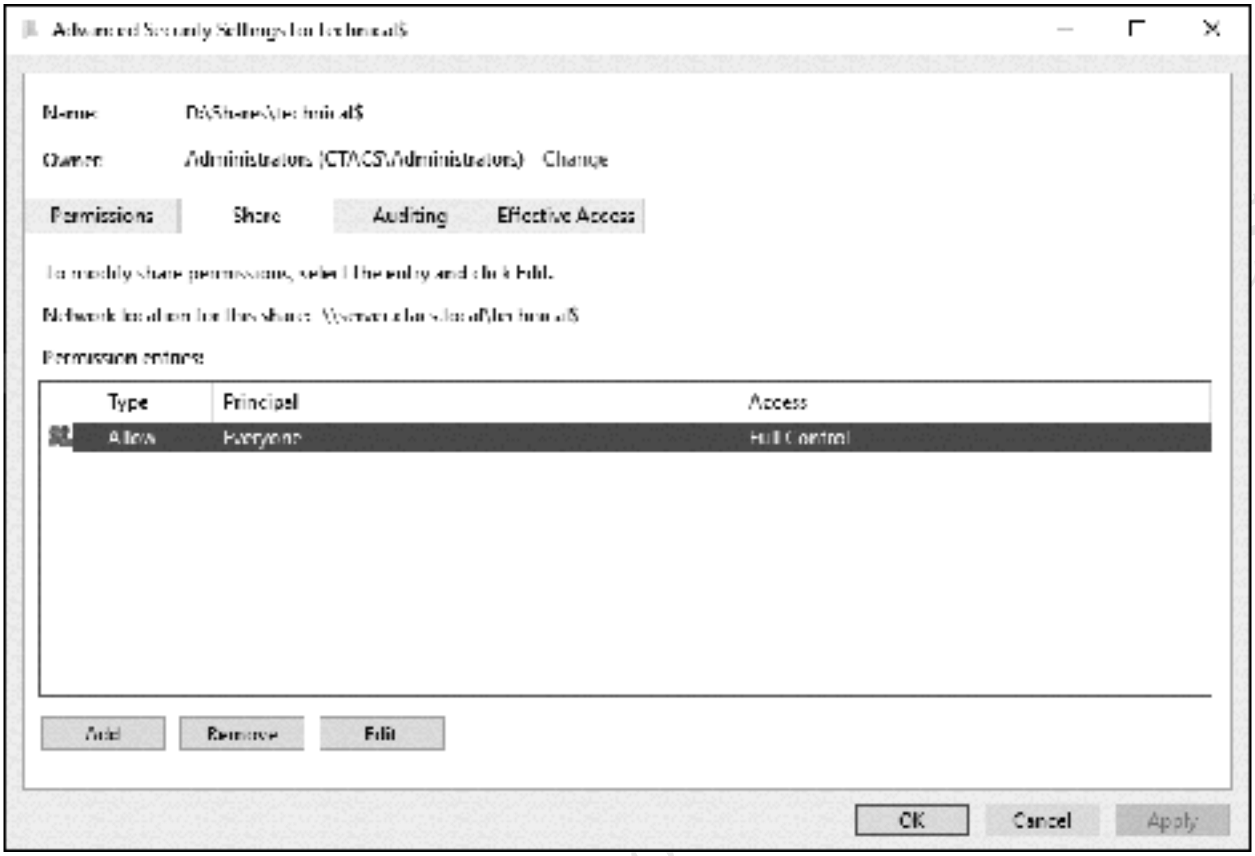
Figure 47: Specify permissions

The subsequent screen is simply to confirm the selections - press **Create** to continue. The share will be created in a few seconds – click **Close** on the resultant screen. You will be returned to the main Shares screen where the new share will be listed, alongside the two built-in ones of *NETLOGON* and *SYSVOL*.

Repeat the steps as described above and create another shared folder, this time called *shared*, which will act as a common area for all users to access.

Shared folders are normally visible to all users, but can be made hidden. The purpose of doing so is only partly related to security but is also to keep the overall system tidy and avoiding confusing users with a superfluous number of folders, as there may be dozens or even hundreds on a network. Shares are made hidden by placing a dollar sign ($) at the end of the share name. Repeat the steps described above to create a third shared folder and call the share *profiles$.*

Our fourth and final shared folder for now will be called *technical$*, also a hidden folder. This folder is for use by the person(s) supporting the system and contains master copies of software, utilities, technical documentation and other items of use to an administrator. Begin by creating it using the wizard as described above, only this time pause when you reach the *Specify permissions to control access* panel and click the **Customize permissions** button. On the resultant panel click the **Share** tab to show the following:



Advanced Security Settings for technical$

Name: D:\Shares\technical$

Owner: Administrators (CTACS\Administrators) Change

To modify share permissions, select the entry and click Edit.

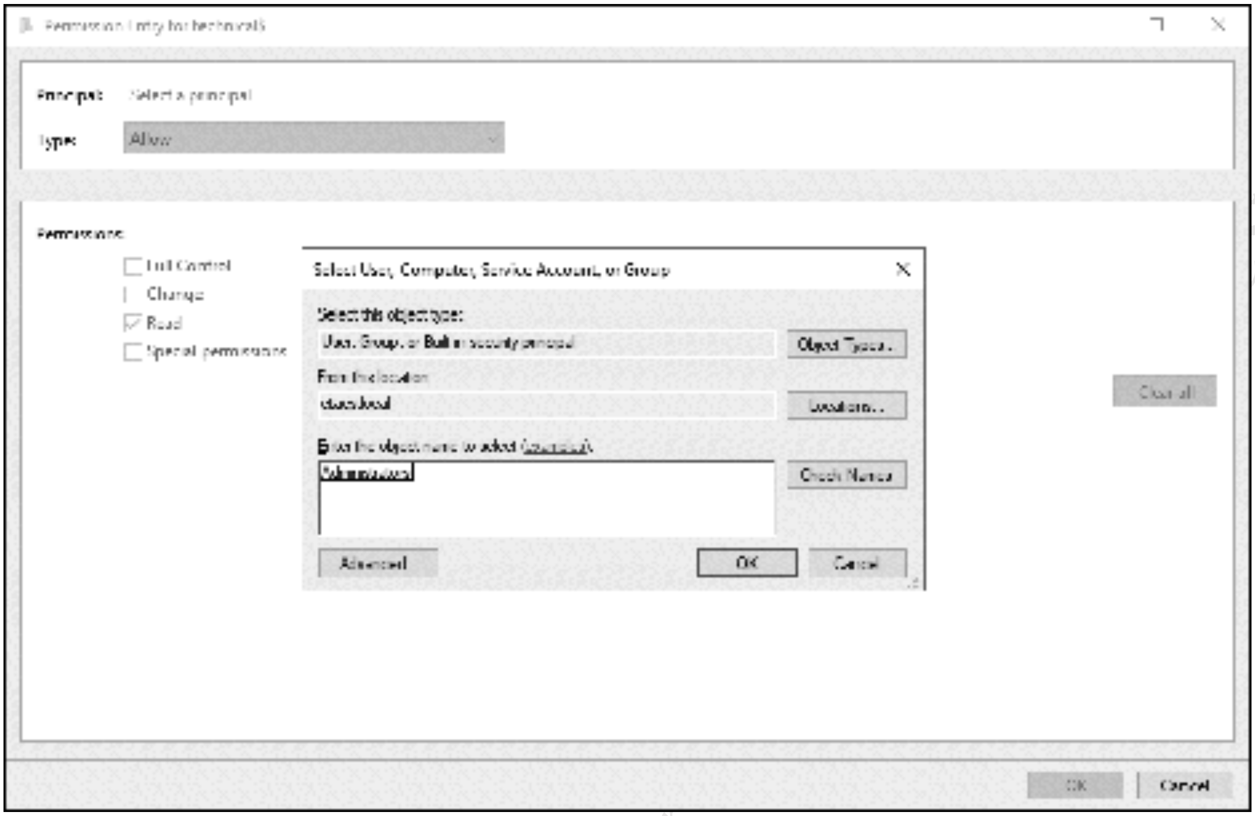
Network location for this share: \\sysman.ctacs.local\technical$

Permission entries:

Type	Principal	Access
Allow	Everyone	Full Control

Figure 48: Advanced security settings

We wish to restrict this share to Administrators only. Highlight the current entry for *Everyone* and click **Remove**. Then, click **Add** and on the next screen click **Select a principal**. A panel pops up: in the field that reads **Enter the object name to select,** type in the name of the user(s), in this case *Administrators*. Click **Check Names** and the user name will become underlined. Click **OK**.



Permission Entry for technical$

Principal: Select a principal

Type: Allow

Permissions:

□ Full Control
□ Change
☑ Read
□ Special permissions

Select User, Computer, Service Account, or Group

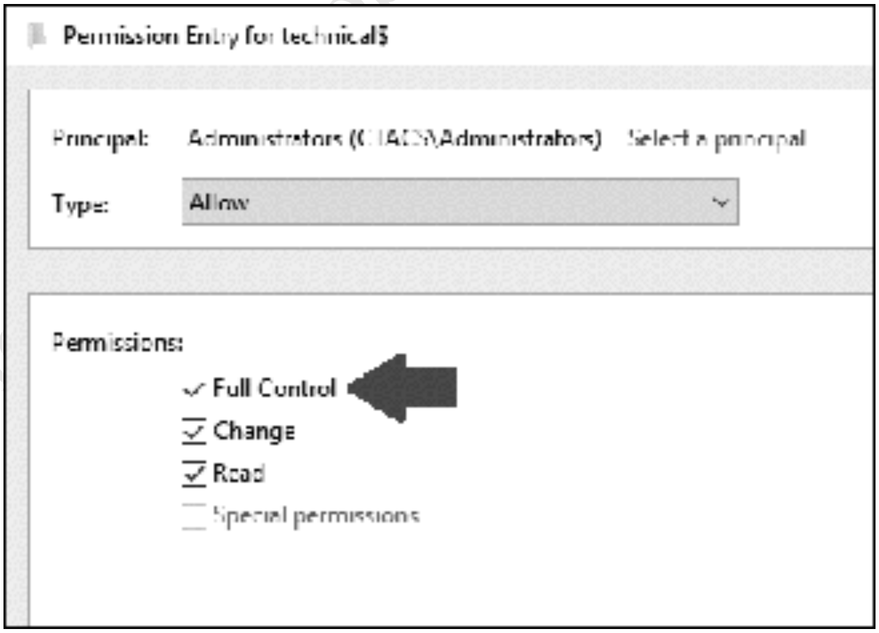
Select this object type:
Users, Groups, or Built-in security principals

From this location:
[illegible].local

Enter the object name to select (examples):
Administrators

Figure 49: Select Administrators

On returning to the previous panel tick **Full Control** - the other boxes will then be filled automatically - followed by **OK**:



Permission Entry for technical$

Principal: Administrators ([illegible]\Administrators) Select a principal

Type: Allow

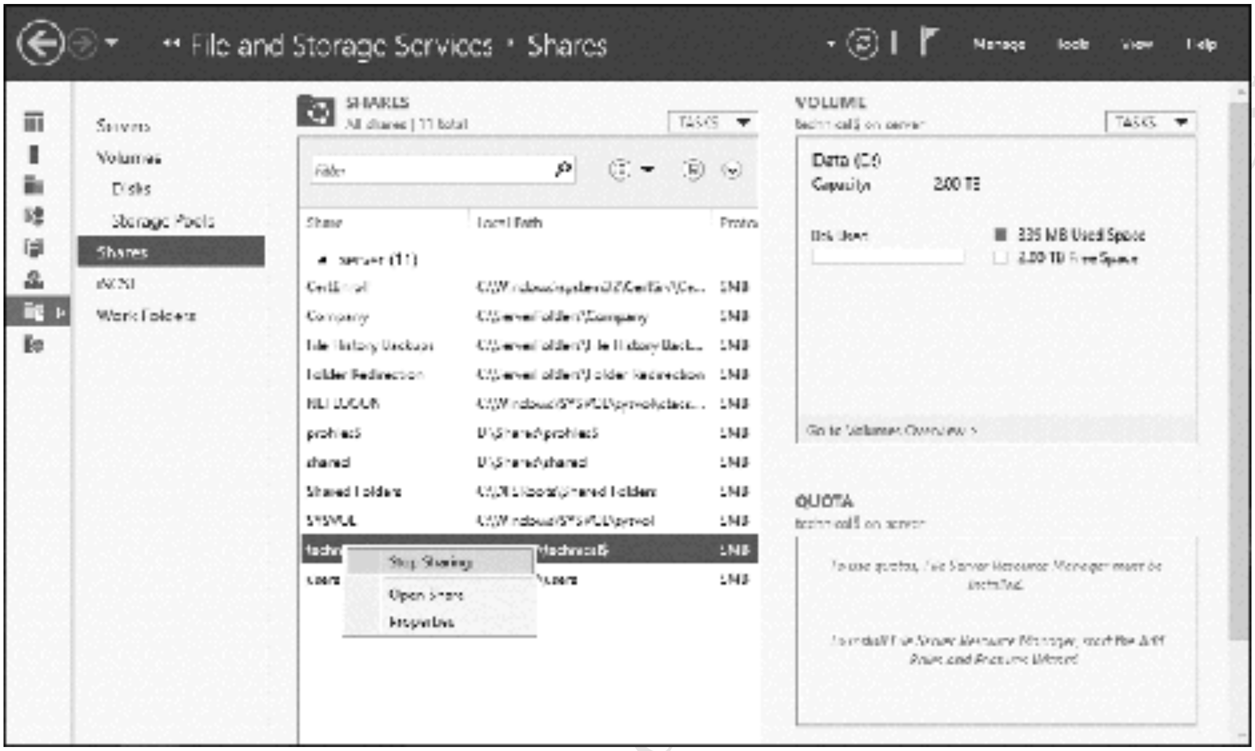
Permissions:

☑ Full Control
☑ Change
☑ Read
□ Special permissions

Figure 50: Specify permissions for Administrators

Returning to the previous panel, click **Apply**, **OK**, **Next**, **Create** to complete the creation of the share, followed by **Close**.

The share folders will now be listed in the main *Shares* screen. If it is every necessary to subsequent modify a share, it can be done by right-clicking on it and choosing one of the options from the pop-up menu:



SHARES
All shares | 11 total

Share	Local Path	Protocol
◢ server (11)		
CertEnroll	C:\Windows\system32\CertSrv\Ce...	SMB
Company	C:\ServerFolders\Company	SMB
File History Backups	C:\ServerFolders\File History Back...	SMB
Folder Redirection	C:\ServerFolders\Folder Redirection	SMB
NETLOGON	C:\Windows\SYSVOL\sysvol\techn...	SMB
projects	D:\Shared\projects	SMB
shared	D:\Shared\shared	SMB
Shared Folders	C:\ServerFolders\Shared Folders	SMB
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB
techn...	...\technical5	SMB
Users	...\Users	SMB

VOLUME
technical5 on server

Data (D:)
Capacity: 2.00 TB

Disk Used
■ 335 MB Used Space
□ 2.00 TB Free Space

QUOTA
technical5 on server

To use quotas, File Server Resource Manager must be installed.

To install File Server Resource Manager, start the Add Roles and Features Wizard.

Figure 51: List of shares within Server Manager

Launch *File Manager* and the structure of the volume will appear along the following lines. However, the thing to keep in mind is that such shared folders are ‘special’ and you should always manage them using Server Manager rather than File Manager.

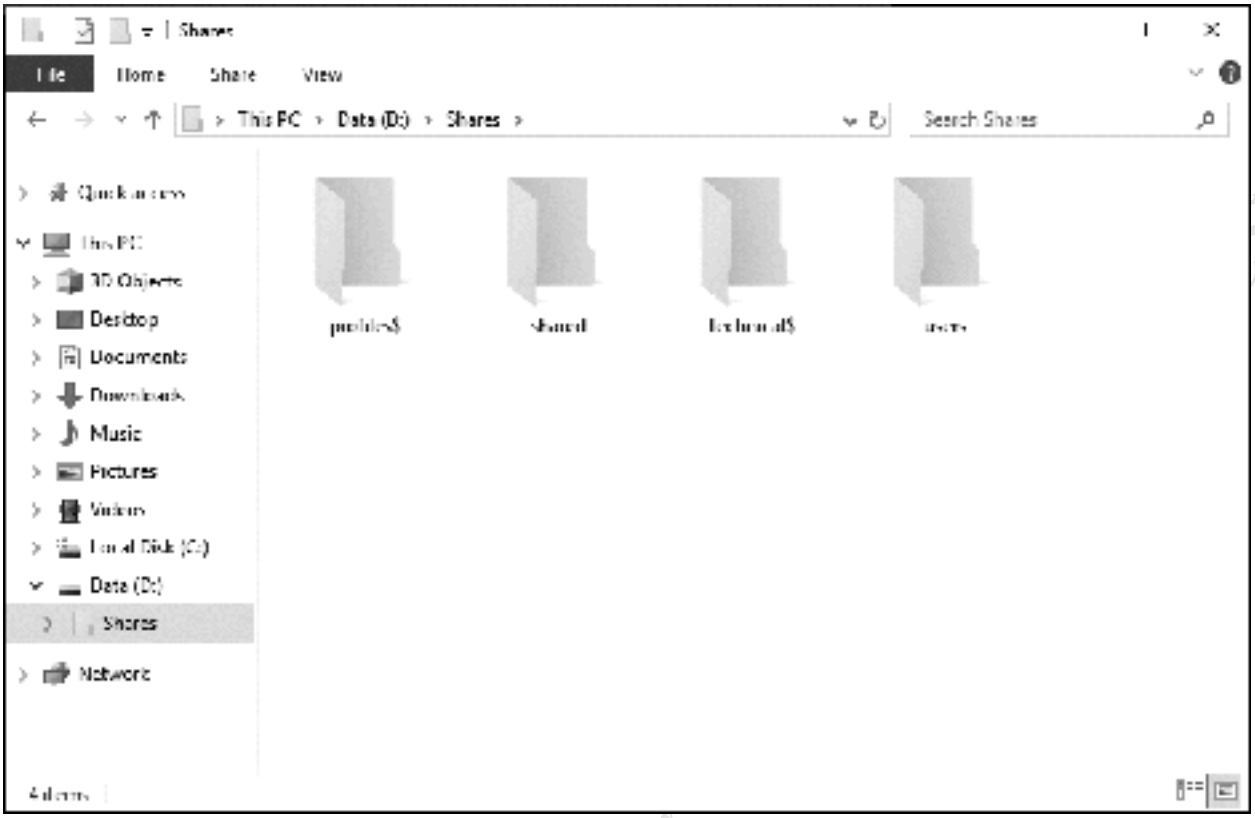


Figure 52: Listing of shares from File Manager

3.4 Loading Existing Data into Shared Folders

There may be a requirement to load data from existing computers or systems onto the server, into the new shared folders that have been created. There are a couple of ways to do so:

Method One: Wait until the network is up and running i.e. shared folders have been created, users have been defined, computers are connected and able to access the server. Then, connect from each computer and copy data from the user's folders to the appropriate folders on the server.

Method Two: Visit each individual computer and copy data from the user's folders to an external plug-in USB drive. Then, connect the USB drive to the server and copy it to the appropriate folders on the server. The advantage of this method is that it can be done before or in parallel with setting up the server.

Regardless of which method is used, an anti-virus/malware check should be run on the computers *before* copying any data. It is also a good idea to first review the data on the computers and prune (delete) any unrequired and duplicated data, rather than carry it forward to the new environment.

4. USERS

4.1 Overview

In order to access the server, each user needs an account. Before creating the user accounts, some thought should be given to a naming convention. As a general principle, aim for consistency. For user account names, two common conventions are to use the first name plus the initial of the surname, alternatively the initial of the first name plus the surname, although in some parts of the world other conventions might be more appropriate. In the case of particularly long names and double-barrelled names it might be a good idea to abbreviate them. For example:

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

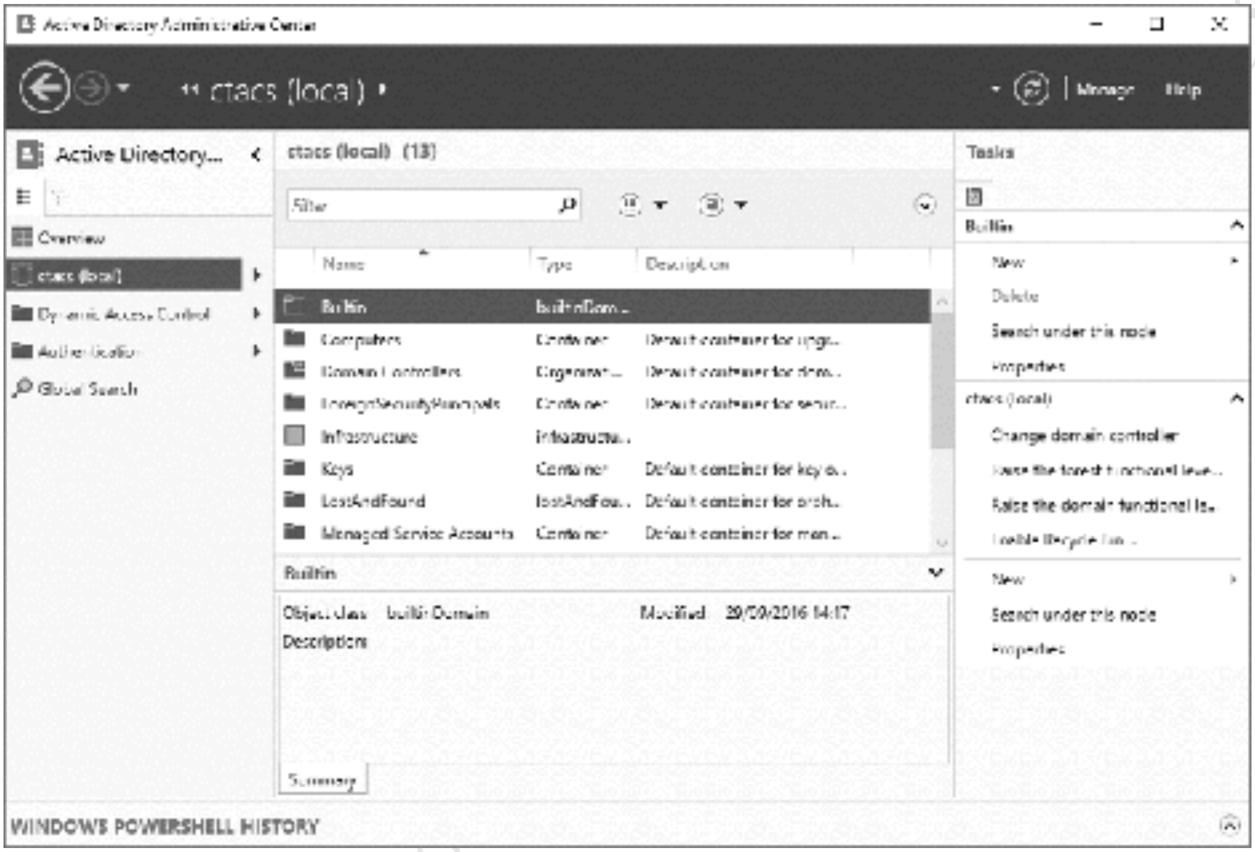
Alternatively:

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

Users are created and subsequently modified and managed using the *Active Directory Administrative Centre*.

4.2 Creating Users

Within *Server Manager*, click **Tools** in the top right-hand corner and choose **Active Directory Administrative Center** from the drop-down list. Alternatively click **Start** > **Windows Administrative Tools** > **Active Directory Administrative Center**. An *Overview* page is displayed; on the left-hand side of the screen click the domain name (*ctacs.local* in our example) to display the following screen:



Name	Type	Description
Builtin	builtinDom...	
Computers	Container	Default container for upgr...
Domain Controllers	Organizat...	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secur...
Infrastructure	infrastructu...	
Keys	Container	Default container for key c...
LostAndFound	lostAndFou...	Default container for orph...
Managed Service Accounts	Container	Default container for man...

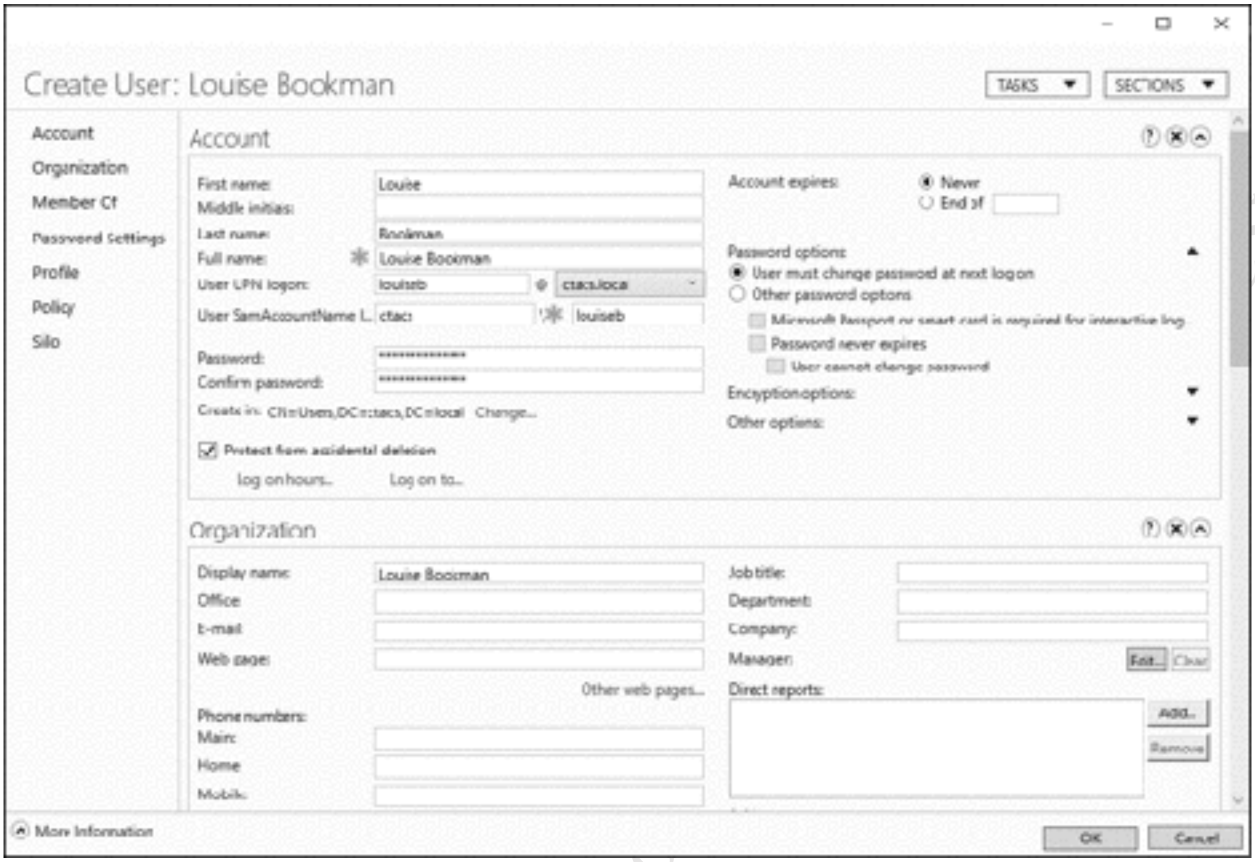
Builtin

Object class: builtinDomain   Modified: 29/09/2016 14:17
Description:

Figure 53: Active Directory Administrative Center

The screen comprises main sections: the left-hand one can be thought of as a top-level menu or control area; the centre one is the main work area; the right-hand one lists a number of tasks and its contents vary depending on what you are doing and where you are. In the above screenshot, the centre panel is listing *Containers*. Containers are the different type of objects that exist in the system and built-in ones include *Computers* and *Users* amongst others. By keeping objects in containers it makes them easier to manage and, in addition to the built-in ones, you can create your own. For instance, double-clicking the *Users* container reveals that the system already contains a number of pre-defined special users and groups (although some of them are never used, except in larger networks) including *Administrator.* When you create users on a small system, you can place them in the *Users* container. But in a large organization, with hundreds or maybe thousands of users, you may wish to create additional containers first and place them in those, organized according to department or location, for instance.

If you are viewing the initial screen as shown above, the right-hand panel will have a section under *Tasks* called *Builtin*. If you double-clicked the *Users* container, the *Builtin* section will have been replaced by the *Users* section. Either way, click **New** followed by **User** and the following panel opens:



Create User: Louise Bookman

Account

First name:	Louise
Middle initials:	
Last name:	Bookman
Full name:	Louise Bookman
User UPN logon:	louiseb @ ctacs.local
User SamAccountName L.:	ctacs\ louiseb
Password:	**************
Confirm password:	**************

Create in: CN=Users,DC=ctacs,DC=local

☑ Protect from accidental deletion

Account expires: ● Never ○ End of

Password options:

● User must change password at next log on

○ Other password options

□ Microsoft Passport or smart card is required for interactive log

□ Password never expires

□ User cannot change password

Organization

Display name:	Louise Bookman
Office:	
E-mail:	
Web page:	
Job title:	
Department:	
Company:	
Manager:	
Direct reports:	
Phone numbers: Main:	
Home:	
Mobile:	

Figure 54: Create User

Enter the user’s *First name* and *Last name*, which will auto-complete the *Full name* field. Specify the *User UPN logon* – which is the actual logon name - in accordance with the naming convention you are following. Specify and confirm a *Password*; the best passwords are: non-obvious; not the user’s name; not too short; a mixture of upper and lower case letters plus numbers and special characters (such as exclamation marks). It is suggested that you tick the **Protect from accidental deletion** box.

On the right-hand side of the form you would normally leave *Account expires* set to **Never**. However, if the user was, for example, a temporary employee or a student in a college you could specify a date upon which the account would automatically expire. Underneath it are some *Password options*:

User must change password at next log on – this is the default and is considered best practice. If instead you click *Other password options,* three other options become available:

Microsoft Passport or smart card is required for interactive log on – additional security that may be used in larger organizations

Password never expires and *User cannot change password* – useful when several people share an account or in some educational settings

As can be appreciated, there are many other options on the form relating to the creation of users and some will be considered below or later on. However, what we have entered is sufficient to create the user so click **OK**.

If the password does not meet the criteria described above a message to that effect will be displayed at the bottom of the screen, in which case you should correct the password and try again. Whilst not generally recommended, it is possible to remove the requirement for complex passwords altogether and how to do so is described in section 8.6 Changing the Password Policy.

Creating users can be time consuming. In a small network this may not be an issue, but in an organization with hundreds of users it may well be. Fortunately, tools are available to bulk-create users. A free one comes with Windows Server; it is called *csvde.exe* and is located in the *C:\Windows\System32* folder. The basic principle is that a CSV file containing the names of the users and other information is first created in, for instance, Excel. In some instances, it might be possible to generate a suitable file from another application, such as a payroll, human resources system or school ledger. Or, if this is a replacement network, a list of user names can be exported from Active Directory on the old system and then imported into Active Directory on the new one using *csvde.exe*. However, the tool is basic and some effort is still required. Easier and more sophisticated commercial alternatives are also available.

Creating Users Using PowerShell

Some people are wary of working using the command prompt, but it is a very efficient way of doing some tasks and, particularly if you have multiple users to create, somewhat quicker than other techniques. The caveat is that the users will be 'plain vanilla' and it will probably be necessary to later edit them or provide additional details using *Active Directory Administrative Centre*, but even so it can be a time saver.

You can use the traditional Command Prompt (if you are old enough you may still think of this as the 'DOS prompt') or the more sophisticated *Windows PowerShell*. PowerShell is located on the main Start menu; Command Prompt can be found at **Start** > **All apps** > **Windows System** > **Command Prompt**. Alternatively, you can press the **Windows** key and the letter **R** simultaneously, type **cmd** and press **Enter**.

Once you have a Command Prompt, type *net user username password /add /domain*

For example: *net user laurar !zel892!ee# /add /domain*

When you have finished creating the users, type **exit** and press **Enter** to return to the system.

If you are an experienced user, you will probably realise that you could create a script or batch file that could be used to create multiple users at once.

As mentioned, the user details will need to be filled out using *Active Directory Administrative Centre* and you may find the technique described at the end of this chapter to be of some help.

Bulk Creation of Users

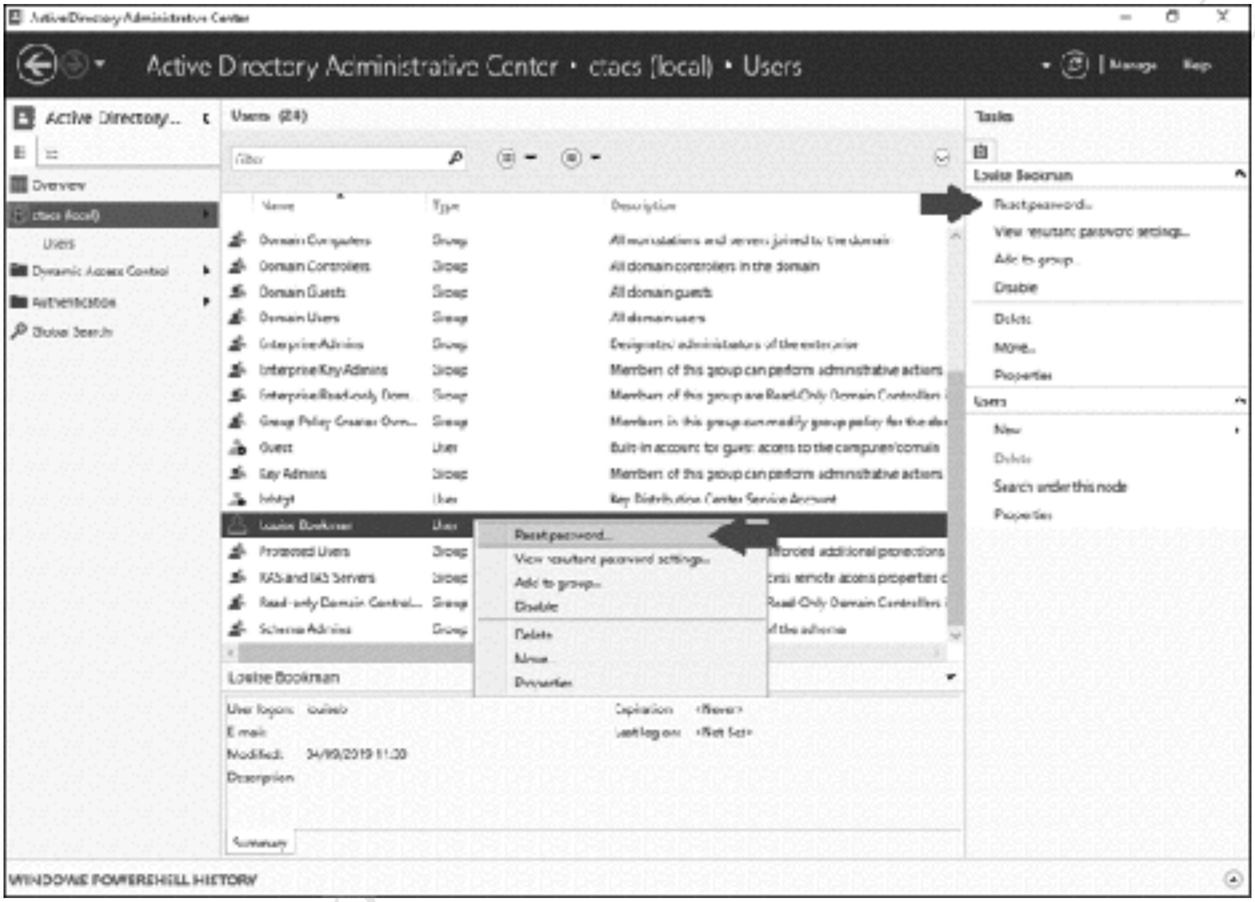
Creating users can be time consuming. In a small network this may not be an issue, but in an organization with hundreds of users it may well be. Fortunately, tools are available to bulk-create users. A free one comes with Windows Server; it is called *csvde.exe* and is located in the *C:\Windows\System32* folder. The basic principle is that a CSV file containing the names of the users and other information is first created in, for instance, Excel. In some instances, it might be possible to generate a suitable file from another application, such as a payroll, human resources system or school ledger. Or, if this is a replacement network, a list of user names can be exported from Active Directory on the old system and then imported into Active Directory on the new one using *csvde.exe*. However, the tool is basic and some effort is still required. Easier and more sophisticated commercial alternatives are also available.

Note for Users of Earlier Versions of Windows Server

If you have used earlier versions of Windows Server, you might like to know that the older tools for creating users are still available e.g. *Active Directory Users and Computers*, which can be located at **Server Manager** > **Tools** > **Active Directory Users and Computers** or by clicking **Start** > **All Apps** > **Windows Administrative Tools** > **Active Directory Users and Computers**. There are some differences between the old and the new methods, with the most noticeable one being that the multiple tabs of *Active Directory Users and Computers* have been replaced by a single 'one-stop-shop' form in the *Active Directory Administrative Center*.

4.3 Resetting a Password

There is commonly a need to reset or change a user's password; for instance, they may have forgotten it or it has become compromised. There is no way to find out what a user's password is or was; the only thing that can be done in such situations is to reset it to something different. To do so, go into the *Active Directory Administrative Center*, click the domain name and expand the *Users* container. Click on the user's name to highlight it and a list of tasks for the user will be displayed on the right-hand side of the screen; alternatively, right-click the user's name to display the same list. Click **Reset password**. In the resultant dialog box specify and confirm the new password, then click **OK**.



Name	Type	Description
Domain Computers	Group	All workstations and servers joined to the domain
Domain Controllers	Group	All domain controllers in the domain
Domain Guests	Group	All domain guests
Domain Users	Group	All domain users
Enterprise Admins	Group	Designated administrators of the enterprise
Enterprise Key Admins	Group	Members of this group can perform administrative actions
Enterprise Read-only Dom...	Group	Members of this group are Read-Only Domain Controllers
Group Policy Creator Own...	Group	Members in this group can modify group policy for the do
Guest	User	Built-in account for guest access to the computer/domain
Key Admins	Group	Members of this group can perform administrative actions
krbtgt	User	Key Distribution Center Service Account
Louise Bookman	User	
Protected Users	Group	nforced additional protections
RAS and IAS Servers	Group	ers remote access properties c
Read-only Domain Control...	Group	Read-Only Domain Controllers
Schema Admins	Group	f the schema

Louise Bookman

User logon: louiseb
E-mail:
Modified: 04/09/2019 11:30
Description:

Expiration: <Never>
Last log on: <Not Set>

Figure 55: Reset a password

4.4 Disabling an Account

When a user leaves the organization, their account should in the first instance be disabled to prevent it being used. It is preferable to do this rather than immediately deleting the account, as there may subsequently be a need to access it or the user may later return. Go into the *Active Directory Administrative Center*, click the domain name and expand the *Users* container. Click on the user's name to highlight it and a list of tasks for the user will be displayed on the right-hand side of the screen. Alternatively right-click the user's name to display the same list. Click **Disable**. To re-enable the user, repeat the process and click **Enable**.

4.5 Deleting an Account

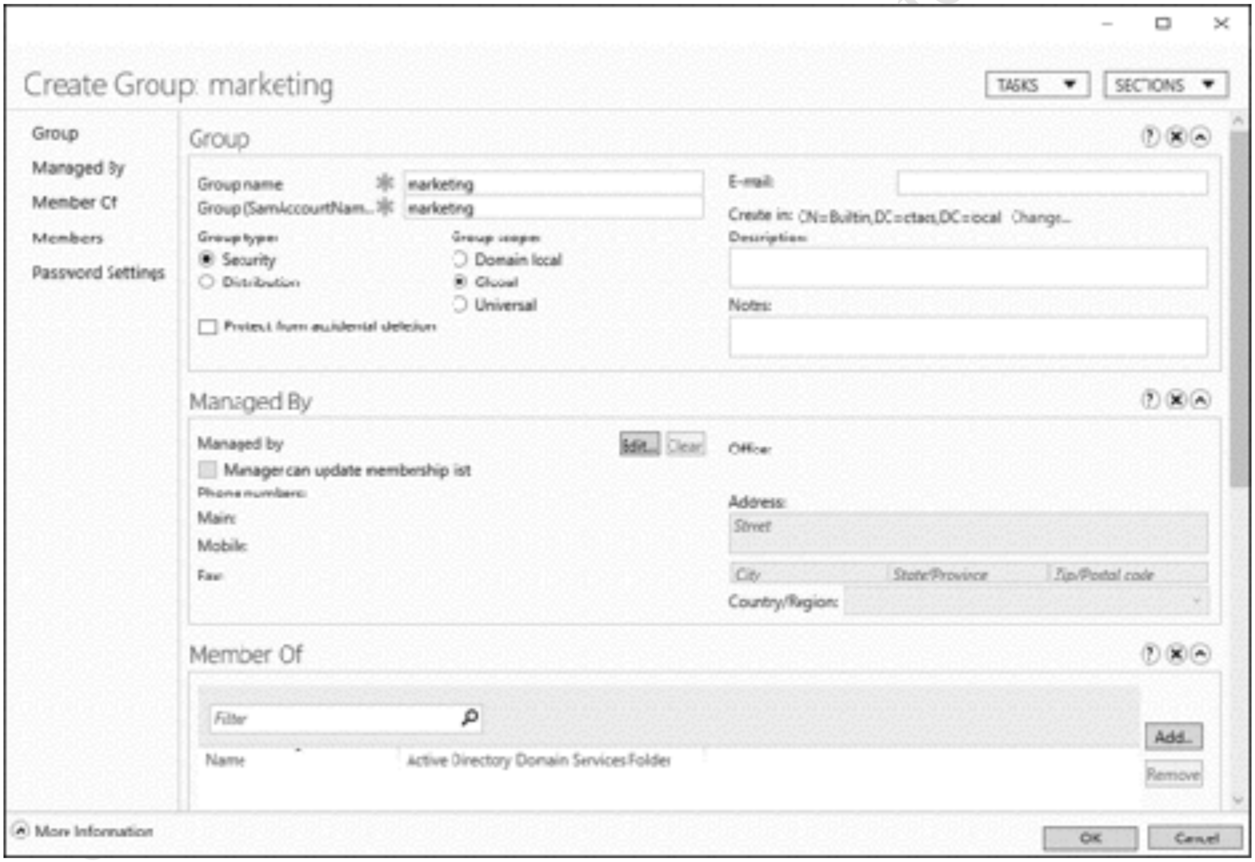
To delete an account, Go into *Active Directory Administrative Center* and drill-down to find the user as described above. Click on the user's name to highlight it and a list of tasks for the user will be displayed on the right-hand side of the screen. Alternatively, right-click the user's name to display the same list. Click **Delete**; a warning message is displayed – click **Yes** to continue.

4.6 User Groups

In an organization with a small number of users, specifying who has access rights to folders is fairly easy to manage. But if there are more users it becomes more time consuming; for instance, you might have to specify the level of access for hundreds or even thousands of 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, Windows Server features the concept of groups. A group consists of multiple users who have something in common within the organization, for instance they are all members of the same team. Access rights can be specified for a 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 new group, launch Server Manager and go into Active Directory Administrative Center. Click on the domain name and from the list of Builtin Tasks on the right-hand panel choose New > Group. The following screen is shown:



Create Group: marketing

Group

Group name * marketing
Group (SamAccountNam... * marketing
Group type: ● Security ○ Distribution
Group scope: ○ Domain local ● Global ○ Universal
□ Protect from accidental deletion
E-mail:
Create in: CN=Builtin,DC=ctacs,DC=local Change...
Description:
Notes:

Managed By

Managed by
□ Manager can update membership list
Phone numbers:
Main:
Mobile:
Fax:
Office:
Address:
Street
City State/Province Zip/Postal code
Country/Region:

Member Of

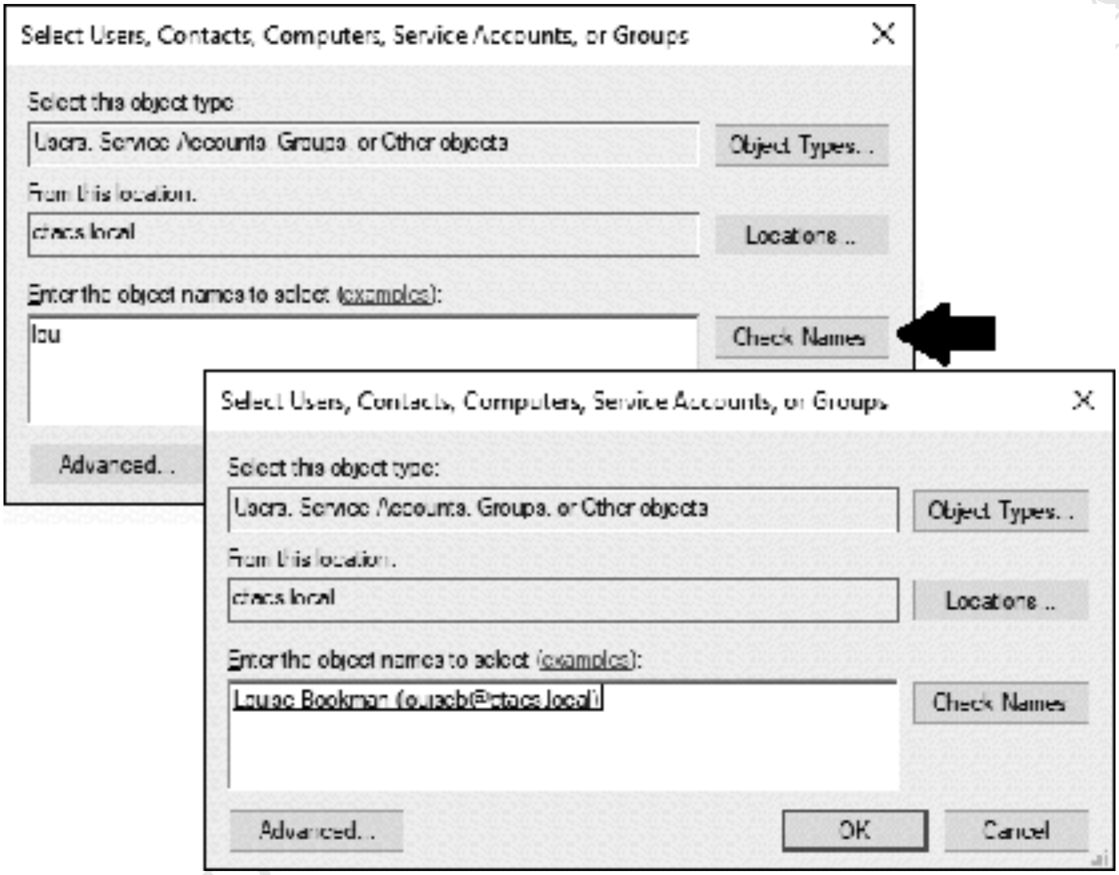
Filter
Name Active Directory Domain Services Folder

Figure 56: Creating a new Group

As when creating users, there are lots of possible options. But the only required ones are those towards the top of the screen. Enter the *Group name* and the *Group (SamAccountName)* and use the same value for both e.g. *marketing*. The *Group type* can be left with its default value of *Security* and the *Group scope* can be left with its default value of *Global* (the other options are not applicable in a small network). Click **OK**.

Having created the group, it now has to be populated with members (users) and there are two ways of doing so:

The first method is with the screen we have just used, either at the time of creating the group or by modifying it thereafter. Within the screen is a section titled *Members*; scroll down if necessary to find it and click the **Add** button. A small dialog box is displayed. Type in the name of the object, meaning the logon name of the user, and click the **Check Names** button. You do not have to type in the full name – just enough to make it unique. It will be validated and if found will then appear underlined. Click **OK** to add the user:



Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, Groups, or Other objects

From this location:
ctacs.local

Enter the object names to select (examples):
lou

Select Users, Contacts, Computers, Service Accounts, or Groups

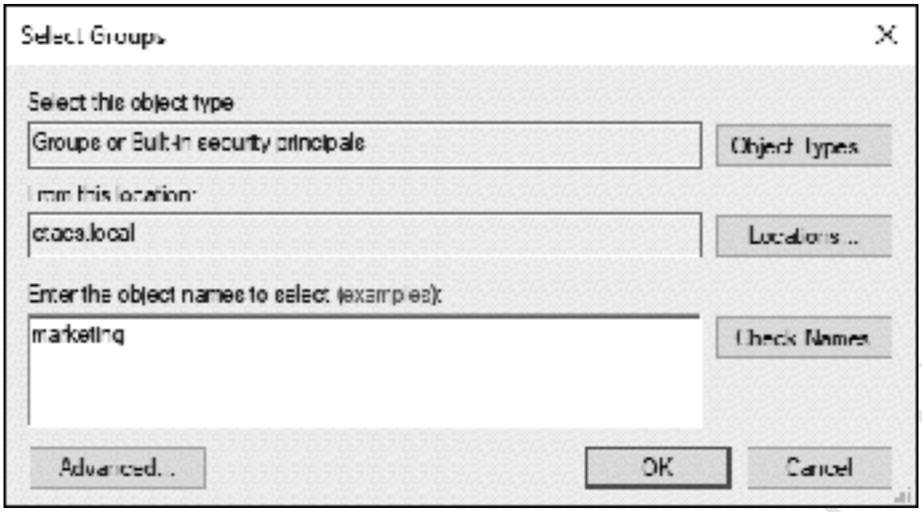
Select this object type:
Users, Service Accounts, Groups, or Other objects

From this location:
ctacs.local

Enter the object names to select (examples):
Louise Bookman (louiseb@ctacs.local)

Figure 57: Selecting a user to add to a group

The second method is to display the list of users within the *Active Directory Administrative Center*. Right-click a user, click **Add to group…** and the same dialog box as above is displayed. However, this time type in the name of the group – *marketing* in our example - and click the **Check Names** button. It will be validated and if correct will then appear underlined. Click **OK**.



Select Groups

Select this object type:

Groups or Built-in security principals

From this location:

ctacs.local

Enter the object names to select (examples):

marketing

Figure 58: Selecting a group

4.7 Home Folders, User Profiles and Logon Scripts

Chapter 3 outlined a structure of shared folders for the system. To help make the network workable from a user perspective there are three, related mechanisms: *Home folders*, *User profiles* and *Logon scripts*.

Home folders – each user can have a home or personal folder, where they can store data on the network that they can then access from any computer, but which they do not need to share with other people. In our design, these will reside under the shared *users* folder.

User profiles - a user profile is a collection of settings that personalize a computer for a particular user, including the desktop background (wallpaper), screen saver, sounds, toolbars and so on. Using a technique called *roaming profiles*, a user's profile is automatically picked up no matter which computer they login to, giving them a consistent, personalized environment.

Logon script – many users are accustomed to working with drive letters e.g. C: drive, D: drive and so on, and hence it is useful to be able to relate the shared folders to drive letters in a process known as *drive mapping*. Logon scripts are executed when a user logs on and are commonly used to map drives (although can do other things as well).

Home Folders

Using *File Explorer*, navigate to the shared *Users* folder that we created previously and now create individual folders within it for each user; the names of the folders must correspond **exactly** to the names of the users as created in section 4.2 Creating Users. These are ordinary folders and can be created by clicking the *New Folder* icon on the *Home* tab of the *Quick Access Toolbar* or Ribbon, or by right-clicking and choosing **New** > **Folder**, or by pressing **Shift Ctrl N** simultaneously:

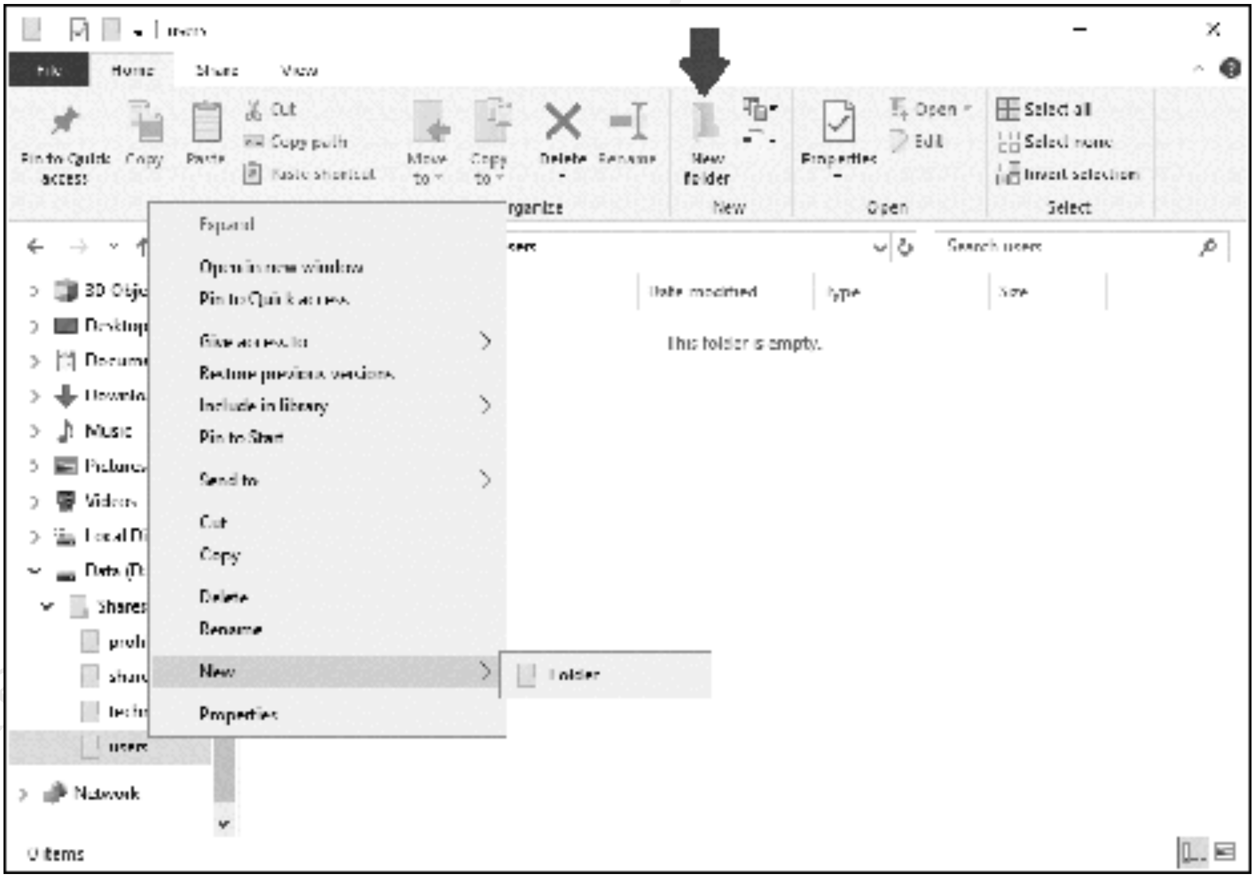
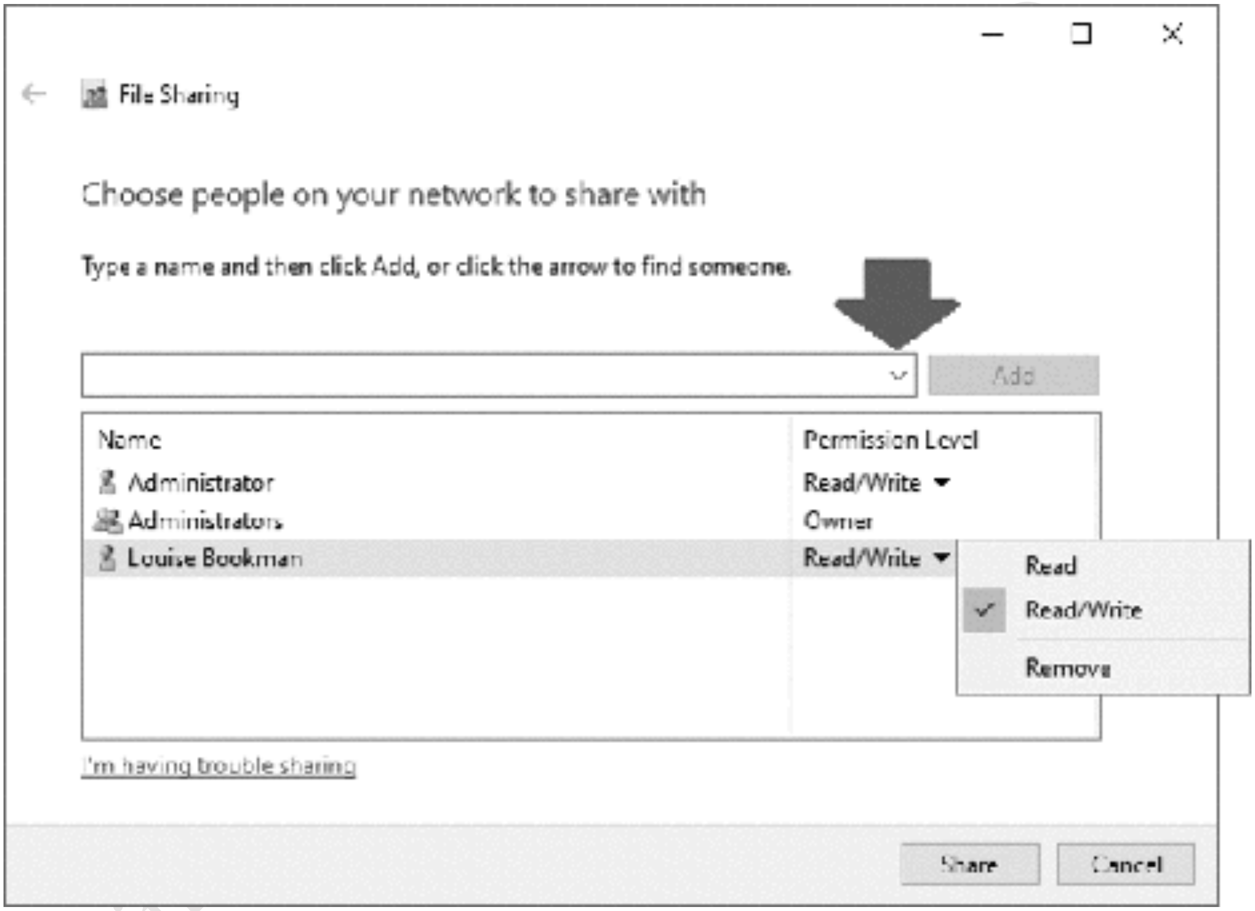


Figure 59: Create a new folder

The question of security needs to be considered. As things stand, any user can access any other user's home folder; in other words, the folders are *personal* but they are not *private*. In a very small business setting this might not be an issue, in which case you can skip to the next section. But if it is, then access to the home folders can be controlled and this is done as follows:

Right-click on a particular user's home folder and choose **Share with** > **Specific people..**. On the panel that appears enter the user's logon name and click **Add**. Alternatively, click the chevron on the drop-down (as indicated by large arrow in below illustration) and click **Find people**. Enter some of the user's name and click **Check Names** – if the user is found the name will be corrected and appear underlined, at which point click **OK**. Having added the user, click on **Permission Level** against their name and change it from *Read* to *Read/Write* and click the **Share** button. After a few seconds, there will be a confirmatory message that the folder is now shared – acknowledge it by clicking **Done**. **Repeat** this step for all the users in turn, so that each user is sharing just their own individual folder:



File Sharing

Choose people on your network to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
Administrator	Read/Write ▾
Administrators	Owner
Louise Bookman	Read/Write ▾

Figure 60: Specifying the permissions

As can be appreciated, this process could become time consuming on a large system with hundreds or even thousands of users, but is acceptable on small systems. In a corporate environment Microsoft would suggest the use of a feature called *Work Folders*, although it is unduly complicated for a small network.

User Profiles

One thing to note is that user profiles have evolved through the different versions of Windows Server and Windows Clients. Windows XP used the original profile format; Windows Vista, Windows 7 and Windows 8 use V2 ('Version 2') profiles, plus there are some subtle variations between V2 profiles in Windows 7 and those in Windows 8. Windows 10 uses V5 ('Version 5' profiles). When a user connects for the first time, the profile folder is created automatically for that user, with a name based upon the username plus a possible suffix. For instance, suppose *louiseb* logged on using a Windows XP machine – a profile named *\\server\profiles$\louiseb* would be created. If she then logged on using a Windows 7 computer, a profile named *\\server\profiles$\louiseb.v2* would be created. Finally, if she logged on using a Windows 10 machine a third profile named *\\server\profiles$\louiseb.v5* would be created. All of these profiles can exist concurrently, but note that the features they support vary. For instance, if she set her wallpaper whilst using a Windows 7 machine, it would not be the same on the Windows XP computer. Best practice? If possible, have all the client computers in the organization running the same version of Windows.

Logon Scripts

There are several techniques for creating logon scripts but the simplest method is via a cmd file (also known as a batch file). Using Notepad or another simple text editor, create two batch files named *user.cmd* and *admin.cmd* as shown below. These should be placed in *C:\Windows\sysvol\sysvol\domainname.local\scripts* where *domainname.local* is the name of the domain. This folder is automatically mapped by the server as a share called *NETLOGON*. It is assumed that you have called the server *'server'* – if this is not the case you will need to amend the scripts accordingly:

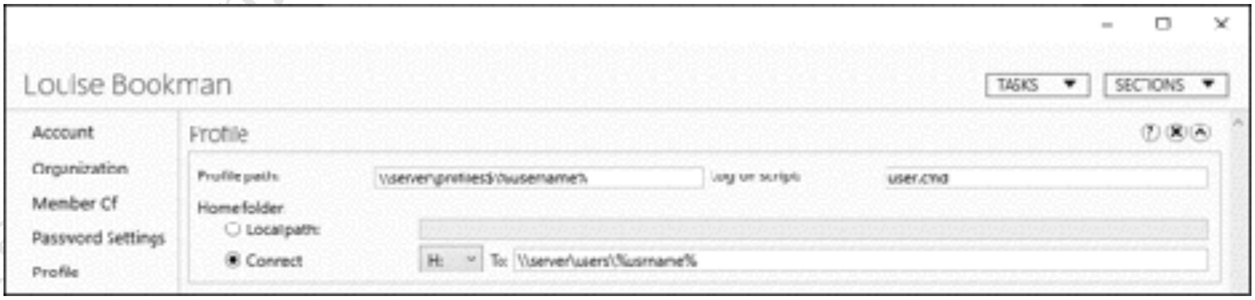
User.cmd script:

```
@echo off
: User logon script
net use s: \\server\shared /persistent:no
```

Admin.cmd script:

```
@echo off
: Admin logon script
net use s: \\server\shared /persistent:no
net use t: \\server\technical$ /persistent:no
```

The logon file now needs to be associated with the user accounts. Go into *Active Directory Administrative Center*, drill-down through the list of users and double-click on one to display their details. Scroll down to the section called *Profile* and specify the *Profile path* and the *Log on script*. The Profile path takes the form *\\server\profiles$\%username%*; note the use of the *%username%*, which is a *system variable* that Windows Server will automatically associate with the user as they login. For general purpose users, the login script is *user.cmd* whilst for the Administrator it is *admin.cmd*. In the *Home Folder* area choose *H:* from the **Connect** drop-down and specify a value of *\\server\users\username* for it e.g. *\\server\users\aarong*. Click **OK**.



Profile

Profile path: \\server\profiles$\%username%

Log on script: user.cmd

Home folder

○ Local path:

● Connect H: To: \\server\users\%usrname%

Figure 61: Specify user profile details

The effect of this is that when a user logs on they will have access to two network drives. The shared folder that everyone can see will appear as *S:* whilst their personal or home folder will appear as the *H:*

drive. For the Administrator user(s), specify a logon script of *admin.cmd* rather than *user.cmd*, which will map the shared, home and technical folders.

Troubleshooting: if the home folder is not mapped or the profile does not appear to be working, explicitly specify the user's login name rather than the *%username%* system variable. For example, user *dpetrova* would have a profile path of *\\server\\profiles$\dpetrova* and the H: drive would connect to *\\server\users\dpetrova*.

Editing Multiple Users Simultaneously

A useful time saver when assigning profiles to users is the ability to work with multiple users simultaneously. Go into *Active Directory Administrative Center*, locate the users and, holding down the Control key, click them one at a time to highlight them. Then, right-click one and choose **Properties** from the pop-up menu. A subset of the main screen but with four sections is displayed: *Account*; *Organization*; *Member Of* and *Profile*. Scroll down to **Profile** – this is the same dialog box as shown above but anything entered here will apply to all the selected users. It is thus a very fast way of assigning, say, the same logon script to many users at once.

5. CONNECTING DEVICES TO THE SERVER

5.1 Overview

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

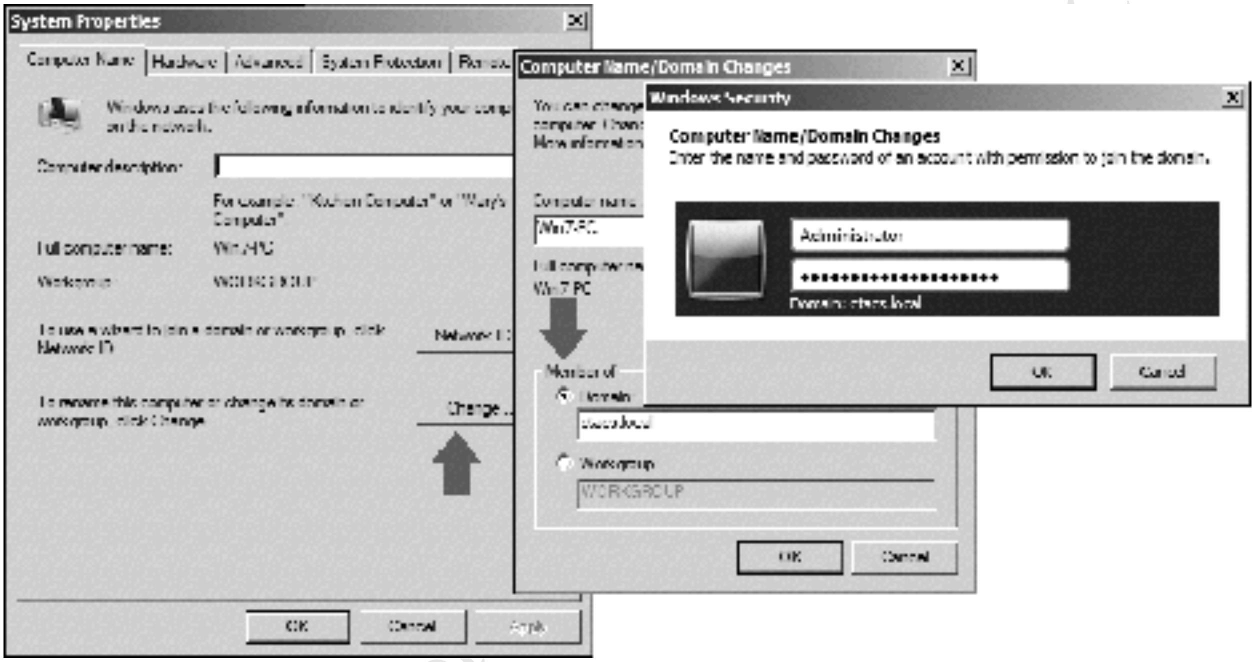
- The computer has to be running a Professional or better version of Windows, such as Windows 7 Professional with SP1 or Windows 10 Professional.
- The latest Windows updates should first be applied to the computer.
- Each computer must have a unique name within the network to identify it. It is best to follow a scheme of some description: this could be as simple as PC01, PC02, PC03 etc., or one that relates to its location or function. To change the name of a Windows 10 computer:
  Right-click the **Start** button and choose **System** > **About**; under *Device specifications*, click **Rename this PC**; enter the new name and click **Next**. To change the name of a Windows 7 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; if you are working on a wireless laptop, temporarily use an Ethernet cable and plug it in.
- Logon to the computer as a local administrator or other user that has administrative rights.

Computers using Home or Starter editions of Windows cannot be added to the domain; however, see section 5.5 Connecting Computers with Home Editions of Windows for a limited workaround. There are several different methods for connecting Macs – see section 5.6 Connecting Macs. Linux computers can be connected in a limited manner, described in section 5.7 Connecting Linux Computers. To connect iOS tablets and smartphones, albeit in a limited fashion, see section 5.8 Accessing the File System with File Browser.

5.2 Adding a Computer to the Domain

Connecting Windows 7 Clients to the domain

Click the **Start** button, right-click **Computer** and 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.
In the *Member of* section, click on **Domain**. Enter the name of your domain, followed by the .local suffix (for example, *ctacs.local).*
You will be prompted to enter the Administrator name and password for the domain. Do so and click **OK**.



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer"

Full computer name: Win7-PC

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Computer name: Win7-PC

Full computer name: Win7-PC

Member of

○ Domain: ctacs.local

○ Workgroup: WORKGROUP

Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

Administrator

****

Domain: ctacs.local

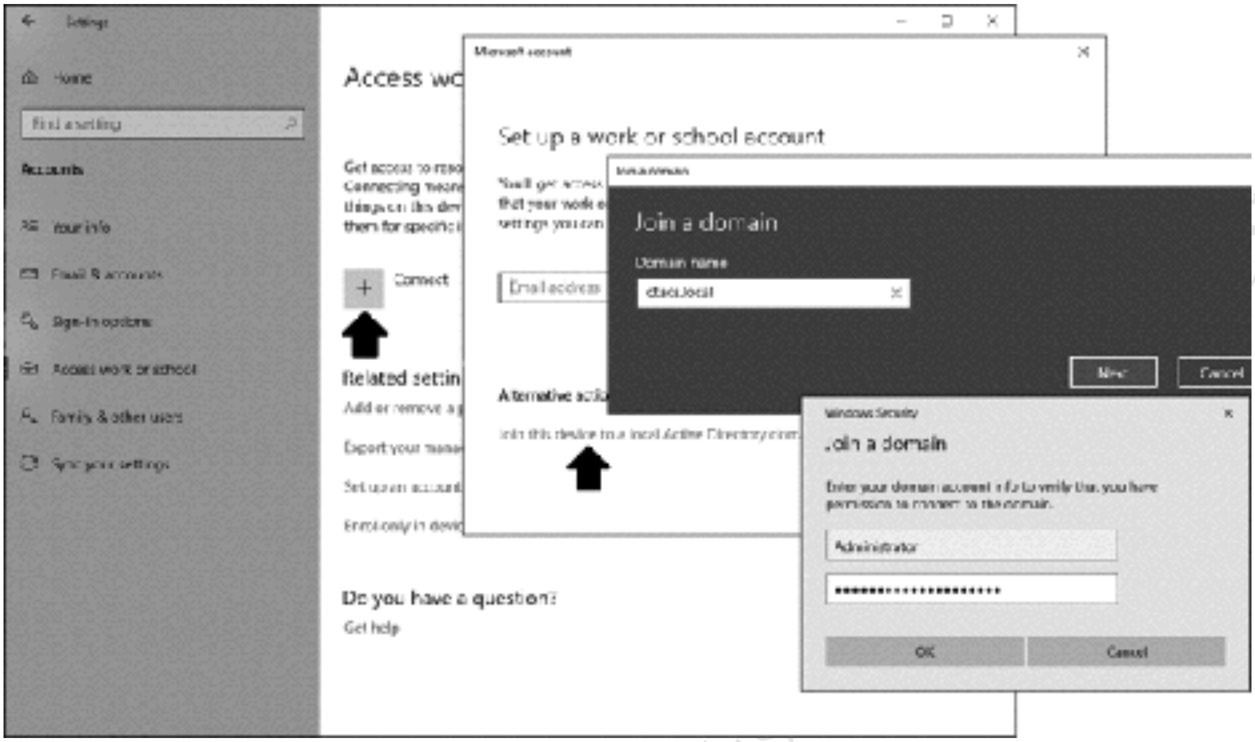
Figure 62: Adding Windows 7 computer to domain

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. Note: you may need to choose other user and specify the logon name as *domain\Administrator* e.g. *ctacs\Administrator.*

Connecting Windows 10 Clients to the domain

Note: it is recommended that the computer should have initially been setup to use a local account rather than an online Microsoft account.

Click **Start** > **Settings** > **Accounts** > **Access work or school.**
Click **Connect+**
On the resultant panel, ignore the email box and instead click the **Join this device to a local Active Directory domain** link at the bottom of the screen.
Enter your *Domain name* followed by the .local suffix e.g. *ctacs.local* in our example.
When prompted, enter the Administrator name and password for the domain. Do so and click **OK**.



Domain name: ctacs.local

Administrator

Figure 63: Adding Windows 10 computer to domain

An additional panel pops up, enabling you to add an account for the person who will be using the computer: ignore it by clicking **Skip**.
Follow the instructions to restart the computer.
Check that you can logon as Administrator. Note: you may need to choose Other user and specify the logon name as *domain\Administrator* e.g. *ctacs\Administrator*.

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 8.1 Clients to the domain

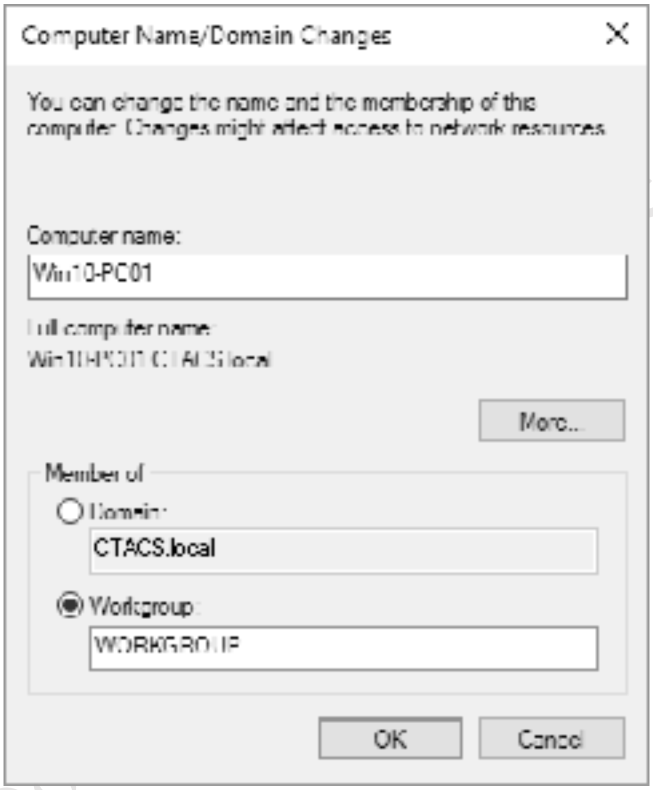
A couple of considerations apply when using Windows 8. Firstly, when installing or configuring Windows 8, specify that it is to use a local ID rather than a Microsoft ID. Secondly, make sure that it is running Windows 8.1 (a free upgrade from Windows 8 to Windows 8.1 is available through the Windows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

5.3 Removing a Windows Computer from the Domain

There is sometimes a need to remove a computer from the domain, for instance when it is being decommissioned or replaced. Very rarely, an existing computer may develop problems connecting to the server and sometimes the solution is to remove and then add it back to the domain.

To remove a Windows computer that is connected to the domain, go into **Control Panel** and click **System** followed by **Change Settings**. On the **Computer Name** tab, click the **Change** button. The computer will currently be a member of the domain. Click **Workgroup** and enter a name for it – it can be anything you wish but the usual convention is to call it *Workgroup*. Click **OK**. You may have to enter administrative credentials and restart the computer when prompted.



Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
Win10-PC01

Full computer name:
Win10-PC01.CTACS.local

Member of

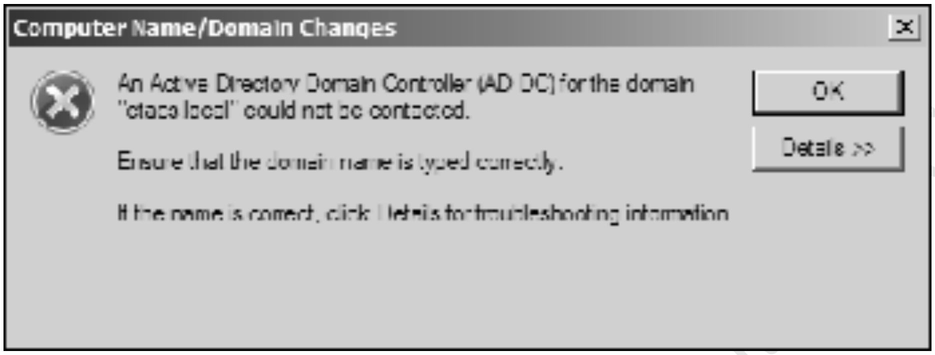
○ Domain:
CTACS.local

● Workgroup:
WORKGROUP

Figure 64: Computer Name/Domain Changes

5.4 Troubleshooting DNS Settings with All-in-One Routers

In a very small business, internet connectivity is frequently through an all-in-one router that also provides DHCP and DNS services, rather than have Windows Server itself provide DHCP and DNS. This can cause problems with DNS, such that computers on the network cannot “see” each other. Therefore, attempting to connect a computer to the server may result in failure, with a message to the effect that “a domain controller cannot be found”:



Computer Name/Domain Changes

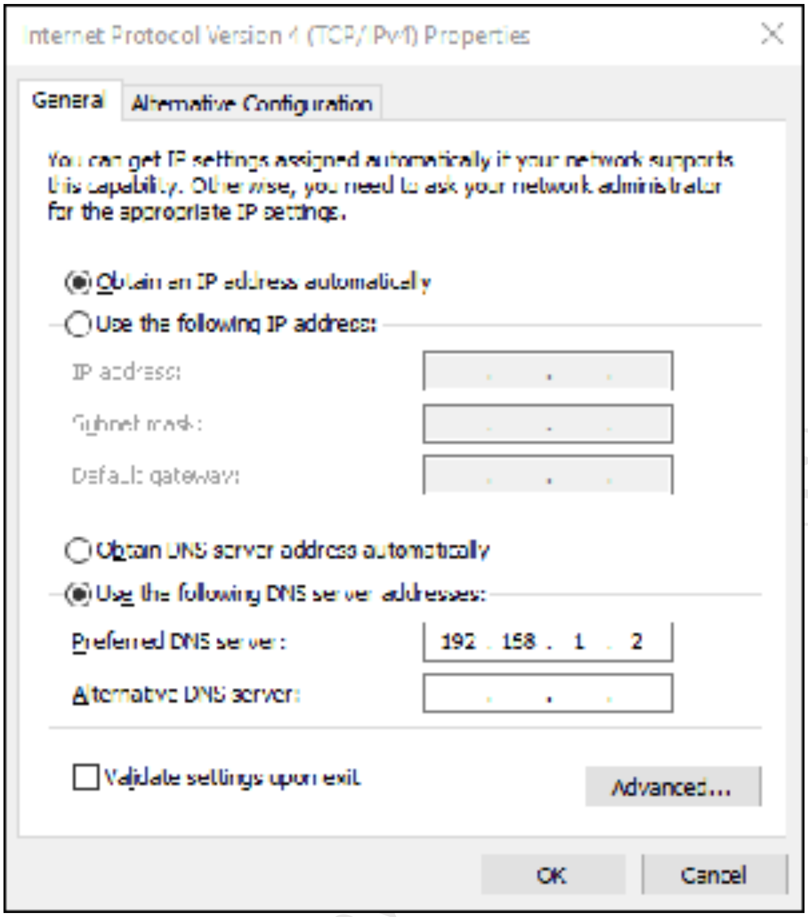
An Active Directory Domain Controller (AD DC) for the domain "ctacs.local" could not be contacted.

Ensure that the domain name is typed correctly.

If the name is correct, click Details for troubleshooting information

Figure 65: DNS-related error

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). Highlight **Internet Protocol Version 4 (TCP/ Ipv4)** and click **Properties**. 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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternative Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 158 . 1 . 2

Alternative DNS server: . . .

□ Validate settings upon exit

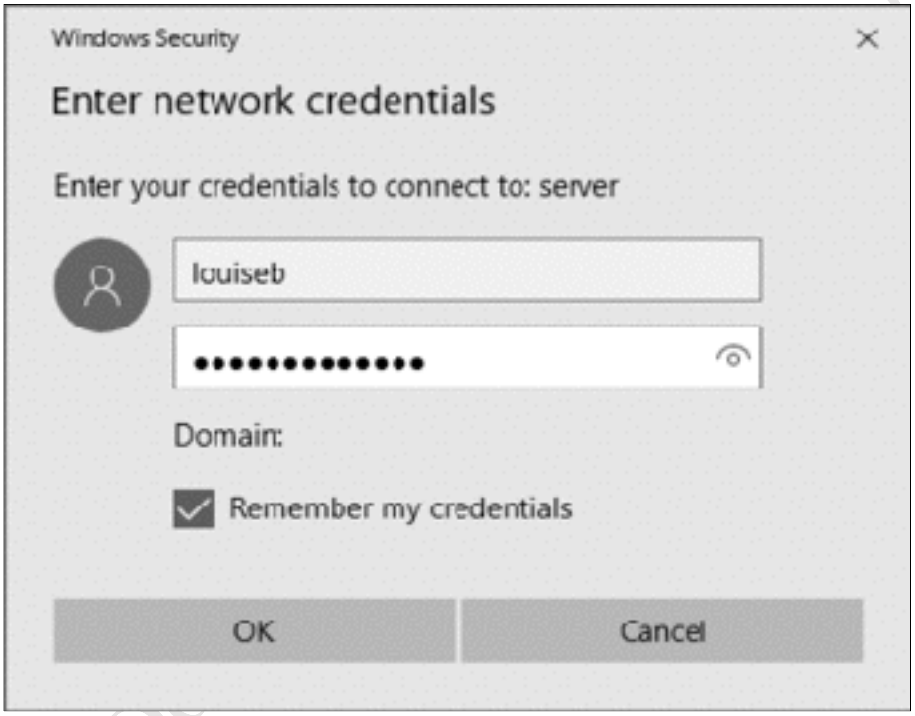
Figure 66: Manually specify the DNS server

If this still does not work, also try disabling IPv6 protocol on the client computer (provided your organization does not need to use IPv6 for some reason).

5.5 Connecting Computers with Home Editions of Windows

In theory, only computers running recent versions of Windows Professional or better can be connected to Windows Server. However, it is feasible to connect computers running Home Editions of Windows from Windows XP upwards, albeit in a simplified fashion. It will be possible to access the shared data folders, but not take advantage of the specific features that Windows Server offers in terms of control and management.

To connect a computer running a Home Edition of Windows, click **Start** (or right-click **Start** in 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. *\\192.168.1.253*). 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:



Windows Security

Enter network credentials

Enter your credentials to connect to: server

louiseb

••••••••••••••

Domain:

☑ Remember my credentials

Figure 67: Enter user name and password

A list of shared folders on the server will be displayed:

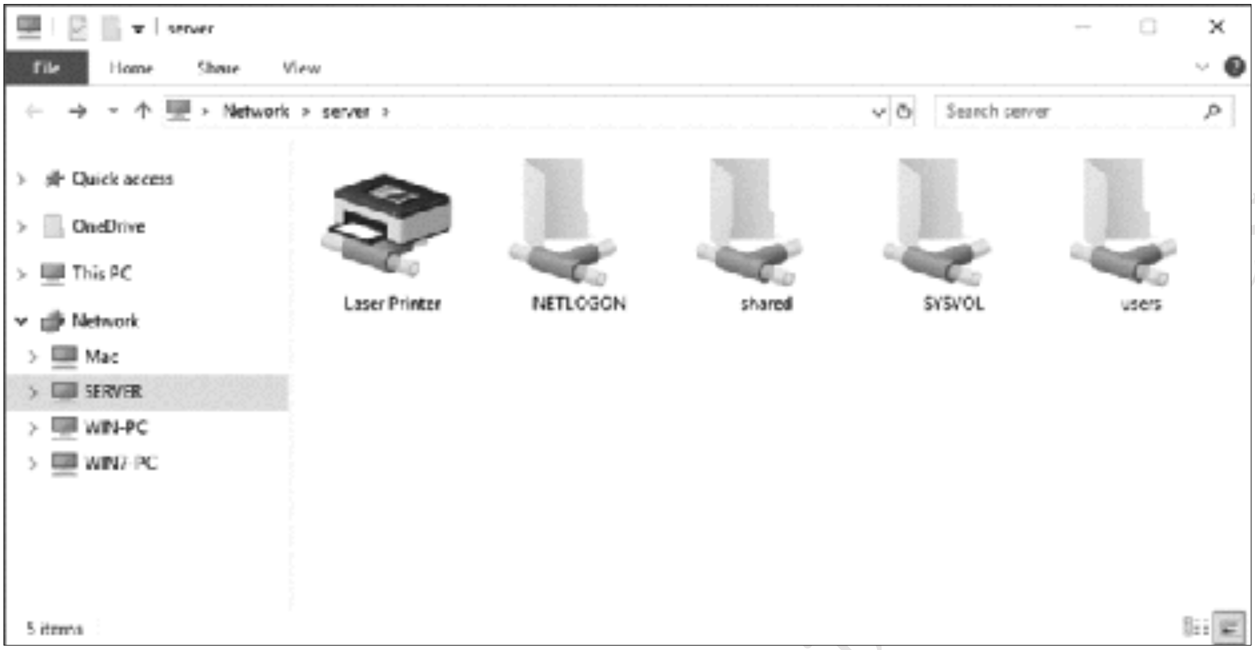


Figure 68: List of network folders

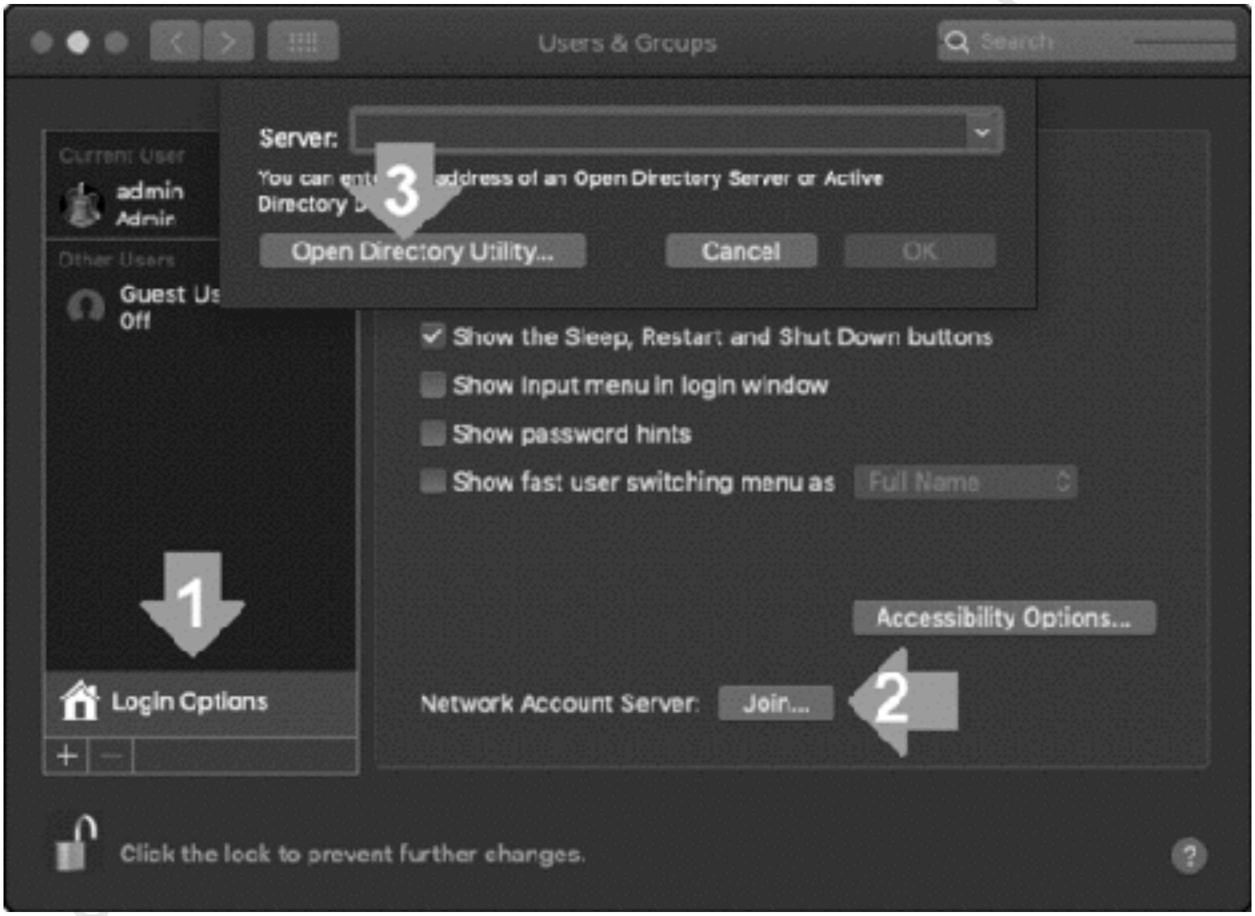
The user can work with any of the folders to which they have been granted access. To access their home folder, they should double-click the *Users* folder then double-click the folder that has their user name. Note that although they can see the names of other people's home folders, they will not be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

5.6 Connecting Macs

Most organizations using Windows Server will be working with Windows client PCs. However, many organizations will also have some Macs as well, perhaps to meet specialized requirements or simply through preference and these can be connected to the network using a variety of techniques: they can be added to the domain; they can be equipped with Windows and connected in exactly the same way as the organization’s other Windows PCs; they can be connected as workgroup computers.

Adding to the Domain

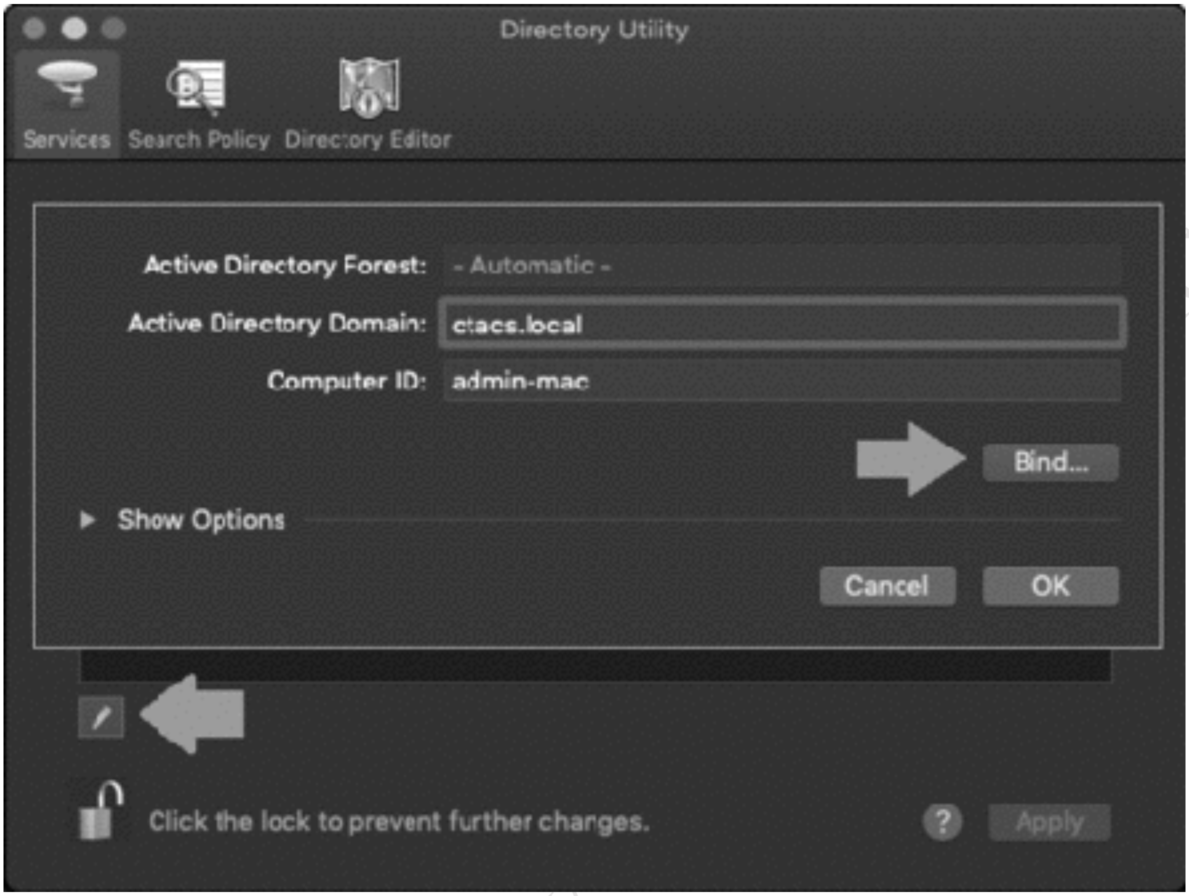
Login as a user with local admin rights on the Mac. To prevent possible DNS issues, ensure that both the server and the router have their IP addresses entered on the Mac’s network adaptor: **System Preferences** > **Network** > **Advanced** > **DNS**. Then, go into **System Preferences** > **Users & Groups**. Open the padlock – you may need to provide details of a user with administrative rights. Click **Login Options** then click the **Join** button next to *Network Account Server*. On the pop-up panel click **Open Directory Utility**:



☑ Show the Sleep, Restart and Shut Down buttons
□ Show Input menu in login window
□ Show password hints
□ Show fast user switching menu as Full Name

Figure 69: Login Options

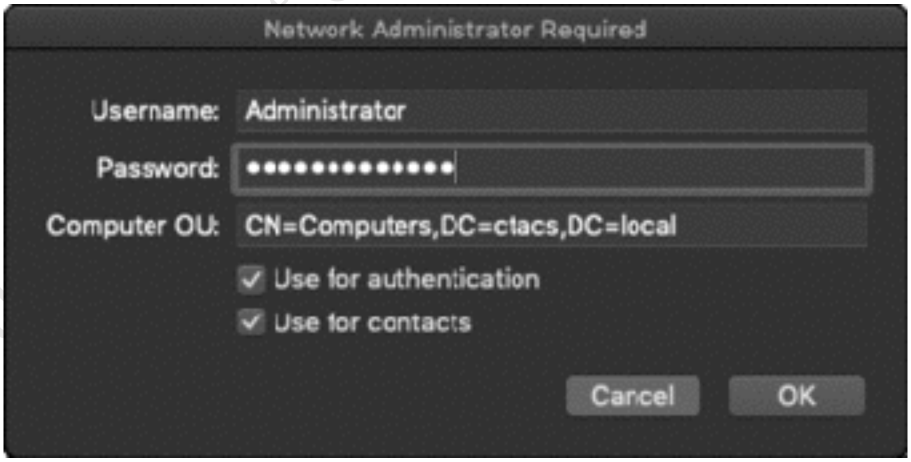
On the *Directory Utility* panel, open the padlock by providing admin credentials and clicking **Modify Configuration**. Highlight **Active Directory** and click the mini pencil icon to make changes. Type in the name of the Active Directory Domain and click **Bind**. Note: you may be prompted to enter the local admin credentials numerous times during this process.



Active Directory Forest: - Automatic -
Active Directory Domain: ctacs.local
Computer ID: admin-mac

Figure 70: Enter details of the domain

Enter the logon credentials for the administrator of the server and click **OK**:



Username: Administrator
Password: ••••••••••••••
Computer OU: CN=Computers,DC=ctacs,DC=local
☑ Use for authentication
☑ Use for contacts

Figure 71: Enter details for the domain administrator

After a short while you will be added to the domain.

Whilst this method works on a technical level, it does not actually do very much and the support from both Microsoft and Apple has been described as ‘lukewarm’.

Running Windows on the Mac

All modern Macs can run Windows in addition to macOS, thus enabling them to connect and behave exactly the same (from a networking perspective) as a regular Windows PC. If this is done, the Mac is then added to the domain using the technique detailed in section 5.2 Adding a Computer to the Domain.

There are two methods of running Windows on a Mac:

Boot Camp: Apple's Boot Camp utility is a standard component of macOS, located in the Applications > Utilities folder. The Boot Camp Assistant partitions the Mac's hard drive, allowing a copy of Windows to be installed. At startup time, macOS or Windows can then be selected. 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 macOS, 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.

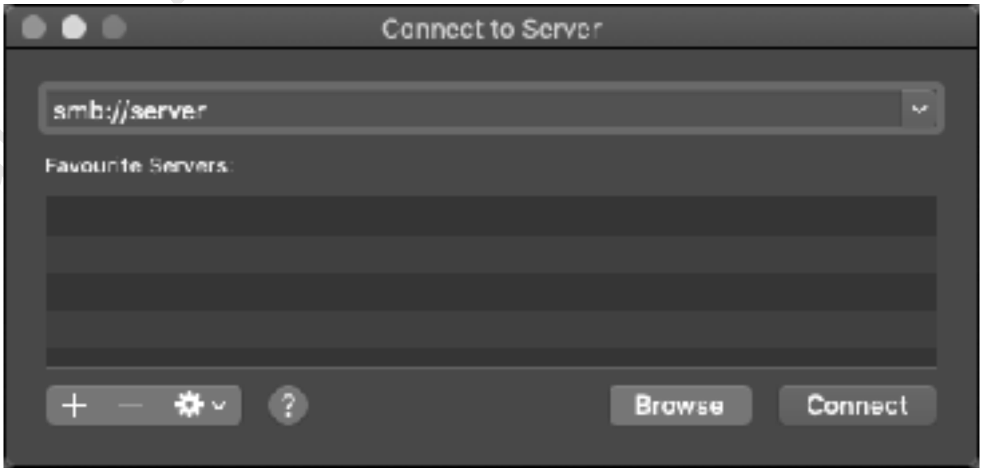
Virtualization Software: This enables the Mac to operate as normal under macOS and run a separate copy of Windows in its own self-contained window at the same time, as though it was just another application. This is particularly useful where a user prefers to work predominantly in a Mac environment, 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. 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 licensed copy of Windows still has to be obtained and used for the installation. This needs to be a Professional edition or better.

Connecting as a Workgroup Member

Rather than connect to the domain in the 'proper' way, Macs can be connected as Workgroup members, analogous to the manner in which computers running unsupported versions of Windows can be, as described in section 5.5 Connecting Computers with Home Editions of Windows. The technique is as follows:

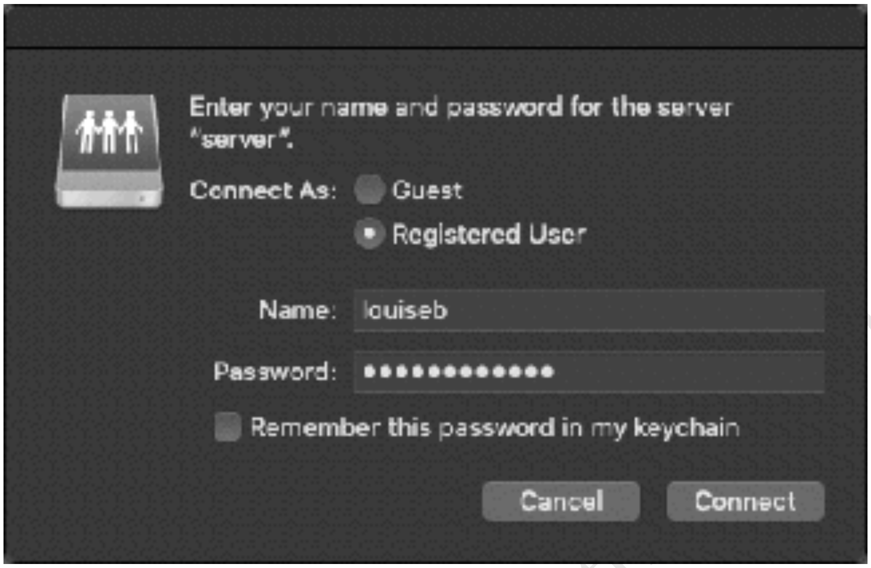
From Finder click **Go** followed by **Connect to Server** (or use **Command K** as a shortcut). On the resultant dialog box enter *smb://* followed by the name of the server or its internal IP address e.g. *smb://server* or *smb://192.168.1.253*. Click **Connect**:



smb://server

Figure 72: Enter the name or address of the server

You will be prompted for details of a Registered User; enter the user's name and password (as defined on the server) and optionally tick the **Remember this password in my keychain** box:



Enter your name and password for the server "server".

Connect As: ○ Guest

● Registered User

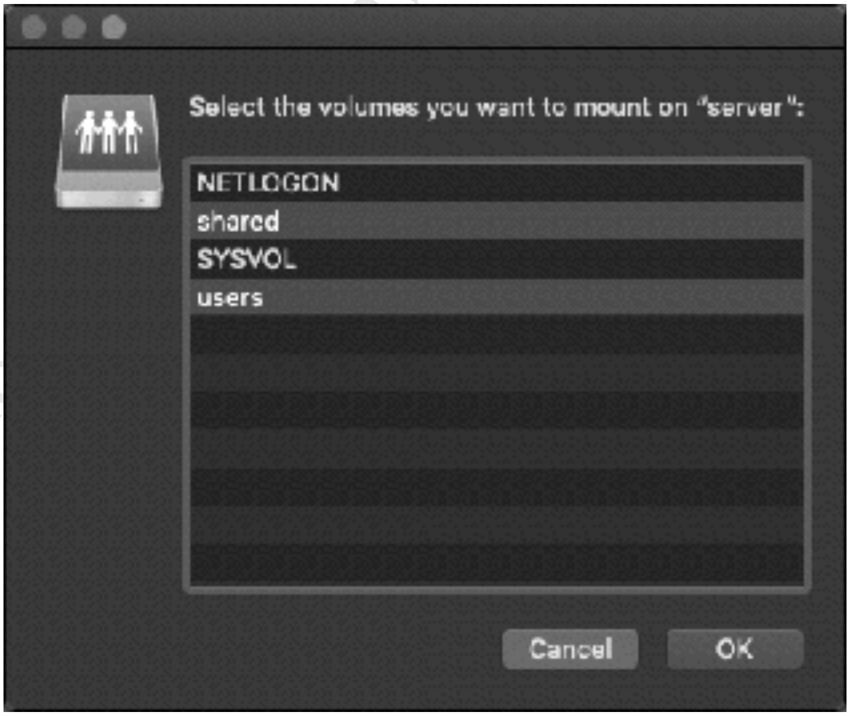
Name: louiseb

Password: ••••••••••••

□ Remember this password in my keychain

Figure 73: Enter the user's name and password from the server

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 and to which they may not have permissions:



Select the volumes you want to mount on "server":

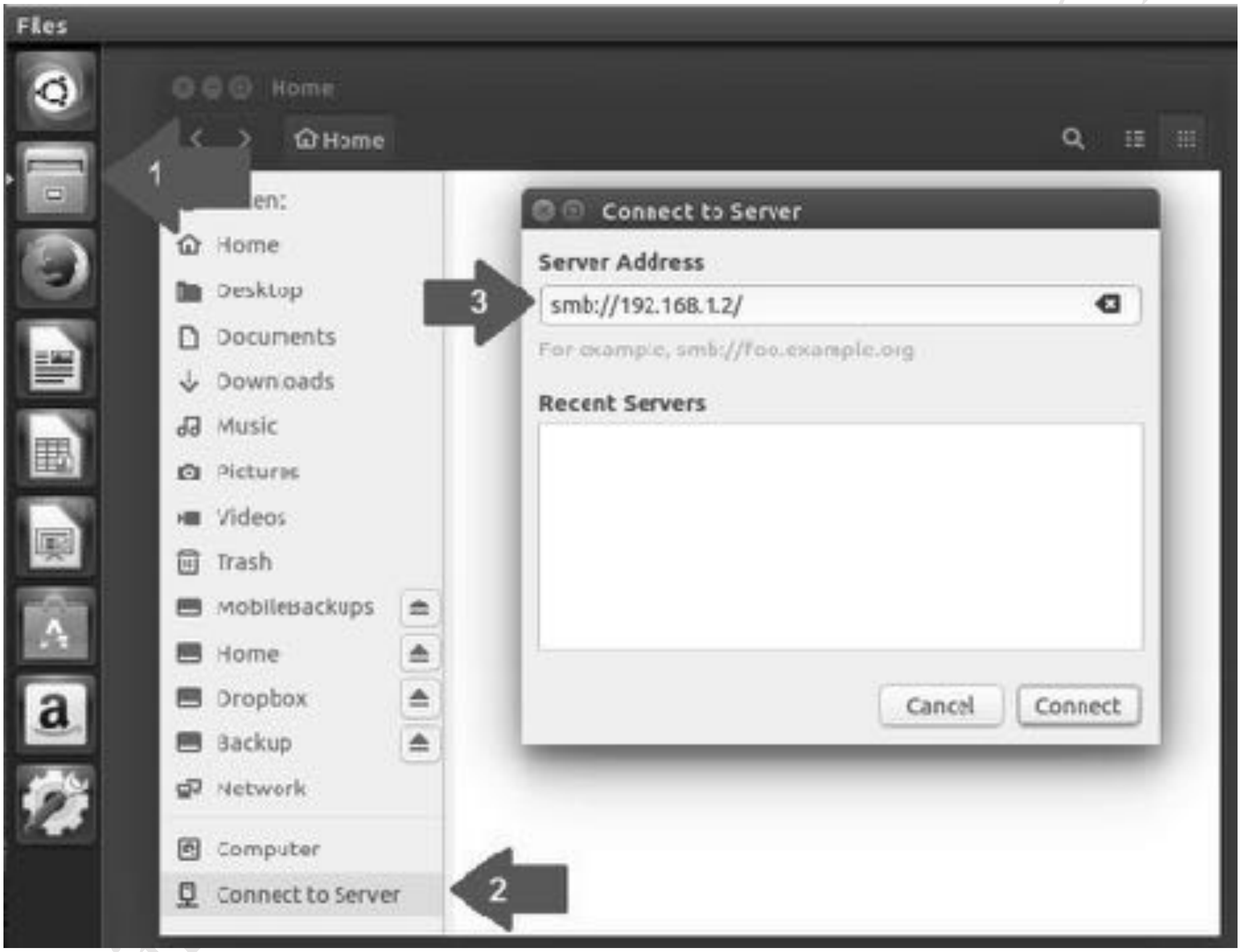
NETLOGON
shared
SYSVOL
users

Figure 74: Select the volume(s) to mount

An icon for each mounted volume 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.

5.7 Connecting Linux Computers

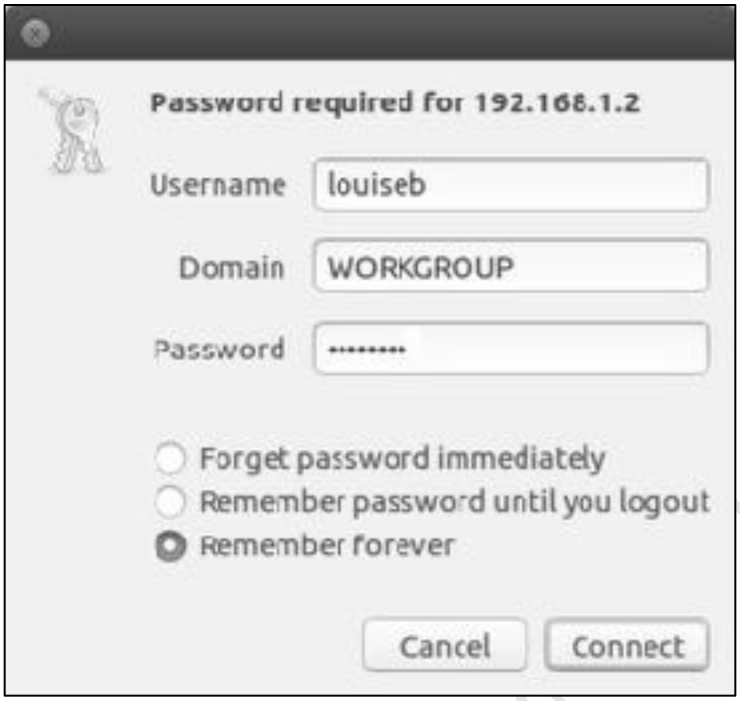
Most Linux distributions do not come with the native capability to connect to a Windows Server. However, Linux PCs can be connected as Workgroup members, in much the same way as computers running unsupported versions of Windows can as described in section 5.5 Connecting Computers with Home Editions of Windows. 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**:



Server Address: smb://192.168.1.2/

Figure 75: 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):



Password required for 192.168.1.2

Username: louiseb

Domain: WORKGROUP

Password: •••••••••

○ Forget password immediately
○ Remember password until you logout
● Remember forever

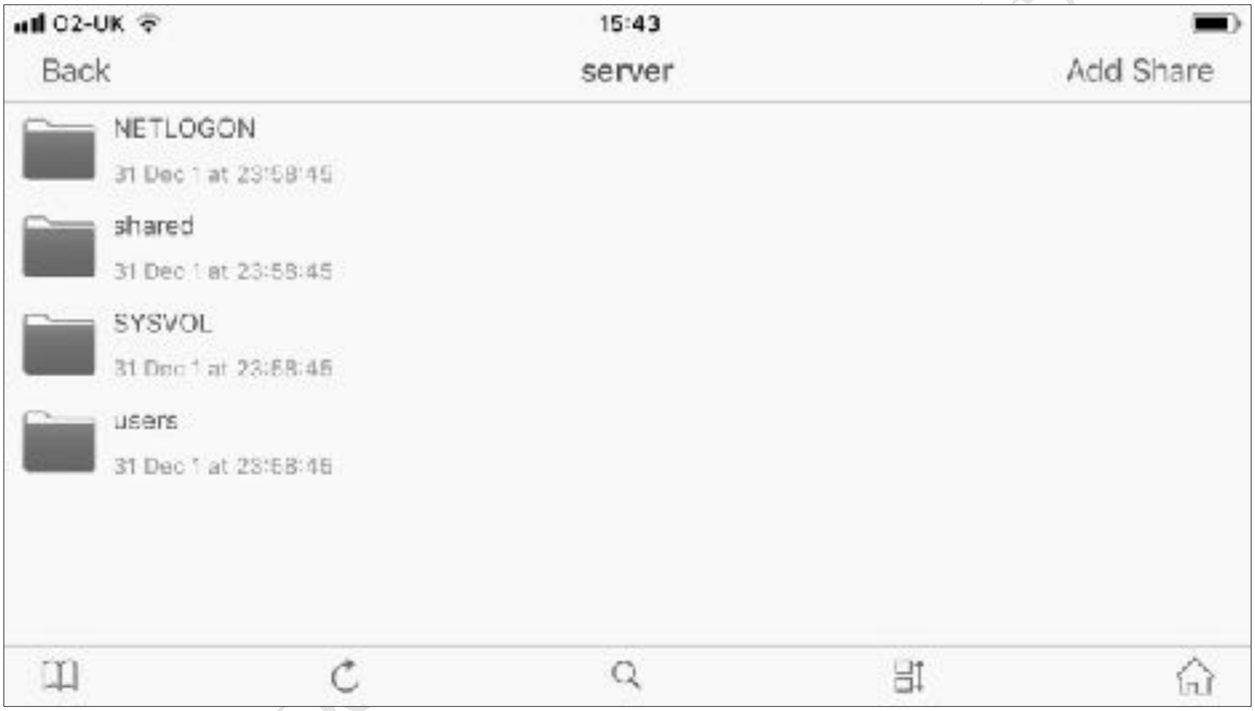
Figure 76: Enter the user's details

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.

5.8 Accessing the File System with 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 Apple App Store, but is inexpensive and well worth buying. It is not specifically designed for Windows Server, rather it is a generic tool for accessing most computer systems. It does not connect to the domain; rather it connects as a workgroup device, in much the same way as computers running unsupported versions of Windows can be as described in section 5.5 Connecting Computers with Home Editions of Windows.

To use, enter the IP address of the server plus a valid user name and password. The user can work with any of the folders to which they have been granted access. To access their home folder, they should double-click the *Users* folder then double-click the folder that has 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.



NETLOGON
31 Dec 1 at 23:58:45

shared
31 Dec 1 at 23:58:45

SYSVOL
31 Dec 1 at 23:58:46

users
31 Dec 1 at 23:58:46

Figure 77: File Browser from Stratospherix running on iPhone

6. BACKUPS AND RESTORES

6.1 Overview

The importance of backing up data on a regular basis, in order to cope with the problems that can arise with computers, cannot be over-emphasized. Potential problems include: deleting files by accident; malware infections; data corruption; computer failure; equipment being lost or 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 and able to produce 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 fallback 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:

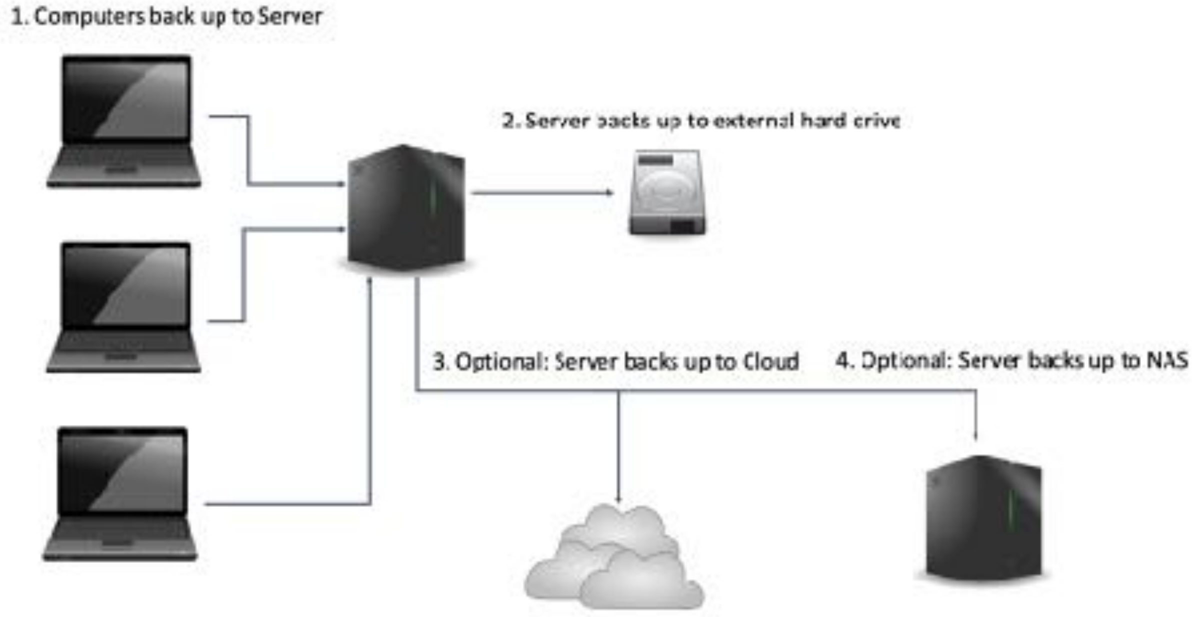
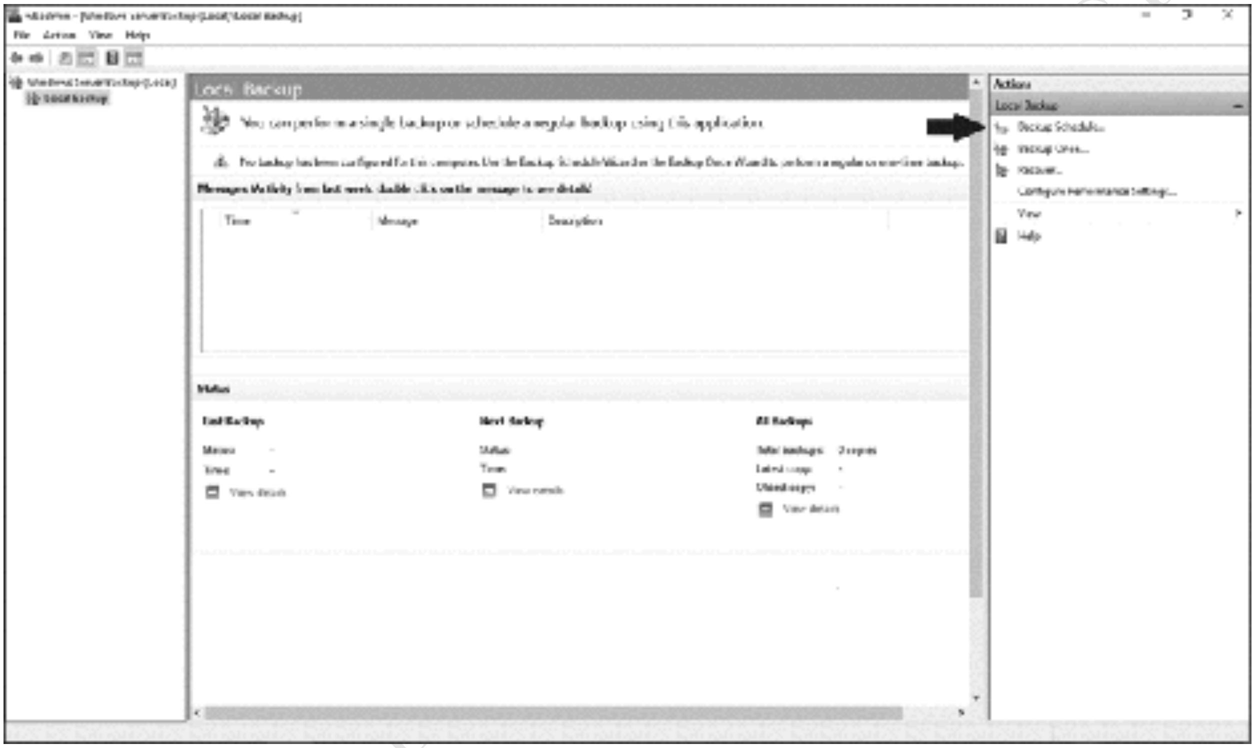

1. Computers back up to Server
2. Server backs up to external hard drive
3. Optional: Server backs up to Cloud
4. Optional: Server backs up to NAS

Figure 78: Multi-tiered approach to backups

6.2 Installation of Windows Server Backup

Windows Server Backup is a standard component of Windows Server 2016 but has first to be installed. To do so, go into **Server Manager** and click **Manage** followed by **Add Roles and Features**. Choose **Role-based or feature-based installation**, click **Next**, select the server on the follow-on screen and click **Next**. Click **Features** on the left-hand panel and select **Windows Server Backup** in the middle, followed by **Next**. On the subsequent screen click **Install**. The installation will only take a minute or two; when complete, click **Close**.

Returning to the **Server Manager**, click **Tools** > **Windows Server Backup**. On the left-hand panel, click **Local Backup** and the screen will appear as follows:


wbadmin - [Windows Server Backup (Local)\Local Backup]
File Action View Help
Windows Server Backup (Local)
Local Backup
Local Backup
Actions
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performance Settings...
View
Help

You can perform a single backup or schedule a regular backup using this application.

No backup has been configured for this computer. Use the Backup Schedule Wizard or the Backup Once Wizard to perform a regular or one-time backup.

Messages (Activity from last week, double click on the message to see details)

Time	Message	Description

Status

Last Backup

Status: -
Time: -
View details

Next Backup

Status:
Time:
View details

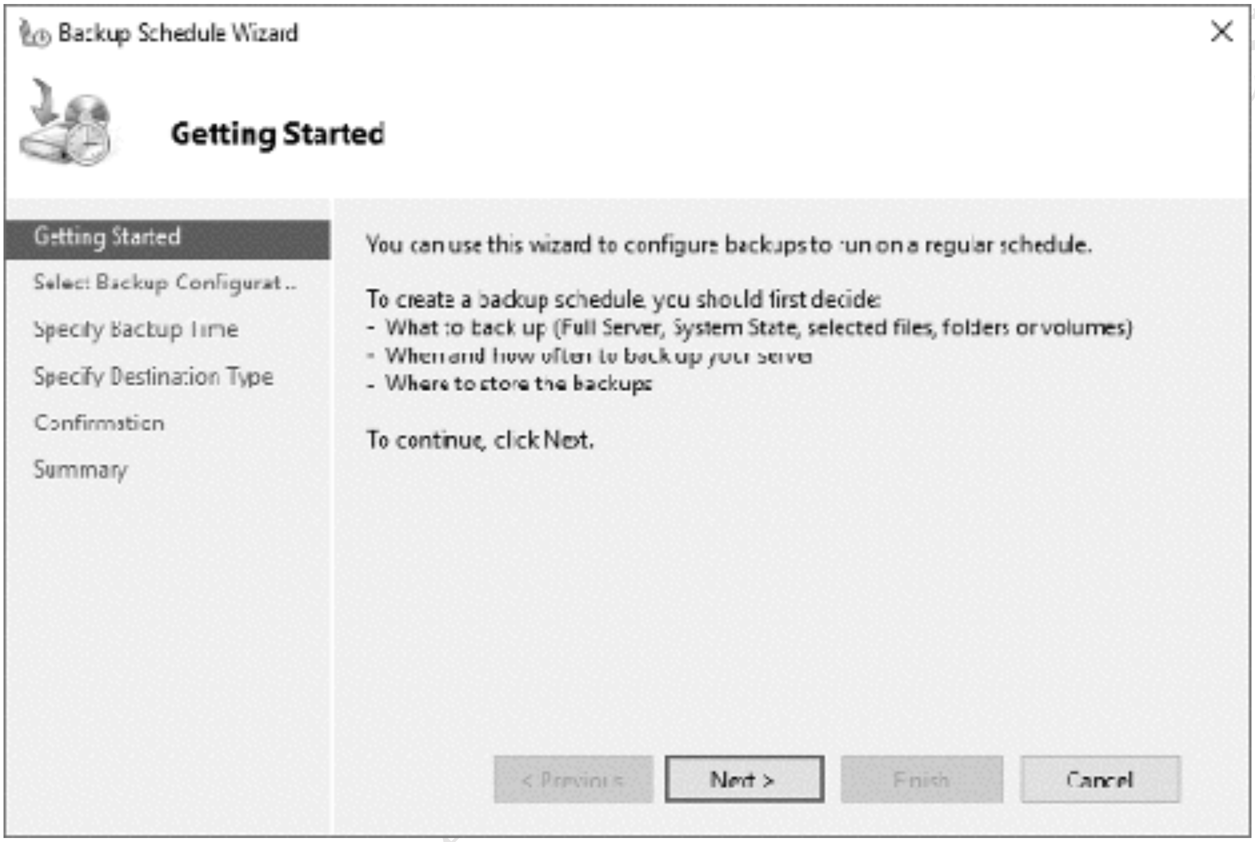
All Backups

Total backups: 0 copies
Latest copy: -
Oldest copy: -
View details

Figure 79: The main Windows Server Backup console

6.3 Setting up a Scheduled Backup

Backups can be run as and when required or, more usefully, scheduled to run on a regular basis. To setup a scheduled backup, click **Backup Schedule** on the right-hand of the screen, listed under *Actions*, which will start the *Backup Schedule Wizard*:



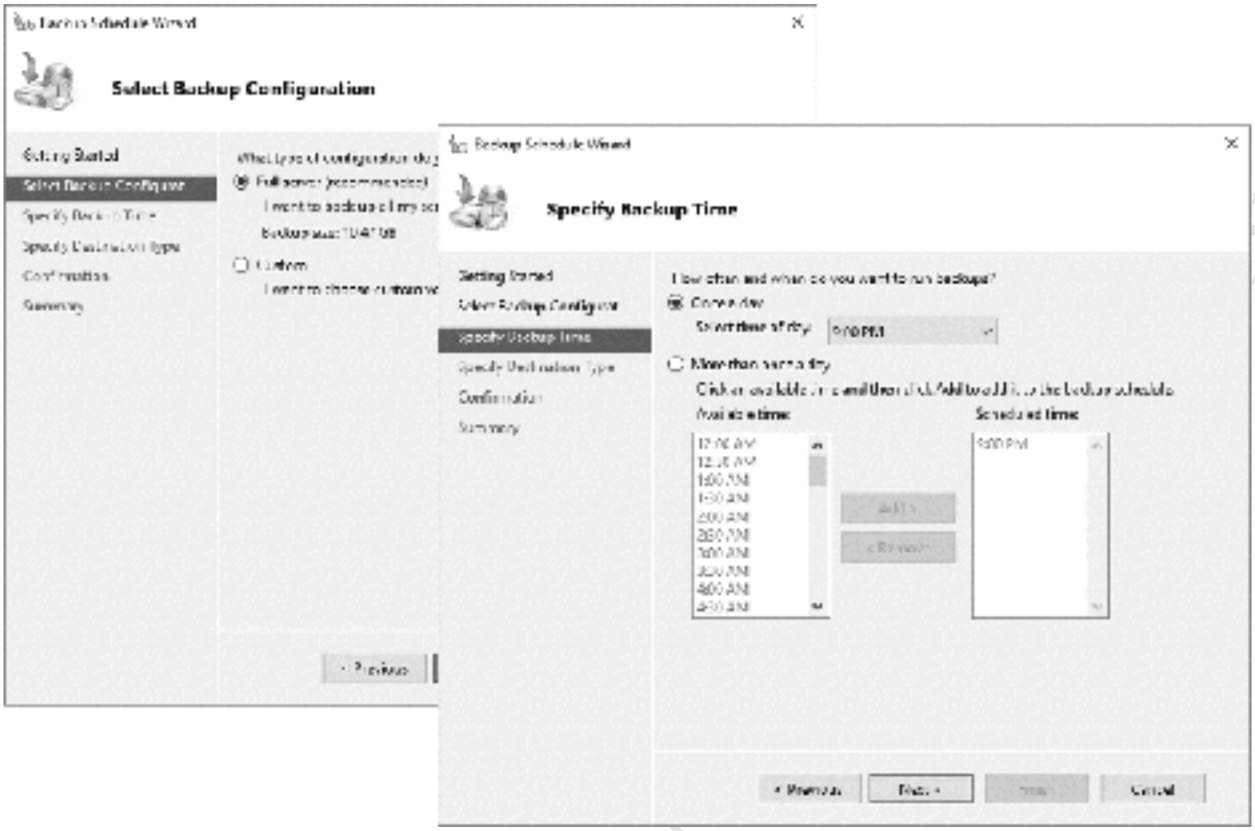
You can use this wizard to configure backups to run on a regular schedule.

To create a backup schedule, you should first decide:
- What to back up (Full Server, System State, selected files, folders or volumes)
- When and how often to back up your server
- Where to store the backups

To continue, click Next.

Figure 80: Backup Schedule Wizard

Click **Next**. On the subsequent screen, there is a choice between a *Full Server (recommended)* or *Custom* backup. As the name implies, the former backs up absolutely everything whereas the latter allows greater control over what is backed up. We will choose **Full Server (recommended)**. Click **Next** and a screen to specify the backup time is then shown:



What type of configuration do you want to schedule?

● Full server (recommended)

I want to back up all my server data...

Backup size: 10.47 GB

○ Custom

I want to choose custom volumes, files...

How often and when do you want to run backups?

● Once a day

Select time of day: 9:00 PM

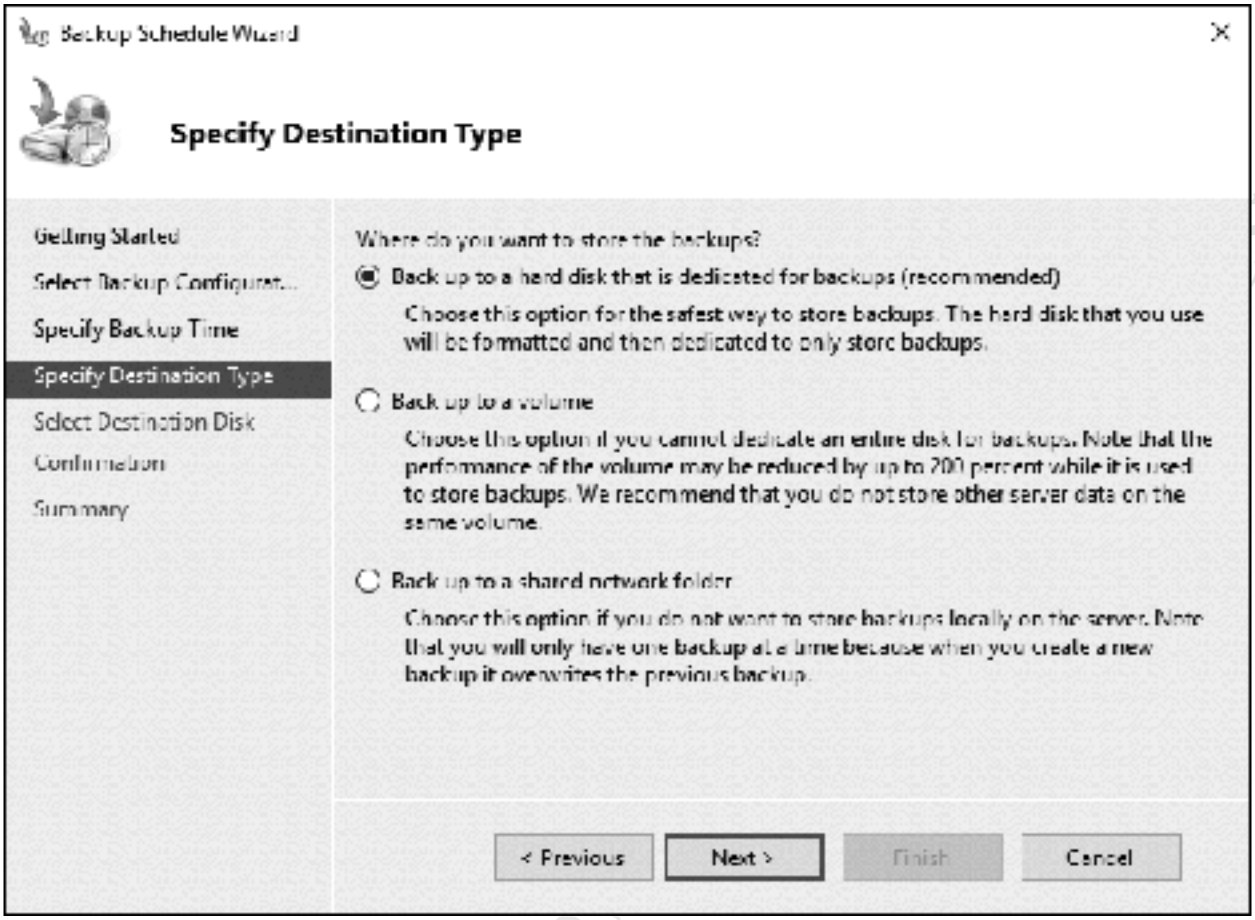
○ More than once a day

Click an available time and then click Add to add it to the backup schedule.

Figure 81: Specifying the Backup time

The default of a daily backup performed at 9:00pm (21:00) will be suitable for many small organizations, else can easily be changed using the drop-down. As a general principle, the backup should be scheduled to run outside of normal working hours or at least during a quiet time, as it can impact server performance. However, it is possible to have the backup run more frequently if needed; this might be more relevant with a custom backup, where a specific volume or folder needs backing up more regularly. Click **Next**.

The destination of the backup is specified on the subsequent screen. Usually the first option – **Back up to a hard disk that is dedicated for backups (recommended)** – is used, although we will also consider another option later:



Specify Destination Type

Where do you want to store the backups?

● Back up to a hard disk that is dedicated for backups (recommended)

Choose this option for the safest way to store backups. The hard disk that you use will be formatted and then dedicated to only store backups.

○ Back up to a volume

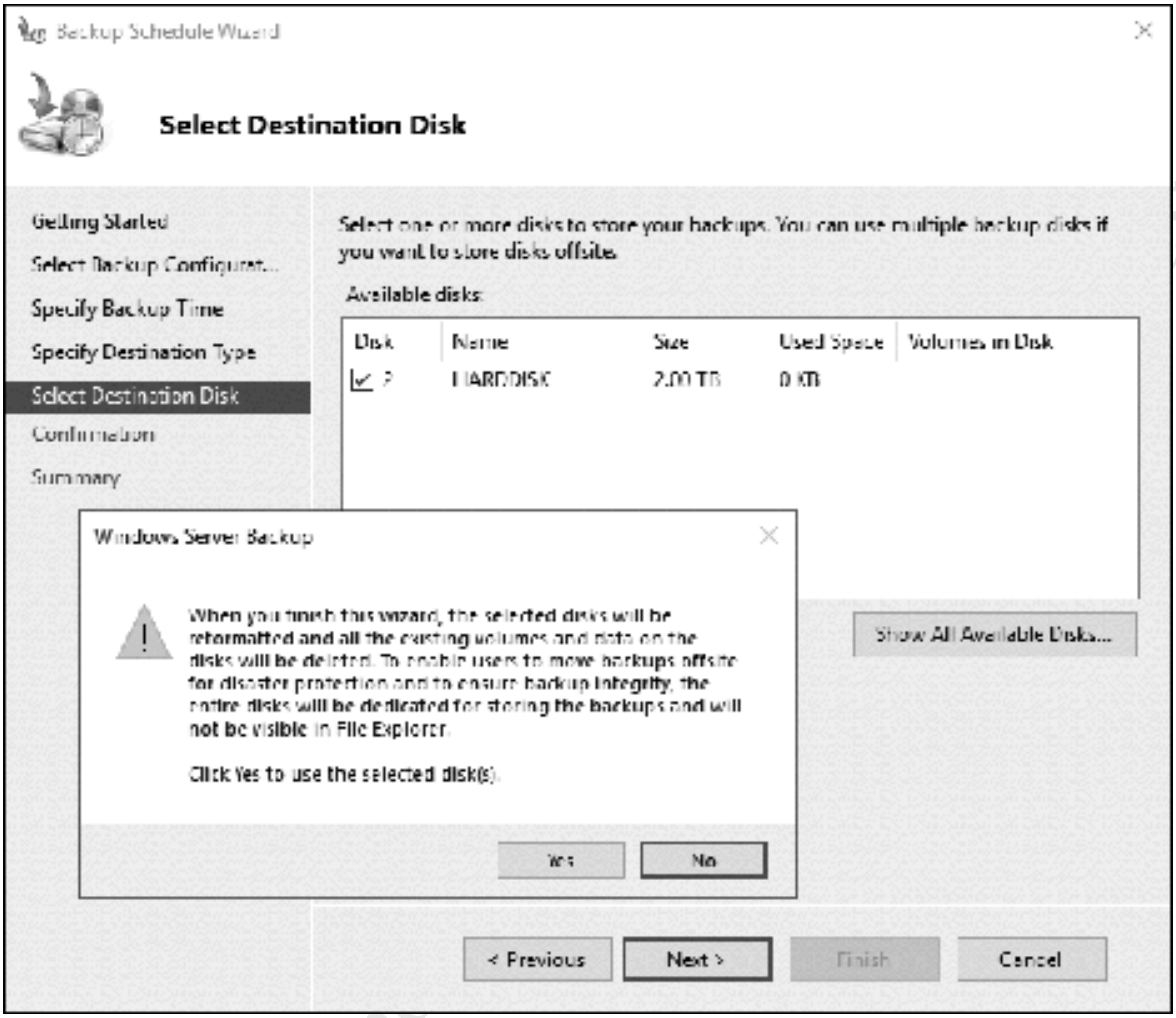
Choose this option if you cannot dedicate an entire disk for backups. Note that the performance of the volume may be reduced by up to 200 percent while it is used to store backups. We recommend that you do not store other server data on the same volume.

○ Back up to a shared network folder

Choose this option if you do not want to store backups locally on the server. Note that you will only have one backup at a time because when you create a new backup it overwrites the previous backup.

Figure 82: Specify the destination type for the backup

Click **Next** to show this screen:



Backup Schedule Wizard

Select Destination Disk

Select one or more disks to store your backups. You can use multiple backup disks if you want to store disks offsite.

Available disks:

Disk	Name	Size	Used Space	Volumes in Disk
☑ 2	HARDDISK	2.00 TB	0 KB	

Windows Server Backup

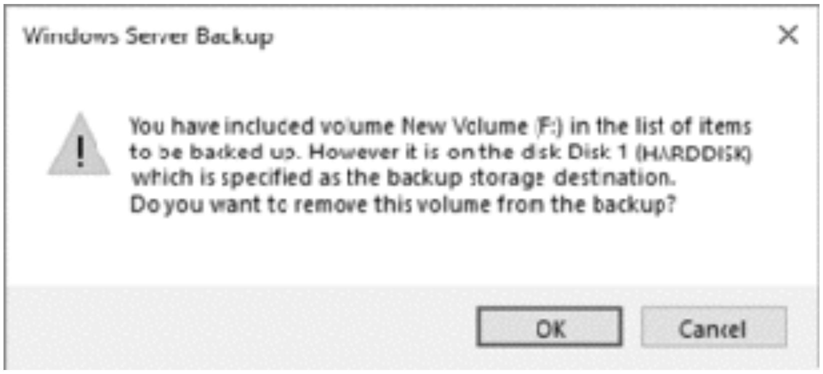
When you finish this wizard, the selected disks will be reformatted and all the existing volumes and data on the disks will be deleted. To enable users to move backups offsite for disaster protection and to ensure backup integrity, the entire disks will be dedicated for storing the backups and will not be visible in File Explorer.

Click Yes to use the selected disk(s).

Figure 83: Specify the destination disk for the backup

Tick the external drive to be used. If no drives are listed, wait 10-15 seconds then click the **Show All Available Disks** button. Having selected the drive, click **Next**. If the drive is not already formatted, there will be a message to that effect and you will need to click **Yes** to format the drive and continue.

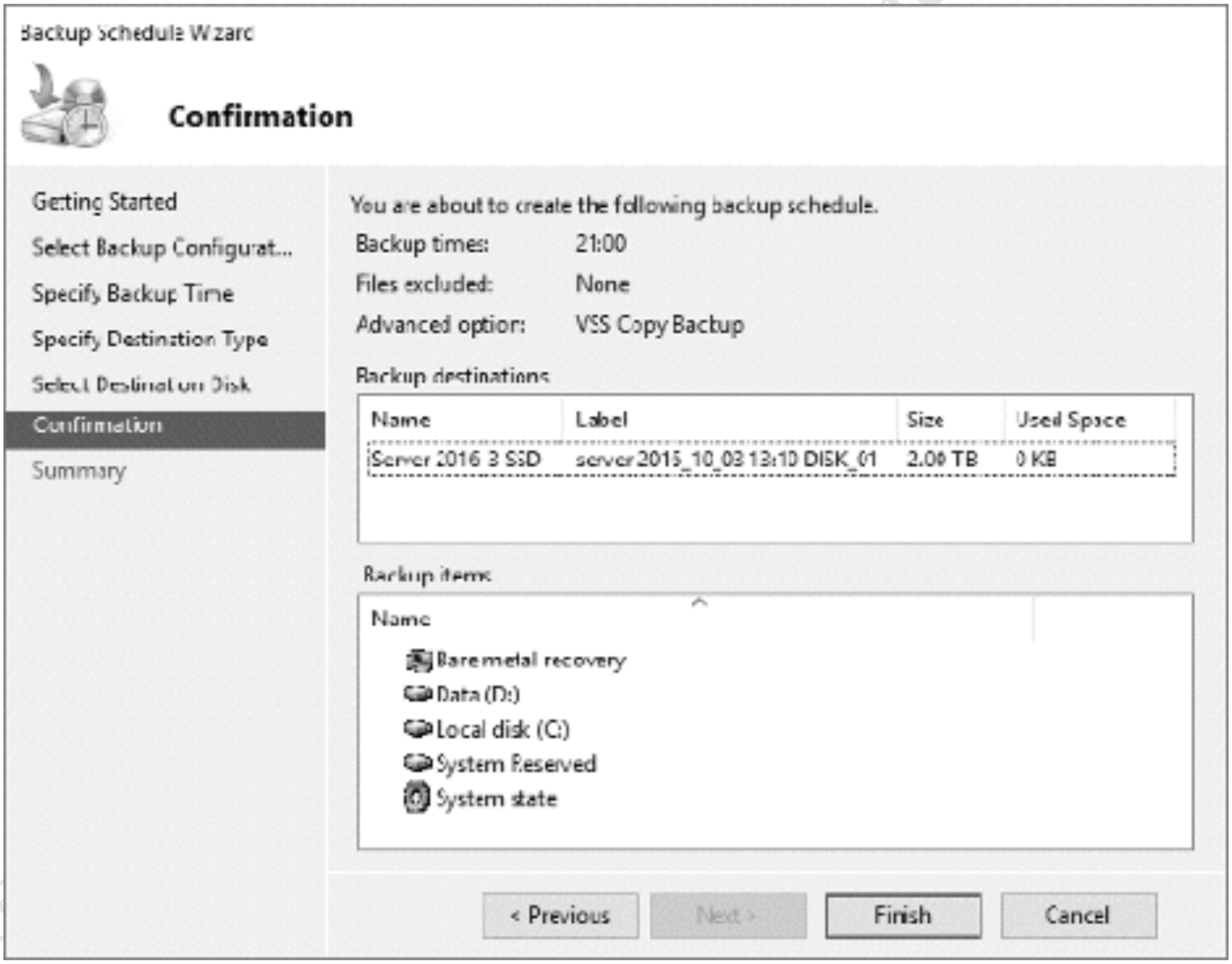
The backup program might detect that the external drive will be *included* within the backup rather than used as a separate backup drive, which you do not want as it would be backing up itself! If the following message is received click **OK** to fix the problem:



You have included volume New Volume (F:) in the list of items to be backed up. However it is on the disk Disk 1 (HARDDISK) which is specified as the backup storage destination.
Do you want to remove this volume from the backup?

Figure 84: Backup warning message

There may be a warning message about formatting. Backup disks use a special file system that is not visible to regular Windows and hence it is not possible to plug a backup disk into a standard Windows computer and read it like a normal drive once it has been formatted for backup purposes. Click **Yes** to the message then click on **Finish** on the Confirmation screen that follows:



You are about to create the following backup schedule.

Backup times: 21:00

Files excluded: None

Advanced option: VSS Copy Backup

Backup destinations

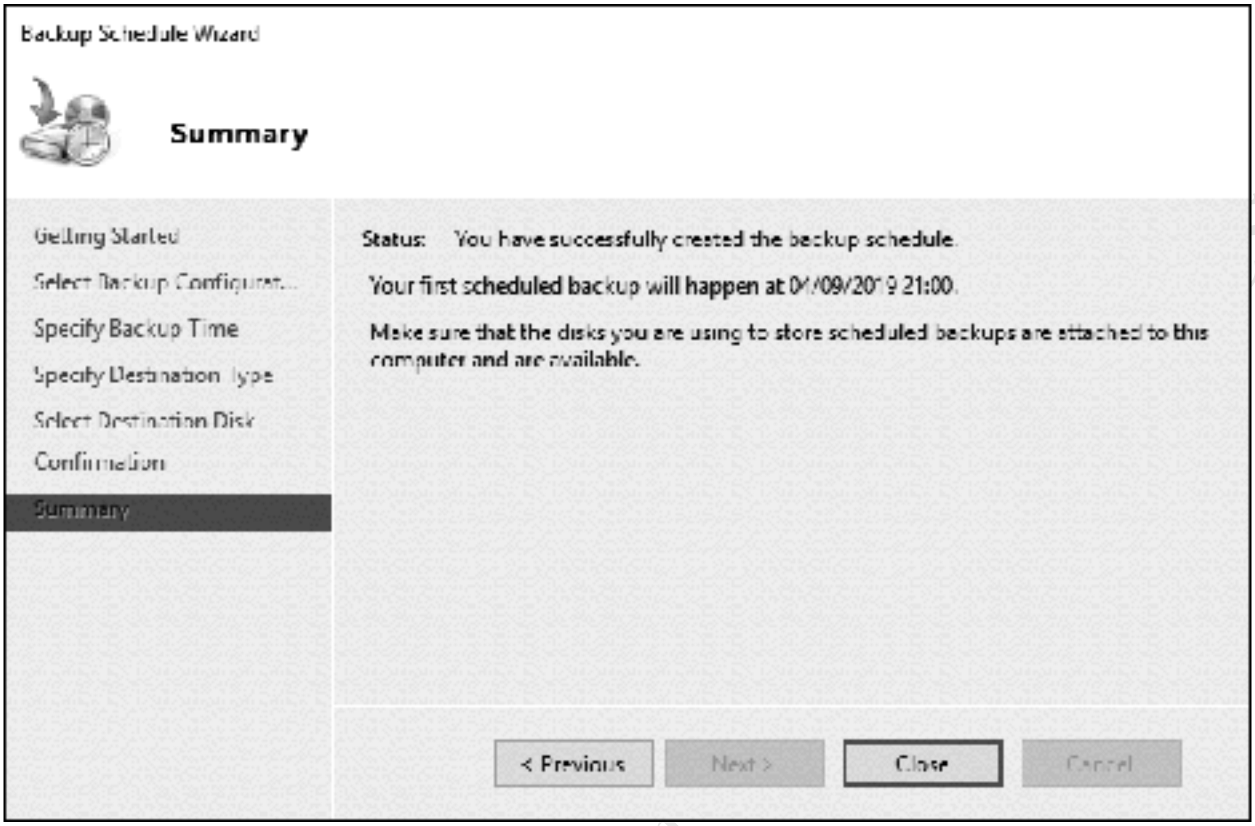
Name	Label	Size	Used Space
Server 2016 3 SSD	server 2015_10_03 13:10 DISK_01	2.00 TB	0 KB

Backup items

Name
Bare metal recovery
Data (D:)
Local disk (C:)
System Reserved
System state

Figure 85: Confirmation of settings

After a short while a Summary screen is displayed:



Status: You have successfully created the backup schedule.

Your first scheduled backup will happen at 04/09/2019 21:00.

Make sure that the disks you are using to store scheduled backups are attached to this computer and are available.

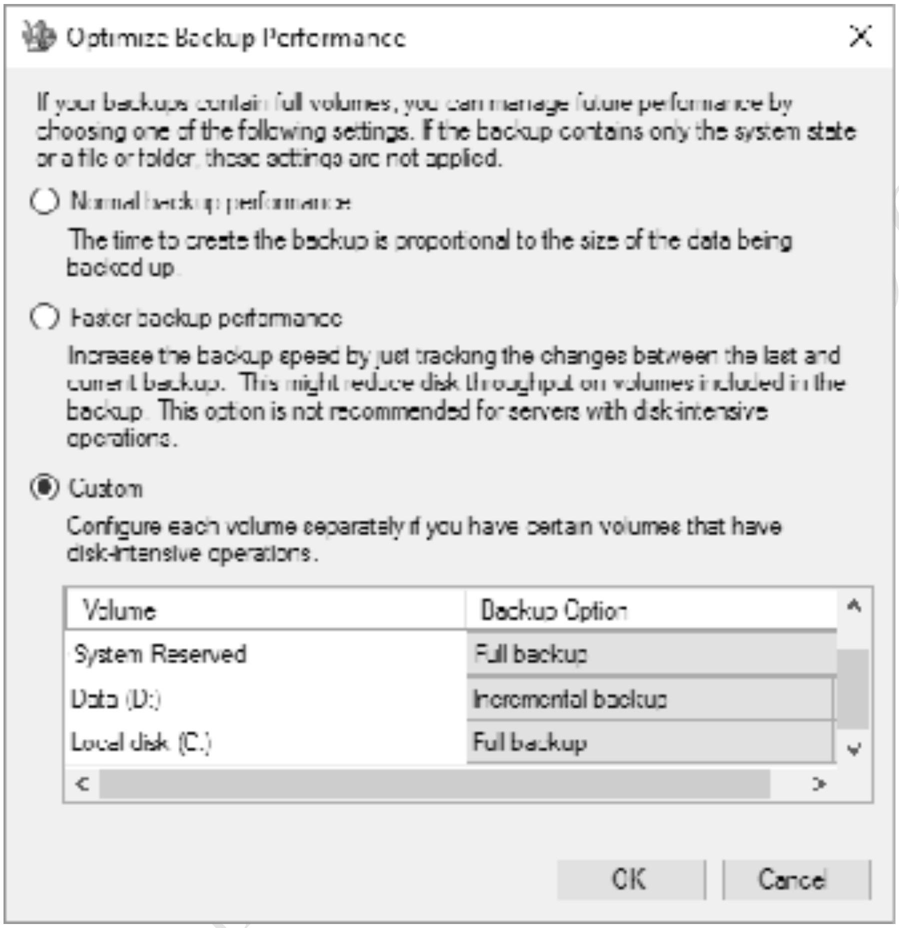
Figure 86: Summary screen from the Backup Schedule Wizard

Using the main *Windows Server Backup* screen, the backup job can be checked each day to make sure that it has completed successfully.

Having created a backup, you may wish to run it immediately to test that it is working, rather than wait for the scheduled time. From the main backup screen, click **Backup Once** in the *Actions* column. On the *Backup Options* screen that appears, choose **Scheduled backup options** and click **Next**. The next screen is the *Confirmation* screen – click **Backup** and the backup will run immediately. When it has completed, click **Close**. The scheduled job will not be affected in any way.

6.4 Backup Performance Settings

As mentioned previously, the backup process can be quite intensive in terms of impacting the performance of the server and for this reason it is possible to 'fine tune' it to some degree. From the main backup screen click **Configure Performance Settings…** to display the following panel:



Optimize Backup Performance

If your backups contain full volumes, you can manage future performance by choosing one of the following settings. If the backup contains only the system state or a file or folder, these settings are not applied.

○ Normal backup performance

The time to create the backup is proportional to the size of the data being backed up.

○ Faster backup performance

Increase the backup speed by just tracking the changes between the last and current backup. This might reduce disk throughput on volumes included in the backup. This option is not recommended for servers with disk-intensive operations.

● Custom

Configure each volume separately if you have certain volumes that have disk-intensive operations.

Volume	Backup Option
System Reserved	Full backup
Data (D:)	Incremental backup
Local disk (C:)	Full backup

Figure 87: Optimize Backup Performance

There are three options:

Normal backup performance – the default – results in a full backup in which everything on the volume is backed up

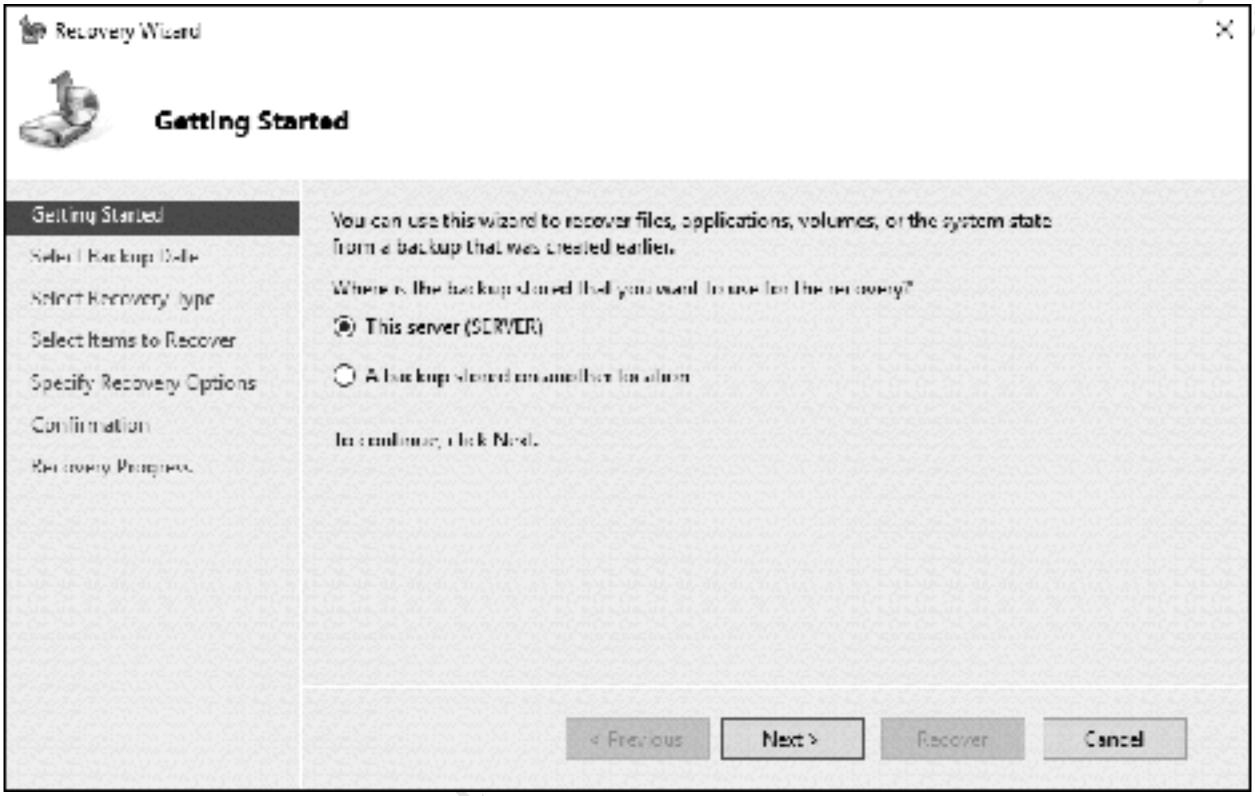
Faster backup performance – only items which have changed since the last backup are backed up. Also known as an incremental backup

Custom – allows different volumes to be treated differently. For instance, you could choose to always do a full backup of the C: drive containing Windows, but incremental backups of the data drive(s) as shown above

Having made any changes click **OK**.

6.5 Restoring Files to the Server

In the event of data loss or there being a need to recover (restore) deleted or older versions of files, the *Recovery Wizard* can be used. Launch Windows Server Backup (**Server Manager** > **Tools** > **Windows Server Backup)**. On the left-hand panel, click **Local Backup** and on the right-hand of the screen, listed under **Actions**, click **Recover,** which will cause the *Recovery Wizard* to run. Make sure **This server (SERVER)** is selected and click **Next**:



You can use this wizard to recover files, applications, volumes, or the system state from a backup that was created earlier.

Where is the backup stored that you want to use for the recovery?

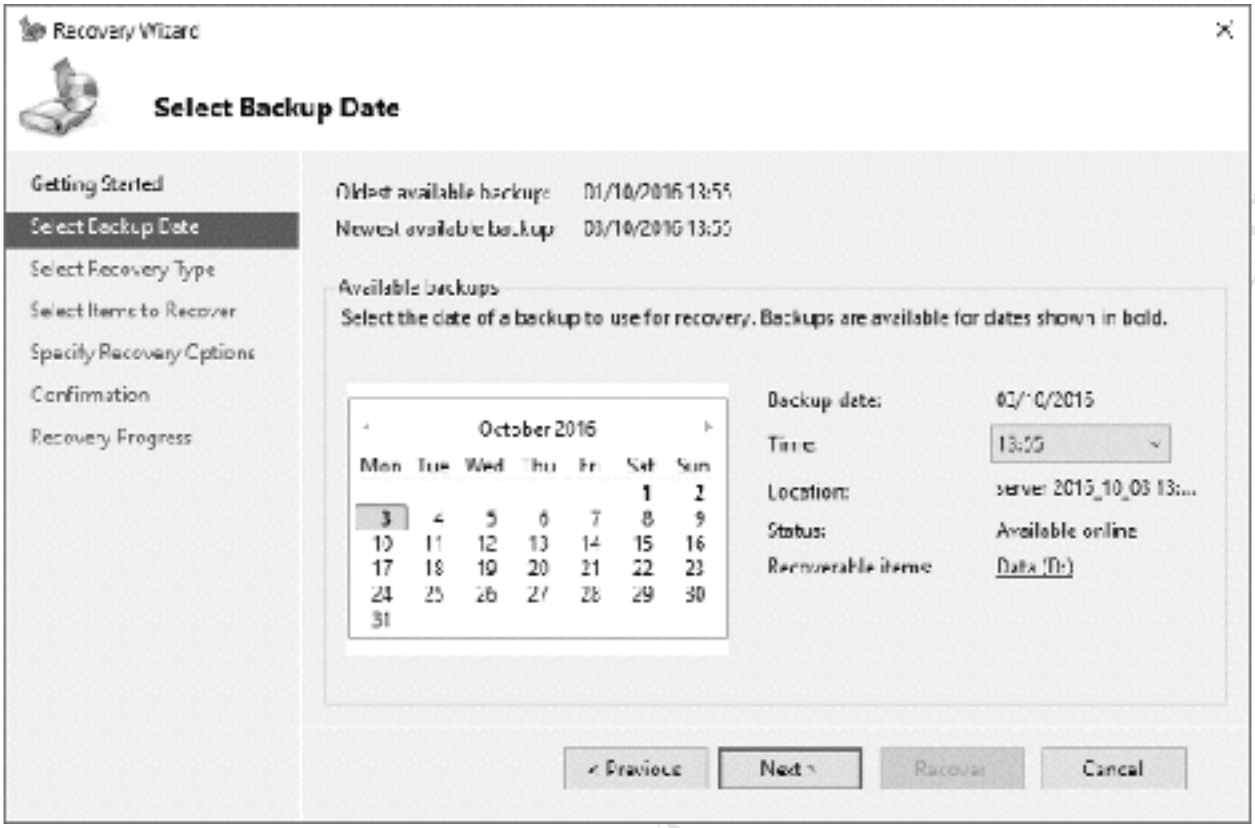
● This server (SERVER)

○ A backup stored on another location

To continue, click Next.

Figure 88: Recovery Wizard Getting Started screen

On the next screen, select a backup to be restored using the calendar and time fields – days for which backups are available are highlighted in bold - then click **Next**:



Oldest available backup: 01/10/2016 13:55
Newest available backup: 03/10/2016 13:55

Available backups

Select the date of a backup to use for recovery. Backups are available for dates shown in bold.

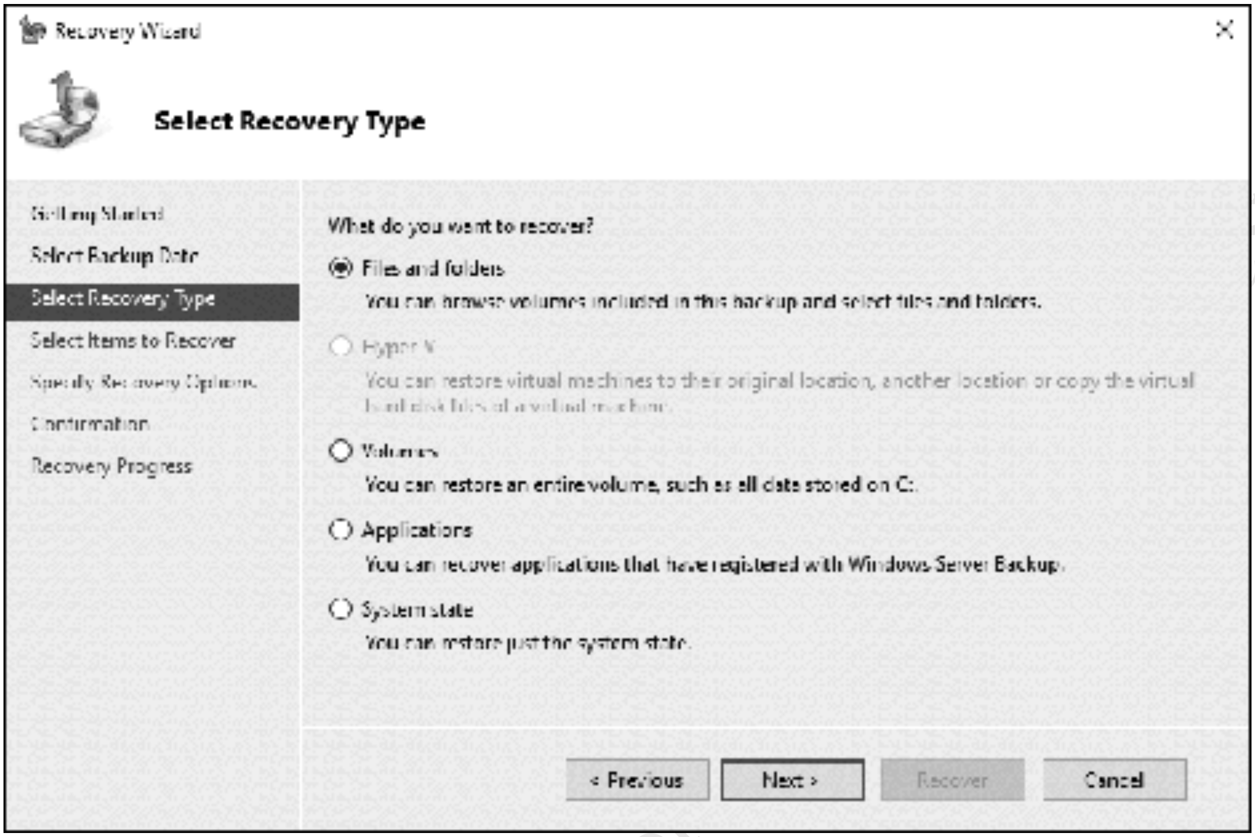
October 2016

Mon	Tue	Wed	Thu	Fri	Sat	Sun
					1	**2**
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Backup date: 03/10/2016
Time: 13:55
Location: server 2016_10_03 13:...
Status: Available online
Recoverable items: Data (D:)

Figure 89: Choose a backup to recover from

The subsequent screen is for specifying what needs to be recovered. Most commonly, you would be recovering files and folders:



Select Recovery Type

What do you want to recover?

● Files and folders
You can browse volumes included in this backup and select files and folders.

○ Hyper-V
You can restore virtual machines to their original location, another location or copy the virtual hard disk files of a virtual machine.

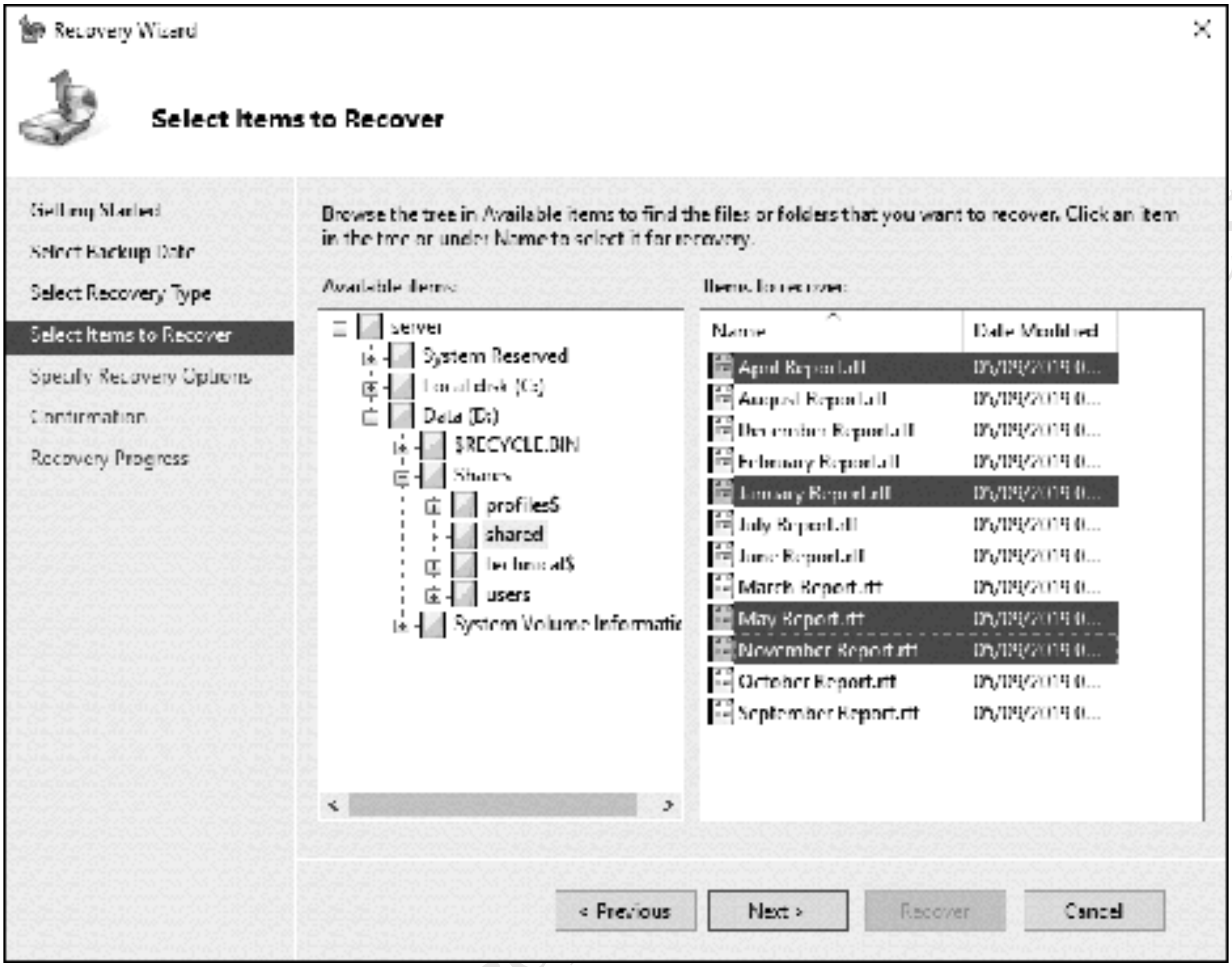
○ Volumes
You can restore an entire volume, such as all data stored on C:.

○ Applications
You can recover applications that have registered with Windows Server Backup.

○ System state
You can restore just the system state.

Figure 90: Select the recovery type

This is followed by a screen where the actual folders and files to be recovered are specified. Drill-down through the file structure in the left-hand panel, highlight the resultant items in the right-hand one. Then click **Next**:



Recovery Wizard

Select Items to Recover

- Getting Started
- Select Backup Date
- Select Recovery Type
- Select Items to Recover
- Specify Recovery Options
- Confirmation
- Recovery Progress

Browse the tree in Available items to find the files or folders that you want to recover. Click an item in the tree or under Name to select it for recovery.

Available items:

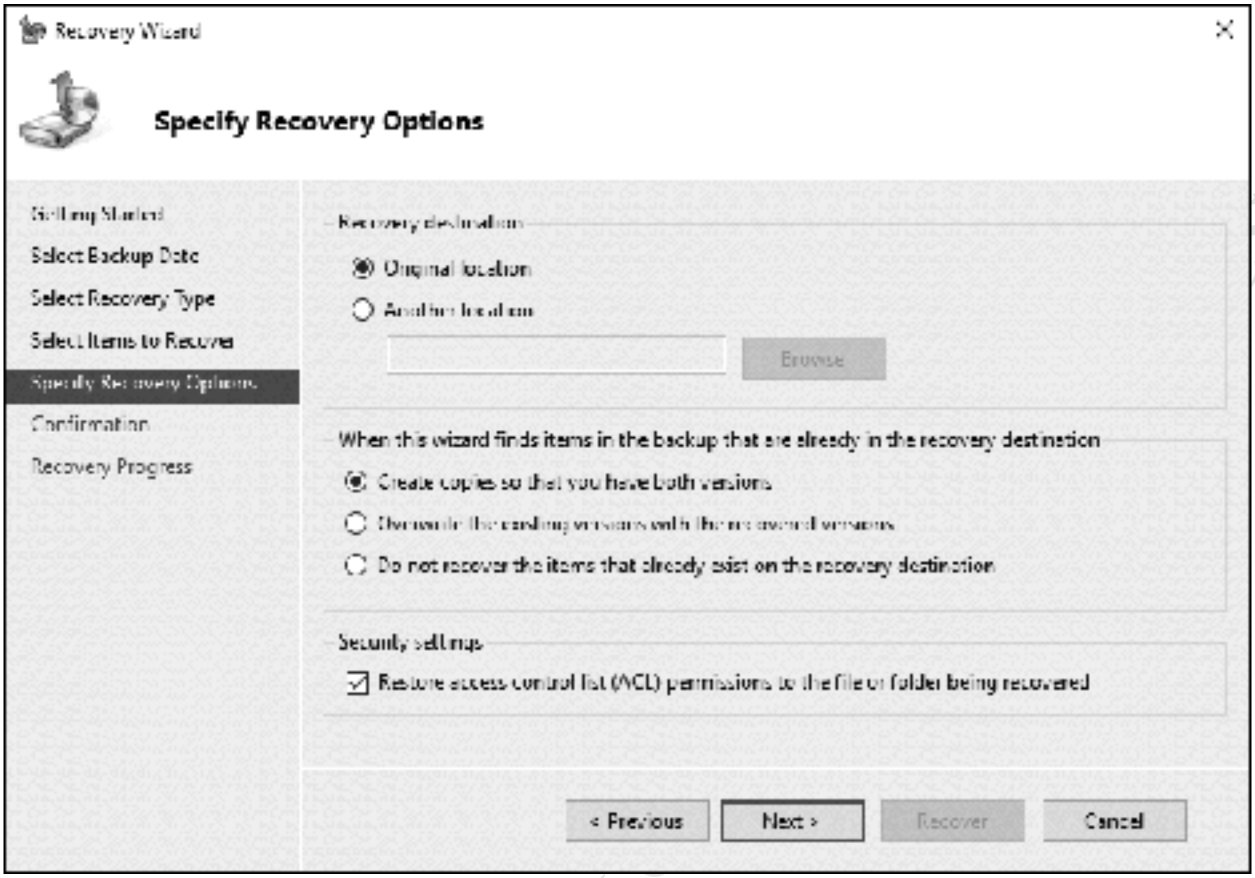
```
server
  System Reserved
  Local disk (C:)
  Data (D:)
    $RECYCLE.BIN
    Shares
      profiles$
      shared
      technical$
      users
    System Volume Informatic
```

Items to recover:

Name	Date Modified
April Report.rtf	05/09/2019 0...
August Report.rtf	05/09/2019 0...
December Report.rtf	05/09/2019 0...
February Report.rtf	05/09/2019 0...
January Report.rtf	05/09/2019 0...
July Report.rtf	05/09/2019 0...
June Report.rtf	05/09/2019 0...
March Report.rtf	05/09/2019 0...
May Report.rtf	05/09/2019 0...
November Report.rtf	05/09/2019 0...
October Report.rtf	05/09/2019 0...
September Report.rtf	05/09/2019 0...

Figure 91: Select the items to recover

The next screen is for specifying options when recovering files. Specifically, should they be recovered to the original location or to another location and what to do when duplicates are found? Make a decision, leave the *Security settings* box ticked and click **Next**:


Recovery Wizard

Specify Recovery Options

Recovery destination

● Original location

○ Another location

When this wizard finds items in the backup that are already in the recovery destination

● Create copies so that you have both versions

○ Overwrite the existing versions with the recovered versions

○ Do not recover the items that already exist on the recovery destination

Security settings

☑ Restore access control list (ACL) permissions to the file or folder being recovered

Figure 92: Specify recovery options

After clicking **Next**, a Confirmation screen is displayed. Click the **Recover** button to begin restoring the folders and files, during which time a status screen is shown. When complete, click **Close**.

6.6 Backing up the Server to a NAS Drive

One potential downside of using an USB drive for the backups is that it must 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 (Network Attached Storage) device. This gives a lot more flexibility as to where it is located, such as in a totally different part of the building. The network drive can be in addition to or in place of the USB drive; a further advantage of using NAS drives is that they are available in higher capacities that regular USB drives.

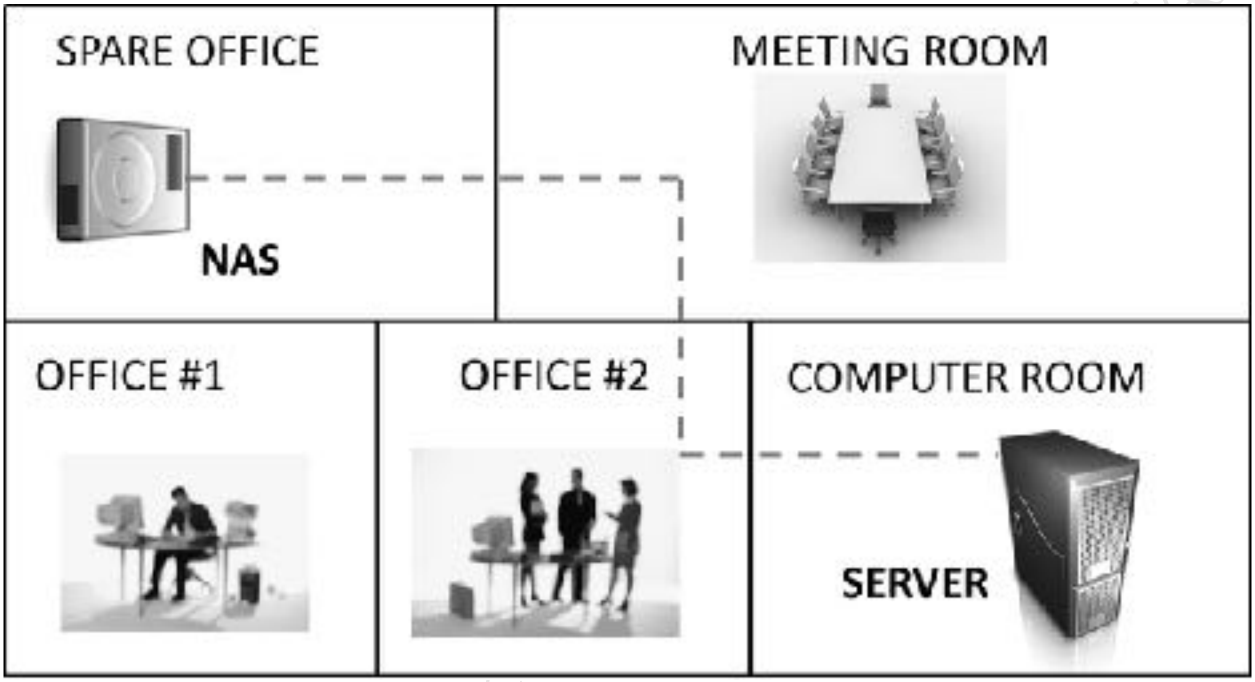
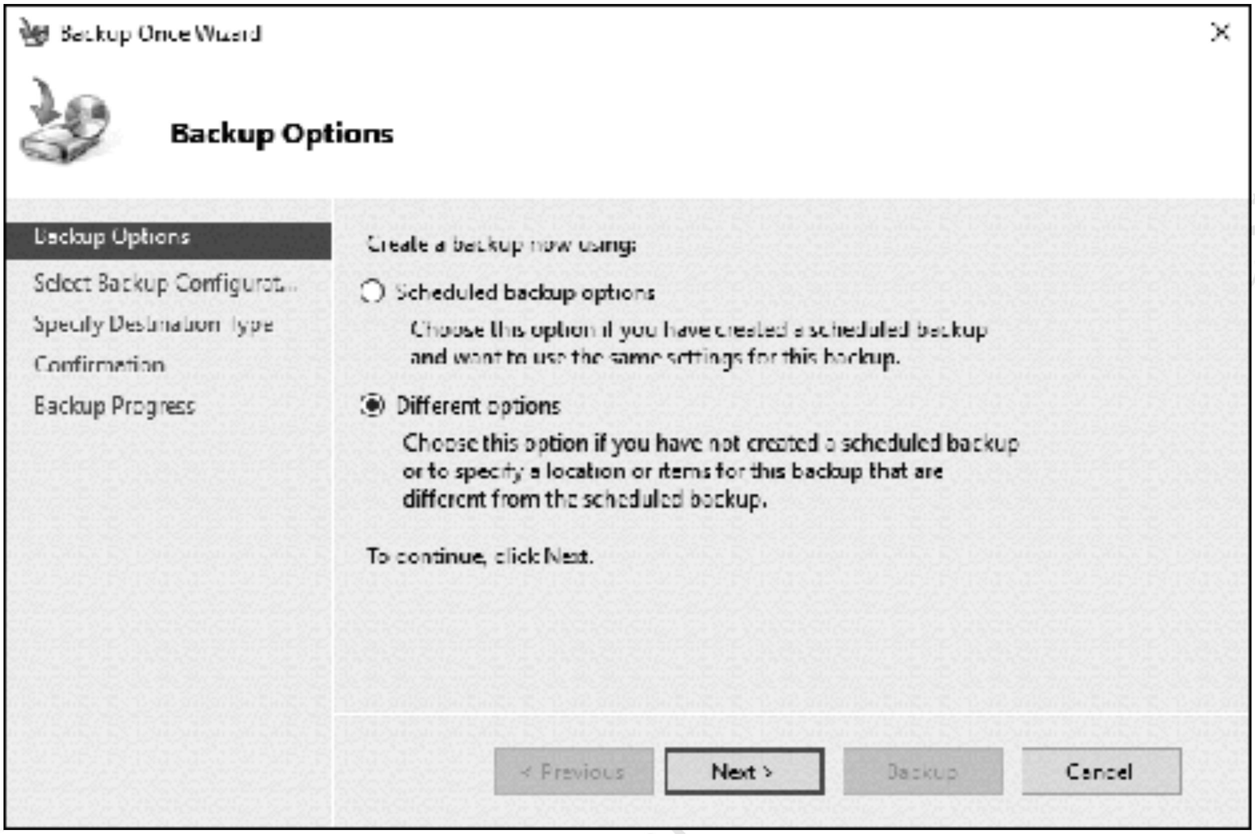


Figure 93: Locate the NAS drive in a separate part of the premises

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 brand 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 backup account which will typically have administrative rights.

On the server run *Windows Server Backup*, click **Local Backup** (even though you could argue it is not a local backup at all) and click **Backup Once…** to create a new backup job. On the screen that appears choose **Different options** and click **Next**:



Create a backup now using:

○ Scheduled backup options

Choose this option if you have created a scheduled backup and want to use the same settings for this backup.

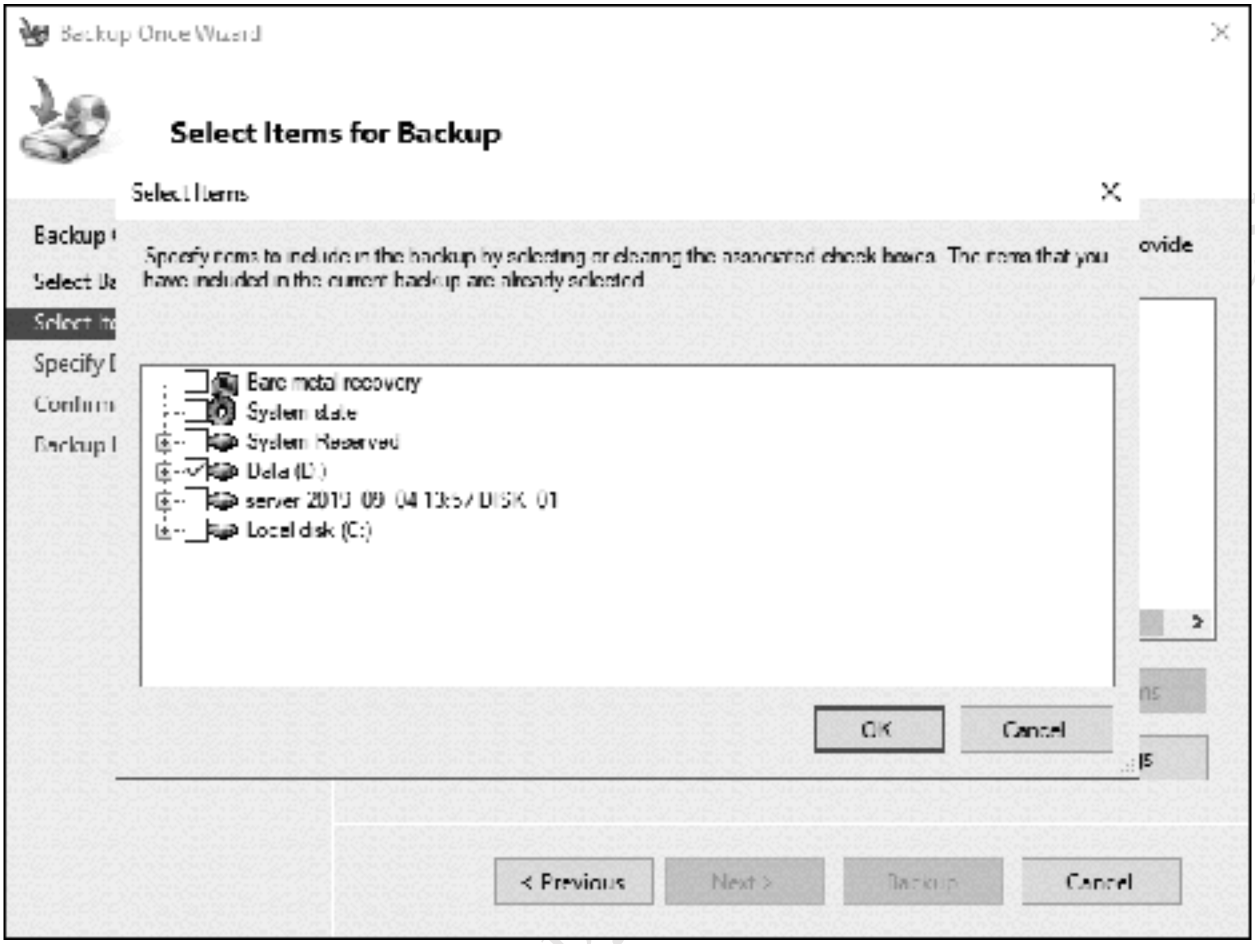
● Different options

Choose this option if you have not created a scheduled backup or to specify a location or items for this backup that are different from the scheduled backup.

To continue, click Next.

Figure 94: 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**. On the following screen click **Add Items** and choose the items to be backed up. This would normally be just the disk volume containing the data, in our example the E: drive. Click **OK**.

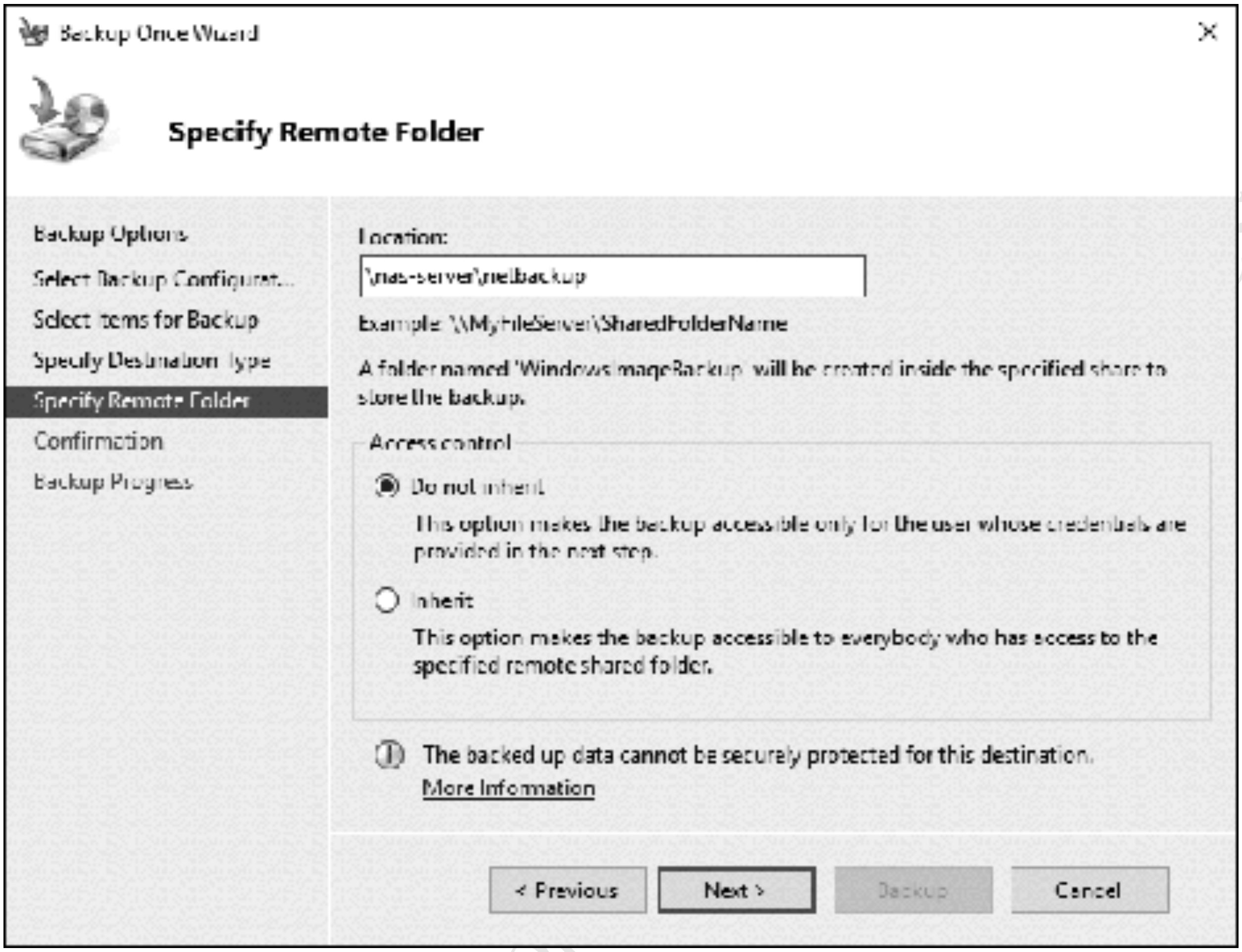


Specify items to include in the backup by selecting or clearing the associated check boxes. The items that you have included in the current backup are already selected.

- ☐ Bare metal recovery
- ☐ System state
- ☐ System Reserved
- ☑ Data (D:)
- ☐ server 2019_09_04 13:57 DISK_01
- ☐ Local disk (C:)

Figure 95: Select items to backup

You will be returned to the previous screen, where you should click **Next**. On the following screen the backup destination type has to be chosen – click **Remote shared folder** followed by **Next**. On the subsequent screen, enter the location of the NAS folder in the form *\\NAS_name\folder_name*. In this example, the NAS is called *nas-server* and the backup folder is called *netbackup*, hence *\\nas-server\netbackup*. Choose the **Do not inherit** option and click **Next**:



Location: \nas-server\netbackup

Example: \\MyFileServer\SharedFolderName

A folder named 'WindowsImageBackup' will be created inside the specified share to store the backup.

Access control

● Do not inherit

This option makes the backup accessible only for the user whose credentials are provided in the next step.

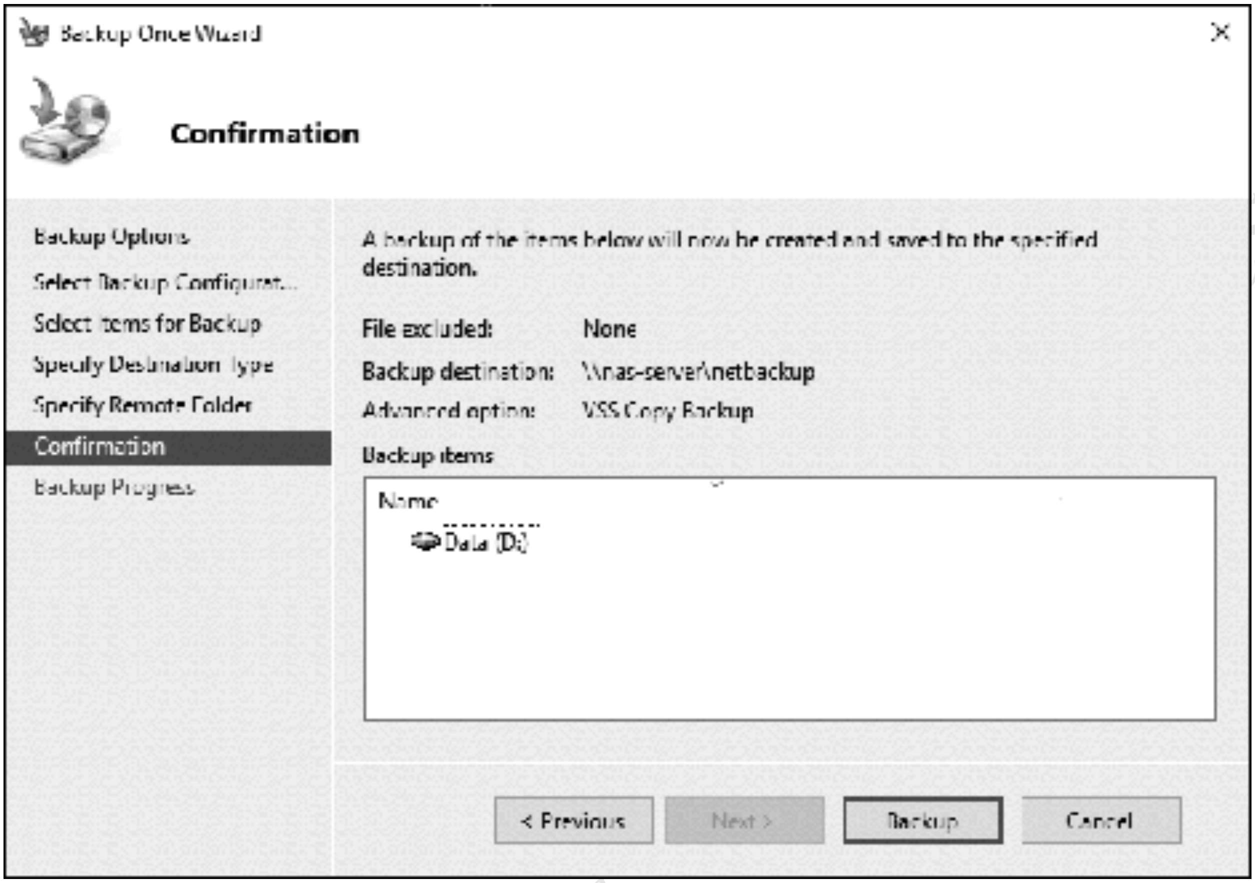
○ Inherit

This option makes the backup accessible to everybody who has access to the specified remote shared folder.

The backed up data cannot be securely protected for this destination.
More Information

Figure 96: Specify the remote location

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



Confirmation

A backup of the items below will now be created and saved to the specified destination.

File excluded: None

Backup destination: \\nas-server\netbackup

Advanced option: VSS Copy Backup

Backup items

Name

Data (D:)

Figure 97: 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, 8 TB 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. Consequently, NAS might be more appropriate as a secondary or archive backup solution.

6.7 Third Party Server Backup Programs

In the early days of Windows Server, the Microsoft-supplied backup program was rudimentary, such that a market was opened for more sophisticated and capable products. Windows Server Backup has improved significantly over the years and can meet the backup requirements of many organizations, but alternatives are available for those who require additional capabilities e.g. tape backup, backing up virtual machines, archiving, cloud backups, cross-platform compatibility and so on. Many are available and examples of popular products include: *Veritas Backup Exec*; *Acronis Backup*; *NovaStor NovaBACKUP*; *Cortex IT Labs' BackupAssist*. Most of these offer free trials so you can determine their suitability. By way of illustration, this section considers the latter one, *BackupAssist*, which has a relatively low price. It is not a detailed 'how to' walkthrough or a sales pitch, but is rather intended to show the sort of capabilities that such commercial programs offer and how they compare to Windows Server Backup.

The first thing to do is install the standard Windows Server Backup feature as described in [6.2 Installation of Windows Server Backup](), as BackupAssist makes use of some underlying features. Then, download and install BackupAssist. In the BackupAssist Console, click **Create a New Backup Job**. There are several backup types available – choose **System Protection**. On the next screen, choose the volumes to be backed up – there is a choice of backing up the entire system or selected items only:

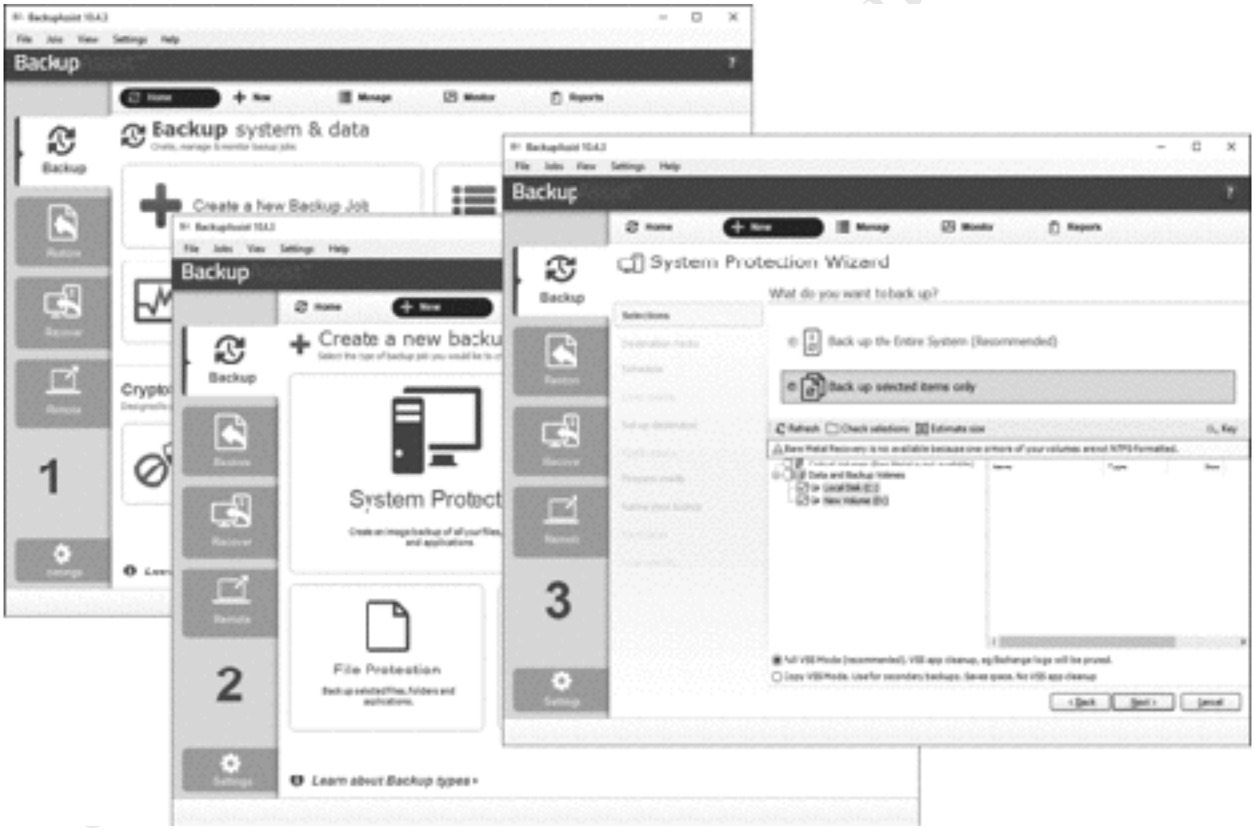
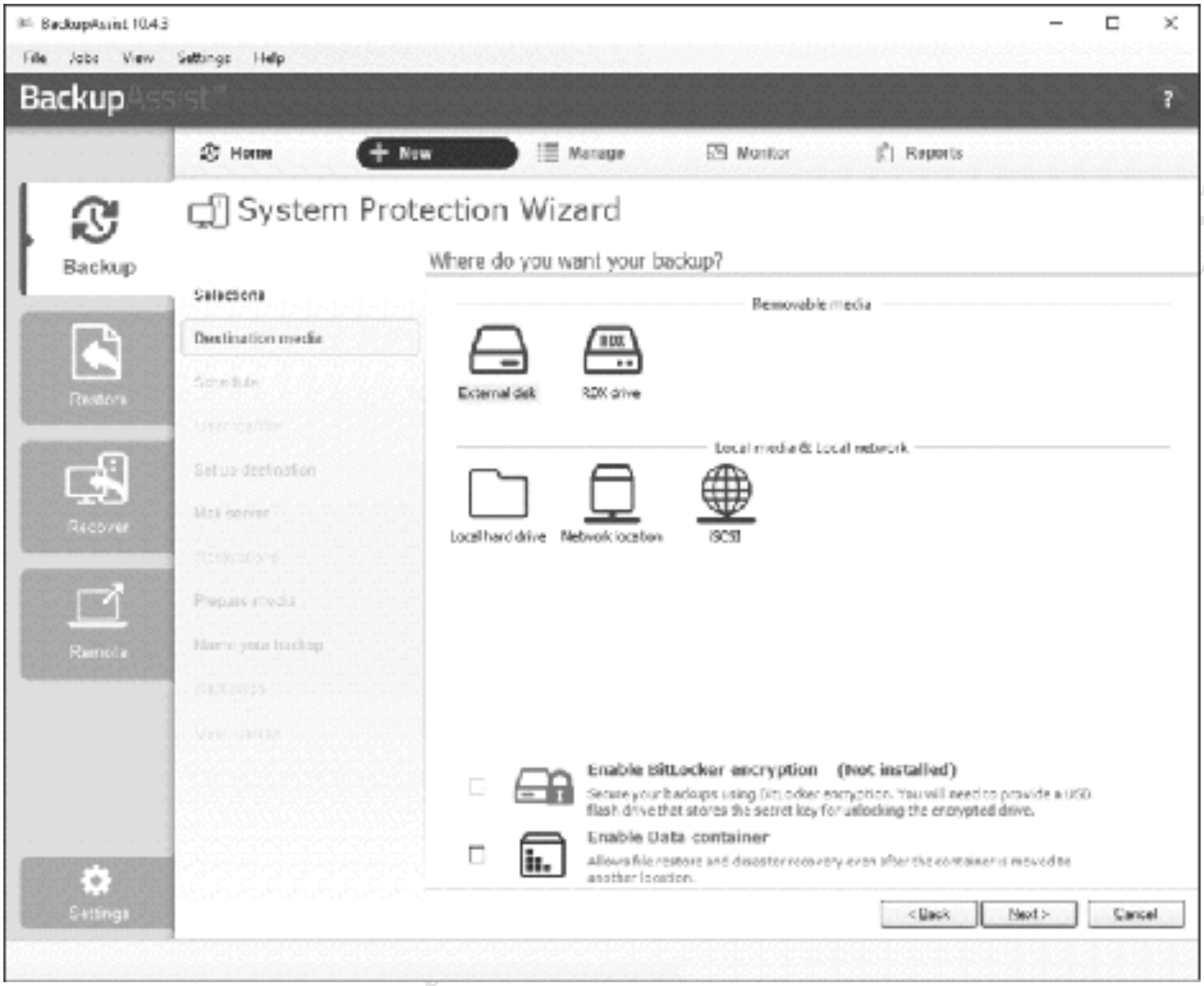


Figure 98: BackupAssist Console and creating a new job

Having clicked **Next**, you will be given a choice of destination. This illustrates the sort of flexibility offered by third party backup programs; whereas Windows Server Backup largely assumes you are backing up to an external hard drive, BackupAssist gives a choice of: external disk; RDX drive (removeable cartridge); local hard drive; network location; iSCSI volume. Make your choice and click **Next**:



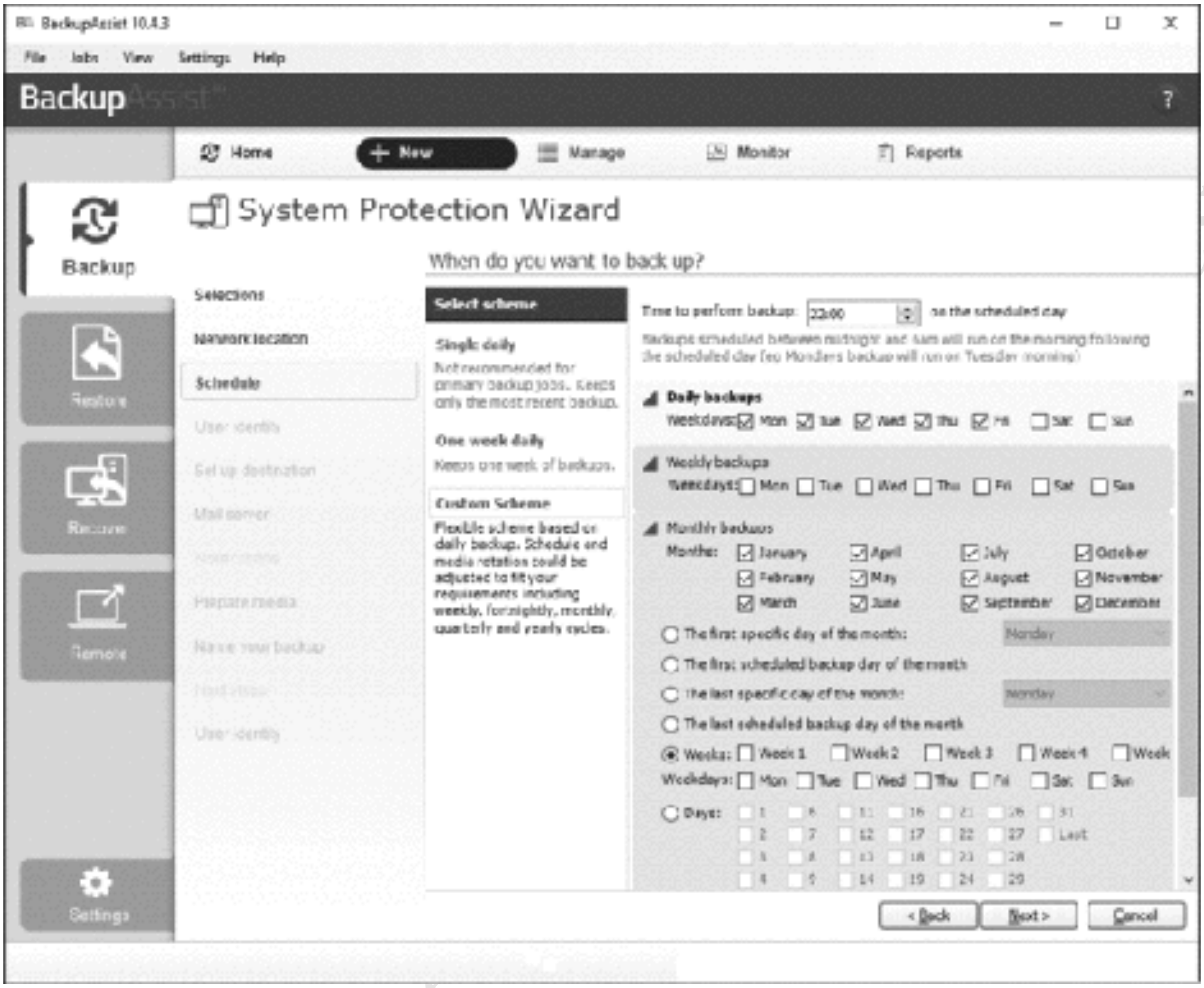
Where do you want your backup?

□ **Enable BitLocker encryption (Not installed)**
Secure your backups using BitLocker encryption. You will need to provide a USB flash drive that stores the secret key for unlocking the encrypted drive.

□ **Enable Data container**
Allows file restore and disaster recovery even after the container is moved to another location.

Figure 99: Choose a destination for the backup

The subsequent screen is for scheduling. This can be as simple as choosing a daily backup at a fixed time, but a wider range of options are available in some products to allow for backup rotation and archiving:



System Protection Wizard

When do you want to back up?

Select scheme

Single daily
Not recommended for primary backup jobs. Keeps only the most recent backup.

One week daily
Keeps one week of backups.

Custom Scheme
Flexible scheme based on daily backup. Schedule and media rotation could be adjusted to fit your requirements including weekly, fortnightly, monthly, quarterly and yearly cycles.

Time to perform backup: 22:00 on the scheduled day

Backups scheduled between midnight and 5am will run on the morning following the scheduled day (eg Mondays backup will run on Tuesday morning)

Daily backups
Weekdays: ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun

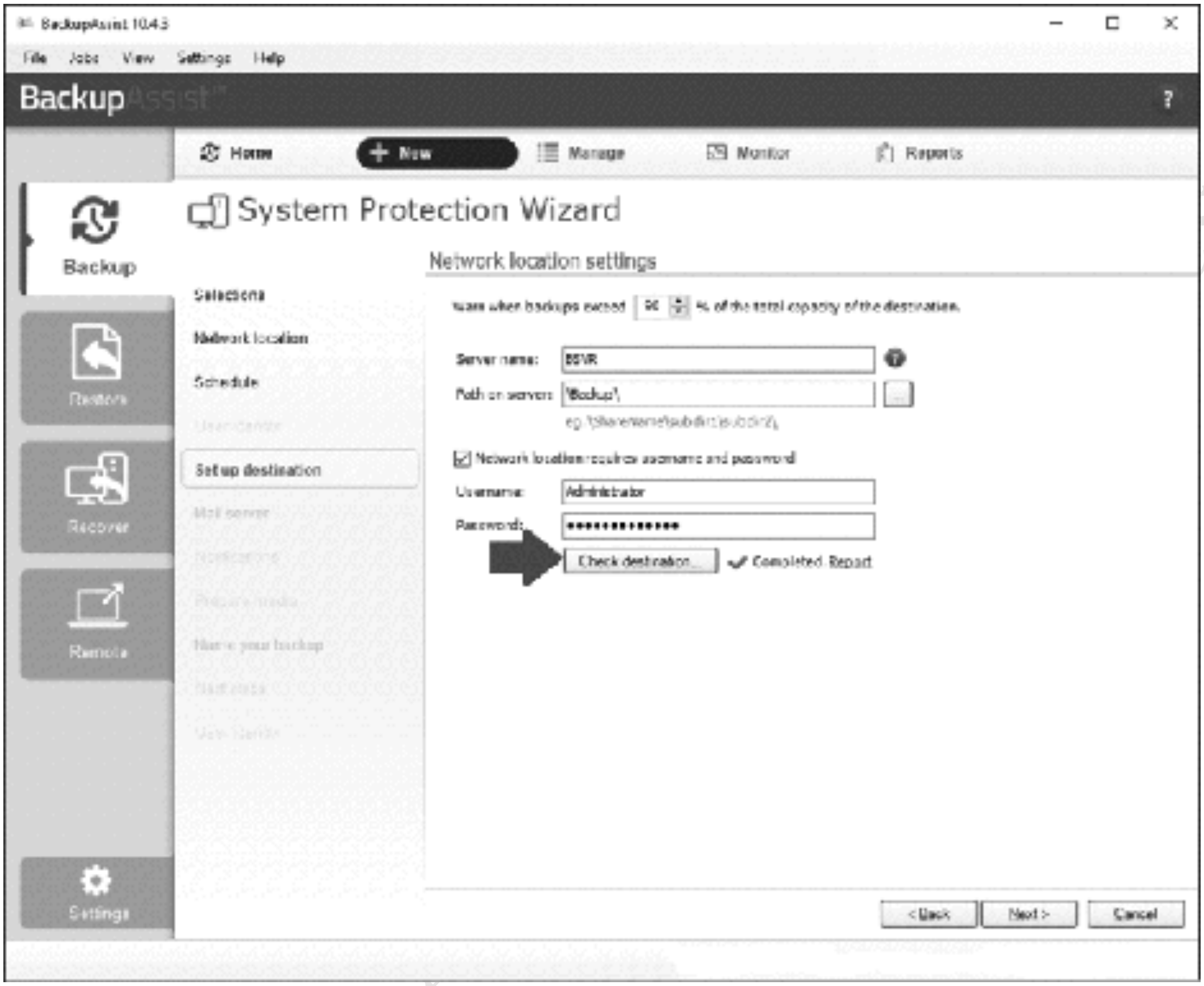
Weekly backups
Weekdays: □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Monthly backups
Months: ☑ January ☑ April ☑ July ☑ October ☑ February ☑ May ☑ August ☑ November ☑ March ☑ June ☑ September ☑ December

○ The first specific day of the month: Monday
○ The first scheduled backup day of the month
○ The last specific day of the month: Monday
○ The last scheduled backup day of the month
● Weeks: □ Week 1 □ Week 2 □ Week 3 □ Week 4 □ Week
Weekdays: □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun
○ Days: □ 1 □ 6 □ 11 □ 16 □ 21 □ 26 □ 31 □ 2 □ 7 □ 12 □ 17 □ 22 □ 27 □ Last □ 3 □ 8 □ 13 □ 18 □ 23 □ 28 □ 4 □ 9 □ 14 □ 19 □ 24 □ 29

Figure 100: Select a scheduling scheme

With BackupAssist, the next screen that is shown is dependent upon the type of backup destination. In this example, we are backing up to a network location. Note the useful feature for checking that the backup destination is reachable:



Network location settings

Warn when backups exceed 90 % of the total capacity of the destination.

Server name: BSVR

Path on server: \Backup\

eg. \[sharename]\subdir1\subdir2\

☑ Network location requires username and password

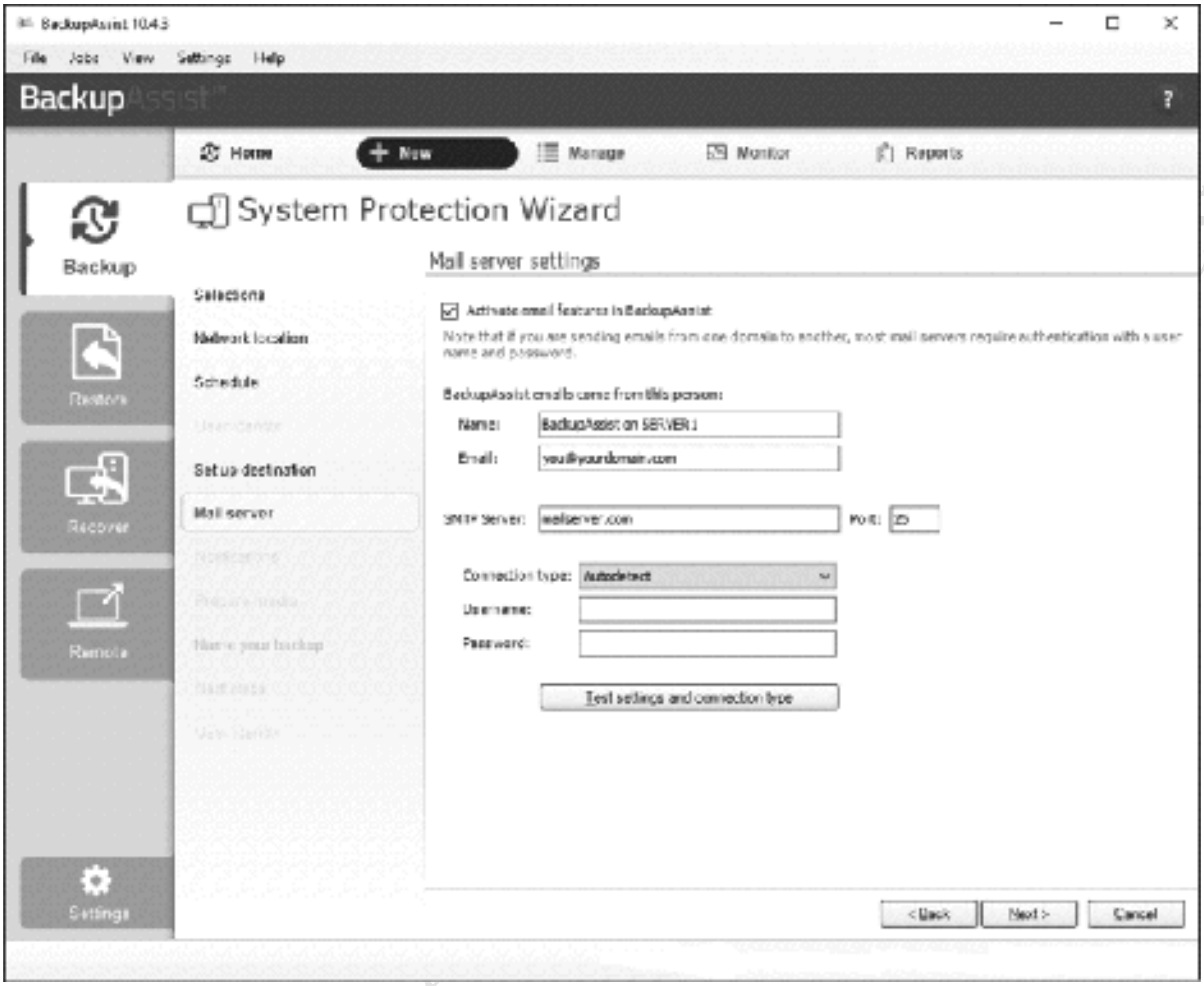
Username: Administrator

Password: ••••••••••••••

Check destination... ✓ Completed. Report

Figure 101: Network location settings

In the case of this particular program, there is an option to have it email the results of the backup job, which is useful for support and monitoring purposes:



System Protection Wizard

Mail server settings

☑ Activate email features in BackupAssist

Note that if you are sending emails from one domain to another, most mail servers require authentication with a user name and password.

BackupAssist emails come from this person:

Name: BackupAssist on SERVER1

Email: you@yourdomain.com

SMTP Server: mailserver.com Port: 25

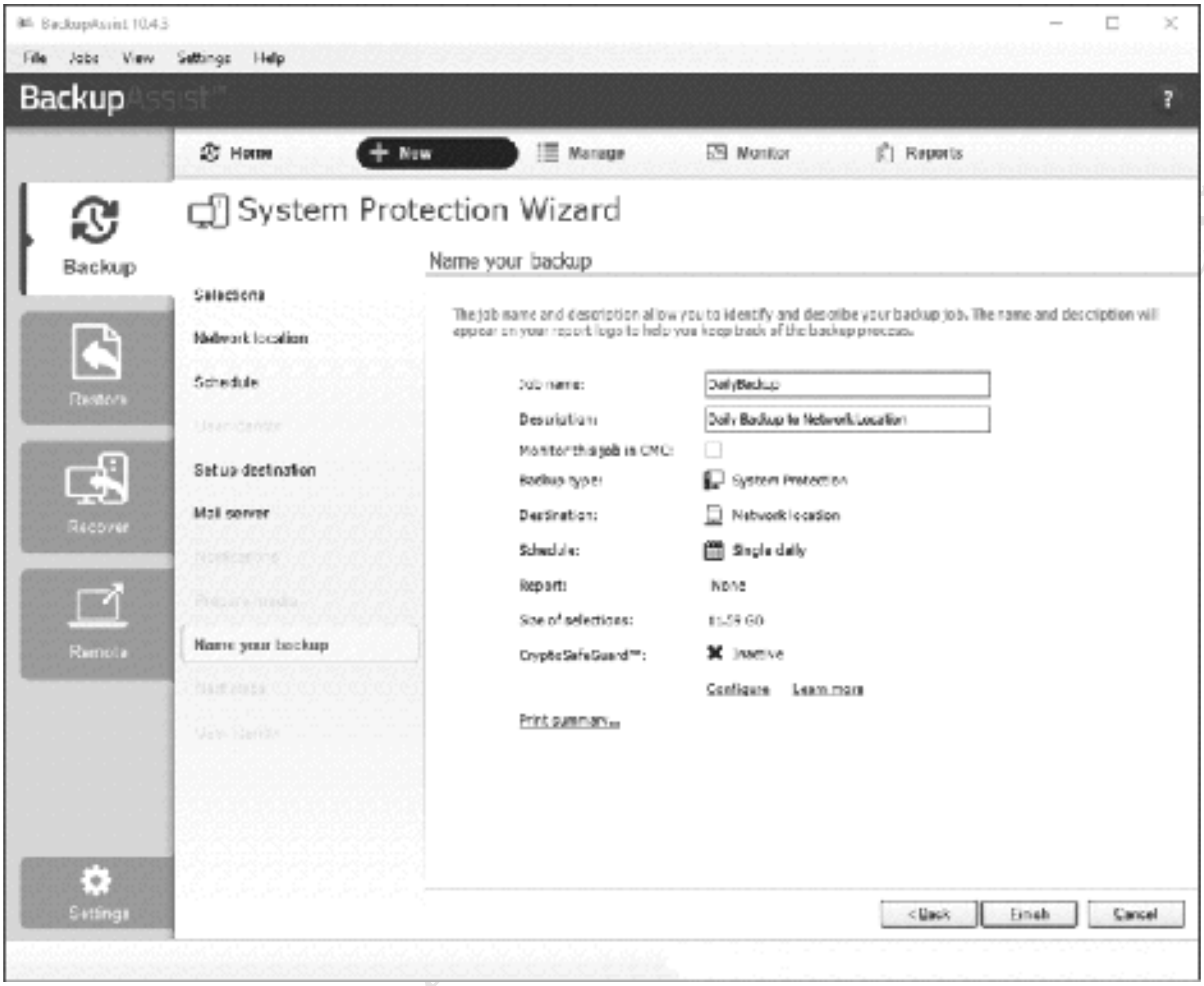
Connection type: Autodetect

Username:

Password:

Figure 102: Email features in BackupAssist

A summary screen is shown. Give the backup job a descriptive name and click **Finish**.



System Protection Wizard

Name your backup

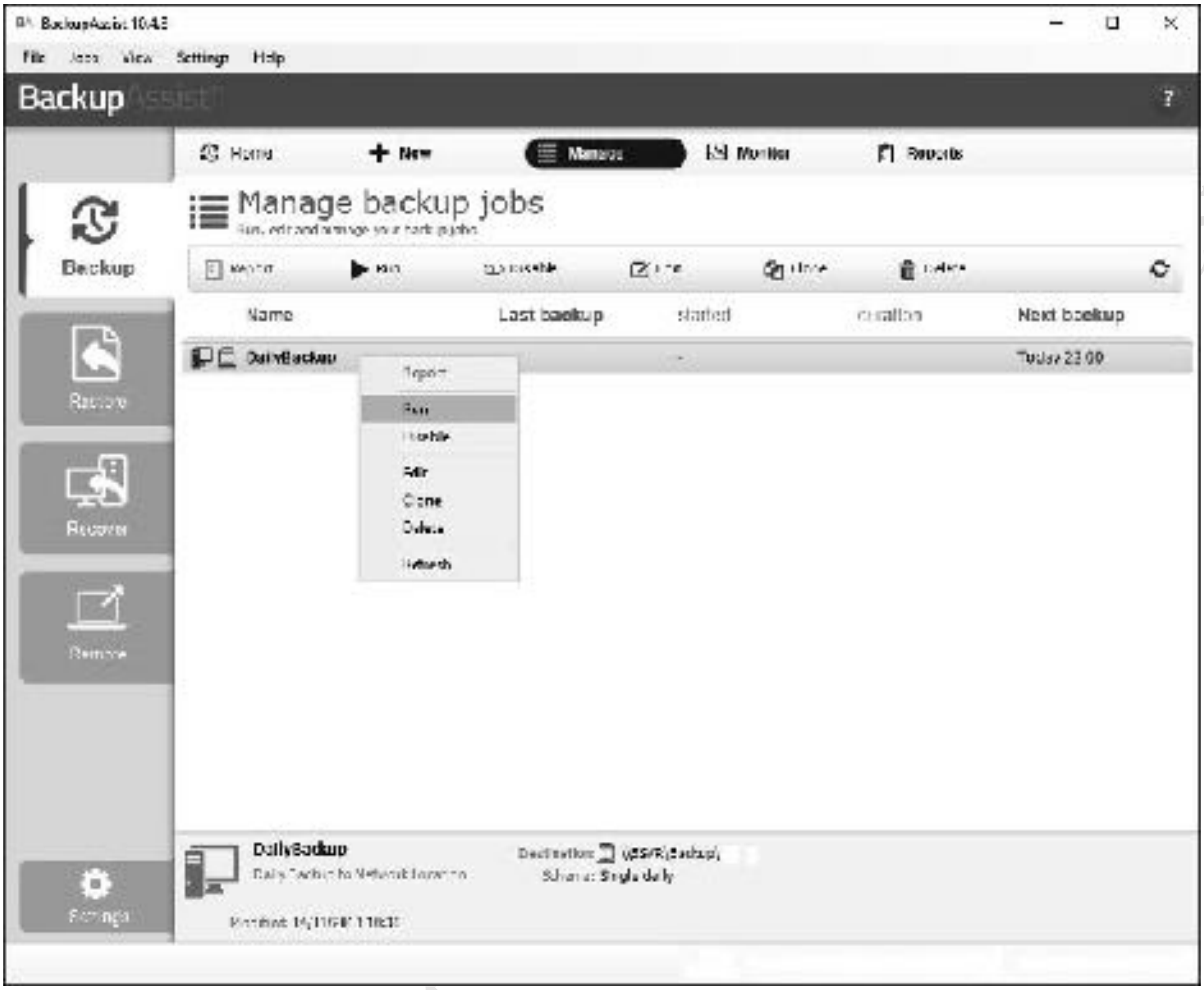
The job name and description allow you to identify and describe your backup job. The name and description will appear on your report logs to help you keep track of the backup process.

Job name:	DailyBackup
Description:	Daily Backup to Network Location
Monitor this job in CMC:	□
Backup type:	System Protection
Destination:	Network location
Schedule:	Single daily
Report:	None
Size of selections:	11.59 GB
CryptoSafeGuard™:	✖ Inactive
	Configure Learn more

Print summary...

Figure 103: Summary screen

The newly defined backup job will be listed on the *Manage backup jobs* screen. Rather than wait for it to run at the scheduled time, it can be tested immediately by right-clicking it and choosing **Run** or by clicking the **Run** icon:



Name	Last backup	Started	Duration	Next backup
DailyBackup		-		Today 23:00

DailyBackup
Daily backup to Network location
Destination: \\BS\R\Backup\
Scheme: Single daily
Modified: 14/11/2018 11:38

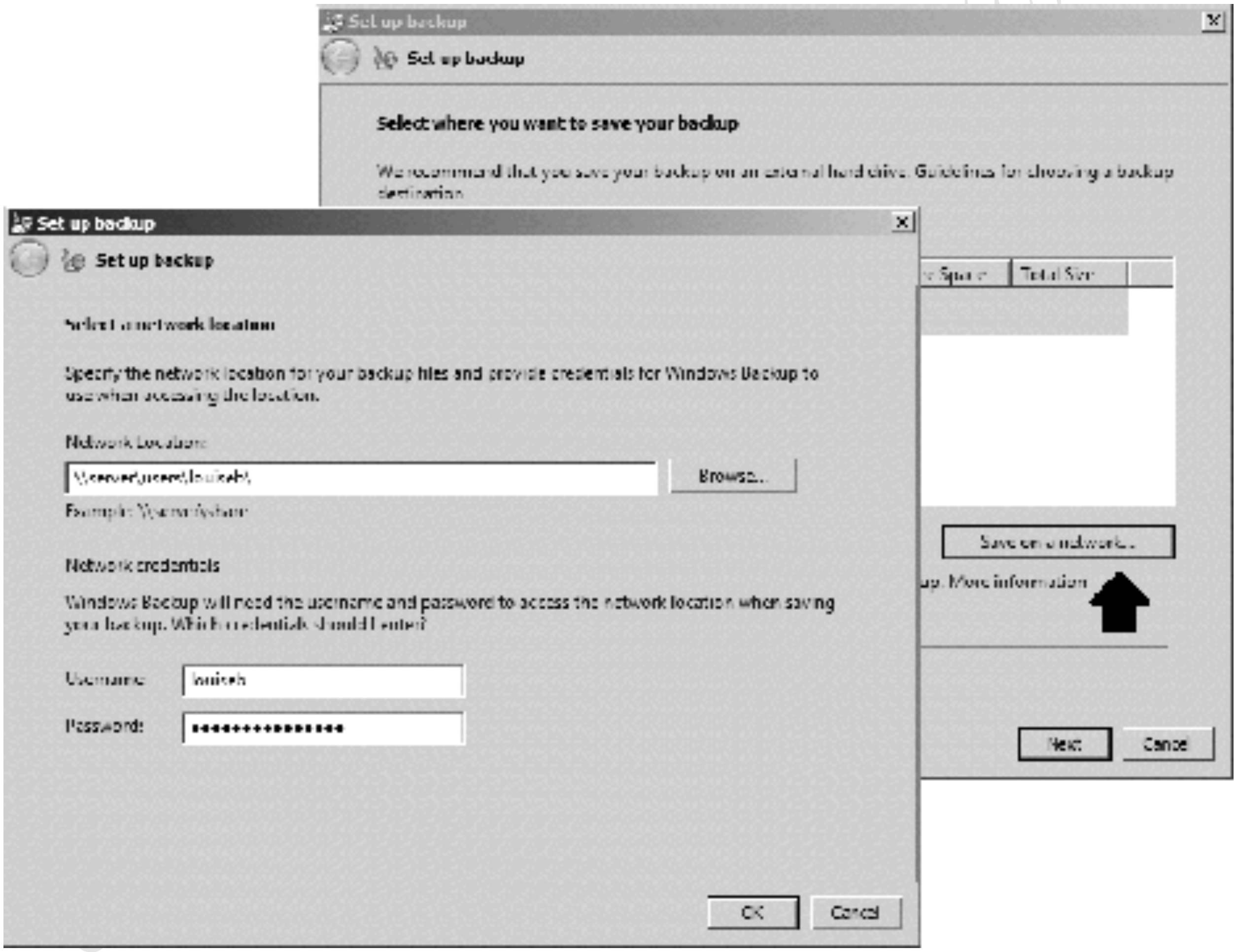
Figure 104: List of backup jobs and Run option

6.8 Backing up Computers to the Server

If users store data on their computers rather than on the network, then there is probably a requirement to be able to backup that data. This can be done using the built-in backup programs in Windows Professional clients, with the actual backups stored on the server. As the server itself is being backed up, this will ensure multiple copies of the data, hopefully enough to cope with any eventuality.

Backing up Windows 7 Computers

Click **Start**, followed by **All Programs**, **Maintenance** then **Backup and Restore**. Click **Set up Backup** and then the **Save on a network** button. On the next panel, enter the **Network Location**. Specify the user's home folder, using the format *\\server\homes\username* (or click the **Browse** button to navigate to it). You may be prompted to login - enter the user name and password as defined on the server and click **OK**:



Set up backup

Select where you want to save your backup

We recommend that you save your backup on an external hard drive. Guidelines for choosing a backup destination

...up. More information

Set up backup

Select a network location

Specify the network location for your backup files and provide credentials for Windows Backup to use when accessing the location.

Network Location: \\server\users\louiseh\

Example: \\server\share

Network credentials

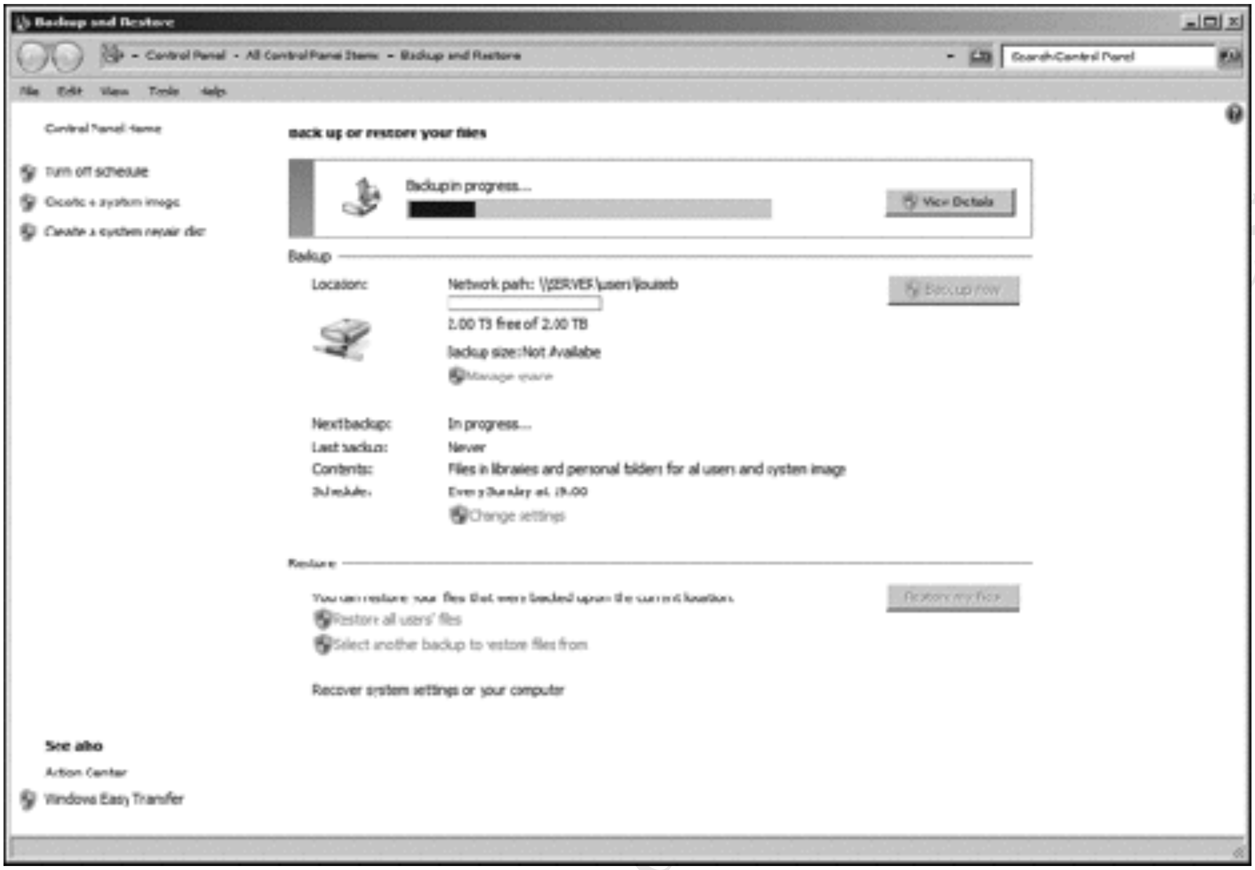
Windows Backup will need the username and password to access the network location when saving your backup. Which credentials should I enter?

Username: louiseh

Password: •••••••••••••••

Figure 105: Enter network details

The subsequent screen is for choosing what data files are backed up. The default option of **Let Windows choose (recommended)** is fine in most cases, so just click **Next**. The follow-on screen is a summary of settings: click **Save settings and run backup**. The backup will then run for the first time, during which the status is displayed. By default, Windows has defined a schedule to subsequently run backups automatically on a regular basis (in this case, every Sunday at 7:00pm). If this setting is not suitable it can be changed by clicking **Change settings**.



Back up or restore your files

Backup in progress...

Backup

Location: Network path: \\SERVER\users\louiseb

2.00 TB free of 2.00 TB

Backup size: Not Availabe

Next backup: In progress...

Last backup: Never

Contents: Files in libraries and personal folders for all users and system image

Schedule: Every Sunday at 19:00

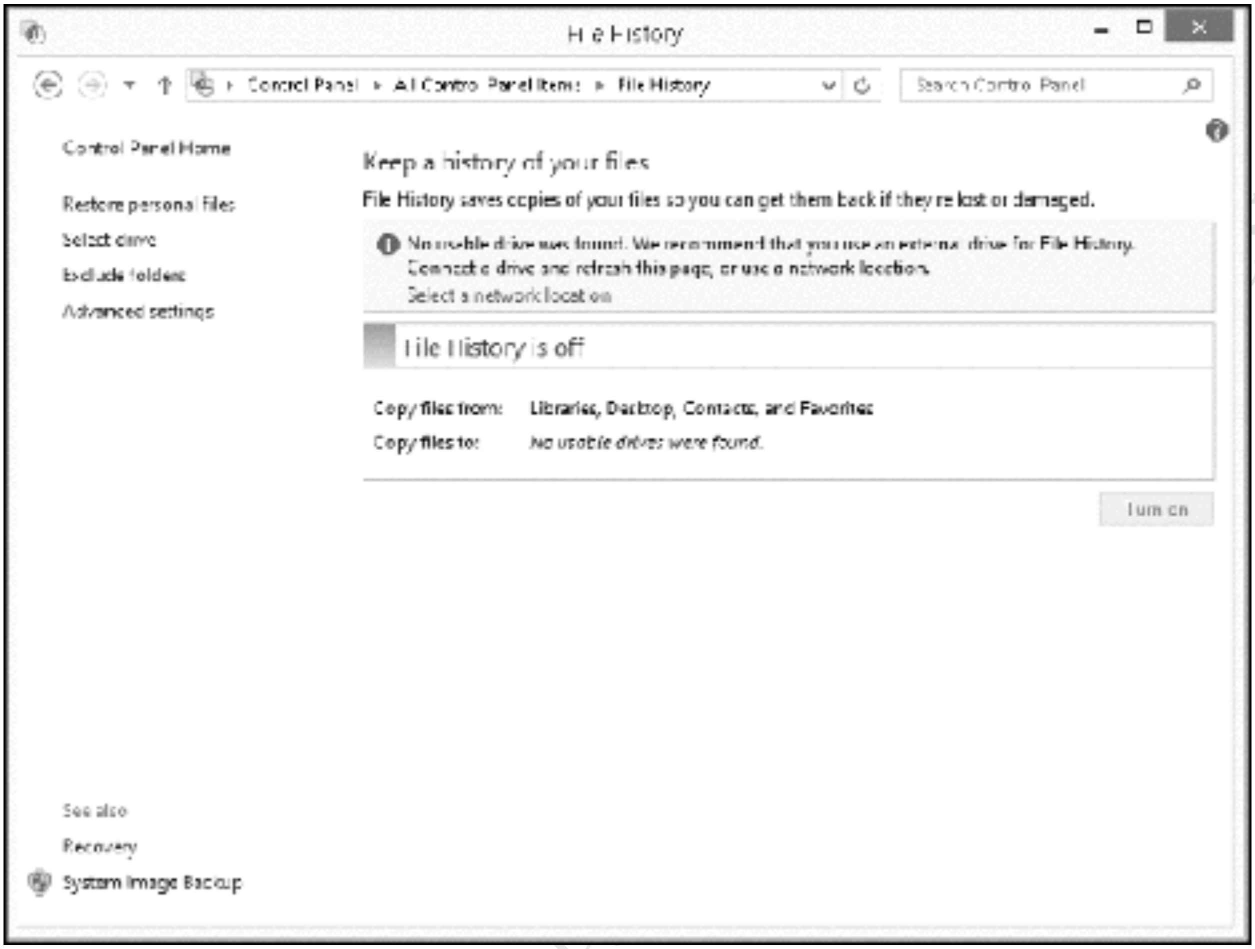
Restore

You can restore your files that were backed up on the current location.

Figure 106: Backup in progress

Backing up Windows 8/8.1 Computers

Begin by mapping the user’s home drive on the network drive using one of the techniques described in section 5. CONNECTING DEVICES TO THE SERVER. Then go into the **Control Panel** and click **File History** (remember that in Windows 8.1 and Windows 10 you can right-click the Start button to find the Control Panel):



Keep a history of your files

File History saves copies of your files so you can get them back if they're lost or damaged.

No usable drive was found. We recommend that you use an external drive for File History. Connect a drive and refresh this page, or use a network location.

Select a network location

File History is off

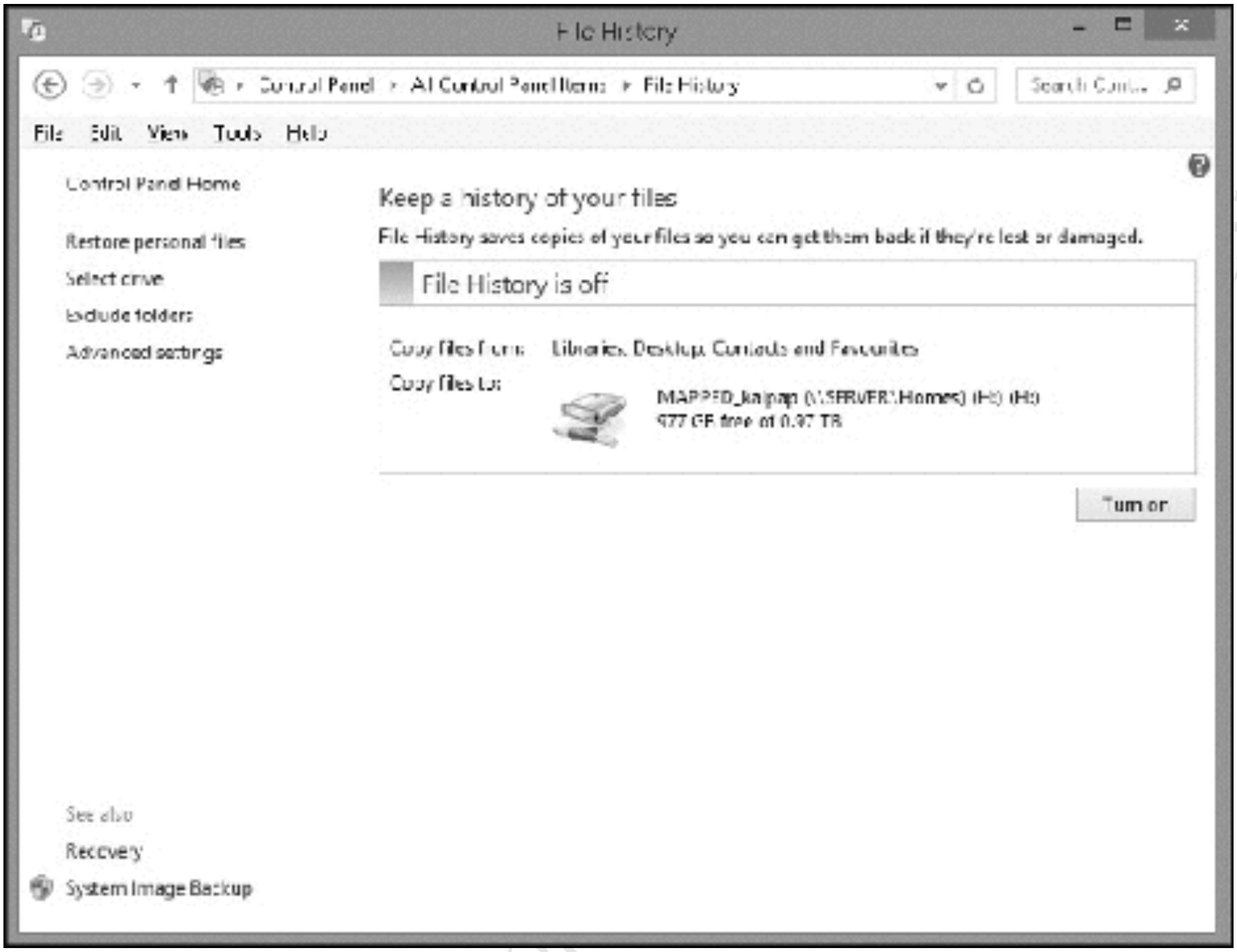
Copy files from: Libraries, Desktop, Contacts, and Favorites

Copy files to: *No usable drives were found.*

Figure 107: Initial screen in File History

Click **Select a network location**. On the screen that is displayed click **Show all network locations**. From the list, choose the user's home folder and click **Verify your credentials**. Enter the user name and password as defined on the server if prompted; if the computer is only ever used by one person you can tick the **Remember my credentials** box.

Click **OK** to return to the initial File History screen and on it click the **Turn on** button. After a few seconds, the backup will run for the first time. Thereafter, it can be run at any point by clicking **Run now**.



Keep a history of your files

File History saves copies of your files so you can get them back if they're lost or damaged.

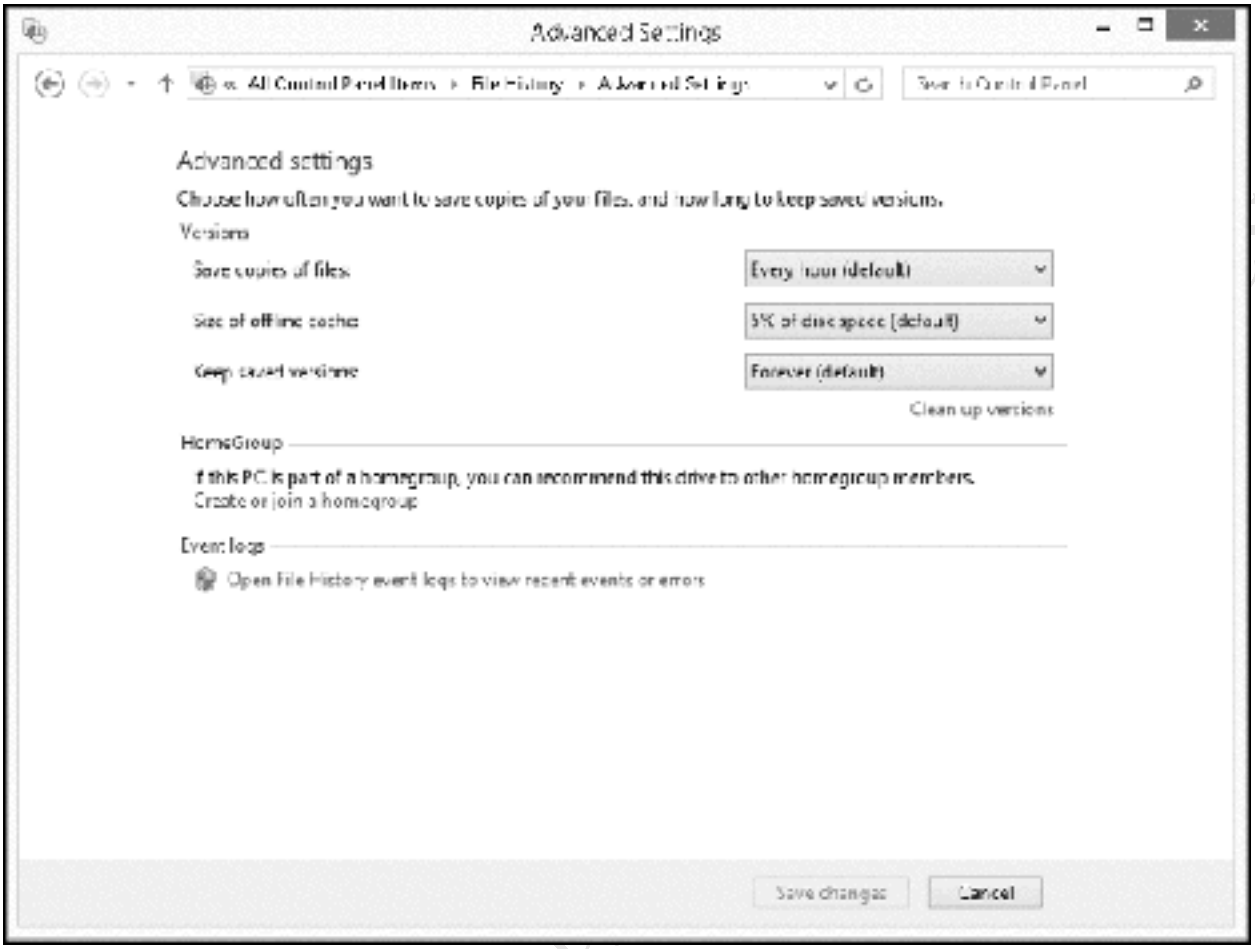
File History is off

Copy files from: Libraries, Desktop, Contacts and Favourites

Copy files to: MAPPED_kaipap (\\SERVER\Homes) (H:) (H:)
977 GB free of 0.97 TB

Figure 108: Turn on File History

For greater control over the process, such as controlling the frequency at which the backup runs, click **Advanced settings**:



Advanced settings

Choose how often you want to save copies of your files, and how long to keep saved versions.

Versions

Save copies of files: Every hour (default)

Size of offline cache: 5% of disk space (default)

Keep saved versions: Forever (default)

Clean up versions

HomeGroup

If this PC is part of a homegroup, you can recommend this drive to other homegroup members.

Create or join a homegroup

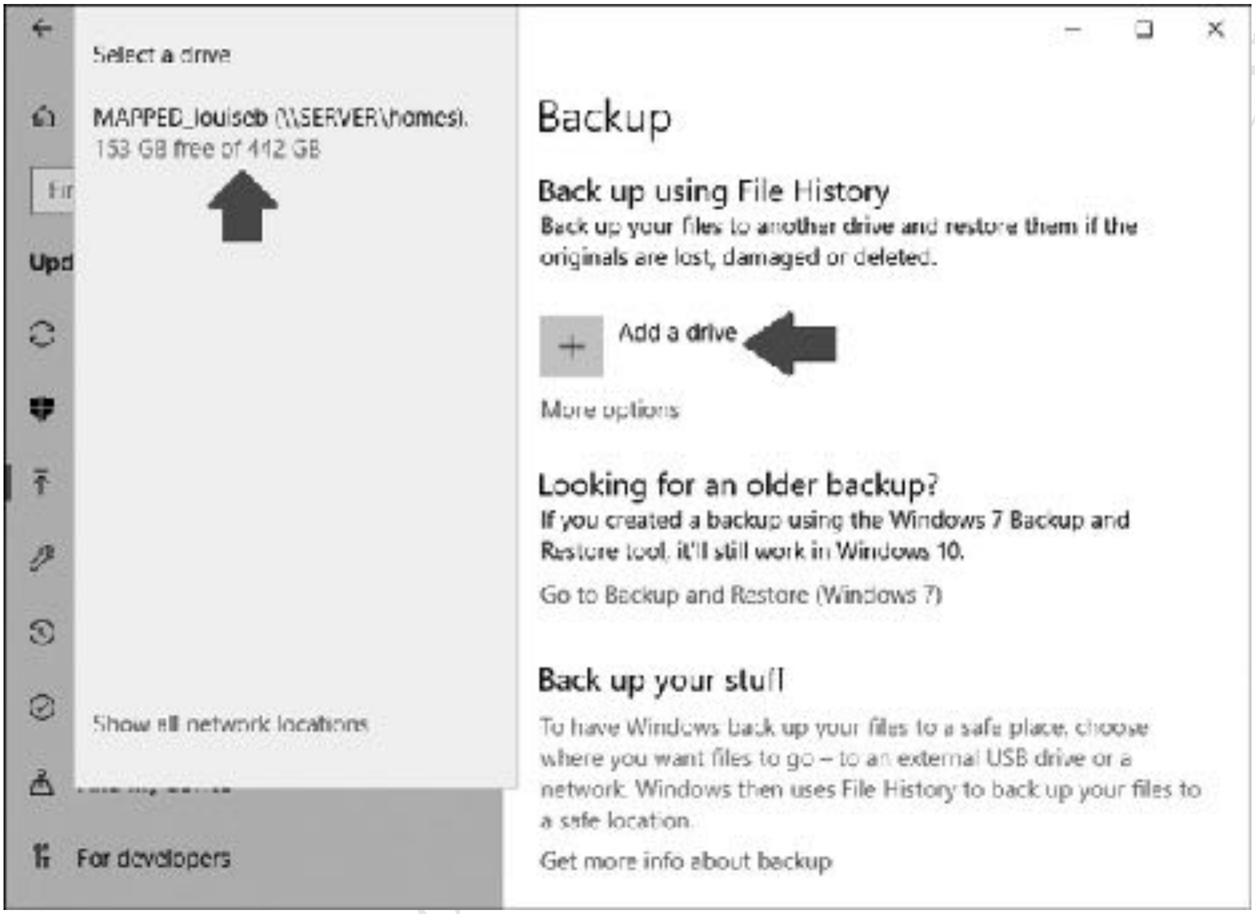
Event logs

Open File History event logs to view recent events or errors

Figure 109: File History Advanced settings

Backing up Windows 10 Computers

Click **Start** > **Settings** > **Update & Security** > **Backup**. Click **Add a drive** and after a few seconds the list of mapped drives will be displayed – click on the user's home drive:



Select a drive

MAPPED_louisdb (\\SERVER\homes).
153 GB free of 412 GB

Show all network locations

Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged or deleted.

Add a drive

More options

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Go to Backup and Restore (Windows 7)

Back up your stuff

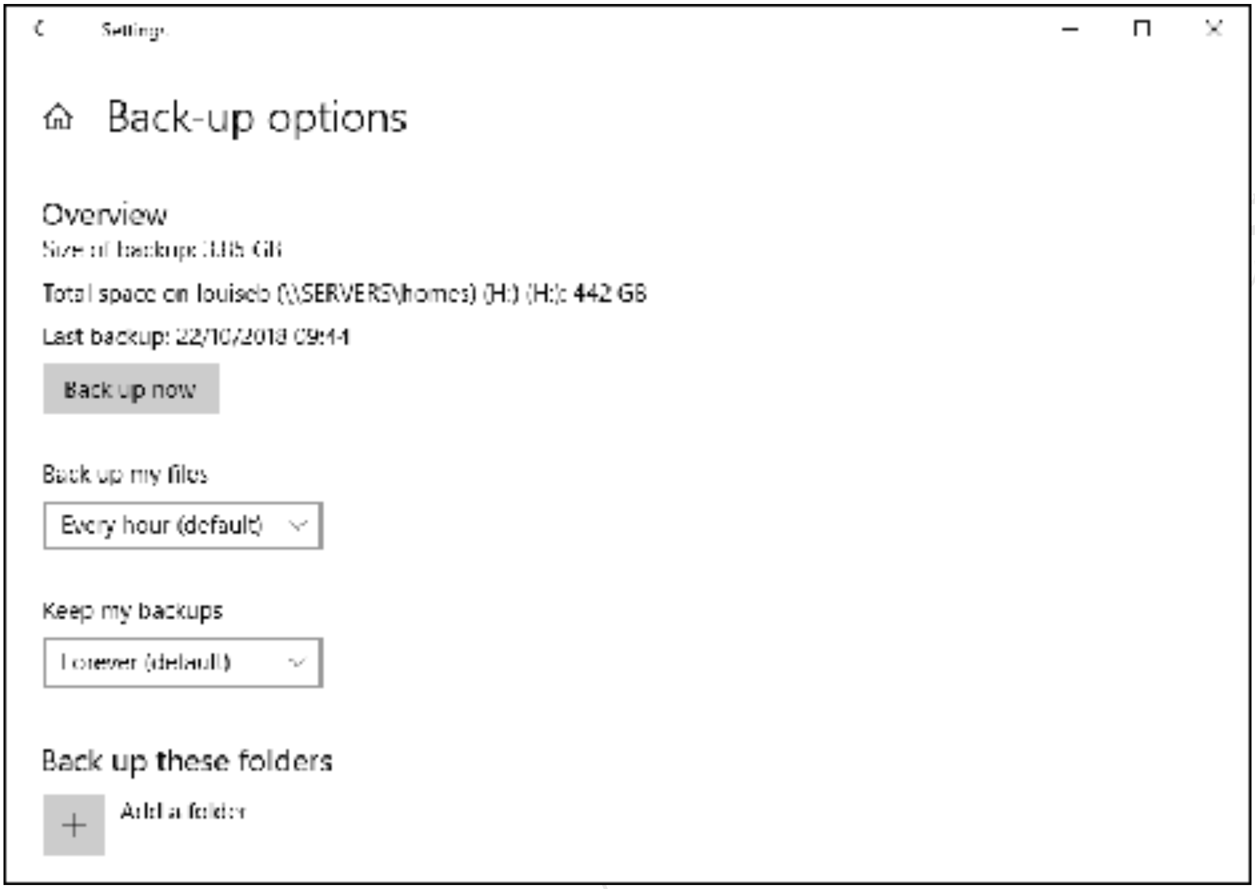
To have Windows back up your files to a safe place, choose where you want files to go – to an external USB drive or a network. Windows then uses File History to back up your files to a safe location.

Get more info about backup

Figure 110: Specify the user's home folder as the backup drive

Having done so you will be returned to the main Backup panel, where an option to *Automatically back up my files will have appeared* and been set to **On**. That's it – a backup will now run on an hourly basis, copying the user's files from the computer to their home drive on the server.

For greater control over the process, such as controlling the frequency at which the backup runs, click M**ore options**. From here you can: review the backup status; make the backup run immediately; change the backup frequency (anything from every 10 minutes through to 1 day); change the retention period for the backed-up data:



Back-up options

Overview

Size of backup: 3.85 GB

Total space on louiseb (\\SERVERS\homes) (H:) (H:): 442 GB

Last backup: 22/10/2018 09:44

Back up my files: Every hour (default)

Keep my backups: Forever (default)

Back up these folders

Figure 111: Additional backup options

7. PRINTING

7.1 Overview

An advantage of networking is that it allows printers to be shared, thus potentially saving money as well as physical space. There are several different techniques for setting up printers in a networked environment and two of them 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. Also, 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 utilise them.

Next, physically setup the printer and give it a static IP address consistent with the IP addressing scheme used in the network. This can be done on the printer itself, or via an IP reservation on the router or other source of DHCP. 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.

7.2 Networked Printer

Most printers, other than very low cost and elderly 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 relatively small network. This approach also works very well in a scenario where multiple operating systems are in use.

The printer(s) should be installed **before** the computers are added to the domain.

- 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 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 etc.)
- Remove any superfluous virtual printers (e.g. OneNote, fax, XPS and so on)
- 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 to make it their default printer.

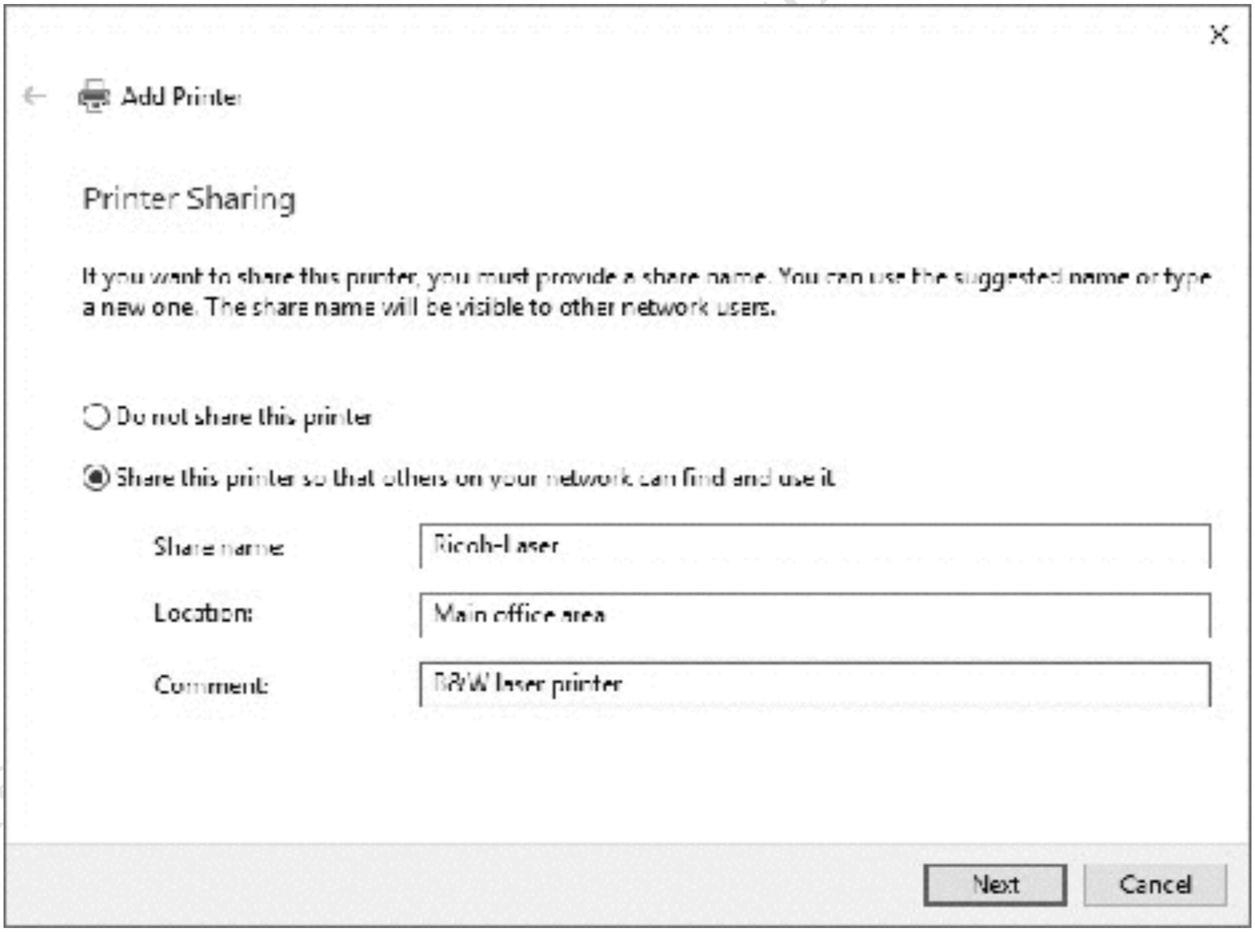
7.3 Shared Printer via Server

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 savvy. 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. One technique is to set up an additional or dummy administrative account as described in 11.2 Setup Alternative Administrator Account(s).

- Install the printer on the server using **Control Panel** > **Devices and Printers** > **Add Printer**) or by using the manufacturer's provided installation program (do not bother with the **Start** > **Devices** > **Printers & scanners** method). If there is no available driver for Server 2016, try using the Windows 10 64-bit driver. Note: if the printers were in place and powered on during the installation of Essentials then they may have been installed automatically – this can be checked through **Start** > **Settings** > **Devices**.

- Specify the printer as being on a TCP/IP port ("*Add a printer using a TCP/IP address or hostname*"). 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**:



Printer Sharing

If you want to share this printer, you must provide a share name. You can use the suggested name or type a new one. The share name will be visible to other network users.

○ Do not share this printer

● Share this printer so that others on your network can find and use it

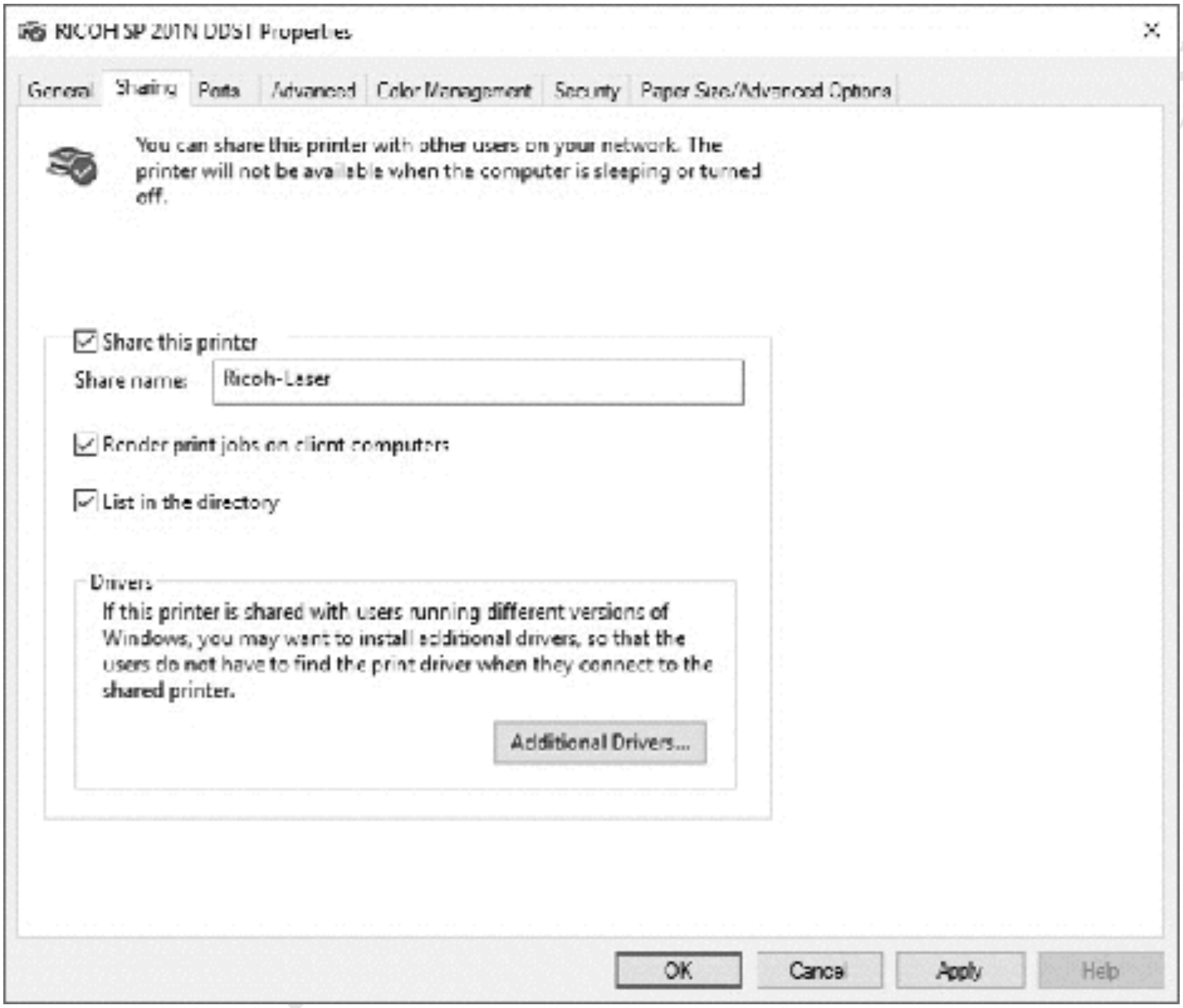
Share name: Ricoh-Laser

Location: Main office area

Comment: B/W laser printer

Figure 112: 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 **Render print jobs on client computers** and **List in the directory** boxes are ticked (there may be a *Change Sharing Options* button that you must click first):



You can share this printer with other users on your network. The printer will not be available when the computer is sleeping or turned off.

☑ Share this printer

Share name: Ricoh-Laser

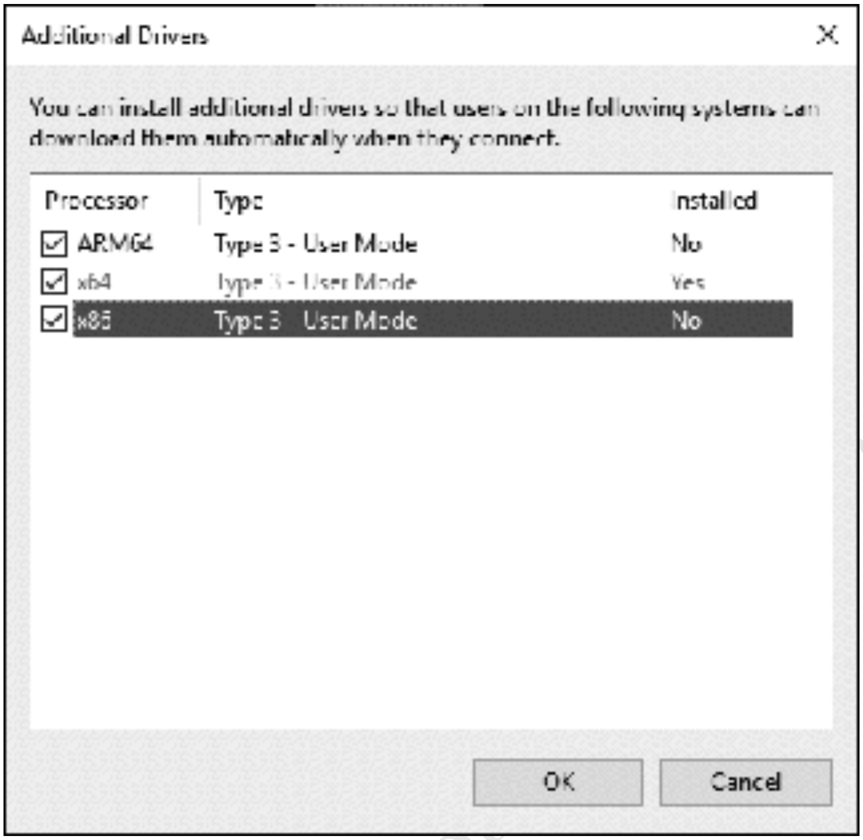
☑ Render print jobs on client computers

☑ List in the directory

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

Figure 113: 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**. This reflects the most common scenario with printers, referred to by Microsoft as *Type 3* printers. With some printers – usually more recent models known by Microsoft 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:



Additional Drivers

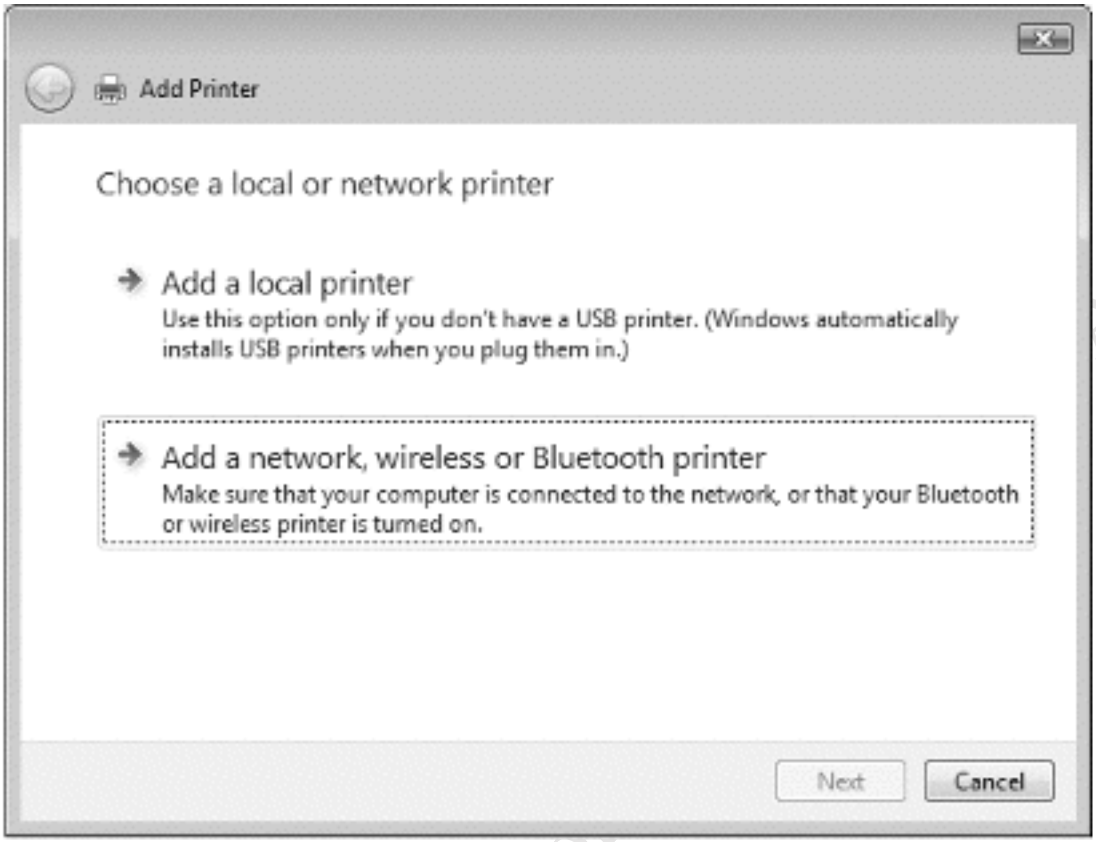
You can install additional drivers so that users on the following systems can download them automatically when they connect.

Processor	Type	Installed
☑ ARM64	Type 3 - User Mode	No
☑ x64	Type 3 - User Mode	Yes
☑ x86	Type 3 - User Mode	No

Figure 114: 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**:



Add Printer

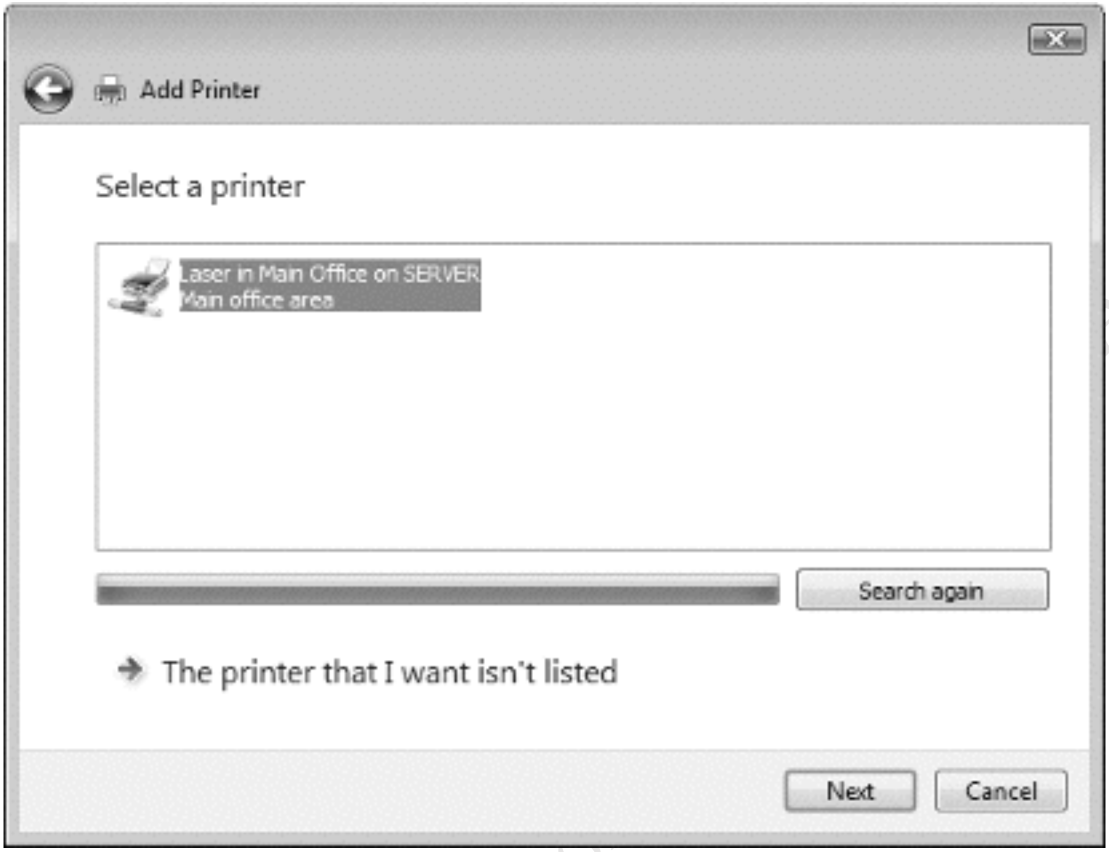
Choose a local or network printer

Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)

Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

Figure 115: Adding a printer

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



Add Printer

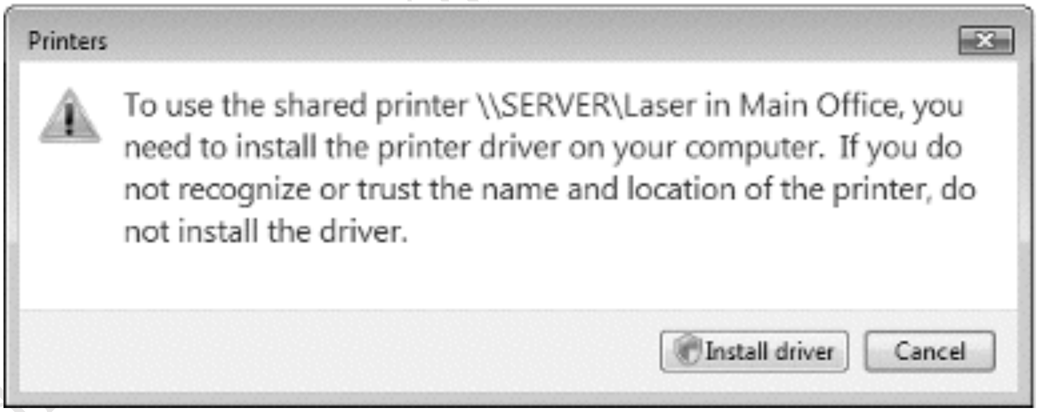
Select a printer

Laser in Main Office on SERVER
Main office area

The printer that I want isn't listed

Figure 116: Select a printer

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



Printers

To use the shared printer \\SERVER\Laser in Main Office, you need to install the printer driver on your computer. If you do not recognize or trust the name and location of the printer, do not install the driver.

Figure 117: 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.

8. GROUP POLICY

8.1 Overview

This chapter is concerned with making the network more professional, easier to use and more manageable by using a facility called *Group Policy*. 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. This chapter is not intended as an in-depth tutorial about Group Policy, rather it is concerned with some simple practical examples of using it.

Note for users of earlier versions of Windows Server: Group Policy Management Console is installed automatically during the server installation phase so no longer has to be added as a separate feature.

8.2 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 a variety of ways:

- Click **Start** > **Windows Administrative Tools** > **Group Policy Management** or
- Click **Start** > **All apps** > **Windows Administrative Tools** > **Group Policy Management** or
- Right-click **Start** > **Control Panel** > **Administrative Tools** > **Group Policy Management** or
- Press **Windows key** + **R**. Type **gpmc.msc** in the box and press **Enter**

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 might imply, 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:

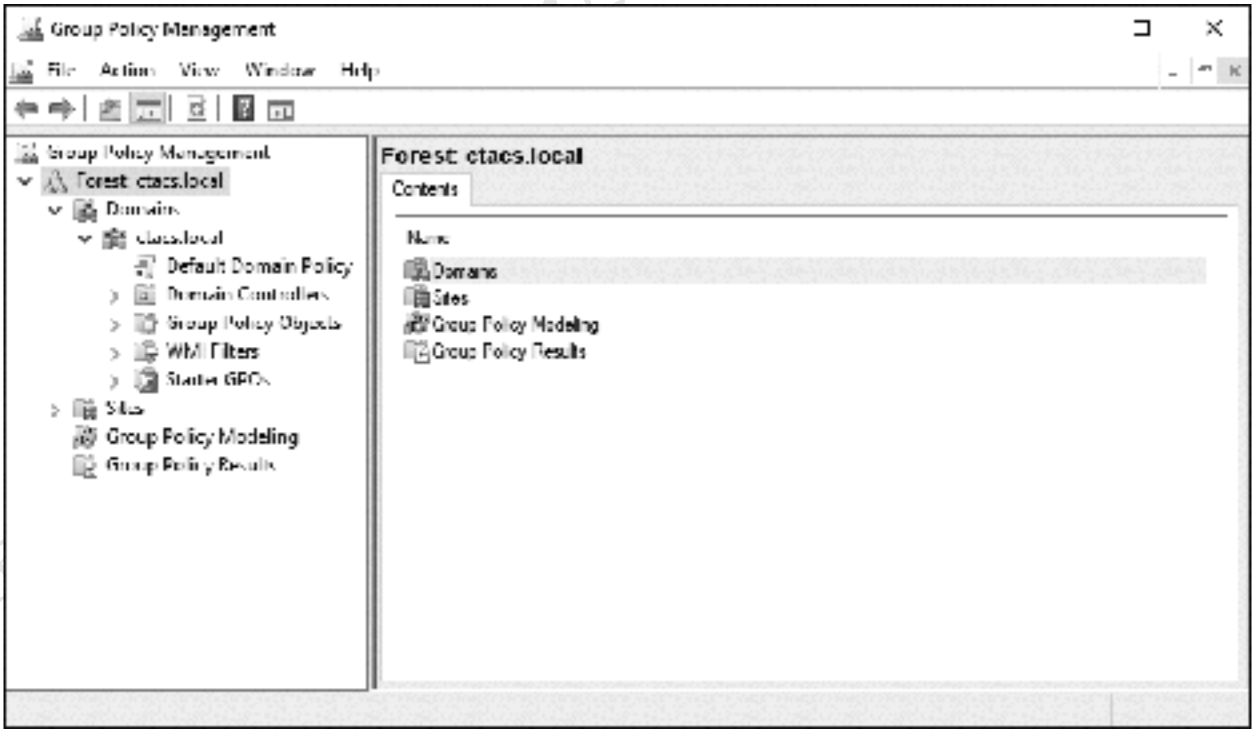
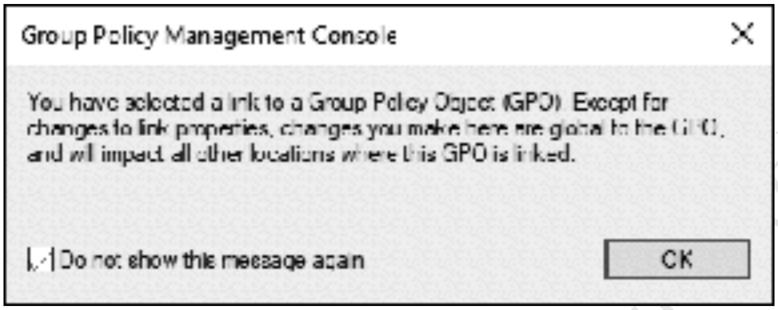


Figure 118: Group Policy Management Console

Expand the tree in the left-hand panel to display the overall structure of the domain. In the above example, the default structure for a newly-created domain with a single server is shown. 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 perhaps 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 efforts will focus on it.

Making a change involves right-clicking an item – such as *Default Domain Policy* – and choosing **Edit**. Sometimes when doing so you will receive the following warning – you may wish to tick the **Do not show this message again** box:



You have selected a link to a Group Policy Object (GPO). Except for changes to link properties, changes you make here are global to the GPO, and will impact all other locations where this GPO is linked.

☑ Do not show this message again

Figure 119: Group Policy Management console warning message

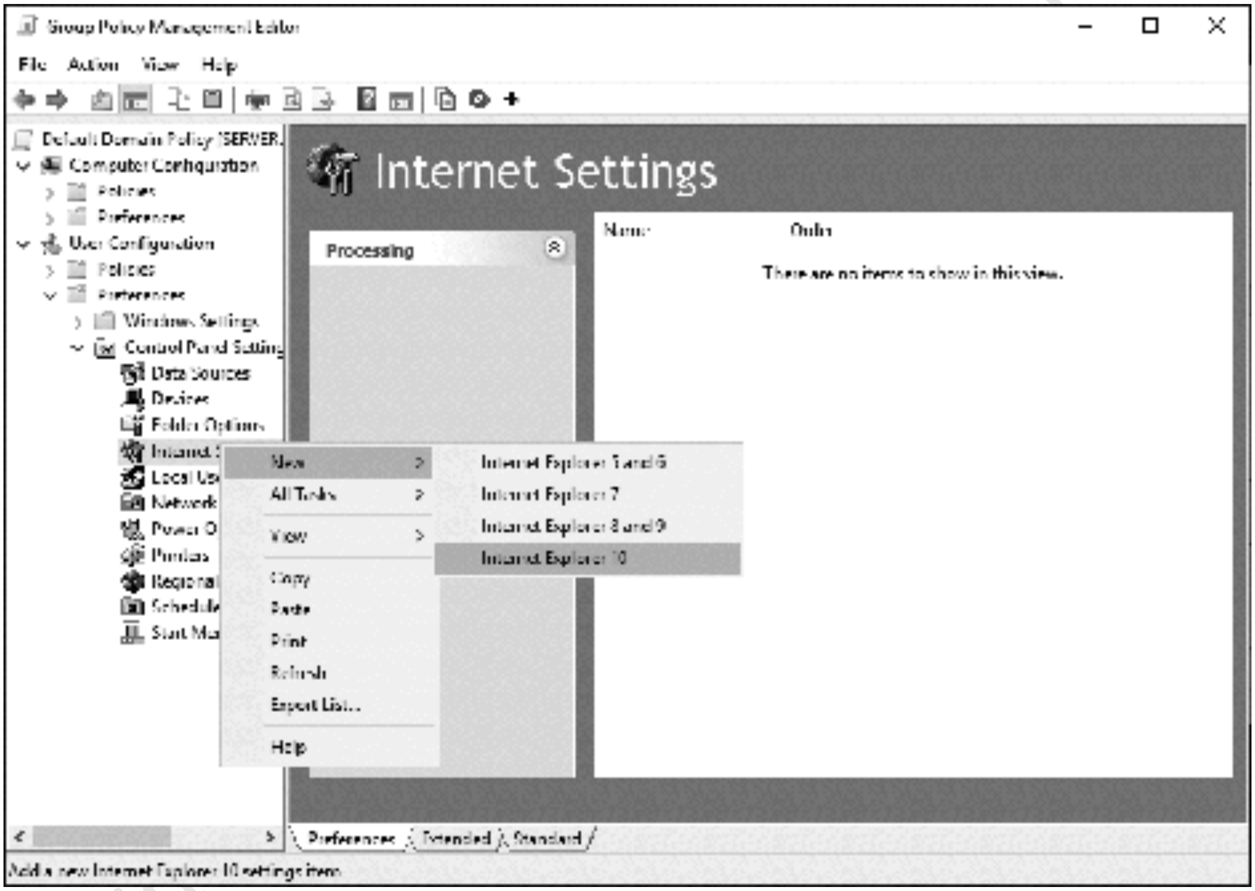
Policies are created or modified for the *Computer Configuration* or *User Configuration*, the former affecting a defined group of computers and the latter affecting a defined group of users. There is no requirement to explicitly save changes, as it is implicit when making modifications. The policies 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 7 and not relevant to, say, Windows XP at all. However, the majority are applicable to all versions of Windows.

8.3 Specifying the Home Page

Some organizations require that all users have a standard home page within Internet Explorer, for example the company's website or an email system such as *Office365* or *Google Mail* and Group Policy can be used to achieve this.

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 **User Configuration** > **Preferences** > **Control Panel Settings**. Right-click the entry for **Internet Settings** and choose **New**. A pop-up listing various versions of Internet Explorer is shown; note that most of these are now long obsolete and should no longer be in general use, also that the most recent version from 2013, Internet Explorer 11, is not listed (it will in fact use the Internet Explorer 10 settings), nor is the Edge browser:

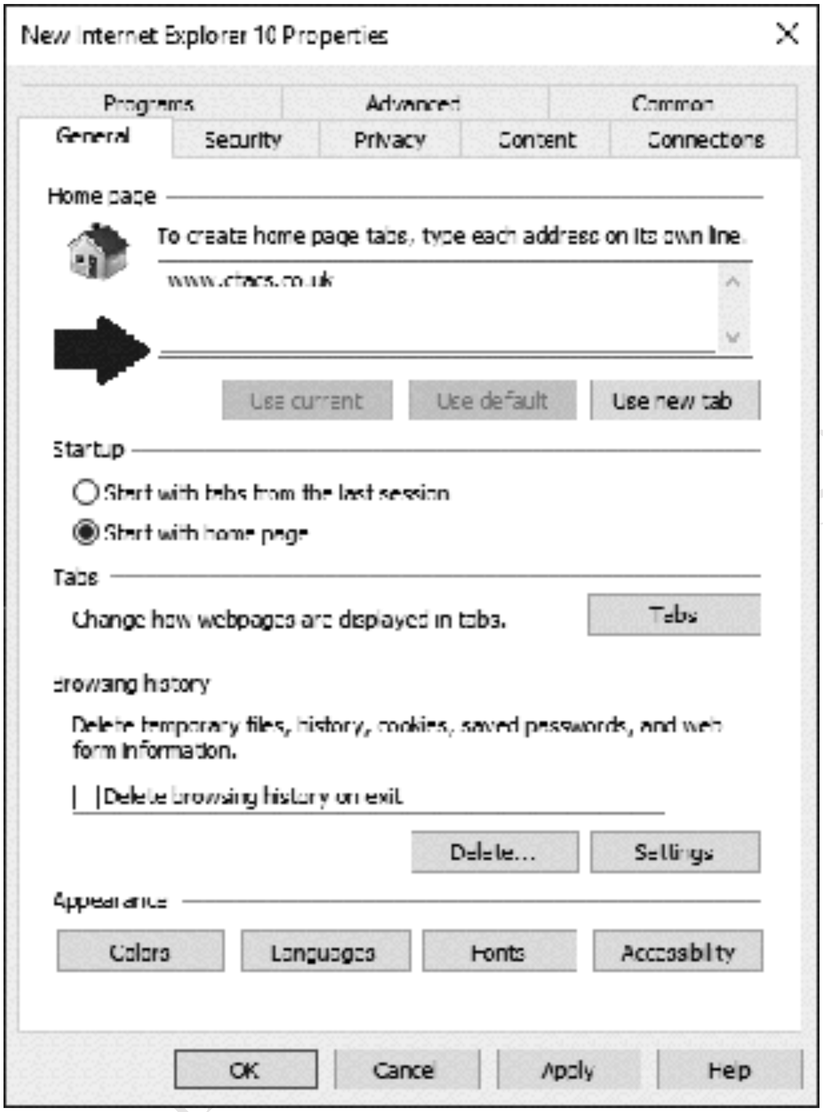


There are no items to show in this view.

Add a new Internet Explorer 10 settings item.

Figure 120: 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. Type in the details for the desired standard home page:



New Internet Explorer 10 Properties

Home page

To create home page tabs, type each address on its own line.

www.ctacs.co.uk

Startup

○ Start with tabs from the last session

● Start with home page

Tabs

Change how webpages are displayed in tabs.

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

Appearance

Figure 121: 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. This step is very important and unless this is done the setting will not apply. Also, click the **Start with home page** option. Click **Apply** and **OK**. Close the Group Policy Management Console.

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

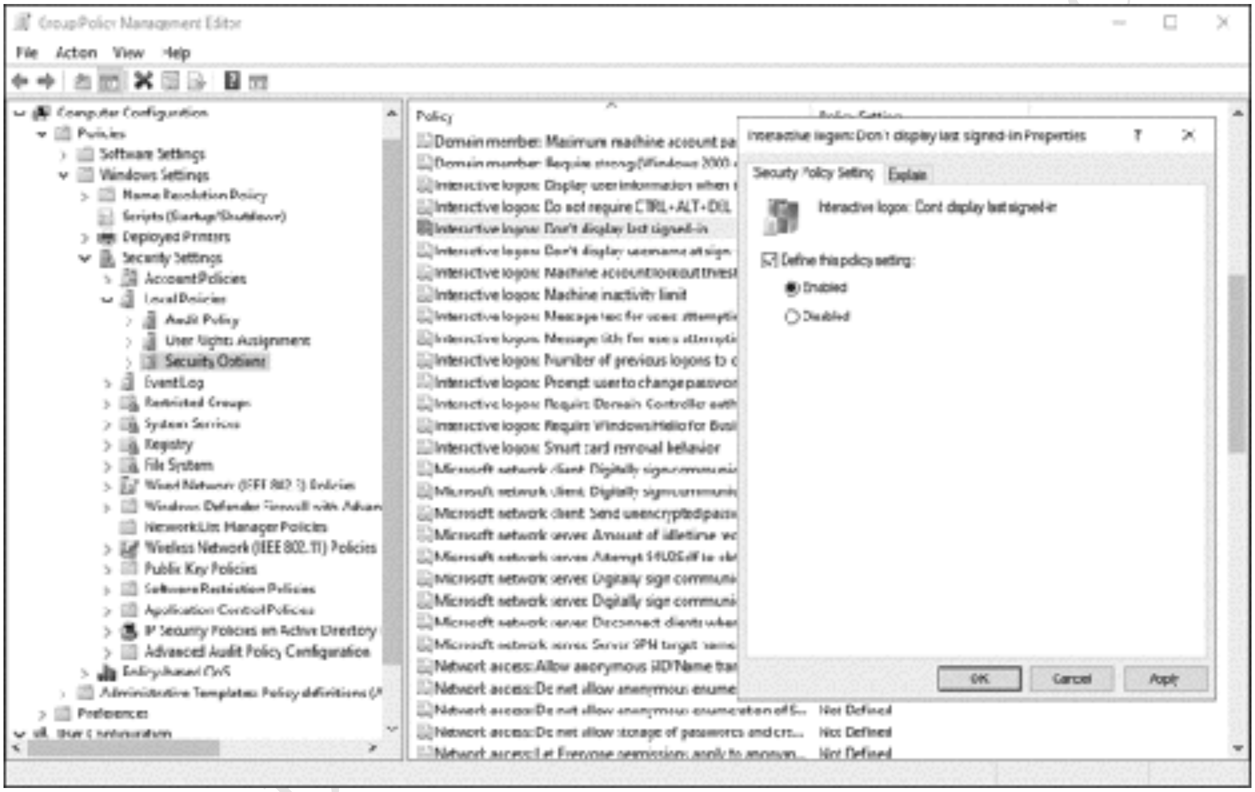
Internet Explorer is the only browser supported by Microsoft through Group Policy. If Firefox or Chrome are used, then various solutions and workarounds can be found by Googling the topic.

Incidentally, it is not widely known but individual policies can be renamed. For instance, the one we have just created above will have a name of *Internet Explorer 10*. Right-click it, choose **Rename** and change it to something more meaningful, such as *Home Page*.

8.4 Windows Logon Behaviour

By default, Windows 7 clients and later 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.

On the server, launch the **Group Policy Management** Console. Right-click the *Default Domain Policy* and click **Edit**. Drill down to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options.** Find **Interactive login: Do not display last user name**. Double-click it then click **Define this policy setting** and **Enabled**, followed by **OK**.


Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advan
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions
Preferences
User Configuration
Policy
Policy Setting
Interactive logon: Don't display last signed-in Properties
Security Policy Setting
Explain
Interactive logon: Dont display last signed-in
OK
Cancel
Apply

☑ Define this policy setting:

● Enabled

○ Disabled

Figure 122: Interactive logon settings

8.5 Logon Warning/Security Message

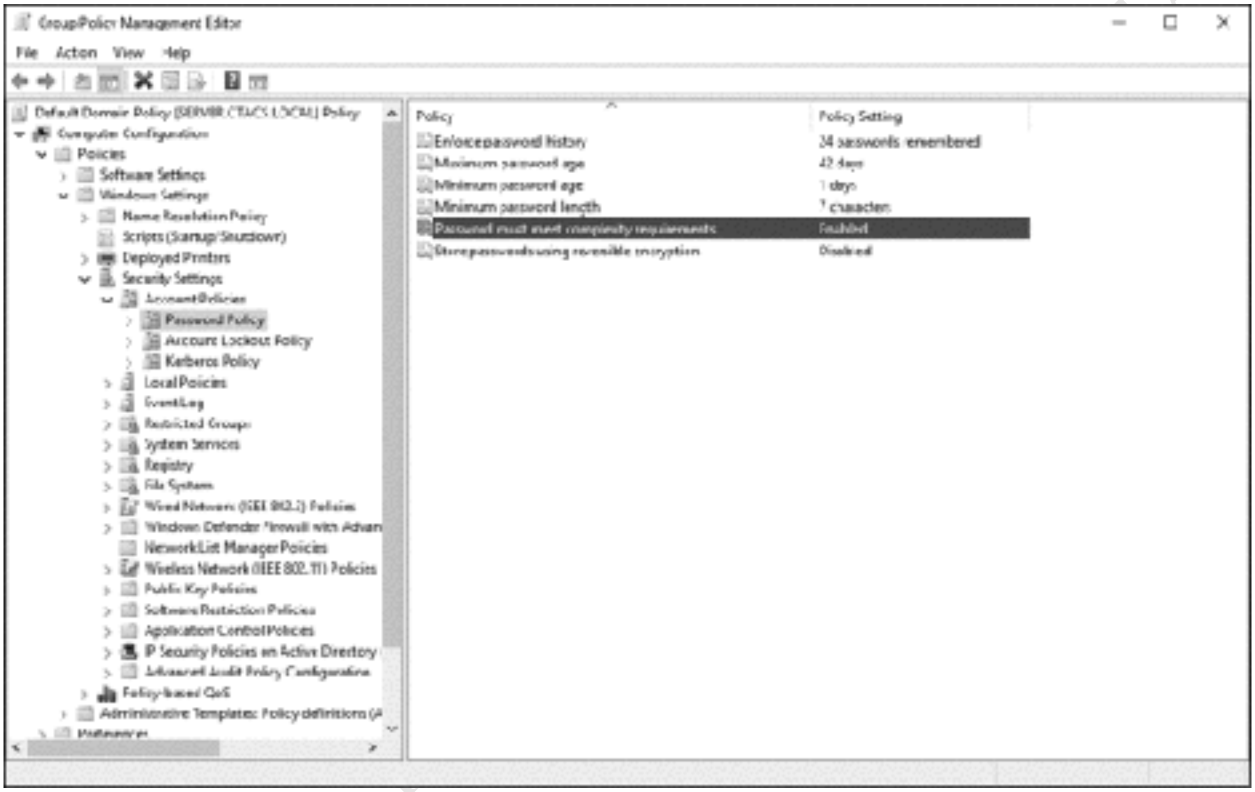
Group Policy can be used to specify a message that appears at the logon screen. For instance, the message could state the name of the organization (“ACME Inc.”) along with an advisory or warning message (“Do not attempt to use this computer system unless you have been authorized to do so”). There are 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**.

8.6 Changing the Password Policy

By default, Windows Server 2016 has a password policy of *complex passwords*, which means that passwords must comprise a mixture of letters, numbers and special characters. By using complex passwords, security is enhanced. For instance, it is very unlikely that an unauthorised user or hacker would be able to guess a password such as *!!40#mgzjeu23!398ab*. However, in some scenarios such passwords are too complicated - for example, in a school or in a work environment with many casual users - in which case the policy can be adjusted.

To do so, go into **Group Policy Management;** expand the tree to display the *Default Domain Policy*, right-click it and choose **Edit**. Drill down to: **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Account Policies** > **Password Policy**:


GroupPolicy Management Editor
File
Action
View
Help
Default Domain Policy [SERVER.CTACS.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advan
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (A
Preferences

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Figure 123: Specifying the Password Policy

To remove the requirement for complex passwords, change **Password must meet complexity requirements** to **Disabled**.

To prevent users being forced to change their passwords on a regular basis, change **Maximum password age** to 0 and **Minimum password age** to 0.

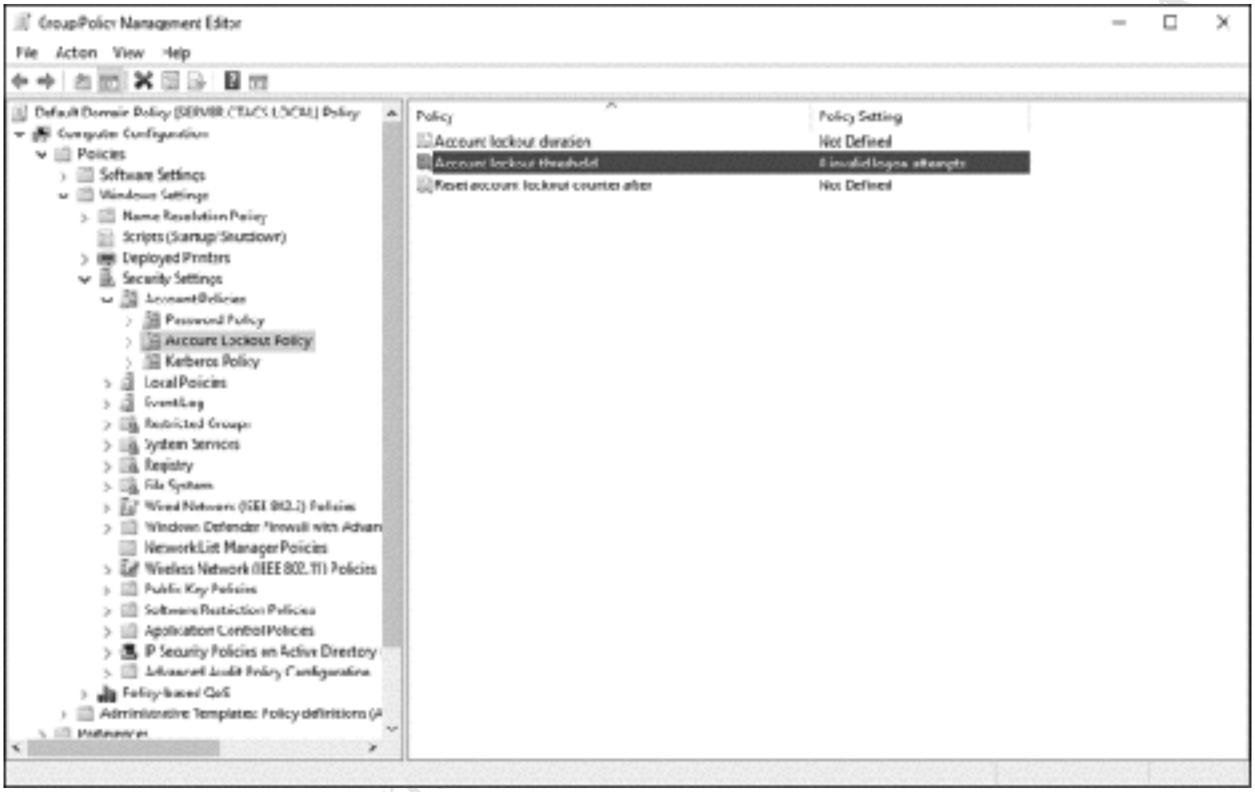
To remove the requirement for passwords to be of a minimum length, change **Minimum password length** to 0.

The defaults provided by Microsoft are sensible and designed to support a secure environment. You are free to change them as described above, but best practice is not to make them too weak.

8.7 Account Lockout Policy

Windows Server can be configured to temporarily lock a user account if there are too many unsuccessful login attempts. This can improve security, as multiple failed logins may indicate that an unauthorized user is guessing passwords in order to gain access.

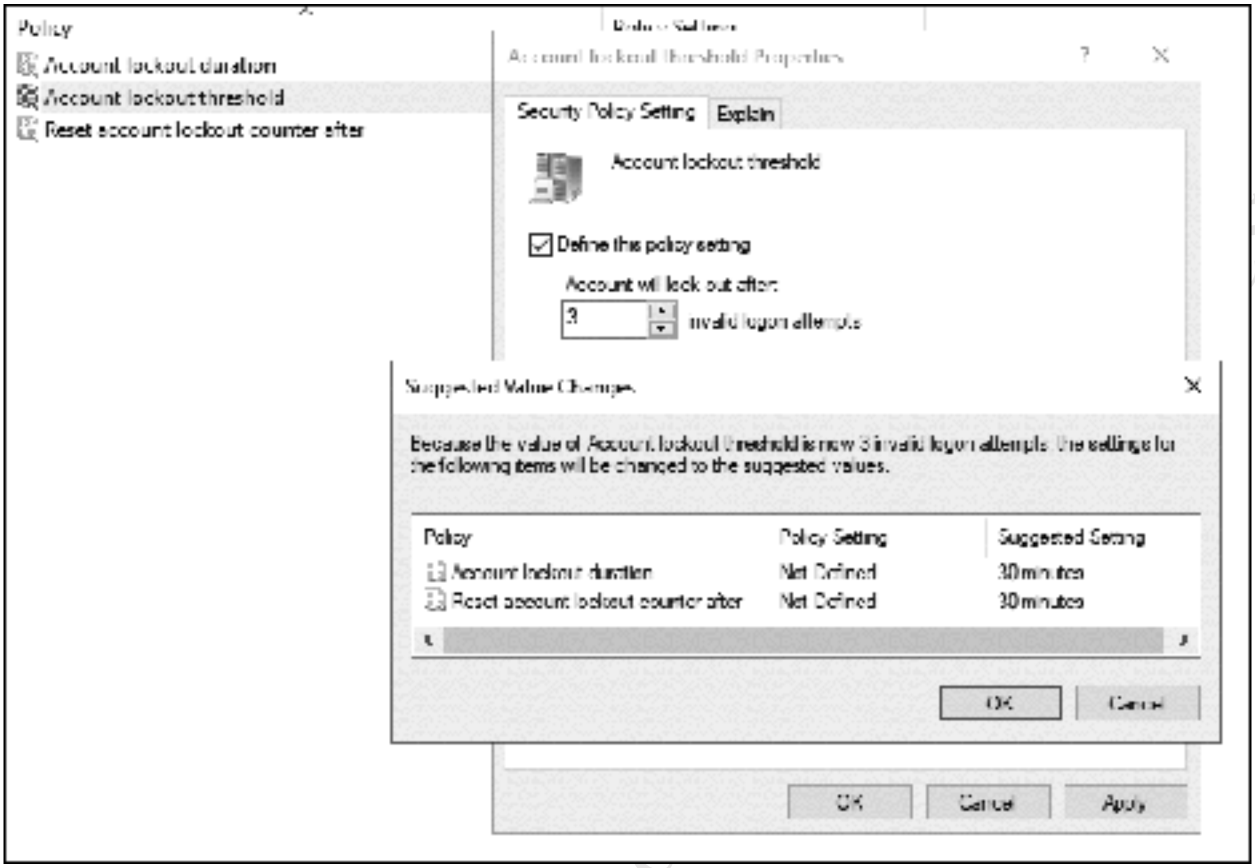
To configure this, go into **Group Policy Management;** expand the tree to display the *Default Domain Policy*, right-click it and choose **Edit**. Drill down to: **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Account Policies** > **Account Lockout Policy**:


Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [SERVER.CTACS.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advan
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (A
Preferences

Policy	Policy Setting
Account lockout duration	Not Defined
Account lockout threshold	0 invalid logon attempts
Reset account lockout counter after	Not Defined

Figure 124: Account Lockout Policy

To enable account lockout: double-click **Account lockout threshold**; tick the **Define this policy setting** box; specify the number of invalid logon attempts (typically, a value of 3 is used); click **OK**. A message is displayed with suggested values of 30 minutes for the two other items, which define the duration of an account lock and how long must pass before the account lockout counter is reset. If these values are acceptable, click **OK**. If they are not, they can be altered using the **Account lockout duration** and **Reset account lockout counter after** properties.



Policy
Account lockout duration
Account lockout threshold
Reset account lockout counter after
Policy Setting
Account lockout threshold Properties
?
X
Security Policy Setting
Explain
Account lockout threshold

☑ Define this policy setting

Account will lock out after:

3 invalid logon attempts

Suggested Value Changes

Because the value of Account lockout threshold is now 3 invalid logon attempts, the settings for the following items will be changed to the suggested values.

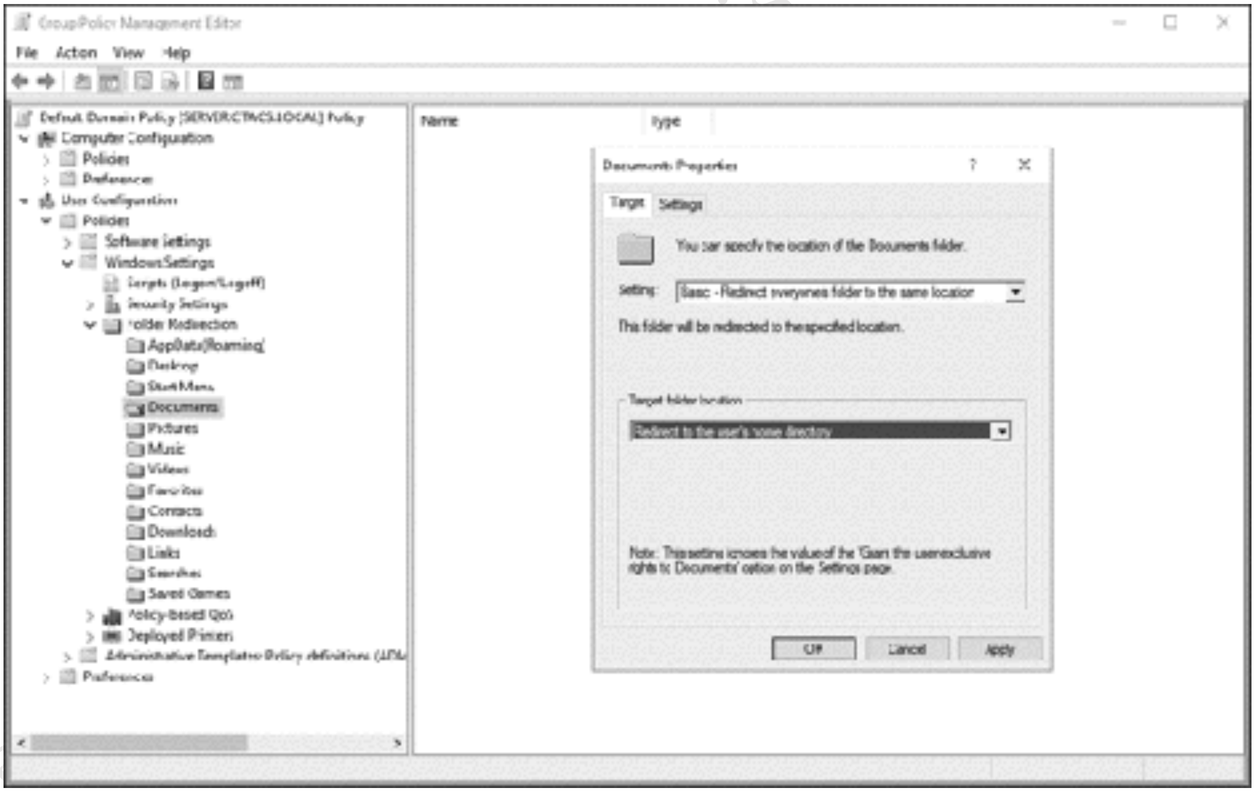
Policy	Policy Setting	Suggested Setting
Account lockout duration	Not Defined	30 minutes
Reset account lockout counter after	Not Defined	30 minutes

Figure 125: Suggested account lockout policies

8.8 Redirect the User’s Documents Folder

The purpose of this is to redirect the user’s *Documents* folder (also sometimes known as *My Documents*) from their computer to their home drive on the network. By doing so, any files the user creates will automatically be stored on the network and hence be available from any computer on the network, without the user having specifically to remember to store them on the H: drive. Another consequence of redirecting the home folder is that a feature called *offline folders* is also enabled; users who have laptops will still have their home folder documents available when working offsite and any changes made will be automatically synced when they come back into the office.

- Launch the **Group Policy Management** console
- Expand the console tree. Right-click the *Default Domain Policy* and choose **Edit**
- Expand the tree to **User Configuration** > **Policies** > **Windows Settings** > **Folder Redirections** > **Documents**
- Right-click **Documents** and choose **Properties**
- On the **Target** tab, change the **Setting** to *Basic - redirect everyone's folder to the same location* and the **Target folder location** to *Redirect to the user's home directory*.
- Click **Apply** then click **Yes** to the warning. Click the **Settings** tab.



You can specify the location of the Documents folder.

Setting: Basic - Redirect everyones folder to the same location

This folder will be redirected to the specified location.

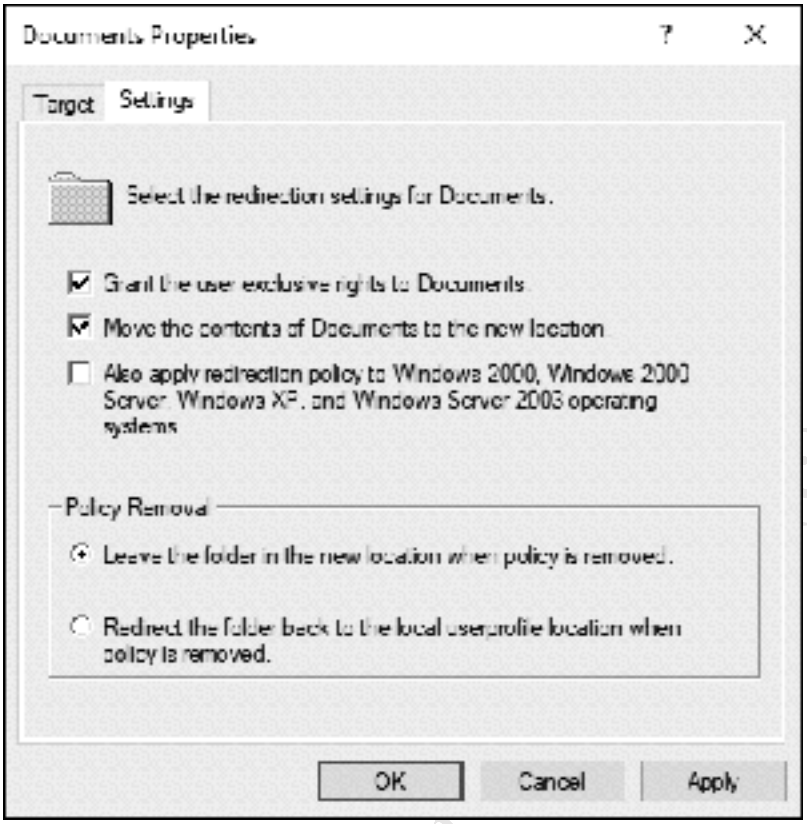
Target folder location

Redirect to the user's home directory

Note: This setting ignores the value of the 'Grant the user exclusive rights to Documents' option on the Settings page.

Figure 126: Specify location of the Documents folder

- Make sure it looks as shown below. If older versions of Windows are in use at the site, ensure the box for Windows XP and other earlier operating systems is ticked. Then click on **Apply** and **OK**.
- A warning message may be displayed. This can safely be ignored by clicking **Yes**.



Documents Properties

Target | Settings

Select the redirection settings for Documents.

☑ Grant the user exclusive rights to Documents

☑ Move the contents of Documents to the new location

□ Also apply redirection policy to Windows 2000, Windows 2000 Server, Windows XP, and Windows Server 2003 operating systems

Policy Removal

● Leave the folder in the new location when policy is removed.

○ Redirect the folder back to the local userprofile location when policy is removed.

Figure 127: Redirection settings

An additional step is needed:

From within **Group Policy Management** view the settings for the *Default Domain Policy***.** Expand to **Computer Configuration** > **Policies** > **Administrative Templates** > **Network** > **Offline Files**. The setting in the right-hand panel for **Allow or Disallow use of the Offline Files feature** should be set to **Enabled**. The setting for **Subfolders always available offline** should be set to **Enabled** if very old versions of Windows are in use.

Troubleshooting: Unfortunately, it is not uncommon to experience problems with the Offline files facility, particularly with older versions of Windows. If it is not working, try this additional change to Group Policy. For the *Default Domain Policy*, go to **Computer Configuration** > **Policies** > **Administrative Templates** > **System** > **Logon**. Enable the **Always wait for the network at computer startup and logon** option.

9. REMOTE ACCESS & VPN

9.1 Overview

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/km 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 full access to files and folders for editing, just as in the office. One big disadvantage: VPNs can be notoriously difficult to setup, configure and diagnose. For many users, virtual private networks are an advanced topic and because of this, some small business users may wish to look at simpler alternatives for remote access, for example a cloud-based service such as Dropbox (see 12.11 Using Dropbox with Windows Server).

To use a VPN, you will need a *domain name* or *host name*. You may recall that you have an *internal domain name*, for example *ctacs.local*, but this cannot be accessed from over the internet and you therefore also require an *external domain name*, which can be accessed. Examples of external domain names would be *www.ctacs.co.uk*, *www.google.com*, *www.microsoft.com* and so on. They can be obtained from domain registration companies such as *GoDaddy*, *Register.Com*, *Name.Com* and others. Your internet service provider (ISP) may also be able to provide a domain name.

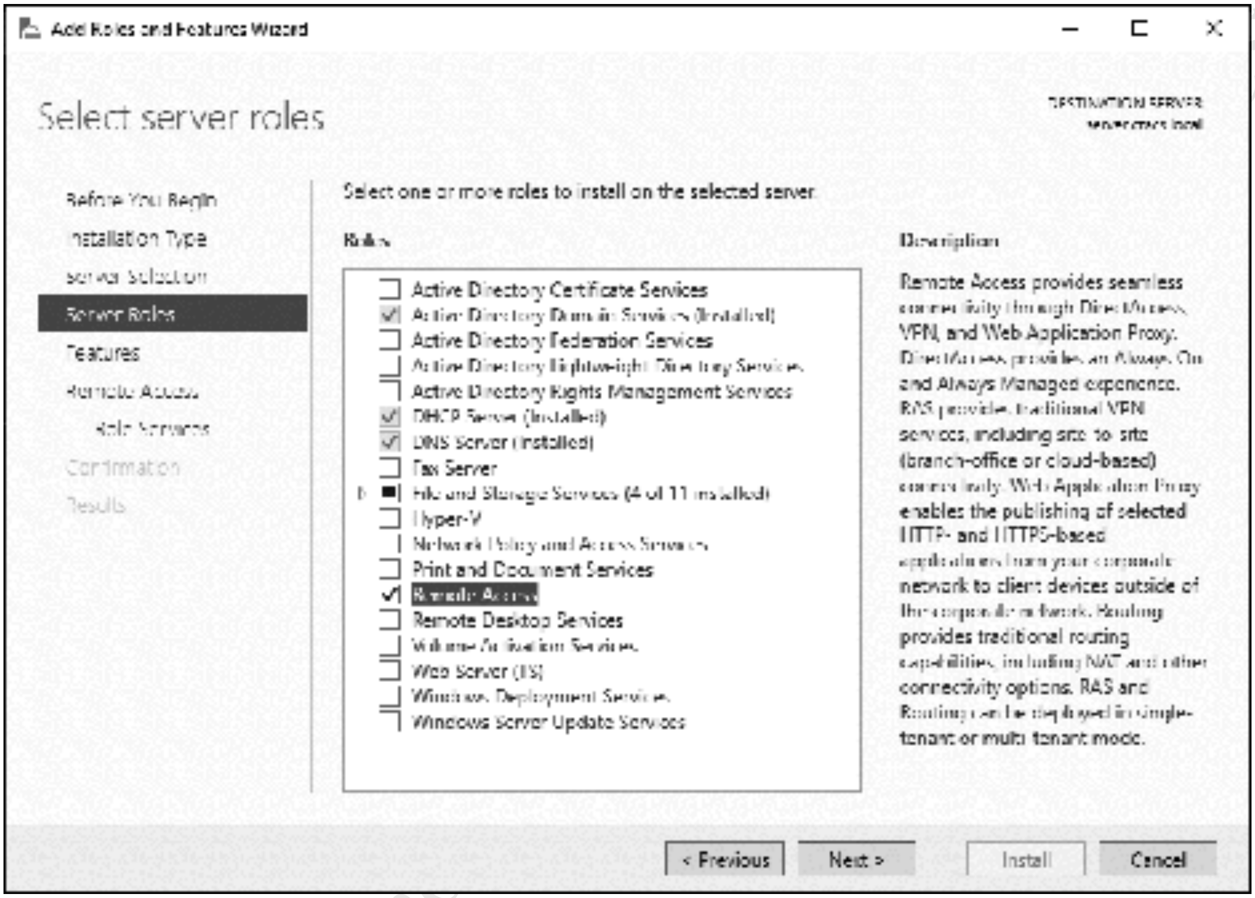
An alternative is to use a *Dynamic Domain Naming Service* or *DDNS*. Rather than registering your own domain name, you use an off-the-shelf name from a DDNS provider, some of which operate on a commercial basis, whilst others are totally free. The name is programmed into your router; if the IP address provided by your ISP changes (as it usually does when the router is restarted for instance), then the router advises the DDNS provider and their records are instantly updated. Do not be discouraged by the use of the term ‘programmed’ – this feature is supported in most routers and it is just a matter of typing in the name of the domain, although not all DDNS providers are supported by all routers. Free DDNS providers include *No-IP*, *DNSdynamic.org*, *zonedit* and others.

VPNs come in a variety of ‘flavors’, based around different protocols. The most popular one is called *L2TP/IPSec*; it has good security and is supported natively by modern versions of Windows and other platforms. In this walkthrough we will concentrate on connecting Windows 10 and Windows 7 clients, as this is likely to be the most popular requirement for people reading this book.

There are four stages to setting up a VPN: first, install the appropriate role on the server; second, configure the router; thirdly, enable remote access for users; finally, configure the client computers.

9.2 Installing & Configuring Remote Access

Begin by installing the *Remote Access* role to the server. From Server Manager, click **Manage** > **Add Roles and Features**. Choose **Role-based or feature-based installation** > **Next**. Select the server on the following screen and click **Next**. Tick **Remote Access** and click **Next**:



Select one or more roles to install on the selected server.

Roles

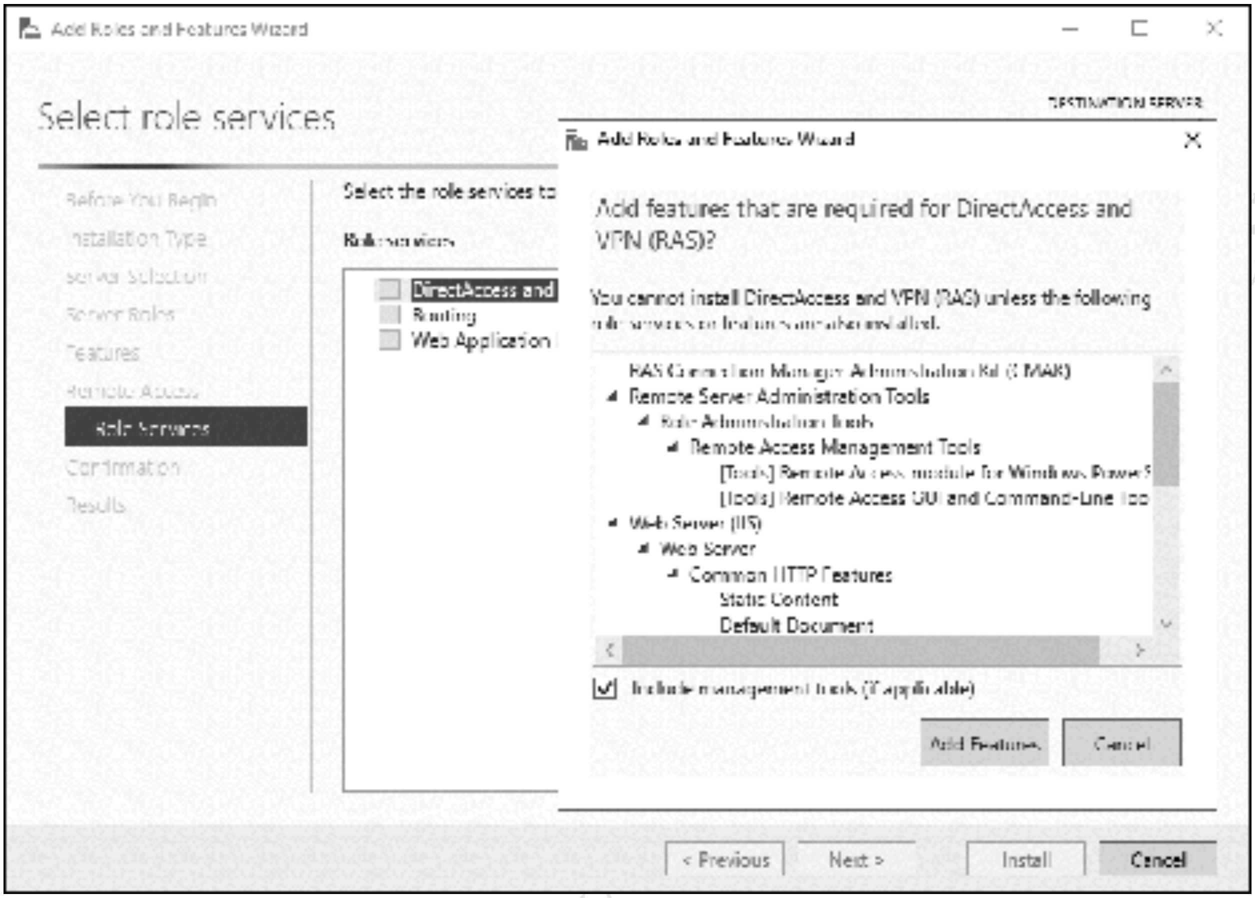
- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (4 of 11 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- ☑ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.

Figure 129: Select Remote Access role

Click **Next** on the following two screens then, on the *Role Services* screen, tick **Direct Access and VPN (RAS)**. Immediately, another panel will appear, about adding features that are required. Click **Add Features** and then **Next** when returned to the previous screen:



□ DirectAccess and
□ Routing
□ Web Application

Add Roles and Features Wizard

Add features that are required for DirectAccess and VPN (RAS)?

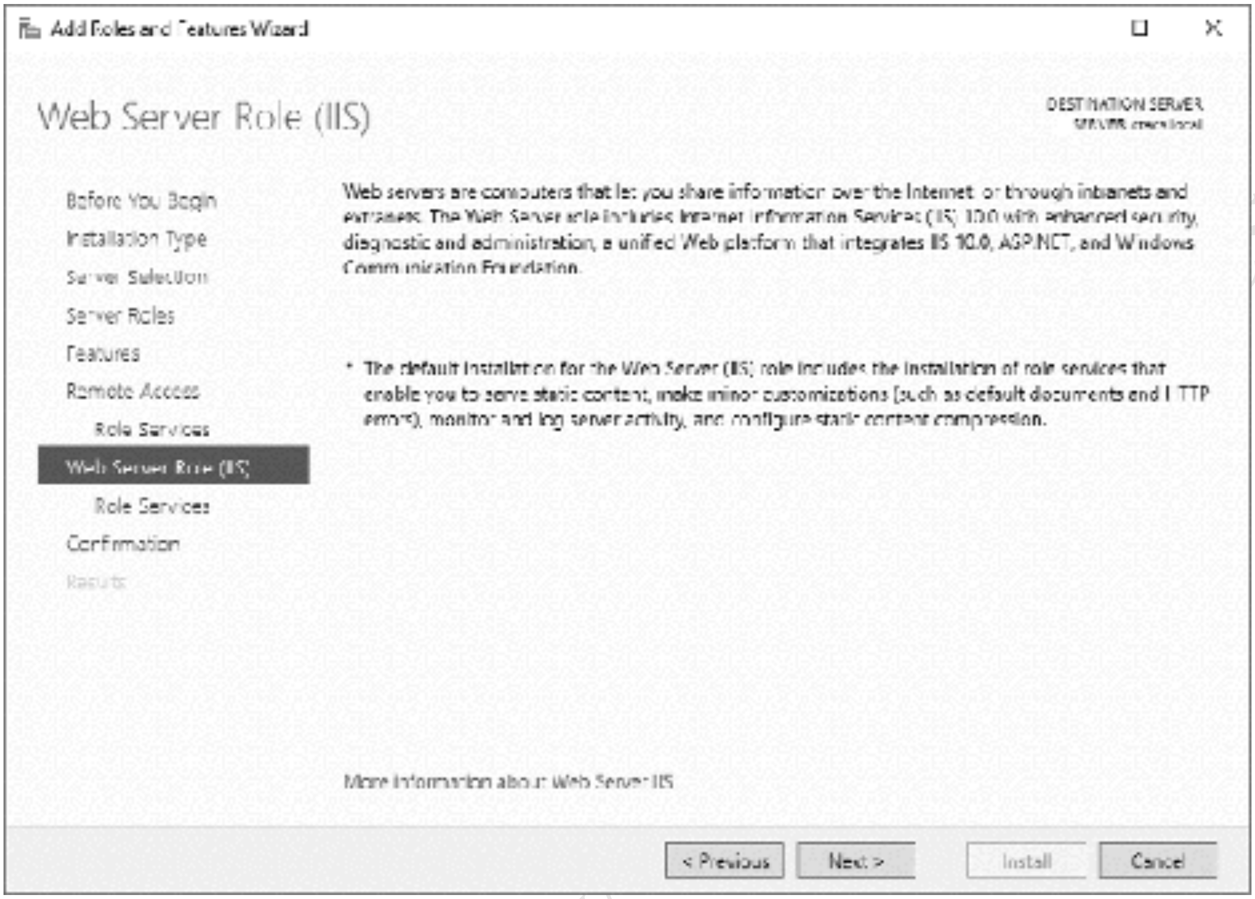
You cannot install DirectAccess and VPN (RAS) unless the following role services or features are also installed.

```
    RAS Connection Manager Administration Kit (CMAK)
◢ Remote Server Administration Tools
    ◢ Role Administration Tools
        ◢ Remote Access Management Tools
                [Tools] Remote Access module for Windows PowerS
                [Tools] Remote Access GUI and Command-Line Too
◢ Web Server (IIS)
    ◢ Web Server
        ◢ Common HTTP Features
                Static Content
                Default Document
```

☑ Include management tools (if applicable)

Figure 130: Add additional features

A screen about installing the *Web Server Role (IIS)* is displayed – click **Next** and then **Next** on the subsequent screen:

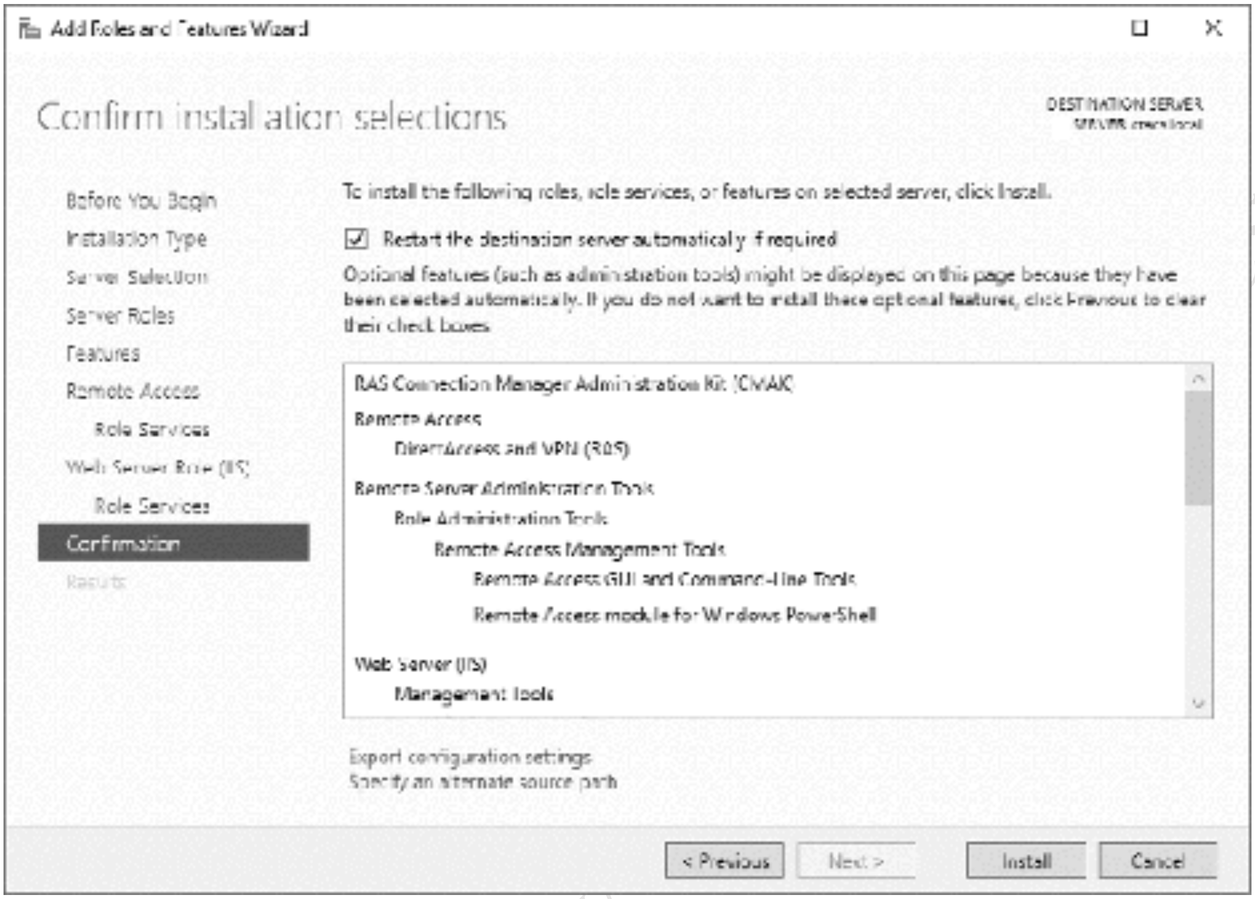


Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.

* The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

Figure 131: Web Server Role (IIS)

On the *Confirm installation selections* screen, tick the **Restart the destination server automatically if required box**, followed by **Install**:



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
SERVER.[illegible].local

To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

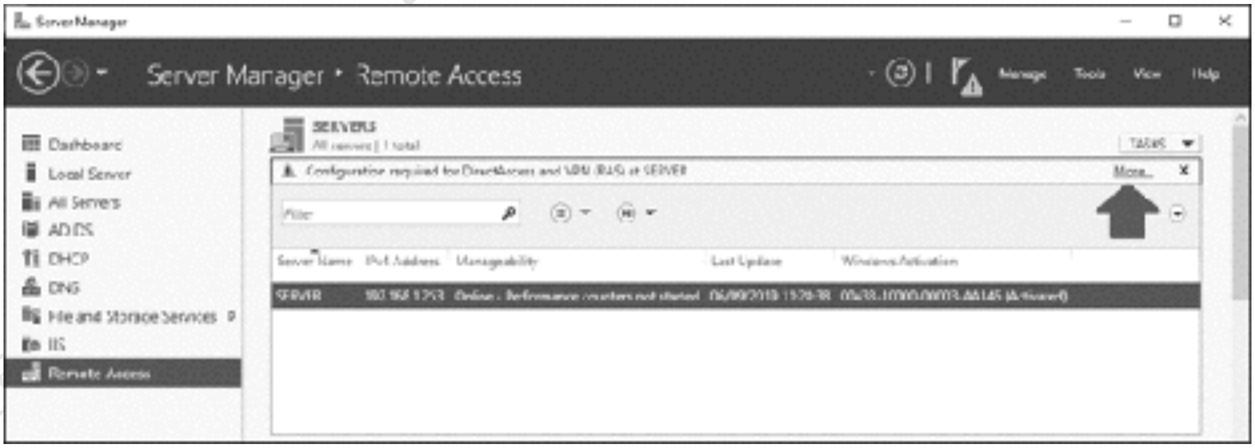
RAS Connection Manager Administration Kit (CMAK)
Remote Access
    DirectAccess and VPN (RAS)
Remote Server Administration Tools
    Role Administration Tools
        Remote Access Management Tools
            Remote Access GUI and Command-Line Tools
            Remote Access module for Windows PowerShell
Web Server (IIS)
    Management Tools

Export configuration settings
Specify an alternate source path

Figure 132: Confirm installation selections

When the installation has completed, which will take a couple of minutes, click **Close**.

Within the main Server Manager screen, click the newly added *Remote Access* option on the left-hand side. There is a message towards the top of the screen, advising *'Configuration required for DirectAccess and VPN(RAS)…'*; click where it reads **More:**



Server Manager

Server Manager • Remote Access

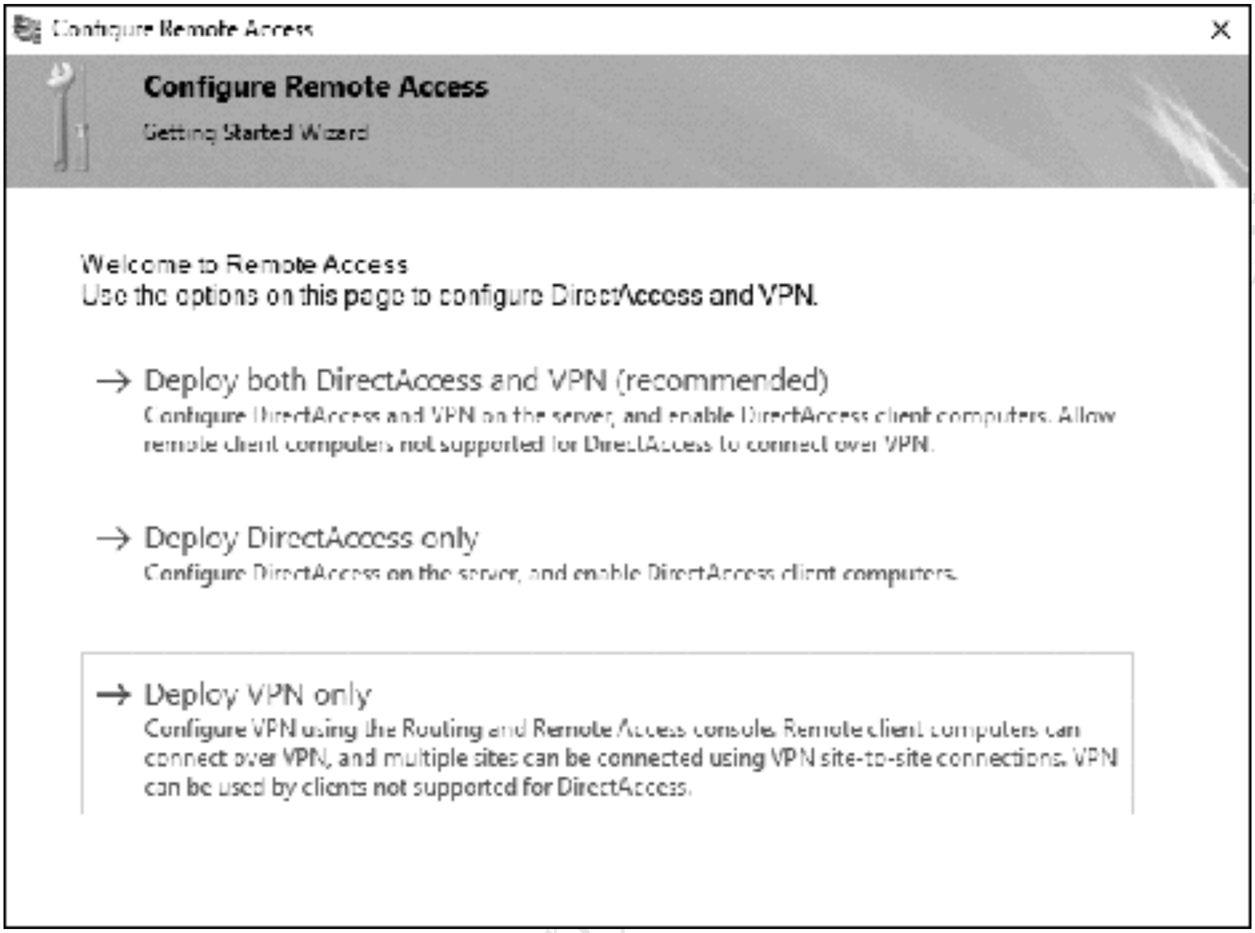
SERVERS
All servers | 1 total

Configuration required for DirectAccess and VPN (RAS) at SERVER More... ✕

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
SERVER	192.168.1.253	Online - Performance counters not started	06/09/2019 15:29:38	00438-10000-00013-AA145 (Activated)

Figure 133: Configuration required message

On the resultant panel, click **Open the Getting Started Wizard** to display the following. Click **Deploy VPN only**:



Configure Remote Access

Configure Remote Access

Getting Started Wizard

Welcome to Remote Access

Use the options on this page to configure DirectAccess and VPN.

→ Deploy both DirectAccess and VPN (recommended)

Configure DirectAccess and VPN on the server, and enable DirectAccess client computers. Allow remote client computers not supported for DirectAccess to connect over VPN.

→ Deploy DirectAccess only

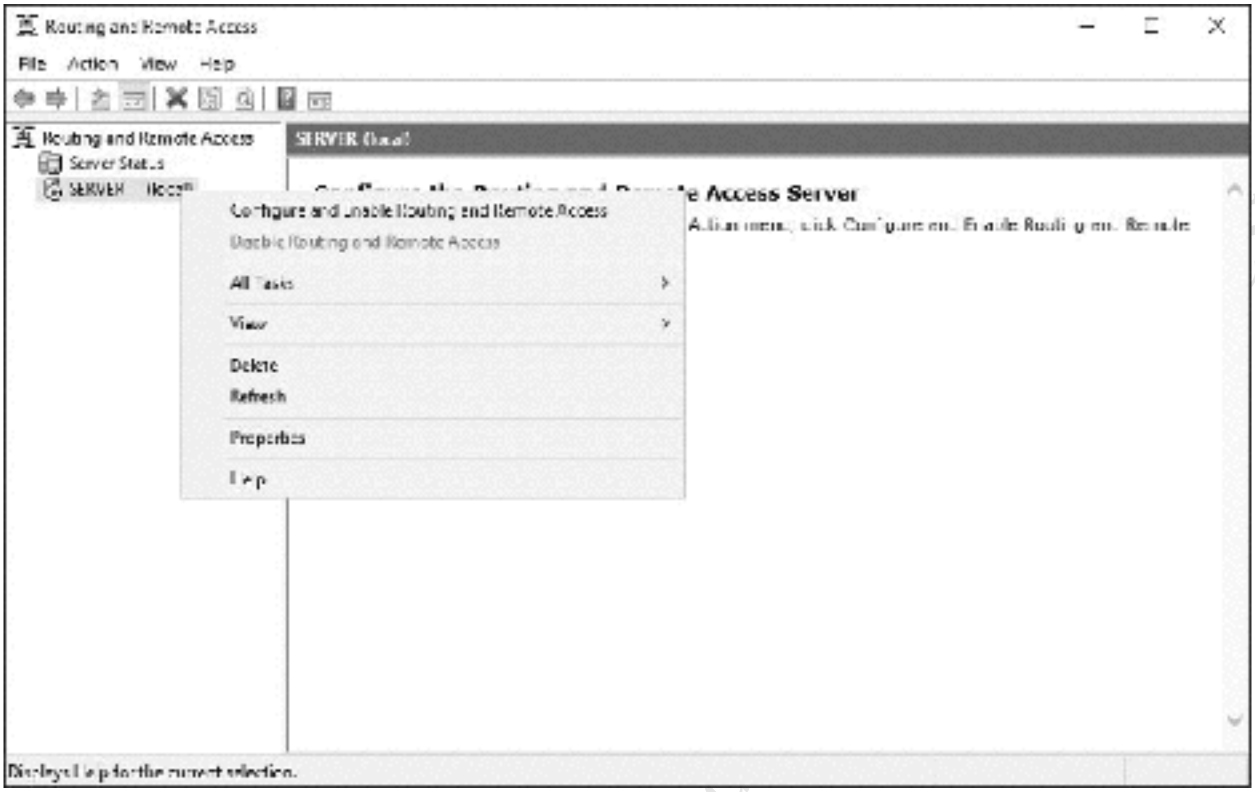
Configure DirectAccess on the server, and enable DirectAccess client computers.

→ Deploy VPN only

Configure VPN using the Routing and Remote Access console. Remote client computers can connect over VPN, and multiple sites can be connected using VPN site-to-site connections. VPN can be used by clients not supported for DirectAccess.

Figure 134: Configure Remote Access Wizard

The *Routing and Remote Access Management Console* is displayed; right-click the server and choose **Configure and Enable Routing and Remote Access** from the pop-up menu:


Routing and Remote Access
File
Action
View
Help
Routing and Remote Access
Server Status
SERVER (local)
SERVER (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help

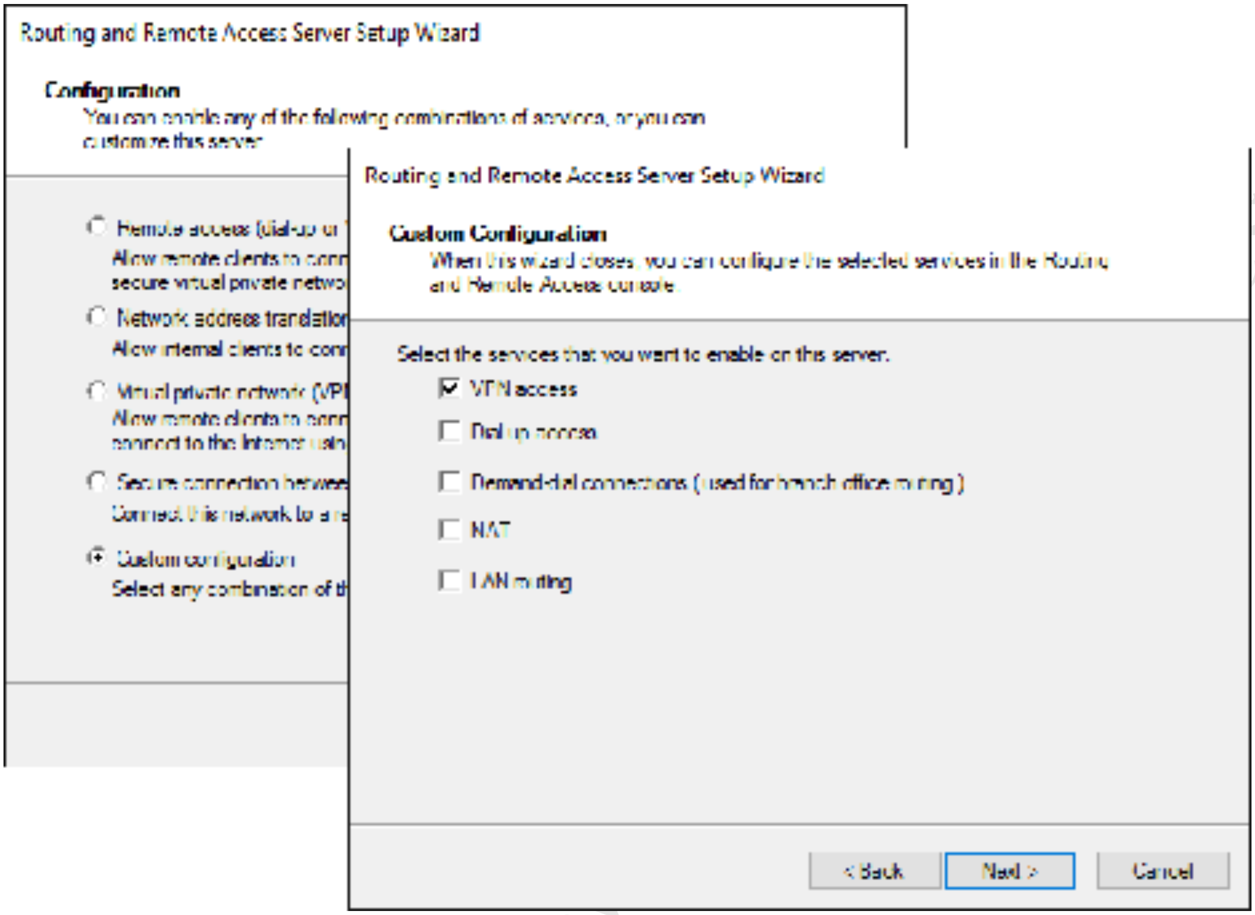
...e Access Server

...Action menu, click Configure and Enable Routing and Remote

Displays Help for the current selection.

Figure 135: Routing and Remote Access Management Console

The *Routing and Remote Access Server Setup Wizard* will run. Click **Next** on the first panel. On the second one, choose **Custom configuration**, click **Next**, followed by **VPN access** and **Next** on the subsequent one:



Routing and Remote Access Server Setup Wizard

Configuration

You can enable any of the following combinations of services, or you can customize this server.

○ Remote access (dial-up or

Allow remote clients to conn
secure virtual private netwo

○ Network address translatio

Allow internal clients to conn

○ Virtual private network (VP

Allow remote clients to conn
connect to the Internet usin

○ Secure connection betwee

Connect this network to a re

● Custom configuration

Select any combination of th

Routing and Remote Access Server Setup Wizard

Custom Configuration

When this wizard closes, you can configure the selected services in the Routing and Remote Access console.

Select the services that you want to enable on this server.

☑ VPN access

☐ Dial-up access

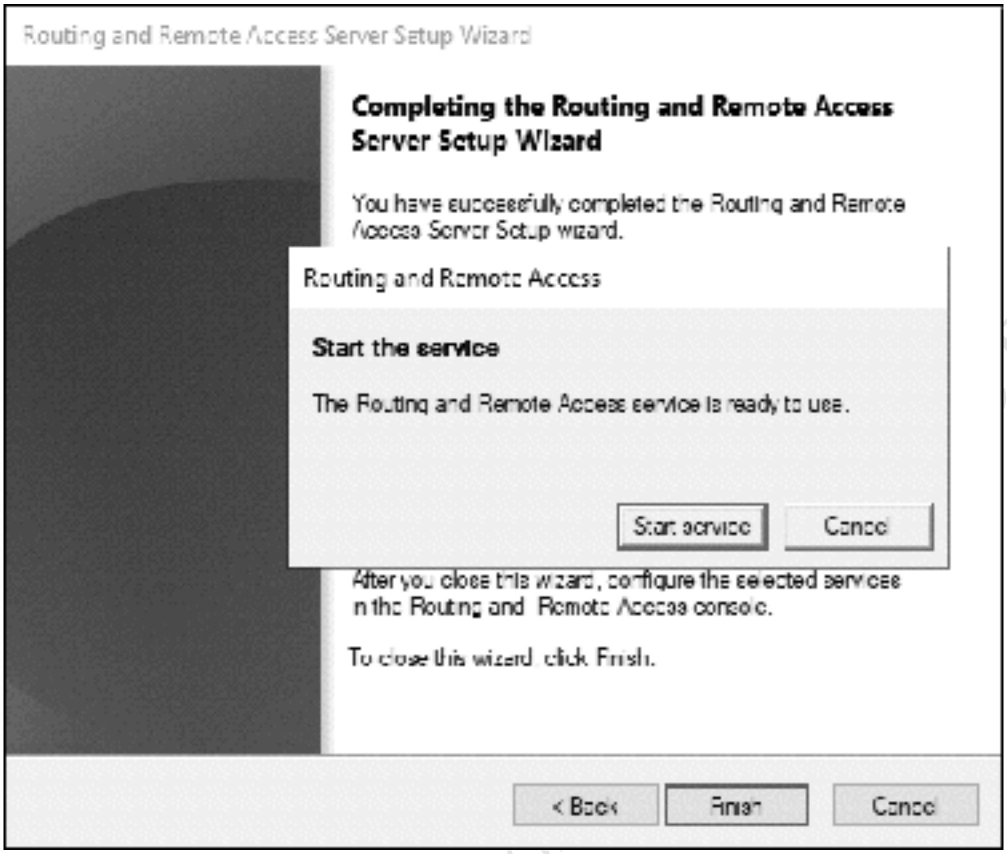
☐ Demand-dial connections (used for branch office routing)

☐ NAT

☐ LAN routing

Figure 136: Choose Custom Configuration

A confirmation message is then displayed; click **Finish**, followed by **Start Service**:



Routing and Remote Access Server Setup Wizard

Completing the Routing and Remote Access Server Setup Wizard

You have successfully completed the Routing and Remote Access Server Setup wizard.

Routing and Remote Access

Start the service

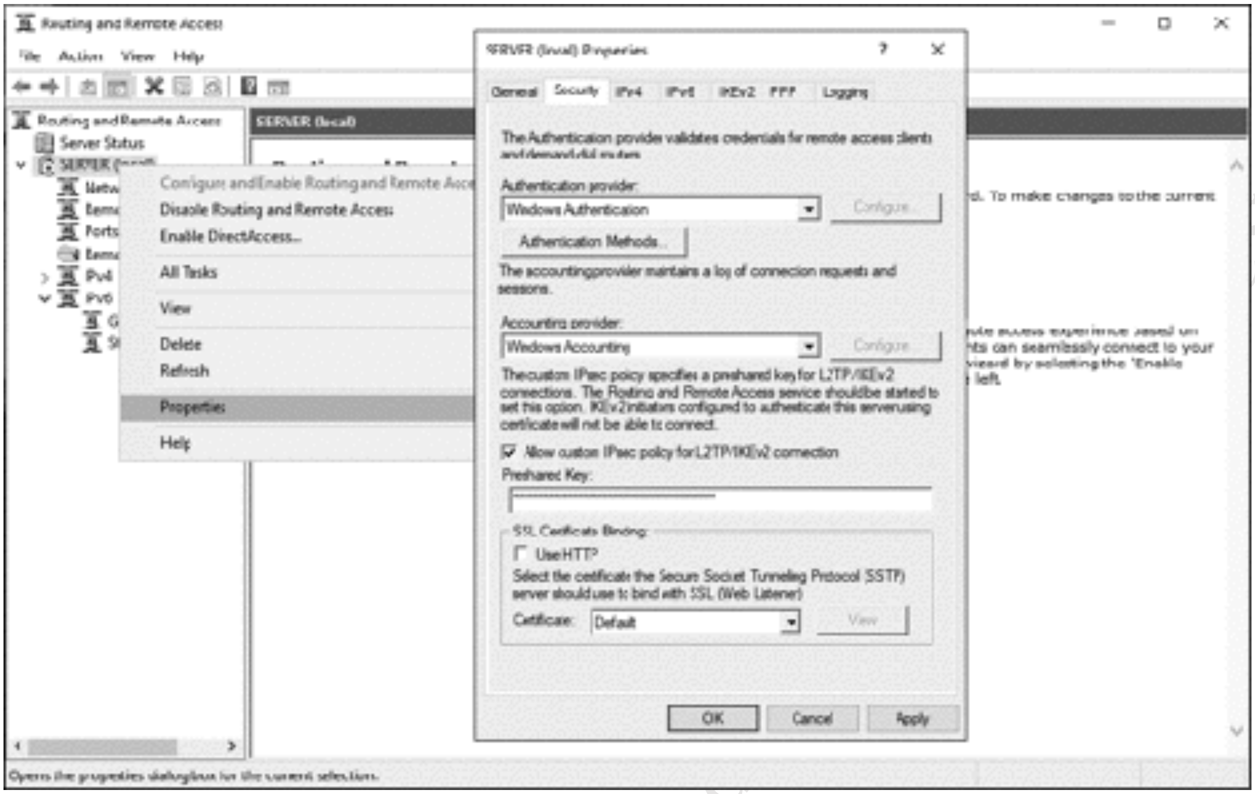
The Routing and Remote Access service is ready to use.

After you close this wizard, configure the selected services in the Routing and Remote Access console.

To close this wizard, click Finish.

Figure 137: Start the Routing and Remote Access service

It was mentioned previously that VPNs are available in several varieties and we will be using L2TP/IPSec flavor. Within the Routing and Remote Access console, right-click the server, click **Properties** on the pop-up menu, then click the **Security** tab on the resultant panel. Tick the **Allow custom Ipsec policy for L2TP/IKEv2 connection** box and specify a **Preshared Key**, which can be considered as a type of system-wide password. It is best to choose something non-obvious, such as a random mix of upper- and lower-case letters, numbers and symbols:



The Authentication provider validates credentials for remote access clients and demand-dial routers.

The accounting provider maintains a log of connection requests and sessions.

The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.

☑ Allow custom IPsec policy for L2TP/IKEv2 connection

Preshared Key:

□ Use HTTP

Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)

Figure 138: Specify the Preshared Key

Click **OK**. A message is displayed, advising that Routing and Remote Access needs to be restarted. Click **OK** to return to the main screen and on it right-click the server and choose **All Tasks** > **Restart**.

9.3 Configure the Router

For remote access to work, the appropriate ports on the router need to be forwarded to the internal IP address of the server. Specifically:

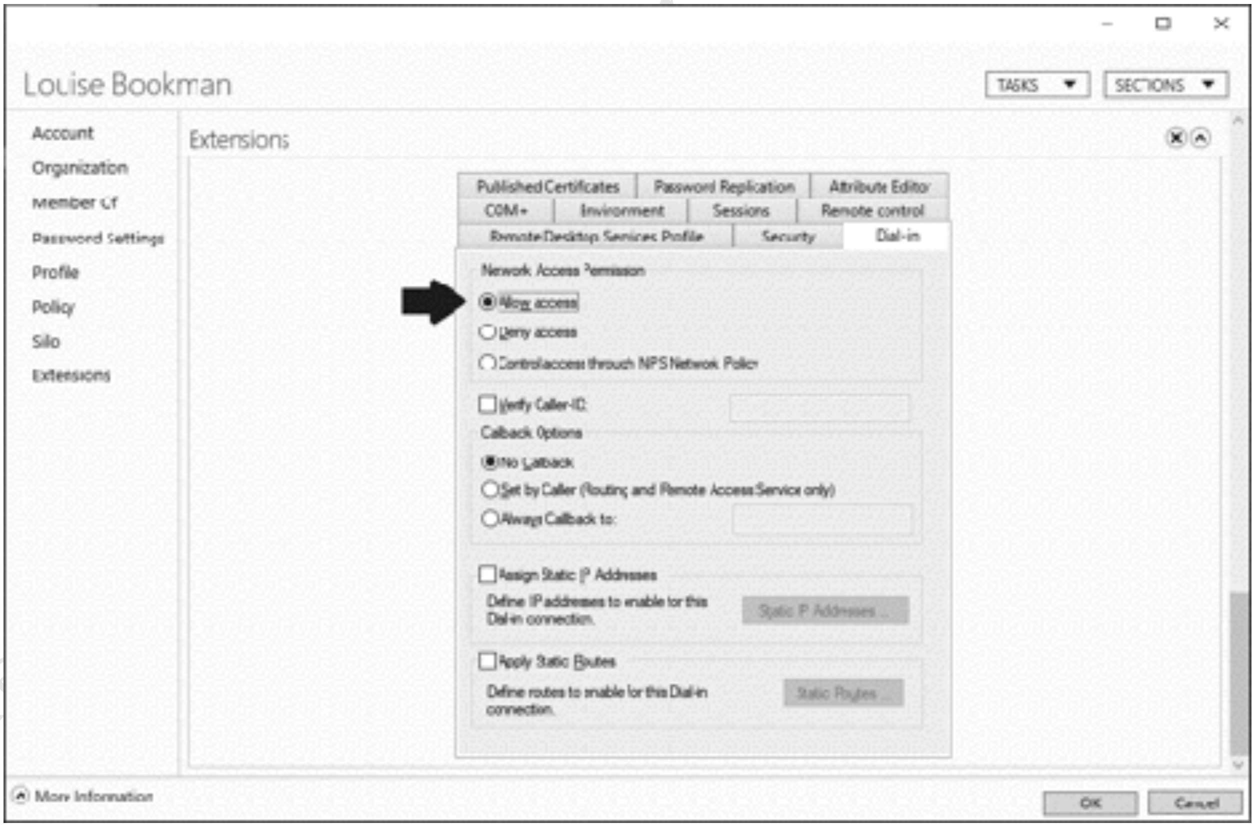
- For PPTP, port 1723 TCP should be forwarded
- For L2TP/IPSEC, ports 1701 TCP and 500 UDP need to be forwarded
- For SSTP, port 443 TCP needs to be forwarded

Windows Server cannot setup the port forwarding by itself; rather, it is necessary to login to the router and configure it. As there are thousands of different routers available, it is not appropriate to give a worked example here. However, instructions for doing so for most popular routers can be found at the *www.portforward.com* website.

If you are working in an environment with a separate firewall appliance, this should also be configured to allow network traffic through the appropriate ports reference above.

9.4 Enabling Remote Access for Users

Users do not receive remote access capabilities by default and have to be specifically enabled. From the Server Manager Dashboard, choose **Tools** > **Active Directory Administrative Centre**. Locate the user and double-click their name, else right-click the name and choose **Properties**. Scroll down to the *Extensions* section and click the embedded **Dial-in** tab. In the *Network Access Permission section*, click **Allow access**, followed by **OK**:



Network Access Permission
● Allow access
○ Deny access
○ Control access through NPS Network Policy

□ Verify Caller-ID:

Callback Options
● No Callback
○ Set by Caller (Routing and Remote Access Service only)
○ Always Callback to:

□ Assign Static IP Addresses
Define IP addresses to enable for this Dial-in connection.

□ Apply Static Routes
Define routes to enable for this Dial-in connection.

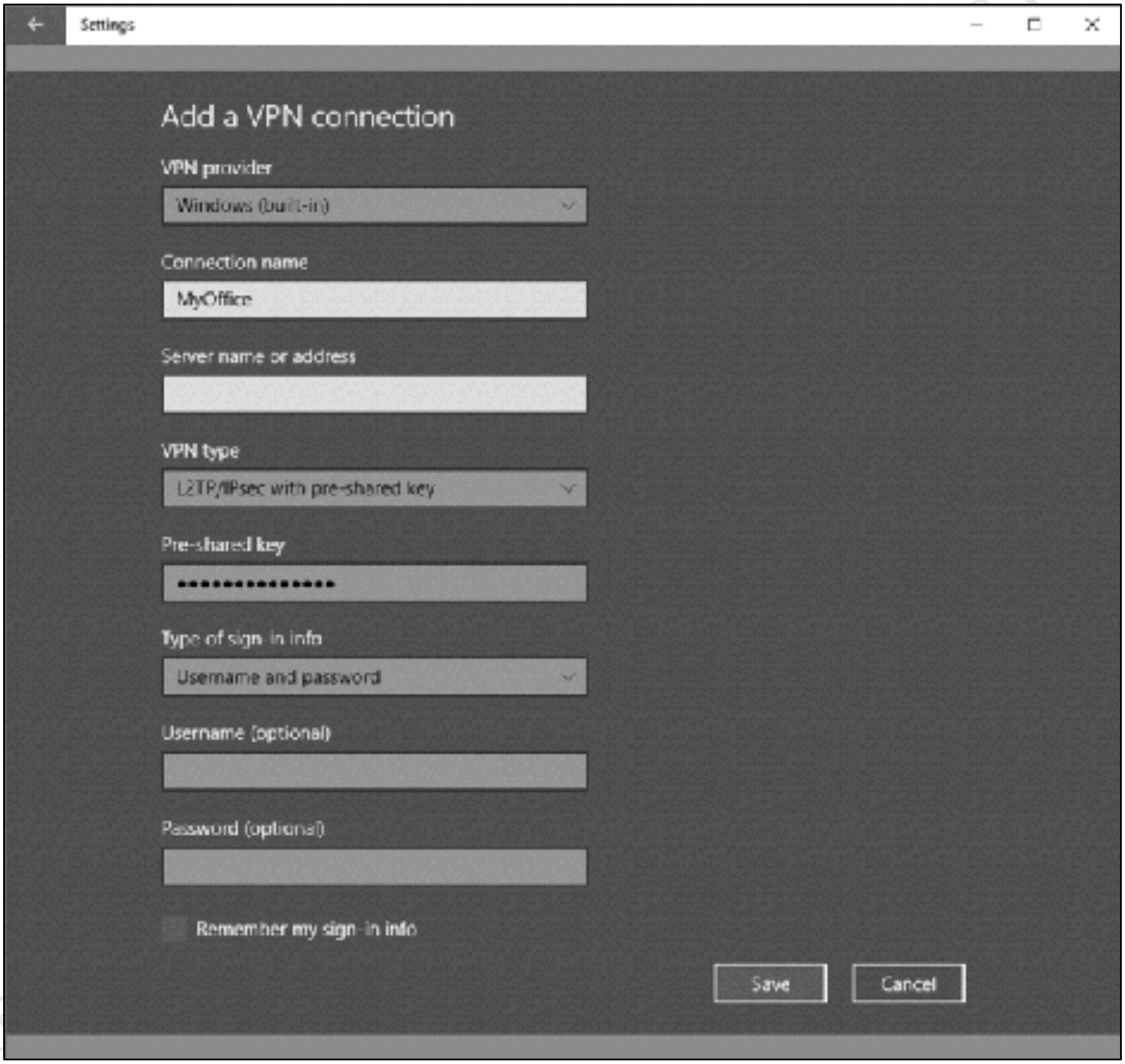
Figure 139: Enable remote access for a user

9.5 Connecting Client Computers

VPN support is built-in on most versions of Windows and client software is readily available for other platforms. This section covers installation on two popular platforms: Windows 10 and Windows 7. There may be some minor variations depending on what type of VPN you are using plus any security options you may have chosen (here we are using L2TP/IPSec).

Windows 10 Clients

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



Settings

Add a VPN connection

VPN provider

Windows (built-in)

Connection name

MyOffice

Server name or address

VPN type

L2TP/IPsec with pre-shared key

Pre-shared key

•••••••••••••••

Type of sign-in info

Username and password

Username (optional)

Password (optional)

□ Remember my sign-in info

Figure 140: 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 name or IP address of the server. Set the **VPN type** to **L2TP/Ipsec with pre-shared key** and enter the pre-shared key you specified when configuring Routing and Remote Access on the server. 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**.

The newly defined connection will now be listed on the VPN section within *Settings*. Click it and then click the **Connect** button. You will be prompted to Sign in – enter your **Username** and **Password** as defined on the server and click **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\shared* to display and access the shared folder.

When you have finished using the VPN, click the **Disconnect** button.

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)**:

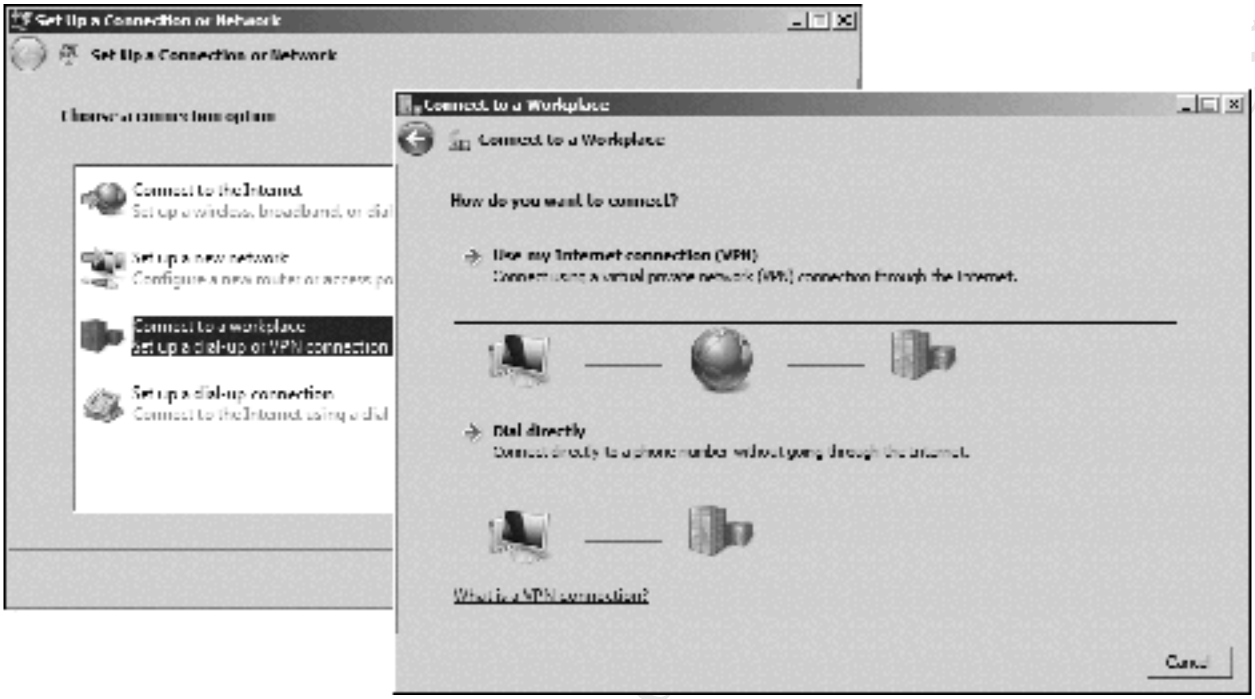
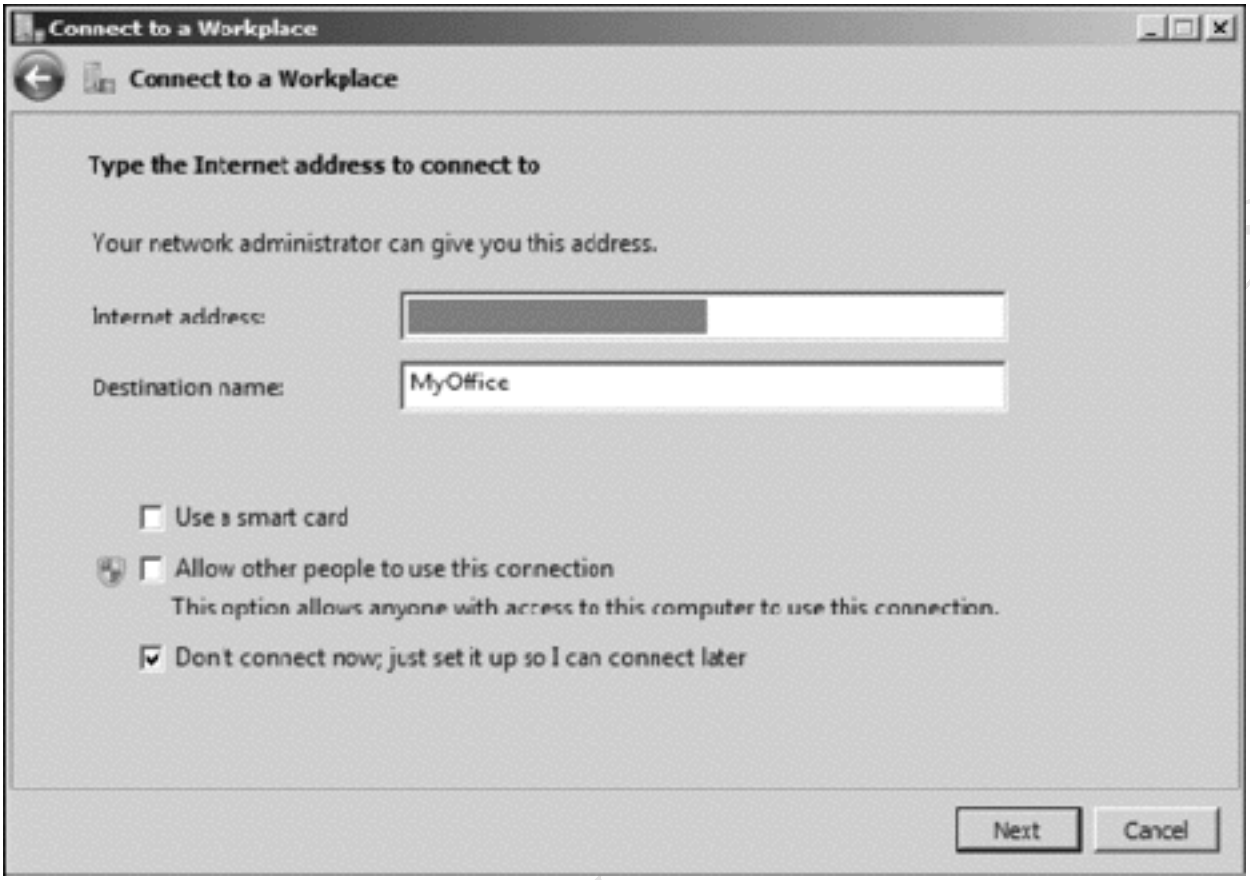

Set Up a Connection or Network
Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial
Set up a new network
Configure a new router or access po
Connect to a workplace
Set up a dial-up or VPN connection
Set up a dial-up connection
Connect to the Internet using a dial
Connect to a Workplace
Connect to a Workplace
How do you want to connect?
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.
Dial directly
Connect directly to a phone number without going through the Internet.
What is a VPN connection?
Cancel

Figure 141: Setup a new connection in Windows 7

On the next panel, specify the external domain name or IP address of the server. Specify a **Destination name**, such as *MyOffice*. Tick the **Don't connect now** box and click **Next**:



Connect to a Workplace

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: [redacted]

Destination name: MyOffice

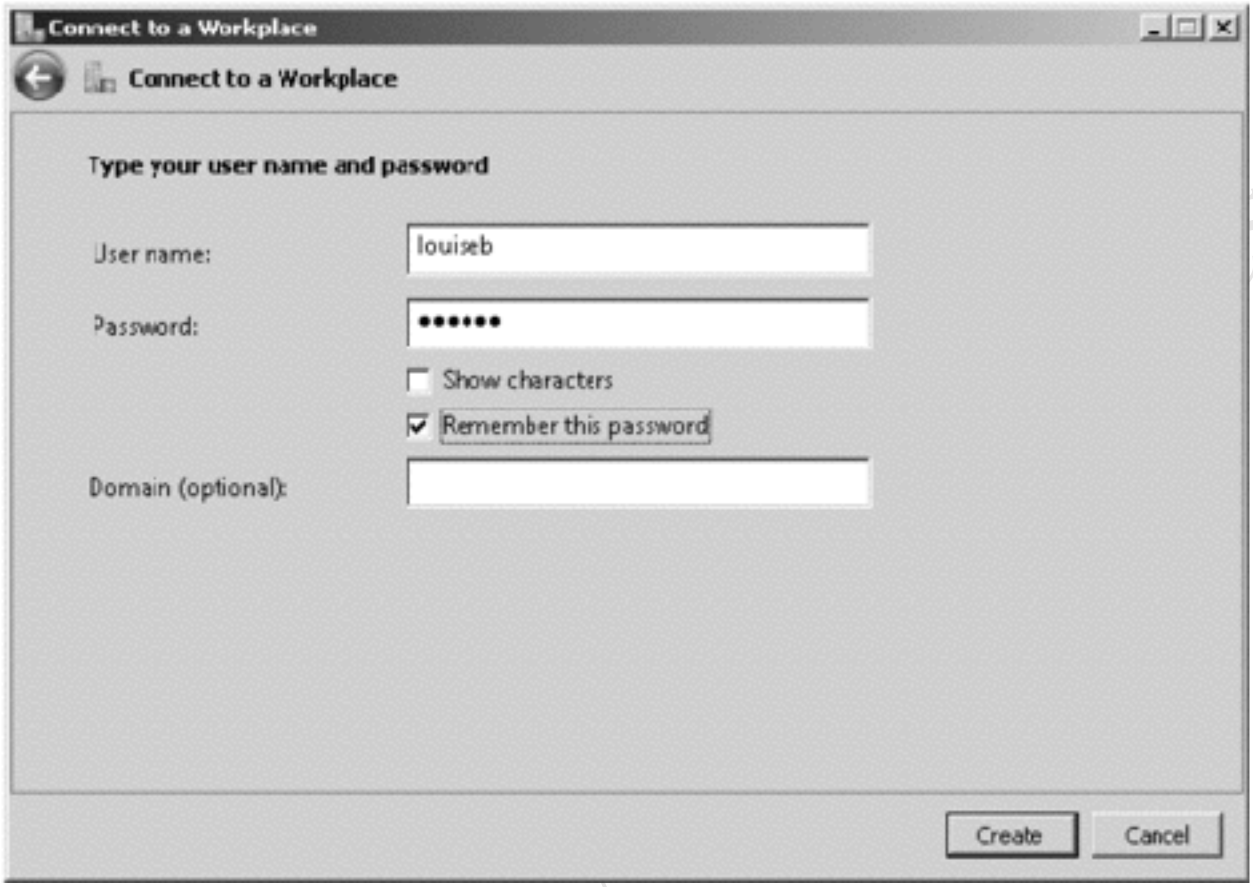
□ Use a smart card

□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

Figure 142: 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):



Type your user name and password

User name: louiseb

Password: ••••••

□ Show characters

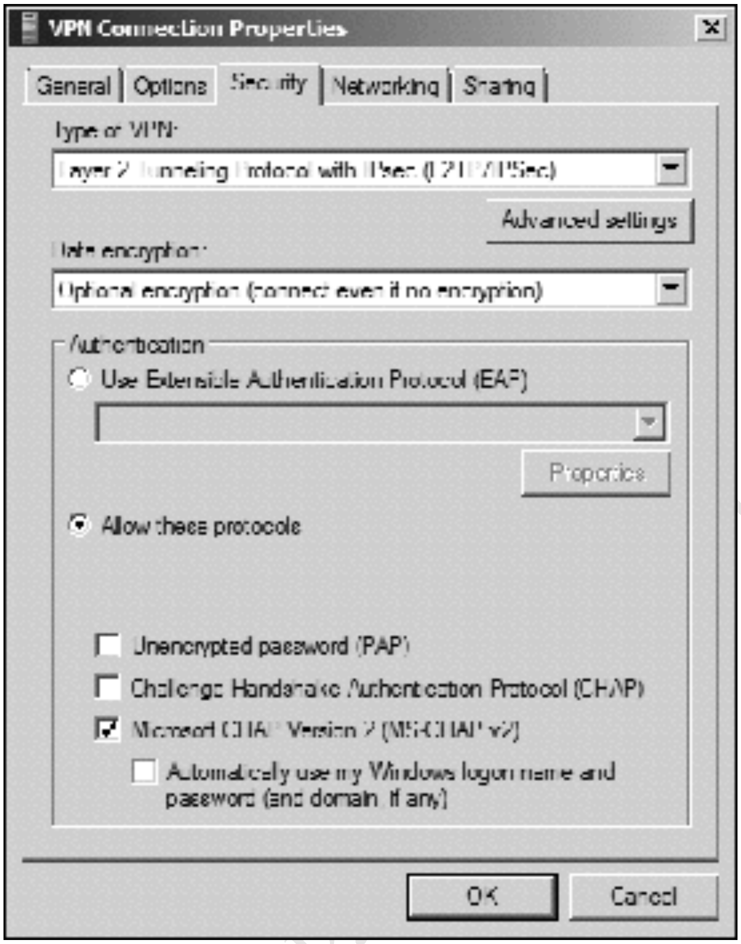
☑ Remember this password

Domain (optional):

Figure 143: Enter user name and password

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

Return to the **Control Panel** and choose **Network and Sharing Center**. Click **Change adapter settings**; the newly created VPN connection will be listed alongside the computer's normal network connection(s). Right-click it and choose **Properties**. Click the **Security** tab. Change the *Type of VPN* to **Layer 2 Tunneling Protocol with IPSec (L2TP/IPSec)** and change *Data Encryption* to read **Optional encryption (connect even if no encryption).** Click the **Allow these protocols** option. Click the **Advanced settings** button and enter the *Pre-shared key for authentication* which you specified when configuring Routing and Remote Access on the server. Click **OK**. The panel should now appear as follows; click **OK**:



VPN Connection Properties

Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)

Data encryption:

Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

□ Unencrypted password (PAP)

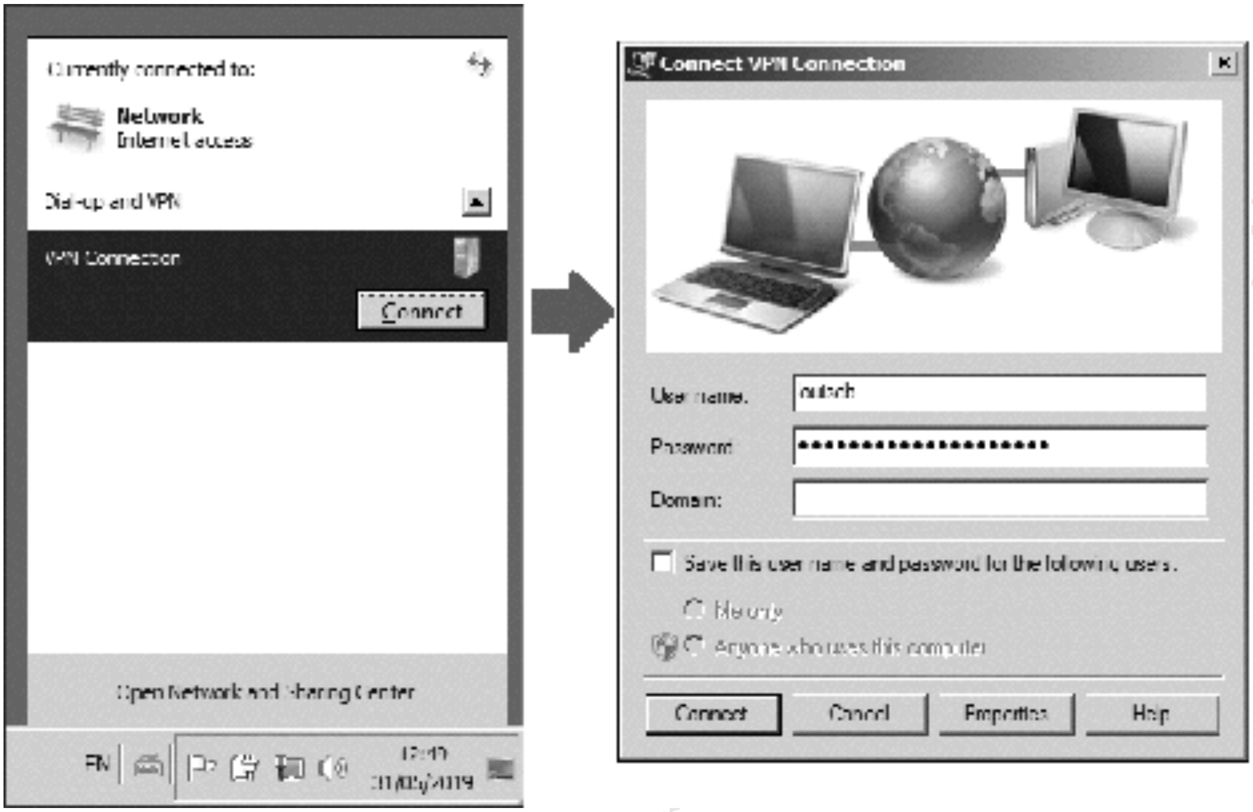
□ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain if any)

Figure 144: 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**:



Connect VPN Connection

User name: outsch

Password: ••••••••••••••••••••

Domain:

☐ Save this user name and password for the following users:

○ Me only

○ Anyone who uses this computer

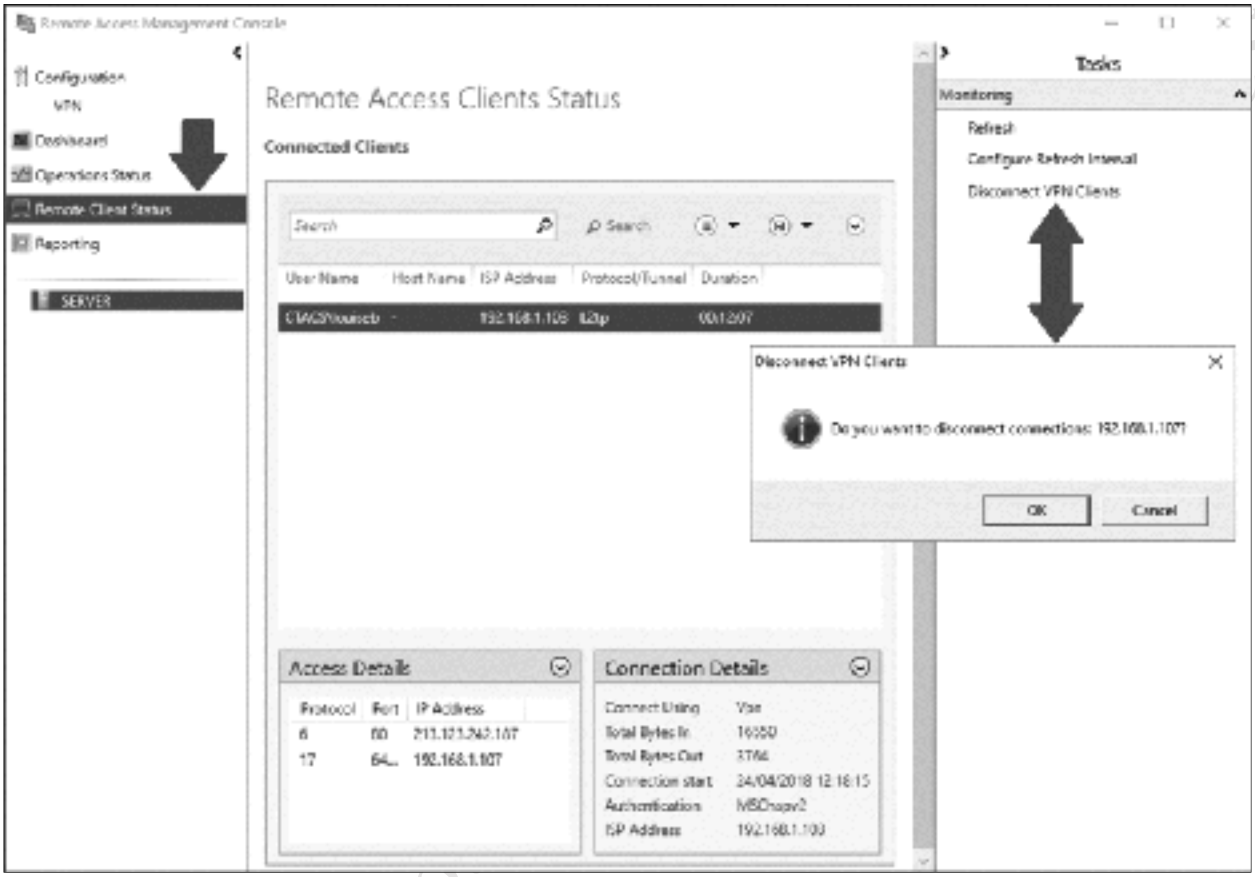
Figure 145: Connecting to the VPN

A few seconds later you should be connected. The first time you connect you may receive a prompt asking you to choose the network location; a choice of *Home*, *Work* and *Public* is given, if so choose **Home** or **Work** (they are effectively the same thing). You can now access resources on the server as though you were in the office. For instance, press the **Windows key** and the **R key** simultaneously and in the run box type *\\server\shared* to display and access the shared folder.

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.

9.6 Checking and Monitoring Remote Users

To manage remote users, go into Server Manager and choose **Tools** > **Remote Access Management**. On the resultant screen that appears – the *Remote Access Dashboard* – click **Remote Client Status** on the left-hand side and the list of connected users will be displayed.



Remote Access Clients Status

Connected Clients

User Name	Host Name	ISP Address	Protocol/Tunnel	Duration
CTAG2\ouiseb	-	192.168.1.108	l2tp	00:12:07

Disconnect VPN Clients

Do you want to disconnect connections: 192.168.1.107?

OK Cancel

Access Details

Protocol	Port	IP Address
6	80	211.121.242.107
17	64...	192.168.1.107

Connection Details

Connect Using	Vpn
Total Bytes In	16350
Total Bytes Out	3766
Connection start	24/04/2018 12:18:15
Authentication	MSChapv2
ISP Address	192.168.1.100

Figure 146: Remote Access Clients Status

To disconnect clients, click **Disconnect VPN Clients** from the right-hand side of the screen. A confirmation message is displayed, which has to be acknowledged.

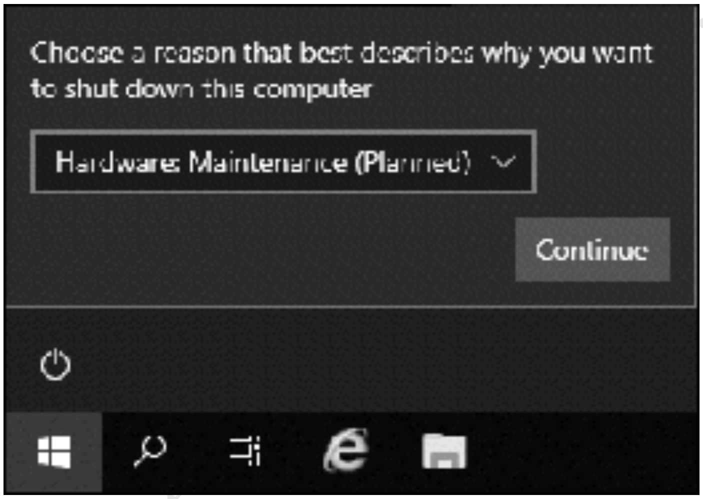
10. HOUSEKEEPING

10.1 Overview

Servers need to be checked on a regular basis to ensure that there are no problems and that they are in good health. Clearly some type of problems 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? Additionally, there are some housekeeping tasks that need to be carried out on an occasional basis. This section also includes some ideas for making the server more convenient to work with for the administrator.

10.2 Shutting Down & 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. To do so click **Start** followed by **Power**; you will be given a choice of **Shut down** or **Restart**. You will then be prompted to enter a reason for shutting down the server – choose one from the drop-down menu and click **Continue**.



Choose a reason that best describes why you want to shut down this computer

Hardware: Maintenance (Planned)

Figure 147: Shutting down

You can also shut down the server from Server Manager. Make sure you are on the Local Server *Properties* page, click **Tasks** and choose **Shut Down Local Server**. You will be prompted to provide a reason for doing so.

10.3 Setup Alternative Administrator Account(s)

For a variety of reasons, it is not good practice to use the main Administrator account any more than is strictly necessary. Firstly, in case the account accidentally gets locked or disabled. Secondly, it can be confusing when using Windows 7 clients, which have a built-in local account of the same name. Instead, an alternative administrative account should be setup and, once the server has gone live, this is the one that should be normally used. This could be called *systemadmin*, for instance. To create it:

- Go into **Administrative Tools** and choose **Active Directory Users and Computers**.
- Find *Administrator* in the *Users* section.
- Right-click on *Administrator* and choose **Copy**.
- Complete the dialogue box and create a new user called *systemadmin*. You could set the password to the same as that of the *Administrator.*

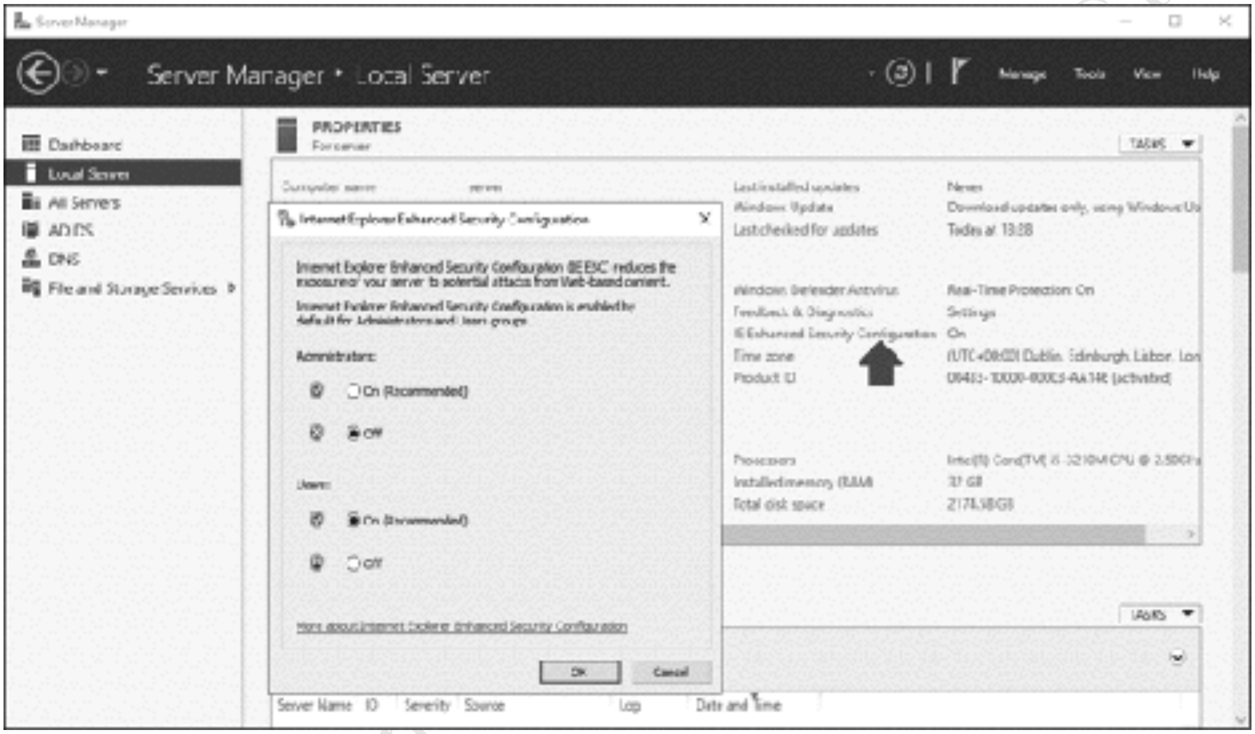
- Having created the user, go into **Properties** and specify any drives, scripts, settings as used by the regular Administrator account.

Suggestion: in order to install some software and printers on client's PCs, administrative rights may be required. If you wish users to be able to do these things themselves, setup another administrative account, perhaps called *userinstaller*. Do not use the same password as the main Administrator/Systemadmin accounts and do not bother with any profile information. The details of this account can then be passed to selected users.

10.4 Disabling Internet Explorer Enhanced Security

By default, Windows Server has limited internet connectivity due to a feature called *Internet Explorer Enhanced Security* being enabled. There are good reasons why general internet browsing is not a good idea on a server - such as the risk of picking up malware from an infected website - but not being able to access the internet freely makes things difficult, particularly in a small network. It is therefore useful to disable Enhanced Security.

Go into **Server Manager** and click **Local Server** to display the Properties for the server. On the right-hand side of the first panel is an entry for *IE Enhanced Security Configuration*; click where it reads **On** and the following dialog box will be displayed:



Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:

○ On (Recommended)

● Off

Users:

● On (Recommended)

○ Off

More about Internet Explorer Enhanced Security Configuration

Last installed updates	Never
Windows Update	Download updates only, using Windows Update
Last checked for updates	Today at 13:38
Windows Defender Antivirus	Real-Time Protection: On
Feedback & Diagnostics	Settings
IE Enhanced Security Configuration	On
Time zone	(UTC+00:00) Dublin, Edinburgh, Lisbon, London
Product ID	00431-10000-00000-AA148 (activated)
Processors	Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz
Installed memory (RAM)	32 GB
Total disk space	2174.58 GB

Figure 148: Internet Explorer Enhanced Security Configuration

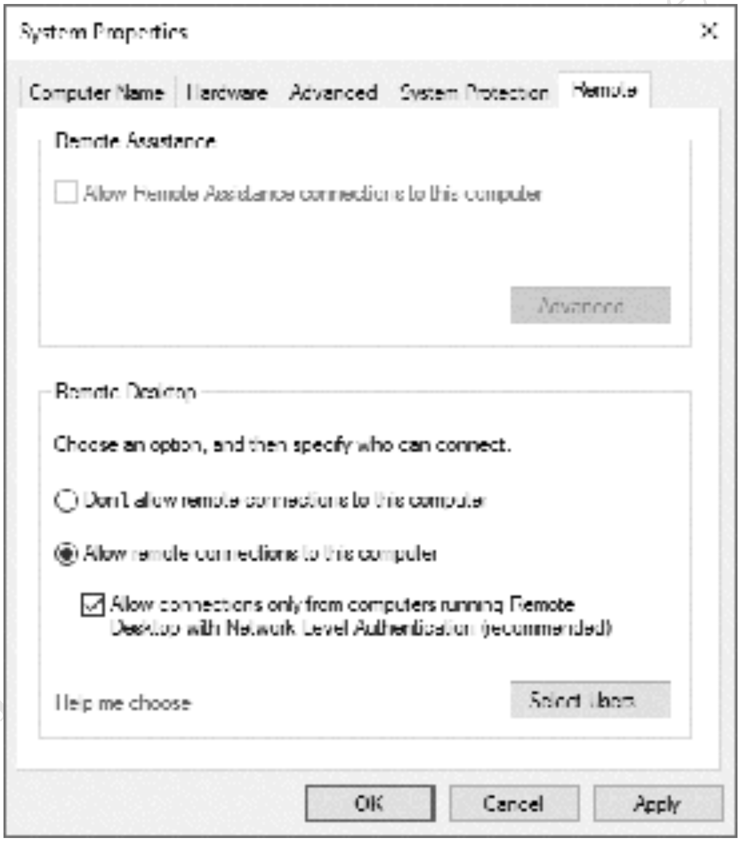
Change the entry for Administrators to **Off** and click **OK**. It is not necessary to change the entry for Users as nobody other than an Administrator should ever have direct access to the server. You may receive a message that *'Protected mode is turned off for the Local intranet zone'*, in which case click **Don't show this message again**.

If Internet Explorer is not to your liking, it is possible to install and run other browsers such as Mozilla Firefox and Google Chrome.

10.5 Headless Operation/Remote Desktop

When installing Windows Server, it is necessary to use a standard monitor, keyboard and mouse (usually - some manufacturers have workarounds). However, once the server is up and running these can be dispensed with and it can be run in so-called *headless* mode. To access it for support purposes, the *Remote Desktop* capability is used. This has several advantages: firstly, the server can be accessed using any computer on the network and it is not necessary to have physical access to the server, which may be a consideration if it is situated in a secure, locked or otherwise inaccessible location. Secondly, dispensing with a physical screen, keyboard and mouse saves space and possibly a small amount of electrical power. Thirdly, in some small organizations the server may have to be physically located in a general-purpose office; not having a keyboard and screen will reduce the temptation for staff to treat it as just another computer.

Go into the **Control Panel** and clicking the **System** icon. Click **Remote Settings** and the Remote tab of System Properties will be displayed. Make sure that the **Allow remote connections to this computer** option is selected and that the box underneath is ticked All members of the Administrators group have access to the Remote Desktop by default, so it is not necessary to use the **Select Users** button. Click **OK**.



System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Remote Assistance

□ Allow Remote Assistance connections to this computer

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

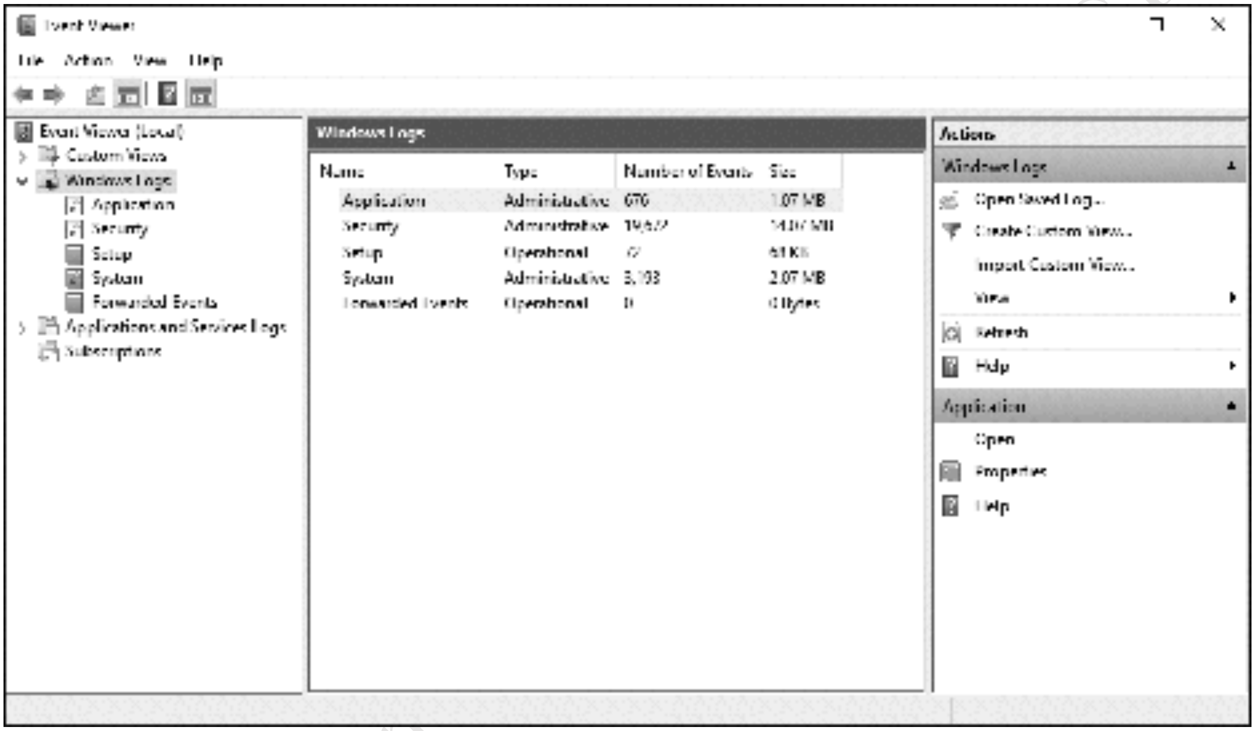
Figure 149: Enabling remote connections on the server

Test the facility by going to a computer on the network and launching the *Remote Desktop Connection* program. This program is a standard part of Windows and can be located at **Start** > **All Programs** > **Accessories** in Windows 7, from the Start Screen in Windows 8/8.1 and at **Start** > **All Apps** > **Windows Accessories in Windows 10**. Remote Desktop programs are also available for the Mac and iPad. Enter the name of the server or its IP address. Provide logon credentials i.e. the name of an Administrative account and its password. Note that when the remote session is established, the current user on the physical server, if there is one, will be logged out. Once everything has been tested, the physical screen, keyboard and mouse of the server can be dispensed with.

10.6 Checking the Event Logs

Windows Server maintains comprehensive records of the myriad events that take place during the operation of the server. Some of these are simply records of normal usage (user logs on, user logs off and so on), whereas others are generated in response to error conditions and can be used to help diagnose problems. The events are categorized into several main types and recorded in log files, which should be specifically checked in the event of problems and otherwise on an occasional basis.

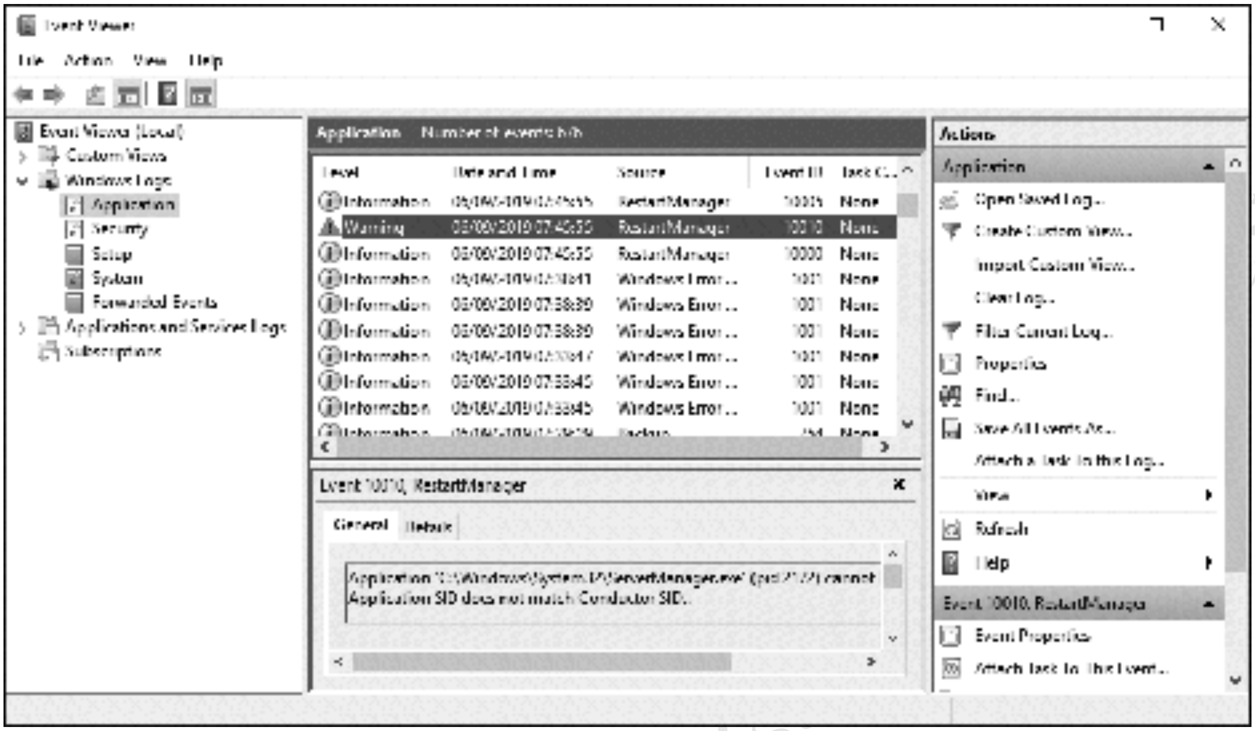
To access the Event Logs, right-click the **Start** button and choose **Event Viewer**. Click **Windows Logs** in the left-hand panel and a screen along the following lines is displayed (it may take some seconds to fully populate):



Name	Type	Number of Events	Size
Application	Administrative	670	1.07 MB
Security	Administrative	[illegible]	[illegible]
Setup	Operational	[illegible]	68 KB
System	Administrative	5,193	2.07 MB
Forwarded Events	Operational	0	0 Bytes

Figure 150: The Event Viewer

Some of the event logs are more useful than others. In the left-hand panel, expand the tree to display the **Windows Logs** section. There are five main logs: *Application*, *Security*, *Setup*, *System* and *Forwarded Events*. To view a particular log, click on it. Each event is categorized as Error, Warning or Information, along with a timestamp plus a short description. The listing can be sorted by clicking on the heading for a column:



Level	Date and Time	Source	Event ID	Task C...
Information	06/06/2019 07:45:55	RestartManager	10005	None
Warning	06/06/2019 07:45:55	RestartManager	10010	None
Information	06/06/2019 07:45:55	RestartManager	10000	None
Information	06/06/2019 07:38:41	Windows Error ...	1001	None
Information	06/06/2019 07:38:39	Windows Error ...	1001	None
Information	06/06/2019 07:38:39	Windows Error ...	1001	None
Information	06/06/2019 07:38:47	Windows Error ...	1001	None
Information	06/06/2019 07:38:45	Windows Error ...	1001	None
Information	06/06/2019 07:38:45	Windows Error ...	1001	None

Event 10010, RestartManager

```
Application 'C:\Windows\System32\ServerManager.exe' (pid 2172) cannot
Application SID does not match Conductor SID..
```

Figure 151: Example of an Event log

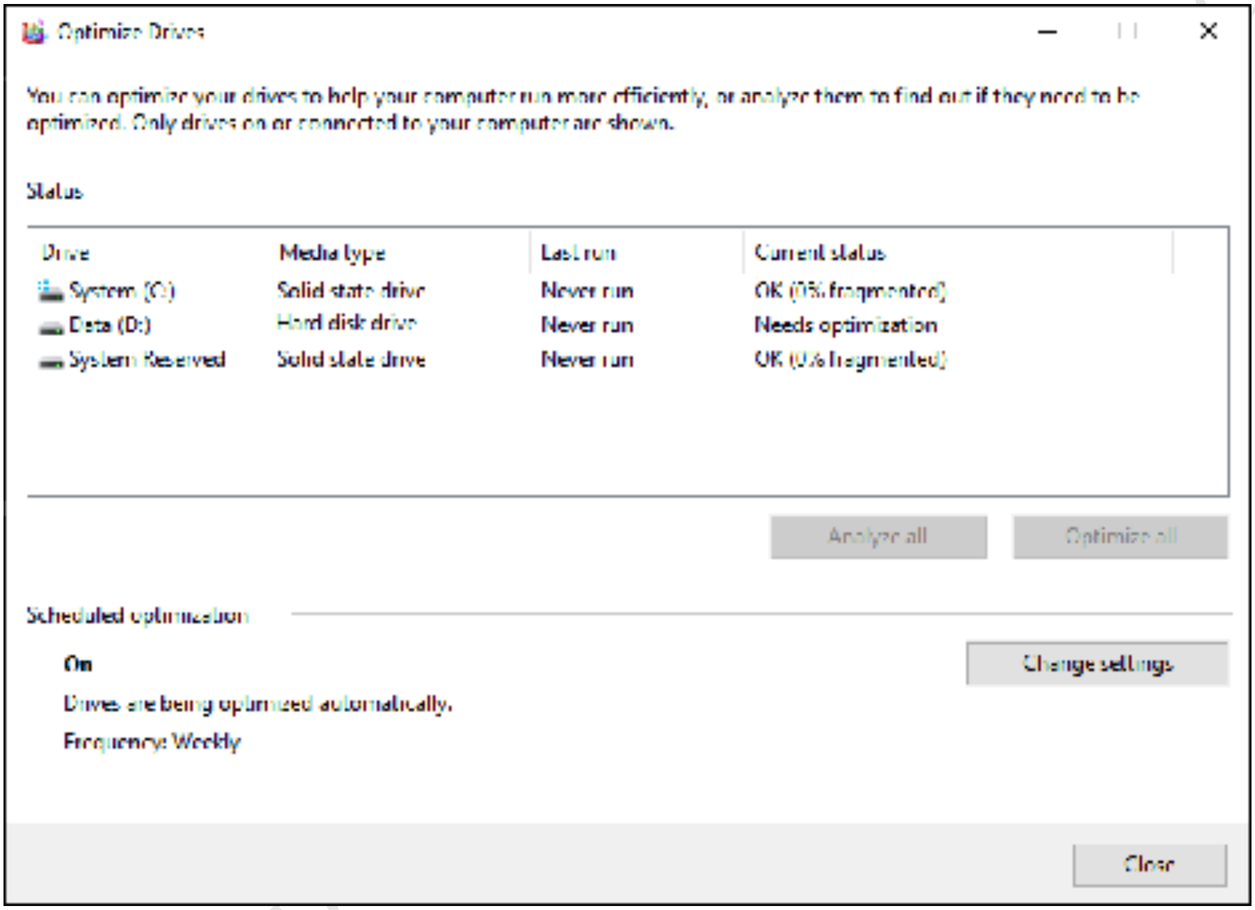
For most purposes the System and Application logs contain the most relevant information. If a server crashes or freezes – which is a very rare occurrence – there may well be clues in the System log. If there are suspected security violations, then the Security log may contain details. However, note that the Security log is very “noisy” and may generate thousands of events every hour.

The Event logs will eventually start to overwrite when they are full. If required, they can be archived as permanent records or to preserve evidence. To do so, right-click on an Event Log and from the pop-up menu choose **Clear Log**. A message is displayed offering three choices – click the **Save and Clear** button. In the resultant dialog box specify a name for the file: a good choice is its name plus the date e.g. *setup-12092016*.

10.7 Optimizing the Hard Drives

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

Launch **Server Manager**, click **Tools** and choose **Defragment and Optimize Drives** to show the following panel:



You can optimize your drives to help your computer run more efficiently, or analyze them to find out if they need to be optimized. Only drives on or connected to your computer are shown.

Status

Drive	Media type	Last run	Current status
System (C:)	Solid state drive	Never run	OK (0% fragmented)
Data (D:)	Hard disk drive	Never run	Needs optimization
System Reserved	Solid state drive	Never run	OK (0% fragmented)

Scheduled optimization

On

Drives are being optimized automatically.

Frequency: Weekly

Figure 152: Optimize the hard drives

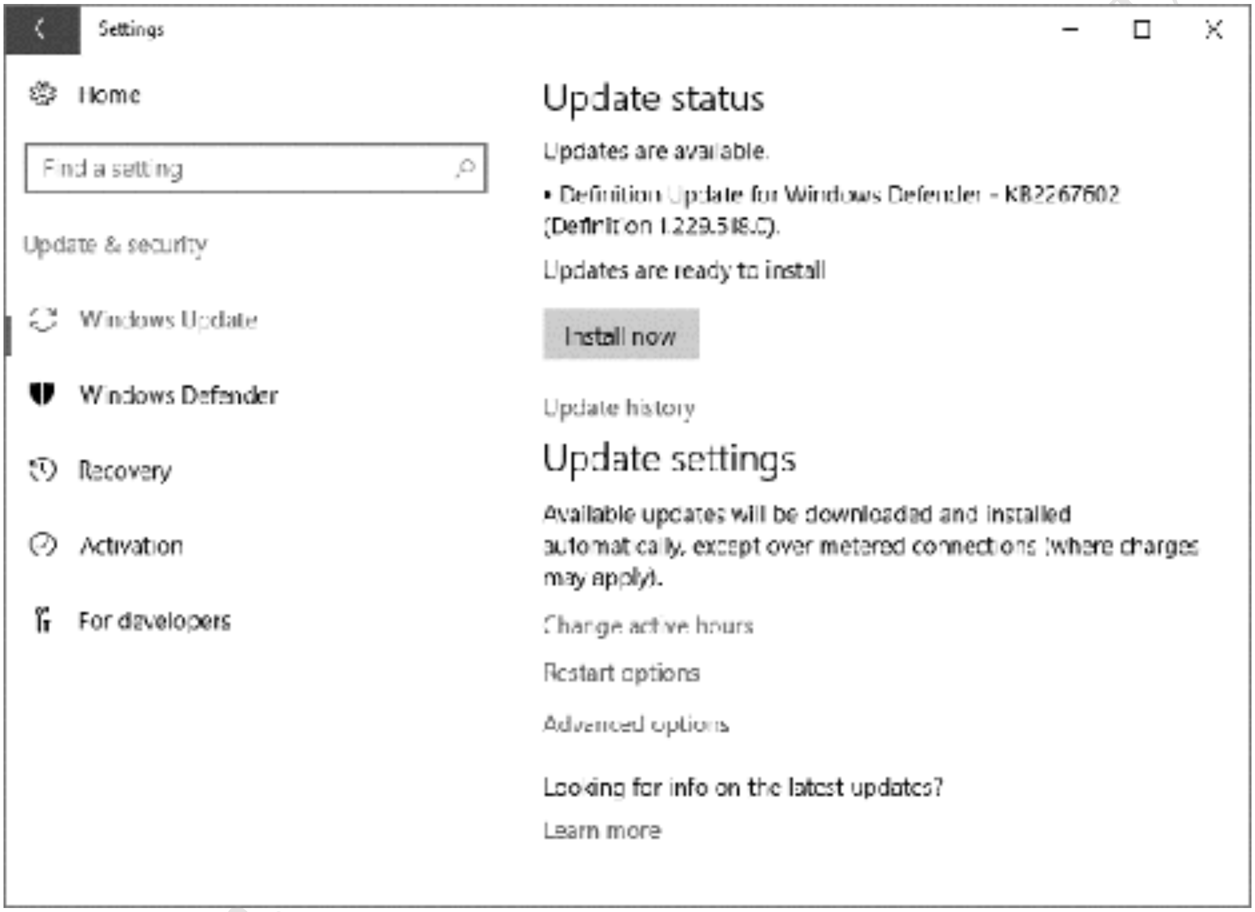
Towards the bottom left-hand corner, it should read that Scheduled optimization is ‘On’ and that the drives are being optimized automatically on a weekly frequency. If this is not the case, click the **Change settings** button and adjust the settings accordingly.

If you have used earlier versions of Windows, you may be aware that you are not supposed to defragment Solid State Drives (SSDs) as it is not necessary and will shorten their lifespan. However, in Windows Server 2016 you do not have to worry about this, as the Optimize process simply runs the TRIM command but does not attempt to defragment SSDs.

10.8 Applying Windows Updates to the Server

Microsoft provides updates to Windows Server on a regular basis. Such updates may provide improved or additional functionality, but more typically address security issues that could compromise the system. In previous versions of Windows Server, there was considerable latitude as to when updates were applied, such that it was even possible to switch them off altogether, thereby incurring security risks. In Windows Server 2016 things have been greatly tightened up and updates are largely applied automatically; however, there are some parameters that can usefully be adjusted.

Go into **Settings** and click **Update & security** and make sure you are in the *Windows Update* section:



Update status

Updates are available.

• Definition Update for Windows Defender - KB2267602 (Definition 1.229.518.0).

Updates are ready to install

Update settings

Available updates will be downloaded and installed automatically, except over metered connections (where charges may apply).

Looking for info on the latest updates?

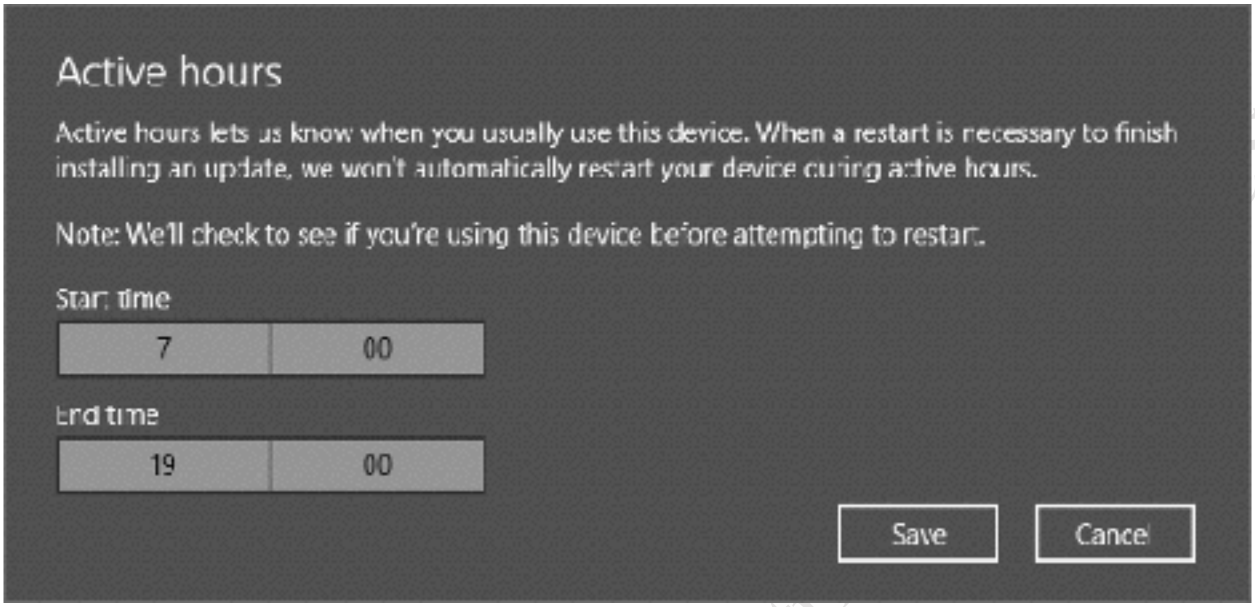
Figure 153: Windows Update settings

Any available updates will be listed, along with an option to **Install now**. Invariably, there will be a Definition Update for the Windows Defender security package, as it is updated every day or two. Underneath is an option to view the Update history, so you can see which updates have recently been applied. You can also Uninstall Updates from here, should that ever be necessary for some reason.

The next section controls the Update settings and there are three options: *Change active hours*; *Restart options*; *Advanced options*.

Change active hours – this controls when the server restarts after applying updates. Clearly the server should not suddenly restart during the working day, as this would be highly disruptive, so you can define the active hours when the server is normally in use (and hence, by implication, when it is not). Click **Change active hours** to display the following panel, change the Start and End times as required and click

Save. Somewhat bizarrely, Microsoft have decided that the server cannot be ‘active’ for more than 12 hours:



Active hours

Active hours lets us know when you usually use this device. When a restart is necessary to finish installing an update, we won't automatically restart your device during active hours.

Note: We'll check to see if you're using this device before attempting to restart.

Start time

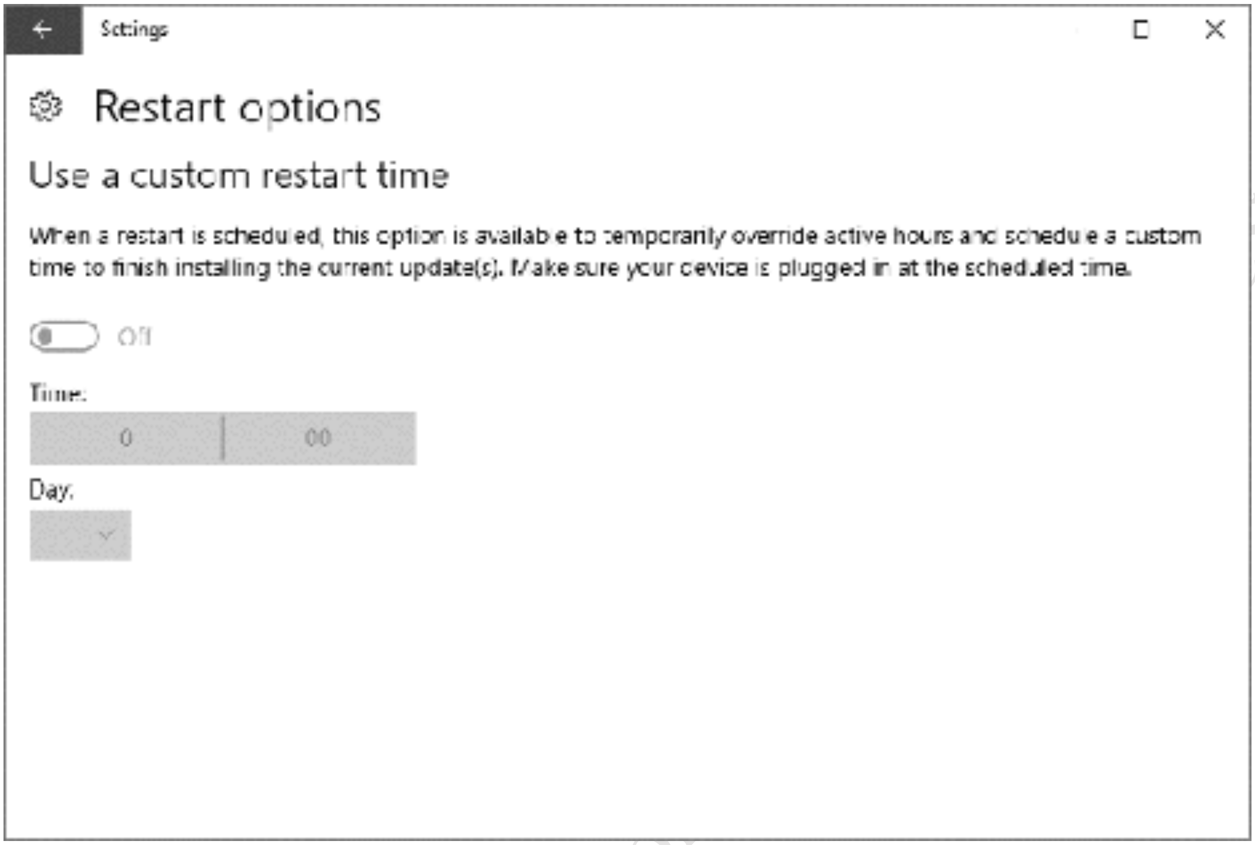
7 00

End time

19 00

Figure 154: Set the Active hours

Restart options – having Active hours restricted to a maximum of 12 may cause problems in some organizations. To get around, this you can temporarily disable them and use a custom restart time instead. Click **Restart options**; if a restart is currently scheduled you will be able to slide the switch to the On position and choose a specific time and date for the restart:



Settings

Restart options

Use a custom restart time

When a restart is scheduled, this option is available to temporarily override active hours and schedule a custom time to finish installing the current update(s). Make sure your device is plugged in at the scheduled time.

Off

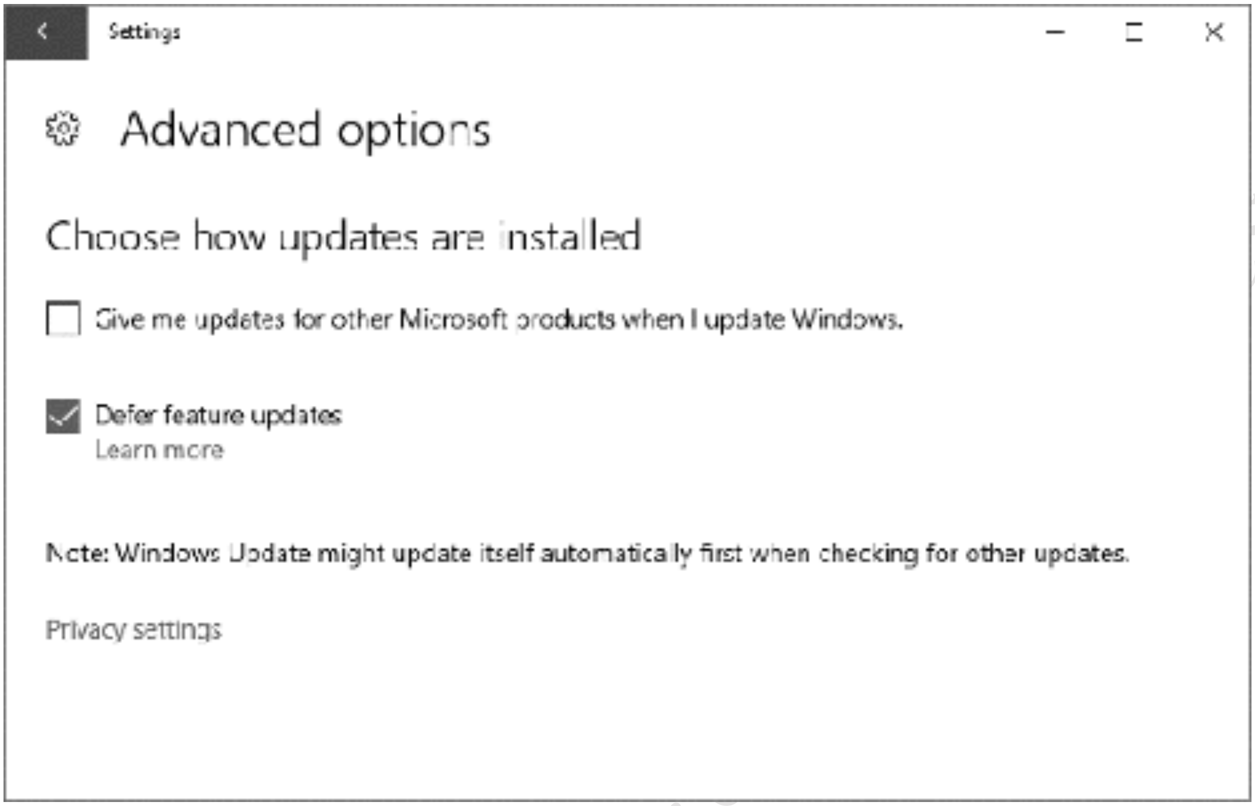
Time:

0 | 00

Day:

Figure 155: Set a custom restart time

Advanced options – this has two sub-options. The first controls whether any other Microsoft products on the server will be updated alongside Windows. The second is called *Defer feature updates* – if it is ticked then security updates for Windows Server are applied, but not updates that provide new or significantly changed functionality. You might want to enable this so as avoid any surprises and keep the server environment stable:



Advanced options

Choose how updates are installed

□ Give me updates for other Microsoft products when I update Windows.

☑ Defer feature updates

Learn more

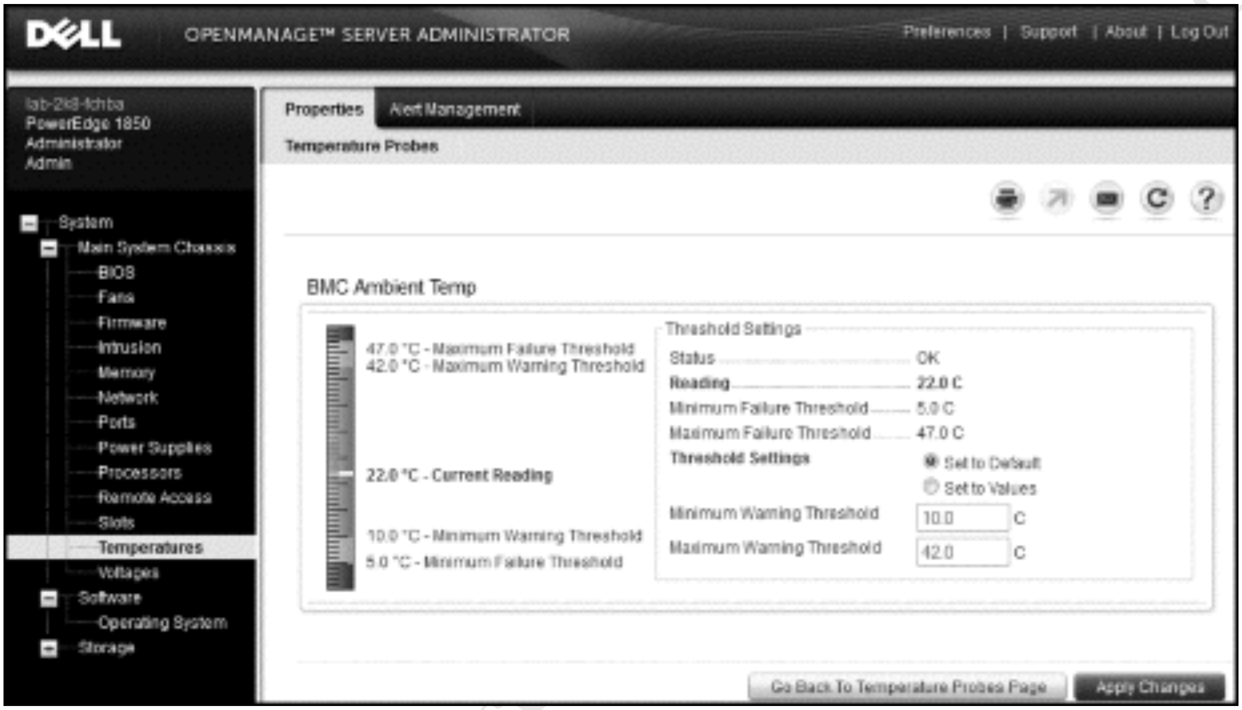
Note: Windows Update might update itself automatically first when checking for other updates.

Privacy settings

Figure 156: Windows Update Advanced options

10.9 Install Server Management Software

Most tier one server suppliers provide some form of management software to help monitor and manage the health of their server hardware e.g. the RAID sub-system, operating temperatures etc. For instance, Dell have a program called *OpenManage*. This should be installed on the server once the main build is complete. It should be checked on a regular basis, as it may provide valuable information about the status of the hardware and the RAID array. Some of the management packages can be configured to generate email alerts in the event of problems, which is useful.



BMC Ambient Temp

47.0 °C - Maximum Failure Threshold
42.0 °C - Maximum Warning Threshold
22.0 °C - Current Reading
10.0 °C - Minimum Warning Threshold
5.0 °C - Minimum Failure Threshold

Threshold Settings

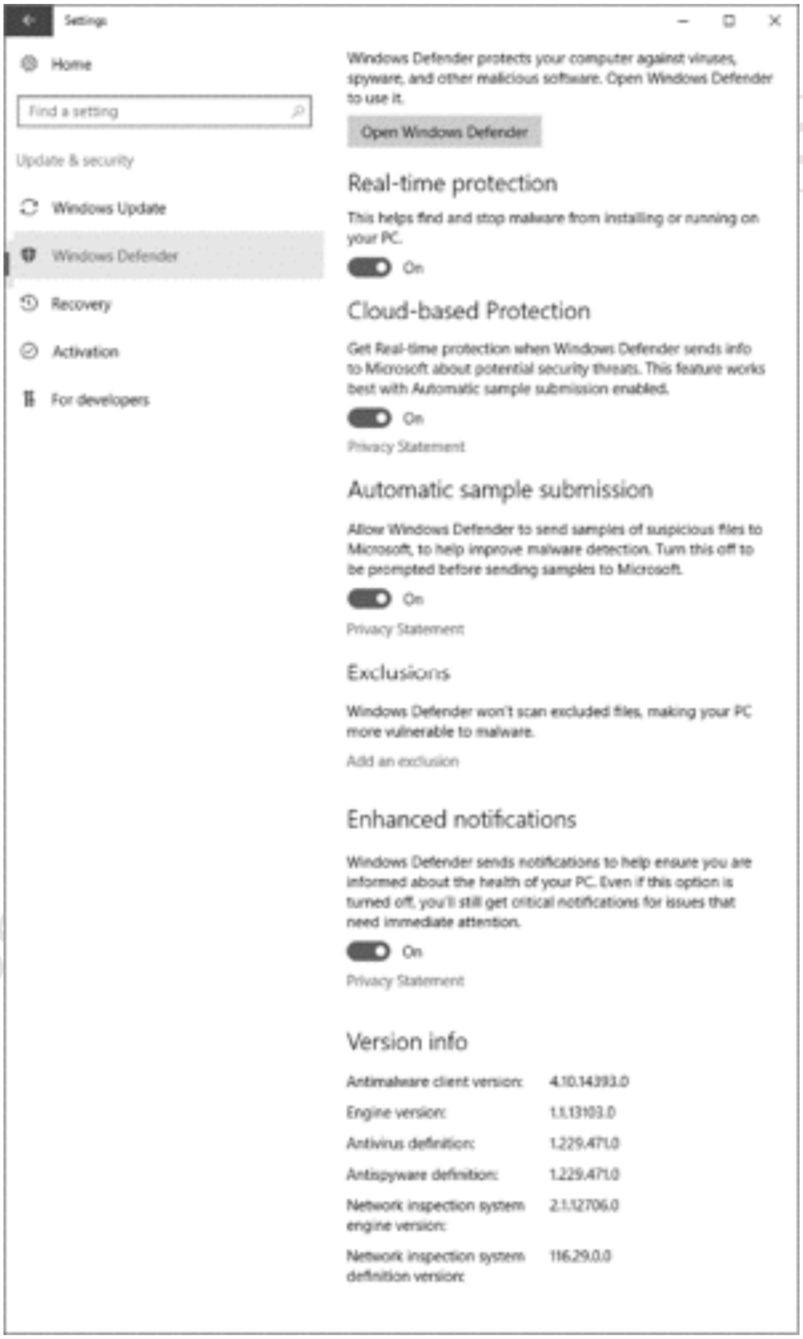
Status .... OK
Reading .... **22.0 C**
Minimum Failure Threshold .... 5.0 C
Maximum Failure Threshold .... 47.0 C
Threshold Settings ● Set to Default ○ Set to Values
Minimum Warning Threshold 10.0 C
Maximum Warning Threshold 42.0 C

Figure 157: Example of server management software

10.10 Windows Defender

Servers are susceptible to viruses and malware in the same way that regular Windows computers can be and for this reason need to be protected. Microsoft have a free product called *Windows Defender*, which is an integral part of the Windows Server package. It is installed automatically by default.

To check the status of Windows Defender, click **Start** > **Settings** > **Update & security** > **Windows Defender** to display the following screen. *Real-time protection* should be set to **On**; the other settings are optional but if you set them to **On** the server will send more information to Microsoft, which you may or may not wish to do:



Windows Defender protects your computer against viruses, spyware, and other malicious software. Open Windows Defender to use it.

Real-time protection

This helps find and stop malware from installing or running on your PC.

On

Cloud-based Protection

Get Real-time protection when Windows Defender sends info to Microsoft about potential security threats. This feature works best with Automatic sample submission enabled.

On

Privacy Statement

Automatic sample submission

Allow Windows Defender to send samples of suspicious files to Microsoft, to help improve malware detection. Turn this off to be prompted before sending samples to Microsoft.

On

Privacy Statement

Exclusions

Windows Defender won't scan excluded files, making your PC more vulnerable to malware.

Add an exclusion

Enhanced notifications

Windows Defender sends notifications to help ensure you are informed about the health of your PC. Even if this option is turned off, you'll still get critical notifications for issues that need immediate attention.

On

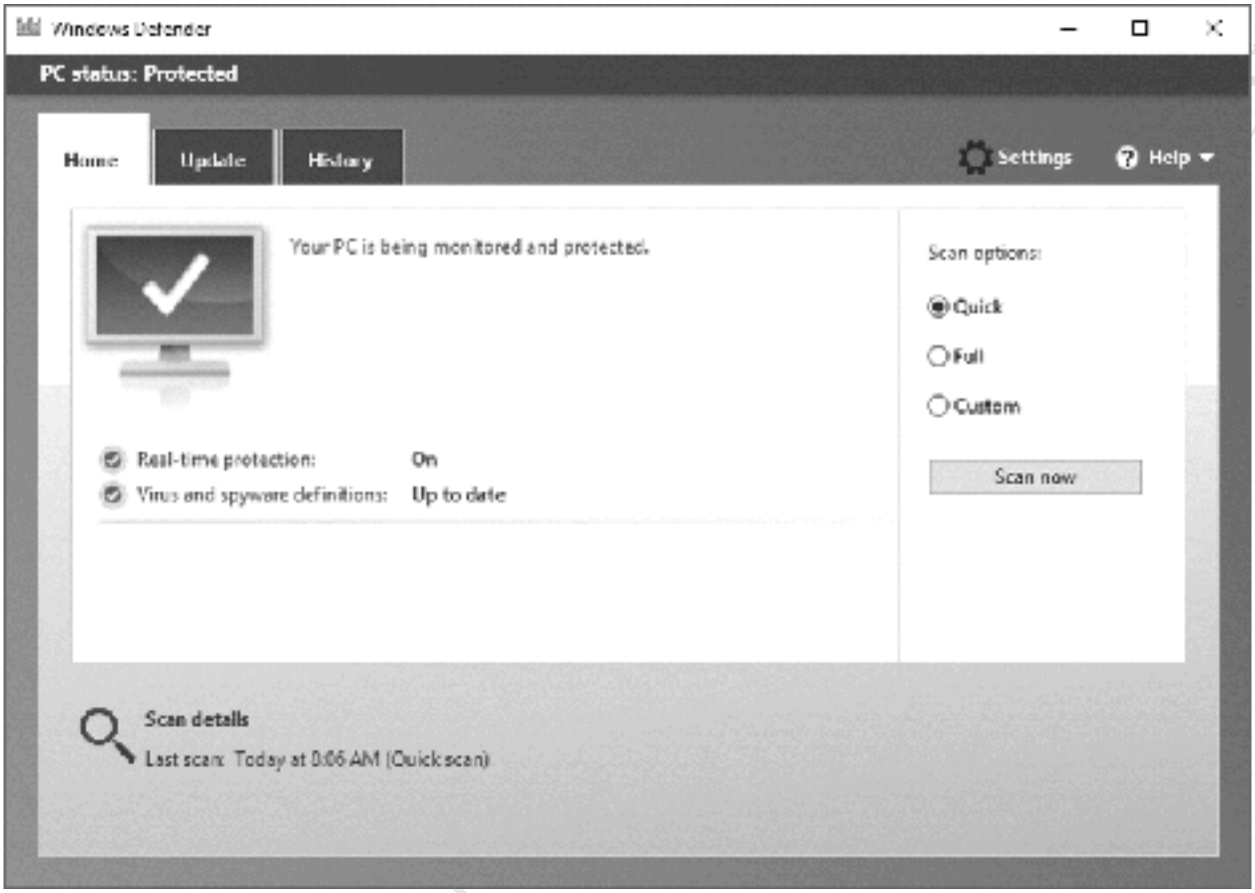
Privacy Statement

Version info

Antimalware client version:	4.10.14393.0
Engine version:	1.1.13103.0
Antivirus definition:	1.229.471.0
Antispyware definition:	1.229.471.0
Network inspection system engine version:	2.1.12706.0
Network inspection system definition version:	116.29.0.0

Figure 158: Settings for Windows Defender

For greater control over Windows Defender, click where it reads Use **Open Windows Defender** at the top of the panel. This will display a console screen from where you can initiate scans and view the results. You may recognise this screen, as Windows Defender is also available for Windows 10, Windows 8 and Windows 7 (where it is known as Windows Security Essentials):



PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On

Virus and spyware definitions: Up to date

Scan options:

● Quick

○ Full

○ Custom

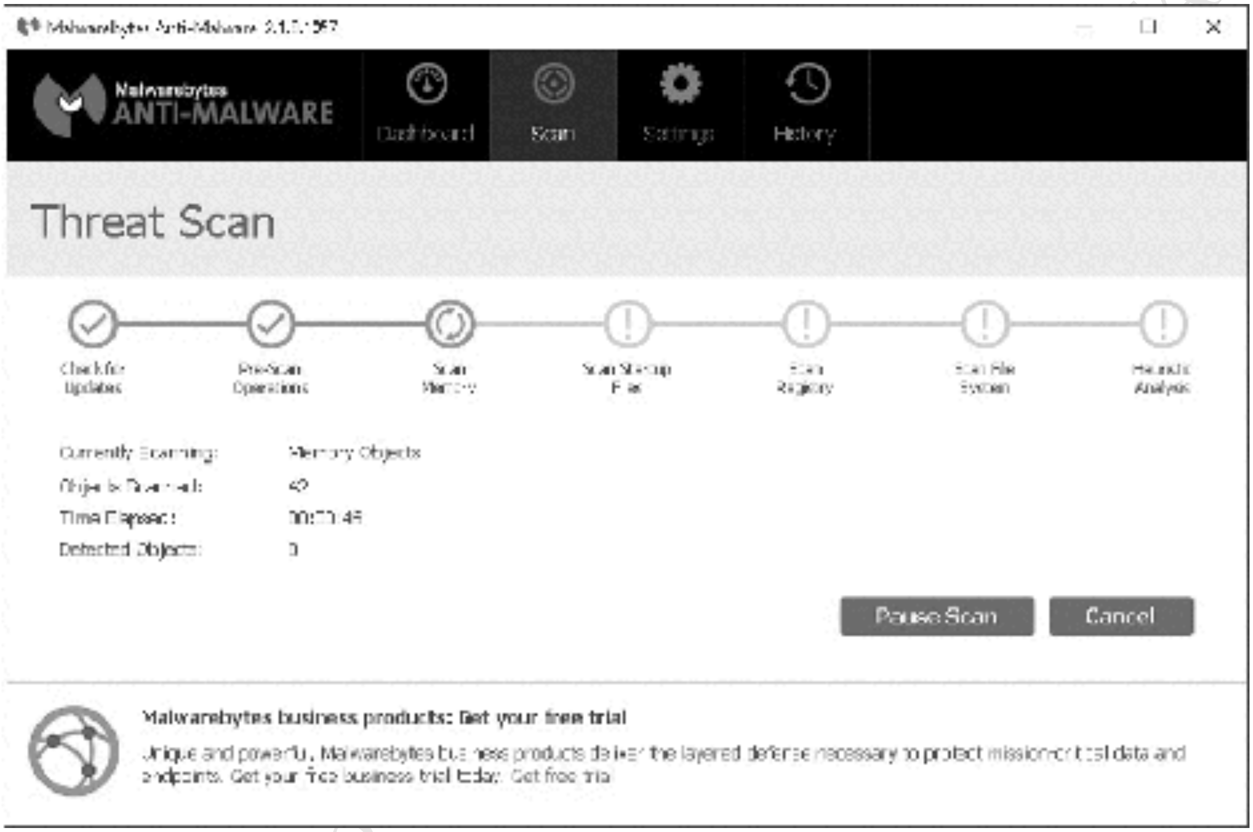
Scan details

Last scan: Today at 8:06 AM (Quick scan)

Figure 159: Windows Defender console

10.11 Third Party Antimalware/Antivirus Software

Windows Server Antimalware provides a high degree of protection against malware but some people may wish to use a third-party product in addition or as a replacement to it. Malwarebytes is a highly regarded piece of software for protecting against and cleaning up malware on computers and will often sort out the 'nasties' that even the best anti-virus software misses, providing a valuable second line of defence. It works well on Windows Server and is available in both free and paid versions. The paid version is very low cost and has the advantage that scans can be scheduled to take place automatically, as opposed to run manually. It is best obtained by downloading it directly from the *www.malwarebytes.org* website.



Currently Scanning: Memory Objects
Objects Scanned: 42
Time Elapsed: 00:00:45
Detected Objects: 0

Malwarebytes business products: Get your free trial

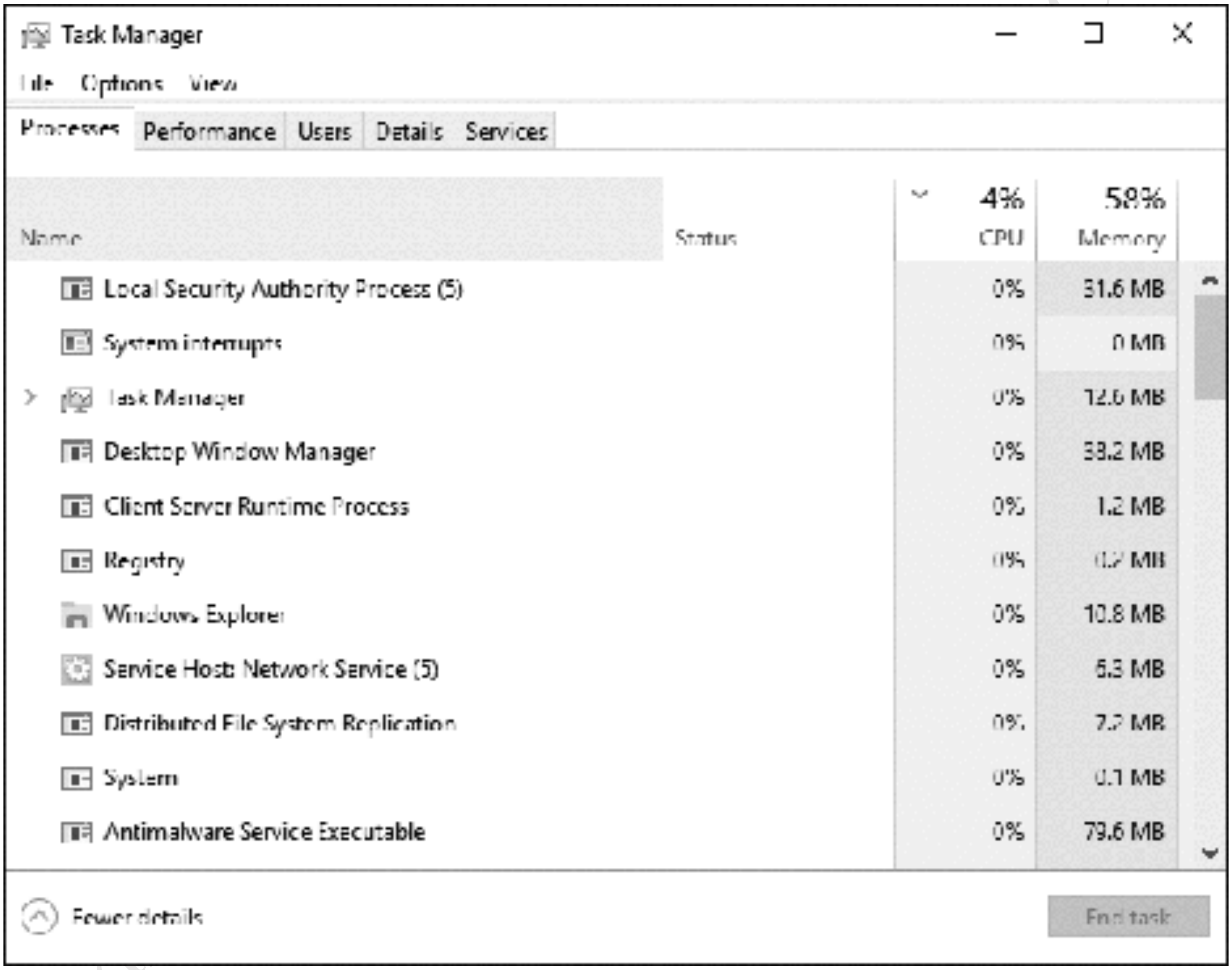
Unique and powerful, Malwarebytes business products deliver the layered defense necessary to protect mission-critical data and endpoints. Get your free business trial today. Get free trial

Figure 160: Main Malwarebytes scan screen

10.12 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 12.9 Multiple Network Adapters (NIC Teaming).

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 will appear as a blank panel – click **More details** in the bottom left-hand corner to display the following screen:

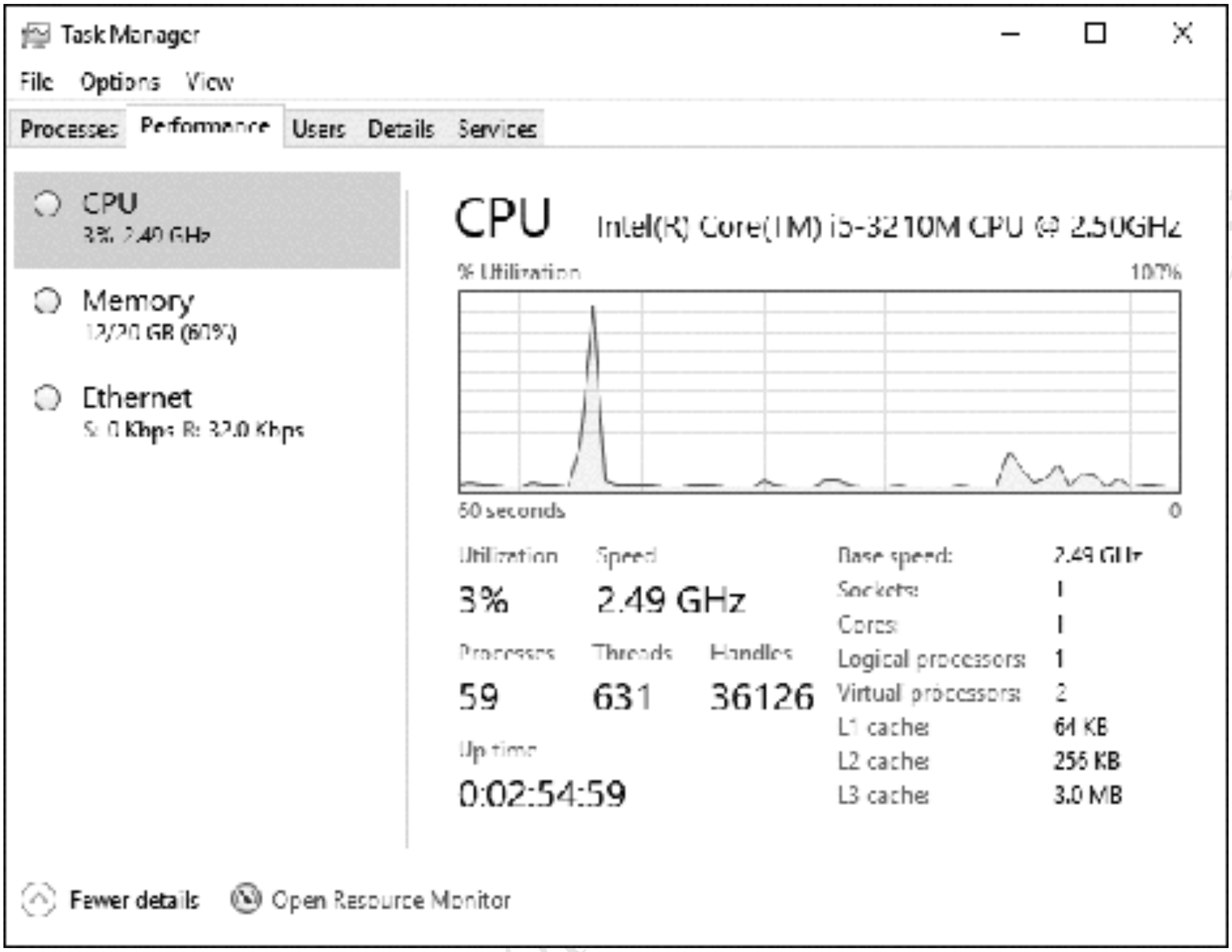


Name	Status	4% CPU	58% Memory
Local Security Authority Process (5)		0%	31.6 MB
System interrupts		0%	0 MB
Task Manager		0%	12.6 MB
Desktop Window Manager		0%	38.2 MB
Client Server Runtime Process		0%	1.2 MB
Registry		0%	0.7 MB
Windows Explorer		0%	10.8 MB
Service Host: Network Service (5)		0%	6.3 MB
Distributed File System Replication		0%	7.7 MB
System		0%	0.1 MB
Antimalware Service Executable		0%	79.6 MB

Figure 161: 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:



CPU
3% 2.49 GHz

Memory
12/20 GB (60%)

Ethernet
S: 0 Kbps R: 32.0 Kbps

CPU Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz

Utilization 3%
Speed 2.49 GHz
Processes 59
Threads 631
Handles 36126
Up time 0:02:54:59

Base speed: 2.49 GHz
Sockets: 1
Cores: 1
Logical processors: 1
Virtual processors: 2
L1 cache: 64 KB
L2 cache: 256 KB
L3 cache: 3.0 MB

Figure 162: Task Manager Performance tab

More detailed information can be obtained by clicking **Open Resource Monitor** 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):

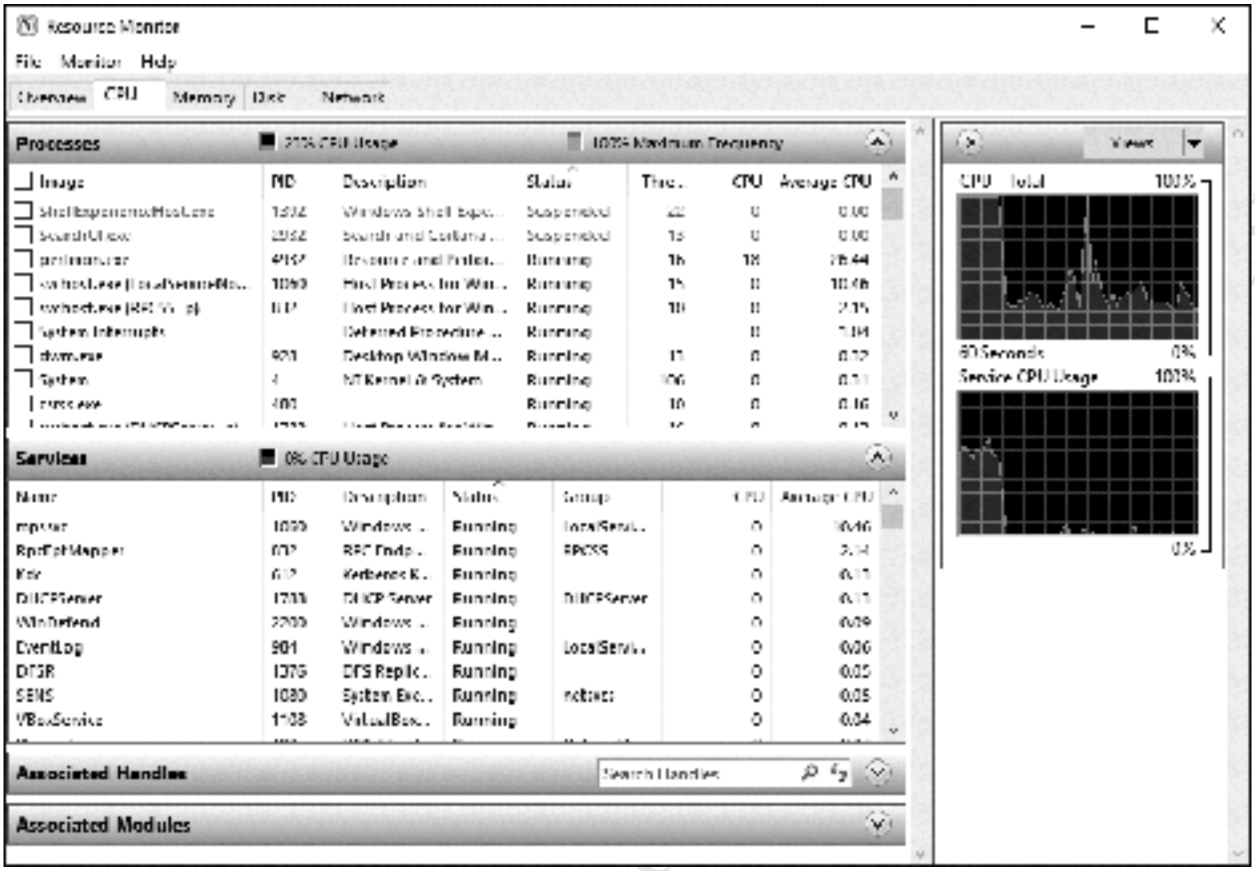


Image	PID	Description	Status	Threads	CPU	Average CPU
ShellExperienceHost.exe	1532	Windows Shell Expe...	Suspended	22	0	0.00
SearchUI.exe	2952	Search and Cortana ...	Suspended	15	0	0.00
perfmon.exe	4192	Resource and Perfor...	Running	16	18	26.44
svchost.exe (LocalServiceNo...	1060	Host Process for Win...	Running	15	0	10.46
svchost.exe (RPCSS -p)	812	Host Process for Win...	Running	10	0	2.15
System Interrupts		Deferred Procedure ...	Running		0	1.04
dwm.exe	920	Desktop Window M...	Running	11	0	0.72
System	4	NT Kernel & System	Running	106	0	0.11
csrss.exe	400		Running	10	0	0.16

Name	PID	Description	Status	Group	CPU	Average CPU
mpssvc	1060	Windows ...	Running	LocalServi...	0	10.46
RpcEptMapper	812	RPC Endp...	Running	RPCSS	0	2.14
Kdc	612	Kerberos K...	Running		0	0.17
DHCPServer	1788	DHCP Server	Running	DHCPServer	0	0.17
WinDefend	2200	Windows ...	Running		0	0.09
EventLog	904	Windows ...	Running	LocalServi...	0	0.06
DFSR	1076	DFS Replic...	Running		0	0.05
SENS	1080	System Eve...	Running	netsvcs	0	0.05
VBoxService	1108	VirtualBox...	Running		0	0.04

Figure 163: Resource Monitor screen

10.13 Windows Admin Center

There are several methods for accessing a server in order to manage it. The simplest method is by logging into it directly. Another method is by using Remote Desktop, as described previously. Microsoft offer several other tools, some of which are targeted at enterprise users. *Windows Admin Center* or *WAC* (known as *Project Honolulu* whilst it was under development), is a browser-based app for managing both servers and Windows 10 PCs and may be a long-term attempt at a universal solution. It does not have to be installed on the server itself, nor does it require anything to be installed on the server. It can be run from another Windows server, but it will not install on a domain controller (so if you have a single server, which by definition will therefore be a domain controller, you cannot run it on that). More typically, WAC is run from a Windows 10 PC and it needs to be running the 64-bit version of Windows 10. Begin by downloading and installing WAC from the official Microsoft website. During installation, it will default to using port 6516: it is suggested that you leave this as is and do not change it. Upon opening WAC for the first time, if prompted to select a certificate, choose the **Windows Admin Center Client**. WAC will display using the default browser on the PC and in this instance we are using Microsoft Edge.

Initially, the Windows 10 PC upon which WAC is running will be listed under *All Connections* (i.e. the computers that can be managed). To add the server, click where it read **+Add** on the left-hand side of the screen. On the panel that appears, click **Add Server Connection**:

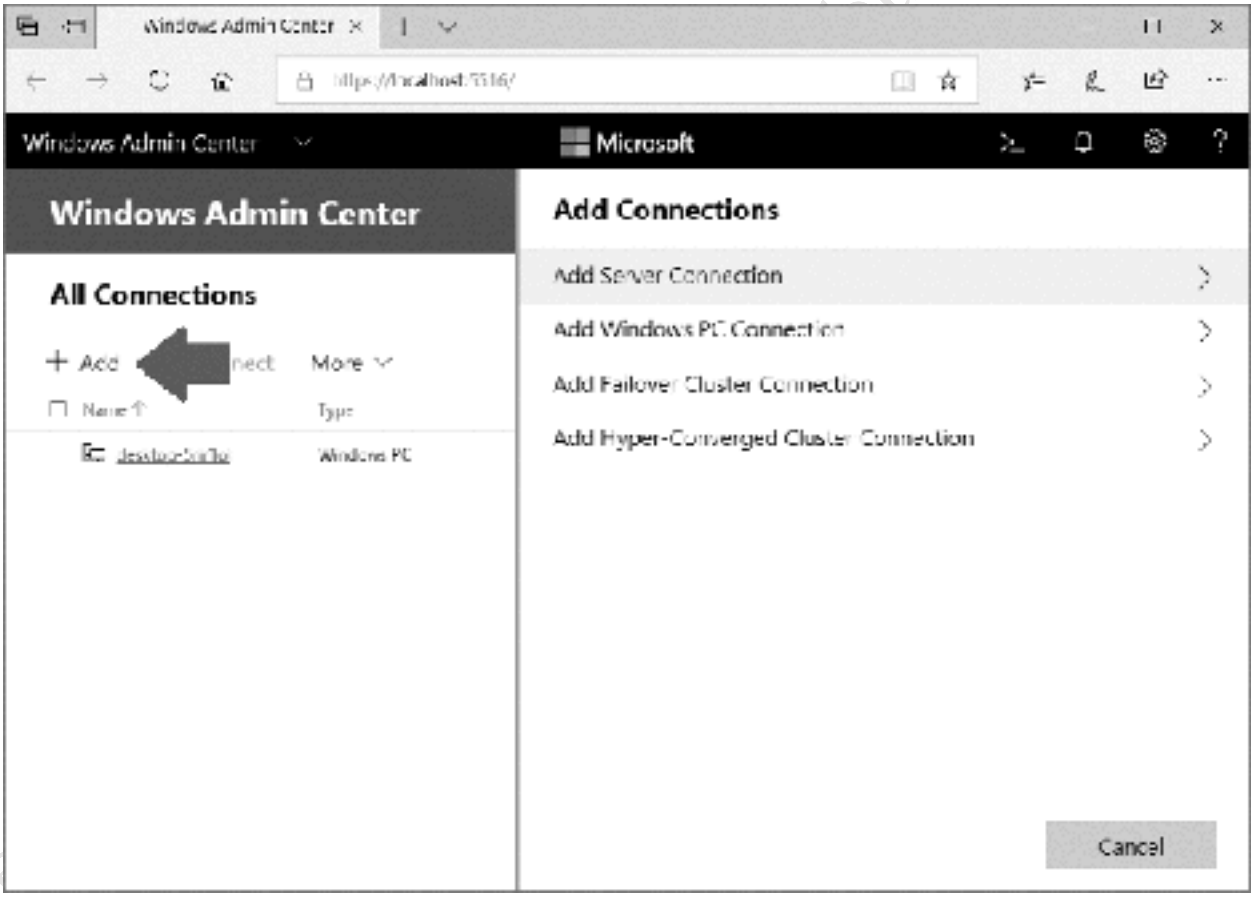
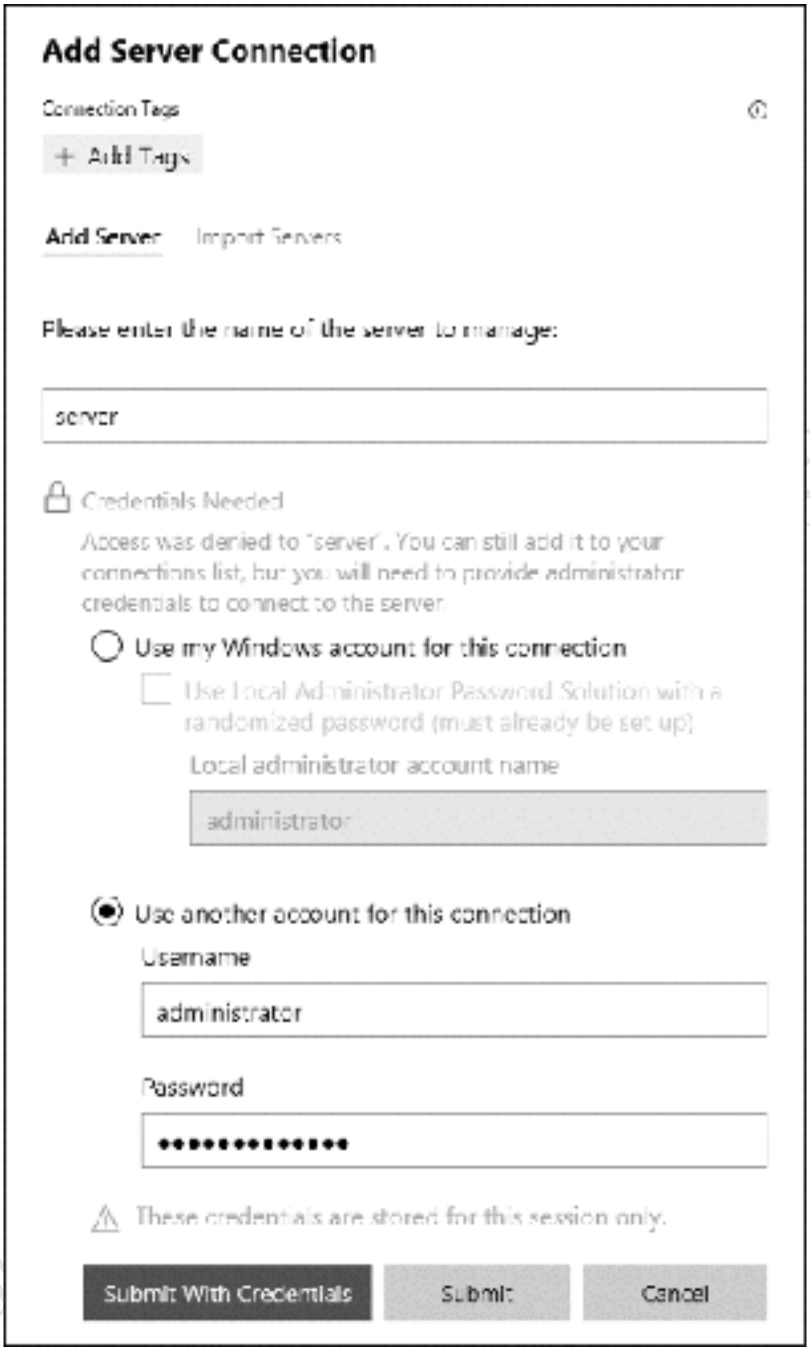


Figure 164: WAC – Adding a new connection

On the next panel, enter the name of the server it is desired to manage, which in our example is *server*. It is necessary to specify login credentials; the easiest option is to choose **Use another account for this connection a**nd enter the administrator account and password of the server. Click **Submit With Credentials**:



Add Server Connection

Connection Tags

+ Add Tags

Add Server   Import Servers

Please enter the name of the server to manage:

server

Credentials Needed

Access was denied to "server". You can still add it to your connections list, but you will need to provide administrator credentials to connect to the server.

○ Use my Windows account for this connection

□ Use Local Administrator Password Solution with a randomized password (must already be set up)

Local administrator account name

administrator

● Use another account for this connection

Username

administrator

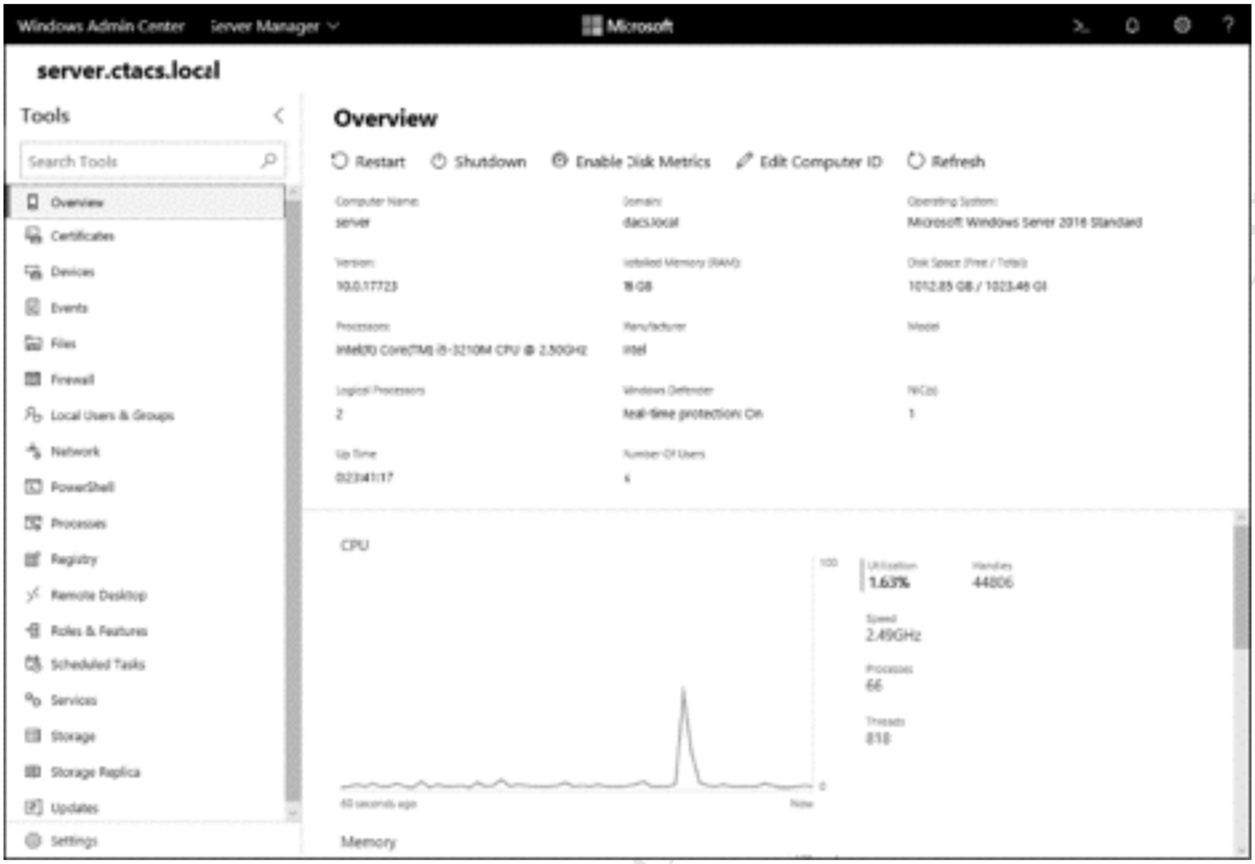
Password

•••••••••••••

These credentials are stored for this session only.

Figure 165: WAC – Add Server Connection

After a few seconds, the server will be added to the list of available connections. Click it, and enter the administrator logon credentials when prompted. After a few seconds, an overview screen will be displayed:



Computer Name: server
Domain: ctacs.local
Operating System: Microsoft Windows Server 2016 Standard
Version: 10.0.17723
Installed Memory (RAM): 16 GB
Disk Space (Free / Total): 1012.85 GB / 1023.46 GB
Processors: Intel(R) Core(TM) i5-3210M CPU @ 2.50GHz
Manufacturer: Intel
Model:
Logical Processors: 2
Windows Defender: Real-time protection: On
NIC(s): 1
Up Time: 0:23:41:17
Number Of Users: 4

Utilization: 1.63%
Handles: 44806
Speed: 2.49GHz
Processes: 66
Threads: 818

Figure 166: Overview of Server

With WAC, most aspects of the remote server, as covered in this chapter and elsewhere, can be configured and managed. Additionally, it is possible to directly access the file system of the server, use PowerShell, run Remote Desktop, add new Roles and Features to the server, plus restart or shut it down.

WAC is particularly useful if the network environment consists exclusively of Windows 10 PCs, as everything can be managed from one place. Any legacy servers running Windows Server 2012 can also be managed.

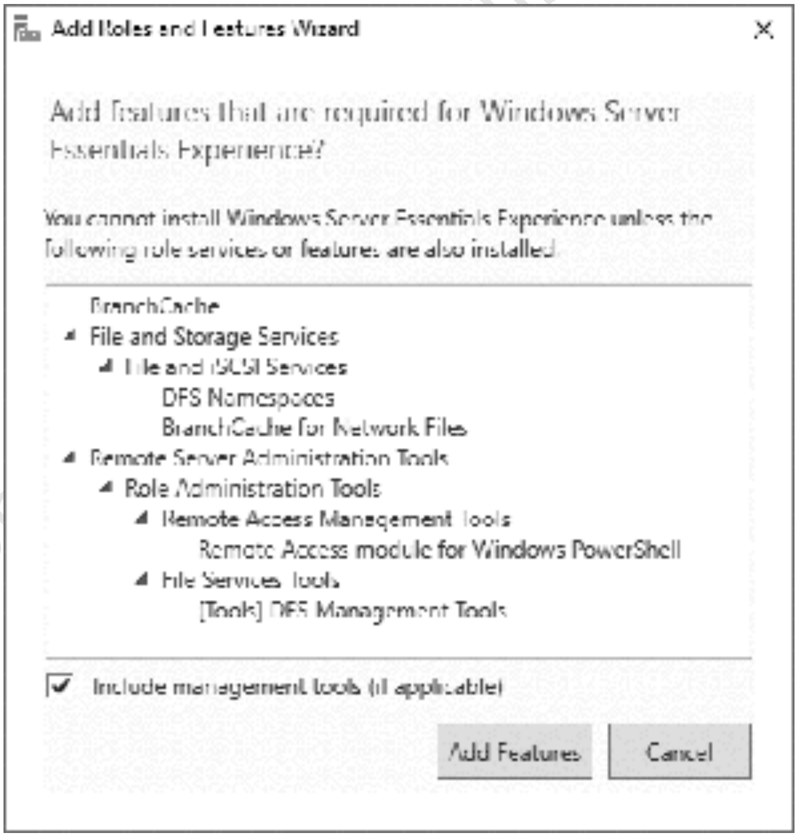
11. WINDOWS SERVER ESSENTIALS EXPERIENCE

11.1 Overview

Windows Server Essentials 2016 is an edition of Windows Server specifically aimed at small businesses that do not have in-house IT support. It includes a simplified user interface, designed to make it easier to configure and manage the server. However, beneath the hood it is a regular version of Windows Server and the simplified interface – known as the *Windows Server Essentials Dashboard* – can also be added to the standard versions of Windows Server, where it is known as the *Windows Server Essentials Experience*. Why would you wish to do this? There are three possible reasons. One reason is that Window Server 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. The second reason is that the Windows Server Essentials Dashboard is easier to work with than the regular Windows Server tools, both for everyday tasks as well as some more advanced ones (an example of which is remote connectivity, discussed later); it is thus useful for organizations with limited IT resources. The final reason is that you might just prefer to use it.

11.2 Installing Windows Server Essentials Experience

To install Windows Server Essentials Experience, 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. A message about the requirement for additional features is displayed – click the **Add Features** button to proceed:



Add Features that are required for Windows Server Essentials Experience?

You cannot install Windows Server Essentials Experience unless the following role services or features are also installed.

BranchCache
- File and Storage Services
  - File and iSCSI Services
    - DFS Namespaces
    - BranchCache for Network Files
- Remote Server Administration Tools
  - Role Administration Tools
    - Remote Access Management Tools
      - Remote Access module for Windows PowerShell
    - File Services Tools
      - [Tools] DFS Management Tools

☑ Include management tools (if applicable)

Figure 167: Add Roles and Features Wizard

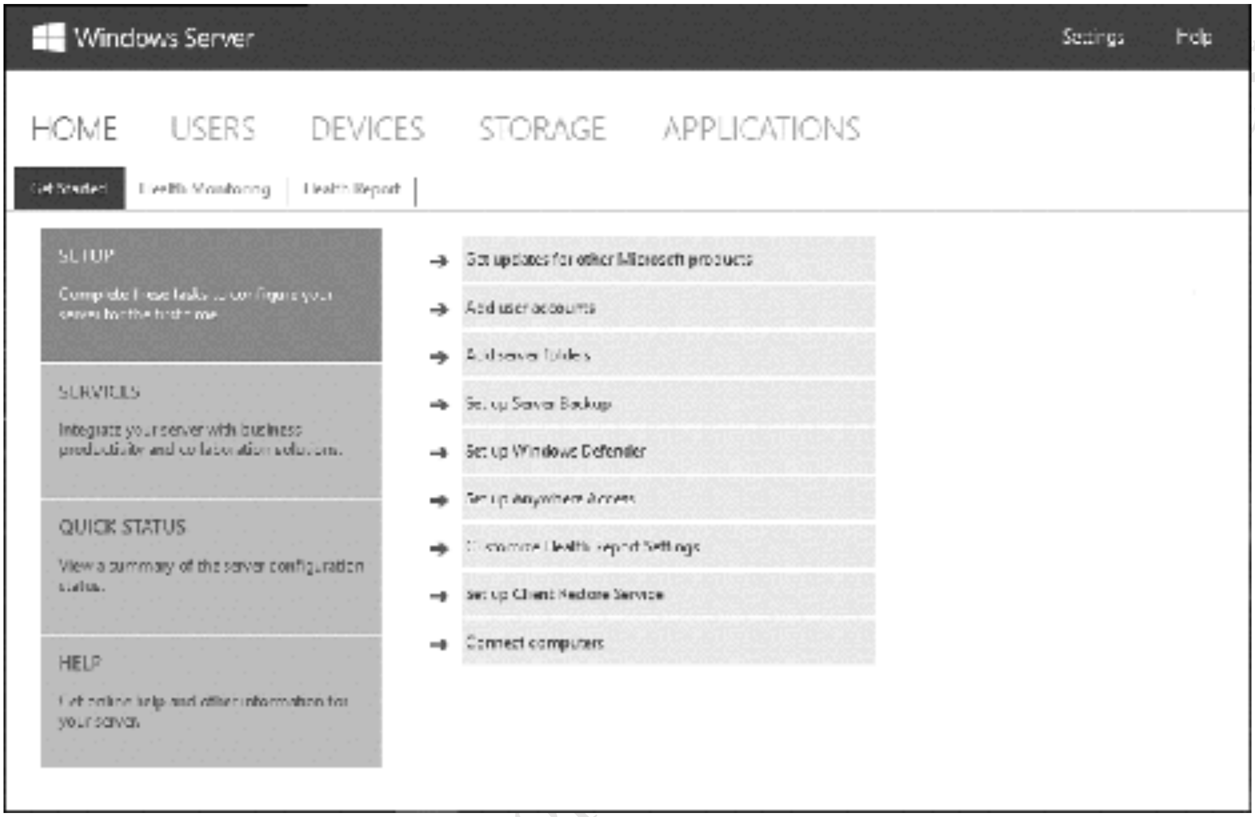
Click **Next** on the subsequent screens until you reach the *Confirm installation selections* screen. Tick the **Restart the destination server automatically if required** box, acknowledge the message, then click **Install**.

The installation will run for several minutes. When complete, click Close. A new entry will have appeared in the left-hand panel of Server Manager, entitled *Windows Server Essentials Experience*. Click it and on the resultant panel there will be a message that configuration work is required; click it and also the **Configure Windows Server Essentials** link. After a short while a screen entitled *Configure Windows Server Essentials* is displayed; click the **Configure** button. The configuration process will then take at least several minutes to complete. When done, click **Close**.

A new icon called *Windows Server Essentials Dashboard* will have been placed on the Desktop of the server. Note that this is the Dashboard from Windows Server Essentials and quite separate and different from the regular Windows Server Manager Dashboard.

11.3 Windows Server Essentials Dashboard: Quick Overview

Double-click the *Windows Server Essentials Dashboard* icon to display the standard console for managing Essentials (there may be a short delay while it loads):



SETUP

Complete these tasks to configure your server for the first time

SERVICES

Integrate your server with business productivity and collaboration solutions.

QUICK STATUS

View a summary of the server configuration status.

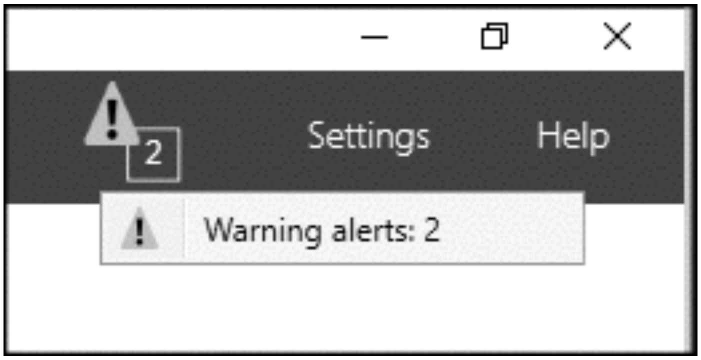
HELP

Get online help and other information for your server.

Figure 168: Windows Server Essentials Dashboard

The Dashboard is organized into several sections: *USERS*, *DEVICES*, *STORAGE* and *APPLICATIONS*. Each of these displays the status and characteristics of that topic and lists a number of clickable tasks pertaining to it. The *HOME* page – displayed above – is structured in a way to help setup the server using a checklist of tasks to be completed: *Add user accounts*, *Add server folders*, *Setup Server Backup* and so on. If you have already performed some of these activities using the standard Windows Server tools, then Essentials should correctly pick up the existing information. However, best practise is to stick with one or the other, rather than mix and match.

At the top of the screen is a status section and there may sometimes be warning or error messages indicated (see illustration below). If there are messages, click in the area to expand and then click on them for a more detailed screen. 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).

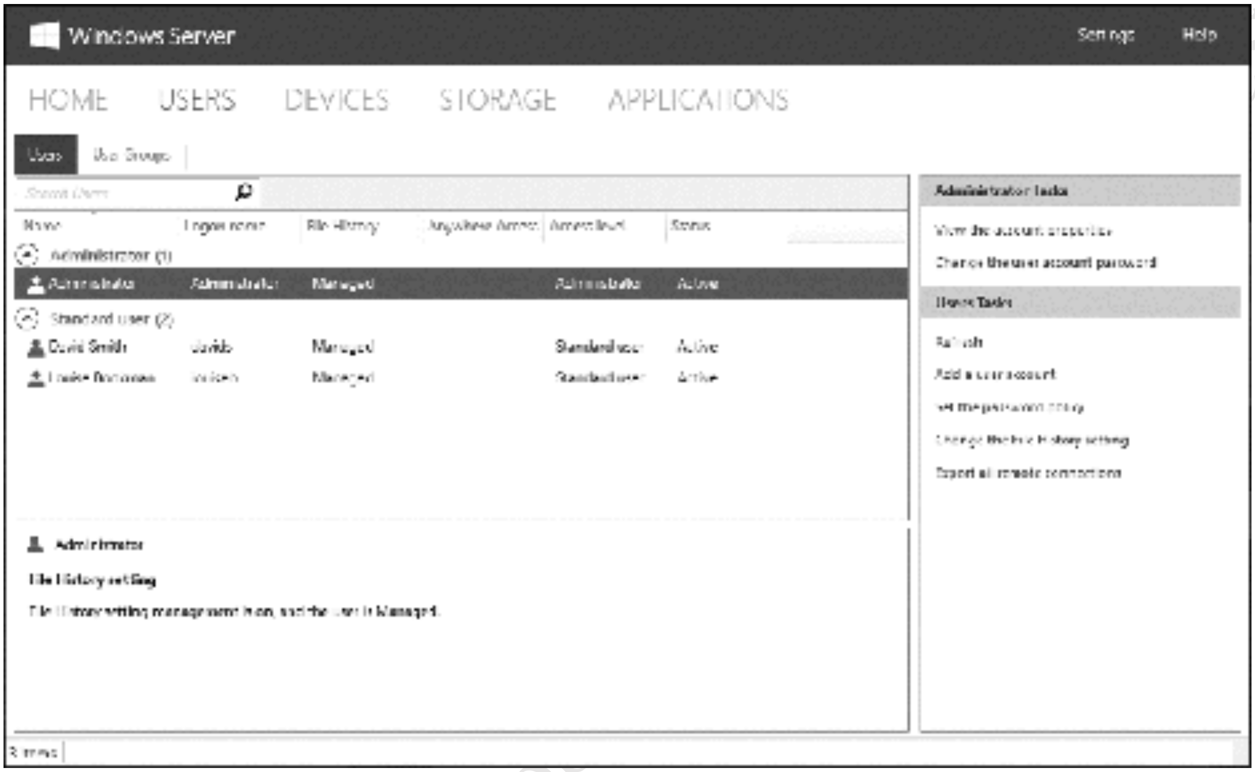


Warning alerts: 2

Figure 169: Messages on the Dashboard

11.4 Managing Users from the Windows Server Essentials Dashboard

One of the most common tasks on an operational server is managing users so by way of example we will look at how this is done using Windows Server Experience Essentials. Launch the *Windows Server Essentials Dashboard* and click the *USERS* tab to display the following screen:



Name	Logon name	File History	Anywhere Access	Access level	Status
Administrator (1)					
Administrator	Administrator	Managed		Administrator	Active
Standard user (2)					
David Smith	davids	Managed		Standard user	Active
Louise [illegible]	[illegible]	Managed		Standard user	Active

Administrator

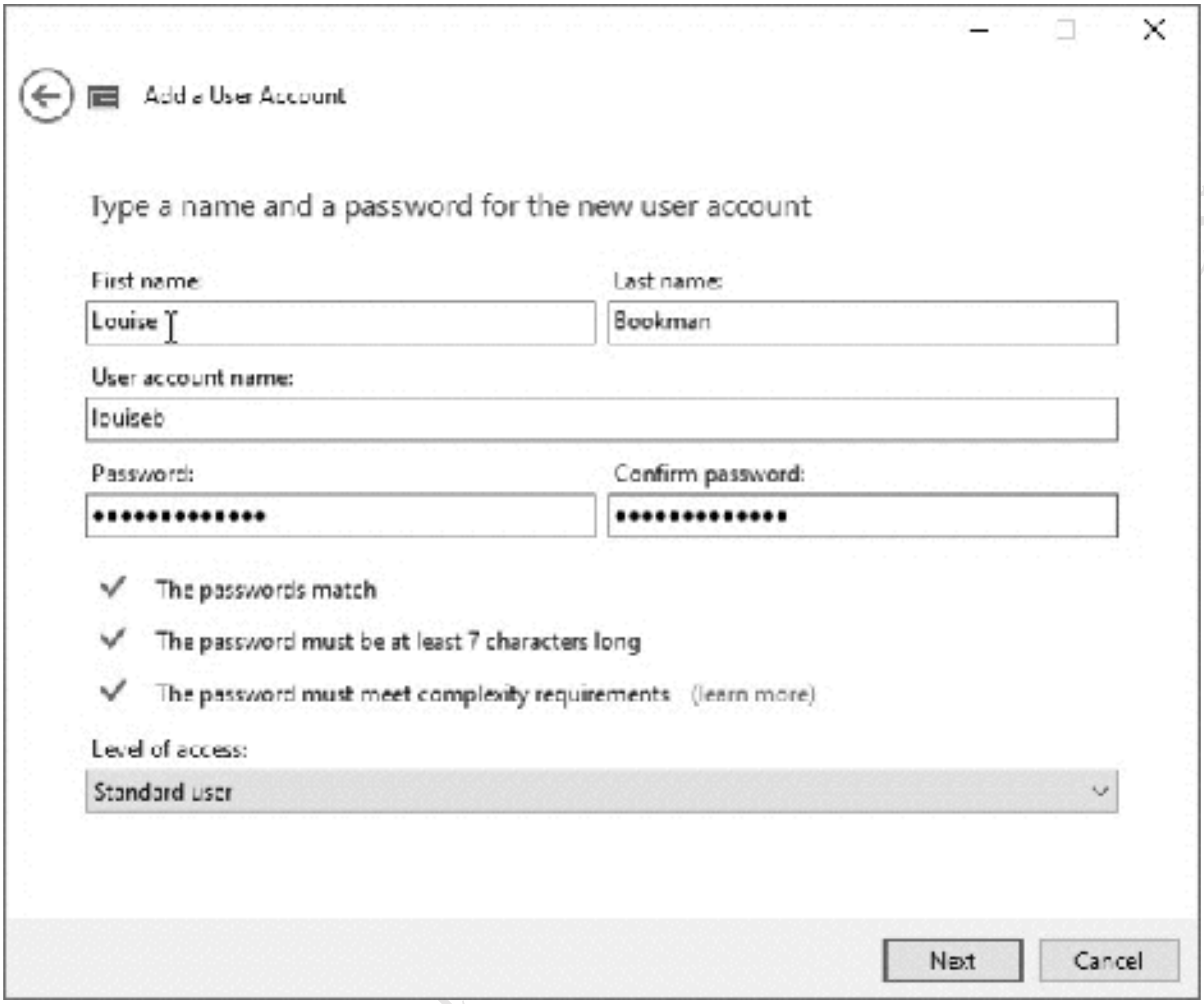
File History setting

File History setting management is on, and the user is Managed.

3 items

Figure 170: Users tab on the Windows Server Essentials Dashboard

On the right-hand side of the screen is a panel headed *User Tasks* - click **Add a user account** to display the following form:



Type a name and a password for the new user account

First name: Louise

Last name: Bookman

User account name: louiseb

Password: •••••••••••••

Confirm password: •••••••••••••

✓ The passwords match

✓ The password must be at least 7 characters long

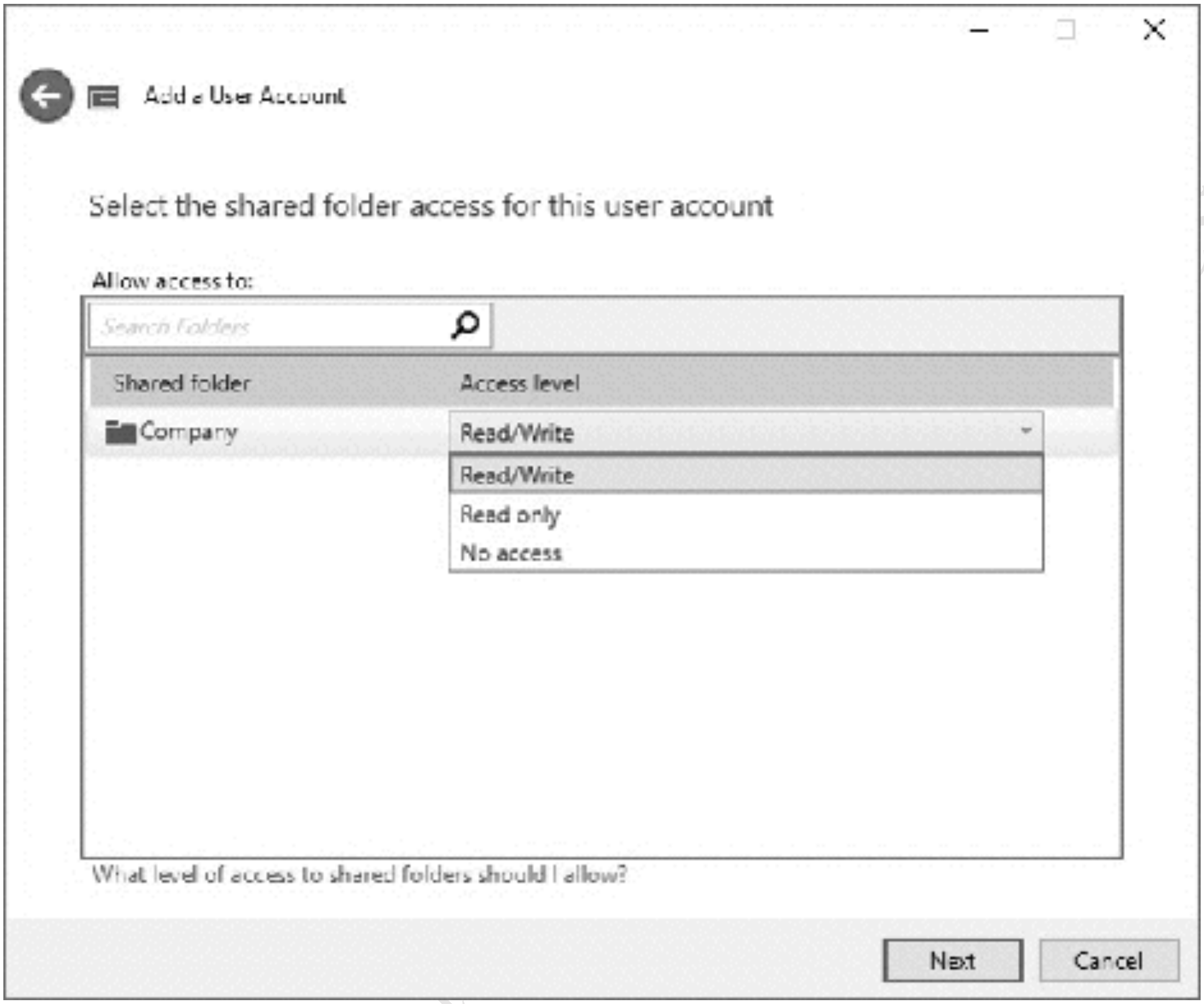
✓ The password must meet complexity requirements (learn more)

Level of access: Standard user

Figure 171: Adding a new user account

Enter the user's first and last names and Essentials will propose a *User account name* (i.e. logon name) of the two concatenated together. However, you might want to simplify things 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 network, note their role within the organization. Click **Next**.

The subsequent screen specifies what shared folders the user should have access to. There will always be at least one folder available – a built-in folder called *Company* is created during the installation of Windows Server Essentials Experience and the system is proposing *Read only* access to it; change it to the more useful **Read/Write** and click **Next**. Incidentally, the *Company* folder has most likely been created on the C: drive as a subfolder within one called *ServerFolders*. Unless you have a single drive, system this is not an ideal location and can be moved to another drive using the Windows Server Essentials Dashboard by clicking on the *STORAGE* tab followed by **Move the folder**.



Add a User Account

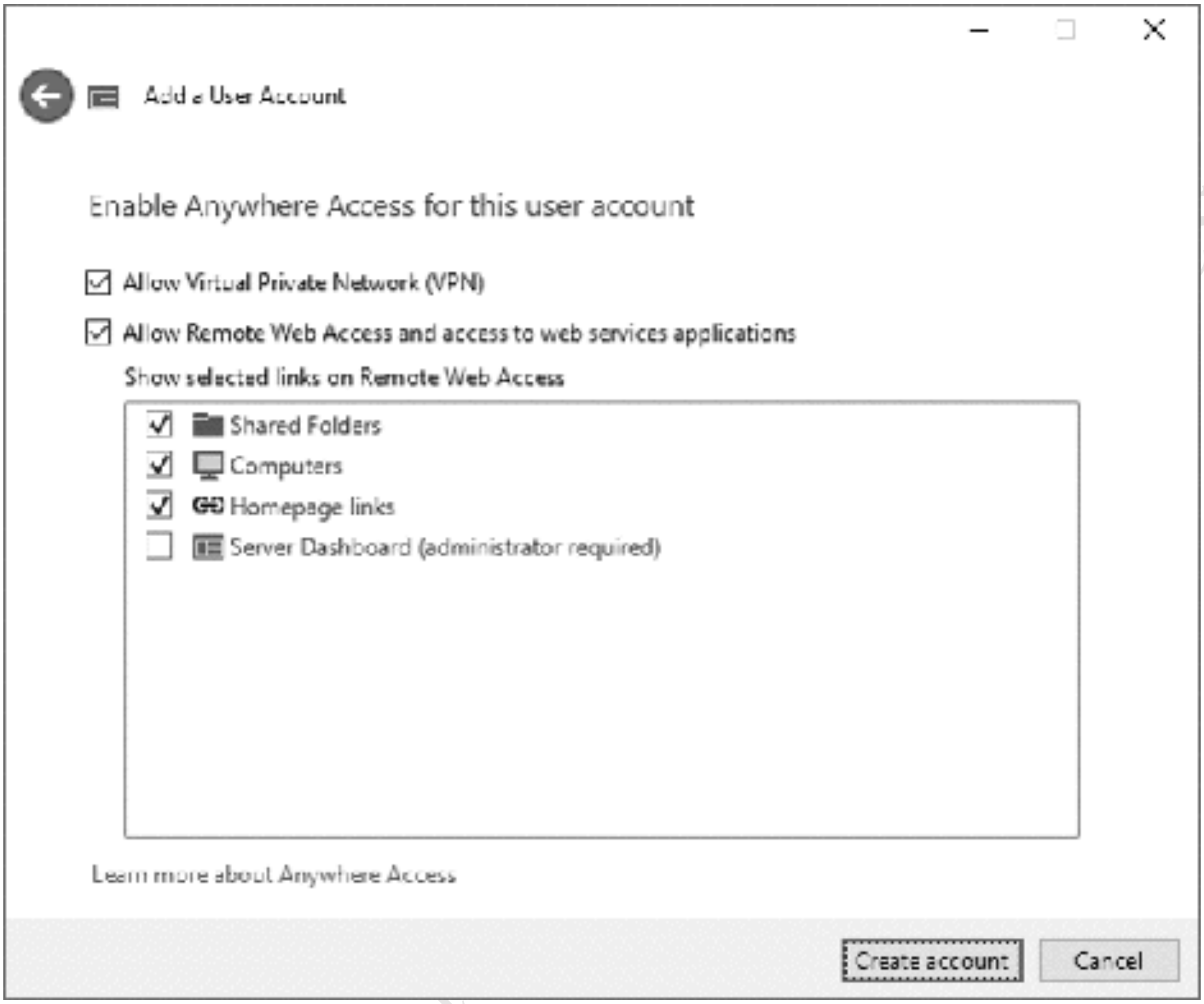
Select the shared folder access for this user account

Allow access to:

Shared folder	Access level
Company	Read/Write

Figure 172: Specify access to folder

The subsequent panel 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**.



Add a User Account

Enable Anywhere Access for this user account

☑ Allow Virtual Private Network (VPN)

☑ Allow Remote Web Access and access to web services applications

Show selected links on Remote Web Access

☑ Shared Folders
☑ Computers
☑ Homepage links
☐ Server Dashboard (administrator required)

Learn more about Anywhere Access

Figure 173: Specify Anywhere Access for user

Essentials will process for a few seconds and then display a confirmation that the user has successfully been created. Check the details then click **Close**.

11.5 Making Changes to Users

To change a user's password, go into the Dashboard and click the **USERS** tab. Click on 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 password**. 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**.

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.

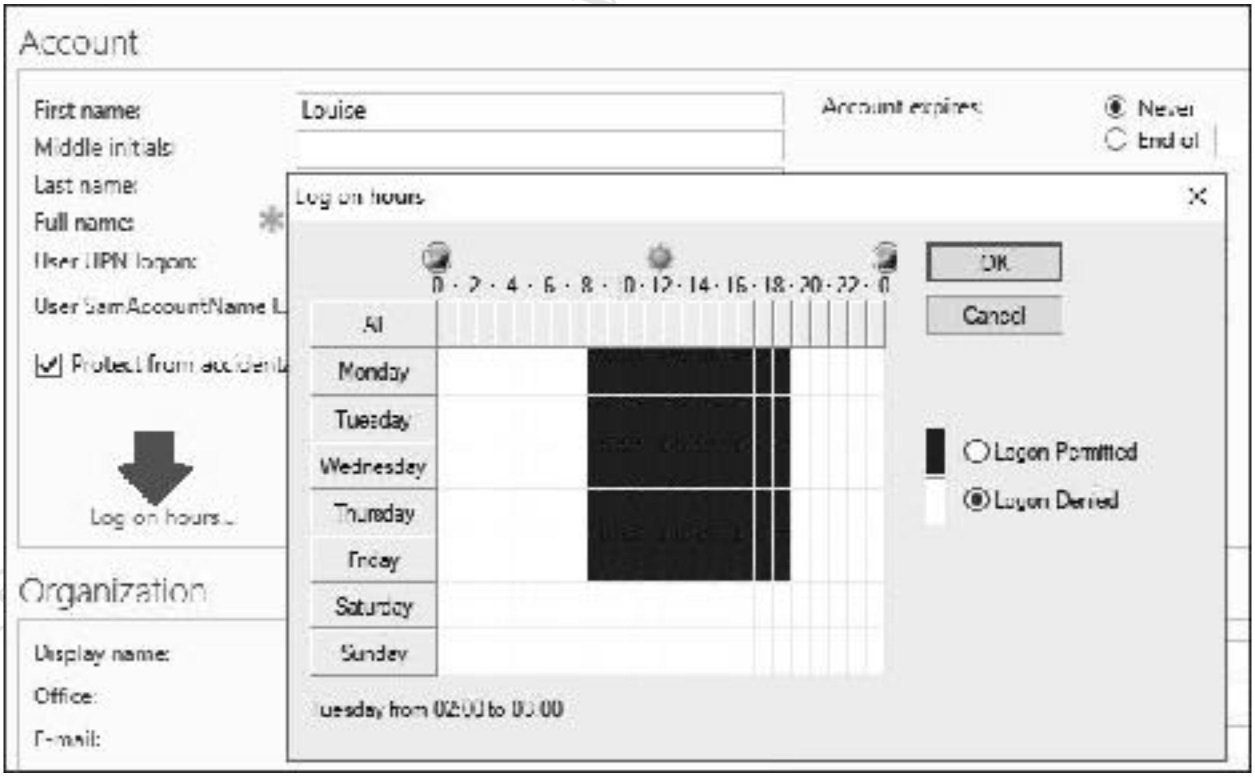
12.2 Windows Activation

Depending on the licence and type of installation you have, you may need to activate Windows Server. If this is the case, you will receive warning messages and may also find that some functions do not work properly. To check and activate if necessary, click **Start** > **Settings** > **Update & Security** > **Activation**. If Windows is not activated, click **Change product key** and enter your product key. The key is 25-digits long and is located on the Windows Server packaging or disk, as a sticker on the server, or in an email if it was purchased online. If you are in a corporate environment you may have a licensing agreement that provides product key information.

12.3 Controlling User Logon Times

It is possible to control the times when a particular user can logon to the system. Most organizations will probably not bother with this facility, but there are some situations when it can be useful. For instance, a school or college may not wish for students to be able to use the system outside of normal hours. Or, a business may have an important application which is updated overnight and whilst this is taking place they do not want users to access it.

Go into *Active Directory Administrative Center* and drill down to find the user as described previously. Double-click on the user's name to bring up the main form that summarises their details. Click where it reads **Log on hours…** in the *Accounts* section. Click on the segments – you can select more than one at a time by holding down the mouse button – and click **Logon Permitted** or **Logon Denied** as required. When finished click **OK**.



Account

First name: Louise

Account expires: ● Never ○ End of

Organization

Log on hours

○ Logon Permitted

● Logon Denied

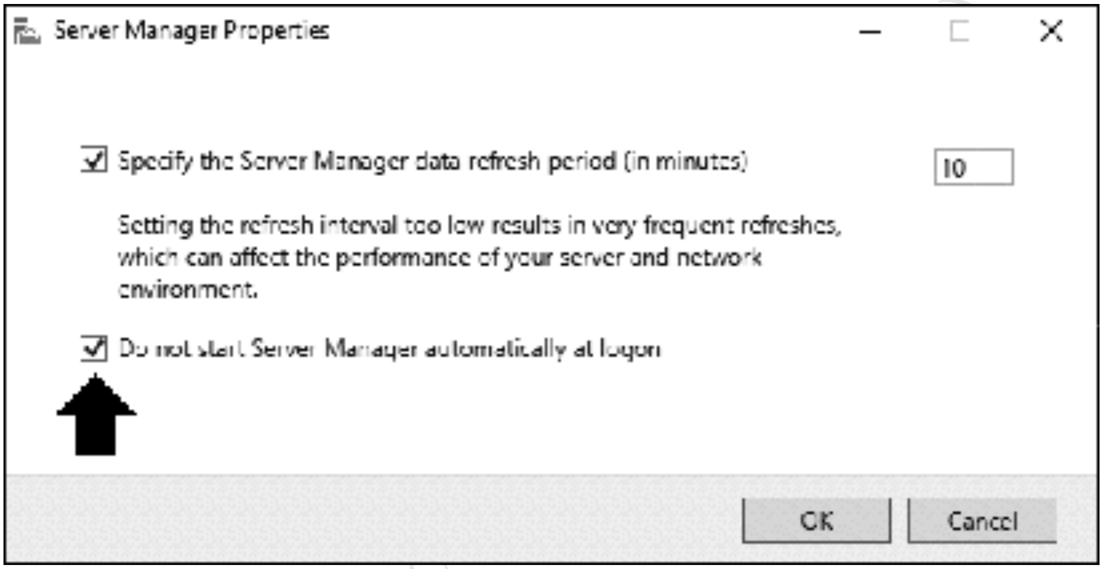
Tuesday from 02:00 to 03:00

Figure 174: Controlling logon hours for a user

Being able to control the permitted logon times for individuals gives a great deal of flexibility, but clearly requires a great deal of effort in an organization with many users. Consider, for instance, a college with several hundred students where it is required to restrict the logon times. The way to do this is through group policy, by creating an organization unit, making the applicable users part of the organization unit, then defining the logon times for that unit.

12.4 Controlling Server Manager Startup

By default, Server Manager starts up automatically when you login to the server. Many people will find this useful, but if you do not then it can be disabled. From within Server Manager, click **Manage** > **Server Manager Properties**. On the resultant panel, place a tick against **Do not start Server Manager automatically at logon** followed by **OK**. It is also possible to change the data refresh period for Server Manager, although the default value of 10 minutes is fine for most purposes.



Server Manager Properties

☑ Specify the Server Manager data refresh period (in minutes) 10

Setting the refresh interval too low results in very frequent refreshes, which can affect the performance of your server and network environment.

☑ Do not start Server Manager automatically at logon

OK Cancel

Figure 175: Server Manager logon behavior

12.5 My Server App for Windows Phone

My Server is an official app from Microsoft for use with Windows Phone devices. It is really designed for managing Windows Essentials servers, but if the Windows Server Essentials Experience is installed on top of regular Windows Server it can be useful (see 11. WINDOWS SERVER ESSENTIALS EXPERIENCE). It is used for managing users, devices and alerts, analogous to a mobile version of the Essentials Dashboard. It also provides access to the shared folders, although some people find it fairly rudimentary.

12.6 Microsoft Remote Desktop app for iOS

Microsoft have an official app for iOS that enables a Windows server to be accessed remotely for administrative purposes. It is basically an RDP client and can be downloaded free of charge from the App Store. To use this, the Remote Desktop capability of Windows Server needs to be enabled, as described in section 10.5 Headless Operation/Remote Desktop.

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, which can be moved around the screen, plus 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.

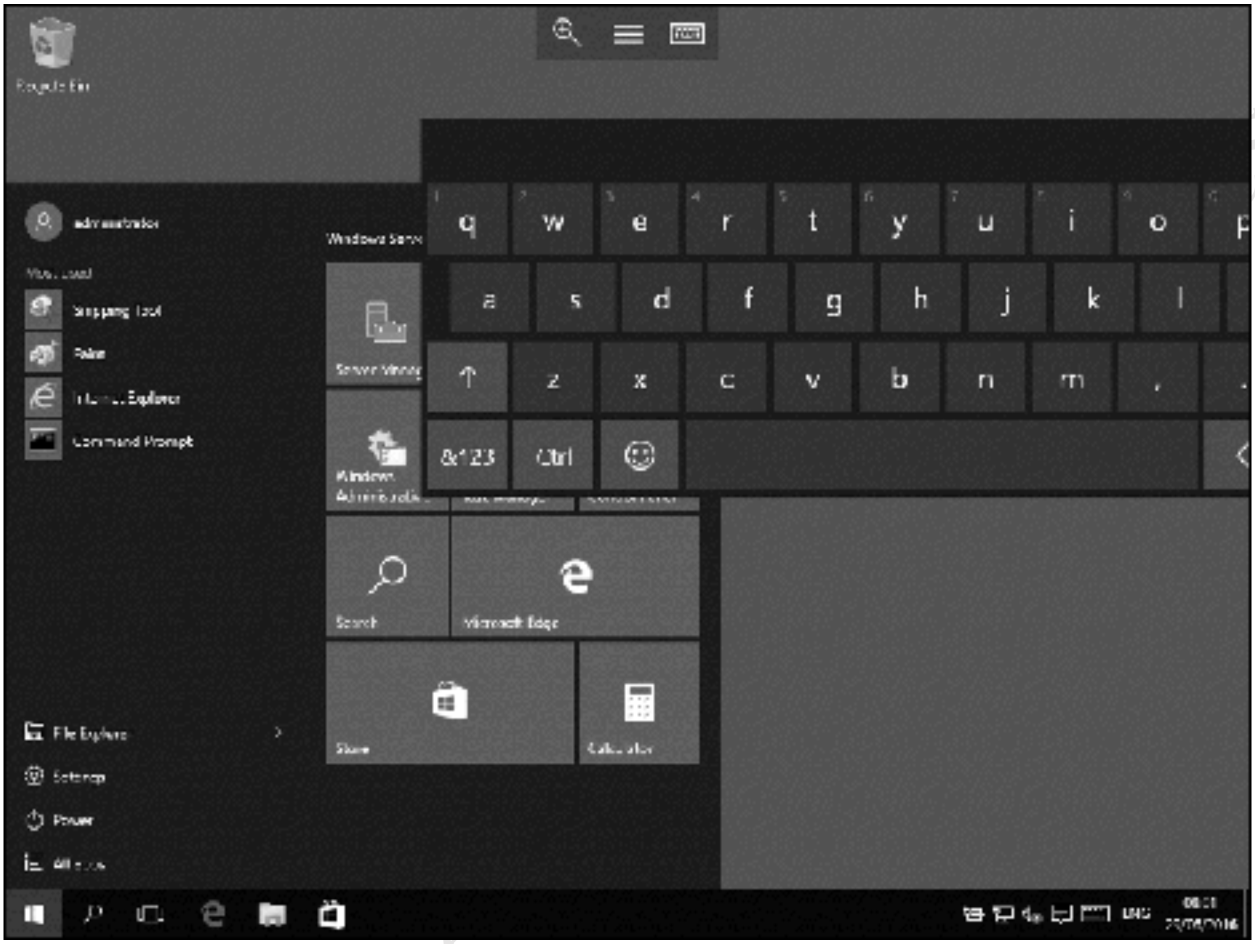


Figure 176: Microsoft Remote Desktop app running on iPad

12.7 Chromebooks

Chromebooks are an increasingly popular computing choice for many people. In essence a Chromebook is a laptop that only runs a browser; the key idea is that data is stored online on the cloud rather than as folders and files on the local computer or a network. The operating system – Chrome OS – is relatively minimalist compared to Windows or Mac OS X and this limits its capabilities.

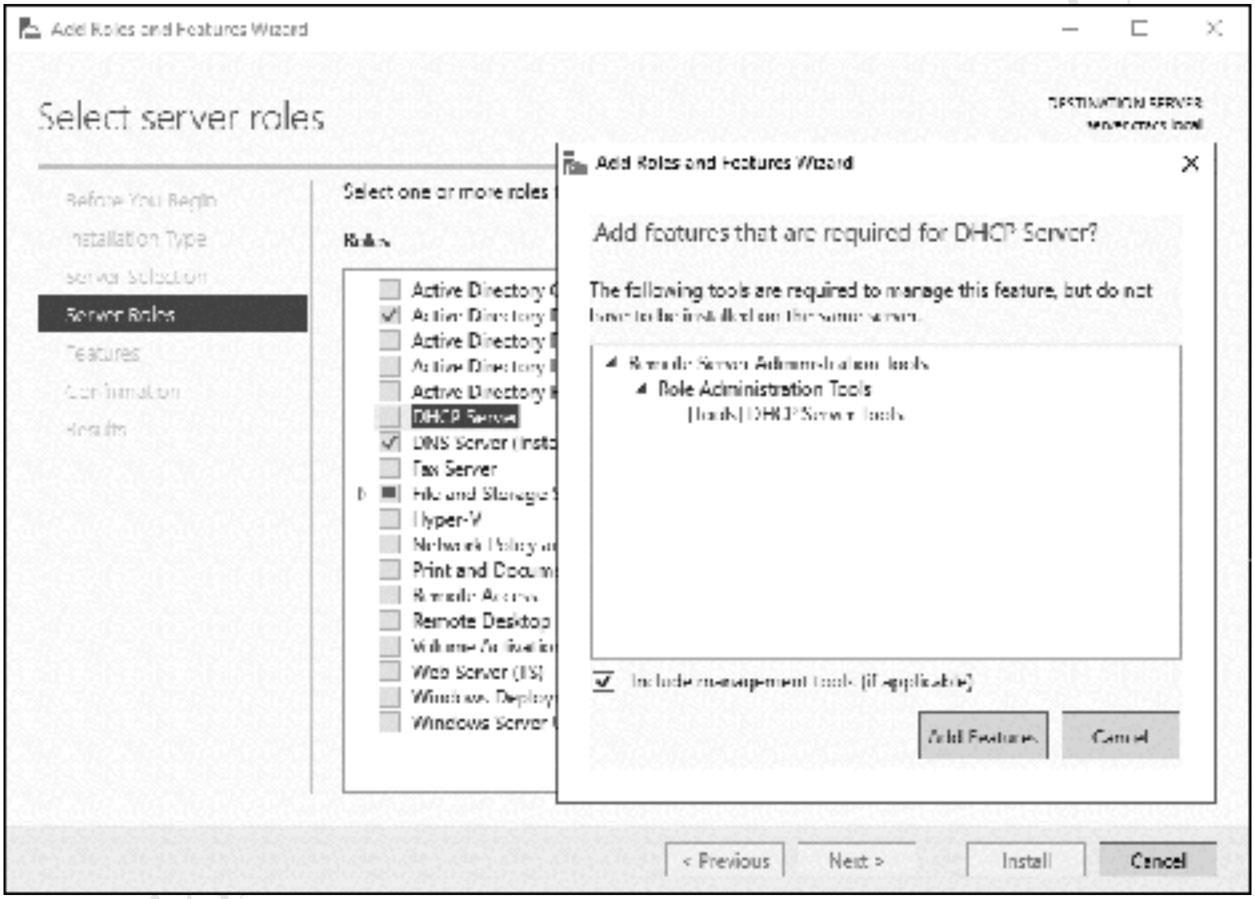
Nevertheless, a Chromebook can be used in several different ways:

- A Chromebook can be used to remotely administer the server (see section 10.5 Headless Operation/Remote Desktop) for general information on this topic). To do so requires RDP client software; there are several examples 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.

12.8 Installing DHCP

If the server is being installed in a small business environment, then it is possibly the case that there is an all-in-one router providing the DHCP service. However, if this is not the case then it will be necessary to install DHCP on the server itself, described below.

Go into the Server Manager and 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 (we are assuming there is only one) 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.



Add Roles and Features Wizard

Add features that are required for DHCP Server?

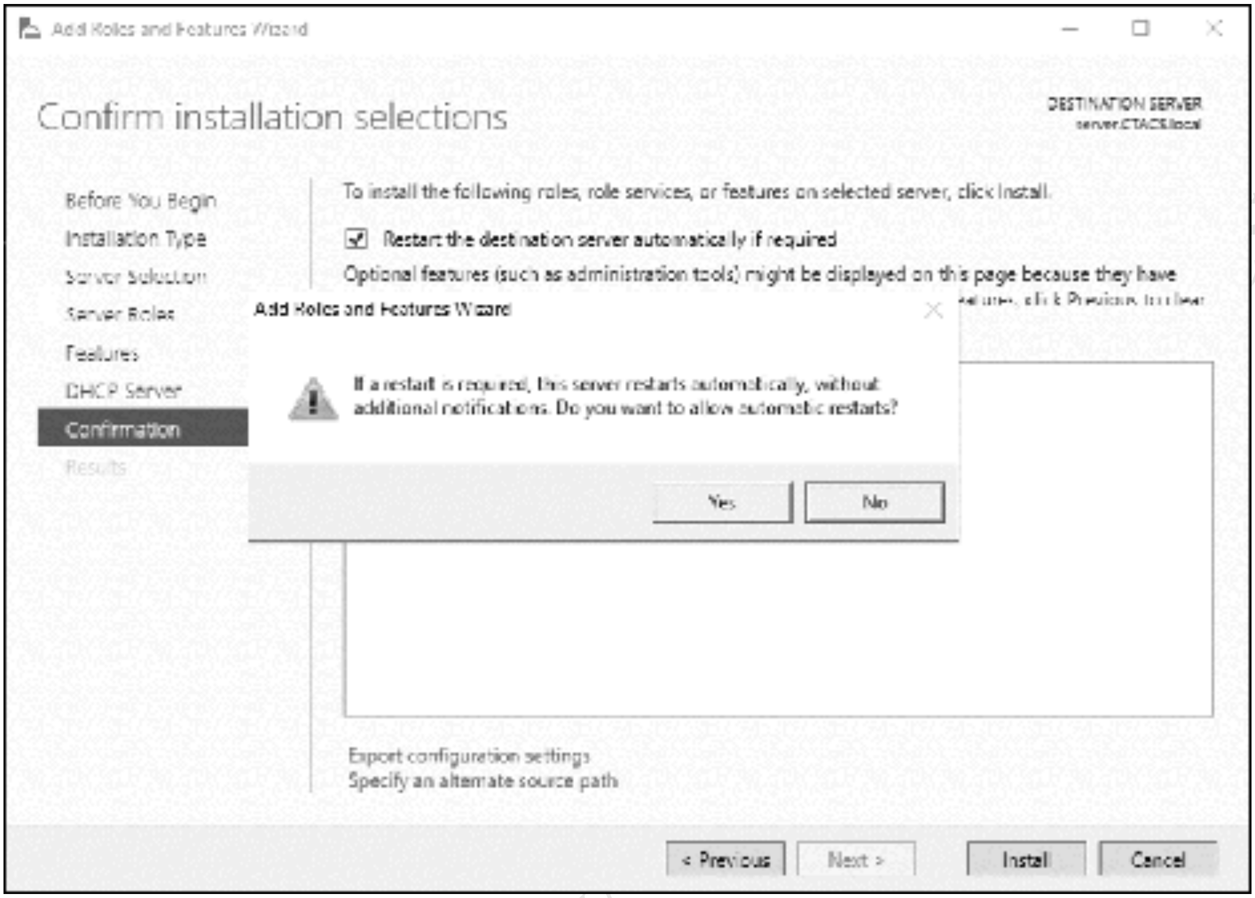
The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] DHCP Server Tools

☑ Include management tools (if applicable)

Figure 177: 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:



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
server.CTACS.local

To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have ... features, click Previous to clear

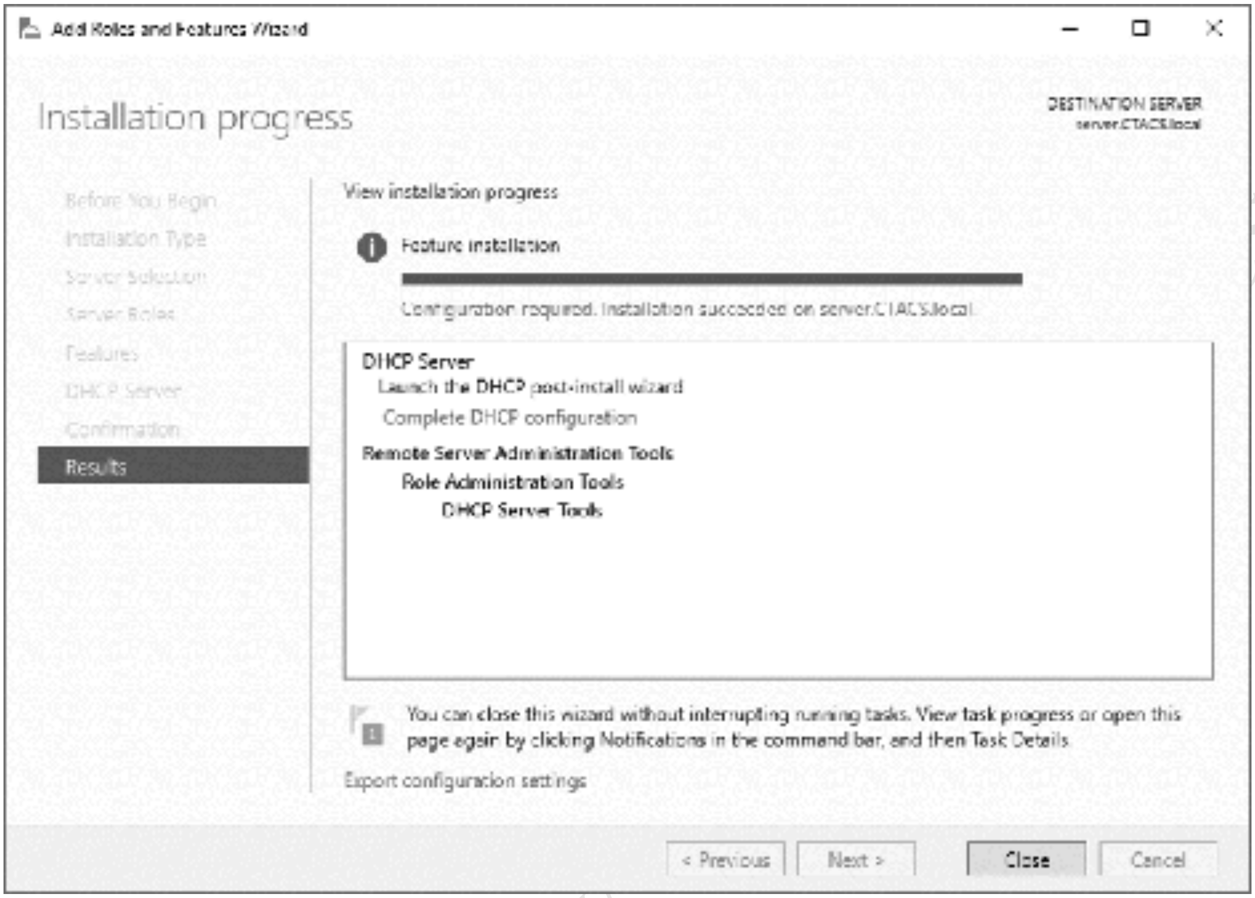
Add Roles and Features Wizard

If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?

Export configuration settings
Specify an alternate source path

Figure 178: 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**:



Installation progress

DESTINATION SERVER
server.CTACS.local

View installation progress

Feature installation

Configuration required. Installation succeeded on server.CTACS.local.

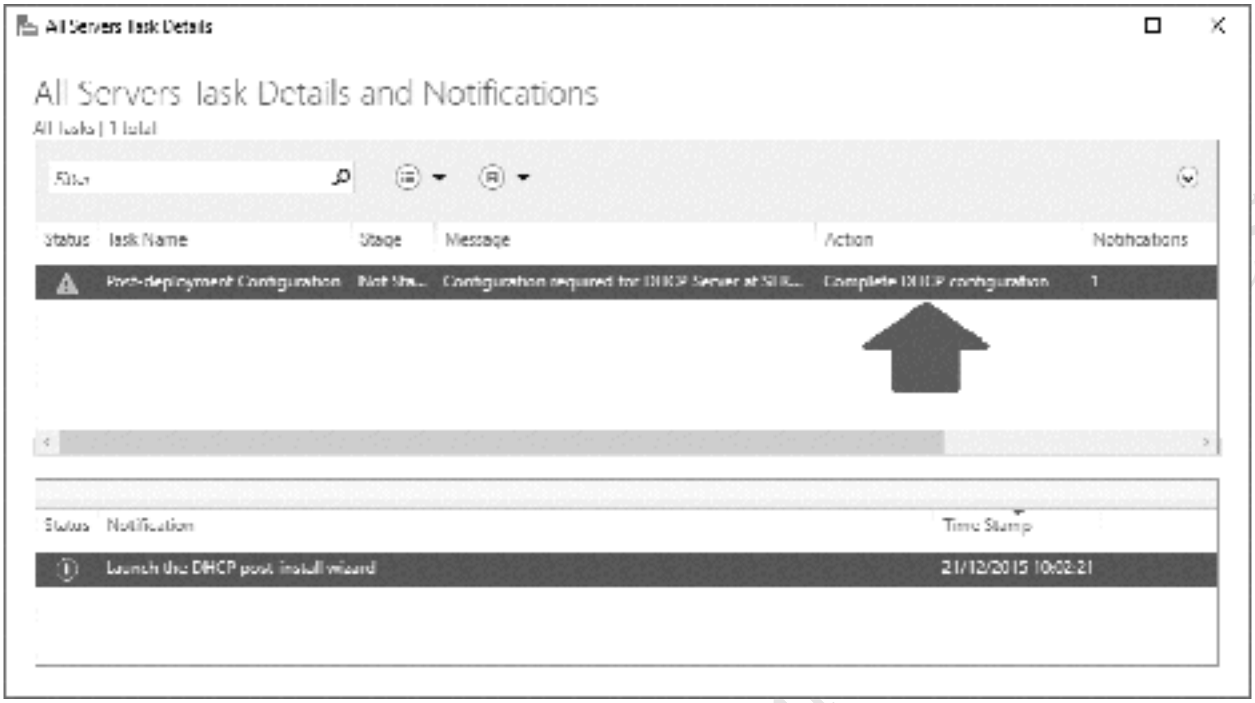
DHCP Server
  Launch the DHCP post-install wizard
  Complete DHCP configuration
Remote Server Administration Tools
  Role Administration Tools
    DHCP Server Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Figure 179: Installation progress screen

Restart the server at this point. When the server comes back up, run Server Manager again. There will now be an entry for DHCP in the left-hand panel – click it. At the top of the screen is a warning message that reads ‘Configuration required for DHCP Server’ - click where it says **More…** to display the following panel. Click **Complete DHCP configuration**:



All Servers Task Details

All Servers Task Details and Notifications

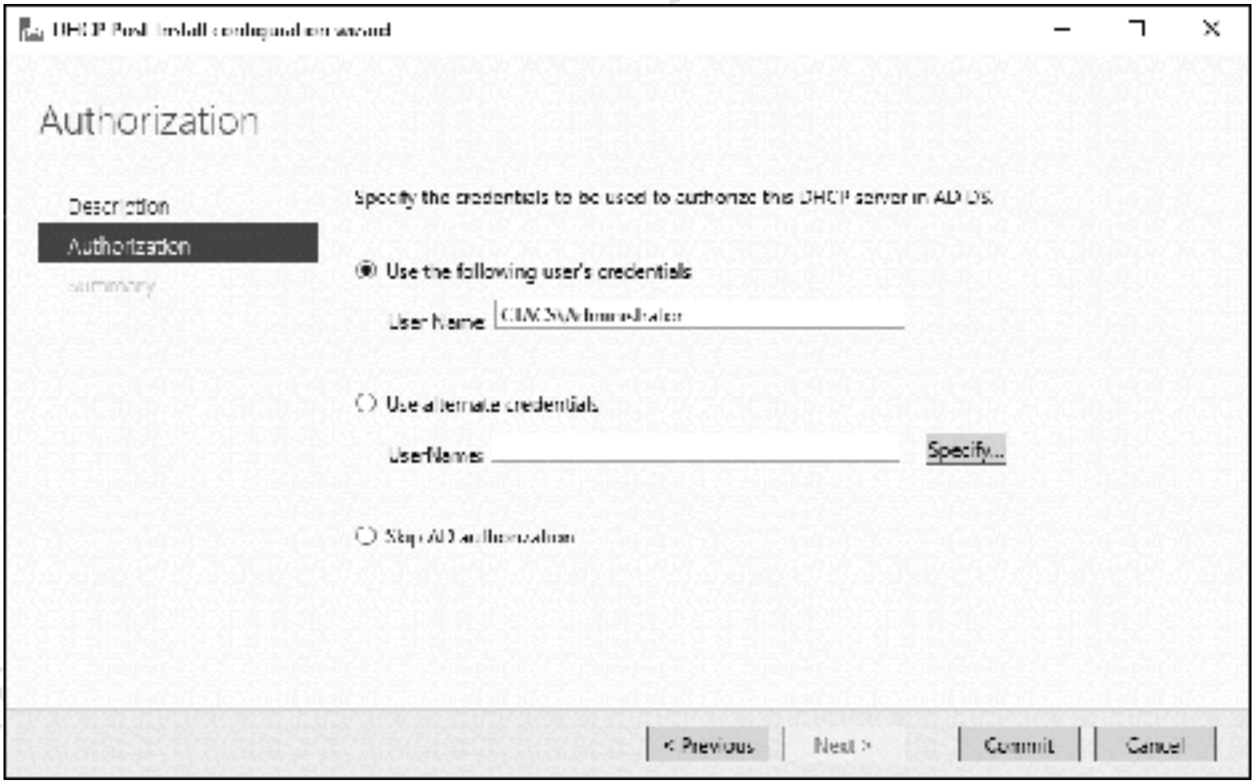
All Tasks | 1 Total

Status	Task Name	Stage	Message	Action	Notifications
⚠	Post-deployment Configuration	Not Sta...	Configuration required for DHCP Server at SER...	Complete DHCP configuration	1

Status	Notification	Time Stamp
ⓘ	Launch the DHCP post-install wizard	21/12/2015 10:02:21

Figure 180: Message about further configuration

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



DHCP Post-Install configuration wizard

Authorization

Specify the credentials to be used to authorize this DHCP server in AD DS.

● Use the following user's credentials

User Name CIMCS\Administrator

○ Use alternate credentials

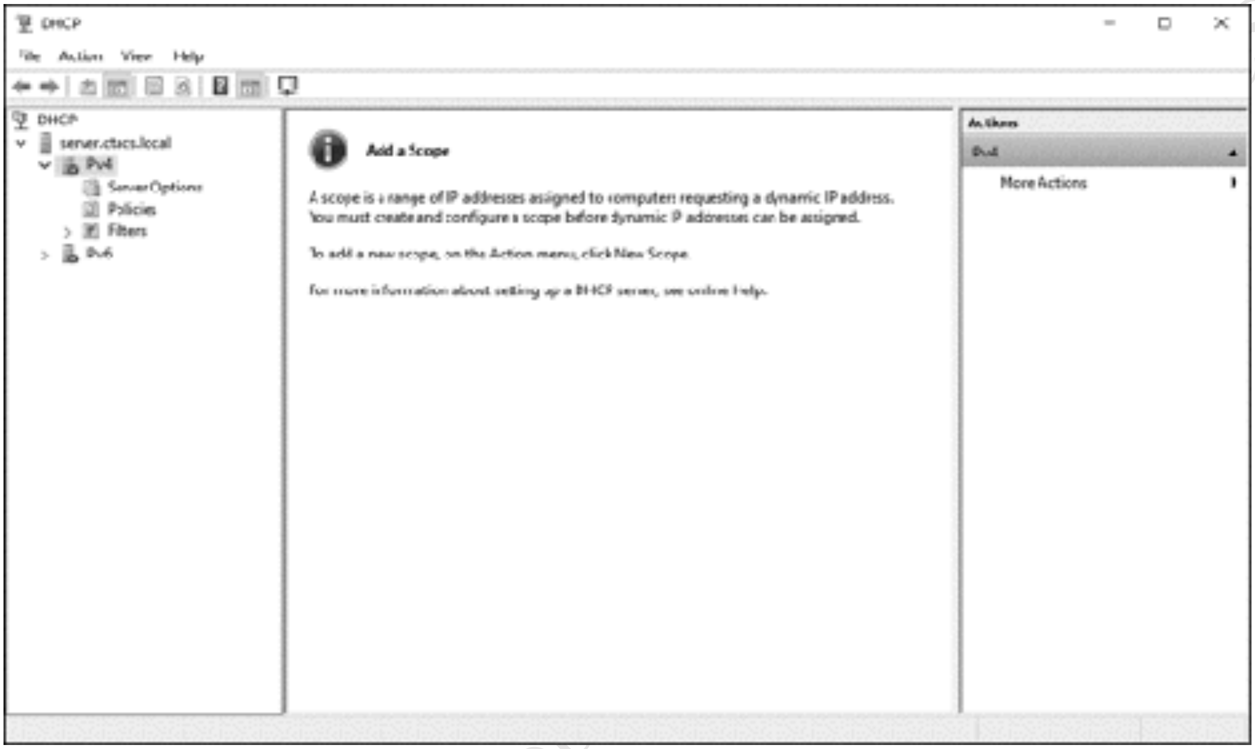
UserName ______ Specify...

○ Skip AD authorization

Figure 181: Post-Install configuration wizard

The existing user credentials (*"Administrator"*) are fine so just click the **Commit** button. After a few seconds a Summary panel will be shown. Click **Close** and you will be returned to the *All Servers Task Details and Notifications panel*, which you can close.

It is now necessary to configure the IP scope. Still within Server Manager, click **Tools** followed by **DHCP**. Expand the tree down the left-hand side so it appears as follows:



Add a Scope

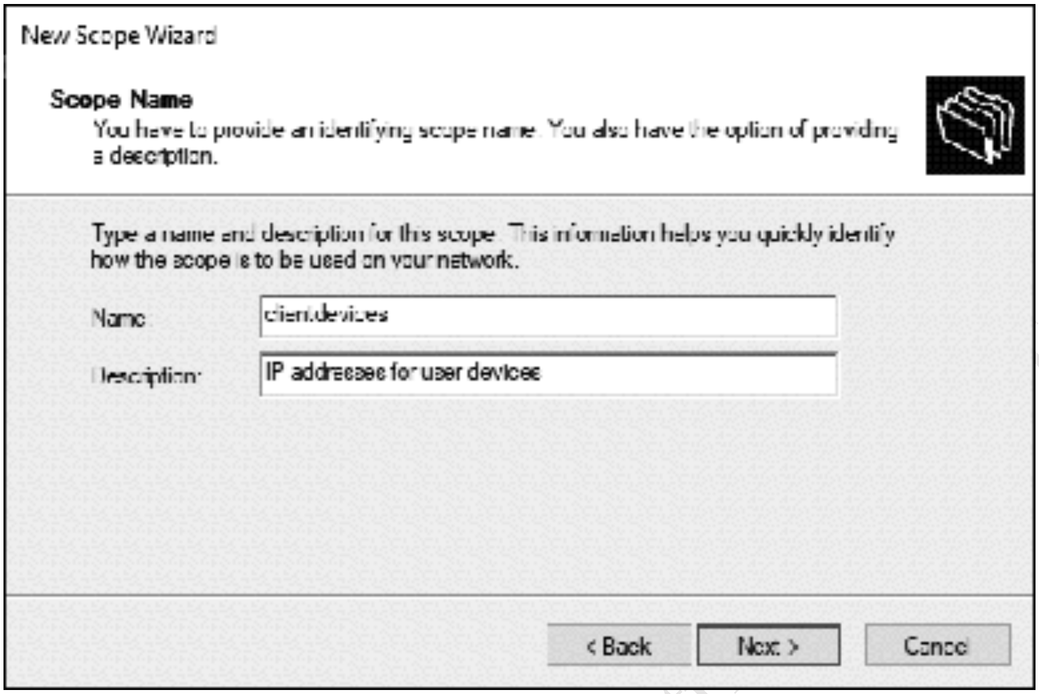
A scope is a range of IP addresses assigned to computers requesting a dynamic IP address. You must create and configure a scope before dynamic IP addresses can be assigned.

To add a new scope, on the Action menu, click New Scope.

For more information about setting up a DHCP server, see online Help.

Figure 182: Configure DHCP Server

Right-click on the entry for **IPv4** and choose **New Scope** to start the *New Scope Wizard*. Click **Next** and the following panel is displayed. Give it a suitable name e.g. *clientdevices* and an optional description, then click the **Next** button:


New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.

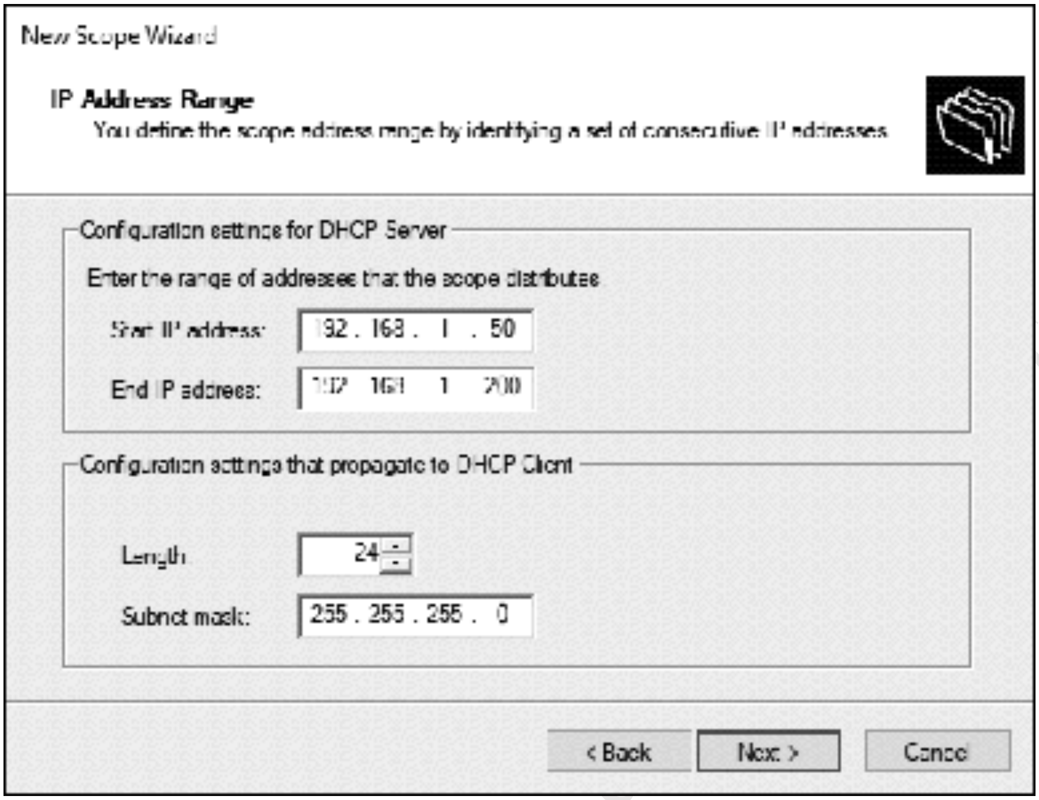
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: client.devices

Description: IP addresses for user devices

Figure 183: New Scope Wizard

On the subsequent screen enter the addresses as outlined in the earlier section *IP Considerations*. In this example, our server is on 192.168.1.2 and the scope for the workstations will be 192.168.1.50 to 192.168.1.200. Set the Length to 24 and the Subnet mask will automatically adjust to 255.255.255.0. Then click **Next**:



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 1 . 50

End IP address: 192 . 168 . 1 . 200

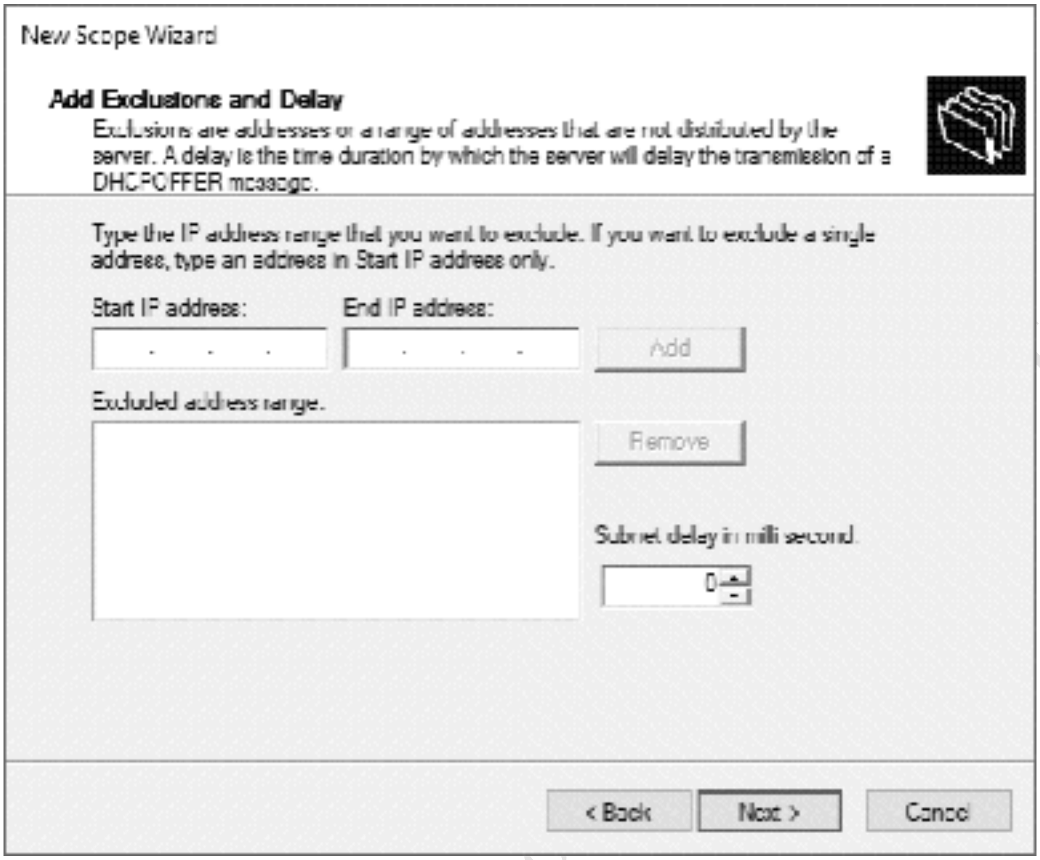
Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

Figure 184: IP address range for DHCP server

The next panel allows you to specify any exclusions (that is, gaps) in the IP scope. Unless you have very specific requirements just click **Next**.



New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCPOFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: . . .

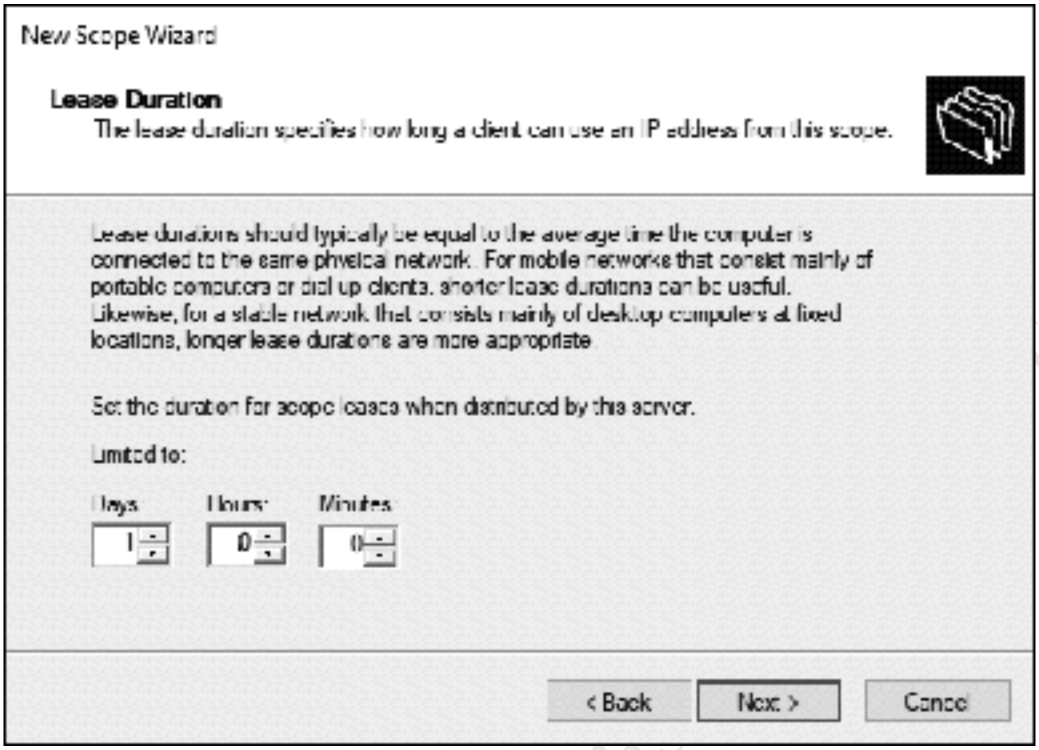
End IP address: . . .

Excluded address range:

Subnet delay in milli second: 0

Figure 185: Add Exclusions and Delay

The subsequent screen is for specifying how long a lease will last. The default value of 8 days is not a great choice, so reduce it to a single day and click **Next**.


New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

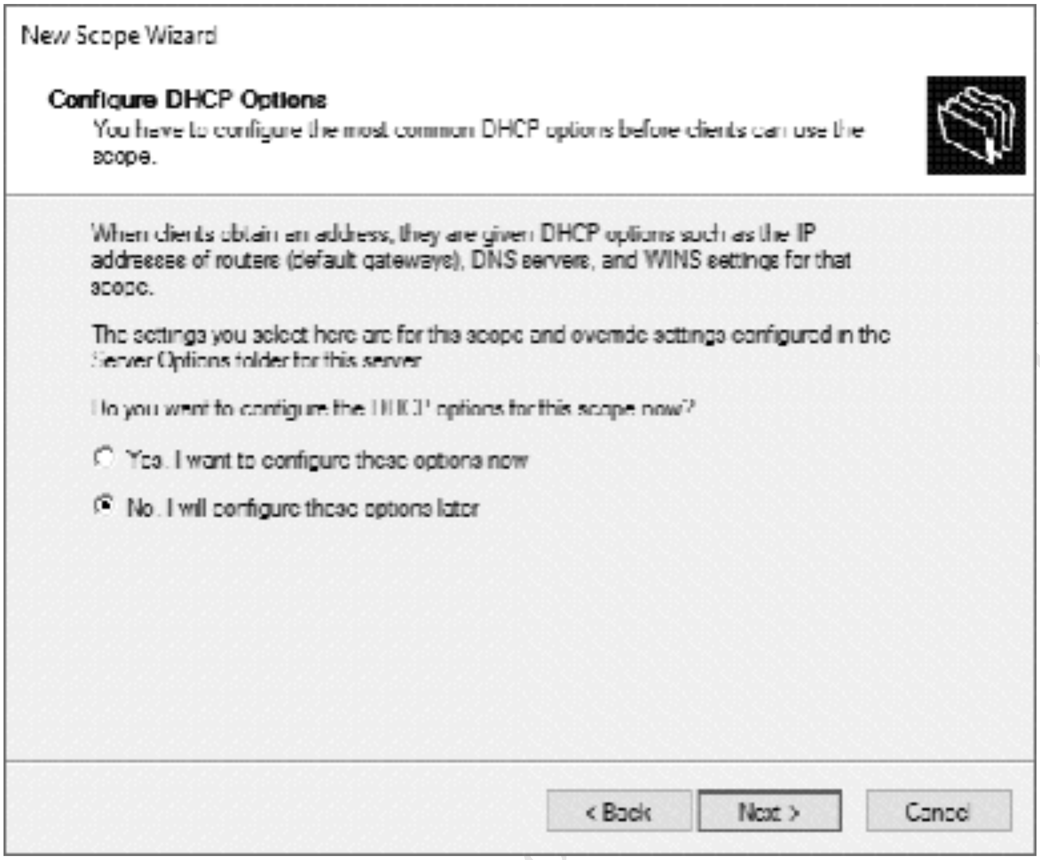
Set the duration for scope leases when distributed by this server.

Limited to:

Days: 1 Hours: 0 Minutes: 0

Figure 186: Specify Lease Duration

The following screen is concerned with more sophisticated options. They are of no great importance in a small network so choose **No, I will configure these options later** and click **Next**.


New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

○ Yes, I want to configure these options now

● No, I will configure these options later

Figure 187: Configure more advanced DHCP options

Upon completion (which is a matter of seconds) a confirmation screen is shown. Click **Finish**. The scope must now 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, 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. It is suggested that you restart the server at this point.

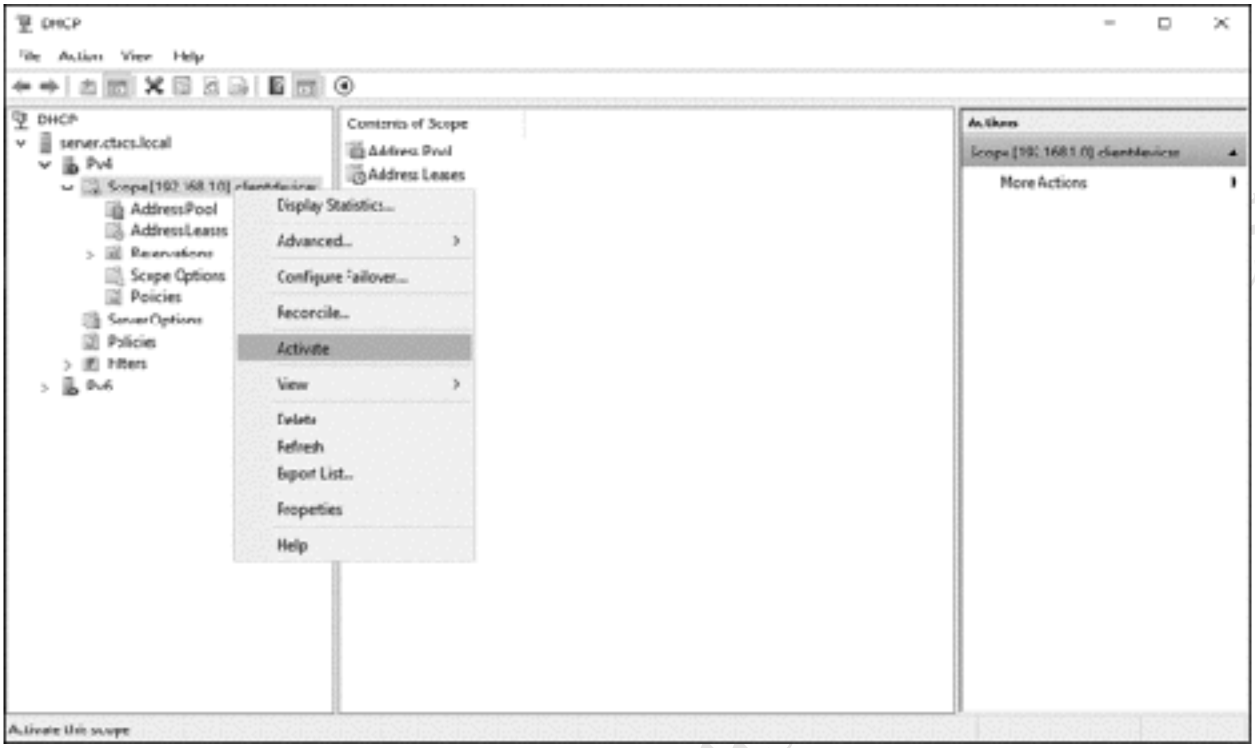


Figure 188: DHCP after configuration

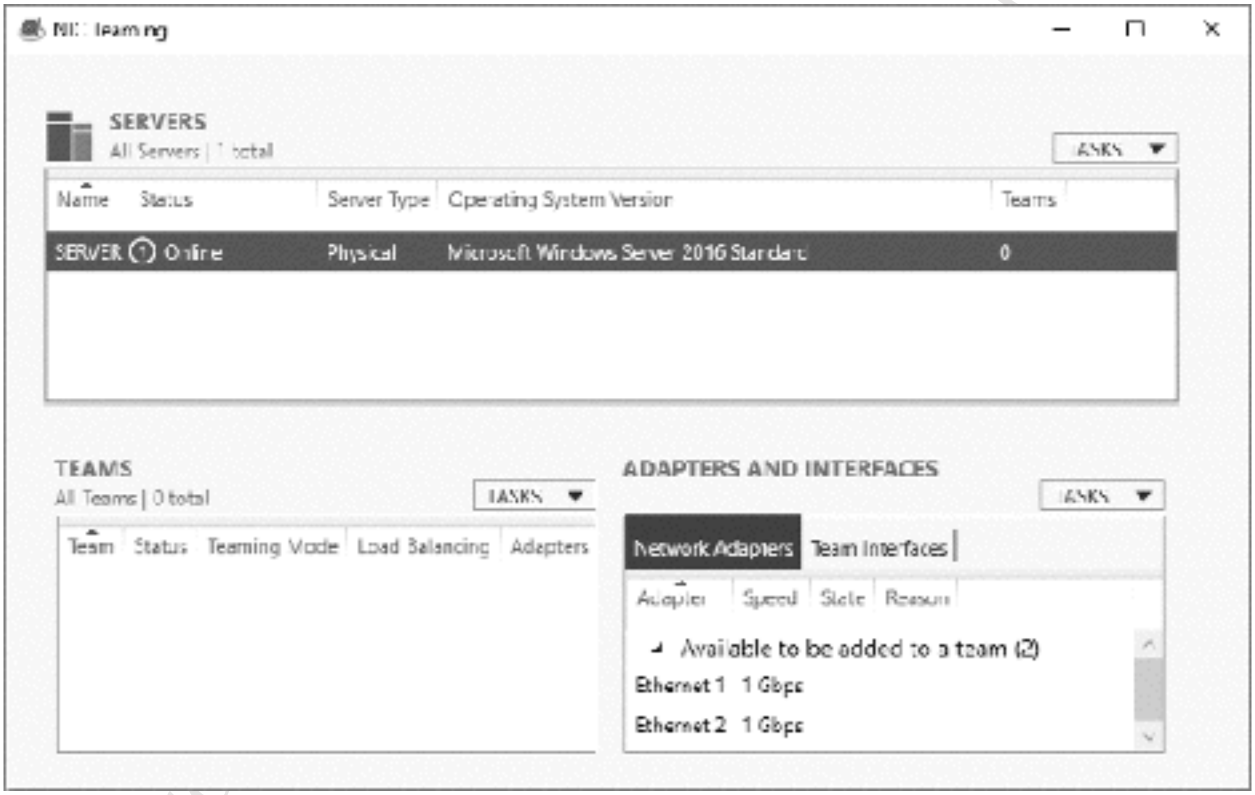
Supplementary note: if you have experience of DHCP then you may appreciate that this is a relatively simple configuration, suitable for use in a small network, and that it is possible to do a lot more with DHCP. Also, we have stuck to IPv4 although IPv6 can be used in addition or in place of it.

12.9 Multiple Network Adapters (NIC Teaming)

A file server can and ideally should have more than one network (Ethernet) adapter; multiple adapters can be used together in different ways to improve resilience and/or performance using a technique known as *Teaming* or *NIC Teaming* (NIC is short for *Network Interface Card*).

The main network card represents a single point of failure – if it is lost then the server is out of action as nobody can access it. Ethernet adapters can fail, as can the ports on the switch that they are connected to, or the cable may accidentally be pulled out. In this example, a second Ethernet adapter has been installed in the server to improve network resilience; if the first or main adapter fails, it will take over automatically, such that service continues without interruption. Important: before progressing, make a note of the settings of the first adapter, which was given a fixed IP address in section 2. BASIC INSTALLATION AND CONFIGURATION, as it may be necessary to re-enter them later on.

On the server, launch *Server Manager* and click on **Local Server**. In the Properties panel locate the *NIC Teaming* entry. Click where it reads **Disabled** and the following panel is shown:



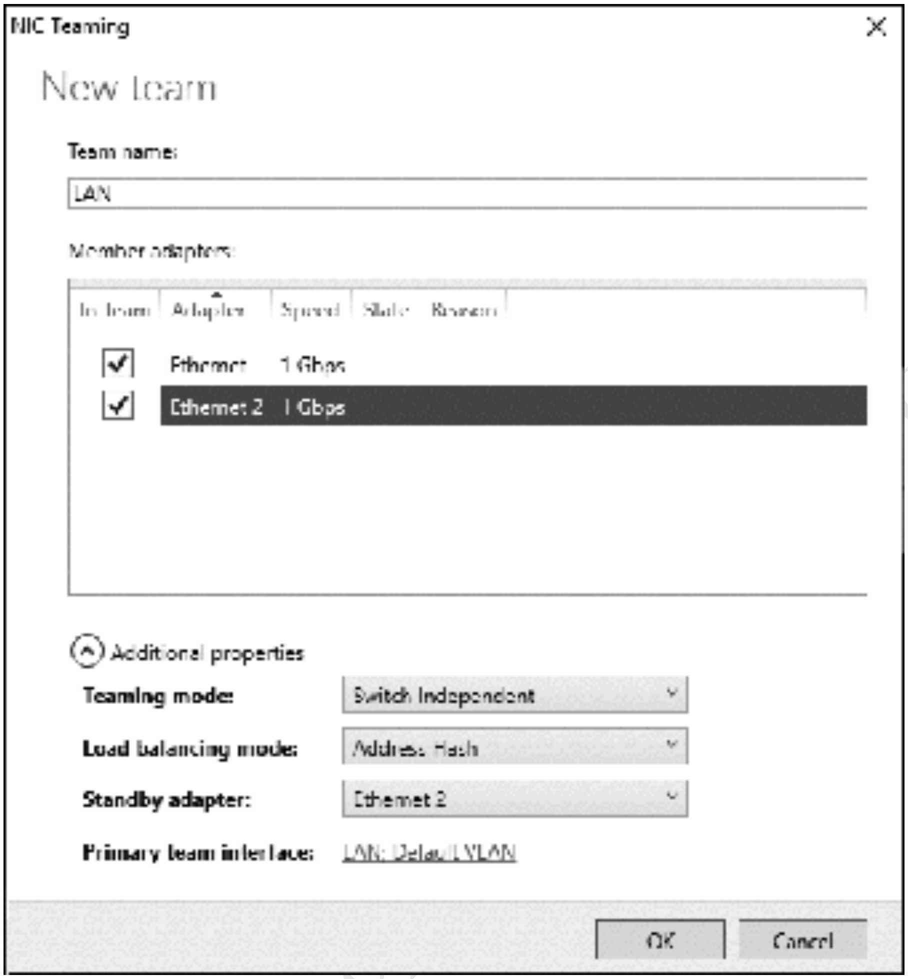
Name	Status	Server Type	Operating System Version	Teams
SERVER	Online	Physical	Microsoft Windows Server 2016 Standard	0

Team	Status	Teaming Mode	Load Balancing	Adapters

Adapter	Speed	State	Reason
Available to be added to a team (2)			
Ethernet 1	1 Gbps		
Ethernet 2	1 Gbps		

Figure 189: NIC Teaming screen

In the Teams section, click the **TASKS** drop-down and choose **New Team**. On the resultant panel, specify a *Team name* (e.g. *LAN*) and tick the boxes for the network adapters. If you were to just click **OK** at this point, then by default the adapters will be bonded together to double network throughput. However, we need to click **Additional properties** to change the settings: **Teaming mode** should be **Switch Independent**; **Load balancing mode** should be **Address Hash**; **Standby adapter** should be **Ethernet 2** (or whatever your second adapter is called). Click **OK**.



NIC Teaming

New team

Team name: LAN

Member adapters:

In Team	Adapter	Speed	State	Reason
☑	Ethernet	1 Gbps		
☑	Ethernet 2	1 Gbps		

Additional properties

Teaming mode: Switch Independent

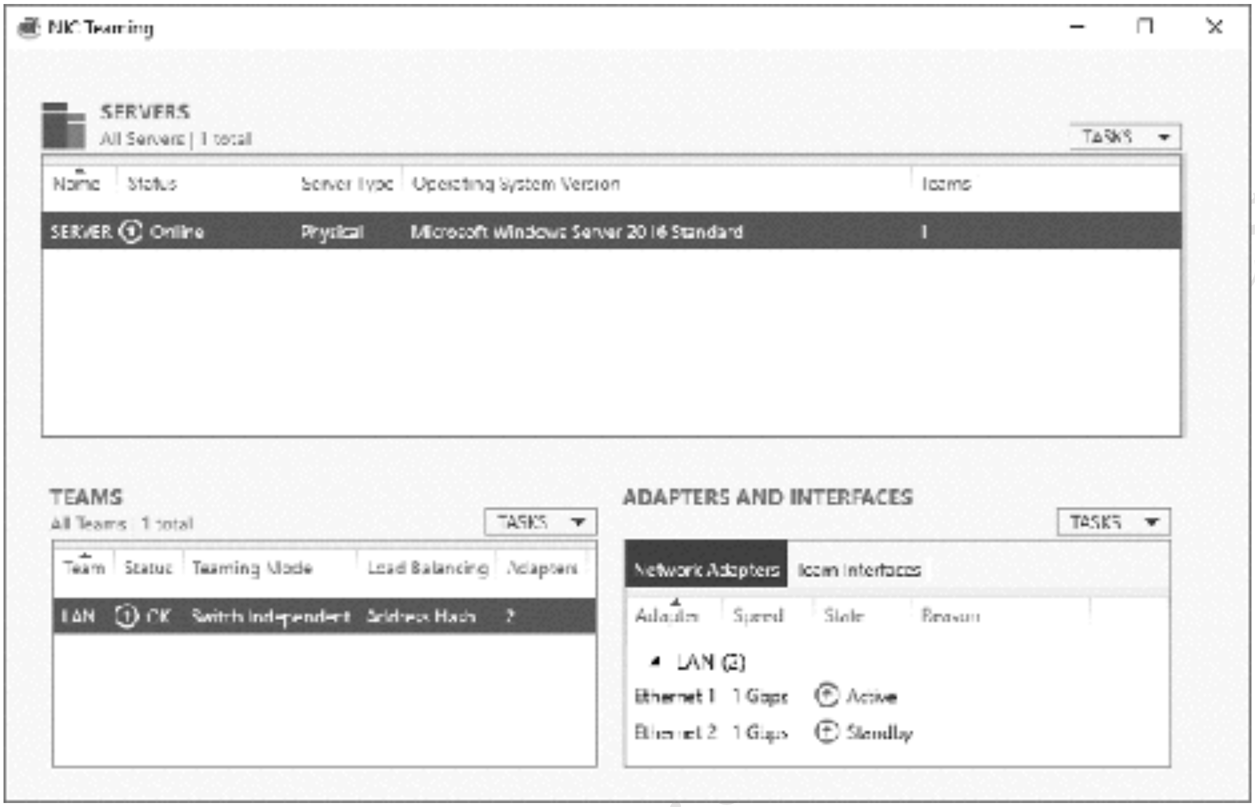
Load balancing mode: Address Hash

Standby adapter: Ethernet 2

Primary team interface: LAN: Default VLAN

Figure 190: 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 matters have settled down, it should appear along the following lines:



NIC Teaming

SERVERS
All Servers | 1 total

Name	Status	Server Type	Operating System Version	Teams
SERVER	Online	Physical	Microsoft Windows Server 2016 Standard	1

TEAMS
All Teams | 1 total

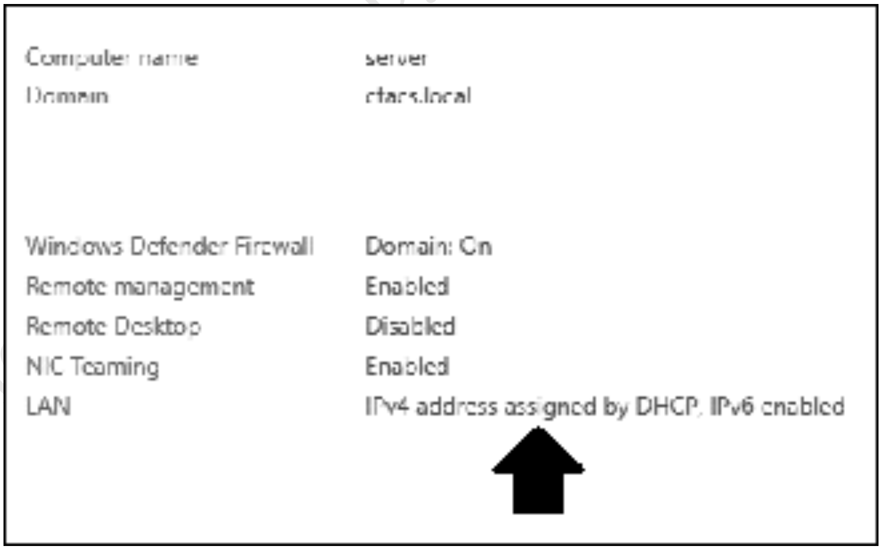
Team	Status	Teaming Mode	Load Balancing	Adapters
LAN	OK	Switch Independent	Address Hash	2

ADAPTERS AND INTERFACES

Adapter	Speed	State	Reason
LAN (2)			
Ethernet 1	1 Gbps	Active	
Ethernet 2	1 Gbps	Standby	

Figure 191: NIC Teaming status

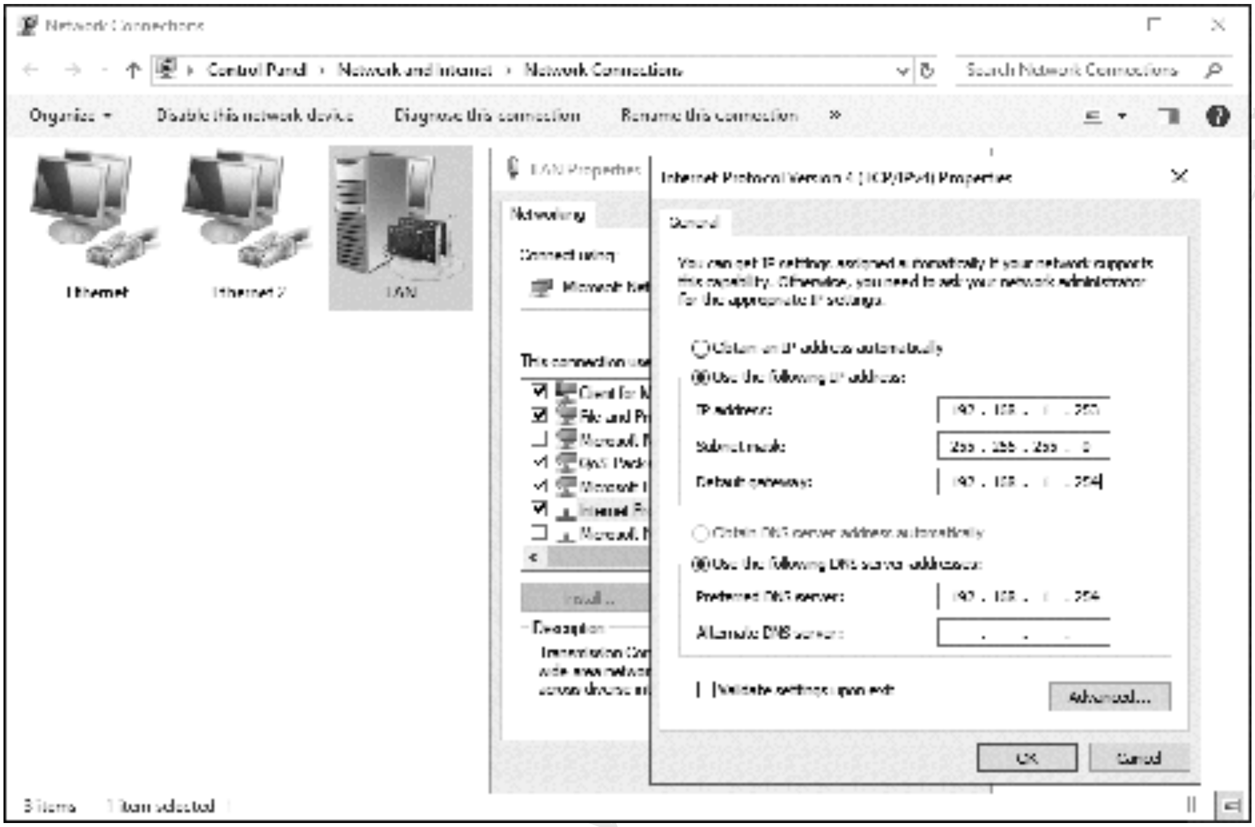
Returning to the Local Server Properties screen within Server Manager – you may need to refresh it - there should now be an entry underneath NIC Teaming for *LAN* (or whatever you called the Team):



Computer name	server
Domain	ctacs.local
Windows Defender Firewall	Domain: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Enabled
LAN	IPv4 address assigned by DHCP, IPv6 enabled

Figure 192: LAN entry in Server Properties

What have just done has implications for the IP address of the server and so we now need to fix matters. Click on the blue writing to the right of *LAN* and it will display the Network Connections. Right-click the entry for the team (*LAN* in our example) and choose **Properties**. Highlight **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. Change the entries to be the same as the original single adapter was before beginning this exercise. Again, there may be an interruption to the connectivity whilst this takes effect.


Network Connections

Control Panel › Network and Internet › Network Connections

Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 250

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 254

Alternate DNS server: . . .

☐ Validate settings upon exit

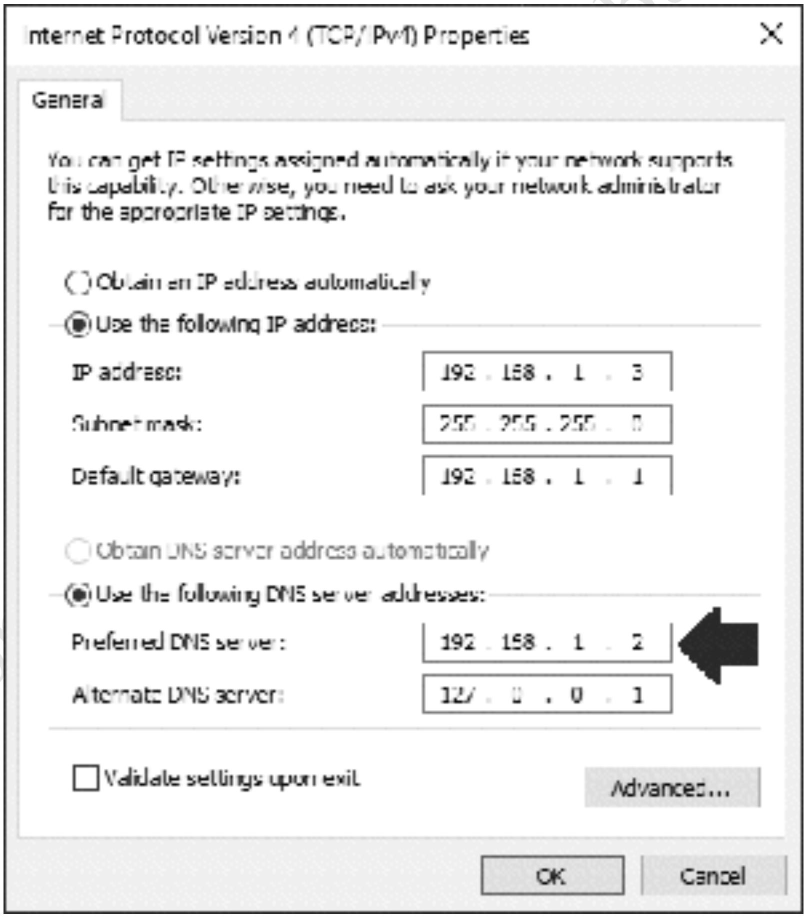
Figure 193: Network Connections

It should now be tested. Remove the network cable from the first Ethernet adapter; the second one should take over automatically and the server still be accessible.

12.10 Adding an Additional Server

In a small organization, there is typically just one server. However, in a larger organization there may be multiple servers, providing different roles and capacity. Critical to the operation of the entire network is the Domain Controller running Active Directory, which defines every server, computer, user and so on in the system. If the Domain Controller is unavailable for any reason, for instance, hardware problems or it has crashed, then everything comes to a halt. To avoid this possibility, it is standard practice to have one or more additional domain controllers which can take over and/or share the workload in a larger network. In this example, we will add another server to fulfil this role (and having done so, you can then add further roles to that server if required).

In this example, we will refer to the original server as *server1* and the additional one as *server2*. Using the instructions in section 2. BASIC INSTALLATION AND CONFIGURATION, install Windows Server on the second server and add the Active Directory role, to the point where it is ready to be promoted to be a domain controller. Then, change the settings of the network adapter, giving it a static IP address in accordance with your IP scheme. For instance, if *server1* is on 192.168.1.2 then you might choose to make *server2* 192.168.1.3. The *Preferred DNS server* should be changed to explicitly point to the first server – this is very important (the alternate can be set to the loopback adapter, 127.0.0.1). Make sure the two servers can 'see' each other, for instance by use of the PING command.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 3
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

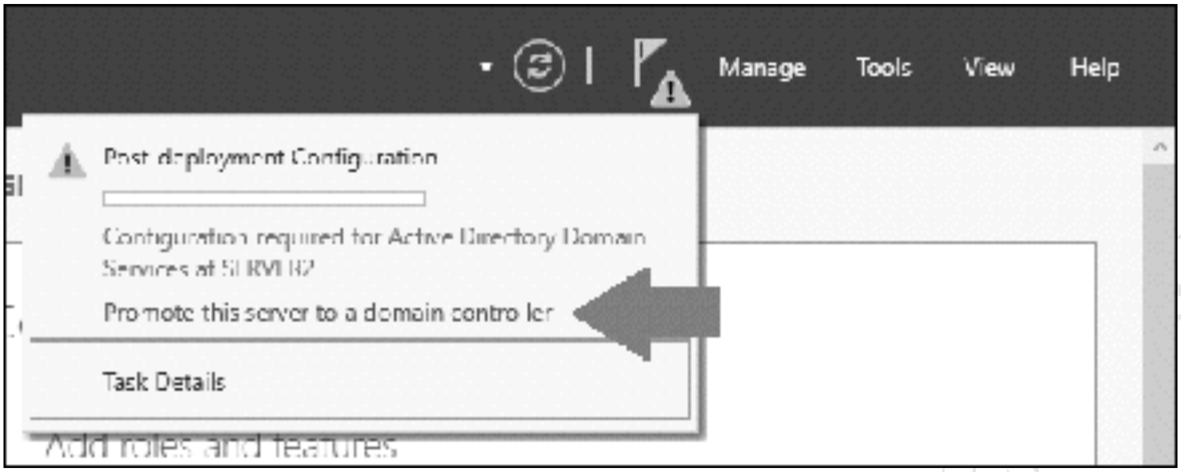
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 2
Alternate DNS server: 127 . 0 . 0 . 1

□ Validate settings upon exit

Figure 194: Set Preferred DNS to IP address of the first server

The second server should now be promoted by clicking on the message that appears at the top of Server Manager:



Post-deployment Configuration

Configuration required for Active Directory Domain Services at SERVER2

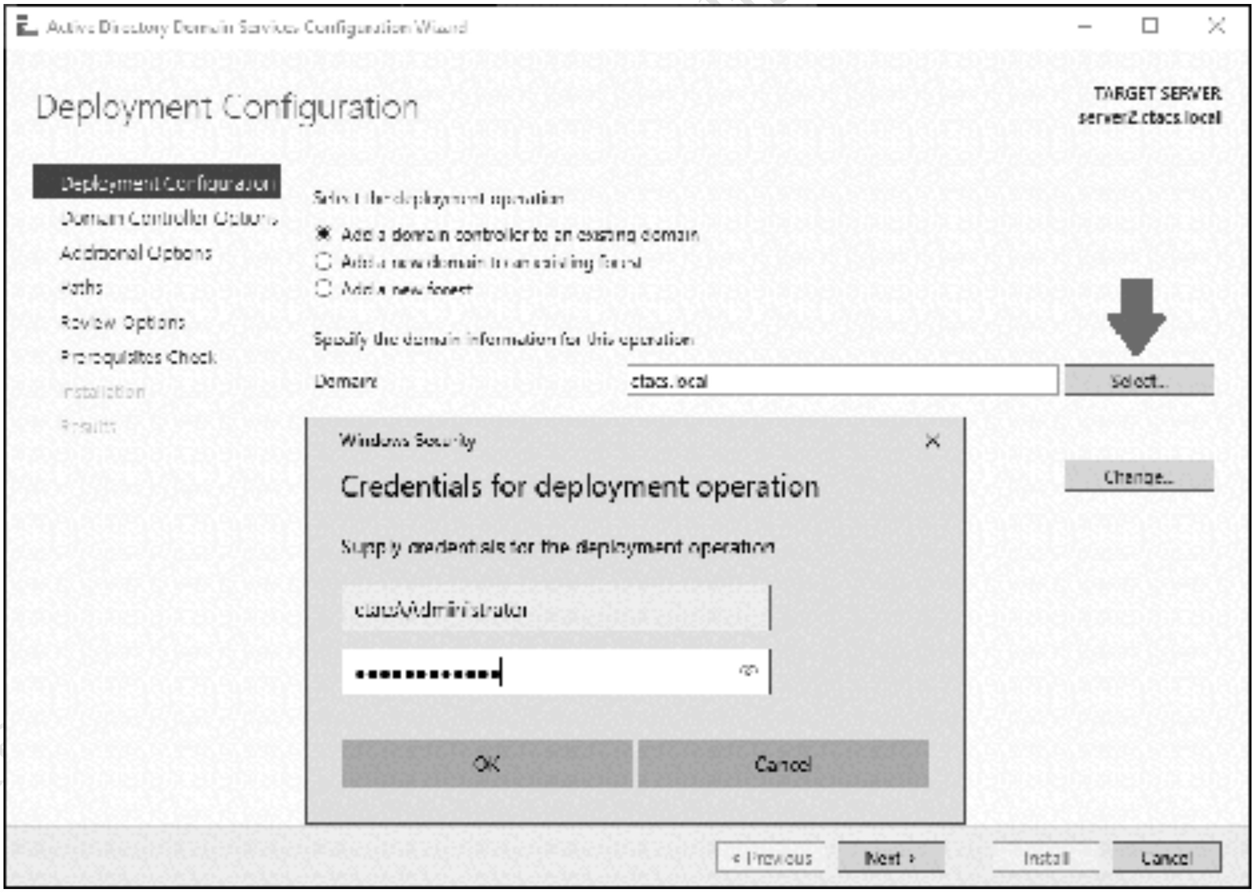
Promote this server to a domain controller

Task Details

Add roles and features

Figure 195: Promote the second server

The *Active Directory Domain Services Configuration Wizard* runs. On the *Deployment Configuration* screen choose **Add a domain controller to an existing domain**. Click the **Select** button to search for the domain – if it cannot find it, this will almost certainly be due to a DNS error, so check the DNS settings on both servers. You need to supply credentials to affect the change, so click the **Change** button and enter the Administrator account details for this server; it is not apparent, but this should be in the format *domain_name\username* e.g. *ctacs\administrator*. Then click **Next** to proceed:



TARGET SERVER
server2.ctacs.local

Select the deployment operation

● Add a domain controller to an existing domain
○ Add a new domain to an existing forest
○ Add a new forest

Specify the domain information for this operation

Domain: ctacs.local

Credentials for deployment operation

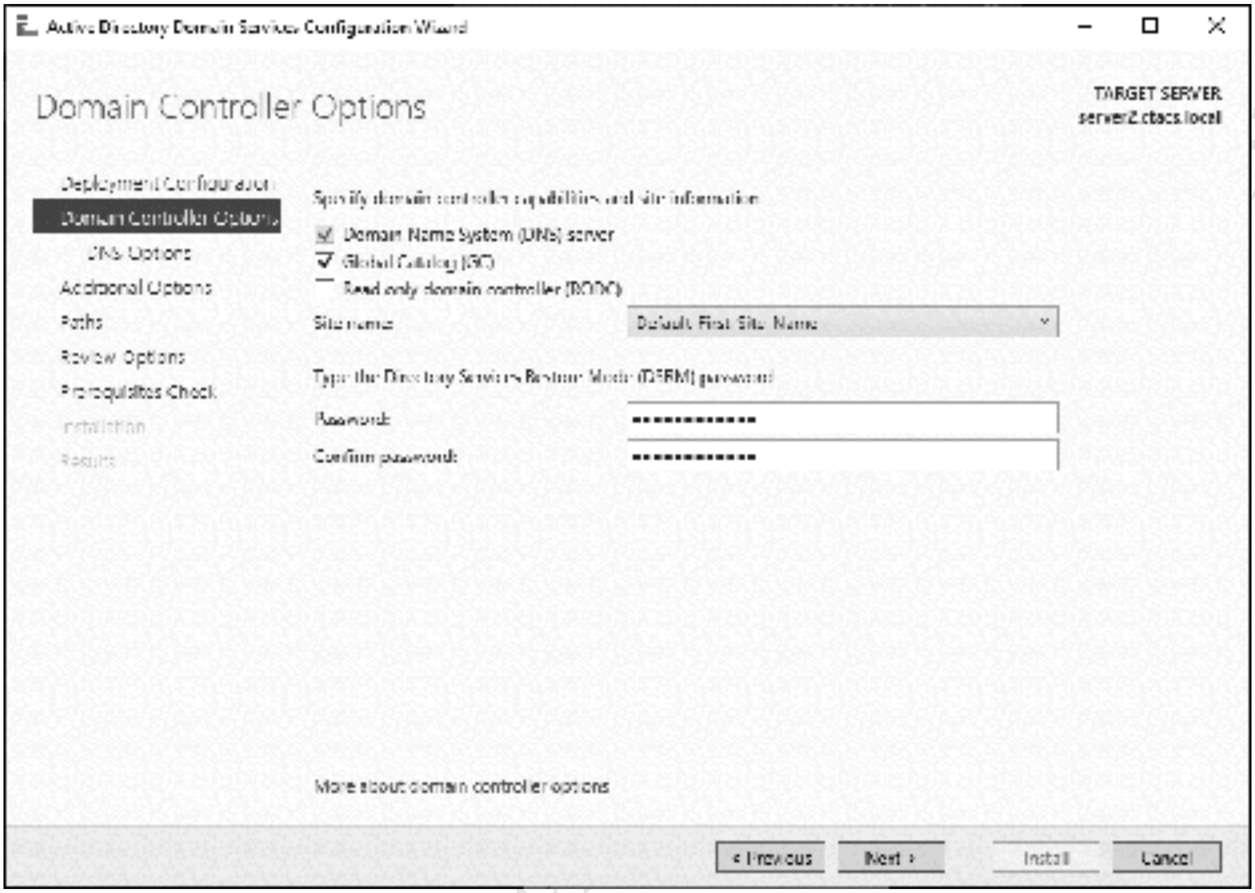
Supply credentials for the deployment operation

ctacs\Administrator

•••••••••••••

Figure 196: Choose the deployment option

On the second screen, specify the *Directory Services Restore Mode (DSRM)* password. For convenience, you may wish to use the same password as the Administrator account. Click **Next**:



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
server2.ctacs.local

- Deployment Configuration
- Domain Controller Options
- DNS Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Specify domain controller capabilities and site information

☑ Domain Name System (DNS) server
☑ Global Catalog (GC)
□ Read only domain controller (RODC)

Site name: Default-First-Site-Name

Type the Directory Services Restore Mode (DSRM) password

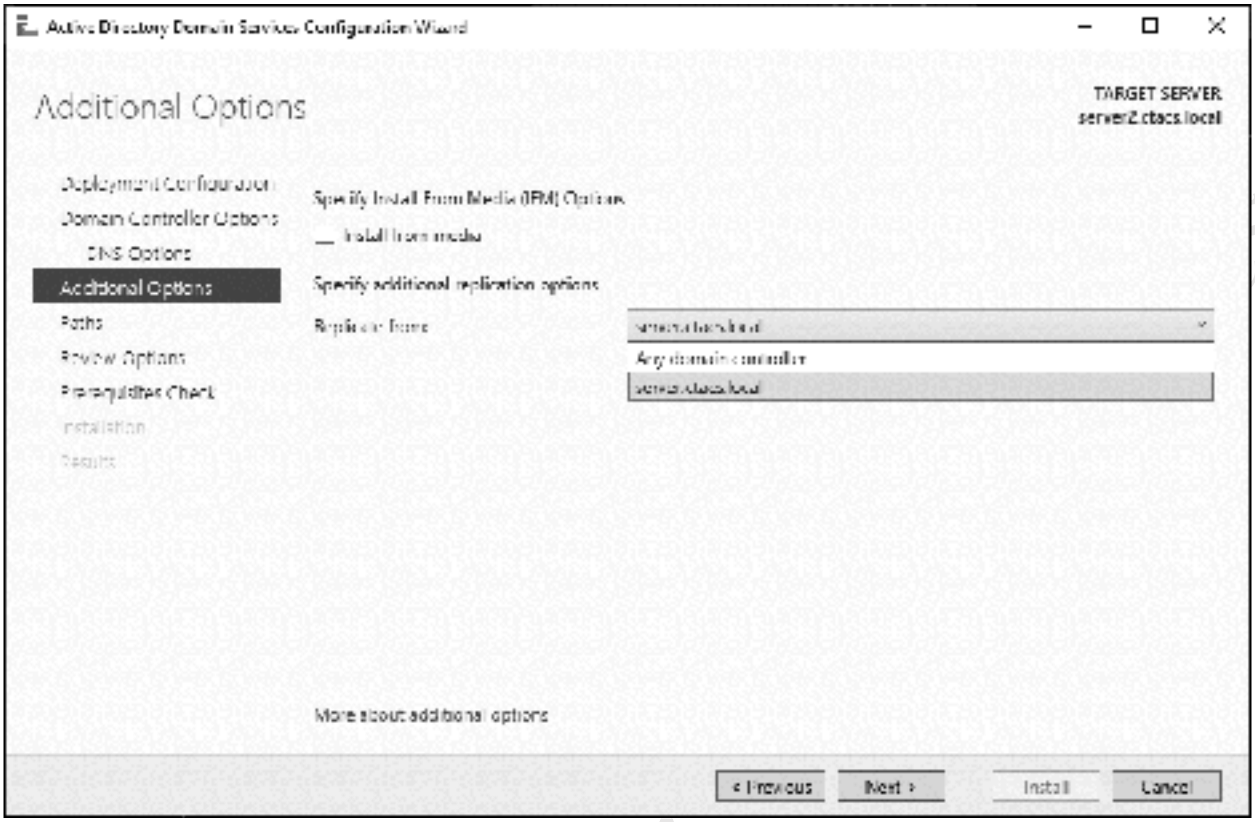
Password: •••••••••••••
Confirm password: ••••••••••••

More about domain controller options

Figure 197: Domain Controller options

You may receive a message that states '*A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found…*', particularly if you are working in an environment where DNS is being provided by an all-in-one router. For now, ignore it by clicking **Next**.

On the subsequent screen, there may be an error message relating to *adprep*. To get through this, use the *Replicate from* drop-down field and change the value from *Any domain controller* to the full name of the first server. Click **Next**:



Additional Options

Specify Install From Media (IFM) Options

__ Install from media

Specify additional replication options

Replicate from: server1.ctacs.local

Any domain controller
server1.ctacs.local

Figure 198: Specify the first server for replication

The next screen is for specifying the location of the database and log files associated with Active Directory; usually you will just click **Next**. There will then be a screen to review the options – click **Next** to continue. The wizard will run a pre-requisites check; there may be some warning messages but if the *'All prerequisite checks passed successfully'* message is displayed, you can click **Install** to being the installation proper. Installation will take a minute or so, after which the server will restart.

To prove that things are working, go back to the original server and create a new user using the Active Directory Administrative Center (as described in section 4.2 Creating Users). Wait a few minutes, go the second, newly added server, and launch the Active Directory Administrative Center on it – the newly created user should be listed, proving that the servers are synchronizing.

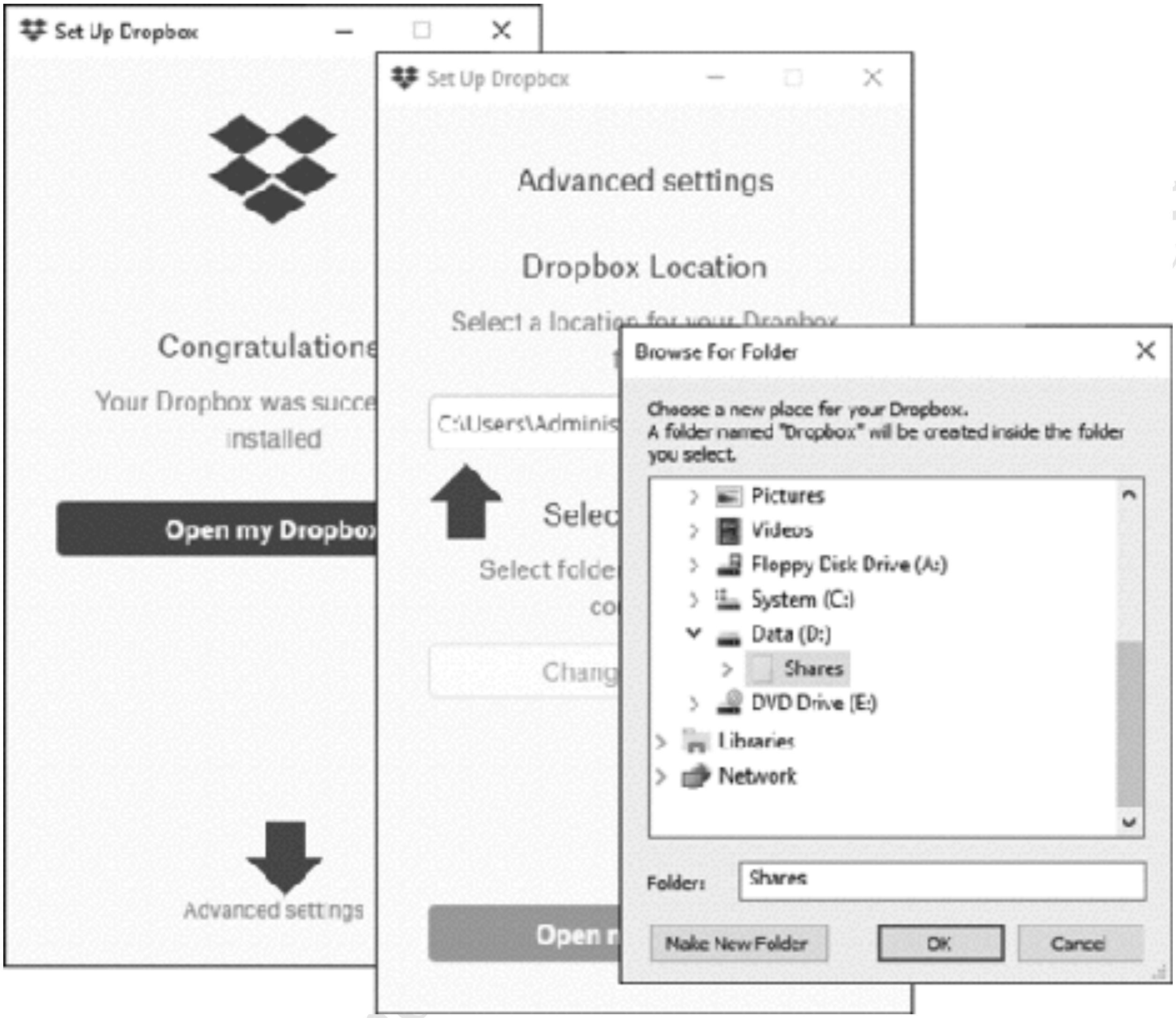
12.11 Using Dropbox with Windows Server

Windows Server has several features to enable remote working, although they can be difficult to configure and operate. However, a simple and popular method that can complement these and provide additional capabilities is to use a Cloud-based file sync service such as *Dropbox*, which 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 have a similar offering in the form of *OneDrive* and Google has Google Drive, but in practice Dropbox seems to work a lot better.

There are five main considerations when using Dropbox with Windows Server:

1. A single Dropbox account is 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. Decide 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, which is best done by downloading it directly from the Dropbox website home page. Note: this will be easier if you first disable the Internet Explorer Enhanced Security feature as described in 10.4 Disabling Internet Explorer Enhanced Security. Immediately after initial installation, click the **Advanced Settings** option as this allows you to specify the location of the Dropbox folder. Choose the main *Shares* location, which is *D:\Shares* in our example system and which will result in the creation of a folder called *D:\Shares\dropbox*. Note that Dropbox automatically installs itself as a service, meaning it will start-up automatically each time the server starts.



Choose a new place for your Dropbox.
A folder named "Dropbox" will be created inside the folder you select.

Folder: Shares

Figure 199: Dropbox folder location on server

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, Mac OS X, 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 *Shares\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 organization's data from the former user's computer.

Thank you!

We hope that you have found this guide helpful and interesting.

We pride ourselves on the accuracy of our guides and they are reviewed and updated several times a year. However, as the software and utilities are regularly updated it is possible that very recent changes may not be reflected. If you have any suggestions or have found errors or areas for improvement, please let us know at enquiry@ctacs.co.uk. Please quote the date that is stated at the beginning of page 2 so we know what edition you have. Thank you.