

The Little Book of macOS Server

Nicholas Rushton, BA Hons.
Callisto Technology And Consultancy Services
© 2022

Free edition. Do not copy or contribute. (c) CTACS

Updated August 2022
Version 5.12.2

Copyright © Nicholas Rushton, 2022

The right of Nicholas Rushton to be identified as the author of this work has been asserted by him in accordance with the Copyright, Designs and Patents Act 1988.

All rights reserved. No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form, or by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior permission of the author. Any person who does any unauthorized act in relation to this publication may be left liable to criminal prosecution and civil claims for damages. An exception is granted in that up to 750 words in total may be quoted for the purpose of review. The information in this publication is provided without warranty or liability and it is up to the reader to determine its suitability and applicability to their own requirements. This book and its author are unconnected with Apple and this is an independently produced publication.

This book is sold subject to the condition that it shall not, by way of trade or otherwise, be lent, resold, hired out, or otherwise circulated without the author's prior consent in any form of binding or cover other than that in which it was published and without a similar condition including this condition being imposed on the subsequent purchaser.

All copyrighted terms and trademarks of the registered owners are respectfully acknowledged.

Free edition. Do not copy or distribute. © CFAAS

Table of Contents

1 Introduction and Getting Ready	8
1.1 What is macOS Server?	9
1.2 Mac Operating System and Server Versions	12
1.3 Typical Small Network	13
1.4 Choice of Server Hardware	15
1.5 Storage and RAID	17
1.6 Switch and Wireless Access Points	20
1.7 Location & Electrical Considerations	21
2 Installation of macOS Server Software	22
2.1 Overview	23
2.2 Installation of Server software	24
2.3 Changing the Computer Name, Host Name and IP Address	27
2.4 Enable Open Directory	30
2.5 Energy Saver Settings	34
2.6 Automatic Startup of Server	36
3 Users	37
3.1 Overview	38
3.2 User Naming Conventions	38
3.3 Creating a User	39
3.4 Modifying a User	42
3.5 Deleting or Disabling a User Account	43
3.6 Tidying up the Login Screen	44
3.7 Groups	45
4 Shared Folders	47
4.1 Overview	48
4.2 Enable File Sharing	49
4.3 Creating Shared Folders	51
4.4 Making Shared Folders available to Specific Users	54
4.5 Removing or Changing a Shared Folder	56
4.6 Loading Existing Data into Shared Folders	57
5 Accessing the Server	58
5.1 Overview	59
5.2 Macs	60
5.3 iPads and iPhones	66
5.4 Windows Computers	72
5.5 Linux Computers	82
5.6 Chromebooks	83
5.7 Android Smartphones and Tablets	84
6 Backups	85
6.1 Overview	86
6.2 Backing Up the Server using Time Machine	88
6.3 Backing Up the Server using Carbon Copy Cloner	90
6.4 Backing Up Macs to the Server	93
6.5 Backing Up Windows PCs to the Server	96

7 Housekeeping, Maintenance and Security	101
7.1 Overview	102
7.2 Software Updates	102
7.3 Monitoring Server Performance	104
7.4 Alerts	105
7.5 Log Files	107
7.6 CCleaner	108
7.7 Care and Maintenance of Open Directory	109
7.8 Certificate Error	112
8 Profile Manager	114
8.1 Overview	115
8.2 Configuring and Using Profile Manager	116
9 Using Cloud Storage Services	127
9.1 Overview	128
9.2 Using Microsoft OneDrive with macOS Server	129
9.3 Using Dropbox with macOS Server	134
10 Miscellaneous Topics	137
10.1 Overview	138
10.2 Screen Sharing	138
10.3 Accounts Browser	140
10.4 Sharing Media Files.....	141
10.5 Configuring Additional Storage for RAID	145
10.6 Link Aggregation for Network Adapters	150
10.7 DNS Issues	154
10.8 Content Caching	157
10.9 Printing	158
Appendix The Serverless Server	159
A1: Overview	160
A2: Installation and Configuration of macOS.....	161
A3: Creating and Managing Users	166
A4: Connecting Macs to the Serverless Server	174
A5: Screen Sharing.....	177

Free edition. Do not copy or distribute. (c) CTAN 2015

PREFACE

“Useful information and insight. With all the changes Apple is making to its Server product this is definitely a useful book.” – MAK

“The Just Right Guide for Installing OS X Server. This is the OS X Server book for the rest of us, to paraphrase another author's titles. If I could, I would give this book 6 Stars. Its purpose is to enable a technically proficient Mac individual to install and manage an OS X Server application in his home, in a small business, or a small organization such as a church. It succeeds admirably! The material is covered in enough detail to do the job but not in enough detail to make you crazy.” – TJ

“Five Stars. Perfect for all levels” – MI

“Great Little Book. I have gone through a number of costly books on installing OS X Server. This book is by far the best and easiest to use. Lacks very little but does offer outside help. Worth every cent.” – TA

“Good reference. A great reference to have.” – Jeffrey

This guide describes how to setup a network based around Apple's macOS Server software, which runs on the company's own Mac hardware, whether Apple Silicon or Intel based. It is intended for someone who is responsible for setting up a network for use in a small business, home, home-based office or other organization such as a church, charity, small school and so on. It addresses what some refer to as 'the Goldilocks problem', meaning that the built-in help system of macOS Server is too basic and lacking in practical information, whereas the limited, pricey and often outdated reference guides that are available are just too complicated for many people. Hopefully, this is somewhere towards the middle ground. It assumes a reasonable working knowledge of the Mac and a general appreciation of what is involved in small computer networking, whilst trying to avoid the geeky stuff. Incidentally, the guide is not exclusively for Apple users and, in recognition of the fact that many people work in a mixed environment, includes information on how to connect and use Windows computers, Linux computers and Chromebooks as well.

Although this book is about macOS Server, it is also possible to create a functional server without using it at all, using the built-in networking features in all modern versions of macOS; this lacks a small number of management features but is suitable for smaller networks and supplementary information how to go about it is described in the Appendix.

Chapter 1 is concerned with preparation and provides useful background information about buying and preparing for macOS Server. Chapter 2 covers the initial installation and configuration of macOS Server. Chapter 3 discusses the creation of users and groups, whilst Chapter 4 describes how to create shared folders. Chapter 5 covers how to connect Macs, iOS devices, Windows and Linux PCs and Chromebooks to the server to access data. Chapter 6 is all about backups, and Chapter 7 is about housekeeping, maintenance and security to help ensure the server stays healthy. Chapter 8 covers Profile Management. Chapter 9 describes how to use Server with the OneDrive and Dropbox cloud services. Chapter 10 wraps up with a selection of miscellaneous topics to help you get more out of your network, for example, how-to setup a RAID system and manage the server from another Mac.

In this guide, we will generally refer to ‘macOS Server’ or just ‘Server’. Also, when we talk about it, we will use a capital letter at the beginning (‘Server’); if we use the word without a capital letter (‘server’) then we mean the hardware on which it is running or as a generic reference to any file server.

This book has been written using a mixture of American and British English, which is hopefully understandable and acceptable to most readers.

Difficulties with the Artwork?

Pictures and illustrations can sometimes be problematic with eBooks. If you would like a free printable PDF version of this book, just forward a copy of the email confirmation you received when you bought it to ctacs@outlook.com. Please make sure there is no personal financial information in your email. We do not use email addresses for any other purposes, simply for sending out the guides.

Alternatively, this guide is also available for purchase in paperback format in selected markets.

About the Author

The author has worked in IT for several decades, on systems of all sizes and types throughout the world, from the largest companies to the smallest. In recent years, much of his professional interest 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. He has used Macs for more than 30 years.

1

Introduction and Getting Ready



Free edition. Do not copy or distribute. (c) CTACS

1.1 What is macOS Server?

Home and small business computer networks come in two main types: *peer-to-peer* and *centralized*. In a peer-to-peer network, any or all the computers may store the shared data. In this example of a peer-to-peer network there are five computers in a small organization, with the accounts on one machine, the supplier details on another, the customer list on a third and so on:

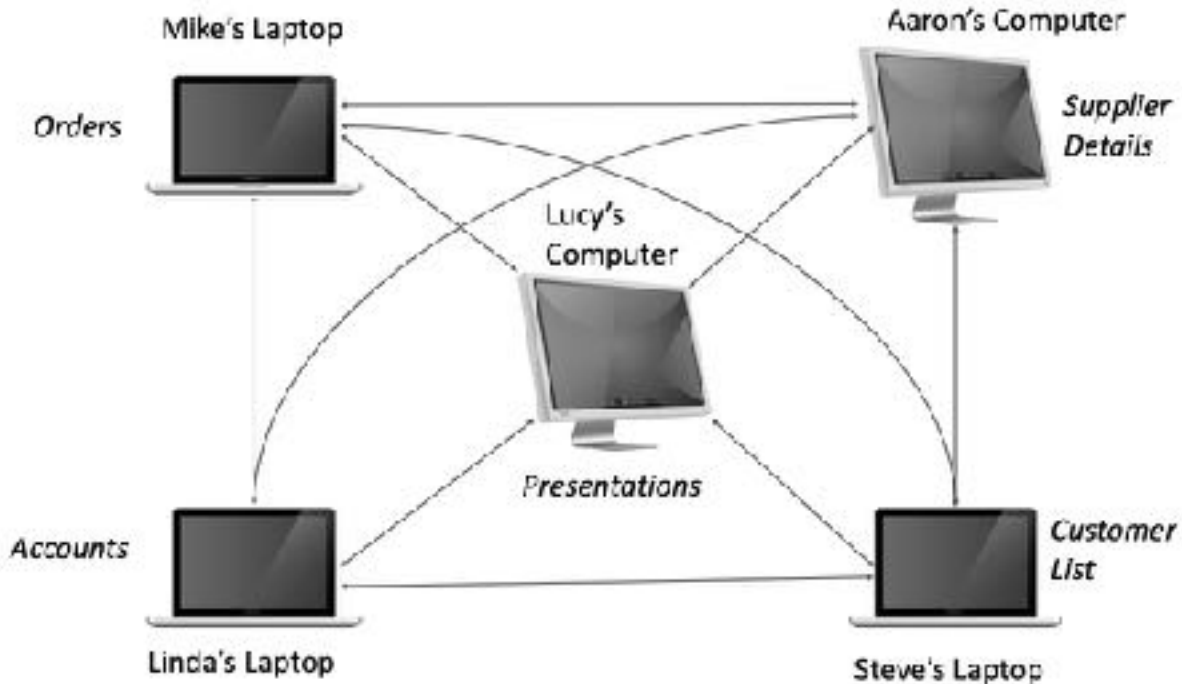


Figure 1: Peer-to-peer network

The computers have been configured so they can connect to each other to access data as required. For instance, if Linda wants to check the orders she connects to Mike's laptop, or if Steve wants a copy of the latest marketing presentation he connects to Lucy's computer. This method of working was developed when the company consisted of just two people and has grown along with it. In the early stages it was satisfactory, but with time has become increasingly problematic. For instance, Mike is often out of the office and takes his laptop with him. When this happens, nobody can access the latest order status; to try and work around it the others have taken to keeping copies of the orders file on their own computers, but this leads to confusion over which is the most up-to-date version. Recently, the company had to hire a temporary worker after one of the team went on extended leave and it proved very problematic explaining to them where everything was stored and how it all worked.

All versions of macOS have the built-in ability to create such peer-to-peer networks (using **System Preferences > Sharing**), as do other operating systems such as Windows. Peer-to-peer networks were very common in households and in small businesses a decade or more ago and can still work well in some very small environments, but they quickly become impractical as the

number of computers and users increases. At such a point a centralized network becomes a much better method of working; here all the data is held on a single and preferably dedicated machine – known as a *server* or *file server*. This is not used as a general-purpose computer and may not even have a mouse, keyboard and screen. Rather, it acts as a repository for all the data, whether that is business information or the type of data that may be found in a typical household, such as photos, music and videos. Being a dedicated machine, it is always there and there are single master copies of the most important files. Crucially, the contorted methods of working that are invariably dictated by a large peer-to-peer network are avoided:

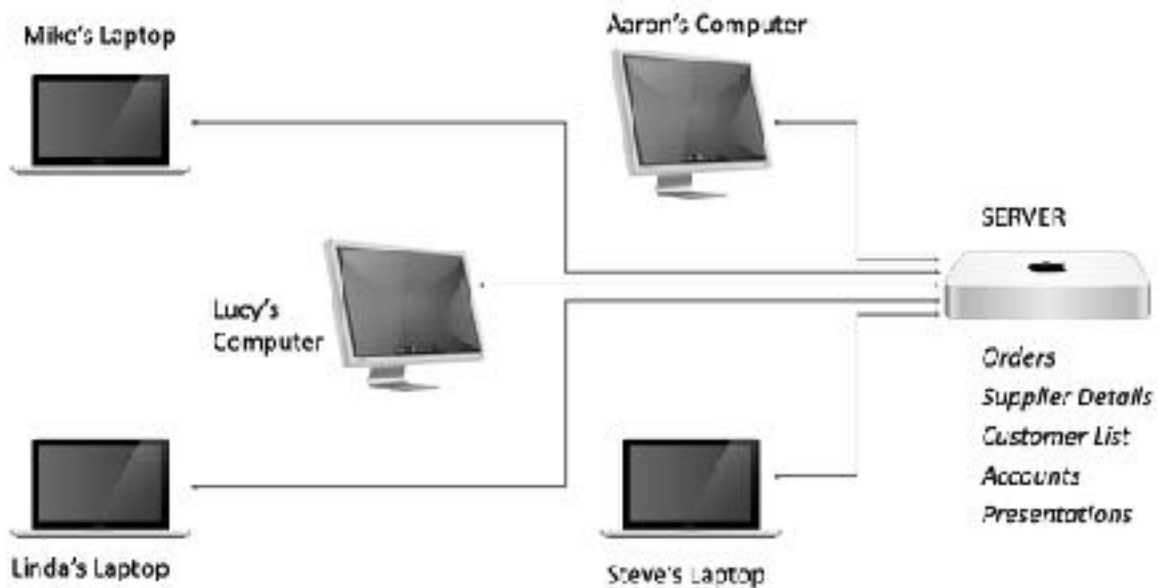


Figure 2: Centralized, server-based network

Besides the benefits of information always being accessible and in a known place, it becomes much easier to backup the data and administer the network. Compare the links between the computers as shown in the two diagrams above, then imagine the implications if another five or ten machines were added in each case: the first example becomes increasingly complicated, but the second remains straightforward and understandable as nothing fundamental changes.

To centralize things in this way usually requires special server software. With Microsoft Windows, there are specific server variants of the operating system, for example, *Windows Server Essentials* is popular with small businesses, whilst some organizations use Linux. However, on the Mac the server software is simply an app which can be added to an existing copy of mac OS (and it is even possible to just use standard macOS on its own in some circumstances, which is also covered in this guide). It is also very affordable: whereas Windows Server Essentials sells for about US\$400/£300, Apple's Server software is priced at just \$19.99/£19.99. This means that it is cheap enough to play with, without the commitment of a large or long-term investment.

1.2 Mac Operating System and Server Versions

There is a fundamental link between the macOS Server software and the Mac operating system itself, such that you need to be using recent if not current versions of both. Specifically, Server 5.12.2 requires macOS Monterey 12.0 or later, nor will earlier versions of Server run on macOS Monterey. A similar dependency applies to earlier versions of macOS and Server e.g. 5.11 required macOS Big Sur 11.0 or later and Server 5.10 and Server 5.9 required macOS Catalina 10.15. Functionally, there are few substantial differences between any of these versions of Server and hence most of this guide applies to all of them, although there may be some minor cosmetic variations in screens. The changes between them relate mainly to controlling and managing connected macOS, iOS, iPadOS and tvOS devices, as more recent versions of these have additional features. This management is done through the Profile Manager feature, which is described in Chapter [8 Profile Manager](#).

Server is a piece of software that has changed over the years, and it is important to understand the nature of these changes. Originally, it was a far more comprehensive product and besides the ability to store and serve data, it could also provide email, calendars, software updates and more. But, starting with Server 5.4, Apple began to depreciate many features and move others into macOS itself, such that it now concentrates on file sharing and device management. In many ways, this makes a lot of sense, as many home and small business users will nowadays use products such as iCloud, Office 365 or Google Workspace for their mail, calendar and contacts, rather than want to be responsible for running their own services. If you are an existing user of an older version of Server and currently running services such email, calendar, contacts, wiki and so on, they do not exist in Server 5.12 and if you move to it then they will disappear. You therefore have four choices: stick to the older version of Server and do not update; switch to online services such as iCloud, Office 365 or Google Workspace; adopt open source or commercial software from other vendors, which is Apple's suggestion if you need additional functionality; switch to another server platform altogether e.g. a Mac-friendly NAS such as Synology or QNAP, which include comparable apps (and for which CTACS also publish setup guides). Apple announced in April 2022 that Server has been discontinued and that 5.12.2 is the final version.

On a more general point, it is suggested that you keep all your regular Mac and iOS clients up to date. When preparing your network, make sure that everything is on the latest version of macOS or iOS as appropriate and allow time for applying the software updates. But, if you are using slightly earlier versions of Apple's client software, you will still find most of this guide applicable.

1.3 Typical Small Network

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

Server - this Mac is at the heart of the network, running the macOS Server software and managing storage and other resources

Extra storage – additional drive(s) to provide greater storage capacity

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 – macOS, Windows or Linux, connected using Ethernet or wireless

Laptops, iPads and iPhones – 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.

Free edition. Do not copy or distribute. © CTACS

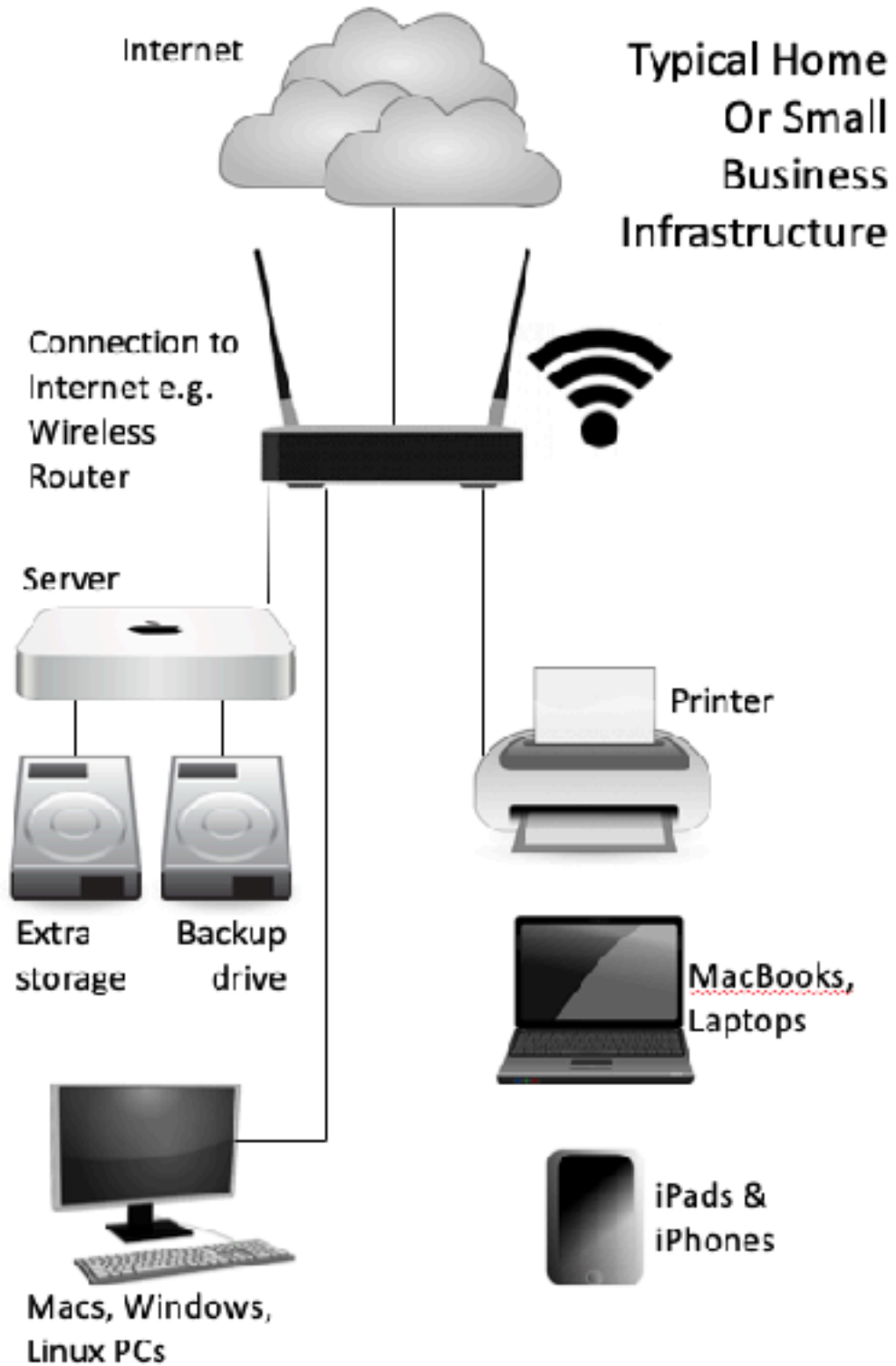


Figure 3: Typical Small Network

Free e

ACS

1.4 Choice of Server Hardware

In the Windows and Linux worlds, a wide variety of hardware is available from many different manufacturers upon which to run server software, for example from Dell, HP and Lenovo to name but a few. This hardware ranges from low-cost and affordable through to expensive and massively powerful, capable of meeting the needs of organizations from the smallest through to the largest. The server hardware may have special features to improve performance and reliability, such as spare hard drives, multiple network adapters, redundant power supplies and so on. Apple used to sell its own server hardware at one time, called Xserve, but no longer does so. Instead, macOS Server can run on any modern Mac, Intel or Apple Silicon, which basically means one that can run the current version of macOS and has at least 8GB RAM. However, the fact that Server can run on any Mac does not necessarily mean that every Mac is suitable; for instance, running it on a laptop is not a particularly good idea as they are not designed for 24x7 operation and may overheat. Rather, a desktop computer of some sort is preferable, of which Apple makes several: Mac mini, the Mac Pro and the iMac. Any of these are potentially suitable, but for many organizations, the Mac mini is the obvious choice as it is small, inexpensive and does not consume much electricity. It is well built, reliable and quite happy to be left running all the time provided it is in a reasonably well-ventilated location. Apple used to sell a Mac mini-based server at one point, which was basically a standard Mac mini but with two internal disk drives, so it has good pedigree.

At the time of writing, the Mac mini is currently available in Apple Silicon and Intel variants and has options for memory and storage. The Server software is not particularly demanding in terms of hardware, while memory and processor speed are unlikely to be issues in small setups. For many organizations and households, a sensible choice would be to buy the smallest amount of storage as possible, as internal storage options are relatively expensive, and then add additional external storage as described in the next section. The Intel variant features more USB/Thunderbolt sockets, which are required for external storage. Both Intel and Apple Silicon models can be ordered with a built-in 10 GbE Ethernet adapter for the highest performance and future-proofing.

It is not necessary to purchase a brand-new Mac for use as a server and a used or secondhand model can be a good option, provided it is in good condition and not so old that it cannot run the current version of macOS (Monterey, at the time of writing). The key question is how reliable will it be, given that it will be used to store important data for the organization or household? For instance, a three-year-old Mac mini that is being replaced because there have been disk or overheating problems is not going to be suitable for use in this role. However, if it is being replaced because a member of the team needs a newer, faster model or is switched from Intel to Apple Silicon, then it might well be suitable for re-assignment as a server. Alternatively, a used machine in good condition might be worth considering. If going down this route, make sure there is no important data on the used Mac that is being repurposed (back it up, if necessary). The computer should then be wiped clean and a fresh copy of macOS installed, as described in [2.1 Overview](#).

One thing to keep in mind is that ideally the server needs to be dedicated to the role and not used for other purposes as well, with the possible exception of small home networks. In other words, it is not a general-purpose Mac for use with spreadsheets, video editing, browsing the internet and other tasks.

Free edition. Do not copy or distribute. (c) CTACS

1.5 Storage and RAID

The Mac being used as the server may not have enough disk storage on it, in which case it will be necessary to add some more. Adding additional internal hard drives to most Macs is difficult or impossible; fortunately, adding external storage is easy and provides flexibility. The simplest method is by plugging in one or more external hard drives, which are available with USB or Thunderbolt interfaces:

USB – low cost; wide range of manufacturers and models to suit all requirements; each drive requires its own USB socket; USB hubs can be used to allow more drives to be connected.

Thunderbolt – more expensive; higher performance; limited range of manufacturers and models; multiple drives can be daisy-chained to each other, up to 6 per port.

Both USB and Thunderbolt have been through multiple iterations and connectors, indicated by designations such as USB 3.0, USB-C, Thunderbolt 3, Thunderbolt 4 and so on. The most recent versions feature a common connector, although the older ‘USB-A’ port is still prevalent. At a minimum, USB 3.0 specification drives should be used. If you are using external drives, you need to be careful that the drives cannot be accidentally unplugged or disconnected, as this can have potentially disastrous consequences for any data stored on them. For maximum performance, throughput and reliability, Thunderbolt is best.

Another option for Mac mini users are certain USB-C hubs, which match the Mac mini cosmetically and sit underneath or on top of the unit. The hub features space for a 2.5 inch SATA drive, which can be a SSD or a mechanical drive. These can be very cost effective: a hub with a 2TB SSD costs around US \$300, whereas Apple charge US \$800 for a 2TB SSD drive in a new Mac mini. If considering one of these, read reviews and forums before purchase, as some models are reported as problematic.

One stage up from individual plug-in drives and hubs are drive arrays, which are available with all interface types, with Thunderbolt being the most popular. Manufacturers include LaCie, QNAP, TerraMaster, Drobo and Yottamaster. Here, multiple drives are contained within one case, but connect to the Mac using a single cable. Depending on brand, the array may be unpopulated and you have to add the drives yourself, or may come ready-populated and ready to use.

The drives in the array could be operated independently, but more commonly are configured as a *RAID* system, which stands for *Redundant Array of Independent (or Inexpensive) Disks*. There are various levels 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 home and small business systems are RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 and JBOD:

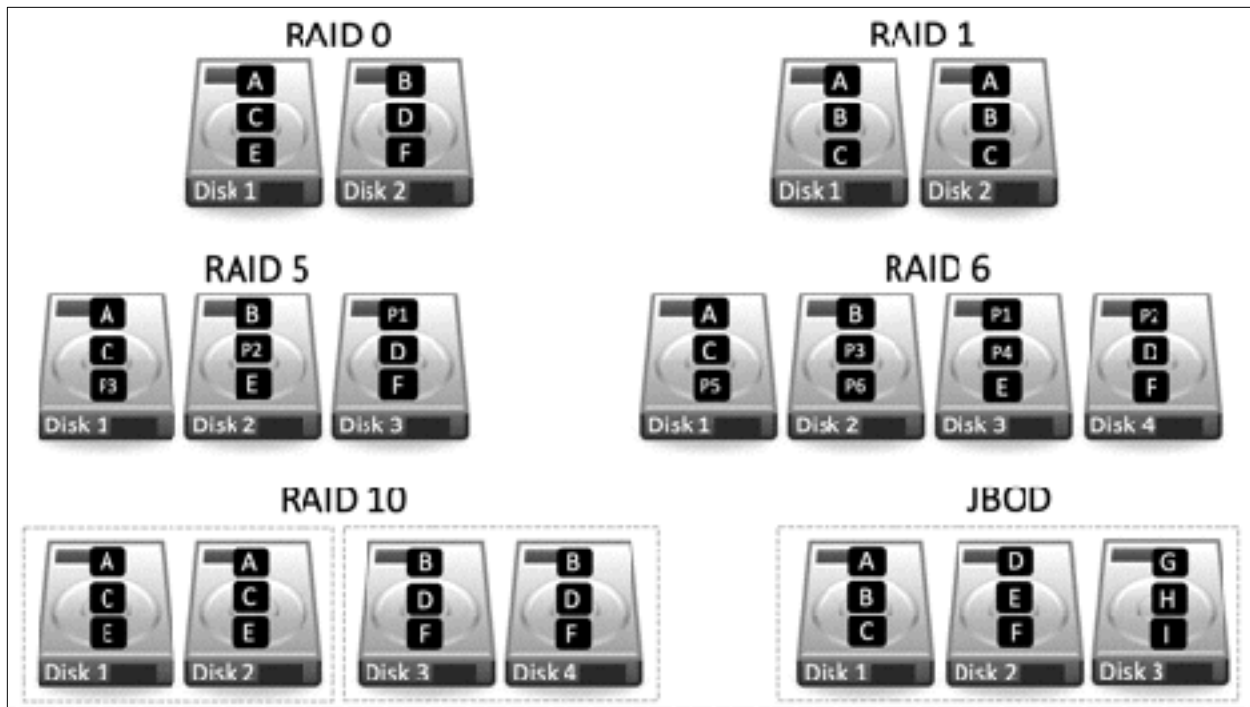


Figure 4: Popular RAID options

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 segments 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 is less commonly used.

RAID 1 consists of two identical drives that mirror each other. When a file is saved there are physically two separate but identical copies behind the scenes, one held on each drive, though you can only see one as the mirroring process itself is invisible. If one of the drives fails, the second one automatically takes over and the system carries on without interruption. At the earliest opportunity the faulty drive should be replaced with a new one; the system is then synced so it becomes a true copy of the remaining healthy drive in a process known as ‘rebuilding the array’. In a RAID 1 system, the total usable storage capacity is half that of the total drive capacity installed. For example, if a disk array has two 4TB drives installed then the total amount of usable storage capacity is 4TB rather than 8TB.

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 loses only 1/3rd on a 3-drive system and 1/4 on a 4-drive system. For instance, if a disk array has three 4TB drives installed then the total amount of usable storage capacity is 8TB rather than 12TB.

RAID 6 uses at least four but preferably five or more drives. It is like 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 to provide that resilience. There may also be a performance hit compared with RAID 5 due to the additional parity processing, but overall RAID 6 is considered superior. If a disk array has five 4TB drives installed in a RAID configuration, then the total amount of usable storage capacity is 12TB rather than 20TB.

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 performance (RAID 0) and redundancy (RAID 1), making it of particular interest where high throughput is needed, for instance in demanding applications such as 4K video editing. The amount of available storage is half that of the total drive capacity e.g. a disk array with four 4TB drives would give 8TB of usable space rather than 16TB.

JBOD stands for *Just a Bunch of Disks* and is not actually a RAID system at all. Rather, it aggregates all the drives together to create one large volume that provides the maximum amount of storage space, albeit without any protection. For example, with two x 2TB drives you would have 4TB of storage, with three x 2TB drives you would have 6TB storage, and so on.

Most external hard drives and many disk arrays, unless they are Mac-specific models, assume that you are using Windows and will have been formatted using the NTFS or exFAT filing system. They should be reformatted as Mac OS Extended (Journaled) or APFS using the Disk Utility in macOS.

External disc drives can be configured for RAID using the Disk Utility in macOS and how to do so is described in section [10.5 Configuring Additional Storage for RAID](#). However, external RAID boxes are often configured using switches or jumpers, or are supplied with their own suitable software, such as *SoftRAID*.

An 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.

1.6 Switch and Wireless Access Points

The devices in a network are connected using Ethernet cabling and wireless access points (WAPs). The difference between a home setup and a business setup tends to be one of scale, as the equipment and principles are essentially the same.

In a home or very small business setup, an all-in-one wireless router is typically used. This connects to the internet, which may be a cable, fiber, satellite, ADSL or 4G/5G service, directly or possibly via a separate box (commonly referred to, albeit incorrectly, as a modem). It has wireless capabilities for linking laptops, tablets and smartphones. There will be several Ethernet ports, used for connected wired devices such as desktop computers. The server Mac preferably needs to be wired directly to one of these ports.

A larger organization may be linked to the internet via cable, fiber, satellite, ADSL or 4G/5G, or may have its own leased line connection, connected using a router. The router may be integrated with or be connected to a separate firewall. In turn this connects to a network switch, to which the server should be connected using an Ethernet cable. Desktop computers, printers and wireless access points or WAPs are wired into the switch; depending on the amount of kit and layout of the office there may be one or more additional switches also connected.

The above descriptions are generic but should bear some resemblance to your infrastructure. Some key points are:

- The server Mac should be connected to the main network switch or combined wireless router, preferably using an Ethernet cable.
- Use wired connections whenever possible as performance is often much better than wireless. Wired devices should be of Gigabit specification. For maximum performance and futureproofing, consider using 10Gbe Ethernet, which is available as a low-cost option for the Mac mini at the time of purchase. It is worth connecting the server to a 10GbE switch, even if most of the infrastructure still runs at Gigabit speeds. External Thunderbolt to 10Gbe Ethernet converters are also available for all modern Macs.
- For wireless devices such as laptops and tablets, make sure they operate at 801.11n, 801.11ac or 801.11ax ('Wi-Fi 6') specification.
- Check the specification of the combined wireless router if you are using one. Many ISPs (Internet Service Providers) supply relatively low-cost models, sometimes free of charge when you sign-up with them. These are often of average quality, for instance the Ethernet ports may not be Gigabit or the latest wireless standards may not be supported. Spending money on professional or prosumer ("professional consumer") routers and switches will usually give better performance and reliability.

1.7 Location & Electrical Considerations

The server should be placed away from direct sunlight and any source of heat, such as a radiator. Avoid locations that are wet or damp. As little physical access is required the unit can be located out of sight and reach, for instance in a cupboard or a locked room or generally out of reach. Mac minis generate very little noise and can usually be operated in an office or family room without any disruption.

It is possible that data loss can occur if the electrical mains power fails whilst the server is running. The best way to mitigate against this is to use an intelligent UPS (*Uninterruptible Power Supply*), as in the event of power problems this will enable the server to continue operating for short periods and to then shut it down in an orderly manner if necessary. Most popular brands work with the Mac operating system e.g. APC, CyberPower, Powercom. The UPS connects to the Mac with a USB cable and plugging one in will cause new options to be displayed in the **System Preferences > Energy Saver** panel. Some UPS vendors supply special software with their kit, but you may not wish to install it as the built-in Mac support is often sufficient.

In a business environment, the use of a UPS should be considered mandatory.

If a UPS is not used, which is commonly the case in a domestic environment, then the server should at least be connected to a clean electrical power supply via a surge protector.

Free edition. Do not copy or distribute without permission.

2

Installation of macOS Server Software



Free edition. Do not copy or distribute. (c) STACS

2.1 Overview

This chapter describes how to install the macOS Server software and how to configure and customize a Mac, such that it is optimized for use as a server.

The Mac that is being used for the server role should be ‘clean’. You could start with a brand-new computer, otherwise reset an existing Mac and install a fresh copy of macOS, which can be done as follows:

- Connect the Mac to the Internet using a wired Ethernet connection
- Turn on the Mac
- When you hear the startup sound, hold down the **Command (⌘)** and **R** keys on the keyboard, releasing them once the Apple logo appears
- After a short while, the Utilities menu will appear. Choose **Reinstall macOS**
- Work through the prompts about selecting a destination disk and installing the OS

When the OS has installed and you are running through the setup process, you want as little customization and personalization as possible. For instance, you do not want to specify an iCloud account, turn on location information, register with Apple or any of the other things that it encourages you to do, as these are of little relevance on a server machine.

Make sure that everything is fully updated by going into **System Preferences**. Updated versions of applications are not necessarily important, but you need to make sure that any macOS updates are applied as these often address security issues, may add or improve functionality, or may be pre-requisite for macOS Server. It is possible that the current version of macOS may not have been installed and it may be necessary to upgrade to a later version, so this entire process can be time consuming.

Note: all Apple Silicon-based Macs and late model Intel Macs feature the Apple T2 Security Chip. If you have such a Mac running macOS Monterey or later, it is possible to restore it to factory settings without having to reinstall the operating system from scratch. Launch **System Preferences** and from the menu bar click **Erase All Content and Settings**. It will then be necessary to enter the administrator details, after which you can optionally backup the machine. It is then necessary to enter your Apple ID details before finally erasing it. If further information is required, refer to <https://support.apple.com/en-gb/HT212749>

2.2 Installation of Server software

Server is obtained through the App Store, so you will need an Apple account if you do not already have one. At the time of writing, it costs \$19.99 in the USA, £19.99 in the UK and equivalent amounts in other currencies. If you have purchased a copy of Server previously, you will be able to download the current version at no additional charge. It does not take long to download, as it is a relatively small app. It will be placed in the Applications folder along with an icon on Launchpad, which you should click to begin the installation. Most likely you will be installing it on the same Mac, in which case click **Continue**, but there is an option to install it on another Mac located on the same local network if required:



Figure 5: Server Installation screen

Review the software license agreement. On the agreement is a box marked *Use Apple services to determine this server's Internet reachability*, and you need to have this ticked. You will require administrator access to install the server software. Installation is relatively quick and upon completion the main Server screen is revealed, although it may take a couple of minutes to appear on first run and up to a minute on subsequent occasions. The left-hand side of the screen can be thought of as a type of menu, listing aspects of the server that can be managed, and is broken down into four categories of *Server*, *Accounts*, *Services* and *Advanced*, all of which can be expanded or hidden as required.



Figure 6: Server Main Screen

These four main categories are:

Server – used for managing key aspects of the server, particularly those relating to its overall configuration e.g. network settings.

Accounts – for managing users of the server.

Services – used for configuring and managing the various facilities provided by Server. In a new installation, only *Profile Manager* is available.

Advanced – this is used to cover more advanced and specialized topics. Initially it will be empty, with no entries.

When an item on the left-hand side is clicked, the right-hand panel shows the corresponding details. In some cases, the right-hand panel may then have multiple tabbed sections within; for instance, in the screen above we are viewing the main details of the server and it has three tabs: *Overview*, *Settings* and *Access*.

Server also has a conventional menu bar at the top of the screen (not visible in above screen shot). This largely duplicates the options summarized above, but also provides access to some other tools and features.

For convenience, you may wish to place the icon for Server on the Dock, which you can do by dragging its icon from the Applications folder onto the Dock. When Server is launched, it will give you the option of managing the server computer itself, or another Mac on the network. You will need to provide the password for an administrator account on whichever Mac you connect to.

Server includes a built-in help system, accessible by clicking **Help** > **Server Help** on the menu bar, whilst **Help** > **Server Support** gives access to additional online information from Apple, via the Safari browser.



Figure 7: Server's Help System

Note: Server does not support the Dark mode of macOS. However, the screenshots for regular macOS operations in this guide are in a mixture of Light and Dark modes.

2.3 Changing the Computer Name, Host Name and IP Address

The *Host name* is the unique name by which the server is known on the network. By default, it is derived from the name of the computer and hence may not be suitable, such that you may wish to change it. In our example, the Mac being used for the server below is originally called *Nicks-Mac-mini* and the host name has become *Nicks-Mac-mini.local*. A better choice would be something more descriptive, for example *server* or *macserver*, as that is what it is. However, if you have or envisage ever having multiple servers you need to adopt some naming scheme such as *server1*, *server2*, *server3*, or perhaps one based on location or department or class or whatever is appropriate for your organization.

On Server's main screen, in the Overview section, click the **Edit Computer Name** button. Change the *Computer Name* to (e.g.) *server*; which will also have the effect of changing the *Local Hostname* to *server.local*. Click **OK**. It is **very important** that there are no duplicated computer names on the network: if Server ever finds another device with the same name, it may rename itself and the network will not function correctly.

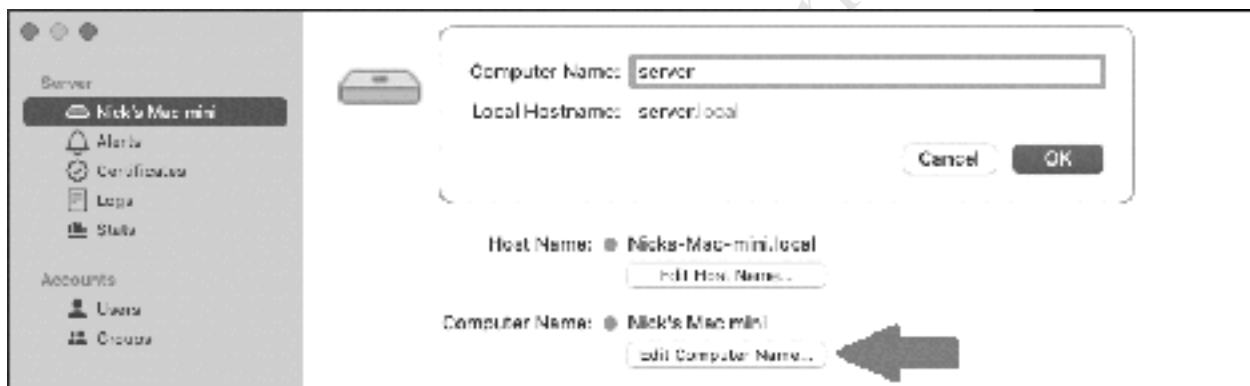


Figure 8: Computer name and local hostname

Next, click the **Edit Host Name** button. On the resultant screen, it will 'evaluate' the network for several seconds; after it finishes click **Next**. You are presented with three options: *Local Network* – the network can only be accessed from within the premises; *Local Network and VPN* – the network can be accessed both from within the premises and from also outside the premises using a *Virtual Private Network (VPN)*; *Internet* – the network can be accessed both from within the premises and from also outside the premises over the internet via a domain name:

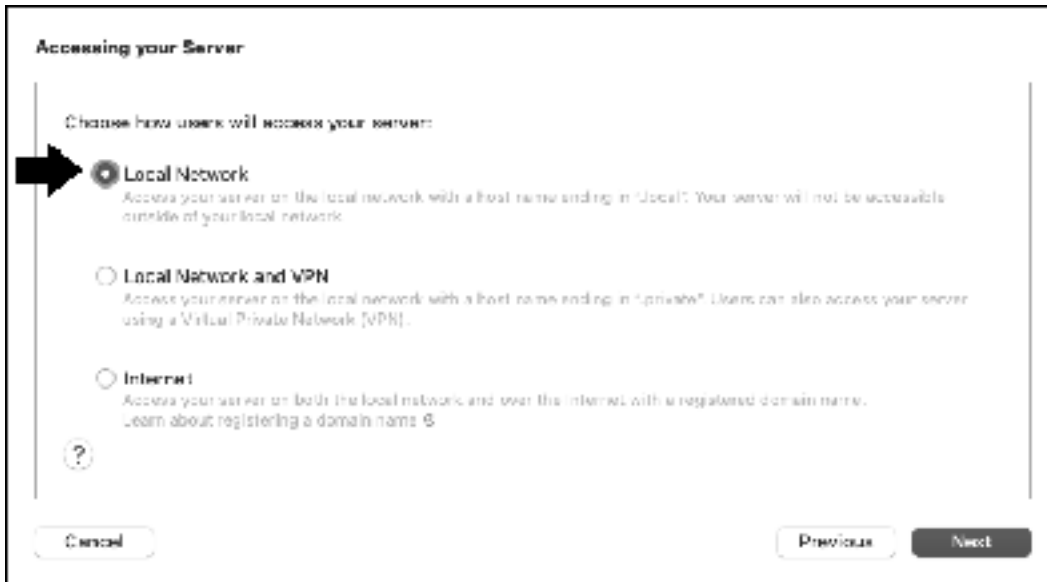


Figure 9: Choose the type of access

It is suggested that you choose **Local Network**. Click **Next** and on the subsequent screen change the *Host Name* so that it matches the computer name but with an extension of *.local*, for example *server.local*. Note that sometimes Server chooses an extension of *.home*, in which case you will need to change it.



Figure 10: Edit the network address

You also need to decide about the IP address for the server. Every device has a number within a network to uniquely identify it, known as the *IP address*. The router itself will have a default fixed IP address decided by the manufacturer, for instance 192.168.1.1 or 192.168.1.254 are common choices. It will then allocate numbers to computers and devices as they connect, for example the first computer might become 192.168.1.101, the second computer might become

192.168.1.102 and so on. A piece of software inside the router – known as a *DHCP server* – handles this process. The ‘D’ in DHCP stands for dynamic and indicates that the IP addresses are handled dynamically and recycled. So, for example, the next time the first computer is switched on it might be allocated a totally different number e.g. 192.168.1.87. The fact that the numbers change does not make any difference to computers, but some devices require a fixed IP address, which is why routers have them.

At present the server Mac is probably operating on an IP address received from the router’s DHCP server. However, servers work better with fixed or static IP addresses, so we need to change matters. To the right of the *Network Address* – current reading *192.168.1.87 on Ethernet* on our system in the above screenshot – is a button marked **Edit**. Click it and on the resultant screen, change the drop-down marked *Configure IPv4* from *Using DHCP* to *Using DHCP with manual address*. Change the IP Address to something that is outside of the DHCP scope of the router; if you do not know what the scope is, it is usually safe to choose an address next to the router or at the opposite end. In this example, the *Router* is 192.168.1.1, so a suitable address would be something like 192.168.1.2. The *Subnet mask* should be set to 255.255.255.0 and the *DNS Server* set to the same address as the Router (it may default to it automatically). The *Search Domains* field should be blank or grayed out. Click **Apply**. After you are returned to the previous screen click **Finish**. It may take around a minute before the changes take effect.

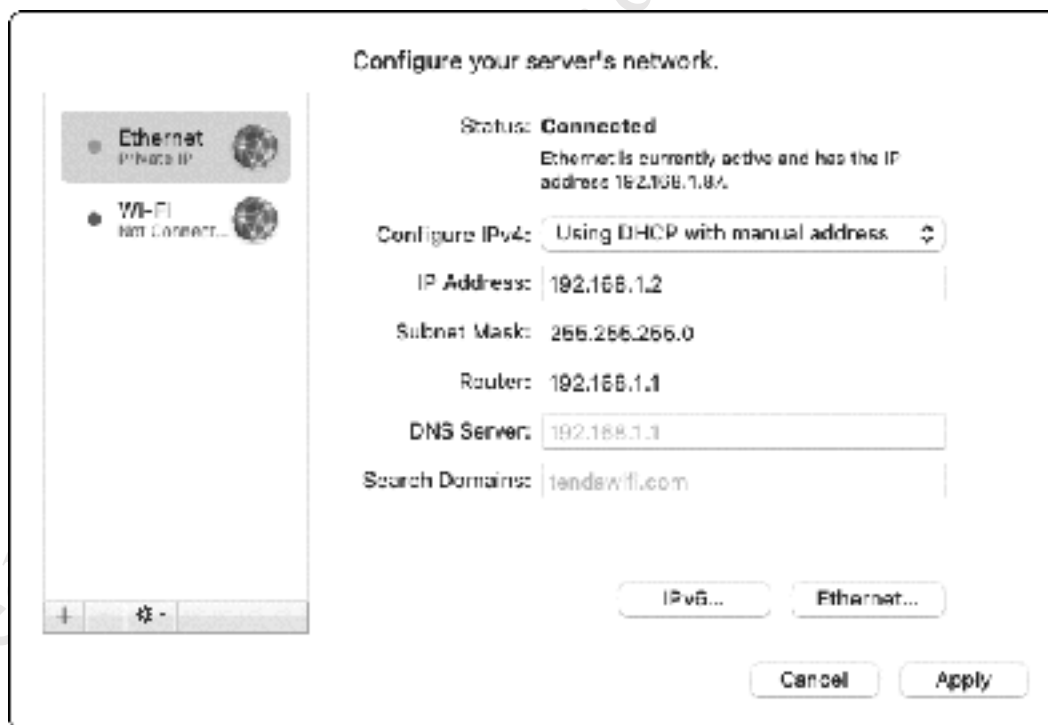


Figure 11: IP address details

Note: Subnet masks are used to help organize and manage larger networks. Using a value of 255.255.255.0 means that the maximum number of devices in the network is 255, which is typically sufficient in a home or small business network.

2.4 Enable Open Directory

A network comprises computers, users, shared storage areas and other resources. There needs to be a method for organizing these resources and advertising their availability and this is the purpose of a *directory*. In very simple terms, the directory is a list of what is available on the network, in much the same way that a telephone directory is a list of people and businesses you can call. Several different directory systems exist: *X.500*, *LDAP*, *Microsoft Active Directory* and *Open Directory*, which is the one used by Apple. The concepts behind them are all similar and most derive from a common ancestor, so if you have worked with any of them before you will find Open Directory very straightforward.

Within Server, choose **View > Open Directory** from the menu bar, which will cause it to be added to the left-hand side of the screen in the Advanced section. Click the ON/OFF switch in the top right-hand corner of the screen to enable it; this will cause a wizard to run, giving three options: *Create a new Open Directory domain*; *Join an existing Open Directory domain*; *Restore Open Directory domain from an archive*. Choose the first option to **Create a new Open Directory domain** and click **Next**:

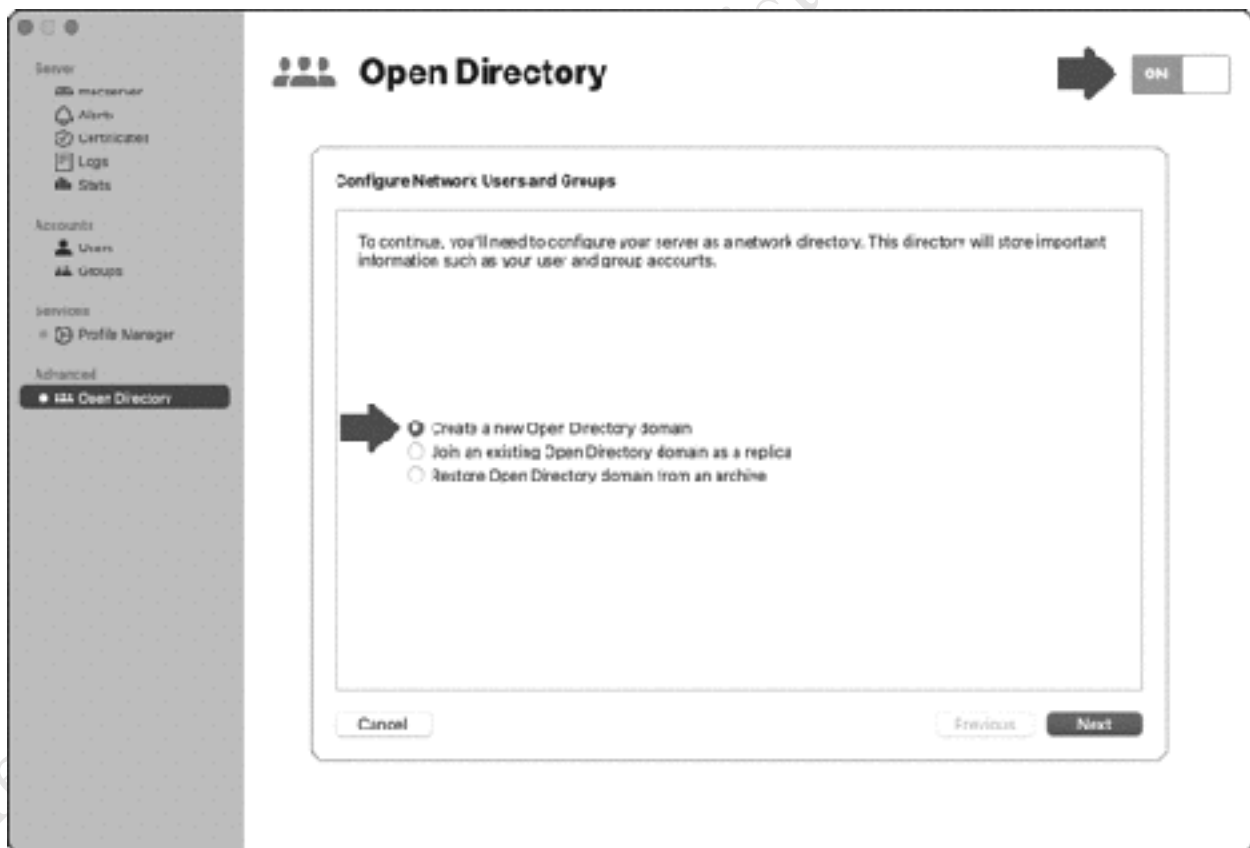


Figure 12: Create a new Open Directory domain

The initial step is to setup a separate administrator for the domain; this is really intended to meet the requirements of large organizations with many users and multiple of servers but still has to be

done, even in the smallest network. The account name defaults to *diradmin* – you could potentially change it, but it is suggested you do not do so. However, for convenience you may want to use the same password as you use for managing the server i.e. the administrator’s password. When you make any changes to users within Server, you may be asked to enter the Administrator name and password, however, what this really means is the *Directory Administrator* and password, so it is important not to forget it.



The screenshot shows a dialog box titled "Directory Administrator". Inside, there is a text instruction: "Enter account information for the new directory administrator account. This user account will have administrative privileges for managing network users and groups." Below this, there are four input fields: "Name" with the value "Directory Administrator", "Account Name" with the value "diradmin", "Password" with masked characters "*****", and "Verify" with masked characters "*****". A checkbox labeled "Remember this password in my keychain" is checked. At the bottom, there are three buttons: "Cancel", "Previous", and "Next".

Figure 13: Specify the Directory Administrator account

On the next panel, enter a name for the organization. If the organization’s name is lengthy, then consider abbreviating it; for instance, here we have used *CTACS* rather than *Callisto Technology And Consultancy Services*. Underneath, enter an email address, which can be used for support purposes:

Organization Information

Enter the name of your organization. This information will be shown to users to help them identify your server.

Organization Name:

Provide an email address that users can use to contact you. This will be used to verify your server's authenticity as well as for support.

Admin Email Address:

Figure 14: Organization information

Click **Next** and on the resultant *Confirm Settings* panel click the **Set Up** button. After a minute or two, configuration will be complete and the main screen will now appear along the following lines, showing that Open Directory is operational:

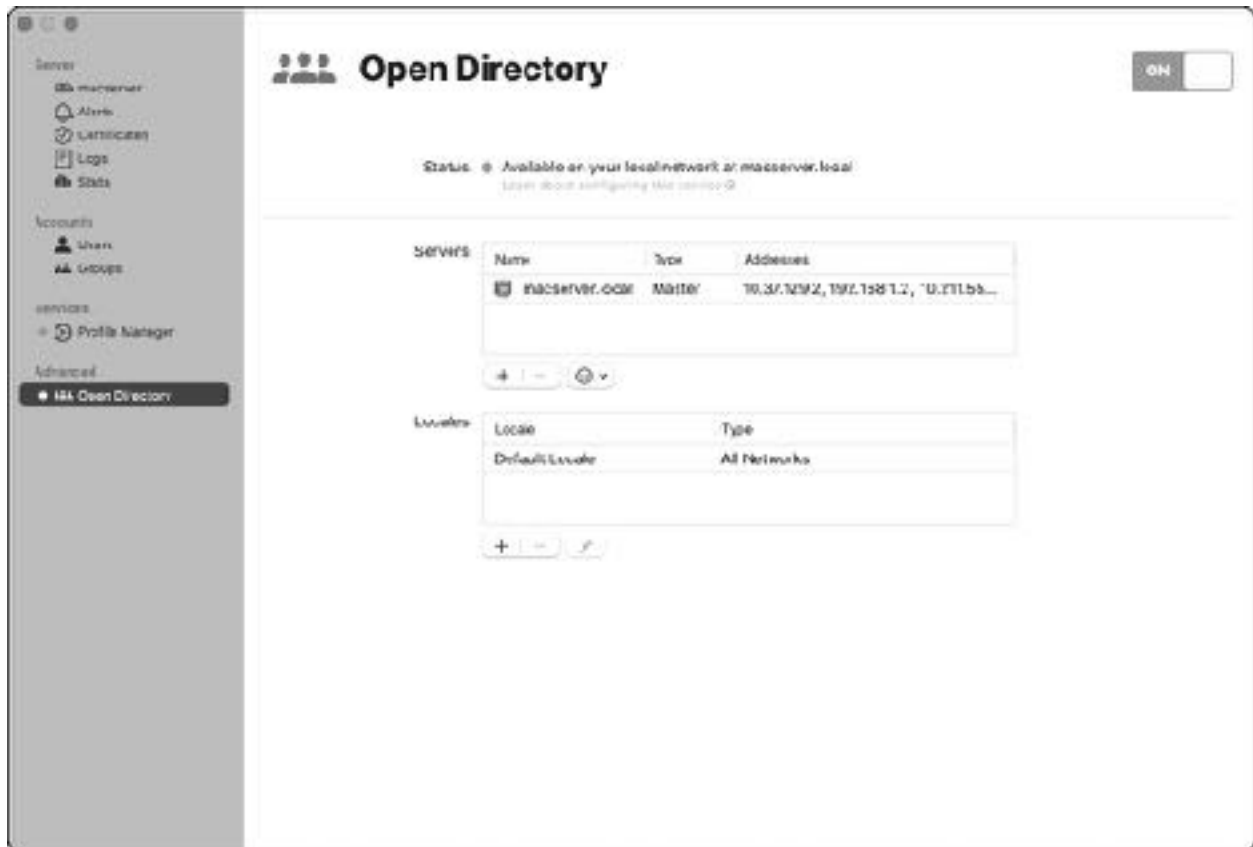


Figure 15: Open Directory up and running

Troubleshooting: Most problems relating to Open Directory are caused by DNS issues. If DNS is configured incorrectly, you will see the following error message:



Figure 16: Indicates DNS problems

Check that your DNS settings are correct and that you are using a domain name with a suffix of `.local` as previously advised, then try again to configure Open Directory. More detailed information about resolving DNS issues can be found in section [10.7 DNS Issues](#).

2.5 Energy Saver Settings

macOS has power management features to help reduce power consumption, such as putting the computer to sleep or in hibernation mode when it has not been used for any length of time. Whilst very useful on a laptop, such features are less so on a computer being used as a server. For instance, if the server has gone to sleep you do not want the delay and inconvenience of having to wait until it starts up again when you want to save or retrieve a file – you expect it to be always available. For this reason, the power management features in macOS may need to be adjusted.

Go into **System Preferences** and choose **Energy Saver**. On the **Power** section, move the *Turn display off after* slider to 1 minute and remove the tick from the *Put hard disks to sleep when possible* box:

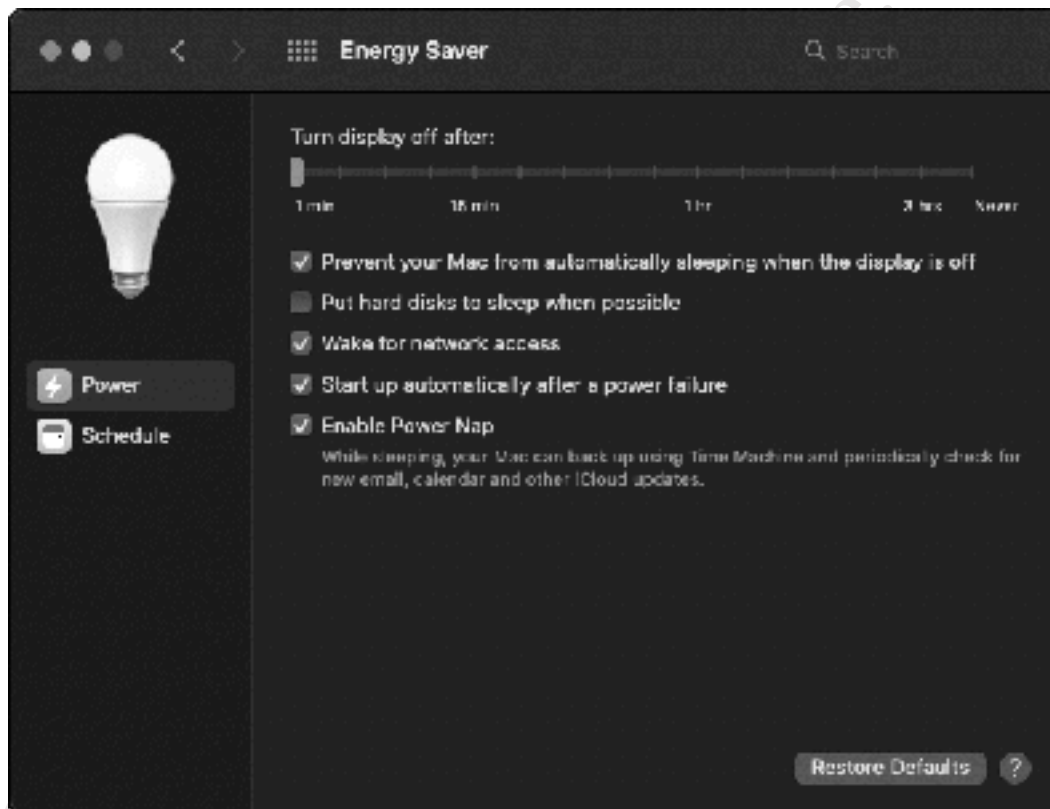


Figure 17: Energy Saver settings

Optionally, you may wish to set a schedule so that the server starts up and shuts down automatically each day. This can be useful in, say, a business or educational setting where there is no requirement to use it out of hours. To do so, click **Schedule** and adjust the timings as required. In this example, the server is set to power up at 06:30/6.30am and shutdown at 23:00/11:00pm every day. Doing this allows energy to be saved and provides some security, as a computer that is not powered up cannot be hacked.

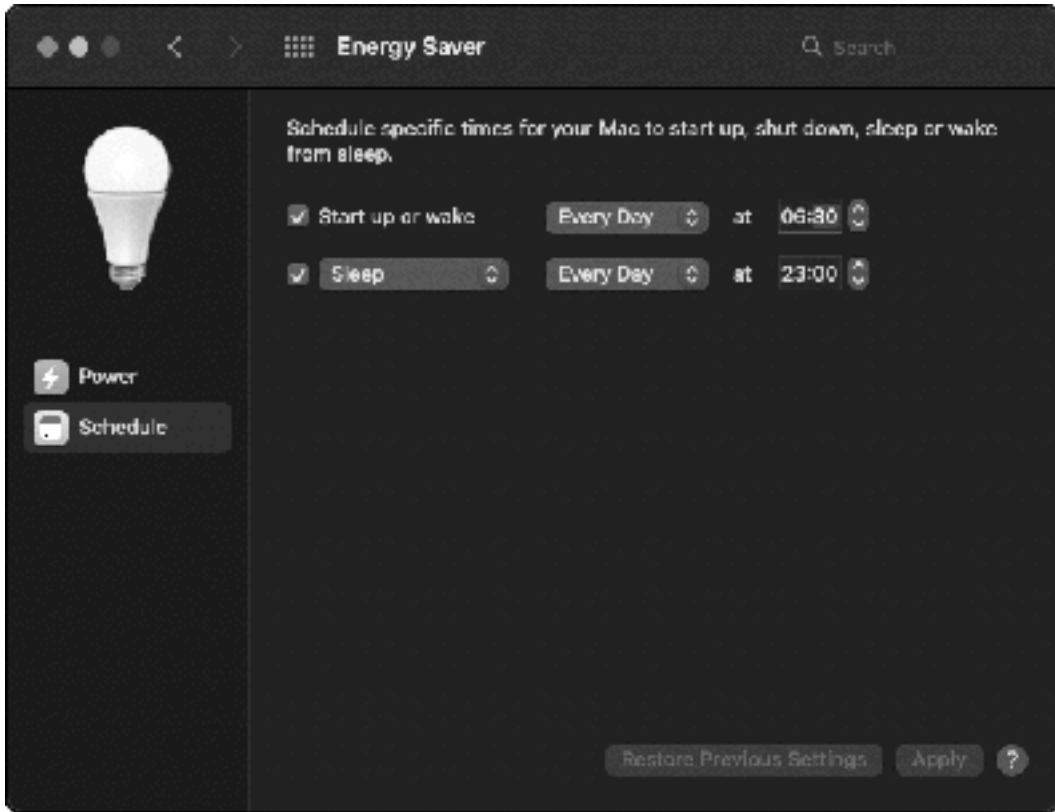


Figure 18: Specifying a schedule

Free edition. Do not copy

2.6 Automatic Startup of Server

In the event that the server is restarted for any reason e.g. you have setup a power-on schedule as described in the previous section, you want Server to startup automatically rather than need someone to login and run it (suppose, for instance, that it is your responsibility, but you happen to be on holiday). To arrange this:

Login to the server Mac using your normal credentials. Go into **System Preferences > Users & Groups**. Highlight the *Admin* user name. Click the **Login Items** tab (you will probably need to unlock the padlock to authenticate and make changes). Click the Plus sign (+). Navigate to the Applications folder, find *Server* and click **Add**. You may wish to then click the lock to prevent further changes.

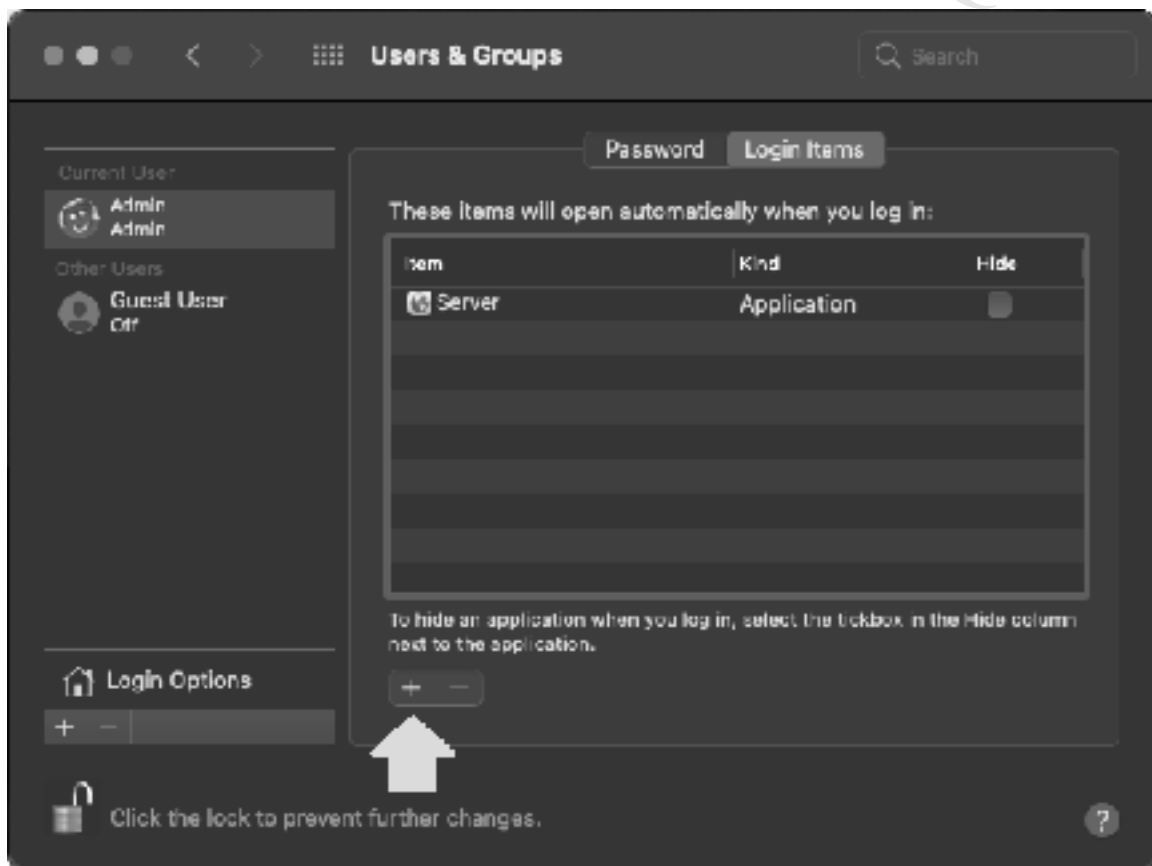


Figure 19: Login options

3

Users



Free edition. Do not copy or distribute. (c) CTACS

3.1 Overview

There are two types of user accounts in a network environment. Firstly, there are the familiar *local user accounts*, of which there is always at least one on a standalone Mac. Unless you have one of these accounts on a particular machine, you cannot use it. Secondly, there are *network user accounts*. These are held centrally on the server and with a network account you can use any Mac in the network to connect to the Server. Why is it done like this? Basically, because it is far more flexible, efficient and practical. Suppose you work in an organization that has 10 Macs and 10 people and you want any person to be able to work with any computer. With local user accounts, you would need to visit each of the 10 Macs and create 10 local accounts, giving a total of 100 to be created. You would also need to maintain 100 corresponding passwords. However, with network accounts it would only be necessary to define the 10 users once, on the server, requiring a fraction of the effort.

Before creating any users on the server, you should first enable Open Directory, as described in section [2.4 Enable Open Directory](#). This step is essential as it enables network user accounts to be created and maintained. And when making any alterations to users and groups, you may be required to authenticate using the Directory Administrator ('diradmin') credentials that were specified when setting up Open Directory.

3.2 User Naming Conventions

You should decide upon a naming convention and this is one area where a different approach can be taken depending on whether it is a home or business network. In the case of a home network the user names can be anything you want, although there is merit in following a scheme. For instance, you could use the first names of the family or household members. In a business or educational environment a more formal approach may be more appropriate. As a general point, the greater consistency there is, the better. For user names, two common conventions are to use the first name plus the initial of the surname, or the initial of the first name plus the surname, although in some cultures other conventions might be more appropriate. In the case of particularly long names and double-barreled names, consider abbreviating them. For example:

Name of Person	User Name	or	User Name
Nick Rushton	nickr		nrushton
Mary O'Hara	maryoh		mohara
Ian Smith	ians		ismith
Amber Williams	amberw		awilliams
Daniela Petrova	danielap		dpetrova

3.3 Creating a User

To create a new user, go into Server and click on **Users** within the *Accounts* section. Alternatively, click **View > Users**. There is also a shortcut: **Shift Command (⌘)U**. Click the plus sign (+) in the bottom left-hand corner to display the following panel. The first entry on the panel reads *Directory* and **must** be set to *Local Network Directory* – if the option does not appear then it means that you have not successfully setup Open Directory as described in section [2.4 Enable Open Directory](#)). The importance of choosing Local Network Directory cannot be over-emphasized, particularly as Server defaults to the Local Directory option and once created the user cannot be changed (if the wrong choice is made the user will have to be deleted and re-created correctly).

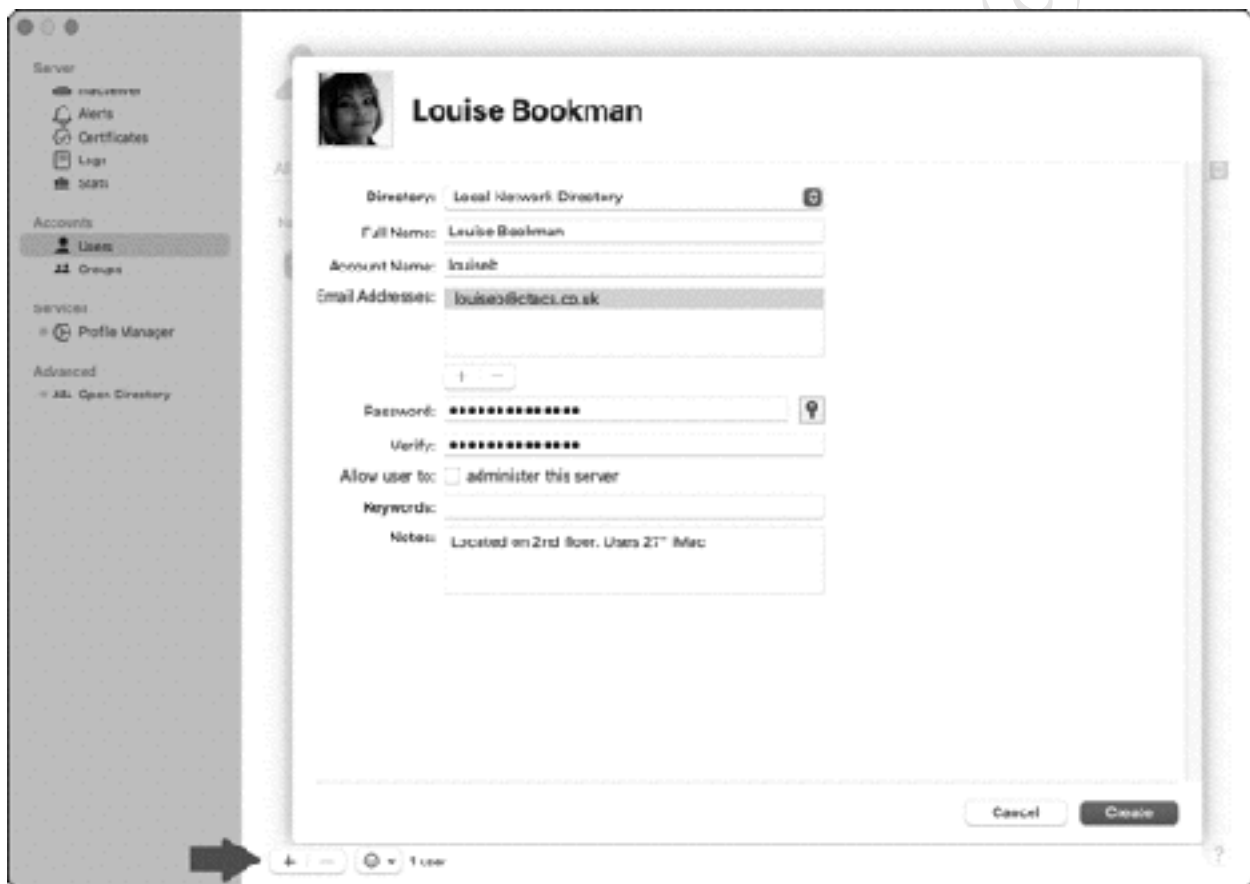


Figure 20: Creating a new user

Enter: the user's full name; an account name e.g. a shortened version of the full name; an optional email address for the user; a password, plus enter the password again to verify it. The best passwords are non-obvious and contain a mixture of letters, numbers and special characters. To the right of the password is a small icon that looks like a key and clicking it will run the *Password Assistant*, which generates a random password for the user. The Password Assistant allows considerable flexibility over the type and length of the password and provides a visual clue over its quality (strength). Whilst passwords should ideally be as strong as possible,

common-sense should also be exercised. For instance, in a school network where there are young children then passwords will need to be quite simple. The password should be noted as there is no way of subsequently determining a user's password, although you can change it:

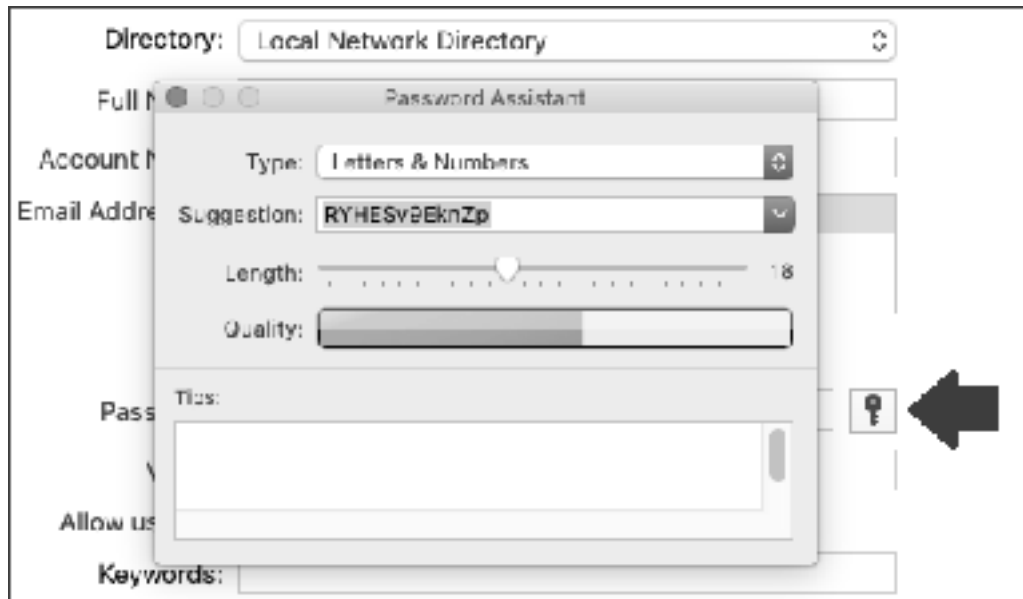


Figure 21: Password Assistant

You could choose to allow the user to administer the server, although you would not want to do this in most scenarios.

Keywords and *Notes* can be ignored but could be used for maintaining useful information about the user, such as contact details.

In the top left-hand corner of the panel next to the user's name, is a silhouette. This is clickable and doing so enables a picture to be optionally specified. There is a small selection of built-in ones, or an image or photograph can be used. Alternatively, you can drag a file onto it. If you add a photograph, keep it relatively small, for example a JPEG of no more than a few 100 KB.

Having completed the panel, click **Create**. The newly created user will be listed on the main Users screen. The process should be repeated until all the users have been created. If you have many users to create, you may find it helpful to first create a checklist of their names and to make a note of the passwords.

Note: when reviewing the Users screen, it may display a long list of unfamiliar users. If so, click the drop-down and set it to the **Local Network Users** option:

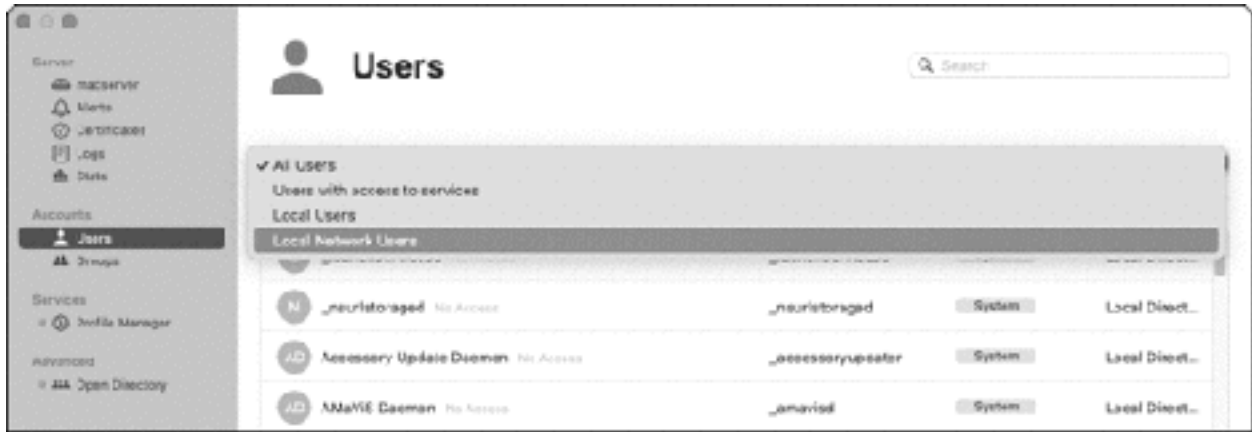


Figure 22: Filtering the list of users

Free edition. Do not copy or distribute. (c)

3.4 Modifying a User

To subsequently modify a user, go into Server and click on *Users* within the Accounts section. Right-click a user's name and a pop-up menu appears:

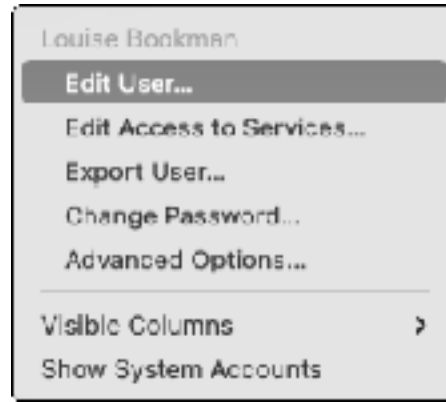


Figure 23: Modify an existing user

To change their key details, such as their full name, their picture, email address or notes, click **Edit User**. This displays the same basic form that was used when creating the user.

To control which facilities they have access to, click **Edit Access to Services** (basically this means access to *Screen Sharing* – see section [10.2 Screen Sharing](#)).

To change the user's password, click **Change Password**. This brings up a box into which the new password is entered and verified. Alternatively, click the key icon to have the system generate a password. If required, the user can be forced to change their password the next time they login. This is useful in organizations that have a policy of not divulging passwords to the network administrator:

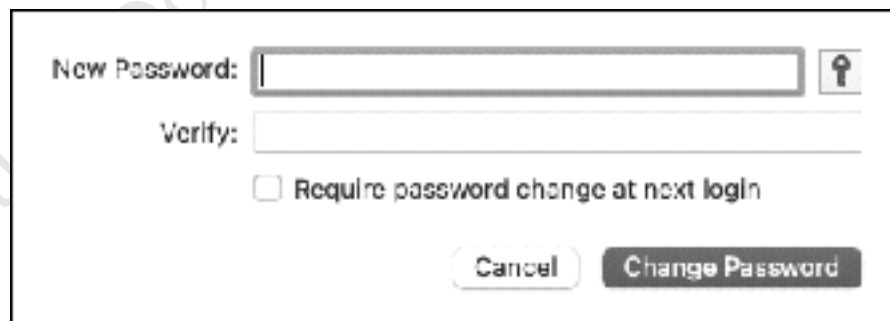


Figure 24: Change password

The other options on the menu are less commonly used.

3.5 Deleting or Disabling a User Account

To delete a user, highlight their name within the list of users then click the minus (-) sign in the bottom left-hand corner of the screen. A confirmation message is displayed – click **Delete** to delete the user or **Cancel** if you have changed your mind or selected it accidentally.

Note that deleting a user is a permanent action and cannot be undone. Because of this, an alternative strategy is to first disable their account. Then, after a suitable interval has passed and you are sure that they are not returning, you can delete them. To temporarily disable an account: right-click the user's name. Choose **Edit User** from the pop-up menu. Remove the tick from the **Allow user to log in** box. Click **OK**. This technique is also of use in a business when employees go on extended leave.

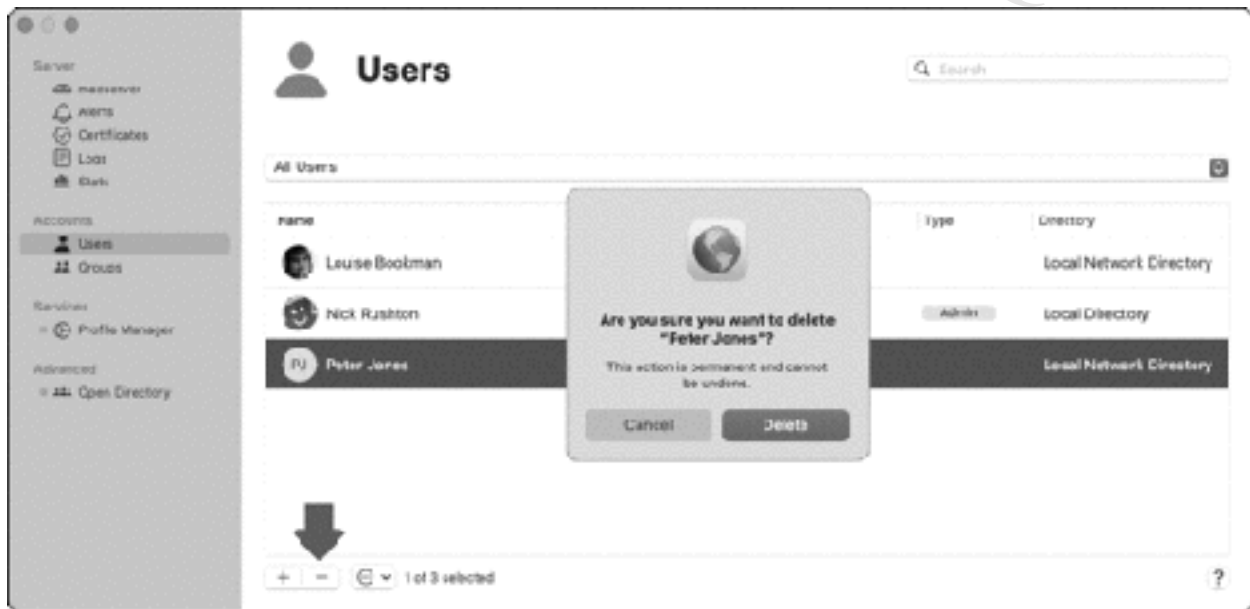


Figure 25: Deleting a user

3.6 Tidying up the Login Screen

By default, the Mac operating system displays a list of all local users on the login window. Whilst this is fine on a personal system with only one or two users, on a server, which may have many more users defined on it, it results in a very cluttered screen and can also have the effect of encouraging people to believe that this is a standard computer they can use. To change this behavior, go into **System Preferences > Users & Groups**. Choose **Login Options** (you will need to click the padlock and specify your admin user credentials) and ensure the *Display login window as* is set to **Name and password**. Also, remove the ticks from all the boxes except the first one:

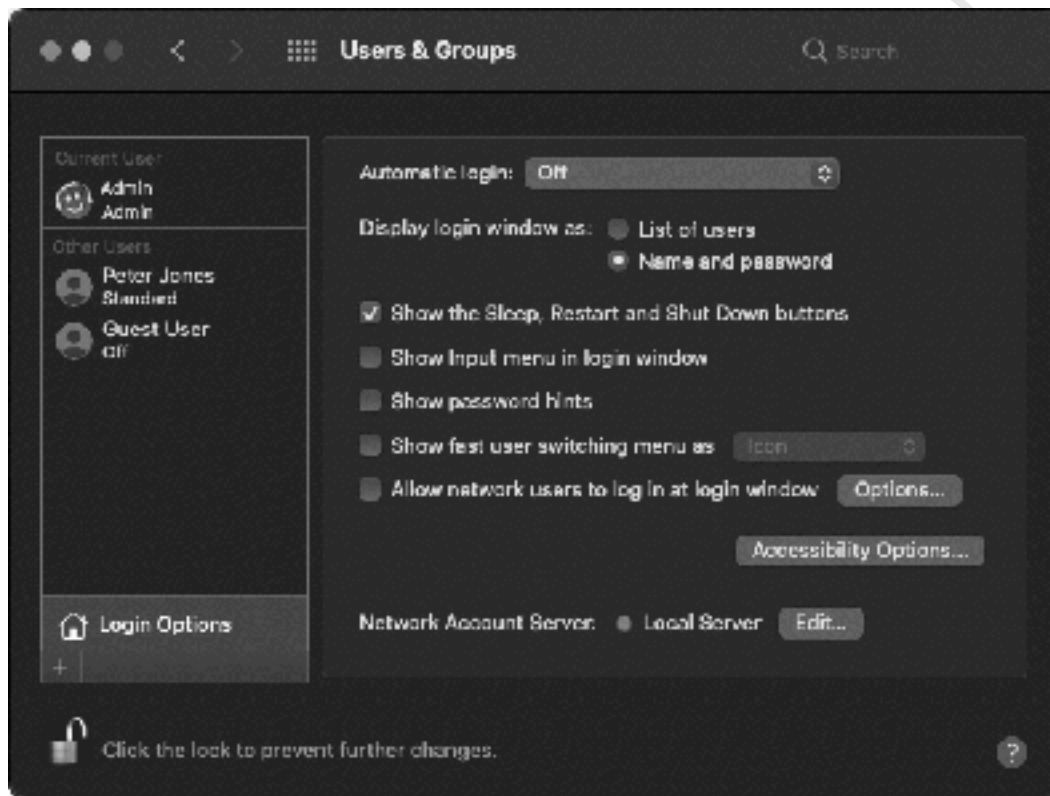


Figure 26: Login Options

As an additional security measure, it is possible to restrict login on the computer to specific users. To do so, click the **Options** button and add or remove users as required.

3.7 Groups

In an organization with a relatively small number of users, specifying who has rights to resources is relatively easy to manage. But as the number of users increases it naturally becomes more time consuming: for example, consider having to define the access rights for, say, fifty people. Such organizations are generally 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, some in marketing and so on. Or, in an educational establishment, students would commonly be organized into classes.

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

To create a group, go into the *Groups* section within *Accounts*. Alternatively, click **View > Groups** from the menu bar or use the shortcut of **Shift Command (⌘)P**. Click the plus sign (+) in the bottom left-hand corner of the screen:

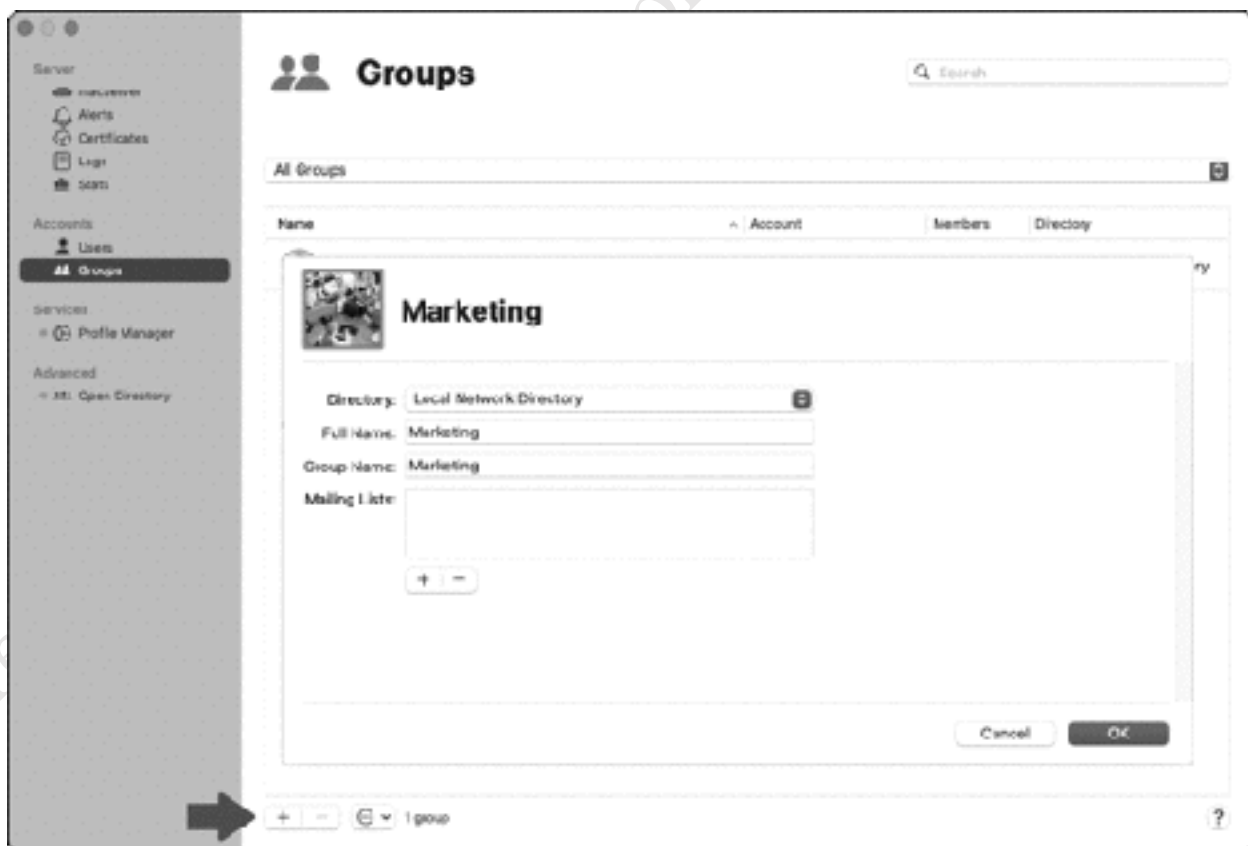
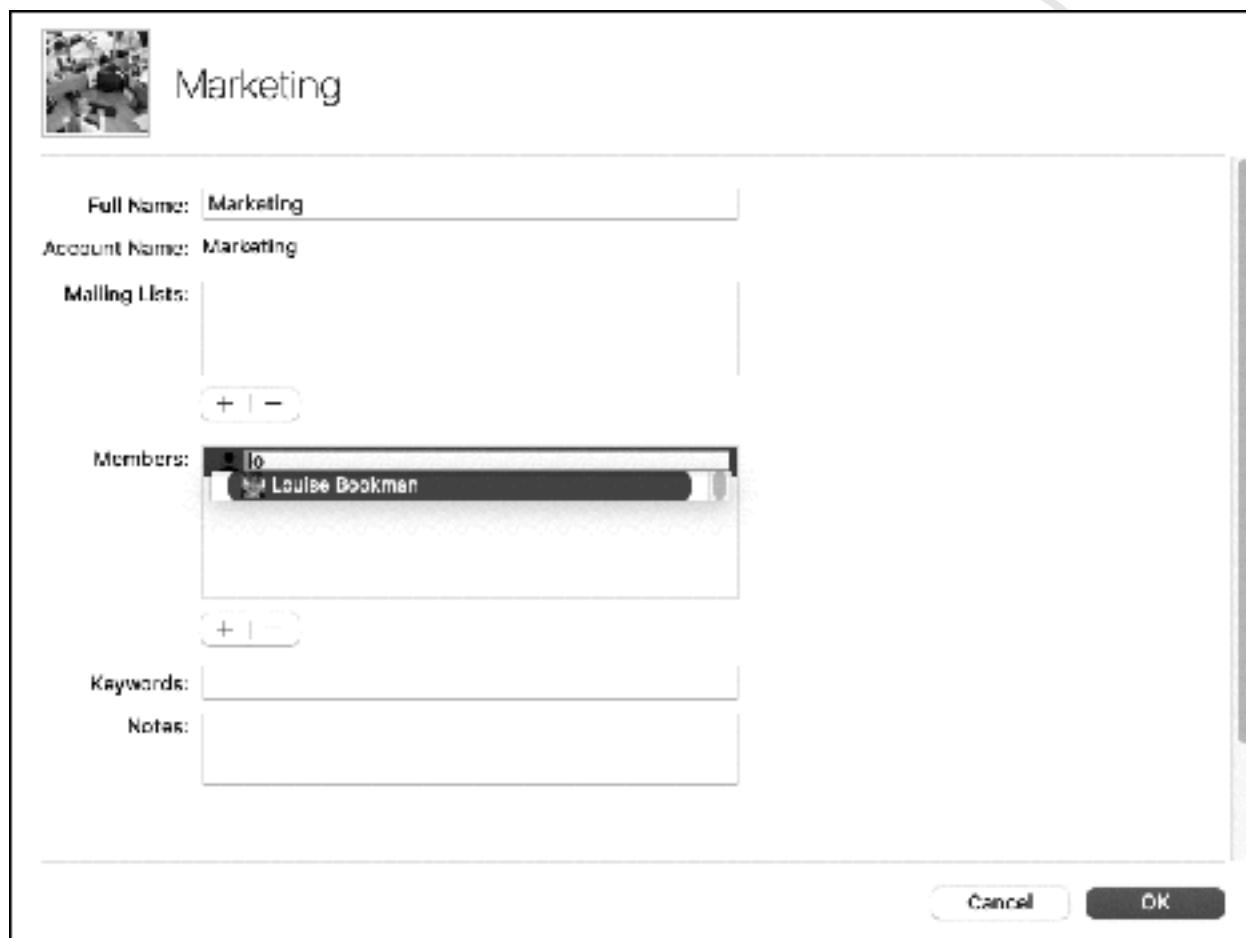


Figure 27: Creating a new Group

As when creating individual users, make sure that the *Directory* is set to **Local Network Directory**. Enter the *Full Name* and the *Group Name* for the new group – you might choose to make them the same, although this is not essential. It is not necessary to specify any Mailing Lists. If you wish, you can assign a picture to the group, in the same way you can when creating an individual user. Click **OK**.

Having created the group, you will be returned to the previous screen, where it will now be listed. The next step is to add the users who will be members of it. Right-click the group and choose **Edit Group** from the pop-up menu to show the following screen:



The screenshot shows a dialog box titled "Marketing" with a small image icon on the left. The dialog contains several fields and controls:

- Full Name:** A text box containing "Marketing".
- Account Name:** A text box containing "Marketing".
- Mailing Lists:** An empty list box with a "+ | -" control below it.
- Members:** A list box containing one member, "Louise Bookman", with a "+ | -" control below it.
- Keywords:** An empty text box.
- Notes:** An empty text box.

At the bottom right of the dialog are two buttons: "Cancel" and "OK".

Figure 28: Editing a Group

To add a user, click the plus (+) sign and begin typing the user's name. Once the system has found the user – and usually it is only necessary to type a few characters from their name – click to add them. Repeat until all the required users have been added, then click **OK**.

One thing to know is that Server has many built-in groups, although most of these are to do with the underlying functioning of the system and are largely invisible in everyday use. However, one

particularly useful group to know about is *Workgroup* – any users created are automatically members of *Workgroup*, so if you want to make something available to everybody, you can give the rights to *Workgroup* (you may have noticed it was already listed on the Groups screen).

4

Shared Folders



Free edition. Do not copy or distribute. (c) CTACS

4.1 Overview

The main purpose of most networks is to provide an environment for users to store and share information. This is done by creating shared folders on the server and defining permissions to control who can access them. The structure of these folders will depend upon the requirements of the household or organization, but a typical starting arrangement might be:

- A shared folder that everyone has access to
- Folders for music, photos and videos (particularly so for a home system)
- A location to store master copies of apps, drivers, utilities and so on

Before proceeding, you should make sure that any additional storage has been connected and configured. An overview of adding storage can be found in section [1.5 Storage and RAID](#); if you are creating your own RAID using plug-in external hard drives, you might want to look at the walkthrough in section [10.5 Configuring Additional Storage for RAID](#).

4.2 Enable File Sharing

Shared folders are created using the built-in facilities of macOS, rather than with a specific tool in Server itself (if you have used earlier versions of Server, this may represent a significant change for you). The first step is to enable file sharing. In **System Preferences**, click **Sharing**, then place a tick against the **File Sharing** option in the left-hand section. Also click the **Options** button and confirm that the **Share files and folders using SMB** box is ticked. SMB is a widely used protocol in networks, used by Macs since macOS 10.9 Mavericks, as well as by most other computer systems (older versions of macOS used Apple's AFP protocol, but this is no longer supported).



Figure 29: Enable File Sharing

Windows Computers

If you have any computers using Microsoft Windows, you will need to do the following on the server. Click the **Options** button within **System Preferences > Sharing**. At the bottom of the panel is a section called *Windows File Sharing*, within which the users that were created in Chapter 3 are listed (see screenshot above). Against each of the users who use a Windows

computer, tick the small box to the left of the user's name. You will be prompted to enter the password which was specified when creating that user to make the change.

Free edition. Do not copy or distribute. (c) CTACS

4.3 Creating Shared Folders

We will start off by creating a new, shared folder that everyone can see and, to make it obvious what it is, we will explicitly call it *shared* (note that this is unrelated to the Shared folder facility provided by iCloud). Shared folders are created using the **System Preferences > Sharing** feature.

Highlight the **File Sharing** Service and underneath the *Shared Folders* area, click the plus sign (+). Navigate to your designated storage area, such as an external drive or RAID storage unit (if you were using a Mac with just the single built-in drive you could use the *Documents* folder). Click **New Folder** and give the folder a name, in our case *shared*, followed by **Create**, then click **Add**:

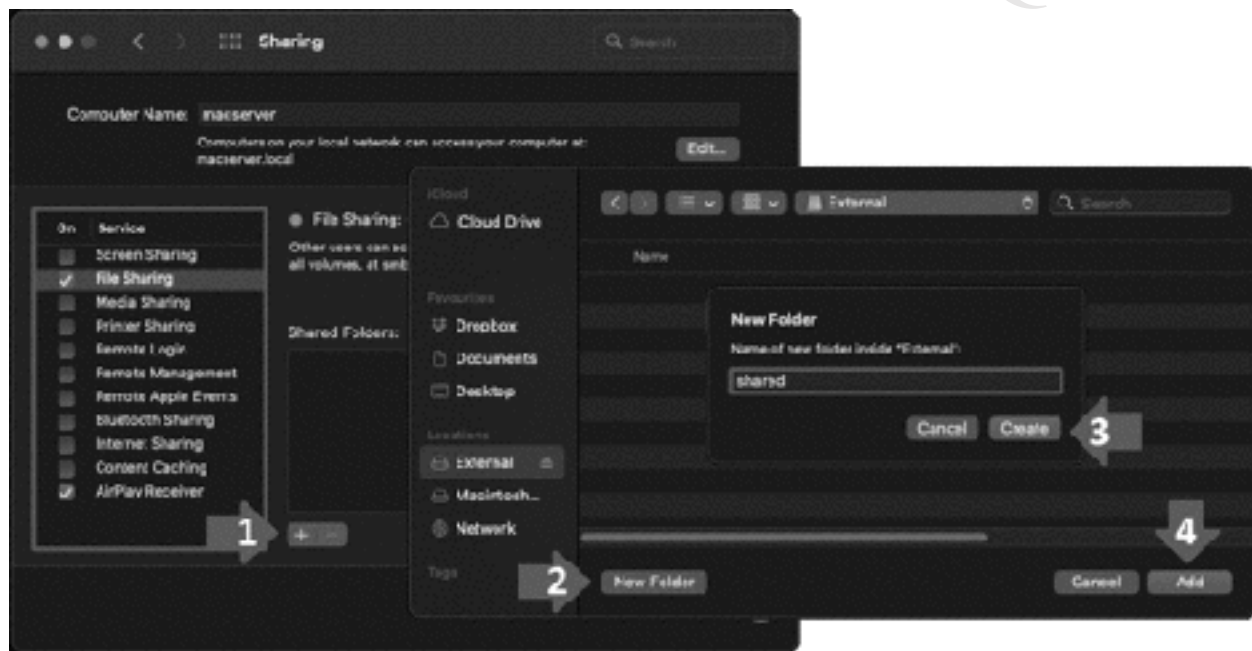


Figure 30: Creating a new Shared Folder

Returning to the main Sharing screen, the folder will now be listed in the *Shared Folders* section. Highlight it and in the *Users* section click the plus sign (+). In the pop-up panel you specify the Network User(s) or Network Group(s) who will have access to the folder. In this instance we want all users to have access, so click *Network Groups* and *Workgroup*, followed by **Select**:



Figure 31: Specifying who has access to a Shared Folder

Next, notice that the Users section of the Sharing screen is split in two. On the left-hand side is the list of user names, whereas on the right-hand side is the type of access they have. There is a choice of three: *Read Only*, meaning that users can work with (read) files in the folder but not modify them; *Write Only*, meaning they can only add new files to the folder (also called a *Drop Box* - not commonly used outside of education and totally unrelated to the cloud service of that name); *Read & Write* i.e. full and normal access to the folder. By default, the system will have given *Read Only* access to the shared folder, whereas we want full access. Click the current access level and change it to **Read & Write**:

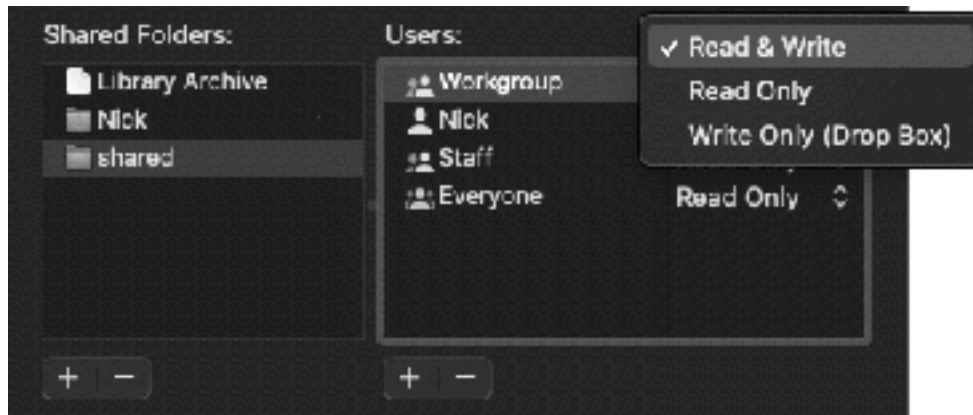


Figure 32: Specify the type of access

Now repeat the process and create additional folders called *music*, *pictures* and *movies* in your designated storage location, along with any other shared folders you require. Make all these available to *Workgroup*, with *Read & Write* access.

Optionally, create a folder called *technical*. This can be used for storing software, utilities, documentation and so on. Give *Read & Write* permissions to *admin* and to the *Administrators* group.

Looking at the main Sharing screen, the list of Shared Folders will now appear along the following lines:



Figure 33: List of Shared Folders

At this point the server should be visible from other computers on the network. If you go to another Mac and open Finder, you should see the server listed in the Shared section. Press **Command (⌘) K** or **Go > Connect to Server** from the menu bar and login as a Registered User with the credentials of a user that you defined in section [3.3 Creating a User](#) – the shared folders should be accessible.

4.4 Making Shared Folders available to Specific Users

Whilst creating shared folders in the previous section, it was assumed that all users (i.e. corresponding to ‘*Workgroup*’) would have access to them, but there may be a requirement to make some folders available to only a selection of users. Doing so involves a slight change to the procedure.

Begin by creating a new shared folder. From within **System Preferences** > **Sharing**, underneath the *Shared Folders* section, click the plus sign (+). Navigate to your designated storage area, such as an external drive or RAID storage unit. Click **New Folder** and give the folder a name e.g. *marketing* in our example, followed by **Create**, then click **Add**:



Figure 34: Creating a new shared folder

Returning to the initial screen, click the plus sign (+) under the Users section. A list of users is displayed – click the one(s) within the *Network Users* section who will be given access to the new folder and click **Select**. Alternatively, choose a group from the *Network Groups* section:

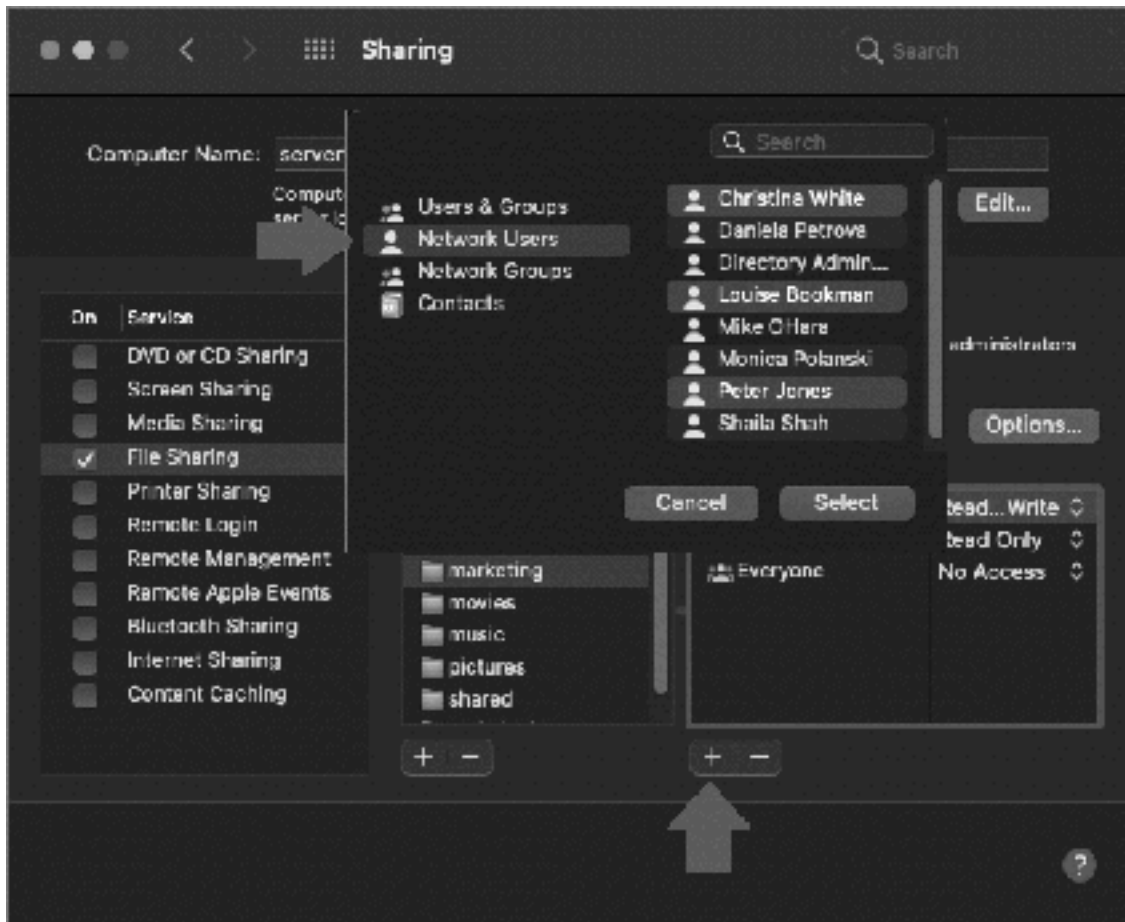


Figure 35: Specifying the users

The newly added names will now appear in the *Users* section; however, their access levels will need changing (depending on your requirements). By default they are Read Only, so change them to **Read & Write**. Then, to prevent unauthorized access by other users, change *Workgroup* and *Everyone* to **No Access**:

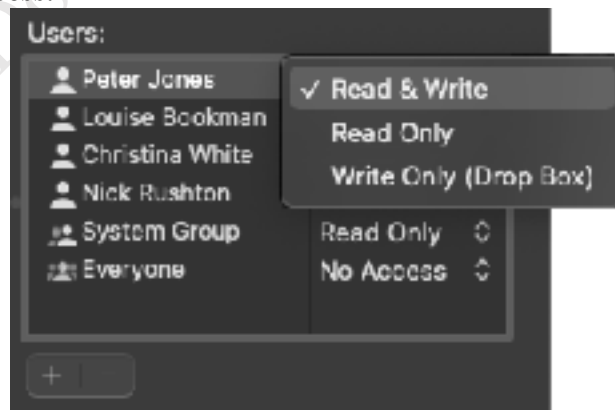


Figure 36: Set the access levels

Another possible use of this technique is to create personal folders for the use of individuals only, similar to a 'home' folder i.e. create a shared folder but set the access level such that only one user can work with it.

4.5 Removing or Changing a Shared Folder

Be aware that in the list of Shared Folders there may be a Public Folder associated with the administrator user on the server, for example *admin's Public Folder*, that can be accessed by other users. Allowing such access is not considered good practice on networks, where an important principle is to control who has access to resources. Highlight the Public Folder and click the minus sign (-) underneath the Shared Folders box – there will be a warning message asking you to confirm that you want to stop sharing it – click **OK**. This does not delete the folder, which could have untoward effects, it simply stops it being shared and reverts it into a standard, non-shared folder. Likewise, you can change who has access and what type of access from here.

It is also worth knowing that although we created our folders in the previous section by using the **System Preferences > Sharing** screen panel, you can create folders by any technique you wish and then use **Sharing** to make them shared and specify the access permissions.

Free edition. Do not copy or distribute.

4.6 Loading Existing Data into Shared Folders

There may be a requirement to load data from existing computers or systems onto the server and 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, login 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 drive. Then, connect the external 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 duplicate data, rather than carry it forward to the new environment.

Free edition. Do not copy or distribute. ©CTA'S

5

Accessing the Server



Free edition. Do not copy or distribute. (c) CTACS

5.1 Overview

There are several different ways of accessing the server:

- From Macs
- Using iPhones and iPads
- From File Explorer/Windows Explorer (Windows PCs)
- Accessing a shared folder using the Run command (Windows PCs)
- Mapping drives manually (Windows PCs)
- Using a batch file (Windows PCs)
- From Linux computers
- From Chromebooks

Free edition. Do not copy or distribute. (c) CTACS

5.2 Macs

Individual Macs need to be ‘joined’ to the network, which enables users to then login to the server rather than to their local computer. For this to work correctly, each Mac in the network must have a unique name. In a small setup, this could be as simple as something like *Mike’s Mac*, *Sue’s Mac*, *Daniela’s Mac* and so on. In a larger setup, a more structured approach is better, perhaps based on location or function or some other classification that is meaningful to the organization e.g. *Class1-01*, *Class1-02*, *Class1-03* or *Accounts01*, *Accounts02*, *Accounts03*. So, when setting up the computers, decide upon and adhere to a suitable naming convention. To check and if necessary change the name of a Mac and its *local hostname*:

Go into **System Preferences** > **Sharing**. Change the *Computer Name* by overtyping it. Then, click the **Edit** button and on the resultant panel check the *Local Hostname*, which should be the same but with a suffix of *.local*. Click **OK**. Whilst not strictly necessary, it is a good idea to restart the Mac at this point.

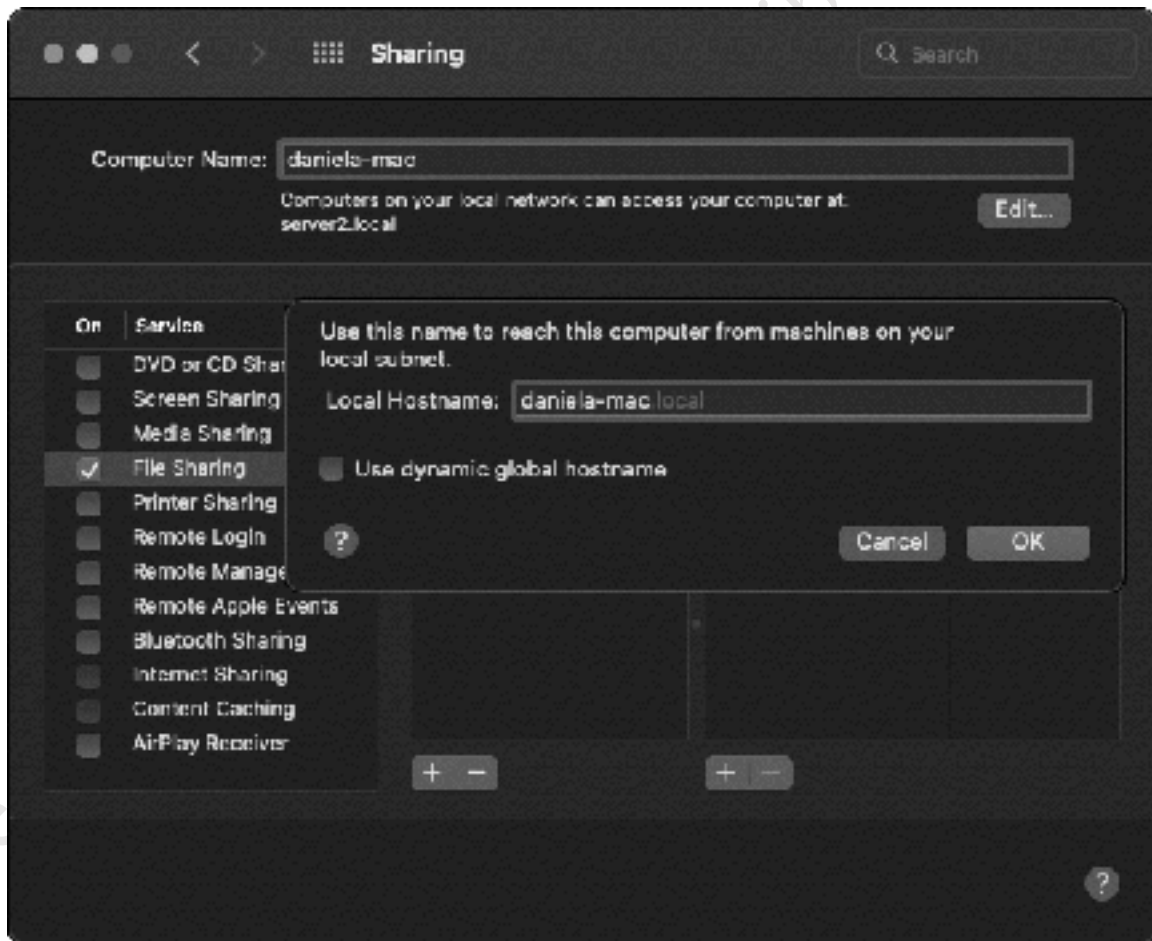


Figure 37: Changing the local hostname of a Mac client

Having made sure that the local hostname is unique, then go into **System Preferences > Users & Groups**. Click **Login Options** – you will need to unlock the padlock so you can make changes, by providing the password for the local admin account on the Mac. Where it reads *Network Account Server*, click the **Join...** button. On the pop-up panel, click the drop-down arrow and select the server, which should be listed:

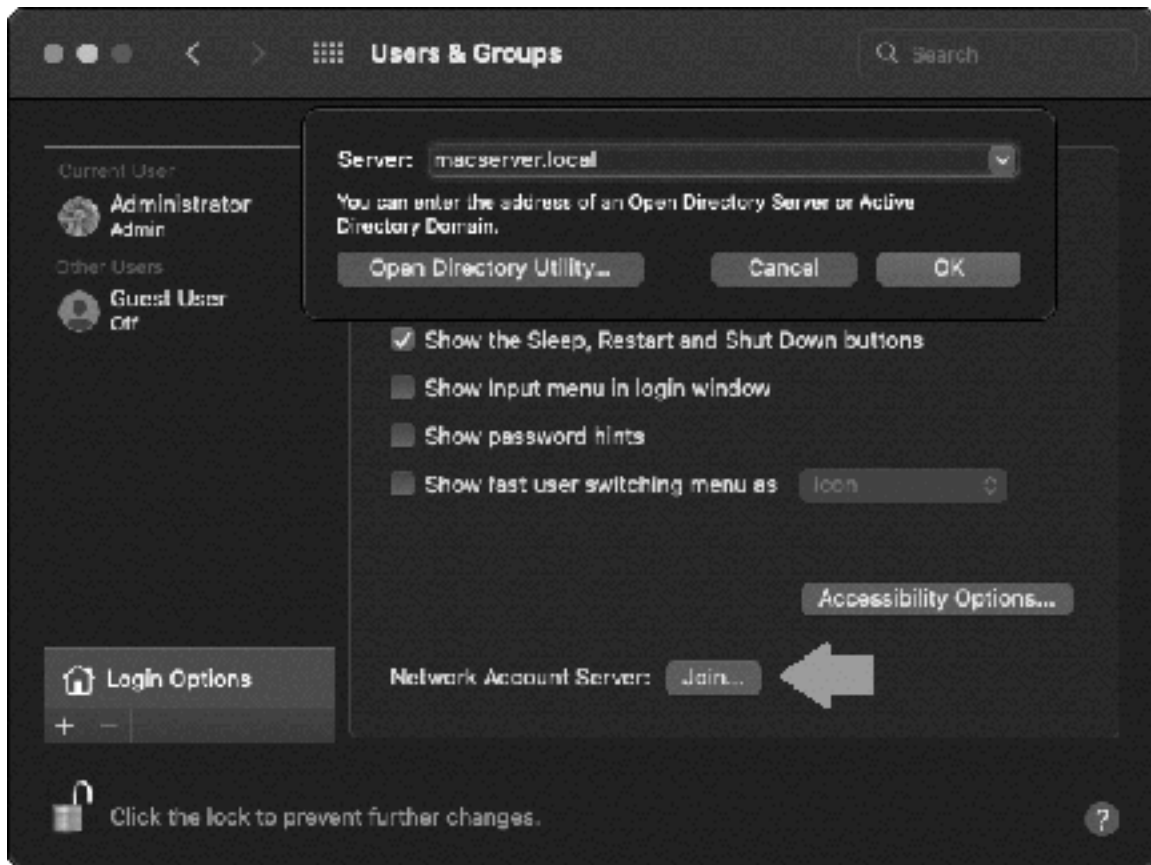


Figure 38: Joining a Mac to the server

Click **OK**. You may receive a message stating asking if you want to ‘trust the certificates’ from the server. You do, so click **Trust** and **Continue** on the subsequent messages. You may also receive a message asking for administrator credentials to modify the Directory Services configuration – provide them and click **Modify Configuration**. The Mac will now join the network; success is indicated by the *Network Account Server* section showing the name of the server, a green indicator and the *Join* button changing from *Join* to *Edit*.

Where it reads ‘*Display login window as:*’ on the *Users & Groups* screen, click **Name and Password** if you have anything more than a handful of users. If you do not do this, the login screen will look very cluttered. Also, make sure that **Automatic login option** is set to **Off** and the **Allow network users to log in at login window** option is ticked. The screen should now look like this (you may wish to close the padlock to prevent further changes):

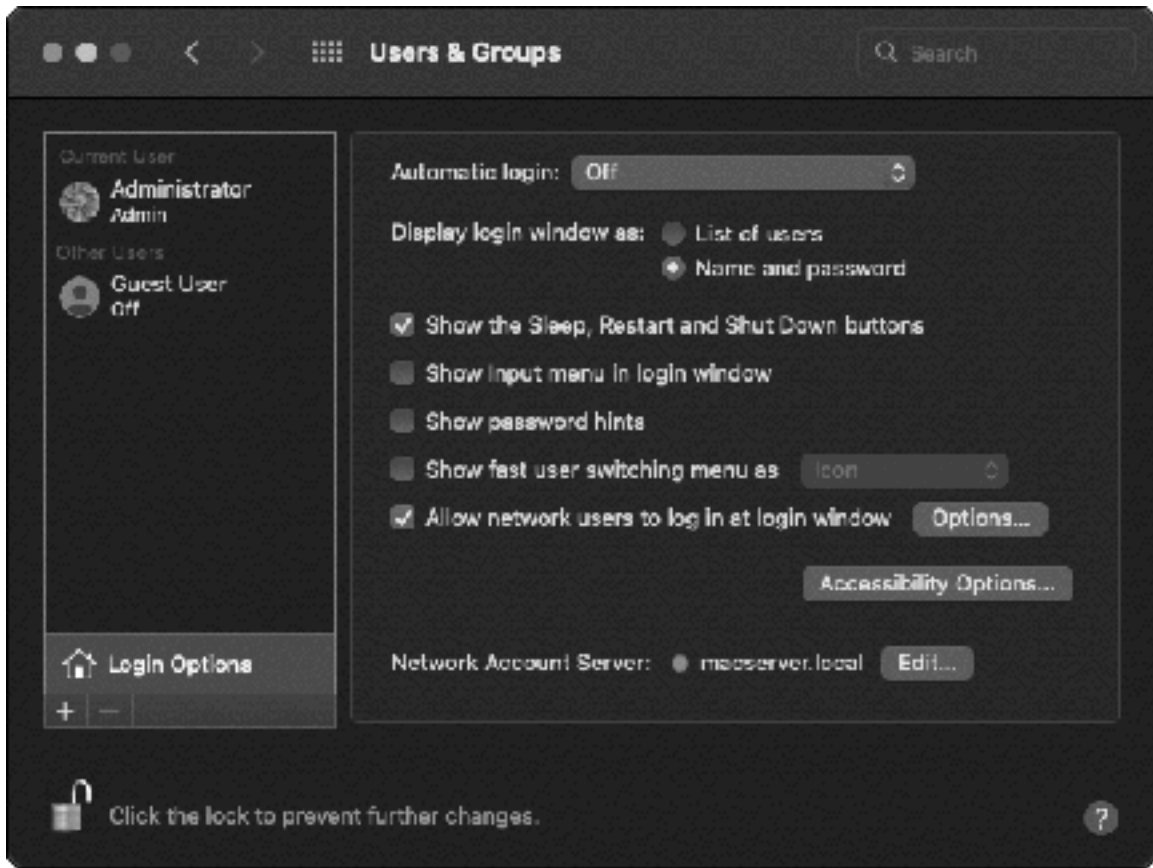


Figure 39: Changing login window options

Close down *Users & Groups* and restart the Mac. When it has restarted, you will be presented with a login screen along the following lines. You may see a message stating that ‘network accounts are available’:



Figure 40: Login Screen

Enter the name and address of any network user to confirm that they can connect to the server. If no users can login, even though you are satisfied that you have done everything correctly, it might well be a DNS issue so change network settings on the Mac to explicitly reference the server (see [10.7 DNS Issues](#) for further information).

Having logged in, the standard desktop is displayed and nothing seems to have changed, with the possible exception of the desktop background. You need to check that you can mount the network folders. From the menu bar click **Go > Connect to Server**, or press **Command (⌘)K**, and in the resultant dialog box enter *server.local* (or whatever your server is called. You can optionally prefix it with *smb://*) and click **Connect**.

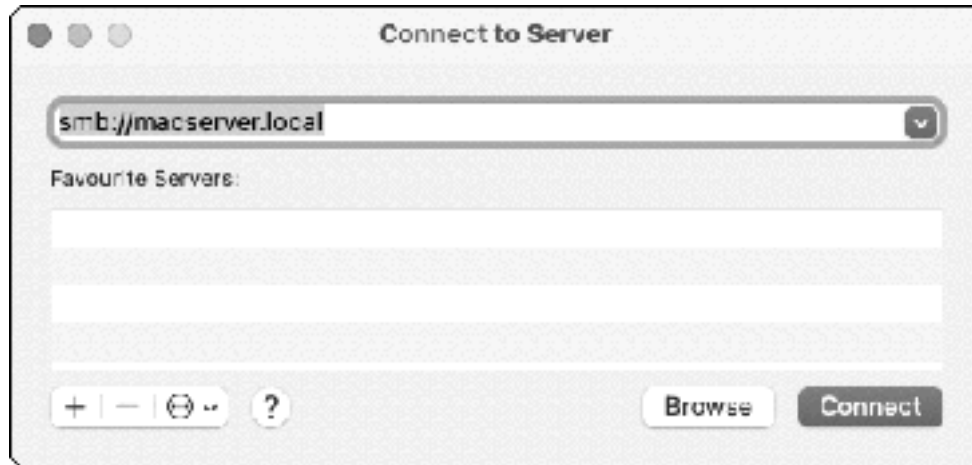


Figure 41: Connect to Server

On the subsequent panel, select the volumes (shared folders) to be mounted. To select multiple volumes, hold down the **Command** key (⌘) whilst clicking each in turn. Click **OK**. Note: the user may be able to see some folders to which they do not have access:

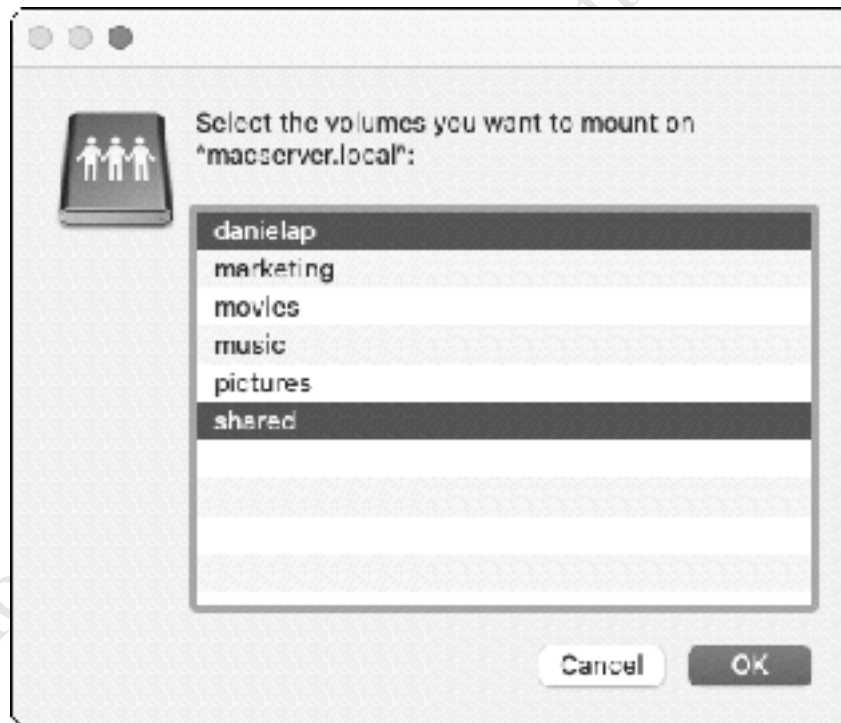


Figure 42: Select the volumes to mount

The volumes will be mounted and opened. If the icons for the volumes are not shown on the desktop, go into **Finder > Preferences** and place a tick against *Connected servers*.

Some people prefer to have the volumes mount automatically when they login. A simple method of doing this is as follows:

- Go into **System Preferences > User & Groups**
- For the *Current User*, click **Login Items** (you will need to click the padlock and authenticate as an admin user to make changes)
- Drag the required volume(s) onto the panel

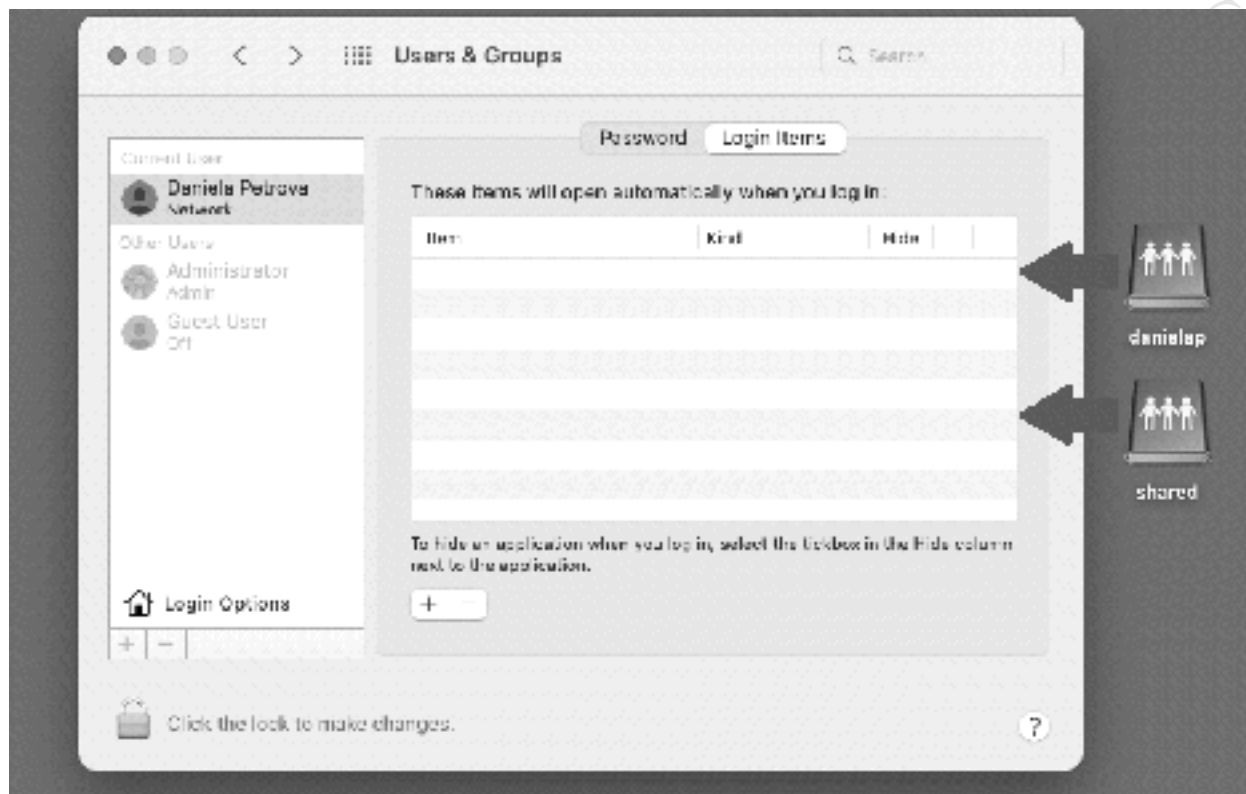


Figure 43: Mount folders automatically at login

Tech-savvy users will probably realize that it is possible to write scripts, use *Automator* or *Profile Manager* to automatically mount volumes, although these are more advanced topics and outside the scope of this guide.

Visit each Mac in turn, join it to the server and confirm that it can login. The first time that a user logs in to the network on a Mac, the process will be slower than usual as several configuration and customization changes are taking place in the background.

5.3 iPads and iPhones

In many organizations and households, iPads and iPhones are connected to the Wi-Fi system solely to obtain an internet connection for browsing and email. With previous iterations of Server, there was considerable support for iOS devices, including email, calendar, contacts, as well as the ability to save and retrieve files created by Pages, Numbers and Keynote. However, in current versions of macOS Server and iOS, most of this functionality has been removed and the focus now is on device management using *Profile Manager*, which is mainly for deploying apps and configuring devices. This is very useful in an educational or business setting, but many home and small business users will only want to access files and folders on the server and in a relatively conventional manner, much as they do with the Macs and PCs. This can be done using the built-in *Files* app in iOS 13 or later. If you have devices running earlier versions of iOS or require additional features, you could use a third-party app, such as *FileBrowser* from Stratospherix.

Note that if you want to use the device management features described in Chapter [8 Profile Manager](#), then you will need to enroll the device as described there.

Files App

The Files App is an integral part of iOS. Launch it, and in Browse mode click the three-dot menu at the top of the screen and tap **Connect to Server**:

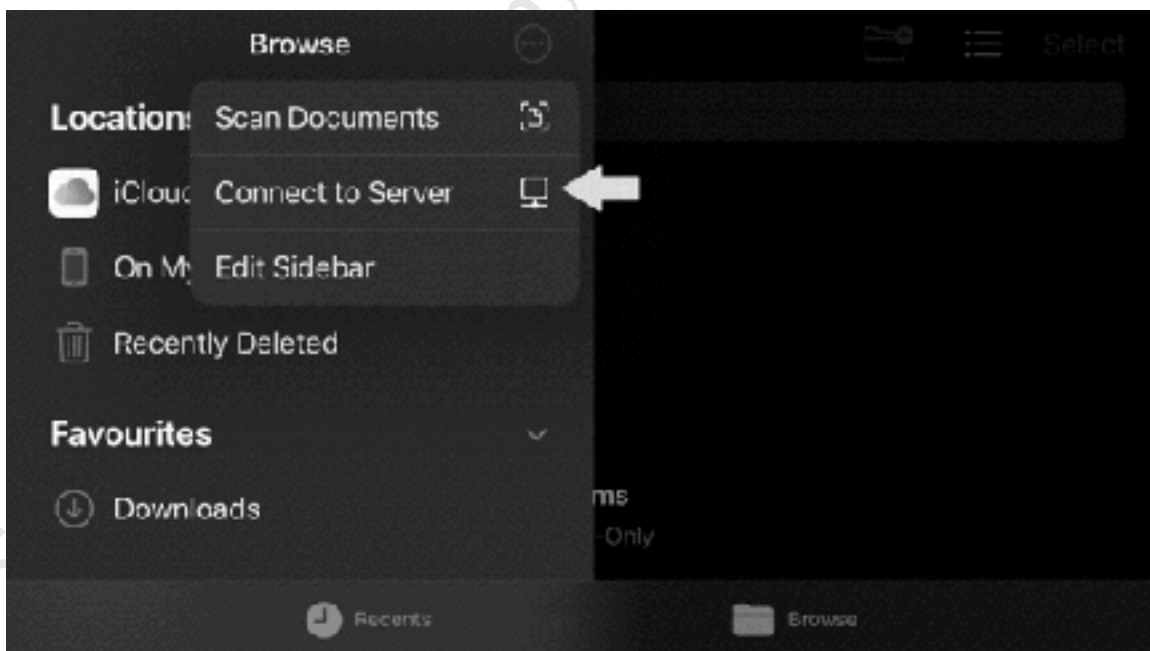


Figure 44: File App on iPhone/iOS

On the subsequent panels: enter the name of the server or its IP address preceded with *smb://* and click **Connect**; choose the **Registered User** option; enter the name and password of a user

that has previously been defined on the server and click **Next**. After a few seconds, you should be connected to the server, from where you can navigate through the file system to locate folders and files:

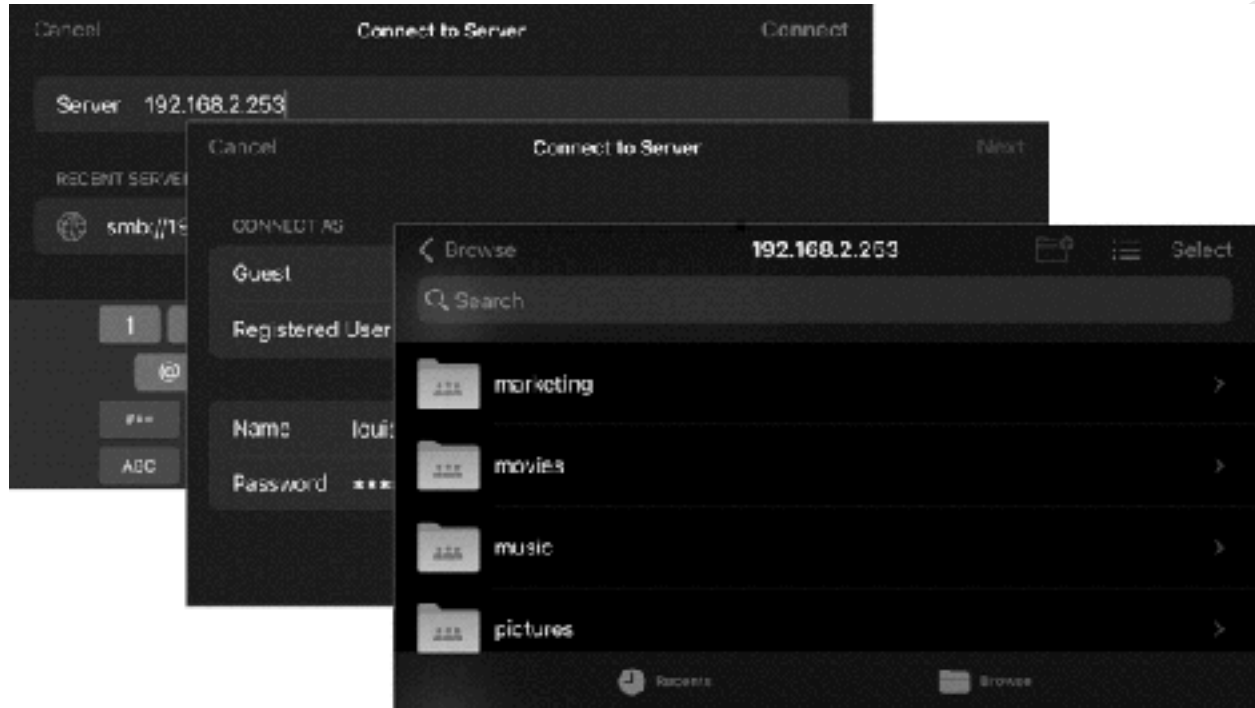


Figure 45: Connecting to and browsing folders on the server

Free edition. Do not copy

FileBrowser

FileBrowser from Stratospherix provides an alternative way of accessing a macOS-based server. It works with a wide variety of iOS versions, including older ones, and provides more features than the built-in Files app. This is a commercial product but is inexpensive, with a basic version at \$6.99 US, a professional version at \$12.99 US, and a subscription version at \$0.49 per month. It operates as a standalone app, but also can be integrated into the iOS Files app. It is not specifically designed for accessing macOS, rather it is a generic tool for accessing any networked computer.

Begin by downloading and installing FileBrowser from the App Store. From the main screen, tap **Add Location** or the Plus Sign (+) in the bottom right-hand corner of the screen:

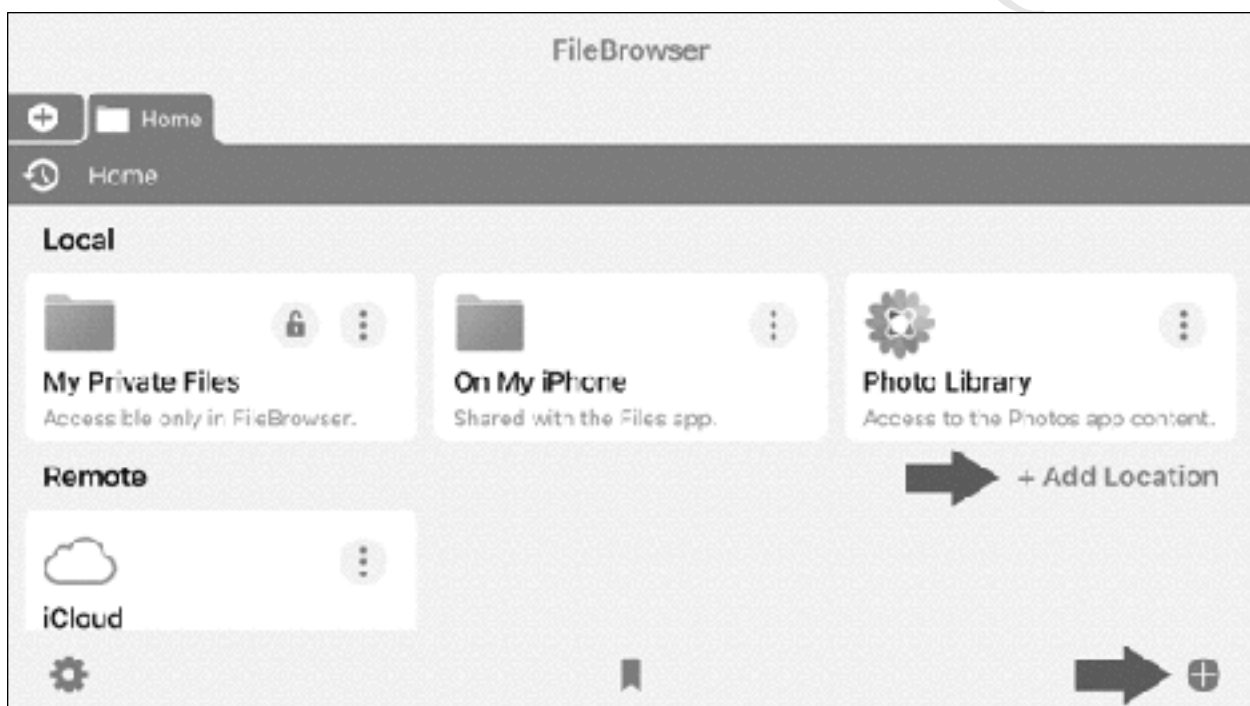


Figure 46: Adding a new location in FileBrowser

On the 'Connect to?' screen, choose **Computer/Network Drive**. File Browser will now scan the network and should find the server Mac. Once it has done so, you can tap **Stop scan**:

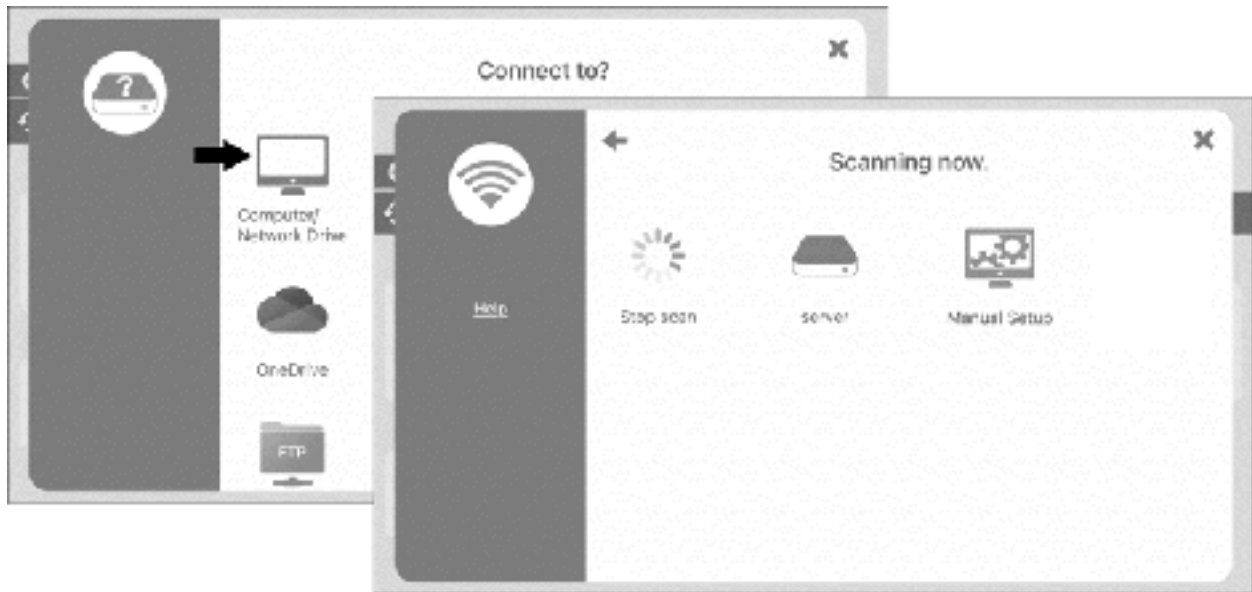


Figure 47: Scanning for the server

On the subsequent screen is for entering the account credentials for the user, as previously defined on the server. The details can be left blank, requested each time, or hard-coded. Having done so, tap **Save**:

Free edition. Do not copy or distribute

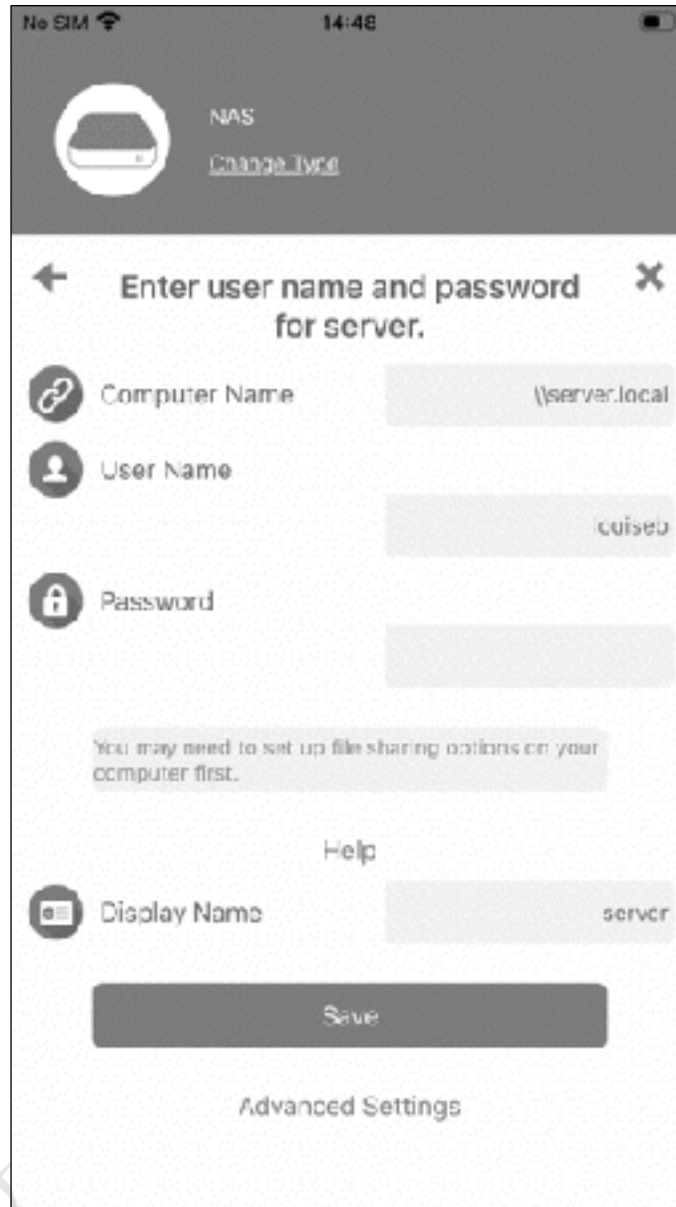


Figure 48: Enter the use name and password

Having successfully logged in, the user can then see any of the shared folders to which they have been granted access. Note that they may be able to see the names of other folders, even though they may not be able to access them because of security restrictions. Files can be viewed, although not necessarily edited, and many common media types (e.g. music and video) can be played. It is also possible to move, copy and download files onto the local device for offline usage.

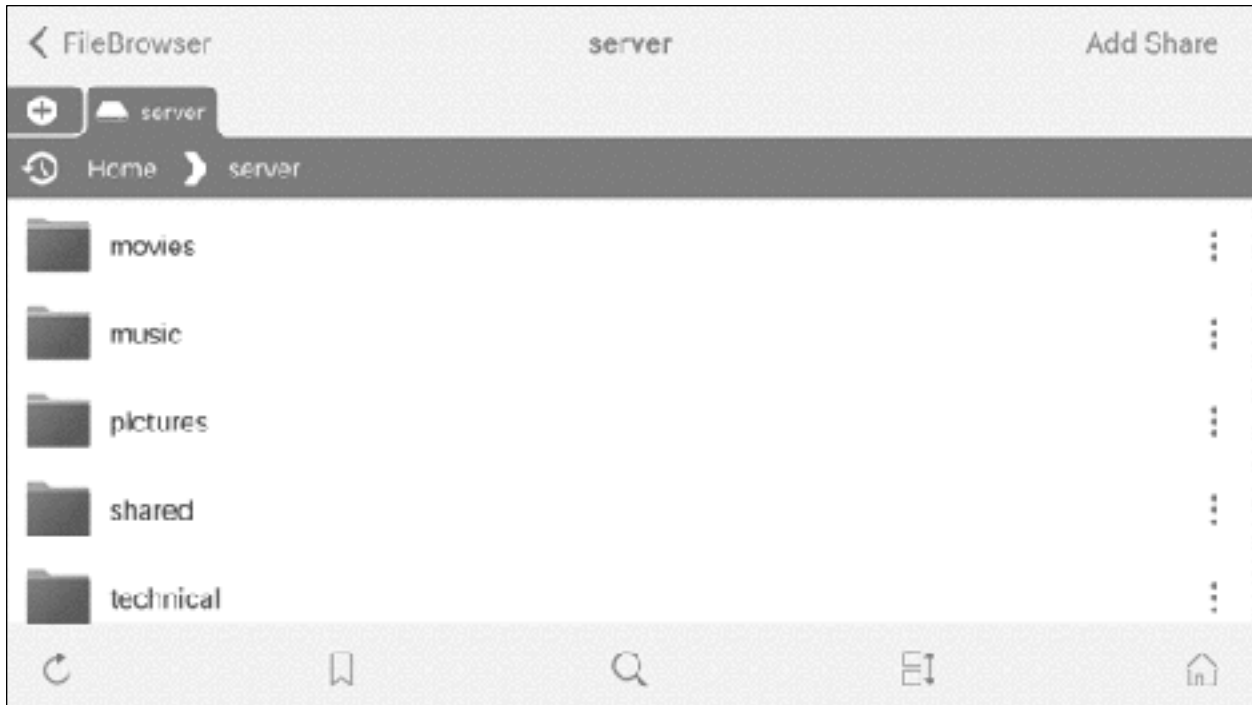


Figure 49: FileBrowser running on iPhone

Free edition. Do not copy or distribute.

5.4 Windows Computers

Windows computers connect to Server in a different manner than Macs, as they are unable to use Open Directory. However, there are several options available for connecting, varying in complexity and convenience. As with Macs, each Windows computer on the network should have a unique name. To change the name of a Windows 11 computer, click **Start > Settings > System > Rename**. For 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**. For a Windows 7 computer, go to **Control Panel > System** and click **Change settings** in the *Computer name, domain and workgroup* settings section.

Using File Explorer/Windows Explorer

A simple way to access the server directly is by going into *File Explorer* (called *Windows Explorer* in older versions of Windows). Expand the left-hand panel to view the Network and down the left-hand side the server should be visible. Click on it and you will be prompted to enter the login details for a user who has been previously defined on the server. If you wish, tick the option box to remember the login credentials, although you should only do this if you are the sole user of the computer.

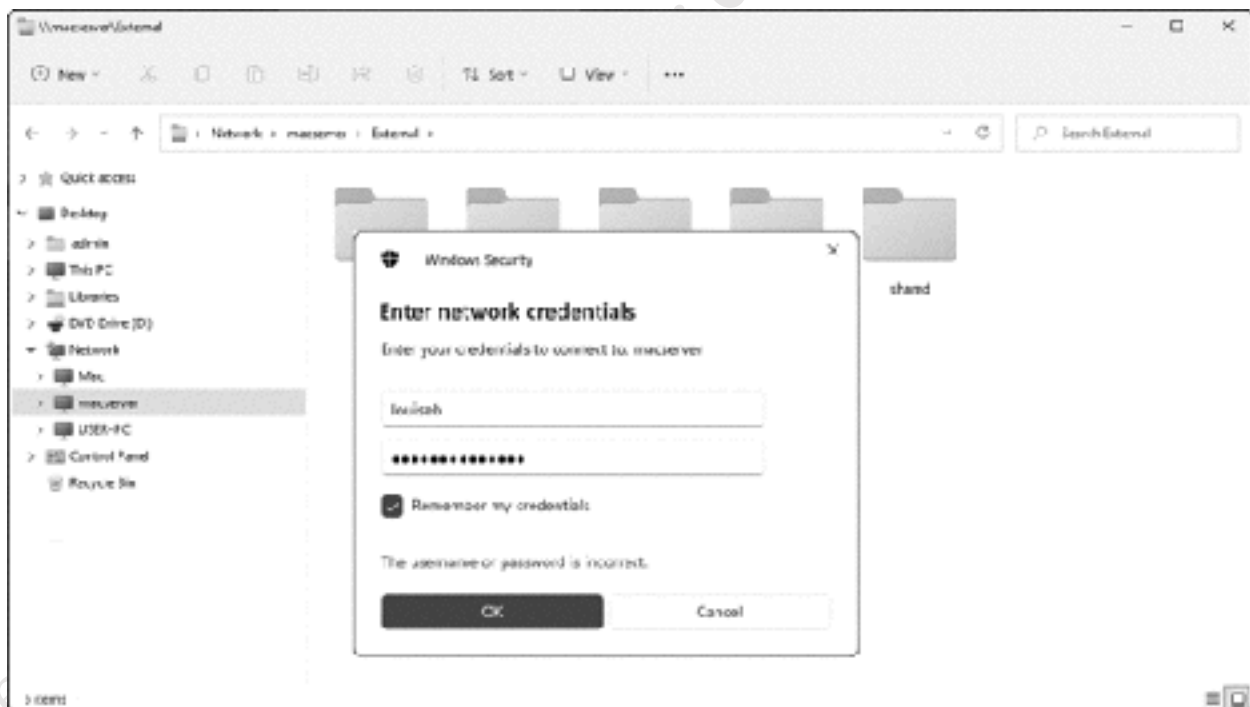


Figure 50: Enter the username and password

The list of shared folders on the server will be displayed, allowing access to the files within them in the normal manner. Although many shared folders may be visible, you can only access the ones to which you have appropriate access rights.

Accessing Shared Folders using the Run Command

To access a shared folder from a Windows computer, right-click the **Start** button and choose **Run** (Windows 11, 10 or 8.1) or click **Start** button and choose **Run** (Windows 7). Alternatively, hold down the **Windows key** and press the letter **R**. In the small dialog box that appears, type in the name of the shared folder using the format `\\server\name_of_folder` e.g. `\\server\shared` then click **OK**.

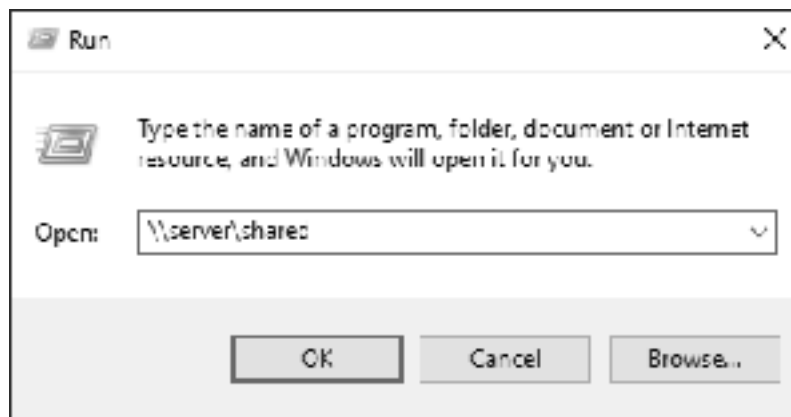


Figure 51: Using the Run Command

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

Mapping Drives Manually

The techniques considered so far provide access to shared folders by referring to them using what are called UNC or *Universal Naming Convention* names, which take the form of `\\server\shared`. However, many Windows users are accustomed to and prefer to use drive letters, such as C:, D: and so on. The process by which a UNC name can be turned into a drive letter is known as *mapping* and there are several ways to go about it, discussed in the following sections. You can use whatever drive letters you wish, provided they are not already in use (for instance you cannot use C as that is always in use on a Windows computer). However, using sensible letters makes things easier, for example:

Drive	Folder
M	\\server\music
P	\\server\pictures
S	\\server\shared

The first method uses File Explorer and varies between different versions of Windows.

Windows 11

Open File Explorer, which appears on the Taskbar by default. Expand the left-hand panel to view the Network and click the server to display the list of shared folders. Note: you may be prompted to enter a valid user name and password as previously defined on the server. If you wish, tick the option box to remember the login details, although you should only do this if you are the sole user of the computer. Right-click the shared folder and choose **Show more options**, followed by **Map network drive**. On the resultant panel, specify the Drive letter using the dropdown and click **Finish**. Upon a successful connection, the contents of the newly mapped drive will be displayed. The process should now be repeated for each folder that the user needs access to.

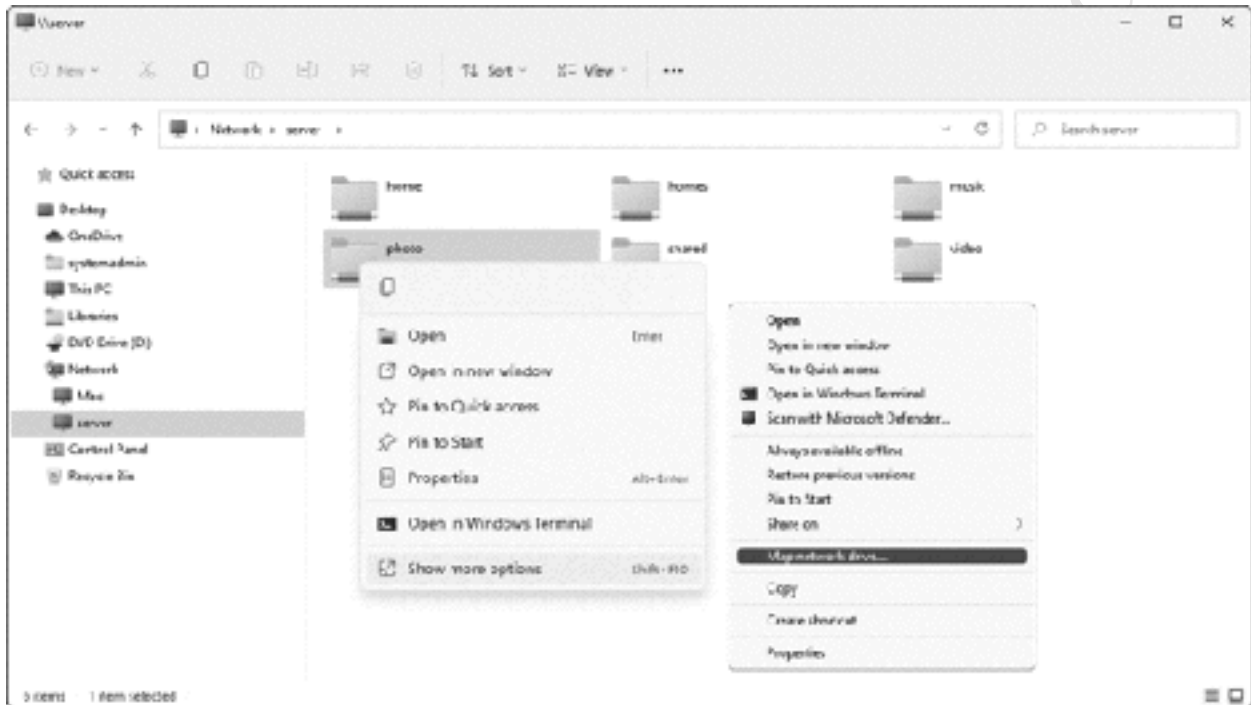


Figure 52: Mapping a drive in Windows 11

Free edition. Do

Windows 10

Open File Explorer, which appears on the Taskbar by default. Expand the left-hand panel to view the Network and click on the server to display the list of shared folders. Note: you may be prompted to enter a valid user name and password as previously defined on the server. If you wish, tick the option box to remember the login details, although you should only do this if you are the sole user of the computer. Right-click the shared folder and on the pop-up menu click **Map network drive**.

On the resultant panel, specify the Drive letter using the dropdown and click **Finish**. Upon a successful connection, the contents of the newly mapped drive will be displayed. The process should now be repeated for each folder that the user needs access to.

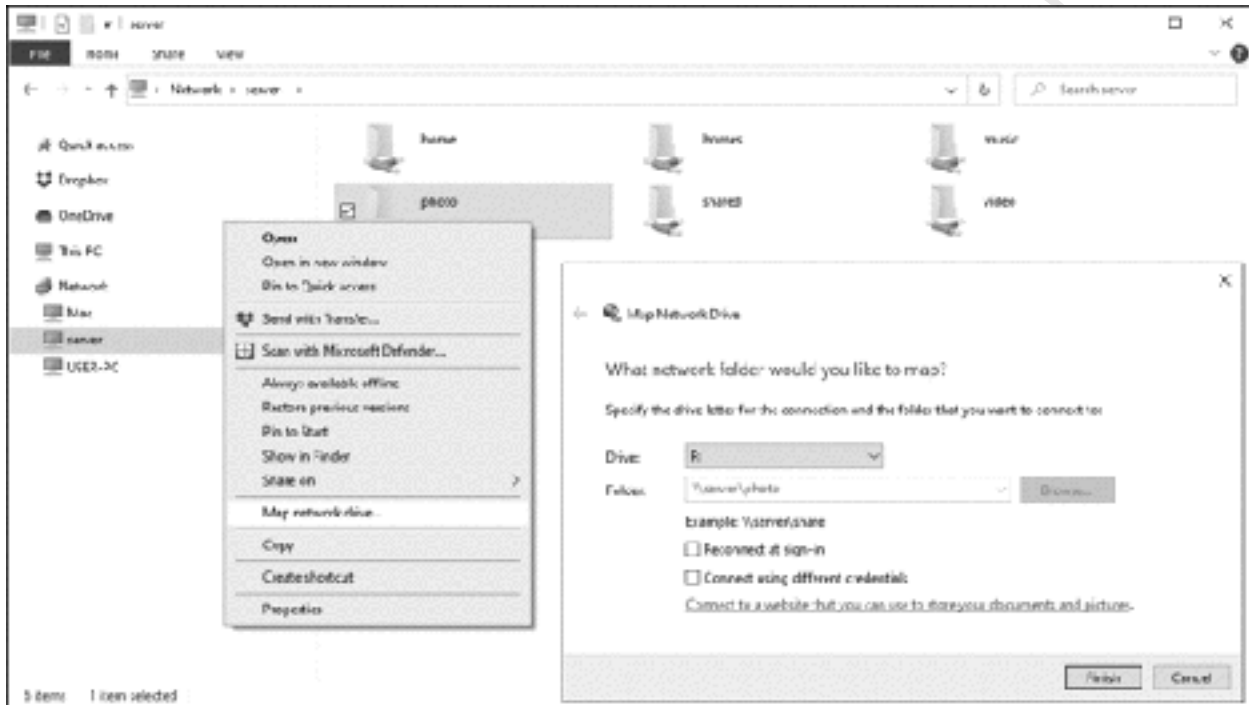


Figure 53: Mapping a drive in Windows 10

Windows 7

Open Windows Explorer, which usually appears on the Taskbar by default, else click **My Computer** on the Start menu. If the menu bar is not displayed, click **Organize > Layout > Menu bar** to display it. Expand the left-hand panel to view the Network and click on the server to display the list of shared folders. Note: you may be prompted to enter a valid user name and password as previously defined on the server. If you wish, tick the option box to remember the login details, although you should only do this if you are the sole user of the computer. Right-click the shared folder and choose **Map network drive**. On the resultant panel, specify the Drive letter using the dropdown and click **Finish**. Upon a successful connection, the contents of the newly mapped drive will be displayed. The process should now be repeated for each folder that the user needs access to.

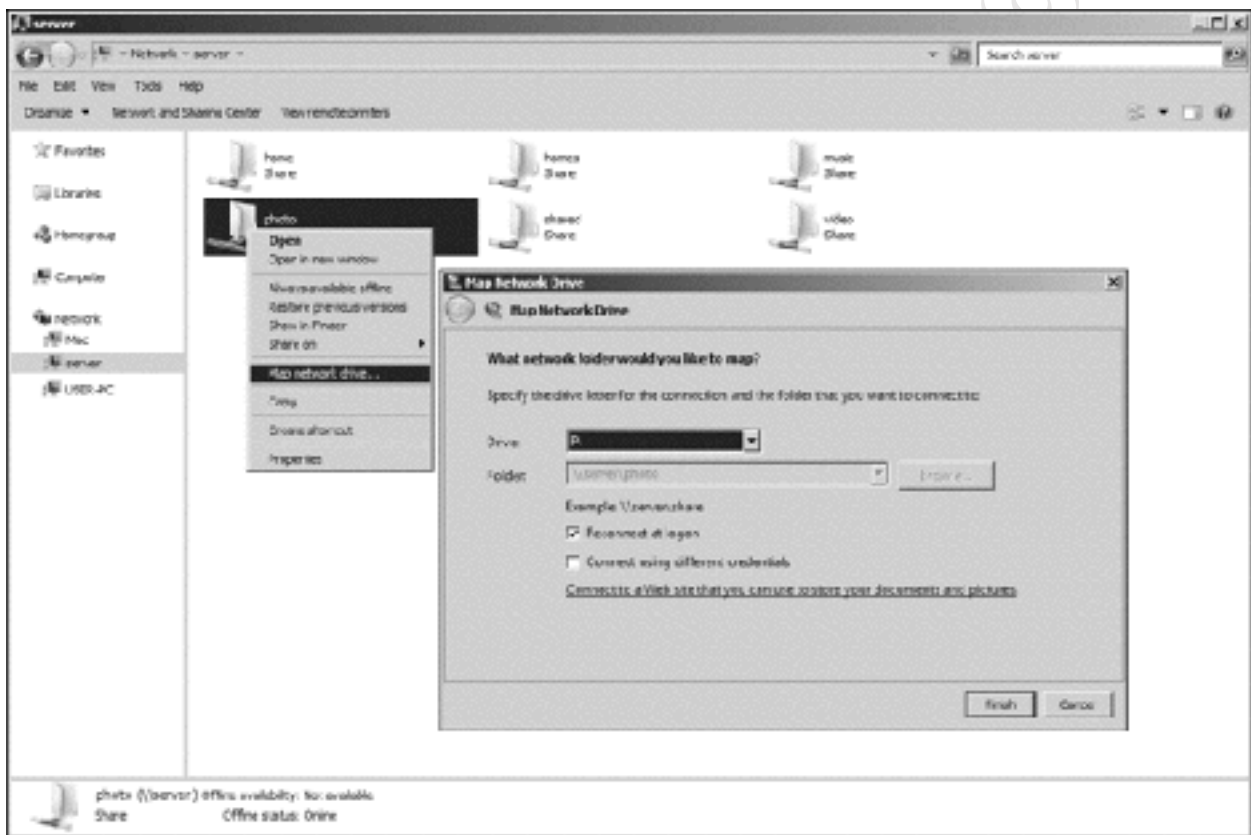


Figure 54: Mapping a drive in Windows 7

Using a Batch File

Setting up a batch file is a more advanced technique for Windows PCs but can be useful when a particular computer is used by more than one person. As such, it is probably of more benefit in a small business environment or school rather than in a home system. Start off by creating a plain text file called *Connect.cmd* using a tool such as Windows WordPad or Notepad. The contents of the file will need to vary depending on the folders to be mapped or if the server is not called 'server'. In this example, there are three shared folders called *music*, *photo* and *shared*:

```
@echo off
cls
ping server -n 1 > nul
if errorlevel 1 goto offline
:online
: remove any drive mappings already present
net use * /delete /y > nul
: prompt for username and password
set /p uname=Enter Username: %=%%
set /p upwd=Enter Password: %=%%
: map the drives
net use m: \\server\music /persistent:no
net use p: \\server\pictures /persistent:no
net use s: \\server\shared /persistent:no
goto end
:offline
cls
echo You are not connected to the network.
echo If you are outside the premises then this is expected.
echo If you are inside the premises then it means there is a problem.
echo Data stored on the network is not currently available.
pause
:end
```

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

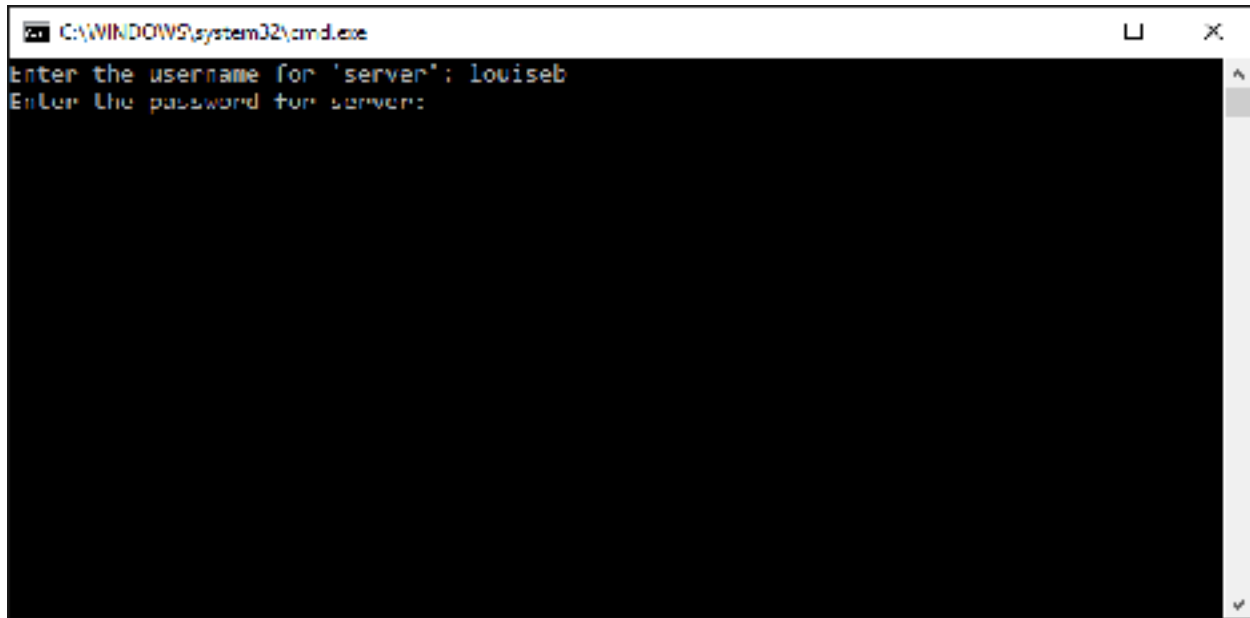


Figure 55: Enter the username and password

After the user has successfully entered their details, the mapped drives will be available until the computer is shutdown or they logoff using the Start menu. The drive mappings can be verified by launching Windows Explorer/File Explorer, which appears by default on the Taskbar in Windows 7 and later versions.

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

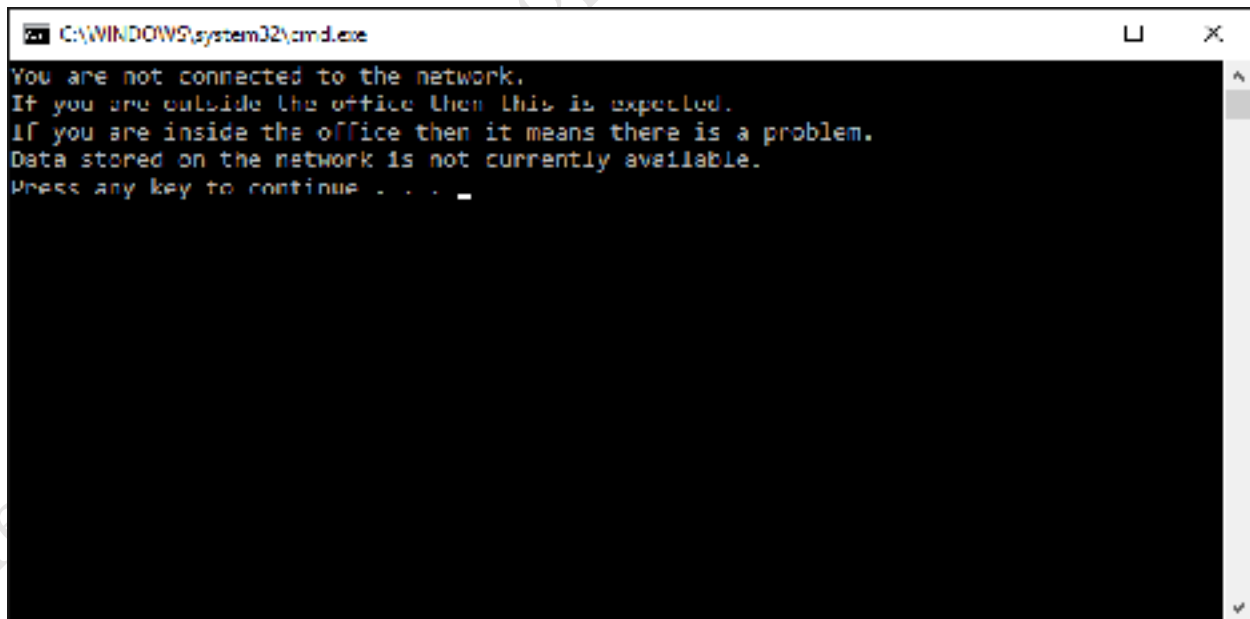


Figure 56: Warning message if not connected

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

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

Ideally, computers should be setup with only one Windows user defined on them. If this is not the case, then the *Connect.cmd* file needs to be placed in *C:\Users\Public\Public Desktop*, which will cause it to appear on the Desktop for all users. The Public Desktop folder is a hidden folder and will therefore first need to be made visible before it can be used. To do this, go to **Control Panel** on the computer and choose **Folder Options** or **File Explorer Options** depending on your version of Windows. Click on the **View** tab, enable **Show hidden files, folders and drives** and click **OK**. Copy the *Connect.cmd* file to the Public Desktop folder, then make the Public Desktop folder hidden again.

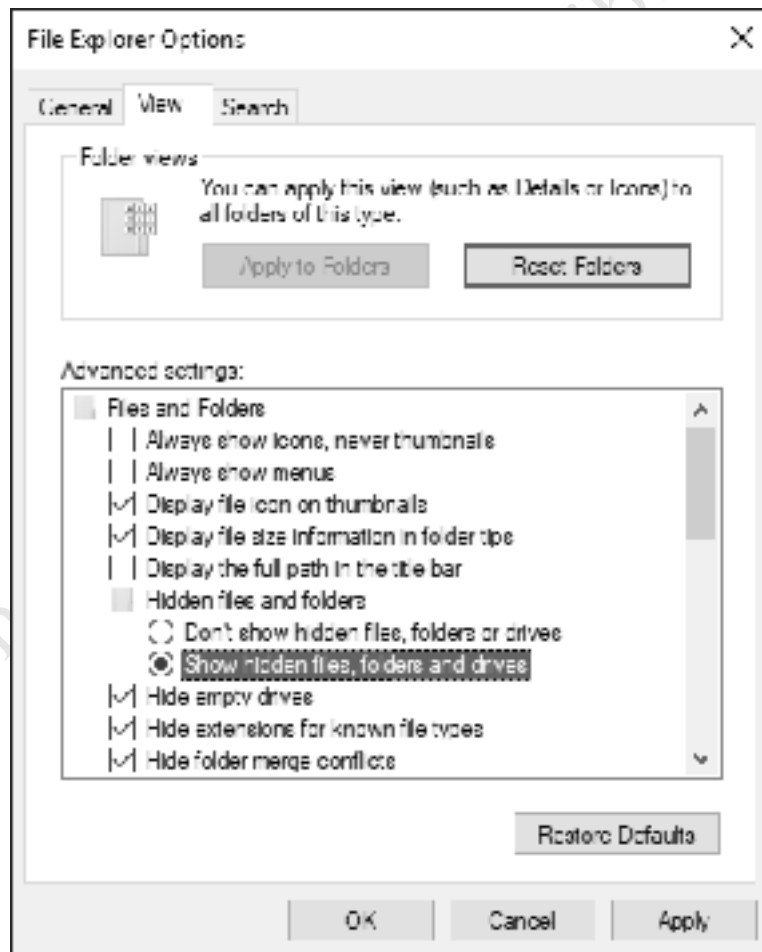


Figure 57: Folder Options to view hidden files

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

Troubleshooting Connection Problems with Windows

Suggestion #1: Reboot the PC. Windows computers broadcast their availability to other computers on the network, but there are sometimes delays and anomalies associated with this process. Rebooting a computer will generally force it to 'see' the server.

Suggestion #2: If the server cannot be seen from File Explorer, try referencing it using the local IP address rather than its name e.g. \\192.168.1.2 rather than *server*.

Suggestion #3: Check that the users have been enabled for Windows File Sharing, as described in section [4.2 Enable File Sharing](#).

Suggestion #4: Make sure that the Windows computers are members of *Workgroup* (they invariably are but may possibly have been configured for a different group). This can be checked and changed if necessary by going into **Control Panel > System** on each computer.

Suggestion #5: Disable use of Internet Protocol Version 6 (TCP/Ipv6) if using Windows 7: right-click the network adapter on the taskbar, click **Open Network and Sharing Center > Change adapter settings**. Right-click adapter and click Properties.

Suggestion #6: If you are using a batch file to map drives but it is not working, then the most likely problem is that there may be a typo – check spellings, spaces and the use of percentage (%) signs.

Suggestion #7: Turn off the firewall. On Windows 7 computers, go into **Control Panel > Windows Firewall > Turn off Windows Firewall**. On Windows 10 computers, click **Start > Settings > Update & Security > Windows Security > Firewall & network protection**. Click **Private network** and set the **Microsoft Defender Firewall** switch to the **Off** position. Acknowledge the *User Account Control message* by clicking **Yes**. On Windows 11 computers, right-click **Start** and choose **Network Connections**. Click **Advanced network settings** followed by **Windows Firewall**. Click **Private network** and set the **Microsoft Defender Firewall** switch to the **Off** position. Acknowledge the *User Account Control message* by clicking **Yes**.

Important: you should never turn the firewall off for public networks.

5.5 Linux Computers

Most Linux distributions include support for the SMB filing system used by macOS Server; this is usually built-in or can be added by downloading what is commonly described as a Samba client. The following example is based around a popular Ubuntu distribution.

On the Linux computer, click on the **Files** icon, followed by **Other Locations**. The server should be listed under the Networks section; click on it and on the resultant panel, enter the user's name and password as defined on the server and click **Connect** (the *Domain* field can be ignored). The shared folders on the server will be listed. To access one, double-click it. 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 standard manner.

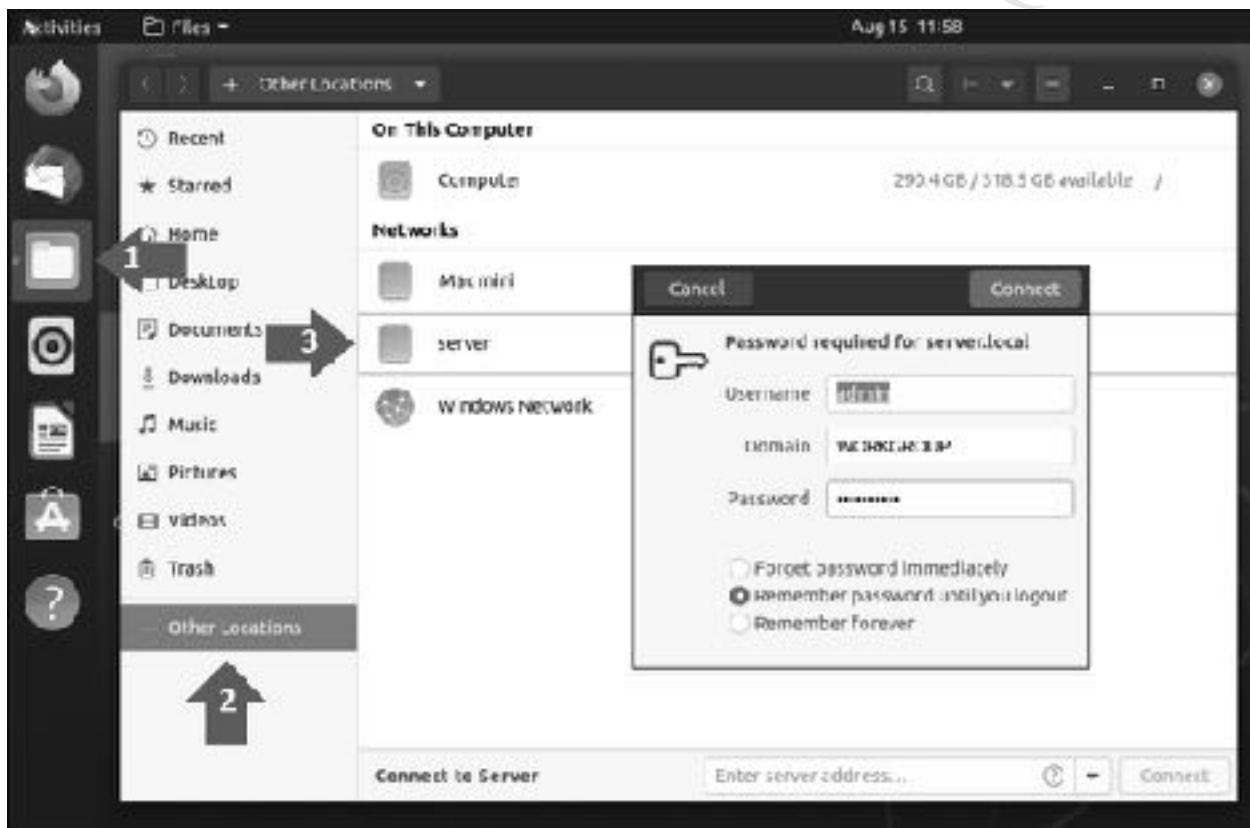


Figure 58: Enter the address of the server

5.6 Chromebooks

Chromebooks are a popular computing choice, particularly in education. In essence a Chromebook is a laptop that primarily runs Google's Chrome browser, and the underlying operating system is minimalist compared to macOS or Windows. Although there are no specific features for working with macOS Server, Chromebooks can connect to the SMB-based file shares that it provides.

To access the folders and files on the server, use the Chromebook *Files* utility. Click the three-dot menu icon followed by **Add new service** > **SMB file share**. On the resultant panel, enter the File share URL e.g. `\\server\shared`, an optional Display name, plus the Username and Password of a user that has been defined on Server. Optionally, tick the **Remember sign-in info** box. Click **Add**. The shared folder will now be added to the Chromebook's filing system.

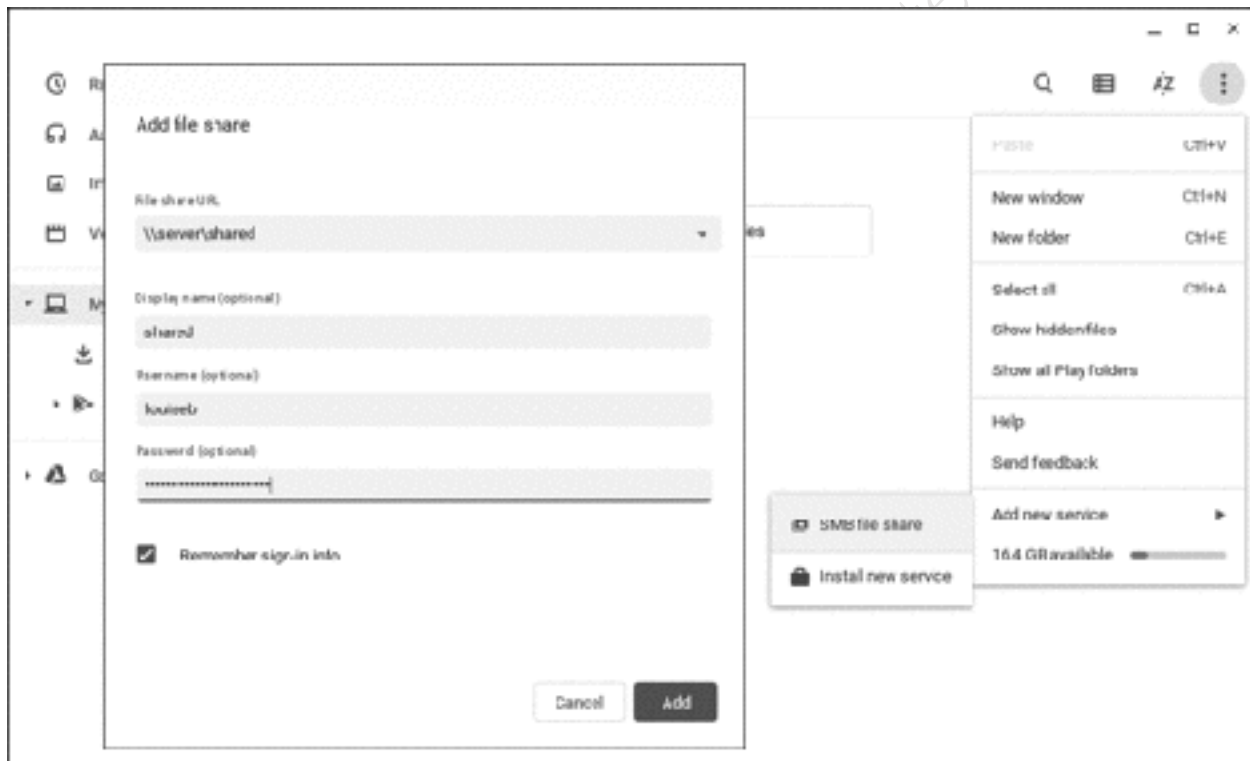


Figure 59: Adding a file share

5.7 Android Smartphones and Tablets

Most Android smartphones and tablets do directly not recognize network drives. However, these capabilities can be added by downloading a suitable app from the Play Store. Typically, these apps have names such as 'File Manager', 'File Explorer' or variants thereof. One example is ES File Explorer; although most people use it for exploring and managing the file system on their device, it also understands SMB-based network systems, such as macOS. The basic app is free; it includes advertisements, but it is possible to upgrade to remove them if they are considered intrusive, plus add further features.

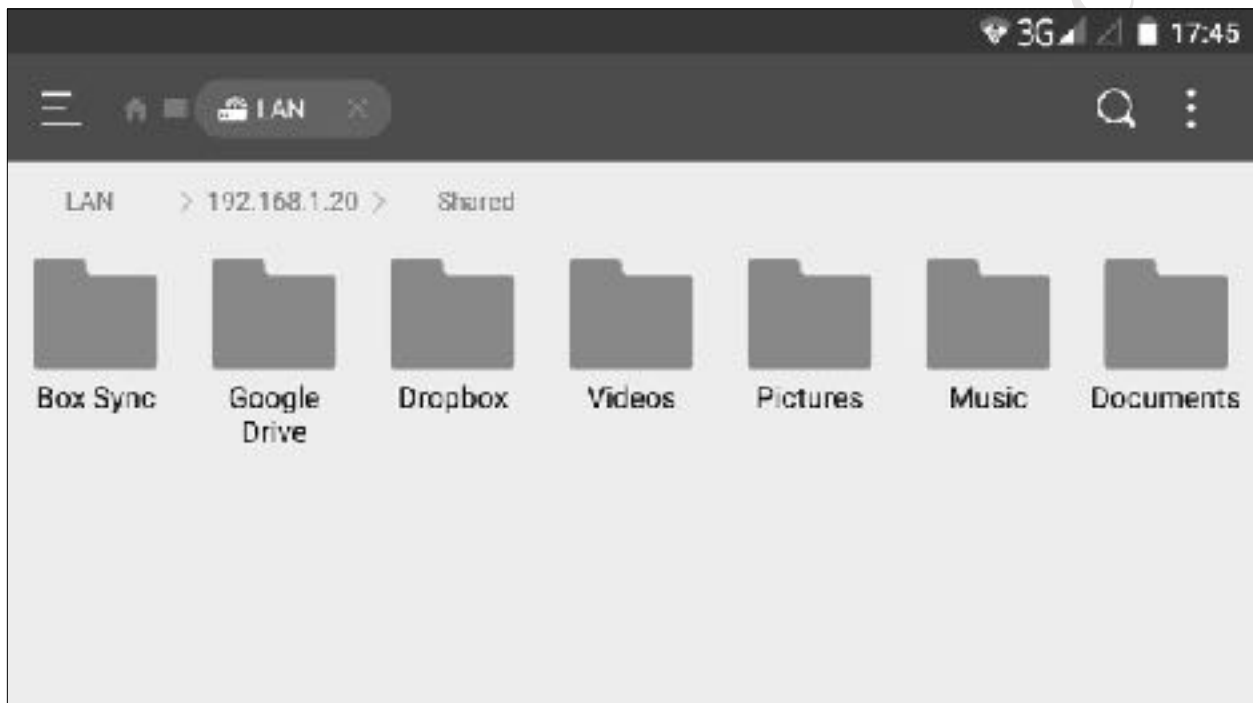


Figure 60: ES File Explorer running on Android phone

6

Backups



Free edition. Do not copy or distribute. (c) CTACS

6.1 Overview

It is important to backup data on a regular basis, to cope with the possible problems that can arise with computers. Examples of things that can go wrong include deleting files by accident; data corruption; virus and malware infections; computer failure; equipment being lost or stolen. In general, the value of data far outweighs the value of the computers; for instance, what price could be attached to the irreplaceable photos of a Wedding Day, children's first steps or other important occasion? In the case of businesses, around half that have a serious data loss subsequently cease trading within twelve months, plus there may be statutory requirements to retain certain data and be able to produce it when required 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.

Backups are like pay rises or happy memories – you cannot have too many of them. A server-based system forms the ideal heart of any backup solution and enables you to implement a multi-tiered approach. Basically, that means there are multiple backups to multiple places, ensuring that there is always a fallback plan in the event of problems. For instance:

The computers in the home or office are backed up to the server. The server in turn is backed up to a local external hard drive. Optionally, the server or at least the most important data on it are backed up to a Cloud-based service such as OneDrive or Dropbox (information about using these services can be found in Chapter [9 Using Cloud Storage Services](#)).

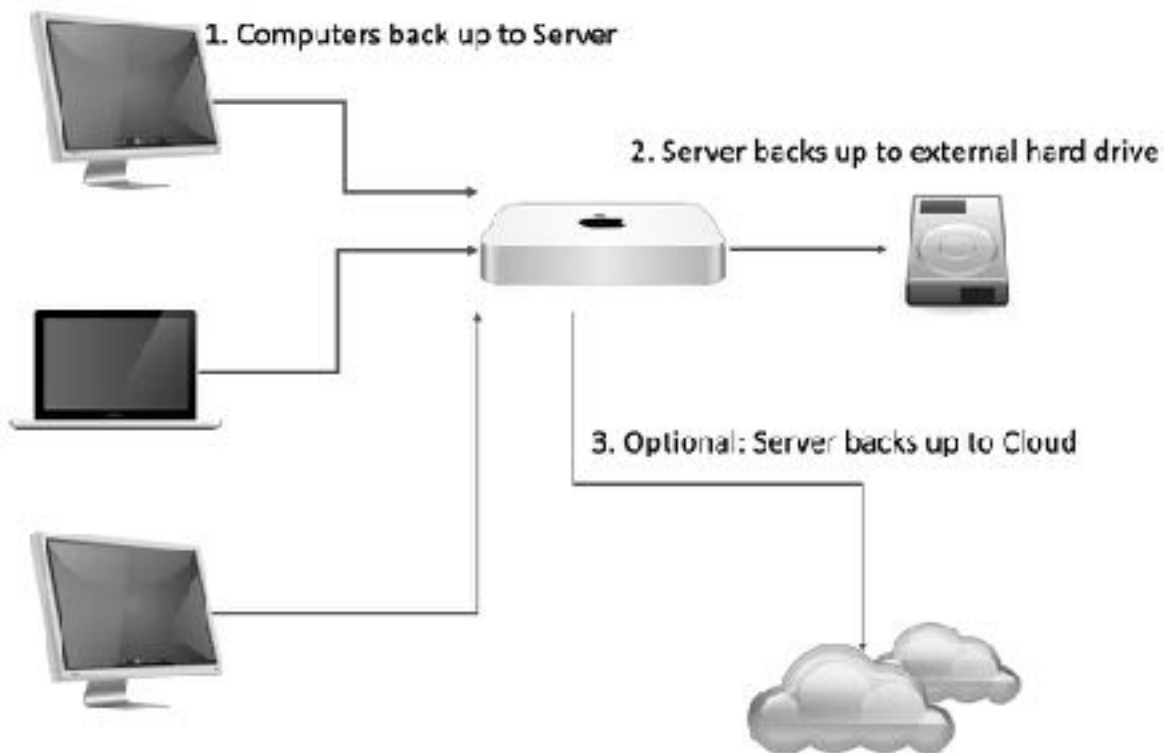


Figure 61: A comprehensive backup regime

The standard backup program in a Mac environment is *Time Machine* and, as with any Mac, the server can use Time Machine to backup to an external drive (there is no need for an additional or specific backup program for Server). Additionally, the server can be configured to provide Time Machine services itself, enabling it to appear to other Macs as a Time Machine destination for their backups. These two separate instances of Time Machine should be understood and kept in mind.

Free edition. Do not copy or distribute. (c) CTACS

6.2 Backing Up the Server using Time Machine

The server Mac is backed up using Time Machine and this requires an external drive of some type, such as a USB drive, Thunderbolt drive, Time Capsule or compatible NAS device (Network Attached Storage). This drive should be of at least equal storage capacity to the server but preferably with more storage, which will better enable Time Machine to maintain multiple versions of data. The pros and cons of the different drives are as follows:

USB drives – these represent the lowest cost solution. Portable drives have the advantages of not requiring external power supplies and can easily be taken off-site. For instance, the drive could be removed at the weekends or overnight and kept in a separate location, which means that a copy of the data would still be available in the event of catastrophe such as fire, flooding, or theft. Portable drives are readily available in sizes of up to 5TB at the time of writing; mains-powered external drives are available in greater capacities should this be insufficient, plus can be cheaper per GByte of storage, particularly with larger capacity drives.

Thunderbolt drives – these are more expensive than USB drives, although their additional performance does not necessarily offer any significant benefit when used solely for backup purposes.

Time Capsule – Apple's Time Capsule was the equivalent of a 'Swiss army knife' for small businesses and home users, combining a network switch, high-performance wireless access point, a hard drive for backup purposes, and for some would be all the infrastructure they need. Whereas a locally connected hard drive could be lost along with the server in the event of disaster, the Time Machine could be located in a different part of the building, thereby reducing the risk. The disadvantages of Time Capsules were that they were only available in capacities of up to 3TB, plus they were relatively expensive. Unfortunately, Apple discontinued the Time Capsule several years ago and they are now only available through the secondhand market and on eBay etc.

NAS – Most brands of Network Attached Storage can be configured to operate with Time Machine and can be considered as replacements to Apple's own Time Capsule in some sense. Because they connect to the network using Ethernet, they offer the same advantage of being locatable away from the server and in another part of the premises. There are three main advantages over Time Capsule: firstly, they are less expensive, for instance a WD My Cloud 3TB NAS is less than half the price that a 3TB Time Capsule was. Secondly, they are available in larger capacities, for instance a Synology DS1815+ can hold 80TB of storage, which is additionally useful for backing-up multiple servers. Thirdly, they can be purchased new. The main disadvantage is that a NAS constitutes another item of technology which needs to be learned and managed. It is also the case that some brands of NAS e.g. Synology and QNAP, provide considerably more functionality than Apple's Server, which rather negates against using it in the first place.

For even greater protection, it is possible to run more than one backup solution. For instance, regular backups might be to a NAS or Time Capsule, with additional backups to an external drive, which is then taken off-site for safe keeping.

To setup the backup, first configure your external drive. In the case of a Time Capsule or NAS, make sure it is accessible over the network; in the case of a regular external hard drive, you may need to use *Disk Utility* to format it as most drives come pre-formatted for Windows usage rather than Mac, although a limited selection of pre-formatted Mac drives are available. Go into **System Preferences** and click **Time Machine**. Click **Select Disk** and specify the backup drive. If security is important to you, tick the **Encrypt backups** box. Click **Use Disk**. If using a Time Capsule, enter the password for it when prompted.

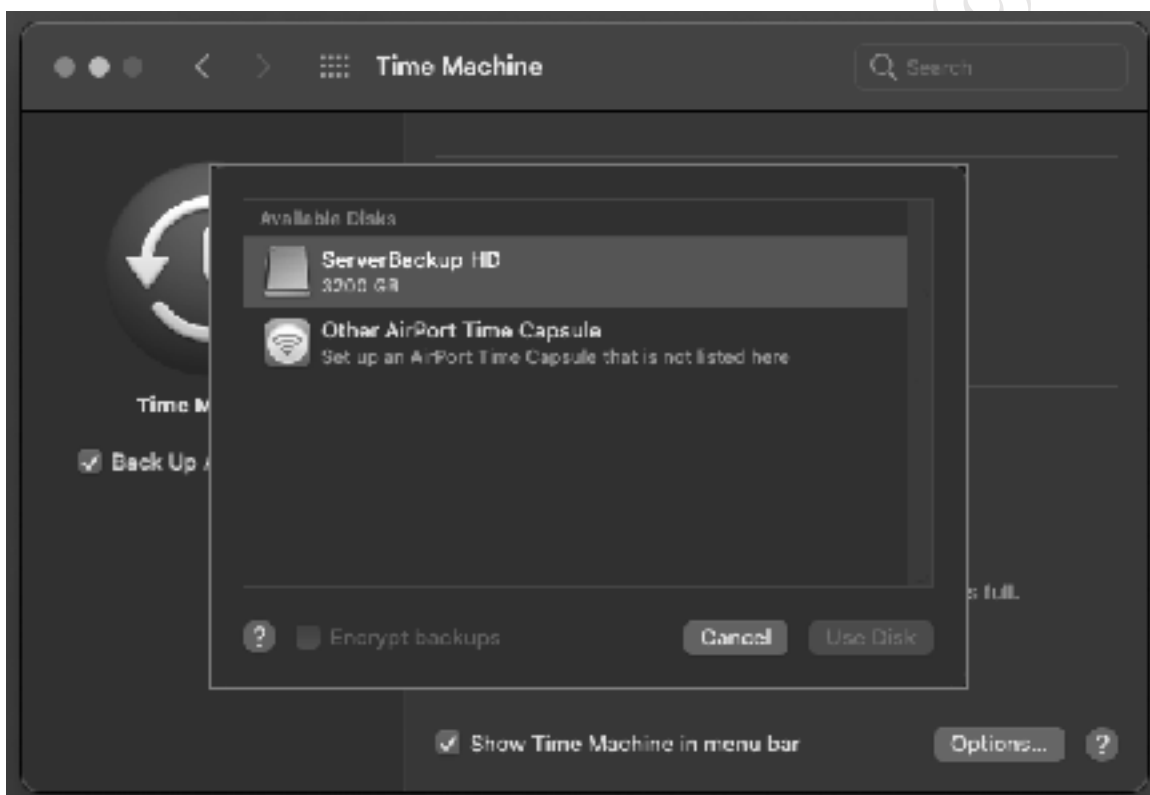


Figure 62: Choose the disk to be used by Time Machine

And that is it. The server backup should now start running. By default, Time Machine will keep hourly backups for the past 24 hours, daily backups for the past month and weekly backups for all previous months. When the disk becomes full, the oldest backups are deleted automatically; use of a high-capacity drive will ensure that it is possible to ‘roll back in time’ for a long way.

To help keep track of status, you may wish to tick the **Show Time Machine in menu bar** option.

6.3 Backing Up the Server using Carbon Copy Cloner

Although Time Machine is the *de facto* method for backing up Macs, there are alternatives, which may have additional features, making them a better choice for some people in some situations. One of the most popular is *Carbon Copy Cloner* from *Bombich Software*. The main difference is this: Time Machine creates a backup of the system, which in the event of a serious problem can be used to restore the system. Depending on the amount of data, this may take several or more hours, during which time the network will be down and unusable. With Carbon Copy Cloner, the backup drive can be a complete, bootable clone of the system. All that is necessary is to change the Startup Disk (**System Preferences > Startup Disk**) to point to the backup drive and boot directly from that. Potentially, the system can be up and running again in a matter of minutes. At a less critical time, out of hours or at the weekend for example, the server can be sorted out and restored or rebuilt properly. This makes Carbon Copy Cloner very useful as a disaster recovery tool. It can be used as an alternative to Time Machine or to complement it.

Begin by downloading Carbon Copy Cloner from www.bombich.com and installing it. It is very affordable, but a 30-day trial version is available so you can first see if it meets your needs before purchasing. You will need an external drive to hold the backups; this can be of any interface type and should be of a suitable capacity. For instance, if your server has a 1TB drive, then the backup drive should also be 1TB. If you wish the backup to be bootable, the drive needs to be formatted as APFS with GUID Partition Map, else it can only be used for backing up data volumes (drives are formatted using the macOS Disk Utility). The first-time Carbon Copy Cloner is used, it may request to install a helper tool on the server, which you should allow it to do (and which will then request permission to give notifications).

Run Carbon Copy Cloner. It can be used in Simple mode or Standard mode and we will use the latter as it has more features (although it is still very simple). To switch between modes, click the **Carbon Copy Cloner > Standard Mode** menu option. The interface is very clear and straightforward. Click on **SOURCE** and select the drive that holds macOS Server and which might also hold your data, for instance if you were running everything on a Mac mini and using the internal drive only. Click on **DESTINATION** and select the drive that will hold the backup. Click **Start** and the cloning process will begin.

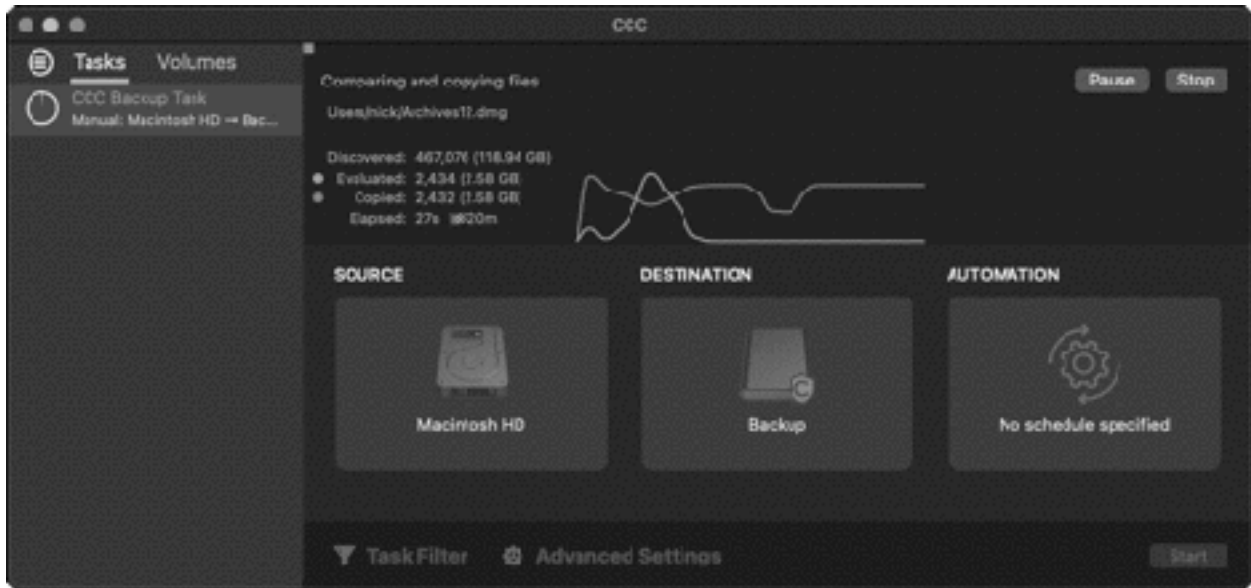


Figure 63: Carbon Copy Cloner, Standard mode

Rather than run immediately, you can also schedule a backup. Click **AUTOMATION** and from the dropdown choose an option e.g. hourly, daily, weekly and so on. On the resultant panel, the schedule can be fine-tuned. Click **Done** and on the main screen click **Save**.

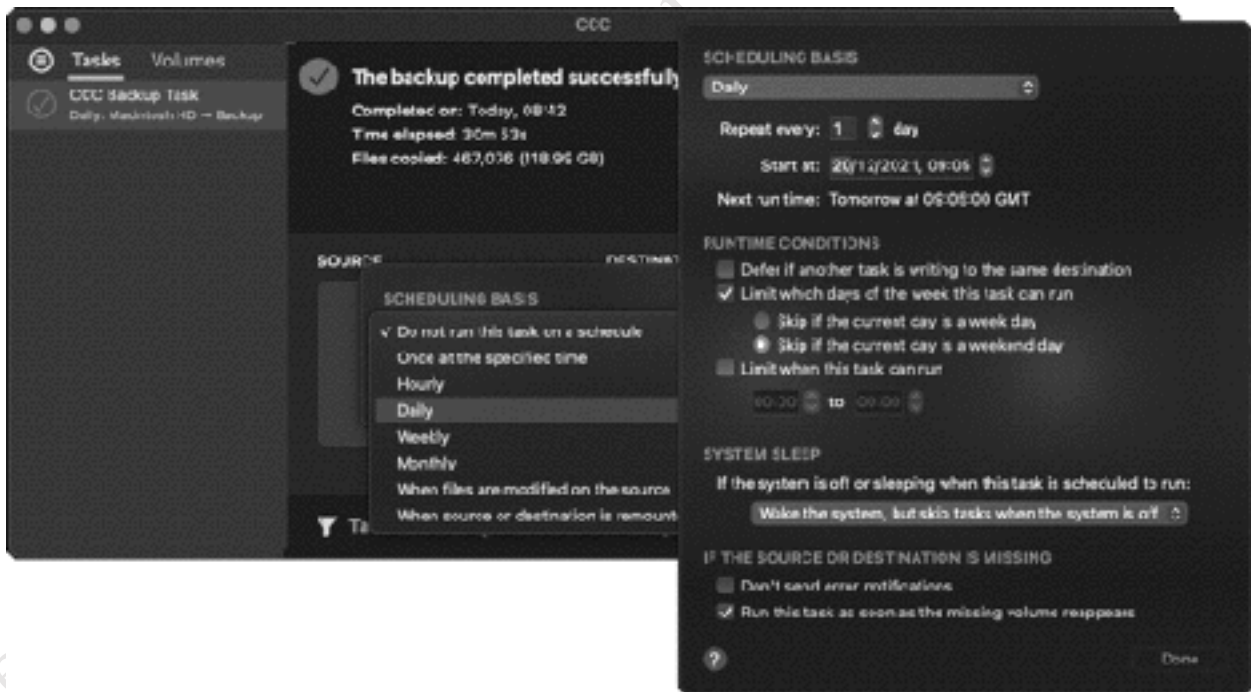


Figure 64: Carbon Copy Cloner scheduling screen

The time taken for the backup depends on the amount of data; the first one is slower as everything has to be backed up, but subsequent ones will be faster as Carbon Copy Cloner tracks the files and folders that have changed and only backs up the changes i.e. 'incremental backup'.

Additional options are available for managing and reporting upon backups. These can be accessed by clicking the **Advanced Settings** cogwheel on the main screen, and by clicking **Carbon Copy Cloner > Preferences** on the menu bar.

To recover data from a backup, click **Task > New Restore Task** from the menu bar. Click the SOURCE and DESTINATION buttons and make the appropriate choices.

Free edition. Do not copy or distribute. (c) CTACS

6.4 Backing Up Macs to the Server

The server can act as a centralized destination for Time Machine backups, meaning it can be used for backups by Macs on the network. Before enabling this feature, consider the implications; in particular, how much space will be required to hold the backups and where it will be located? A starting point is to add up the amount of storage being used on the client Macs, then double it. For example, suppose there are 10 Macs in the network and on average each one is using an average of 50 GB of local storage space. That would give us $10 \times 50 \times 2$ for a total of 1000 GB / 1 TB space needed to hold the backups, although more space would allow greater backup retention periods.

On the designated storage location on the server, create a standard folder for the Time Machine backups; give it a meaningful name, for instance, something like *tmbackups*. This folder should be made into a shared folder, so that users can access it. Go into **System Preferences > Sharing** on the server. Underneath the Shared Folders section, click the plus sign (+), navigate to where the Time Machine backup folder is, highlight it and click **Add**:

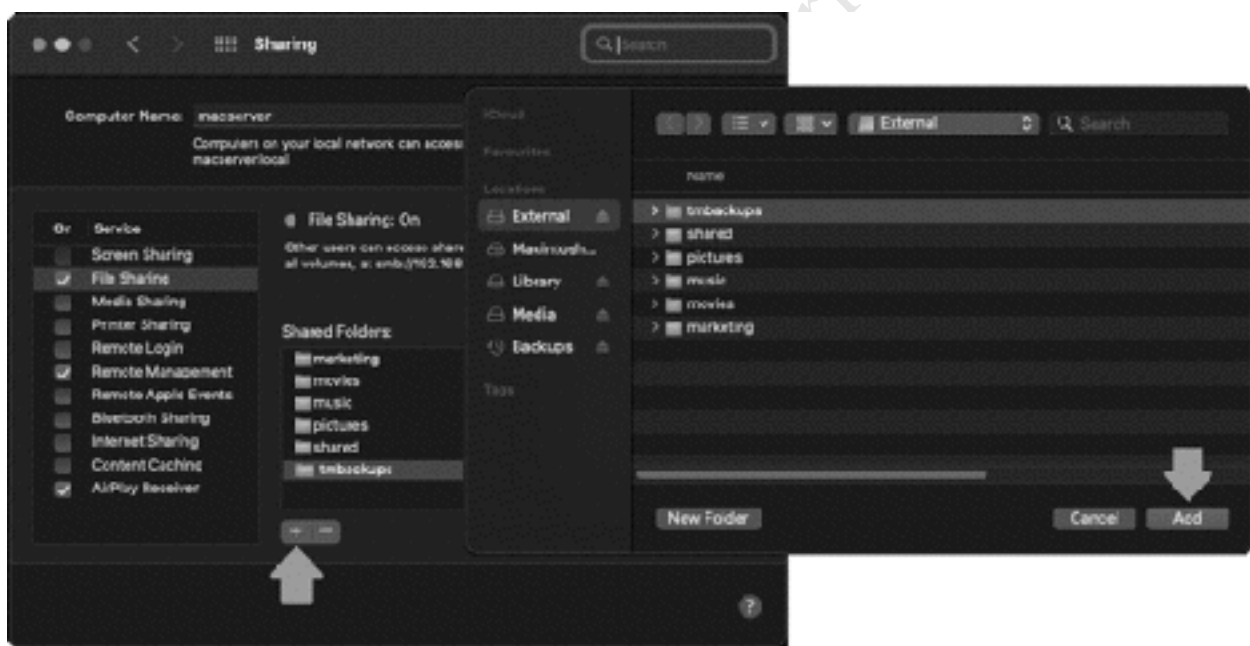


Figure 65: Add Time Machine backup folder to the list of shared folders

Upon returning to the main Sharing screen, right-click the designated Time Machine backup folder, choose **Advanced Options** and tick the **Share as a Time Machine backup destination** box. You may want to limit the size of the backups folder in accordance with the calculation above, if you do not do so, it will potentially grow until it fills the entire disk. Click **OK**:

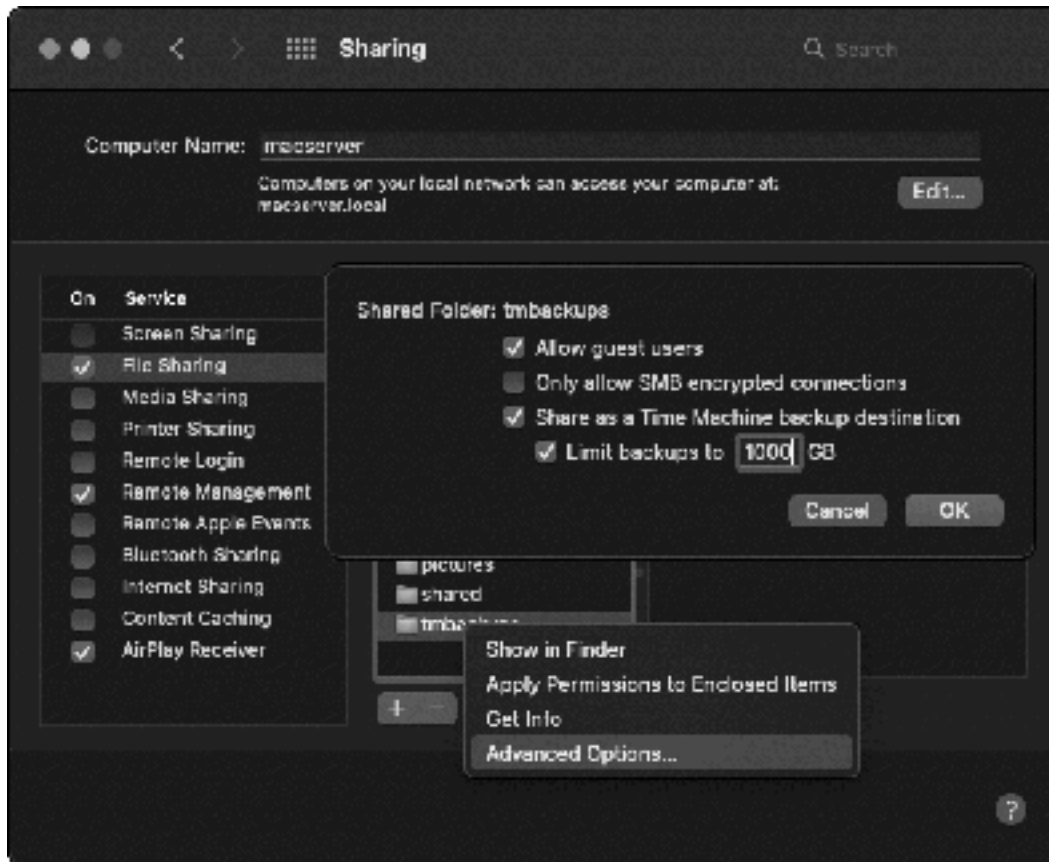


Figure 66: Set the folder as a Time Machine backup destination

On the user's Mac, go into **System Preferences** and choose **Time Machine**. Click the padlock to make changes (it may be necessary to specify an administrator's name and password to do this), click **Select Backup Disk** and choose the server destination. The user may be prompted to enter their own network name and password. Click **Connect**. Thereafter, as far as the user is concerned, Time Machine operates in the same manner as if it was a locally connected external drive.

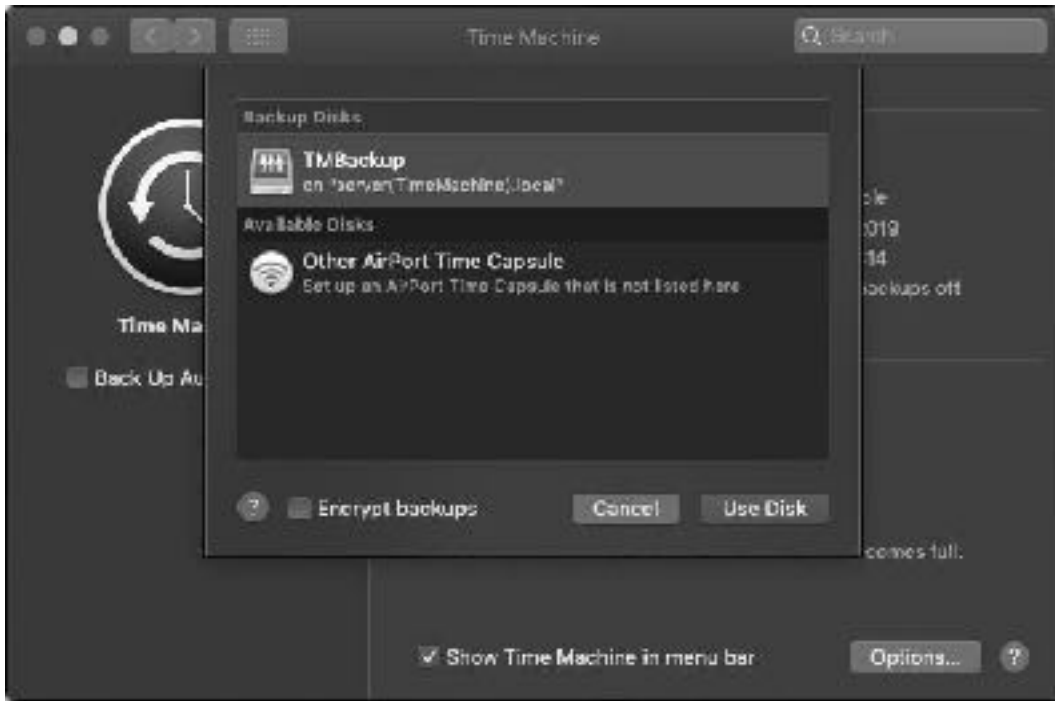


Figure 67: Choose the network folder as the Time Machine destination

Free edition. Do not copy or dis

6.5 Backing Up Windows PCs to the Server

If users store data on their own computers rather than on the network, then there is probably a requirement to be able to backup that data. All versions of Windows have a built-in backup program but there is a restriction: they assume you are backing up to a local USB drive and it is only the more expensive Professional versions of Windows that can backup to network drives i.e. to a server. If you have Home editions of Windows, which are more common in home and small organization settings, then it will be necessary to use a third-party backup program. There are many to choose from; the one we will use here is *FBackup* by Softland, which is totally free both for commercial as well as private use (see www.fbackup.com). It works with all versions of Windows, thereby providing a consistent solution. A further advantage of *FBackup* is that it does not suffer the idiosyncrasies of Windows Backup, which sometimes just plain refuses to talk to network drives on a macOS-based server.

A location on the server needs to be set aside for the backups. For instance, create a shared folder called *pcbackups* on your designated storage area and give Read & Write access to all the users who have Windows computers (creating shared folders is described in section [4.3 Creating Shared Folders](#)).

Download and install *Fbackup* on the PC to be backed up; when downloading it, take care not to download additional unrequired programs such as other utilities and browser add-ins, particularly if using a third-party download site.

Launch *FBackup* and click the **New** icon to define a new backup task. For the destination of the backup, choose **Network** and enter the username and password as defined on the server. A nice touch is that you can click the **Test** button to make sure the backup folder can be 'seen'. Click **Next**. Suggestion: if *FBackup* cannot 'see' the server when using the Browse button, type in its full address e.g. `\\server\pcbackups`

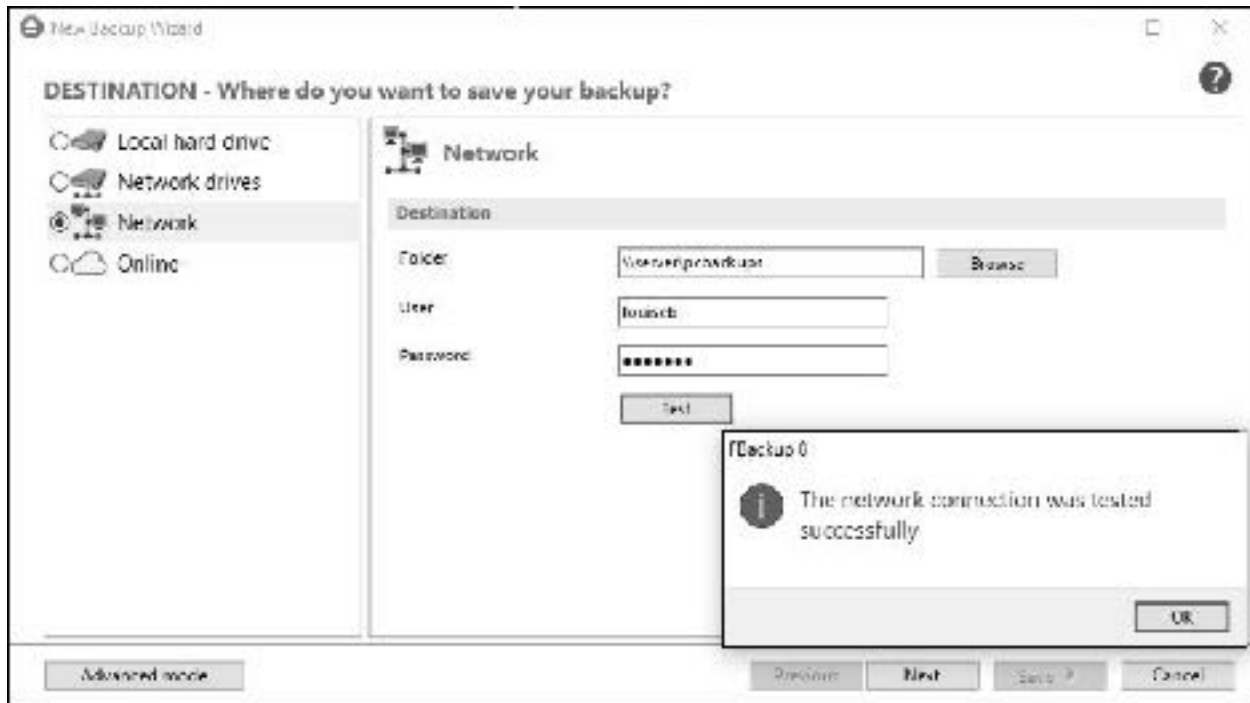


Figure 68: Specify the destination for the backup

On the next screen, choose the folders and files to be backed up. For simplicity, simply tick the C: drive; alternatively, expand it and manually choose the folders and files (for instance, you probably would not want to backup the *hiberfil.sys*, *pagefile.sys* and *swapfile.sys* files or the Windows folder). There is also specific support for many applications, including popular browsers and Microsoft Office, selectable by clicking the **More applications** link. Make your selection and click **Next**:

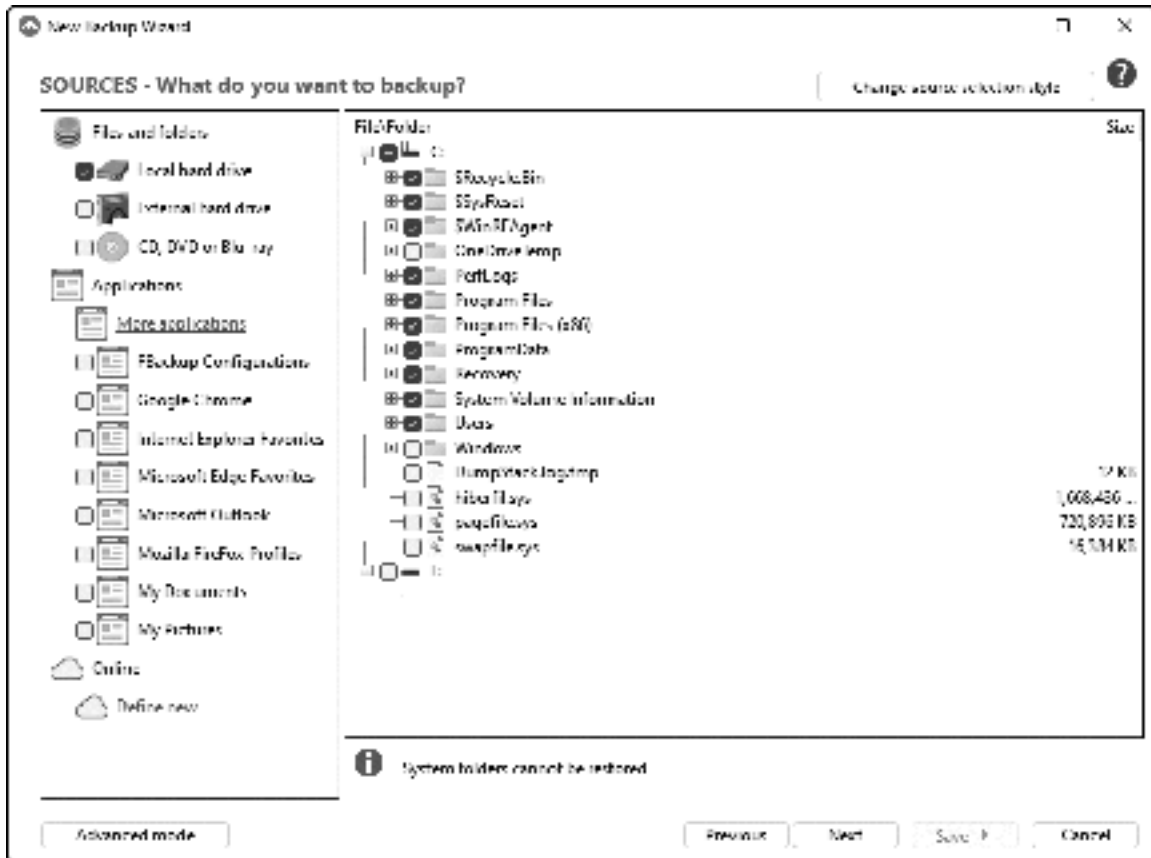


Figure 69: Choose the data to backup

The following screen is for specifying the type of backup and the choices are *Make full* or *Make mirror*. With the former, everything is backed up and stored as a zip file, which you can optionally encrypt and protect with a password. If you have specific security requirements e.g. you are backing up confidential information, then you might want to choose this option (be sure to make a note of the password). With the *Make mirror* option, the backup is stored in a standard file format that can be read with Windows File Explorer if required. Make a choice and click **Next**.

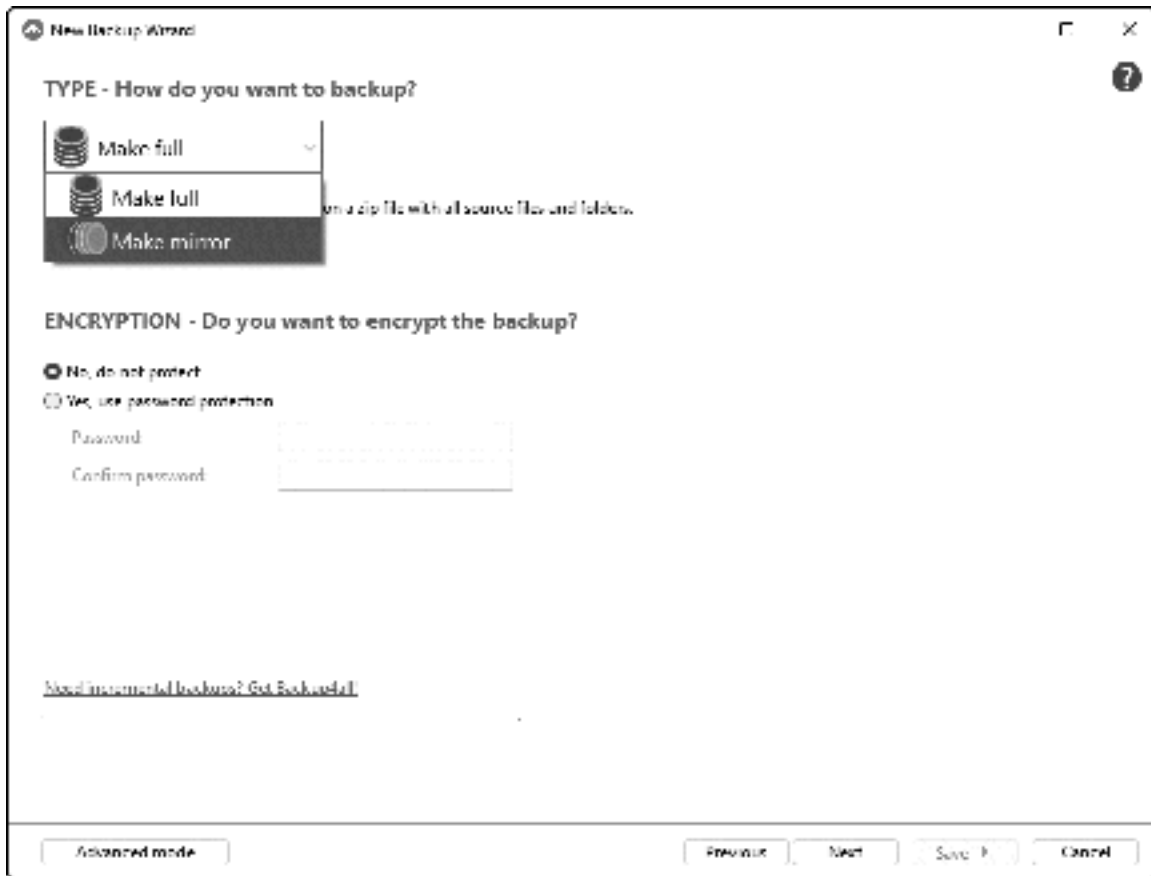


Figure 70: Backup type and encryption options

The subsequent screen allows the backup to be scheduled to run on an automatic basis - in this example the backup will run daily at 2200/10:00pm:

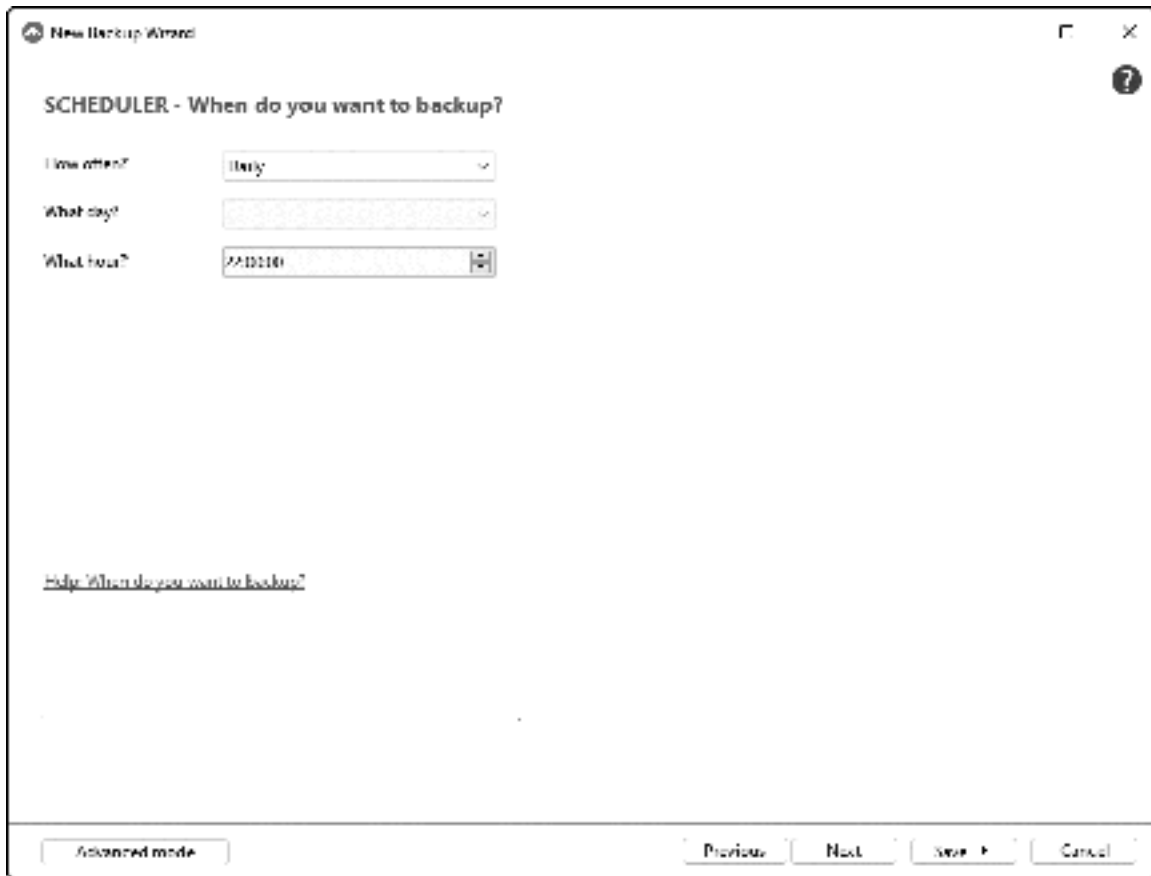


Figure 71: Specify the backup schedule

Having specified the schedule, click the **Save** button. There is a choice of *Save* or *Save and Run*; the latter option is useful as it will cause the newly created backup job to run immediately, constituting a useful test and first backup. The time taken for the backups depends mainly upon the amount of data. When the backup is complete a log file and message are generated – these should be checked to confirm that the scheduled backups are working. It is quite unusual to have a completely ‘clean’ backup and there will often be errors and warnings. However, many of these relate to unimportant matters and can usually be ignored.

7

Housekeeping, Maintenance and Security



Free edition. Do not copy or distribute. (c) CTACS

7.1 Overview

The server needs to be checked on a regular basis to ensure that there are no problems and that it is in good health. Clearly some type of problems will be immediately apparent; for example, if the server is powered down for some reason then nobody will be able to use it. But there are plenty of other things that need to be monitored: Has the backup completed successfully? Is the server running out of storage space? Additionally, there are some housekeeping tasks that should be performed on an occasional basis.

7.2 Software Updates

It is strongly recommended that you keep the server and all computers on the network up to date with software updates, which typically address security issues, fix problems and improve functionality.

Server Updates

If Server needs updating, this will be indicated when launching it. Apple update macOS Server on a regular basis, usually coordinated with updates to macOS itself, although there may be minor updates in-between this cycle to address specific issues and security vulnerabilities. As with all Apple software, updates to Server are provided through the App Store. Some thought needs to be given as to whether a new update should necessarily be applied. As described in section [1.2 Mac Operating System and Server Versions](#), Apple have been deprecating (removing) features from Server for several years, so it is important to first check that a feature you required is not about to be removed.

Because Server must be shutdown before it can be updated, which may be disruptive to users, updates should take place out of hours or at an otherwise agreed time. If you are in a business or educational environment, you may wish to test the new version on a single, non-critical server before a wider roll-out.

macOS Updates

Regular software updates to macOS are provided through the App Store and controlled through System Preferences. The default settings are usually fine for user computers, but on a server it is suggested that you do not allow it to automatically apply updates. The reason for this is that you want to exercise some control over the process; for instance, some updates require that the server will be restarted and to avoid disruption you would normally do this out of hours, especially in a business or educational setting. It is also the case that some updates introduce new problems of their own, so a good strategy is often to wait a few days or weeks after a new one is released, check what people are saying on internet forums and other platforms, then decide as to whether to apply it to the server at the current time.

To change settings on the server, go to **System Preferences > Software Update**. Untick the **Automatically keep my Mac up to date** box, plus click the **Advanced** button and remove the ticks from all the options (it is necessary to provide admin credentials to do so):

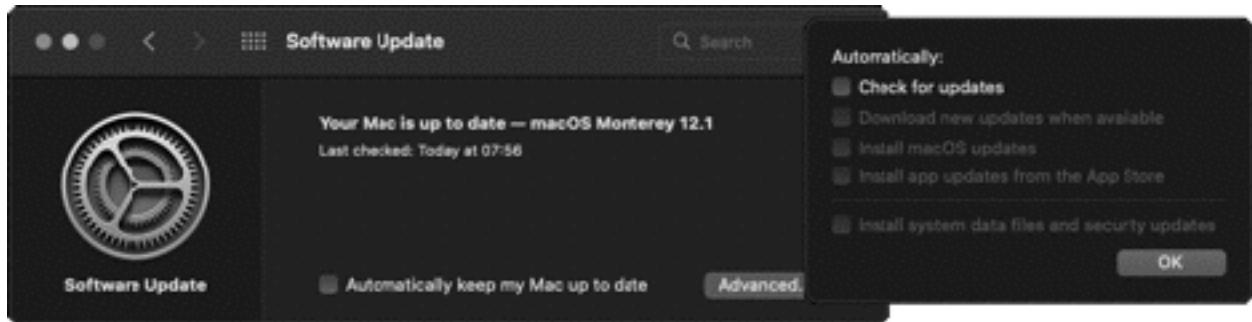


Figure 72: Software Update options

Free edition. Do not copy or distribute.

7.3 Monitoring Server Performance

macOS Server maintains detailed usage statistics, which is information that can be of help when diagnosing problems or identifying bottlenecks in a poorly performing system and, whilst it may be too specialized for some users, can be helpful to IT professionals. For instance, if it was found that network traffic was consistently high, then this might suggest using an additional network adapter to alleviate the problem (see section [10.6 Link Aggregation for Network Adapters](#)). To access the information, go into Server and click **Stats** (or **View > Stats** from the Menu bar):

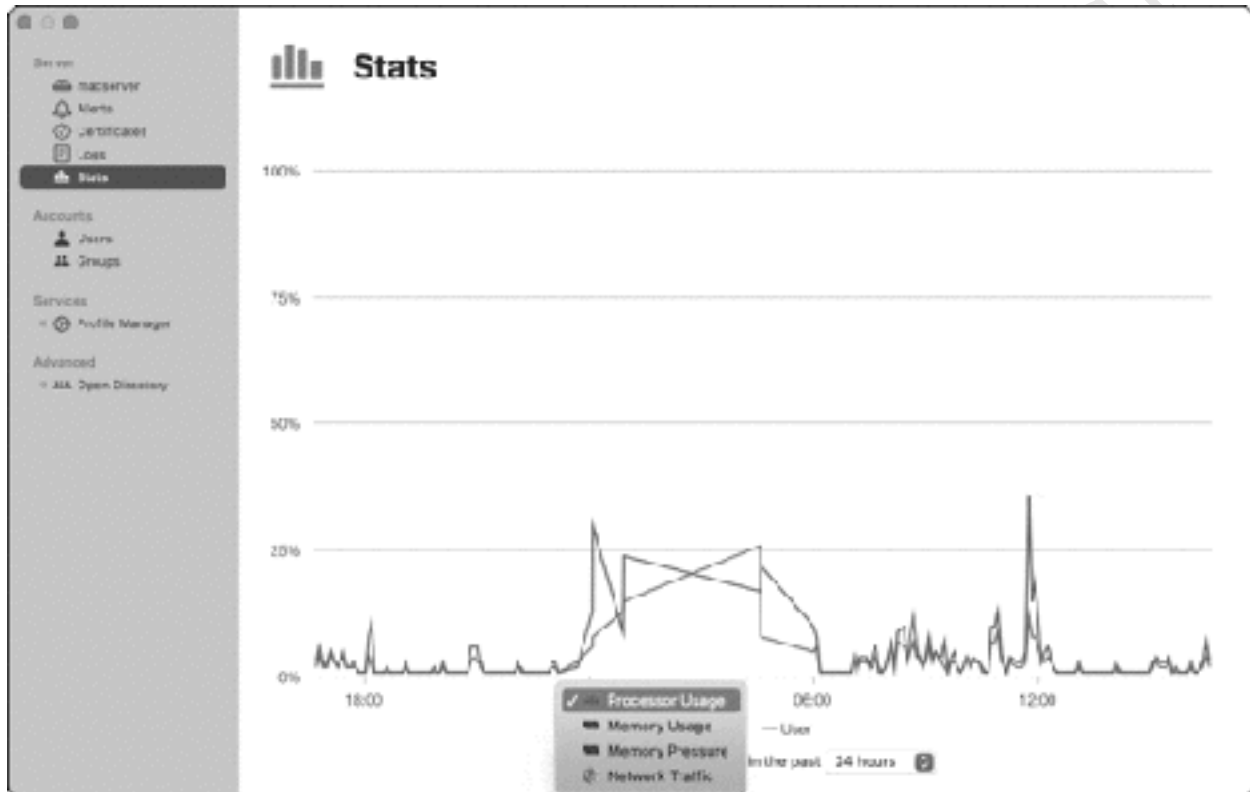


Figure 73: Performance Stats

At the bottom of the screen are two filters. The first is for choosing the type of information to be displayed and gives a choice of: *Processor Usage*; *Memory Usage*; *Memory Pressure*; *Network Traffic*. The second is for choosing the time period to be checked, ranging from the past hour through to the past week.

In addition, there are other features within macOS for monitoring performance, of which the main one is the *Activity Monitor* (**Applications > Utilities > Activity Monitor**).

7.4 Alerts

When significant events occur, Server generates an *alert*. These alerts are indicated on the main screen; this example shows that alerts are outstanding and need responding to:



Figure 74: Outstanding Alerts

To manage the alerts, go to the *Alerts* section of the main Server screen or click **View > Alerts** from the menu bar. There are two tabs – *Alerts*, which is a listing of the events – and *Delivery*, which defines what events are reported upon. Double-clicking on an alert may result in more information being displayed. To delete an alert: click to highlight it; click the menu options at the bottom of the screen and select **Delete Alert**. To delete all the alerts, choose **Clear All**.

Click the **Delivery** tab to display the following screen:

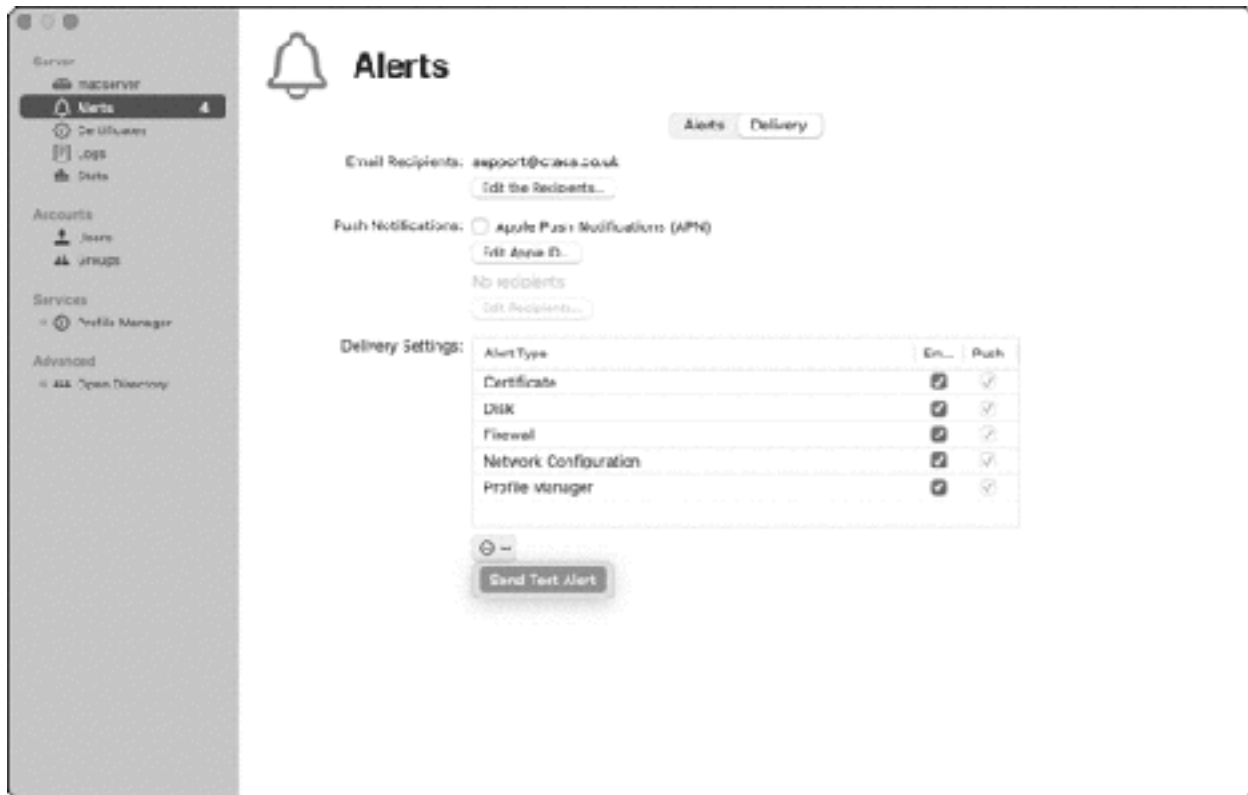


Figure 75: Configuring Alerts

The first thing to do is define who will receive the alerts and how: there are two options and either or both can be used. With *Push Notifications*, the server administrator(s) receives alerts whenever they log in - click **Edit Notifications** to set this up. It will be necessary to login with a valid iCloud ID to do so, which will also result in the generation of a suitable 'certificate'. The other option, email, is possibly more useful as the person who looks after the server may not always be located in the premises. Click **Edit Recipients** to set this up. Having done so, click the menu options at the bottom of the screen followed by **Send Test Alert**.

It will now be possible to choose the sub-systems that generate the alerts, which will have been grayed out until the recipients were defined. This consists of removing or adding ticks to the *Email* and *Push* columns as appropriate.

7.5 Log Files

Server maintains detailed log files of all system activities. Some of these are the standard logs generated by the underlying BSD UNIX-based system that macOS is derived from, whereas others are Apple-specific. To access, click **Logs** on the left-hand side of the screen. To switch between the different type of log files, use the pop-up menu towards the bottom of the screen:



Figure 76: Log Files

The use and interpretation of this data can be a specialized activity, as much of the information will only be meaningful to someone experienced in Mac and BSD UNIX networking topics. Nevertheless, it is possible to gain useful clues about what is going on. For instance, suppose a particular user is unable to access the server – performing a search on that user’s name in, say, the System Log might provide some information as to what the problem might be.

7.6 CCleaner

Any computer accumulates ‘junk’ during its normal operation – unused files, temporary files, cookies and so on. The effect of this is to use up storage space and gradually slow down the computer, and to mitigate against this so-called ‘Cleaning tools’ are available. The reputation of these varies, but one which is well regarded by many people is *CCleaner for Mac* from Piriform. This is available in both free and paid versions; the paid version has some additional features and is a low-cost purchase.

Begin by downloading and installing CCleaner for Mac – it is suggested you do this directly from the Piriform website. Run the application; click the **Analyze** button and it will scan the computer for files that can safely be removed. Once it has done so, click the **Run Cleaner** button to delete the files:



Figure 77: CCleaner main screen

There are other options available within CCleaner, but unless you are an experienced user you may wish to leave them alone.

7.7 Care and Maintenance of Open Directory

A lot of key information about the network is held in Open Directory and which, if lost or corrupted, would be time consuming to recreate. It is not properly covered by the normal backup mechanisms; rather a separate facility is provided, known as an *archive*. If the server was totally lost and had to be rebuilt, being able to restore a copy of the directory information would be hugely beneficial.

However, before taking an archive, you should first take a separate backup of the users and groups. From within the *Users* section of macOS Server, click the three-dot menu at the bottom of the screen. Scroll down the pop-up menu and choose **Export Users**. On the resultant panel, choose a location for the export file and give it a meaningful name. At the bottom of the panel, the *Export* field provides a choice of *Selected User(s)*, *Local Users* or *Local Network Users* – you want the latter. Click **Export**. Next, go to the *Groups* section of macOS Server and repeat the above, but this time you want to export the *Local Network Groups*.

Next, click on **Open Directory**. Underneath the *Servers* section, click the three-dot menu and choose **Archive Open Directory Master**:

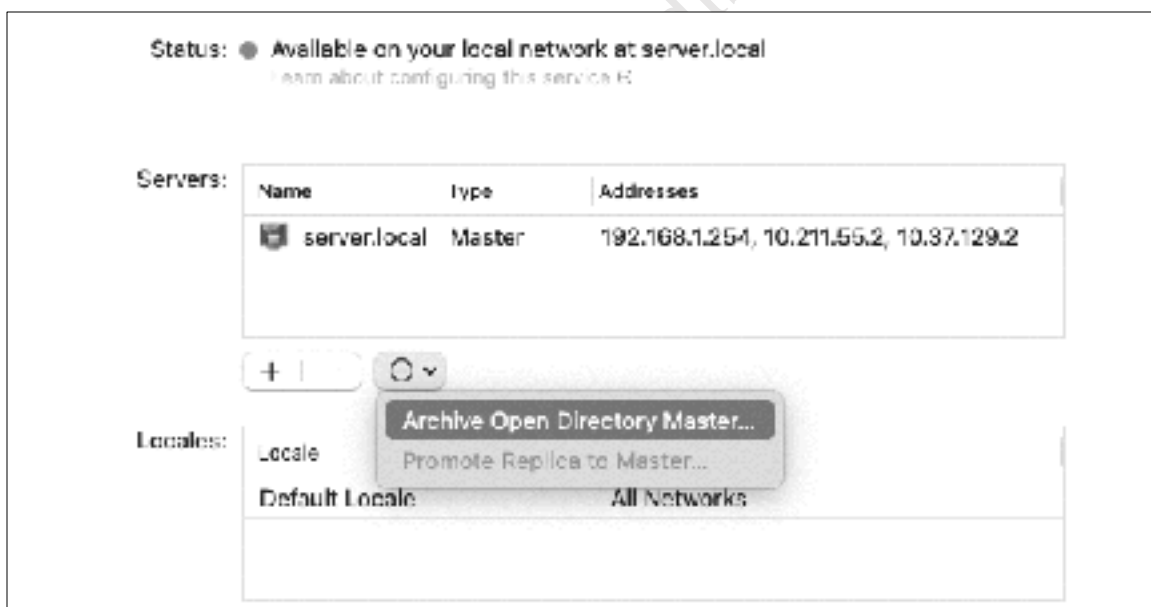


Figure 78: Archive Open Directory Master

Click the **Choose** button and specify a name and location for the archive file. It is suggested that you do not keep it on the server itself, instead place it on a backup drive, USB stick or other external location. A useful technique is to specify today's date as part of the filename so you can see immediately when it was created. Specify and verify a password for the archive file and make a note of it. Click **Next**, followed by **Archive** on the subsequent screen. The time taken to generate the archive depends on the number of entries in the directory but is not long.



Figure 79: Specify name and location for the archive

Hopefully you will never need to use this archive, but there are two scenarios in which you may need to:

Open Directory is Corrupt

Close down the macOS Server application.

Go into **Applications > Utilities** and launch **Terminal**.

Type the following and hit Enter: `sudo slapconfig --destroyldapservers`

Enter the password for *diradmin* when prompted

Close down Terminal

Run macOS Server

Start Open Directory

From within the *Users* section of macOS Server, click the cogwheel at the bottom of the screen.

Scroll down the pop-up menu and choose **Import Users**. Locate the backup file you made.

Repeat, but this time go to *Groups* section and **Import Groups**.

Rebuilding the Server from Scratch

Install macOS

Install and configure macOS Server

From within macOS Server, click on **Open Directory** within the *Advanced* section (alternatively, choose **View > Open Directory** from the main menu) and click the On/Off switch in the top

right-hand corner of the screen to enable it. This will cause a wizard to run, giving three options – choose **Restore Open Directory** domain from an archive.
Specify the location of the archive file and load it.
Restore the users and groups as described above.

Free edition. Do not copy or distribute. (c) CTACS

7.8 Certificate Error

Sometimes, when connecting to a service running on macOS Server you may receive a ‘certificate error’ from your browser. Certificates are a method of ensuring that a website is what it says it is, rather than a hoax or bonus one, and they are issued by several respected authorities. As obtaining and managing a certificate involves a certain amount of time, money and effort of the sort that many home users and small businesses will not wish to incur, Server comes with a self-certified one. However, when you use an internet browser or other piece of software, it recognizes that the certificate is not ‘real’ and generates the error. As you are aware of what is going on you can ignore the error (e.g. by clicking **Continue** in Safari) but you can permanently suppress it using the instructions below. It is important to emphasize that you should only do this for the internal macOS Server only – when working with normal, external websites you need to exercise great caution when certificate errors arise.

In Safari, the certificate error appears as follows. Click **Show Details**. The panel expands – click the **visit this website** link, followed by the **Visit Website** button on the subsequent pop-up.

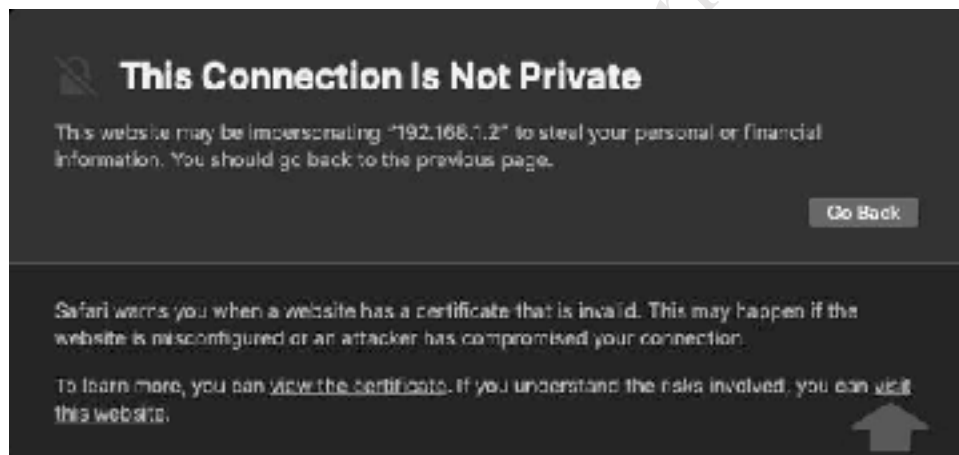


Figure 80: Certificate error in Safari

You will be prompted to enter your Mac logon credentials to ‘make changes to your Certificate Trust Settings’, which means you are marking the server as a ‘safe site’. Click **Update Settings** and the webpage from the server will be displayed.

Some parts of Server may also generate certificate warnings. Provided you are satisfied that these are being generated by the Server app itself, then they can be trusted.

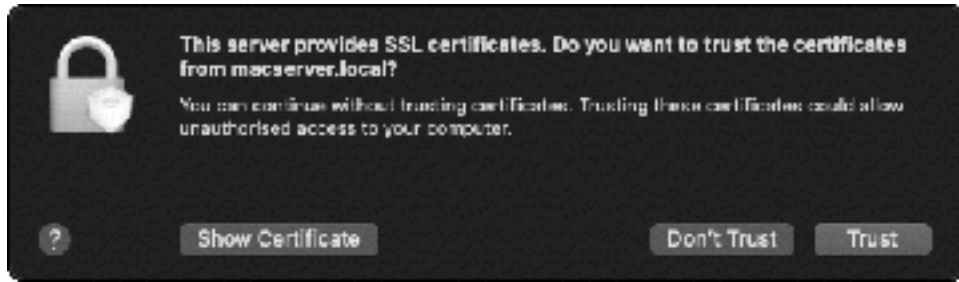


Figure 81: Certificate error generated by Server app

Free edition. Do not copy or distribute. (c) CTACS

8

Profile Manager



Free edition. Do not copy or distribute. (c) CTACS

8.1 Overview

Profile Manager is a service that enables Macs, iPads, iPhones and Apple TV devices to be centrally configured and managed. Some of the characteristics that can be controlled include:

- Distribution of Apps and Books to devices
- Remote wipe of devices
- Configure Printing
- Configuration of Dock, Login Items, Finder
- Configuration of options on iPhones
- Software updates on devices running iOS 14 and macOS 10.14 onwards

The settings can be specified for individual users and devices or, more commonly, for groups of users and devices. A collection of settings constitutes a *profile*. Devices are *enrolled* into Profile Manager. Profiles can be mandatory and pushed out to devices automatically, optional ones that users can load at their discretion, or a mixture of the two. Although earlier versions of macOS and iOS than the current ones are supported, some features may only be applicable for devices running the latest versions of macOS, iOS, iPadOS and tvOS.

In a very small network, Profile Manager is not commonly used, but the bigger the network is the more useful it becomes. Consider, for example, a school where there may be hundreds of users and dozens of Macs and iPads to be managed. The pupils are organized into classes and the apps and the books and features that are available to each class may need to be different, based upon age, ability, and other criteria. Profile Manager offers a powerful means to achieve this, providing a common experience as well as reducing the overheads of looking after it all. It is analogous to Group Policy Manager in a Windows Server environment, although note that Profile Manager cannot manage any Windows PCs that you may have on your network. It is also the case that Profile Manager places more emphasis on the management of mobile devices than its Windows counterpart, reflecting Apple's interests and dominance in this area.

Because Profile Manager is less applicable to the small business and home networks which are the focus of this book, we are going to restrict ourselves to the basics and just give a flavor of how it works. If the capabilities outlined above are applicable to your organization, then you may wish to check the more detailed usage documentation available on Apple's website, or simply play around with it to see how it works and what it is capable of.

8.2 Configuring and Using Profile Manager

Go to Profile Manager in Server and click the large ON-OFF button in the top right-hand corner of the screen. There will be a message regarding *Configure Device Management* – wait until the process completes and click **Next**. You will then be prompted to enter some basic information about your organization: do so, then click **Next**.

Following this, a message about *Configuring an SSL Certificate* is displayed. Certificates are a method of ensuring that a website is what it says it is, rather than a hoax or bonus one and are issued by a number of recognized authorities and agencies. As obtaining and managing a certificate involves a certain amount of time, money and effort of the sort that many home users and small businesses will not wish to incur, Server comes with a self-certified one. If the server is only accessed from within the premises, then this may be sufficient. However, if you are accessing the server from the outside world, typically over the internet, then you may want to investigate the topic of certificates in greater detail (also see section [7.8 Certificate Error](#)). Click the dropdown and change it from 'None' to the self-certified one that it has created. Click **Next**:

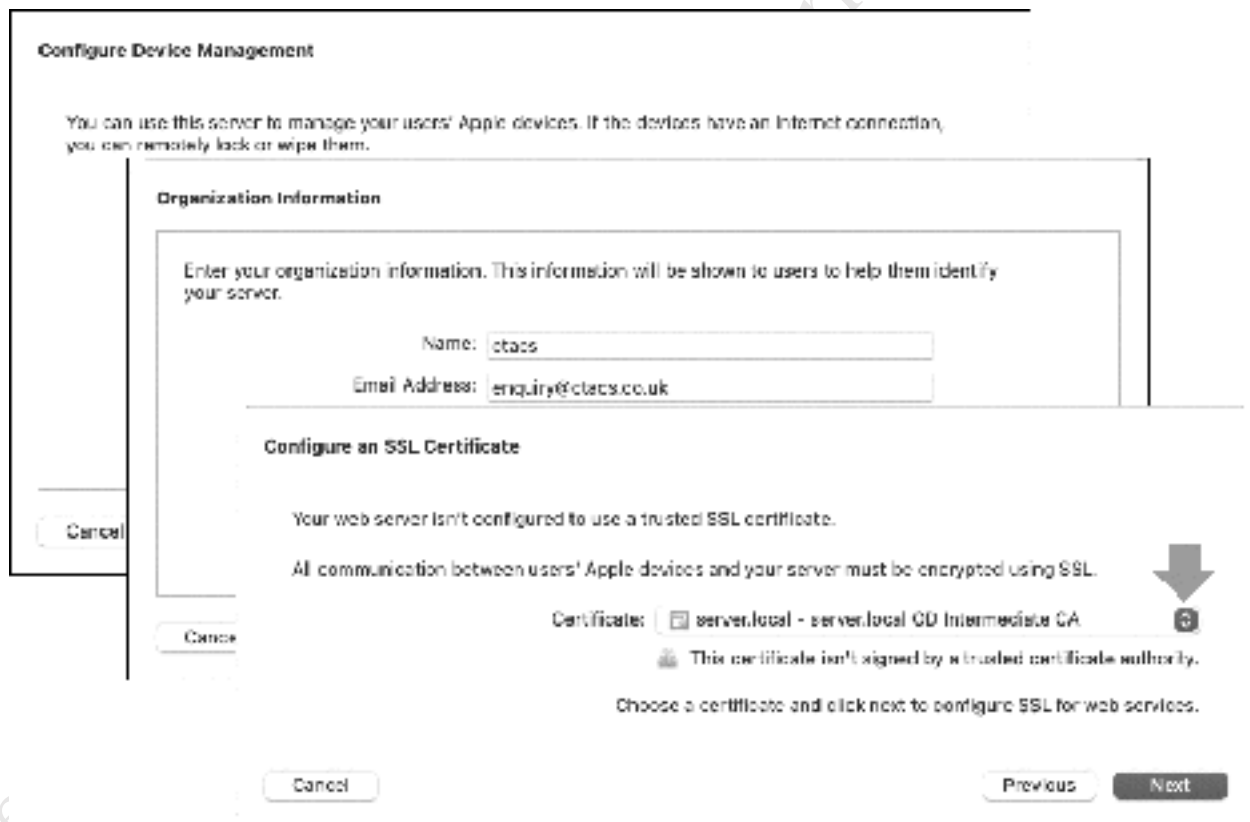


Figure 82: Configure an SSL Certificate

The subsequent panel is for setting up a certificate to receive notifications using the Apple Push Notification service. Enter a valid Apple ID and password and click **Next** then **Finish** on the end screen.

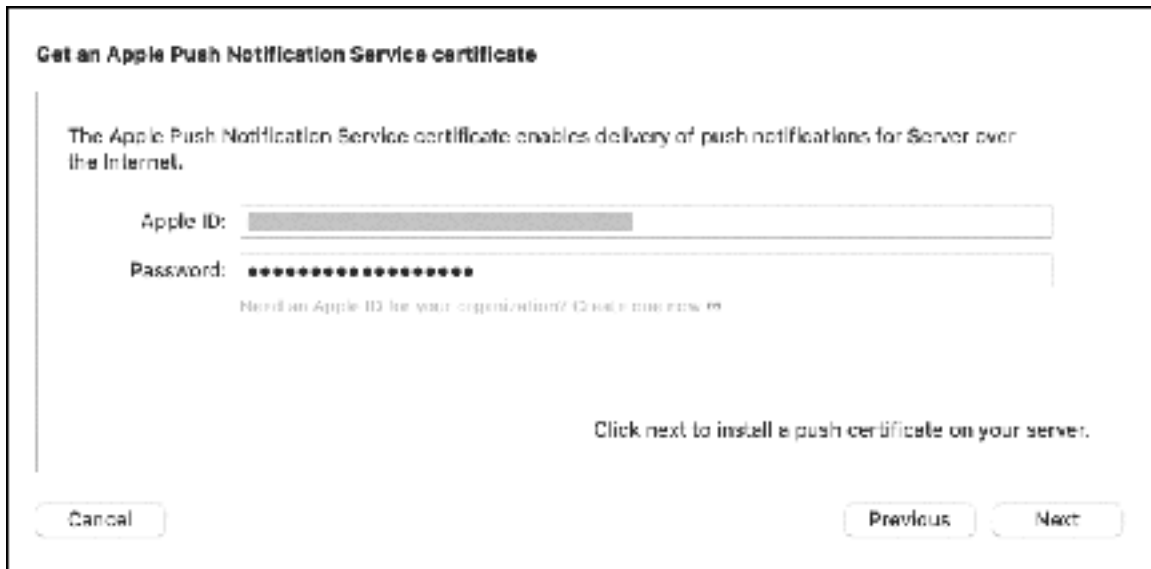


Figure 83: Apple Push Notification Service

There may be a warning message about ‘how your password is stored’ - click **Change**. The service will take several seconds to startup, at which point the *Status* will change to ‘*Available at macserver.local/profilemanager*’ (in this example our server is called *macserver*, yours may be different):

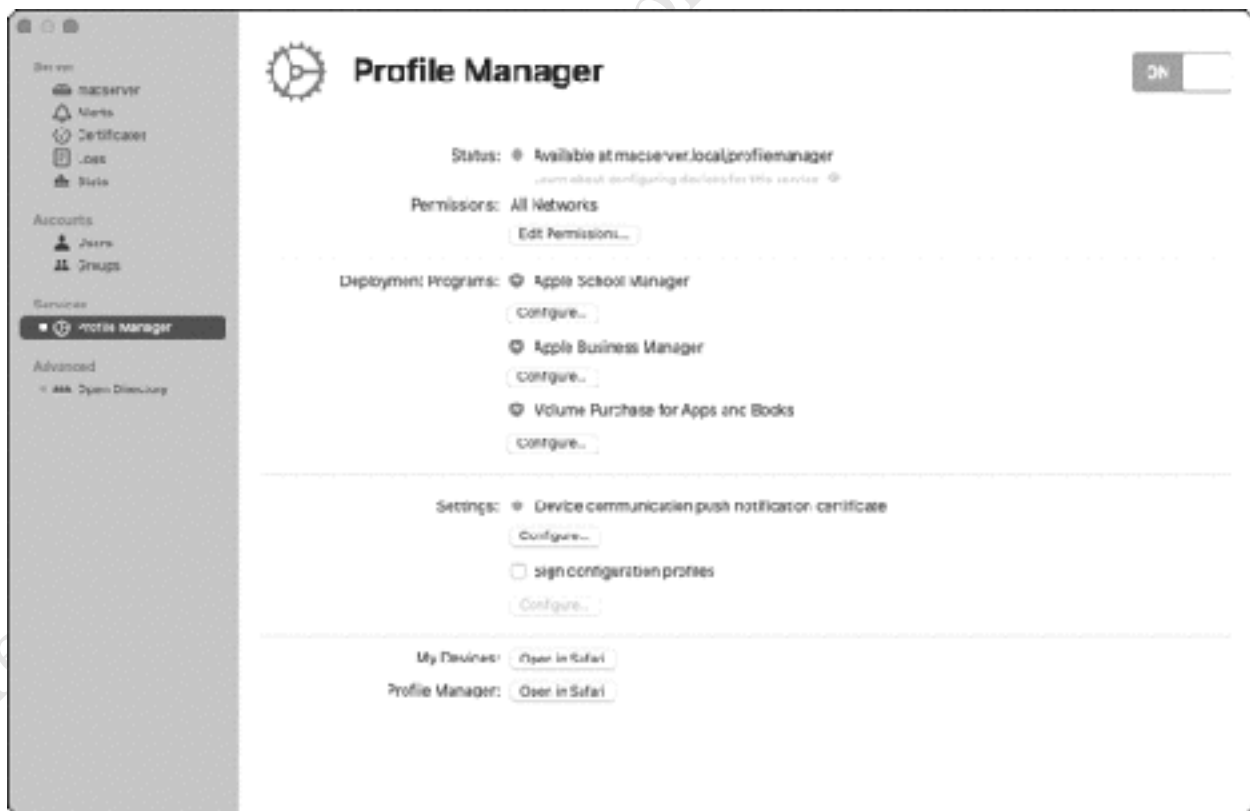


Figure 84: Profile Manager screen within Server

As Profile Manager is web-based - albeit an internal web or intranet - you can manage it from any computer on the local network. At the bottom of the screen are two links, one for managing *My Devices* and one for *Profile Manager*, which might seem a bit strange but think of the latter as leading to Profile Manager ‘proper’, whereas the current screen is only an initial setup and status screen.

Each device on the network must first be enrolled to enable it to be managed using Profile Manager. If you are enrolling a user’s Mac or iOS device such as an iPhone or iPad, you use the copy of Safari on it and browse to <https://macserver.local/profilemanager> (or *server.local* or whatever you have named your server). On the screen that is displayed, click the **Login to My Devices** link and login with the user’s network details when prompted. If the device is not currently enrolled, the following screen is shown:

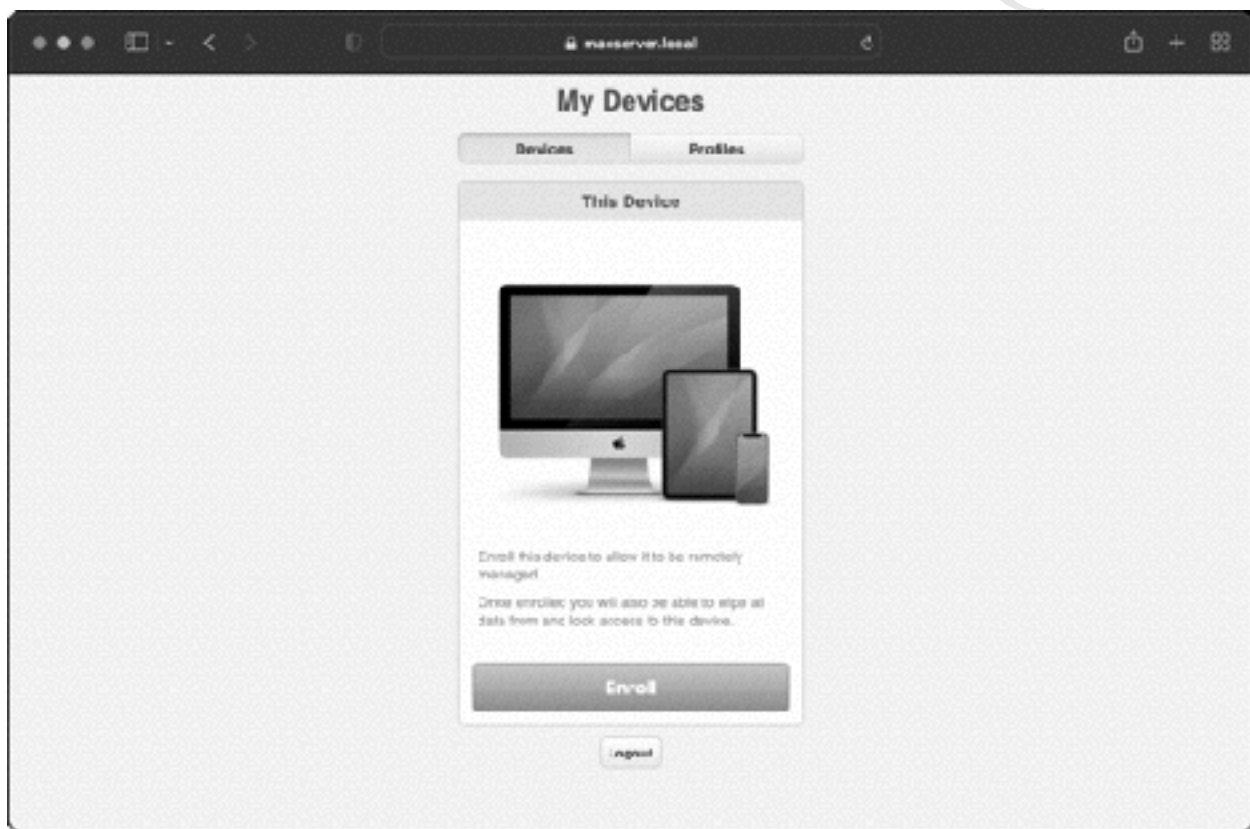


Figure 85: Enrollment screen

Click the large **Enroll** button, which will result in a prompt asking if you wish to allow downloads from the server – click **Allow** and a ‘Profile’ will be downloaded. Go into **System Preferences** and a new item called *Profiles* will have appeared. Click it and you will be looking at something like this:

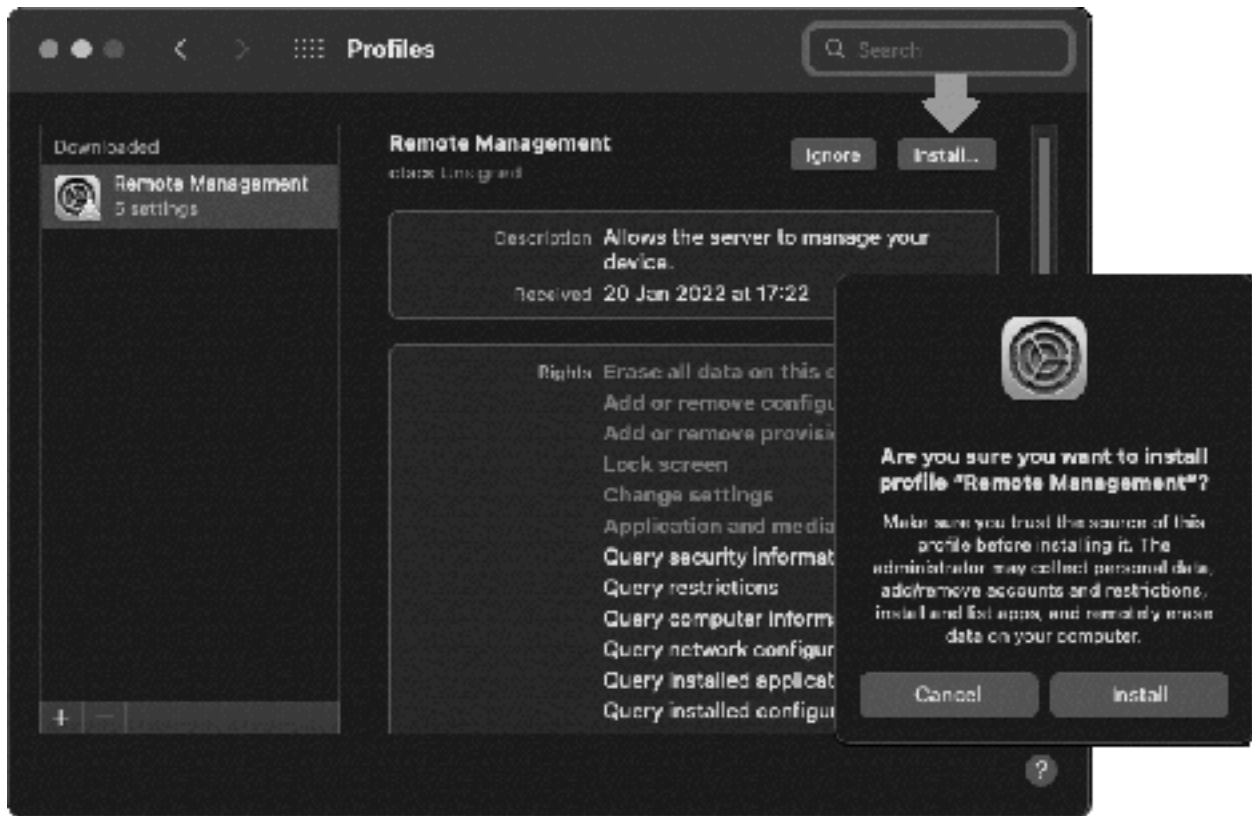


Figure 86: Installing a Profile

Click the **Install...** button in the top right-hand corner and then click **Install** on the pop-up panel. It is then necessary to enter the Administrator's password and click the **Enroll** button. After a few minutes the Profiles entry will be updated, confirming that the Mac has been successfully enrolled and is under the control of Profile Manager:

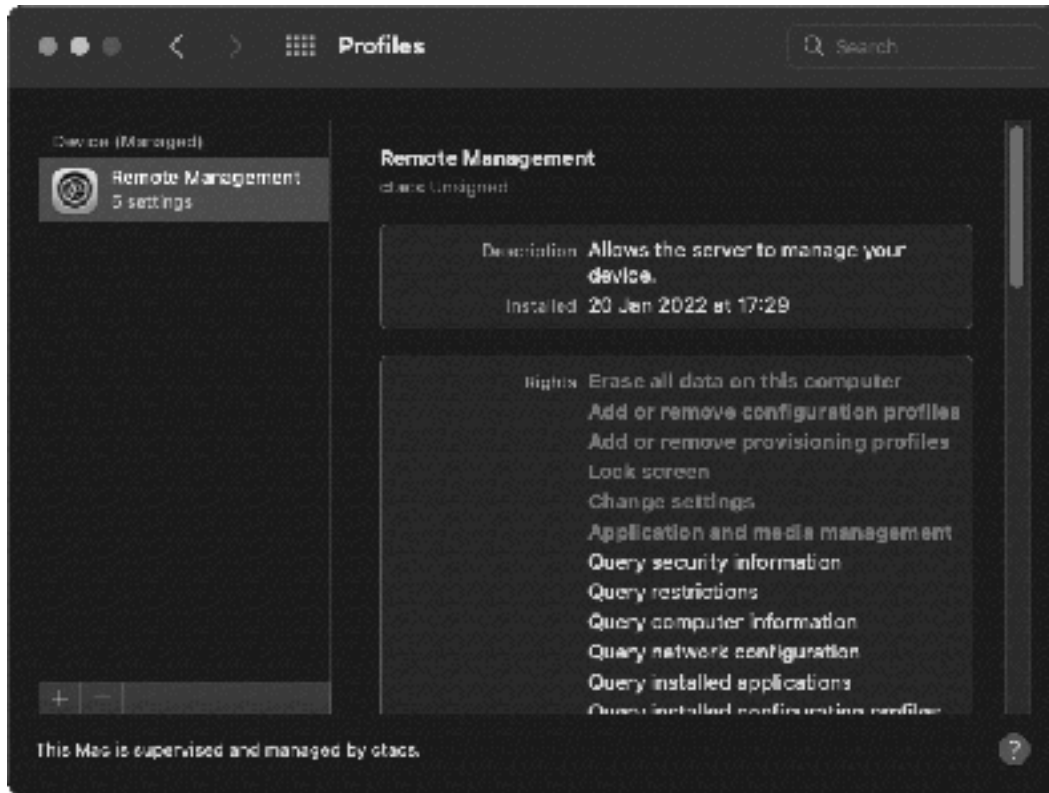


Figure 87: Successfully installed Profile

Note that in the above example the user's Mac is running macOS Monterey. With earlier versions of macOS, there may be some minor differences although the overall process is the same.

Returning to Safari, it will now appear as follows:

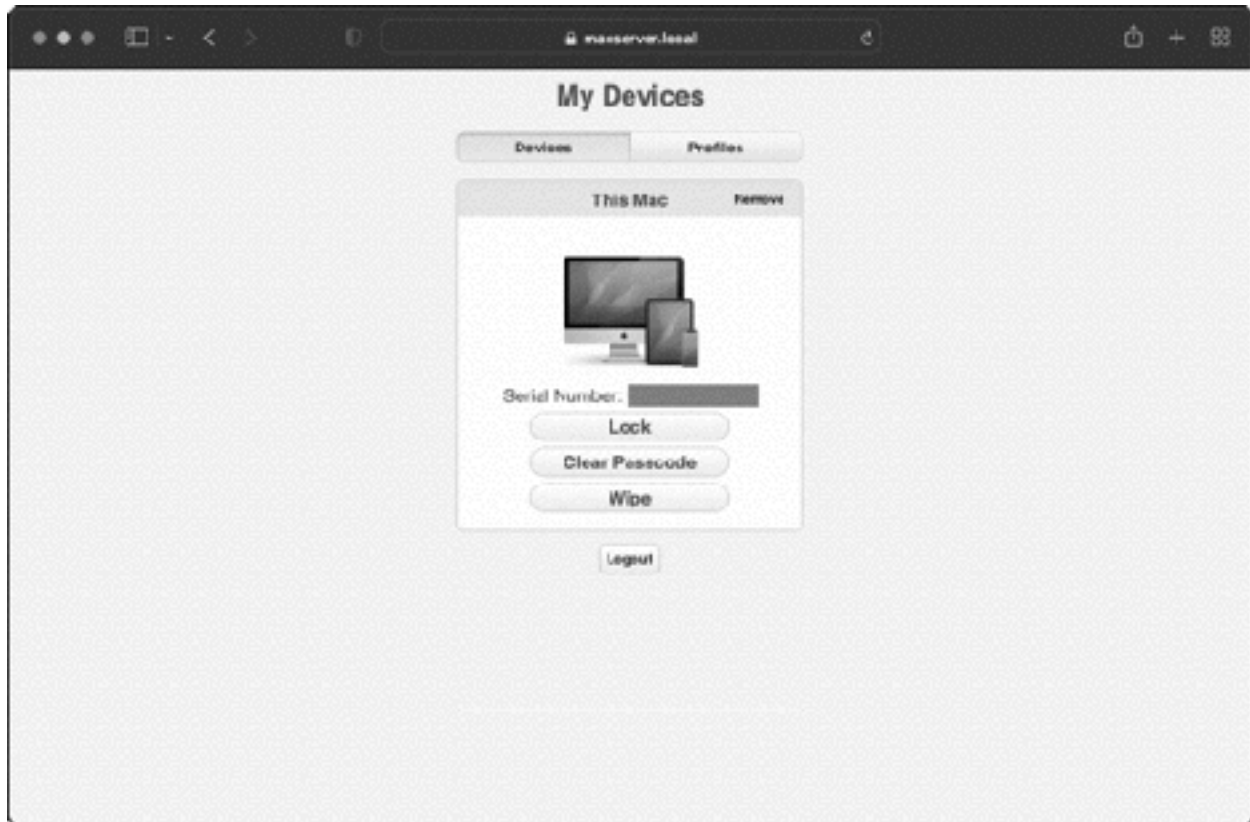


Figure 88: Enrolled computer

Having enrolled the device(s), specific profiles can now be created. On the server, click the **Open in Safari** button in *Profile Manager*. Within Safari, login to the server using *admin* credentials. You may receive a certificate warning, advising that ‘This Connection Is Not Private’. If you saw this message whilst accessing an external website, it would be a security concern, but as we know what we are connecting to it is safe. Click the **visit this website** link, followed by the **Visit Website** button on the subsequent pop-up (see section for [7.8 Certificate Error](#) additional information). Login to Profile Manager as the admin user for the server and the following screen is displayed:

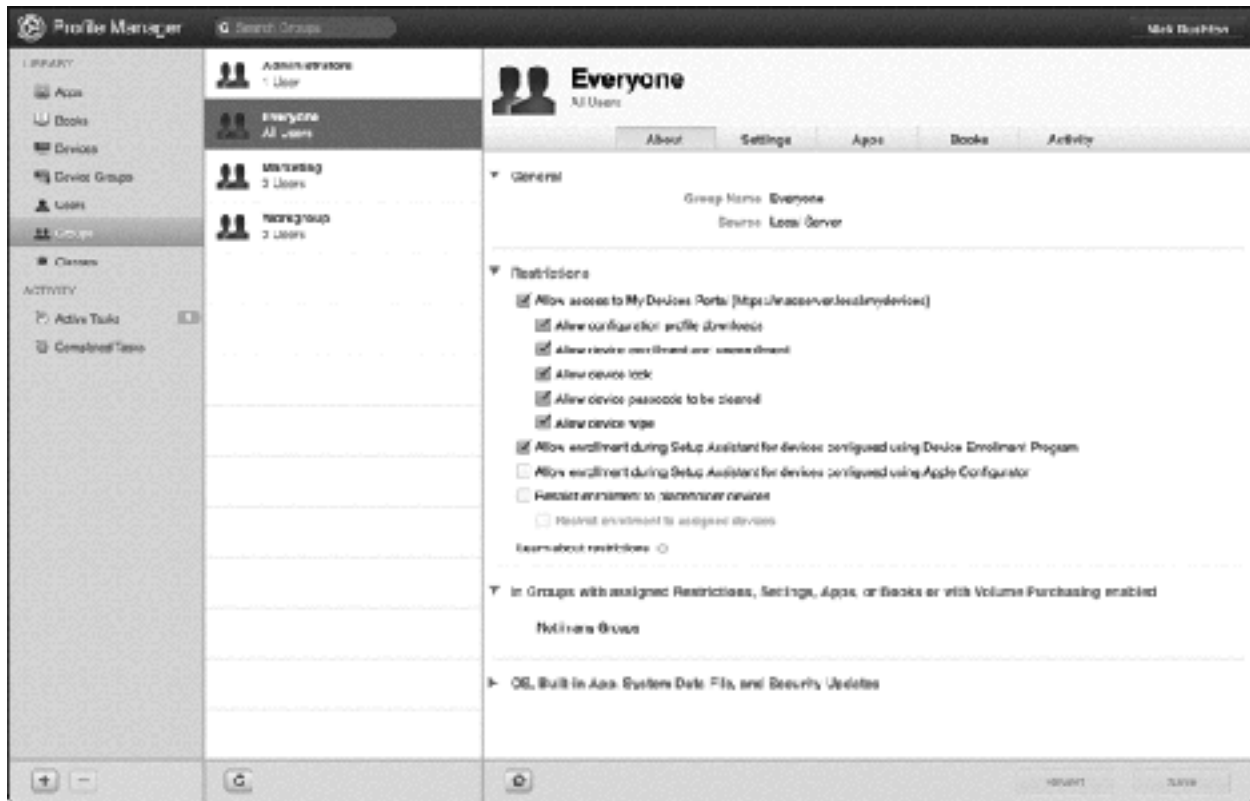


Figure 89: Profile Manager, main view in Safari

The screen is organized as three main panels. Down the left-hand side is the *LIBRARY* of categories that can be managed, consisting of: *Apps*; *Books*; *Devices*; *Device Groups*; *Users*; *Groups* and *Classes* (some of these are designed for use in schools and other educational institutions and may not be applicable in a business setting). Beneath the Library is an *ACTIVITY* section, which lists active and completed tasks; for example, enrolling a device would count as a task. The middle panel lists the items in the currently highlighted category; for instance, in the above screenshot *Groups* is highlighted so all the groups are listed i.e. *Administrators*, *Everyone*, *Marketing* and *Workgroup* in this case. On the right-hand panel are the details for the current item, frequently organized into a set of tabs.

Any users and groups that have been created within Server are automatically available to Profile Manager. For example, if you click on **Users** in the left-hand panel a list of all the users that have been created is shown. Clicking a particular user will then display their details in the right-hand panel.

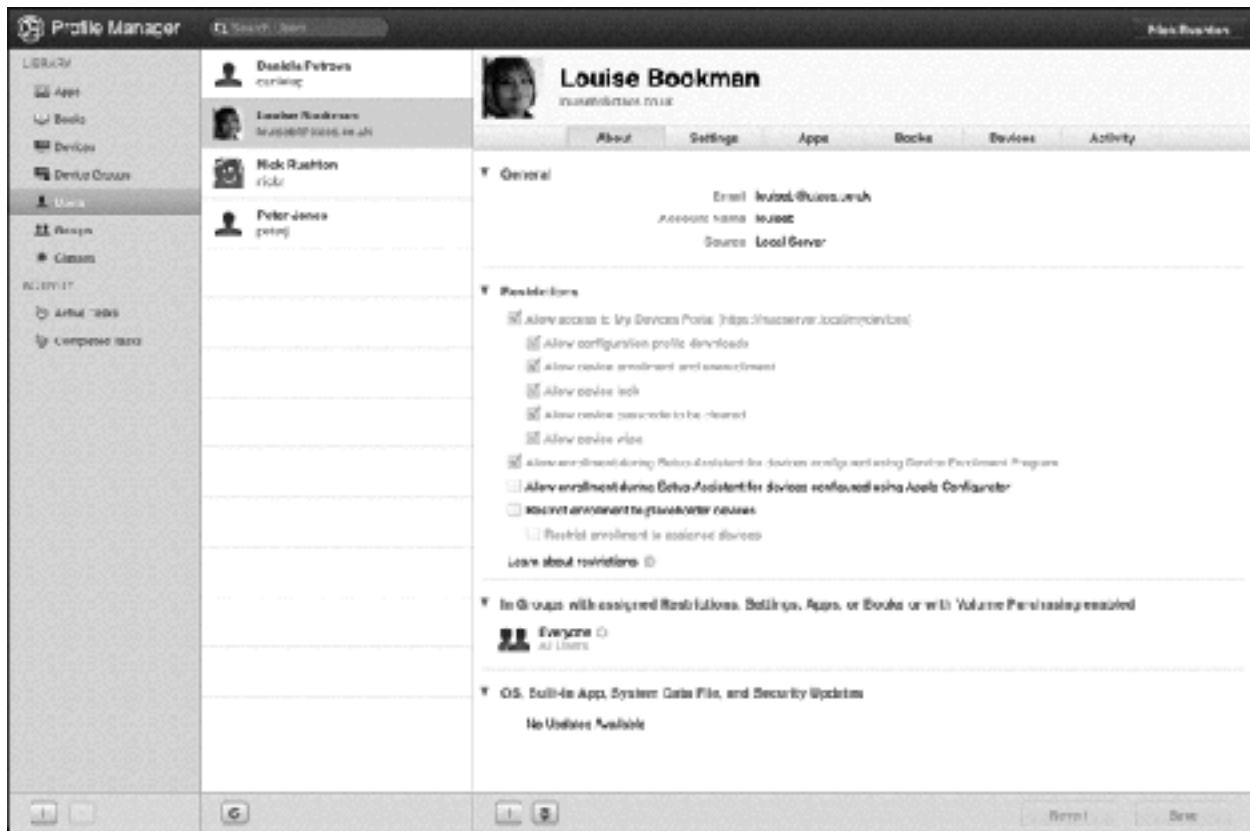


Figure 90: Details for a user

There are multiple tabs for the user, providing information about them and allowing management of various features and facilities. For instance, clicking **Devices** will display details of the devices associated with the user. In some instances, these tabs may have multiple panels within them or link to other sections within the wider Library:



Figure 91: Details of an enrolled device

Now click on *Users* in the left-hand panel. In the middle panel, find the user who was logged into a Mac that was enrolled and click their name to select them (in our example, Louise Bookman). Click the **Settings** tab. Towards the top of the screen is an on-off switch marked **General** and a button marked **Edit** – click either and the screen changes to this:

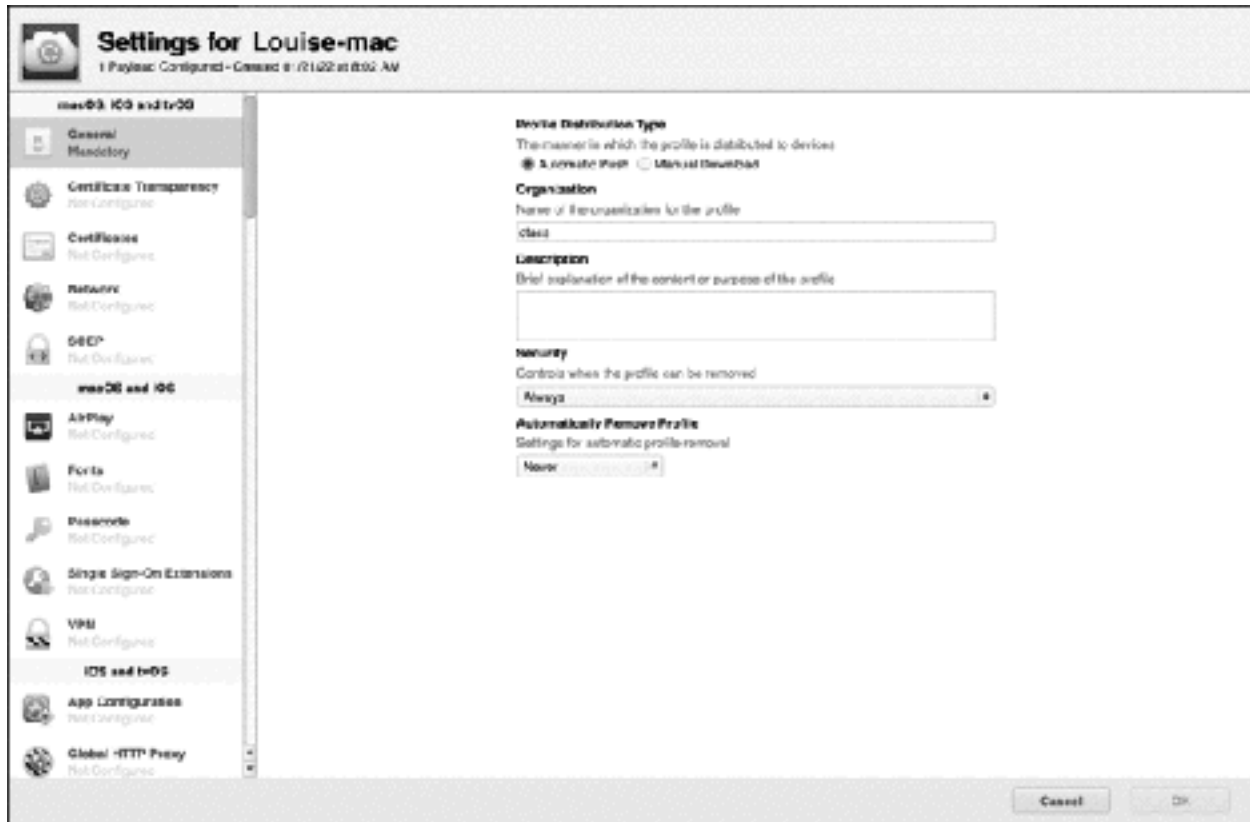


Figure 92: Settings for a user

Down the left-hand side of the screen are the various settings that can be controlled, categorized into macOS, iOS and tvOS (for Apple TV). This is where applications, server settings, the contents of the Home screens, plus many other items can be defined. For example, scroll down until you locate **Dock** in the macOS section and click the **Configure** button. There is a section marked *Dock Apps* – click the plus sign (+) underneath it and a list of apps is displayed. Find one and click **Add**, followed by **Done**. Continue scrolling down and at the bottom of the screen tick the **Network Home** box, plus make sure that the **Merge with User's Dock** box is ticked. Click **OK**:

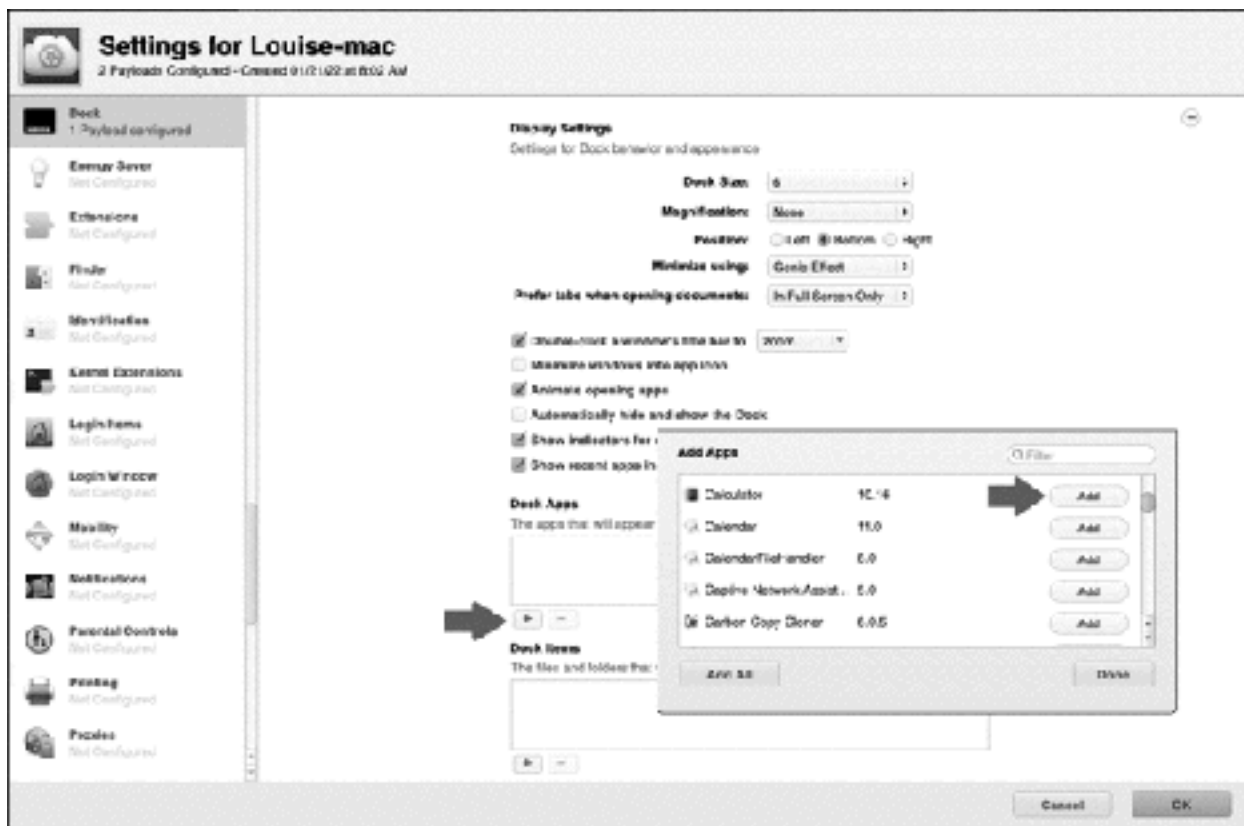


Figure 93: Settings for the Dock

Having been returned to the previous screen, click **Save**. The left-hand panel will update, with *Active Tasks* in the *ACTIVITY* section showing at least one active task. Go to the Mac you enrolled, restart it, and log in as the same user as before. The calculator and the user's network home folder should now be in place on the Dock.

9

Using Cloud Storage Services



Free edition. Do not copy or distribute. (c) CTACS

9.1 Overview

macOS has some basic features to enable remote access and working (for example, see [10.2 Screen Sharing](#)), plus it is also possible to obtain third party products that can improve on them. However, a simple and popular method to indirectly give remote access to data is by using a Cloud-based file sync service. These services can provide remote access to data in a simpler method with less effort and on a wider range of devices, plus may be able to provide controlled access to selected files for third parties via emailed links. They can also or alternatively be used as a way of backing up data from the server, providing offsite storage to complement the onsite backup. Examples of popular file sync services include *Dropbox* and *Microsoft OneDrive*. Apple have a similar offering in the form of iCloud and that may seem to be the obvious choice, but it is too intimately related to other Mac services to be a good choice for what we are going to do here.

There are six main considerations when using a cloud service with Server:

1. A single account is used for everyone.
2. The account should have sufficient space. Free accounts have limited space, so you may want to consider a paid subscription.
3. The number of devices supported. For instance, a free Dropbox account permits only three devices to use it (this restriction does not apply with paid accounts).
4. Decide whether it will be used for additional backups or as a means of providing remote access to data when away from the premises.
5. Who has access to it? If used for backups only, then only the server administrator needs access.
6. Who will be responsible for managing it, which is usually the person who controls the server administrator account.

9.2 Using Microsoft OneDrive with macOS Server

OneDrive is Microsoft's competitor to Dropbox and iCloud. Many homes and small businesses, even if otherwise committed to Apple's 'ecosphere', will use Microsoft Office. Subscription versions of Office include a generous 1TB of online storage via OneDrive; alternatively, 5GB of storage is available free of charge to anyone, or 100GB storage for £1.99/\$1.99 per month. OneDrive, and other cloud products such as Dropbox, have a crucial advantage over iCloud: it is possible to easily choose the location of the folders to be synced.

Begin by downloading OneDrive for Mac on the server – it can be found in the Mac App Store and on Microsoft's own website. Launch it by clicking its icon in the Applications folder, then enter the email address and password of your Microsoft account and Sign In. On the first proper screen, click the **Change Location** link, navigate to where you want the OneDrive folder to be in your storage area, and click **Choose this location**:

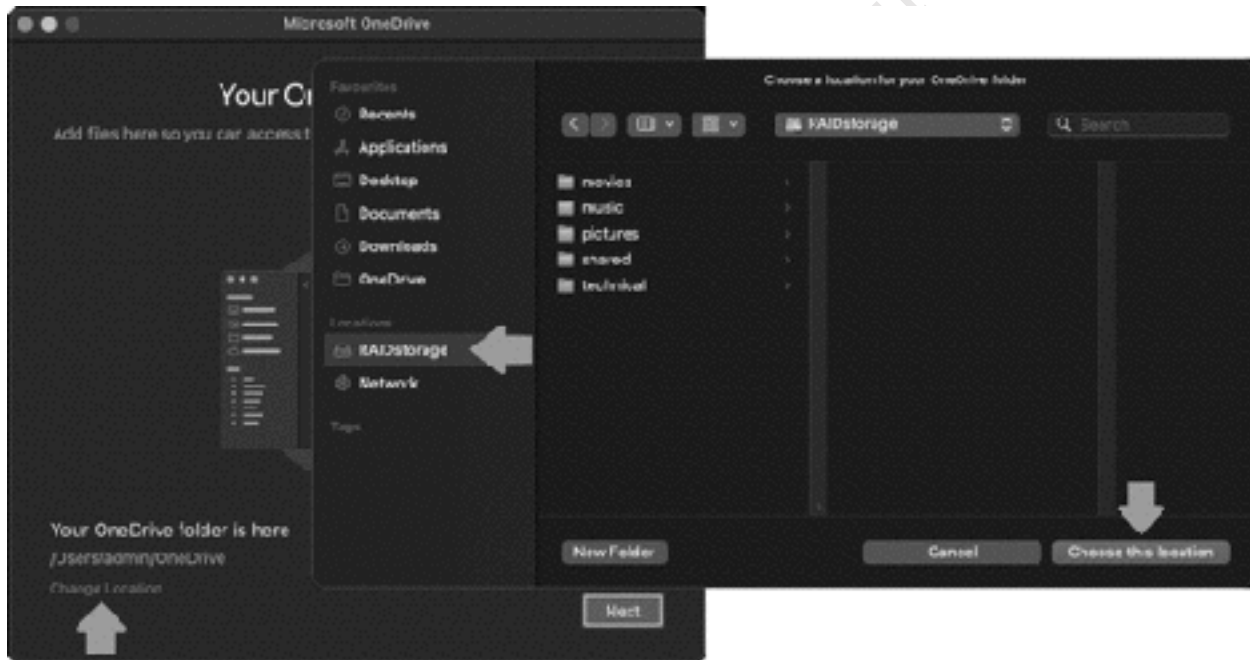


Figure 94: Specifying the location for the OneDrive folder

Having been returned to the original screen, click **Next** and allow the installation to continue. A small icon for OneDrive is placed in macOS's notification area; clicking it will display a status panel, from where the OneDrive folder can be accessed and from where settings can be adjusted. The OneDrive folder can also be accessed directly from Finder, or by clicking the OneDrive icon in Launchpad.

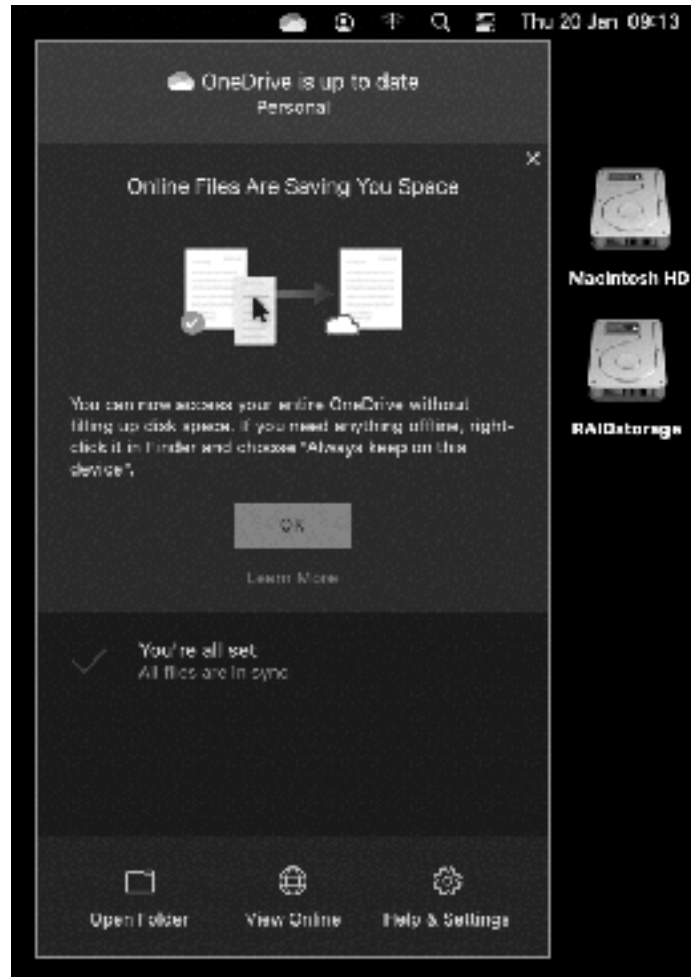


Figure 95: OneDrive control panel

The OneDrive folder can be used in two different ways. If you wish to use it for backup purposes only, simply place copies of files in it whilst logged in as the *admin* user. However, if you wish to use it to provide remote file access for users, it needs to be made into a shared folder so they can see it. Go into **System Preferences > Sharing**. Underneath the Shared Folders section, click the plus sign (+), navigate to where the OneDrive folder is, highlight it and click **Add**:

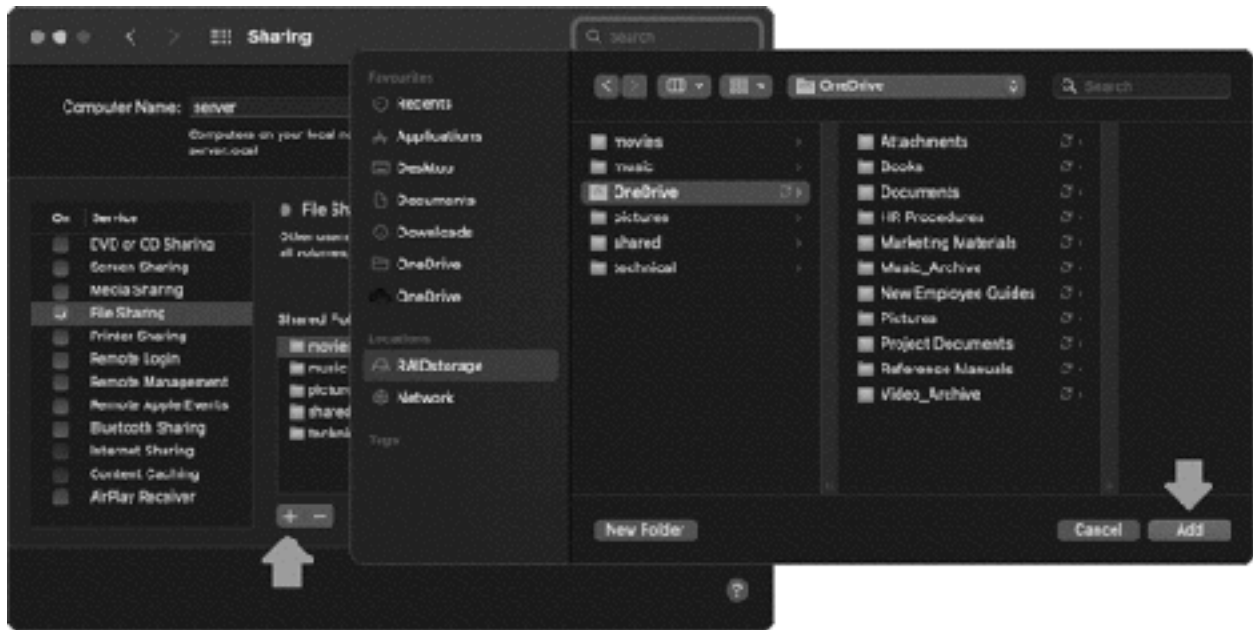


Figure 96: Add OneDrive to the list of shared folders

It is now necessary to specify the permissions. Click the plus sign (+) under the list of Users, highlight the users and/or groups that you wish to have access and click **Select**. Then, having added them, give them Read & Write permissions. If you want all users to have access, just add the *Everyone* group, as in this example. Also, check that the *OneDrive* user that was created automatically has Read & Write permissions:

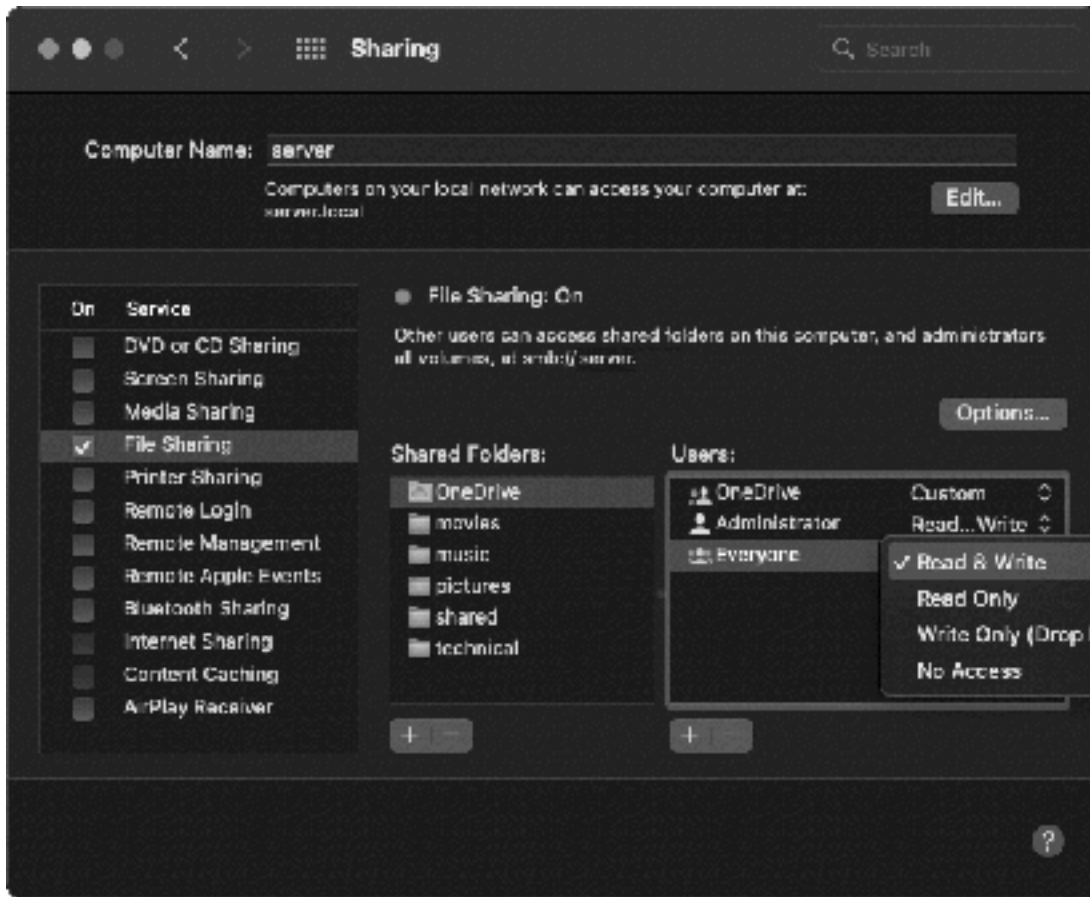


Figure 97: Specify permissions for the OneDrive folder

Users who have been granted access will now be able to place items in the OneDrive folder. To gain access from outside, the permitted users should have the OneDrive client installed on the devices they use outside of the premises, downloadable from www.microsoft.com or appropriate App stores. In a business setting, it is suggested that the users are not given the password and allowed to install it themselves to reduce the risk of errors or abuse, but rather it should be done for them. At the time of writing, OneDrive is available for: macOS, iOS, Windows, Xbox and Android.

One thing to consider is what happens when people leave the organization, as if they have OneDrive installed on a home-based computer, they will continue to have access to whatever is stored on the server's OneDrive folder. In such circumstances, it will be necessary for the administrator to change the password of the OneDrive account and advise remaining staff of the new password.

Using OneDrive to Expand Storage on the Server

By default, OneDrive operates in what Microsoft call *File On-Demand* mode. What this means is that although the folders and files appear to be stored on the computer, these are just icons or pointers and the data is actually stored at Microsoft. When a file is accessed e.g. by double clicking it or loading it into an application such as Word, Excel, PowerPoint etc, it is downloaded from Microsoft at that point i.e. on demand. This has three implications: firstly, there may be a slight delay as the file is retrieved, depending on its size and if the speed of the internet connection, although this may not be particularly noticeable. Secondly, if the server is not connected to the internet for whatever reason, then the file or the latest version of it may not be available. Thirdly, OneDrive can effectively be used to expand the storage capacity of the server, as it constitutes a 'virtual drive'. For instance, suppose the server is a Mac mini with a 256GB SSD drive. If there is a OneDrive subscription with 1TB storage, the server now potentially has access to 1.25TB of data, which represents a considerable increase.

With regards to the first two points about delays and availability, this can be resolved by turning off the File On-Demand feature. This will cause all the data to be downloaded from OneDrive to the Mac; however, this cancels the virtual storage capability and requires that the server has enough physical (real) disk storage to hold the data. To switch it off, go into OneDrive Preferences and click the **Turn Off Files On-Demand** button. There will be a warning message – click **OK** and the data will be downloaded (this may take a considerable amount of time, depending on the amount of data).

9.3 Using Dropbox with macOS Server

Install the Dropbox software on the server, which is best done by downloading it directly from the Dropbox website home page. Immediately after initial installation and before doing anything else, such as opening or accessing Dropbox, click the **Advanced Settings** option as this allows you to specify the location of the Dropbox folder.

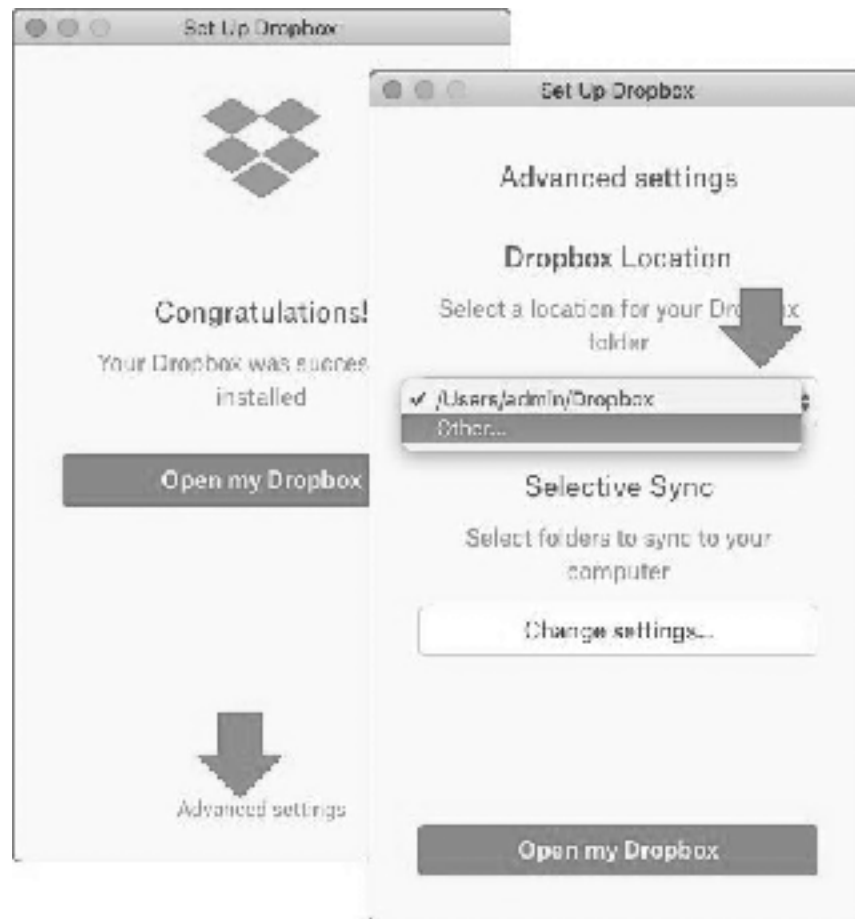


Figure 98: Click Advanced settings

Navigate to the location where you are storing the shared folders and click **Select**. Note that it is not necessary to click the *New Folder* button, as Dropbox is controlling matters and will create an appropriate folder automatically. In our example, we are using a location called *RAIDstorage*. If you are prompted to specify the admin credentials, do so. Upon installation, there is a short tour of Dropbox.

The Dropbox folder can be used in two different ways. If you wish to use it for backup purposes only, simply place copies of files in it whilst logged in as the *admin* user. However, if you wish to use it to provide remote file access for users, it needs to be made into a shared folder so they can see it. Go into **System Preferences > Sharing**. Underneath the *Shared Folders* section, click the plus sign (+), navigate to where the Dropbox folder is, highlight it and click **Add**:

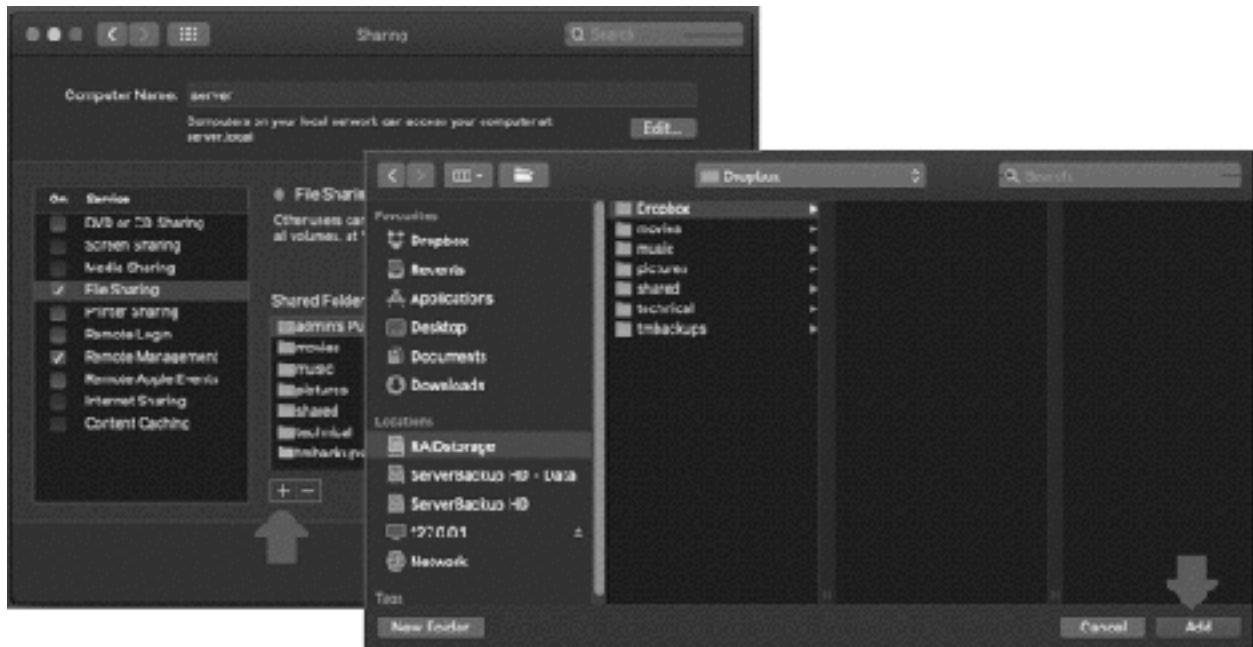


Figure 99: Add Dropbox to the list of shared folders

It is now necessary to specify the permissions. Click the plus sign (+) under the list of Users, highlight the users and/or groups that you wish to have access and click **Select**. Then, having added them, give them Read & Write permissions. If you want everyone to have access, just add the Workgroup group, as in this example. Also, make sure the *Dropbox* user that was created automatically has Read & Write permissions. Remember that the permissions option of *Write Only (Drop Box)* is, confusingly, nothing to do with Dropbox itself.



Figure 100: Specify permissions for the Dropbox folder

Users who have been granted access will now be able to place items in the Dropbox folder. To gain access from outside, the permitted users should have the Dropbox client installed on the devices they use outside of the premises, downloadable from www.dropbox.com. In a business setting, it is suggested that the users are not given the password and allowed to install it themselves, to reduce the risk of errors or abuse, but rather it should be done for them. At the time of writing, Dropbox is available for: Windows, Mac, iPad & iPhone, Android and selected Linux distributions.

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 Business has the capability to 'remote wipe' devices and this can be used to remove the organization's data from the former user's computer.

10

Miscellaneous Topics



Free edition. Do not copy or distribute. (c) CTACS

10.1 Overview

This chapter contains a selection of miscellaneous topics which do not fit elsewhere, such as sharing media files and content caching, plus those of a more advanced nature such as RAID configuration and using multiple network adapters.

10.2 Screen Sharing

To run the server without a monitor, keyboard and mouse - sometimes described as *headless* mode - and to access it for support and other purposes, the *Screen Sharing* capability of Server can be used. This has several advantages: firstly, the server can be managed using any Mac on the network and it is not necessary to have physical access to it, 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 a small amount of electrical power. Thirdly, in some small organizations the server may have to be physically located in a general purpose office and not having a keyboard and screen will reduce the temptation for staff to treat it as 'just another computer' that they can use. And in larger organizations, with multiple servers, the ability to manage any of them from the comfort of your own desk would clearly be very convenient.

Begin by enabling the feature on the server. On the main screen of Server, click the **Settings** tab and on it tick the box for **Screen Sharing and Apple Remote Desktop app**:



Figure 101: Enabling Screen Sharing and Apple Remote Desktop app

Go to another Mac, for example the one you normally use yourself, and open a Finder window. Double-click on the server to highlight it, then click the **Share Screen** button at the top of the window. You will be prompted to enter the administrator's name and password as defined on the server:

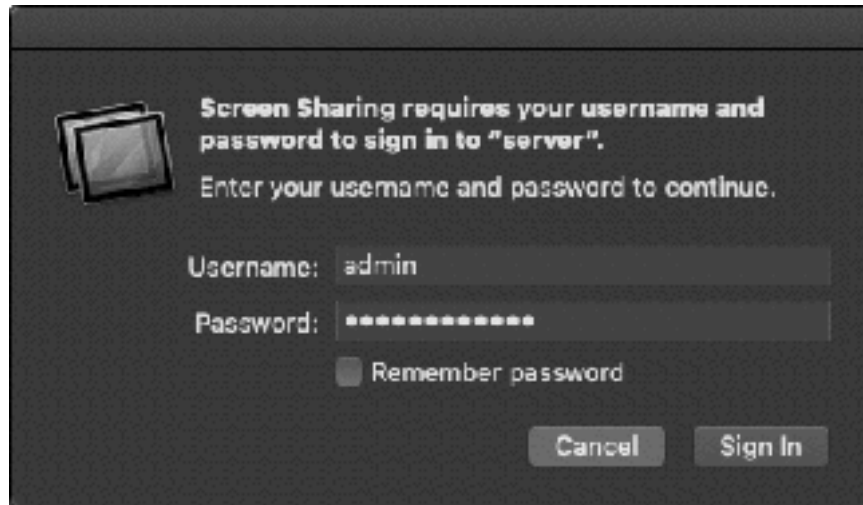


Figure 102: Enter credentials for the server

Having logged in, you will be presented with the main screen of the server but contained within its own window. To all intents and purposes, it is as though you were sitting in front of it and you can do the same things that you could if you were doing so.

10.3 Accounts Browser

The *Accounts Browser* provides an alternative way of selecting user names and can be useful on larger networks. It is invoked by choosing **Window > Show Accounts Browser** from the server's menu bar, alternatively you can press **Command (⌘)B**. It comprises a scrollable list of all user accounts, which can then simply be dragged onto the feature you are working with. To select multiple users at once, hold down the **Command (⌘)** key and click the user names. It is also possible to search for specific users. In this example, the Accounts Browser is being used to help populate a group with additional users.

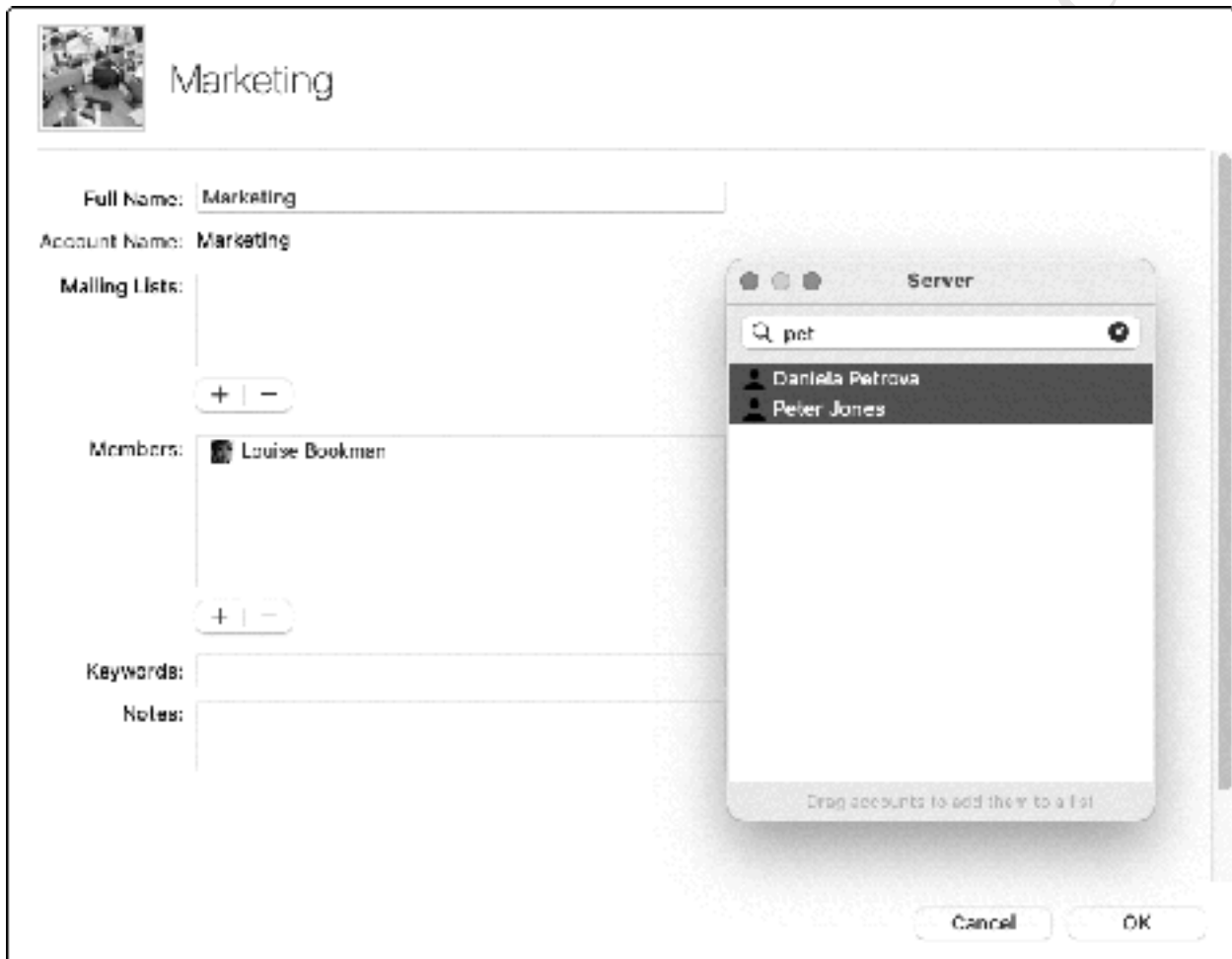


Figure 103: Drag names from the Accounts Browser

The Accounts Browser can optionally be left on display all the time. Alternatively, to put it away press **Command (⌘)B** again or choose **Windows > Hide Accounts Browser** from the menu bar.

10.4 Sharing Media Files

Music, videos and photographs stored on the server can easily be shared by other computers on the network, by both Macs and Windows PCs. Begin by copying your media into the folders we created earlier in section [4.3 Creating Shared Folders](#) i.e. music into *music*, photos into *pictures*, videos into *movies* (although you could create and/or use additional shared folders if you wished).

To access the media from another computer, connect to the server using one of the techniques described in Chapter [5 Accessing the Server](#) and open the *music*, *pictures* or *movies* shared folder(s) as required. Double-click the file to play it using the computer's default media player, or right-click it and choose the **Open With** option. Some of the common media players include:

Versions of macOS from Catalina onwards

Use *Music* or *QuickTime* for audio files; *QuickTime* for videos; *Preview* for photographs.

Versions of macOS before Catalina

Use *iTunes* or *QuickTime* for audio files; *QuickTime* for videos; *Preview* for photographs.

Windows 10 and Windows 11

Use *Windows Media Player* or *Groove Music* for audio files; *Films & TV* for videos; *Photos* for photographs. In recent versions of Windows 11, use *Media Player* for audio files and videos.

Windows 7

Use *Windows Media Player* for audio files; *Windows Media Player* for videos; *Windows Photo Viewer* for photographs

Alternatively, using the *Music* app on the server, you can make the content available to other users through it. Launch Music and import your music files (**File > Import**, then navigate to the *music* folder in your shared storage area). When complete, go into **System Preferences > Sharing**. Tick the **Share media with guests** box in the *Media Sharing* section, which will also cause the **Media Sharing** box to be ticked. Click **Options** and select **All songs, films and TV shows** or **Selected playlists** followed by **OK** (optionally, you can also specify a password to restrict access). You may also wish to change the **Library Name**.



Figure 104: Setting up Media Sharing

To access the media from other computers:

macOS 10.15 onwards

Launch Music. On the left-hand side of the screen, change where it reads 'My Library' to 'Server Library' (or whatever your library is named). The local copy of Music can now play the music collection stored on the server.

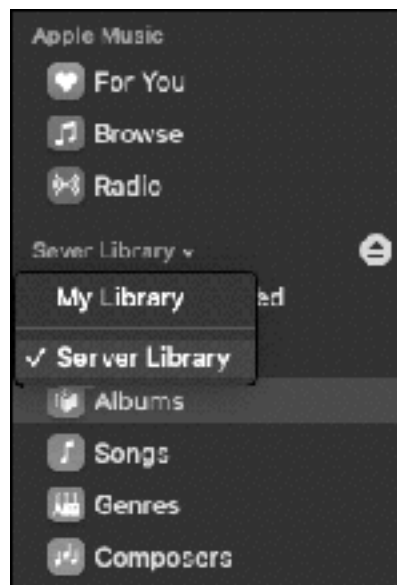


Figure 105: Connect to Music on the server

macOS before 10.15, or Windows

Launch iTunes (if you are using Windows, a copy of iTunes will need to be downloaded and installed, as it is not an integral part of the operating system as on a Mac). Click where it reads 'Music' in the top left-hand corner of iTunes and the server should be listed; however, note that it may refer to it as *admin's Library* or similar, rather than as 'server'. Click to select it. The local copy of iTunes can now play the music collection stored on the server.

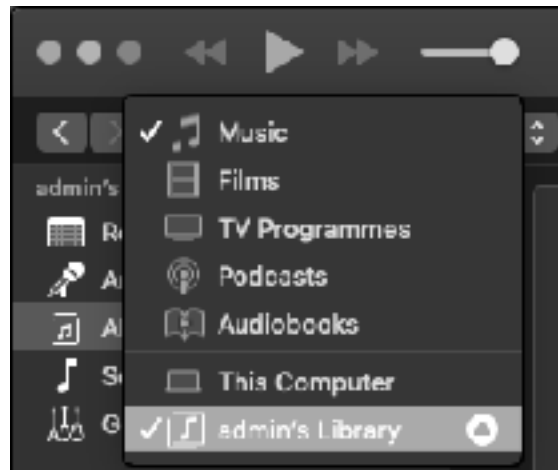


Figure 106: Connect to iTunes on the server

Universal Media Server

The media sharing as described above is rudimentary. For a more sophisticated solution, third party products are available, which can stream to a wider variety of devices e.g. smart TVs, and include features such as transcoding. An example of a totally free product that can do this is *Universal Media Server*, downloadable from www.universalmediaserver.com. Having installed it, click on the **Shared Content** tab and set the *Shared folders* to point at where your videos and music are stored. Also, on the **General Settings** tab, in the *Network settings (advanced)* section, use the *Force networking on interface* dropdown to use the main network interface e.g. en0.

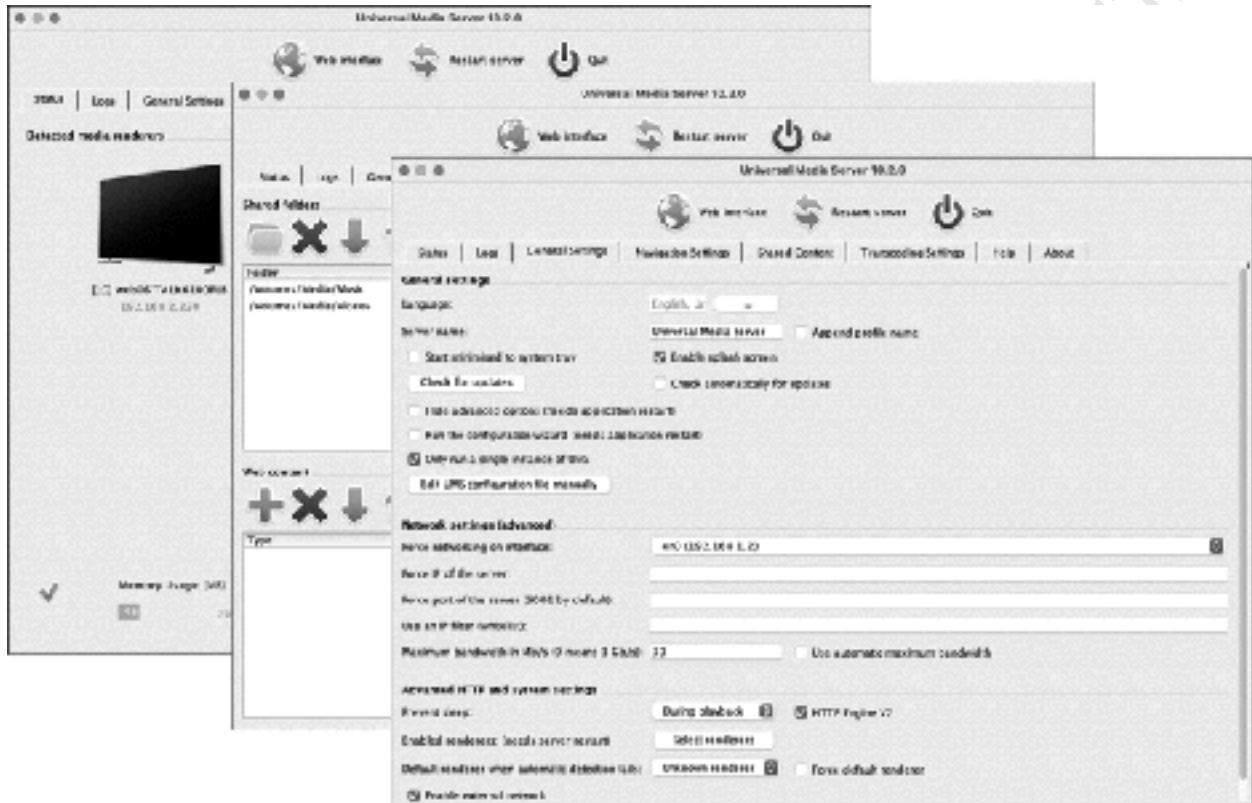


Figure 107: Configuring Universal Media Server

10.5 Configuring Additional Storage for RAID

As discussed earlier in section [1.5 Storage and RAID](#), you may need or want to add additional storage to the server. There are several ways of going about this, but a common solution in a small network is to add one or more external hard drives to the server. In this example, our server has a single built-in drive, upon which macOS and macOS Server have been installed. A pair of external drives will now be added to the server and configured for RAID operation, upon which all shared and user data will be stored. For best results, these drives should be identical in terms of brand and capacity.

Connect the drives. It is very important that external drives are firmly connected, as a drive being removed or becoming disconnected during operation of the server will result in data loss and other problems. You may want to consider such techniques as using cable ties and keeping the server and drives locked in a cabinet or cupboard.

Go into *Disk Utility*, which can be accessed by clicking **Launchpad** > **Other** > **Disk Utility**. Make sure that the external drives are listed, then click **File** > **RAID Assistant**:

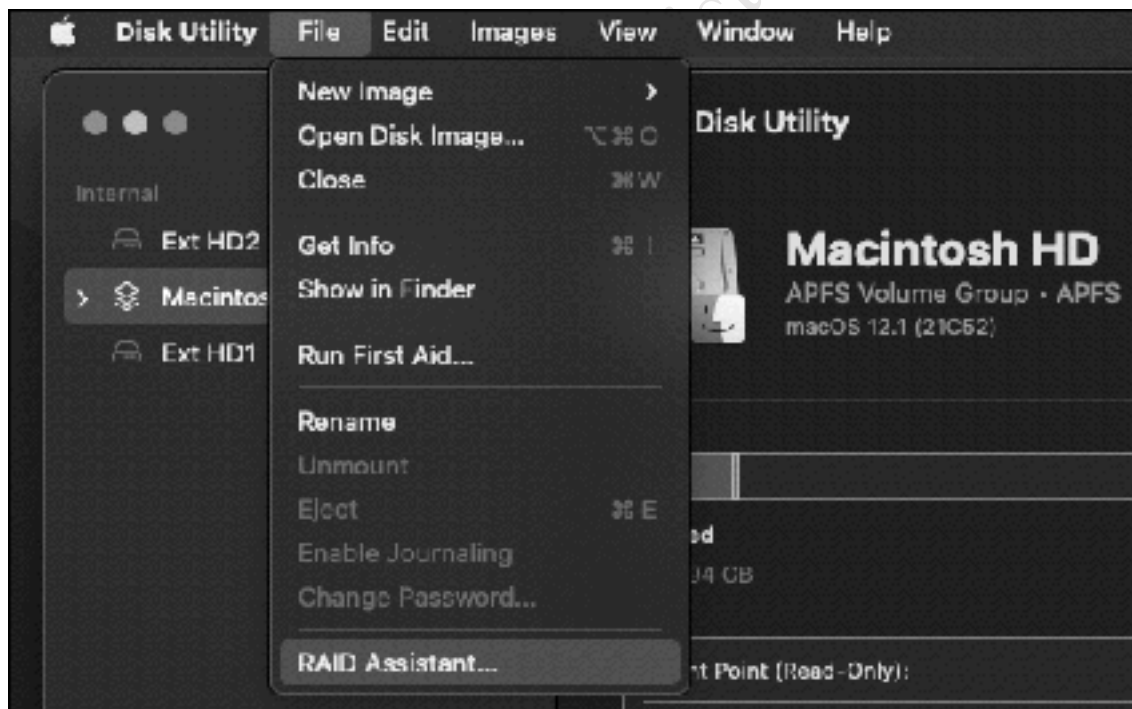


Figure 108: Disk Utility

Within RAID Assistant, select the RAID type. A description of the different RAID modes can be found in section [1.5 Storage and RAID](#), but in summary: RAID 0 ('Striped') provides maximum performance; RAID 1 ('Mirrored') provides data security; JBOD ('Concatenated') provides the maximum amount of storage. Note that the RAID Assistant is not sophisticated enough to handle

all the possible RAID levels that exist but is still perfectly adequate for many setups. We will use RAID 1, which is a common choice in a small network:



Figure 109: Select RAID type

Click **Next**. On the subsequent screen, tick the drives that will be used for the RAID storage and click **Next** (when selected, their role will change to 'RAID Slice'):

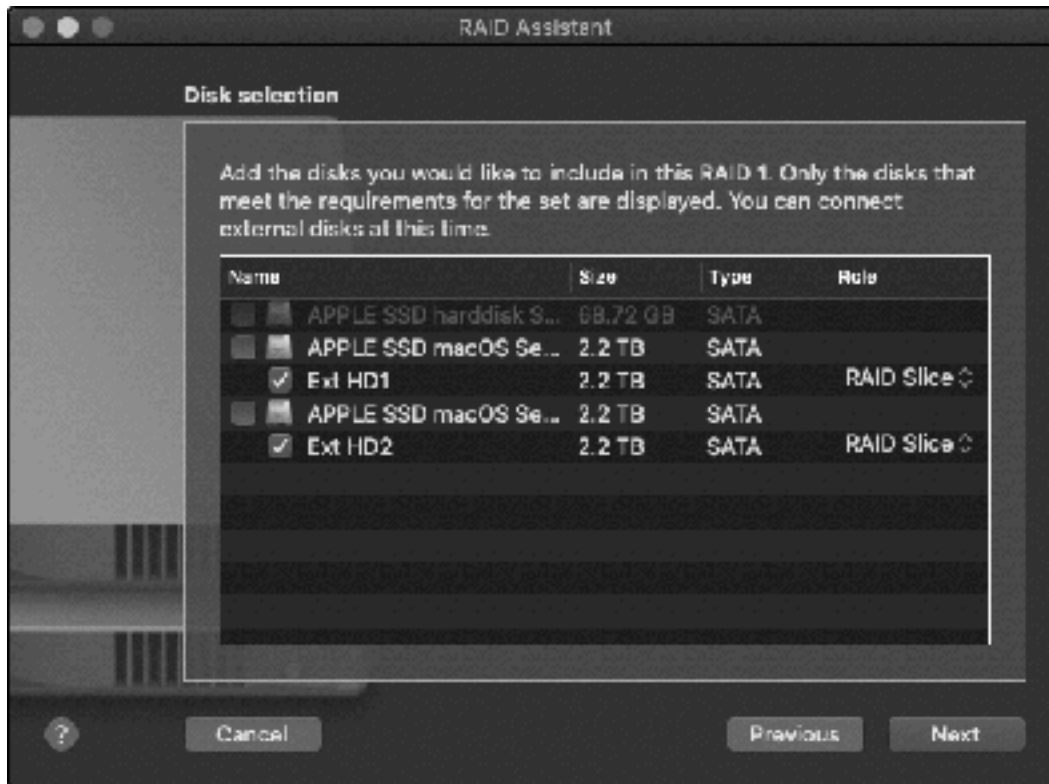


Figure 110: Select the drives

The defaults on the next screen will be suitable in most instances, but you may wish to change the *Name* to something more descriptive e.g. *RAIDstorage*. Click **Next** to continue:

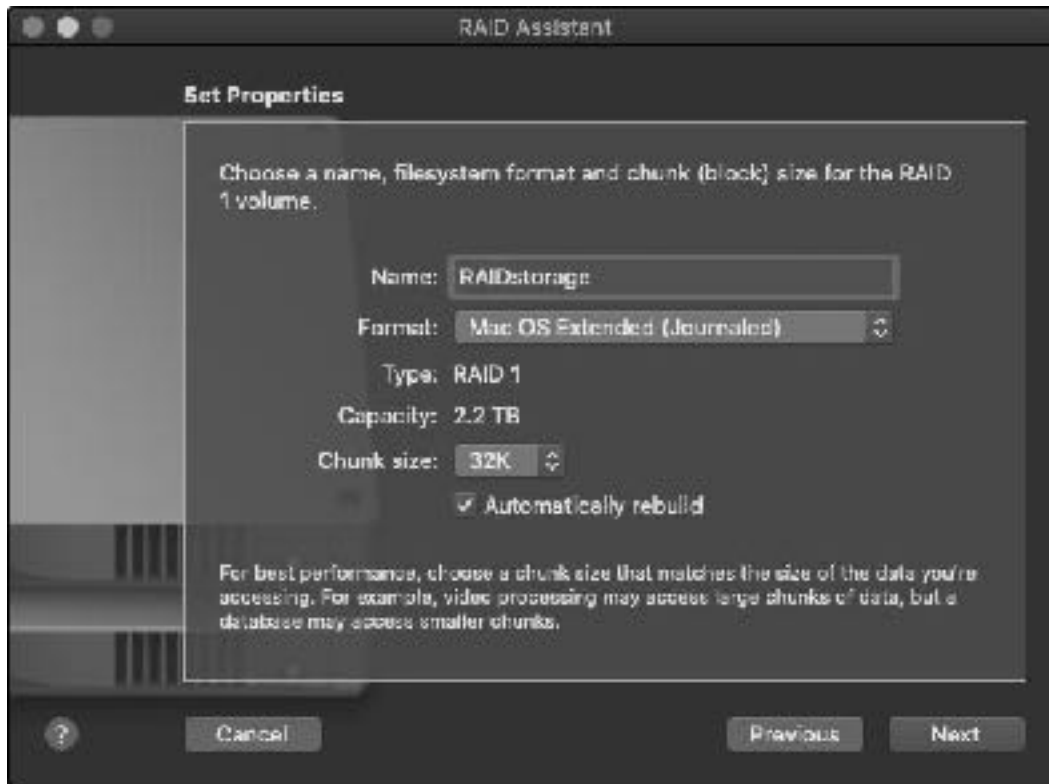


Figure 111: Set Properties

A warning message will be displayed, advising that any data on the RAID drives will be deleted. Click **Create** to proceed. The time taken for the RAID array to be created depends upon the capacity of the drives, their type, plus the connection method; for instance, a pair of 1TB SSDs with Thunderbolt connections will initialize more quickly than a pair of 10TB mechanical hard drives with USB 3.0 connections. When the RAID is ready, a confirmation message is displayed – click **Done** then close the Disk Utility. If Finder Preferences have been set to show external drives, the RAID storage will appear on the Desktop.

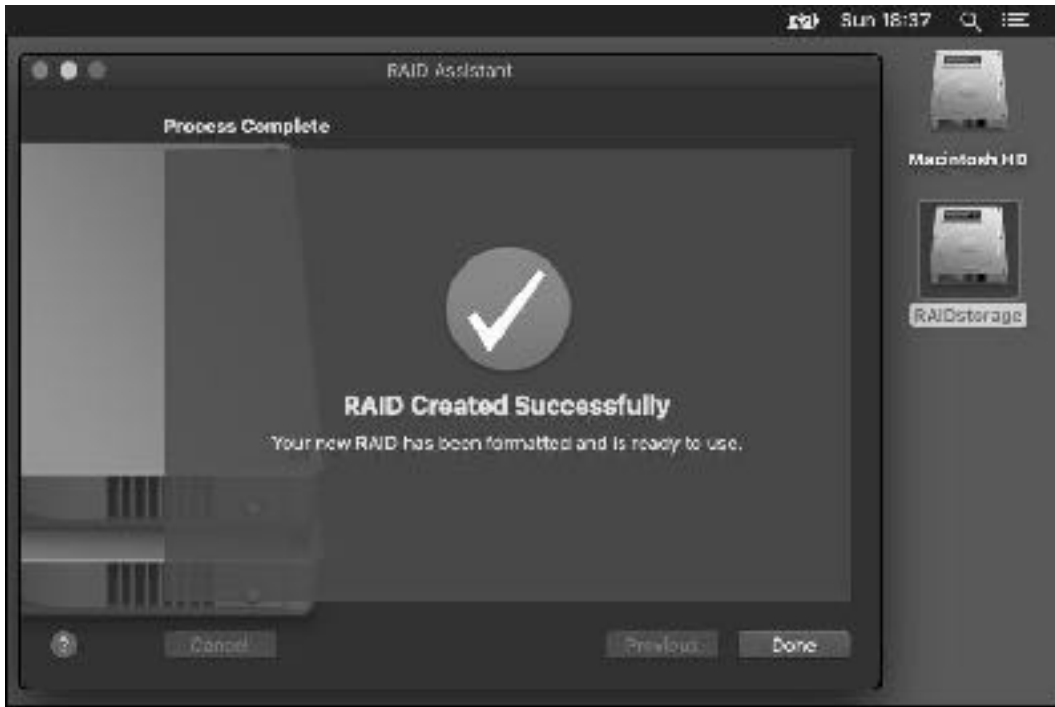


Figure 112: RAID created successfully

Free edition. Do not copy or distribute.

10.6 Link Aggregation for Network Adapters

Link Aggregation – also known as network teaming or bonding – is a technique whereby two or more Ethernet network adapters on the server can be linked together. There are two key advantages in doing so; firstly, network performance is improved, for example two 1Gbit adaptors will potentially double the throughput to 2Gbits. Secondly, resilience is improved, as if one connection fails then the other can be configured to take over automatically. There are several types of failure that can occur: an adapter can fail; a port on a network switch can fail; an Ethernet cable can become unplugged.

The use of multiple network adapters is standard on business file servers; however, Apple do not manufacture file servers and at the time of writing the only model with dual network adapters is the Mac Pro. However, additional adapters can be added to many Macs using Thunderbolt-to-Ethernet Adapters, available at relatively low cost from Apple. Also, some older Mac models can take PCI Express cards and Ethernet adapters are readily available in this format.

In this example, we will assume that the server has been equipped with a second Ethernet adapter. Both adapters should be connected to the same network switch. This should be a managed switch and one that supports 802.3ad protocol.

Go into **System Preferences**, click on **Network** and verify that both Ethernet adapters are working. The first adapter should have a fixed or static IP address, as described in section [2.3 Changing the Computer Name, Host Name and IP Address](#); the second adaptor should be set to pick up an address using DHCP. Click on the menu wheel at the bottom of the screen and choose **Manage Virtual Interfaces**:

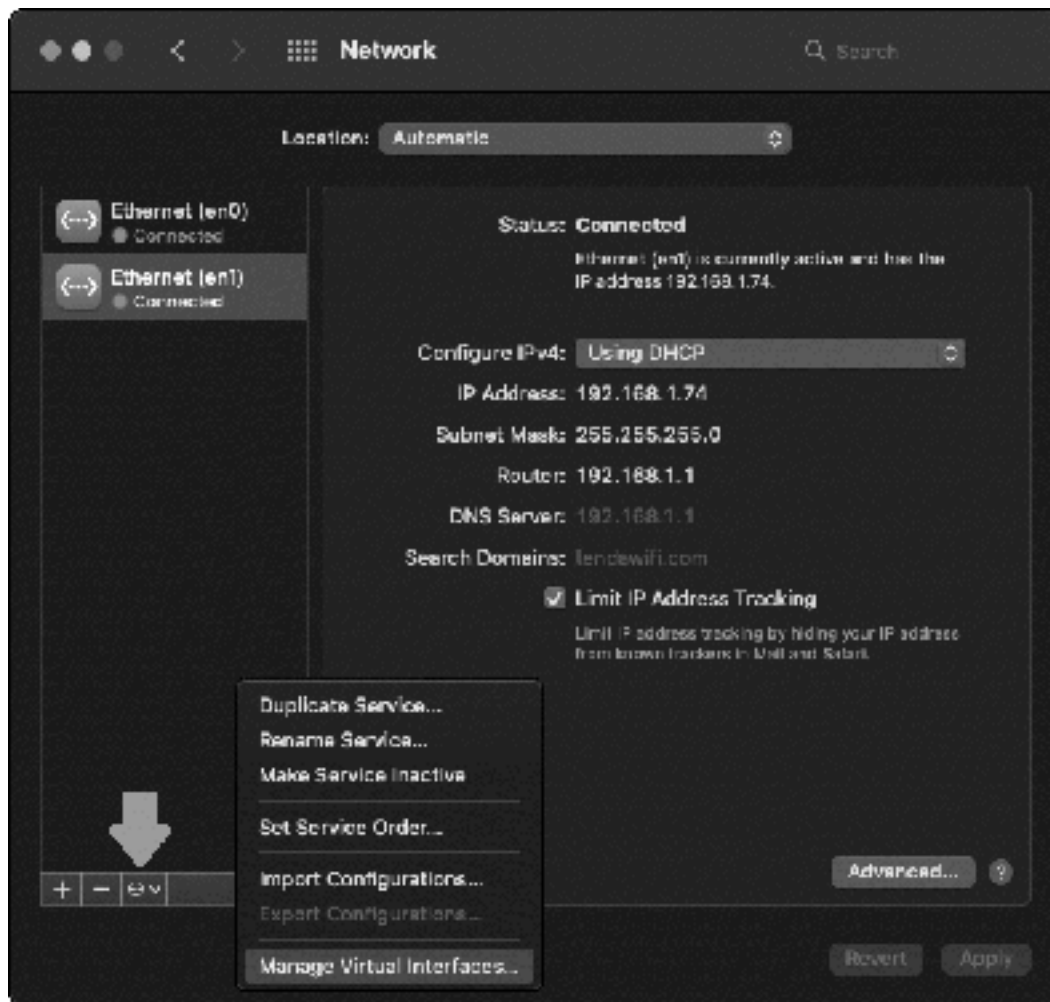


Figure 113: Network settings before aggregation

On the resultant pop-up panel, click the plus sign (+) in the bottom left-hand corner and select **New Link Aggregate**. On the subsequent panel, tick the two Ethernet adapters, optionally specify a name, click **Create**. Upon returning to the previous panel, click **Done**.



Figure 114: Defining the New Link Aggregate

They may be a disruption to service for several seconds, after which the new bonded adapter should start working (don't panic if it takes a little longer). There is a possibility that it has reverted to DHCP and picked up the wrong IP address, in which case it should be set back manually to the original address of the server i.e. the address that was being used by the first adapter prior to aggregation. It can be reset within **System Preferences > Network**, after which it should appear along these lines. It is suggested that you test the bonding by removed one of the network cables – the server should stay online. Then, try restoring the cable and removing the second one.

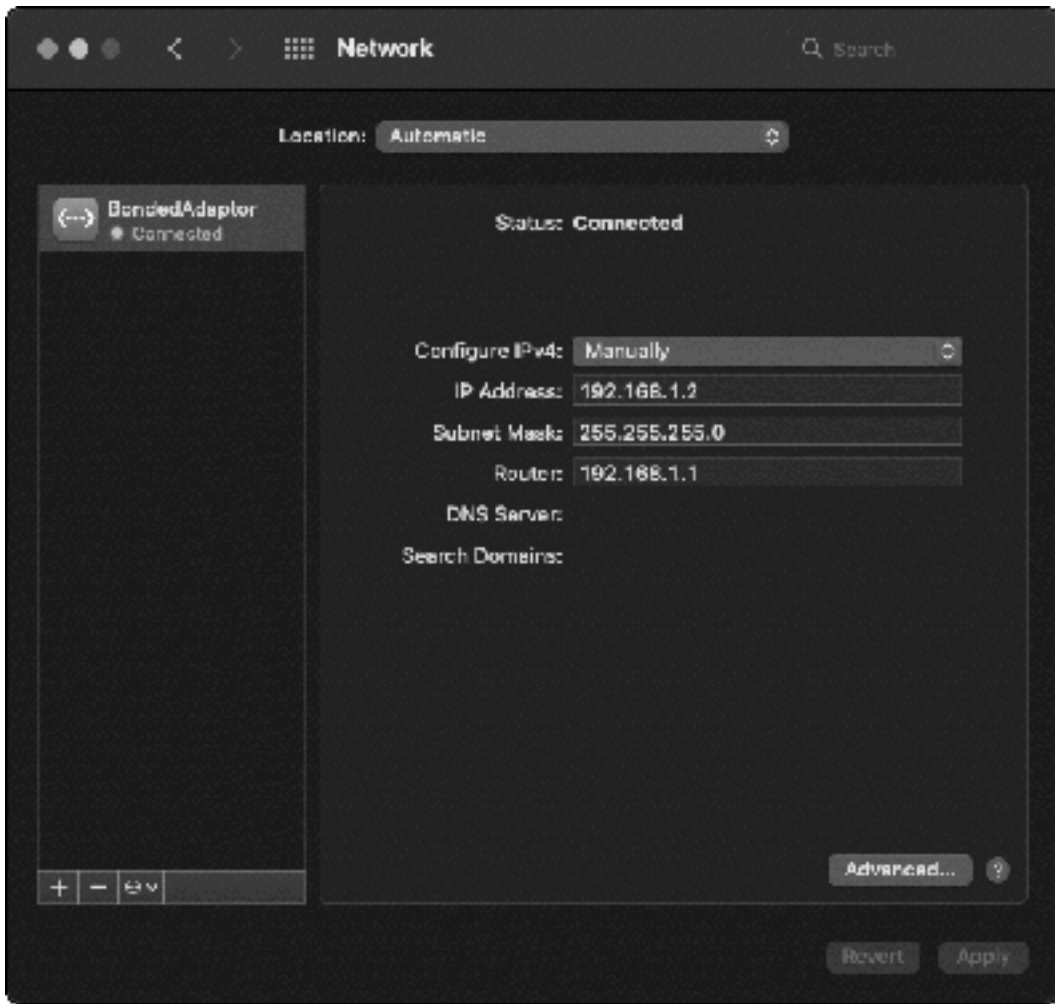


Figure 115: Network settings after aggregation

10.7 DNS Issues

DNS, or *Domain Name Service*, is how IP numbers are resolved into websites on the internet and device names on a local area network, to make them more manageable. For instance, it is easier to remember a name like *www.ctacs.co.uk* rather than a number like 84.22.161.134. Similarly, in a local area network, it is easier to refer to, say, *louise-mac* rather than an IP address such as 192.168.1.88. In a typical small network, DNS is handled by the router (earlier versions of macOS Server were able to provide their own DNS service, but this frequently tended to be problematic and was eventually dropped).

A common problem when trying to connect client computers to the network is that the macOS server cannot be found and an error message will be given, or something will simply not work. This is often caused by DNS difficulties. There is a workaround that you may get away with in a very small setup: try referring to the server by its IP address rather than its name e.g. *192.168.1.2* rather than *macserver*. However, the proper solution is to make sure that DNS is configured correctly on the computers and that they explicitly reference the router for DNS.

In the case of Macs, this is done by going into **System Preferences** > **Network**. Identify the network connection, highlight it and confirm that the *DNS Server* corresponds to IP address of the router. If it does not, click the **Advanced** button. On the resultant screen, click the **DNS** tab. Using the plus (+) and minus (-) signs in the bottom left-hand corner of the screen, add or remove the entries such that only the IP address of the router is listed. Also, remove any Search Domains that may be listed. Click **OK**, followed by **Apply** on the original screen.

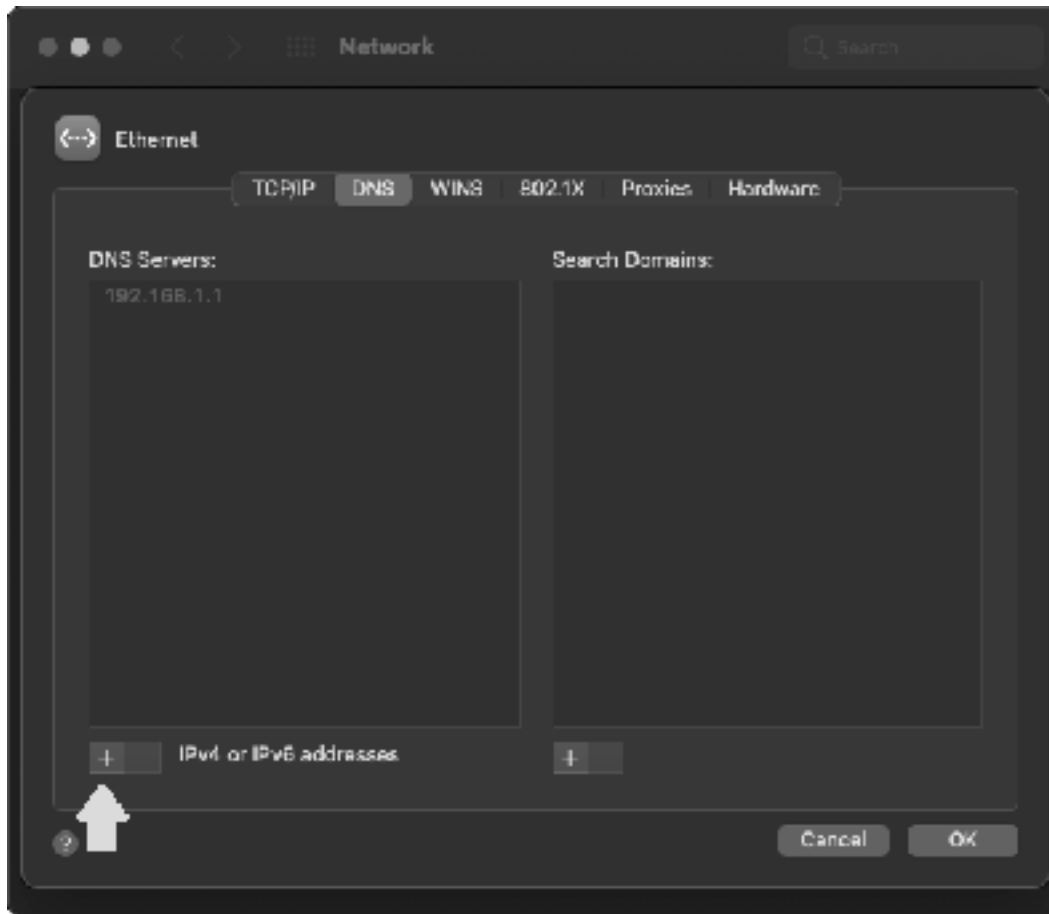


Figure 116: DNS settings in macOS

In the case of Windows PCs, go into the network adapter settings for each PC:

For Windows 11, right-click **Start** and choose **Network Connections**. Click **Ethernet**. Where it reads *DNS server assignment*, click **Edit**. Change the dropdown from Automatic (DHCP) to **Manual**. Slide the IPv4 switch to the right-hand side (which is the 'On' position). On the resultant panel, enter the *Preferred DNS address* i.e. the IP address of the router and click **Save**.

For Windows 10, click **Settings** > **Network & Internet** and the active network adapter e.g. **Ethernet**. **Change Adapter Settings**. Right-click the adapter, choose **Properties**, highlight **Internet Protocol Version 4 (TCP/IPv4)**, click **Properties**. Click **Use the following DNS server addresses** and specify the IP address of the router. Click **OK** and **Close**.

For earlier versions of Windows, it is usually: **Control Panel > Network and Sharing Center > Change Adapter Settings**. Right-click the adapter, choose **Properties**, highlight **Internet Protocol Version 4 (TCP/IPv4)**, click **Properties**. Click **Use the following DNS server addresses** and specify the IP address of the router. Click **OK** and **Close**.

Free edition. Do not copy or distribute. (c) CTACS

10.8 Content Caching

Consider this scenario: an update to macOS has become available and needs to be applied to all the Macs in the organization. Suppose that the update is 4GB in size and there are 50 Macs – that is 200GB of data that needs to be downloaded. That is time consuming, impacts the bandwidth available for other purposes, plus may have cost and other implications if the organization does not have an unlimited internet bandwidth plan. It is also very wasteful as the same thing is being downloaded 50 separate times.

Apple's answer to this is a simple but effective solution in the form of *Content Caching*. Here, the updates are downloaded just once, to the server. In turn, Mac, iOS and tvOS clients connect to the server and pick up the updates from there, which is a far more efficient way of doing things. If you are familiar with the way things are done in a Microsoft server environment, there are some analogies to Windows Software Update Services (WSUS). It is not necessary to perform any configuration on the clients: if they can 'see' a content caching server on the local network, they will use it.

To enable content caching on the server, go into **System Preferences > Sharing**. Tick **Content Caching** on the left-hand side of the screen. It will take a few seconds to start up, plus the computers on the network will need to be restarted at some point to make use of it.

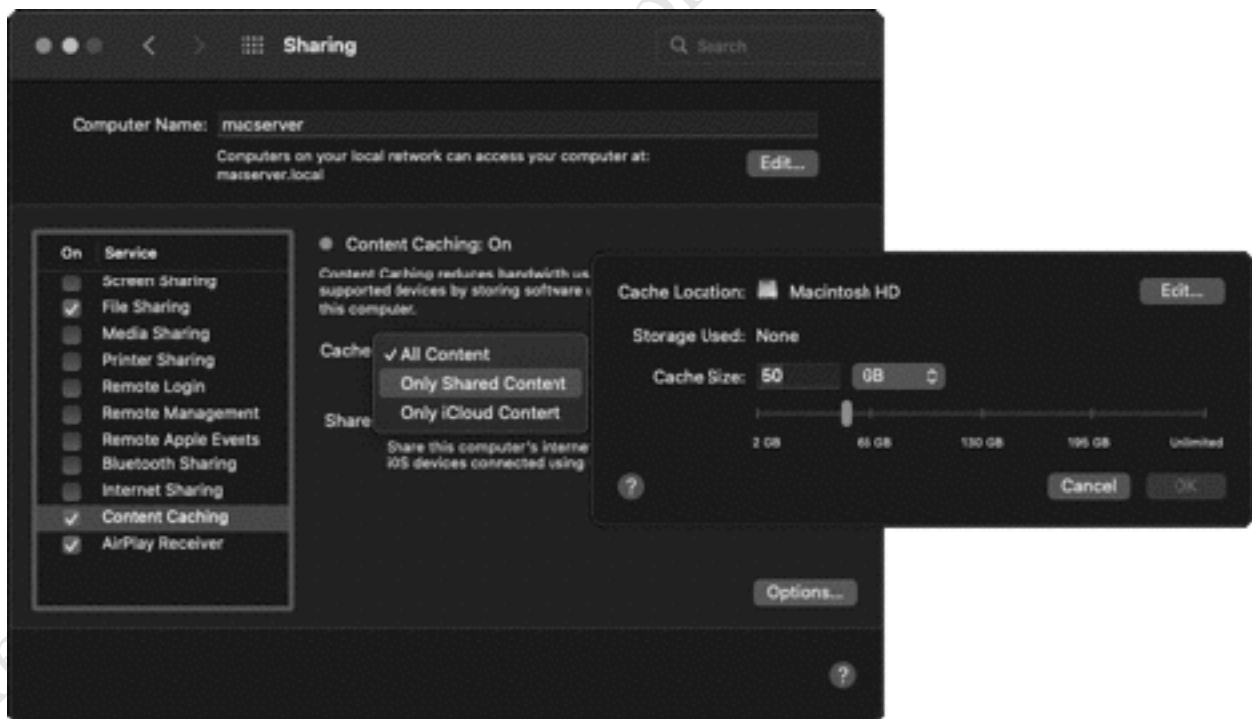


Figure 117: Configure Content Caching

There is a choice of what is cached; for software updates, it is suggested that you restrict it to **Only Shared Content**. Upon selecting it, you may receive a message advising that doing so will ‘delete all iCloud from the cache immediately’ – click **Delete** to continue.

You may also wish to specify the location of the cache and the maximum size it can grow to; you do not want it set at unlimited, otherwise it will grow to fill the available disc space. To change these settings, click **Options** and then **Edit** on the resultant panel.

Note that having enabled Content Caching, it may take some time before it is fully ready, as updates may first to be downloaded by the server.

10.9 Printing

One potential advantage of networking is that it allows printers to be shared, thus potentially saving money as well as physical space. An old-fashioned method of sharing a printer is to plug it directly into the server with a USB cable and configure it using sharing features built-in to the Mac operating system; to do this, make sure the printer is online and go into **System Preferences > Sharing > Printer Sharing**. However, it can be difficult to get this working and diagnose it when it does not, such that it is not even worth bothering with in the first instance. Fortunately, most modern printers have built-in Ethernet and/or wireless connections, giving them an existence on the network totally independent of any server or the computers and this is by far the best approach to shared printing.

Appendix

The Serverless Server

Free edition. Do not copy or distribute. (c) CTACS

A1: Overview

In a book written specifically about macOS Server, the topic might seem paradoxical, but it is possible to create a fully functional server *without* using Apple's Server App at all; you can think of this as a 'serverless server'. The explanation for this is contained within section [1.2 Mac Operating System and Server Versions](#); in recent years, Apple has moved most of the functionality that was originally in Server into regular macOS itself. Consequently, if you require only the ability to share and backup data, which is commonly the case in home and small business networks, but do not require the capability to manage devices as outlined in Chapter [8 Profile Manager](#), then you do not need to install and use the official Server App at all. You might wish to go down this route for the following reasons:

- Server app has few advantages over standard macOS in very small networks
- You do not wish to systematically manage and control devices
- It avoids another layer of software that must be learned and managed
- Everything can be done using the standard, familiar macOS interface
- You want to see if regular macOS is sufficient for your needs before committing to Server
- It saves a small amount of money, albeit the Server App is not expensive to purchase

The good news is that much of this guide is still totally applicable when creating a 'serverless server', with the key differences as follows:

Chapter 2 – Installation of macOS Server Software – is not applicable. The instructions for configuring regular macOS are provided below.

Chapter 3 – Users are created and managed differently. Instructions for working with standard macOS are provided below.

Chapter 5 – Mac clients are connected in a different manner, meaning that section 5.2 is not applicable. Revised instructions can be found below.

Chapter 7 – Housekeeping, Maintenance and Security. Most of this chapter does not apply.

Chapter 8 – Profile Manager is not applicable at all and hence this chapter is not relevant.

Chapter 10 – Miscellaneous Topics. Item 10.2 (Screen Sharing) is different and described below in section A5 Screen Sharing. Item 10.3 is not applicable.

A2: Installation and Configuration of macOS

This section describes how to install the macOS Server software and how to configure and customize a Mac, such that it is optimized for use as a server.

The Mac that is being used for the server role should be 'clean'. You could start with a brand-new computer, otherwise reset an existing Mac and install a fresh copy of macOS, which can be done as follows:

- Connect the Mac to the Internet using a wired Ethernet connection
- Turn on the Mac
- When you hear the startup sound, hold down the **Command (⌘)** and **R** keys on the keyboard, releasing them once the Apple logo appears
- After a short while, the Utilities menu will appear. Choose **Reinstall macOS**
- Work through the prompts about selecting a destination disk and installing the OS

When the OS has installed and you are running through the setup process, you want as little customization and personalization as possible. For instance, you do not want to specify an iCloud account, turn on location information, register with Apple or any of the other things that it encourages you to do, as these are of little relevance on a server machine.

Make sure that everything is fully updated by going into **System Preferences**. Updated versions of applications are not necessarily important, but you need to make sure that any macOS updates are applied as these often address security issues, may add or improve functionality, or may be pre-requisite for macOS Server. It is possible that the current version of macOS may not have been installed and it may be necessary to upgrade to a later version, so this entire process can be time consuming.

Note: all Apple Silicon-based Macs and late model Intel Macs feature the Apple T2 Security Chip. If you have such a Mac running macOS Monterey or later, it is possible to restore it to factory settings without having to reinstall the operating system from scratch. Launch **System Preferences** and from the menu bar click **Erase All Content and Settings**. It will then be necessary to enter the administrator details, after which you can optionally backup the machine. It is then necessary to enter your Apple ID details before finally erasing it. If further information is required, refer to <https://support.apple.com/en-gb/HT212749>

Naming the Server

Every computer in a network needs a unique name. Whilst the choice of name does not affect the operation of the server, it is preferable that it is something memorable and meaningful. For instance, you could give it the name of your household or organization or simply call it ‘*server*’ or ‘*macserver*’, as that is what it is and would avoid any confusion (all subsequent examples in this appendix assume it is called *server*).

Go into **Apple > System Preferences > Sharing**. Click the **Edit** button and change the name. Note that it needs to end with a suffix of *.local*, e.g. *server.local*. Click **OK**. Then, in the *Computer Name* box, give it the same name but without the suffix.

Having changed the name, it is a good idea to restart the Mac at this point.

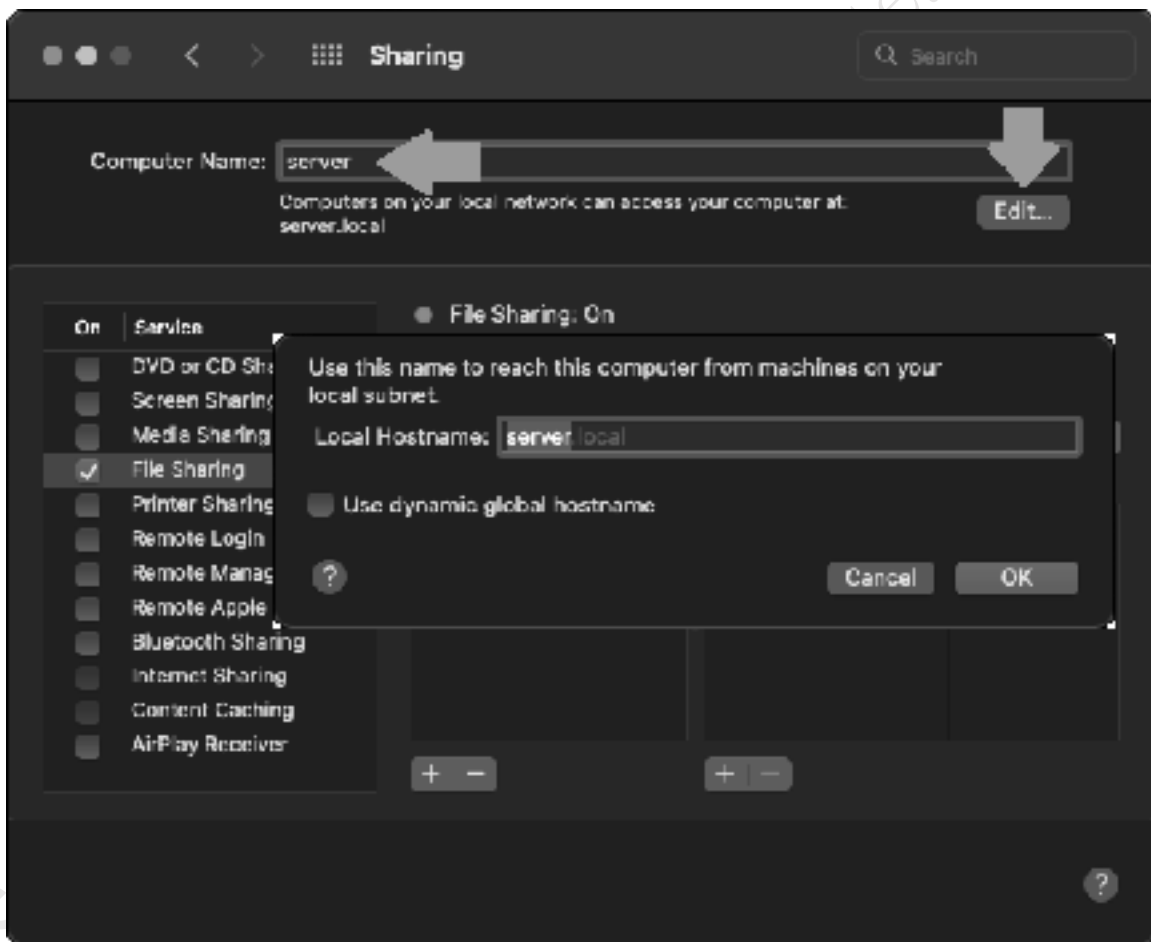


Figure 118: Changing the Computer's name

Setting the IP Address

The next thing to do is set the IP address of the server. The next five paragraphs are explanatory – if you understand the topic you can skip them and jump to the paragraph that starts ‘It is a good idea to have an IP addressing scheme to follow’.

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*, where *nnn* is a number from 0 to 255. Nearly all 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 is 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 the brand. Although these addresses can be changed, there is rarely any need and it is best not to do so unless one has an appreciation of the implications.

Devices such as computers and printers do not come with IP addresses already allocated; instead, they must 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 configure it. For instance, you might set the first Mac to *192.168.1.101*, the second to *192.168.1.102*, the third to *192.168.1.103* and so on. You must 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 is 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 computer, rather it is a piece of software and most all-in-one routers of the sort used in small businesses and homes have DHCP server software built-in.

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 assign such devices with static addresses but have the general-purpose computing devices – the computers, laptops, tablets and smartphones – using dynamic addresses.

It is a good idea to have an IP addressing 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 the computers, tablets and smartphones should be a contiguous block of numbers elsewhere, allocated dynamically by the router or other DHCP source. So, for instance, a typical setup might be as follows:

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

One implication of the above is that the network has a maximum of 255 devices in it, although this is unlikely to be an issue in a home or small business network. In larger networks, *subnets* are used to expand the size of the network, but we will assume there is only one subnet in use and it is commonly set to or defaults to 255.255.255.0 in a small network.

At present the server Mac is probably operating on an IP address received from the router's DHCP server; however, as mentioned above servers work better with fixed or static IP addresses, so we need to change matters. Go into **Apple > System Preferences > Network**. To the right of the Network Address – current reading 192.168.1.38 on our system in the above screenshot – is a drop-down called **Configure IPv4**. Click it and change it from *Using DHCP* to *Manually*. Change the IP Address to something that is outside of the DHCP scope of the router; if you do not know what the DHCP scope is, it is usually safe to choose an address next to the router or at the opposite end. In this example, the Router is 192.168.1.1, so a suitable address might be something such as 192.168.1.253. The Subnet mask should be set to 255.255.255.0 and the DNS Server set to the same address as the Router (it may default to it automatically). Click **Apply**.

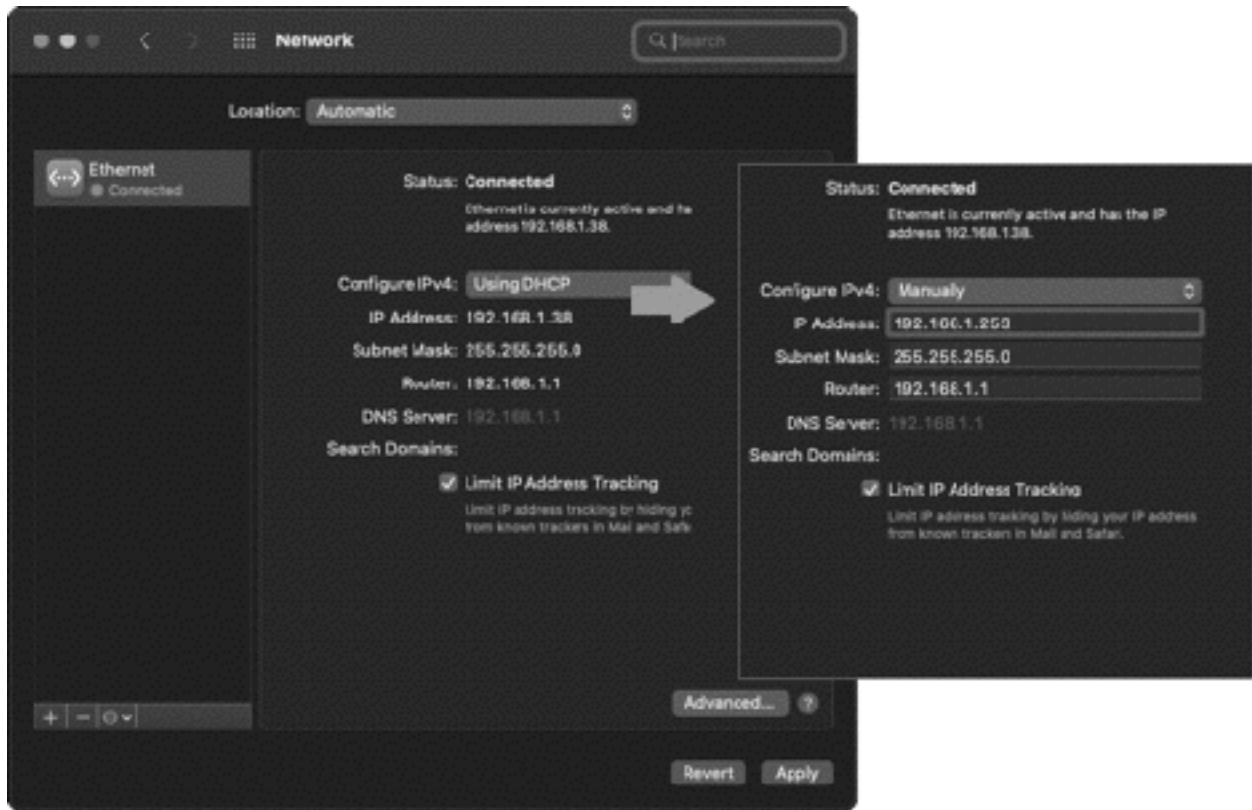


Figure 119: IP address details (before and after)

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 numeric addresses such as 192.168.1.254 rather than something like, say, 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

A3: Creating and Managing Users

Overview of User Accounts

To access the Mac server from another computer, it is necessary to enter the details of an account name that exists on the server, along with a password. The use of account names and passwords provides the most basic degree of security and management in a networked computer system.

You should decide upon a naming convention and this is one area where a different approach can be taken depending on whether it is a home or business network. In the case of a home network the user names can be anything you want, although there is some merit in following a scheme. For instance, you could use the first names of the family or household members. In a business environment a more formal approach may be more appropriate. As a general point, the greater consistency there is then the better. For user names, two common conventions are to use the first name plus the initial of the surname, or the initial of the first name plus the surname, although in some parts of the world other conventions might be more appropriate. In the case of particularly long names and double-barreled names, it might be an idea to abbreviate them. For example:

Name of Person	User Name	or	User Name
Nick Rushton	nickr		nrushton
Mary O'Hara	maryoh		mohara
Ian Smith	ians		ismith
Amber Williams	amberw		awilliams
Daniela Petrova	danielap		dpetrova

Creating a User

To create a new user, go onto the server and click **Apple > System Preferences > Users & Groups**. To add a new user, click the plus sign (+) in the bottom left-hand corner of the screen (it will be necessary to unlock the padlock using administrative rights to do so).

There are several different types of user accounts, selectable using the **New Account** dropdown. You need to choose the **Sharing Only** option – this is a special user account designed specifically for network use. Such users can access files and folders on the server but cannot login to it and use it as a local computer. Specify the user's name and give them an account name in accordance with your user naming convention as discussed above. Specify and verify a password for the new user; the best passwords are non-obvious and comprise a mixture of upper- and lower-case letters, numbers and symbols. If desired, the system can generate a password automatically: click the key icon to the right of the Password field to invoke the *Password Assistant*. The Password Assistant allows considerable flexibility over the type and length of the password and provides a visual clue over its quality or strength. Whilst passwords should generally be as strong as possible, common-sense should also be exercised. For instance, in a household network where there are young children then passwords will probably have to be quite simple. It is possible to create users without passwords, but this is not advised.



Figure 120: Creating a new user

Having specified all the details, click the **Create User** button. The newly created user will then be listed in the left-hand side of the main panel.

The process should be repeated until all the users have been created. If you have many users to create, you may find it helpful to first create a checklist of their names and to make a note of the passwords.

Tip: When the server Mac is at the login screen, only the *admin* user should be available. If other users are listed, it means you have created them as *Standard* rather than *Sharing Only* accounts. Unfortunately, it is not possible to change the account type, so you will need to delete the incorrect users and recreate them. Choosing the wrong account type is the most common error when creating new errors as macOS defaults to a *Standard* rather than *Sharing Only* user, meaning it always has to be changed.

Free edition. Do not copy or distribute. (c) CIPRO

Modifying a User

To subsequently modify a user, go to **Apple > System Preferences > Users & Groups**. Highlight the user name in the left-hand column then click their icon in the main section (the word 'edit' will appear as you do so):

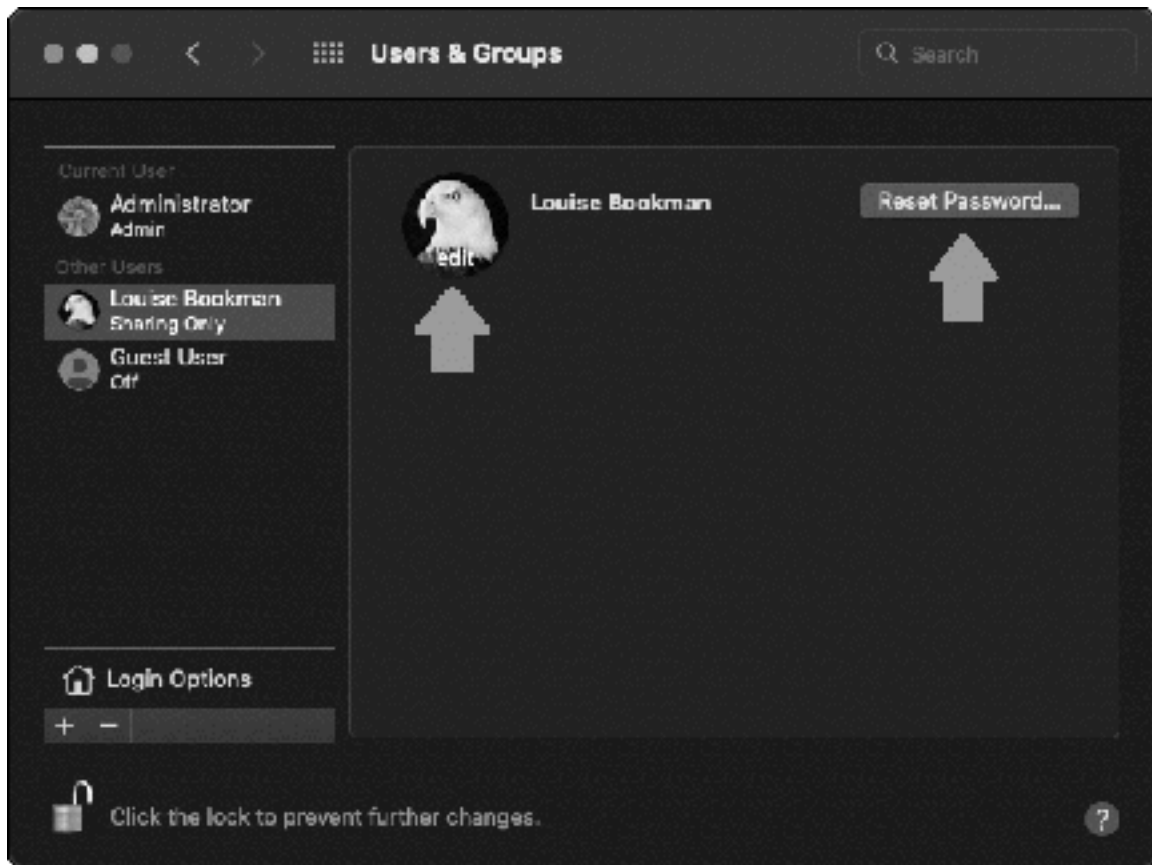


Figure 121: Modify an existing user

To change the user's password, click **Reset Password**. This brings up a dialog box into the which the new password is entered and verified. Alternatively, click the key icon to have the system automatically generate a password as described previously.

To change the user's picture, click the existing one. There is a choice of alternative built-in ones plus emojis, or you can select an existing image or take a new photograph if the Mac is equipped with a camera.

Deleting a User

To delete a user, go to **Apple > System Preferences > Users & Groups** and highlight the user name in the left-hand column. Click the minus sign (-) in the bottom left-hand corner of the screen (it will probably be necessary to unlock the padlock using administrative rights to do so). There will be a warning message: click **OK** to permanently delete the user. Note that this action cannot be subsequently undone.

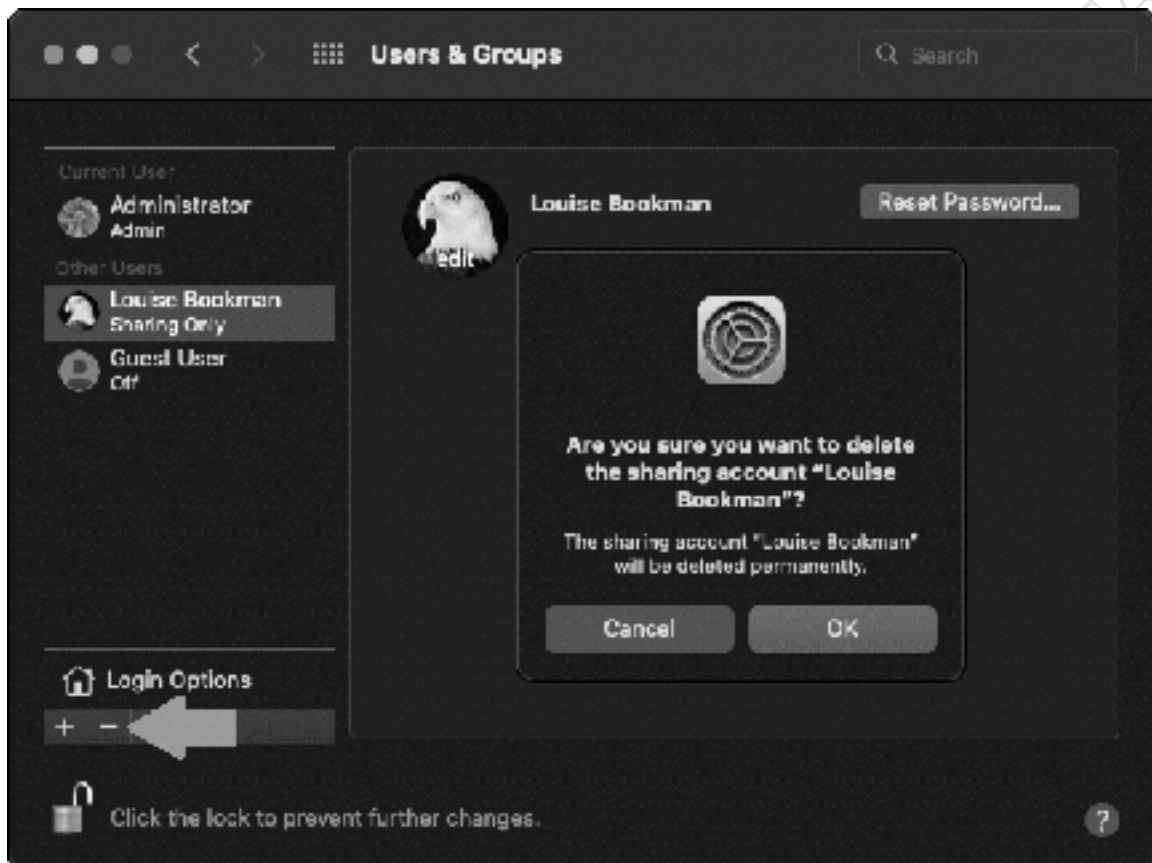


Figure 122: Deleting a user

Groups

In an organization with a small number of users, specifying who has rights to shared folders is relatively easy to manage. But as the number of users increases it clearly becomes more time consuming: for example, consider having to define the access rights for, say, twenty 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, some in marketing and so on. Or, in an educational establishment, students would commonly be organized into classes.

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

To create a group, go into **Apple > System Preferences > Users & Groups** and click the plus sign (+) in the bottom left-hand corner of the screen (it will probably be necessary to unlock the padlock using administrative rights to do so). From the **New Account** dropdown, choose *Group* and on the panel that appears enter a name for the group (referred to as 'Full Name' in macOS, despite there being no facility for abbreviated names). Click **Create Group**:

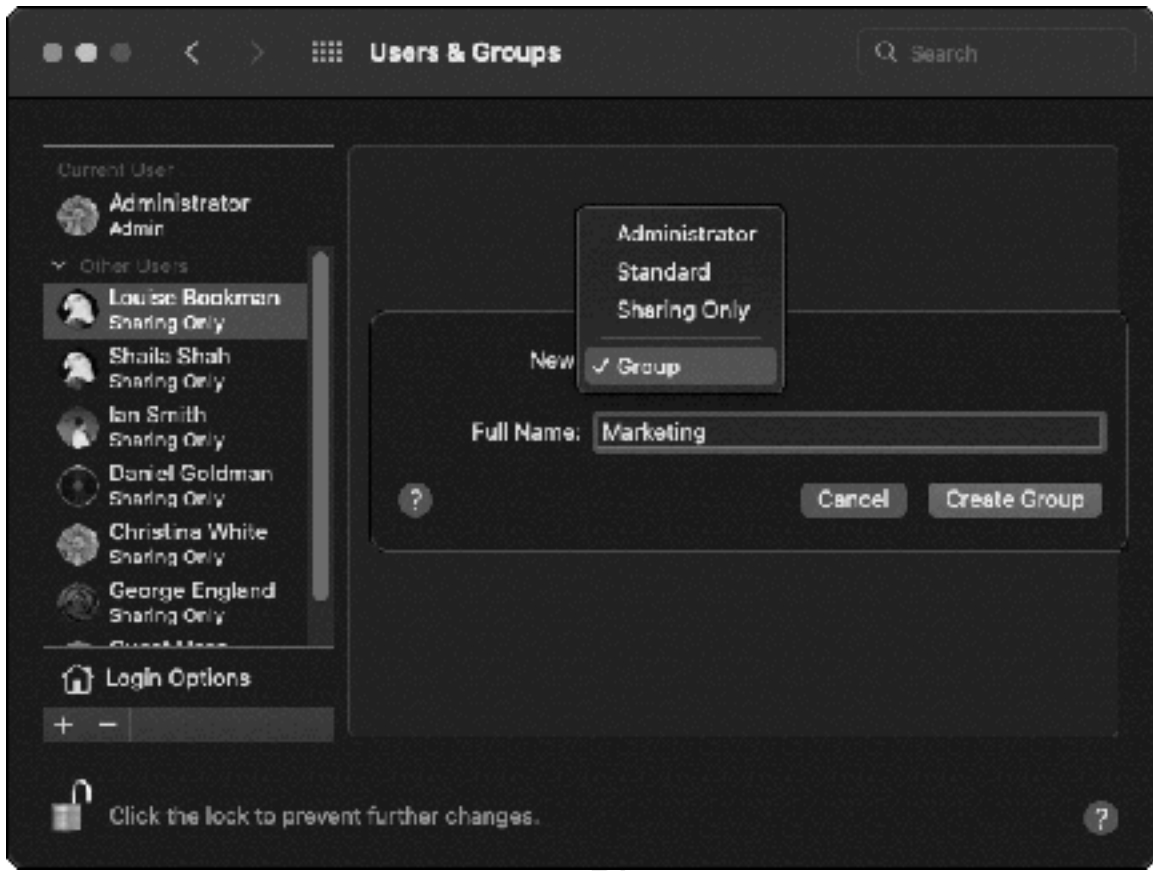


Figure 123: Creating a new Group

Having created the group, you will be returned to the previous screen, where it will now be listed in the left-hand side of the screen. The next step is to add the users who will be members of it, which is done by placing ticks against the names of the users:

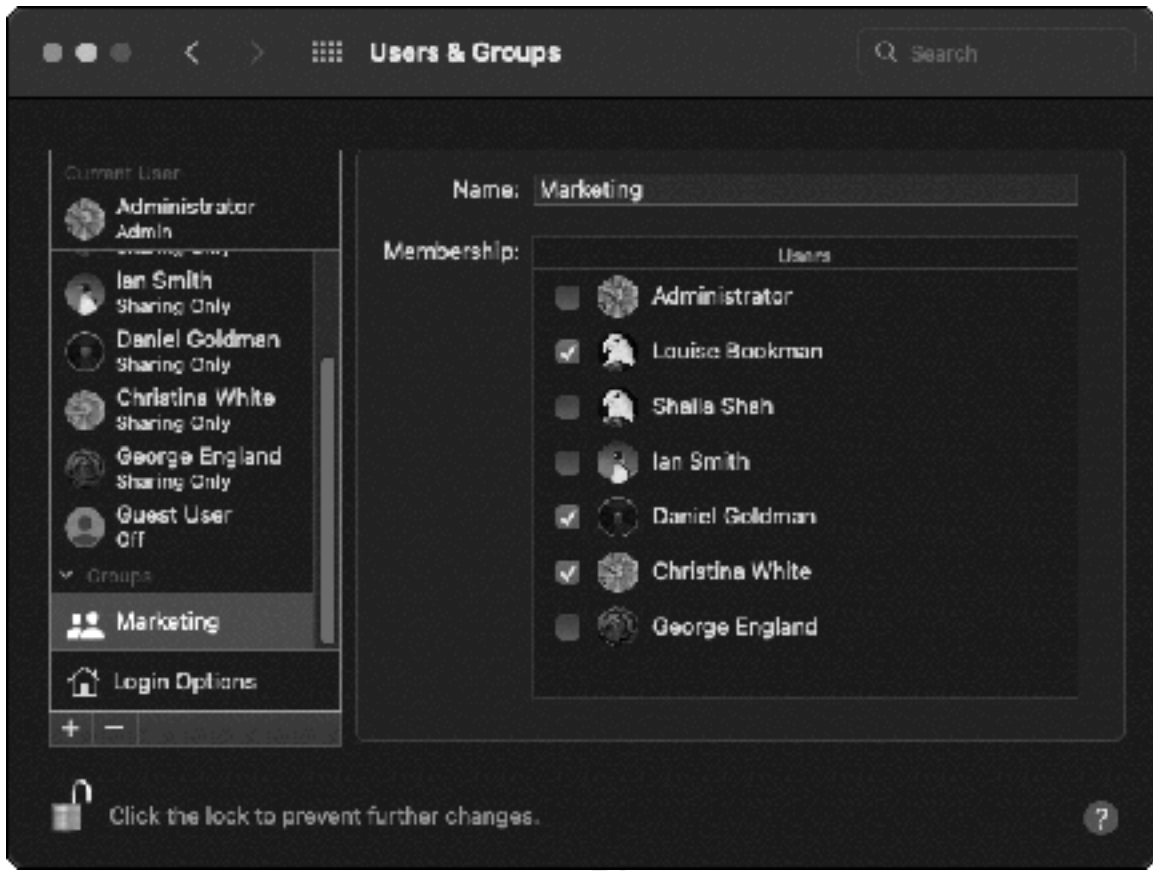


Figure 124: Adding users to a Group

To add or remove users at a later stage, go into **Users & Groups**, highlight the group and place or remove ticks against user names as required.

A4: Connecting Macs to the Serverless Server

As might be expected, connecting another Mac to the server is easy and straightforward. The first requirement is to make sure that each Mac has a unique computer name. In a small setup, this could be as simple as something like *Mike's Mac*, *Sue's Mac*, *Daniela's Mac* and so on. In a larger setup, a more structured approach is better, perhaps based on location or function or some other classification that is meaningful to the organization e.g. *Class1-01*, *Class1-02*, *Class1-03* or *Design01*, *Design02*, *Design03*. So, when setting up the computers, decide upon and adhere to a suitable naming convention. To check, and if necessary change, the name of a Mac and its *local hostname*:

Go into **System Preferences** > **Sharing**. Change the name of the *Computer Name*. Then, click the **Edit** button and on the resultant panel check the *Local Hostname*, which should be the same but with a suffix of *.local*. Click **OK**. Whilst not strictly necessary, it is a good idea to restart the Mac at this point.

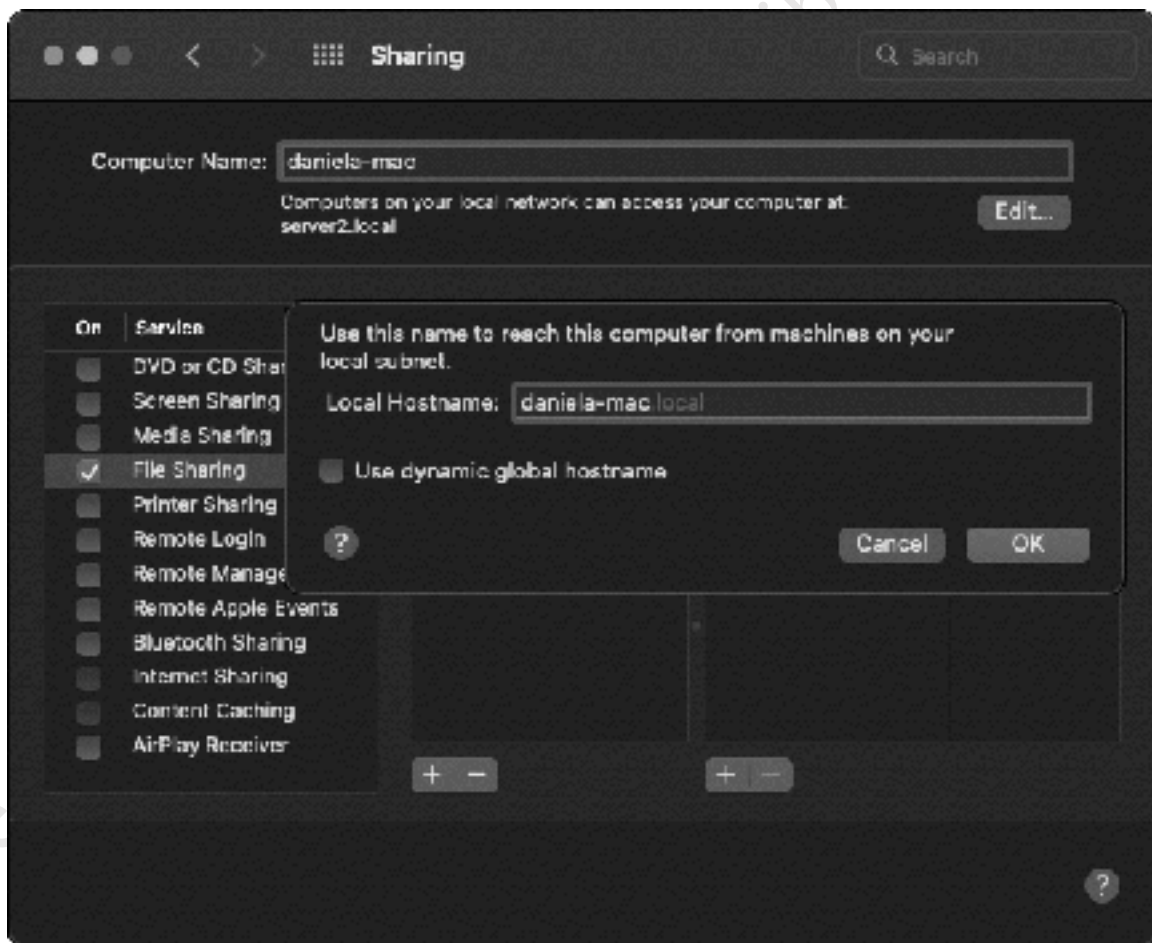


Figure 125: Changing the local hostname of a Mac

On the menu bar of the Mac, click **Go** followed by **Connect to Server** (alternatively, press **⌘ K**). A dialog box is displayed. Enter the name of the server preceded with `smb://` e.g. `smb://server`. To add the server to your list of Favorites for future reference click the **+** button. Then click **Connect**. Enter a user name and password as previously defined on the server and click **Connect**. You can also tick the **Remember this password in my keychain** box if desired, although this should only be done if you are the sole user of the computer:

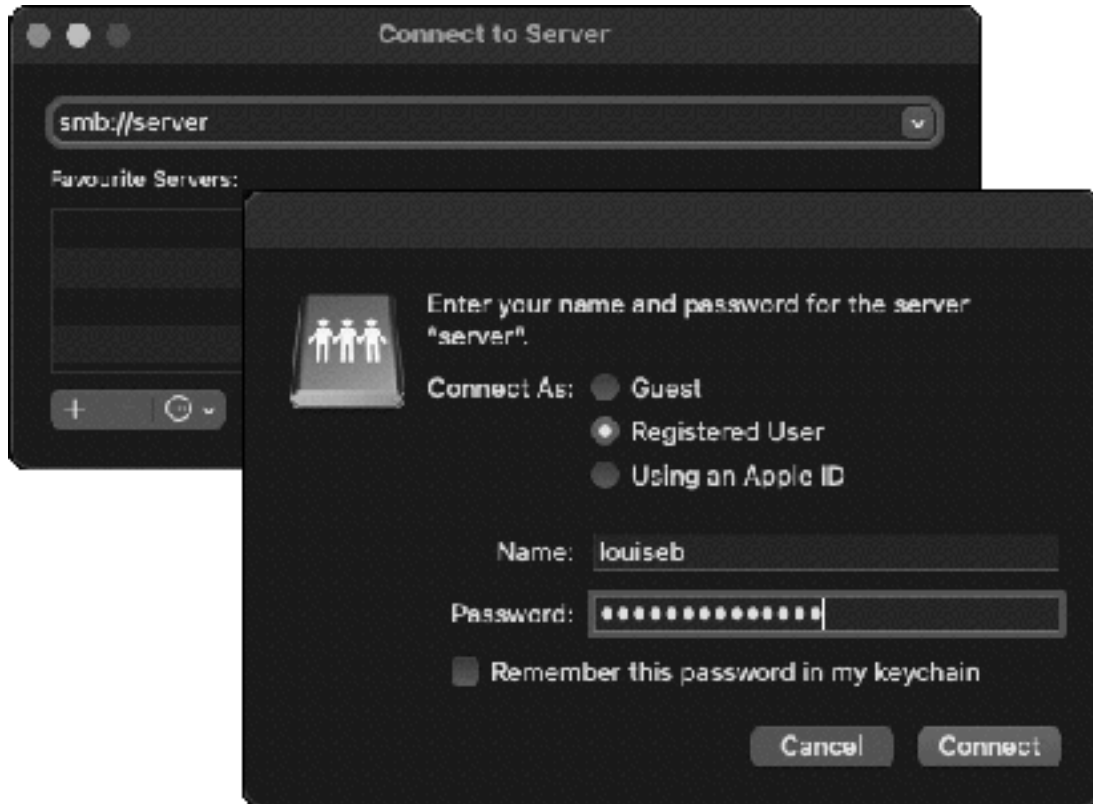


Figure 126: Specify server and user logon details

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

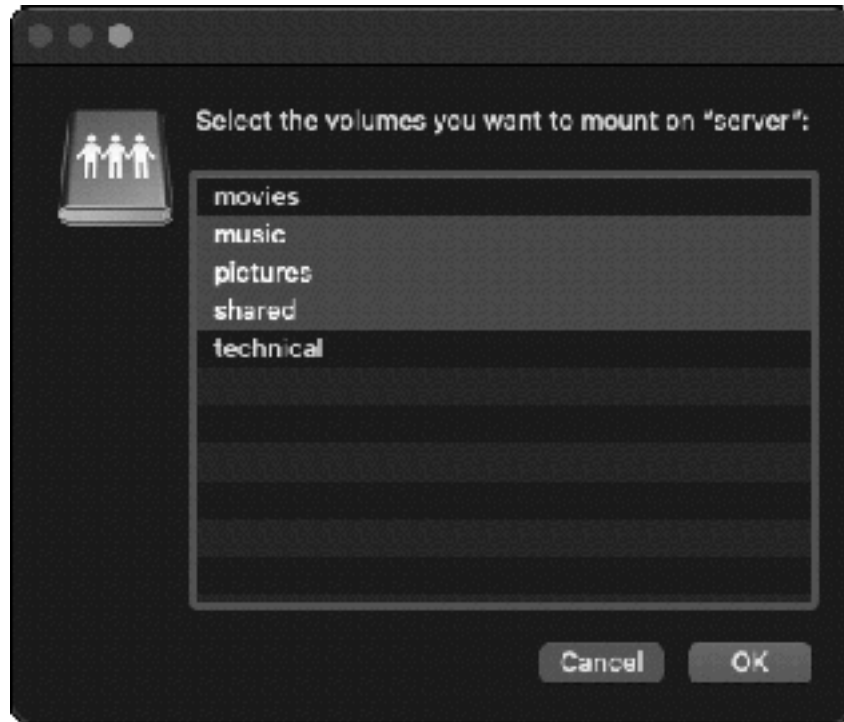


Figure 127: Select the volume(s) to mount

An icon for each volume will appear on the Desktop – click it to display the contents. They behave as any standard Mac folder, allowing files to be accessed, manipulated and so on.

To connect other types of clients, see sections [5.3 iPads and iPhones](#), [5.4 Windows Computers](#), [5.5 Linux Computers](#), and [5.6 Chromebooks](#)

A5: Screen Sharing

To run the server without a monitor, keyboard and mouse - sometimes described as *headless* mode - and to access it for support and other purposes, the *Screen Sharing* capability of macOS can be used. This has several advantages: firstly, the server can be managed using any Mac on the network and it is not necessary to have physical access to it, 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 a small amount of electrical power. Thirdly, in some small organizations the server may have to be physically located in a general-purpose office and not having a keyboard and screen will reduce the temptation for staff to treat it as just another computer. Plus, the ability to manage the server computer from the comfort of your own desk is clearly very convenient.

Begin by enabling the feature on the server Mac. Go into **System Preferences > Sharing** and place a tick against **Screen Sharing**:

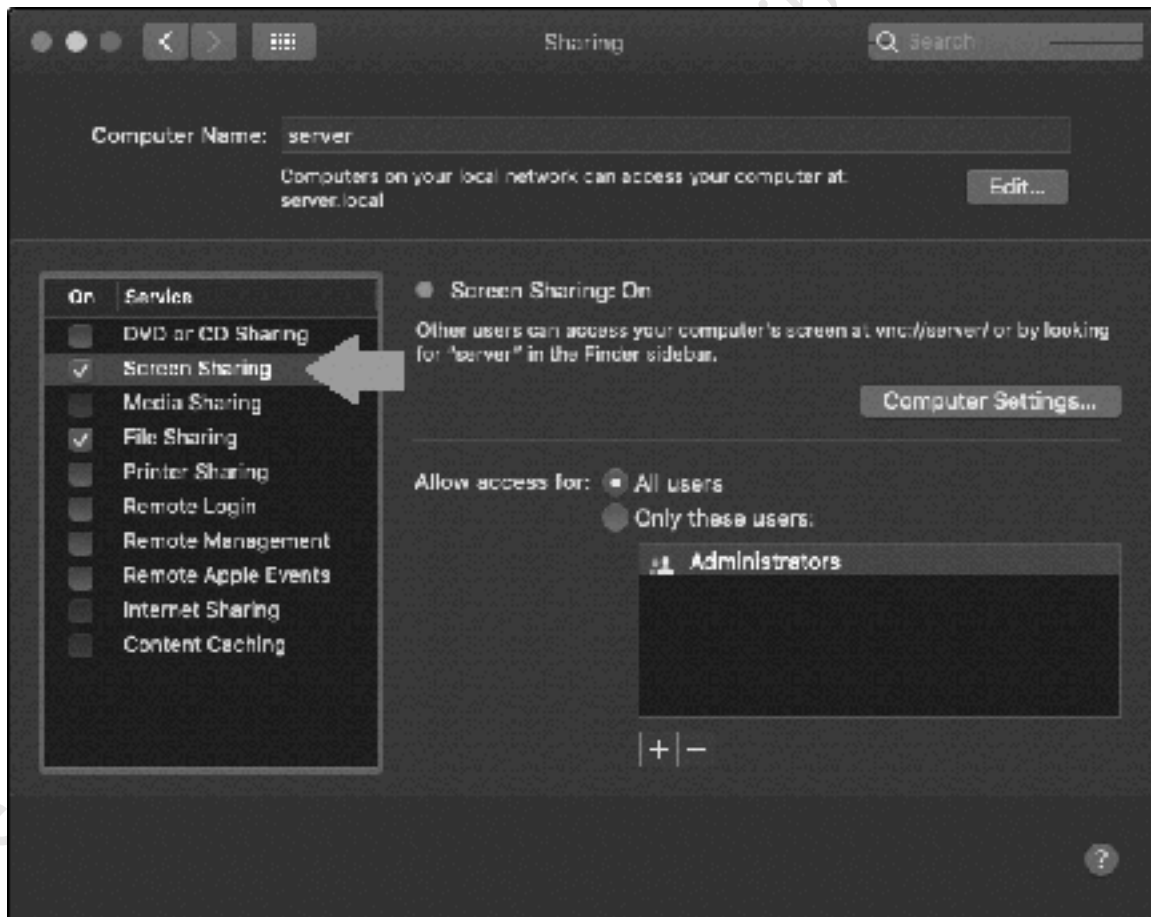


Figure 128: Enabling Screen Sharing

If the requirement is for anyone to access and manage the server, then that is all that needs to be done. However, there are several options that may be of interest:

To restrict access to a particular group of users, for example Administrators, click **Allow access for: Only these users:** and use the plus (+) and minus (-) buttons to add or remove users.

To allow anyone to request access plus optionally specify a password, click the **Computer Settings** button.

Having enabled Screen Sharing, there are two methods for using it from another Mac:

Using A Browser e.g. Safari

Launch the browser and type `vnc://server/` in the address bar, where 'server' is the name of your server Mac (alternatively you could enter its IP address). A message is displayed, asking if you want to open Screen Sharing – click **Allow**. On the next pop-up, click **Connect** and enter your login credentials.

Note: you do not have to use Safari as other browsers e.g. Firefox, also work.

Using Finder

Open a Finder window, look for the server in the sidebar and double-click it. Click the **Share Screen** button and enter your login credentials when prompted. For convenience, you could choose to optionally tick the **Remember password** box.

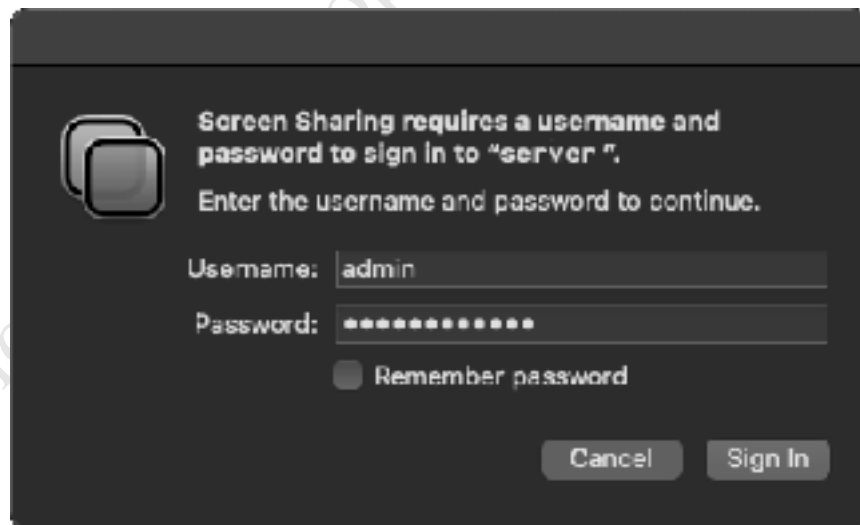


Figure 129: Enter credentials for the server

Having logged in, you will be presented with the main screen of the server but contained within its own window. To all intents and purposes, it is as though you were sitting in front of it.