SEAGATE

IRONWOLF™

Seagate Guide To Network Attached Storage

Everyone has been in a situation where they need a document or file, but it's stored on a computer back at home or in the office. Or their computer malfunctions, leaving important files inaccessible.

A network attached storage (NAS) device can combat both these situations. It can act like a personal cloud, providing a secure central space to store your files on the local network, with the option to share over the Internet as well.

In this guide, we will explain some of the many capabilities of NAS for homes and small businesses, how to set a typical device up, and how to keep everything secure from malicious intruders.

IRONWOLF HEALTH

EUROPEAN HARDWARE AWARDS 2024 BEST HARD DRIVE Seagate IronWolf / IronWolf Pro

EUROPEAN HARDWARE AWARDS 2025 BEST HARD DRIVE Seagate IronWolf / IronWolf Pro

EUROPEAN HARDWARE AWARDS 2026 BEST HARD DRIVE Seagate IronWolf / IronWolf Pro

Choosing the right drives for your NAS

A NAS device is primarily a box of storage devices, usually mechanical hard disks, although they can be SSDs, or even NVMe drives. But you want your NAS to be equipped with storage devices that have much greater resilience than typical desktop computer drives, such as Seagate hard disks aimed at NAS applications incorporating heat-assisted magnetic recording (HAMR) technology. This provides greater assurance that your files will be safely stored, and is available on Seagate drives with 24TB of capacity and above. SSDs typically don't offer this level of durability, even if they are more resilient against physical shocks.

For this reason, while you can install any hard drives in a NAS, you're better off using models that are specifically designed for this application, such as Seagate's IronWolf and IronWolf Pro. The IronWolf range is aimed at home users and home offices, with a million-hour mean time before failure (MTBF). This means the drives can run continually for many years without risk of failure. IronWolf Pro drives offer two million hours MTBF, so you can be even more sure that you will never lose any data.

Drive model	Capacity	Workload rating	Cache	MTBF	Warranty	AgriNAS Health Management	Rotational Vibration sensors	Rescue Data Recovery Services
 **Seagate IronWolf** (suited to 1-8 bay NAS)	1TB – 16TB	180TB/ year	64MB-256MB	1 million hours	3 years	IronWolf Health Management	4TB plus	3 years
 **Seagate IronWolf Pro** (suited to 4 bay NAS and above)	2TB – 32TB	300TB/ year	256MB-512MB	2 million hours	5 years	IronWolf Health Management	All drives	3 years
 **Seagate Exos** (enterprise grade storage)	600GB – 32TB	550TB/ year	256MB-512MB	2.5 million hours	5 years	Server-level	All drives	N/A

2025 European Hardware Award Winner

Typical desktop drives can also offer a strong MTBF of 1 million hours, they don't tend to come with such a long warranty (2 years versus 3 or 5 years). They also won't include rotational vibration sensors, which Seagate IronWolf drives incorporate to help protect the drives from damage via Seagate IronWolf Health Management (IWHM).

This is an embedded diagnostic and monitoring system developed by Seagate Technology, designed to proactively maintain drive and system reliability. It operates within compatible NAS operating systems to continuously track a wide range of environmental and performance parameters, such as temperature, vibration, shock, connection stability, and data transfer integrity, to assess overall drive health.

Unlike basic S.M.A.R.T. monitoring, IWHM uses advanced algorithms and hundreds of data points to provide three layers of protection: prevention (identifying risks and suggesting corrective actions), intervention (warning users and recommending backups before failure), and recovery (including access to data recovery services if needed). Overall, it functions as an intelligent health management system tailored specifically for NAS environments, helping users minimize downtime and reduce the risk of data loss.

IronWolf Pro models also come with Rescue Data Recovery Services, so if a drive does go down, it can be sent off to a professional lab to retrieve the information on the disk, which is generally over 90% successful.

How to install hard drives into your NAS

Once you've identified the drives you want to use for your NAS system, you can start planning.

Some NAS devices come with drives pre-installed. But many arrive unpopulated, leaving the owner to put their own disks inside. This provides greater flexibility, giving a wide range of capacity options. For example, Seagate's IronWolf Pro NAS hard drives come in sizes from 2TB to 32TB.

While some NAS devices will require removing screws and taking off an external casing to install disks, easily accessible bays on the front are more typical. These make installing the drives quite painless. For example, with the Ugreen NASync DXP4800 Pro, pressing a button on the front of a drive bay pops out a handle, which you can use to pull out an individual caddy. Very similar methods are available with NAS devices from other popular brands such as QNAP and ASUSTOR (a list of relevant ecosystem partner links can be found at the end of this guide).

Installing the drive into the caddy is tool free in this NAS. You press a tab to slide one edge outwards slightly. There are pins at the locations of the drive screw holes, so when you slide the edge back after placing the drive in the caddy, it will be held firmly in place. However, smaller 2.5in drives will need to be screwed in place. Some NAS devices also require 3.5in drives to be screwed into the caddy. However, many have a system like this, which means installing a drive takes less than a minute.

Another great thing about drive bay caddies for SATA disks is that the power and data connectors should make contact automatically as the caddy is slid back in and locked into place and will disconnect again just as easily as the drive is slid out. With some NAS devices, if one of the drives has a mechanical failure, it's even possible to remove it without powering off the device. Once a replacement is installed, it will be powered up and integrated into the system. This is called hot swapping. Other NAS boxes require powering down first. This is called cold swapping.

NAS RAID levels

Once you have drives inside your NAS, powered the device up, and navigated to the administration interface, the next step is to set up the drive array. This is the first area where a NAS will transcend a locally attached USB storage device. The key to this is RAID, which stands for “redundant array of inexpensive disks”. The key word in this acronym is “redundant”. Most types of RAID enable one or more disks to act as backups within the system itself, so if a drive fails you don’t lose any data.

RAID 0

RAID is divided into levels. Here we’ll just describe the main ones you’re likely to want to use in a typical home or small business NAS. The first one is RAID 0, which doesn’t provide additional protection, but it does increase performance. With RAID 0, the system splits your data into chunks and writes these to multiple disks in parallel, theoretically multiplying reading and writing performance by the number of drives you have.

RAID 1

With RAID 1, in contrast, all your data is written to multiple disks at once (called mirroring), so it is stored on at least two drives. If you lose one disk, there will be another identical one where all your data is intact. If you have four or more disks, you can combine RAID 0 and 1 to create RAID 10, where data is written in parallel to two disks which are then mirrored onto two more. You get the performance boost of RAID 0 with the security of RAID 1.

RAID 5

However, you’re still sacrificing a lot of drive capacity that you paid for. While RAID 0 gives you all the capacity of your drives, RAID 1 and 10 cut it in half. This is where RAID 5 comes in. With RAID 5, a “parity” system is employed. You need at least three drives and lose some of the capacity, but all your data is stored on two drives, albeit not a complete mirror. If you lose a disk, you won’t lose any data. There will be some performance benefits from reading and writing data in parallel too. This is why RAID 5 is usually considered the optimal choice for a NAS with three or more drive bays.

RAID 6

You might also have the option of RAID 6, which uses parity like RAID 5 but with your data stored on three disks instead of two. This means you can lose two drives without losing data, but the total capacity will be less than for RAID 5.

The RAID level you choose depends on your storage priority - whether you want greater performance (RAID 0), easy fault tolerance but lower capacity (RAID 1), or a balance between the two (RAID 10, 5 or 6). Typically, you want some protection, so RAID 1 for a two-bay NAS is optimal, or RAID 5 for four bays and above, and RAID 6 if you’re really worried about failures.

What kind of NAS do you need?

The kind of NAS device you need will depend on your use case. For a home users or media sharing, a **one- or two-bay** device using Seagate IronWolf drives will be sufficient. This can replace cloud storage with your own private cloud, saving you monthly fees. It will give you centralised storage, automatic backup (of which more later), and media streaming at home. With a two-bay device, you can employ RAID 1 for strong protection from hardware failure, too.

For creative professionals or a small studio, a **four-bay** NAS will be more appropriate, populated with Seagate IronWolf Pro drives. Using RAID 5 or 10 for increased throughput alongside data security, the team will have fast network access to shared large files, while maintaining resiliency. The Pro drives will also mean data can still be recovered even in the absolute worst-case scenario, giving full professional confidence.

A four-bay NAS might also suit a small business, but one supporting six or eight drives would be more appropriate for a medium-sized enterprise. Seagate IronWolf Pro drives will be recommended, for maximum data security in an always-on environment. Rather than relying on expensive multi-user cloud subscriptions, the business can retain full control over their costs while still protecting their data. An **eight-bay** NAS could offer up to 256TB of storage using 32TB drives.

User levels and file sharing

Set clear permissions so every user sees only what they're meant to.

When you first configure your NAS, you will set up an administrator login and password. This will give you complete access to all features via the system interface. But for security reasons, you won't want to use this for general file sharing across the network, which is where user management comes in.

When you're logged into the interface (generally a web page or a smartphone app) as an administrator, you can add new standard users. These will have access to certain folders on the NAS storage but won't be able to change any settings. When the administrator creates and shares folders on the NAS, they can define which users have access – either as read only or read-write. A user can have their own personal folder on the NAS for placing their files. But unless explicitly given access, they won't be able to see other users' folders.

These folders aren't automatically visible over the network, however. The NAS administrator will need to turn on appropriate filesharing protocols. For Windows systems, this is called SMB or Samba, which Macs can also see, although Macs also support AFP, while NFS is supported by Macs and Unix or Linux systems. Macs also have an option called Time Machine aimed at client system backup, which we will discuss shortly.

Then there are FTP, SFTP and WebDAV. These can also provide access over a local network but are more focused on Internet sharing. FTP (file transfer protocol) is the standard system existing for decades, requiring client software to access, with SFTP being the secure encrypted version. WebDAV presents shared folders as webpages, making it possible to use a simple browser to download files, although typically this just provides read-only access.

Remote access and security

However, none of these are automatically visible outside the local area network. To make FTP, SFTP and WebDAV externally visible, you will need to jump onto your Internet router's administration interface. You then direct separate protocols like FTP to the device. This is called port forwarding. FTP typically uses port 21, while SFTP uses 22. WebDAV can use the typical 80 for HTTP and 443 HTTPS, which are the usual ones for websites, although 5005 and 5006 are also possible if you already have a webserver.

You need to know the IP address your NAS has been given on the local network. Then, on the router, you redirect the required port to the NAS IP number. When an external Internet user asks for a connection on that port from the router, the router will redirect the call to the NAS on the local network.

However, your router will probably have a changing IP address on the Internet, so the final piece of the puzzle is a dynamic DNS service like DynDNS or No-IP, which enables you to use a typical word-based URL instead of numbers. This will remain static as the numbers change via an agent that keeps the numerical location updated. Most competent routers support dynamic DNS services such as the ones already named, and some vendors even offer their own option.

Of course, making any aspect of an internal system on your local network available to the external Internet opens it up to malicious actors. It's generally sensible to have a different set of folders and user logins for FTP and SFTP, so that if anyone does gain unwanted access, they will only be able to see a controlled area of your NAS's storage. Unless you have sufficient expertise, don't make the NAS's administration interface accessible externally.

File storage, media, backups and beyond

Once your NAS is up and running with a RAID, some shared folders, and users, it's time to start storing your data on it. With a Windows or Mac computer and a network sharing protocol like SMB enabled, users can simply copy files across to a network folder. With Windows, it's most convenient to map the NAS file share folder to a spare local drive letter for easy access. If the folder is also shared externally via WebDAV, you'll have access to the files anywhere with an Internet connection.

Backing up your local files to a NAS on a regular basis is a great way to ensure you never lose anything important. It's best to automate this. PC users can employ Windows File History, pointing to the NAS mapped drive. Alternatively, Robocopy and Task Scheduler can make a periodic backup. Mac users have software called Time Machine, which will back up their files regularly in the background. This can be to an external drive, but with a NAS that supports Time Machine, it can be across the network to this device. Some NAS systems then offer the option to back up selected folders to a cloud provider such as Google Drive or Dropbox, for even greater file security.

Your NAS can also make your photos, video and audio accessible across the network. Turning on UPnP if supported can facilitate this kind of sharing. Premium NAS devices might even have a built-in server called DLNA, which media player devices like smart TVs can see and stream media files from without much user configuration.

Some NAS devices will let you install software like DLNA, or more sophisticated media servers like Flex, via downloadable applications. The most premium NAS devices will offer a huge library of software, such as webservers, VPN servers or even container systems like Docker that open a world of options.

The humble NAS is not really humble at all. It's a very powerful device to have on your network. It can keep your files safe, make them available across multiple machines and the Internet, plus so much more.