SEAGATE

# Seagate NAS OS 4 User Manual

Seagate Technology LLC
47488 Kato Road
Fremont, CA 94538
USA

**Click here to access an up-to-date online version**
of this document. You will also find the most recent content as well as expandable illustrations, easier navigation, and search capability.

# Contents

# Regulatory Compliance

## Trademarks

Apple, Mac, Time Machine, and Macintosh are registered trademarks of Apple Computer, Inc. Microsoft, Windows XP, Windows Vista, Windows 7, and Windows 8 are registered trademarks of Microsoft Corporation. Other trademarks mentioned in this manual are the property of their respective owners.

## Licenses and Free Software

Your Seagate product ships with copyrighted software that are licensed under the GPL, AFL, Apache, Apple, BSD, GNU LGPL, MIT, OpenLDAP, OpenSSL, PHP, Python, and Creative Common. It also includes free software, the source code for which can be downloaded from the Seagate website: www.seagate.com/support/

**krb5:**
Copyright, OpenVision Technologies, Inc., 1996, All Rights Reserved
Copyright © 1985-2006 by the Massachusetts Institute of Technology.
Copyright 2000 by Zero-Knowledge Systems, Inc.
Copyright © 2001, Dr Brian Gladman, Worcester, UK. All rights reserved.
Copyright © 2004 Sun Microsystems, Inc.
**bzip2:**
Copyright © 1996-2006 Julian R Seward. All rights reserved.
**berkeleydb:**
Copyright © 1990, 1993, 1994, 1995 The Regents of the University of California. All rights reserved.
Copyright © 1990-2003 Sleepycat Software. All rights reserved.
Copyright © 1995, 1996 The President and Fellows of Harvard University. All rights reserved.
**libnatpmp:**
Copyright © 2007-2008, Thomas BERNARD
**python-flup:**
Copyright © 2005, 2006 Allan Saddi All rights reserved.
**net-snmp:**
Copyright © 1990, 1991, 1992 by Carnegie Mellon University. All rights reserved.
**lighttpd:**
Copyright © 2004, Jan Kneschke, incremental. All rights reserved.
**python-transmissionrpc:**
Copyright © 2008-2010 Erik Svensson
**libfreetype2:**
Copyright 1996-2002, 2006 by David Turner, Robert Wilhelm, and Werner Lemberg
**cyrus-sasl:**
Copyright © 1998-2003 Carnegie Mellon University. All rights reserved.

**openssl:**

Copyright © 1995-1998 Eric Young. All rights reserved.
Copyright © 1998-2008 The OpenSSL Project. All rights reserved.

**miniupnpc:**

Copyright © 2005-2011, Thomas BERNARD

**python-werkzeug:**

Copyright © 2011 by the Werkzeug Team, see AUTHORS for more details.

**openldap:**

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved.

**uefishell:**

Copyright © 2004, Intel Corporation

**python-simplejson:**

Copyright © 2006 Bob Ippolito

**libevent:**

Copyright 2003 Michael A. Davis
Copyright © 2007 Niels Provos
Copyright © 1998 Todd C. Miller
Copyright © 2007 Sun Microsystems. All rights reserved.
Copyright © 2005 Nick Mathewson
Copyright © 2000 Artur Grabowski
Copyright © 2006 Maxim Yegorushkin
Copyright © 2000 Dug Song

**ajaxplorer:**

Copyright 2007-2011 Charles du Jeu

**php:**

Copyright © 1999 - 2006 The PHP Group. All rights reserved.

**python-webpy:**

Copyright © 2004-2007, CherryPy Team All rights reserved.

**python-pydispatch:**

Copyright © 2001-2006, Patrick K. O'Brien and Contributors. All rights reserved.

This list of licenses can evolve over time and can be found on the user interface under the heading “Credits.”

# Precautions

## Data

Any loss, corruption or destruction of data while using a Seagate drive or Seagate drive system or Seagate network storage is the sole responsibility of the user, and under no circumstances will Seagate be held liable for the recovery or restoration of this data. To help prevent the loss of your data, Seagate highly recommends that you keep TWO copies of your data; one copy on your external hard disk, for instance, and a second copy either on your internal hard disk, another external hard disk or some other form of removable storage media. If you would like more information on backup, refer to our website.

## Disk capacity

1TB (Terabyte) = 1,000GB. 1GB = 1000MB. 1MB = 1,000,000 Bytes. Total accessible capacity varies depending upon operating environment (typically up to 10% less per TB).

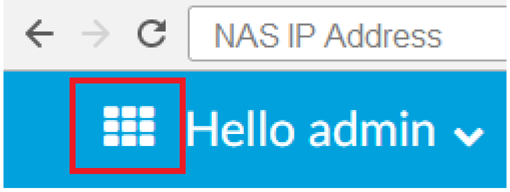
# Seagate NAS OS 4

## Introduction

Congratulations on your purchase of Seagate Business Storage featuring Seagate NAS OS. Designed to satisfy the data sharing and backup needs of small, medium, and branch offices, Seagate NAS OS is an intuitive interface accessible to a wide range of administrators. Additionally, NAS OS offers a rich set of collaborative and data protection tools to help manage your content.

## New 4.3 feature: App Button replaces Home Page

The default Home Page in NAS OS 4.2 has been replaced by the App Button, located in the top left corner of the screen and available at all times while browsing the NAS OS Webboard.



When logging into your NAS OS device, it will now default to the Filebrowser for immediate access to your files. The App Button can then be used to access all the apps you use (such as the Device Manager and Backup Manager) with just a few easy clicks.

The Filebrowser itself has been substantially updated to include drag and drop folder uploads, added Advanced Settings for a more personalized experience, and other improvements to functionality and performance.

NAS OS 4.3 also introduces a new method for accessing your Seagate NAS OS device remotely. The Seagate Access service is available to access your device using Sdrive, and this service's functionality has been enhanced to include a Web Manager that can be accessed both locally and remotely. The Web Manager lists any NAS OS device added to your new or existing Seagate Access account, giving you easy access using any web browser with Internet access using the following web link:

https://nas.seagate.com

See NAS OS 4.3 New Features for further information on features added to NAS OS 4.

# New 4.2 feature: App-based management

Among the many features added to NAS OS 4.2, experienced administrators will notice a new look to the interface as well as a critical update to NAS management: apps. Core NAS OS 3 features have been divided into default apps for NAS OS 4.2:

- **Backup Manager:** Formerly the Backup setting for NAS OS 3. Launch Backup Manager to create and manage backup jobs.
- **Device Manager:** Formerly the NAS OS 3 interface. Launch Device Manager to change the settings, add users, create shares, and much more.
- **Download Manager:** Formerly the Download setting for NAS OS 3. Launch Download Manager to create and manage download jobs.
- **Filebrowser:** Formerly the File Browser setting for NAS OS 3 and NAS OS 4. The new Filebrowser is a web-based file viewer. Launch it to view and share files stored on your NAS device.

The administrator can add new apps to the Seagate NAS device using the all-new **App Manager.**

See NAS OS 4.2 New Features for further information on features added to NAS OS 4.

# Content for this manual

This manual will guide you through the process of configuring NAS OS on your Seagate NAS and assist you in troubleshooting any issues that might arise. If you encounter problems, check Getting Help and the Seagate support page. Note that most problems can be resolved by resetting the product to factory conditions (see NAS OS Rescue and Repair ).

# Minimum system requirements

# Client OS:

- Windows 10 (32-bit/64-bit)
- Windows 8 (32-bit/64-bit)
- Windows 7 (32-bit/64-bit)
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Mac OS 10.6 and later
- Linux 2.6 and later

# Web browsers:

- Internet Explorer™ 7.0 or higher

- Firefox™ 3.0 or higher
- Safari™ 3.0 or higher
- Chrome 2.0 or higher

## Network:

- Computer with an Ethernet network adapter
- Ethernet switch or router 10/100/1000 (Mb/s)

i **Important info:**

- External forces such as network activity, hardware, distance, and setup can affect your NAS's performance.
- For optimal performance, use Gigabit Ethernet equipment.

# NAS OS 4.3 New Features

NAS OS 4.3 improves the way you access your NAS OS device using a web browser with an enhanced Filebrowser app. You can now directly access your apps using the App Button in the top left corner of the page instead of defaulting to an “App Home screen”. In addition, a new Remote Access function has been added to your new or existing Seagate Access account.

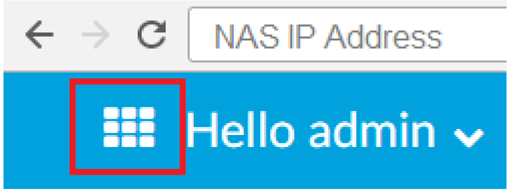
Review the details below to learn more.

## Filebrowser app for NAS OS

- The Filebrowser has been updated and is now the default landing page when logging into the NAS OS user interface.
- Compatible web browsers now support dragging and dropping folders from Windows Explorer or Mac Finder using the 1.2.7.2 Filebrowser app and later.
- Filebrowser now also includes Advanced Settings to provide a more personalized experiencer.

## App Button

- With the introduction of the App Button all your installed apps are always available using this button in the top left corner of the page.



## Seagate Access

- Use your Seagate Access account to remotely access your NAS OS 4.3 device.
- Sign into https://nas.seagate.com using your Seagate Access account
- Any NAS OS device which has been added to your Seagate Access account will be listed here
- Manage your device or access your files from any computer connected to the internet

# NAS OS 4.2 New Features

NAS OS 4.2 has new features for enhanced data access, sharing and security. Review the list below to learn more.

## Filebrowser app for NAS OS

- Browse files anywhere: Use the Filebrowser app to access your files via a web browser.
- Easy USB ingest: Copy files stored on USB devices with Filebrowser ingest.
- Share using web links: Share files and folders via secure web links in the Filebrowser.

## Backup Manager

- Support for more cloud services: Back up files stored on your Seagate network storage to new cloud services.
- Restore from the cloud: Restore backups saved to your cloud storage.
- Back up your cloud storage: Back up files and folders stored on your cloud storage to your Seagate network storage.

## Security in Device Manager

- New Security tab: Manage DDOS filtering, Block and White lists, and SSL certificate upload.

## iSCSI Targets and LUNs

- iSCSI enhancements: Use the new iSCSI setup to create multiple targets and LUNs or, a SimplyiSCSI volume.

## NAS OS Web Board

- New look: Check out NAS OS's new, modern interface.

# Features added for NAS OS 4

Below is a list of the new features available when updating from NAS OS 3 to NAS 4.

## Apps

The Home page for NAS OS 4 presents apps from Seagate and third party developers.  The administrator can add new apps to a Seagate NAS OS device using the **App Manager**.

Core NAS OS 3 features have been divided into default apps for NAS OS 4:

- **Backup Manager:** Formerly the Backup setting for NAS OS 3. Launch Backup Manager to create and manage backup jobs.
- **Device Manager:** Formerly the NAS OS 3 interface. Launch Device Manager to change the settings, add users, create shares, and much more.
- **Download Manager:** Formerly the Download setting for NAS OS 3. Launch Download Manager to create

and manage download jobs.
- **File Browser:** Formerly the File Browser setting for NAS OS 3. File Browser is a web-based file viewer. Launch it to view files stored on your NAS device. File Browser requires Java.

## Sdrive: remote access

Sdrive gives users remote access to data stored on their NAS OS 4 devices. The Sdrive service is available on your NAS OS 4 network storage with separate apps available for:

- Desktop:
  - Windows® 7 and higher
  - Mac® OS 10.7 and higher
- Mobile:
  - iOS® 6.1.2 and higher
  - Android® 4.0 and higher

Upon launching the desktop app for the first time, users can create a Seagate Access account and link it to any Seagate NAS OS 4 device.

## Network discovery

Configuring new NAS OS 4 devices is now easier using a web-based network discovery tool. Once the new NAS OS 4 device is connected to the network, the administrator can launch a browser and enter the URL: http://discover.seagate.com.

## Volume encryption

Protect new volumes from unauthorized access using NAS OS 4 encryption. The administrator can choose the level of encryption: a password or a file key to unlock the volume. The file key is stored on a USB key or thumb drive.

To prevent access to a volume's shares across a network, the administrator can lock an encrypted volume. Further, data is safe in case the hard drives are moved to a different enclosure. The encrypted volumes will prompt the user for the password or file key when first using the hard drives in the foreign enclosure. This can become important if hard drives are stolen or moved without permission.

## Internet protocol version 6 (IPv6)

Administrators now have the option to add IPv6 addresses to NAS OS 4 devices.

## Jumbo frames

A frame is a packet of data that carries hardware identifiers for network devices such as a source server, a destination NAS, and a router. The router uses frame data to facilitate communication between computers and network devices. Also known as an Ethernet frame, a frame's size is generally limited to 1500 bytes. Such a limitation in frame size can have a negative impact upon network devices.

Most modern Gigabit Ethernet routers and switches support jumbo frames, which are frames larger than 1500 bytes. Enabling jumbo frames on your router can improve performance among devices on the network, including your NAS OS 4 network storage.

## Network and cloud backup

In addition to NAS OS and rsync-compatible servers, administrators now have the option to choose backup destination servers that use the following protocols:

- FTP
- SMB
- Web Distributed Authoring and Versioning (WebDav)
- NFS

NAS OS 4 also supports backup to cloud storage such as AmazonS3, Box and more.

## Cloud sync

NAS OS 4 supports sync to Google Drive and Dropbox.

## Web distributed authoring and versioning (WebDAV)

WebDAV is a standard for collaborative workflows and data sharing. You can give remote servers access to shares by enabling the WebDAV service on your NAS OS 4 device.

## Distributed file system namespaces (DFS-N)

During the course of a day, a user may access multiple files stored on many shares connected to your local network (local area network or, LAN). To find all the shares and volumes spread about the network, a user can hunt through a long list of NAS devices and servers.

NAS OS 4 DFS-N allows administrators to add compatible shares to a single NAS OS 4 device. Accessing shares on a single device simplifies data management for the administrator and the user. Similar to creating a new share, the administrator adds remote shares to the Seagate NAS OS 4 device. The shares can come from any NAS OS device or server on the LAN.

NAS OS 4 DFS-N supports NAS OS shares and SMB volumes.

# Simple network management protocol (SNMP)

NAS OS 4 supports SNMP, a standard Internet protocol for managing network devices such as printers, routers, servers, and computers. Enable the SNMP agent in Notifications to give an SNMP server access your NAS OS 4 device. Additionally, the administrator has the option to turn on SNMP traps so that the NAS OS 4 device contacts the SNMP server.

Administrators have the option to choose SNMP v1/v2 or v3.

# Network recycle bin (NRB)

Deleting data on a share permanently removes all associated files. By enabling the NRB service, deleted files will be moved to the share's recycle bin. This can be very helpful if a user accidentally removes data that a co-worker is using on a project. The data is easily recovered from the recycle bin rather than desperately searching through the last NAS backup.

NRB is compatible with shares that use the SMB protocol, which is also a service.

# iSCSI logical unit number (LUN) export/import/clone

A logical unit number (LUN) is addressable data on an iSCSI target. Some versions of iSCSI management support multiple LUNs on a single target. While NAS OS gives the administrator the ability to create one or more iSCSI targets on a volume, each iSCSI target supports only one LUN.

However, NAS OS 4 gives administrators additional options to help create and manage iSCSI targets. Rather than creating new targets each time iSCSI is required, the administrator can export the LUN from an existing target and import the LUN's data. Additionally, NAS OS 4 includes the option to clone an existing target.

# Expand existing volumes beyond 16TB

NAS OS 3 prevented users from expanding an existing volume beyond 16TB. For example, a 14TB volume could not accept an additional 3TB for expansion. This limitation has been removed for NAS OS 4.

# Network uninterruptible power supply (UPS)

Previous versions of NAS OS support connecting an uninterruptible power supply (UPS) to a NAS OS device via the power and USB connections. UPS management is performed on the USB connection. If the working environment experiences a loss of power, the UPS allows the NAS to save data before automatically shutting down.

NAS OS 4 gives the administrator greater flexibility in power management with network UPS. A single UPS can now be used as a backup power solution for multiple NAS OS 4 devices. For example, the first NAS is connected to the UPS via power and USB. This is the master NAS to the UPS and it acts as the UPS server on the network. NAS devices on the network access the UPS server and add their power connections to the UPS.

NAS OS 4 also supports connection to select UPS devices that have an Ethernet port and are SNMP compliant.

## Export/Import NAS OS 4 settings

NAS settings include the following:

- Shares
- Users
- Groups
- Services
- Network
- Power
- Monitoring
- Notifications

NAS OS 4 settings can be exported from one NAS OS 4 device and imported into another NAS OS 4 device. Exporting settings is also a great tool for:

- Backup: Essential metadata is kept safe in case a NAS fails.
- Cloning: Use the same settings on additional NAS OS devices.

## Secure shell (SSH)

Administrators with advanced networking skills can log in to NAS OS 4 using secure shell (SSH), an encrypted protocol used for communication between devices. Using a command-line interface, the administrator can automate data management and backups as well as review the NAS's settings. The administrator also has the right to access data stored on the NAS via SSH.

## Process monitoring

The Monitoring page now features a list of processes with the following data:

- **Application:** The application using the process.
- **Status:** The process state (e.g. running, sleeping, disk sleeping)
- **CPU Usage:** The percent of the CPU being used for the process.
- **Memory:** The amount of RAM being used for the process.

## Search

NAS OS 4 has a magnifying glass icon on the top right of the interface. Click on the magnifying glass to enable an empty field and enter a search term. Results are limited to NAS OS.

# Event log

A bell icon on the top right of the interface provides instant access to NAS events. Click on the bell icon to see recent activity.

# LED Behavior and Device Buttons

NAS OS manages your device's:

- Status LEDS
- Hard drive LEDs
- Buttons

## LEDs

## Rackmount Seagate NAS

| Color | State |
|---|---|
| Blinking blue | Startup; shutdown; activity |
| Blinking red and blue | RAID synchronization; software update |
| Blinking red | Warning |
| Solid red | Error |
| Solid purple | Updating hardware |
| Blinking purple | Communication has been lost |

## Seagate NAS and Seagate NAS Pro

| Color | State |
|---|---|
| Solid white | Ready |
| Blinking white | Startup; shutdown; activity |
| Alternating red and white | RAID synchronization; software update |
| Blinking red | Warning or notice |
| Solid red | Error |

The status and hard drive LEDs work together to provide up-to-date details on your NAS device's health. For specific information on the meaning of the LED indications, see the user manual for your device:

- Seagate Business Storage 8-Bay Rackmount NAS
- Seagate Business Storage 4-Bay Rackmount NAS
- Seagate NAS Pro
- Seagate NAS

# Buttons

All Seagate NAS have a power button on the face of the device. Certain models also have identification and mute buttons. Check the user manual for your Seagate NAS to locate the buttons.

NAS OS manages the buttons via push types:

- Short push: A depression upon the button for one second or less.
- Long push: A depression upon the button for four seconds or more.

# Power button

The power button turns your NAS on when it is powered off. It can also help you power down the NAS without the need to launch NAS OS. Always make certain that no one is accessing the NAS before turning it off.

## Power button: short push

A short push is no longer than two seconds. When the product is powered on, a short push of the power button will:

- Turn the NAS off.
- Place it into deep sleep mode if the option has been configured in NAS OS. See Power for details on deep sleep mode.

## Power button: long push (select models)

A long push is longer than four seconds. Applying a long push will cut the power from the NAS, forcing it to shut down immediately. A long push is not recommended since it can result in data loss.

# Identification buttons: front and rear (select models)

Only use a short push on the identification buttons.

Pushing the identification button will cause the identification LEDs in the front and rear of the device to flash amber and the alarm to sound. The flashing LEDs allows you to identify the NAS among a group of racked devices. There is another identification button on the rear of the device that can also be pushed to turn on the identification LEDs and sound the alarm. Both buttons work in tandem, allowing you to turn the visual and audio identifications on and off. For example, you can use the identification button on the front of the device to turn them on and then turn them off via the rear identification button.

A third identification option is available in NAS OS Monitoring.

# Mute button (select models)

An audible alarm will sound when someone pushes an identification button or chooses the option in the NAS OS administration tool. It will also sound if the unit senses a problem with the hardware, such as a faulty power supply unit or elevated temperatures.

## Mute button: short push

A short push will turn off an existing audio alarm. When it is pushed, its LED will turn amber, indicating that the alarm has been muted.

## Mute button: long push

Apply a long push on the mute button to:

- Turn off an existing audio alarm off.
- Prevent the system from sounding an audio alarm.

Following a long push, the mute LED will turn amber, indicating the audible alarm is off. Even if a problem is found in the hardware, the alarm will remain muted. Examples of hardware problems include, but are not limited to, high temperatures, a faulty power supply unit, and fan failure.

The mute button can be pushed if the alarm is not ringing, guaranteeing that it will remain off. To turn the audible alarm back on, apply another long push.

# NAS OS Setup

Once your Seagate NAS has been configured per the instructions of the included quick start guide, the NAS OS Setup Wizard will guide you through the remainder of the installation. The NAS's administrator must complete the setup wizard since a password will be created to access the NAS OS management features. The time to complete the setup wizard varies based upon your NAS. Choose the option below that matches your Seagate NAS:

- Enclosure with disks: If you purchased an enclosure with disks, go to First Use: Enclosures with Disks.
- Enclosure without disks: If you purchased an enclosure that did not include disks, go to First Use: Empty Enclosure.

## First use: Enclosure with disks

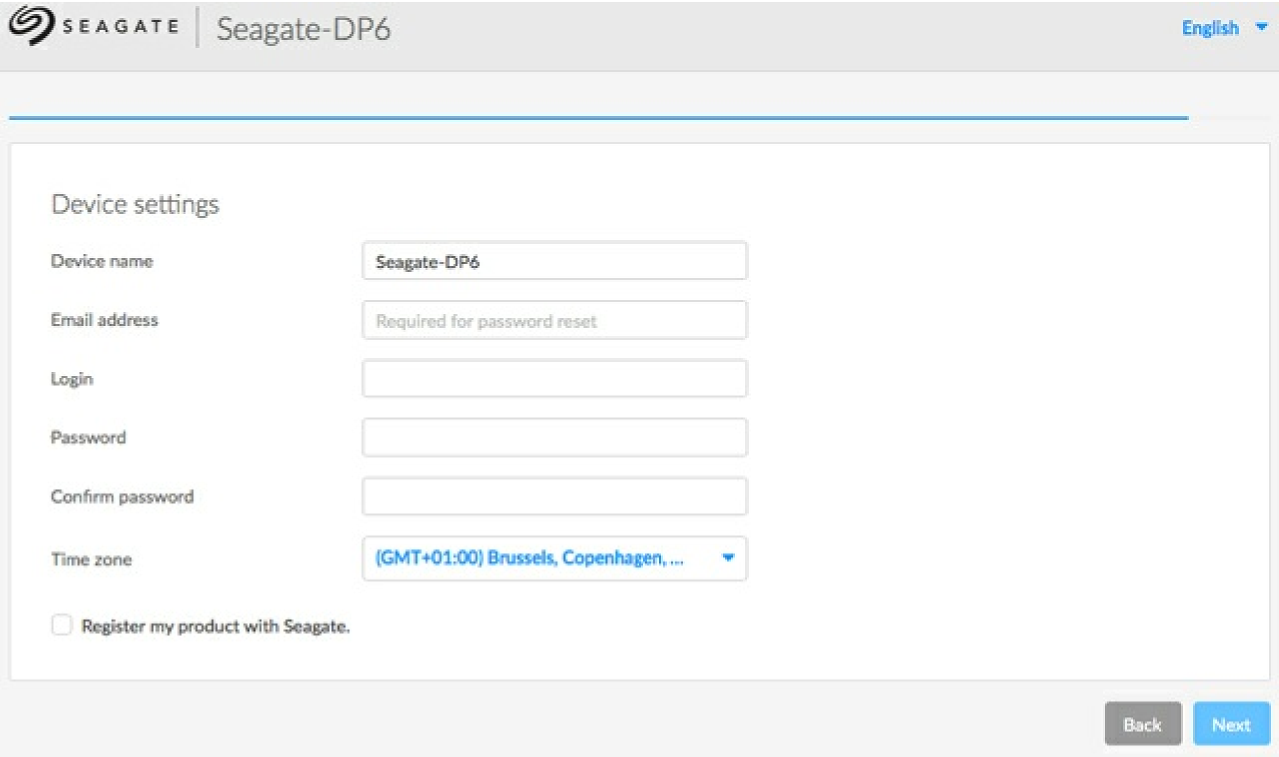
Before connecting to NAS OS, configure the Seagate NAS on your network. For instructions, review your NAS's user manual and quick start guide.

ℹ **Enclosure without disks:** If you purchased an empty enclosure, go to First use: Empty enclosure for instructions on how to set up Seagate NAS OS.

Consider the following before installing Seagate NAS OS:

- The NAS OS device's administrator should complete the installation steps.
- NAS OS checks for software updates during the installation. An error message informs you if it cannot check for updates due to a missing Internet connection. You have the option to search for updates after the installation.

1. Power on the device. The device is ready to be accessed once the status LED turns solid.
2. From a PC/Mac connected to the same network as your NAS, launch an Internet browser and type **http://discover.seagate.com**
3. Follow the on-screen instructions.



Device settings

Device name: Seagate-DP6

Email address: Required for password reset

Login

Password

Confirm password

Time zone: (GMT+01:00) Brussels, Copenhagen, ...

□ Register my product with Seagate.

During the setup, you can:

- Create or change the name of the device.
- Create or change the administrator login (the default is *admin*).
- Create a Seagate Access account for remote access.
- Configure or change the RAID level.
- Adjust the time zone.

Make certain to note your login and password for future use.

## Next steps

- **Simplify NAS access:** Seagate recommends that you install the software utility *Seagate Network Assistant* before moving forward with the device configuration. Seagate Network Assistant gives you instant information on your Seagate NAS, such as firmware version, IP address, and MAC address. It will also provide quick access to shares and NAS OS. See Seagate Network Assistant for instructions.
- **Configure your NAS:** For details on how to configure and use your Seagate NAS, go to Shares: Access and Transfer Files and Device Manager.
- **Install Sdrive for local and remote access:** Sdrive gives you easy access to shares and NAS OS on local and offsite networks. For more information, see Remote Access.

# First Use: Empty enclosure

Before connecting to NAS OS, configure the Seagate NAS on your network. For instructions, review your NAS's user manual and quick start guide.

**Enclosure with disks:** If you purchased an enclosure with disks, go to First Use: Enclosures with Disks for instructions on how to set up Seagate NAS OS.

# Choose compatible hard drives

Seagate NAS are compatible with most SATA I, SATA II, and SATA III hard drives. Older hard drives that are not constructed for NAS can experience reduced performance or failure. If you have any questions regarding hard drive compatibility, contact Seagate customer support.

Seagate hard drives are specially prepared for use with your Seagate NAS. Choose the link below to view hard drives that are optimized for your Seagate NAS:

- Seagate 8-bay Rackmount NAS
- Seagate 4-bay Rackmount NAS
- Seagate NAS Pro
- Seagate NAS

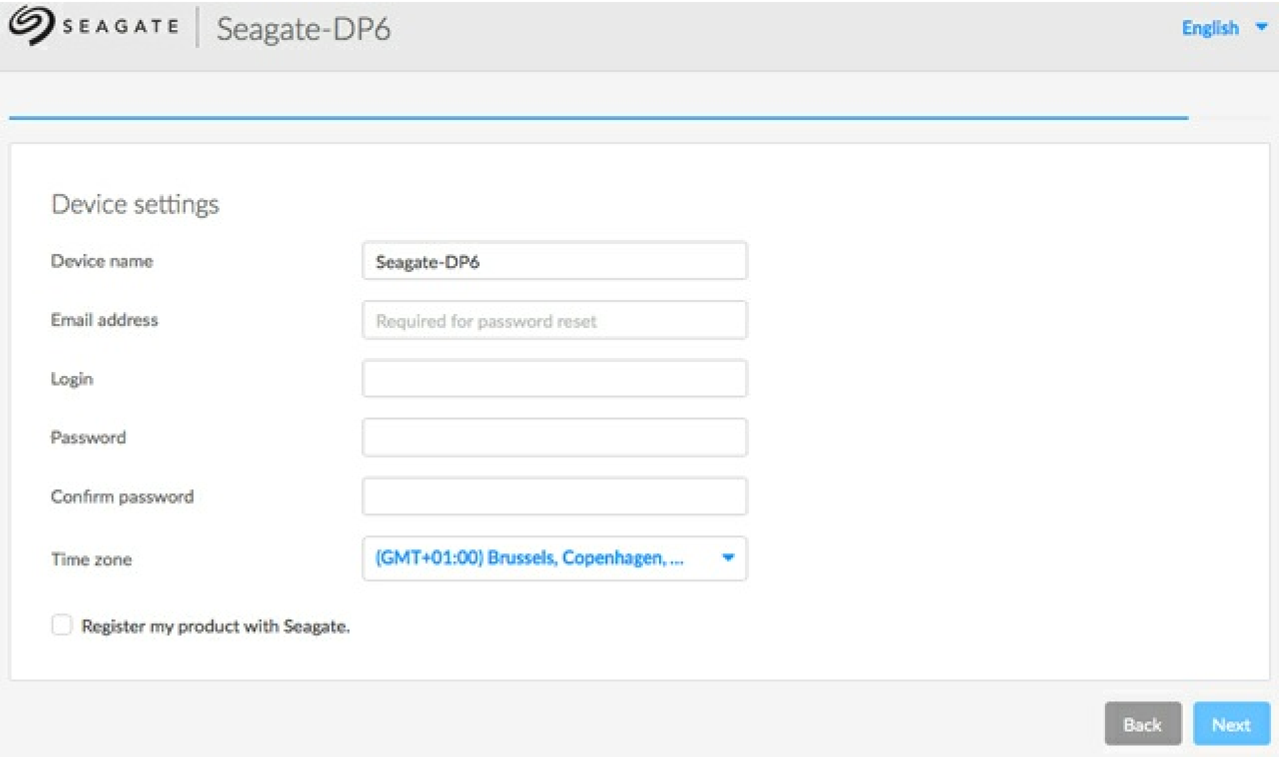
## Install Seagate NAS OS

**Important info:** The Seagate NAS OS installer must format the hard drives inserted into the NAS. **Data stored on the hard drives will be deleted. Make certain to back up data on the hard drives before installing them in the Seagate NAS enclosure.**

Consider the following before installing Seagate NAS OS:

- The NAS OS device's administrator should complete the installation steps.
- Make certain to boot the NAS before inserting new hard drives. Since the boot order for the NAS starts with the hard drives, you can encounter a problem if it detects an earlier version of NAS OS or another operating system.
- Insert the hard drives once the diskless enclosure is powered on and the status LED is blinking.
- The NAS checks for software updates during the installation. An error message informs you if it cannot check for updates due to a missing connection to the Internet. You have the option to search for updates after the installation.

The instructions for hardware installation are available on the quick start guide and user manual for your Seagate NAS. Make certain to follow the instructions before continuing with the steps below.



Device settings

| | |
|---|---|
| Device name | Seagate-DP6 |
| Email address | Required for password reset |
| Login | |
| Password | |
| Confirm password | |
| Time zone | (GMT+01:00) Brussels, Copenhagen, ... |

□ Register my product with Seagate.

1. Power on your Seagate NAS device. The device is ready to be accessed once the status LED turns solid.
2. From a PC/Mac connected to the same network as your NAS, launch an Internet browser and type **http://discover.seagate.com**
3. Follow the on-screen instructions. The setup formats the drives and installs NAS OS. During the installation, you can:
   - Create or change the name of the device.
   - Create or change the administrator login (the default is admin).
   - Create a Seagate Access account for remote access.
   - Configure or change the RAID level.
   - Adjust the time zone.

Make certain to note your login and password for future use. Upon completion, you are prompted to restart the NAS.

**Note on USB keys:** If your Seagate NAS requires a USB key to boot to the NAS OS installer, **you must remove the USB key before rebooting the device**. The NAS will use the USB key as the boot disk if it is not removed.
Upon reboot, the status LED turns on and begins to blink. The device is ready to be accessed once the status LED has turned solid and the welcome page appears on the NAS Setup Wizard.

## Next steps

- **Simplify NAS access:** Seagate recommends that you install the software utility *Seagate Network Assistant* before moving forward with the device configuration. Seagate Network Assistant gives you instant information on your Seagate NAS, such as firmware version, IP address, and MAC address. It will also provide quick access to shares and NAS OS. See Seagate Network Assistant for instructions.

- **Configure your NAS:** For details on how to configure and use your Seagate NAS, go to Shares: Access and Transfer Files and Device Manager.
- **Install Sdrive for local and remote access:** Sdrive gives you easy access to shares and NAS OS on local and offsite networks. For more information, see Remote Access.

# First Use: Update from NAS OS 3 to NAS OS 4

Your NAS OS 3 device alerts you when an update is available to NAS OS 4 or higher. You can update your Seagate NAS device by following the prompts to download and install NAS OS 4. The last step for the NAS OS update is rebooting the NAS OS device.

## NAS OS 3 and volume encryption

The first time you log into NAS OS 4, a pop-up window appears with important information regarding support for volume encryption. Since NAS OS 3 does not recognize volume encryption and other new features, you can lose important data when attempting to restore a NAS OS 4 device with NAS OS 3.

For further information, go to: Seagate NAS OS Installer.

You can find software downloads and instructions on how to update the USB rescue key from the NAS OS 3 installer to the NAS OS 4 installer.

# Seagate Network Assistant

Install Seagate Network Assistant on one or more computers connected to the same network as your NAS OS device. It is a software utility that helps you detect and access NAS OS devices on the network. Seagate Network Assistant gives you instant information on the NAS OS device's:

- IP address
- Version of software/firmware
- MAC address (hardware ID number)

Seagate Network Assistant can also help you:

- Launch NAS OS
- Mount one or more shares
- Auto-mount one or more shares

> **Important info on Seagate Network Assistant and NAS LAN Ports:** Seagate Network Assistant will always provide information on LAN 1, even if you have connected the NAS to your network using LAN 2.

**Note on LaCie NAS OS devices:** Seagate Network Assistant recognizes LaCie NAS devices running LaCie NAS OS 2.0 or higher.

# Install Seagate Network Assistant

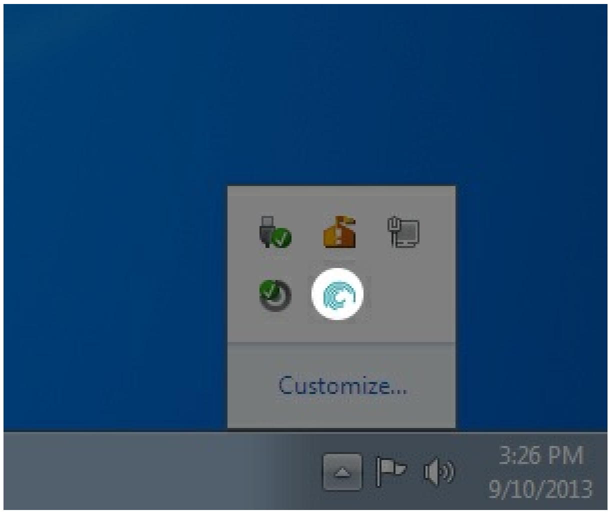
To avoid NAS detection conflicts, make certain that you are running the latest version of Seagate Network Assistant.

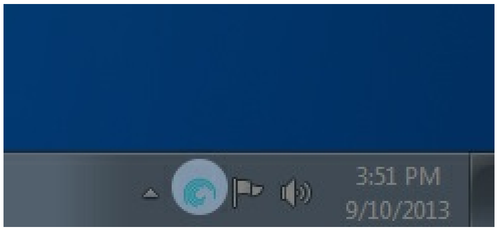
1. Download the Seagate Network Assistant installer for your operating system:
   - Windows
   - Mac
2. Follow the wizard to complete the installation.

# Launch Seagate Network Assistant

## Windows:

1. Select Seagate Network Assistant in **Start > All Programs/Programs.** The application icon will appear in the taskbar.



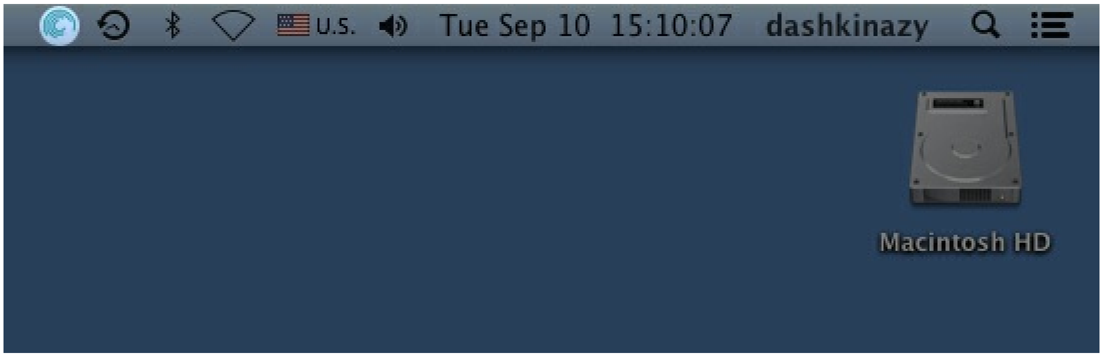


2. Right-click on the icon in the taskbar.

## Mac:

1. Select Seagate Network Assistant at **Go > Applications > Seagate Network Assistant**. The application icon

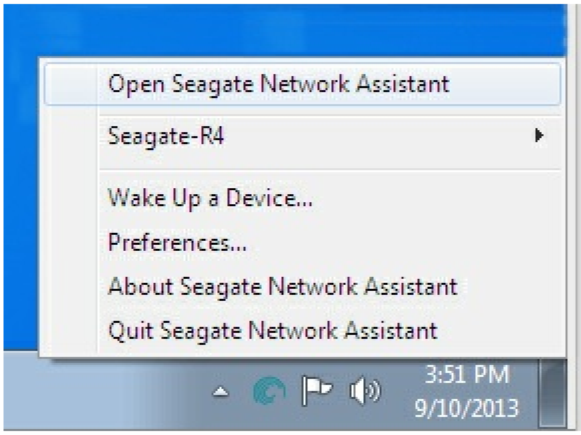
will appear in the menu bar.



2. Select the icon in the menu bar.

# Find your Seagate NAS's address information

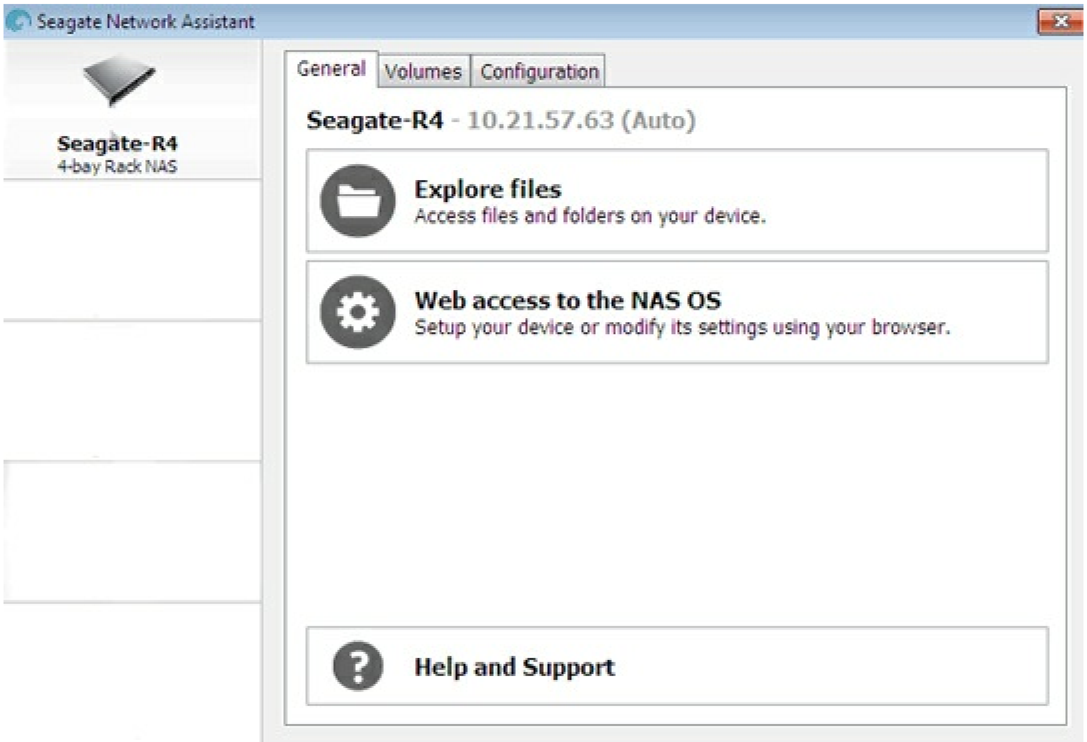
1. Launch Seagate Network Assistant.
2. *Windows users:* Right-click on the Seagate Network Assistant icon and choose **Open Seagate Network Assistant.** *Mac users:* Choose the Seagate Network Assistant icon in the menu bar to select **Open Seagate Network Assistant.**


Open Seagate Network Assistant
Seagate-R4
Wake Up a Device...
Preferences...
About Seagate Network Assistant
Quit Seagate Network Assistant
3:51 PM
9/10/2013

3. If you have multiple NAS OS devices, select the NAS you wish to access from the list on the left-hand column.
4. Choose the **Configuration** tab.
5. Review the device's:
   - IP address
   - Version of software/firmware
   - MAC address (hardware ID number)

# Access NAS OS with Seagate Network Assistant

1. Launch Seagate Network Assistant.
2. Choose your device:
   - *Windows:* Right-click on the Seagate Network Assistant icon in the taskbar to select your Seagate NAS.
   - *Mac:* Choose the Seagate Network Assistant icon in the menu bar to select your Seagate NAS.
3. Select **Web access to the NAS OS.**


Seagate Network Assistant

Seagate-R4
4-bay Rack NAS

Seagate-R4 - 10.21.57.63 (Auto)

**Explore files**
Access files and folders on your device.

**Web access to the NAS OS**
Setup your device or modify its settings using your browser.

**Help and Support**

4. The NAS OS login page will launch in an Internet browser.

# Mount shares

Seagate Network Assistant gives you many options to access your Seagate NAS's public and private shares.

## Quick access

1. Launch Seagate Network Assistant.
2. Choose your device:
   - *Windows:* From the taskbar, right-click on the Seagate Network Assistant icon and move the cursor to your Seagate NAS. Available shares will be listed.
   - *Mac:* From the menu bar, select the Seagate Network Assistant icon and move the cursor to your Seagate NAS. Available shares will be listed.
3. Choose the share you want to access.
4. The share will open in an Explorer window (Windows) or a Finder window (Mac). Public shares are available to everyone on the network. Private shares will prompt a user for a username and password .
   - *Administrator:* Use the credentials created during the initial setup or NAS OS login.
   - *User:* Type the login and password prepared by the administrator (see Users).
5. Transfer files normally between your computer and the share. *Mac users*: If the share does not open in a Finder window, navigate in the Finder to **SHARED > [machine name] > [share name].**

**Note on Quick Access to shares:** Private shares require a valid username and password.

# Mount

1. Launch Seagate Network Assistant.
2. Right-click on the icon in the taskbar (Windows) or choose the icon in the menu bar (Mac) and select **Open Seagate Network Assistant.**
3. If you have multiple NAS OS devices, select the NAS you wish to access from the list on the left-hand column.
4. Choose the **Volume** tab.
5. Double-click the share you wish to access. The share will open in an Explorer window (Windows) or a Finder window (Mac). Transfer files normally from your computer to the share.

**Technical note:** Mac users: If the share does not open in a Finder window, navigate in the Finder to **SHARED > [machine name] > [share name].**

**Note on mounting shares:** Private shares require a valid username and password.

# Authenticate private shares

1. Launch Seagate Network Assistant.
2. Right-click on the icon in the taskbar (Windows) or choose the icon in the menu bar (Mac) and select **Open Seagate Network Assistant.**
3. If you have multiple NAS OS devices, select the NAS you wish to access from the list on the left-hand column.
4. Choose the **Volumes** tab.
5. Select **Authentication.**
6. In the pop-up window, choose **Registered User** and enter your Username and Password. Select **OK.**
7. All available shares will appear in the list of volumes. If you do not see your volume, confirm that you have access to it (see Shares). Only the NAS administrator can set access rights to shares.
8. Select **Mount as drive** (Windows) or **Mount** (Mac) to open the share.
9. The share will be available in an Explorer window (Windows) or a Finder window (Mac).

# Auto-mount

1. Launch Seagate Network Assistant.
2. Right-click on the icon in the taskbar (Windows) or choose the icon in the menu bar (Mac) and select **Open Seagate Network Assistant**.
3. If you have multiple NAS OS devices, select the NAS you wish to access from the list on the left-hand column.
4. Choose the **Volumes** tab.
5. If the shares you wish to auto-mount is private, choose **Authentication** to enter your credentials. In the pop-up window, choose **Registered User** and enter the Username and Password for the share.
6. Choose **OK.** All available shares will appear in the list of volumes.
7. Select the checkbox for **Auto** to open the share. The share will now mount each time you boot the

computer. To cancel auto-mount, uncheck the box for **Auto.**

8. *Windows:* The share will mount in **Computer/My Computer** automatically when the computer detects it on the network. *Mac users:* The share icon will appear in your Finder automatically when the computer detects it on the network.

# Shares: Access and Transfer Files

## About shares

A *share* is a network volume that you can configure to store and share data. Your Seagate NAS has two shares by default: admin and Public. Following the initial login, the share *admin* changes to the name used by the administrator.

The following table lists the differences between private and public shares:

| Type | Accessibility | Login | Availability | Default share |
|---|---|---|---|---|
| Private | Login and password required | Password-protected | Computers on the network and remote access (must be enabled) | *admin* or user defined |
| Public | Available to any user on the network | None | Computers on the network and remote access (must be enabled) | Public |

For instructions on how to create and manage shares, see Shares.

## Access shares

You have several options for accessing shares.

*Option 1: Seagate Network Assistant - quick share access*
Use Seagate Network Assistant for quick access to public shares. See Seagate Network Assistant for details.

*Option 2: Seagate Network Assistant - authenticate for private shares*
Use Seagate Network Assistant to enter your username and password. See Seagate Network Assistant for details.

*Option 3: Operating system*
Use your operating system to open your NAS's shares.

*Option 4: Sdrive*
Sdrive gives users and administrators easy access to shares and NAS OS on local and remote networks. Sdrive's unique file integration places a volume in an Explorer window (Windows) or on the desktop (Mac). The volume contains all public shares and the private shares allotted to the user by the administrator. See

Remote Access for details.

## Windows

1. In an Explorer window address field, type the \\**[machine name]** or \\**[IP address]]** for your Seagate NAS.
2. Double click on the share you want to open.
3. Private shares will prompt you for your NAS OS username and password.

Alternatively, from the Start menu, select **Run** then type \\**[machine name]** or \\**[IP address]]**. Choose **OK.**

**Note on Bonjour:** If your Windows computer is running Bonjour, the address name must include **.local.** For example, \\**[machine name].local.**

## Mac

1. From the desktop, navigate to **Go > Connect to Server.**
2. In the dialogue window, type one of the following:

- **afp://[machine name].local**
- **smb://[machine name].local**
- **afp://[IP address]**
- **smb://[IP address]**

# Creating Shortcuts to Shares

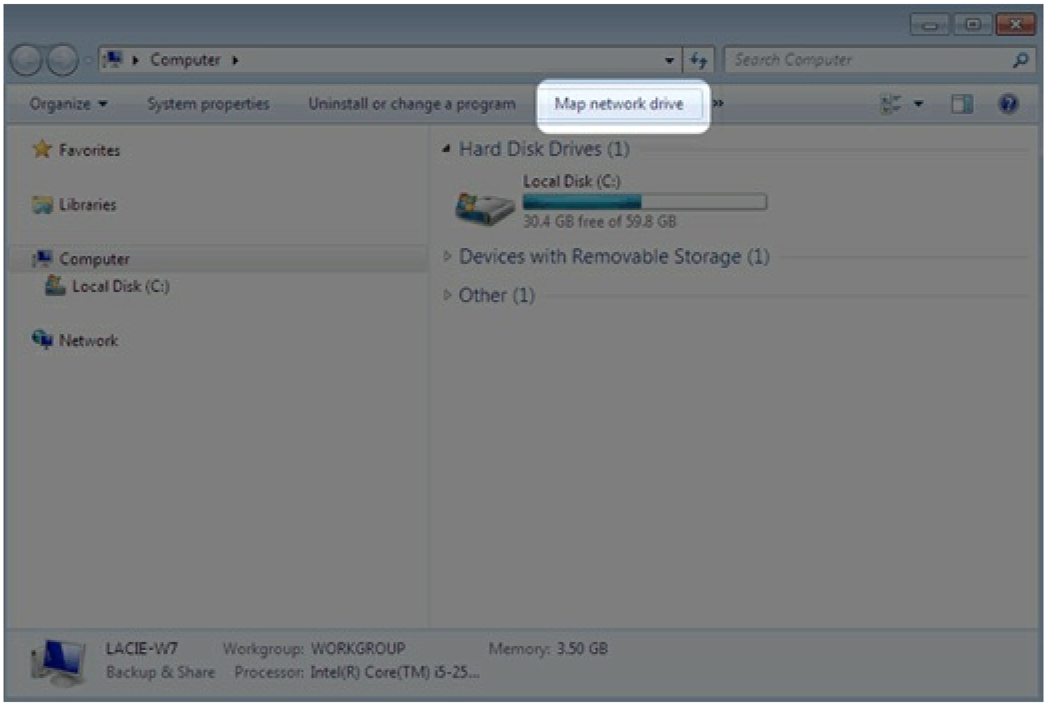
Create shortcuts to shares for quick access to your data

# Create shortcuts using Seagate Network Assistant

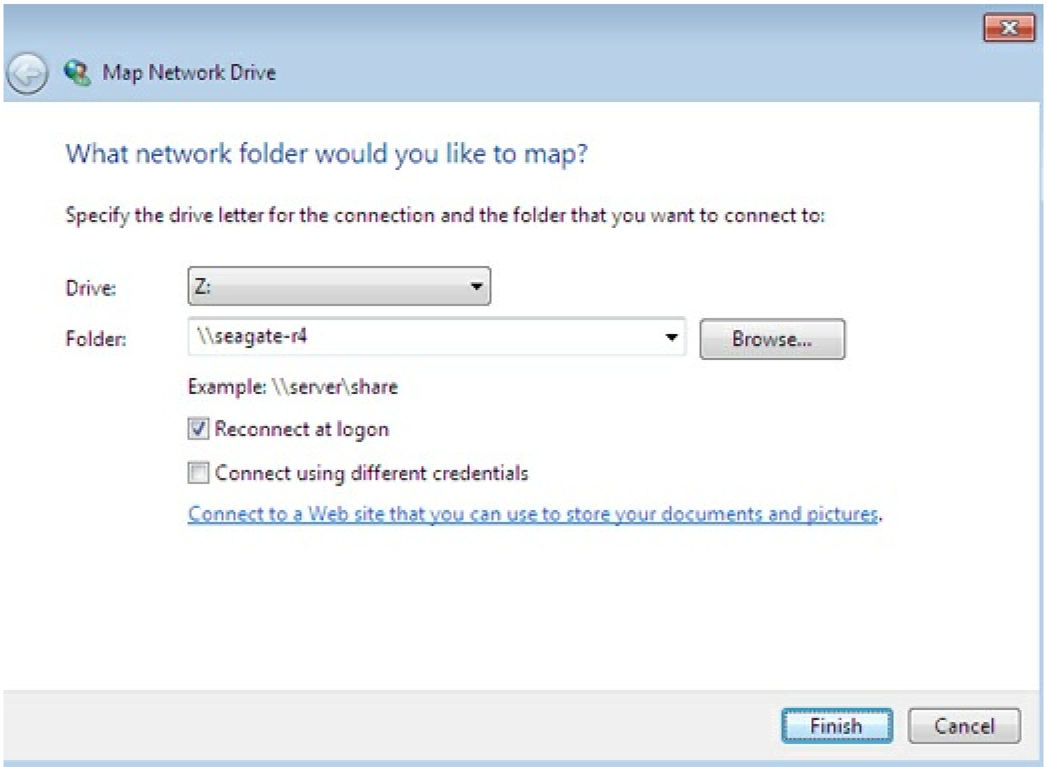
Seagate Network Assistant can be configured to automatically mount shares on your computer. See Seagate Network Assistant for details.

# Create shortcuts using the operating system: Windows 7

1. Open an Explorer window and navigate to **Computer.**
2. Choose **Map Network Drive.**



4. Browse to and select the share you want to access (private shares will prompt you for your NAS OS user name and password). Choose **OK.**
5. Select a drive letter in the pull-down menu and make certain that **Reconnect at logon** is selected.
6. Choose **Finish.**



What network folder would you like to map?

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

Drive: Z:

Folder: \\seagate-r4

Example: \\server\share

☑ Reconnect at logon

□ Connect using different credentials

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

## Windows 8 and 10

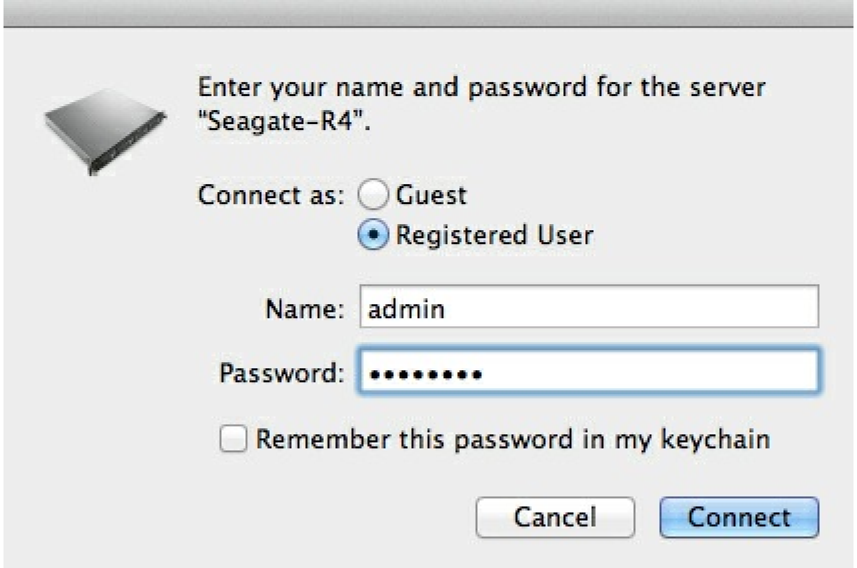
1. In an Explorer window address field, type the \\**[machine name]** or \\**[IP address]]** for your Seagate NAS.
2. Right click on the share you want to access and choose **Map Network Drive**.
3. Select a drive letter in the pull-down menu and make certain that **Reconnect at sign-in** is selected.

4. Choose **Finish**. Private shares will prompt you for your NAS OS user name and password.

# Create shortcuts using the operating system: Mac

## Mount

1. Open a new Finder window and choose your NAS in **SHARED > [machine name]**. All public shares will appear. To access private shares, choose **Connect As** and enter your NAS OS username and password.



Enter your name and password for the server "Seagate-R4".

Connect as: ○ Guest
● Registered User

Name: admin

Password: •••••••••

□ Remember this password in my keychain

3. Choose **Connect**.

## Mount at boot

1. Before following the steps below, make certain to mount the shares as described above.
2. From the Apple icon in the menu bar, select **System Preferences > Accounts > Login Items**.
3. Choose the "+" sign to add a new item to the list and browse for the shares that you mounted.

When you log on to the Mac operating system, the shares will automatically mount on your desktop. If the shares do not mount on the desktop, open a Finder window and check **SHARED**. If the shares are available in **SHARED** but are not visible on the desktop, go to the Finder preferences and change the settings to display connected servers on your desktop.

# Backup: Seagate NAS and PC/Mac

# Back up your NAS

See Backup Manager for a complete explanation on how to automate backups of data stored on your NAS. You can back up your data to:

- Direct-attached storage (DAS).

- Direct-attached storage (DAS).
- Another Seagate NAS OS device or compatible server on your local network.
- Another Seagate NAS OS device or compatible server on a remote/offsite network.
- Cloud storage (Amazon S3, Box, and more)

**Important info on NAS backup and RAID:** RAID is a great solution to keep your NAS running in case of disk failure. However, RAID is not a backup solution and it does not offer protection against all types of hardware failure. Therefore, administrators should back up NAS data to DAS or another NAS on a regular basis. See Backup Manager for details.

# Back up your computers

Your NAS is fully compatible with popular backup solutions such as:

- Windows Backup and Windows File History
- Apple Time Machine®

A share on your NAS can be set as a backup target for these and other backup software. Make certain that the user has access to the target share. Keep in mind that deleting the target share will also delete all associated computer backups.

**Note on Time Machine:** Time Machine must be enabled in NAS OS before a NAS share can be used as a backup destination. Go to **Device Manager > Services** to enable the Time Machine service. See Services for further details.

# Media Server

# UPnP/DLNA

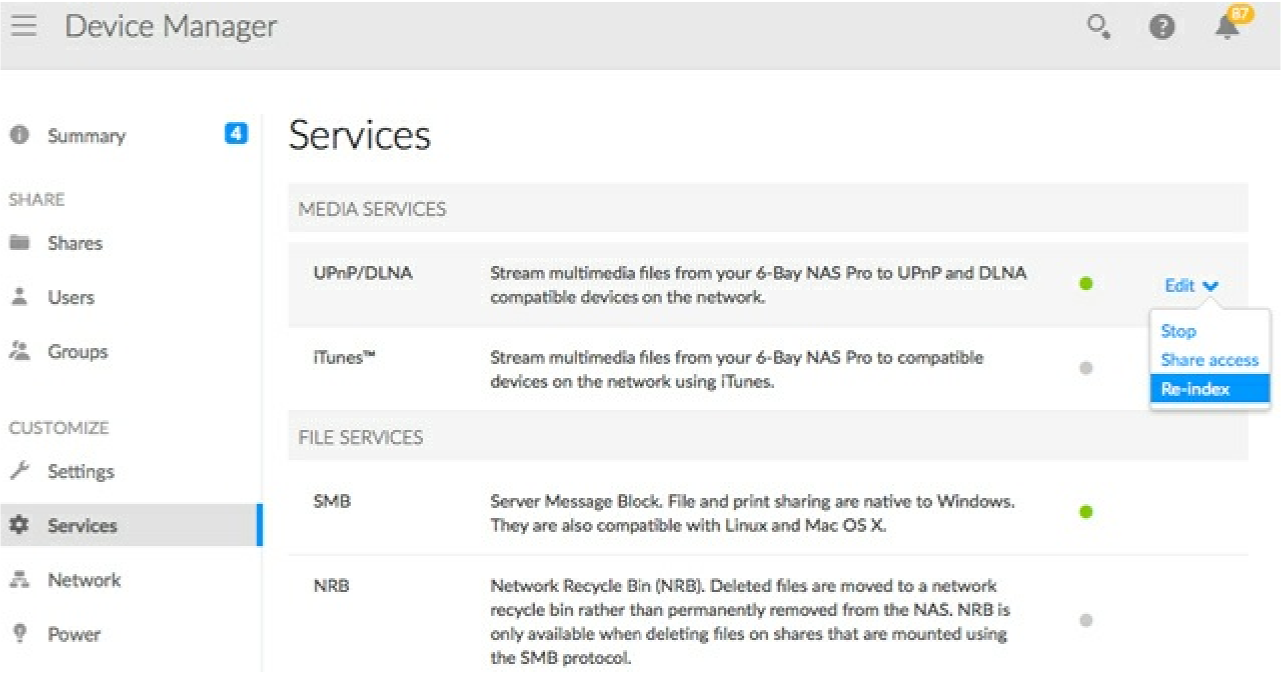
Configure your NAS to be a media server for UPnP/DLNA devices. To get started, enable UPnP/DLNA at **Device Manager** > **Services** (see Services). Once enabled, UPnP/DLNA-certified players connected to your network can play files located on your NAS. Examples of UPnP/DLNA players include Xbox, PlayStation, Smart TVs and many more.

Media files stored on public shares are identified without the need to enter a login and password. If you keep media files on private shares, make certain that your playback device is capable of requesting the credentials.

## Re-index the media server

To take an inventory of available multimedia files, you can re-index your NAS shares and desktop attached storage (DAS) connected to the NAS's ports.

1. If applicable, make certain that your DAS are connected to the NAS OS device.
2. Confirm that **UPnP/DLNA** is enabled at **Device Manager > Services** (see Services).
3. Pass the cursor to the right side of the **UPnP/DLNA** row to enable the pull-down menu and select **Edit**.
4. Choose **Re-index**.



Services

| MEDIA SERVICES | | |
|---|---|---|
| UPnP/DLNA | Stream multimedia files from your 6-Bay NAS Pro to UPnP and DLNA compatible devices on the network. | ● |
| iTunes™ | Stream multimedia files from your 6-Bay NAS Pro to compatible devices on the network using iTunes. | ● |
| FILE SERVICES | | |
| SMB | Server Message Block. File and print sharing are native to Windows. They are also compatible with Linux and Mac OS X. | ● |
| NRB | Network Recycle Bin (NRB). Deleted files are moved to a network recycle bin rather than permanently removed from the NAS. NRB is only available when deleting files on shares that are mounted using the SMB protocol. | ● |

Start a re-index as described above if files appear to be missing on your multimedia shares or connected devices.

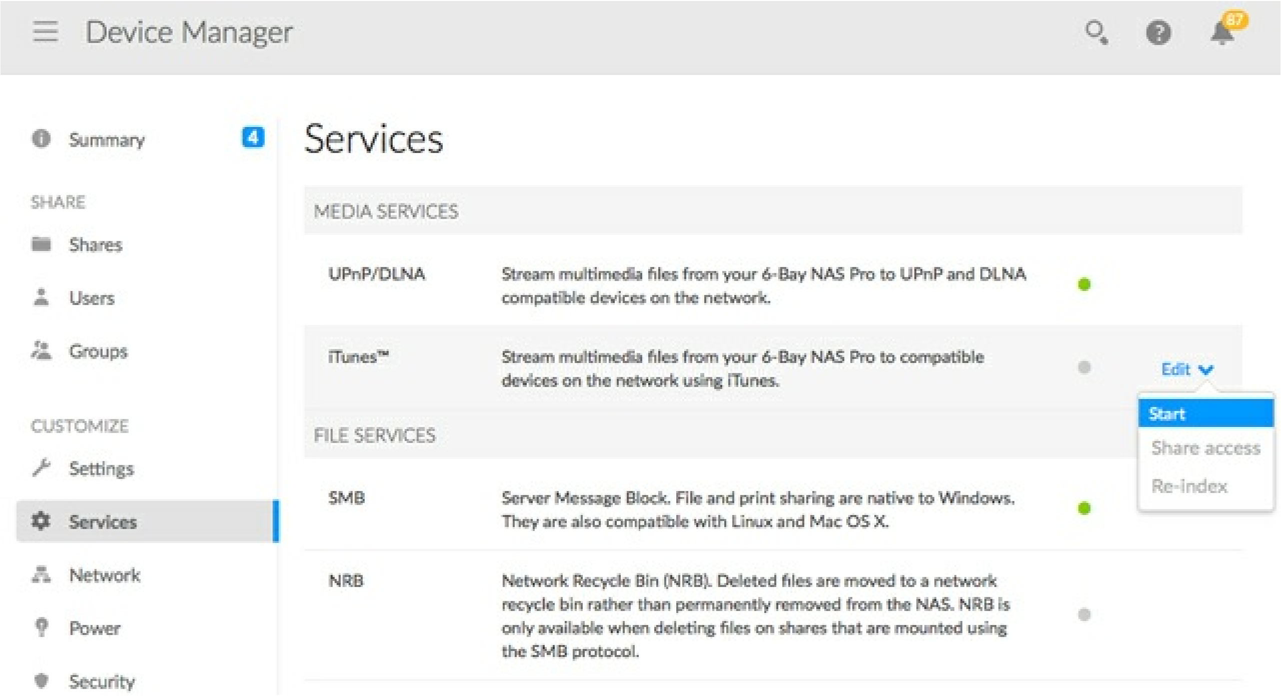
The time for indexing to complete depends upon the total capacity of your storage and the size of your multimedia library. If you have created many shares on your NAS, re-indexing can tax the CPU's resources. Before starting the re-index, consider shutting off multimedia support for shares that do not store media files. See Services and Shares for further information on how to manage services.

# iTunes

Your NAS can act as an iTunes music server. Copy your iTunes library to a share on your NAS and audio files will be available to compatible devices on the network. For easy access on the entire network, use a public share. To limit access to an iTunes library, use a private share with Seagate Network Assistant's **Authentication** (see Seagate Network Assistant).

To turn on network sharing, follow the steps below for your version of iTunes.

1. Enable the iTunes service on your NAS OS device. Go to **Device Manager > Services** (see Services).
2. Pass the cursor to the right side of the iTunes row and enable the **Edit** pull-down menu.
3. Choose **Start**.



Services

| MEDIA SERVICES | | |
|---|---|---|
| UPnP/DLNA | Stream multimedia files from your 6-Bay NAS Pro to UPnP and DLNA compatible devices on the network. | ● |
| iTunes™ | Stream multimedia files from your 6-Bay NAS Pro to compatible devices on the network using iTunes. | ● |
| **FILE SERVICES** | | |
| SMB | Server Message Block. File and print sharing are native to Windows. They are also compatible with Linux and Mac OS X. | ● |
| NRB | Network Recycle Bin (NRB). Deleted files are moved to a network recycle bin rather than permanently removed from the NAS. NRB is only available when deleting files on shares that are mounted using the SMB protocol. | ● |

4. To access the iTunes library, computers on the network should launch the iTunes application and choose the NAS OS device as the source for music.

**Technical note:** The iTunes Server Service supports the following file types: .mp3, .wav, .aac, .pls, and .m3u.

## Share music with iOS 9 devices

To share the iTunes library with iOS mobile devices:

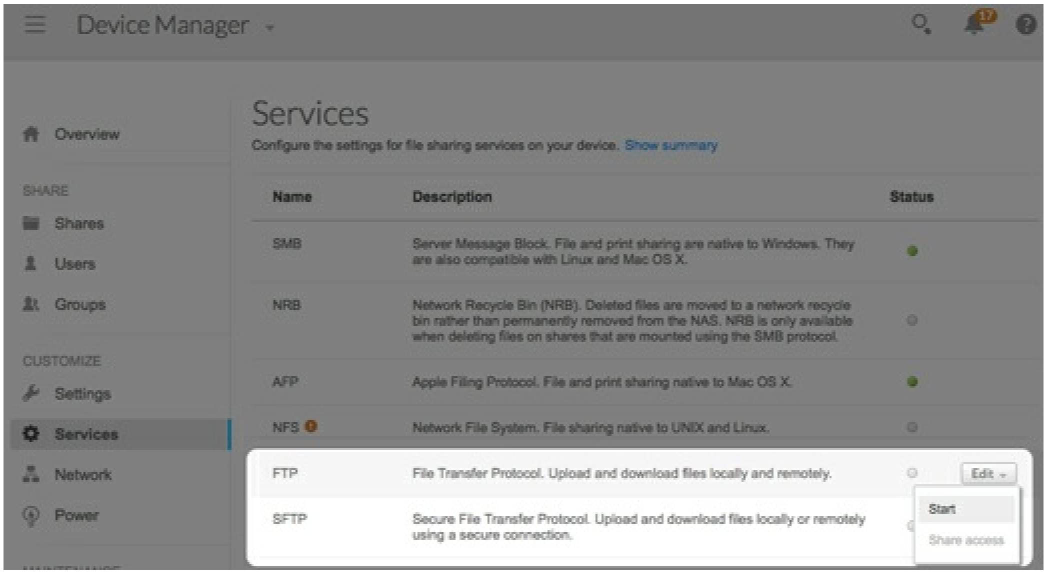
1. Mount the share with the iTunes library on a computer on the network.
2. Launch the iTunes application on the computer.
3. Enable sharing in iTunes Preferences.
4. On the iOS device, launch the Music app and tap the category pulldown menu.
5. Tap the home sharing option to view the iTunes library on your NAS.

Use public shares with iOS devices.

# FTP

FTP (file transfer protocol) is used to transfer files from one computer to another via the local network or the Internet. This protocol allows you to exchange files with your colleagues, clients, or business partners securely, as only people with a user account will have access.

The FTP service is disabled by default but you can start it at **Device Manager** > **Services** page (see Services).



Services

Configure the settings for file sharing services on your device. Show summary

| Name | Description | Status |
|---|---|---|
| SMB | Server Message Block. File and print sharing are native to Windows. They are also compatible with Linux and Mac OS X. | ● |
| NRB | Network Recycle Bin (NRB). Deleted files are moved to a network recycle bin rather than permanently removed from the NAS. NRB is only available when deleting files on shares that are mounted using the SMB protocol. | ○ |
| AFP | Apple Filing Protocol. File and print sharing native to Mac OS X. | ● |
| NFS | Network File System. File sharing native to UNIX and Linux. | ○ |
| FTP | File Transfer Protocol. Upload and download files locally and remotely. | ○ |
| SFTP | Secure File Transfer Protocol. Upload and download files locally or remotely using a secure connection. | ○ |

Once FTP is enabled, your NAS can be accessed using an Internet browser or FTP client software. FTP client software is very helpful if you wish to share, download, and upload data within a dedicated application rather than an Internet browser. Examples of FTP client software include Filezilla and Cyberduck.

# Local FTP access

To use the FTP service on your local network, enter your NAS's IP address or device name in the FTP client's address field or in an Internet browser's address field. Your NAS's IP address is available on the Network page or Seagate Network Assistant (see Network and Seagate Network Assistant).

## Public Access Folders (non-password protected)

ftp://[IP-address]/ (For example, ftp://192.168.10.149)
ftp://[machine name]/ (For example, ftp://seagate-r8 or ftp://seagate-r8.local )

## Private Access Folders (password protected)

When following the directions below, usernames and passwords can vary depending upon the user. For example, the administrator's username and password are not the same as another user's name and password.

- ftp://[username:password@IP-address] (For example, ftp://admin:adminpassword@192.168.10.149)
- ftp://[username:password@machine name]/ (For example, ftp://admin:adminpassword@seagate-r8/ or ftp://admin:adminpassword@seagate-r8.local/)

# Remote FTP access

You can access and share your NAS's files from a computer outside of your network. To use FTP, you will need to know your router's public IP address.

1. From a computer on the same local network as the NAS, visit this page to learn your public IP address: http://www.whatismyip.com/
2. Note your public IP address.
3. Launch an Internet browser or FTP client software. Within the Internet browser or FTP client's address field, type:

- Public folders only: ftp://[Public IP-address (For example, ftp://94.10.72.149)
- Public and private folders: ftp://[username:password@Public IP-address (For example, ftp://admin:adminpassword@94.10.72.149)

For further information on the public IP address for your router, see your router's user manual or your Internet service provider.

## SFTP

SFTP is a secure version of the FTP service. Data is more secure when using SFTP but transfer rates are slower. Similar to FTP, SFTP is disabled by default but you can start it at **Device Manager > Services**.

**Note on Network Backup Server and SFTP**: Activating Network Backup server will disable SFTP (see Backup Manager for details).

# NFS

p>Network File System (NFS) is a distributed file system protocol allowing the NAS to share directories and files with others over a network. Like SMB, NFS grants file-level access to users and programs.

NFS is widely distributed to host VMWare datastores or shared network folders in a Linux/UNIX environment.

When enabling the NFS service on a share, it can be accessed with the following path: [NAS_NAME_OR_IP_ADDRESS]:/shares/[SHARE_NAME]

The NFS protocol is not active by default. To activate it:

1. Go to **Device Manager > Services** (see Services).
2. Pass the cursor to the right side of the NFS row to enable the **Edit** pull-down menu.
3. Choose **Start**.

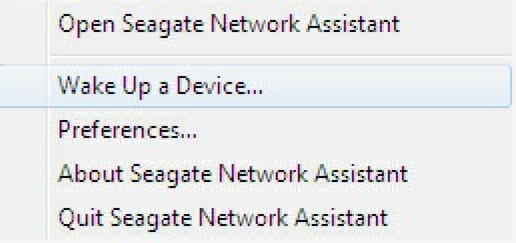
**Important info:** All NFS shares are public and available to everyone on the network.

# Wake on LAN (WOL)

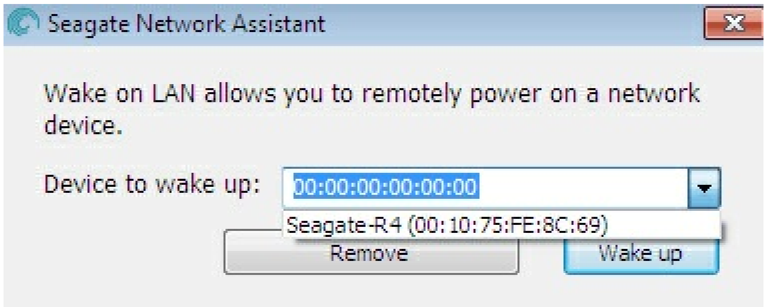
Your Seagate NAS can conserve energy by entering power saving mode. Use NAS OS to schedule power saving mode when no one accesses the Seagate NAS and wake it up when your office is ready to work. See Power for more information on power saving modes.

Seagate Network Assistant can wake your NAS if you require access before it is scheduled to exit power saving mode. This feature is called Wake on LAN (WOL). Follow the steps below:

1. Right-click the Seagate Network Assistant icon in the taskbar (Windows) or choose it in the menu bar (Mac).
2. Select **Wake Up a Device**.


Open Seagate Network Assistant
Wake Up a Device...
Preferences...
About Seagate Network Assistant
Quit Seagate Network Assistant

3. Choose the NAS from the pull-down menu.



Wake on LAN allows you to remotely power on a network device.

Device to wake up: 00:00:00:00:00:00

Seagate-R4 (00:10:75:FE:8C:69)

4. Choose **Wake up**.

**Note on the MAC address list**: If the list is empty the first time you launch **Wake Up a Device**, enter the device's MAC address in the field and select **Wake up**. Once entered, Seagate Network Assistant will keep the device's MAC address on the list.

You can also wake up a NAS by applying a short push to its power button.

# NAS OS Login and Navigation

Seagate NAS OS is a browser-based administration tool. Launch NAS OS to access apps, manage storage, add users, create shares, and much more.

## Log in to NAS OS

Access the NAS OS login page with one of the following:

- Seagate Network Assistant
- An Internet browser

## Seagate Network Assistant

See Seagate Network Assistant for instructions on software installation.

1. **Windows:** Right-click on the Seagate Network Assistant icon in the system tray.
   **Mac:** Choose the Seagate Network Assistant icon in the menu bar.
2. Select **[machine name] > Web Access.**
3. The login page will open in a new browser window or tab. If your browser is not open, Seagate Network Assistant will open it for you.

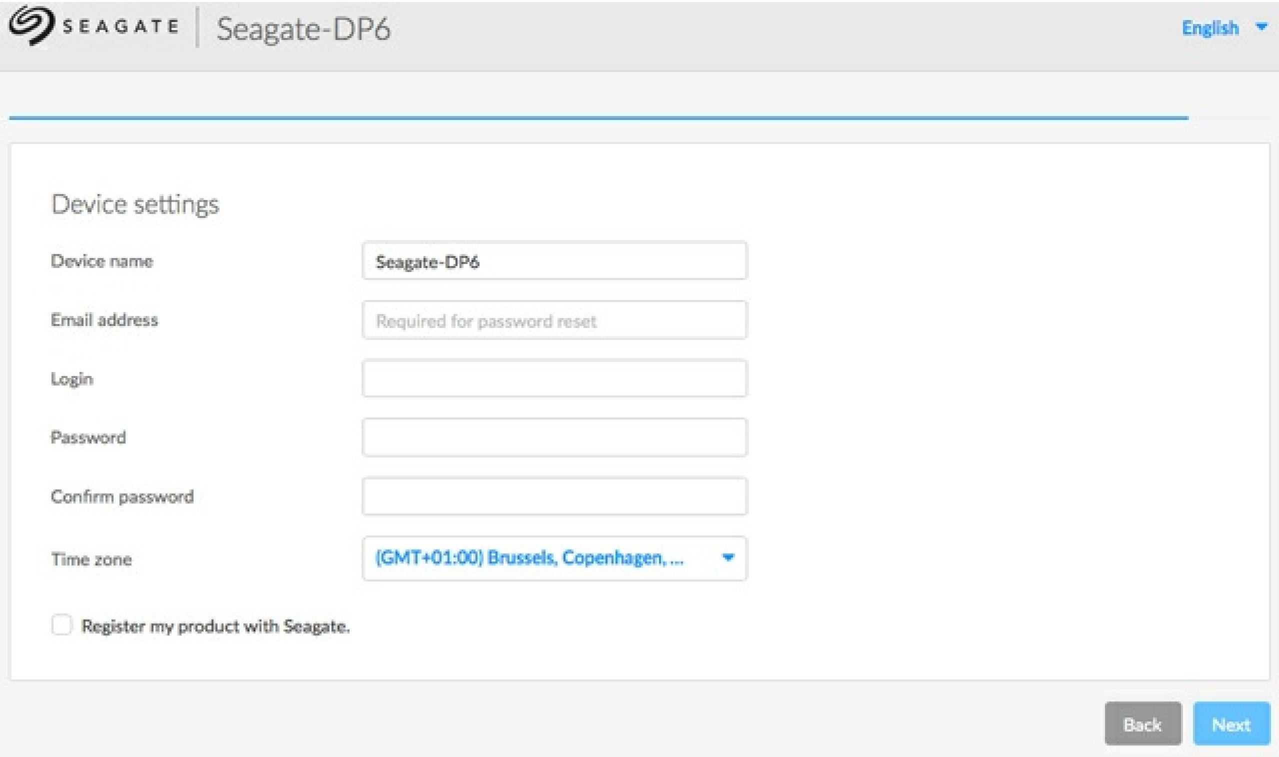
## Internet browser

Launch an Internet browser and type the default address for the NAS OS device:

- Windows without Bonjour: http://seagate-r4 or http://seagate-dp6
- Windows with Bonjour and Mac: http://seagate-r4.local or http://seagate-dp6.local.

You can also type your NAS's IP address in the browser's URL (web address) field. For example: http://[IP-address]. The IP address may be found in Seagate Network Assistant (see Seagate Network Assistant).

### First login



Device settings

Device name: Seagate-DP6

Email address: Required for password reset

Login:

Password:

Confirm password:

Time zone: (GMT+01:00) Brussels, Copenhagen, ...

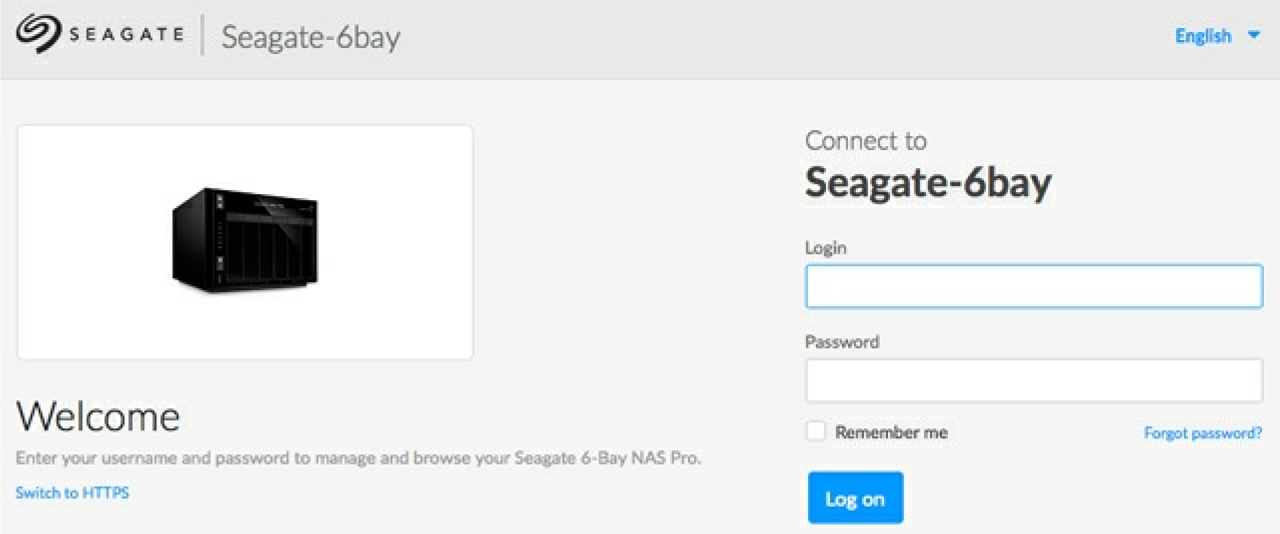
□ Register my product with Seagate.

For most users, the first NAS OS login is the final step of the setup wizard. You are prompted to:

- **Create a device name.** The default name of your NAS is based upon the product model. You can change it to meet the needs of your environment.
- **Create an administrator login name.** The default is *admin* but you have the option to change it. A login name should be from 1-20 alphanumeric characters.
- **Create and confirm the administrator's password.** The password should be from 4-20 alphanumeric characters and symbols. Consider using a strong password that is difficult for others to guess.
- **Create or reconfigure the RAID level.**
- **Set the time zone.**
- **Read and agree to Seagate's Terms and Conditions.** The box must be checked to complete the installation.

i **Important info on login credentials**: Make certain to note your login credentials. NAS OS can help users create a new password if the original password is not available. However, the option to recover a password requires that the administrator add settings to Notifications and Users. Further information on how to set up password recovery is listed below.

# Login



Welcome

Enter your username and password to manage and browse your Seagate 6-Bay NAS Pro.

Switch to HTTPS

NAS OS prompts you for your login name and password. To avoid entering your credentials with each login, check the box next to **Remember me.**

For added security when logging in, choose **Switch to HTTPS** at the NAS OS login page. While it offers more protection than HTTP, using HTTPS can affect your NAS's performance.

# Recover a Lost Password

The administrator can configure NAS OS to help users recover forgotten or lost passwords. The administrator must:

- Assign an email server (see Notifications).
- Enter an email address for users (see Users).

If the above conditions have been met, the administrator or user can follow the steps below to recover a password:

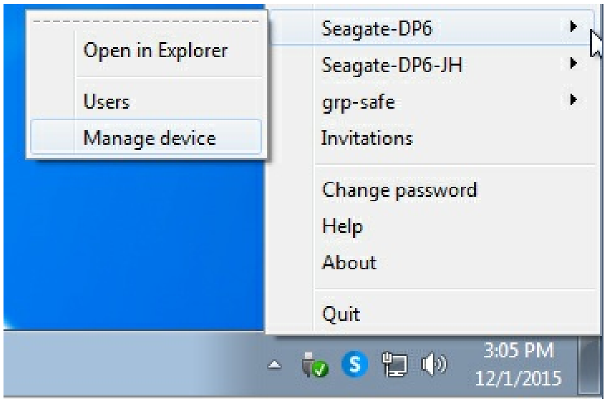
1. On the login page, choose **Can't access your account?**
2. Enter the login and type the Word verification (this ensures that the request is coming from a person).
3. Choose **Send.**
4. A recovery email arrives in the user's inbox. In the email, choose the **Click here** link.
5. In the **Reinitialize your password** window, type your login and new password.
6. Choose **Send.**

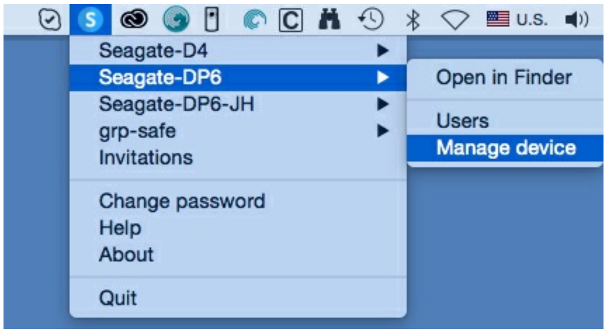
# Launch NAS OS using Sdrive

Install Seagate Sdrive on your PC/Mac to access your device's home page. You must have a Seagate Access account to use Sdrive. See Sdrive for instructions on how to download and install the application.

Make certain that Sdrive has been launched before following the directions below:

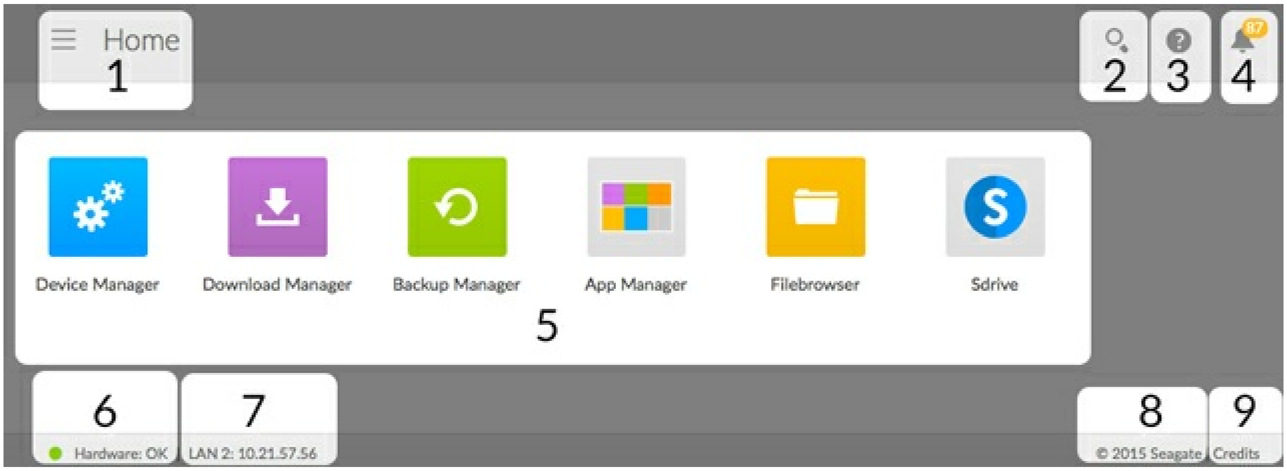
1. Choose the device you want to access.
    - **Windows**: Right click the Sdrive icon in the system tray to choose the Seagate device.
    - **Mac**: Click the Sdrive icon in the system tray to choose the Seagate device.
2. Choose **Manage device**.



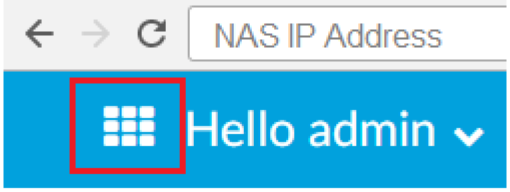


# NAS OS Navigation

NAS OS provides options to access apps, get help, review events, and much more. While the central pane interface will adjust to the app that you select, the framed options remain available for easy access. The central pane is number 6 in the graphic below.



**Important note**: Since NAS OS 4.3, there is no longer a Home Page. After logging into the NAS OS User Interface, it will default to the Filebrowser app. All other apps such as Device Manager and Backup Manager are easily accessible using the App Button located in the top left corner:



1. **Menu**: Select the menu to:
    - Choose an app

    - Quit an open app
    - Logout
    - Restart
    - Shut down
2. **Search**: Choose the magnifying glass icon to enable the search field. Type a search term that applies to your NAS OS device.
3. **Help**: Choose the question mark to review the NAS OS user manual or create a support case.
4. **Notifications**: Choose the bell icon to review the latest events on your NAS OS device. Event options include *All*, *Warning*, and *Error*. You can also select **View all notifications** to be directed to the Notifications page.
5. **Apps**: The Home page's central pane presents apps from Seagate and third party developers. Choose an app to be directed to its interface. Only the central pane will change based upon the app you have selected. Core NAS OS features are divided into default apps:
    - **App Manager**: Add and manage apps.
    - **Backup Manager**: Create and manage backup jobs.
    - **Device Manager**: Change the settings, add users, create shares, and much more.
    - **Download Manager**: Create and manage download jobs.
6. **Hardware state**: A green light indicates that the NAS 's hardware is operating as expected. Click it to see a pop-up window with additional details regarding the hardware.
7. **LAN connection and IP address**: The LAN ports connected to the network and their IP addresses.
8. **Copyright**
9. **Credits**: Click **Credits** to see the open source licensing information.

# Login: administrator and user

# Administrator

An administrator has access to all NAS OS management functions. However, an administrator does not have access to all shares by default. The administrator must assign access to himself, similar to standard users.

# User

The default apps for a user are:

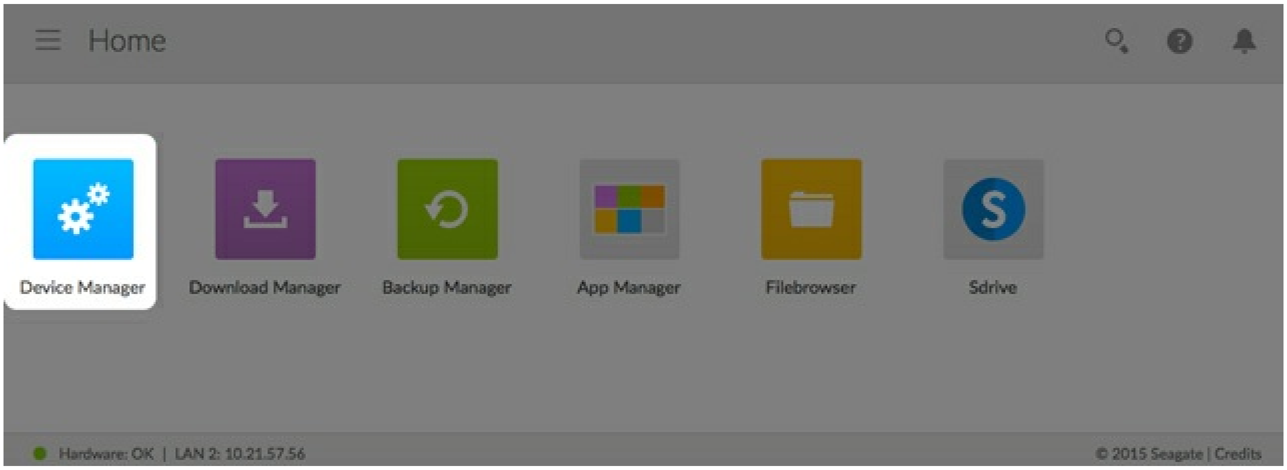
- **Filebrowser**: Internet-based browser for shares that the user has been granted access to.
- **Device Manager** (limited): The user can change his language and password preferences. The administrator has the right to change a user's password at any time.

# Device Manager

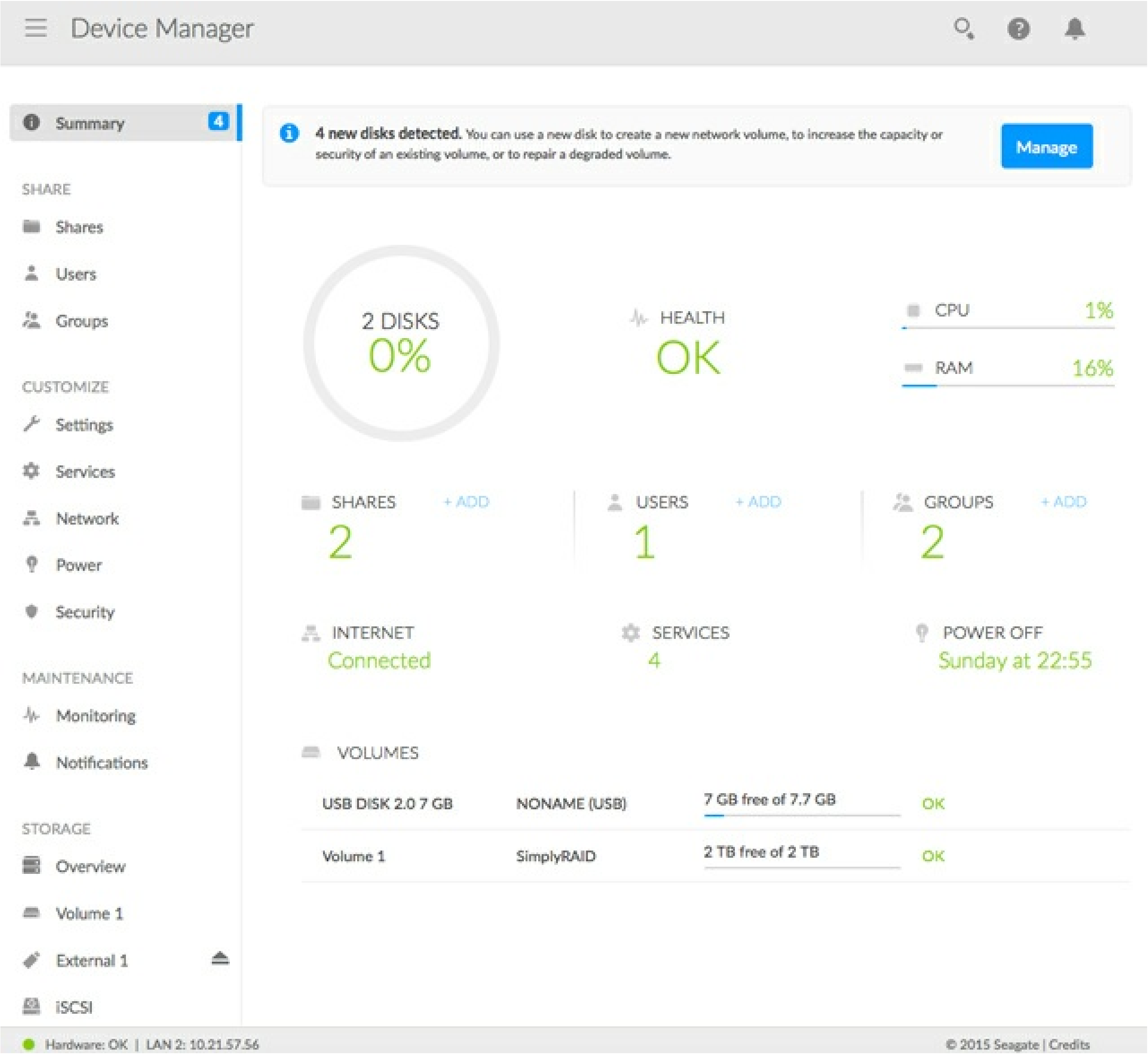
The Device Manager app is the heart of NAS OS management. Use Device Manager to configure important settings such as users, shares, storage, and much more.

## Launch Device Manager

Launch Device Manager from the Home page by choosing its app icon.



## Device Manager navigation



**4 new disks detected.** You can use a new disk to create a new network volume, to increase the capacity or security of an existing volume, or to repair a degraded volume.

2 DISKS 0%

HEALTH OK

CPU 1%

RAM 16%

SHARES 2

USERS 1

GROUPS 2

INTERNET Connected

SERVICES 4

POWER OFF Sunday at 22:55

VOLUMES

| | | | |
|---|---|---|---|
| USB DISK 2.0 7 GB | NONAME (USB) | 7 GB free of 7.7 GB | OK |
| Volume 1 | SimplyRAID | 2 TB free of 2 TB | OK |

Hardware: OK | LAN 2: 10.21.57.56

© 2015 Seagate | Credits

The left pane lists the NAS OS management pages. Choose a page to manage its settings. The central pane changes to reflect the selected page.

For example, click **Network** to review or revise settings for the Ethernet ports, port forwarding, MyNAS, and more. Upon choosing *Network*, the central pane changes to the interface for the page.

*Overview* is the default page when first launching Device Manager. It gives you a summary of the NAS's health and shortcuts to important settings.

- Review the storage capacity, health and processor/RAM consumption.
- *Get* quick summaries of the settings *Shares*, *Users*, *Groups*, *Network*, *Services* and *Power*.
- Click on a summary to go to its page. You can also add *Shares*, *Users*, and *Groups* from the *Overview* page by choosing +**Add** at the applicable setting.

## Toggle to another app

On the upper left of the window, click the menu icon (three horizontal lines) and then choose **Device Manager** or **the down arrow > [App name].**

# Shares

Your NAS's storage is divided into shares, also known as network folders. The Shares page allows you to create new shares, assign access rights to users and groups, and to adjust services by share. By default, your NAS OS device has two shares, *admin* and *Public*. You can begin working with these shares immediately and create new shares as needed.

**Note on the admin share name:** The name of the share *admin* will update automatically if the administrator changes the login name from the default **admin**. For example, if the administrator used her name, Sally, during the installation, *admin* becomes *Sally*.

**Important info**: In text fields, you can enter 1 to 20 characters using letters, numbers, hyphens, and underscores. No other symbols, special characters, punctuation, or spaces may be used. Do not begin or end with a hyphen or underscore.

# Shares, Users, and Groups

Allotting storage and network permissions for multiple departments and users in a branch office or corporate network can be complicated. It takes forethought and planning to configure which user is part of what group with access to how many shares. For this reason, the settings *Shares*, *Users*, and *Groups* are closely related in NAS OS. The cross-functionality between these three settings allows the administrator to add users to groups in the *Users* or *Groups* settings as well as shares to users and groups in the *Users* and *Groups* settings. The wizard for each setting prompts the administrator to choose shares, users, and groups. Additionally, users and groups can be added to a new share when following the *Add share* wizard.

However, creating a new share, user, or group requires that the administrator use its respective setting. For example, the administrator must choose the *Shares* setting to add a new share and the *Users* setting to add a new user. Though each setting can be revised at any time, it is highly recommended that the administrator plan ahead when first adding shares, users, and groups to NAS OS. With a map of users, groups, and shares, the administrator can simplify access rights. See the example below.

## Sample setup: Shares, Users, and Groups

An administrator has mapped permissions for 40 shares, 20 users, and 10 groups.

To get started, the administrator adds the 20 shares using the *Add share* wizard on the *Shares* page. The administrator ignores the prompts to add users and groups to each share since new users and groups have yet to be created.

Next, the administrator adds the 20 users using the *Add user* wizard on the *Users* page. The administrator ignores the prompts to add users to shares and groups since new groups have yet to be created.

Finally, the administrator adds the 10 groups using the *Add group* wizard on the *Groups* page. In this step, the administrator will assign:

- Each user to a specific group
- Share permissions for each group

The *Groups* setting is the last step since it can cover more users at one time rather than assigning share permissions for each new user.

The generic sample setup may not apply to all environments. However, NAS OS gives the administrator free reign to configure permissions on the Shares, Users, and Groups pages.

# Public and private shares

The following table shows the differences between private and public shares:

| Type | Accessibility | Login | Availability | Default share |
|---|---|---|---|---|
| Private | Login and password required | Password-protected | Computers on the network and remote access (must be enabled) | *admin* or user defined |
| Public | Available to any user on the network | None | Computers on the network and remote access (must be enabled) | Public |

# Existing shares

Shares are organized in a table:

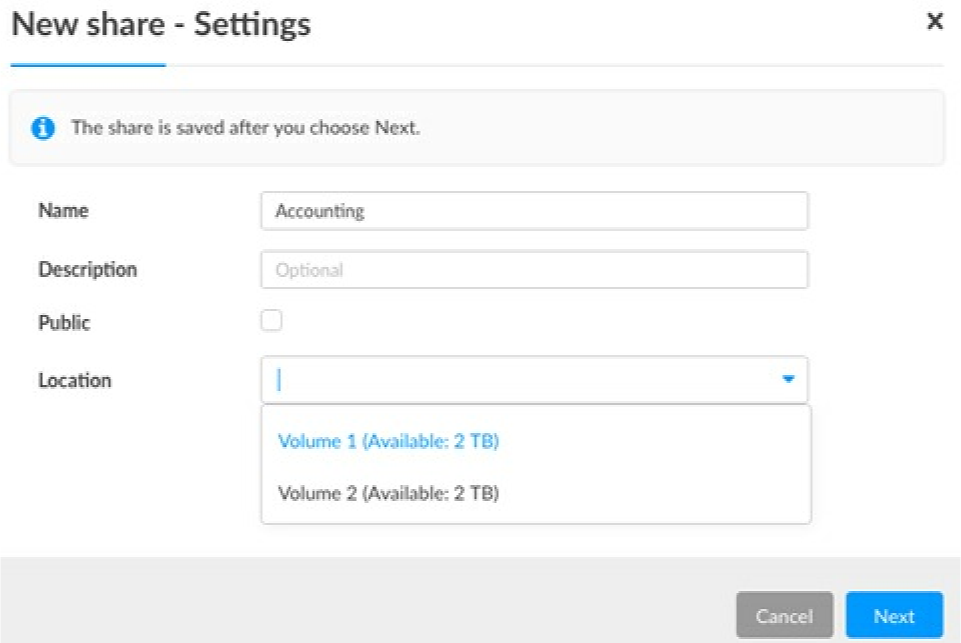
- Click on the text in the **Name** column to change the share name.
- Click on the empty space or text in the **Description** column to add or revise details for the share (optional).
- The number in the **Groups** column (two silhouettes) shows how many groups have access to the share. Click on the number to view and edit the group. *Public* indicates that the share is available to everyone on the network.
- The number in the **Users** column (one silhouette) shows how many users have access to the share. Click on the number to view and edit user access. *Public* indicates that the share is available to everyone on the network.
- Click on the text in the **Services** column to add or remove services. Only active services are available. See below for instructions on how to adjust services on a share and Services for details on how to enable and disable services in NAS OS.

- To review and edit the options for a share, pass the cursor to the far right of its row to make the **Edit** pull-down menu visible. Most of the options are explained above. Additional options include changing network access (public or private) and deleting the share.

# Add share

Choose **Add share** and follow the wizard to completion. Consider the following when creating your share:

- The **Add share** wizard features four steps: *name the share*, *Set group permissions*, *Set user permissions*, and *Summary*.
- *Name the share*: A share must have a name from 1 to 20 characters using letters, numbers, hyphens, and underscores. Do not begin or end with a hyphen or an underscore.
- *Name the share*: If your NAS OS device has more than one volume, a pull-down menu allows you to select the volume for the share.



New share - Settings

The share is saved after you choose Next.

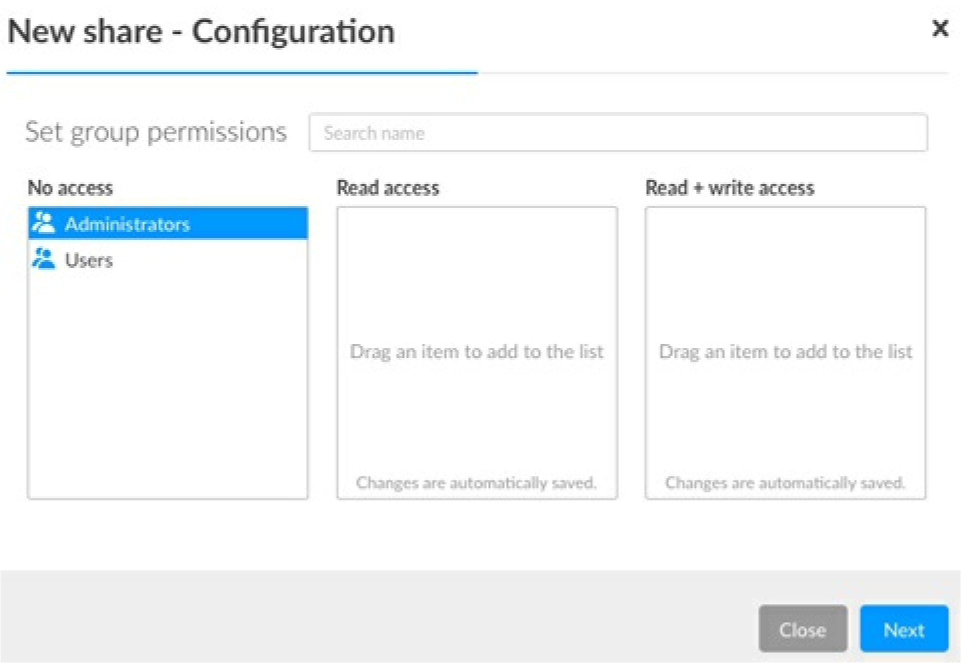
Name: Accounting

Description: Optional

Public: □

Location:

- *Name the share*: Checking the box next to **Public** gives everyone on the local network access to the share.
- *Set group permissions/Set user permissions*: The administrator can skip these steps if permissions will be assigned in the Users or Groups settings. Choose **Next** to reach the *Summary*.
- *Set group permissions/Set user permissions*: When adding groups or user permissions, you must drag selected items to the *Read access* column or the *Read+write access* column. To add multiple items, make all your selections before dragging them to a column.


New share - Configuration
×
Set group permissions
Search name
No access
Administrators
Users
Read access
Drag an item to add to the list
Changes are automatically saved.
Read + write access
Drag an item to add to the list
Changes are automatically saved.
Close
Next

- *Set group permissions/Set user permissions*: If a user or group is mistakenly dragged to the *Read access* column or *Read+write access* column, you can drag it back to the *No access* column.
- *Set user permissions*: Checking the box next to **Enable Read access to guests on the network** allows all users on the network to view files on the share. However, they cannot modify files or write data to the share.

# Add remote share: distributed file system namespaces (DFS-N)

During the course of a day, a user may access multiple files stored on many shares connected to your local area network (LAN). To find all the shares and volumes spread about the network, a user can hunt through a long list of NAS devices and servers.

NAS OS DFS-N allows administrators to add compatible shares to a single NAS OS device. Accessing shares on a single device simplifies data management for the administrator and the user. Similar to creating a new share, the administrator adds remote shares from other NAS OS devices or servers on the LAN. The other NAS OS device or server is called the Host.

NAS OS DFS-N supports NAS OS shares and SMB shares/volumes. SMB or, server message block, is a standard protocol for sharing network volumes. It is native to Windows and supported on Mac OS.

## Add remote share

Choose **Add remote share** and follow the instructions below for your Host type:

**NAS OS Host**

1. The wizard searches the local network for NAS OS devices. Select the host NAS OS device for the shares

you want to add and choose **Next**.

2. Enter your credentials for the host NAS OS device and choose **Next**. In most instances, you will use a login with administrator rights. You can choose **Guest** when adding public shares.
3. Select the shares to add and choose **Next**. If you do not see the shares you want to add, make certain that the credentials you entered in step 2 have access rights to the shares on the host NAS OS device.
4. Review the Summary page and choose **Finish**.

### Third party NAS or server Host

1. Enter the IP address for the host in the empty field and choose **Next**. Though an IP address is generally more reliable, you can also enter the NAS's/server's network name.

> i **Important info**: Even if you succeed in adding the share/volume using the Host's name, you can experience problems when attempting to access the volume on a PC/Mac. This may be due to the network's naming service. Should you encounter issues with the network name, it is recommended that you try again using the IP address.

2. Enter the name of the share on the host NAS/server and choose **Next**.
3. Review the *Summary* page and choose **Finish**.

## Adding remote shares on offsite networks

NAS OS gives you the option to add shares/volumes from NAS OS and third party NAS/server devices that are located outside the LAN (offsite network). When choosing the Host NAS, follow the instructions for *Third party NAS or server Host*, even if you want to access a NAS OS device. When choosing the NAS, you must enter its public IP address and use the proper credentials.

Seagate cannot guarantee the stability and performance of remote shares/volumes from offsite networks. There are many factors that can affect the connection including, but not limited to: firewalls, security settings, routers, Internet service providers, and administration.

## Share tabs

Adding remote shares to the NAS changes the *Shares* page. There are two tabs:

- **Local**: Access all shares created on the NAS.
- **Remote**: Access all shares added from other NAS devices.

## Managing remote shares/volumes

The host NAS/server manages its shares. Only the administrator for the host NAS device can adjust the remote shares' credentials, access rights, quotas, etc.

To avoid potential conflicts with accessing remote shares, administrators should use the same credentials on the NAS OS device and the host NAS/server. For example, Logan is a user on the NAS OS device *Seagate-DP6*. The administrator for *Seagate-DP6* has added a remote volume called *Data*. The host server for Data is called *Seagate-DWSS4*, a Windows server. The administrator for *Seagate-DWSS4* must create a login and password for Logan. To make the login experience to *Data* easier for Logan, the administrators for *Seagate-DP6* and *Seagate-DWSS4* agree to use the same credentials on both NAS devices.

The administrator for the NAS OS device can revise how the name appears on the *Shares* page and users on the network:

1. Choose the **Remote** tab
2. Locate the remote share you want to rename and click on the words in its name column.
3. Enter the name in the field.

## Accessing remote shares/volumes

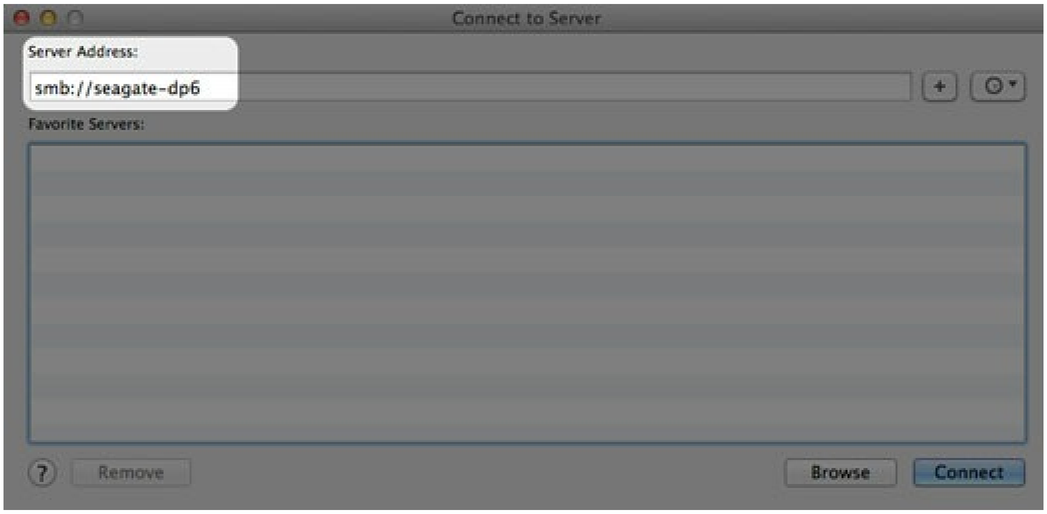
Accessing remotes shares is similar to accessing shares created on the NAS OS device. There are minor differences that administrators should consider before authorizing users to access remote shares. Review the information below before adding remote shares to your NAS OS device.

**The host NAS/server manages the remote share/volume**. Since management includes credentials, make certain that applicable usernames and passwords have been added to the host NAS/server. For example, Logan is a user on the NAS OS device *Seagate-DP6*. The administrator for *Seagate-DP6* has added a remote volume called *Data*. The host server for *Data* is called *Seagate-DWSS4*, a Windows server. The administrator for *Seagate-DWSS4* must create a login and password for Logan. To make the login experience to Data easier for Logan, the administrators for *Seagate-DP6* and *Seagate-DWSS4* agree to use the same credentials on both NAS/server devices.

**SMB is native to Windows**. Users with Windows computers can access remote shares/volumes using the operating system or Seagate Network Assistant. For further details, see Shares: Access and Transfer Files. When first accessing the remote share, the user will be prompted for the username and password created on the host NAS/server.

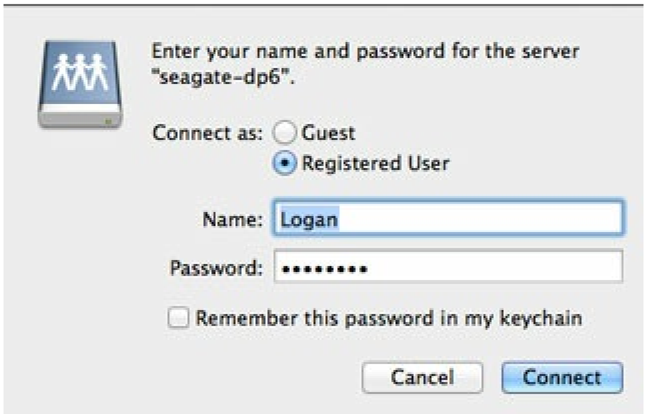
**SMB is supported on Mac OS**. The native protocol for Mac OS is Apple File Protocol (AFP). Each time that a Mac user attempts to access a network drive, it will automatically use AFP rather than SMB. Therefore, a Mac user cannot access remote shares with Seagate Network Assistant since the application uses the operating system's default network settings. Mac users should follow the instructions below when accessing a remote share/volume:

1. Go to **Finder > Go > Connect to server**.
2. In the *Server Address field*, enter **smb://[name of NAS OS device]** and choose **Connect**. Entering **smb** is very important since it tells the operating system to use the SMB protocol when searching for shares/volumes on the NAS.



Server Address: smb://seagate-dp6

3. The user is prompted for a *Name* and *Password*. As recommended above, the administrators for the NAS OS and host devices should use the same credentials for users. Enter the username and password created on both devices. Choose **Connect**.



Enter your name and password for the server "seagate-dp6".

Connect as: ○ Guest
● Registered User

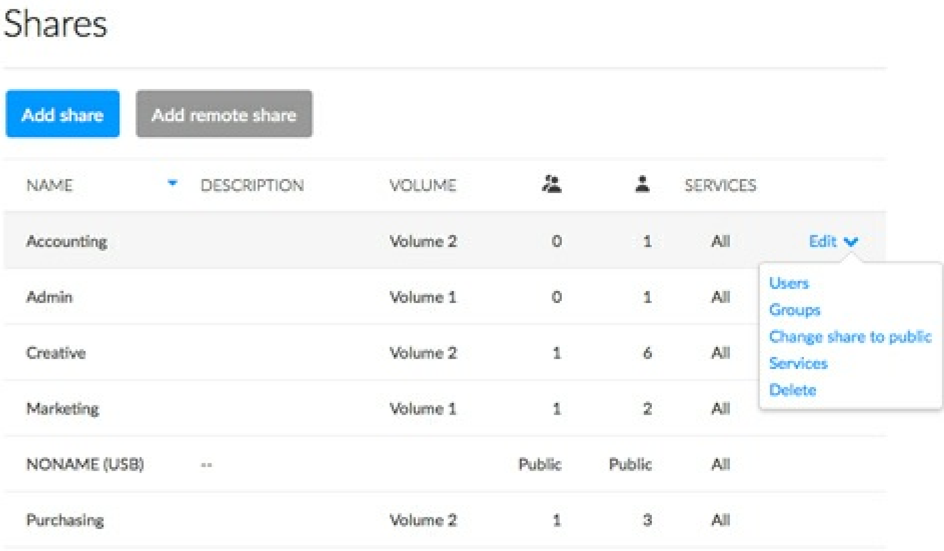
Name: Logan

Password: •••••••••

□ Remember this password in my keychain

4. The remote share/volume is ready to use.

## Revise share settings



Shares

| NAME | DESCRIPTION | VOLUME | 👥 | 👤 | SERVICES |
|---|---|---|---|---|---|
| Accounting | | Volume 2 | 0 | 1 | All |
| Admin | | Volume 1 | 0 | 1 | All |
| Creative | | Volume 2 | 1 | 6 | All |
| Marketing | | Volume 1 | 1 | 2 | All |
| NONAME (USB) | -- | | Public | Public | All |
| Purchasing | | Volume 2 | 1 | 3 | All |

To revise a share's settings, pass the cursor to the far right of its row to make the **Edit** pull-down menu visible. Options on the **Edit** pull-down menu differ for public and private shares:

- **Public**: *Change to private share*, *Services*, and *Delete*
- **Private**: *Users*, *Groups*, *Change share to public*, *Services*, and *Delete*

Since public shares are available to everyone on the network, there is no need to manage user and group access.

> i **Important info regarding remote shares**: Settings for remote shares can be revised on the host NAS/server.

## Users/Groups: change access rights

From the **Edit** pull-down menu, choose **Users** or **Groups**. The pop-up window includes three tabs for *Users*, *Groups*, and *Overview*.

1. Select the tab you wish to manage.
2. The left-hand column lists the users or groups with *No access* to the share. Select the user or group to be granted access and drag it to the *Read access* column or the *Read+write* access column. You can enable read access for everyone on the network by checking the box next to **Enable Read access to guests on the network**.
3. Choose **Close** to confirm the changes.

## Private and public: change the share's network status

Select the applicable setting to:

- Change a public share into a private share
- Change a private share into a public share

## Services: change the services for a specific share

File protocols and service applications can be enabled and disabled on the Services page. A service is available to all shares when it is enabled and not available when it is disabled. However, an administrator may want to enable a service for certain shares but turn it off for others.

**Example 1**: The administrator creates a share called *Time Machine* to use as the backup destination for a Mac on the network. Since the Mac runs Time Machine® for its backups, the share must have Apple File Protocol (AFP) and Time Machine services. Both services can be enabled on the NAS's Services page. However, all other computers on the network are PCs. Therefore, the administrator disables AFP and Time Machine on all other shares.

**Example 2**: A doctor's office wants to use a share called *Entertainment* to store media files. A player in the waiting room that is UPnP/DLNA compatible will access the media files. All other shares store patient information and office files. The administrator knows that enabling UPnP/DLNA on all shares can tax the processor. It will also slow down Re-Indexing the media. Therefore, the administrator disables UPnP/DLNA on all shares except *Entertainment*.

**Enable/Disable a service on a specific share**

1. Pass the cursor to the far right of the share's row to make the **Edit** pull-down menu visible.
2. Choose **Services**.
3. Perform one of the following:
    - Deselect the check box next to the service you want to disable
    - Select the check box next to the service you want to enable

    If you do not see the service you want enable/disable, confirm that it has been enabled on the NAS's Services page.
4. Choose **Save**.

**Important info**: Services must be enabled on the Services page for them to appear on a share.

## Delete

**Deleting a share and data**: Deleting a share also deletes all files on the share and will cause any associated backup jobs to fail.

1. Pass the cursor to the far right of the share's row to make the **Edit** pull-down menu visible.
2. Choose **Delete**.
3. Confirm in the dialogue window.

# Users

Choose the Users page to add and manage user accounts.

# Shares, Users, and Groups

Allotting storage and network permissions for multiple departments and users in a branch office or corporate network can be complicated. It takes forethought and planning to configure which user is part of what group with access to how many shares. For this reason, the settings *Shares*, *Users*, and *Groups* are closely related in NAS OS. The cross-functionality between these three settings allows the administrator to add users to groups in the *Users* or *Groups* settings as well as shares to users and groups in the *Users* and *Groups* settings. The wizard for each setting prompts the administrator to choose shares, users, and groups. Additionally, users and groups can be added to a new share when following the *Add share* wizard.

However, creating a new share, user, or group requires that the administrator use its respective setting. For example, the administrator must choose the *Shares* setting to add a new share and the *Users* setting to add a new user. Though each setting can be revised at any time, it is highly recommended that the administrator plan ahead when first adding shares, users, and groups to NAS OS. With a map of users, groups, and shares, the administrator can simplify access rights. See the example below.

## Sample setup: Shares, Users, and Groups

An administrator has mapped permissions for 40 shares, 20 users, and 10 groups.

To get started, the administrator adds the 20 shares using the *Add share* wizard on the *Shares* page. The administrator ignores the prompts to add users and groups to each share since new users and groups have yet to be created.

Next, the administrator adds the 20 users using the *Add user* wizard on the *Users* page. The administrator ignores the prompts to add users to shares and groups since new groups have yet to be created.

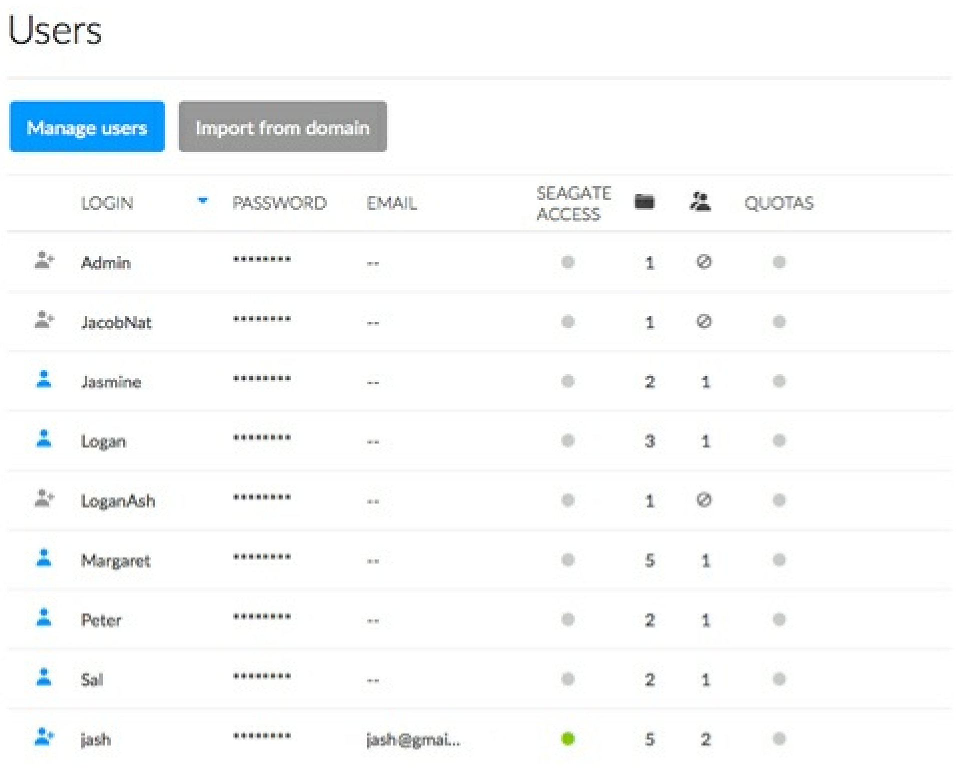
Finally, the administrator adds the 10 groups using the *Add group* wizard on the *Groups* page. In this step, the administrator will assign:

- Each user to a specific group
- Share permissions for each group

The *Groups* setting is the last step since it can cover more users at one time rather than assigning share permissions for each new user.

The generic sample setup may not apply to all environments. However, NAS OS gives the administrator free reign to configure permissions on the Shares, Users, and Groups pages.

# Existing users



| | LOGIN | PASSWORD | EMAIL | SEAGATE ACCESS | 📁 | 👥 | QUOTAS |
|---|---|---|---|---|---|---|---|
| | Admin | ******** | -- | ● | 1 | ⊘ | ● |
| | JacobNat | ******** | -- | ● | 1 | ⊘ | ● |
| | Jasmine | ******** | -- | ● | 2 | 1 | ● |
| | Logan | ******** | -- | ● | 3 | 1 | ● |
| | LoganAsh | ******** | -- | ● | 1 | ⊘ | ● |
| | Margaret | ******** | -- | ● | 5 | 1 | ● |
| | Peter | ******** | -- | ● | 2 | 1 | ● |
| | Sal | ******** | -- | ● | 2 | 1 | ● |
| | jash | ******** | jash@gmai... | ● | 5 | 2 | ● |

User data is organized in a table.

- The icons in the far left column indicate a user's rights:
  - Blue user with plus sign: Administrative privileges.
  - Blue user: Standard user privileges.
  - Grey user: The user was imported from an active directory with no administrative privileges.
- Choose the text in the **Login** column to change the user name.
- Choose the text in the **Password** column to change the user's password. A password is created during the setup for the first administrator and in Manage users for additional users.
  - Passwords can only be changed for users created on the NAS. Contact the administrator for the active directory to change settings for imported users.
  - Passwords that are linked to Seagate Access accounts can be changed for signing into the NAS. However, changes to the password on the NAS are not taken into account by the user's Seagate Access account. Therefore, users must continue to enter the original password that was created for the Seagate Access account. It is highly recommended to keep passwords as consistent as possible.
- The email address can be filled in automatically when associating a user with a Seagate Access account. With or without a Seagate Access account, the administrator can click the text in the **Email** column to change a user's email address. However, if a user is associated with a Seagate Access account, it is highly recommended to keep the email address unchanged.
- The light in the Seagate Access column is green if the user is associated with a Seagate Access account. It is grey if the user does not have a Seagate Access account.
  - Click a green light to log out of the Seagate Access account.
  - Click a grey light to create a Seagate Access account for a user.
- The number in the **Shares** column (folder icon) indicates how many shares the user can access. Choose the number to view the assigned shares.
- The number in the **Groups** column (double silhouette icon) shows to how many groups the user belongs. Choose the number to view the groups.
- To set a storage capacity limit for a user, click on the white circle in the **Quota** column. Once the quota is

set, the white circle will turn green.

# Add a user

Choose **Manage users** and follow the wizard to completion. You can:

- **Invite users**: invite local and remote users to join your NAS and to create a Seagate Access account. Use this option for users who require remote access to the NAS. You must enter an email address for a user to create a Seagate Access account. The user receives the invitation via email with instructions on how to complete the account.
- **See invites**: review pending user invitations.
- **Create user**: create a user for local access to the NAS. You can create a local user and add the Seagate Access account later.

Consider the following when completing the fields in this step:

- A login can have from 1 to 20 characters using letters, numbers, hyphens, and underscores. Do not begin or end with a hyphen or an underscore.
- A password can have from 4 to 20 characters and is case-sensitive.
- An email address is optional when creating a local user. It can be helpful for quota notifications and password recovery.
- To give the user administration privileges to the NAS, check the box next to **Administrator**.
- *Set group permissions:* To add a user to a group, drag the group name from the No access column to the Access column. To add the user to multiple groups, make all your selections before dragging them to the Access column. The administrator can skip the group membership step if membership will be assigned in the Groups settings.
- *Set share permissions*: To give the user access to a share, drag the share to the Read access column or the *Read+write* access column. To give access to multiple shares, make all your selections before dragging them to one of the columns. If a share is mistakenly dragged to the *Read access* column or *Read+write* access column, you can drag it back to the *No access* column. The administrator can skip this step if access will be assigned in the Shares or Groups settings.

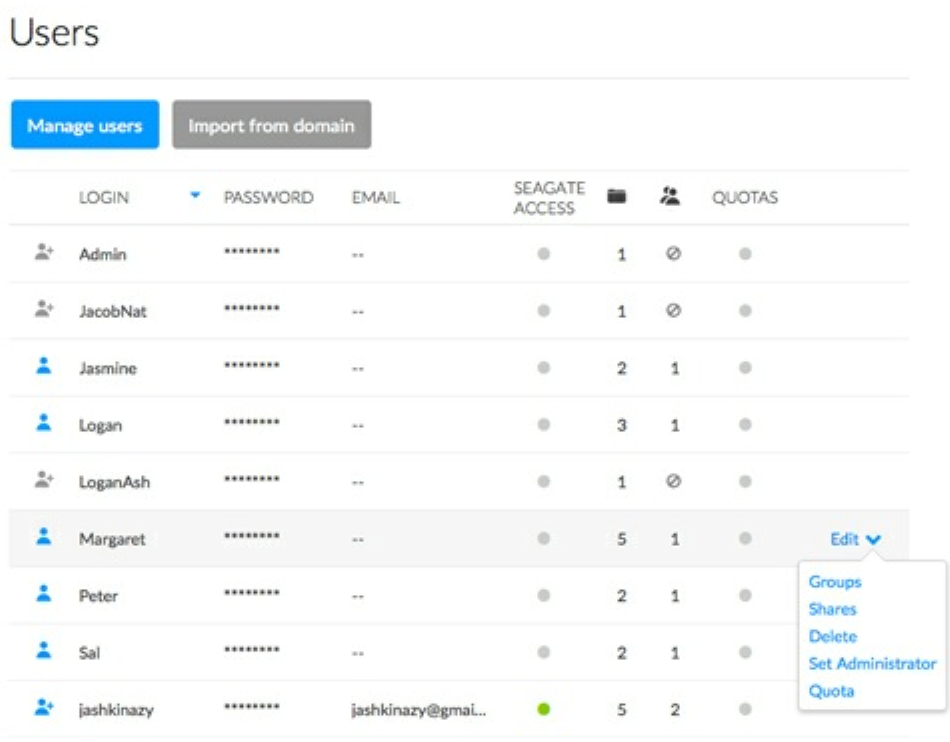
# User: access to shares and rights

A user can access NAS shares that have been assigned to him by the administrator (see Shares ). When accessing the shares for the first time, the user is prompted for the password created by the administrator on the Users page (see Shares: Access and Transfer Files). In addition, a user can log on to NAS OS using his login and password, which is very helpful with Seagate MyNAS remote access. However, NAS OS management rights are limited for standard users.

Access the Filebrowser app to upload, download, and share files via the Internet (see Filebrowser).

An administrator has access to all NAS OS management features, including the ability to revise a password that has been changed by a user.

# Revise user settings



| LOGIN | PASSWORD | EMAIL | SEAGATE ACCESS | 📁 | 👥 | QUOTAS | |
|---|---|---|---|---|---|---|---|
| Admin | ******** | -- | ● | 1 | ⊘ | ● | |
| JacobNat | ******** | -- | ● | 1 | ⊘ | ● | |
| Jasmine | ******** | -- | ● | 2 | 1 | ● | |
| Logan | ******** | -- | ● | 3 | 1 | ● | |
| LoganAsh | ******** | -- | ● | 1 | ⊘ | ● | |
| Margaret | ******** | -- | ● | 5 | 1 | ● | Edit |
| Peter | ******** | -- | ● | 2 | 1 | ● | |
| Sal | ******** | -- | ● | 2 | 1 | ● | |
| jashkinazy | ******** | jashkinazy@gmai... | ● | 5 | 2 | ● | |

To revise a user's settings, pass the cursor to the far right of its row to make the **Edit** pull-down menu visible. Options on the **Edit** pull-down menu differ for users and administrators:

- **Users**: *Groups*, *Shares*, *Delete*, *Set Administrator*, *and Quota*
- **Administrator**: *Groups*, *Shares*, *and Quota*

## Groups/Shares: change groups and access rights

From the **Edit** pull-down menu, choose **Groups** or **Shares**. The pop-up window includes three tabs for *Shares*, *Groups*, and *Overview*.

### Edit access rights to shares

1. Select the *Shares* tab.
2. The column *No access* lists the shares that the user cannot open.
   - **Add access to shares**: Select the applicable shares in the *No access* column and drag them to the *Read access* column or the *Read+write* access column.
   - **Remove access to shares**: Select the applicable shares in the *Read access* column or the *Read+write* access column and drag them to the *No access* column.
3. Choose **Close** to confirm the changes.

### Edit group membership

1. Select the **Groups** tab.

2. The column *No access* lists the groups that the user has not joined.
    - **Add a user to groups**: Select the applicable groups in the *No access* column and drag them to the *Access* column.
    - **Remove a user from groups**: Select the applicable groups in the *Access* column and drag them to the *No Access* column.
3. Choose **Close** to confirm the changes.

## Delete a user

1. Pass the cursor to the far right of the user's row to make the **Edit** pull-down menu visible.
2. Choose **Delete**.
3. Confirm in the dialogue window.

## Change NAS OS management rights: administrator and user

An administrator can be changed to a standard user and a standard user can be elevated to an administrator.

1. Pass the cursor to the far right of the user's row to make the **Edit** pull-down menu visible.
2. Select the applicable setting to:
    - **Set Administrator**
    - **Set local user**

> **i** **Important info on the first administrator**: The original administrator who configured the NAS OS device remains an administrator. It is not possible to delete or change the original administrator.

## Set storage quotas

Limit the user’s storage capacity by following the steps below:

1. Pass the cursor to the far right of the user's row to make the **Edit** pull-down menu visible.
2. Choose **Quota**.
3. Click on the text in the *Quota* column.
4. Choose the radio button next to **Set limit** and enter the quota in gigabytes (GB).
5. Choose **Save**.

# Importing users from an active directory

If you have successfully connected to an active directory domain, you will see a button on the Users page labeled **Import from domain**. Go to Settings for instructions on how to join your NAS OS device to an active directory.

To add users from the active directory:

1. Choose **Import from domain**.

1. Choose **Import from domain**.
2. At the prompt, type a few characters in the text field to find the users you want to import.
3. Hold down the control key (Windows users) or command key (Mac users) to select multiple users.
4. Choose **Import**.
5. The imported users will appear in the table. You can identify users imported from the domain by their grey icons.

## Managing users imported from an active directory

The administrator of the original domain manages users imported from an active directory. For example, passwords, email accounts, and groups are all determined within the original domain. See Settings for instructions on synchronizing changes from an active directory to NAS OS.

The administrator of the NAS OS device can adjust the following settings for imported users:

- Access rights to shares on the NAS OS device
- Delete an imported user from the NAS OS device
- Set quotas for storage capacity on NAS OS volumes

# Groups

Administrators can use *Groups* to set access rights for many users at once rather than individually.

# Shares, Users, and Groups

Allotting storage and network permissions for multiple departments and users in a branch office or corporate network can be complicated. It takes forethought and planning to configure which user is part of what group with access to how many shares. For this reason, the settings *Shares*, *Users*, and *Groups* are closely related in NAS OS. The cross-functionality between these three settings allows the administrator to add users to groups in the *Users* or *Groups* settings as well as shares to users and groups in the *Users* and *Groups* settings. The wizard for each setting prompts the administrator to choose shares, users, and groups. Additionally, users and groups can be added to a new share when following the *Add share* wizard.

However, creating a new share, user, or group requires that the administrator use its respective setting. For example, the administrator must choose the *Shares* setting to add a new share and the *Users* setting to add a new user. Though each setting can be revised at any time, it is highly recommended that the administrator plan ahead when first adding shares, users, and groups to NAS OS. With a map of users, groups, and shares, the administrator can simplify access rights. See the example below.

## Sample setup: Shares, Users, and Groups

An administrator has mapped permissions for 40 shares, 20 users, and 10 groups.

To get started, the administrator adds the 20 shares using the *Add share* wizard on the *Shares* page. The administrator ignores the prompts to add users and groups to each share since new users and groups have yet to be created.

Next, the administrator adds the 20 users using the *Add user* wizard on the *Users* page. The administrator ignores the prompts to add users to shares and groups since new groups have yet to be created.

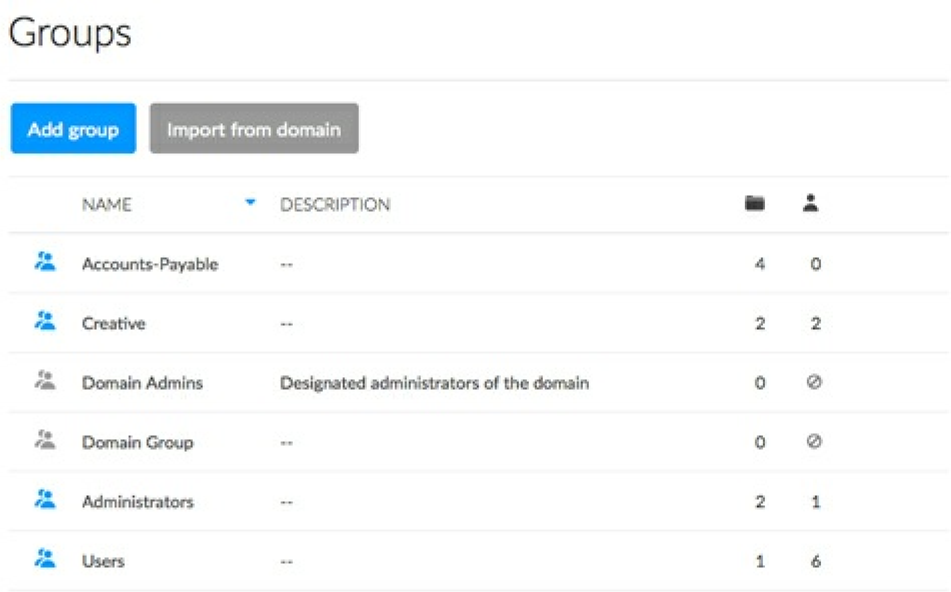
Finally, the administrator adds the 10 groups using the *Add group* wizard on the *Groups* page. In this step, the administrator will assign:

- Each user to a specific group
- Share permissions for each group

The *Groups* setting is the last step since it can cover more users at one time rather than assigning share permissions for each new user.

The generic sample setup may not apply to all environments. However, NAS OS gives the administrator free reign to configure permissions on the Shares, Users, and Groups pages.

# Existing groups



Groups

| NAME | DESCRIPTION | 📁 | 👤 |
|---|---|---|---|
| Accounts-Payable | -- | 4 | 0 |
| Creative | -- | 2 | 2 |
| Domain Admins | Designated administrators of the domain | 0 | ⊘ |
| Domain Group | -- | 0 | ⊘ |
| Administrators | -- | 2 | 1 |
| Users | -- | 1 | 6 |

Group data is organized in a table.

- A blue icon on the far left indicates that the group has been created in NAS OS.
- A grey icon on the far left indicates that the group has been imported from a domain.
- Choose the text in the **Name** column to change the group name. The name of a group from a domain cannot be changed in NAS OS.
- Choose the empty space or text in the **Description** column to add or revise details for the group (optional).
- The number in the **Shares** column (folder icon) shows how many shares the group has access to. Choose

the number to view the shares.
- The number in the **Users** column (user icon) shows how many users belong to the group. Choose the number to view the users.
- To review settings for the group, pass the cursor to the right of the group's row to make the **Edit** pull-down menu visible.

# Add a group

NAS OS provides two default groups, *Administrators* and *Users*.

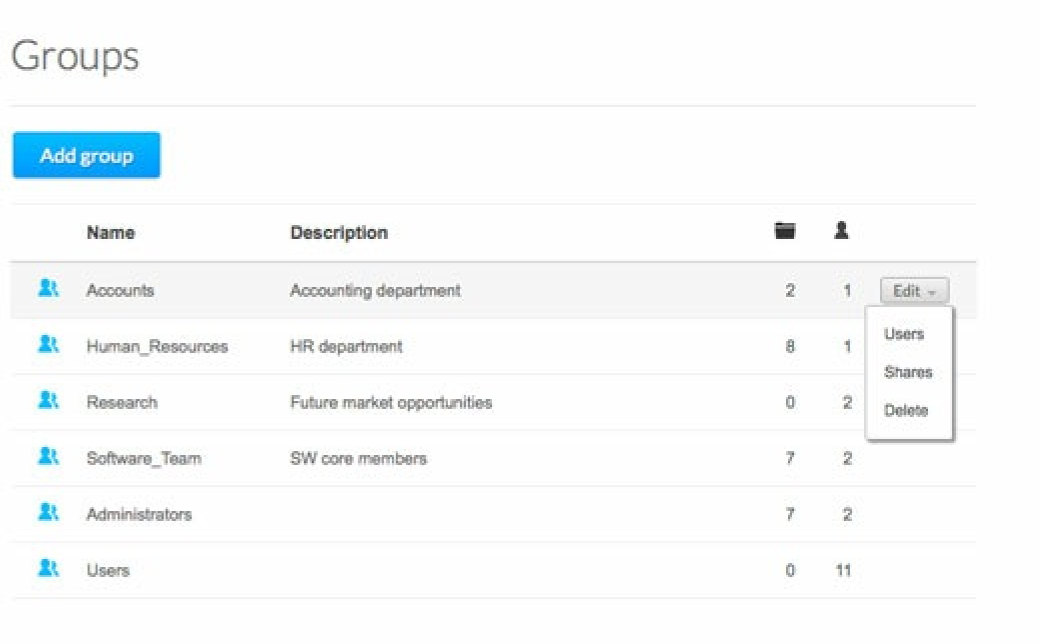
- All Administrators are automatically added to the Administrators group.
- All users are automatically added to the Users group.

> **i** **Default groups:** The default shares Administrators and User cannot be deleted.

To create a new group, choose **Add group** and follow the wizard to completion. Consider the following when creating a user:

- The **Add group** wizard features the following steps: *name the group*, *set share permissions*, *set user membership to the group*, *set app permissions and Summary*.
- *Name the group*: A group name can have from 1 to 20 characters using letters, numbers, hyphens, and underscores. Do not begin or end with a hyphen or an underscore.
- *Set share permissions:* The administrator can skip this step if access will be assigned in the Shares or Users settings. To skip the step, choose **Next**.
- *Set share permissions*: To give the group access to a share, drag the share to the *Read access* column or the *Read+write access* column. To give access to multiple shares, make all your selections before dragging them to the one of the columns.
- *Set share permissions*: If a share is mistakenly dragged to the *Read access* column or *Read+write access* column, you can drag it back to the *No access* column. The administrator can skip this step if membership will be assigned in the Users settings. To skip the step, choose **Next**.
- *Set user membership to the group:* To add a user to the group, drag the user’s name from the *No access* column to the *Access* column. To add multiple users to the groups, make all your selections before dragging them to the *Access* column.
- *Set app permissions:* Drag the apps that the group can access.

# Revise group settings



| Name | Description | 📁 | 👤 |
|---|---|---|---|
| Accounts | Accounting department | 2 | 1 |
| Human_Resources | HR department | 8 | 1 |
| Research | Future market opportunities | 0 | 2 |
| Software_Team | SW core members | 7 | 2 |
| Administrators | | 7 | 2 |
| Users | | 0 | 11 |

To revise a group's settings, pass the cursor to the far right of its row to make the **Edit** pull-down menu visible. Options on the **Edit** pull-down menu include:

- *Users*
- *Shares*
- *Delete*

## Users/Shares: change user membership to the group and access rights to shares

From the **Edit** pull-down menu, choose **Users** or **Shares**. The pop-up window includes two tabs for *Shares* and Users.

### Edit user membership to the group

1. Select the **Users** tab.
2. The column *No access* lists the users that are not members of the group.
   - **Add a user to groups**: Select the users in the *No access* column and drag them to the *Access* column.
   - **Remove a user from the group**: Select users in the *Access* column and drag them to the *No Access* column.
3. Choose **Close** to confirm the changes.

### Edit access rights to shares

1. Select the **Shares** tab.
2. The column *No access* lists the shares that the group cannot open.
   - **Add access to shares**: Select the applicable shares in the *No access* column and drag them to the *Read access* column or the *Read+write access* column.
   - **Remove access to shares**: Select the applicable shares in the *Read access* column or the *Read+write*

*access* column and drag them to the *No access* column.
3. Choose **Close** to confirm the changes.

## Delete a user

1. Pass the cursor to the far right of the user's row to make the **Edit** pull-down menu visible.
2. Choose **Delete**.
3. Confirm in the dialogue window.

# Importing groups from an active directory

If you have successfully connected to an active directory domain, you will see a button on the Groups page labeled **Import from domain**. (Go to Settings for instructions on how to join your NAS OS device to an active directory.)

To add users from the active directory:

1. Choose **Import from domain**.
2. At the prompt, type a few characters in the text field to find the users you want to import.
3. Hold down the control key (Windows users) or command key (Mac users) to select multiple users.
4. Choose **Import**.
5. The imported users will appear in the table. You can identify users imported from the domain by their grey icons.

## Managing groups imported from an active directory

The administrator of the original domain manages groups imported from an active directory. For example, passwords, email accounts, and users are all determined within the original domain. See Settings for instructions on synchronizing changes from an active directory to NAS OS.

The administrator of the NAS OS device can adjust the following settings for imported users:

- Access rights to shares on the NAS OS device.
- Delete an imported group from the NAS OS device.

# Settings

Configure your NAS's basic settings on the Settings page.

# General

- **Device name**: The device name identifies the Seagate NAS OS device on your network. You can change it from the default by passing the cursor to the right of the name. Choose the pencil icon when it appears and enter a new name.

The device name is limited to 15 characters and is case-sensitive. Use alphanumeric characters without spaces or hyphens. Do not begin or end the name with a hyphen.

If a NAS OS device is connected to the network with a name that already exists, an alternate name is automatically created to avoid conflicts. For example, a second Seagate 8-bay Rackmount NAS on your network will automatically be called *Seagate-R8-1* if *Seagate-R8* is present.

- **Language**: Pass the cursor to the right and choose the pencil icon to change the NAS OS language.
- **Temperature unit**: To change the unit, pass the cursor to the right and choose the pencil icon.

# Time

You can set the time manually or, synchronize with a local or network time server.

- **Synchronization**: Use the slider to turn time synchronization on or off. It also enables a pop-up window to choose a time server or enter your own.
  - ***On***: If synchronization is on or off and you want to change the time server, click on the slider. The *Synchronization* pop-up window includes a pull-down menu in *Registered* and a field for *Custom*. Use the *Registered* pull-down menu to select a popular time server. For a local time server or a network time server that is not on the *Registered* pull-down menu, enter the URL in the *Custom* field. Choose **Save** to update the time server.
  - ***Off***: Click on the slider and choose **Cancel** in the *Synchronization* pop-up window.
- **Date/Time**: The date and time are set automatically if you assign a time server in synchronization. If a time server is not selected, you can change the date and time by passing the cursor to the right and choosing the pencil icon.
- **Zone**: Pass the cursor to the right and select the pencil icon. You can choose your time zone from the drop-down window.

# Workgroup/Domain

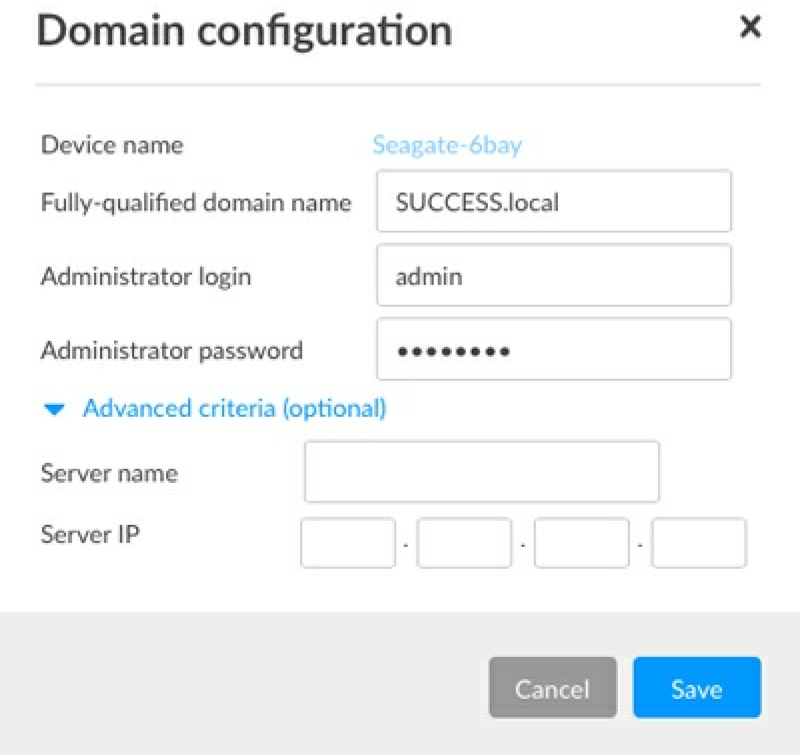
Your NAS can join a Windows Workgroup or a Windows Active Directory:

- **Workgroup**: Select the radio button for **Workgroup** and choose the pencil icon to type its name (use from 1 to 15 alphanumeric characters).
- **Domain**: Select the radio button for **Domain** to join a Windows Active Directory on your network (see the next paragraph for instructions on entering your Active Directory credentials). Joining an Active Directory allows the administrator to import existing users and groups, foregoing the need to re-enter credentials.

**Active Domain Troubleshooting:** The information below provides general information on joining and leaving a domain. For additional information, see Getting Help.

## Connect to an Active Directory

1. Select the **Domain** radio button.
2. At the prompt, fill in the **Fully-qualified domain name, Administrator login**, and **Administrator password**. For more complex network configurations, choose the **Advanced Criteria** arrow and fill in the **Server name** and **Server IP** fields.



Domain configuration

Device name: Seagate-6bay
Fully-qualified domain name: SUCCESS.local
Administrator login: admin
Administrator password: ••••••••
Advanced criteria (optional)
Server name:
Server IP: . . .

3. Once connected, you can import users and groups from the domain. See Users and Groups for details.

## Synchronize Users/Groups

Except for access rights to shares on the NAS OS device, the domain’s administrator manages all users and groups imported from the domain. If a user's/group's account has been changed by the domain administrator within the Windows Active Directory server (e.g. password revision, deleted from the domain, etc.), you can update the account in NAS OS by choosing the button **Synchronize imported users/groups**. The button only appears once you have joined a domain.

## Leave the domain

To remove the NAS's connection to a domain:

1. Choose the **Leave** button.
2. Authenticate by entering the domain administrator's username and password.
3. Users and groups that were imported may still be listed on the Users and Groups pages. To remove all

imported users and groups from the NAS, choose the button **Remove the imported users/groups** (this button replaces **Synchronize imported users/groups** once you leave a domain).

# NAS OS

This section of the Settings page provides basic hardware and software information. NAS OS automatically checks for updates to the software. You can change the frequency by passing the cursor to the right and choosing the pencil icon. To manually check for an update to NAS OS, choose **Check now**.

# Services

The Services page provides a list of file protocols and application services available to the NAS OS device. Based upon the needs of computers on the network, the administrator can choose to maintain certain services while leaving others turned off.

Examples:

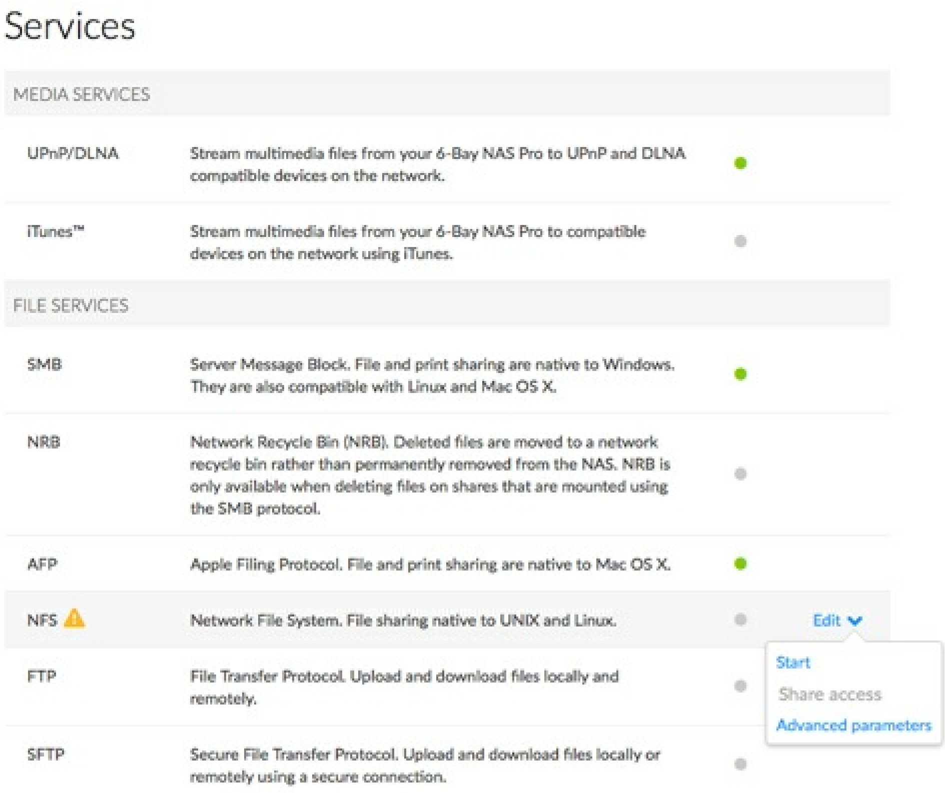
- The administrator may wish to turn AFP (Apple Filing Protocol) off if there are no Apple computers on the network.
- The administrator can enable the FTP service in order to provide access to the NAS via a third-party FTP application. See FTP for details.

# Status colors

The Status column provides details on the state of the service.

| Color | State |
|---|---|
| Green | Started |
| White | Stopped |
| Orange | Ready for use |

# Service options: start/stop, share access, advanced parameters



Services

| MEDIA SERVICES | | |
|---|---|---|
| UPnP/DLNA | Stream multimedia files from your 6-Bay NAS Pro to UPnP and DLNA compatible devices on the network. | ● |
| iTunes™ | Stream multimedia files from your 6-Bay NAS Pro to compatible devices on the network using iTunes. | ○ |
| **FILE SERVICES** | | |
| SMB | Server Message Block. File and print sharing are native to Windows. They are also compatible with Linux and Mac OS X. | ● |
| NRB | Network Recycle Bin (NRB). Deleted files are moved to a network recycle bin rather than permanently removed from the NAS. NRB is only available when deleting files on shares that are mounted using the SMB protocol. | ○ |
| AFP | Apple Filing Protocol. File and print sharing are native to Mac OS X. | ● |
| NFS ⚠ | Network File System. File sharing native to UNIX and Linux. | ○ |
| FTP | File Transfer Protocol. Upload and download files locally and remotely. | ○ |
| SFTP | Secure File Transfer Protocol. Upload and download files locally or remotely using a secure connection. | ○ |

Options for a service are available in the Edit pull-down menu. Service options can include: *Start/Stop*, *Share access*, and *Advanced parameters*. Some services have options specific to its features. For example, the iTunes and UPnP services include *Re-Index* to take inventory of media files.

To enable the Edit pull-down menu, pass the cursor to the far right of a service.

## Start/Stop a service

1. Pass the cursor to the far right of its row to make the Edit pull-down menu visible.
2. Choose **Start** or **Stop**.

## Share access: services for a specific share

A service is available to all shares when Start is selected and not available when Stop is selected. However, an administrator may want to enable a service for certain shares but turn it off for others.

**Example 1:** The administrator creates a share called *Time Machine* to use as the backup destination for a Mac on the network. Since the Mac runs Time Machine® for its backups, the share must use the Apple File Protocol (AFP) and Time Machine services. Both services can be enabled on the Services page. However, all other computers on the network are PCs. Therefore, the administrator disables AFP and Time Machine on all other shares.

**Example 2:** A doctor's office wants to use a share called *Entertainment* to store media files. A player in the waiting room that is UPnP/DLNA compatible will access the media files. All other shares store patient information and office files. The administrator knows that enabling UPnP/DLNA on all shares can tax the processor and slow down Re-Indexing the media. Therefore, the administrator disables UPnP/DLNA on all shares except *Entertainment*.

The administrator can enable or disable services on specific shares on the Services page or the Shares page. For details on managing services on the Shares page, see Shares .

Follow the directions below to enable/disable an active service on specific shares:

1. Pass the cursor to the far right of the share's row to make the Edit pull-down menu visible.
2. Choose **Share access**.
3. Select an option below:
    - **Enabled on all shares**: Click on the radio button next to **Enabled on shares by default** and choose **Save**.
    - **Enabled on specific shares**: Click on the radio button next to **Specific shares**. In the window, click on the check boxes next to the shares that will use the service. Choose **Save** once you have selected the shares.

## Services summary

Review the types of services below.

## File services

- *SMB*: SMB (server message block) is enabled by default since it is native to Windows and supported on Mac OS.
- *NRB*: Deleting data on a share permanently removes all associated files. By enabling the NRB (network recycle bin) service, deleted files will be moved to the share's recycle bin. This can be very helpful if a user accidentally removes data that a co-worker is using on a project. The data is easily recovered from the recycle bin rather than desperately searching through the last NAS backup. NRB is only compatible with shares that use SMB and it appears as a folder on the share.
- *AFP*: AFP can be started manually for computers running Mac OS. AFP must be started if the Time Machine service will be enabled.
- *NFS*: See NFS.
- *FTP/SFTP*: See FTP.
- *WebDAV*: WebDAV (Web-based distributed authoring and versioning) is a standard format for collaborative workflows and data sharing. You can give local and remote servers access to shares by enabling the WebDAV service on your NAS OS device.

## Application services

- *Seagate Access*: See Remote Access
- *Time Machine*: See Backup: Seagate NAS and PC/Mac
- *UPnP/DLNA*: See Media Server
- *iTunes*: See Media Server

- *Network Backup*: See Backup Manager. Note: Activating Network Backup server will disable SFTP.
- *Download machine*: See Download Manager

## SSH Access

Administrators with advanced networking skills can log in to NAS OS using secure shell (SSH), an encrypted protocol used for communication between devices. Using a command-line interface, the administrator can automate data management and backups as well as review the NAS's settings. The administrator also has the right to access data stored on the NAS via SSH.

## Printer server

Printer server is enabled by default. An orange light means that NAS OS does not detect a printer connected to one of the NAS's USB ports. The light will turn green once a compatible printer is found. Follow the directions below to share a printer on the network via the NAS OS device:

1. Connect your printer to a USB port on your NAS.
2. Pass the cursor to the far right of the printer row to make the Edit pull-down menu visible and choose **Start**.
3. Check the status of the **Printer server**.

Computers on your network may require specific drivers to use the printer. See your printer's user manual for details.

> i **Important info**: For multi-function printers, only the print feature is supported. If your printer has a scan feature, it will not work when connected to the NAS. In addition, only PostScript printers are supported. If your printer does not appear in the printer service, it is likely that it does not support PostScript printing. This is frequently the case with multi-function and photo printers. Seagate cannot guarantee that your printer supports the proper protocols to make it a networked printer.

# Network

The Network page features four tabs to manage the NAS's network settings.

- Connections: Review or change settings for the LAN ports; link aggregation; and IPv4 or IPv6 addresses.
- Proxy: Assign a proxy server for Internet access.
- Remote access: Configure remote access using Seagate MyNAS or DynDNS. Details on Seagate's remote access solutions are available at Remote access.
- Port forwarding: Review and adjust the router's port numbers for select services.

# Connections tab

# IPv6 mode

You can turn on IPv6 addressing by clicking on the IPv6 mode slider.

# Connections table

The Connections table lists the general network settings for the LAN ports. The number of LAN ports depends upon your NAS model.

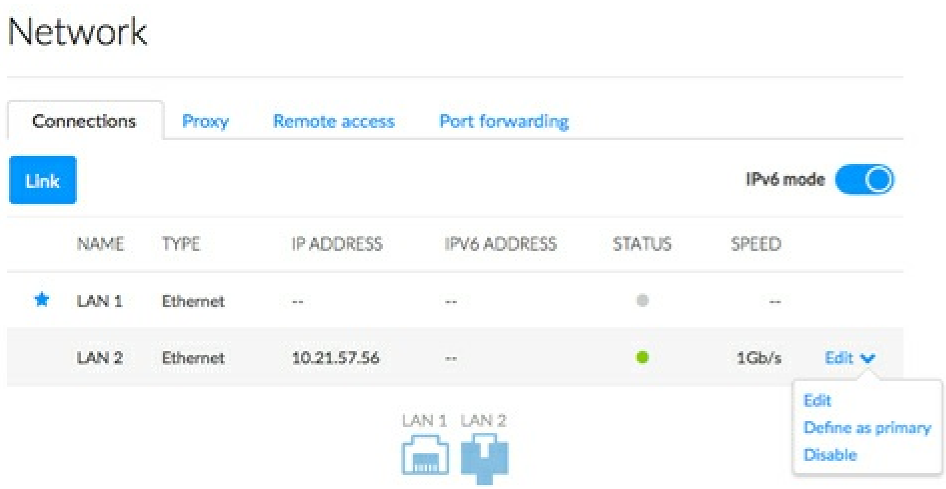
- **Star icon**: The star appears on the primary LAN. See the note below regarding the primary LAN.
- **Name**: The default names for the LAN ports are LAN 1, LAN 2, etc. Click on the name to enter a new name for the LAN port.
- **Type**: The type of cable attached to the LAN port.
- **IP address**: This column shows the NAS's IPv4 addresses. If your network is DHCP-enabled for IPv4, the LAN ports are automatically assigned IPv4 addresses.
- **IPv6 address**: This column shows the NAS's IPv6 addresses. If IPv6 is turned on and your network is DHCP-enabled, the LAN ports are automatically assigned IPv6 addresses.
- **Status**: A green circle means that the LAN port is connected to an active network. A white circle shows there is no connection to a network.
- **Speed**: The speed of the network.

Icons representing the LAN ports sit below the Connections table. An icon will become highlighted when the cursor is passed over the port's row. The icons also indicate the following:

- *Connected Ethernet end*: The port is connected to a network.
- *Disconnected Ethernet end*: The port is not connected to a network.

# LAN Edit menu

To review or modify settings for a LAN port, pass the cursor to the far right of its row to make the **Edit** pull-down menu visible. Available settings in the pull-down menu differ based upon the NAS's LAN connections. Specifically, Define as primary will only appear if the NAS has more than one LAN connection



| | NAME | TYPE | IP ADDRESS | IPV6 ADDRESS | STATUS | SPEED | |
|---|---|---|---|---|---|---|---|
| ★ | LAN 1 | Ethernet | -- | -- | ● | -- | |
| | LAN 2 | Ethernet | 10.21.57.56 | -- | ● | 1Gb/s | Edit |

# LAN Edit menu: Edit

Choose **Edit** to review and update important settings on the LAN port.

- **Name**: Type a new name in the LAN port's **Name** field.
- **IPv4 tab**: The default *IP configuration* setting for the LAN port is Automatic (DHCP). To use a static IP, click on the pull-down menu and choose **Manual**. For the static IP address to take effect, all fields (including *Default gateway* and *DNS server*) must be completed before choosing **Save**. Check the box next to **Default gateway** to enter or revise the gateway address. The LAN port will revert to automatic if a field is left blank.
- **IPv6 tab**: This tab is available when the IPv6 slider is turned on. The default *IP configuration* setting for the LAN port is Automatic (DHCP). To change the LAN port's address, click on the pull-down menu and choose **Manual**. For the new address to take effect, complete the **Global IPv6 address** and **IPv6 default gateway** fields before choosing **Save**.
- **Advanced tab**: Click on the pull-down menu to adjust the frame size for your NAS. **Note**: Changing the size of the frames can affect the NAS's performance. It is highly recommended that administrators confirm that the router and other network devices support jumbo frames before choosing a higher frame size on the NAS.

> **Important info on static IP addresses**: Changes to the IP address must be consistent with the values of the router and network. You can lose contact with your NAS by typing addresses that are not available on your network.

# LAN Edit menu: Define as primary

- A star next to the LAN's name marks it as the primary Ethernet port. The primary Ethernet port:
  - Carries the data when the NAS is configured for fault tolerance.
  - Acts as the gateway to the Internet when the NAS is bridged across two separate networks.
- You can reassign the role of primary port.
  1. Pass the cursor to the far right of the secondary LAN port (no star) to make the **Edit** pull-down menu visible.
  2. Choose **Define as primary**.
  3. The star icon will move to the port to reflect the change.

> **The primary LAN and Seagate Network Assistant**: If you experience problems with Seagate Network Assistant, confirm that LAN 1 is connected to the network and that it is the primary LAN.

# LAN Edit menu: Disable/Enable

- Turn the LAN port off/on.

# Port aggregation and linking LAN ports

Seagate NAS OS supports port aggregation for NAS devices equipped with two or more LAN ports. Review the instructions below to learn how to configure your NAS for port aggregation.

> **Important info on connecting multiple LAN ports**: When connecting both LAN ports to one or more routers, make certain to configure your NAS OS device for multiple networks, load balancing, or fault tolerance. Leaving all ports active without creating a bridge or bond can create problems with the NAS OS device's network identification, potentially losing its IP address.

## Port aggregation: Bridge the data on your NAS OS device between two networks

Two separate networks can share the NAS. Connect LAN 1 to the router on the first network and LAN 2 to the router on the second network.

Both LANs should have green circles in the Status column. If one of the LAN ports is not active, try to enable it in the Edit menu.

With a bridged connection, each LAN port should have its own unique IP address to reflect separate networks. You can confirm the bridge by checking the subnets of the IP addresses. The subnet is the third segment of numbers in an IP address. For example, the subnet of the address 192.168.3.20 is 3.

## Port aggregation: Enhance your NAS's performance with load balance

Configure both Ethernet ports to act together for speeds up to 1.5 times faster than a single LAN connection. You also get added security should one of the Ethernet cables or ports fail.

Before following the directions below, make certain that your switch or router supports link aggregation.

1. Connect LAN 1 and LAN 2 to the same switch or router.
2. If one LAN is listed as inactive:
   - Confirm that it is securely connected to the device and to your router.
   - Pass the cursor to the far right of the LAN port to make the **Edit** pull-down menu visible. If the option is available, choose **Enable**.
3. With both LANs enabled, choose **Link**.
4. Select **Load balancing** and choose **Next**.
5. Check the boxes next to each LAN port and choose **Next**.
6. You can give a unique name to the load balance bond in the **Name** field. This type of Ethernet bonding will create a unified IP address (DHCP or static). To use a static address, choose **Manual** in the IPv4 or IPv6 pull-down menus and complete all the fields. The manual IP address must be consistent with the values of your network.

7. Choose **Finish**.

The two LAN ports are listed as one on the Connections tab. Note that the number in the Speed column has also changed.

**Break the load balance bond:**

1. Pass the cursor to the far right of the LAN's row to make the **Edit** pull-down menu visible.
2. Choose **Remove link** and **Continue** at the prompt.
3. Removing the link can disable the secondary LAN interface. Pass the cursor to the far right of the disabled LAN port to make the **Edit** pull-down menu visible and choose **Enable**.

## Port aggregation: Failover protection using fault tolerance

Configure fault tolerance to keep your NAS connected to the network even if one Ethernet port or cable fails. Before following the directions below, make certain that your network switch or router supports link aggregation.

1. Connect LAN 1 and LAN 2 to the same switch or router.
2. If one LAN is listed as inactive:
   - Confirm that it is securely connected to the device and to your router.
   - Pass the cursor to the far right of the LAN port to make the **Edit** pull-down menu visible. If the option is available, choose **Enable**.
3. With both LANs enabled, choose **Link**.
4. Select **Fault tolerance** and choose **Next**.
5. Check the boxes next to each LAN port and choose **Next**.
6. Fault tolerance automatically switches to the secondary LAN if it cannot detect the primary LAN. In this step, click on the pull-down menu and choose the type of fault detection for the bond: **Physical** (e.g. a bad Ethernet cable or Ethernet port) or **Logical** (e.g. contact with another IP address). For logical fault tolerance, enter the IP address that the NAS OS device will ping to confirm the stability of the primary LAN, as well as the frequency of the ping. The IP address should target a separate server, a computer on the network, or another device that can manage the task.
7. Choose **Next**.
8. You can give a unique name to the fault tolerance bond in the **Name** field. This type of Ethernet bonding will create a unified IP address (DHCP or static). To use a static address, choose **Manual** in the IPv4 or IPv6 pull-down menus and complete all the fields. The IP address must be consistent with the values of your network.
9. Choose **Finish**.

The two LAN ports are listed as one on the Connections tab.

**Break the fault tolerance bond:**

1. Pass the cursor to the far right of the LAN's row to make the **Edit** pull-down menu visible.
2. Choose **Remove link** and **Continue** at the prompt.
3. Removing the link can disable the secondary LAN interface. Pass the cursor to the far right of the

disabled LAN port to make the **Edit** pull-down menu visible and choose **Enable**.

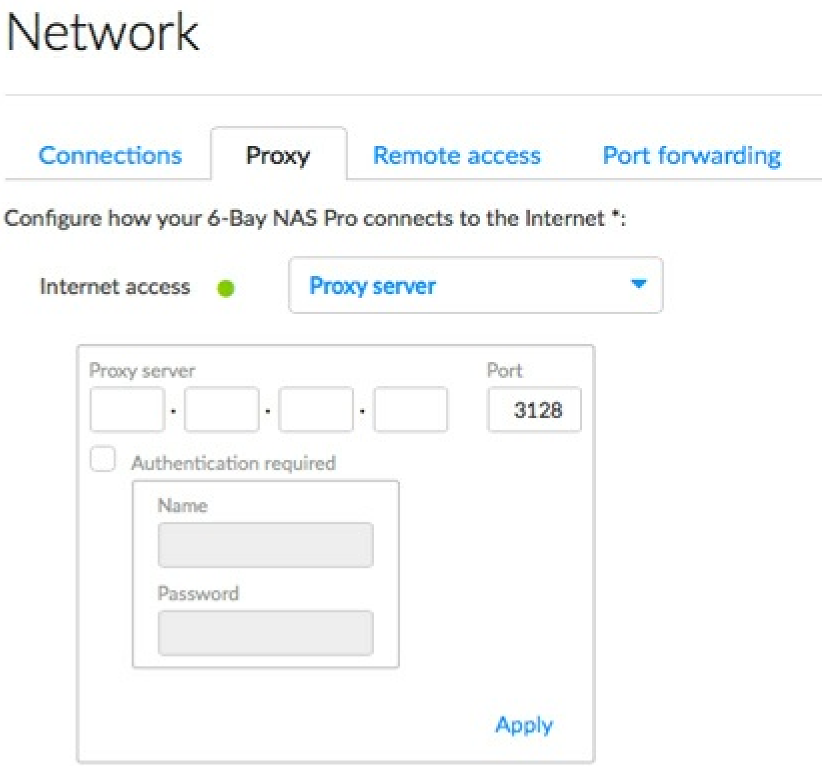
## Port aggregation: LAN failover for load balancing versus fault tolerance

Both bonding and fault tolerance can save you from losing productivity should a single LAN fail (e.g. NAS port, router port, or cable). In the event of LAN failure in a load balance bond, it can take a few minutes for the NAS to switch to single LAN mode. Fault tolerance will make the switch instantly, allowing for uninterrupted communication with the NAS.

# Proxy tab

A proxy server is used to connect network devices to the Internet. If necessary, your NAS can be configured to use a proxy server.

1. Click on the **Internet access** pull-down menu and choose **Proxy server**.
2. Complete the fields for the proxy server's IP address, port, and optional authentication information.



Network

Configure how your 6-Bay NAS Pro connects to the Internet *:

Internet access ● Proxy server

Proxy server . . .

Port 3128

□ Authentication required

3. Choose **Apply**.

# Remote access tab

See Remote Access.

# Port forwarding tab

Use this tab to manage the port forwarding rules for your NAS.

Port numbers on the NAS and the network router are used to direct traffic for diverse features such as Internet access, file services (e.g. SMB, AFP, NFS), and application services (e.g. remote access, Download Manager, etc.). Automatic port forwarding is turned on by default and the port numbers are the same for both the NAS port and Router port columns.

In most instances, automatic port forwarding should help you access services on the NAS. However, enterprise-level network security or port availability on a router can prevent access to ports. Therefore, it may be necessary to change the router port numbers manually for one or more services. Before adjusting numbers in the port forwarding table, confirm that the ports are available on your router. For example, if you intend to change download machine to router port number 8800, you must make certain that port 8800 is available on your router and assigned to your NAS. Additionally, your router must be compatible with UPnP-IGD/NAT-PMP protocols. See your router's user manual for details.

To change the router port for a service on the NAS, choose its value in the **Router port** column.

To disable port forwarding for a service, pass the cursor to the far right of its column to make the **Edit** pull-down menu visible and choose **Disable**.

# Power

Use the Power page to review and change settings for:

- NAS power management
- UPS management

# NAS power management

The NAS OS Power page provides two levels of energy economy:

- Power conservation
- Power saving mode

## Power conservation

During periods of inactivity, NAS OS spins down the hard drives. In addition to conserving energy, spinning down the hard drives when they are not in use can help to extend their life spans.

The default period of inactivity before spinning down the hard drives is 20 minutes. To revise this time, click on the pull-down menu for **Turn off the hard drives**.

## Power saving mode

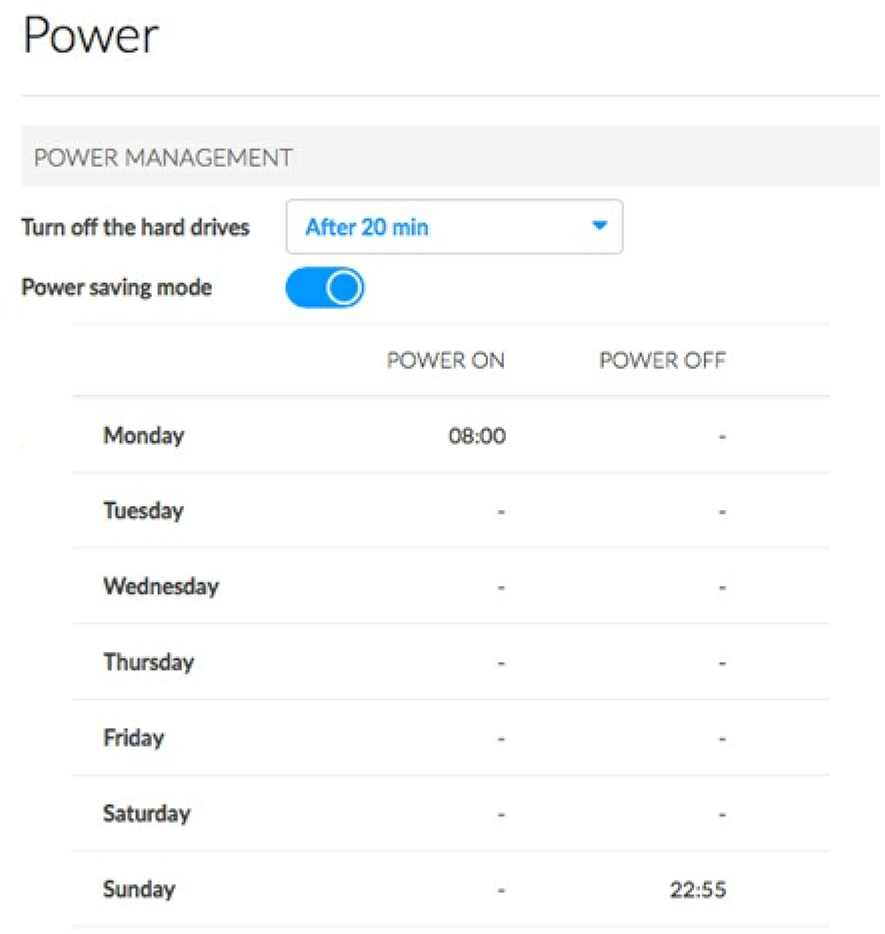
Many work environments may not require the NAS to be active all hours of the day or even the entire week. The administrator can take advantage of anticipated down time by scheduling the NAS to power off and power on as needed.

While in power saving mode, the NAS suspends all activity, including spinning down the hard drives and turning off its fans and LEDs. All processes enabled in NAS OS, including downloads and backups, will be terminated. Since the shares are not accessible and the device cannot be managed via NAS OS, power saving mode should be used when no one is accessing the NAS's data.

Example 1: The six employees of a small printing company arrive at the office no earlier than 6:00 AM and all activity stops after 10:00 PM. To save power and extend the life of the NAS’s hardware, the administrator schedules the NAS to power on at 5:00 AM and power off at 11:00 PM.

Example 2: The 50 employees at a branch office require 24-hour access to the NAS Monday through Friday. However, the branch office manager prefers that employees do not work during the weekend. Therefore, the administrator decides to schedule the NAS to power on Monday at 6:00 AM and power off Friday at 11:00 PM.

**Schedule power saving mode**



Power

POWER MANAGEMENT

Turn off the hard drives: After 20 min

Power saving mode: ●

|  | POWER ON | POWER OFF |
|---|---|---|
| Monday | 08:00 | - |
| Tuesday | - | - |
| Wednesday | - | - |
| Thursday | - | - |
| Friday | - | - |
| Saturday | - | - |
| Sunday | - | 22:55 |

1. Click the slider for **Power saving mode** to enable the schedule.
2. Set the time of day that the NAS will wake from power saving mode. Click on the day of the week in the **Power on** column.
3. In the pop-up window, choose the radio button next to **Scheduled** and set the time.
4. Choose **Save.**
5. Set the time of day that the NAS will enter power saving mode. Click on the day of the week in the **Power off** column.
6. In the pop-up window, choose the radio button next to **Scheduled** and set the time.
7. Choose **Save**.

## Wake the NAS from power saving mode

To wake the NAS from power saving mode, apply a short press to the power button. You can also use the Wake on LAN function in Seagate Network Assistant (see Wake on LAN (WOL)).

# UPS management

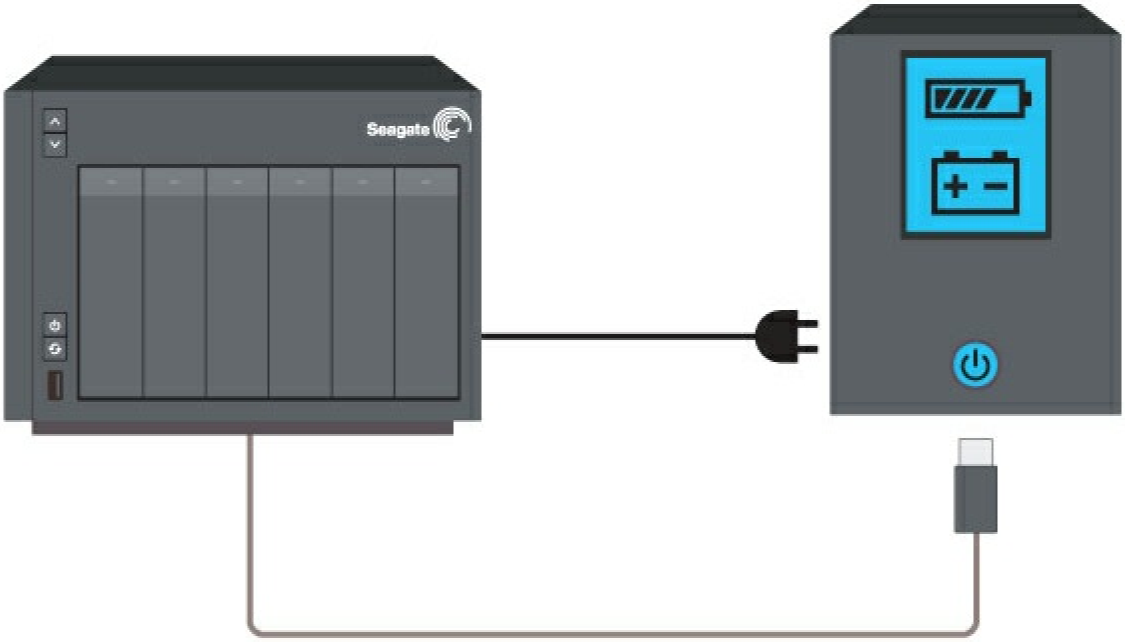
NAS OS supports three types of UPS (uninterruptible power source) management:

- Single NAS device: Direct connection to a UPS
- Multiple NAS devices A: One NAS OS device takes the role of Network UPS server
- Multiple NAS devices B: The UPS connects directly to the router and acts as the Network UPS server

**Important info**: Seagate cannot guarantee that all UPS devices are compatible with NAS OS UPS management.

**Important info**: Make certain to review the UPS's documentation before connecting it to your NAS devices.

## Single NAS: Direct connection



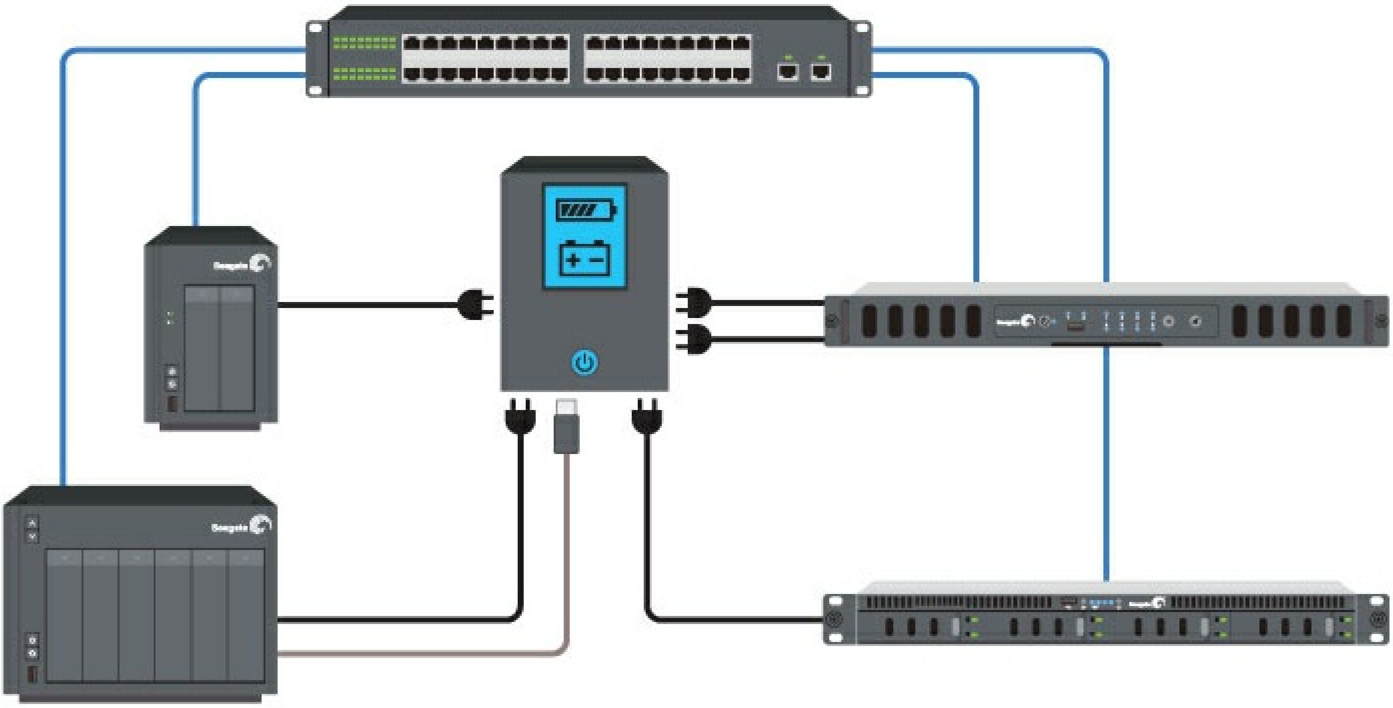
Follow the directions below when connecting a single NAS OS device to a UPS.

1. Confirm that no one is accessing the NAS OS device and power it off.
2. Connect the NAS to a supported UPS via power and USB cables. The USB cable is required for the UPS management information.
3. Power on the NAS and go to the Power page. The UPS should appear in the UPS management section.

*Battery threshold level* refers to the percentage of power available to the UPS's battery. In the event that a working environment loses power, the NAS automatically powers off when the UPS reaches the threshold level. Without the UPS's threshold level, power is suddenly cut off to the NAS, potentially causing the loss and corruption of data.

The administrator can adjust the threshold by clicking on the pencil icon.

## Multiple NAS devices A: A NAS OS device is the network UPS server



The instructions below suggest adding all NAS OS devices to the UPS at once. However, you can connect each NAS OS device as required by your working environment.

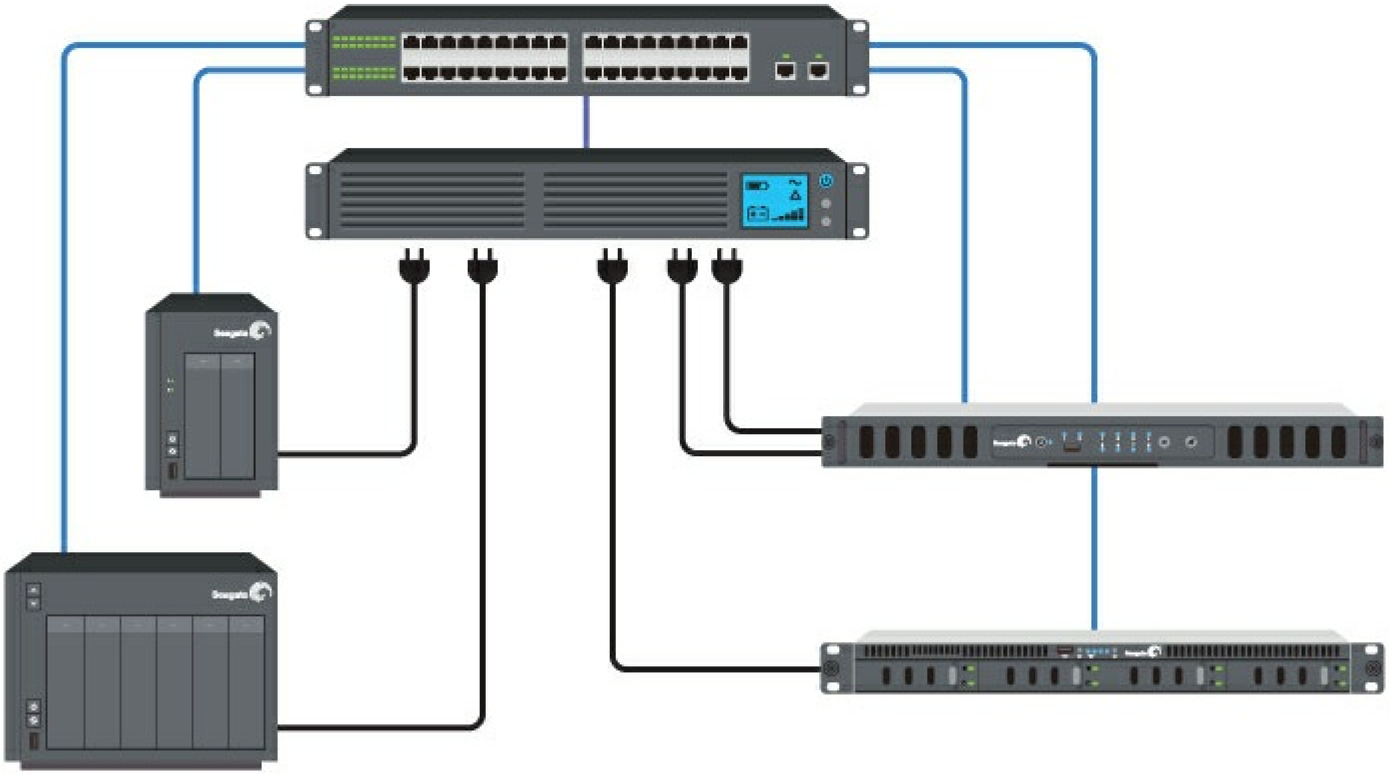
1. Confirm that no one is accessing the first NAS OS device and power it off. This NAS will become Network UPS server.
2. Connect the first NAS to a supported UPS via power and USB cables. The USB cable is required for the UPS management information.
3. Power on the first NAS and go to the Power page. The UPS should appear in the UPS management section.
4. Check the box next to **Network UPS server**.
5. Confirm that no one is accessing the other NAS OS devices on the same network and power them off.
6. Connect the other NAS devices to the UPS via power cables only and power them on.
7. For each NAS OS device, go to the Power page and choose **Add a network UPS server**.
8. In the pull-down menu for **Network UPS type**, select **Seagate NAS UPS server**.
9. Select the first NAS and choose **Save**.

*Battery threshold level* refers to the percentage of power available to the UPS's battery. In the event that a working environment loses power, the NAS devices automatically power off when the UPS reaches the threshold level. Without the UPS's threshold level, power is suddenly cut off to the NAS devices, potentially causing the loss and corruption of data.

The administrator can adjust the threshold on the first NAS by clicking on the pencil icon. Unlike the first NAS, the other NAS devices cannot adjust the battery threshold level.

**Remove the network UPS server**
Choose **Remove the network server** to disconnect a NAS from the network UPS server.

## Multiple NAS devices B: The UPS is the network UPS server



The following configuration requires a UPS with an Ethernet port to connect to the same router as the NAS OS devices. Additionally, the UPS must support SNMP to communicate with the NAS OS devices on the network. Refer to your UPS's documentation for further details.

The instructions below suggest adding all NAS OS devices at once. However, you can connect each NAS OS device as required by your working environment.

1. Connect the UPS to a power source and the network router according to the instructions provided in the UPS's documentation.
2. Confirm that no one is accessing the NAS OS devices and power them off.
3. Connect the NAS OS devices to the UPS via power cables only and power them on.
4. For each NAS OS device, go to the Power page and choose **Add a network UPS server**.
5. In the pull-down menu for **Network UPS type**, select **SNMP UPS**.
6. Enter the UPS's IP address and, if applicable, SNMP community. Refer to the UPS's administration tool for its IP address.
7. Choose **Save.**

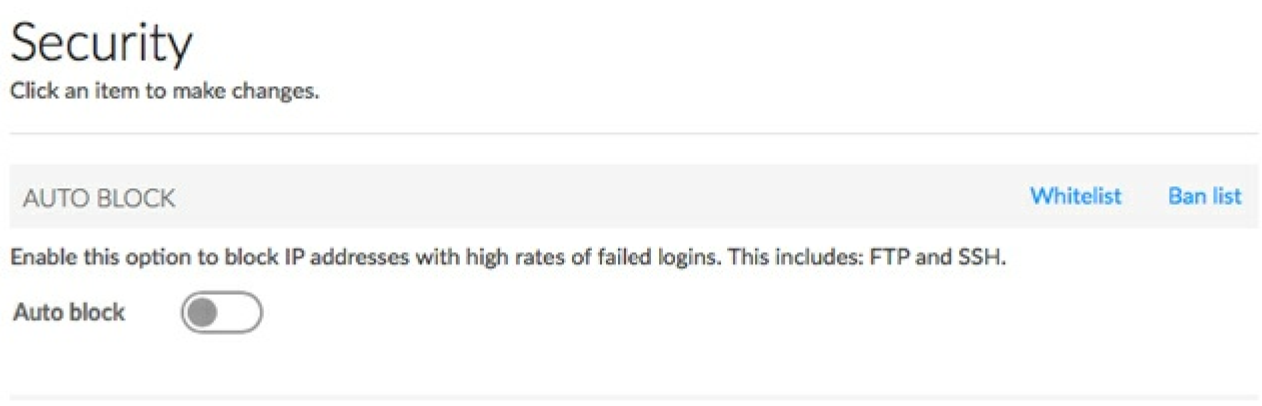
NAS OS cannot adjust the battery threshold level when connecting to a UPS server via the network. Check the documentation for your UPS to learn more on how to manage the device.

**Remove the network UPS server**
Choose **Remove the network server** to disconnect a NAS from the network UPS server.

# Security

Use the Security tab to prevent potential attackers from reaching your NAS OS device. You can also control access to your NAS OS device using Ban and White lists.

## Auto Block


Security

Click an item to make changes.

Enable this option to block IP addresses with high rates of failed logins. This includes: FTP and SSH.

Enable *auto block* to block IP addresses that have made numerous failed attempts to log into the device and automatically add them to the *Ban list*. IP addresses on the ban list are prevented from accessing your NAS OS device.

Click the switch to enable auto block. See below for the default settings for auto block:

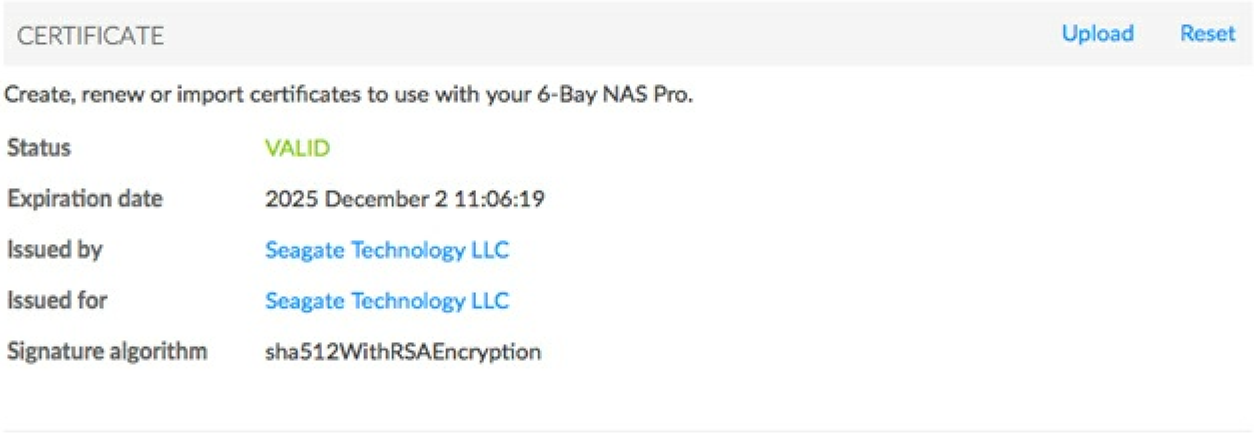
- Maximum failed logins: 3
- Failed logins within (minutes): 2
- Block for (minutes): 2

The settings can be changed when auto block is enabled.

To prevent users from losing access due to failed logins, add their IP addresses to the *Whitelist*. Click **Whitelist** and then enter the IP addresses.

Auto block is optimized for FTP and SSH protocols. You can manage the ban list by clicking **Ban list** and manually entering or removing IP addresses.

## Certificate



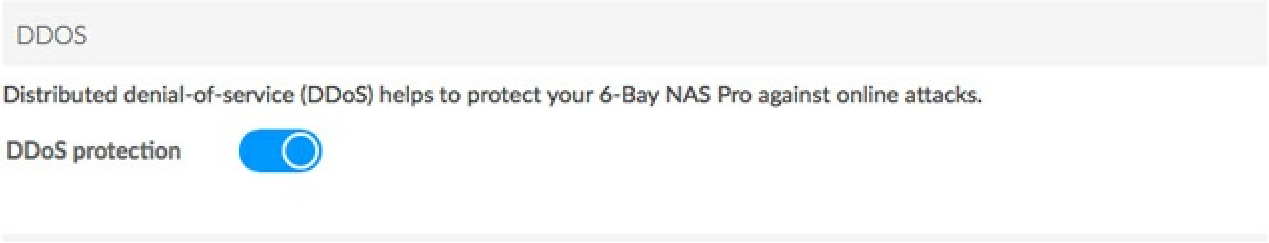
Create, renew or import certificates to use with your 6-Bay NAS Pro.

| | |
|---|---|
| Status | VALID |
| Expiration date | 2025 December 2 11:06:19 |
| Issued by | Seagate Technology LLC |
| Issued for | Seagate Technology LLC |
| Signature algorithm | sha512WithRSAEncryption |

An SSL Certificate is a data file with an encrypted key targeted for use by your company or organization. While your NAS OS device's default certificate offers high security, you can create a unique certificate for use with your NAS OS device. Costs for SSL Certificates vary by third-party provider.

Custom SSL Certificates can be uploaded to your NAS OS device to replace the default certificate. To take advantage of the security provided by an SSL Certificate, make certain to choose **Switch to HTTPS** at the NAS OS login page.

## DDOS

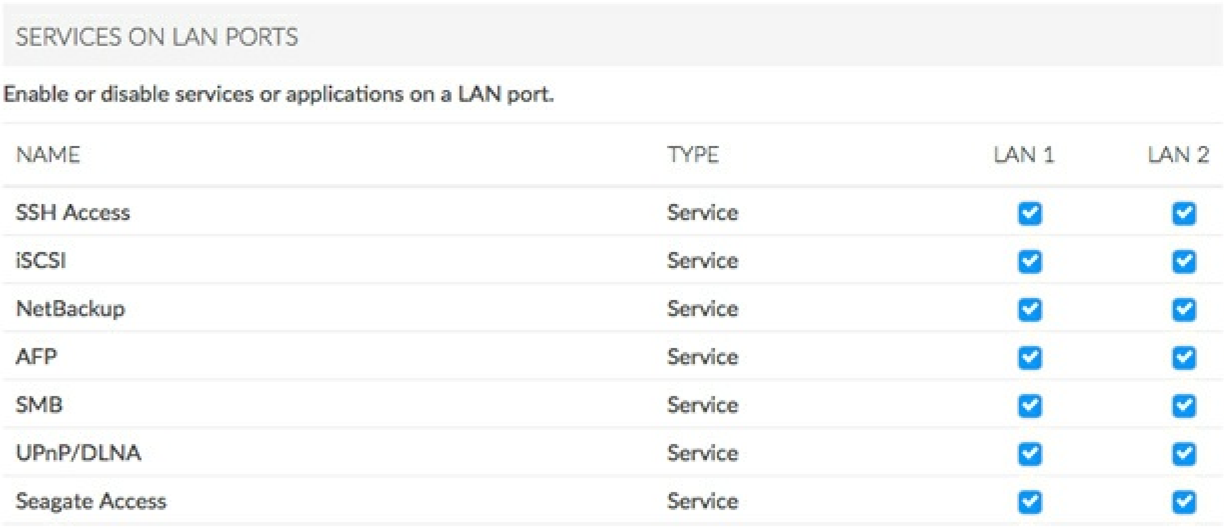


Distributed denial-of-service (DDoS) helps to protect your 6-Bay NAS Pro against online attacks.

DDoS protection ●

Distributed denial-of-service (DDoS) is a type of attack in which multiple devices target a single device. The multiple devices can attack from local and wide area networks or via the Internet and are often infected with a Trojan. The end result is a denial of service for the target device. You can improve your NAS OS device's chances of avoiding such an attack by clicking the switch to enable DDoS protection.

## Services on LAN Ports



SERVICES ON LAN PORTS

Enable or disable services or applications on a LAN port.

| NAME | TYPE | LAN 1 | LAN 2 |
|---|---|---|---|
| SSH Access | Service | ☑ | ☑ |
| iSCSI | Service | ☑ | ☑ |
| NetBackup | Service | ☑ | ☑ |
| AFP | Service | ☑ | ☑ |
| SMB | Service | ☑ | ☑ |
| UPnP/DLNA | Service | ☑ | ☑ |
| Seagate Access | Service | ☑ | ☑ |

Enable or disable select services on one or both of your NAS OS device's LAN ports.

# Monitoring

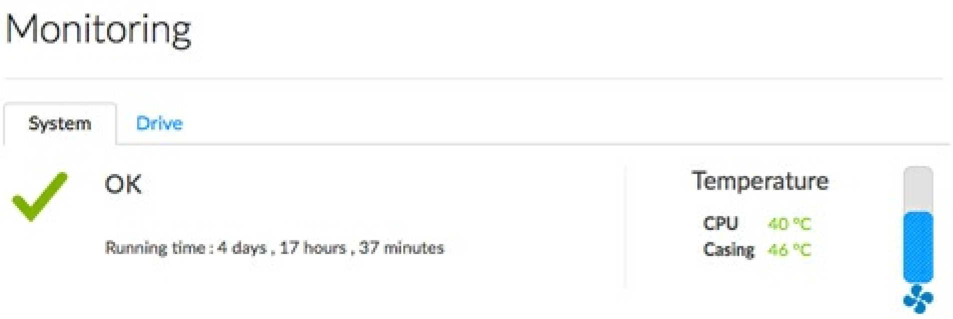
Monitoring provides a summary of the NAS OS device's hardware and the health of its components.

# System tab

System details will vary based upon your NAS OS device. For example, an enclosure with a single Ethernet port can only list one LAN. Also, NAS OS devices with audible alarms include the option to turn the sound on or off.

When reviewing the System tab, place your cursor over the charts and graphics on the page for additional readings. Moving the cursor over the graphic for the fan shows its current revolutions per minute (RPM). Additional readings are available with RAM, CPU, and Network.

## Upper pane: General health, temperature, and fans



OK

Running time : 4 days , 17 hours , 37 minutes

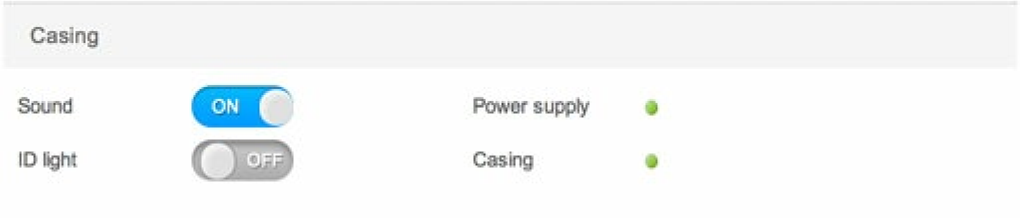
Temperature

CPU 40 °C

Casing 46 °C

- A green check mark on the upper left indicates that your hardware is operational and there are no problems. A red "X" alerts you to potential problems with the hardware. It is accompanied by an error

message, such as the device has reached a critical temperature.
- The running time below the check mark indicates consecutive hours and minutes of operation. The clock will restart each time the device is powered on, restarted, or wakes up from power saving or deep sleep modes.
- The temperatures of the device's CPU and casing are located on the upper right



Casing

Sound ON

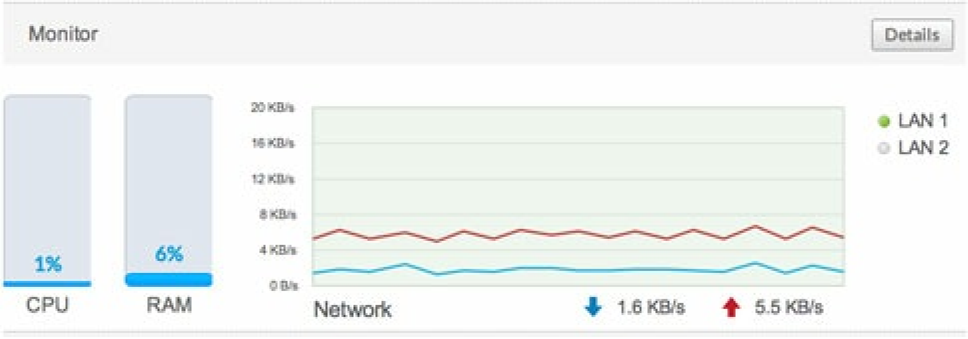
ID light OFF

Power supply ●

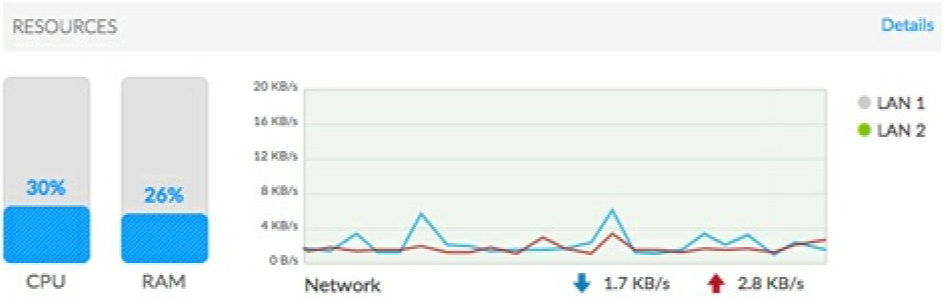
Casing ●

## Upper middle pane: Casing (select NAS OS devices only)

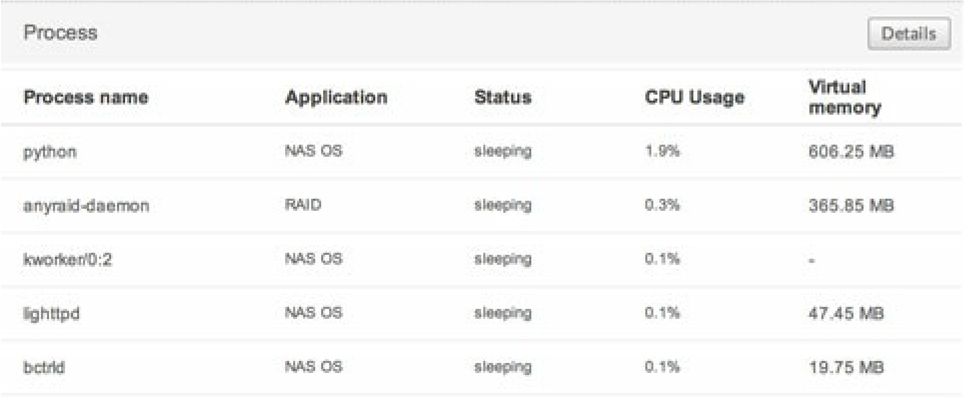
- Click on the **ID light** slider to make the identification LED blink. This is helpful when locating a rackmount NAS on a rack with many devices.
- Click on the **Sound** slider to enable or disable the audible alert.
- *Casing*: A green circle means that the enclosure’s top cover is closed. Check the cover if the circle is not green.
- *Power*: A green circle indicates that the power supplies are working as expected. Check the power supplies if the circle is not green.



## Middle pane: Resources



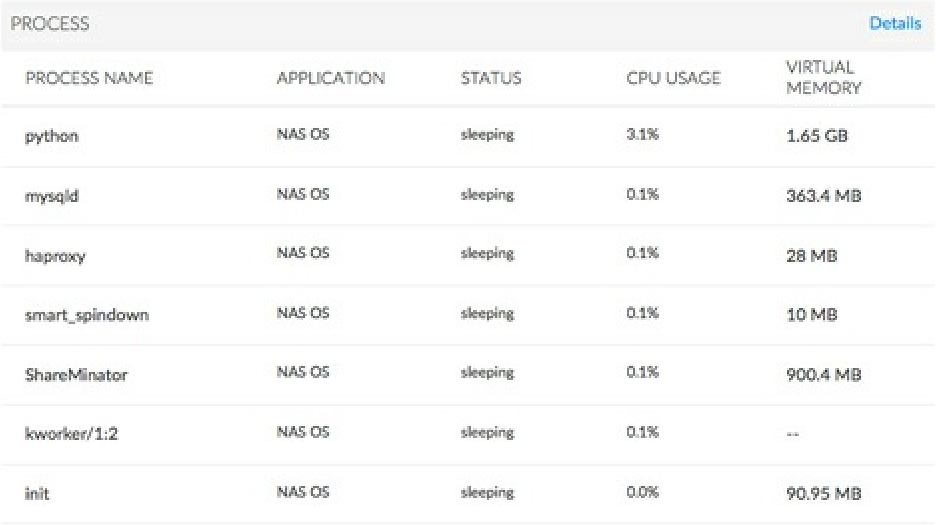
- The *Resources* pane shows dynamic graphics of the demands placed upon the CPU and RAM. To the right, a real-time graph offers constant updates on the NAS’s network transfer rates. For an expanded look at CPU, RAM, and network performance, click **Details** in the *Resources* pane.
- A green circle next to the LAN means that it is connected to the network. A white circle means that the LAN is not connected to the network.



Process

| Process name | Application | Status | CPU Usage | Virtual memory |
|---|---|---|---|---|
| python | NAS OS | sleeping | 1.9% | 606.25 MB |
| anyraid-daemon | RAID | sleeping | 0.3% | 365.85 MB |
| kworker/0:2 | NAS OS | sleeping | 0.1% | - |
| lighttpd | NAS OS | sleeping | 0.1% | 47.45 MB |
| bctrld | NAS OS | sleeping | 0.1% | 19.75 MB |

## Lower pane: Process



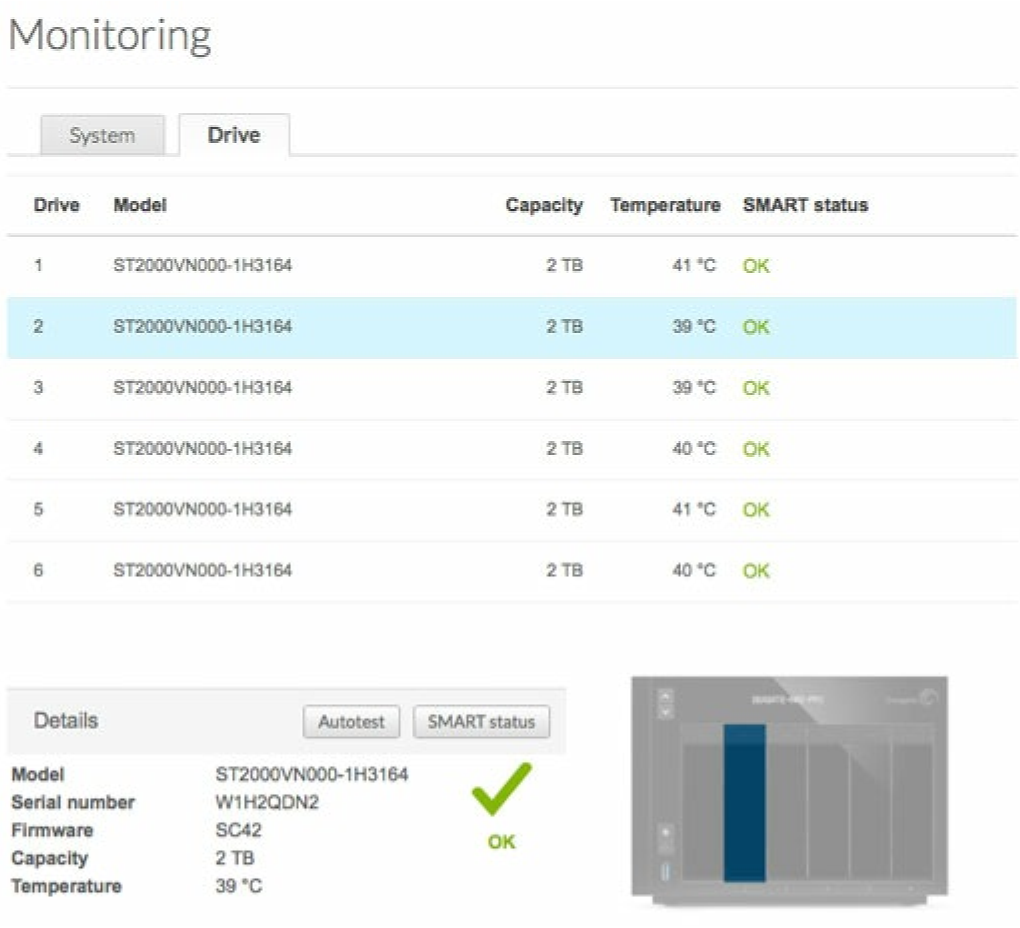
PROCESS

| PROCESS NAME | APPLICATION | STATUS | CPU USAGE | VIRTUAL MEMORY |
|---|---|---|---|---|
| python | NAS OS | sleeping | 3.1% | 1.65 GB |
| mysqld | NAS OS | sleeping | 0.1% | 363.4 MB |
| haproxy | NAS OS | sleeping | 0.1% | 28 MB |
| smart_spindown | NAS OS | sleeping | 0.1% | 10 MB |
| ShareMinator | NAS OS | sleeping | 0.1% | 900.4 MB |
| kworker/1:2 | NAS OS | sleeping | 0.1% | -- |
| init | NAS OS | sleeping | 0.0% | 90.95 MB |

- The *Process* pane lists the five processes that are placing the highest demands upon the CPU. Click on **Details** in the *Process* pane to see the full list of processes.

## Temperature and fan warnings

- *Temperature error*: Check the placement of your NAS to make certain that it is not receiving an abnormal amount of heat from external sources (e.g. sun from a window, heating duct, exhaust from other electronics, etc.). If the problem persists, see **Getting Help** for links to contact customer support.
- *Fan error*: Check the fan performance line graph to determine if the fans are running too high or not at all.
- *Drive error*: Select the **Drive** tab to review the status for the NAS's hard drives.



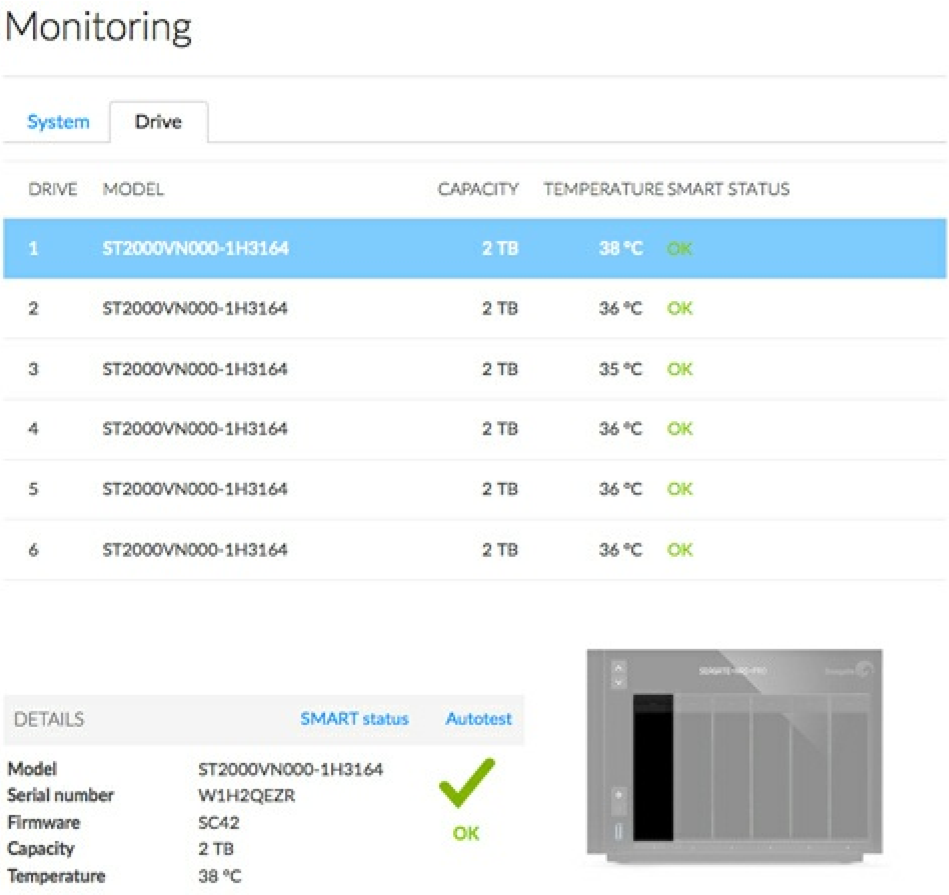
Monitoring

| Drive | Model | Capacity | Temperature | SMART status |
|---|---|---|---|---|
| 1 | ST2000VN000-1H3164 | 2 TB | 41 °C | OK |
| 2 | ST2000VN000-1H3164 | 2 TB | 39 °C | OK |
| 3 | ST2000VN000-1H3164 | 2 TB | 39 °C | OK |
| 4 | ST2000VN000-1H3164 | 2 TB | 40 °C | OK |
| 5 | ST2000VN000-1H3164 | 2 TB | 41 °C | OK |
| 6 | ST2000VN000-1H3164 | 2 TB | 40 °C | OK |

Details

| | |
|---|---|
| Model | ST2000VN000-1H3164 |
| Serial number | W1H2QDN2 |
| Firmware | SC42 |
| Capacity | 2 TB |
| Temperature | 39 °C |

# Drive tab



Monitoring

| DRIVE | MODEL | CAPACITY | TEMPERATURE | SMART STATUS |
|---|---|---|---|---|
| 1 | ST2000VN000-1H3164 | 2 TB | 38 °C | OK |
| 2 | ST2000VN000-1H3164 | 2 TB | 36 °C | OK |
| 3 | ST2000VN000-1H3164 | 2 TB | 35 °C | OK |
| 4 | ST2000VN000-1H3164 | 2 TB | 36 °C | OK |
| 5 | ST2000VN000-1H3164 | 2 TB | 36 °C | OK |
| 6 | ST2000VN000-1H3164 | 2 TB | 36 °C | OK |

| | |
|---|---|
| Model | ST2000VN000-1H3164 |
| Serial number | W1H2QEZR |
| Firmware | SC42 |
| Capacity | 2 TB |
| Temperature | 38 °C |

Review basic information for each hard drive in the enclosure, including the model number, capacity, temperature, and SMART status. SMART stands for Self-Monitoring, Analysis and Reporting Technology. SMART status should be used for informational purposes only, specifically when diagnosing hard drives. It lets you know if the hard drive is reporting or experiencing errors. If a hard drive has an error, run a SMART test by selecting the **Autotest** button.

Additional notes on the Drive tab:

- Acceptable **Temperature** values may differ based upon the make and model of the hard drive.
- The dynamic photo of your NAS will highlight the hard drive selected in the hard drive table.
- Choose **SMART status** to review the full SMART report on the selected hard drive.

# Notifications

Use the Notifications page to manage how the administrator receives updates on the health of the NAS OS device. The page has two tabs:

- Notifications: NAS OS alerts and activity
- SNMP: Monitoring and managing the NAS using the Simple Network Management Protocol

# Notifications tab

# Email notifications

NAS OS can send important activity updates to the administrator via email. See the table below for events that trigger email notifications.

**Email notification triggers**

| Event identifier | Description | Recipient |
|---|---|---|
| Capacity | The total available capacity is less than 10% | Administrator |
| Quota | The user has reached 90% of his storage quota | Administrator |
| Download | A download job has completed or a download job error has occurred | Administrator |
| Backup | A backup job has failed | Administrator |
| Fan | The fan has stopped | Administrator |
| Temperature | The product has remained at maximum temperature for at least one minute | Administrator |
| Password recovery | A user has recovered his/her password | Administrator or user, depending on who made the request |

Turn **Email notifications** on or off by clicking on its slider. The default server for email notifications is *Seagate*, a secure email system.

Administrators have the option to use an alternative email server. Pass the cursor over *Seagate* and click on the pencil icon. Choose **Custom** in the pull-down menu and complete the fields in the pop-up window:

- Enter the SMTP address for your email server. You can use an in-house SMTP server or third-party providers such as Gmail, Outlook, and Yahoo.
- You have the option to enable SSL by checking its box.
- If your email server requires verification, check the box next to **SMTP authentication** to enter the username and password.
- Test the connection by checking the box next to **Send a verification email**.

# Recent activity

Review the events for the NAS OS device. To parse the events list into categories and sub-categories, choose **Filter**.

The events list is important when troubleshooting the NAS OS device with Seagate technical support. A full log of events is available for download by choosing **Download System Log**.

To purge all events from the log list, choose **Clear logs**.

# SNMP tab

Administrators with advanced networks that include SNMP can add the NAS OS device as an agent. NAS OS supports SNMP versions v1/v2 and, for enhanced security, v3.

Turn on the **SNMP agent** by clicking on its slider. To make changes to the SNMP configuration, pass the cursor over a setting and click on it.

# Storage

The information below identifies and explains the functions on the Storage page. For directions on how to configure RAID for your NAS OS device, go to RAID.

# NAS OS volume and RAID management

NAS OS supports multiple volumes, each with its own level of RAID. The maximum number of supported volumes depends upon the amount of disks in the NAS's enclosure. For example, a NAS OS device with eight hard drives can have up to eight volumes.

## Enhanced data protection: NAS OS SimplyRAID

No matter the capacity of your hard drives, NAS OS SimplyRAID will prepare the storage for immediate use as well as future expansion. SimplyRAID allows you to:

- Install disks of varying capacities
- Replace smaller capacity hard drives with larger capacity hard drives
- Upgrade storage capacity without deleting or moving data
- Protect data without compromising performance

When using hard drives of varying capacities, SimplyRAID will attempt to optimize available storage for your data.

## Standard disk configuration: Manual RAID

While the benefits of SimplyRAID are highly recommended, the Storage page also gives you the option to manually configure your hard disks as:

- JBOD

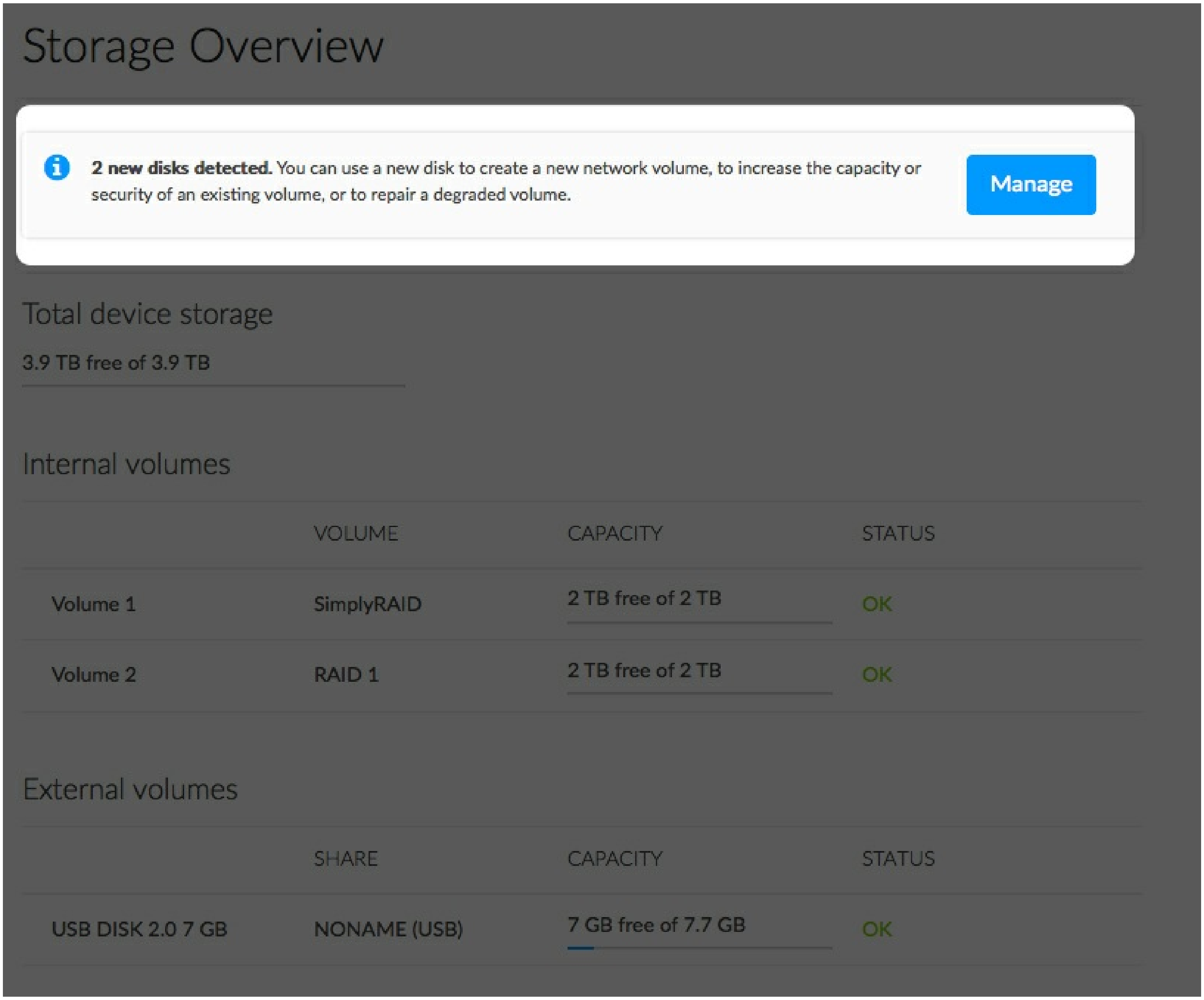
- RAID 0 (minimum two hard drives)
- RAID 1 (minimum two hard drives for data protection)
- RAID 1+Spare (minimum three hard drives)
- RAID 5 (minimum three hard drives)
- RAID 5+Spare (minimum four hard drives)
- RAID 6 (minimum four hard drives)
- RAID 6+Spare (minimum five hard drives)
- RAID 10 (minimum four hard drives)
- RAID 10+Spare (minimum five hard drives)

# Storage overview

Choose **Storage > Overview** to:

- Review the list of the NAS's volumes and their current state.
- Configure new hard drives added to the NAS.

## Manage



Storage Overview

**2 new disks detected.** You can use a new disk to create a new network volume, to increase the capacity or security of an existing volume, or to repair a degraded volume.

Total device storage

3.9 TB free of 3.9 TB

Internal volumes

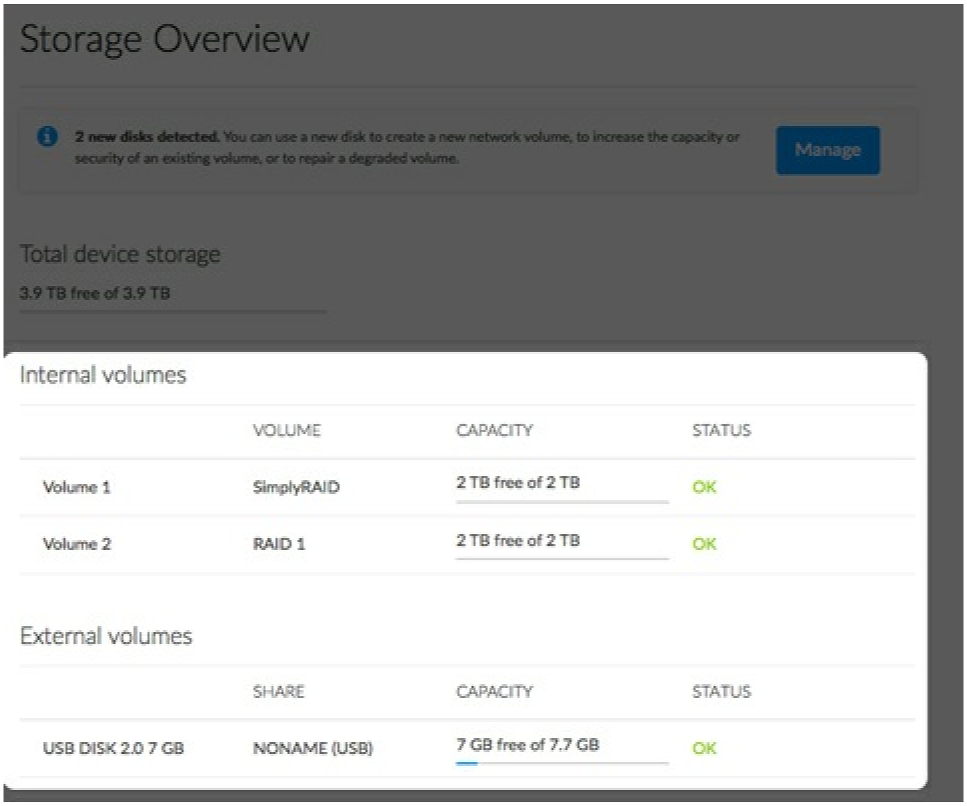
| | VOLUME | CAPACITY | STATUS |
|---|---|---|---|
| Volume 1 | SimplyRAID | 2 TB free of 2 TB | OK |
| Volume 2 | RAID 1 | 2 TB free of 2 TB | OK |

External volumes

| | SHARE | CAPACITY | STATUS |
|---|---|---|---|
| USB DISK 2.0 7 GB | NONAME (USB) | 7 GB free of 7.7 GB | OK |

The Manage button is available when the enclosure has new or unused hard drives. Choose **Manage** on the Storage Overview page to create a new volume. For further information, see RAID.

## Internal and External volumes



Storage Overview

**2 new disks detected.** You can use a new disk to create a new network volume, to increase the capacity or security of an existing volume, or to repair a degraded volume.

Total device storage

3.9 TB free of 3.9 TB

Internal volumes

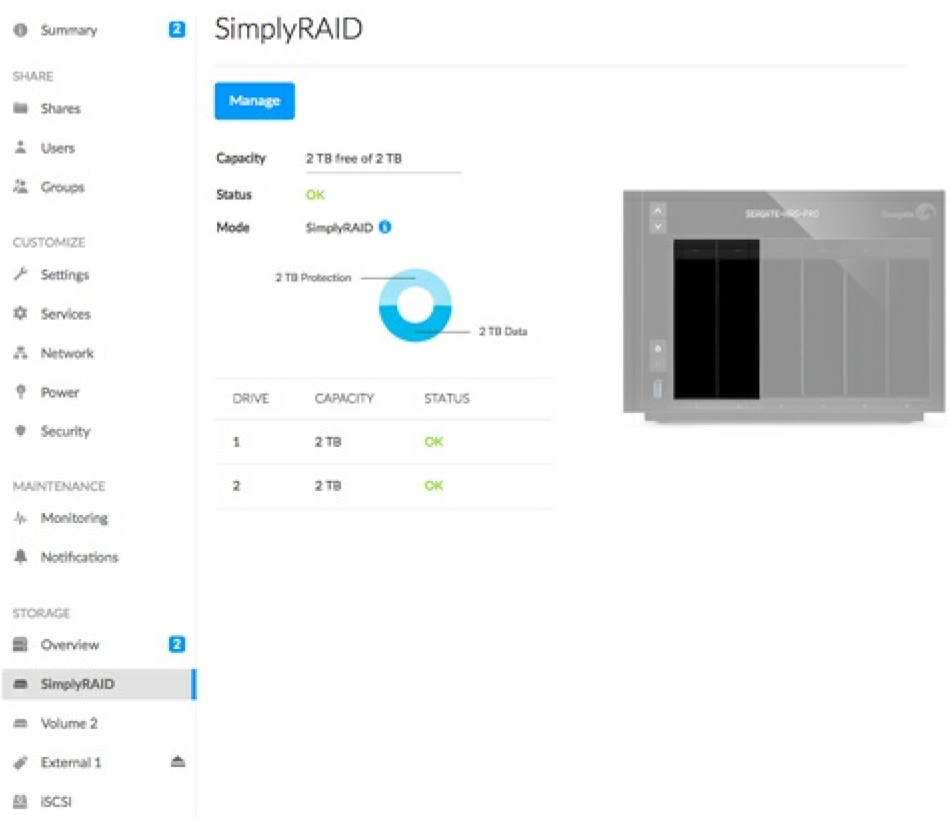
| | VOLUME | CAPACITY | STATUS |
|---|---|---|---|
| Volume 1 | SimplyRAID | 2 TB free of 2 TB | OK |
| Volume 2 | RAID 1 | 2 TB free of 2 TB | OK |

External volumes

| | SHARE | CAPACITY | STATUS |
|---|---|---|---|
| USB DISK 2.0 7 GB | NONAME (USB) | 7 GB free of 7.7 GB | OK |

Internal volumes are the volumes created from the disks inserted into the NAS's enclosure. External volumes are storage devices connected to the USB or eSATA ports. Click on a volume to review and adjust its settings.

## Volume settings



SimplyRAID

Capacity 2 TB free of 2 TB

Status OK

Mode SimplyRAID

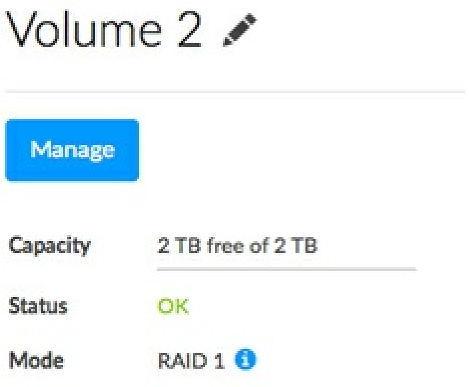
| DRIVE | CAPACITY | STATUS |
|---|---|---|
| 1 | 2 TB | OK |
| 2 | 2 TB | OK |

Choose a volume's name on the left to view the tools to manage it.

### Name

The default name for the first new volume is Volume 1. The number will rise incrementally when adding new volumes, Volume 2, Volume 3, etc. To change the name:

1. Pass the cursor over the name of the volume and choose the pencil icon.



Volume 2

Capacity 2 TB free of 2 TB

Status OK

Mode RAID 1

2. Type the new name in the pop-up window
3. Choose **Save**.

Due to the high level of security, an encrypted volume retains its default name.

### Manage

Choose **Manage** on the volume page to:

- Add hard drives to the volume.
- Add a spare hard drive to the volume.
- Repair the volume.
- Expand the volume’s storage capacity.
- Change the encryption settings (if applicable).
- Upgrade the volume from single-disk security to double-disk security.
- Format the volume (delete all data without deleting the volume).
- Delete the volume (permanently remove the volume and all of its data).

**Capacity**
A quick reference of the volume's:

- Total storage capacity.
- Available storage capacity.

An *i* tooltip appears in the capacity row following the creation of an iSCSI target. Pass the cursor over the tooltip to view the amount of storage assigned to the volume's iSCSI target.

**Status**
**Status** gives you immediate feedback on the health of the volume's RAID configuration:

- **OK**. The RAID is operational and no problems have been detected.
- **No data protection**. Data is intact but one or more hard drives are missing or reporting errors. The amount of hard drives that can fail before this message appears is contingent upon the level of RAID.
- **Protected if one disk fails**. RAID configurations with double-disk security will see this message if a single hard drive is missing or reporting errors.
- **Broken**. The RAID is broken resulting in a loss of data.
- **Synchronizing**. The system is synchronizing data across all the hard drives in the volume.
  - The volume is available for use while the RAID is synchronizing but NAS performance may be affected.
  - RAID data protection will be available once synchronizing is complete.
  - Choose the tooltip next to **Synchronizing** for details on its progress.

**Mode**
**Mode** lists the volume's RAID level. Pass the cursor over the tooltip for details on the RAID's level of data protection.

**Storage graph**
A multicolor circle shows how the RAID distributes the volume's storage.

- **Dark blue**: Storage capacity for your data.
- **Light blue**: Protection in case one or two hard drives fail. The light blue indicator will vary in size depending upon single or double disk protection.

- **Green**: Disk capacity that spans beyond the level of RAID. This space is reserved for expansion should you add new or, larger capacity hard drives.

Factors that determine the storage capacities for data, protection, and expansion:

- The amount of hard drives in the enclosure.
- The storage capacity of each hard drive (see note below on mixed capacities).
- RAID mode
- Single-disk or double-disk security

Examples:

- **RAID 0 with five hard drives**. The only color is dark blue for data capacity since RAID 0 has no protection.
- **SimplyRAID with two hard drives of equal capacity**. Dark and light blue for data and protection, respectively.
- **RAID 6 with five hard drives of mixed capacities**. All colors are represented since the RAID 6 uses double-disk security and the hard drives are of mixed capacities.

**Volume list and dynamic photo**
Review the hard drives' capacities and status. The dynamic photo of the NAS highlights:

- The hard drives associated with the volume.
- Hard drives available for a new or existing volume.
- Empty slots available for expansion.
- Failed or missing disks.

# RAID

Refer to the table below for an overview of the RAID modes available to your NAS OS device. Note that the levels of performance and protection will differ based upon the number of drives in the volume. The NAS OS New network volume wizard includes a helpful tooltip with star ratings for performance and protection based upon the amount of disks in the volume.

| RAID mode | Minimum hard drives |
|---|---|
| SimplyRAID | 1 (no data protection) or 2 (with data protection) |
| SimplyRAID dual | 3 |
| JBOD | 1 |
| RAID 0 | 2 |
| RAID 1 | 1 (no data protection) or 2 (with data protection) |
| RAID 5 | 3 |
| RAID 6 | 4 |
| RAID 10 | 4 |

The factory default RAID for a NAS OS device varies upon the amount of hard drives in the enclosure:

- 0 hard drives: SimplyRAID with single-disk protection will be configured during the NAS OS installation.
- 2 hard drives: SimplyRAID with single-disk protection
- 4 hard drives: SimplyRAID with single-disk protection
- 8 hard drives: SimplyRAID dual with double-disk protection

Single-disk protection: data is safe if one hard drive fails.

Double-disk protection: data is safe if two hard drives fail.

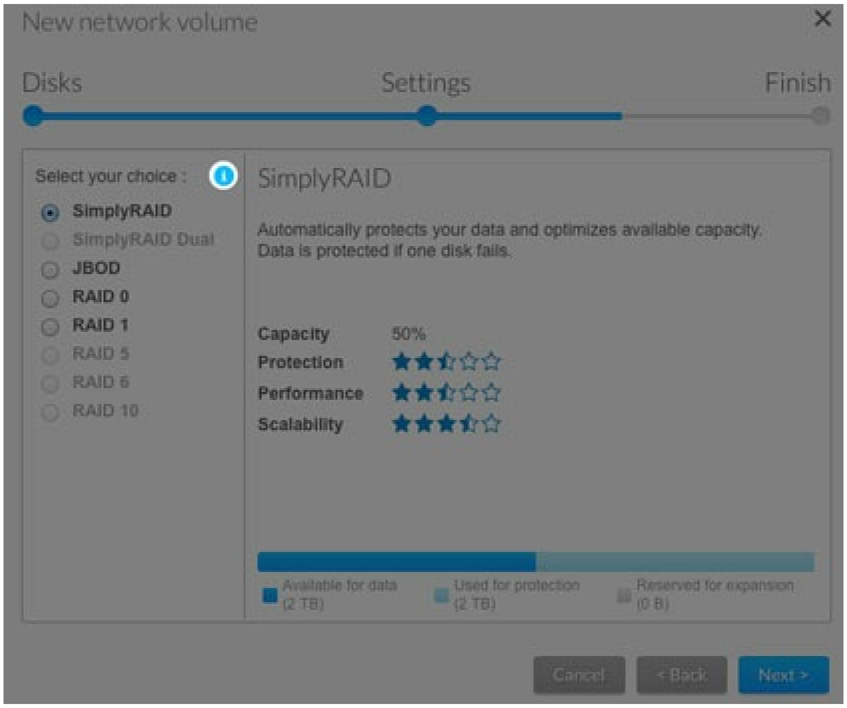
**Note on enclosures with one hard drive**: You can create a SimplyRAID or a RAID 1 volume with a single hard drive. However, there is NO DATA PROTECTION when the volume has only one hard drive. Therefore, when new hard drives in the enclosure are available, it is highly recommended that you expand the single-disk volume to protect your data (see Single-disk and unprotected volumes:expansion).

**Important info on NAS backup**: To further protect data against the loss of a hard drive or secondary points of failure (e.g. hardware, network, etc.), it is recommended that all users back up data to a DAS or another NAS. See Backup Manager for details.

# Get help choosing your RAID

## Tooltip: star ratings for RAID

Understanding NAS OS RAID is critical when deciding how best to apportion the hard drives in your NAS. To help administrators configure RAID volumes, the NAS OS **New network volume** wizard provides a star rating system with an intuitive storage capacity bar. The star ratings are available within the tooltip on the RAID selection step. Click on the *i* next to **Select your choice** to review the ratings.



Select your choice :

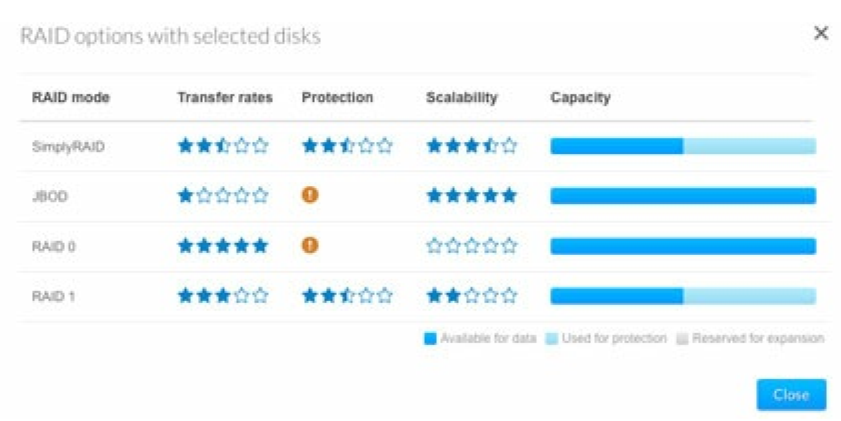
- ● SimplyRAID
- ○ SimplyRAID Dual
- ○ JBOD
- ○ RAID 0
- ○ RAID 1
- ○ RAID 5
- ○ RAID 6
- ○ RAID 10

SimplyRAID

Automatically protects your data and optimizes available capacity.
Data is protected if one disk fails.

| | |
|---|---|
| Capacity | 50% |
| Protection | ★★⯪☆☆ |
| Performance | ★★⯪☆☆ |
| Scalability | ★★★⯪☆ |

■ Available for data (2 TB) ■ Used for protection (2 TB) ■ Reserved for expansion (0 B)



RAID options with selected disks

| RAID mode | Transfer rates | Protection | Scalability | Capacity |
|---|---|---|---|---|
| SimplyRAID | ★★⯪☆☆ | ★★⯪☆☆ | ★★★⯪☆ | ■■■□□□ |
| JBOD | ★☆☆☆☆ | ! | ★★★★★ | ■■■■■■ |
| RAID 0 | ★★★★★ | ! | ☆☆☆☆☆ | ■■■■■■ |
| RAID 1 | ★★★☆☆ | ★★⯪☆☆ | ★★☆☆☆ | ■■■□□□ |

■ Available for data □ Used for protection ▨ Reserved for expansion

**Note**: Step-by-step instructions on how to create a new volume are available in New network volume wizard.

## RAID comparisons

The level of RAID available to a volume is contingent upon the amount of hard drives in the enclosure. For example, a volume with four hard drives supports all levels of RAID except for RAID 1, which is not compatible with volumes greater than three hard drives. The **New network volume** wizard offers star ratings for each RAID at the RAID selection step. Choose a RAID's radio button to review its strengths and weaknesses in the center of the window.

Example 1: When making comparisons in a volume with four hard drives, RAID 0 is the best choice for storage capacity. However, it has a major weakness: no data protection. Further, RAID 0 performance approximates that of RAID 5, which provides data protection if a hard drive fails.

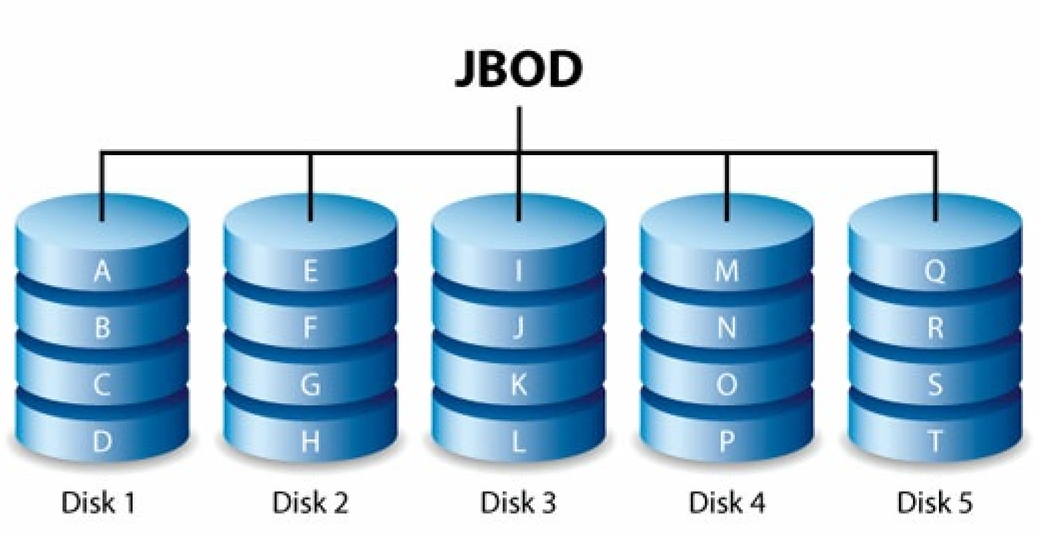
Example 2: Both RAID 6 and SimplyRAID Dual offer data protection even if two hard drives fail. However, SimplyRAID will optimize storage capacity far better than RAID 6 in mixed capacity configurations.

# RAID levels

## NAS OS SimplyRAID

Most RAID modes use equal disk capacities among the pool of hard drives to protect data. Rather then lose storage capacity overhead in mixed hard drive environments, SimplyRAID preserves the extra space for use when new hard drives are added to the enclosure. This means that, unlike standard RAID models, you can easily expand the array without losing data. For example, two 1TB hard drives will create a RAID 1 array without any storage capacity overhead. However, one 1TB hard drive paired with one 2TB hard drive only creates 1TB of protection since data cannot surpass the storage capacity of the smallest hard drive. SimplyRAID will calculate the overhead and prepare it for future expansion.

# JBOD (Just a Bunch of Disks)

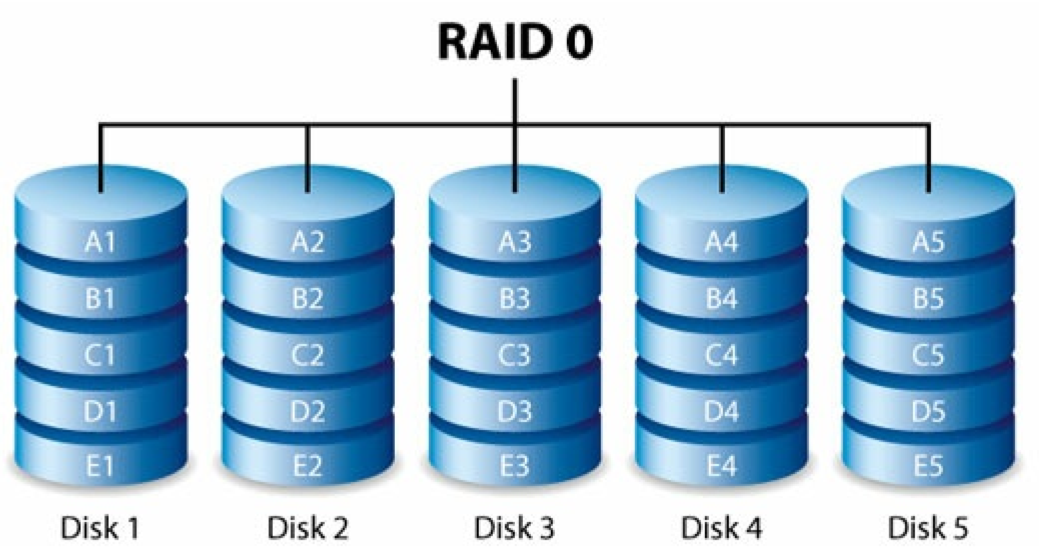


Hard drives in a JBOD configuration store data sequentially. For example, data is written to Disk 1 first. Once Disk 1 is full, data will be written to Disk 2, then Disk 3, etc. Two advantages to this level of RAID are:

- 100% availability of the hard drives' total storage capacity
- Easy expansion

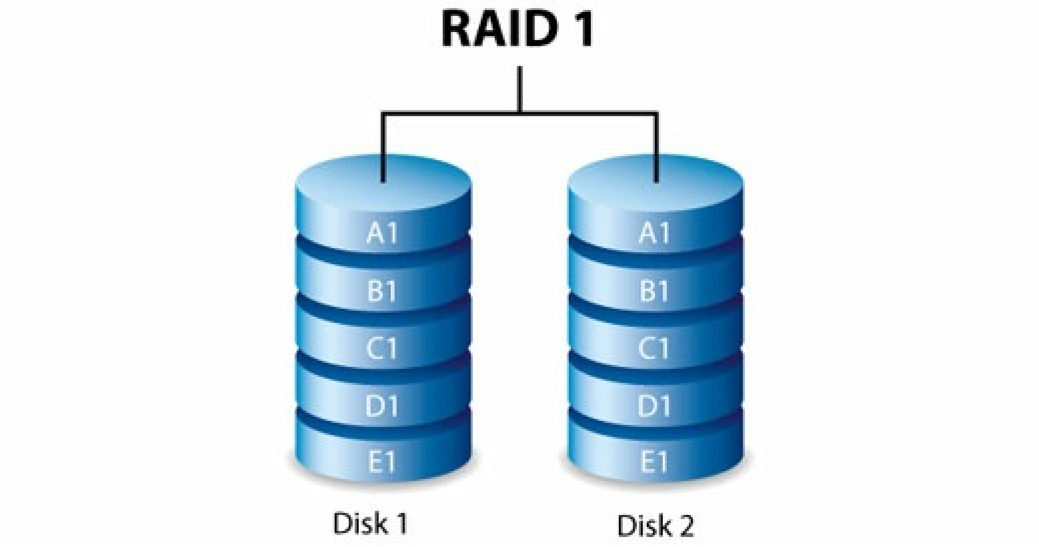
JBOD's weakness is that it has no data protection. Should a hard drive fail, all data on that hard drive will be lost.

# RAID 0



RAID 0 is the fastest RAID mode since it writes data across all of the volume's hard drives. Further, the capacities of each hard drive are added together for optimal data storage. However, RAID 0 lacks a very important feature: data protection. If one hard drive fails, all data becomes inaccessible. A recommended option is SimplyRAID or RAID 5, which offer comparable performance and data protection in case a single hard drive fails.

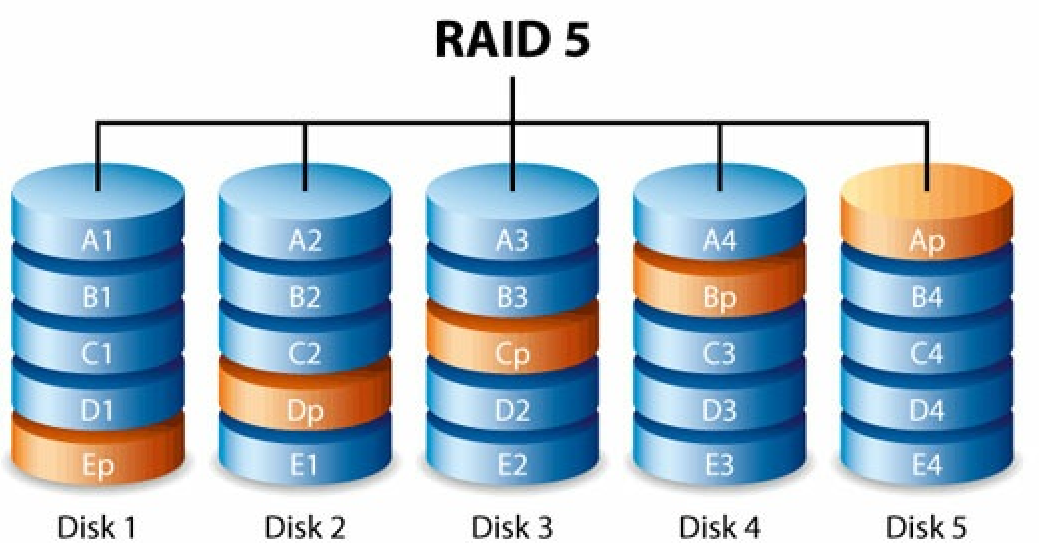
## RAID 1



RAID 1 provides enhanced data security since all data is written to each hard drive in the volume. If a single hard drive fails, data remains available on the other hard drive in the volume. However, due to the time it takes to write data multiple times, performance is reduced. Additionally, RAID 1 cuts storage capacity by 50% or more since each bit of data is stored on all disks in the volume.

**Note on RAID 1 hard drive requirements:** A standard RAID 1 configuration includes two hard drives of equal capacity. However, NAS OS allows you to create a RAID 1 volume with up to three hard drives or, three hard drives plus a spare. It is also possible to create a RAID 1 volume using a single hard drive. While a volume with one hard drive cannot provide data protection, it is ready for expansion when new hard drives are available. Data protection would become available once a second hard drive is added to the RAID 1 volume.

## RAID 5



RAID 5 writes data across all hard drives in the volume and a parity block for each data block. If one hard drive fails, the data can be rebuilt onto a replacement hard drive. No data is lost if a single hard drive fails. However, if a second hard drive fails before data can be rebuilt on the replacement hard drive, all data in the array is lost. A minimum of three hard drives is required to create a RAID 5 volume.

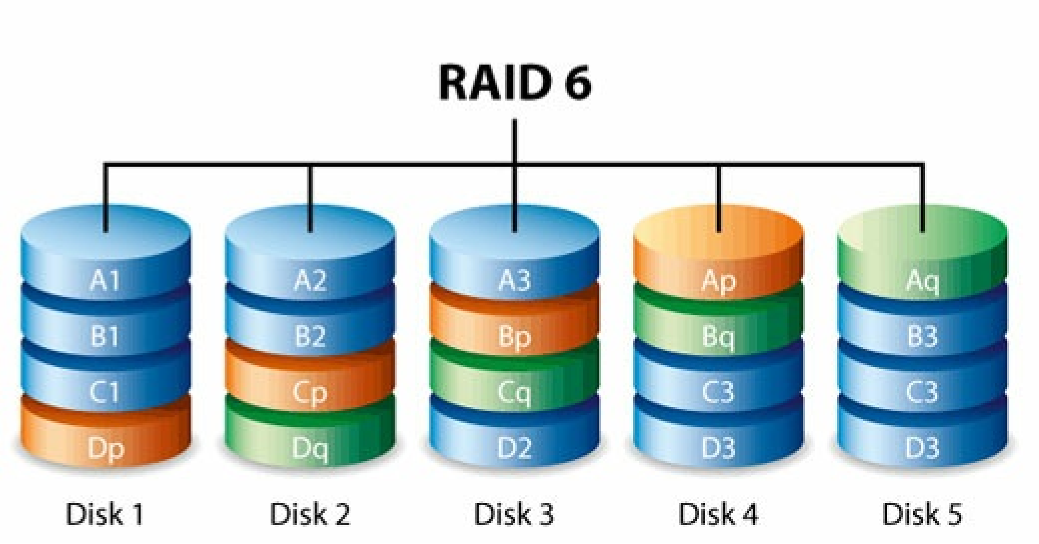
RAID 5 offers performance that can approach RAID 0. The strong advantage that RAID 5 gives you is data protection. Additionally, you still have approximately 75% of the storage capacity of a RAID 0 array (based upon total available hard drives and storage capacities). The equation for determining the storage is:

(The size of the hard drive with the smallest capacity in the array)*(Total hard drives-1).

Example 1: An array is assigned five 3TB hard drives for a total of 15TB. The equation is: 3TB * 4= 12TB.

Example 2: An array is assigned three 2TB hard drives and one 3TB hard drive for a total of 9TB. The equation is: 2TB * 3= 6TB.

# RAID 6

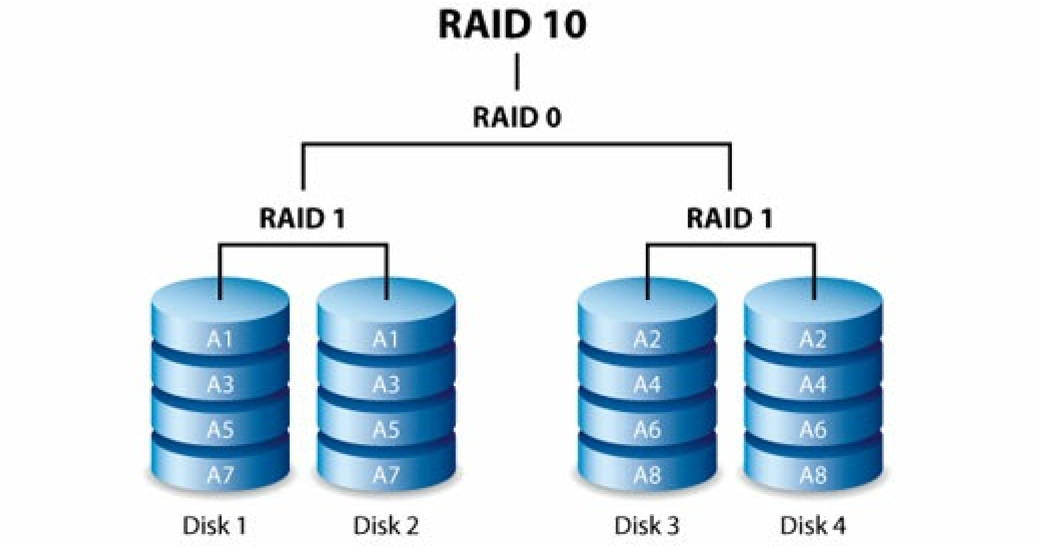


RAID 6 writes data across all hard drives in the volume and two parity blocks for each data block. If one hard drive fails, the data can be rebuilt onto a replacement hard drive. With two parity blocks per data block, RAID 6 supports up to two hard drive failures with no data loss.

RAID 6 synchronizing from a failed hard drive is slower than RAID 5 due to the use of double parity. However, it is far less critical due to double-disk security. A minimum of four hard drives is required to create a RAID 6 volume.

RAID 6 offers very good data protection with a slight loss in performance compared to RAID 5.

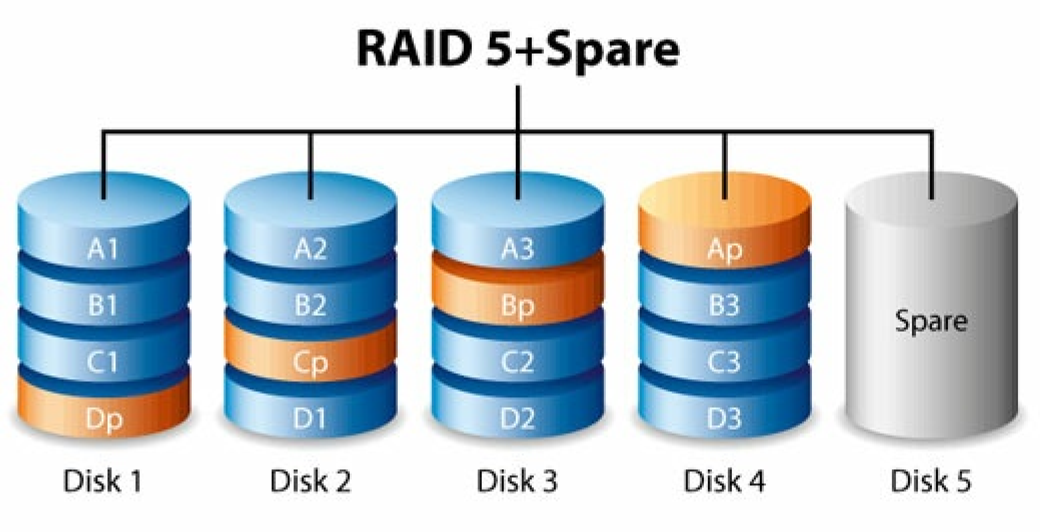
## RAID 10



RAID 10 combines the protection of RAID 1 with the performance of RAID 0. Consider a volume with four hard drives. RAID 10 creates two RAID 1 segments, and then combines them into a RAID 0 stripe. With eight hard drives, the RAID 0 stripe will include four RAID 1 segments. Such configurations offer exceptional data protection, allowing for two hard drives to fail across two RAID 1 segments. Additionally, RAID 10 writes data at the file level and, due to the RAID 0 stripe, gives users higher performance when managing greater amounts of smaller files. This means a more generous input/output per second for data (IOPS).

RAID 10 is a great choice for database managers that need to read and write many small files across the volume. The impressive IOPS and data protection offered by RAID 10 gives database managers impressive reliability both in keeping files safe and rapid access.

## RAID 1+Spare(s), RAID 5+Spare(s), RAID 6+Spare, and RAID 10+Spare



| RAID Mode | Maximum Spare Drives |
|---|---|
| RAID 1 | 5 |
| RAID 10 | 4 |
| RAID 5 | 5 |
| RAID 6 | 4 |

- RAID 1: The same data is written across all hard drives in the volume, protecting data against the loss of one hard drive.
- RAID 10: Comprised of two or more RAID 1 segments, RAID 10 allows for single-disk failure in each segment.
- RAID 5 and RAID 6: Data is written in parity blocks on all hard drives in the volume. Files are protected against single- or double-disk failure, respectively.

A RAID+Spare volume gives you a "hot-spare" that is ready to synchronize data immediately should a hard drive fail. If a hard drive fails, the data starts to synchronize with the spare. The clear advantage for a RAID volume with a spare is that you do not have to wait for a replacement hard drive.

When the failed hard drive is replaced, the replacement hard drive becomes the new hot spare.

To create a volume with a spare hard drive, you must choose **Custom** in the *New network volume* wizard. Selecting **Quick setup** in the *New network volume wizard* will automatically configure a volume with SimplyRAID and single disk protection. SimplyRAID optimizes disk space across all hard drives to maximize data storage. Therefore, it does not include the option to add a spare drive. See New network volume wizard for instructions on creating volumes.

i **Important info**: For RAID+Spare volumes, data remains intact when a single disk fails and the spare begins synchronizing automatically. If a second disk in the volume fails before synchronization is complete, all data in the volume will be lost. RAID 6 allows for two disks to fail.

# New network volume wizard

Build one or more volumes using the *New network volume* wizard. You can select:

- **Quick setup**: Skip multiple configuration steps with NAS OS SimplyRAID, Seagate's smart RAID. SimplyRAID will review the amount of hard drives in the volume and the total storage to optimize data capacity and protect your data. To provide the most storage space for your data, *Quick setup* configures a SimplyRAID volume with single-disk security. For additional protection, SimplyRAID is also available with double-disk security when selecting *Custom*.
- **Custom**: Configure a volume using NAS OS SimplyRAID or standard RAID models. *Custom* offers a wide range of RAID configurations:

- SimplyRAID with single-disk protection (minimum of two hard drives for data protection)
- SimplyRAID Dual with double-disk protection (minimum of three hard drives) JBOD
- RAID 0 (minimum of two hard drives)
- RAID 1 (minimum of two hard drives for data protection)
- RAID 1+Spare (minimum of three hard drives). Additional steps required for the spare. RAID 5
- (minimum of three hard drives)
- RAID 5+Spare (minimum of four hard drives) Additional steps required for the spare. RAID
- 6 (minimum of four hard drives)
- RAID 6+Spare (minimum of five hard drives). Additional steps required for the spare. RAID
- 10 (minimum of four hard drives)
- RAID 10+Spare (minimum of five hard drives). Additional steps required for the spare.

**SimplyRAID and spare disks**: NAS OS optimizes storage capacity using all the hard drives in a SimplyRAID volume. Therefore, a spare hard drive is not supported with SimplyRAID.

ℹ **Important note on SimplyRAID Dual:**

- You must use **Custom** to configure SimplyRAID Dual.
- The *New network volume* wizard does not offer a migration path from SimplyRAID to SimplyRAID Dual.

ℹ **Important info regarding NAS backup :** As further protection against the loss of a hard drive or secondary points of failure (e.g. hardware, network, etc.), it is recommended that all users back up data to a DAS or another NAS. See Backup Manager for details.

ℹ **Important info on creating a single-disk volume :** Single-disk volumes can be created with expansion in mind. For example, you can launch the *New network volume* wizard to create a single-disk volume using SimplyRAID, JBOD, or RAID 1. Though the volume will not provide data protection in a single-disk configuration, it is prepared for expansion when you add one or more hard drives. If you intend to expand the volume to four or more hard drives, consider using SimplyRAID since RAID 1 cannot reach beyond three hard drives.

# New network volume wizard steps

Consider the following when creating a new volume:

- **Volume names**: The default names for newly created volumes are Volume 1, Volume 2, etc. For instructions on how to change the name of the volume, see Storage. An encrypted volume retains the default name and it cannot be changed.
- **Planning for volume expansion**:
  - Apart from RAID 0 and RAID 10, RAID volumes can be expanded with new hard drives. However, it is

not possible to add new hard drives with inferior capacities. For example, a RAID 5 or SimplyRAID volume with three 2TB hard drives supports the addition of a fourth hard drive that is 2TB or higher.

## Quick setup

1. Go to **Device Manager** > **Storage** > **Storage Overview**.
2. NAS OS detects new hard drives in the enclosure. Choose **Manage** to launch the New network volume wizard.
3. In the *Select disks* window, hard drives with white checkboxes can be selected for the new volume. An existing volume is using hard drives with grey checkboxes. Select the white checkbox under the hard drives you want to use for the new volume and choose **Next**.

   > **Important :** All data on the selected hard drives is deleted to create the RAID volume.

4. Select **Quick setup** to create a SimplyRAID volume. With two or more hard drives, SimplyRAID creates a RAID volume using single security. If you choose *Custom*, refer to the instructions below.
5. Choose **Next**.
6. Review the summary window then choose **Finish**. A popup window cautions you that all data on the selected hard drives will be deleted to create the volume. Select **Yes** to build the SimplyRAID volume.

You can start using the volume immediately. See Shares for instructions on how to create new shares on the volume to store and share data.

## Custom

Your options to select the level of RAID are predicated upon the number of hard drives in the array. For example, a three-disk configuration allows you to select from SimplyRAID, JBOD, RAID 0, RAID 1, and RAID 5. A four-disk configuration offers SimplyRAID, JBOD, RAID 0, RAID 5, RAID 6, and RAID 10.

### Adding a spare

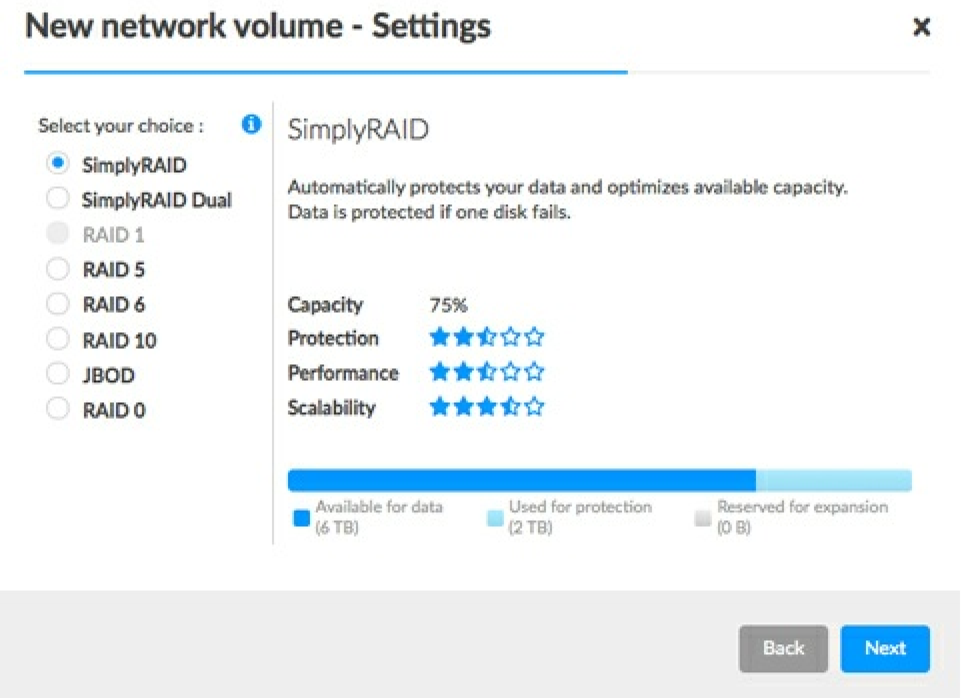
If you intend to create a volume with a spare hard drive, you must leave at least one hard drive free. For example, a four-disk RAID 6+Spare would require that you create the RAID 6 volume with the first four hard drives before adding the fifth hard drive as the spare. See the next section for details on adding the spare.

### Build a RAID volume:

1. Go to **Device Manager** > **Storage** > **Storage Overview**.
2. NAS OS detects new hard drives in the enclosure. Choose **Manage** to launch the New network volume wizard.
3. In the *Select disks* window, hard drives with white checkboxes can be selected for the new volume. An existing volume is using hard drives with grey checkboxes. Select the white checkboxes under the hard drives you want to use for the new volume and choose **Next**.

> **Important info:** All data on the selected hard drives is deleted to create the RAID volume.

4. Select **Custom** and choose **Next**.
5. The RAID selection window helps you choose the optimal configuration for your environment: Select a
   - RAID mode's radio button to view an explanation of its strengths and weaknesses.



New network volume - Settings ✕

Select your choice :

● SimplyRAID
○ SimplyRAID Dual
○ RAID 1
○ RAID 5
○ RAID 6
○ RAID 10
○ JBOD
○ RAID 0

SimplyRAID

Automatically protects your data and optimizes available capacity.
Data is protected if one disk fails.

| | |
|---|---|
| Capacity | 75% |
| Protection | ★★⯪☆☆ |
| Performance | ★★⯪☆☆ |
| Scalability | ★★★⯪☆ |

■ Available for data (6 TB)
■ Used for protection (2 TB)
■ Reserved for expansion (0 B)

   - Use the cursor to choose the i tooltip to see a graphic summary of the strengths and weaknesses of each RAID level.
6. Select your level of RAID and choose **Next**.
7. Choose *No encryption* to move to the summary page or, *Encrypt the volume*. When choosing encryption, you have two options to unlock the volume: password only or, a password plus a USB device. Enter the password and/or insert a USB device into one of the NAS's USB ports. Choose **Next**.

> **Important info:** An encrypted volume can experience a reduction in performance.

8. Choose **Next**.
9. Review the summary window then choose **Finish**. A popup window cautions you that all data on the selected hard drives will be deleted to create the volume. Select **Yes** to build the volume.

## Custom+Spare

A spare drive can be added to RAID 1, RAID 5, RAID 6, and RAID 10 volumes. Before adding a spare hard drive, you must follow the instructions above (Custom) to create the RAID volume. When creating the volume, leave a minimum of one hard drive free for the spare. For example, a four-disk RAID 6+spare would require that you create the RAID 6 volume with the first four hard drives. Once the RAID has been synchronized, review the steps in this section to add the fifth hard drive as the spare. A spare hard drive must have a capacity equal to or greater than the largest hard drive in the RAID volume.

1. On the Storage section at the lower left, choose the volume add a spare disk.

1. On the Storage section at the lower left, choose the volume add a spare disk.
2. Choose **Manage**.
3. Select **Add drive** and choose **Next**.
4. NAS OS detects hard drives in the enclosure that are not in use by other volumes. Check the box under the hard drive to use as the spare. You can add more than one spare.
5. Choose **Next**.
6. Select **Custom** and choose **Next**.
7. Select **Add spare drives** and choose **Next**.
8. Review the summary and choose **Finish**. A popup window cautions you that all data on the selected hard drives will be deleted. Choose **Yes** to continue.

# Single-disk volume

NAS OS allows you to create a volume with only one hard drive and then expand as you add hard drives to the enclosure. A volume with a single hard drive can be configured for SimplyRAID (single-disk security only), JBOD, or RAID 1. Each level of RAID has its own advantages, as described in RAID Modes.

## SimplyRAID

1. Go to **Storage > Storage Overview**.
2. Choose **Manage** to launch the *New network volume* wizard.
3. In the *Select disks* window, hard drives with white checkboxes can be selected for a new volume. Hard drives with grey checkboxes are being used by volumes and cannot be selected. Select the box under a free hard drive for the new volume and choose **Next**.

   > **Important :** All data on the selected hard drive is deleted to create the RAID volume.

4. Select **Quick setup** and then choose **Next**.
5. Choose *No encryption* to move to the summary page or, *Encrypt the volume*. When choosing encryption, you have two options to unlock the volume: password only or, a password plus a USB device. Enter the password and/or insert a USB device into one of the NAS's USB ports. Choose **Next**.
6. Review the summary window and then choose **Finish**. A popup window cautions you that all data on the selected hard drive will be deleted to create the volume. Select **Yes** to build the SimplyRAID volume.

   > **Important :** A volume with only one hard drive cannot protect data. Consider adding new hard drives as soon as possible.

To expand a single-disk volume, see Single-disk and unprotected volumes: expansion.

## RAID 1 or JBOD

1. Go to **Storage > Storage Overview**.
2. NAS OS detects new hard drives in the enclosure. Choose **Manage** to launch the *New network volume* wizard.
3. In the *Select disks* window, hard drives with white checkboxes can be selected for a new volume. Hard

drives with grey checkboxes are being used by volumes and cannot be selected. Select the box under a free hard drive for the new volume and choose **Next**.

> **Important :** All data on the selected hard drive will be deleted to create the RAID volume.

4. Select **Custom** and then choose **Next**.
5. Select JBOD or RAID 1 and then choose **Next**.
6. Choose *No encryption* to move to the summary page or, *Encrypt the volume*. When choosing encryption, you have two options to unlock the volume: password only or, a password plus a USB device. Enter the password and/or insert a USB device into one of the NAS's USB ports. Choose **Next**.
7. Review the summary window and then choose **Finish**. A popup window cautions you that all data on the selected hard drive will be deleted to create the volume. Select **Yes** to build the SimplyRAID volume.

> **Important :** A volume with only one hard drive cannot protect data. Consider adding new hard drives as soon as possible.

To expand a single-disk volume, see Single-disk and unprotected volumes: expansion.

## Multiple volumes

You can create multiple volumes on one NAS OS device. While this manual cannot list every option for multiple volumes, you can use the steps below as a guide.

This example demonstrates the creation of two volumes using RAID 5 (performance and protection) and SimplyRAID (protection).

### Create the first volume (RAID 5):

1. Go to **Storage > Storage Overview**.
2. NAS OS detects new hard drives in the enclosure. Choose **Manage** to launch the New network volume wizard.
3. In the Select disks window, hard drives with white checkboxes can be selected for a new volume. Hard drives with grey checkboxes are being used by volumes and cannot be selected. Select the boxes under the hard drives for the new volume and choose **Next**. Important: All data on the hard drives that you select is deleted to create the RAID volume.
4. Select **Custom** and then choose **Next**.
5. Select your preferred level of RAID and choose **Next**. In this example, it is RAID 5.
6. Choose *No encryption* to move to the summary page or, Encrypt the volume. When choosing encryption, you have two options to unlock the volume: password only or, a password plus a USB device. Enter the password and/or insert a USB device into one of the NAS's USB ports.Choose **Next**.
7. Review the summary window then choose **Finish**. A popup window cautions you that all data on the selected hard drives will be deleted. Choose **Yes** to build the volume.

### Create the second volume (SimplyRAID):

1. Go to **Storage > Storage Overview**.
2. NAS OS detects new hard drives in the enclosure. Choose **Manage** to launch the *New network volume* wizard.
3. In the Select disks window, hard drives with white checkboxes can be selected for a new volume. Hard drives with grey checkboxes are being used by volumes and cannot be selected. Select the boxes under the hard drives for the new volume and choose **Next**. Important: All data on the hard drives that you select is deleted to create the RAID volume.
4. Select **Quick setup** to create a SimplyRAID volume. With two or more hard drives, SimplyRAID creates a RAID volume using single security. Choose **Next**.
5. Choose No encryption to move to the summary page or, Encrypt the volume. When choosing encryption, you have two options to unlock the volume: password only or, a password plus a USB device. Enter the password and/or insert a USB device into one of the NAS's USB ports. Choose **Next**.
6. Review the summary window then choose **Finish**. A popup window cautions you that all data on the selected disks will be deleted to create the volume. Select **Yes** to build the SimplyRAID volume.

# Synchronizing times

Synchronizing a volume can take from five minutes to many hours, depending on:

- The level of RAID
- The capacities of the hard drives in the volume
- The NAS's available resources (concurrent tasks such as backups or downloads will slow synchronizing)

For example, creating an unprotected RAID volume takes less than five minutes while RAID 6 with large capacity hard drives can run for many days. You can access the volume while it is synchronizing.

It is important to note that during synchronization:

- NAS performance is reduced due to a heavier demand upon the CPU RAID
- protection is not available until the synchronization is complete
- Older hard drives can fail, especially models that are not constructed for NAS

# Single-disk and unprotected volumes: Expansion

**Important info on NAS backup**: It is recommended that all users back up data to DAS or another NAS as further protection against the loss of a hard drive and secondary points of failure (e.g. hardware, network, etc.). See Backup Manager for details.

# Removing healthy hard drives from an unprotected volume

An unprotected volume can be:

- SimplyRAID single-disk
- RAID 1 single-disk
- JBOD
- RAID 0

**Removing a healthy hard drive from an unprotected volume while the NAS OS device is powered on will delete all of the volume's data.** While removing healthy hard drives is not recommended, you can avoid losing data by shutting down the NAS first. Return the hard drives to their proper bays before powering on the NAS.

Additionally, powering on the NAS with a missing hard drive in an unprotected volume will break its RAID and all data will be lost.

# Volume expansion

Apart from RAID 0, RAID volumes can be expanded with new hard drives. However, it is not possible to add new hard drives with inferior capacities. For example, a RAID 5 or SimplyRAID volume with three 2TB disks supports the addition of a fourth hard drive that is 2TB or higher.

Choose your RAID and follow the instructions on expanding the volume. RAID 0 does not support volume expansion.

**Encrypted volume**: Unlock the volume before following the steps below.

## SimplyRAID

1. On the Storage section at the lower left, choose the SimplyRAID volume you want to expand.
2. Choose **Manage**.
3. Choose **Add drive** and **Next**.
4. In the *Select disks* window, hard drives with white checkboxes can be selected for the existing volume. Hard drives with grey checkboxes are being used by volumes and cannot be selected. Select the boxes under the hard drives that you want to add to the existing volume and choose **Next**.

   > **i** **Important :** All data on the selected hard drives is deleted.

5. Review the summary and then choose **Finish**. A popup window cautions you that all data on the selected hard drives will be deleted. Choose **Yes** to continue.

You can use the volume during the RAID synchronization.

## RAID 1

When adding a hard drive to a RAID 1 volume, you can:

- Increase security to protect data.
- Change the RAID to SimplyRAID.

> ℹ **Important:** Data stored on the volume is deleted when changing RAID levels.

1. On the Storage section at the lower left, choose the RAID 1 volume you want to expand.
2. Choose **Manage**.
3. Choose **Add drive** and then **Next**.
4. In the *Select disks* window, hard drives with white checkboxes can be selected for the existing volume. Hard drives with grey checkboxes are being used by volumes and cannot be selected. Select the boxes under the hard drives that you want to add to the existing volume and choose **Next**.

   > ℹ **Important :** All data on the selected hard drives is deleted.

5. Select one of the following:
   - **Increase security** to enable protection on the RAID 1 volume.
   - **Custom** to change the RAID to SimplyRAID.

     > ℹ **Important :** Data stored on the volume is deleted when changing RAID levels.

6. Choose **Next**.
7. Review the summary page and then choose **Finish**. A popup window cautions you that all data on the selected hard drives will be deleted. Choose **Yes** to continue.

You can use the volume during the RAID synchronization.

## JBOD

1. On the Storage section at the lower left, choose the JBOD volume you want to expand.
2. Choose **Manage**.
3. Choose **Add drive** and **Next**.
4. In the *Select disks* window, hard drives with white checkboxes can be selected for the existing volume. Hard drives with grey checkboxes are being used by volumes and cannot be selected. Select the boxes under the hard drives that you want to add to the existing volume and choose **Next**.

   > ℹ **Important :** All data on the selected hard drives is deleted.

5. Review the summary page and then choose **Finish**. A popup window cautions you that all data on the selected hard drives will be deleted. Choose **Yes** to continue.

# Protected volumes: Expansion and hard drive replacement

# Removing healthy hard drives from a protected volume

A protected volume can be:

- SimplyRAID (single-disk or double-disk security)
- RAID 1/RAID 1+Spare (two hard drives minimum)
- RAID 5/RAID 5+Spare
- RAID 6/RAID 6+Spare
- RAID 10/RAID 10+Spare

**Removing a healthy hard drive from a protected volume while the NAS OS device is powered on will render the volume unprotected. If the volume has double-disk security, removing two healthy hard drives while the device is powered on will render the volume unprotected**. While removing healthy hard drives is not recommended, you can avoid breaking the RAID by shutting down the NAS first. Return the hard drives to their proper slots before powering on the NAS.

If a healthy hard drive has been removed while the NAS is powered on, you can reinsert it into its slot. NAS OS synchronizes the RAID following the reinsertion of the hard drive. It is important to note that during synchronization:

- NAS performance is reduced due to a heavier demand upon the CPU
- RAID protection is not available until the synchronization is complete
- Older hard drives can fail, especially models that are not constructed for NAS

i **Important info on NAS backup**: It is recommended that all users back up data to DAS or another NAS as further protection against the loss of a hard drive and secondary points of failure (e.g. hardware, network, etc.). See Backup Manager for details.

# Hard drive expansion and replacement

Apart from RAID 10, protected RAID volumes can be expanded with new hard drives. However, it is not possible to add new hard drives with inferior capacities. For example, a RAID 5 or SimplyRAID volume with three 2TB hard drives supports the addition of a fourth hard drive that is 2TB or higher.

## Expand a volume's storage capacity: add hard drives to the enclosure

The instructions below pertain to storage expansion in a NAS OS device with available or empty drive slots. If you are exchanging an existing hard drive in your enclosure for a hard drive of greater capacity or, repairing a failed hard drive, follow the instructions in Repair a failed hard drive or expand storage capacity.

NAS OS gives you the freedom to configure RAID volumes for your network. While it is not possible to list every option for expansion, review the examples below and apply them to your NAS OS device.

> **Important info on adding hard drives**: Make certain to add a new hard drive without data. While data on the NAS OS volume is safe, performing the steps below will **delete files stored on the new hard drive you are adding to the volume**.

**Encrypted volume**: Unlock the volume before following the steps below.

## SimplyRAID

1. Insert one or more hard drives into available bays on your NAS. Review your NAS's hardware user manual for instructions.
2. On the Storage section at the lower left, choose the SimplyRAID volume you want to expand.
3. Choose **Manage**.
4. Choose **Add drive** and then **Next**.
5. In the *Select disks* window, hard drives with white checkboxes can be selected to expand the volume. Hard drives with grey checkboxes are being used by volumes and cannot be selected. Check the boxes under the hard drives you want to use and choose **Next**.

   > **Important :** All data on the selected hard drives is deleted when expanding the volume.

6. Review the summary and choose **Finish**. A popup window cautions you that all data on the selected disks will be deleted. Choose **Yes** to continue.

You can use the volume while it synchronizes the data. NAS performance can be affected during synchronization

## Custom RAID: RAID 1, RAID 5, and RAID 6

1. Insert one or more hard drives into available hard drive slots on your NAS. Review your NAS's hardware user manual for instructions.
2. On the Storage section at the lower left, choose the volume you want to expand.
3. Choose **Manage**.
4. Choose **Add drive** and **Next**.
5. In the *Select disks* window, hard drives with white checkboxes can be selected to expand the volume. Hard drives with grey checkboxes are being used by volumes and cannot be selected. Check the boxes under the hard drives you want to use and choose **Next**.

   > **Important:** All data on the selected hard drives is deleted when expanding the volume.

6. You can select:
   - **Expand storage capacity** to add the new hard drives to the RAID. Data is synchronized with the new

hard drives.

- **Increase security** to migrate the RAID to another level. For example, upgrade the level from RAID 1 to RAID 5/6 or, RAID 5 to RAID 6. Data is synchronized to the new hard drives.
- **Custom** to create a new RAID volume. All data on the existing volume is deleted to create the new RAID volume.

7. Review the summary and choose **Finish**. A popup window cautions you that all data on the selected disks will be deleted. Choose **Yes** to continue.

The total capacity of the volume will be available once the synchronization is complete.

# Repair a failed hard drive or expand storage capacity

Follow the instructions below to:

- Replace a failed hard drive.
- Expand a volume's total storage capacity by replacing a hard drive with a larger capacity hard drive.

**Important info**: If a hard drive that you purchased from Seagate fails, contact Seagate customer support.

## Hot-swapping

When replacing or expanding hard drives in a protected RAID volume:

- Perform the operation while the NAS is powered on, also known as hot swapping.
- Use hard drives that do not contain important data, also known as clean hard drives.

If a volume is protected, you can remove an existing hard drive and replace it with a new hard drive while the product is turned on. This process is referred to as hot swapping. It is highly recommended that you hot swap when replacing or expanding hard drives.

**Important info**:

- It is not possible to replace existing hard disks with lower capacity hard disks.
- All data stored on the replacement hard drive will be deleted.

## Hard drive replacement and expansion

> **Important info on expanding storage capacity on more than one hard drive:** A volume can be expanded one hard drive at a time. Follow the steps below for each hard drive that you add to the volume. Performing the steps on multiple hard drives at the same time will break the RAID.

**Encrypted volume**: Unlock the volume before following the steps below.

## SimplyRAID

1. Remove the hard drive that you want to replace.
2. Go to **Device Manager > Storage Overview**.

   > **Important:** Do not choose **Manage** on the Storage Overview page.

3. On the Storage Overview page, choose the volume that you want to expand or repair with the new hard drive. If you are replacing a failed or missing disk, the NAS's image shows the missing hard drive.
4. Insert the replacement hard drive into the enclosure per the instructions provided in the NAS's hardware user manual.
5. Choose **Manage** on the volume's storage page.
6. Select **Repair** and choose **Next**.
7. In the *Select disks* window, hard drives with white checkboxes can be selected to expand the volume. Hard drives with grey checkboxes are being used by existing volumes and cannot be selected. Select the box under the hard drive that you want to use to expand or repair the volume and choose **Next.**

   > **Important :** All data on the selected hard drive is deleted when repairing or expanding the volume.

8. Review the summary and choose **Finish**. A popup window cautions you that all data on the selected hard drive will be deleted. Choose **Yes** to continue.

You can access files stored on the volume while it synchronizes data. Consider the following:

- The time to synchronize depends upon the amount of hard drives in the volume and its total capacity. NAS performance can be reduced due to a heavier demand upon the CPU.
- RAID protection is not available until the synchronization is complete.
- Older hard drives can fail, especially models that are not constructed for NAS.
- The volume's storage page will update its capacity following the synchronization.

## Custom: RAID 1, RAID 5, and RAID 6

Use the instructions below when swapping an existing hard disk in your custom RAID for a failed or higher capacity hard drive.

ℹ **Important info on expanding storage capacity on more than one hard drive**: A volume can be expanded one hard drive at a time. Follow the steps below for each hard drive that you add to the volume. Performing the steps on multiple hard drives at the same time will break the RAID.

ℹ **Important info on Custom RAID (1, 5, and 6) expansion and synchronizing**: The volume must synchronize twice when expanding capacity on a Custom RAID volume. SimplyRAID expansion requires a single synchronization.

**Encrypted volume**: Unlock the volume before following the steps below.

1. Remove the hard drive that you want to replace according to the instructions on the NAS's hardware user manual.
2. On the Storage section at the lower left, choose the volume you want to repair.
3. If you are replacing a failed or missing disk, the NAS's image shows the missing hard drive. Insert the replacement hard drive into the enclosure per the instructions provided in the NAS's hardware user manual.
4. Choose **Manage**.
5. Select **Repair** and choose **Next**.
6. In the *Select disks* window, hard drives with white checkboxes can be selected to expand the volume. Hard drives with grey checkboxes are being used by existing volumes and cannot be selected. Select the box under the hard drive that you want to use to expand or repair the volume and choose **Next**.

   ℹ **Important :** All data on the selected hard drive is deleted when repairing or expanding the volume.

7. Review the summary and choose **Finish**. A popup window cautions you that all data on the selected hard drive will be deleted. Choose **Yes** to continue.
8. Depending upon the amount of hard drives and the total capacity, the synchronization can run for a few hours to several days. The synchronization is complete once the Status is **OK**. If you inserted a larger capacity hard drive, the volume's storage page does not reflect the additional storage. Continue with the next steps to optimize the additional capacity.
9. On the Storage Overview page, click on the volume. The volume's storage page will load in the browser.
10. Choose **Manage**.
11. Select **Optimize storage capacity** and choose **Next**.
12. Choose **Finish**.
13. The volume will synchronize once more to update the storage capacity.

You can access files stored on your NAS during the RAID synchronization.

## No replacement disk: reset the volume's RAID

If a hard drive in a protected volume fails and you do not have a replacement hard drive, you can reset the RAID using the *New network volume* wizard. Resetting the RAID deletes all data stored on the volume. Make certain to back up your files before you reset the RAID.

To reset the RAID:

1. **On the Storage section at the lower left, choose the volume you want to reset.**
2. Choose **Manage**.
3. Choose **Delete** and select **Yes** at the popup window.
4. Go to the New network volume wizard for instructions on how to create a new RAID volume.

# Advanced Storage: Direct-Attached Storage and iSCSI

You can use your NAS OS device to share direct-attached storage (DAS) on the network and to create iSCSI volumes. For details and instructions, see:

- NAS Ports and Direct-Attached Storage
- iSCSI

# NAS ports and direct-attached storage

Use the USB and, if applicable, eSATA ports on your NAS OS device to connect external storage and compatible peripherals.

## Direct-attached storage (DAS)

### Connect

A DAS connected to the NAS OS device via USB is listed at **Device Manager > Storage Overview**. If you do not see your DAS, confirm that it has been formatted using one of the following file systems:

- FAT32
- NTFS
- HFS+
- EXT2, EXT3, EXT4
- XFS

Unlike volumes created within NAS OS, the name of the DAS cannot be changed on its storage page.

### DAS share

By default, a DAS becomes a public share when it is connected to the NAS OS device.

You can change the DAS from a public share to a private share:

1. Choose **Shares**.
2. Pass the cursor to the far right of the DAS share's row to make the **Edit** pull-down menu visible.
3. Choose **Change to private share**.

4. Configure access to the share by following the instructions in Shares.

## Disconnect

To avoid damaging your DAS's file system, follow the instructions below to properly disconnect the device from the NAS OS device.

1. On the Storage section at the lower left, choose the volume you want to eject.
2. Choose **Eject**.
3. Disconnect the DAS.

## Ingest or back up DAS content

You can copy content on a connected DAS using:

- **Filebrowser ingest**. Use the Filebrowser to copy data from your USB storage to the NAS. Ingest is a good option when copying select files or images. For example, ingest images from a camera. See Filebrowser.
- **Backup Manager backup**. Use Backup Manager to back up all or select files stored on your USB storage. Backup Manager is a good option for large and recurring backups. See Backup Manager.

# Multimedia indexing

You can take an inventory of available multimedia files on your NAS and all connected DAS. See Media Server for details.

# USB printer

Your NAS OS device features a printer server service. See Services for details.

# iSCSI

iSCSI (Internet Small Computer System Interface) provides local storage performance for network shares similar to that of a traditional direct attached storage device (DAS). A DAS can be an external hard drive such as a disk that connects via USB. NAS OS can reserve all or part of a volume as an iSCSI volume for a computer to use via the network. The computer that connects to the iSCSI volume is called the *initiator*. The iSCSI volume is called the *target*. When the initiator connects to the target, the computer reads and writes to the iSCSI volume the same way it would access a DAS.

iSCSI works on top of the Transport Control Protocol (TCP) and allows SCSI commands to be sent along a local area networks (LAN), wide area network (WAN) or the Internet. It transports block-level data between an iSCSI initiator (client computer) and an iSCSI target (storage device). The iSCSI protocol is made of SCSI commands and, to send them on a network, assembles the data in packets.

Since it accesses data at the block level, iSCSI can offer enhanced performance for your NAS. Further, iSCSI writes data directly to the volume rather than at the file level placing a lower demand upon the NAS OS device. Managing IP and networking protocols such as AFP and SMB places a burden upon the processor.

Review the list below to determine the capacity you can assign to iSCSI volumes:

- Seagate NAS: up to 8TB
- Seagate NAS Pro and rackmounts: up 16TB

Target volumes can be simple iSCSI volumes called *SimplyiSCSI*. Use SimplyiSCSI when creating an iSCSI target that does not require multiple LUNs, or logical unit numbers. A LUN is an allotment of virtual storage that can be created from the NAS OS device's pool of available space. It is highly recommended to create iSCSI targets on protected volumes, such as SimplyRAID or RAID 5.

NAS OS supports advanced iSCSI configurations that allow you to assign several LUNs to a single target. The iSCSI wizard guides you through the configuration to help create iSCSI volumes suitable for your working environment.

Additionally, you can boost iSCSI performance by creating the target on a RAID 5 volume and configuring the LAN ports as bonding. See Network for further information.

Once an iSCSI initiator has connected to an iSCSI target, the target volume must be formatted as would happen with standard DAS. An iSCSI volume cannot be accessed through the NAS OS Filebrowser.

**Note on Mac and Windows operating systems and iSCSI initiators:** Windows professional and business editions offer native support to act as iSCSI initiators. The Mac operatng system does not offer native support to act as an iSCSI initiator. However, third-party applications are available to add support for the Mac operating system.

## Setting up an iSCSI target

A volume must be available before using the iSCSI wizard. For instructions on how to create a volume, see Storage.

1. Go to **Device Manager** and click **iSCSI** on the lower left.
2. Click **Manage** to launch the iSCSI wizard.
3. Follow the iSCSI wizard to create one of the following:
   - SimplyiSCSI (simple iSCSI volume)
   - LUN (the virtual volume)
   - Target (what the Initiator connects to)

Review the descriptions below for further information regarding the iSCSI options.

## SimplyiSCSI

Create one LUN associated with one target and limited options.

1. Select SimplyiSCSI and click **Next**. Choose:
   - A name for the iSCSI volume.
   - Capacity. Use the slider or fill it in manually (GB).
   - Select **Thin provisioning** to allocate more space than the volume's current storage capacity. Use thin provisioning if you expect to add more storage to your device in the future. The new hard drive capacity can be integrated into the iSCSI volume once it is added to the enclosure.
   - To password protect your iSCSI volume, you can configure CHAP (Challenge Handshake Authentication Protocol). CHAP restricts iSCSI access to initiators that supply the correct account name and password for the target.
   - Select and configure Mutual CHAP to implement two-way authentication for both the initiator and target.
2. Complete the wizard to create the SimplyiSCSI volume.

The time to create the iSCSI volume depends upon its capacity.

## Create LUN

Create a new LUN that can be mapped to a target.

1. Choose **Create LUN**.
2. Choose how you want to create the LUN:
   - *New LUN* creates a new LUN.
   - *Import LUN* imports a LUN file from a share on the NAS OS device. The LUN must have been previously exported on the same NAS OS device.
   - *Clone LUN* clones an existing LUN on the NAS OS device.

Review the details for each type of LUN below.

## New LUN

1. Choose **New LUN** and click **Next**.
2. You can choose:
   - A name for the LUN.
   - Capacity. Use the slider to configure its capacity or fill it in manually (in GB).
   - Select **Thin provisioning** to allocate more space than the volume's current storage capacity. Use thin provisioning if you expect to add more storage to your device in the future. The new hard drive capacity can be integrated into the iSCSI volume once it is added to the enclosure.
3. Click **Next**
4. Choose the target you want to associate with the LUN., You can also leave the LUN empty by not associating it with a target. However, the LUN cannot be used until it is associated with a target. Click **Next**.
5. Review the summary and click **Finish**.

## Import LUN

### Exporting a LUN

Before importing a LUN, you must export an existing LUN on the NAS OS device. Follow the steps below to export a LUN:

1. Go to **Device Manager** and choose **iSCSI**. A table lists available iSCSI targets.
2. Click the **LUNs** tab.
3. Hover to the right of an existing LUN and click **Edit > Export**.
4. Browse and choose the share and folder to store the LUN file.
5. Choose a name for the .iscsi file and then click **Save**.

### Importing a LUN

A LUN can only be imported if it is stored on one of the NAS OS device's shares. See the instructions above for exporting an existing LUN to a share.

1. Go to **Device Manager** and then choose **iSCSI**.
2. Click **Manage** and then select **Create LUN**. Click **Next**.
3. Select **Import LUN** and then click **Next**.
4. Browse for the LUN file (.iscsi) and then click **Next**.
5. Choose a target to map the LUN and then click **Finish**.

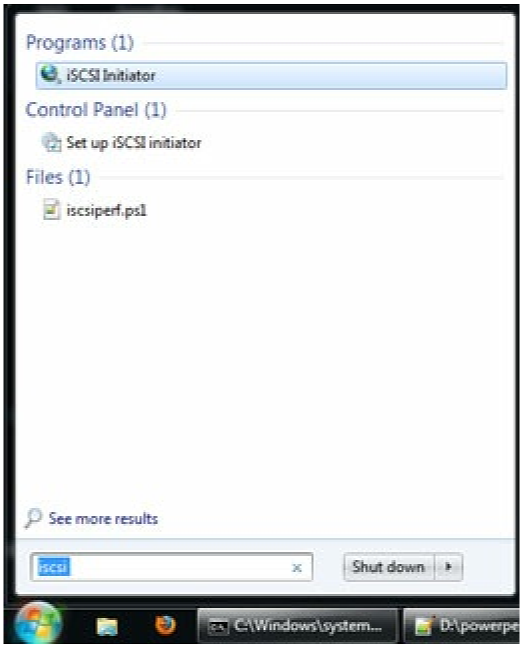
## Create a Target

1. Go to **Device Manager** and then choose **iSCSI**.
2. Click **Manage** and then select **Create a Target**. Click **Next**.
3. Review the options for your target. Only configure options that match your needs.
   - Name the iSCSI Target.
   - Password protect your iSCSI volume. Select CHAP (Challenge Handshake Authentication Protocol) to restrict iSCSI access to initiators that supply the correct account name and password. Select Mutual CHAP for two-way authentication between the initiator and target.
   - **Data digest**. Increases data integrity. When data digest is enabled, the system performs a checksum over each PDU's data part and verifies using the CRC32C algorithm.
   - **Header digest**. Increases data integrity. When header digest is enabled, the system performs a checksum over each iSCSI Protocol Data Unit's (PDU's) header part and verifies using the CRC32C algorithm.
   - **Multiple Sessions**. Select this option only if your iSCSI target will be managed within a SAN cluster environment. The SAN cluster allows multiple iSCSI initiators to access the iSCSI target at once.
   - **Authorized initiator**. Configure which iSCSI initiators are allowed to connect to this target.
4. Click **Next**.
5. Choose LUNs to map to this target and click **Next**.
6. Click **Finish**.

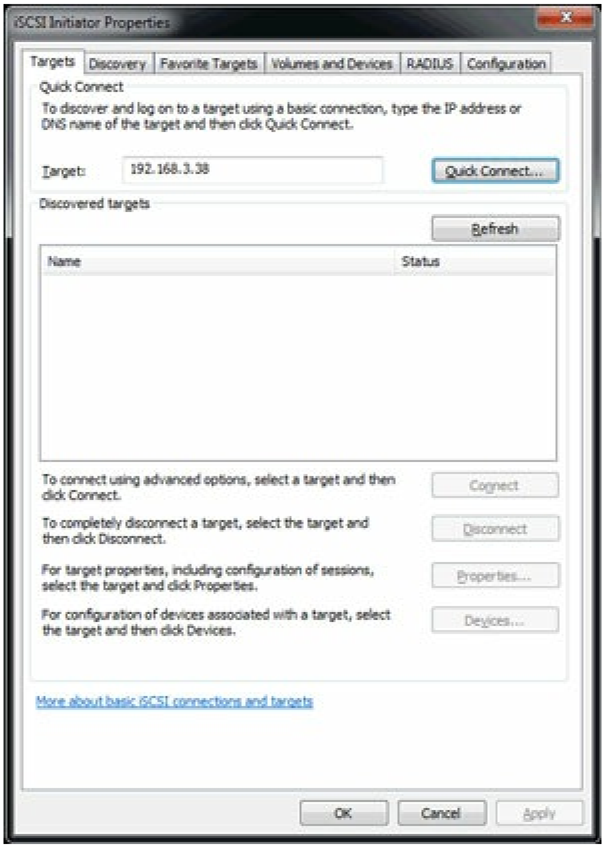
# iSCSI initiator: Example

The steps below demonstrate a single connection to an iSCSI target using Windows 7 as the initiator. For the example, a CHAP has been configured on the iSCSI target only. Configurations will vary but you can review the instructions below and make adjustments for your operating system and network.

1. Search for and launch **iSCSI Initiator** or equivalent.



2. Enter the network name or IP address of the server that hosts the iSCSI target. In this example, the NAS OS device.



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

Target: 192.168.3.38

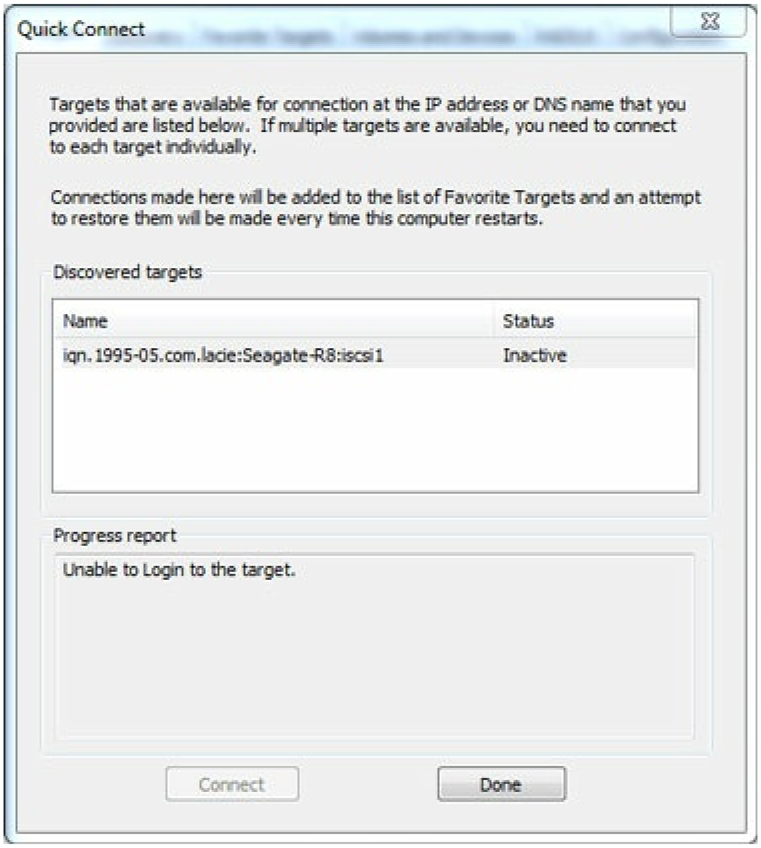
To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

3. Choose **Quick connect** or equivalent.
4. Without and with CHAP:
   - If the iSCSI target does not include a CHAP, the connection is immediate. If it is the first time that the iSCSI target has connected to an initiator, you are prompted to format the disk.
   - If the iSCSI target includes a CHAP, a prompt alerts you that a connection is not possible. Close the prompt.



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

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

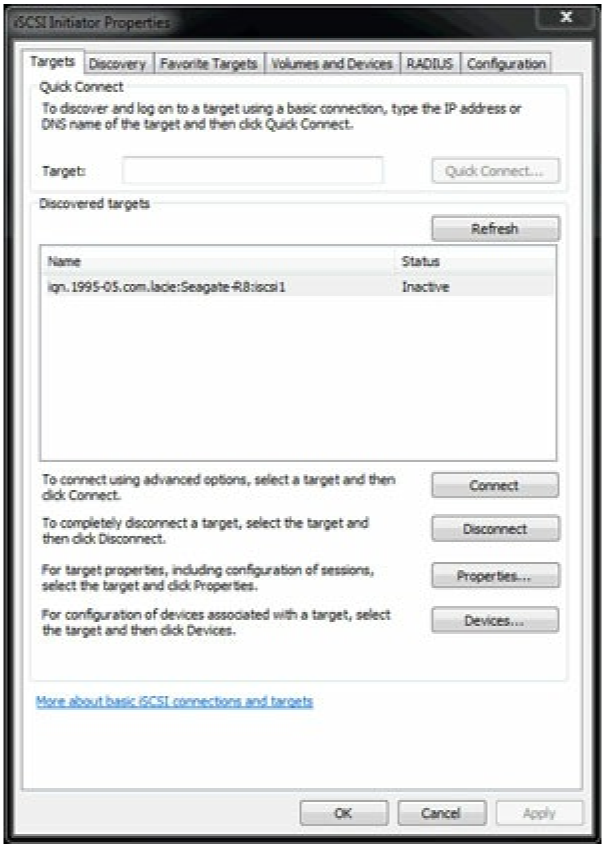
Discovered targets

| Name | Status |
|---|---|
| iqn.1995-05.com.lacie:Seagate-R8:iscsi1 | Inactive |

Progress report

Unable to Login to the target.

5. Select the NAS's iSCSI target in the list of discovered agents and choose **Connect**.



Quick Connect

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

Target:

Discovered targets

| Name | Status |
|---|---|
| iqn.1995-05.com.lacie:Seagate-R8:iscsi1 | Inactive |

To connect using advanced options, select a target and then click Connect.

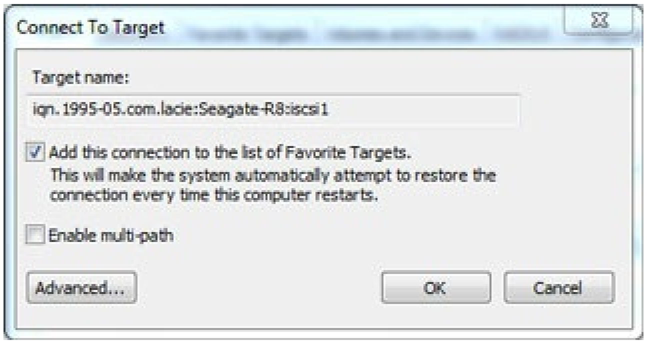
To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

More about basic iSCSI connections and targets

6. Choose **Advanced**.



Connect To Target

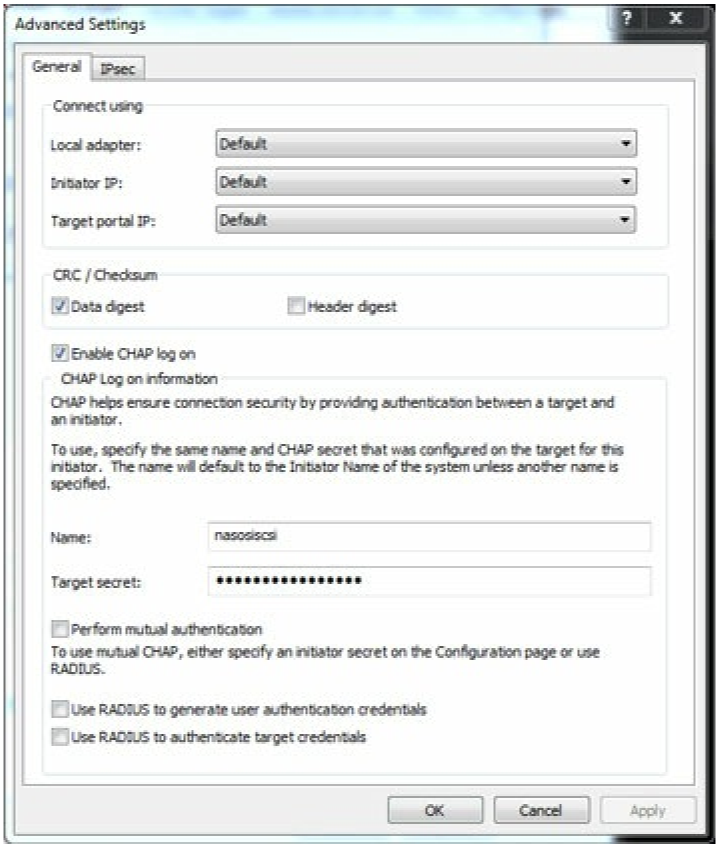
Target name:

iqn.1995-05.com.lacie:Seagate-R8:iscsi1

☑ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

□ Enable multi-path

7. Select **Enable CHAP log on** and enter the **Name** and **Target secret** (password) for the iSCSI target.



Advanced Settings

Connect using

Local adapter: Default

Initiator IP: Default

Target portal IP: Default

CRC / Checksum

☑ Data digest □ Header digest

☑ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: nasosiscsi

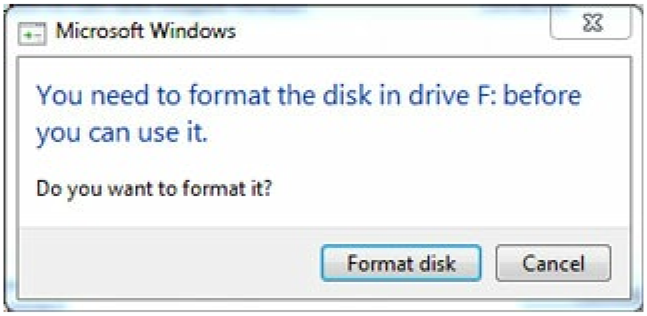
Target secret: ••••••••••••••••

□ Perform mutual authentication
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

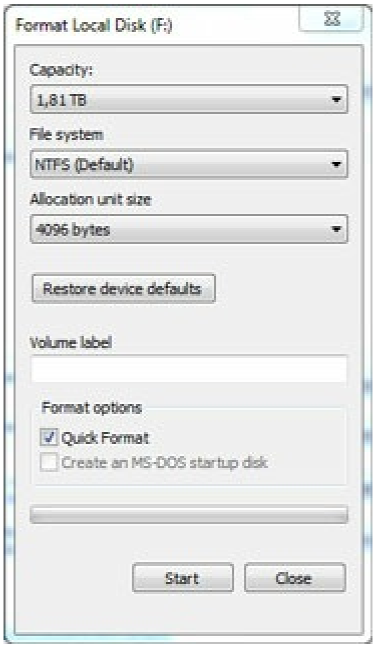
8. A window may appear prompting you to add the target to your favorites. Make your selection and exit.
9. If it is the first time that the iSCSI target has connected to an initiator, you are prompted to format the disk.



Microsoft Windows

You need to format the disk in drive F: before you can use it.

Do you want to format it?



Format Local Disk (F:)

Capacity: 1,81 TB

File system: NTFS (Default)

Allocation unit size: 4096 bytes

Volume label:

Format options

☑ Quick Format

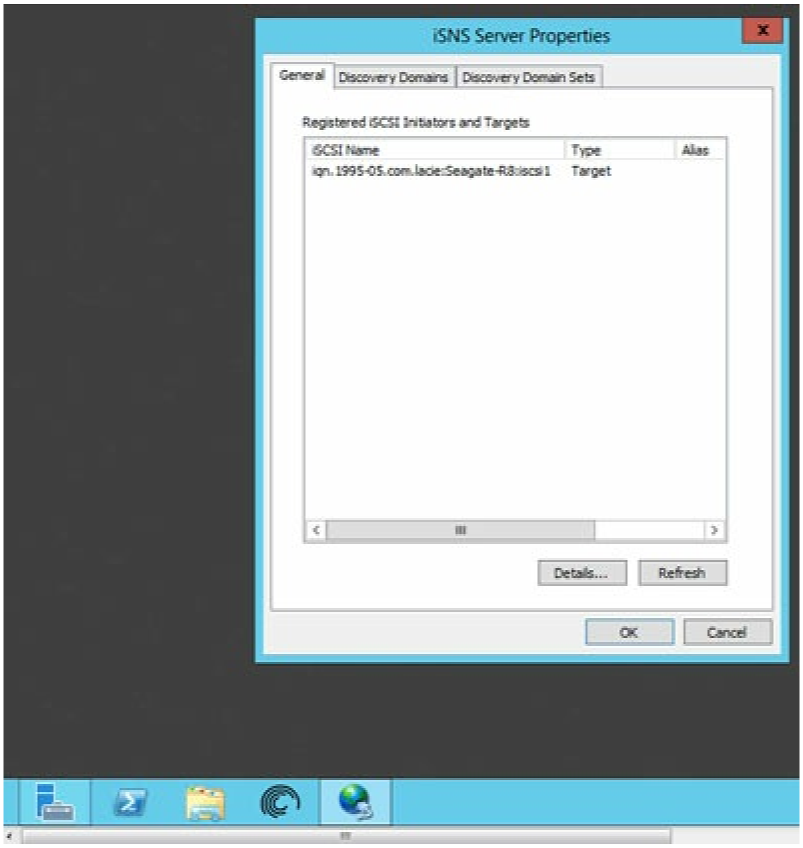
□ Create an MS-DOS startup disk

The iSCSI target appears in **Computer/My Computer** as a local disk.

# iSNS: Internet Storage Name Service

The Internet Storage Name Service (iSNS) manages multiple iSCSI targets on a network. Certain versions of Windows Server include the iSNS feature. Using an iSNS can save time for each iSCSI initiator. For example, rather than searching the network for an iSCSI target, the initiator can look for a connection in a single location, the iSNS server. The iSNS server keeps tabs on all the iSCSI targets on the network, thus allowing the initiator to connect to one that is available.

Configure iSNS on your network server then review the instructions below to add your NAS's iSCSI target.



Registered iSCSI Initiators and Targets

| iSCSI Name | Type | Alias |
|---|---|---|
| iqn.1995-05.com.lacie:Seagate-R8:iscsi1 | Target | |

## Enable iSNS server and enter its IP address:

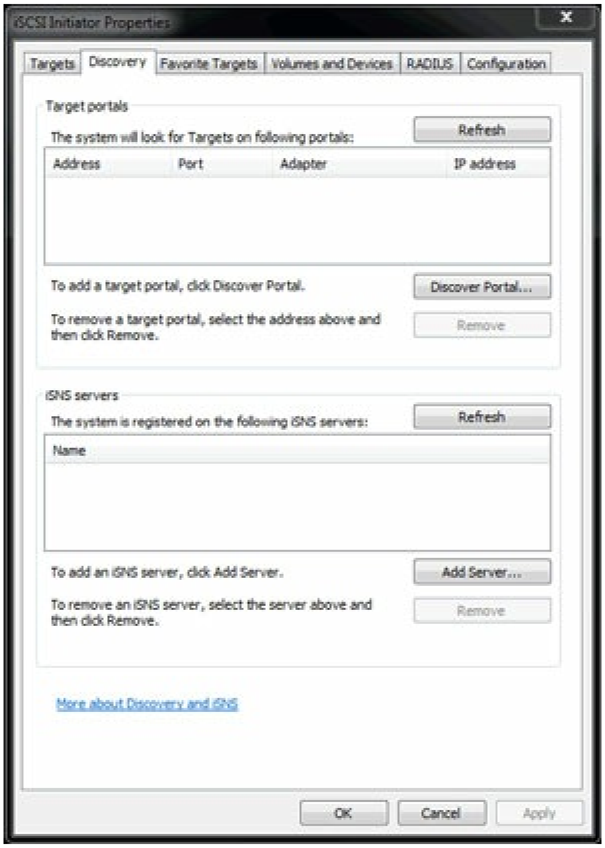
1. Go to **Device Manager** and then click **iSCSI**.
2. Click the slider on the top right to enable **iSNS**.
3. Enter the IP address for the iSNS and then click **Save**.

**Important info regarding iSCSI volume sharing :** Mounting an iSCSI volume on multiple computers at the same time leads to serious file corruption. An exception can be found with SAN cluster environments that include servers and software dedicated to managing iSCSI volume sharing. An iSNS server is not considered to be a SAN cluster environment.

## iSNS: iSCSI initiator

The steps below demonstrate a single connection to an iSNS server using Windows 7 as the initiator. Configurations will vary but you can review the instructions below and make adjustments for your operating system and network.

1. Search for and launch **iSCSI Initiator** or equivalent.
2. Choose **Discovery** and **Add server**.



The system will look for Targets on following portals:

To add a target portal, click Discover Portal.

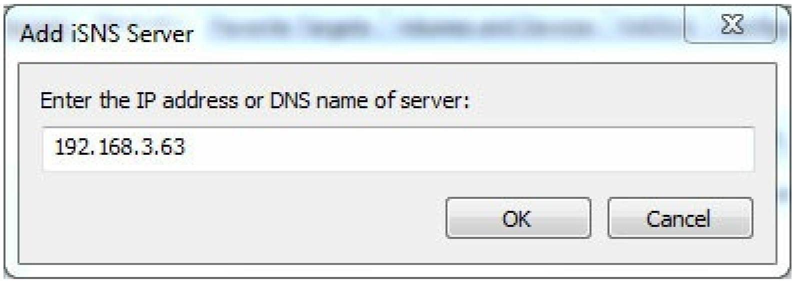
To remove a target portal, select the address above and then click Remove.

The system is registered on the following iSNS servers:

To add an iSNS server, click Add Server.

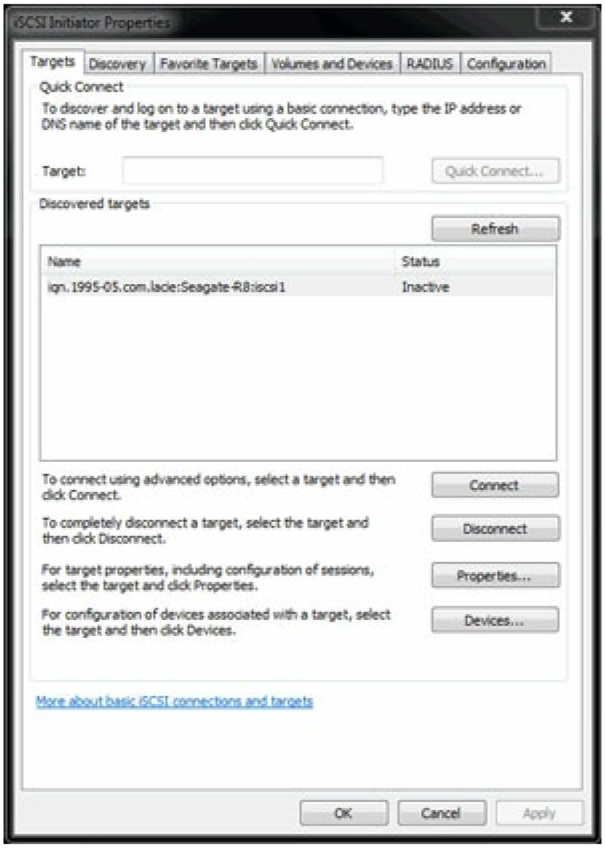
To remove an iSNS server, select the server above and then click Remove.

3. Enter the iSNS server's IP address.



Enter the IP address or DNS name of server: 192.168.3.63

4. The list of discovered targets shows the iSCSI targets that are connected to the iSNS server.



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

| Name | Status |
|---|---|
| iqn.1995-05.com.lacie:Seagate-R8:iscsi1 | Inactive |

To connect using advanced options, select a target and then click Connect.

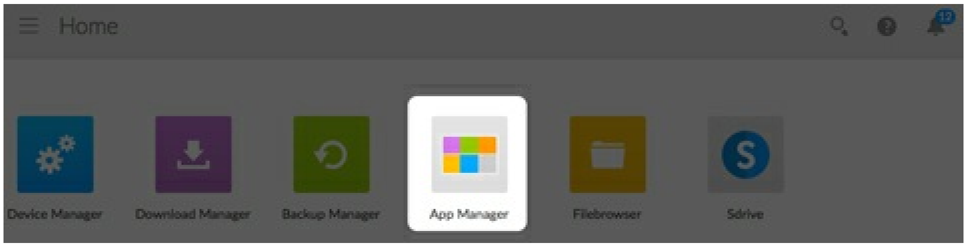
To completely disconnect a target, select the target and then click Disconnect.

For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

5. To connect to the iSCSI target, follow the instructions in iSCSI initiator.

# App Manager



Use the App Manager to install and manage apps on your device. Apps give your device additional functions and features. The App Manager includes apps that are Seagate branded as well as apps that are developed by third parties specifically for Seagate network devices.

## Overview

Review the list below to learn about the App Manager categories:

- **My Apps:** Your installed apps.
- **Updates:** Available updates for installed apps.
- **All:** All available apps.
- **Backup:** Apps used to back up your data.
- **Business:** Apps used to for commercial purposes.
- **Multimedia:** Apps used for sorting your media.
- **Security:** Antivirus apps.
- **Utilities:** Utility apps.
- **Advanced:** Install third party apps that are not available in the App Manager.

**Note:** LaCie 5big NAS Pro and LaCie 2big NAS support two apps, Filebrowser and Sdrive. All other apps are not available to these NAS devices.

## How to Install Apps

Follow the steps below to install an app.

1. From the **Categories** menu select a category.
2. Hover the cursor over the desired app and click **Install**.
3. Once the app is installed, a new button called **Action** is available. Click the button and select the action you would like to perform from the drop down menu:
    - **Open:** Opens the app so that you can use it.

**Note:** You can also open the app from the **Home** screen.

- **Details:** Shows the app's details and allows you to set permissions. Note: Third party apps provide support details on this page.
- **Stop:** Stops the app. You must return to this option to turn it back on.
- **Uninstall:** Uninstalls the app.

# Maintenance

Check for updates regularly in Maintenance.

1. Open **App Manager**.
2. Check **Installed > Updates**.
3. If one or more updates are available, a number appears next to **Updates**. The number represents the number of updates that are available for the apps you have installed.
4. Click **Updates** to see a list of apps that are ready for updates.
5. Click the **Update** button that corresponds with the app you want to update.

**Note:** There are two buttons at the top right corner of the Updates screen, **Check Apps** and **Update all**. Use Check Apps to check for updates. Use the Update all to update all your apps at once. Update all can take some time to finish.

# Advanced

The advanced section is used for installing third party apps and updates that are not available in the App Manager. Follow the instructions below to use the advanced section.

**Note:** Seagate does not provide support for third party apps. If you have trouble with a third party app, contact the app's vendor.

To install an app, review the instructions below. Note that apps must have been created specifically for NAS OS and have the file extension .rbw.

1. Click **Advanced**.
2. Turn **Manual install mode to ON**.
3. Note the status of the Dependencies. They should be OK.
4. Click **Install**.
5. Browse to the app you wish to install and accept the terms.

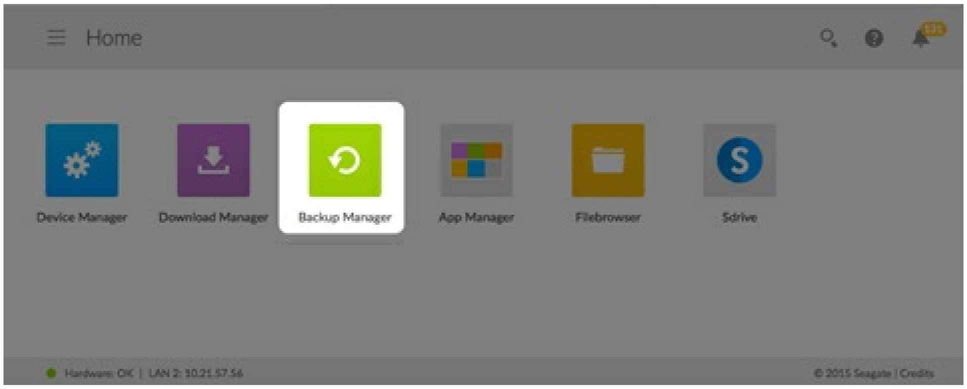
   **Note:** The app file type must be .rbw.

6. Click **Install**.

Once the app has installed it is located under **My Apps**.

**Note:** Seagate only provides support for Seagate branded apps. If you need support with a third party app, contact the app manufacturer.

# Backup Manager



The Backup Manager has four options: Backup, Restore, Sync and Network Backup server. Backup, Restore, and Sync feature intuitive setup wizards.

## Backup

Use Backup Manager to perform the following types of backups:

- Back up the Seagate storage device to:
  - External storage (USB direct attached storage)
  - Network storage (Seagate or third-party)
  - Cloud storage
- Back up external storage (USB direct attached storage) to the Seagate storage device.
- Back up network storage (Seagate or third-party) to the Seagate storage device.
- Back up cloud storage to the Seagate storage device.

Cloud services supported by Backup include:

- Amazon S3
- Baidu
- Box
- Dropbox
- Google Drive
- Strato HiDrive
- Yandex.disk

**Note on computer backups:** You can back up your computers to the Seagate storage device. Backup applications such as Seagate Dashboard, Windows File History and Apple Time Machine manage how the computer backups are performed. Use your preferred backup application and choose a shared folder on your Seagate storage device as the destination for the computer backup. When performing a backup to a private share, make certain that a user can access the share.

# Restore

Restore a backup that has been performed by the Backup.

# Sync

Choose one or more folders on your Seagate storage device to sync with your cloud storage account. Cloud services supported by Sync include:

- Baidu
- Dropbox
- Google Drive

# Network Backup disk

Enable Network Backup so that other Seagate network storage devices can back up to your primary Seagate network storage device.

**Important info on backups:** It is recommended that all users back up data to a DAS, another network storage device or cloud storage as further protection against a missing hard drive or secondary points of failure (e.g. hardware, network, etc.)

**Note on backup job order:** To conserve processing resources, the Seagate network device runs one job at time. If more than one job is scheduled for the same time or started manually, Backup Manager places them in a queue.

## Backup, Sync, and Restore examples

### Back up to a USB storage device (DAS)

An administrator keeps important files on her private share. Since remote access is not always available when she travels, the administrator backs up her share to a portable USB storage device.

### Back up to a Seagate network storage device on the local network

To prevent data loss due to hardware failure, the administrator schedules regular backups of Seagate Network Device 1 to Seagate Network Device 2. They are both on the same local network. Alternatively, the administrator can back up Seagate Network Device 1 to a compatible third-party network storage device.

### Back up to a network storage device outside the local network (offsite)

To prevent data loss due to onsite fire, flood, or theft, the administrator backs up data on Seagate Network Device 1 in her company's headquarters to Seagate Network Device 2 at a branch office. A compatible third-party storage device can also act as the destination storage.

### Back up to a cloud service (offsite)

To prevent data loss due to onsite fire, flood, or theft, the administrator backs up data on Seagate Network Device 1 to the company's Amazon S3 account.

### Restore

Someone in the office accidentally deleted an important spreadsheet from his personal share. Fortunately, the administrator backs up to another storage solution, such as USB storage, another Seagate network storage device or cloud storage. The administrator can:

- Restore a backup to revert the share to an earlier state.
- Connect to the destination storage device from a computer and browse for the missing file.

> **Important info:** The time to complete the first backup job can vary based upon the amount of data and the speed of your network. It can take several hours or, if it is an offsite or cloud backup, several days.

## Create a backup

To create a backup:

1. Launch the Backup Manager app.
2. Choose **Backup**.
3. Click **Add backup** to launch the Backup Wizard.

Follow the Backup Wizard to perform one of the following types of backup:

- Back up the Seagate storage device to:
  - External storage (USB direct attached storage)
  - Network storage (Seagate or third-party)
  - Cloud storage
- Back up external storage (USB direct attached storage) to the Seagate storage device.

- Back up network storage (Seagate or third-party) to the Seagate storage device.
- Back up cloud storage to the Seagate storage device.

Review the topics below to better understand the settings and requirements for the type of backup you want to perform.

# Back up using USB storage

Perform the following types of backups with USB storage connected to your Seagate storage device:

- The Seagate storage device to USB storage.
- USB storage to the Seagate storage device.

You can optimize backups to and from a USB storage device connected to one of the USB ports on your Seagate storage device. Refer to the table below for the file formats that work best with your Seagate device. When configuring a backup with a USB device, the Backup Wizard gives you the option to format your USB storage for optimized backups. By using an optimized format, you have the option to perform incremental backups.

An incremental backup allows you to back up new or modified files following the first backup. If the format is not optimized, you must perform full backups each time a job is run. A full backup copies everything on the source each time the backup is run.

| Operating systems | Hard disk file system | Optimized backup (incremental) |
|---|---|---|
| Linux | EXT2, EXT 3, EXT 4, and XFS | Yes |
| Mac | HFS Non-Journaled | Yes |
| Mac | HFS+ Journaled | No |
| Windows/Mac | FAT32 | No |
| Windows | NTFS | No |

# Back up using network storage

Perform the following types of backup with a second Seagate network storage device or a third-party network storage device:

- The primary Seagate storage device to a second Seagate network storage device or third-party network storage device.
- A second Seagate network storage device or third-party network storage device to the primary Seagate storage device.

The second Seagate network storage device or third-party network storage device can be located on the same network as the primary Seagate storage device or, on a network at a different location (offsite).

# Backups with network storage

Backups to and from Seagate network devices require a unique destination share called Network Backup *server*.

Backups to and from third-party network devices can use an existing shared folder.

For example, the administrator wants to back up shares on Seagate Device A to Seagate Device B. Seagate Device A is the source network device and Seagate Device B is the destination network device. To receive the backup data from Seagate Device A, the destination device, Seagate Device B, must enable its Network Backup server. Refer to the table below for examples of backups to and from Seagate and third-party network devices.

| Type of network backup | Source device | Destination device | Destination folder |
|---|---|---|---|
| Backup to a Seagate network storage device | Seagate Device A on the local network | Seagate Device B on the local or remote network (offsite). | Network Backup server |
| Backup to a third-party network storage device | Seagate Device on the local network | Third-party network device on the local or remote network (offsite). | Shared folder on the third-party network device that supports a compatible network protocol (see below). |
| Backup from a third-party network storage device | Third-party network device on the local or remote network (offsite). The device's shared folders must support a compatible network protocol (see below). | Seagate Device on the local network. | Shared folder on the Seagate network device. |

## Enable Network Backup server

Before configuring network backups between Seagate devices, the administrator must enable the Network Backup server on the destination device.

1. Go to **Backup Manager** > **Network Backup server**.
2. Choose **Enable**.
3. At the prompt, enter and confirm a password. The password can be different from the password you use for your Seagate Access login (between 4 and 20 characters). Your Network Backup password will be

needed when you set up a network backup.

4. If you have more than one volume, select the *Location* pull-down menu to choose a volume for the Network Backup server. It is highly recommended that you use a volume with RAID protection (SimplyRAID, RAID 1, RAID 5, RAID 6, or RAID 10).
5. Choose **Save**.

## Network Backup server settings

The Network Backup server table provides a summary of its settings. You can return to the Network Backup server page if you forget the password or you want to disable it.

- Only the administrator can access the Network Backup server settings.
- The administrator can find the Network Backup password if it is forgotten. Go to **Backup Manager** > **Network Backup server** and click on the magnifying glass icon.
- To change the Network Backup server password, pass the cursor to the right of the asterisks and choose the configuration icon (pencil).
- For offsite backups, administrators must confirm that the ports used by NAS OS backup jobs are available on the network router. The default port numbers are:
  - Port 873
  - Port 22 (encrypted backups)
- To delete the Network Backup server, choose **Disable**. A prompt will ask if you wish to keep data or delete all files within the share.

## Backups with third-party network storage

The Backup Wizard can help you create backups to and from third-party network storage devices that support the following protocols:

- Rsync
- SMB
- FTP
- NFS
- WebDav (Web Distributed Authoring and Versioning)

# Backups to network storage devices

## Local network

When performing network backups on a local network, make certain that:

- The source and destination network devices are powered on.
- The destination network storage device is connected to the same network as your source device.
- (Seagate network storage) The Network Backup server has been enabled and you have the password.
- (Third-party network storage) The third-party network device supports one of the five network protocols listed above.
- (Third-party network storage) You have noted the third-party network device’s IP address or network name. Network naming services are not as reliable as IP addressing.
- (Third-party network storage) You have the username and password for the network device’s backup

service.

Similar to Seagate network devices, many third-party network devices have separate credentials for login and backup.

### Remote network

When performing network backups to a remote network, make certain that:

- The source and destination network devices are powered on.
- You have the network device's **public IP address**. You can find the public IP address by visiting http://www.whatismyip.com/ or by accessing your remote network's router management software. When searching for the public IP address, use a computer connected to the same router as the destination network storage device. For further information, review the user manual for the offsite network router or contact your Internet service provider.
- The ports are open for the backup. You may need to open ports using your router's management software. The ports to open are listed at **Backup Manager** > **Network Backup server**. Review your router's user manual for instructions on how to open ports for a device on the network.
- (Seagate network storage) The Network Backup server has been enabled on the destination device and you have the password.
- (Third-party network storage) The third-party network storage device supports one of the five network protocols listed above.
- (Third-party network storage) You have the username and password for the network device's backup service. Similar to Seagate network devices, many third-party network devices have separate credentials for login and backup.

### Advanced parameters for backups to network storage devices

The Backup Wizard includes four options for your backup. See the explanations below for each option. It is not mandatory to select one or more of the parameters to continue with the backup:

- *Secure data transfers* uses encryption during the data transfer. The data is not encrypted once it is stored on the destination NAS. This option is ideal for offsite backups.
- *Compressing data during* a transfer optimizes data transmission rates. Data is compressed during the transfer only. While this option is good for low bandwidth networks, it can affect the NAS's performance.
- *Send only modified parts of files* is best used with backups that include files larger than 50MB. For example, if you edit a document that has already been backed up, only the edits will be copied during the next backup. This option can affect the NAS's performance.
- *Never delete files on the destination folder* keeps files on the destination NAS even if they are deleted from the original NAS's source folder.

# Back up using cloud storage

Before performing a backup to or from cloud storage, make certain:

- You have an account with one of the following services:
  - Amazon S3

    - Baidu
    - Box
    - Dropbox
    - Google Drive
    - Strato HiDrive
    - Yandex.disk
- You have the necessary login and access credentials for your account. You cannot create a backup without your credentials.

### Advanced parameters for backups to cloud storage

The Backup Wizard includes one or more options for your backup. See the explanations below. It is not mandatory to select one or more options to continue with the backup:

- *Secure data transfers* uses encryption during the data transfer. The data is not encrypted once it is stored on the destination NAS. This option is ideal for offsite backups.
- *Never delete files on the destination folder* keeps files on the destination even if they are deleted from the source's folder.

# Sync folders

Use Sync to keep data in one or more folders on your Seagate storage device consistent with a folder in a cloud storage service. For example, you run a Sync job for Folder A on your Seagate storage device. It has 25 files when the Sync job is first created with a similarly named folder on Dropbox. Soon after, you copy file 26 to Folder A on your Seagate storage device. The same file 26 is automatically uploaded to Dropbox to keep both folders in sync. You can also add files to the folder on Dropbox and they will automatically sync with Folder A.

Before performing a sync to cloud storage, make certain:

- You have an account with one of the following services:
    - Baidu
    - Dropbox
    - Google Drive
- You have the necessary login and access credentials for your account. You cannot create a sync without your credentials.

## Create a sync:

1. Launch the Backup Manager app.
2. Choose **Sync**.
3. Click **Add sync job** to launch the Sync Wizard and follow it to completion.

# Restore a backup

Backups to or from your Seagate storage device can be restored. You can restore a backup to the original source folder or choose another folder for your backed up files. Follow the directions below to restore a backup.

- Launch the Backup Manager app.
- Choose **Restore**.
- Click **Add restore** to launch the Restore Wizard and follow it to completion.

# Backup and sync job options and start/stop

## Options

Follow the steps below to review and change options for a backup or sync job.

1. Launch the Backup Manager app.
2. For backups, locate the backup you want to modify and then pass the cursor to the far right of its row to enable the Edit pull-down menu.
3. For sync jobs, click **Sync** and locate the sync you want to modify then pass the cursor to the far right of its row to enable the Edit pull-down menu.
4. You can choose:
   - Details
   - Enable/Disable the OneTouch button (if applicable)
   - Edit authentication
   - Edit description
   - Edit schedule
   - Disable
   - Restore
   - Delete

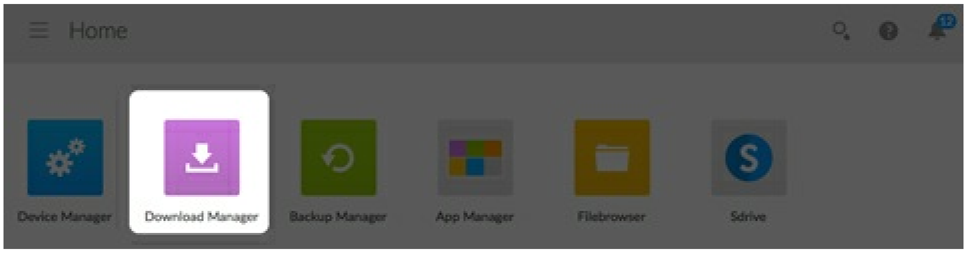
If you disable a scheduled job, it will not run until it is enabled again.

## Starting/stopping jobs

Locate the backup or sync job you wish to stop or start and pass the cursor to the far right of its row to view the triangular and square icons:

- **Start a job**: choose the triangular icon.
- **Stop a job that is in progress**: choose the square icon.

# Download Manager



Use your NAS OS device as a download server to:

- Download files from the Internet (PDF, Torrent, Binary).
- Upload files from the local disk (Torrent).

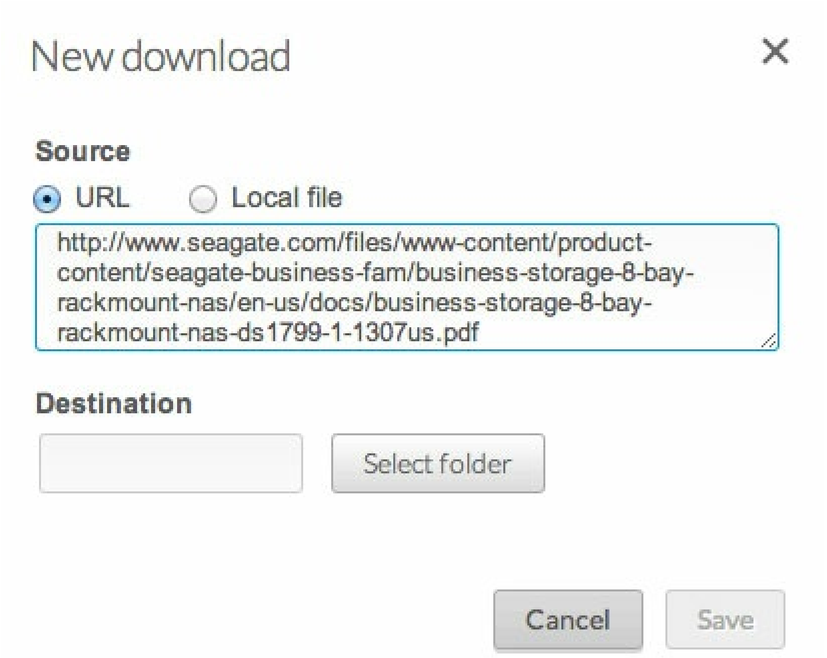
## Enable the download machine

The download machine service must be enabled to use the Download Manager.

1. Go to the **Download Manager.**
2. Click the slider on the upper right

## Create a download job

1. Go to the **Download Manager.**
2. Choose **Add download.**
3. At the prompt, choose file's location:
    - URL: Type or paste the web address.


New download

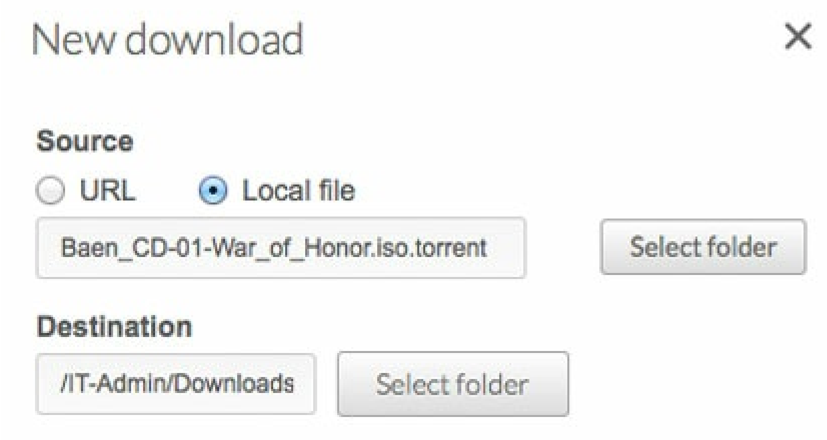
Source

● URL ○ Local file

http://www.seagate.com/files/www-content/product-content/seagate-business-fam/business-storage-8-bay-rackmount-nas/en-us/docs/business-storage-8-bay-rackmount-nas-ds1799-1-1307us.pdf

Destination

- Local File: Select **Browse** to search for the file.


New download

Source

○ URL ● Local file

Baen_CD-01-War_of_Honor.iso.torrent

Destination

/IT-Admin/Downloads

4. Select the destination share by clicking inside the **Destination** field. Choose the share in the pop-up window.
5. To better organize your downloads, you can choose **Create folder** at the prompt to add a folder.
6. Choose **Save** to begin the download.

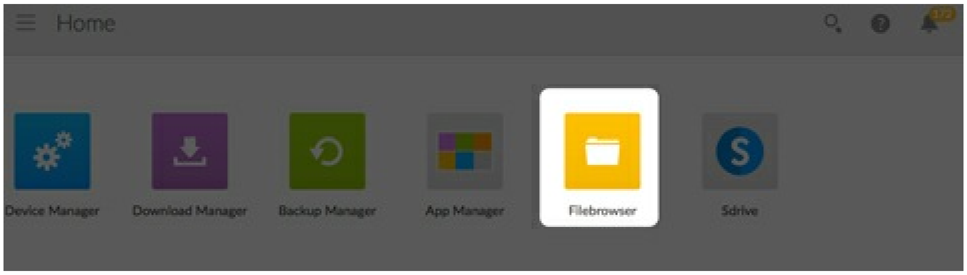
# Download settings

Go to **Download Manager > Settings** to review and change settings. You can edit a setting by passing the cursor to its right and clicking on the configuration icon (pencil).

- **Maximum active downloads:** Enter the number of download jobs that can run simultaneously.
- **Download rate limit:** Select the pull-down menu and choose **Custom.** Enter a number from 1KB/s to 102400KB/s.
- **Upload limit rate:** Select the pull-down menu and choose **Custom.** Enter a number from 1KB/s to 102400KB/s.
- **TCP Listening port:** Enter a router port number through which the download service can operate.

**Technical note:** Multiple simultaneous downloads can impact your NAS's performance. In some instances, even after a download has completed, the download service may continue to use system resources.

# Filebrowser



Use Filebrowser to view, share and manage your files on your Seagate storage device. You can:

- Upload files
- View files
- Share files with family, friends and colleagues
- Play back audio and video files supported by your web browser
- Create folders
- Organize content
- Ingest from external drives

## Upload files

1. Go to the destination folder for your files.
2. Click the **Plus Sign** on the top right and choose **Upload**.
3. Select the files you want to upload.
4. Click **Choose**.

## Share files

1. Navigate to the item you want to share.
2. Click **Share link**.You can:
   - Email the link from the Filebrowser's native email client or copy the link to your preferred email client.
   - Add a password or expiration date by clicking **Add password and expiration date**.

**Note on the share link:** The link to share a file or folder is created when you click **Share link**. Even if you do not send the link using the Filebrowser email client or copy it to your email client, the link has been created. If you mistakenly created the link or you do not want to keep it, click **Remove the link** in the Share link pop-up window.

# Viewing or listening to files

You can play media content in Filebrowser. If your browser supports the file type you should be able to play, view and listen to your content within the Filebrowser app.

# Manage content

1. Select the file or folder you want to manage.
2. Click **Actions.**
3. You can:
   - **Download**: Allows you to download the file
   - **Copy**: Allows you to navigate another folder and paste the item
   - **Rename**: Allows you to rename the file or folder
   - **Delete**: Deletes the selected item

# Create a Folder

1. Choose a share or folder to create the new folder.Click the **Plus Sign** choose **New Folder**.
2. Type the name of the new folder and click **Save**.

# Ingest from an external drive

1. Connect your external USB hard drive to one of the Personal Cloud's USB ports. Use the USB 3.0 port if your hard drive supports USB 3.0.
2. Open **Filebrowser.**
3. The following message appears: External storage connected. **Copy to Seagate [device name].** Click **Copy to Seagate [device name]. Note**: The **[device name]** is the name of your Seagate storage device.
4. Click **Copy to Seagate Device Name**.
5. Select the folders and files you want to copy and click **Copy**.
6. Select the destination folder and click **Copy**.
7. Choose how you would like to manage file conflicts and click **Save**.

# Remote Access

Remote access to your NAS OS device is available using:

- Sdrive
- MyNAS
- FTP (see FTP)

While Sdrive and MyNAS are easy to configure, they differ in accessing data and managing the NAS from remote locations:

- Sdrive is an application with file system integration. Once Sdrive is launched, a separate volume becomes available on your computer similar to a standard DAS or NAS. Sdrive also gives you access to NAS OS.
- MyNAS provides direct access to NAS OS using an Internet browser and does not require additional software. However, file integration is not available with MyNAS so files must be uploaded and downloaded via the File Browser (see File Browser).

## Sdrive

### Sdrive and Seagate Access

Sdrive is now linked to a Seagate Access account. Generally, an administrator creates a Seagate Access account for a user. The administrator’s Seagate Access account is created automatically when first configuring the NAS. Administrators who upgrade the NAS from earlier versions of NAS OS can create Seagate Access accounts in **Device Manager > Users.**

A standard user can also create a Seagate Access account using Sdrive. See Invitation sent to a user without a Seagate Access account for instructions.

Your Seagate Access account can be used with the following applications:

- **Sdrive–**Available for Windows and Mac.
- **Seagate Media app (Seagate Personal Cloud only)–**Available for Android and iOS mobile devices.

i **Important info:** Professional NAS devices do not support using the Seagate Media app as a playback app for media. Use Seagate Media with the Seagate Personal Cloud for your home.

# Sdrive: PC/Mac

Sdrive is an application for your PC/Mac in the office, at home and anywhere with a connection to the Internet. It creates a special Sdrive volume with all the files stored on your compatible Seagate NAS devices. The Sdrive volume is easy to access since it appears on your computer like a standard hard drive.

Administrators can also use Sdrive to access the NAS's management tool.

**Example:** You have important work files that you backed up to your Seagate NAS at the office. Only upon arriving home do you realize that you forgot to copy them to make final edits. Fortunately, Sdrive is installed on your work and home computers and both are linked to your Seagate Access account. You open the Sdrive volume and copy the important files from your NAS to your home computer.

## How do I get started?

### I started with NAS OS 4.1 and higher

The NAS OS setup wizard for version 4.1 prompts the administrator to create a Seagate Access account. If you created the account, skip to Download and install Sdrive.

If you did not create a Seagate Access account during the setup wizard, go to Create a Seagate Access account in NAS OS.

### I upgraded from NAS OS 4.0.x

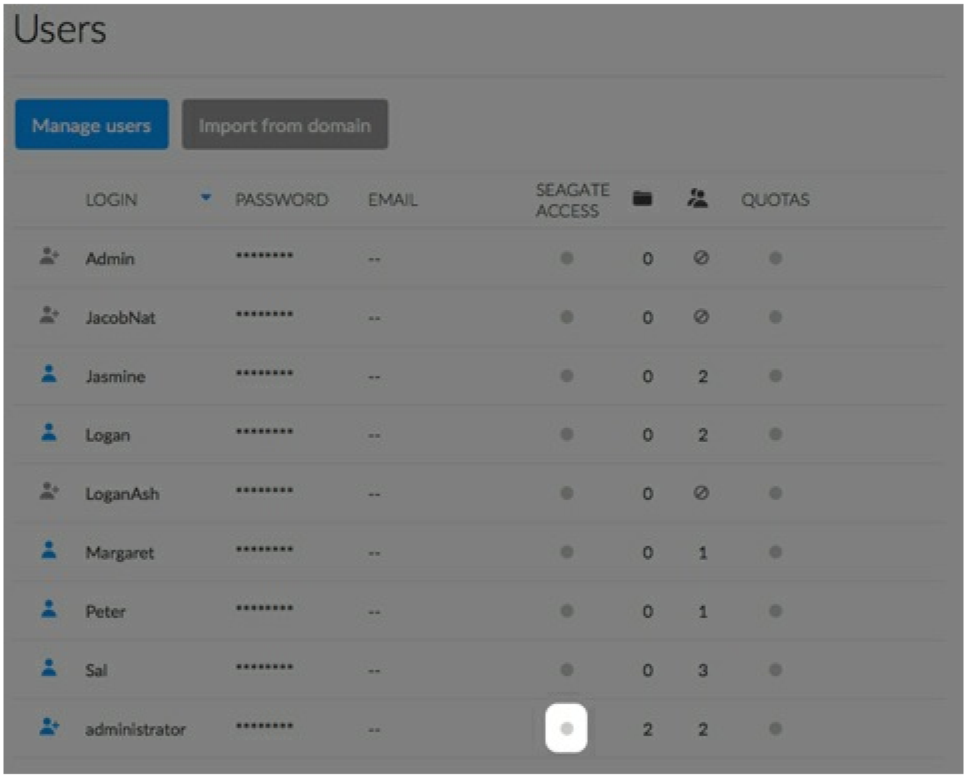
Administrators upgrading from an earlier version of NAS OS, 4.0 and below, can begin with Create a Seagate Access account in NAS OS.

## Create a Seagate Access account in NAS OS

Administrators can create Seagate Access their accounts from the Users page. Once an administrator has a Seagate Access account, invitations to join the device can be sent to users. Follow the applicable instructions below to add Seagate Accounts for administrators and users.

### NAS OS administrator: create a Seagate Access account

1. Go to **Device Manager > Users**.
2. Find the administrator's Login name and then click the white circle in the Seagate Access column.

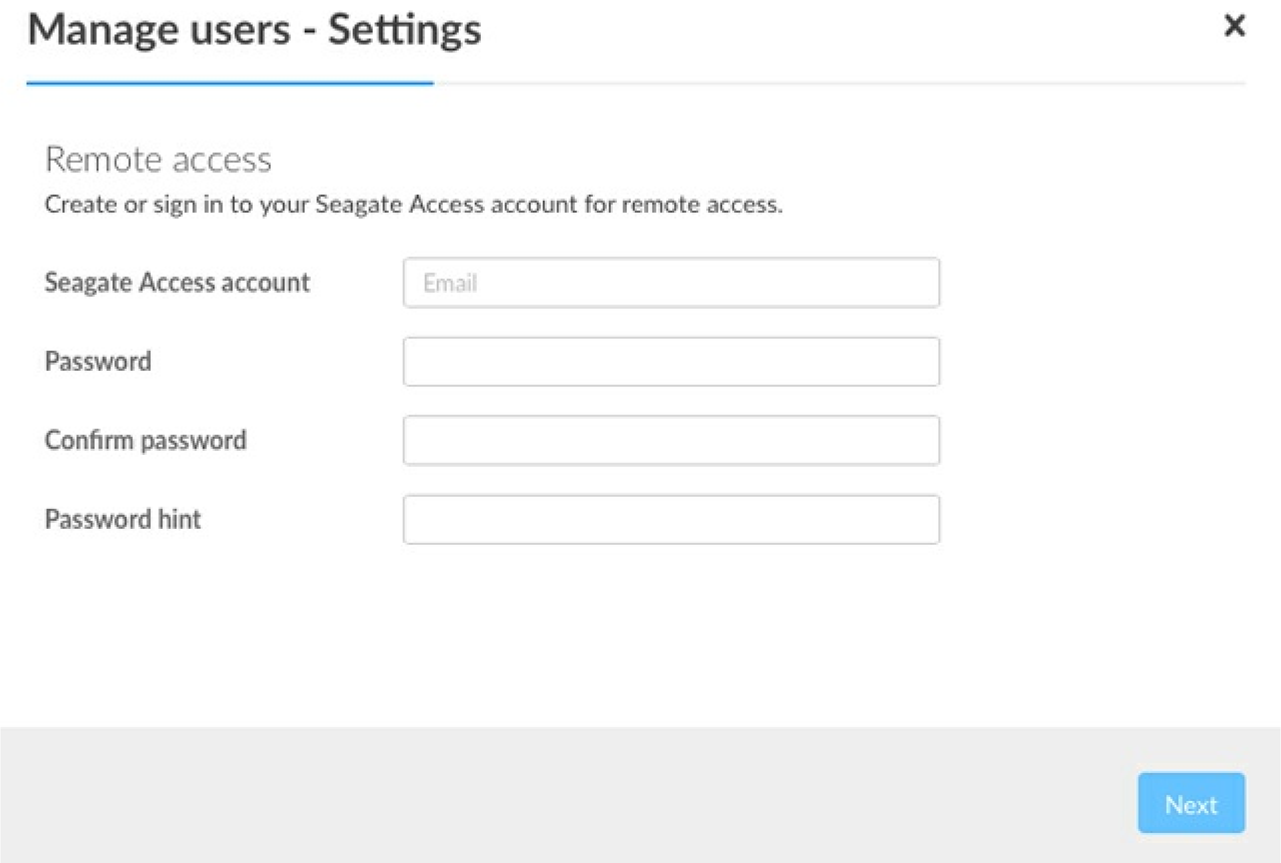


Users

Manage users | Import from domain

| LOGIN | PASSWORD | EMAIL | SEAGATE ACCESS | | | QUOTAS |
|---|---|---|---|---|---|---|
| Admin | ******** | -- | ● | 0 | ⊘ | ● |
| JacobNat | ******** | -- | ● | 0 | ⊘ | ● |
| Jasmine | ******** | -- | ● | 0 | 2 | ● |
| Logan | ******** | -- | ● | 0 | 2 | ● |
| LoganAsh | ******** | -- | ● | 0 | ⊘ | ● |
| Margaret | ******** | -- | ● | 0 | 1 | ● |
| Peter | ******** | -- | ● | 0 | 1 | ● |
| Sal | ******** | -- | ● | 0 | 3 | ● |
| administrator | ******** | -- | ● | 2 | 2 | ● |

3. Complete the fields in the Seagate Access wizard and then click **Next**.



Manage users - Settings

Remote access

Create or sign in to your Seagate Access account for remote access.

| | |
|---|---|
| Seagate Access account | Email |
| Password | |
| Confirm password | |
| Password hint | |

4. An email has been sent to the address that you entered in the previous step. Open your email and check for the confirmation code. If you do not see an email, check your spam folder.
5. Copy the confirmation code in the email and paste it to the **Confirm email** window in NAS OS.
6. Click **Finish.**

**NAS OS user: invite to join the device**

The administrator can invite a user to join the NAS. An invitation is sent to the user with instructions on how to create a Seagate Access account.

> **Important info:** The administrator must have a Seagate Access account to invite users to join the NAS. Make certain to follow the steps in NAS OS administrator: create a Seagate Access account before following the steps below.

1. Go to **Device Manager** > **Users.**
2. Find the user's Login name and then click the white circle in the Seagate Access column.
3. Enter the user's email address.
4. Enter the administrator's Seagate Access password.
5. An email is sent to the user. The user follows the directions below based upon having or not having a Seagate Access account:
   - Has an account: see Invitation sent to a user with a Seagate Access account
   - Does not have an account : see Invitation sent to a user without a Seagate Access account

# Download and install Sdrive

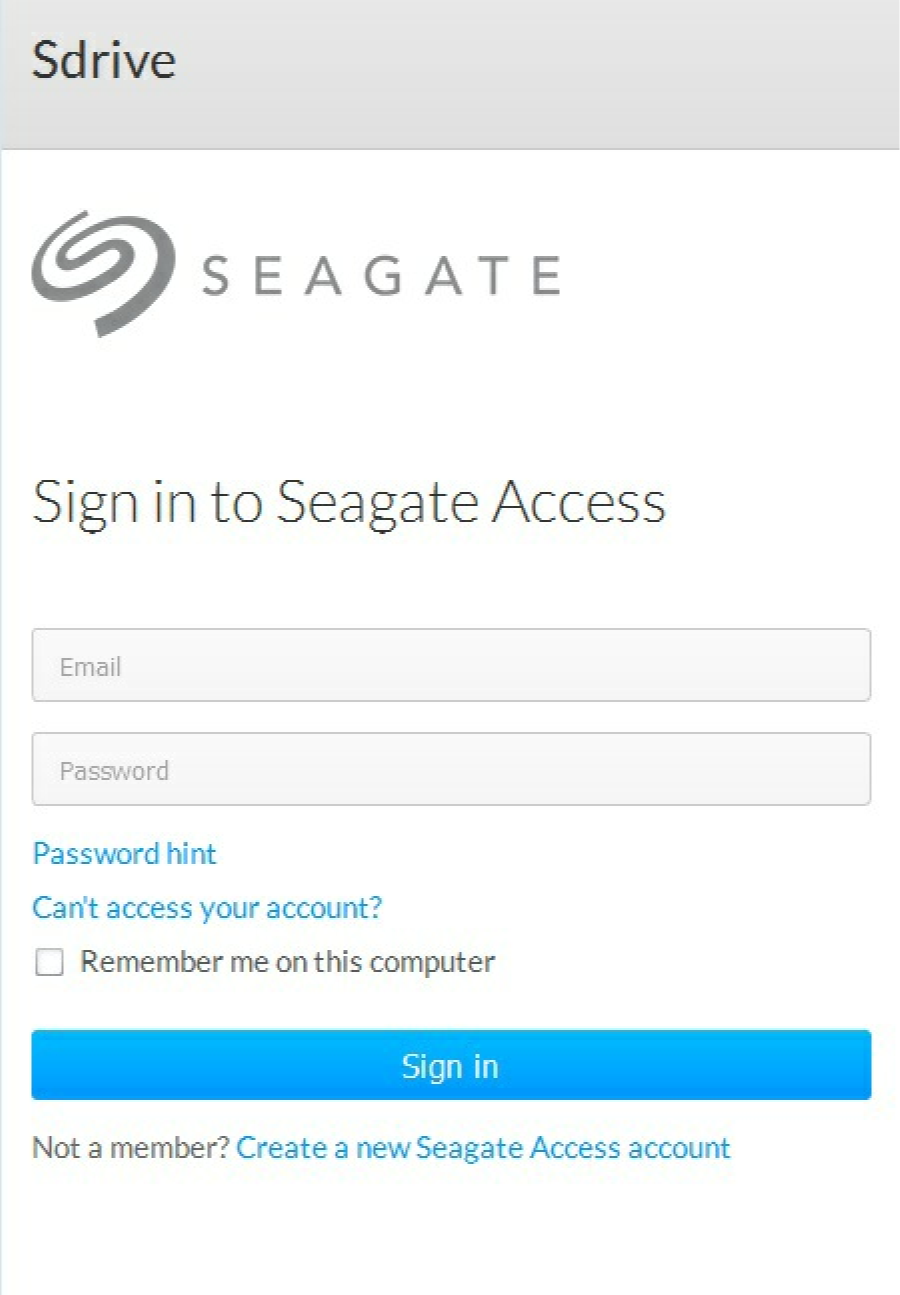
Follow the directions below to install Sdrive.

1. Download Sdrive for your device:
   - Seagate NAS
   - Seagate NAS Pro
   - Seagate 4-bay Rackmount NAS
   - Seagate 8-bay Rackmount NAS
2. Check the Downloads folder for the Sdrive installer and open it.
3. Follow the Sdrive installer to completion. You are prompted to restart your computer.

## Connect to your Seagate NAS

> **Important info for users:** Your Seagate Access account must be associated with your Seagate NAS before you use Sdrive to access files and media. The administrator should have sent you an invitation email with instructions on how to link your account to the NAS. Contact the administrator if you do not know your Seagate Access credentials.

The Sdrive login window launches automatically each time you boot your computer. You can enter your Seagate Access account to mount the Sdrive volume or close the window.


Sdrive

Sign in to Seagate Access

Email
Password
Password hint
Can't access your account?
□ Remember me on this computer
Sign in
Not a member? Create a new Seagate Access account

Once it is launched, Sdrive takes on two roles:

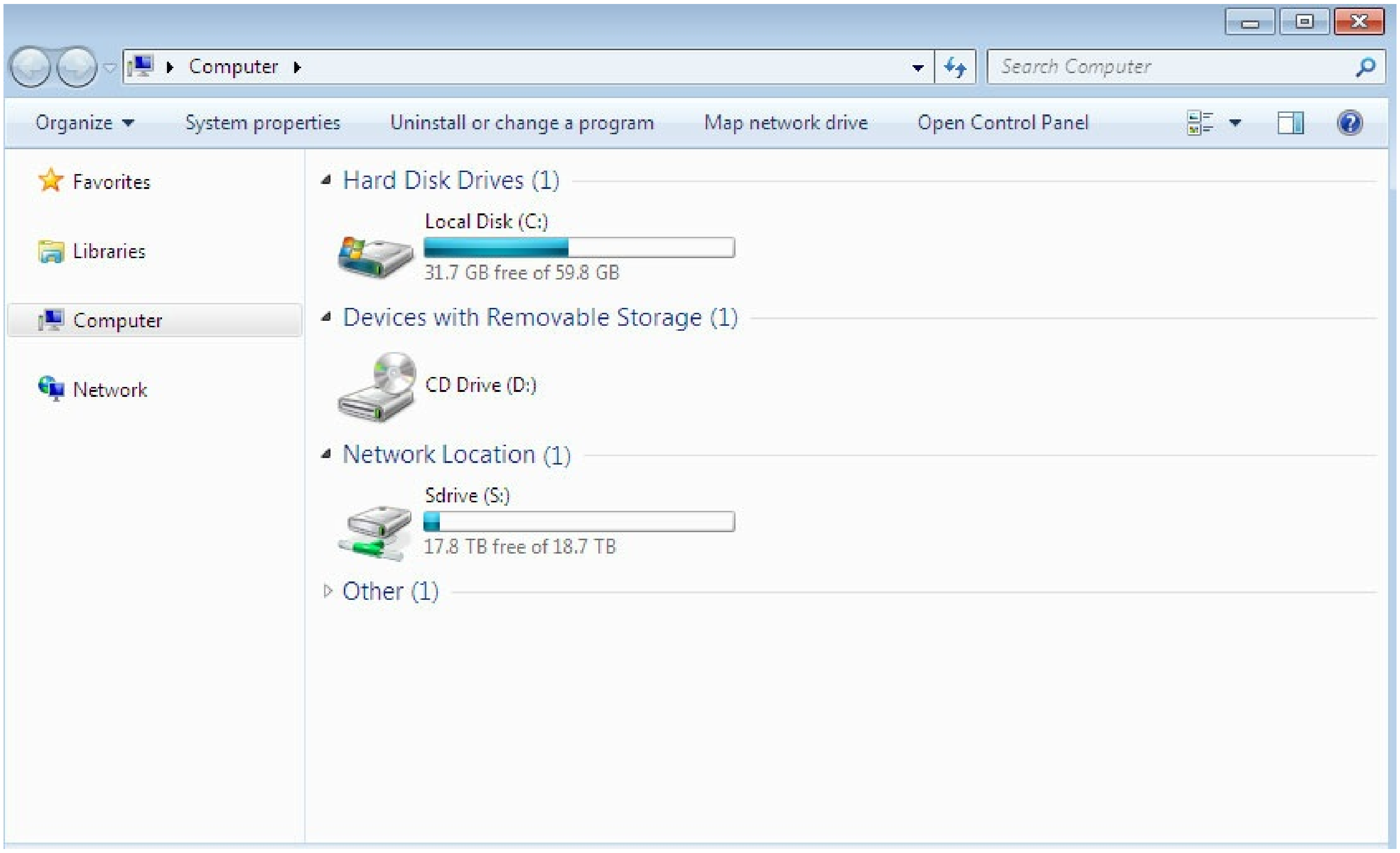
- **Administrator and users:** an Sdrive volume to access content at the file level. This means that you can open your NAS's folders and see your files on any computer with a connection to the Internet.
- **Administrator:** an application to manage your compatible Seagate NAS devices.

**Forgotten password**
If you forgot your password, enter your Seagate Access sign-in and click "Can't access your account?" An email is sent with a link to reset your password.

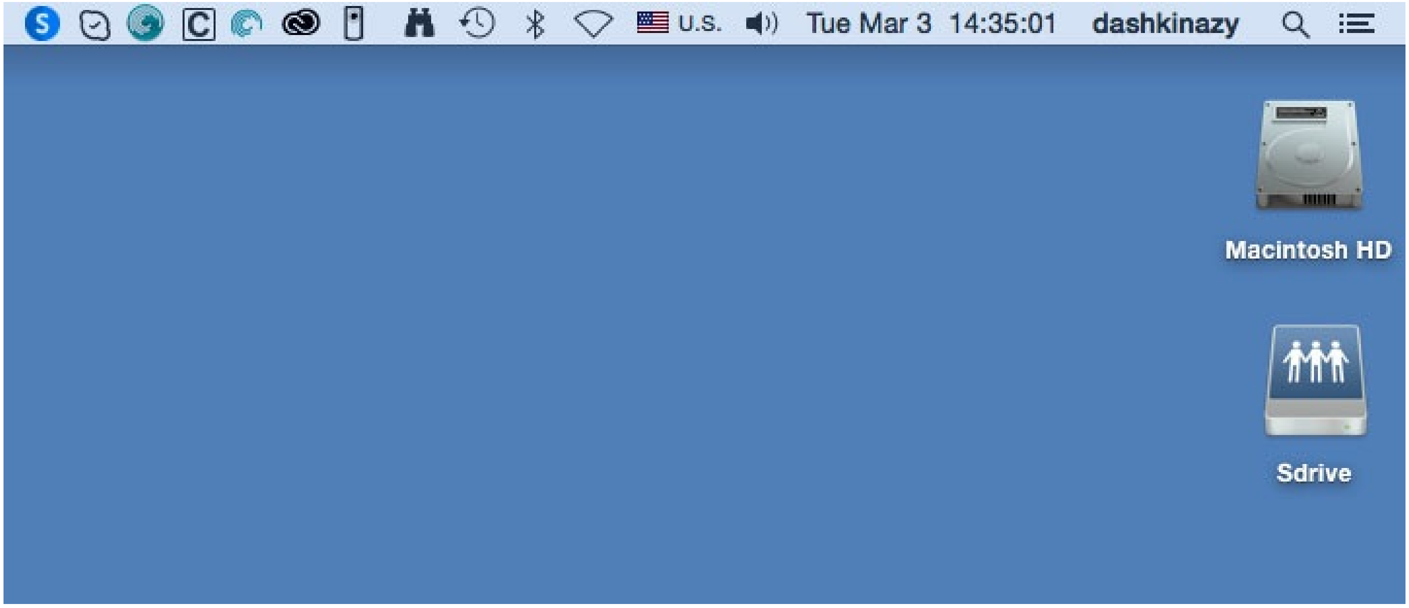
## Sdrive volume

Following a successful login, the Sdrive volume is available in the following locations:

- **PC**: Explorer window > Network location



- **Mac**: Desktop



The Sdrive volume gives users quick access to their files on the NAS. Users can access:

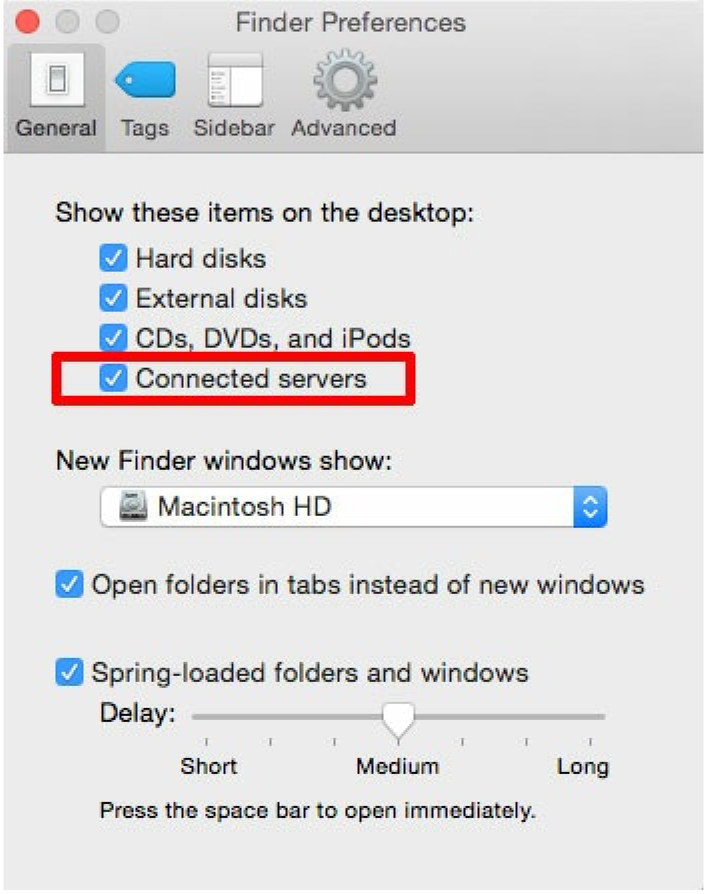
- Public shares
- Shares they have been given permission to open (read or read+write)

Users with Seagate Access accounts associated with multiple Seagate NAS devices can access all of them in the Sdrive volume.

## Mac: missing Sdrive volume

If the Sdrive volume does not appear on your desktop after you successfully log in with your Seagate Access account, there may be a setting to change. Review the instructions below.

1. On your Mac desktop, go to **Finder > Preferences**.
2. Make certain that the box next to **Connected servers** is checked.



Show these items on the desktop:

☑ Hard disks
☑ External disks
☑ CDs, DVDs, and iPods
☑ Connected servers

New Finder windows show:

Macintosh HD

☑ Open folders in tabs instead of new windows

☑ Spring-loaded folders and windows

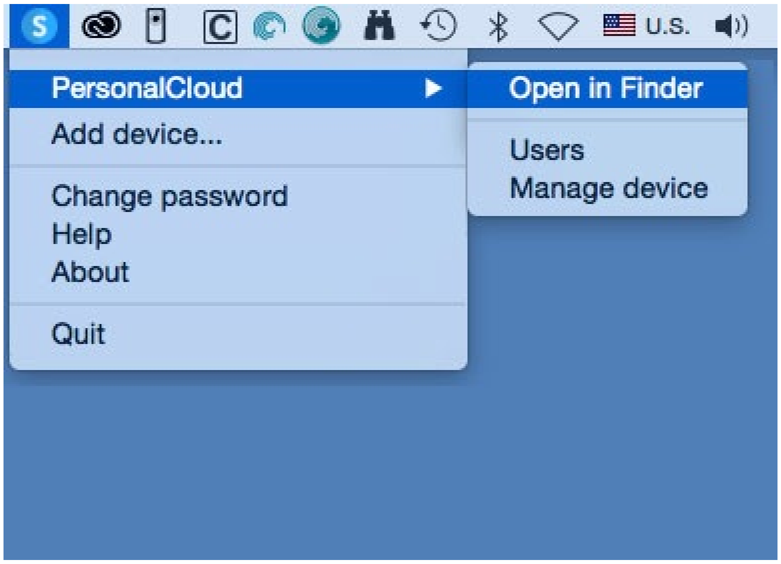
Delay: Short Medium Long

Press the space bar to open immediately.

# Sdrive application

Click the Sdrive application icon to access its features. The application icon location differs by operating system:

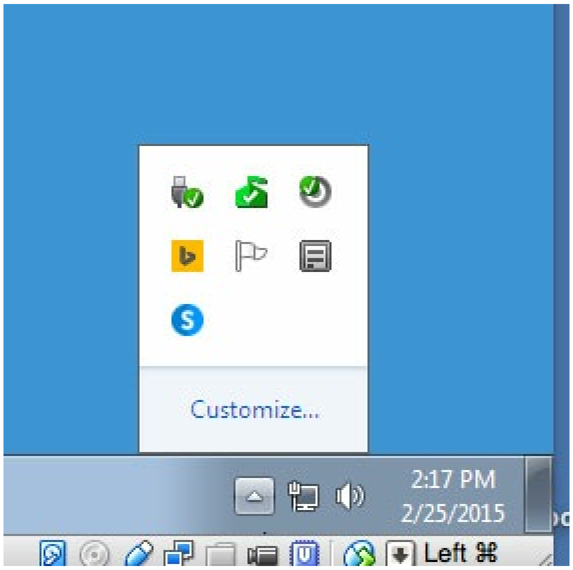
- **Windows:** System tray > Hidden icons (up arrow in the system tray). See below for instructions on how to move the Sdrive application icon to the system tray for easy access.
- **Mac:** Menu bar.



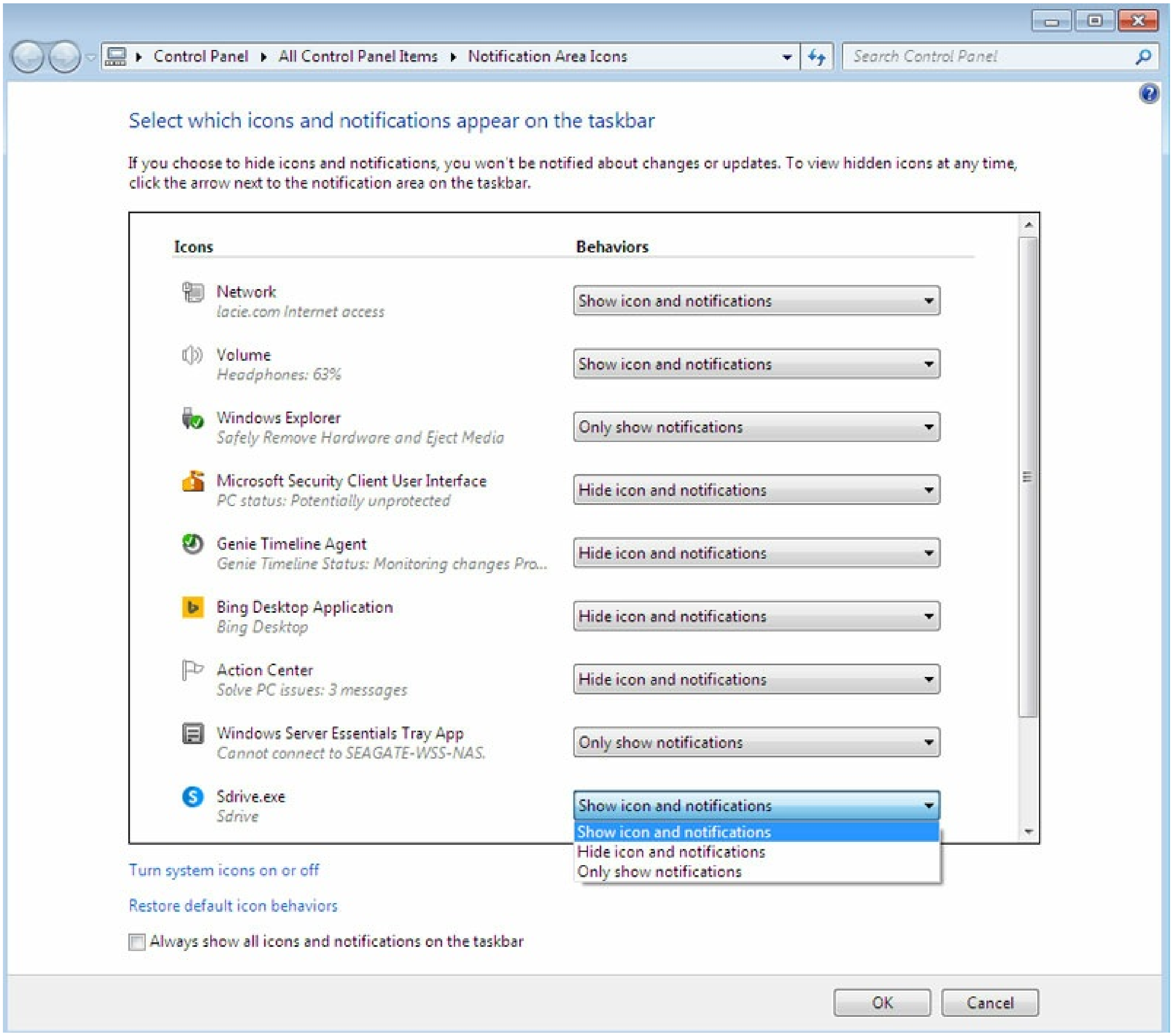
Similar to most applications in the system tray or menu bar, actions are dependent upon the operating system. For example, Windows users must apply a right click on the Sdrive application icon to access most of its features. A left click in Windows launches the Sdrive volume in an Explorer window. Mac users can use a standard left click.

## Windows: move the Sdrive application icon to the system tray

1. In the system tray, click **Hidden icons** (up arrow).



2. Choose **Customize**.
3. Click the pull-down menu for Sdrive and choose **Show icon and notifications.**


Control Panel ▸ All Control Panel Items ▸ Notification Area Icons
Search Control Panel

Select which icons and notifications appear on the taskbar

If you choose to hide icons and notifications, you won't be notified about changes or updates. To view hidden icons at any time, click the arrow next to the notification area on the taskbar.

| Icons | Behaviors |
|---|---|
| Network<br>*lacie.com Internet access* | Show icon and notifications |
| Volume<br>*Headphones: 63%* | Show icon and notifications |
| Windows Explorer<br>*Safely Remove Hardware and Eject Media* | Only show notifications |
| Microsoft Security Client User Interface<br>*PC status: Potentially unprotected* | Hide icon and notifications |
| Genie Timeline Agent<br>*Genie Timeline Status: Monitoring changes Pro...* | Hide icon and notifications |
| Bing Desktop Application<br>*Bing Desktop* | Hide icon and notifications |
| Action Center<br>*Solve PC issues: 3 messages* | Hide icon and notifications |
| Windows Server Essentials Tray App<br>*Cannot connect to SEAGATE-WSS-NAS.* | Only show notifications |
| Sdrive.exe<br>*Sdrive* | Show icon and notifications |

Turn system icons on or off

Restore default icon behaviors

□ Always show all icons and notifications on the taskbar

4. Choose **OK.**
5. Sdrive is available in the system tray. Right click it to access folders or manage your Seagate NAS devices.

# Sdrive features

Sdrive can help administrators and users perform the following actions:

- Accept invitations to join Seagate NAS devices
- Change the Seagate NAS / Seagate Access password
- Manage Seagate NAS (administrator)

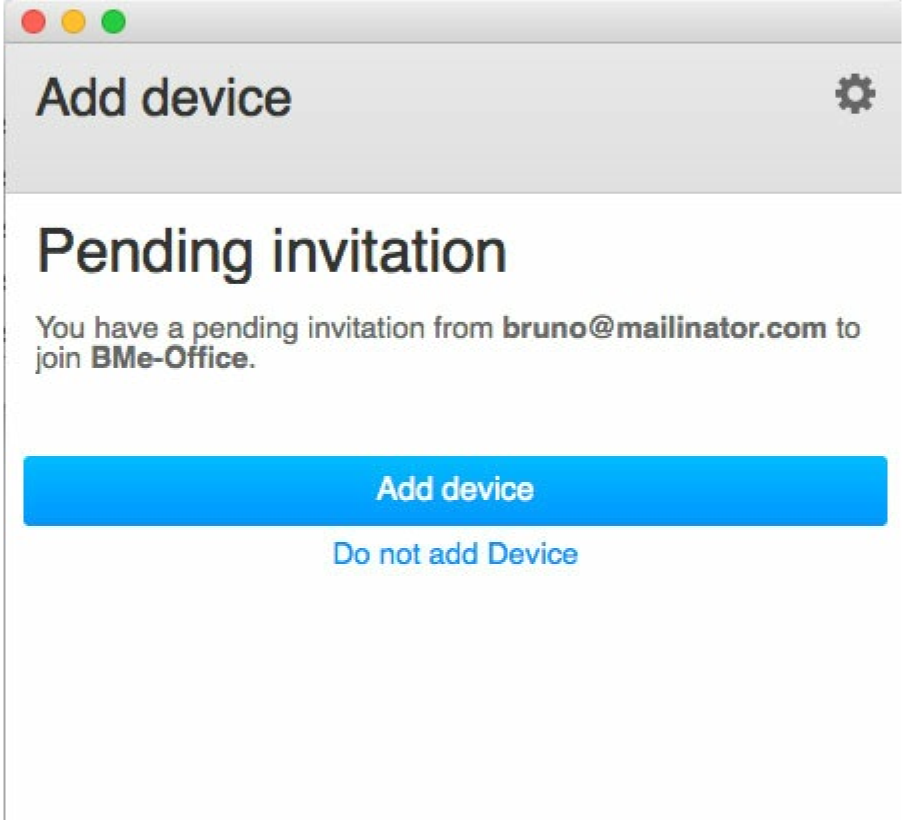
## Accept an invitation

An administrator can invite users who work inside and outside the office to join the NAS. An email is sent to the user with instructions on how to confirm the invitation. The instructions below offer the same steps found in the email.

**Note:** If the email does not appear in your Inbox, check your Spam.

**Invitation sent to a user with a Seagate Access account:**

1. Click Sdrive in the system tray (PC) / menu bar (Mac).
2. Choose **Add device**. If you do not see the *Add device* window, look behind open applications or windows.
3. The pending invitation should be listed. Choose **Add device** to add the NAS or **Do not add Device** to refuse the invitation.



Add device

Pending invitation

You have a pending invitation from **bruno@mailinator.com** to join **BMe-Office**.

**Invitation sent to a user without a Seagate Access account**
A user who does not have a Seagate Access account must first create one. Once the Seagate Access account is created, the user can accept the invitation using the code sent in the email.

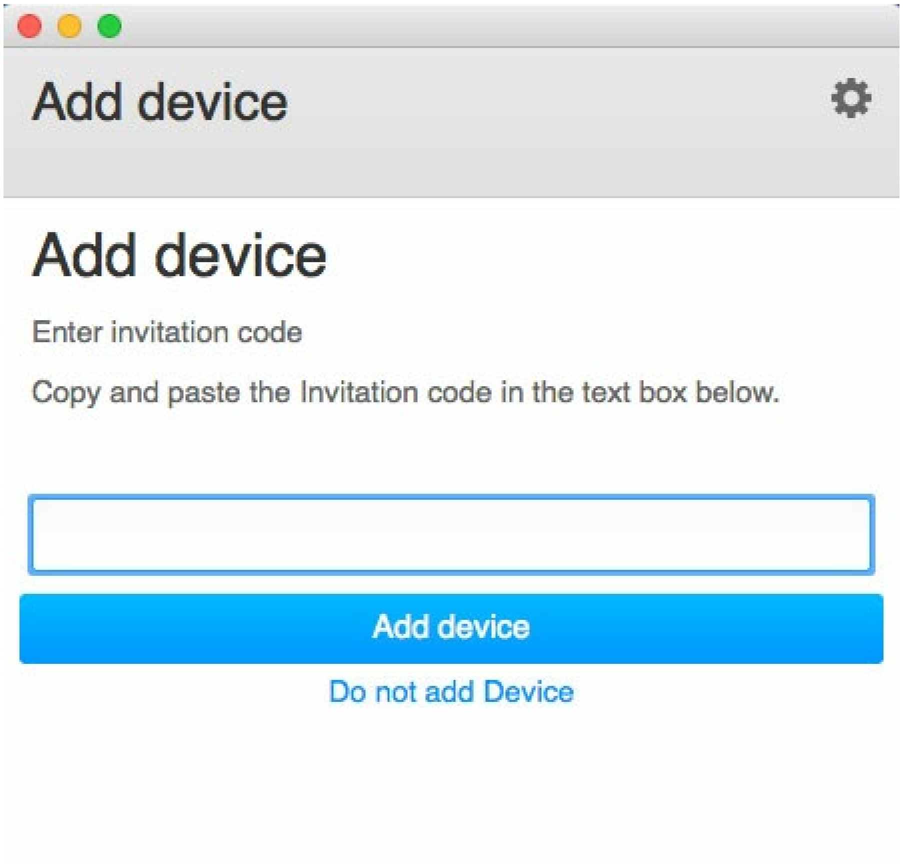
**Note:** If the email does not appear in your Inbox, check your Spam.

1. Download and install Sdrive per the instructions in the invitation email.
2. Upon reboot, the Sdrive sign in window opens. Choose **Create a new Seagate Access account.**
3. Complete all fields and choose **Create account.** An email has been sent to the address you entered.
4. The verification window opens. Check your email for the confirmation code and copy it to the applicable field. If the email does not appear in your Inbox, check your Spam.

5. Choose **Verify** to create your Seagate Access account.
6. At the sign in window, enter your Seagate Access credentials and choose **Sign in.**
7. Choose **Sdrive** and select **Add device**. Sdrive is available in the following locations.
   - **Windows:** hidden icons (up arrow in the system tray). Right click Sdrive to choose **Add device.** For instructions on how to move Sdrive to the system tray for easy access, see Windows: move the Sdrive icon to the system tray.
   - **Mac**: menu bar. Left click Sdrive to choose **Add device.**

   > **Note:** If you do not see the Add device window, look behind open applications or windows.

8. Copy the code found in the invitation email to the field in the Add device window.



Add device

Enter invitation code

Copy and paste the Invitation code in the text box below.

9. Choose **Add device.**

**Invitation sent to a user with a Seagate Account but to the wrong email address**
Many people have multiple email accounts but only one is linked to Seagate Access. Follow the directions below if you receive an invitation at an email account that is not linked to Seagate Access.

> **Note:** If the email does not appear in your Inbox, check your Spam.

1. Click Sdrive and select Add device.
   - **Windows:** hidden icons (up arrow in the system tray) or system tray. Right click Sdrive to choose Add device. For instructions on how to move Sdrive to the system tray for easy access, see

Windows: move the Sdrive icon to the system tray.

- **Mac:** menu bar. Left click Sdrive to choose Add device.

2. Copy the code found in the invitation email.
3. Choose **Add device.**

### Change your Seagate Access password

You can change your Seagate Access password in Sdrive. The change does not apply to the password that you use when signing into NAS OS, also known as the web board.

1. Click **Sdrive** and select **Change password.**
   - **Windows:** hidden icons (up arrow in the system tray) or system tray. Right click Sdrive to choose **Add device.** For instructions on how to move Sdrive to the system tray for easy access, see Windows: move the Sdrive icon to the system tray.
   - **Mac:** menu bar. Left click Sdrive to choose **Add device.**
2. Complete all the fields.
3. Choose **Change password**.

## Manage your Seagate NAS devices (administrator)

Use Sdrive to access your NAS's management tool, also known as the web board.

1. Click **Sdrive** and select **[NAS Name] > Manage Device** or **[NAS Name] > Users.**
   - **Windows:** hidden icons (up arrow in the system tray) or system tray. Right click Sdrive to choose **[NAS Name] > Manage Device.** For instructions on how to move Sdrive to the system tray for easy access, see Windows: move the Sdrive icon to the system tray.
   - **Mac: menu bar. Left click Sdrive to choose [NAS Name] > Manage Device.**
2. Choose your NAS and select **Manage device** or **Users.**
   - **Manage device:** your default browser opens to the NAS's Overview page.

# MyNAS

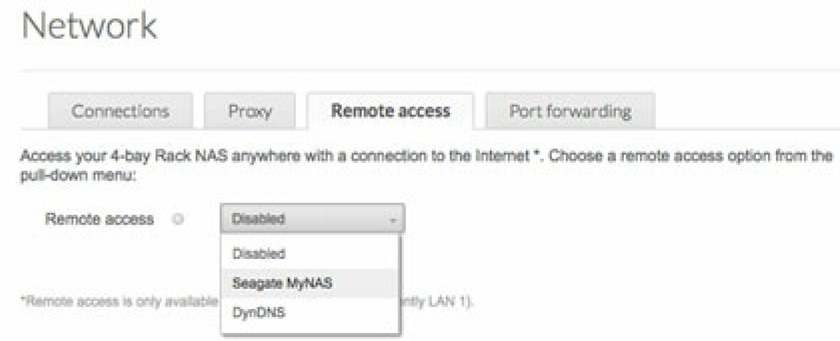
**Important info:** The MyNAS app for Android and iOS is not compatible with NAS OS 4.2 and higher. You can connect to your NAS using a browser on your mobile device at mynas.seagate.com.

MyNAS provides direct access to NAS OS using an Internet browser. However, MyNAS does not offer the type of file integration found with Sdrive. Therefore, files must be uploaded and downloaded via the File Browser (see File Browser).

# Set up MyNAS remote access

**Important info**: In order to prevent unauthorized access, it is critical to protect user and administrator accounts registered to your NAS OS device with a strong password BEFORE setting up remote access. Since MyNAS lets you access your data with a simple URL, unwanted users could access the NAS's files unless each authorized user is protected by a strong password. For added protection, a user can select secure authentication by choosing **Switch to HTTPS** at the NAS OS login.

1. Go to **NAS OS** > **Device Manager** > **Network** > **Remote access**.
2. In the **Remote access** drop-down menu, choose **Seagate MyNAS**.

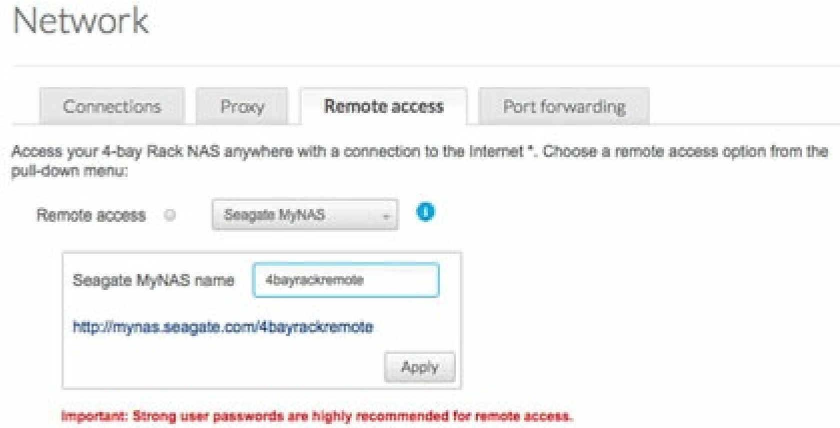


Access your 4-bay Rack NAS anywhere with a connection to the Internet *. Choose a remote access option from the pull-down menu:

Remote access: Disabled

*Remote access is only available ... ntly LAN 1).

3. Type a name for the NAS OS device in the **Name** field. The name should be different than the NAS OS device’s network name.



Access your 4-bay Rack NAS anywhere with a connection to the Internet *. Choose a remote access option from the pull-down menu:

Remote access: Seagate MyNAS

Seagate MyNAS name: 4bayrackremote

http://mynas.seagate.com/4bayrackremote

Important: Strong user passwords are highly recommended for remote access.

4. Choose **Apply**. NAS OS will query the MyNAS server to see if the name is available. If so, a message appears confirming the connection.

If the name is already chosen, type a new one and choose **Apply**.

## Failed connection

If you receive an error that the NAS is unable to connect to the Internet:

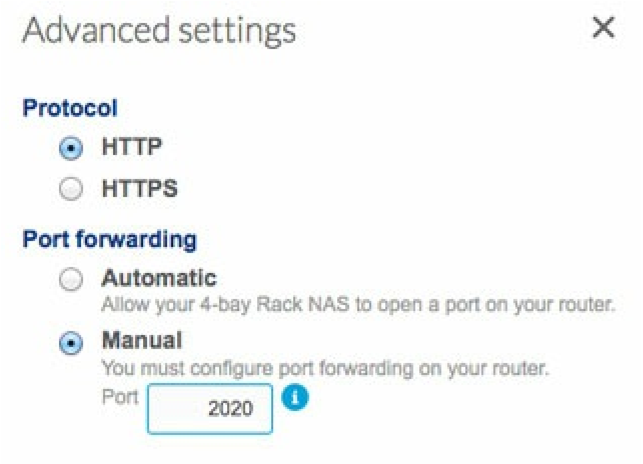
- Check if a proxy server is required to access the Internet. Contact your network administrator or Internet provider then review Network for further instructions on how to add your proxy server's address.
- Port forwarding may be required on your router. See the steps below.

## Router

If the issue is related to your router, you will need to access its administration page in order to forward a port (by default, 8080). Once the port is opened for the NAS, MyNAS can gain access to it anywhere with a connection to the Internet. From the router's administration page, select its port forwarding tab to assign a port to the NAS. Refer to your router's documentation for details.

Once a port has been selected on your router, you must assign the port on the NAS:

1. Go to **NAS OS** > **Device Manager** > **Network** > **Remote access**.
2. Pass the cursor next to the **Name** field to enable the edit pull-down menu.
3. Choose **Advanced settings**.
4. In the dialogue window, choose **Manual**.



Advanced settings ×

Protocol

● HTTP

○ HTTPS

Port forwarding

○ Automatic
Allow your 4-bay Rack NAS to open a port on your router.

● Manual
You must configure port forwarding on your router.
Port 2020

5. Enter the port you forwarded on your router.
6. Choose **Apply**.

# Using MyNAS remote access

Once MyNAS is configured, type your NAS's URL into any browser: http://mynas.seagate.com/name.

The *name* is the name selected on the remote access page and not the NAS's network name.

After entering the URL, you are prompted to log in to NAS OS. Enter the username and password created by the administrator in **NAS OS** > **Users**.

Once logged in, an administrator can access NAS OS to administer the NAS. Users and administrators can use File Browser to upload and download files (see File Browser).

# Getting Help

Review the list of troubleshooting topics below for answers to questions that might arise during the installation and operation of your Seagate product.

Additional technical assistance for Seagate products is available online at Seagate support.

## Software updates

### The NAS's automatic update does not seem to be working.

### Q: Does your NAS OS device have access to the Internet? Do you use a proxy server to access the Internet?

A: Seagate frequently releases firmware updates to improve the functionality of products. The automatic update on the Settings page will alert you to update your device when new firmware is available. In order to search for and download the most recent firmware, the NAS OS device must have access to the Internet. Confirm that it has access to the Internet or, if necessary, add your proxy server to the NAS OS device's Network settings (see Network for further details).

If automatic update is not available or experiencing problems, the administrator can follow the steps below:

1. Create a private share with read+write access for the administrator.
2. Download the most recent NAS OS capsule for your product. Go to the Seagate support page and enter your product. The most recent firmware capsule should be available for download.
3. While the capsule is downloading, mount the private share on your computer.
4. On the root level of the private share, create a folder called **Update** (case-sensitive).
5. Copy the capsule into the folder **Update**.
6. Reboot the NAS OS device.

The update will run automatically.

## Troubleshooting topics

## Troubleshooting the network connection

### Shares do not appear on the network.

Q: Is the NAS's power supply connected and is the status light on?
A: Make sure that the power supply is properly connected; that the system has been powered on; and that

the outlet is powered on or has a sufficient supply of power.

Q: Is the status light on the front of the device flickering for an inordinate period of time?
A: See LED Behavior and Device Buttons for details.

Q: Did you follow the correct installation steps?
A: Review your NAS OS device's user manual and quick start guide.

Q: Are both ends of the Ethernet cable firmly connected?
A:

- Disconnect the Ethernet cable, wait 10 seconds and then reconnect it.
- Ensure that the interface connectors are properly aligned. The Ethernet cable can only be inserted one way.
- Check that the Ethernet connectors are straight and fully seated in the Ethernet ports.

Q: IP address problem?
A: By default the NAS OS device is configured to retrieve its IP address from a DHCP server. If a DHCP server manages your network and you cannot access your NAS, try checking your DHCP server's log. To find the IP address for your NAS, run Seagate Network Assistant (see Seagate Network Assistant). If no DHCP server is detected, the product will run APIPA to assign itself an IP address. Additionally, confirm that your computer is connected to the same network as the NAS OS device.

Q: How can I find the public IP address for advanced features such as offsite backups and remote FTP access?
A: You can find the public IP address at http://www.whatismyip.com/. You must use a computer connected to the same router as the NAS.

## A user does not have access to NAS OS or shares.

Q: Has the administrator created an account for the user?
A: In order for a user to access NAS OS, two conditions must be met:

1. The administrator must create and provide the user with a username and password
2. The NAS OS device must be connected to the network via Ethernet for users to access the shares.

## I cannot access my account. I enter my login and password and receive an error message.

Q: Is your password correct?
A: If you added an email address (see Users) and configured the SMTP server (see Notifications ), you can reset your password. To do this, click on the **Can't access your account**? link on the login page. Follow the instructions to complete the reset. *User*: If you cannot recover the password, contact the NAS OS device’s administrator. *Administrator*: If you cannot recover the password, contact the alternate NAS administrator. If you are the sole administrator for the NAS, you can revert the NAS to its factory settings (see NAS OS Rescue and Repair).

### I've noticed a delay in accessing the shares.

Q: Are you transferring multiple files simultaneously, using the download feature, or synchronizing the RAID?
A: Running all or some of the following operations at once can impact NAS performance: accessing shares; file transfers; downloads; synchronizing the RAID. Enabling the UPnP service can also slow performance due to media indexing. For information on services, see Services. To review CPU performance, go to Monitoring (see Monitoring).

## Troubleshooting the multimedia server

### I cannot see the media files stored on the NAS OS device.

Q: Are the media files stored on a public share? Is the multimedia service active?
A: UPnP AV devices can discover media files stored on public shares. Certain devices may have difficulty locating files on a private share or, you will be prompted for a password. Make certain that the multimedia service is enabled in NAS OS (see Media Server and Services ).

### iTunes

Q: Some files appear in my iTunes™ shared playlist, but some do not.
A: The iTunes Server Service supports certain file types. See the iTunes website for further details:http://www.apple.com/itunes/

Q: I've activated the NAS OS device's iTunes service in Services, but I don't see its machine name in iTunes.
A: In iTunes preferences, make certain that the box next to **Shared Libraries** is checked.

Q: Why aren't files stored on the NAS OS device appearing in iTunes?
A: iTunes Server Service will only access public folders. Therefore, put your music on public folders if you wish to play it using iTunes.

### UPnP/DLNA-Compatible Game Consoles and Set Top Boxes

Q: Some files stored on the NAS OS device appear on my UPnP/DLNA compatible device, but others do not.
A: Each UPnP/DLNA media player has unique file type restrictions. See their respective websites and documentation for complete lists of compatible file types.

## Troubleshooting expansion devices

### I connected a USB hard drive to the enclosure, but it does not appear on the Storage page.

Q: Is the hard drive's file system supported by NAS OS?
A: NAS OS recognizes external hard drives with the following file systems: FAT32, NTFS, HFS+, EXT2, EXT3,

EXT, and XFS. If your hard drive's file system is not listed here, reformat it and reconnect it to the NAS.

## I can't copy a file from a share to the DAS connected to my NAS.

Q: Is the DAS formatted in FAT32 and is the file larger than 4GB?
A: Files larger than 4GB cannot be transferred to a FAT32 volume.

## Hard drive noise and VGA monitor

## I think that the hard drive is making unusual noises.

Q: Is the sound "soft clicking" or "hard clicking"?
A:

- Soft clicking can be the normal sound of the hard drive working. If the hard drive is functional, this is normal. Hard drives do not typically give an indication of any problems prior to failure, so it does not mean it is about to fail if the hard drive is making a clicking sound and still functioning. You can check the status of your hard drives by running a SMART test (see Monitoring).
- Hard clicking is a very noticeable sound, and is akin to hearing metal-on-metal impacts. This behavior is usually indicative of a physical failure. If nothing traumatic happened to the hard drive prior to this starting, consider it to be soft clicking, and troubleshoot the problem as suggested above.

## The VGA monitor that I connected to the NAS appears to be receiving a signal but the screen is black (applies to select NAS).

Q: How long has the VGA monitor been connected to the NAS?
A: The VGA signal reverts to energy saving mode within a few minutes. If the monitor appears to be receiving a signal but no image is present, try to connect a USB keyboard to one of the NAS's USB ports. Tap on one of the keys to view the NAS's VGA signal.

## Troubleshooting the active directory (AD)

The numbered list below provides general troubleshooting recommendations to resolve problems with AD.

### *NAS OS*

- Confirm that your NAS is running the latest NAS OS firmware.
- Check Monitoring to review CPU usage (see Monitoring). You can experience AD connection problems if the CPU is running high. Actions or jobs that can burden the CPU include:
  - RAID synchronization (in this case, wait until the RAID is built)
  - Multiple download jobs are running (stop or wait until download is finished)
  - Multimedia re-indexing (disable UPnP)
  - Backup jobs are running (stop or wait until backup jobs are finished)
  - Multiple simultaneous data transfers to/from the NAS from computers on the network (wait until the transfers are complete)
- Make sure the product is assigned the correct date, time, and time zone. A time discrepancy of more than five minutes between the domain and the product may prevent or cause disruptions to the AD

connection. This tolerance is defined in Domain Controller Policy, and the default value is usually five minutes.
- Make sure that the DNS server address provided to the NAS is a domain DNS, not an Internet DNS provided by an Internet service provider (see Network). The NAS must connect to the local network domain, not to a server on the Internet. Therefore, make certain that the NAS is assigned an IP address by the DNS server on the local network. To verify that the NAS is using a DNS IP address, try to ping the DNS server from a computer on the same network. **Settings > Workgroup/Domain**:
  - Enter the domain's Full Qualified Domain Name (FQDN). For example: **directory-example.domain.com** (Active Directory Users and Computers Tool on Primary Domain Controller)
  - Administrator login: The AD's administrator username.
  - Administrator password: The AD's administrator password.
- Advanced criteria (optional).
  - **Server Name** is the Domain Controller Host Name
  - **Server IP** is the Domain Controller IP

## Active directory

The AD administrator can check the following:

- Verify if Kerberos Server and Time Server are registered in the domain DNS, allowing the NAS to connect. Kerberos Server and Time Server need to be accessible to the NAS, as these servers are involved in the joining process.
- Confirm that the machine name object is placed in the right container (not the default "computer" container) and check access rights for the machine name (such as who can log on). If necessary, delete the machine name in order to reset the object in AD. The domain administrator can create a computer account in AD and place it in the right container prior to joining the NAS to the domain (the computer account name is the NAS's name).
- Sub-domains can create problems when joining a domain. Confirm that the proper domain is being used and review the machine name object location/rights. As well, see if the user belongs to a different sub-domain. If so, review the user's rights to determine if there is an authorization conflict that prevents access to the NAS.

# Maximum Elements by Feature and NAS

The table below provides the maximum amount of elements allowed for specific features.

| Feature | 4-bay Rackmount NAS | NAS 2bay \| 4 bay | NAS Pro 2bay \| 4 bay \| 6bay | 8-bay NAS Rackmount NAS |
|---|---|---|---|---|
| Users | 2048 | 2048 | 2048 | 4096 |
| Groups | 256 | 256 | 256 | 512 |
| Shares | 256 | 256 | 256 | 512 |
| iSCSI Targets | 32 | 10 | 32 | 64 |

| | | | | |
|---|---|---|---|---|
| Volumes | 4 | 2 \| 4 | 2 \| 4 \| 6 | 8 |
| Volume size | 108TB | 16TB | 108TB | 108TB |

# NAS OS Rescue and Repair

The NAS OS Rescue tool is preconfigured on a USB key for Rackmount NAS OS devices and on the motherboard for Desktop NAS OS devices. In addition to installing NAS OS, it can act as a bootable rescue tool to help you troubleshoot technical problems. The NAS OS Rescue includes three recovery options:

- **Recover data**: Enable FTP Access to the data on your NAS OS device. Once enabled, you can use FTP client software or a web browser to back up the data stored on your NAS.
- **Restore to factory settings**: Reset your NAS OS device to its factory default while attempting to preserve the shares and data. Seagate cannot guarantee that all your data will be saved. Factory default includes the reversion of all NAS OS parameters (e.g. Users, Shares, Network, etc.) to their original states.
- **Format the drives and install NAS OS**: The Installer will format the NAS's hard drives before reinstalling NAS OS. Since all data will be deleted during the format, Seagate highly recommends that you back up your files before selecting this option.

## Rackmount NAS

**Note for NAS OS devices shipped with NAS OS 3**: The NAS OS 3 installer is available on the USB key shipped with your NAS OS device. You must download the most recent version onto the USB key before following the steps below. Running the NAS OS 3 installer on a device that runs NAS OS 4 can have unwanted consequences. See the instructions below to update the USB key.

### Prepare for a rescue and repair

To connect to the Installer, you will need the NAS OS device’s MAC address. Your NAS OS device has two MAC addresses, one for each LAN port (see the hardware user manual for your device). You may use either MAC address for the installer.

You have multiple options for finding the MAC address:

- Check the MAC address label on the NAS OS device.
- Connect a VGA monitor to the NAS's VGA port.
- Launch Seagate Network Assistant (see Seagate Network Assistant).

### VGA monitor

While not obligatory, you can connect a compatible monitor to the NAS before following the recovery steps. Doing so will help you confirm that the NAS boots from the USB key. You can also review the device's IP and

MAC addresses.

The VGA signal reverts to energy saving mode within a few minutes. If the monitor appears to be receiving a signal but no image is present, try to connect a USB keyboard to one of the NAS's USB ports. Tap on one of the keys to view the NAS's VGA signal.

# Seagate Network Assistant

If you do not see the NAS OS device in Seagate Network Assistant, confirm that your NAS is:

- Connected to the same network as the computer you are using. In certain configurations, the NAS is connected to two separate networks.
- Connected to the same network as the computer you are using via the LAN 1 Ethernet port. Seagate Network Assistant requires that LAN 1 act as the primary Ethernet port for your NAS.

If you still do not see your device in Seagate Network Assistant, follow the instructions below:

1. Launch Seagate Network Assistant.
2. Select **Preferences**
   - *Windows*: Right-click on the Seagate Network Assistant icon in the system tray.
   - *Mac*: Click on the Seagate Network Assistant icon in the menu.
3. Enable IPConf Support by clicking on **Activate**.

# Rescue and repair steps

## Step 1: Update the USB key

The included USB key allows you to boot the NAS OS device and run the NAS OS installer. However, before using the USB key, it is highly recommended that you download a more recent version of the Installer as it may have been updated since you received your NAS.

**Note on download**: The software that you download is not NAS OS. Rather, it is a utility to install the NAS OS Installer onto the key so that you can install or repair the NAS OS.

To update the USB key:

1. Insert it into a USB port on a computer with a connection to the Internet.
2. Launch an Internet browser and enter the following address: http://www.seagate.com/naskey.
3. Follow the on-screen directions to update the software on the key.
4. Eject the key from your computer.

## Step 2: Back up and power off the NAS OS device

The NAS OS installer will attempt to repair or reset the NAS OS. To guarantee that data stored on the NAS is preserved, Seagate highly recommends that you back up all shares before moving forward with the Installer. If you cannot access the NAS OS volumes, the Rescue provides an option to retrieve data via FTP.

Following the backup (if applicable), turn the NAS off. If you have access to NAS OS, use the power icon on the upper right of the window to select **Shut down**. Otherwise, apply a short push to the power button.

### Step 3: Connect the USB key and boot the NAS

1. Connect the USB key to one of the USB ports on the NAS.
2. Push the power button to boot the NAS.

### Step 4: Launch the NAS OS Installer

1. Go to http://discover.seagate.com.
2. Choose **Find**.
3. Select your NAS and choose **Connect**.
4. Enter the NAS's MAC address and choose **Connect**.

Select an option and follow the on-screen prompts to complete the Rescue. The NAS OS Installer may perform a file system check (*fsck*) to determine if the device was improperly powered off or crashed, causing an inconsistent state for NAS OS. The fsck will attempt to repair or recover damaged system files.

# Desktop NAS

## Prepare for a rescue and repair

### Back up the NAS device

The NAS OS Rescue will attempt to repair or reset NAS OS. To guarantee that data stored on the NAS is preserved, Seagate highly recommends that you back up all shares before moving forward with the Installer. If you cannot access the NAS volumes, the Rescue provides an option to retrieve data via FTP.

Following the backup (if applicable), turn the NAS off. If you have access to NAS OS, use the power icon on the upper right of the window to select Shutdown. Otherwise, apply a short push to the power button.

### Recovery button

The NAS OS Rescue tool is enabled upon booting the NAS by simultaneously pushing the Recovery and power buttons. The recovery button is located on the back of the NAS within a small recessed niche. To push the recovery button, you will need a thin pointed object such as a paperclip or a small screwdriver. See your NAS OS device's hardware user manual for details.

## MAC address

Once it is enabled, the NAS OS Rescue prompts you for the NAS OS device's MAC address. Your NAS OS device has two MAC addresses, one for each LAN port. Check the MAC address labels on the back of your device and note one for the rescue.

## Perform a rescue

1. Confirm that users on the network are not accessing the NAS.
2. If the NAS is powered on, use NAS OS to shut down the NAS.
3. Use a thin pointed object (e.g. paperclip, thin screwdriver, etc.) to push the recovery button.
4. Hold the recovery button while pushing the power button. Continue to push the recovery button for five seconds.
5. Wait for the LED to turn solid.
6. From a computer on the network, launch a web browser and enter http://discover.seagate.com.
7. Choose **Find**.
8. Select your NAS and choose **Connect**.
9. Enter the NAS’s MAC address and choose **Connect**.
10. Choose an option and follow the on-screen prompts to complete the Rescue.