

The Little Book of TerraMaster NAS

Nicholas Rushton, BA Hons.

Callisto Technology And Consultancy Services

TOS 4.2 Version © 2021

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

TOS 4.2 Version. Updated June 2021

Copyright © Nicholas Rushton 2021

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 unauthorised 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 500 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 TerraMaster Technology Company Limited 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.

Contents

1	GETTING STARTED.....	7
1.1	Overview.....	8
1.2	Choosing a TerraMaster NAS.....	11
1.3	Disk Drives.....	13
1.4	Switch and Wireless Access Points.....	15
1.5	Location and Electrical Considerations.....	15
2	INSTALLATION OF TOS.....	16
2.1	Overview.....	17
2.2	Initial Installation.....	17
2.3	Five Minute Tour of TOS.....	25
2.4	Configure Networking.....	31
2.5	Power Management.....	33
2.6	File Service.....	36
2.7	Setup Remote Access.....	39
3	SHARED FOLDERS.....	41
3.1	Overview.....	42
3.2	Creating Shared Folders.....	42
3.3	Changing or Deleting a Shared Folder.....	46
3.4	Home Folders.....	46
3.5	Loading Existing Data into Shared Folders.....	47
4	USERS.....	48
4.1	Overview.....	49
4.2	Creating Users.....	50
4.3	Modifying, Disabling and Deleting Users.....	54
4.4	Importing a List of Users.....	55
4.5	User Groups.....	56
5	ACCESSING THE SERVER.....	59
5.1	Overview.....	60
5.2	Using a Browser and File Manager.....	60
5.3	Connecting Windows Computers.....	62
5.4	Connecting Macs.....	71
5.5	Connecting Linux Computers.....	73
5.6	Connecting Smartphones and Tablets.....	74
5.7	Connecting Chromebooks.....	78
6	SECURITY.....	80
6.1	Overview.....	81
6.2	Clam Antivirus.....	81

6.3	SSL Certificate.....	83
6.4	Firewall.....	84
6.5	Account Safety.....	86
6.6	DoS Protection.....	87
6.7	Disable Unused Connectivity Services.....	88
6.8	Password Settings.....	89
6.9	Disable the Guest Account.....	91
7	BACKUPS.....	92
7.1	Overview.....	93
7.2	Backing Up to An External Drive.....	93
7.3	Restoring Files from a Backup.....	99
7.4	Backing up to Cloud Services using Duple Backup.....	101
7.5	NAS to NAS Backups Using Rsync.....	105
7.6	Backing up the System Configuration.....	110
7.7	Backing up Windows Computers.....	111
7.8	Backing Up Macs.....	120
8	HOUSEKEEPING & MAINTENANCE.....	122
8.1	Overview.....	123
8.2	Hardware Information.....	123
8.3	Service Status.....	124
8.4	Resource Monitor.....	125
8.5	System Log.....	127
8.6	Checking Disk Health.....	128
8.7	Checking for TOS Updates.....	130
8.8	Notifications.....	132
9	MULTIMEDIA & STREAMING.....	134
9.1	Overview.....	135
9.2	DLNA Media Server.....	135
9.3	iTunes Server.....	138
9.4	Plex and Emby Server.....	140
10	STORAGE.....	141
10.1	Overview.....	142
10.2	RAID.....	142
10.3	Modifying a Storage Pool/Changing a Drive.....	146
10.4	Snapshots.....	149
10.5	iSCSI.....	152
10.6	SSD Caching.....	157
10.7	SSD TRIM.....	160

11 MISCELLANEOUS & ADVANCED TOPICS.....	161
11.1 Overview.....	162
11.2 Applications.....	162
11.3 Date and Time Settings.....	165
11.4 Renaming the Server.....	166
11.5 User Settings.....	167
11.6 Printing.....	170
11.7 Text Editor.....	171
11.8 PDF Reader.....	172
11.9 Docker.....	173
11.10 Dynamic DNS (DDNS).....	177
11.11 VPN (Virtual Private Network).....	179
11.12 Connecting Via a Proxy Server.....	189
11.13 Alternative Operating Systems.....	190
11.14 Unable to Login as Admin User.....	190
11.15 Contacting TerraMaster for Support.....	191
11.16 Preparing a TNAS for Disposal.....	192

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

INTRODUCTION

“Once I had bought the TerraMaster, this book started to come into its own. The manufacturer supplies a PDF with the “Fundamentals and Preliminaries” of setup but this book explained much more, guiding us through the hows and whys of setting up the NAS, explaining options and providing guidance through the maze. Within a few days I was mapping drive letters on to my new hardware and finally, I could address the NAS from my own software, as if the data was sitting on a local drive. I am sure that all these things can be completed using a combination of other sources: the manufacturer’s documentation, online tips and videos, but having the process wrapped up in a single book has been great. One worry I had was that this book would deal with processes for a TerraMaster NAS that was different to mine. This has not been the case. Its advice has consistently guided me through the tricky setup process. My advice to everyone new to this field would be: If you buy a TerraMaster, then buy this book.” – Mr Zambei

With its combination of capable, well-designed and cost-effective hardware, matched with the elegant, streamlined TOS software with its modern interface and rich functionality, TerraMaster have risen rapidly to become of the main players in network attached storage for home and small business users. But this power and flexibility comes at a price and setting up a TerraMaster NAS for the very first time can seem a daunting prospect for someone who has not done so before. This guide is based around the latest version of TOS and with copious illustrations, easy-to-follow instructions and based on years of real-world experience, will take you through it from start to finish and help ensure that your home or small business (or church, charity, school) network is a success. It is written according to the Goldilocks Principle: not too little information, not too much information, but just the right amount.

The guide is structured as follows:

Chapters 1 to 5 cover the essentials, the things you absolutely must do, which consists of setting up the hardware, installing TOS, creating some shared folders, creating the users and then connecting your computers and mobile devices to the NAS.

Chapters 6 to 8 comprise things which are strongly recommended: setting up security; setting up backups for the server and the connected computers; learning about housekeeping and maintenance to keep the server in good health.

Chapters 9 through 11 are other topics to investigate and includes ways to make your system more capable and useful, such as multimedia and more sophisticated ways of managing storage.

In a hurry? The first five chapters will get you up and running ASAP. Then return and explore at leisure.

About the Author

The author has worked in IT for over 35 years, on systems of all sizes and types throughout the world, from the largest companies to the smallest and including several of his own. He currently runs his own independent consultancy and is the author of numerous networking guides, published through CTACS as eBooks and paperbacks. Titles include: *Little Book of TerraMaster NAS*; *QNAS Setup Guide*; *Windows Server 2019*; *Windows Server 2016*; *Windows Server 2019 Essentials*; *Windows Server 2016 Essentials*; *Little Book of macOS Server*; *Synology Setup Guide*; *Little Book of Synology*; *Using Windows 10 as a Server*; *ASUSTor NAS Setup Guide*.

Problems with the Artwork?

Pictures and illustrations can sometimes be problematic with eBooks. If you would like a free printable PDF version of the guide, just forward a copy of the email confirmation you received when you bought the book to ctacs@outlook.com. Please make sure there is no personal financial information in your email. We aim to respond within 24 hours.

1

GETTING STARTED



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

1.1 Overview

If you are reading this, then chances are you already know what Network Attached Storage (NAS) is and may have purchased or are about to purchase a TerraMaster NAS unit. But for those who do not, or by way of recap:

When two or more computing devices are connected together, a network is created. The Internet is a worldwide, public network comprising billions of users, computers and servers.

A private, or local area network, is typically intended for the use of a household, business or educational establishment. Such networks are commonly built around a NAS unit.

The keyword here is ‘storage’. A NAS device consists of a large amount of disk storage contained in its own box. Unlike most external drives, which typically connect to a single computer with a USB or Thunderbolt connection, a NAS links to a router or network switch using an Ethernet cable and this enables it to be accessed and shared by computers and other devices on the local network.

The NAS can also be accessed remotely from anywhere via the Internet. It is protected by user accounts, passwords, encryption and other security measures so that only authorized people can access it, not the public at large.

A NAS device runs its own operating system. This is not Windows or macOS, rather, it is a proprietary system and in the case of TerraMaster it is called TOS (TerraMaster Operating System). Usually, the term firmware rather than operating system is used to describe it. Although specifically designed for NAS duties, TOS also has the ability to run apps that provide additional capabilities.

A NAS does not need its own screen, keyboard and mouse. Rather, it is interacted with using a browser (such as Chrome, Firefox, Safari etc) from any computer on the network. At the simplest level it can simply be thought of as a ‘black box’ or computing appliance.

What can a NAS do? Some popular uses are:

- Providing extra storage for computers
- Providing a backup system for computers
- Providing a shared, common area where a business or family can store their documents and other files
- Being the heart of a home entertainment system, providing a central library for music, photos and videos, with the ability to stream them to computers, tablets and smartphones
- Acting as a private cloud system, providing controlled remote access to your data. Similar in principle to Dropbox or iCloud or OneDrive, but totally under your own control and with effectively unlimited usage and no subscription charges
- As an alternative to a traditional business file server running Windows Server or Linux

TerraMaster are one of the leading and most innovative suppliers of NAS and have many units. They offer a wide range of affordable hardware, suitable for individual users all the way through to large enterprises. TerraMaster’s approach is to keep everything streamlined and focused on the essentials, rather than weigh the system down with complexity and multiple ways of doing things. It can sometimes seem idiosyncratic, but this guide will help steer you through the potential ‘gotchas’.

Besides NAS, the terms *TNAS* (TerraMaster NAS) and *server* are used in this book; they all refer to the exact same thing and are used interchangeably.

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

NAS (server) - this is the heart of the network, which runs TOS and upon which the data is stored

Backup device – for example, an external USB drive connected to the server

Internet connection - this may be a separate router or an all-in-one wi-fi router

Switch and Wireless Access Point(s) – to provide expansion in larger networks

Printer(s) – may be wired or wireless

Desktops PCs – running Windows, macOS or Linux, connected using Ethernet or wireless

Laptops, tablets and smartphones – connected wirelessly

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

Just about any modern computer can be used with a TNAS. The computers can be running any mixture of Windows 10, Windows 8/8.1, Windows 7, Windows Vista or Windows XP. Home or Professional versions of Windows are equally suitable. Apple Macintosh computers running most versions of macOS can be connected, as can Linux PCs and Chromebooks. Devices running iOS (iPad, iPhone) or Android (tablets and Smartphones) can be connected, as can many smart televisions and gaming boxes.

Free edition. Do not copy or distribute. CRACS

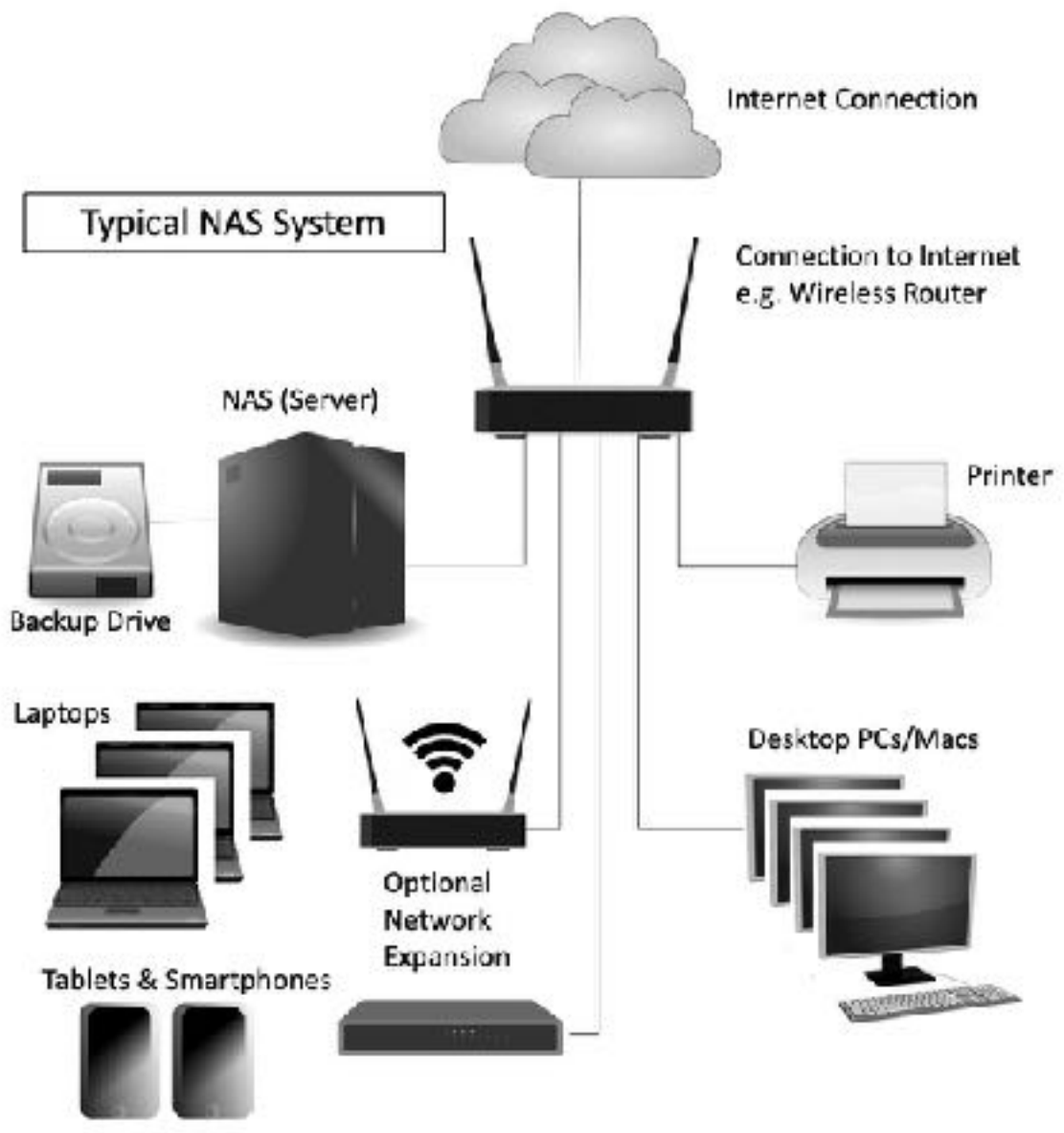


Figure 1: Typical NAS System

Free edition.

1.2 Choosing a TerraMaster NAS

TerraMaster offer more than 20 different models of their NAS hardware, designed to cater for everyone from single and home users, through to large businesses with hundreds of users and high availability requirements. The models vary according to form factor, number of hard drives that can be used, performance and price.

Form Factor – Most TNAS units are standalone and designed to sit on top of a cupboard or desk. Enterprise-class models are designed to be mounted in standard computer cabinets (racks) that take devices which are 19” (48cm) wide. Home and small business users will typically use the compact, desktop TNAS units, but some businesses may have a cabinet (perhaps to hold other equipment as well), in which case a rackmount version may be a better choice.

Number of Hard Drives – TerraMaster NAS units can hold between 2 and 24 hard drives, depending on the model. Having more drives allows more storage capacity and permits the use of RAID to improve both resilience and throughput.

Networking – all models feature at least Gigabit Ethernet and many models have multiple network adapters. Some models have 10 Gbe, for higher network throughput.

Performance - Some TNAS models have more powerful processors and more memory (RAM). These are typically aimed at business users or home users with more demanding requirements. Some advanced features, mainly of interest to enterprise rather than home or small business users, require more powerful TNAS models. The majority of models use Intel processors, but some are ARM-based. ARM processors are highly optimized for multimedia usage, so can be a good choice for video streaming and are equally capable in most other roles. Lower-cost TNAS models are ARM-based.

Choosing the right model can be confusing as there is considerable overlap between some of them, but in general you want to buy the most capable one you can afford. If you have or are planning to have large amounts of data, consider buying a model with more than two drive bays.

A used or second-hand TNAS might be an option for some people. There are relatively few parts that can go wrong on a NAS, most commonly it is the fan or power supply that might develop a fault and these are usually easy to replace. If the unit is supplied with disk drives already installed, confirm that they are healthy; for instance, the drives in a NAS that has been used 24x7 for a number of years may be becoming worn out and in need of replacement and you should budget accordingly.

Typical Usage Scenarios

These are some examples of how some people are using TerraMaster NAS and the equipment choices they made:

Individual – Sue has a Windows desktop PC as well as a MacBook. She wanted additional storage space and the ability to share files between them, along with the ability to backup her MacBook using Time Machine. Her choice was the very affordable 2-bay FS-210. The portable USB drive she previously used for backups has been redesignated for use with the TNAS.

Enthusiast – Andy had previously owned a very basic NAS device from another manufacturer but had outgrown it and wanted something more capable. As a semi-professional photographer, he was concerned about data safety and wanted a unit with multiple drives. As an IT enthusiast, he also wanted to be able to explore the additional capabilities offered with a modern NAS. His choice was a 2-bay F2-421.

Family – The Palmer family comprises two adults and two children. All have computers, plus tablets and smartphones. They are very keen on movies and music and want the ability to store their large collections in a single location, then stream to any device in the household. Their choice was the 4-bay FS-210. For backing up the most important family data, they have connected it with a Dropbox account.

Small Business – Helen Inc. wanted a capable in-house network, but without the costs and complexity associated with traditional Windows or Unix-based file servers. As they have several offsite and home-

based staff, they also wanted remote access, but without the ongoing costs associated with commercial cloud services. They also felt more comfortable with the idea of their data being under their direct control, rather than with a third party. Their solution was the 8-bay F8-421, which is backed up to a separate F5-221 located elsewhere in the premises.

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

1.3 Disk Drives

NAS units are not supplied by TerraMaster with disk drives already installed in them. Rather, the idea is that the customer buys the drives separately and installs them, which is easy to do and TerraMaster even provide a screwdriver for this purpose. This approach is generally better because it offers more choice.

Most disk drives can be used in a NAS unit. However, it is recommended to use the models listed on the TerraMaster website, especially the drives that have been specifically designed for use with NAS. These drives differ from regular desktop and laptop drives in that they are optimized for continuous 24x7 operation over several years and take into account the heat and vibration characteristics of NAS enclosures, along with other specific requirements. Although such drives are slightly more expensive than the regular disk drives as used by desktop PCs, the investment can be justified given the importance of data integrity. The main NAS-specific drives are as follows:

Western Digital Red – designed for use in NAS systems with 1 to 8 bays. For system with more drive bays, WD Red Pro drives are available.

Seagate IronWolf – intended for NAS systems with 1 to 8 bays. Iron Wolf Pro drives are available for systems with up to 24 drive bays.

Toshiba N300 – designed for use in NAS systems with 1 to 8 bays.

Disk drives are manufactured in 3.5” (8.9cm) and 2.5” (6.4cm) form factors and TNAS boxes can use either, without the need for the adaptor brackets required by some other NAS manufacturers. 3.5” drives offer higher capacities and better price performance, whereas 2.5” drives use less power, generate less vibration and are generally quieter in operation. For systems with more than one drive, it is preferable that all the drives are the same model and capacity, although this not a prerequisite. In a TNAS equipped with multiple drives, they can be configured for *RAID*, short for *Redundant Array of Independent (or Inexpensive) Disks*. There are various types of RAID, referred to using a numbering system i.e. RAID 1, RAID 5, RAID 6 etc. The basic idea is to improve reliability and performance through the use of multiple drives to provide redundancy and share the workload (a more comprehensive description can be found in section [10.2 RAID](#)).

Although the majority of today’s disk drives are mechanical, solid state drives based around flash memory, known as SSDs, are increasingly being used in laptop computers and elsewhere and will probably become the norm in all computing devices. Besides fast performance, SSDs have reduced power consumption and no mechanical noise, which makes them more suitable for some environments. NAS-specific SSDs are available from Seagate and Western Digital. At present, SSD’s are more expensive than their mechanical counterparts, especially for the high-capacity ones that would be of most use in NAS, although prices are expected to fall.

It is strongly advised that new, unused drives are used with the NAS. If previously used ones are utilized, they should be reformatted to remove any previous data and volumes; if this is not done, TOS may be unable to recognize them.



Figure 2: Hard drives being mounted inside a TerraMaster NAS

Free edition. Do not copy

1.4 Switch and Wireless Access Points

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

- The NAS should be connected to the main network switch or combined wireless router using an Ethernet cable.
- Use wired connections whenever possible as performance is better than with wireless. Wired devices should be of Gigabit (1Gb) specification or better. Some models support the higher speed 10 Gbe standard; if so, it is worthwhile connecting at least the NAS to a high-speed switch, even if much of the remaining infrastructure runs at a slower speed.
- 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, often free of charge when signing-up with them. These may be of average specification, 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.

1.5 Location and Electrical Considerations

TNAS boxes are fairly rugged, but as with any electrical apparatus some thought needs to be given to the location. They 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 otherwise out of reach. Most models generate very little noise and can usually be operated in an office or family room without too much disruption.

It is possible that data loss can occur if the mains electrical power fails unexpectedly whilst the TNAS is running. The best way to mitigate against this is to use a UPS (Uninterruptible Power Supply) with the TNAS; in the event of power problems this will enable it to continue operating for short periods. TerraMaster support a wide range of UPS from major vendors, including APC, Cyber Power Systems and Tripp Lite. In a business environment, the use of an UPS should be considered essential. If a UPS is not used, which is usually the case in a domestic environment, then the TNAS should at least be connected to a clean electrical power supply via a surge protector.

2

INSTALLATION OF TOS



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

2.1 Overview

This chapter describes how to install the TerraMaster Operating System (TOS) and perform some essential configuration work. The current version at the time of writing is TOS 4.2.n and this guide is based around it; however, if you have a slightly different release (e.g. TOS 4.1.n) you should still find nearly all of this book applicable as most changes tend to be bug-fixes, minor tweaks and slight cosmetic changes. Having installed TOS, you will then be able to define shared folders ([3 SHARED FOLDERS](#)), setup the users ([4 USERS](#)) and connect computers and other devices ([5 ACCESSING THE SERVER](#)).

The assumption in this chapter is that you are installing a brand new TNAS. If this is not the case – maybe you have obtained a previously used model, for instance – you might find it helpful to first take a quick look at section [11.16 Preparing a TNAS for Disposal](#).

2.2 Initial Installation

Commence by physically installing the hard drive(s). The drives have to be screwed into the supplied removable caddies, which should then be carefully inserted into the TNAS. TerraMaster helpfully provide stickers to label the caddies; this is useful if a drive ever needs to be replaced, because once installed they have to remain in sequence.

Connect the TNAS to the network using an Ethernet cable; if the TNAS has multiple network adapters, only the first one should be connected for now (this is important). Plug in the power adapter and switch the unit on. After a minute or two, the unit should settle down and all of the small lights on the front should be glowing green.

To install the TOS software you need a Windows or macOS computer with an internet connection. Go to the TerraMaster website – www.terra-master.com – and click **Support** followed by **Download**. Use the dropdowns to select your model and click **Start**. Click the **Desktop and system** tab and download and install the *TNAS PC App* for Windows or macOS as appropriate. Although functionally similar, they may be some cosmetic differences between them and generally speaking, the Windows version is updated more frequently than those of the other platforms. Having installed the software, run it. If you receive a message from your computer's firewall, you should grant permission to the application.

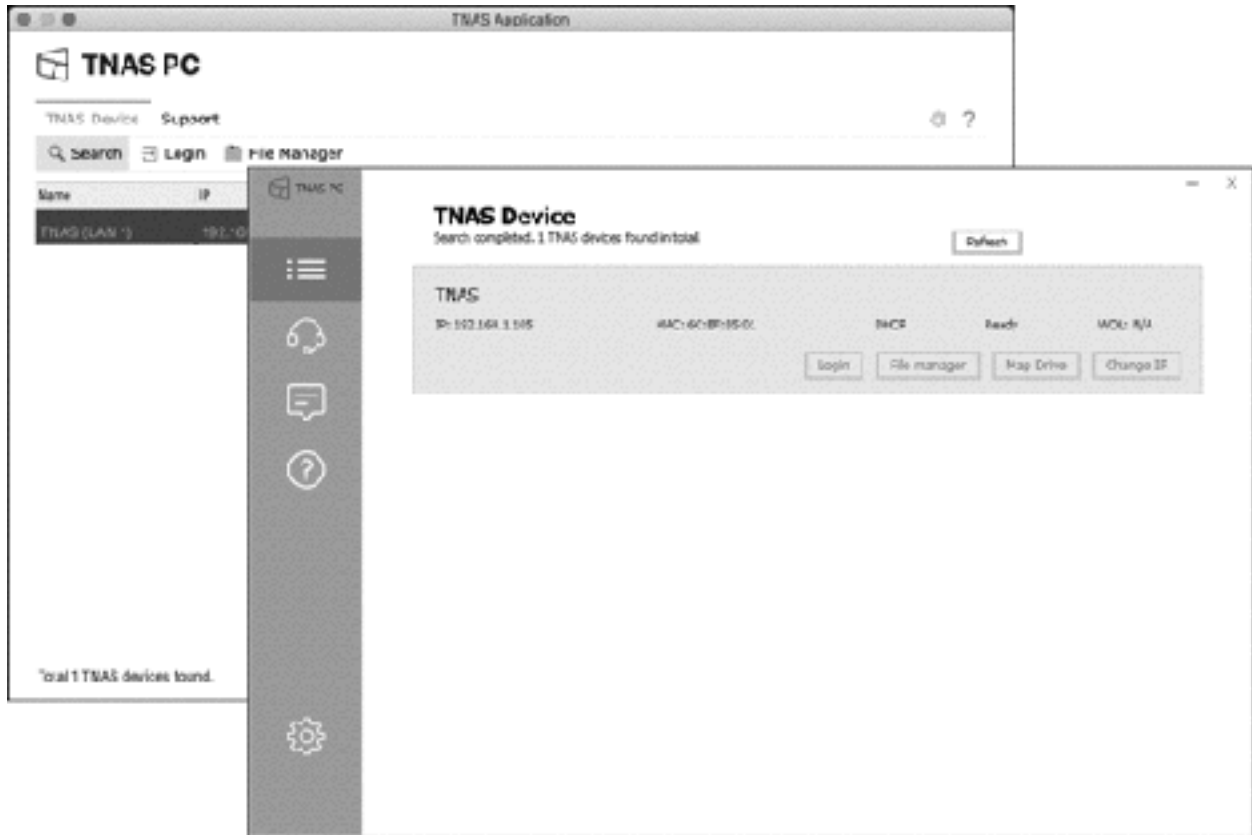


Figure 3: TNAS Applications for Mac and Windows

Highlight the TNAS and click **Login** to display the following screen in your browser:

Free edition. Do not copy



Figure 4: Starting the installation of TOS

The number on the screen – 192.168.2.31 in this example but yours will be different – is the IP address of the NAS and should be noted. Click the **Start** button. On the subsequent screen, click **Confirm** to check the health of the hard drive(s); the time taken for this depends on the number and capacity of the drive(s), but when complete – and assuming no problems – the system will start downloading and installing TOS, during which time a status screen is displayed:

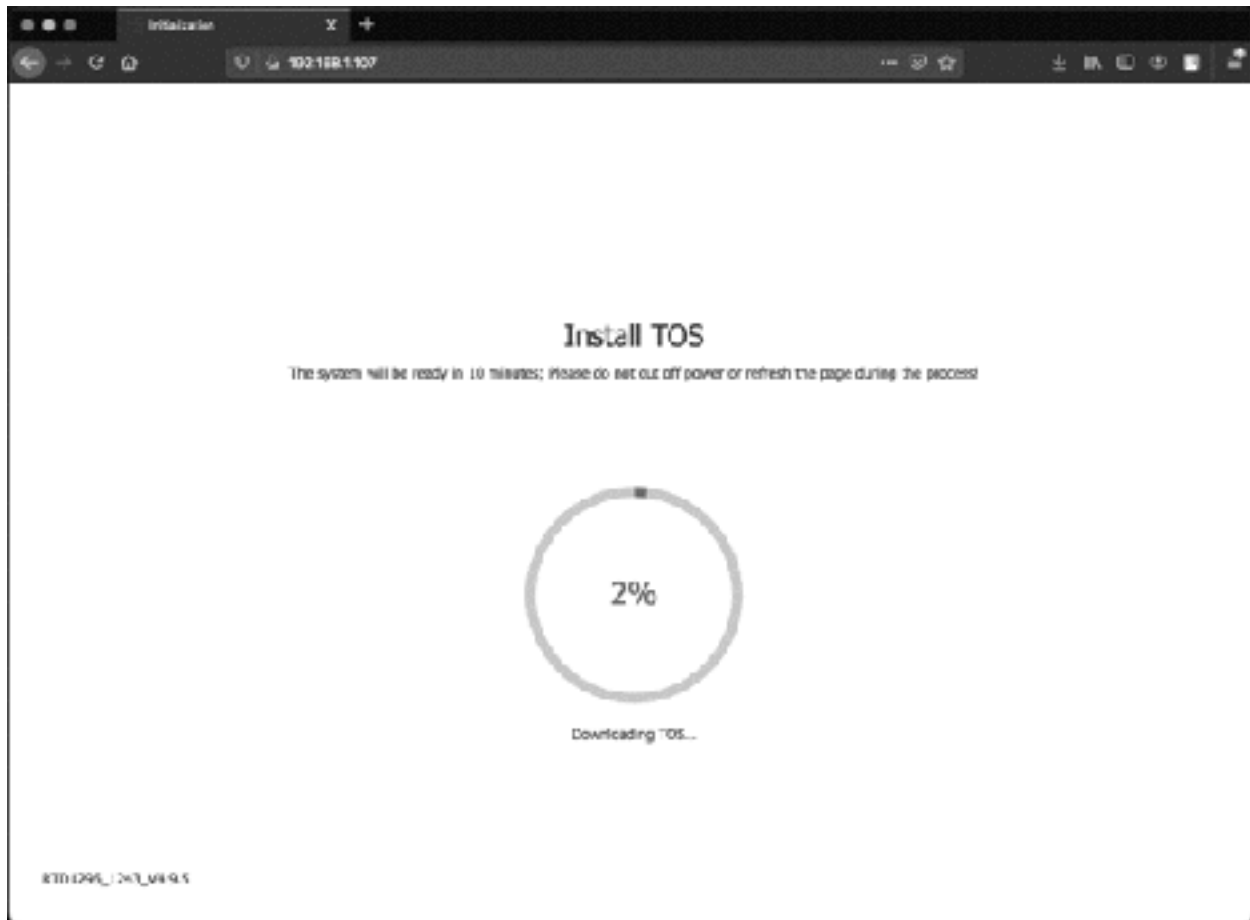


Figure 5: TOS Download screen

Specify a *Username* for the Admin account, which is used for administering and managing the server. Traditionally, this has tended to be *admin* on TerraMaster but it can be whatever you choose. As hackers tend to look for obvious names such as 'admin', an alternative may be preferable and in our example we have chosen the name *systemadmin*.

Specify and confirm a password, which should be non-obvious, more than 8 characters on length and comprising a mixture of letters and numbers. Do not try to use words like *password*, *admin* or *TerraMaster*. Choose a time zone corresponding to your location in the world, using the dropdown. Note: the dropdown defaults to Chinese Standard Time.

The initialization process requires you to provide a valid email address, referred to as the *Security Email*, to obtain a verification code. It is strongly recommended that you do this because if, for whatever reason, you lose or forget the admin password you can contact TerraMaster using the registered security email address to reset it. However, although the Security Email field is mandatory, you do not actually need a verification code to proceed:

Happy to send a security email? Enter your email address and click **Send code**. Within about 30 seconds, you should receive the code. Enter it into the *Verification code* field (you may want to cut and paste it to avoid errors) and click **Next**. If you cannot see the email, check your spam/junk folder. If it is not there, click **Send code** to try again. If all else fails, click **Can't receive email? Skip this**.

Do not want to send a security email? Enter any email address but do not click the **Send code** button. Instead, click the **Can't receive email? Skip this** link which appears after entering it.

Admin Settings

Device name
server

Username
systemadmin

Password

Confirm password

Time zone
(GMT 00:00) Dublin, Edinburgh, Lisbon, London

Security Email
youname@email.com

If you forget the password, you can retrieve password with this email.

Verification code

Send code

Can't receive email? [Skip this.](#)

Next

Figure 6: Specify the admin password and security email

What happens next depends upon the TerraMaster model and the version of TOS. If it is an ARM-based model and TOS 4.2.13 or later is being installed, no further action is needed and you can jump to section [2.3 Five Minute Tour of TOS](#). But in some cases you will eventually be taken to the next screen, which is concerned with configuring storage space. You have two choices here: if you are new to NAS or a non-technical person or simply want to progress as quickly as possible, simply accept what the installation process is proposing (let's call this the 'easy option'). If you are an advanced or technical user and wish to have control over the process, click **Cancel** and choose your options from the resultant screen (let's call this the 'advanced option'). Note that we are only using these terms for convenience and understanding and they are not actually used by TerraMaster themselves.

Easy Option

If you do nothing, after 10 seconds the configuration process will commence. TOS will make a sensible choice and all you have to do is click the **Confirm** button:



Figure 7: Click Confirm to configure storage space

TOS will configure and format the drive(s), a process which typically takes between 3-20 minutes depending upon their number and capacity. When complete, you will be presented with the TOS login screen. Please jump to section [2.3 Five Minute Tour of TOS](#) below to continue.

Advanced Option

If you clicked Cancel, you will be taken a series of screens where you can manually define the storage. The key concepts are that the drives constitute a *Storage Pool*, upon which one or more *volumes* are created. The drives can be configured for *RAID* to provide redundancy (data performance) and/or maximize performance. The storage is then formatted with a *file system*.

Firstly, a panel about the hard drive setup is then shown, the contents of which and the options available depend upon what drives you have. In this example, there are two hard drives and TOS is proposing that they are configured as RAID 1. The default suggestion will be suitable for most people, but if you would prefer another arrangement, click the drop-down and choose another configuration e.g. JBOD for maximum space (you cannot select modes that are incompatible with the number of installed drives). A detailed description of RAID levels can be found in section [10.2 RAID](#). It is important to think carefully about your requirements as, although it is possible to subsequently change matters, it will potentially result in data loss and other complexities. Tick the drives to be used, make a decision about RAID and click **Next**. A warning message that any existing data on the drives will be deleted is shown – click **OK**.

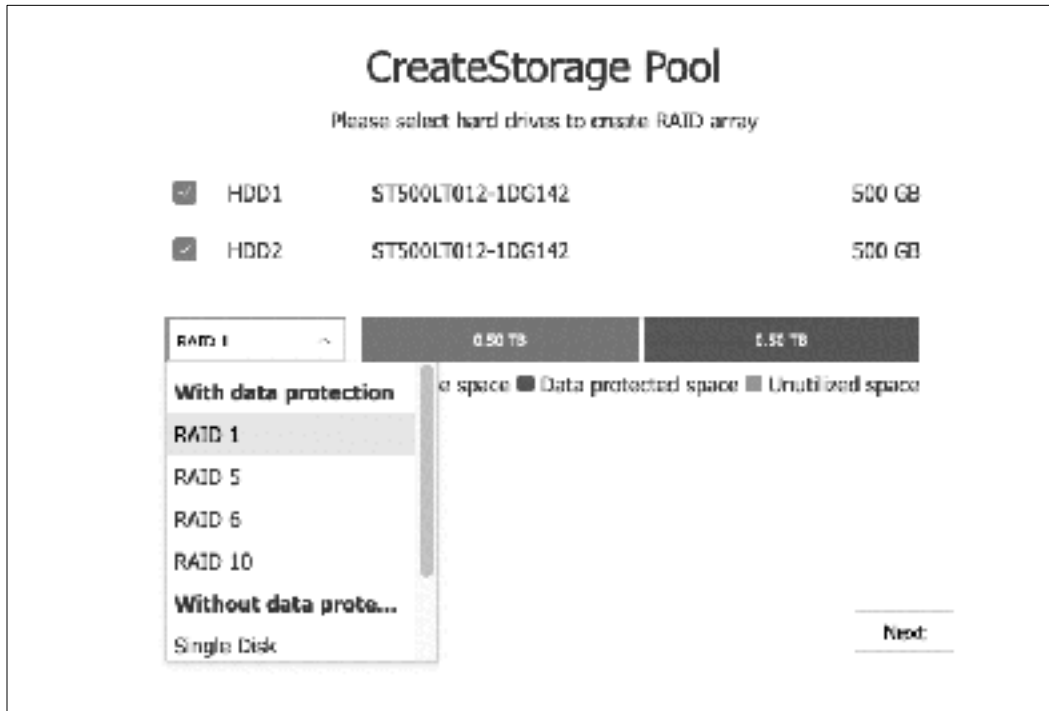


Figure 8: Select the drives and specify the RAID level

On the subsequent panel, optionally give the volume a *Description*. You could potentially reduce the Volume capacity, although this would be highly unusual and not recommended. Click **Next**:



Figure 9: Volume details

The subsequent screen is for choosing the file system on x86-based models. Before they can be used, volumes have to be formatted. You may be familiar with the disk formats used by Windows PCs and Macs, such as NTFS, FAT-32, ex-FAT and APFS. In the case of TNAS, there are two alternative disk

filing systems, *ext4* and *Btrfs* (sometimes pronounced 'butter-F-S'). *Ext4* is a universal format, common to most brands of NAS. *Btrfs* is a more sophisticated file system that supports additional features, one of which is *snapshots*, a built-in automatic backup mechanism where the system makes a note of what has been altered when a file or folder has changed, then writes away those details to a different part of the disk. The potential downside of *Btrfs* is that it has more demanding hardware requirements and will use a portion of the available storage space. How to choose? Generally speaking, *Btrfs* is considered superior, but *Ext4* may be a better choice on lower cost models. Make a choice and click **Next**:



Figure 10: Select a file system

A screen to confirm the settings is shown; click **Next** and acknowledge the subsequent message by clicking **Confirm**. TOS will configure and format the drive(s), a process which typically takes between 3-20 minutes depending upon their number and capacity. When complete, you will be presented with the TOS login screen. Please continue below with section [2.3 Five Minute Tour of TOS](#).

2.3 Five Minute Tour of TOS

The TOS login screen appears as follows. The attractive wallpaper background is different each time round, so your login screen may have a different appearance. The login screen is only valid for a fixed time and if you do not login within about 15 minutes, it will expire and you will receive a ‘token warning’. Simply reload the screen to refresh and re-enable it. If the browser is not displaying the screen, enter the IP address of the server in the address bar. If you did not make a note of the IP address, you can use the TNAS PC utility to ‘find’ the server.

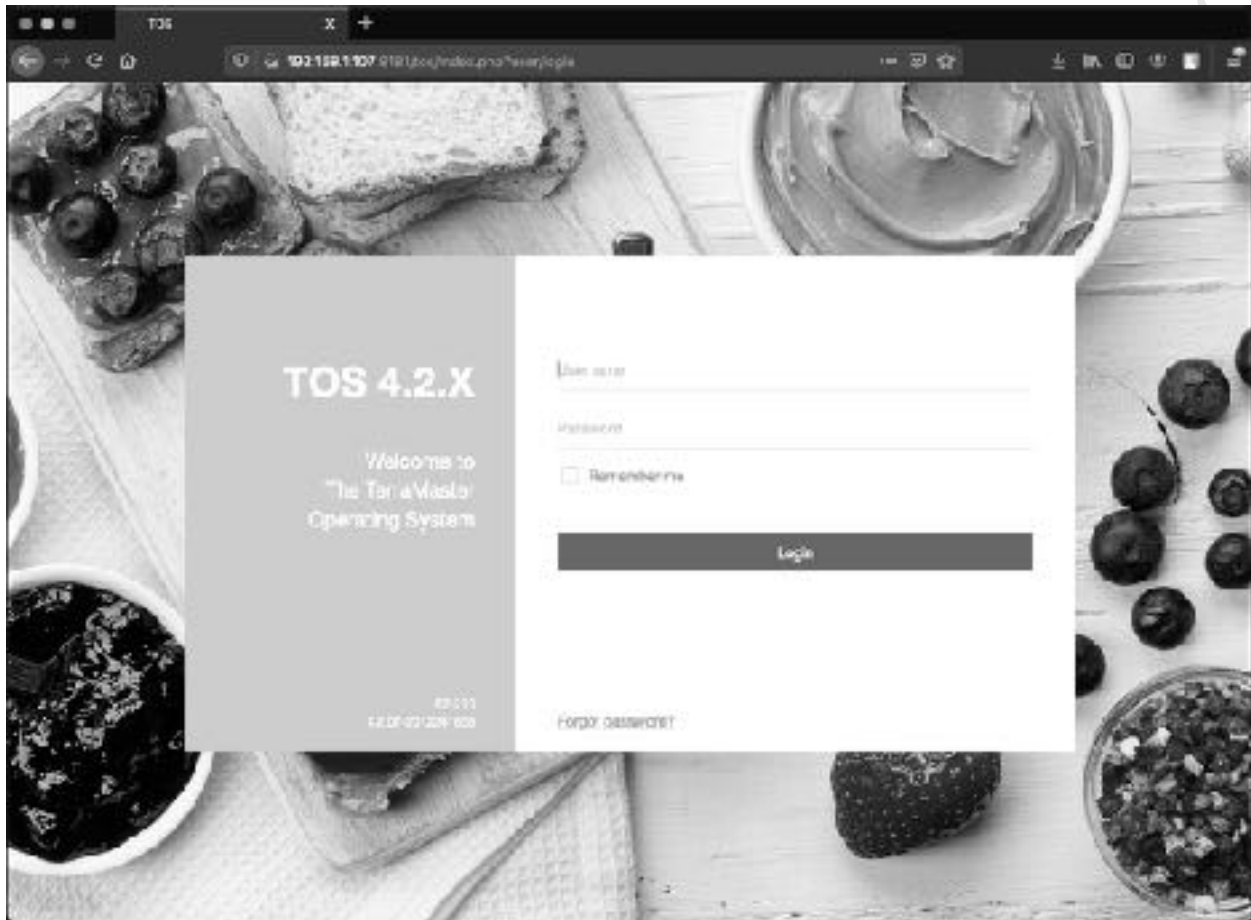


Figure 11: TOS login screen

After logging in as admin and using the password defined earlier, the main TOS screen is shown, which is clean and streamlined and will look familiar to anyone who has used a desktop or laptop computer. There is a Desktop area, containing a number of icons, which are clicked to run the underlying program or feature. Most of these icons are only available to the *admin* user. There is something akin to a combined menu bar and taskbar at the top of the screen. A panel to launch the help system is displayed – if you do not wish to see this each time, tick the **Don't prompt me again** box and click **Close**.

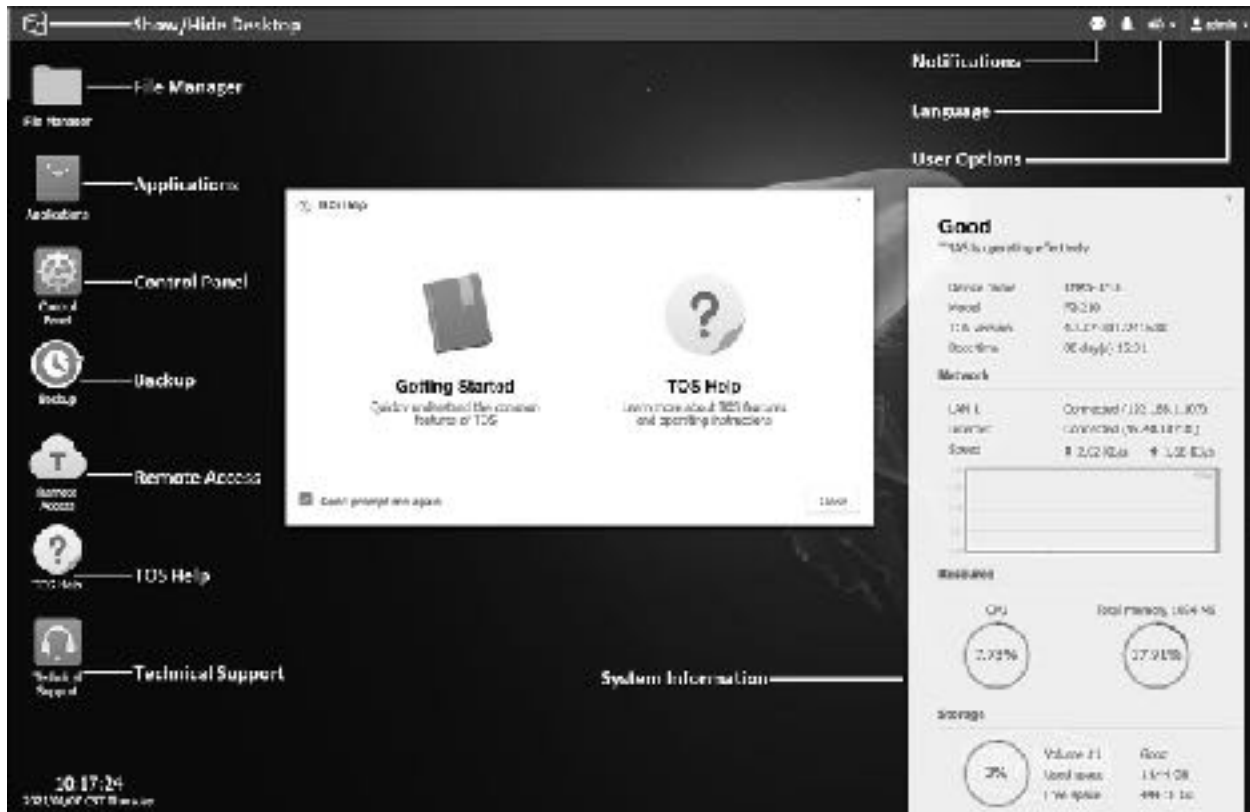


Figure 12: Overview of the Desktop

Starting in the top left-hand corner, the functions of the icons are as follows:

Show/Hide Desktop – the small TerraMaster logo is a toggle switch and clicking it temporarily hides any open windows on the desktop; clicking it again restores them.

File Manager - displays the contents of the disk volumes and folders and can be used for manipulating files, similar in principle to Windows Explorer/File Explorer on a PC or Finder on a Mac. It is covered later in section [5.2 Using a Browser and File Manager](#).

Applications - used for downloading and maintaining apps from TerraMaster that provide additional capabilities (think of it as an ‘app store’). It is discussed in detail in section [11.2 Applications](#).

Control Panel - provides icons to setup, customize and manage the TNAS, grouped into five main categories of *Privileges*, *Network Services*, *Storage Manager*, *General Settings* and *System Information*. Click on an icon to make something happen. Most of these icons are covered in this guide. The Control Panel and most windows can be resized, minimized or closed using the small icons in the top-right hand corner. Windows can also be moved around and resized using a mouse.

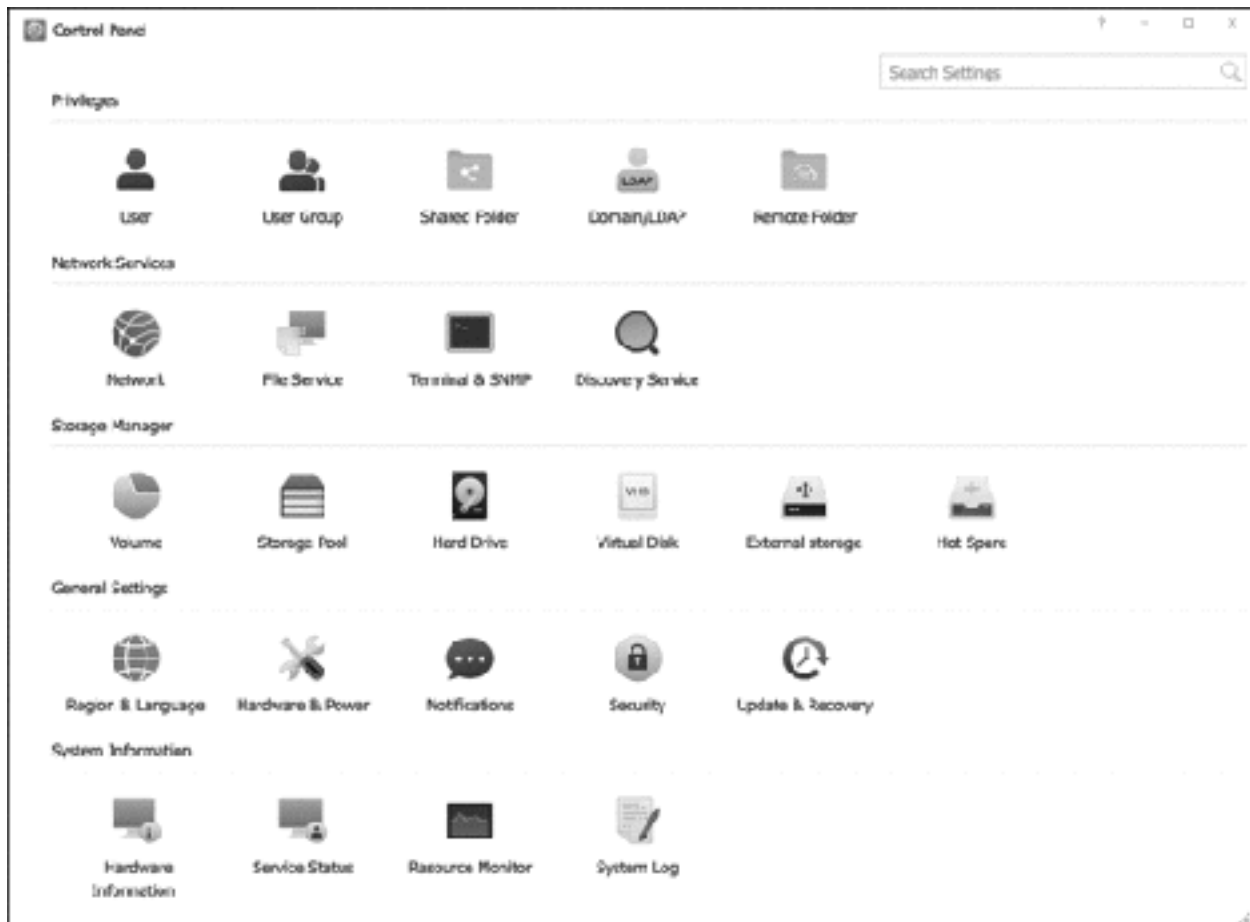


Figure 13: Control Panel

Backup - provides access to backup tools. These are covered comprehensively in chapter [7 BACKUPS](#).

Remote Access - used for configuring the TNAS so it can be accessed from outside the home or office.

TOS Help – this icon does exactly what the name suggests. It provides basic information about many aspects of TOS, albeit some sections are outdated and less comprehensive than this guide. In addition, many screens in TOS have a link to the online help system, accessed by clicking the small question mark icon in their top right-hand corner.

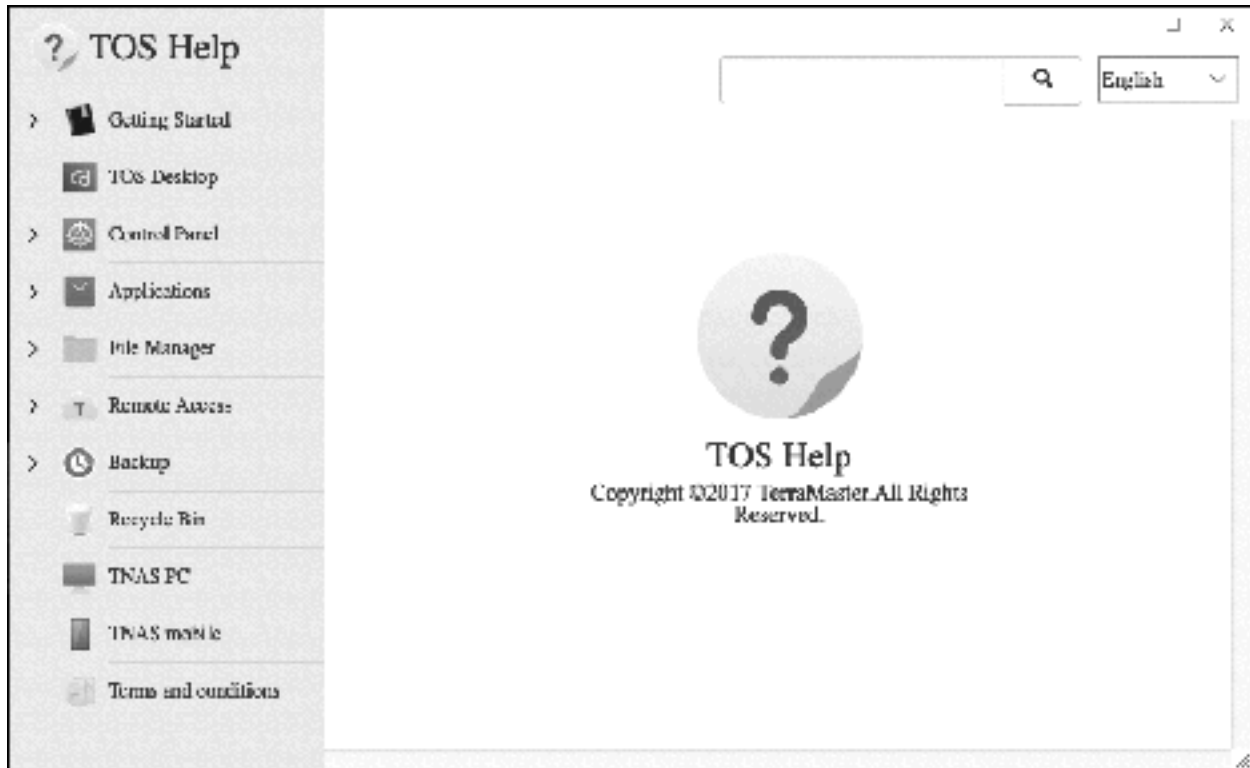


Figure 14: TOS Help

Technical Support – enables TerraMaster, with your permission, to access the TNAS for support purposes. This mechanism is described in section [11.15 Contacting TerraMaster for Support](#).

In the top right-hand corner of the main screen are several small icons. The first one is the *Notifications* icon, which displays warnings, errors and other messages. Immediately to its right is a bell icon, which controls the buzzer in the TNAS. The third one, a small globe icon, is a drop-down which enables the language of the device to be changed and there is a choice of 13 widely used ones. The final icon lists the current user name and is used for customizing the user's settings. It is also used for restarting and shutting down the TNAS, although only the *admin* user can do so.

In the bottom right-hand corner of the screen, the *System Information* panel is displayed. This gives a useful 'at a glance' summary of the health of the server and the utilization of key resources. The panel can be moved to a different part of the screen but will always snap to the bottom of it. To close System Information, click the cross in its top-right hand corner. When closed, a white bar appears in its place at the bottom of the screen and clicking it will restore the panel.

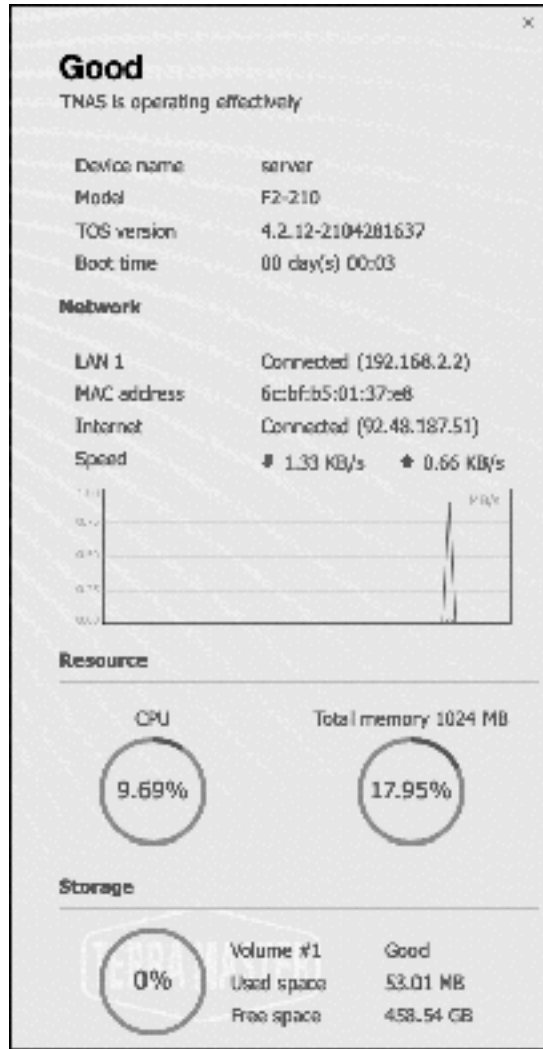


Figure 15: Control Panel

The Desktop itself can be right-clicked to produce a menu of options. For instance, the items on the Desktop can be sorted, new files and folders can be created, the background wallpaper can be changed and so on.

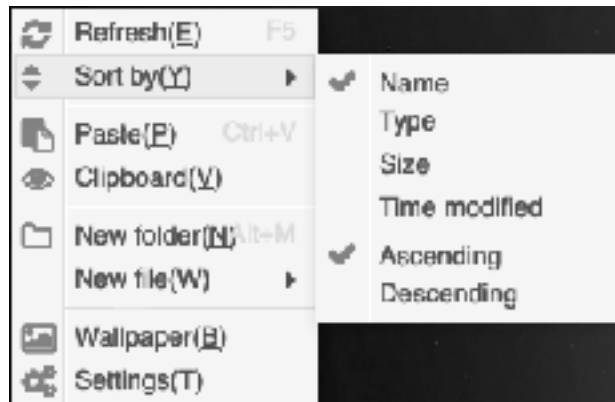


Figure 16: Right-click options

2.4 Configure Networking

Note: if you already understand what IP addresses are, you can skip the first four paragraphs and jump to the one that begins ‘Click Control Panel followed by Network...’.

The second thing we need to do is make a decision about the IP address for the TNAS. Every device within a network is represented by a unique number, known as the IP address. This consists of four sets of three digits, separated by periods, ranging from 000.000.000.000 through to 255.255.255.255. Most of these IP addresses are reserved for websites and other internet applications, although they are not generally used in a direct manner, thanks to the Domain Naming System or DNS, which removes the need to memorize them (for instance, it is easier to remember google.com rather than 216.58.210.238). These addresses are known as public IP addresses. However, a limited set of numbers are not routable over the internet, making them ‘invisible’ to it, and these private IP addresses are used in local area networks. The sequences which must be used are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255 and 192.168.0.0 to 192.168.255.255. As these addresses are isolated, they can safely be used by anyone without risk of duplication and the same numbers are used worldwide in millions of networks.

Much of the equipment intended for use in small businesses and homes tends to assume a *192.168.nnn.nnn* numbering scheme; for instance, internet routers commonly have addresses such as *192.168.1.1* or *192.168.0.254* or similar pre-defined, depending on the brand. However, devices such as computers, printers and NAS boxes do not come with IP addresses already allocated; instead, they have to be configured with a suitable address and there are two ways of doing so: you can use *static IP addresses* or *dynamic IP addresses*.

With static IP addresses, it is necessary to visit each device and individually configure it. For instance, you might set the first computer to *192.168.1.101*, the second to *192.168.1.102*, the third to *192.168.1.103* and so on. You have to be careful to keep track of everything and above all make sure there are no duplicates. If this sounds like hard work then that’s because it is – you might get away with it if there are only a handful of devices, 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 separate device or physical server (although it could be in a large network) and most all-in-one routers of the sort used in small businesses and homes have DHCP server software built-in. During the installation the TNAS received an IP address from the router’s DHCP server. However, servers and NAS boxes work better with fixed or static IP addresses, so we need to change matters.

Click **Control Panel** followed by **Network** and the **Network Interface** tab. The first or only *LAN* entry will have a status of *Connected* – click to highlight it, then click the **Edit** button:

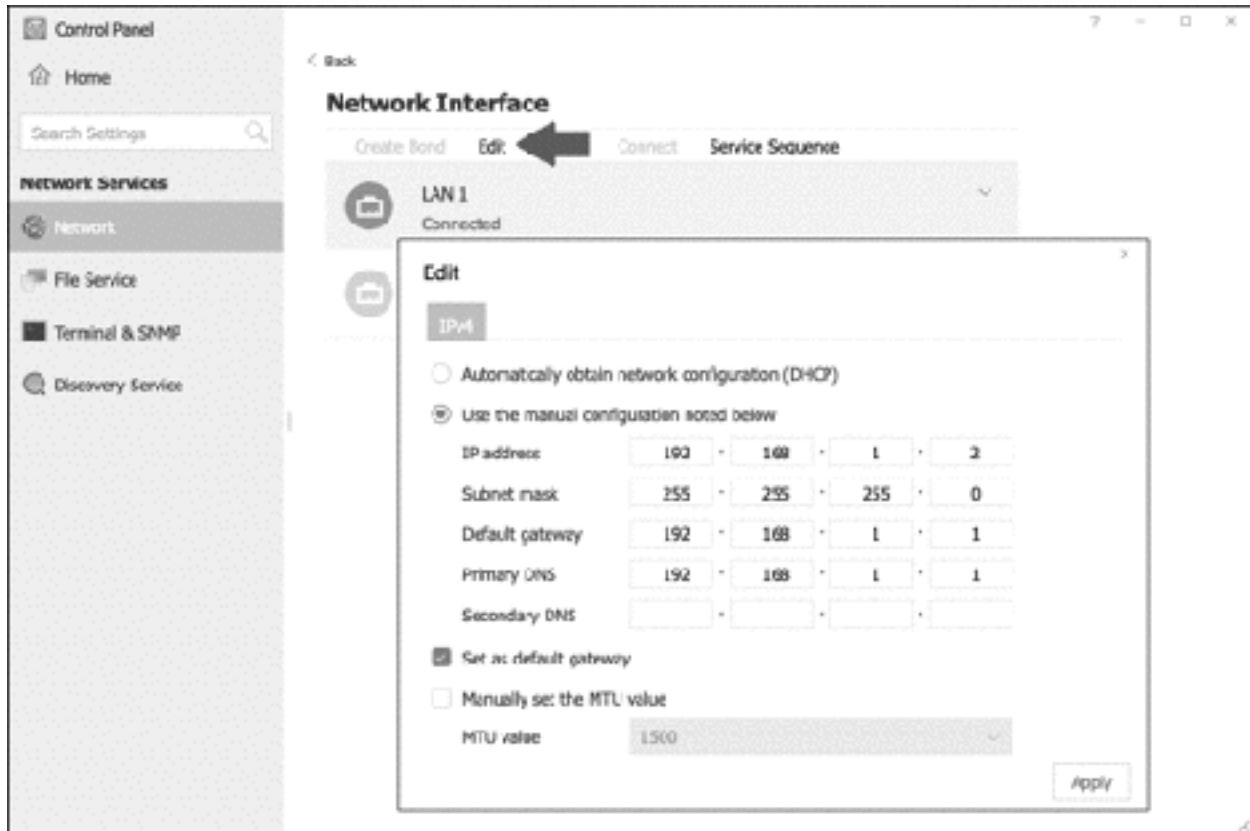


Figure 17: Setting the server's IP address

Click the **Use the manual configuration noted below** option and specify an IP address that is close to that of the router, which is shown on the screen with the alternative name of *Default gateway*. It is the fourth and final set of digits that is significant in small networks, defined as those with less than 255 devices, and the first three sets should not be altered. In this example, the router/gateway is 192.168.1.1, so a suitable address for the NAS would be something like 192.168.1.2. The *Subnet mask* should normally be set to 255.255.255.0. The *Primary DNS* should be the same address as the router/gateway. The *Secondary DNS* setting can be ignored, although you could set it to an external DNS (e.g. 8.8.8.8, which is Google's). Tick the **Set as default gateway** box and click **Apply**. Note that having made a change to the IP address, you may lose connectivity to the TNAS and have to refresh the browser and login again.

Note 1: if you have multiple servers, you could use sequential IP addresses. For instance, the first server might be 192.168.1.2, the second 192.168.1.3, the third 192.168.1.4 and so on.

2.5 Power Management

TNAS systems have various options relating to power management. Some of these are concerned with energy saving and can be used to reduce power consumption and hence save money. To access them, go into **Control Panel** and click **Hardware & Power**. On the resultant panel there are three options: *Hardware*, *Power* and *UPS*. Click **Hardware**.

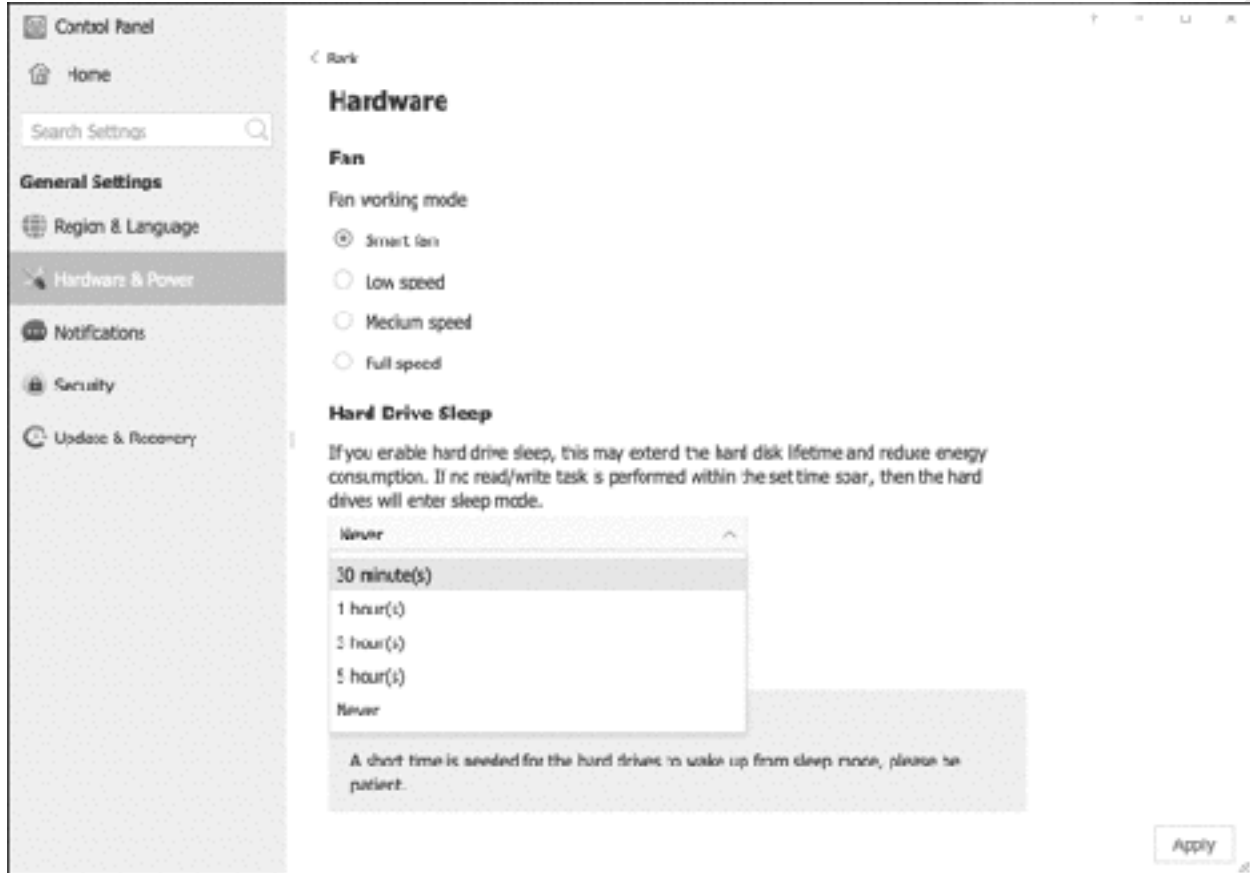


Figure 18: Control Panel for Hardware

The first section controls the fan. Set the *Fan working mode* to **Low speed** if the TNAS is located in a quiet area (e.g. at home) or to **Smart Fan** or **Medium speed** if a small amount of noise is acceptable (e.g. typical office environment). If the TNAS is located in a warm place, or where noise levels are unimportant, you may want to set it to **Full speed** for maximum cooling.

The second section controls the *Hard Drive Sleep* time, which enables to be programmed to hibernate after a set period e.g. 30 minutes. This saves energy but may result in a short delay when someone attempts to access the TNAS, typically in the order of about 15-30 seconds, whilst the disks spin up again (although there is no delay if using Solid State Drives). Click **Apply** and acknowledge the confirmation message that is displayed.

Returning to the main panel, click **Power**. Tick the **Enable auto power on** box. This will cause the TNAS to switch itself on following any power failures.

The TNAS can be scheduled to power itself on and off automatically. Doing this can save on energy costs and enhance security. However, note that if this is done then it is important to ensure that the TNAS will not be powered down when an activity such as backup or an anti-virus scan is scheduled to take place. To set the power schedule, tick the **Enable scheduled power on/off** box and click **Create**. On the resultant panel, click **Power on** and set the Date dropdown to **everyday** (although you can specify it on a daily basis, if required) and choose a Time. Click **Save**. Repeat, and this time set a **Power off** time. Click **Save**.

The Power screen will now be updated. In this example, the NAS has been set to switch on at 07:00am (07:00) and shut down at 10:00pm (22:00). Double-check that the **Enable scheduled power on/off** and **Enable auto power on** boxes are still ticked and click **Apply**.

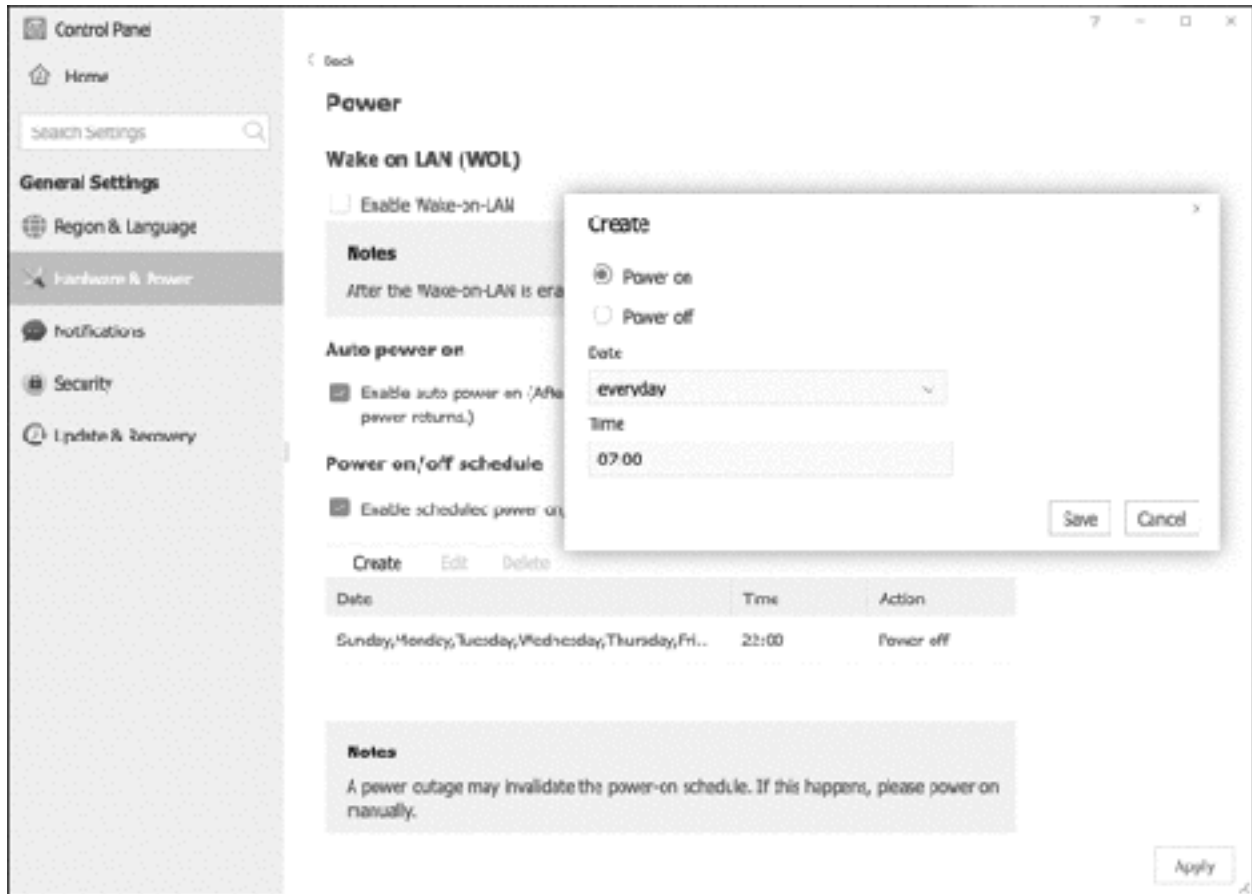


Figure 19: Power settings

To reduce the impact of power failures, which can result in lost data, the TNAS can be connected to an Uninterruptible Power Supply (UPS), which enables it to shut itself down in an orderly manner. To manage this, click on **UPS** from the main panel. If an UPS is not used, which is often the case in a domestic setting, connect the TNAS to the electrical supply via a surge protector.

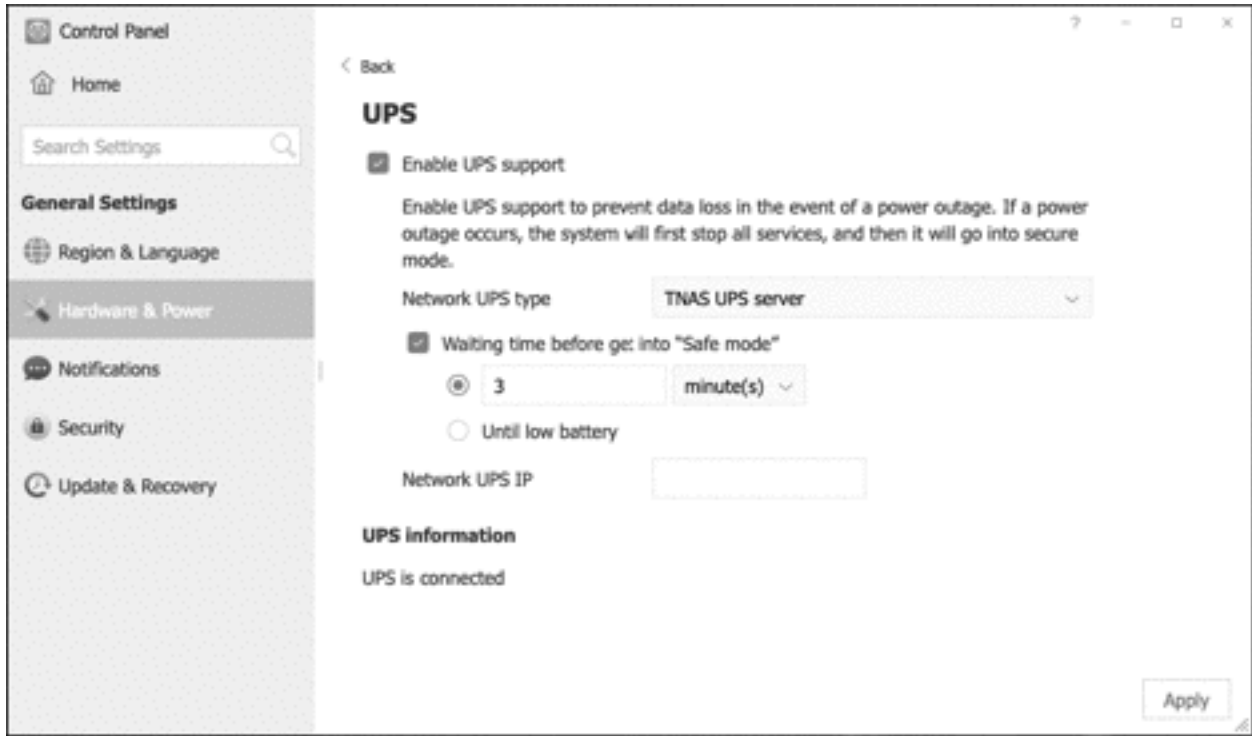


Figure 20: UPS support

Free edition. Do not copy or circulate

2.6 File Service

File Service refers to the means by which TOS provides access to files and folders for different types of client computers. These clients can be Windows PCs, Macs, or Linux machines. Other devices, such as tablets and smartphones, may be able to access files on the TNAS if they understand the underlying protocols associated with these computer types or are equipped with suitable apps.

By default, the TOS installation assumes that you will be using Windows PCs and Macs and it is not usually necessary to change any of the settings for File Service. So, most people reading this can simply skip to the next section. However, if any of the following conditions apply, then you may need to make changes: the Windows workgroup is not called *Workgroup* (although it usually is); you want to backup Macs to the server using Time Machine; you wish to use Linux or other Unix-based computers in a manner which uses their specific characteristics.

If you have multiple TNAS devices and are using one to receive backups from another, you will need to enable *Rsync*. This topic is discussed separately in section [7.5 NAS to NAS Backups Using Rsync](#).

Windows Workgroup Name

To change settings, go to **Control Panel**, click the **File Service** icon, followed by **SMB/CIFS File Service** (which is what Windows uses). If your workgroup is not called *Workgroup*, change the name to match that of your computers. Note: having to do this would be quite unusual as *workgroup* is the standard name. Click **Apply**.

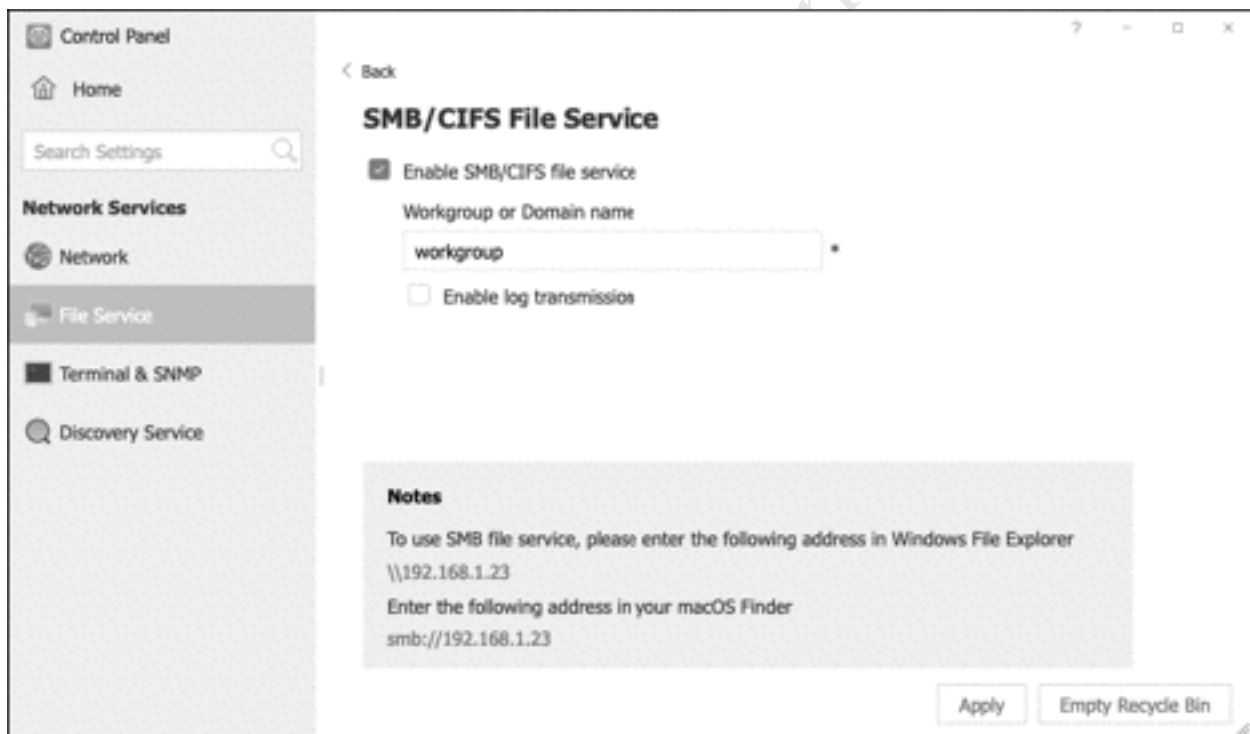


Figure 21: SMB/CIFS File Service

Macs

Historically, Apple computers used a network protocol called AFP (*Apple Filing Protocol*) whilst Windows computers used SMB (Server Message Block). However, beginning with OS X 10.9 ('Mavericks') Macs switched to SMB for their default network protocol, too. In theory, you could operate without AFP support, but it is recommended that you keep the AFP service enabled. You will certainly need it if you are using older versions of OS X. Best practise is to keep it enabled if you have any Macs whatsoever.

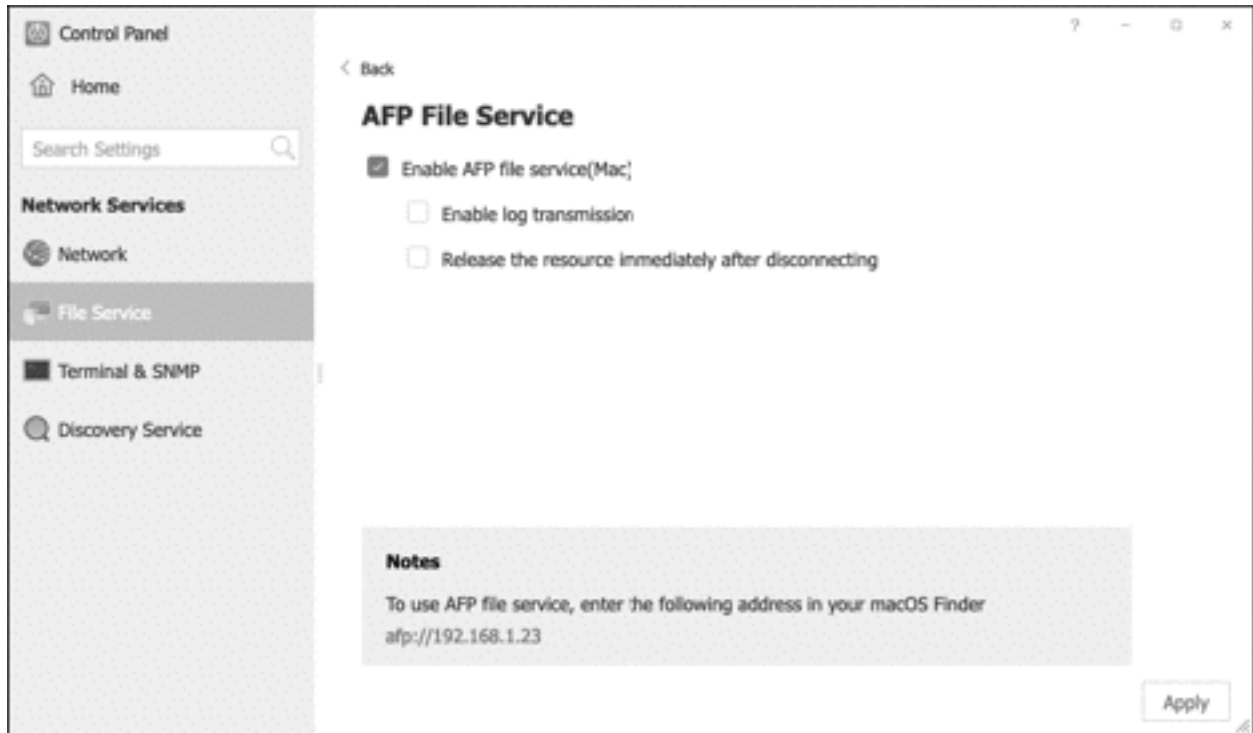


Figure 22: AFP File Service

Linux/Unix Computers

Most Linux and Unix distributions include the ability to connect to SMB-based systems, which is what TOS is. Unless you have a specific need, you may find it easier to use SMB, in which case you do not need to do anything additional. However, if you use Linux or other Unix-type variant computers in an 'advanced' manner – defined here as specific use of the NFS protocol – you will need to enable NFS on the TNAS. Within **Control Panel**, click the **File Service** icon and on it click **NFS File Service**. Check that the **NFS File Service** box is ticked. If NFS v4.1 is being used, it is necessary to tick the appropriate box and specify the NFS v4 domain. Having made any changes, click **Apply**.

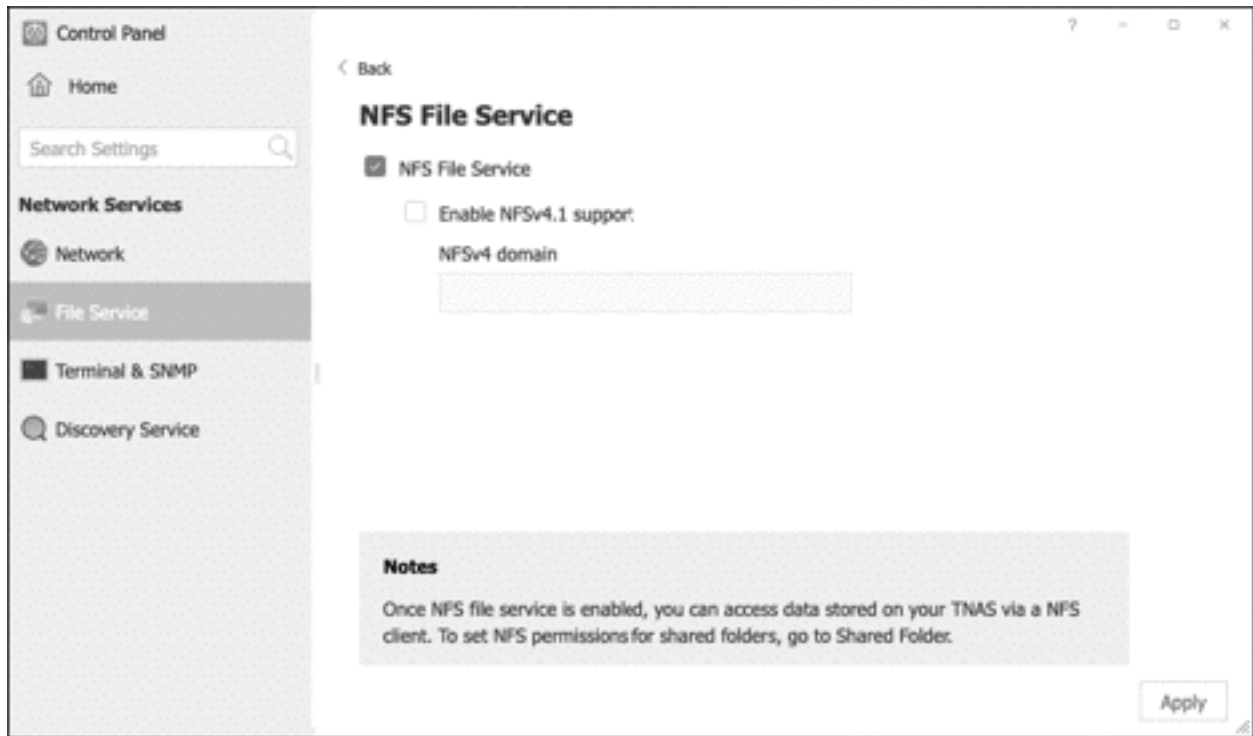


Figure 23: NFS File Service

2.7 Setup Remote Access

Remote access has two aspects. Firstly, there are the actual capabilities: cloud storage, syncing, backup and so on that TOS and the optional packages provide. The second aspect is how to connect the TNAS to the internet and be able to access it in a simple, secure and safe manner and this is what *TNAS.online* does: it provides an easy, straightforward mechanism for remote access, suitable for most home and small business users. It works as a relay service, passing data to and from computers and the NAS over the internet via TerraMaster. No data is stored at TerraMaster itself and it remains your data on your computers. Because the service uses standard web protocols, it avoids the need for techniques such as port forwarding, router configuration and domain services. This also means remote access can be made available in many places where there may be no option to make technical changes to the underlying environment, such as in schools, colleges, corporate workplaces and so on.

TNAS.online is configured by launching *Remote Access* from the Desktop screen. Tick the **Enable TNAS.online remote access** box and enter a name (*'TNAS ID'*) for the TNAS. The name should be at least 6 characters in length and comprise a mixture of letters, numbers and punctuation. It needs to be unique, although you have no way of knowing if it is until you try to apply it. You do not have to enter your own name: a default one is suggested that you can use and which is unique, although it is not a 'friendly' name. Select a server using the dropdown – this should be **Global (Recommended)** unless you are based in China. Click **Apply**. If all is well, the ID status will change to *'Registered successfully!'* and an address for the TNAS will be displayed, in the format *TNAS.online* followed by the registration name e.g. *http://TNAS.online/CTACS*:

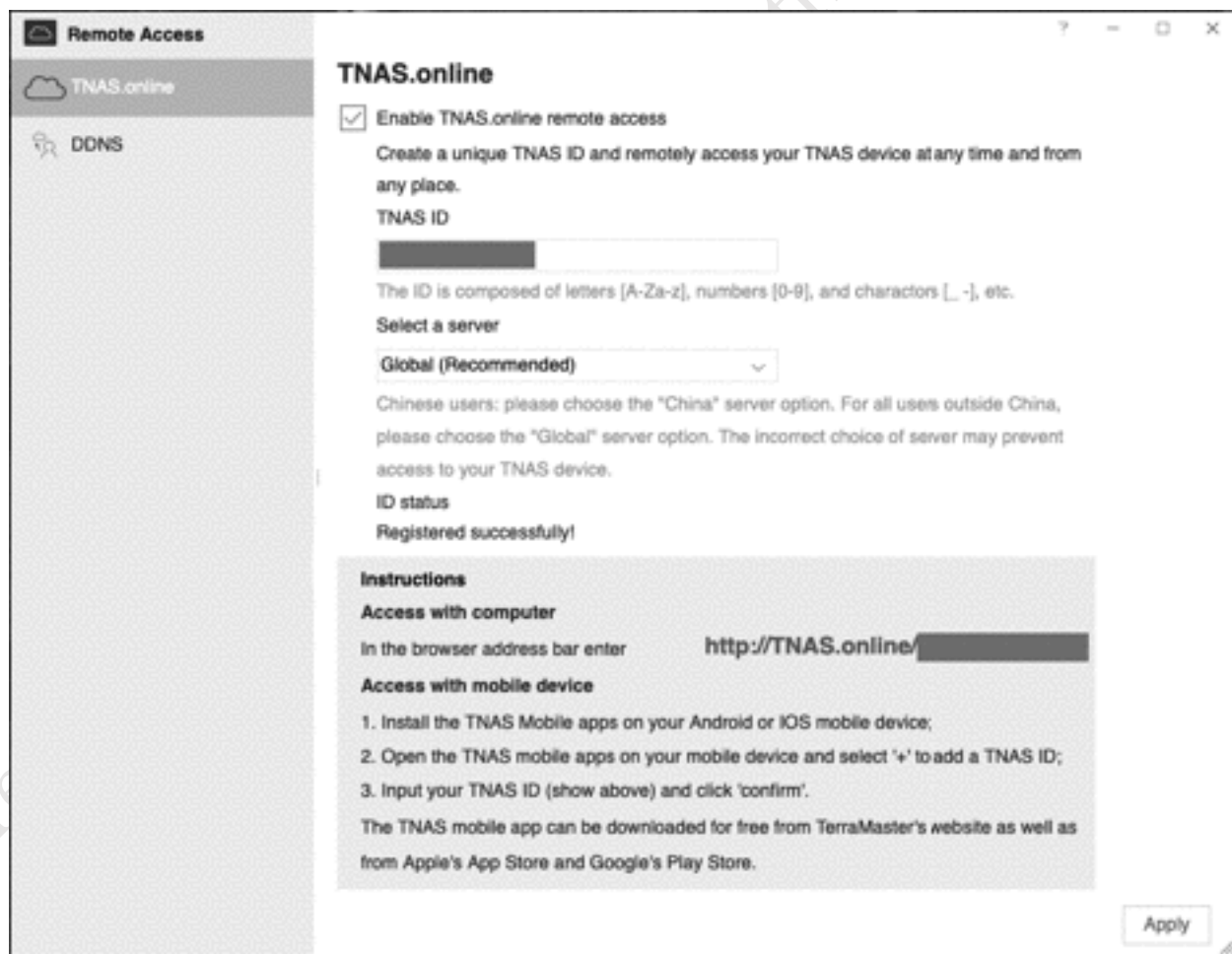


Figure 24: Enabling Remote Access

Assuming no problems, you can now test the system. From a computer, launch an internet browser such as Chrome/Safari/Firefox and enter the TNAS ID e.g. <http://TNAS.online/CTACS> or whatever your ID is. After a few seconds, you should be greeted with the standard TOS logon screen. Having logged on, it is exactly the same as if you were connected locally.

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

3

SHARED FOLDERS



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

3.1 Overview

The main purpose of most networks is to provide an environment for users to safely store and share information. This is done by creating folders on the server, some shared and some private, then defining access rights to control who sees what. The structure of these folders will depend upon the requirements of the household or organization, but a typical arrangement might be: one or more shared folders that everyone has access to; folders for the different departments and functions within a business; folders for music, photos and videos (particularly so for a home system); individual private or 'home' folders for each user, analogous to the Documents folder on a PC or Mac. These folders are referred to as *shared folders* and they reside on storage *volumes*. During the installation of TOS, an initial storage volume would have been created.

In our examples we have one volume, upon which all the folders are created. In a larger system, there may be multiple volumes with the shared folders allocated across them; this technique can be used to enhance security, for instance an organization might keep confidential information on a separate volume away from the main company data. Additional shared folders can be created at any time as required, not just when setting up the system for the first time.

3.2 Creating Shared Folders

To create a shared folder, go to **Control Panel > Shared Folder > Shared Folder**. Notice that there are already two folders in place, which were created automatically during the installation of TOS: *appdata* and *public*. The former is a special folder used by TOS when additional applications are installed and should not be touched. *Public* will be used as a shared folder to which everyone will have access and will be returned to shortly ('public' in this sense means all users of the TNAS, not the world at large). We are going to create an additional shared folder, to be used for storing a location to store master copies of programs, drivers, utilities and so on. Click **Create**:

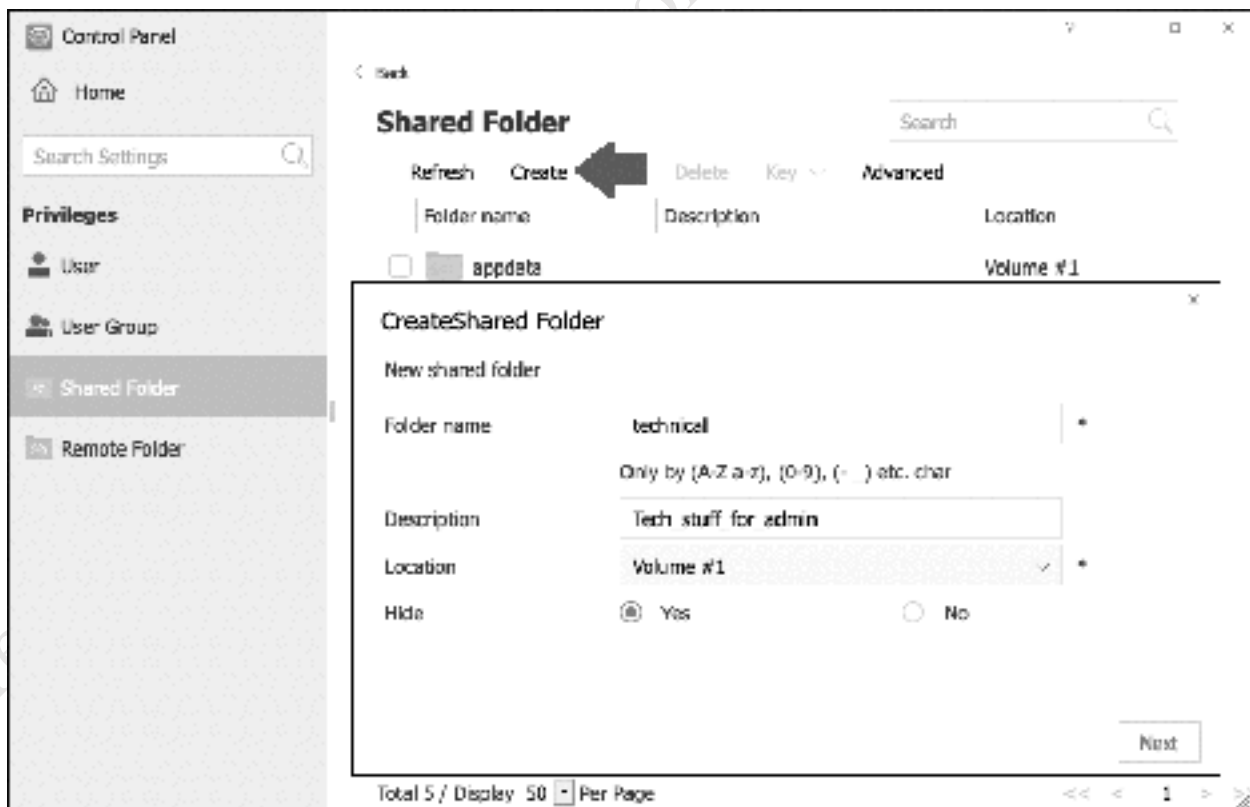


Figure 25: Creating a shared folder

Give the folder a meaningful name, in this case *technical*, along with an optional description. If you have multiple volumes on the system, you can make use of the *Location* drop-down. It is possible to hide a folder, so that users without permissions will not be able to see it. This is not so much a security measure as a means of keeping the system tidy from a user perspective as there could, potentially, be dozens of folders on the system. In this particular case we are choosing to hide this folder. Click **Next**.

On the subsequent panel there is the option to encrypt the shared folder. This provides a higher level of security by encrypting the contents of the folder; in the event that the hard disks were removed from the TNAS and loaded onto another computer system, it would not be possible to read the contents of the folder unless the other party had a copy of the encryption key. If you are storing confidential information you may wish to encrypt folders but be aware that there is no way to recover the data if the encryption key is lost, and that access to encrypted folders is slightly slower than to normal, unencrypted ones. Because of these considerations, only encrypt folders when you need to do so and not as a matter of course. To create an encrypted folder, tick the **Encrypt this shared folder** box and enter and confirm the encryption key; the key needs to be at least 8 characters in length and you should use something obscure, such as a mixture of random letters and numerals. You may wish to make a note of the encryption key and keep it in a safe place.

Optionally, you can enable the recycle bin for the folder, which will allow you to recover files that have been deleted, whether intentionally or by accident. To do so, tick the **Enable Recycle Bin** box and choose how long the deleted files will be retained for possible recovery.

Having made your choices, click **Next**:

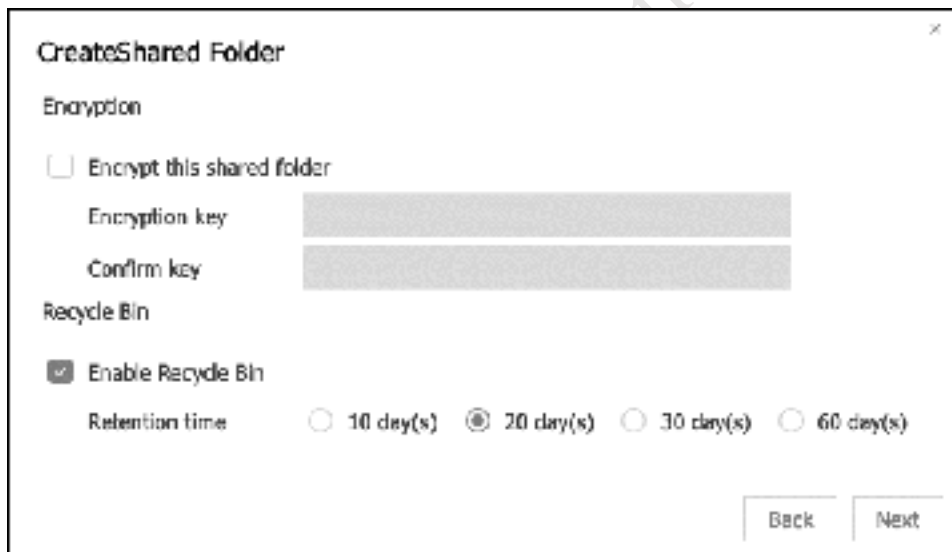
The image shows a screenshot of a Windows dialog box titled "Create Shared Folder". The dialog is divided into two sections: "Encryption" and "Recycle Bin". In the "Encryption" section, the checkbox "Encrypt this shared folder" is unchecked. Below it are two text input fields labeled "Encryption key" and "Confirm key", both of which are currently empty. In the "Recycle Bin" section, the checkbox "Enable Recycle Bin" is checked. Below this, there are four radio button options for "Retention time": "10 day(s)", "20 day(s)", "30 day(s)", and "60 day(s)". The "20 day(s)" option is selected. At the bottom right of the dialog, there are two buttons: "Back" and "Next".

Figure 26: Encryption and Recycle Bin options

The next panel defines permissions for the users, meaning who has access to the folder and the nature of that access. This is something of a chicken-and-egg situation, as we have yet to create any users and you may therefore want to refer to section [4 USERS](#) to gain a fuller understanding. There are four options:

Full access – everyone can do anything with the folder

By user – the folder is available to a specific user or number of users

By user group – the folder is available to a pre-defined group of users (user groups are discussed later)

Administrator – the admin user can do anything, whereas other users can see but not change the folder

In this instance we want to restrict access to a specific user, so choose the **By user** option and click **Next**:

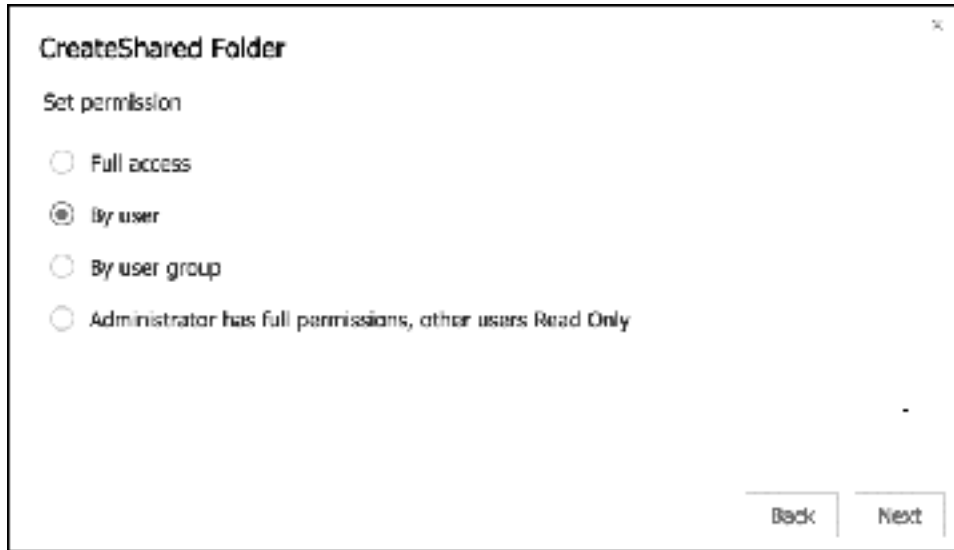


Figure 27: Set permission

The subsequent panel is for defining the type of access and there are three types of access: *Read/Write* (do anything); *Read only* (access it, but no changes allowed); *Deny*, meaning no access at all. Give *admin* **Read/Write** access and set *guest* to **Deny** (*guest* is an unsecured user on most computer systems and should not be used). Click **Next**. A panel to confirm the settings is shown, click **Create** and the folder will be created and listed on the main Shared Folder screen.



Figure 28: User permission

There are some circumstances in which the User permission panel is not displayed. If you choose the *Full access* option on the previous panel, then it becomes redundant, likewise if you choose the *Administrator has full permissions, other users Read Only* option. You may have realised that we could have done the latter in this particular example, although we did otherwise to illustrate some wider principles of creating folders.

The next panel enables a quota (maximum size) to be specified for the folder. As disk space is cheap and plentiful this is not commonly done, but can be a useful feature in, for instance, educational institutions to discourage students from storing large amounts of videos and downloads. Make a decision and click **Next**.

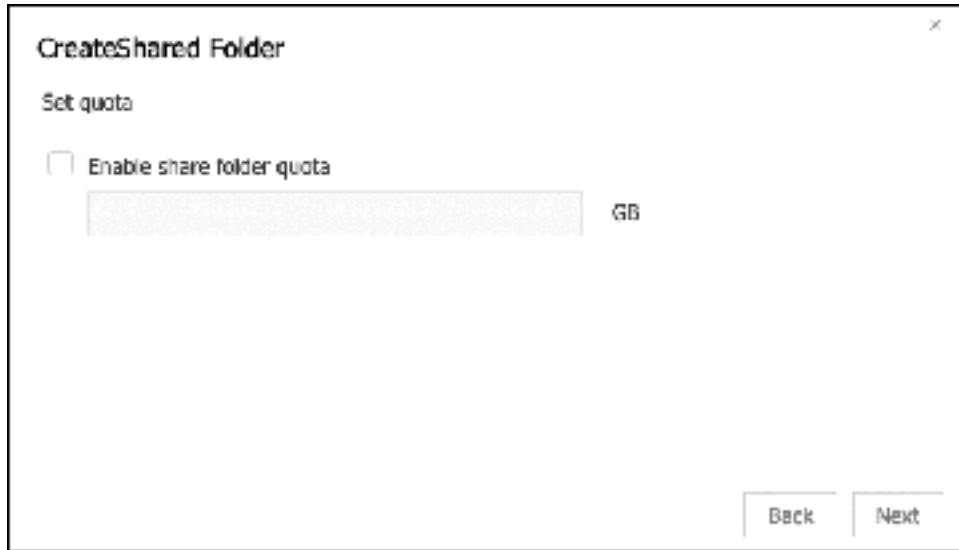


Figure 29: Storage Quota

The final panel is to confirm the settings for the new shared folder. Click **Create**, and the folder will be created and added to the list of shared folders. It is now available for use.

Free edition. Do not copy or distribute. TACS

3.3 Changing or Deleting a Shared Folder

Should it ever be necessary to change a shared folder, for instance to rename it or change the access permissions, this has to be done from the **Shared Folder** option in **Control Panel**; specifically, it cannot be done from *File Manager*, which is a common error that catches some people out. Place a tick against the folder and click the **Edit** button; alternatively, just double-click the folder. Having made the changes, click the **Confirm** button.

To delete a shared folder, place a tick against it and click **Delete**; there will be a warning message that has to be acknowledged to proceed.

3.4 Home Folders

Most folders on a server are shared folders, potentially for the use of everyone on the network. It is also useful to have *home folders* for each user where they can store things that nobody else needs access to, analogous to the 'Documents' folder that people have on their individual computers. To enable home folders, go to **Control Panel > User** and on the **User** tab click **More > Advanced settings**. Tick the **Enable user home directory** box, followed by **Apply**. Thereafter, when a new user is created a home folder is created for them automatically. The name of the home folder is the same as the username e.g. a user called *louiseb* would have a home folder called *louiseb* (creating users is described in [4 USERS](#)).

A user's home folder is private to them and cannot be seen by other users, with the exception that the *admin* user also has access because of administrative and support requirements. The home folders are located within a folder called *User* at the top (root) of the main storage volume and can be accessed by *admin* using File Manager:

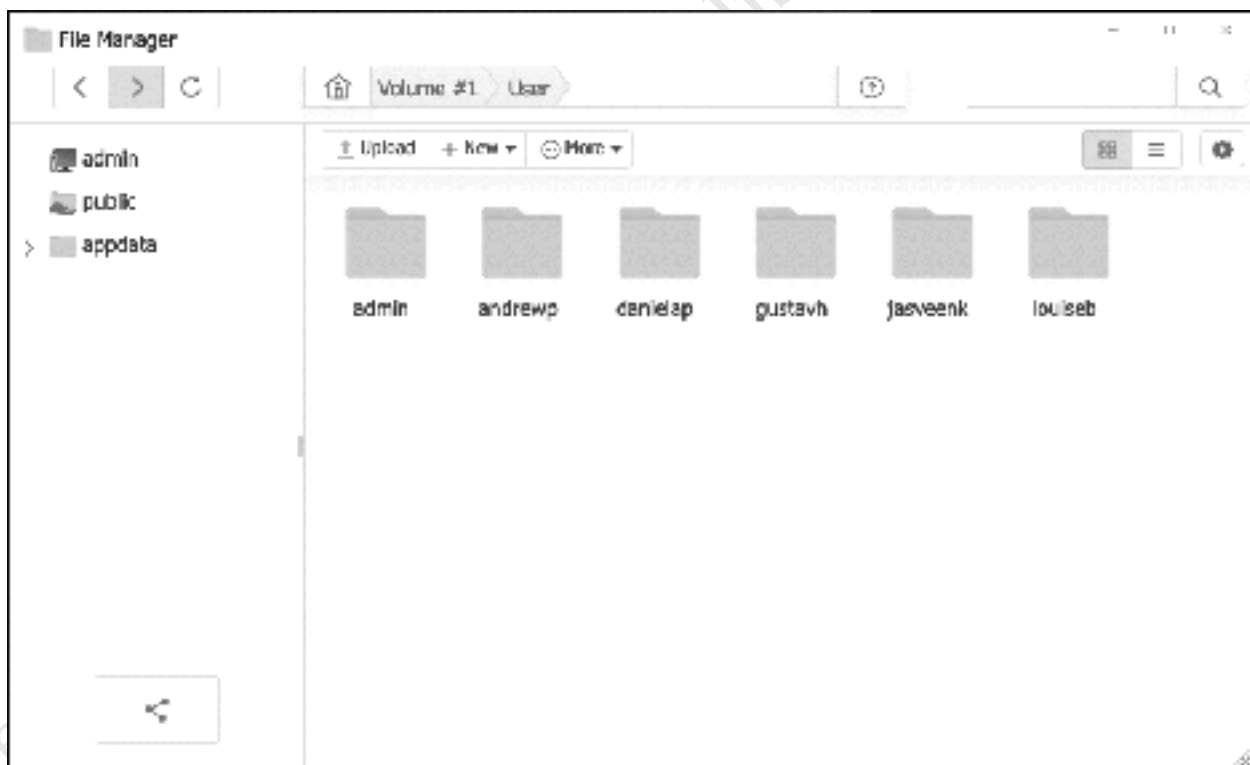


Figure 30: Location of Home folders

3.5 Loading Existing Data into Shared Folders

There may be a requirement to load data from existing computers or systems into the new shared folders that have been created on the NAS and 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 drive to the server and copy the data to the appropriate folders on the server. The advantages of this method are that it can be started before or in parallel with setting up the server, plus it can be retained as a long-term archive.

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

Free edition. Do not copy or distribute. (C) 2005

4

USERS



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

4.1 Overview

In order to use the TNAS, it is necessary to have a *user account* on it. During the installation of TOS an initial user was created – *admin*. If you are the only person who will ever use the TNAS, you can work with that user account for everything and skip this chapter altogether. However, if other people will also be using the TNAS, which is usually the case in a home, business or education environment, then you will need to create user accounts for them.

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 just about anything you want, although it is sensible to follow a scheme. For instance, you could use the first names of the family or household members.

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

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

Free edition. Do not copy or distribute.

4.2 Creating Users

To create a user, go into **Control Panel** and click the **User** icon, followed by **Create**. Enter the Username, an optional Description, plus a password and its confirmation. Passwords have to contain at least eight characters, should be non-obvious and comprise a mixture of upper- and lower-case letters, mixed with numbers and symbols and TOS will not let you proceed if the password is unsuitable (to change these requirements, see [6.8 Password Settings](#)). Tip: click the small eye logo to see the password whilst you are typing it. SSH (Secure Shell) access is an optional feature, not commonly used and should not be enabled. Having completed the form, click **Next**.

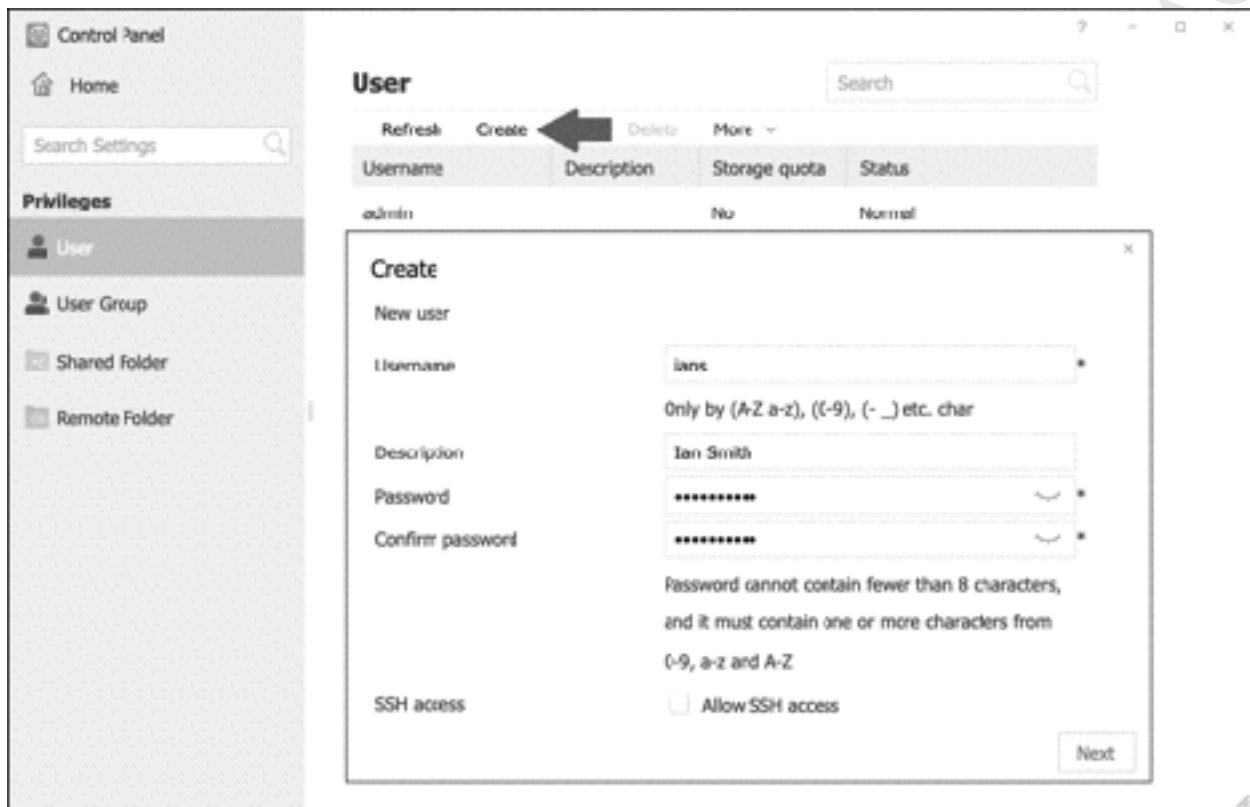


Figure 31: Creating a User

The follow-on screen is for setting a storage quota i.e. how much disk space in Gigabytes (GB) the user is permitted. However, it only applies to storage volumes which have been formatted using the *EXT4* filing system and with Btrfs volumes cannot be set anyway. As disk space is cheap and plentiful this is not commonly done in a home or small business setting, although may be useful in an educational setting, so you may wish to ignore this step by clicking **Next**.

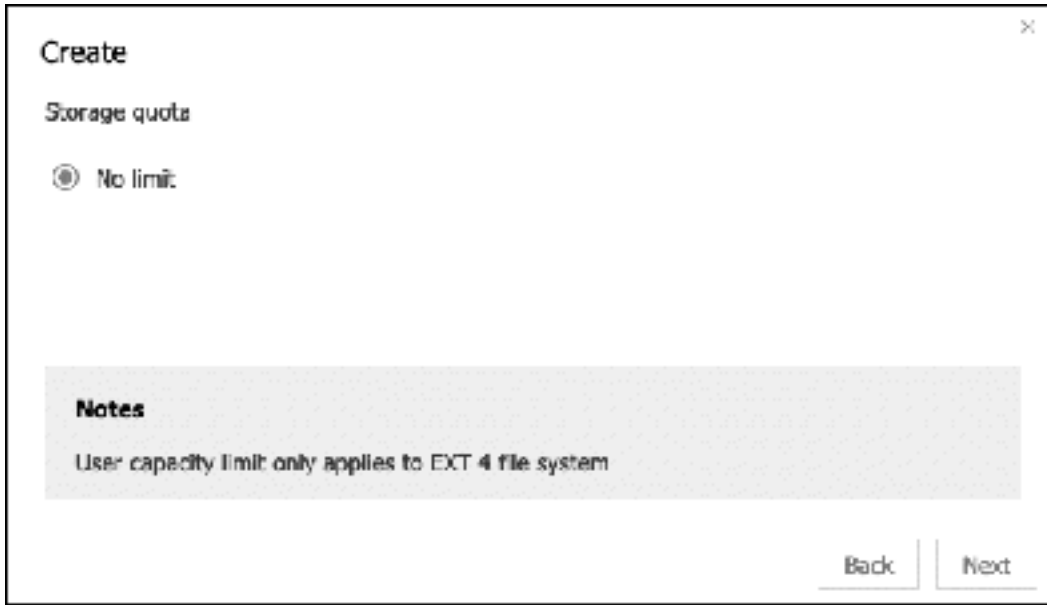


Figure 32: Storage quota

On the next panel, you can specify which group(s) the user is to be a member of. Groups are described in section [4.5 User Groups](#); for now, note that users are automatically a member of a built-in one called *allusers*. You should not make users members of the *admin* group, which should only be used selectively due to the additional capabilities it has. Click **Next**:

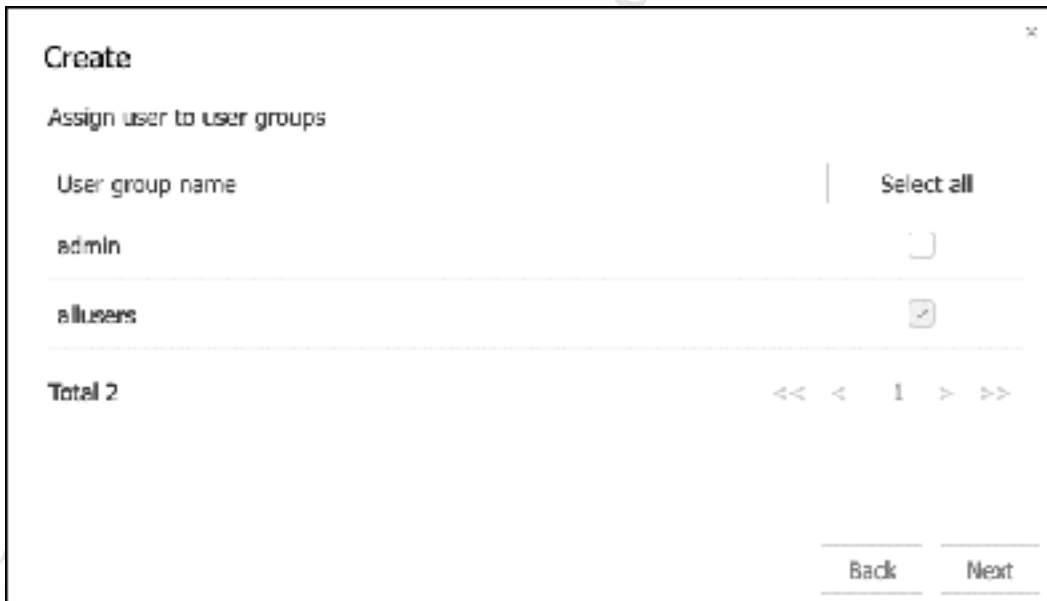


Figure 33: Joining a Group

The following panel defines which shared folders the user has access to and will have been seen previously whilst setting up shared folders in section [3 SHARED FOLDERS](#). Give the user **Read/Write** permissions to the *public* folder and ignore the other ones (although you could set *technical* to 'Deny'). Click **Next**:



Figure 34: Assigning shared folder permissions

A *Confirm Settings* screen is displayed - click **Create** to proceed and the user will be created within a few seconds.

This 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 assigned.

To create a user with TNAS Mobile:

Tap **TNAS administrator**, followed by **Privileges > User**. Tap the + (plus) sign in top right-hand corner. Enter the Username, plus a password and its confirmation. Passwords have to contain at least eight characters, should be non-obvious and comprise a mixture of upper- and lower-case letters, mixed with numbers and symbols and TOS will not let you proceed if the password is unsuitable (to change these requirements, see [6.8 Password Settings](#)). Tip: tap the small eye logo to see the password whilst you are typing it.

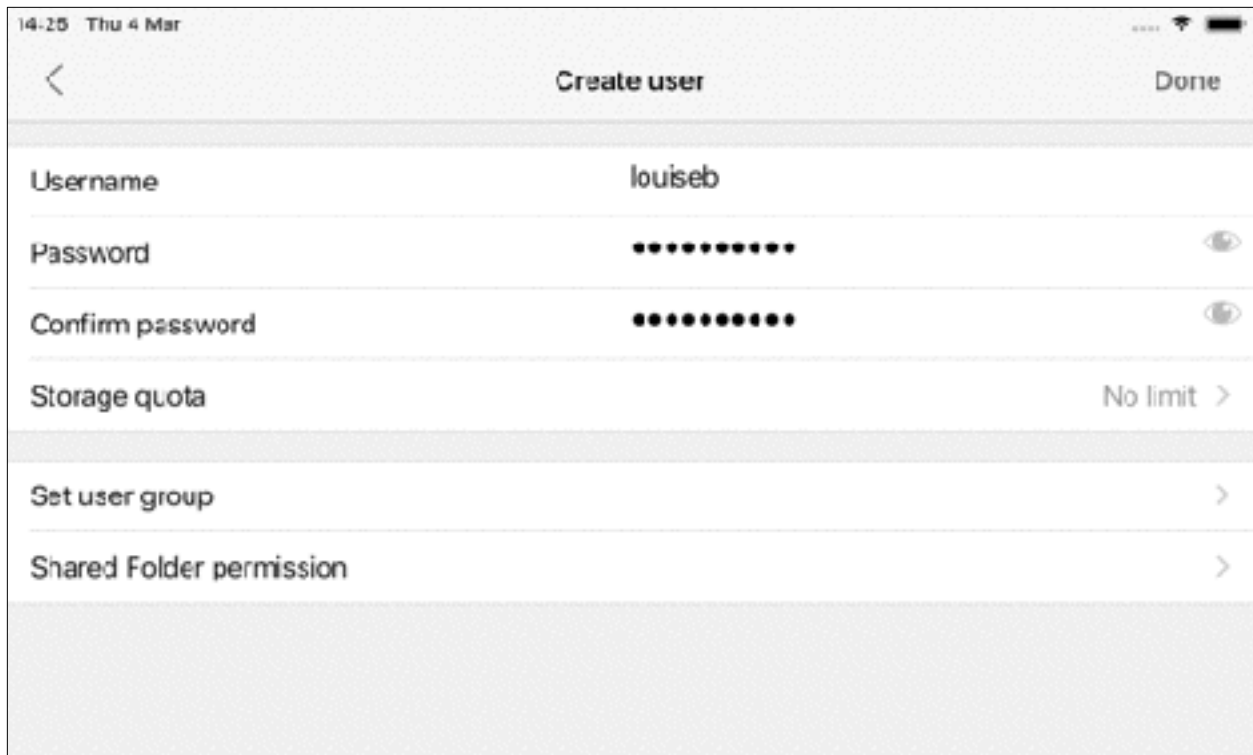


Figure 35: Creating a user with TNAS Mobile (on iPad)

To optionally specify which group(s) the user is to be a member of, tap **Set user group**. Groups are described in section [4.5 User Groups](#); for now, note that users are automatically a member of a built-in one called *allusers*. You should not make users members of the *admin* group, which should only be used selectively due to the additional capabilities it has.

To define which shared folders the user has access to, tap **Shared Folder permission**. On the resultant panel tap the folder and then tap the appropriate permissions. Give the user **Read/Write** permissions to the *public* folder and ignore the other ones (although you could set *technical* to 'Deny').

Work back to the original 'Create user' screen and tap **Done** to create the new user.

4.3 Modifying, Disabling and Deleting Users

To modify an existing user, go to **Control Panel > User**. Highlight the user's name and click **Edit**. This provides access to the information that was specified when the user was created and which can now be modified if required. For instance, the user's password can be changed on the **User** tab or folder permissions can be changed on the **Permission** tab. Having made any changes click **Apply**.

When a user leaves an organization, their account should in the first instance be disabled to prevent it being used. It is preferable to do this rather than immediately delete the account, as there may subsequently be a need to access it or the user may return at a later date e.g. if they are on maternity/paternity or long-term sick leave. To disable an account, edit the user as above but click the **Advanced settings** tab. Tick the **Disable this user account** box and choose **Immediately** or specify an expiry date (the latter is useful in education as it can correspond with the end of the school term or year, for instance). Click **Apply**.

To permanently delete a user, go to **Control Panel > User**. Highlight the user's name and click **Delete**. A warning message is displayed, advising that the user's data will be deleted. Acknowledge it by clicking **OK**.

Free edition. Do not copy or distribute.

4.4 Importing a List of Users

In a domestic or small business setting, creating users one at a time is unlikely to be problematic. But when many need to be created, such as in a larger business or an educational setting, it can be time consuming. Fortunately, TOS has the ability to create users in from a list in Excel spreadsheet format; this list can be created manually, or it might be possible to generate it from another computer system, such as a school registration or human resources application.

The spreadsheet needs to be formatted as follows:

Column A – Username

Column B – Password

Column C – Email address (optional)

Column D – Phone number (optional)

Column E – SSH (set to NO)

Column F – User Group (generally set to *allusers*)

Column G – Storage quota (as required, set to 0 for unlimited if not used, only applicable to Ext4 volumes)

Column H – Read only folders (specify name if applicable)

Column I – Read/Write folders (e.g. *public*)

Column J – Deny (specify name is applicable)

For columns H, I and J it is possible to specify multiple folders. The names should be specified using the ‘|’ character e.g. *public | folder1 | folder2*

	A	B	C	D	E	F	G	H	I	J
1	Username	Password	Email	Phone	SSH	User Group	Storage quota	Read only	Read/Write	Deny
2	danielap	Bulgaria1234			NO	allusers	0		public	
3	stevew	France5678			NO	allusers	0		public	
4	jans	Canada9012			NO	allusers	0		public	
5	jasveenk	India3456			NO	allusers	0		public	
6	gustavh	Germany7890			NO	allusers	0		public	
7	maryo	Ireland1234			NO	allusers	0		public	
8	andrewp	America5678			NO	allusers	0		public	

Figure 36: Example spreadsheet format for creating users

Save the spreadsheet in regular Excel format (XLSX).

To import the list, go to **Control Panel > User** and click **More > Import**. Browse to where the file is located and select it. Click **Confirm** within TOS, then again on the ‘Confirm settings’ panel.

Similarly, it is possible to generate an Excel file containing a list of users from TOS. Go to **Control Panel > User**. Highlight the user(s) and click **More > Export**.

4.5 User Groups

In an organization with a relatively small number of users, specifying who has rights to shared folders is fairly easy to manage. But as the number of users increases it naturally becomes more time consuming; for instance, consider having to define the access rights for, say, 30 people or even 300 people. Such organizations are usually large enough that they contain departments or teams to carry out the different functions; for example, there might be several people working in accounts, several in sales, several in marketing and so on, whereas in an educational institution there might be classes or consorts.

To support these typical structures, TOS features the concept of *groups*. A group consists of a number of users who have something in common within the organization, such as they are all members of the same team. Access rights can be specified for the group, which means they then apply to all members of that group. If a new person joins the team they can be defined as a member of the group, at which point they inherit all the relevant access rights. As we have already seen, there is a built-in group in TOS called *allusers* and which all users are automatically members of, but you can create additional ones to reflect the specific needs of the organization.

In this example, we will create a group called *sales* whose members alone have access to a corresponding folder of the same name (although it does not need to have the same name – we are just doing this for convenience).

Launch the **Control Panel** and click the **User Group** icon. On the User Group screen click **Create**. Name the group *sales* and make sure the *Add users now* option is set to **Yes**. Click **Next**:

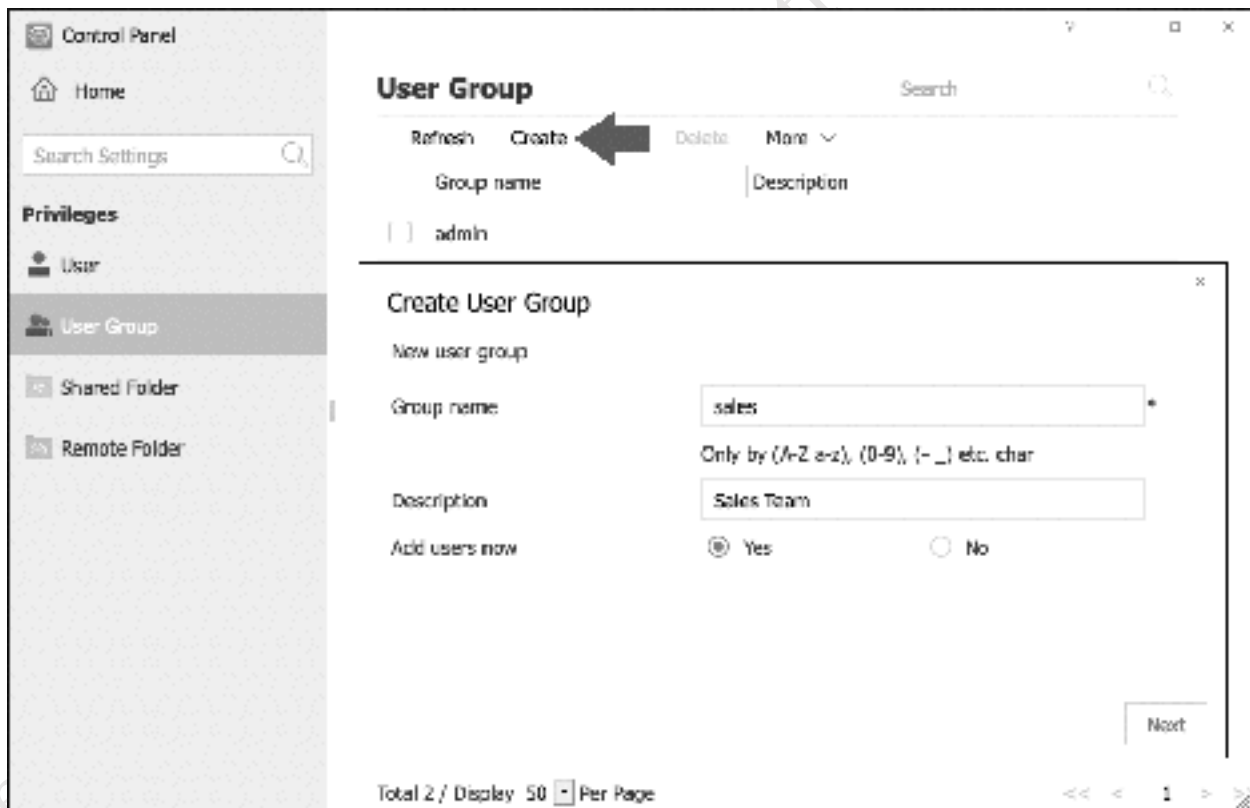


Figure 37: Create User Group – initial screen

On the second screen, place ticks against the names of users who will be members of the group (depending on how many users there are, they may be on multiple pages). When complete, click **Next** and on the third, *Confirm settings* screen, click **Create**:



Figure 38: Selecting users for a group

Next, create a shared folder for the group. The method for creating shared folders is detailed in [3.2 Creating Shared Folders](#), but in summary: **Control Panel > Shared Folder > Create**. Name the folder *sales*, tick the **Hide** option and click **Next**:



Figure 39: Create a folder for the group

On the next panel, there are the usual options to encrypt the shared folder plus enable the recycle bin and specify the retention time for deleted files. Having made your choices, click **Next**. On the subsequent screens, set the permission **By user group** and give the *sales* group **Read/Write** permissions (it is

sensible to also give access to *admin*). Click **Next**. The subsequent screen allows a storage quota to be specified is required. Click **Create** on the *Confirm settings* panel.

The screenshot shows a window titled "CreateShared Folder" with a close button (X) in the top right corner. On the left side, under "Set permission", there are four radio button options: "Full access", "By user", "By user group" (which is selected), and "Administrator has".

The main area is titled "CreateShared Folder" and contains a table for "Group permission". The table has three columns: "Group name", "Read only", "Read/Write", and "Deny".

Group name	Read only	Read/Write	Deny
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
allusers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
sales	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Below the table, it says "Total 3". At the bottom right of the table area, there are navigation arrows: "<< < 1 > >>". At the very bottom of the window, there are two buttons: "Back" and "Next".

Figure 40: Assign shared folder permissions

The benefit of this is that the creation of additional users or changes to existing users becomes easier. For instance, when a user is created they just have to be specified as being a member of a particular group to automatically inherit all the rights associated with that group. The larger and more structured the organization, the more benefits accrue from this approach.

You may have noticed that there were already some groups in existence: *admin* and *allusers*, of which the latter has already been referenced. These are special built-in groups created by TOS and should not be modified in any way.

5

ACCESSING THE SERVER



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

5.1 Overview

There are multiple methods for accessing the TNAS, some of which are specific to Windows only, some to Mac only, whereas some work for most platforms. There is also an app available for portable devices such as smartphones and tablets.

5.2 Using a Browser and File Manager

This is a universal method for accessing the TNAS and works for Windows PCs, Macs, Linux computers and Chromebooks. Using any computer on the local network, launch a browser such as Firefox, Internet Explorer, Chrome or Safari and type in the name or IP address of the server e.g. *server*, *192.168.1.2* etc. The standard TOS login screen is displayed; the user should enter their name and password and they will be presented with a fairly minimalist Desktop; in essence, all they can access is File Manager and which can be launched by double-clicking on its icon, which appears on the Desktop. Within File Manager they can see the folders and files that belong to them or to which they have been granted access, such as their home folder and any shared folders.

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

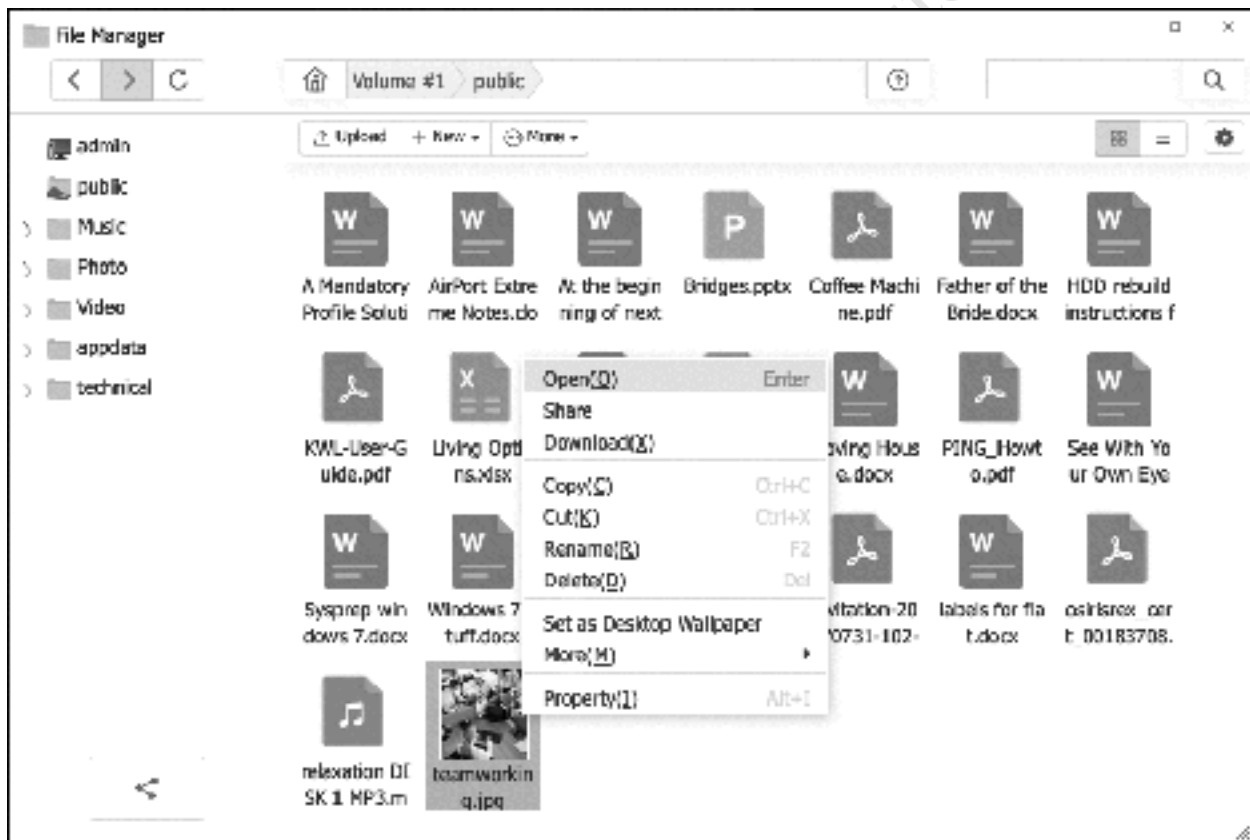


Figure 41: Using File Manager

In the above screenshot, notice that the files have icons to identify their type e.g. Word, Excel, JPG, PDF and so on. File Manager has built-in viewers for some common graphics formats, plus PDFs can be opened if PDF Reader has been installed (see [11.8 PDF Reader](#)). However, TOS does not have the ability to preview Microsoft Office documents. To edit a file, right-click it and choose the **Download** option to first download it to the local computer; make the changes to the document using Word, Excel or other preferred application; use the **Upload** button in File Manager to upload the new version back to the server.

The user can create their own personal folders on the Desktop, which is done by right-clicking it and choosing **New Folder** from the pop-up menu. Files can be uploaded to these folders using File Manager or copied/moved from other areas on the NAS that the user has access to.

When the user has finished with accessing the TNAS, they should logout by clicking on their username in the top right-hand corner and choosing **Logout**:

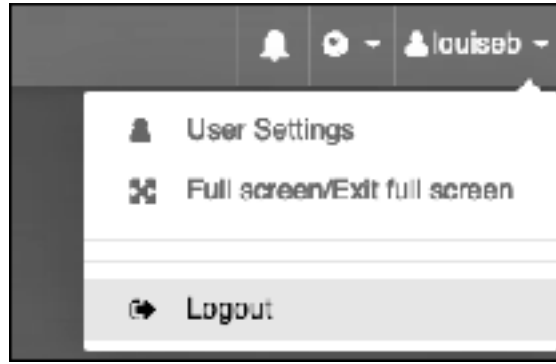


Figure 42: Logout option

External Access

If you have configured remote access as described in section [2.7 Setup Remote Access](#), you can also access the server from outside the premises, over the internet. The only difference is that instead of entering the local IP address or name of the server, you enter the TNAS ID e.g. <http://TNAS.online/CTACS> or whatever your ID is. After a few seconds, you should be greeted with the standard TOS logon screen. Having logged on, it is exactly the same as if you were connected locally, as described above.

Suggestion

When launching File Explorer, a panel showing some tips is displayed. To stop seeing this on every occasion, tick the **Don't prompt me again** box and click **Confirm**:

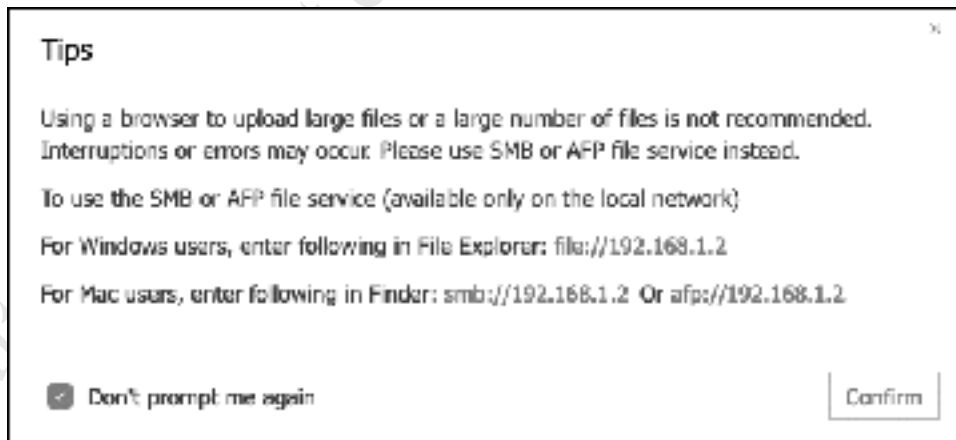


Figure 43: Message about Tips

5.3 Connecting Windows Computers

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 it and the list of shared folders will be displayed. You may be prompted to enter a username and password as defined previously 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.



Figure 44: List of folders from File Explorer/Windows Explorer

To access a shared folder, double-click it. Although a number of shared folders may be visible, you can only access the ones to which you have privileges.

Note: the point at which you are prompted to enter the username and password may vary, depending on which version of Windows is being used.

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 10, Windows 8.1) or click **Start** 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\public` and click **OK**. You may be prompted to enter the username and password, as defined previously on the server:

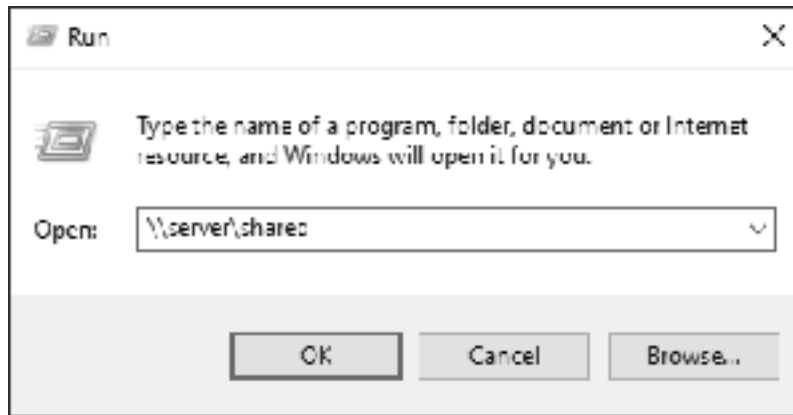


Figure 45: Accessing a shared folder

The contents of the folder will be displayed in Windows Explorer/File Explorer, from where the files can be used in the standard way. Note that you may be prompted to enter a user name and password as defined previously on the server.

Mapping Drives Manually

The techniques described so far provide access to shared folders from Windows computers by referring to them using what are called UNC or *Universal Naming Convention* names and which take the form `\server\shared_folder_name`. 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.

Network drives can be mapped manually using Windows Explorer/File Explorer on the user's PC. The first stage of the process is slightly different, depending on the version of Windows, so check the relevant version below then jump to the common 'Map Network Drive' section underneath.

Windows 10

Open File Explorer, which usually 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. 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 on the shared folder to highlight it. On the menu bar click **Home** and in the *New* section click the small icon and choose **Map as drive**:

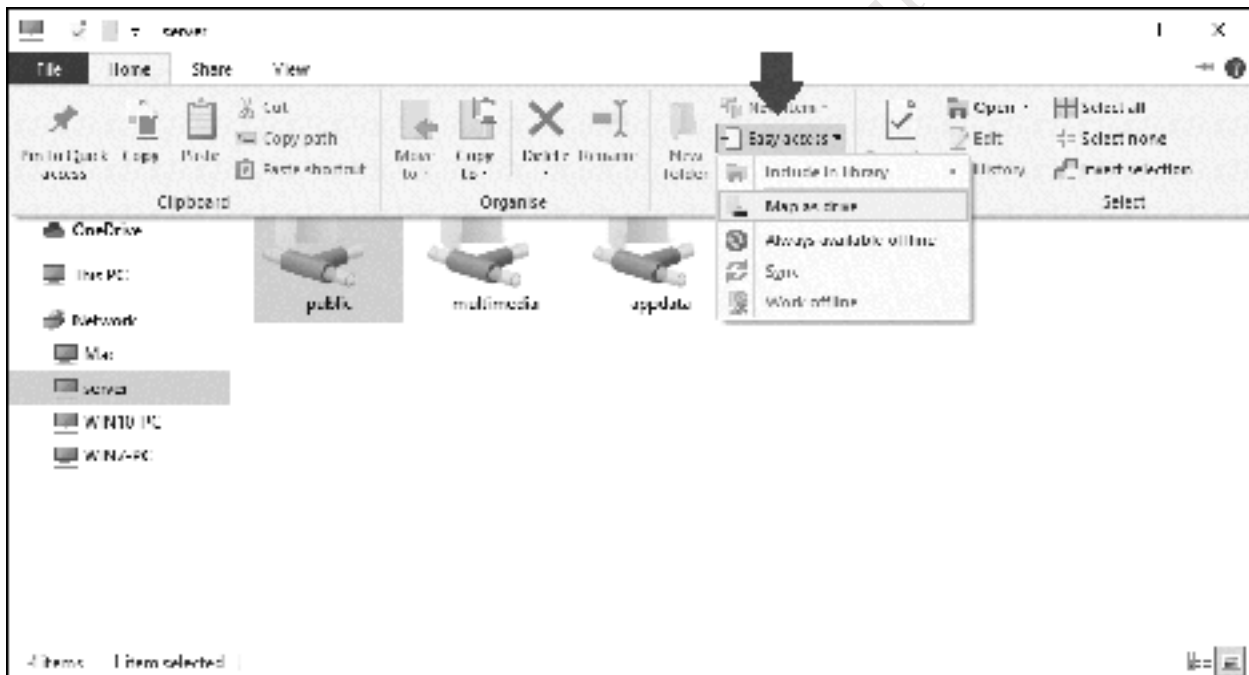


Figure 46: Mapping a drive in Windows 10

Windows 8.1

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

Windows 7

If using 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. From the Menu bar choose **Tools** > **Map Network Drive**.

Windows Vista

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

Windows XP

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

Map Network Drive

On the resultant panel choose a drive letter from the drop-down. For the Folder, click on the **Browse** button and navigate through the network to find the server and the desired folder. Alternatively, just type in the name of the folder. If the computer is only ever used by one person tick the **Reconnect at sign-in** box, which will cause Windows to remember the mapping. Then click **Finish**. You may be prompted to enter the user's name and password that were defined earlier on the NAS. Again, if the computer is used just by one person tick the **Remember my credentials** box. Then click **OK**.

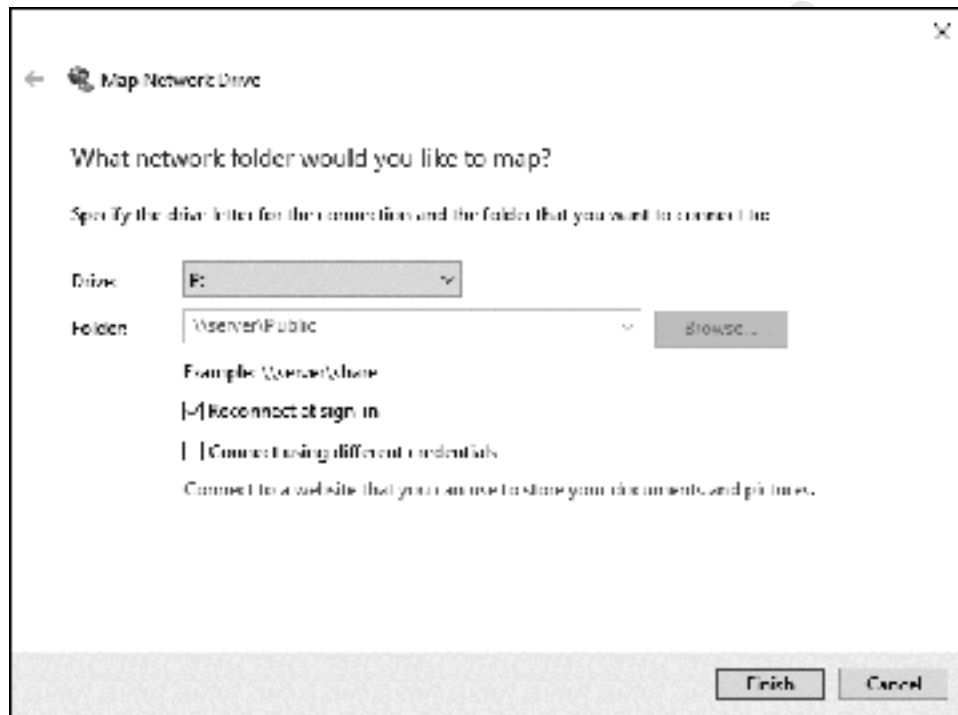


Figure 47: Mapping a drive

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.

You can use whatever drive letters you wish, as long as they are not already in use (for instance you cannot specify C as that is always in use on a Windows computer). However, using sensible letters makes things easier. For example, map *public* to P. Also, the user's home folder can be mapped to H.

Drive	Folder
P	\\server\public
H	\\server\username

Using TNAS PC Windows Utility

The TNAS PC utility is used when initially setting up a TNAS, as described in section [2 INSTALLATION OF TOS](#), but it is a flexible piece of software that can do several other things as well, one of which is mapping drives. One possible advantage of using it is consistency; when drives are mapped manually in Windows as described in the previous section, there are small variations in the process depending on what version of Windows is being used. However, when using the TNAS PC utility it is the same process regardless of the Windows version.

Download and install TNAS PC on the computer. If you receive a message from the computer's firewall, grant access to TNAS PC. An icon will be placed on the computer's desktop – double-click it to run it. The server should be listed, although utility may take a few seconds to find it. If it does not appear, click the **Refresh** button; if it still does not appear then there is a problem of some sort, such as: computer not connected to network; TNAS not powered on; firewall needs configuring on computer. Highlight the server and click the **Map Drive** button. When prompted, enter the logon details for the user and click **OK**:



Figure 48: Enter user name and password

On the subsequent screen, choose a drive letter for the folder from the drop-down and choose a shared folder from its dropdown. Click **Confirm**.

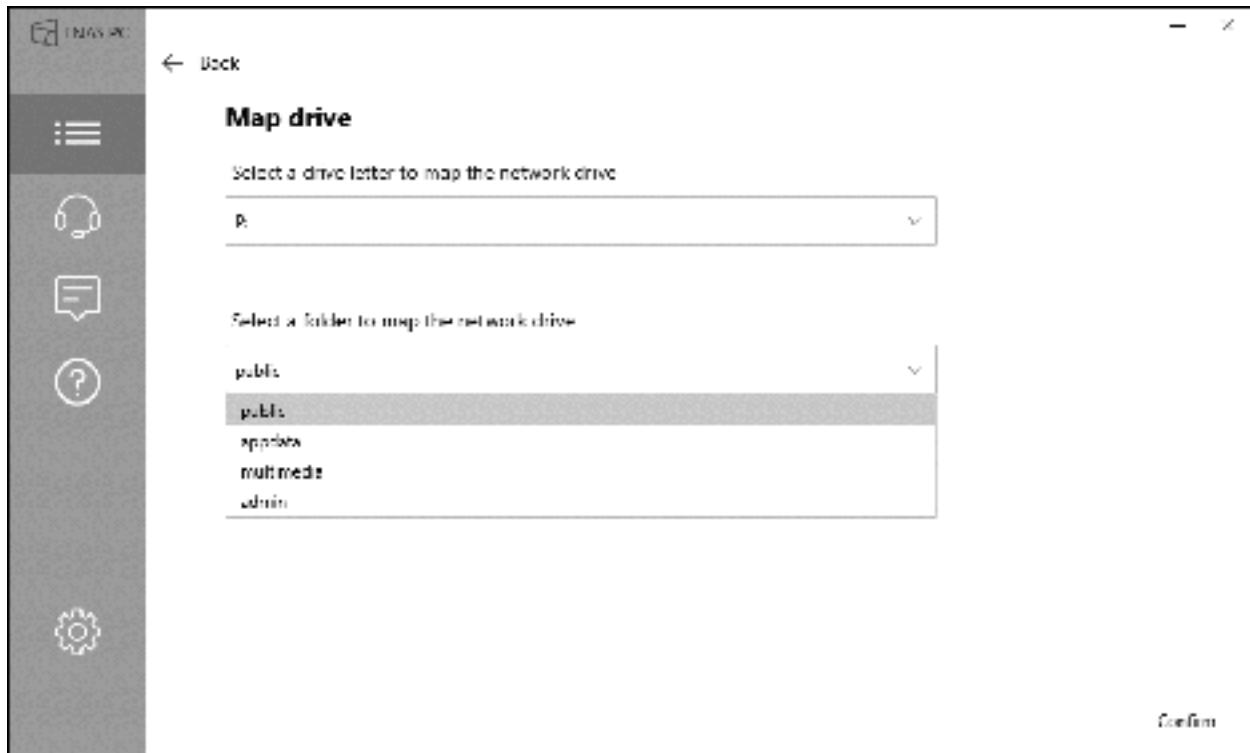


Figure 49: Mapping a network drive

You may receive an additional logon prompt from Windows, in which case enter the login details, tick the **Remember my credentials** box if only one person uses the computer, followed by **OK** and the drive will then be mapped. Repeat the process for as many times as is necessary to provide access to all the desired folders. When complete, open Windows Explorer/File Explorer to verify that the folders have been mapped to drives.

Note that the drive mappings are permanent - assuming any **Reconnect at logon** and **Remember my credentials** boxes were ticked - and hence will survive reboots of the computer. It is not necessary to run TNAS PC again unless it is required to make changes to the mappings.

You can use whatever drive letters you wish, as long as they are not already in use (for instance you cannot specify C as that is always in use on a Windows computer). However, using sensible letters makes things easier. For example, map *public* to P. Also, the user's home folder can be mapped to H.

Drive	Folder
P	\\server\public
H	\\server\username

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 use in a small business environment rather than in a home system. Start off by creating a plain text file called *Connect to TNAS.cmd* using a tool such as Windows WordPad or Notepad. The contents of the file may need to change depending on the folders to be mapped or if the TNAS is not actually called 'server'. In this example each user has a personal home folder and there are two shared folders called *music* and *public*:

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

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

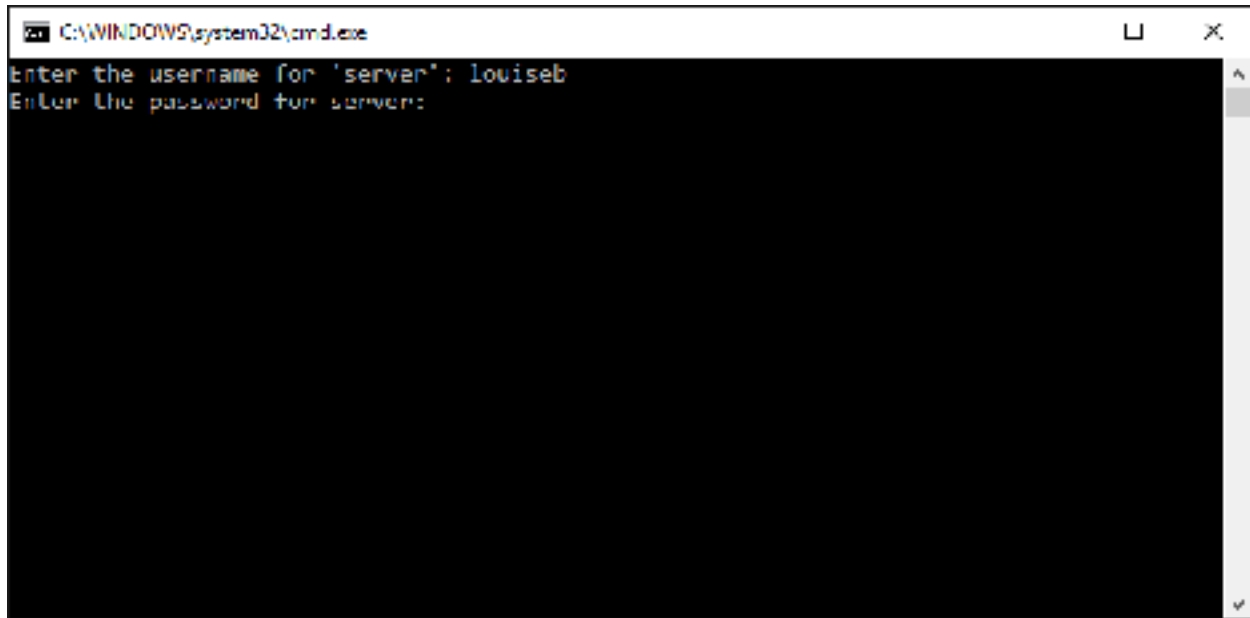


Figure 50: Enter user details

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

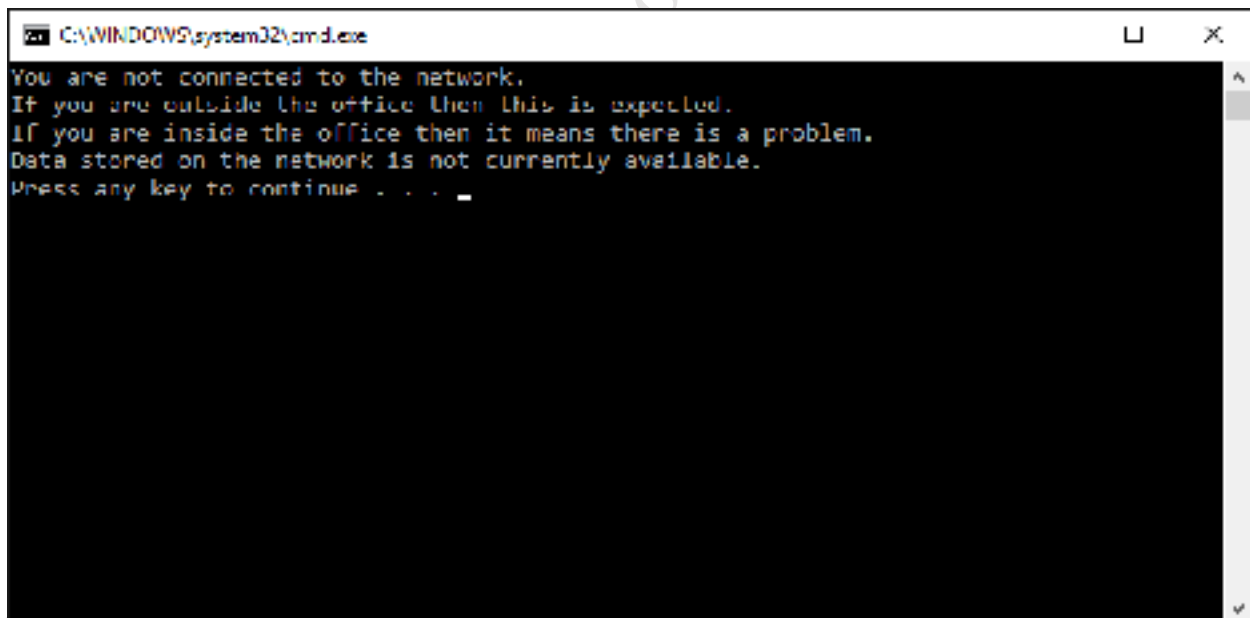


Figure 51: Warning message if not connected

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 TNAS may be powered off or otherwise out of action.

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

Ideally, computers should be setup with only one Windows user defined on them. If this is not the case, then the *Connect to TNAS.cmd* file needs to be placed on the Desktop for each individual user. More efficiently, it can be placed in the following location where it will appear on the Desktop for all users:

Windows XP	C:\Documents and Settings\All Users\Desktop
Windows Vista	C:\Users\Public\Public Desktop
Windows 7	C:\Users\Public\Public Desktop
Windows 8/8.1	C:\Users\Public\Public Desktop
Windows 10	C:\Users\Public\Public Desktop

The Public Desktop folder is a hidden folder on Windows 10, 8, 7 and Vista and will therefore first need to be made visible before it can be accessed. 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**:

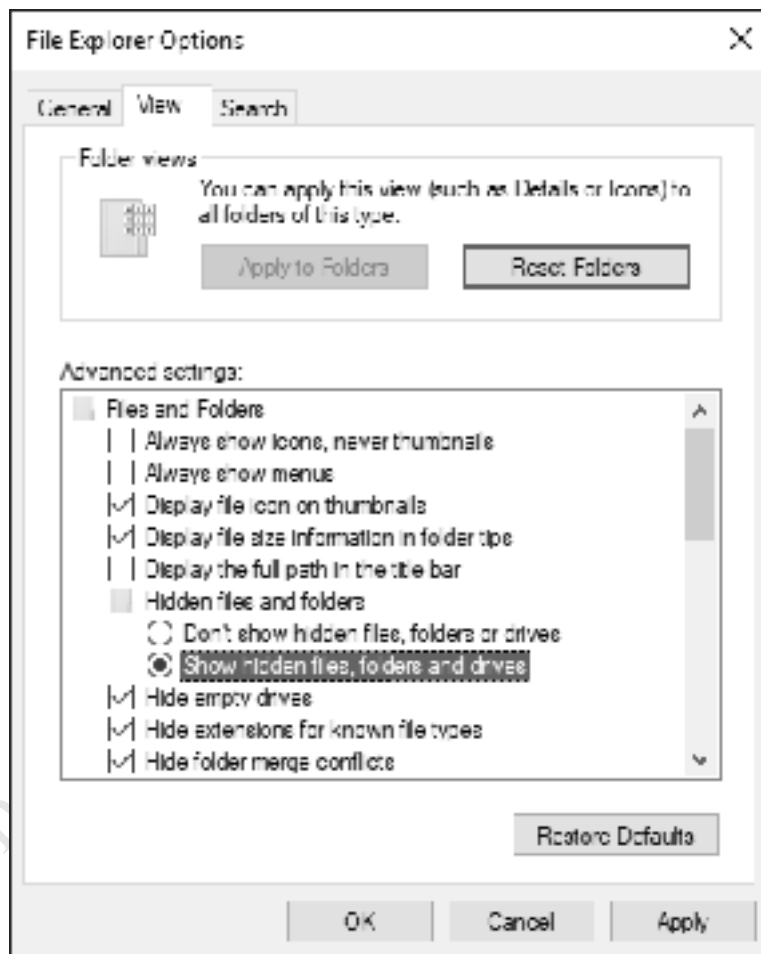


Figure 52: Folder Options to view hidden files

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

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

5.4 Connecting Macs

There are numerous iterations of the Mac operating system and some minor differences between them; however, the following technique should work with all versions. Modern versions of macOS use the same SMB protocol as Windows, but nevertheless it is suggested that AFP (the Mac File Service) is enabled on the TNAS; this is the default on a new TOS installation but can be confirmed by going to **Control Panel > File Service > Mac File Service** (see section [2.6 File Service](#)).

On the menu bar of the Mac, click **Go** followed by **Connect to Server**; alternatively, press **Command K**. A dialog box is displayed. Enter the name or IP address of the server preceded with *smb://* or *afp://* e.g. *smb://192.168.1.2* or *smb://server* or *afp://server*. To add the server to your list of Favorites for future reference click the + button. Click **Connect**. Enter the user name and password as previously defined on the NAS and click **Connect**. You can also tick the **Remember this password in my keychain** box if you are the only person who uses the computer:



Figure 53: Specify server and user logon details

A list of shared folders is displayed, referred to as *volumes* in Apple parlance. Choose the volume to mount and click **OK**. To mount multiple volumes in one go, hold down the **Command** key and click on the required folders in turn. Tip: there is no purpose in mapping the *appdata* folder.

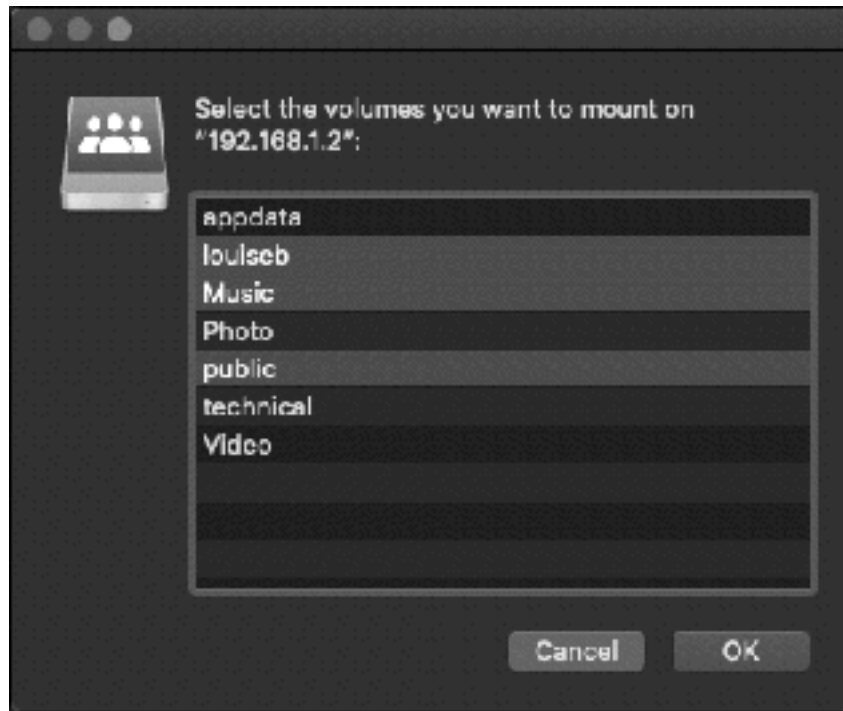


Figure 54: Select the folders to mount

Icon(s) for the folder(s) will appear on the Desktop (assuming you have set Preferences in Finder to show Connected Servers). Click an icon to display the contents - they behave exactly the same as standard Mac folders.

Whilst there is a Mac version of the TNAS PC Mac utility, unlike the Windows version it cannot be used for mapping drives, as the concept does not apply in macOS.

5.5 Connecting Linux Computers

Although TOS includes specific support for the NFS filing system used by Linux and UNIX computers (see [2.6 File Service](#)), most Linux distributions include support for the SMB filing system used by TOS for servicing Windows computers and modern Macs. Unless you have specific reason not to, it is suggested that you use SMB for connecting. The ability to do this is usually inherent, although in some cases it may have to be added by downloading what is commonly described as a *Samba client*. In this example, we are using a popular Ubuntu Linux distribution. In this example, we are using the popular Ubuntu Linux distribution.

On the Linux computer, click on the **Files** icon, followed by **Other Locations**. The NAS 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 55: Enter the address of the server

5.6 Connecting Smartphones and Tablets

TerraMaster provide an app – *TNAS Mobile* – for connecting smartphones and tablets to the TNAS that works both locally and with a remote connection. It provides access to the file system, enables music to be played and photos to be viewed, plus can upload photos from the device to the server. It is available free-of-charge for Android and iOS devices and the two versions are largely identical in appearance and operation.

Download TNAS Mobile from the appropriate app store. If you are installing it whilst connected to the same local network it will detect the TNAS automatically; however, to use it remotely you need to specify your TNAS ID, which you can do by pressing the plus sign (+) on the initial screen and then entering the details, followed by **Confirm**. You may receive a message from iOS or Android requesting permission from the app to access your photos.

Reminder: the TNAS ID was setup in section [2.7 Setup Remote Access](#).



Figure 56: Specify the address of the TNAS

If you receive an error message after entering the TNAS address, this is not necessarily a problem and could be a consequence of being connected to the same local network. To properly test the link, you should be connected to a different network. For instance, with a smartphone you could temporarily disable the wireless connection and use the 5G/4G/3G data link. Enter the name and password of a user who has already been defined on the TNAS and tap **Login**. The login process may take several seconds, after which you will be presented with the Home screen.

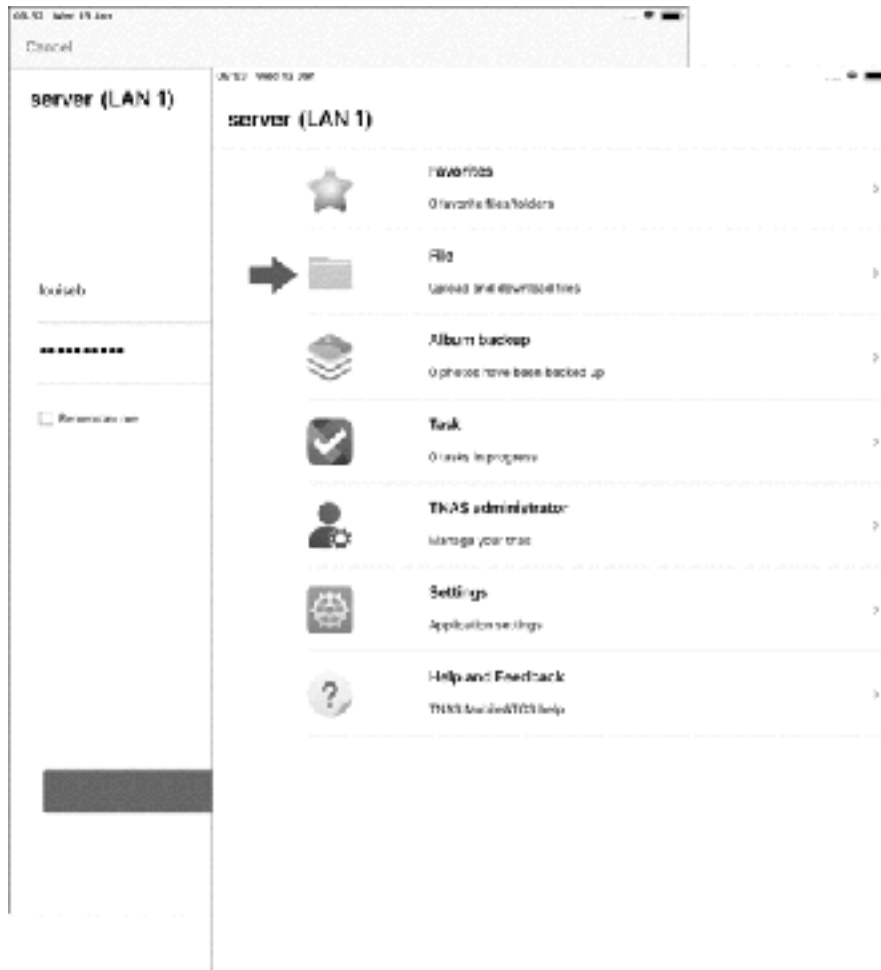


Figure 57: Logging in and Home screen

Tap the **File** option to show the folders on the server, which can be navigated through by tapping on them. TNAS Mobile recognizes many file formats and includes viewers or players for some popular ones. For example, tapping a MP3 file will cause it to play. Files can be sorted by name or time, and new folders can be created.

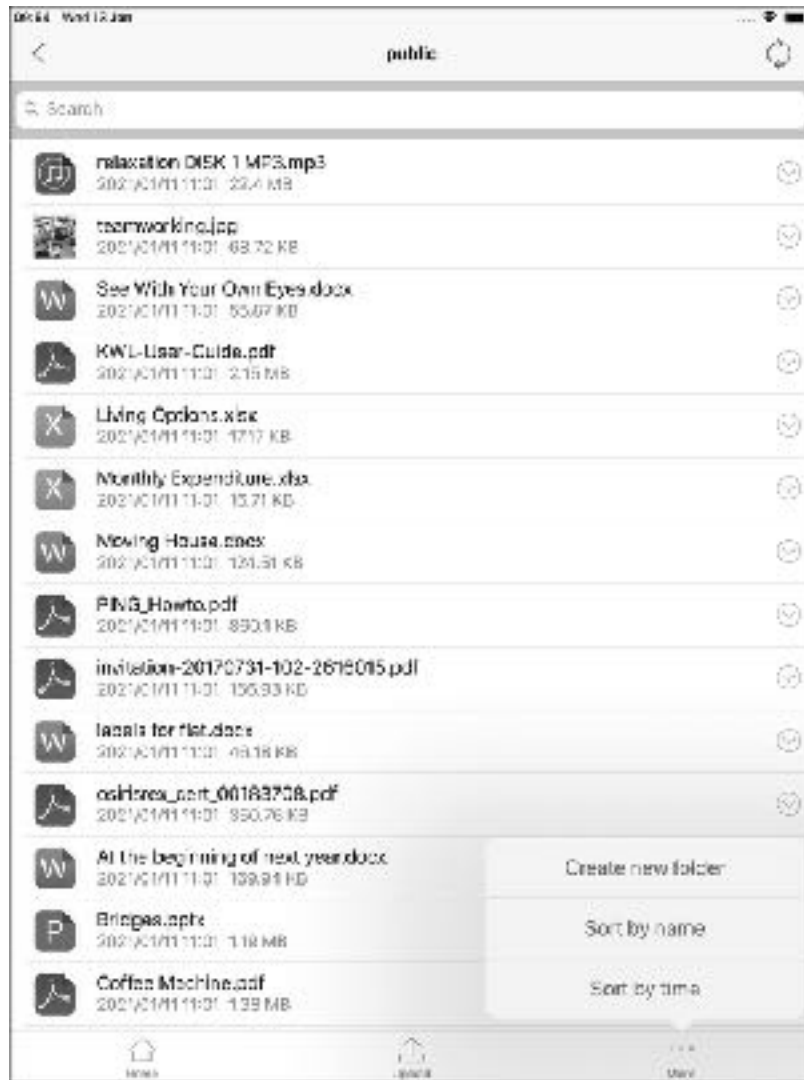


Figure 58: Download and file options

TNAS Mobile can be used to automatically backup photos from a mobile device to the TNAS. To enable this feature, go to the Home screen, tap **Settings** > **Album backup** and slide the switch to the 'On' position. There is a choice of backing up photos, backing up videos, or both.

Uploading photos and videos from a mobile device can significantly eat into your data plan and may incur substantial roaming costs. For this reason, you may prefer that uploads only take place when a Wi-Fi connection is available. To configure this, go to the Home screen, tap **Settings** and set the **Only use Wi-Fi for downloads and uploads** switch to the 'On' position. Also, from Settings, you can clear down any local temporary files (cache) generated by the App, which can be useful if your mobile device has only a limited amount of storage space available.



Figure 59: Settings for downloads and cache

The TNAS Mobile app can be used for managing many aspects of the server, using the TNAS Administrator option from the Home Screen. Some examples are given throughout this manual.

Files App (iOS)

The Files App is an integral part of recent versions of iOS. Having launched it, tap the three-dot menu at the top of the screen and tap **Connect to Server**:

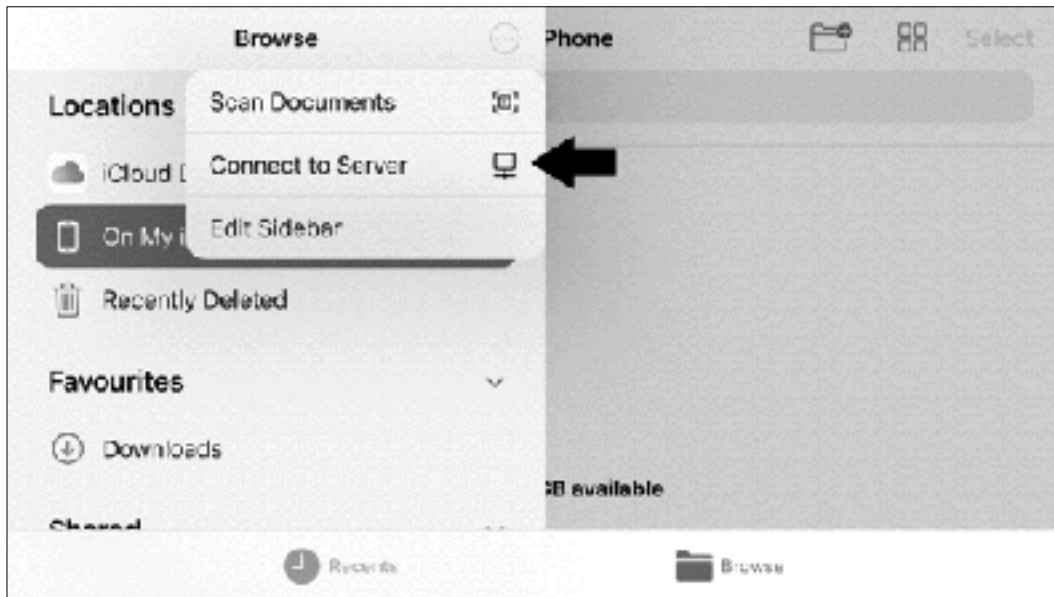


Figure 60: File App on iPhone/iOS

On the subsequent panels: enter the name of the server or its IP address 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:

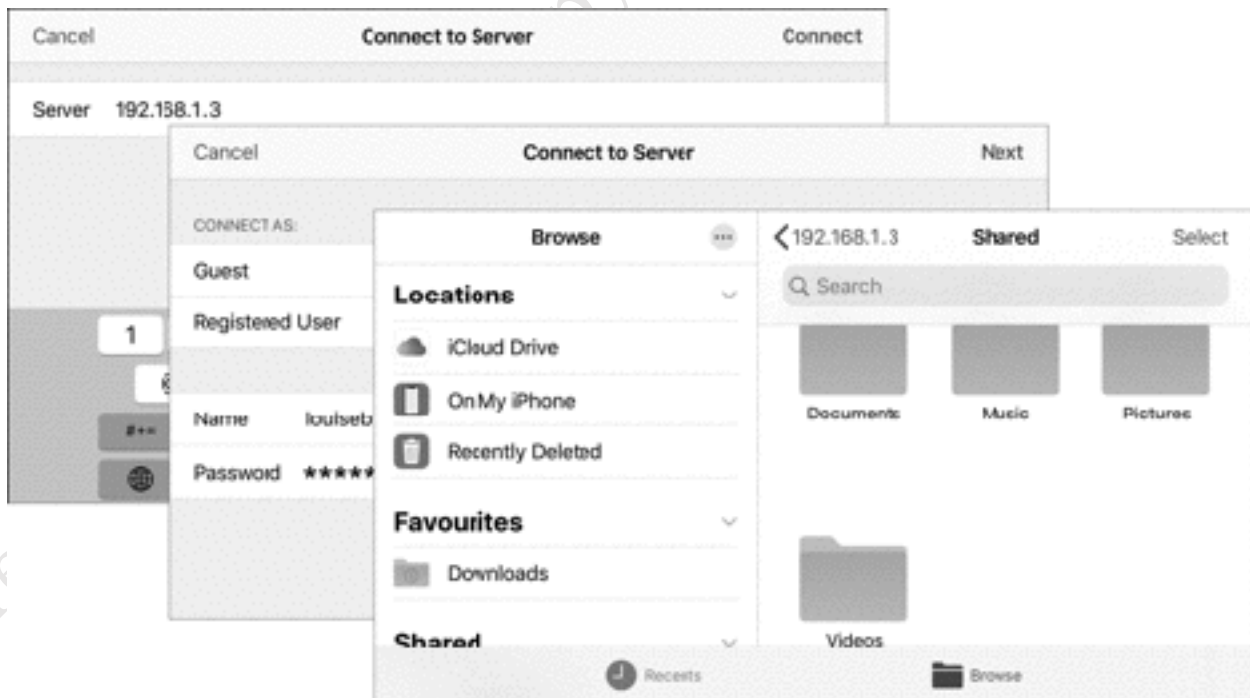


Figure 61: Connecting to and viewing files and folders on the server

5.7 Connecting 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 Windows or macOS. However, Chromebooks work well with NAS and can be used in two ways:

Browser

With the browser, as described earlier in section [5.2 Using a Browser and File Manager](#), for tasks such as working with File Manager, downloading and uploading files and administering TNAS.

Files

To access the folders and files on the NAS, 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\public`, an optional Display name, Username and Password. Optionally, tick the **Remember sign-in info** box. Click **Add**. The shared folder will now be added to the Chromebook's filing system.

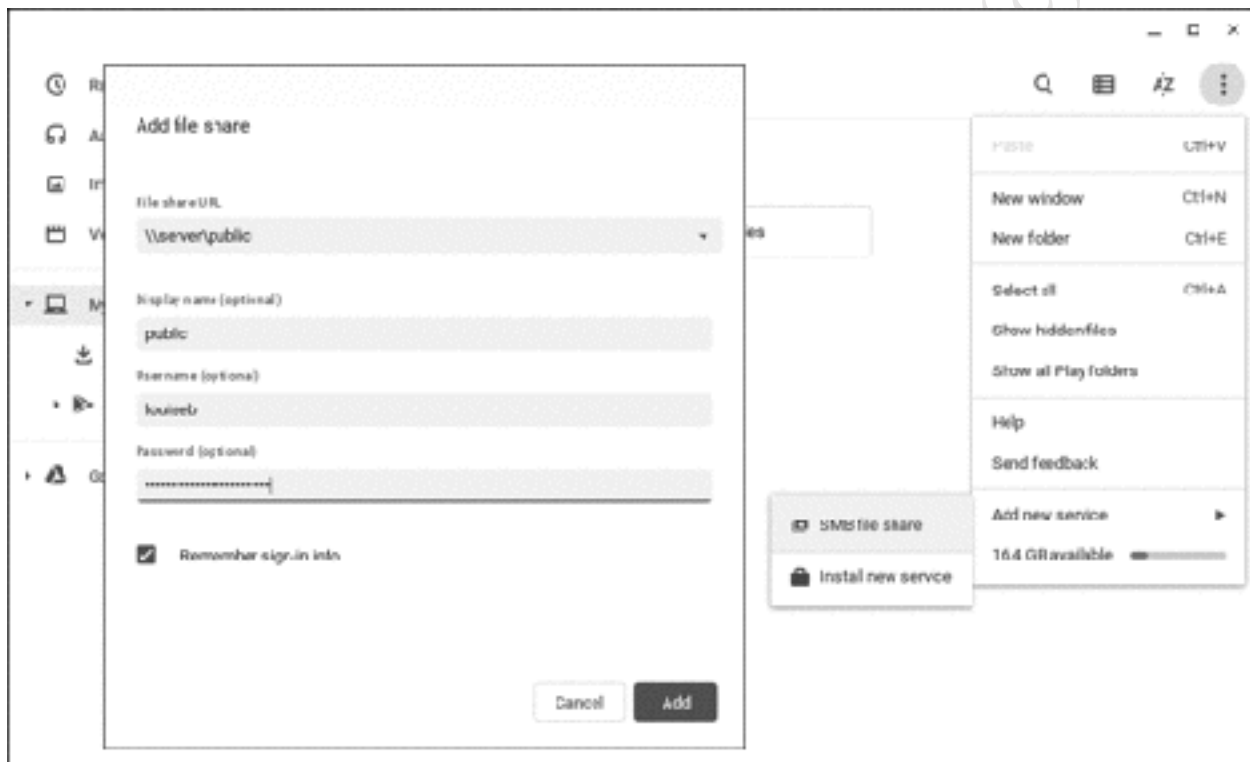


Figure 62: Adding a file share

6

SECURITY



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

6.1 Overview

The TOS software at the heart of the TNAS is a very secure platform, but it is not and cannot be totally immune to the numerous security threats associated with running any sophisticated computer system. To help protect it, TerraMaster provide a variety of tools and mechanisms and it is recommended that you familiarise yourself with and use them. These include an icon in the **Control Panel** called **Security**, which is used to improve security on the TNAS and help protect it against malicious attacks by hackers and other people; a well-regarded anti-virus/anti-malware program; control over several TOS services.

6.2 Clam Antivirus

The chances of a TNAS becoming infected with malware are low as TOS is based on a customized version of Linux and not particularly susceptible, although it is unfortunately possible. However, the files being stored on it by Windows computers and other clients may be infected and these are what need to be checked to prevent further distribution. *Clam Antivirus* is a free download and runs on the TNAS itself. But, note that separate provision still needs to be made for the workstations (e.g. using products such as Microsoft Defender, AVG, McAfee and so on in the case of Windows PCs) as there is no linkage between them and the server, nor is this intended as a replacement for security software on desktops and laptops.

Download and install Clam Antivirus from Applications and send the icon to the desktop. Launching it will display the Overview screen:

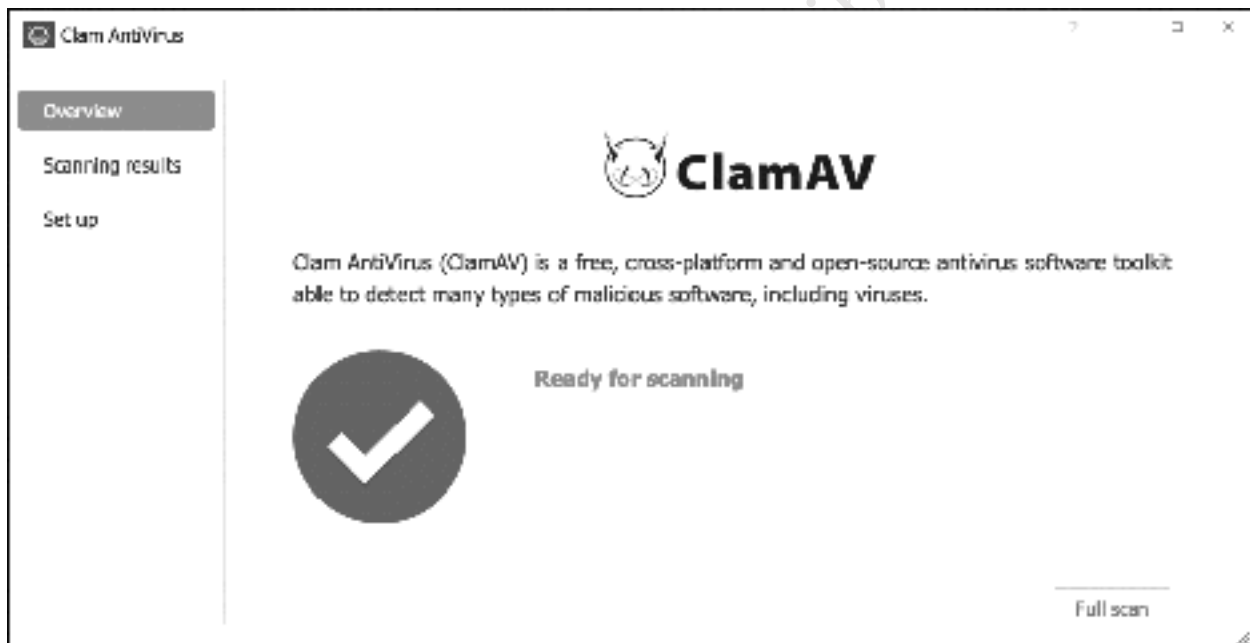


Figure 63: Clam Antivirus Overview screen

Scans can be performed manually as required or can be scheduled to take place automatically on a regular basis. To manually run a scan, click the **Full scan** button on the *Overview* screen.

The virus definitions used by Clam Antivirus are updated automatically and on a regular basis. To check the date of the definitions, click **Set up**. Make sure that the **Enable automatic upgrade function** box is ticked.

Scanning can result in high CPU and memory utilization and, depending on the amount of data stored on the TNAS, may be time consuming. For this reason, it is best done as a scheduled task out of hours, for instance during the middle of the night or at the weekend. Scheduled scans are defined from the **Set up** screen: tick the **Initiate** box; the day(s) for scanning; specify a time using the drop-down box; click **Apply**. In this example, the TNAS is set to do a scan every Sunday morning, starting at midnight:

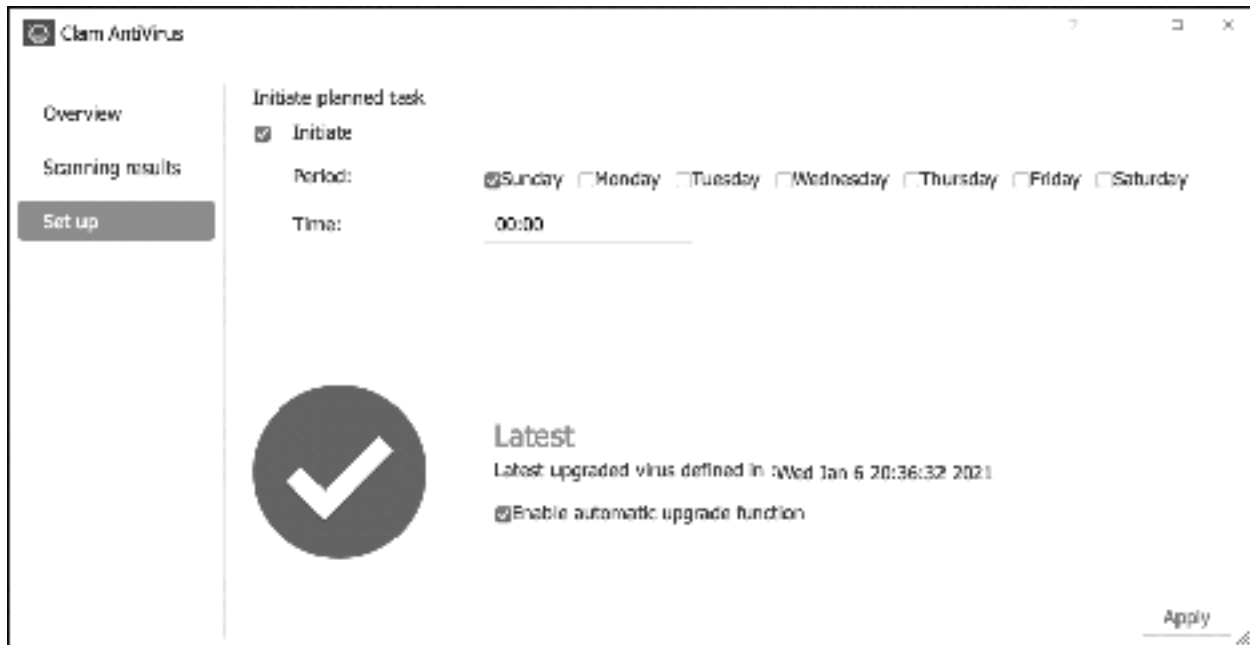


Figure 64: Scheduling a scan

The results of scans and other activities pertaining to the app are recorded in log files. These can be found by clicking on **Scanning results**. If infected files are found on the server:

1. Go to the *Scanning results* section within Clam Antivirus and delete them.
2. Try to identify the source of the infected files (i.e. the computer they came from) and clean-up that computer using anti-virus and malware tools appropriate to the platform.

6.3 SSL Certificate

SSL (Secure Socket Layer) certificates offer higher levels of security when computers are handling encrypted web-based services, which are indicated by website names that begin with *https* rather than *http*. The basic principle is that certificates are provided by recognized issuing authorities – known as *CAs* or *Certificate Authorities* – and constitute a form of guarantee that a site is what it purports to be. Certificates may be provided on a commercial basis but are also available freely from some sources (although there may be restrictions). Certificates can also be self-certified, although these are not so secure.

If you are a home or small business user or just starting out, you may not want to worry too much about this section. If you are an experienced IT professional and/or external access to your network is important and you wish to maximise security, then you may want to take action. This section does not discuss the detailed use of certificates, just how to get started.

Click on **Control Panel** > **Security** > **SSL Certificate** to display the following screen. This shows that the system currently has two certificates in place, which were installed automatically by TOS to support secured remote access:

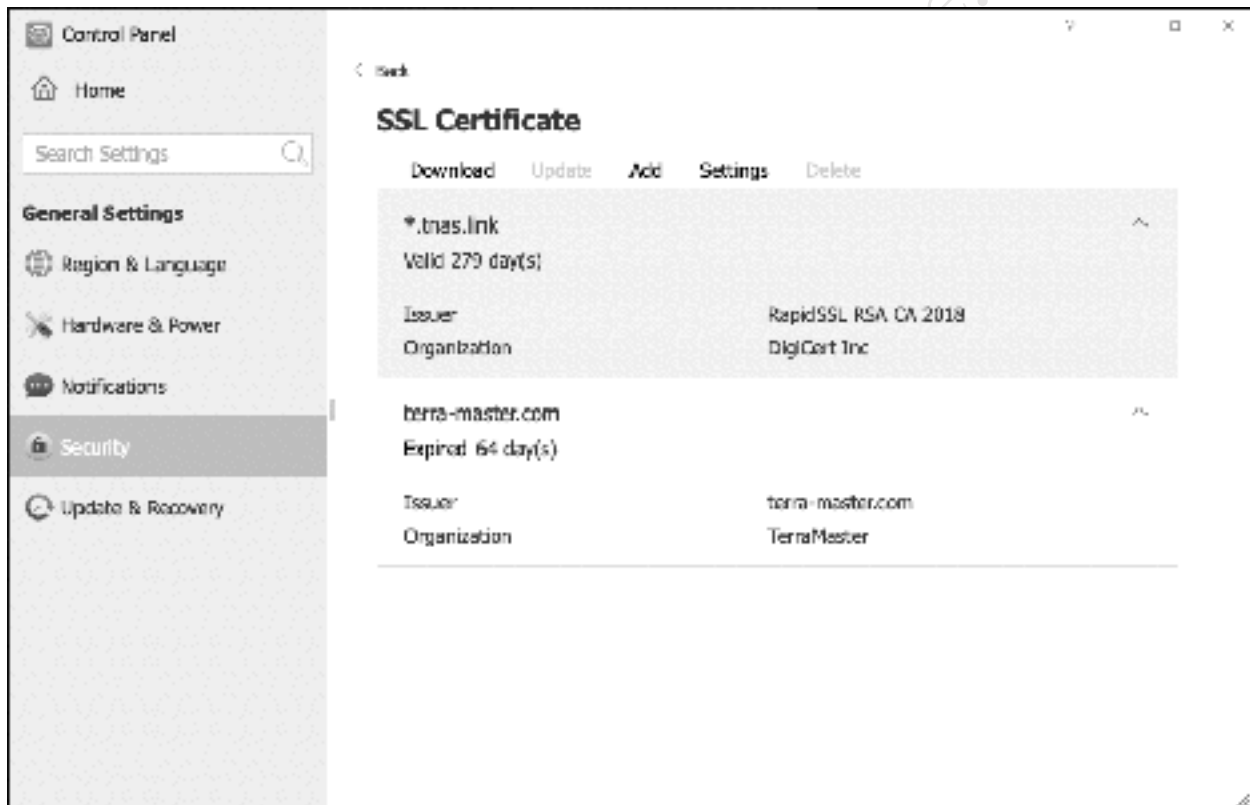


Figure 65: Certificate section within Security

A certificate is valid for a fixed period, which may be anywhere from a month to several years. The first certificate shown above - **.tnas.lnk* - is current but the second one – *terra-master.com* – has expired. To correct matters, highlight it and click **Generate New Certificate & Key**. Within a few seconds, it should be replaced by an updated certificate from TerraMaster, valid for a year.

To add a new certificate, whether self-certified or acquired from a Certificate Authority, use the **Add** option. To assign certificates to specific TOS services, click **Settings**.

More general information about working with certificates can be located at <https://letsencrypt.org/docs/>

6.4 Firewall

TOS includes its own firewall program, which is accessed by clicking **Control Panel** > **Security** > **Firewall**. This operates in the same way as other firewalls, allowing the creation of rules that define which applications may or may not access the TNAS. It is almost certainly the case that your internet connection already has a firewall of some sort, either within the router itself or in the form of a separate appliance if you are a larger business user. However, used selectively the TOS firewall can provide additional security.

In this example, systematic attempts are being made by a hacker to try and telnet into the TNAS - see section [8.5 System Log](#) for how this might be determined. Telnet uses port 23 by default, so we are going to create a firewall rule to block this port.

Go to **Control Panel** > **Security** > **Firewall** and click **Create**. Give the rule a meaningful name, tick the **Enable** box, along with the **TCP** and **UDP** boxes. As we are stopping something, the **Reject** option should be used. Click **Next**.

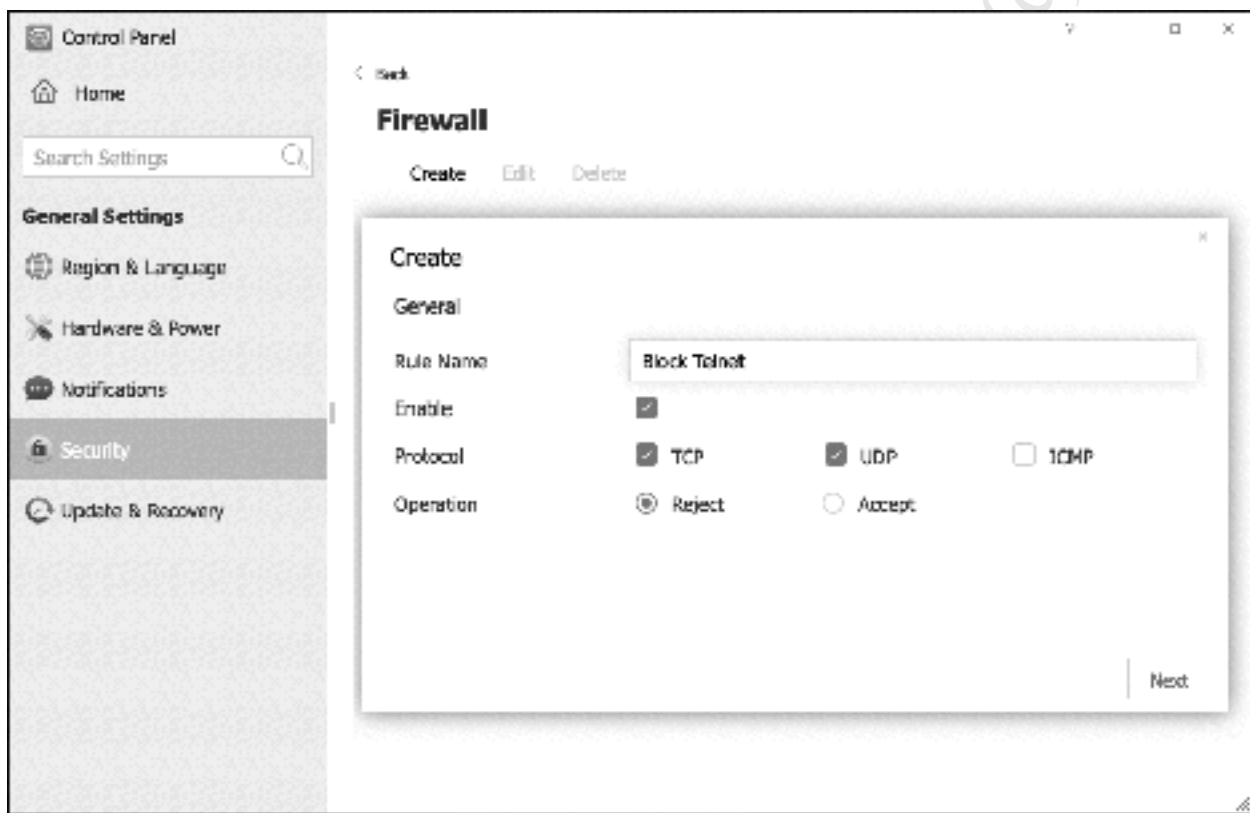


Figure 66: Firewall – creating a new rule

On the next panel, specify the incoming IP address(es) of the thing to be blocked; commonly, this will be for all IP addresses so select **All** and click **Next**. On the panel after that, specify the port number. Click **Apply**. The rule will then be listed on the firewall screen.

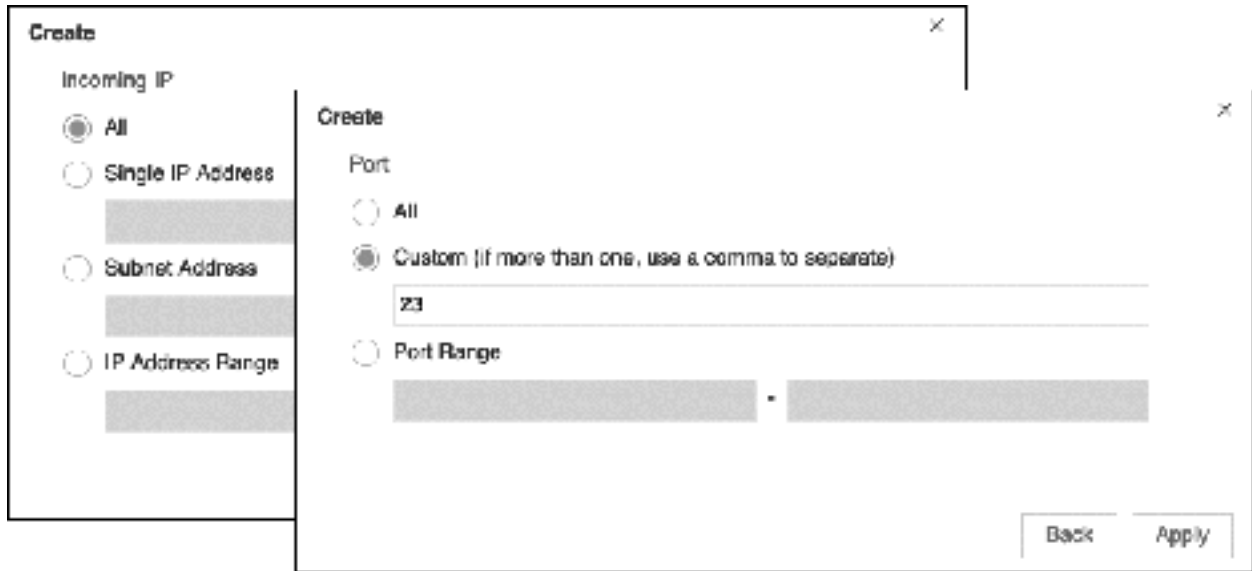


Figure 67: Firewall – IP address and port numbers

Free edition. Do not copy or distribute

6.5 Account Safety

Click on the **Control Panel** > **Security** > **Account Safety** tab. *Automatic Block* is used to block IP addresses that are repeatedly trying to access the TNAS and are failing to do so because the user name and/or password they are using is incorrect. Most computer systems have admin or administrator accounts and hackers try to login to them using commonly used passwords, which is why you should never use obvious passwords such as ‘password’, ‘secret’, ‘admin’, ‘TerraMaster’ and so on. The auto-block facility can provide some protection against such attempts. It is suggested that **Enable Automatic block** is ticked and the number of failed login attempts is set at the default value of 10 within a 5 minute period. Also, tick the **Enable Automatic Block Expiry** option and set it at 3 days. Having made any changes, click **Apply**. To see which IP addresses have been blocked, click the **Block List** button.

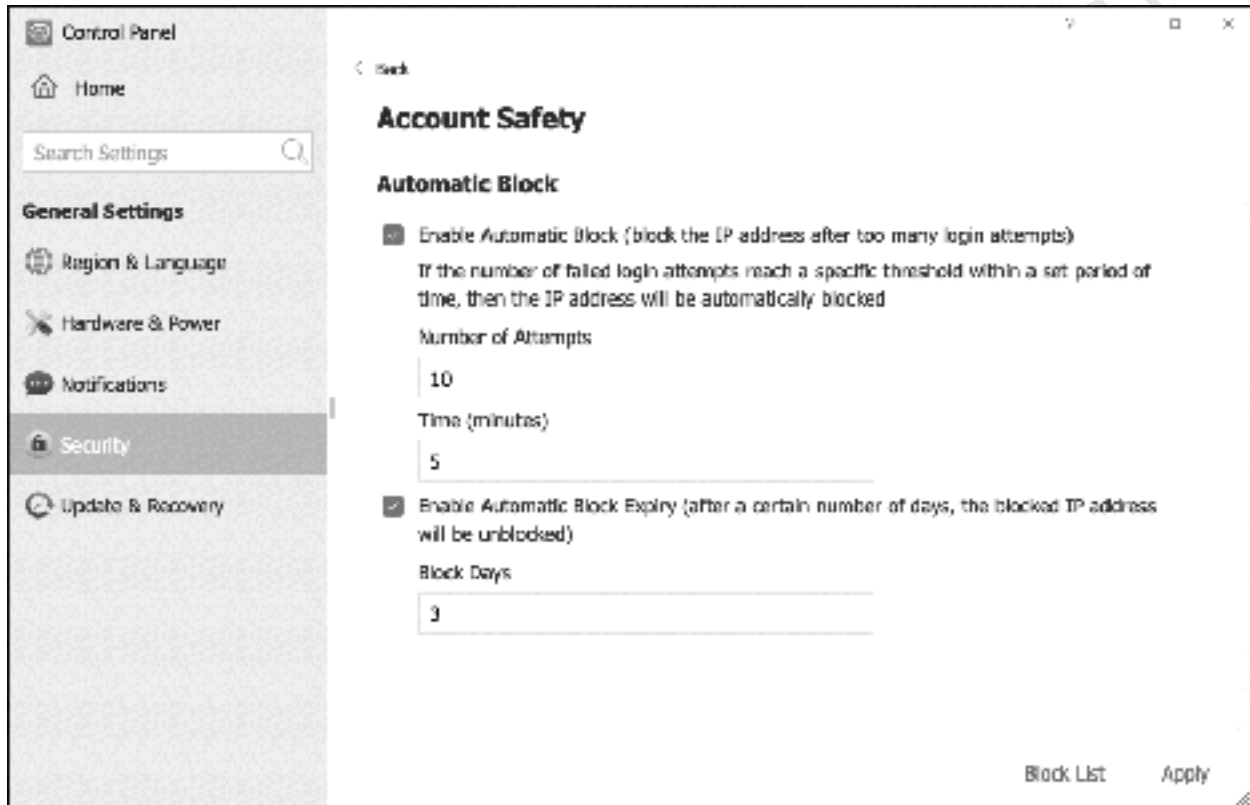


Figure 68: Account Safety screen

6.6 DoS Protection

A *Denial-of-Service* or *DoS* attack is a common technique of hackers and miscreants to make a computer system unusable, typically by trying to overload it with bogus access attempts. TOS offers some protection against this; to access it go to **Control Panel > Security > DoS protection**. The **Enable DoS protection** box should be ticked. Click **Apply**.

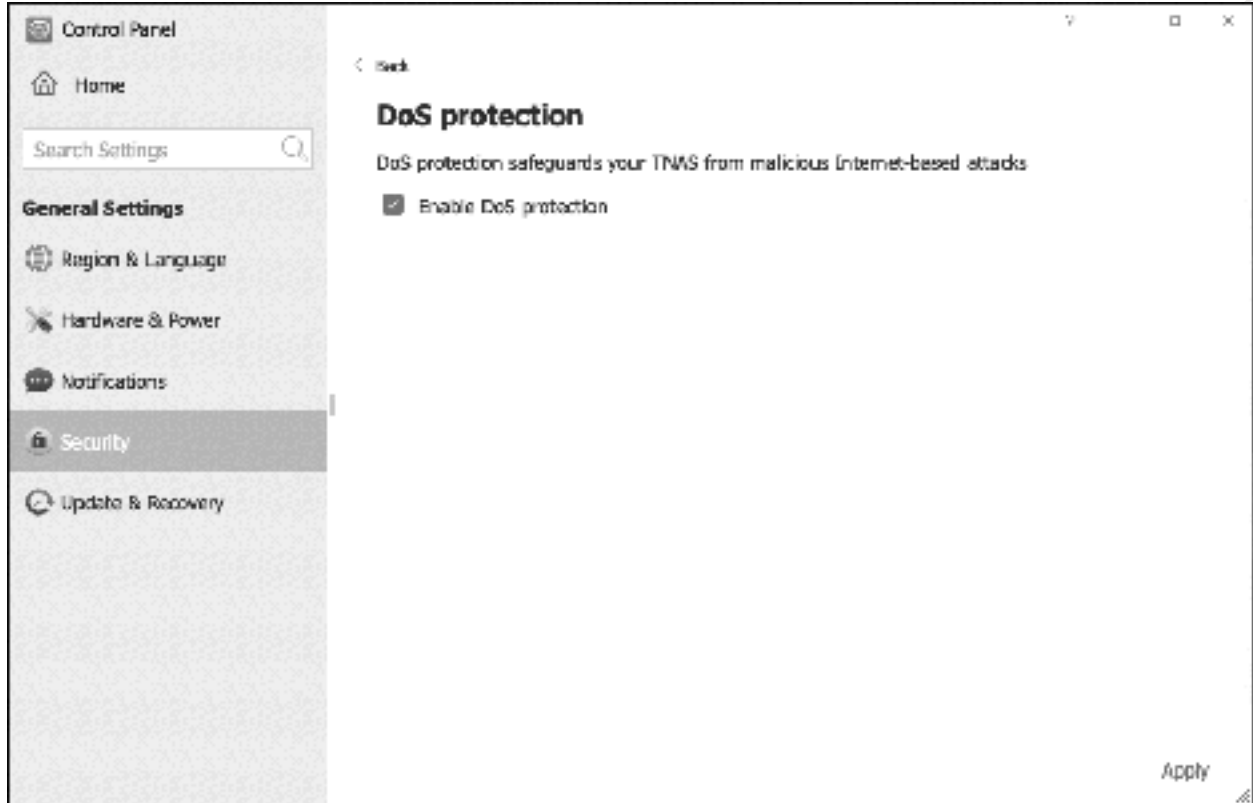


Figure 69: DoS Protection

Free edition. Do not

6.7 Disable Unused Connectivity Services

As the TNAS is connected to the internet, there is a security risk that it can be attacked by external cyber criminals. One way to reduce the risk is to turn off or disable services relating to connectivity that are not being used or are only used infrequently or under special circumstances. For instance, if you do not use FTP then there is no need to have it enabled. The effect of this is to reduce the so-called ‘attack surface’.

To see which services are running, check the Service Status, as described in section [8.3 Service Status](#). Having identified unrequired services, they can be turned off. Mostly these are the Network Services listed in Control Panel. The main candidates are:

Terminal & SSH

Go to **Control Panel > Terminal & SNMP > Telnet/SSH**. Remove the ticks from the **Allow Telnet connection** and **Allow SSH access** boxes. The box which permits use within the local network only can be left enabled if required. Click **Apply**.

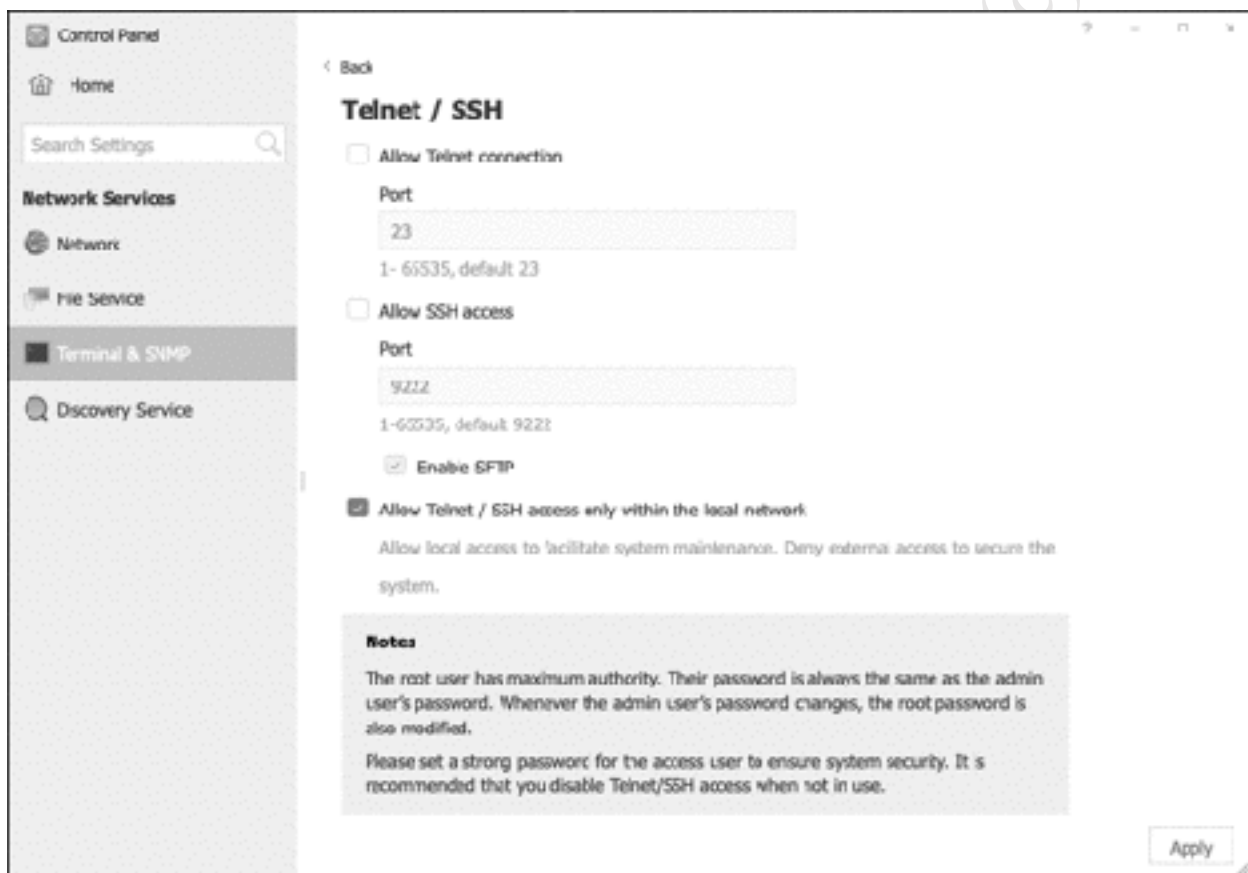


Figure 70: Suggested Telnet/SSH settings

FTP

Go to **Control Panel > File Service > FTP File Service**. Remove the tick from the **Enable FTP File service** box. Click **Apply**.

6.8 Password Settings

When a user account is created on the TNAS, a password has to be specified. Passwords should be non-obvious – under no circumstances should words such as ‘password’, ‘secret’, ‘terramaster’, ‘admin’ and so on be used as these are easily guessed, nor is it a good idea to have the password the same as the user’s name or a close variant thereof. The best passwords combine a mixture of upper and lower letters, numbers and special characters, and are not too short in length. For instance, a password such as *!N3y! YoRk!* would be quite difficult for someone to guess (although as many copies of this guide have been sold you probably don’t want to use it either!). A judgement has to be made regarding how strong the passwords should be; by way of guidance, businesses generally require stronger passwords than home systems and if the server is accessed remotely then the passwords should be as strong as possible. Conversely, in a primary or elementary school it might be better to use simple passwords.

To manage this, go to **Control Panel** and click the **User** icon, followed by **More > Advanced settings** to display the following panel:

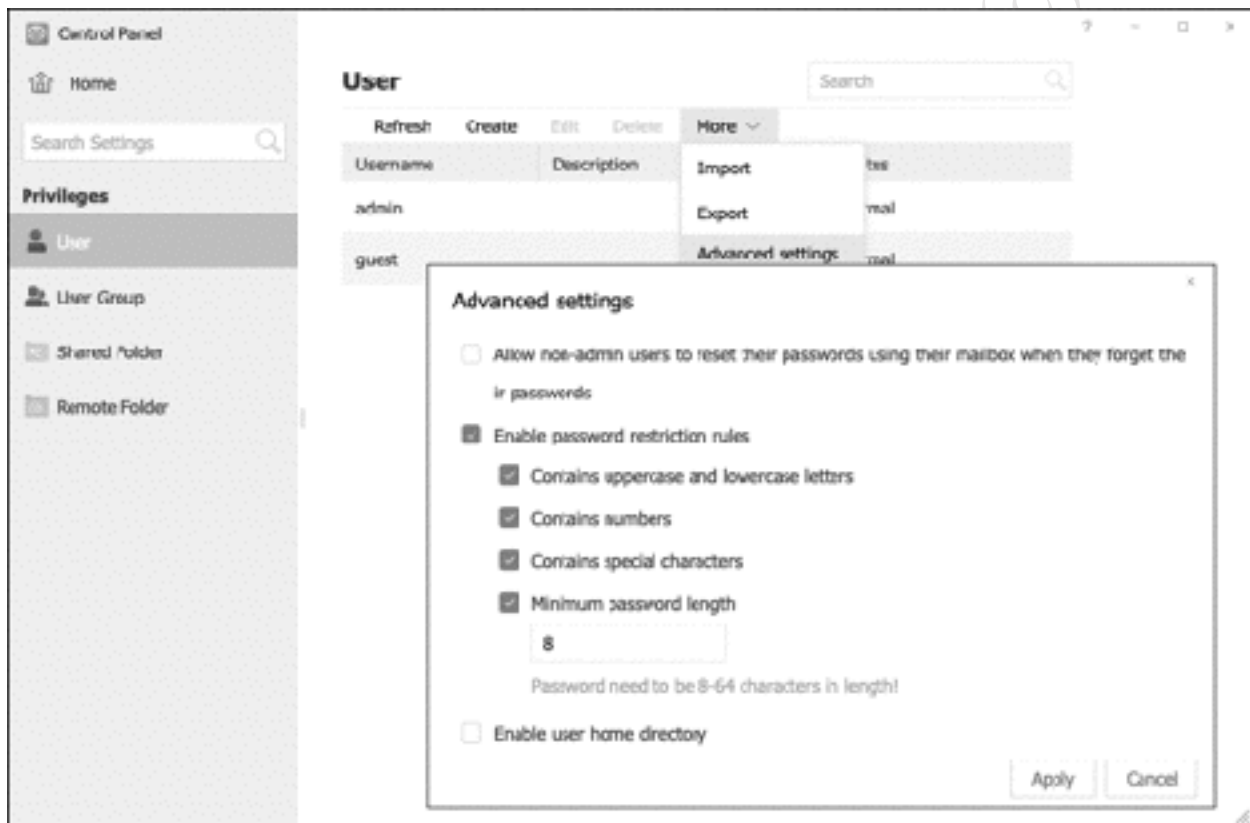


Figure 71: Password Settings

Tick the **Enable password restriction rules** box and tick the conditions to apply. In the above example a mixture of upper- and lower-case letters have to be used, along with numbers and special characters (punctuation), plus the password must be at least 8 characters long. Click **Apply** to make the changes.

Note that these settings apply to all users of the system, although it is possible to exclude the administrator user from password expiration.

If a user has forgotten their password or it needs to be changed for any other reason, it is done as follows:

Within **Control Panel > User**, highlight the user’s name on the **User** tab and click the **Edit** button. On the **User** tab, enter and confirm the new password. Click **Apply**.

A user can also choose to change their own password at any time and how to do so is described in section [11.5 User Settings](#).

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

6.9 Disable the Guest Account

When TOS is installed, two initial accounts are created: *admin* and *guest*. It is considered good practice to disable the guest account, as using it can compromise security. To do so, go into **Control Panel** > **User**, highlight *guest* and click **Edit**. Click the **Advanced settings** tab, tick the **Disable this user account** box and click **Apply**.

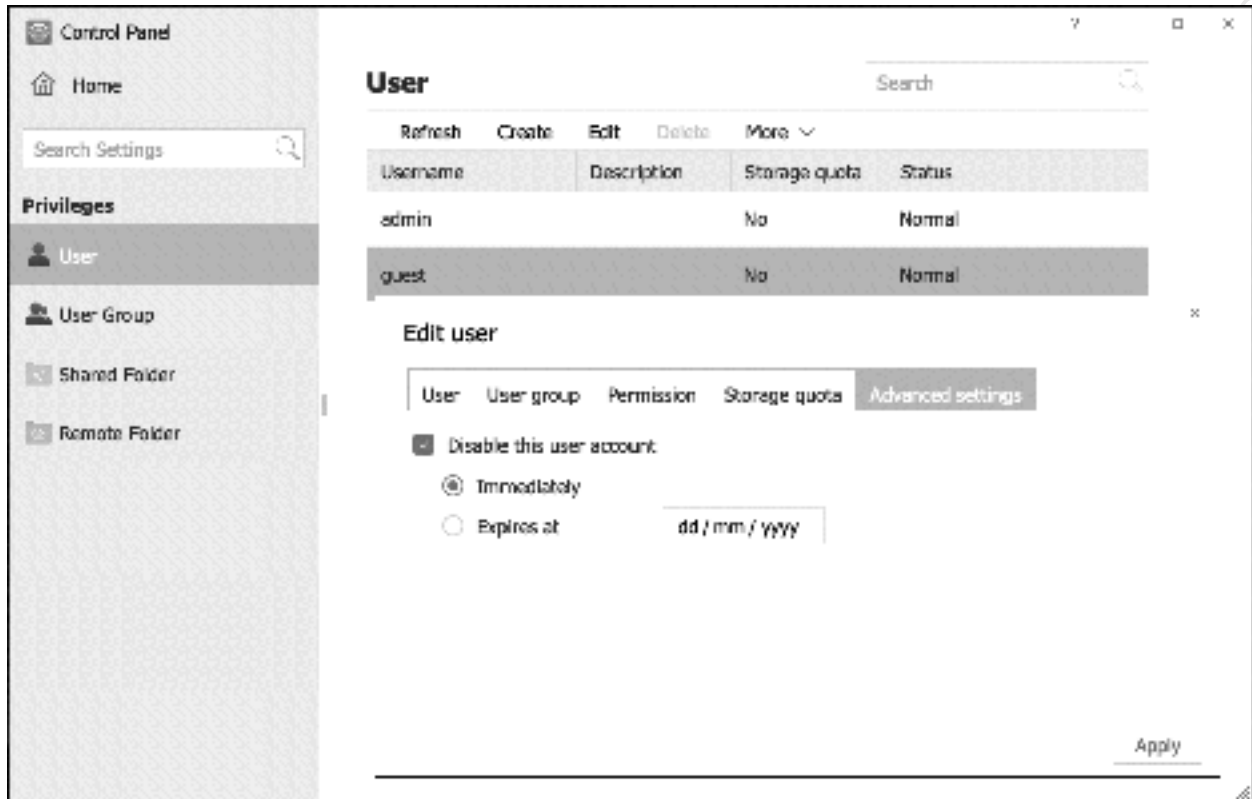


Figure 72: Disable Guest user

Free edition. Do not

7

BACKUPS



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

7.1 Overview

It is important to backup data on a regular basis, in order to cope with the problems that can arise with computers. Examples of things that can go wrong include deleting files by accident, virus and malware infections, data corruption, computer failure and equipment being lost or stolen. In general, the value of data far outweighs the value of 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 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 a bit like pay rises or happy memories: you cannot have too many of them. A NAS system such as a TerraMaster NAS forms the ideal heart of any backup solution and enables you to take a tiered approach, where there are multiple backups to multiple places, thereby ensuring that there is always a fall-back plan in the event of problems. For example:

The computers in the home or office are backed up to the TNAS. The TNAS in turn is backed up to a local USB hard drive. Optionally, the TNAS or at least the most important data are backed up to a Cloud-based service. In the case of a slightly larger business, the TNAS may also be backed up to a second TNAS located on or off the premises:

1. Computers back up to NAS

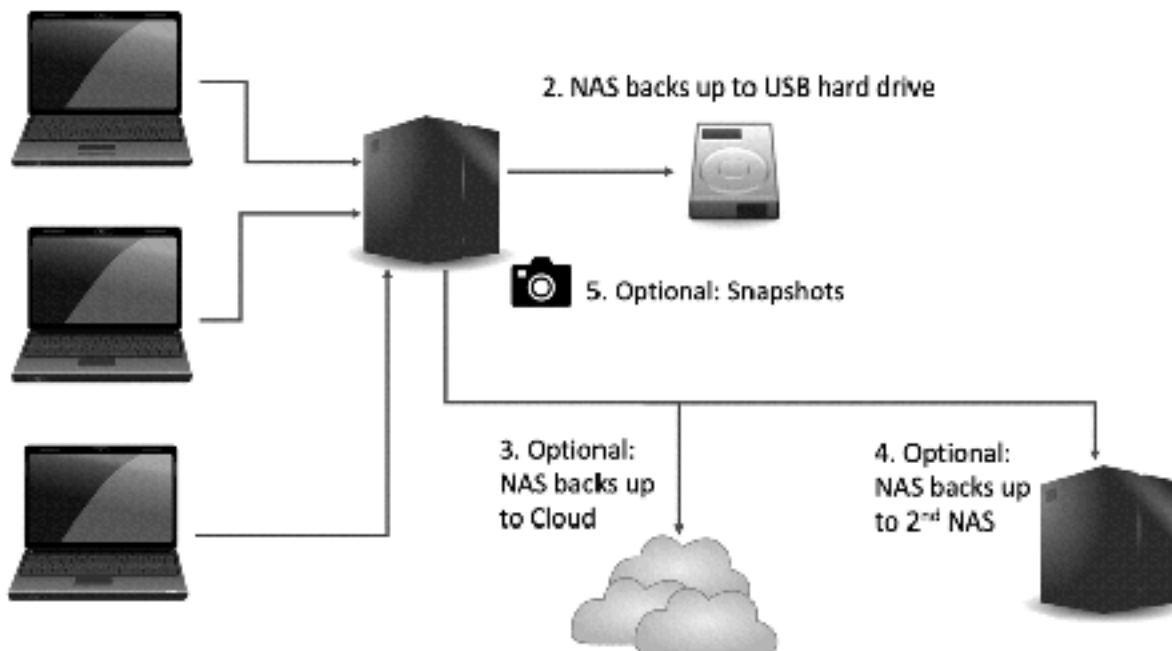


Figure 73: Example of multi-faceted backup approach

To handle these different types of backups, TerraMaster have a variety of tools. For local backups to USB drives, an app called *USB Copy* is used. For cloud backups, an app called *Duple Backup* is available. Both of these have to be downloaded. For backing up a TNAS to another TNAS, the built-in *Backup* app on the Desktop is used (or *Duple Backup* can be used). The *Backup* app is also used for setting up Time Machine for Mac backups. Besides these comprehensive facilities, TNAP also features *Snapshots*, whereby data is effectively 'photographed' at particular moments in time. This is defined as a storage-related rather than conventional backup mechanism and is discussed separately in section [10.4 Snapshots](#).

7.2 Backing Up to An External Drive

Begin by downloading and installing the *USB Copy* app – see [11.2 Applications](#) for information on installing apps.

The external drive should be of USB 3.0 specification or better (USB 2.0 drives will work but are slower); of sufficient capacity to hold all the data but preferably larger (for example if there are 2TB data then use at least a 2TB drive, but a 3TB drive would be better); portable if possible, as they do not require mains power and are more convenient to store. To prepare for backup usage, plug the drive into a spare USB socket on the TNAS. Note that on some TNAS models not all of the USB sockets are of USB 3.n specification.

Click **Control Panel** followed by **External storage**. The drive should appear after a few seconds; highlight it and click **Format**. Choose to format the **Whole disk**. There is a choice of three different file systems. Choose **EXT4**; the only reason for choosing one of the others is that the drive can then be read by other computer types, thus potentially allowing more options for data recovery in the event of extreme circumstances. Click **Confirm** and acknowledge the warning message that is displayed. The formatting may take some time, depending on the capacity and speed of the drive. It is suggested that you do this step, regardless of whether the drive is a new, blank one, or one that was purchased pre-formatted (generally, such drives will have been pre-formatted with the Windows NTFS or exFAT filing system):

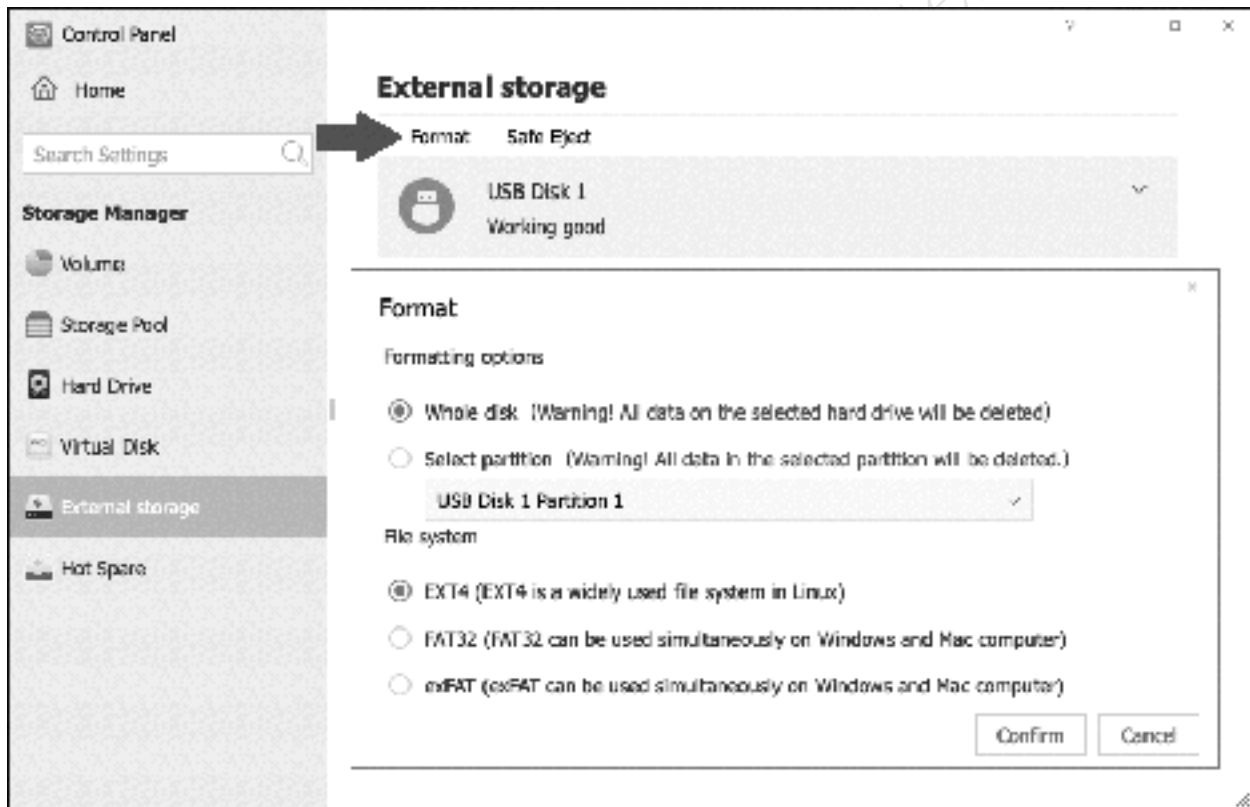


Figure 74: Format external backup drive

When the USB drive has been formatted, quit External storage, go to the Desktop, launch **USB Copy** and click **Create** to begin a new task. Specify a name for the task e.g. *DailyBackup*. For the Backup method, choose **Backup from TNAS to USB** from the dropdown:

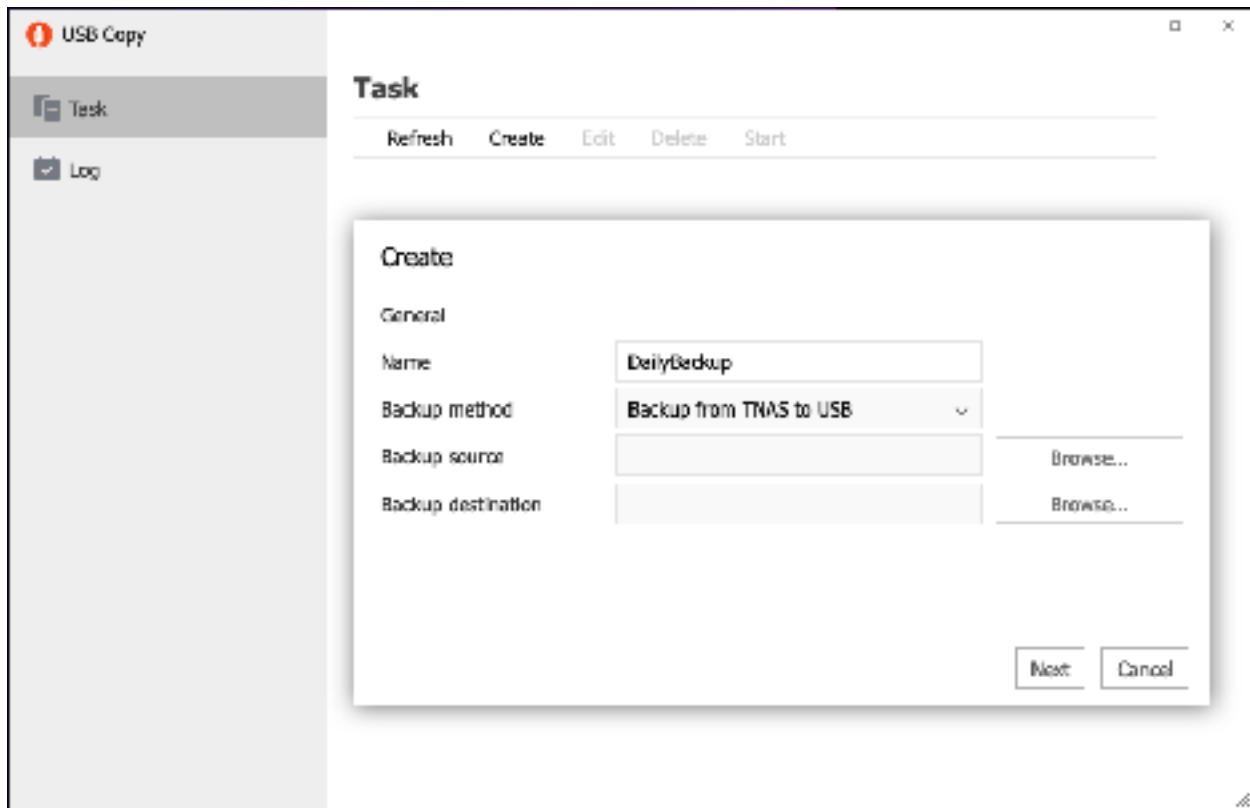


Figure 75: Creating a new backup task

To specify the folder to be backed up – the *Backup source* – click the **Browse** button to the right of the field. On the pop-up panel, choose the folder and click **Confirm**. To specify where it will be backed up to – the *Backup destination* – click the **Browse** button to the right of that panel. On the pop-up panel, choose the USB drive and click **Confirm**:

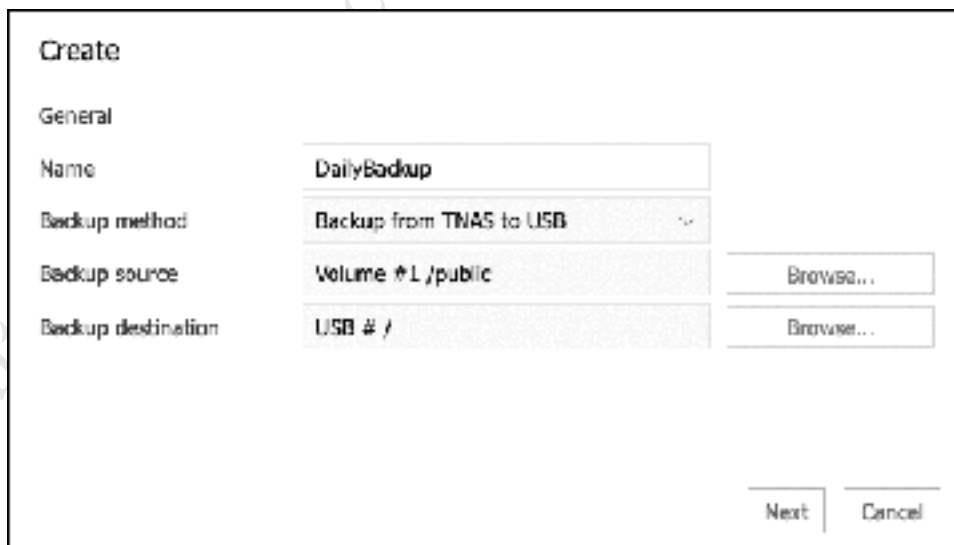


Figure 76: Select source and destination

Click **Next**. The subsequent screen is for defining the backup method and there are three options:

Multi-versions – a complete copy of the source is taken with each backup. Having multiple copies enables you to ‘roll back in time’. For instance, you might be taking daily backups but need to be able to

restore a version of a file from, say, a month ago. With multi-versions you can do this, provided you have sufficient capacity on the backup drive.

Mirror – the backup will be an exact copy of the source. Conceptually this is very simple and straightforward. The potential downside is that if a file or folder is deleted on the NAS then it will subsequently also be deleted from the backup.

Incremental – only newly added files and folders or ones that have changed are added to the backup. This ensures that a copy of all data is available and makes for backups that are efficient in terms of storage space and time.

There isn't really a 'right answer' in deciding which route to take and in this example we have selected incremental. It is suggested that the boxes to delete files are not ticked, but that the **Overwrite** option is selected. Click **Next**:

The screenshot shows a 'Create' backup configuration window. The 'Backup method' dropdown menu is open, displaying four options: 'Incremental' (which is selected and highlighted), 'Multi-versions', 'Mirror', and another 'Incremental' option. Below the dropdown, there are two unchecked checkboxes: 'Delete the original file structure in the destination folder (flatten all files)' and 'Delete source files after backup'. Under the section 'Apply following policy when file conflict', there are two radio buttons: 'Rename' and 'Overwrite', with 'Overwrite' being the selected option. At the bottom right of the window, there are three buttons: 'Back', 'Next', and 'Cancel'.

Figure 77: Backup method and options

The subsequent screen is for specifying the backup time and there are four options:

Do not backup – i.e. the backup is suspended/non-operational

Backup now – run the backup immediately

Copy task starts immediately... - run the backup whenever the USB drive is plugged-in

Backup Schedule – run the backup regularly on a scheduled day and time

Of these options, a scheduled backup is possibly of most use. Use the **Date** and **Time** dropdowns to specify the backup frequency; in this example, the backup will run every day at 22:00 / 10:00pm. Click **Next**:

Edit

Backup time

Do not backup

Backup now

The copy task starts immediately after the USB device is plugged in.

Backup schedule

Date: everyday

Time: 22:00

Back Next Cancel

Figure 78: Backup schedule

A panel to confirm the settings is displayed – click **Confirm** to continue and the newly created task will be listed on the main screen:

USB Copy

Task

Log

Task

Create Edit Delete Execute

	DailyBackup	Completed
Type	Backup from TNAS to USB	
Backup source	Volume #1 /public	
Backup destination	USB #1	
Backup method	Incremental	
Backup time	everyday 22:00	
Last backup	2020-05-07 09:38:27	

Figure 79: Newly added backup task

Rather than wait until the scheduled time to see if the backup has worked, it is suggested that you test it immediately. To do so, highlight the backup and click **Execute**. The time taken for the backup to run depends upon the amount of data. In the case of incremental backups, the first one will take longer but subsequent ones will be quicker as only the changed data is being added.

Each backup generates an entry in the logfile. To view the logs, click **Log** on the main screen. On a regular basis e.g. once a month, the logfile can be cleared by clicking **Clear**. If it is required to keep a permanent record, click **Export** first to generate a copy in Excel format.

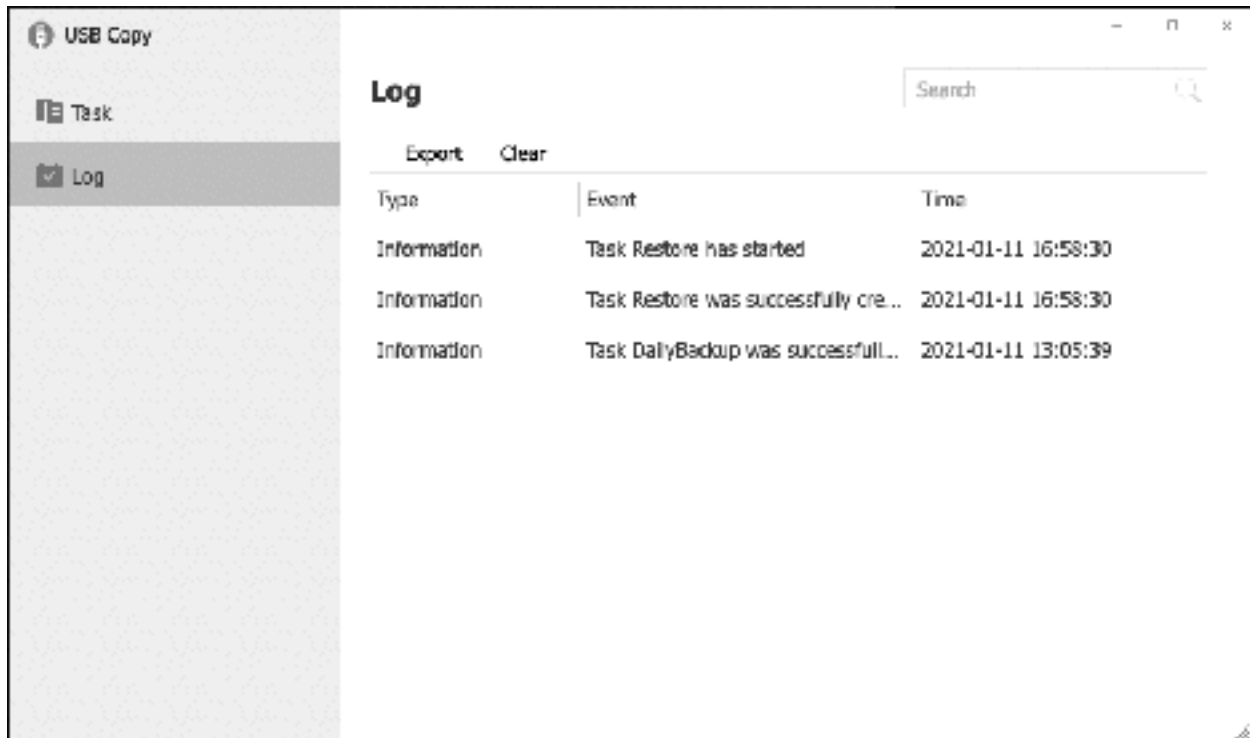


Figure 80: Backup logs

If you are doing daily backups, you may wish to leave the USB drive permanently connected to the TNAS. If you are doing weekly or manual backups, it is a good idea to remove the drive once the backup has completed and keep the drive in a safe place, away from the TNAS. Before removing the drive, it should be ejected, which is done by clicking on the mini-icon in the top right-hand corner of the screen:



Figure 81: Ejecting an external drive

One common question is: as only one folder can be copied to the USB drive, what happens if there are multiple folders that need backing up? The answer is to define multiple backup tasks for individual folders and schedule them accordingly.

7.3 Restoring Files from a Backup

Restoring files from a backup consists of creating a task in USB Copy, but running in the opposite direction, so to speak. From the main USB Copy screen, click **Create** to begin a new task. The *Backup method* should be set to **Backup from USB to TNAS**. For the *Backup source*, click **Browse** and select the USB drive; if you have been using the Multi-versions backup option, you can choose a backup from a specific date or time. For the *Backup destination*, click **Browse** and choose a folder where the restored data will go. This could be the original folder that was backed up, but you could restore it to a different one (you could, for instance, create a temporary folder specifically for this purpose and check the restored data before subsequently moving it to the original location using File Manager).



Figure 82: Example restoration settings

Click **Next**. For the *Backup method*, choose **Mirror**, regardless of the method that was used for making the original backup:



Figure 83: Set Backup method to Mirror

Click **Next**. The subsequent screen is for specifying the *Backup time*. When there is a need to restore files, chances are it needs to be done quickly so select **Backup now** and click **Next**. However, if you were restoring a large amount of data you could, of course, schedule to run at some other time, such as

overnight. Click **Confirm** on the confirmation screen and the 'backup' will run. When complete, check the logfile and use File Manager to verify that the data has been restored.

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

7.4 Backing up to Cloud Services using Duple Backup

Using *Duple Backup*, downloadable from Applications, the TNAS can be backed up to a variety of destinations including popular commercial and public cloud services including Amazon S3, Alibaba Cloud OSS, Dropbox, Google Drive, Microsoft OneDrive and Yandex. Upon launching it for the first time, it will prompt to create a new task and there is a choice of backing up a shared folder or an iSCSI LUN (for information on iSCSI, see section [10.5 iSCSI](#)). To create additional tasks in the future, click **Create** on the Task pane.

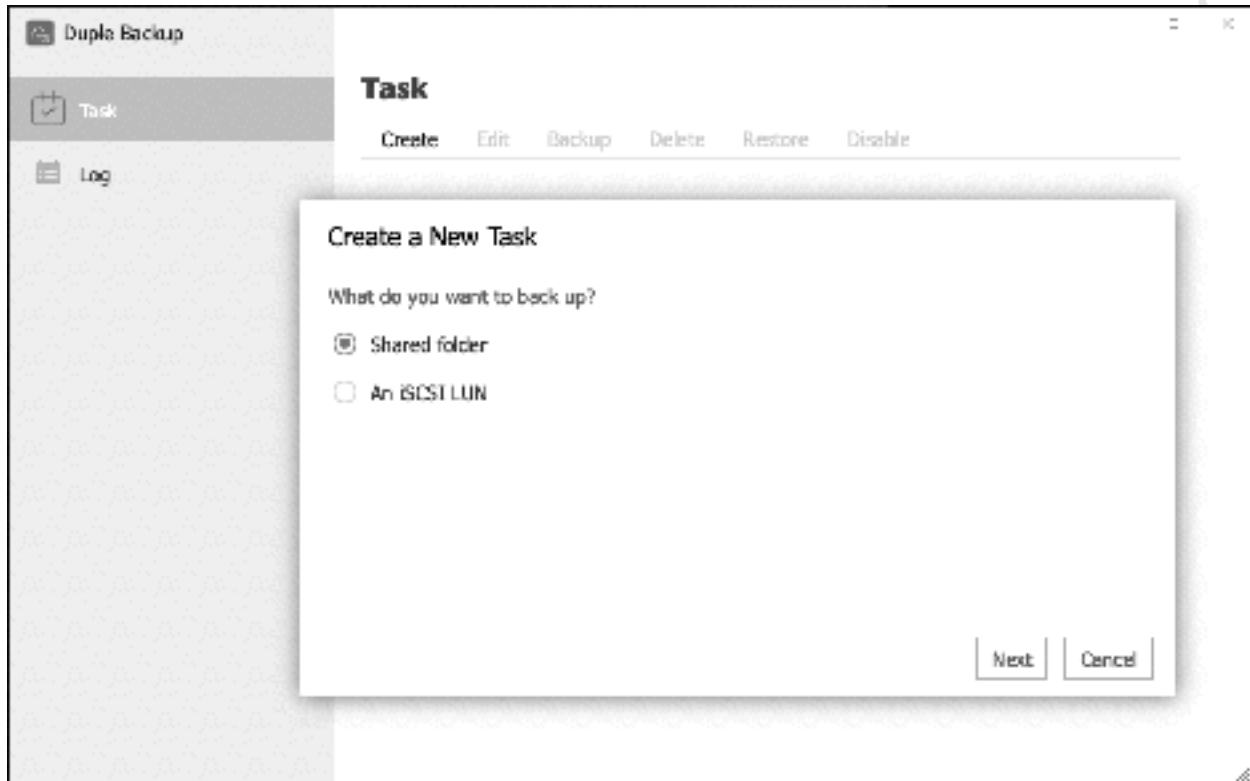


Figure 84: Create New Task

Click **Next** and on the subsequent pane choose the destination for the backup. There is a choice of *Server* or *Cloud drive*, of which we want the latter. Use the dropdown to select the cloud service to be used, which needs to be one where you already have an account, and click **Next**:

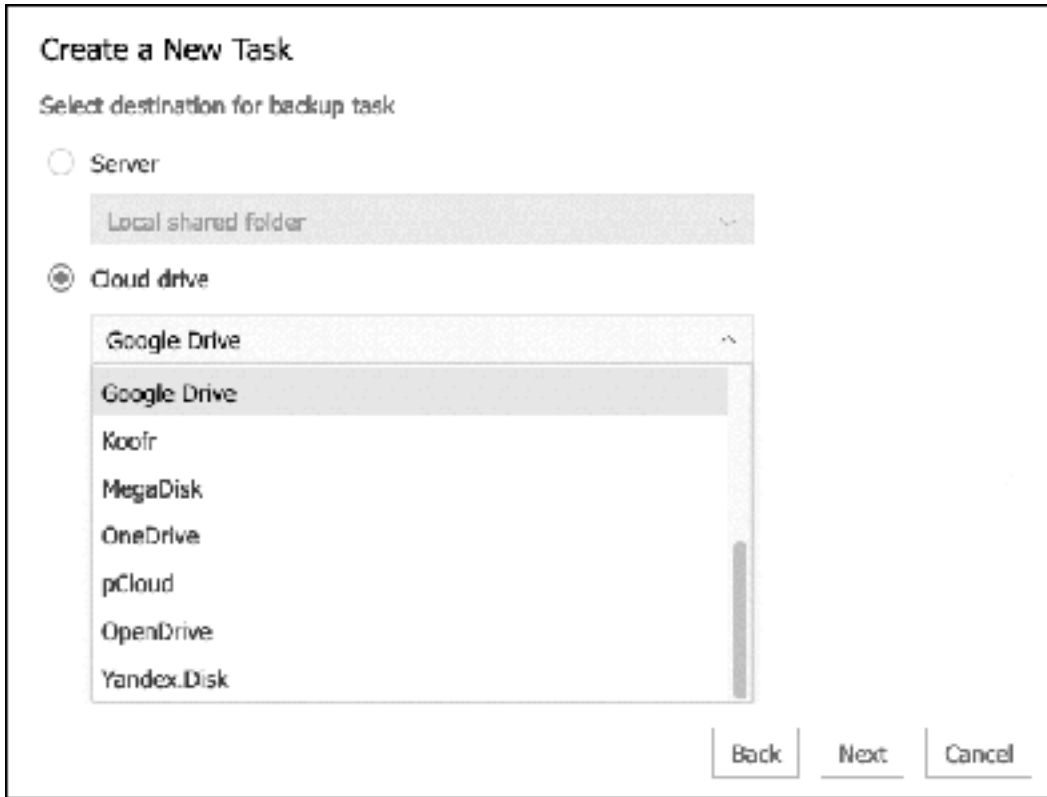


Figure 85: Choose a cloud service

You will be prompted to confirm that you wish to grant access to TerraMaster Cloud Sync by the provider's website, the specifics of which will vary depending on the provider. Having done so you will be returned to the Duple Backup app and the Backup destination settings panel. The *Shared folder* refers to the destination on the cloud - usually this is set as the top level or root (/) or may not be alterable. The *Directory* (again, this refers to the cloud side) is what will be created on the cloud and the default can be accepted:

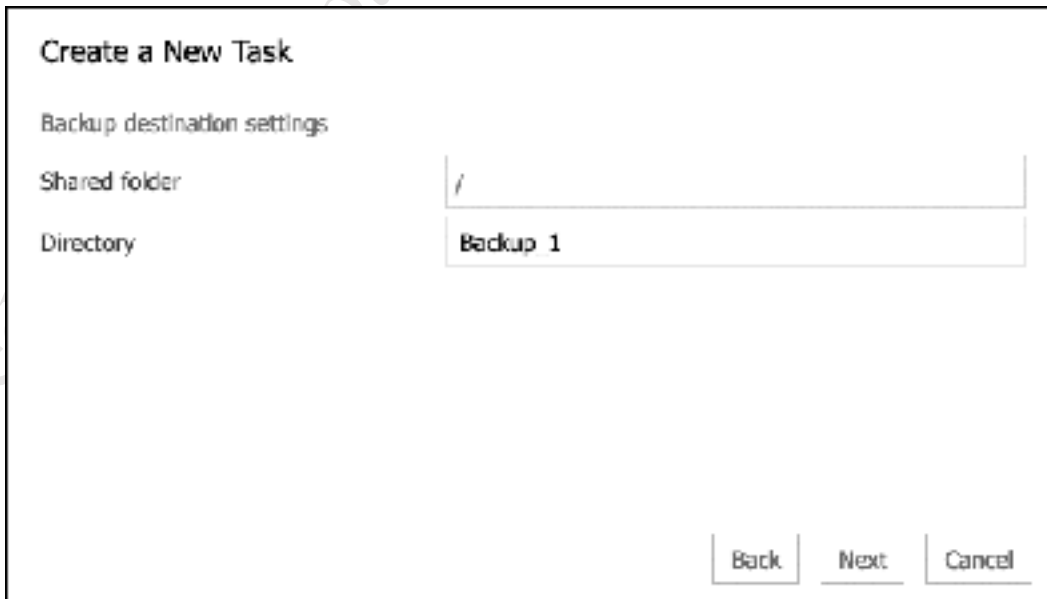
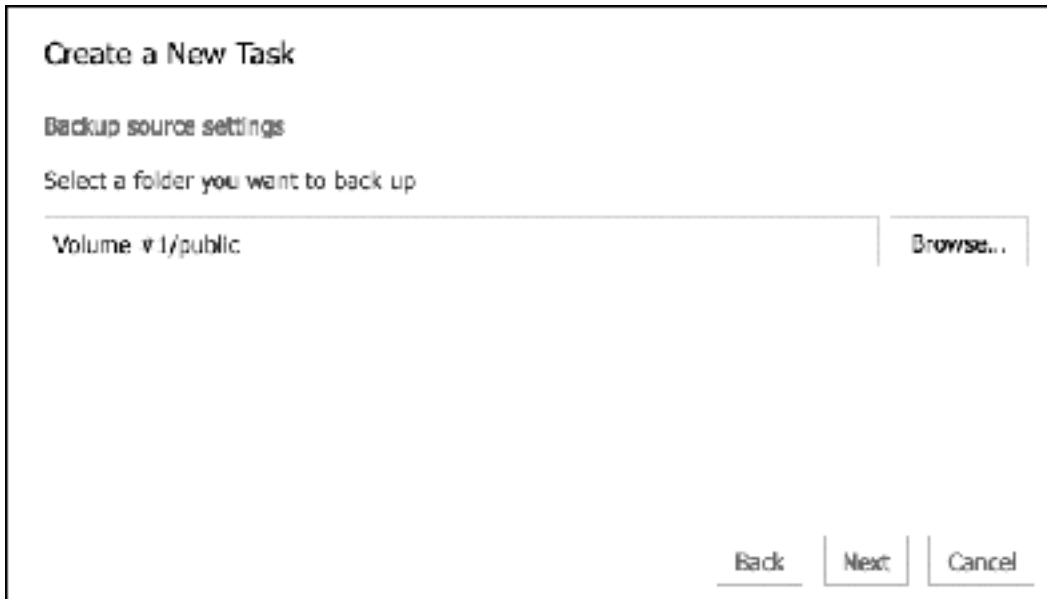


Figure 86: Backup destination settings on cloud service

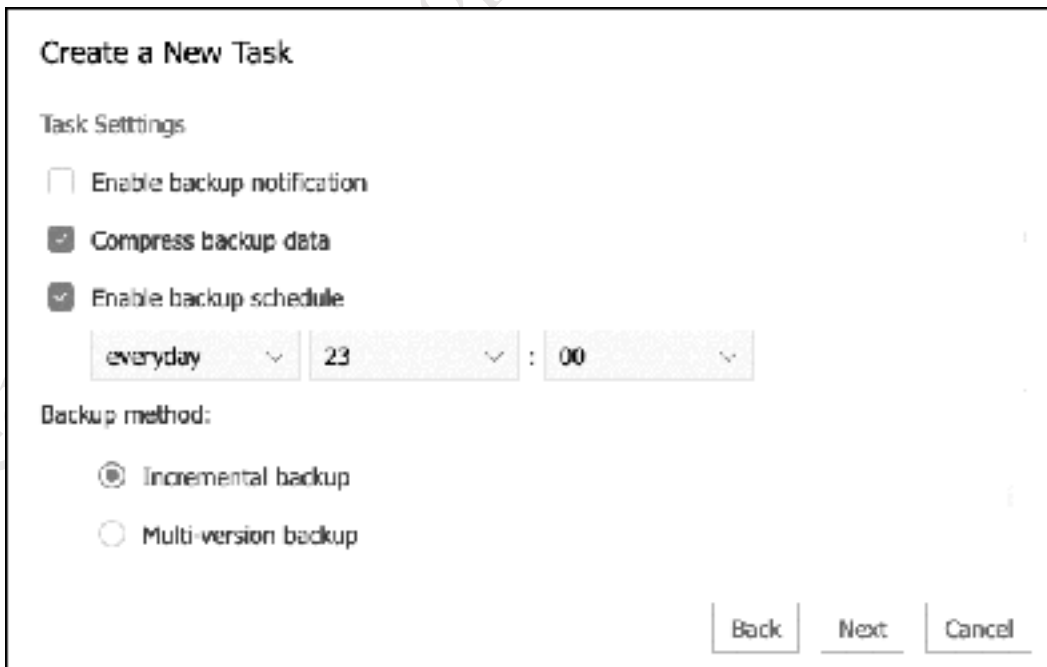
Click **Next** and on the following panel click **Browse** and choose the folder on the TNAS that will be backed up. Click **Next**:



The screenshot shows a dialog box titled "Create a New Task". Under the heading "Backup source settings", there is a prompt "Select a folder you want to back up". Below this is a text input field containing "Volume #1/public" and a "Browse..." button to its right. At the bottom right of the dialog are three buttons: "Back", "Next", and "Cancel".

Figure 87: Select folder to be backed up

On the following screen specify a *Task name* and click **Next**. On the one after that there are several options that can be specified, including a backup schedule (daily in the example below) and compressing the backup data (so it will use less space on the cloud). There is a choice of Backup method: *Incremental backup* is more efficient as only changed files are backed up, whereas with Multi-version backup it will be possible to 'roll back in time' to previous versions of files. However, multi-version backups can use a lot more space and as cloud storage usually has to be paid for this may be an important consideration. Click **Next**.



The screenshot shows the "Create a New Task" dialog box, "Task Settings" section. It includes three checkboxes: "Enable backup notification" (unchecked), "Compress backup data" (checked), and "Enable backup schedule" (checked). Below the "Enable backup schedule" checkbox is a time selection interface with three dropdown menus showing "everyday", "23", and "00". Under the heading "Backup method:", there are two radio buttons: "Incremental backup" (selected) and "Multi-version backup" (unselected). At the bottom right are three buttons: "Back", "Next", and "Cancel".

Figure 88: Task settings and Backup method

A screen to confirm the settings is displayed – click the **Confirm** button and the task will be created and added to the main screen. If the task has been scheduled, rather than wait until the allotted time it can be tested immediately by clicking **Backup**. The task can also be changed, deleted and disabled from here:

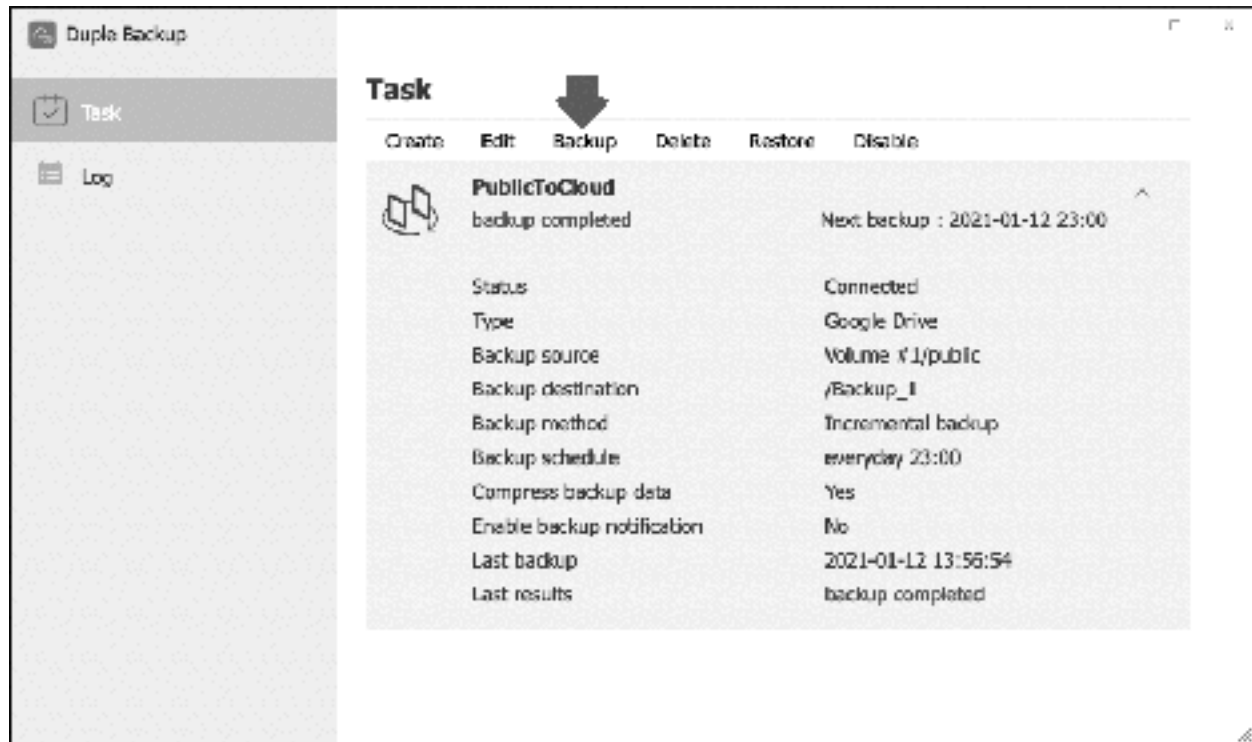


Figure 89: Task list

The speed of backup to a cloud service is largely dependent upon the speed of the internet connection but is typically many times slower than backup to a local drive. For guidance, a backup of 1 terabyte that might take under an hour to a USB drive may take several days over the internet, even with a relatively good upload speed. For this reason, rather than use a cloud backup as the primary backup solution, it might be better to use it as a secondary backup for a limited selection of important data.

One important consideration is that you have sufficient space in the public cloud account. For example, a free Dropbox account only has 2GB of space, although additional space can be gained through referrals. This may not be enough so you may want to consider a paid account such as Dropbox Plus or Professional. Another approach is to have accounts with multiple providers, in which case you could backup different folders to them e.g. public to Google Drive, multimedia to OneDrive and so on. You can add further cloud services by clicking **Create** on the Task screen.

Note: in addition to Duple Backup, TerraMaster also have separate apps for individual cloud services e.g. Dropbox (*Dropbox Sync*), Google Drive (*Google Drive Sync*) and OneDrive (*OneDrive Sync*). As these largely duplicate the functionality of Duple Backup, which can handle all of them anyway, there is little point in using them.

7.5 NAS to NAS Backups Using Rsync

One potential downside of using a USB drive for backups is that it has to be physically located close to the server. In the event of a disaster – for instance, fire, flood or theft – not only might the server be lost but the backup drive might be as well. One way to mitigate against this is to use another NAS unit as a backup device. This gives a lot more flexibility as to where it is located; for instance, it could be in a totally different part of the building or another building altogether. The second NAS can be in addition to or in place of the USB backup drive.

Note that we have used the term ‘NAS’ rather than ‘TNAS’, as it is possible to use just about any brand of network attached storage and you are not restricted to TerraMaster, although this would be an obvious choice for most people. But consider a scenario where you are upgrading from another vendor to TerraMaster, in which case you might be able to re-designate the old NAS as a backup unit. This is possible because most NAS operating systems, including TOS, are based on or derived from Linux. Linux itself is a derivative of UNIX, and in the UNIX world a program called *rsync* – remote sync – gives the capability to backup one computer to another. When doing so, the one containing the original data is referred to as the *source* and the one that will hold the backup is the *destination*.

The first thing to do is setup the destination server. We will assume that the destination is a TNAS; if this is not the case then these exact instructions will not apply, but there should be something analogous. Create a shared folder called *NetBackup* and give access to the *admin* user only (creating shared folders is described in section [3.2 Creating Shared Folders](#)).

Next, go into **Control Panel > File Service > Rsync Server** and tick the **Enable Rsync server** box. Leave the Port number as 873, which is the standard for Rsync. There is a default username of *rsync*, although you could change it if you wish. In the Authorized Directory section, click **Add** and choose the newly created *NetBackup* folder. Click **Apply**:

Free edition. Do not copy or distribute.

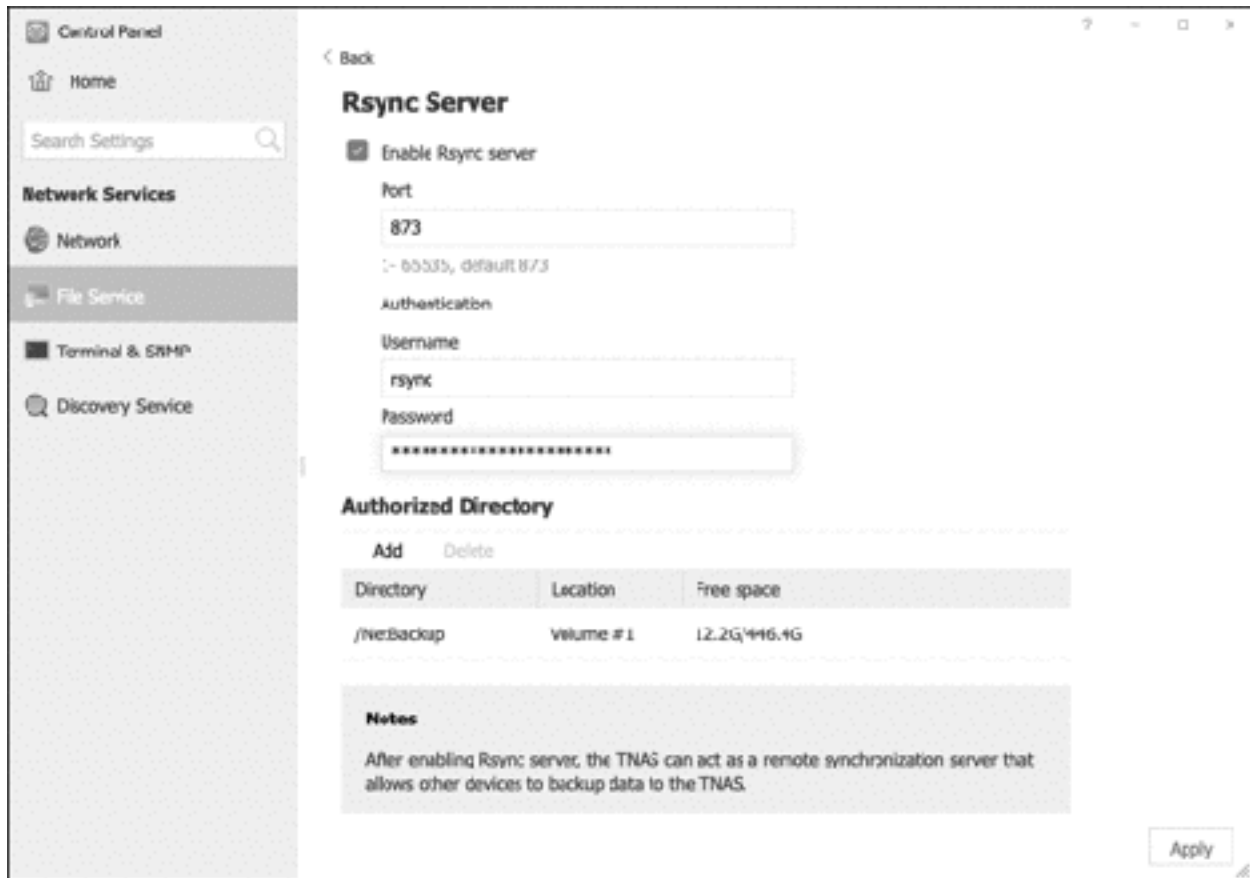


Figure 90: Enabling the rsync service

Moving to the source TNAS, launch **Backup** from the Desktop and click **Rsync Backup**, followed by **Create**. Give the backup task a name e.g. *RemoteBackup*. Specify the IP address of the destination server, leave the Port as 873, specify the username and password on the destination server. Click **Test** - if the source cannot 'see' the destination, an error message is shown, otherwise things are looking good and you can click **Next**:

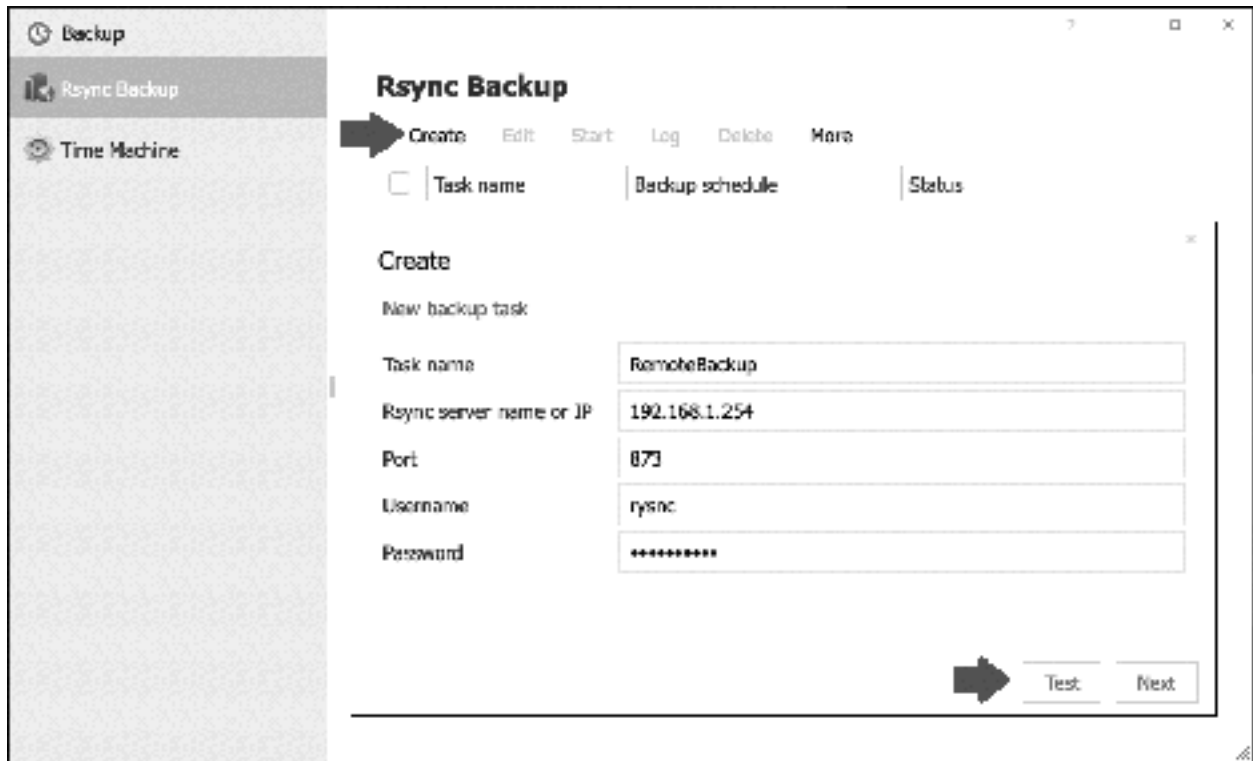


Figure 91: Specify the Backup Destination Settings

On the subsequent panel, use the dropdowns to specify the source folder or path, which in our example is the *public* folder, and the destination folder or path, *NetBackup*. Note that you can only backup one folder at a time. Click Next:

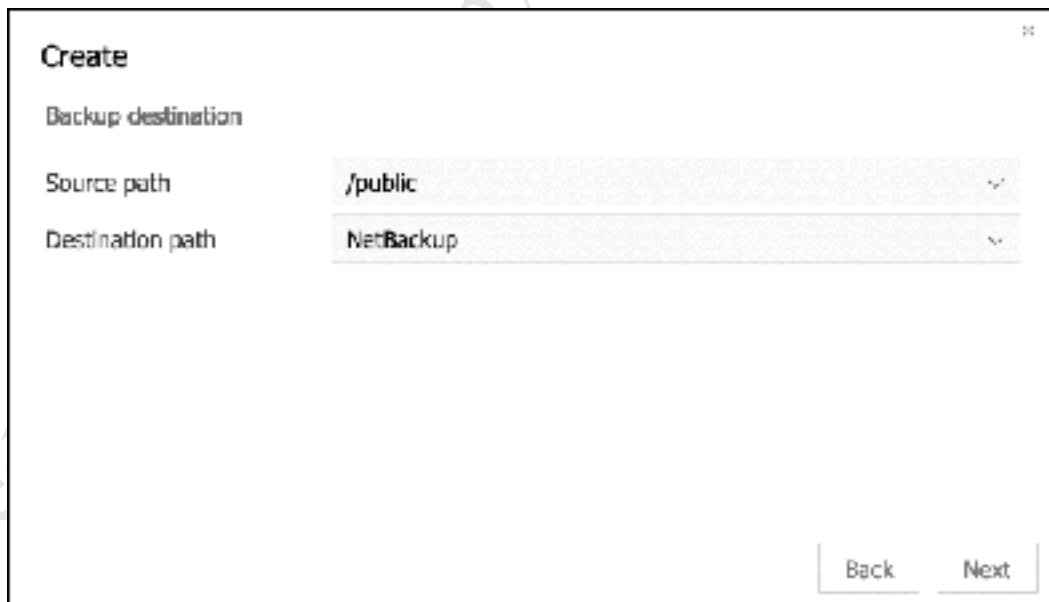


Figure 92: Select the Source and Destination folders

The following screen allows you specify a schedule, or you can choose to run the backup now:

Create

Backup schedule

Do not backup

Backup now

Every day

Every week Sunday

Every month 01

Time 00:00

Back Next

Figure 93: Backup Scheduling

The final screen provides a number of options to fine tune the backup process. In a small setup you might choose to ignore them, but in a larger setup they become more significant:

Create

Option

Activate the encryption. Required to input the SSH ports

[Text Field]

{Note: You need to enable SSH encryption option on destination host. Meanwhile, SSH port needs to be consistent with the destination host port.}

Compression backup

Suspend all reading and writing operations during backup

Backup modified files and folders only

Backup all

Sparse file backup

Back Complete

Figure 94: Rsync options

Activate the encryption - The first option is to activate encryption, which you should certainly do if you are backing up to a NAS at another physical location over the internet. In this case, port 22 will need to be opened on the firewalls and SSH enabled at both ends.

Compression backup – reduces the size of the backup and hence the amount of data that needs to be transmitted. This is useful if backing up to a remote NAS over the internet to reduce the amount of traffic.

Suspend all reading and writing operations during backup – this can speed-up the backup and improve integrity

Backup modified files and folders only – only changed files are backed up i.e. incremental backup

Backup all – all files and sub-folders are backed up

Sparse file backup – a more efficient method of storing data

Having specified (any) options, click **Complete**.

The newly defined backup job will now be listed on the main screen, from where it can be managed. It can be edited, executed, disabled or deleted from this screen; also, there is an option to view the log files generated by the backup jobs.

One common question is: as only one folder at a time can be backed up to the remote NAS, what happens if there are multiple folders that need backing up? The answer is to define multiple backup tasks for the different individual folders.

Free edition. Do not copy or distribute. (c) 2013

7.6 Backing up the System Configuration

Although we have discussed how to backup data from the server in this chapter, there is another type of backup that should be carried out on an occasional basis. A lot of customization may have gone into the server in terms of defining users, shares, permissions, settings and so on. In the event of serious problems with the server - for example, of the sort necessitating a complete re-installation - all this configuration information would have to be re-entered. This can be both difficult and time consuming on all but the smallest of systems. Fortunately, there is a facility to quickly backup and restore the configuration.

Go into **Control Panel > Update & Recovery > Backup & Restore**. Select **Back up system configuration**, followed by **Apply**. Enter the admin password when prompted and click **Confirm**. The system will process for a few seconds and then prompt you to save the file it has generated, called *terramaster_server_config_backup.bin*, onto the computer you are using (the exact message will depend upon what browser you are using). Keep the file in a safe place; you might want to consider keeping a copy on a USB memory stick, for instance.

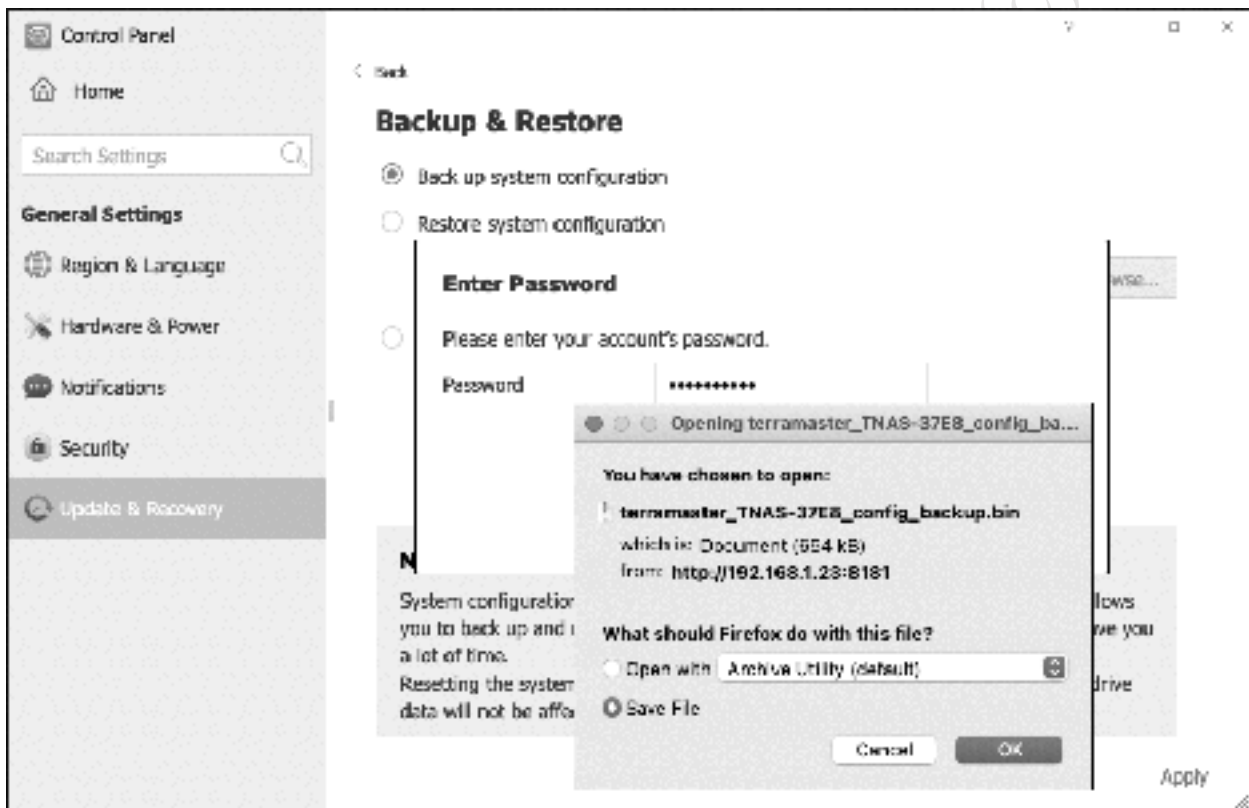


Figure 95: Back up System Configuration

Should it ever prove necessary to use this configuration file, go into **Control Panel > Update & Recovery > Backup & Restore** and click **Restore system configuration**. Click the **Browse** button, navigate to the location of the configuration file, then click **Apply**. Restart the TNAS when prompted.

7.7 Backing up Windows Computers

Backing up Windows Computers using AOMEI Backupper

AOMEI Backupper is a program used for backing up Windows PCs to the server, available free of charge from TerraMaster. It is particularly useful where laptops are in use and being taken outside the business or home, as they may have data stored on them locally that is not otherwise being backed up. Although all versions of Windows have a built-in backup program of some sort, *AOMEI Backupper* has three key advantages:

- It is more flexible and capable than the Microsoft offerings
- Only Professional editions of Windows can backup to network drives, with Home editions being restricted to external USB drives only. In contrast, *AOMEI Backupper* allows any Windows PC to backup to the network
- Different versions of Windows have different backup programs e.g. Backup & Restore in Windows 7, File History in Windows 8 and 10. *AOMEI Backupper* runs identically on all versions of Windows, including older versions such as XP and Vista, making it a universal solution

It is downloaded from Applications (see [11.2 Applications](#)); however, it does not download and install onto the TNAS but is placed in the computer's *Downloads* folder, from where it can be installed onto the computer that you wish to back up. If you wish to install it on many computers, you could copy the download into a shared folder on the server e.g. *public* or a dedicated *technical* folder such as we created in [3.2 Creating Shared Folders](#) and then subsequently copy it from there to each computer.

AOMEI is a very comprehensive backup and imaging utility. Additionally, although it is genuinely free, further features are available through optional paid versions which might be of interest to IT support professionals. It is no exaggeration to say that the program could justify a full manual on its own, rather than a section in this one. In this example, we will explain how to backup folders from a computer to the server using the free edition.

Running AOMEI for the first time will display the following screen:

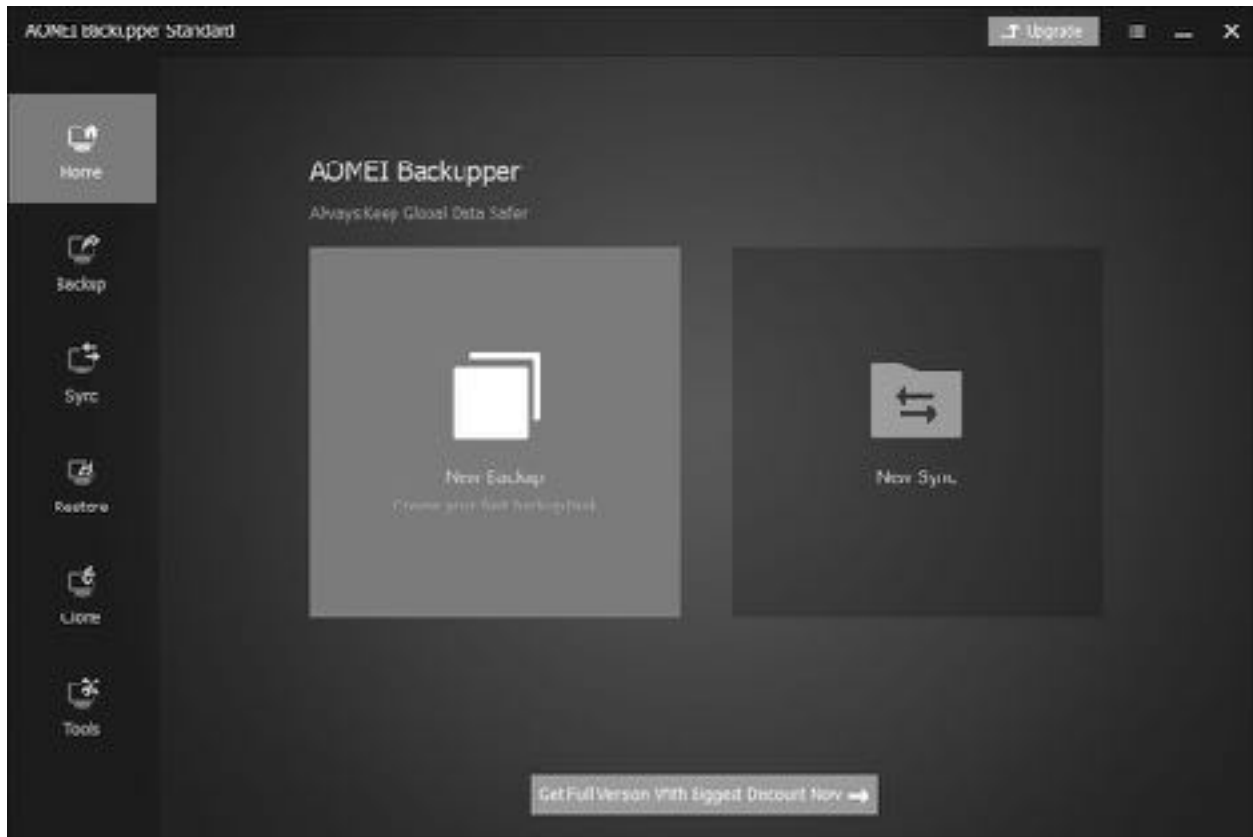


Figure 96: Home screen of AOMEI Backupper

Click the large **New Backup** square and the screen will change to the following. Many of these options are concerned with imaging and recovery rather than everyday backups. Click **File Backup**:

Free edition. Do not copy

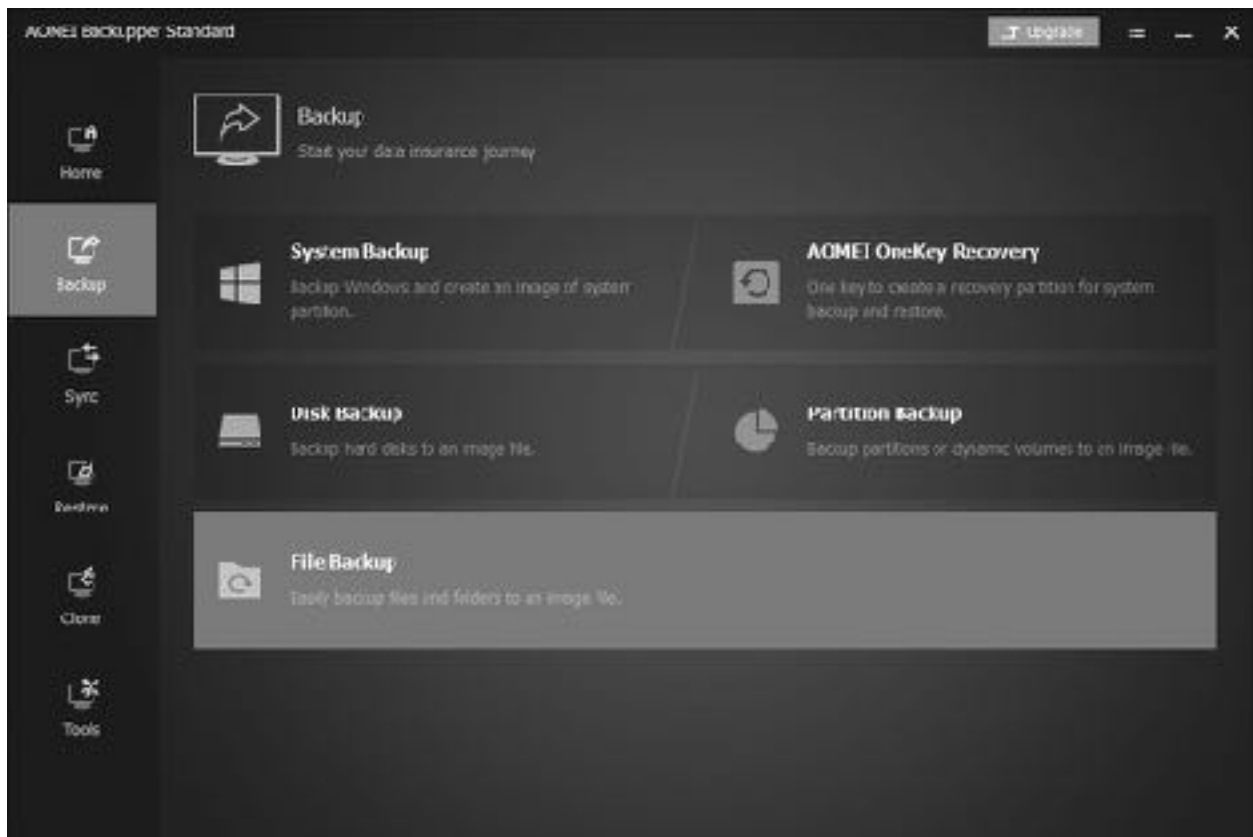


Figure 97: Click File Backup

On the next screen, click the dropdown in the bottom half of the screen and for the destination choose **Select a network location**:

Free edition. Do not copy

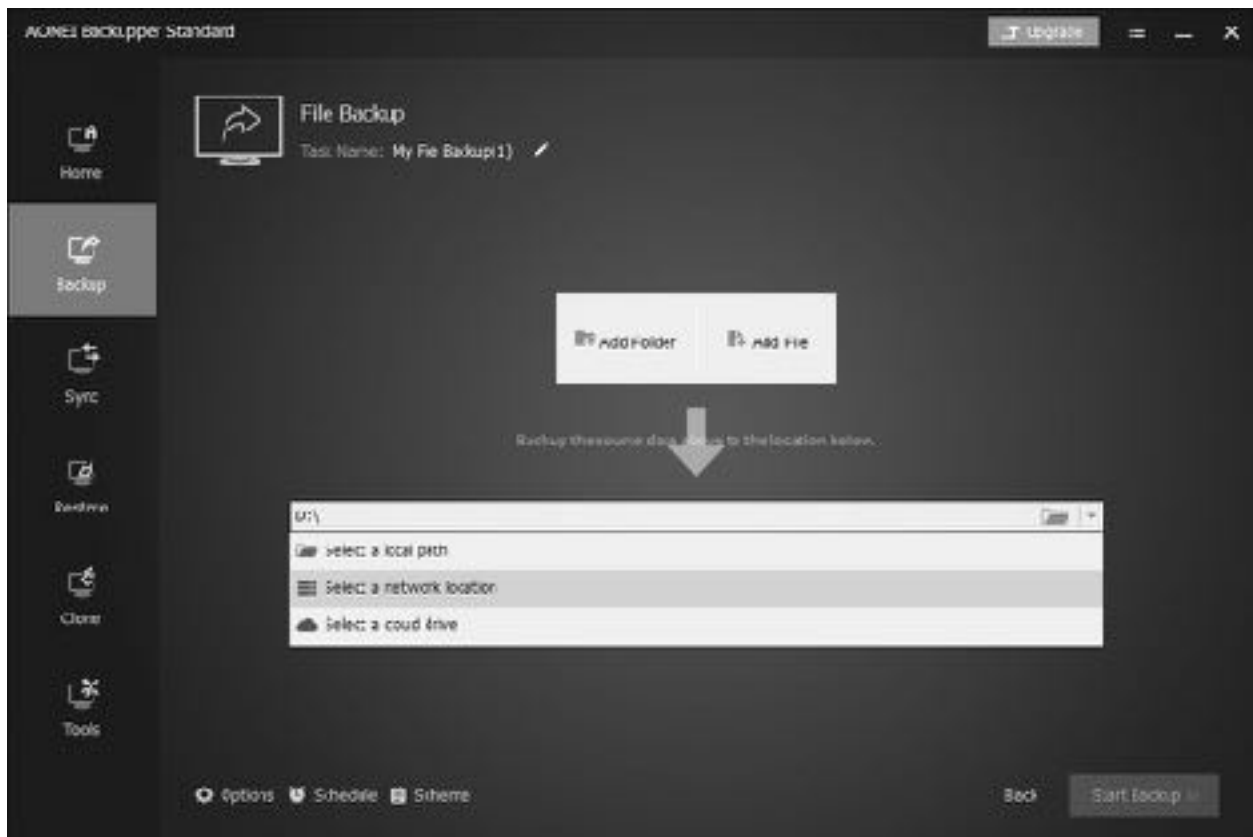


Figure 98: Choose network location

On the resultant panel, click **Add Share or NAS Device**. Specify a *Display Name* – this is just for reference and has no particular significance. Enter the *Network Path*, where the backup will be stored. A sensible choice for this is the user's home folder on the server, as it is unique and private to each user. Enter it in the form of the server's IP address and the user's logon name e.g. `\\192.168.1.2\danielap`. Turn off *Anonymous* by moving the switch to the left-hand position. Enter the user's name and password as defined on the TNAS and click **OK**:

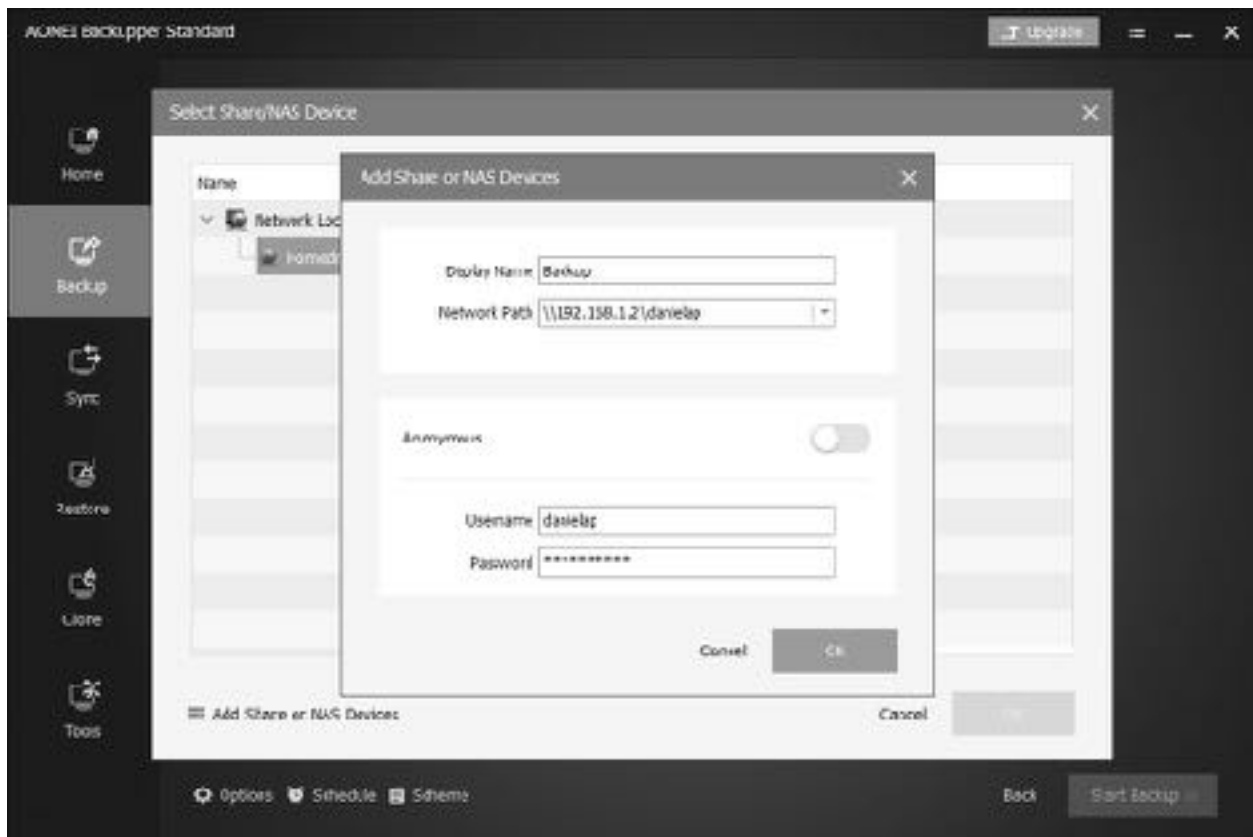


Figure 99: User details and network path

You will be returned to the previous panel – click **OK** and the earlier screen is displayed. Click **Add Folder** and navigate to the folder on the computer that you wish to backup, in this example, the *Documents* folder. You are not restricted to just one folder, so this step of adding folders can be repeated to add further ones to the backup.

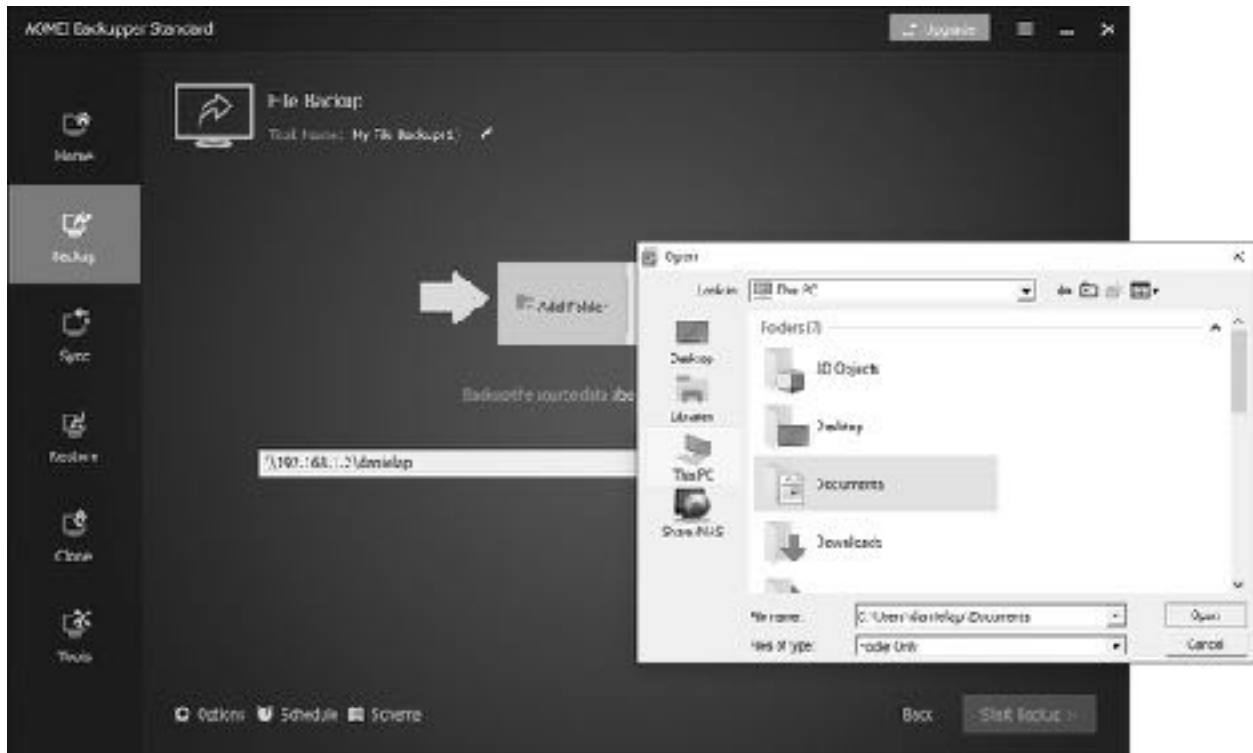


Figure 100: Specify the folders to be backed up

Having completed all the details, click the **Start Backup** button in the bottom right-hand corner of the screen. Whilst the backup is running, a progress screen is displayed. The time taken for the backup is largely dependent on the amount of data.

Thereafter, the backup job is listed on the home screen. To run it again at any point, click the right-pointing chevron. Alternatively, click the three-line menu, where a wider range of options are available:

Free edition. Do not copy

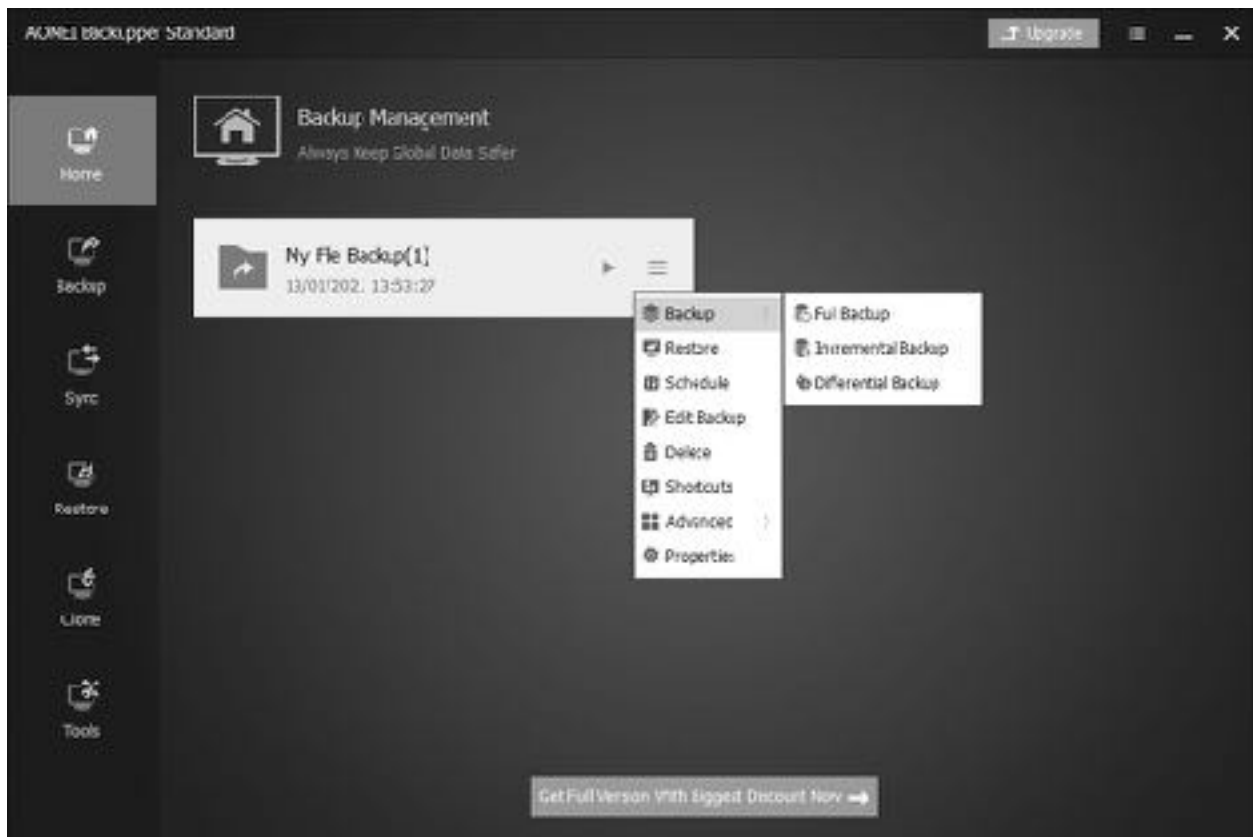


Figure 101: Updated Home screen with backup management options

To schedule regular backups, choose the **Schedule** option from the pop-up menu. The backup could be configured to run daily, weekly, monthly etc.

To restore files from a backup, click **Restore** from the pop-up menu or click the **Restore** icon on the left-hand side of the screen. Choose the folder/files to be restored and click **Next**. On the subsequent screen, specify whether they should be restored to the original location on the computer or to somewhere else. Click the **Start Restore** button to proceed.

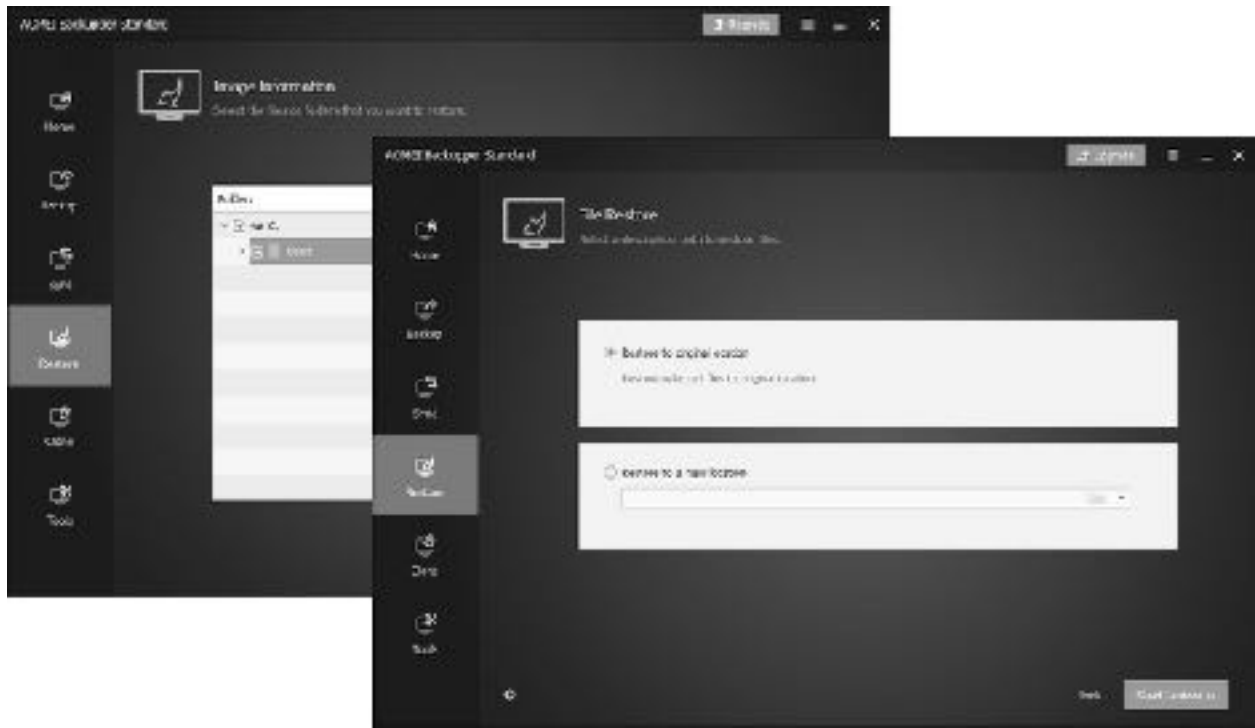


Figure 102: Restoring files

Free edition. Do not copy or dis

Backing up Windows Professional Clients using the built-in Program

Although AOMEI Backupper is a capable program, all versions of Windows include a built-in backup program that some people may prefer to use and this might be a simple matter of preference or familiarity. However, only Professional (and not Home) editions of Windows are able to use network drives. In Windows 7 the program is called *Backup and Restore*, in Windows 8, 8.1 and 10 it is called *File History*. The Windows backup program assumes that you will be using an external USB drive; all that is necessary is to change the backup location so that it points to the user's home folder on the server and thereafter it can be used in the normal fashion.

Windows 7 Professional Clients

Click **Start**, followed by **All Programs**, **Maintenance** then **Backup and Restore**.

Click **Set up Backup**.

Click the **Save on a network** button. On the next panel, enter the **Network Location**. Specify the user's home folder, using the format `\\server\username` or click the **Browse** button to navigate to it. Enter the user name and password as defined on the server then click **OK**.

The subsequent screen is for choosing what data files are backed up. The default option of **Let Windows choose (recommended)** is fine in many cases so just click **Next**.

The follow-on screen is a summary of settings; click **Save settings and run backup**.

The backup will run for the first time, during which the status is displayed. Windows will have defined a schedule to subsequently run backups automatically on a regular basis, but if this setting is not suitable it can be changed by clicking **Change settings**.

Windows 8 & 8.1 Professional Clients

Go into **Control Panel** and click **File History** (in Windows 8.1 you can right-click the **Start** button to find the **Control Panel**).

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

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

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

Windows 10 Professional Clients

Begin by mapping the user's home drive on the server using one of the techniques described in [5 ACCESSING THE SERVER](#).

Click **Start > Settings > Update & security > Backup**. Click **Add a drive** and after a few seconds the list of mapped drives will be displayed – click on the user's home drive. Having done so you will be returned to the main Backup panel, where an option to *Automatically back up my files* will have appeared and been set to *On*. That's it – a backup will now run on an hourly basis, copying the user's files from the computer to their home drive on the server.

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

7.8 Backing Up Macs

Time Machine is the standard backup solution for Mac users, first introduced with Mac OS X 10.5. It was designed to operate with Apple's Time Capsule, a now-discontinued combined router/wireless access point/hard drive. However, support is provided in TOS, allowing the server to be specified as a backup destination for use by Time Machine (macOS) clients.

Begin by creating a dedicated shared folder where the Time Machine backups will be stored, for example called *MacBackup* (how to create shared folders is covered in section [3.2 Creating Shared Folders](#)). All Mac users should have Read/Write permissions to this folder (suggestion: consider creating a group for the Mac users if there are many of them). Consider setting a storage quota for the shared folder – 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 60 GB of disk space. That would give us $10 \times 60 \times 2$ for a total of 1200 GB / 1.2TB space needed to hold the backups, although more space would allow greater backup retention periods.

Next, from the Desktop launch the **Backup** application and click **Time Machine** > **Settings**. Tick the **Enable Time Machine Backup** box. Click the **Select Folders for Backup** button and navigate to the newly created backup folder. Click **Apply** and then **Apply** on the original screen:

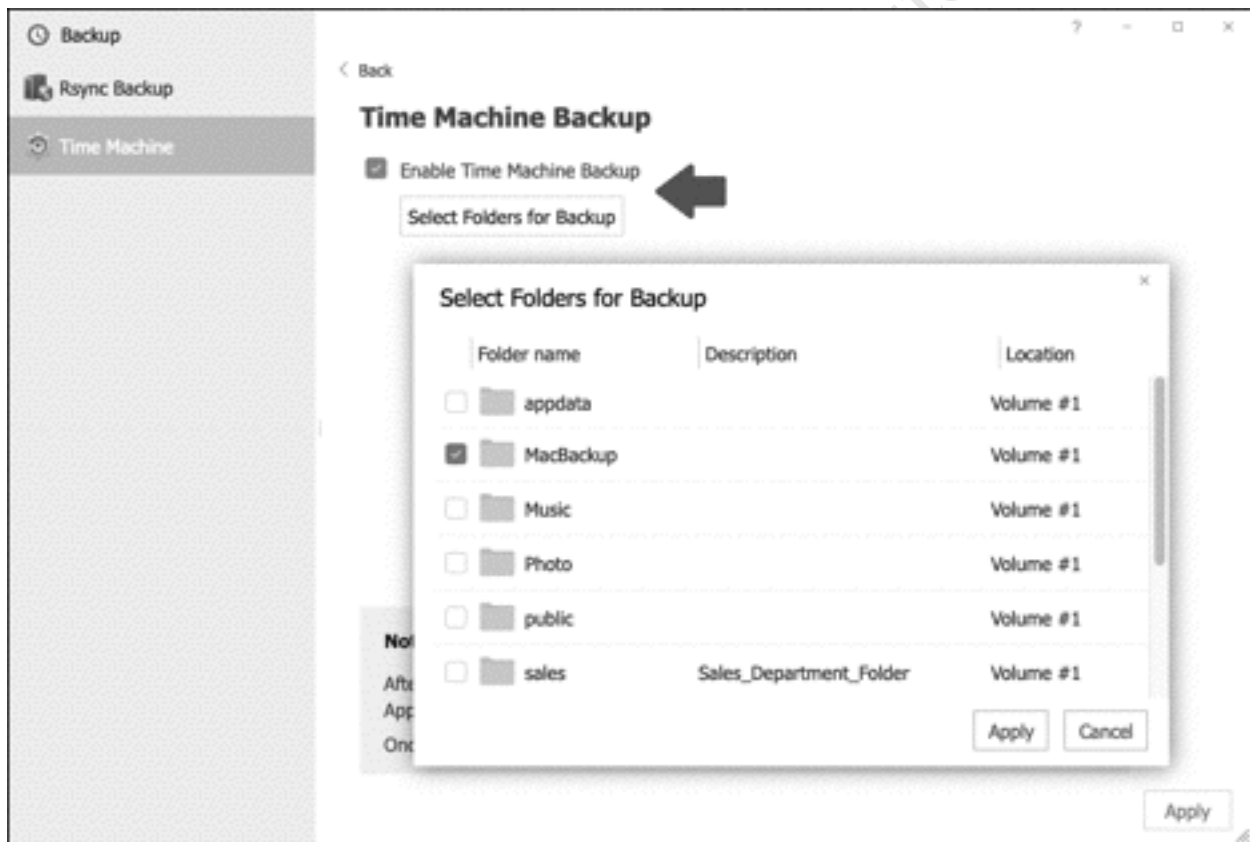


Figure 103: Enabling Time Machine support

To perform a backup, go to a Mac and launch **System Preferences** > **Time Machine** (there may be some minor differences in the screenshot below, depending on which version of macOS is being used). Click **Select Disk** and you should see the backup folder on the server as an option; highlight it and click the **Use Disk** button. It will then be necessary to enter the user's name and password as previously defined on the TNAS.

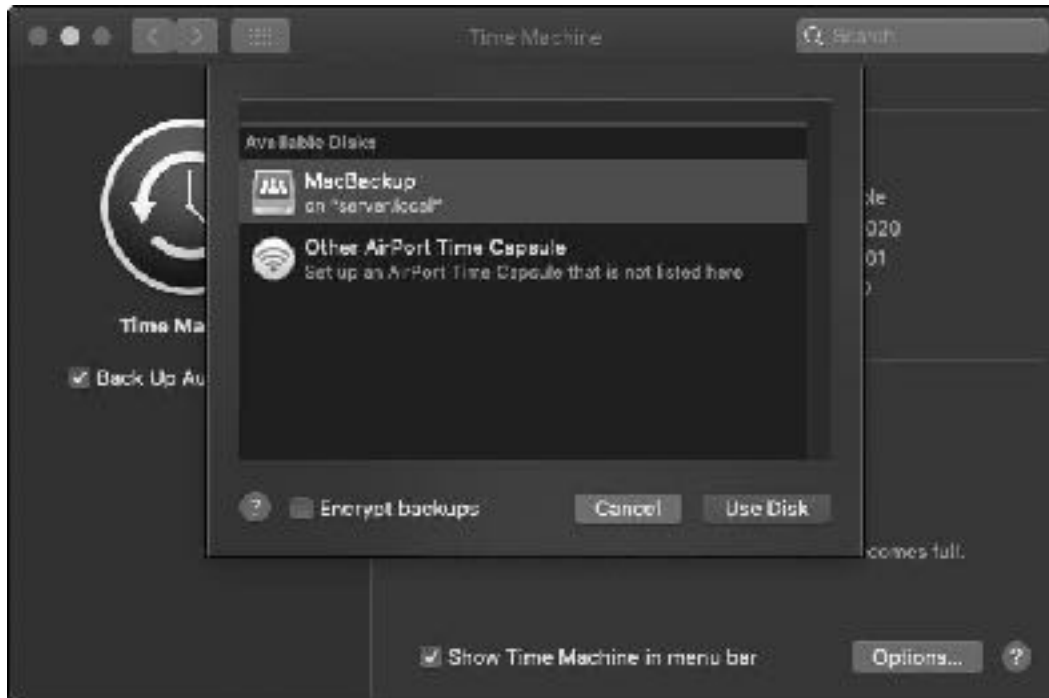


Figure 104: Select backup folder on the server

Thereafter Time Machine behaves in a totally standard method i.e. exactly the same as though you were using Apple's own Time Capsule product or a plug-in USB drive.

Housekeeping can be managed on the TNAS. Within the **Backup** app, click **Time Machine > Backup List** to display a list of backups. To delete a backup – for instance, for purposes of managing disk space on the TNAS – place a tick against it and click **Delete**.

8

HOUSEKEEPING & MAINTENANCE



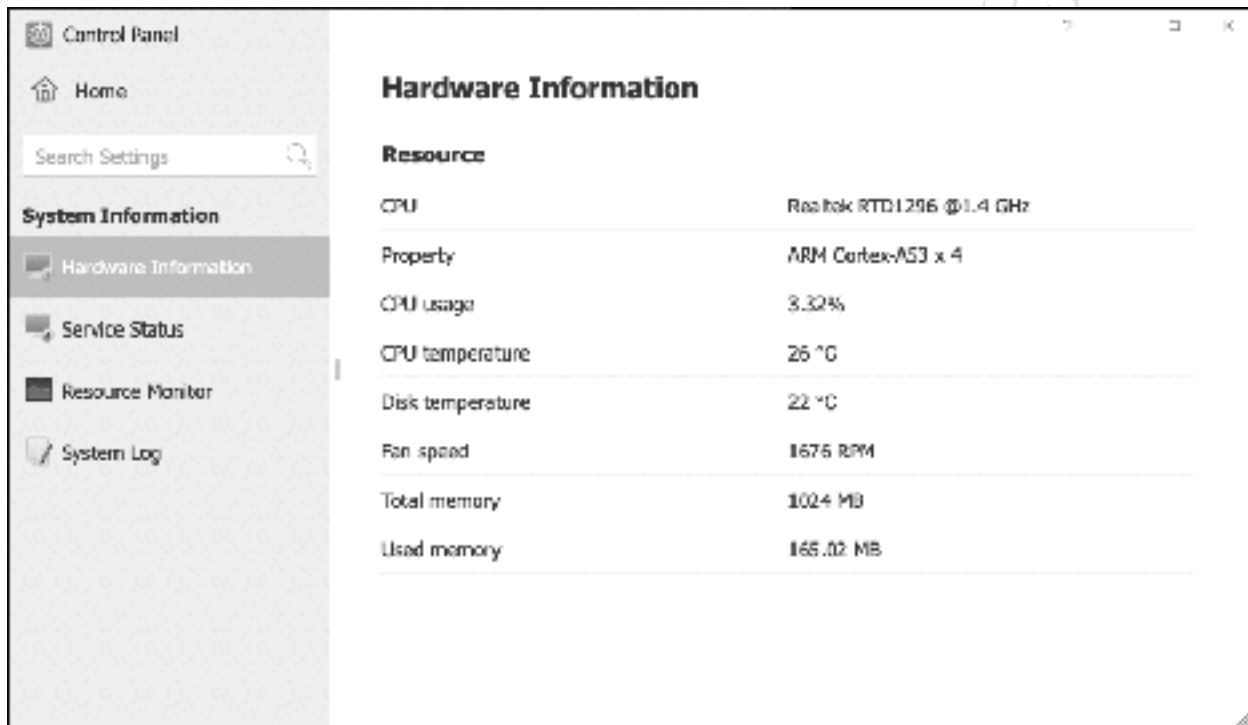
Free edition. Do not copy or distribute. (c) CTACS

8.1 Overview

The server should be checked on a regular basis to ensure there are no problems. In the case of a home system this only needs doing every few weeks, but in a business environment a more systematic approach is better, say once a week at least or maybe even a daily check. Things that can be usefully looked at include checking for TOS Updates, storage space, health of disk drives, confirmation that the backup has completed successfully, log files generated by anti-virus scans, plus possible security issues and violations.

8.2 Hardware Information

The *Hardware Information* screen provides a quick summary of the hardware status of the TNAS, including its operating temperature, fan speed and memory usage. As such, it provides a useful ‘at a glance view’ which may be of help in identifying problems. It is accessed by going into **Control Panel > Hardware Information**:



Hardware Information	
Resource	
CPU	Realtek RTD1296 @1.4 GHz
Property	ARM Cortex-A53 x 4
CPU usage	3.32%
CPU temperature	26 °C
Disk temperature	22 °C
Fan speed	1675 RPM
Total memory	1024 MB
Used memory	165.02 MB

Figure 105: Hardware Information

The *CPU temperature* and *Disk temperature* are of interest. If they are consistently high, try increasing the fan speed (see [2.5 Power Management](#)) or locate the TNAS in a cooler location.

If the amount of *Used memory* is high relative to the *Total memory*, which might be the case if there are many applications open and many users of the system, then one option might be to upgrade the memory (RAM) if this option is available on the model.

8.3 Service Status

The *Service Status* screen shows which services are currently running on the TNAS and it accessed by going into **Control Panel > Service Status**:

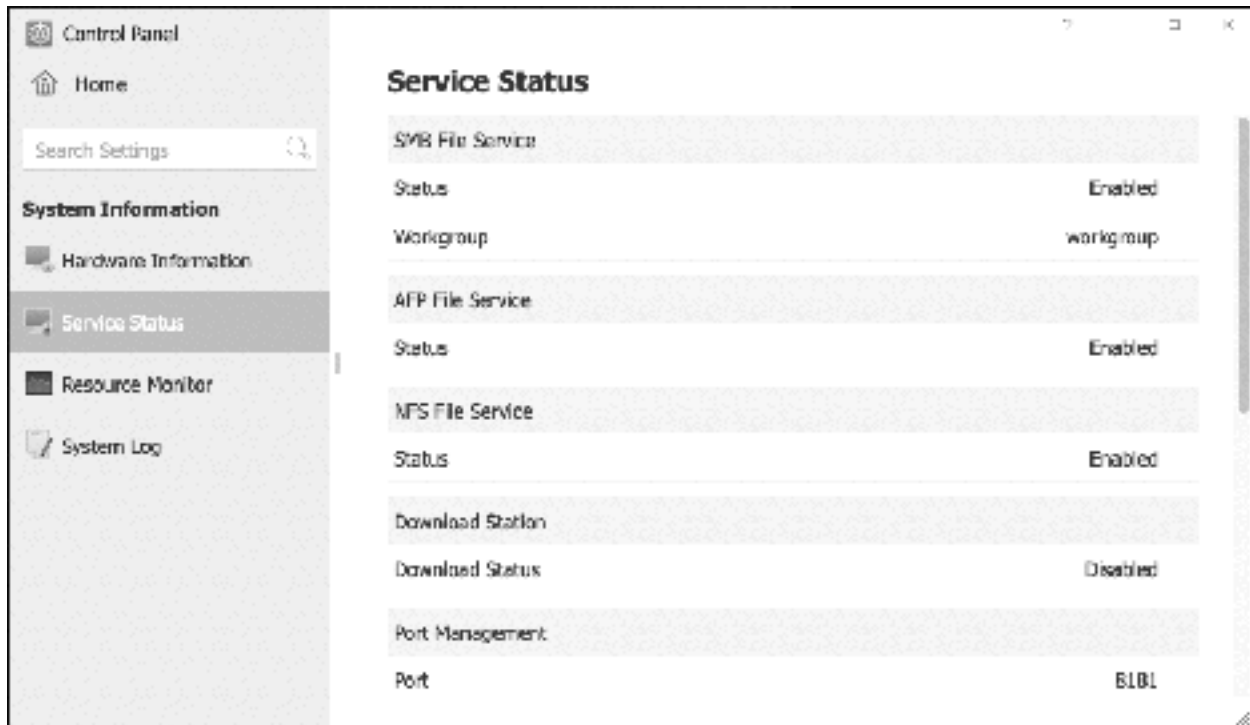


Figure 106: Service Status

Some services are optional or unnecessary and disabling them can free up memory and improve security. However, this cannot be done from here and it is necessary to go elsewhere in Control Panel to change matters e.g. see section [6.7 Disable Unused Connectivity Services](#).

8.4 Resource Monitor

The *Resource Monitor* is used for monitoring the performance of a TNAS and is similar to tools provided in other computing environments, such as the Task Manager in Windows or Activity Monitor in macOS. It monitors CPU, Memory, Storage and Network (Bandwidth) utilization amongst other things. This information can be of use when diagnosing problem or identifying bottlenecks in a poorly performing system; for instance, if the TNAS is short of memory then a RAM upgrade might be appropriate. To launch Resource Monitor, click on its icon in **Control Panel**. Each of the topics has its own tab and clicking on it will result in a larger screen of more detailed information:

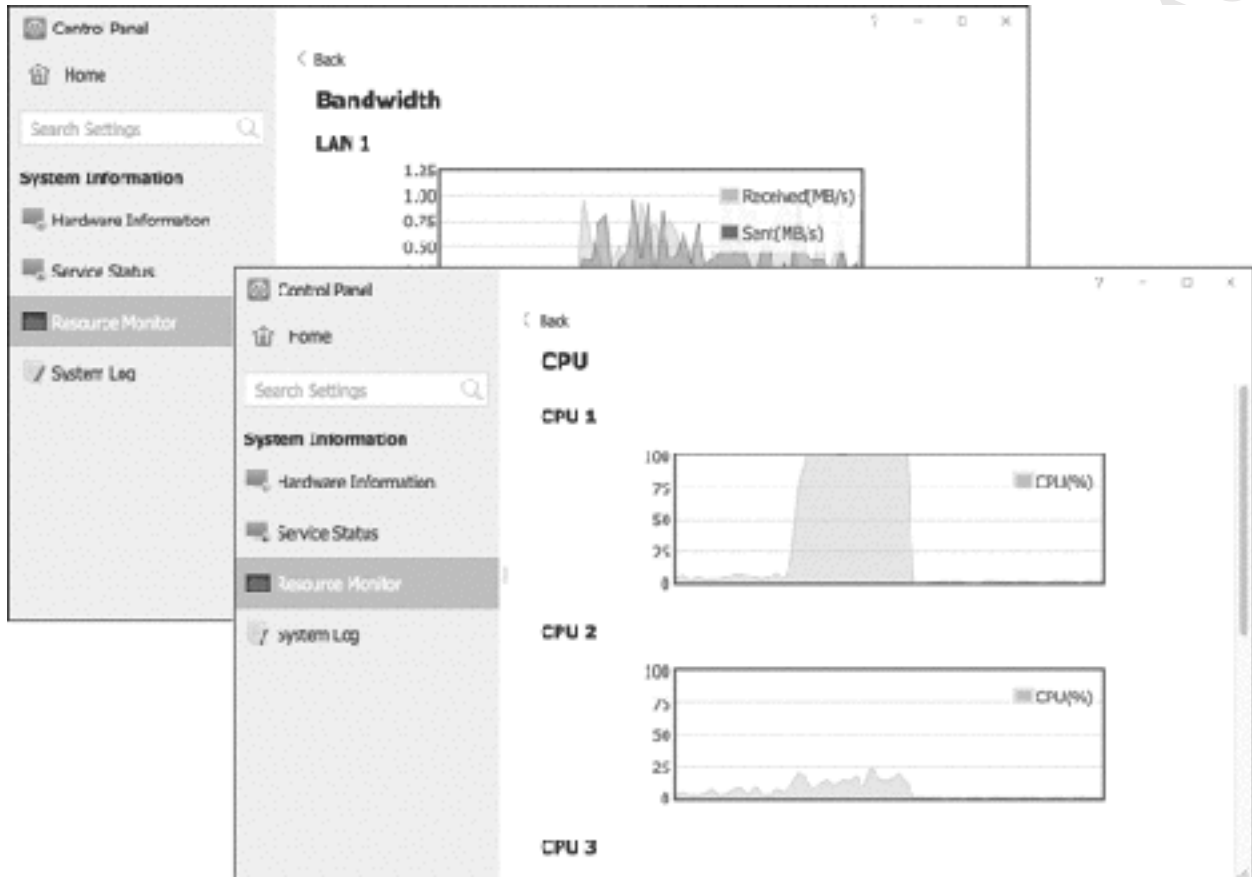


Figure 107: Resource Monitor

The fifth tab – *Process* – lists the processes running on the TNAS. If the server appears busy or is performing slowly, this can help identify the culprit(s) which are using excessive CPU or memory.

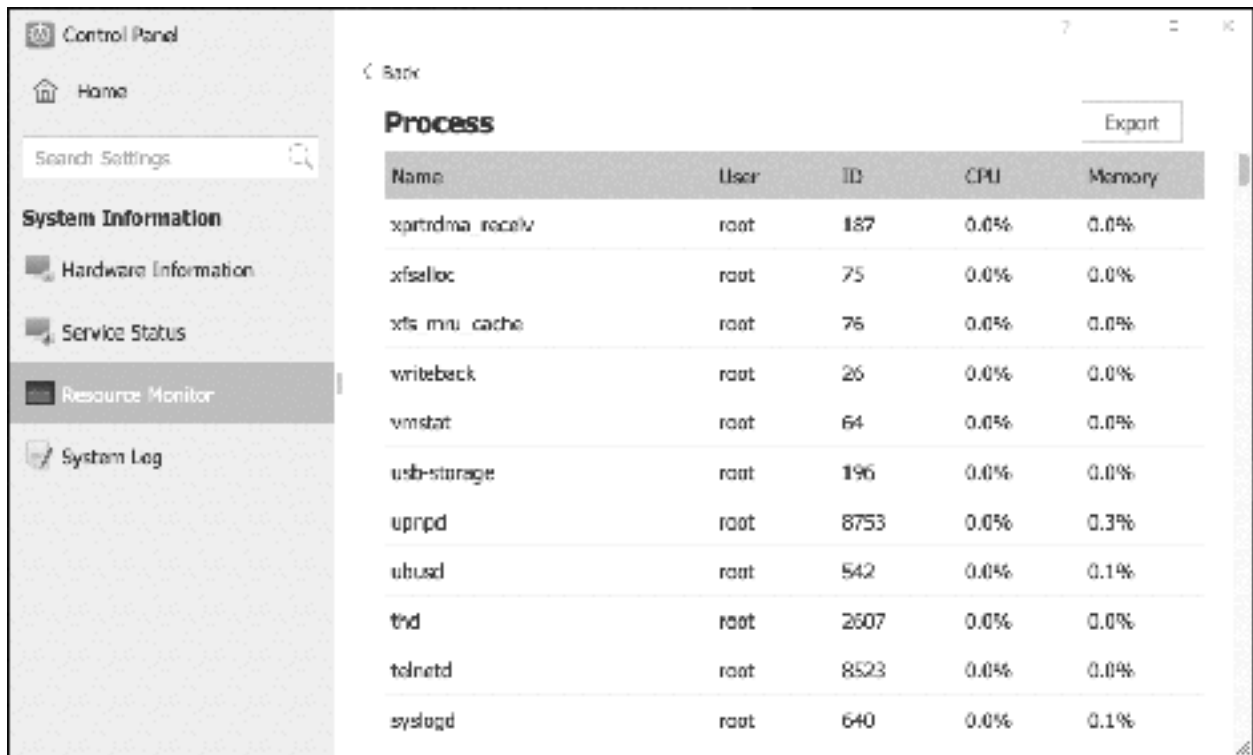


Figure 108: Process tab within Resource Monitor

Free edition. Do not copy or

8.5 System Log

To see who has been using the system, go to **Control Panel > System Log**. This lists all logon attempts by service type e.g. Samba, FTP, Telnet and so on. To restrict the view to just one service type, use the **Services** dropdown. The log should be cleared down on a regular basis e.g. once a week; to do so, click **Clear**. You can also click **Export log** to generate a permanent copy in Excel spreadsheet format.

Type	Time	User	IP	Port	Event
HTTP	2021-01-09 07:...	admin	192.168.1....	63310	Login S...
HTTP	2021-01-09 07:...	admin	192.168.1....	63288	Web Lo...
HTTP	2021-01-08 18:...	admin	192.168.1....	62214	Web Logout Successful!
HTTP	2021-01-08 18:...	admin	192.168.1....	62160	Create folder[sales] Successful!
HTTP	2021-01-08 17:...	admin	192.168.1....	62123	Create group[sales] Successful!
HTTP	2021-01-08 17:...	admin	192.168.1....	61978	Edit User[andrewp] Privileges!
HTTP	2021-01-08 17:...	admin	192.168.1....	61978	Create user[andrewp] Successful...
HTTP	2021-01-08 17:...	admin	192.168.1....	61978	Edit User[maryo] Privileges!
HTTP	2021-01-08 17:...	admin	192.168.1....	61978	Create user[maryo] Successful!
HTTP	2021-01-08 17:...	admin	192.168.1....	61978	Edit User[gustavh] Privileges!

Total 165 / Display 10 Per Page

Figure 109: System Log

8.6 Checking Disk Health

The health of the hard drives in the TNAS should be checked on a regular basis, especially if there appear to be problems or if the TNAS has shut down unexpectedly for any reason. To do so, go to **Control Panel > Hard Drive**, which will display a list of the hard drives and their status on the **Hard Drive** tab. The first time this done following a reboot, the status of the drives will be automatically checked and updated:

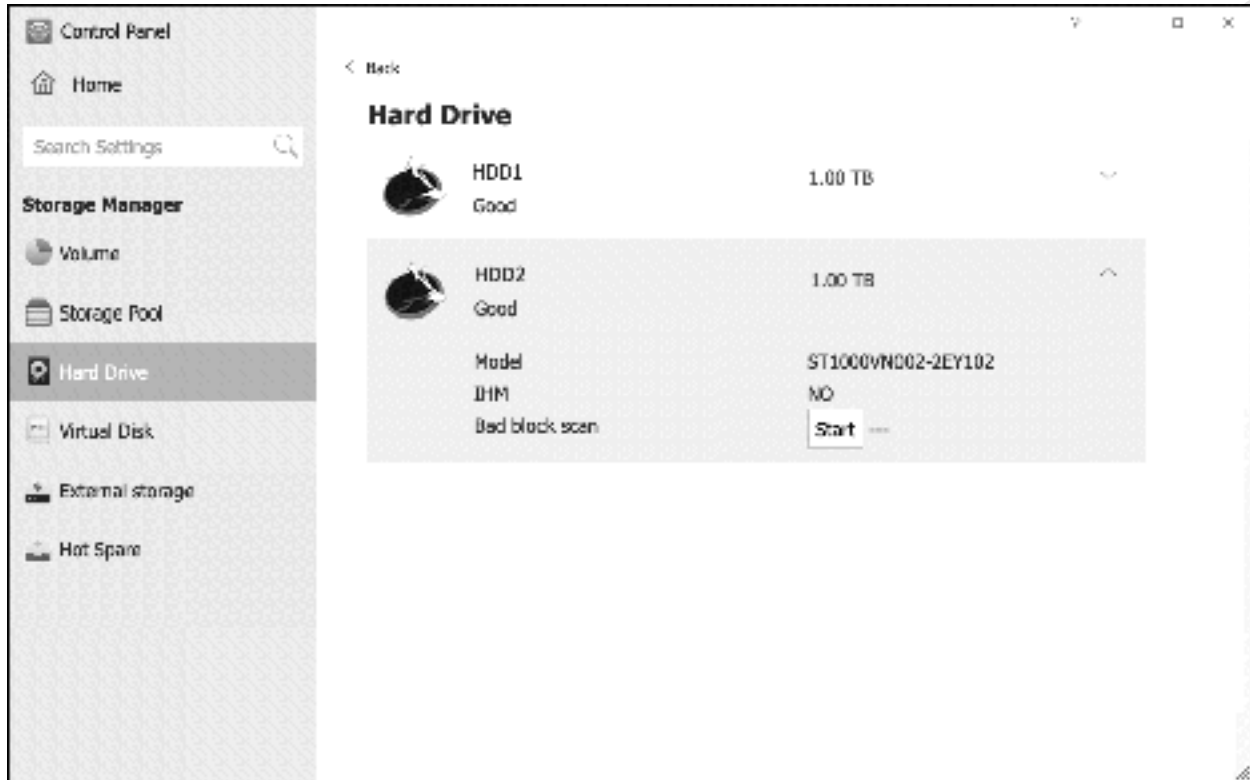


Figure 110: Hard Drive status

The status of a drive should always be ‘Good’. If it is not, expand the section by clicking on the chevron on the right-hand side of the screen and run a *Bad block scan* by clicking the **Start** button against the drive. The time taken to run a bad block scan depends upon the capacity of the drive but can be lengthy and it is possible that the overall performance of the TNAS will be reduced during this process. If this does not fix the problem, replace the drive. For information about making changes to storage, see section [10.3 Making Changes to Storage Pools](#).

For more detailed information, go into the **Disk S.M.A.R.T.** section (**Control Panel > Hard Drive > Disk SMART**). ‘S.M.A.R.T.’ is the abbreviation for *Self Monitoring Analysis and Reporting Technology* and is a mechanism by which hard drives monitor their own status and report it back to computer systems. If the system has multiple drives installed, select the one to test using the dropdown option:

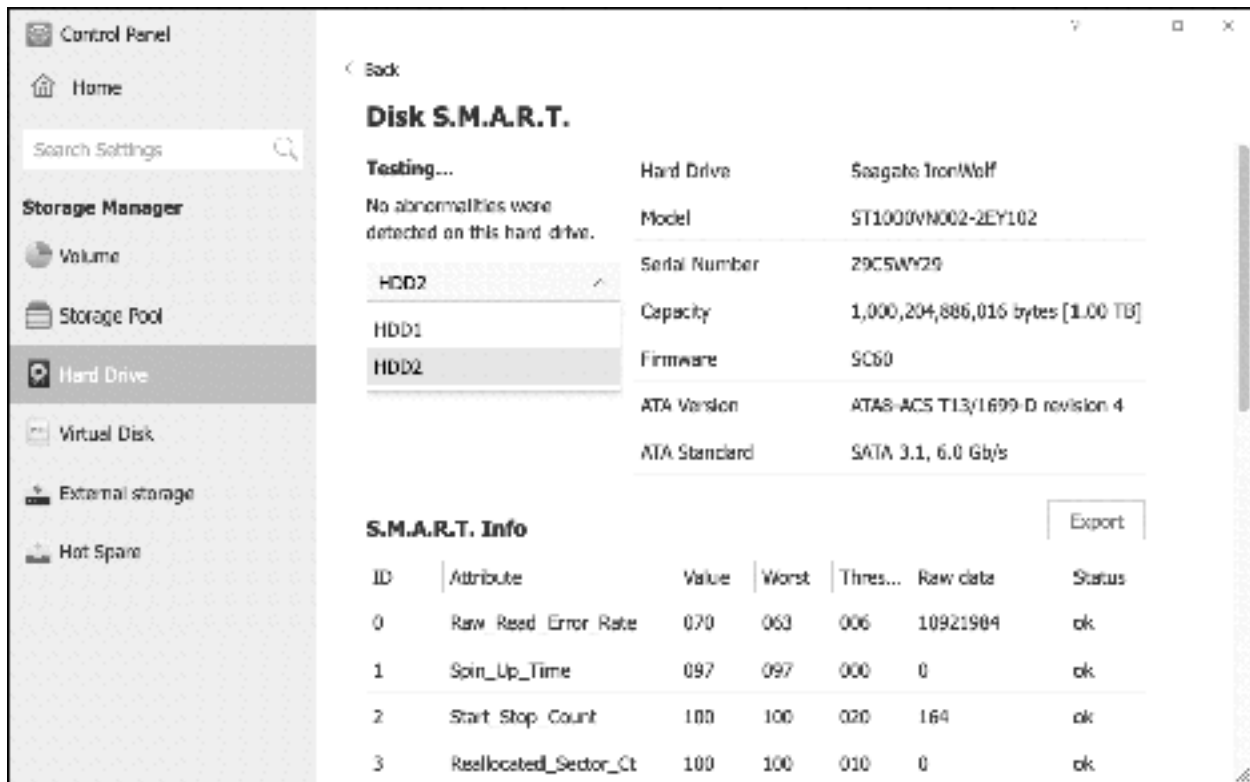


Figure 111: S.M.A.R.T. status

If a drive fails the S.M.A.R.T. test and has a status of 'RISK', then it should be replaced at the earliest opportunity.

Free edition. Do not copy

8.7 Checking for TOS Updates

The TOS software is updated on a regular basis by TerraMaster. Updates may be major e.g. from TOS 3 to TOS 4, although typically these only occur every couple of years. Significant updates e.g. from TOS 4.2 to TOS 4.3 are more frequent, perhaps once a year. Additionally, there are more rapid minor updates to fix problems and improve functionality and these are made available by TerraMaster as necessary e.g. 4.2.08 to 4.2.09.

To control and check for TOS updates, go into **Control Panel > Update & Recovery > Software Update**. The panel displays the current TOS version and allows you to choose between **Online update (recommended)** or **Manual update**. TerraMaster advise the use of Online update; if you use this option you can also force it to check for new software at any point by clicking the **Apply** button:

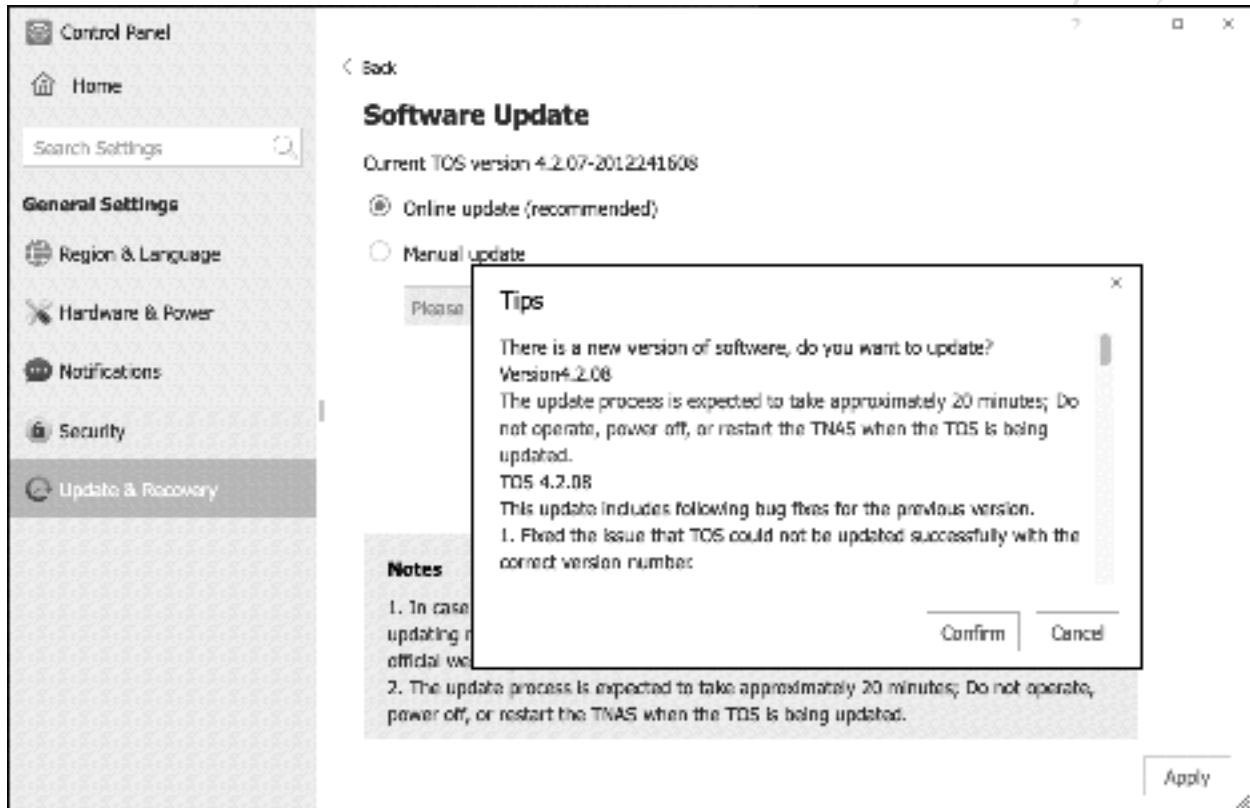


Figure 112: TOS Software Update

However, in some circumstances, you may prefer to use *Manual update*. There are four scenarios in which you might want to do this:

1. Whilst keeping TOS up-to-date is recommended for most installations, a more cautious approach to updating may be required to avoid disruption, particularly in a business environment.
2. There may be a need to use an earlier version of the TOS software.
3. The update is being done in an offline mode, using a previously downloaded version of TOS.
4. The online update does not work, in that the latest version of the software is not detected (this seems to be a common problem).

In such instances, the required copy of the TOS firmware should first be downloaded using a computer. From the TerraMaster website, click the **Download** link. Select your model. On the subsequent screen, there may be several variants available e.g. the latest and previous versions; each of these in turn may have two options: the complete package, including the setup components, and the system update

(firmware) only. For an existing, working system, you would download the latter. Returning to the TNAS, choose **Manual update**; click the **Browse** button and navigate to the downloaded software; click **Apply**.

TerraMaster also make available test or 'beta' versions of forthcoming TOS releases. If you wish to participate, tick the appropriate box on the Software Update screen. Beta versions are not suitable for use on production or important servers.

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

8.8 Notifications

Significant events generate notifications, which can be viewed by clicking the small ‘speech bubble’ in the top right-hand corner of the screen, which will cause it to expand. They may also cause the system buzzer – indicated by the bell icon – to flash and buzz. Some notifications have links within them, which can be clicked to obtain more information or invoke the underlying utility responsible for generating the notification. For instance, in this example a message has been generated by Storage Manager and clicking the link will take you to it.

To clear the notifications, click the **Clear All** button at the bottom of the Notifications panel.

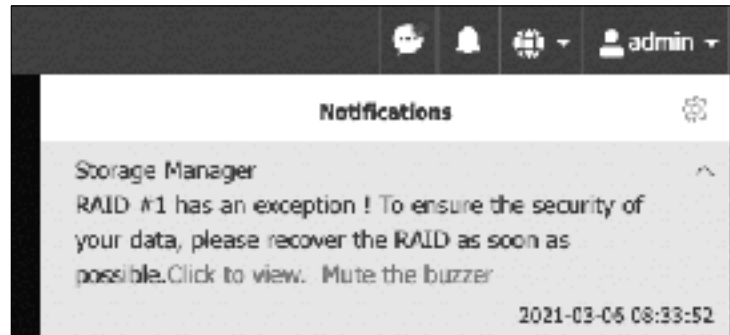


Figure 113: Notifications

To control which type of events are reported upon, click the **Settings** cogwheel at the top of the screen. Place or remove ticks against the different classifications, followed by **Apply**.



Figure 114: Event categories

Configuring Email Notifications

It is important to check the TNAS on a regular basis, but this may not always be practical. For instance, the person who looks after the system – you, perhaps - may not be located in the premises. Also, it is better to deal with some problems sooner rather than later. For these reasons, TOS can proactively advise when issues occur – referred to as ‘exceptions’ by TerraMaster – using automatic notifications sent out by email.

To set this up, go to the **Control Panel** and click **Notification**. Tick the **Enable alert notification** box and enter up to two recipient email addresses. Click the **Test Email** button and a test email should shortly be received. Allow a couple of minutes, plus check the Spam/Junk email folders if it has not arrived.

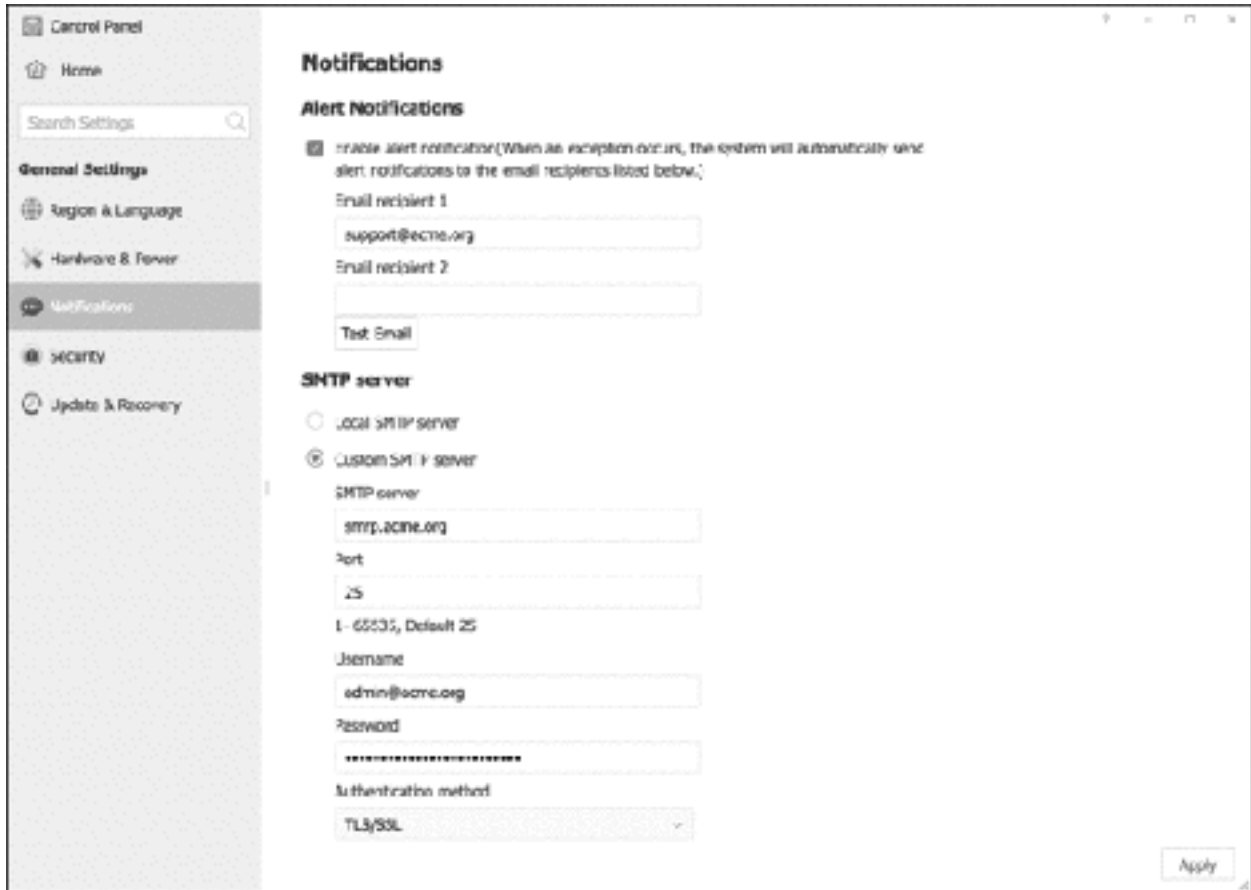


Figure 115: Configuring email notifications

These email notifications are sent via the TerraMaster email server. If you prefer to use your own organization's email service, expand the SMTP server section on the screen and tick the **Custom SMTP server** option. If SMTP is used then it is necessary to enter the details of the SMTP server (name, port number, email address and password, protocol type), which should be available from whoever runs or controls your email service. Having made change, click the **Apply** button.

9

MULTIMEDIA & STREAMING



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

9.1 Overview

One of the most popular uses of a home network is for the storage and playback of media such as photos, music and videos. CDs and DVDs can be “ripped” into formats such as MP3 and MP4 and these copies played back from the TNAS, thus protecting the originals against wear and tear. By maintaining a central library, the entire family can access their media from both inside and outside the household. The TNAS is able to playback the stored media onto a variety of devices including computers, gaming consoles, smart TVs, streaming TV devices and suitably equipped audio systems. For playback on smartphones and tablets, the TNAS Mobile app can be used (see [5.10 Connecting Smartphones and Tablets with TNAS Mobile](#)).

9.2 DLNA Media Server

DLNA stands for *Digital Living Network Alliance*. It is a widely used standard for interconnecting home network devices in order that they can stream and play multimedia, with the design goal that DLNA devices can do so without worrying about passwords, network protocols and other technical issues. Many devices are DLNA-compliant including computers, smart televisions, media streamers, gaming boxes such as the Xbox and PS4, smartphones, Blu-ray players, suitably equipped audio systems and more. TerraMaster have an application – *DLNA Media Server* – which turns the TNAS into a DLNA server.

Download and install DLNA Media Server from the Applications store. It will place an icon on the desktop, from where it can be launched. There are four options, listed down the left-hand side of the screen:

Overview – a summary screen. Initially it is empty, as the media server will be disabled by default

General – the most useful screen, used for configuring the DLNA Media Server

Browser Settings – this refers to browsing for media when using DLNA client devices and how the media will appear, and is unconnected with internet browsers such as Chrome, Safari etc.

Format Compatibility – additional configuration options

Initially DLNA Media Server will be disabled, so click **General** and on the resultant screen tick the **Enable Multimedia Server** box. Underneath it is a section to specify the shared folders that hold the media files – use the left and right arrow keys to change the status of folders between ‘Available’ and ‘Enabled’. However, TerraMaster have thoughtfully arranged matters such that the very act of enabling the multimedia server will result in the automatic creation of three shared folders called *Video*, *Photo* and *Music*, with access for the *allusers* group, and this will be sufficient for many people’s needs. The *Port* number and *SSDP Broadcast Interval* should be left at the default values. Click **Apply**:

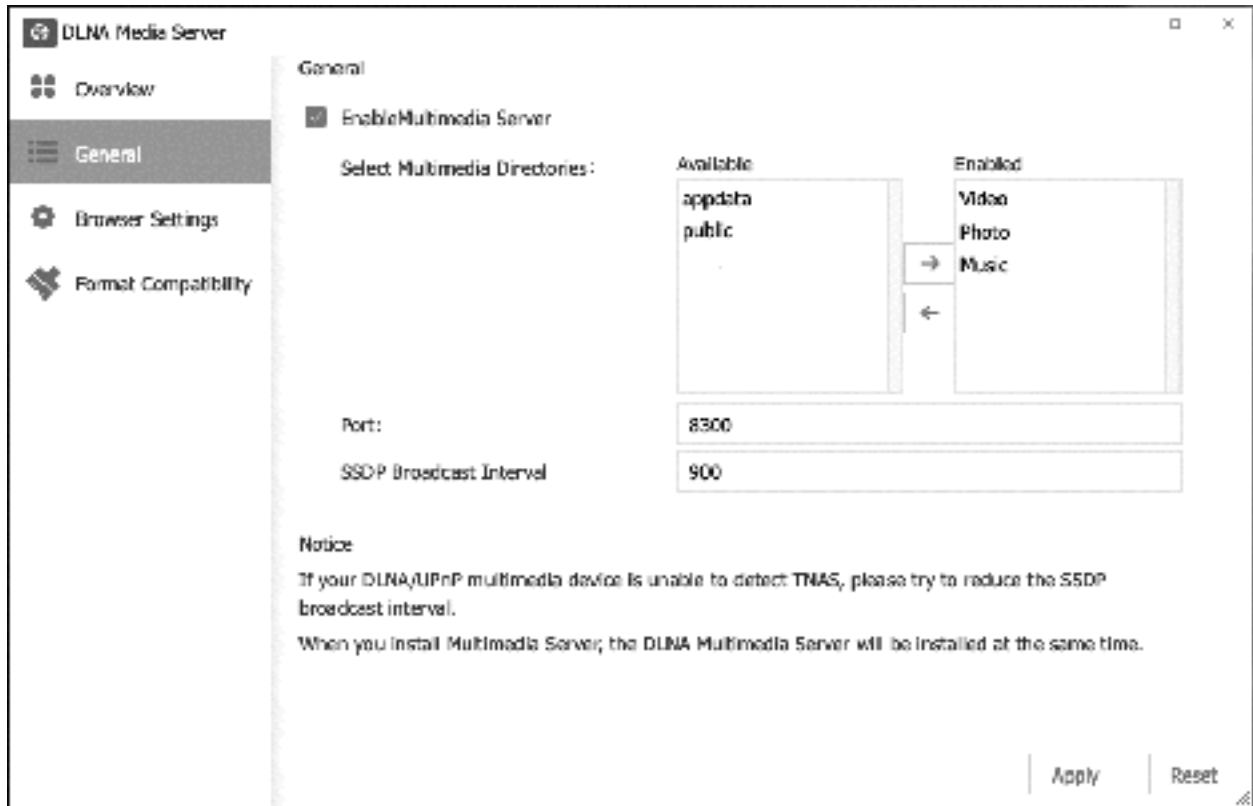


Figure 116: DLNA Media Server, General screen

After a few seconds, click **Overview** to return to the main screen, which will now appear along the following lines:

Free edition. Do not copy

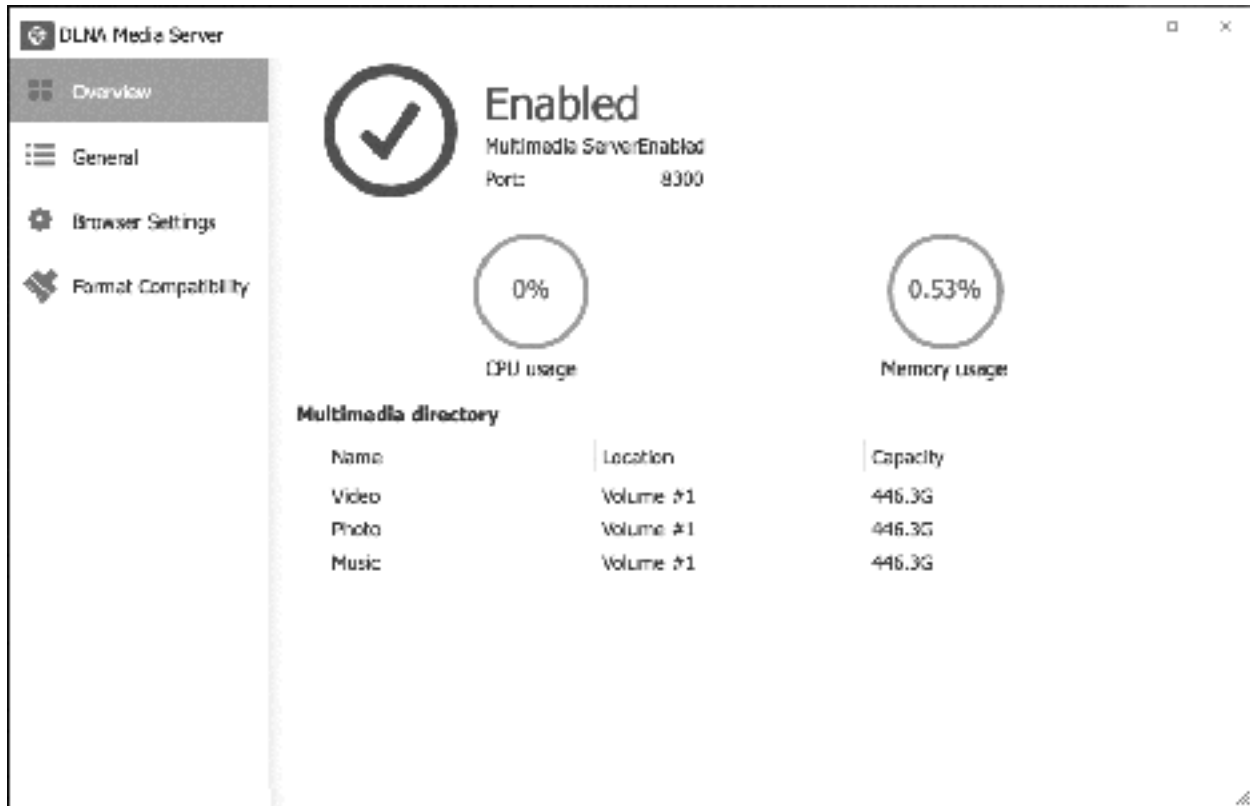


Figure 117: DLNA Media Server, Overview screen

At this point you should be able to connect your DLNA client to the server. As DLNA devices vary considerably, there is no single method for doing so. Some clients, for instance Windows PCs, will see the media server within Windows Explorer/File Explorer. Double-click the server entry and the computer's default media player should open – you should then be able to access photo, music and videos. In the case of Windows Media Player, the server will be listed underneath the *Other Libraries* section. In the case of Windows 10, Groove Music should be configured to point at `\\server\music`, Photos should be configured to point at `\\server\photo` and Films & TV configured to point at `\\server\video`. On other devices, such as smart TVs and set-top boxes, it may be necessary to explicitly go into network settings or there may be an option to search for media servers - refer to the manufacturer's instructions or website for details.

9.3 iTunes Server

Apple's iTunes is a popular choice for listening to music on PCs and Macs. Begin by copying your music to the server. If you are also running DLNA Media Server as described in the previous section, there will be a shared folder called *Music* that can be used. Otherwise, create a shared folder with this name and give access to all users, as described in section [3.2 Creating Shared Folders](#). Having done so, download and install the *iTunes Server* from Applications (see section [11.2 Applications](#)). Launching the app will display the following screen:

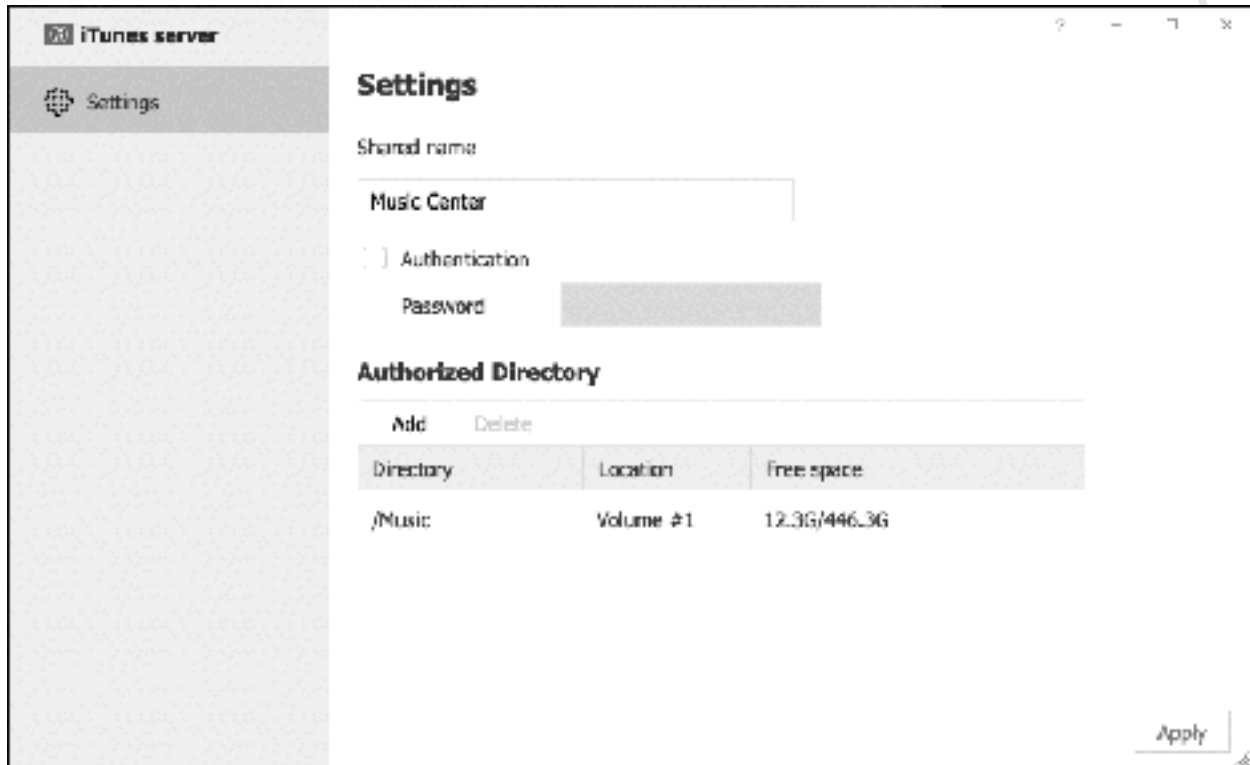


Figure 118: iTunes Server screen

There is no particular reason to change the *Shared name*, which by default takes the name *Music Center*, although you can do so if you wish (for example, to *server*). An authentication password is not required unless you want to restrict access to the music for some reason e.g. because of explicit lyrics or in a work environment.

By default, the app will use *public* as the Authorized Directory i.e. the shared folder. To change this, highlight *public* and click **Delete**. Then, click **Add**, select another shared folder from the dropdown, click **Save**. If desired, you can add multiple folders. Returning to the main screen, click **Apply**.

To access the media from another computer:

macOS 10.15 onwards

Launch *Music*. On the left-hand side of the screen, click the Library section and change it from '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.

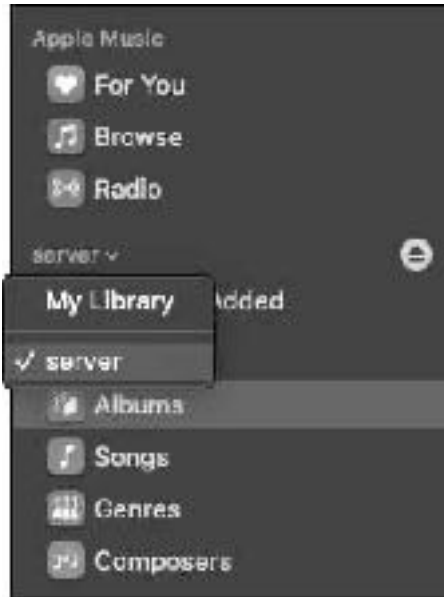


Figure 119: Connect to Music on the server

macOS before 10.15, or Windows PC

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 Mac. Launch iTunes. 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.

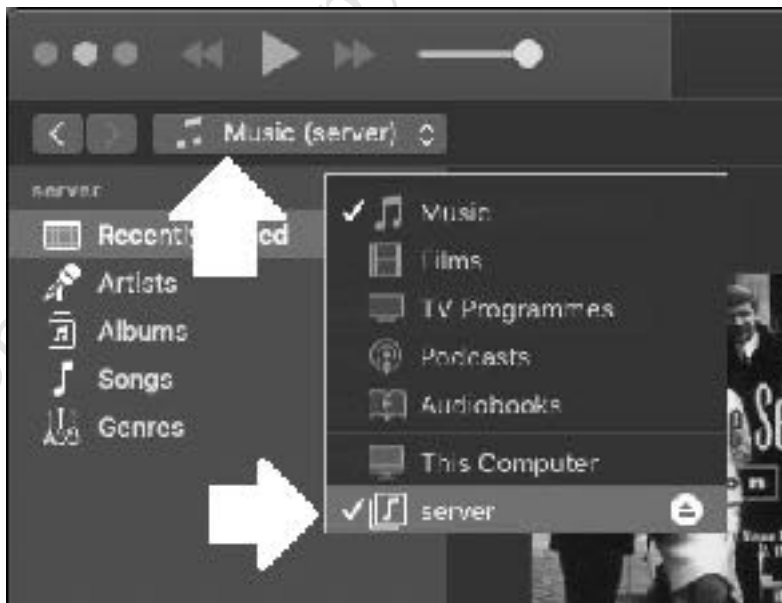


Figure 120: Connect to iTunes server from iTunes

As mentioned in the opening sentence, this works for PCs and Macs. Due to the way iTunes operates, it is **not** possible to directly access the shared library from an iPhone or iPad. Instead, use the TNAS Mobile app as described in [5.10 Connecting Smartphones and Tablets with TNAS Mobile](#) to play music from the server.

9.4 Plex and Emby Server

In addition to the DNLA Media Server, there are third-party alternatives available for download from Applications. *Plex Media Server* and *Emby Server* provide additional and improved capabilities, interface to a wider variety of devices for playback, and may be more familiar or preferable to some people. Both of these are cross-platform systems which, although they run on TNAS, were not specifically designed with it in mind and hence operate differently to native TOS packages. Some people specifically invest in a NAS system just in order to run Plex or Emby. Some of their features include:

- Ability to consolidate all your media – videos, music, photos – in one place
- Support for virtually all media types and file formats
- Access to your media from any location worldwide
- Mobile Sync, enabling media to be viewed offline on tablets and smartphones
- Share media with friends and family
- Parental controls
- Customizable playlists
- Access to live TV, with recording (DVR) capabilities

In order to use Plex Media Server or Emby Server, it is necessary to have an account with the respective companies. Also, some features require a paid subscription.

Plex or Emby can be downloaded and installed from Applications in the same way as any other app. Plex and Emby clients, for connecting devices to the server, are available for Windows, Internet Browsers, Android, iOS, Apple TV, Roku, Amazon Fire TV, Chromecast, Xbox, PlayStation, NVidia Shield and selected smart TVs; however, these have to be loaded from the companies' websites or from the appropriate app stores.

10 STORAGE



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

10.1 Overview

The first section of this chapter is an overview of RAID, whilst the remainder of the chapter explains how to configure and use various storage options, including making changes to Storage Pools, changing a drive, setting up and using Snapshots, working with iSCSI virtualized storage and SSD caching.

10.2 RAID

RAID is short for *Redundant Array of Independent (or Inexpensive) Disks*. The basic idea is to improve reliability and performance through the use of multiple drives to provide redundancy (protection against drive failure) and share the workload. There are various types of RAID and they referred to using a numbering system i.e. RAID 0, RAID 1, RAID 5 and so on. TerraMaster support many different RAID levels and depending on the model and the physical drives installed, the following RAID levels might be available: RAID 0; RAID 1; RAID 5; RAID 6; RAID 10; JBOD.

RAID 0 consists of two identical drives. When data is written, some goes on one drive and some goes on the other. As both drives are being written to (or subsequently read) simultaneously, throughput is maximized. However, as sections of files are scattered across the two drives, if one drive fails then everything is lost. Also, the speed of the disk drives may not be a bottleneck in some NAS systems. For these reasons, RAID 0 on its own is not commonly used. In a RAID 0 system, the total usable storage amount is equal to that of the total drive capacity installed. For example, if a NAS has two 4TB drives installed then the total amount of usable storage capacity is 8TB.

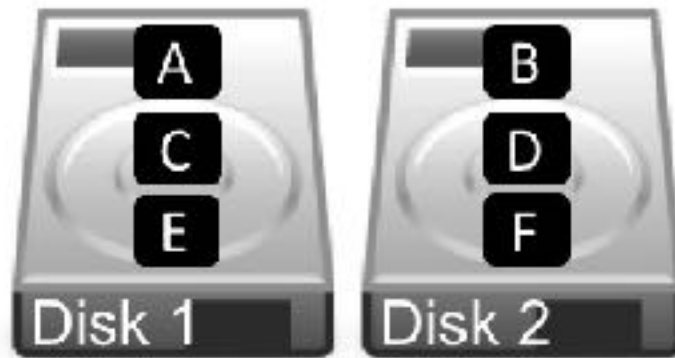


Figure 121: RAID 0 – Data striped across two drives

RAID 1 consists of two identical drives that mirror each other. When a file is saved there are physically two separate but identical copies behind the scenes, one held on each drive, even though you can only see one as the mirroring process itself is invisible. If one of the drives fails, the second one automatically takes over and the system carries on without 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 server has two 4TB drives installed then the total amount of usable storage capacity is 4TB rather than 8TB.

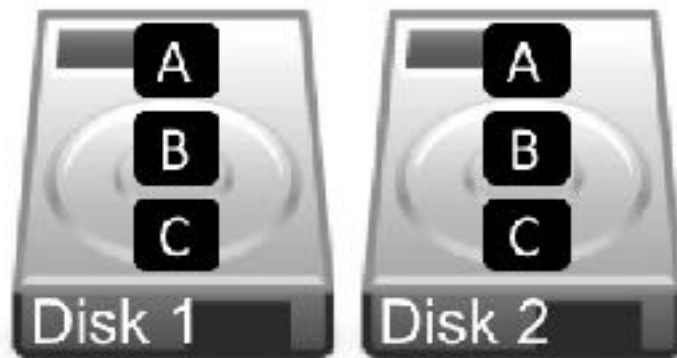


Figure 122: RAID 1 – Data mirrored across two drives

RAID 5 needs three or more drives. Data is written across all the drives, along with what is known as *parity information* (in simple terms, ‘clues’ that enable lost data to be reconstructed). 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 half of the total drive capacity in order to provide resilience, RAID 5 loses only a third on a 3-drive system and a quarter on a 4-drive system. For instance, if a NAS has three 4TB drives installed then the total amount of usable storage capacity is 8TB rather than 12TB; if the NAS had four 4TB drives installed, the total amount of usable storage capacity would be 12TB rather than 16TB



Figure 123: RAID 5 – Multiple drives with parity information

RAID 6 needs four or more drives. It is similar to RAID 5 but uses two sets of parity information written across the drives instead of one. The benefit of this approach is that the system can cope with the simultaneous failure of two of the drives, thereby making it more resilient than RAID 5, but it loses more capacity in order 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 server has five 4TB drives installed in a RAID configuration, then the total amount of usable storage capacity is 12TB rather than 20TB.

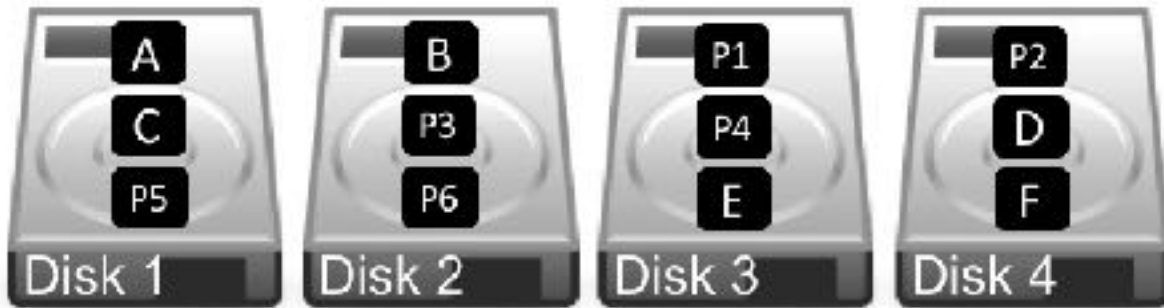


Figure 124: RAID 6 – Multiple drives with double parity information

RAID 10 (also known as RAID 1+0) combines RAID 1 and RAID 0 techniques. Requiring an even number and 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 system with four 4TB drives would give 8TB of usable space rather than 16TB.

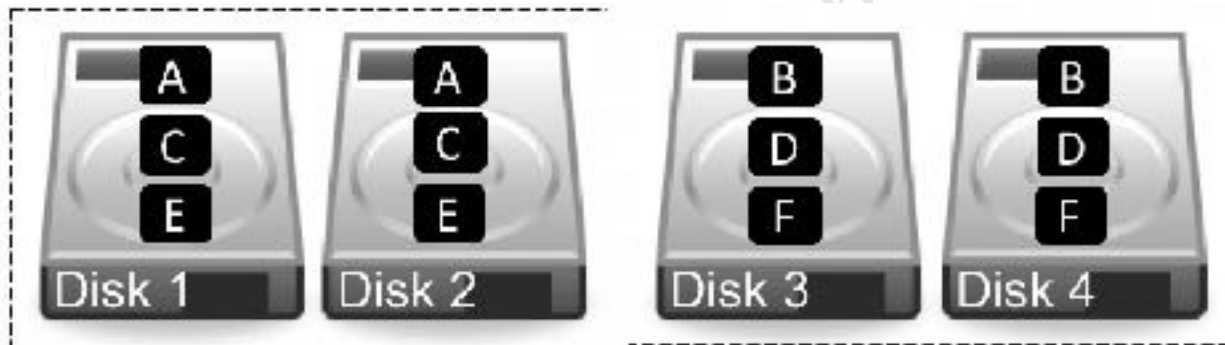


Figure 125: RAID 10 – Simultaneous striping and mirroring

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, but without any protection. For example, three drives of 4TB capacity each would provide 12TB of aggregated storage. In the event of a drive failure, you will lose the data stored on that drive. The drives do not have to be of identical capacities plus you can use as many drives as are in the NAS.

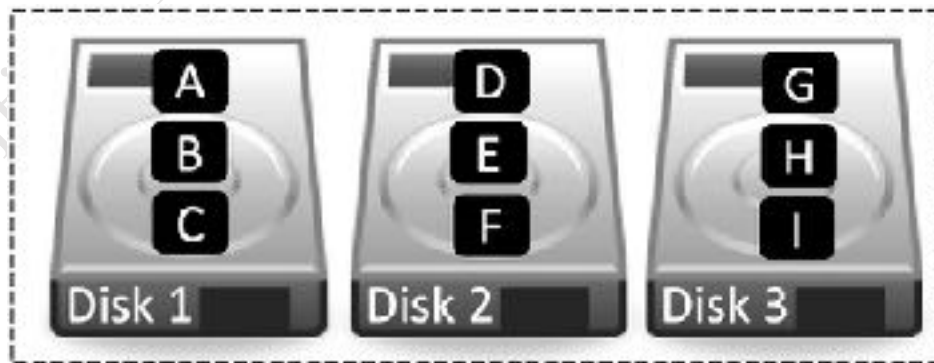


Figure 126: JBOD – Multiple drives act as single one

What to do? If you have a NAS with a single drive, then the question of RAID does not arise. If you have a NAS with two drives, then you can use RAID 1 if data protection is most important to you or use JBOD

if you need the maximum amount of space. If you have a NAS with four drive bays, it can be configured as RAID 5 if protection is most important or JBOD if you need the maximum amount of space. If you have a NAS with five or more drives, it can be configured as RAID 6 if protection is most important or JBOD if you need the maximum amount of space.

One important thing to note is that a RAID system is **not** a backup system. Whilst it can help prevent data loss in the event of problems, 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.

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

10.3 Modifying a Storage Pool/Changing a Drive

There may be occasions when it is necessary to make changes to an existing storage pool. Three typical scenarios are: upgrading a single drive system to a multi-drive RAID system; adding further drives to an existing RAID setup; repairing a RAID system i.e. having to replace a faulty drive. The process for each of these is broadly similar. In this example we will consider the first case: a NAS has a single hard drive, a second drive will now be added, and they will be configured for RAID 1 operation. Before making any changes, take a full backup of the system. Having done so, install the new drive. Some models allow drives to be added or replace on-the-fly – so-called *hot swapping* – but it is best to power off the server if possible when making hardware changes.

Having installed the drive, go into **Control Panel** > **Hard Drive** and on the **Hard Drive** screen check that the new drive has been recognized and has a status of 'Good'. Although time consuming, best practice is to run a Bad Block Scan on a newly added drive before proceeding. Assuming all is well, click **Storage pool**, highlight the existing pool and click **Edit**. On the pop-up panel, choose the option – **Online RAID Level Migration** in this instance – and click **Next**. A message about inserting the new drive is displayed, but as we have already done so you can click Next.

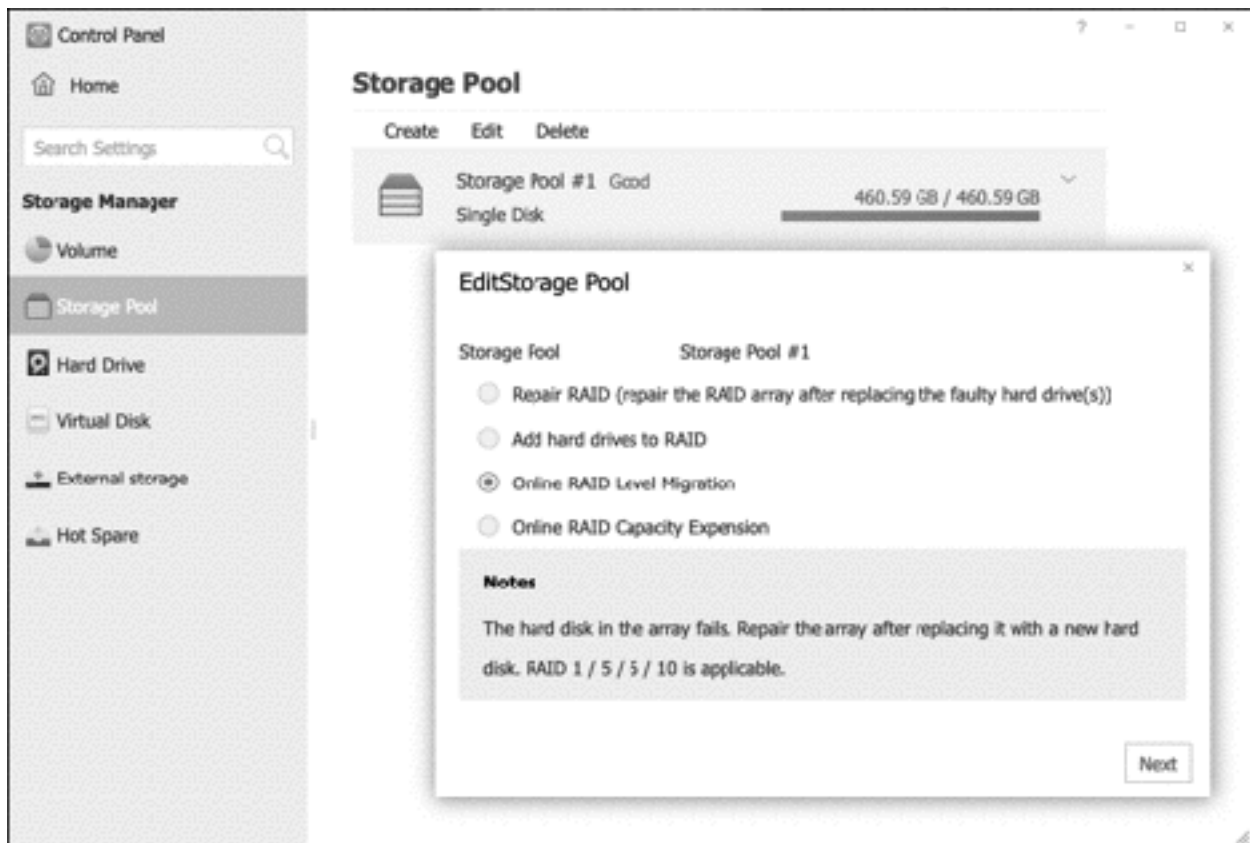


Figure 127: Editing a Storage Pool

A message about inserting the new drive is displayed, but as we have already done so you can click **Next**. On the subsequent screen, select the new disk and click **Next**, followed by **Next** on the Confirm Settings screen:

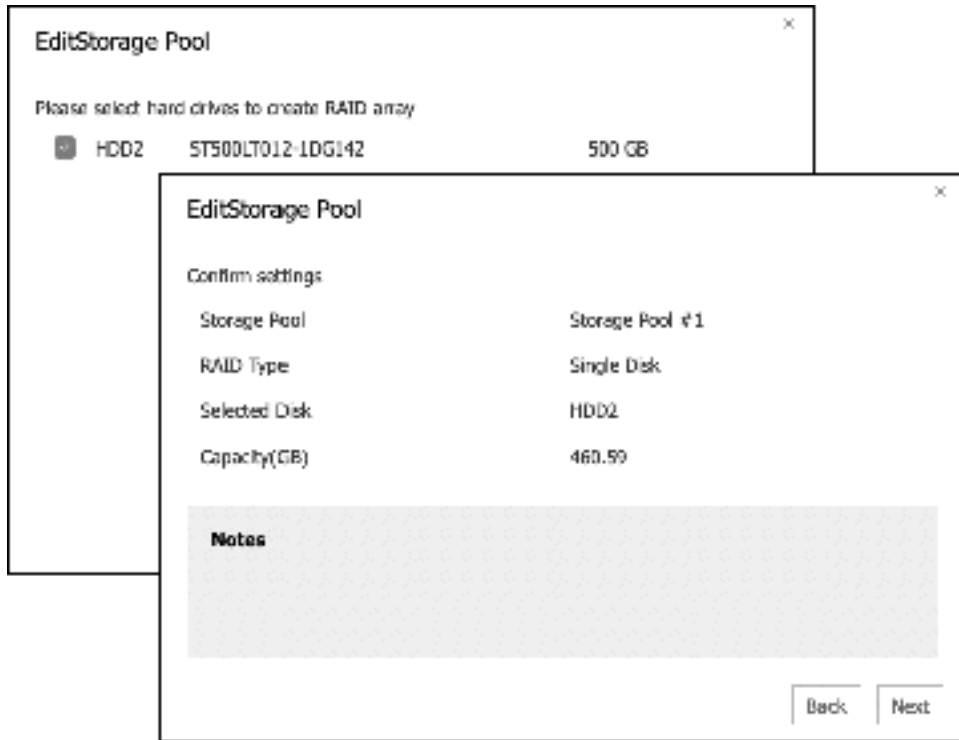


Figure 128: Select disk and confirm

Whilst the RAID is 'rebuilding', the status can be viewed. Depending on the type and capacity of the drives and the RAID level, this process can take many hours. Data on the storage pool is still available at this time, albeit performance of the NAS may be limited overall.

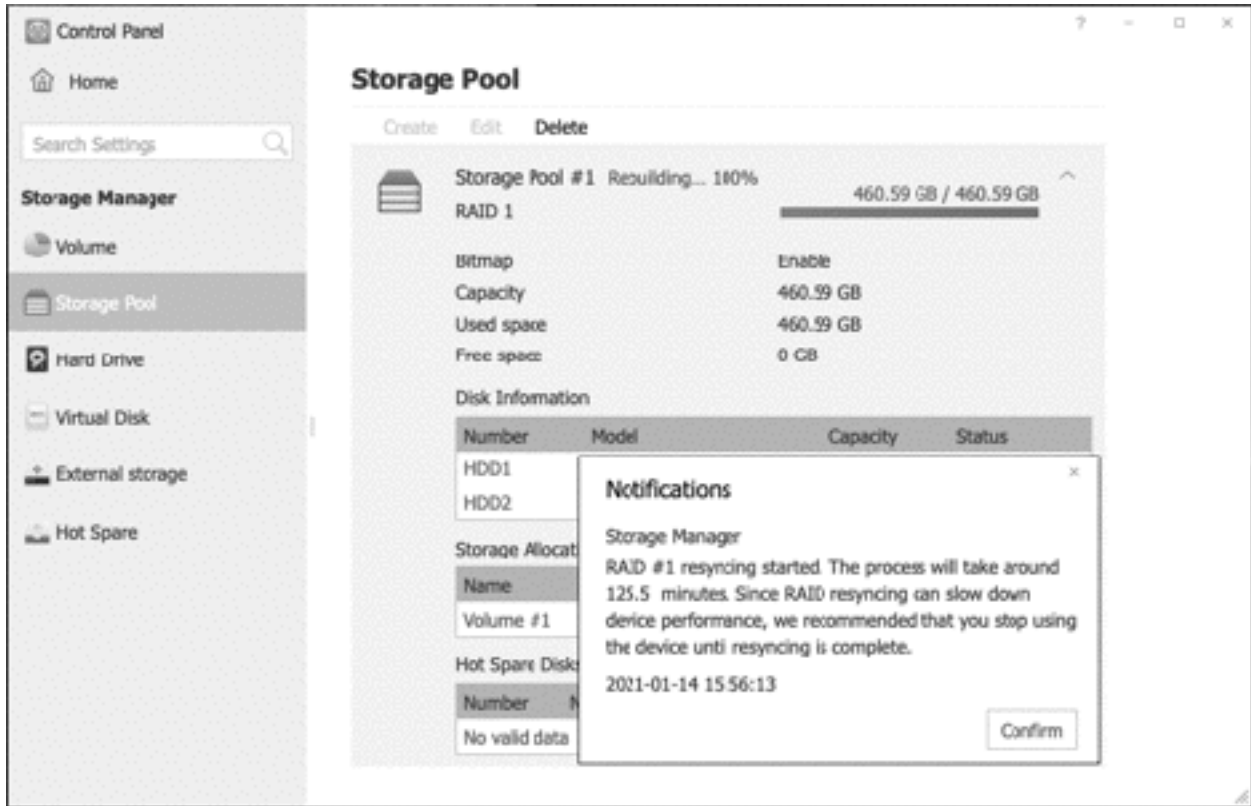


Figure 129: Status as RAID is rebuilt

Free edition. Do not copy or

10.4 Snapshots

Snapshots are a backup mechanism that allows the NAS to backup data in a very efficient manner. In simple terms, the system makes a note of what has been altered when a file or folder has changed and takes a ‘snapshot’ of the changes. It does not make a complete copy of the file or folder, just the differences, which can then be used to restore the data should it ever prove necessary. Snapshots can be taken manually or scheduled to run as frequently as required (once a week, once a day, once an hour etc.). Because only the changes are being recorded, the system is very efficient, both in terms of time taken and disk space used. For instance, imagine you had a 10 Mbyte spreadsheet and changed a single number; with a conventional backup the system would create a 10 Mbyte copy, whereas with a Snapshot the backup might only be a few dozen bytes. All current TNAS models support Snapshots, the only proviso being that the Btrfs filing system has to be used.

Note for the knowledgeable: Snapshots operate at the block level rather than the byte level, the above explanation has been simplified to aid understanding.

Setting Up Snapshots

Snapshots are managed using the Snapshot app, downloadable from Applications. Having installed it, click the icon on the Desktop, which will result in a screen that lists the shared folders:

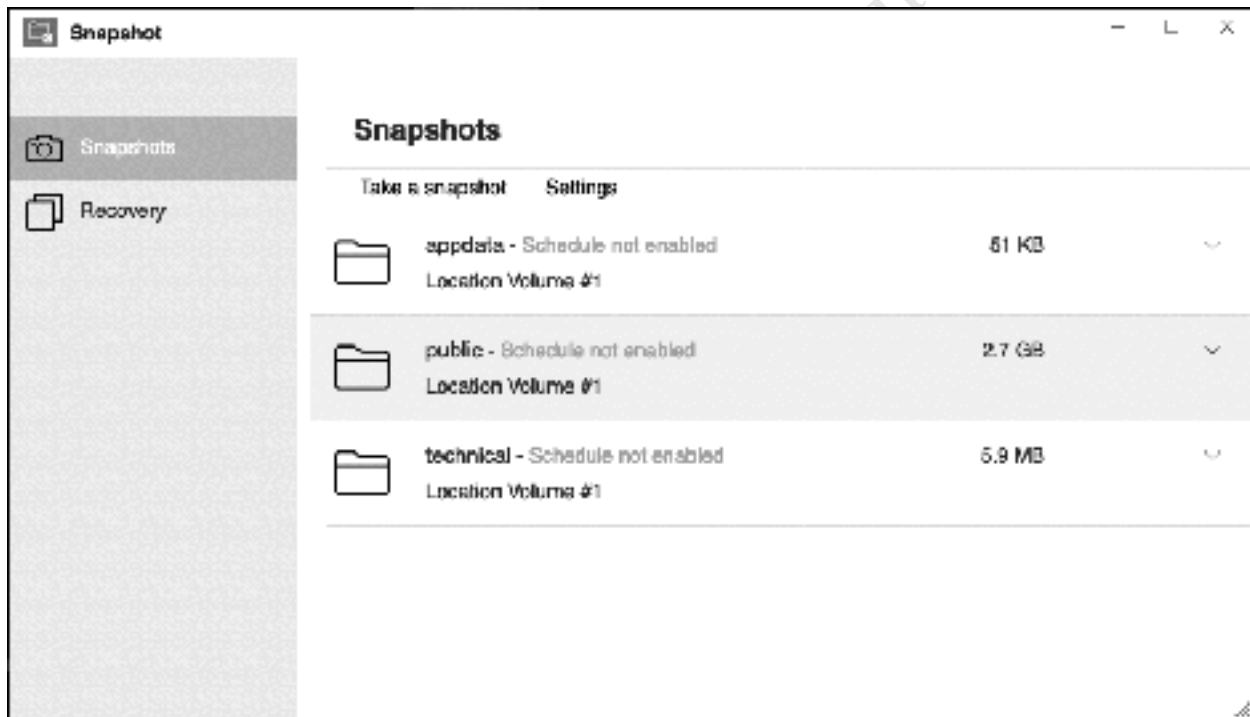


Figure 130: Snapshots screen

Snapshots are controlled on a per folder basis. They can be taken as required on a manual basis, or on a scheduled basis. To manually take a snapshot, highlight the folder and click **Take a snapshot**. To setup a scheduled snapshot, highlight the folder and click **Settings**, which will display the following panel:

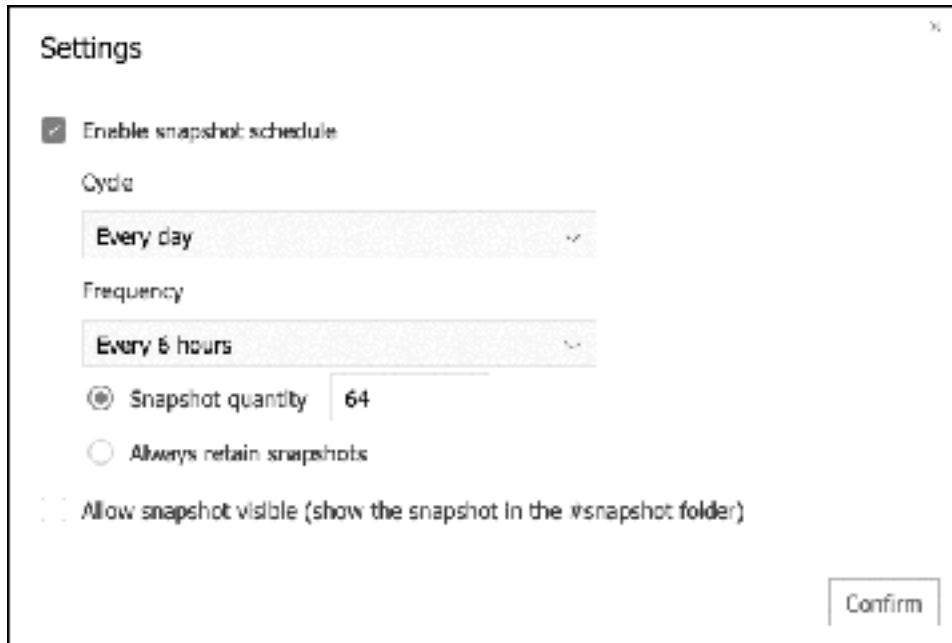


Figure 131: Snapshot schedule settings

Tick the **Enable snapshot schedule** box. Use the **Cycle** dropdown to specify the day that the snapshot is taken; there is a choice of a particular day, all working days, or every day. Use the **Frequency** dropdown to specify how often the snapshots are taken, which can be anything from every 5 minutes to once per day. The **Snapshot quantity** field defines how many snapshots are retained (after which, the space is recycled), or you can choose to retain them indefinitely. There is no single right answer to these questions as 'it all depends', but mainly it relates to how important the data is, how often it changes, how long does it need to be retained and the size of the shared folder. In the above example, a snapshot will be taken every 6 hours i.e. 4 times per day. As the snapshot quantity has been set at 64, in the event of problems it would be possible to roll-back the data to up to 16 days.

The final box controls whether the snapshots are visible from within File Manager. Snapshots are stored in a sub-folder called `#snapshot` within the folder itself e.g. if the public folder was being snapshotted then they would be stored in `public/#snapshot`.

Having made your choices, click **Confirm**.

Recovering Data

To recover data from a snapshot, click **Recovery** on the main screen. Highlight the folder and click **Recovery** at the top of the screen. A list of snapshots is displayed; highlight the required one and click **Recovery**. A message is displayed upon completion.

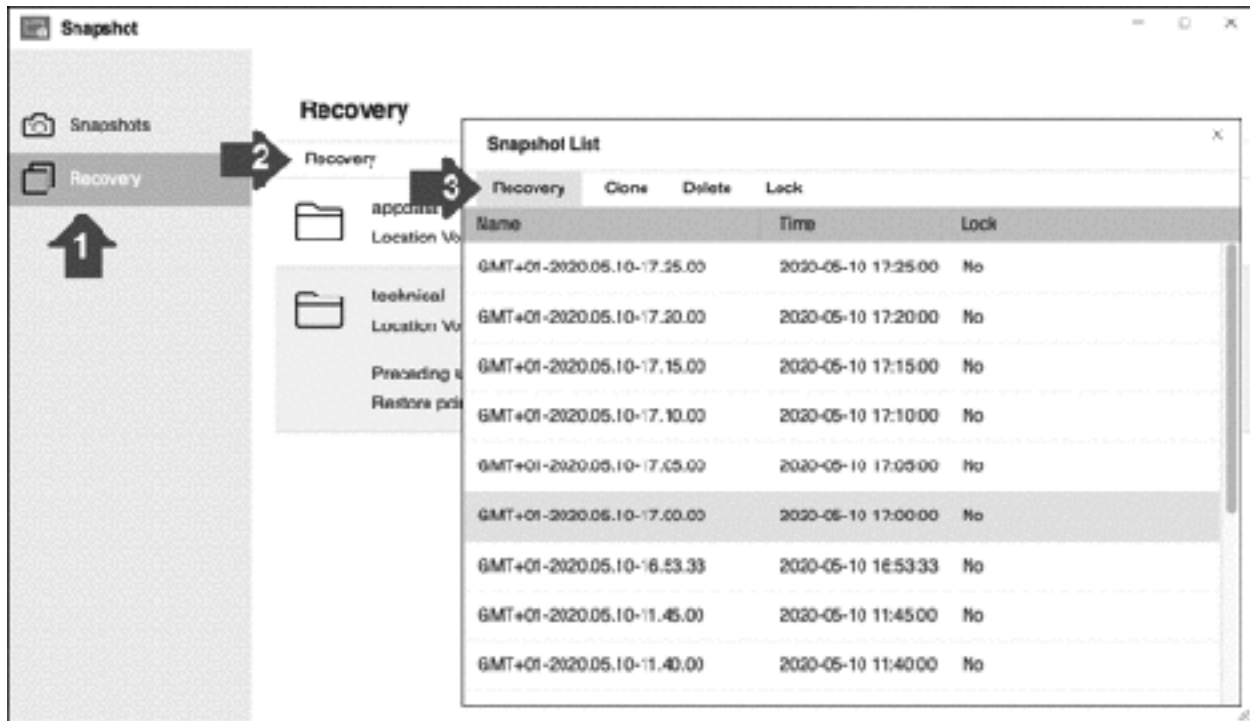


Figure 132: Recovering a Snapshot

The individual snapshots can also be managed from the above screen. To make a copy of a snapshot, highlight it and click **Clone**. To remove one which is no longer required, highlight it and click **Delete**. To mark one for permanent retention, click **Lock**. Note that locking a snapshot prevents it being recycled as part of the normal 'Snapshot quantity' mechanism; however, it can still be deleted manually if required.

Free edition. Do not copy

10.5 iSCSI

iSCSI - *Internet Small Computer Systems Interface* – is a standard for connecting virtualized storage to computers. Its origins lie with large computer systems and it is of particular relevance to organizations that run multiple servers, have large amounts of storage and require great flexibility when it comes to managing that storage. However, the exact same technology is available within TOS and may be of interest to small businesses and even home users.

First, we need to consider how it operates. So far, we have used shared folders on the server. For Windows users, it is possible to map drive letters to shared folders, as described in section [5.3 Connecting Windows Computers](#). This enables us to refer to, say, `\\server\public` as drive P, but it is not a ‘real’ drive in the sense that the C: drive of a computer is and we are simply using the letter P as a shortcut. With iSCSI, an amount of space is set aside on the server. The server is referred to as the *iSCSI host* and the space is known as the *iSCSI target*, which is given a *LUN (Logical Unit Number)* to help reference it. A computer – known as the *iSCSI client* or *initiator* – connects to the LUN (target), which it ‘sees’ as a complete disk drive. This drive, to most intents and purposes, behaves like a real physical drive and can be partitioned, formatted and used in any way the user requires. There is a one-to-one relationship between target and initiator (in practice, if not in theory), meaning a single target should not be connected to multiple clients. It is possible to move targets from one server to another without unduly affecting the clients, hence the reason for its relevance to larger organizations with requirements for redundancy and disaster recovery. One aspect of iSCSI is that it is very efficient, resulting in high data transfer speeds.

Creating an iSCSI LUN

Download and install the *iSCSI Target* app from Applications. Launch it and on the Target tab click **Create**. Enter a short name for the *Target* (e.g. *Target#1*) and an *IQN (iSCSI alias)* will be generated automatically. Ticking the *Data summary* and *Header summary* boxes will enable checksums to be taken, which improves data integrity. Optionally, *CHAP certification* can be enabled; this can be used to specify a username and password in order to restrict access to the iSCSI LUN, although in a home or small business environment you might choose not to do this. Click **Next**, followed by **Next** on the Confirm settings screen as well:

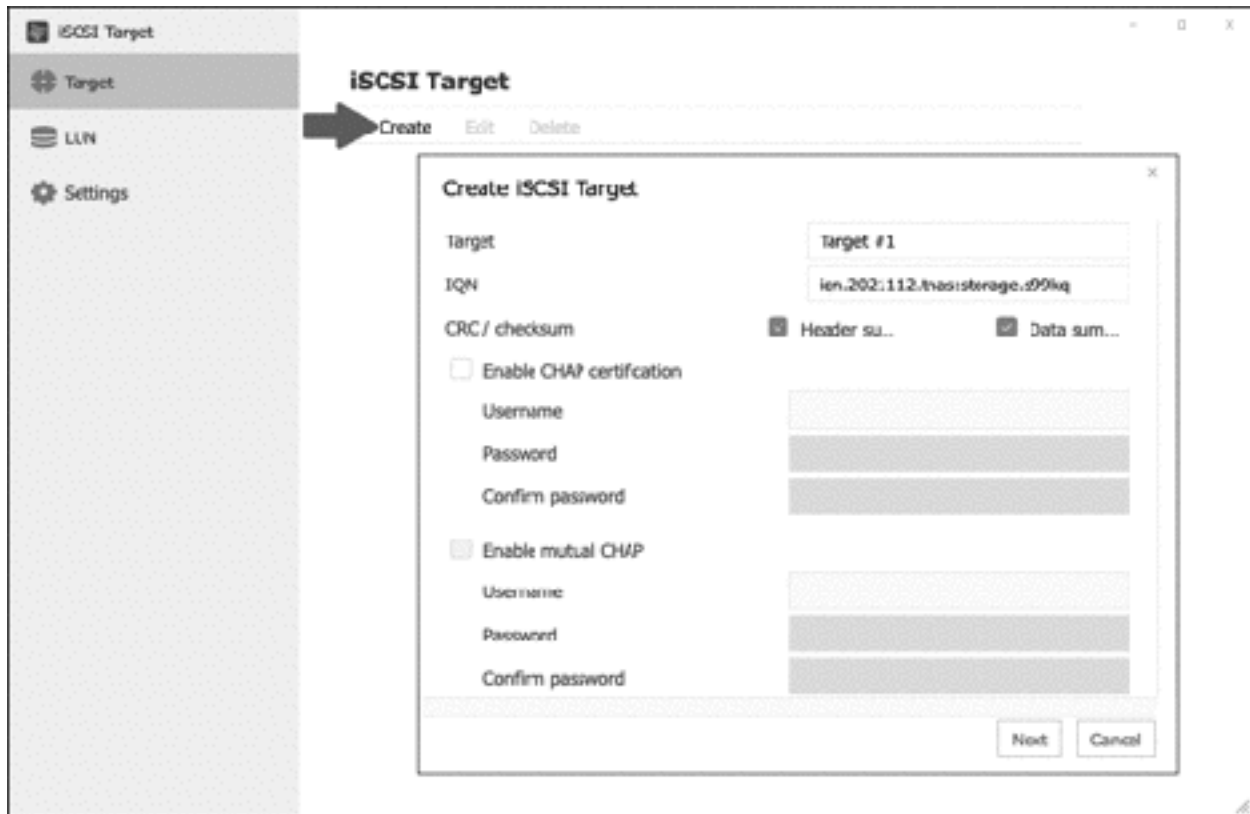


Figure 133: Creating a new iSCSI target

A panel is displayed, asking ‘Do you want to create a LUN now?’ – answer **Yes** and click **Next**.

The subsequent panel controls the name, type, location and size of the iSCSI LUN. LUNs are available in two options, *Thin* and *Thick*. With Thin Provisioning, storage space is allocated dynamically and only as required. Suppose you specify 100GB capacity; initially, whilst it is empty, the LUN will be tiny. You then copy 10GB of data to it, at which point it grows to 10GB. Add another 10GB and it increases in size to 20GB, and so on until it reaches its maximum size. In contrast, with Thick provisioning all of the space is allocated up front, so 100GB would immediately be taken from the available drive space. In general terms, Thin Provisioning is more flexible and economical with space, whilst Thick offers better performance. Choose the type (if in doubt, select *Thick*); the *Location* (if you have more than one to choose from) and the *Capacity* (in GBytes). Click **Next**:

Create iSCSI Target

Create iSCSI LUN

LUN

Storage allocation

Thin provisioning

Thick provisioning

Location

Free space 446.37GB

Capacity

Mapped iSCSI Target

Figure 134: iSCSI LUN provisioning

Click **Apply** on the Confirm settings screen. The newly created LUN will then be listed on the *iSCSI Target List* screen.

Connecting a client

Having defined the iSCSI LUN(s) on the server, the client computer(s) can now be connected. This section describes how to do so with modern versions of Windows (i.e. Windows 7 onwards). There is no built-in capability on macOS, although third party solutions may be available.

Go into the **Control Panel** on the Windows PC, choose **Administrative Tools** and within it launch **iSCSI Initiator** (for recent versions of Windows 10, go into **Settings** and type *iSCSI* in the *Find a setting* search box). The first time you do this you may receive a message stating that the Microsoft iSCSI service is not running – click **Yes** to start the service and it will start up automatically on subsequent occasions. In the *Target* field on the Targets tab, enter the IP address of the server and click the **Quick Connect** button. The target should be quickly found and a status of *Connected* shown:

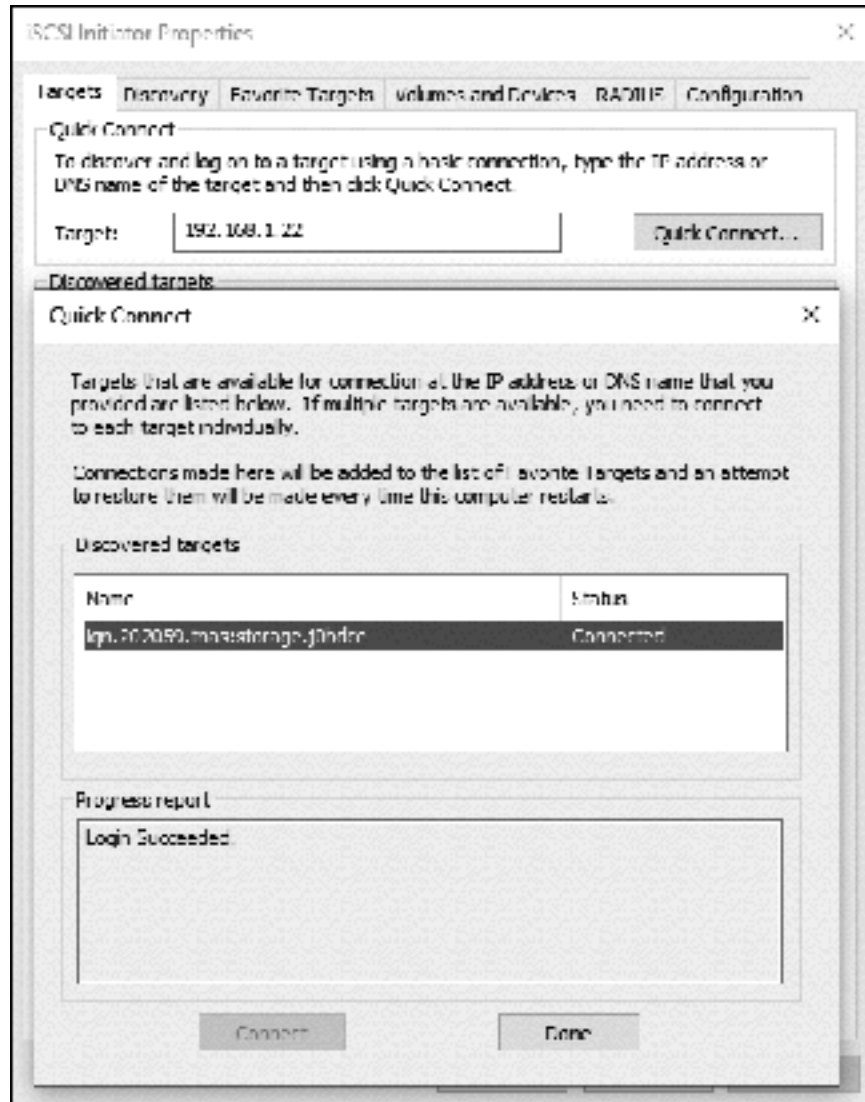


Figure 135: Connecting to the Target

Click **Done** and **OK**. Go back to **Administrative Tools** and choose **Computer Management** and within it choose **Disk Management**. You will receive a message about having to initialize the new disk. If the disk is less than 2TB in size choose MBR, if greater than 2TB you will need to choose GPT. Click **OK**.

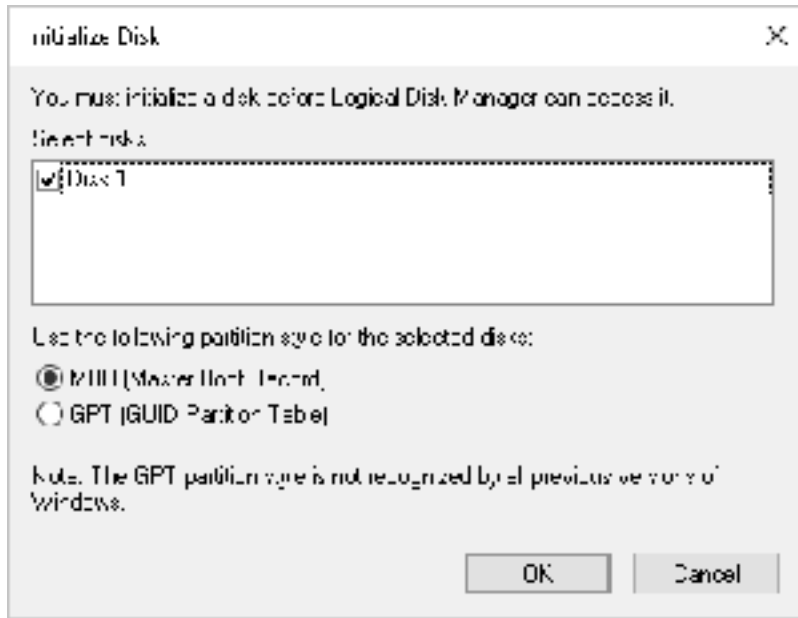


Figure 136: Disk initialization

The new disk will then be visible within Disk Management. Right-click it and choose **New Simple Volume**. Run through the *New Simple Volume Wizard* to create and format the volume and assign a drive letter to it; thereafter it can be used as a regular disk drive by the computer.

Backing up an iSCSI LUN

iSCSI LUNs can be backed up using the Duple Backup utility, which is downloaded from Applications. For general information on Duple Backup, see section [7.4 Backing up to Cloud Services using Duple Backup](#).

10.6 SSD Caching

Solid State Drives or SSDs are very fast in operation, many times more so than traditional mechanical hard drives. However, they are also considerably more expensive, particularly for the larger capacity ones which are of most use in a NAS. For instance, at the time of writing a 4TB SSD sells for around US \$500 online, whereas a NAS-certified 4TB mechanical hard drive can be picked up for US \$100 and, whilst SSD prices will continue to fall, it may be several years before they match the prices and capacities of mechanical drives. The concept of caching is that copies of frequently used data are kept on SSD, making it quickly available when required, as opposed to it being accessed from the much slower mechanical drives. This process happens automatically and transparently, with TOS keeping track of the data. By using a combination of SSD for performance and lower-priced mechanical drives for capacity, it is possible to obtain the ‘best of both worlds’ for a reasonable price. A good ratio of mechanical to SSD storage is 10:1 e.g. if you have 10 TB of mechanical storage you should aim to supplement it with 1TB of SSD as cache, although in practice any amount of SSD should be beneficial.

Most TerraMaster models are able to use regular 2.5” SATA-format SSD drives, such as are commonly used in laptops, for caching. As drives used for caching take a lot of hits, it is essential to use high quality ones, rather than low-cost consumer ones.

Setting Up Caching

Install the SSD into a spare drive bay on the NAS. Having done so, go into TOS and click **Control Panel** > **Volume** > **Edit**. Specify a *Description* and select the *SSD cache* using the dropdown. Set the *Number of partitions* for the cache – typically you would only have one, but you could divide it and allocate the partitions to different volumes. Click **Confirm**. Setting up the cache may take some time and it is necessary to wait until the completion message is displayed (do not navigate away from the screen). The TNAS will then restart and having done so the cache will be operational.

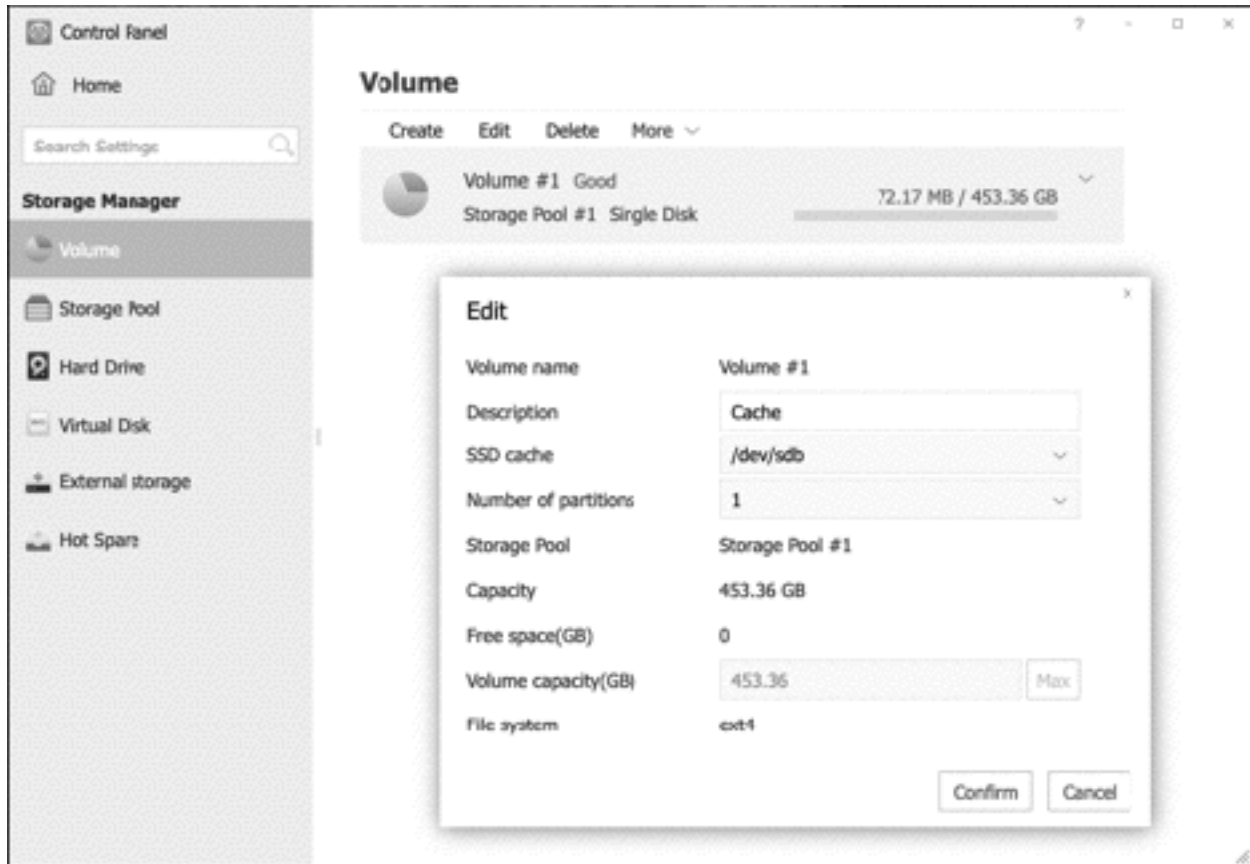


Figure 137: Adding an SSD Cache

Disabling Caching

If it is required to subsequently disable the caching in the future, go into **Control Panel > Volume > Edit**. Untick the **Enable SSD Cache** box and click **Confirm**. The TNAS will then restart and having done so the cache will no longer be operational.



Figure 138: Disabling an SSD Cache

Free edition. Do not copy or distribute.

CTACS

10.7 SSD TRIM

Note: this section only applies if SSDs are being used for regular storage. It does not apply when SSDs are used for caching.

The SSD TRIM feature improves both the performance and lifespan of SSD devices and hence should be enabled if they are being used. To do so, go into **Control Panel** > **Volume**, highlight the SSD-based volume and choose **More** > **SSD TRIM**. On the resultant panel, tick the **Enable SSD TRIM** box. An *Execution cycle* (or schedule, in plain English) can be specified; by default, SSD TRIM will run once a day at midnight and this setting is fine. Click **Confirm**.

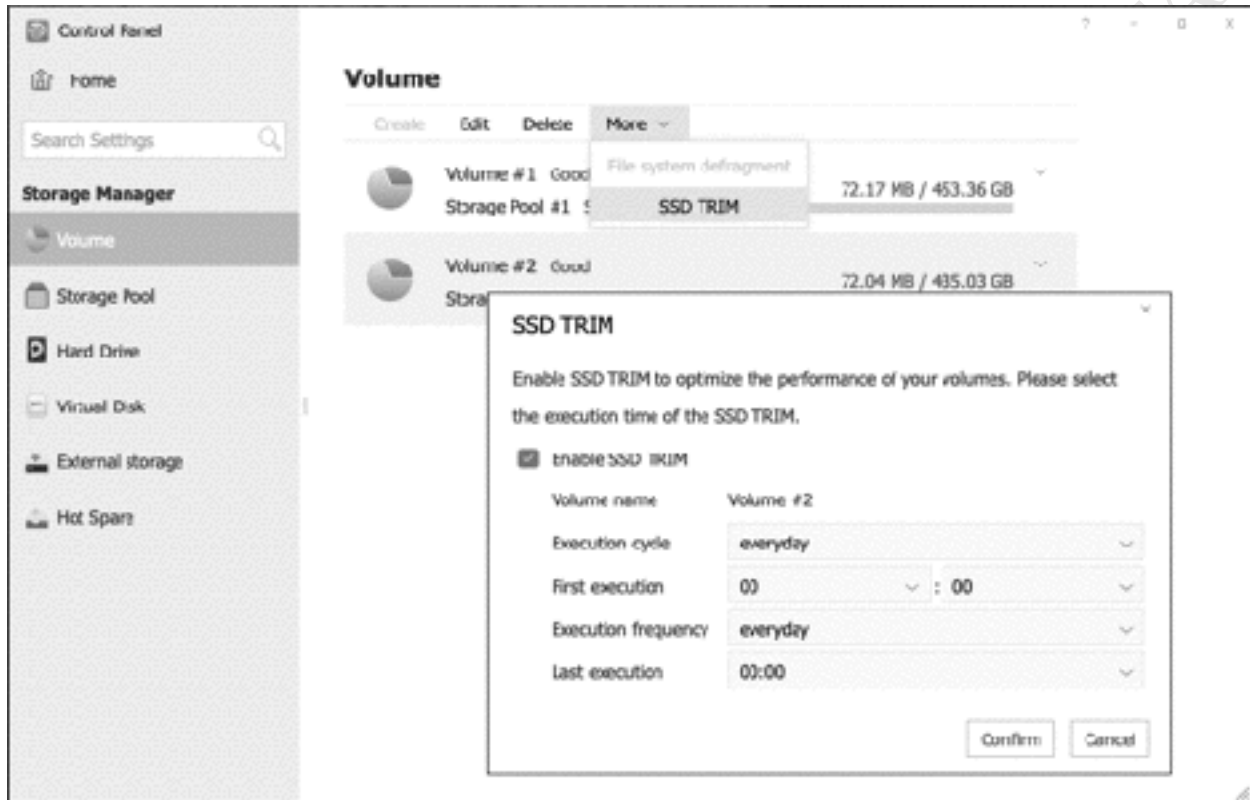


Figure 139: Enabling SSD TRIM

Free edition. Do not

11

MISCELLANEOUS & ADVANCED TOPICS



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

11.1 Overview

This chapter contains a selection of miscellaneous topics which do not easily fit elsewhere, along with those of a more advanced or specialized nature.

11.2 Applications

Whilst the TOS operating system has a huge amount of useful functionality built-in, it is possible to extend it further through the installation of free, optional apps and this process is managed through *Applications*, which can be thought of as an app store for TNAS. Click the *Applications* icon to display the following screen:

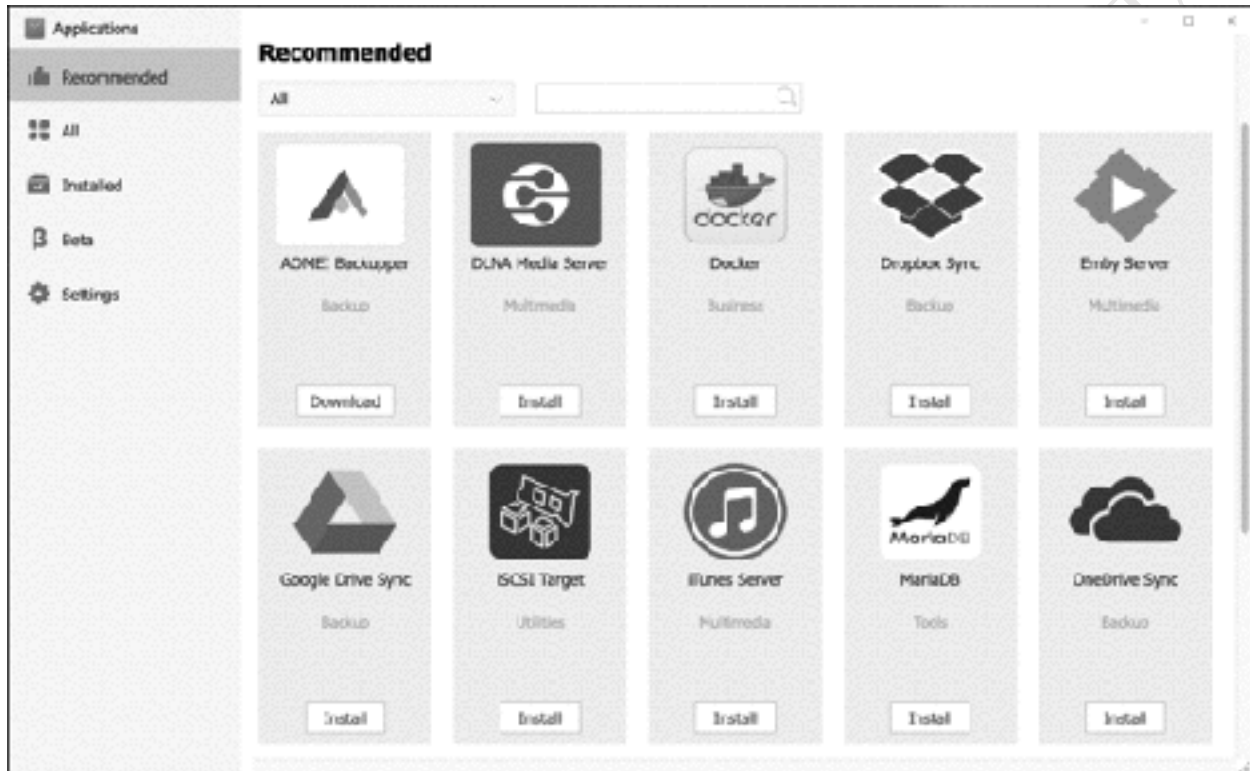


Figure 140: Applications

At the time of writing, around 80 official apps are available and this number can be expected to increase in the future. Most apps are available for both Intel x86 and ARM platforms, although some are only for the former and new apps sometimes appear for Intel before they appear for ARM. Apps which are not available for your particular model will not be listed.

The following selection gives an idea of what is available:

Emby Server – A popular media server application, used for streaming music and video

Plex Media Server – another popular media server application

Mail Server – turns the TNAS into a fully-fledged email server

MariaDB – the popular open-source relational database management system, forked from MySQL

WordPress – enables the TNAS to host WordPress blogs

Transmission – BitTorrent/download manager

Dropbox Sync – provides file synchronization between the TNAS and the public cloud

Joomla – Content management system for building websites and managing applications

To download and install a package, click on its **Install** button. Upon completion, a new icon may appear on the desktop. If it does not, an option may have appeared against the package, giving the option to

‘Send to desktop’. There will also be an option to uninstall it should this be necessary for any reason (note that simply deleting an icon from the desktop does not delete the underlying application). To subsequently control an app, find it by clicking on the **Installed** section with Applications.



Figure 141: Controlling an installed package

You can also click the **Manage** button in the same section, from where installed apps can be started, updated and uninstalled:



Figure 142: Manage options for apps

Updates to individual applications may be made available. When this happens, the Applications icon on the desktop will display a small number on it, indicating the number of update(s) available. Go into Applications and look for the package(s); the ‘Install’ button will have been replaced by one reading ‘Update’.

New applications and updated versions of apps may be available from the ‘Beta’ section. Beta versions provide early access to apps but are not considered suitable for use in production environments. To avoid Beta apps being listed, click **Settings** and remove the tick from **Show the beta app**.

Although apps are developed or authorised by TerraMaster, there are also ‘unofficial’ ones available from other sources. These apps may provide extra capabilities or do things in a different way; or, you may need

to test ones that you are developing yourself. Before using them, it is important to understand that none of these apps are supported by TerraMaster and if things go wrong then you are on your own. You should only explore such apps if you fully understand and are happy with the implications of this. Having downloaded such an app, click on the **Browse** button within Settings to locate it, then click **Apply**.

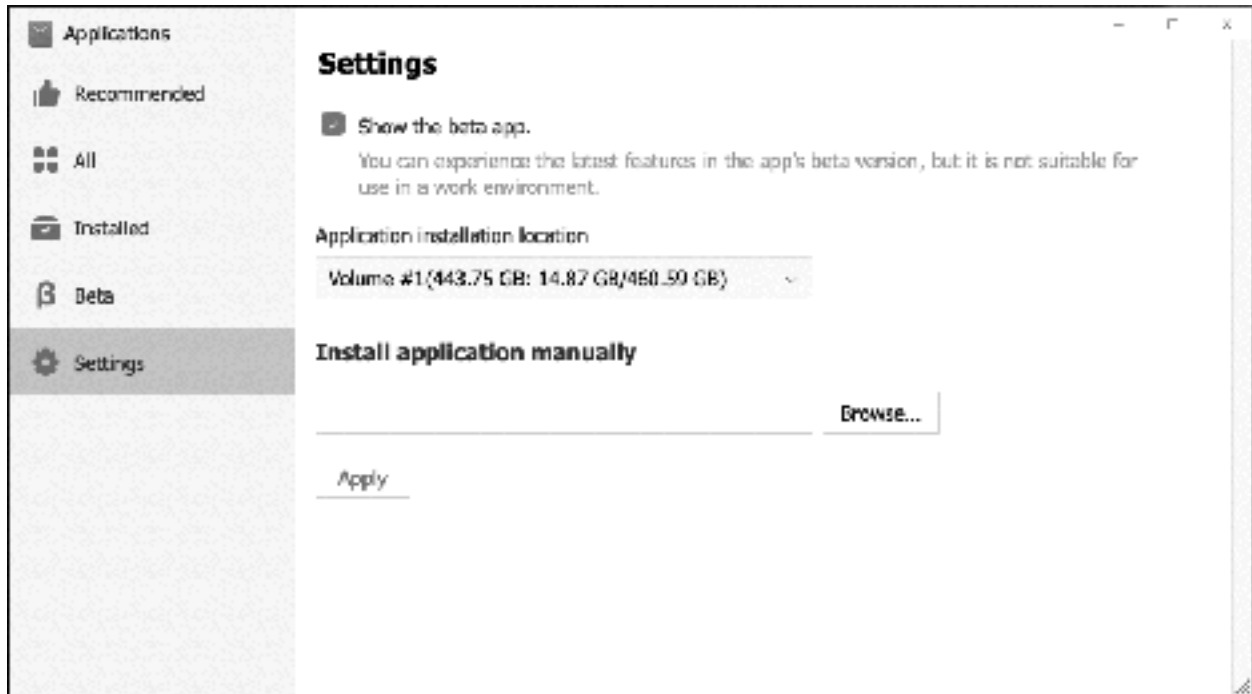


Figure 143: Settings screen

Free edition. Do not copy

11.3 Date and Time Settings

The TNAS should pick up the correct date and time automatically from the internet. If it is incorrect or needs to be adjusted, or you need to change the time zone for some reason e.g. it has defaulted to Chinese Standard Time (CST) but you are not located in that part of the world, you can do this from the Control Panel. Click **Control Panel > Region & Language > Time** to display the following screen:

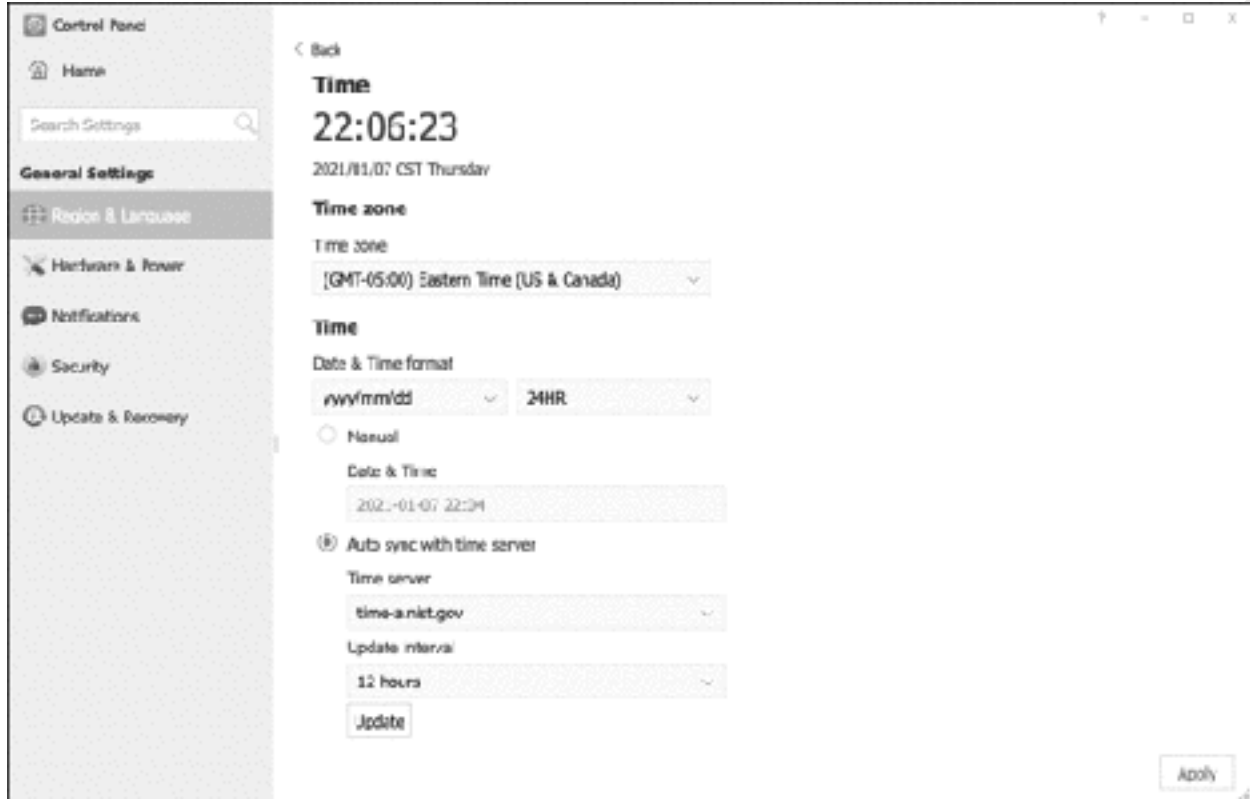


Figure 144: Date and Time Settings

Underneath *Time zone* is a drop-down, listing the international time zones. Beneath that is the *Time* section, where you can change the date format (e.g. yyyy/mm/dd, mm-dd-yyyy and so on) plus switch between the 24 Hour and the 12 Hour clock schemes. The **Auto sync with time server** option should be selected, which enables the NAS to obtain the correct time from an internet-based time server. However, if you wish to set the time manually, click **Manual** and choose the correct date and time from the combined pop-up clock and calendar.

Having made any changes, click **Apply**.

11.4 Renaming the Server

Although not a common requirement, it is ever necessary to rename a server if it is possible. For instance, when initially setting it up and installing TOS you may have omitted to rename it from its default name (which may have been something seemingly random e.g. *TNAS-37E8*) to something more meaningful and memorable, such as *server*. To do so, click **Control Panel** followed by **Network**. On the **General** tab, type in the new *Device name* and click **Apply**. Do not change any of the other settings.

Keep in mind that changing the name have implications. For example, computers and mobile devices may need to be reconfigured so that they connect to the new name rather than the old one. It may also be necessary to advise the users of the system of the change.

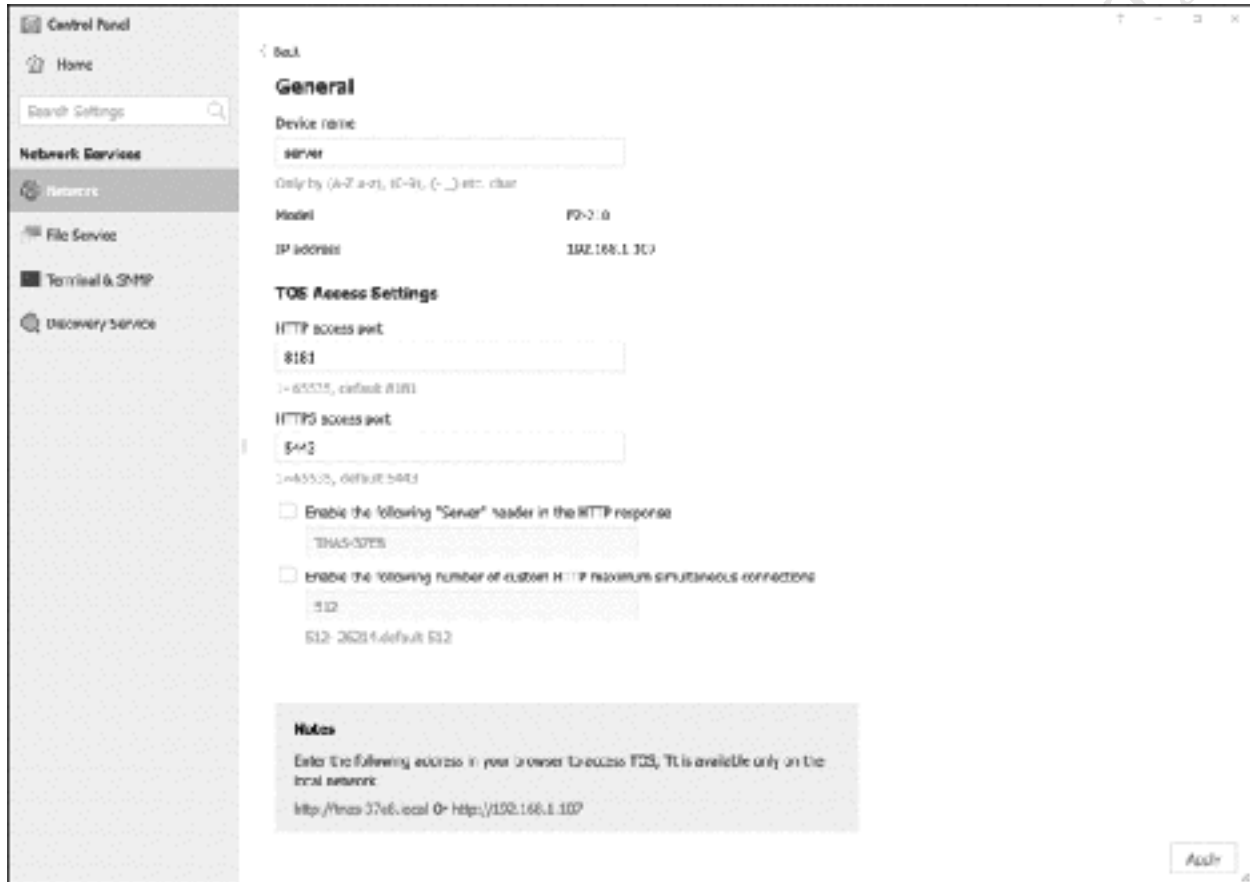


Figure 145: Changing the device name of the server

11.5 User Settings

Each user of the system can personalize their individual desktop or view of TOS whilst logged-in using a browser. There are four items that can be customized or changed: wallpaper, language; password; other settings. Items are changed using the mini-icons in the top right-hand corner of the screen or by right-clicking the desktop.

Wallpaper

Right-click the Desktop and choose **Wallpaper** from the pop-up menu. A selection of wallpapers is displayed: simply click the one you want:



Figure 146: Desktop wallpapers

You can also set a custom wallpaper, for instance by using a favourite photograph. There are two methods for doing this:

Next to the *Custom wallpaper* field, click **Browse** and navigate to where the photo is stored on the local computer. Click **Apply**.

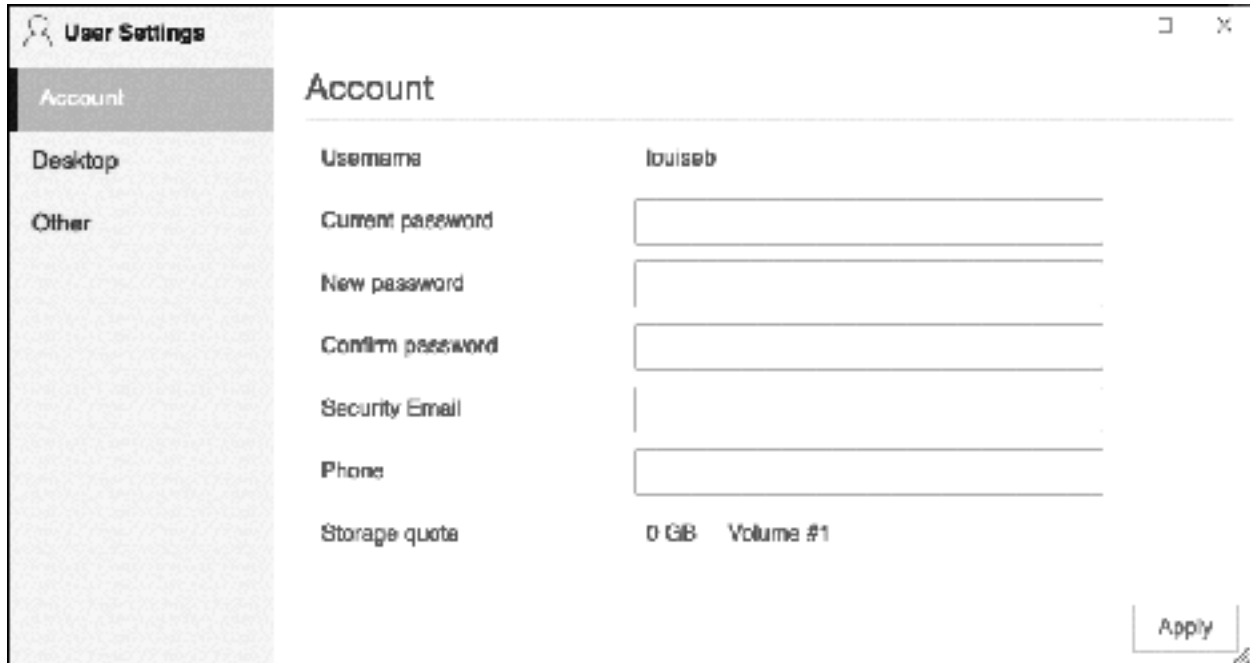
Alternatively, using File Manager, navigate to where the picture is stored on the NAS. Right-click the picture and from the pop-up menu choose **Set as Desktop Wallpaper**.

Language

A user can work with TOS in the language of their choice, regardless of whatever language the server is configured in. This can be very useful in environments where multiple languages are used, such as international organizations and countries with more than one national language. To switch language, click the small globe icon in the top right-hand corner of the screen and select a language from the dropdown. The languages currently available are English, German, French, Spanish, Italian, Hungarian, Polish, Turkish, Russian, Simplified and Traditional Chinese, Japanese and Korean.

Password

If a user wants or needs to change their password, they should click their username in the top right-hand corner of the screen and from the pop-up menu choose **User Settings** to display the following form (alternatively, right-click the Desktop and choose **Settings**). It is necessary to enter the current password, the new password, and to confirm the new password. Then click **Apply**. Passwords have to be at least 8 characters in length and comprise a mixture of letters and numbers.



Account	
Username	louiseb
Current password	<input type="password"/>
New password	<input type="password"/>
Confirm password	<input type="password"/>
Security Email	<input type="text"/>
Phone	<input type="text"/>
Storage quota	0 GB Volume #1

Apply

Figure 147: Changing the user password

Other Settings

There are several settings that can be changed, relating to logging and logging off. To access them, click the username in the top right-hand corner of the screen and from the pop-up menu choose **User Settings**, then click on **Other** (alternatively, right-click the Desktop and choose **Settings** then click **Other**). Place or remove ticks against the various options. Note that some may not apply for all users (for instance, only the admin user can shutdown the server).

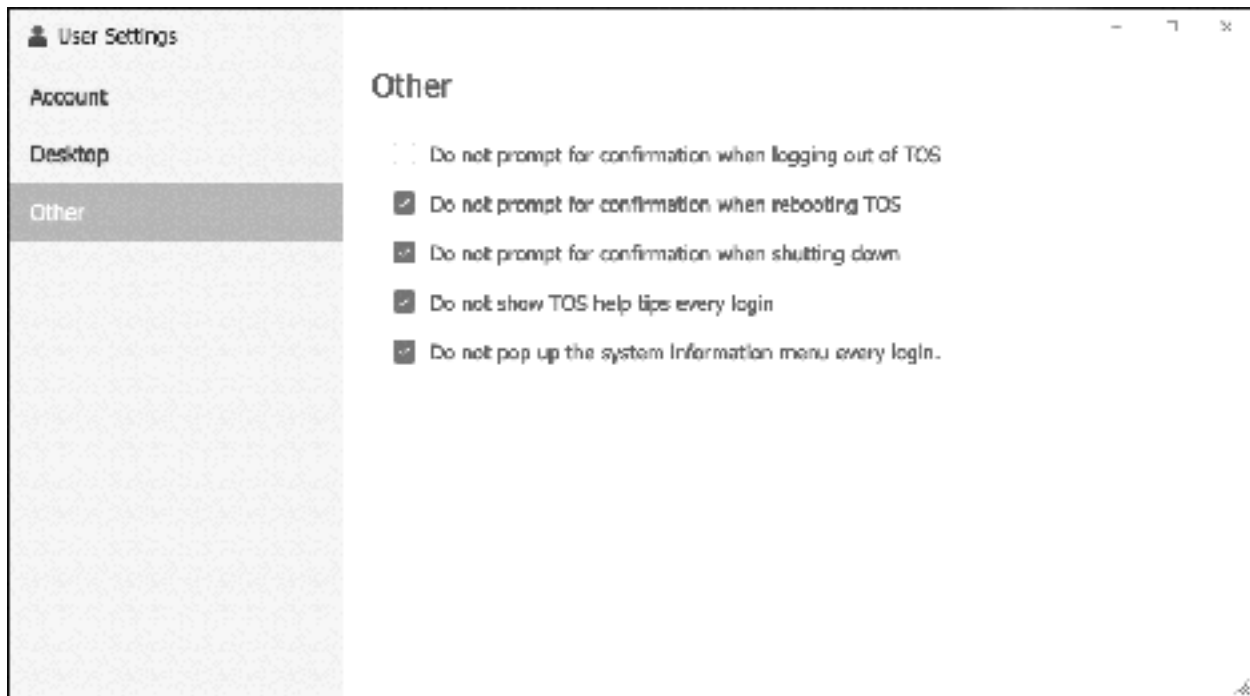


Figure 148: Other settings

Free edition. Do not copy or distribute.

11.6 Printing

TOS does not have any specific features relating to printing. Some NAS brands do have the ability to share USB printers which, several years ago, would have been considered an important feature. However, these days most new printers have built-in Ethernet or wireless connections, meaning it is no longer the killer feature that it once was. In the case of such printers the TNAS has no significance at all and you simply follow the manufacturer's normal installation procedure on each of your computers.

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

- Printers typically have wireless and/or wired connections. Wired connections are preferable although by no means essential, as performance is often better compared to wireless.
- Configure the printer with a fixed or static IP address. This should be adjacent to the address of the server and away from the address range used by the computers. Suppose, for instance, that the internet gateway is 192.168.1.1 and the server is 192.168.1.2. If two printers were added to the network, then suitable addresses would be 192.168.1.3 and 192.168.1.4. The simplest way to set the IP address is on the printer itself; alternatively, the technique of reserving an IP address on the DHCP server (commonly the router in a home or small business setup) can be used.
- Download the latest drivers for the printers. Consider storing the drivers on the TNAS so that they can then be easily copied to the individual computers, rather than have to download them from the internet each time. The *technical* folder is a good location for this.
- Printer manufacturers sometimes offer a choice of drivers, for instance a basic one as well as a full-featured one. Use the basic one, as the full-feature ones sometimes have superfluous features designed to capture marketing information and sell you more cartridges. However, be aware that with some multifunction devices (combined printers/copiers/scanners) not all functions may be available in a networked environment or may require additional software from the manufacturer to fully utilise them.

11.7 Text Editor

There may be a requirement to create and edit text and other files for the NAS. Rather than use a program on a Windows PC (e.g. WordPad) or Mac (e.g. TextEdit) and then have to upload it to the TNAS, it is possible to edit files directly using a small app that can be downloaded from Applications, called *Text Editor*. However, rather than place an icon on the Desktop in the conventional manner, Text Editor integrates itself with the Desktop and File Manager and hence has to be used in a specific way.

To create a simple text file, right-click the Desktop and from the pop-up menu choose **New file > txt File**. A file is created on the Desktop called *newfile.txt* by default, although you can rename it at the time of creation or subsequently. You can then edit it by double-clicking it or right-clicking it and choosing **Open** or **Edit** from the pop-up menu. If a text file is within a folder, you can open or edit it by right-clicking it from File Manager.

Text Editor has many features for web developers and programmers. Right-click the Desktop and create a new file, called *index.html*. Right-click it and choose **Edit** (do not choose Open). The file can now be worked upon. As the editor is 'aware' that it is an HTML file, it provides keywords and auto-completion as you type and automatically indents the lines. These features are controlled from the **View** menu, along with font size, coloring scheme and choice of syntax highlighter (e.g. Python, Ruby, PHP, Java etc).

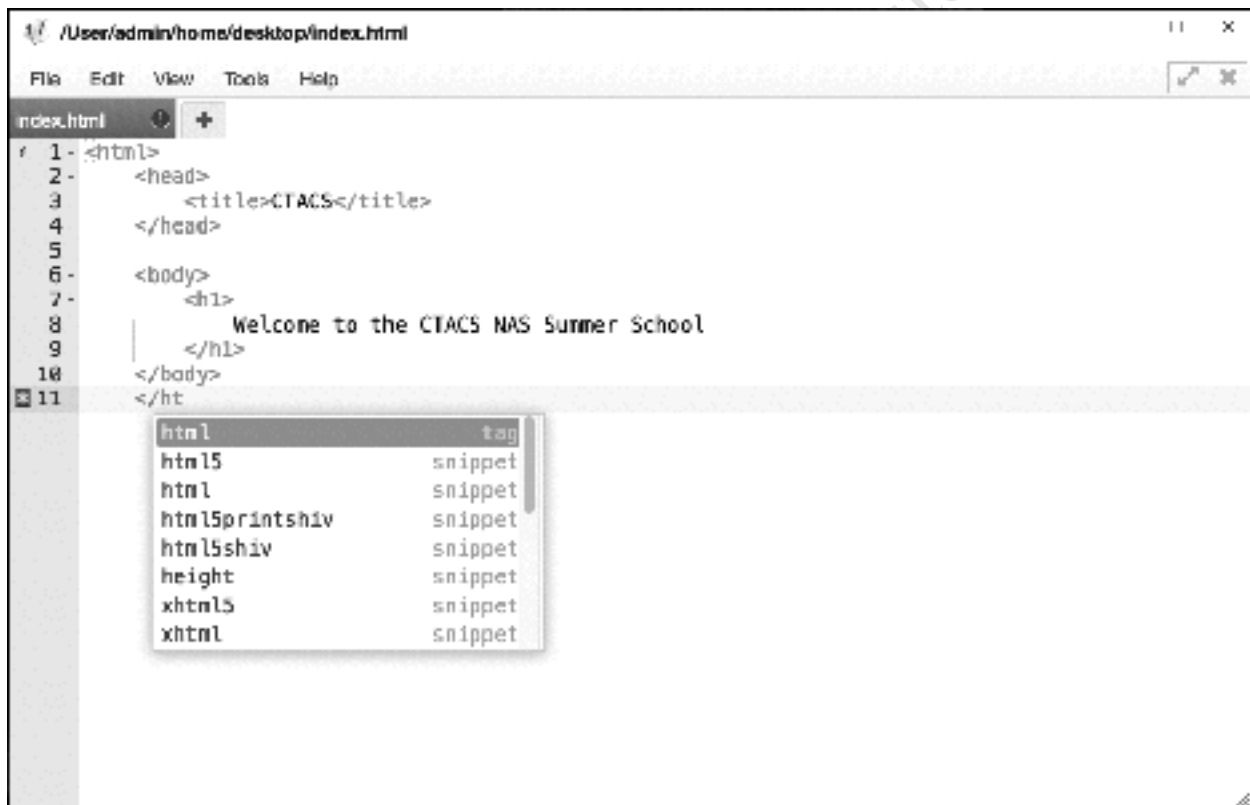


Figure 149: Editing a HTML file

To save a file, click **File > Confirm**. To preview it and obtain an approximate rendition, click **Tools > Preview**. To render it fully within the local computer's browser, click **Tools > Open with browser**. When finished working on the file, click **File > Close**. Text Editor is closed by clicking the cross in the top-right corner of the screen.

11.8 PDF Reader

The PDF Reader adds PDF viewing support to TOS. It is downloaded and installed from Applications; once installed, PDF documents can be opened by clicking on them from the File Manager or Desktop. Alternatively, launch it from the Desktop and open files by clicking on the small folder icon in the top-left hand corner of the screen.

The standard range of PDF functionality is provided including search, navigation, different zoom levels, document rotation and printing (when a document is printed, it will be to the computer's default printer).

PDF Reader is closed by clicking the cross in the top-right corner of the screen.

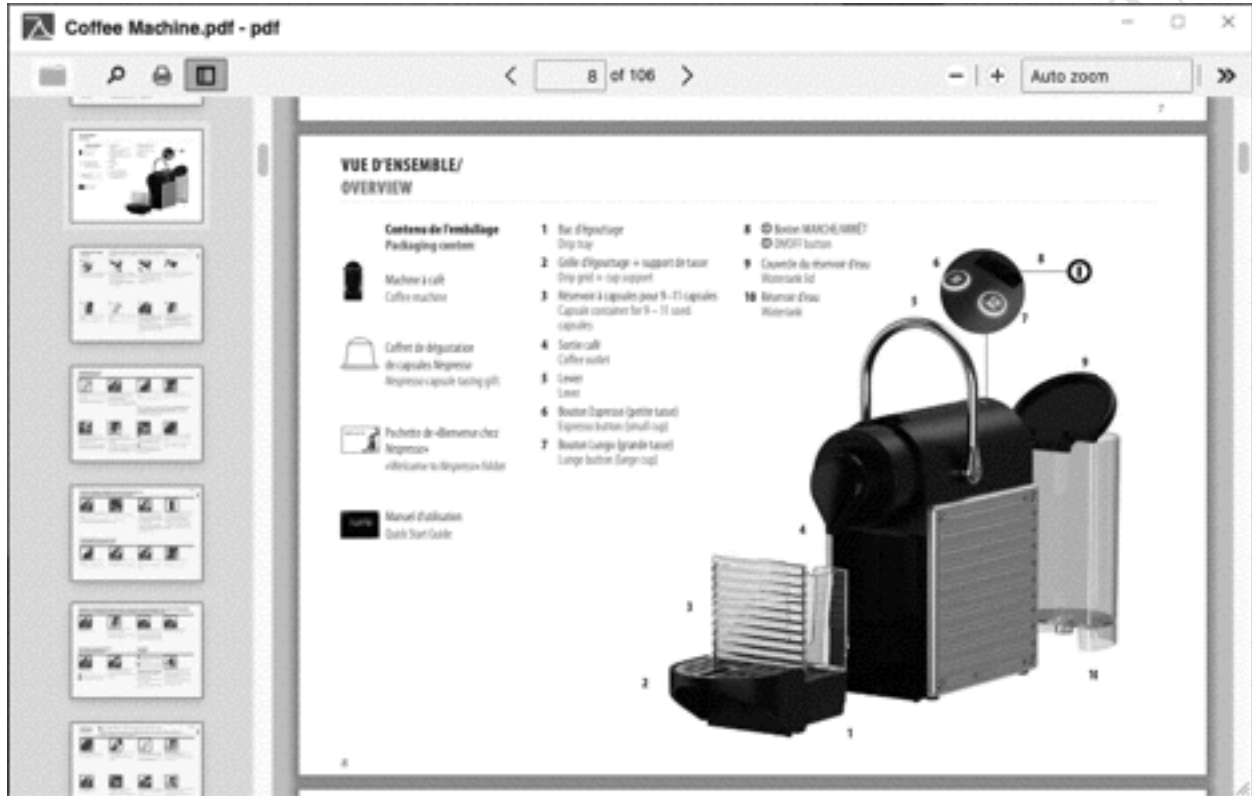


Figure 150: PDF Reader

11.9 Docker

Docker is a ‘lite’ form of virtualization that runs Linux virtual machines and specific applications and is particularly popular with software developers. All TerraMaster NAS units support it, unlike most competing manufacturers, where it is often restricted to more powerful models only. This section is intended only as a brief introduction to what can be quite a sophisticated topic. If you are new to containers and Docker, you might find it slightly underwhelming as they are mostly for running ‘black box’ appliances and do not appear to do very much in a conventional sense.

Docker is downloaded and installed from Applications, which places an icon on the Desktop. Launching it will display the following Overview screen:

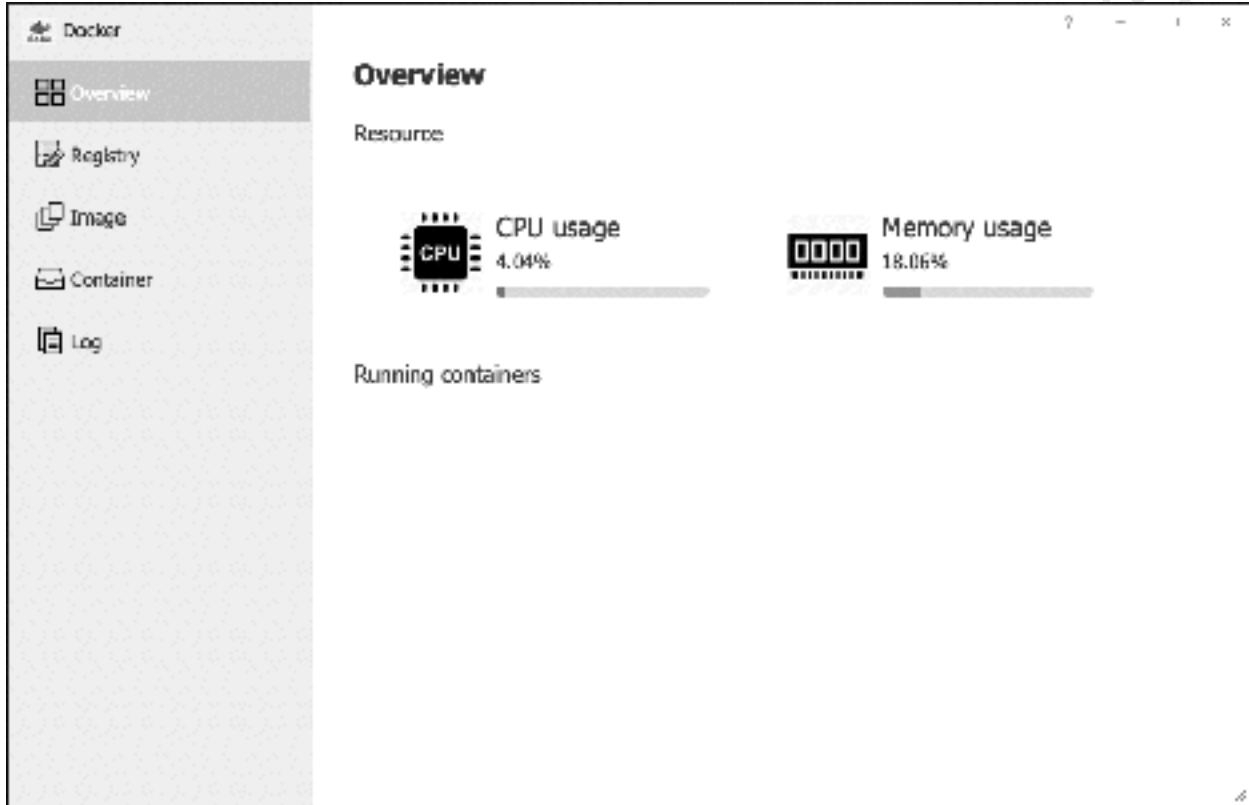


Figure 151: Docker Overview screen

Docker is based around the concept of *Containers*. A Container is a self-contained applications environment, largely isolated from the supporting operating system, which in this case is TOS. This approach offers good performance and enhanced security. Tens of thousands of ready-to-use containers are available from many different sources; often these are grouped together in hubs/repositories/registries and Docker on TOS has been pre-set to the most popular one. Note that the quality of these containers varies enormously: a degree of diligence is required and specialized technical knowledge may be required to use most of them.

In this example, we will install a simple example. Click on **Registry**, to display a scrollable list of containers (in simple terms, the Registry can be thought of as a type of App Store). To search for a particular container or type of container, enter a keyword in the search area and, having found it, highlight and click the **Download** button. In some instances this may result in an additional dialog box, giving some variants e.g. based on version number.

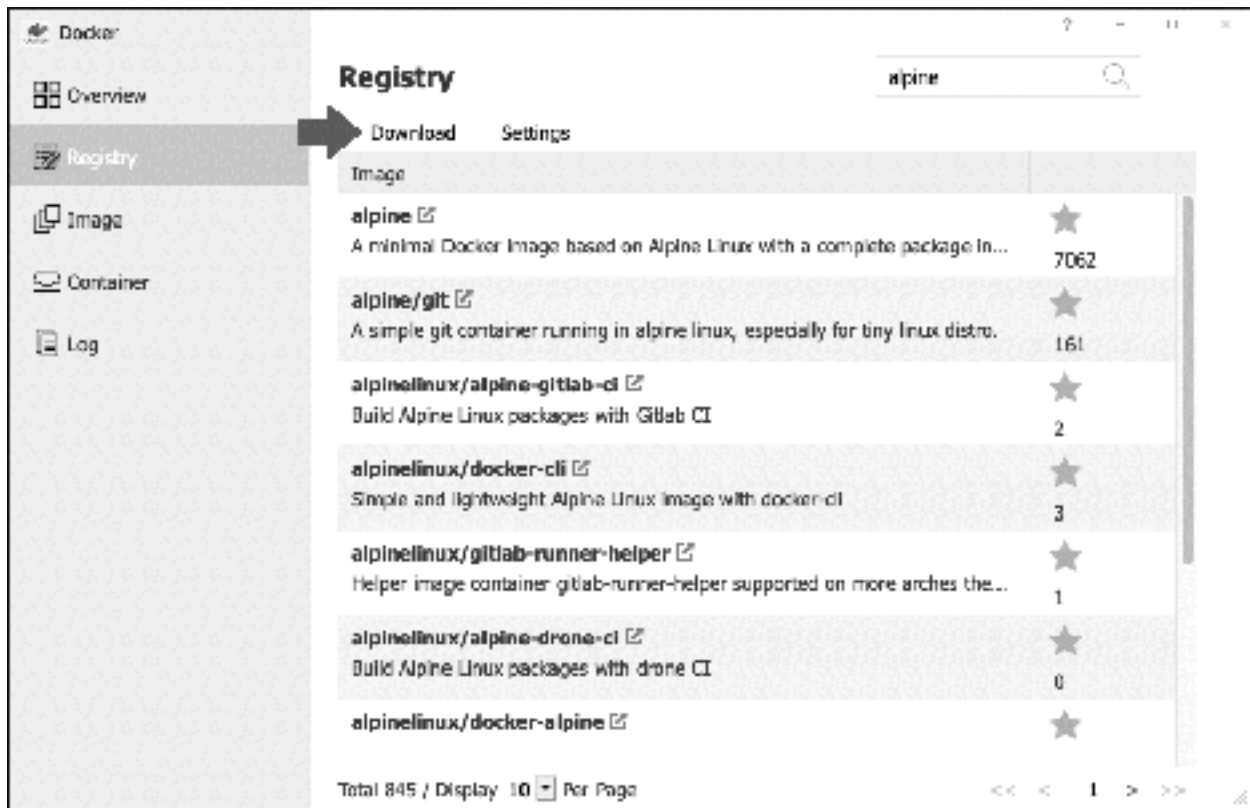


Figure 152: Registry listing/search

Containers are often quite small and so download relatively quickly. Downloaded ones appear on the *Image* tab. Highlight it and click the **Launch** button to display and define the settings. On the *General Settings* tab, ticking the **Enable** box enables the *CPU priority* to be set and *Memory limit* to be defined, along with automatic restart. The additional tabs are for Network, Port Settings and other parameters, as may be advised by the developer of the container or in accordance with your own requirements. Click **Apply**.

Free edition. Do not

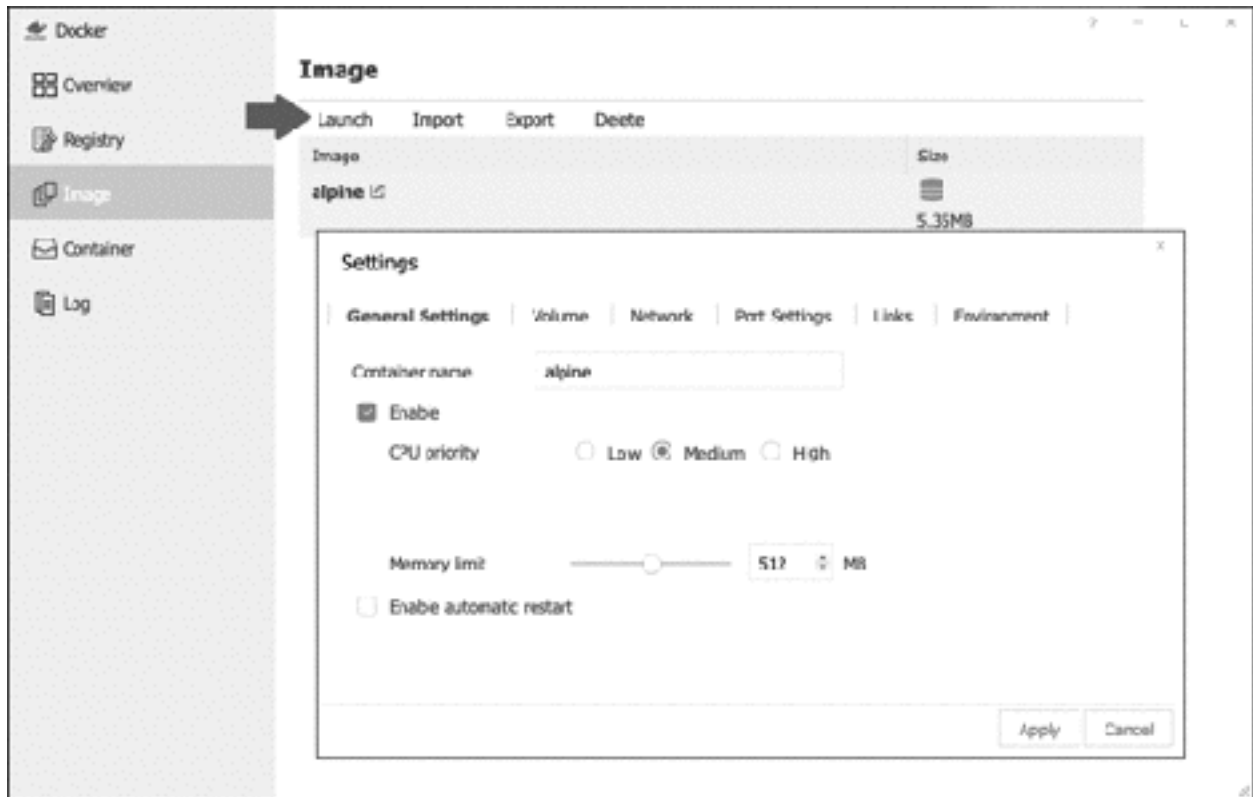


Figure 153: Image Settings

The Container will now begin execution. The Overview screen provides a quick summary of running containers, but they are managed from the **Container** section of Docker. Use the **Operation** dropdown to Start, Stop, Restart or Delete the container. Clicking the **Details** button displays detailed information and provides Process and Log details.

Free edition. Do not copy.

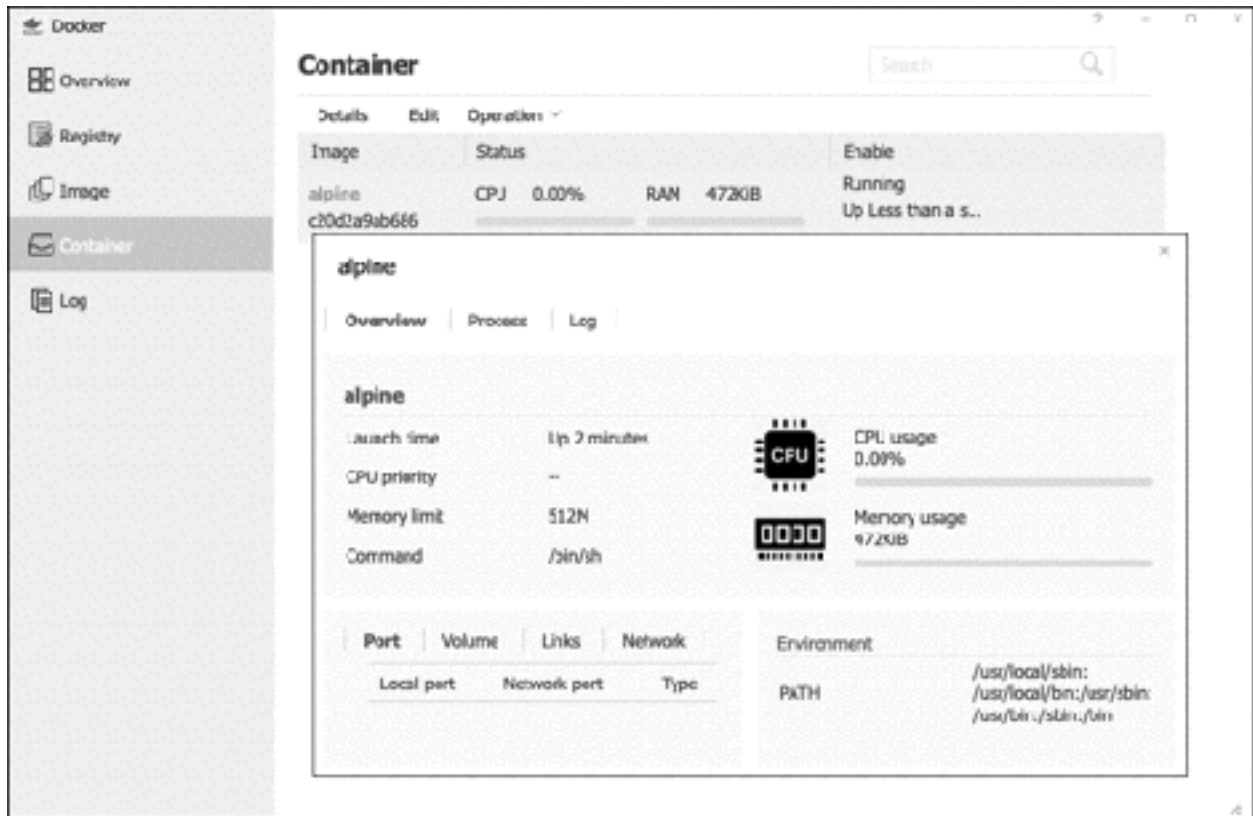


Figure 154: Details for a running container

11.10 Dynamic DNS (DDNS)

The Remote Access capability of TOS as described in [2.7 Setup Remote Access](#) will suit most people. As an alternative to the TNAS ID, it is possible to use *Dynamic DNS* (DDNS). This can be more efficient when handling a larger number of users, plus removes any dependency on the TerraMaster relay services, for those who may have concerns about such matters. Also, consider setting up a DDNS address if you intend using a VPN, as discussed in a subsequent section.

The first step is to setup DDNS. It is easy to find a website on the internet – you simply enter its name e.g. www.ctacs.co.uk, www.Terra-Master.com or whatever you are interested in. But what is the name - strictly speaking, the *hostname* - of your TNAS on the internet? The answer is: it does not have one as standard; it just has a number in the form of a public IP address; you might not be aware of what that number is; that number may be changed from time-to-time by your internet service provider. DDNS services address these issues by giving you a unique name and automatically updating what goes on behind the scenes when the underlying IP address changes. Numerous organizations provide DDNS services, some for free and others on a commercial basis and numerous popular ones are supported by TerraMaster. Before progressing, you will need to register an account with one, which you can do from their websites.

To setup DDNS, launch **Remote Access** from the desktop and click **DDNS** to display this screen (note that some information has been blocked out for privacy purposes):

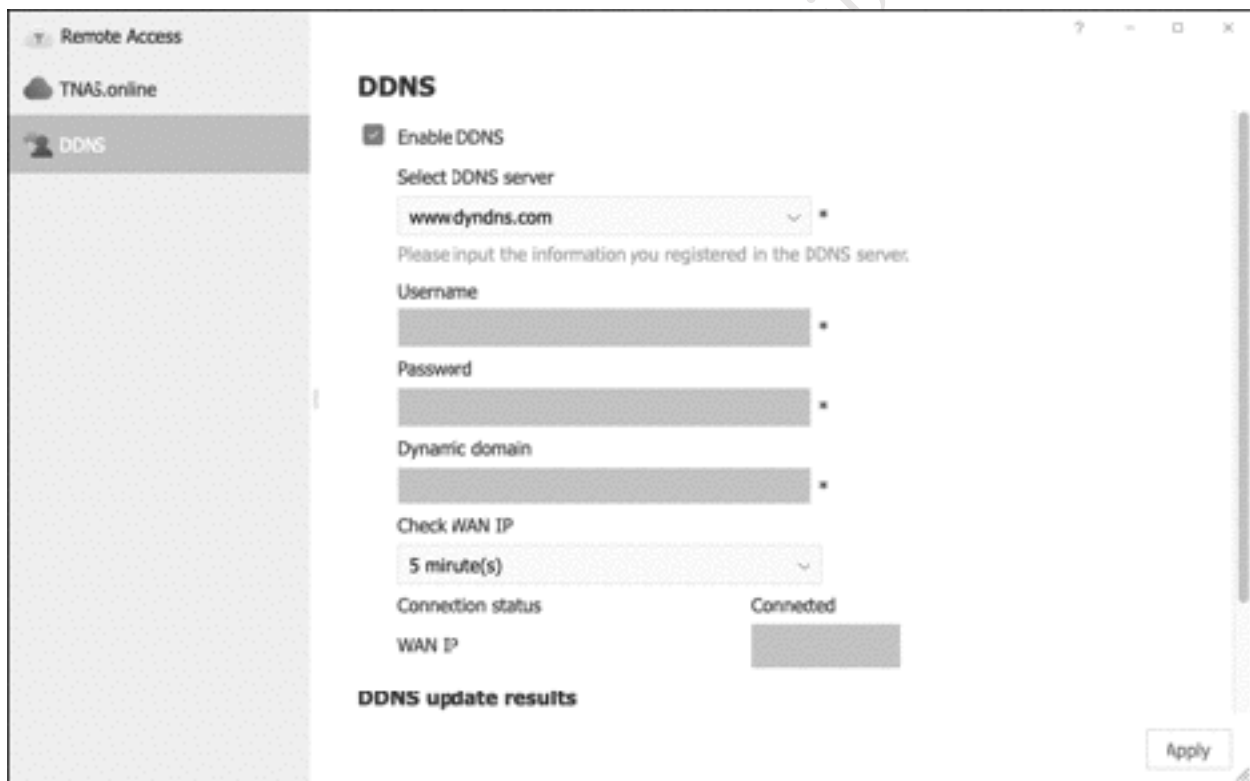


Figure 155: Screen for configuring DDNS

Tick the **Enable DDNS** box. Use the **Select DDNS server** dropdown to choose your provider. Enter your *Username*, *Password* and the *Dynamic domain* name that you acquired during registration. Click **Apply** and after a few seconds the status should change to 'Connected'.

The next step is to configure the router and as TOS cannot do this automatically, it will have to be done manually. This consists of forwarding ports 8181 to the internal IP address of the server and instructions for doing so with most popular routers can be found at the www.portforward.com website.

You can now test the system. Go to a computer, launch a browser (e.g. Chrome, Firefox, Safari) and enter the DDNS hostname that you registered. You should be greeted with the main TOS logon screen after a few seconds. If it cannot be found or you see the logon screen for your router instead, do not worry: some routers do not support a feature called *NAT Loopback*, which is required for this type of internal testing. So, the next step is to check if the server can be accessed from outside the premises; if it can then everything is working.

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

11.11 VPN (Virtual Private Network)

The purpose of a *Virtual Private Network* or VPN is to securely extend a network to users who are offsite, such as home workers or those in a remote office - you can think of it as equivalent to having a very long network cable that reaches out from the office for 10, 100, 1000 miles/kilometres or more. However, instead of an actual cable, the connection goes over the internet and uses powerful encryption and other techniques to maintain security. One advantage of a VPN is that it allows full access to files and folders for editing, just as if in the office. The downside is that a VPN can be difficult to setup, configure and diagnose. TOS goes a long way towards making it easier and it usually works, but if it does not then be prepared for some pain.

VPNs come in several variants, based around different protocols: *PPTP*, *OpenVPN* and *L2TP/IPSec*. PPTP (“*Point-To-Point Protocol*”) is widely supported on many different types of clients but is relatively old and has some security weaknesses compared to the alternatives. OpenVPN is popular, although requires a third-party piece of software to be installed on Windows PCs. L2TP/IPsec may be considered to be the best practical solution as it is supported natively by Windows, Mac and other clients. The focus is on L2TP/IPSec in this guide, although the others are basically similar in setup and operation should you have reason to use them instead.

Note 1: some governments block VPN access, particularly to computer systems located outside of their territory.

Note 2: VPN services are also used to provide anonymous access to the internet, for instance to avoid censorship and geographical restrictions. That is a different use of the term and NAS-based VPNs do not provide this capability.

Note 3: At the time of writing, TerraMaster’s app – *VPN Server* - is available only for x86-based TNAS and not for ARM-based models.

Setting up the VPN Service

Begin by downloading and installing *VPN Server* from Applications. Launch it using the icon on the Desktop. All aspects of managing the VPN are controlled from this app, which initially has a spartan appearance on the *Overview* screen. Configuration is controlled from the *Settings* screens:

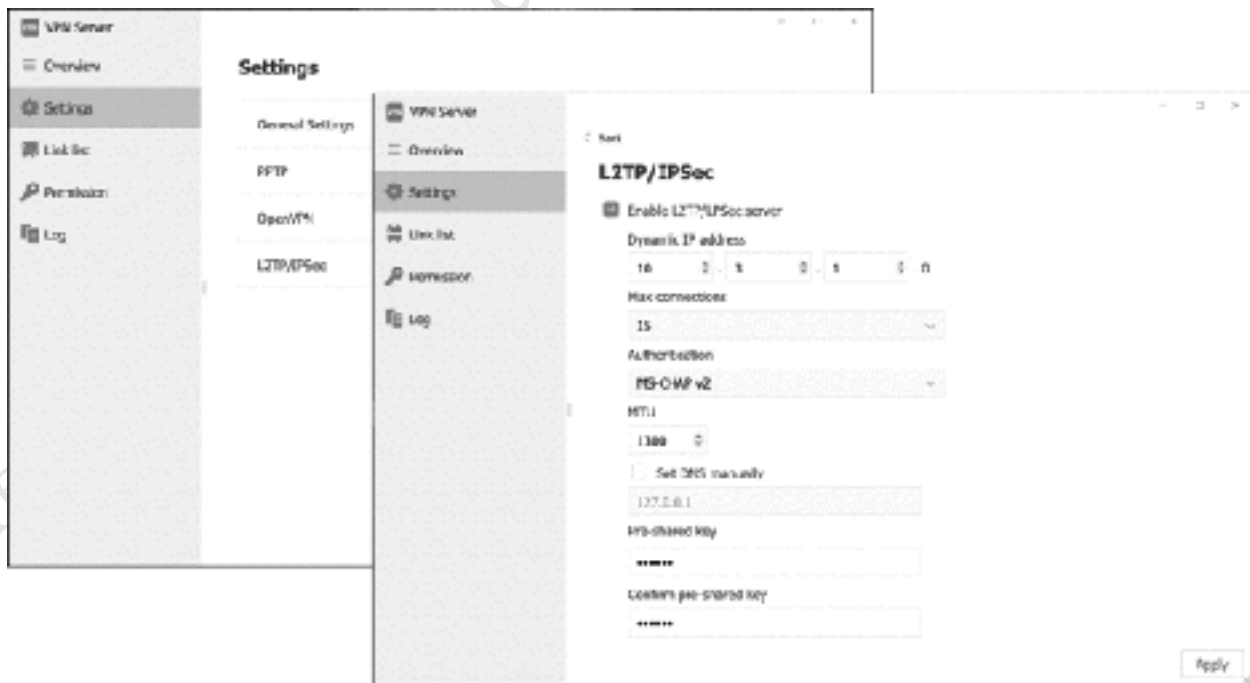


Figure 156: L2TP/IPSec configuration screen

Minimal work is required to get VPN running on the server. Click **Settings > L2TP/IPSec** and tick the **Enable L2TP/PPTP VPN server** box. The VPN has a range of dynamic IP addresses associated with it; the key principle here is that the IP range is different from that used within the internal network so if, for example, the internal network uses the *192.168.nnn.nnn* addressing scheme, then the VPN could be set to use the *10.nnn.nnn.nnn* addressing scheme (or the other way around). In most cases, VPN Server will propose a suitable range, which can simply be accepted. The maximum number of concurrent connections can be specified using the dropdown, which you might want to do for performance considerations. The *Authentication* and *MTU* values can be left as is. To optionally improve performance in larger configurations with dozens or hundreds of VPN users, the DNS Server value can be set manually. The *Pre-shared key* is effectively a password. It should be between 6 to 12 characters in length, non-obvious and include a mixture of letters, numbers and special characters. Having made the changes, click the **Apply** button.

The users who will have access to the VPN need to be specified. Click **Permission** and on the resultant screen place ticks against the required users and the protocols they are permitted to use. In this example, *admin* has access to all protocols and *louiseb* has access to L2TP/IPSec protocol. In order to add a user, the password (Pre-shared key) defined above needs to be provided.

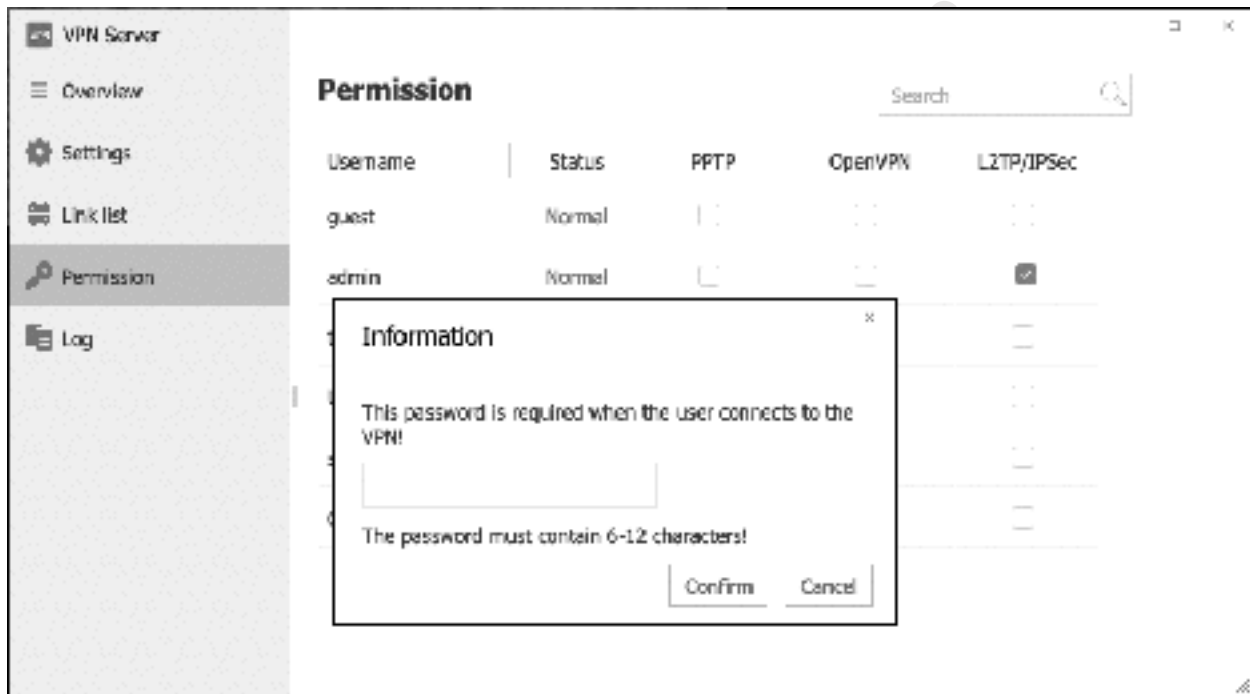


Figure 157: Adding VPN users

An optional screen is **Settings > General Settings**. On a TNAS with multiple network interfaces, you could choose to run the VPN over a dedicated one for performance reasons. For instance, if there were two interfaces you could run the internal network from one and the VPN over the other. There is also a link from this screen to *Automatic Block*, a security feature described in [6.5 Account Safety](#). Click **Apply**.

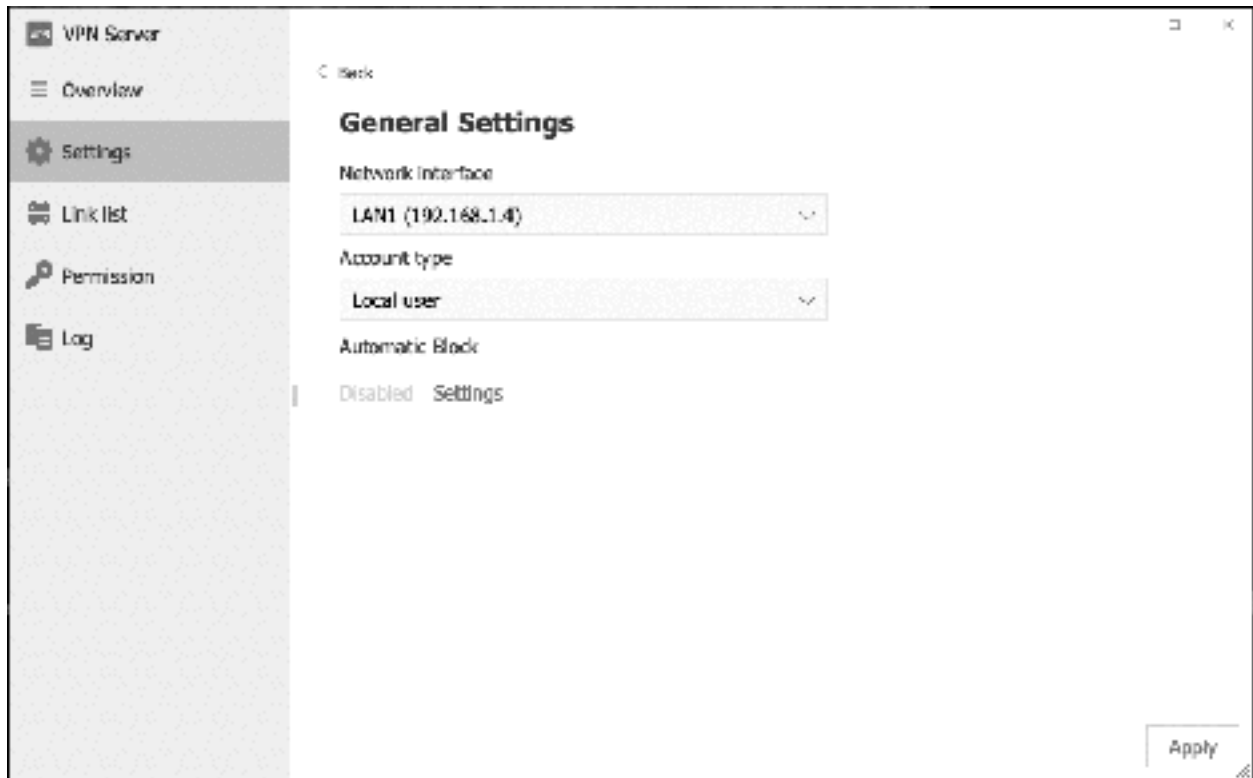


Figure 158: General Settings

At this point, the VPN is ready and the clients can be configured. Instructions for three popular platforms are given below.

Configuring Windows 10 Clients

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

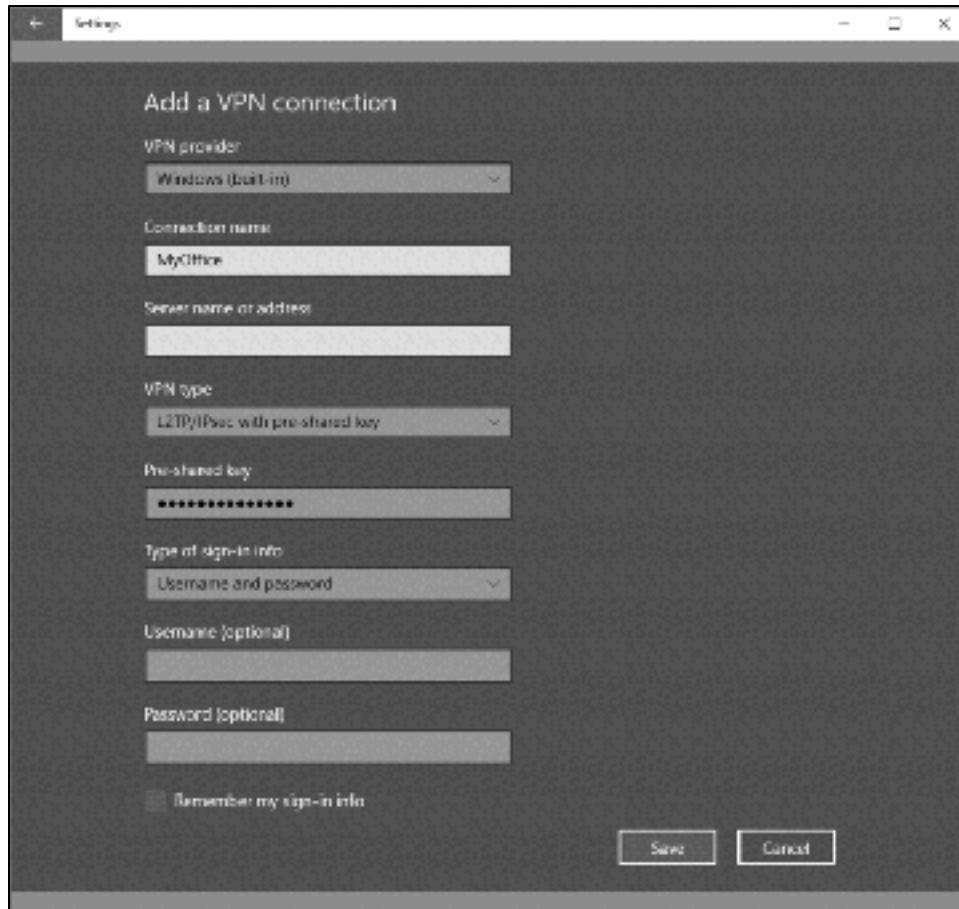


Figure 159: Adding a new VPN connection

Click **VPN provider** and choose *Windows (built-in)*, which will normally be the only option available. Specify a **Connection name** e.g. *MyOffice*. For the **Server name or address** enter the TNAS Online address that you registered in [2.7 Setup Remote Access](#) or a DDNS address as discussed in [11.10 Dynamic DNS \(DDNS\)](#).

Set the **VPN type** to *L2TP/IPsec with pre-shared key*, then enter the pre-shared key you specified when configuring the VPN Server. The **Type of sign-in info** should be *Username and password*. For security reasons it is suggested that you do not hardcode the **Username** and **Password** do not tick the **Remember my sign-in info** box. Click **Save**.

The newly defined connection will now be listed on the VPN section within Settings. Click it and then click the **Connect** button. You will be prompted to Sign in – enter your **Username** and **Password** as defined on the server and click **OK**. After a short while, the status will change to *Connected*.

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

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

Configuring Windows 7 Clients

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

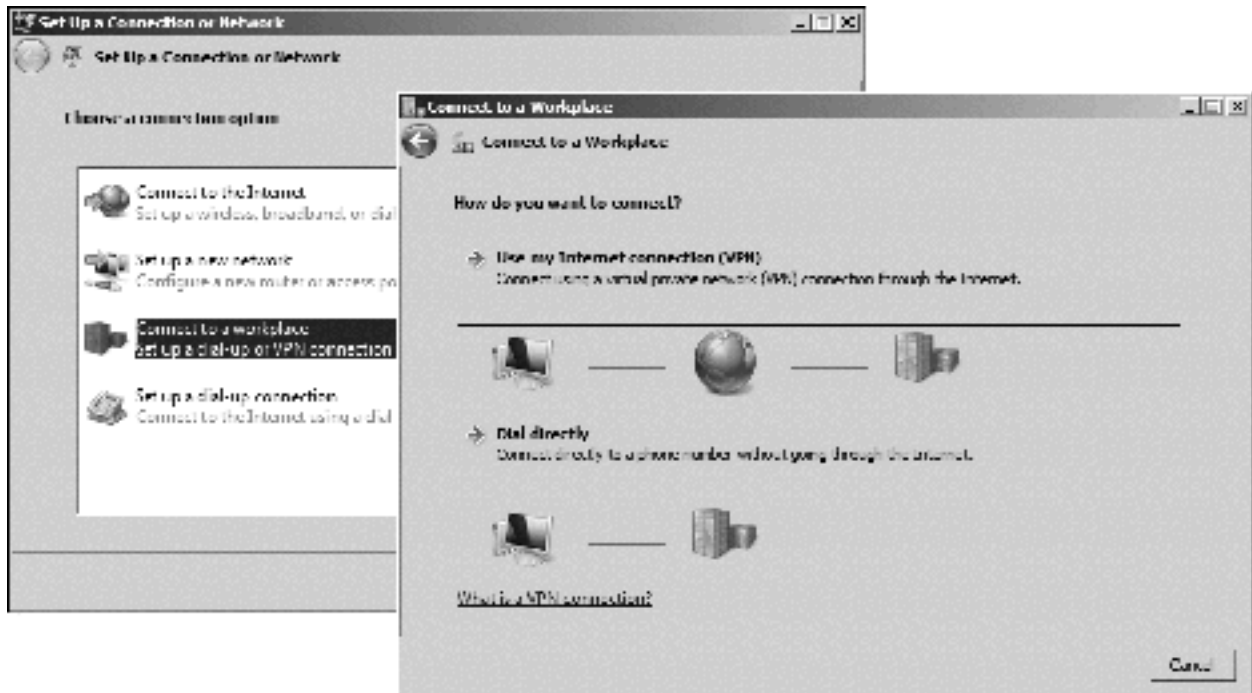


Figure 160: Setup a new connection in Windows 7

You will need to enter the TNAS Online address that you registered in [2.7 Setup Remote Access](#) or a DDNS address as discussed in [11.10 Dynamic DNS \(DDNS\)](#) as the **Internet address**. Tick the **Don't connect now** box and click **Create**:

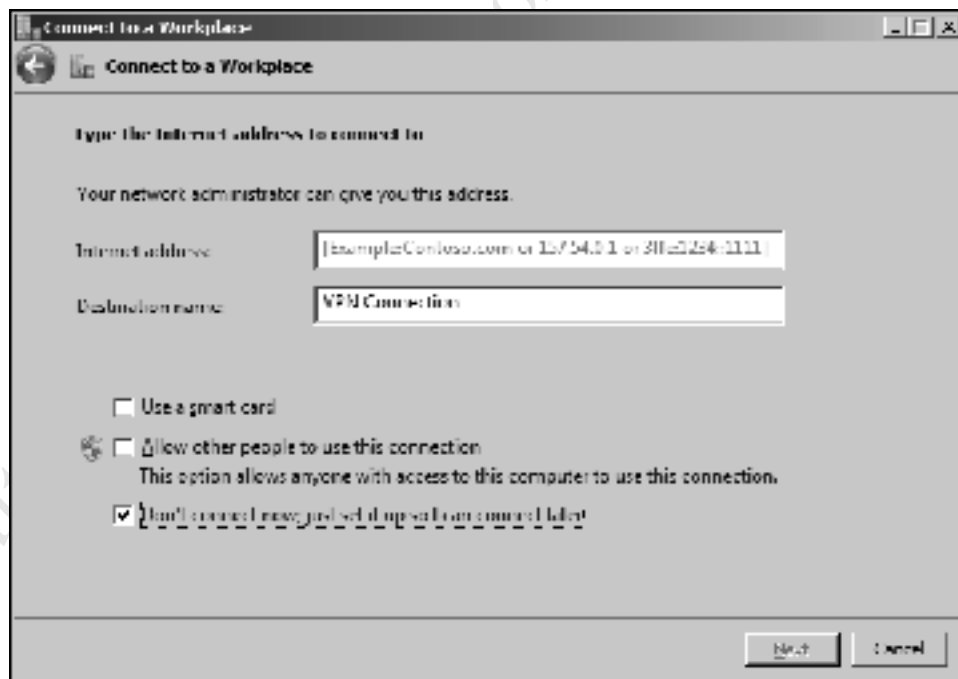


Figure 161: Specify the internet address of the server

A confirmation message is displayed, stating that 'The connection is ready to use'. However, we still need to do something else first, so click **Close**.

Return to the **Control Panel** and choose **Network and Sharing Center**. Click **Change adapter settings**; the newly created VPN connection will be listed alongside the computer's normal network connection(s).

Right-click it and choose **Properties**. Click the **Security** tab. *Change the Type of VPN to **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)** and change *Data Encryption* to read **Optional encryption (connect even if no encryption)**. Click the **Allow these protocols** option. Click the **Advanced settings** button and enter the pre-shared key which you specified when installing the VPN Server (password?). Click **OK**. The panel should appear as follows; click **OK**:*

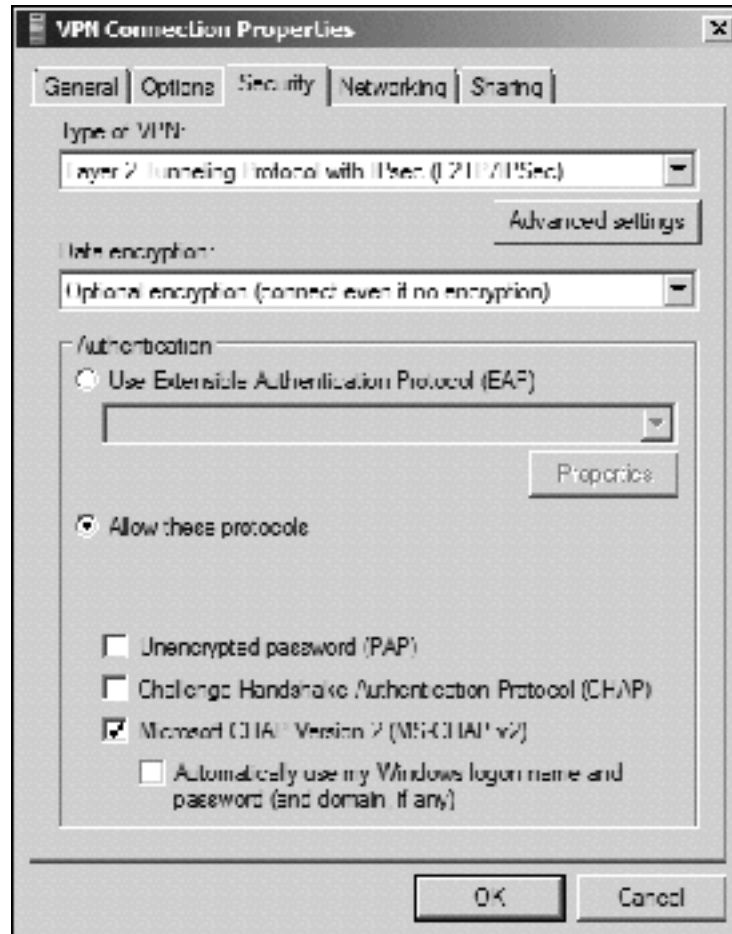


Figure 162: VPN Connection properties

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

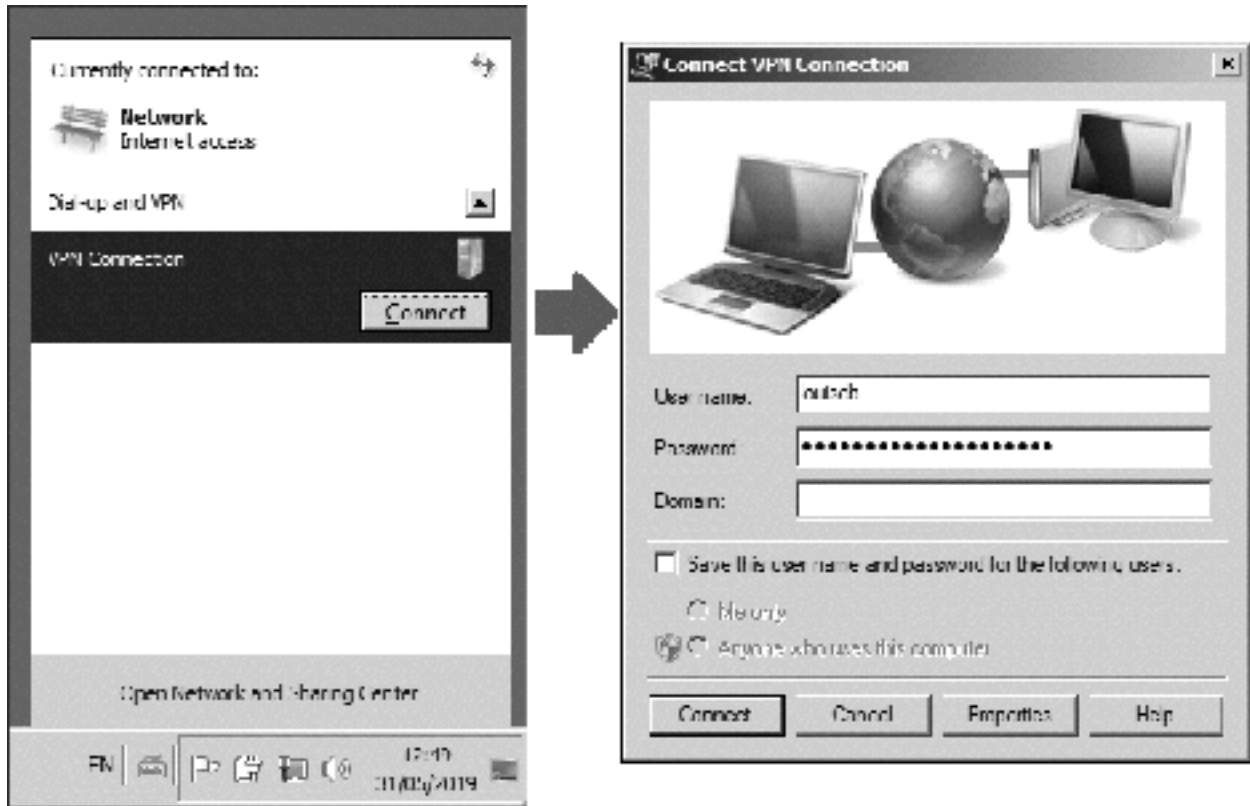


Figure 163: Connecting to the VPN

A few seconds later you should be connected. The first time you connect you may receive a prompt asking to choose the network location; a choice of Home, Work and Public is offered and you should choose **Home** or **Work** (there are no significant differences between them in this context).

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

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

Configuring Mac VPN Clients

Go into **System Preferences** and click **Network**. Add a new network service, with an **Interface** of **VPN** and a **VPN Type** of **L2TP over IPSec**:



Figure 164: Add a new network service

Enter the **Server Address** (the TNAS Online address that you registered in [2.7 Setup Remote Access](#) or a DDNS address as discussed in [11.10 Dynamic DNS \(DDNS\)](#)) and the user's **Account Name**. Click the **Authentication Settings** button and specify the **User Authentication Password** (i.e. the user's password on the server) and the **Machine Authentication Shared Secret** (i.e. the Pre-shared key which was defined during the configuration of the VPN Server). Click **OK**. On the main screen, tick the **Show VPN status in menu bar** option, followed by **Apply**:

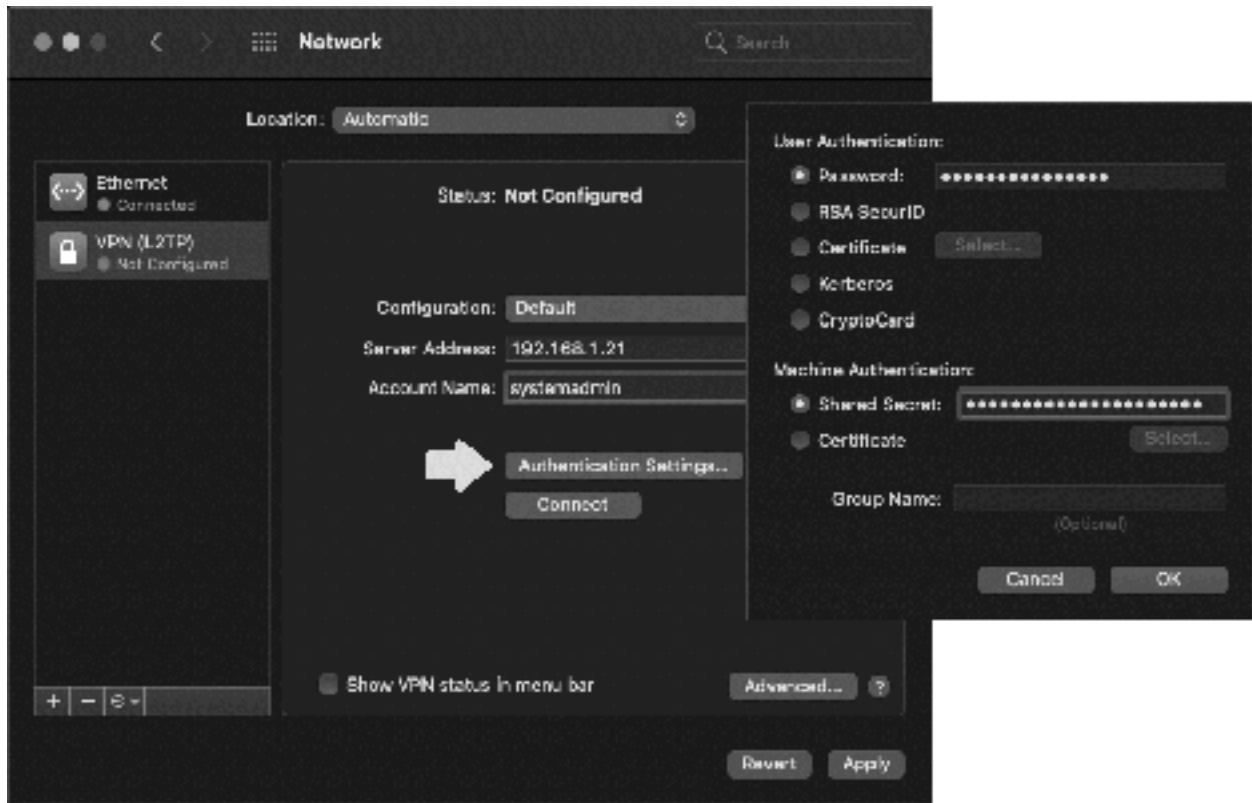


Figure 165: Configure the VPN Service

Click the VPN icon on the menu bar and choose **Connect VPN (L2TP)**. Click **Connect** and enter your user name and password when prompted.

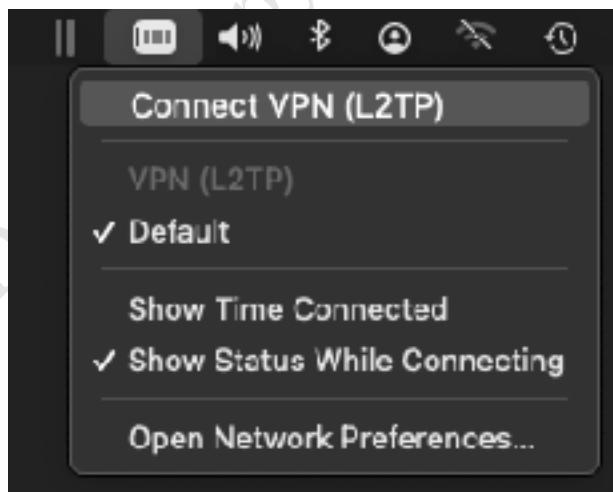
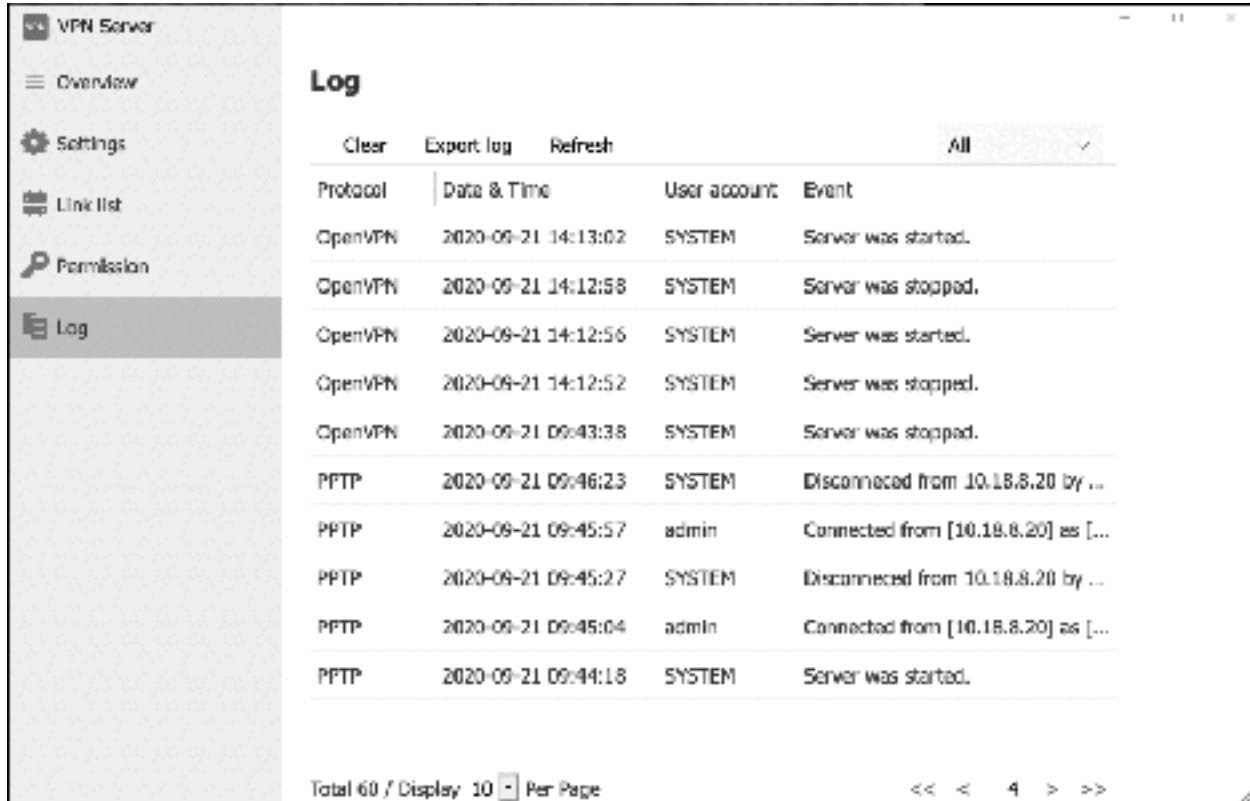


Figure 166: VPN icon on Menu bar

You can now access resources on the Server as though you were in the office. When you have finished, click the VPN icon on the Menu bar and click **Disconnect**.

Monitoring the VPN

The status of the VPN can be monitored from the server in two ways. A log file of VPN activity is generated; to access it, go into the **VPN Server** app and click **Log**. The log should be cleared down on a regular basis e.g. once a week; to do so, click **Clear**. You can also click **Export log** to generate a permanent copy in Excel spreadsheet format.



Protocol	Data & Time	User account	Event
OpenVPN	2020-09-21 14:13:02	SYSTEM	Server was started.
OpenVPN	2020-09-21 14:12:58	SYSTEM	Server was stopped.
OpenVPN	2020-09-21 14:12:56	SYSTEM	Server was started.
OpenVPN	2020-09-21 14:12:52	SYSTEM	Server was stopped.
OpenVPN	2020-09-21 09:43:38	SYSTEM	Server was stopped.
PPTP	2020-09-21 09:46:23	SYSTEM	Disconnected from 10.18.8.20 by ...
PPTP	2020-09-21 09:45:57	admin	Connected from [10.18.8.20] as [...
PPTP	2020-09-21 09:45:27	SYSTEM	Disconnected from 10.18.8.20 by ...
PPTP	2020-09-21 09:45:04	admin	Connected from [10.18.8.20] as [...
PPTP	2020-09-21 09:44:18	SYSTEM	Server was started.

Figure 167: VPN Log file

To view a list of connected clients, click **Link List**. If required, a user can be forcibly disconnected from the VPN by highlighting their entry and clicking **Disconnect**.

11.12 Connecting Via a Proxy Server

In a typical small business environment, a router is used to connect the server and network directly to the internet. However, in some circumstances the connection might be indirect and through a *proxy server*. An example of such a circumstance might be where managed or serviced offices are being used or in an educational establishment, in which case the TNAS needs to be configured appropriately.

Click **Control Panel > Network > Proxy Connection**. Tick the **Connect through a proxy server** box and enter the details of the proxy server, which will need to be obtained from the person or organization that controls it. Generally, this will consist of entering an IP address or domain name and port number and ticking the **Do not enable proxy server for local address** option. If authentication details are required, tick the **Enable proxy server authentication** box and enter them. If there are separate proxy servers for HTTP and HTTPS traffic, click **Advanced** and enter the details. Click **Apply**.

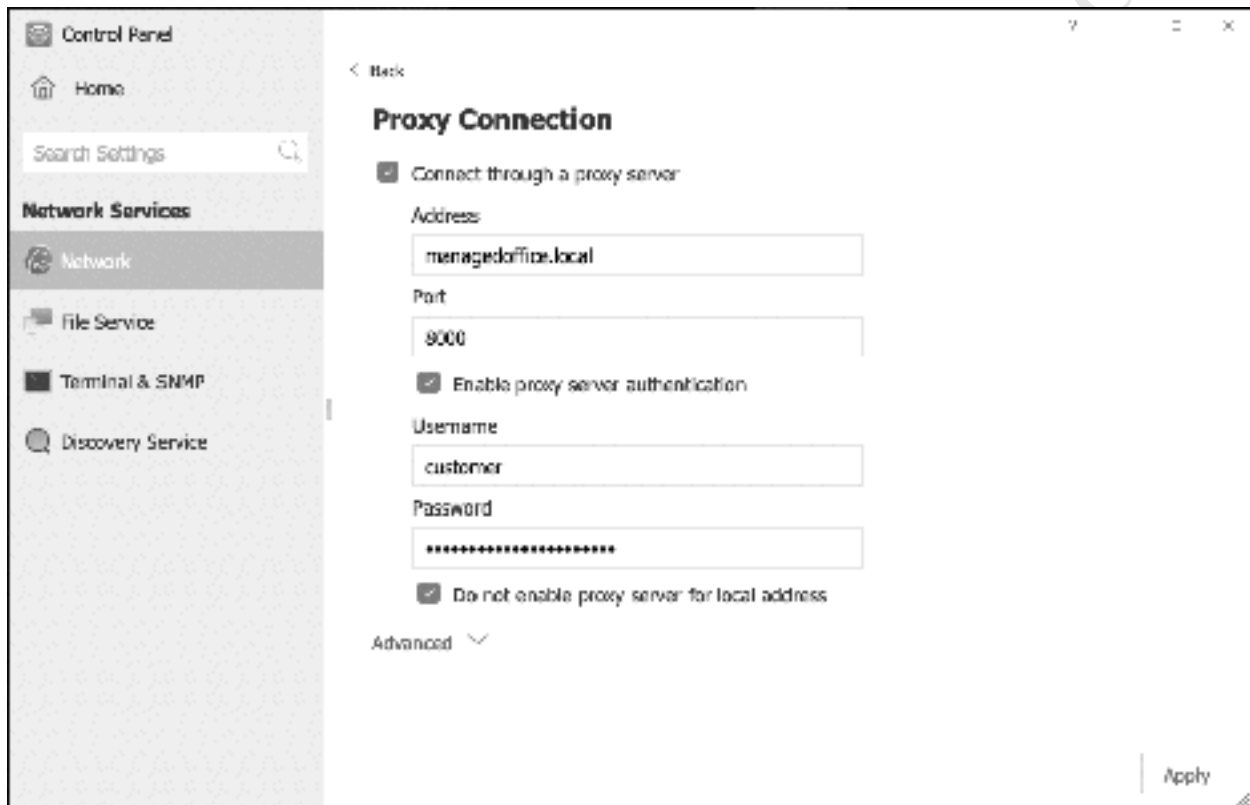


Figure 168: Proxy Connection settings

Free edition.

11.13 Alternative Operating Systems

TerraMaster NAS devices run the TerraMaster Operating System, TOS. However, the underlying hardware on Intel-based models is largely identical to that of a standard computer and, on some models at least, TOS is stored on a small memory stick/thumb drive plugged into an internal USB socket on the TNAS motherboard. Additionally, some motherboards contain built-in display circuitry and if the correct cable is obtained, can be connected to a standard computer monitor. All of this raises an intriguing possibility, as it opens the possibility of replacing that memory stick with one containing another operating system altogether. Whilst this is a highly specialized project and one that will only appeal to enthusiasts, it is possible. For an example of what can be done, go to YouTube and search for ‘terramaster server 2016’. It should be emphasized that this is strictly a project for enthusiasts and that it is not supported in any way by TerraMaster, who advise against it.

11.14 Unable to Login as Admin User

It is possible to encounter a problem where you cannot login as the *admin* user because the password is no longer recognized, giving a ‘Password error!’ message. If you try the Reset password option from the login screen, a message of ‘Email error!’ instantly appears. Nothing that you are aware of has changed and everything was working previously; in fact, ordinary user accounts may still be working normally and able to access data.

Your first port of call should be to contact TerraMaster for support, as described below. The following advice is ***last resort*** when all else has failed, comes without warranty and is done entirely at your own risk, but may work in some situations. It involves re-installing TOS but relies on the fact that it is harder than you might think to trash the data on the drives (something that needs to be kept in mind when disposing of a TNAS, as described in a subsequent section). The steps are as follows:

- Power off the TNAS
- Remove the hard drives; if there are multiple drives, be sure to make a note of the sequence
- Power the TNAS back on
- Use the TNAP PC utility to search for the device on the network and click to login
- A message will appear, advising ‘No HDD detected’. Re-insert the hard drives and work through the steps
- A message appears, asking if you want to ‘use the system already installed on the hard drives’ or to ‘install new TOS system’ – choose the latter. Follow the remaining steps to complete the installation.
- There will be a reminder that the data on the hard drives will be lost, but in fact there is a very good chance that it will be retained (although there is no guarantee).

Once installation has been completed, check that you can login as *admin*.

11.15 Contacting TerraMaster for Support

TerraMaster are able to offer technical support by telephone and email throughout the world, with dedicated accounts in several territories. If you need to contact them, provide as much information about the problem as possible, including model number; version of TOS being used; symptoms of problem; anything which may have occurred leading up to the problem; any attempts you have taken to rectify matters.

Contact details (telephone):

USA, Canada, Mexico: +1 866 658 7798
UK: 0800 048 8283

Contact details (email):

USA: support_us@terra-master.com
UK: support_uk@terra-master.com
Germany: support_de@terra-master.com
Italy: support_it@terra-master.com
France: support_fr@terra-master.com
Spain: support_es@terra-master.com
Worldwide: support@terra-master.com

It is also possible to grant temporary remote access to TerraMaster's support team, so they can access the TNAS to diagnose and fix problems. To do this, click the **Technical Support** icon on the Desktop. Tick the **Enable remote assistance** box and specify how long it is available. Copy the *Identification key* that is generated and provide it and your admin password to the support team when requested.

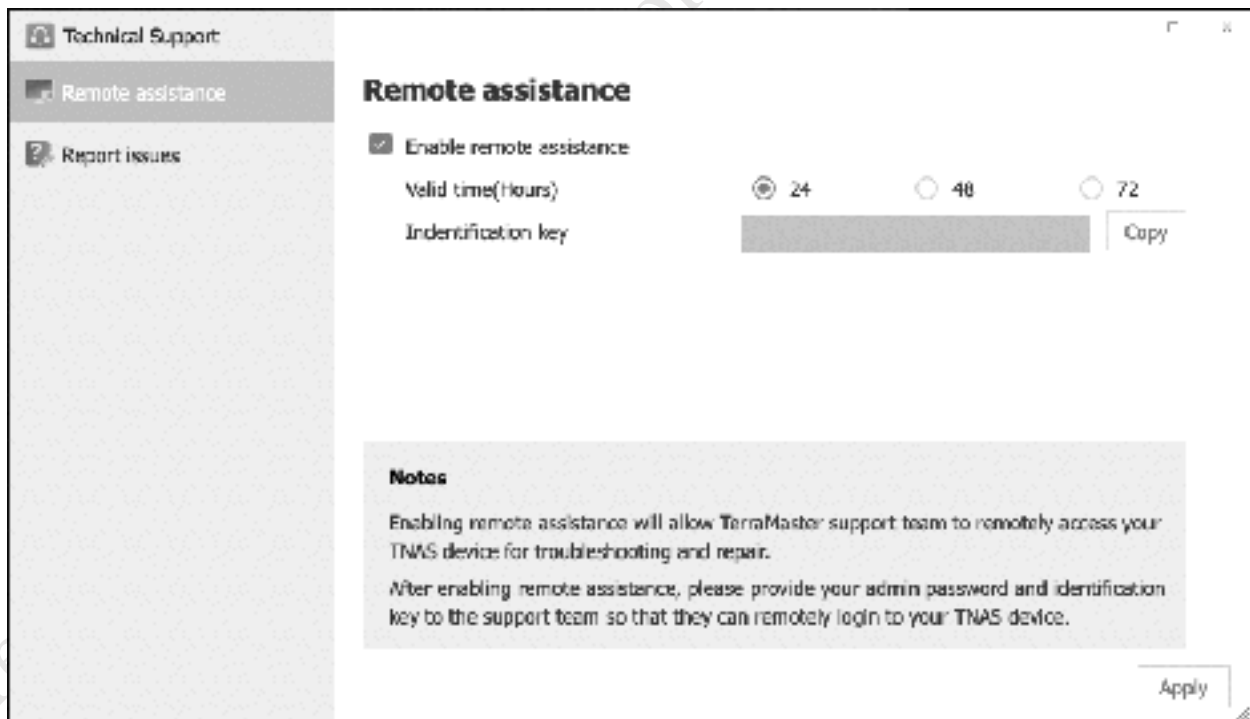


Figure 169: Remote Assistance panel

11.16 Preparing a TNAS for Disposal

There may come a time when the TNAS needs to be disposed of or repositioned, perhaps because it is being replaced with a newer model. There are two steps that need to be followed: firstly, remove the data; secondly, reset the TNAS.

Remove data

If there is a requirement to re-use the data with another TNAS, it should be safely backed up using one of the techniques described in section [7 BACKUPS](#). The drives can then be removed. If the drives are to be re-used elsewhere or disposed of, they should be reformatted. One way to do this is with an external USB-to-SATA adapter or docking station, used in conjunction with a separate desktop or laptop computer.

Reset the device

Go to **Control Panel > Update & Recovery > Restore to Factory Default**. Tick the **Restore to factory default** box, followed by **Apply**. In the confirmatory panel that pops up, enter the admin password and click **Confirm** to proceed:

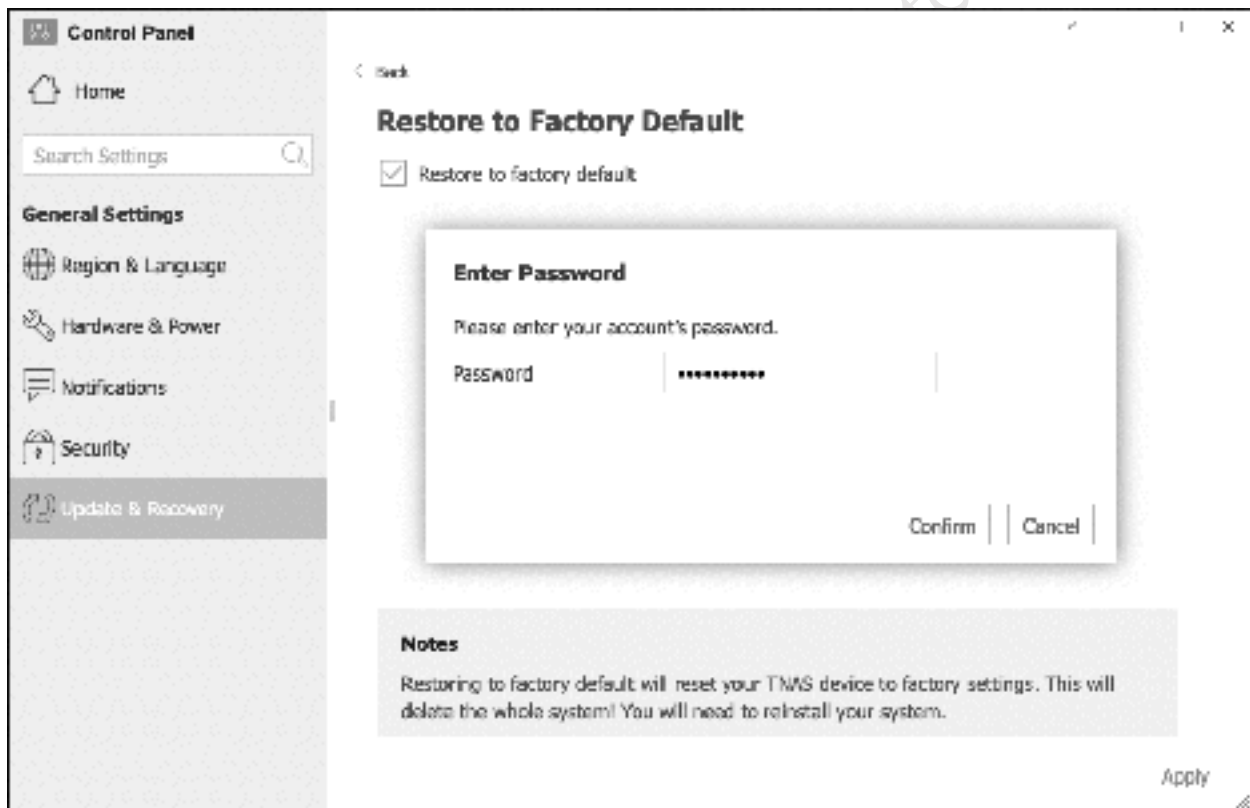


Figure 170: Restore the TNAS to factory default

A warning message will be displayed, which needs to be confirmed to continue. It is important to note that resetting the TNAS does not destroy any data on the drives, which is why they need to be removed if it is being disposed of.