Asustor NAS Setup Guide

Nicholas Rushton, BA Hons.
Callisto Technology and Consultancy Services

ADM 3.5.5, Updated May 2021

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 ASUSTOR Systems Inc. and this is an independently produced publication.

Table of Contents

ABOUT THIS BOOK

ASUSTOR is the NAS device of choice for discerning purchasers: great hardware able to provide shared storage, backups, cloud services, multimedia streaming, run applications and more, combined with flexibility and ease of use through the ADM software. But this power and capability comes at a price and setting up an ASUSTOR 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 ADM 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 organized as follows and can be considered in three main parts:

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

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

Chapters 9 through 12 are other topics to investigate and includes ways to make your system more capable and useful, such as multimedia, surveillance and setting up remote access for using the server from outside the home or office.

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 four decades, 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: *ASUSTOR NAS 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; QNAS Setup Guide; Using Windows 10 as a Server; Little Book of TerraMaster.*

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. Please be sure to check your junk/spam folder if you have not received a reply in your inbox.

1
GETTING STARTED

1.1 Overview

If you are reading this, then it is likely you already know what Network Attached Storage (NAS) is and may have purchased or are about to purchase an ASUSTOR 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 by 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 ASUSTOR it is called ADM. Usually, the term *firmware* rather than operating system is used to describe it. ADM has such familiar features as a Desktop, taskbar and a drag-and-drop interface, analogous to what people are accustomed to with Windows, Mac and Linux PCs and, although specifically designed for NAS duties, ADM also has the ability to run apps that provide additional capabilities. The current version at the time of writing is ADM 3.5 and this guide is based around it; however, if you have a slightly different version you should still find most of it applicable.

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? Many things, but some popular uses include:

- Providing extra storage for computers
- Being 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
- Running a private cloud system, with controlled remote access to your data. Similar in principle to services such as Dropbox, OneDrive and iCloud, but totally under your own control and with effectively unlimited usage plus no subscription charges
- Providing a sophisticated video surveillance system for the home, office or other premises
- Being a comprehensive development platform for software developers
- As an alternative to a traditional business file server running Windows Server or Linux

An alternative name for a NAS box is *server* and we will use both terms interchangeably in this book.

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

NAS (server) - this is the heart of the network, which runs ADM and upon which data is stored
Backup device – for example, an external USB drive connected to the server
Internet connection - this may be a separate router or an all-in-one wi-fi router
Switch and Wireless Access Point(s) – to provide expansion in larger networks
Printer(s) – may be networked or plugged into the server with a USB cable
Desktops PCs and Laptops – running Windows, macOS or Linux, connected using Ethernet or wireless
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 in the following sections and later sections of the guide.

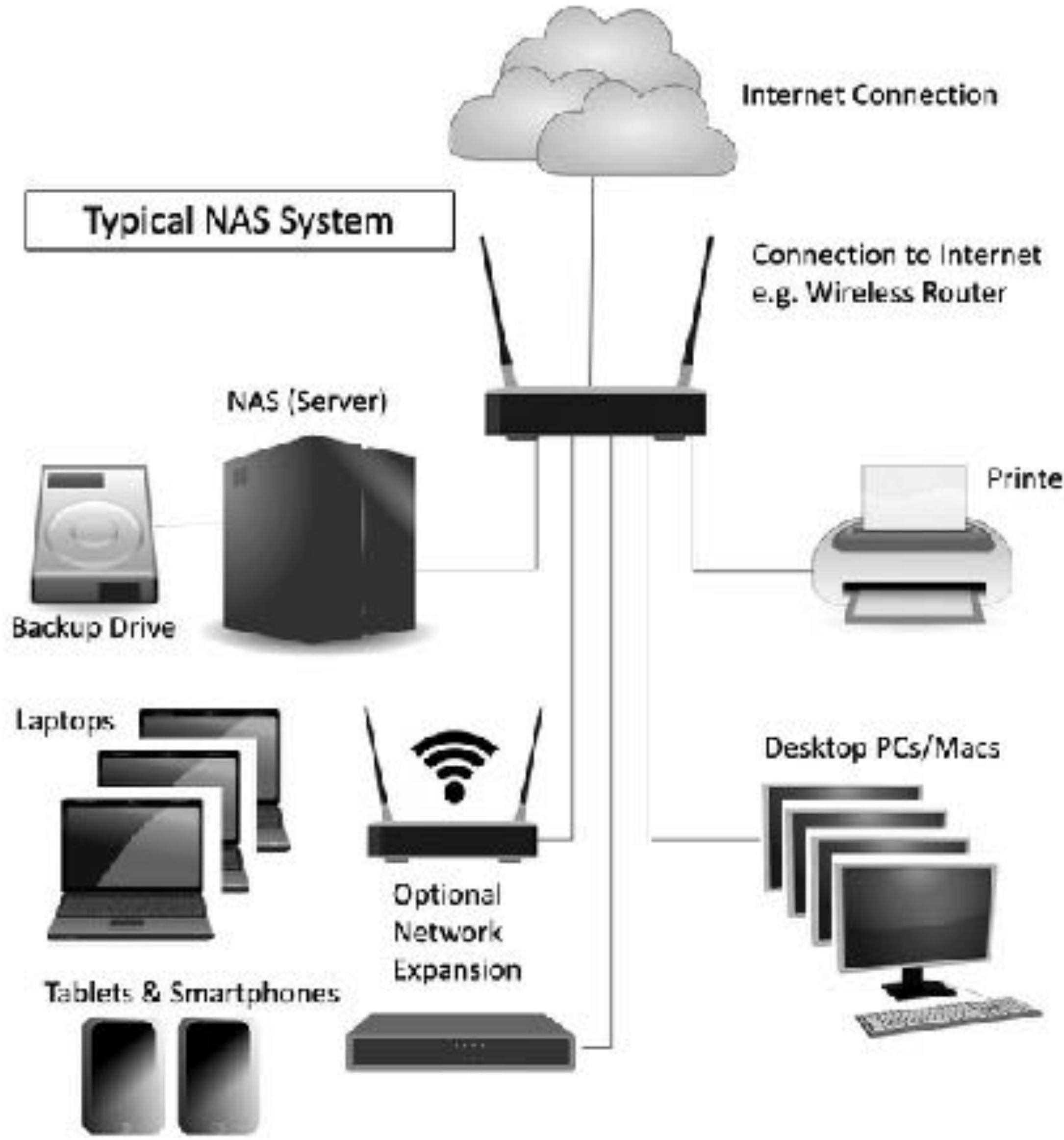


Figure 1: Typical NAS System

Just about any modern computer can be used with the NAS. 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 macOS and older versions of Mac OS X can be connected, as can Linux PCs. Devices running iOS (iPad, iPhone) and Android (tablets and Smartphones) can be connected, as can many smart televisions and gaming boxes. Chromebooks can also be used.

Suggestion: if you are at the research stage and yet to purchase or setup your ASUSTOR NAS, you may want to try out the free ADM Live Demo system, accessible from the ASUSTOR website. This allows you to test-drive the ADM interface and see how it is in operation.

1.2 Choosing an ASUSTOR NAS Model

ASUSTOR 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. The models vary according to form factor, number of disk drives that can be used, network adapters, performance, expandability and price.

Form Factor – ASUSTOR NAS boxes come in two basic varieties. Most are standalone units designed to sit on top of a cupboard or desk, whereas some are designed to be mounted in standard computer cabinets (racks) that take devices that are 19 inches/48cm wide. Home and small business users will typically use a standalone unit, but some businesses may already have a cabinet in place, perhaps to hold other equipment, in which case a rack-mounted version may be the better choice.

Number of Disk Drives – ASUSTOR NAS units can hold between 2 and 16 disk drives, depending on the model. Having more drives allows greater storage capacity and permits the use of RAID to improve resilience and throughput. Systems can be expanded through the use of external cases to allow more drives.

Networking – all models feature at least Gigabit Ethernet and many models have multiple network adapters. ASUSTOR have led the way in offering 2.5 Gbe and 10 Gbe adapters, for greater network speeds and throughput.

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

Expandability – Some models feature PCIe expansion slots, enabling M2 SSD cache memory or additional network adapters to be added. Sometimes the memory is upgradeable.

ASUSTOR have grouped their models into four broad groups:

Personal to Home – aimed at personal and home users

Home to Power User– some of these models are designated NIMBUSTOR. They feature 2.5 GbE network ports and are targeted at enthusiasts and gamers

Power User to Business – some of these models are designated LOCKERSTOR and feature 2.5 GbE network ports

Small & Medium Business – targeted at larger organisations. Some of these models are designated as LOCKERSTOR Pro.

Choosing the right model can be confusing as there is often overlap between them, but in general you want to buy the most capable model you can afford. If you have or are planning to have large amounts of data, then you should buy a model with multiple drive bays, especially one that supports SSD caching as this gives a good performance boost. If you are particularly interested in multimedia and home entertainment, a number of models feature HDMI output for direct connection to a television set.

Typical Usage Scenarios

These are some examples of how some people are using ASUSTOR 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. She was also curious about exploring the other possibilities offered by NAS, such as surveillance cameras, whilst minimizing the costs. Her choice was the 2-bay AS3102T v2. The portable USB hard drive she was using previously was re-positioned as an external backup drive for the NAS.

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 run other operating systems such as Windows and Linux. His choice was a 2-bay NIMBUSTOR 2 (AS5202T), with upgraded memory to run virtualization software.

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 NIMBUSTOR (AS5304T), with the ability to hold 72TB storage and which has a HDMI socket for direct connection to the family television set.

Small Business – Helen Translation Services 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 full remote access, but without the ongoing costs associated with commercial cloud services. They also felt more comfortable with the idea of their data being totally under their direct control, rather than with a third party. Their solution was the 8-bay LOCKERSTOR 8 (AS6508T), which is backed up over 10 Gigabit Ethernet to a separate AS4004T located elsewhere in the main premises.

1.3 Disk Drives

NAS devices are not supplied by ASUSTOR with disk drives already installed in them. Instead, the idea is that the customer buys the drives separately and installs them, which is quite easy to do and does not even need a screwdriver on most models, else buys a ready-populated unit from a reseller. This approach is generally better because it offers more choice.

ASUSTOR NAS units are very flexible in terms of the brand and type of disk drives that can be used in them. However, it is strongly recommended to use drives that have been specifically designed for use with NAS, as such drives are optimized for continuous 24x7 operation over several years and take into account the heat and vibration characteristics of NAS enclosures, along with other requirements. Although such drives are typically 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 a greater number of 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 most NAS models can use either, although some may require adaptor brackets to use 2.5” drives. The 3.5” drives offer higher capacities and better price performance, but 2.5” drives use less power, generate less vibration, are generally quieter in operation and increasingly popular. For systems with more than one drive, it is preferable that all the drives are the same model and capacity, although this not an absolute prerequisite. In a NAS 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 0, RAID 1, RAID 5 and so on. The idea is to improve reliability and performance through the use of multiple drives to provide redundancy and share the workload and a more comprehensive description can be found in section 11.2 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 will fall.

ADM is able to take full advantage of SSDs for regular storage but can also use them to boost performance through *caching*, where they act as a high-speed buffer to the mechanical hard drives. Depending on the model, caching can be done using 2.5” SSD (SATA) drives or with M.2 or M.2 NVMe drives in dedicated slots. As drives used for caching take a lot of hits, it is recommended to use high quality ones, rather than low-cost consumer units. This topic is discussed in section 11.5 SSD Caching.

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 domestic setting or small business, everything might link back to an internet-connected all-in-one router or wireless router, whereas in a larger business 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 where possible. Wired devices should be of Gigabit (1Gb) specification or better. Some models support higher speed Ethernet connections of 2.5 Gbe or 10 Gbe; if so, it is worthwhile connecting at least the NAS to a high-speed switch, even if much of the infrastructure runs at slower speeds.
- 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 you sign-up with them. These are often of average quality, for instance the Ethernet ports may not be Gigabit or the latest wireless standards may not be supported. Spending money on professional or prosumer (“professional consumer”) routers and switches will usually give better performance and reliability.

1.5 Location and Electrical Considerations

NAS 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 causing disruption.

It is possible that data loss can occur if the electrical mains power fails whilst the NAS is running. The best way to mitigate against this is to use an intelligent UPS (Uninterruptible Power Supply) with the NAS; in the event of power problems this will enable it to continue operating for short periods and then to shut it down in an orderly manner if necessary. Most popular brands work with ASUSTOR (e.g. APC, CyberPower, Powercom) and a full list of supported UPS’s can be found on the ASUSTOR website. In a business environment, the use of an UPS should be considered essential. If a UPS is not used, which is commonly the case in a domestic environment, then the NAS should at least be connected to a clean electrical power supply via a surge protector.

2

INSTALLATION OF ADM

2.1 Overview

Unlike a desktop computer or laptop, which usually come with an operating system already installed, such as Windows 10 or macOS, a NAS does not and hence the first thing to do is to install ADM. There are two main* ways of doing so:

ASUSTOR Control Center – this is a utility program available for Windows and macOS computers. It locates the NAS on the local network, downloads and installs the latest firmware, plus performs the initial configuration work.

AiMaster – this is a utility for initializing and managing the NAS using a smartphone or tablet. It is available for both iOS and Android from the respective app stores.

Both methods are comprehensively described in this chapter. Having installed ADM, you will then be able to setup the users (3 USERS), define shared folders (4 SHARED FOLDERS) and connect computers and other devices (5 ACCESSING THE SERVER).

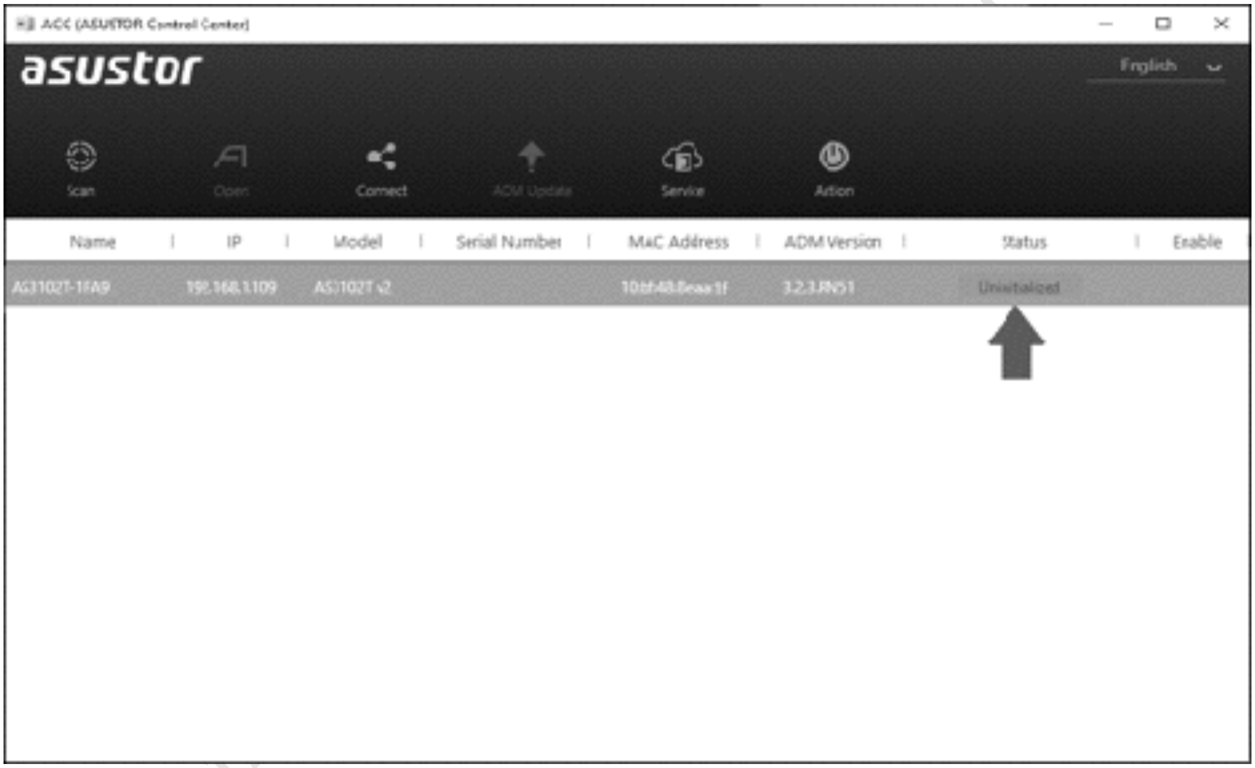
** There is also a third way. A small number of ASUStor models feature an LCD screen and control buttons and ADM can be installed using them, without the need for a computer or mobile device. This less-common method is not covered in this guide.*

2.2 Installation Using ASUSTOR Control Center

Having installed disk drives in the NAS and connected an Ethernet cable, power on the NAS. It will take a minute or two to start up, during which time is will beep a couple of times.

Go to the *acc.asustor.com* website and download and install the Windows or macOS version of the *Asustor Control Center* utility as appropriate to your computer and region of the world. Depending on how updated your copy of Windows is, ACC may load additional supporting components from Microsoft. At the time of writing, the macOS version generates a security warning when you try to run it for the first time; to resolve this, go to the Applications folder on the Mac and hold down the Ctrl key when clicking on its icon, then click **Open**.

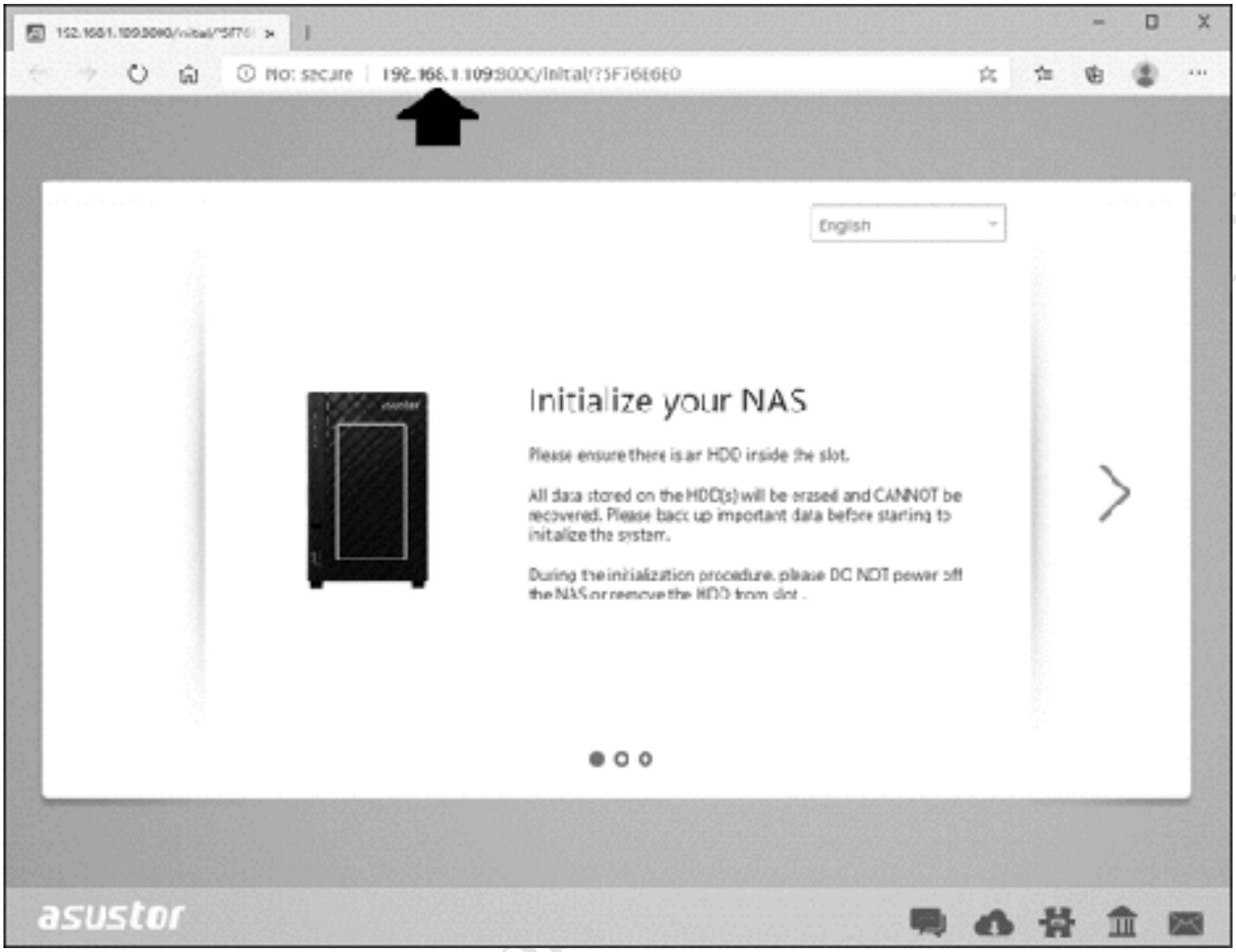
Upon running it for the first time, you may receive a warning message that the computer's firewall has blocked some features and you will need to click **Allow Access**. After a few seconds the following screen will appear; if the NAS has not been found, click the **Scan** icon in the top left-hand corner. If it still does not appear, check that it is powered on and that there is no problem with the network connection.



Name	IP	Model	Serial Number	MAC Address	ADM Version	Status	Enable
AS3102T-1FA9	192.168.1.109	AS3102T v2		10:bf:48:8e:aa:1f	3.2.3.RN51	Uninitialized	

Figure 2: ACC utility

Click where it reads **Uninitialized** and the computer's browser will launch. Make a note of the numbers that appear in the address bar – it is the first four numbers that are important e.g. 192.168.1.109 in this example.



152.168.1.109:8000/initial/?5F76
Not secure
192.168.1.109:8000/initial/?5F76E6E0
English
asustor

Initialize your NAS

Please ensure there is an HDD inside the slot.

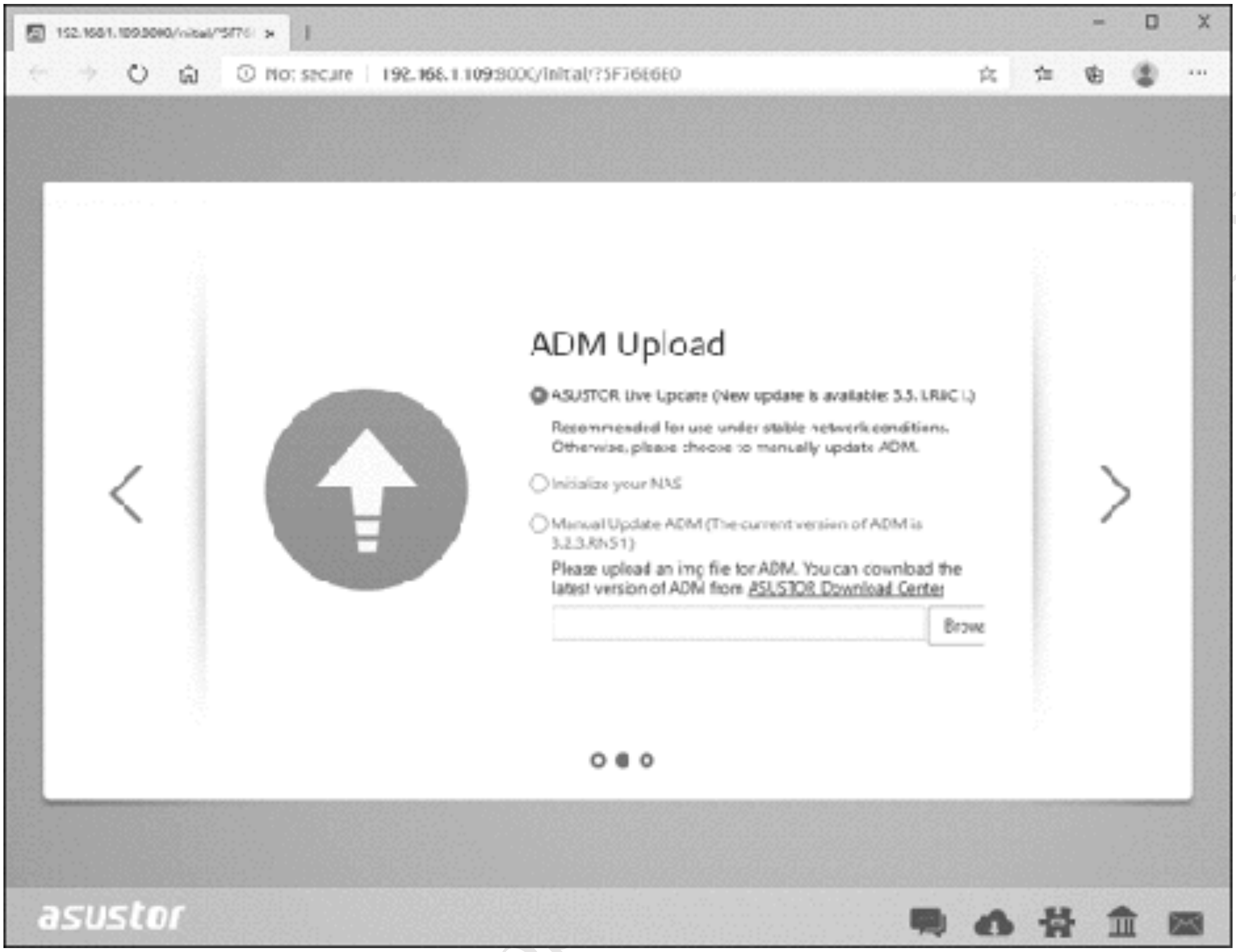
All data stored on the HDD(s) will be erased and CANNOT be recovered. Please back up important data before starting to initalize the system.

During the initialization procedure, please DO NOT power off the NAS or remove the HDD from slot .

Figure 3: Message about disk drives

The first screen is a reminder that the NAS needs to have at least one disk drive inside it and that any existing data on the drive(s) will be erased. Click the chevron (arrow) on the right-hand side of the screen to continue.

The next screen is for uploading a copy of ADM. There are three options: select the first one to upload the latest version of ADM. Click the arrow on the right-hand side of the screen to continue.



ADM Upload

● ASUSTOR Live Update (New update is available: 3.5.1.R8C1)

Recommended for use under stable network conditions. Otherwise, please choose to manually update ADM.

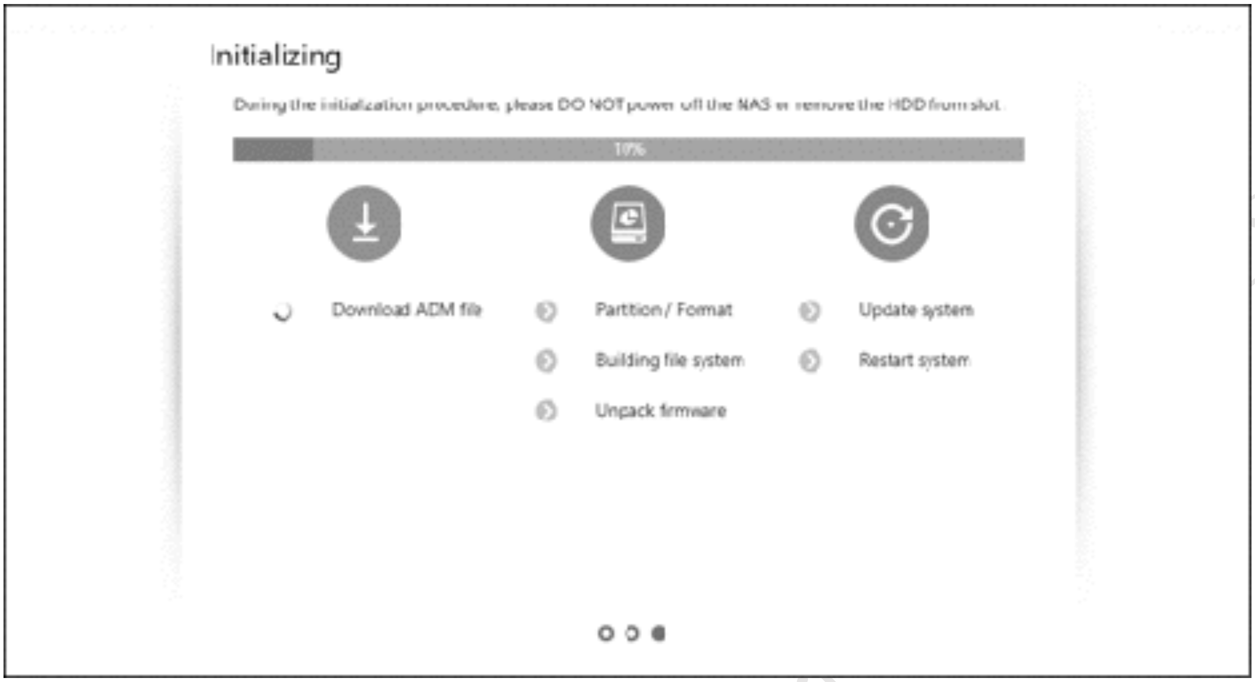
○ Initialize your NAS

○ Manual Update ADM (The current version of ADM is 3.2.3.RN51)

Please upload an img file for ADM. You can download the latest version of ADM from ASUSTOR Download Center

Figure 4: ADM Upload screen

Whilst the NAS is initializing, a status screen is displayed. This stage will take several minutes.



Initializing

During the initialization procedure, please DO NOT power off the NAS or remove the HDD from slot.

10%

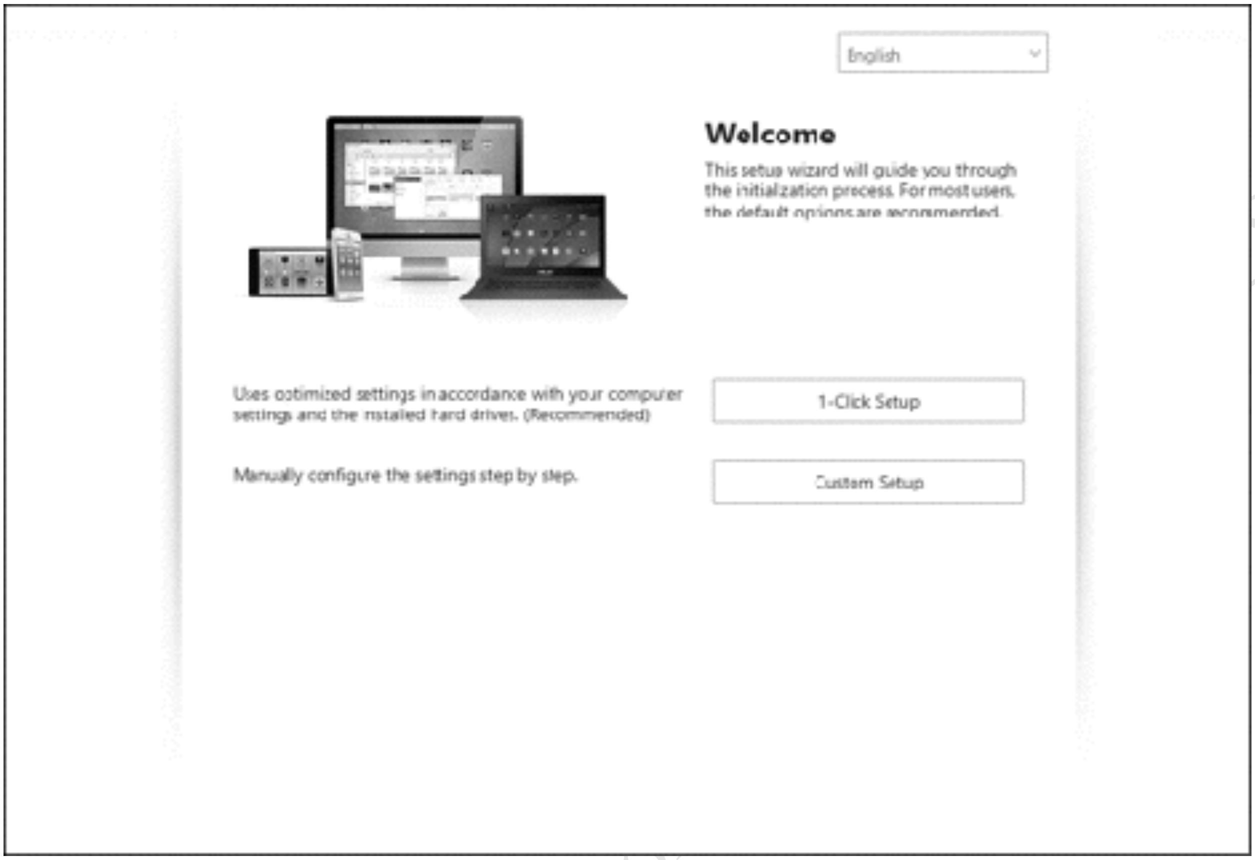
- Download ADM file
- Partition / Format
- Building file system
- Unpack firmware
- Update system
- Restart system

Figure 5: NAS Initializing

When the initialization process is complete, the setup wizard appears. There are two choices:

1-Click Setup – this is the easiest option, where the setup process makes a number of assumptions in order to get you up and running as quickly as possible. Many people will want to choose this option, particularly if new to NAS.

Custom Setup – as the name implies, this allows detailed control over the setup process. This is more suitable for experienced users or those with specific requirements.



Welcome

This setup wizard will guide you through the initialization process. For most users, the default options are recommended.

Uses optimized settings in accordance with your computer settings and the installed hard drives. (Recommended)

Manually configure the settings step by step.

Figure 6: Choose between 1-Click and Custom Setup

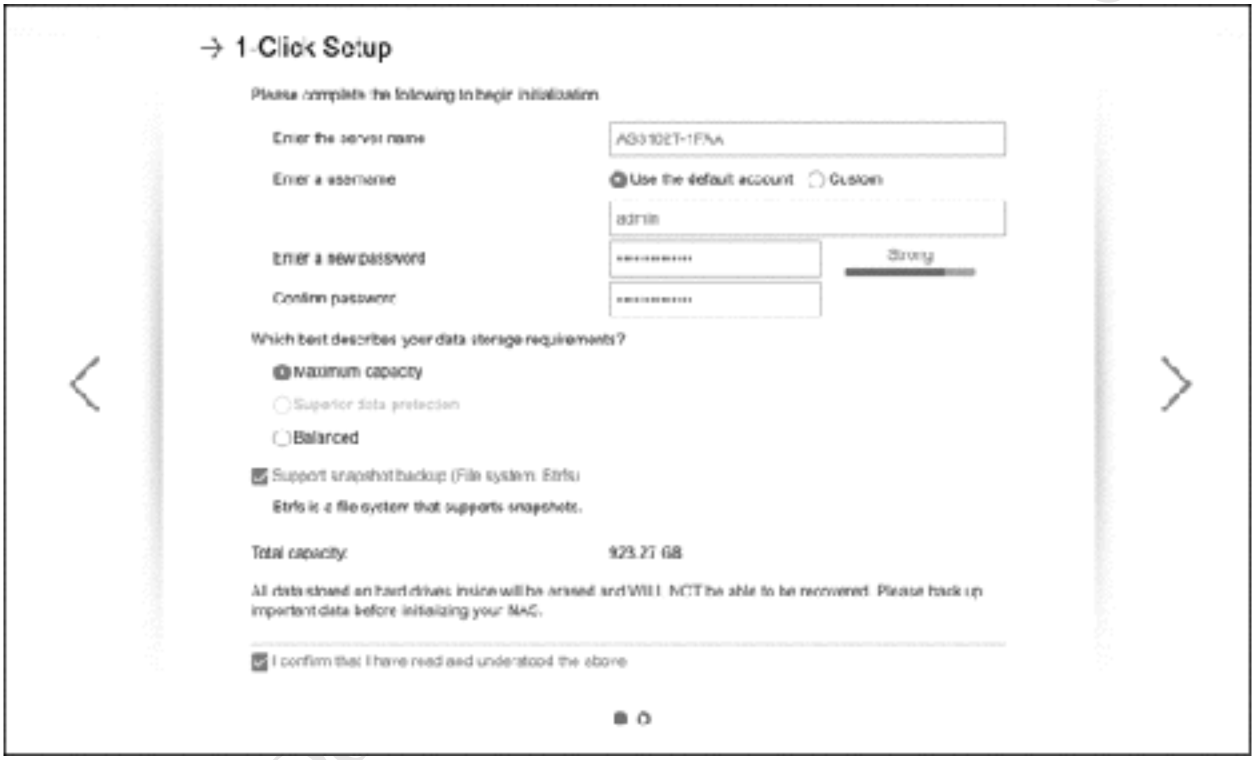
Make a choice. If you are taking the 1-Click Setup option, continue with 2.3 ACC 1-Click Setup Option below. If you are using the Custom Setup option, go to 2.4 ACC Custom Setup Option instead.

2.3 ACC 1-Click Setup Option

This first screen is for defining the essential characteristics of the NAS.

For the *server name*, it is suggested that you simply call it ‘*server’*, although if you have or envisage having further servers you may want to adopt a logical naming scheme e.g. *server1*, *server2,* or something meaningful to your organization such as location, business function, classroom etc.

The *username account* is the main account, used for administering and managing the server. The default is *admin* but can be changed to a customized name if you wish. Enter and confirm a password - use something non-obvious and preferably a mixture of upper- and lower-case letters, numbers and symbols and which does not include the username. ADM will provide feedback on the strength of the password and you want something that it considers to be ‘Strong’.



→ 1-Click Setup

Please complete the following to begin initialization

Enter the server name: AS3102T-1FAA

Enter a username: ● Use the default account ○ Custom

admin

Enter a new password: •••••••••• Strong

Confirm password: ••••••••••

Which best describes your data storage requirements?

● Maximum capacity

○ Superior data protection

○ Balanced

☑ Support snapshot backup (File system: Btrfs)

Btrfs is a file system that supports snapshots.

Total capacity: 923.27 GB

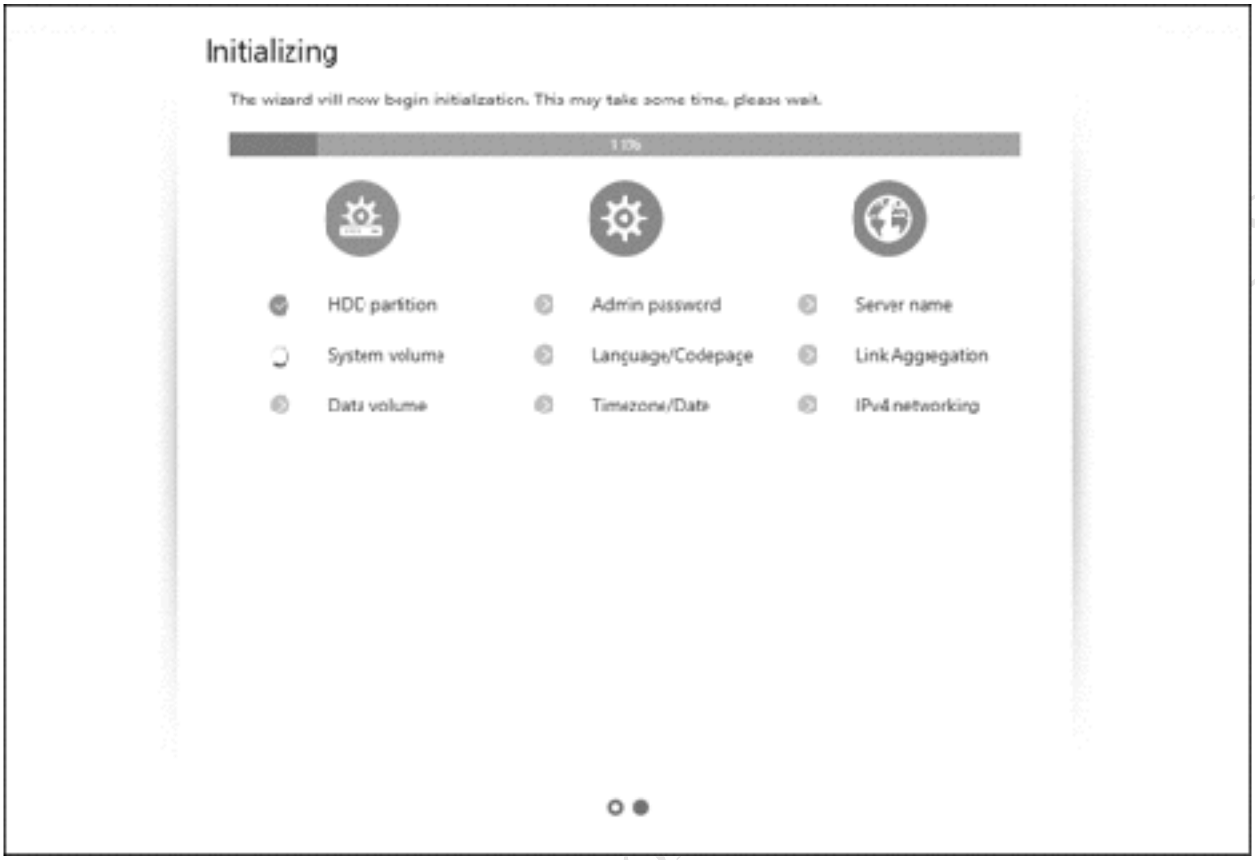
All data stored on hard drives inside will be erased and WILL NOT be able to be recovered. Please back up important data before initializing your NAS.

☑ I confirm that I have read and understood the above

Figure 7: 1-Click Setup screen

Underneath the password section is a question about your data storage requirements and the options available depend on what drives are installed in the NAS. Make a choice between *Maximum capacity*, *Superior data protection* or *Balanced*. You also need to decide if you want to use *Snapshots*, a backup feature whereby data is effectively ‘photographed’ at regular moments in time (if you have the option you should take it). Having made your choices, tick the **I confirm that I have read and understood the above** box and click the chevron (arrow) on the right-hand side of the screen.

A status screen is displayed whilst the NAS is initializing:

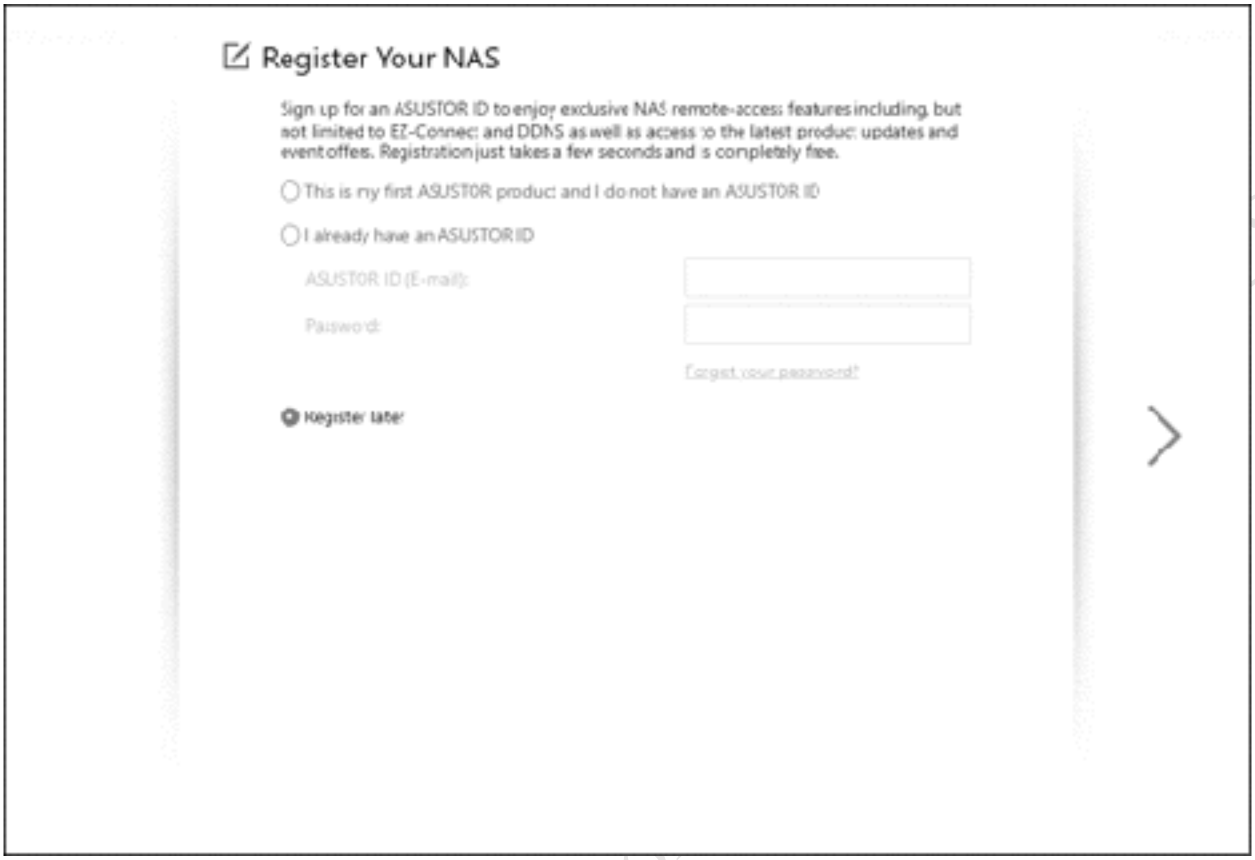


Initializing

The wizard will now begin initialization. This may take some time, please wait.

Figure 8: Initializing

You will then be invited to register your NAS and obtain an ASUSTOR ID or, if you already have one, you can enter its details. This is optional and is required for setting up remote access to the NAS, but for now we will skip it. Click **Register later** and click the large chevron on the right-hand side of the screen to continue.



Register Your NAS

Sign up for an ASUSTOR ID to enjoy exclusive NAS remote-access features including, but not limited to EZ-Connect and DDNS as well as access to the latest product updates and event offers. Registration just takes a few seconds and is completely free.

○ This is my first ASUSTOR product and I do not have an ASUSTOR ID

○ I already have an ASUSTOR ID

ASUSTOR ID (E-mail):

Password:

Forgot your password?

● Register later

Figure 9: Registration screen

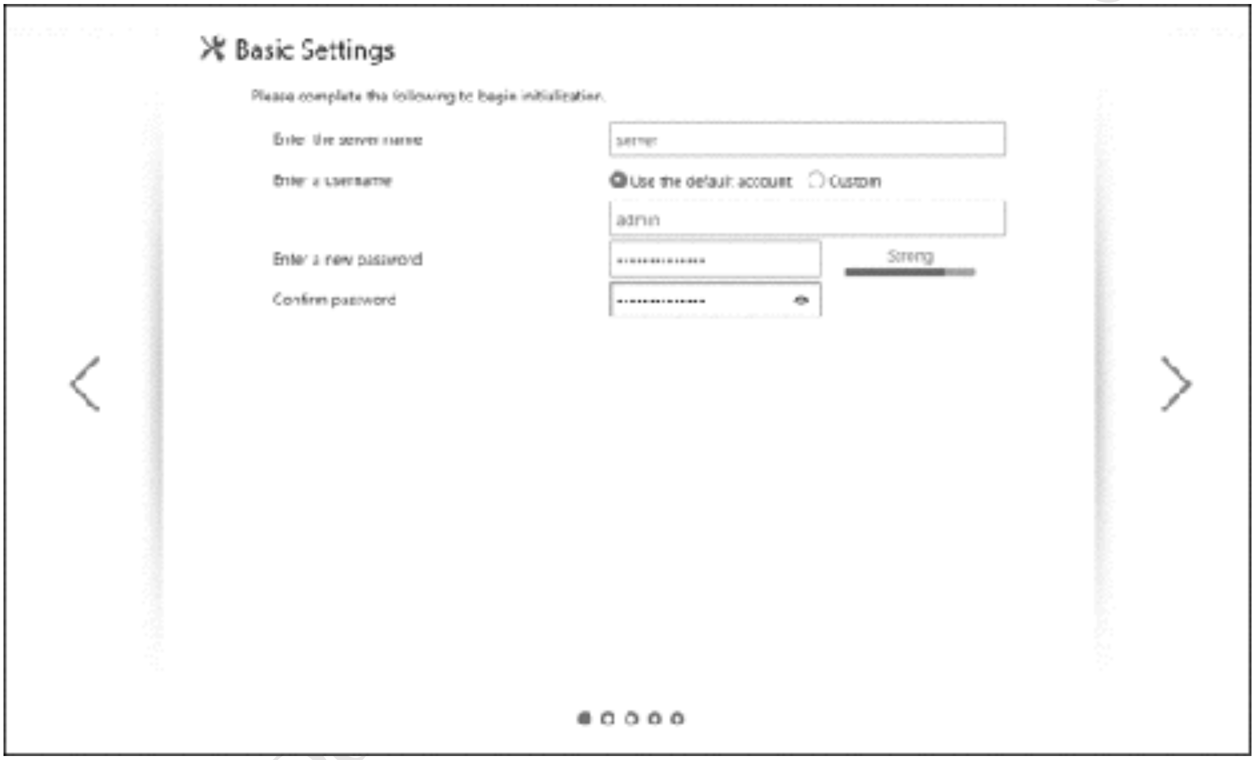
On the final screen, click the **Start** button and you will be connected to ADM. Please skip the following sections and continue with 2.8 Five Minute Tour of ADM.

2.4 ACC Custom Setup Option

For the *server name*, it is suggested that you simply call it '*server*', although if you have or envisage having further servers you may want to adopt a logical naming scheme e.g. *server1*, *server2,* or something meaningful to your organization such as location, business function, classroom etc.

The *username account* is the main account, used for administering and managing the server. The default is *admin* but can be changed to a customized name if you wish. Enter and confirm a password - use something non-obvious and preferably a mixture of upper- and lower-case letters, numbers and symbols and which does not include the username. ADM will provide feedback on the strength of the password and you want something that it considers to be 'Strong'.

Having entered the details, click the large chevron (arrow) on the right-hand side of the screen.



Basic Settings

Please complete the following to begin initialization.

Enter the server name: server

Enter a username: ● Use the default account ○ Custom

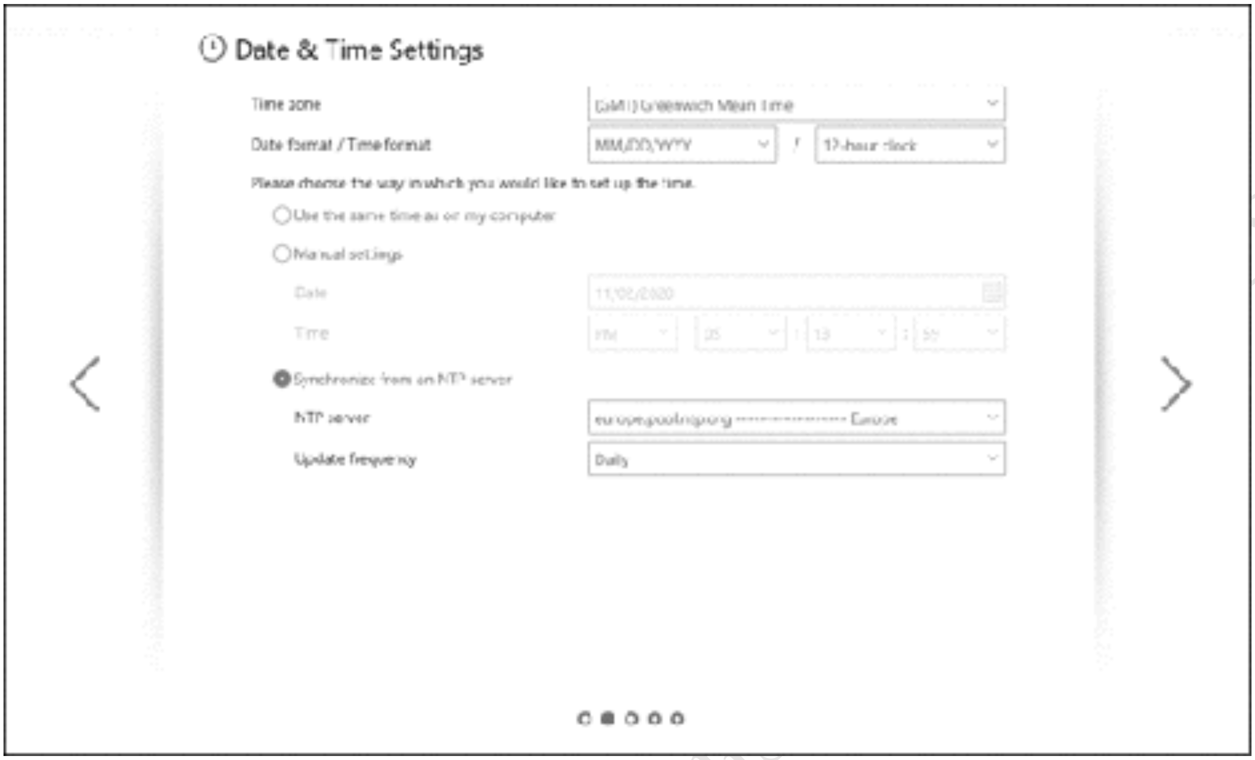
admin

Enter a new password: ••••••••••••• Strong

Confirm password: •••••••••••••

Figure 10: Server name and admin details

On the next screen, choose your *Time zone* from the dropdown box if it is incorrect. You are not happy with the *Date format* and *Time format*, these can be changed using the dropdowns. It is recommended to use an NTP (time) server, as accurate time keeping is required for cloud and synchronization services to work correctly, so select the **Synchronize from an NTP server** option. There a number of regional NTP servers to choose from and an *Update frequency* of *Daily* is suitable. Click the large chevron on the right-hand side of the screen to continue.



Date & Time Settings

Time zone: (GMT) Greenwich Mean Time

Date format / Time format: MM/DD/YYYY / 12-hour clock

Please choose the way in which you would like to set up the time.

○ Use the same time as on my computer

○ Manual settings

Date: 11/02/2020

Time: PM 05 : 13 : 55

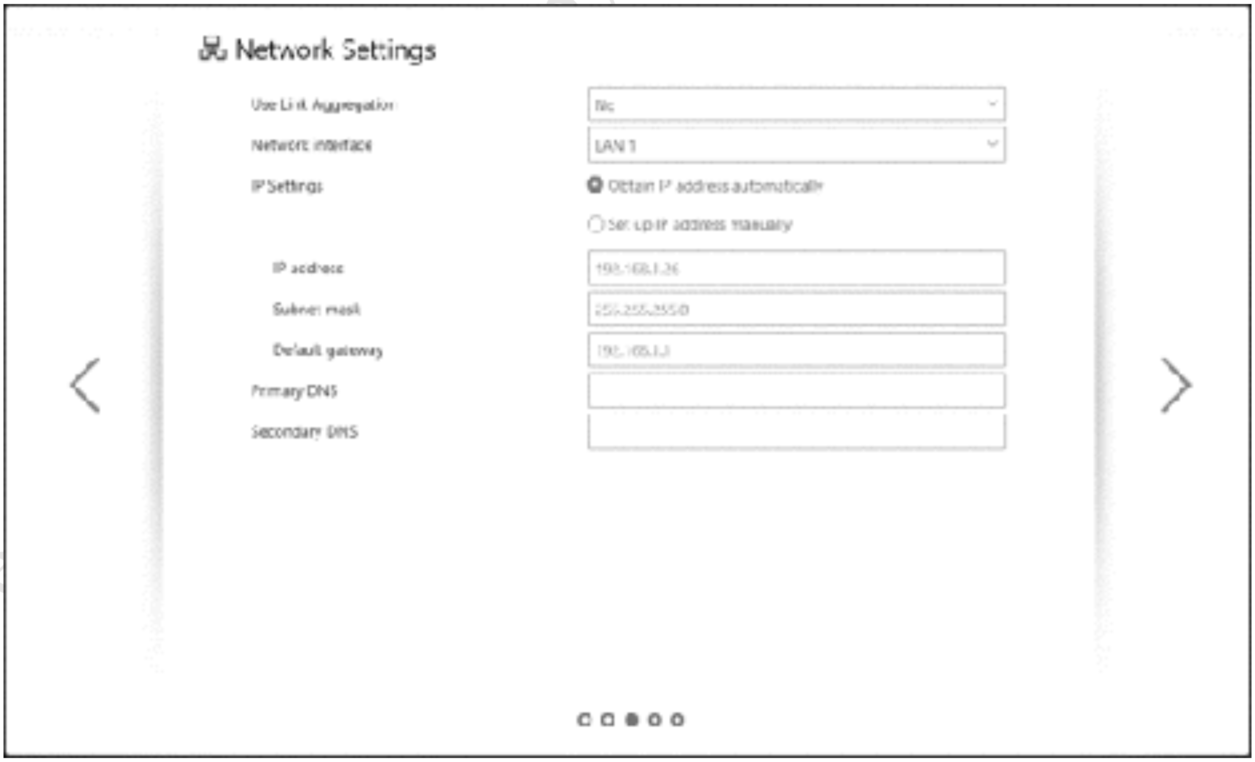
● Synchronize from an NTP server

NTP server: europe.pool.ntp.org ---------------- Europe

Update frequency: Daily

Figure 11: Date & Time Settings

The next screen defines the *Network Settings*. For now, accept the defaults i.e. obtain IP address automatically, do not use Link Aggregation, use LAN 1 as the Network interface. Click the large chevron on the right-hand side of the screen to continue.



Network Settings

Use Link Aggregation: No

Network interface: LAN 1

IP Settings: ● Obtain IP address automatically

○ Set up IP address manually

IP address: 192.168.1.26

Subnet mask: 255.255.255.0

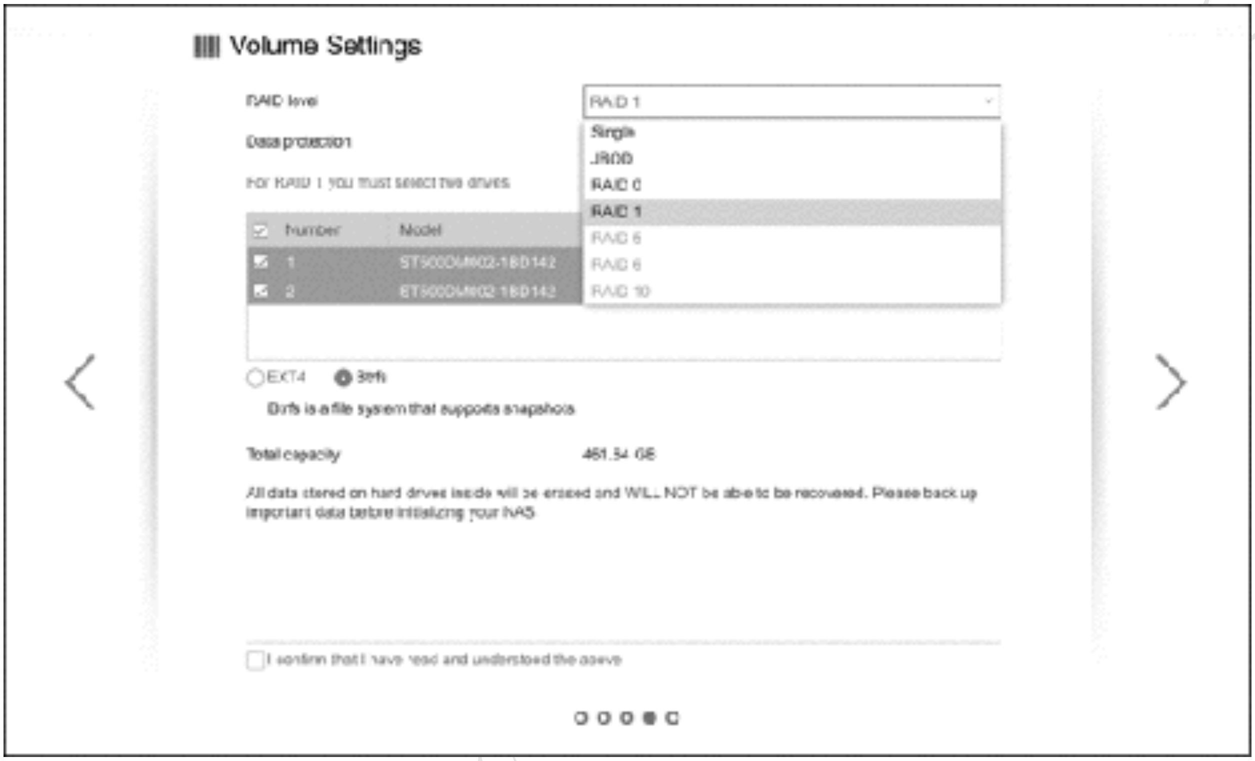
Default gateway: 192.168.1.1

Primary DNS:

Secondary DNS:

Figure 12: Network Settings

The subsequent screen is for specifying storage. Choose a RAID level; the options available depend upon what drives are installed in the NAS and what your requirements are. If the NAS has a single drive, then the only option is Single. If it has two drives, as in this example, then JBOD (maximum space), RAID 0 (maximum performance) and RAID 1 (data protection) are available. If three or more drives are installed, RAID 5 becomes available with four or more drives then RAID 6 is an option. Make sure the drives are selected by clicking on them and choose the RAID level using the dropdown (a more detailed description of RAID can be found in section 11.2 RAID).



Volume Settings

RAID level: RAID 1

Data protection

For RAID 1 you must select two drives

☑	Number	Model
☑	1	ST500DM002-1BD142
☑	2	ST500DM002-1BD142

○ EXT4 ● Btrfs

Btrfs is a file system that supports snapshots

Total capacity: 461.54 GB

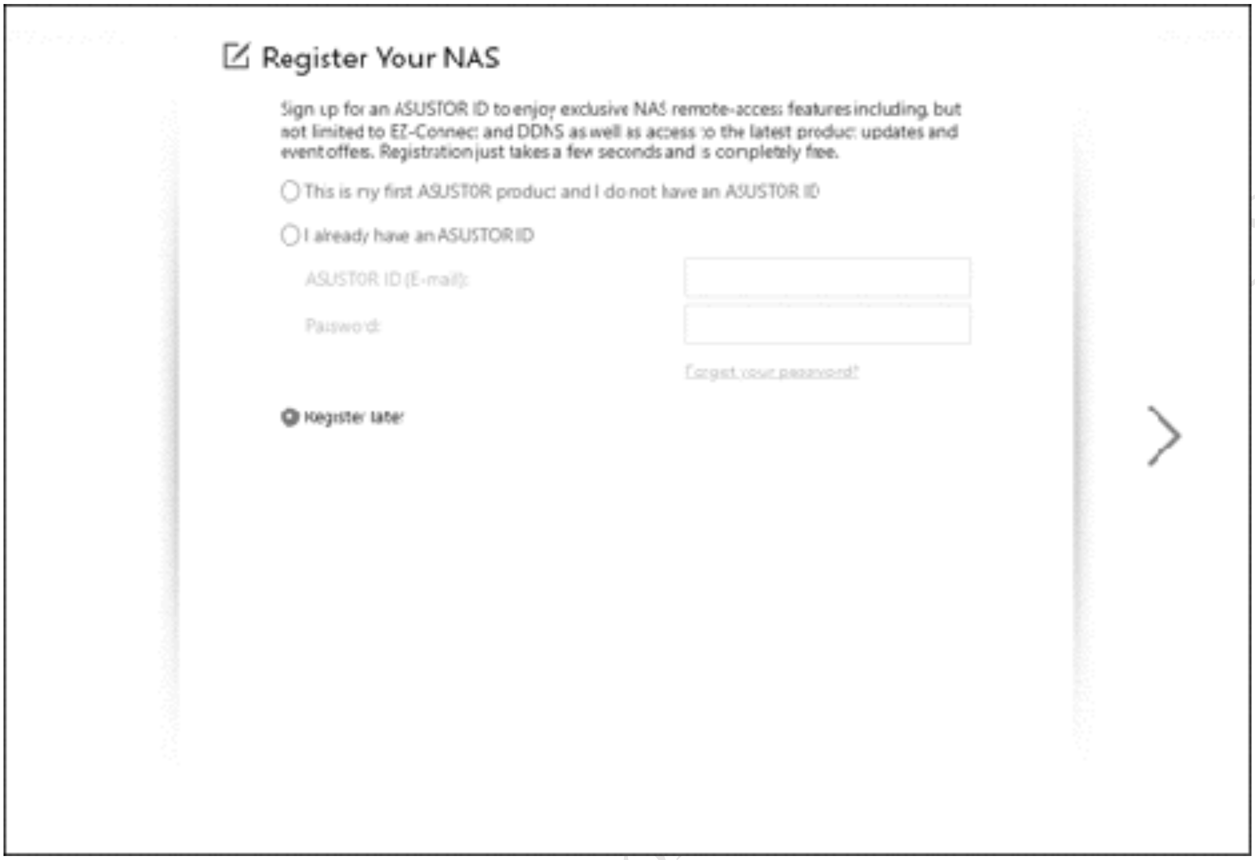
All data stored on hard drives inside will be erased and WILL NOT be able to be recovered. Please back up important data before initializing your NAS

□ I confirm that I have read and understood the above

Figure 13: Volume Settings

In the bottom half of the screen is a choice of file systems. *EXT4* is the default file system for Linux-based systems such as ADM and is available on all models. Many models, excluding some ARM-based and older units, support a more advanced system called *Btrfs* (sometimes pronounced ‘Butter-F-S’), which includes additional data protection and backup features. If Btrfs is available, you should choose it.

Having made your choices, tick the **I confirm that I have read and understood the above** box and click the large chevron (arrow) on the right-hand side of the screen. A status screen is shown whilst the NAS is initializing. When complete, you will be invited to register your NAS and obtain an ASUSTOR ID (or, if you already have one, you can enter the details). This is optional and is required for setting up remote access to the NAS, but for now we will skip it. Click **Register later** and click the large chevron on the right-hand side of the screen to continue.



Register Your NAS

Sign up for an ASUSTOR ID to enjoy exclusive NAS remote-access features including, but not limited to EZ-Connect and DDNS as well as access to the latest product updates and event offers. Registration just takes a few seconds and is completely free.

○ This is my first ASUSTOR product and I do not have an ASUSTOR ID

○ I already have an ASUSTOR ID

ASUSTOR ID (E-mail):

Password:

● Register later

Figure 14: Registration screen

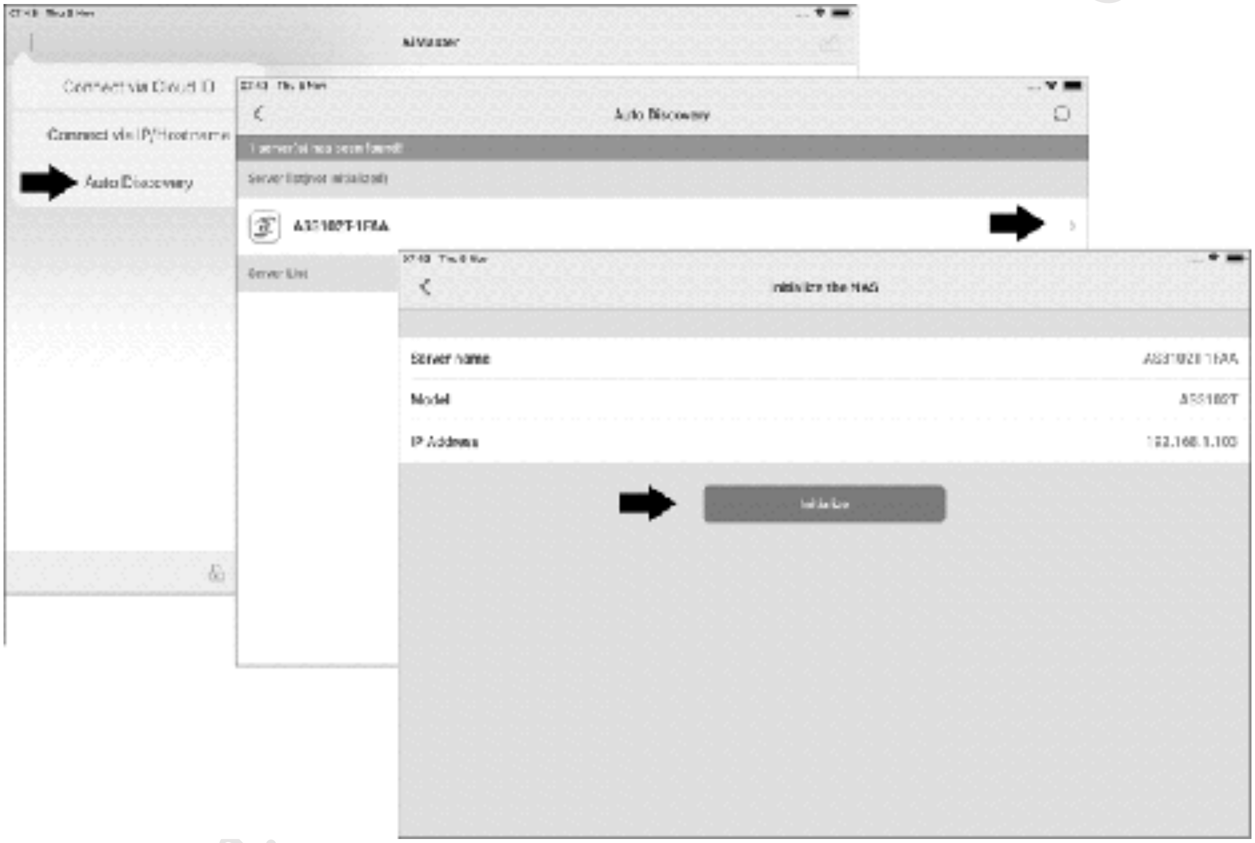
On the final screen, click the **Start** button and you will be connected to ADM. Please skip the following sections and continue with 2.8 Five Minute Tour of ADM.

2.5 Installation Using AiMaster

Having installed disk drives in the NAS and connected an Ethernet cable, power on the NAS. It will take a minute or two to start up, during which time is will beep a couple of times.

AiMaster is an app for smartphones and tablets that is used for installing ADM onto and subsequently managing a NAS. It is available for iOS (Apple) and Android (Google) from the appropriate app stores. Download and install it. In the following walkthrough we are using it on an iPad, but the overall experience is similar on other mobile devices.

Running it for the first time will display the following screen. Tap **Auto Discovery** and the NAS should be located. Tap it, make a note of the *IP Address* on the subsequent screen, tap the **Initialize** button and acknowledge the prompt:



Server name AS3102T-1FAA

Model AS3102T

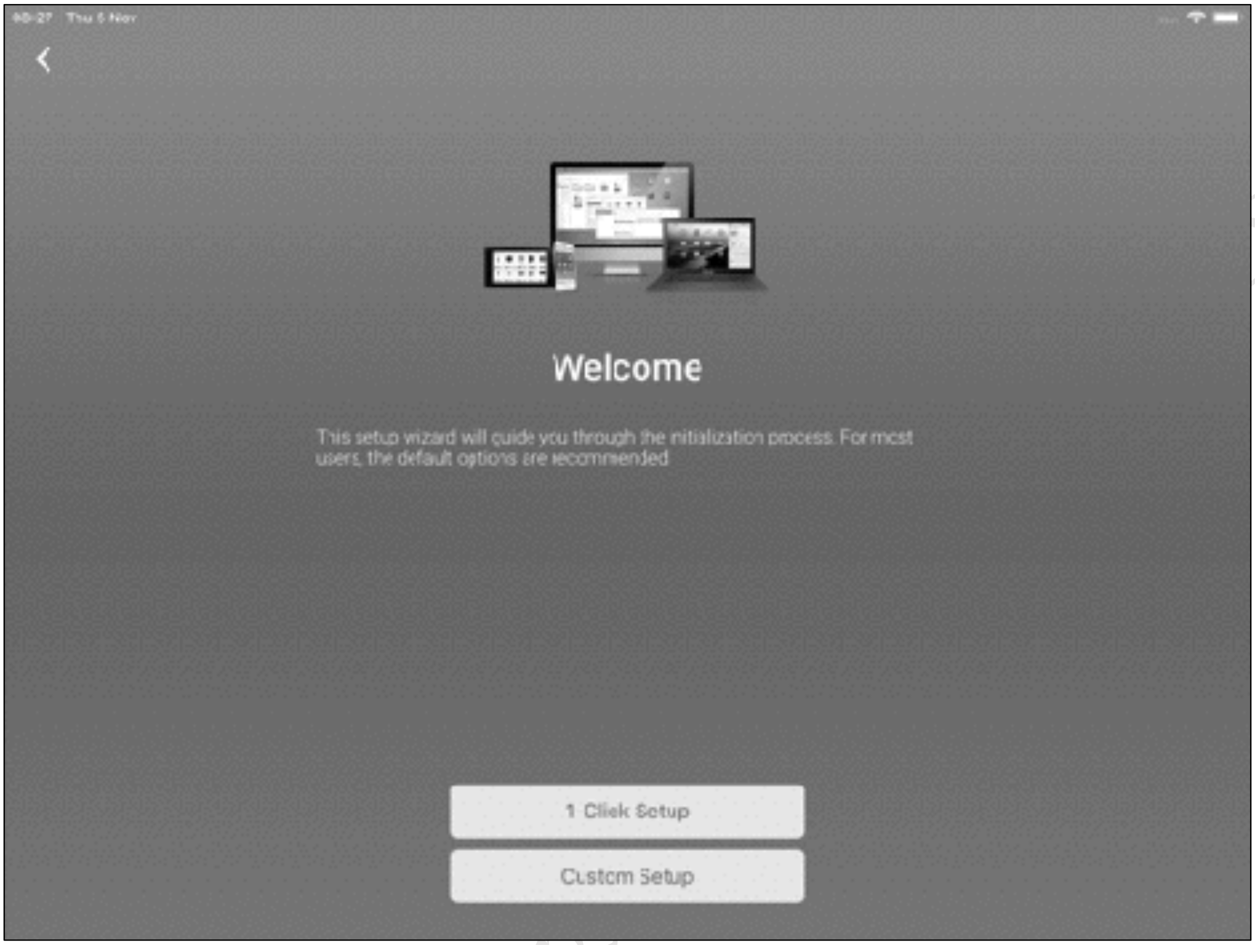
IP Address 192.168.1.103

Figure 15: Initial AiMaster screens

On the next screen, there are two choices:

1-Click Setup – this is the easiest option, where the setup process makes a number of assumptions in order to get you up and running as quickly as possible (although the description of '1-Click' is slightly misleading as it is more involved than that). Most people should choose this option.

Custom Setup – as the name suggests, this allows detailed control over the setup process. This is more suitable for experienced users or those with specific requirements.



Welcome

This setup wizard will guide you through the initialization process. For most users, the default options are recommended

Figure 16: Choose between 1-Click and Custom Setup

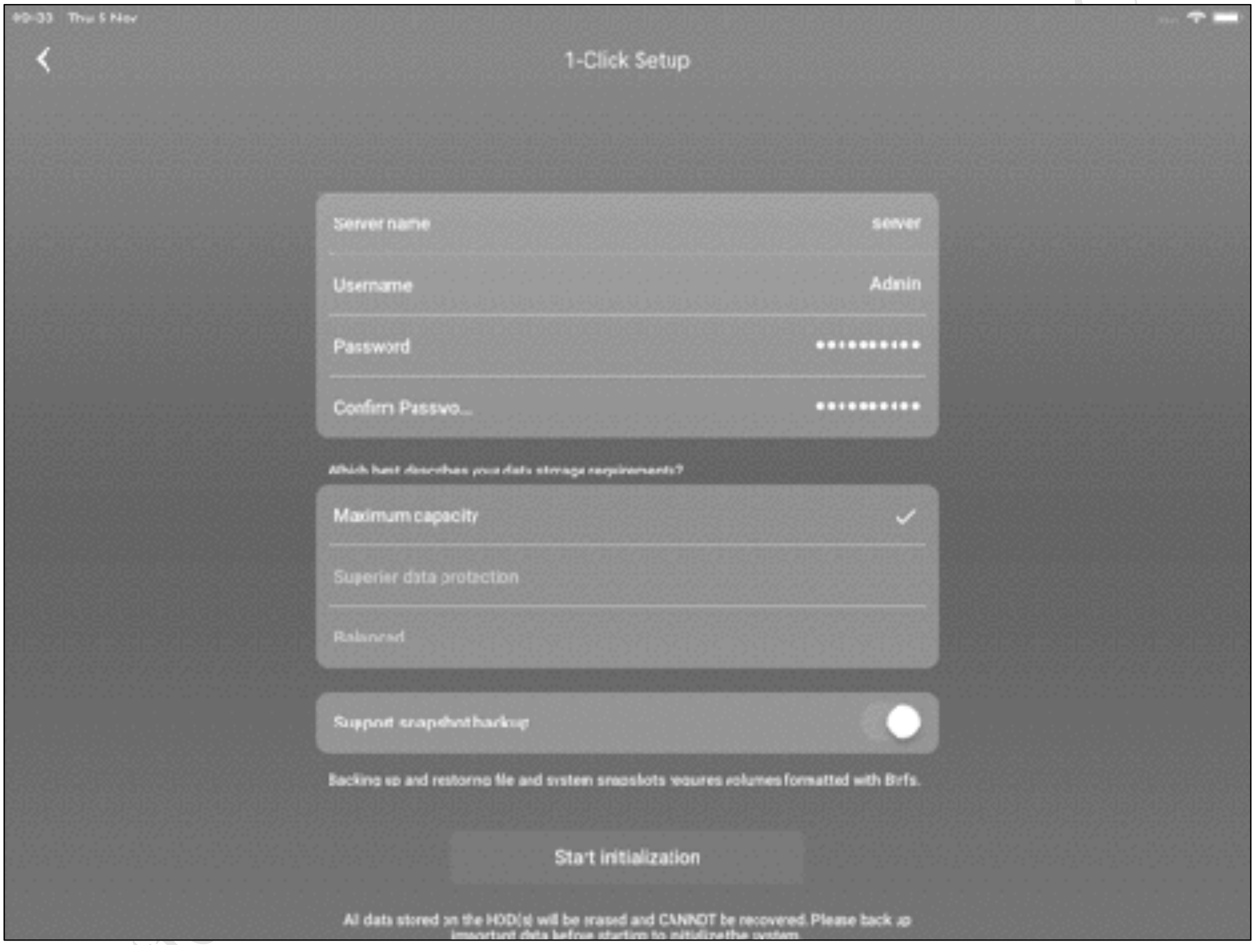
Make a choice and follow 2.6 AiMaster 1-Click Setup Option or 2.7 AiMaster Custom Setup Option as appropriate.

2.6 AiMaster 1-Click Setup Option

This first screen is for defining the essential characteristics of the NAS.

For the *server name*, it is suggested that you simply call it '*server'*, although if you have or envisage having further servers you may want to adopt a logical naming scheme e.g. *server1*, *server2,* or something meaningful to your organization such as location, business function, classroom etc.

The *username account* is the main account, used for administering and managing the server. The default is *admin* but can be changed to a customized name if you wish. Enter and confirm a password: use something non-obvious and preferably a mixture of upper- and lower-case letters, numbers and symbols and which does not include the username.



Server name server

Username Admin

Password ••••••••••

Confirm Passwo... ••••••••••

Which best describes your data storage requirements?

Maximum capacity ✓

Superior data protection

Balanced

Support snapshot backup

Backing up and restoring file and system snapshots requires volumes formatted with Btrfs.

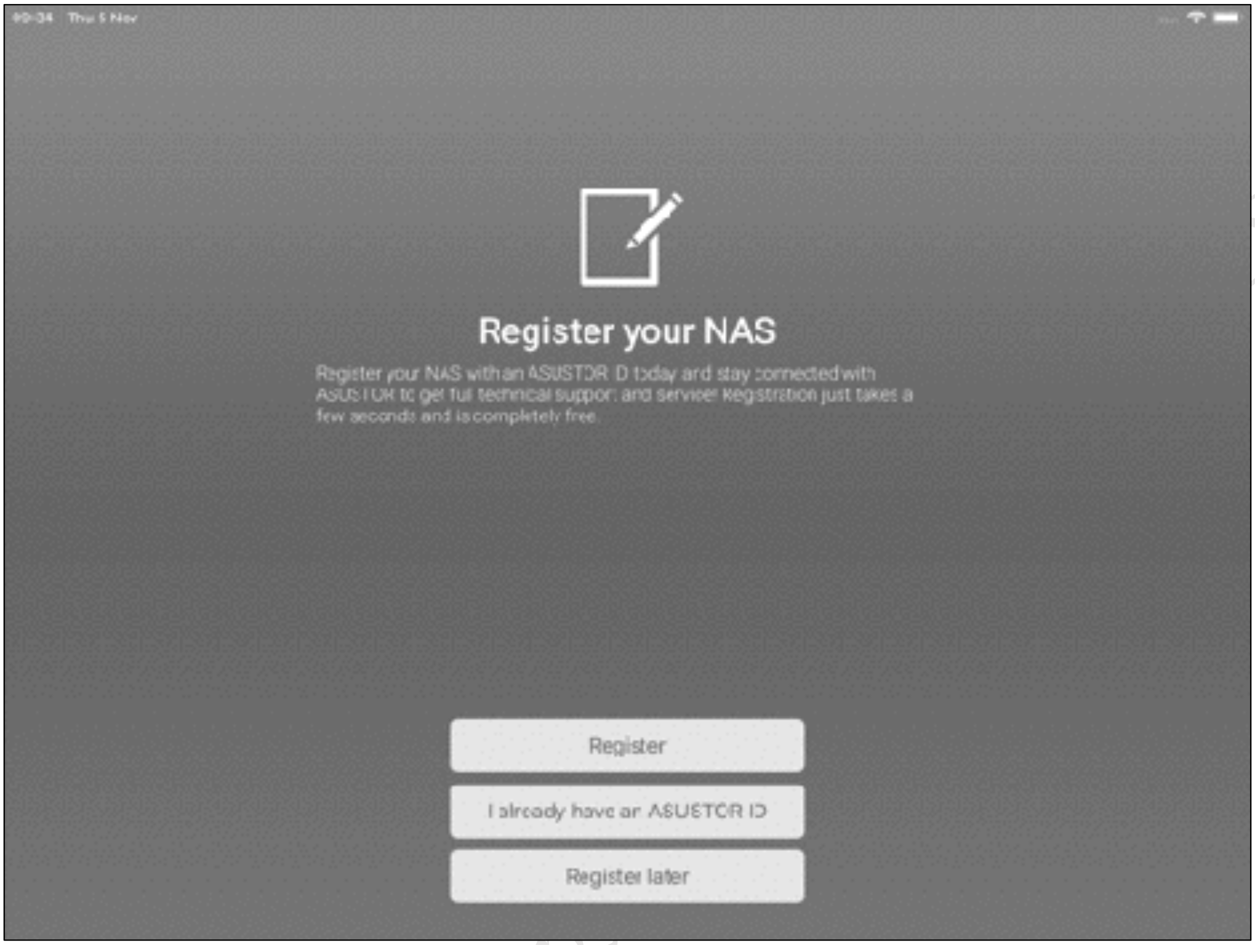
Start initialization

All data stored on the HDD(s) will be erased and CANNOT be recovered. Please back up important data before starting to initialize the system.

Figure 17: Specify the key information for the server

Underneath the password section is a question about your data storage requirements and the options available depend on what drives are installed in the NAS. Make a choice between *Maximum capacity*, *Superior data protection* or *Balanced*. You also need to decide if you want to use *Snapshots*, a backup feature whereby data is effectively 'photographed' at regular moments in time (if this option is available you should take it). Having made your choices, tap the **Start initialization** button.

Eventually there will be a screen inviting you to register your NAS and obtain an ASUSTOR ID or, if you already have one, you can enter the details. This is optional although is required for setting up remote access to the NAS, but for now we will skip it. Tap the **Register later** button.



09:34 Thu 5 Nov

Register your NAS

Register your NAS with an ASUSTOR ID today and stay connected with ASUSTOR to get full technical support and services! Registration just takes a few seconds and is completely free.

Figure 18: Registration screen

After installation is complete, you will be presented with the ADM Desktop screen. This provides a subset of the management features available in ADM and will be referenced where applicable throughout this guide for those who wish to use a mobile device. However, to complete the installation it is necessary to switch to a regular internet browser. Accordingly, please skip the following section and continue with 2.8 Five Minute Tour of ADM.

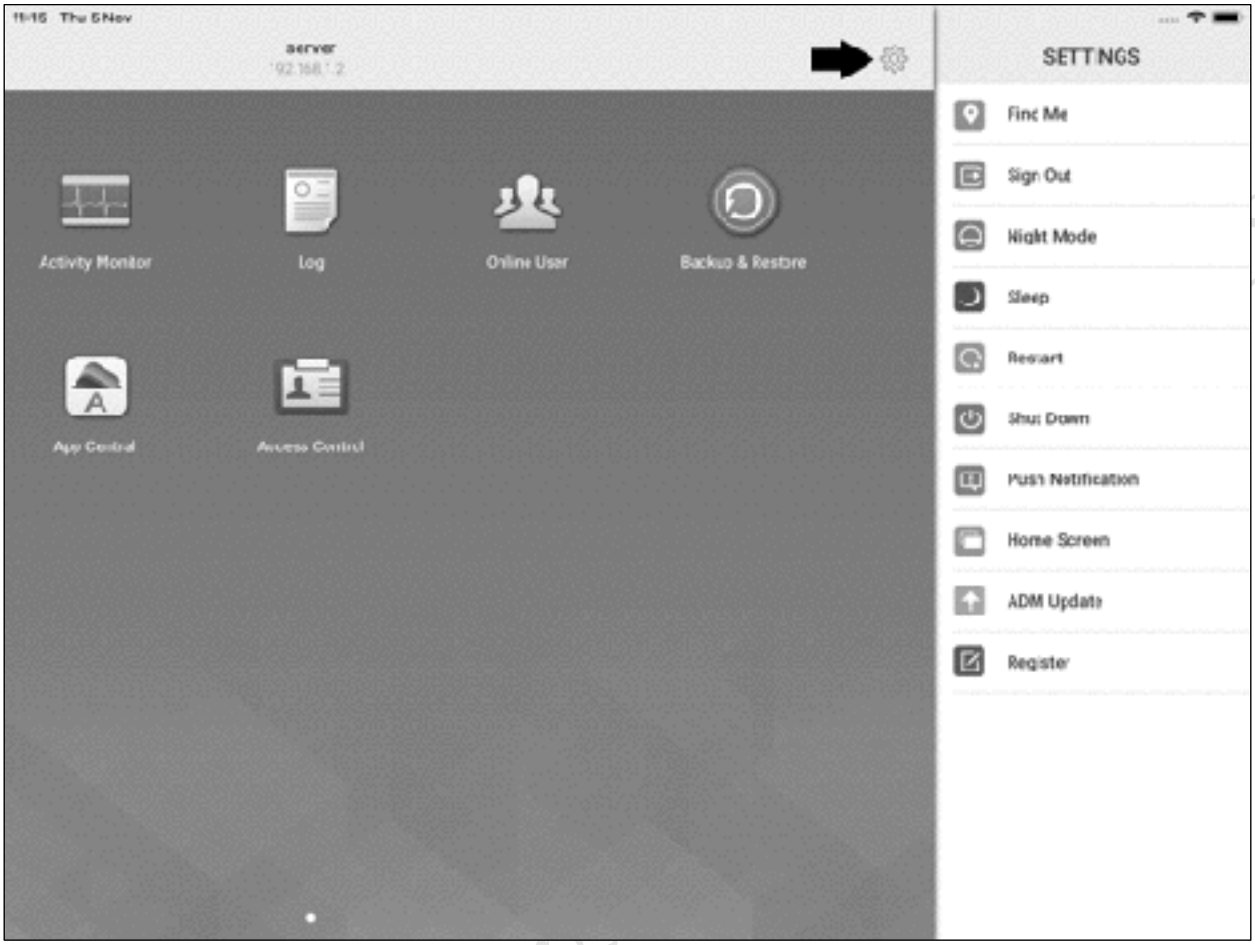
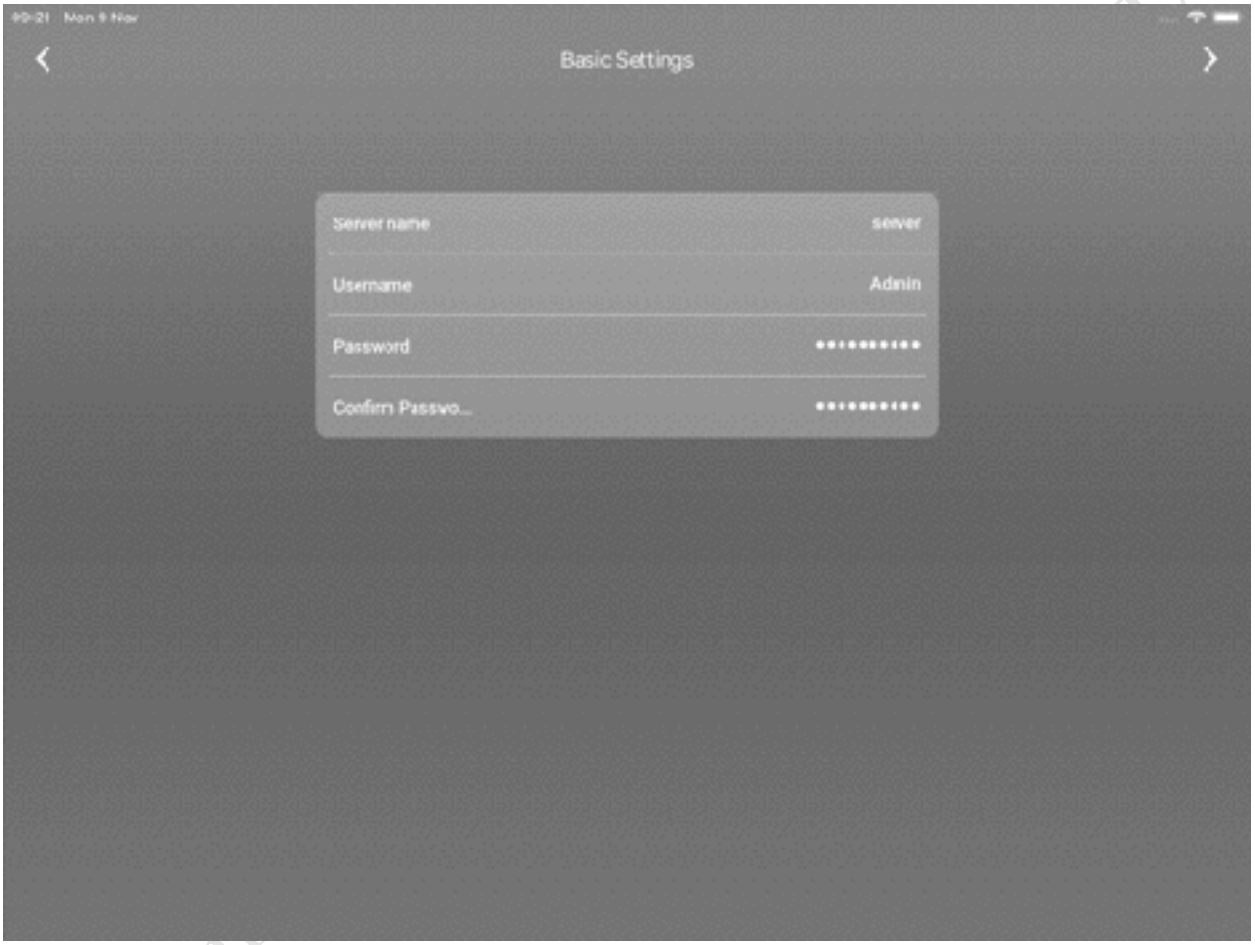


Figure 19: ADM Desktop, as viewed in AiMaster on iPad

2.7 AiMaster Custom Setup Option

For the *server name*, it is suggested that you simply call it '*server'*, although if you have or envisage having further servers you may want to adopt a logical naming scheme e.g. *server1*, *server2,* or something meaningful to your organization such as location, business function, classroom etc.

The *usernamer account* is the main account, used for administering and managing the server. The default is *admin* but can be changed if you wish. Enter and confirm a password: use something non-obvious and preferably a mixture of upper- and lower-case letters, numbers and symbols and which does not include the username. Tap the chevron (arrow) in the top right-hand corner of the screen:



Server name server

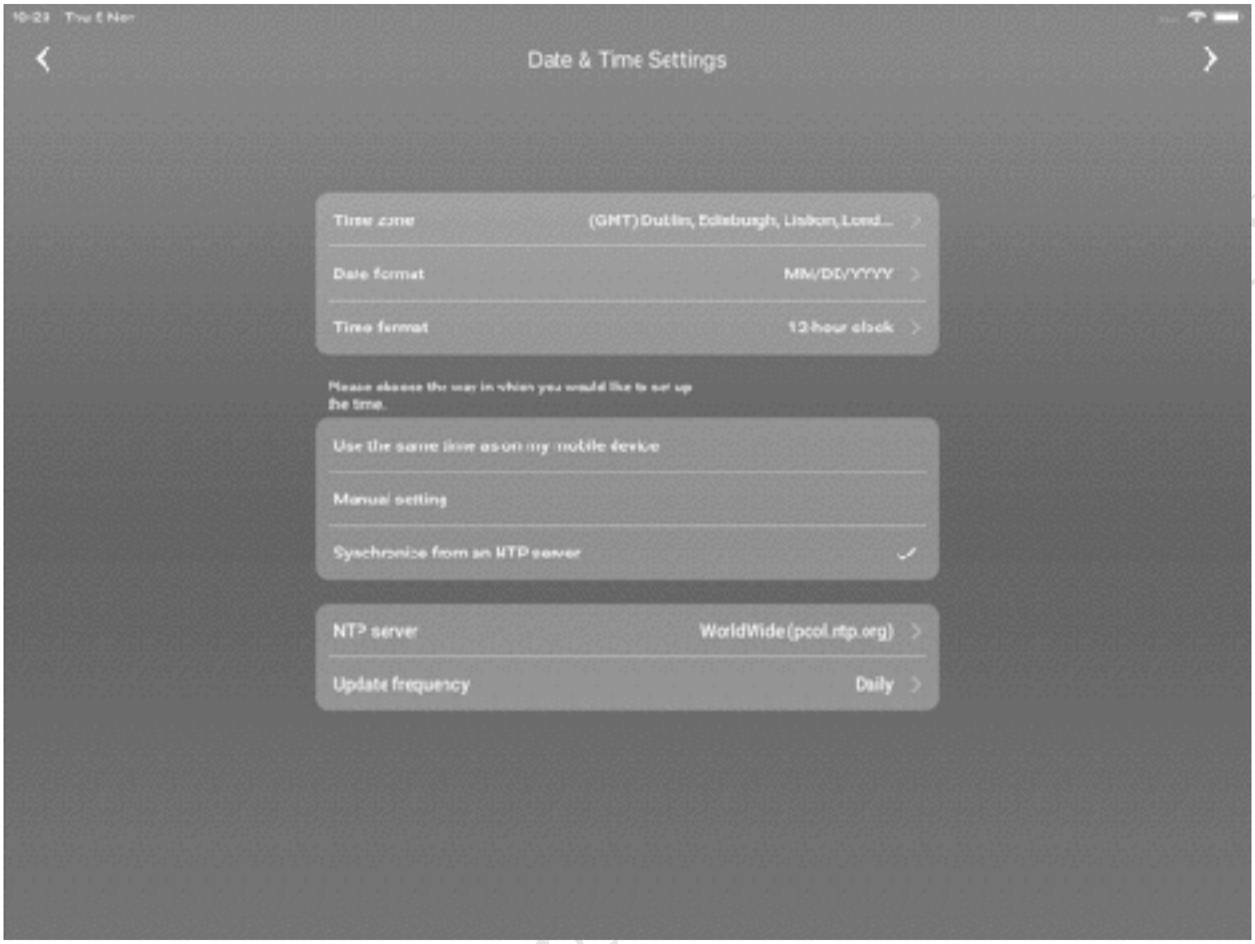
Username Admin

Password ●●●●●●●●●●

Confirm Passwo... ●●●●●●●●●●

Figure 20: Basic Settings

On the next screen, choose your *Time zone* from the dropdown box if it is incorrect. You are not happy with the *Date format* and *Time format*, these can be changed using the dropdowns. It is recommended to use an NTP (time) server, as accurate time keeping is required for cloud and synchronization services to work correctly, so select the **Synchronize from an NTP server** option. There a number of regional NTP servers to choose from and an *Update frequency* of *Daily* is suitable. Click the large chevron on the right-hand side of the screen to continue.



Date & Time Settings

Time zone	(GMT) Dublin, Edinburgh, Lisbon, Lond...
Date format	MM/DD/YYYY
Time format	12-hour clock

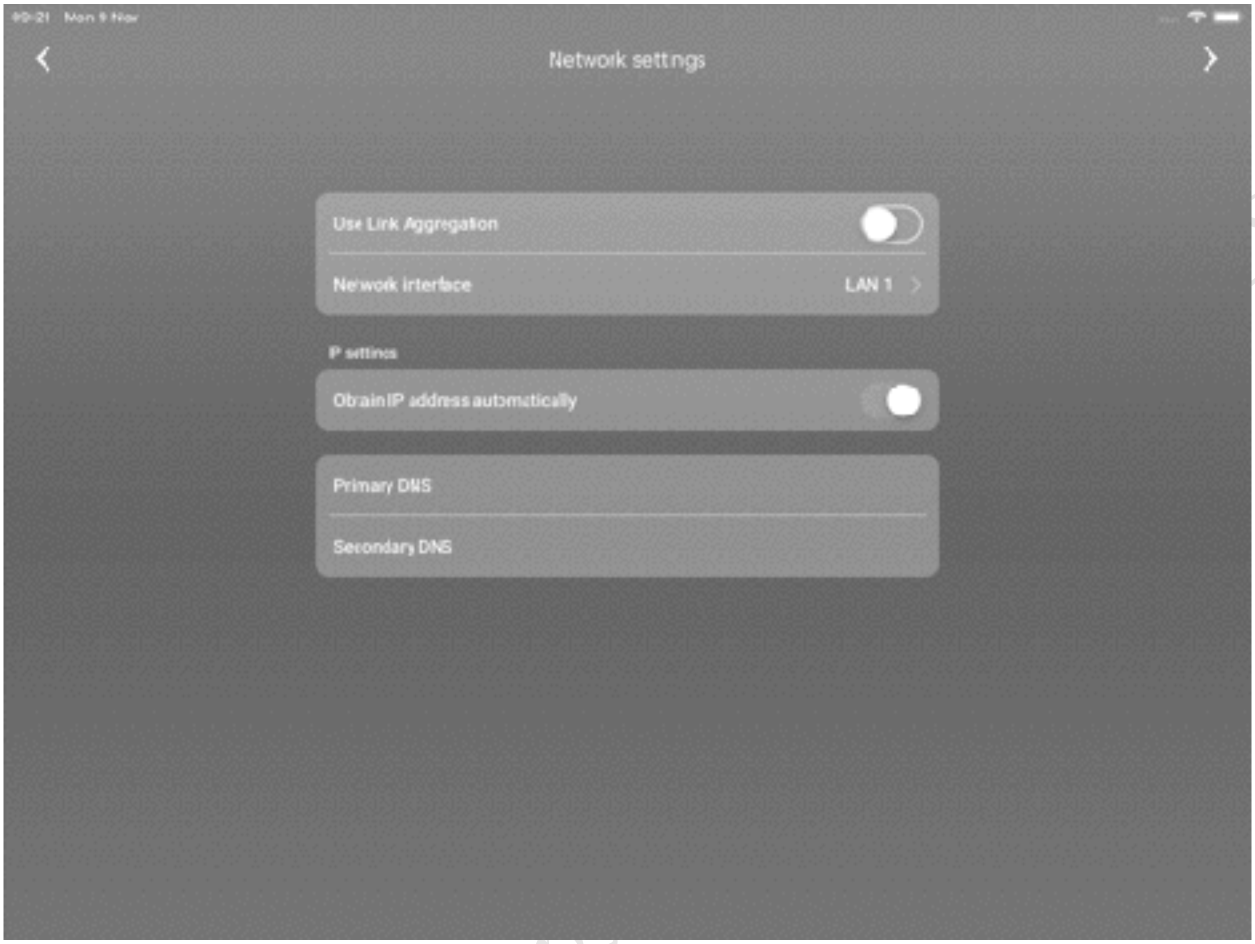
Please choose the way in which you would like to set up the time.

- Use the same time as on my mobile device
- Manual setting
- Synchronize from an NTP server ✓

NTP server	WorldWide (pool.ntp.org)
Update frequency	Daily

Figure 21: Date & Time Settings

The next screen defines the *Network Settings*. For now, accept the defaults i.e. obtain IP address automatically, do not use Link Aggregation, use LAN 1 as the Network interface. Click the large chevron on the right-hand side of the screen to continue.



Network settings

Use Link Aggregation ○

Network interface LAN 1 >

IP settings

Obtain IP address automatically ●

Primary DNS

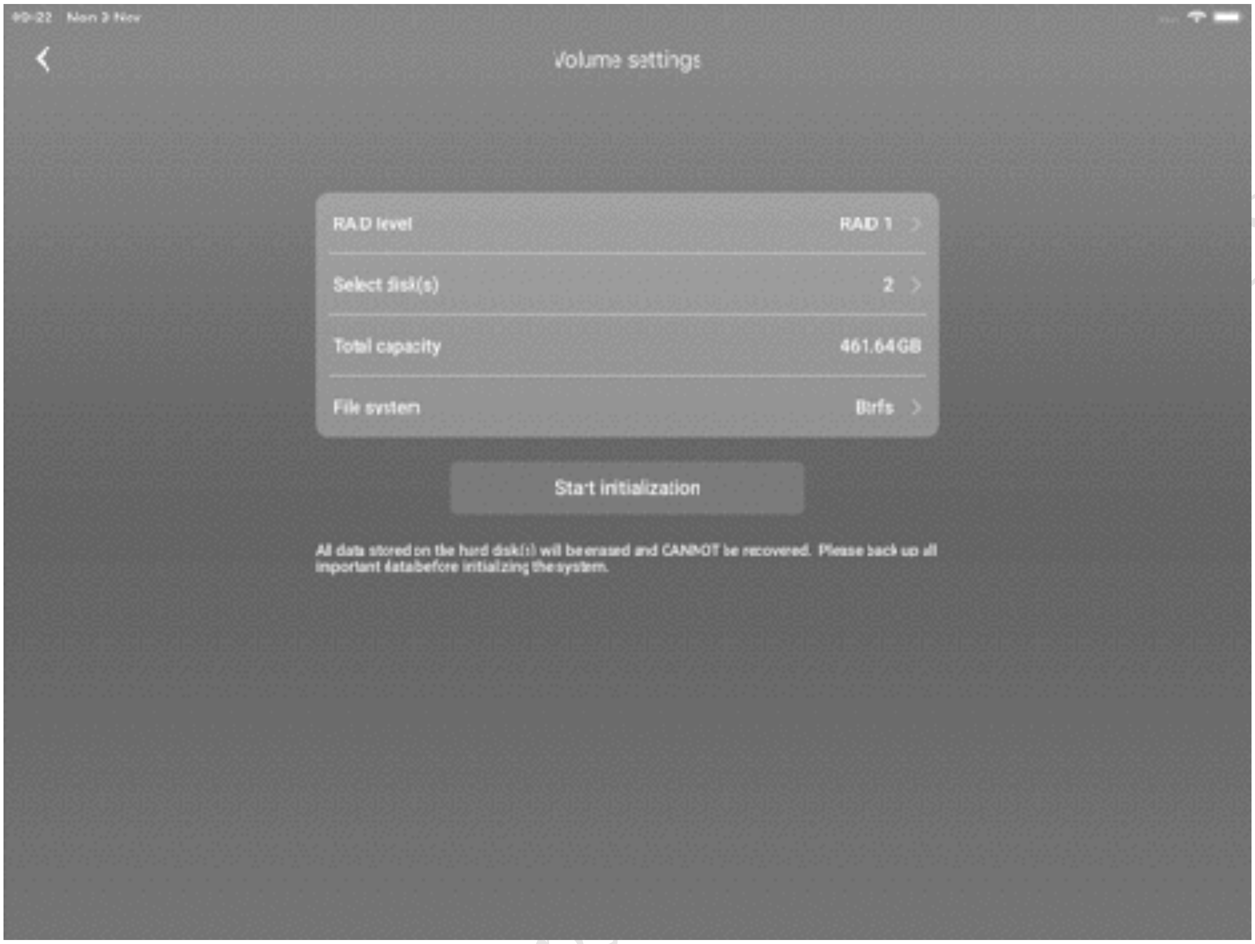
Secondary DNS

Figure 22: Network Settings

The subsequent screen is for specifying storage. Choose a RAID level; the options available depend upon what drives are installed in the NAS and what your requirements are. If the NAS has a single drive, then the only option is Single. If it has two drives, as in this example, then JBOD (maximum space), RAID 0 (maximum performance) and RAID 1 (data protection) are available. If three or more drives are installed, RAID 5 becomes available with four or more drives then RAID 6 is an option. Make sure the drives are selected by tapping on them and choose the RAID level using the dropdown (a more detailed description of RAID can be found in section 11.2 RAID).

There is a choice of file systems. *EXT4* is the default file system for Linux-based systems such as ADM and is available on all models. Many models, excluding some ARM-based and older units, support a more advanced system called *Btrfs* (sometimes pronounced ‘Butter-F-S’), which includes additional data protection and backup features. If Btrfs is available, you should choose it.

The tap the **Start initialization** button to proceed.



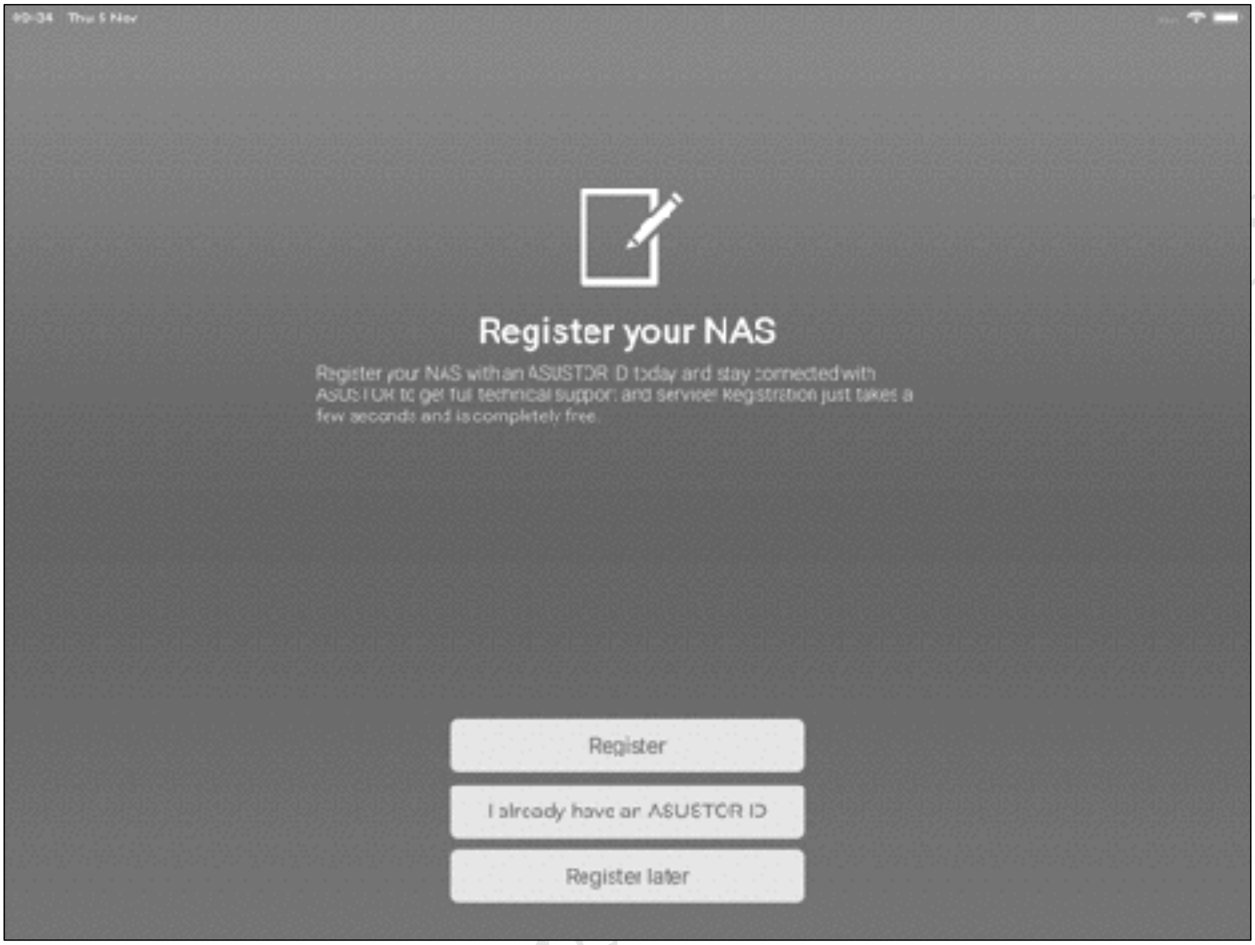
Volume settings

RAID level: RAID 1
Select disk(s): 2
Total capacity: 461.64GB
File system: Btrfs

All data stored on the hard disk(s) will be erased and CANNOT be recovered. Please back up all important databefore initializing the system.

Figure 23: Volume Settings

Eventually there will be a screen inviting you to register your NAS and obtain an ASUSTOR ID or, if you already have one, you can enter the details. This is optional although is required for setting up remote access to the NAS, but for now we will skip it. Tap the **Register later** button.



Register your NAS

Register your NAS with an ASUSTOR ID today and stay connected with ASUSTOR to get full technical support and services. Registration just takes a few seconds and is completely free.

Figure 24: Registration screen

After installation is complete, you will be presented with the ADM Desktop screen. This provides a subset of the management features available in ADM and will be referenced where applicable throughout this guide for those who wish to use a mobile device. However, to complete the installation it is necessary to switch to a regular internet browser. Accordingly, please skip the following section and continue with 2.8 Five Minute Tour of ADM.

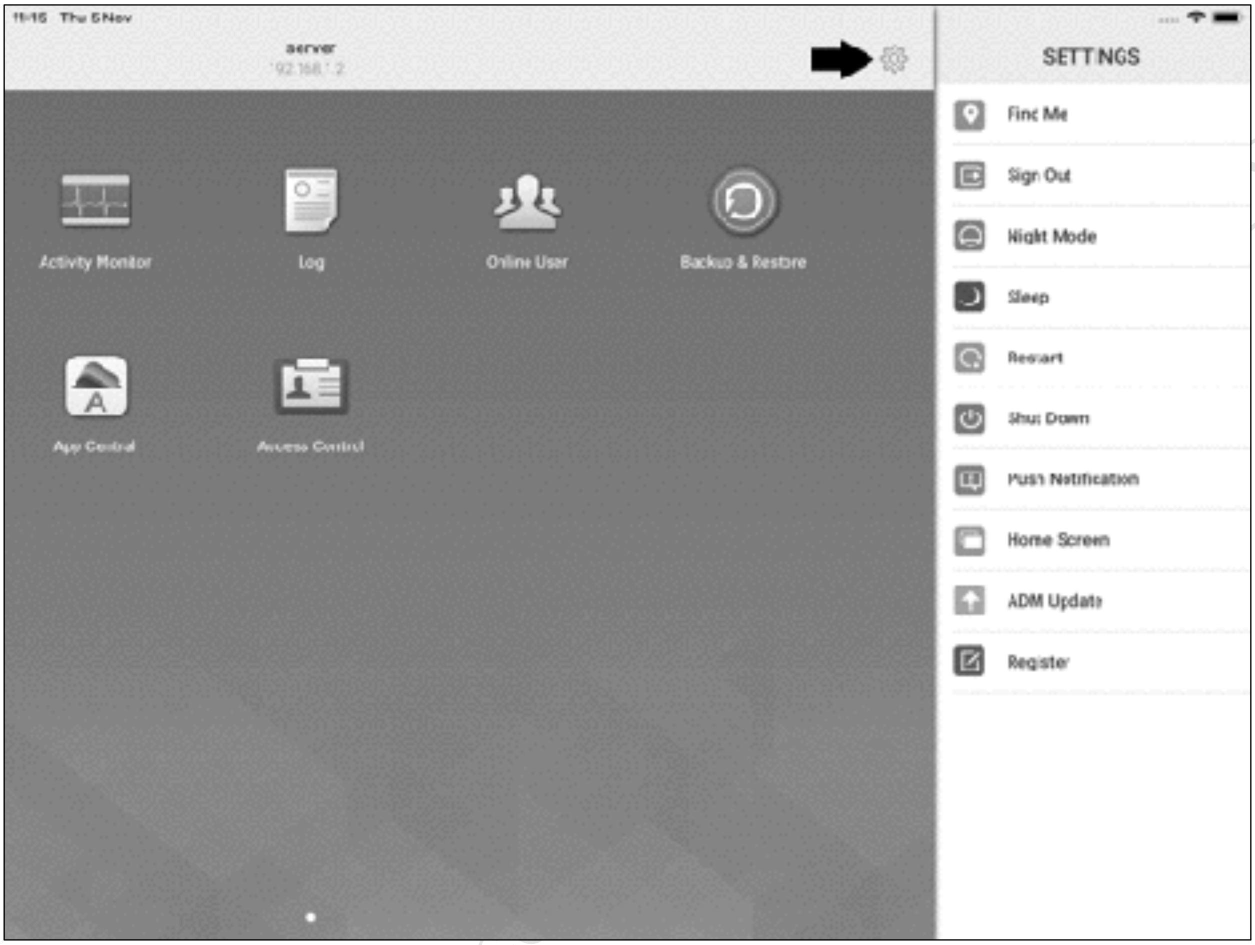


Figure 25: ADM Desktop, as viewed in AiMaster on iPad

2.8 Five Minute Tour of ADM

If the login screen is not being displayed, enter *http://server* in the address bar of the browser (assuming you called your NAS *'server',* otherwise enter the name you specified). If it cannot be found, try entering the IP address of the server instead e.g. *http://192.168.1.2*. If you did not make a note of the IP address during installation, you can use the ASUSTOR Control Center to discover it.

Enter the user name of *admin* along with the password you defined earlier. Upon first login, ASUSTOR's statement about privacy is shown – click **Continue**. You will then be offered a short 'Welcome to ASUSTOR Data Master' tour – click **Start** if you wish to work through it. You may not want to see it on subsequent logins, in which case tick the **Do not show this again** box. To close the tour, click the small red circle in the top right-hand corner.

The main ADM screen is easy to use and somewhat reminiscent of an iPad or other tablet. There is the *Desktop*, which can be customized. There are a number of icons on the Desktop, the selection of which can vary slightly depending upon the model. Some of these are for running system functions and others are for running applications. The icons will be distributed over multiple screens if there are too many to fit on a single screen.

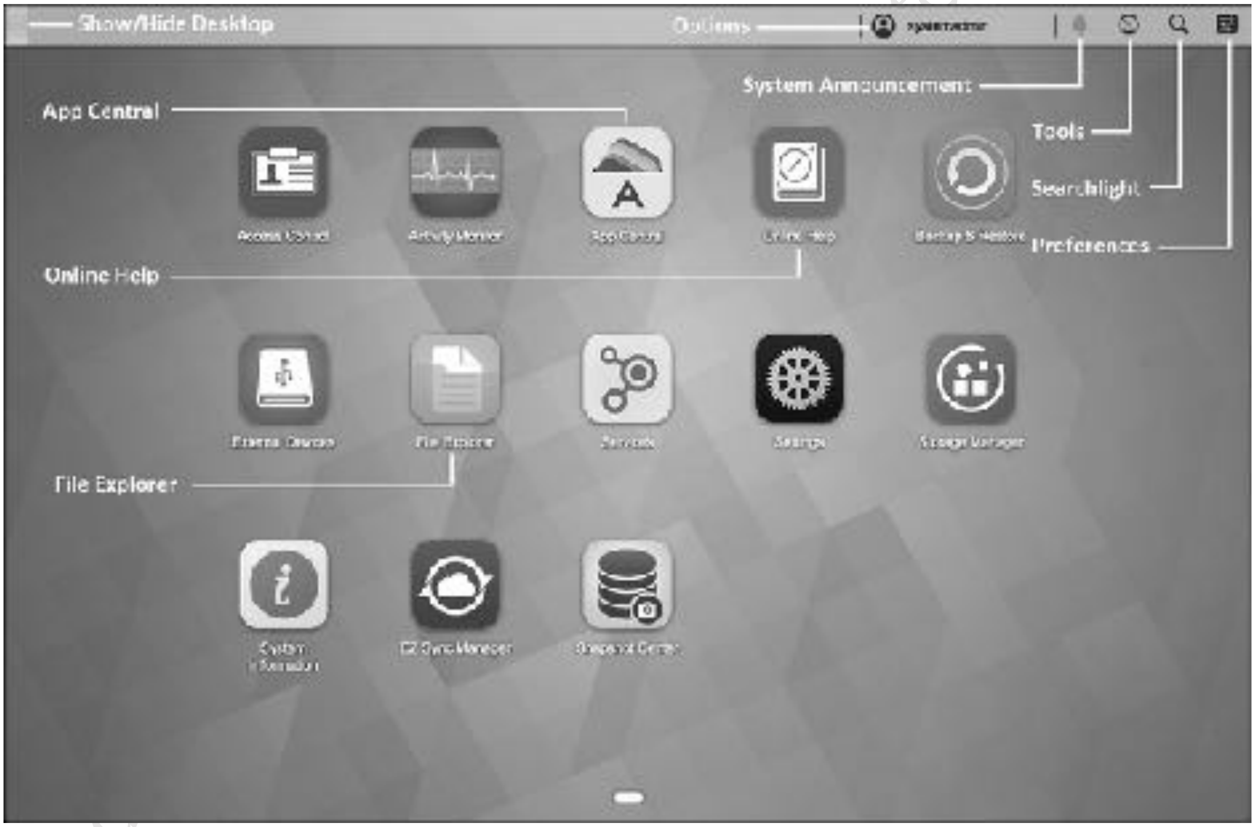


Figure 26: Overview of the ADM Desktop

Most apps and features run in resizable windows on the Desktop, although some open in a new browser tab. In the top right-hand corner of the window are four small controls: context-sensitive help; minimize the window; maximize the window; close the window. A very small number of apps have a fifth control, which displays data privacy or licensing information:

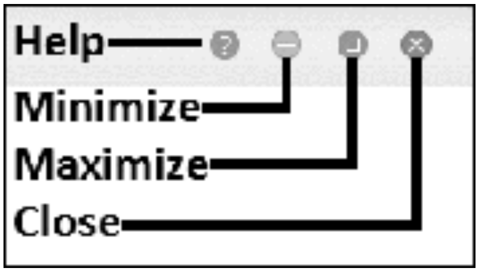


Figure 27: Controls for windows

Some important Desktop icons include:

App Central - access to a portal from where applications can be downloaded to provide additional functionality. This is described in detail in section 12.2 App Central.

Online Help - links to the online help portal at ASUSTOR. This is used by the window control just described.

File Explorer - displays the contents of the disk volumes and folders and is used for manipulating files, similar in principle to Windows Explorer/File Explorer on a PC or Finder on a Mac. Further information can be found in 5.2 Using a Browser and File Explorer.

At the top of the screen is a task bar that show running apps and also provides the following functions:

Show/Hide Desktop - clicking the top left-hand corner of the screen will temporarily hide any items on the desktop.

Options – used for personalizing the desktop and logging out. The administrator can also shut the system down from here.

System Announcement – view messages from the administrator. This is a useful mechanism for providing short messages to all users.

Tools – described shortly.

Searchlight – comprehensive search facility for locating files, folders and ADM features.

Preferences - provides options to setup and customize the server, organized into three categories of *Settings*, *Access Control* and *Services*, all of which also have their own icons on the Desktop. The great benefit of Preferences is that everything is in one place and it can be invoked at any time, regardless of what else you might be doing:

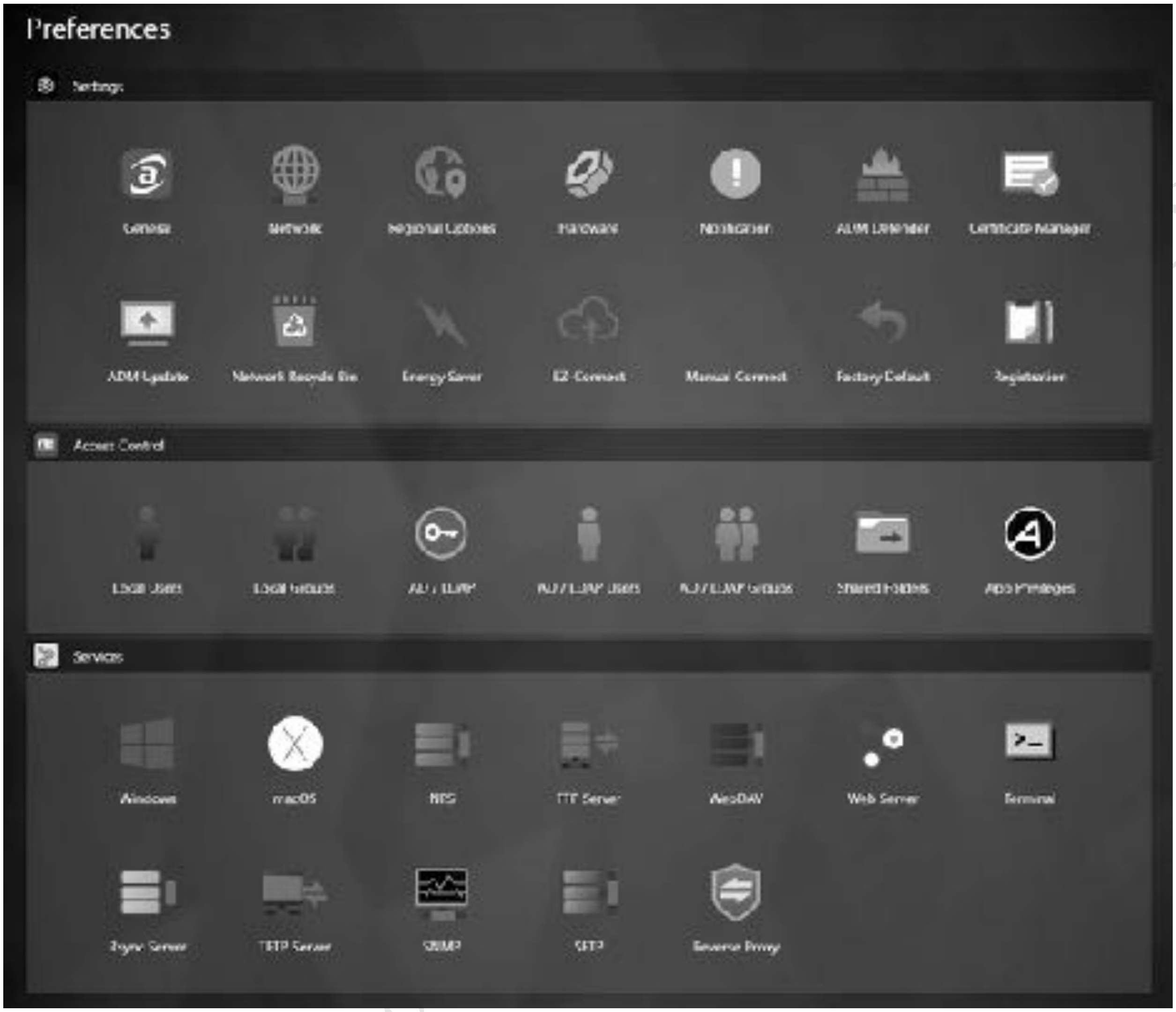
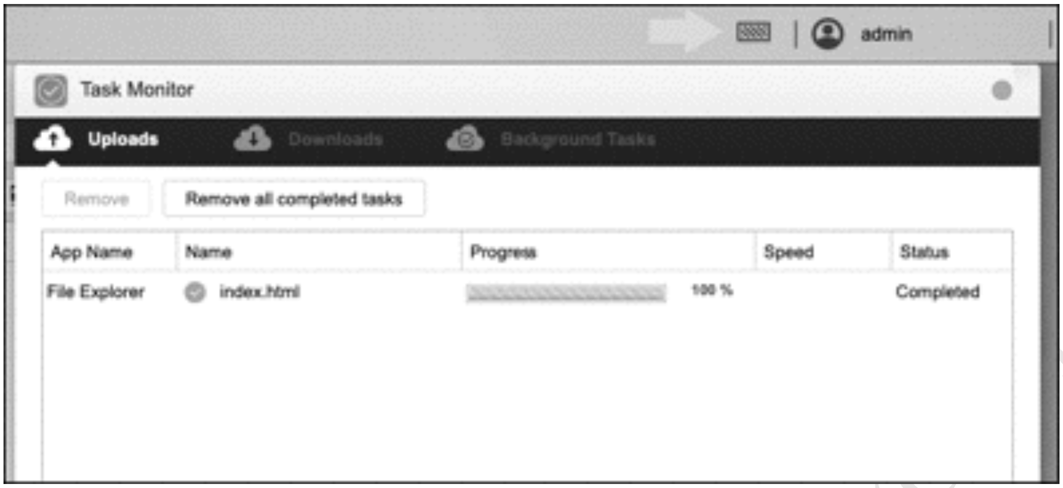


Figure 28: Preferences

When certain tasks are running e.g. copying or uploading files, the *Task Monitor* might be displayed. This can be cleared down by clicking it and choosing **Remove** or **Remove all completed tasks**:



App Name	Name	Progress	Speed	Status
File Explorer	index.html	100 %		Completed

Figure 29: Task Monitor

In the top right-hand corner of the screen is an icon that looks like a small dial or speedometer and which, when clicked, shows the *Tools*. These are widgets which provide an ‘at a glance’ overview of the health and status of the server. Initially the Tools panel is empty – click on the plus (+) sign to populate it using the available selection. If the cursor is hovered over a tool, two mini icons appear in its top right-hand corner, one to close it and the other to open the underlying app or utility that generates the information.

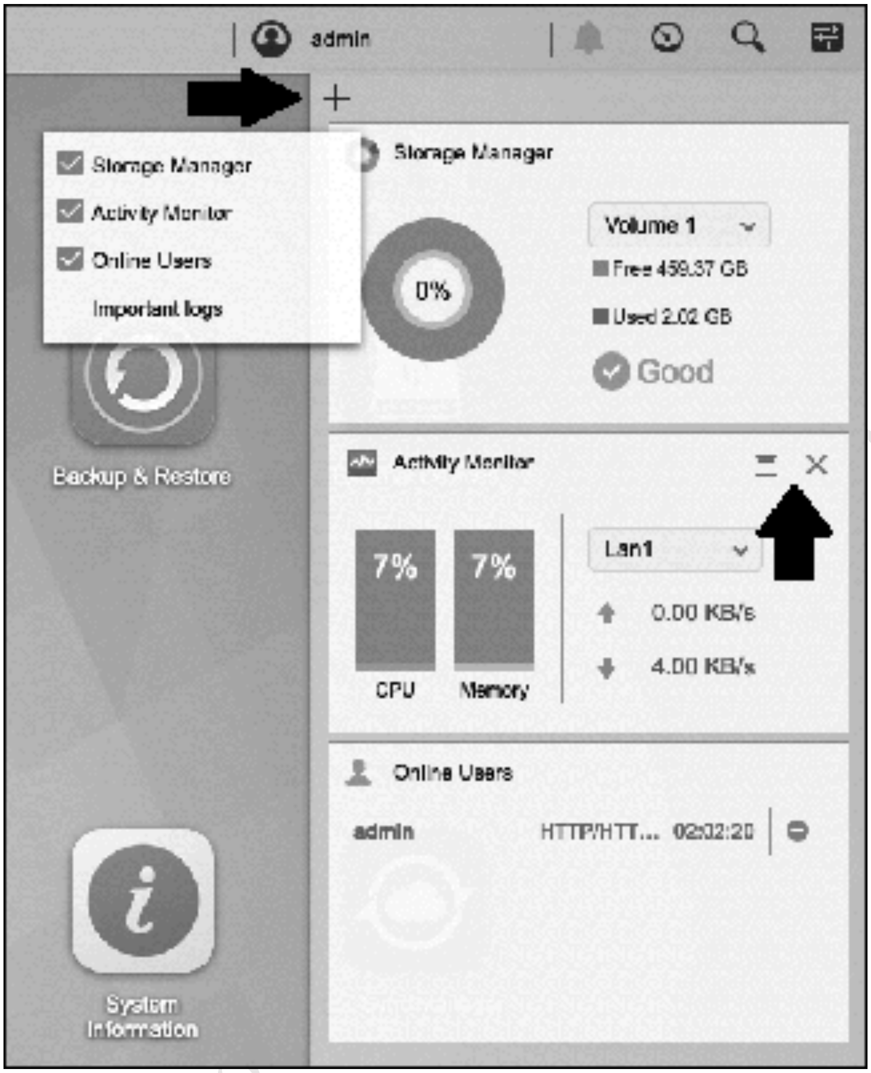


Figure 30: Tools

2.9 Change the IP Address

Note: if you already understand what IP addresses are, you can skip the first four paragraphs and jump to the one that begins 'To view and change the IP address…'.

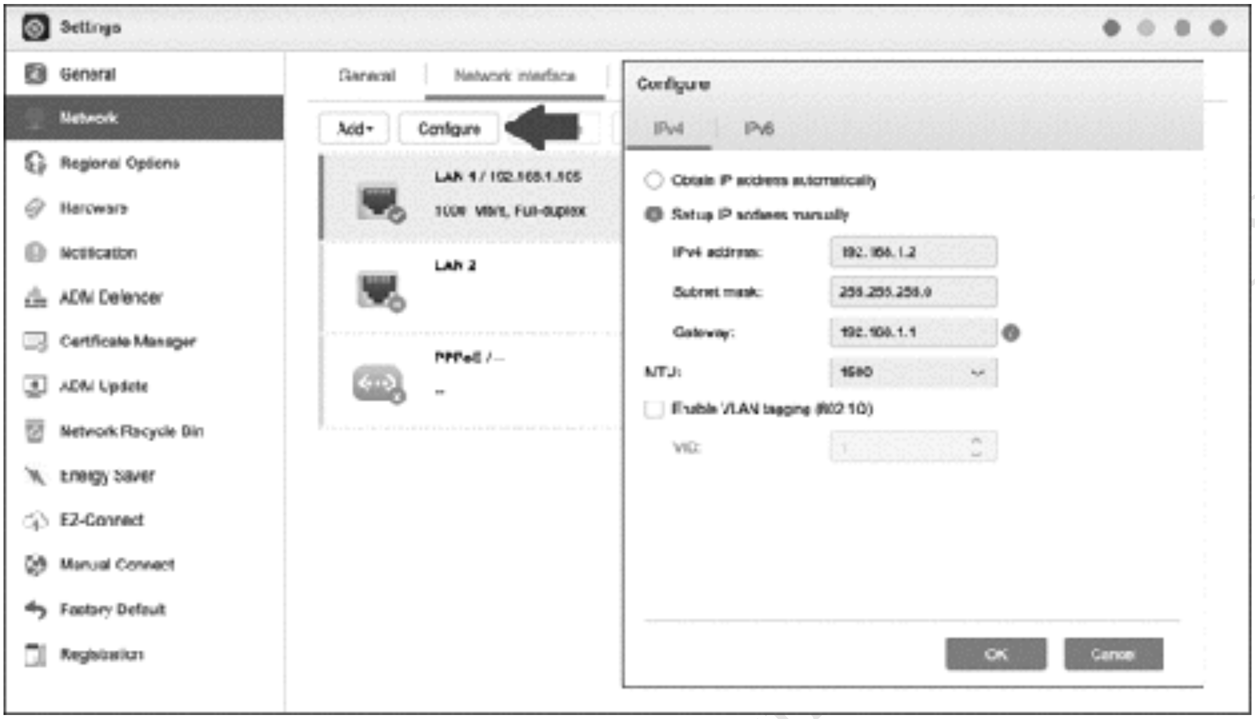
Every device within a network is represented by a unique number, known as the IP address. This consists of four sets of three digits, separated by periods, ranging from 000.000.000.000 through to 255.255.255.255. Most of these IP addresses are reserved for websites and other internet applications, although 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 of ADM, the NAS will have received a dynamic IP address from the router's DHCP server. Although dynamic IP is more practical for devices such as computers and tablets and smartphones, as per the previous paragraph, servers and NAS boxes work better with fixed or static addresses so we need to change matters.

To view and change the IP address, click **Preferences** followed by **Network** (alternatively you can click **Settings** followed by **Network**). Click the **Network Interface** tab. Highlight the first or only network adapter, which will be called *LAN 1*, and click **Configure**.



Configure

○ Obtain IP address automatically

● Setup IP address manually

IPv4 address: 192.168.1.2

Subnet mask: 255.255.255.0

Gateway: 192.168.1.1

MTU: 1500

□ Enable VLAN tagging (802.1Q)

VID: 1

Figure 31: Network Interface screen

The panel will state that the server is currently configured to *Obtain IP address automatically*, so we need to click the **Set up IP address manually** option instead. In this example our internet router – referred to by ASUSTOR using the alternative name of *Gateway* - is on 192.168.1.1, so we have chosen a nearby address of 192.168.1.2 for the NAS (it is the fourth and final set of digits that is significant in small networks and the first three sets should not be altered). The *Subnet Mask* can be left as 255.255.255.0 (unless you are in a large network, containing more than 255 devices). Click **OK**. Having made the change, the ADM screen will refresh and it will be necessary to log back in.

2.10 File Services

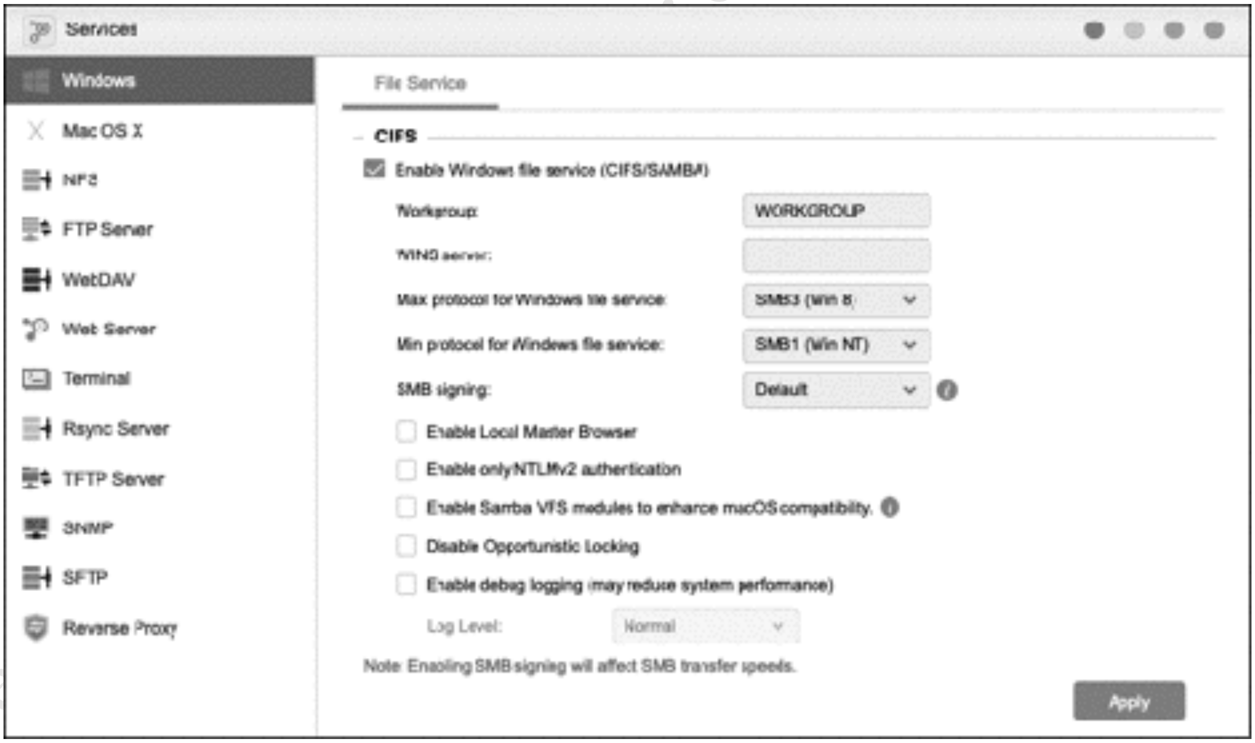
File Services refers to the technical means or *protocols* by which ADM provides access to files and folders for different types of client devices. These clients can be Windows PCs, Macs, or Linux machines and other Unix variants. Other devices, such as tablets and smartphones, may be able to access files on the NAS if they understand the underlying protocols associated with these computer types or are equipped with suitable apps. Further file services are also available for more specialized purposes, for example *Rsync Server*, which is used in certain types of backups and is covered later in this manual.

By default, ADM assumes that you will be using Windows PCs and Macs and it is not usually necessary to change any of the settings for File Services. So, most people reading 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 actually called *Workgroup*; you are using older versions of macOS i.e. OS X 10.8 or earlier; 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 special characteristics.

Launch **Services** from the Desktop and click **Windows**. If your workgroup is not called *Workgroup*, change the name of the **Workgroup** to match that of your computers. Having to do this would be unusual, as *WORKGROUP* is the default name on Windows computers. There are also some options and advanced settings relating to the SMB protocol and which may be of interest to experienced Windows Server administrators.

If, for some reason, you wanted to disable support for CIFS/SAMBA/SMB (not recommended), you would do so by unticking the **Enable Windows file service (CIFS/SAMBA)** box.

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



CIFS

☑ Enable Windows file service (CIFS/SAMBA)

Workgroup: WORKGROUP

WINS server:

Max protocol for Windows file service: SMB3 (Win 8)

Min protocol for Windows file service: SMB1 (Win NT)

SMB signing: Default

☐ Enable Local Master Browser

☐ Enable only NTLMv2 authentication

☐ Enable Samba VFS modules to enhance macOS compatibility.

☐ Disable Opportunistic Locking

☐ Enable debug logging (may reduce system performance)

Log Level: Normal

Note: Enabling SMB signing will affect SMB transfer speeds.

Figure 32: Windows File Service

One common question is: what is the difference between CIFS and SMB? The answer is that for most intents and purposes there isn't one. The names reflect small variants in the same networking protocol, which has been modified since its original introduction in the 1980s. In some respects, CIFS is considered an archaic term and SMB is more generally used, which is what we will do in this book.

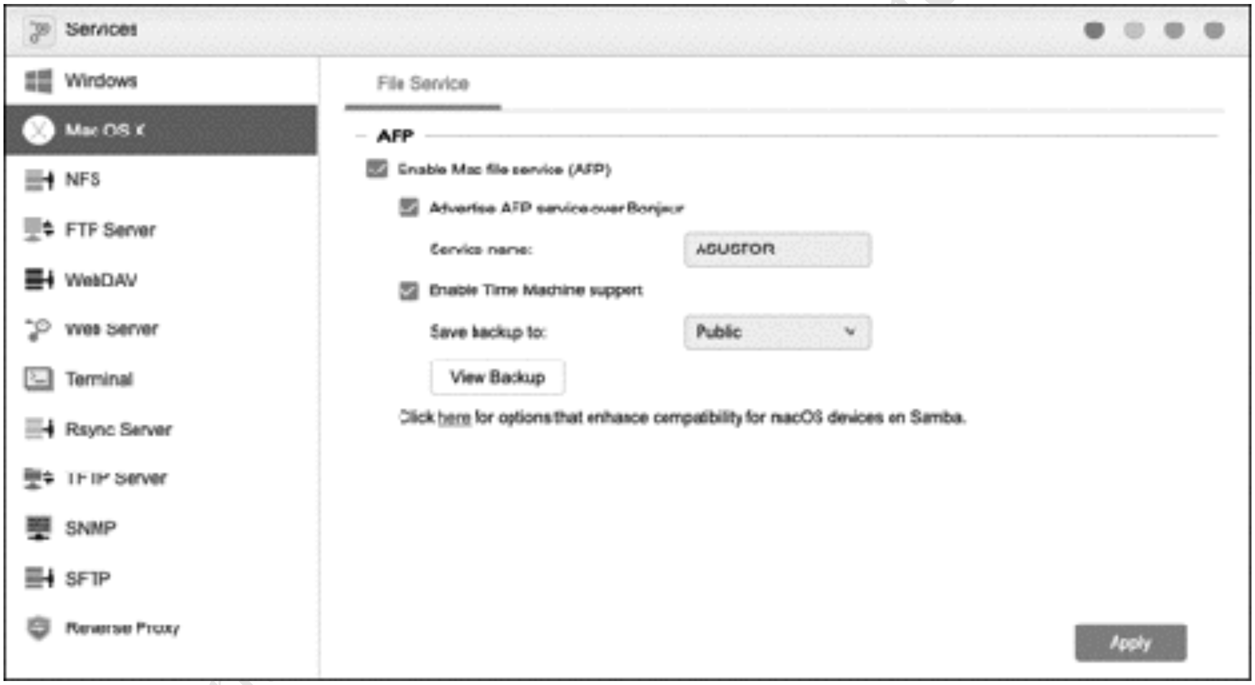
Macs

Historically, Apple computers used a network protocol called AFP (*Apple Filing Protocol*) whilst Windows computers used SMB (Server Message Block), also called CIFS. 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 have AFP service enabled if you have any Macs; you will certainly need it if you are using older versions of OS X. To enable: launch **Services** from the Desktop, click **Mac OS X** and tick the **Enable Mac file service (AFP)** box.

If you are planning to use Time Machine, which is covered in detail in section 7.10 Backing Up Macs, tick the **Enable Time Machine support** box.

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

Note: in some cases, it is possible to improve the support for macOS with Samba/CIFS and there is a link on the screen to 'enhance compatibility' that takes you back to the Windows options.



AFP

☑ Enable Mac file service (AFP)

☑ Advertise AFP service over Bonjour

Service name: ASUSTOR

☑ Enable Time Machine support

Save backup to: Public

View Backup

Click here for options that enhance compatibility for macOS devices on Samba.

Apply

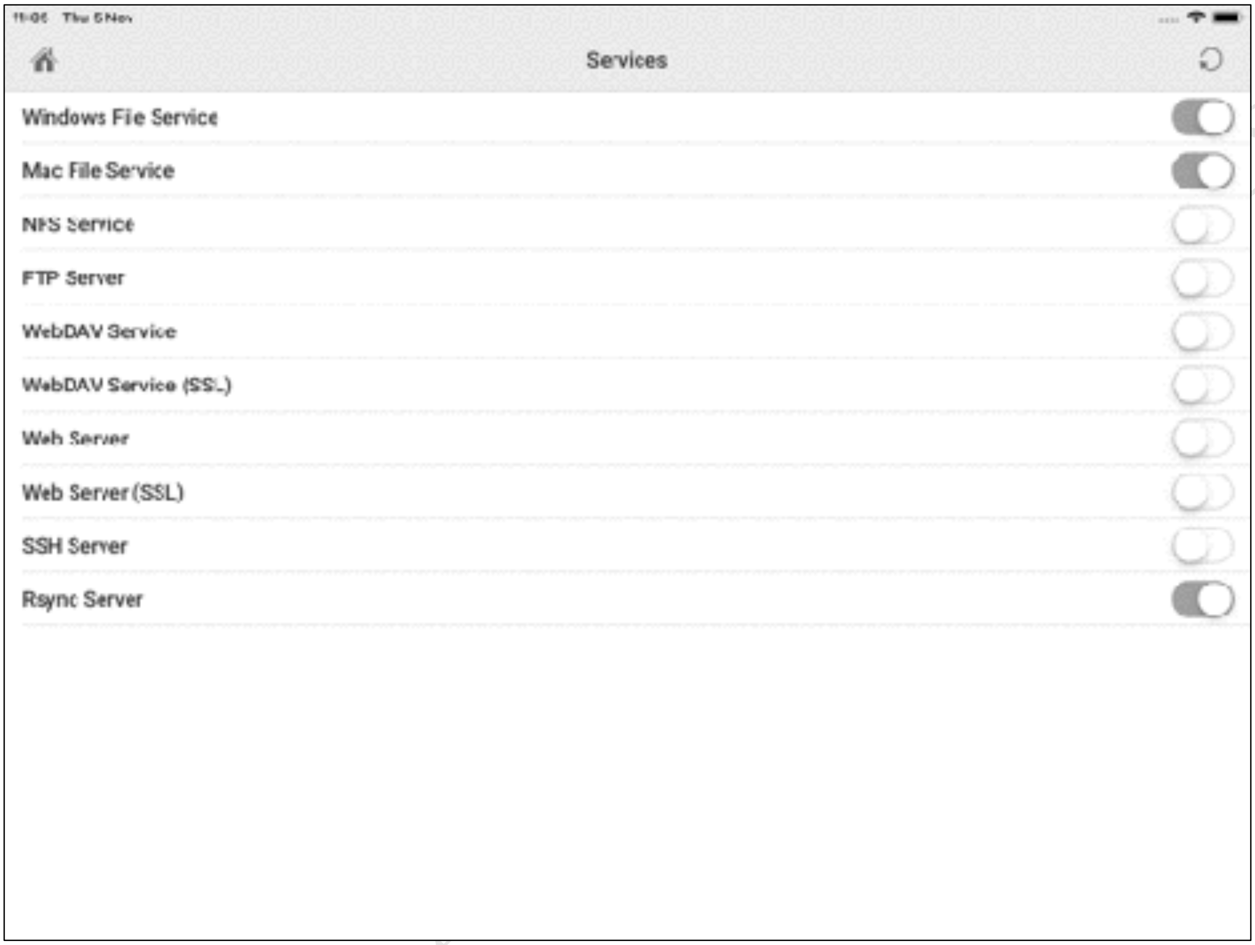
Figure 33: Mac OS X File Service

Linux/Unix Computers

Most Linux/Unix distributions include the ability to connect to SMB-based systems, which ADM 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 NAS. To so, Launch **Services** from the Desktop, click **NFS** and on that panel tick the **Enable NFS service** box, followed by **Apply**.

Setting File Services in AiMaster

Individual file services can be enabled/disabled in AiMaster. However, it is not possible to specify the parameters of the individual services from here, only by using the full web interface as described above.



11:06 Thu 5 Nov

Services

- Windows File Service ●
- Mac File Service ●
- NFS Service ○
- FTP Server ○
- WebDAV Service ○
- WebDAV Service (SSL) ○
- Web Server ○
- Web Server (SSL) ○
- SSH Server ○
- Rsync Server ●

Figure 34: File Services in AiMaster

2.11 Hardware & Power Management

This section is optional or can be returned to at a later date. There are three courses of action available:

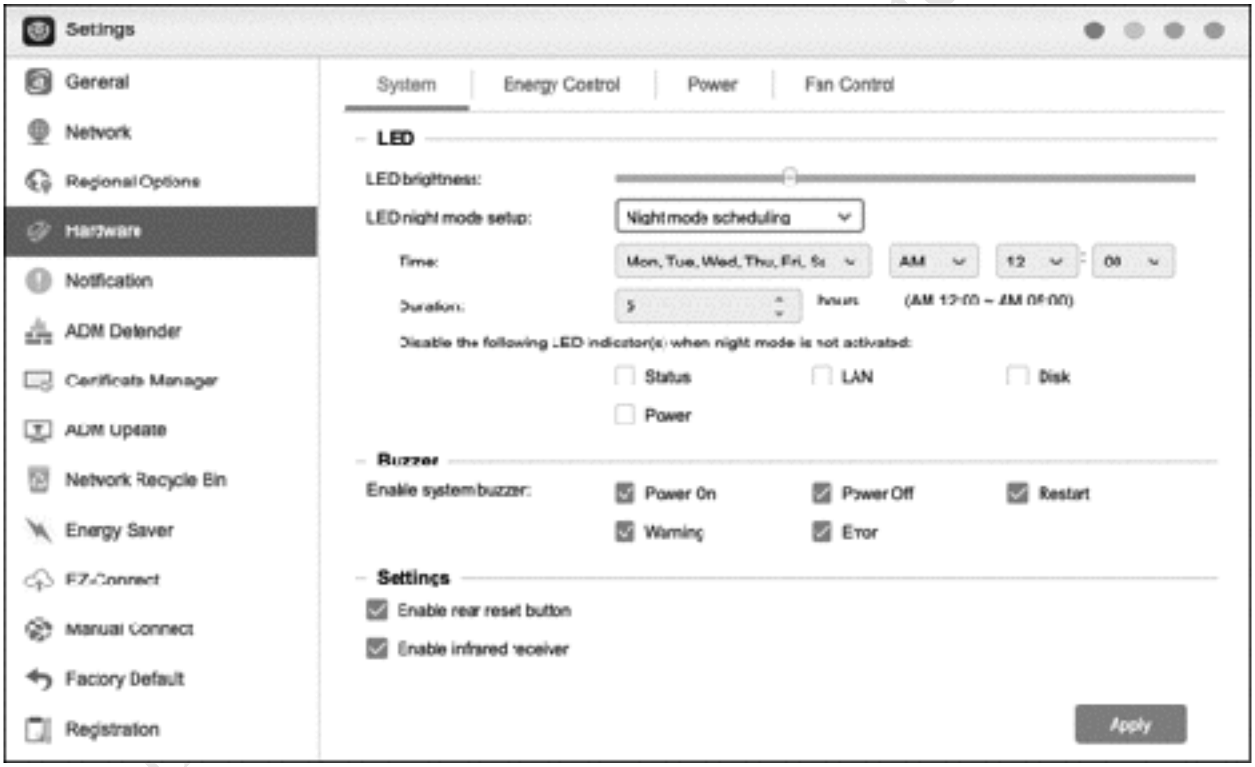
1 – Ignore altogether and jump to 3 USERS.

2 – Take the shortcut. Click **Settings** > **Energy Saver** (alternatively **Preferences** > **Energy Saver**), make sure the **ASUSTOR Energy Saver (recommended)** option is selected and click **Apply**. Then continue with 3 USERS.

3 – Use individual settings to fine tune power consumption, noise levels and certain features, plus schedule the NAS to power on and shutdown automatically. How to do this is described below. Note that the contents of the following screens may vary, depending on the ASUSTOR model.

Controlling the LED Lights

On most models, it is possible to set the brightness of the LED indicators on the unit. Not only does this reduce energy consumption, it can also reduce distraction if the server is located in, say, a bedroom or next to a television set. Go into **Settings** > **Hardware** and click the **System** tab:



LED

LED brightness:

LED night mode setup: Night mode scheduling

Time: Mon, Tue, Wed, Thu, Fri, Sa AM 12 : 00

Duration: 5 hours (AM 12:00 ~ AM 05:00)

Disable the following LED indicator(s) when night mode is not activated:

□ Status □ LAN □ Disk

□ Power

Buzzer

Enable system buzzer: ☑ Power On ☑ Power Off ☑ Restart

☑ Warning ☑ Error

Settings

☑ Enable rear reset button

☑ Enable infrared receiver

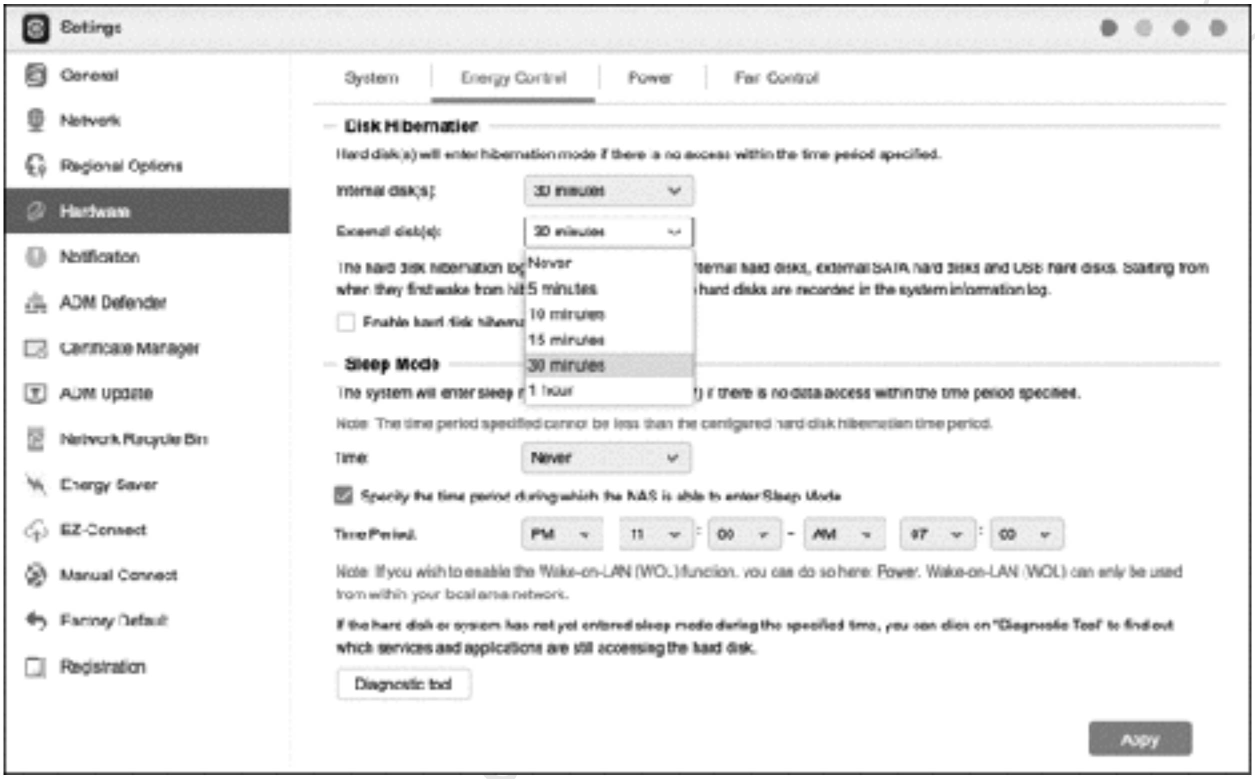
Figure 35: Hardware System settings

The LED section is at the top of the screen. Use the slider control to set the brightness of the LEDs. Additionally, the LEDs can be scheduled for ‘Night mode’, during which they are switched off altogether, other than the power indicator which will flash every 10 seconds. To switch off individual LEDs at other times, place ticks in the *Disable the following LED indicator…* section.

Having made changes, click the **Apply** button.

Disk Hibernation

The disk drive(s) can be configured to go into hibernation mode after a set period. This saves energy but will result in a short delay when someone next accesses the server, typically in the order of about 15-30 seconds while the disks spin up again, unless you are using SSDs – *Solid State Drives* – which have no spin time and are instantly available. To control this feature, go to **Preferences > Hardware** > **Energy Control**. Use the dropdowns to specify the hibernation time; if the server is only used infrequently it can be set to a short interval (e.g. 5 minutes), but if it is constantly in use then a higher value (e.g. 30 minutes or an hour) might be more appropriate. Choose values and click **Apply**.



Disk Hibernation

Hard disk(s) will enter hibernation mode if there is no access within the time period specified.

Internal disk(s): 30 minutes

External disk(s): 30 minutes

Never
5 minutes
10 minutes
15 minutes
30 minutes
1 hour

The hard disk hibernation log … internal hard disks, external SATA hard disks and USB hard disks. Starting from when they first wake from hi… hard disks are recorded in the system information log.

□ Enable hard disk hiberna…

Sleep Mode

The system will enter sleep … if there is no data access within the time period specified.

Note: The time period specified cannot be less than the configured hard disk hibernation time period.

Time: Never

☑ Specify the time period during which the NAS is able to enter Sleep Mode

Time Period: PM 11 : 00 - AM 07 : 00

Note: If you wish to enable the Wake-on-LAN (WOL) function, you can do so here: Power. Wake-on-LAN (WOL) can only be used from within your local area network.

If the hard disk or system has not yet entered sleep mode during the specified time, you can click on "Diagnostic Tool" to find out which services and applications are still accessing the hard disk.

Figure 36: Disk Hibernation settings

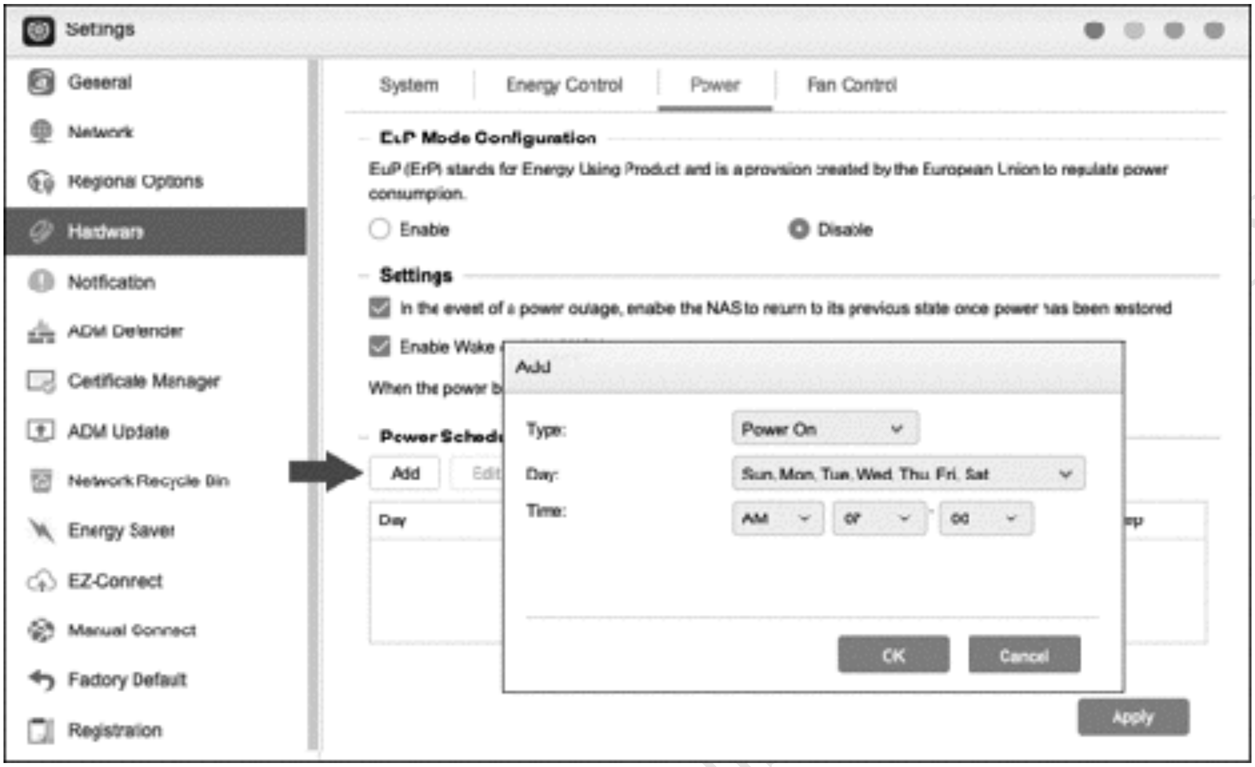
Sleep Mode

If the NAS has not been accessed for a specified time period, it can be programmed to hibernate, thus saving energy. To control this, use the dropdown in the *Sleep Mode* section of the Energy Control panel. To restrict sleep mode to a particular time of day, tick the **Specify the time period during which the NAS is able to enter Sleep Mode** box and use the dropdowns to define the hours. In the above screen shot, the NAS will only enter sleep mode due to inactivity between the hours of 11:00 pm (23:00) and 7:00 am (07:00). Having made any changes, click **Apply**.

Power Scheduling

Unlike desktop and laptops, NAS boxes are usually left running 24x7. However, the server can be scheduled to power itself on and off automatically and doing so can save on energy costs and possibly enhance security (as security problems cannot occur when the server is switched off). If this is done, then it is important to ensure that the NAS will not be powered down when an activity such as backup or an anti-virus scan is scheduled to take place.

To create a schedule, go to **Preferences** > **Hardware** > **Power**. In the *Power Scheduling* section, click **Add**. On the resultant panel, from the *Type* dropdown choose **Power On** and specify the *Day* and *Time* using their dropdowns. Click **OK**. Now repeat, but this time choose a **Power Off** event. Having made changes, click **Apply**.



EuP Mode Configuration

EuP (ErP) stands for Energy Using Product and is a provision created by the European Union to regulate power consumption.

○ Enable ● Disable

Settings

☑ In the event of a power outage, enable the NAS to return to its previous state once power has been restored

☑ Enable Wake

When the power b

Power Schedu

Add

Type: Power On

Day: Sun, Mon, Tue, Wed, Thu, Fri, Sat

Time: AM 07 00

Figure 37: Power Scheduling

Fan Control

NAS units have fans in them to keep them running cool and the settings can be adjusted to reduce the noise levels and/or cope with warmer environments. To adjust, click **Settings > Hardware > Fan Control**.

The default setting is *Auto* and in most cases this is the best setting to have. Alternatively, the Fan rotation speed setting can be set to Low, Medium or High. In a domestic environment you might wish to have the fan on low speed to minimize noise, whereas in a hot office during the Summer you would probably want high speed.

After making any changes, click the **Apply** button.

3

USERS

3.1 Overview

To access the NAS, it is necessary to have a *user account* on it. During the installation of ADM an initial administrator user was created; if you are the only person who will ever use the NAS, you can work with that user account for everything and skip this chapter altogether. However, if other people will also be using the NAS, such as in a typical home, business or educational environment, then you will need to create user accounts for them.

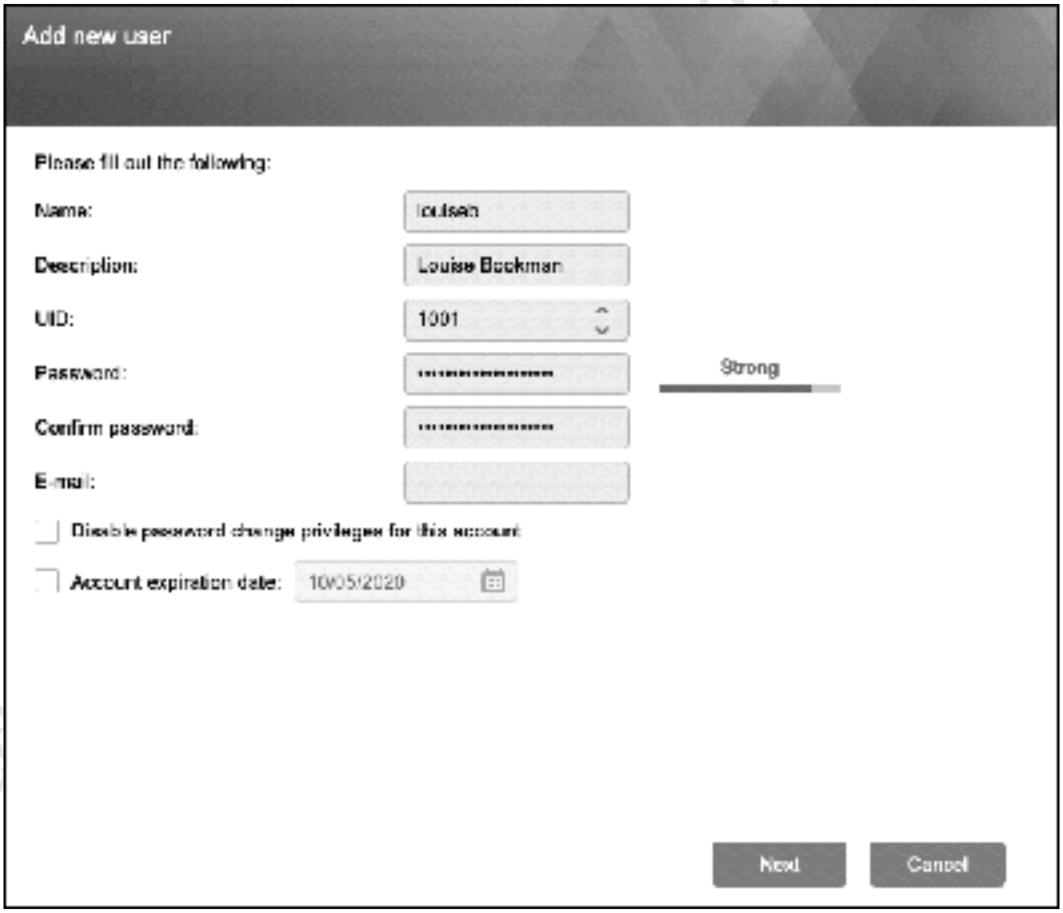
This is one area where a different approach can be taken depending on whether it is a home or business network. In the case of a home network the user names can be anything you want, although there is merit in following a scheme. For instance, you could use the first names of the family or household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

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

3.2 Adding Users

To add (create) a new user, go to **Preferences** and click **Local Users**. Click the **Add** button, which is a drop-down with three entries: *Add new user* – for creating individual users, one at a time; *Add Multiple Users* – for creating users in bulk, as might be done in a large organization such as a business or educational establishment, using an arbitrary naming scheme e.g. *pupil001*, *pupil002*, *pupil003* etc.; *Import Users* – for creating users in bulk, such as might be done in a large organization, using a spreadsheet containing names extracted from another computer system e.g. a registration or HR application.

As a household or typical small business will only have a relatively small number of users, we will create them one at a time using the first option, so click **Add new user**. Enter the user's *Name* and an optional *Description*; names can be up to 32 characters in length and can use Latin (Western/'ABC'), Chinese, Japanese, Korean or Cyrillic characters. The system will generate a unique numeric *UID* (User ID) for each user – this is used internally by ADM and is not normally referenced when using the NAS. Enter a *Password* along with its confirmation; the password should be at least 8 characters in length and include both letters and numbers; as the password is entered, ADM will advise how strong it is. Optionally, specify the user's email address. You can use the first tickbox to prevent the user from changing their password and the second tickbox to specify an *Account expiration date* – this can be useful in schools with young children, or where shared accounts are used. Click **Next**:



Add new user

Please fill out the following:

Name: louiseb

Description: Louise Bookman

UID: 1001

Password: •••••••••••••• Strong

Confirm password: ••••••••••••••

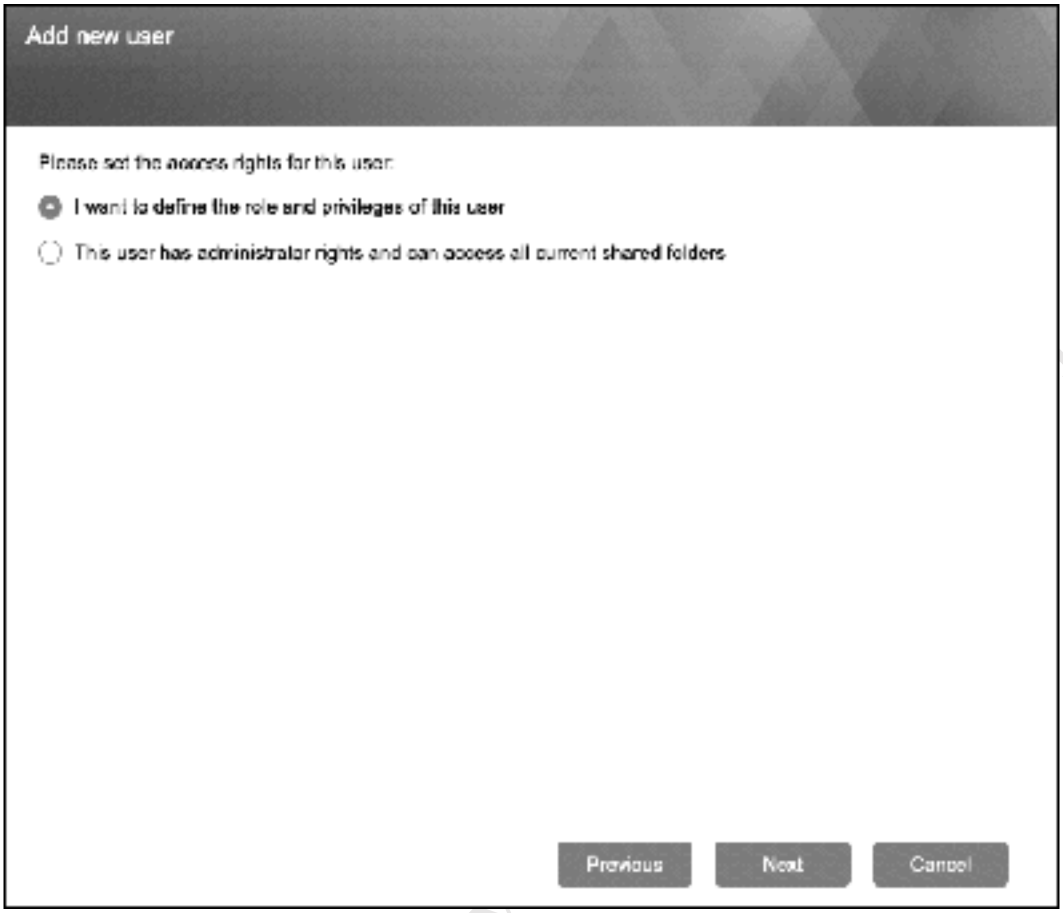
E-mail:

□ Disable password change privileges for this account

□ Account expiration date: 10/05/2020

Figure 38: Add new user

The second screen is for defining access rights for the user, meaning what shared folders they can use. Normally the first option should be selected and it is considered bad practice to have more than one user with administrative rights. Click **Next**:



Add new user

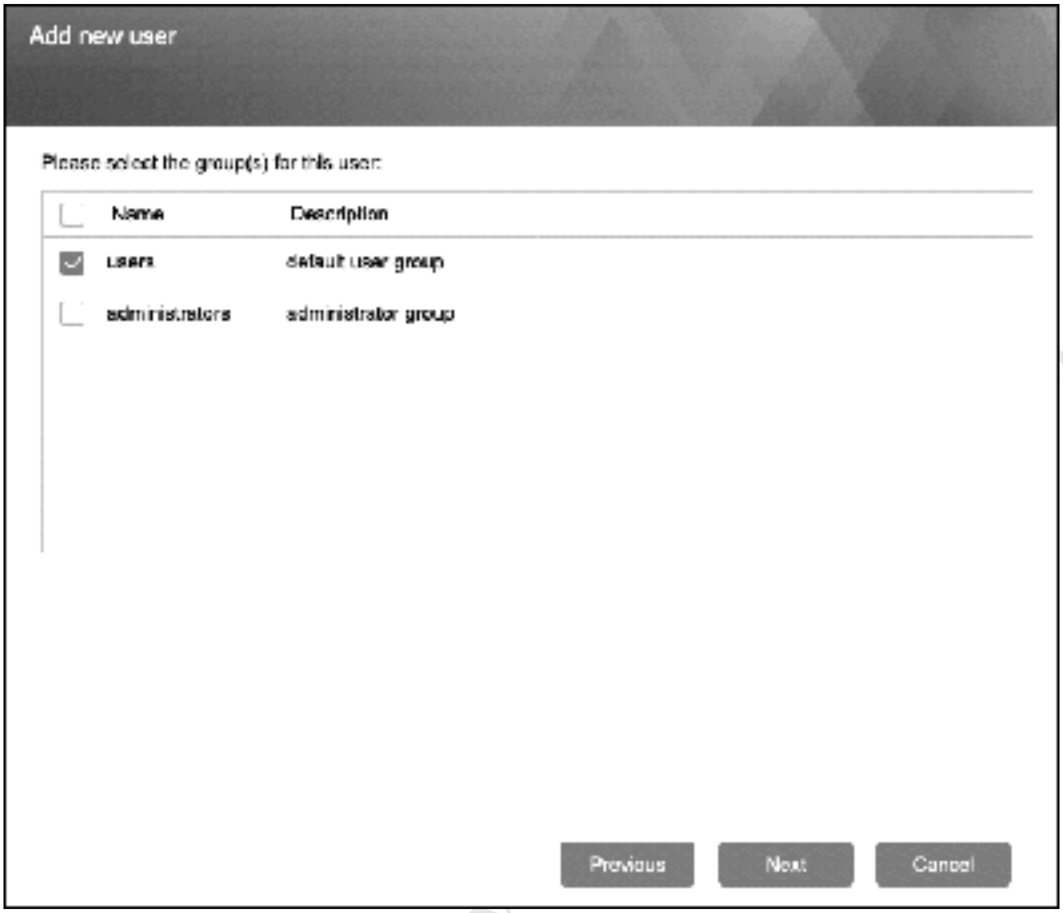
Please set the access rights for this user:

● I want to define the role and privileges of this user

○ This user has administrator rights and can access all current shared folders

Figure 39: Access rights

On the subsequent screen check that they are a member of the *users* group. Do not make them a member of the *administrators* group, as access to this should be restricted to the main administrator user(s) only. Click **Next**:



Add new user

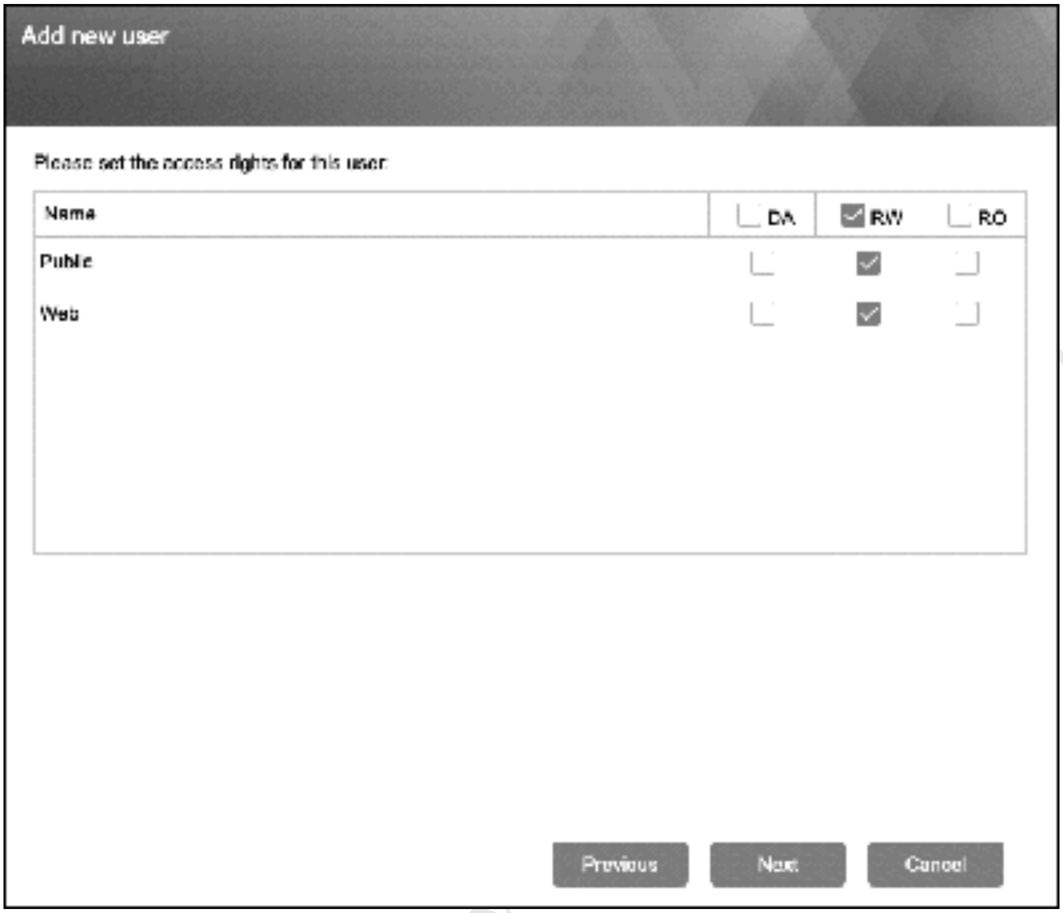
Please select the group(s) for this user:

□	Name	Description
☑	users	default user group
□	administrators	administrator group

Figure 40: Group membership

The following screen defines which shared folders the user has access to. Shared folders are covered in detail in chapter 4 SHARED FOLDERS, but on a fresh installation there will be at least two, called *Public* and *Web*. The three types of access are: *DA – Denied Access*, meaning they have no access at all to the folder; *RW - Read/Write*, meaning they can do anything with the folder; *RO - Read Only*, meaning that the user can use the files in the folder but cannot update them or add more to the folder.

Give the user Read Write access to the *Public* and *Web* folders and click **Next**.



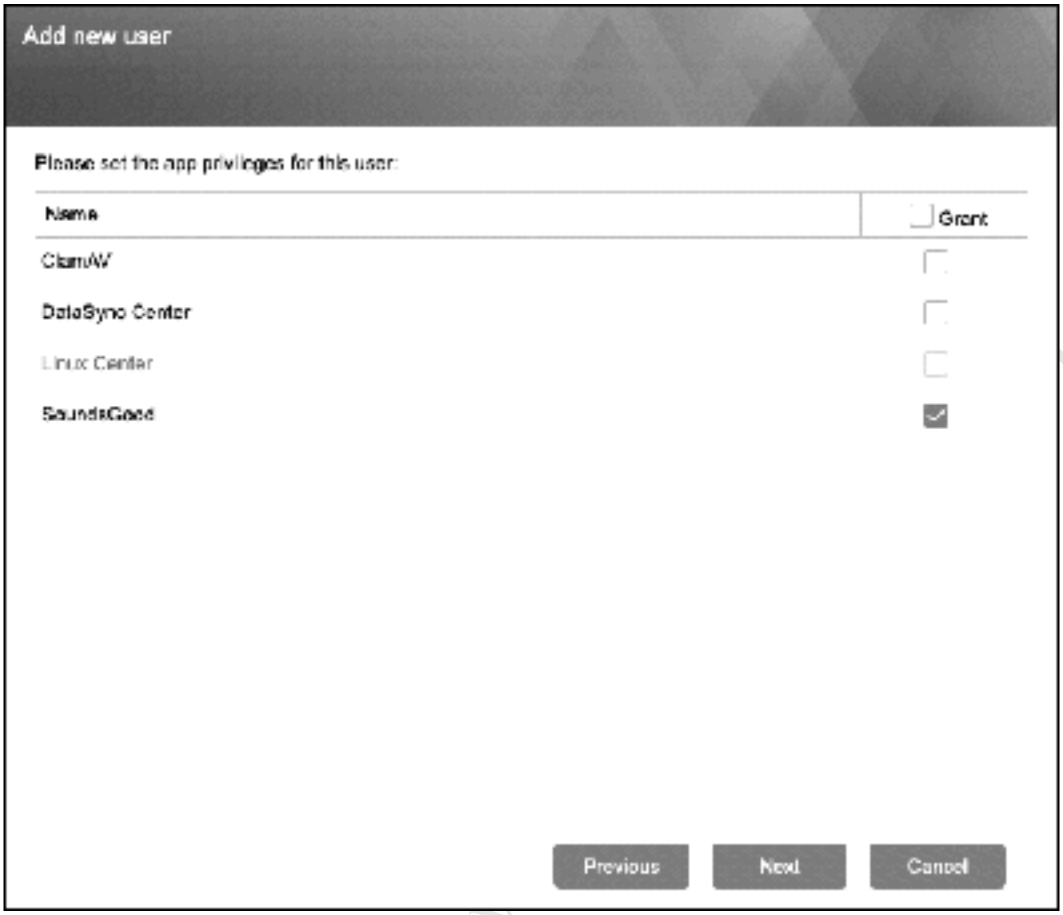
Add new user

Please set the access rights for this user:

Name	□ DA	☑ RW	□ RO
Public	□	☑	□
Web	□	☑	□

Figure 41: Shared Folder Permission

On the next screen, specify which applications the user is allowed to use (the contents of this screen will vary, depending on which apps have been installed). Click **Next**.



Add new user

Please set the app privileges for this user:

Name	□ Grant
ClamAV	□
DataSync Center	□
Linux Center	□
SoundsGood	☑

Figure 42: Set app privileges

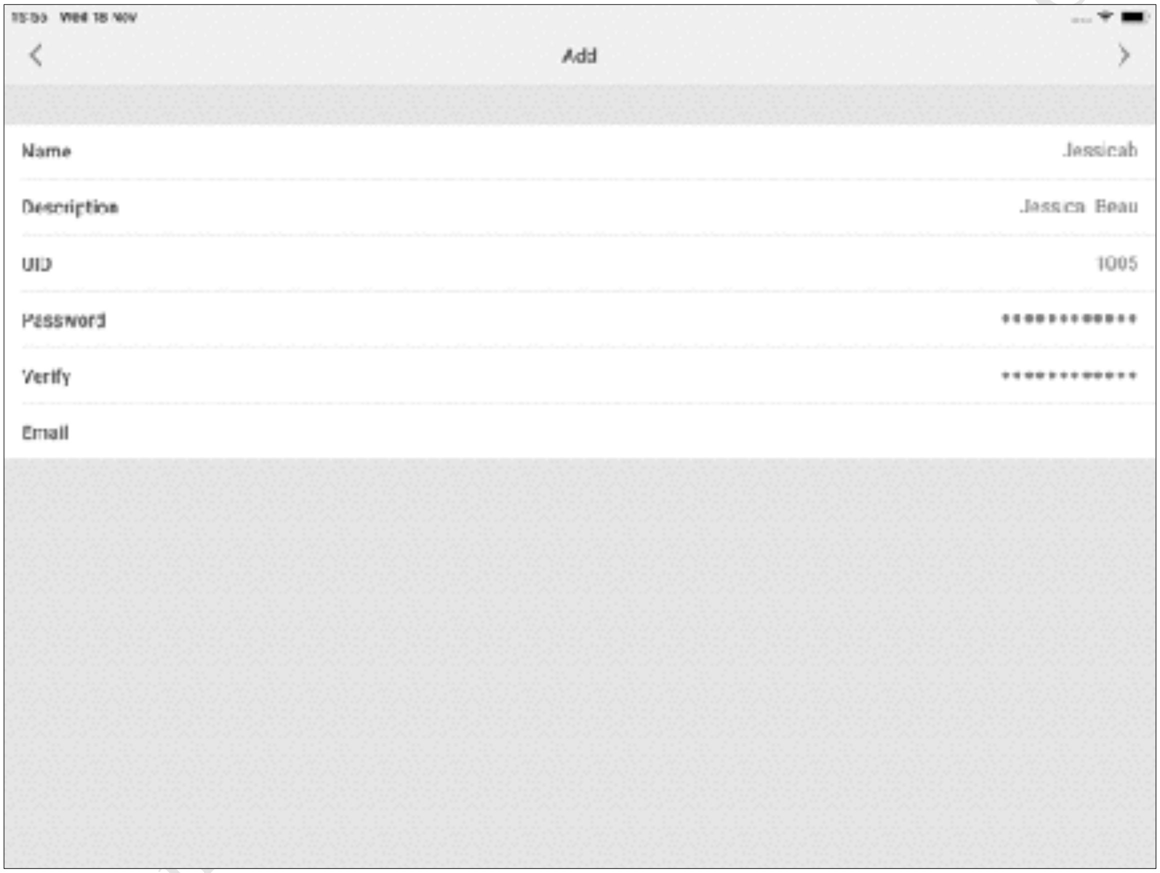
A confirmation screen appears. If everything is satisfactory, click **Finish** to add the new user, otherwise use the **Previous** button to go back and make corrections. The newly created user will now be listed on the Local Users screen.

This process should be repeated until all the users have been created. If you are working in an organization and have a relatively large number of users to be created, you might find it helpful to first create a checklist of names and passwords to work through. As the users are created, the main Users screen will be populated with their details.

Note: you may have noticed on the Access Control screen that there are two types of users: *Local Users* and *AD/LDAP* Users. Throughout this book we will be working with local users, which are the regular ones on a NAS system. AD/LDAP Users are only used when the NAS is integrated with a Windows Server-based network running Active Directory, which is a scenario more applicable to large businesses rather than homes or small businesses.

Adding Users with AiMaster

Users can also be created using the AiMaster utility. Tap the **Access Control** icon; at the bottom of the screen are three small icons, which, working from left to right, are for Local Users, Local Groups and App Privileges. Tap the first one to display a list of existing users, then tap the plus sign (+) in the top right-hand corner of the screen to add a new one. Enter the user’s *Name* and an optional *Description*; names can be up to 32 characters in length and can use Latin (Western/‘ABC’), Chinese, Japanese, Korean or Cyrillic characters. The system will generate a unique numeric *UID* (User ID) for them – this is used internally by ADM and is not normally referenced when using the NAS. Enter a *Password* and its confirmation; the password should be at least 8 characters in length and include both letters and numbers. Optionally, specify the user’s email address. Tap the right-pointing chevron (arrow) at the top of the screen:



Name Jessicab

Description Jessica Beau

UID 1005

Password ************

Verify ************

Email

Figure 43: Adding a new user in AiMaster

On the subsequent screen, choose the *Access Rights*, which will usually be **Self Define** rather than *Administrator Rights*. Tap the right-pointing chevron at the top of the screen to continue. On the next screen, specify which group(s) the user will be a member of – usually this will be the default user group, called **users**. Tap the right-pointing chevron at the top of the screen to proceed.

The following screen defines which shared folders the user has access to. Shared folders are covered in detail in chapter 4 SHARED FOLDERS, but on a fresh installation there will be at least two, called *Public* and *Web*. The three types of access are: *DA – Denied Access*, meaning they have no access at all to the folder; *RW - Read/Write*, meaning they can do anything with the folder; *RO - Read Only*, meaning that the user can use the files in the folder but cannot update them or add to the folder. Tap each folder in turn and on the linked screen tap the access type. Give the user Read Write access to the *Public* and *Web* folders and click **Next**. When complete, tap the right-pointing chevron at the top of the screen.

The subsequent screen is for setting a storage quota for the user i.e. how much space the user is allowed. Storage quotas are not supported on Btrfs volumes, but in any case it is suggested you ignore this feature and just tap the tick in the top right-hand corner of the screen to create the user.

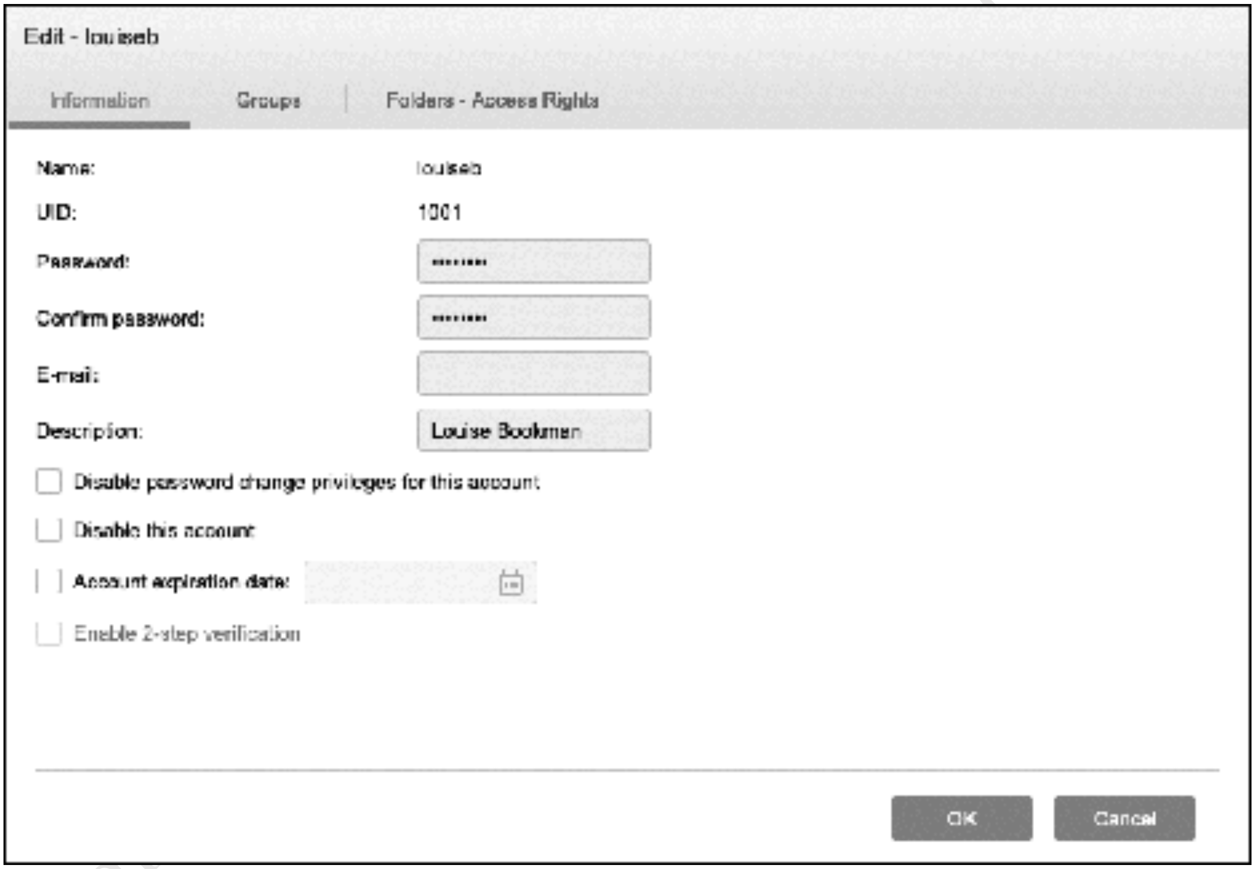
It then is necessary to specify which applications the user is allowed to use. To do this, tap the third mini-icon on the Access Control screen (it looks like a star) and a list of installed apps will be displayed. Click an app and on the resultant screen tap the name of the user, which will cause a tick to be placed against it.

3.3 Modifying, Disabling and Deleting Users

To modify an existing user, go to **Preferences** and click **Local Users** (alternatively, click **Access Control** followed by **Local Users**). Click to highlight the user's name, then click the **Edit** button. This provides access to the information that was specified when the user was added and which can now be modified. For instance, the user's password can be changed on the **Information** panel. Having made any changes click **OK**.

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, highlight the user's name, click **Edit**, place a tick in the **Disable this account** box and click **OK**.

To permanently delete a user, click on the user's name to highlight then click the **Remote** button. A warning message is displayed, advising that the user's data will be deleted. Acknowledge it and click **OK**.



Edit - louiseb

Name: louiseb

UID: 1001

Password: ••••••••

Confirm password: ••••••••

E-mail:

Description: Louise Bookman

□ Disable password change privileges for this account

□ Disable this account

□ Account expiration date:

□ Enable 2-step verification

Figure 44: Edit user details screen

Modifying Users with AiMaster

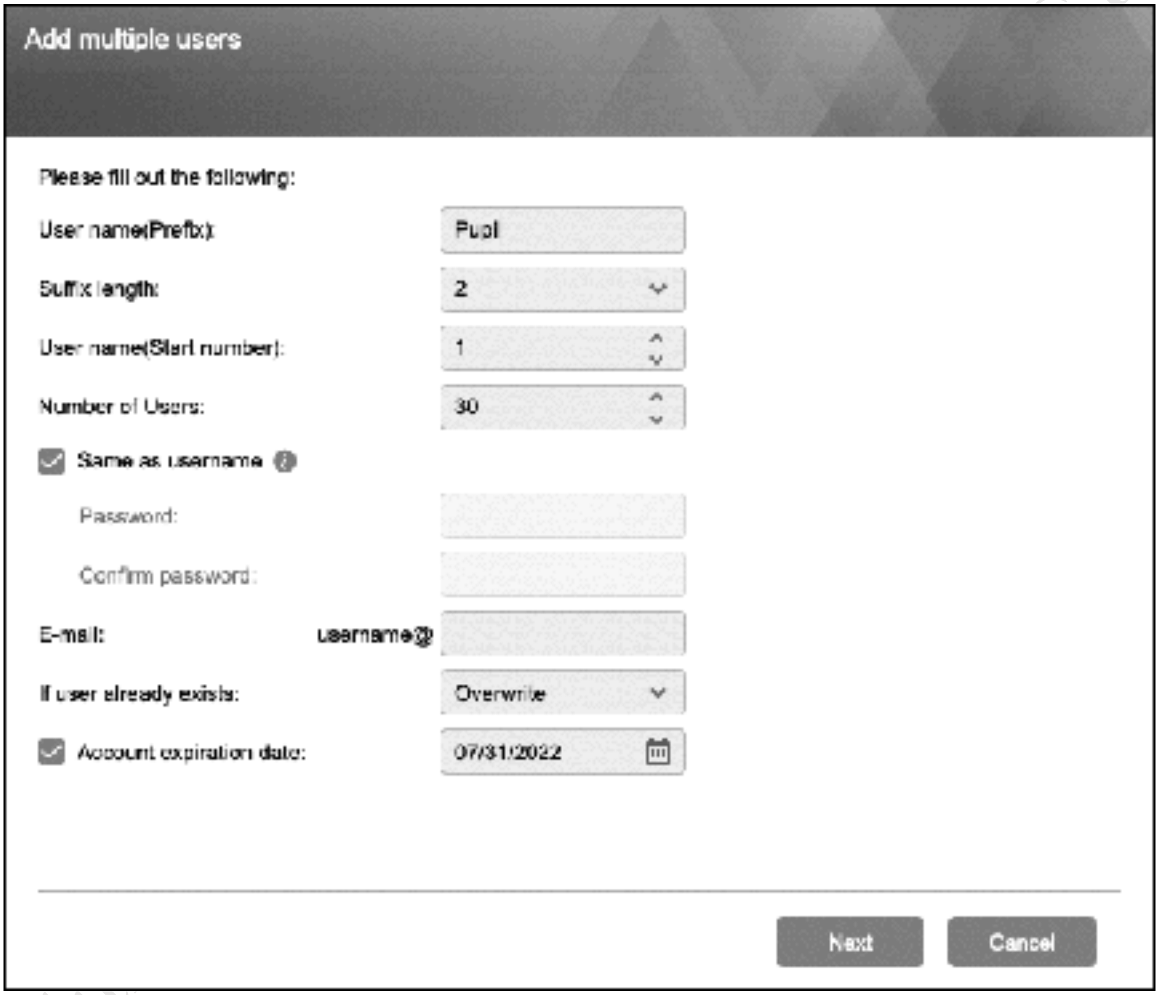
To modify an existing user with AiMaster, Tap the **Access Control** icon to display a list of existing users. Tap a user name to switch to edit mode and change their details by overtyping in the fields. It is not possible to delete a user from within AiMaster at the time of writing.

3.4 Adding Multiple Users

In a domestic or small business setting, creating users one at a time is unlikely to be arduous. But when many need to be created, such as in a larger business or an educational setting, it can be time consuming. Fortunately, ADM has two mechanisms to create users in bulk.

Method One – Add multiple users

Go into **Preferences** > **Local Users** (alternatively, **Access Control** > **Local Users**). Click the **Add** button and choose **Add Multiple Users** to display the following panel. In this example, we are setting up users for a classroom in a school.



Add multiple users

Please fill out the following:

User name(Prefix): Pupil

Suffix length: 2

User name(Start number): 1

Number of Users: 30

☑ Same as username

Password:

Confirm password:

E-mail: username@

If user already exists: Overwrite

☑ Account expiration date: 07/31/2022

Figure 45: Add multiple users

The way it operates is that user names are created in the form *prefix* + *suffix*, where suffix is a numeric value. For the *User name (Prefix)* we are using 'Pupil', the *Suffix length* is 2, the *User name (Start number)* is 1 and the *Number of Users* is 30. The effect of this will be to create 30 users, named *Pupil01* through *Pupil30*. Passwords will be generated, with the same values as the user names (although this is bad practice, so users should subsequently change them). Optionally, an *Account expiration date* can be specified, for example in the case of a school this might correspond to the end of the school year. Click **Next**. On the subsequent screen, specify the group(s) that the users will be members of and click **Next**. After that is a confirmation screen – click **Finish** and the users will be created, with a Results screen displayed when the process is complete.

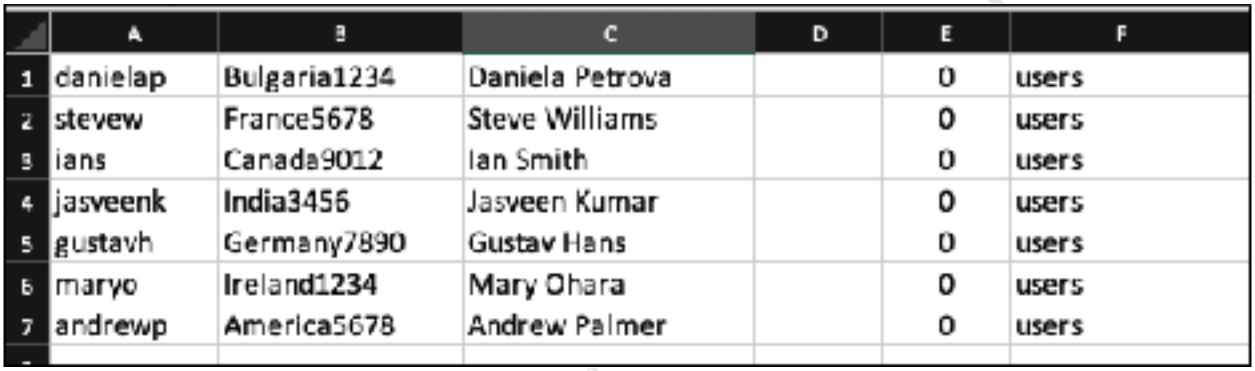
Method Two – Import users

ADM has the ability to create users from a file in CSV format, which can be created using Microsoft Excel or it might be possible to generate it from another computer system, such a school registration or human resources application.

The spreadsheet needs to be formatted as follows:

Column A – Username
Column B – Password
Column C – Description e.g. full user name
Column D – Email - optional
Column E – Quota in GBytes - optional, otherwise set to 0 (quotas are not supported on Btrfs volumes)
Column F – User Groups e.g. *users*. If members of multiple groups, separate names with commas

The spreadsheet needs to be saved in CSV format with UTF-8 encoding.



	A	B	C	D	E	F
1	danielap	Bulgaria1234	Daniela Petrova		0	users
2	stevew	France5678	Steve Williams		0	users
3	ians	Canada9012	Ian Smith		0	users
4	jasveenk	India3456	Jasveen Kumar		0	users
5	gustavh	Germany7890	Gustav Hans		0	users
6	maryo	Ireland1234	Mary Ohara		0	users
7	andrewp	America5678	Andrew Palmer		0	users

Figure 46: Example spreadsheet format for creating users

Go into **Preferences** > **Local Users** (alternatively, **Access Control** > **Local Users**). Click the **Add** button and choose **Import users**. Click **Browse** to navigate to and select the spreadsheet file; click **Preview** and the users to be added will be listed. The *Status* column needs to be blank, meaning there are no problems and you can click **OK** to create the users; otherwise click **Cancel** and correct the error(s) in the spreadsheet and try again.

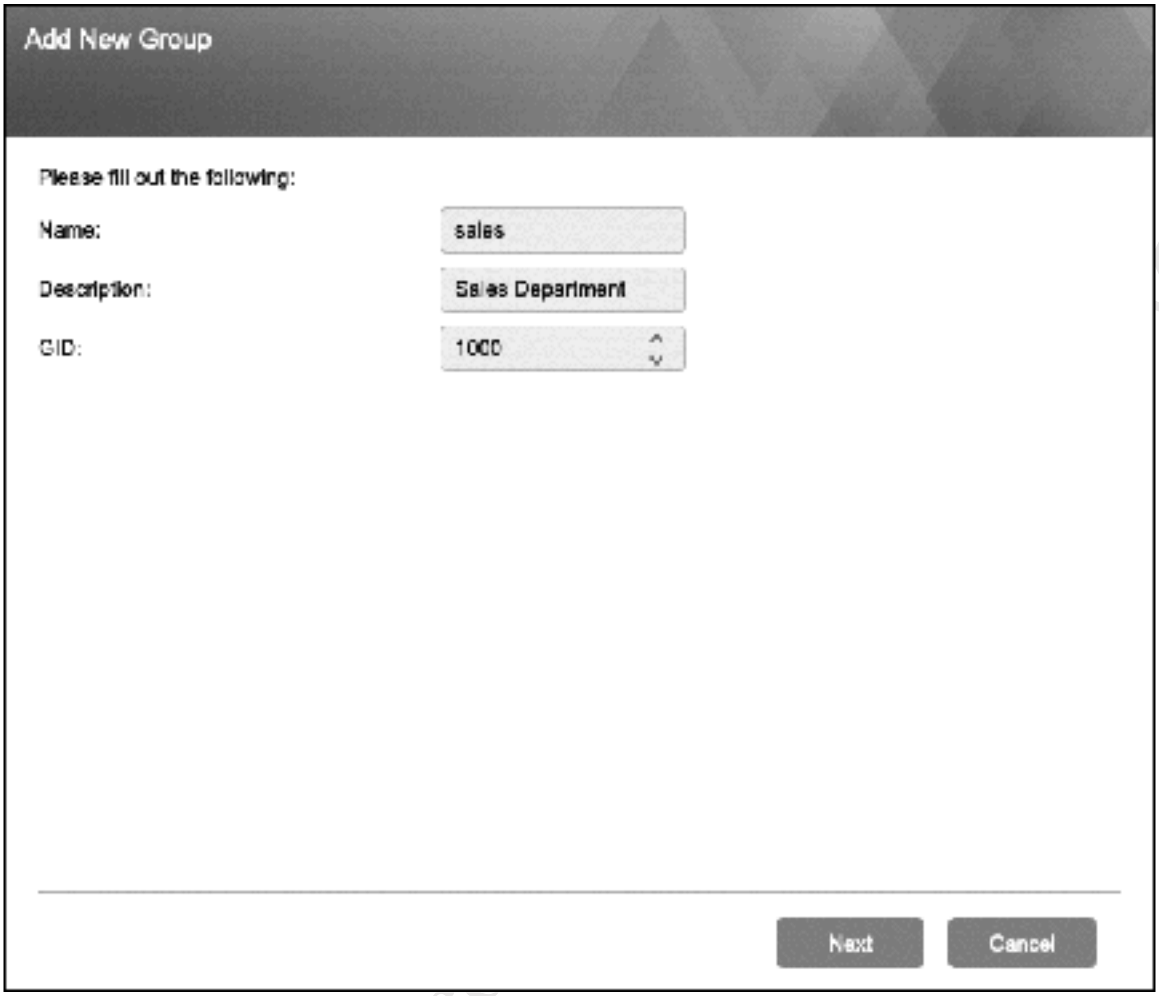
3.5 User Groups

In a household or 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 clearly becomes more time consuming; for instance, consider having to define the access rights for, say, 30 people. Such organizations are usually large enough that they contain departments or teams to carry out the different functions; for example, there might be some people working in accounts, some in sales, some in marketing and so on.

To support these typical business structures, ADM 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. There is a built-in group in ADM called *users* 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. Begin by creating a shared folder called *sales*. The method for creating shared folders is described in detail in 4.2 Adding a Shared Folder, but in summary: **Preferences** > **Shared Folders** > **Add**, name the folder *sales* and set access rights as *Deny Access* for the *users* group.

To add a new group, go to **Preferences** > **Local Groups** (alternatively, **Access Control** > **Local Groups**) and click **Add**. Specify a *Name* and optional *Description* for the new group. The *GID* or *Group Identification* number is generated automatically and there is no need to change it. Click **Next**:



Add New Group

Please fill out the following:

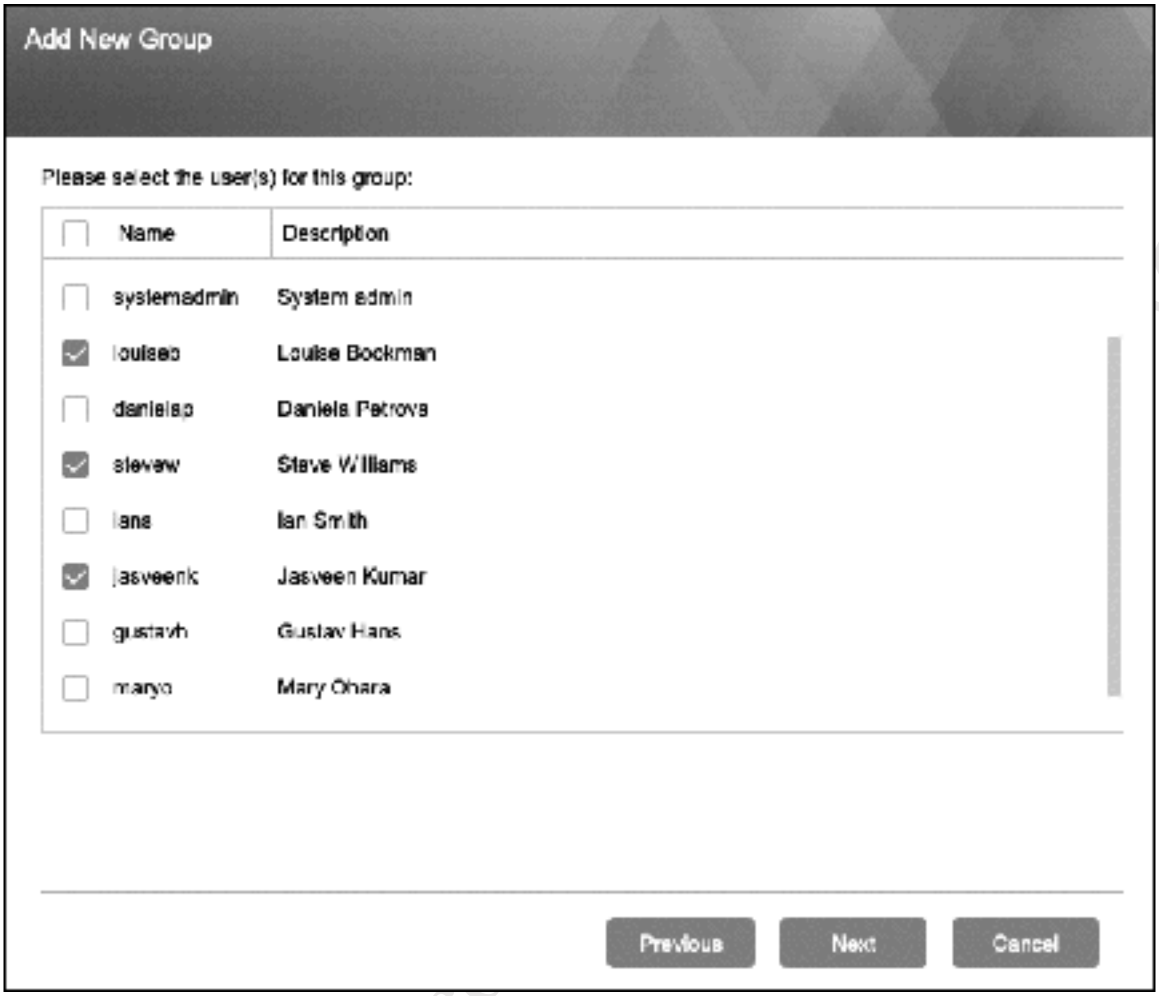
Name: sales

Description: Sales Department

GID: 1000

Figure 47: Add New Group

On the subsequent screen, select the users for the group by placing ticks against their names, then click **Next**:



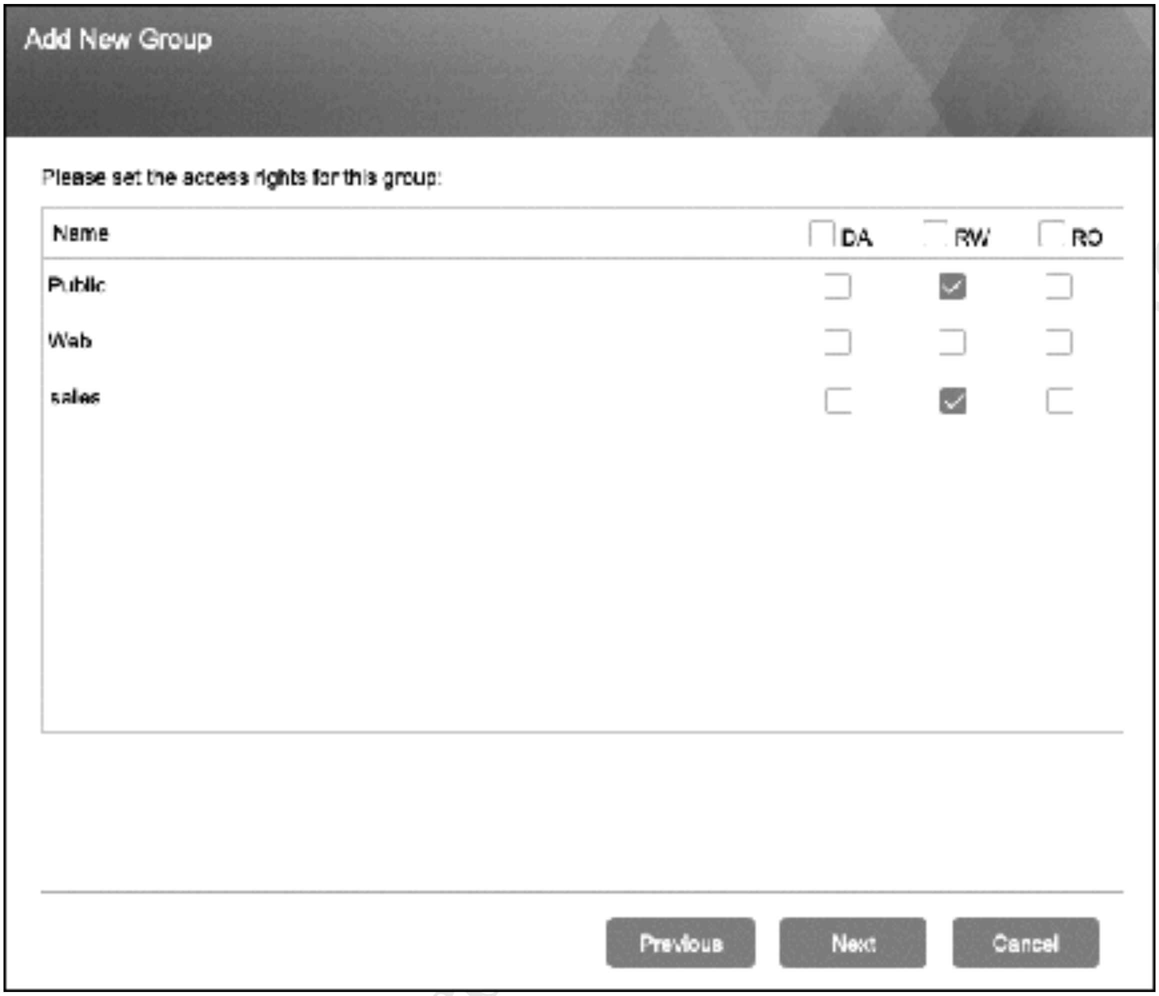
Add New Group

Please select the user(s) for this group:

☐	Name	Description
☐	systemadmin	System admin
☑	louiseb	Louise Bockman
☐	danielap	Daniela Petrova
☑	stevew	Steve Williams
☐	ians	Ian Smith
☑	jasveenk	Jasveen Kumar
☐	gustavh	Gustav Hans
☐	maryo	Mary Ohara

Figure 48: Specify the users for the group

On the following screen, set *Read Write* access rights for the *sales* group and click **Next**.



Add New Group

Please set the access rights for this group:

Name	□ DA	□ RW	□ RO
Public	□	☑	□
Web	□	□	□
sales	□	☑	□

Figure 49: Access rights for the group

A confirmation screen is shown – click **Finish** to create the group.

The benefit of groups 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.

Adding Groups with AiMaster

Groups can be created using the AiMaster utility. Tap the **Access Control** icon; at the bottom of the screen are three small icons, which, working from left to right, are for Local Users, Local Groups and App Privileges. Tap the central one to display a list of existing groups, followed by the plus sign (+) in the top right-hand corner of the screen to add a new one. On the resultant screen, specify a *Name* and optional *Description* for the new group. The *GID* or *Group Identification* number is generated automatically and there is no need to change it. Tap the right-pointing chevron (arrow) at the top of the screen.

On the next screen, tap the names of the users who are to be members of the new group. As a name is tapped, a tick appears against it. When complete, tap the right-pointing chevron at the top of the screen to continue.

On the third screen, specify which folder(s) the group will have access to. Tap the name of a folder and on the resultant screen specify whether the access is *Read Only*, *Read & Write* or *Deny Access*. When complete, tap the tick in the top right-hand corner of the screen to create the group.

4

SHARED FOLDERS

4.1 Overview

The main purpose of 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; a location to store master copies of programs, drivers, utilities and so on. These folders are referred to as *shared folders* and they reside on storage *volumes*.

The good news is that ADM has already created a number of suitable folders as part of the installation process. Additionally, some popular apps create their own shared folders when they are installed and together this may be sufficient for your purposes. But if it is not, then it is easy to create additional ones.

The default shared folder is called *Public*. In this instance, public means everyone in the household or company, not the rest of the world. The private folders for each user are known as *home folders* and are for each user to do with as they please, as what is stored in them does not affect anybody else.

The following screenshot shows the folder structure on a newly installed system as viewed using *File Explorer*, the ADM equivalent to Windows Explorer/File Explorer or the macOS Finder:

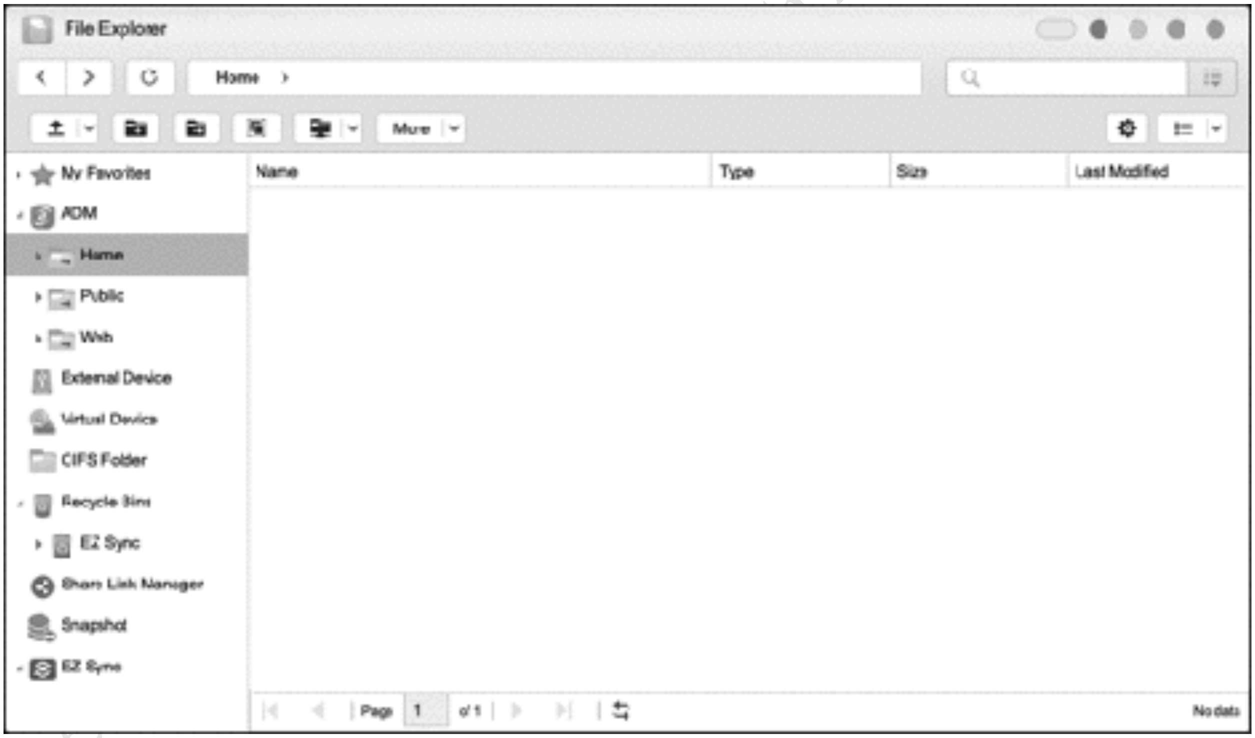
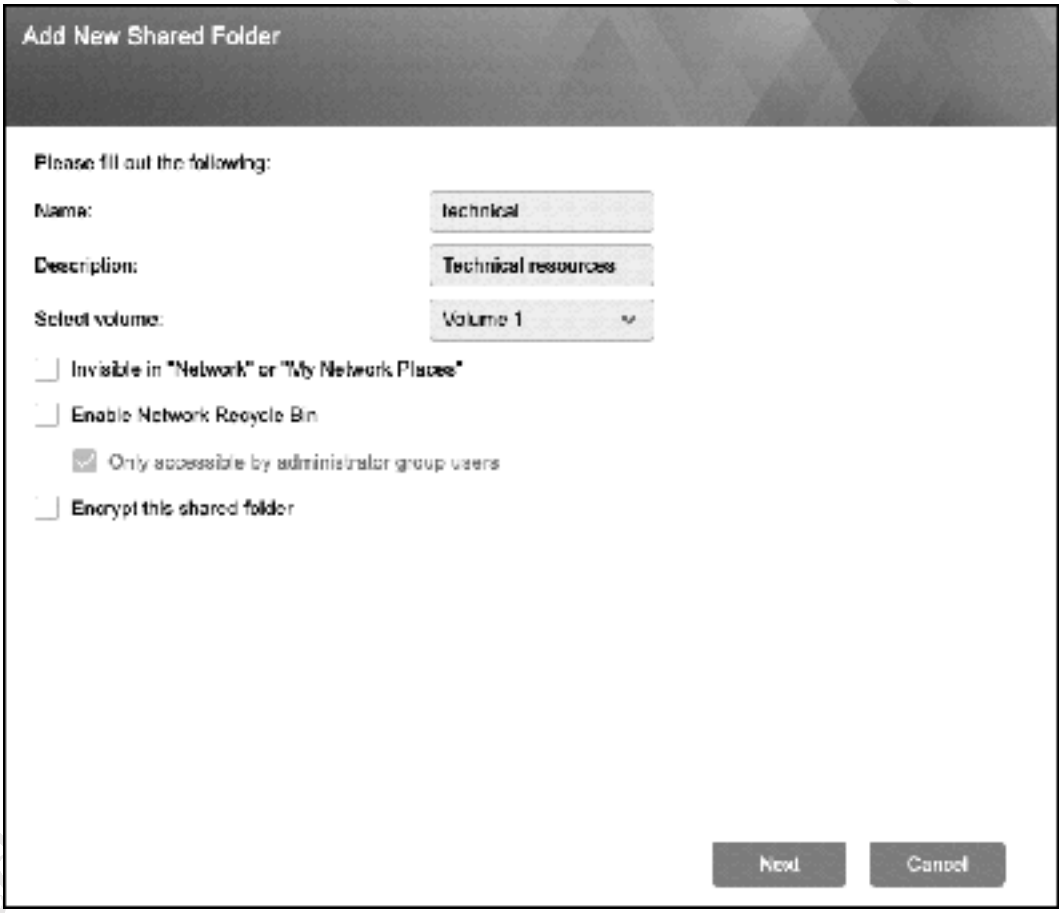


Figure 50: Default folder structure

4.2 Adding a Shared Folder

To add (create) a new shared folder, click **Preferences** > **Shared Folders**. On the **Shared Folders** tab of the screen that is displayed, click **Add**. Specify the *Name* for the folder and optionally give it a *Description*. In this example we will create a folder called *Technical* that will be used for holding utilities, documentation, log files and so on. If there is more than one disk volume in your system, choose the one you want using the dropdown. Optionally, tick the box to make the folder **Invisible in "Network" or "My Network Places"**, which can help reduce the amount of clutter on a busy system. If you want to be able to recover files that have been deleted, tick the **Enable Recycle Bin** and optionally the **Only accessible by administrator group users** boxes.

There is an option to encrypt the contents of the folder. This provides a higher level of security and if you are storing confidential information you may wish to do so, or you may need to do so to help comply with local legislation regarding data protection and privacy. Because additional considerations apply, details of this topic are discussed separately (4.6 Encrypted Shared Folders) and for now we will assume we are using a regular, unencrypted folder. Click **Next**.



Add New Shared Folder

Please fill out the following:

Name: technical

Description: Technical resources

Select volume: Volume 1

□ Invisible in "Network" or "My Network Places"

□ Enable Network Recycle Bin

☑ Only accessible by administrator group users

□ Encrypt this shared folder

Figure 51: Add a new Shared Folder

The second screen is for setting the access rights for the shared folder and there are four options:

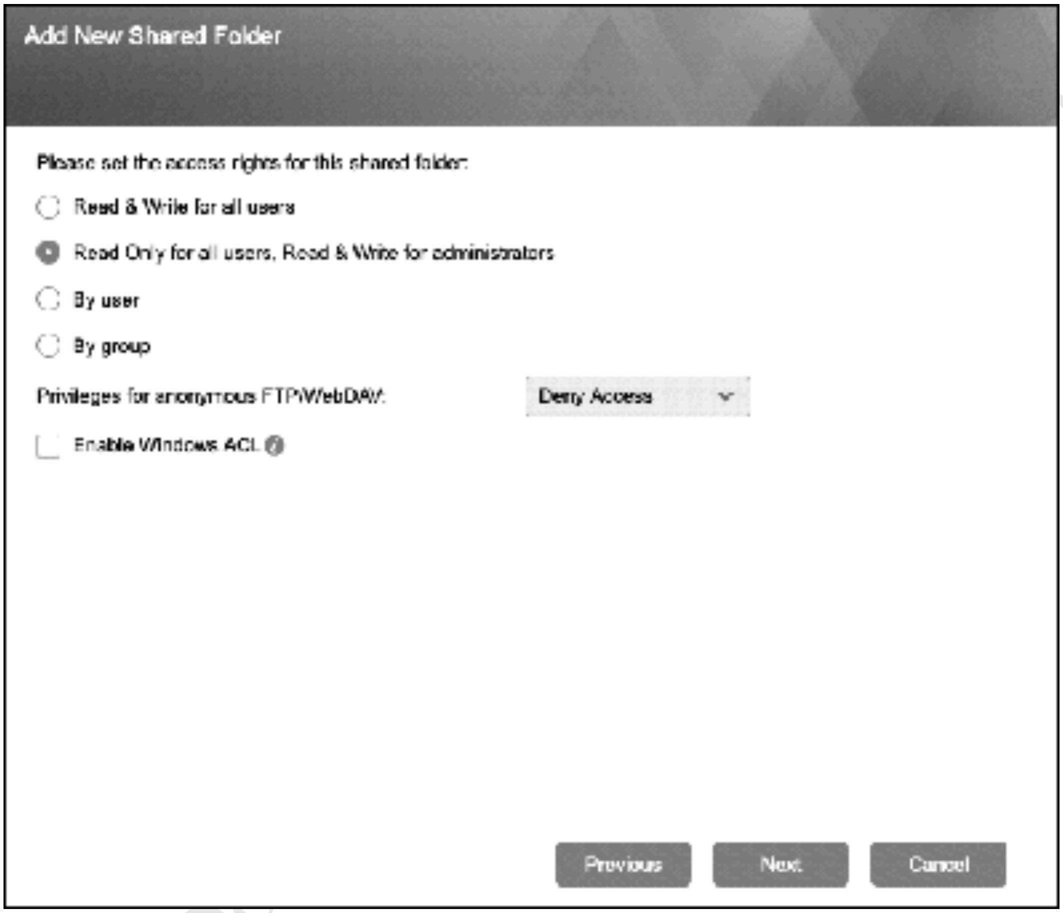
All users can be given *Read & Write* access, meaning that they have full access to items in the folder and can do as they wish.

Users can be given *Read Only* access, meaning they can access items in the folder but not update them. However, administrative users have full access, as with the previous option.

Access is restricted to a particular user or set of users.

Access is restricted to a particular group (groups are described in 3.5 User Groups).

In this example we want the admin users to have full access (so they can update it) and for regular users to have read only access (so they can retrieve items from it). Always leave *Privileges for anonymous FTP/ WebDAV* as Deny. *Enable Windows ACL* should be left unticked - this topic is discussed in 12.7 ACL (Access Control Lists). Click **Next**:



Add New Shared Folder

Please set the access rights for this shared folder:

○ Read & Write for all users

● Read Only for all users, Read & Write for administrators

○ By user

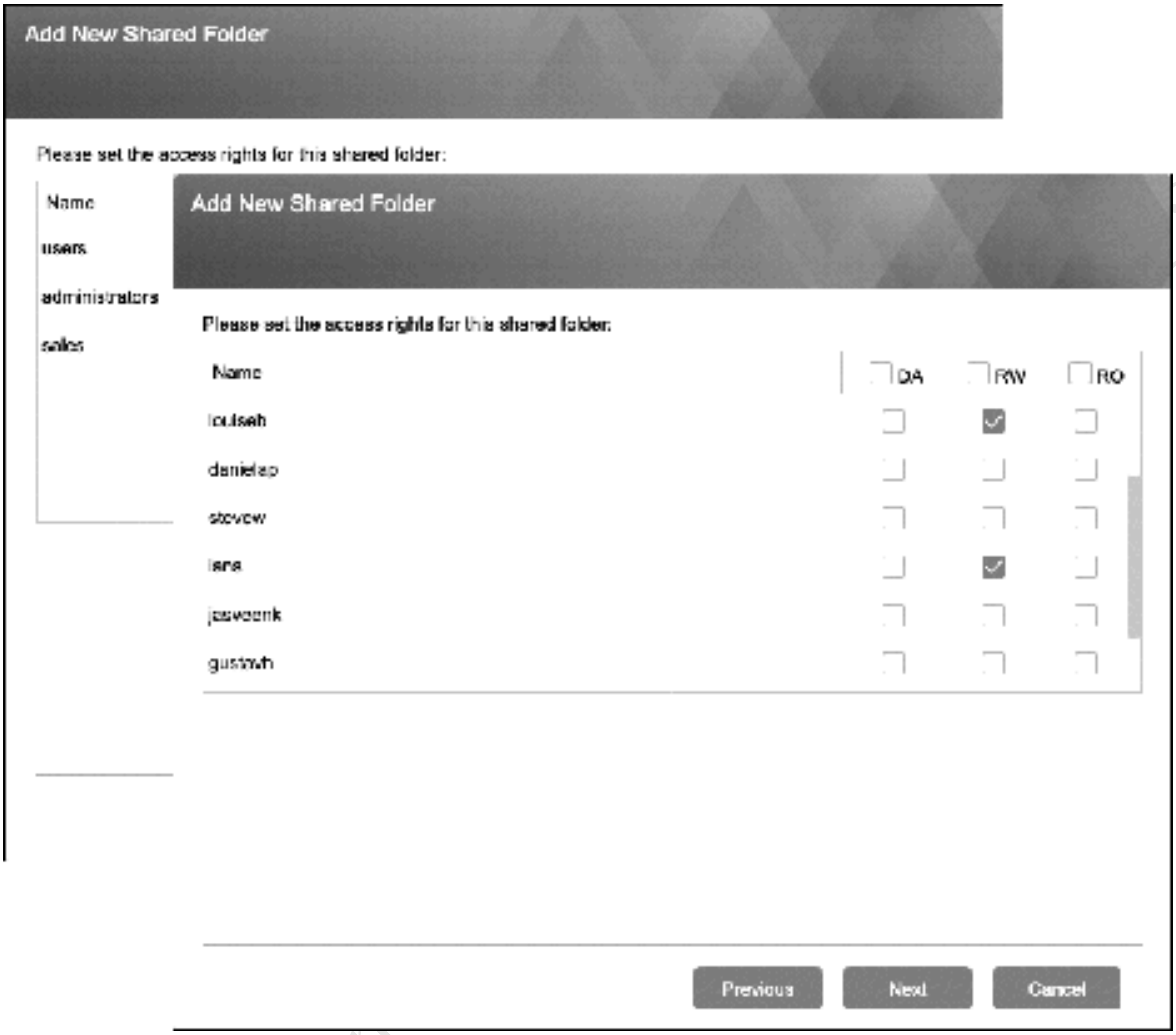
○ By group

Privileges for anonymous FTP/WebDAV: Deny Access

□ Enable Windows ACL

Figure 52: Setting the access rights for a Shared folder

If the *By user* or *By group* option is chosen, an additional screen appears in which the users or groups are specified by placing ticks in the boxes alongside their names:



Add New Shared Folder

Please set the access rights for this shared folder:

Name

users

administrators

sales

Add New Shared Folder

Please set the access rights for this shared folder:

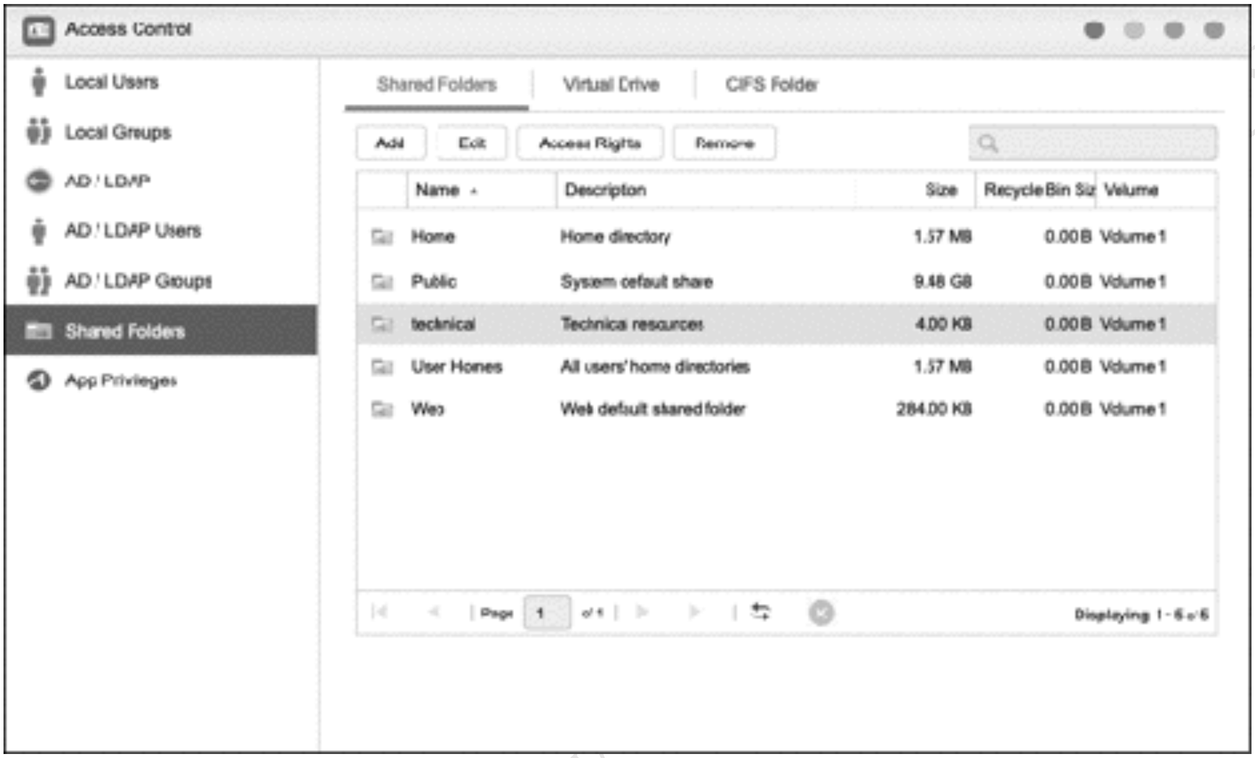
Name	□ DA	□ RW	□ RO
louiseh	□	☑	□
danielap	□	□	□
stevew	□	□	□
lisa	□	☑	□
jasveenk	□	□	□
gustavh	□	□	□

Figure 53: Setting the access rights for groups and users

A confirmation screen is displayed; click **Finish** to proceed and create the new shared folder, which will be added to the list of shared folders.

4.3 Making Changes to a Shared Folder

To make changes to any aspect of a shared folder, go to **Access Control** and click **Shared Folders** to display a list of folders:



Name	Description	Size	Recycle Bin Siz	Volume
Home	Home directory	1.57 MB	0.00 B	Volume 1
Public	System default share	9.48 GB	0.00 B	Volume 1
technical	Technical resources	4.00 KB	0.00 B	Volume 1
User Homes	All users' home directories	1.57 MB	0.00 B	Volume 1
Web	Web default shared folder	284.00 KB	0.00 B	Volume 1

Figure 54: List of shared folders

To rename, make invisible, enable the recycle bin or encrypt a folder, highlight it and click the **Edit** button.

To change the access rights (permissions) for the folder, highlight it and click the **Access Rights** button.

To delete a folder, highlight it and click the **Remove** button. There will be a confirmation message – click **OK** to continue with the deletion.

Should it ever be necessary to change a shared folder, it can only be done from **Access Control** > **Shared Folders**. Specifically, it cannot be done from *File Explorer* - this is a common mistake to be wary of.

4.4 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 files that nobody else needs access to, analogous to the '*Documents*' folder that people have on their individual computers. When a new user is created in ADM, a home folder for them is created 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 3 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.

4.5 Loading Existing Data into Shared Folders

There may be a requirement to load data from existing computers or systems onto the NAS and into the new shared folders that have been created. There are two 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 local folders to the appropriate folders on the server.

Method Two: Visit each individual computer and copy data from the user's folders to an external plug-in USB drive. Then, connect the 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 delete any unrequired and duplicate data, rather than carry it forward to the new environment.

4.6 Encrypted Shared Folders

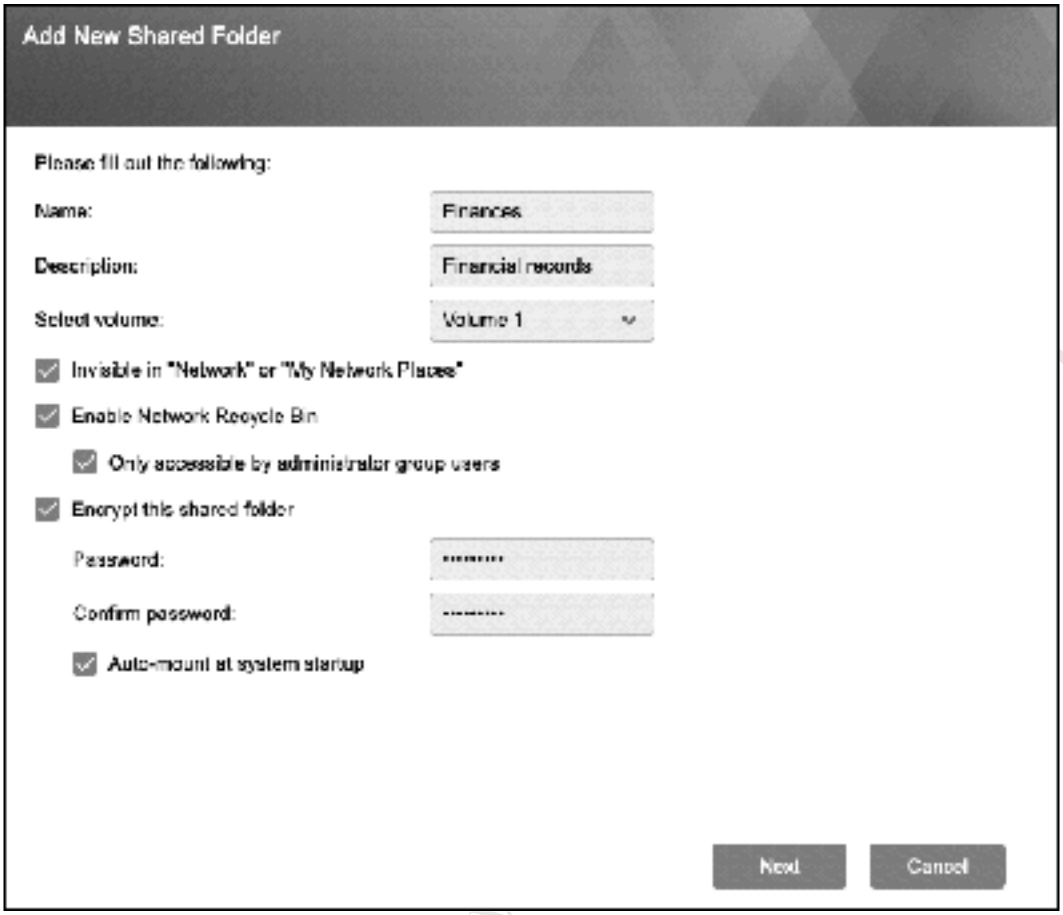
When creating a shared folder, there is the option to encrypt the contents of the folder. This provides a higher level of security when storing confidential information and, in the case of businesses, may help in compliance with local legislation regarding data protection and privacy. In the event that the disk drives were removed from the NAS 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.

The following considerations apply with encrypted folders:

- The encryption key needs to be at least 8 characters in length
- There is no way to recover the data if the encryption key is lost
- Access to encrypted folders is slower than to normal, unencrypted ones and this may be a consideration on less powerful systems
- Encrypted folders cannot be accessed by Linux/Unix machines
- The name of any file or folder within an encrypted folder must be less than 143 Latin characters or 43 Asian characters in length

To add (create) a new encrypted shared folder, click **Preferences** > **Shared Folders**. On the **Shared Folders** tab of the screen that is displayed, click **Add**. Specify the *Name* for the folder and optionally give it a *Description*. In this example we will create a folder called *Finances*. If there is more than one disk volume in your system, choose the one you want to use from the dropdown. Optionally, tick the box to make the folder **Invisible in "Network" or "My Network Places"**, which can help reduce the amount of clutter on a busy system. If you want to be able to recover files that have been deleted, tick the **Enable Recycle Bin** and optionally the **Only accessible by administrator group users** boxes.

Tick the **Encrypt this shared folder** box. A reminder message about the implications of encrypted folders is displayed – click **OK** to acknowledge it. Returning to the main panel, type in and confirm the password. A decision needs to be made about how the folder 'mounts'. If the **Auto-mount at system startup** box is ticked, the folder will automatically be made available to authorized users whenever the server boots. If it is left unticked, the folder will need to be manually mounted by *admin* each time the server starts.



Add New Shared Folder

Please fill out the following:

Name: Finances

Description: Financial records

Select volume: Volume 1

☑ Invisible in "Network" or "My Network Places"

☑ Enable Network Recycle Bin

☑ Only accessible by administrator group users

☑ Encrypt this shared folder

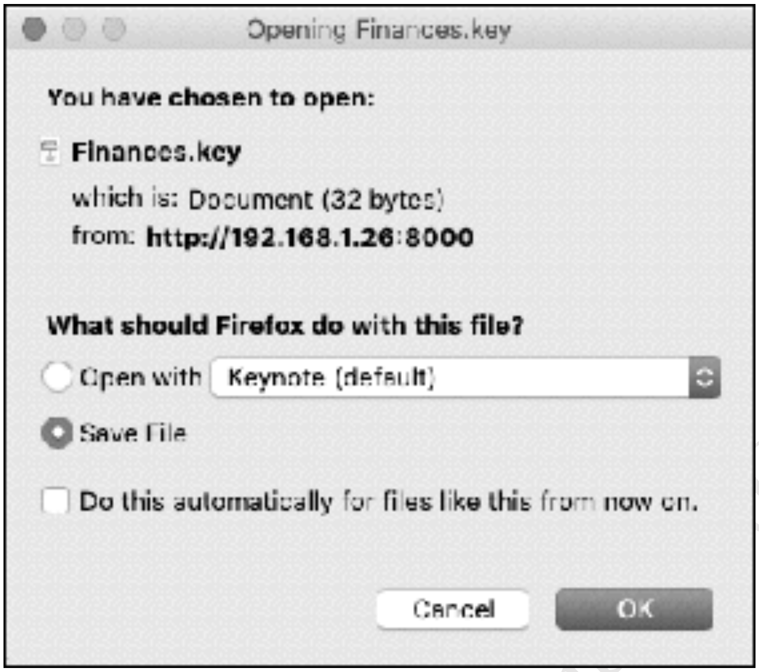
Password: ••••••••••

Confirm password: ••••••••••

☑ Auto-mount at system startup

Figure 55: Adding a new encrypted shared folder

Click **Next**. Specify the access rights for the folder, as described in section 4.2 Adding a Shared Folder. Accept the confirmation screen. You will be prompted to save a copy of the key i.e. a file containing a copy of the encryption password and the format of this message may vary, depending on what browser you are using. Keep the key in a safe place, for instance on a USB key which is kept in a drawer or safe. If the password is ever forgotten, the key file can be used to restore access to the folder.


Opening Finances.key

You have chosen to open:

Finances.key

which is: Document (32 bytes)

from: http://192.168.1.26:8000

What should Firefox do with this file?

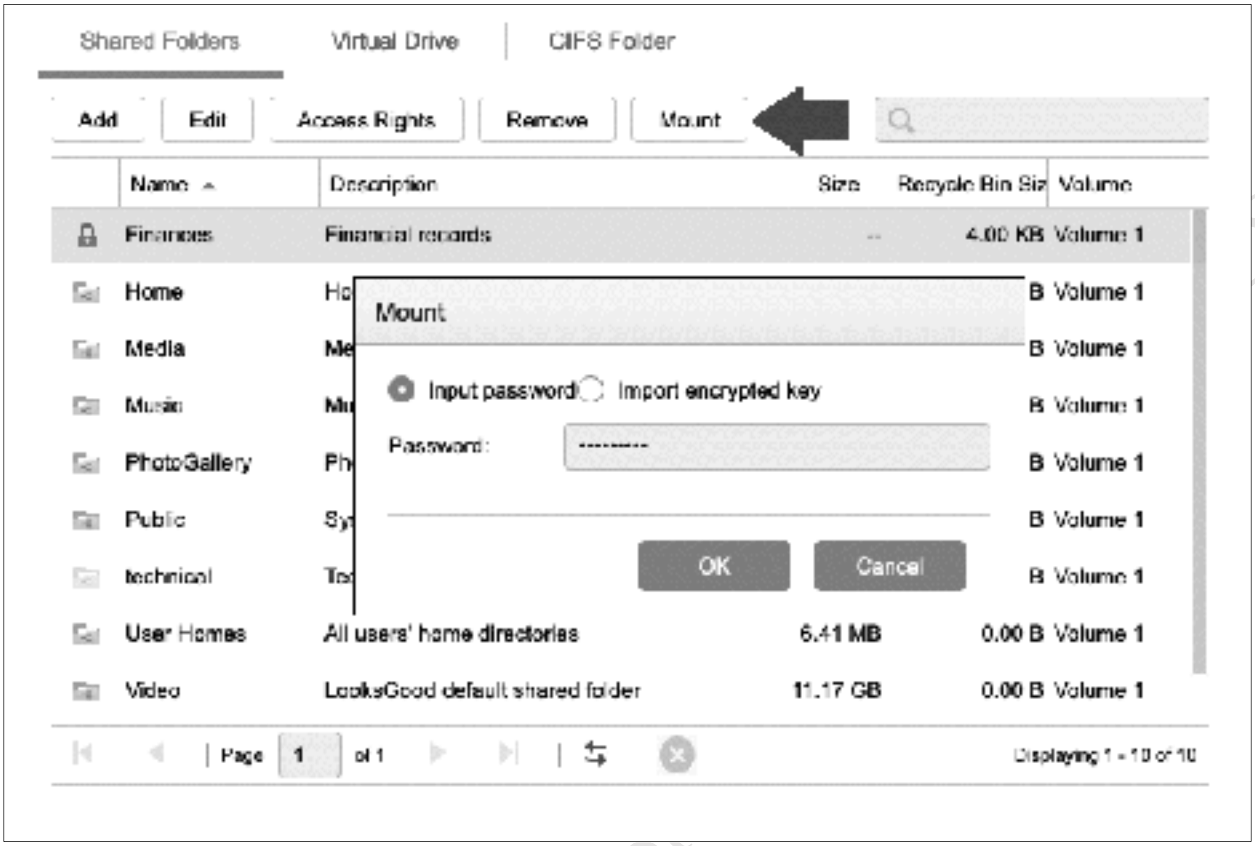
○ Open with Keynote (default)

● Save File

□ Do this automatically for files like this from now on.

Figure 56: Save the key to a safe location

The encrypted folder has now been created. If auto-mount was selected, it will be available next time the server restarts. If auto-mount was not selected, it will need to be mounted manually. To do this, click **Preferences** > **Shared Folders**. The encrypted folder will have a closed padlock against it, showing that it is locked i.e. unmounted. Highlight the folder, click the **Mount** button and enter the password when prompted (or, you could choose to load a file copy of it), click **OK**. The padlock will open, showing that the folder is now mounted and available.



	Name	Description	Size	Recycle Bin Siz	Volume
	Finances	Financial records	--	4.00 KB	Volume 1
	Home	Ho		B	Volume 1
	Media	Me		B	Volume 1
	Music	Mu		B	Volume 1
	PhotoGallery	Ph		B	Volume 1
	Public	Sy		B	Volume 1
	technical	Te		B	Volume 1
	User Homes	All users' home directories	6.41 MB	0.00 B	Volume 1
	Video	LooksGood default shared folder	11.17 GB	0.00 B	Volume 1

Mount

● Input password ○ Import encrypted key

Password: ---------

Figure 57: Mounted an encrypted folder

5

ACCESSING THE SERVER

5.1 Overview

There are multiple methods for accessing the NAS; some of these are available to Windows users only, some to Mac users only, whereas others are available for multiple platforms. There are also specific apps available for portable devices such as smartphones and tablets.

5.2 Using a Browser and File Explorer

This is the universal method for accessing the NAS and works for Windows PCs, Macs, Linux computers and Chromebooks. Using any computer on the local network, launch a browser such as Firefox, Chrome or Safari and type in the name of the server ("*server*" in our example) or its IP address. The standard ADM login screen is displayed; the user should enter their name and password and they will be presented with a minimalist Desktop; in essence, all they can access is *File Explorer*, *EZ Sync Manager* and *Online Help* (unless additional options have been granted to them).

Within *File Explorer* they can see the folders and files that belong to them or to which they have been granted access, such as their *home* folder plus the *multimedia* and *public* folders. To work with a file or folder, right-click it and a pop-up menu will appear with the available options. Alternatively, use the icons at the top of the screen and the commands available from the dropdown menu:

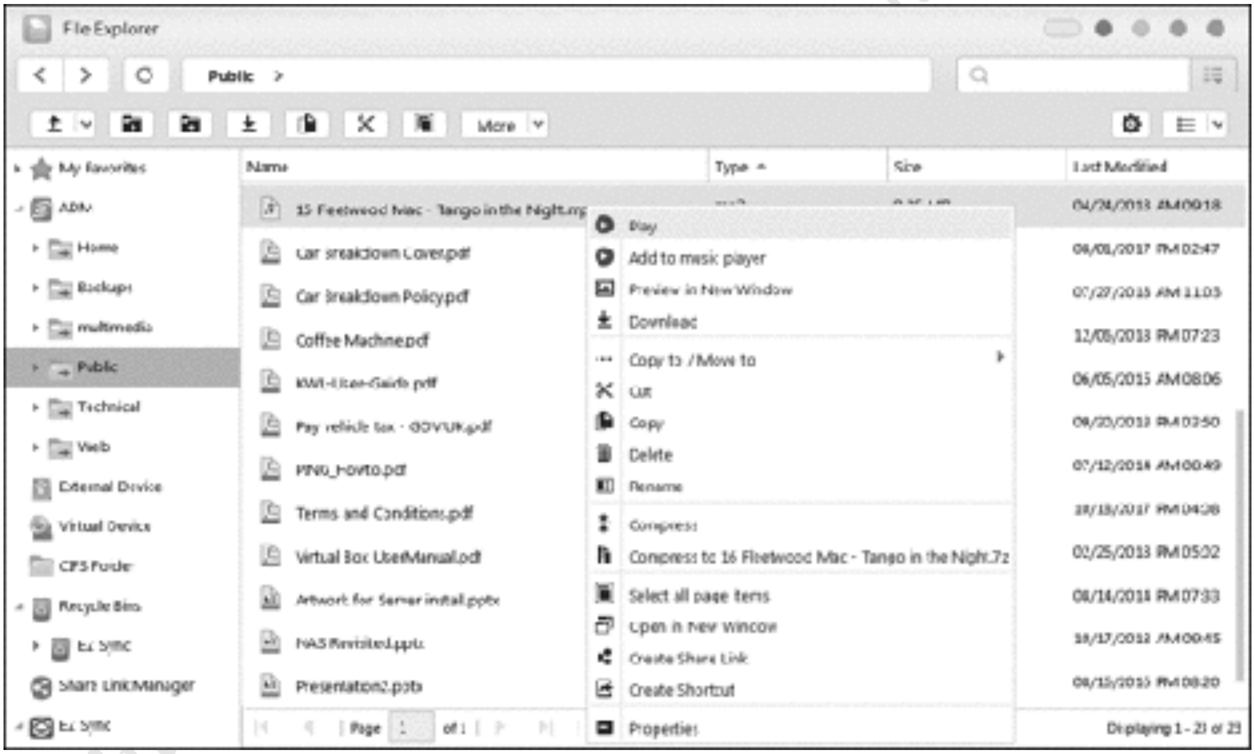


Figure 58: Working with File Explorer

There are options to upload and download files, copy and delete them, create new folders and so on. To edit a file, choose the **Download** option to first download it to the local computer, make the changes to the document using Word, Excel or other preferred application, then use the **Upload** button in File Explorer to return the new version back to the server. Many graphic files and photographs can be viewed by double-clicking them and MP3 music files can also be played directly.

When the user has finished, they should logoff. This is done by clicking their user name in the top right-corner of the screen and choosing the **Sign out** option:

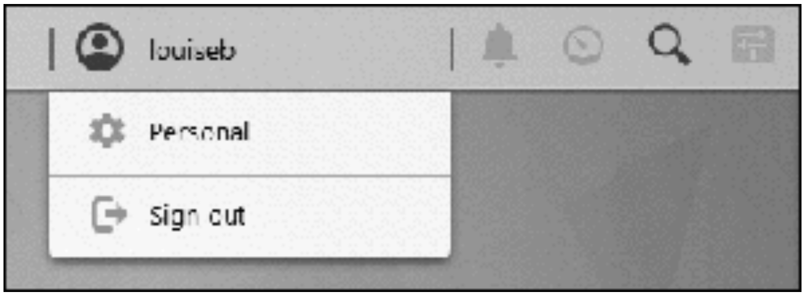


Figure 59: User Options menu

5.3 Connecting Windows Computers

Using Windows Explorer/File Explorer

A simple way to access the server is by going into Windows Explorer/File Explorer, which is on the taskbar in most 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, although you may be prompted to first enter a 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.

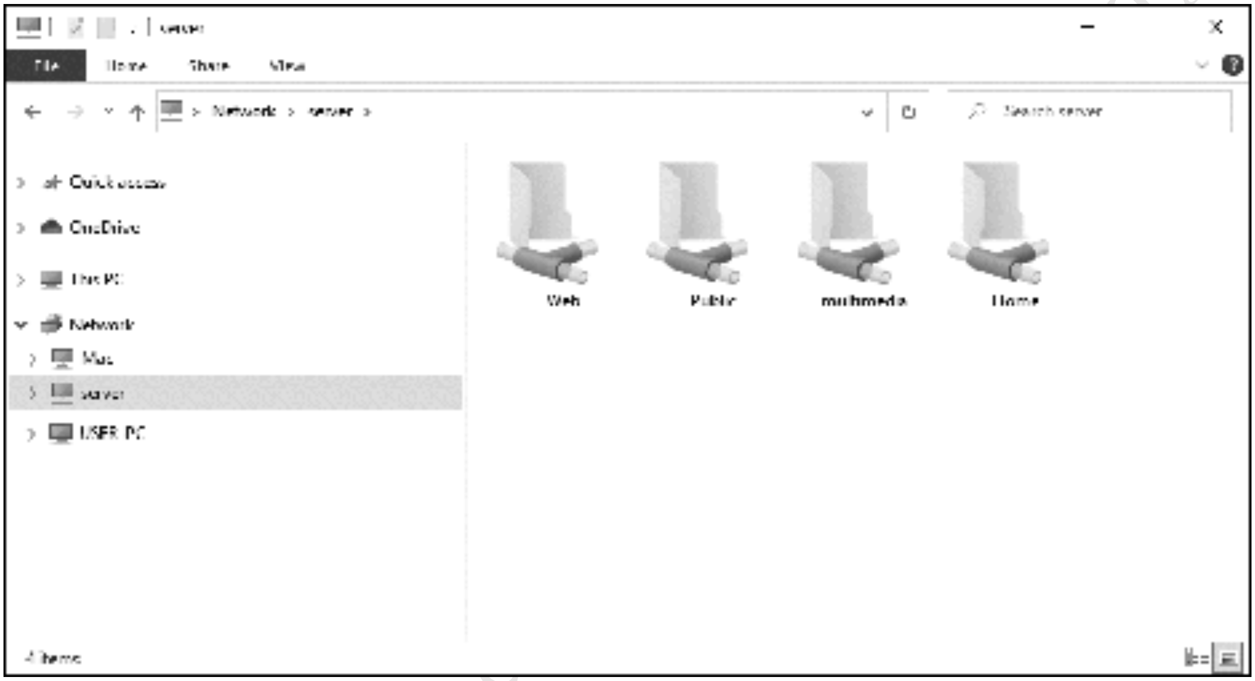
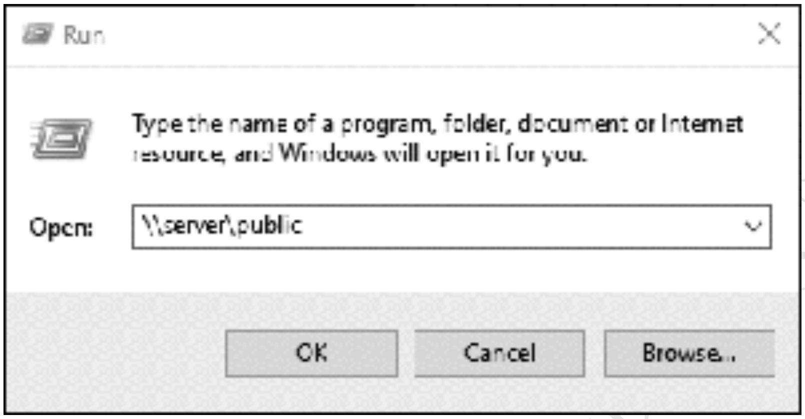


Figure 60: List of shared folders from Windows Explorer/File Explorer

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

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 your username and password, as defined previously on the server:



Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

Open: \\server\public

Figure 61: Accessing a shared folder using Windows Run command

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

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\foldername*. 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. Note: you may be prompted to enter a valid user name and password as previously defined on the server. If you wish, tick the option box to remember the login details, although you should only do this if you are the sole user of the computer. Right-click 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**:

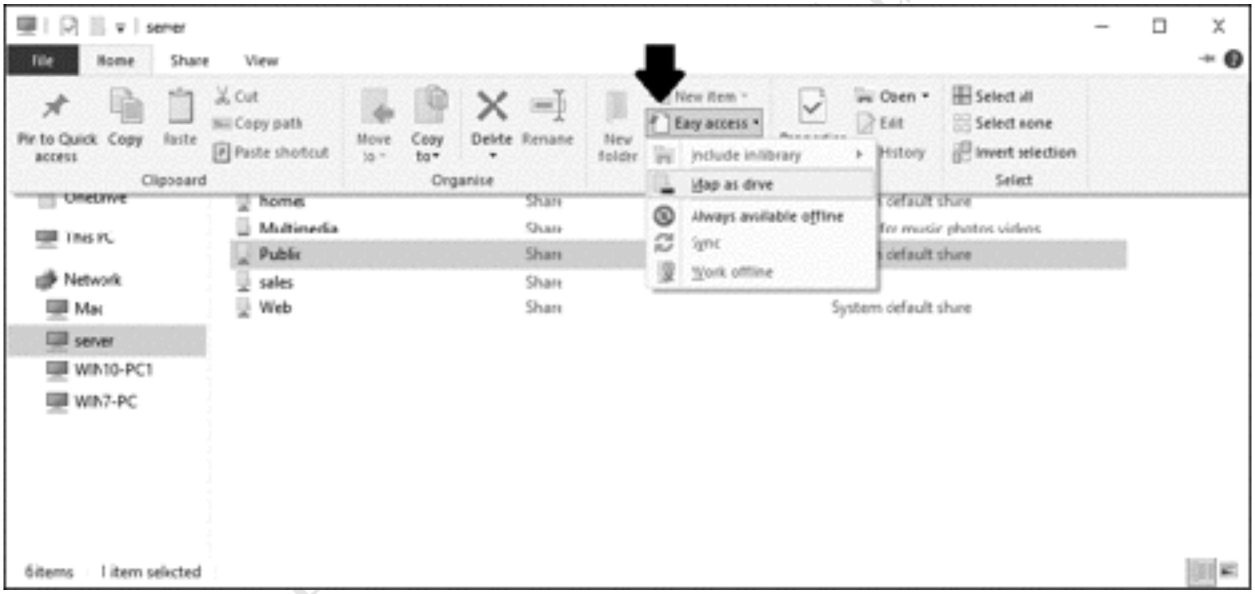


Figure 62: Mapping a drive in Windows 10

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

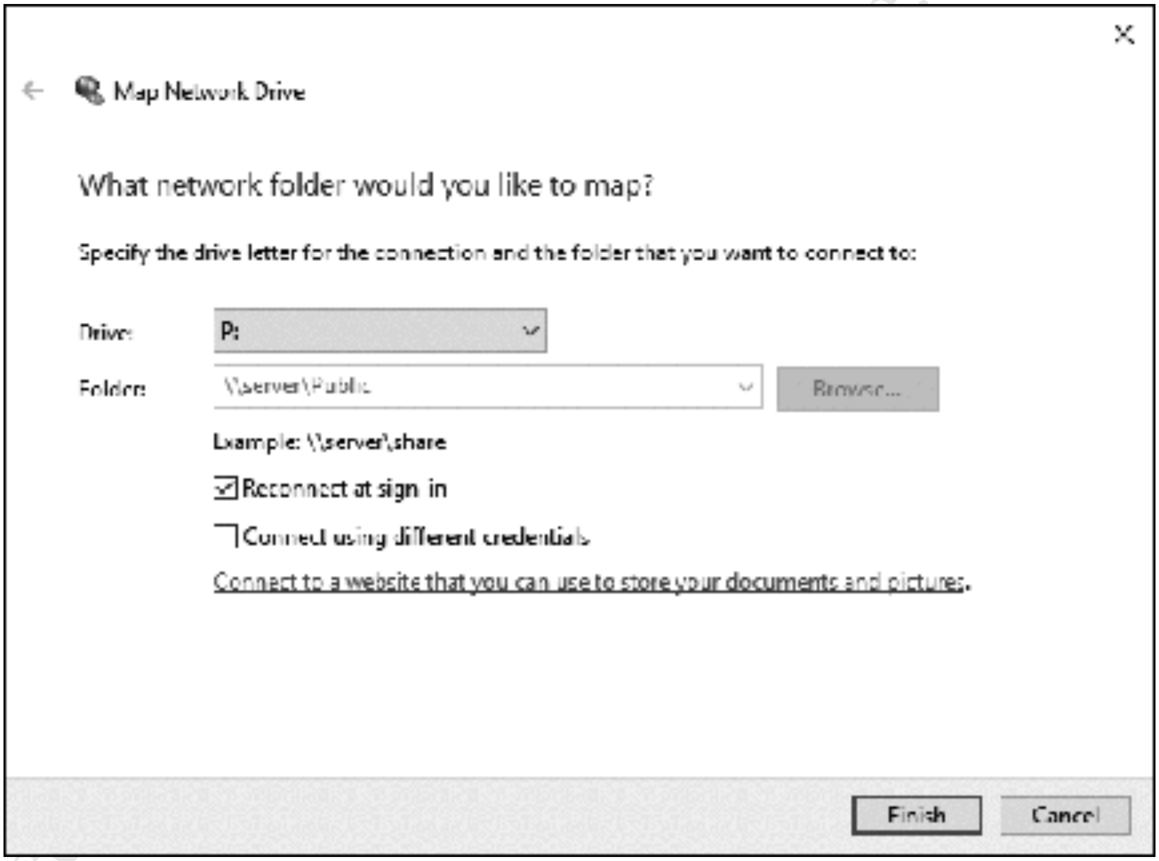
If using Windows Vista, run Windows Explorer by clicking **Start** > **All Programs** > **Accessories** > **Windows Explorer**, else click Computer on the **Start** menu. If the menu bar is not displayed, click **Organize** > **Layout** > **Menu bar** to display it. From the Menu bar choose **Tools**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



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: P:

Folder: \\server\Public

Example: \\server\share

☑ Reconnect at sign in

□ Connect using different credentials

Connect to a website that you can use to store your documents and pictures.

Figure 63: Mapping a drive

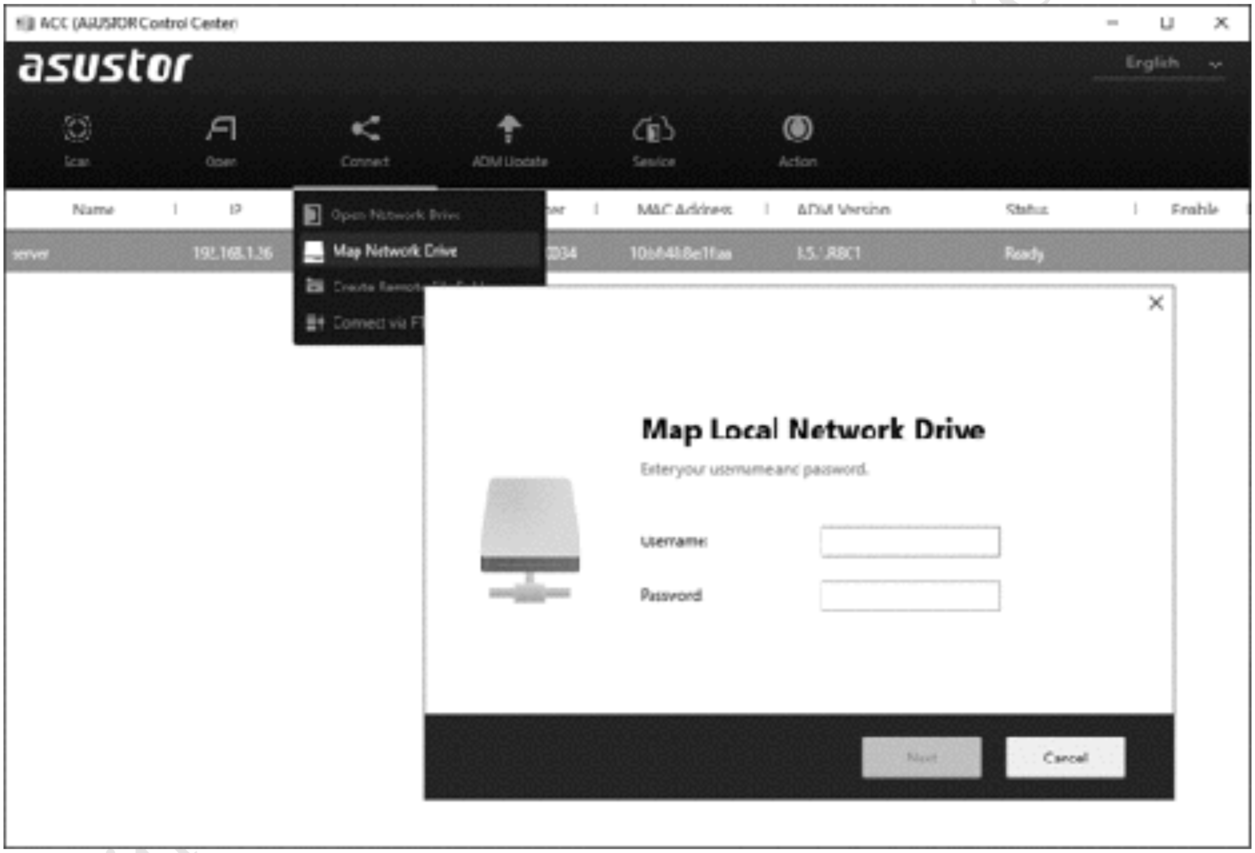
Upon a successful connection, the contents of the newly mapped drive will be displayed. The process now needs to be repeated for each folder that the user requires access to.

Note that you can use whatever drive letters you wish, as long as they are not already in use; for instance, you cannot map C as that is always in use on a computer. However, using logical letters makes things easier. For example, map *home* to H, *public* to P and so on.

Using ASUSTOR Control Center (Windows)

ASUSTOR Control Center utility (ACC) is used when initially setting up a NAS from a desktop computer, but is a flexible piece of software that does other things as well, one of which is mapping drives. One advantage of using it is consistency; when drives are mapped manually in Windows as described in a previous section, there are small variations in the process depending on which version of Windows is being used. However, by using *ACC* it is always the same process regardless of the Windows version.

Download and install *ACC* onto each computer. If you receive a message from the computer's firewall, grant access to *ACC*. An icon will be in placed on the computer's desktop – double-click to run it. The server should be listed, although *ACC* may take a few seconds to find it. If it does not appear then there is a problem of some sort, such as: computer not connected to network; NAS not powered on; firewall needs configuring on computer. Click **Connect** followed by **Map Network Drive**, enter a user name and password as previously defined on the server and click **Next**:



Map Local Network Drive

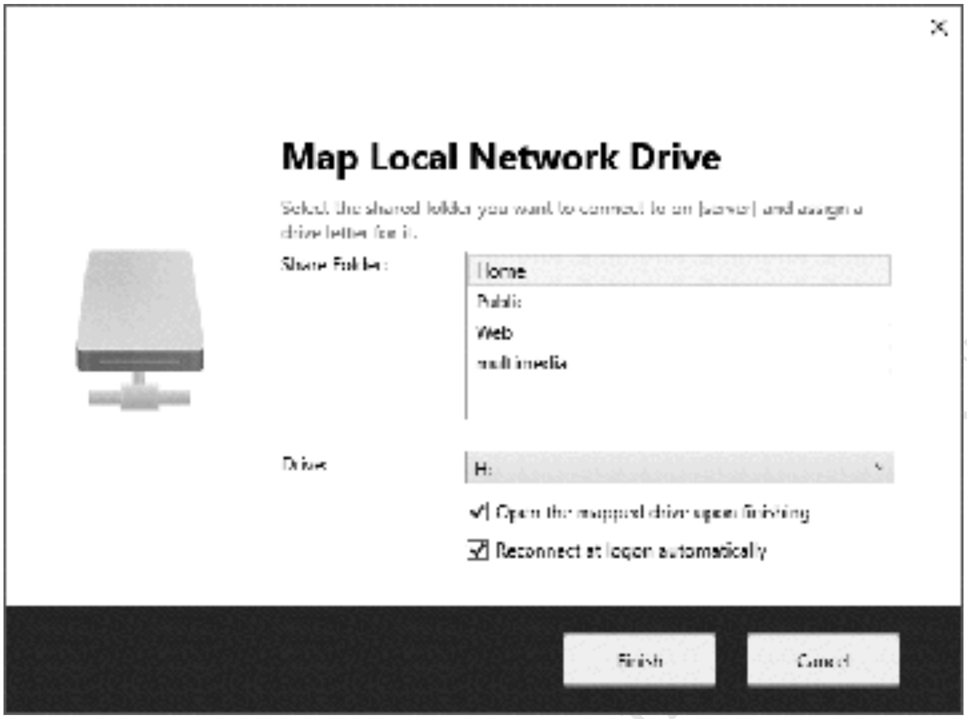
Enter your username and password.

Username:

Password:

Figure 64: Mapping a network drive using ACC

On the following panel, highlight a folder and choose a drive letter for the folder using the dropdown. You can use whatever drive letters you wish, as long as they are not already in use (for instance you cannot use C as that is always in use on a Windows computer). However, using logical letters makes things easier. For example, map *public* to P and *home* to H. If the computer is only ever used by one person you can tick the **Reconnect at logon automatically** box, then click **Finish**:



Map Local Network Drive

Select the shared folder you want to connect to on [server] and assign a drive letter for it.

Share Folder: Home

- Home
- Public
- Web
- multimedia

Drive: H:

☑ Open the mapped drive upon finishing

☑ Reconnect at logon automatically

Figure 65: Mapping a network drive

Repeat the process for as many times as is necessary to provide access to all the desired folders. When complete, close *ACC.* The drive mappings are permanent, assuming the **Reconnect at logon** box was ticked, and will survive reboots. It is not necessary to run *ACC* again unless it is required to make changes to the mappings.

Using a Batch File (Windows)

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 possibly more applicable to a small business or educational environment rather than to a home system. Start off by using Notepad or WordPad to create a plain text file called *Connect-to-NAS.cmd*. The contents of the file will vary depending on the folders to be mapped. 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
: map the drives
net use h: \\server\home /persistent:no
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 each 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. After the user has successfully entered their details, the mapped drives will be available until the computer is shutdown or they logoff from 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 NAS is not available, the drives cannot be mapped and a warning message is displayed. It is to be expected that this message will appear if using, say, a laptop computer outside of an office, but if it appears when inside then it indicates a problem. This could be a connectivity issue on the computer e.g. Ethernet cable unplugged or wireless switched off. If everyone in the office is receiving it then it would suggest that the server is powered off or otherwise out of action.

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

Ideally, computers should be setup with only one Windows user defined on them. If this is not the case, then the *Connect-to-NAS.cmd* file needs to be placed where it will appear on the Desktop for all users:

Windows XP: C:\Documents and Settings\All Users\Desktop

Windows 10, 8.1/8, 7, Vista: C:\Users\Public\Public Desktop

Note that 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 used. To do this, go to **Control Panel** on the computer and choose **Folder Options** or **File Explorer Options** depending on your version of Windows. Click on the **View** tab, enable **Show hidden files, folders and drives** and click **OK**.

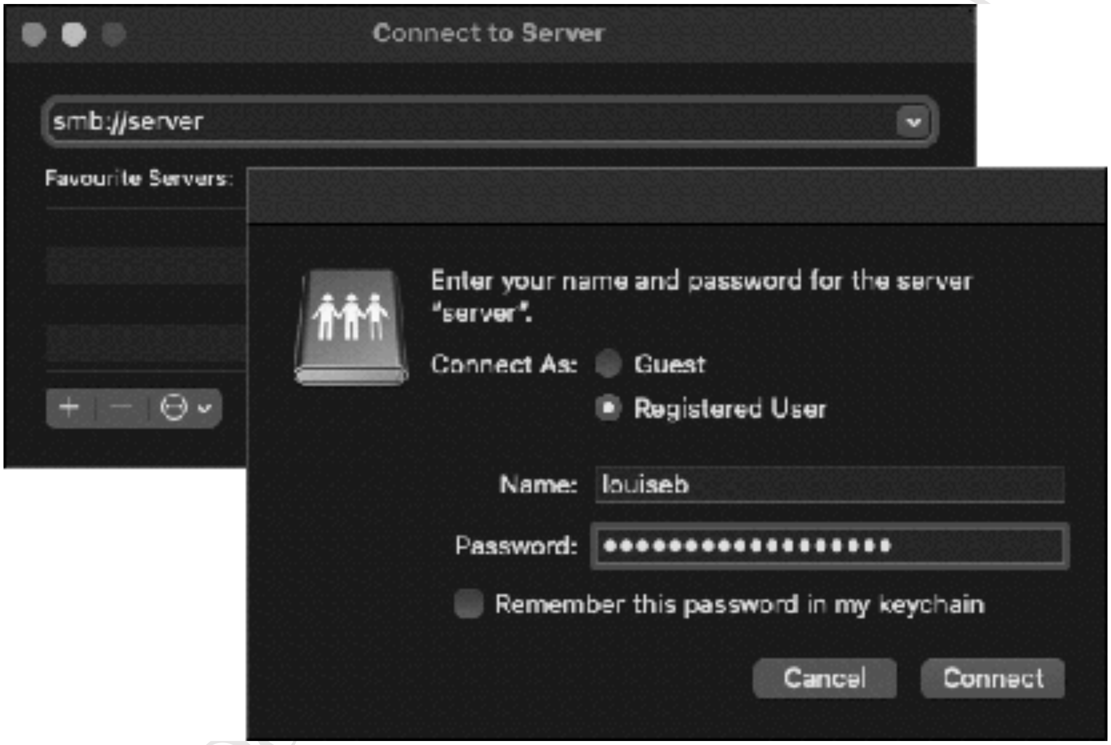
Copy the *Connect-to-NAS.cmd* file to the Public Desktop folder, then make the Public Desktop folder hidden again.

Unfortunately, *Connect-to-NAS.cmd* is not very tolerant 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 various iterations of the Mac operating system, with some minor differences between them, but the following technique should work with all versions. If you are using older versions of macOS (before 10.9 Mavericks), you should check that the Mac File Service (AFP) is enabled on the NAS, as described in section 2.10 File Services.

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:



smb://server

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

Connect As: ○ Guest
● Registered User

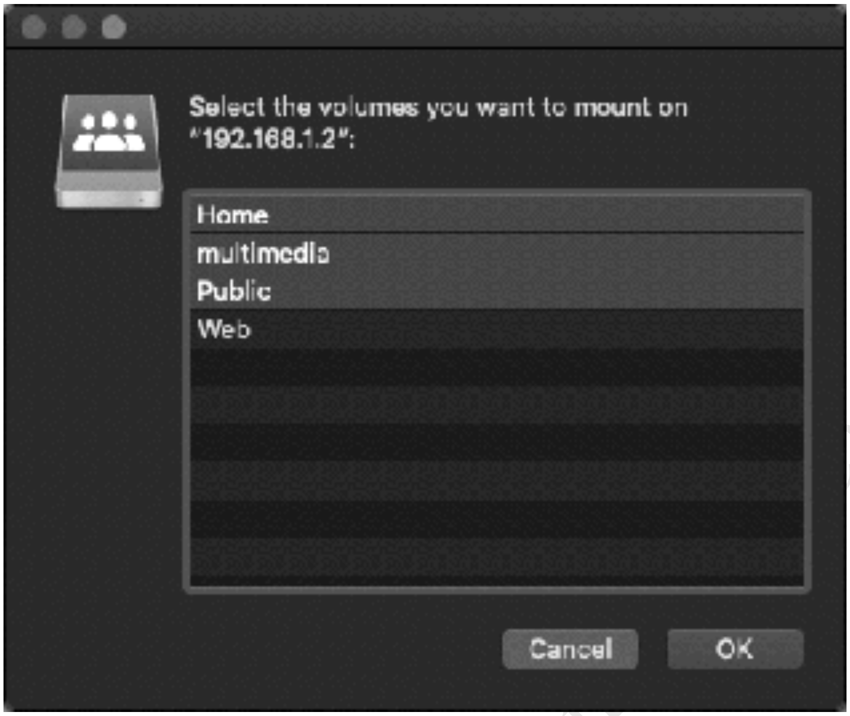
Name: louiseb

Password: ••••••••••••••••••

□ Remember this password in my keychain

Figure 66: Enter the user name and password

A list of available shared folders (*volumes)* is displayed. Choose the volume to mount and click **OK.** To mount multiple volumes at once, hold down the **Command key** and click on the required folders in turn:


Select the volumes you want to mount on "192.168.1.2":

Home
multimedia
Public
Web

Figure 67: Select the volume(s) to mount

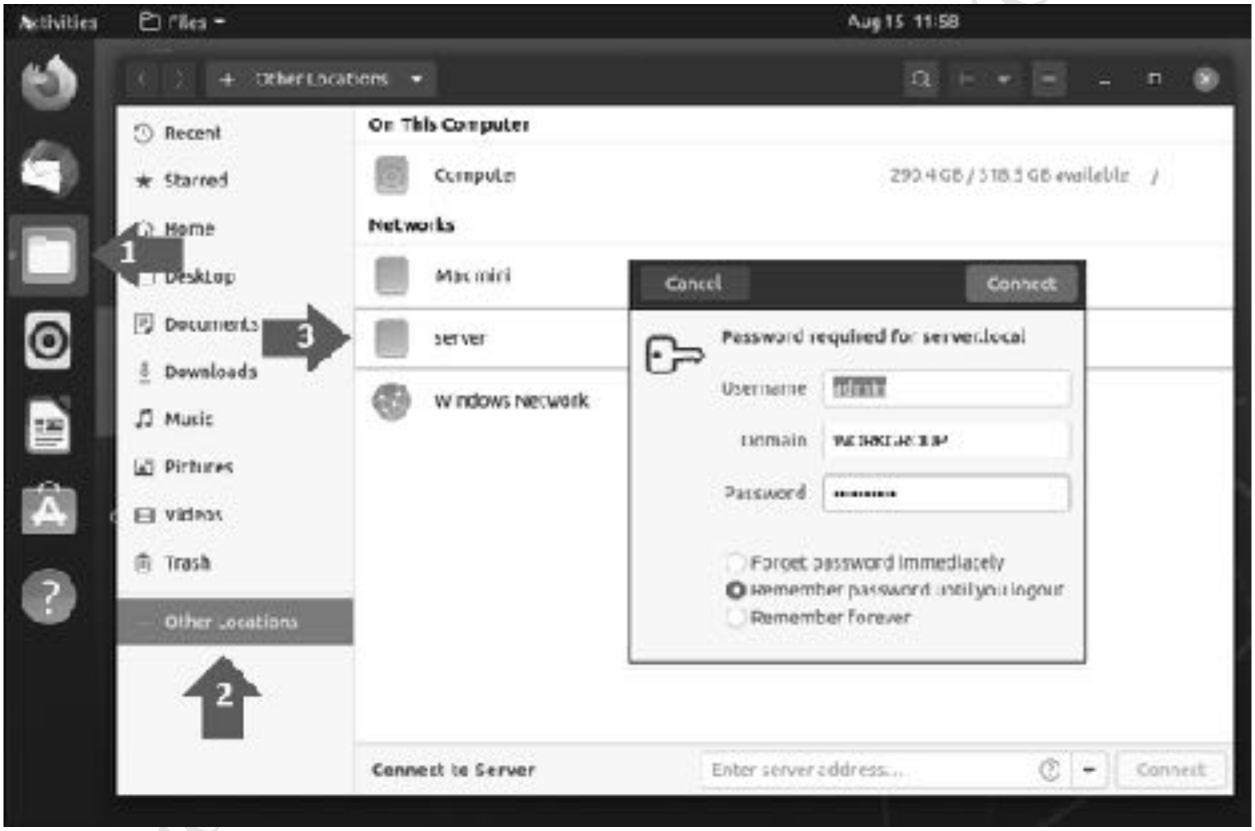
Icon(s) for the folder(s) will appear on the Desktop, assuming you have set Preferences in Finder to show Connected Servers. Click an icon to display the contents - they behave exactly the same as standard Mac folders.

Alternatively, click Finder and navigate to the server in Locations, click the **Connect As** button and then login and mount one or more volumes/shared folders.

5.5 Connecting Linux Computers

Although ADM includes comprehensive support for the NFS filing system used by Linux and UNIX computers (see 2.10 File Services), most Linux distributions include support for the SMB filing system used by ADM. 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 the popular Ubuntu Linux distribution.

Click on the **Files** icon in Ubuntu, 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 previously 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.



Password required for server.local

Username [redacted]

Domain WORKGROUP

Password ••••••••

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

Figure 68: Enter the address of the server

5.6 Connecting Smartphones and Tablets

Mobile devices such as smartphones and tablets are connected to ASUSTOR servers using apps, available for download from the Apple and Google app stores. Many of the apps are specific to playing certain media types or have specialist purposes; the two discussed here are more generic methods for accessing the file system on the server.

AiData

AiData is from ASUSTOR and is available for iOS and Android. It is used for browsing and managing files and shared folders. Common file formats can be viewed, plus graphics and photos, and music files can be played. There are commands to copy, rename, move files and so on. As such, it is an ideal ‘universal’ app for many users.

When running AiData for the first time, tap the plus (+) sign in the top left-hand corner of the screen and enter the details of the server. If you are connected locally you can let the app find your server on the network via Auto Discovery, else manually specify the name or IP address. If you also want to be able to use AiData remotely you should enter your Cloud ID, which you may have registered during the installation of ADM, else see section 10.2 Setting up EZ-Connect for how to do so. It is suggested that you flip the HTTPS switch to the ‘On’ position to improve security.

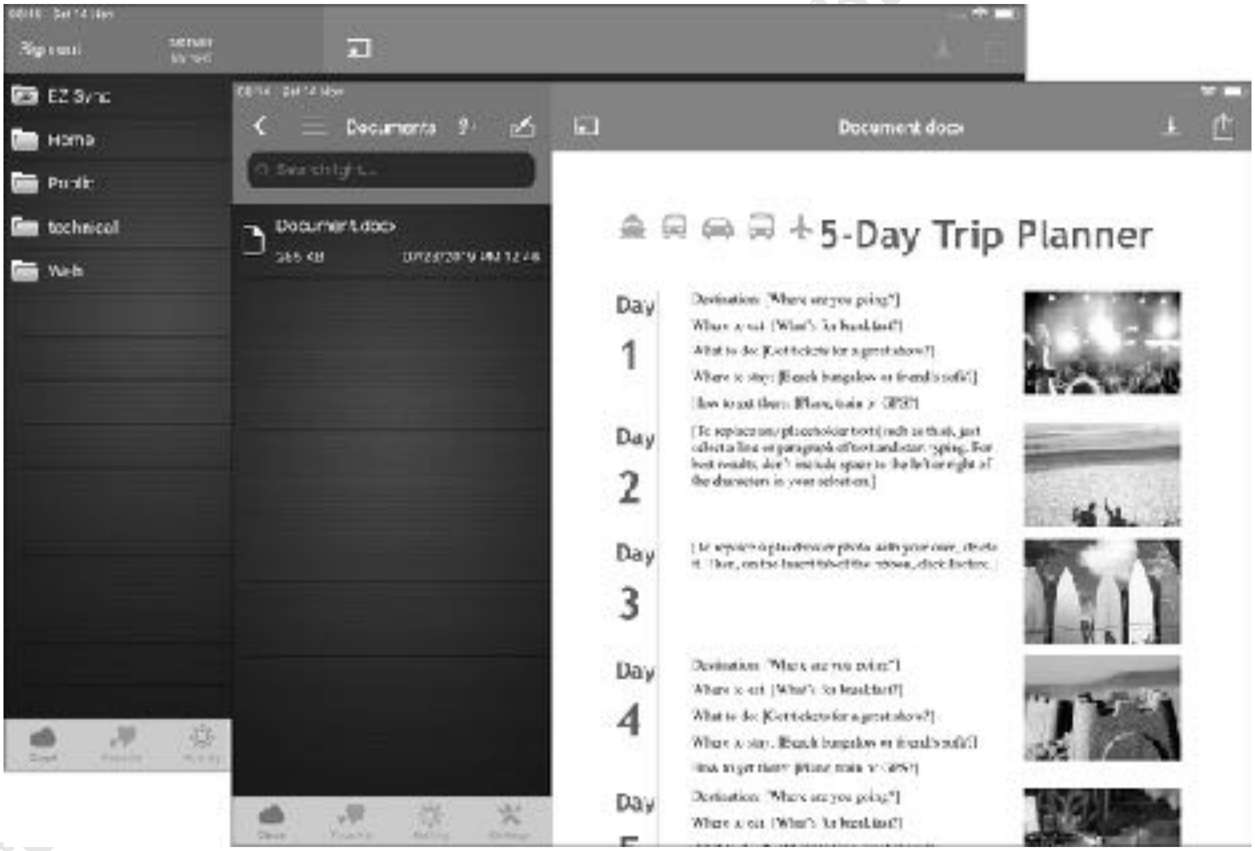


Figure 69: AiData running on iPad

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**:

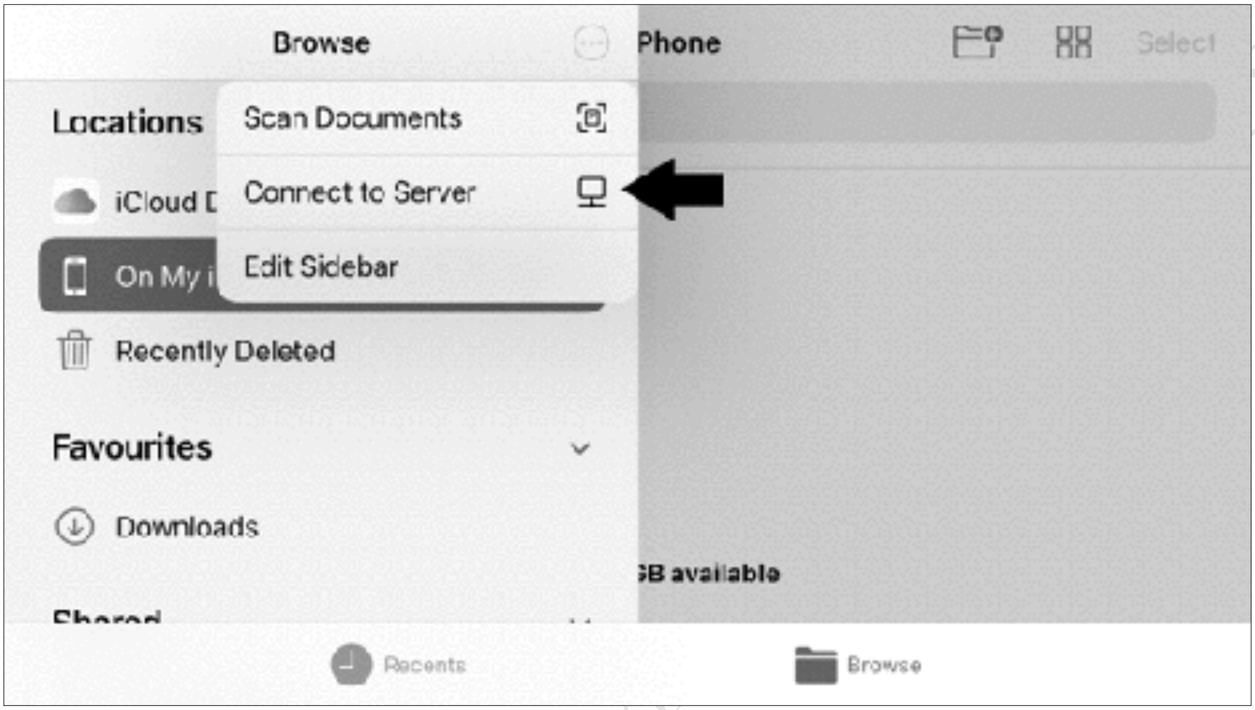
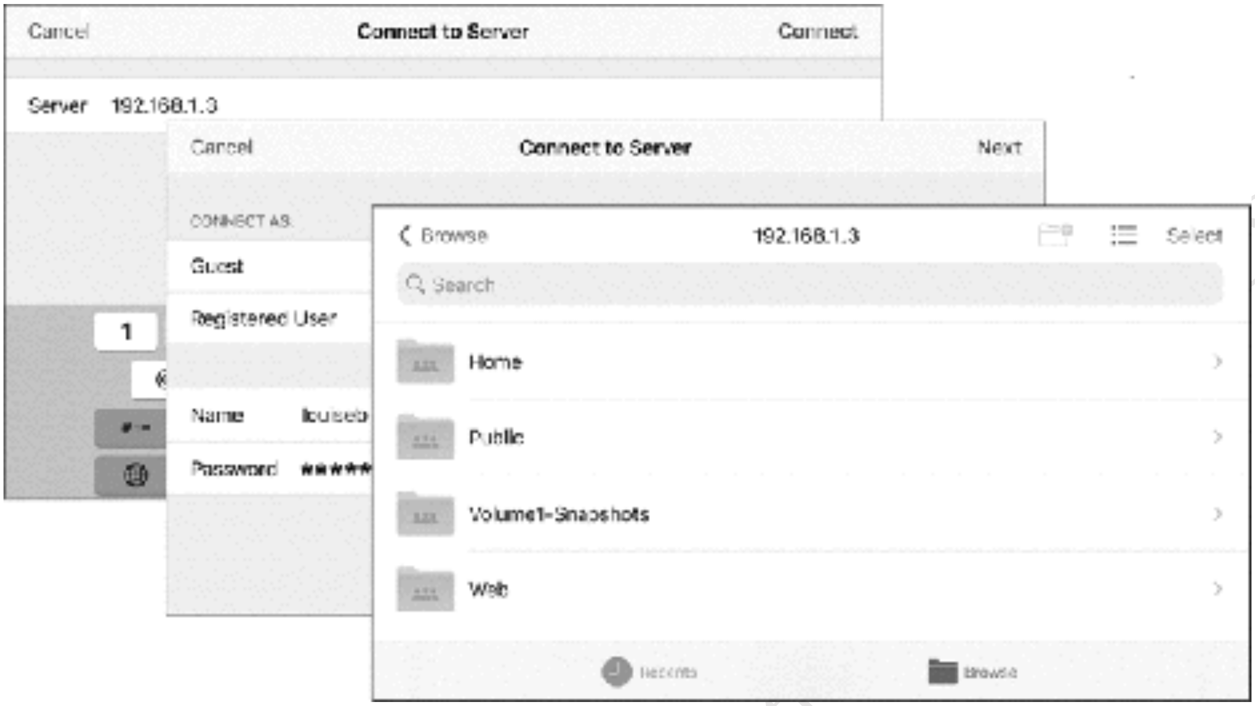


Figure 70: File App on iPhone/iOS

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:



Server 192.168.1.3

Name louiseb

Password *****

Figure 71: Connecting to and viewing files and folders on the server

5.7 Connecting Chromebooks

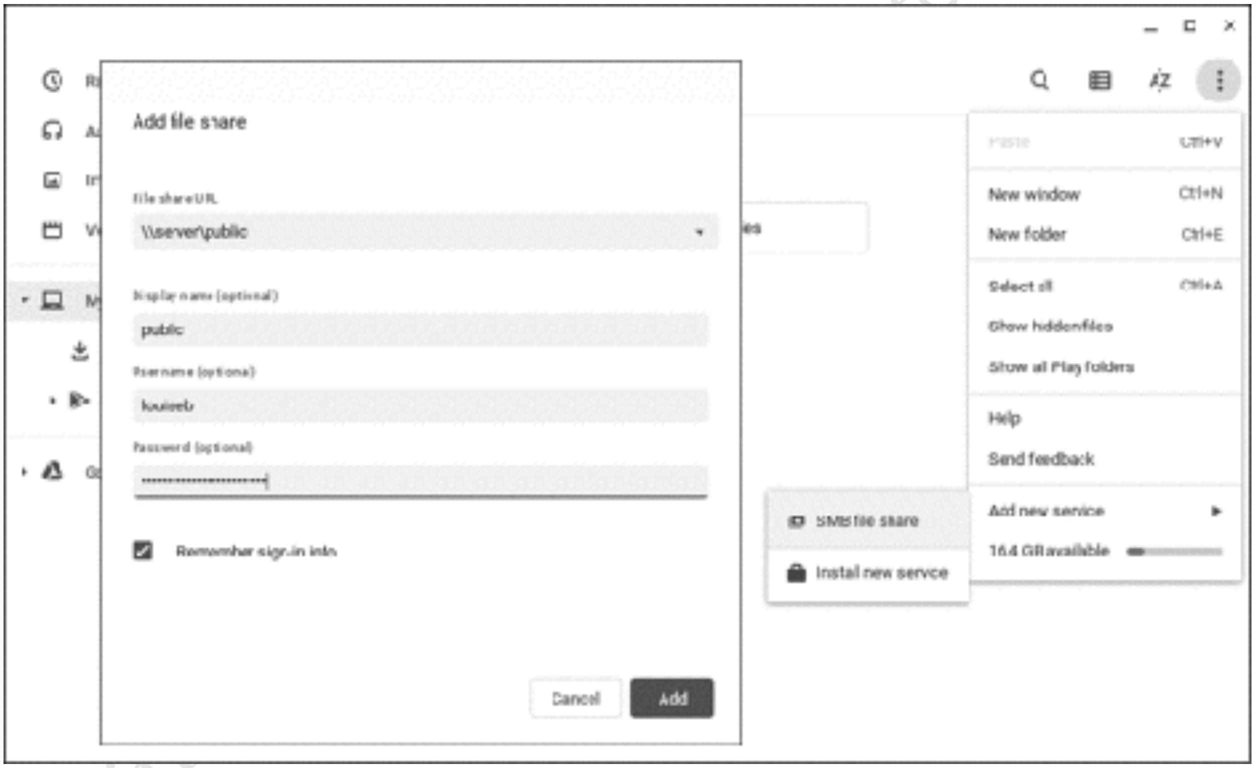
Chromebooks are a popular computing choice, particularly in education. In essence a Chromebook is a laptop that primarily runs Google's Chrome browser and the underlying operating system is minimalist compared to Windows or macOS. However, Chromebooks work well with NAS and can be used in the following ways:

Browser

Using the browser, as described earlier in section 5.2 Using a Browser and File Explorer, for tasks such as working with File Station, playing back music using its audio player, downloading and uploading files and administering ADM.

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.



Add file share

File share URL: \\server\public

Display name (optional): public

Username (optional): louiseb

Password (optional): ••••••••••••••••••••••

☑ Remember sign-in info

Figure 72: Adding a file share

Android Apps

As Chromebooks can run Android Apps from the Play Store, this means that many of ASUStor's mobile apps are available, such as the multimedia apps of AiMusic (see 9.3 SoundsGood), AiVideos (see 9.4 LooksGood) and AiFoto3 (9.5 Photo Gallery 3).

6

SECURITY

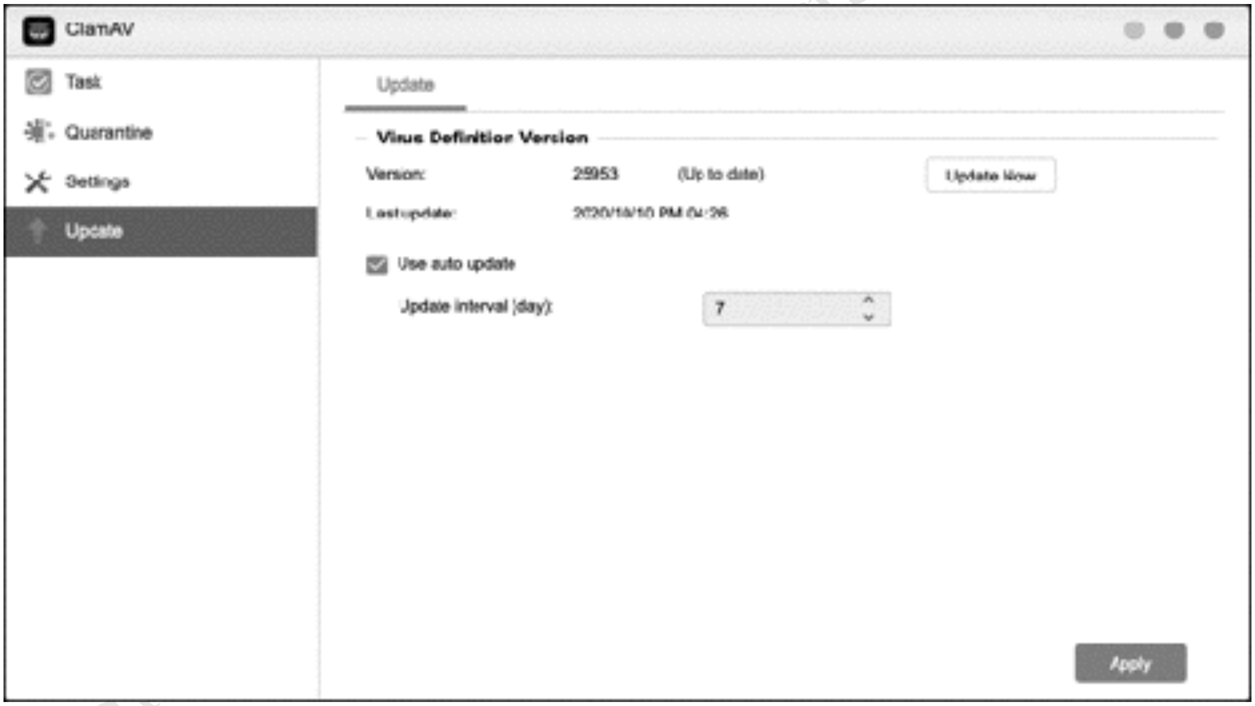
6.1 Overview

Whilst the ADM software is a very secure platform, it is not and cannot be totally immune to the numerous security threats associated with running a sophisticated computer system. To help protect it, ASUSTOR provide a variety of tools and mechanisms and it is recommended that you familiarize yourself with and make use of them.

6.2 ClamAV Antivirus

The chances of the NAS becoming infected with malware are low, as ADM is based on a customized version of Linux and is not particularly susceptible, although it is still 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. *ClamAV* is a free download from App Central and runs on the NAS itself. Separate provision still needs to be made for the workstations themselves using an anti-virus program such as Microsoft Security, AVG, McAfee etc. as there is no linkage between them and the server, nor is this intended as a replacement for security software on desktops and laptops.

Having downloaded and installed ClamAV, an icon will be placed on the Desktop - click it to display the console. It is suggested that you update the virus definitions before continuing; click the **Update** tab followed by the **Update Now** button if it is showing. You may also want to tick the **Use auto update** box and specify an *Update interval* e.g. 7 days. Click **Apply**.



Virus Definition Version

Version: 25953 (Up to date)

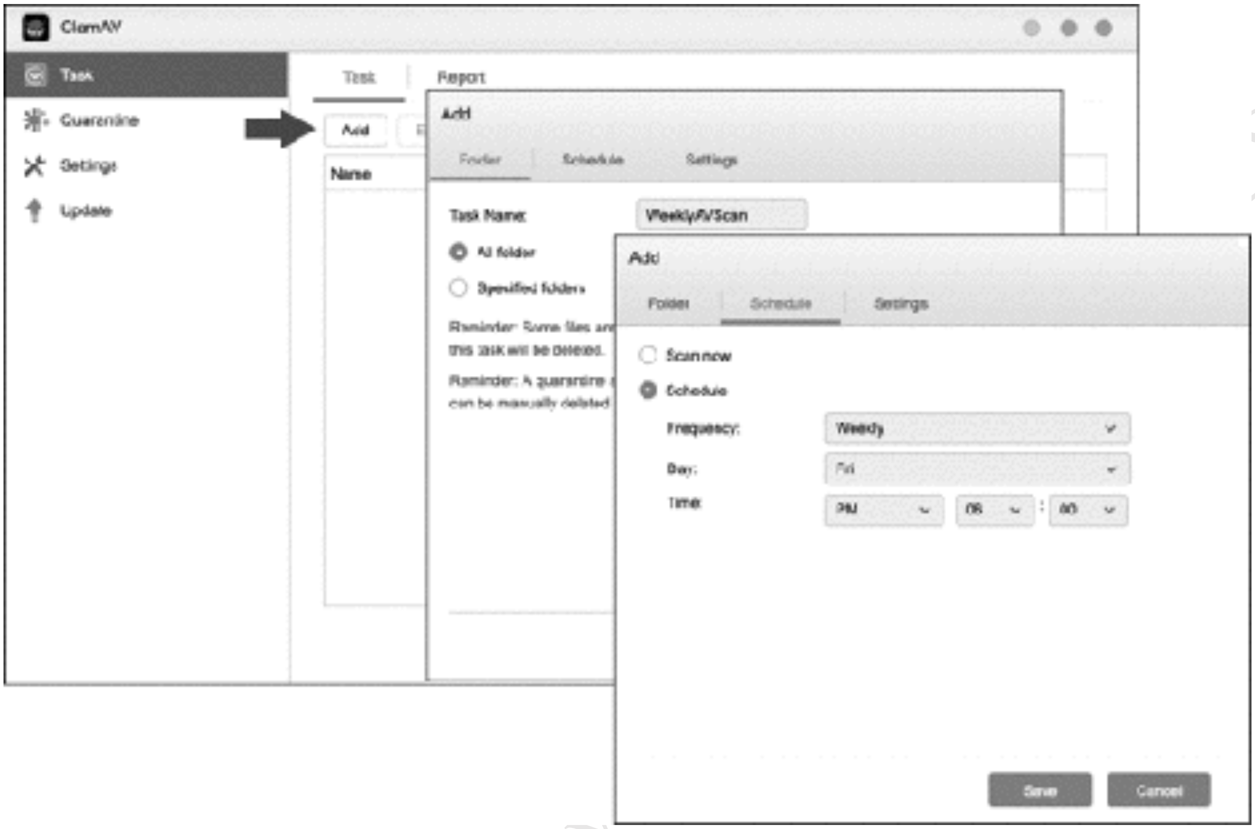
Last update: 2020/10/10 PM 04:26

☑ Use auto update

Jpdate interval (day): 7

Figure 73: Configuring ClamAV updates

The antivirus program does not run constantly in the background in the way that an antivirus program on a Windows computer typically does; rather, scans are run manually else carried out on a scheduled basis. To setup a schedule, go to the **Task** tab and click **Add**. There are three tabs on the resultant panel; on the first one, specify a name for the task and choose whether all folders or just specific folders will be scanned. On the second tab, choose between an immediate scan (**Scan now**) or a scheduled one. Scanning can result in high CPU and memory utilization and, depending on the amount of data stored on the server, can be time consuming; for this reason, it is best done at a quiet time. In this example, we are creating a scan that will run weekly on a Friday at 6:00pm/18:00. Optionally, click the **Settings** tab, where the scanned maximum file size limit can be specified and the default action when a virus is found can be set. Click **Save**.



Task Name: WeeklyAVScan

● All folder

○ Specified folders

Reminder: Some files are … this task will be deleted.

Reminder: A quarantine … can be manually deleted …

○ Scan now

● Schedule

Frequency: Weekly

Day: Fri

Time: PM 08 : 00

Figure 74: Configuring an anti-virus scan

The newly created job will be listed on the main screen. To run a scan manually at any time, click the small 'play' icon against the task.

A report is generated for each scan. To download a report, click on the **Report** tab, highlight the report and click **Download Report**.

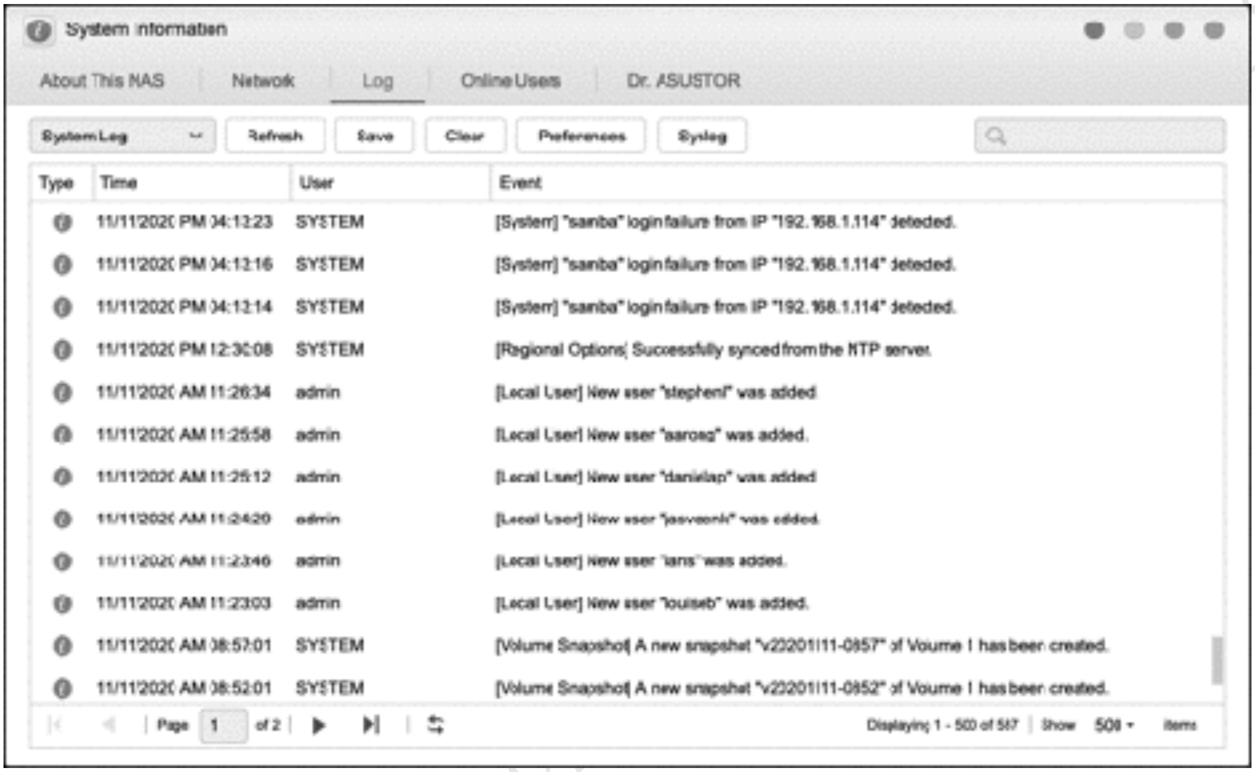
If infected files are found on the server:

1. Go to the *Quarantine* section within ClamAV 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 System Log

The *System Log* provides a comprehensive audit trail of key system activities. When specific security events occur, it is a useful way of determining ‘Who, What, When’, particularly when used in conjunction with the associated log files described in subsequent sections. It is accessed through **Preferences** > **System Information**, then choose **System Log** using the dropdown in the top left-hand corner:

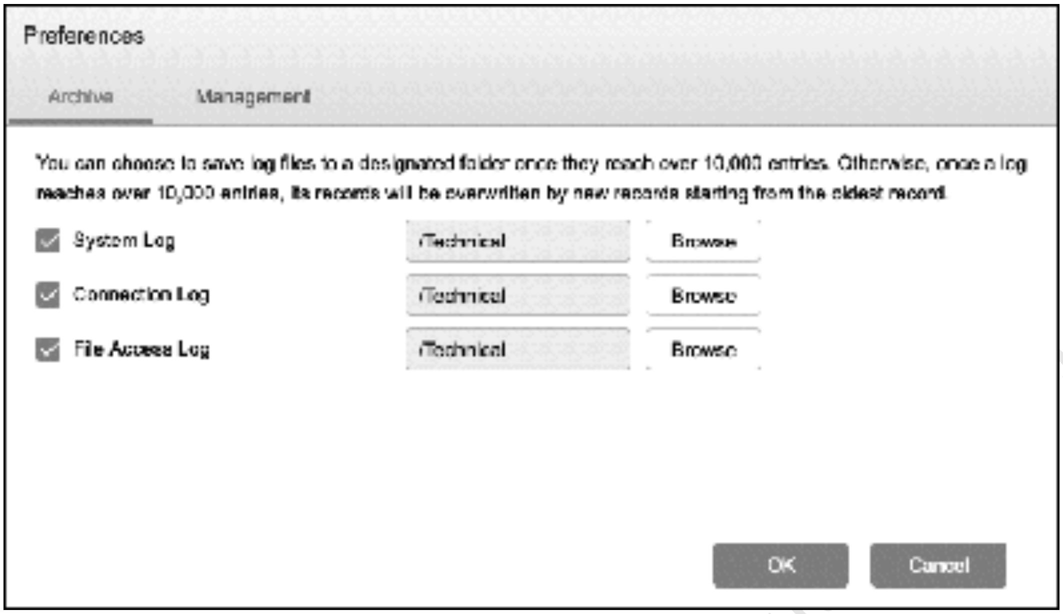


Type	Time	User	Event
●	11/11/2020 PM 04:12:23	SYSTEM	[System] "samba" login failure from IP "192.168.1.114" detected.
●	11/11/2020 PM 04:12:16	SYSTEM	[System] "samba" login failure from IP "192.168.1.114" detected.
●	11/11/2020 PM 04:12:14	SYSTEM	[System] "samba" login failure from IP "192.168.1.114" detected.
●	11/11/2020 PM 12:30:08	SYSTEM	[Regional Options] Successfully synced from the NTP server.
●	11/11/2020 AM 11:26:34	admin	[Local User] New user "stephenl" was added.
●	11/11/2020 AM 11:25:58	admin	[Local User] New user "aaronq" was added.
●	11/11/2020 AM 11:25:12	admin	[Local User] New user "danielap" was added.
●	11/11/2020 AM 11:24:20	admin	[Local User] New user "jasveenh" was added.
●	11/11/2020 AM 11:23:46	admin	[Local User] New user "ians" was added.
●	11/11/2020 AM 11:23:03	admin	[Local User] New user "louiseb" was added.
●	11/11/2020 AM 08:57:01	SYSTEM	[Volume Snapshot] A new snapshot "v20201111-0857" of Volume 1 has been created.
●	11/11/2020 AM 08:52:01	SYSTEM	[Volume Snapshot] A new snapshot "v20201111-0852" of Volume 1 has been created.

Figure 75: System Log

The Type (i.e. severity), Date and User associated with an event are logged. The entries can be sorted by any of these categories, which is done by clicking on the column name, and the information can also be searched.

Because the System Log generates so many events, it needs to be cleared down periodically and this is done by clicking the **Clear** button; if required, the log file can first be saved. Alternatively, it can be configured to automatically save the log file once it reaches 10,000 entries. This is done by clicking the **Preferences** button; on the **Archive** tab, place a tick against the **System Log** entry and specify a folder where the archived log file will be stored. You can also so this for the Connection and File Access Logs, which are discussed in the subsequent sections.



You can choose to save log files to a designated folder once they reach over 10,000 entries. Otherwise, once a log reaches over 10,000 entries, its records will be overwritten by new records starting from the oldest record.

☑ System Log /Technical Browse

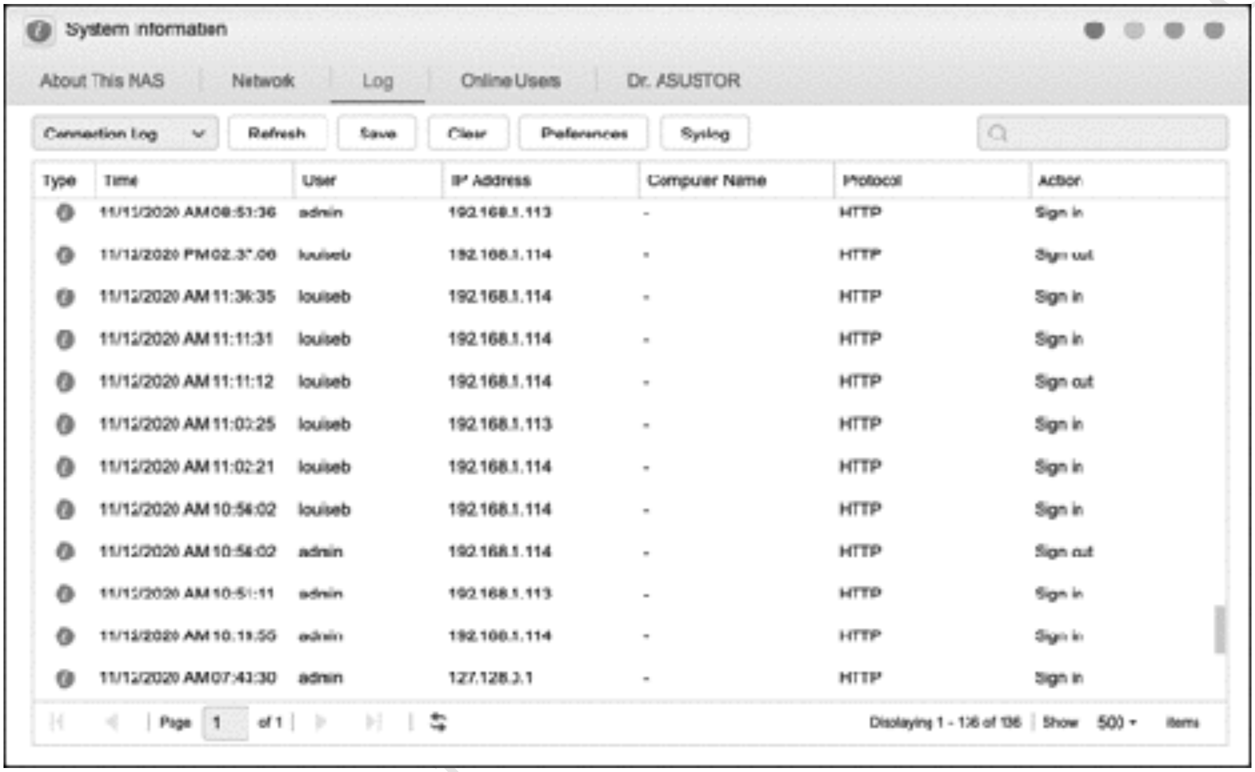
☑ Connection Log /Technical Browse

☑ File Access Log /Technical Browse

Figure 76: Archive settings for Log file(s)

6.4 Connection Log

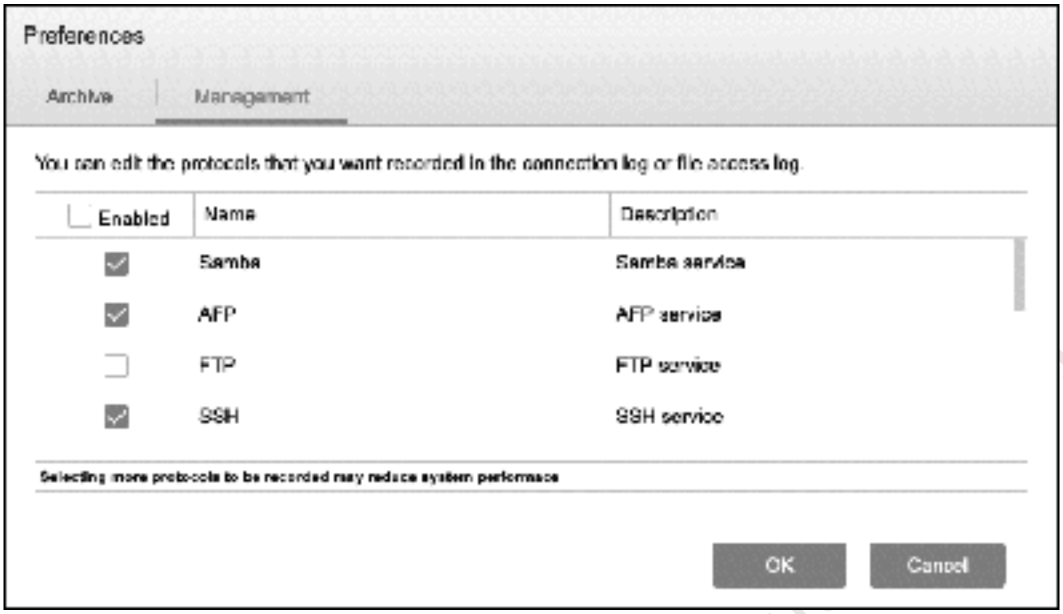
The *Connection Log* is a record of when users login and logout from the system. It records the date and time, username, the IP address of their device and the network protocol used. When specific security events occur, it is a useful way of determining ‘Who, What, When’, particularly when used in conjunction with the associated log files described in the previous and subsequent sections. It is accessed through **Preferences** > **System Information**, then choose **Connection Log** using the dropdown in the top left-hand corner:



Type	Time	User	IP Address	Computer Name	Protocol	Action
●	11/11/2020 AM08:51:36	admin	192.168.1.113	-	HTTP	Sign in
●	11/12/2020 PM02:37:06	louiseb	192.168.1.114	-	HTTP	Sign out
●	11/12/2020 AM 11:36:35	louiseb	192.168.1.114	-	HTTP	Sign in
●	11/12/2020 AM 11:11:31	louiseb	192.168.1.114	-	HTTP	Sign in
●	11/12/2020 AM 11:11:12	louiseb	192.168.1.114	-	HTTP	Sign out
●	11/12/2020 AM 11:03:25	louiseb	192.168.1.113	-	HTTP	Sign in
●	11/12/2020 AM 11:02:21	louiseb	192.168.1.114	-	HTTP	Sign in
●	11/12/2020 AM 10:56:02	louiseb	192.168.1.114	-	HTTP	Sign in
●	11/12/2020 AM 10:56:02	admin	192.168.1.114	-	HTTP	Sign out
●	11/12/2020 AM 10:51:11	admin	192.168.1.113	-	HTTP	Sign in
●	11/12/2020 AM 10:13:55	admin	192.168.1.114	-	HTTP	Sign in
●	11/12/2020 AM07:43:30	admin	127.128.3.1	-	HTTP	Sign in

Figure 77: Connection Log

The protocols that are logged can be customized, for instance, if older Macs are not used then there is no point in logging AFP activity. To control which types are logged, click the **Preferences** button and on the **Management** tab place ticks against the required protocols, noting that ticking every single box can slow down the overall responsiveness of the system. The log file can be cleared down and archived in the same manner as described in section 6.3 System Log.



Preferences

You can edit the protocols that you want recorded in the connection log or file access log.

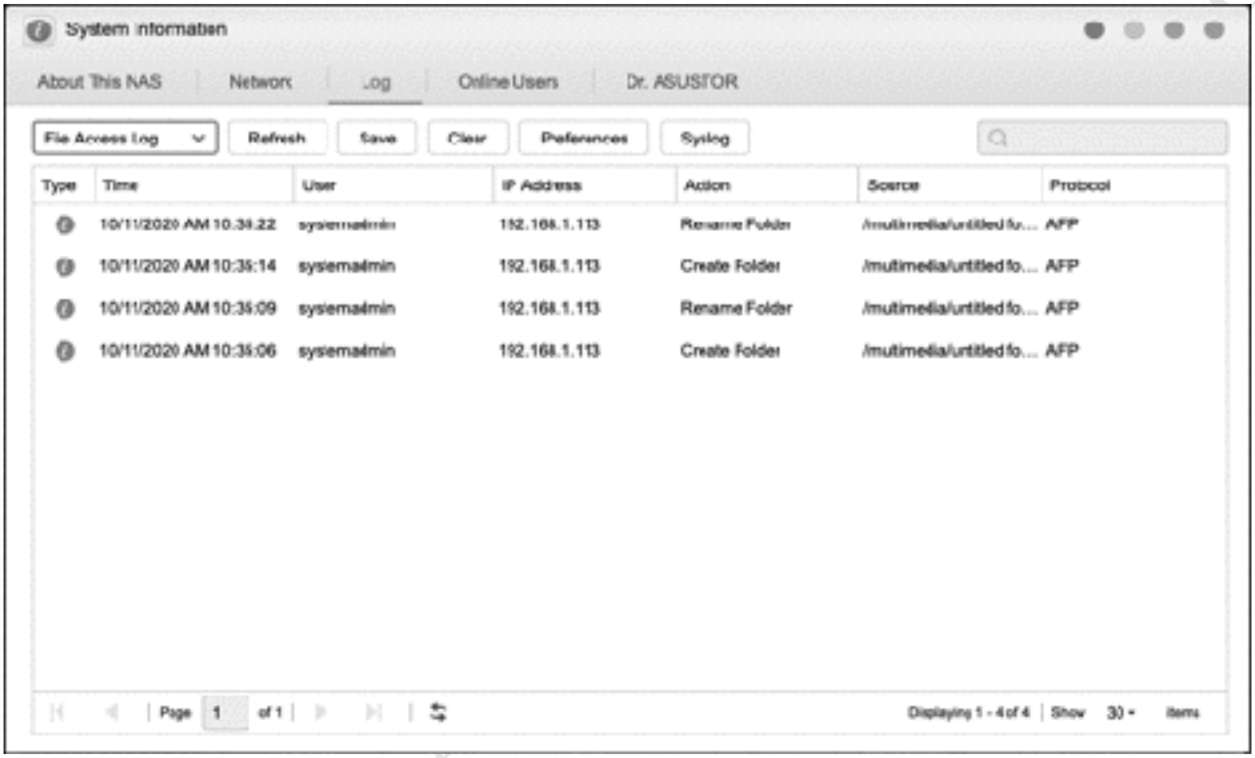
□ Enabled	Name	Description
☑	Samba	Samba service
☑	AFP	AFP service
□	FTP	FTP service
☑	SSH	SSH service

Selecting more protocols to be recorded may reduce system performace

Figure 78: Management settings for network protocols

6.5 File Access Log

The *File Access Log* is a record of the files and folders accessed by users. It records the date and time, username, IP address of their device, activity, name of the file or folder and the network protocol it used. When specific security events occur, it is a useful way of determining ‘Who, What, When’, particularly when used in conjunction with the associated log files described in the two previous sections. It is accessed through **Preferences** > **System Information**, then choose **File Access Log** using the dropdown in the top left-hand corner:



Type	Time	User	IP Address	Action	Source	Protocol
●	10/11/2020 AM 10:36:22	systemadmin	192.168.1.113	Rename Folder	/multimedia/untitled fo...	AFP
●	10/11/2020 AM 10:35:14	systemadmin	192.168.1.113	Create Folder	/multimedia/untitled fo...	AFP
●	10/11/2020 AM 10:35:09	systemadmin	192.168.1.113	Rename Folder	/multimedia/untitled fo...	AFP
●	10/11/2020 AM 10:35:06	systemadmin	192.168.1.113	Create Folder	/multimedia/untitled fo...	AFP

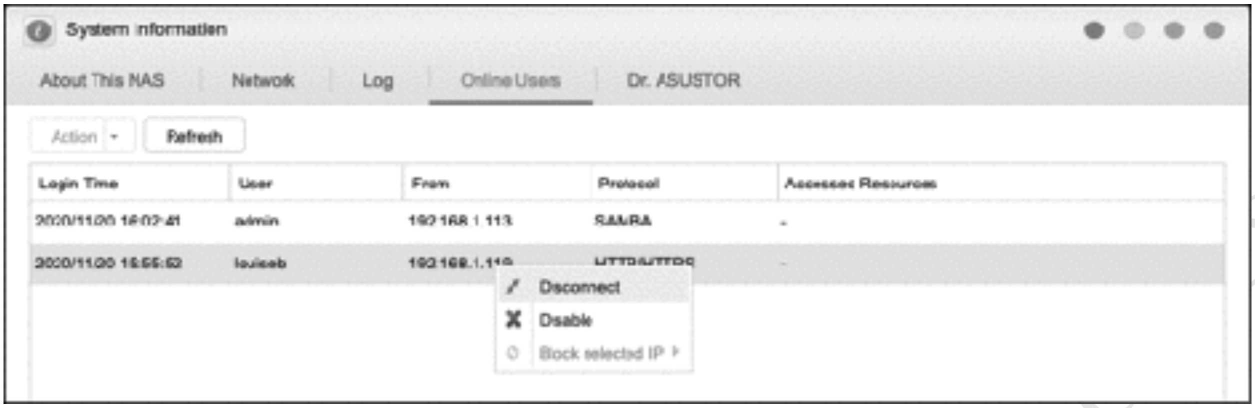
Figure 79: File Access Log

The protocols that are logged can be customized. To do so, click the **Preferences** button and on the **Management** tab place ticks against the required protocols, noting that ticking every single box can slow down the overall responsiveness of the system. The log file can be cleared down and archived in the same manner as described in section 6.3 System Log.

6.6 Online Users

To check who is currently using the system, click **Preferences** > **System Information** and click the **Online Users** tab. The current users are listed by Login Time, Username, IP address and network protocol.

To disconnect or disable a user, or block the IP address they are using, highlight the name and right-click (or click the **Action** button) then choose the required option from the pop-up menu.



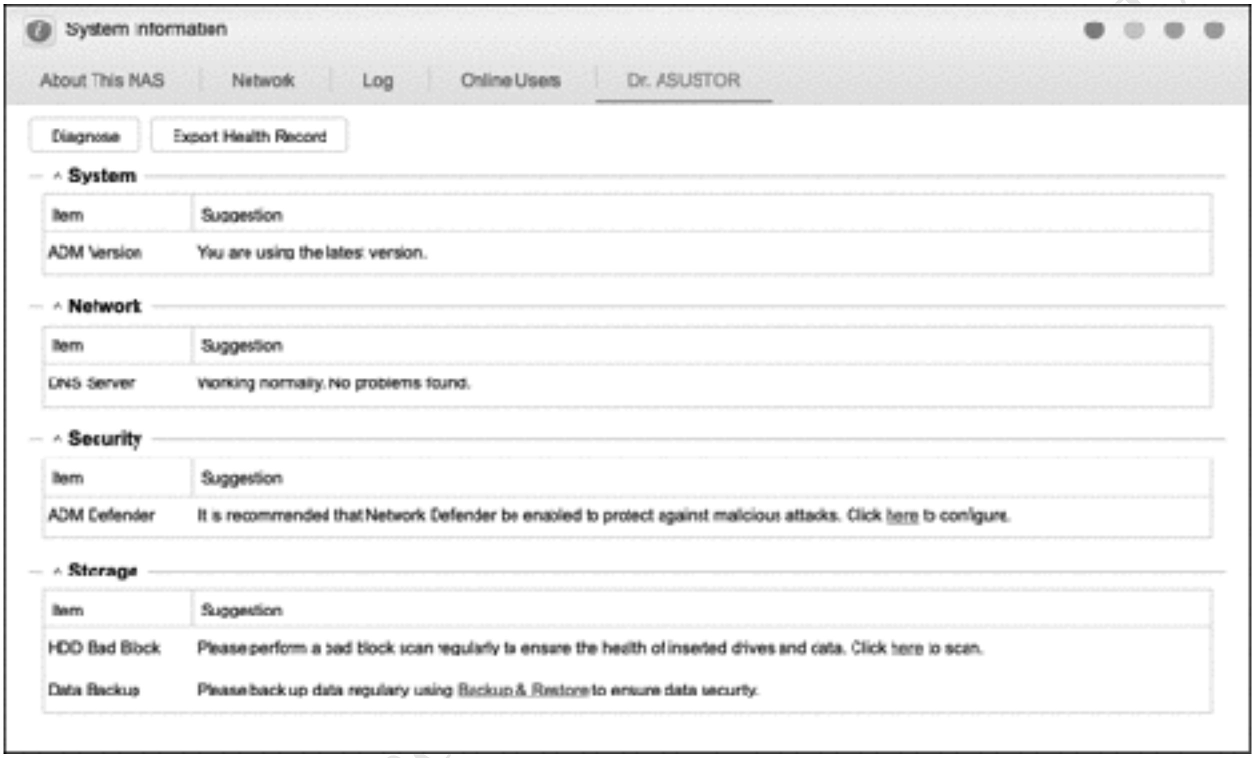
Login Time	User	From	Protocol	Accesses Resources
2020/11/20 16:02:41	admin	192.168.1.113	SAMBA	-
2020/11/20 15:55:52	louiseb	192.168.1.119	HTTP/HTTPS	-

Figure 80: Online Users

6.7 Dr. ASUSTOR

Dr. ASUSTOR is a feature than performs a health check of the NAS, looking at key settings in the four categories of System, Network, Security and Storage. Any areas requiring investigation will be diagnosed and recommendations provided on how to resolve them, along with links to do so. Some of the recommendations are specific, whereas others are more generic and really suggestions about good practice.

Dr. ASUSTOR is located on its own tab within the System Information utility. Click the **Diagnose** button and a report will be quickly generated:



System

Item	Suggestion
ADM Version	You are using the lates version.

Network

Item	Suggestion
DNS Server	Working normally. No problems found.

Security

Item	Suggestion
ADM Defender	It is recommended that Network Defender be enabled to protect against malicious attacks. Click here to configure.

Storage

Item	Suggestion
HDD Bad Block	Please perform a bad block scan regularly to ensure the health of inserted drives and data. Click here to scan.
Data Backup	Please back up data regulary using Backup & Restore to ensure data security.

Figure 81: Dr. ASUSTOR

In the above example, there are no issues with the System (we are running the latest version of ADM) or the Network. In Security, it has been detected that ADM Defender has not been configured and a link to do so has been provided (see section 6.8 ADM Defender). In Storage, it is suggested that a bad block scan in run on a regular basis and a link is provided (this topic is covered in 8.4 Checking the Health of the Drives), and that a regular backup is performed (backups are comprehensively described in 7 BACKUPS).

If you are receiving technical support from ASUSTOR to resolve a problem, they may request that you send them a copy of the health record. This can be generated by clicking the **Export Health Record** button and saving the resultant file. The file contains additional information over and above that described above and is password protected to prevent unauthorized viewing.

6.8 ADM Defender

ADM Defender is a feature within ADM for enforcing network security. It is accessed from **Preferences** > **ADM Defender**, which displays the following screen consisting of two tabs, *Firewall* and *Network Defender*:

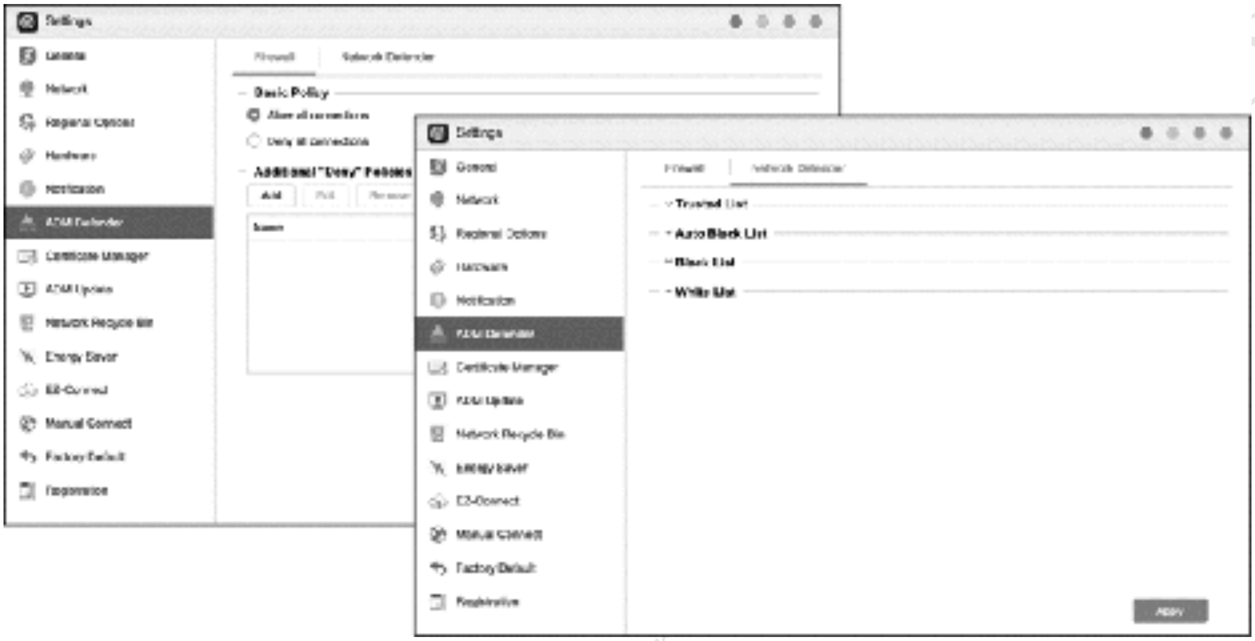


Figure 82: ADM Defender

Firewall

Firewalls allow the creation of rules which define which applications may or may not access the NAS and 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. The firewall within ADM is much simpler and concerned with control over the IP addresses of devices that can access the server, or conversely are to be denied access. By default, all connections are allowed, but there may be circumstances when this needs to be changed. Here is an example:

A specific external IP address is constantly trying to gain access, which may indicate a hacker or some other attempt to compromise the system. In such a case, make sure **Allow all connections** is selected then click **Add** in the *Additional Deny Policies* section and specify the IP address to be blocked.

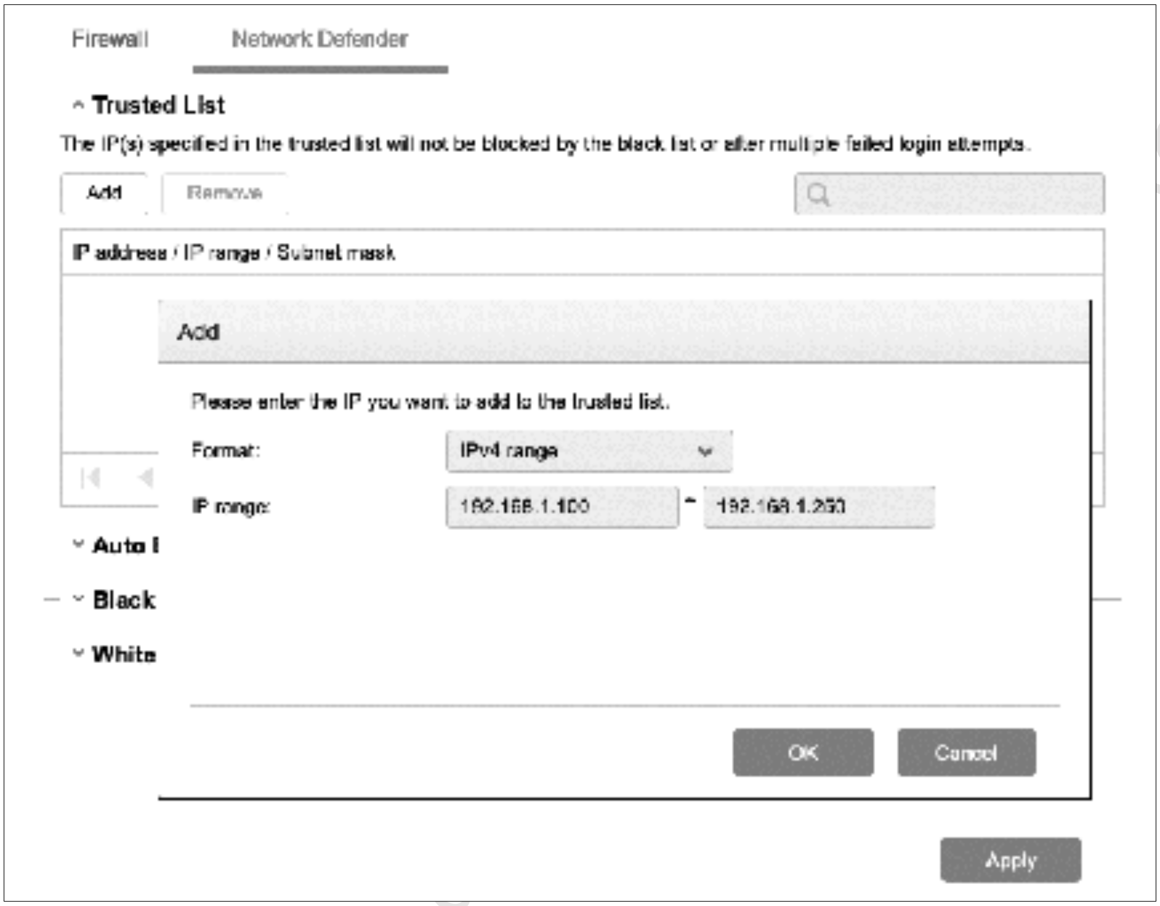
Network Defender

Network Defender is used to disable accounts if there are too many failed login attempts within a specified time period. This security measure can help with both external and internal threats (for instance, imagine a scenario in which a curious or disgruntled employee is trying to access somebody else's account). Network Defender is based around IP addresses; optionally it can be supplemented with the *Geo IP Database*, enabling particular countries to be blocked. The Geo IP Database has to be downloaded separately from App Central and in the following examples this has been done.

Within Network Defender there are four sections:

Trusted List – IP addresses in the Trusted List will never be blocked, regardless of multiple failed login attempts. You might choose to use this if your users are within a local, safe environment, such as a household. Another instance might be in a primary/elementary school with young children. To setup a trusted list:

Click **Add** and for the *Format* choose **IPv4 range** from the dropdown. For the IP range, enter the start and end addresses within your internal network. In this example, the IP range runs from 192.168.1.100 through to 192.168.1.250. Click **OK**, followed by **Apply**.



Trusted List

The IP(s) specified in the trusted list will not be blocked by the black list or after multiple failed login attempts.

IP address / IP range / Subnet mask

Add

Please enter the IP you want to add to the trusted list.

Format: IPv4 range

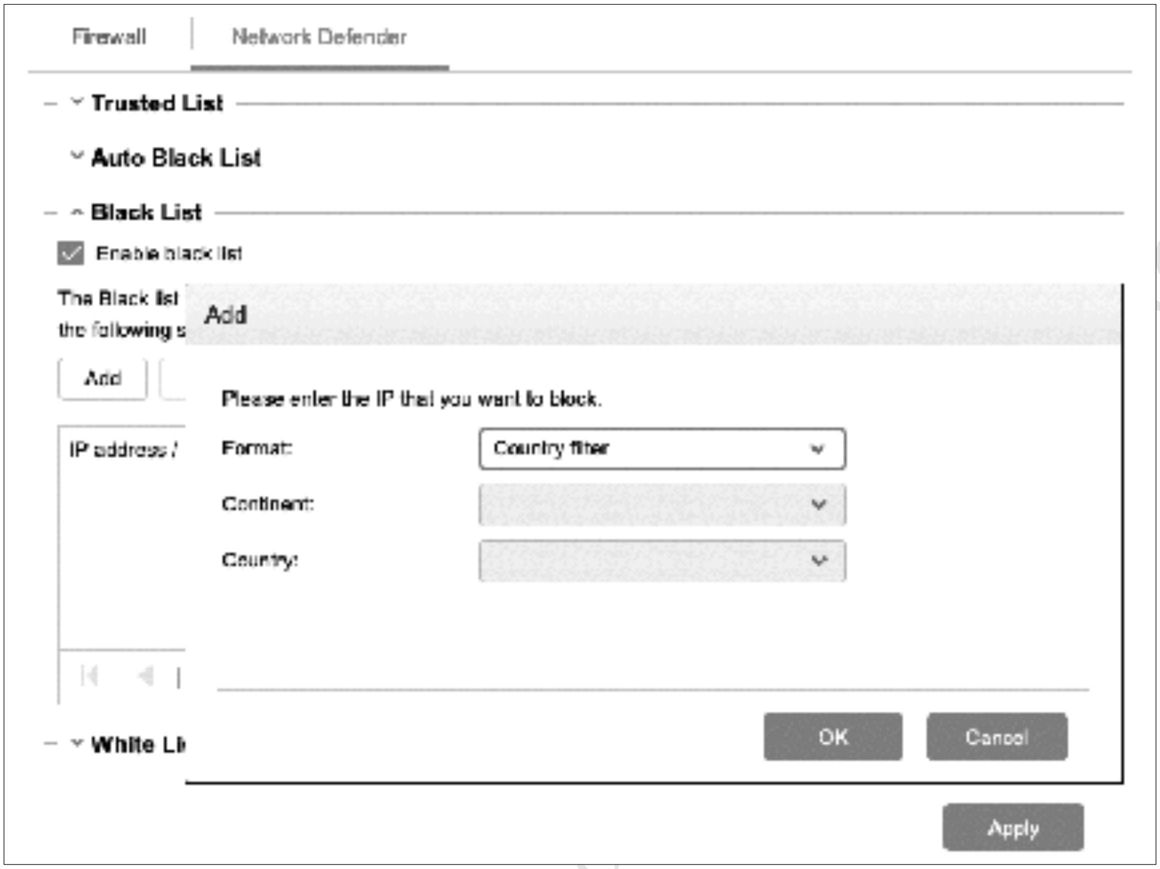
IP range: 192.168.1.100 ~ 192.168.1.250

Figure 83: Setting up a Trusted List

Auto Black List – if this function is enabled, the client IP address will be blocked if there are too many unsuccessful login attempts within a specified time period.

Black List – The Black List can be defined using IP addresses and geolocation. Blocked users are not allowed to use the SAMBA, AFP, FTP, ADM and SSH protocols which are required for normal access.

Tick the **Enable black list** box and click **Add**. On the resultant panel, choose the *Format* from the dropdown. In this example we are applying a country filter; specify the continent and country using the dropdowns and click **OK**. Click **Apply**.



☑ Enable black list

The Black list
the following s

IP address /

Add

Please enter the IP that you want to block.

Format: Country filter

Continent:

Country:

Figure 84: Setting up a Black List

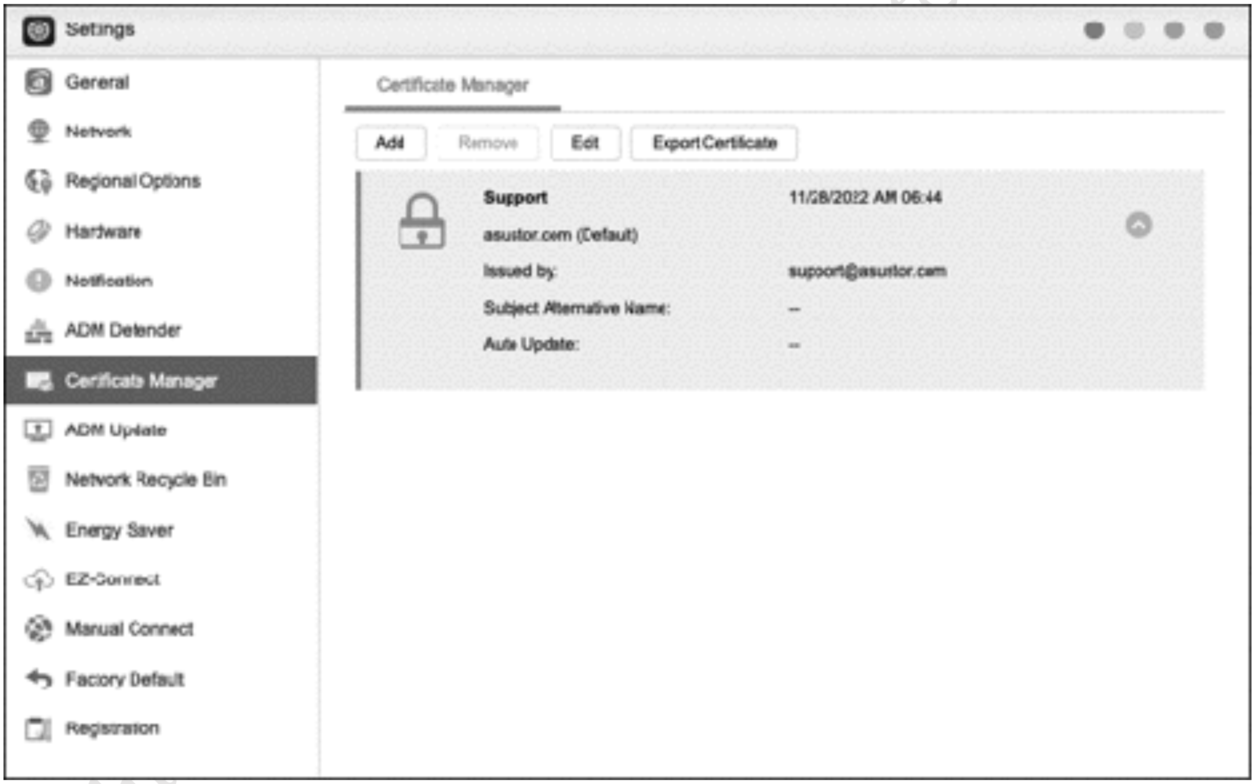
White List – rather than block an IP address or location, the white list serves the opposite purpose and only allows specified IP addresses or geolocations to use the standard protocols required for normal network access.

6.9 Certificate Manager

SSL (Secure Socket Layer) Certificates offer higher levels of security when computers are handling encrypted web-based services, which are those 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 topic. If you are an experienced IT professional and/or external access to your network is important and you wish to maximize security, then you may want to take action. This section does not discuss the detailed use of certificates, just how to get started.

Certificates in ADM are managed using *Certificate Manager*, which is accessed by clicking **Preferences** > **Certificate Manager**. It shows that a default certificate issued by ASUSTOR for its NAS users is installed, along with its expiry date:



Support 11/28/2022 AM 06:44

asustor.com (Default)

Issued by: support@asustor.com

Subject Alternative Name: --

Auto Update: --

Figure 85: Certificate Manager

Four options are available:

Add – This allows you to import an existing certificate, or to add a new one from the open certificate authority *Let's Encrypt*, which provides certificates free of charge (although they will accept donations).

Remove – to remove an existing certificate.

Edit – for making changes to a certificate, such as its name and to set it as the default certificate.

Export Certificate – this allows you to download a copy of the certificate from the NAS for safety and backup purposes.

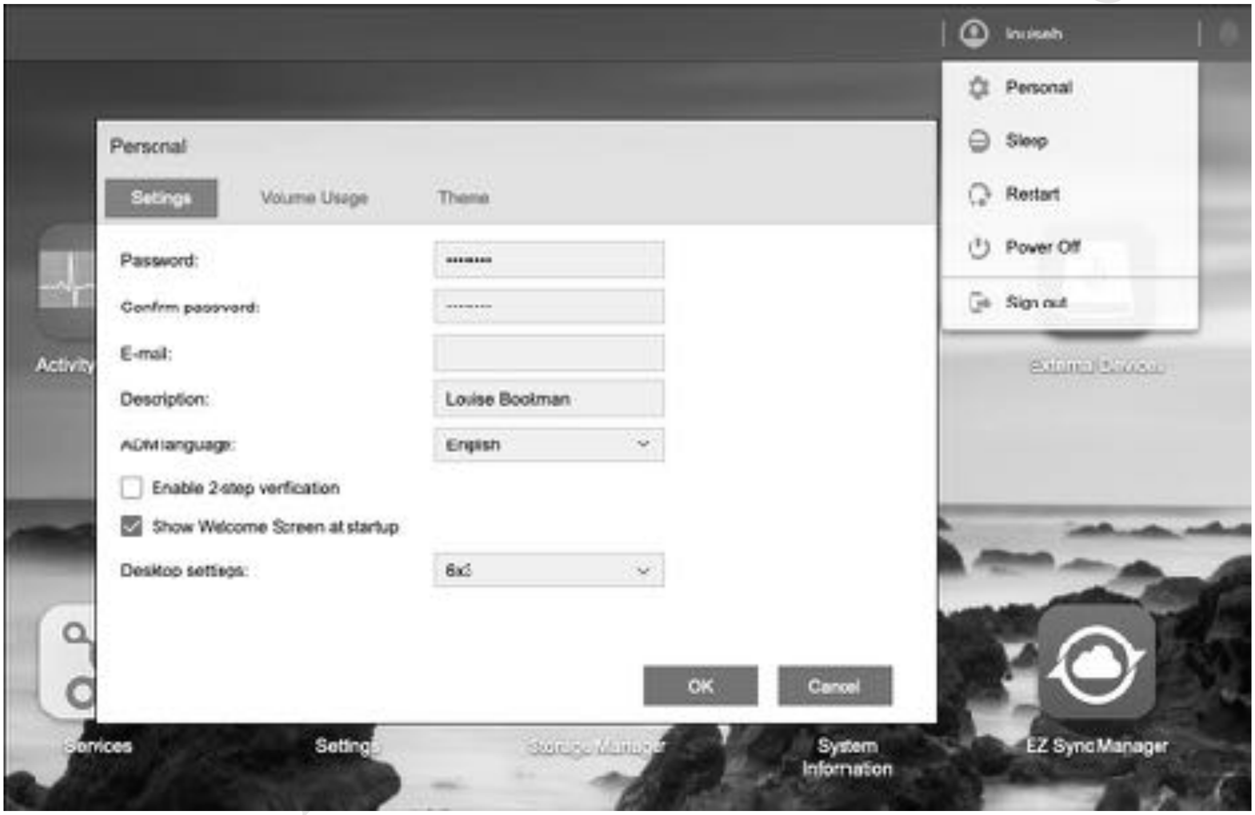
More general information about using certificates can be located at the https://letsencrypt.org/docs/ website.

6.10 Changing Passwords

It may be necessary to change a user's password, for example if they have forgotten it or if there is reason to believe that it has been compromised. It is not possible to determine what the is, rather a new one has to be specified by the admin user.

Click **Preferences** > **Access Control** > **Local Users**. Highlight the user's name and click **Edit**. On the **Information** tab, type in and confirm the new password and click **OK**, then advise the user.

It is considered good practice to change passwords on a regular basis and users can do so at any time. Having logged in, they should click their username in the top right-hand corner of the screen and click **Personal** on the popup menu. On the resultant panel they should type and confirm their new password, then click **OK**.



Personal

Settings | Volume Usage | Theme

Password: ••••••••

Confirm password: ••••••••

E-mail:

Description: Louise Bookman

ADM language: English

☐ Enable 2-step verification

☑ Show Welcome Screen at startup

Desktop settings: 6x3

Figure 86: Changing the password

7

BACKUPS

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, which include deleting files by accident, malware infections, data corruption, computer failure and equipment being lost or stolen. In general, the value of data far outweighs the value of the computers themselves; 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 in some parts of the world. The assumption to follow is that it is more a question of *when* rather than *if* data will be lost at some point, which is when the backups will be needed.

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

The computers in the home or office are backed up to the NAS. The NAS in turn is backed up to an external USB drive. Optionally, the NAS or at least the most important data on it are backed up to a Cloud-based service. Additionally, the NAS can also be backed up to a second NAS located on or off the premises:

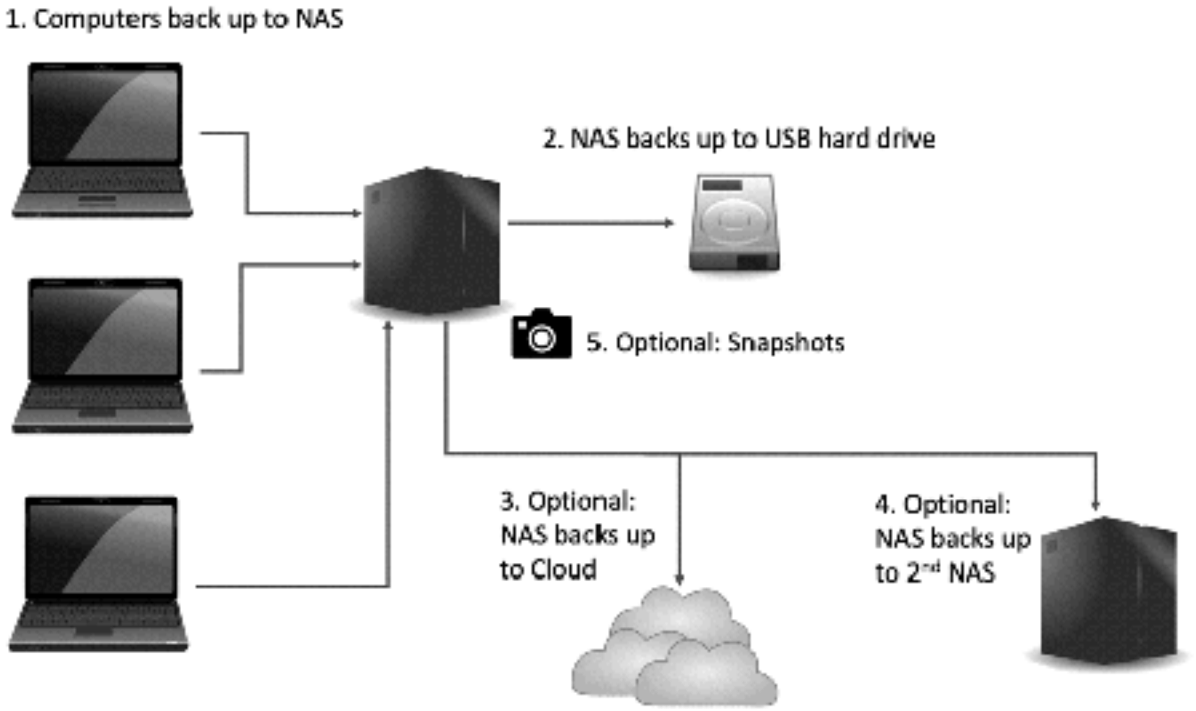

1. Computers back up to NAS
2. NAS backs up to USB hard drive
5. Optional: Snapshots
3. Optional: NAS backs up to Cloud
4. Optional: NAS backs up to 2nd NAS

Figure 87: Example of multi-faceted backup approach

ADM has provision for all these types of backup and provides a single app – *Backup & Restore* – to handle them. It is installed automatically during the installation of ADM and is accessed from the Desktop.

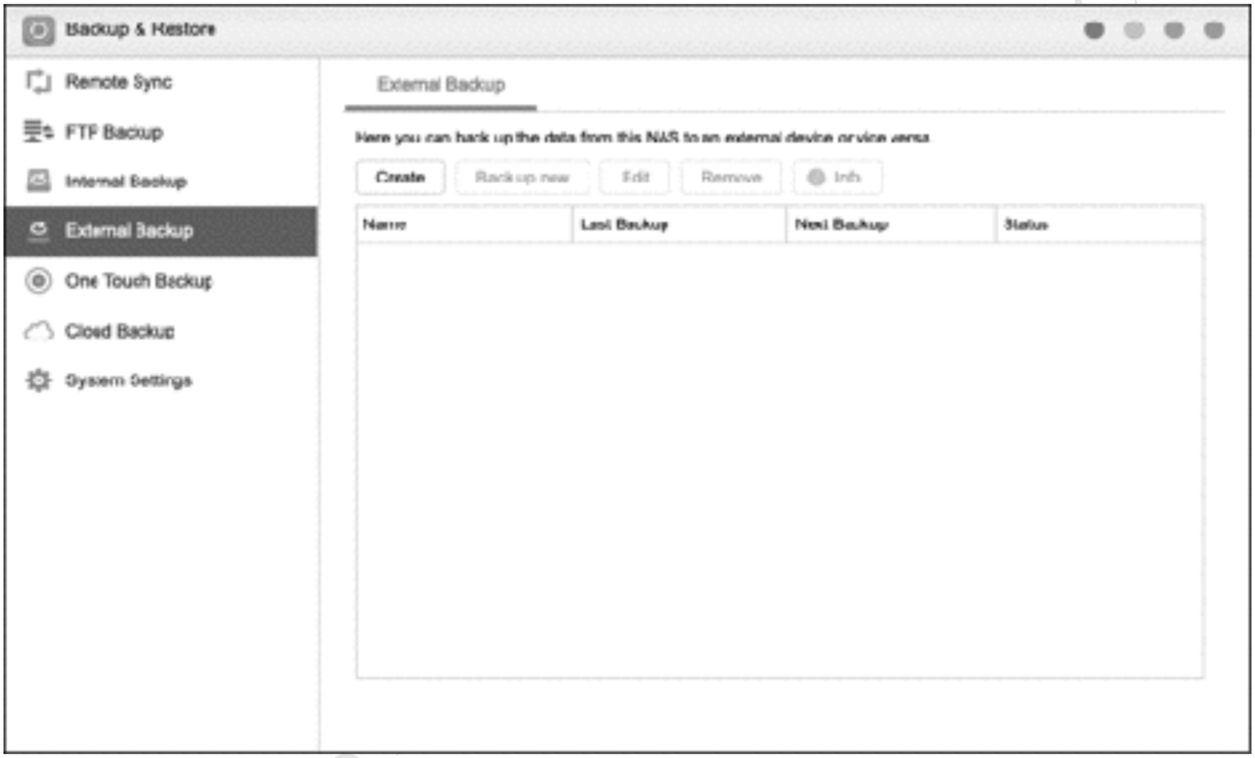
Besides the comprehensive facilities available through Backup & Restore, ADM also features *Snapshots*, whereby data is effectively 'photographed' at regular moments in time. This is defined as a storage-related rather than conventional backup mechanism and is discussed separately in section 12.3 Snapshots.

7.2 Backup & Restore Utility

Backup & Restore is an app that offers a comprehensive ‘one stop shop’ for backup and sync. The basic principle is ‘any type of backup, to any destination’ i.e. you can perform most types of backup operation with external drives, to other NAS boxes and to a wide selection of popular cloud services.

As mentioned above, the best approach with backups is to take a multi-tiered approach involving different types of backup technology and an important concept here is *off-site storage*, whereby a copy of data is held in a different location altogether. The extensive support for cloud services in Backup & Restore makes it very suitable for handling off-site backups.

Launch Backup & Restore by clicking on its icon on the Desktop, which will display this screen:



Here you can back up the data from this NAS to an external device or vice versa.

Figure 88: Backup & Restore utility

On the left-hand side of the screen are links to the different options:

Remote Sync – enables data to be backed up to another NAS. See [7.7 NAS-to-NAS Backups Using Remote Sync](#).

FTP Backup – for backing up to another computer system running an FTP server. This is a less common choice and is not covered in this guide.

Internal Backup – enables data to be backed up from one folder to another folder on the NAS.

External Backup – for backing up data from the NAS to an external USB drive. This is the most widely used backup option and is detailed below in [7.3 Backup to External Drive](#).

One Touch Backup - Some models have a feature called *One Touch Backup*, whereby files can be copied to or from a drive plugged-in to a USB socket on the NAS. This option will be listed only if your model has this feature.

Cloud Backup – enables data to be backed up to Amazon's S3 (Simple Storage Service). This is mainly of relevance to corporate users and is not covered in this guide. However, backing data to public cloud services such as Dropbox, Google Drive and OneDrive is described in 7.9 Backup Using DataSync Center and Cloud Services.

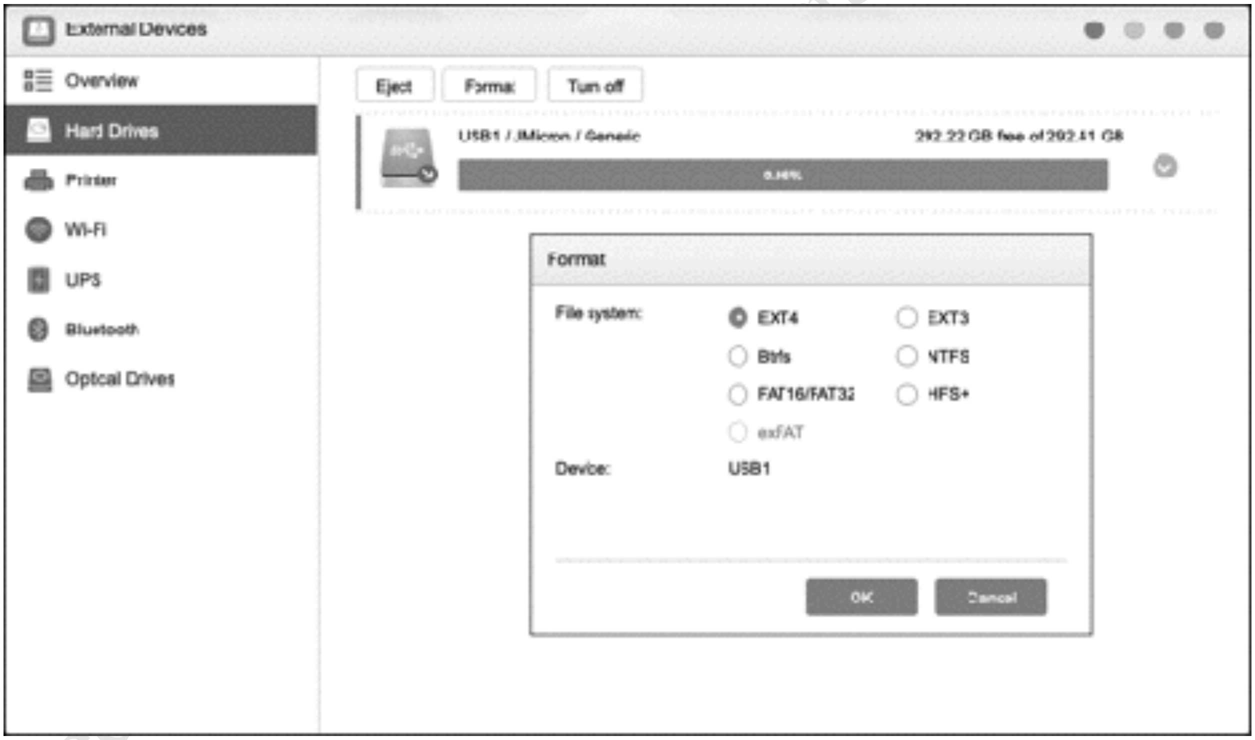
System Settings – backup destinations, whether NAS or cloud-based, are referred to as Storage Spaces by ASUSTOR and their details can be checked from here.

7.3 Backup to External Drive

This backup solution uses an external USB hard drive. The drive should preferably be USB 3.0 specification or better; of sufficient capacity to hold all the data (for instance, if there is 4TB data then use at least a 4TB drive); portable if possible, as they do not require mains power and are more convenient to store, although there are capacity restrictions when compared to powered external drives.

To prepare it for backup usage, plug the external drive into a spare USB socket on the NAS, noting that on some models not all of the USB sockets are of USB 3.0 specification. Wait a short while (say, 30 seconds), during which time the LED on the drive will flash occasionally. Launch **External Devices** from the Desktop and the drive should be listed in the *Hard Drives* panel (it will also appear in the *Overview* screen). If the drive is not listed, check that support for external drives is enabled and if necessary click the **Turn on** button.

Within the Hard Drives panel, make sure the drive is highlighted and click the **Format** button. There are multiple file systems to choose from, but you need ADM's preferred file system type of **EXT4**. Click **OK** 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, as often such drives will have been formatted with the Windows exFAT or NTFS filing systems, which are unsuitable here. When complete, quit the External Devices utility.



USB1 / JMicron / Generic 292.22 GB free of 292.41 GB

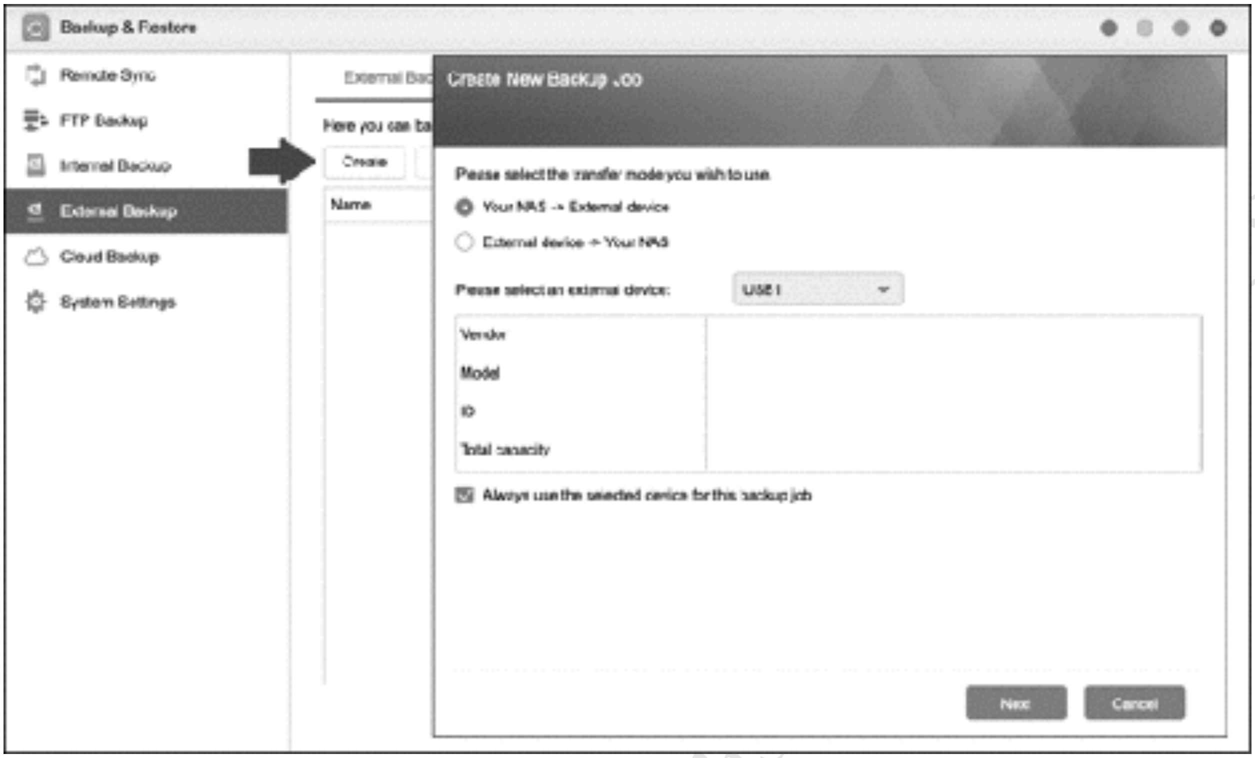
0.06%

File system: ● EXT4 ○ EXT3 ○ Btrfs ○ NTFS ○ FAT16/FAT32 ○ HFS+ ○ exFAT

Device: USB1

Figure 89: Format External Drive

Go into **Backup & Restore** and click **External Backup**. Click the **Create** button. Choose the transfer mode option of **Your NAS -> External device** and select the external USB drive using the dropdown. You will probably want to tick the **Always use the selected device for this backup job** option. Click **Next**.



Please select the transfer mode you wish to use.

● Your NAS -> External device

○ External device -> Your NAS

Please select an external device: USB I

Vendor

Model

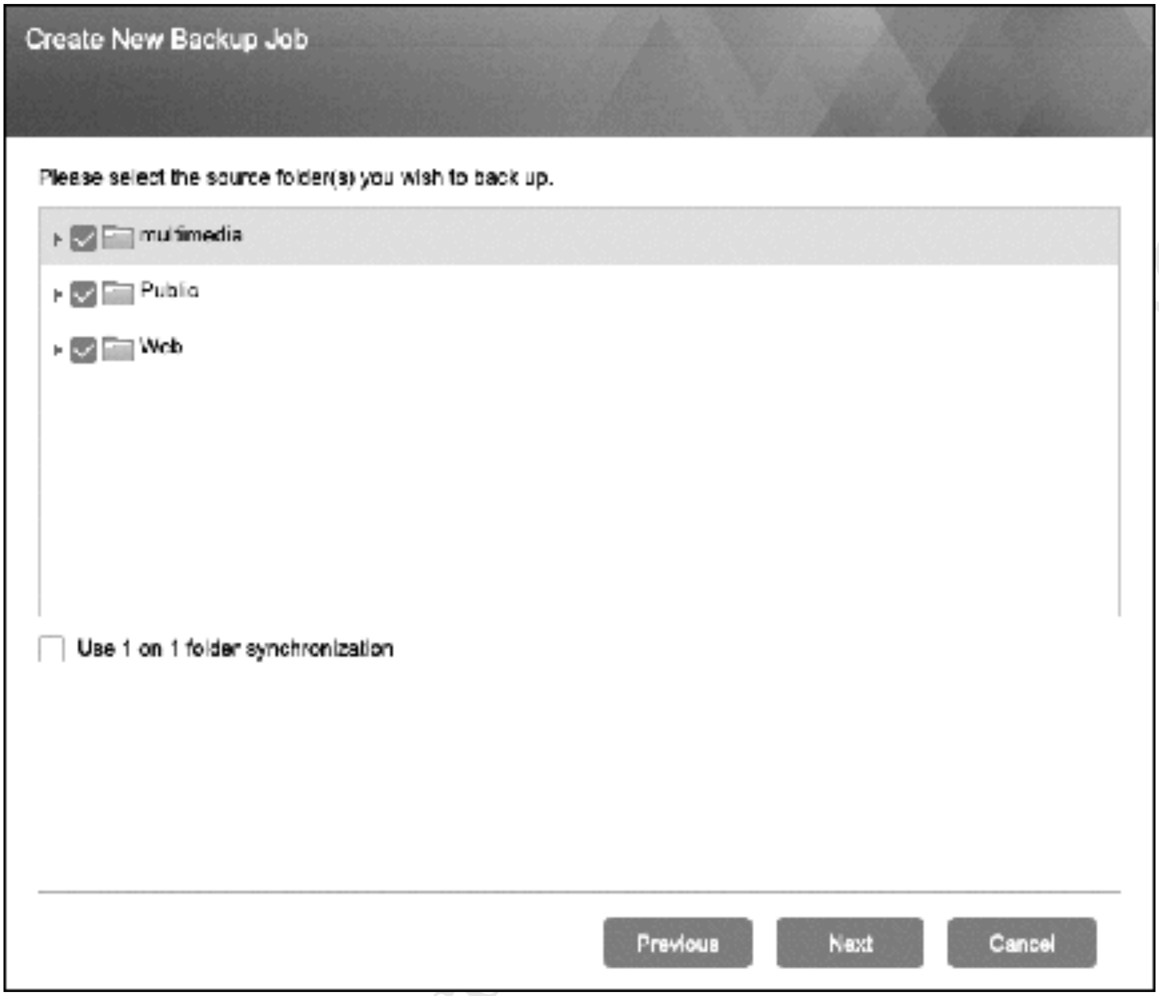
ID

Total capacity

☒ Always use the selected device for this backup job

Figure 90: Start a new backup job

On the subsequent screen, select the source folders to be backed up. Folders can be expanded by clicking on the chevrons and individual files within them excluded/included in the backup, if required. In this example, we will back up everything. Do not tick the *Use 1 on 1 folder synchronization* box. Having made a selection, click **Next**:



Create New Backup Job

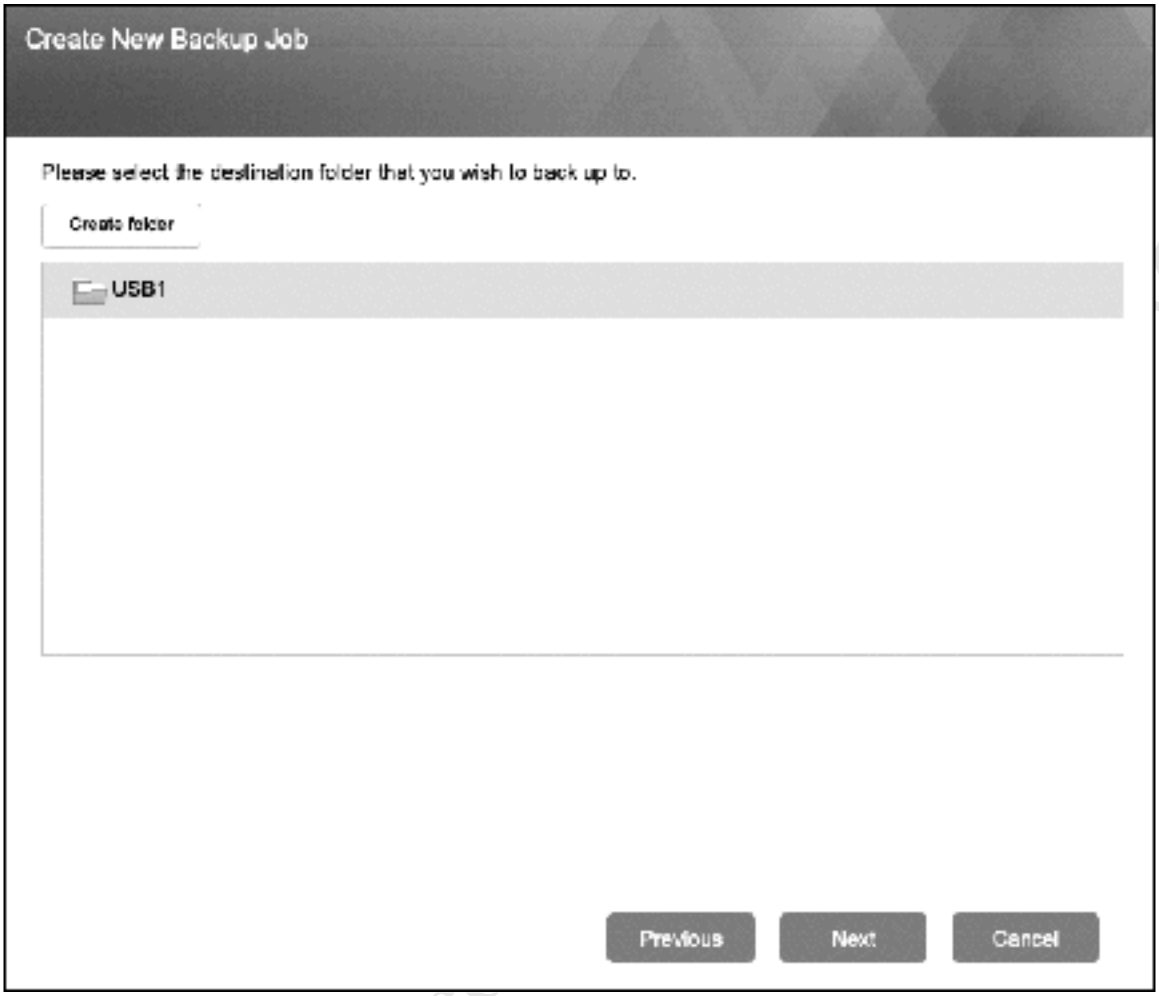
Please select the source folder(s) you wish to back up.

- ☑ multimedia
- ☑ Public
- ☑ Web

□ Use 1 on 1 folder synchronization

Figure 91: Select source folders for backup

If required, a destination folder for the backup can be created on the external drive. However, you can skip this so the backup will be at the 'top' or 'root' of the drive. Click **Next**:

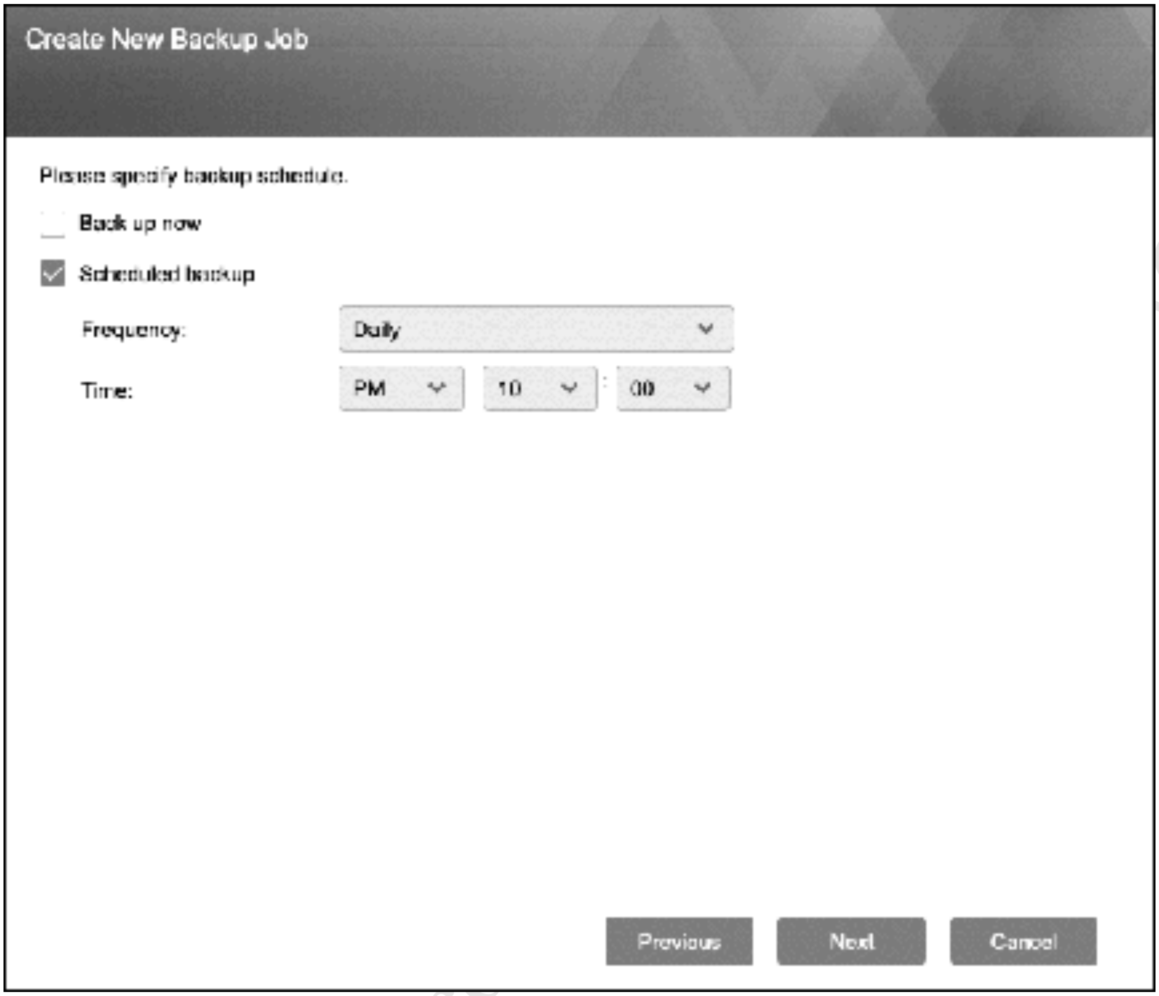


Create New Backup Job

Please select the destination folder that you wish to back up to.

Figure 92: Select destination folder for backup

On the next screen, the backup job can be scheduled to run on a regular basis e.g. daily, weekly, monthly. The backup should preferably run at a time when the server is not being used or is not busy, which will depend upon the circumstances of your household or business. In this example the backup is set to run daily at 10:00pm/2200h in the evening. Click **Next**.



Please specify backup schedule.

□ Back up now

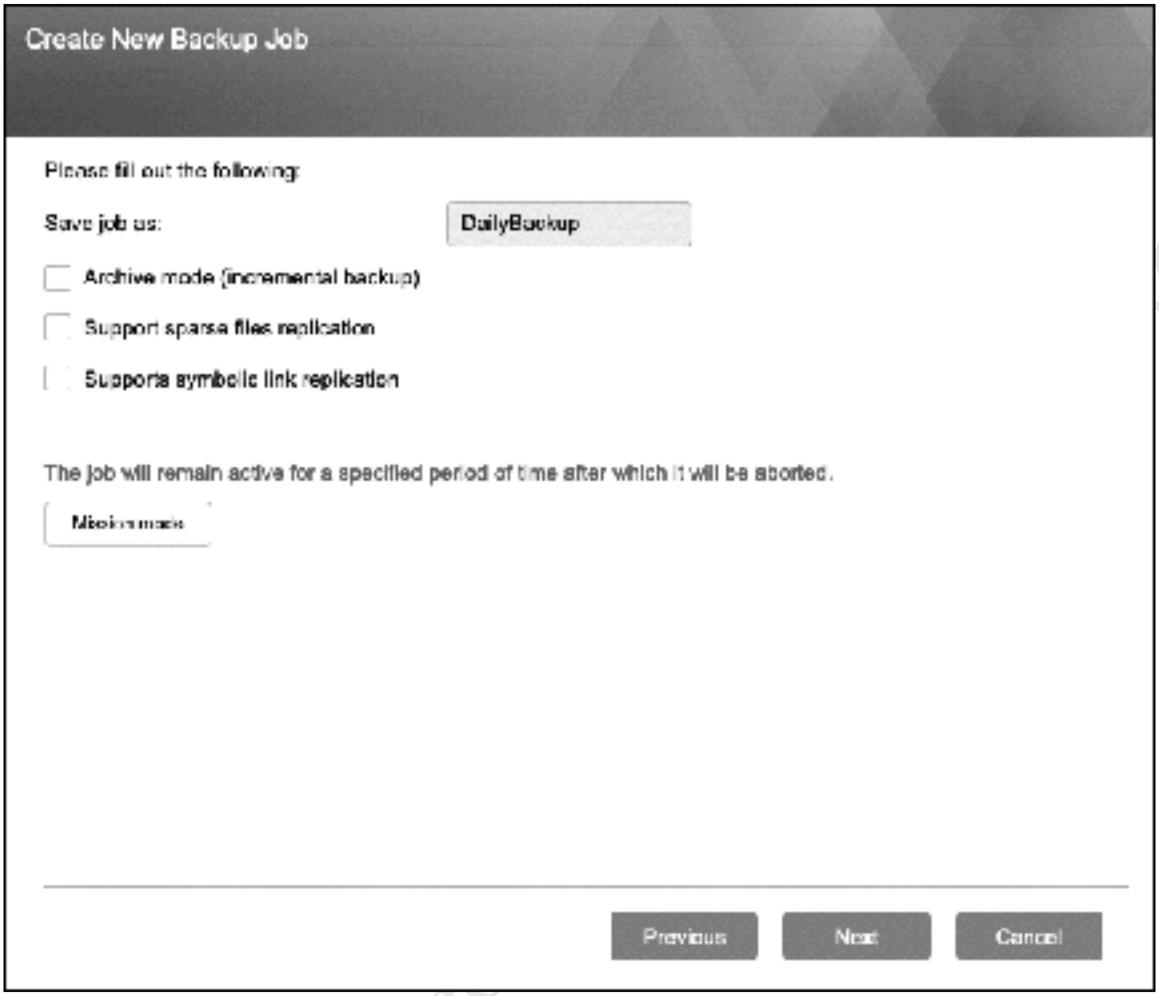
☑ Scheduled backup

Frequency: Daily

Time: PM 10 : 00

Figure 93: Create a job schedule

On the subsequent screen, specify a name for the backup job e.g. *DailyBackup*. There are a number of optional parameters that can be specified; if **Archive mode (incremental backup)** is ticked then only folders and files that have changed since the previous backup will be backed up, meaning that subsequent backups will be quicker. *Mission mode* enables a backup to be terminated automatically if it has been running too long or 'hung'. Click **Next**.



Create New Backup Job

Please fill out the following:

Save job as: DailyBackup

□ Archive mode (incremental backup)

□ Support sparse files replication

□ Supports symbolic link replication

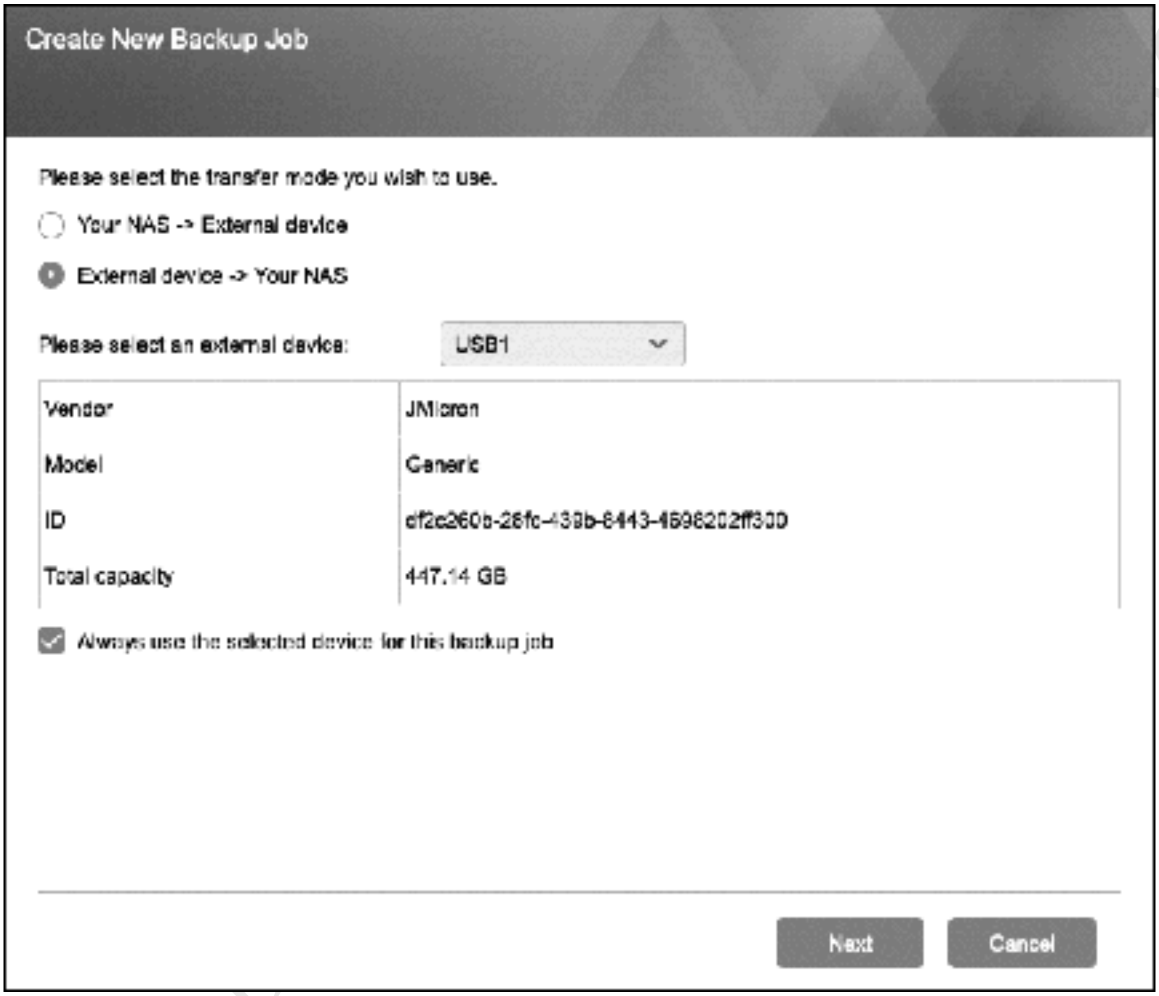
The job will remain active for a specified period of time after which it will be aborted.

Figure 94: Specify a job name

A summary screen is displayed. Assuming all is well, click **Finish** to create the job, which will then be listed in the *External Backup* panel. To run it immediately, which is useful for testing purposes, or manually at any time, click the **Back up Now** button. There are also options to Edit and Remove the job, plus create additional ones.

7.4 Restoring Data from an External Backup

Restoring files from a backup consists of creating a task in Backup & Restore but running in the other direction i.e. ‘backing up’ from an external USB drive to the NAS. Go into **Backup & Restore** and click **External Backup**. Click the **Create** button. Choose the transfer mode option of **External device -> Your NAS** and select the external USB drive using the dropdown. Click **Next**.



Create New Backup Job

Please select the transfer mode you wish to use.

○ Your NAS -> External device

● External device -> Your NAS

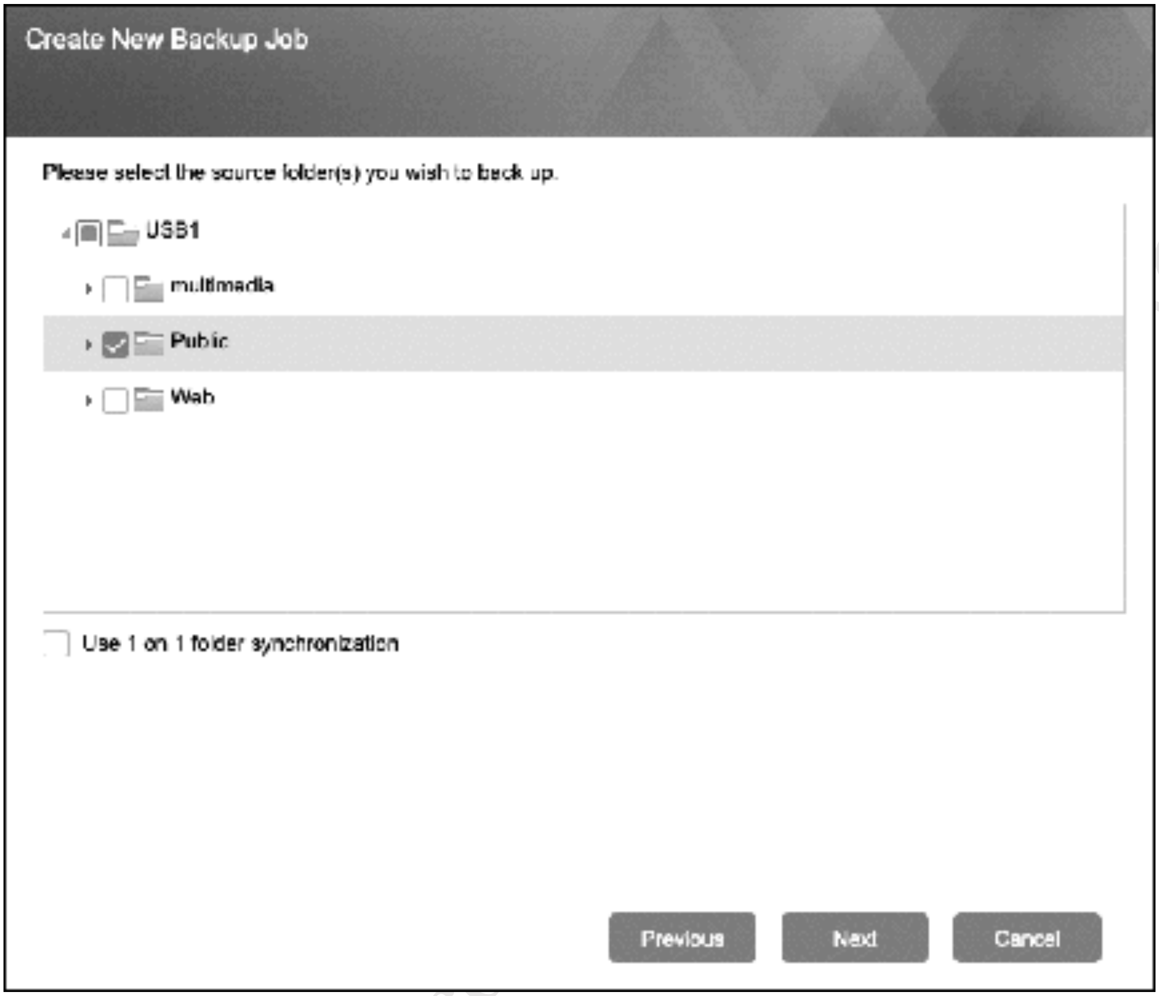
Please select an external device: USB1

Vendor	JMicron
Model	Generic
ID	cf2c260b-28fc-439b-8443-4696202ff300
Total capacity	447.14 GB

☑ Always use the selected device for this backup job

Figure 95: Start a new restore job

On the subsequent screen, select the folder(s) to be restored. To restore everything you would choose the USB drive, otherwise expand the drive and mark the folder(s). The folders themselves can be expanded, to just restore specific files. In this example we will restore the *Public* folder. Having made a selection, click **Next**:



Create New Backup Job

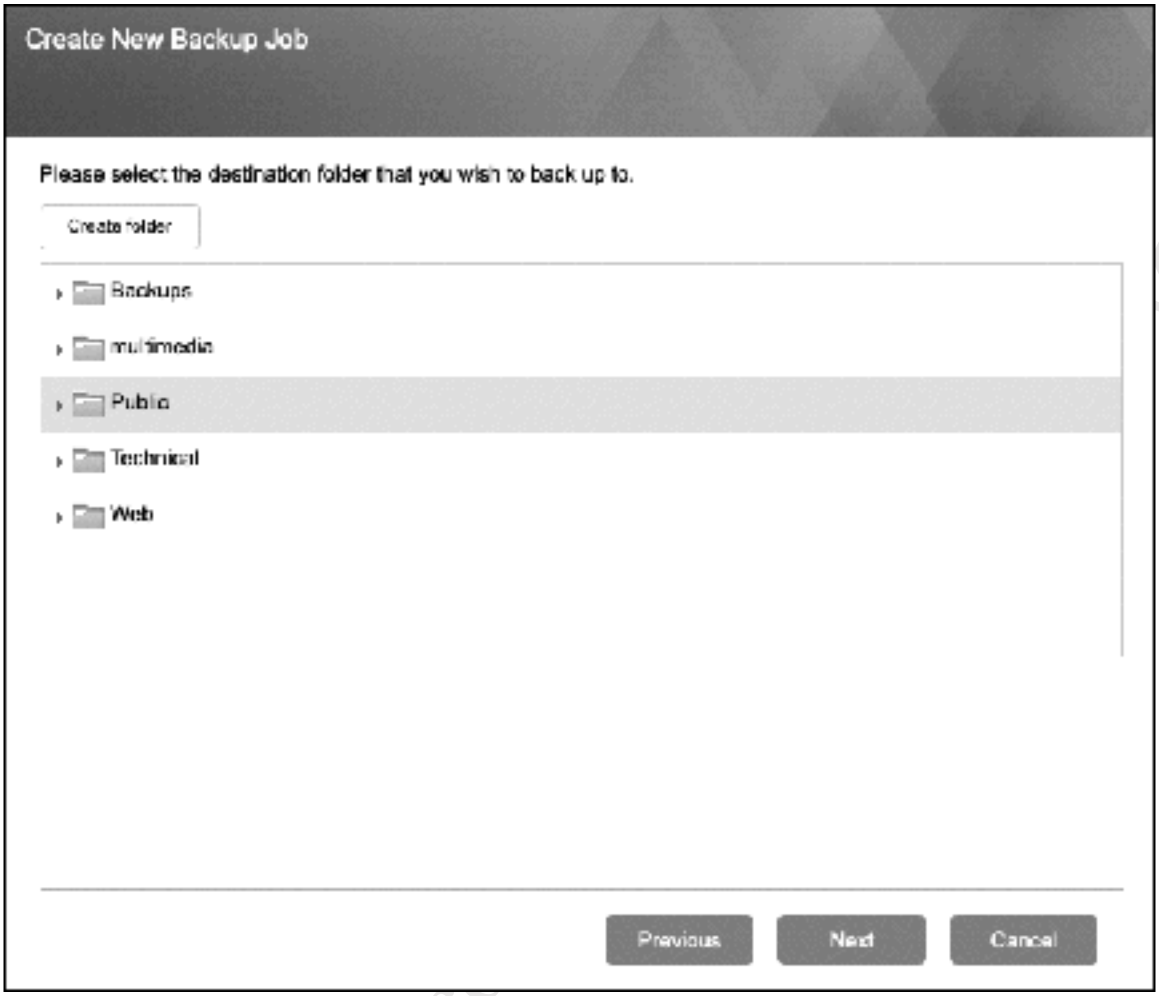
Please select the source folder(s) you wish to back up.

- ▪ USB1
  - □ multimedia
  - ☑ Public
  - □ Web

□ Use 1 on 1 folder synchronization

Figure 96: Select items to be restored

On the following screen, 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 Explorer:

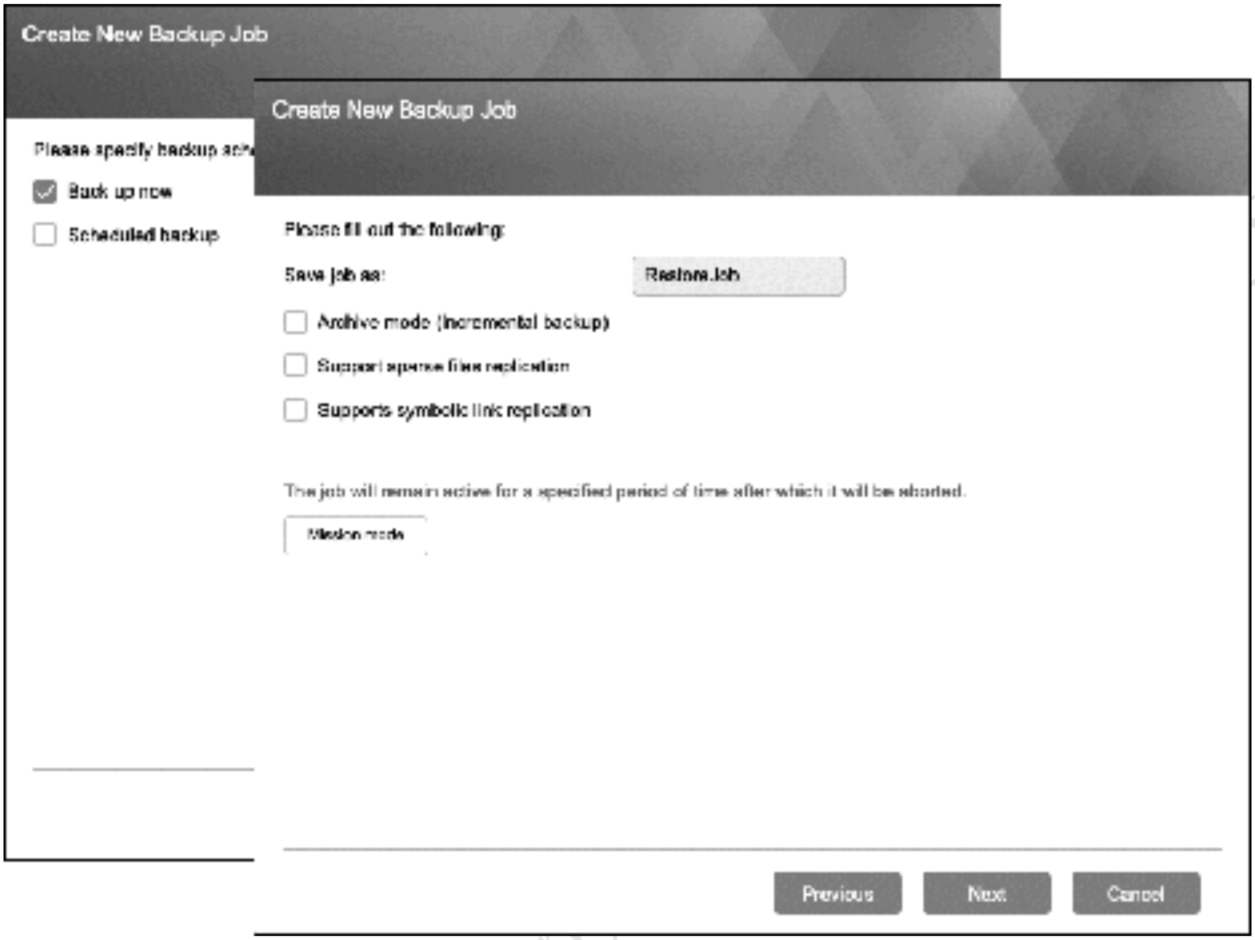


Create New Backup Job

Please select the destination folder that you wish to back up to.

Figure 97: Choose where the data will be restored to

On the next screen you can choose to restore now or schedule it for later. When there is a need to restore files, chances are it needs to be done soon so select **Back up now** and click **Next**. However, if you were restoring a large amount of data you could schedule it to run at some other time, such as overnight. Having made a choice, click **Next**. On the screen after that you can optionally name the job and set some optional parameters. Click **Next**.



Create New Backup Job

Please specify backup sche

☑ Back up now

☐ Scheduled backup

Create New Backup Job

Please fill out the following:

Save job as: Restore.Job

☐ Archive mode (incremental backup)

☐ Support sparse files replication

☐ Supports symbolic link replication

The job will remain active for a specified period of time after which it will be aborted.

Figure 98: Additional parameters

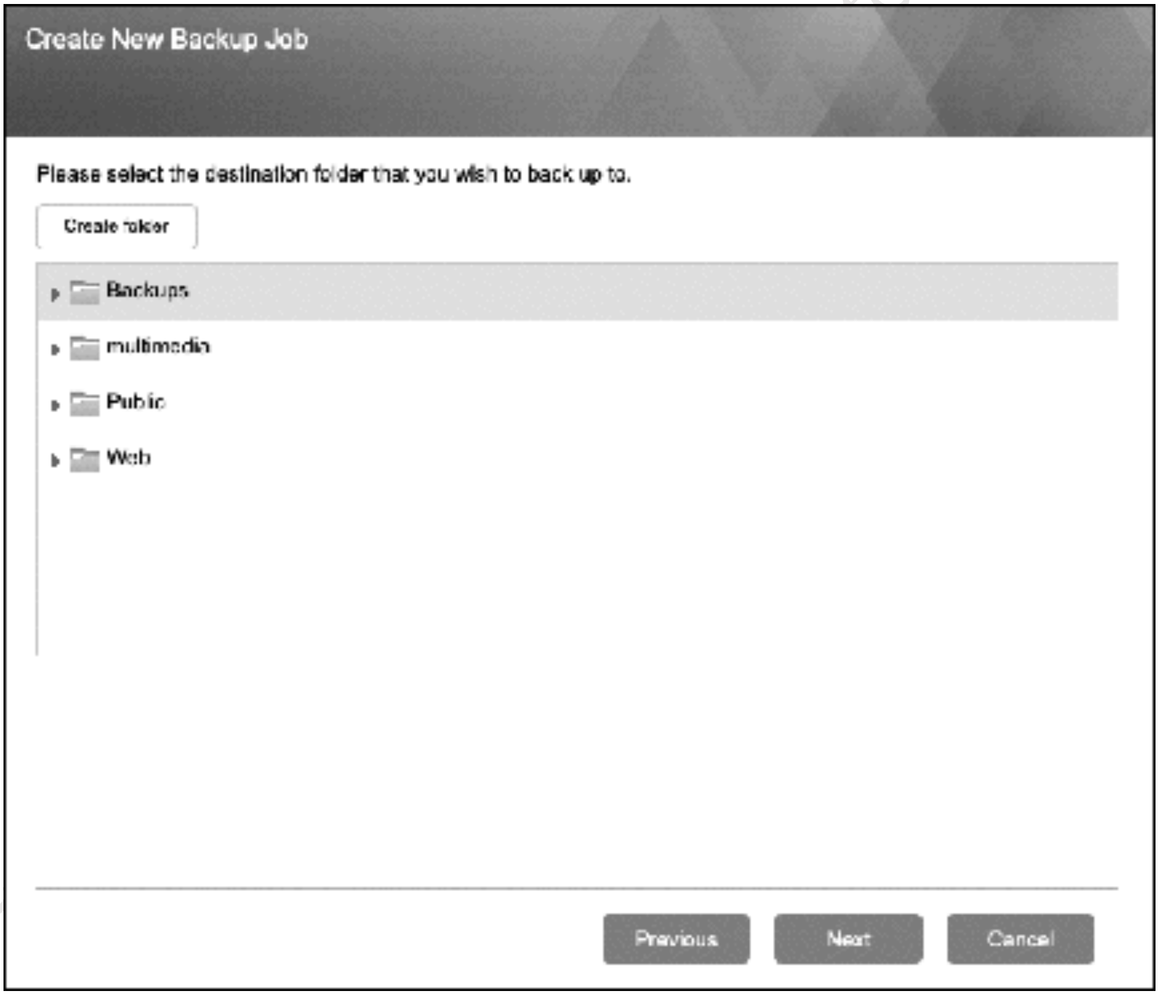
A summary screen is displayed. Assuming all is well, click **Finish** to create the job, which will then be listed in the *External Backup* panel. If you chose the ‘Back up now’ option it will run immediately, otherwise it will run at the scheduled time.

7.5 Backup to Internal Drive

In addition to or as an alternative to external backups there are also internal backups, where data is backed up from one folder to another on the server. This does not protect against drive failures in the way that external backups can, but does provide copies of data that can quickly be reverted to in the event of problems. For example, consider the following scenario: a small organization uses a weekly external backup for all of its data. However, as it makes extensive use of the shared *public* folder, it decides to add an internal backup that effectively 'clones' it each day.

It is suggested that a dedicated shared folder for the backups is created, with a meaningful name e.g. *Backups*. Creating shared folders is described in section 4.2 Adding a Shared Folder, but in summary is **Preferences** > **Shared Folders** or **Access** > **Shared Folders**. Optionally, make the folder 'Invisible in Network or My Network Places' and give the folder Read & Write access for Administrators only.

Launch **Backup & Restore** and click **Internal Backup**. The steps for internal backups are identical to those for external backups as described in the previous section, but with one key difference. When the destination folder is specified, the external drive is not listed. Instead, the internal folder structure of the server is shown, from where the *Backup* folder should be selected:



Create New Backup Job

Please select the destination folder that you wish to back up to.

Figure 99: Select destination folder for backup

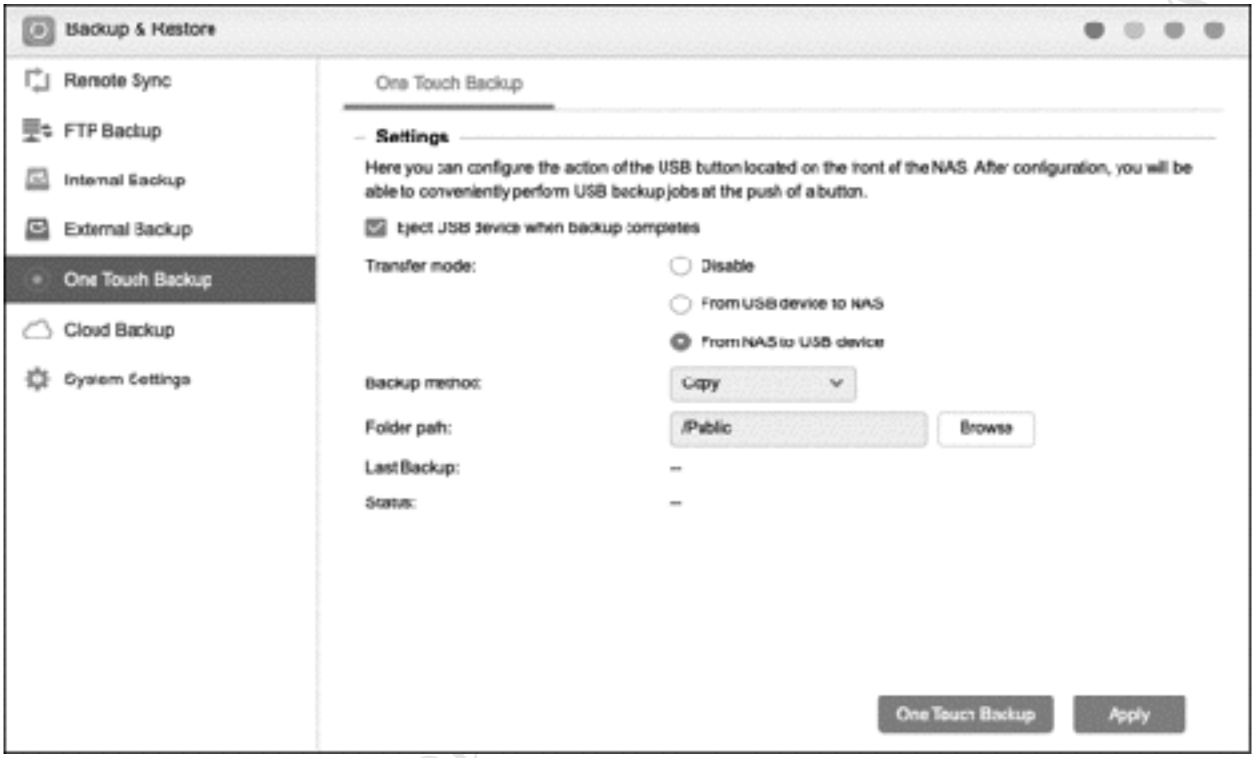
Backup jobs are listed on the *Internal Backup* panel. One potential advantage of internal backups is that they may run more quickly than external backups, depending on the disk drive types and their configuration.

As an alternative to an internal backup, you could use the snapshot feature (see 11.3 Snapshots).

7.6 One Touch Backup

Some NAS models have a front-mounted USB socket, along with a dedicated copy button and this facility can utilized as a simple backup mechanism.

Launch **Backup & Restore** and click **One Touch Backup**. Click the **From NAS to USB device** option. Set the *Backup method* dropdown to **Copy**. Choose the *Folder path* by clicking the **Browse** button – this is the folder on the NAS which you want to backup. It is suggested you tick the **Eject USB device when backup completes** box. Click **Apply**.



Settings

Here you can configure the action of the USB button located on the front of the NAS. After configuration, you will be able to conveniently perform USB backup jobs at the push of a button.

☑ Eject USB device when backup completes

Transfer mode: ○ Disable ○ From USB device to NAS ● From NAS to USB device

Backup method: Copy

Folder path: /Public

Last Backup: --

Status: --

Figure 100: One Touch Backup settings

To take a backup, insert a USB drive into the front USB socket. Wait 30 seconds for it to be recognized. Press the USB backup button for 1½ seconds and the backup will commence. Whilst the backup process is running, the USB backup LED indicator will blink continuously. Upon completion, the LED light will stop flashing. Remove the USB drive and keep it in a safe place until next time.

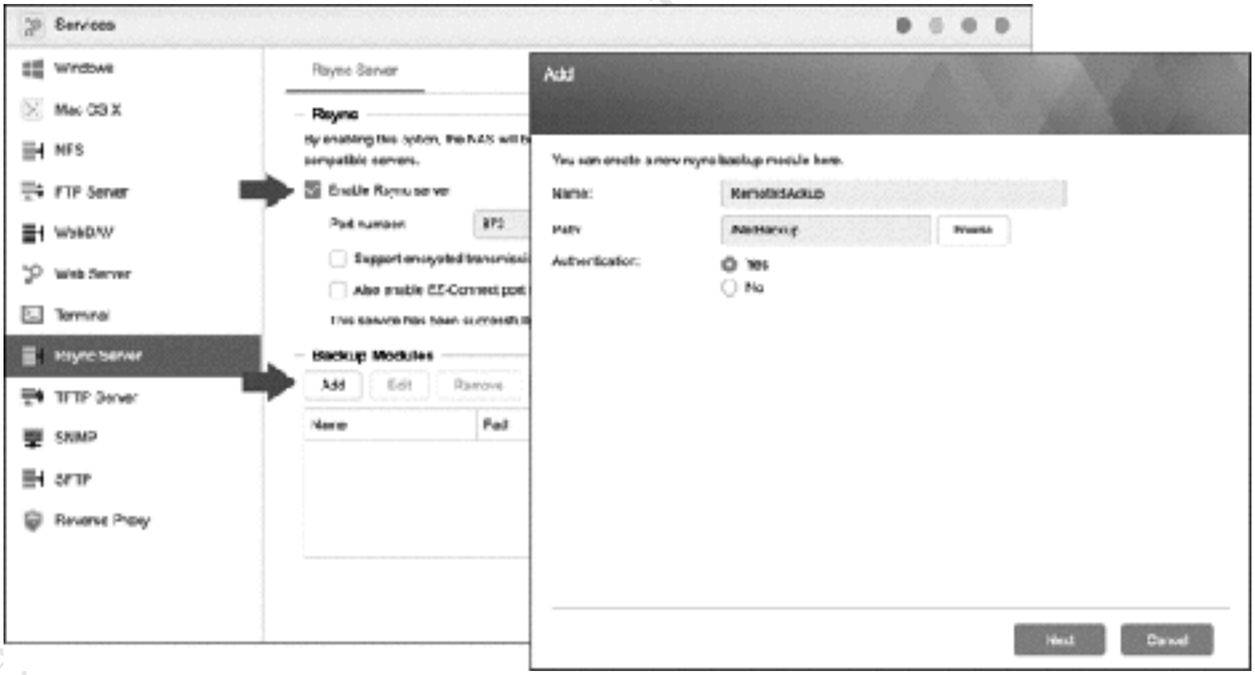
Should it ever be required to restore data, it is basically a matter of going back into the **Backup & Restore** > **One Touch Backup** screen, changing the *Transfer mode* to **From USB device to NAS**, then running a One Touch backup as described in the previous paragraph.

7.7 NAS-to-NAS Backups Using Remote Sync

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 ASUSTOR, as it is possible to use just about any brand of network attached storage and you are not restricted to ASUSTOR, although this would be the obvious and choice for most people. But consider a scenario where you are upgrading from another vendor to ASUSTOR, 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 ADM, are based on or derived from Linux. Linux itself is a derivative of UNIX, and in the UNIX world a program called Remote Sync - *rsync* – gives the capability to backup one server 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*.

Start off by enabling the network backup capability on the destination NAS. The method for doing so with ASUSTOR is as follows and if you are backing up to a different brand of NAS these exact instructions will not apply, but there should be something analogous. Create a shared folder on it called *NetBackup* and give access to the *admin* user only (creating shared folders is described in section 4.2 Adding a Shared Folder). Then, go into **Services > Rsync Server** and tick the **Enable Rsync server** box. The backup folder needs to be associated and ASUSTOR use the term 'Backup Module' to describe this. Click **Add**, give the module a name e.g. *RemoteBackup*, click **Browse** and locate the backup folder. *Authentication* should be set to **Yes**. Click **Next**:



☑ Enable Rsync server

You can create a new rsync backup module here.

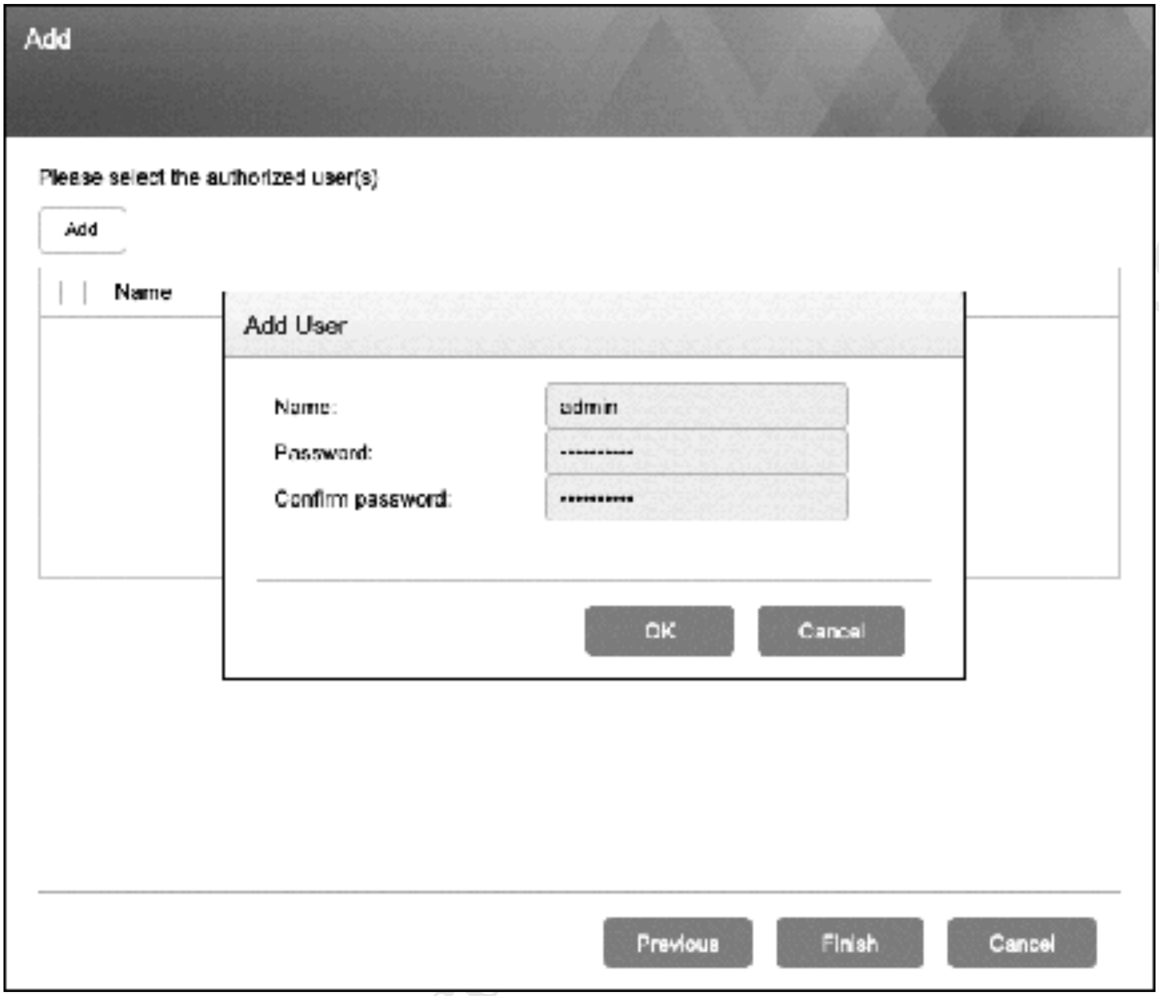
Name: RemoteBackup

Path: NetBackup

Authentication: ● Yes ○ No

Figure 101: Enable Rsync on destination server

On the following screen, click the **Add** button and specify the user that will be used with the backup module. In a small network you might choose to use the same credentials on all your servers, although in a larger setup it is better to use a dedicated account for rysnc backups. Highlight the created user and click **Finish** to return to the main Rsync Server screen.



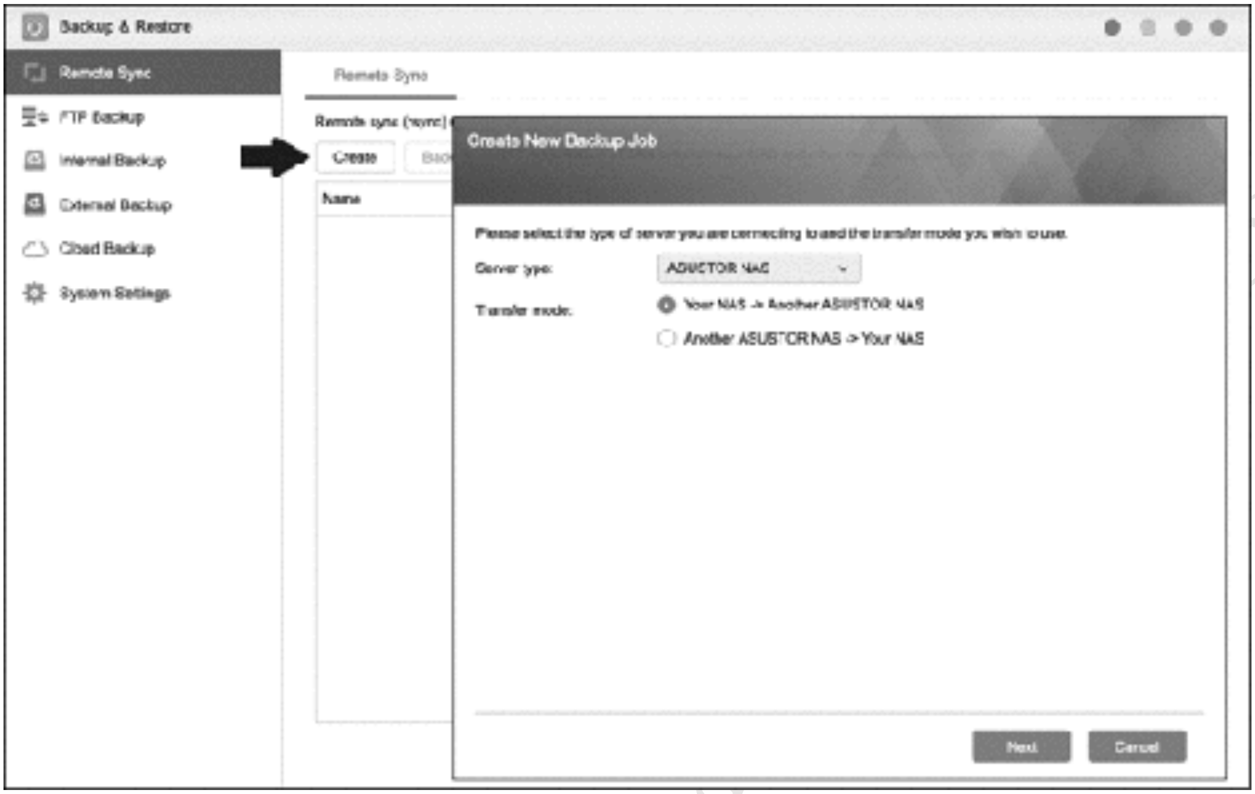
Name: admin

Password: ----------

Confirm password: ••••••••••

Figure 102: Specify the authorized user

Having setup the destination, we can now switch to the source machine. Launch **Backup & Restore** and on the **Remote Sync** tab click **Create**. Specify the *Server type* of the destination; if it is another ASUSTOR then chose *ASUSTOR NAS*, otherwise it will be *Rysnc-compatible server*. Set the *Transfer mode*; this will be **Your NAS -> Another ASUSTOR NAS** when you are backing up. Click **Next**.



Create New Backup Job

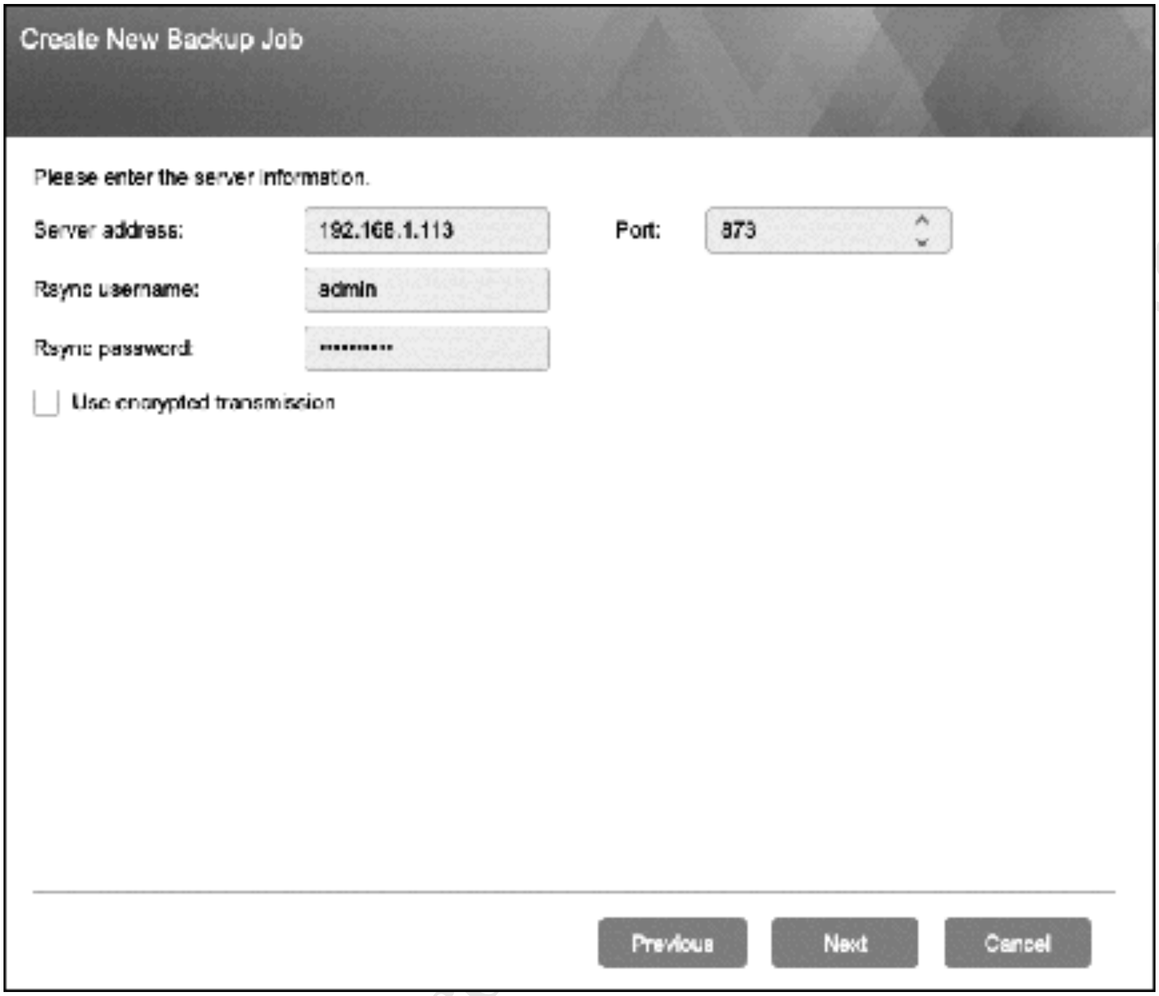
Please select the type of server you are connecting to and the transfer mode you wish to use.

Server type: ASUSTOR NAS

Transfer mode:
● Your NAS -> Another ASUSTOR NAS
○ Another ASUSTOR NAS -> Your NAS

Figure 103: Creating a new Backup job

On the subsequent panel enter the IP address of the destination server, along with the username and password that were specified earlier. Leave the Port as 873, which is standard for rsync. Click **Next**.


Create New Backup Job

Please enter the server information.

Server address: 192.168.1.113

Port: 873

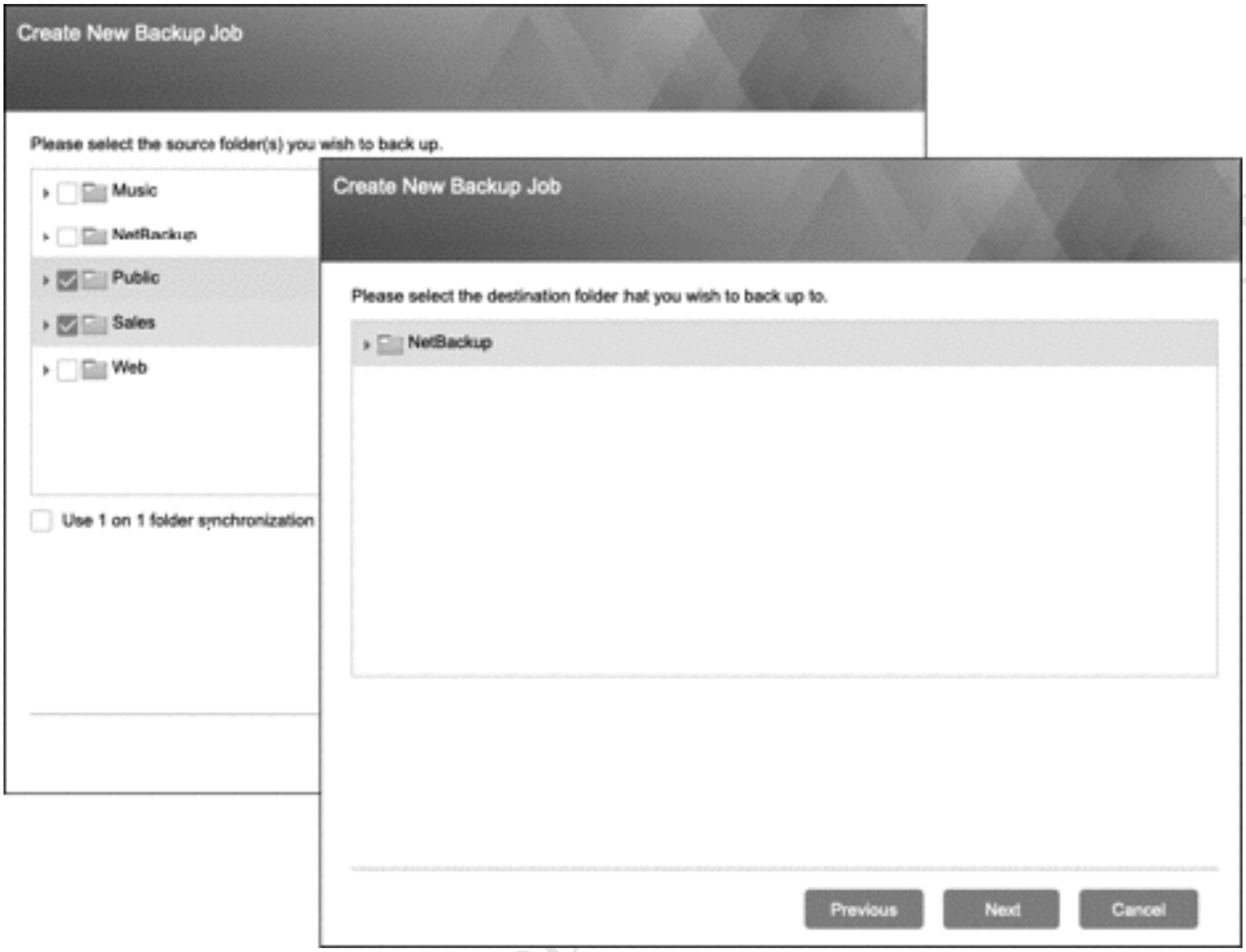
Rsync username: admin

Rsync password: ••••••••••

□ Use encrypted transmission

Figure 104: Enter details for destination server

Choose the folders to be backed up. If the *Use 1 on 1 folder synchronization* box is ticked, the folders will be backed up whenever their contents change. Otherwise it will be a conventional backup job, which is what we are doing here. Click **Next**. On the subsequent screen, select the folder on the destination server where the backup will be stored. Click **Next**:



Create New Backup Job

Please select the source folder(s) you wish to back up.

- ☐ Music
- ☐ NetBackup
- ☑ Public
- ☑ Sales
- ☐ Web

☐ Use 1 on 1 folder synchronization

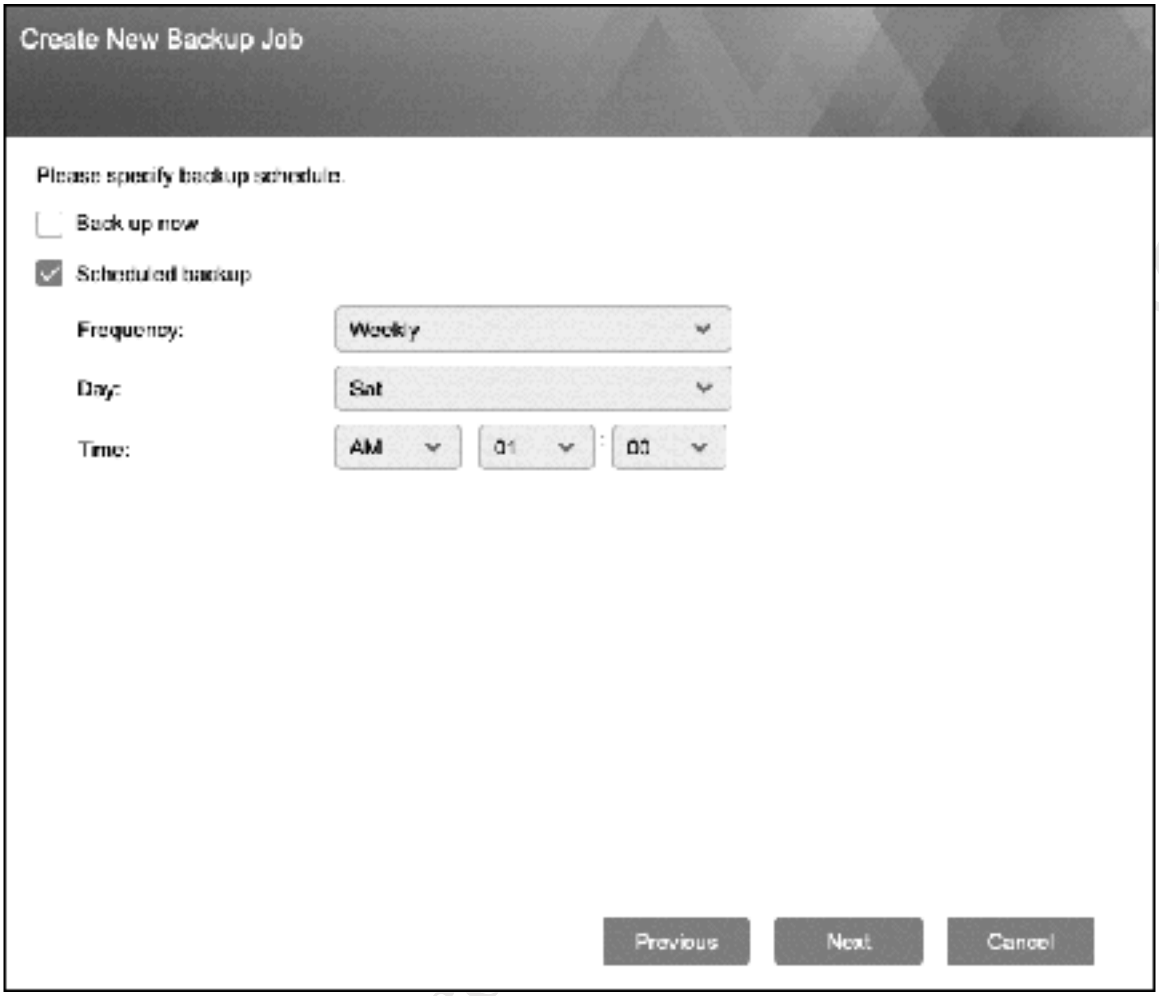
Create New Backup Job

Please select the destination folder hat you wish to back up to.

- NetBackup

Figure 105: Select the folders to be backed up and destination

The next screen enables the backup job to be scheduled. If you want to do this, tick the **Scheduled backup** box and use the dropdowns to specify the frequency and time. In this example the backup is scheduled to run weekly on a Saturday at 01:00 (1:00am). Click **Next**.



Create New Backup Job

Please specify backup schedule.

□ Back up now

☑ Scheduled backup

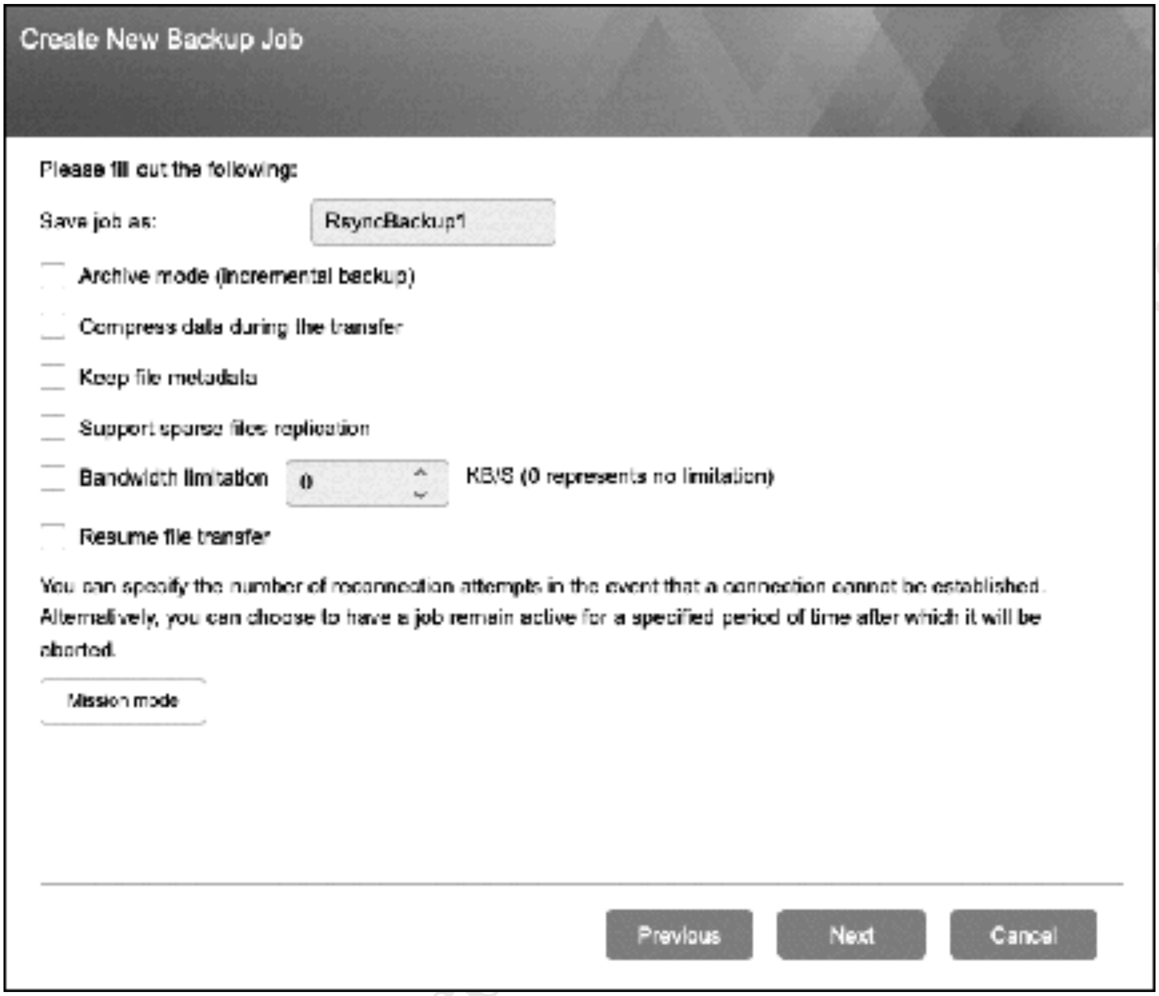
Frequency: Weekly

Day: Sat

Time: AM 01 : 00

Figure 106: Scheduling options

The backup job can be named on the subsequent screen and optional parameters specified. For instance, if *Archive mode (incremental backup)* is ticked, only data that have changed since the previous backup will be processed. Some of these options are more applicable when backing up to a NAS that is located externally at another site.



Create New Backup Job

Please fill out the following:

Save job as: RsyncBackup1

□ Archive mode (incremental backup)

□ Compress data during the transfer

□ Keep file metadata

□ Support sparse files replication

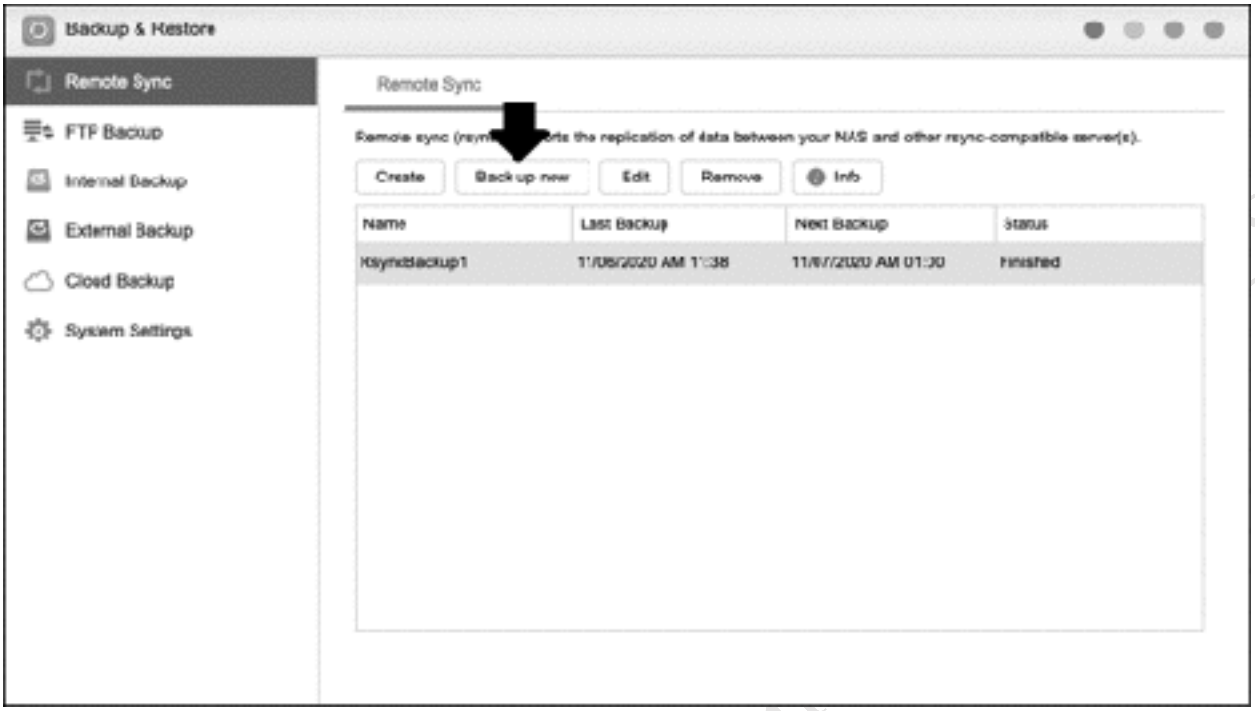
□ Bandwidth limitation 0 KB/S (0 represents no limitation)

□ Resume file transfer

You can specify the number of reconnection attempts in the event that a connection cannot be established. Alternatively, you can choose to have a job remain active for a specified period of time after which it will be aborted.

Figure 107: Optional parameters

A confirmation screen is shown. Click **Finish** and the newly created job will be listed on the main Remote Sync screen. It is a good idea to test it immediately by clicking the **Back up** now button.



Remote sync (rsyn orts the replication of data between your NAS and other rsync-compatible server(s).

Name	Last Backup	Next Backup	Status
RsyncBackup1	11/06/2020 AM 11:38	11/07/2020 AM 01:30	Finished

Figure 108: Job listed on main Sync screen

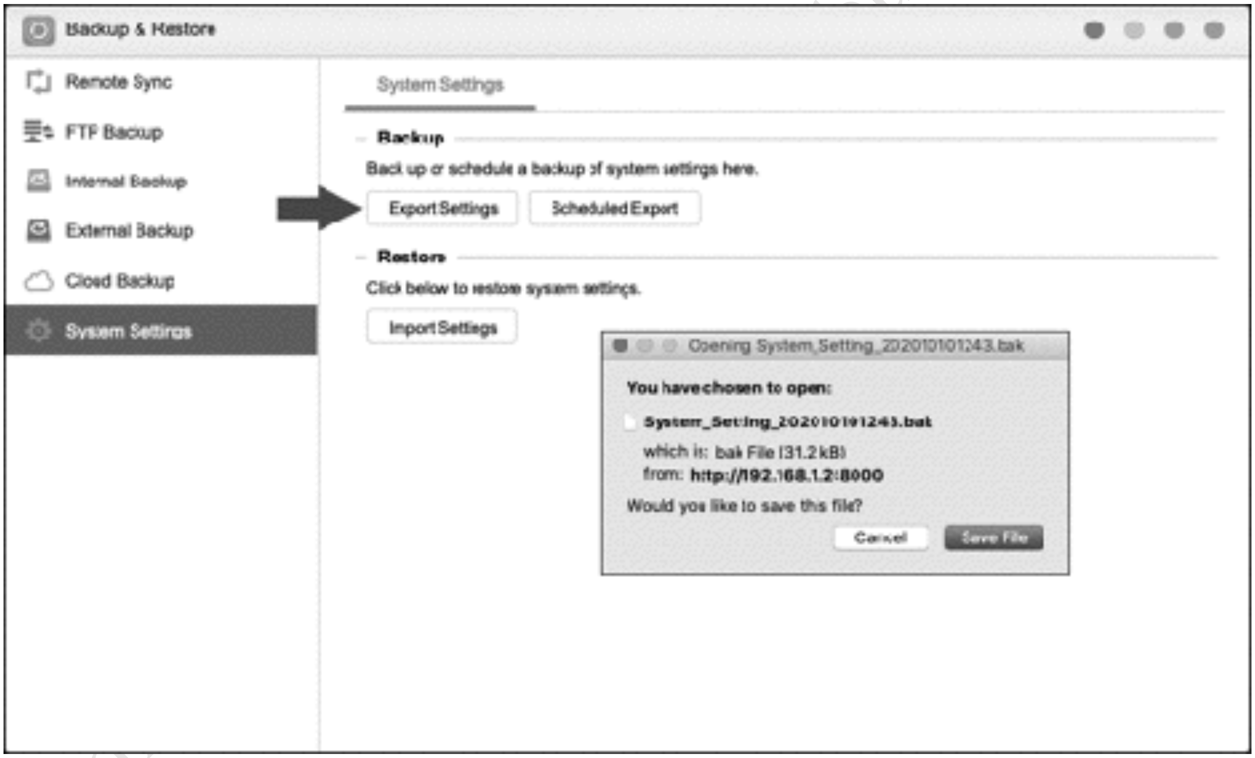
7.8 System Settings

Although we have discussed how to backup data from the server, there is another, more specialized 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 and other settings. 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 may be both difficult and time consuming on all but the simplest of systems. Fortunately, there is a facility to quickly backup and restore the configuration.

Launch **Backup & Restore** and click the **System Settings** tab. Click the **Export Settings** button. The system will process for a short while and then prompt you to save the file it has generated, with the exact message will depend upon which browser you are using. The file has a name in the form *System_Setting_yyyymmddhhmm.bak*. Keep the file in a safe place (you might want to consider putting a copy on a USB memory stick, for instance).

If desired, a schedule can be setup to export the settings on a regular basis e.g. daily, weekly, monthly. To do this, click **Scheduled Export**.

Should it ever prove necessary to use this configuration file, click the **Import Settings** button and navigate to the location of the configuration file. Then click the **OK** button.



Back up or schedule a backup of system settings here.

Click below to restore system settings.

You have chosen to open:

System_Setting_202010191243.bak

which is: bak File (31.2 kB)

from: http://192.168.1.2:8000

Would you like to save this file?

Figure 109: Backing up the System Settings

7.9 Backup Using DataSync Center and Cloud Services

Backup & Restore has a Cloud Backup option, but it is for use with Amazon's S3 (Simple Storage Service) only. They also have a separate app, called *Cloud Backup Center*, which works with Microsoft Azure, IBM Cloud, Rackspace, Alibaba and Baidu. These services are popular with larger businesses and enterprises but are not commonly used by home users and small businesses, who are more likely to use public cloud services such as those from *Dropbox*, *Google* and *OneDrive*. ASUSTOR have several apps for connecting to these individual services available from App Central, along with one called *DataSync Center* which can connect to multiple services, thus making it more flexible. Download and install it, which will place its icon on the desktop. Launch it, click **Start** and the following screen will be displayed:

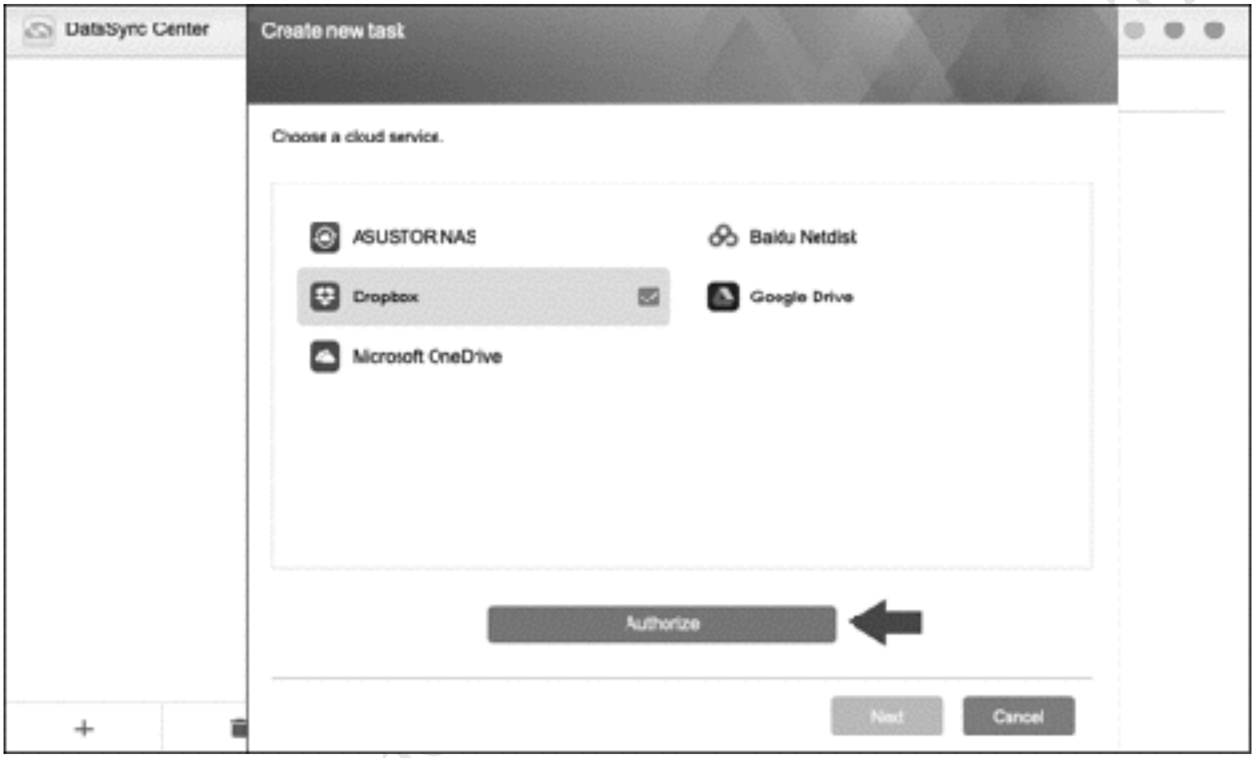
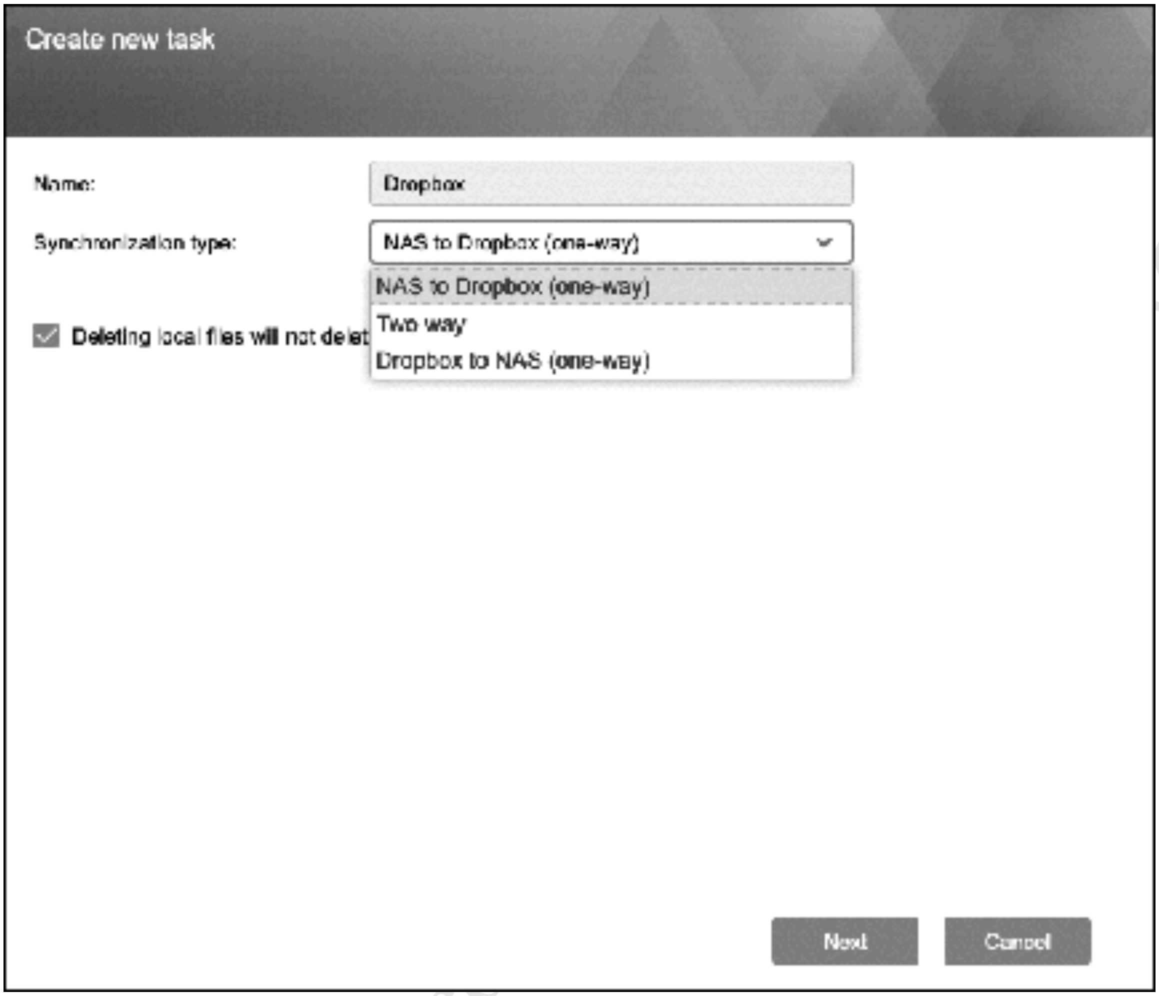


Figure 110: Choose a cloud service

Choose a cloud service and click **Authorize**. You will be prompted to login and authenticate with it, the details of which vary depending upon which one you are using. Once you have done so you will be returned to *DataSync Center* and the following panel. The *Name* defaults to the cloud service but can be changed if required.

There is a choice of *Synchronization type* using a dropdown. We are using *DataSync Center* for backing up, so we want the **NAS to Dropbox (one-way)** option (if you are using a different cloud service then that name will appear instead of *Dropbox*). However, the app can be used in other ways. If it was set to *Two way*, any changes on one side would be replicated to the other. This would enable it to provide a form of remote access to the server for offsite computer users, keeping them in sync with the server. If it was set to *Dropbox to NAS (one-way)*, the effect would be to backup the cloud data to the server, which could be useful for some individuals and organizations (you would also choose this option for restoring your backed up data, if needed). If the **Deleting local files will not delete remote files box** is ticked, permanent copies of files will be kept at the cloud end, which enables you to recover files that are accidentally deleted on the server. Click **Next**.



Create new task

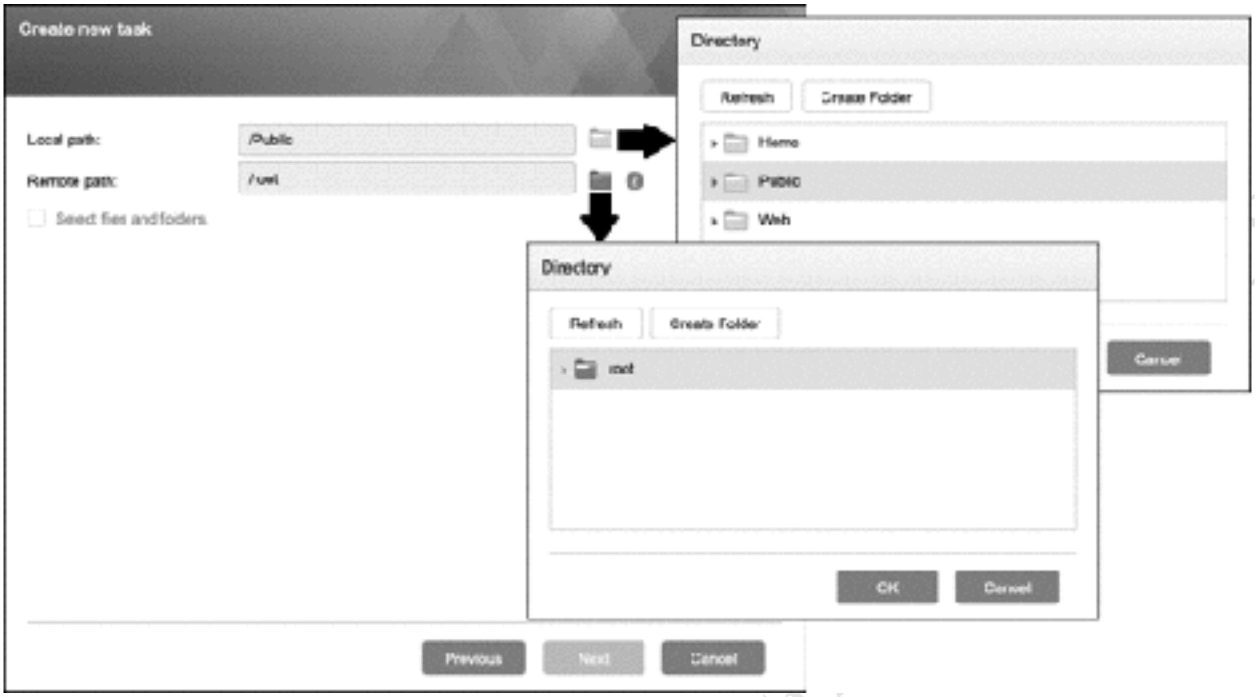
Name: Dropbox

Synchronization type: NAS to Dropbox (one-way)

☑ Deleting local files will not delet

Figure 111: Specify the Synchronization type

On the following panel, click the small icon and choose the *Local Path* – this is the folder on the NAS that you want to sync to the cloud service. By ticking the **Select files and folders** box you can specify individual files and sub-folders within in, if required. The *Remote path* is the location on the cloud; usually this is set as the top level or root (/) but you can specify an existing or create a new folder instead. Click **Next**:



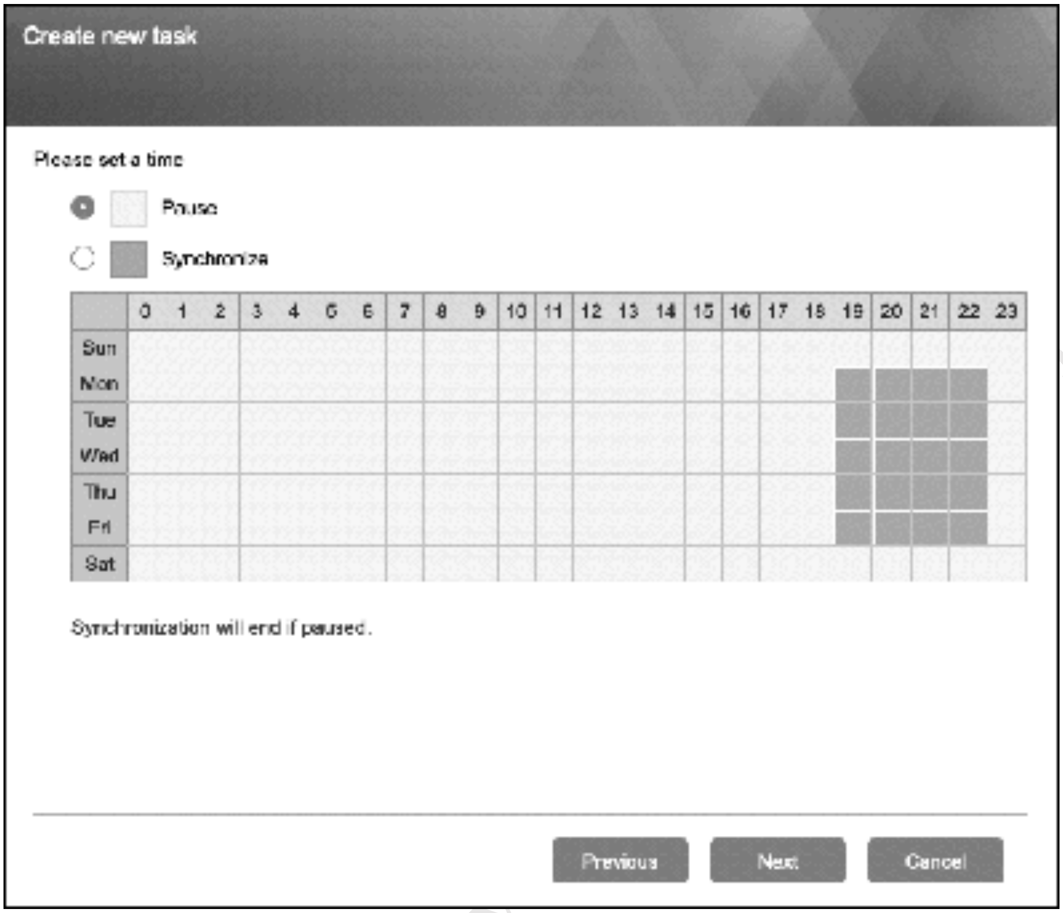
Create new task

Local path: /Public

Remote path: /usr

Figure 112: Specify local and remote paths

The next screen enables a schedule for synchronization to be set. Use the mouse to ‘paint’ the squares for when it occurs. There is no one right answer here, as it depends upon your requirements. In this example, we are syncing each evening during the week but not at all during weekends. Having specified the times, click **Next**:



Please set a time

● Pause

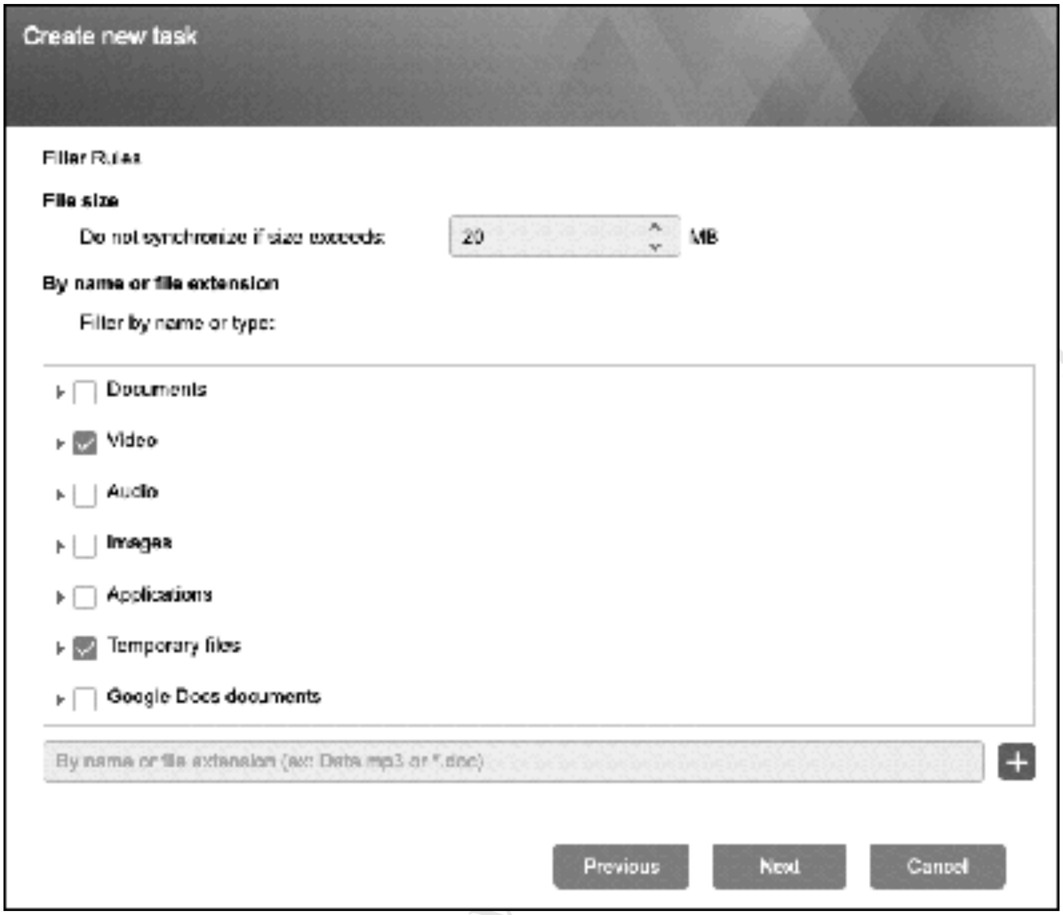
○ ▨ Synchronize

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun																								
Mon																				▨	▨	▨	▨	
Tue																				▨	▨	▨	▨	
Wed																				▨	▨	▨	▨	
Thu																				▨	▨	▨	▨	
Fri																				▨	▨	▨	▨	
Sat																								

Synchronization will end if paused.

Figure 113: Synchronization schedule

The subsequent panel enables filters to be specified. This prevents certain categories of files being synced and allows file size limits to be specified. For instance, you might not want to sync temporary files or videos greater than, say, 20 Mbytes. Each of the categories can be expanded by clicking its chevron (arrow), enabling specific file extensions to be excluded/included e.g. you could sync DOCX, PPTX and XLSX files but no other Document types. Click **Next** to continue.



Create new task

Filter Rules

File size

Do not synchronize if size exceeds: 20 MB

By name or file extension

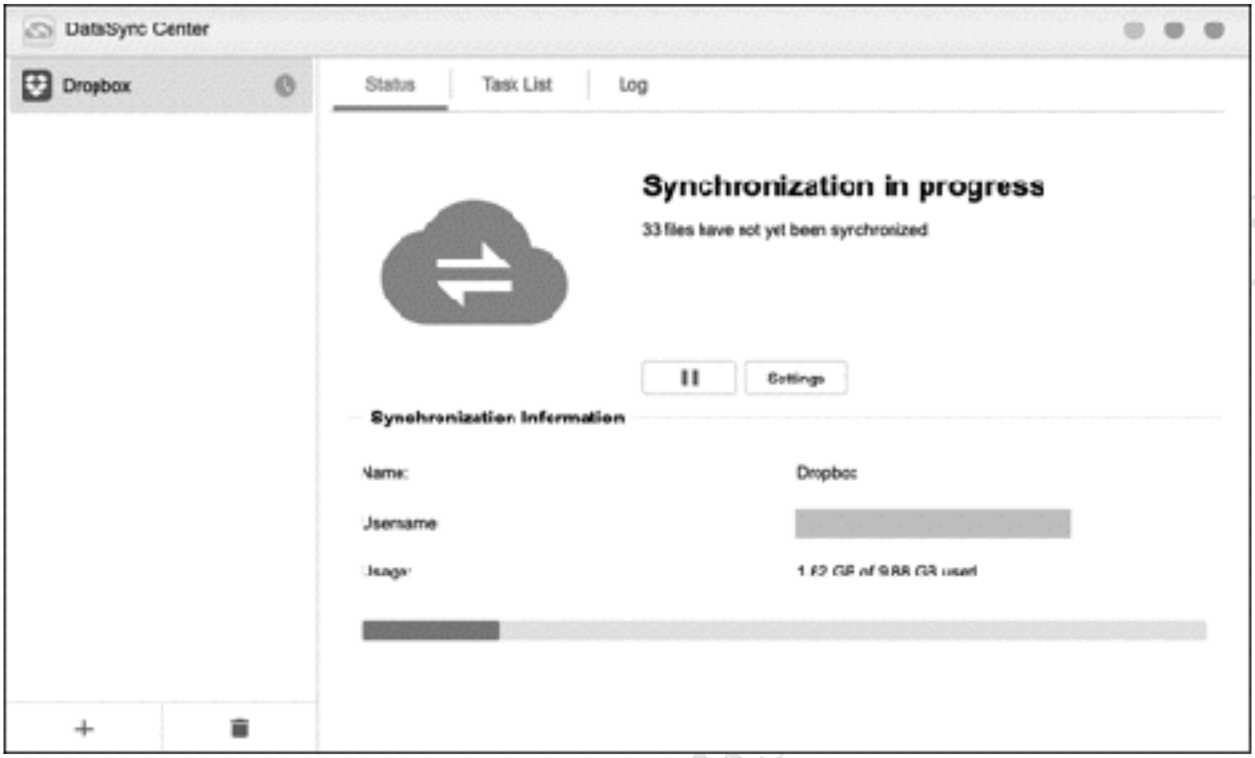
Filter by name or type:

- □ Documents
- ☑ Video
- □ Audio
- □ Images
- □ Applications
- ☑ Temporary files
- □ Google Docs documents

By name or file extension (ex: Data.mp3 or *.doc)

Figure 114: Filter Rules

A *Summary* screen is displayed. Assuming everything is okay, click **Finish** and the newly defined sync job will be listed on the main *DataSync Center* screen. There are options to pause a running job and change the Settings. A more comprehensive set of options are available from the **Task List** tab. A detailed list of all synchronization tasks can be obtained by clicking on the **Log** tab.



Synchronization in progress

33 files have not yet been synchronized

Synchronization Information

Name: Dropbox

Username [redacted]

Usage: 1.62 GB of 9.88 GB used

Figure 115: Synchronization in progress

The speed of backup to a cloud service is dependent upon the speed of your internet connection but is typically many times slower than backup to a local drive. For instance, a backup of 1 terabyte of data that might take under an hour to a USB drive might take several days over the internet. 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 common question is: as only one folder can be synced to the cloud service, 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.

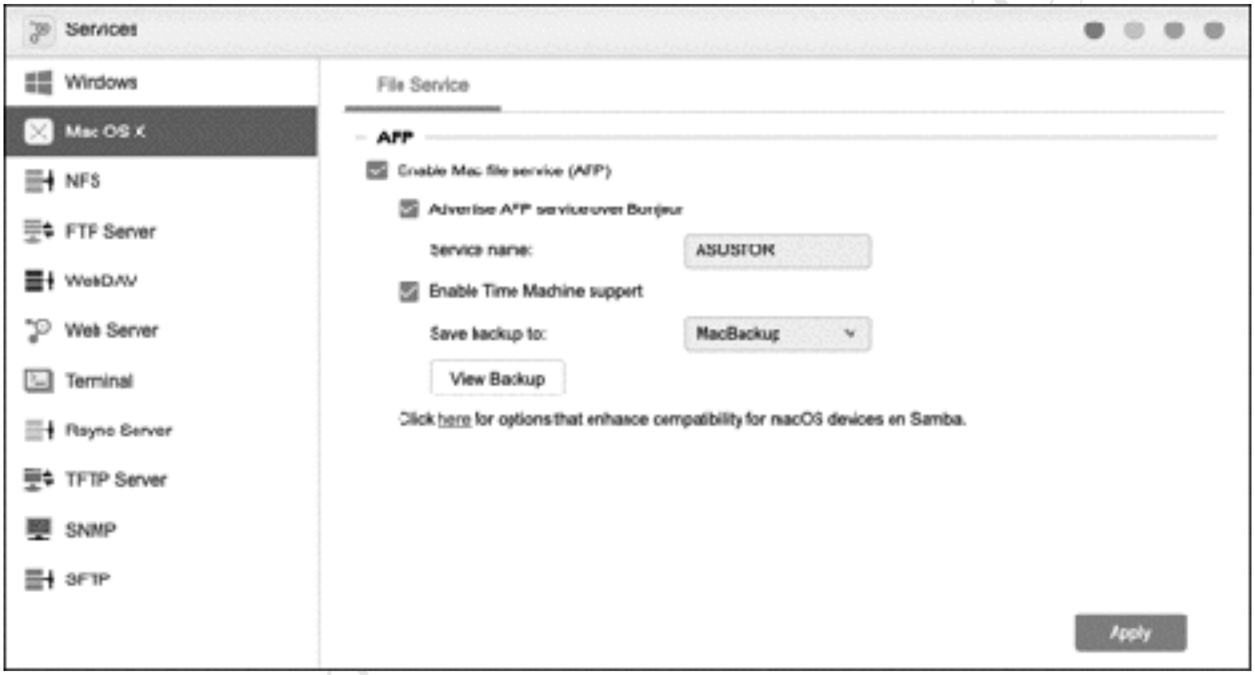
Another consideration is that you have sufficient space in the public cloud account, particularly if you are, say, a home user and making use of the limited amount of space available with free accounts. One approach is to have accounts with multiple providers, in which case you could backup some folders to Dropbox, some to Google and others to OneDrive. To create a synchronization task with another provider, click the plus sign at the bottom left-hand corner of the *DataSync Center* screen.

7.10 Backing Up Macs

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

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 4.2 Adding a Shared Folder). 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.

Launch the File Service utility and click the Mac **OS X** tab. Tick the **Enable Time Machine support** box, plus the other two boxes if they are not already ticked. Use the Save backup to dropdown to point to the newly created *MacBackup* folder. Click **Apply**.



AFP

☑ Enable Mac file service (AFP)

☑ Advertise AFP service over Bonjour

Service name: ASUSTOR

☑ Enable Time Machine support

Save backup to: MacBackup

Click here for options that enhance compatibility for macOS devices on Samba.

Figure 116: Enabling Time Machine support

To perform a backup, go to the 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 NAS.

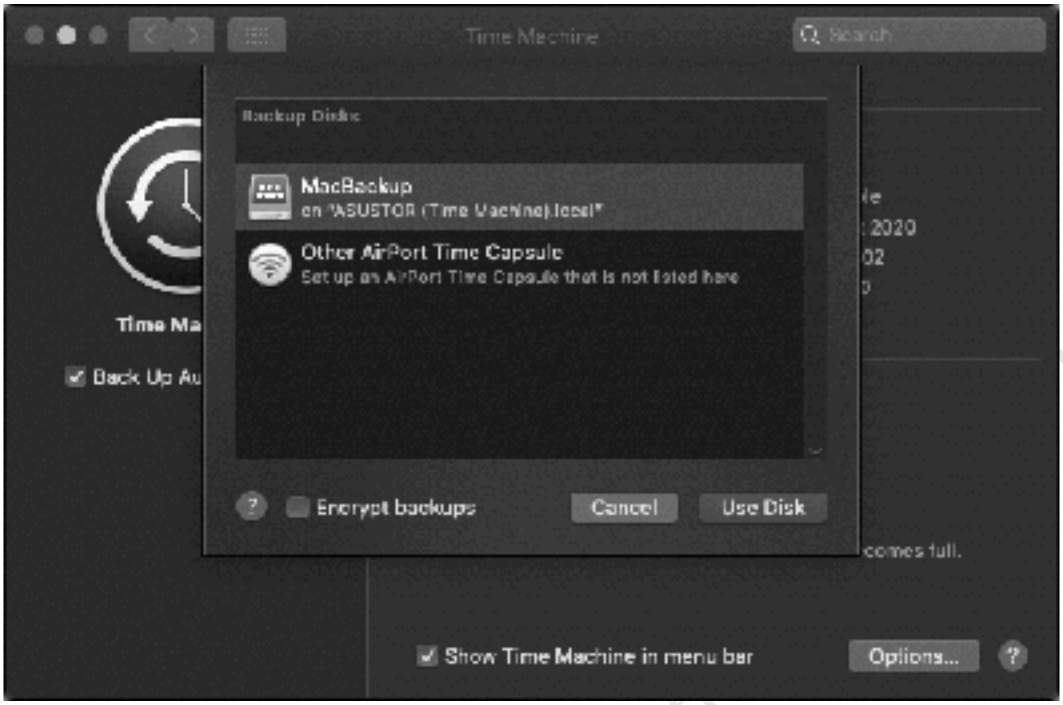
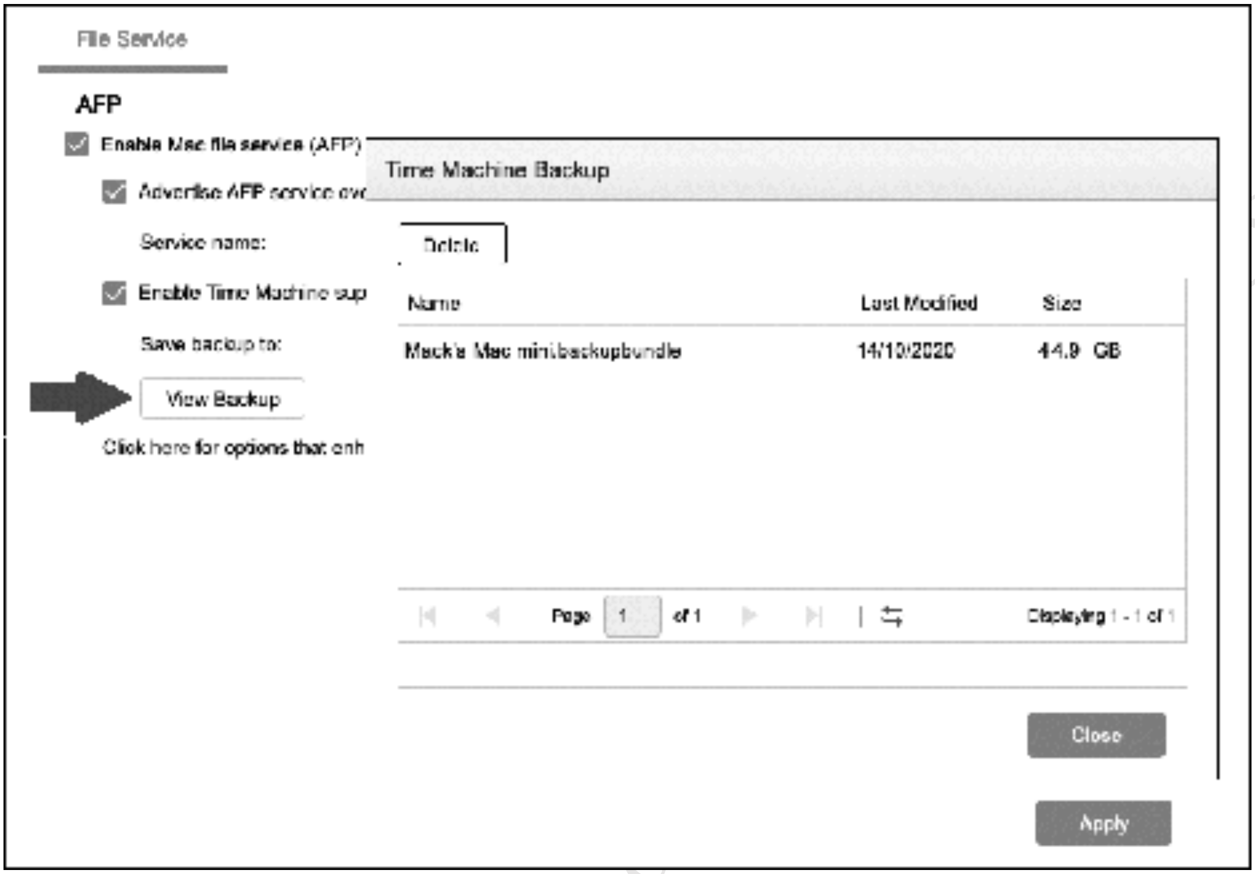

Time Machine
Search
Backup Disks
MacBackup
on "ASUSTOR (Time Machine).local"
Other AirPort Time Capsule
Set up an AirPort Time Capsule that is not listed here
Time Ma
☑ Back Up Au
? □ Encrypt backups
Cancel
Use Disk
comes full.
☑ Show Time Machine in menu bar
Options...
?

Figure 117: Select the 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 NAS. Within File Service, on the Mac OS X tab, click **View Backup** to display a list of backups. To delete a backup – for instance, for purposes of managing disk space on the server – highlight it and click **Delete**.



File Service

AFP

☑ Enable Mac file service (AFP)

☑ Advertise AFP service ove

Service name:

☑ Enable Time Machine sup

Save backup to:

Click here for options that enh

Time Machine Backup

Name	Last Modified	Size
Mack's Mac mini.backupbundle	14/10/2020	44.9 GB

Page 1 of 1

Displaying 1 - 1 of 1

Figure 118: Deleting an old backup on the server

7.11 ASUSTOR Backup Plan

ASUSTOR Backup Plan can be used for backing up Windows PCs to the server. 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, *ASUSTOR Backup Plan* 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, *ASUSTOR Backup Plan* allows any Windows PC to backup to a network.
- Different versions of Windows have different backup programs e.g. Backup & Restore in Windows 7, File History in Windows 8 and 10. *ASUSTOR Backup Plan* runs on all versions of Windows, including some older versions, making it a consistent solution.

It is not necessary to install any additional components on the server to use it, as everything is done by the Windows client program.

Installation and Getting Started

Download *ASUSTOR Backup Plan* from the ASUSTOR website and accept all the defaults during installation. Having launched it, click **Create**. It has the ability to backup data from the PC to several different types of destination – choose ASUSTOR NAS:

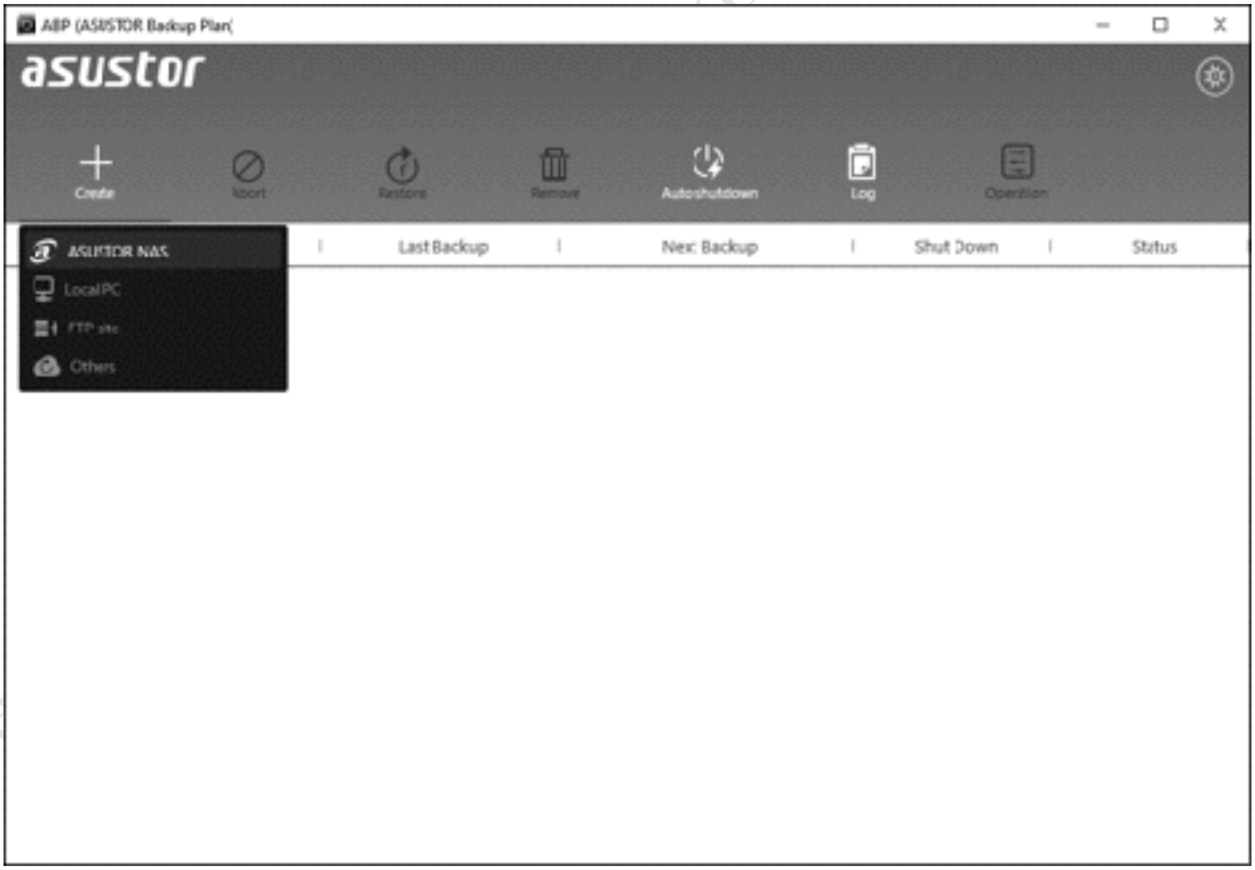
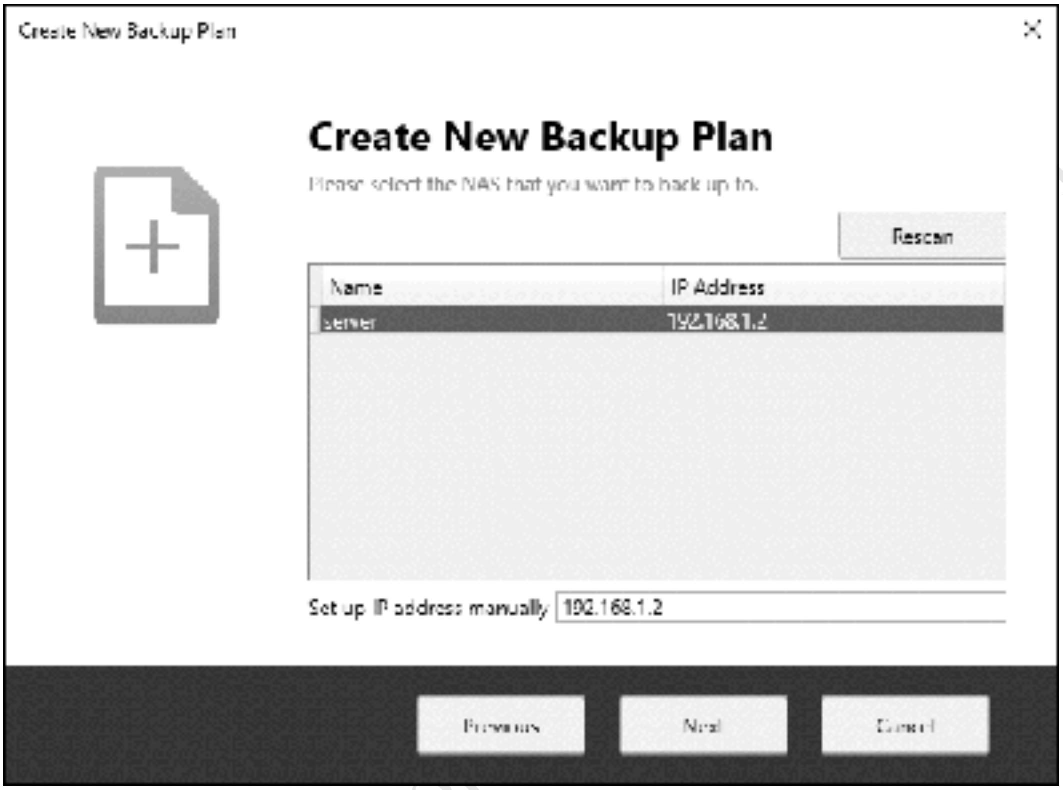


Figure 119: ASUSTOR Backup Plan main screen

Specify a name for the new backup plan and click **Next**. On the subsequent screen choose the NAS where the backups will be stored. If the server is not listed, click **Rescan** as it might just be a timing issue. Alternatively, you can enter the address of the server manually. Click **Next**. You will be prompted to provide your user name and password, as previously defined on the server (this is unconnected with any login credentials you might have on the computer itself).



Create New Backup Plan

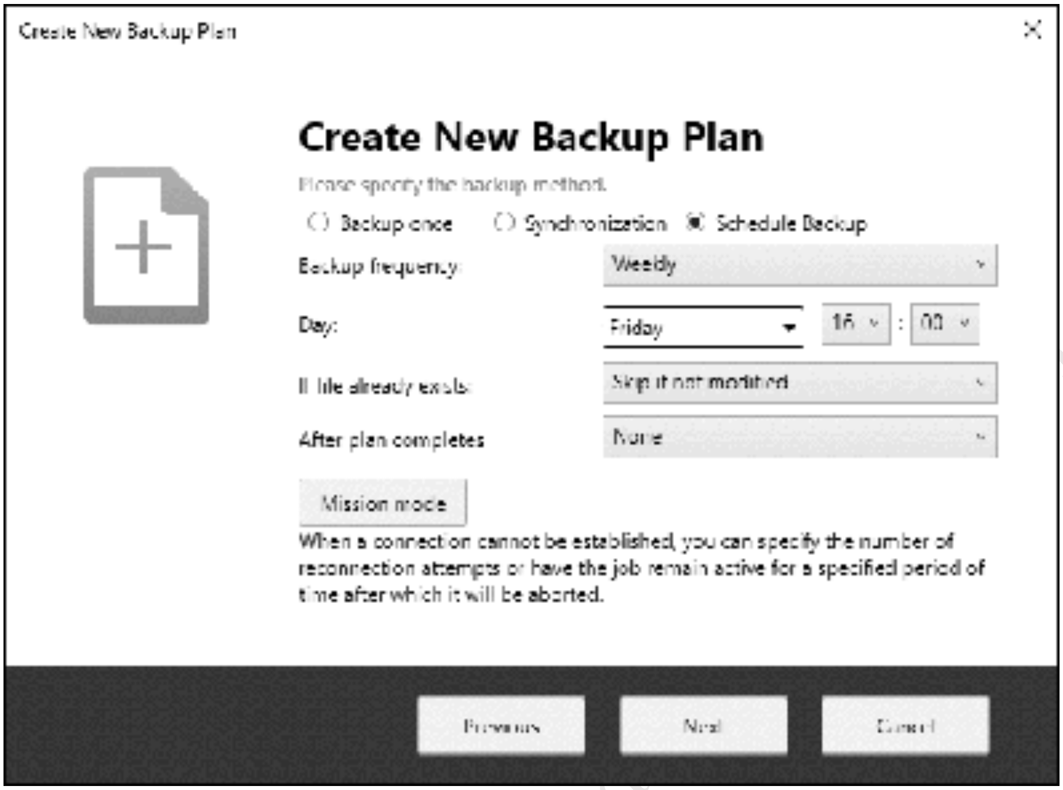
Please select the NAS that you want to back up to.

Name	IP Address
server	192.168.1.2

Set up IP address manually 192.168.1.2

Figure 120: Choose the server

On the subsequent panel, specify the backup method. This can be a one-off backup, synchronization, where any changes on the PC are mirrored to the server, or a scheduled backup, which we will choose. Specify the backup frequency, such as daily, weekly or monthly and enter its details. In this example we are defining a weekly backup, which will run on Fridays at 16:00 (4:00pm). Choose what to do a file already exists on an earlier backup, the choice is to skip it if it has not been subsequently modified or overwrite it. You can also choose what happens once the job has completed (in this example, nothing). Having defined the backup method and its parameters, click **Next**:



Create New Backup Plan

Create New Backup Plan

Please specify the backup method.

○ Backup once ○ Synchronization ● Schedule Backup

Backup frequency: Weekly

Day: Friday 16 : 00

If file already exists: Skip if not modified

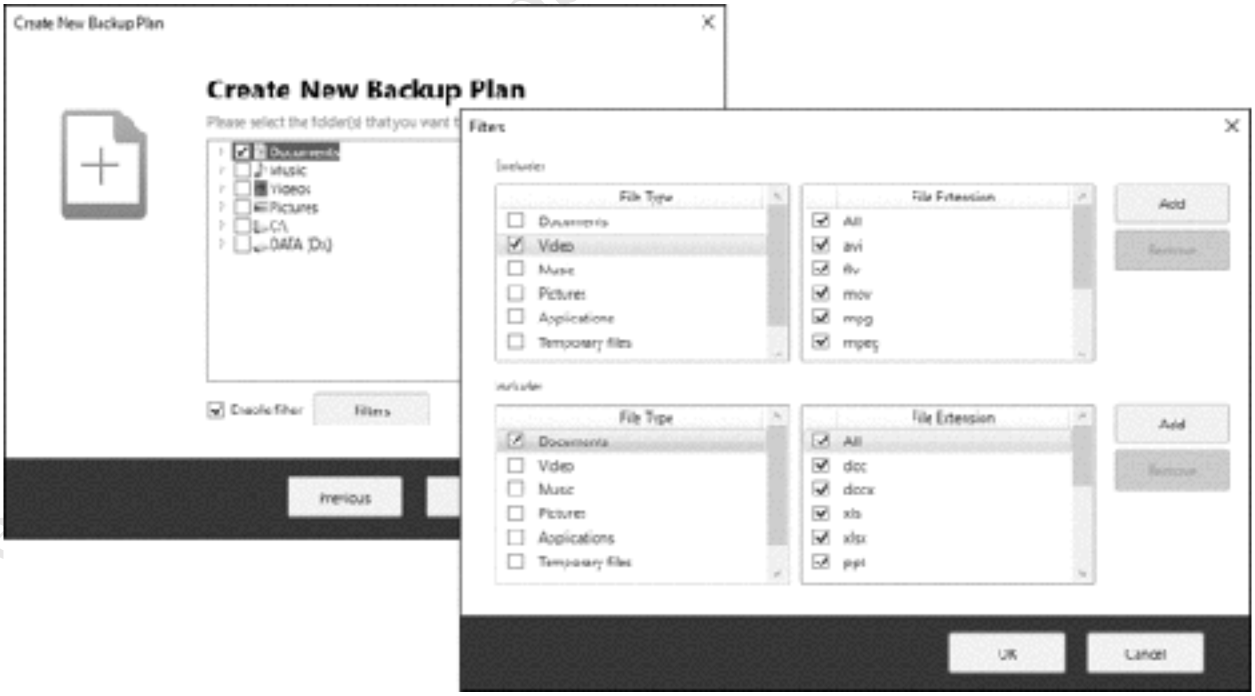
After plan completes: None

Mission mode

When a connection cannot be established, you can specify the number of reconnection attempts or have the job remain active for a specified period of time after which it will be aborted.

Figure 121: Specify the backup method

On the next panel, choose the items on the PC to be backed up e.g. the Documents folder. Optionally, specific file types can be included/excluded by clicking **Filters** and making a choice on the resultant panel:



Create New Backup Plan

Create New Backup Plan

Please select the folder(s) that you want t

☑ Documents
□ Music
□ Videos
□ Pictures
□ C:\
□ DATA (D:)

☑ Enable filter

Filters

Exclude:

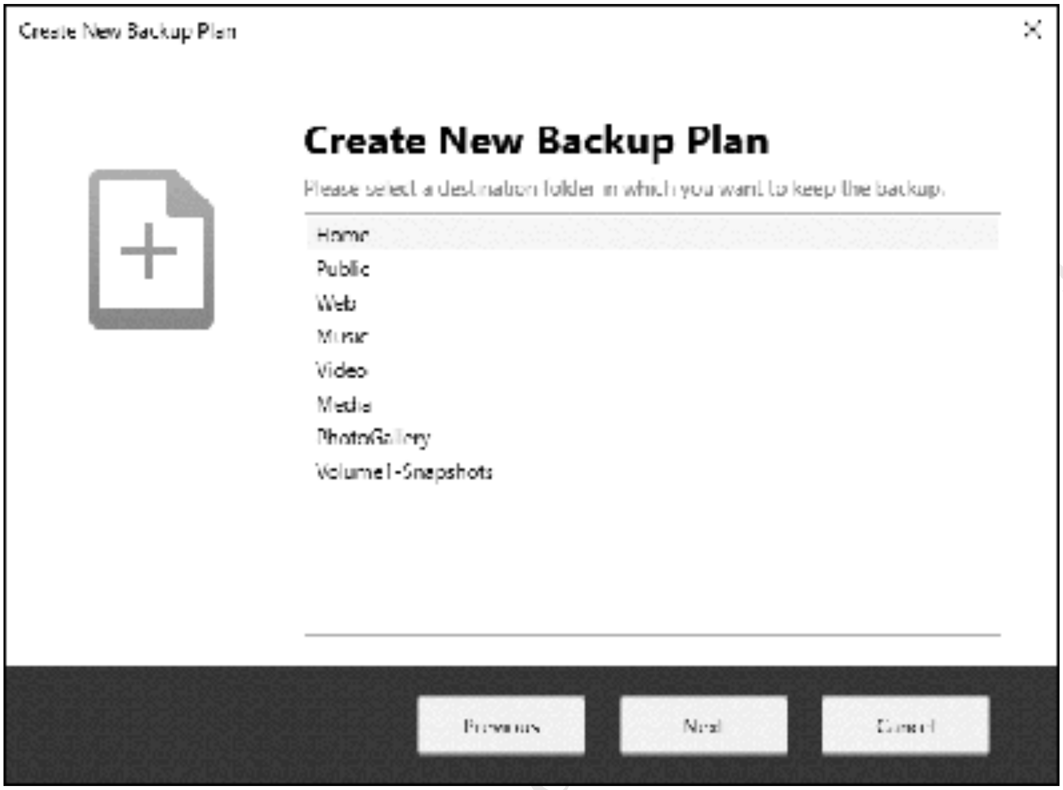
File Type	File Extension
□ Documents	☑ All
☑ Video	☑ avi
□ Music	☑ flv
□ Pictures	☑ mov
□ Applications	☑ mpg
□ Temporary files	☑ mpeg

Include:

File Type	File Extension
☑ Documents	☑ All
□ Video	☑ doc
□ Music	☑ docx
□ Pictures	☑ xls
□ Applications	☑ xlsx
□ Temporary files	☑ ppt

Figure 122: Choose the categories to be backed up

The final step is to specify the destination for the backup. The best choice is usually the *home* folder, as this is unique to each user. Click **Next**.



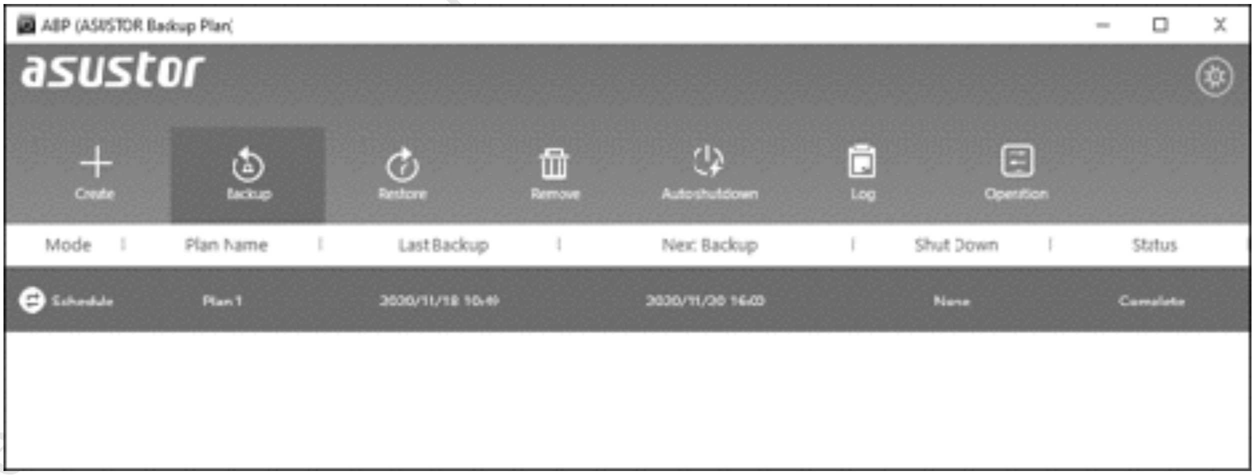
Create New Backup Plan

Please select a destination folder in which you want to keep the backup.

- Home
- Public
- Web
- Music
- Video
- Media
- PhotoGallery
- Volume1-Snapshots

Figure 123: Select the destination folder

The newly defined backup plan will now be listed on the main screen. In the case of a scheduled backup, rather than wait for the designated time you might want to click the **Backup** icon to run it immediately to ascertain that it is working correctly.

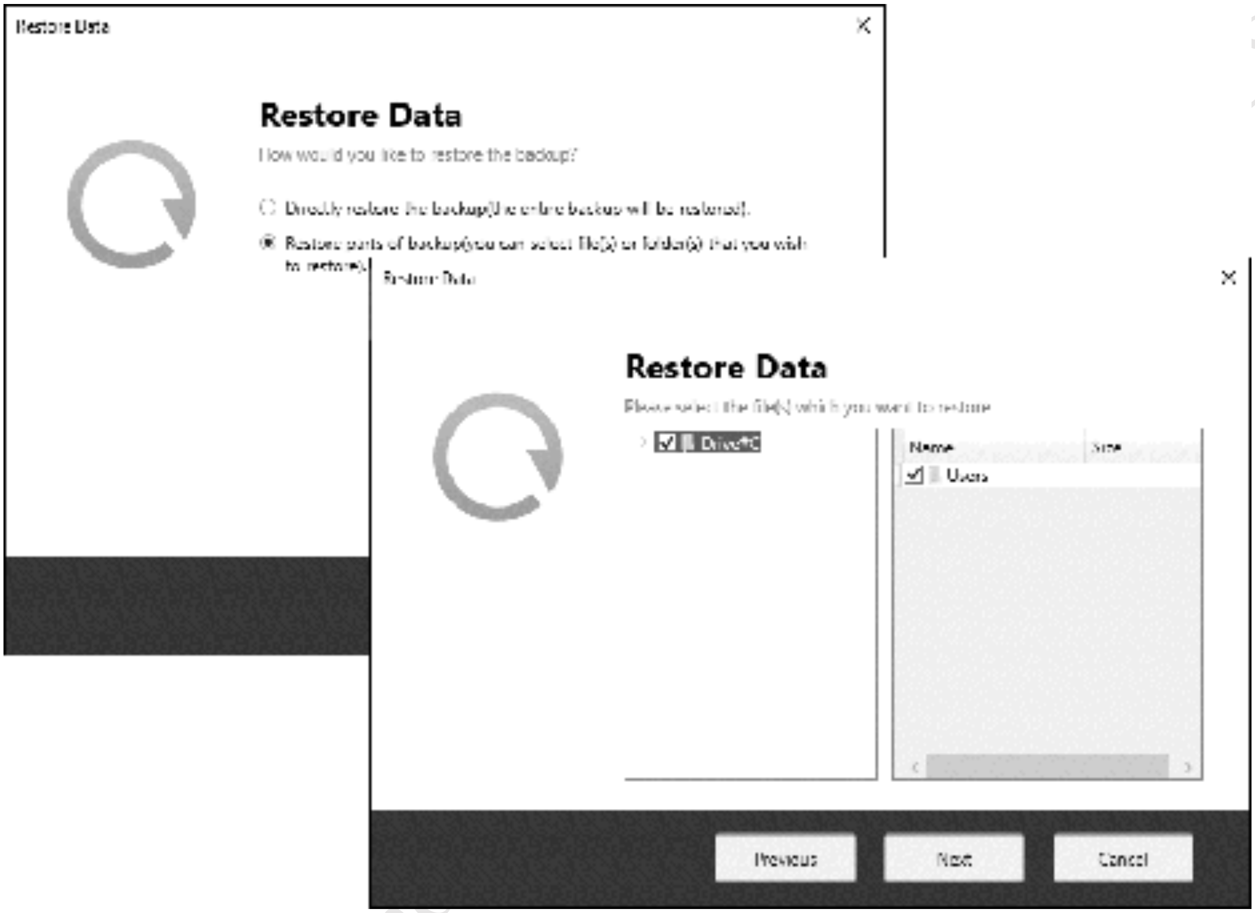


Mode	Plan Name	Last Backup	Next Backup	Shut Down	Status
Schedule	Plan 1	2020/11/18 10:49	2020/11/30 16:00	None	Complete

Figure 124: Backup plan listed on main screen

Restoring from a Backup

To restore data from a backup, click the **Restore** icon. Choose whether to restore an entire backup or selected files and folders (in this example we are doing the latter) and click **Next**. On the next panel, choose the items to restore:



Restore Data

Restore Data

How would you like to restore the backup?

○ Directly restore the backup(the entire backup will be restored).

● Restore parts of backup(you can select file(s) or folder(s) that you wish to restore).

Restore Data

Restore Data

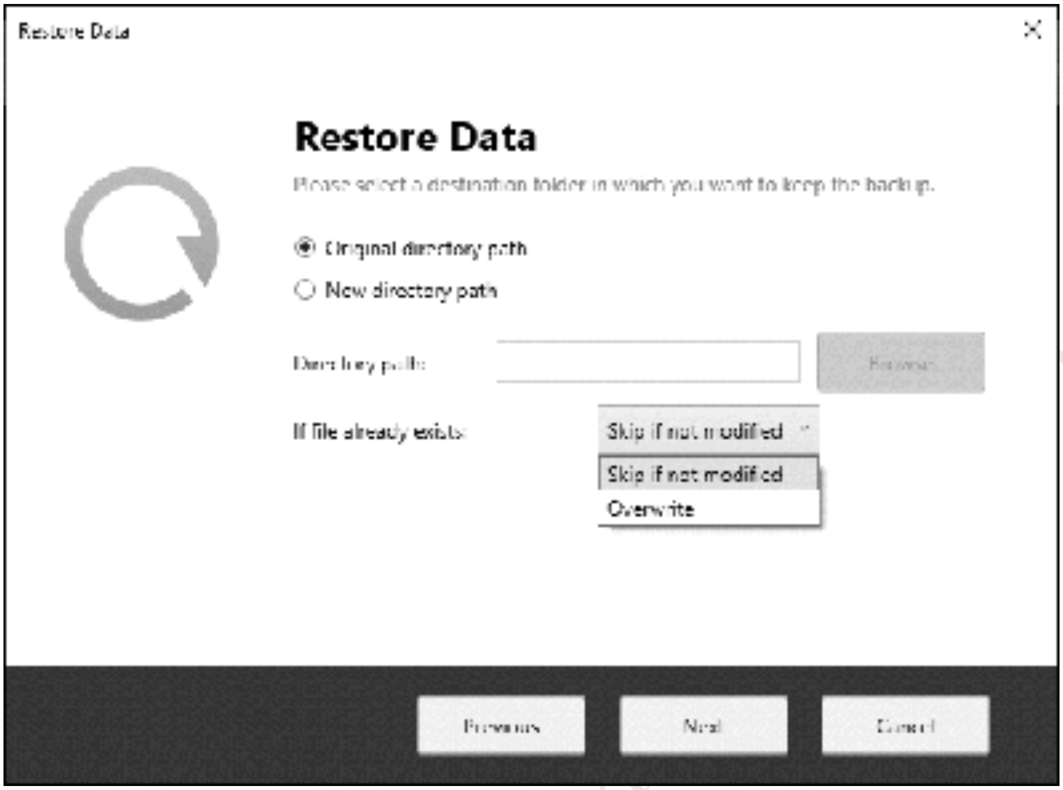
Please select the file(s) which you want to restore

☑ Drive#C

Name	Size
☑ Users	

Figure 125: Restoring data

The following panel is for specifying where the data will be restored to. This could be to the original location on the PC folder that was backed up, referred to as the original directory path, but you could restore it to a different place. 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 Explorer. You can also choose what happens if a file already exists: skip if it has not been modified since the backup, else overwrite regardless. Click **Next** and the restore will run immediately.



Restore Data

Restore Data

Please select a destination folder in which you want to keep the backup.

● Original directory path

○ New directory path

Directory path:

If file already exists: Skip if not modified

Figure 126: Choose where the data will be restored to

7.12 Backing up Computers using built-in Windows Backup Programs

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 and familiarity. However, only Professional (and not Home) editions 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 10 Professional Clients

Begin by mapping the user's home drive on the server using one of the techniques described in section 5 ACCESSING THE SERVER if not already mapped.

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 is 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); change the retention period for the backed-up data.

Windows 8 & 8.1 Professional Clients

Go into the **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 7 Professional Clients

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

Click on **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 suitable 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, in this example every Sunday at 7:00pm. If this setting is not suitable it can be altered by clicking **Change settings**.

8

HOUSEKEEPING & MAINTENANCE

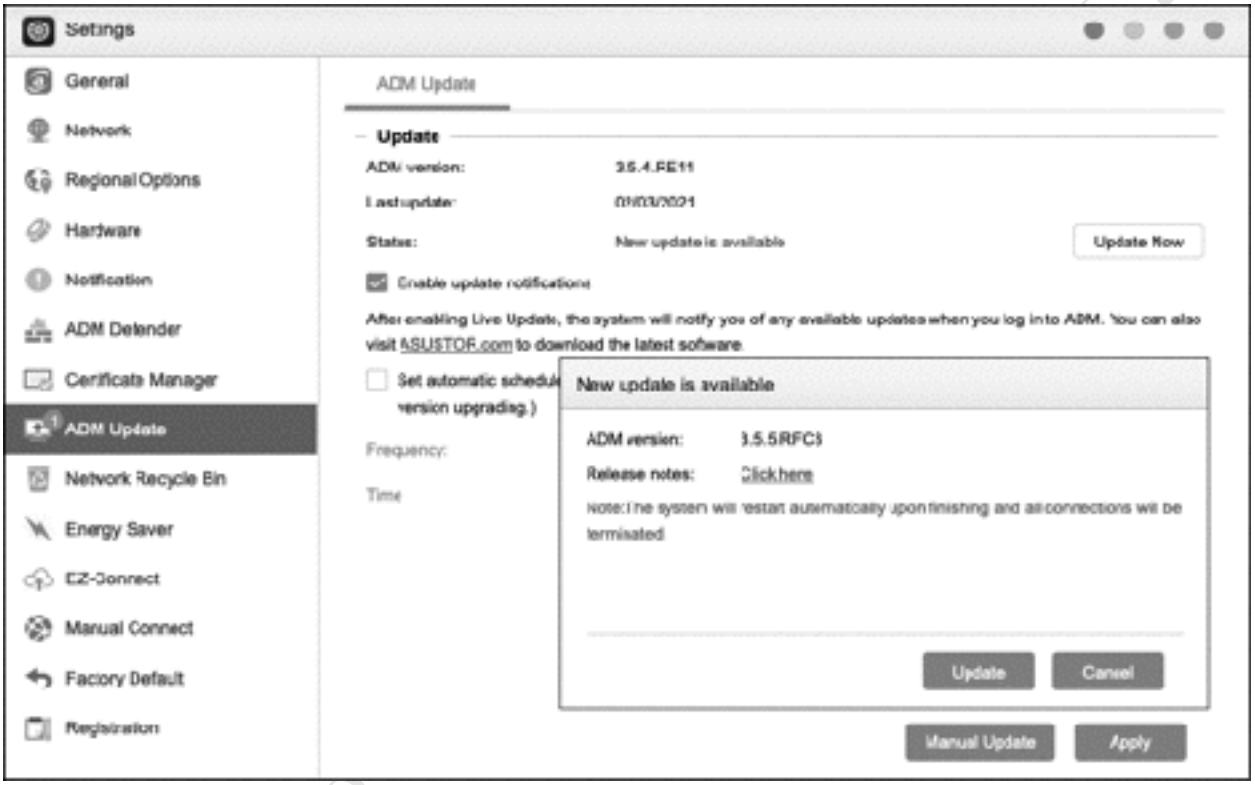
8.1 Overview

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 depending on its scale and importance. Things that can be usefully looked at include checking for ADM Updates; storage space; health of the disk drives; confirmation that the backup has completed successfully; log files; potential security issues and violations. ASUSTOR provide a variety of tools and methods to do so.

8.2 Checking for ADM Updates

The ADM software is updated on a regular basis by ASUSTOR. Updates may be major e.g. from ADM 3 to ADM 4, although typically these only occur every couple of years. Significant updates e.g. from ADM 3.5 to 3.6 are more frequent, typically once a year. ASUSTOR also make minor updates available on a regular basis – often these address potential security issues and so the best strategy is generally to be running the latest release of ADM.

If an update is available, it will be indicated in two ways: a message is displayed when logging in as an admin user and by the appearance of a notification on the ADM Update icon within **Settings**. On the **ADM Update** screen, the **Enable update notifications** box should be ticked.



ADM version: 3.5.4.RE11

Last update: 01/03/2021

Status: New update is available

☑ Enable update notifications

After enabling Live Update, the system will notify you of any available updates when you log into ADM. You can also visit ASUSTOR.com to download the latest software.

□ Set automatic schedul... version upgrading.)

New update is available

ADM version: 3.5.5.RFC3

Release notes: Click here

Note: The system will restart automatically upon finishing and all connections will be terminated.

Figure 127: Firmware Update available

Updates can optionally be checked for and performed on a scheduled basis. To enable this, tick the **Set automatic scheduled updates** box and choose the frequency and time using the dropdown; the choice is Daily, Weekly, Monthly or each time the NAS is powered on. However, as stability is desirable, especially in business and larger networks, you may not wish to do so.

One thing to remember is that firmware updates necessitate a reboot of the system. It is therefore suggested that they are performed at a time when nobody needs to use the system, so as to minimize disruption. It is also advised that a complete backup of the data and server configuration is made before updating ADM, using the techniques described in chapter 7 BACKUPS.

Downgrading to Earlier Version of ADM

One question which is sometimes asked is: Is it possible to downgrade the version of ADM, e.g. from 3.5 to 3.4 e.g. to meet a specific requirement and the answer is ‘no’. When ADM is installed or upgraded, flash memory inside the NAS is updated. As part of the installation, this memory is checked and the process will not proceed if it detects that a more modern version has previously been used. It is important to be aware of this if you want to try installing a beta version of ADM, for example, as you will not subsequently be able to revert to an earlier release.

Checking from within AiMaster

To check for updates from within AiMaster, tap the **Settings** wheel and then tap **ADM Update** from the dropdown menu that is shown.

8.3 Tools

In the top right-hand corner of the screen is an icon that looks like a small dial or speedometer and which, when clicked, shows the *Tools*. These are widgets which provide an ‘at a glance’ overview of the health and status of the server. Initially the Tools panel is empty – click on the plus (+) sign to populate it from the available selection. If the cursor is hovered over a tool, two mini icons appear in its top right-hand corner, one to close it and the other to open the underlying app or utility that feeds it and provides more detailed information and configuration options.

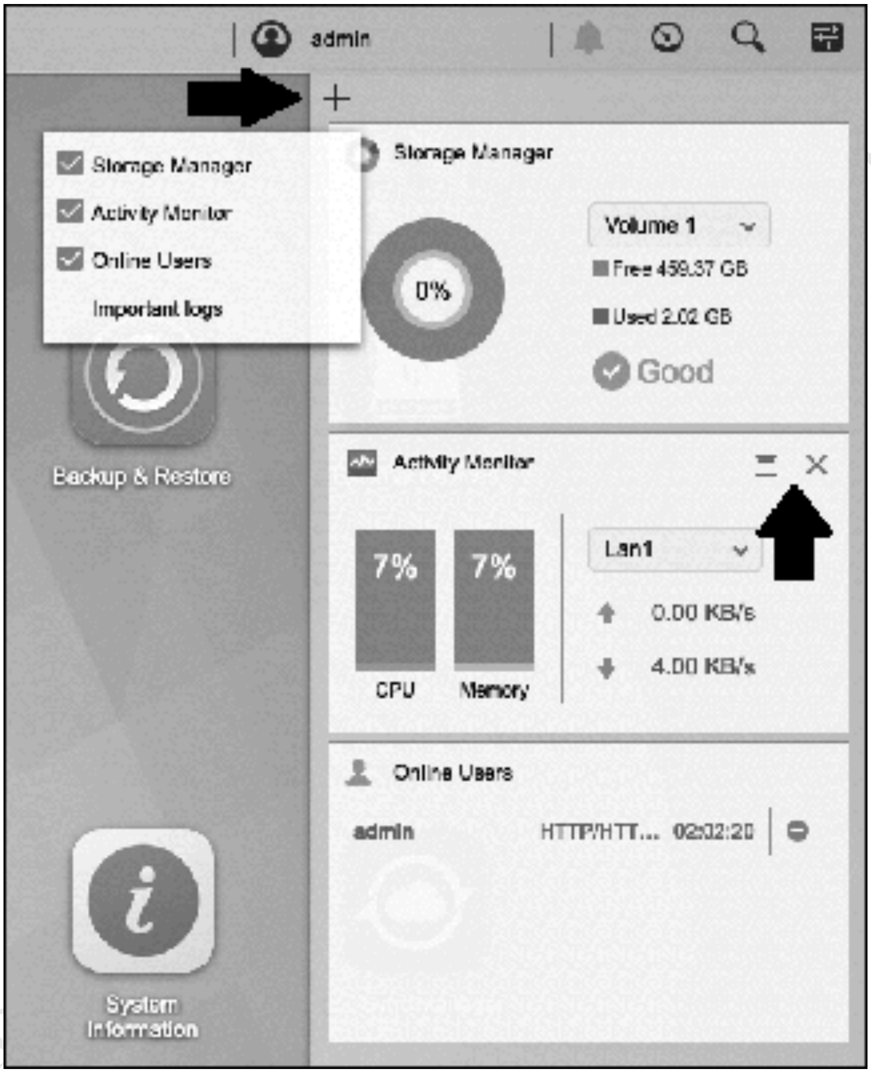
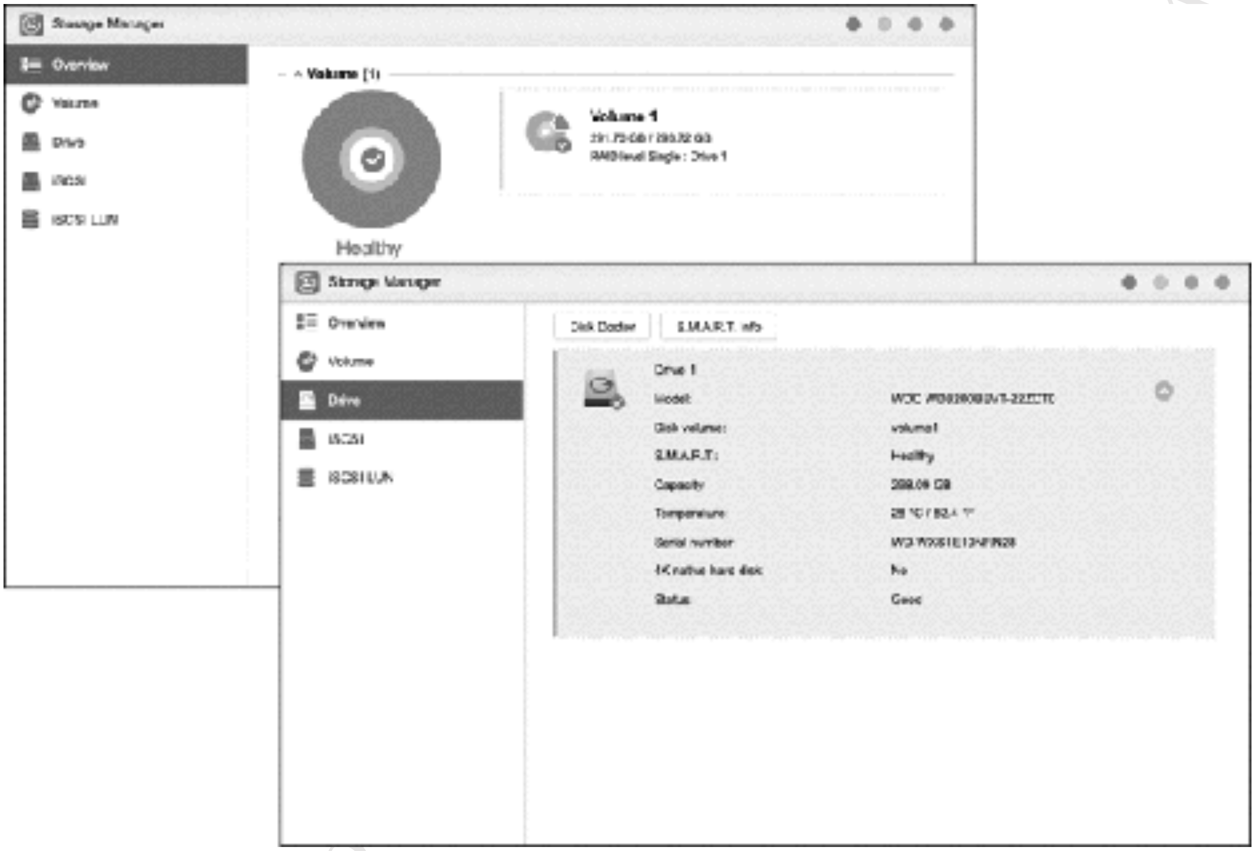


Figure 128: Tools

8.4 Checking the Health of the Drives

It is important to check the health of the disk drives in the server on a regular basis, especially if there appear to be problems or if the NAS has shut down unexpectedly for any reason, as this can result in damage and potential data loss. Checking can be done manually or scheduled to take place automatically.

To manually check the health of the drives, launch **Storage Manager**. On the **Overview** panel, the volume(s) should have a status of 'Healthy'. Click **Drive** on the left-hand side of the screen to display the drive(s) and click the downward pointing chevron to show more information:



Volume 1
291.75 GB / 293.72 GB
RAID level Single : Drive 1

Drive 1

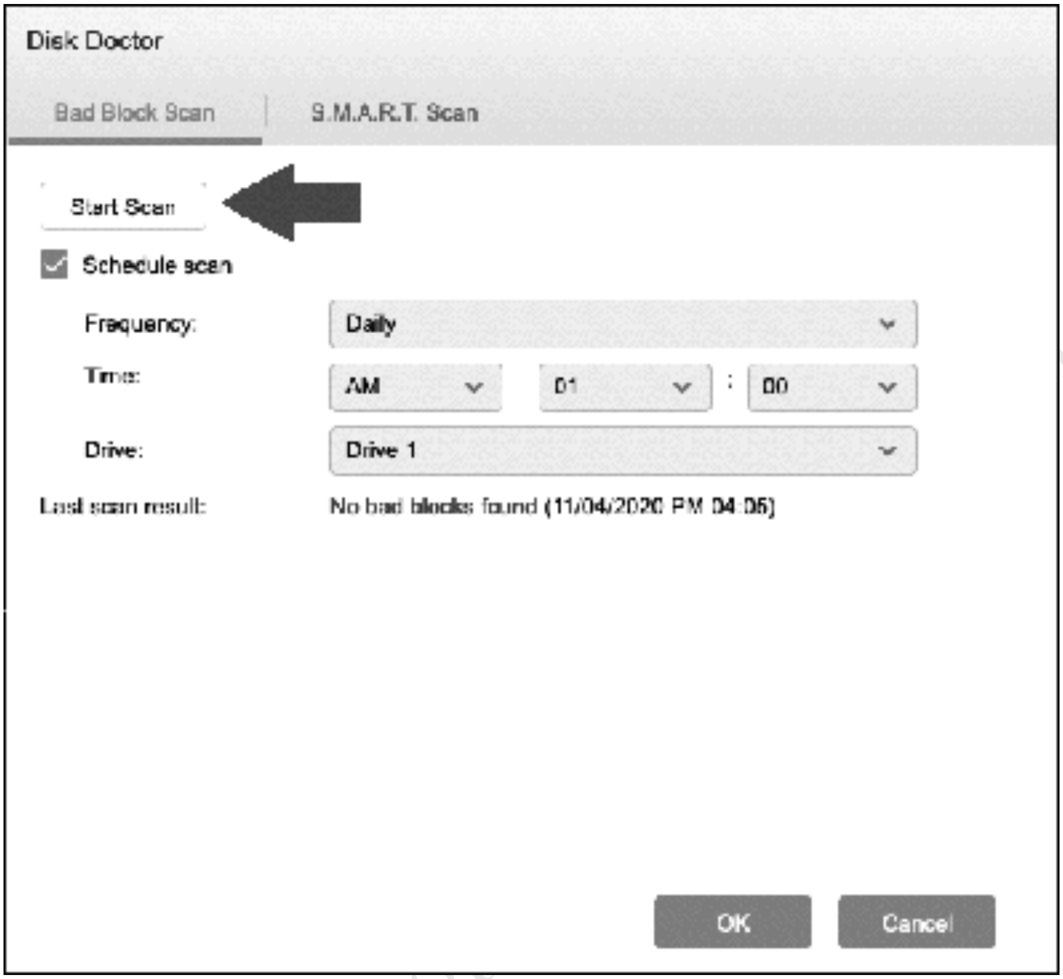
Model: WDC WD3200BEVT-22ZCT0
Disk volume: volume1
S.M.A.R.T.: Healthy
Capacity: 298.09 GB
Temperature: 28 °C / 82.4 °F
Serial number: WD-WX61E13HF928
4K native hard disk: No
Status: Good

Figure 129: Drive status

Under most circumstances the status of the disk(s) will be 'Good', meaning no further action is required. If there are any concerns, click the **Disk Doctor** button; if you have more than one drive in the system you will first need to select the drive, which you can do by clicking on it. Two options are available:

Bad Block Scan

The purpose of this test is to check the drive for any corruption. Click the **Bad Block Scan** tab. To run immediately, click the **Start Scan** button. The time taken to complete depends upon the capacity of the drive but may run into several hours. To run on a scheduled basis, tick the **Schedule scan** box and specify a frequency and time using the dropdowns. Generally speaking, a monthly test is sufficient. As the scan can affect drive performance, it is best executed out of hours so as to avoid disruption.



☑ Schedule scan

Frequency: Daily

Time: AM 01 : 00

Drive: Drive 1

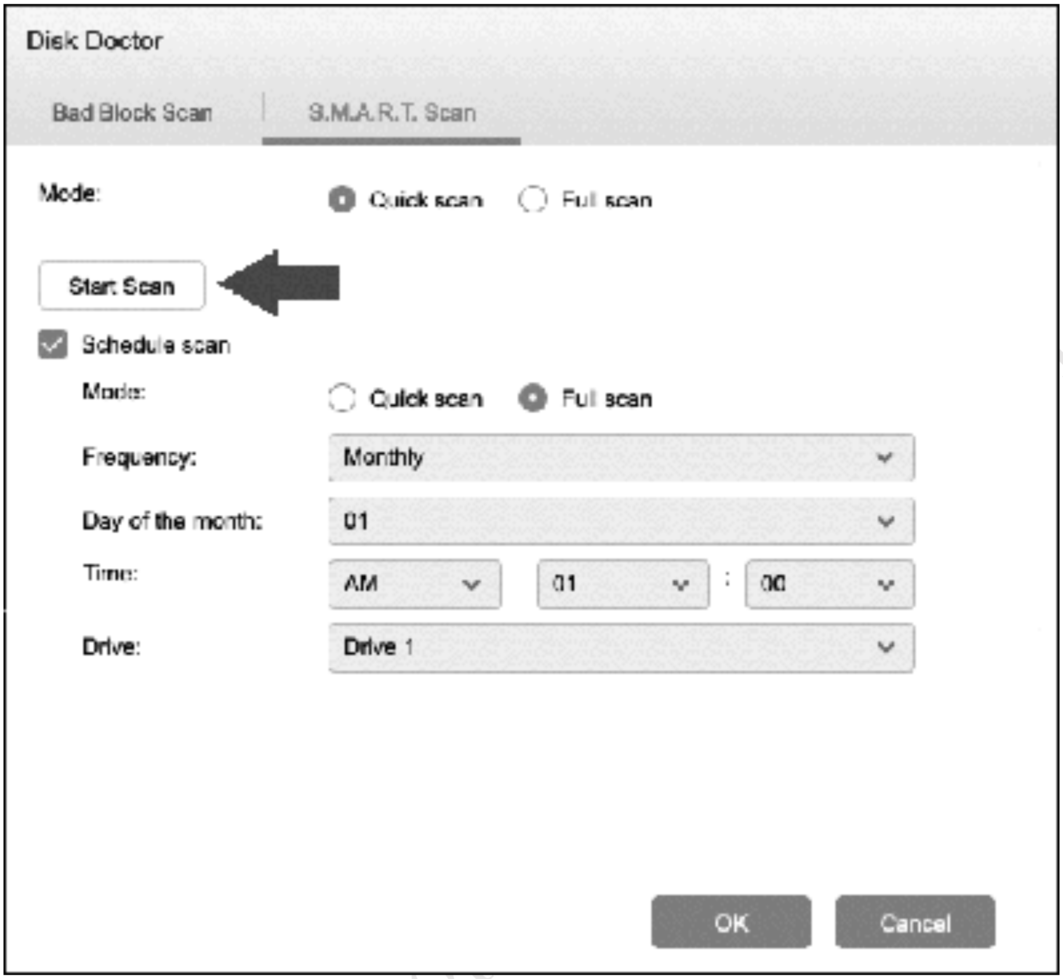
Last scan result: No bad blocks found (11/04/2020 PM 04:05)

Figure 130: Bad Block Scan

S.M.A.R.T. Scan

S.M.A.R.T. or *Self-Monitoring, Analysis and Reporting Technology* is a monitoring system built-in to disk drives. Its purpose is to check various electrical and mechanical parameters relating to drive reliability, with the intent of anticipating imminent hardware failures. If a drive fails the S.M.A.R.T. scan it should be replaced at the earliest opportunity so as to reduce the risk of data loss.

Click the **S.M.A.R.T. Scan** tab. Choose a mode: *Quick scan* takes a few minutes, whereas a *Full scan* takes much longer and is best done during a quiet time. To run immediately, click **Start Scan**.



Mode: ● Quick scan ○ Full scan

☑ Schedule scan

Mode: ○ Quick scan ● Full scan

Frequency: Monthly

Day of the month: 01

Time: AM 01 : 00

Drive: Drive 1

Figure 131: S.M.A.R.T. Scan

Best practice is to automate the testing process, which can be done by setting a schedule. To run on a scheduled basis, tick the **Schedule scan** box, choose the **Mode** and specify a frequency and time using the dropdowns. Generally speaking, a monthly test is sufficient. As the scan can affect drive performance, it is best executed out of hours so as to avoid disruption.

Defragmentation

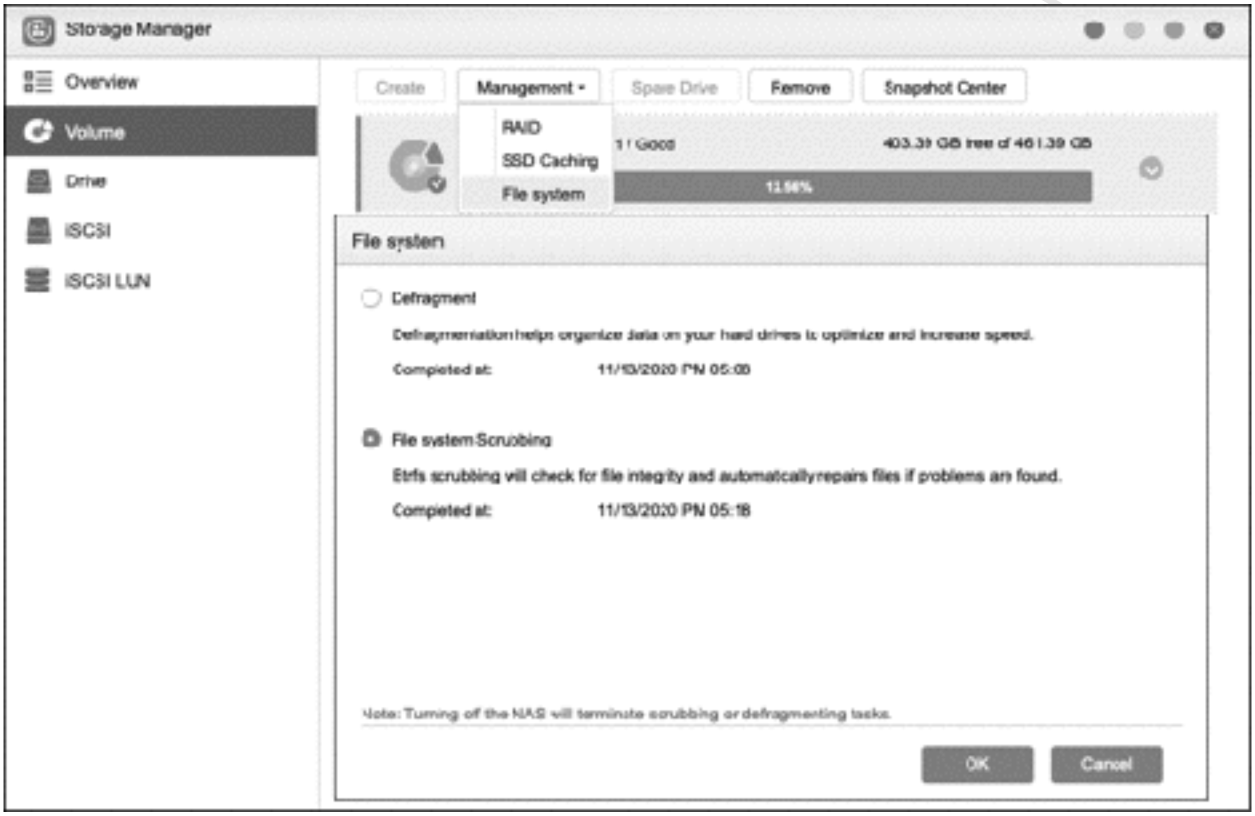
When data is stored on a mechanical hard drive, it is not necessarily held in one contiguous area. Rather, the operating system may have to break it down into multiple chunks in order to make use of the available storage space. Consider, for instance, if a video file of 2 GBytes has to be written to disc, but the largest amount of contiguous space remaining is only 1 GByte; clearly it cannot fit and so will have to be stored in separate segments. This fragmentation can affect disk performance, as the drive heads will be moving across the platters to locate the segments. *Defragmentation* is a process which re-organizes the data to ensure files are stored in contiguous areas.

Within **Storage Manager**, click on the **Volume** panel. Highlight a volume and click **Management** > **File System**. On the resultant panel, click **Defragment** then **OK**. The time taken will depend upon the capacity of the volume, the amount of data stored upon it and how badly fragmented it is. Note that this procedure only needs to be performed on an occasion basis, such as every six months or annually.

File System Scrubbing

Due to the nature of computer systems and disk drives, there is always the risk of potential data corruption. Invariably, corrupt data is not detected until an attempt is made to access it, by which time it is too late. To try and alleviate this problem, a process called *File System Scrubbing* can be used. This is an error detection process whereby data stored in a volume is systematically checked for any errors, which are then corrected using checksums or copies of data. File System Scrubbing is managed from within Storage Manager and is available for use on volumes formatted with the Btrfs filing system (it is not applicable to ext4).

Within **Storage Manager**, click the **Volume** panel. Highlight a volume and click **Management** > **File System**. On the resultant panel, click **File system Scrubbing** then **OK**. The time taken will depend upon the capacity of the volume, the amount of data stored upon it and how much (if any) repair work is needed. Note that this procedure only needs to be performed on an occasion basis, such as quarterly or every six months.



1 / Good

403.39 GB free of 461.39 GB

File system

○ Defragment

Defragmentation helps organize data on your hard drives to optimize and increase speed.

Completed at: 11/13/2020 PM 05:08

● File system Scrubbing

Btrfs scrubbing will check for file integrity and automatically repairs files if problems are found.

Completed at: 11/13/2020 PM 05:18

Note: Turning off the NAS will terminate scrubbing or defragmenting tasks.

Figure 132: Defragment and File System Scrubbing

IronWolf Health Management

If Seagate IronWolf drives are being used in the NAS, the *IronWolf Health Management* add-in can be downloaded from App Central (it may have already been installed automatically). This will integrate itself within Storage Manager to provide status information about the drives. Both IronWolf hard drives (HDDs) and Solid State Drives (SSDs) are supported.

8.5 Activity Monitor

The *Activity Monitor,* located on the Desktop, generates charts that provide real-time information about key sub-system performance, process information and drive usage. This information can be useful when trying to identify performance problems and bottlenecks in a system. For instance, if the NAS is short on memory then one option might be to upgrade the RAM, should that be an option on the particular model. Or, if network utilization is high then one option might be to add an additional network adapter (again, assuming that is an option for the model in question).

There are four sections: *Performance*, *Processes*, *Drive Usage* and *Settings*

Performance

The Performance screen consists of five tabs. The Overview tab gives an 'at a glance' summary of activity in five key areas: CPU, Memory, Network, Drive and iSCSI (iSCSI might only be present if it has been enabled). Each topic also has its own separate tab, which provides a larger chart with more detailed information.

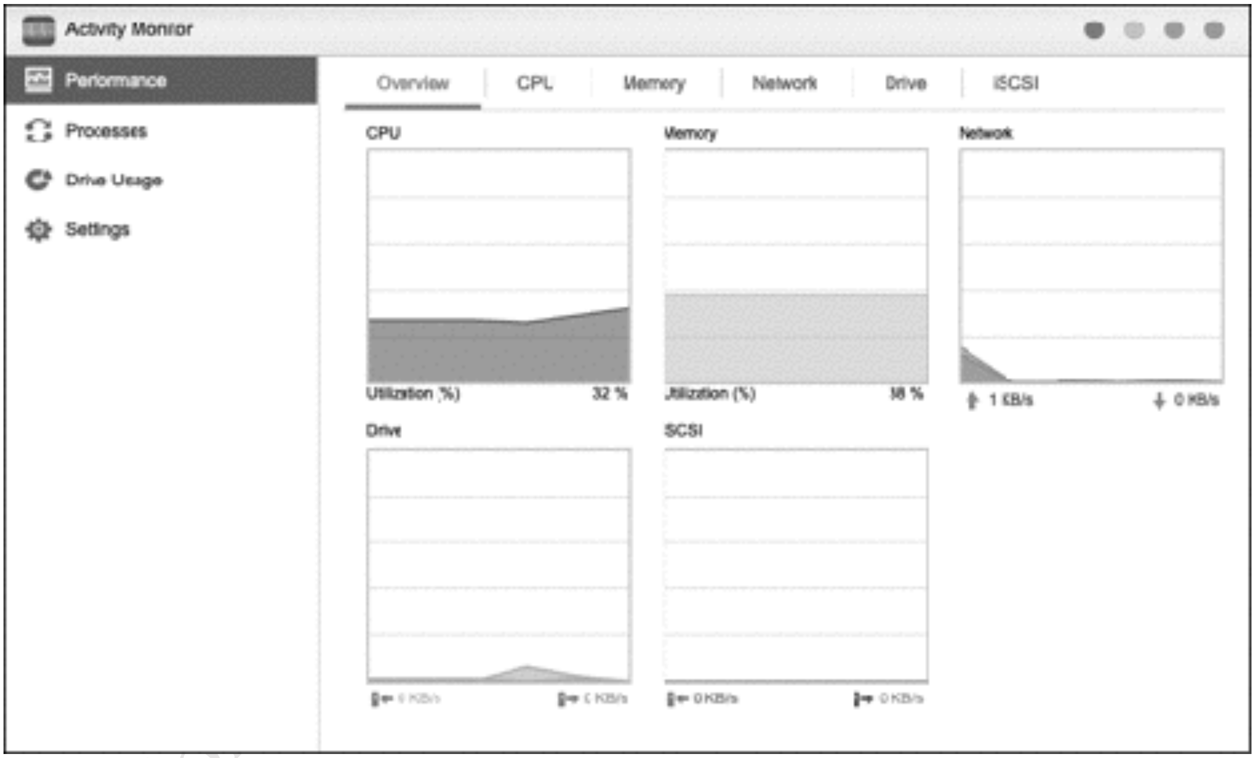
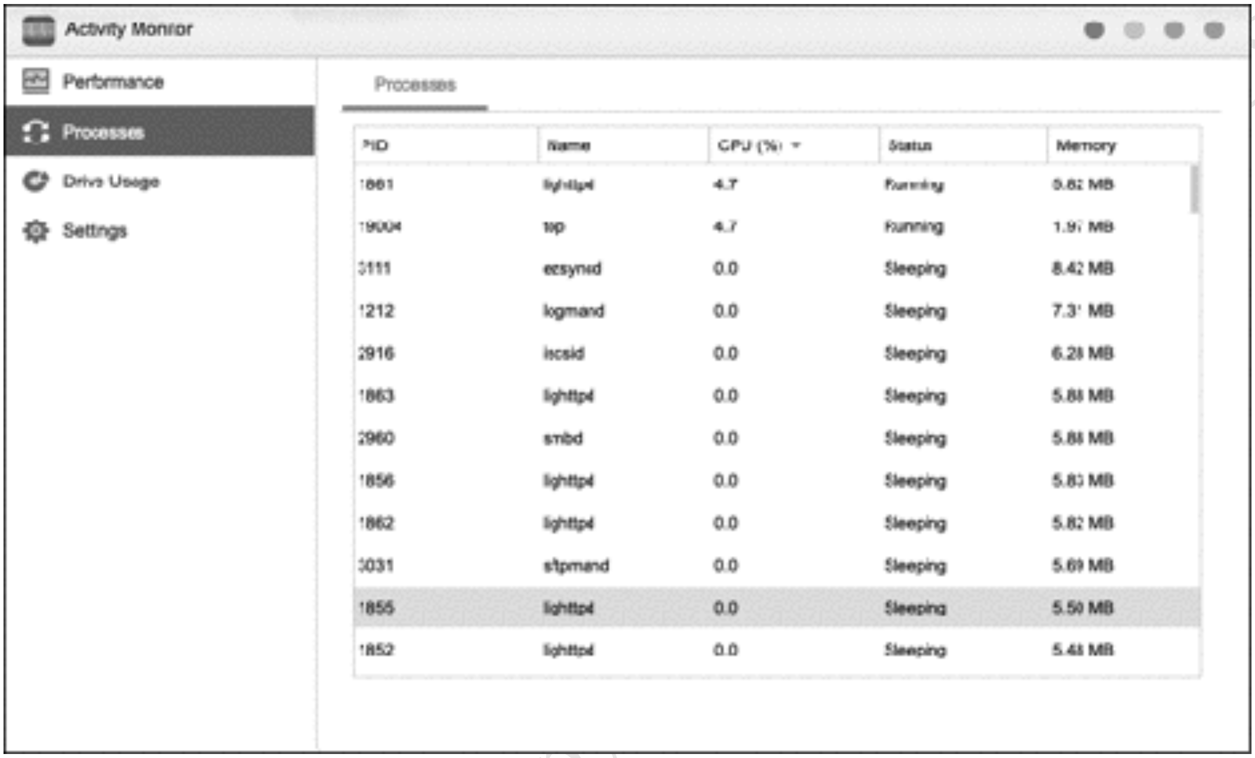


Figure 133: Activity Monitor Performance screen

Processes

The second screen – *Processes* – lists the processes running on the NAS. If the server appears busy or is performing slowly, this can help identify the culprit(s) which are using excessive CPU or memory. To sort by a column, click its name.

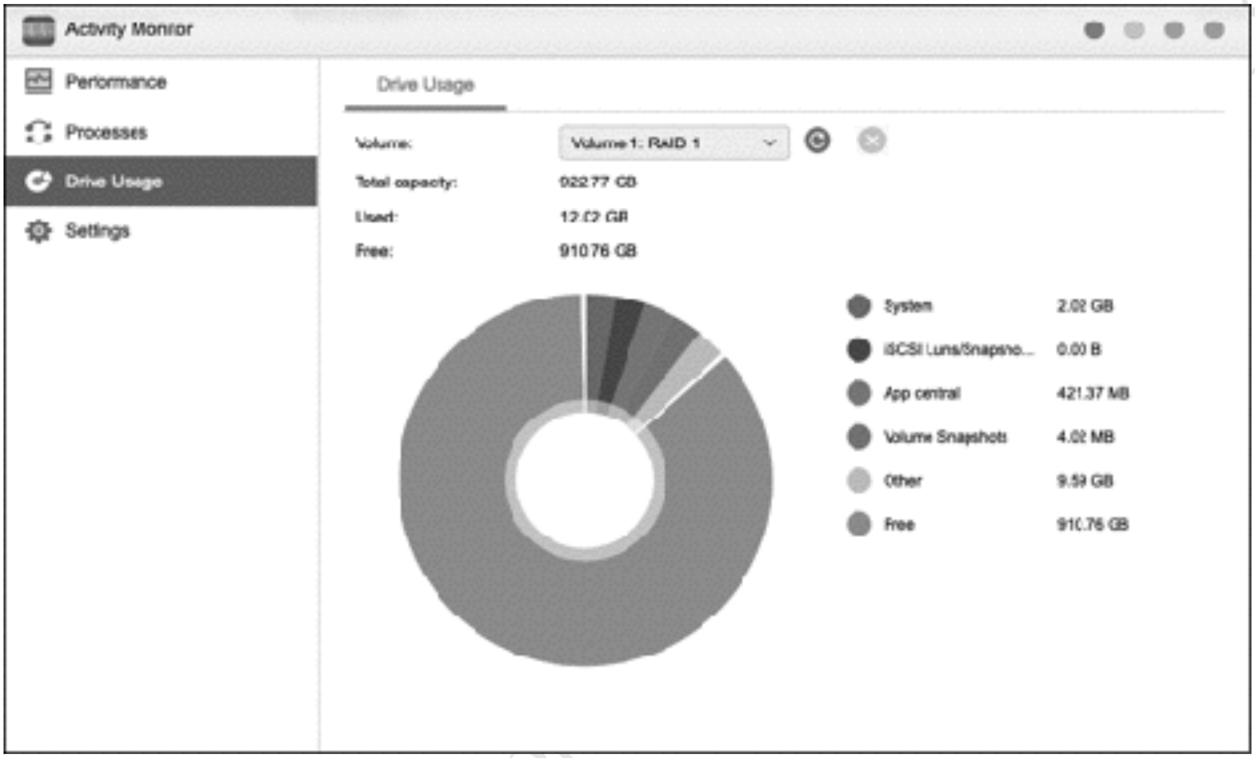


PID	Name	CPU (%) ▾	Status	Memory
1861	lighttpd	4.7	Running	5.82 MB
19004	top	4.7	Running	1.97 MB
3111	ezsyncd	0.0	Sleeping	8.42 MB
1212	logmand	0.0	Sleeping	7.31 MB
2916	iscsid	0.0	Sleeping	6.28 MB
1863	lighttpd	0.0	Sleeping	5.88 MB
2960	smbd	0.0	Sleeping	5.88 MB
1856	lighttpd	0.0	Sleeping	5.83 MB
1862	lighttpd	0.0	Sleeping	5.82 MB
3031	sftpmand	0.0	Sleeping	5.69 MB
1855	lighttpd	0.0	Sleeping	5.50 MB
1852	lighttpd	0.0	Sleeping	5.48 MB

Figure 134: Process screen within Activity Monitor

Drive Usage

The Drive Usage section gives a visual representation of how storage space is being used on a volume. If the NAS has more than one volume, use the dropdown to select the one you are interested in. The category that most people will be interested in is the amount of free space. The category of 'Other' actually refers to the user data stored on the volume.



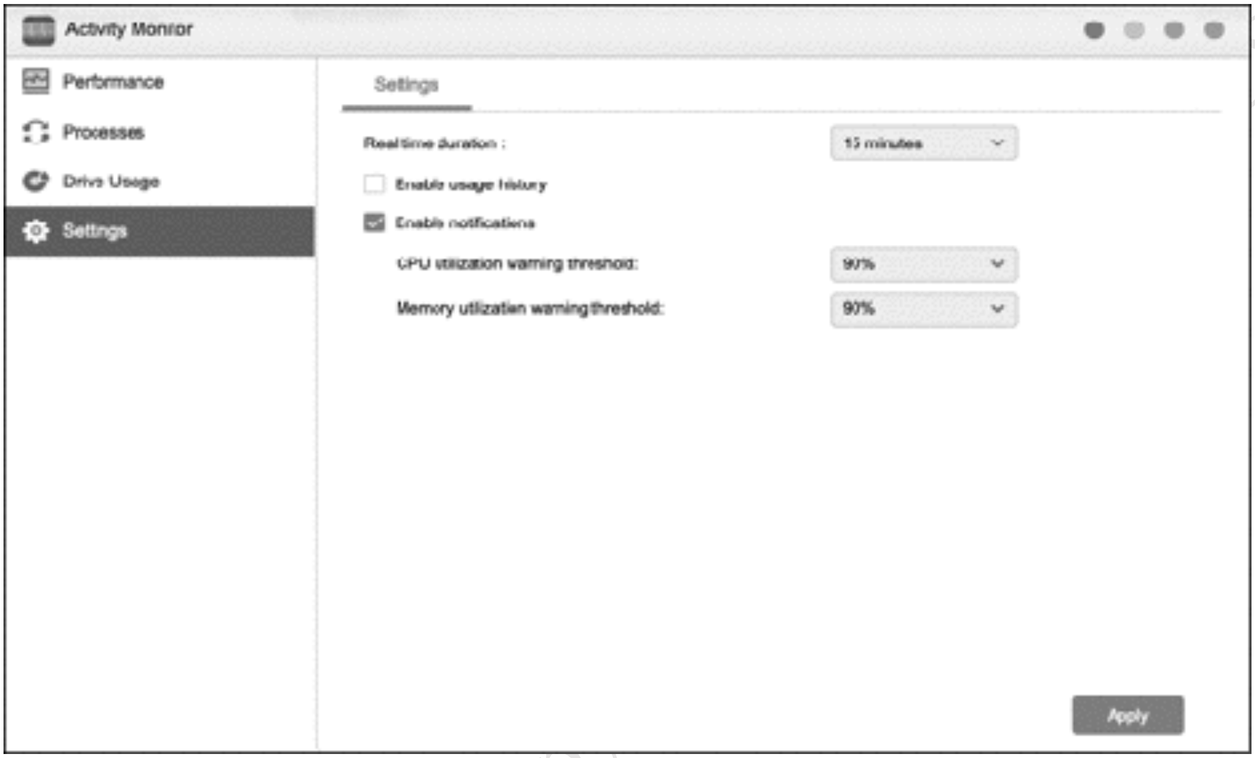
Volume: Volume 1: RAID 1
Total capacity: 922.77 GB
Used: 12.02 GB
Free: 910.76 GB

●	System	2.02 GB
●	iSCSI Luns/Snapsho...	0.00 B
●	App central	421.37 MB
●	Volume Snapshots	4.02 MB
●	Other	9.59 GB
●	Free	910.76 GB

Figure 135: Drive Usage screen

Settings

The final screen – *Settings* – enables some of the characteristics of Activity Monitor to be adjusted. In particular, notifications for CPU and memory utilizations – with adjustable thresholds – can be set (for more information about notifications, see section 8.7 Notifications). Having made changes, click **Apply**.



Realtime duration : 15 minutes

□ Enable usage history

☑ Enable notifications

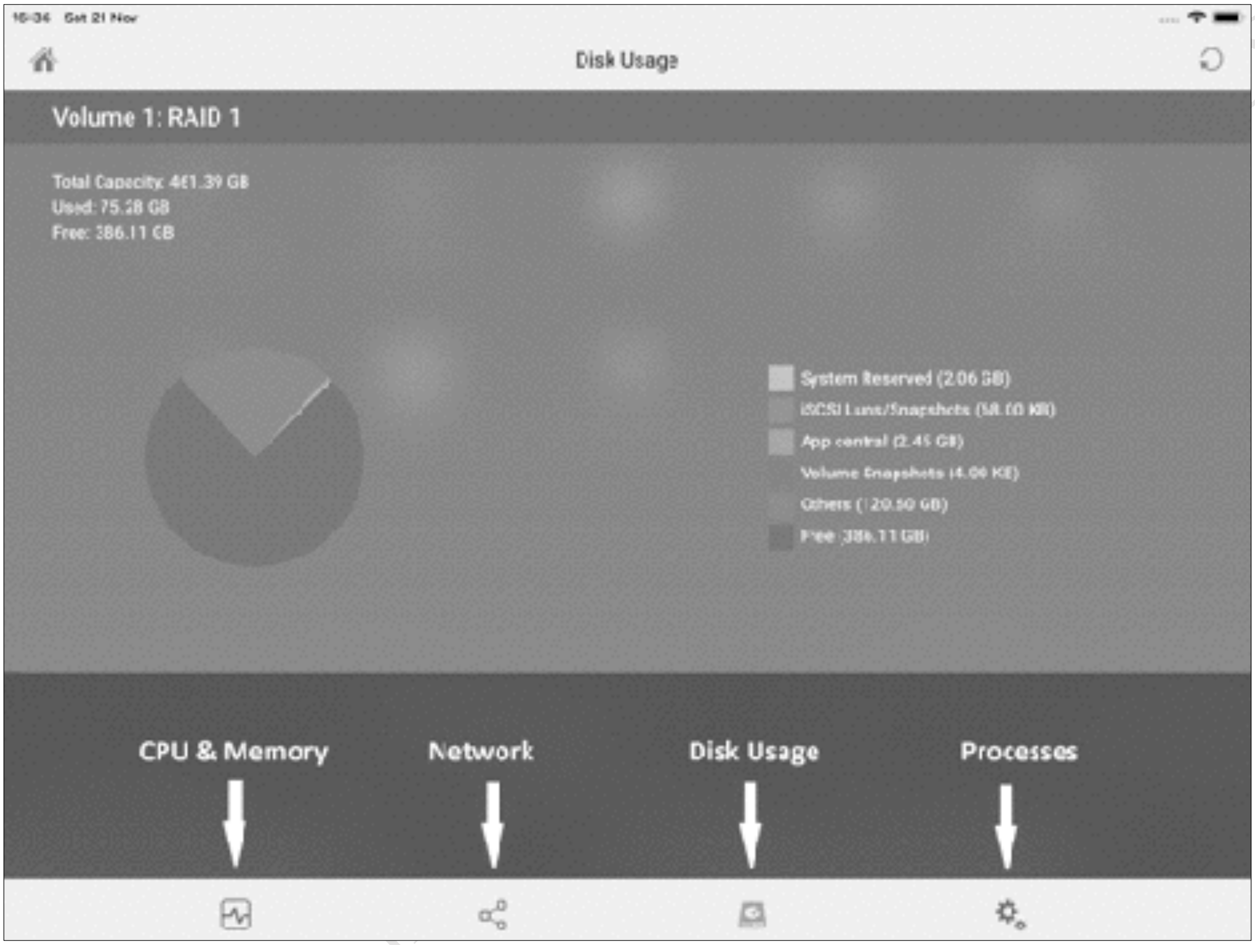
CPU utilization warning threshold: 90%

Memory utilization warning threshold: 90%

Figure 136: Activity Monitor Settings

Accessing Activity Manager with AiMaster

Tap the Activity Manager icon on the main AiMaster screen. The utility is controlled using the four small icons at the bottom of the screen. Working from left to right, they provide access to CPU and Memory utilization; network performance; disk usage; list of running processes.



Volume 1: RAID 1

Total Capacity: 461.39 GB
Used: 75.28 GB
Free: 386.11 GB

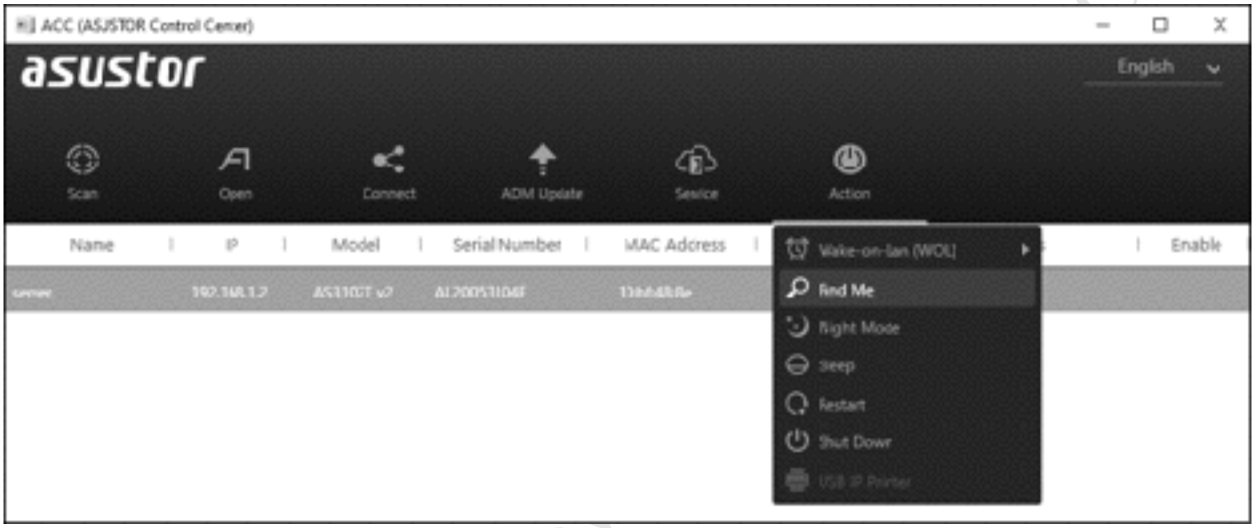
- System Reserved (2.06 GB)
- iSCSI Luns/Snapshots (58.00 KB)
- App central (2.45 GB)
- Volume Snapshots (4.00 KB)
- Others (120.50 GB)
- Free (386.11 GB)

Figure 137: Activity Monitor within AiMaster

8.6 Locating a NAS

The ASUSTOR Control Center (ACC) utility has the ability to locate a NAS by beeping the buzzer and making the LEDs on the front of the unit flash. You might consider it unlikely that you would ‘lose’ a NAS and need such a facility, but there are several scenarios in which it is useful. For instance, you may be unfamiliar with the location of the NAS in someone else’s home or office. Or, you might be in an environment where there are multiple units, maybe even dozens or hundreds of them in racks and finding the one you want could be a challenge.

To locate a NAS, load ACC on a computer. If the server is not listed, click **Scan**. Highlight the server and click **Action** followed by **Find Me**, then login to it using the administrator username and password. The server will begin buzzing and the power LED will flash. To stop it, click **Cancel**.



Name	IP	Model	Serial Number	MAC Address		Enable
server	192.168.1.2	AS3102T v2	AI20051104F	[illegible]		

Figure 138: Locating a NAS using ACC

Locating a NAS using AiMaster

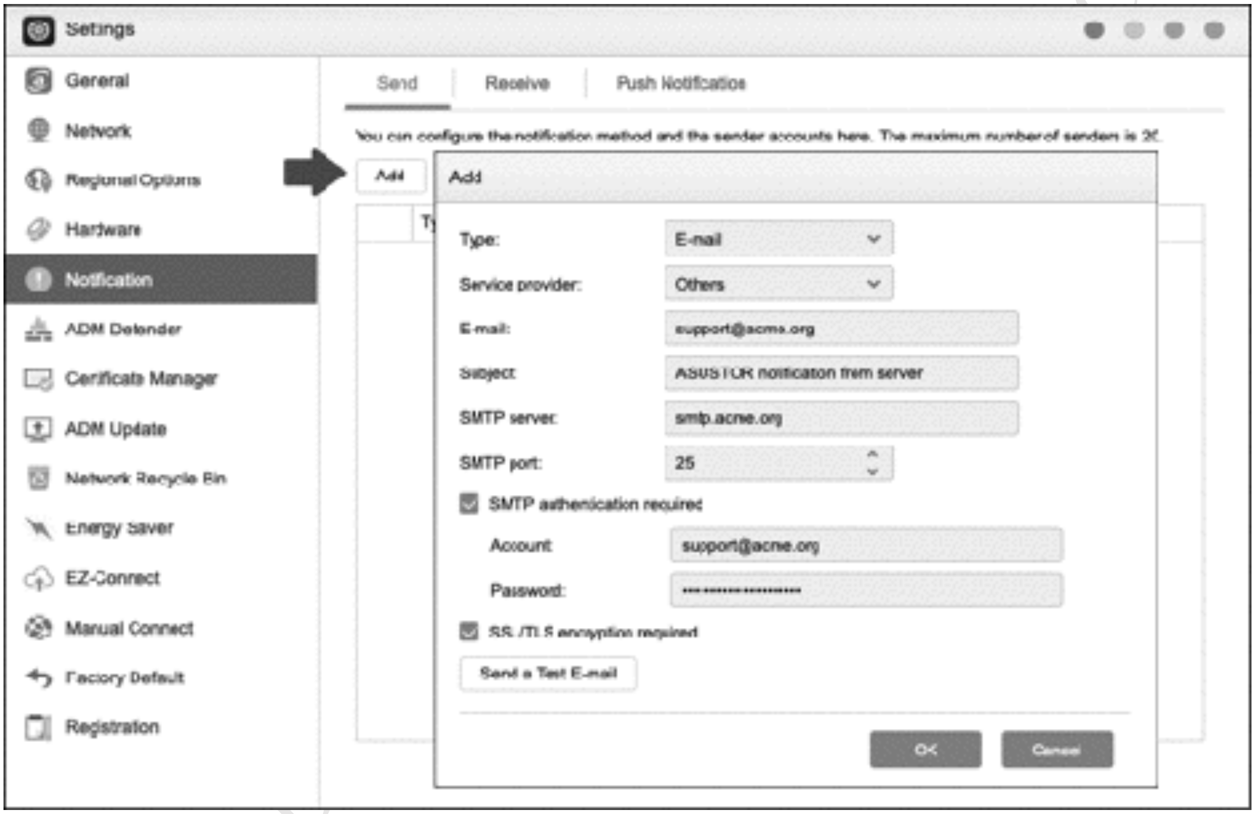
Within AiMaster, tap the **Settings** wheel in the top right-hand corner of the screen, followed by **Find Me**. To stop it, tap the small panel then tap **Cancel**.

8.7 Notifications

Whilst it is important to check the server on a regular basis, it may not always be practical to do so in person. For instance, the person responsible – you, presumably - may not be located on the premises. Also, it is better to deal with some problems as soon as they arise, rather than learn about them later. For these reasons, ADM can pro-actively advise when issues occur, using automatic notifications sent by email, SMS, or pushed to a mobile device. However, as the SMS method uses commercial services which may not be available worldwide, we will not cover that method.

Setting Up Email Notifications

To setup email notifications, click **Preferences** > **General** > **Notification**. On the **Send** tab, click **Add**.



You can configure the notification method and the sender accounts here. The maximum number of senders is 20.

Type: E-mail

Service provider: Others

E-mail: support@acms.org

Subject: ASUSTOR notification from server

SMTP server: smtp.acne.org

SMTP port: 25

☑ SMTP authentication required

Account: support@acne.org

Password: ••••••••••••••••••

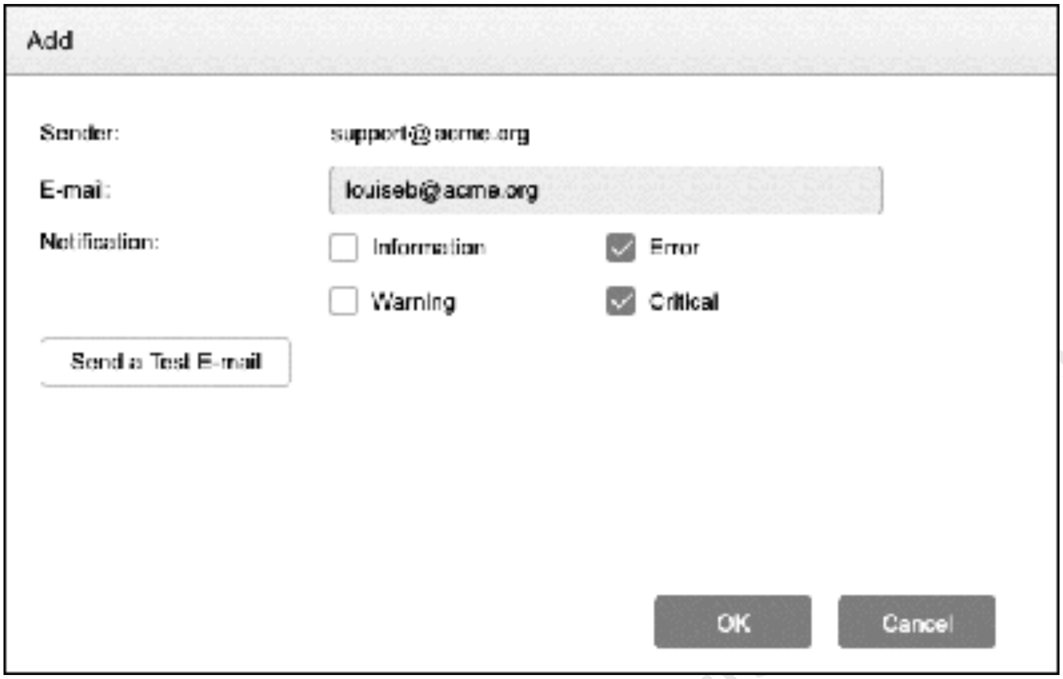
☑ SSL/TLS encryption required

Figure 139: Configuring email notifications

The *Type* dropdown should be set to **E-Mail**. Click the *Service provider* dropdown: there is built-in support for Google, Microsoft and Yahoo email services. If you prefer to use another or your own organization's email service, choose *Others* and enter the SMTP details (server name, port number, email address, authentication details), which should be available from whoever runs or controls your email service. Enter the name and password of the account sending the emails. If desired, overtype the *Subject*. Click the **Send a Test E-mail** button and enter the address of the recipient. Assuming the test message is received, all is well and you can click **OK**.

Having setup the sending side, the recipients of notification emails can now be defined, of which there can be a maximum of 20. Click the **Receive** tab and on the resultant tab click **Add**. Enter the email address of the recipient and tick the box(es) for the desired notification types. Click the **Send a Test E-mail** button; assuming the test message is received, you can then click **OK**.

Suggestion: notifications are best restricted to error and/or critical events only.



Sender: support@acme.org

E-mail: louiseb@acme.org

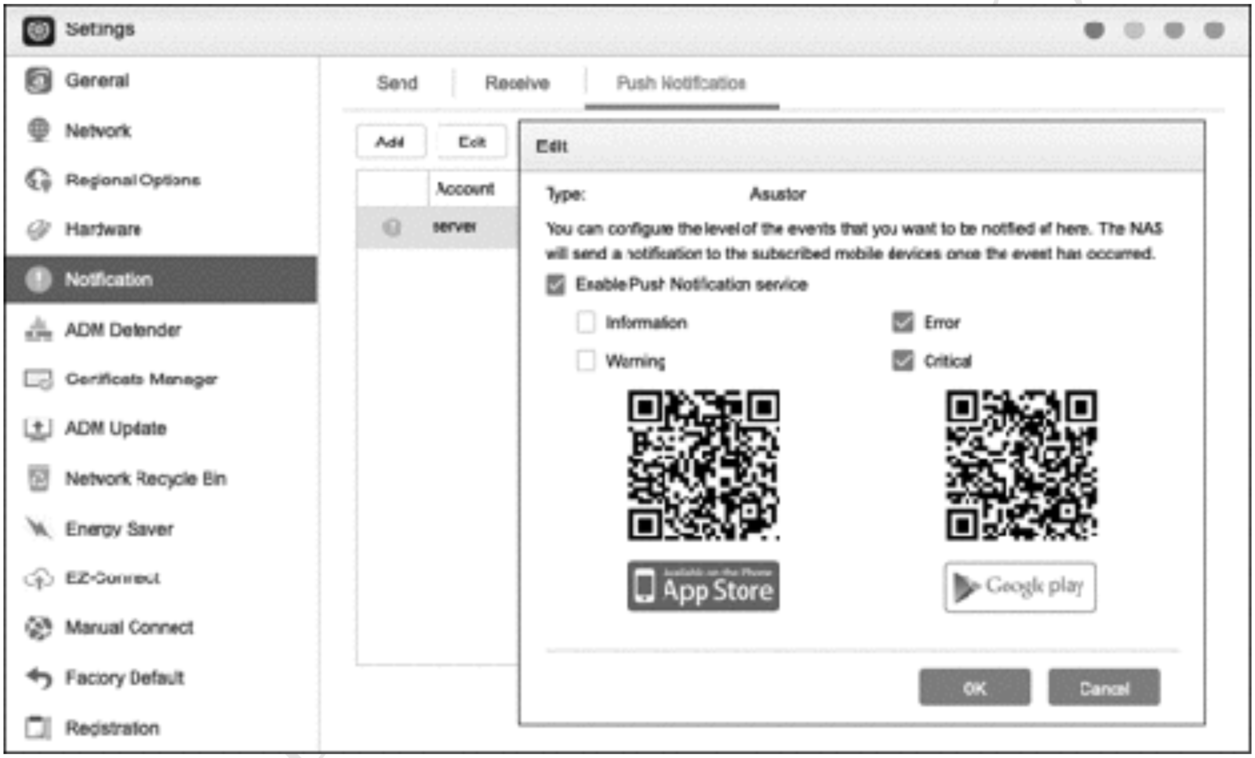
Notification: □ Information ☑ Error □ Warning ☑ Critical

Figure 140: Setting up an email recipient

Setting Up Email Notifications

Notifications can also be sent to mobile devices, such as iOS and Android smartphones and tablets. This is done through AiMaster, so this needs to be installed and working. Within AiMaster, tap the **Settings** cogwheel then tap **Push Notification** and make sure that it is enabled. You should also check the notification settings on the device itself to ensure that AiMaster has the appropriate permissions.

On the server side, click **Preferences** > **General** > **Notification**. On the **Push Notification** tab there should already be an entry for the server, but it will not yet be working. Tick the **Enable Push notification** service box and tick the box(es) for the desired notification types (suggestion: notifications are best restricted to errors and/or critical events only). The QR codes are for downloading AiMaster, so if this is already installed you can ignore them. Click **OK**. Returning to the main screen, there is a useful **Test** button. It may take a few minutes for the test message to appear, so there is no need to worry about any delay.



Type: Asustor

You can configure the level of the events that you want to be notified of here. The NAS will send a notification to the subscribed mobile devices once the event has occurred.

☑ Enable Push Notification service

□ Information ☑ Error

□ Warning ☑ Critical

Figure 141: Setting up push notifications

9

MULTIMEDIA & STREAMING

9.1 Overview

One of the most popular uses of a home network is for the storage and playback of media such as music and videos and the viewing of photographs. The NAS is able to playback the stored media onto a variety of devices including computers, gaming consoles, tablets, smartphones, smart TVs and streaming devices. Some ASUSTOR models are equipped with a HDMI port, enabling them to be connected directly to a suitable television set and to act as a home theater media player, using an app called *ASUSTOR Portal* and which is described in section 12.3 ASUSTOR Portal.

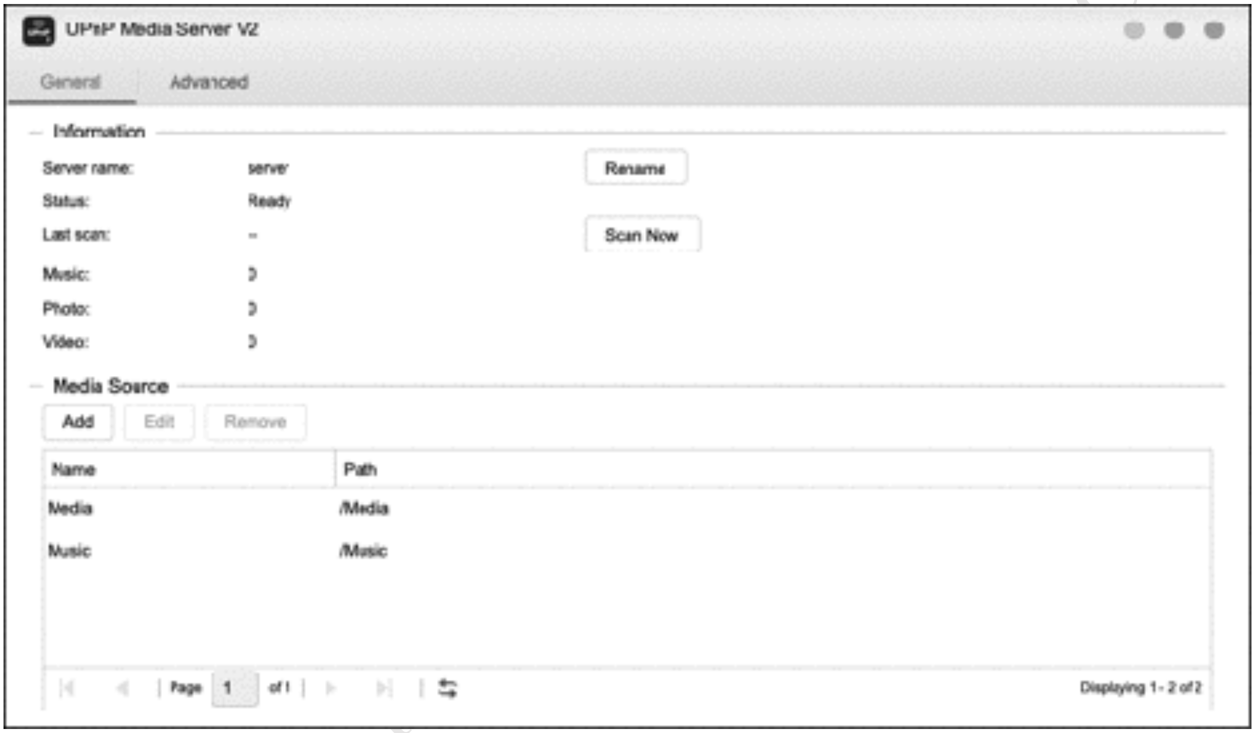
ASUSTOR offer a wide range of multimedia apps, including:

DLNA Media Server – a universal system for media playback to many types of devices
SoundsGood – for playback of music and audio files
LooksGood – for playing back videos and movies
Photo Gallery 3 – for managing and displaying photographs and other images
Hi-Res Player – enables playback of high-resolution audio files, such as DSD and FLAC
iTunes Server – enables playback of music on PCs and Macs using Apple’s iTunes and Music apps

9.2 UPnP Media Server V2

DLNA is the abbreviation for *Digital Living Network Alliance*. It is a standard for interconnecting home network devices so they can stream and play multimedia. The goal is that DLNA devices can do this without worrying about passwords, network protocols and other technical issues. Many devices are DLNA-compliant including computers, smart televisions, media streamers such as Roku, Apple TV and Chromecast, gaming boxes such as Xbox and PlayStation, smartphones, Blu-ray players and suitably equipped audio systems. The NAS can be turned into a DLNA server by installing the *UPnP Media Server V2* app, downloadable from App Central (be sure to download this version, rather than the much older *UPnP Media Server*).

Initially, UPnP Media Server V2 has a spartan appearance:



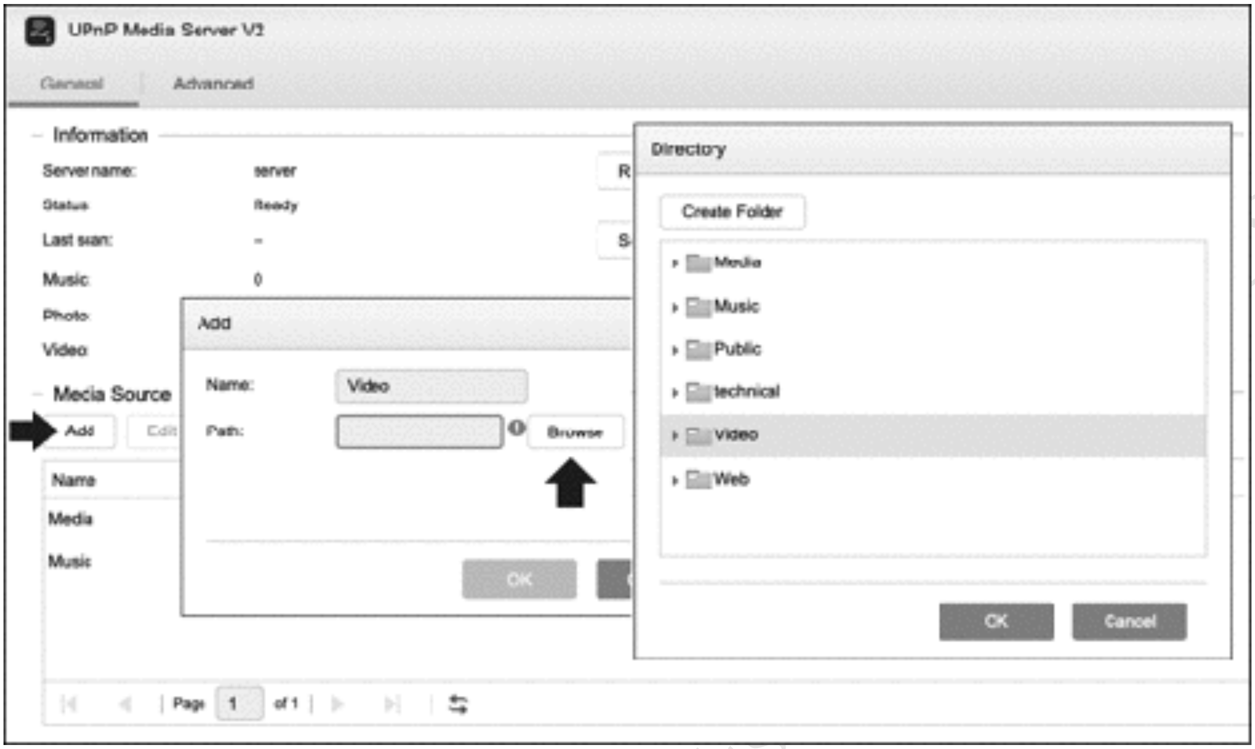
Server name: server
Status: Ready
Last scan: --
Music: 0
Photo: 0
Video: 0

Name	Path
Media	/Media
Music	/Music

Displaying 1 - 2 of 2

Figure 142: UPnP Media Server V2 immediately following installation

The first thing to do is define where the media files are located, which is done in the *Media Source* section of the app. During installation, a shared folder called *Media* will have been created; you can use this and/or any other folder. In this example, we already have some videos stored in a shared folder call *Video*, so we will add this. Click **Add**; in the resultant popup give the source a name and click the **Browse** button to navigate the filing system and choose your folder:



Server name: server
Status: Ready
Last scan: -
Music: 0
Photo:
Video:

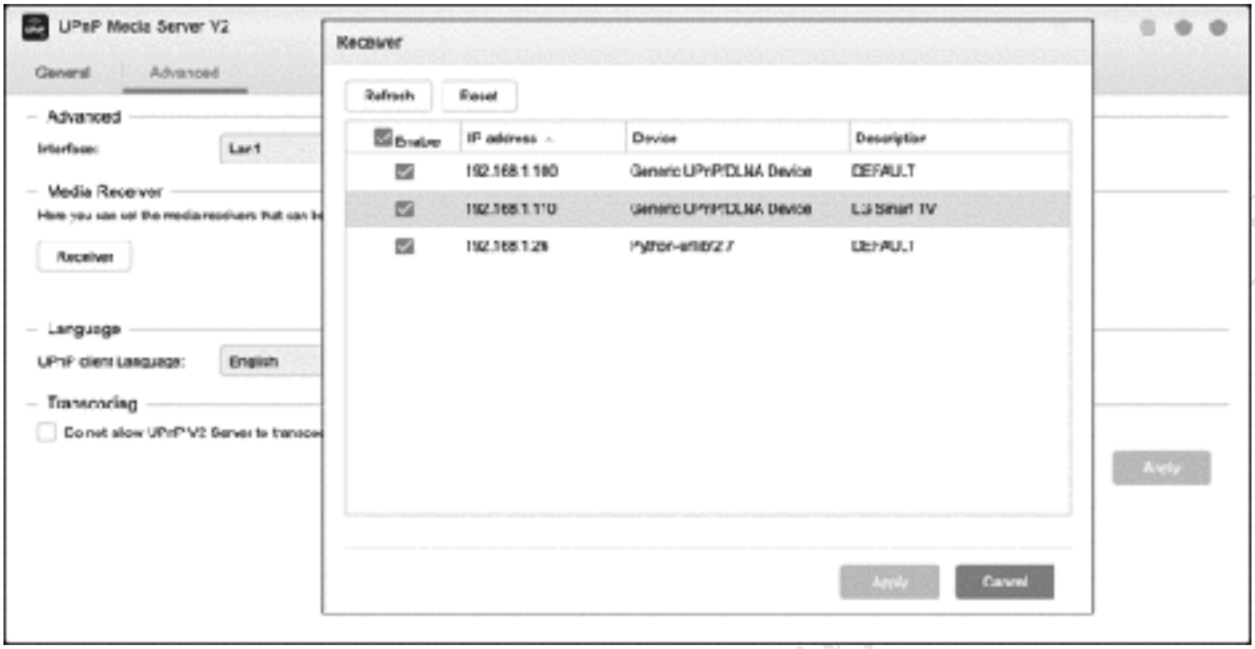
Name: Video
Path:

Figure 143: Specify the media sources

Having specified the media sources, click the **Scan Now** button, which will cause UPnP Media Server V2 to index the files; depending on the number and type of files, plus the performance of the NAS, this may take some time. Whenever changes are made subsequently, such as adding more media files or additional source folders, you should re-index.

Next, click the **Advanced** tab. The first section, called *Advanced*, allows the network interface to be defined on servers that have more than one. You might want to do this if a lot of media devices are being used, for example, in a household with several smart TVs you could specify Lan2 for the media server, thus freeing up Lan1 for ‘ordinary’ traffic.

The *Media Receiver* section allows ‘receivers’ (that is, DLNA clients) to have or not to have access to the media server. For instance, if you did not want the LG Smart TV in this example to have access you would remove the tick.



Interface: Lan1

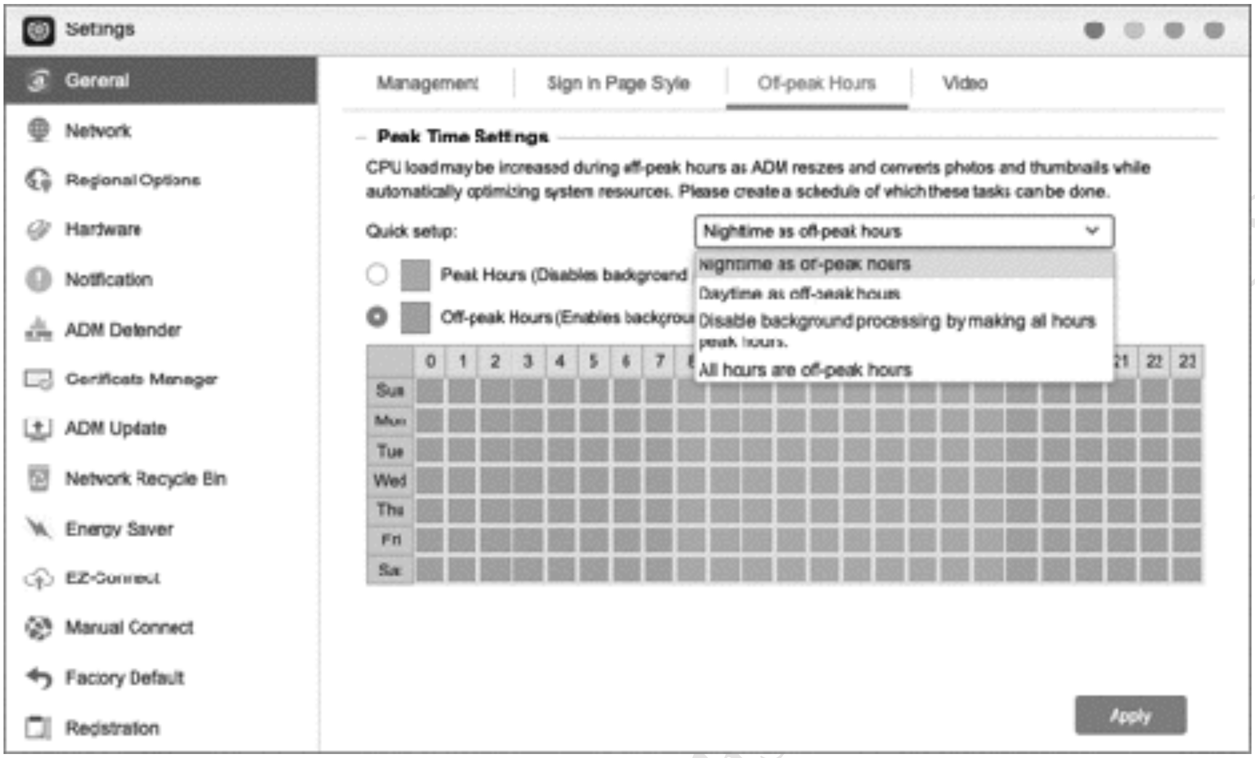
UPnP client language: English

☐ Do not allow UPnP V2 Server to transco

☑ Enable	IP address ^	Device	Description
☑	192.168.1.180	Generic UPnP/DLNA Device	DEFAULT
☑	192.168.1.110	Generic UPnP/DLNA Device	LG Smart TV
☑	192.168.1.29	Python-urllib/2.7	DEFAULT

Figure 144: Media Receivers

The *Language* section does exactly what you would expect. *Transcoding* is a process where the resolution of videos is optimized (reduced) to match the client device as, for instance, there is no point in sending a 4K resolution to a television set that works at a maximum resolution of 720p. Transcoding uses a lot of resources on the NAS, so you may wish to disable this feature on less powerful models. If you do decide to use it, leave the box unticked, then click **Preferences** > **General** > **Video**. There are three options: *Do not convert*, *Automatically convert* and *Always ask*. If you choose the second one, conversion will take place during off-peak hours, to avoid impacting on regular activities and usage. To define this time, click the **Off-peak Hours** tab. Use the mouse cursor to ‘paint’ the peak and off-peak hours, else use dropdown to choose a pre-defined scheme. Click **Apply**.



Peak Time Settings

CPU load may be increased during off-peak hours as ADM resizes and converts photos and thumbnails while automatically optimizing system resources. Please create a schedule of which these tasks can be done.

Quick setup: Nighttime as off-peak hours

- Nighttime as off-peak hours
- Daytime as off-peak hours
- Disable background processing by making all hours peak hours.
- All hours are off-peak hours

○ Peak Hours (Disables background

● Off-peak Hours (Enables backgrou

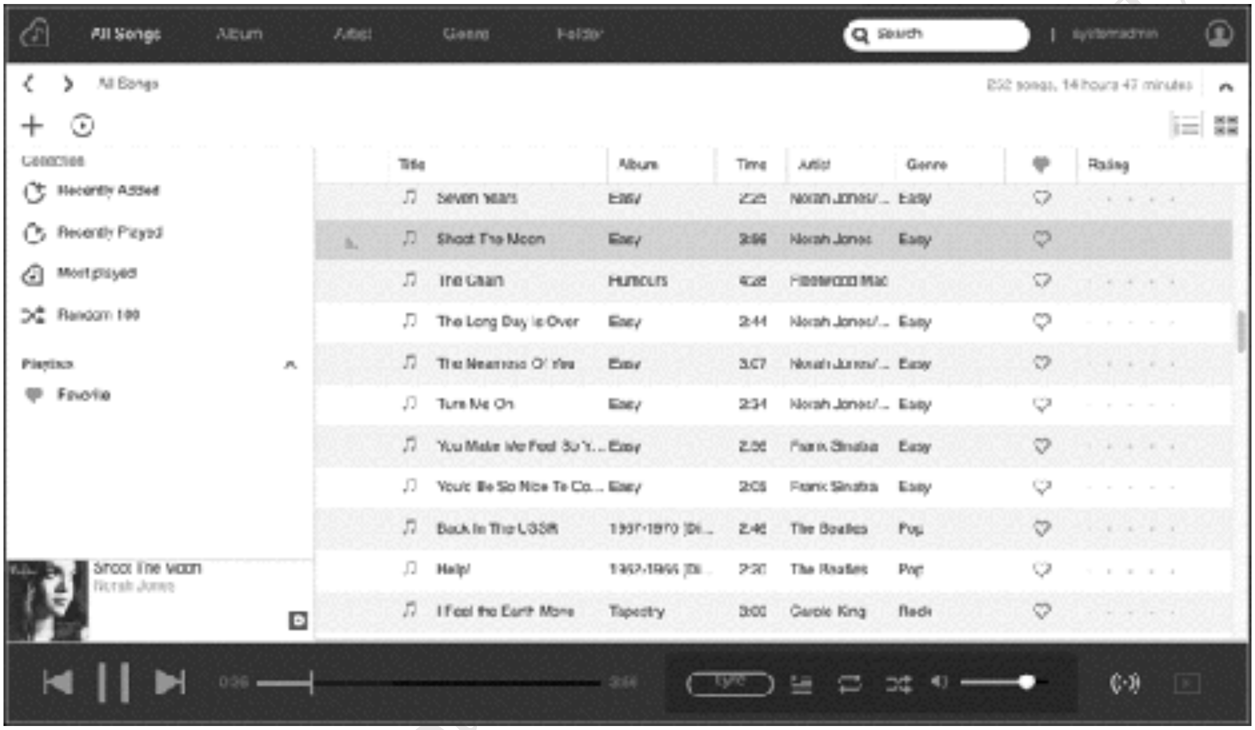
Figure 145: Defining Peak Time Settings

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). 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 SoundsGood

SoundsGood is an application that allows a music collection to be held and managed on the NAS and played back through a browser or streamed to other devices. It is downloaded from App Central. During installation, additional supporting components may also be installed. Upon completion, an icon is placed on the Desktop.

As part of the installation process, a shared folder called *Music* is automatically created. Start off by copying your music to this folder; files should be in a widely used format, such as MP3 or WAV. Once this is done, click the SoundsGood icon, which will cause it to open in a new browser tab:



Title	Album	Time	Artist	Genre	♥	Rating
Seven Years	Easy	2:25	Norah Jones/...	Easy	♡	
Shoot The Moon	Easy	3:56	Norah Jones	Easy	♡	
The Chain	Rumours	4:28	Fleetwood Mac		♡	
The Long Day Is Over	Easy	2:44	Norah Jones/...	Easy	♡	
The Nearness Of You	Easy	3:07	Norah Jones/...	Easy	♡	
Turn Me On	Easy	2:34	Norah Jones/...	Easy	♡	
You Make Me Feel So Y...	Easy	2:56	Frank Sinatra	Easy	♡	
You'd Be So Nice To Co...	Easy	2:05	Frank Sinatra	Easy	♡	
Back In The USSR	1967-1970 [Di...	2:46	The Beatles	Pop	♡	
Help!	1962-1966 [Di...	2:20	The Beatles	Pop	♡	
I Feel the Earth Move	Tapestry	3:00	Carole King	Rock	♡	

Figure 146: SoundsGood, All Songs view

The music can be viewed and sorted in various ways such as by song title, album, artist, genre and so on, which can be done by clicking on the main categories at the top of the screen and/or by clicking on the captions of the columns. Titles can be displayed as a text list or as icons.

There are numerous options for playing back music:

- Highlight a track and click the play icon, or double-click a track, and it will play on the computer you are using via SoundsGood and though the browser.
- If the Music folder is being accessed from a computer, double-click a track and it should playback via the computer's default audio application e.g. Windows Media Player, Groove Music, QuickTime etc.
- If the NAS has a HDMI connection, it can play through that using ASUSTOR Portal.

Access to SoundsGood is controlled on an individual user basis. Go into P**references** > **App Privileges**, highlight the SoundsGood app and click the **Edit** button. Place ticks against the users who should have access and click **OK**. Next, go to **Preferences** > **Shared Folders**, highlight the *Music* folder and click the **Access Rights** button. Place ticks in the appropriate columns; if you want them to be able to add additional tracks to the shared *Music* folder give them Read-Write (RW) access, otherwise give them

Read-Only (RO) access. Click **OK**. Suggestion: if you want to make SoundsGood available to many users, consider creating a dedicated group e.g. *musicusers* and give access to it. If you want everyone to have it, give access to the built-in *users* group.

AiMusic

AiMusic is an app for listening to music on smartphones and tablets. It can operate in two modes: in the first mode it streams directly from the NAS to the mobile device, whereas in the second mode it plays files which have been downloaded to the device and stored locally. This second mode allows it to be used when offline, such as when travelling or without an internet connection. AiMusic is available as a free download for iOS and Android from the respective app stores.

When running for the first time, work through the overview and eventually there is a screen offering a choice between **Add NAS** and *Browse offline music*. Choose the former, acknowledge the privacy statement and specify the details of the server by tapping the plus sign (+) in the top right-hand corner of the screen. If you are connected locally you can let the app find your server on the network via Auto Discovery, else manually specify the name or IP address. If you also want to be able to use AiMusic remotely you should enter your Cloud ID, which you may have registered during the installation of ADM (else see section 10.2 Setting up EZ-Connect for how to do so). It is suggested that you flip the HTTPS switch to the 'On' position to improve security.

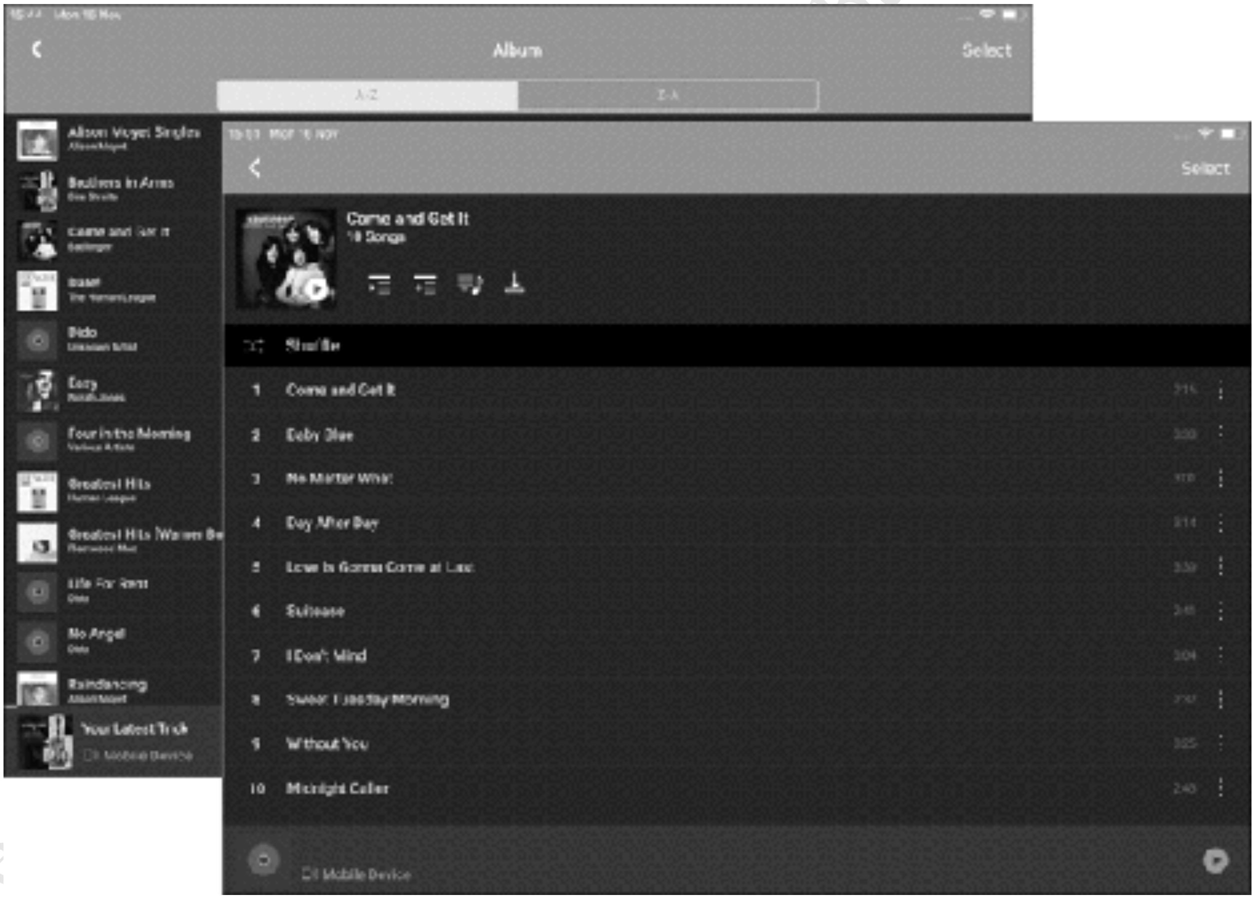


Figure 147: AiMusic, on iPad

Once connected, the music can be viewed and sorted in multiple ways e.g. by album, artist, genre and so on. Having found a track, simply tap to play it.

To download a song or album for local (offline) playback, tap the ‘three dot’ menu against it then tap **Download**.

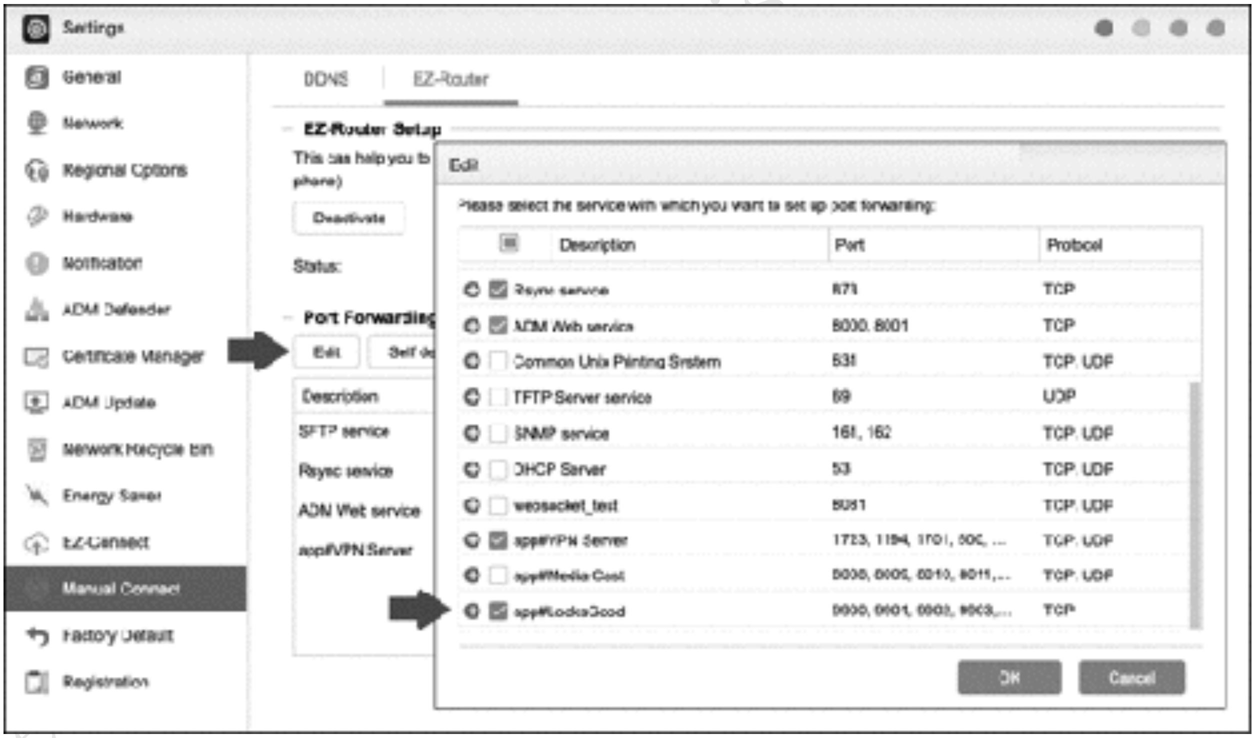
To switch between NAS and local modes, tap the three-line menu in the top left-hand corner of the screen and choose between the NAS or the Local Device. In local mode, you can only playback songs that you have downloaded from the NAS. Any music on the device from other sources (e.g. the Music or iTunes app in the case of Apple devices) is not accessible through AiMusic.

9.4 LooksGood

LooksGood is ASUSTOR's web-based application for watching videos and movies, played back within an internet browser. It is downloadable from App Central (see section 12.2 App Central). Additional components are required and if these are not already in place they will be downloaded and installed as well, which will add to the installation time.

On a suitably equipped computer, DVDs can be 'ripped' into a format such as MP4 and these copies can be played back from the NAS, thus protecting the originals against wear and tear. It may be necessary to experiment to determine the video format that gives best results, but some people report that MP4 format videos created by tools such as *Handbrake* and *DVDFab* work well. Be aware that the copying of commercial DVDs is prohibited in many countries and local copyright and other legal restrictions should be observed. Place your ripped videos into the shared folder called *Video*, which is created automatically during the installation of *LooksGood*. Suggestion: if you have many videos it might take several hours to copy them to the server. Rather than do this from your computer to the server over the network, it might be quicker to first copy them to a USB drive, then plug the drive into the NAS and copy them using File Explorer.

To function correctly, LooksGood requires that port forwarding is correctly configured and this may need to be done manually. To do so, click **Preferences** > **Manual Connect** > **EZ-Router**. In the *Port Forwarding* section, click **Edit**. On the resultant panel, find the entry for *app#LooksGood* (you may have to scroll down), make sure the box is ticked and click **OK**. The entry for *app#LooksGood* will be added to the main EZ-Router screen, which can now be closed.



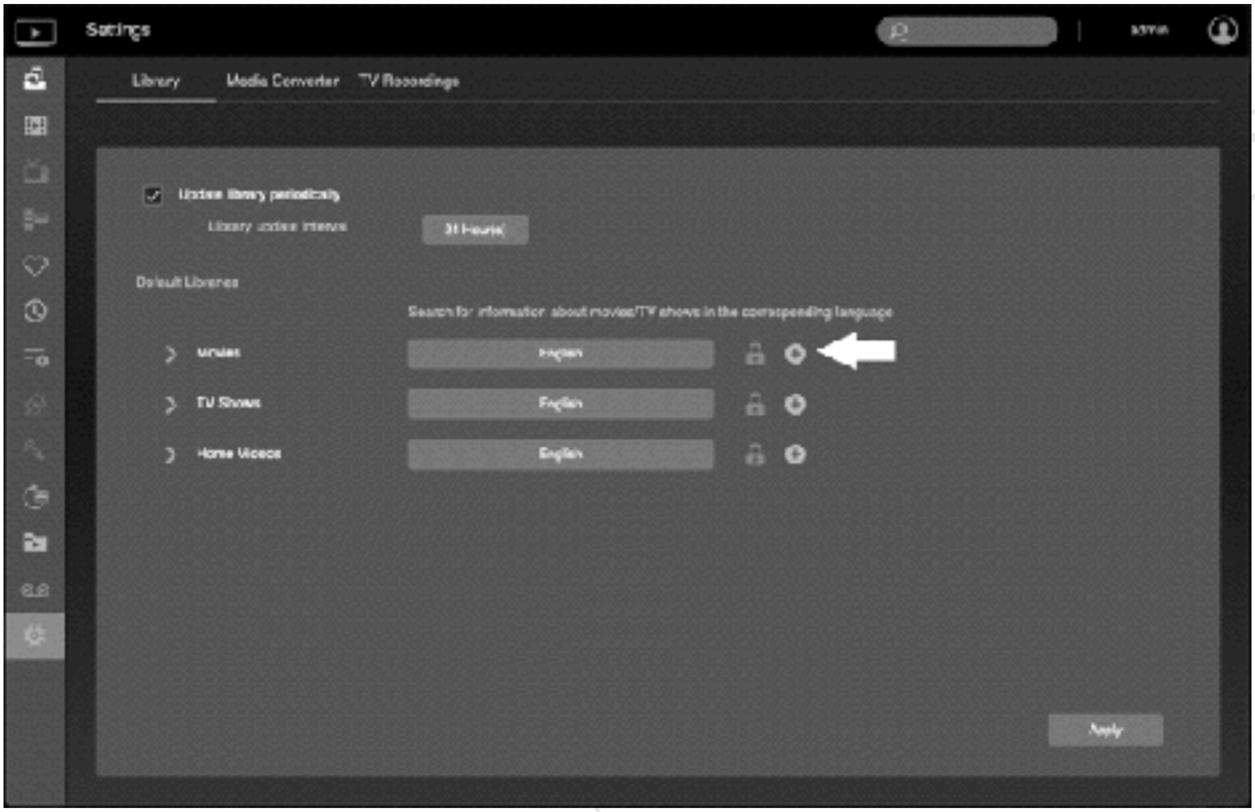
Please select the service with which you want to set up port forwarding:

	Description	Port	Protocol
☑	Rsync service	873	TCP
☑	ADM Web service	8000, 8001	TCP
□	Common Unix Printing System	631	TCP, UDP
□	TFTP Server service	69	UDP
□	SNMP service	161, 162	TCP, UDP
□	DHCP Server	53	TCP, UDP
□	websocket_test	8081	TCP, UDP
☑	app#VPN Server	1723, 1194, 1701, 500, ...	TCP, UDP
□	app#Media Cost	8008, 8005, 8010, 8011,...	TCP, UDP
☑	app#LooksGood	8000, 8001, 8002, 8003,...	TCP

Figure 148: Setup port forwarding for LooksGood

Click the Desktop icon for LooksGood, which will cause it to open in a new browser window. The first screen is a reminder about port forwarding, which we have just checked. Tick the **Do not show this again** box and click **Next**. The second screen has QR barcodes for downloading AiVideos, a mobile app for viewing videos. Tick the **Do not show this again** box and click **Next**. The third screen is basically a reminder about additional capabilities and features; again, tick the **Do not show this again** box and click

Next. On the fourth screen, click the **Start** button at the bottom of the screen and click **OK** on the screen after that to display the **Settings** screen in LooksGood:



☑ Update library periodically

Library update interval: 24 Hours

Default Libraries

Search for information about movies/TV shows in the corresponding language

Movies	English
TV Shows	English
Home Videos	English

Figure 149: Settings screen for LooksGood

Click the plus sign (+) which at the right-hand side of the entry for Movies, as indicated above. The resultant panel is for specifying the location of the videos; any folder can be used, but we will use the *Video* folder that the app created and in which we placed our movies. Highlight your choice and click **Yes**:

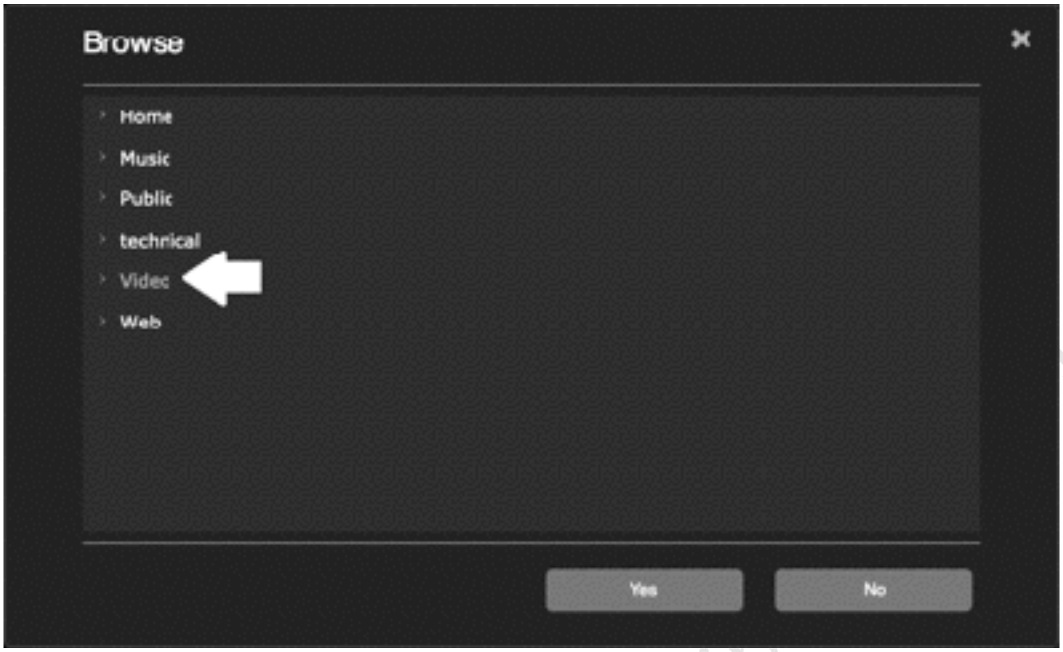


Figure 150: Specify the location of your videos

Upon returning to the previous screen, tick the **Update library periodically** box and set the Library update interval e.g. to 24 Hours. Click **Apply**. Optionally, you could choose to store recorded TV shows and your home videos in other locations, which you can also specify. The videos will now be indexed; the amount of time for this depends the number of videos and the processing power of the NAS but can be considerable. Eventually they will appear on the Movies tab, which is selectable by clicking its icon (indicated below). The titles can be viewed as thumbnails or as a detailed list and the view can be filtered in different ways e.g. by Year, Genre and Actor.

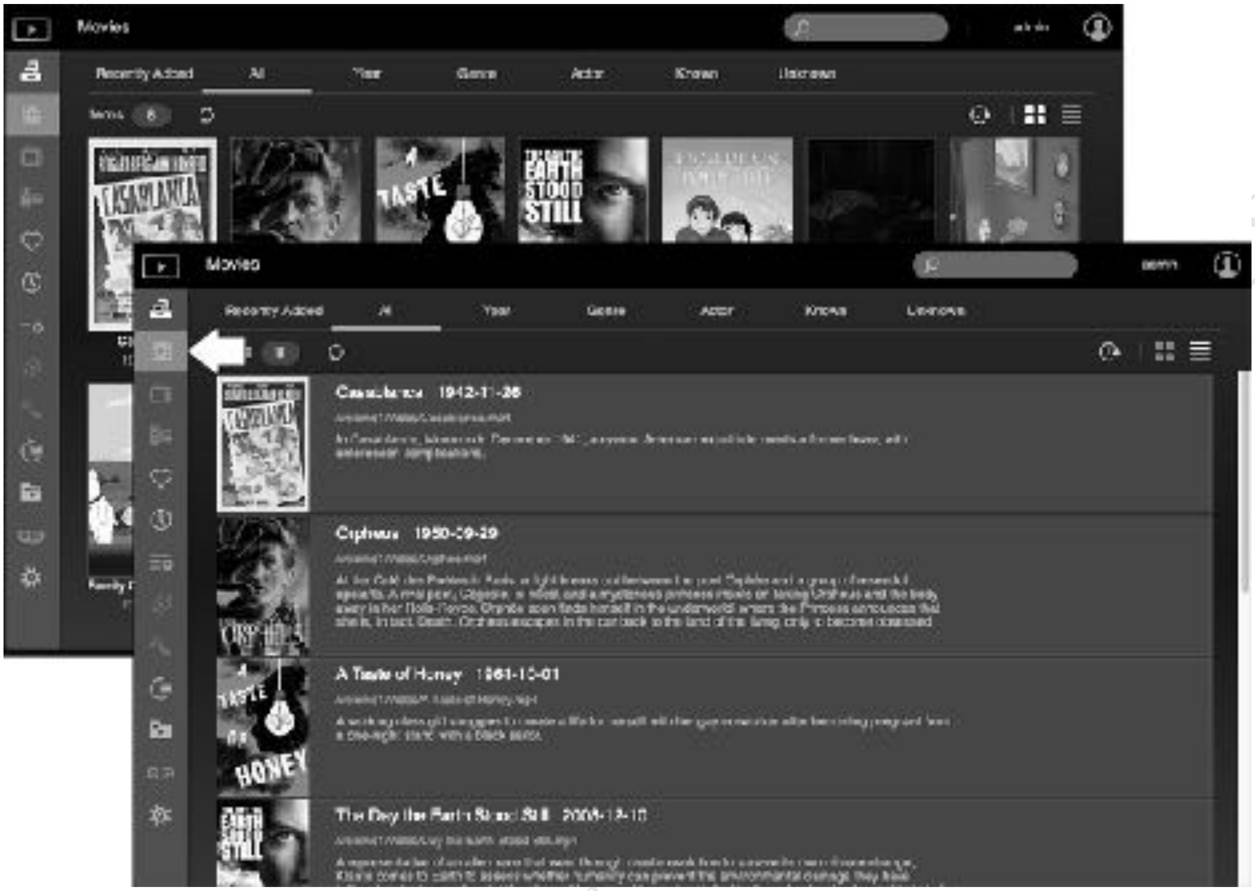


Figure 151: Movie screen in LooksGood

The information for the movies – artwork, synopsis, credits and such - is retrieved over the internet but may sometimes be incomplete or missing altogether. Movies which cannot be identified are listed on the **Unknown** tab. In such instances, the information can be added manually. To do so:

Move the mouse cursor over the thumbnail. Click the mini-menu indicated by three dots (…) and click **Edit** from the pop-up:

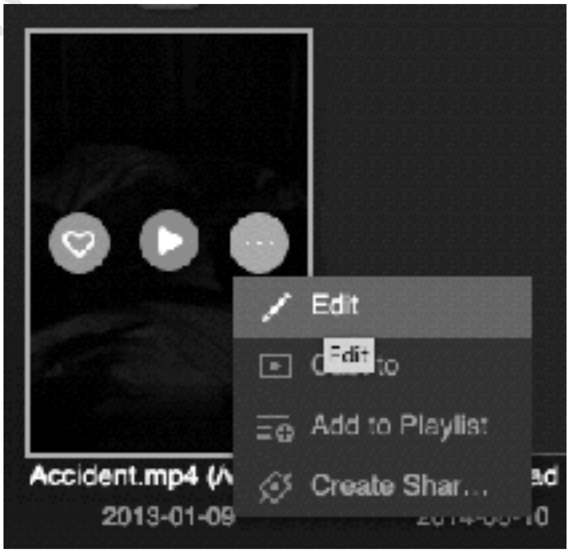
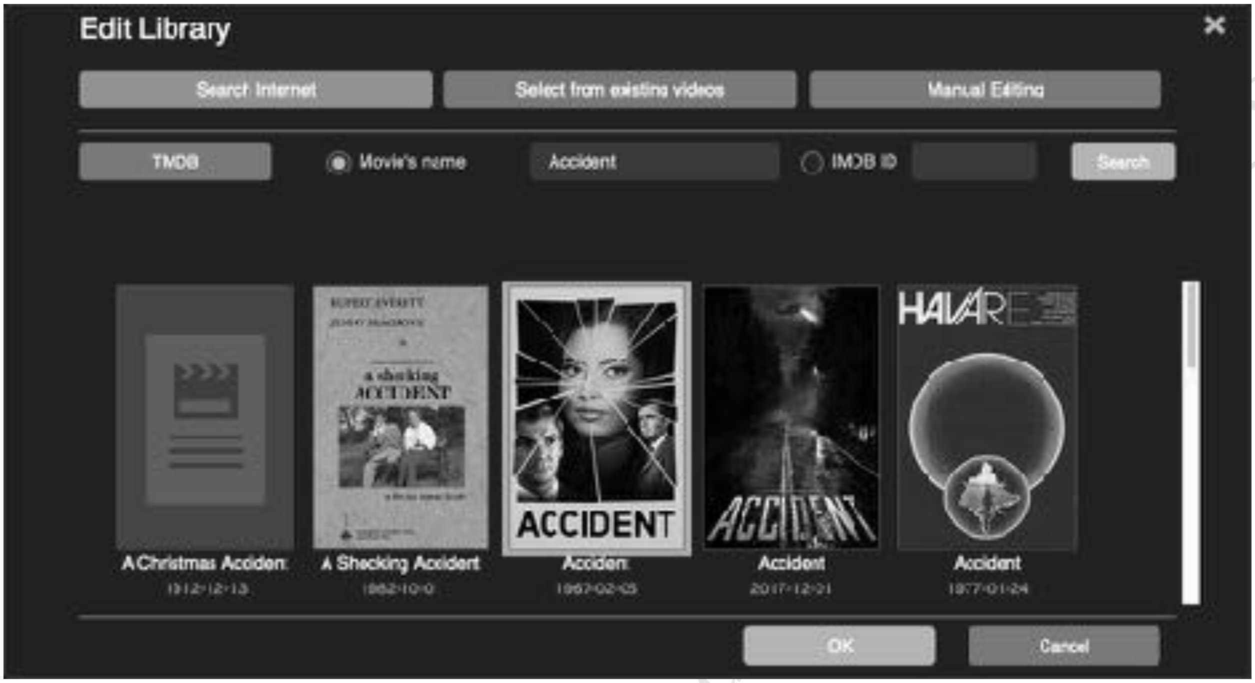


Figure 152: Movie with missing information

On the resultant panel, the information can be typed in. However, there is also a ‘Search Internet’ panel and sometimes typing in the name of the movie and clicking **Search** will find a suitable candidate, as in this case. Highlight the candidate movie and click **OK** to update the listing.



Edit Library

● Movie's name: Accident

○ IMDB ID

A Christmas Acciden 1912-12-13

A Shocking Accident 1982-10-0

Accident 1967-02-05

Accident 2017-12-21

Accident 1977-01-24

Figure 153: Updating movie with missing information

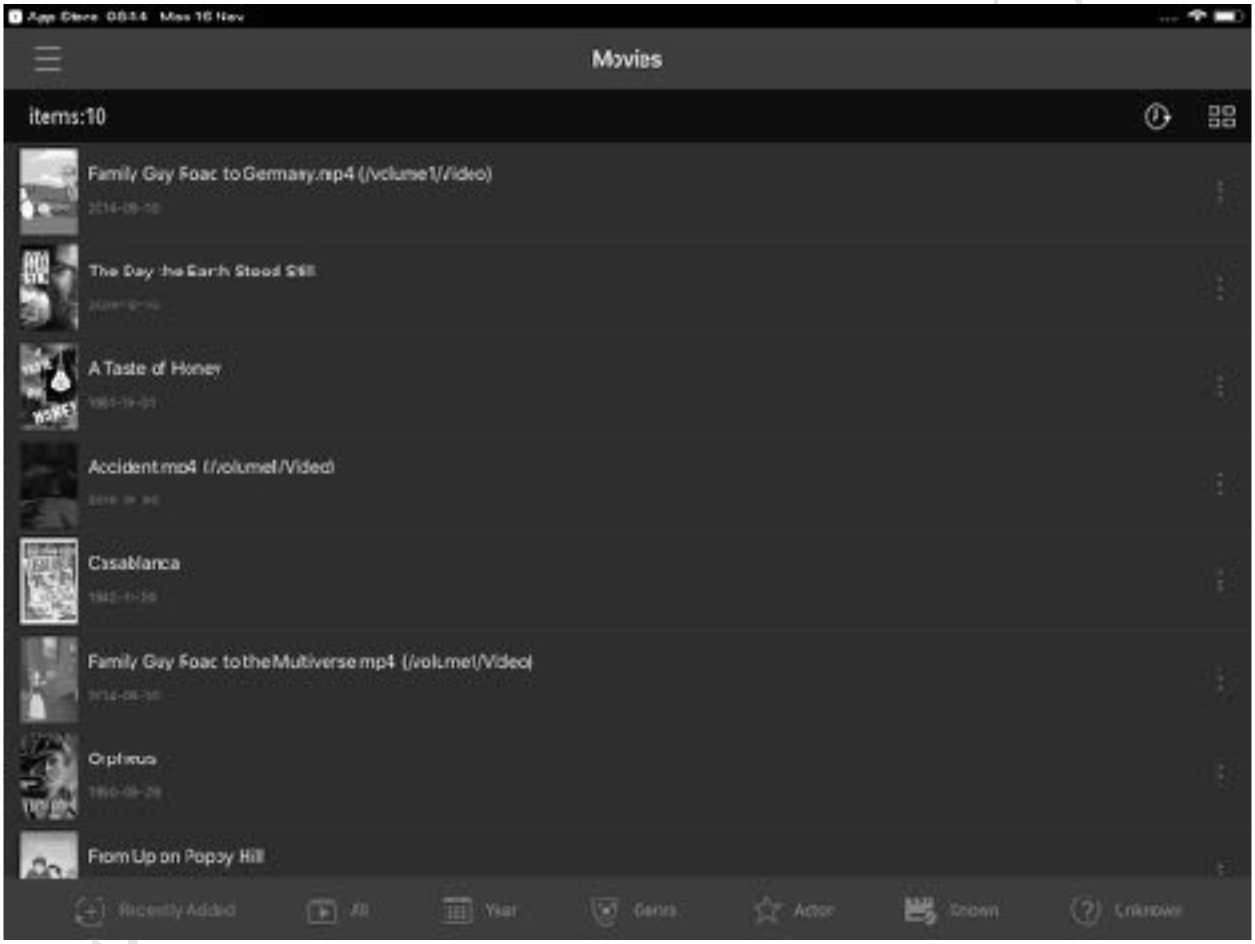
To play a video, move the mouse cursor over the thumbnail and click the small ‘Play’ icon. You may be offered a choice of video resolution for the playback: the higher the number, the better the quality, but if you were connected remotely you may need to choose a lower resolution because of the speed of the internet connection. Another option is to simply click **Auto**. Click **Play** and the movie will open in a new browser tab for playback. If the mouse cursor is allowed to hover over the bottom of the screen, a status bar and controls for pausing the movie and changing the volume will appear.

Access to LooksGood can be controlled on an individual user basis. Go into P**references** > **App Privileges**, highlight the LooksGood app and click the **Edit** button. Place ticks against the users who should have access and click **OK**. Next, go to **Preferences** > **Shared Folders**, highlight the *Video* folder and click the **Access Rights** button. Place ticks in the appropriate columns; if you want them to be able to add additional videos to the shared *Video* folder give them Read-Write (RW) access, otherwise give them Read-Only (RO) access. Click **OK**. Suggestion: if you want to make LooksGood available to many users, consider creating a dedicated group e.g. *videousers* and give access to it. If you want everyone to have it, give access to the built-in *users* group.

AiVideos

AiVideos is an app for watching videos on smartphones and tablets, designed to work in conjunction with LooksGood on the server. It is available as a free download for iOS and Android from the respective app stores. Having installed it and acknowledged the privacy statement, the first thing to do is specify the details of the server by tapping the plus sign (+) in the top left-hand corner of the screen. If you are connected locally you can let the app find your server on the network via Auto Discovery, else manually specify the name or IP address. If you also want to be able to use AiVideos remotely you should enter your Cloud ID, which you may have registered during the installation of ADM (else see section 10.2 Setting up EZ-Connect for how to do so). It is suggested that you flip the HTTPS switch to the 'On' position to improve security.

The interface mimics that of the browser interface of LooksGood. The titles can be viewed as thumbnails or as a detailed list. The view can be filtered in different ways e.g. by Year, Genre and Actor.



items:10

Family Guy Road to Germany.mp4 (/volume1/Video)

The Day the Earth Stood Still

A Taste of Honey

Accident.mp4 (/volume1/Video)

Casablanca

Family Guy Road to the Multiverse.mp4 (/volume1/Video)

Orpheus

From Up on Poppy Hill

Figure 154: AiVideos running on iPad

To watch a video, tap it. An information screen about the video is displayed – tap the 'Play' icon to continue, then the Local Play option on the subsequent screens.

Videos can be downloaded to the portable device so they can be played back when there is no network connection, for example whilst travelling. Against each video are three small dots, which represent a menu. Tap it and choose the **Download** option.

9.5 Photo Gallery 3

Photo Gallery 3 is an application from ASUSTOR, downloadable from App Central, that allows photo collections to be managed on the NAS and viewed through an internet browser or on a mobile device. Launching Photo Gallery 3 will cause it to open in a new browser tab:

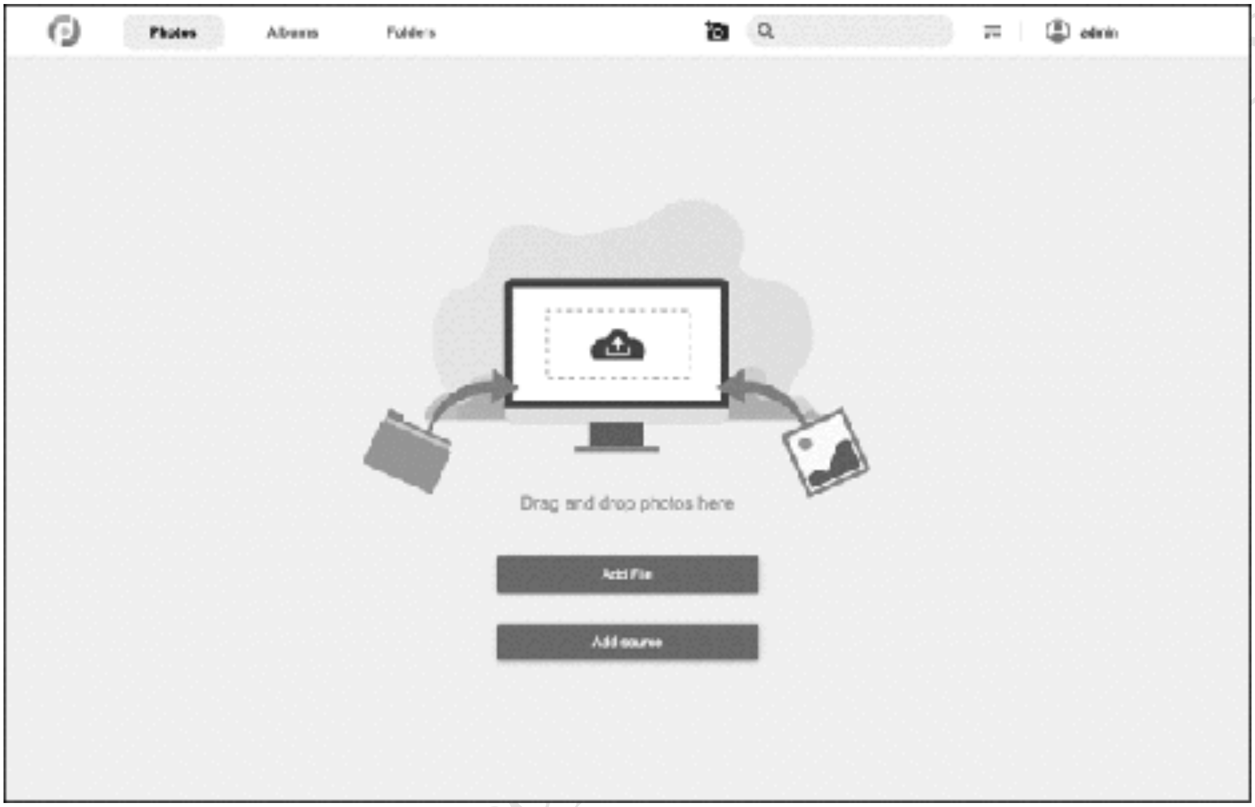


Figure 155: Photo Gallery 3

Each user receives their own folder, called *MyPhoto* and which resides in their personal *Home* folder on the server - any photos stored here are private to them. The installation of Photo Gallery 3 also creates a shared folder called *PhotoGallery*; if there is a requirement to have photos than multiple users can see e.g. family photos in a domestic environment, then they can be placed there.

The first time Photo Gallery 3 is used there may be a delay as the photos are indexed and, depending on the number and size of them, plus the overall performance of the NAS, this may be considerable. Thereafter the photos will be displayed, organized by date in a scrollable timeline format. The view can be switched to Albums or Folders:

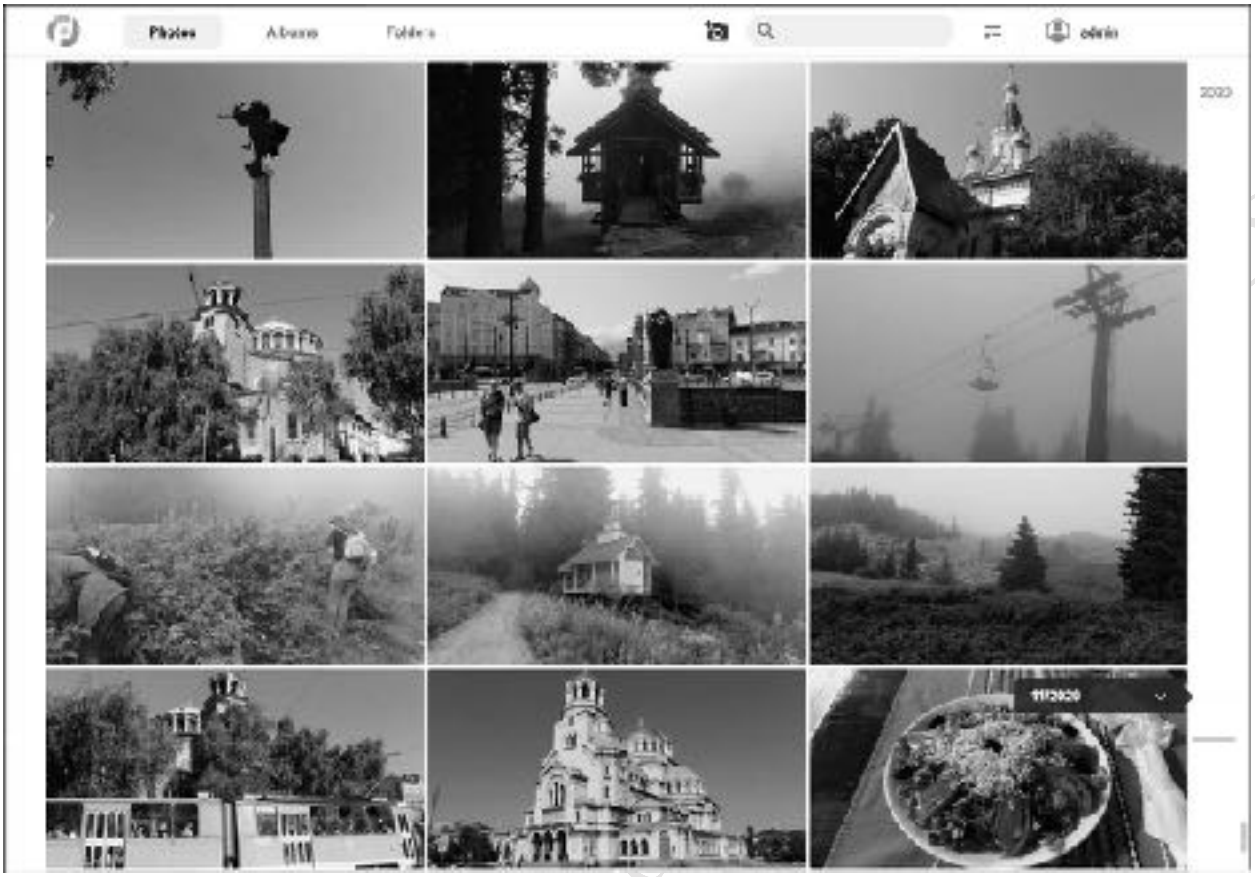
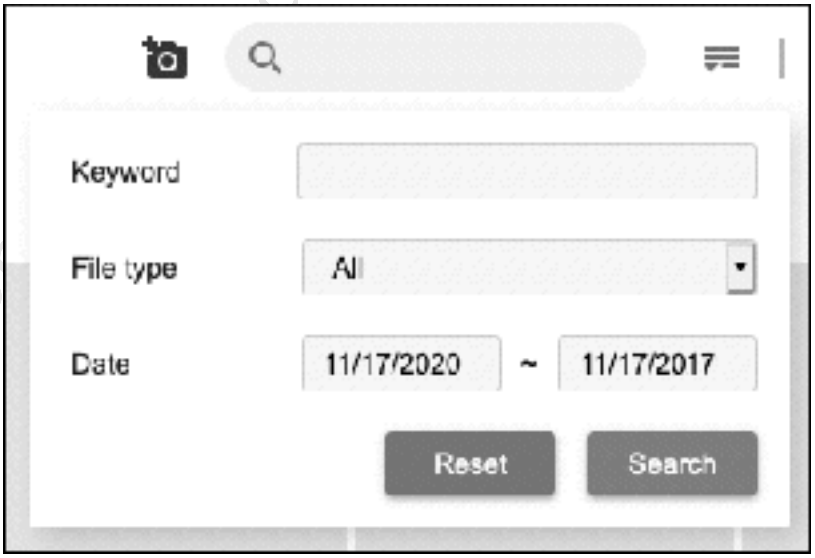


Figure 156: Photo Gallery 3, timeline view

At the top of the screen are icons to upload additional photos, search, plus set filters e.g. restrict view to a range of dates. When photos are added, there may be a warning about a delay caused by indexing.



Keyword

File type All

Date 11/17/2020 ~ 11/17/2017

Figure 157: Upload, Search and Filter options

To view a particular photo, click it. Hovering the mouse cursor over it will cause controls to be displayed, enabling the photo to fill the window, downloaded to the local computer, rotated or played as part of a slideshow. Controls are provided to view the previous and next photos; there is also a ‘film strip’ control at the bottom of the screen. To zoom into a picture, double-click whilst viewing it.

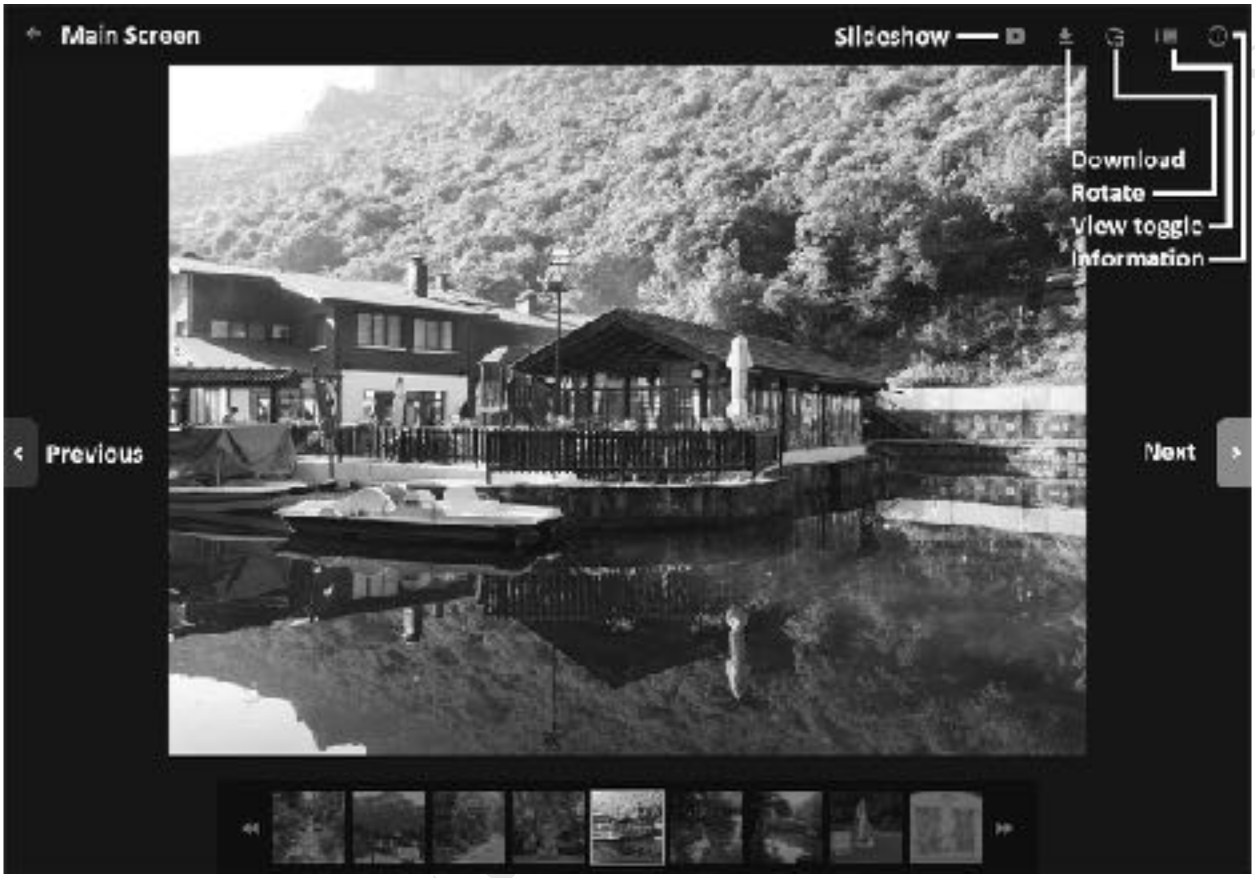


Figure 158: Working with an individual photo

When finished viewing photos, close Photo Gallery 3 by closing the browser tab.

Access to Photo Gallery 3 can be controlled on an individual user basis. Go into P**references** > **App Privileges**, highlight the Photo Gallery 3 app and click the **Edit** button. Place ticks against the users who should have access then click **OK**. Suggestion: if you want to make Photo Gallery 3 available to many users, consider creating a dedicated group e.g. *photousers* and give access to it. If you want everyone to have it, give access to the built-in *users* group.

AiFoto 3

Photos and videos stored on the server can be viewed on smartphones and tablets using the *AiFoto 3* app, available for iOS and Android and downloadable from the respective App Stores (important: be sure to download *AiFoto 3* rather than the earlier *AiFoto* app).

When running it for the first time, it will ask for access to the photos stored on the device, which you should grant. There is a quick overview, which you can work though, then enter your server and login details. It is suggested you enter your Cloud ID, which you may have registered during the installation of ADM (else see section 10.2 Setting up EZ-Connect for how to do so), as this will enable you to use the app remotely.

Photos are displayed as thumbnails on a ‘photo wall’. The view can be switched from this to Albums or Folders. The search facility and ‘three dot’ menu in the corner of the screen can be used to filter the selection of photos. Tap an individual photo to view it in detail, at which point you can also use pinch’n’zoom to magnify it further. Photos can be downloaded onto the device, so they can be viewed offline.

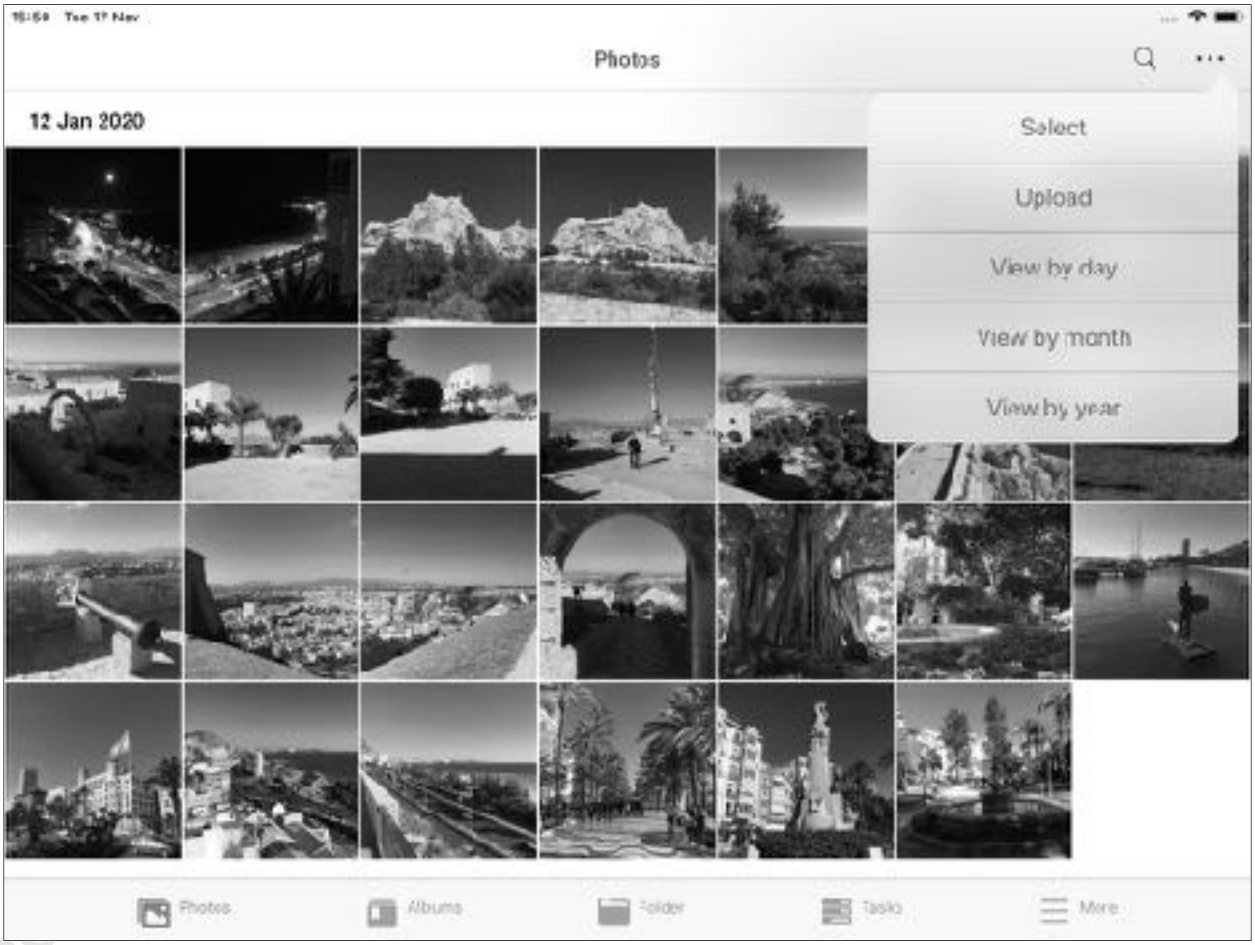


Figure 159: AiFoto 3 running on iPad

AiFoto 3 can be configured to backup photos taken on the device to the server. To enable this, tap the three line ‘More’ option. On the resultant screen, tap Photo Backup and slide the switch to the ‘On’ position. There is considerable control over the process: you can choose to backup photos from now on or include the ones already on the device; you can specify that photos only are backed up (i.e. exclude videos, which may be large in size); you can restrict uploads to Wi-Fi only (you may want to do this unless you have an unlimited or generous cellular/mobile data plan). Finally, you can restrict uploads to only when the device is charging, to avoid excessive battery usage whilst out and about:

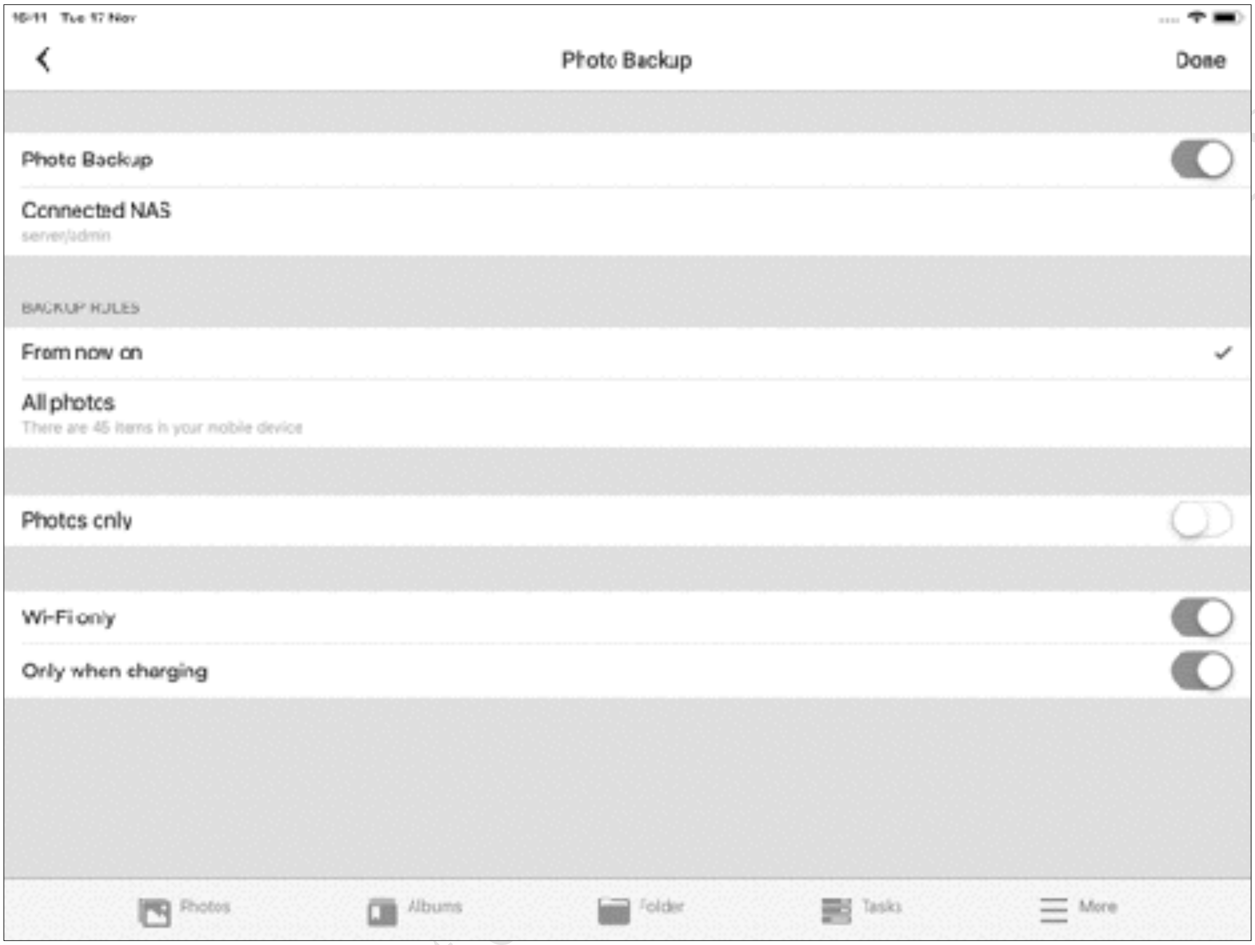


Photo Backup

Photo Backup ●

Connected NAS
server/admin

BACKUP RULES

From now on ✓

All photos
There are 45 items in your mobile device

Photos only ○

Wi-Fi only ●

Only when charging ●

Figure 160: Photo Backup options

9.6 Other Multimedia Apps

ASUSTOR provide a wide range of multimedia applications and additional ones are available from third parties. These apps may provide additional and improved capabilities, interface to a wider variety of devices for playback, or may just be more familiar or preferable to some people. Some of these are cross-platform systems which, although they run on ASUSTOR, were not specifically designed with it in mind and may not be quite as user-friendly as native ADM apps.

Plex

A good example of this is the highly popular *Plex Media Server*; in fact, may people specifically invest in a NAS system just in order to run this widely regarded piece of software. Some of its 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

An official Plex Media Server can be downloaded and installed from App Central. In order to use Plex Media Server, it is necessary to have an account with Plex. Also, some features require a paid subscription.

Most ASUSTOR models can run the Plex Media Server. However, entry level and less powerful models may not support hardware transcoding, which enables Plex to reformat videos into formats and resolutions which are better suited to playing on portable devices.

Plex clients, for connecting devices to the Plex Media Server, are available for Windows, Internet Browsers, Android, iOS, Apple TV, Roku, Amazon Fire TV, Chromecast, Xbox, PlayStation, Nvidia Shield and selected Smart TVs.

iTunes Server

This app from ASUSTOR turns the NAS into an iTunes server than can stream music and videos to Macs (using *Music* or *iTunes*) and Windows PCs (using *iTunes*). However, it does not work with iOS devices.

ASUSTOR Portal

The ASUSTOR Portal is not a multimedia app as such, but gives NAS models equipped with HDMI access to streaming services such as Amazon Prime and Netflix. It is covered separately in section 12.3 ASUSTOR Portal.

10

REMOTE ACCESS & CLOUD

10.1 Overview

Being able to access data remotely is an important requirement for most people and there are multiple ways of doing so with ASUSTOR NAS. Firstly, the NAS can be accessed using nothing more than a browser from any internet-connected device. Secondly, there is *EZ Sync,* which is analogous to a private version of *Dropbox.* Thirdly, there is *DataSync Center*, which integrates the NAS with popular cloud-based file sharing services such as *Google Drive*, *OneDrive*, *Dropbox* and others. Finally, it is possible to setup a *Virtual Private Network* (VPN), which may be of particular interest to business users. Computers or portable devices such as tablets and smartphones can be used with these connection methods.

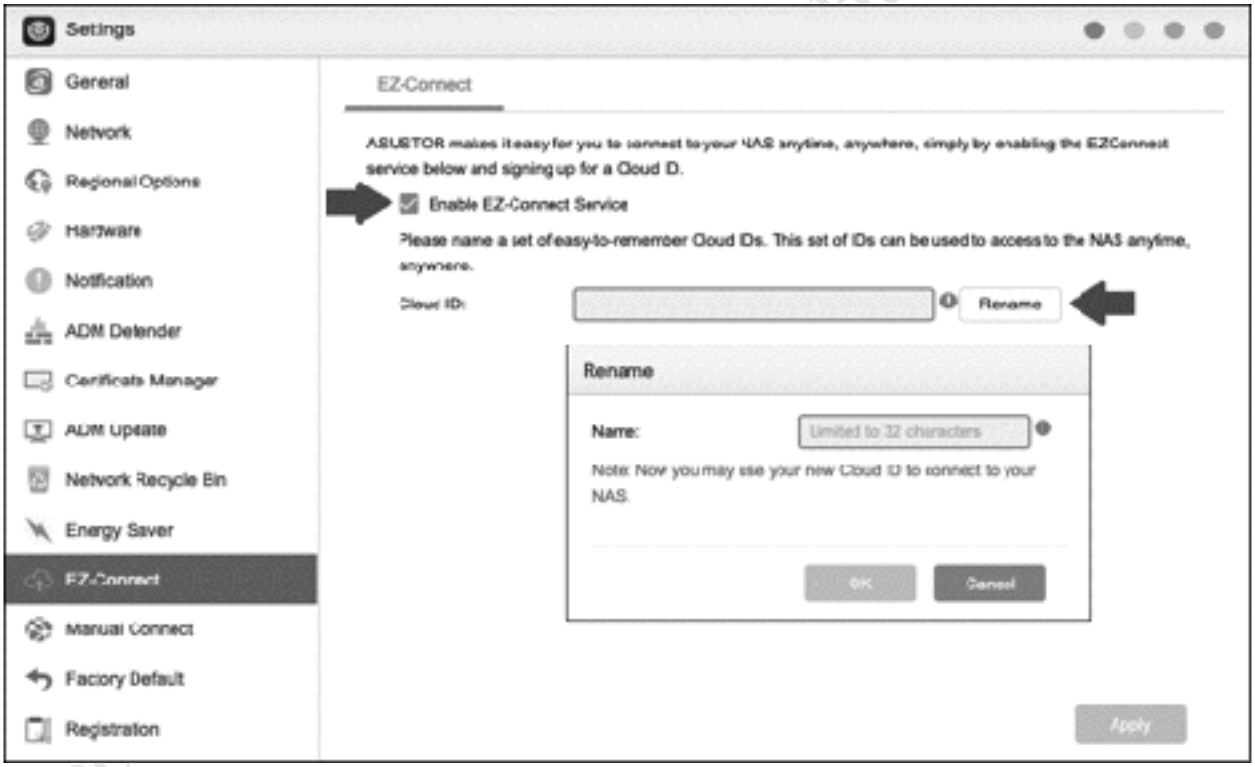
In order to access the NAS remotely, it first needs to be connected securely to the internet and configured in such a manner that it can be 'seen' from outside the home or office. There are two ways of doing so: a simple and straightforward method that will suit most home and many small business users, plus a more advanced method for more demanding requirements and which requires a certain amount of technical knowledge.

10.2 Setting up EZ-Connect

EZ-Connect provides an easy, straightforward mechanism for remotely accessing the NAS and works as a relay service, passing data to and from computers and the NAS over the internet via ASUSTOR. No data is stored at ASUSTOR itself and it always remains your data on your computers. Because the service uses standard web protocols it removes the need for techniques such as port forwarding, router configuration and domain services in most instances. This also means remote access is often available in many places where there is no opportunity to make technical changes to the underlying environment, such as in schools, colleges, workplaces and so on. *EZ-Connect* is suitable for most home and small business users.

To setup EZ-Connect you first need an ASUSTOR ID. You may have registered for one during the installation of ADM, else you can do it now by clicking **Preferences** > **Registration**. Click the **Create new account** link and complete the resultant form. For the ASUSTOR ID, use an existing email address.

Go to **Preferences** > **EZ-Connect** and tick the **Enable EZ-Connect Service** box. Enter a name for the *Cloud ID*, which will become the internet address of the server. This step is not intuitive, as rather than type in the provided field directly you need to click the **Rename** button and type it in there. The Cloud ID can be up to 32 characters in length and can largely be whatever you want, with the proviso that all the obvious names have long since been taken. You could, for instance, base it on the name of your household or organization. Click **OK**, then **Apply** on the original screen.



ASUSTOR makes it easy for you to connect to your NAS anytime, anywhere, simply by enabling the EZConnect service below and signing up for a Cloud D.

☑ Enable EZ-Connect Service

Please name a set of easy-to-remember Cloud IDs. This set of IDs can be used to access to the NAS anytime, anywhere.

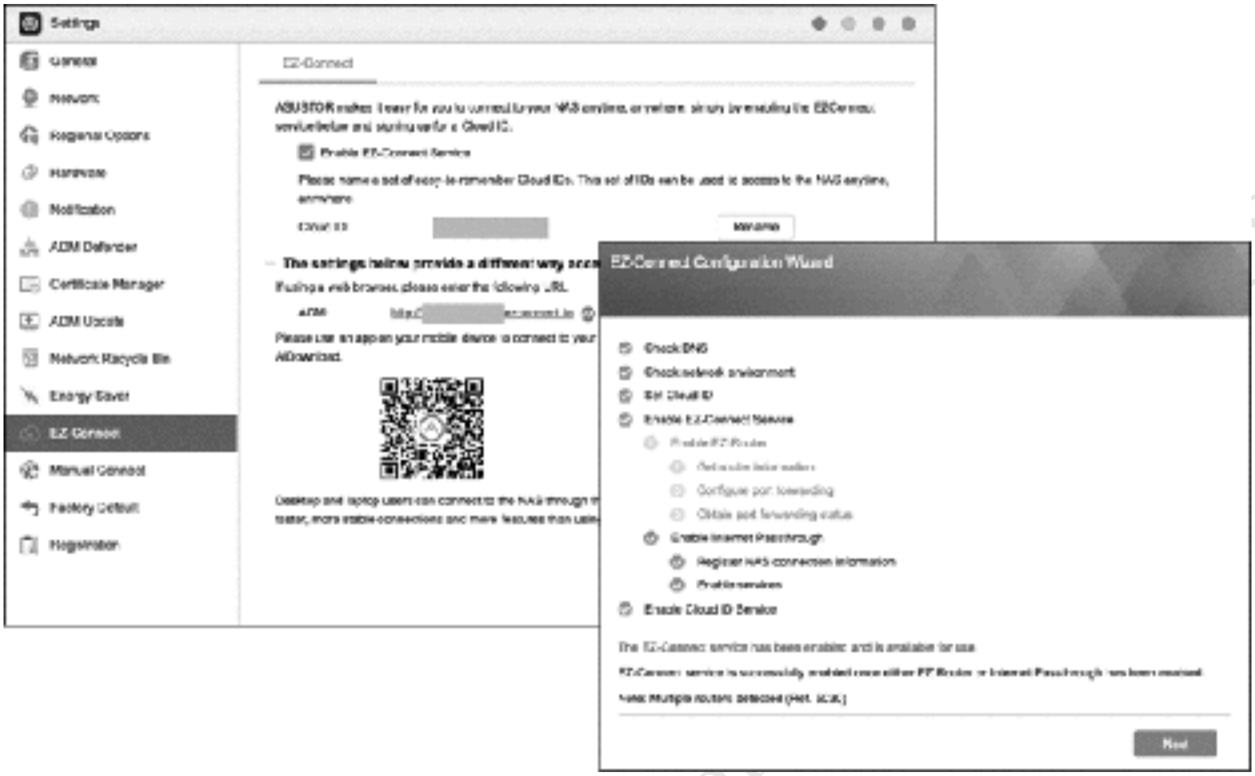
Cloud ID:

Name: Limited to 32 characters

Note: Now you may use your new Cloud ID to connect to your NAS.

Figure 161: Setting up EZ-Connect

The *EZ-Connect Configuration Wizard* will now run, which takes under one minute. This might result in a few errors and warnings, but provided the *Enable Internet Passthrough* and *Enable Cloud ID Service* entries have green ticks against them, then you should be good to go. Click **Next**, followed by **Finish** to return to the updated EZ-Connect screen, which will have been updated and will now include QR codes for connecting mobile devices.



The EZ-Connect service has been enabled and is available for use.

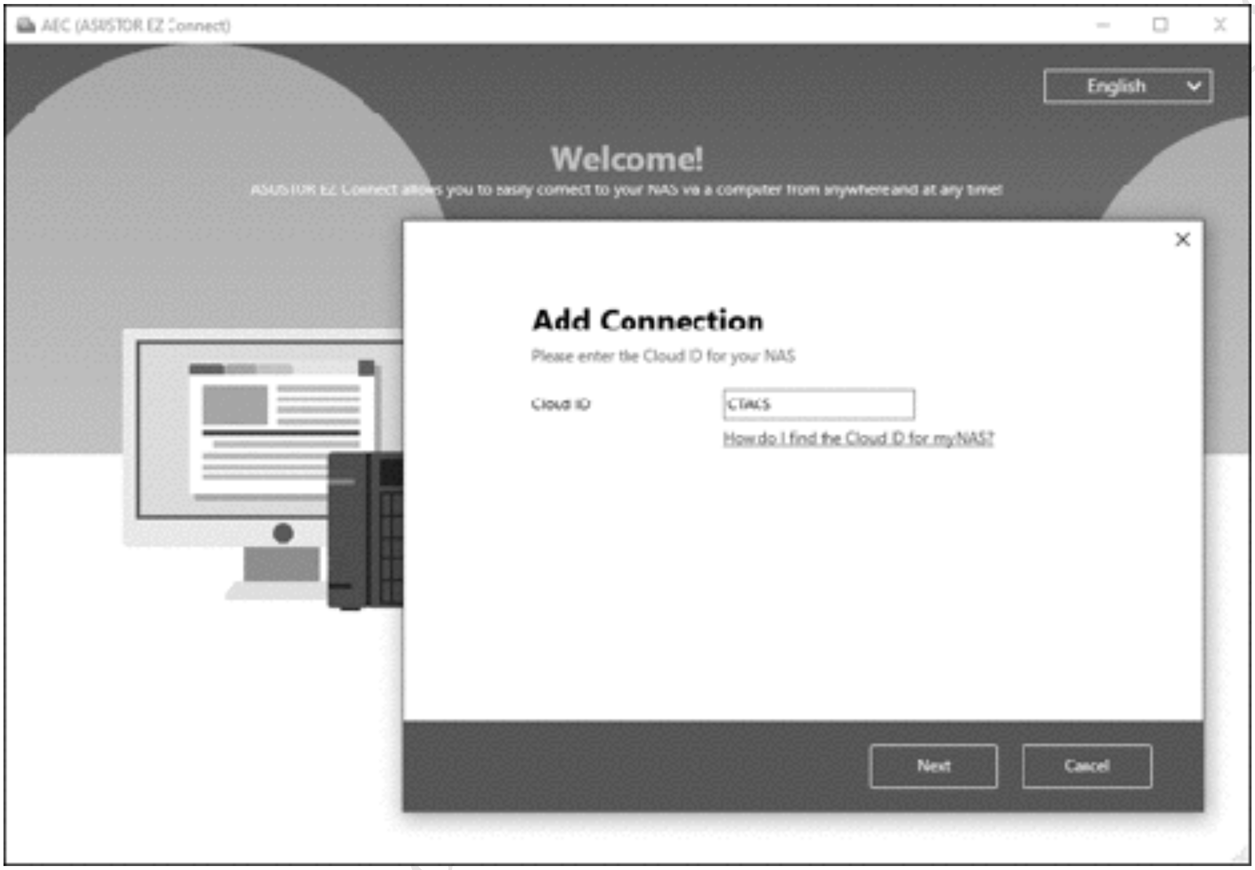
Figure 162: EZ-Connect Configuration Wizard & updated screen

At this point the NAS should be accessible over the internet. Its address consists of the Cloud ID followed by *ezconnect.to*, for example if you had called it *smithfamily* then the address would be *http://smithfamily.ezconnect.to* and if you enter this address in a browser you should see the standard ADM login screen of your NAS. As this this method of access is browser based, it is available to Windows, Mac, Linux, iPad and other platforms. ASUSTOR also have a dedicated utility for connecting Windows PCs, called *ASUSTOR EZ Connect*. Apps for mobile devices – *AiMaster*, *AiData*, *AiMusic*, *AiFoto* and *AiDownload* – can also connect using EZ-Connect.

Note: You may not be able to test remote connectivity from inside the home or office using your standard internet connection, as this requires a feature called NAT Loopback which most but not all routers support. To confirm things are working correctly, testing should be done from outside the office or home, for example by using a wireless hotspot in a coffee shop; alternatively, use a separate internet connection, such as a mobile broadband connection or a smartphone that supports tethering.

10.3 ASUSTOR EZ Connect Client for Windows PCs

ASUSTOR EZ Connect is a utility for Windows that allows easy connection to the NAS from remote locations. It is downloadable from the ASUSTOR website; during the installation, other supporting components may be downloaded and installed. Having installed it, click **Start** and enter the Cloud ID you registered earlier:



AEC (ASUSTOR EZ Connect)

Welcome!

ASUSTOR EZ Connect allows you to easily connect to your NAS via a computer from anywhere and at any time!

Add Connection

Please enter the Cloud ID for your NAS

Cloud ID: CTACS

How do I find the Cloud ID for my NAS?

Figure 163: Adding a connection

When prompted, enter your username and password. The first time it is run, a short tour is displayed, which you can work through or close. Upon a successful connection, the main screen appears as follows:

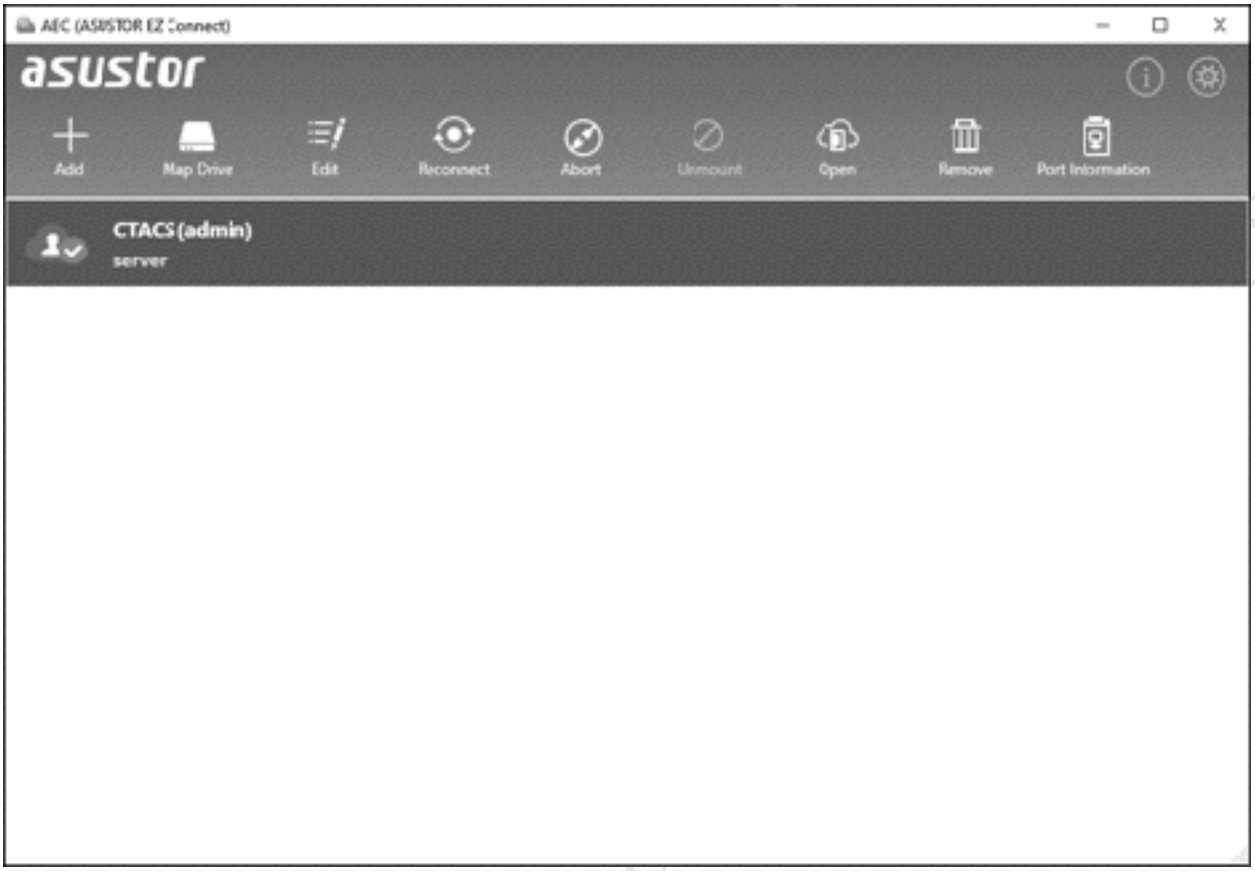
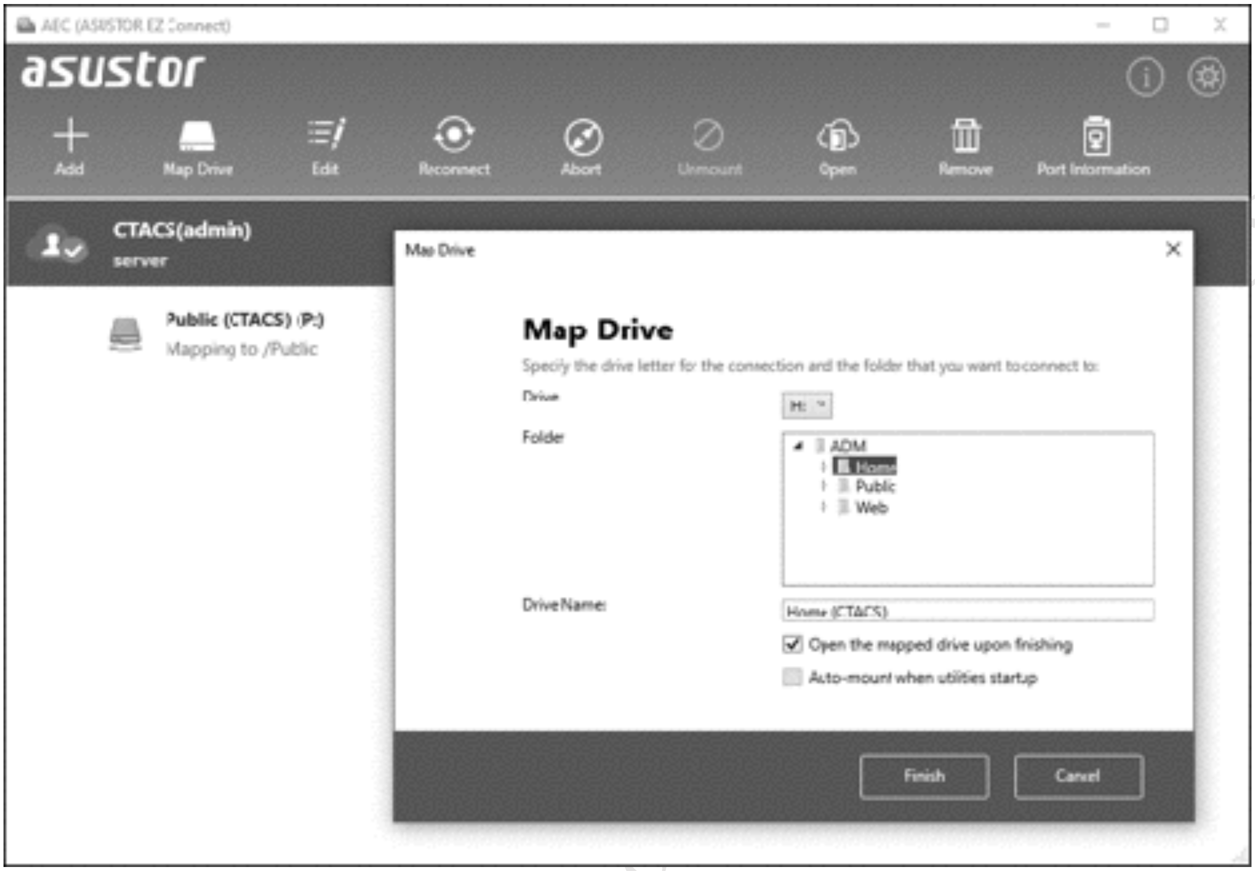


Figure 164: ASUSTOR EZ Connect main screen

Highlight the server and click the **Open** icon and you will be taken to the ADM Desktop, where you can use it in the normal manner, exactly as if you were at home or in the office.

Mapping a drive will enable you to use files and folders from within File Explorer/Windows Explorer and standard Windows applications. Click the **Map Drive** icon; select a folder and choose a drive letter from the dropdown e.g. P for Public, H for Home etc. If the **Auto-mount when utilities startup** box is ticked, then the drive will be available every time the computer is used. Click **Finish**.



CTACS(admin)
server

Public (CTACS) (P:)
Mapping to /Public

Map Drive

Map Drive

Specify the drive letter for the connection and the folder that you want toconnect to:

Drive: H:

Folder: ADM / Home / Public / Web

Drive Name: Home (CTACS)

☑ Open the mapped drive upon finishing

☐ Auto-mount when utilities startup

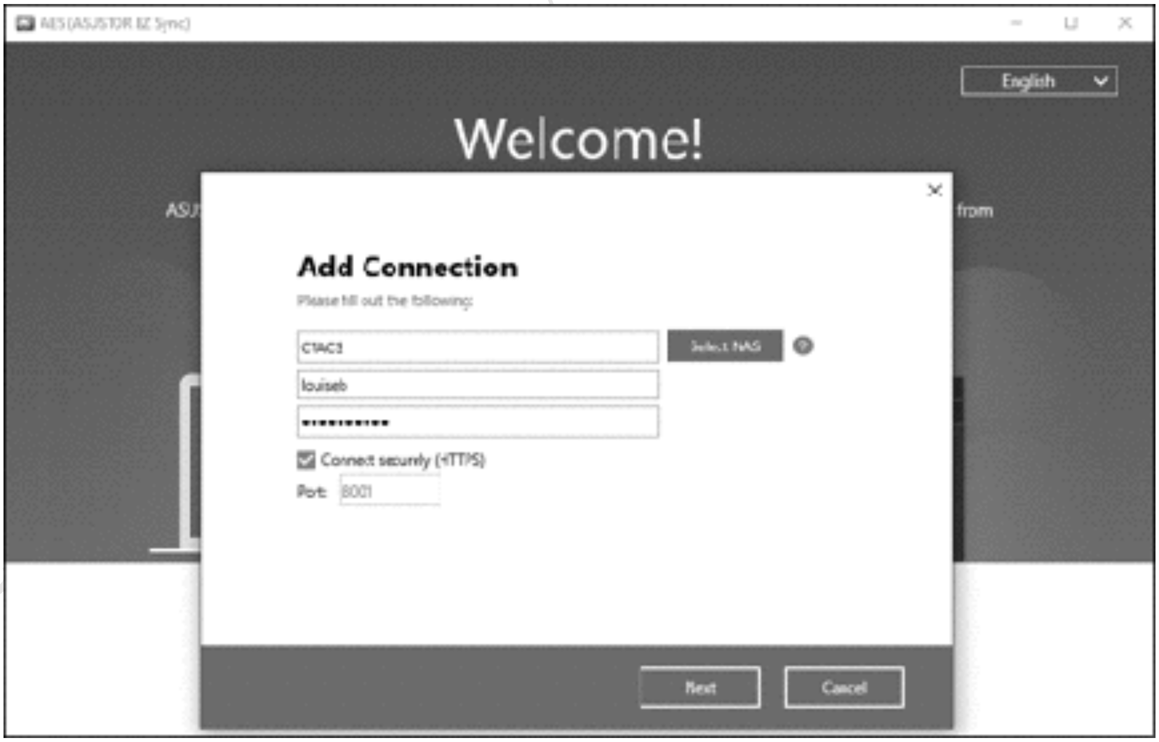
Figure 165: Mapping a drive

10.4 ASUSTOR EZ Sync

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

Whilst incredibly useful and popular, these public cloud services have limitations. Firstly, although they usually give some free storage space, it may not be very much and if you need more you have to pay for it. And, whilst these services may be relatively affordable, a regular monthly payment over several years may eventually amount to more than the cost of a NAS. Secondly, most services have restrictions on file sizes and how much data you can store on them. Finally, some people are just not comfortable with the idea of their data being held by Microsoft or Google or someone else. *ASUSTOR EZ Sync* gets around all of these issues: it is free to obtain and use; there are no practical restrictions on space and usage; data remains stored on your own server, meaning everything is under your control. Put simply – *ASUSTOR EZ Sync* enables you to have a *private cloud*. It is thus particularly suitable for people who travel away from home or the office where their NAS is located but who need to access their data.

ASUSTOR EZ Sync is a utility for Windows that allows easy connection to the NAS, both from within the office as well as from remote locations. It is downloadable from the ASUSTOR website; during the installation, other supporting components may also be downloaded and installed. Having installed it, click **Start** and enter the Cloud ID you registered earlier, along with your user name and password. It is suggested that you tick the **Connect securely (HTTPS)** box. Click **Next**. Note: if you only ever intend to use EZ Sync whilst in the home or office, you could click the **Select NAS** button and choose the NAS from the list.



Add Connection

Please fill out the following:

CTAC3

louiseb

•••••••••••

☑ Connect securely (HTTPS)

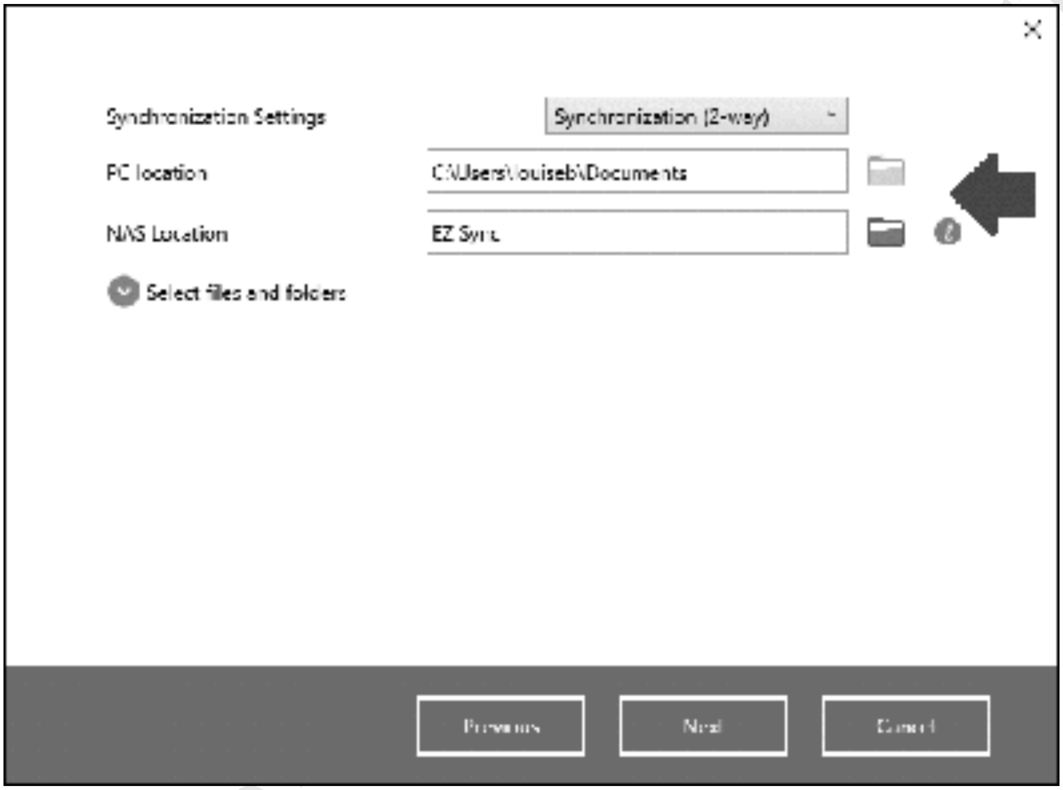
Port: 8001

Figure 166: Adding a connection

On the second panel you designate the folders to be synced. The basic principle here is to choose a shared folder on the PC and one on the NAS that EZ Sync will then keep in sync. Click the small icons on the right-hand side of the panel to select folders; for the PC location, you might choose the user's documents folder, whereas for the NAS location there is a built-in folder called EZ Sync for each individual user.

There are three possibilities for the *Synchronization Settings* dropdown. Most commonly you would want **Synchronization (2-way)**, which will cause the folders to mirror each other. However, you could choose *PC to NAS*, which would just back up the PC's folder to the NAS, or *NAS to PC*, which would do the opposite.

Having specified the folders, click **Next**.



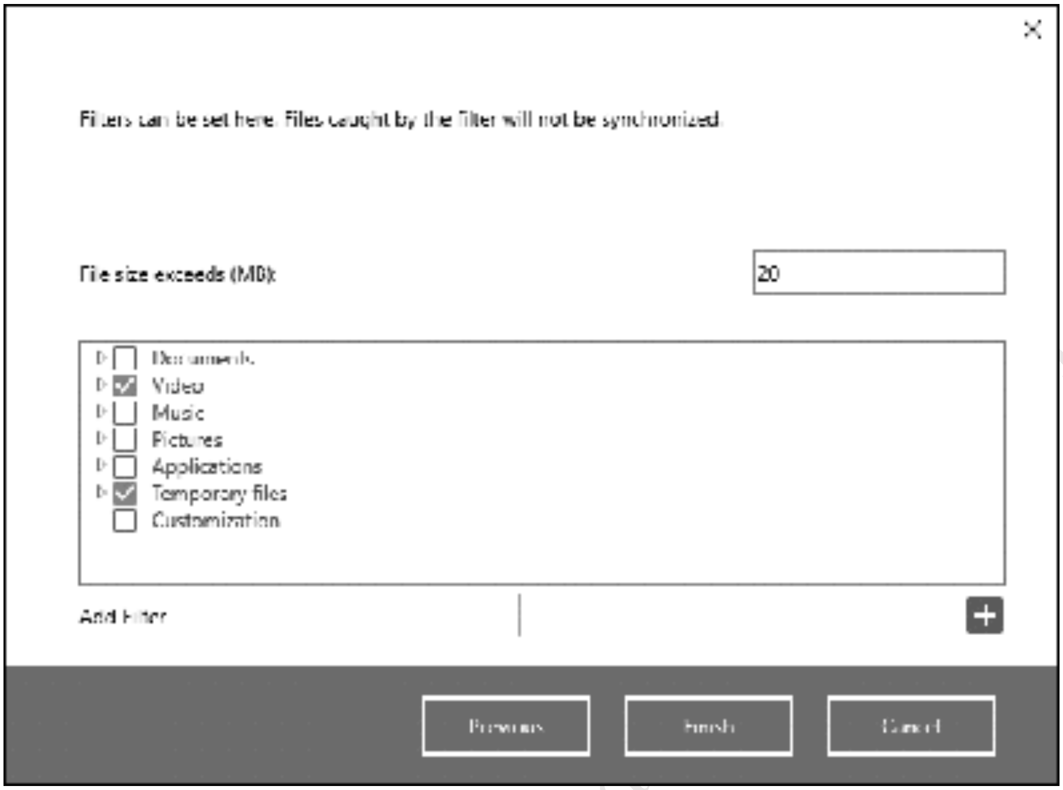
Synchronization Settings: Synchronization (2-way)

PC location: C:\Users\louiseb\Documents

NAS Location: EZ Sync

Figure 167: Specify the folders for synchronization

The subsequent panel enables filters to be specified. This prevents certain categories of files being synced and allows file size limits to be specified. For instance, you might not want to sync temporary files or videos larger than a certain size. Each of the categories can be expanded by clicking its chevron (arrow), enabling specific file extensions to be excluded/included e.g. you could sync DOCX, PPTX and XLSX files but no other Document types.



Filters can be set here. Files caught by the filter will not be synchronized.

File size exceeds (MB): 20

- ☐ Documents
- ☑ Video
- ☐ Music
- ☐ Pictures
- ☐ Applications
- ☑ Temporary files
- ☐ Customization

Add Filter

Figure 168: Filters

Having clicked **Finish**, a quick overview of the process is displayed and the main EZ Sync screen is shown. From here the status can be reviewed; the paired folders on the PC and NAS can be opened; synced folders can be added, edited or deleted. If you have access to more than one NAS, additional synchronization tasks for them can be added. There is also a widget placed on the taskbar. To sync files from the computer, just drag then into the designated folder on the PC. Synchronization occurs immediately, subject to the speed of your connection.

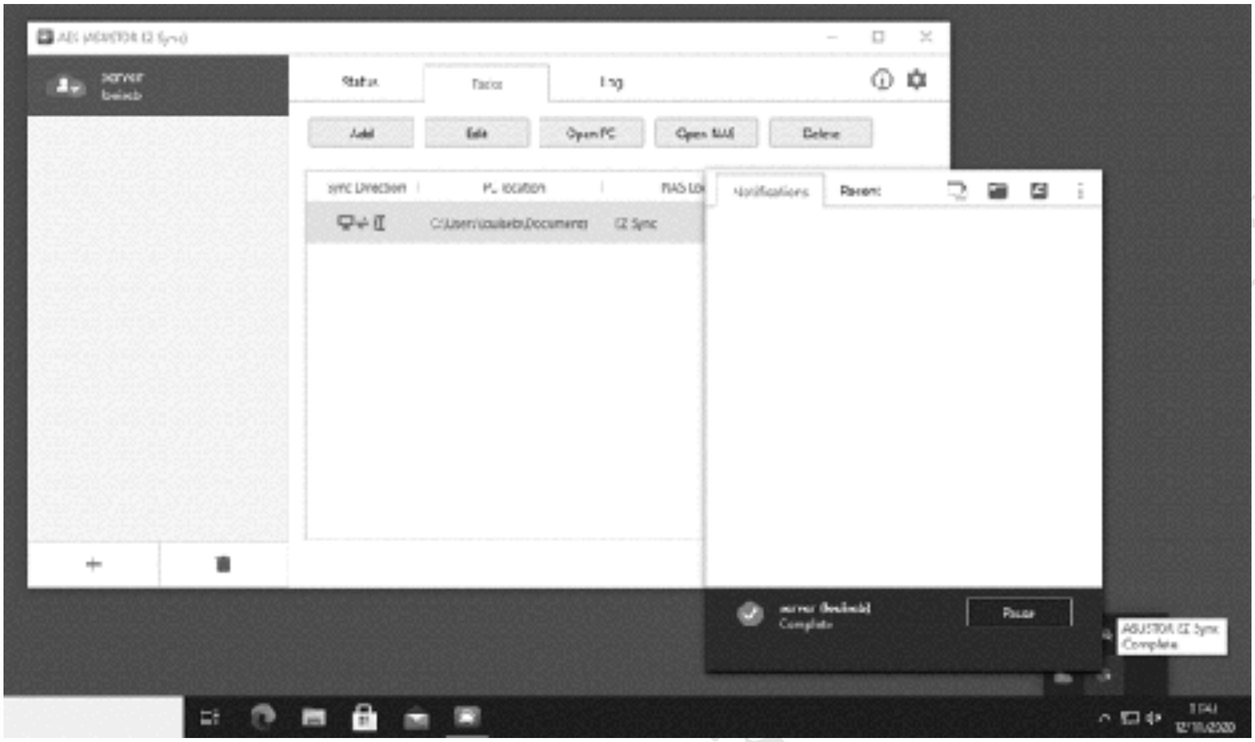


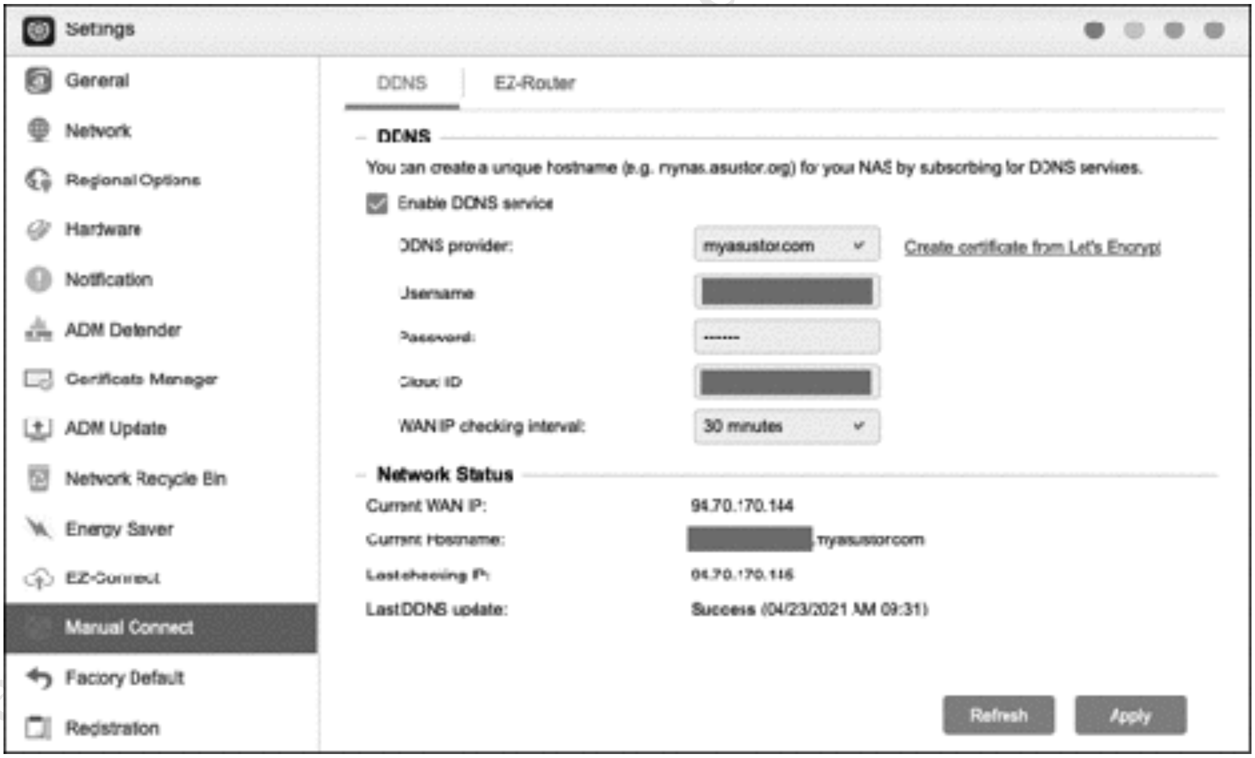
Figure 169: Main screen and widget

10.5 Dynamic DNS (DDNS)

The remote access capability of EZ-Connect as described in this chapter will suit many people. As an alternative to the ASUSTOR 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 ASUSTOR 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.asustor.com* or whatever you are interested in. But what is the name - strictly speaking, the *hostname* - of your NAS 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. However, for many people the simplest option is to use the *myasustor.com* service.

Click **Preferences** > **Manual Connect**. On the DDNS tab, tick the **Enable DDNS service** box and use the *DDNS provider* dropdown to select your service. Enter your *Username*, *Password* and the *Hostname* name that you acquired during registration (if you are using myasustor.com, *Hostname* will change to *Cloud ID*). There may be an additional dropdown for the WAP IP checking interval, but the default is usually fine. Click **Apply** and the Network Status section will be updated accordingly. In the case of myasustor.com, the DDNS Hostname will be your Cloud ID followed by myasustor.com e.g. *smithfamily.myasustor.com*.



DDNS

You can create a unique hostname (e.g. mynas.asustor.org) for your NAS by subscribing for DDNS services.

☑ Enable DDNS service

DDNS provider: myasustor.com

Username: [redacted]

Password: -------

Cloud ID: [redacted]

WAN IP checking interval: 30 minutes

Network Status

Current WAN IP: 94.70.170.144

Current Hostname: [redacted].myasustor.com

Last checking IP: 94.70.170.146

Last DDNS update: Success (04/23/2021 AM 09:31)

Figure 170: Screen for configuring DDNS

10.6 Virtual Private Networks (VPN)

The purpose of a *Virtual Private Network* or VPN is to securely extend a network to users who are offsite, such as home workers or those in a remote office, and 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 regular access to files and folders for editing, just as if in the office. The downside is that a VPN can sometimes be difficult to setup, configure and diagnose. ADM 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 weaknesses compared to later systems. 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 very different use of the term and NAS-based VPNs do not provide this capability.

Setting up the VPN Server

Begin by downloading and installing *VPN Server* from App Central. The initial screen asks for confirmation about the port numbers – assume everything is already in place and click the **Install** button. All aspects of managing the VPN are controlled from this app, which initially has a spartan appearance on the Overview screen. At the top of the screen, enable the type of VPN service you will be using by sliding its switch, which is L2TP/IPSec in our example. You can use multiple services simultaneously if required.

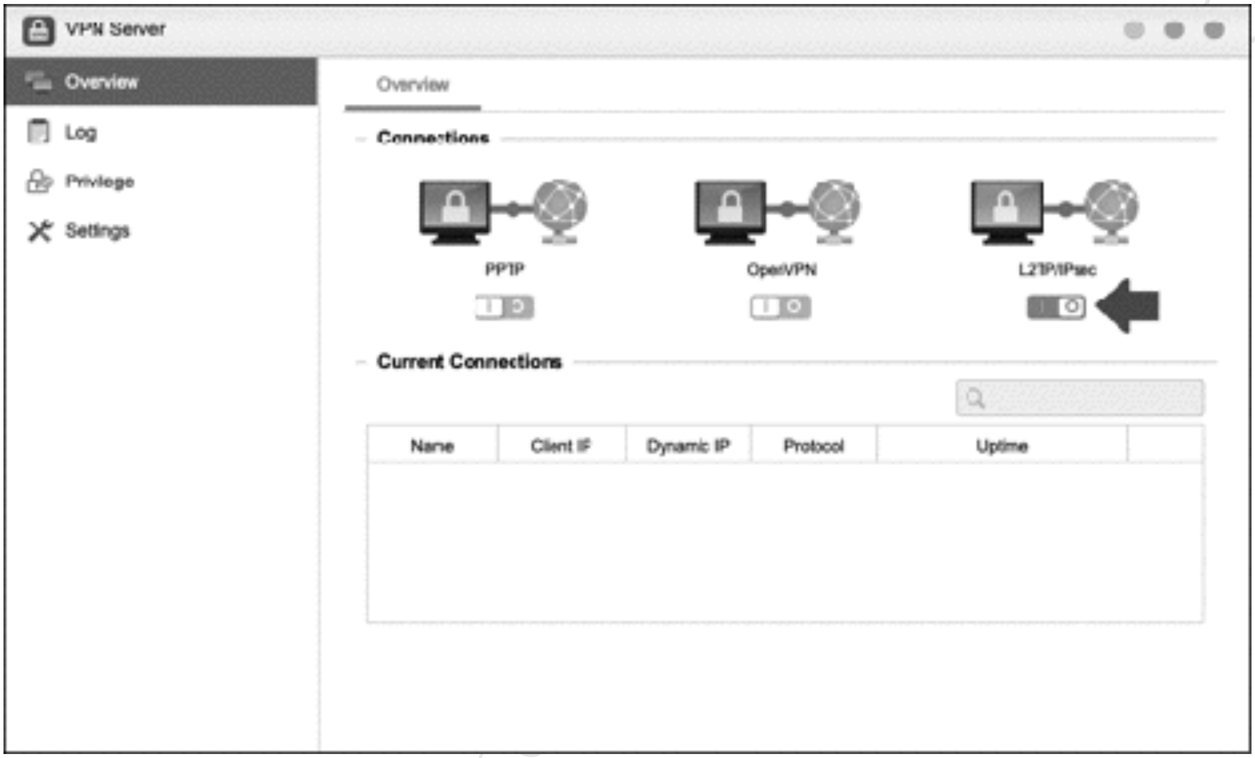
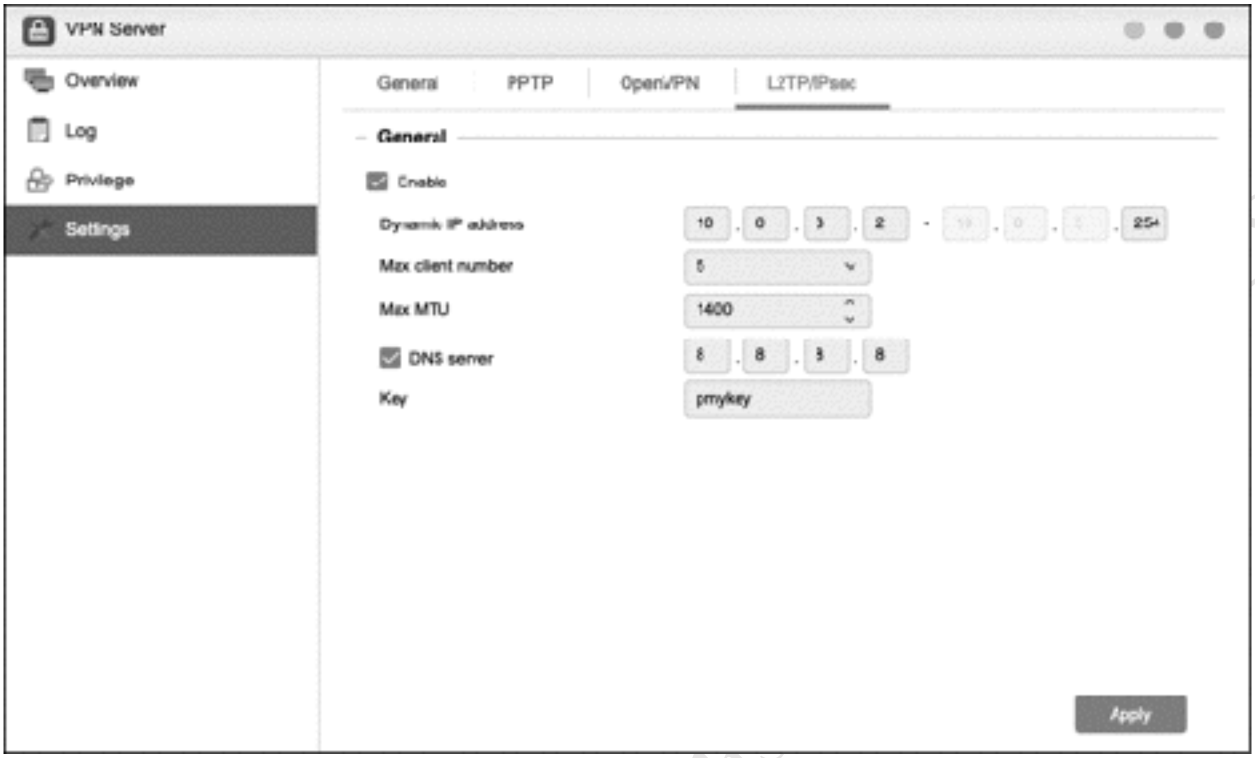


Figure 171: VPN Server Overview screen

Minimal work is required to get VPN running on the server and often it is just a matter of enabling the service. If it is necessary to change any of the parameters for some reason, click **Settings**, followed by the appropriate tab. In the case of L2TP/IPsec it looks like this:



☑ Enable

Dynamic IP address: 10 . 0 . 3 . 2 - 10 . 0 . 3 . 254

Max client number: 5

Max MTU: 1400

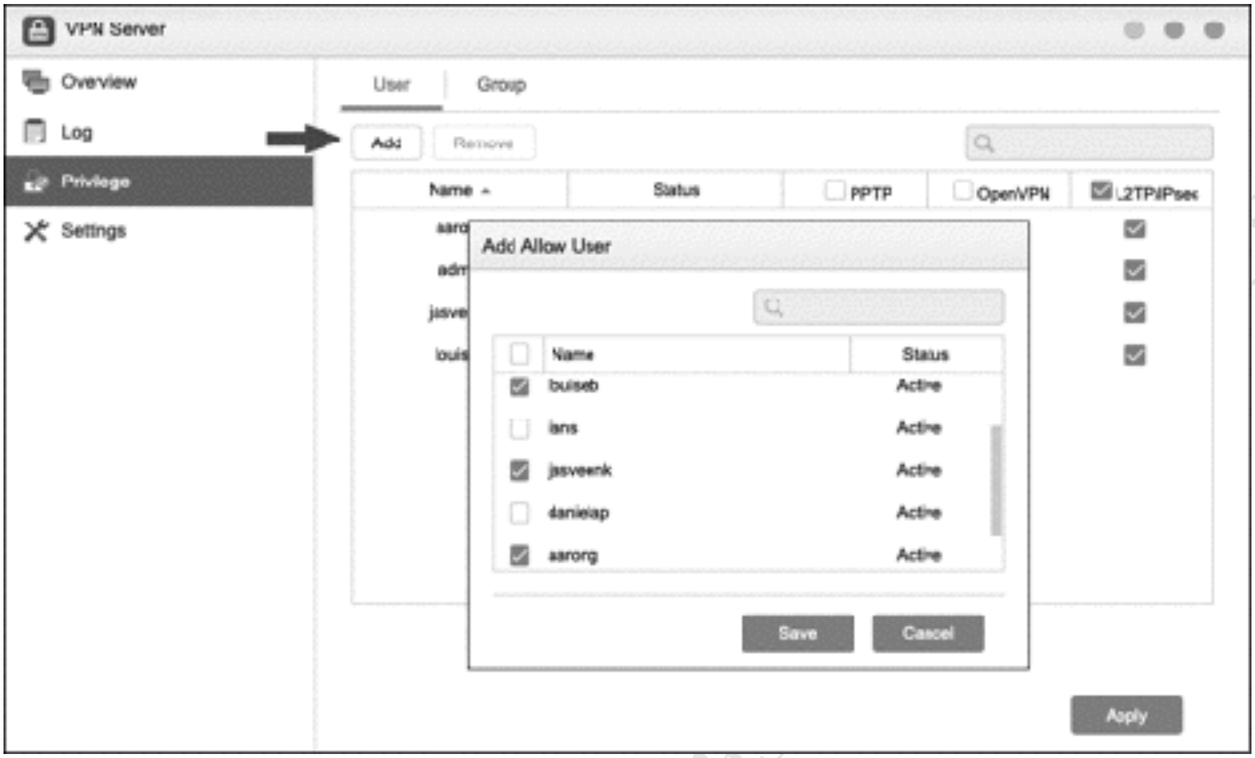
☑ DNS server: 8 . 8 . 8 . 8

Key: pmykey

Figure 172: L2TP/IPsec

The VPN has a range of IP addresses associated with it for use by the clients. 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 *Key* – effectively a password – should be changed to something less obvious, preferably much longer and involving a mixture of letters, numbers and special characters. It is not usually necessary to change any of the other parameters. Having made any changes, click the **Apply** button**.**

The users who will have access to the VPN now need to be defined. Click **Privilege**, followed by **Add**. Place ticks against the required users and click the **Save** button. Returning the main screen, place ticks in the appropriate columns for the chosen VPN types and click **Apply**.



□	Name	Status
☑	buiseb	Active
□	ians	Active
☑	jasveenk	Active
□	danielap	Active
☑	aarorg	Active

Figure 173: Adding users

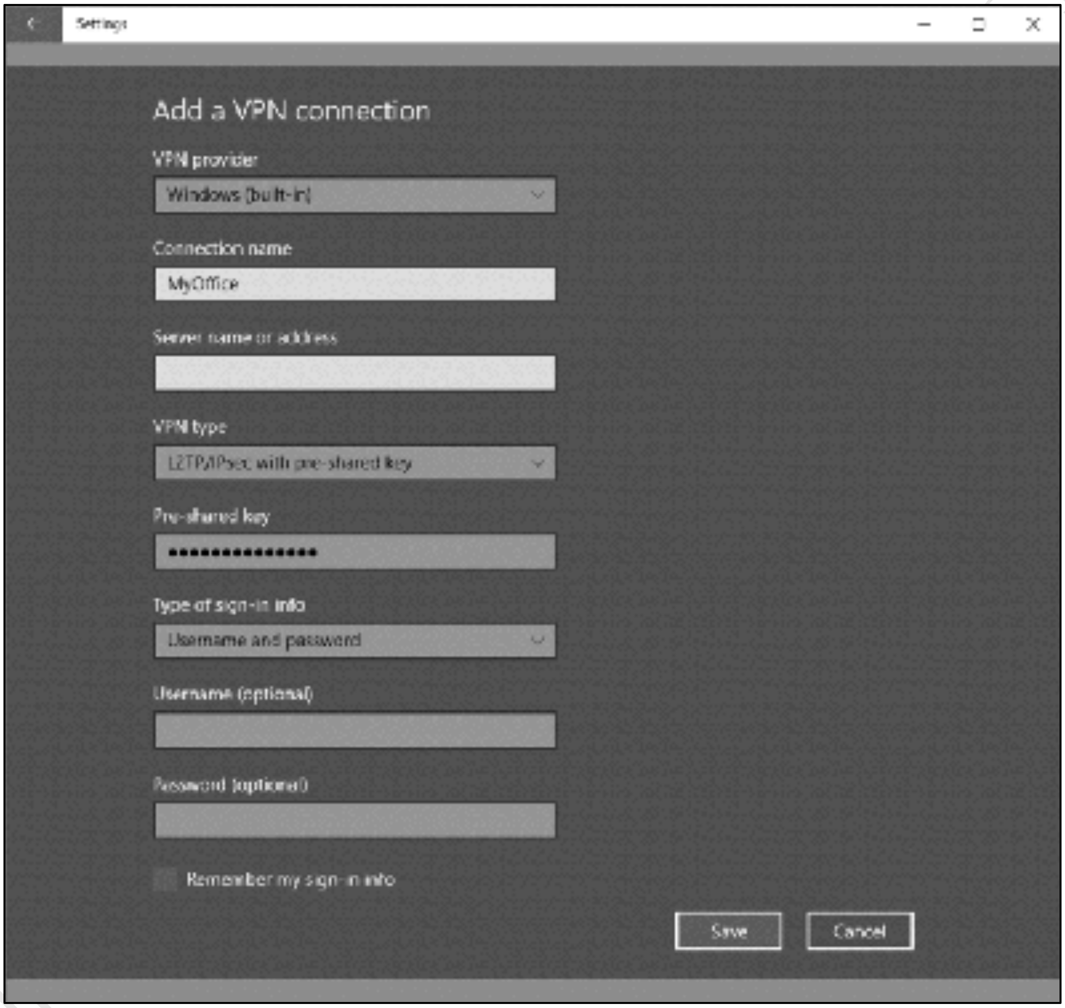
You need a hostname in order to access the VPN service. An easy way to obtain one is by setting up DDNS as described in 10.5 Dynamic DNS (DDNS).

Configuring VPN Clients

VPN client software is available for most platforms, including mobile devices. This section covers installation on three popular desktop platforms: Windows 10, Windows 7, macOS. There may be some minor variations depending on what type of VPN you are using plus any security options you may have chosen. Here we are using L2TP/IPSec.

Windows 10 Clients

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



Settings

Add a VPN connection

VPN provider

Windows (built-in)

Connection name

MyOffice

Server name or address

VPN type

L2TP/IPsec with pre-shared key

Pre-shared key

•••••••••••••••

Type of sign-in info

Username and password

Username (optional)

Password (optional)

□ Remember my sign-in info

Figure 174: 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 DDNS host name, such as that setup in 10.5 Dynamic DNS (DDNS) e.g. *smithfamily.myasustor.com*.

Set the **VPN type** to *L2TP/Ipsec with pre-shared key*, then enter the pre-shared key you specified when installing 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** and do not tick the **Remember my sign-in info** box. Click **Save**.

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

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

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

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)**:

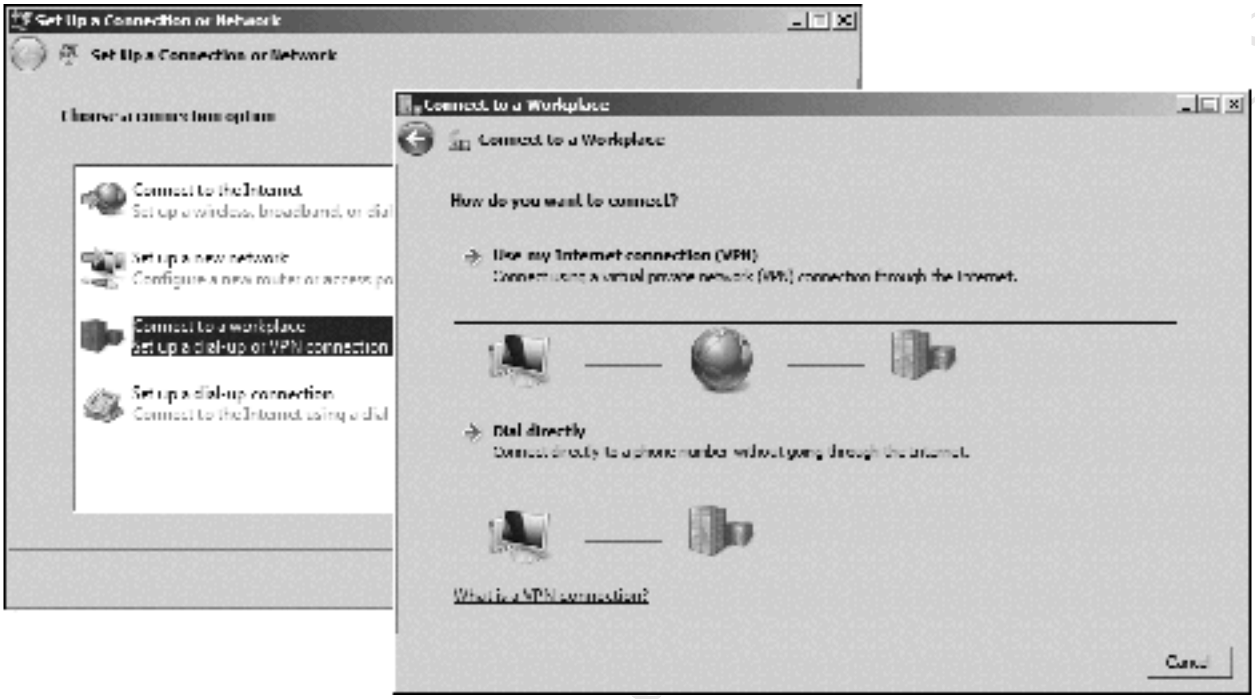
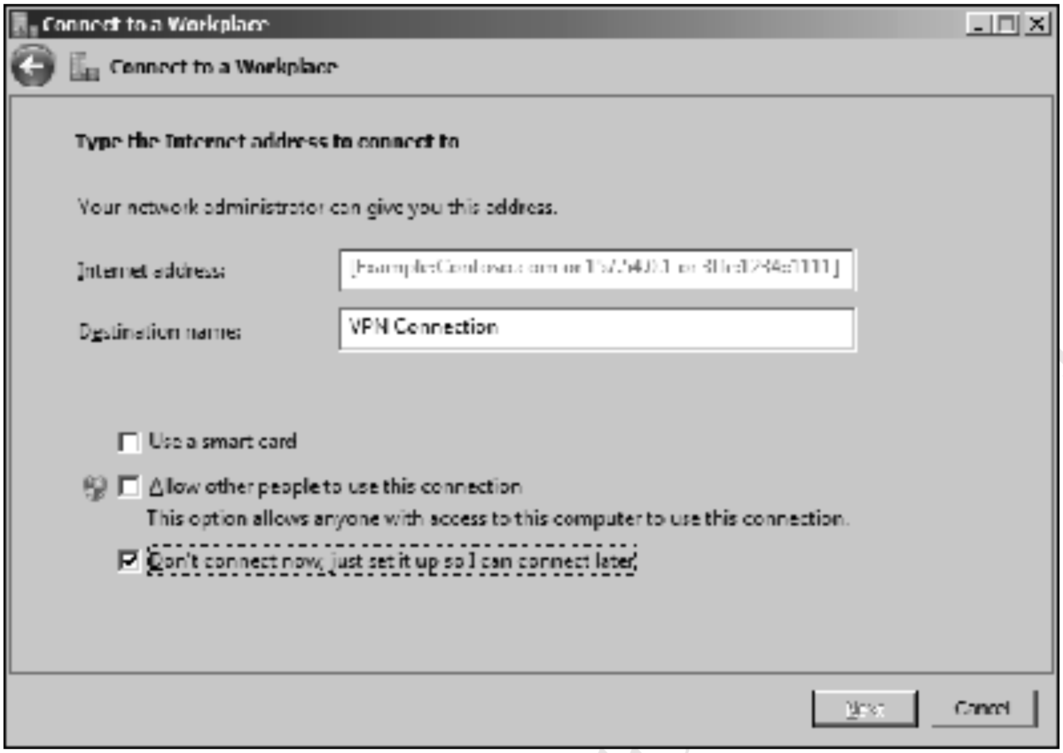

Set Up a Connection or Network
Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial
Set up a new network
Configure a new router or access po
Connect to a workplace
Set up a dial-up or VPN connection
Set up a dial-up connection
Connect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

Figure 175: Setup a new connection in Windows 7

For the **Internt address** enter the DDNS host name, such as that setup in 10.5 Dynamic DNS (DDNS) e.g. *smithfamily.myasustor.com*.Tick the **Don't connect now box** and click **Create**:



Connect to a Workplace

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: [Example:Contoso.com or 157.54.0.1 or 3ffe:1234::1111]

Destination name: VPN Connection

□ Use a smart card

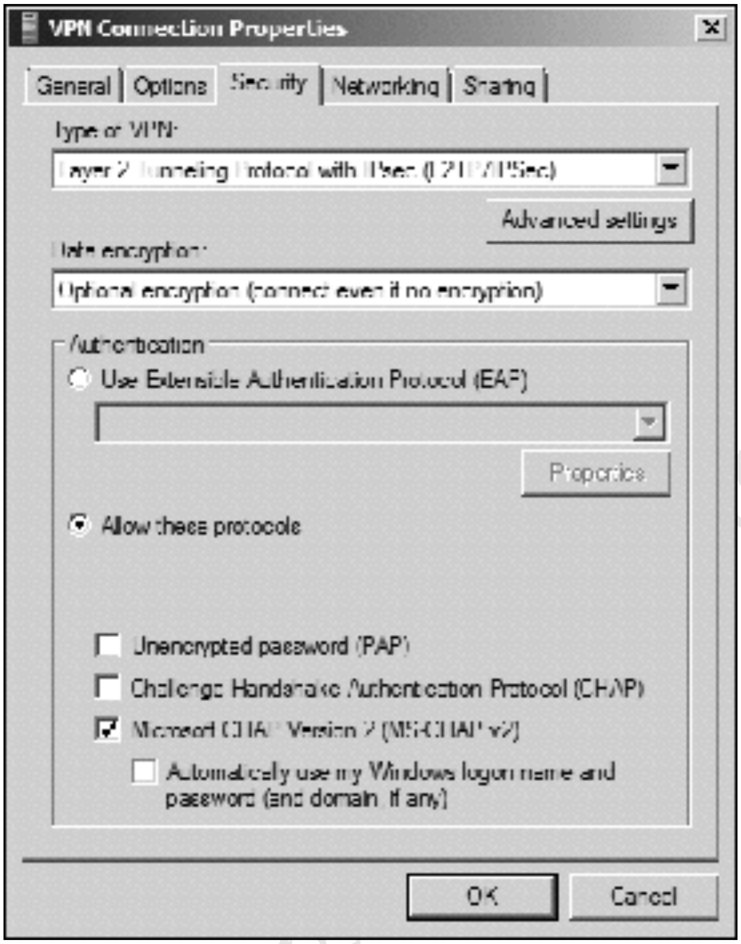
□ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

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

Figure 176: Specify the internet address of the server

You may be prompted to enter a *User name* and *Password* – this should be for a user that has already been defined on the server. The *Domain field* should be left blank. Click **Create** and a confirmation panel 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 *Key* which you specified when setting up the VPN Server (the 'password'). Click **OK**. The panel should appear as follows; click **OK**:



Type of VPN:

Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)

Data encryption:

Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

□ Unencrypted password (PAP)

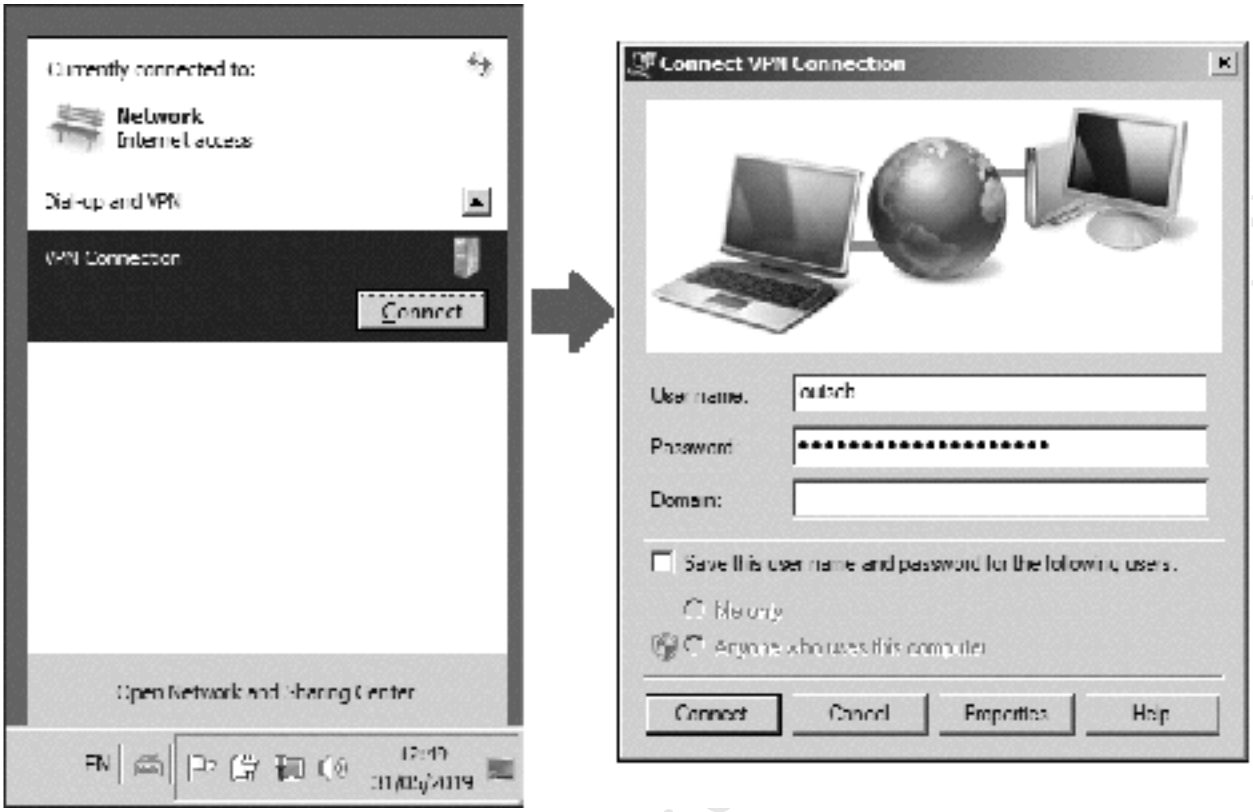
□ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

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

Figure 177: 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**:



User name: outsch

Password: ●●●●●●●●●●●●●●●●●●●●

Domain:

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

○ Me only

○ Anyone who uses this computer

Figure 178: Connecting to the VPN

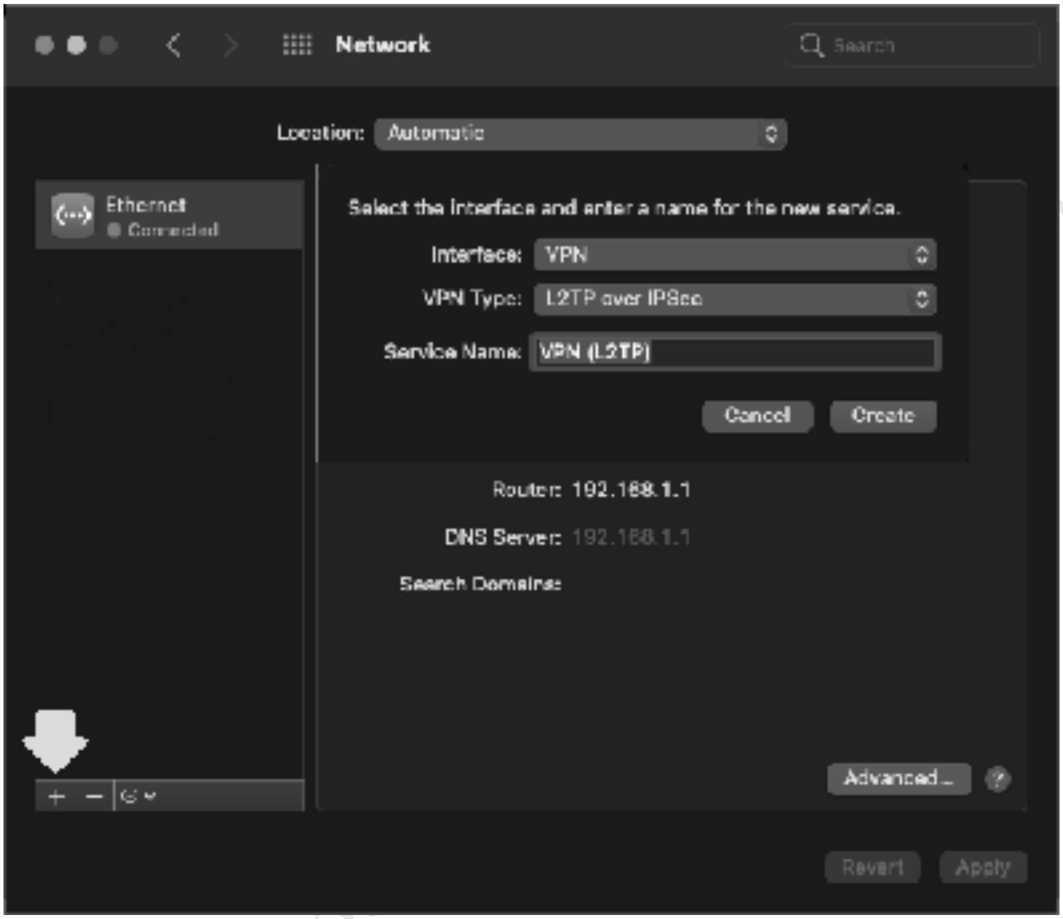
A few seconds later you should be connected. The first time you connect you may receive a prompt asking to choose the network location; a choice of Home, Work and Public is offered and you should choose **Home** or **Work** (there are no significant differences between them in this context).

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 *public* 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.

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.** Click **Create**:



Select the Interface and enter a name for the new service.

Interface: VPN

VPN Type: L2TP over IPSec

Service Name: VPN (L2TP)

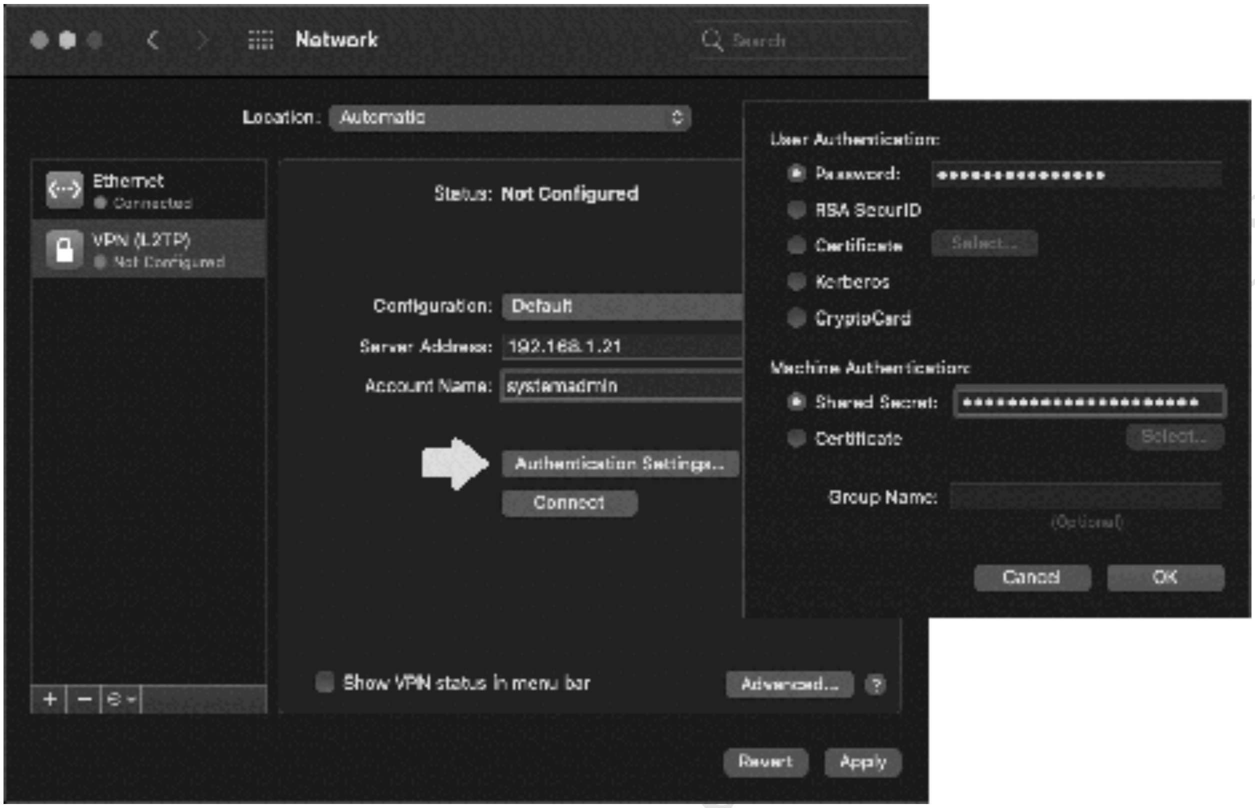
Router: 192.168.1.1

DNS Server: 192.168.1.1

Search Domains:

Figure 179: Add a new network service

Enter the **Server Address** enter the DDNS host name, such as that setup in 10.5 Dynamic DNS (DDNS) e.g. *smithfamily.myasustor.com*. 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 *Key*, which was defined during the configuration of VPN Server). Click **OK**. On the main screen, tick the **Show VPN status in menu bar** option, followed by **Apply**:



Location: Automatic

Status: Not Configured

Configuration: Default

Server Address: 192.168.1.21

Account Name: systemadmin

☐ Show VPN status in menu bar

User Authentication:

● Password: •••••••••••••••

○ RSA SecurID

○ Certificate

○ Kerberos

○ CryptoCard

Machine Authentication:

● Shared Secret: ••••••••••••••••••••••

○ Certificate

Group Name: (Optional)

Figure 180: 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.

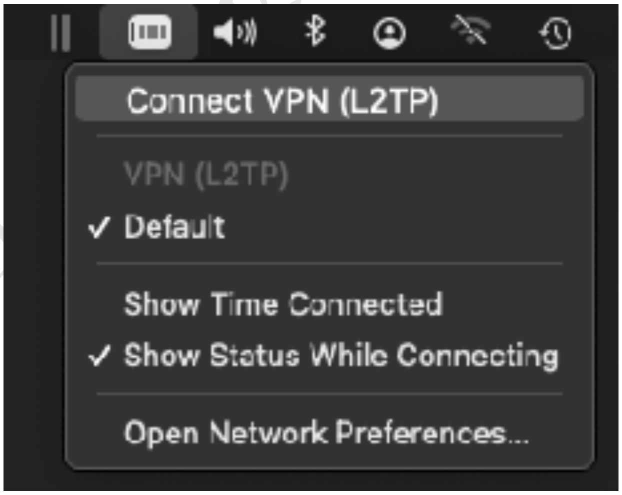


Figure 181: VPN icon on Menu bar

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**.

11

STORAGE

11.1 Overview

The basic principles of how ADM handles storage are described below. It is not strictly necessary to understand how it works, but it is useful. The remainder of the chapter explains RAID in detail, plus how to configure and use various storage options.

Basic Concepts of Storage

NAS devices use disk drives, which might be traditional mechanical hard disk drives (HDD) or solid-state drives (SSD). If the latter, they can be used for conventional storage, but on some models can also be used for *caching*, which provides high speed access to frequently used data (discussed in 11.5 SSD Caching).

The basic storage unit is the *volume*. All data – shared folders, documents, applications and so on - are stored on volumes. Before you can store anything, it is therefore necessary to have at least one volume and this is created during the initial installation of ADM in Chapter 2 INSTALLATION OF ADM.

A volume is made up of one or more drives. These drives can be configured for RAID to provide redundancy (data protection) and/or maximize performance. Various RAID types are available, described in the next section.

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 ADM, there are two different disk filing systems, *ext4* and *Btrfs* (sometimes pronounced 'butter-F-S'). Ext4 is a universal format, available to all ASUSTOR NAS users. Btrfs is a more sophisticated file system with advanced features, available on all models except entry-level ARM-based models. One of these advanced features 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.

Most aspects of storage are managed using the Storage Manager utility.

11.2 RAID

RAID is short for *Redundant Array of Independent (or Inexpensive) Disks*. There are various types of RAID, referred to using a numbering system: RAID 0, RAID 1, RAID 5 and so on. The basic idea is to improve reliability and performance by using multiple disks to provide redundancy and share the workload. ASUSTOR support many different RAID levels, depending on the model and the physical drives installed. The most common scenarios in home and small business systems are RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 and 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.

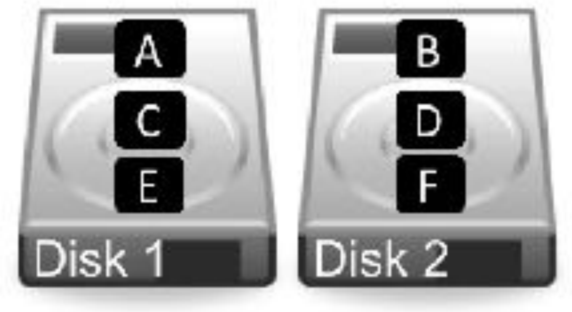


Figure 182: RAID 0 – Data striped across two drives

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 NAS has two 4TB drives installed then the total amount of usable storage capacity is 4TB rather than 8TB.

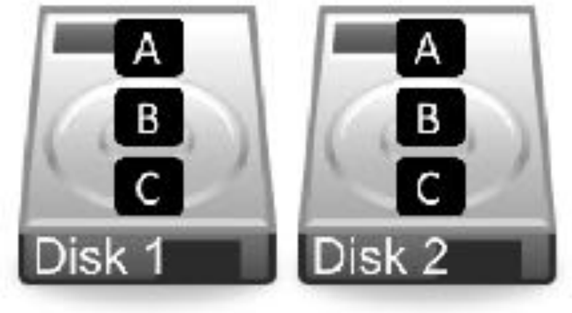


Figure 183: RAID 1 – Data mirrored across two drives

RAID 5 needs three or more four 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

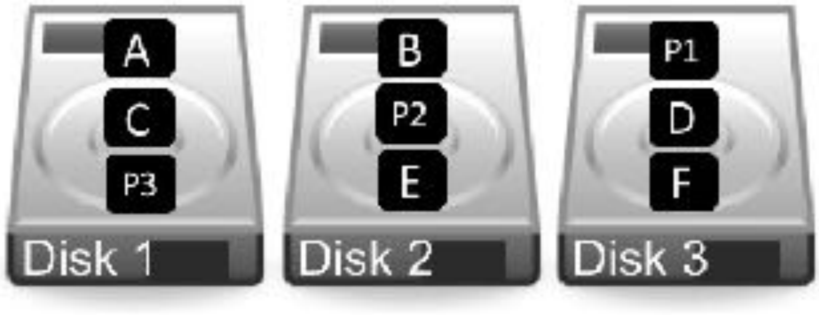


Figure 184: RAID 5 – Multiple drives with parity information

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.

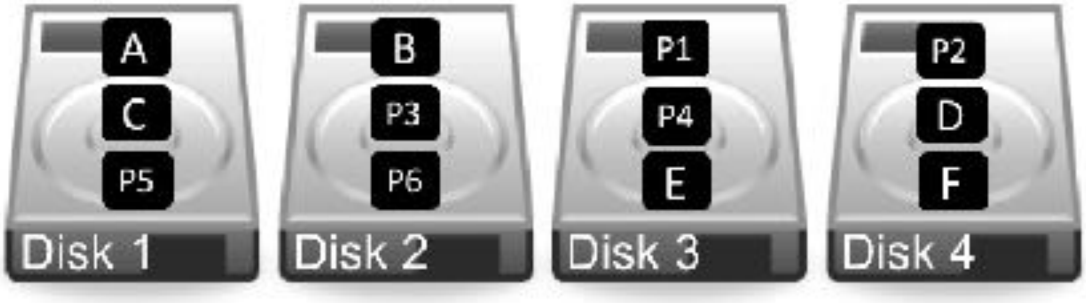


Figure 185: RAID 6 – Multiple drives with double parity information

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 in 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.

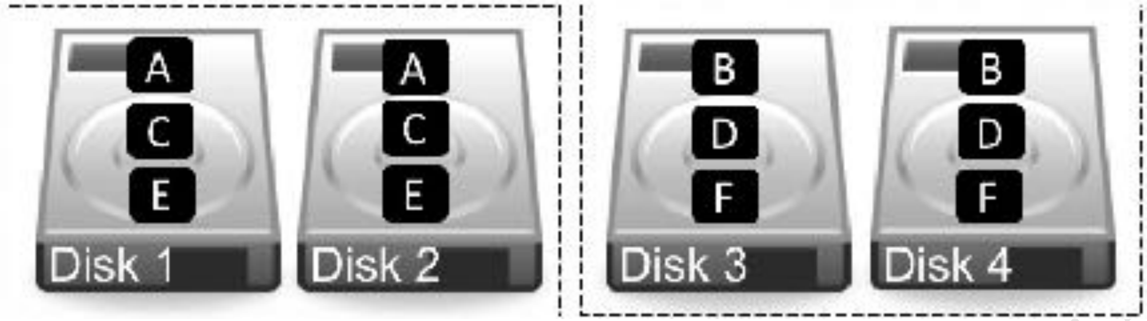


Figure 186: RAID 10 – Simultaneous striping and mirroring

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.

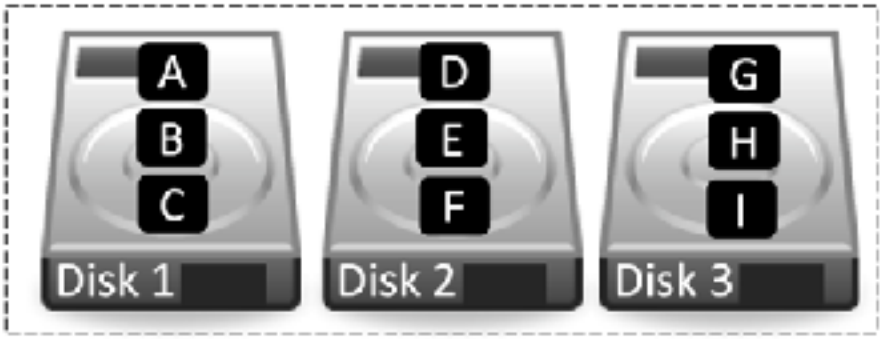


Figure 187: JBOD – Multiple drives act as single one

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 drive bays, then you should 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 three or four drive bays, it should 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 should 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.

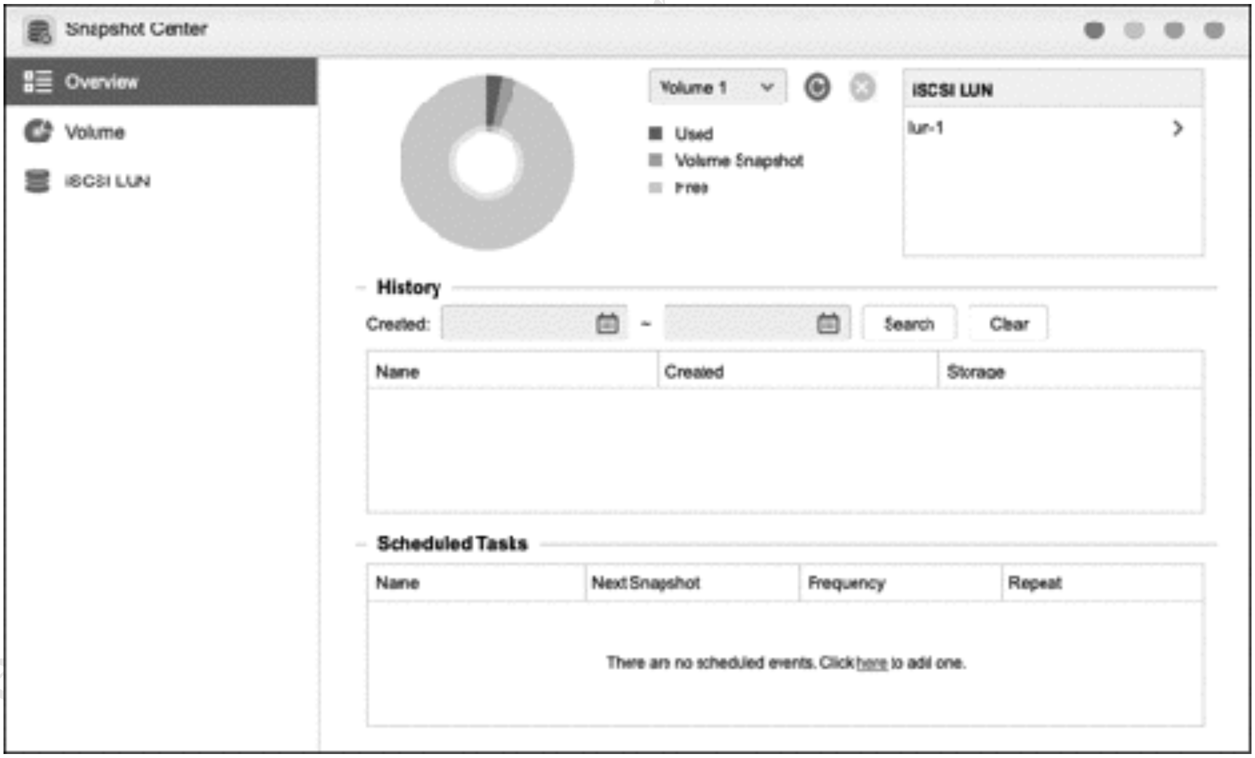
11.3 Snapshots

Snapshots are a 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, then writes away those details to a different part of the disk. 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 take place 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. However, although Snapshots are very efficient, the mechanism requires a certain level of hardware support. All x86-based ASUSTOR NAS boxes support it, as do recent ARM-based ones with 1GB RAM or more, but Snapshots may not be available on older models. Snapshots are only available if the Btrfs file system is being used; during the initial setup of ADM, regardless of the method used, there was an option to enable Btrfs or Snapshot support.

Enabling Snapshots will may reduce the overall speed of access to a disk or volume, although this may be considered a worthwhile trade-off between performance and protection. Snapshots can be stored on volumes and/or LUNs.

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

Snapshots are managed from the *Snapshot Center* app, which is installed during the installation of ADM on suitable models. Launching Snapshot Center from the Desktop will display the following screen (the iSCSI LUN entry in the top right-hand corner will only be present if LUNs have been defined).



Name	Created	Storage

Name	Next Snapshot	Frequency	Repeat

There are no scheduled events. Click here to add one.

Figure 188: Snapshot Center

There are three sections:

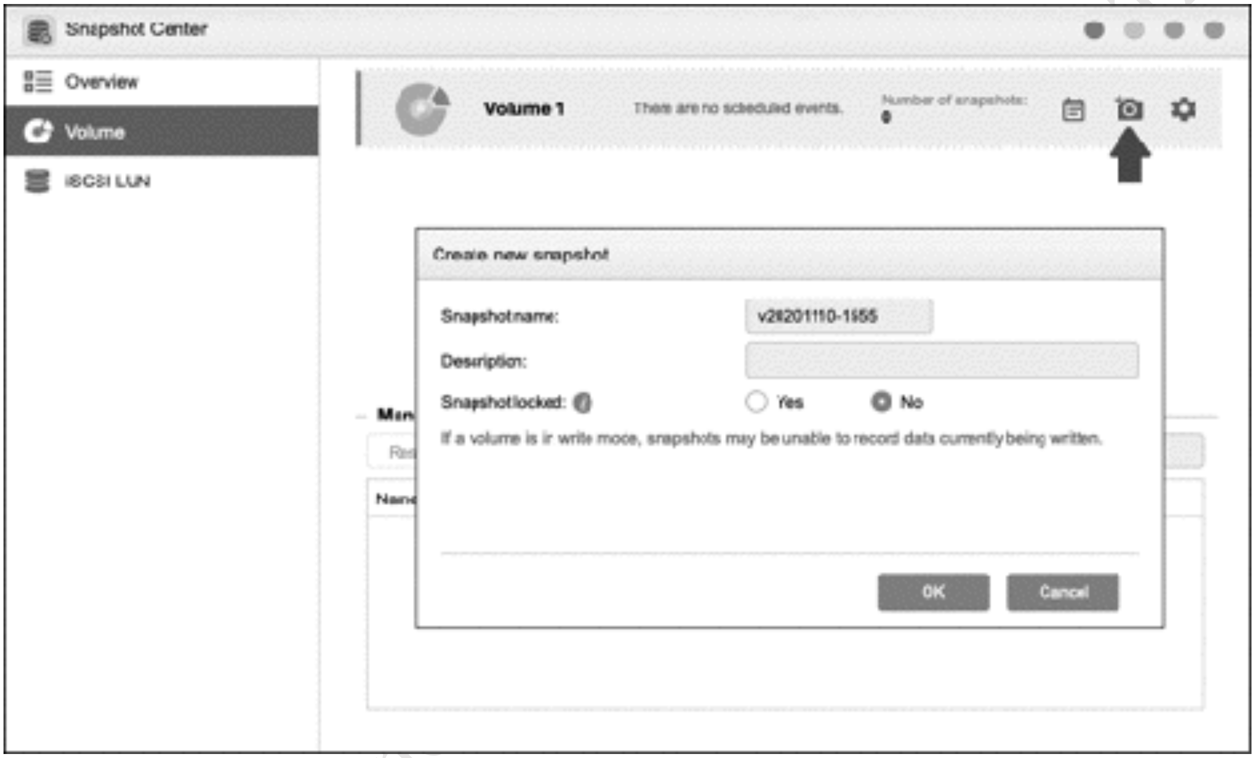
Overview – provides an ‘at a glance’ view of volume usage, history log file of snapshots and any scheduled tasks.

Volume – used for taking, scheduling and restoring snapshots, using conventional storage volumes.

iSCSI LUN – used for taking, scheduling and restoring snapshots, using iSCSI LUNs.

Manual Snapshots

To manually take a Snapshot, go to the **Volume** section and click the small camera icon in the top right-hand corner of the screen and a small panel will pop up. At the simplest level, the only thing necessary is to click the **OK** button; however, there are a number of options that can be exercised. By default, the *Snapshot Name* is derived from the current date and time and which is useful but can be changed if desired and given a more meaningful name e.g. '*month_end_snapshot*'. It can optionally be given a *Description*. If required, the snapshot can be locked, meaning it cannot be removed automatically but only manually. After clicking **OK**, the Snapshot is created, with the time taken depending on the amount of data that has changed. The completed snapshots are listed on both the Overview and Volume screens.



Create new snapshot

Snapshot name: v2#201110-1955

Description:

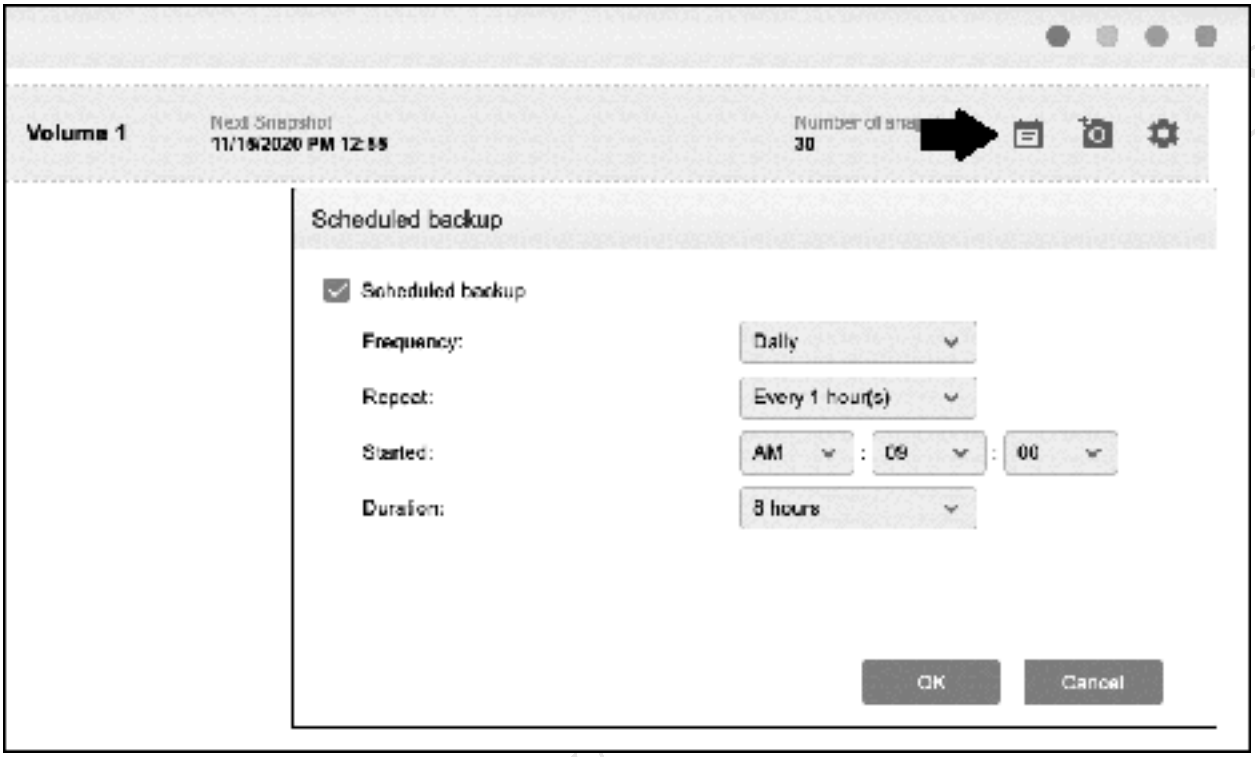
Snapshot locked: ○ Yes ● No

If a volume is in write mode, snapshots may be unable to record data currently being written.

Figure 189: Taking a manual Snapshot

Scheduled Snapshots

To setup scheduled Snapshots, go to the Volume page in *Snapshot Center* to and click the small scheduler icon in the top right-hand side of the screen to display the following panel:



Volume 1

Next Snapshot
11/16/2020 PM 12:55

Number of sna
30

Scheduled backup

☑ Scheduled backup

Frequency: Daily

Repeat: Every 1 hour(s)

Started: AM : 09 : 00

Duration: 8 hours

Figure 190: Schedule Snapshot Settings

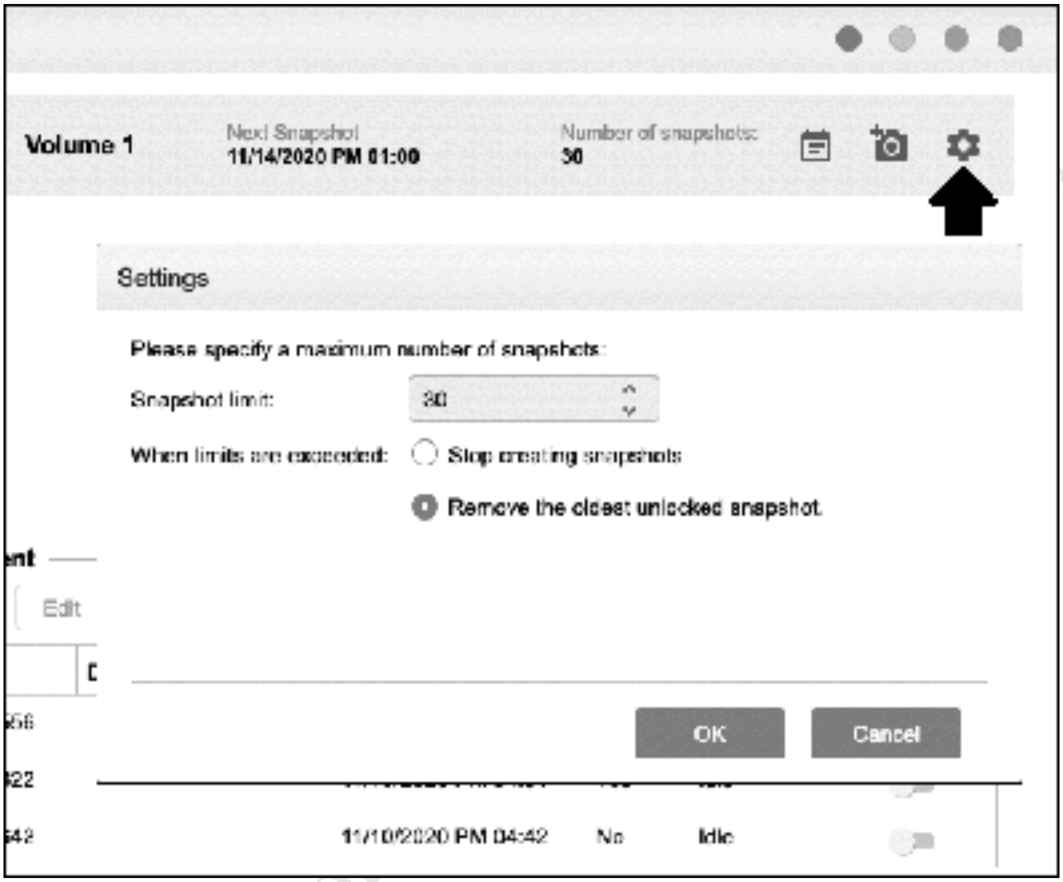
Tick the **Scheduled backup** box and select the *Frequency* from the dropdown: there is a choice of Once, Daily or Weekly. The *Repeat* dropdown defines how often the snapshot will be repeated; *Started* specifies when the snapshots commence and *Duration* defines how long they will continue. This may not seem intuitive but think of it as defining a sequence rather than a single event. With reference to the above example:

Snapshots will run daily. One will be taken every hour, with the first one at 09:00 AM / 09:00. These hourly snapshots will continue for a period of 8 hours i.e. the last one will be at 5:00 PM / 17:00 (8 hours after the start time). Or in other words, it is a schedule suitable for many offices and business premises.

Having defined the schedule, click **OK**.

Snapshot Retention

If every snapshot ever taken was retained, then eventually the system would run out of storage space for them and grind to a halt. A policy for the retention of snapshots therefore needs to be specified, which controls how many are kept. To define this, click the **Settings** icon on the **Volume** screen:



Volume 1

Next Snapshot
11/14/2020 PM 01:00

Number of snapshots:
30

Settings

Please specify a maximum number of snapshots:

Snapshot limit: 30

When limits are exceeded: ○ Stop creating snapshots

● Remove the oldest unlocked snapshot

11/10/2020 PM 04:42 No Idle

Figure 191: Snapshot Retention Settings

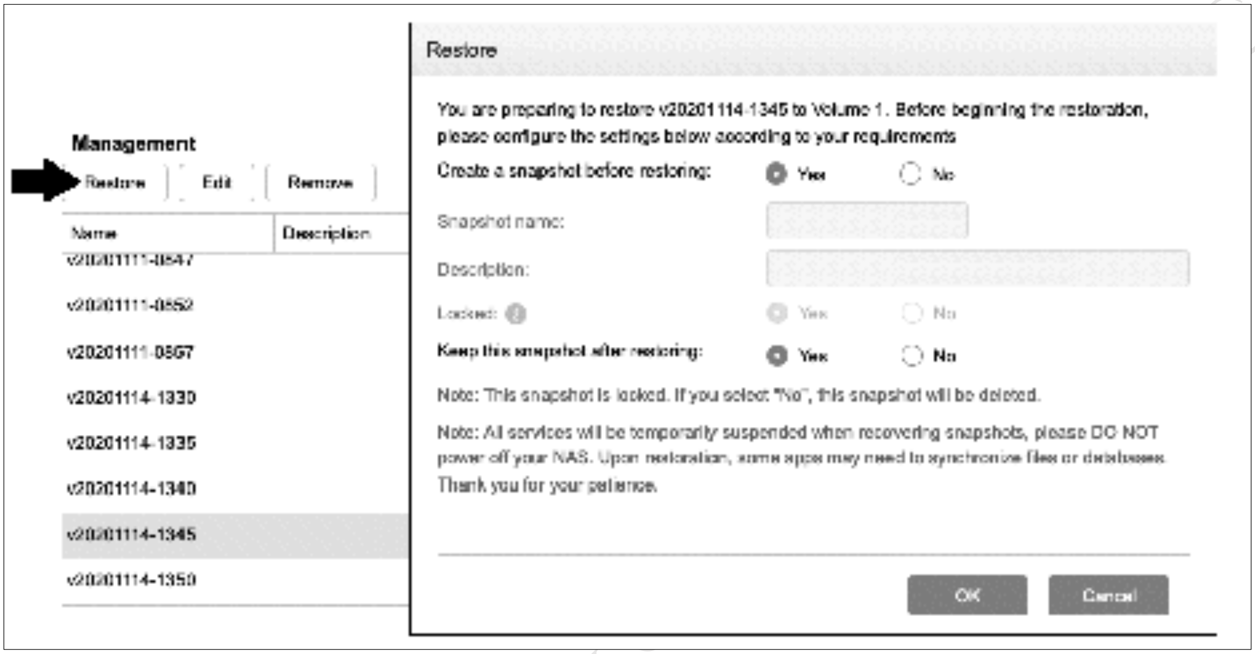
The number of snapshots to be retained is controlled by the *Snapshot limit* field and the decision here depends on how far back in time you might want to revert to. For instance, if you specified a limit of 30 and were taking one snapshot an hour, you would be able to roll back just over one day, whereas with one a week you could roll back about seven months. Make a decision about what to do when the limit is reached: the choice is to stop creating further snapshots or to remove the oldest unlocked snapshot so processing can continue (the latter is generally more useful).

Having made a choice, click **OK**.

Restoring a Snapshot and Managing Snapshots

Should there ever be a need to recover data, this is done as follows:

Go into the **Volume** screen in **Snapshot Center**. The available snapshots are listed in the bottom half of the screen in the *Management* section. Highlight the one to be restored and click the **Restore** button, which will have become enabled.



Management

Name	Description
v20201111-0847	
v20201111-0852	
v20201111-0857	
v20201114-1330	
v20201114-1335	
v20201114-1340	
v20201114-1345	
v20201114-1350	

Restore

You are preparing to restore v20201114-1345 to Volume 1. Before beginning the restoration, please configure the settings below according to your requirements

Create a snapshot before restoring: ● Yes ○ No

Snapshot name:

Description:

Locked: ● Yes ○ No

Keep this snapshot after restoring: ● Yes ○ No

Note: This snapshot is locked. If you select "No", this snapshot will be deleted.

Note: All services will be temporarily suspended when recovering snapshots, please DO NOT power off your NAS. Upon restoration, some apps may need to synchronize files or databases. Thank you for your patience.

Figure 192: Restoring a Snapshot

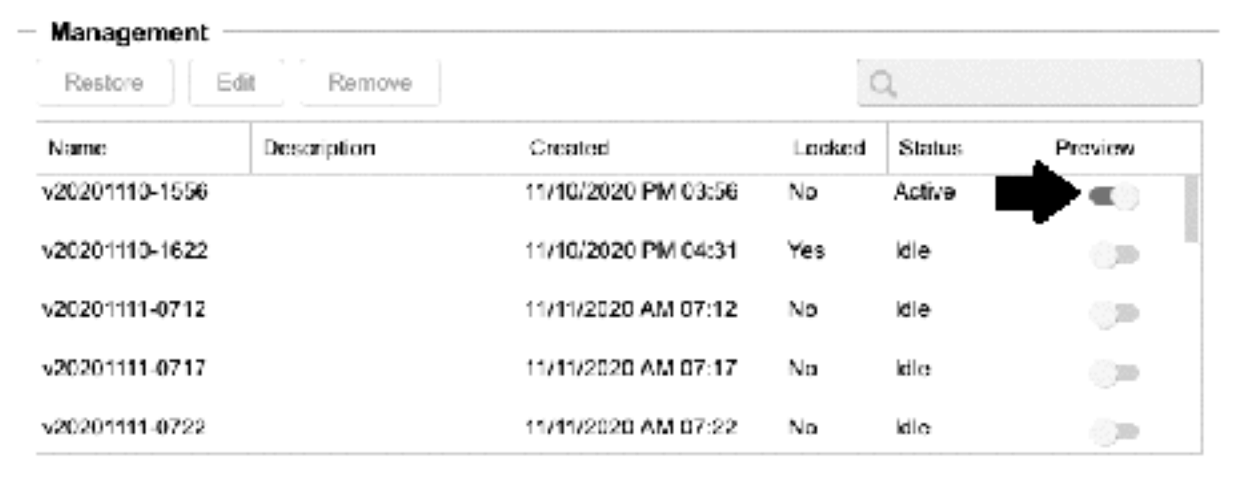
On the panel that appears, you can specify that a new snapshot is created before the restoration takes place; this is useful as you can use it to 'undo' the restored data should it prove unsuitable. You can also choose whether or not to keep this new snapshot after the restoration. Click **OK** to begin restoring and acknowledge any reminder message.

The time taken depends upon the amount of data. As the process can be disruptive, unless it is a matter of urgency it is best done during a quiet time or out of hours.

Individual snapshots can be managed using the same screen. To change the name of a snapshot or change its status between locked or unlocked, highlight it and click **Edit**. To delete one, highlight it and click **Remove**.

Working with Snapshots in File Explorer

The contents of snapshots can be accessed directly from File Explorer, where they appear as part of the regular file system. By default, snapshots are ‘invisible’ to File Explorer; to make them visible, go to the Management section on the **Volume** page within **Snapshot Center**. Against each individual is a *Preview* switch; moving it to the ‘On’ position will cause File Explorer to launch and display it (thereafter it will remain visible unless switched off again).



Name	Description	Created	Locked	Status	Preview
v20201110-1556		11/10/2020 PM 03:56	No	Active	●
v20201110-1622		11/10/2020 PM 04:31	Yes	Idle	○
v20201111-0712		11/11/2020 AM 07:12	No	Idle	○
v20201111-0717		11/11/2020 AM 07:17	No	Idle	○
v20201111-0722		11/11/2020 AM 07:22	No	Idle	○

Figure 193: Making a snapshot visible in File Explorer

From within File Explorer, the contents of a snapshot can be viewed and the files and folders manipulated. For instance, a file can be restored by dragging it from the snapshot to a regular folder in the main file system.

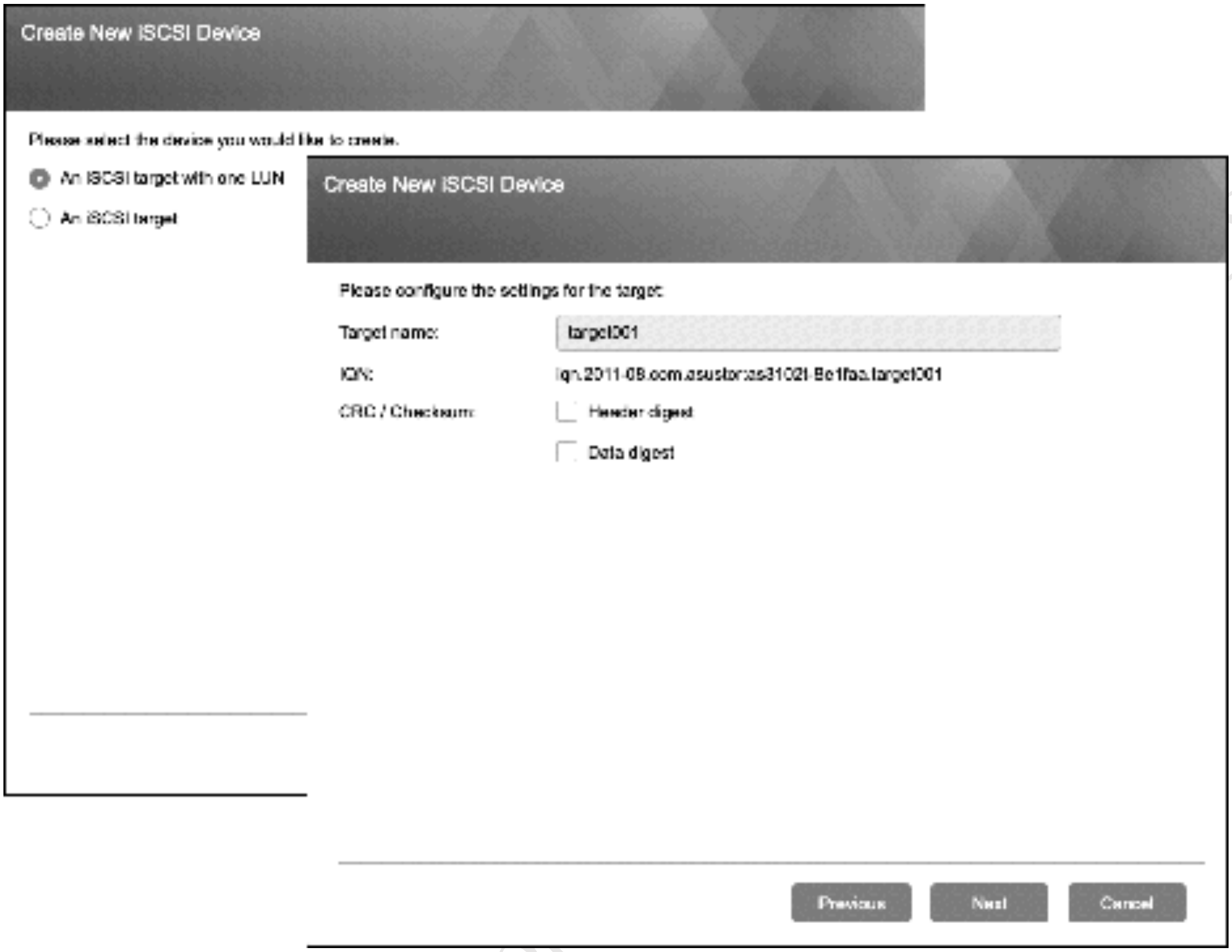
11.4 iSCSI

iSCSI - *Internet Small Computer Systems Interface* – is a standard for connecting storage to computers over networks. Its origins lie with larger computer systems and it is of particular benefit to organizations that run many servers, have vast amounts of storage and require great flexibility when it comes to managing that storage. However, the exact same technology is available within ADM and may be of interest to small businesses and 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 5.5 Mapping Drives Manually. This enables us to refer to, say, \\server\home as drive H, but it is not a real (physical) drive in the sense that the C: drive on a Windows computer is and we are simply using the letter H as a form of shorthand. 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. An attractive feature about iSCSI is that it uses an efficient protocol, resulting in high data transfer speeds.

Creating an iSCSI LUN

Launch Storage Manager and click on the **iSCSI** entry on the left-hand side of the screen. Click **Create**, choose the **An iSCSI target with one LUN** option and click **Next**. The defaults on the next screen can be accepted, although you could overtype the *Target name* if you wished. Click **Next**.



Create New iSCSI Device

Please select the device you would like to create.

● An iSCSI target with one LUN

○ An iSCSI target

Create New iSCSI Device

Please configure the settings for the target.

Target name: target001

IQN: iqn.2011-08.com.asustor:as3102t-8e1faa.target001

CRC / Checksum: □ Header digest

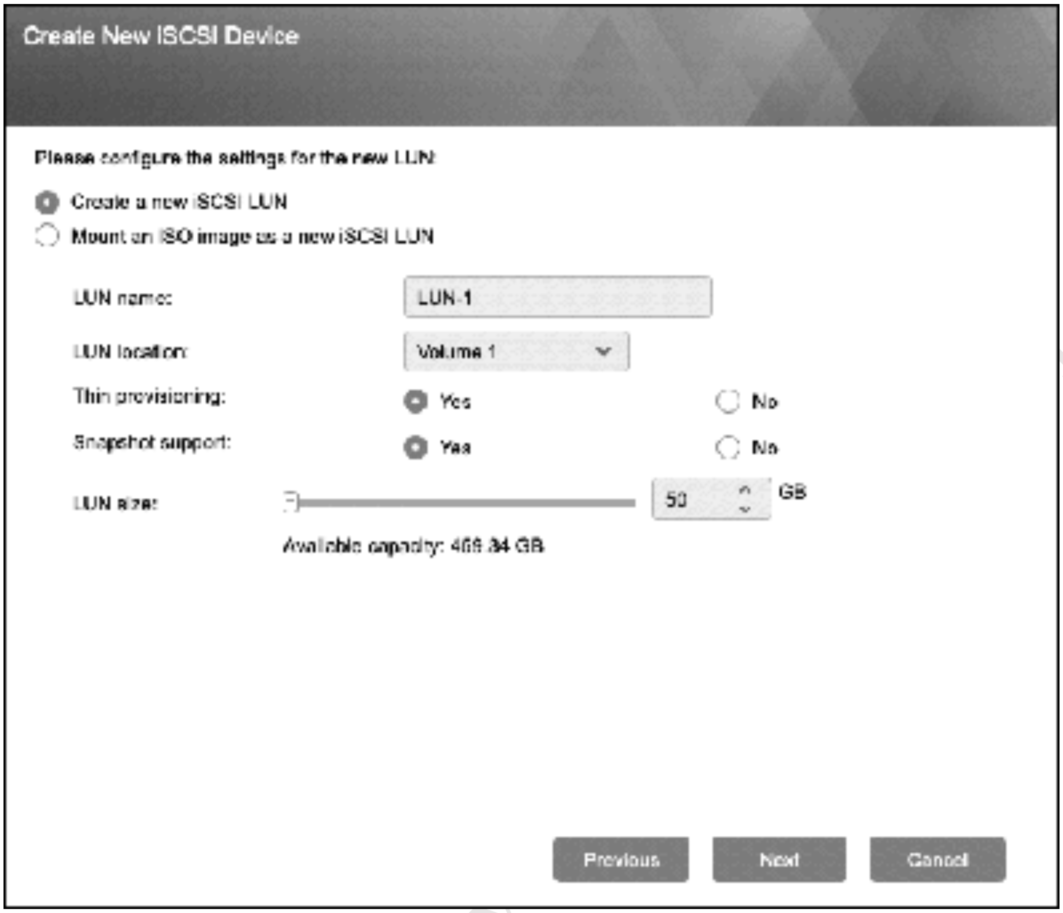
□ Data digest

Figure 194: Create new iSCSI Device

On the subsequent screen, *CHAP certification* can optionally be specified. 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. Make a decision and click **Next**.

A decision needs to be made about *provisioning*. LUNs are available in two options, *Thin* and *Thick* (the latter is not explicitly named on the panel but it is what you get if thin is not chosen).

With Thin Provisioning, storage space is allocated dynamically and only as required. Suppose you specify 50GB 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 50GB would immediately be taken from the available drive space. Overall, Thin Provisioning is more flexible and economical with space, whilst Thick offers better performance. In this example, we will choose Thin. If you wish to use Snapshots with LUNs, choose **Yes** for Snapshot support. Specify the size of the LUN in Gbytes and click **Next**. A summary panel is displayed – click **Finish** to create the LUN, which will then be listed in the iSCSI and iSCSI LUN sections of Storage Manager.



Create New iSCSI Device

Please configure the settings for the new LUN:

● Create a new iSCSI LUN

○ Mount an ISO image as a new iSCSI LUN

LUN name: LUN-1

LUN location: Volume 1

Thin provisioning: ● Yes ○ No

Snapshot support: ● Yes ○ No

LUN size: 50 GB

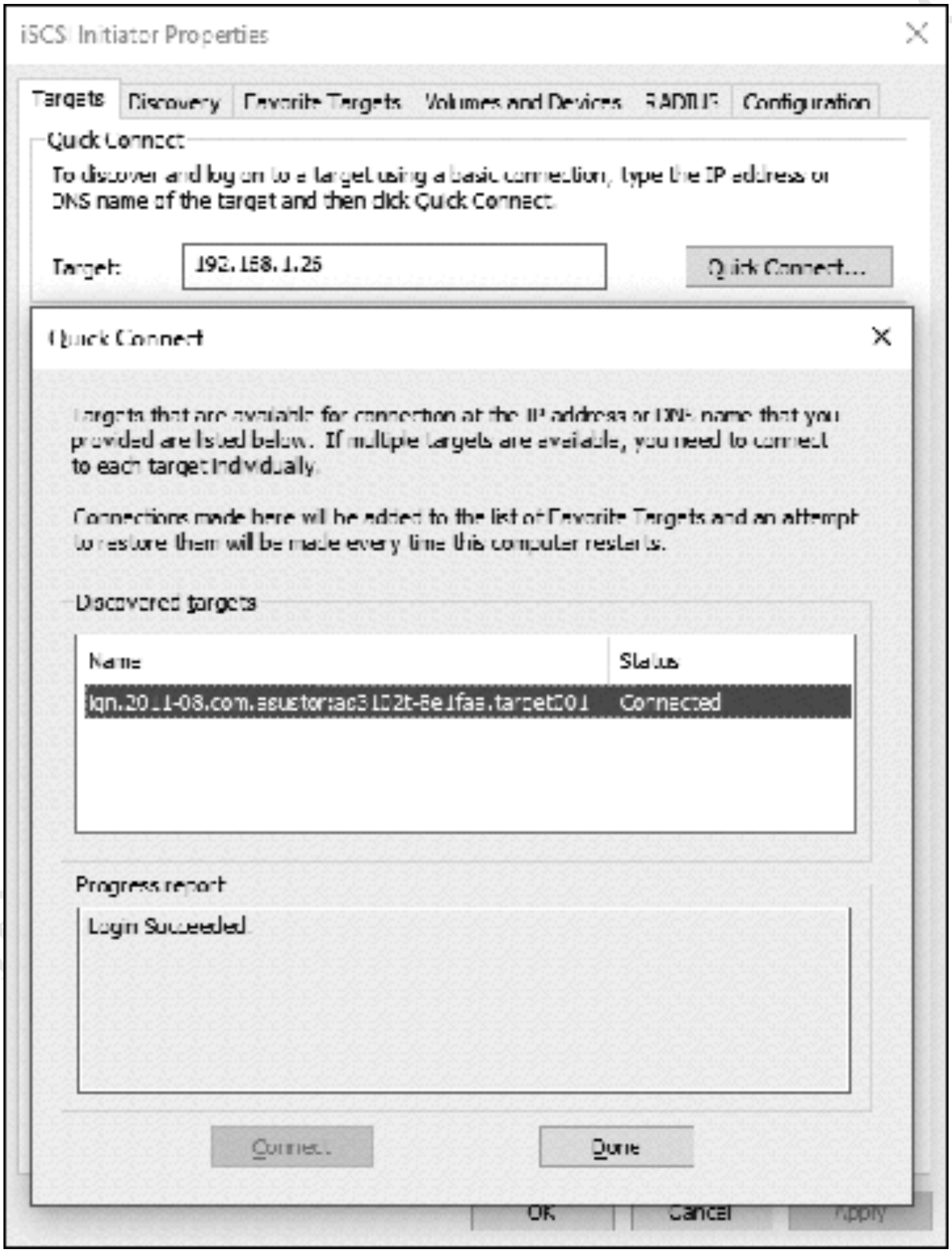
Available capacity: 468.84 GB

Figure 195: Provisioning and capacity

Connecting a Client

Having set up the iSCSI LUN(s) on the server, the client computer(s) can now be connected. This section describes how to do so with a modern version 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 **Quick Connect**. The target should be found and a status of *Connected* shown:



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target: 192.168.1.25

Targets that are available for connection at the IP address or DNS name that you provided are listed below. If multiple targets are available, you need to connect to each target individually.

Connections made here will be added to the list of Favorite Targets and an attempt to restore them will be made every time this computer restarts.

Discovered targets

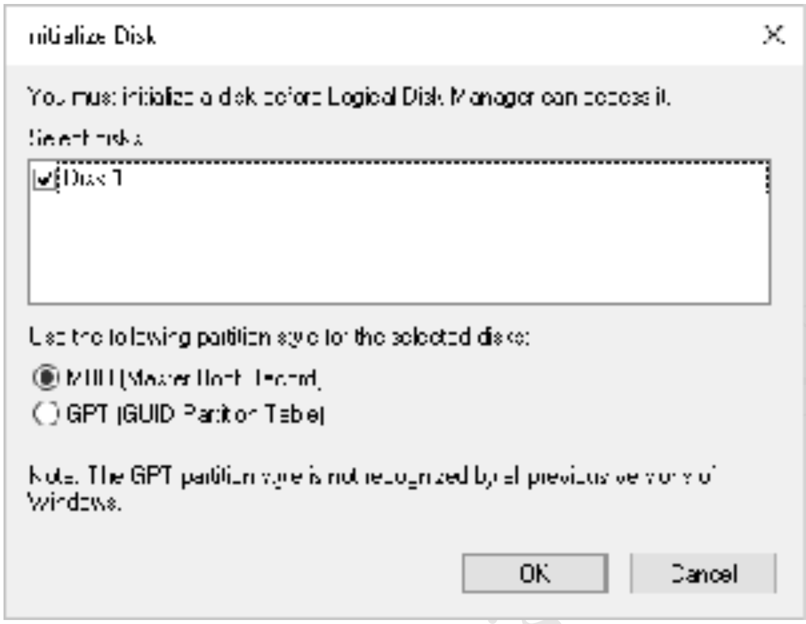
Name	Status
iqn.2011-08.com.asustor:as3102t-8e1fa8.target001	Connected

Progress report

Login Succeeded.

Figure 196: Connecting to the Target

Click **Done** and **OK**. Go back to **Administrative Tools** and choose **Computer Management**; 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**.



Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 1

Use the following partition style for the selected disks:

● MBR (Master Boot Record)

○ GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows.

Figure 197: 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.

11.5 SSD Caching

Solid State Drives or SSDs are very fast in operation, much more so than traditional mechanical hard drives. However, they are also 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 $400 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 them quickly available when required, as opposed to being accessed from the much slower mechanical drives. This process happens automatically and transparently, with ADM 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. Although any reasonable amount of SSD should be beneficial, you should consider a ratio of 10:1 e.g. if you have 10TB of mechanical storage you should aim to supplement it with 1TB of SSD as cache.

Two types of SSD are supported. Some NAS models feature PCIe slots and can use M.2 SSD cards; these give the best results in terms of speed. However, many recent models can also use regular 2.5” SATA-format SSD drives, such as are used in laptops and, whilst these are slower, still give a considerable boost to storage performance.

Setting Up Caching

To setup caching, go into **Storage Manager** and check that the SSD drive has been identified within the **Overview** or **Drive** sections. On the **Volume** tab, highlight the volume to be cached if there is more than one and click **Management** > **SD Caching**:

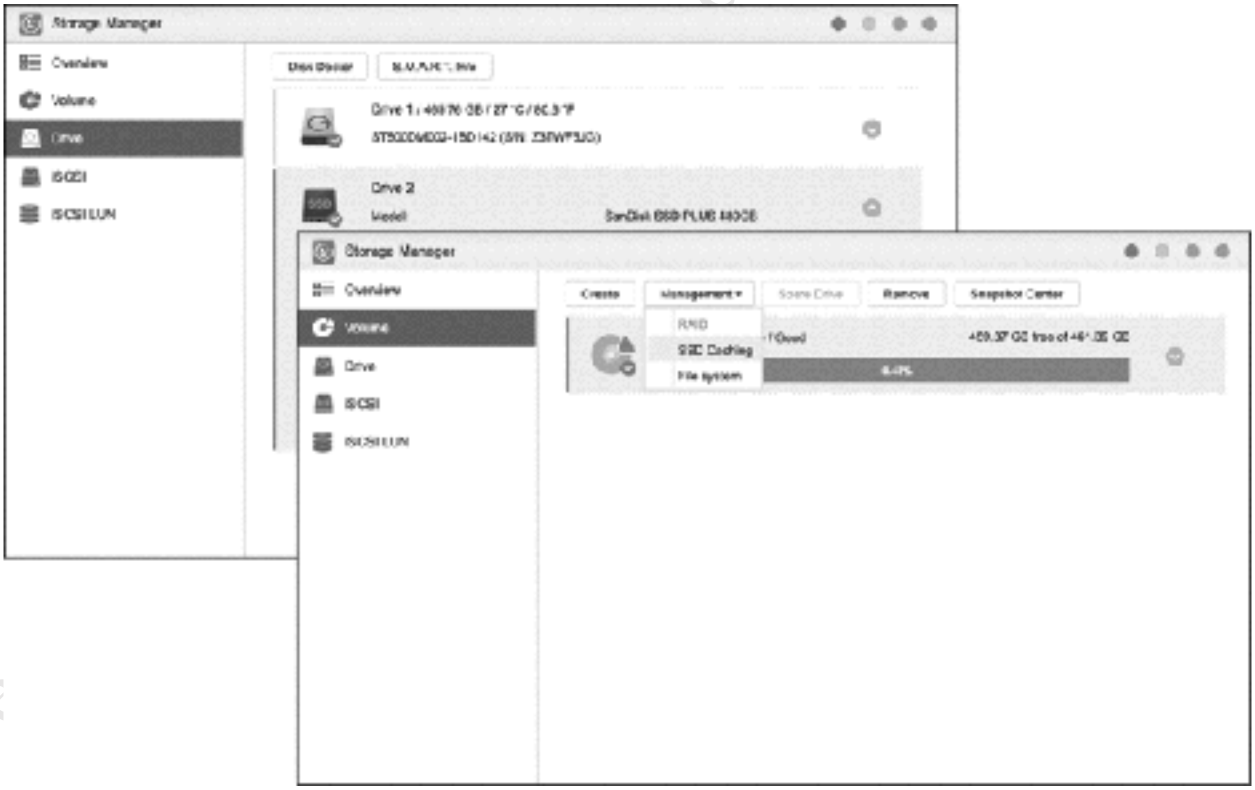
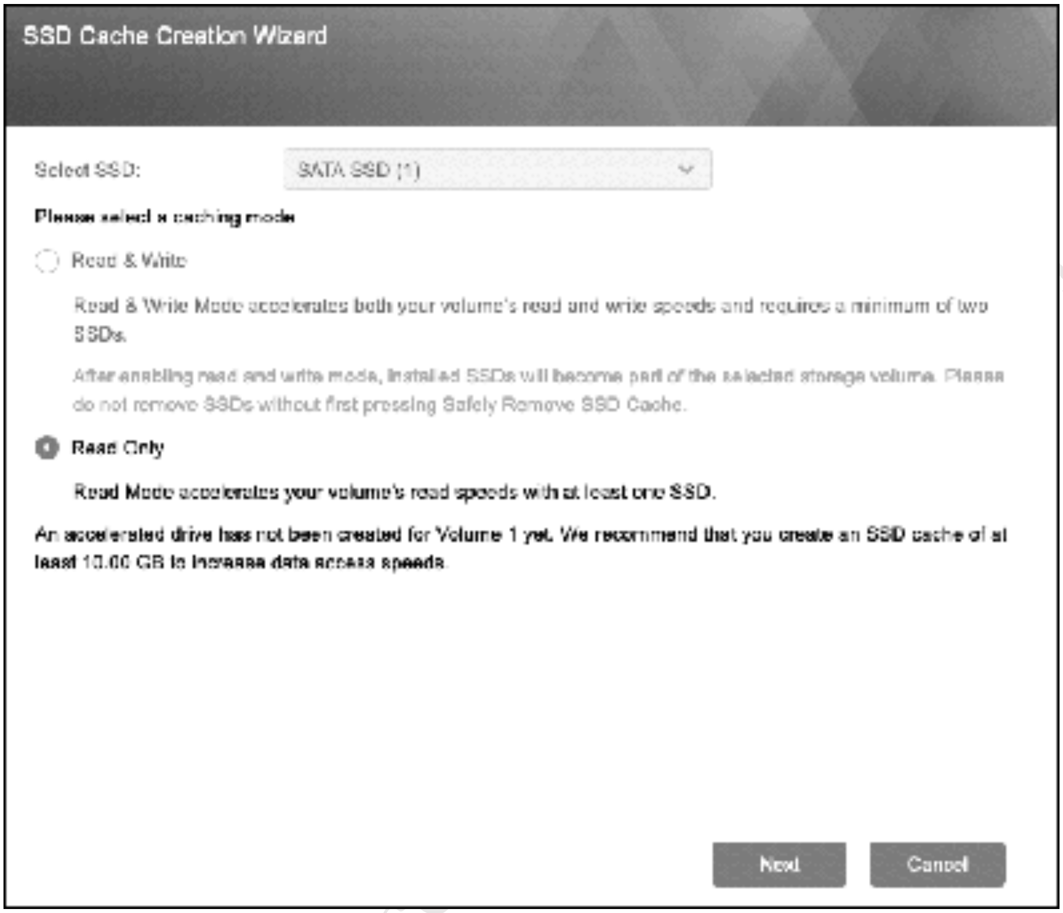


Figure 198: SSD option in Storage Manager

This will cause the *SSD Cache Creation Wizard* to run. The first decision is to select a caching mode; if there is a single SSD drive then the only choice is *Read Only*. If there are multiple SSDs then *Read &*

Write mode is also available and which gives even better performance. Also, the *Select SSD* dropdown becomes available if there is more than one drive to choose from. Click **Next**.



SSD Cache Creation Wizard

Select SSD: SATA SSD (1)

Please select a caching mode

○ Read & Write

Read & Write Mode accelerates both your volume's read and write speeds and requires a minimum of two SSDs.

After enabling read and write mode, installed SSDs will become part of the selected storage volume. Please do not remove SSDs without first pressing Safely Remove SSD Cache.

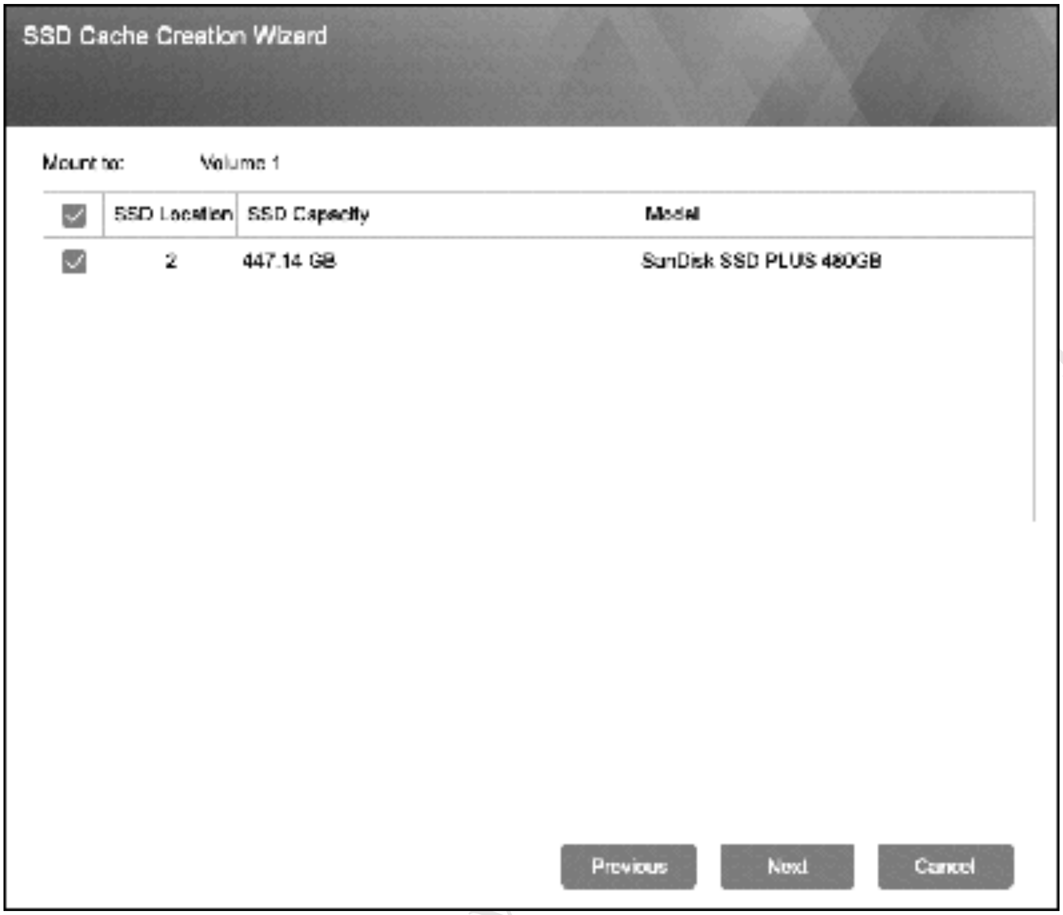
● Read Only

Read Mode accelerates your volume's read speeds with at least one SSD.

An accelerated drive has not been created for Volume 1 yet. We recommend that you create an SSD cache of at least 10.00 GB to increase data access speeds.

Figure 199: Select caching mode

On the subsequent screen, select the SSD drive(s) to be used and click **Next**:



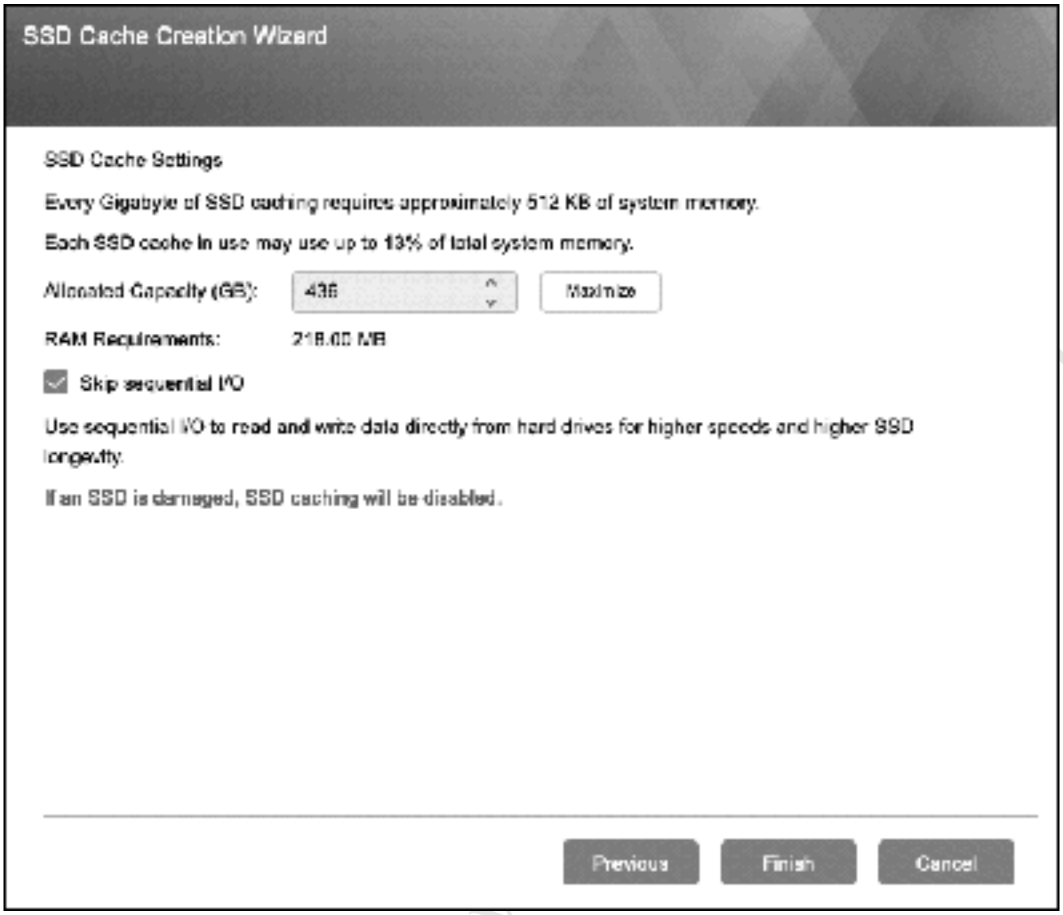
SSD Cache Creation Wizard

Mount to: Volume 1

☑	SSD Location	SSD Capacity	Model
☑	2	447.14 GB	SanDisk SSD PLUS 480GB

Figure 200: Select the SSD disk(s)

On the screen after that, specify the size of the cache. One possible consideration is that a portion of the server's RAM is used to support caching operations. In this example, we have a 436 GB cache and this will use up 218 MB RAM, which is not excessive. However, in a large setup with several GBytes of cache this could become a factor. Having made a decision - and for simplicity you may wish to choose the *Maximize* option - click **Finish**:



SSD Cache Settings

Every Gigabyte of SSD caching requires approximately 512 KB of system memory.

Each SSD cache in use may use up to 13% of total system memory.

Allocated Capacity (GB): 436

RAM Requirements: 218.00 MB

☑ Skip sequential I/O

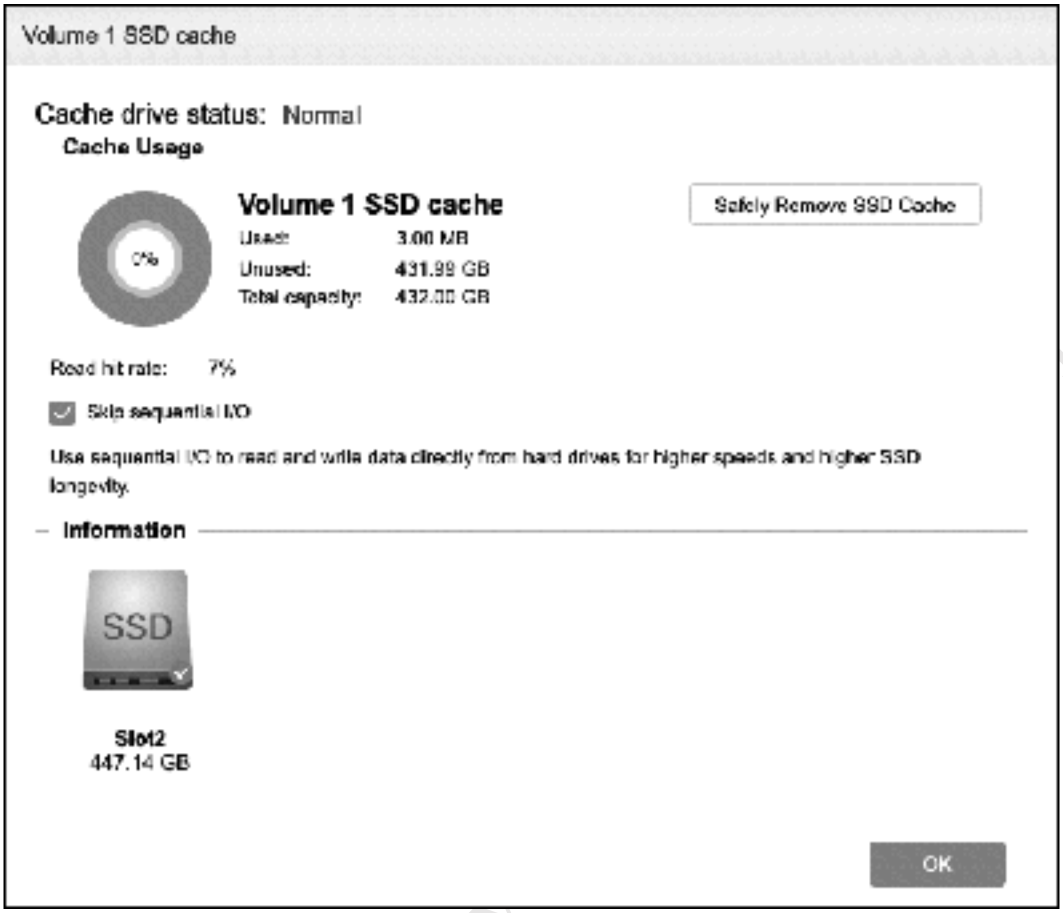
Use sequential I/O to read and write data directly from hard drives for higher speeds and higher SSD longevity.

If an SSD is damaged, SSD caching will be disabled.

Figure 201: SSD Cache Settings

There is a warning message – click **OK** to proceed and the SSD cache drive will be mounted, which may take a short while. When complete, indicated by the process reaching 100%, click **OK**.

To monitor the performance of the caching, click **Management** > **SD Caching** on the **Volume** tab, highlight the volume being cached if there is more than one, and the following panel is shown. Should there ever be a need to remove the cache, it has to done from here.


Volume 1 SSD cache

Cache drive status: Normal

Cache Usage

Volume 1 SSD cache

Used: 3.00 MB

Unused: 431.99 GB

Total capacity: 432.00 GB

Read hit rate: 7%

☑ Skip sequential I/O

Use sequential I/O to read and write data directly from hard drives for higher speeds and higher SSD longevity.

Information

Slot2
447.14 GB

Figure 202: Details of SSD Cache

12
MISCELLANEOUS & ADVANCED TOPICS

12.1 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.

12.2 App Central

Whilst the ADM operating system has a huge amount of useful functionality built-in, one of the great attractions is that it is possible to extend it further through the installation of optional packages or apps, the vast majority of which are free. Some of these have already been discussed during the course of this book, but many others are available. Some have been developed by ASUSTOR, whilst others have been supplied by third parties. Some are business focused, others are aimed more at home users and some are suitable for both.

To review what is available, click on the **App Central** icon located on the ADM Desktop. The first time it is accessed, Terms of Use and Privacy Statement messages have to be agreed. This is followed by a panel offering a choice of categories, such as home/personal applications and business applications. However, if you click **Skip** the full list of apps is accessible:

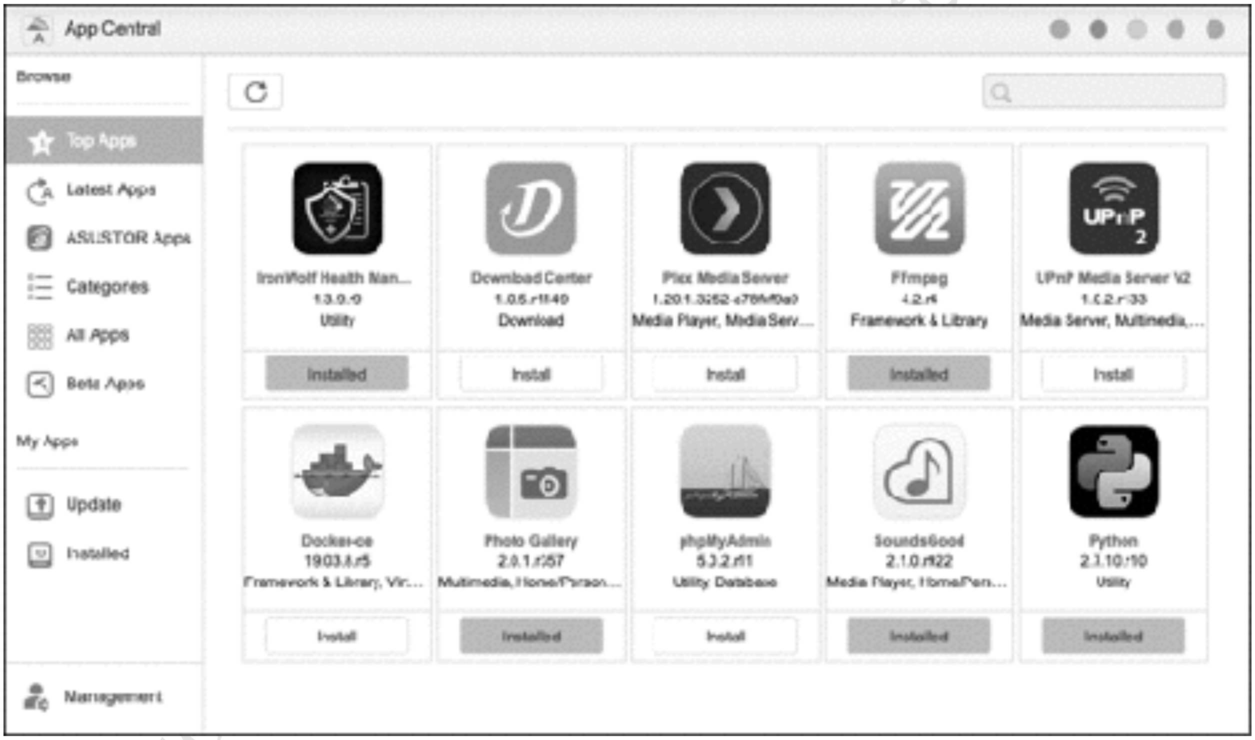


Figure 203: App Central

At the time of writing, around 300 apps are available, broken down into categories such as Backup/Sync, Business, Multimedia, Utilities and so on. Not all apps are available for or suitable for all NAS models, although the majority are and those which are unsuitable for your NAS will not be listed. On the left-hand side of the screen, constituting a type of menu, the apps are additionally organized into top apps, the latest apps and those developed by ASUSTOR. There is also a search facility for locating specific apps by name.

Having located an app, click on its **Install** button. Many apps will initially display a panel called *About This App*, which lists dependencies about the app, but this is for information only and does not require any actions. Once an app is installed, its button will read *Installed*. Alternatively, click on **Installed** in the left-hand panel to obtain a list of all installed apps.

New versions of apps are made available from time to time. Apps requiring updates can be seen by clicking **Update** in the left-hand panel.

Managing Apps

App Central is not just for downloading apps, it is also used for managing them. Once an app has been installed, options appear beneath it in the *Installed* section of App Central, enabling it to be controlled. Apps can be uninstalled and infrequently used ones can be temporarily disabled without the necessity of having to uninstall them.

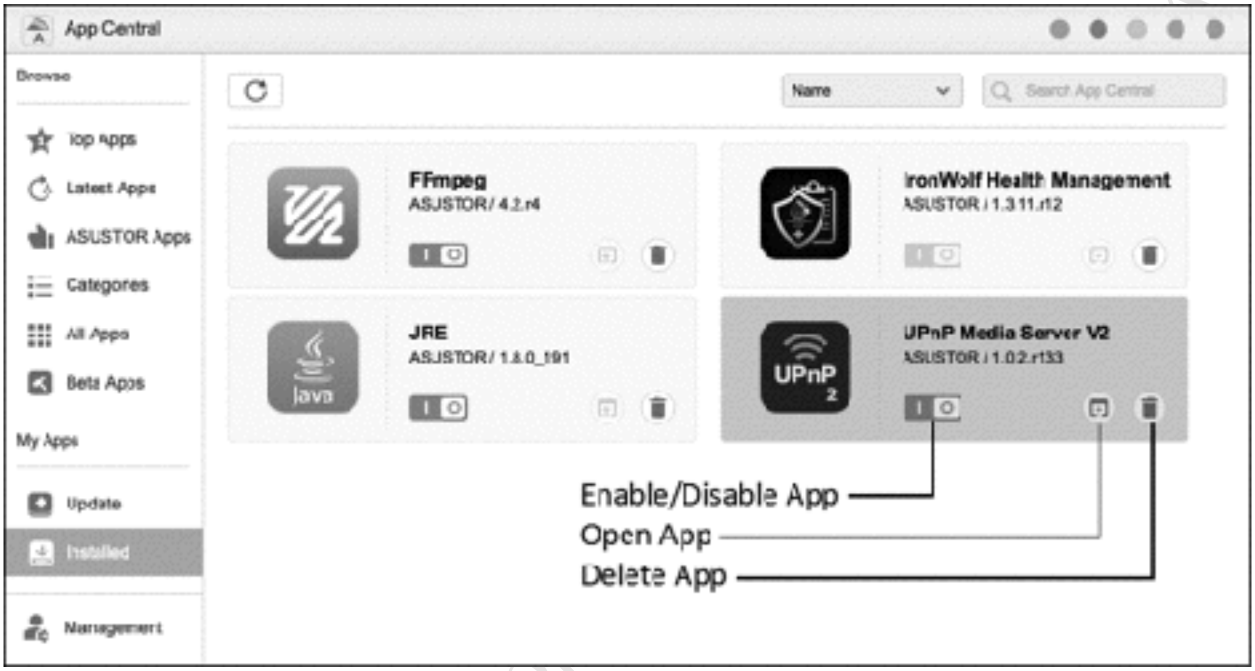
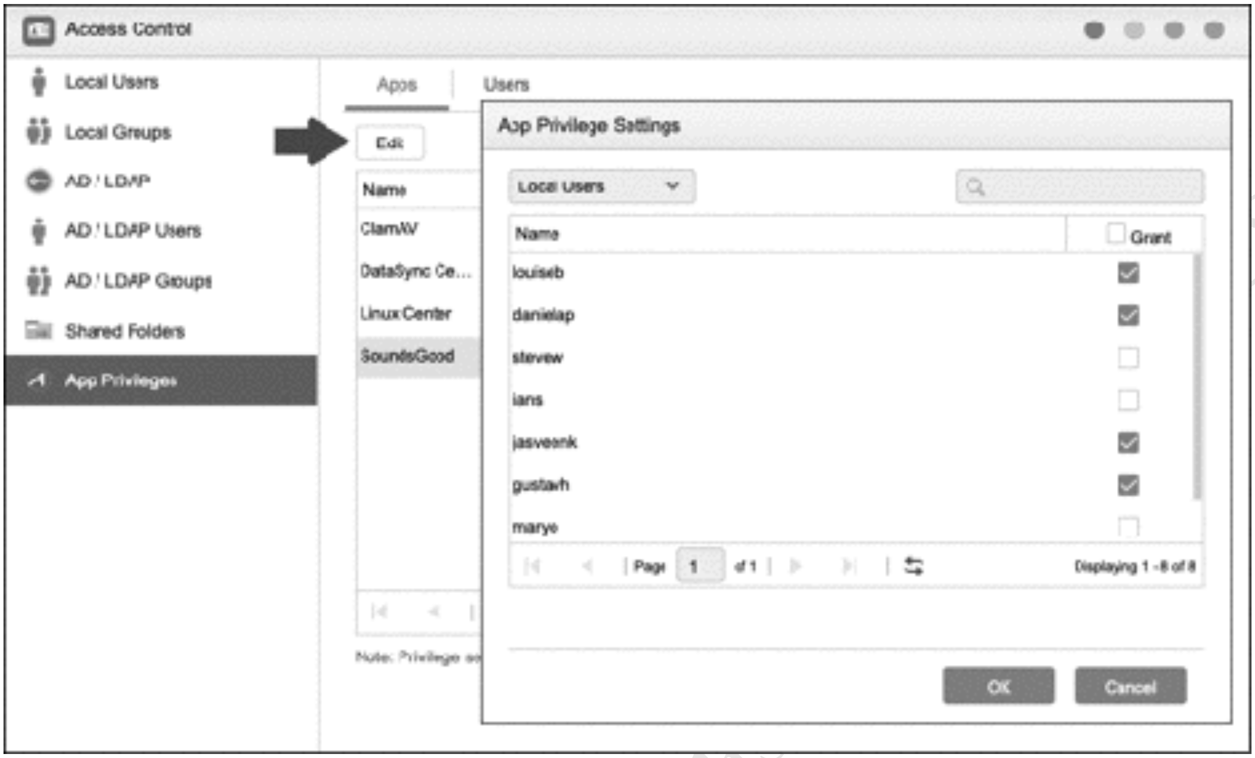


Figure 204: Managing an App

Making Apps Available to Users

When apps are installed, they are only usually available by default to the admin user and have to be specifically made available to any other users, if required. To do this, go into **Preferences** > **App Privileges**, highlight the app on the **Apps** panel and click the **Edit** button. Place ticks against the users who should have access then click **OK**. To make it available to all users, tick the box at the top of the screen (labelled 'Grant').



Name	□ Grant
louiseb	☑
danielap	☑
stevew	□
ians	□
jasveenk	☑
gustavh	☑
marye	□

Figure 205: Making an App available to users

Installing an App Manually

Whilst apps are normally downloaded and installed from the large selection available in App Central, there may be occasions when you need to do so manually, bypassing the standard mechanism. For instance: ASUSTOR have released an early or test version of the app and it is not yet in App Central, even in the Beta Apps section; you are a software developer, producing your own apps; a third-party has an app but which is not available through App Central (although you need to be careful in these circumstances as unauthorized apps may harm your data or system or leave it open to attack).

To install an app manually: download the app onto your computer; within App Central, click **Management** > **Manual Install**; browse to the download, select it and click the **Upload** button.

Installing Apps Using AiMaster

Apps can be installed from AiMaster, which has an icon for App Central. At the bottom of the screen are five mini-icons: *Favorites* (meaning those apps which have already been installed); *Category view*; *View all apps*; *Search*; *Beta apps*.

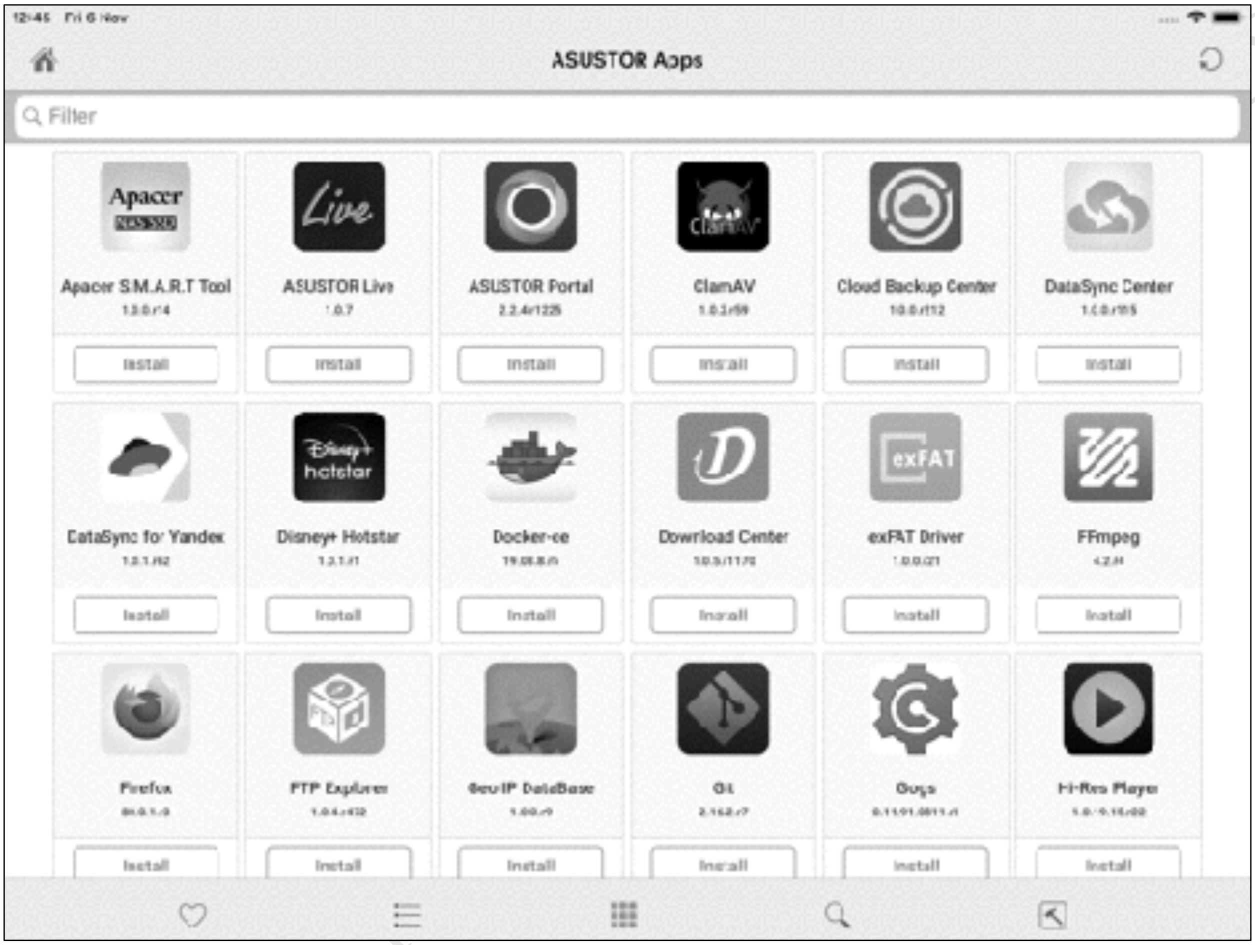
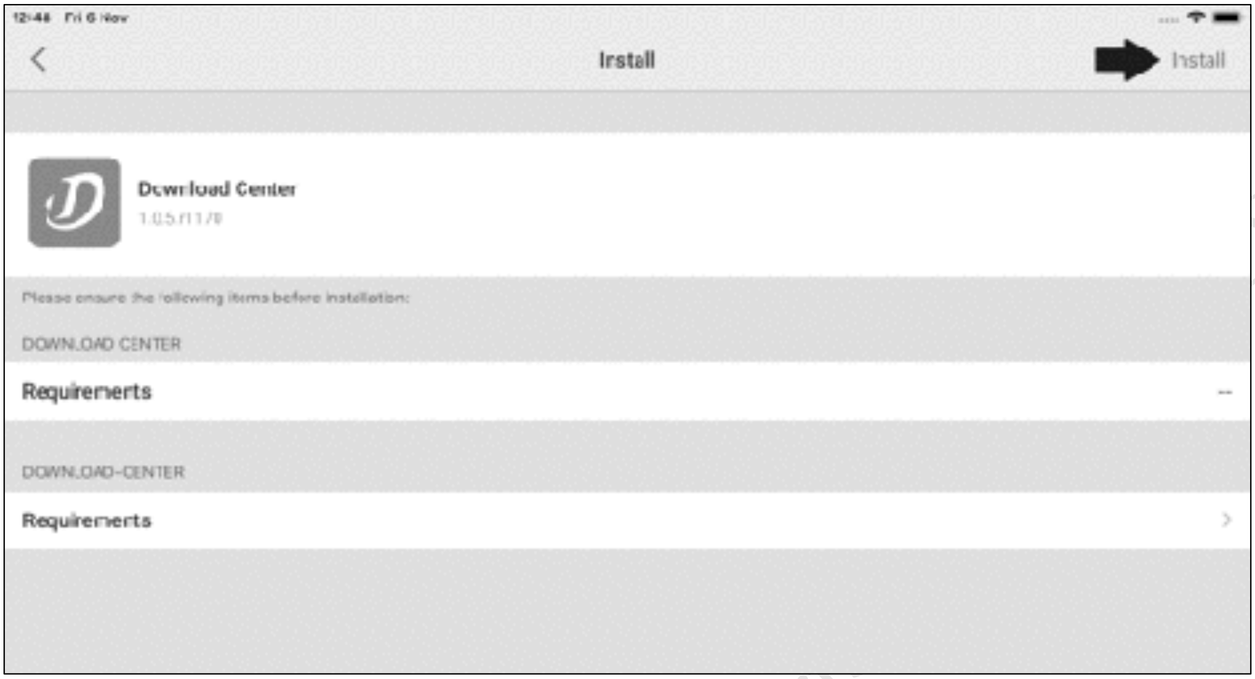


Figure 206: App Central viewed from AiMaster

To install an app, tap its **Install** button. A screen is displayed, showing any requirements/dependencies. To proceed, tap **Install** in the top right-hand corner of the screen.



Please ensure the following items before installation:

Figure 207: Installing an App from AiMaster

Installed apps can be managed from the Favorites screen, where they can be enabled/disabled, updated and deleted.

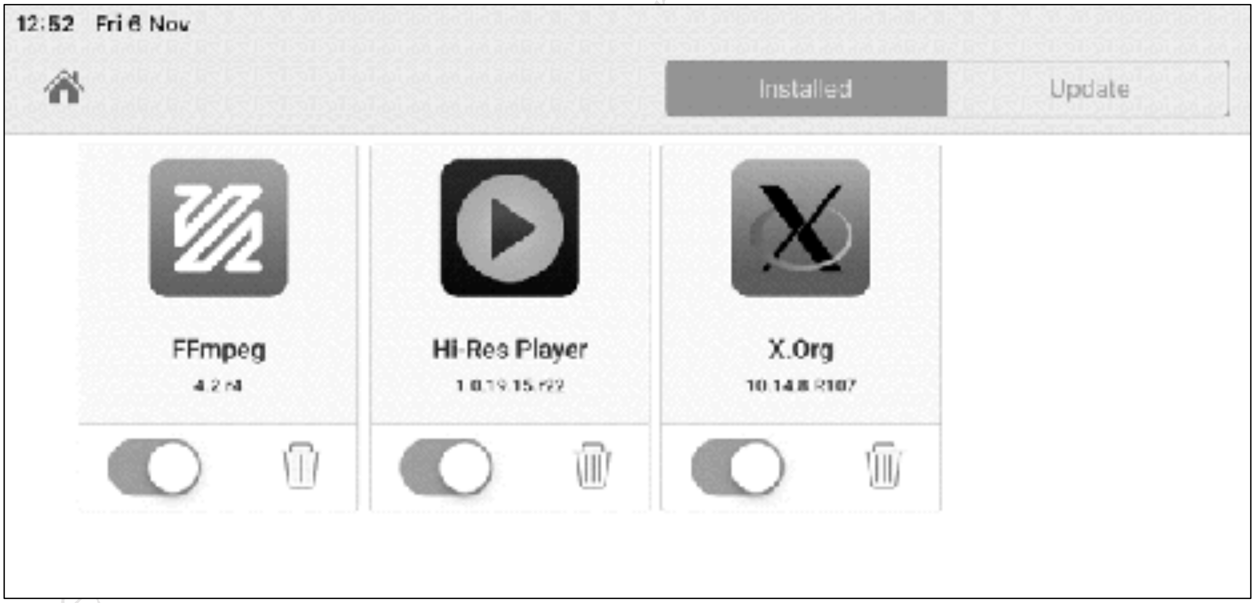


Figure 208: Managing an App from AiMaster

12.3 ASUSTOR Portal

Some ASUSTOR models feature HDMI output, enabling them to be connected directly to a HDMI-equipped television or screen. The NAS can then be used as though it was a regular PC in conjunction with a keyboard and mouse, for instance for browsing the internet or running a selection of applications. This is managed through the ASUSTOR Portal application, which needs to be downloaded from App Central. When installing it, other components will be automatically downloaded and some configuration changes will be made.

Once installed, connect the NAS to a suitable screen using a HDMI cable and connect a USB keyboard and mouse. The display will be along the following lines:

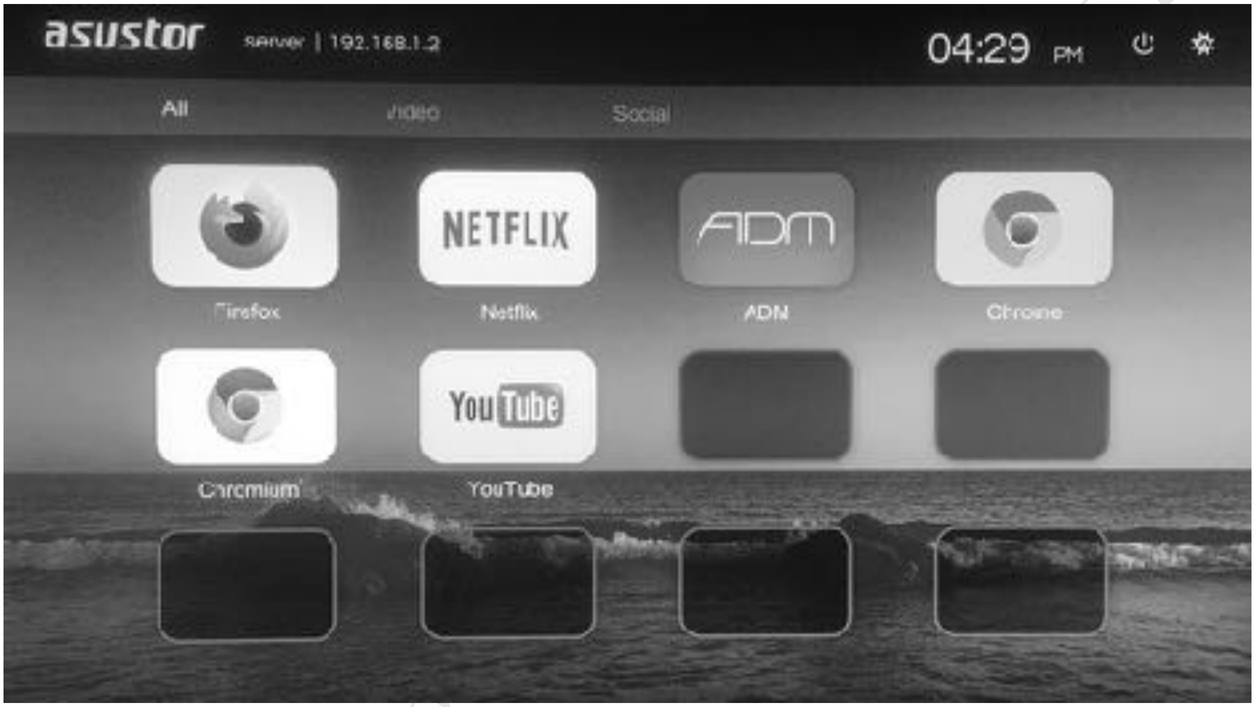
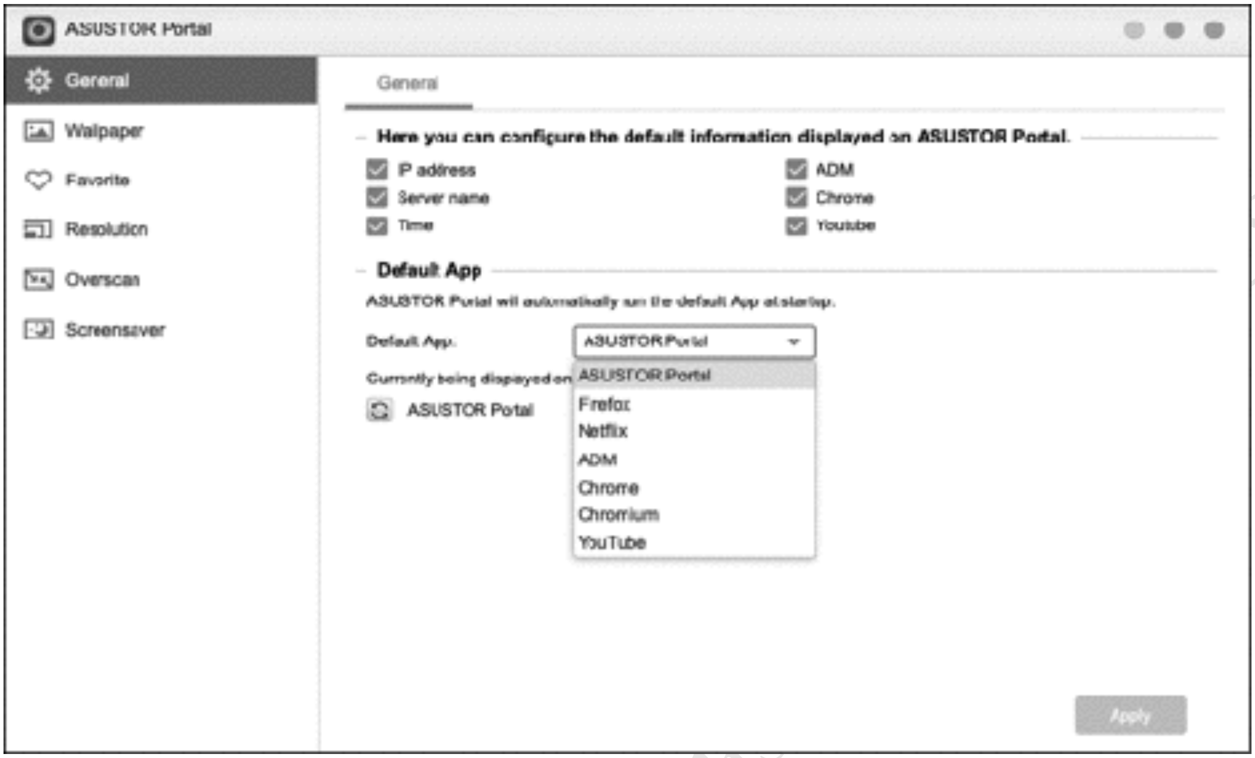


Figure 209: ASUSTOR Portal viewed on TV screen

The Portal is pre-populated with some popular items, including the Firefox and Chrome browsers and a link to YouTube. There is also an icon for Netflix, however, this is a link to the Netflix website rather than a dedicated app, which is actually the mechanism by which the 'apps' on the Portal are implemented. Clicking the ADM icon will present you with the standard login screen, where you can use ADM in the normal manner.

The Portal can be customized by clicking the **Settings** wheel in the top right-hand corner of the screen, or from within 'regular' ADM. The options are largely identical with both routes, but we will use the latter. Clicking on the ASUSTOR Portal on the Desktop will display the following screen:



ASUSTOR Portal

Here you can configure the default information displayed on ASUSTOR Portal.

☑ IP address ☑ ADM
☑ Server name ☑ Chrome
☑ Time ☑ Youtube

Default App

ASUSTOR Portal will automatically run the default App at startup.

Default App: ASUSTOR Portal

Currently being displayed on: ASUSTOR Portal

Figure 210: ASUSTOR Portal app

The first page – *General* – allows control over which information is displayed on the ASUSTOR Portal screen and whether the icons for ADM, Chrome and YouTube are displayed. The default app is the Portal itself, but you could skip this and run, say, Netflix or YouTube instead. This capability is useful if, say, the NAS is permanently plugged into a television set to provide entertainment. Having made any changes, click **Apply**.

The second page – *Wallpaper* – is for customizing the background of the Portal screen. A selection of wallpapers are provided, or you can upload your own images from the NAS or a computer.

The third page – *Favorites* – control which icons are displayed on the Portal, along with their position. As the icons are links to websites, you can add your own favourite websites to the Portal screen.

Resolution and *Overscan* enable you to adjust the size and resolution of the Portal as it is viewed on the HDMI screen.

The sixth and final page controls the *Screensaver*. A small selection are provided, or you can use one of your own photographs.

Additional Apps/Links from App Central

Further apps and links for ASUSTOR Portal are available from within App Central. Use the search facility to look for 'portal', which will return around 30 candidates at the time of writing. The list includes:

Amazon Prime - available for Australia, Canada, Spain, France, Germany, India, Italy, Japan, UK and USA. This provides a connection both to Prime Video and Amazon Music.

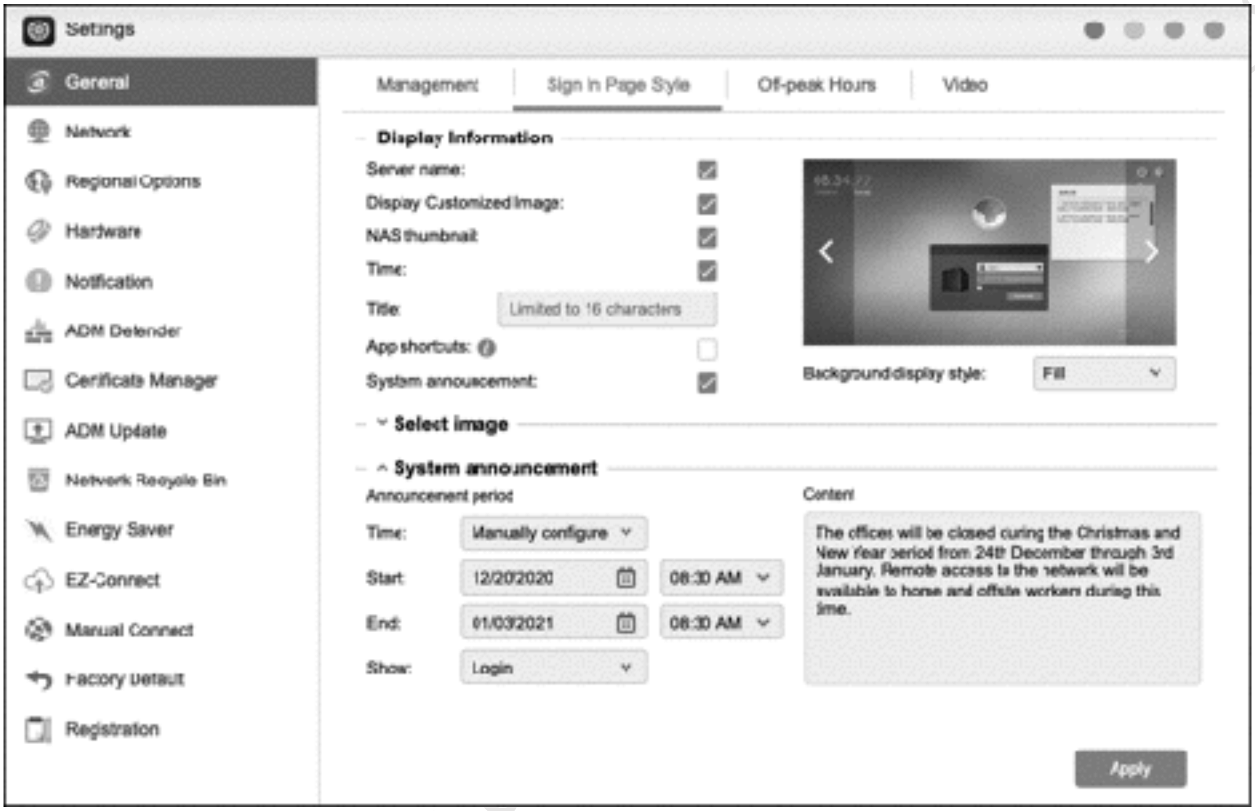
Asunder – enables a CD to ripped, for playback within SoundsGood.

LibreOffice – popular open source package, compatible with Microsoft Office and that provides word processing, spreadsheets and presentations.

SNES9X – an emulator for the Super Nintendo.

12.4 Customizing the Sign In Page

The sign in page (login screen) for ADM can be changed and customized. You might wish to do this in a business or educational establishment, say, to enforce ‘branding’ for the organization, or simply to have a different or more distinct appearance. To do, click **Preferences** > **General** and click the **Sign In Page Style** tab.



Display Information

Server name: ☑

Display Customized Image: ☑

NAS thumbnail: ☑

Time: ☑

Title: Limited to 16 characters

App shortcuts: □

System annoucement: ☑

Background display style: Fill

Select image

System announcement

Announcement period

Time: Manually configure

Start: 12/20/2020 08:30 AM

End: 01/03/2021 08:30 AM

Show: Login

Content

The offices will be closed during the Christmas and New Year period from 24th December through 3rd January. Remote access to the network will be available to home and offsite workers during this time.

Figure 211: Sign In Page Style

A selection of information items can be shown on the sign in page, such as the *Server name*, the *Time* and a *NAS thumbnail* picture. If the *App shortcuts* box is ticked, small icons for Photo Gallery, LooksGood, SoundsGood and Surveillance Center are displayed, enabling users to directly login to the applications, rather than login to ADM first. A short *Title* of up to 16 characters can also be specified.

If the *Display Customized Image* box is ticked, a small image can be specified from the *Select image* section to appear above the login panel. In a business this could be the company logo, for instance. The overall *Background Image* can also be defined by clicking on the mini folder icon – a small selection is provided, else you can use any image of your choosing:

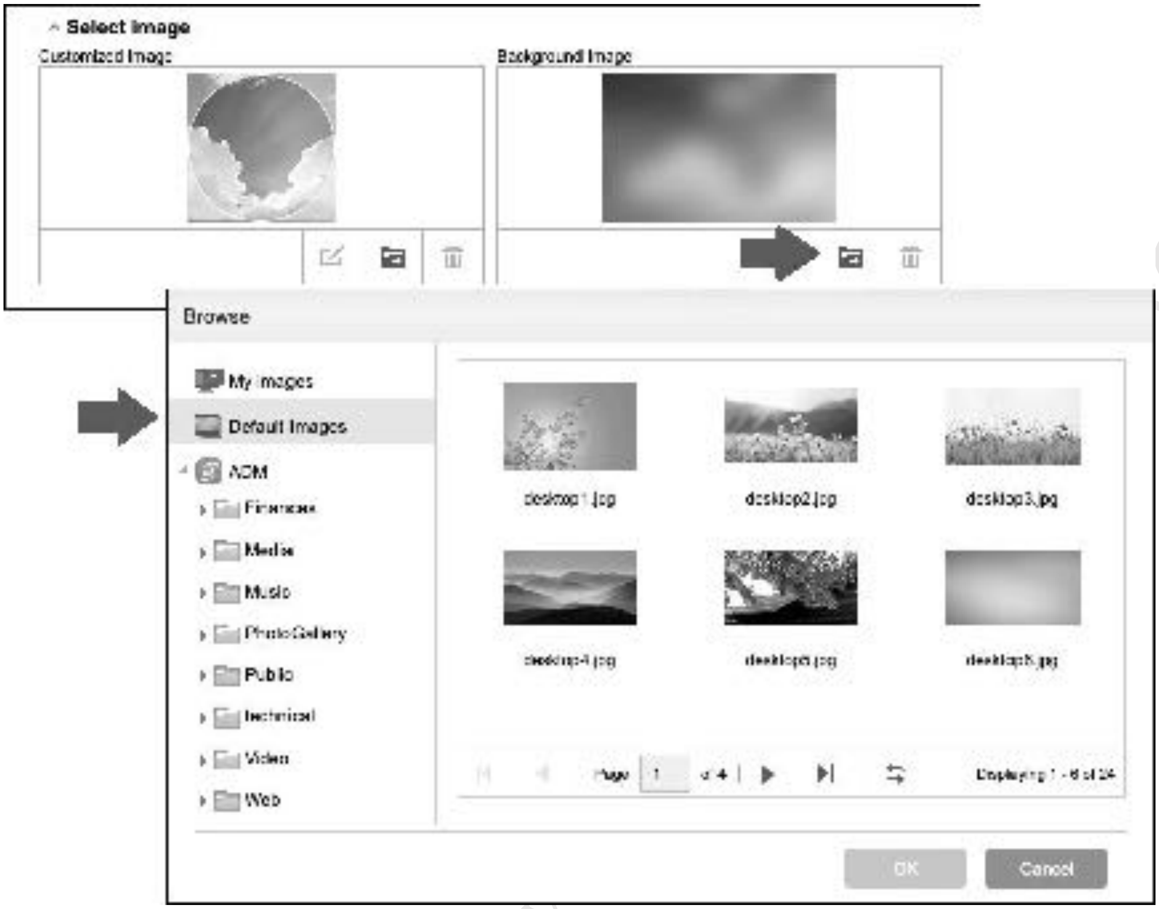


Figure 212: Choosing a Background image

The System Announcement facility can be used to send a message to all users of the system. This could be a permanent message e.g. advising what they should do in the event of problems, or a timed message to give news e.g. notification of holidays.

To define the announcement, go to **Preferences** > **General** > **Sign In Page Style**. Tick the **System announcement** box. In the section below, enter the announcement ('Content') and choose whether it is displayed permanently or for a specific time and so on. Having defined it, click **Apply**. In this example at the start of this section, a message will be displayed from 20th December to 3rd January.

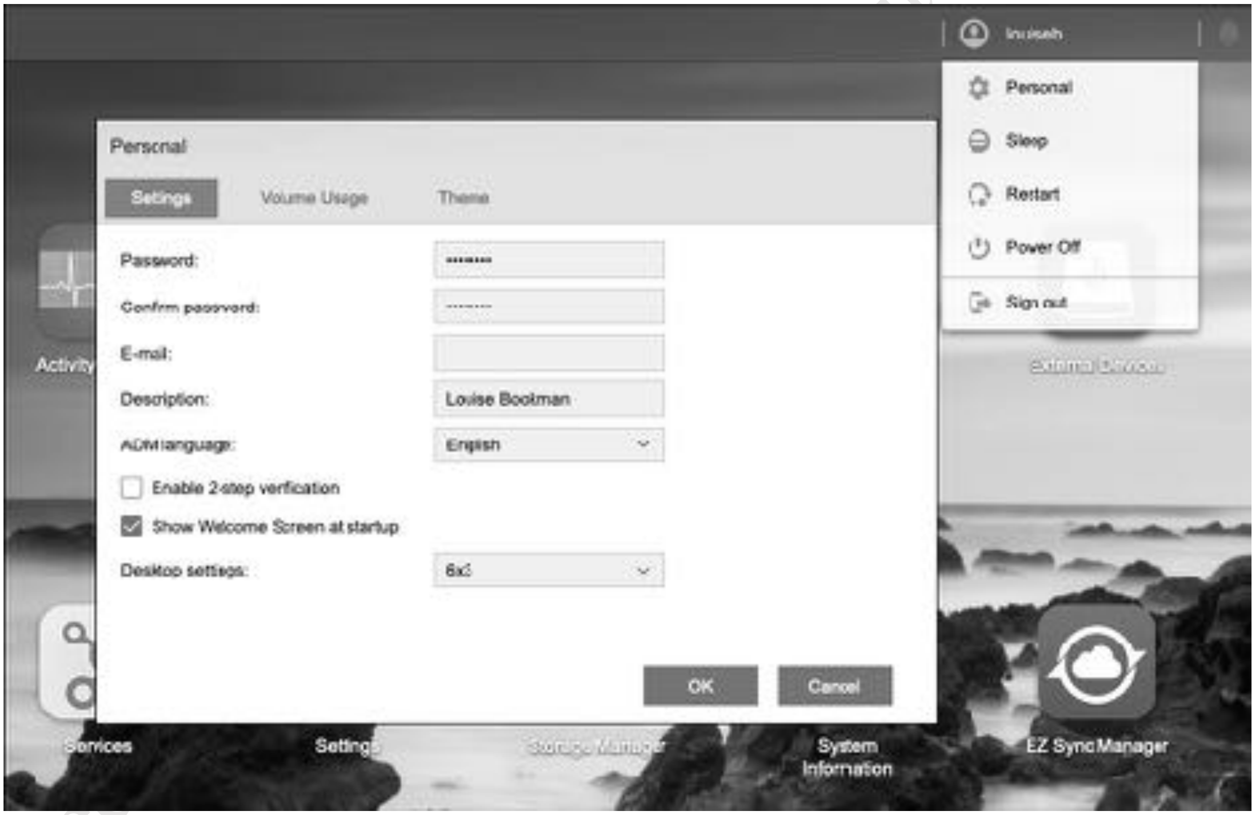
12.5 Customizing the Desktop

The Desktop can be customized by each user on an individual basis in several ways:

Icons - Frequently used icons can be pinned to the taskbar for easy access. Right-click an icon and click the **Pin to Taskbar** message. This is particularly useful if there are many apps installed on the system, such that it may be necessary to switch between multiple pages to find them. To subsequently remove an icon on the Taskbar, right-click it and choose **Unpin from Taskbar**.

The overall layout of the icons on the Desktop can be changed to improve the appearance on screens of different sizes and resolutions. Click the username in the top right-hand corner of the screen, followed by **Personal**. On the **Settings** tab, use the *Desktop settings* dropdown to switch between the different layouts.

Language - A user can work with ADM in the language of their choice, regardless of whatever language the server is configured in. This can be particularly useful in environments where multiple languages are in use, such as English and Spanish in parts of the United States, or French and English in Canada. To switch language, the user should click their name in the top right-hand corner of the screen, followed by **Personal**. On the **Settings** tab, use the *ADM language* dropdown to choose the language. A list of more than 20 widely used languages is presented – click on the desired one to switch.



Password: ••••••••

Confirm password: ••••••••

E-mail:

Description: Louise Bookman

ADM language: English

☐ Enable 2-step verification

☑ Show Welcome Screen at startup

Desktop settings: 6x3

Figure 213: Personal settings

Theme – the overall theme (colouring scheme) of the Desktop and windows can be chosen. Click the username in the top right-hand corner of the screen, followed by **Personal**. On the **Theme** tab, click the light or dark theme and make a choice from the *Customize Window* dropdown.

Home Screen (‘Wallpaper’) – the home screen (desktop wallpaper) can also be changed from the Theme tab. Click the mini folder icon – a selection of images is provided, else you can use any image of your choosing:

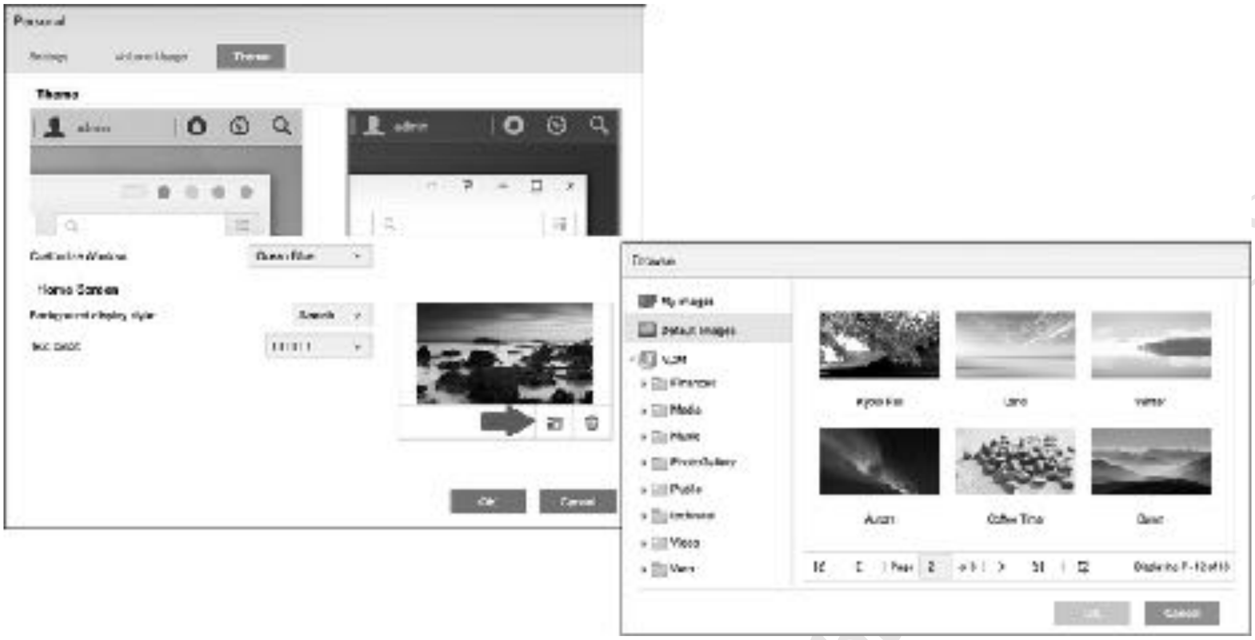


Figure 214: Theme and Home Screen

12.6 Printing

One advantage of networking is that it allows printers to be shared, potentially saving money as well as physical space. There are two techniques for sharing a printer on the network:

Ethernet or Wireless

Most modern printers have built-in Ethernet or wireless connections, giving them an existence on a network that is independent of any server or computer. This is generally the best approach in most households and small organizations. The exact method of 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 generally preferable, as performance is usually better compared to wireless.

The printer should have a fixed IP address. This should be adjacent to the address of the server and apart from the addresses used by the computers. Suppose, for instance, that the internet gateway (router) is 192.168.1.1 and the server is 192.168.1.2. If two printers were added to the network, then suitable addresses might be 192.168.1.3 and 192.168.1.4. IP addresses can usually be configured on the printer else given a reserved IP address from the DHCP server.

Download the latest drivers for the printers. Consider storing the drivers on the NAS so that they can then be copied to the individual computers, rather than have to download them from the internet each time.

Printer manufacturers sometimes offer a choice of drivers, for instance a basic one as well as a full-featured one. Use the basic one 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, specifically combined printer/copier/scanners, not all functions may be available in a networked environment or may require additional software from the manufacturer to fully utilize them.

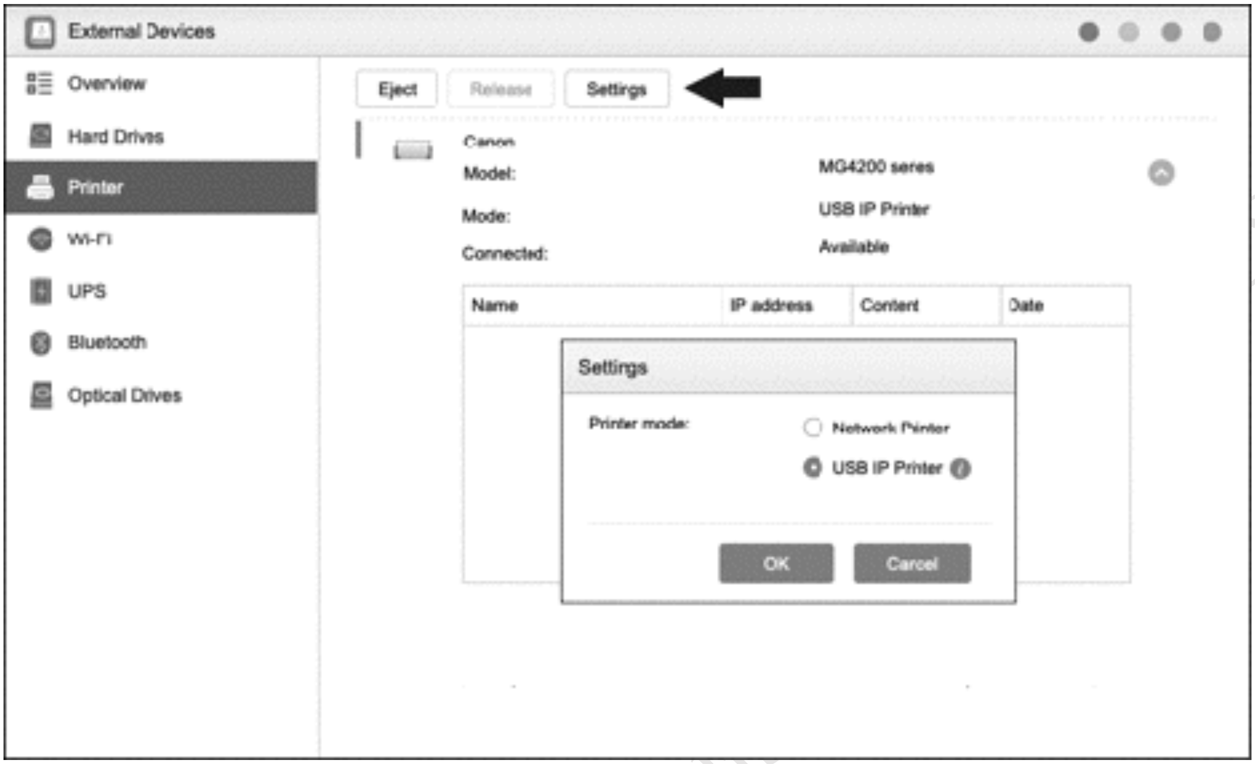
Sharing USB Printers

Several years ago, the ability to share USB printers would have been considered a Big Thing. These days most new printers have built-in Ethernet or wireless connections, meaning it is no longer the important feature that it once was, but the ability to share USB printers can still be useful in some circumstances. Some caveats: although it usually works well, not all printers are necessarily suitable. For instance, all-in-one devices that combine printing with scanning, copying and faxing may not work, or may work for printing only, whilst obscure brands of printer may give difficulties. Up to three USB printers can be shared from the NAS, subject to the availability of USB ports.

Begin by downloading the latest drivers for the printer from the manufacturer’s website and copying them to each computer that will use the printer. Often there is a universal driver available for all versions of Windows, but sometimes it may be necessary to download different versions if there are multiple operating systems in use e.g. for Windows 7, Windows 10, 32-bit, 64-bit etc.

Connect the printer to the NAS using a USB cable. It needs to be plugged directly into a USB socket on the NAS and not via a USB hub. Power on the printer.

Click the **External Devices** icon on the Desktop. The printer should have been recognised and be visible in the **Overview** and **Printer** screens. Click the latter and on it click the **Settings** button and set the *Printer mode* to **USB IP Printer**. Click **OK**. The screen will refresh and the printer should be listed as ‘Connected’ and ‘Available’.



Canon

Model: MG4200 seres

Mode: USB IP Printer

Connected: Available

Name	IP address	Content	Date

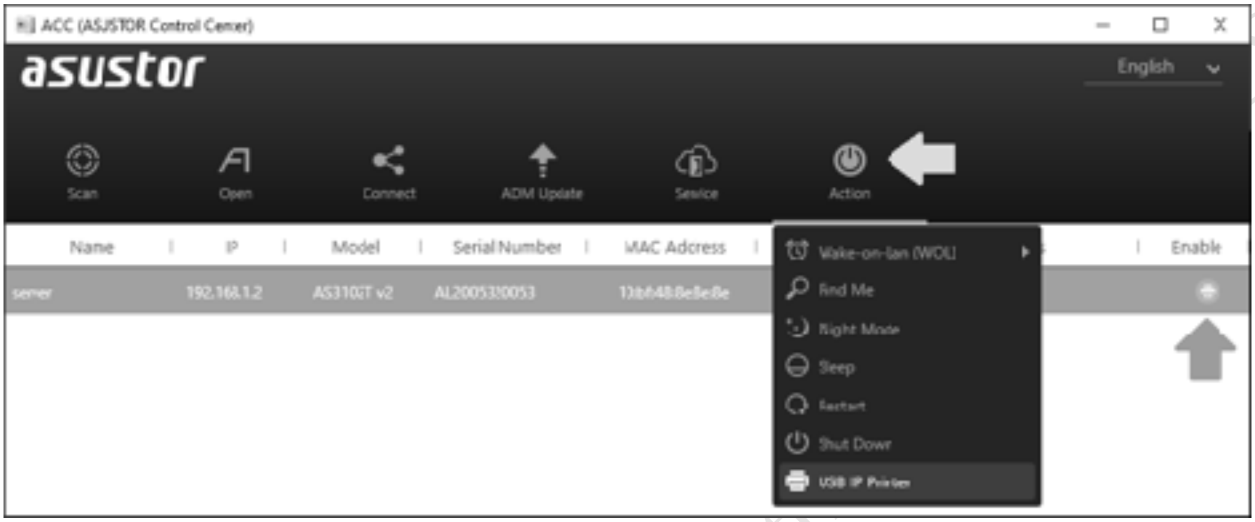
Settings

Printer mode: ○ Network Printer ● USB IP Printer

Figure 215: Settings for USB printer within ADM

Connecting a Windows PC

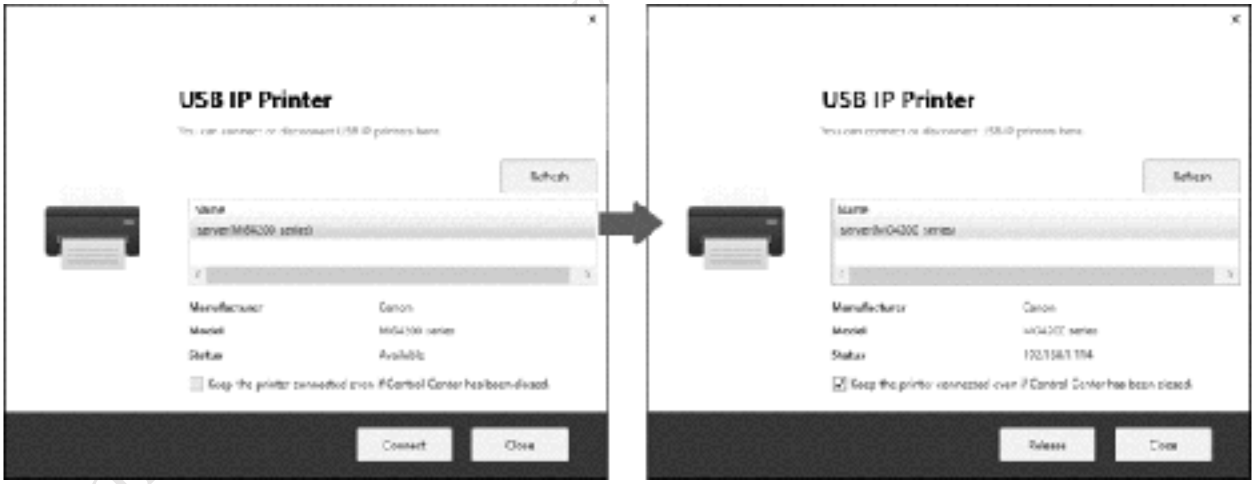
Install and run ASUSTOR Control Center on the computer if it is not already in place. The printer will be indicated by a small icon on the right-hand side of the entry for the server. Click the **Action** icon and choose **USB IP Printer** from the pop-up menu.



Name	IP	Model	Serial Number	MAC Address	Enable
server	192.168.1.2	AS3102T v2	AL2005330053	10:bf:48:8e:8e:8e	

Figure 216: USB IP printer listed in ASUSTOR Control Center

A panel for connecting to the printer is displayed: highlight it and click **Connect**. It should do so after a few seconds; the *Status* will display the IP address and the *Connect* button will change to *Release*. Make a note of the IP address. At this point the **Keep the printer connected even if Control Center has been closed** box can optionally be clicked:


USB IP Printer
You can connect or disconnect USB IP printers here.
Refresh
Connect
Close
USB IP Printer
You can connect or disconnect USB IP printers here.
Refresh
Release
Close

Name
server(MG4200 series)

Manufacturer: Canon
Model: MG4200 series
Status: Available

□ Keep the printer connected even if Control Center has been closed

Name
server(MG4200 series)

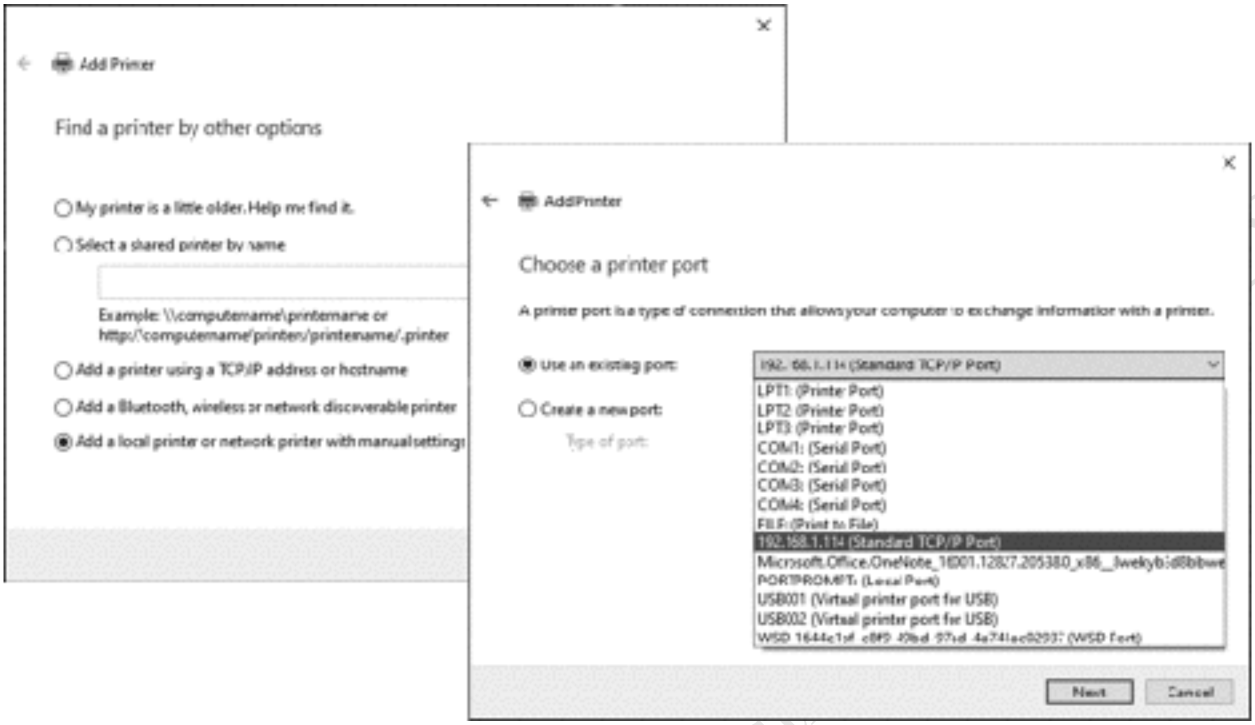
Manufacturer: Canon
Model: MG4200 series
Status: 192.168.1.114

☑ Keep the printer connected even if Control Center has been closed

Figure 217: Connect to the printer in with ASUSTOR Control Center

Within Windows the printer can now be added. In this example we are using Windows 10.

Click **Start** > **Settings** > **Devices** > **Printers & scanners**. Click **Add a printer or scanner**; however, the printer will not be found and after a short while Windows will stop trying. Click **The printer that I want isn’t listed** link and on the resultant panel choose the **Add a local printer or network printer with manual settings** option, followed by **Next**. On the next panel, click **Use an existing port** and from the dropdown look for the IP address that the ASUSTOR Control Center assigned to the printer. Select it and click **Next**.


Add Printer

Find a printer by other options

○ My printer is a little older. Help me find it.
○ Select a shared printer by name

Example: \\computername\printername or http://computername/printers/printername/.printer

○ Add a printer using a TCP/IP address or hostname
○ Add a Bluetooth, wireless or network discoverable printer
● Add a local printer or network printer with manual settings

Add Printer

Choose a printer port

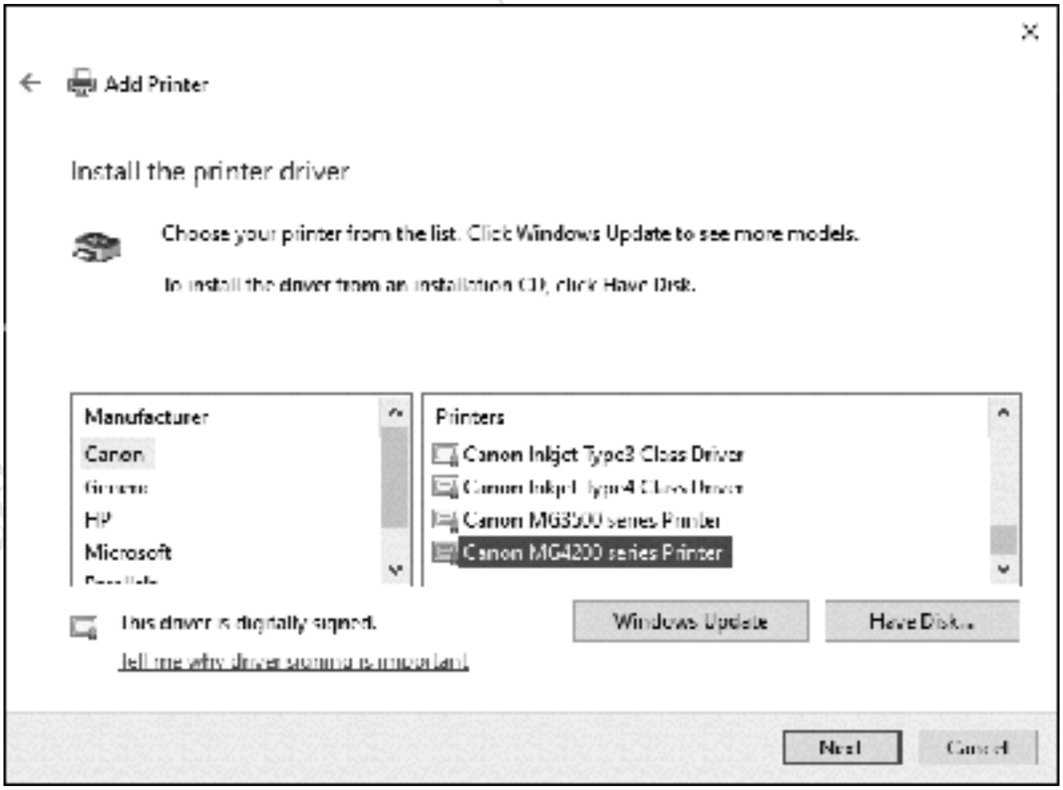
A printer port is a type of connection that allows your computer to exchange information with a printer.

● Use an existing port: 192.168.1.114 (Standard TCP/IP Port)
○ Create a new port:
Type of port:

LPT1: (Printer Port)
LPT2: (Printer Port)
LPT3: (Printer Port)
COM1: (Serial Port)
COM2: (Serial Port)
COM3: (Serial Port)
COM4: (Serial Port)
FILE: (Print to File)
192.168.1.114 (Standard TCP/IP Port)
Microsoft.Office.OneNote_16001.12827.205380_x86__8wekyb3d8bbwe
PORTPROMPT: (Local Port)
USB001 (Virtual printer port for USB)
USB002 (Virtual printer port for USB)
WSD 1644c1af-c8f9-49bd-97ad-4a74lac92937 (WSD Port)

Figure 218: Specifying the port

Choose the printer on the next panel. Most modern printers should be listed, else you can use the printer manufacturer's disk or click **Windows Update** and allow Windows to search for and install a driver (this may prove to be a lengthy process).


Add Printer

Install the printer driver

Choose your printer from the list. Click Windows Update to see more models.

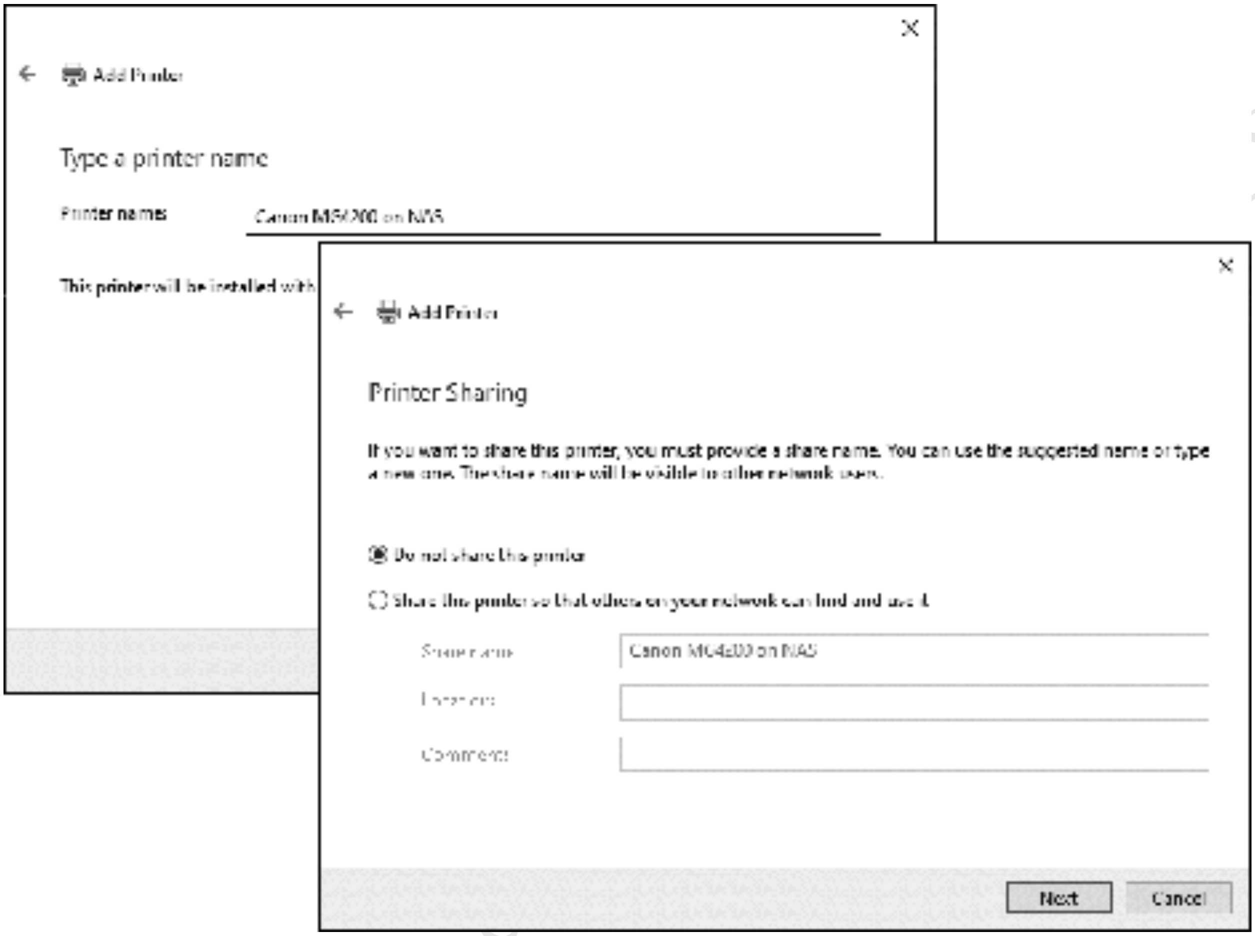
To install the driver from an installation CD, click Have Disk.

Manufacturer	Printers
Canon	Canon Inkjet Type3 Class Driver
Generic	Canon Inkjet Type4 Class Driver
HP	Canon MG3500 series Printer
Microsoft	Canon MG4200 series Printer

This driver is digitally signed.
Tell me why driver signing is important

Figure 219: Install a driver for the printer

On the subsequent panel you can specify a descriptive name for the printer. On the one after that, choose the **Do not share this printer** option and click **Next**.



Add Printer

Type a printer name

Printer name: Canon MG4200 on NAS

This printer will be installed with

Add Printer

Printer Sharing

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

● Do not share this printer

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

Share name: Canon MG4200 on NAS

Location:

Comment:

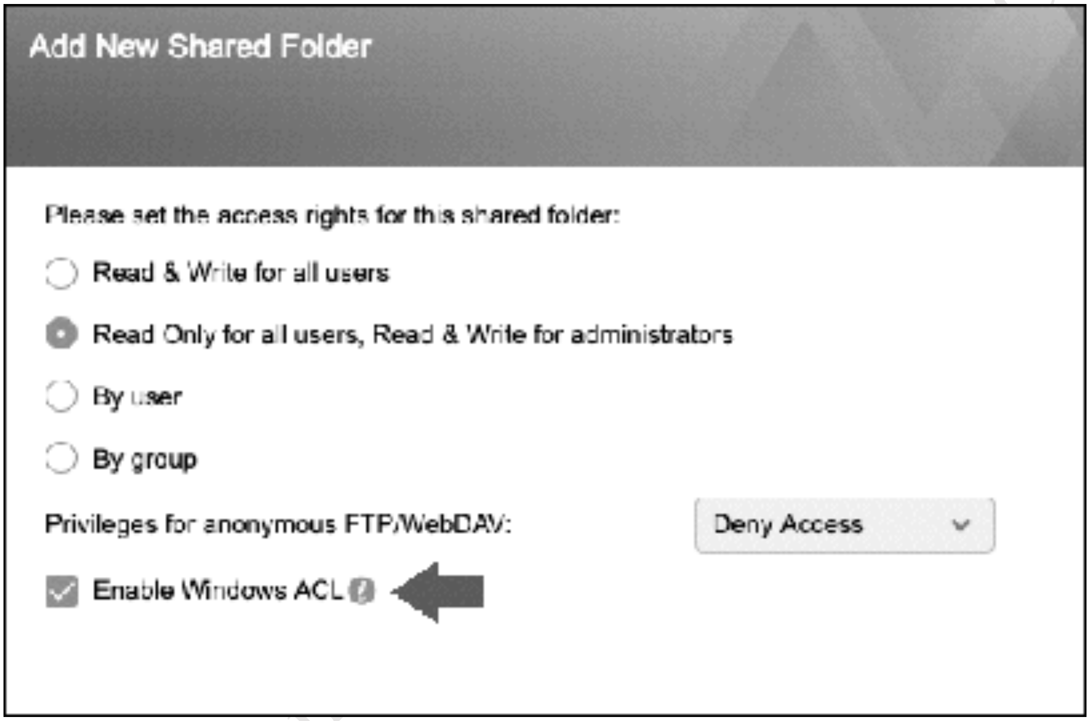
Figure 220: Printer options

When installation is complete, the printer will be listed in **Settings** > **Devices** > **Printers & scanners**. You may wish to print a test page to prove that everything is working. Then, repeat these steps for any other Windows 10 computers that require access to the printer.

12.7 ACL (Access Control Lists)

When a shared folder is created on the NAS, as described in section 4.2 Adding a Shared Folder, access rights are specified as *Read/Write*, *Read Only* or *Deny* and in most home and small business environments that choice of options will be sufficient. However, in some scenarios it may not provide the necessary granularity to provide precise control over the folders and individual files. If you work in information technology and have used Windows Server, then you may be familiar with ACL or *Access Control Lists*, which are designed to do precisely this. ADM also supports the ACL mechanism; the purpose of this section is not to explain ACL in detail, but to illustrate how it is implemented in ADM for the benefit of those who understand and wish to use it.

To enable ACL when creating the folder, tick the **Enable Windows ACL** box:



Add New Shared Folder

Please set the access rights for this shared folder:

○ Read & Write for all users

● Read Only for all users, Read & Write for administrators

○ By user

○ By group

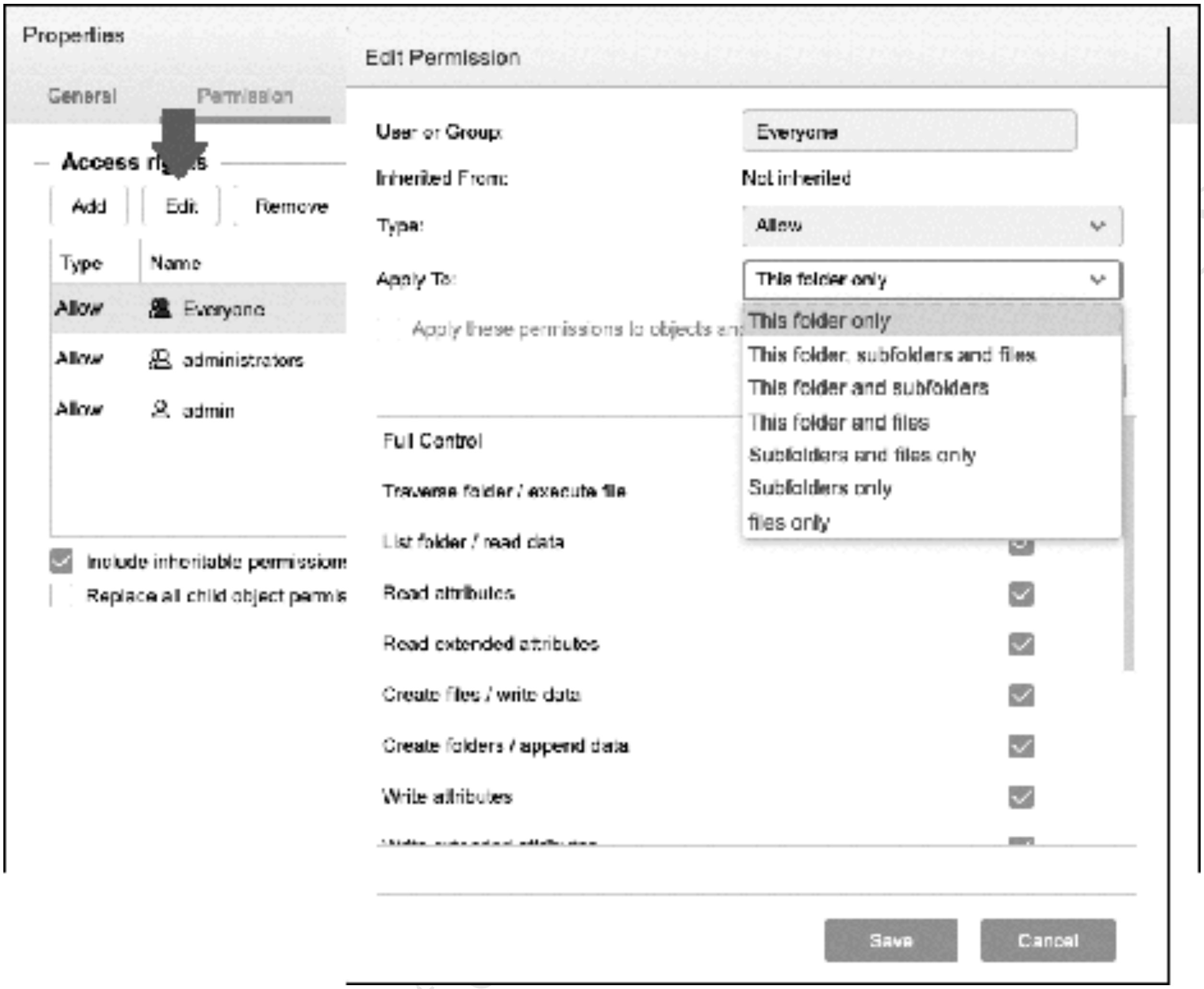
Privileges for anonymous FTP/WebDAV: Deny Access

☑ Enable Windows ACL

Figure 221: Enable ACL during folder creation

Whilst not strictly true in a technical sense, it is usually best to work on the basis that ACL *replaces* the standard access rights. To set the various ACL permissions on an enabled shared folder:

Right-click the folder in File Explorer and choose **Properties** from the pop-up menu. On the **Permission** tab, highlight the user and click **Edit**. From here you can control the access attributes plus whether those rights are inherited and what they apply to (if you have previously done this in a Windows environment it will be very familiar). Having made changes, click **Save**, followed by **Apply** on the original screen.



Properties

General | Permission

Access rights

Add | Edit | Remove

Type	Name
Allow	Everyone
Allow	administrators
Allow	admin

☑ Include inheritable permission

□ Replace all child object permis

Edit Permission

User or Group: Everyone

Inherited From: Not inherited

Type: Allow

Apply To: This folder only

- This folder only
- This folder, subfolders and files
- This folder and subfolders
- This folder and files
- Subfolders and files only
- Subfolders only
- files only

□ Apply these permissions to objects an

Full Control

Traverse folder / execute file

List folder / read data ☑

Read attributes ☑

Read extended attributes ☑

Create files / write data ☑

Create folders / append data ☑

Write attributes ☑

Save | Cancel

Figure 222: ACL attributes

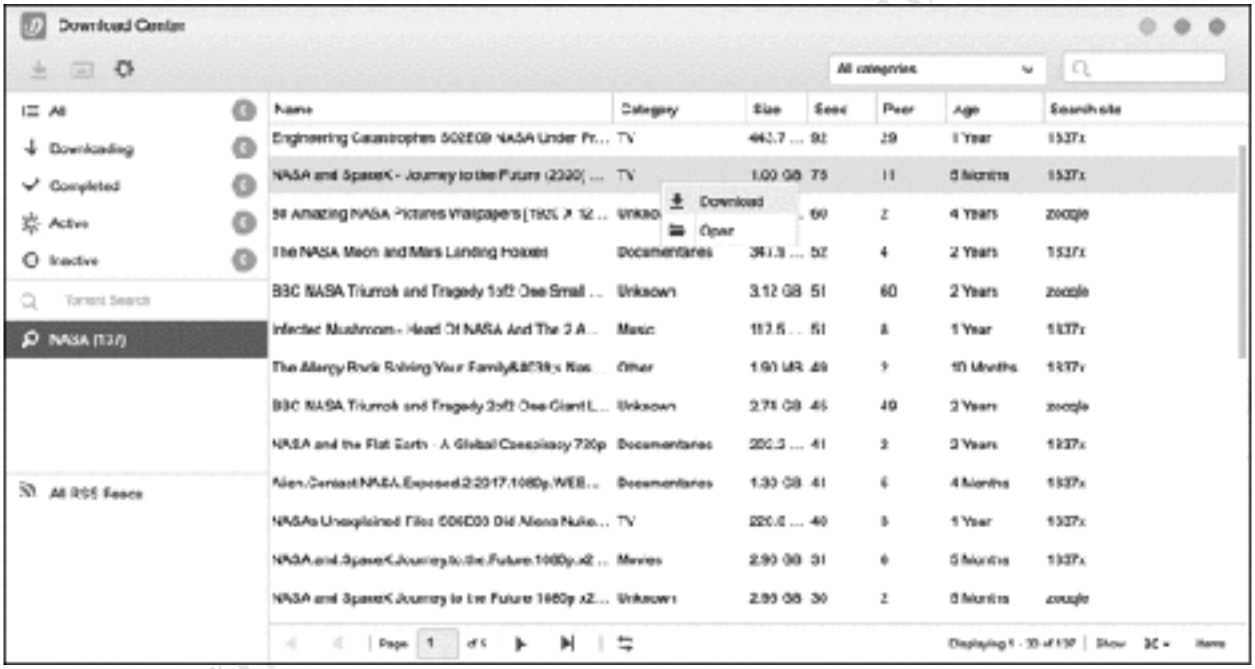
12.8 Download Center

Download Center is one of the most popular applications for ASUSTOR NAS and allows you to download files from Internet-based services such as BitTorrent, FTP, HTTP, plus subscribe to RSS feeds. Many thousands of free and public domain movies and other items are available.

Begin by downloading and installing Download Center from the App Center. Upon running it for the first time, it prompts for a default download folder for storing the files. As part of the installation process it will have created a shared folder called *Download* and most people will choose that. Click **OK** and the main screen will appear.

If you are familiar with BitTorrent, you will find that Download Center is an effective client with all the features that you might expect. If you are new to the topic, it has already been programmed with defaults and features to make it immediately useful and not require any additional knowledge.

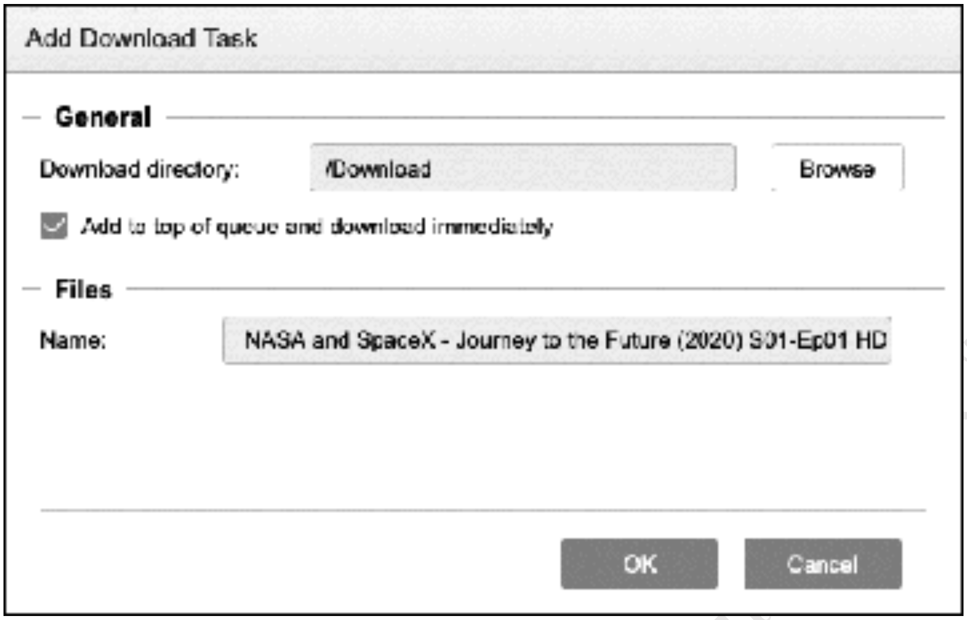
To search for content, type in the topic of interest in the *Torrent Search* field on the left-hand side of the screen and Download Center will search using a number of pre-defined search engines and return a list of suitable titles; depending on the search criteria, this may return none, several or many candidates. In this example we are searching on 'NASA':



Name	Category	Size	Seed	Peer	Age	Search site
Engineering Catastrophes S02E09 NASA Under Pr...	TV	443.7 ...	92	29	1 Year	1337x
NASA and SpaceX - Journey to the Future (2020) ...	TV	1.00 GB	75	11	5 Months	1337x
50 Amazing NASA Pictures Wallpapers [1920 X 12...	Unkno	...	60	2	4 Years	zooqle
The NASA Moon and Mars Landing Hoaxes	Documentaries	341.3 ...	52	4	2 Years	1337x
BBC NASA Triumph and Tragedy 1of2 One Small ...	Unknown	3.12 GB	51	60	2 Years	zooqle
Infected Mushroom - Head Of NASA And The 2 A...	Music	117.5 ...	51	8	1 Year	1337x
The Allergy Book Solving Your Family&#039;s Nas...	Other	1.90 MB	49	7	10 Months	1337x
BBC NASA Triumph and Tragedy 2of2 One Giant L...	Unknown	2.74 GB	45	49	2 Years	zooqle
NASA and the Flat Earth - A Global Conspiracy 720p	Documentaries	200.3 ...	41	3	3 Years	1337x
Alien.Contact.NASA.Exposed.2.2017.1080p.WEB...	Documentaries	1.30 GB	41	6	4 Months	1337x
NASAs Unexplained Files S06E03 Did Aliens Nuke...	TV	220.6 ...	40	5	1 Year	1337x
NASA.and.SpaceX.Journey.to.the.Future.1080p.x2...	Movies	2.90 GB	31	6	5 Months	1337x
NASA and SpaceX Journey to the Future 1080p x2...	Unknown	2.85 GB	30	2	5 Months	zooqle

Figure 223: Searching for BitTorrents

Highlight the desired file(s), right-click and choose **Download** (else click the download icon in the top left-hand corner of the screen). On the pop-up panel that appears the Download directory can be changed if required. Download requests are added to a queue, but if you wish to prioritize the download you can tick the **Add to top of queue and download immediately** box. Click **OK**.


Add Download Task

General

Download directory: /Download

☑ Add to top of queue and download immediately

Files

Name: NASA and SpaceX - Journey to the Future (2020) S01-Ep01 HD

Figure 224: Adding a download task

The status of the downloads can be monitored by clicking the options on the left-hand of the main screen i.e. Downloading, Completed, Active, Inactive.

The various parameters involved with downloading can be controlled by clicking the **Preferences** wheel at the top of the screen. There are five tabs:

General – specify the maximum number of download and change the download folder from here.

Connection – defines the port number (the default is fine, though) and optional encryption.

Bandwidth – allows bandwidth limits for uploading and downloading to be specified (to prevent the internet connection becoming saturated).

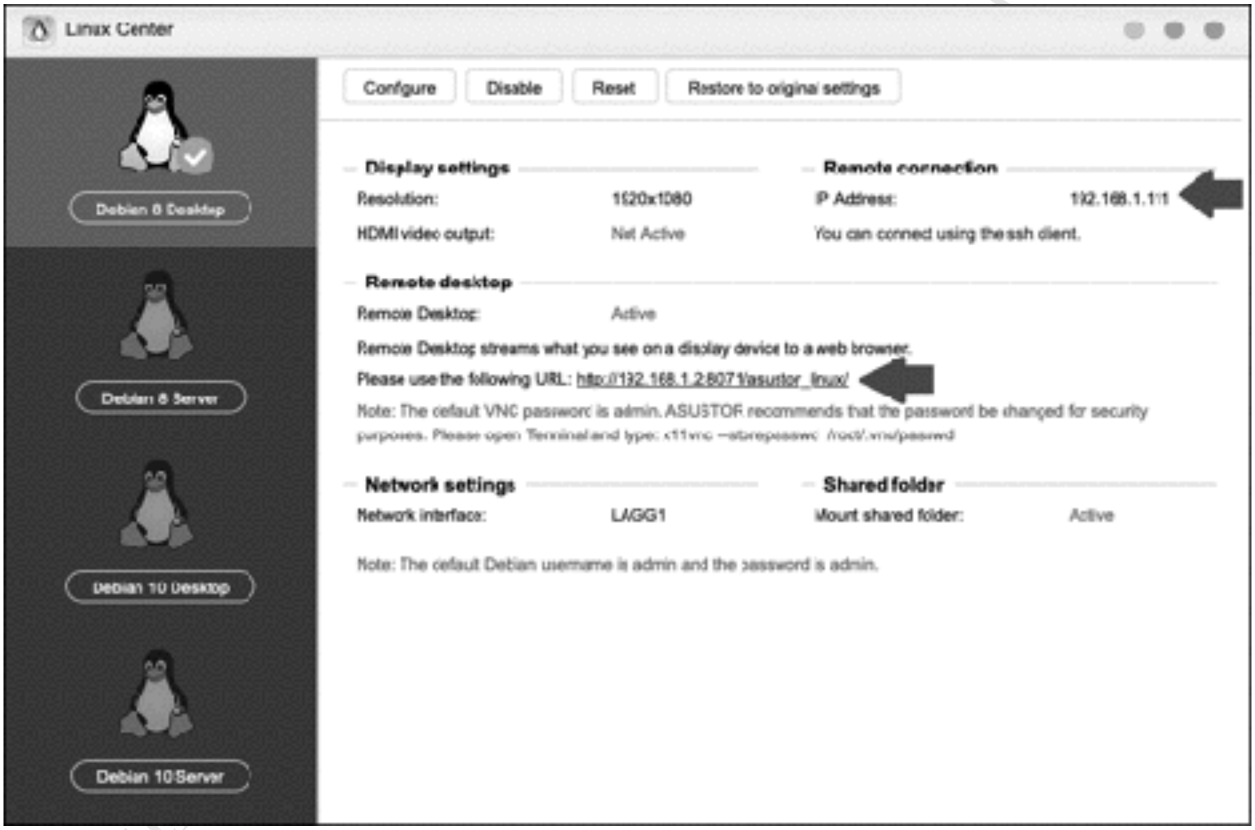
Download Schedule – specify a download schedule. For instance, full-speed downloads could be restricted to overnight.

Torrent Search Engines – manage search engines. It is pre-populated with several popular ones for BitTorrent but they can be removed and/or other ones added.

12.9 Linux Center

Linux Center enables you to run the popular Debian Linux distribution on your NAS. Doing so provides access to a wide variety of applications, including LibreOffice, Chrome, Spotify and Plex, plus is also a good option for software developers. If the NAS has an HDMI output, it can be used as a complete Linux system if a screen is connected and a keyboard and mouse are plugged into the USB ports. Alternatively, Linux can be viewed in a browser tab. To run Linux Center, a supported NAS with at least 2GB RAM is needed, although more memory is better. On HDMI-equipped models, ASUSTOR Portal and Linux Center cannot be used simultaneously as both require use of the HDMI port.

Download and install Linux Center from App Central. Clicking the icon will then give a choice of distributions to download and install, which at the time of writing are *Debian 8 Desktop*, *Debian 8 Server*, *Debian 10 Desktop* and *Debian 10 Server*. Make a choice and click the **Install** button. Depending on the internet connection, this may take some time. Upon completion, a screen along the following lines is shown. Make a note of the IP address that has been assigned to the Linux machine and the Remote Desktop IP address for accessing it, which will have been derived from the IP address of the NAS:



Display settings

Resolution: 1920x1080

HDMI video output: Not Active

Remote connection

IP Address: 192.168.1.111

You can connect using the ssh client.

Remote desktop

Remote Desktop: Active

Remote Desktop streams what you see on a display device to a web browser.

Please use the following URL: http://192.168.1.2:8071/asustor_linux/

Note: The default VNC password is admin. ASUSTOR recommends that the password be changed for security purposes. Please open Terminal and type: x11vnc --storepasswd /root/.vnc/passwd

Network settings

Network interface: LAGG1

Shared folder

Mount shared folder: Active

Note: The default Debian username is admin and the password is admin.

Figure 225: Linux Center

There are basic controls on the screen to *Configure*, *Disable* (so it does not startup automatically), *Reset* or *Restore to original settings.*

To access the Linux system, click or enter the URL/IP address for the remote desktop, which will cause it to be displayed in a new browser tab. A popular utility called *VNC* handles matters; the default password for it is *admin*, although ASUSTOR recommend changing it, using the instructions on the main Linux Center screen. The Debian login screen will be displayed – enter the default user name of *admin*, the password (also *admin*) and click the **Log In** button. After a few seconds you will be presented with the Debian desktop; at this point you have a ‘regular’ Linux system. A useful additional feature is a link to the file system on the NAS, whereby its file system is directly accessible from Debian’s File Manager. When finished with Linux, logout and close the browser window.

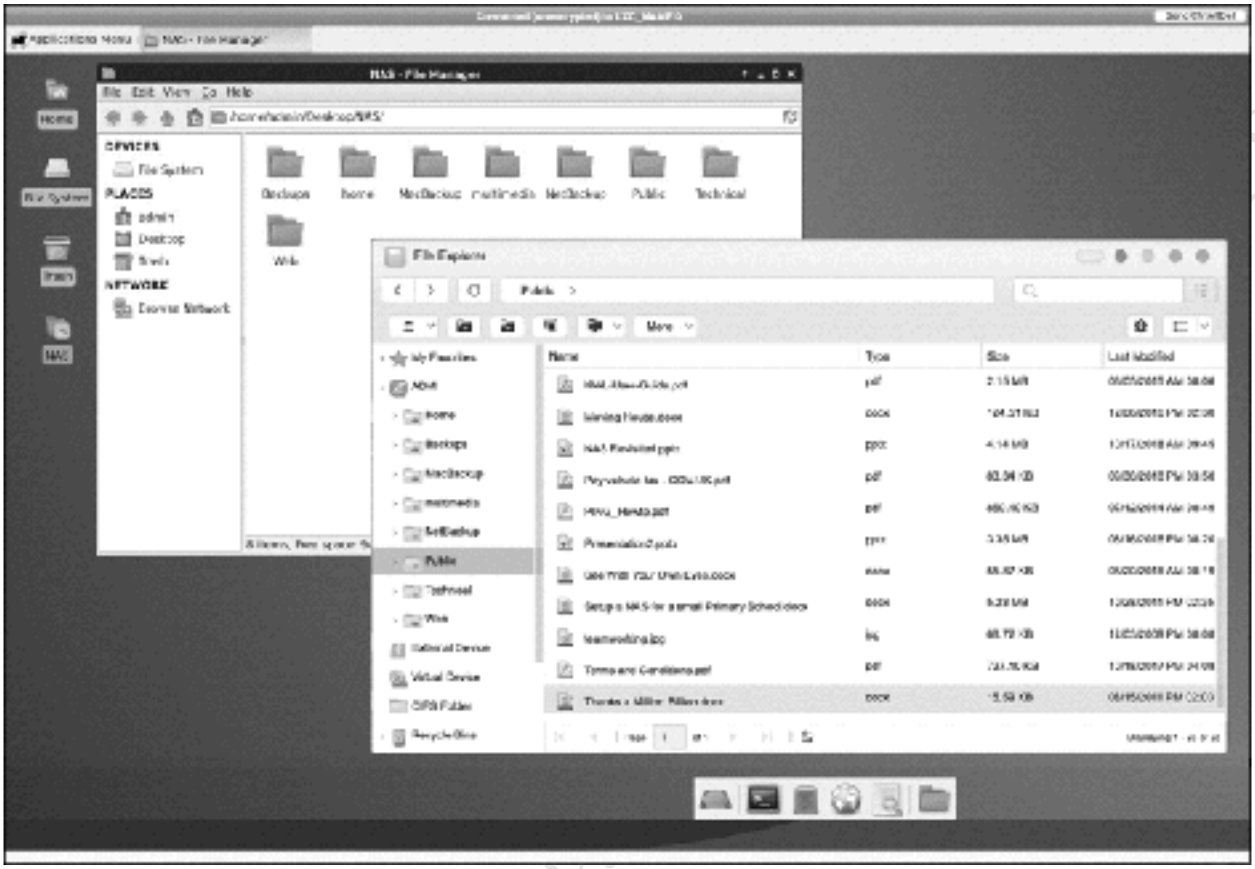


Figure 226: File system viewed simultaneously from Linux Center and ADM

12.10 Surveillance Center

Surveillance Center is an app from ASUSTOR that turns the NAS into a fully functional CCTV surveillance system and network video recorder. It works with a wide variety of IP cameras and includes features such as real-time monitoring, recording and playback and alarm notifications. Whether you wish to setup a single camera to monitor your home, a more sophisticated system monitoring business premises with dozens of cameras, or any other monitoring requirement, then there is a good chance that *Surveillance Center* is suitable. For home users, one advantage is that there are no ongoing subscription fees, which is commonly the case with consumer surveillance camera solutions. Surveillance Center could merit a manual of its own – this section simply describes how to get started.

Note: the number of cameras supported on a particular NAS model varies, depending on its performance capabilities

Installation

Begin by downloading and installing Surveillance Center from App Central. As part of this process it will create a shared folder called *Surveillance*, which is the default location where recordings will be stored. Launching the app will cause it to open in a new browser window; it is necessary to login to use it and it can also be accessed by users without going in to regular ADM initially. On first usage you will be prompted to download and install a viewer component, which must be done (and it is required on any computer which subsequently accesses Surveillance Center). Thereafter the main screen appears so. There are four tabs and it should be apparent what each does based upon their names. On the right-hand side of the screen is a 'remote control' for controlling the system whilst it is in use.

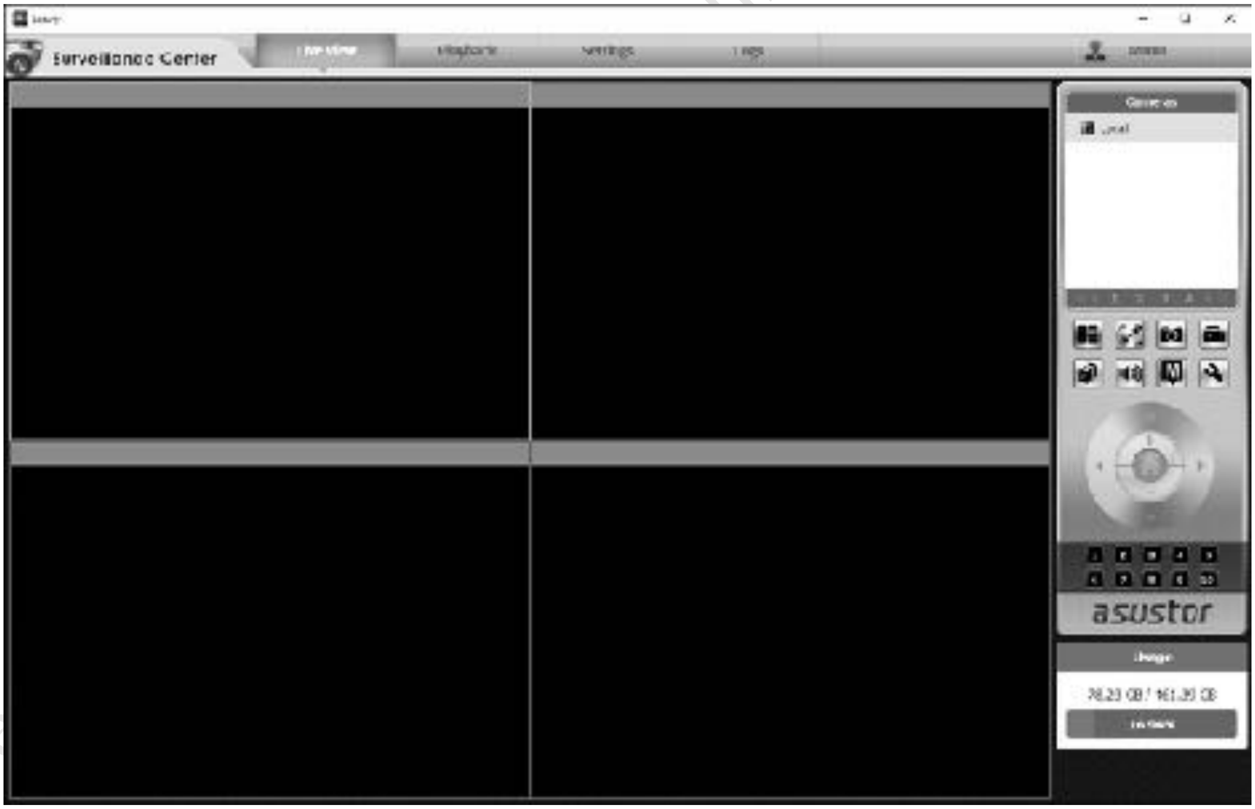
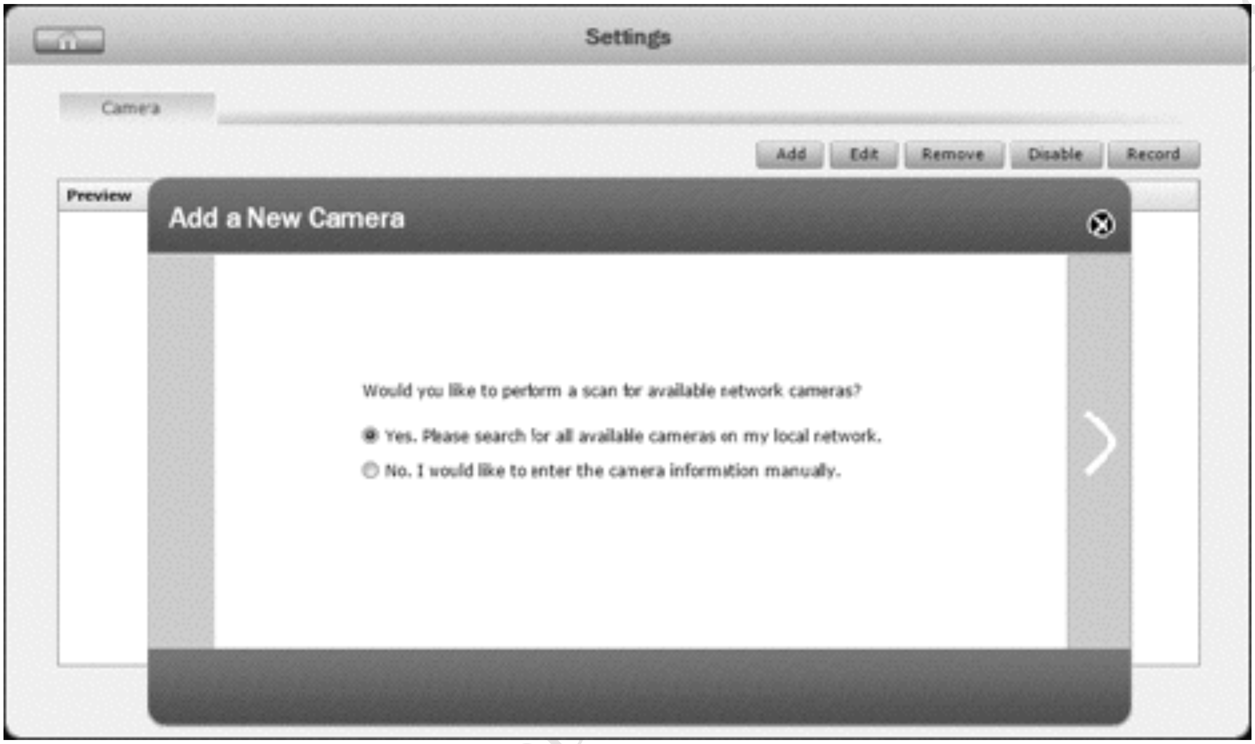


Figure 227: Surveillance Center main screen

Adding and Using Cameras

The cameras now need to be added. These should first be configured separately for the network, using the instructions and any software provided by the manufacturer. Essentially all you require is that the camera is connected and operational: you do not want to sign-up to any services or install any other software for monitoring and recording. If you have multiple cameras, it is suggested that you add them one at a time. In Surveillance Center, click **Settings** and on it click the **Camera** icon. On the resultant panel click **Add**, answer **Yes** to the question about searching for cameras and click on the chevron:



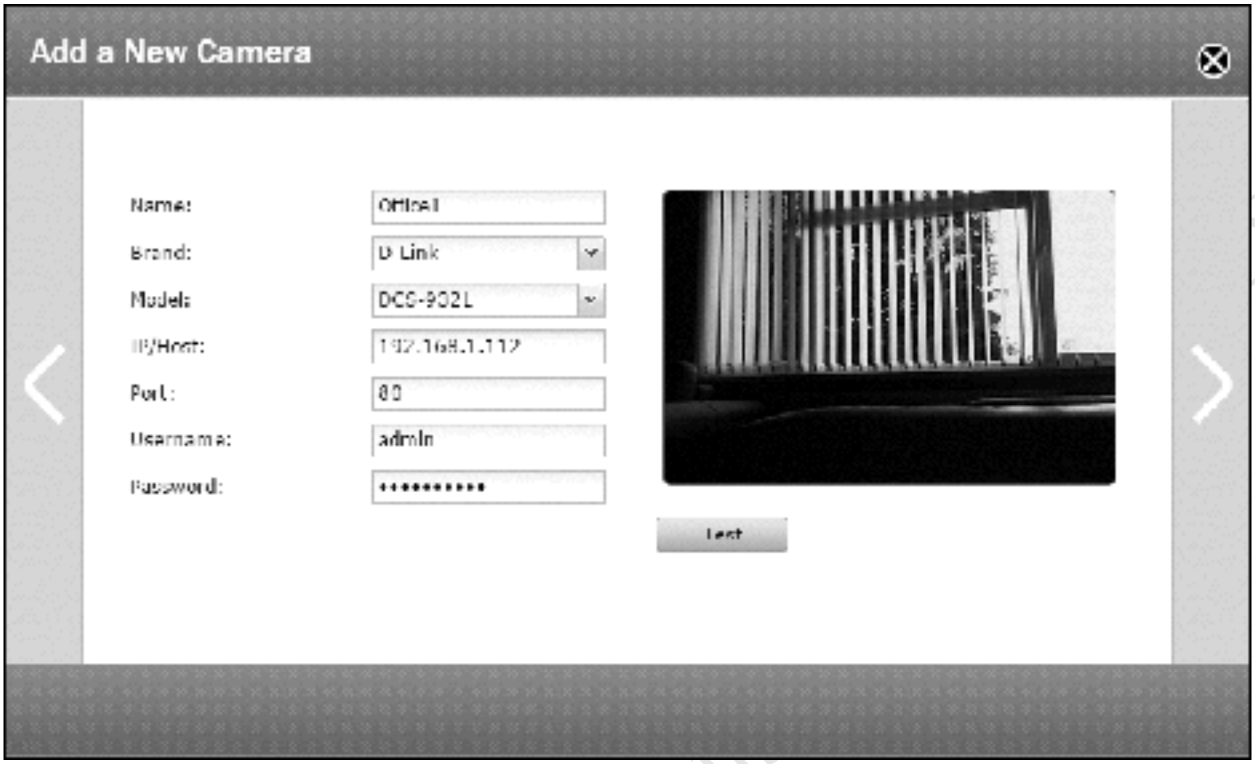
Would you like to perform a scan for available network cameras?

● Yes. Please search for all available cameras on my local network.

○ No. I would like to enter the camera information manually.

Figure 228: Scan for cameras

If the camera is not found, try again but choose the **No. I would like to enter the camera information manually** option. On the resultant panel, optionally give the camera a *Name* (e.g. its location) and choose the correct *Brand* and *Model* using the dropdowns; if the exact model is not listed, choose the closest available e.g. if you had an '*AcmeCam 402'* but only the '*AcmeCam 401'* is listed you could try that. If your camera is not listed at all, try using '*ONVIF*' for the brand; this is a generic standard for IP cameras and should work, although may only provide basic features. Specify the *IP/Host* address but leave the Port number as 80. Specify the *User Name* and *Password* for the camera – these are the ones that were used whilst setting up the camera and are unrelated to any user accounts on the NAS itself. Optionally, tick the **Enable recording on this camera** box. Click the **Test** button and if everything has been done correctly you will be able to see an image from the camera. Click the chevron to continue.



Name: Office1

Brand: D-Link

Model: DCS-932L

IP/Host: 192.168.1.112

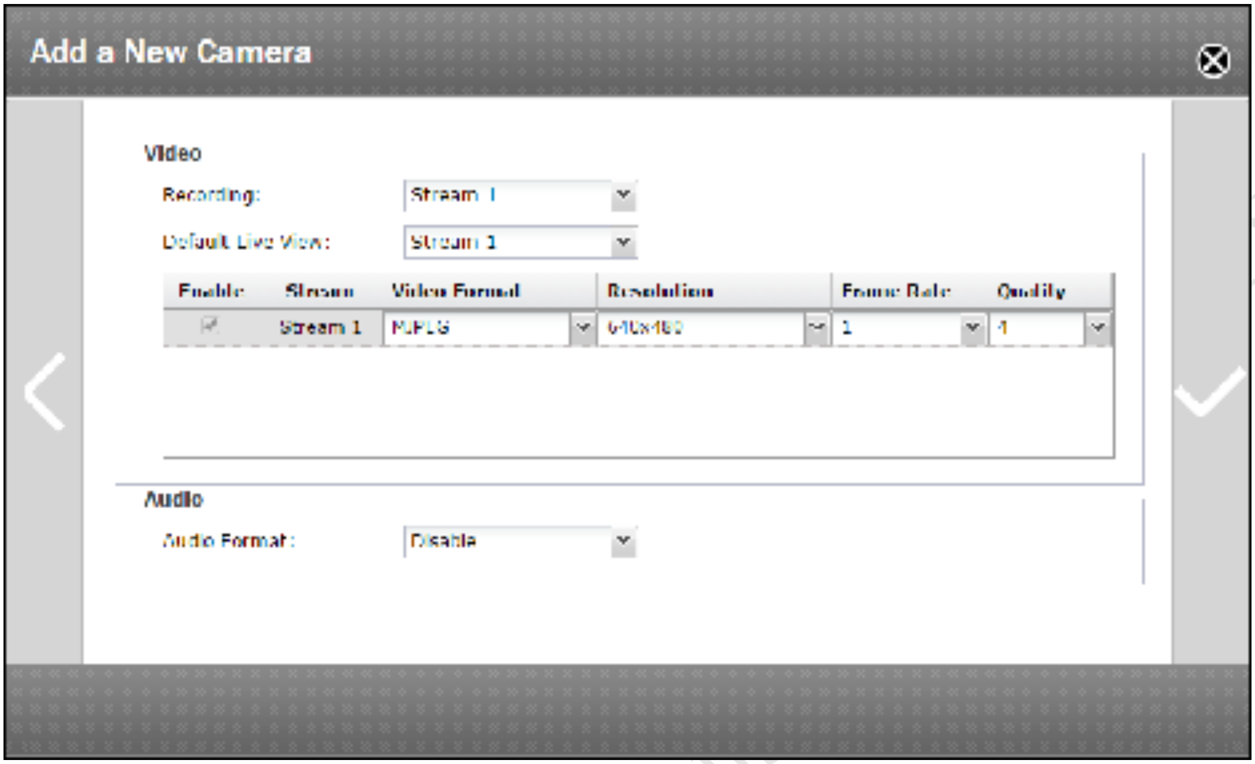
Port: 80

Username: admin

Password: **********

Figure 229: Add a new camera

The subsequent panel is for adjusting the video parameters of the camera, such as resolution, frame rate, recording and sound, with the options here depending on the camera plus your requirements. For instance, it is not uncommon to reduce the frame rate for some applications. Click the large **Tick** when complete.



Add a New Camera

Video

Recording: Stream 1

Default Live View: Stream 1

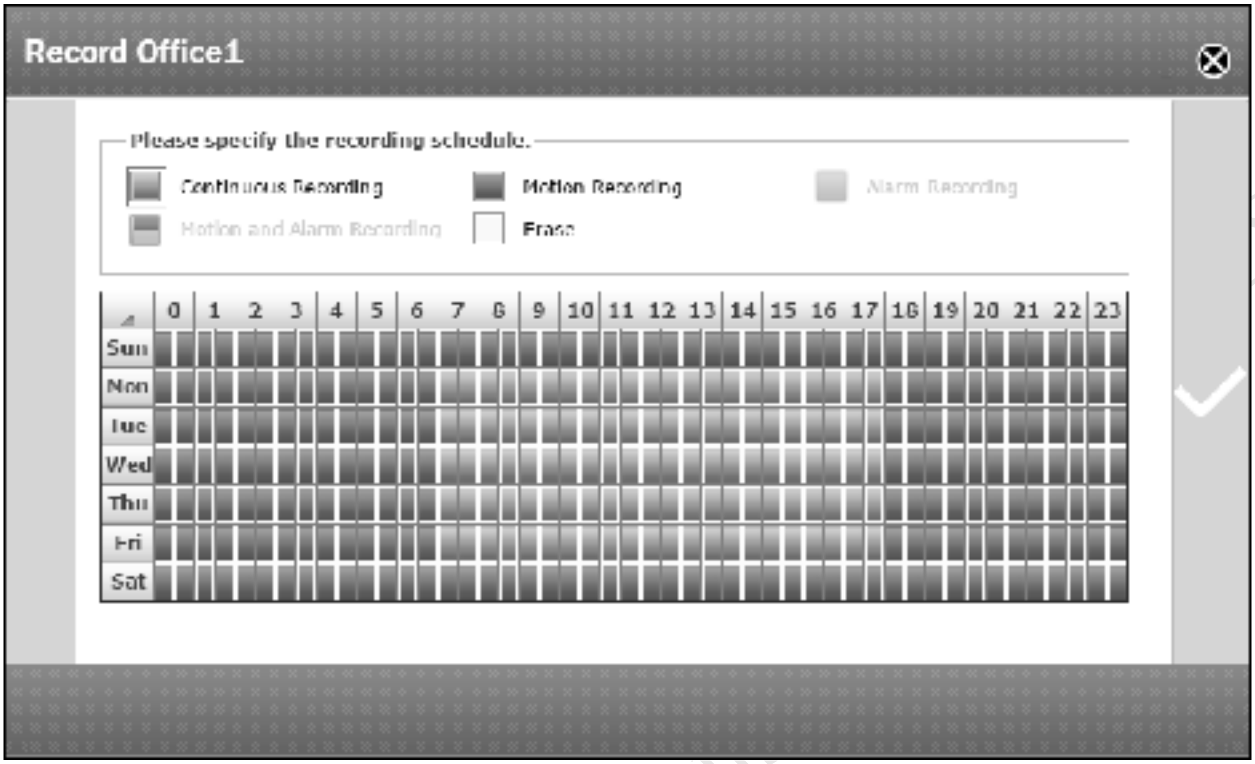
Enable	Stream	Video Format	Resolution	Frame Rate	Quality
☑	Stream 1	MJPEG	640x480	1	4

Audio

Audio Format: Disable

Figure 230: Video and audio settings

The camera will now be listed in the **Settings** tab and its output shown on the **Live View** tab. If your only requirement is to see live pictures, you are complete (although you may need to add any further cameras). If you wish to setup recording, click the **Record** button to display a scheduling screen. The options available depend on the camera i.e. Continuous Recording, Motion Recording, Alarm Recording, Motion and Alarm Recording. Select an option and drag the mouse cursor to ‘paint’ the schedule. When complete, click the large **Tick**.



Record Office1

Please specify the recording schedule.

▨ Continuous Recording ■ Motion Recording ▨ Alarm Recording
▨ Motion and Alarm Recording □ Erase

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Mon	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Tue	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Wed	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Thu	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Fri	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Sat	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨

Figure 231: Schedule settings

At this point the system is operational and the cameras can be controlled using the ‘remote control’ on the **Live View** tab. The features available depend upon the cameras; some, for instance, include zoom and panning. Recording and snapshots can be manually initiated. The layout of the screen can be changed to show more or less cameras. The output of one camera can be expanded to fill the entire screen.

Recordings can be viewed and managed from the **Playback** tab. There is a clickable timeline, to move quickly through recordings. There are search capabilities, for example, a camera can be searched for examples of motion detection during a particular timeframe.

All key events are logged e.g. when a camera starts and stops and who has been using the system.

Having finished using Surveillance Center, the user should Sign Out and close the browser window.

On HDMI-equipped models, Surveillance Center can work through ASUSTOR Portal (see 12.3 ASUSTOR Portal), enabling the output from cameras to be viewed on a screen connected to the NAS.

Licenses

Surveillance Center requires that each camera (also referred to as a ‘channel’) is licensed. ASUSTOR grant a free licence for a limited number of channels and to use more cameras it is necessary to purchase additional licences, which can be done directly from ASUSTOR. To manage licenses from within Surveillance Center, click **Settings** > **License Control**.

Privilege

Users of Surveillance Center are categorised as *Managers* or *Viewers*. All users can view the live and recorded output from the cameras, but Managers have additional capabilities, such as the ability to adjust settings and access the log files, and both roles can be customized to add/remove capabilities. To manage privileges from within Surveillance Center, click **Settings** > **Privilege**.

Notification

If Notifications have been enabled (see section 8.7 Notifications), then Surveillance Center can be configured to send notifications when significant events occur e.g. motion detected, storage full etc. This is controlled through **Settings** > **Notification**.

Maps

Maps can be created to show the location of the cameras. This is done by importing a graphic image of the area under surveillance and then marking where the cameras are.

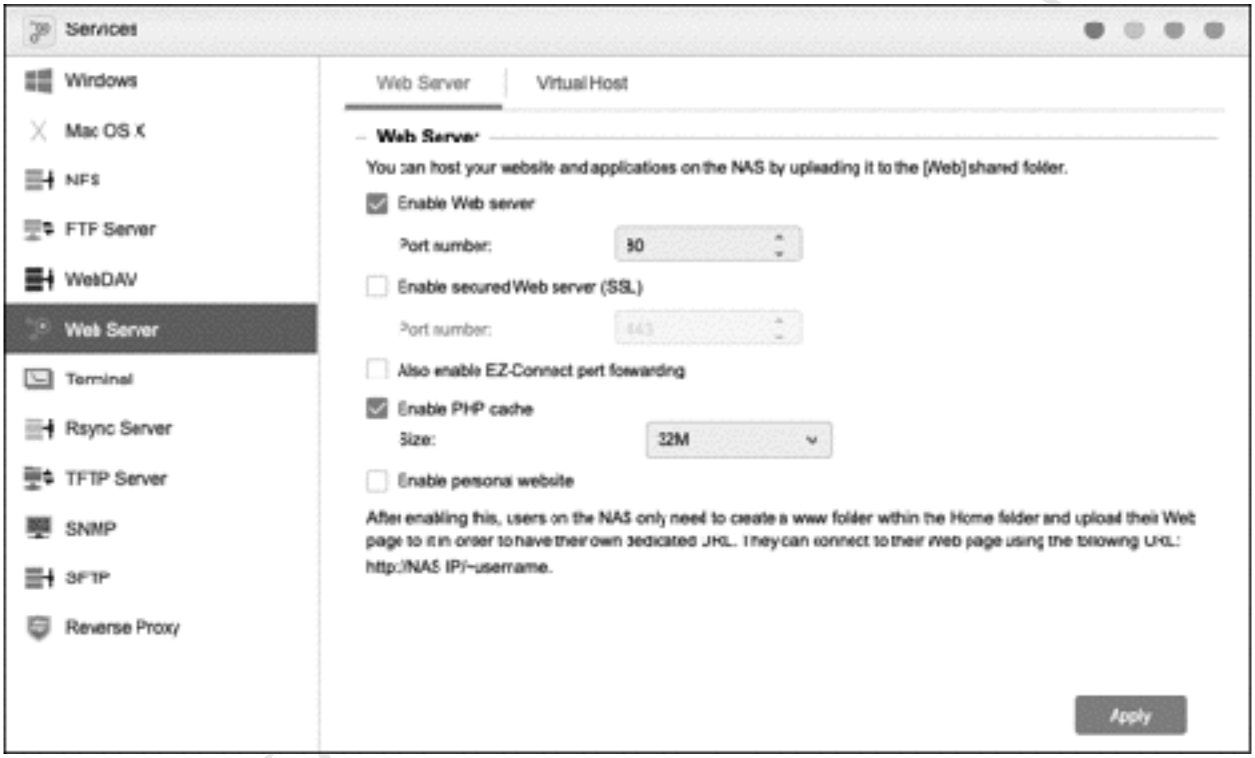
AiSecure

AiSecure is an app for iOS and Android devices which allows you to access Surveillance Center from your smartphone or tablet and can be downloaded through the appropriate app stores. During installation, specify the details of the server(s) being used with Surveillance Center, using the cloud address rather than the internal IP address of the server. This will enable the cameras to be viewed whilst away from the premises that are being monitored. Unless the HTTPS switch is set to the On position, the app cannot be used remotely.

12.11 Web Server

ADM includes the ability to host websites on the internet. Because of security and capacity implications and, given that dedicated web hosting services are available for free or low cost elsewhere, this may not be of interest to everyone. However, it may be of use in organizations that develop websites and wish to work on them in-house i.e. not accessible from outside the organization, as well as individuals wanting to learn about website and applications development. In this introduction, we will consider this to be the requirement.

The ADM interface is web-based, meaning that it clearly already includes a web server. To enable the facility for wider usage, go to **Preferences** > **Web Server** and on the **Web Server** tab tick the **Enable Web Server** box, followed by **Apply**. Note: depending on what apps have been installed, you may find that it is already enabled.



Web Server

You can host your website and applications on the NAS by uploading it to the [Web] shared folder.

☑ Enable Web server

Port number: 80

☐ Enable secured Web server (SSL)

Port number: 443

☐ Also enable EZ-Connect port forwarding

☑ Enable PHP cache

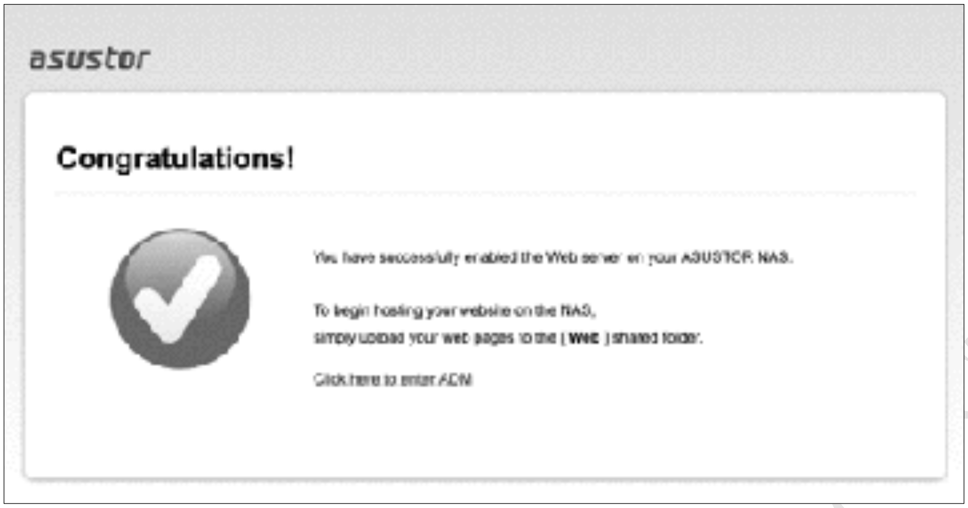
Size: 32M

☐ Enable personal website

After enabling this, users on the NAS only need to create a www folder within the Home folder and upload their Web page to it in order to have their own dedicated URL. They can connect to their web page using the following URL: http://NAS IP/~username.

Figure 232: Enabling Web Server

To confirm that Web Station is running correctly, use a browser to navigate to the IP address of the server. Rather than seeing the regular ADM screen, you should now be presented with the following:



Congratulations!

You have successfully enabled the Web server on your ASUSTOR NAS.

To begin hosting your website on the NAS,
simply upload your web pages to the [Web] shared folder.

Click here to enter ADM

Figure 233: Web Server operational

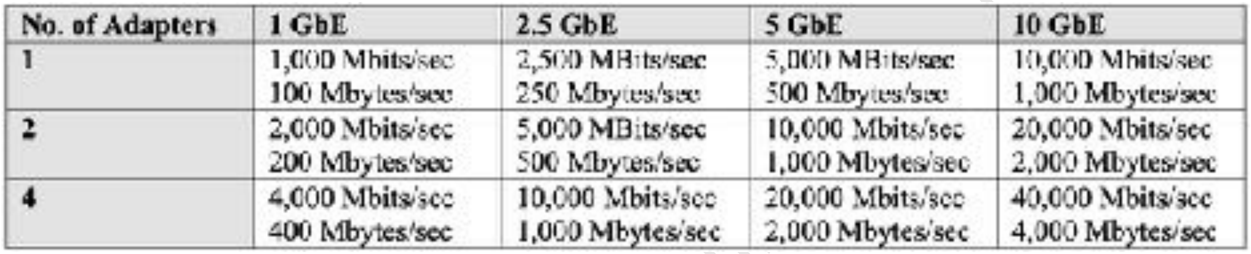
This shows that the default home page has been replaced. If you now place your own code (i.e. HTML and PHP components) in the shared *Web* folder, which was created automatically during the installation of ADM, this will become the home page for the server. To view the standard ADM screen, explicitly type the address of the server followed by *:8000*, for example 192.168.1.2:8000.

12.12 Link Aggregation

Some NAS units have multiple network adapters, which can be joined together using a technique called *Link Aggregation (*also known as trunking, teaming or bonding). This provides two benefits:

Fault tolerance – There are several types of failure that can occur: an adapter can fail; a port on a network switch can fail; an Ethernet cable can become unplugged. These failures can be mitigated against by aggregating the network adapters together, so that if one fails then another takes over automatically.

Load balancing (performance) – The maximum performance of a single gigabit Ethernet adapter is 1,000 Mbits/sec, equating to around 100 Mbytes/sec of data. If there are multiple users, and especially if there are activities such as video streaming or editing, this can be a bottleneck. However, by aggregating multiple adapters, network throughput can be increased e.g. two ports will can double it and four ports can quadruple it (assuming the NAS can actually deliver this amount of data from its disk drives). The following table shows the potential throughput for different numbers and type of network adapters when aggregated:



No. of Adapters	1 GbE	2.5 GbE	5 GbE	10 GbE
1	1,000 Mbits/sec 100 Mbytes/sec	2,500 MBits/sec 250 Mbytes/sec	5,000 MBits/sec 500 Mbytes/sec	10,000 Mbits/sec 1,000 Mbytes/sec
2	2,000 Mbits/sec 200 Mbytes/sec	5,000 MBits/sec 500 Mbytes/sec	10,000 Mbits/sec 1,000 Mbytes/sec	20,000 Mbits/sec 2,000 Mbytes/sec
4	4,000 Mbits/sec 400 Mbytes/sec	10,000 Mbits/sec 1,000 Mbytes/sec	20,000 Mbits/sec 2,000 Mbytes/sec	40,000 Mbits/sec 4,000 Mbytes/sec

Figure 234: Potential throughput with multiple network adapters

If the NAS was setup using the 1-Click method as described in 2 INSTALLATION OF ADM and the unit has multiple adapters, then it is possible that this was detected and they have been aggregated automatically. In this example, we will assume that this was not the case and they are being configured manually. The NAS has two adapters and both are wired to the main network switch.

Go into **Settings** > **Network** and click the **Network Interface** tab. Confirm that the network adapters are active and have picked up IP addresses:

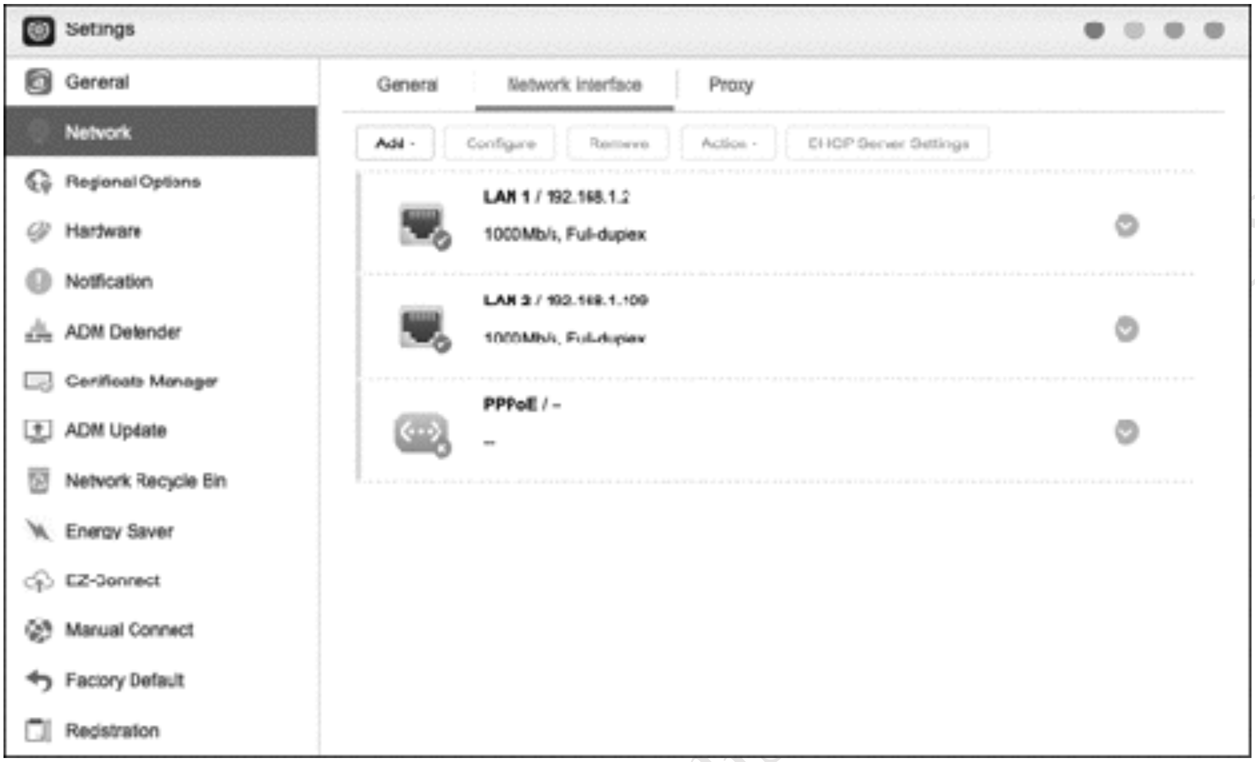
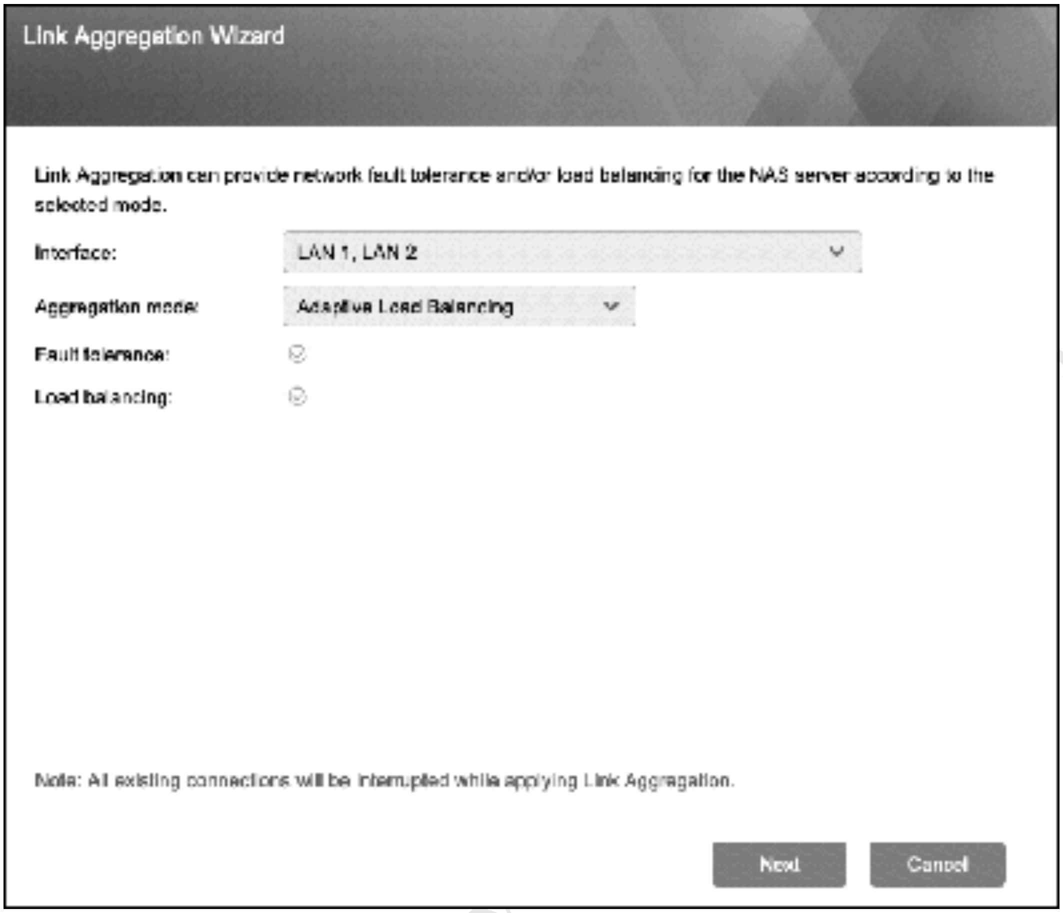


Figure 235: List of network adapters

Click the **Add** button and choose **Create Link Aggregation**. The *Interface* dropdown should have identified the network adapters, although may need reviewing if the NAS has more than two of them. The *Aggregation mode* dropdown lists the available modes, with the proviso that some of them require managed network switches that support IEEE 802.3ad Dynamic Link Aggregation. Underneath the dropdown are indicators that show whether the mode supports fault tolerance or load balancing. Typically, a small network might use *Round-Robin* (provides fault tolerance and load balancing), *Adaptive Load Balancing* (also provides both) or *Active-Backup* (provides fault tolerance only). In this example we have chosen *Adaptive Load Balancing*. Click **Next**:



Link Aggregation Wizard

Link Aggregation can provide network fault tolerance and/or load balancing for the NAS server according to the selected mode.

Interface: LAN 1, LAN 2

Aggregation mode: Adaptive Load Balancing

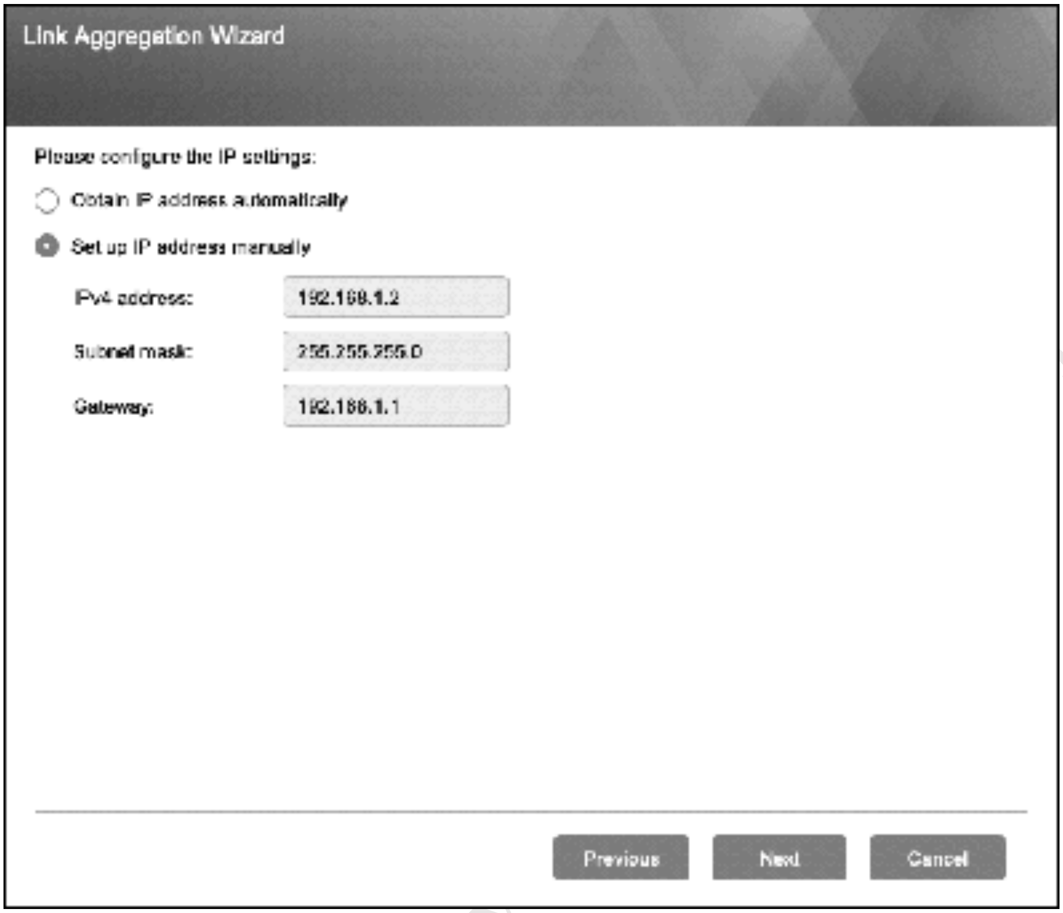
Fault tolerance: ✓

Load balancing: ✓

Note: All existing connections will be interrupted while applying Link Aggregation.

Figure 236: Choose the network adapters and aggregation mode

On the following panel, the IP settings need to be specified. Normally these should be unchanged from what was being used before, which in our case was a manual (static) IP address of 192.168.1.2, a subnet of 255.255.255.0 and the gateway (router) on 192.168.1.1. Click **Next**.



Please configure the IP settings:

○ Obtain IP address automatically

● Set up IP address manually

IPv4 address: 192.168.1.2

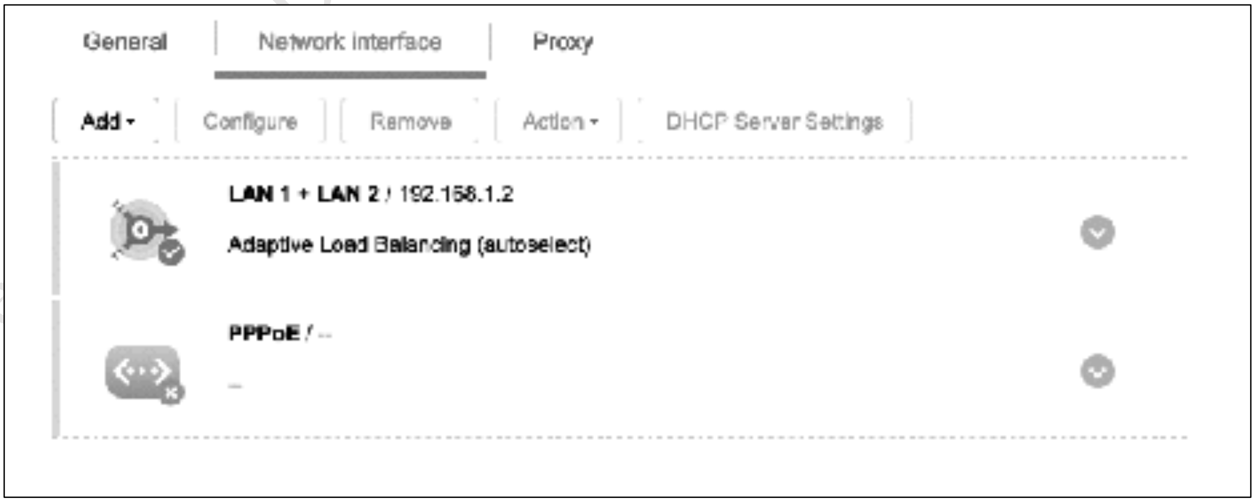
Subnet mask: 255.255.255.0

Gateway: 192.168.1.1

Figure 237: Configure the IP settings

A confirmation screen is shown – click **Finish**. There will be an interruption to services whilst the change takes effect and which may take up to a minute. It may then be necessary to refresh the browser, or login again to the server if the IP address has changed as a result.

Go back into **Settings** > **Network > Network Interface** and notice how the screen has been updated. Test the link aggregation by unplugging one of the network cables - the NAS should remain connected and accessible.



LAN 1 + LAN 2 / 192.168.1.2

Adaptive Load Balancing (autoselect)

PPPoE / --

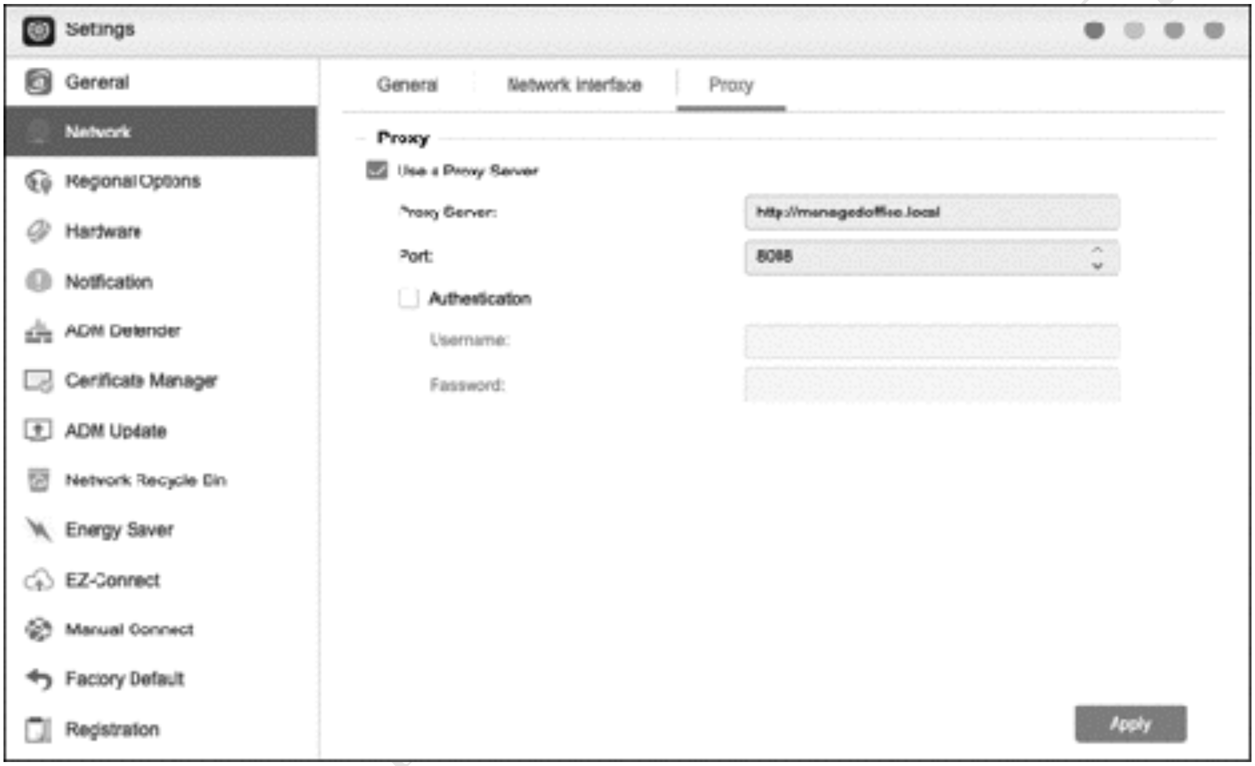
--

Figure 238: Network interface showing aggregated adapters

12.13 Connecting Via a Proxy Server

In most organizations 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 NAS needs to be configured appropriately.

Go into **Settings > Network** and click the **Proxy** tab. Tick the **Use a proxy server** box and enter the details of the proxy server, which will need to be obtained from the person or organization that administers the internet service. Usually this will consist of entering an address and port number but may also require authentication (logon) details. Click the **Apply** button.



Proxy

☑ Use a Proxy Server

Proxy Server: http://managedoffice.local

Port: 8088

□ Authentication

Username:

Password:

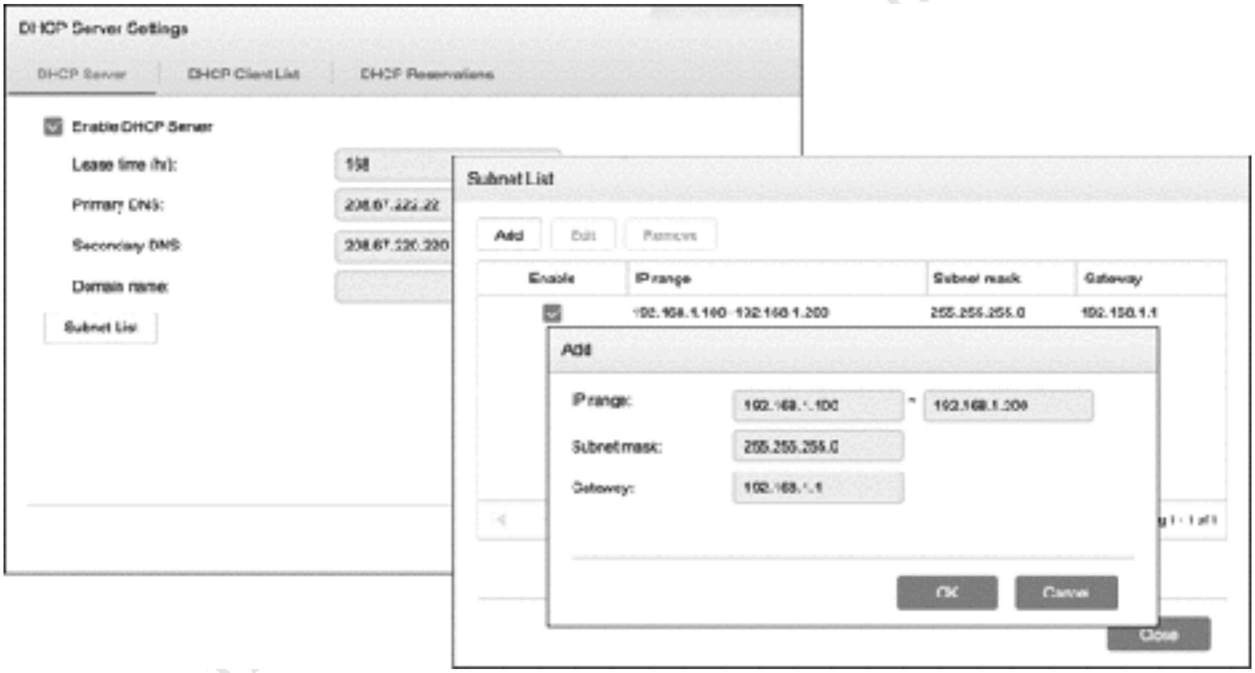
Figure 239: Example proxy server settings

12.14 DHCP Server

In most small business and home environments, the router that connects to the internet will also provide IP addresses for the computers and other devices via a built-in DHCP server. If so, ADM will use it, but if this is not the case then the NAS can be configured to act as a DHCP server itself.

Go into **Preferences** > **Network** > **Network Interface**. Highlight the first or only network adapter and click the **DHCP Server Settings** button, which should have become enabled. On the resultant panel, tick the **Enable DHCP Server** box. The default value for the *Lease time* is fine, but you could consider reducing it to 24 hours if you have mainly laptops and mobile devices. Enter the address of your **Primary DNS** server and optionally add the **Secondary DNS** server address. If you do not know the DNS addresses, login to your router and see what it is using, else consider using the OpenDNS server (208.67.222.222 and 208.67.220.220). Alternatively, go to *https://www.whatsmydns.net/dns* for the DNS details of many popular ISPs worldwide. There is no need to add a Domain name.

Click the **Subnet List** button and enter details of the Subnet list i.e. the range of IP addresses for the DHCP service. In this example the *Start IP address* is 192.168.1.100, the *End IP address* is 192.168.1.200, the *Netmask* is 255.255.255.0 (which it usually is in small networks) and the *Gateway* (i.e. Internet router) is on 192.168.1.1. Click **OK**.



☑ Enable DHCP Server

Lease time (hr): 168

Primary DNS: 208.67.222.22

Secondary DNS: 208.67.220.220

Domain name:

Subnet List

Enable	IP range	Subnet mask	Gateway
☑	192.168.1.100-192.168.1.200	255.255.255.0	192.168.1.1

IP range: 192.168.1.100 ~ 192.168.1.200

Subnet mask: 255.255.255.0

Gateway: 192.168.1.1

Figure 240: DHCP configuration

Returning to the original screen, the second tab is the *DHCP Client List*, which lists the devices that have received leases along with the details of those leases. The third tab is used for making IP reservations, which is the preferred method for handling devices such as printers and wireless access points in larger networks.

12.15 Resetting the Admin Password

If the admin password is forgotten, lost, or otherwise unavailable, it is possible to reset it back to the default i.e. user name *admin* with a password of *admin*. On the back of the NAS is a small reset hole, the position of which varies depending on the model. Insert a paper clip or similar object and press down for five seconds. All data on the NAS is retained. In addition to the system admin account and password being reset to the defaults, the following also occurs:

The HTTP and HTTPS ports used for connecting to ADM are reset to their respective default values of 8000 and 8001.

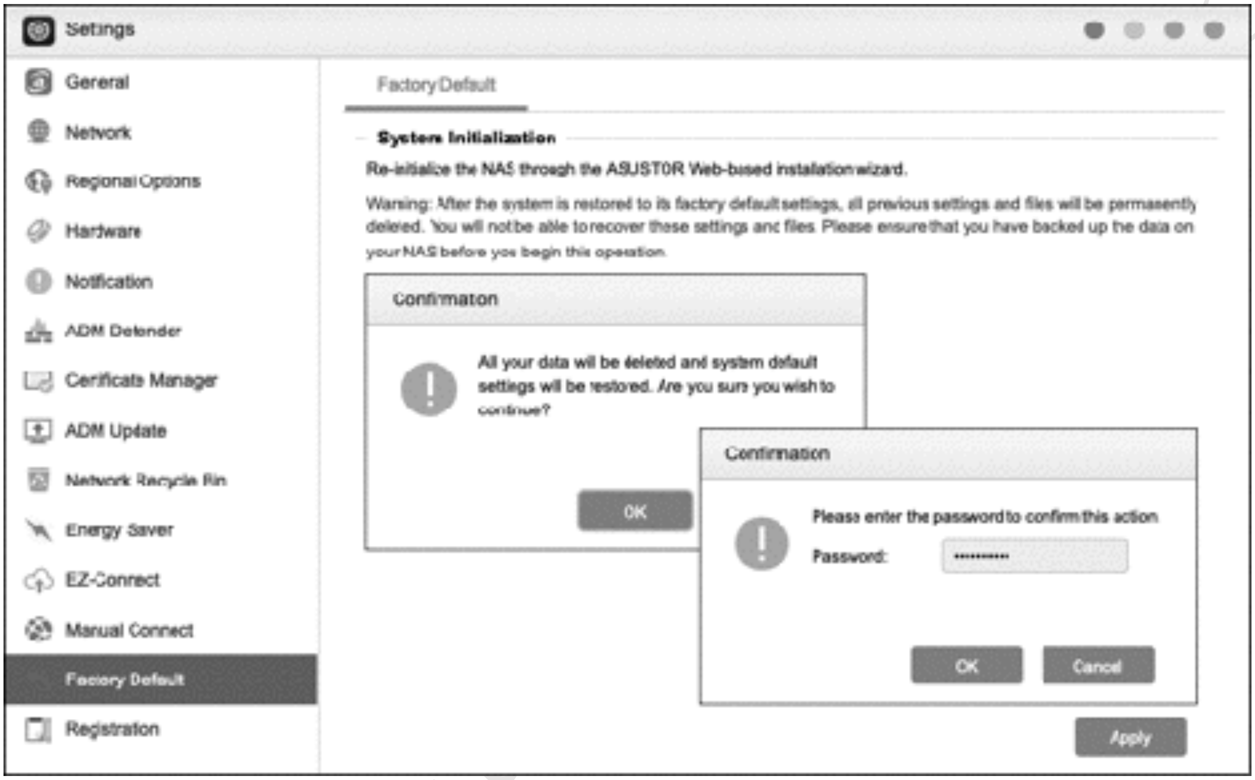
ADM Defender will revert to accepting all connections.

Network settings are reset to the default values. Use ASUSTOR Control Center to re-discover the NAS on the network.

Whilst it is clearly useful to be able to reset the NAS in this way, the security implications of this need to be considered as anyone could do it and gain access to the system and data. For instance, the NAS could be kept in a locked cabinet or equipment rack to prevent unauthorized physical access. Alternatively, or in addition, it is possible to disable the reset button altogether. To do so, go into **Settings** > **Hardware** and on the **System** tab tick the **Disable reset button** box, followed by **Apply**.

12.16 Preparing the NAS for Disposal

If the NAS is to be disposed of, first make sure that backups of all the important data have been taken, using the techniques described in section 7 BACKUPS. Then, go into **Preferences** > **Factory Default** and click **Apply**. A confirmation message is displayed; click **OK** to continue and then enter the administrative password. This will re-initialize the NAS using the web-based installation wizard. All the existing settings and data will be permanently deleted and the NAS will be restored to the original factory settings.



Re-initialize the NAS through the ASUSTOR Web-based installation wizard.

Warning: After the system is restored to its factory default settings, all previous settings and files will be permanently deleted. You will not be able to recover these settings and files. Please ensure that you have backed up the data on your NAS before you begin this operation.

All your data will be deleted and system default settings will be restored. Are you sure you wish to continue?

Please enter the password to confirm this action

Password: ••••••••••

Figure 241: System Initialization