

Lenovo Iomega NAS Setup Guide

Based on LifeLine 4.0

Nicholas Rushton, BA Hons.

Callisto Technology And Consultancy Services

First Edition © 2014

DO NOT COPY

First Edition. Updated 5th May 2014.

Copyright © Nicholas Rushton, 2014

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

All rights reserved. No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form, or by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior permission of the author. Any person who does any unauthorised act in relation to this publication may be left liable to criminal prosecution and civil claims for damages. An exception is granted in that up to 500 words in total may be quoted for the purpose of review. The information in this publication is provided without warranty or liability and it is up to the reader to determine its suitability and applicability to their own requirements. This book and its author are unconnected with LenovoEMC and this is an independently produced publication.

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

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

DO NOT COPY

Contents

1 Preparation	6
1.1 Choice Of Model.....	6
1.2 Diskless Models	7
1.3 Location	8
1.4 Electrical Considerations	9
1.5 Local Infrastructure.....	10
1.6 Computers And Devices	12
2 Initial Setup.....	13
2.1 Managing the Server	14
2.2 Method One – Using a Browser.....	15
2.3 Method Two – Using the LenovoEMC Storage Connector.....	17
2.4 Overview of Main Screen	19
2.5 Checking the Date and Time.....	21
2.6 Changing the Name of the Device	22
2.7 Changing the IP Address of the Device	23
2.8 Enable Security	25
3 Hardware and Power Management	27
3.1 Energy Saving.....	28
3.2 Uninterruptible Power Supply	29
4 Storage & RAID	30
4.1 How to Change the RAID Level.....	31
5 User Accounts.....	33
5.1 Creating a User	34
5.2 Modifying or Deleting a User	35
5.3 Groups.....	36
5.4 Quotas	39
6 Shared Folders	40
6.1 Creating a New Shared Folder.....	41
6.2 Granting Access to a Shared Folder.....	43
7 Accessing the Server.....	45
7.1 Using A Browser.....	46
7.2 Using Windows Explorer.....	49
7.3 Accessing A Shared Folder using the Run command	50
7.4 Mapping The Drives Manually	51
7.5 Using A Batch File.....	53
7.6 Connecting a Mac	56
8 Multimedia & Streaming	61
8.1 Media Server.....	62
8.2 Settings affecting Media Server.....	64

8.3 Managing Twonky.....	65
8.4 iTunes.....	66
8.5 Picture Transfer.....	67
9 Personal Cloud and Remote Working.....	68
9.1 Setting up Personal Cloud.....	69
10 Backups.....	72
10.1 Backing Up the Server to an External USB Drive.....	73
10.2 Restoring Files to the Server.....	77
10.3 Cloud-based Backup Services.....	78
10.4 Backing up the Server Configuration.....	79
10.5 Backing up Windows 7 Computers to the Server.....	80
10.6 Backing up Windows 8 Computers to the Server.....	85
10.7 Time Machine for Mac Users.....	88
11 Printing.....	89
12 Connecting iPads & Other Mobile Devices.....	90
12.1 LenovoEMC Link.....	90
12.2 File Browser.....	93
12.4 Using a Chromebook.....	94
13 Social Media.....	95
13.1 YouTube.....	96
13.2 Facebook.....	97
13.3 Flickr.....	98
14 Housekeeping & Reporting.....	99
14.1 System Status Screen.....	100
14.2 The Event Log.....	101
14.3 Checking The Health Of The Disks.....	102
14.4 Setting Up Automatic Email Notifications.....	104
14.5 Updating the LifeLine Firmware.....	105
15 Miscellaneous Topics.....	108
15.1 Application Manager.....	108
15.2 Feature Selection.....	110
15.3 Customizing the Home Page.....	111
Appendix A: Internet Access Using a Proxy Server.....	113
Appendix B: Reset NAS or Prepare For Disposal.....	114

Introduction

Lenovo are one of the world's largest computer manufacturers and their Network Attached Storage (NAS) systems are extremely popular and rightly so. At the heart of them is the LifeLine firmware (operating system), which gives them their capabilities and power. Whether it is the storage and sharing of information, the streaming of videos, music and photos to computers and smart devices, or the ability to have a private cloud that allows access to information from anywhere, a Lenovo NAS with LifeLine can do it all with aplomb. But this power and flexibility comes at a price: setting up a system for the very first time can seem a daunting prospect for someone who has not done so before. Even when good documentation is available from the manufacturer, it is often based on a run-through of features rather than worked, practical examples of how to go about it in the real world. This guide, based around the latest version of LifeLine and with copious illustrations and easy-to-follow instructions, will take you through the process from start to finish and help ensure that your home or small business 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.

Chapter 1 is concerned with preparation and provides some useful background information about getting ready. Chapter 2 covers the initial setup and configuration of the LifeLine firmware and logging in for the first time, with Chapter 3 describing how to customize the hardware and power options of the server. Chapter 4 is about storage and explains what RAID is. Chapter 5 discusses the creation of user accounts and groups and Chapter 6 describes how to create shared folders. Chapter 7 covers the various methods for connecting PCs and Macs to the server in order to access data. Chapter 8 covers the multimedia and streaming options available in LifeLine. Chapter 9 details how to access data remotely using Personal Cloud. Chapter 10 is all about backups whilst Chapter 11 covers printing. Chapter 12 concentrates on connecting iPads and other mobile devices. Chapter 13 describes how to integrate the server with popular social media sites, whilst Chapter 14 is about housekeeping and reporting to ensure the server remains in good health. Finally, Chapter 15 discusses additional miscellaneous topics to help you get more out of your server.

Some terminology: the terms NAS, server, Lenovo and network storage device are used interchangeably throughout this guide and all mean the same thing.

The guide is supported with a growing website at: <http://www.serverinstallationguides.co.uk> - be sure to check it out on a regular basis for any updates and additional material. You should also familiarise yourself with the excellent support and training material on the Lenovo website plus the built-in help system of LifeLine to get the most out of your NAS.

1 Preparation

1.1 Choice Of Model

Currently, Lenovo offer more than a dozen different models of their network storage devices, designed to cater for everyone from home users through to the largest of enterprises. The models vary according to form factor, number of hard drives that can be used, performance and ultimately price and fall into three broad categories:

Consumer – the models of most relevance to home and small business users are branded Lenovo Iomega and include: the EZ Media & Backup Center; the ix2; the ix4-300D. These are available with differing amounts of disk storage. Prior to the formation of LenovoEMC these models were branded Iomega StorCenter and had similar model names. As long as they run LifeLine 4, this guide is equally applicable to the Iomega models.

Business – these models are branded LenovoEMC and include the px2-300d, px4-300d, px4-400d and px6-300d. These use different processors than the consumer models and are aimed at larger businesses.

Enterprise – as the name suggests, these are aimed at the largest organizations and are more powerful machines, designed to be mounted in racks rather than sit on top of desks or cupboards. Examples include the px4-400r, px4-300r, px12-400r and px12-450r.

What all of these products have in common is the LifeLine operating system. Although the focus in this guide is on home and small business users, some of the information may also be of value to users of larger devices.

Choosing the right model can be confusing as there is some 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.

1.2 Diskless Models

Most of the Lenovo consumer models are supplied with hard drives already installed in them, but it is also possible to buy diskless units. The idea is that the customer buys the drives separately and installs them, which is actually quite easy to do. This approach suits some customers as it offers more choice and flexibility; however, it is not necessarily the case that any drive or combination of drives can be installed. Lenovo have a support website at <https://lenovo-na-en.custhelp.com/> that gives a list of supported drives for each particular model. As might be expected, the big brand names (Western Digital, Seagate, Hitachi, Toshiba) feature. One important consideration is that for models with multiple drive bays, all of the hard drives should be identical i.e. same brand, model, capacity, speed.

One thing to note is that some people report difficulties when trying to use their own drives. It is recommended that most home and small business users stick with units that come with the storage pre-installed so as to avoid these problems.

DO NOT COPY

1.3 Location

The network storage unit should be attached to the physical network via a Gigabit Ethernet connection, for example by plugging it directly into the router. It should be placed away from direct sunlight and any source of heat, such as a radiator. Avoid locations that are wet or damp. As little physical access is required the unit can be located out of sight and reach, for instance in a cupboard or a locked room or generally out of reach. Most models generate very little noise and can usually be operated in an office or family room without too much disruption.

DO NOT COPY

1.4 Electrical Considerations

It is possible that data loss and damage can occur if the electrical mains power fails whilst the network storage unit is running. The best way to mitigate against this is to use an intelligent UPS (Uninterruptible Power Supply) with it; in the event of power problems this will enable it to continue operating normally for a short period and then to shut it down in an orderly manner if necessary. Most popular brands work with Lenovo e.g. APC, CyberPower, Powercom. In a business environment, the use of an UPS should be considered mandatory.

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

DO NOT COPY

1.5 Local Infrastructure

The term infrastructure is used here to describe the physical network, i.e. the boxes and wires that connect everything together and to the outside world. In a home environment, this is typically an all-in-one wireless internet router. In a business environment, it may be a router connected to switch and to one or more wireless access points, depending on how many devices need to be connected:

TYPICAL HOME INFRASTRUCTURE

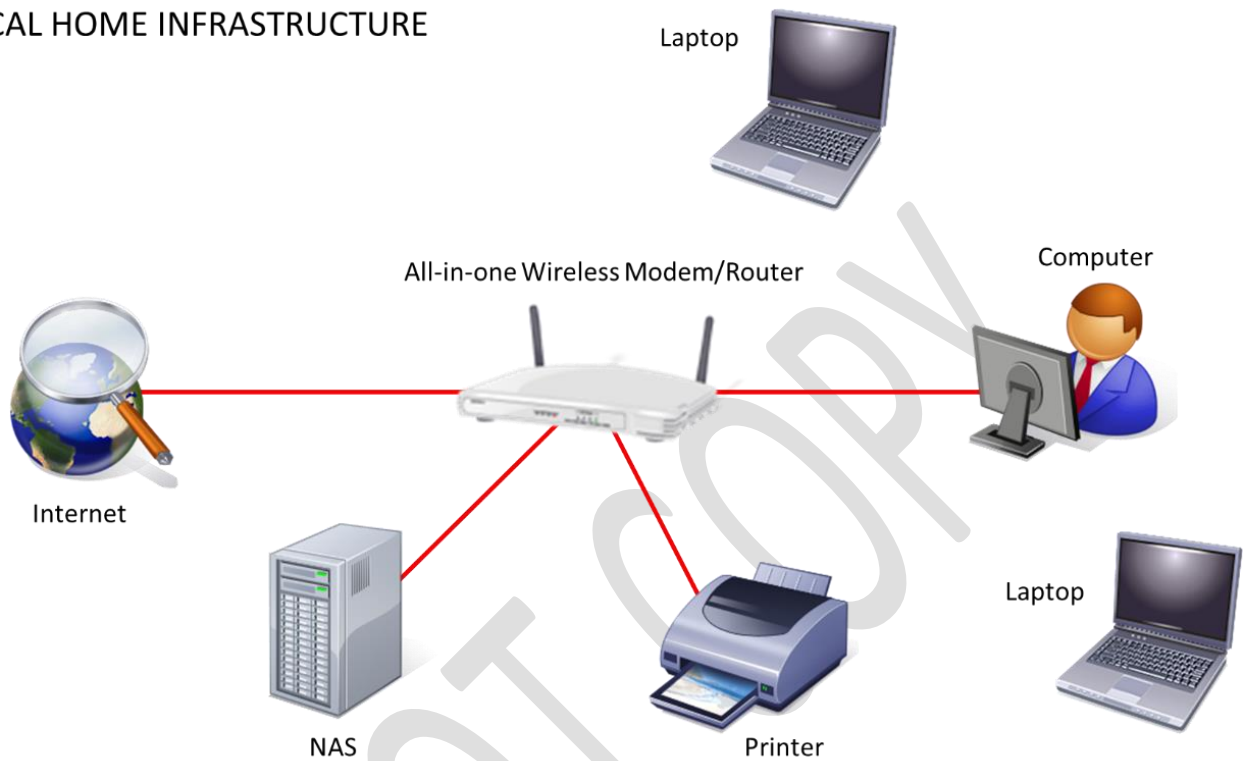


Figure 1: Typical Home Infrastructure

TYPICAL SMALL BUSINESS INFRASTRUCTURE

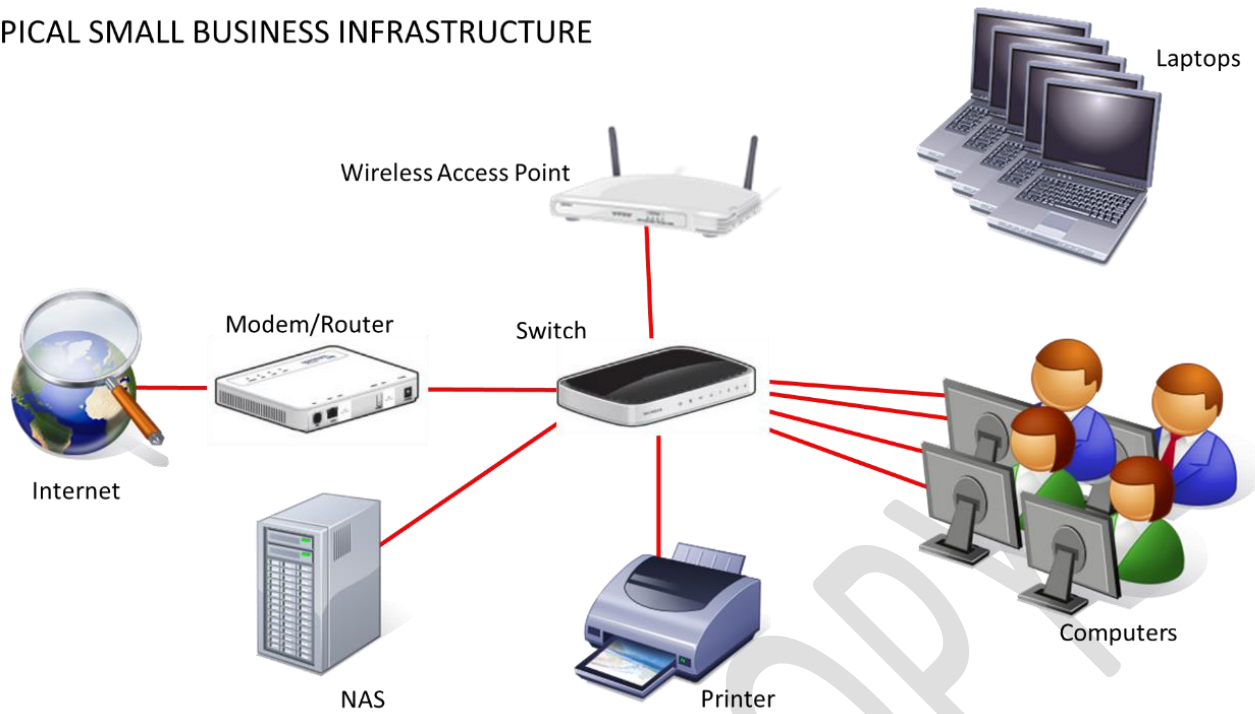


Figure 2: Typical Small Business Infrastructure

There are a number of principles that can usefully be followed here. Firstly, use wired connections whenever possible as performance is so much better than wireless. Secondly, for wireless devices such as laptops, make sure they operate at 801.11n or 801.11ac specification. Thirdly, if you are a home user consider upgrading the router. Many ISPs (Internet Service Providers) supply relatively low-cost models, often free of charge when you sign-up with them. Many of these are of average quality and spending money on professional or prosumer (“professional consumer”) routers and switches will usually give better performance and reliability.

1.6 Computers And Devices

Just about any modern computer can be used with the server. The computers can be running any mixture of Windows 7, Windows 8, Windows Vista or Windows XP. Home or Professional versions of Windows are equally suitable. Apple Mac computers running OS X 10.4 or better can be connected, as can Linux PCs (but the latter are not specifically discussed in this guide). Devices running iOS (iPad, iPhone) or Android (tablets and Smartphones) can be connected, as can many smart televisions and gaming boxes. However, Chromebooks can only be connected in a very limited sense.

DO NOT COPY

2 Initial Setup

Unlike with some brands of NAS, many Lenovo network storage units basically work straight out of the box. Connect it to your network router with an Ethernet cable, plug in the power supply, switch it on (some models power up automatically when you connect power), give it ten minutes to settle and it will be ready for use. It will appear as a device on your network with its network name corresponding to the model number, along with a selection of ready-to-use shared folders. This is what is shown below; in this instance the NAS is called *IX2* and the shared folders are visible (*Backups*, *Documents*, *Movies*, *Music*, *Pictures* and *SharedMedia*):

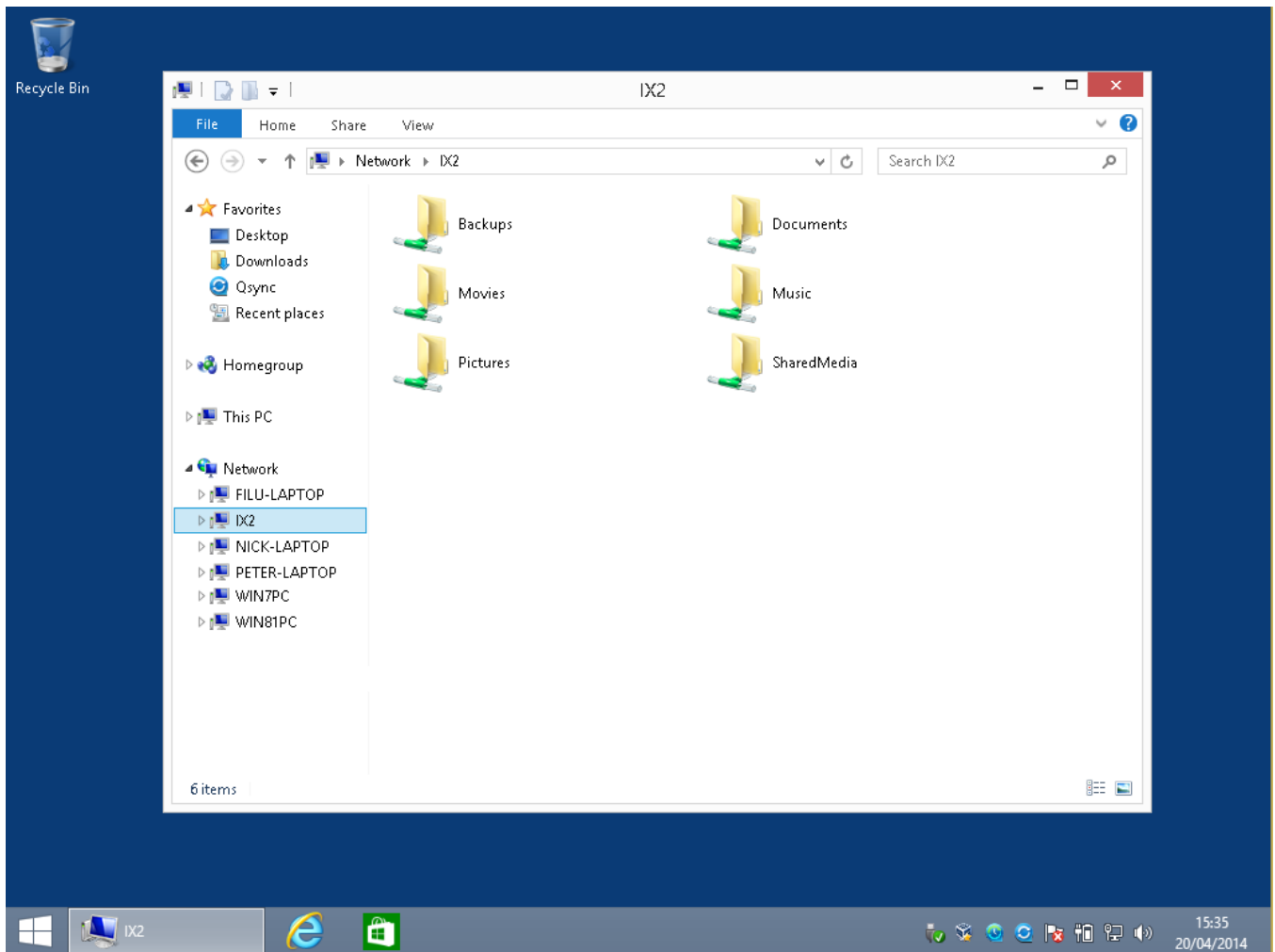


Figure 3: Viewing the default shared folders

Given that this is the case, you might well be asking: so what else needs to be done? The answer is quite a bit, as there are several configurations options that need to be tweaked plus several of the most useful features of the server will not yet be working, including backups and remote access. Nor is there any security whatsoever, and if you are concerned at the sound of that then you are probably right to be so. In short, Lenovo and LifeLine give you a great head start but additional effort is required to make the most of your system.

2.1 Managing the Server

There are two main ways to manage the server. The first method uses an internet browser and hence can be done using a PC, a Mac, an iPad or any other device that has a modern, capable browser. The second method uses a piece of software called the *Lenovo EMC Storage Connector*, which is only available for Windows PCs.

DO NOT COPY

2.2 Method One – Using a Browser

Enter an address of *http://setup.lenovoemc.com* into the browser's address bar. The following screen is displayed:

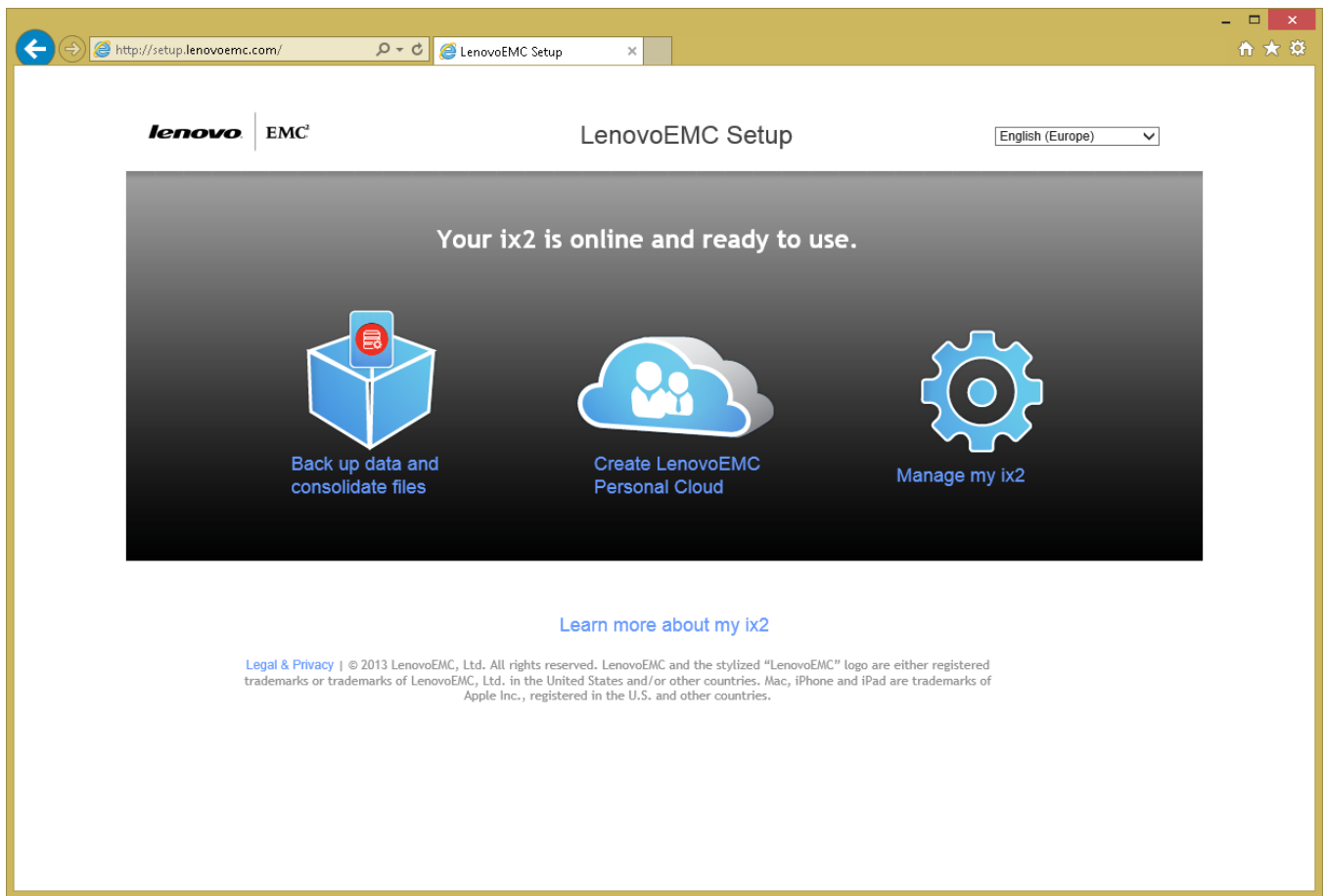


Figure 4: The LenovoEMC Setup screen

Although the first two icons might look interesting, resist the temptation and instead click on the large gearwheel icon that reads **Manage my <model name>** (in the above example it is *Manage my ix2*). The following screen is displayed:

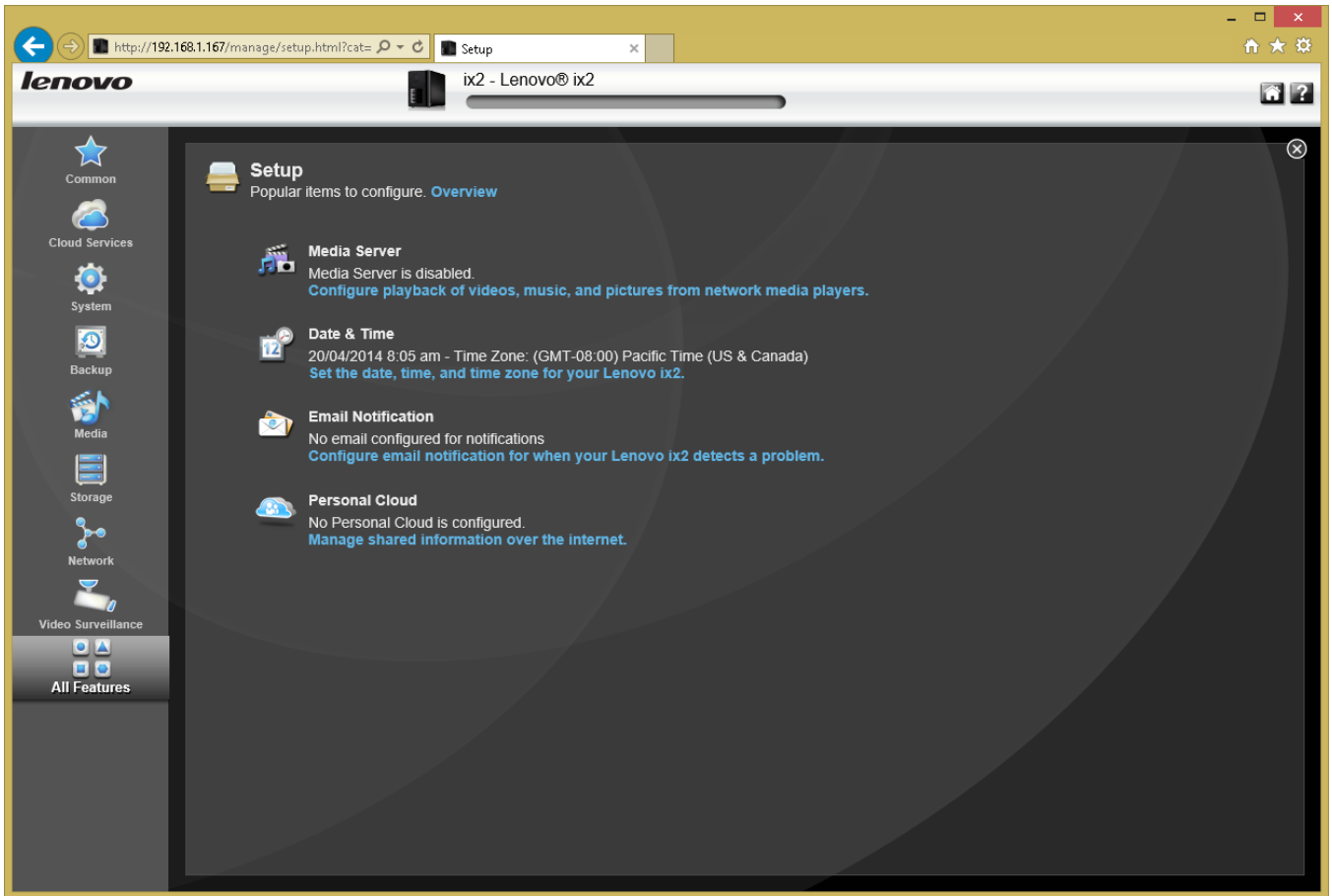


Figure 5: First screen seen after startup

If you are seeing this screen or similar you can go to section [2.4 Overview of Main Screen](#).

2.3 Method Two – Using the LenovoEMC Storage Connector

Download the latest version of the LenovoEMC Storage Connector software from the Lenovo website (note: if you have a recent Lenovo desktop computer or laptop it may even have been pre-installed). Install and run it on a Windows computer. If you receive a message from the firewall on your computer, allow access for the Storage Connector. After a few seconds it should find (discover) the NAS unit. Click the **Configure features** button:



Figure 6: LenovoEMC Storage Connector

A screen like the following should be displayed:

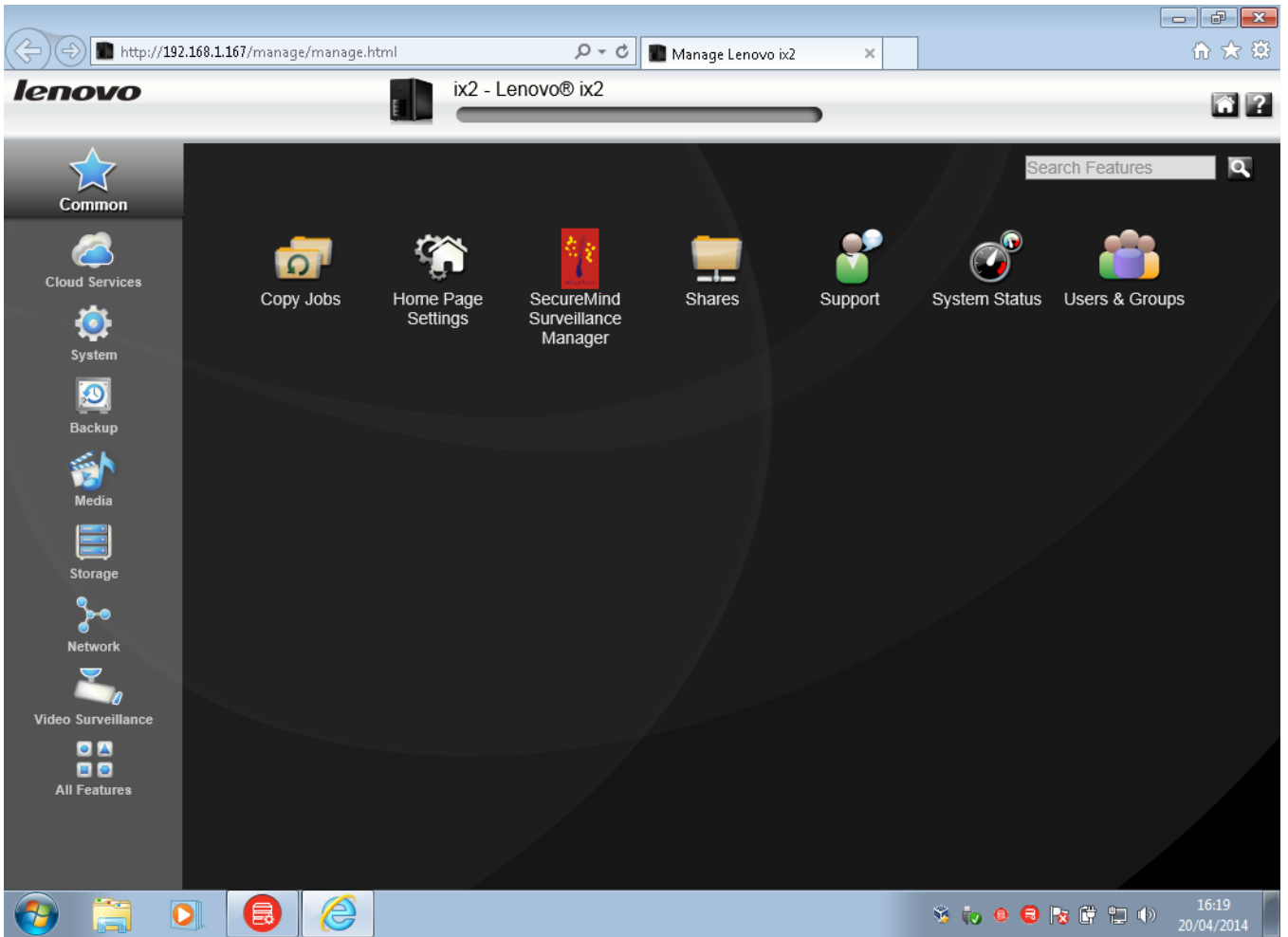


Figure 7: Common items section in LifeLine here

If you are seeing the above continue to the next section.

2.4 Overview of Main Screen

The standard LifeLine screen is divided into two panels. The left-hand side is a narrow panel containing a number of category icons and can be thought of as a sort of menu. Clicking on one of these icons causes a selection of additional icons to be displayed in the larger right-hand panel; these icons can be thought of as a type of sub-menu and clicking on one enables a particular feature to be managed.

On the left-hand side, click the **All Features** icon to display the entire collection of icons. As they are sorted alphabetically, this can be the most efficient way of finding something if you do not know what category it is in:

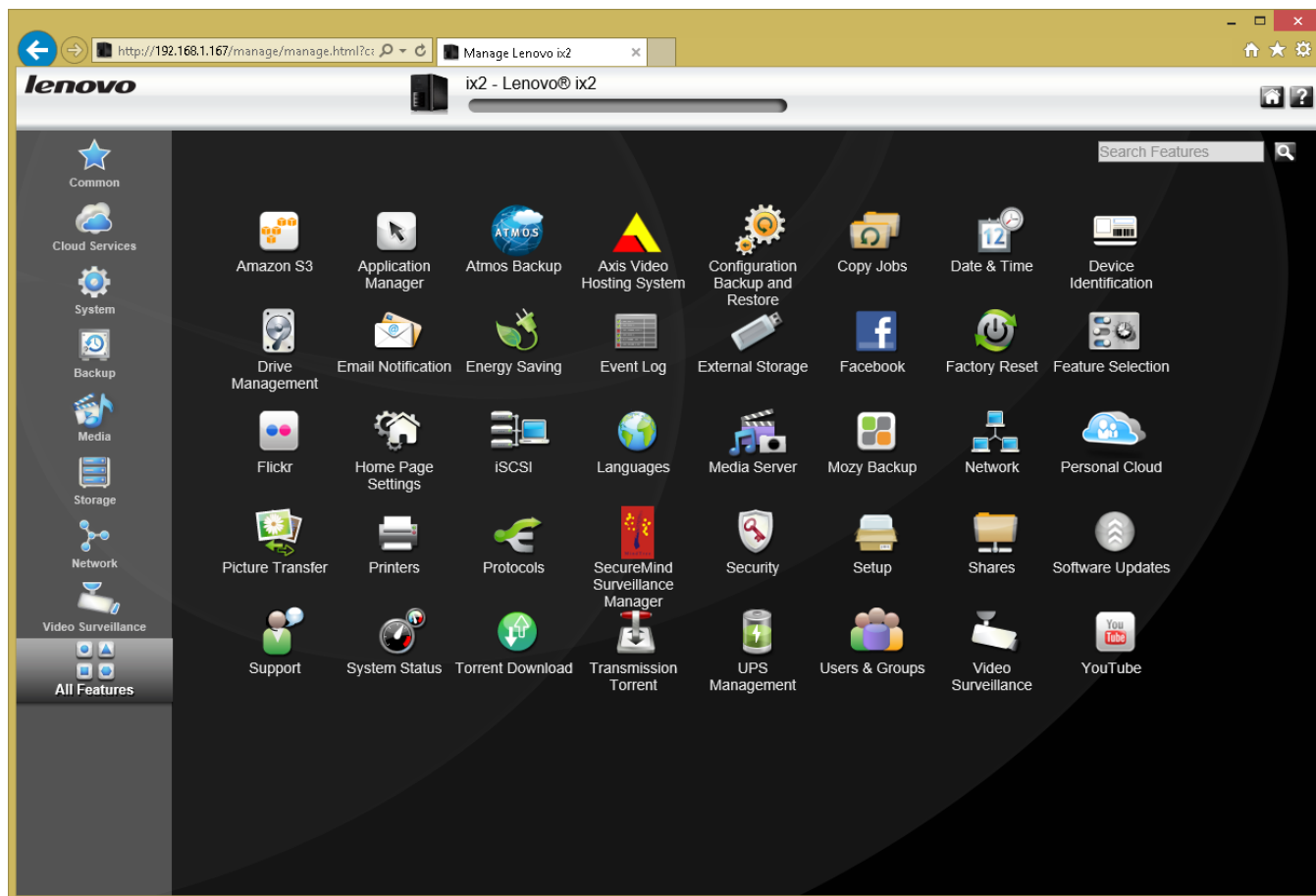
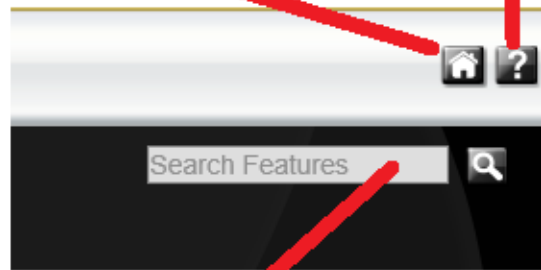


Figure 8: All Features screen in LifeLine

In the top-right corner of the screen are several icons. One of these is an online link to the manual for your particular model. The second allows you to search the help pages built-in to the local system and provides links to the relevant icons for invoking the appropriate function. The third icon takes you to the Home Page – this can be thought of a sort of private website running on the server and will be discussed later on:

Home Page Online Manual

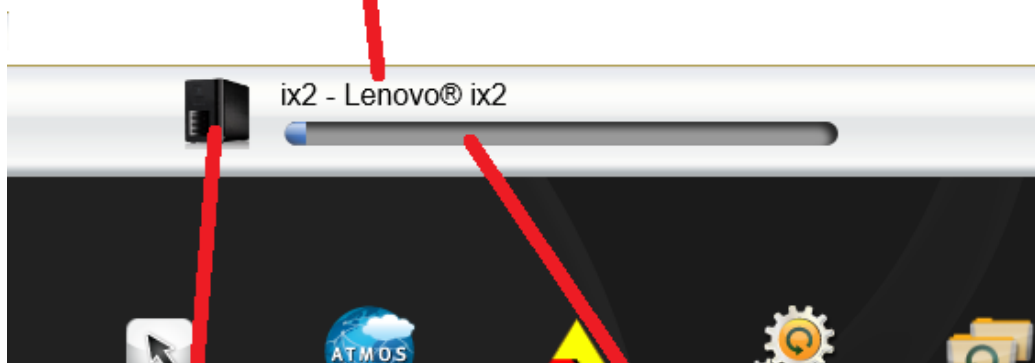


Search the built-in help system

Figure 9: Icons within screen

At the top of the screen, in the middle, is the following section:

Server name & model



Clickable link to System Status

Disk usage indicator

Figure 10: Status within screen

This shows the server name and model; in this case, we have a Lenovo ix2 and its name is *ix2* (although we are shortly going to change the name). To the left of this is a small picture of the server – this is an accurate picture as the LifeLine firmware is intelligent enough to customize itself to reflect the actual model you have i.e. references will generally be to the specific model rather than generic. The picture is actually a clickable icon, which takes you to the *System Status* page (again, we will explore this later). Finally there is a thermometer-style indicator of the disk usage; in this example, only a small amount of the disk storage space is currently used.

2.5 Checking the Date and Time

Start off by checking the date, time and time zone as they may be incorrect. For instance, a new unit will commonly default to Pacific Time, which is not much good if you are in, say, London or New York. Click the **Date & Time** icon in the **System** group and make the appropriate changes. Having done so, click the **Apply** button:

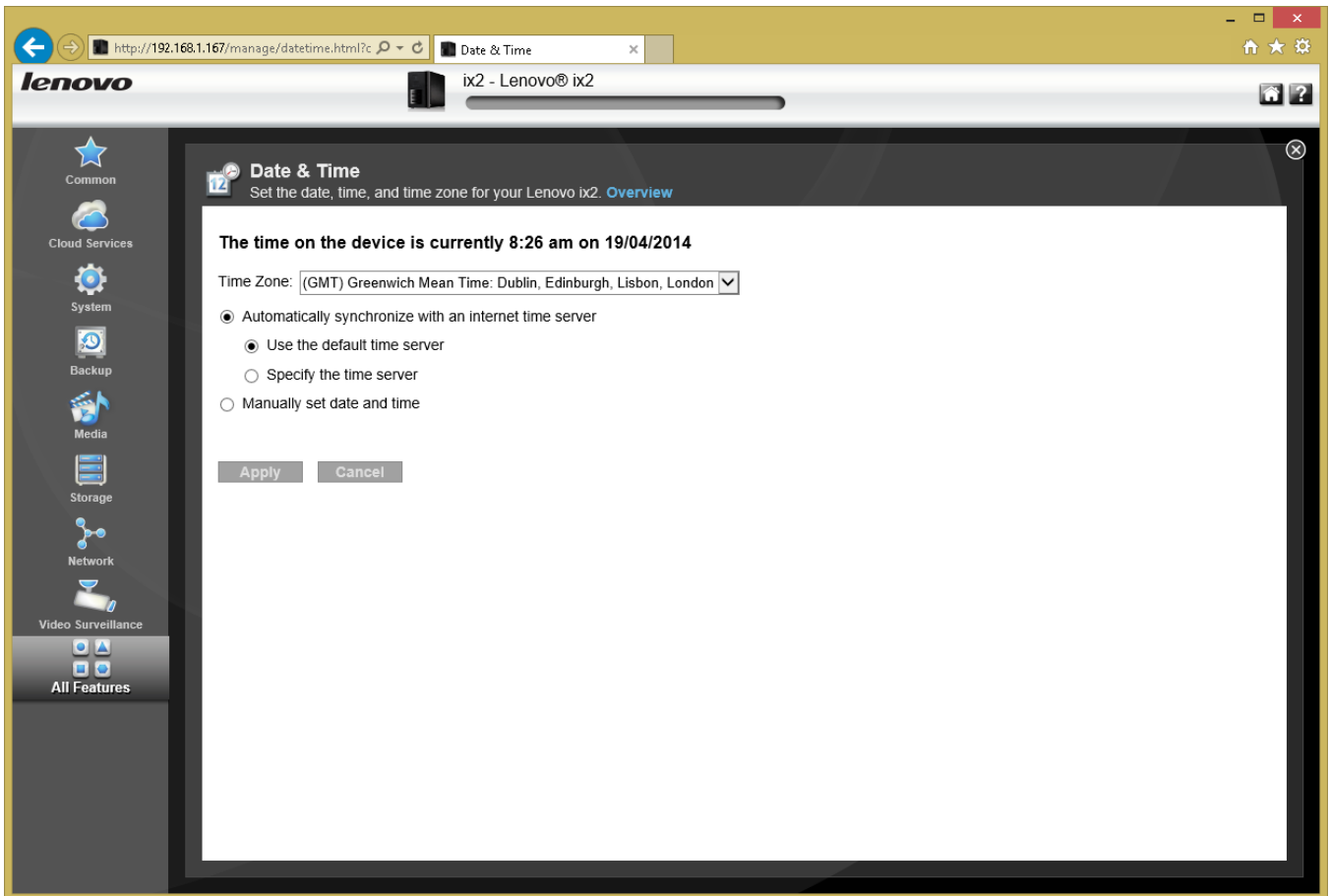


Figure 11: Setting the Date and Time

2.6 Changing the Name of the Device

By default, the name of the device on the network corresponds to the model type e.g. if you have an ix2 it will be displayed within Windows Explorer as *ix2* (see [2 Initial Setup](#) for a screenshot of this). This can be confusing, as some of the model names are a bit abstract and for this reason it is suggested that the name is changed to something more meaningful. For instance, its purpose is to be a server so why not simply call it *server*?

To change the name click on the **Device Identification** icon in the **System** group:

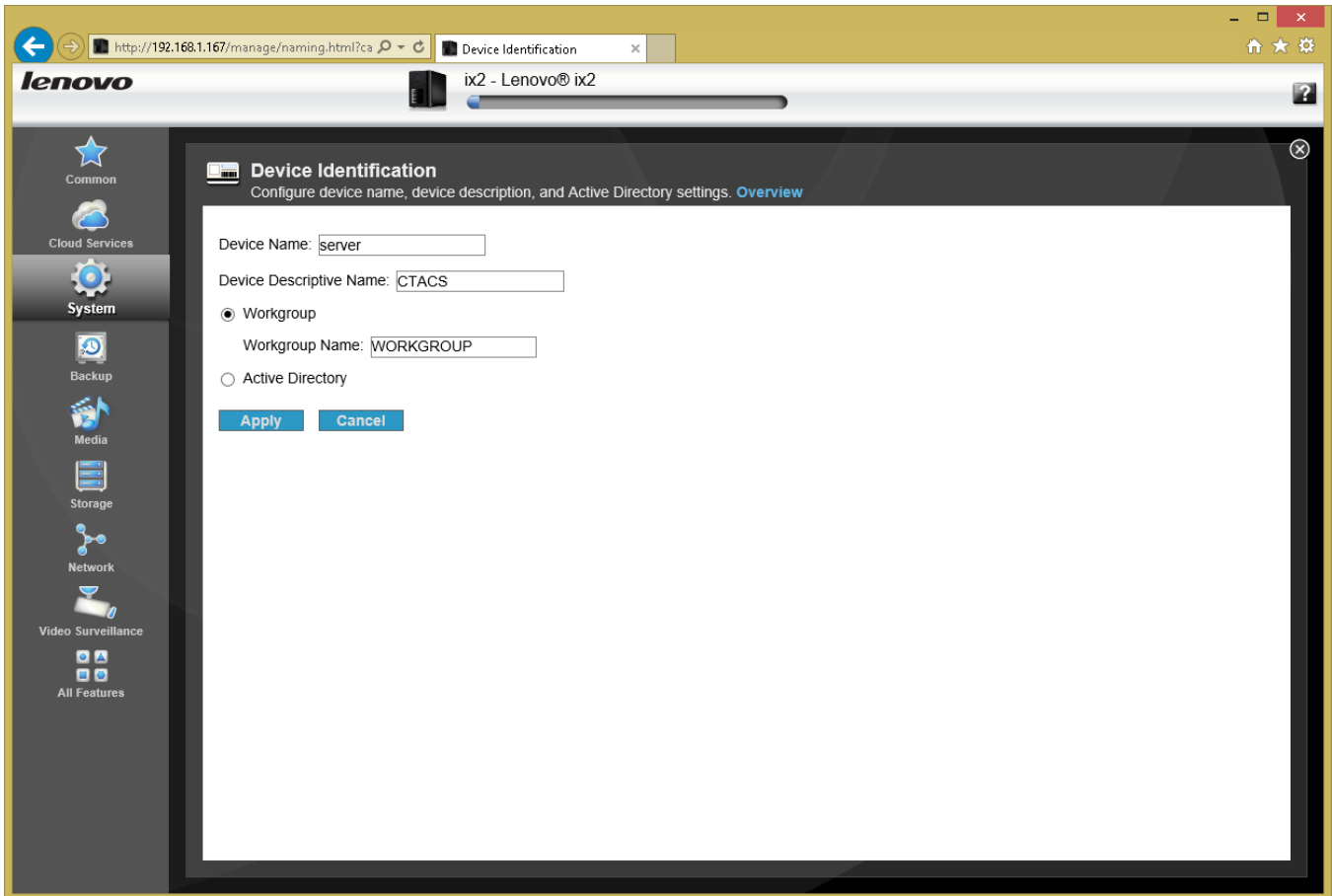


Figure 12: Device Identification screen

Change the **Device Name** to *server*. The **Device Descriptive Name** can optionally be changed if required, for example to the name of your organization or household. It is not usually necessary to change the **Workgroup Name**, as it is called *WORKGROUP* in 99% of networks anyway. **Active Directory** is a more advanced and specialized feature and not covered here as it is not usually applicable to small business and home environments.

Click **Apply** to make the change. Note that changing the device name will require a restart and a warning message to this effect is given. When it restarts it will be back at the same place where it was.

Note that is by no means necessary to change the name of the device or indeed to call it *server*. However, it makes sense and the examples in this manual do assume that this has been done.

2.7 Changing the IP Address of the Device

We need to make a decision about the IP address for the server. Every device has a unique number within a network to identify it, known as its *IP address*. The router itself will have a default fixed IP address decided by the manufacturer, for instance 192.168.1.1 is a common choice. It will then allocate numbers to computers and devices as they connect, for instance the first computer might become 192.168.1.101, the second computer might become 192.168.1.102 and so on. A piece of software inside the router – known as a *DHCP server* – handles this process. The ‘D’ in DHCP stands for dynamic and indicates that the IP addresses are handled dynamically and recycled. So, for example, the next time the first computer is switched on it might be allocated a different number, say 192.168.1.115. The fact that the numbers change does not make any difference to computers but some types of device prefer a fixed address, which is why routers use them. At the moment, the server is running on a dynamic IP address provided by the router, but we want to specify a static or fixed IP address instead. This IP address should be adjacent to that of the router. You may have to refer to the router manufacturer’s documentation for its address but some common ones include: TalkTalk 192.168.1.1; Belkin 192.168.2.1; Buffalo 192.168.11.1; D-Link 192.168.0.1; BT 192.168.1.254; Billion 192.168.1.254; Linksys 192.168.1.1; Netgear 192.168.0.1; Apple 10.0.1.1. In this example the internet router is 192.168.1.1 so we will choose 192.168.1.2 for the server.

Click the **Network** icon in the **Network** section. Remove the ticks off **Automatically configure all network settings** and **Automatically acquire network address (DHCP)**. Set the **IP Address** to the desired value. The **Subnet Mask** should be set to *255.255.255.0* (it will probably insert this value automatically). The **Gateway** is the address of the router i.e. *192.168.1.1* in our example. The **DNS Server** is also the address of the router. **WINS Servers** are not used. It is unlikely that a proxy server is used, but if you know for a fact that one is then refer to [Appendix A: Internet Access Using a Proxy Server](#).

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

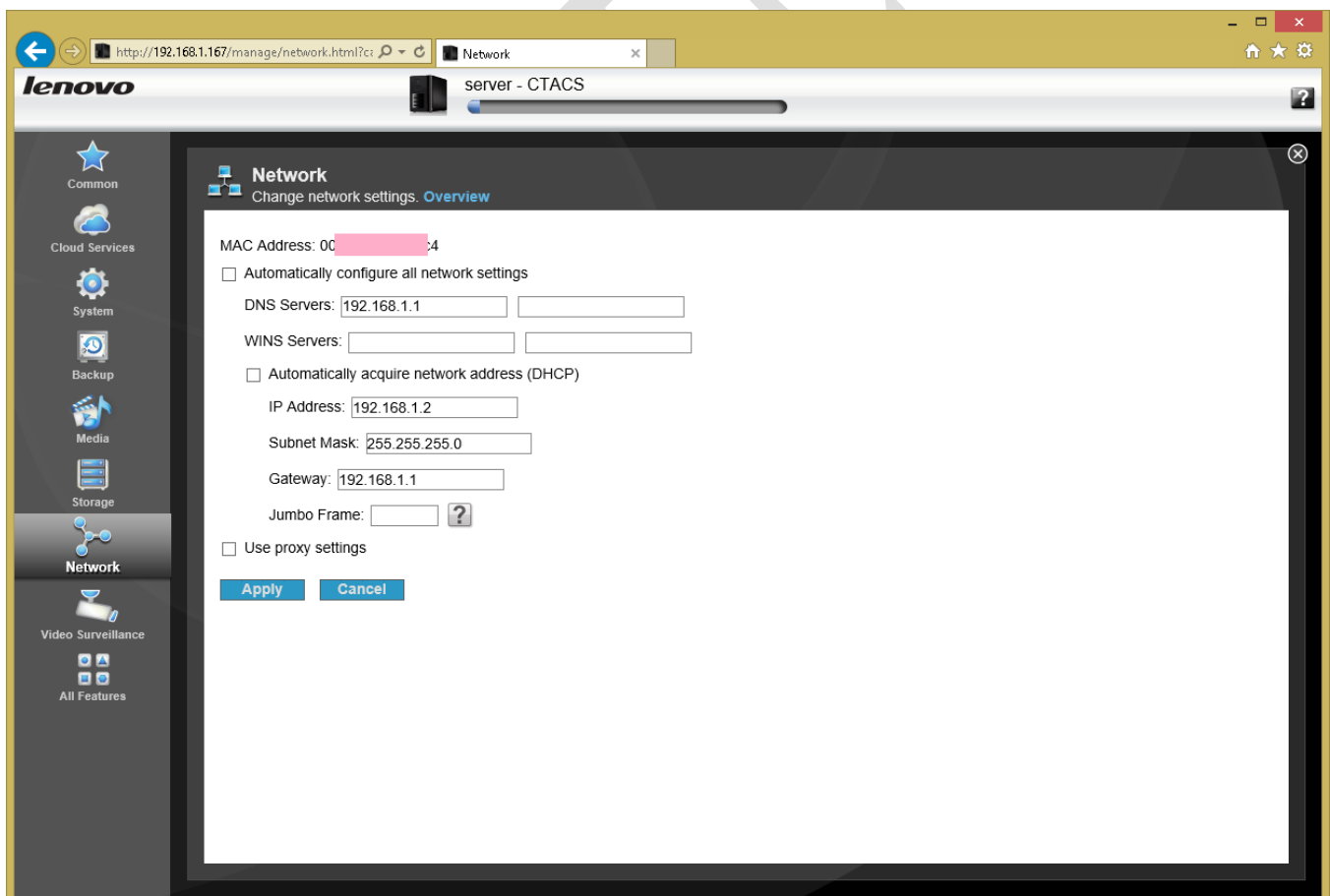


Figure 13: Network settings

There will be interruption to service for a few seconds whilst new IP address is applied. Go to the browser and enter an address of *http://server/manage* to continue the setup.

DO NOT COPY

2.8 Enable Security

The server can be run with or without security. At present we are running without, meaning that anyone on the local network can access the data on it, much as they could do if it was a USB hard drive connected to their computer. They can also make changes to the system, leading to unpredictable or undesirable results. To avoid this and make the server more manageable and usable, security needs to be enabled. This basically means having a system of user names and passwords.

To switch on security, click the **Security** icon in the **System** section. An administrative user – that is, somebody with full access to the system – needs to be defined. Use a meaningful name, such as *systemadmin*. Specify a password; the best passwords are non-obvious, contain a mixture of letters and numbers and are not too short. You may want to make a written note of the user name and password and keep it in a safe place. The default values for the other settings concerning encryption and certificate settings can be left as is.

Click the **Apply** button. A message is displayed advising that access to shared folders will now be restricted to the administrative user, which should be acknowledged (we will correct this later):

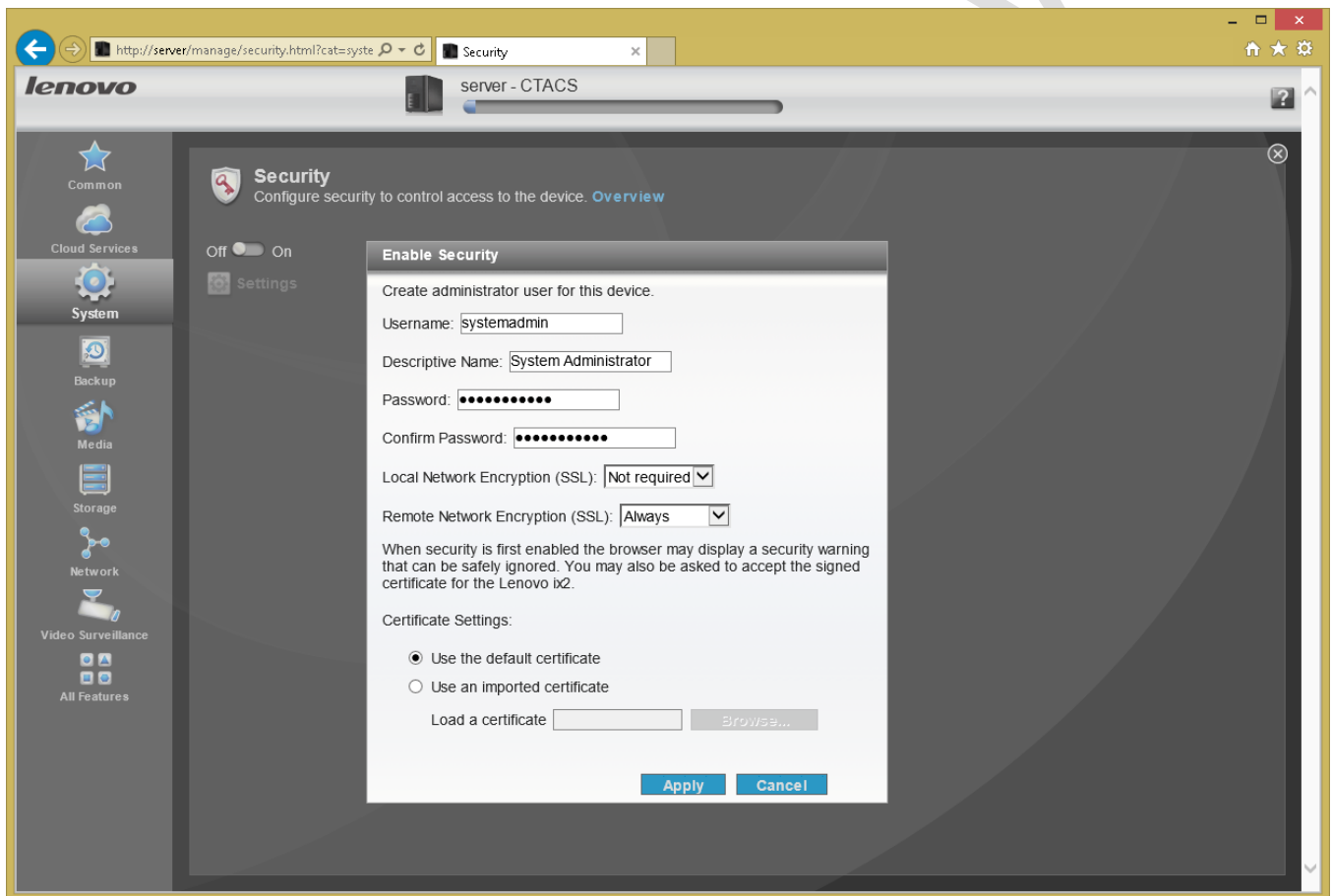


Figure 14: Enabling security

Note that after having just switched on security, the browser may display a message saying that “There is a problem with this website’s security certificate” (the precise message depends upon what browser you are using). This is expected and can safely be ignored – click the **Continue to this website** option or similar. Close the browser, then reload it. Type in an address of *http://server* or the server’s IP address; the screen will now look like this:

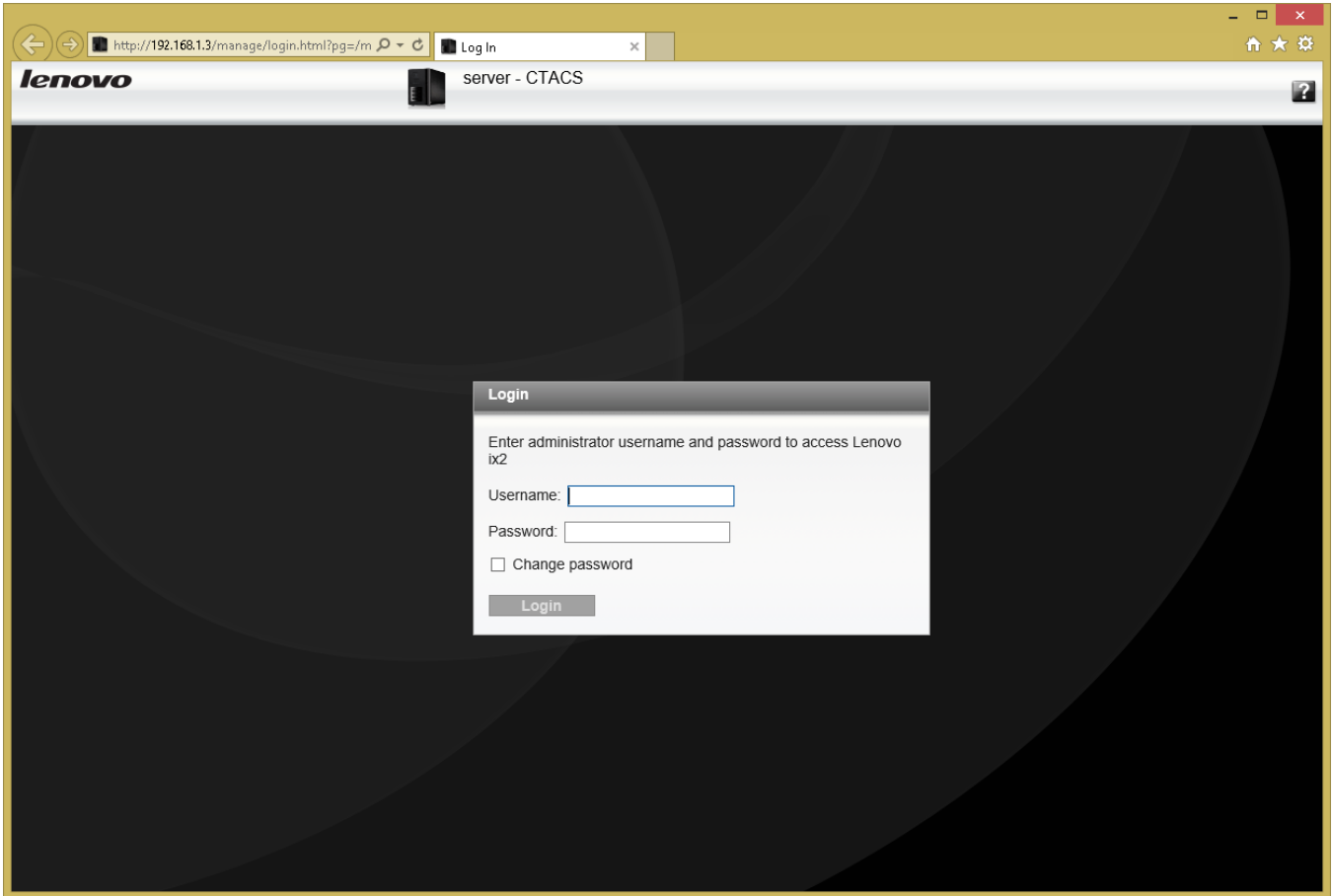


Figure 15: LifeLine login screen

To proceed, enter the administrative user name and password that you created above.

3 Hardware and Power Management

The network storage unit has a number of options related to power management and hardware. Some of these are to do with energy saving and can be used to reduce power consumption and hence save money. The options available may vary depending on the model.

DO NOT COPY

3.1 Energy Saving

There are two settings that can be used to save energy and hence energy costs. Firstly, the hard drives can be set to power down if the server has not been accessed for a while. Secondly, the brightness of the indicator lights on the front of the unit can be controlled (making them dimmer uses less power). As an additional bonus, the noise and light produced by the NAS are reduced, which can be useful if it is used in a domestic environment.

Click on the **Energy Saving** icon under the **System** section:

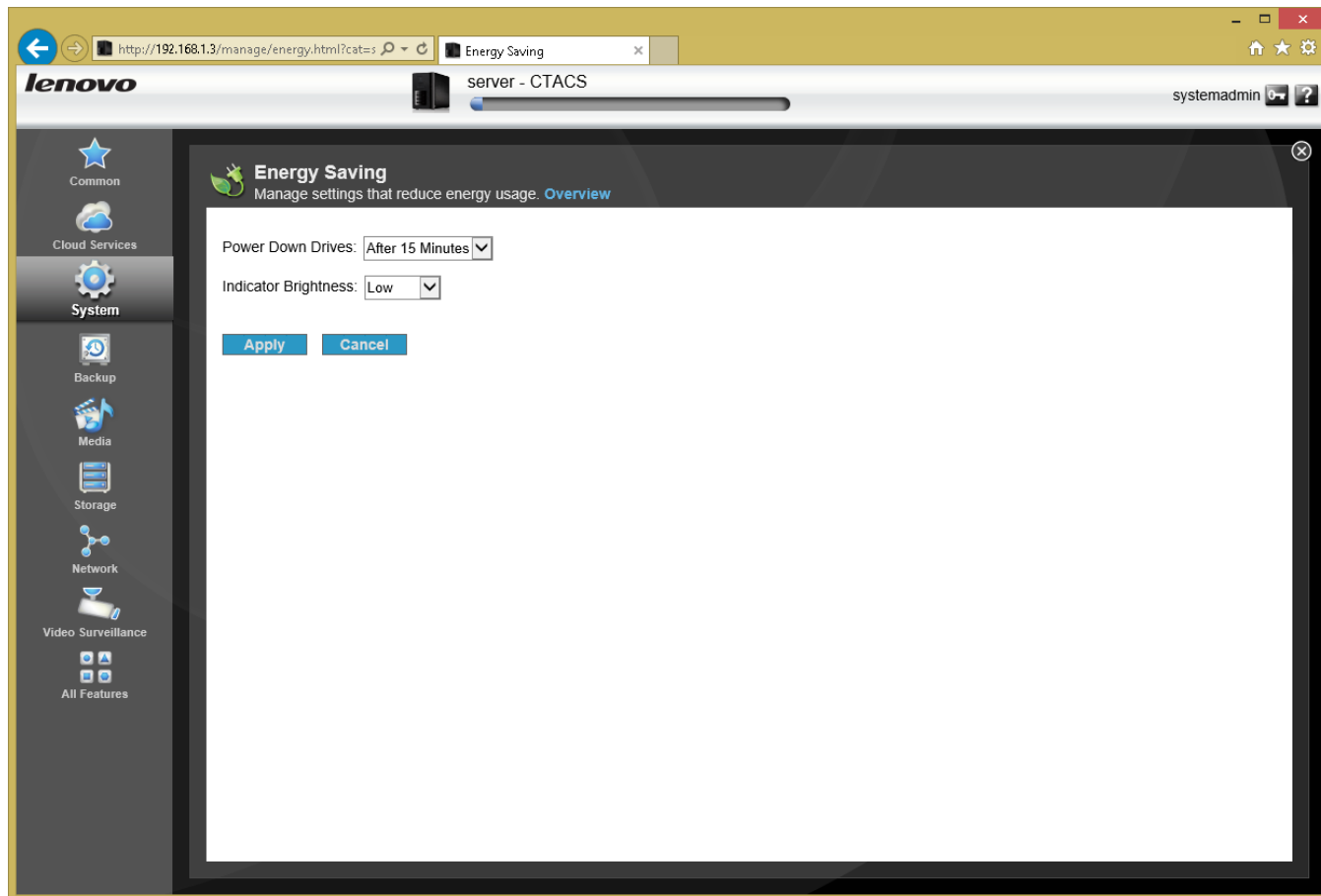


Figure 16: Energy saving options

There are two drop-downs. **Power Down Drives** has values from 5 minutes to an hour, or never. If the system is only used occasionally, set it to a low value e.g. 5 minutes. If the system is used extensively, set it to a higher value e.g. 30 minutes. If the drives have powered down then when someone accesses the server there will be a short delay whilst the drives spin back up to operating speed.

Indicator Brightness is a drop-down that allows the front lights to be set to Low, Medium or High.

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

3.2 Uninterruptible Power Supply

The use of an Uninterruptible Power Supply (UPS) is strongly recommended, particularly in a business environment or if you live in a part of the world where there may be electrical outages or brownouts.

Uninterruptible Power Supplies come in two types: unintelligent and managed. The former is basically a large battery and does not care or indeed know what is connected to it – as such it works equally well with servers, hairdryers, televisions, kitchen mixers or indeed most electrical items. Connect the server's wall plug into the UPS and plug the outlet cable into the server as per usual. Should the mains power fail then the server will continue running for as long as the battery maintains power.

However, a managed UPS is preferable. This is intelligent, in the sense that it can communicate with the server. When the mains power fails and the server starts running off the battery, it knows how much charge is remaining. When it falls to a critical level, the server shuts itself down in an orderly manner to protect itself and the data.

Most popular brands of intelligent UPS work with Lenovo. The UPS connects to server using a USB cable. Some of the network storage units only have a single USB socket; if you have other devices then you might want to buy a USB hub, preferably a powered one (which should also be plugged in to the UPS – think about it!).

If an intelligent UPS is used then its status can be checked by clicking the **UPS Management** icon in the **System** section.

4 Storage & RAID

Depending on the model, a network storage unit may hold 1, 2, 4 or more disk drives. A unit with more than 1 drive can be configured for RAID, which stands 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. Lenovo support many different RAID levels and depending on the model and the physical drives installed, the following RAID levels might be available: RAID 0; 1; 5; 6; 10; JBOD. However, despite all these options the most common scenarios in home and small business systems are RAID 0, RAID 1, RAID 5 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 read simultaneously, throughput is maximised. However, as bits of files are scattered across the two drives, if one drive fails then everything is lost. Also, the speed of disk drives is not actually the bottleneck in many NAS systems. For these reasons RAID 0 should generally be avoided.

RAID 1 consists of two identical drives that mirror each other. So, when a file is saved there are actually two separate but identical copies behind the scenes, one held on each drive, even though you can only see one as the mirroring process itself is invisible. If one of the drives fails, the second one automatically takes over and the system carries on without a blink. At the earliest opportunity the faulty drive should be replaced with a new one; the system is then synced it 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 the NAS has two 2TB drives installed then the total amount of usable storage capacity is 2TB rather than 4TB.

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

JBOD stands for *Just a Bunch of Disks* and is not actually a RAID system at all. Rather, it aggregates all the drives together to create one large volume that provides the maximum amount of storage space, albeit without any protection. For example, with the same drives as in the previous example you would get the full 8TB storage with JBOD rather than just 6TB storage as with RAID 5. In the event of a drive failure, you will lose the data stored on that drive, although it is possible that you could recover some data from the other drives (albeit it may need specialized techniques).

One important thing to note is that a RAID system is not a backup system. It can help prevent data loss in the event of problems but it is still important to make separate provision for backup. For instance, a RAID 1 system will cope with the failure of a single hard drive but if both drives failed then all the data would be lost and you would need a backup to recover.

Many Lenovo network storage units come pre-configured with a certain RAID level. However, you do not have to stick with this and can change it if it does not suit your requirements. For instance, the IX2 is usually sold with two hard drives installed that have been pre-configured as RAID 1. If you would rather have more storage space at the expense of data protection, you could change this to RAID 0 or JBOD.

4.1 How to Change the RAID Level

Note: if you are going to make any changes then it is suggested that you do so at this stage, before any data has been stored on the server, as it will be destroyed. If you are changing the RAID level on a system that is already in use, be sure to take a full backup of the system first.

Click **Drive Management** within the **Storage** section to display the following screen:

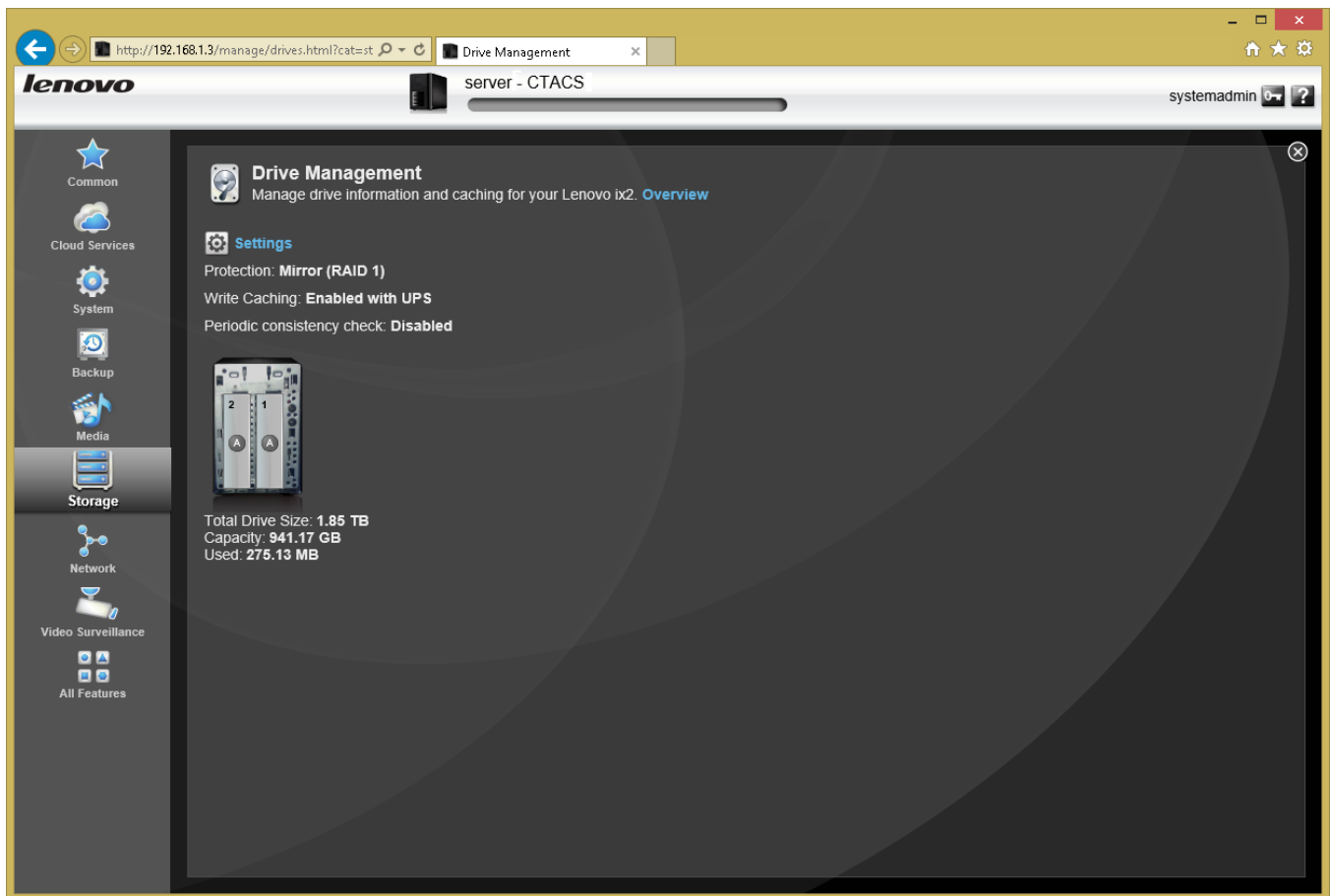


Figure 17: Drive Management screen

The screen gives a visual representation of the hardware you have. In this instance, there are two hard drives configured as RAID 1, giving a total usable capacity of 941 GB (i.e. just under 1 TB). Click **Settings** and the following panel appears:

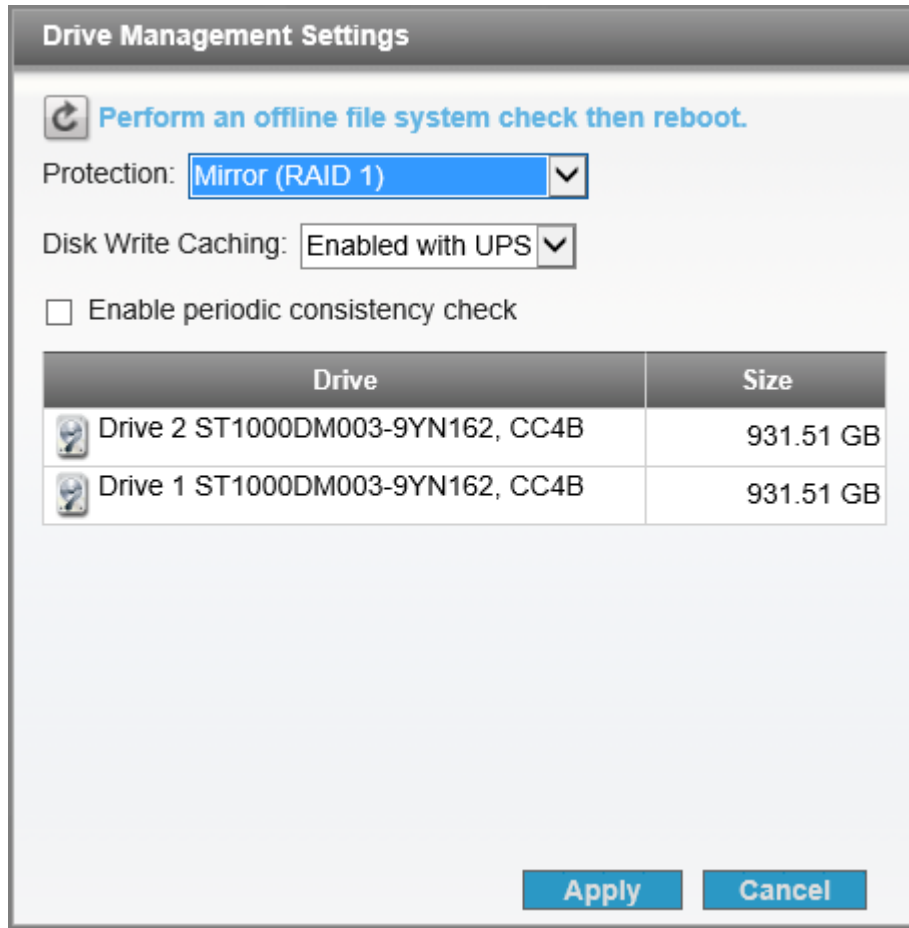


Figure 18: Drive Management settings

Click the **Protection** drop-down box and a list of options will appear. The options depend upon what hard drives are in the unit. If you wanted maximum storage capacity you would choose *RAID 0* or *None*, which is Lenovo-speak for JBOD (and which is preferable to RAID 0). A message is displayed about existing data being lost, which needs to be acknowledged. The conversion process will take a few minutes; when it is complete you will have one large, single volume for data. It is suggested that the server is restarted at this point (to restart click **System Status** and choose **Restart**).

5 User Accounts

At this point the user accounts should be created on the server (it is assumed that security has been enabled on the server at this point – if this is not the case refer to section [2.8 Enable Security](#)). This is one area where a different approach can be taken depending on whether it is a home or business network. In the case of a home network the user names can be just about anything you want, although there is some sense 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 is preferred. As a general point, the more consistency there is then the better things will be. For user names, two common conventions are to use the first name plus the initial of the surname or the initial of the first name plus the surname, although in some parts of the world other conventions might be more appropriate. In the case of particularly long names and double-barrelled names it might be a good idea to abbreviate them. For example:

Name of person	User name
Nick Rushton	nickr
Mary O'Hara	maryoh
Sam Hoffmann	samh
Amber Williams	amberw

Alternatively:

Name of person	User name
Nick Rushton	nrushton
Mary O'Hara	mohara
Sam Hoffmann	shoffmann
Amber Williams	awilliams

5.1 Creating a User

To create a user, click the **Users & Groups** icon in the **Common** section. At present only one user will be listed, the administrative user we created earlier on. Click **Add a User** and a blank form will appear:

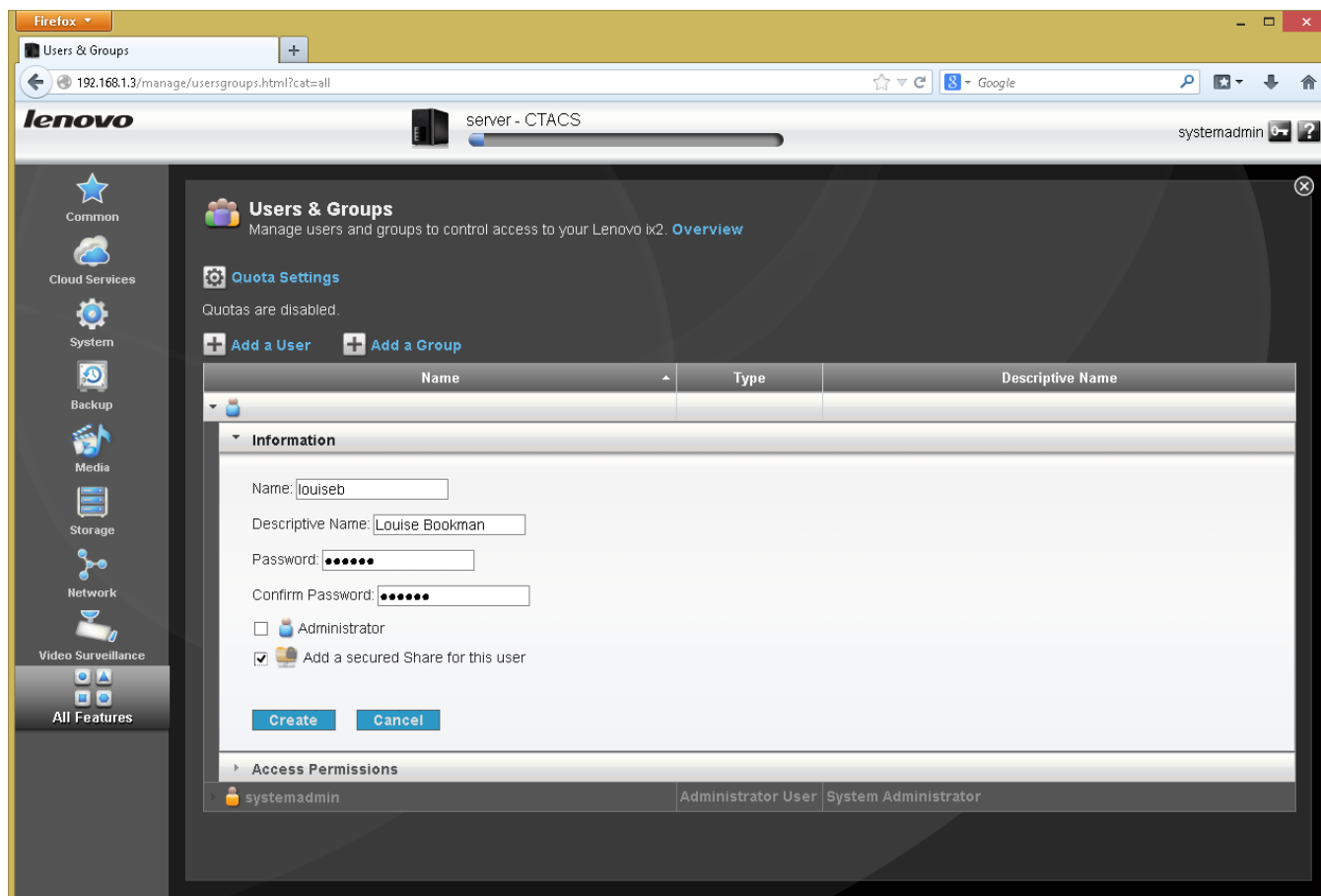


Figure 19: Creating a new user

Type in: the user's **Name**; a **Descriptive Name** for them (e.g. their full name); a **Password** plus a confirmation for the password. The password should be non-obvious (don't use words like 'password' or 'lenovo' or the user's name) and preferably a mixture of letters and numbers. It is suggested that you do not make them an Administrator – best practice is to have as few administrators as possible on a system i.e. just one or two. Tick the **Add a secured Share for this user** box – this will create a personal folder for the user, also commonly known as a *home folder*. Then click the **Create** button and the user will be created.

This process should now be repeated until all the users have been created. If you are working in a business and have a relatively large number of users to be created, you might find it helpful to create a checklist of names and passwords to work with.

5.2 Modifying or Deleting a User

To modify a user who has previously been setup, click the **Users & Groups** icon in the **Common** section. Click the user's name in the list of users. You can change their Descriptive Name and Password and, if ever required, make them an Administrator. You can also change their Access Permissions, although you might want to read section [6.2 Granting Access to a Shared Folder](#) first to understand what this means. Having made any changes, click the **Apply** button.

To delete a user, click the **Delete** button.

DO NOT COPY

5.3 Groups

Note: this section is of more relevance to business users. Home users may wish to skip to the next chapter.

In an organization with a relatively small number of users, specifying who has access rights to things is fairly easy to manage. But as the number of users increases it becomes more time consuming; for example, consider having to define the access rights for, say, 25 people. Such organizations are usually large enough that they contain departments or teams to carry out the different functions; for instance, there might be several people working in accounts, several in sales, several in marketing and so on.

To support these typical business structures, LifeLine 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 that they then apply to all members of that group. If a new person joins the team they just have to be defined as a member of the group, at which point they inherit all the relevant access rights.

In this example, we'll create a group called *accounts*. Click the **Users & Groups** icon in the **Common** section. Click **Add a User** and a blank form will appear. Type in a name for the group and click the **Create** button:

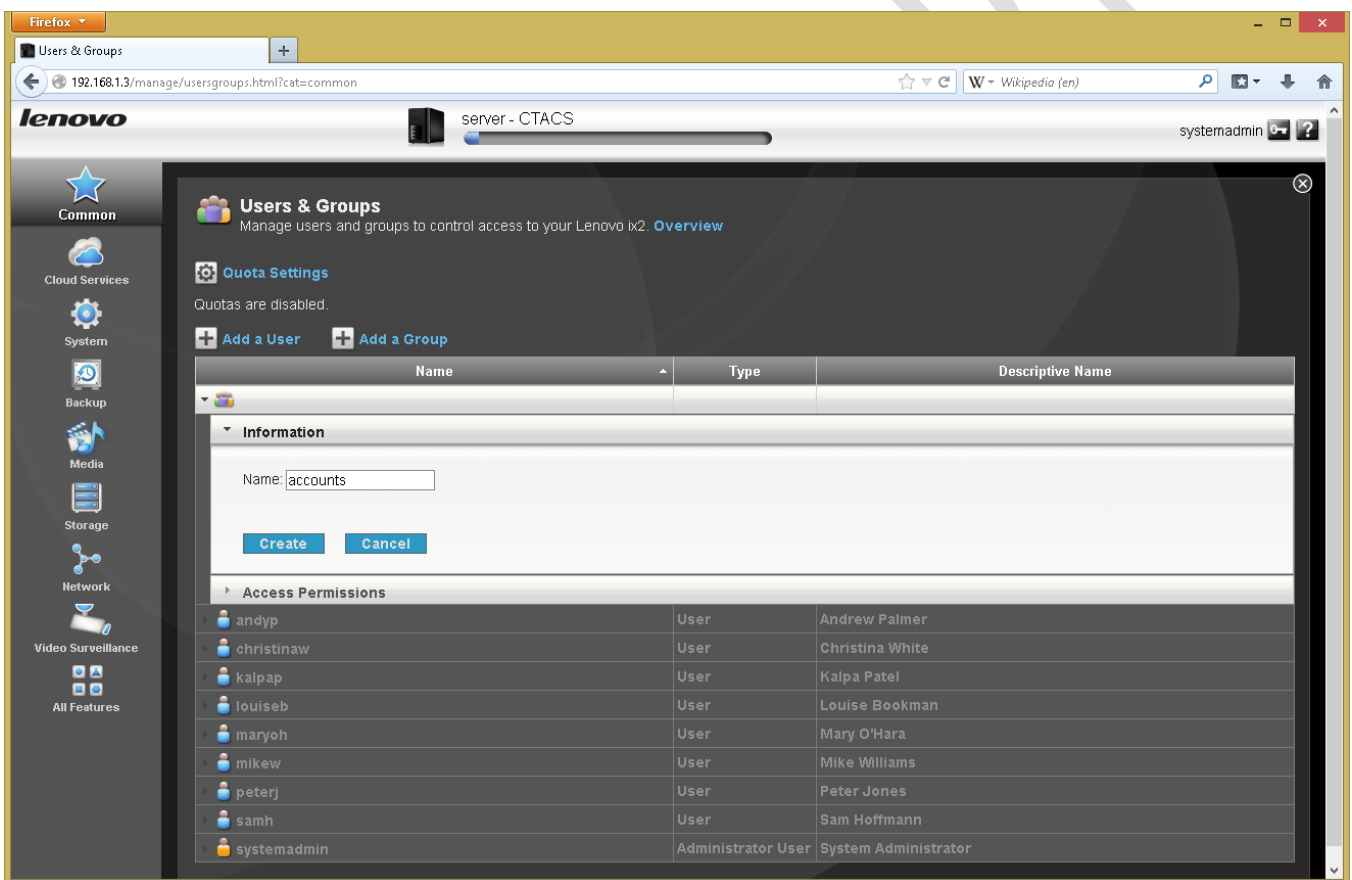


Figure 20: Creating a new group

The screen will refresh, advising that there are currently no users in the newly created group:

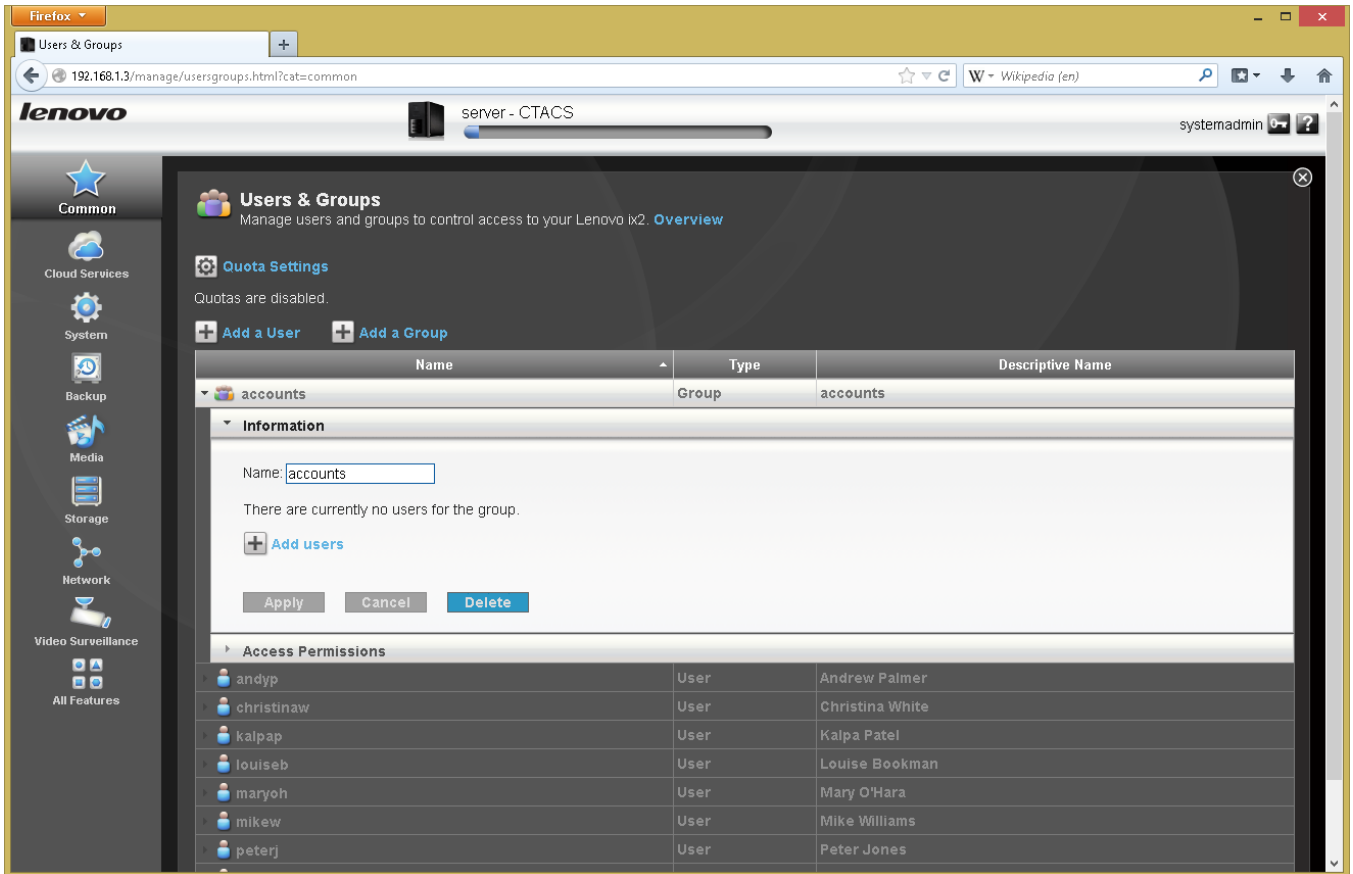


Figure 21: Information for a newly created group

Click **Add users** in the **Information** section for the new group. A list of all users is displayed; to add individual users to the group place a tick in the box against their name then click the **Apply** button:

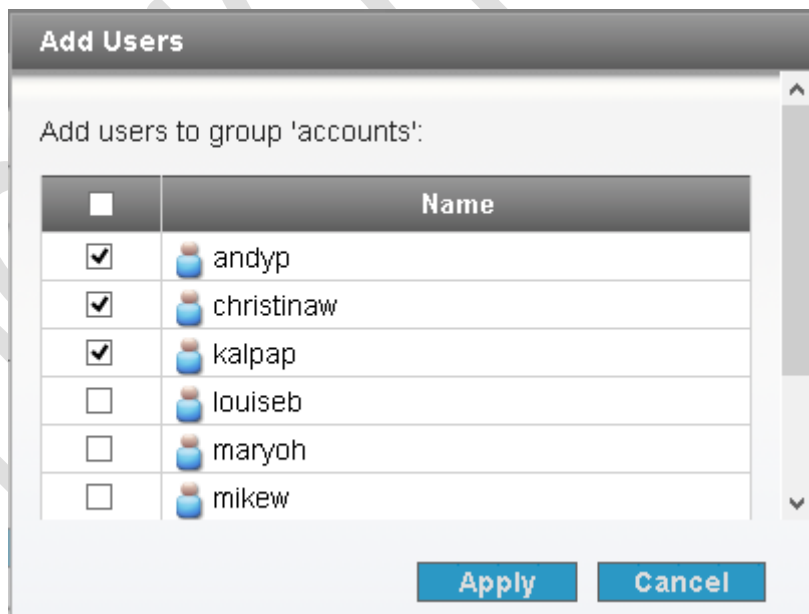


Figure 22: Adding users to a group

Hereafter, the group is included in the regular list of users. By expanding the **Information** section for it, the members can be listed. New users can be added to it and old ones deleted:

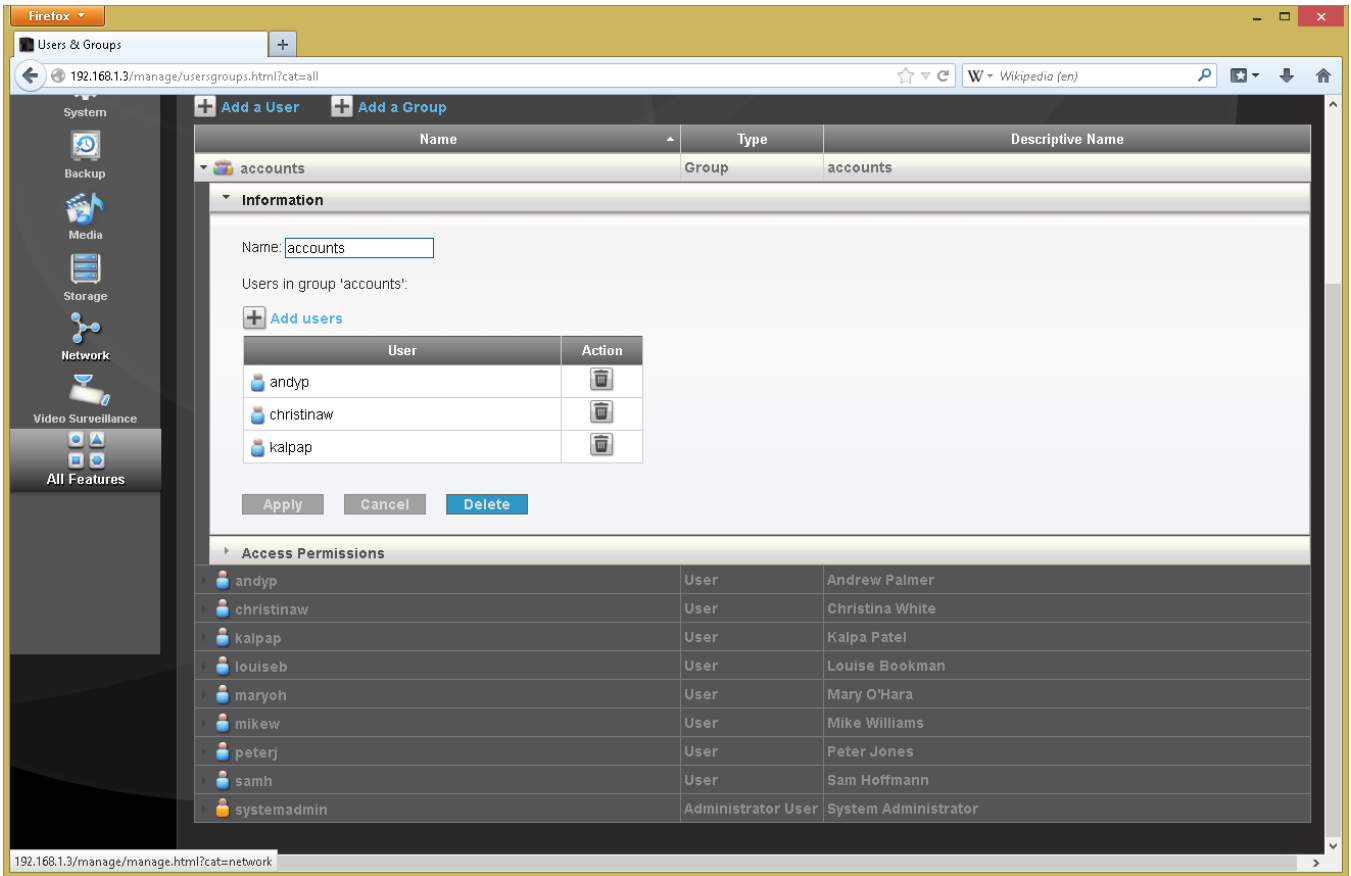


Figure 23: Details of group membership

5.4 Quotas

On the screen for managing users and groups is an icon marked **Quota Settings**. This allows you to define the maximum amount of disk space that users can have. As storage is cheap and plentiful these days, few people in a home or business will bother with it, although it does have possible relevance in some environments, such as education. It can also be useful in a business if, for instance, users are storing large numbers of non-business related data on the system such as videos or bit torrents.

DO NOT COPY

6 Shared Folders

The main purpose of a network is to provide an environment for users to 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 starting arrangement might be:

- At least one shared folder that everyone has access to
- Individual private home folders for each user
- Folders for music, photos and videos (particularly for a home system)
- A place to keep backups

The good news is that LifeLine has already created most of these folders during the initial installation and in many instances these will be quite sufficient. And if they are not, then it is easy to create additional ones.

There are six shared folders created during installation: *Documents*; *Backups*; *Movies*; *Music*; *Pictures*; *SharedMedia*. The purpose of these folders should be largely self-explanatory, based on their names. In a system without security (see section [2.8 Enable Security](#)) these folders are available to everyone, but the act of enabling security changes that. Rather, any shared folders, whether built-in or subsequently created, have to be explicitly made available to users and groups. This is done by granting *Access Permissions*.

6.1 Creating a New Shared Folder

To create a new shared folder, click the **Shares** icon under the **Storage** section. A screen showing a list of existing shares is displayed:

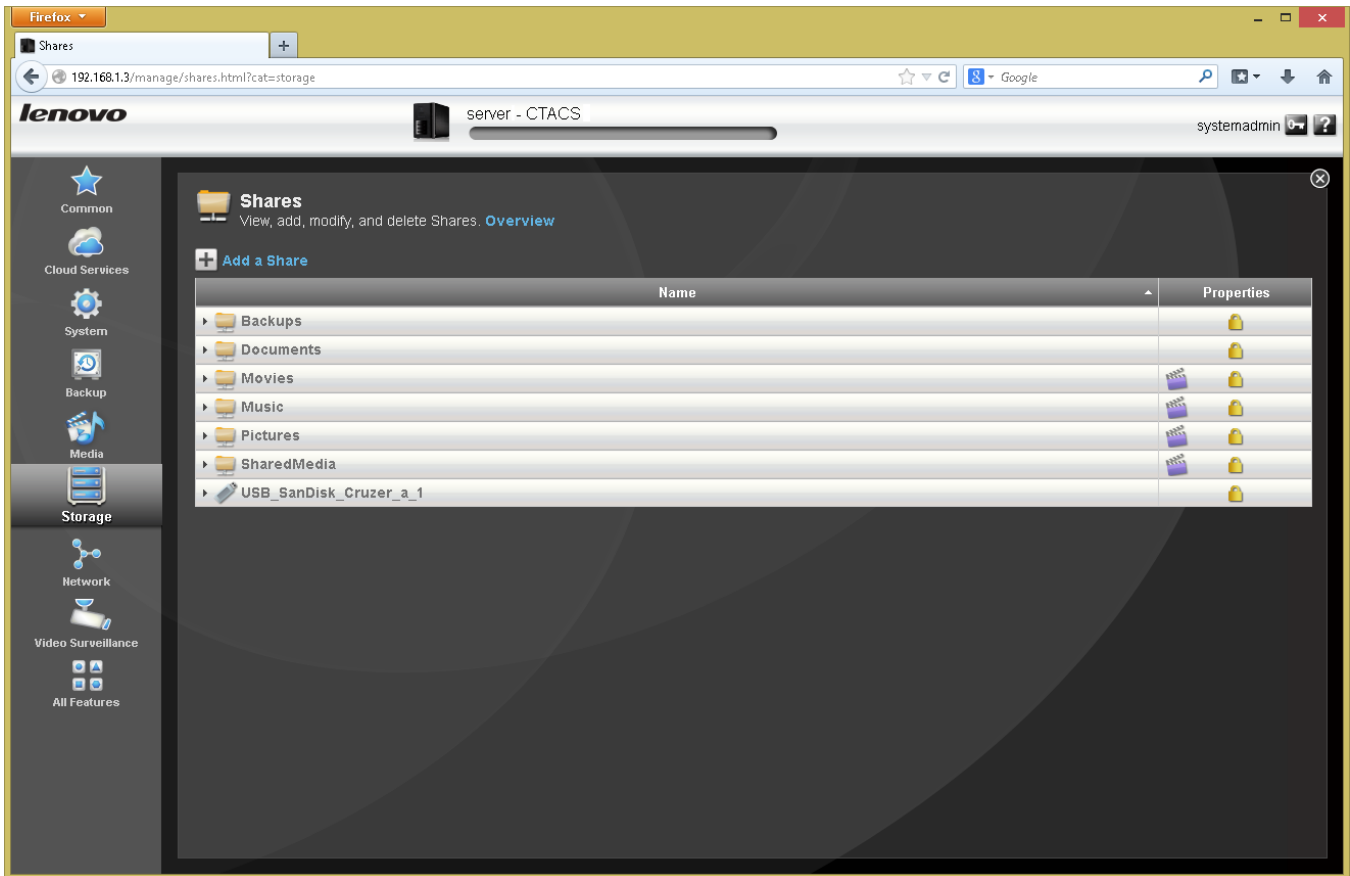


Figure 24: The Shares screen

To create a new share, click **Add a Share**. Specify a **Name** for the new folder. There is a box marked **Media sharing**; if this is ticked then the system will automatically search this folder for any videos, pictures and music and make them available to all users (see section [8 Multimedia & Streaming](#)). You probably do not want to do this in a business environment unless, maybe, the business is about media. Click the **Create** button.

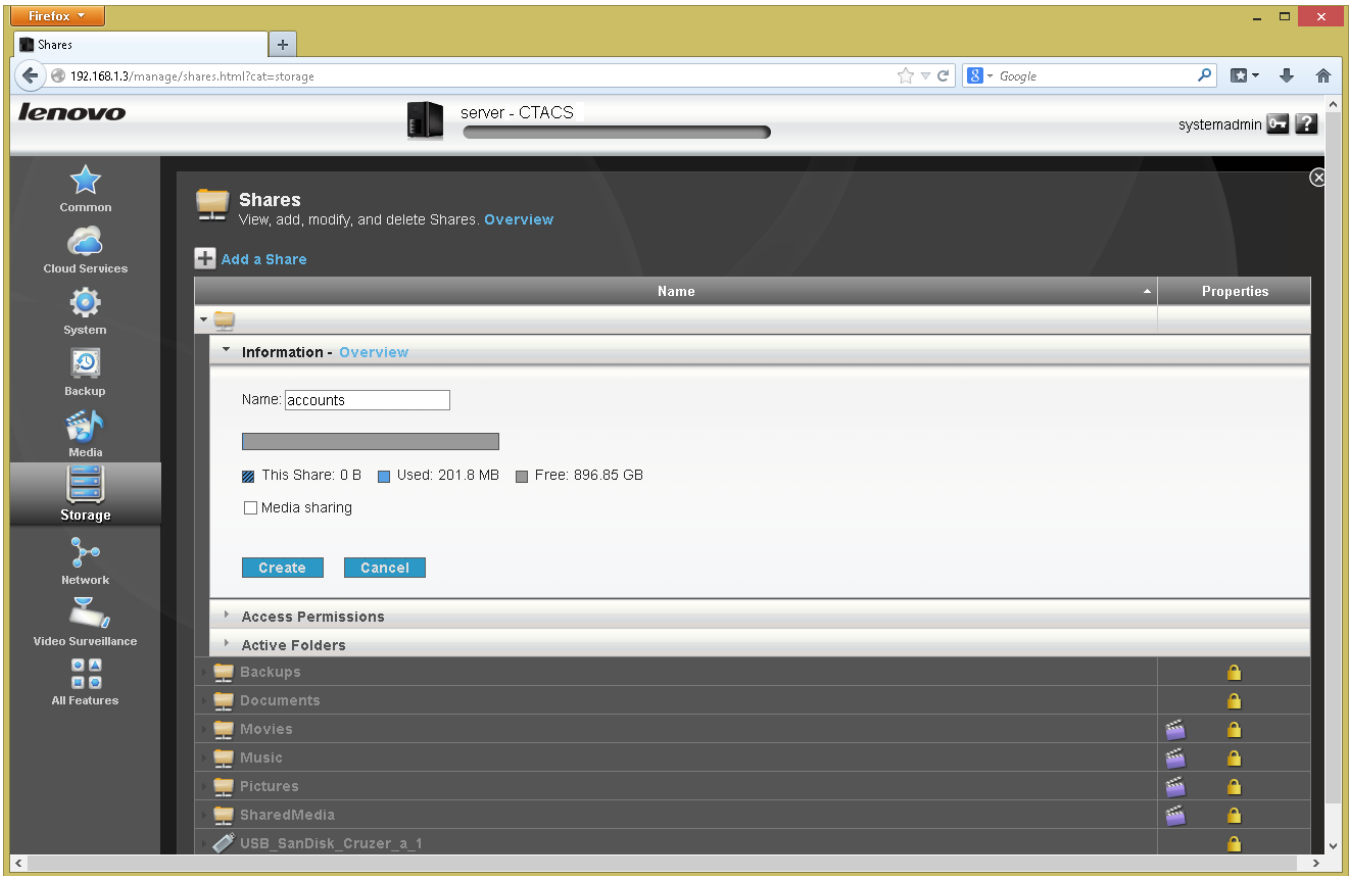


Figure 25: Creating a new shared folder

The folder is created. You can now close down the form by clicking the chevron next to where it reads ‘Information – Overview’.

6.2 Granting Access to a Shared Folder

Having created a folder, it is necessary to specify who has access to the folder and what type of access it is. The choices are:

Read/Write – a user can create, update and access the contents of a folder (in effect no restrictions)

Read – a user can access the contents of a folder but can make no change

No access – a user has no access at all to the folder (this is the implicit default)

Access permissions can be defined for individuals, for groups, or for everyone. The mechanism for doing so is the same throughout:

Click on the **Shares** icon within **Storage**. Click on the folder - in this example we will use the built-in *Documents* folder. Click on **Access Permissions** to expand that section:

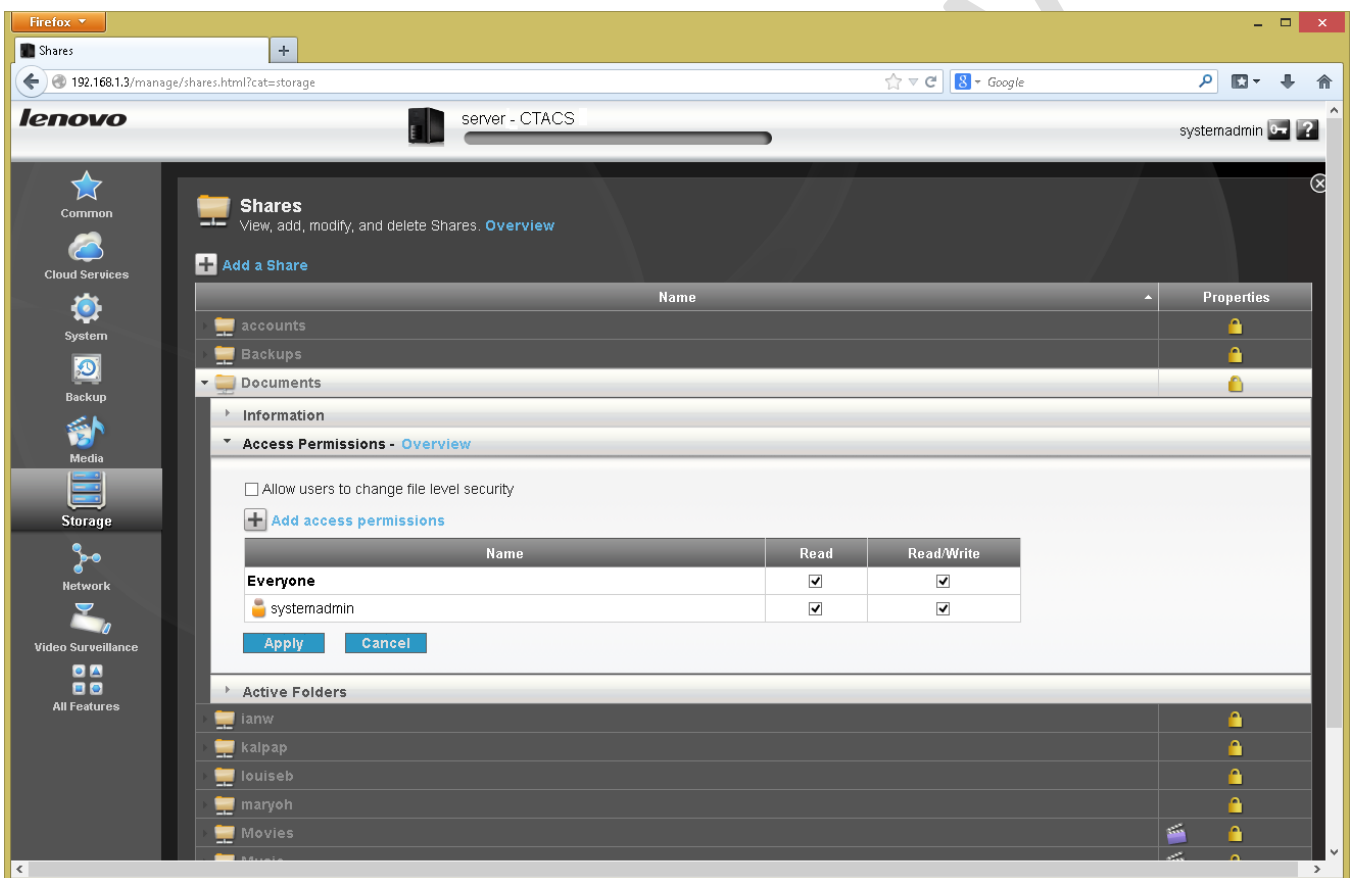


Figure 26: Access Permissions panel

At the moment, only the *systemadmin* user has access. However, note that there is a user called *Everyone* – this is like a built-in group that all users are automatically members of. Tick the box under **Read/Write** to give everyone full access; at the same time the **Read** box will also receive a tick as it is implicit if you specify **Read/Write**. Click **Apply**.

This process should be repeated for the other built-in folders: *Backups*; *Movies*; *Music*; *Pictures*; *SharedMedia*.

To add access for an individual or a group, click **Add access permissions**. A small panel is displayed listing the names of all the users and any groups; place a tick against the desired name(s) and click the **Apply** button:

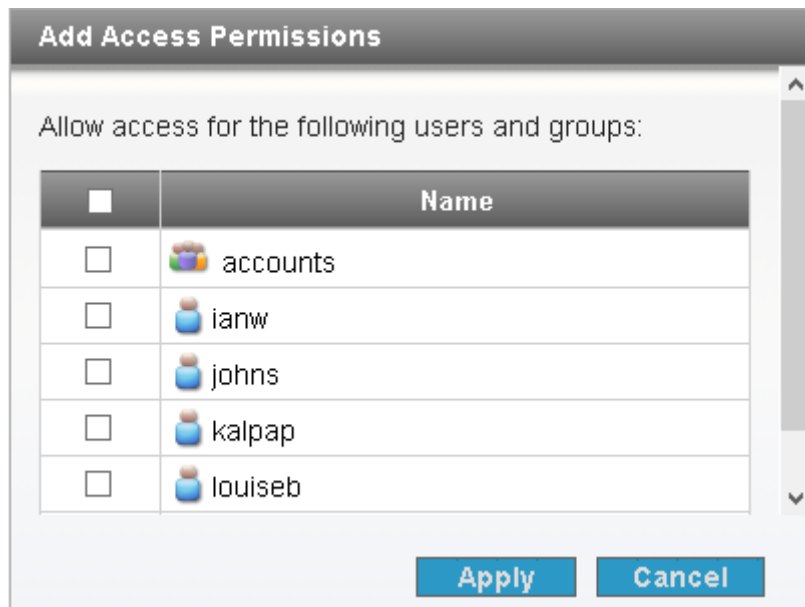


Figure 27: Configure Access Permissions

7 Accessing the Server

There are numerous methods for accessing the network; some of these are available to Windows users only, some to Mac users only and some to both. Each approach has its merits:

- Using a Browser (Windows and Mac)
- Using Windows Explorer (Windows)
- Accessing a shared folder (Windows)
- Mapping drives manually (Windows)
- Using a batch file (Windows)
- Using the Finder (Mac)

In addition, there is a downloadable utility called the *LenovoEMC Storage Manager*. Amongst other things, this allows shared folders to be mapped to drives. However, it offers a strange mixture of functionality and methods of working and it is suggested that it is not normally used.

DO NOT COPY

7.1 Using A Browser

This is the most universal method for accessing the server and works for Windows PCs and Macs. Simply go to any computer on the network, launch a browser such as Firefox, Chrome or Internet Explorer and type in the IP address of the server e.g. 192.168.1.2 or its name i.e. *server*. A web page along the following lines is displayed:

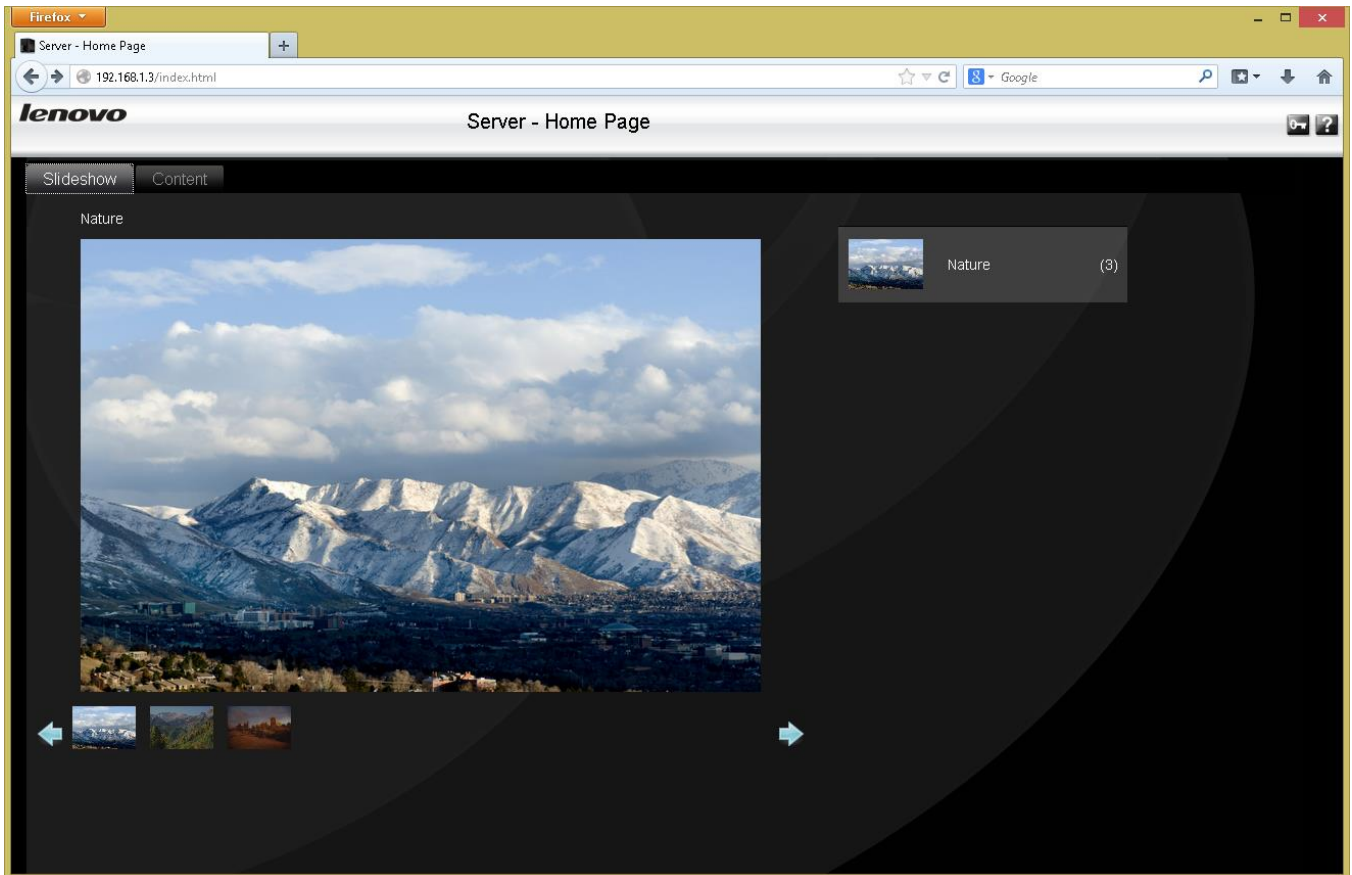


Figure 28: The Home Page

There are two tabs – *Slideshow* and *Content*. Slideshow displays a selection of pictures; these are samples from LifeLine but could be replaced with your own household or business pictures (how to do so is discussed later in section [15.3 Customizing the Home Page](#)). Click **Content** and the screen changes thus:

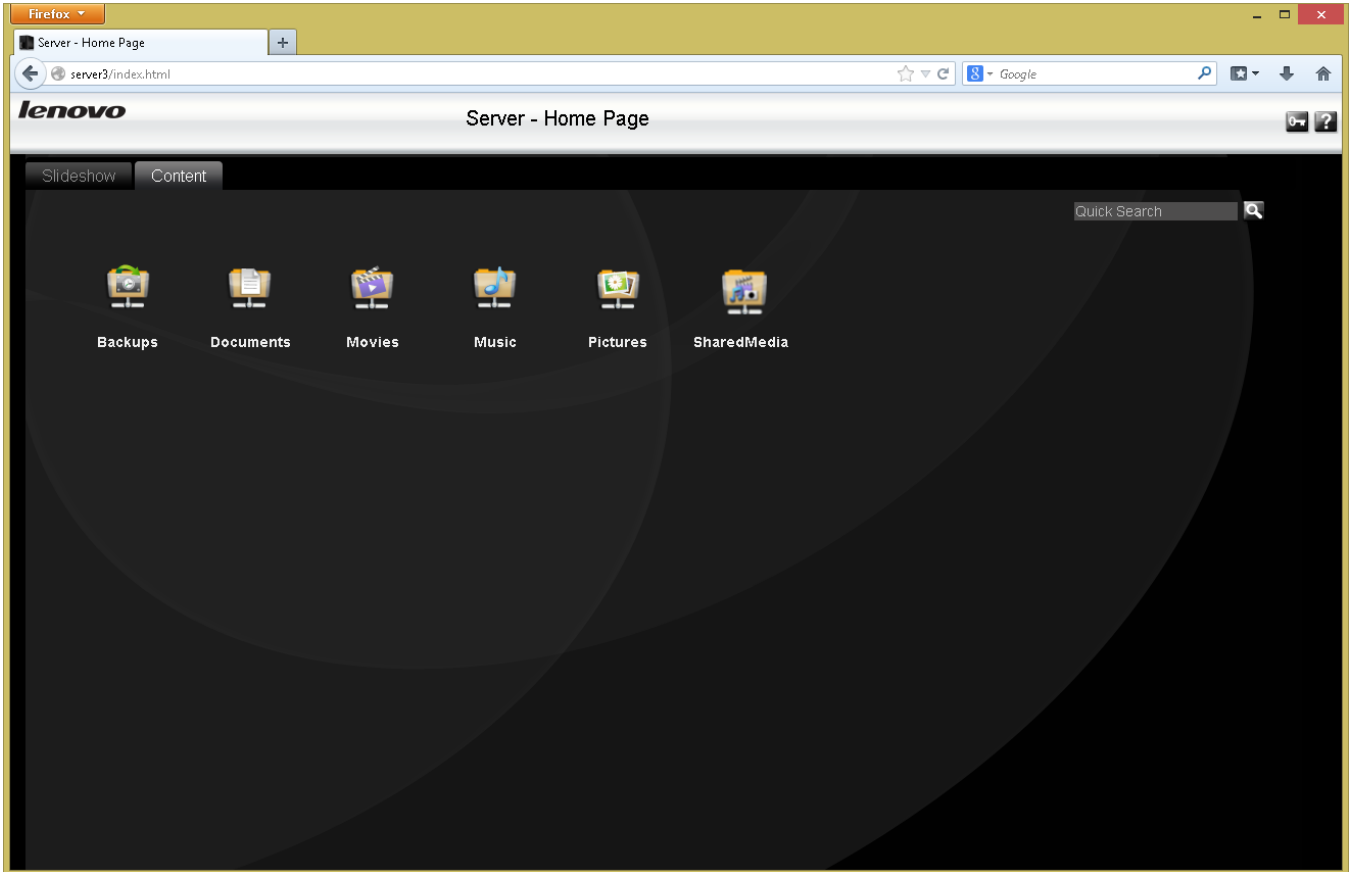


Figure 29: Shared folders as viewed on the Home Page

The default shared folders created during the installation of LifeLine are displayed. Clicking on one causes it to open in a new browser window in the *Content Viewer*, which is analogous to a simplified version of Windows File Manager or the Mac Finder:

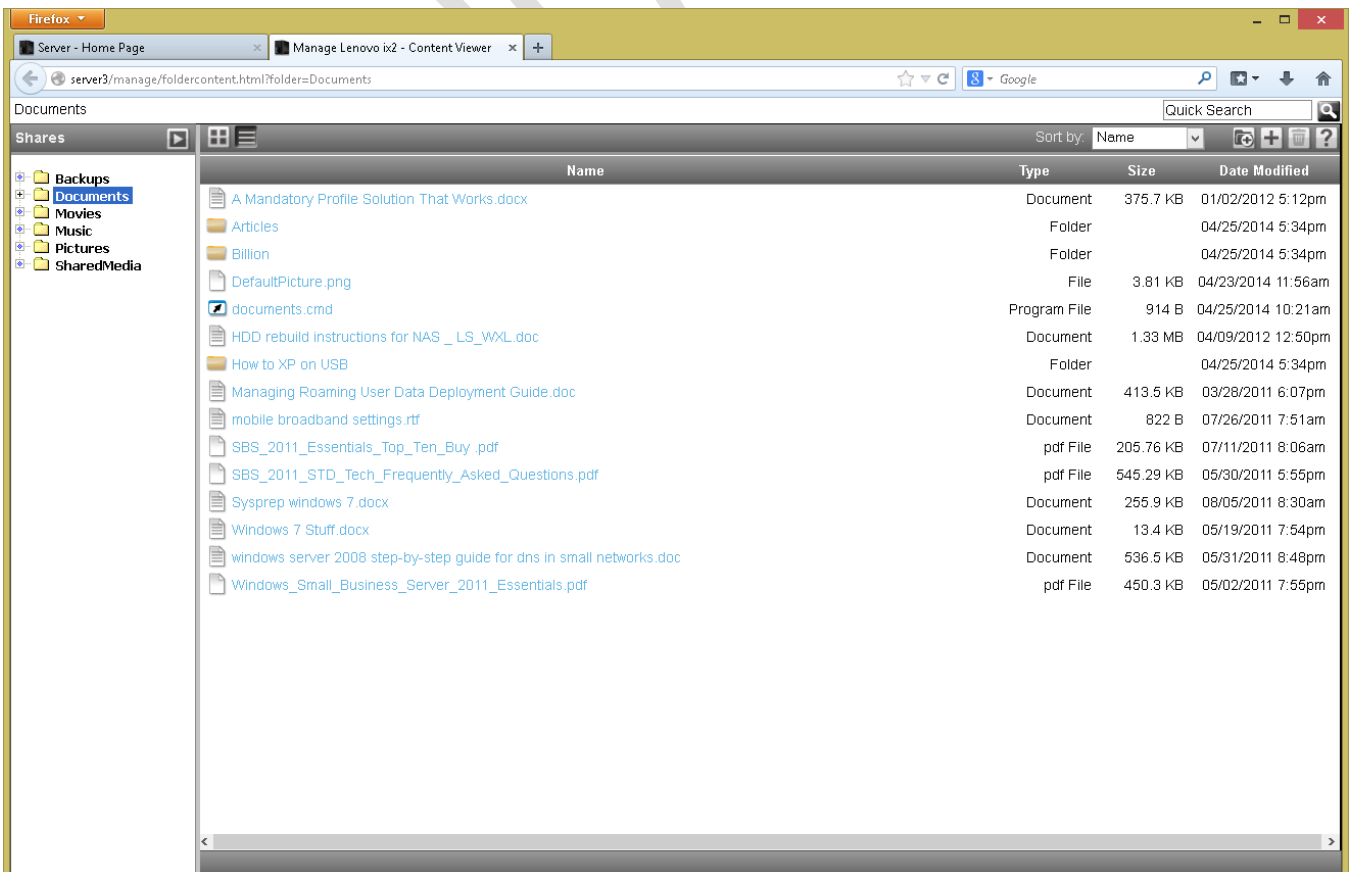


Figure 30: Viewing a folder using the Content Viewer

To work with a file, click on it. Some files can be viewed directly, such as graphics files and PDFs, whilst music files (MP3) will play in the local media player, but many will prompt you to download the file to the local computer. Make the changes to the document using Word, Excel or other preferred application, then use the Upload button – the small icon with a plus sign in the top right-hand corner of the screen - to return the revised version back to the server.

Files can also be deleted. First select the file; the best way to do this is by clicking on its details on the right-hand side of the screen i.e. its Type, Size or Date Modified information, as clicking on its name will cause it to open or download as per the previous paragraph. Then, click the trash can icon in the top right-hand corner of the screen.

Finally, new sub-solders can be created by clicking on the icon in the top right-hand corner of the screen.

Note that it has not been necessary to logon to the server in order to access the shared folders. However, if a user wishes to use their own personal folder, then it is necessary to logon from the home page by clicking the icon in the top right-hand corner of the screen that looks like a key and then entering their user name and password:



Figure 31: Logon icon

If this is done, then their personal home folder (if one exists) will be listed on the Content screen alongside the other shared folders. If an admin user logs in, they can manage the server by clicking on the icon in the top right-hand corner of the screen that looks like a gear wheel:



Figure 32: Manage server icon

7.2 Using Windows Explorer

A simple way to access the server directly is by going into Windows Explorer (called File Explorer in Windows 8). Expand the left-hand panel to view the Network and down the left-hand side the server should be visible. Click on it and the list of shared folders will be displayed:

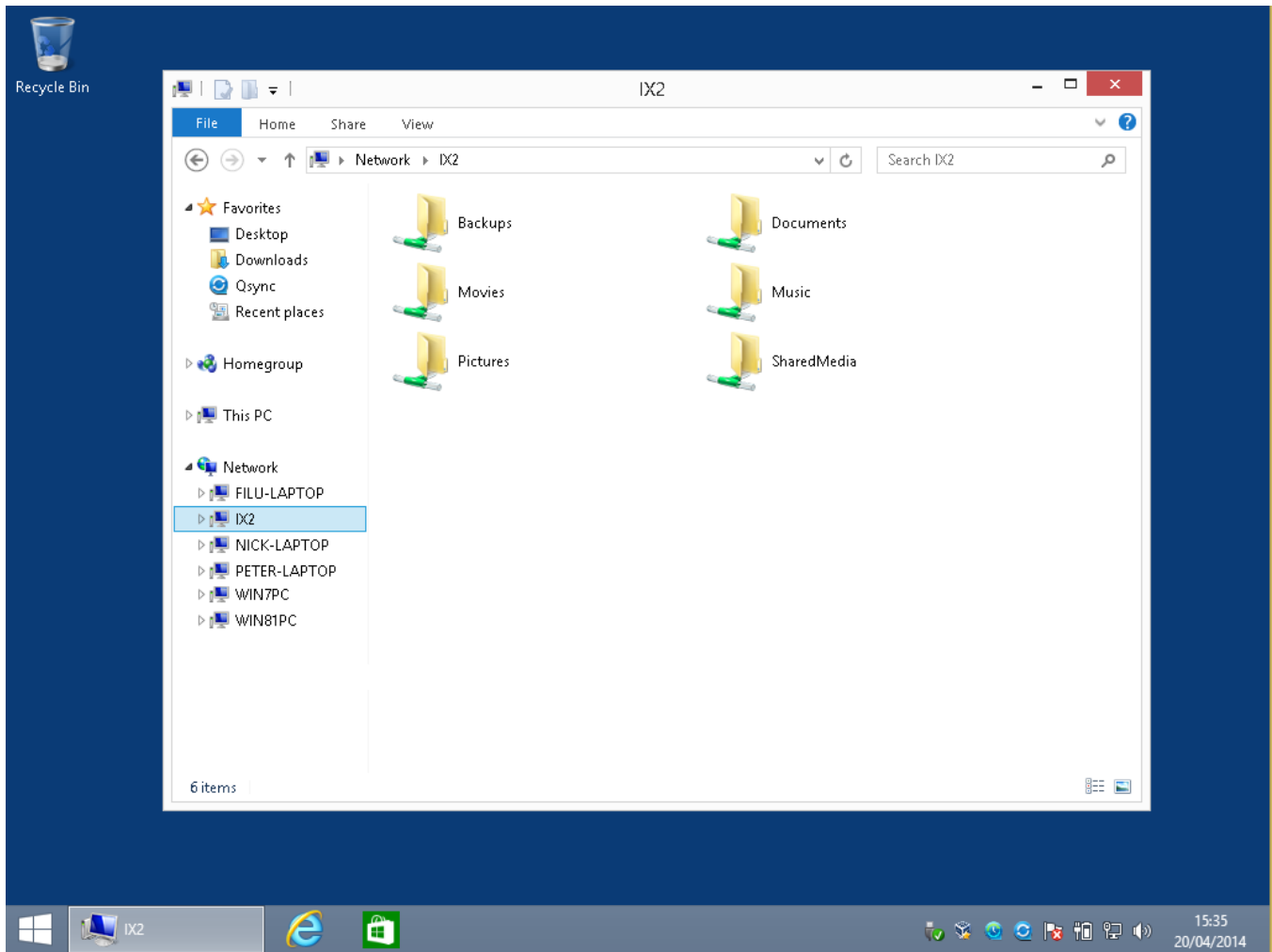


Figure 33: Viewing the shared folders from File Explorer

To access a shared folder, double-click on it – you will be prompted to 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. Although all the shared folders are visible, you can only access the ones to which you have been granted privileges.

7.3 Accessing A Shared Folder using the Run command

To access a shared folder from a Windows PC click **Start** then choose **Run** (in the case of Windows 8.1 right-click the **Start** button then choose **Run**). 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 e.g. `\\server\documents` and click **OK**.

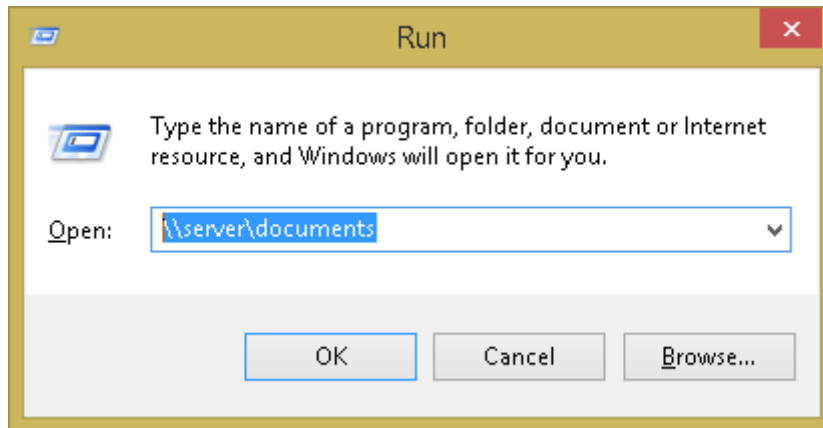


Figure 34: Accessing a shared folder using Windows Run command

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

7.4 Mapping The Drives Manually

Network drives can be mapped using Windows Explorer:

- If using Windows 8 or Windows 8.1, open File Explorer, which 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.
- If using Windows 7, open Windows Explorer, which 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**.
- 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**.
- 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**.

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 shared folder. Or, simpler still, just type in the name of the folder:

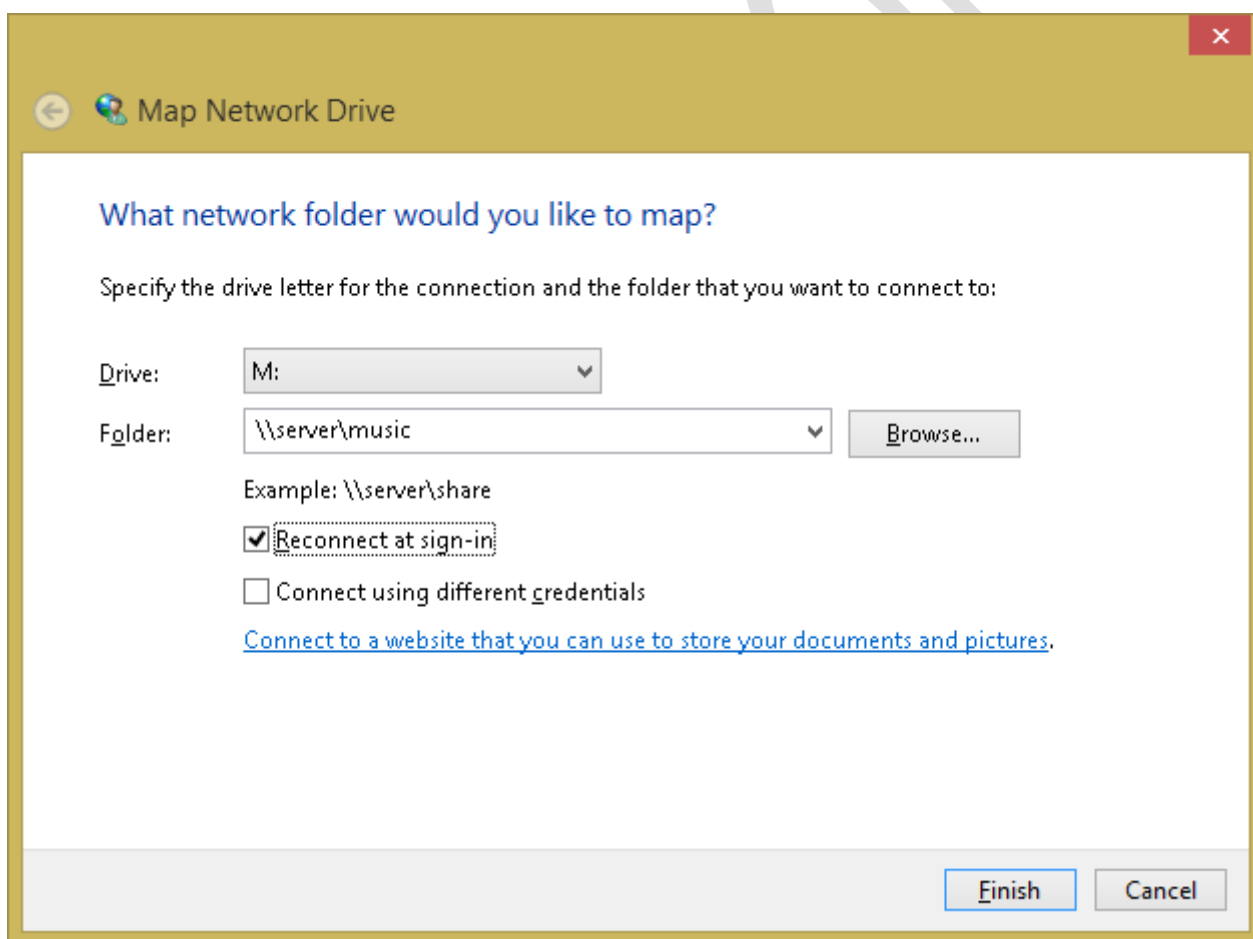


Figure 35: Mapping a network drive in Windows

If the computer is only ever used by one person tick the **Reconnect at sign-in** box – this will cause Windows to remember the mapping. Then click **Finish**. You will be prompted to enter the user's name and password that were defined earlier on the Server. Again, if the computer is used just by one person tick the **Remember my credentials** box. Then click **OK**.

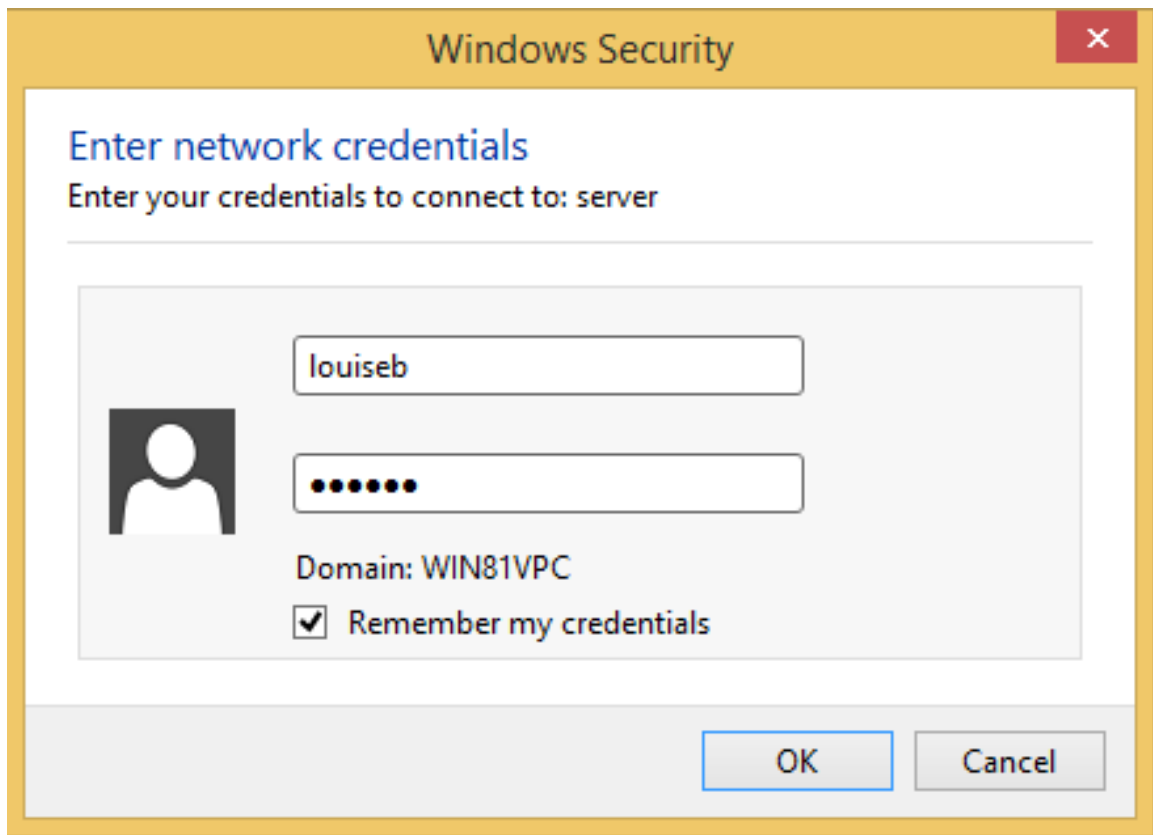


Figure 36: Entering network credentials

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 wants 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 use C as that is always in use on a computer).

7.5 Using A Batch File

Setting up a batch file is a more advanced technique for use on Windows PCs, but can be useful when a particular computer is used by more than one person. As such, it is probably of more relevance in a small business environment than in a home system. Start off by using Notepad or WordPad to create a plain text file called *Connect-to-NAS.cmd* (you can download a ready-to-use copy by going to www.serverinstallationguides.co.uk and clicking the Lenovo tab). The contents of the file will vary depending on the folders to be mapped. In this example the six default folders created by Lifeline plus the user's personal *home* folders are mapped:

```
ping server -n 1 > nul
if errorlevel 1 goto offline
:online
: remove any drive mappings already present
net use * /delete /y > nul
: prompt for NAS username and password
set /p nasname=Enter Username: %= %
set /p naspwd=Enter Password: %= %
: map the drives
net use u: \\server\%nasname% %naspwd% /persistent:no /USER:%nasname%
net use t: \\server\backups /persistent:no
net use v: \\server\music /persistent:no
net use w: \\server\movies /persistent:no
net use x: \\server\pictures /persistent:no
net use y: \\server\sharedmedia /persistent:no
net use z: \\server\documents /persistent:no
goto end
:offline
cls
echo You are not connected to the network.
echo If you are outside the office then this is expected.
echo If you are inside the office then it means there is a problem.
echo Data stored on the network is not currently available.
pause
:end
```

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

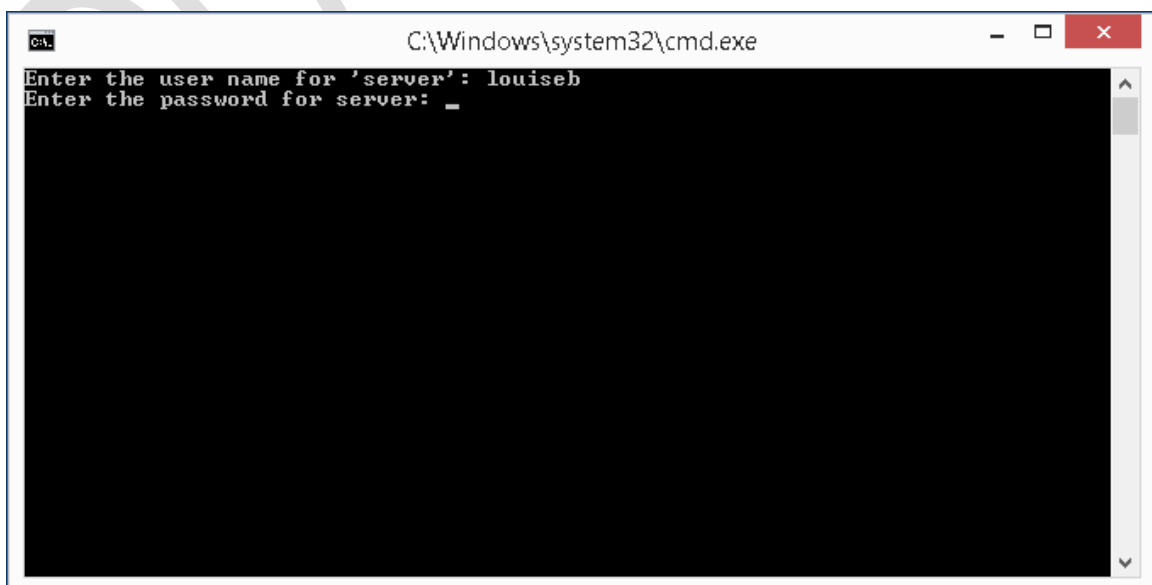


Figure 37: Enter user name and password

After the user has successfully entered their details, the mapped drives will be available until the computer is shutdown or the user logs off. The drive mappings can be verified by launching Windows Explorer, which appears by default on the Taskbar in Windows 7 and Windows 8.

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

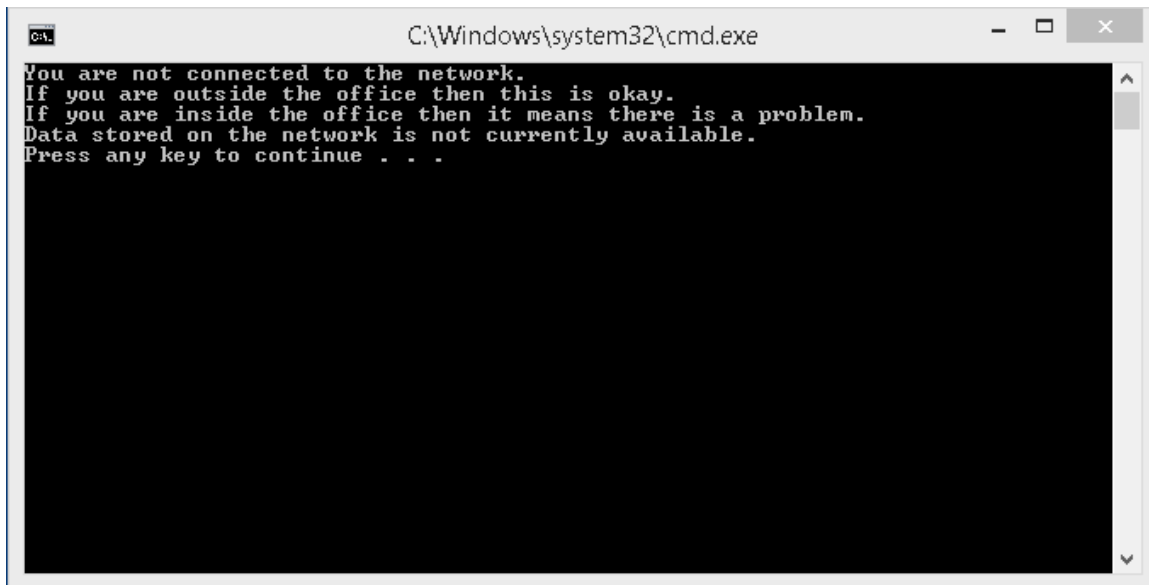


Figure 38: Warning message if not connected

It is to be expected that this message will appear if using, say, a laptop computer outside of an office, but if it appears inside then it indicates a problem. This could be a connectivity issue on the computer e.g. Ethernet cable unplugged or wireless disabled. If everyone in the office is experiencing problems 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 on the Desktop for each individual user. More efficiently, it can be placed in the following location where it will appear on the Desktop for all users:

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

Note that the Public Desktop folder is a hidden folder on Windows 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**. Click on the **View** tab, enable **Show hidden files, folders and drives** and click **OK**:

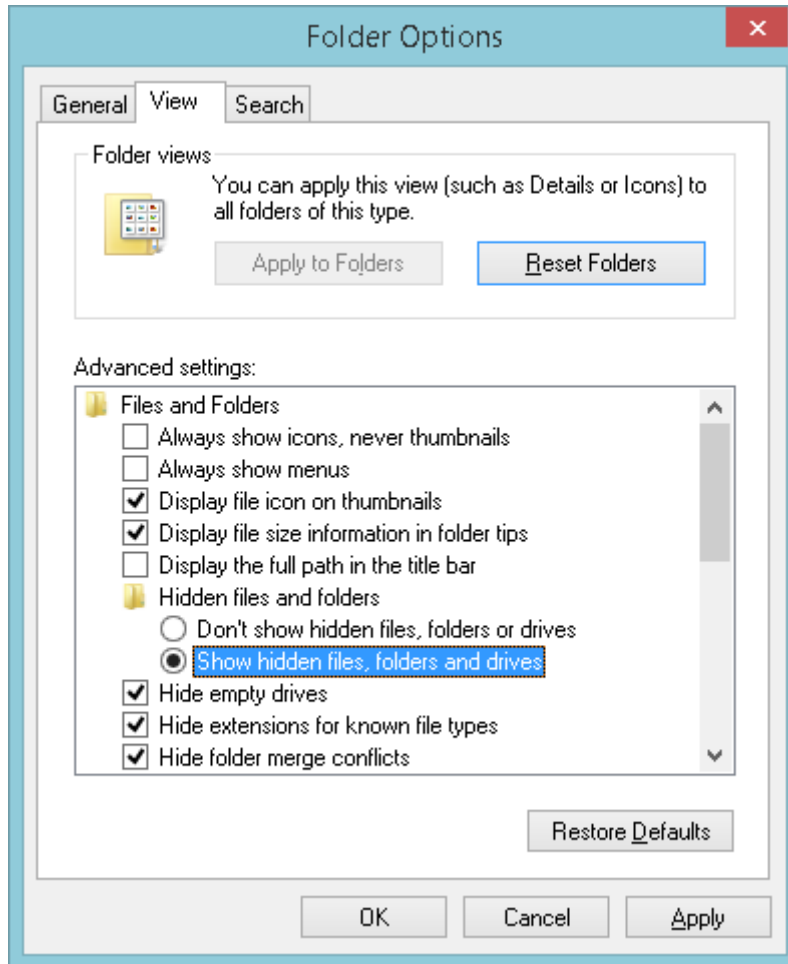


Figure 39: Folder options to view hidden files

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.

7.6 Connecting a Mac

There are various iterations of the OS X operating system and some subtle differences between them. However, the following technique will work with all versions. If Macs are used then Apple File Sharing needs to be enabled on the server; it should already be switched on by default but this can be verified by clicking on **Protocols** in the **Network** section.

On the menu bar of the Mac, click **Go** followed by **Connect to Server**. Alternatively, press **Command K**:

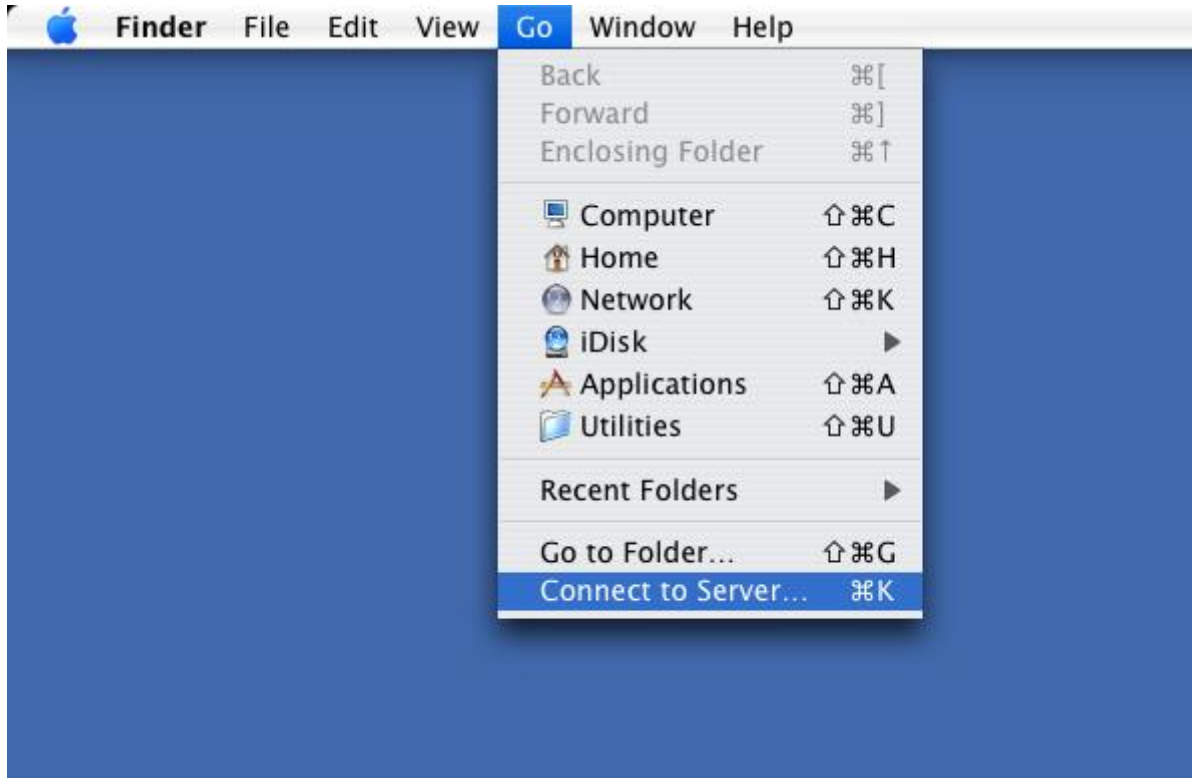


Figure 40: Connect to server from Finder

A dialog box is displayed. Enter the name or IP address of the server preceded with *afp://*

e.g. *afp://192.168.1.2* or *afp://server*

To add the server to your list of Favorites for future reference click the + button. Then click **Connect**:

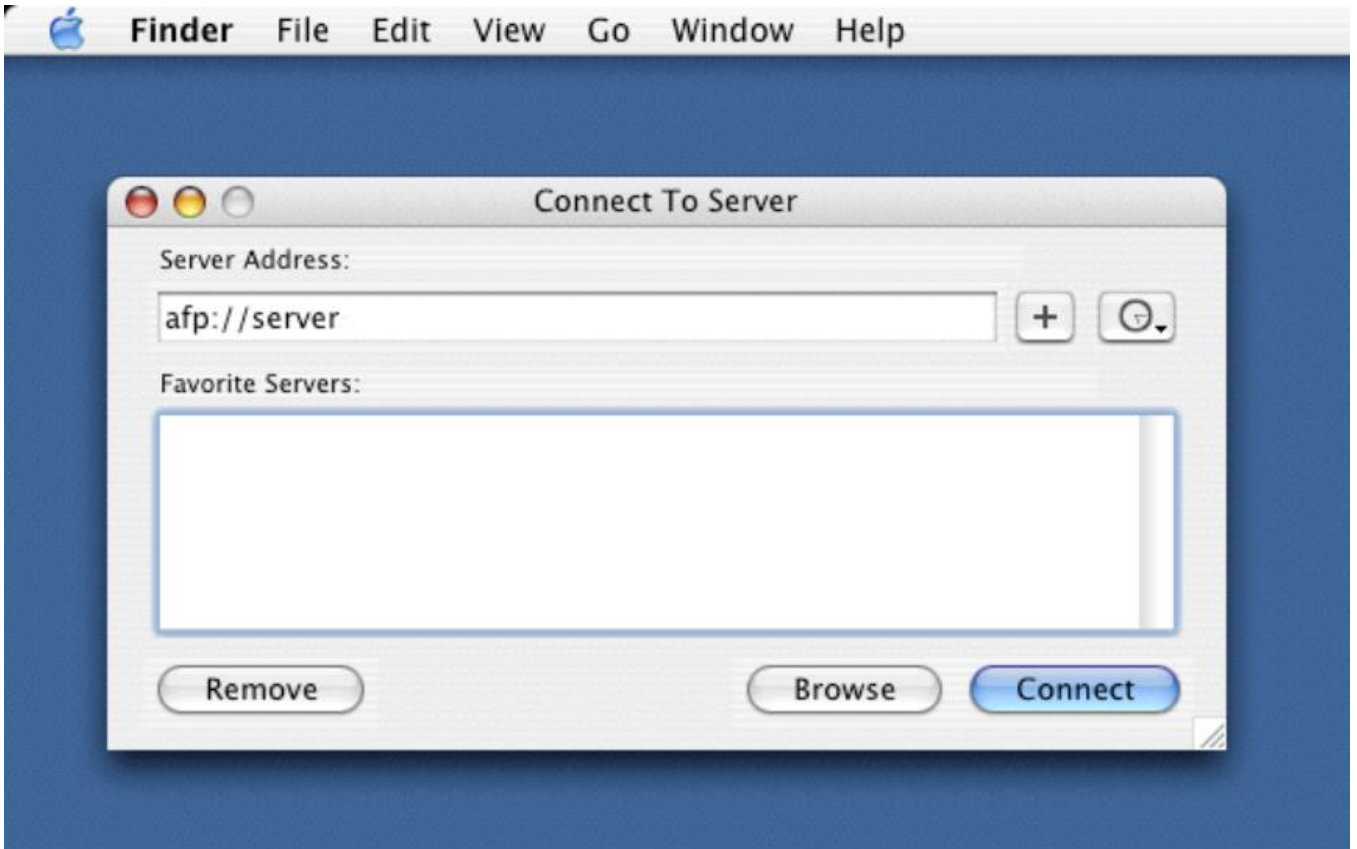


Figure 41: Specifying the name of the server

Specify the user name and password as defined on the server and click **Connect**:

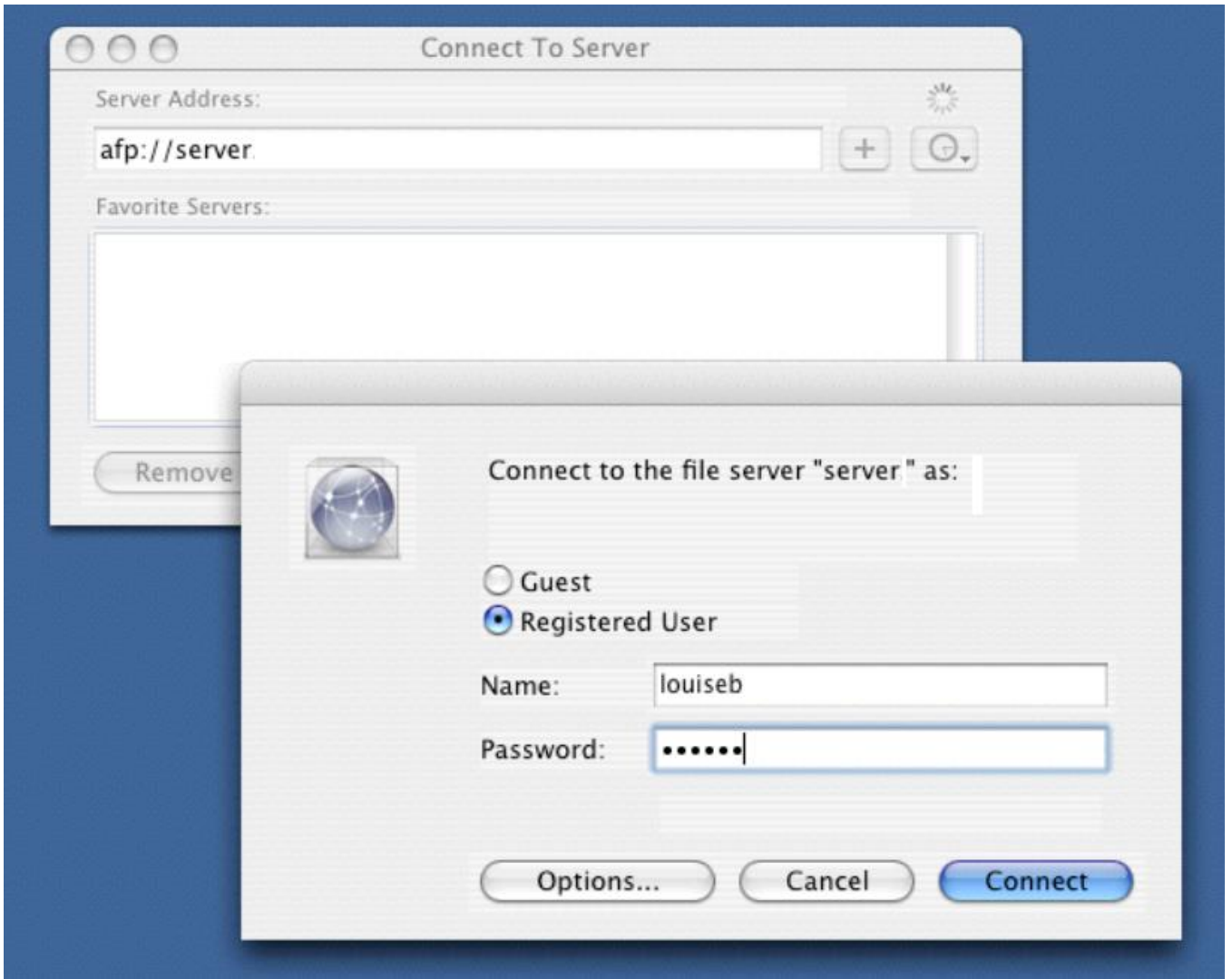


Figure 42: Enter user name and password

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

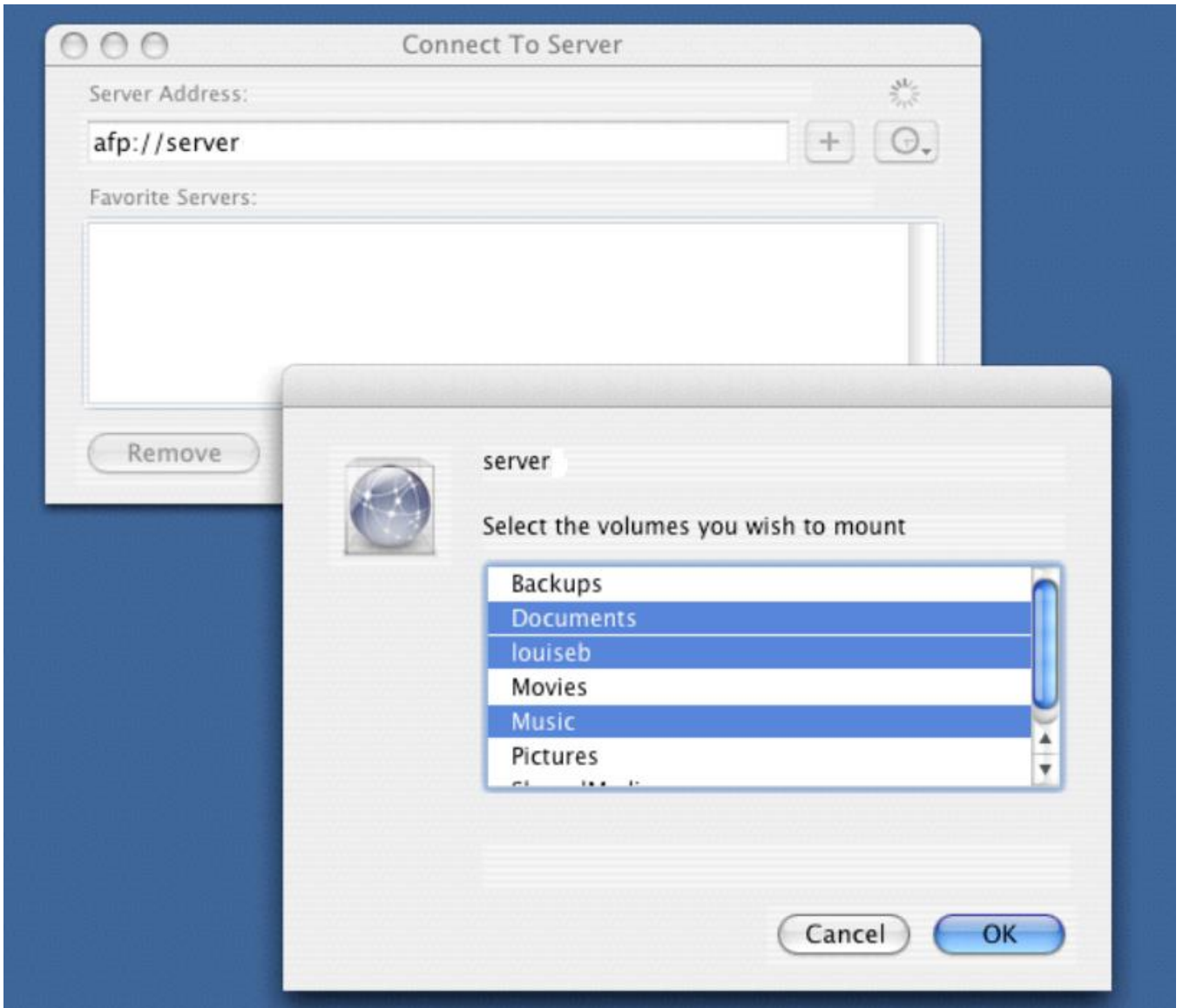


Figure 43: Select the folder(s) to mount

An icon for each mounted folder will appear on the Desktop - click it to display the contents. It behaves like any standard OS X folder:



Figure 44: Viewing contents of mounted folder

8 Multimedia & Streaming

One of the most popular uses of a home network is for the storage and playback of media such as music, photos and videos. CDs and DVDs can be “ripped” into formats such as MP3 and MP4 and these copies played back from the server, thus protecting the originals against wear and tear. The server is able to playback the stored media onto a variety of devices including computers, gaming consoles, tablets, smartphones and streaming TV devices. Note that the unauthorized copying of commercial CDs and DVDs is prohibited in most countries.

Lifeline has a built-in application called *Media Server*, which is compatible with both DLNA and iTunes. DLNA stands for *Digital Living Network Alliance*. It is a standard for interconnecting home network devices so they can stream and play multimedia. The idea 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, gaming boxes such as the Xbox and PS3, smartphones, Blu-ray players and more. The Media Server uses a third party product called *Twonky* so you may sometimes see references to this.

DO NOT COPY

8.1 Media Server

Start off by copying your music, photos and videos to suitable folders. Although several suitable folders were created during the setup of LifeLine i.e. *Music*, *Movies*, *Pictures* and *SharedMedia*, in reality this is just for your convenience and it does not particularly matter where things are stored as far as the system is concerned.

Click on the **Media Server** icon in the **Media** section. Slide the switch from the **Off** position to **On**, then click **Scan now**. This causes the Media Server to examine the entire system in order to index the music, photos and videos. This process can take some time so it runs in the background and a message to this effect is given.

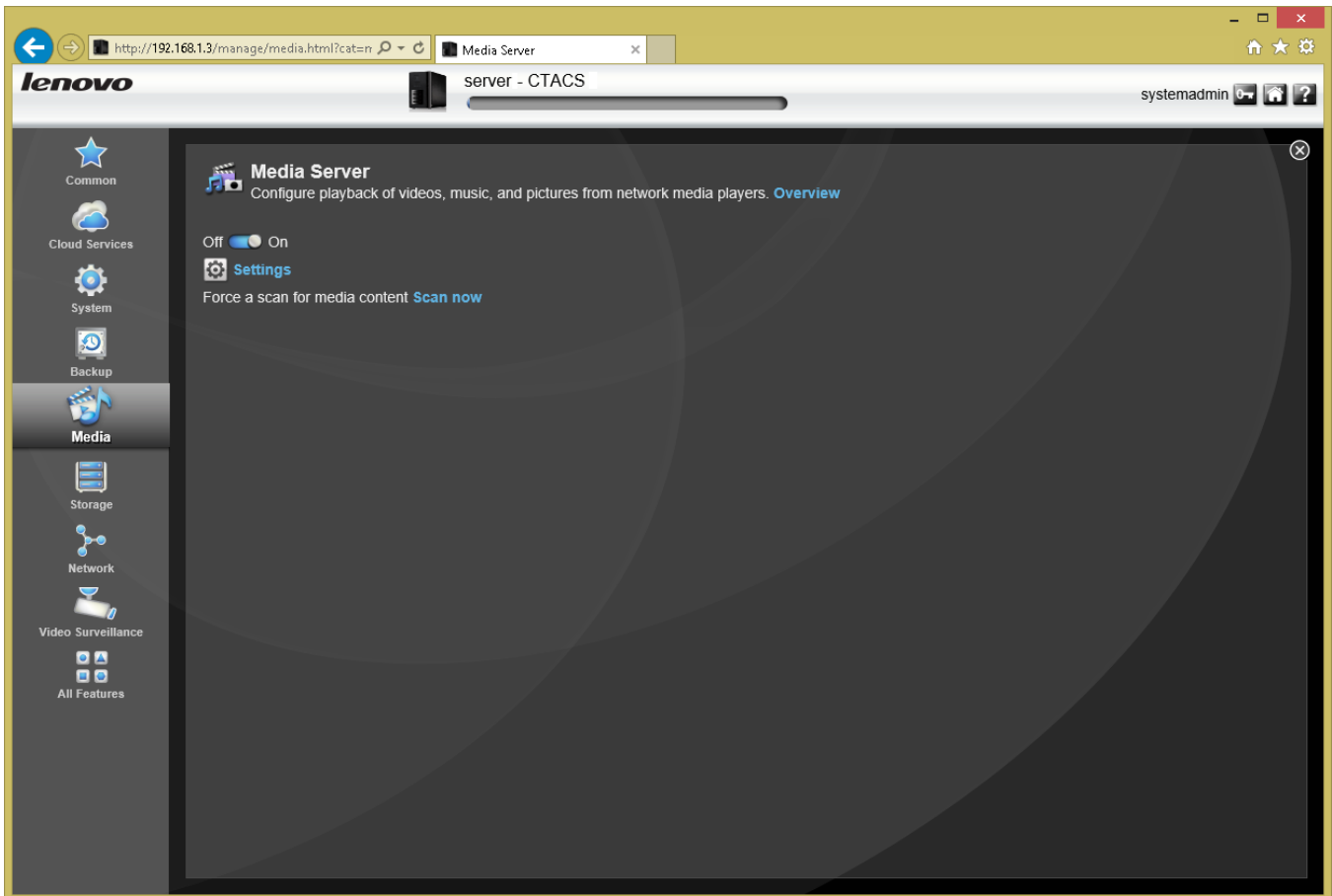


Figure 45: Media Server screen

After a few minutes you should be able to connect your DLNA client to the server. As DLNA devices vary enormously there is no single method for doing so. Some devices will just 'see' the Media Server, whereas on others 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. Note that some devices, particularly smart televisions, may be DLNA-certified but have difficulties connecting to NAS-based DLNA servers (this is usually an issue with the devices themselves, not with Media Server or Twonky).

On PCs running Windows 8.1 or Windows 7, the Media Server should be visible within Windows File Explorer as a LenovoEMC icon. To play back media, double-click it to display the sub-folders and then double-click on a file, which will cause it to play back using the computer's default application for that type of media:

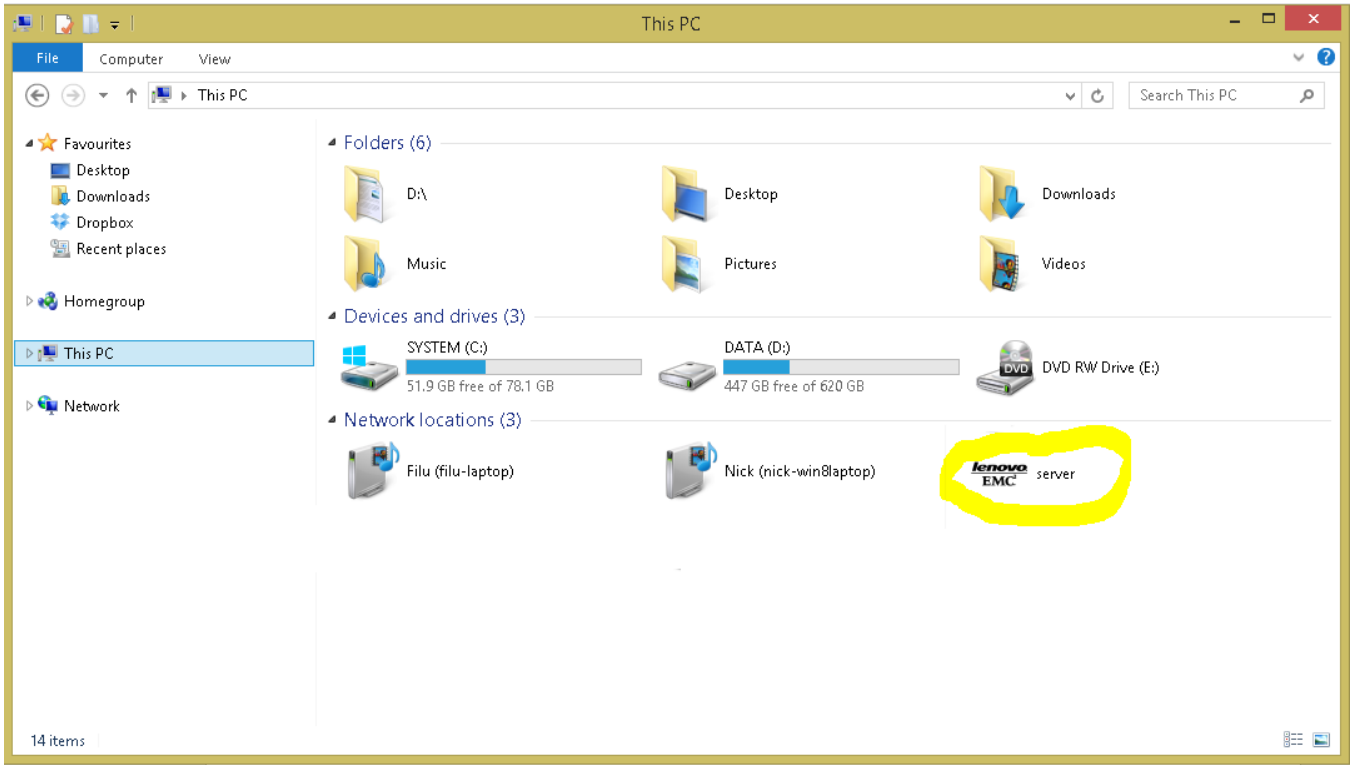


Figure 46: Media Server visible within Windows 8

8.2 Settings affecting Media Server

One of the nice things about Media Server is that ‘it just works’ so there is normally no need to change anything. However, there are some things that can be adjusted if required.

With the Media Server screen click **Settings**. There is an option called **Enable media aggregation** and if this is ticked then the panel expands thus:

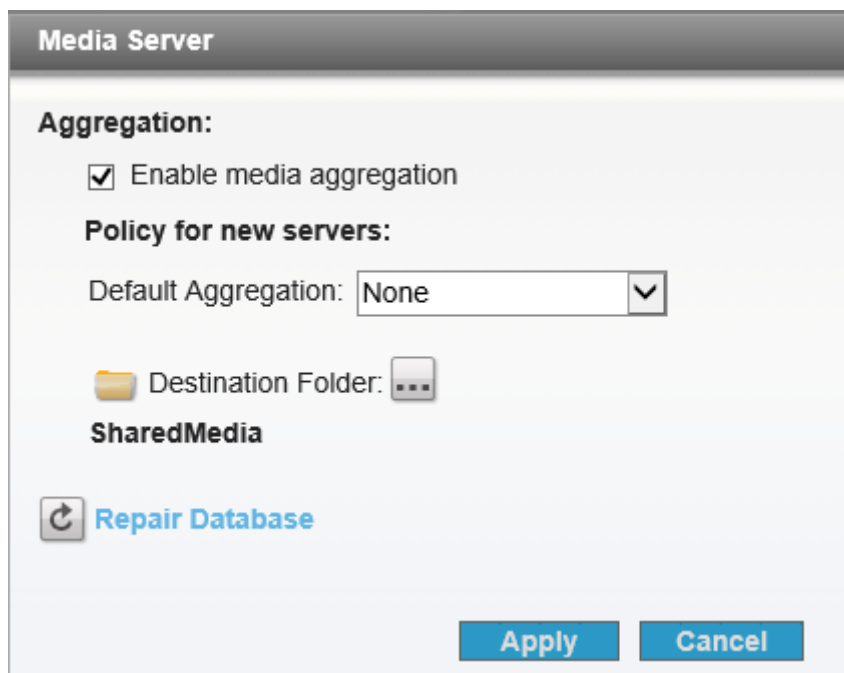


Figure 47: Media Aggregation options

If media aggregation is enabled, the server is able to interrogate any other DLNA servers on the network and gather all the photos, music and videos it finds. It can make them appear as though there is a single DLNA server, or physically copy the media back to the server. This is controlled by the **Default Aggregation** drop-down; if the media is to be copied then **Destination Folder** can be used to set the location on the server for this. This is quite an advanced feature; not everyone will need or want it but it is there if you do.

At the beginning of this section we stated that “*it does not particularly matter where things are stored as far as the system is concerned*”. Whilst this is basically true, it is possible to control what folders are interrogated on the server when it looks for media. To do so, click **Shares** within the **Storage** section to obtain a list of shared folders. Folders that have a small clapperboard icon against them are the ones that Media Server will scan:



Figure 48: Clapperboard icon

To control matters, choose a folder, expand the **Information** section and tick or un-tick the **Media sharing** box as required.

8.3 Managing Twonky

Under normal circumstances there is absolutely no need to manage the underlying Twonky server. However, this option is available for those who wish to do so. There are two ways in:

- On a Windows 7 or Windows 8 computer, double-click the icon for the server that is listed in the Media section within Windows Explorer
- On a Windows PC or Mac, enter the IP address of the server suffixed with :50599. For example, <http://192.168.1.2:50599>.

A web page for Twonky will be displayed:

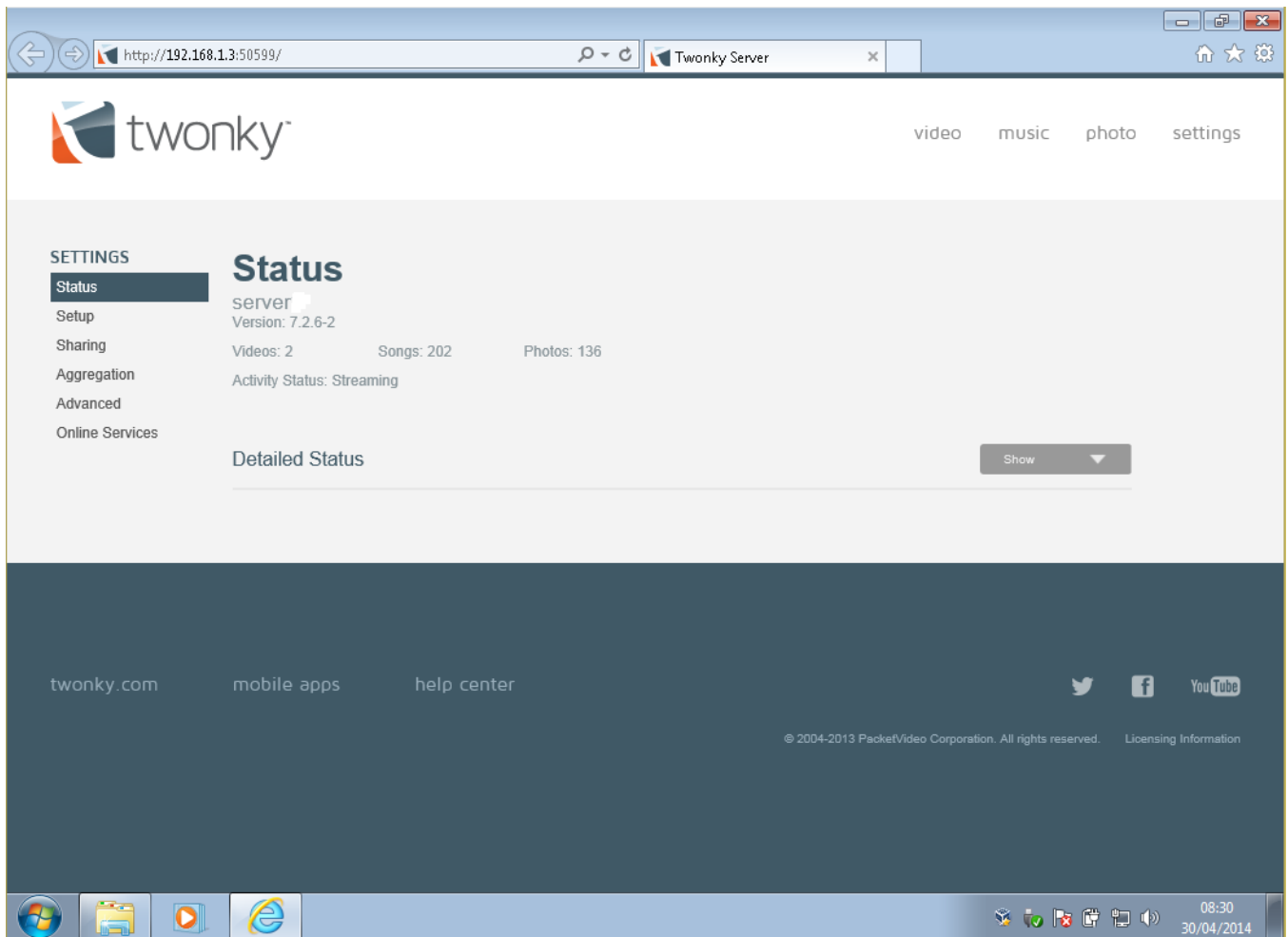


Figure 49: Main Twonky screen

More detailed information about Twonky can be found online or using the built-in help facility.

8.4 iTunes

Apple's iTunes is a popular choice for listening to music on PCs and Macs. Storing the library in a central location – the server – means the entire music collection can be made available to everyone in the household (or business!). If Media Server has been enabled as per section [8.1 Media Server](#) then music can also be accessed using iTunes.

Go to a computer that has iTunes installed on it. Click on the LIBRARY indicator in the top left hand corner of iTunes – it normally reads 'Music' – and the server will be listed under 'SHARED LIBRARIES'. Click on it to select it.

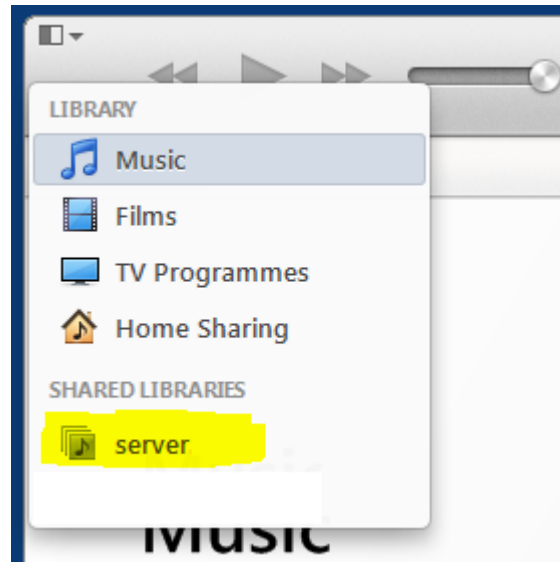


Figure 50: Connect to iTunes server from computer

The local copy of iTunes can now play the music collection stored on the server. As mentioned in the opening sentence, this works for PCs and Macs. However, due to the way iTunes operates it is not possible to directly access the shared library from an iPhone or iPad.

8.5 Picture Transfer

Picture Transfer provides an easy way to transfer photos from a digital camera onto the server and works with many popular brands of camera. The camera needs to connect to the server using an USB cable.

Click the **Picture Transfer** icon within the **Media** section to display the following screen:

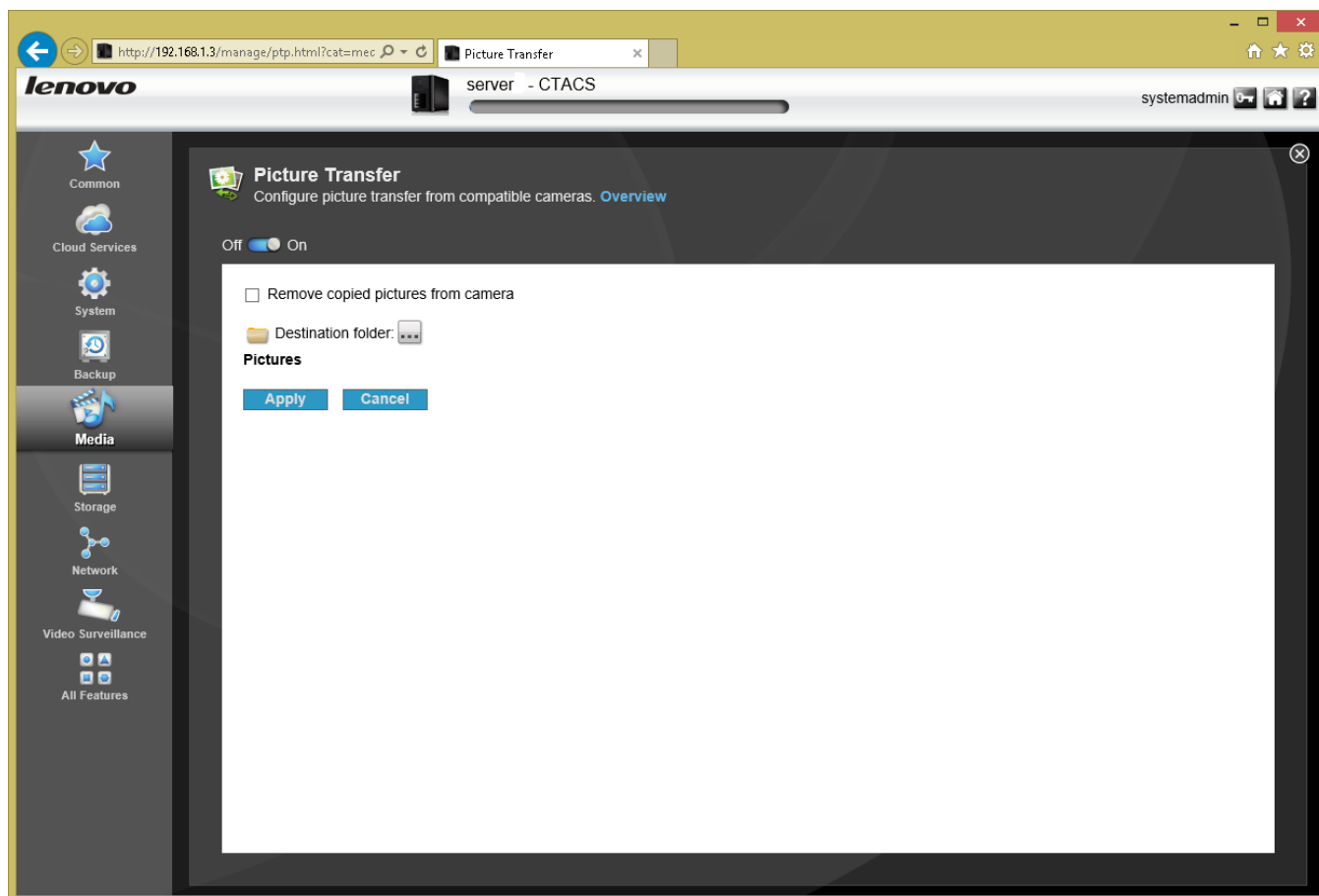


Figure 51: Picture Transfer screen

Slide the switch to the **On** position. By default, the **Destination folder** is the built-in *Pictures* shared folder, but this can be easily changed. There is also a tick-box, which will cause the photos to be automatically deleted from the camera once they have transferred.

Once the Picture Transfer function has been setup, nothing further needs to be done. When a camera is plugged in to a USB socket, the photos on it will be transferred (note: some cameras may display a confirmatory message on their display screens that has to be acknowledged first). Also, it is by no means guaranteed but the facility seems to work with many mobile/cell phones. If the phone offers a choice of mode or connection when plugged in to the server, choose the one that reads 'Image transfer' or similar.

9 Personal Cloud and Remote Working

Being able to access data remotely is an important requirement for many people and this can be done over the internet using Lenovo's *Personal Cloud* feature. Data can be accessed using computers or portable devices such as tablets and smartphones (see section [12 Connecting iPads & Other Mobile Devices](#) for additional information on the latter). When using a PC or a Mac, access to the Personal Cloud is through a browser and works in exactly the same way as described in section [7.1 Using A Browser](#).

Note: to use Personal Cloud it is necessary to have enabled security as described in section [2.8 Enable Security](#).

DO NOT COPY

9.1 Setting up Personal Cloud

Click the **Personal Cloud** icon in the **Cloud Services** section to display the main screen. The implication from the **Overview** section is that there are three stages to work through: Configure, Invite, Share. In practice you only need to do the first one:

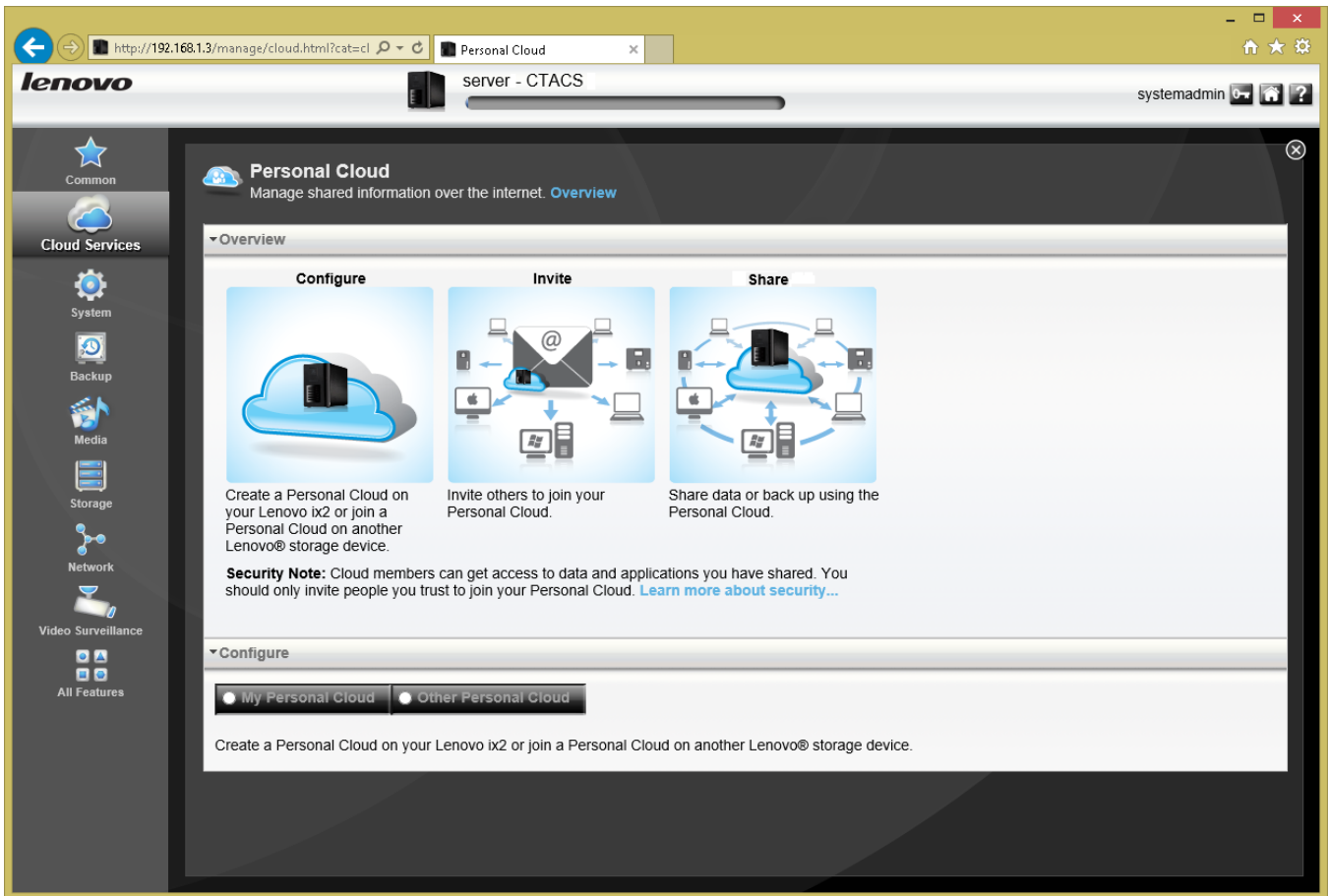


Figure 52: The initial Personal Cloud screen

Towards the bottom of the screen is the **Configure** section, with a choice of setting up Personal Cloud on this server or connecting it to a Personal Cloud running on another server. Click **My Personal Cloud**. The browser may immediately display a security warning stating that “There is a problem with this website’s security certificate”. This can safely be ignored; click the option to “Continue to the website” and the LenovoEMC Personal Cloud website is displayed:

lenovo | EMC[®] Create LenovoEMC Personal Cloud English (Europe)

Personal Cloud Name:

Email:

I have read, understand and agree with the [Security and Privacy Notes](#) associated with LenovoEMC's Personal Cloud technology. I consent to LenovoEMC using and sharing my personal information as described above and in the end user license agreement.

Next →

Figure 53: Signing up for a Personal Cloud Name

Choose a **Personal Cloud Name**. This can be whatever you want, maybe something that reflects the household or business. Note that all the obvious names - *cloud*, *Lenovo*, *server* etc. – are not available. Enter your **Email** address. After some processing, the following panel is displayed, confirming the name of the Personal Cloud plus its internet address. The address consists of the name with *.mylenovoemc.com* as a suffix. For example, if the Personal Cloud Name was *acmecompany* then the internet address would be *acmecompany.mylenovoemc.com*:

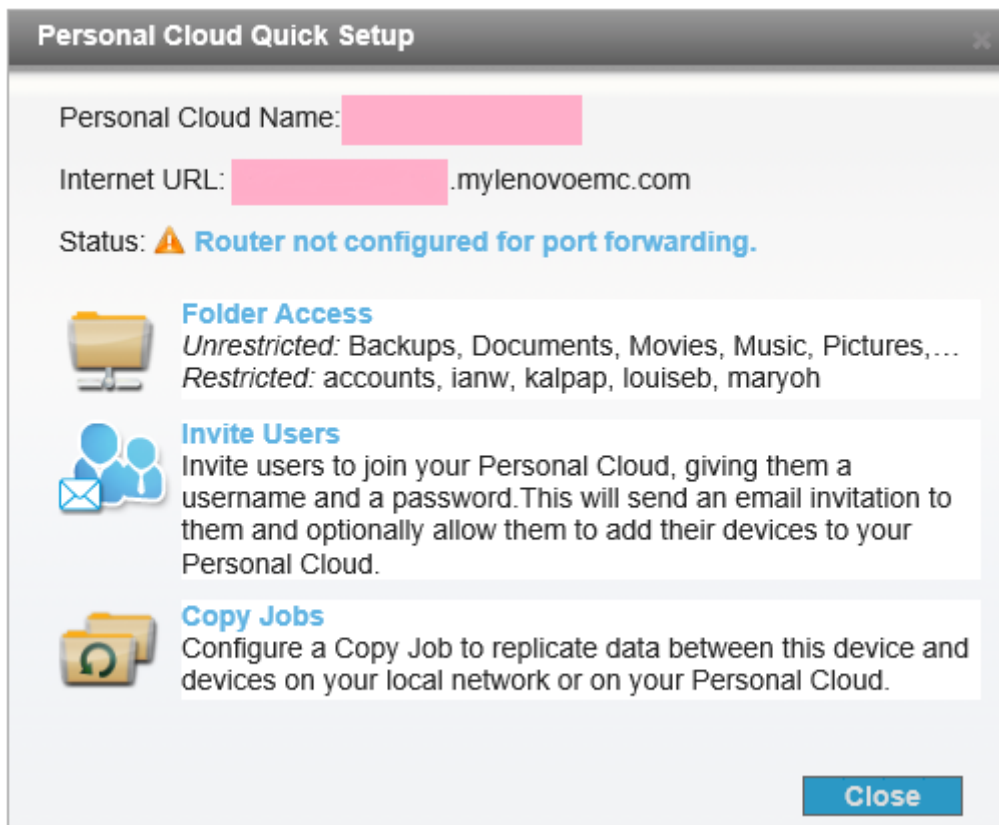


Figure 54: Confirmation of Personal Cloud Name and internet address

As part of this setup, LifeLine will have tried to setup *port forwarding* on the router and without which Personal Cloud will not work. Usually this is executed successfully but it can fail if the router is a rare or unusual model or if it does not support a feature called *UPnP port forwarding* (an example of such a router is the Apple AirPort Extreme). In such cases, the router will have to be configured manually. How to do so in detail is outside the scope of this guide as it depends upon the brand of router; however, instructions for doing so with most routers can be found at the www.portforward.com website. From a technical perspective the requirement is to forward ports 80, 443 and 50500 to the internal IP address of the server. If it proves necessary to manually configure the router, it is suggested that both it and the server are then restarted. Also, note that when going back into the LifeLine Personal Cloud screen it may still state that the “router is not configured for port forwarding” even though it actually is and is working!

The facility can now be tested from a computer. Note that when testing remote connectivity, some Internet Service Providers and some routers do not allow you to pretend to be outside the premises when you are in fact inside. To ensure things work properly, testing should be done from outside the office or home. Alternatively, use a separate internet connection, such as a mobile broadband connection or a smartphone that supports “tethering”.

Enter the internet address of the server into a browser (e.g. acmecompany.mylenovoemc.com) and the standard LifeLine Home Page should be displayed (if it is not, try disabling the firewall on the computer). If any messages relating to security certificates are received, these can be ignored. Having connected, it is exactly the same as if accessing the server locally using a browser as described in section [7.1 Using A Browser](#).

10 Backups

It is extremely important to backup data on a regular basis, in order to cope with the problems that can arise with computers. Things such as: deleting files by accident; virus infections; data corruption; computer failure; equipment being lost or even stolen. In general, the value of data far outweighs the value of computers; for instance, 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.

Backups are a bit like pay rises or happy days – you cannot have too many of them. A network attached storage system forms the ideal heart of any backup solution and enables you to take a multi-tiered approach. Basically that means there are multiple backups to multiple places, ensuring that there is always a fall-back plan in the event of problems. For example:

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

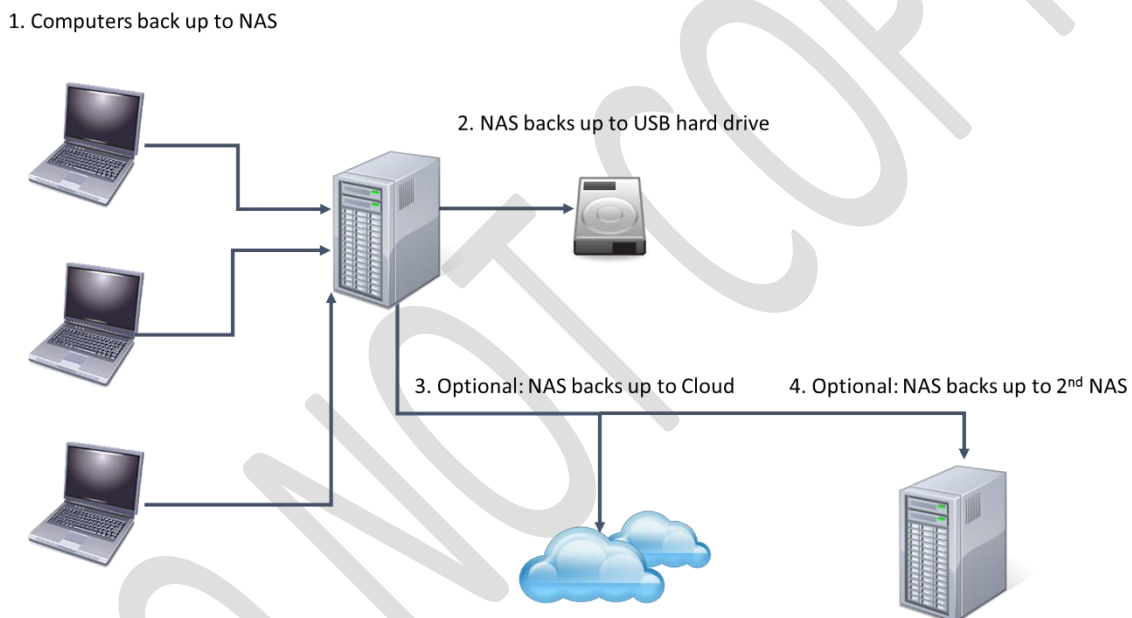


Figure 55: Example of multi-tier approach to backup

LifeLine has provision for all these types of backup. The most common scenario is to backup to a local USB drive so this is what we will concentrate on.

10.1 Backing Up the Server to an External USB Drive

The backup solution requires an external USB hard drive. This should be: USB 3.0 specification (USB 2.0 drives will work but are slower); of sufficient capacity to hold all the data (for example if there are 2TB data then use at least a 2TB drive); portable if possible (as they do not require mains power and are more convenient to store). The USB drive needs to be formatted before use. A newly purchased one is probably already pre-formatted, usually in NTFS format. If it is not then format the drive on a Windows computer.

Plug the external drive into a spare USB socket on the server. Note that on some models not all of the USB sockets are of USB 3.0 specification. Click the **External Storage** icon under the **Storage** section. Wait about 30 seconds or so and the newly connected drive should appear:

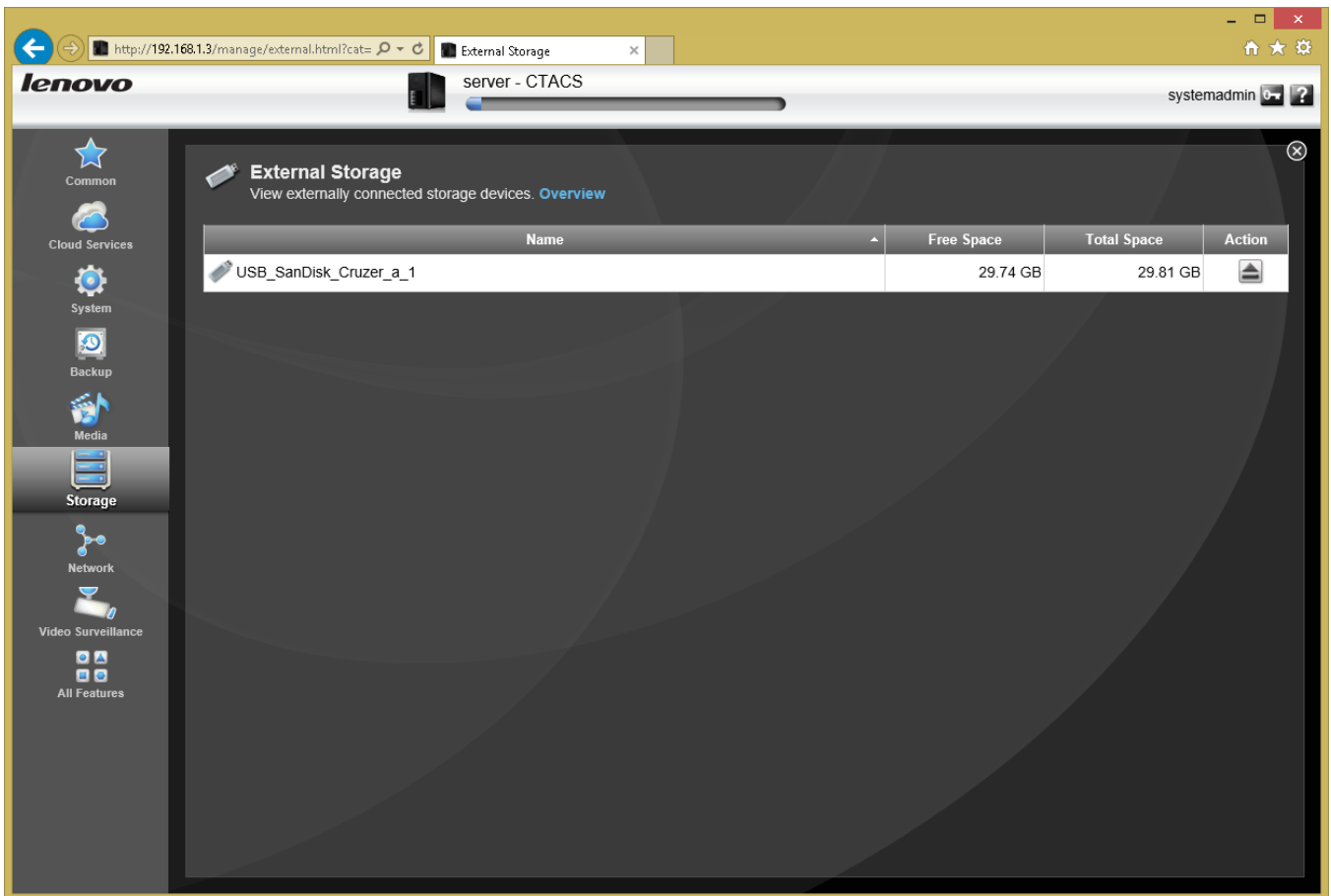


Figure 56: External Storage screen

Assuming all is well, click the **Copy Jobs** icon in the **Backup** section. Click on **Add a Copy Job** to display the following panel:

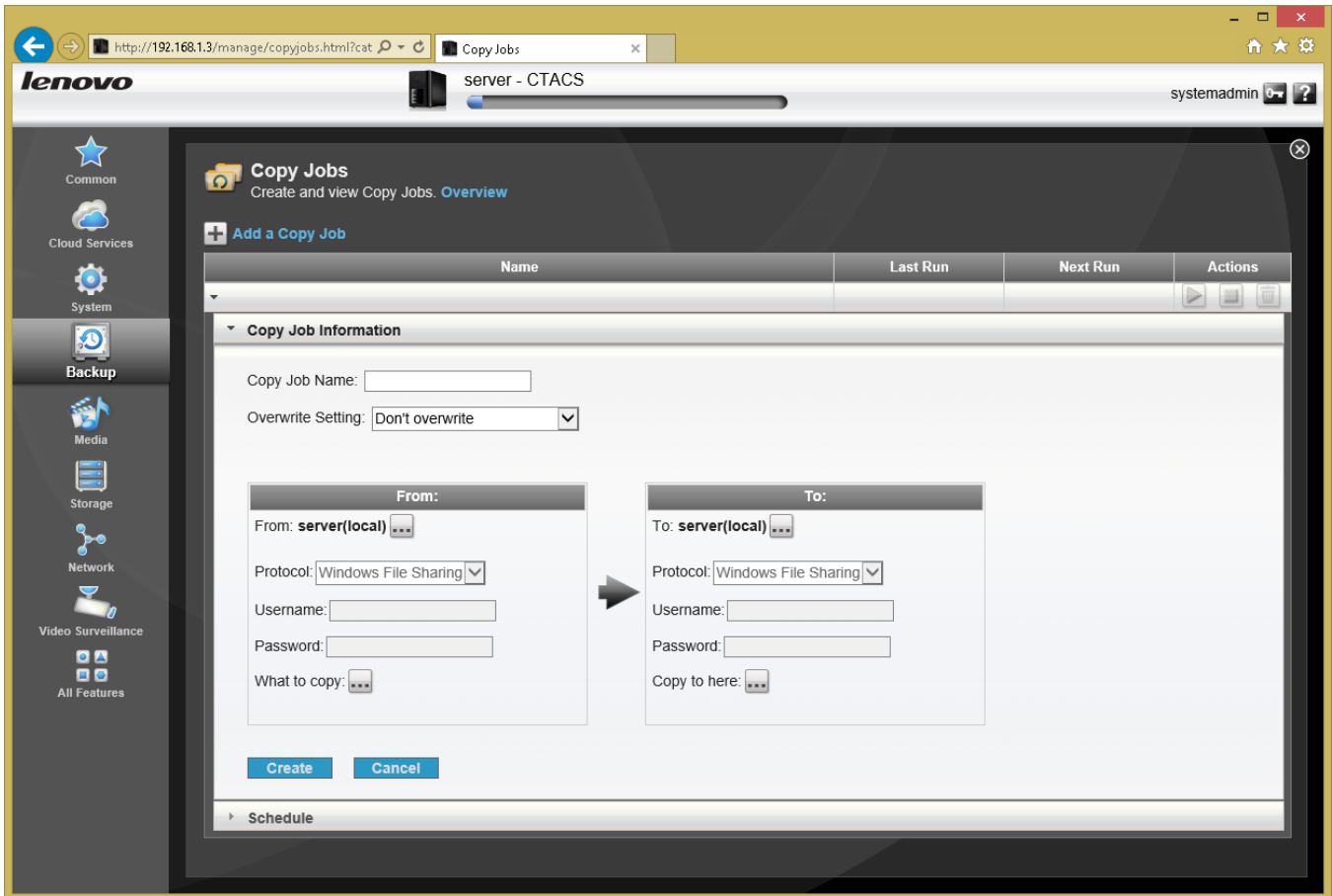


Figure 57: Defining a Copy Job

Start off by specifying a descriptive **Copy Job Name**, for example *WeeklyBackup*. Choose an **Overwrite Setting** from the drop-down – this controls what happens when you copy a file and it already happens to exist on the backup drive and there are three choices:

Overwrite and don't delete — backs up everything but if a file has been backed up before then it is overwritten with the latest version. This is the safest option.

Overwrite and delete — the backup is an exact copy of the original. This is the most understandable option.

Don't overwrite — only files that haven't been backed up before are copied. This is the quickest option.

There is no one right answer to this question as all options have their merits. In our example we will choose **Overwrite and delete**, meaning our backup is an exact copy.

We now need to specify what we are backing up from (also known as the *source*) and what we are backing up to (also known as the *destination*). The Copy Jobs tool is very flexible, inasmuch as it allows you to backup just about any device on the network to any other (you could, in fact, set it up to backup one computer to another under the control of the server). Here we will backup the server to the external USB drive. On the left-hand side of the screen, make sure that **From** is set to *server(local)*. There is no need to worry about **Protocol**, **Username** or **Password**. Click the **What to copy** button and highlight *All folders*. Then click **OK**:

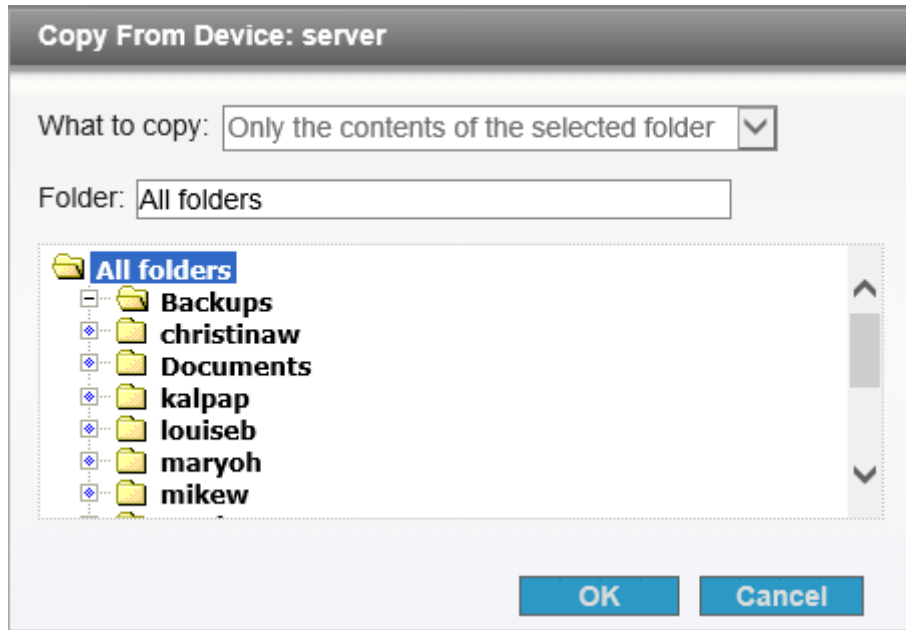


Figure 58: Specifying the source

On the right-hand side of the screen, make sure that **To** is also set to *server(local)*. Again, there is no need to worry about **Protocol**, **Username** or **Password**. Click the **Copy to here** button and highlight the external USB drive, which in this example is called *USB_SanDisk_Cruzer-a_1*. Click **OK**.

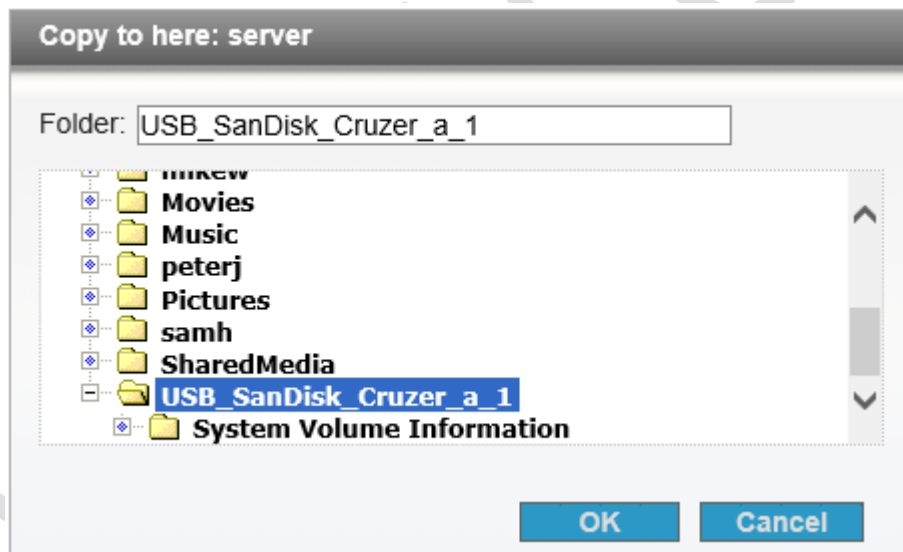


Figure 59: Specifying the destination

Click the **Create** button to create the job. Note that depending on your choices you may receive a warning message about the implications – this can be acknowledged.

You now have a choice. You can run the job immediately, or schedule it to run on a regular basis. To run now, click the run icon in the top-right hand corner of the panel:



Figure 60: “Run now” icon

To schedule the copy job, click the bottom of the screen where it reads **Schedule**, which will cause the panel to expand. Click the **Enable Schedule for Copy Job** box. Specify the day(s) and time when the job should run, then click **Apply**. In this example, it runs every Friday at 11:00pm:

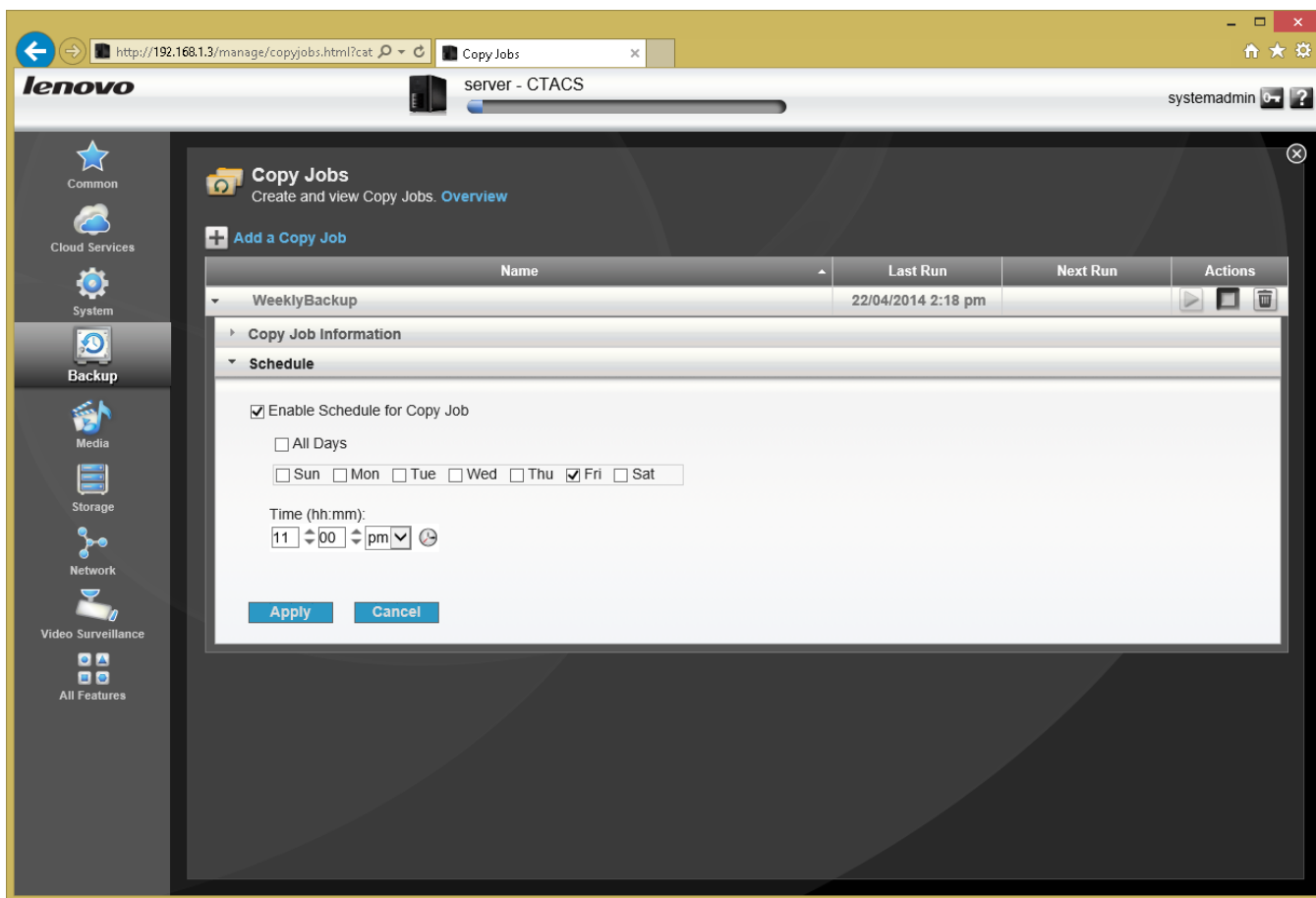


Figure 61: Scheduling a Copy Job

One thing to consider is that backing up the server may take quite a long time, depending on how much data there is. As it can have quite an impact on server performance, you may wish to schedule it to run out-of-hours or when the business or household is not busy.

10.2 Restoring Files to the Server

Should it ever be necessary to restore deleted files and folders, this can be done in two ways:

The first method is to create a new copy job that copies folders and files back from the external USB drive to the internal storage, effectively the reverse of what we setup in section [10.1 Backing Up the Server to an External USB Drive](#).

The second method is to use a computer. Access the folders on the server using the techniques described in section [7 Accessing the Server](#). Copy the contents of the external USB drive back to the folder(s) on the server that need to be restored.

The second method is more convenient for restoring small amounts of data, the first one for recovering large amounts of data in the event of serious problems, such as in a rebuild.

DO NOT COPY

10.3 Cloud-based Backup Services

As mentioned earlier, the best approach to backups is to take a multi-tiered approach involving different types of backup technology. Another important concept is *off-site storage*, whereby a copy of data is held in a different location altogether. One simple way that this can be done is through a cloud-based backup service. The huge advantage of cloud-based backups is that in the event of extreme circumstances involving the complete loss of equipment (due to fire or theft, for example) there will still be an additional copy of important data stored in a safe location.

LifeLine works with three cloud services: *Amazon S3*, *Atmos* and *Mozy*. The first two are largely aimed at large organizations but Mozy is a popular choice for home and small business users (in fact, Mozy is actually owned by Lenovo partner EMC).

To use Mozy, click the **Mozy Backup** icon in the **Cloud Services** section on the server. You can sign-up for an account online and having done so click on the **Backup** tab to define a backup job:

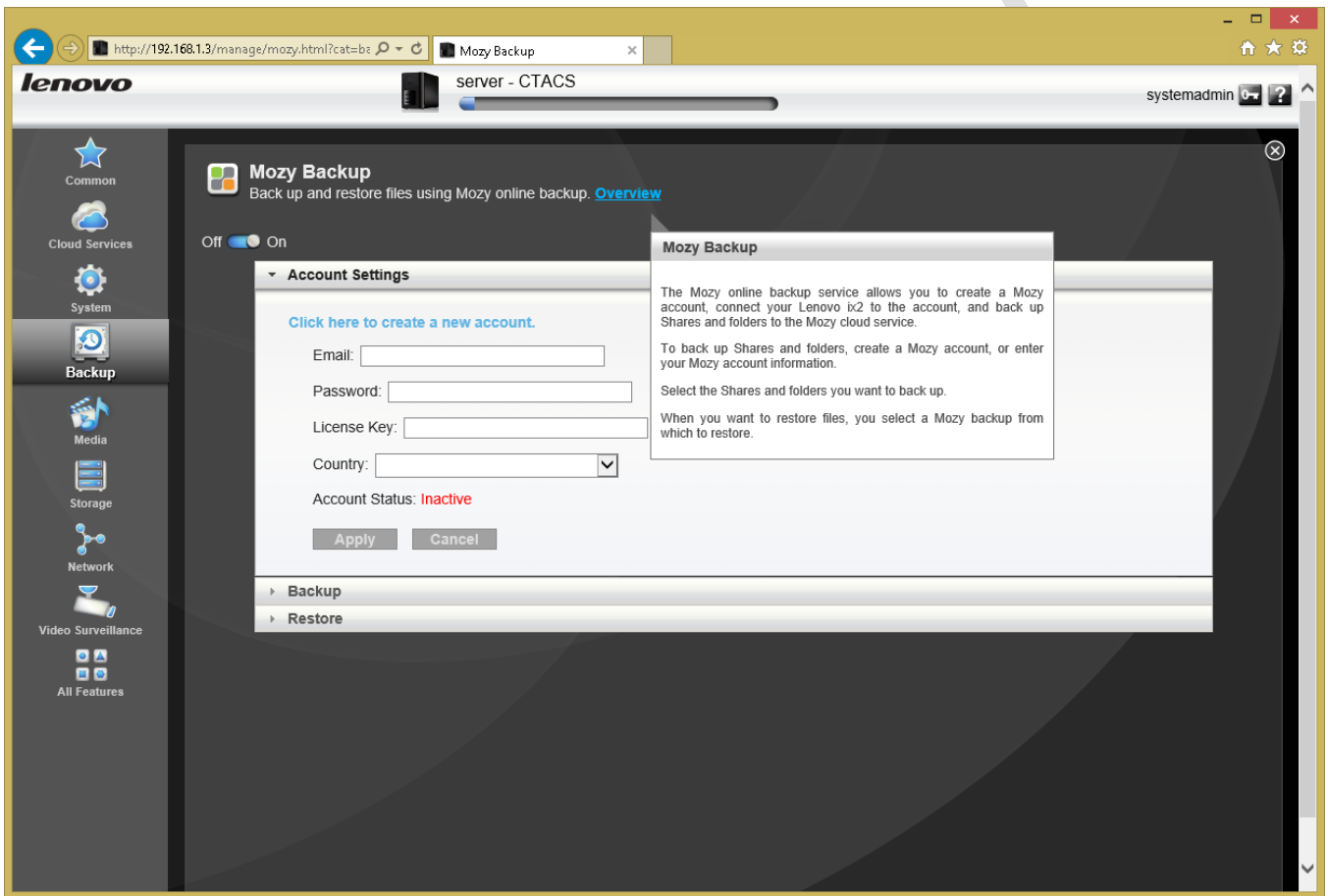


Figure 62: Enter account settings for Mozy Backup

At the time of writing, services such as Dropbox, Google Drive and OneDrive are not directly available for Lenovo network storage units.

10.4 Backing up the Server Configuration

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, settings and so on. In the event of serious problems with the server (for example, of the sort necessitating a complete re-installation), all this configuration information would have to be re-entered. This can be both difficult and time consuming on all but the simplest of systems. Fortunately, there is a facility to quickly backup and restore the configuration.

In the **Backup** section click the **Configuration Backup and Restore** icon. There are two options on the screen: **Backup Configuration** and **Restore Configuration**. Choose the former. The system will process for a short while and then prompt you to save the file it has generated (the exact message will depend upon what browser you are using). The file typically has a name of the style *Lenovo ix2_configuration_xml.icfg* or similar. Keep the file in a safe place (you might want to consider keeping a copy on a USB memory stick, for instance).

Should it ever prove necessary to use this configuration file, choose the **Restore Configuration** option and browse to the location of the configuration file when prompted. There are two options: **Restore settings** and **Restore settings and drive configuration**. The former is most commonly used, but the second option would be used if a hard drive had been changed as part of the re-build.

10.5 Backing up Windows 7 Computers to the Server

Windows 7 includes a built-in backup program. It can be used to backup important data, such as the user's Documents folder, to the server. In the event of problems with the computer, data can be restored.

Click **Start**, followed by **All Programs**, **Maintenance** then **Backup and Restore**. Click on **Set up Backup**:

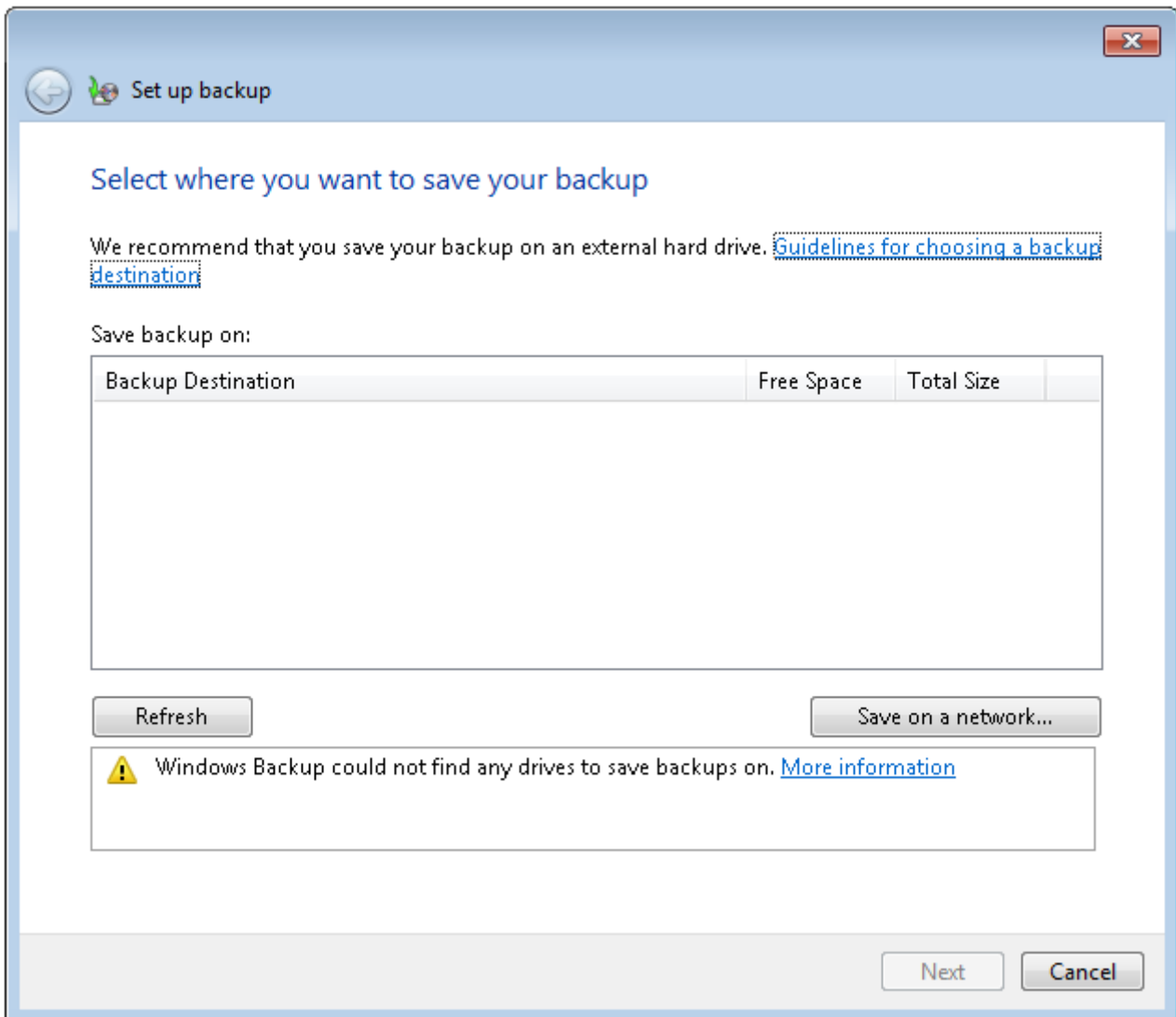


Figure 63: Choose a location for the backup

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). You could use the server's built-in *backups* folder instead, but this is not recommended as any user can access it and the multiplicity of backup files could prove confusing; in contrast, the home folder is unique and private to each person. Enter the user name and password as defined on the server then click **OK**:

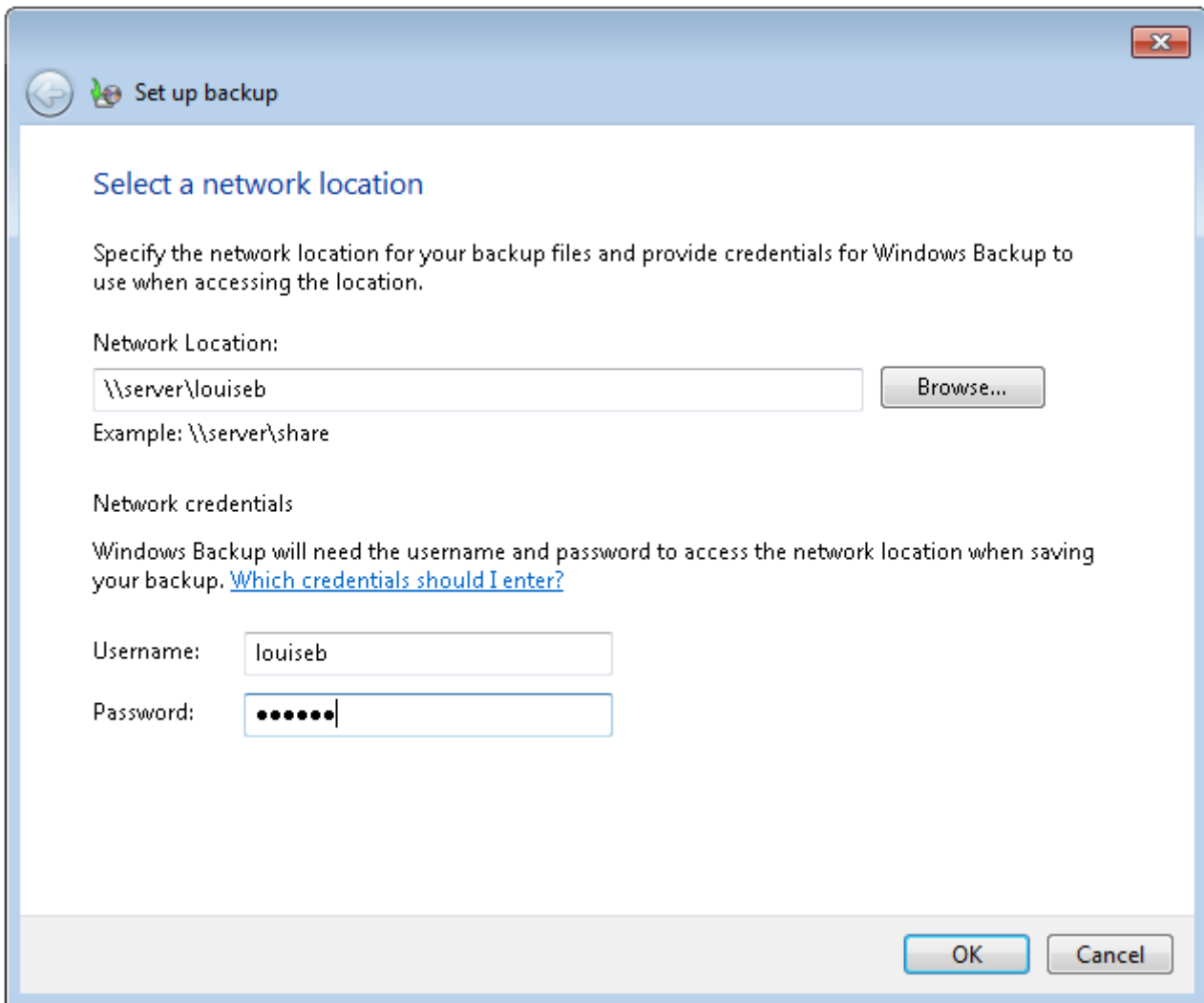


Figure 64: Specifying the network details

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

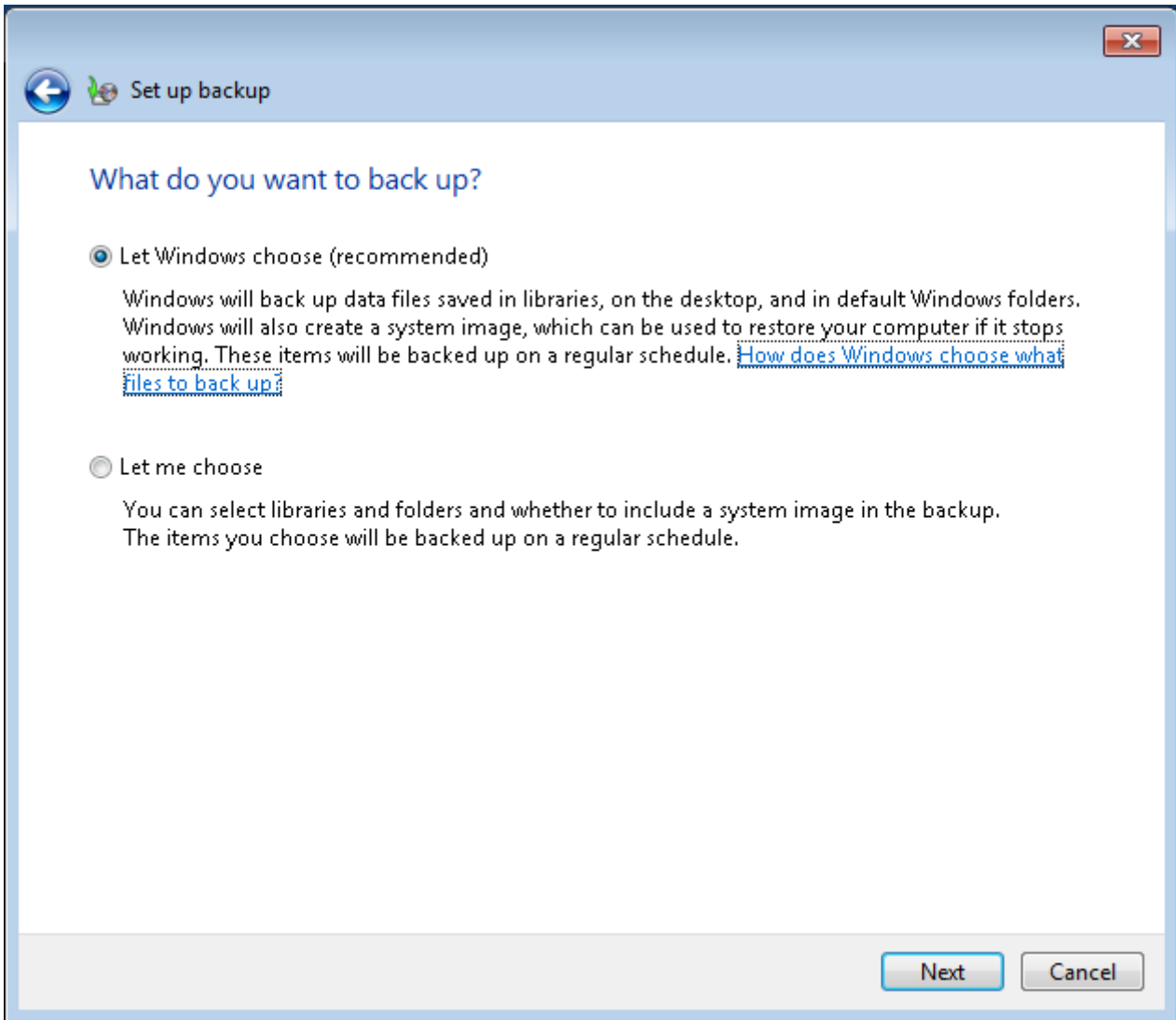


Figure 65: Choose what to back up

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

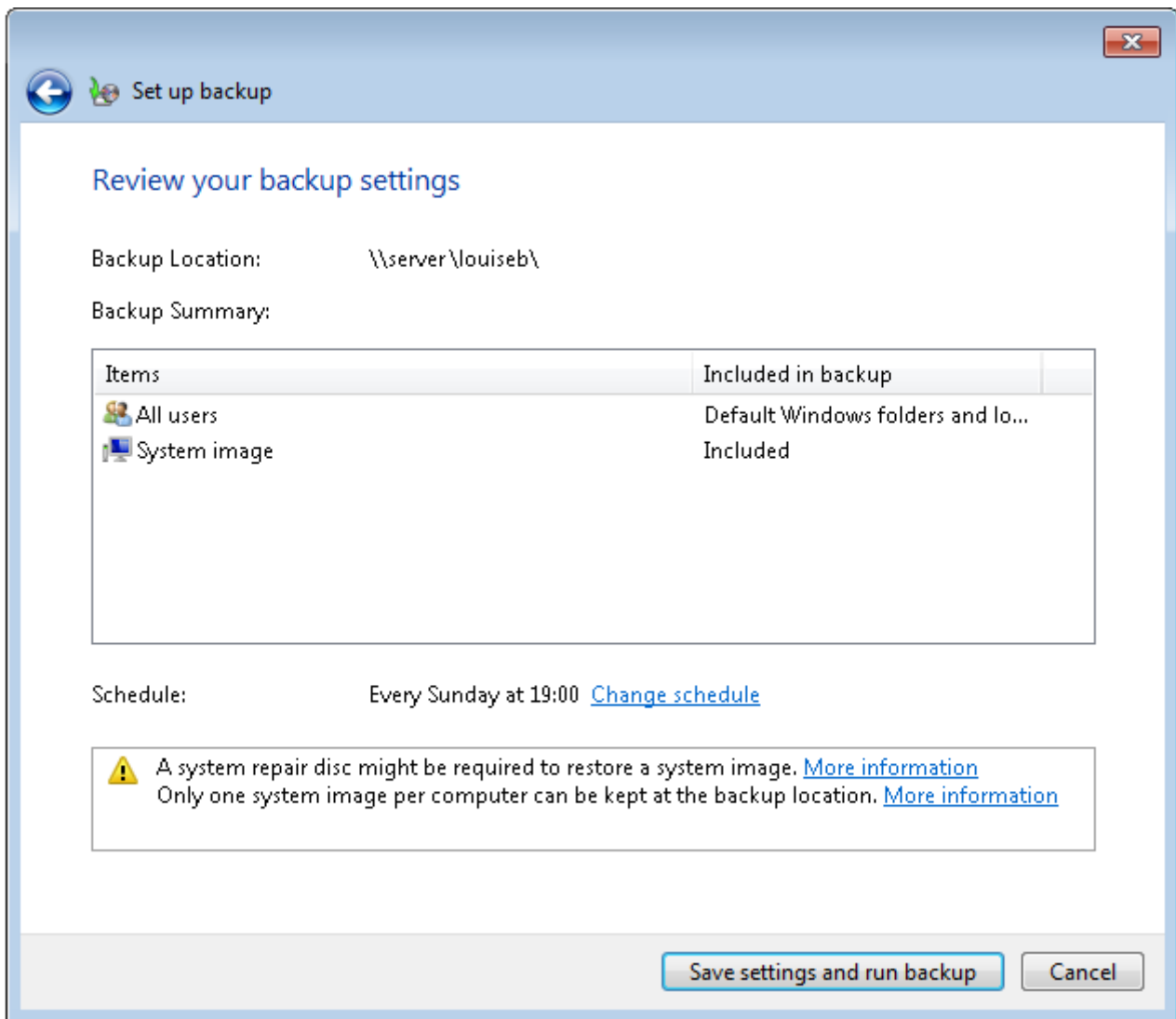


Figure 66: Summary of backup settings

The backup will run for the first time, during which the status is displayed. Windows has defined a schedule to subsequently run backups automatically on a regular basis (in this case, every Sunday at 7:00pm). If this setting is not suitable it can be changed by clicking **Change settings**.

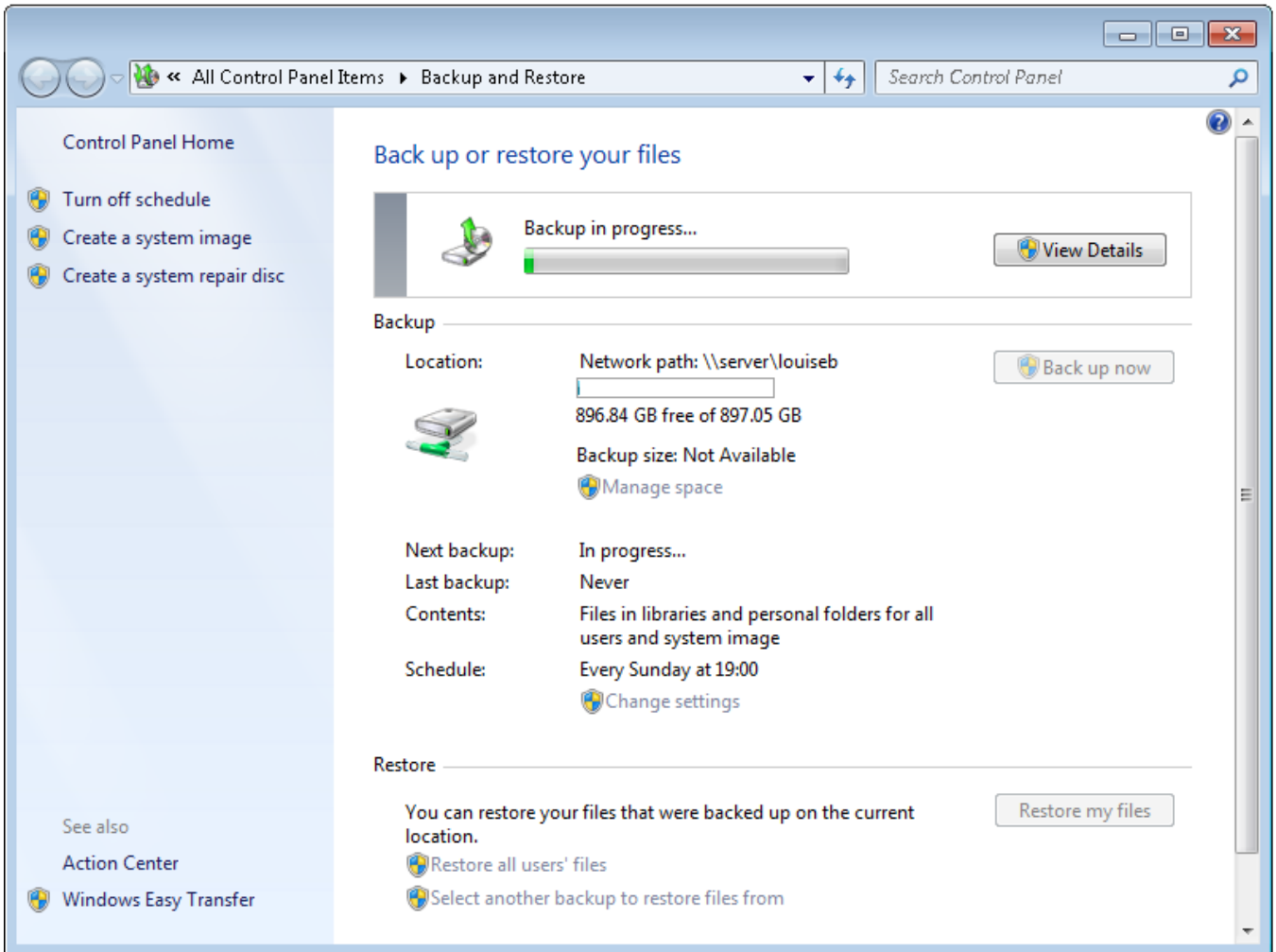


Figure 67: Backup and Restore screen

10.6 Backing up Windows 8 Computers to the Server

Windows 8 includes a built-in backup program known as *File History*. It can be used to backup important data, such as the user's Documents folder, to the server. In the event of problems with the computer, data can be restored.

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):

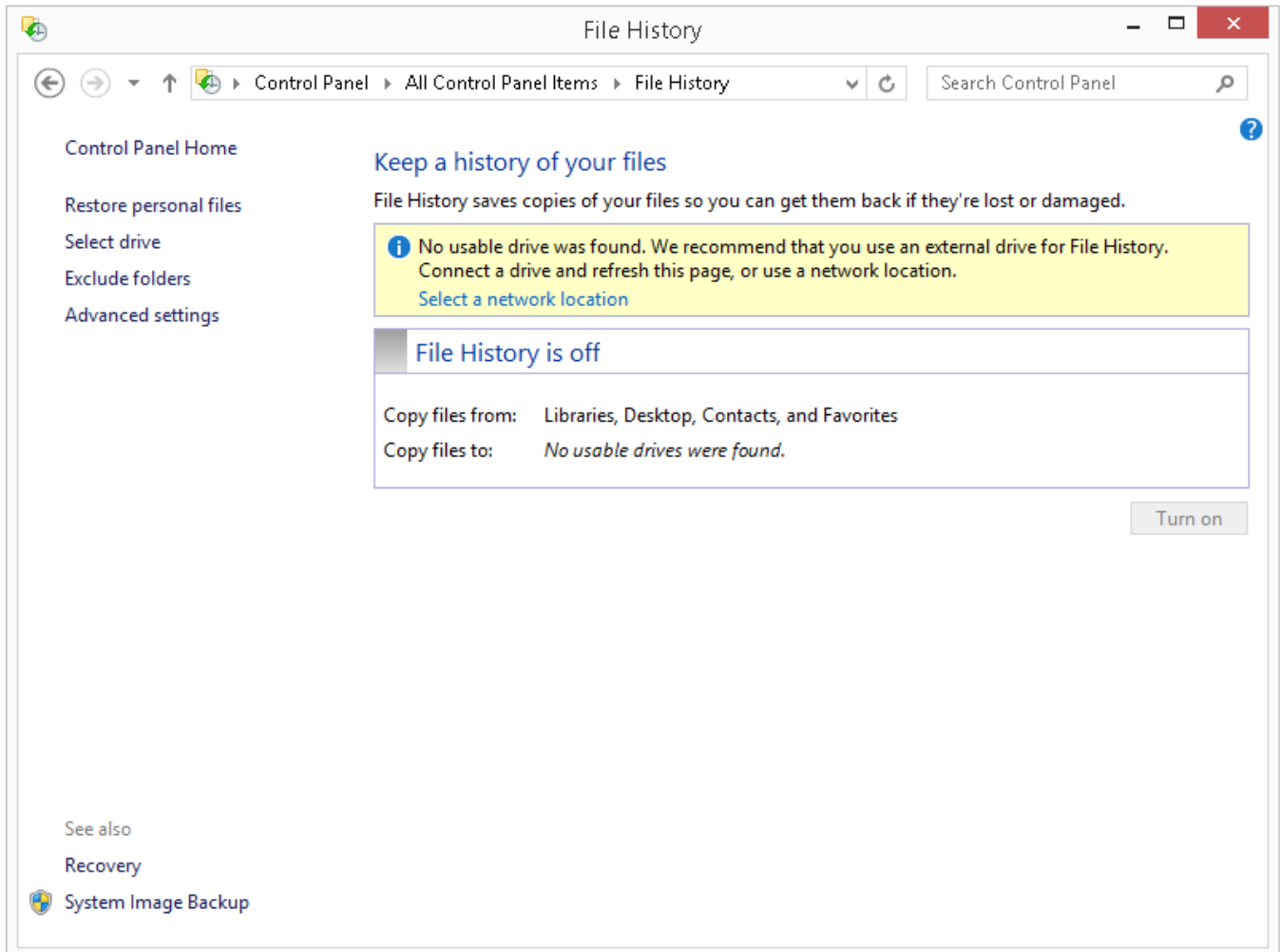


Figure 68: File History screen

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. Note: you could use the server's built-in *backups* folder instead, but this is not recommended as any user can access it and the multiplicity of backup files could prove confusing. In contrast, the home folder is unique and private to each person:

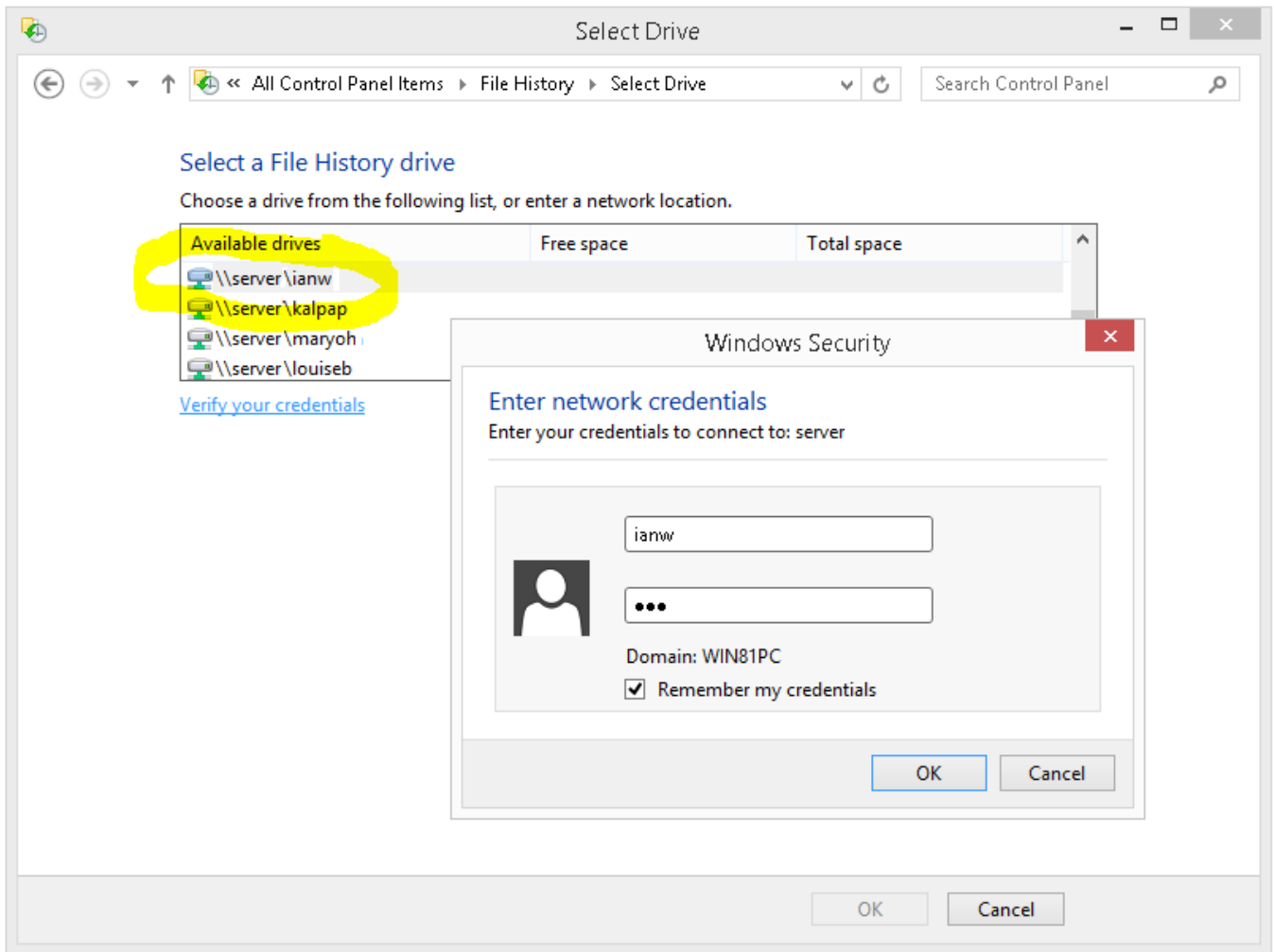


Figure 69: Specify the network destination

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**:

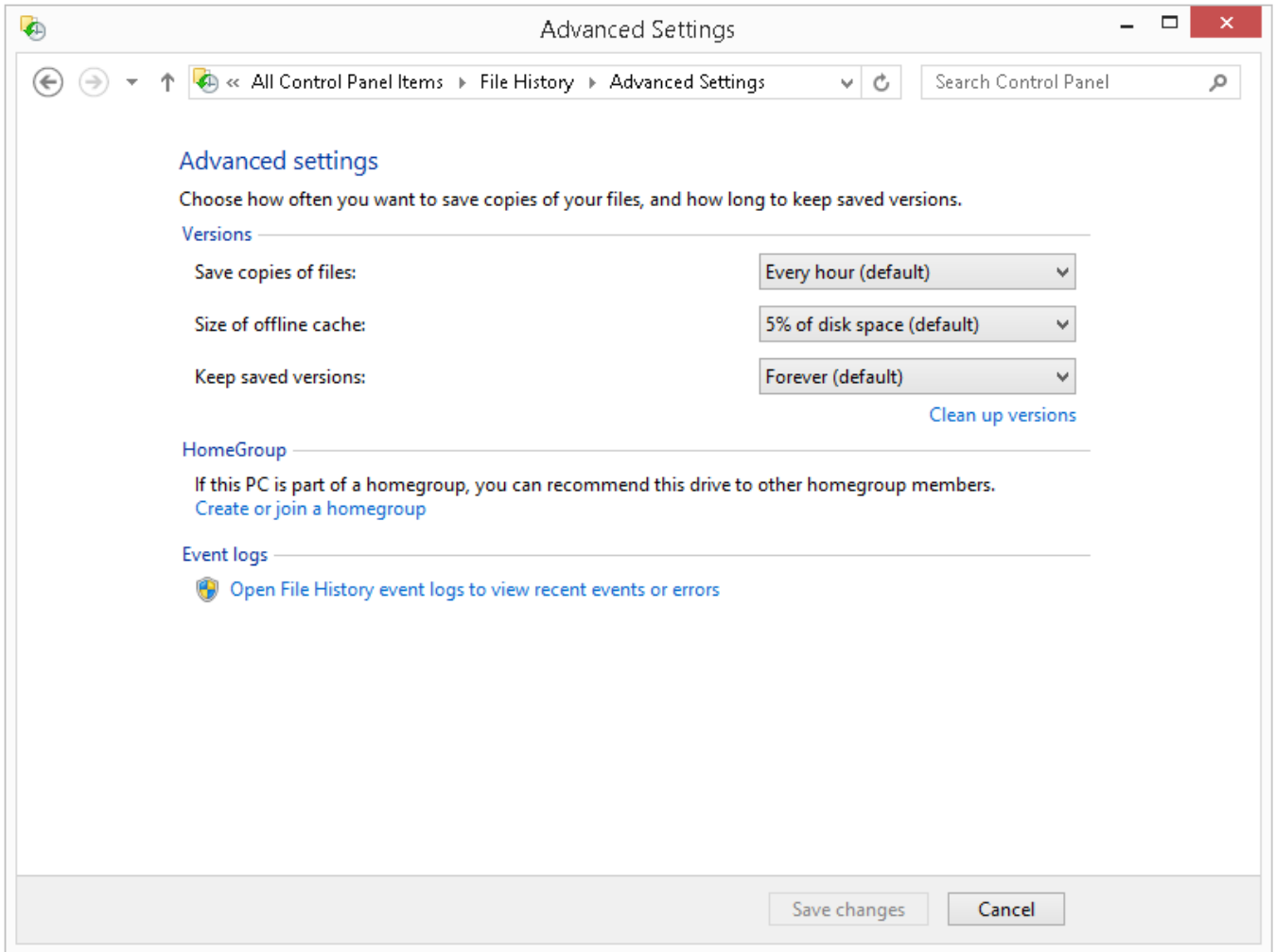


Figure 70: Advanced Settings

10.7 Time Machine for Mac Users

Apple's Time Machine is a popular backup solution for Mac users, introduced with Mac OS X 10.5. It is designed to operate with Apple's Time Capsule, a router/wireless access point/hard drive combo device. However, support is provided in LifeLine, allowing the server can be specified as a backup destination for use by Time Machine.

On the Mac, mount the server's default *Backups* folder (see section [7.6 Connecting a Mac](#) for how to mount folders). Launch *Time Machine*. Click **Select Disk** and the backup folder ("*Backups on server*") should be available. Select it and click the **Use Backup Disk** button. When prompted, enter a user name and password as defined on the server. The first time the backup is run it may take some time, but thereafter the backups should be quicker, as with a regular Time Capsule.

Problems? Make sure that Apple File Sharing has been switched on (see section [7.6 Connecting a Mac](#)) and that the user has Read/Write Access Permissions to the *Backups* folder (see section [6.2 Granting Access to a Shared Folder](#)).

DO NOT COPY

11 Printing

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

USB through Server – Many USB-only printers can be plugged directly into a Lenovo NAS, with LifeLine handling the sharing.

Ethernet or wireless independently – Many modern printers have built-in Ethernet or wireless connections, giving them an existence on the network totally independent of any server or computers.

At this stage, generally only very low cost and older printers have USB-only connectivity and most people will not want to share such printers. Also, such arrangements are something of a kludge and can be very difficult (meaning time consuming and expensive) to diagnose and fix if they do not work, such that it's not even worth bothering with in the first instance. Given that modern printers are intelligent devices in their own right and can talk directly to computers without a server acting as a middleman, this is by far the preferred solution.

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 always preferable, as performance is so much better compared to wireless.
- Configure the printer with a fixed IP address. This should be adjacent to the address of the server and well away from the addresses used by the computers. Suppose, for instance, that the internet gateway is 192.168.1.1 and the server is 192.168.1.2. If two printers were added to the network then suitable addresses would be 192.168.1.3 and 192.168.1.4
- Download the latest drivers for the printers. Consider storing the drivers on the server 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 – the 'full feature' ones sometimes have superfluous features designed to capture marketing information and sell you more cartridges. However, be aware that with some multifunction devices (combined printers/copiers/scanners) not all functions may be available in a networked environment, or may require additional software from the manufacturer to fully utilise them.

12 Connecting iPads & Other Mobile Devices

12.1 LenovoEMC Link

LenovoEMC Link is a free download from Lenovo and is available for iOS and Android. It enables users to browse and manage files and is able to playback media and view many types of files. If a user has administrative rights they can manage some aspects of the server.

When running *LenovoEMC Link* for the first time it is necessary to specify the details of the server. If you are connected locally you can let the app find your server on the network, else manually specify the name or address. If you are using *LenovoEMC Link* remotely you can enter the Personal Cloud internet address e.g. *acmecompany.mylenovoemc.com*. Then enter the user name and password as defined on the server.

There are three main sections to the app: System Status, Content Explorer and Device Management. For a standard user, System Status displays only rudimentary information. For an administrative user, the display and options are more comprehensive:

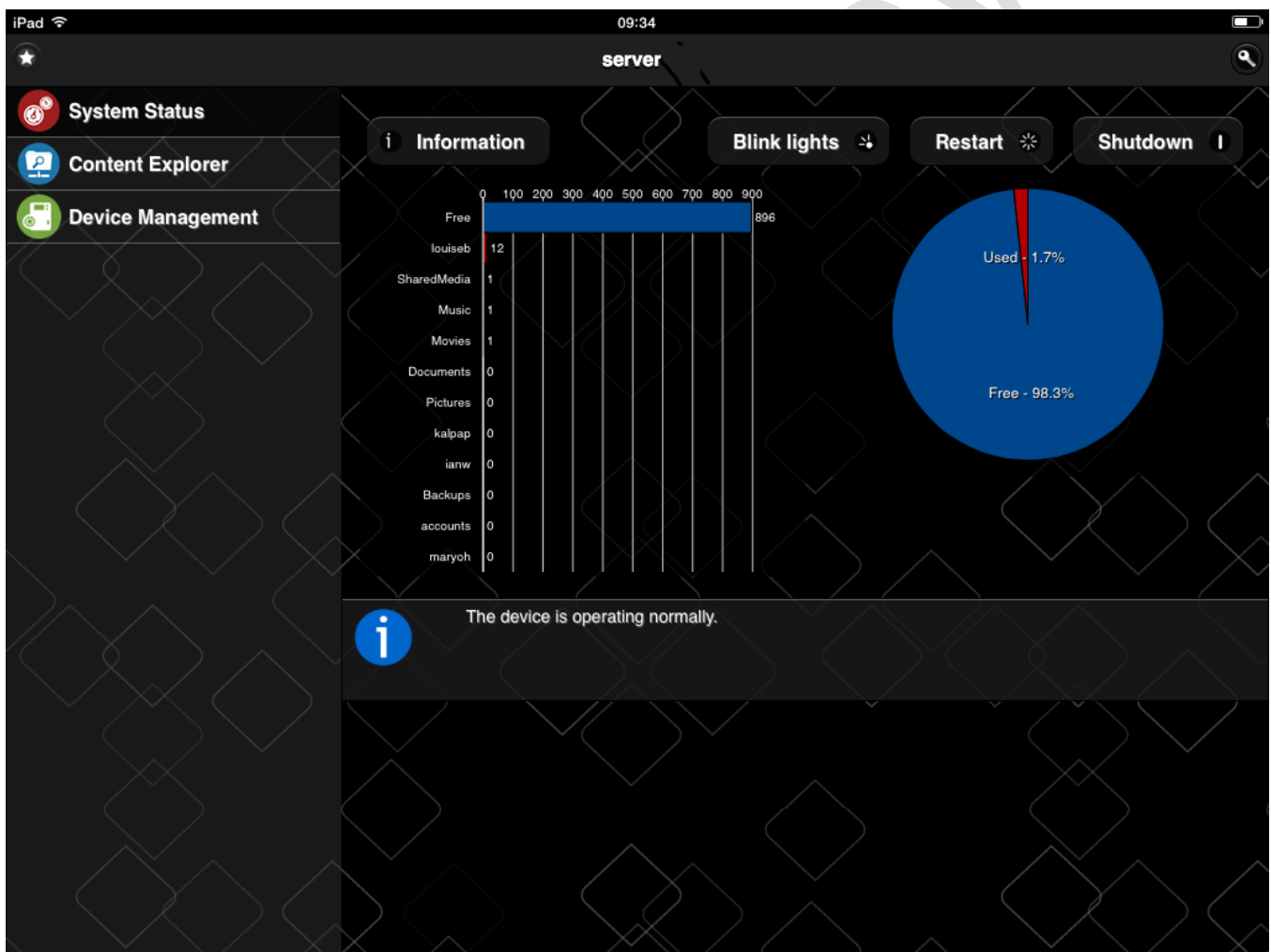


Figure 71: System Status as viewed on iPad

Content Explorer allows users to navigate through the folder structures. Clicking on a file will cause it to play or view as appropriate. Users can also create new folders and search for items:

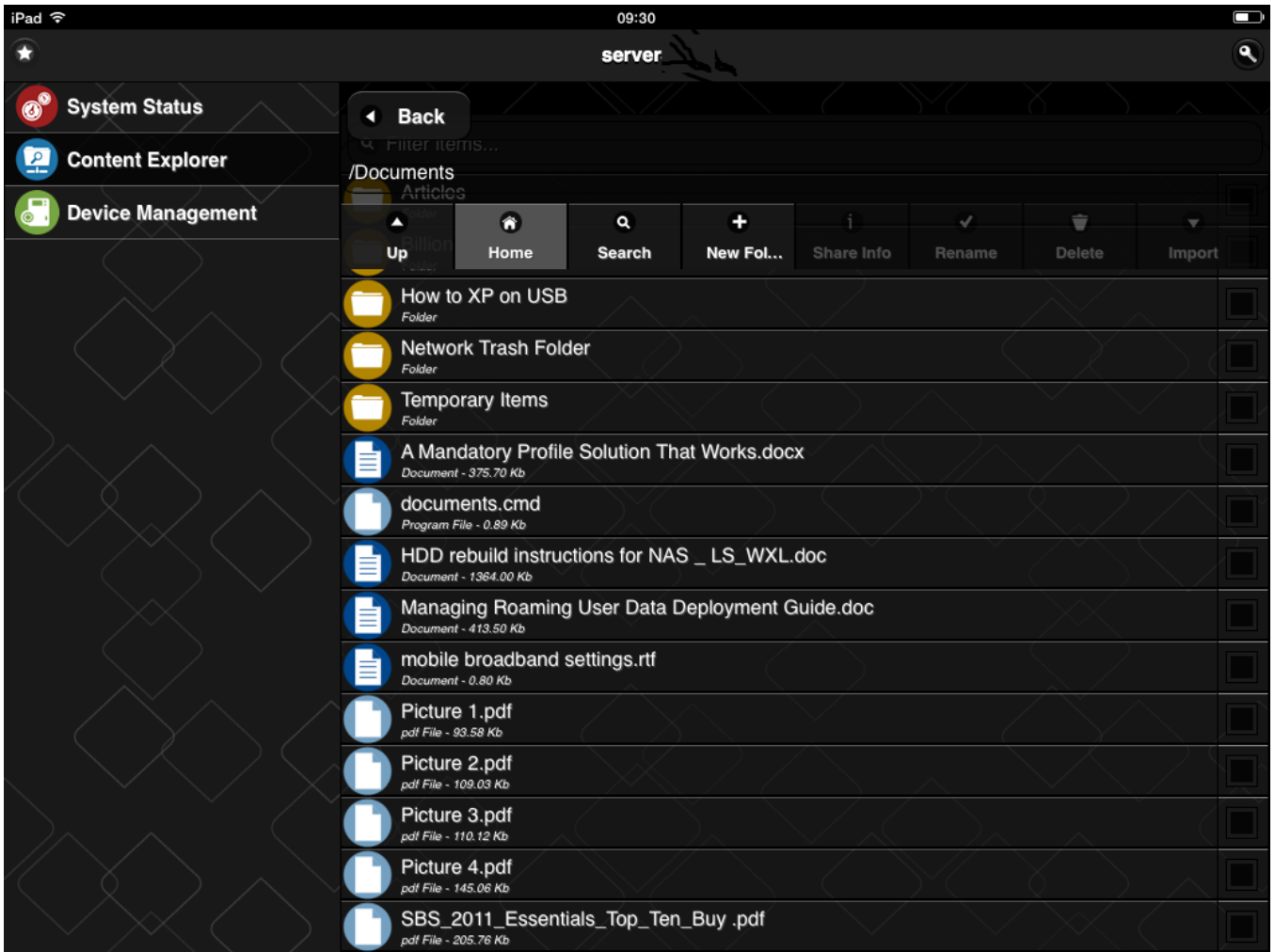


Figure 72: Content Explorer as viewed on iPad

Device Management allows an administrative user to manage some aspects of the server, such as controlling the protocols that are in use:

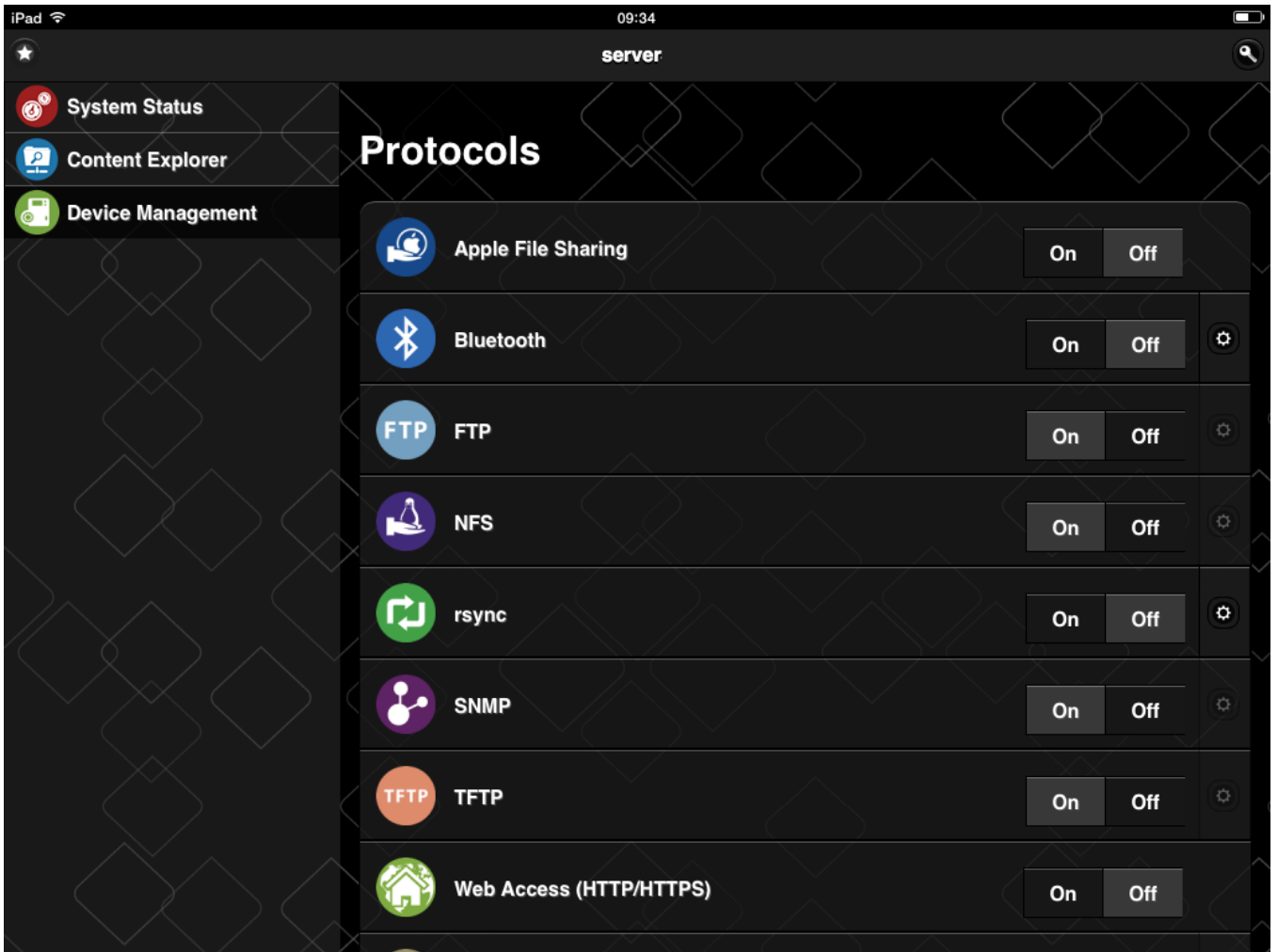


Figure 73: Device Management as viewed on iPad

12.2 File Browser

File Browser from Stratospherix is an inexpensive app for the iOS platform. It allows the shared folders of the server to be accessed and can open many popular file formats for viewing. It also has the ability to integrate with popular cloud services such as Dropbox, OneDrive and Google Drive.

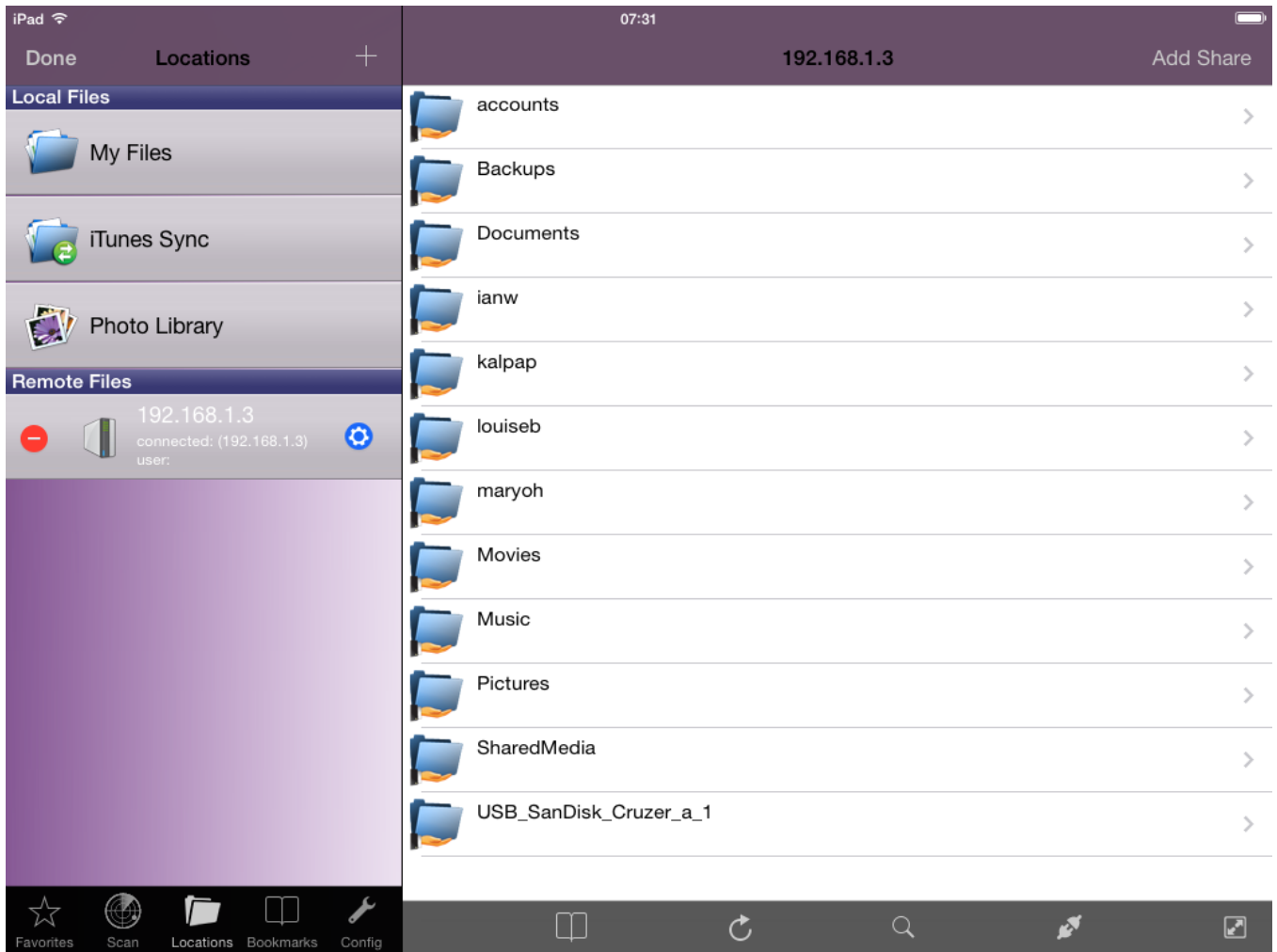


Figure 74: Using File Browser on iPad

12.4 Using a Chromebook

Chromebooks are an increasingly popular computing choice for many people. In essence a Chromebook is a laptop that only runs a browser; the underlying operating system is very minimalist compared to Windows or Mac OS X and this means it does not currently understand the storage on network attached storage devices. It is only possible to do things that can be done wholly within a browser, such as logon to LifeLine for administrative purposes.

DO NOT COPY

13 Social Media

One powerful feature of a Lenovo NAS is its ability to link directly with a number of popular social networking sites including *YouTube*, *Facebook* and *Flickr*. This works as follows:

- A shared folder – known as an *Active Folder* – is linked to a social media account
- Any files placed in the shared folder are automatically uploaded to the social media account website

Within the **Media** section of Lifeline are three icons, corresponding to **YouTube**, **Facebook** and **Flickr**. You can ignore them: they don't actually do anything useful. Instead, everything is configured using the **Shares** icon in the **Storage** section. Each of the three sites are managed in the same basic way.

DO NOT COPY

13.1 YouTube

To do this, you need an account with YouTube (i.e. a Google account as YouTube is a part of Google).

Click on the **Shares** icon in the **Storage** section. Choose a folder where the YouTube videos will be stored. In our example we will use the built-in *Movies* folder, so click on it and expand the **Active Folders** section. Tick the **Enable** box and choose *YouTube* from the drop-down list. Make a decision of what happens to the videos on the server once they have been successfully uploaded to YouTube; if you wish to have them automatically deleted click the **Delete files after upload** box (conversely, do not tick it if you wish to have them retained).

Click **Configure YouTube account access** – this will take you to the YouTube (i.e. Google) sign-on page where you need to give permission for the server to use the account:

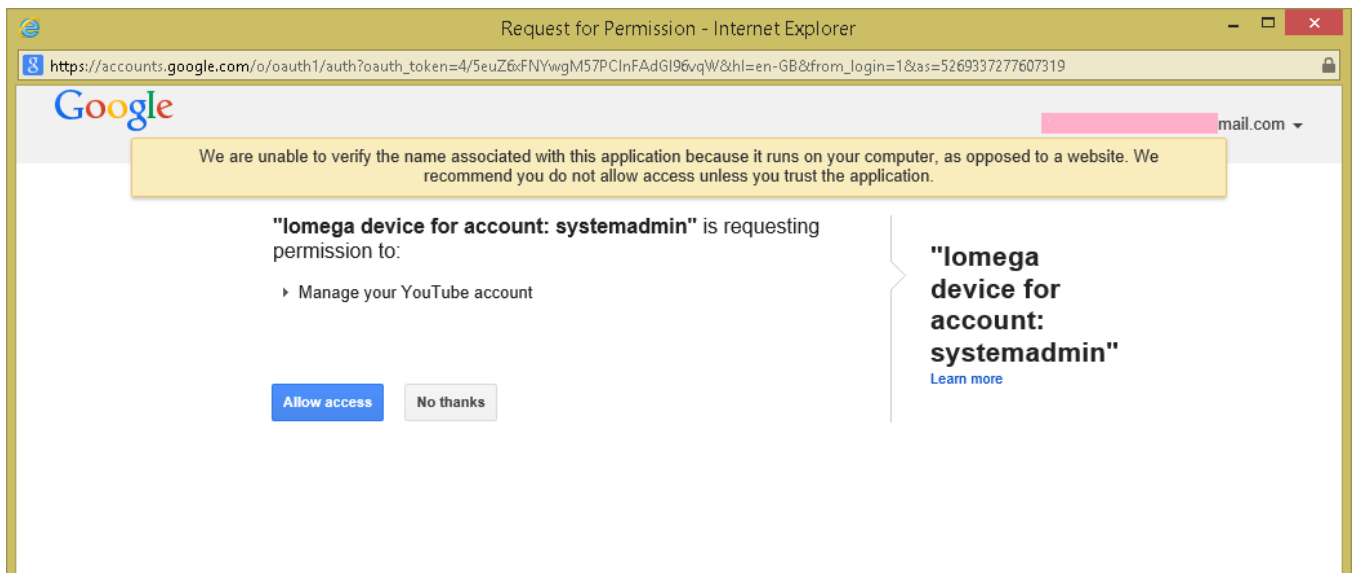


Figure 75: YouTube/Google requesting access permission

Return to the **Shares** screen on the server and click **Apply**.

Any videos now placed in the designated folder (i.e. *Movies* in our example) will be uploaded automatically to YouTube. A new option will appear in the Active Folders entry for the folder called **View transfer history** – this maintains a record of activity for the YouTube account. Note that it will now have a small YouTube icon against it to show that it is linked. To unlink it at any point, simply un-tick the **Enable** box in the **Active Folders** section.

13.2 Facebook

To do this, you need an account with Facebook.

Click on the **Shares** icon in the **Storage** section. Choose a folder where the photos will be stored. In our example, a user is going to use her own home folder, so click on it and expand the **Active Folders** section. Tick the **Enable** box and choose **Facebook** from the drop-down list. Make a decision as to what happens to the photos on the server once they have been successfully uploaded to Facebook; if you wish to have them automatically deleted click the **Delete files after upload** box (conversely, do not tick it if you wish to have them retained). Also, you can choose to have the photos automatically resized to a particular resolution, which is generally a good idea as photos from digital cameras can be quite large:

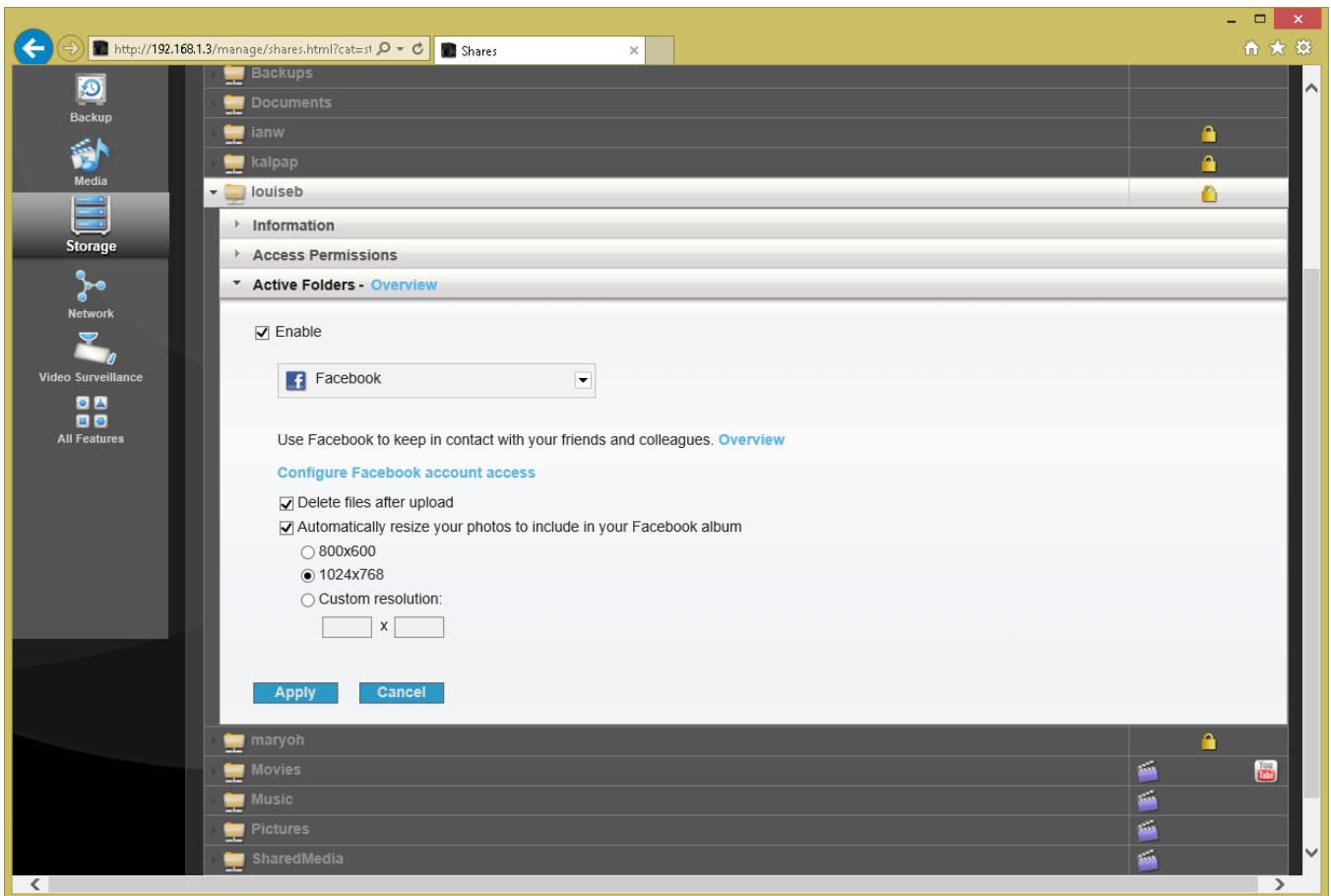


Figure 76: Facebook options

Click **Configure Facebook account access** – this will take you to the Facebook site where you need to sign-on and give permission for the server to use the account.

Return to the **Shares** screen on the server and click **Apply**.

Any photos now placed in the designated folder (i.e. *louiseb* in our example) will be uploaded automatically to Facebook. A new option will appear in the Active Folders entry for the folder called **View transfer history** – this maintains a record of activity for the Facebook account. Note that it will now have a small Facebook icon against it to show that it is linked. To unlink it at any point, simply un-tick the **Enable** box in the **Active Folders** section.

13.3 Flickr

To do this, you need an account with Flickr.

Click on the **Shares** icon in the **Storage** section. Choose a folder where the Flickr photos will be stored. In our example we will use the built-in *Pictures* folder, so click on it and expand the **Active Folders** section. Tick the **Enable** box and choose *Flickr* from the drop-down list. Make a decision of what happens to the photos on the server once they have been successfully uploaded to Flickr; if you wish to have them automatically deleted click the **Delete files after upload** box (conversely, do not tick it if you wish to have them retained).

Click **Configure Flickr account access** – this will take you to the Flickr sign-on page where you need to give permission for the server to use the account.

Return to the **Shares** screen on the server and click **Apply**.

Any photos now placed in the designated folder (i.e. *Pictures* in our example) will be uploaded automatically to Flickr. A new option will appear in the Active Folders entry for the folder called **View transfer history** – this maintains a record of activity for the Flickr account. Note that it will now have a small Flickr icon against it to show that it is linked. To unlink it at any point, simply un-tick the **Enable** box in the **Active Folders** section.

14 Housekeeping & Reporting

The server should be monitored on a regular basis to check that 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 even a daily check. Things that can be usefully looked at include:

- Checking for software updates
- Disk space
- Disk health
- Confirmation that the backup has completed successfully

Monitoring can be done in three different ways:

- Logging in and checking the System Status
- By setting up automatic notifications
- From portable devices by using the LenovoEMC Link app as described in section [12.1 LenovoEMC Link](#)

14.1 System Status Screen

Click on the **System Status** icon in the **System** section to display the following:

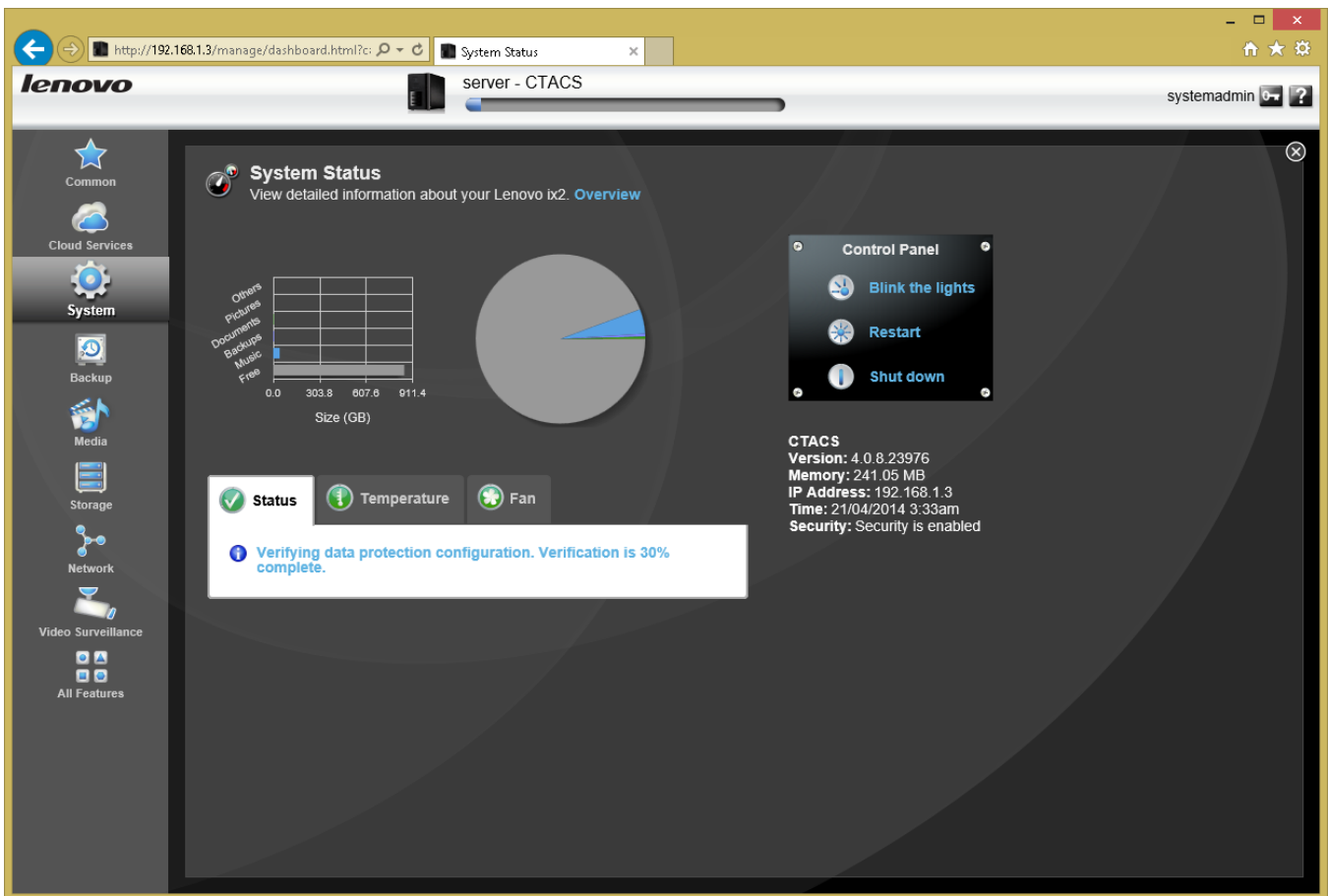


Figure 77: System Status screen

The System Status screen provides an 'at a glance' overview of the health and status of the server. The items displayed include:

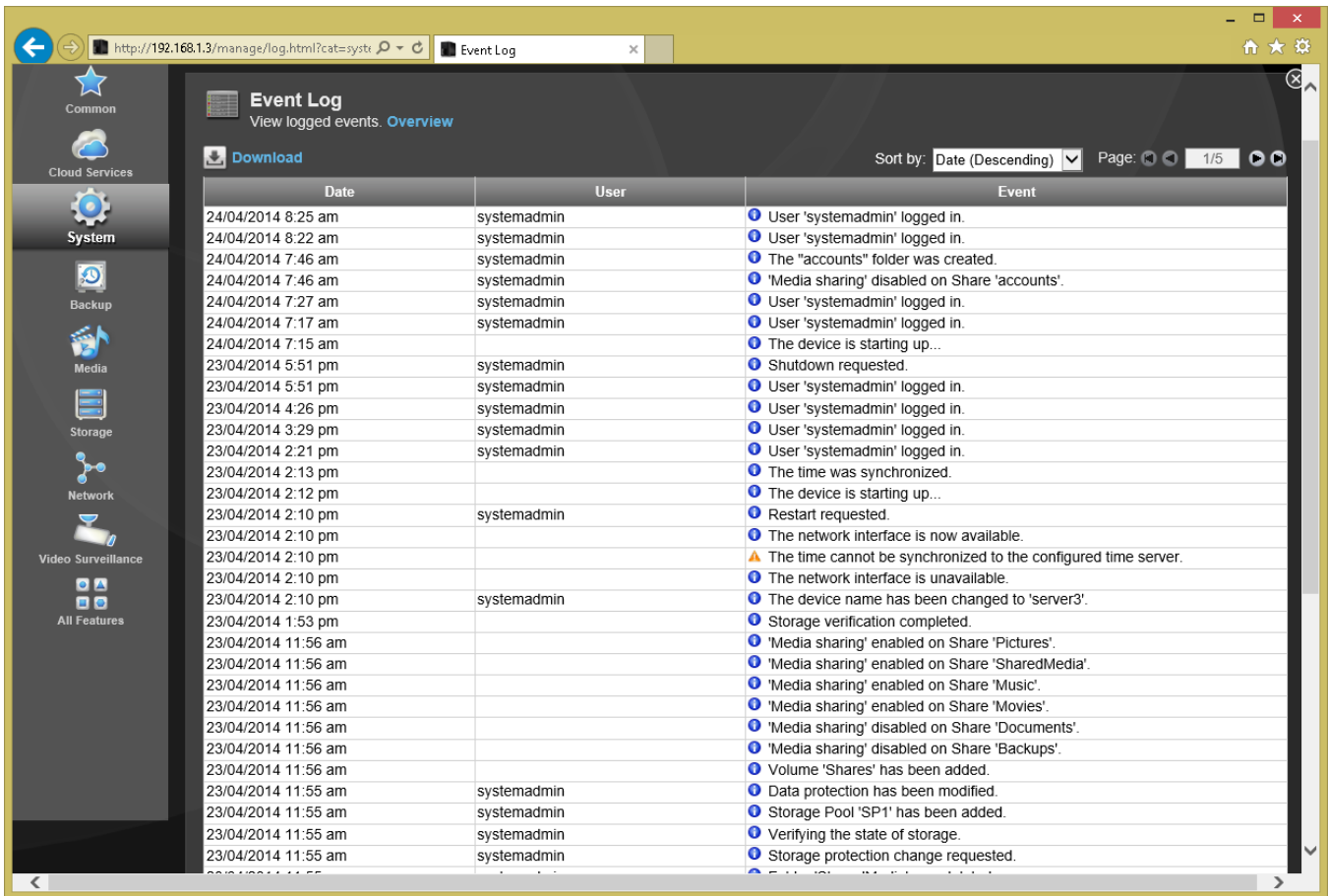
- Overall system health, including server temperature, fan speed and any recent error or activity
- Disk space and shared folder utilization
- Technical information including LifeLine version, device name, IP address and memory

The server can also be shut down or restarted from here.

One option that puzzles some people is why there is an option to 'Blink the lights' i.e. make the front lights on the unit flash. It's not intended as a party trick; the reason for its presence is that larger organizations may have multiple servers and being able to identify a particular one becomes very useful.

14.2 The Event Log

The event log records all significant things that happen to the server and as such is a useful source of information when investigating problems. To view it, click the **Event Log** icon within the **System** section:



The screenshot shows a web browser window displaying the Event Log. The URL is <http://192.168.1.3/manage/log.html?cat=syst>. The page title is "Event Log" and it includes a "Download" button and a "Sort by: Date (Descending)" dropdown menu. The table below lists the events.

Date	User	Event
24/04/2014 8:25 am	systemadmin	User 'systemadmin' logged in.
24/04/2014 8:22 am	systemadmin	User 'systemadmin' logged in.
24/04/2014 7:46 am	systemadmin	The "accounts" folder was created.
24/04/2014 7:46 am	systemadmin	'Media sharing' disabled on Share 'accounts'.
24/04/2014 7:27 am	systemadmin	User 'systemadmin' logged in.
24/04/2014 7:17 am	systemadmin	User 'systemadmin' logged in.
24/04/2014 7:15 am		The device is starting up...
23/04/2014 5:51 pm	systemadmin	Shutdown requested.
23/04/2014 5:51 pm	systemadmin	User 'systemadmin' logged in.
23/04/2014 4:26 pm	systemadmin	User 'systemadmin' logged in.
23/04/2014 3:29 pm	systemadmin	User 'systemadmin' logged in.
23/04/2014 2:21 pm	systemadmin	User 'systemadmin' logged in.
23/04/2014 2:13 pm		The time was synchronized.
23/04/2014 2:12 pm		The device is starting up...
23/04/2014 2:10 pm	systemadmin	Restart requested.
23/04/2014 2:10 pm		The network interface is now available.
23/04/2014 2:10 pm		The time cannot be synchronized to the configured time server.
23/04/2014 2:10 pm		The network interface is unavailable.
23/04/2014 2:10 pm	systemadmin	The device name has been changed to 'server3'.
23/04/2014 1:53 pm		Storage verification completed.
23/04/2014 11:56 am		'Media sharing' enabled on Share 'Pictures'.
23/04/2014 11:56 am		'Media sharing' enabled on Share 'SharedMedia'.
23/04/2014 11:56 am		'Media sharing' enabled on Share 'Music'.
23/04/2014 11:56 am		'Media sharing' enabled on Share 'Movies'.
23/04/2014 11:56 am		'Media sharing' disabled on Share 'Documents'.
23/04/2014 11:56 am		'Media sharing' disabled on Share 'Backups'.
23/04/2014 11:56 am		Volume 'Shares' has been added.
23/04/2014 11:55 am	systemadmin	Data protection has been modified.
23/04/2014 11:55 am	systemadmin	Storage Pool 'SP1' has been added.
23/04/2014 11:55 am	systemadmin	Verifying the state of storage.
23/04/2014 11:55 am	systemadmin	Storage protection change requested.

Figure 78: The Event Log

The 1000 most recent events are listed. The list can be sorted in different ways by clicking on the column headings.

If there is a need to view more events or to keep a separate records, the entire event log can be downloaded by clicking on Download. It is saved in CSV format, which can be opened by spreadsheet programs such as Microsoft Excel.

14.3 Checking The Health Of The Disks

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

Click the **Drive Management** icon in the **Storage** section to display this screen (note: if you have changed the RAID configuration as described in section [4.1 How to Change the RAID Level](#) then you may already be familiar with this screen):

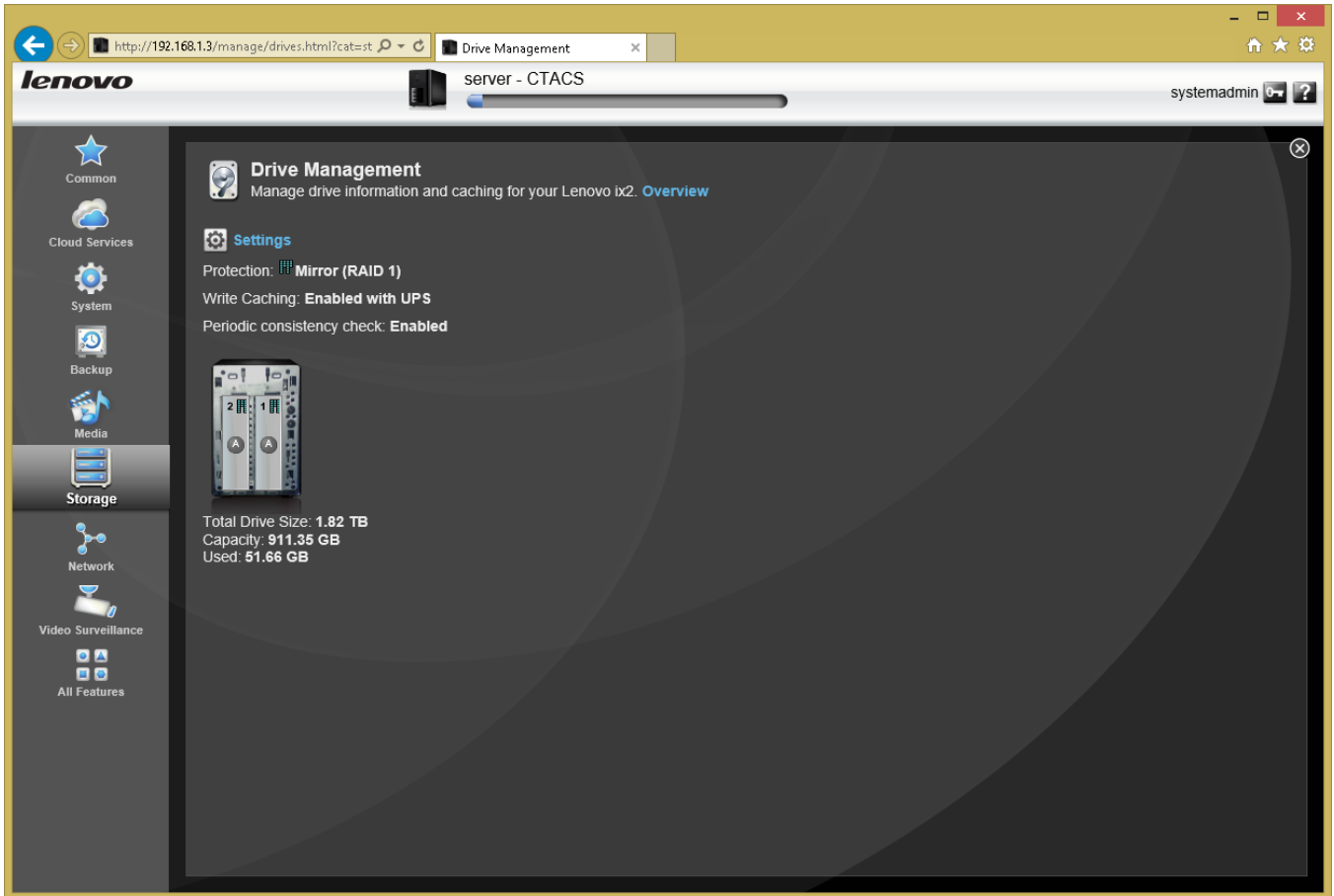


Figure 79: The Drive Management screen

The Drive Management screen gives a helpful visual representation of the hardware you have. In this instance, there are two hard drives configured as RAID 1. The total drive size, capacity and amount of space used are shown. By moving the mouse cursor over a drive, a small tip will be displayed indicating its health and status.

Click **Settings** and this panel appears:

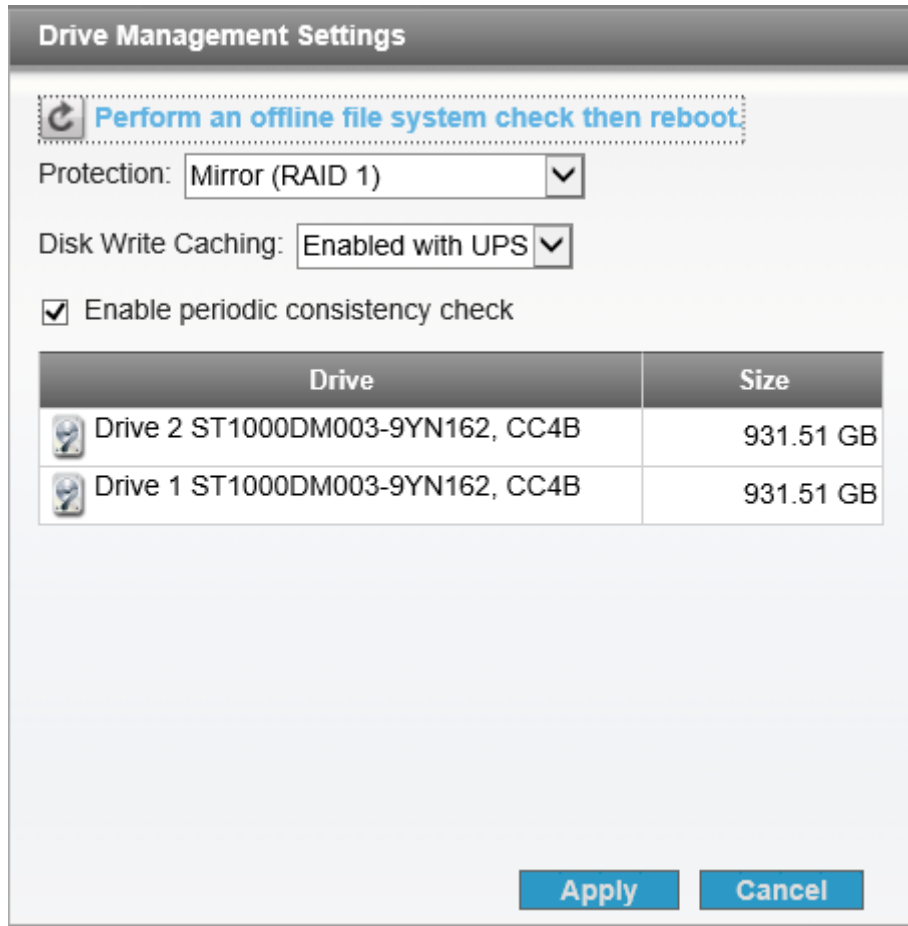


Figure 80: Drive Management Settings

More detailed information about the installed drives is shown, plus there are some options relating to disk health that can be changed. The **Enable periodic consistency** box should be ticked – this will cause the system to check the health of the disks on a regular basis (once a month).

If there has been a problem with the server, such as it shut down unexpectedly due to power problems or there are indications that data is missing, a systematic check of the drives should be done at the earliest opportunity. This is done by clicking **Perform an offline file system check then reboot**. Note that this may take a considerable amount of time and that the server will be unavailable whilst it is taking place.

14.4 Setting Up Automatic Email Notifications

Note: this section is possibly more suitable for business users

Whilst it is important to check the server on a regular basis, this is not always practical. For instance, the person who looks after the system may not be located in the office. Also, it is better to deal with some problems sooner rather than later. For these reasons, LifeLine can pro-actively advise when any issues occur using automatic notifications sent by email.

To set this up click **Email Notification** within the **System** section. Enter the **Destination Email Addresses** – the people who will receive emails. You should include yourself in the this list. Tick the **Send a test email message** box in order to test the setup once complete. Tick the **Configure custom SMTP settings** box. Enter the name of the **Email Server (SMTP)** plus the **Sender Email Address** (usually yourself). Enter the **Email Login** and **Email Password** (and confirm the latter) – these must be for an existing account (again, usually yourself). Click **Apply**, wait a minute and then check that the test email has been received.

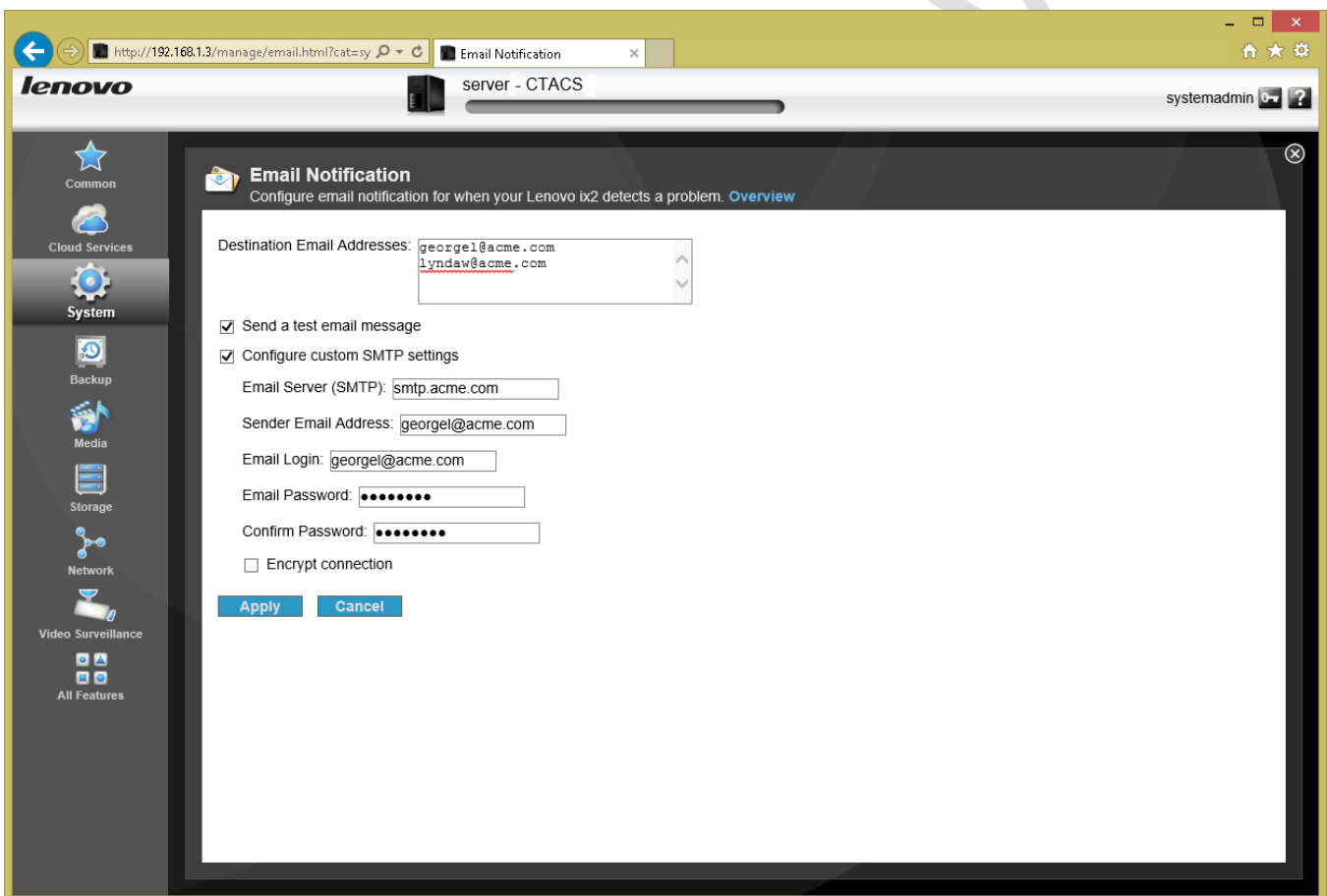


Figure 81: Configuring email notification

14.5 Updating the LifeLine Firmware

The LifeLine software is updated on a regular basis by Lenovo. These firmware updates may improve functionality, or may fix problems and address security issues. To check for any updates to LifeLine, click on the **Software Updates** icon. If an update is available it will be indicated:

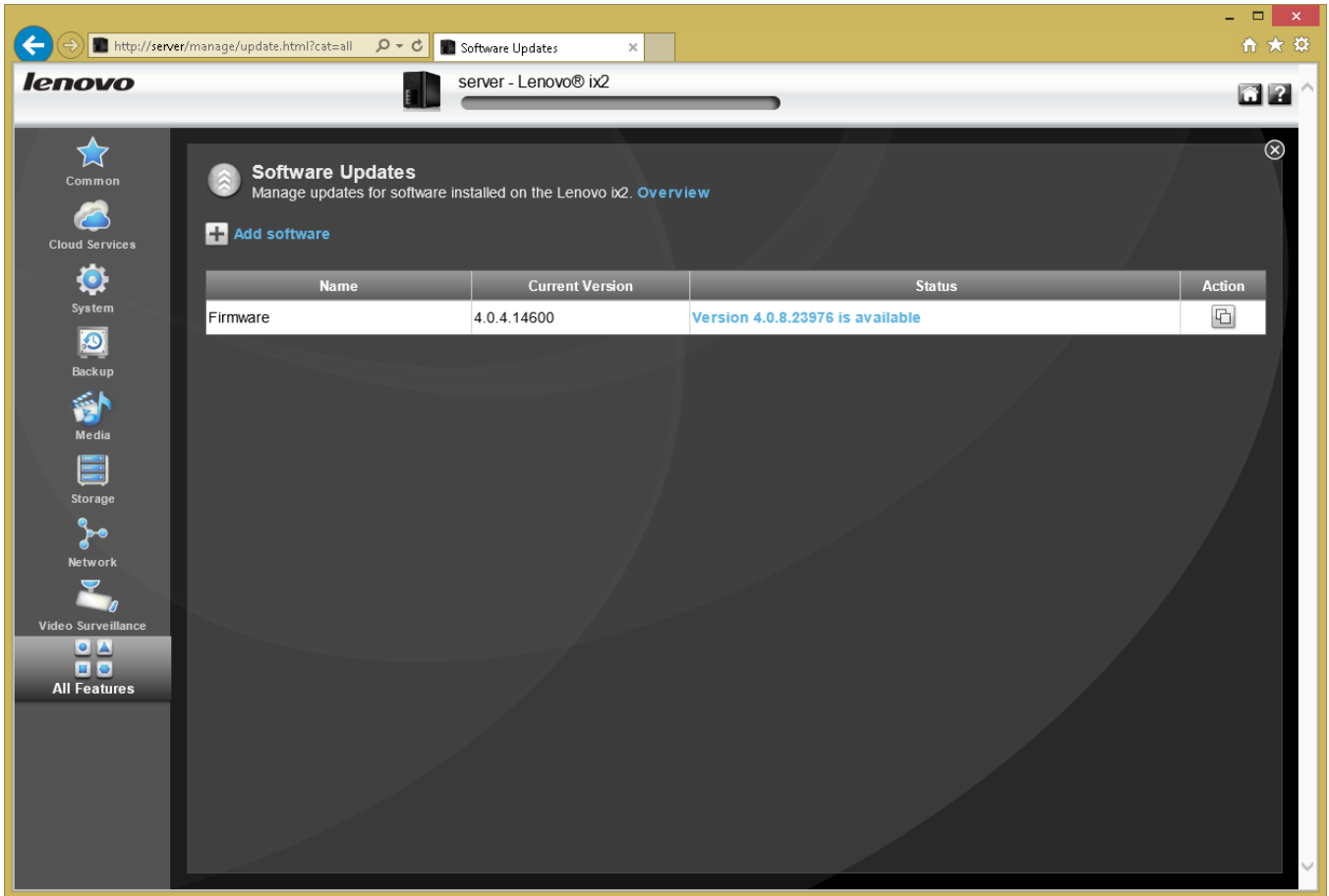


Figure 82: Software Updates screen

Click on the download. A separate browser window will open, containing a 'Download and Updates' section applicable to your model. The latest 'Firmware Version' will be listed here - click on it. The subsequent screen gives information about the update - scroll down to find the actual file and click on it to download to your computer.

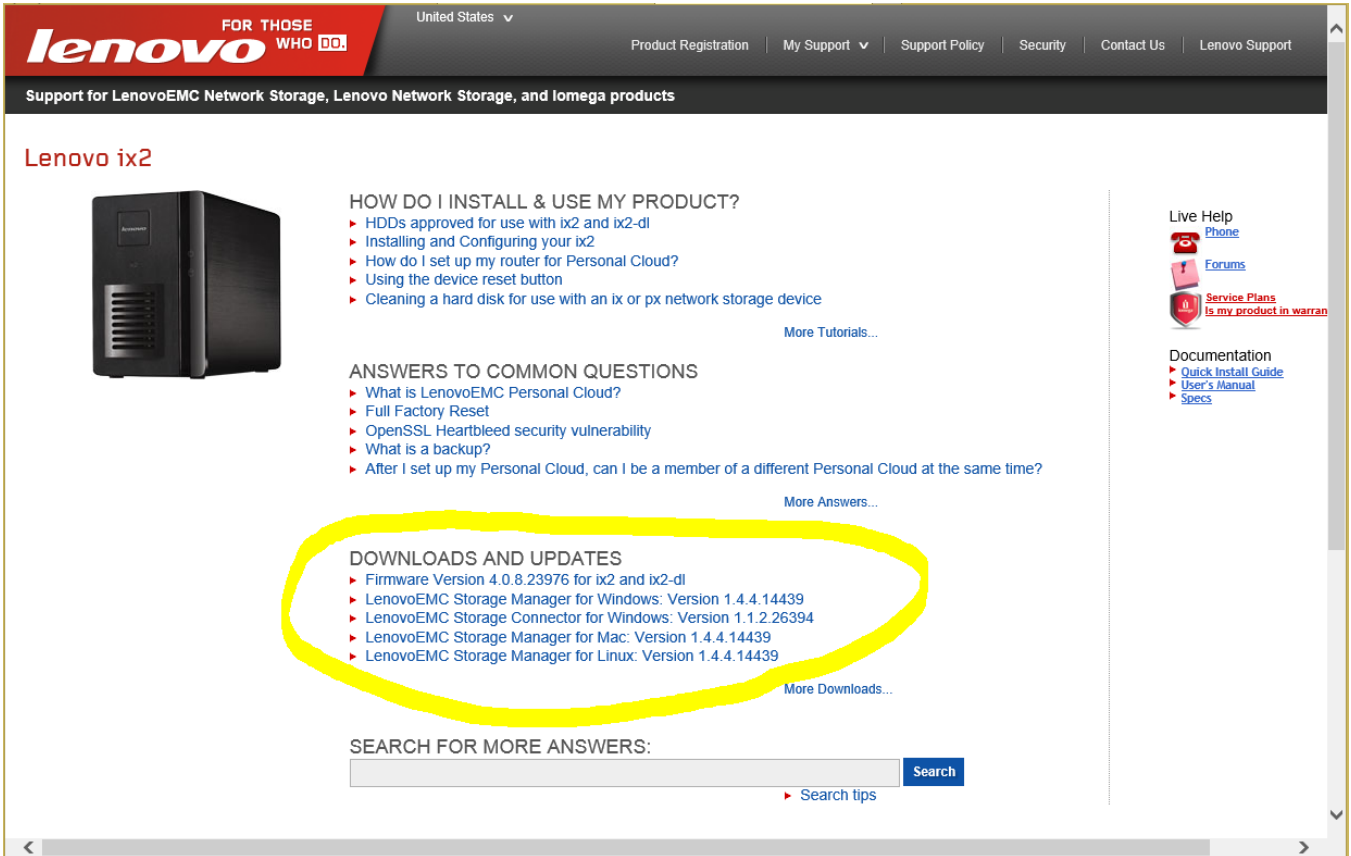


Figure 83: Webpage showing Downloads and Updates

Once the download is finished, close the window and go back to the original screen in LifeLine. Click the **Action** icon at the right-hand side, browse to the downloaded firmware update file and click **Upload**:

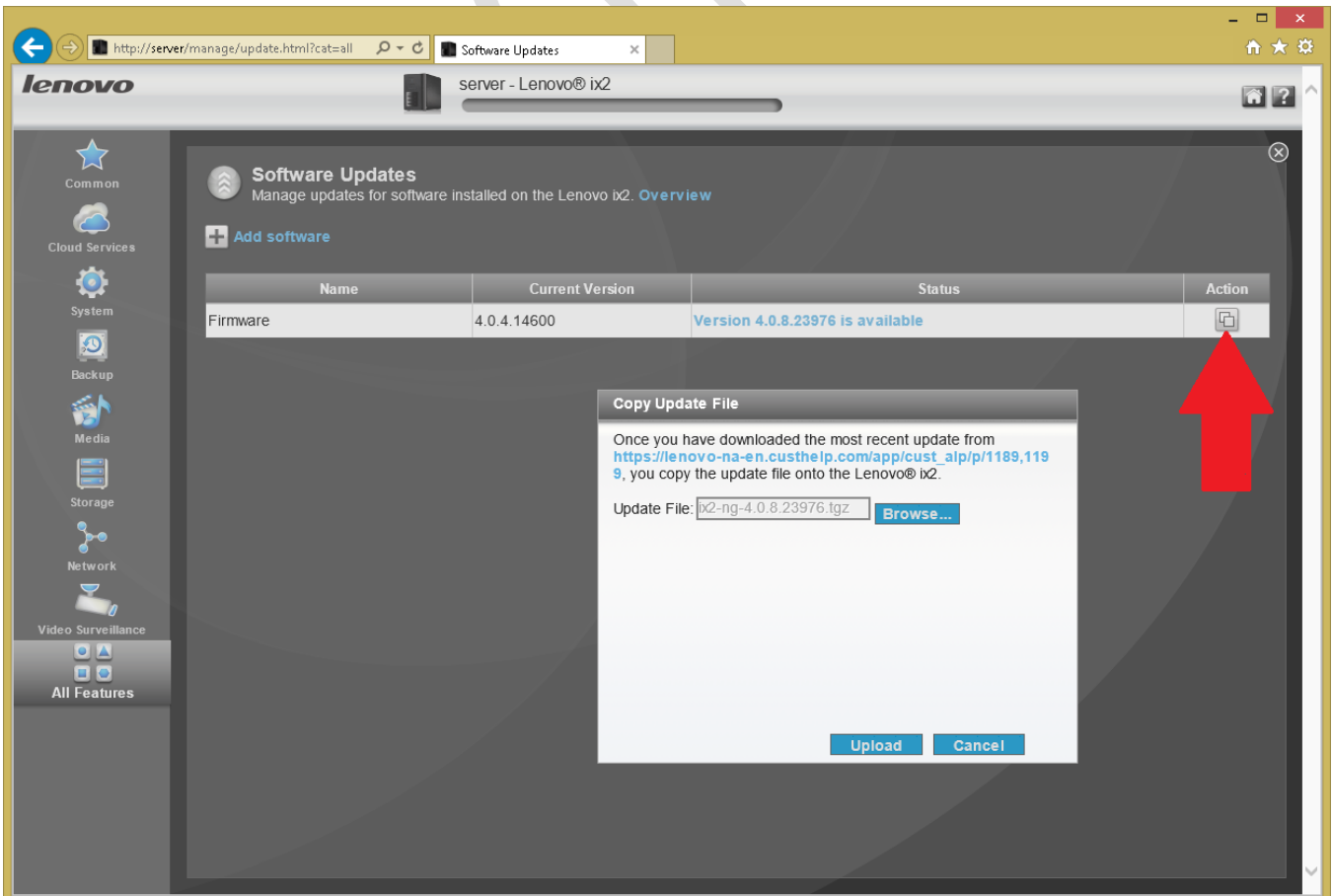


Figure 84: Specifying the Update file

After a few minutes spent processing, a message will appear stating that the update is ready - click **Apply**. This process will take several minutes, after which the server will restart.

The following considerations should be taken into account when updating the LifeLine firmware:

- It is by no means necessary to always be on the 'latest and greatest' version of LifeLine and some people prefer a more cautious approach to updating, particularly in a business environment. Whilst updates are designed to address specific areas, such as fixing security problems, they may in themselves introduce new issues. It is a good idea to check the internet for the experiences of other LifeLine users before applying an update.
- Before upgrading the firmware, make sure that both the data and server configuration have been backed up (see section [10 Backups](#) for general information).
- Updates invariably require a reboot of the system. It is therefore suggested that they are done at a time when nobody needs to use the system so as to minimize disruption.

DO NOT COPY

15 Miscellaneous Topics

15.1 Application Manager

Whilst the LifeLine operating system has a huge amount of useful functionality built-in, it is possible to extend it further through the installation of free, optional packages or apps. However, it should be pointed out that many of these are business oriented rather than aimed at home users. It is also the case that not all apps are available for all models.

To review what is available, click on the **Application Manager** icon in the System section to display the following screen:

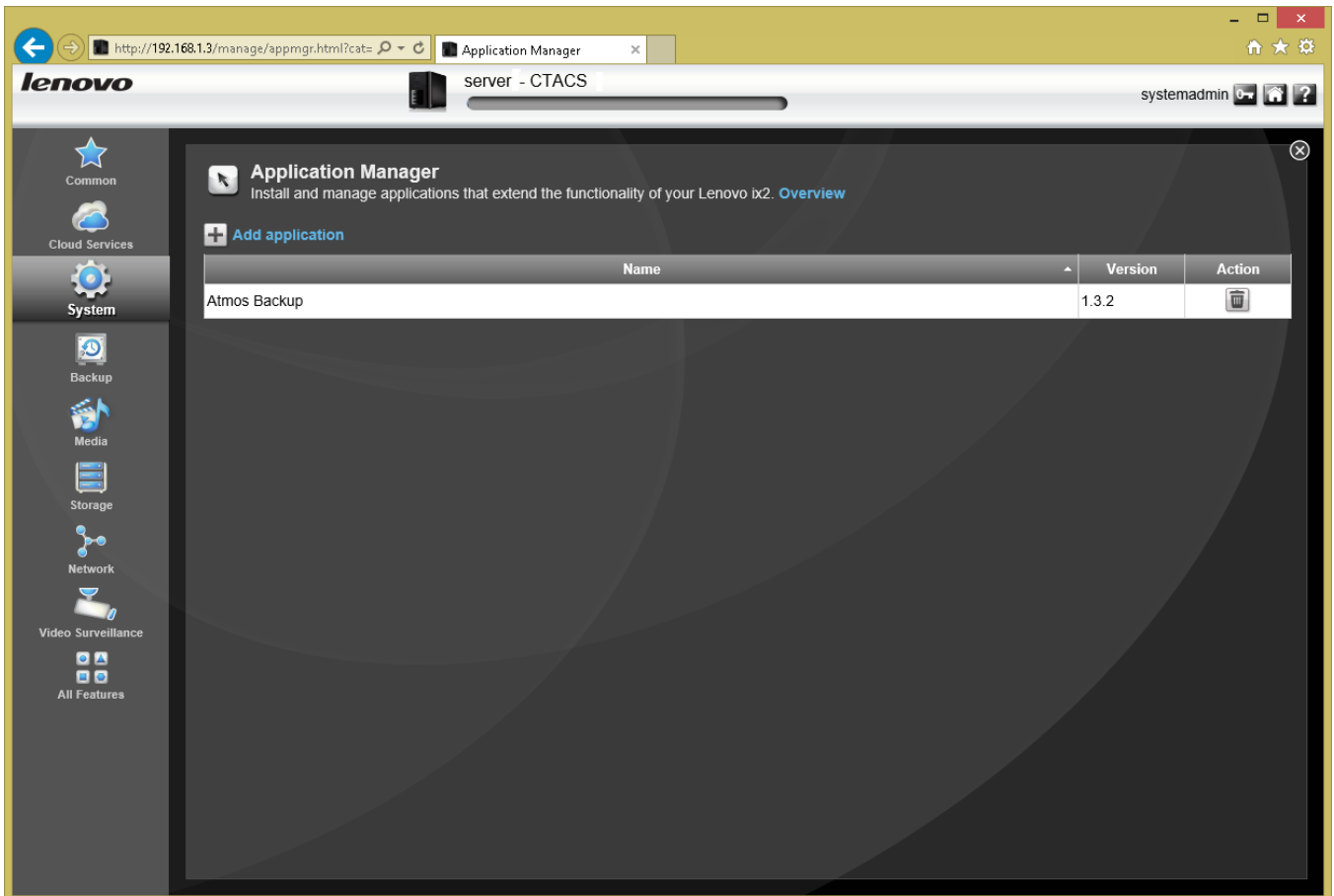


Figure 85: The Application Manager screen

Click **Add application**. A pop-up panel appears, containing a website link to apps for your model. Click the link and a webpage listing compatible apps is displayed:

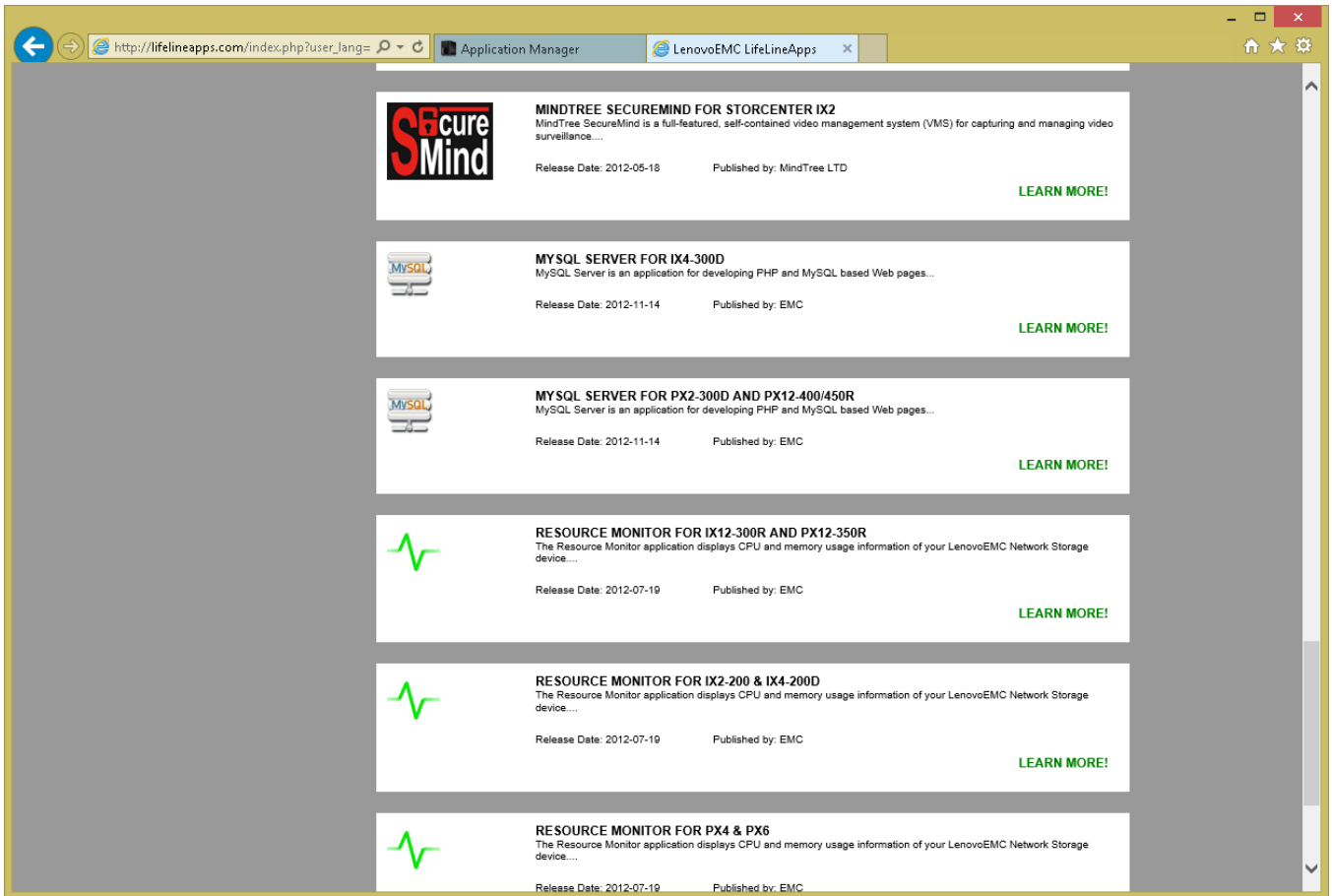


Figure 86: Website showing available LifeLine apps

To download an app, click on its **LEARN MORE!** link. On the resultant page, click the box to accept the terms and conditions and a download link will appear; click on it and save the download to a suitable location on your computer. When the download has finished, close the webpage and go back to the server. Click the **Browse** button, navigate to where the downloaded file is and select it. Then click the **Upload** button. The actual installation may take from several seconds to a minute; when complete, a new icon will have been added to LifeLine. If it is not immediately apparent where the icon has been placed click **All Features** and find it.

The downloaded and installed apps are listed in the Application Manager screen. They can also be deleted from there if necessary.

15.2 Feature Selection

The LifeLine Desktop can be customized by changing the icons that are displayed. You might want to do this to remove items that are never used, or to reduce the risk of accidentally clicking something that might be “dangerous”. Note that removing an icon does not delete the feature as such – it simply removes it from view and it can be easily restored as and when you need it again.

To customize the available features click **Feature Selection** within **System** to display the following screen:

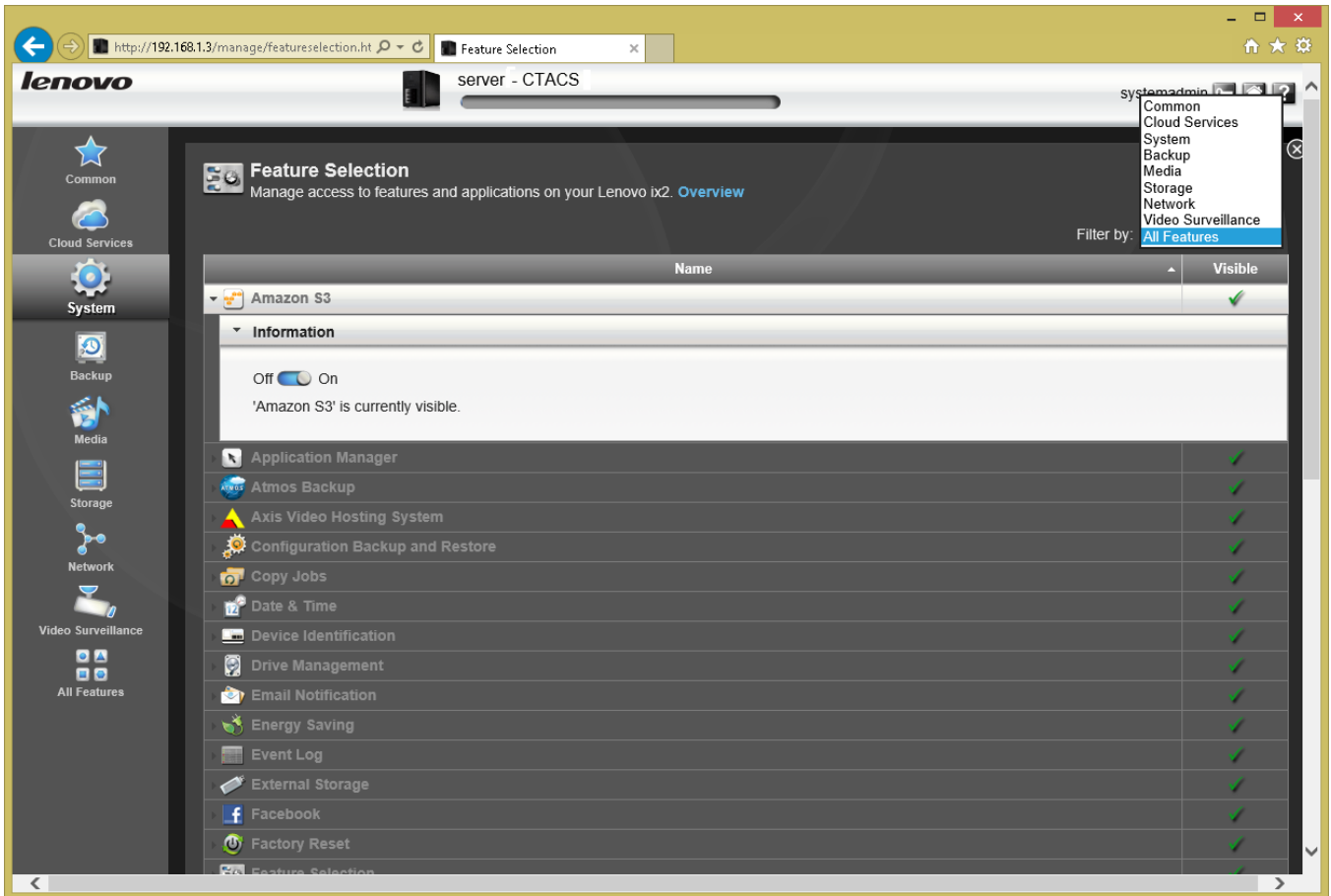


Figure 87: Feature Selection screen

All the possible features are listed, although this view can be filtered to a particular section if more convenient. Each feature has a simple ‘On-Off’ switch associated with it that controls whether the icon is displayed on the Desktop or not. Having made the change(s), close the screen down.

15.3 Customizing the Home Page

The Home Page for server can be changed and customized in several ways. To do, click the **Home Page Settings** icon in the **Common** section:

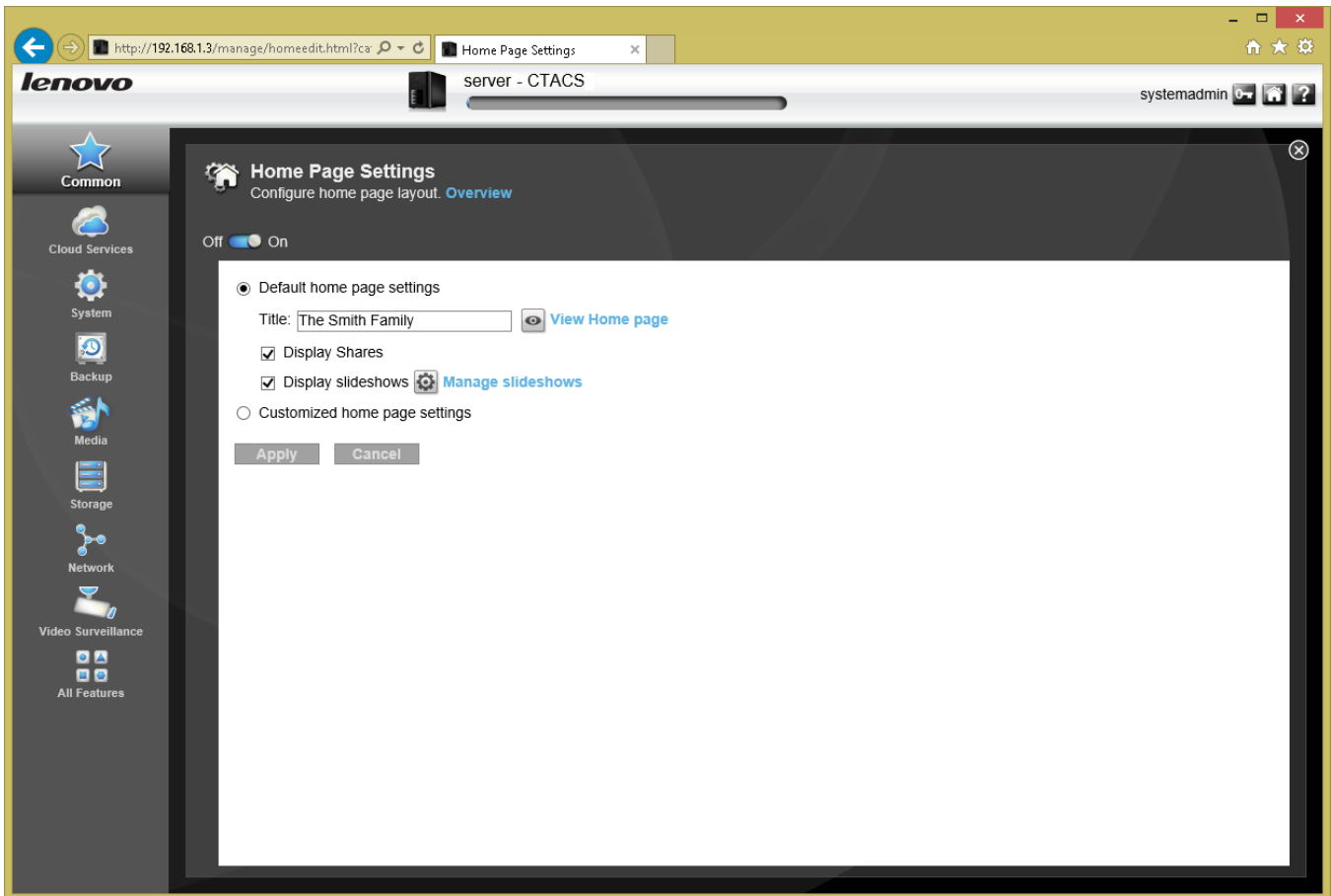


Figure 88: Home Page Settings

The first thing is to decide whether a home page is needed at all. If users do not use or you do not want them to access the server through a browser as in section [7.1 Using A Browser](#), the home page can be disabled by sliding the switch at the top of the screen from the **On** to the **Off** position. If you choose to do that the rest of this section is not applicable.

Assuming the home page is being used, you might want to change its **Title**, perhaps to something that reflects the name of the household or organization e.g. “*The Smith Family*”, “*ACME Inc*” etc. Note that there are some restrictions on the use of punctuation and special characters in the title.

If you do not want the shared folders to be shown, take the tick off the **Display Shares** box.

By default, the home page runs a slideshow of photos from the server. If you do not want this to happen, remove the tick from the **Display slideshows** box. If you do want a slideshow but want your own photos, click **Manage slideshows** followed by **Add a slideshow**. Give the slideshow a **Name** and set the **Location** to point at the folder containing the pictures. If you want it to be the main slideshow tick the **Set as default slideshow in the Home Page** box:

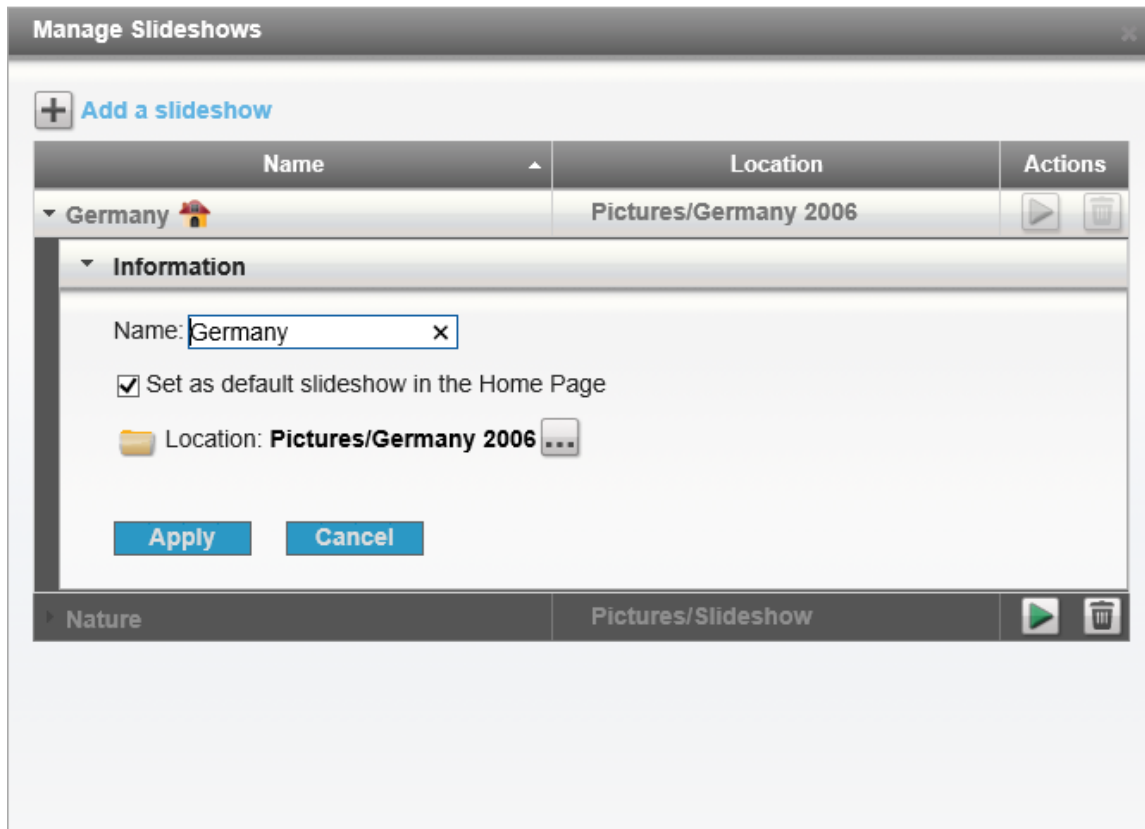


Figure 89: Adding a slideshow

You can have multiple slideshows. For instance, in a home setting you might have a different slideshow for each family member, a selection of photos from different holidays and so on. In a business you might have a slideshow to represent each department.

If this degree of customization is insufficient, it is actually possible to radically change the home page altogether and make it look pretty much any way you want – provided you understand HTML and have a webpage design tool or editor. By clicking the **Customized home page settings** option you can point it at your own HTML pages.

Appendix A: Internet Access Using a Proxy Server

In a typical small business environment, a router is used to connect the server and network directly to the internet. However, in rare circumstances the connection might be through a proxy server. An example of such a circumstance might be where managed or serviced offices are being used and the internet connection is provided as part of the service, in which case the Server needs to be told about it.

Click the **Network** icon under the **Network** group. Tick the **Use proxy settings** box and enter the details of the proxy server, which will need to be obtained from the person or organization that controls the proxy server. Generally this will consist of an address and port number, but may also require a user Name and password. Then click the **Apply** button.

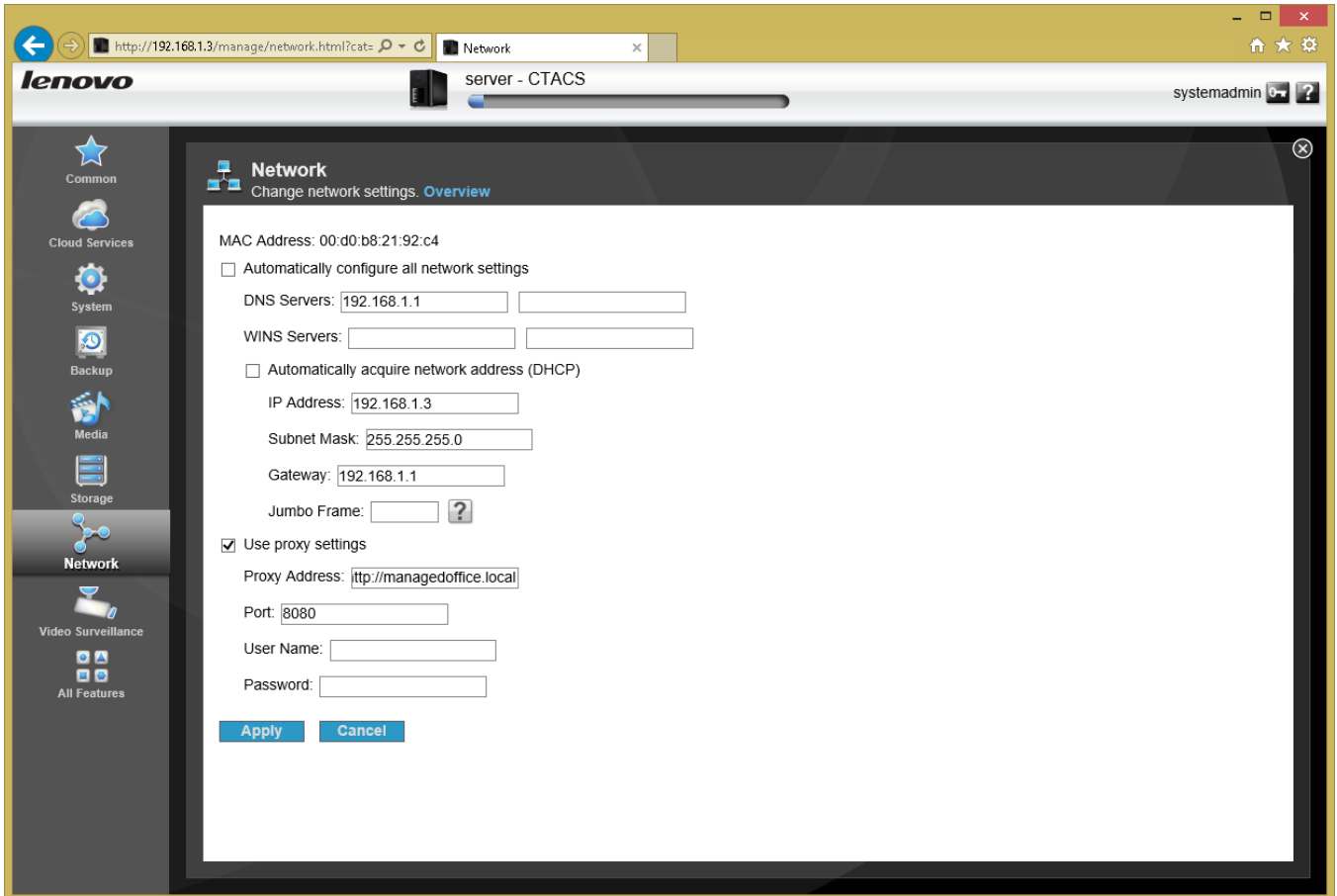


Figure 90: Example proxy server settings

Appendix B: Reset NAS or Prepare For Disposal

There is an option within LifeLine to reset the NAS unit back to the factory settings. There are two situations in which you might need to do this:

1. You wish to re-do the installation from scratch. For instance, you may not be happy with your first attempt at installing the server and wish to try again.
2. The unit is to be disposed of.

To reset it, click on **Factory Reset**, which is in the **System** section. The following screen is displayed:

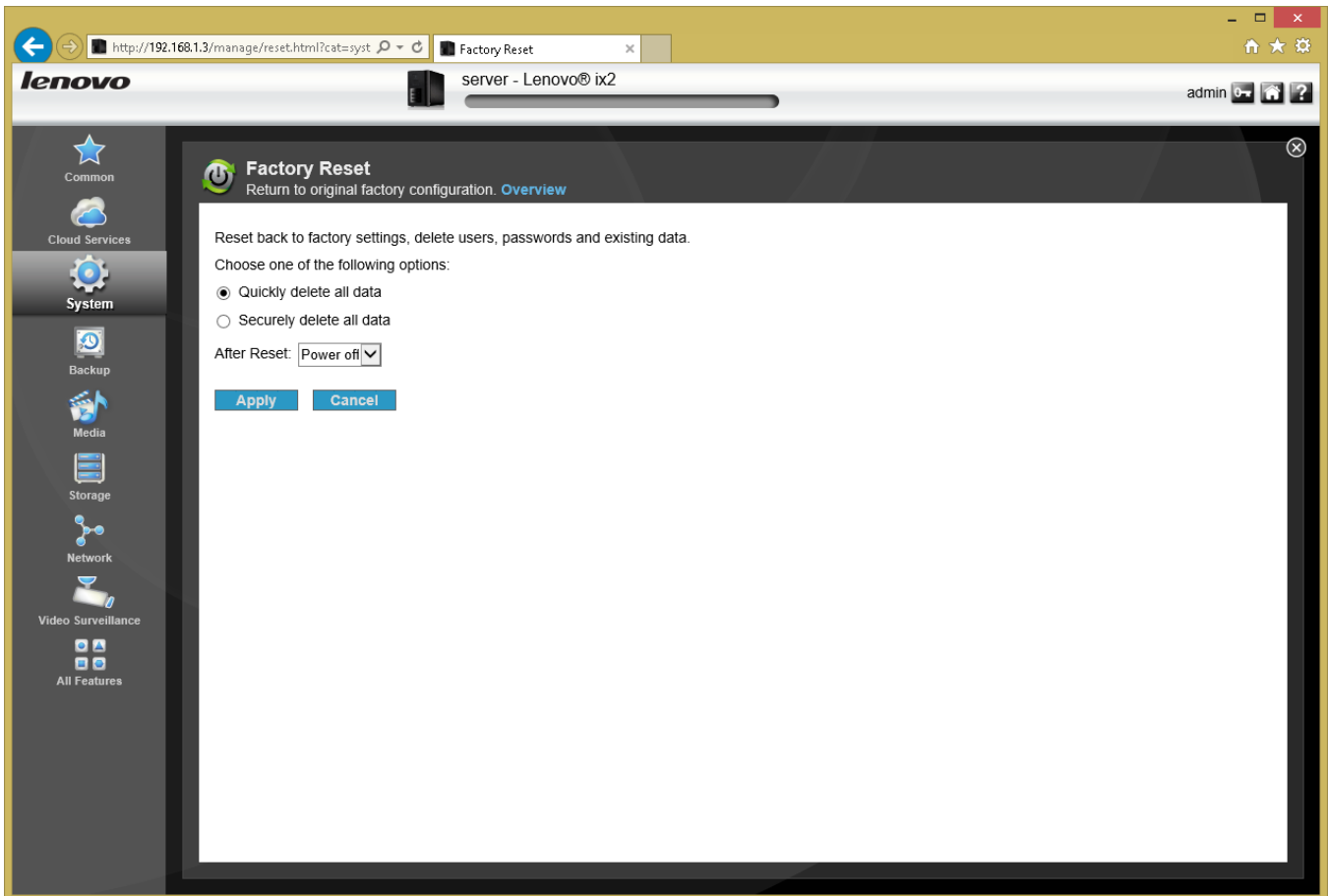


Figure 91: The Factory Reset screen

All information on the server (settings, users, passwords, data) is removed. There is a choice to **Quickly delete all data** or **Securely delete all data**. Within the former, the data is deleted in a way sufficient for most purposes, but could potentially be recovered with specialist forensic tools. If you are intending to re-install the server this option is sufficient. With the second option, random information is written over the hard drives to trash what was there before. This option takes a lot longer but makes it almost impossible to recover any data. Choose this option if the unit is being disposed of.

You can also specify whether the unit with power off or restart when the reset is complete.

Click **Apply** to carry out the reset.

Thank you!

We hope that you have found this guide helpful and interesting. Supplementary and supporting information can be found at the following website: www.serverinstallationguides.co.uk

If you have any suggestions or have found areas for improvement, please let us know at enquiry@ctacs.co.uk

DO NOT COPY