



## ADMINISTRATION GUIDE

**Cisco Small Business**

NSS 322, NSS 324, and NSS 326 Smart Storage

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

<b>Chapter 1: Introducing the NAS</b>	<b>8</b>
Benefits	8
Logging In to the NAS	9
Using the Help	9
Approved Vendor List for Drives and UPS Compatibility	10
<b>Chapter 2: Getting Started</b>	<b>11</b>
Before You Begin	11
Getting to Know the NSS 300 Series Smart Storage	12
NSS 322	12
NSS 324 and NSS 326	15
Installing the NSS 322, NSS 324, and NSS 326	19
Placement Tips	19
Installing the Disk Drives	19
Locking and Unlocking the Disk Trays	22
Connecting the Equipment	23
Verifying the Hardware Installation	24
Starting NAS Configuration	24
Windows Operating System	25
Mac OS X or Linux Operating System	25
System Configuration Using the Windows Setup Wizard	25
System Configuration Using the LCD Display	30
System Configuration Using Mac OS X or Linux	32
Mapping a Network Drive	33
Mapping a Network Drive from the Setup Wizard	33
Mapping a Network Drive From Windows	35
Installing the Client Utility for Windows	35
Install the Tool	36
Run the Tool From the CD	36
Remove or Repair the Tool	37
Accessing the Management GUI Using a Web Browser	37

Suggested Next Steps	38
Set Up Services	38
Set Up Backup	38
Set Up Network Shares	39
Reset Network Settings and Password	39
Inline Power Switch Module	39

## Chapter 3: Managing the System41

Status	41
System Information	42
System Service	43
Resource Monitor	46
View Logs	47
Administration	50
General Settings	50
Network	57
Hardware	66
Security	68
Notification	72
Power Management	77
Network Recycle Bin	79
Backup System Settings	80
System Logs Settings	82
Firmware Upgrade	90
Restore to Factory Default	91
Network Service Discovery	92
Users	95
User Groups	100
Disk Management	103
Volume Management	104
RAID Management	109
HDD SMART	112

Encrypted File System	115
iSCSI	115
Virtual Disk	118
Network Shares	118
Share Folders	119
Quota	122
Network Services	124
Microsoft Networking	124
Apple Networking	127
NFS Service	128
FTP Service	129
Telnet/SSH	131
SNMP Settings	132
Web Server	134
Applications	135
Web File Manager	136
Accessing the Web File Manager	137
Using the Web File Manager	138
Multimedia Station	141
Download Station	142
Accessing the Download Station	143
Using the Download Station	144
iTunes Server	146
UPnP Media Server	147
MySQL Server	148
PKG Plugins	149
Syslog Server	150
RADIUS Server	153
Backup	157
External Drive	158
USB One Touch Copy	159
Remote Replication	160

Time Machine	162
External Device	163
External Storage Device	164
UPS Settings	165
<b>Chapter 4: Configuring the NAS for Active Directory Authentication</b>	<b>168</b>
Before You Begin	168
Joining the NAS to Your Domain	169
Configuring Date and Time	169
Configuring DNS Settings	170
Configuring Microsoft Networking	171
<b>Chapter 5: NAS Maintenance</b>	<b>175</b>
Restart or Shut Down the NAS	176
Hardware System Reset	176
Basic System Reset (3 seconds)	178
Advanced System Reset (10 seconds)	179
Disk Failure or Malfunction	179
Power Outage or Abnormal Shutdown	181
System Software Abnormal Operation	181
System Temperature Protection	181
Product Battery Replacement	182
<b>Chapter 6: Troubleshooting Abnormal RAID Operation</b>	<b>183</b>
Before You Begin the Troubleshooting Process	183
Troubleshooting Abnormal RAID Operation of Your NAS	184
<b>Chapter 7: Using the LCD Display</b>	<b>186</b>
System Configuration Using the LCD Display	186
Viewing System Information Using the LCD Display	190
TCP/ IP	190

Physical Disk	191
Volume	192
System	193
Shut Down	193
Reboot	194
Password	194
Back	195
System Messages	195

## **Appendix A: Specifications** **197**

## **Appendix B: Where to Go From Here** **199**

# Introducing the NAS

The Cisco Network Attached Storage, or NAS, is a data storage device that is connected to a network and provides network access to the data stored on it. The NAS provides centralized data storage for backup and collaboration. Users can access data from devices on the local network or from remote locations. The NAS has many data protection and high availability features to assure data is always protected.

## Benefits

The NAS is a high-performance network storage device that targets the needs of small business. There are three models of the NAS based on the number of disks that they can support internally.

- 2-Bay Desktop Network Storage System (NSS 322)
- 4-Bay Desktop Network Storage System (NSS 324)
- 6-Bay Desktop Network Storage System (NSS 326)

Each NAS model provides the following benefits:

- Next generation protocol Internet Protocol version 6 (IPv6)
- Data protection in the form of Redundant Array of Independent Disks (RAID)
- UPnP DLNA Media Server
- Command line remote access
- iSCSI target feature
- Email or SMS alert integration for remote notification
- One Touch backup button on the front of the NAS
- Ability to transfer and sync data connected to USB devices



- WebDAV/HTTP access to shares
- Included applications, such as WordPress, and the capability to have more added.

## Logging In to the NAS

You can log in to the NAS from your web browser.

**NOTE** You must know the IP address of your NAS log in. If your NAS is equipped with an LCD display, you can find it there. Otherwise, you can determine the IP address from the device that issued the IP address to the NAS.

To log in to your NAS:

---

**STEP 1** Start a web browser. In the Address bar, enter the IP address of the device on port 8080: for example, `http://192.168.0.100:8080`.

**STEP 2** When the login window opens, enter the administrator account username and password.

The default username is **admin**. The default password is **admin**.

Username and password are case sensitive.

**STEP 3** If necessary, choose your language from the Language menu.

**STEP 4** Click **SSL Login** to login using SSL.

**STEP 5** Click **Login**.

**NOTE** If you are logging in to the NAS for the first time, you will be prompted to change the admin password.

---

## Using the Help

Online, content-sensitive help is built-in to the NAS interface and is always available to help you understand the rich features of the NAS.

---

**NOTE** The term “content-sensitive help” means you have instant access to specific help content regarding the window that is currently opened. This makes it quicker to find the answers that you need.

To access content-sensitive, online help:

- 
- STEP 1** Go to a window for which you desire online help.
  - STEP 2** From the top right of the open window, click **Help**. A new help window opens for and provides online help information for that specific feature.
  - STEP 3** After reading online help, you can close the help window.
- 

## Approved Vendor List for Drives and UPS Compatibility

The *Cisco Small Business Smart Storage Approved Disk Drive List* provides recommendations for compatible hard drives, UPS, and external enclosure for use in the NSS 322, NSS 324, and NSS 326 Series of Network Attached Storage (NAS) products. Cisco recommends using enterprise-class hard drives that are rated for 24 x 7 applications. If you are using an external USB or eSATA drive or enclosure that is not on the AVL list, you may be able to read and write to it but for complete feature support and long term data integrity, we recommend a drive or enclosure that has been fully tested and approved.

For more information, see the *Cisco Small Business Smart Storage Approved Disk Drive List*.

## Getting Started

This chapter describes the front and back panels of the NAS, how to physically install your NAS, and how to configure your NAS using the Cisco Setup Wizard or LCD panel. If you are a new NAS user, we recommend that you to use the Setup Wizard that is available on the product CD.

The Setup Wizard will help you with:

- **Installing the Disk Drives**
- **Connecting the Equipment**
- **Starting NAS Configuration**
- **Mapping a Network Drive**
- **Installing the Client Utility for Windows**

## Before You Begin

Before you begin the installation, make sure that you have the following equipment and services:

- Internet connectivity (optional).
- Small Phillips screwdriver.
- Ethernet switch or router.
- 1-6 SATA 2.5-inch disk drives or 3.5-inch disk drives (not included with some models). It is not required that the disk drives be the same physical size.
- Uninterruptible Power Supply (UPS), with a USB connection, which is able to supply power for 10 minutes or more with at least 350 watts of capacity. Strongly recommended to provide backup power and reduce the risk of system damage after power interruptions. After the initial installation of the

NAS device, see **UPS Settings, page 165** to configure the NAS to communicate with the UPS.

- Properly grounded anti-static wrist strap (recommended).

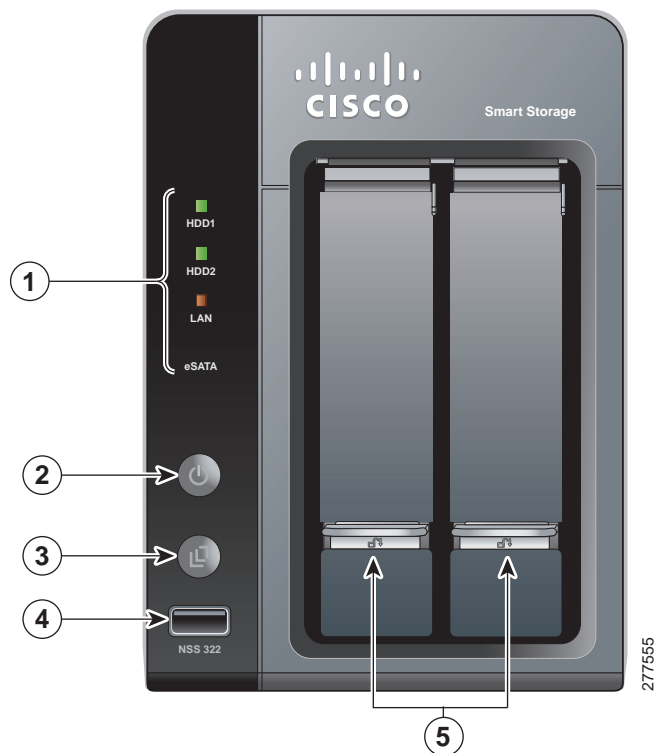
## Getting to Know the NSS 300 Series Smart Storage

The following sections describe the physical features of the NSS 322, NSS 324, and NSS 326 Smart Storage devices.

### NSS 322

The following section describes the front and back panels of the NSS 322 Smart Storage.

#### Front Panel



**NSS 322 Indicators**

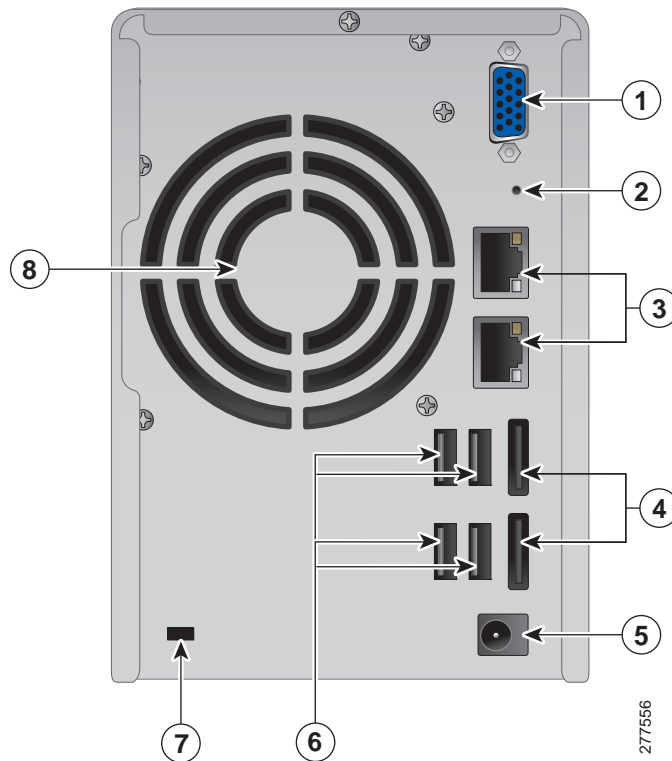
Number	LED Indicator	Description
1	HDD1, HDD2	<ul style="list-style-type: none"> <li>▪ (Green) Flashes green when the disk drive data is accessed. Solid green when the disk drive is accessible.</li> <li>▪ (Red) A hard drive read/write error occurs.</li> </ul>
	LAN	(Orange) Flashes when there is network traffic to or from the NAS. Solid orange when the NAS is connected to the network.
	eSATA	(Orange) Flashes orange when an eSATA device is being accessed.
2	Power	<ul style="list-style-type: none"> <li>▪ (Off) Disk drives are in standby mode or the device is powered off.</li> <li>▪ (Solid Green) The NAS is ready.</li> <li>▪ (Flashing Green) One or more of the following conditions apply: <ul style="list-style-type: none"> <li>- The NAS is starting up.</li> <li>- The NAS is not configured.</li> <li>- Disk drive is not formatted.</li> </ul> </li> <li>▪ (Flashing Red) The NAS is in degraded mode. One of the disk drives failed in RAID 1 configuration.</li> </ul>
		3

**NSS 322 Front Panel Buttons**

Number	Item	Description
2	Power Button	Press Power to power on or shutdown the NAS.
3	One Touch Copy Button	Press One Touch Copy to copy files to or from an external USB drive.

**NSS 322 Front Panel Buttons**

Number	Item	Description
4	USB 2.0	USB port for accessing external USB-attached storage.
5	Disk Tray Lock	Lift the silver tab up to lock the disk tray. Press the silver tab down to unlock the disk tray. See <a href="#">Locking and Unlocking the Disk Trays</a> , page 22.

**Back Panel****NSS 322 Back Panel**

Number	Item	Description
1	VGA	Console output to VGA monitor. Used for device recovery.
2	Reset	Restores the network settings and password to the factory. See <a href="#">Reset Network Settings and Password</a> , page 39.

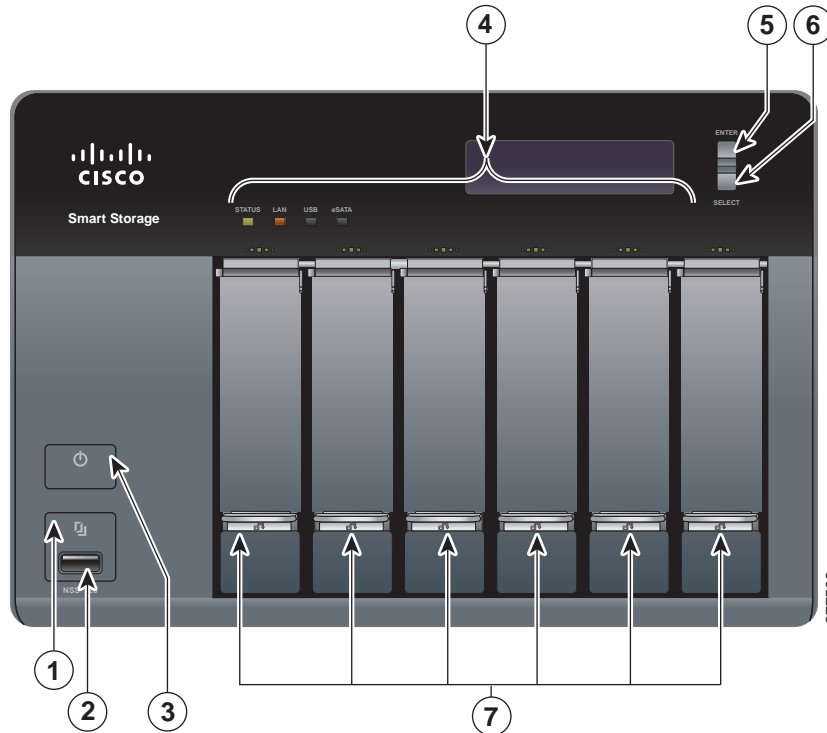
**NSS 322 Back Panel**

<b>Number</b>	<b>Item</b>	<b>Description</b>
3	Ethernet Port (2)	Dual Ethernet ports. The top LAN port is LAN1 and the bottom LAN port is LAN2.
4	eSATA (2)	eSATA ports for accessing external eSATA-attached storage. Use eSATA connector.
5	Power Connector	Connects the device to the external power adapter, which connects to a standard power outlet.
6	USB 2.0 (4)	USB port for accessing USB attached storage and UPS status.
7	Kensington Lock Slot	Attach a Kensington lock to protect the device from theft.
8	Fan	System fan.

**NSS 324 and NSS 326**

The following sections describe the front and back panels of the NSS 324 and NSS 326. The front and back panels of the NSS 326 are shown.

Front Panel



NSS 324 and NSS 326 Indicators

Number	Led Indicator	Description
1	One Touch Copy Button	(Blue) USB device is detected.
4	Status	(Red) Flashes red when the device is initialized and the disk drives are being formatted.  (Green) Flashes green when the disk drives are not initialized. Solid green when the NAS is powered up and finished booting.
	LAN	(Orange) Flashes when there is network traffic to or from the NAS. Solid orange when the NAS is connected to the network.



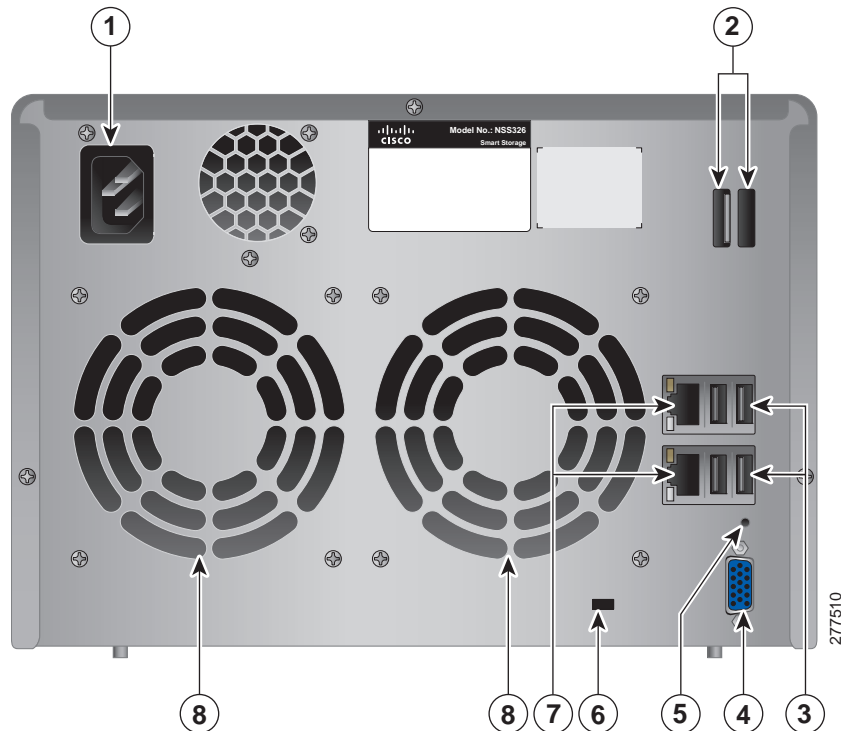
**NSS 324 and NSS 326 Indicators**

Number	Led Indicator	Description
	eSATA	(Orange) Flashes orange when an eSATA device is being accessed.
	HDD	(Green) Flashes green when the disk drive data is accessed. Solid green when the disk drive is accessible.  (Red) A hard drive read/write error occurs.

**NSS 324 and NSS 326 Front Panel Buttons**

Number	Item	Description
1	One Touch Copy	Press One Touch Copy to copy files to or from an external USB drive.
2	USB 2.0	USB port for accessing external USB-attached storage.
3	Power	Press Power to power on or shutdown the device.
5	Enter	Displays options for configuration or status such as bootup progress, disk configuration, and volume. After configuration, you can view the hostname and IP address.
6	Select	Press Select to confirm a configuration or menu option.
7	Disk Tray Lock	Lift the silver tab up to lock the disk tray. Press the silver tab down to unlock the disk tray. See <a href="#">Locking and Unlocking the Disk Trays, page 22</a> .

## Back Panel



## NSS 324 and NSS 326 Back Panel

Number	Item	Description
1	Power Connector	Connects the device to a standard power outlet.
2	eSATA (2)	eSATA ports for accessing external eSATA-attached storage. Use eSATA connector.
3	USB 2.0 (4)	USB port for accessing USB-attached storage and UPS status.
4	VGA	Console output to VGA monitor. Used for device recovery.
5	Reset	Restores the network settings and password to the factory default. See <a href="#">Reset Network Settings and Password, page 39</a> .
6	Kensington Lock Slot	Attach a Kensington lock to protect the device from theft.

**NSS 324 and NSS 326 Back Panel**

Number	Item	Description
7	Ethernet Port (2)	Dual Ethernet ports. The top LAN port is LAN1 and the bottom LAN port is LAN2.
8	Fan	System fan(s).  <b>NOTE:</b> The NSS 324 has one fan.

## Installing the NSS 322, NSS 324, and NSS 326

Please place your NSS 322, NSS 324, or NSS 326 on a desktop or flat surface.

### Placement Tips

- **Ambient Temperature**—To prevent the device from overheating, do not operate it in an area that exceeds an ambient temperature of 104°F (40°C).
- **Air Flow**—Be sure that there is adequate air flow around the device. Avoid any obstructions to air flow either in front of or behind the chassis.
- **Mechanical Loading**—Be sure that the device is level and stable to avoid any hazardous conditions. Do not place any other devices on top of the NAS.
- **Vibration/Impacts**—Be sure that the device is installed in a location where it will not be subject to vibration or impact because this can cause a mechanical shock and premature drive failures.

## Installing the Disk Drives



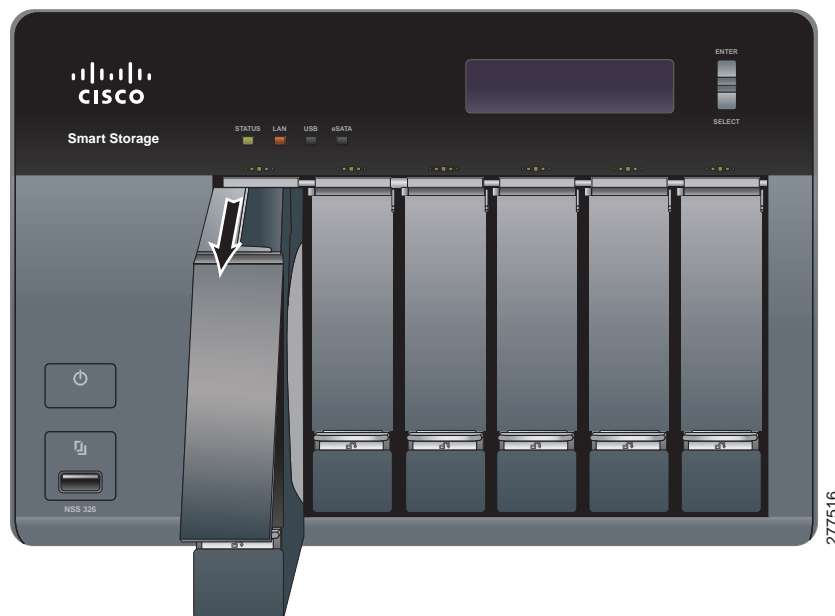
**CAUTION** When storing unused disk drives, do not stack multiple disk drives because this can cause drive failures.

When installing the disk drives, follow the suggestions in *Cisco Electrostatic Discharge and Grounding Best Practices*, located on the product CD.

To install disk drives in the NAS chassis:

- STEP 1** Remove the contents of the NAS package from the box.
- STEP 2** Place the chassis upright on a flat surface.
- STEP 3** From disk bay 1, remove the disk tray.

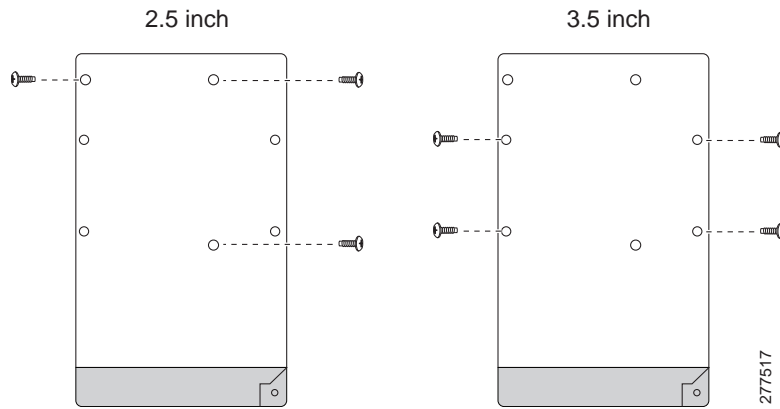
To remove the disk tray, push the silver tab down to unlock the tray, and push the lower tab to release the tray lever. Using the tray lever, pull the tray out.



- NOTE** If your device has the disk drives already installed, continue to the next section, [Connecting the Equipment, page 23](#).
- STEP 4** Position the disk drive into a disk tray. The electrical connectors of the disk drive must face toward the back of the drive tray.
- STEP 5** Attach the disk drive to the tray by inserting the disk drive screws into the four holes at the bottom of the tray and tightening them with a Phillips screwdriver.
- NOTE** Use the screws provided in the box with the device. Using other screws can cause damage to your disk or disk tray.

There are clearly marked disk holes to accommodate the following disk drives:

- 3.5-inch disk drive (use the included silver screws)
- 2.5-inch disk drive (use the included black screws)



**STEP 6** Insert the tray back in the correct sequence into the empty bay of the chassis.

**NOTE** Drive trays should not be swapped from slot to slot.

There is also an HDD sequence label included in the package contents that can be placed on the top of the chassis, showing the disk drive sequence. For example, 1-2 for the NSS 322, 1-4 for the NSS 324, and 1-6 for the NSS 326.



The HDD sequence number is also located on the inside of the disk tray.



- STEP 7** Using your thumb, apply even pressure to the middle of the tray while you insert the tray slowly and fully into position in the chassis.
- STEP 8** The disk tray lever should be in the open position.
- STEP 9** Gently push the disk tray lever down.
- STEP 10** Repeat steps 3 through 9 to install disk drives from slot 2 to slot 4 for the NSS 324 and slot 2 to slot 6 for the NSS 326.

## Locking and Unlocking the Disk Trays

An icon is located on the silver tab indicating:

- When the silver tab is up, the disk tray is locked.
- When the silver tab is down, the disk tray is unlocked.



To lock the disk tray:

- 
- STEP 1** Verify that the disk tray is fully inserted in the chassis with the disk tray lever down.
  - STEP 2** Lift the silver tab up to lock the tray.
  - STEP 3** Continue to [Connecting the Equipment, page 23](#).
- 

To unlock and remove the disk tray:

- 
- STEP 1** On the disk tray, press the silver tab down to unlock the tray.
  - STEP 2** Press the button below the silver tab to release the disk tray lever.
  - STEP 3** Using the disk tray lever, gently pull the disk tray out from the chassis.
- 

## Connecting the Equipment

To connect the NAS device to the network:

- 
- STEP 1** Connect the supplied Ethernet cable to one of the Ethernet ports on the back of the chassis.
  - STEP 2** Connect the other end of the Ethernet cable to a switch or router on your network.
  - STEP 3** Connect the supplied power cord to the Power port on the back of the chassis.

**STEP 4** Plug the other end of the power cord into a battery-backed-up outlet on the UPS, or a standard power outlet if a UPS is not being used.

**STEP 5** To start the NAS, press and release the Power button on the front panel.

Listen for one beep. Wait for one to two minutes until the device beeps another time.

The device has started successfully. The power light turns solid green when the NAS is ready to use.

## Verifying the Hardware Installation

To verify the hardware installation, complete the following tasks:

- Check the cable connections.
- Check the LED states, as described in [Getting to Know the NSS 300 Series Smart Storage, page 12](#).

If you encounter problems, consider the following tips:

- If the NAS does not recognize the disk drives, possible causes and solutions are:
  - Confirm the disk drive is supported by Cisco. See the Cisco approved vendor list at [www.cisco.com/go/smallbizsmartstorage](http://www.cisco.com/go/smallbizsmartstorage).
  - Disk tray is installed incorrectly. Try removing and reseating the disk tray.
  - Power the device off, then back on to recognize the disk drives.

**NOTE** If you need help resolving a problem, visit the Cisco Small Business Support Community at [www.cisco.com/go/smallbizsupport](http://www.cisco.com/go/smallbizsupport). For technical documentation and other links, see [Where to Go From Here, page 199](#).

## Starting NAS Configuration

Before you begin the system configuration, make sure that you have a computer that meets the following requirements:



- Internet browser connectivity to the NAS (internet connectivity optional). The following browsers are supported:
  - Microsoft Internet Explorer 7.0 or later
  - Mozilla Firefox 3.0 or later
  - Apple Safari 3.0 or later
- Supported operating systems:
  - Windows 2000, XP, Vista, Server 2003, Server 2008, Windows 7
  - Mac OS X 10.4 or later
  - Unix or Linux 2.6 or later

## Windows Operating System

If you are using a Windows operating system, you can configure the Smart Storage by using either the Setup Wizard or the LCD display located on the front panel of the device. See the following sections:

- **System Configuration Using the Windows Setup Wizard**—For more advanced users, the Setup Wizard guides you through the initial configuration settings.
- **System Configuration Using the LCD Display**—Easier and quicker installation that uses more default settings. System configuration using the LCD display is supported on the NSS 324 and NSS 326.

## Mac OS X or Linux Operating System

If you are using a Mac OS X or Linux operating system, see the following section:

- **System Configuration Using Mac OS X or Linux**

## System Configuration Using the Windows Setup Wizard

After connecting the equipment and pressing the Power button, the system takes a few minutes to initialize. Listen for one beep. Wait a minute until you hear a second beep. The power light will turn solid green. The NAS device has started successfully and you can configure the device using the First Time Installation Wizard.

**NOTE** If you receive Windows firewall warnings during this process, you may need to allow the installation application to unblock the firewall settings. If the installation does not start, you may also need to temporarily disable any security software on your computer to run the Setup Wizard.

To configure your system using the Setup Wizard:

- 
- STEP 1** Insert the product CD and from the *Welcome* window and choose your NAS model.
- The *Setup Menu* window opens.
- STEP 2** Under First Time Installation, click **Setup**.
- The *First Time Installation Wizard* window opens.
- STEP 3** Click **Next** to launch the wizard.
- The *End-User License Agreement* window opens.
- STEP 4** To accept the End-User License Agreement, check the **I accept this agreement** check box and click **Next**.
- The *Hardware Installation Guide* window opens.
- STEP 5** Click **Next** and follow the prompts to check the package contents, install the disk drives, and connect the equipment.
- NOTE** If you have already installed the disk drives and connected the equipment, click **Skip** until you reach the *System Configuration* window.
- STEP 6** From the *System Configuration* window, click **Next** to go to NAS configuration.
- The *NAS Configuration* window opens.
- STEP 7** Click **Next**.
- The *Discovering the NAS* window opens and advises when the uninitialized device is found.
- NOTE** If your device is already configured, click **Skip** to go to Map Network Drive. See [Mapping a Network Drive, page 33](#).
- STEP 8** Click **Next**.
- The *Web Configuration* window opens.
- STEP 9** The First Time Installation Wizard detects the NAS and prompts you to go through the web configuration process. From the drop-down list, select a NAS device.

**STEP 10** Click **Next** to continue. You are directed to a web configuration window to complete the settings step by step.

The *Welcome* window displays.

**STEP 11** Click **Next**.

You are redirected to a window where you can enter the name for this server.

**STEP 12** In the Server Name field, enter a name to identify the NAS device.

The server name can be a maximum length of 14 characters, which supports alphanumeric characters (a-z, 0-9) and hyphens (-). It is required that the server name begin with a letter versus a number. The server name does not accept names with a space or period (.)

**STEP 13** Click **Next**.

You are redirected to a window where you can change the administrator password.

**NOTE** The default administrator username is **admin**. The default administrator password is **admin**.

**STEP 14** Change the administrator password by entering the new password in the Password field. To verify the password, re-enter it in the Verify Password field.

**STEP 15** Click **Next**.

You are redirected to a window where you can enter the date, time, and time zone for the server.

**STEP 16** Enter the date, time, and time zone for this server. The options are:

- **Time Zone**—Select a time zone from the drop-down menu.
- **Date/Time**—Select the current date and time from the drop-down menus.
- **Synchronize with an Internet time server automatically**—To obtain time automatically from an NTP server, click this check box.
- **Server**—From the drop-down list, select the NTP server name and click **TEST** to verify status.

For example:

- time-a.timefreq.blrdoc.gov (default)
- time-b.timefreq.blrdoc.gov
- time-c.timefreq.blrdoc.gov

- **Set the server time the same as your computer time**—To synchronize the server time/clock with the time/clock on your computer, click this check box.

**STEP 17** Click Next.

You are redirected to a window where you can enter the IP address, subnet mask, and default gateway for the device.

**STEP 18** Enter the IP address, subnet mask, and default gateway for this server. You can either acquire the IP address automatically from a DHCP server or choose to configure a static IP address.

- **Obtain TCP/IP settings automatically via DHCP**—Click this check box to acquire the IP address from a DHCP server. This is enabled by default.
- Click **Use the following settings** to configure a static IP address:
  - **IP Address**—Enter an IP address for the NAS.
  - **Subnet Mask**—Enter the subnet mask of your network.
  - **Default Gateway**—Enter the default gateway address. This is typically the IP address of your router.
  - **Primary DNS Server (optional)**—Enter the IP address of the Domain Name System (DNS) server. This address is typically provided by your Internet Service Provider (ISP).
  - **Secondary DNS Server (optional)**—Enter a second DNS server.

**STEP 19** Click Next.

You are redirected to a window where you can select the services to be enabled.

**STEP 20** Select the services to be enabled. These services can also be enabled or disabled at a later time. The options are:

- **Network services**—Click the check box to enable Microsoft Networking, Apple Networking, or Unix/Linux NFS.
- **File services**—Click the check box to enable Web File Manager, FTP Service, or Download Station.
- **Multimedia services**—Click the check box to enable Multimedia Station, UPnP multimedia server, or iTunes service.
- **Web server services**—Click the check box to enable Web Server or MySQL server.

**STEP 21** Click Next.

You are redirected to a window where you can select the disk configuration.

**STEP 22** Select the disk configuration.

**NOTE** It is recommended to configure the NSS 324 or NSS 326 with RAID 5 if there are three or more disks installed.

- Disk configuration:

The following options are available:

- **Do not set disk configuration**—If you have created disk volume configuration or plan to create multiple disk configurations, select not to initialize the disk drives.
  - **Single Disk**—Uses the disk drives as single disk volumes. When a drive failure occurs, all data is lost.
  - **JBOD (Linear)**—JBOD lets you combine multiple disks of mixed capacities into a single logical storage device. The capacity of the JBOD array is the sum of the total capacities of the individual component disks (that is, it does not have the limitation of RAID 1 where you lose some capacity when using mixed sized disks). JBOD offers no performance increase compared to the component disks. It has lower reliability than the component disks, as the failure of a single disk results in the failure of the whole array.
  - **RAID 0**—Distributes data across several disks in a way that improves speed and full capacity. All data on all disks will be lost if any single disk fails.
  - **RAID 1**—Uses two disks (mirrored disks) each of which store the same data, so that data is not lost as long as one disk survives. Total capacity of the array equals the capacity of the smaller disk.
  - **RAID 5**—Combines three or more disks in a way that protects data against loss of any single disk. RAID 5 is applicable to NSS 324 and NSS 326.
  - **RAID 6**—Combines four or more disks in a way that protects data against loss of any two disks. RAID 6 is applicable to NSS 324 and NSS 326.
- File system:
    - **EXT4**—EXT4 is the successor to EXT3 and provides better performance because the EXT4 file system can support very large volumes (default).

- **EXT3**—EXT3 is commonly used in the Linux environment. EXT3 provides reliable file systems with a maximum capacity support up to 16 terabytes (TB).
- Encrypt disk volume:
  - **No**—Do not encrypt the disk volume (default).
  - **Yes**—Encrypt the disk volume using a password.

If you choose yes, the disk volume is encrypted with a password and provides an extra layer of security against the theft of data in the event that disks are stolen. File transfer performance to encrypted volumes is generally lower than non-encrypted volumes. The default encryption password is the password of the administrator account.

**STEP 23** Click **Next**.

The *Finish* window displays the server configuration.

**STEP 24** Click **Start Installation**. System begins initializing and the configuration progress is displayed.

When the configuration is complete, you are returned to the *Configuring the NAS* window in the Setup Wizard.

**STEP 25** From the *Configuring the NAS* window, click **Next** to continue to Map a Network Drive.

The *Map Network Drive* window opens. Continue to [Mapping a Network Drive, page 33](#).

---

## System Configuration Using the LCD Display

After connecting the equipment and pressing the Power button, the system boots, loads the driver, and mounts the volume. You can optionally configure the NAS device using the options in the LCD display.

**NOTE** If you have configured the NAS using the Setup Wizard, you do not need to setup the NAS using the LCD display.

**NOTE** System configuration using the LCD display is supported on the NSS 324 and NSS 326.

To configure your system using the LCD display:

**STEP 1** At the prompt **Config Disks?** in the LCD display, press **Select** to choose the disk configuration. The following options are available:

The following options are available:

- **Do not set disk configuration**—If you have created disk volume configuration or plan to create multiple disk configurations, select not to initialize the disk drives.
- **Single Disk**—Uses the disk drives as single disk volumes. When a drive failure occurs, all data is lost.
- **JBOD (Linear)**—JBOD lets you combine multiple disks of mixed capacities into a single logical storage device. The capacity of the JBOD array is the sum of the total capacities of the individual component disks (that is, it does not have the limitation of RAID 1 where you lose some capacity when using mixed sized disks). JBOD offers no performance increase compared to the component disks. It has lower reliability than the component disks, as the failure of a single disk results in the failure of the whole array.
- **RAID 0**—Distributes data across several disks in a way which that improves speed and full capacity. All data on all disks will be lost if any single disk fails.
- **RAID 1**—Uses two disks (mirrored disks) which each store the same data, so that data is not lost as long as one disk survives. Total capacity of the array equals the capacity of the smaller disk.
- **RAID 5**—Combines three or more disks in a way that protects data against loss of any single disk. RAID 5 is applicable to the NSS 324 and NSS 326.
- **RAID 6**—Combines four or more disks in a way that protects data against loss of any two disks. RAID 6 is applicable to the NSS 324 and NSS 326.

**STEP 2** After choosing the disk configuration, press **Enter**. The LCD display shows:

```
Choose <Disk Configuration>  
Yes No
```

Yes is the default.

**STEP 3** Press **Enter** to continue. The LCD display shows:

```
Encrypt Volume  
Yes No
```

No is the default. If you choose yes, the disk volume is encrypted with a password and provides an extra layer of security against the theft of data. The default encryption password is a password of the “admin” account.

**STEP 4** Press **Enter** to continue. The system configuration progress is displayed. When the configuration is complete, you will receive an IP address and default NAS device name that is shown in the LCD display

**STEP 5** Start a web browser. In the Address bar, enter the IP address of the device that is shown in the LCD display:

`http://x.x.x.x:8080`

**STEP 6** When the login window opens, enter the administrator account username and password.

The default username is **admin**. The default password is **admin**. Username and password are case sensitive.

**STEP 7** Click **Login**.

**STEP 8** Follow the prompts to change the admin password.

**STEP 9** Click **Submit**.

**STEP 10** When the login window opens, enter the administrator account username **admin** and the new administrator password.

Continue to [Mapping a Network Drive From Windows, page 35](#).

---

## System Configuration Using Mac OS X or Linux

To configure your system using Mac OS X or Linux:

---

**STEP 1** Connect the NAS to the computer directly and power on the device.

The NAS Ethernet ports support MDI/MDI-X auto-switching.

**STEP 2** Verify the IP address of your computer is configured to the same subnet as the NAS device. For example: 192.168.1.1.

**STEP 3** Open a web browser and enter the IP address of the NAS device. For example:

`http://192.168.1.50:8080`



This is the default static IP address if DHCP is not enabled. If the NAS device does not have a static IP address and if the device is not able to receive an IP address via DHCP, it will default to 192.168.1.50. If the DHCP server on your network is enabled, as soon as the DHCP server responds, the NAS device will accept an IP address even if the default static IP address is assigned.

**NOTE** If your operating system is Linux, refer to the LCD display on the front panel of the NAS device and configure the IP address to match the network. The LCD display is located on the NSS 324 and NSS 326.

**STEP 4** Follow the prompts to complete the configuration.

Continue to [Suggested Next Steps, page 38](#).

## Mapping a Network Drive

You can map a network drive either by using the Setup Wizard or from Windows.

### Mapping a Network Drive from the Setup Wizard

**NOTE** Skip steps 1-5 if you are already on the *Map Network Drive* window in the Setup Wizard.

To map a network drive from the Setup Wizard:

**STEP 1** Insert the product CD and from the *Welcome* window, click **NSS 322**, **NSS 324**, or **NSS 326** depending on which NAS device you are installing.

The *Setup Menu* window opens.

**STEP 2** Under First Time Installation, click **Setup**.

The *First Time Installation Wizard* window opens.

**STEP 3** Click **Next** to launch the wizard.

The *End-User License Agreement* window opens.

**STEP 4** To accept the End-User License Agreement, check the **I accept this agreement** check box and click **Next**.

The *Hardware Installation Guide* window opens.

**STEP 5** Click **Skip** until you reach the *Map Network Drive* window.

**STEP 6** From the *Map Network Drive* window, click **Next** to start mapping your network drive.

The *Discovering the NAS* window opens and the First Time Installation Wizard searches for your initialized NAS.

**STEP 7** When the initialized NAS is found, click **Next**.

The *Select the NAS Device* window opens.

**STEP 8** From the drop-down list, select the NAS device that you want to map as a network drive.

**STEP 9** Click **Next**.

The *Mapping Drives* window opens.

**STEP 10** From the drop-down lists, select a folder type and select a drive letter to be mapped.

Preconfigured share folders types are:

- **Public**—Network share for file sharing (default).
- **Usb**—Network share for data copy function using the USB ports.
- **Web**—Network share for Web server.
- **Download**—Network share for Download Station.
- **Multimedia**—Network share for Multimedia Station.
- **Network Recycle Bin 1**—Network share recycle bin.

**STEP 11** From the authentication login window, enter the administrator account username and password.

**STEP 12** Click **Next**.

**STEP 13** The *Mapping Success* window opens.

**STEP 14** Click **More** to map another drive or click **Next** to continue to the Client Utility Installation. See [Installing the Client Utility for Windows, page 35](#).

---

## Mapping a Network Drive From Windows

**NOTE** If you are using Windows Vista, you might receive a security warning and have to temporarily disable any security software on your computer.

To map a network drive from Windows:

**STEP 1** From the Windows desktop, click the **My Computer** icon to open My Computer.

**STEP 2** Choose **Tools > Map Network Drive**.

The *Map Network Drive* window opens.

**STEP 3** From the drop-down lists, select the drive letter to be mapped.

**STEP 4** In the Folder field, type the share name you want to map. For example:

`\\<NAS IP address>\<share name>`

**STEP 5** Click **OK**.

**STEP 6** Click **Finish**.

**NOTE** If you are prompted to enter a username and password for authentication, enter the administrator account username and password.

**STEP 7** Open Windows Explorer to view and use the network share as a local drive.

---

## Installing the Client Utility for Windows

Installing the Client Utility, or NSS Discovery Tool, is optional. The NSS Discovery Tool provides functions for you to search, configure, and manage your NAS devices.

**NOTE** The NSS Discovery Tool is only supported with Windows operating systems. If you receive Windows firewall warnings during this process, you may need to allow the NSS Discovery Tool to unblock the firewall settings.

From the NSS Discovery Tool windows, you have the following options:

- **Install the Tool**
- **Run the Tool From the CD**
- **Remove or Repair the Tool**

---

## Install the Tool

When installed to your computer, the NSS Discovery Tool acts as a standalone discovery tool. If you have numerous devices on your network, the NSS Discovery Tool detects uninitialized and initialized NAS devices.

To install the NSS Discovery Tool:

- 
- STEP 1** Insert the product CD and from the *Welcome* window, click **NSS 322**, **NSS 324**, or **NSS 326** depending on which NAS device you are installing.

The *Setup Menu* window opens.

- STEP 2** From the Setup menu and under Additional Configuration, click **Utility**.

The *NSS Discovery Tool* window opens.

- STEP 3** Click **Install** to install the NSS Discovery Tool.

The *NSS Discovery Tool Setup Wizard* window opens.

- STEP 4** Click **Next**.

The *Select Installation Folder* window opens.

- STEP 5** Click **Next** to install to the default folder or click **Browse** to install to another folder.

- STEP 6** When the *Installation Complete* window opens, click **Close**.
- 

## Run the Tool From the CD

To run the NSS Discovery Tool from the CD:

- 
- STEP 1** Insert the product CD and from the *Welcome* window, click **NSS 322**, **NSS 324**, or **NSS 326** depending on which NAS device you are installing.

The *Setup Menu* window opens.

- STEP 2** From the Setup menu and under Additional Configuration, click **Utility**.

The *NSS Discovery Tool* window opens.

- STEP 3** Click **Run**.

The *NSS Discovery Tool* window opens and shows a list of initialized NAS devices on your network. From this window, you can connect, configure, or view details for the listed devices.

**STEP 4** Click **Exit** to close the tool.

## Remove or Repair the Tool

To remove or repair the NSS Discovery Tool:

**STEP 1** Insert the product CD and from the *Welcome* window, click **NSS 322**, **NSS 324**, or **NSS 326** depending on which NAS device you are installing.

The *Setup Menu* window opens.

**STEP 2** From the Setup menu and under Additional Configuration, click **Utility**.

The *NSS Discovery Tool* window opens.

**STEP 3** Click **Remove**.

The *NSS Discovery Tool Setup Wizard* window opens.

**STEP 4** Select either of the following options:

- Repair NSS Discovery Tool
- Remove NSS Discovery Tool

**STEP 5** Click **Finish**, then **Close** when complete.

## Accessing the Management GUI Using a Web Browser

To access the GUI from a web browser:

**STEP 1** Open a web browser and enter:

**http://<NAS IP address>:8080.**

**STEP 2** When the login window opens, enter the administrator username and password.

---

## Suggested Next Steps

Congratulations, you are now ready to start using your NAS. You may wish to consider taking some of the following steps:

### Set Up Services

If you set up any services, such as network, file, multimedia or web server, you need to configure the detailed settings for the services from the corresponding administration windows. For example, from the Applications menu, you can configure the following:

- **Web File Manager**—When enabled, you can access files on the NAS device using a web browser.
- **Multimedia Station**—From the NAS, you can share photos, music, or video files over the network.
- **Download Station**—Supports HTTP and FTP download.
- **iTunes Service**—When enabled, you can find, browse, and play all the music files on the NAS using computers that are on the network and using iTunes.

For more information, see [Applications, page 135](#).

### Set Up Backup

From the Backup menu, you can configure the following:

- **External Drive**—Back up the local drive data to an external storage device. You can back up immediately, schedule a day and time to execute the backup, or set up an automatic backup.
- **USB One Touch Copy**—Configure the USB One Touch button to copy to or from an external USB drive.
- **Remote Replication**—Back up the files on the NAS to another NAS or rsync server over the LAN or Internet.

For more information, see [Backup, page 157](#).

## Set Up Network Shares

From the Network Shares menu, you can configure the following:

- **Share Folders**—Create share folders on the NAS and edit the access rights of the users and user groups to these share folders.
- **Quota**—Enable the quota settings for all the users and specify the quota size they are allowed to use on each disk volume of the NAS.

For more information, see [Network Shares, page 118](#).

## Reset Network Settings and Password

You can restore the network settings and password for your NAS device using the reset button located on the back panel. The NAS device should be powered on for this procedure. Using a paper clip, press the reset button for 3 seconds, until the NAS beeps.

The following settings are reset to default:

- System administration password: **admin**
- Network settings:
  - Obtain TCP/IP settings automatically via DHCP
  - Disable Jumbo Frame
  - System management port - 8080
- System tools: IP filter settings - Allow all connections
- LCD panel password: (blank)

## Inline Power Switch Module

An inline switch module is provided for customers who wish to have a convenient means of turning the device off during extended inactivity. The switch module is provided in compliance with the requirements of the *European Union Commission Regulation No 1275/2008*. The device is also fully functional without the switch module by plugging the power cord directly into the device. However, the switch module must be used to comply with the European Union regulations.

To use the inline switch module to power off the NAS, you should first press the front panel Power button to shut down the NAS. Wait for the device to fully shut down before connecting and using the inline switch. Failure to do so may result in data loss.

The following shows the AC inline switch module for the NSS 324 and NSS 326.



The following shows the DC inline switch module for the NSS 322.





# Managing the System

This chapter describes how to configure and manage your system Cisco Small Business Smart Storage. The following sections are included:

- **Status**
- **Administration**
- **Network Shares**
- **Network Services**
- **Applications**
- **Backup**
- **External Device**

## Status

This section describes how to check the status of the system and includes the following topics:

- **System Information**
- **System Service**
- **Resource Monitor**
- **View Logs**

## System Information

The *Status > System Information* window displays general information such as system information, port status, and hardware information.

The screenshot shows the Cisco Smart Business NSS 322 Smart Storage administration interface. The left-hand navigation pane includes sections for Overview, Status, System Information, Administration, Disk Management, Network Services, Applications, Backup, and External Device. The 'System Information' section is active, displaying the following data:

**System Information**

- Server Name: nasbd878
- Firmware Version: 1.0.0
- Firmware MD5 Checksum: e73a4e38dctf699e96079f5de031c7
- System Up Time: 1 Day 2 Hour 44 Minute(s)
- Object ID: 1.3.6.1.4.1.9.6.1.41.322.1
- PID VID: NSS322-V01
- Serial Number: NBP09450005EC01

**Port Status**

Port No.	Port Status	IP Address	MAC Address	Packets Received	Packets Sent	Error Packets
Ethernet 1	Down	192.168.15.103	00:08:9b:bd:a8:78	0	0	0
Ethernet 2	Up	192.168.15.103	00:08:9b:bd:a8:78	41451	10287	0

**Hardware Information**

- CPU Usage: 1.9 %
- Total Memory: 999.6 MB
- Free Memory: 835.6 MB
- CPU Temperature: 41°C/105°F
- System Temperature: 48°C/120°F
- HDD 1 Temperature: 37°C/98°F
- HDD 2 Temperature: 35°C/95°F
- System Fan Speed: 1153

### System Information

- **Server Name**—Name of the NAS.
- **Firmware Version**—Firmware version of the NAS.
- **Firmware MD5 Checksum**—MD5 checksum of the current firmware. This number is useful to verify the integrity of the firmware.
- **System Up Time**—Time that the NAS has been in continuous operation in days, hours, and minutes.
- **Object ID**—Object ID of the NAS, used in SNMP applications.
- **PID VID**—Product identifier (PID) and Version identifier (VID) of the NAS.
- **Serial Number**—Serial number of the NAS.

### Port Status

- **Port No.**—Number of the Ethernet port.

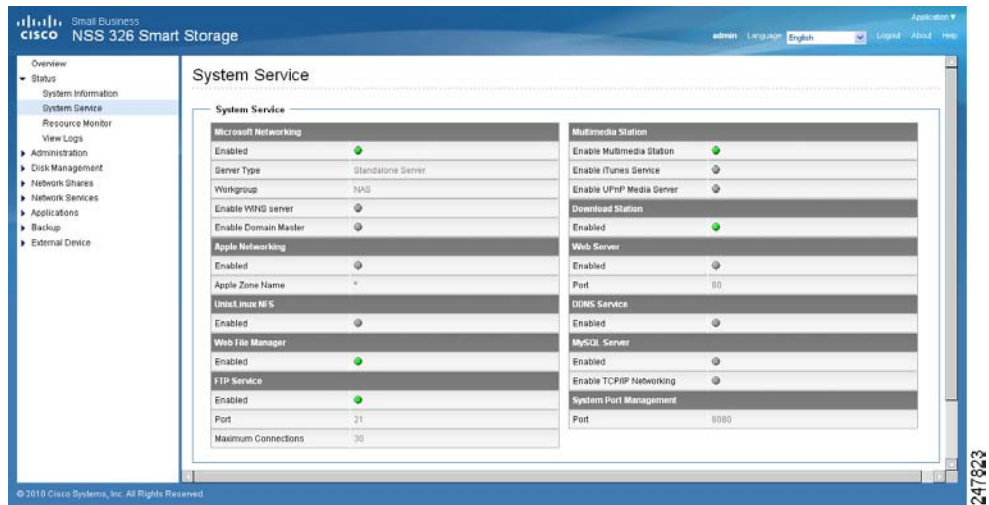
- **Port Status**—Status of the Ethernet port. *Down* indicates that the port is not connected. *Up* indicates that the port is connected and operational.
- **IP Address**—IP address of the Ethernet port.
- **MAC Address**—MAC address of the Ethernet port.
- **Packets Received**—Number of packets received by the Ethernet port.
- **Packets Sent**—Number of packets sent by the Ethernet port.
- **Error Packets**—Number of packets detected with errors.

#### Hardware Information

- **CPU Usage**—Percentage of load on the CPU in the NAS.
- **Total Memory**—Total RAM memory in the NAS.
- **Free Memory**—Amount of free RAM memory in the NAS.
- **CPU Temperature**—Temperature of the CPU in the NAS.
- **System Temperature**—Internal system temperature of the NAS.
- **HDD Temperature**—Temperature of each hard drive in the NAS.
- **System Fan Speed**—RPM of each system cooling fan in the NAS.

## System Service

The *Status > System Service* window displays the current system service settings and status. Status shows a green color dot when the system service is enabled.



**Microsoft Networking**—This service is configured from the *Network Services > Microsoft Networking* window.

- **Enabled**—Status of the Microsoft Networking file service.
- **Server Type**—Displays either Standalone Server or AD Domain Member networking type.
- **Workgroup**—Workgroup to which the NAS belongs.
- **Enable WINS Server**—Status of WINS server.
- **Enable Domain Master**—Status of the Domain Master.

**Apple Networking**—This service is configured from the *Network Services > Apple Networking* window.

- **Enabled**—Status of the Apple Networking protocol.
- **Apple Zone Name**—Name of the Apple zone.

**Unix/Linux NFS**—This service is configured from the *Network Services > NFS Service* window.

- **Enabled**—Status of the Unix/Linux NFS service.

**Web File Manager**—This service is configured from the *Applications > Web File Manager* window.

- **Enabled**—Status of the Web File Manager service.

**FTP Service**—This service is configured from the *Network Services > FTP Service* window.

- **Enabled**—Status of the FTP service.
- **Port**—Port number for FTP service.
- **Maximum Connections**—Maximum number of all FTP connections.

**Multimedia Station**—This service is configured from the *Applications > Multimedia Station* window.

- **Enable Multimedia Station**—Status of the Multimedia Station service.
- **Enable iTunes Service**—Status of the iTunes service. This service is configured from the *Applications > iTunes Service* window.
- **Enable UPnP Media Server**—Status of the UPnP Media Server service. This service is configured from the *Applications > UPnP Media Service* window.

**Download Station**—This service is configured from the *Applications > Download Station* window.

- **Enabled**—Status of the Download Station service.

**Web Server**—This service is configured from the *Network Services > Web Server* window.

- **Enabled**—Status of the Web Server service.
- **Port**—Port number for Web Server service.

**DDNS Service**—This service is configured from the *Administration > Network > DDNS* window.

- **Enabled**—Status of the DDNS Service.

**MySQL Server**—This service is enabled, disabled, and configured from the *Applications > MySQL Server* window.

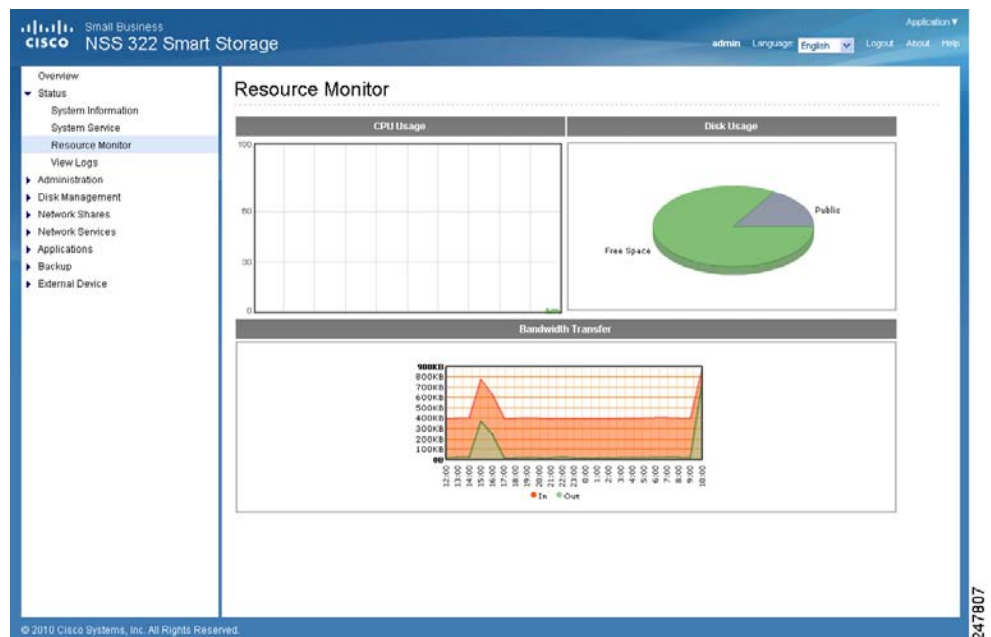
- **Enabled**—Status of the MySQL Server service.
- **Enable TCP/IP Networking**—Status of TCP/IP Networking. This is enabled from the *Administration > Network* window.

**System Port Management**—The System Port is configured from the *Administration > General Settings > System Administration* window.

- **Port**—Value of the System Port.

## Resource Monitor

The *Status > Resource Monitor* window displays the CPU usage, disk usage, and bandwidth transfer statistics.



- **CPU Usage**—Shows the percentage of CPU usage over time.
- **Disk Usage**—Shows the amount of free and used space on the NAS.

**NOTE** If a default share is less than 3 percent of the total space of a RAID array, the disk usage will not display that share in the Disk Usage image. The percentage will display in the image if the disk usage of a default share is over 3 percent.

- **Bandwidth Transfer**—Shows the amount of in-coming and out-going bandwidth traffic over time.

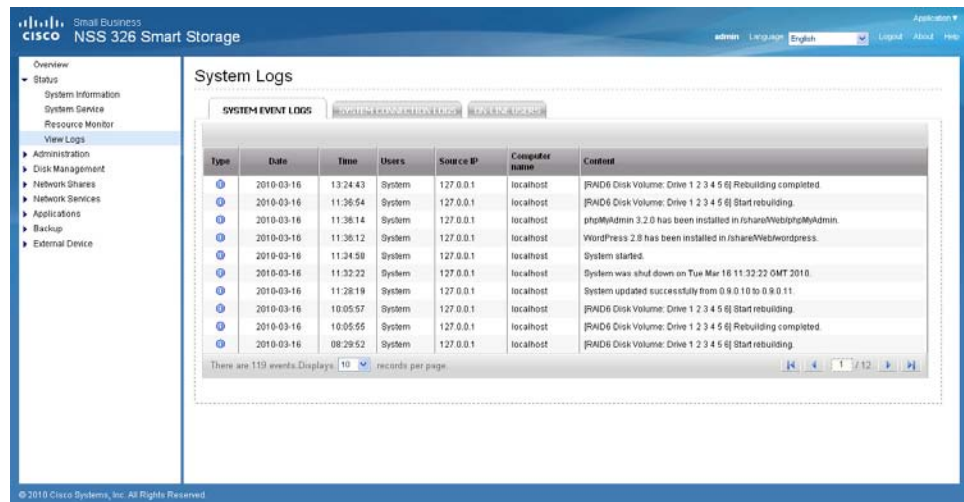
## View Logs

This section provides descriptions for the system logs and includes the following sections:

- **System Event Logs**
- **System Connection Logs**
- **On-Line Users**

### System Event Logs

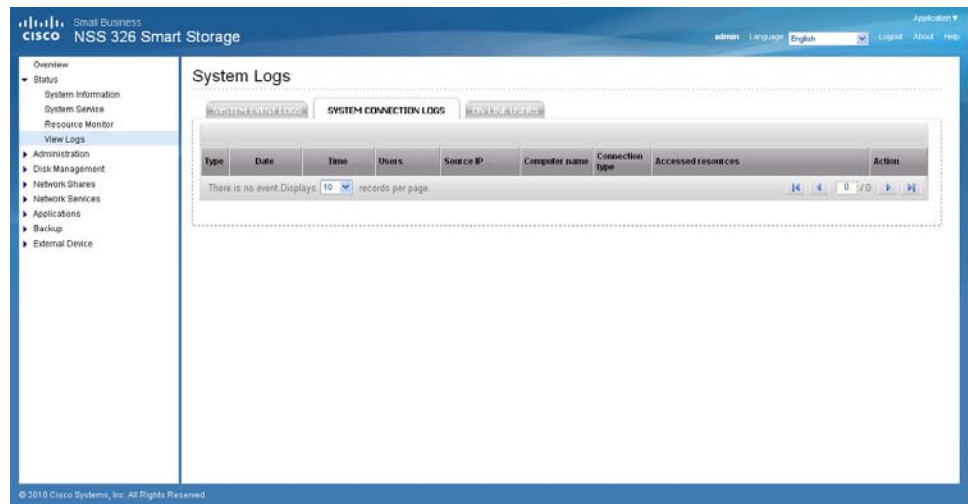
The *Status > View Logs > System Event Logs* window displays the event logs, including warning, error, and information messages. In the event of system malfunction, you can retrieve the event logs to analyze system problems.



- **Type**—Type of log. Possible log types are Informational, Error, and Warning messages.
- **Date**—Date that the log occurred.
- **Time**—Time that the log occurred.
- **Users**—User or system that generated the log entry.
- **Source IP**—IP address of the user.
- **Computer Name**—Name of the computer (if applicable) or local host that generated the log entry.
- **Content**—Description of the log.

## System Connection Logs

The *Status > View Logs > System Connection Logs* window displays the HTTP, FTP, Telnet, SSH, AFP, NFS, SAMBA, RADIUS, and iSCSI connection logs.

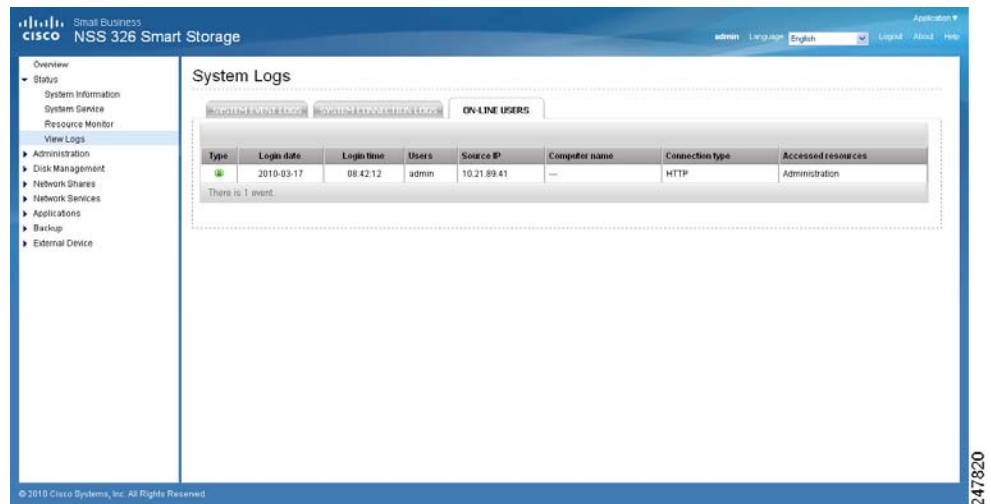


- **Type**—Type of log. Possible log types are Informational, Error, and Warning messages.
- **Date**—Date that the log occurred.
- **Time**—Time that the log occurred.
- **Users**—User or system that generated the log entry.
- **Source IP**—IP address of the user.
- **Computer Name**—Name of the computer (if applicable) or local host that generated the log entry.
- **Connection Type**—Type of connection. For example, HTTP, FTP, Telnet, SSH, AFP, SAMBA, or iSCSI.
- **Accessed Resources**—Type of resource accessed. For example: administrative activity, path, and name of files transferred.
- **Action**—Type of action. For example: login, log out, write, read, delete, and rename.



## On-Line Users

The *Status > View Logs > On-Line Users* window displays the information for the on-line users who are accessing the NAS. This displays real-time status versus system log information, which shows a history.



- **Type**—Real-time status for on-line users.
- **Login Date**—Date that the user logged in.
- **Login Time**—Time that the user logged in.
- **Users**—Name of administrator or users account.
- **Source IP**—IP address of the user.
- **Computer Name**—Name of the computer (if applicable) or remote host IP address that generated the log entry.
- **Connection Type**—Type of connection. For example, HTTP, FTP, Telnet, SSH, AFP, SAMBA, or iSCSI.
- **Accessed Resources**—Type of resource accessed. For example, administrative activity or network share folder.

---

## Administration

From the Administration window, you can configure and view the following parameters:

- **General Settings**
- **Network**
- **Hardware**
- **Security**
- **Notification**
- **Power Management**
- **Network Recycle Bin**
- **Backup System Settings**
- **System Logs Settings**
- **Firmware Upgrade**
- **Restore to Factory Default**
- **Network Service Discovery**
- **Users**
- **User Groups**

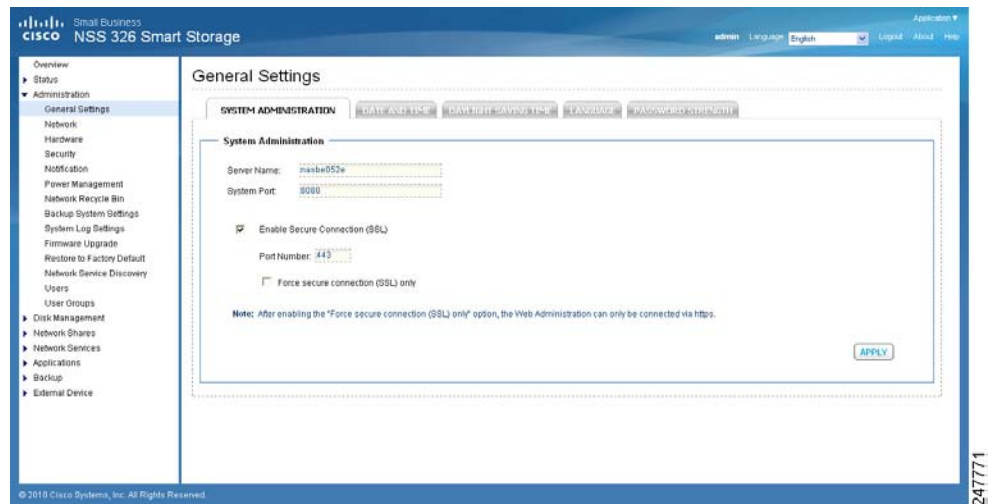
### General Settings

This section describes how to configure the general settings for the NAS.

- **System Administration**
- **Date and Time**
- **Daylight Savings Time**
- **Language**
- **Password Strength**

## System Administration

From the *Administration > General Settings > System Administration* window, you can configure the server name, port settings, and Secure Connection (SSL).



To configure the system administration settings:

**STEP 1** Choose **Administration > General Settings > System Administration** from the Navigation menu. The *System Administration* window opens.

**STEP 2** Enter the parameters:

- **Server Name**—Name of the NAS. The server name can be up to 14 characters long and may contain alphabet characters, numbers, and hyphen (-). The server does not accept names with spaces, periods (.), or names composed of numbers only.
- **System Port**—Port for the system management. The default port is 8080. The services which use this port include: System Management, Web File Manager, Multimedia Station, and Download Station.
- **Enable Secure Connection (SSL)**—Click the check box to enable an SSL secure connection.
  - **Port Number**—Enter the port number for the SSL connection. The default port is 443.
  - **Force secure connection (SSL) only**—This option forces the use of an SSL connection. After enabling the “Force secure connection (SSL) only” option, the Web Administration can only be connected via HTTPS.

**NOTE** If the Web Server is enabled, the default port number is 80 for the Web Server. To access the Web server and System Management, see the following examples.

To access the Web Server:  
**http://<IP Address>**

To access System Management:  
**http://<IP Address>:8080**

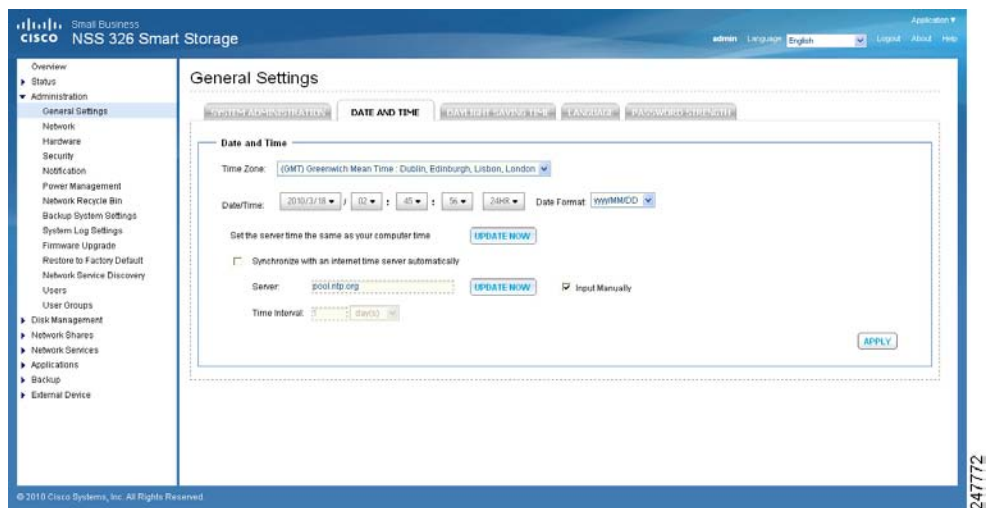
**STEP 3** Click **Apply**. The System Administration settings are updated to the NAS.

### Date and Time

From the *Administration > General Settings > Date and Time* window you can set the date, time, and time zone according to your location. You can also choose whether or not to synchronize the NAS time with a Network Time Protocol (NTP) server, or with the time of your computer.

If the settings are incorrect, the following problems may occur:

- When using a web browser to access the server or save a file, the display time of the action will be incorrect.
- The time of event log displayed will be inconsistent with the actual time when an action occurs.



To define the date and time:

- 
- STEP 1** Choose **Administration > General Settings > Date and Time** from the Navigation menu. The *Date and Time* window opens.
- STEP 2** From the Time Zone drop-down list, choose the time zone that the NAS is set to.
- STEP 3** To set the Date and Time, click the down arrows by each value and select the current date and time.

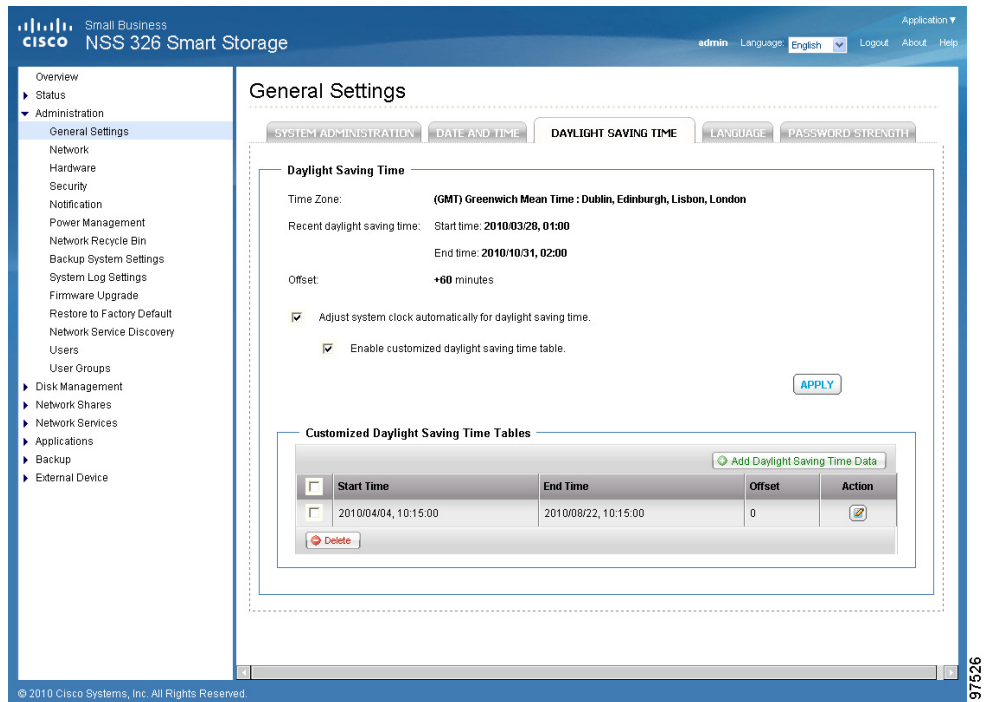
Enter the values for the following:

- **Date Format**—Select the order of how you want the day, month and year to display. For example, DD/MM/yyyy or yyyy/MM/DD.
  - **Set the server time the same as your computer time**—Click **Update Now** to set the time of the NAS to the same time as your computer.
  - **Synchronize with an Internet time server automatically**—To obtain time automatically from an NTP server, click the check box. The first time you enable the NTP server, it may take several minutes for time synchronization before the time is correctly adjusted.
    - **Server**—From the drop-down list, choose the NTP server name and click Update Now.
    - Click the **Input Manually** check box to enter an address that is different from the drop-down list.
    - **Time Interval**—Time interval for the date and time to be updated on the NAS. Choose day(s) or hour(s) and a numeric time value.
- STEP 4** Click **Apply** to update the Date and Time settings.

---

### Daylight Savings Time

From the *Administration > General Settings > Daylight Savings Time* window you can automatically update the time to accommodate daylight savings time on the NAS.



To set the daylight savings time:

**STEP 1** Choose **Administration > General Settings > Daylight Savings Time** from the Navigation menu. The *Daylight Savings Time* window opens.

The following parameters are displayed:

- **Time Zone**—Current time zone that the NAS is set to. To change this value, see [Date and Time, page 52](#).
- **Recent daylight saving time**—Range of time set by the current Daylight Saving Time settings.
- **Offset**—Current time offset by daylight savings time.

**STEP 2** If needed, set the following parameters:

- **Adjust system clock automatically for daylight saving time**—Click the check box to enable the NAS to automatically adjust its time settings to accommodate daylight savings time.
- **Enable customized daylight saving time table**—Click the check box to create a custom Daylight Savings Time table. When selected, the *Customized Daylight Saving Time Tables* opens. Click **Add Daylight**

**Saving Time Data** to create a new table. After a new table has been created, select the option of the Daylight Savings Table that you would like to use.

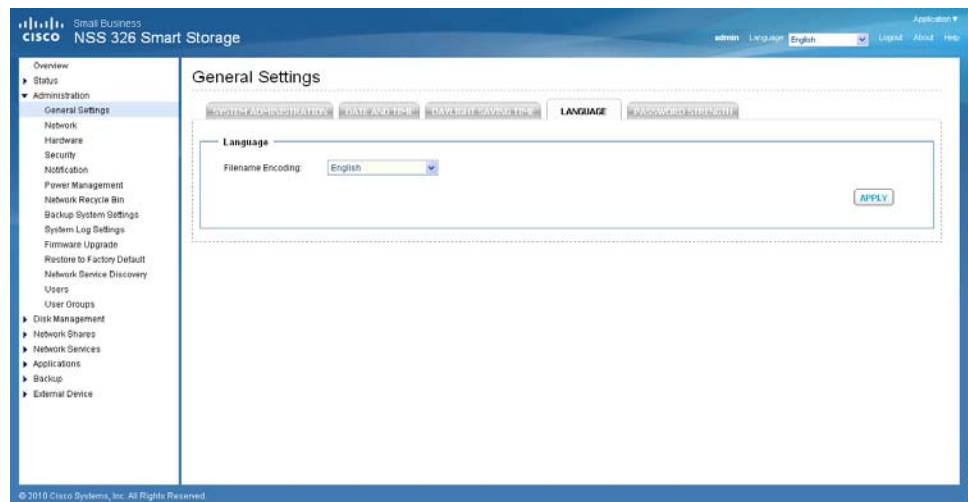
**STEP 3** Click **Apply** to update the NAS with the daylight savings time settings.

## Language

From the *Administration > General Settings > Language* window you can define the language filename encoding. The NAS server uses Unicode as the default filename encoding system and will work with operating systems (OS) that support Unicode, such as Windows XP/Vista and MAC OS X.

If you are using an OS that does not support Unicode, such as Windows 95/98/ME, select the same language as your OS for filename encoding. Since most FTP software clients do not support Unicode, you will need to select the language that your FTP client supports in order to properly display file and folder names on the server. If the filename encoding is not properly selected, the following problems may occur:

- You may be unable to create files or folders in certain languages.
- You may be unable to display filenames or folder names in certain languages.



To define the language filename encoding:

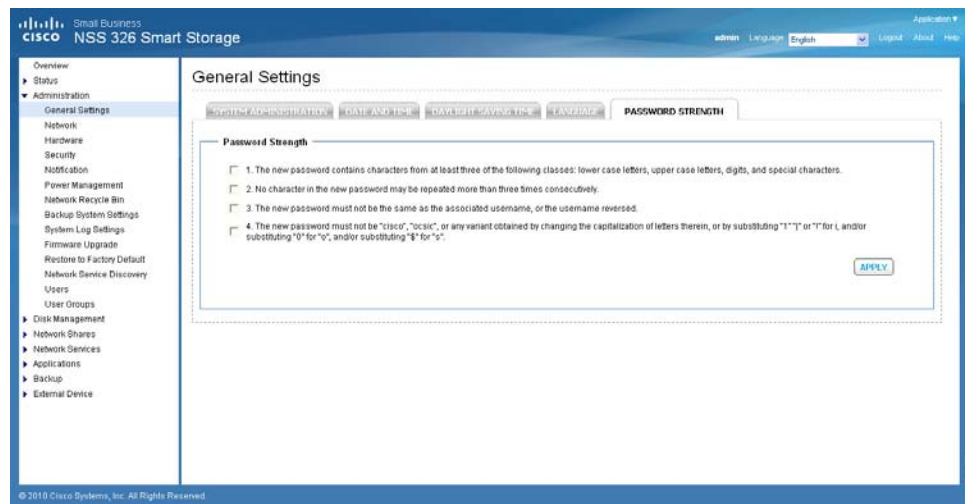
- STEP 1** Choose **Administration > General Settings > Language** from the Navigation menu. The *General Settings* window opens.
- STEP 2** From the Filename Encoding drop-down list, select the language you want to use for filename encoding.

**NOTE** If you are using an OS that does not support Unicode, such as Windows 95/98/ME, please select the same language as your OS for filename encoding.

- STEP 3** Click **Apply**. The language filename encoding is set and the NAS is updated.

## Password Strength

From the *Administration > General Settings > Password Strength* window, you can apply the password rules. You can enable one or more of the Password Strength options to enforce password strength. After the setting has been applied, the system will automatically check the validity of password set by users.





To define the password rules:

- 
- STEP 1** Choose **Administration > General Settings > Password Strength** from the Navigation menu. The *Password Strength* window opens.
- STEP 2** Enable one or more of the Password Strength options to enforce password strength:
- **The new password contains characters from at least three of the following classes: lower case letters, upper case letters, digits, and special characters**—This option forces the user to use at least three of these classes of characters: lower-case letters, upper-case letters, digits, and special characters. Special characters are characters such as “!,” “@,” and “#.”
  - **No character in the new password may be repeated more than three times consecutively**—This option specifies that a password cannot contain characters repeated more than three in a row such as “123ZZZabc.”
  - **The new password must not be the same as the associated username, or the username reversed**—This option specifies that the password cannot contain a variation of the username used to login to the NAS.
  - **The new password must not be "cisco", "ocsic", or any variant obtained by changing the capitalization of letters therein, or by substituting “1” “l” or “!” for i, and/or substituting “0” for “o”, and/or substituting “\$” for “s”**—This option specifies that the password cannot contain a variation of the word “Cisco.”
- STEP 3** Click **Apply**. The password rules are applied to the NAS.
- 

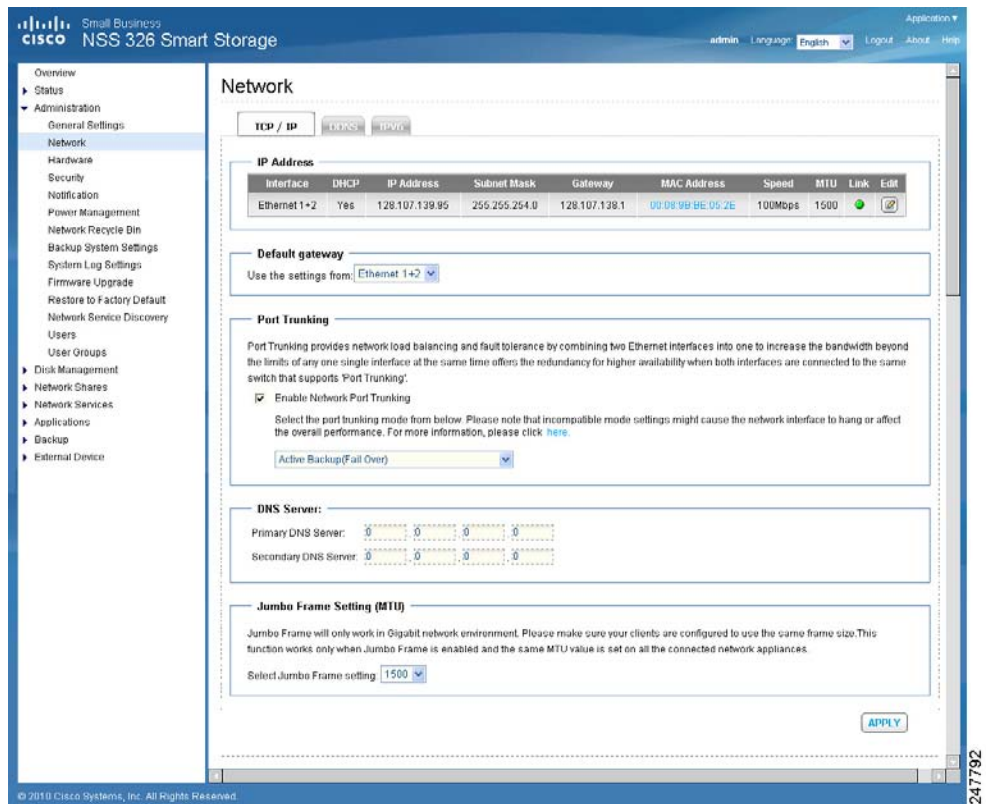
## Network

This section describes how to configure the network settings, such as:

- **TCP/IP**
- **DDNS**
- **IPv6**

## TCP/IP

From the *Administration > Network > TCP/IP* window, you can configure network transfer rates, default gateway, port trunking, DNS server, and Jumbo Frame Setting (MTU).



To configure TCP/IP settings:

- STEP 1** Choose **Administration > Network > TCP/IP** from the Navigation menu. The *TCP/IP* window opens.
- STEP 2** Configure or view the TCP/IP settings.

### IP Address

- **Interface**—Physical NAS network interface.
- **DHCP**—Specifies whether this interface uses Dynamic Host Configuration Protocol (DHCP).
- **IP Address**—IP address of this interface.

- **Subnet Mask**—Subnet mask of this interface.
- **Gateway**—IP address of the network gateway device.
- **MAC Address**—MAC address of this interface.
- **Speed**—Negotiated or specified link speed.
- **MTU**—Maximum Transmission Unit (MTU) for this interface.
- **Link**—Status of this interface. A green light indicates that the interface is active. If only one NIC is used, the web interface will not show the other link as down or not in use. It will only show both NICs if the NSS is configured as a standalone from the discovery tool.
- **Edit**—Allows you to turn off DHCP, specify a static IP address, enable the NAS to be a DHCP server, and allows you to specify link speed or set it to auto negotiation. When you click *Edit*, the TCP/IP-Property window opens and the following options are available:
- **Network Speed**—From the drop-down list, select from the following options:
  - **Auto-negotiation**—Allows the server to adjust transfer rates automatically.
  - **1000 Mbps full-duplex**—Sets this transfer rate.
  - **100 Mbps full-duplex**—Sets this transfer rate.
- **Obtain IP address settings automatically via DHCP**—Select to enable the NAS to acquire the IP address from a DHCP server.
- **Use static IP address**—Select to enable the NAS to use a static IP address. Enter the static IP address, subnet mask, and default gateway.
- **Enable DHCP Server**—If DHCP is not available in the LAN where the NAS is located, you can enable this function to enable the NAS as a DHCP server and allocate dynamic IP address to DHCP clients in the LAN.

You can set the range of IP addresses allocated by the DHCP server and the lease time. Lease time refers to the time that the IP address is leased to the clients by the DHCP server. When the time expires, the client has to acquire an IP address again.

For example, to establish a DLNA network and share the multimedia files on the NAS to a DLNA digital media player via UPnP, without a NAT gateway that supports DHCP server, you can enable DHCP server on the NAS. The NAS will allocate dynamic IP addresses to media players or other clients automatically and set up a local network.

**NOTE** If there is an existing DHCP server in your LAN, do not enable this function. Otherwise, there will be IP address allocation conflicts and network access errors.

### Default Gateway

- **Use the setting from**—From the drop-down list, select the interface to use.

### Port Trunking

All of the NAS models include Dual-LAN ports, which allow port trunking options whereby two network interfaces function as one to increase bandwidth beyond the limits of any single interface, while at the same time offering redundancy and load balancing for higher availability. Following is a list of supported port trunking modes.

**NOTE** Some trunking and redundancy options require a switch that also supports these features. Note that incompatible mode settings may cause the network interface to hang or affect overall network performance.

- **Enable Network Port Trunking**—Enable or disable port trunking. When enabled, the following options are available from the drop-down list:
  - **Balance-rr (Round-Robin)**—Round-Robin mode is good for general purpose load balancing between the adapters. This mode transmits packets in sequential order from the first available slave through the last. Balance-rr provides load balancing and fault tolerance.
  - **Active Backup (Fail Over)**—Active Backup uses just one adapter. It switches to the second adapter if the first adapter fails. Only one slave in the bond is active. The bond's MAC address is only visible externally on one port (network adapter) to avoid confusing the switch. Active Backup mode provides fault tolerance.
  - **Balance XOR**—Balance XOR balances traffic by splitting up outgoing packets between the adapters, using the same one for each specific destination when possible. It transmits based on the selected transmit hash policy. The default policy is a simple slave count operating on Layer 2 where the source MAC address is coupled with destination MAC

address. Alternate transmit policies may be selected via the `xmit_hash_policy` option. Balance XOR mode provides load balancing and fault tolerance.

- **Broadcast**—Broadcast sends traffic on both interfaces. Broadcast mode provides fault tolerance.
- **IEEE 802.3ad (Dynamic Link Aggregation)**—Dynamic Link Aggregation uses a complex algorithm to aggregate adapters by speed and duplex settings. It utilizes all slaves in the active aggregator according to the 802.3ad specification. Dynamic Link Aggregation mode provides load balancing and fault tolerance but requires a switch that supports IEEE 802.3ad with LACP mode properly configured.
- **Balance-tlb (Adaptive Transmit Load Balancing)**—Balance-tlb uses channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load on each slave (computed relative to the speed). Incoming traffic is received by the current slave. If the receiving slave fails, the other slave takes over the MAC address of the failed receiving slave. Balance-tlb mode provides load balancing and fault tolerance.
- **Balance-alb (Adaptive Load Balancing)**—Balance-alb is similar to balance-tlb but also attempts to redistribute incoming (receive load balancing) for IPV4 traffic. This setup does not require any special switch support or configuration. The receive load balancing is achieved by ARP negotiation sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware address for the server. Balance-alb mode provides load balancing and fault tolerance.

**NOTE** If the NAS administration interface cannot be accessed due to an improperly configured port trunking mode or incompatible switch, reset the network settings by pressing the reset button on the back panel of the NAS for 3 seconds.

### DNS Server

You can specify the DNS server address here, or choose to obtain it automatically. If you have selected to obtain the IP address automatically, you do not need to configure the primary and secondary DNS servers.

- **Primary DNS Server**—Enter the IP address of the Domain Name System (DNS) server. This address is typically provided by your Internet Service Provider (ISP).
- **Secondary DNS Server**—Enter a second DNS server.

### Jumbo Frame Settings (MTU)

Jumbo Frames refer to Ethernet frames that are larger than 1500 bytes. Jumbo Frames are designed to enhance Ethernet networking throughput and reduce the CPU utilization of large file transfers by enabling more efficient, larger payloads per packet. Maximum Transmission Unit (MTU) refers to the size (in bytes) of the largest packet that a given layer of a communications protocol can transmit.

The NAS uses standard Ethernet frames, which are 1500 bytes by default. If your network appliances support Jumbo Frame setting, select the appropriate MTU value for your network environment. The NAS supports 4074, 7418, and 9000 bytes for MTU.

**NOTE** Jumbo Frame setting is valid in a Gigabit network environment only. Also, all network appliances connected must enable Jumbo Frame and use the same MTU value.

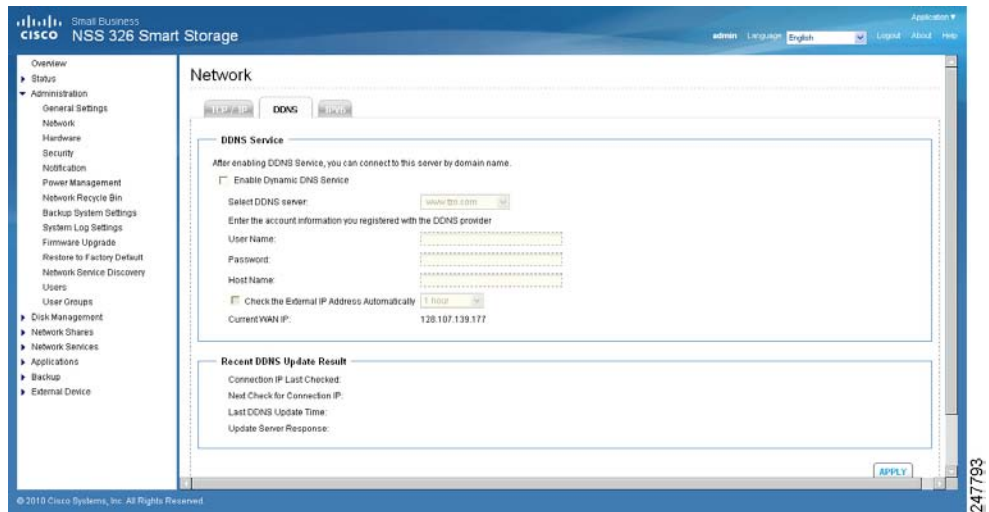
- **Select Jumbo Frame Setting**—From the drop-down list, select the MTU value for your network. The NAS supports 4074, 7418, and 9000 bytes for MTU.

**STEP 3** Click **Apply** to save the settings.

**NOTE** If the NAS administration interface cannot be accessed due to an improperly configured Jumbo Frame setting or incompatible switch, reset the network settings by pressing the reset button on the back panel of the NAS for 3 seconds.

### DDNS

From the *Administration > Network > DDNS* window, you can configure Dynamic DNS Service (DDNS). DDNS allows internet access to the server using a domain name rather than an IP address. DDNS also maintains IP address information even when the client received a dynamic IP assignment subject to frequent change by the ISP. This configuration ensures that the server is always available independent of the IP address. To use this service you must establish an account with a dynamic DNS service provider.



To configure DDNS settings:

- STEP 1** Choose **Administration > Network > DDNS** from the Navigation menu. The *DDNS* window opens.
- STEP 2** Configure the DDNS settings.

### DDNS Service

- **Enable Dynamic DNS Service**—Click this option to enable a DDNS service. DDNS is useful when you are hosting your own website, FTP server, or other server behind the NAS. If DDNS is enabled, you can select a fixed host and domain name to a dynamic Internet IP address. Before you can use this feature, you need to sign up for a DDNS service.
- **Select DDNS Server**— From the drop-down list, select a DDNS server. The NAS supports the following DDNS server providers:
  - [www.tzo.com](http://www.tzo.com)
  - [www.dyndns.org](http://www.dyndns.org)
  - [update.ods.org](http://update.ods.org)
  - [members.dhs.org](http://members.dhs.org)
  - [www.dyns.cx](http://www.dyns.cx)
  - [www.3322.org](http://www.3322.org)
  - [www.no-ip.com](http://www.no-ip.com)

- **Enter the account information you registered with the DDNS provider—** Complete the following fields.
  - **User Name**—Username that you registered with the DDNS provider.
  - **Password**—Password registered with the DDNS provider.
  - **Host Name**—Host name registered with the DDNS provider.
- **Check the External IP Address Automatically**—Enable this option if your NAS is located behind a gateway. The NAS checks the external (WAN) IP automatically at the specified interval. If the IP address is changed, the NAS will inform the DDNS provider automatically to ensure it can be accessed via the host name. From the drop-down list, select the specified interval.
- **Update DDNS using the alternate port 21333 (bypass local web proxy)**— Click to enable updating DDNS using the alternate port 21333.

#### Recent DDNS Update Result

- **Connection IP Last Checked**—WAN IP address last checked.
- **Next Check for Connection IP**—Time schedule that WAN IP address will next be checked. Can also show as a blank field.
- **Last DDNS Update Time**—Time that the DDNS was last updated.
- **Update Server Response**—OK or Failed response.

**STEP 3** Click **Apply** to save the DDNS Service settings.

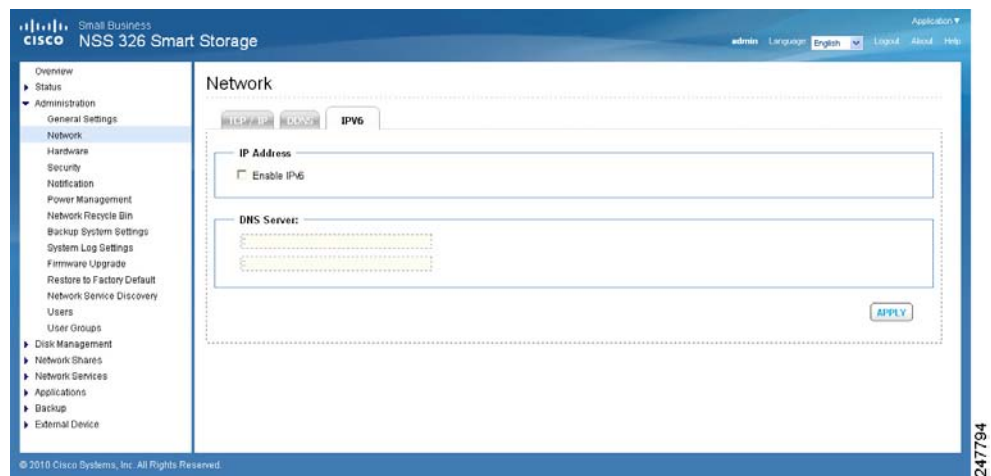
## IPv6

From the *Administration > Network > IPv6* window, you can configure IPv6. The system NAS supports IPv6 connectivity with stateless address configurations. Router Advertisement Daemon (RADVD) is also available for sending out router advertisements described in RFC 2461 for IPv6. Hosts within the same network can automatically configure their addresses. This option should be used when the network router is configured as dual stack (IPv4 and IPv6). The router will send the advertisement. Newer clients such as Windows 7, Vista, MAC OS 10.5 (and greater) will benefit from IPv6, as they will query DNS via IPv6 first and then IPv4. The latest browsers such as IE8, Safari 4, and Firefox prefer IPv6 DNS but will fall back to IPv4 if IPv6 fails. This setting also needs to be applied on the router.



The services on the NAS that support IPv6 include:

- Remote replication
- Web Server
- FTP
- iSCSI (Virtual disk drives)
- SSH



To configure IPv6:

- STEP 1** Choose **Administration > Network > IPv6** from the Navigation menu. The *IPv6* window opens.
- STEP 2** Click the **Enable IPv6** check box to use this function. The NAS will restart automatically. After the system restarts the settings for the IPv6 interface will display in the IPv6 window.
  - **Edit**—Allows you to edit the IPv6 settings. When you click **Edit**, the *IPv6-Property* window opens and the following options are available:
    - **IPv6 Auto Configuration**—If you have an IPv6 enabled router on the network, click this option to allow the NAS to acquire the IPv6 address and the configurations automatically.
    - **Use static IP address**—Click to use a static IP address. Enter the IP address (for example, 2001:bc95:1234:5678), prefix length (for example, 64), and the gateway address for the NAS. Contact your ISP for the prefix and the prefix length information.

- **Enable Router Advertisement Daemon (radvd)**—Click to enable this option and configure the NAS as an IPv6 host that distributes IPv6 addresses to the local clients which support IPv6. Enter the prefix and prefix length.

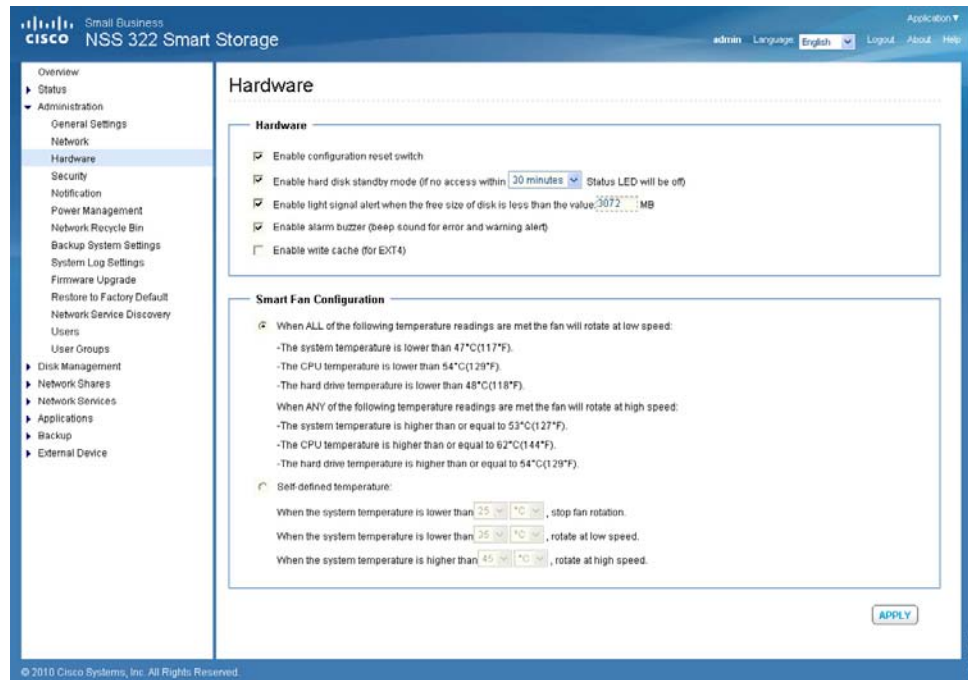
**STEP 3** Enter the name of the primary DNS server in the first field and the name of the secondary DNS server in the second field. Contact your ISP or network administrator for the DNS server information.

**NOTE** If you selected IPv6 auto configuration in the previous steps, leave the double colons (::) in both fields.

**STEP 4** Click **Apply** to save the IPv6 settings.

## Hardware

From the *Administration > Hardware* window, you can configure the hardware related functions of the NAS.



To configure the hardware related functions:

**STEP 1** Choose **Administration > Hardware** from the Navigation menu. The *Hardware* window opens.

**STEP 2** Configure the following settings.

#### Hardware

- **Enable configuration reset switch**—Enables the reset switch at the back panel of the NAS. You can press the reset button for 3 or 10 seconds to reset the administrator password and system settings to default. If disabled, the reset switch cannot be used to set the unit to its default settings. For more information about the reset, see [Hardware System Reset, page 176](#).
- **Enable hard disk standby mode**—Enables disk standby mode if inactive for more than the specified time.
- **Enable light signal alert when the free size of SATA disk is less than the value**—The Status LED indicator flashes red and green when this function is enabled and the free space of the SATA disk is less than the value. The recommended range for this value is 1-51200 MB.
- **Enable alarm buzzer**—Enable to allow an audible beep when an error occurs.
- **Enable write cache (for EXT4)**—Enable to allow the system to use internal cache when the filesystem is configured for EXT4.

#### Smart Fan Configuration

- **When ALL of the following temperature readings are met the fan will rotate at low speed**—Click to use the default smart fan settings. When the system default settings are selected, the fan rotation speed is automatically adjusted when the server temperature, CPU temperature, and hard drive temperature meet the criteria.
- **Self-defined temperature**—Click to define the settings manually. Select the temperature from the drop-down lists.

**STEP 3** Click **Apply** to save the hardware settings.

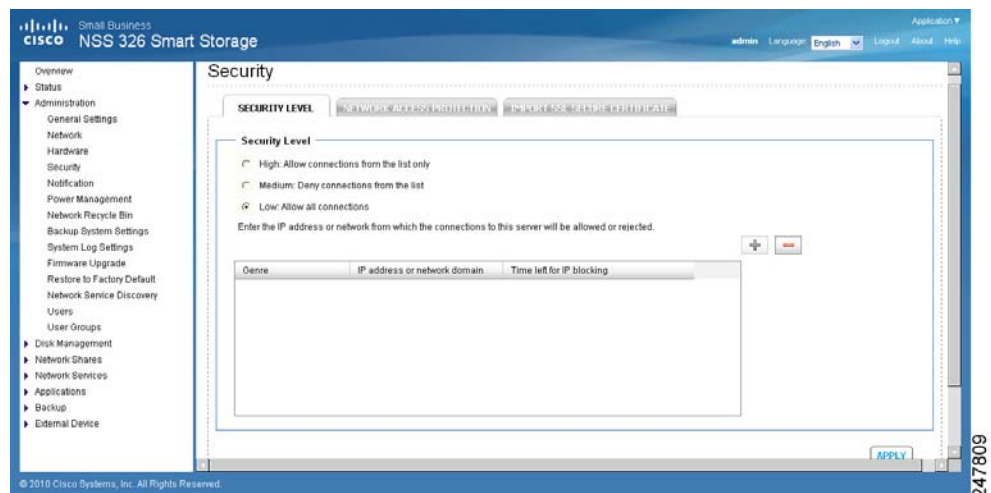
## Security

This section describes how to configure the security on the NAS and includes the following:

- **Security Level**
- **Network Access Protection**
- **Import SSL Secure Certificate**

### Security Level

From the *Administration > Security > Security Level* window, you can configure the security level for the NAS as high, medium, or low.



To configure the security level:

- STEP 1** Choose **Administration > Security > Security Level** from the Navigation menu. The Security Level window opens.
- STEP 2** Select the security level for the NAS.
  - **High**—Only allow connections that are on the list. This is commonly referred to as a white list. To add connections to the list, click the green “+” icon and add the connection. Click the red “-” icon to remove a connection.
  - **Single IP Address**—Enter the IP address from which the connections to this NAS are allowed.

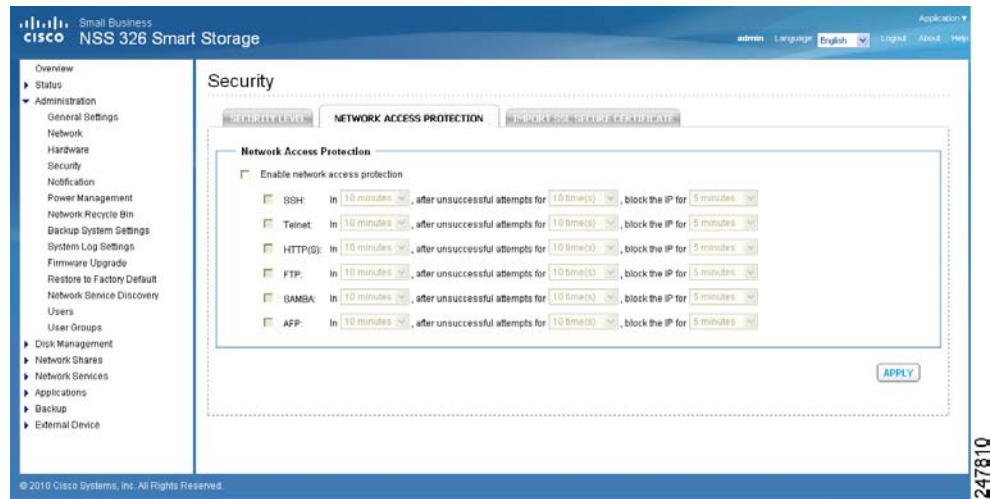
- **Specify IP addresses of certain network by setting IP address and netmask**—Enter the IP address and netmask of the network from which the connections to this NAS are allowed.
  - **IP Range**—Enter the IP address range from which the connections to this NAS are allowed.
  - **Medium**—Deny connections that are on the list. This is commonly referred to as a black list. When the connection of a host server is denied, all protocols of that server are not allowed to access the NAS. To add connections to the list, click the green “+” icon and add the connection. Click the red “-” icon to remove a connection.
    - **Single IP Address**—Enter the IP address from which the connections to this NAS are denied.
    - **Specify IP addresses of certain network by setting IP address and netmask**—Enter the IP address and netmask of the network from which the connections to this NAS are rejected.
    - **IP Range**—Enter the IP address range from which the connections to this NAS are rejected.
  - **Low**—Allow all connections regardless of connections in the list.
- STEP 3** Click **Apply** to save the security settings. The network services will be restarted and current connections to the server will be disconnected.

---

### Network Access Protection

From the *Administration > Security > Network Access Protection* window, you can enhance the security of the system and prevent unwanted intrusion. Network access protection shields the NAS from Internet attacks by automatic IP blocking. You can define the rules of IP blocking for different services or protocols.

**NOTE** If the Security Level is set as High, Network Access Protection will be disabled since only connections from specified IP addresses are permitted access.



- STEP 1** Choose **Administration > Security > Network Access Protection** from the Navigation menu. The *Network Access Protection* window opens.
- STEP 2** Click **Enable network access protection** to enable network access protection.
- STEP 3** Select the different services or protocols and from the drop-down lists, select the time intervals to define the rules. For example:

In 10 minutes, after unsuccessful attempts for 10 times, block the IP for 5 minutes.

You can select the following services or protocols:

- SSH
- Telnet
- HTTP(S)
- FTP
- SAMBA
- AFP

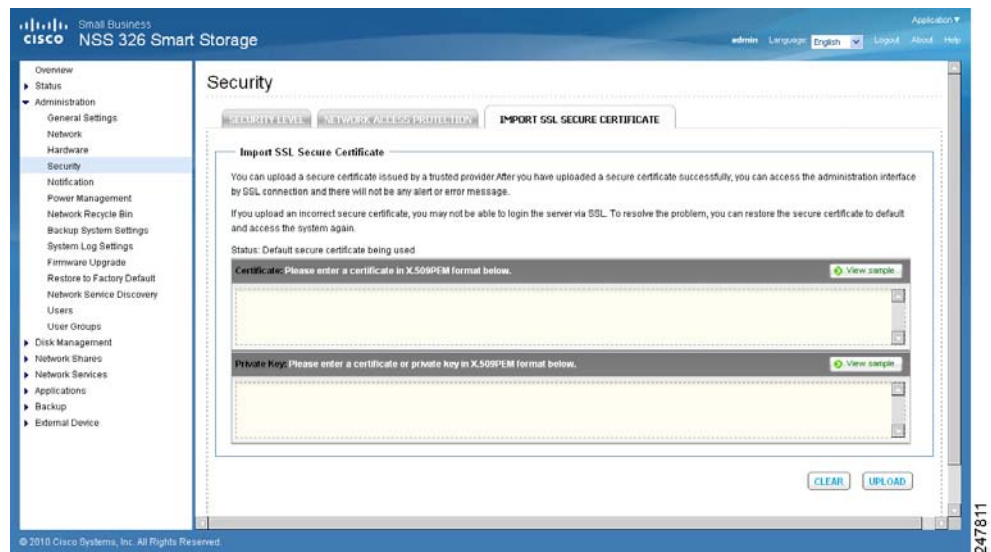
- STEP 4** Click **Apply** to save the settings.

## Import SSL Secure Certificate

The Secure Socket Layer (SSL) is a protocol for encrypted communication between web servers and browsers for secure data transfer. For example, if you set up a secure website to handle ecommerce transactions and you do not want users to receive an “unknown certificate” pop-up message from their web browser. You can generate a certificate, get it signed by a Certificate Authority, and import it into the NAS using the steps described in the procedure below.

From the *Administration > Security > Import SSL Secure Certificate* window, you can use the system default certificate or upload a secure certificate issued by a trusted provider. After you have uploaded a secure certificate, you can access the administration interface by SSL connection. The system supports X.509 certificate and private key only.

**NOTE** If you import an incorrect secure certificate, you may not be able to log into the NAS via SSL. To resolve the problem, you can restore the SSL certificate to default and access the system again.



To import an SSL secure certificate:

- STEP 1** Click **Administration > Security > Import SSL Secure Certificate** from the Navigation menu. The *Import SSL Secure Certificate* window opens.
- STEP 2** Click **View sample** to view a sample certificate or private key.
- STEP 3** Enter the certificate and private key information in the applicable fields.

- STEP 4** Click **Upload** to upload the certificate and private key or click **Clear** to remove any information from the certificate and private key fields.

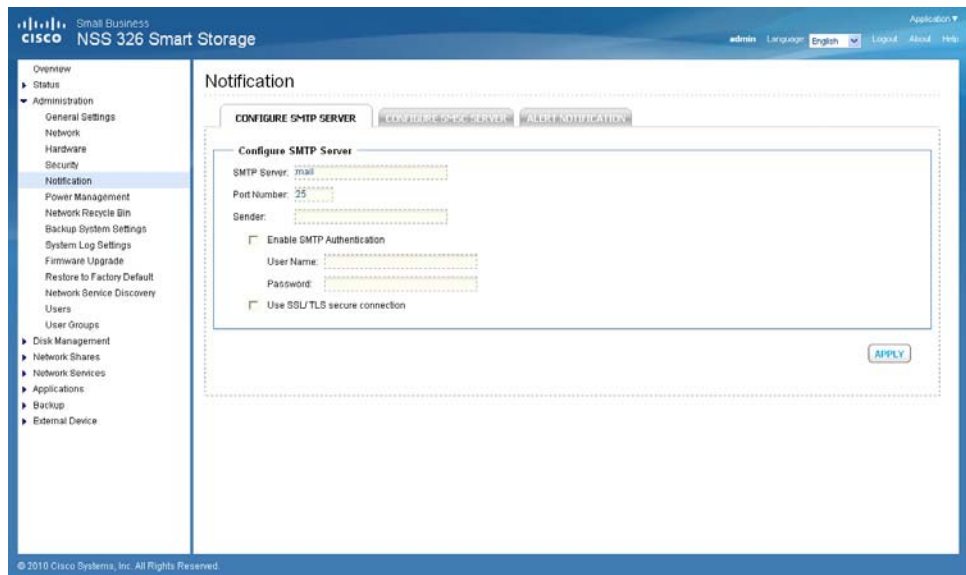
## Notification

This section describes configuring the NAS system notifications settings, such as:

- **Configure SMTP Server**
- **Configure SMSC Server**
- **Alert Notification**

### Configure SMTP Server

From the *Administration > Notification > Configure SMTP Server* window, you can configure the Simple Mail Transfer Protocol (SMTP) server. The NAS supports email alert to inform you about any system warnings or errors. To receive the alert by email, you need configure the SMTP server.





---

To configure the SMTP server:

**STEP 1** Click **Administration > Notification > Configure SMTP Server** from the Navigation menu. The *Configure SMTP Server* window opens.

**STEP 2** Enter the parameters:

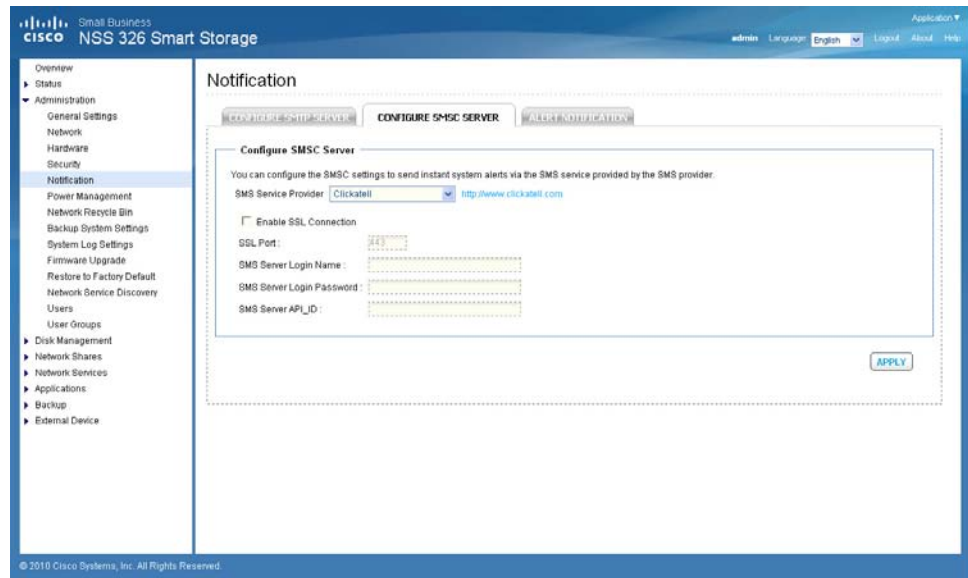
- **SMTP Server**—Enter the name of the SMTP server. For example: smtp.gmail.com.
- **Port Number**—Enter the port number used by the SMTP server. The default port number is 25.
- **Sender**—Enter the email address that you want to appear in the from: field of the email header of each email alert.
- **Enable SMTP Authentication**—Enables SMTP authentication. If enabled, the system will request authentication of the mail server before the message is sent. A user name and password must be specified.
  - **User Name**—Enter your email account user name.
  - **Password**—Enter your email account password.
- **Use SSL/TLS secure connection**—Enables Secure Sockets Layer (SSL) / Transport Level Security (TLS) connections.

**STEP 3** Click **Apply** to save the settings.

---

### Configure SMSC Server

From the *Administration > Notification > Configure SMSC Server* window, you can configure the Short Message Service Center (SMSC) settings to send instant system alerts via the SMS service provided by the SMS provider. The default SMS service provider is Clickatell. You can also add your own SMS service provider.



To configure the SMSC server:

- STEP 1** Click **Administration > Notification > Configure SMSC Server** from the Navigation menu. The *Configure SMSC Server* window opens.
- STEP 2** From the SMS Service Provider drop-down list, select one of the following:
  - **Clickatell**—This is the default SMS service provider.
  - **Add SMS service provider**—Select to add your SMS service provider.

Different parameter settings are displayed dependent on your choice of the default service provider or adding your SMS service provider.

- STEP 3** Enter the parameters for either Clickatell or Add SMS service provider:

#### Clickatell

- **Enable SSL Connection**—Click to enable the SSL connection.
- **SSL Port**—Enter the port number used for the SSL connection. The default port is 443.
- **SMS Server Login Name**—Enter the SMS server login name.
- **SMS Server Login Password**—Enter the SMS server login password.

- **SMS Server API\_ID**—Enter the SMS server API ID provided from your provider. In order to get the API\_ID, the user needs to add the NAS product name to the service provider list. In this case, it will be Cisco. This ID is different from the Client ID that the user receives when product is registered.

**Add SMS service provider**

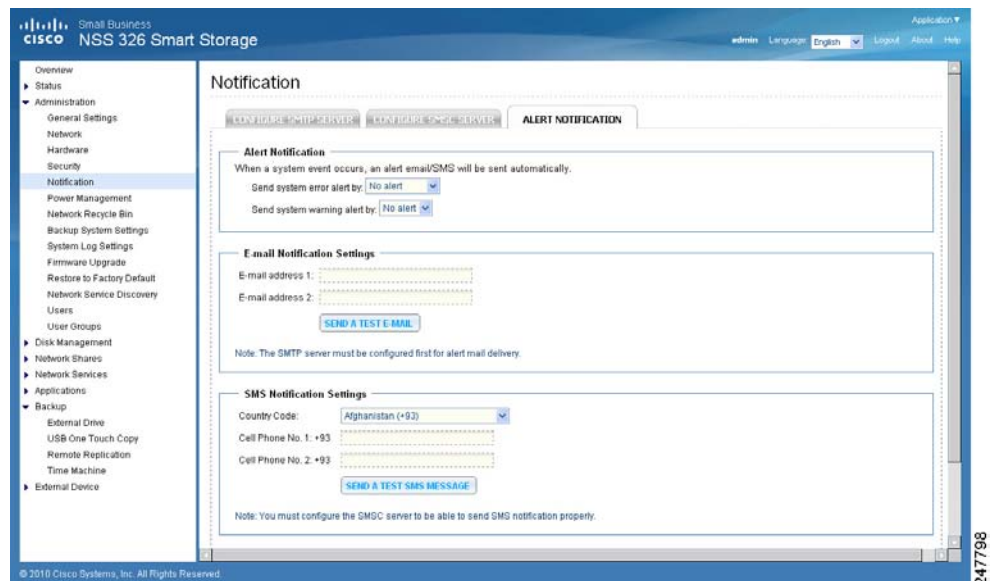
- **SMS Service Provider**—Enter the name of the SMS service provider.
- **URL Template Text**—Enter the text as specified in the URL Template Replaceable Parameters table.

**NOTE** You will not be able to receive the SMS properly if the URL template text entered does not follow your SMS service provider’s format.

**STEP 4** Click **Apply** to save the SMSC server settings.

**Alert Notification**

From the *Administration > Notification > Alert Notification* window, you can configure settings to receive instant SMS messages or email alerts in the event that a system warning or error occurs.



To configure the alert notification:

**STEP 1** Click **Administration > Notification > Alert Notification** from the Navigation menu. The *Alert Notification* window opens.

**STEP 2** Enter the parameters:

#### Alert Notification

- **Send system error alert by**—From the drop-down list, select how you want the system error alert sent. The options are:
  - **No alert**—Select if you do not want system error alerts sent.
  - **Email**—Select to receive system error alerts via email.
  - **SMS**—Select to receive system error alerts via SMS.
  - **Email & SMS**—Select to receive system error alerts via email and SMS.
- **Send system warning alert by**—From the drop-down list, select how you want the system warning alert sent. The options are:
  - **No alert**—Select if you do not want system warning alerts sent.
  - **Email**—Select to receive system warning alerts via email.

#### E-mail Notification Settings

- **E-mail address 1**—Enter the email address to receive the alert notification.
- **E-mail address 2**—Enter a second email address to receive the alert notification.
- **Send A Test E-mail**—Click to send a test email to the email address specified the email notification settings.

**NOTE** The SMTP server must be configured for alert mail delivery.

#### SMS Notification Settings

- **Country Code**—From the drop-down list, select the country code where the cell phone number is located.
- **Cell Phone No. 1**—Enter the cell phone number to receive the SMS notification.
- **Cell Phone No. 2**—Enter a second cell phone number to receive the SMS notification.

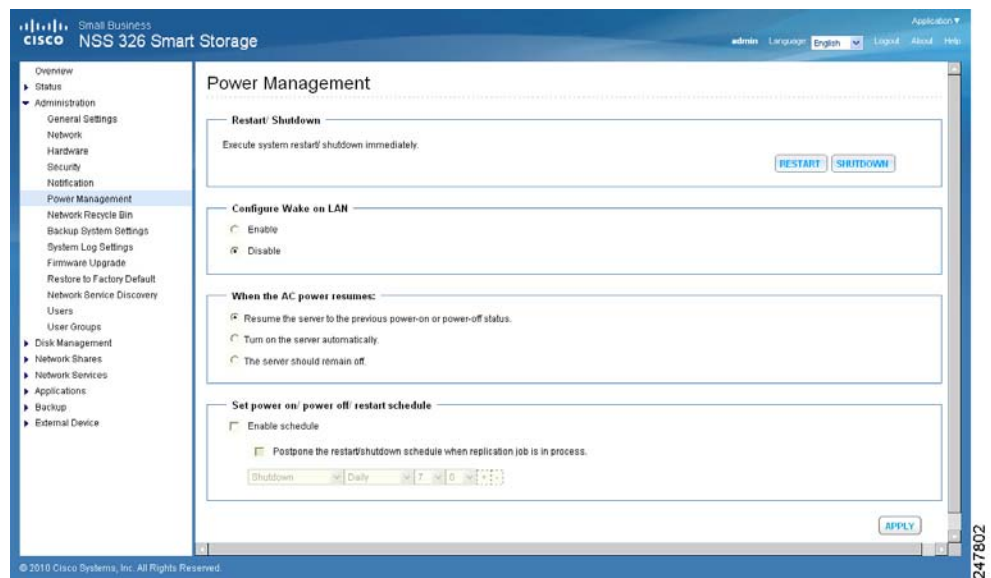
- **Send A Test SMS message**—Click to send a test SMS message to the cell phone numbers specified in the SMS notification settings.

**NOTE** The SMSC server must be configured to send SMS notification.

**STEP 3** Click **Apply** to save the alert notification settings.

## Power Management

From the *Administration > Power Management* window, you can restart or shut down the NAS immediately, define the behavior of the NAS when the power resumes after a power outage, and set a schedule for automatic system power on and off.



To configure power management:

**STEP 1** Click **Administration > Power Management** from the Navigation menu. The *Power Management* window opens.

**STEP 2** Set the parameters:

- **Restart/ Shutdown**—To restart the NAS immediately, click **RESTART**. To shutdown the NAS immediately, click **SHUTDOWN**.

- **Configure Wake on LAN**—Enable this option to power on the NAS remotely by Wake on LAN. If enabled, this feature allows the NAS to be powered on remotely from the LAN by the NSS Discovery Tool included on the Setup Wizard CD.

**NOTE** If the power connection is physically removed when the NAS is turned off, Wake on LAN will not function whether or not the power supply is reconnected afterwards.

- **Enable**—Click to enable Wake on LAN.
- **Disable**—Click to disable Wake on LAN.
- **When the AC power resumes**—Specify the action the NAS should take when the power resumes after power loss.
  - **Resume the server to the previous power-on or power-off status**—The NAS will return to its previous power-on or power-off status.
  - **Turn on the server automatically**—The NAS will power on as soon as power is restored.
  - **The server should remain off**—The NAS will remain off when power returns.
- **Set power on/power off/restart schedule**—This option allows you to power on or power off the NAS on a schedule. From the drop-down lists, select everyday, weekdays, weekend, or any days of the week and set the time for automatic system power on, power off, or restart. Weekdays represent Monday to Friday. Weekend represents Saturday and Sunday. Up to 15 schedules can be set.
  - **Enable schedule**—Click to enable the schedule.
  - **Postpone the restart/shutdown schedule when replication job is on progress**—Enable to allow the scheduled system restart or shutdown to be carried out after a running replication job completes. Otherwise, the system will ignore the running replication job and execute scheduled system restart or shutdown.

**STEP 3** Click **Apply** to save the power management settings.

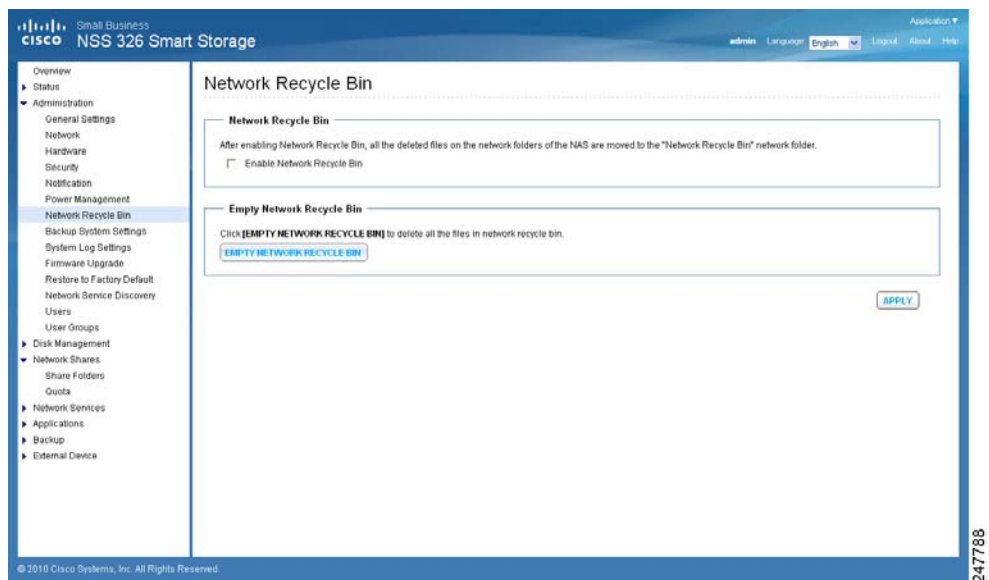
## Network Recycle Bin

From the *Administration > Network Recycle Bin* window, you can enable a network recycle bin or empty the network recycle bin. When enabled, there is a corresponding network recycle bin for each disk/disk volume.

The network recycle bin number is assigned accordingly to the creation of the disk volume number. The first array volume created will be assigned to Network Recycle Bin #1 and second array volume created will be assigned to Network Recycle Bin #2 and so on. For example: The first RAID 5 volume creation will automatically be assigned Network Recycle Bin #1. Then if a user added a new single disk from *Disk Management > Volume Management*, a new Network Recycle Bin #2 will be assigned.

Refer to the Property of the network share in *Administration > Network Shares > Share Folders* to view the details for each network recycle bin.

After enabling Network Recycle Bin, all of the files deleted via Samba/CIFS (not NFS, AFP, FTP) in the network folders of the NAS are moved to the Network Recycle Bin network folder.



---

To enable the network recycle bin:

- 
- STEP 1** Click **Administration > Network Recycle Bin** from the Navigation menu. The *Network Recycle Bin* window opens.
- STEP 2** Click **Enable Network Recycle Bin** to enable the network recycle bin. The system will keep all files deleted from any of the network share folders in the Network Recycle Bin. The files will be kept accordingly with the Network Recycle Bin number respective to the order of the disk volume when it was created.
- **Empty Network Recycle Bin**—To clear network recycle bin, click **EMPTY NETWORK RECYCLE BIN**.



---

**CAUTION** All files in the network recycle bins are permanently deleted when clicking **Empty Network Recycle Bin**.

---

- STEP 3** Click **Apply** to save the settings.
- 

## Backup System Settings

From the *Administration > Backup System Settings* window, you can backup and restore system settings.

- NOTE** It is good practice to periodically back up the system settings, especially if changes are made to the NAS configuration and saved to your computer. Since the NAS backup config files are always named the same (backupdata.bin), you can save the backup config files either in uniquely-named folders (for example, backup041310) or rename the config file (for example, default name is backupdata.bin; rename to backup041310.bin).





To configure the system backup and restore settings:

**STEP 1** Click **Administration > Backup System Settings** from the Navigation menu. The *Backup System Settings* window opens.

**STEP 2** Enter the parameters:

### Backup System Settings

- **Backup**—Click to backup all of the system settings, including the NAS user accounts, server name, system application settings, network services settings, and network configuration.

### Restore System Settings

- **Restore**—Click **Restore** to restore all of the settings.
- **Browse**—Click to select a previously saved setting file and click **Restore**.

**NOTE** It is important for the user to backup the system settings on a weekly basis so that the most current system changes are included in the backup.

**TFTP Configuration**—TFTP configuration is used to enable a saved configuration to be pushed out to the NAS. For instance, a reseller might create a custom configuration to distribute to all of their clients. The custom configuration is pushed out to the NAS as soon as the NAS boots up and makes a DHCP request, such as getting an IP address from the router.

- **Enable Automatic Configuration Download from TFTP Server (Option 66/150 & 67)**—When enabled, the NAS will automatically retrieve the system configuration from a Trivial File Transfer Protocol (TFTP) server which is provided by the DHCP server when the NAS boots up.
  - **Backup TFTP Server**—Enter the name of the backup TFTP server. If the TFTP server provided by the DHCP server cannot be accessed, the NAS will acquire the backup configuration file from the backup TFTP server.
  - **Backup Configuration File**—Enter the name of the backup configuration file from the backup TFTP server you entered in Backup TFTP Server.

**NOTE** If the NAS is configured with a static IP address, the system will not acquire the TFTP configuration from the DHCP server and will use the NAS internal configuration file for system startup, even if Enable Automatic Configuration Download from TFTP Server is enabled.

**STEP 3** Click **Apply** to save the settings.

---

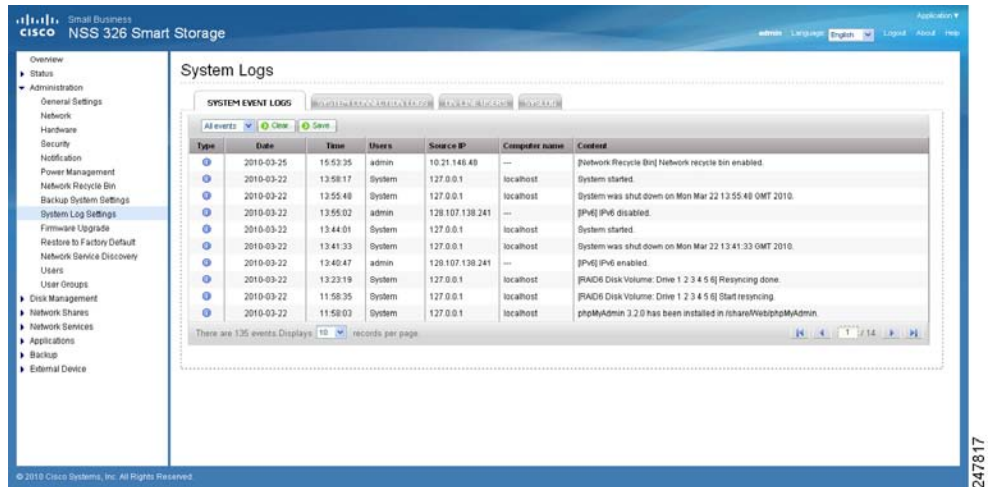
## System Logs Settings

This section describes the system logs and includes the following sections:

- **System Log Settings**
- **System Event Logs**
- **System Connection Logs**
- **On-Line Users**
- **Syslog**

## System Log Settings

From the *Administration > System Log Settings* window, you can view, save, and clear the system event logs.



## System Event Logs

From the *Administration > System Log Settings > System Event Logs* window, you can display warning, error, and informational messages. In the event of a system malfunction or an error indicator light on the front panel, the event logs can be retrieved to help diagnose the system problem.

To view the system event logs:

**STEP 1** Click **Administration > System Log Settings > System Event Logs** from the Navigation menu. The *System Event Logs* window opens and displays the following information.

- **Type**—Type of log. Log types are Informational, Error, and Warning messages.
- **Date**—Date that the log occurred.
- **Time**—Time that the log occurred.
- **Users**—User or system that generated the log entry.
- **Source IP**— IP address of the user.
- **Computer Name**—Name of the computer (if applicable) or local host that generated the log entry.

- **Content**—Description of the log.

- STEP 2** From the drop-down list, you can filter the type of log message displayed. Log types are All events, Informational, Error, and Warning messages.
- STEP 3** From the drop-down list, **Displays records per page**, select the number of records to display.
- STEP 4** Click the arrows in the lower right to navigate forward or back on the System Event Logs window.

---

To clear a system event log:

- STEP 1** From the **Administration > System Log Settings > System Event Logs** from the Navigation menu. The *System Event Logs* window opens.
- STEP 2** Right-click a single log and delete the record. Or click **Clear** to delete all of the system event logs.

---

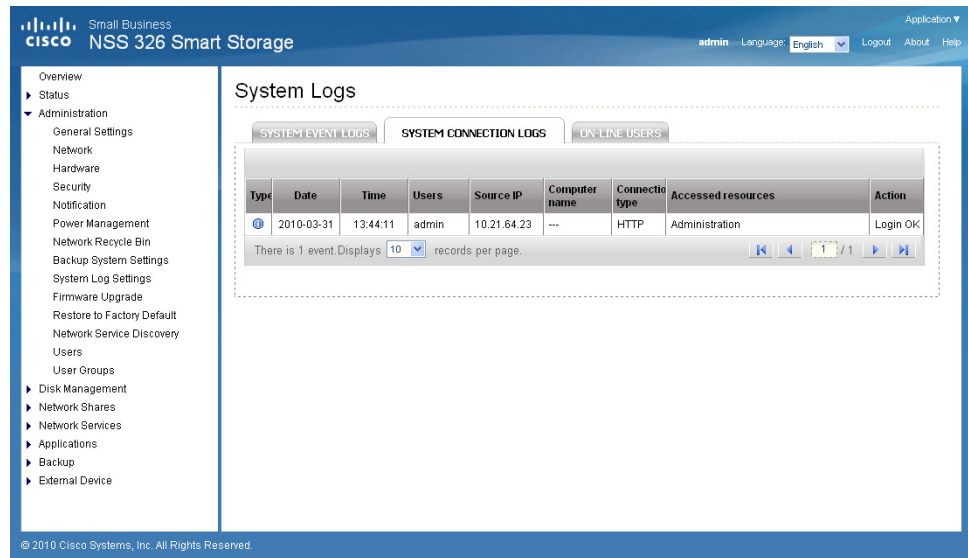
To save the system event logs:

- STEP 1** Click **Administration > System Log Settings > System Event Logs** from the Navigation menu. The *System Event Logs* window opens and displays the following information.
- STEP 2** Click **Save** and save the .csv file generated by the system.

---

### System Connection Logs

From the *Administration > System Log Settings > System Connection Logs* window, you can filter the type of message you want to view, specify connection types to be logged, start or stop logging events, and clear or save the system connection logs. From the System Connection Logs window, you can also disconnect the IP address connection or add the IP address to the black list.



To view the system connection logs:

**STEP 1** Click **Administration > System Log Settings > System Connection Logs** from the Navigation menu. The *System Connection Logs* window opens and displays the following information.

- **Type**—Type of log. Log types are Informational, Error, and Warning messages.
- **Date**—Date that the log occurred.
- **Time**—Time that the log occurred.
- **Users**—User or system that generated the log entry.
- **Source IP**—IP address of the user.
- **Computer Name**—Name of the computer (if applicable) or local host that generated the log entry.
- **Connection Type**—Type of connection. For example, HTTP, FTP, Telnet, SSH, AFP, SAMBA, RADIUS, or iSCSI.
- **Accessed Resources**—Type of resource accessed. For example, administrative activity, folder path, and name of files that have been accessed.
- **Action**—Type of action. Examples of action types are login, log out, write, delete, read, or rename.

- 
- STEP 2** From the drop-down list, you can filter the type of log message displayed. Log types are All events, Informational, Error, and Warning messages.
- STEP 3** From the drop-down list, **Displays records per page**, select the number of records to display.
- STEP 4** Click the arrows in the lower right to navigate forward or back on the System Connection Logs window.
- 

To configure the system connection logs options:

- 
- STEP 1** Click **Administration > System Log Settings > System Connection Logs** from the Navigation menu. The *System Connection Logs* window opens.
- STEP 2** Click **Options** to specify the connection type to be logged. The Connection Type window opens.

Set the following parameters:

- **Select the connection type**—The system supports logging the HTTP, FTP, Telnet, SSH, AFP, SAMBA, RADIUS, and iSCSI connections.
  - **When the number of logs reaches 10,000, archive the connection logs and save the file in the folder**—Click to automatically save the log files in one of the created network share folders when the logs reach 10,000 events.
    - From the drop-down list, select the network share folder location to save the logs.
- STEP 3** Click **Apply** to save the system connection logs options.
- STEP 4** Click **Start Logging** to enable the system connection logs feature. To disable this feature, click **Stop Logging**.
- 

To clear a system connection log:

- 
- STEP 1** Click **Administration > System Log Settings > System Connection Logs** from the Navigation menu. The *System Connection Logs* window opens.
- STEP 2** Right-click a single log and delete the record. Or click **Clear** to delete all of the system connection logs.
-

---

To save the system connection logs:

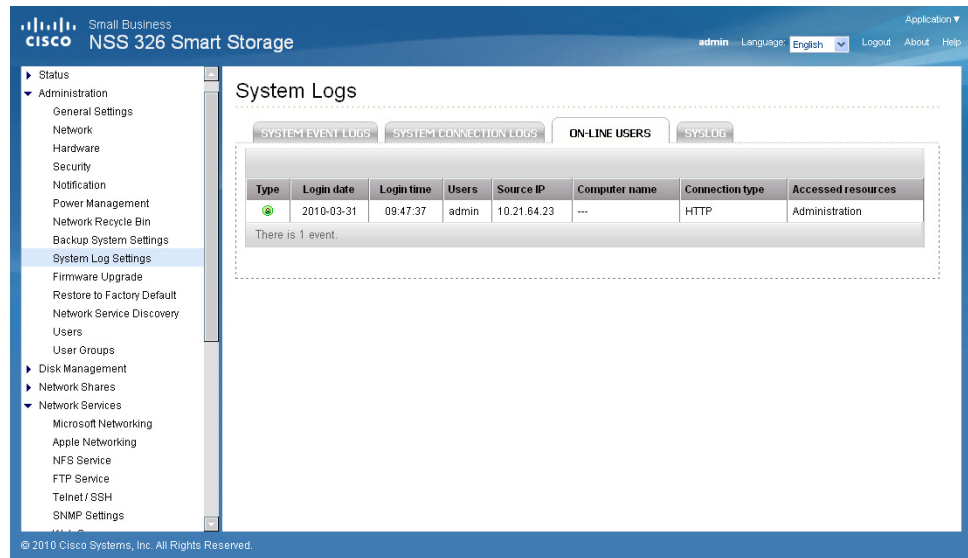
- STEP 1** Click **Administration > System Log Settings > System Connection Logs** from the Navigation menu. The *System Connection Logs* window opens and displays the following information.
- STEP 2** Click **Save** and save the .csv file generated by the system.
- 

To disconnect the IP address connection or add the IP address to the block list:

- STEP 1** Click **Administration > System Log Settings > System Connection Logs** from the Navigation menu. The *System Connection Logs* window opens.
- STEP 2** Right-click a log and select from the following options:
- **Disconnect this connection**—Select to disconnect the selected IP address.
  - **Add to the block list**—Select to block the selected IP address.
    - From the drop-down list, select the time frame that you want the IP address to be blocked.
  - **Disconnect this connection and block the IP**—Select to disconnect the connection and also block the IP address.
- STEP 3** Click **OK** to save the settings or click **Cancel** to exit.
- 

### On-Line Users

From the *Administration > System Log Settings > On-Line Users* window, you can view information about the users accessing the system. This displays real-time status versus system log information.



- **Type**—Real-time status for on-line users.
- **Login Date**—Date that the user logged in.
- **Login Time**—Time that the user logged in.
- **Users**—User or system that generated the log entry.
- **Source IP**—IP address of the user.
- **Computer Name**—Name of the computer (if applicable) or local host that generated the log entry.
- **Connection Type**—Type of connection. For example, HTTP, FTP, Telnet, SSH, AFP, SAMBA, RADIUS, or iSCSI.
- **Accessed Resources**—Type of resource accessed. For example, administrative activity or network share folder.

From the *Administration > System Log Settings > On-Line Users* window, you can disconnect the IP address connection or add the IP address to the block list.

To disconnect the IP address connection or add the IP address to the block list:

**STEP 1** Click **Administration > System Log Settings > On-Line Users** from the Navigation menu. The *On-Line Users* window opens.

**STEP 2** Right-click a log and select from the following options:

- **Disconnect this connection**—Select to disconnect the selected IP address.

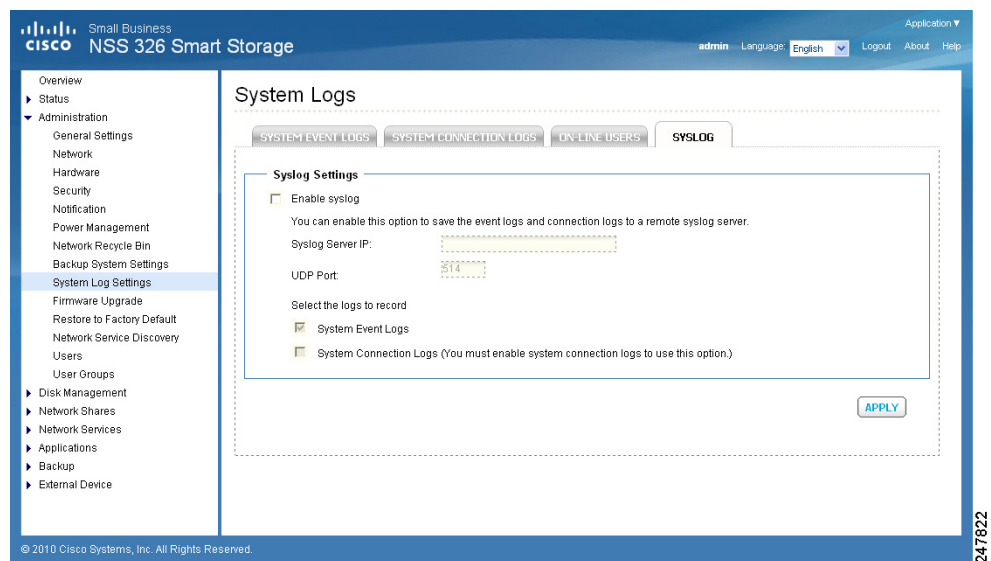


- **Add to the block list**—Select to block the selected IP address.
  - From the drop-down list, select the time frame that you want the IP address to be blocked.
- **Disconnect this connection and block the IP**—Select to disconnect the connection and also block the IP address.

**STEP 3** Click **OK** to save the settings or click **Cancel** to exit.

## Syslog

From the *Administration > System Log Settings > Syslog* window, you can enable syslog to save the event logs and connection logs to a remote syslog server. Syslog is a standard for forwarding log messages in an IP network. The NAS has a built-in syslog server. For more information, see [Syslog Server, page 150](#).



To configure the syslog settings:

- STEP 1** Click **Administration > System Log Settings > Syslog** from the Navigation menu. The *Syslog* window opens.
- STEP 2** Click **Enable syslog**.
- STEP 3** Enter the hostname or IP address of the syslog server in the Syslog Server field.

**STEP 4** In the **UDP Port** field, enter the UDP port number used to transmit syslog messages. Default is 514.

**STEP 5** Select the logs to record.

- **System Event Logs**—Enable to record the system event logs.
- **System Connection Logs**—Enable to record the system connection logs. You must enable and configure the syslog server from *Applications > Syslog Server* in order to use this feature.

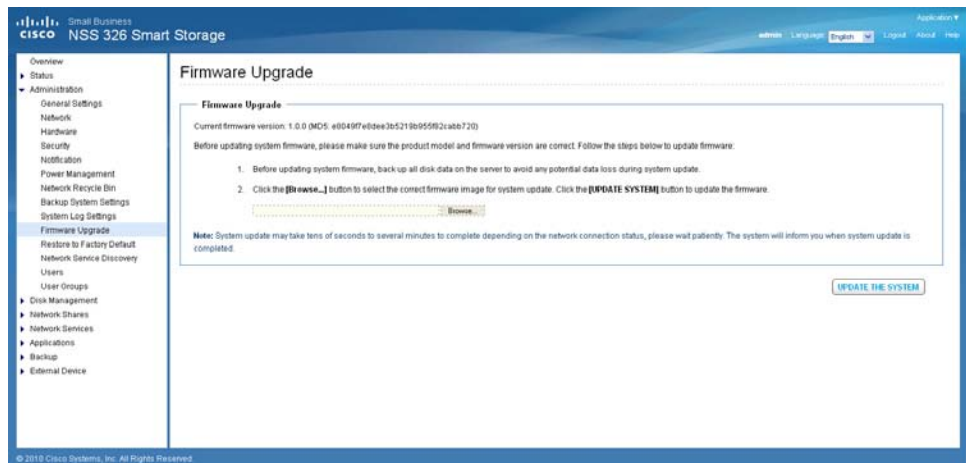
**STEP 6** Click **Apply** to save the syslog settings.

## Firmware Upgrade

From the *Administration > Firmware Upgrade* window, you can view the current firmware version and update the firmware on the NAS. The current NAS settings will not change while performing the firmware version update.



**CAUTION** As a precautionary measure, backup the NAS system configuration before upgrading the firmware.



---

To upgrade the firmware:

- 
- STEP 1** Click **Administration > Firmware Upgrade** from the Navigation menu. The *Firmware Upgrade* window opens. The current firmware version is displayed.
- STEP 2** Click **Browse** to locate the correct firmware file for the system update. Before updating the system, verify that the product model and firmware version you are going to update is correct.



---

**CAUTION** As a precautionary measure, backup the NAS system configuration before upgrading the firmware.

---

- STEP 3** Click **Update The System**.

Within 15 seconds, a MD5 checksum result window will display to confirm the integrity of the system. After the successful integrity check of the NAS, click **OK** for the new firmware file to upload to the NAS. After this has completed, a message displays and asks you to reboot the system. Please wait patiently. A system log in window will automatically display after the successful update to the new firmware.

---

## Restore to Factory Default

From the *Administration > Restore to Factory Default* window, you can restore all NAS settings to the factory default settings.



---

**CAUTION** When you restore to the factory default settings, all of the drive data, user accounts, network shares, and system settings are cleared and restored to default. Please back up all important data and system settings before resetting the NAS.

---



To restore factory defaults:

- STEP 1** Click **Administration > Restore to Factory Default** from the Navigation menu. The *Factory Default* window opens.
- STEP 2** Click **Reset** to reset all settings to factory default.



**CAUTION** When you restore to the factory default settings, all of the drive data, user accounts, network shares, and system settings are cleared and restored to default. Please back up all important data and system settings before resetting the NAS.

- STEP 3** Click **OK** to continue or **Cancel** to exit.

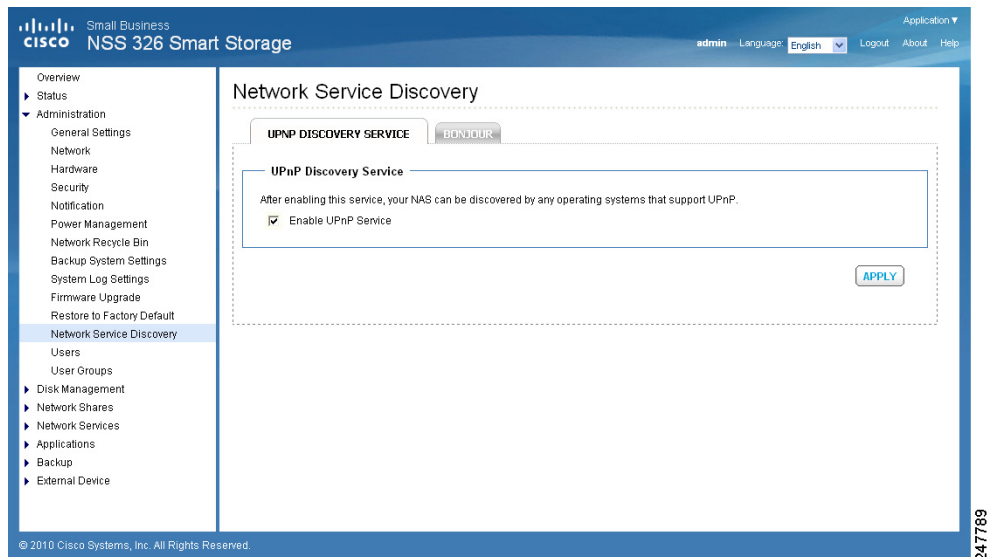
## Network Service Discovery

This section describes the following network discovery configurations:

- **UPnP Discovery Service**
- **Bonjour**

## UPnP Discovery Service

From the *Administration > Network Service Discovery > UPnP Discovery Service* window, you can enable UPnP discovery service. When a device is added to the network, the UPnP discovery protocol allows the device to advertise its services to the control points on the network. By enabling the UPnP Discovery Service, the NAS can be discovered by any operating systems that support UPnP.



To enable UPnP discovery service:

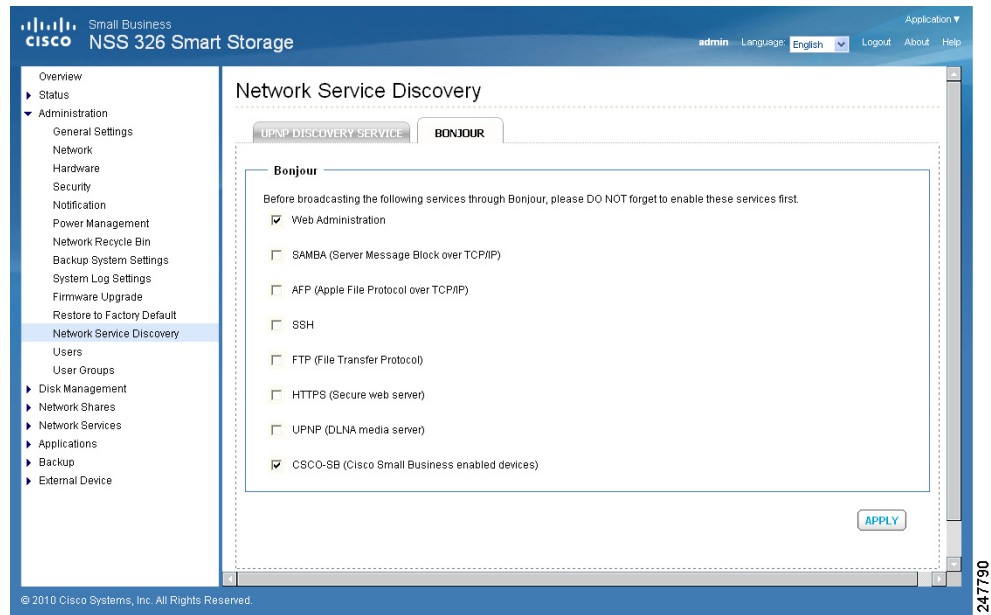
- STEP 1** Click **Administration > Network Service Discovery > UPnP Discovery Service** from the Navigation menu. The *UPnP Discovery Service* window opens.
- STEP 2** Click **Enable UPnP Service**.
- STEP 3** Click **Apply** to save the setting.

## Bonjour

From the *Administration > Network Service Discovery > Bonjour* window, you can broadcast the network services using Bonjour. By broadcasting the network services with Bonjour, your Mac and Windows will automatically discover the network services, such as FTP, which are running on the NAS without the need to enter the IP addresses or configure the DNS servers.

If you are using Windows, you can utilize Bonjour by installing Bonjour for Windows or the Cisco FindIT Network Discovery Utility.

**NOTE** Prior to enabling the service from the *Administration > Network Service Discovery > Bonjour* window, you need to activate each network service, such as FTP, in order to allow the NAS to advertise the service with Bonjour.



To broadcast network services using Bonjour:

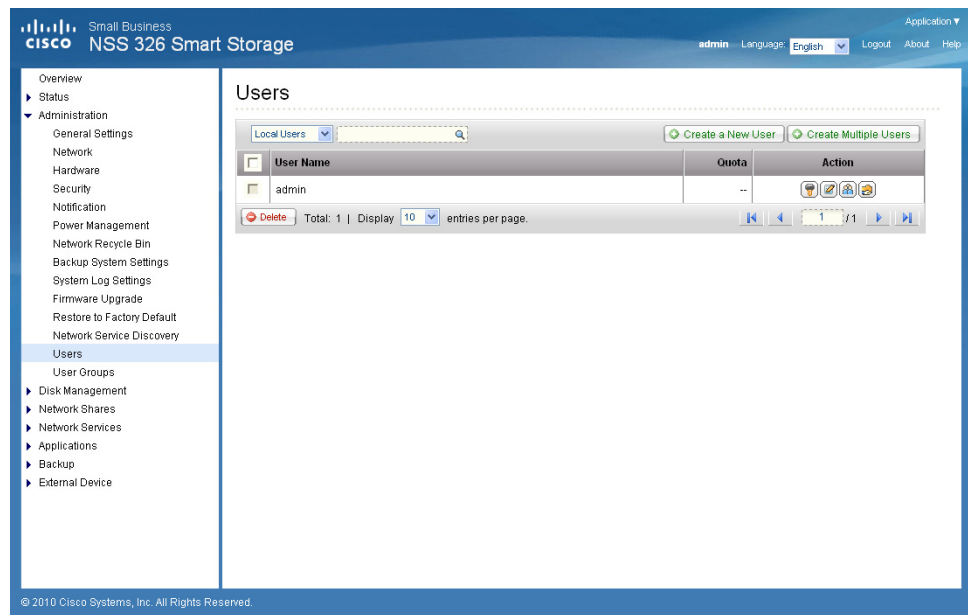
- STEP 1** Click **Administration > Network Service Discovery > Bonjour** from the Navigation menu. The *Bonjour* window opens.
- STEP 2** Select the network services that you want to broadcast with Bonjour. The following network services are listed:
  - **Web Administration**— Web administration
  - **SAMBA**—Server Message Block over TCP/IP
  - **AFP**—Apple File Protocol over TCP/IP
  - **SSH**— Secure Shell
  - **FTP**—File Transfer Protocol
  - **HTTPS**—Secure web server
  - **UPNP**—DLNA media server

- **CSCO-SB**—Cisco Small Business enabled devices

**STEP 3** Click **Apply** to save the settings.

## Users

From the *Administration > Users* window, you can view a list of users, create a new user, create multiple users, configure user settings, and delete users.



The system creates the following users by default:

- **admin**—By default, the administrator **admin** has access to system administration and cannot be deleted.
- **guest**—This user is not displayed on this window. A guest does not belong to any user group. The login password for guest is **guest**.
- **anonymous**—This user is not displayed on this window. When connecting to the server using FTP service, you can use this name to login as a guest.

**NOTE** A maximum of 4096 local users can be created. This number includes the system default users.

---

To view the users:

- 
- STEP 1** Click **Administration > Users** from the Navigation menu. The *Users* window opens and displays the following information.
- **User Name**—A list of the users assigned to this NAS.
  - **Quota**—Space allocated for this user.
  - **Action**—An action to perform for this user. Options are Change Password, Edit Account, User Groups, and Private Network Share.
- STEP 2** From the drop-down list, you can select to view:
- **Local Users**—Select to view the local users assigned to this NAS.
  - **Domain Users**—Select to view the domain users assigned to this NAS.
- STEP 3** Type a user name in the search field to search for a specific user.
- STEP 4** From the drop-down list, **Displays entries per page**, select the number of entries to display.
- STEP 5** Click the arrows in the lower right to navigate forward and back on the User window.

---

To create a user:

- 
- STEP 1** Click **Administration > Users** from the Navigation menu. The *Users* window opens.
- STEP 2** Click **Create a New User**. The *Add a New User* wizard window opens to guide you through the new user settings.
- **User Information**—User Name and password.
  - **Quota**—Quota settings. This is disabled by default when creating a new user.
  - **User Group**—Collection of users with the same access right to the share folders.
  - **Personal Share Folder**—Share folder for the user.
  - **Privilege**—Privilege for the share folders. Privilege access options are read only, read/write, and deny access.
- STEP 3** Click **Next** to continue to User Information settings.



**STEP 4** Enter the user information:

- **User Name**—User name. The user name must not exceed 32 characters. It is case-sensitive and supports double-byte characters, such as Chinese, Japanese, and Korean. The following characters are not supported:

" / \ [ ] : ; | = , + \* ? < > ` ' %

- **Password**—Password. It is recommended to use a password with at least 6 characters.
- **Verify Password**—Enter the password again to verify the password.

**STEP 5** Click **Next** to continue to Quota settings. The Quota settings are disabled by default.

To enable quota settings for all users at a later date from *Network Shares > Quota*. See [Quota, page 122](#). When this feature is enabled and you add a new user account, the quota settings will display as enabled. If quota settings are enabled for all users and you need to set up a specific user, see *Administration > Users* and click **Edit Account** to specify the quota limit.

**STEP 6** Click **Next** to continue to Group Name.

**STEP 7** Select a group from the following options:

- **administrators**—All members in this group have administration rights. You cannot delete this group.
- **everyone**—All users, by default, belong to the everyone group. You cannot delete this group.

**STEP 8** Click **Next** to continue to Personal Share Folder.

**STEP 9** Choose the default settings or configure the following parameters from the Personal Share Folder window:

- **Create Personal Share Folder**—Select to create a personal share folder. The default is No.
- **New Folder Name**—Enter a name for the new folder.
- **Hide Folder**—Select Yes to hide the folder. The default is No. If a personal folder is selected Yes to hide, this personal folder will not be seen by any other user accounts, including administrator accounts, when accessed from a Windows, Unix, or Mac platform. Only an user account assigned to this personal folder can see it. Later if you want to change this folder for others to see, go to that share and edit the account.

- **Lock file (oplocks)**—Yes is the default. Click No to unlock the file. By default, the folder is locked so that another user cannot write to this file. Only an administrator account can override this privilege.
- **Disk Volume**—From the drop-down list, select the disk volume.
- **Path**—Specify the path for the share folder you are creating from the following options:
  - **Specify path automatically**—Select to specify path automatically.
  - **Enter path manually**—Select to manually enter the path and description. Click the left mouse cursor in the field to see the existing network share folder paths. You can choose the path provided from the list to create your personal folder.
- **Description**—Enter the description of the personal share folder.

**STEP 10** Click **Next** to continue to the Share Folders window.

**STEP 11** From the Share Folders window, you can select the user access privilege for the listed share folders. The options are:

- **Read only**—Allow read only access to share folder.
- **Read/Write**—Allow read/write access to share folder.
- **Deny Access**—Deny access to share folder.

**STEP 12** Click **Next** to confirm the settings. The Confirm Settings window opens.

**STEP 13** Click **Next**, then **Finish** to complete adding a new user. The User window opens and the new user is listed.

---

To create multiple users:

---

**STEP 1** Click **Administration > Users** from the Navigation menu. The *Users* window opens.

**STEP 2** Click **Create Multiple Users**. The *Create Multiple Users* wizard window opens to guide you through the settings.

**STEP 3** Click **Next** to continue to the Account Login Info window.

**STEP 4** Enter the parameters.

- **User Name Prefix**—User name prefix. For example, this could be a department prefix such as Engineering or Marketing.

- **User Name Start No**—Number that will be appended to the first user created for the multiple users.
- **Number of Users**—Number of multiple users that you want to create.
- **Password**—Password. It is recommended to use a password with at least 6 characters.
- **Verify Password**—Enter the password again to verify the password.

**STEP 5** Click **Next** to proceed to the *Create Private Network Share* window.

**STEP 6** Select one of the following options from the *Create Private Network Share* window.

- **Yes**—Creates a private network share folder for each user. When selected and Next is clicked, the following parameters display:
  - **Hide Network Drive**—Select Yes to hide the folder. The default is No. If a personal folder is selected Yes to hide, this personal folder will not be seen by any other user accounts, including administrator accounts, when accessed from a Windows, Unix, or Mac platform. Only an user account assigned to this personal folder can see it. Later if you want to change this folder for others to see, go to that share and edit the account.
  - **Lock file (oplocks)**—Yes is the default. Click No to unlock the file. By default, the folder is protected so that another user cannot delete files from this folder. Only an administrator account can override this privilege.
  - **Disk volume**—From the drop-down, select the disk volume.
- **No**—When selected, the wizard completes adding the new multiple users. The share folder privileges can be configured separately and at a later time.

**STEP 7** Click **Next**. The *User* window opens and the new multiple users are listed. If you selected to create private network share folders for each user, the share folders can be viewed by clicking the **Private Network Share** icon in Actions.

---

To delete a user:

**STEP 1** Click **Administration > Users** from the Navigation menu. The Users window opens.

**STEP 2** Click the check box next to the user name that you want to delete.

**STEP 3** Click **Delete**.

---

**STEP 4** Click **OK** to continue or **Cancel** to exit.

---

## User Groups

From the *Administration > User Groups* window, you can view a list of user groups, create a user group, configure user group settings, and delete user groups.

A user group is a collection of users with the same access right to the share folders. User groups simplify group access to a share. A common example is adding new employees to a department. Rather than setting individual share folder permissions for each employee, simply add a new user to the group and that user will have all the share folder privileges of the group.

The NAS has created the following user groups by default:

- **administrators**—All members in this group have administration right. You cannot delete this group.
- **everyone**—All registered users belong to the everyone group. You cannot delete this group.

**NOTE** A maximum of 4096 groups can be created. This number includes the system default user groups.

The screenshot displays the Cisco Small Business NSS 326 Smart Storage Administration web interface. The top navigation bar includes the Cisco logo, the product name 'NSS 326 Smart Storage', the user 'admin', the language 'English', and links for 'Logout', 'About', and 'Help'. A left-hand navigation menu lists various system settings, with 'User Groups' currently selected. The main content area is titled 'User Groups' and features a search bar, a 'Create a User Group' button, and a table listing existing groups. The table has two columns: 'Group Name' and 'Action'. Three groups are listed: 'administrators', 'everyone', and 'testgroup'. Each group has three action icons: a magnifying glass (search), a person icon (add user), and a trash can (delete). Below the table, there is a 'Delete' button, a total count of 3, and a display setting of 10 entries per page. The footer contains the copyright notice '© 2010 Cisco Systems, Inc. All Rights Reserved.' and the ID '247628'.

Group Name	Action
administrators	[Search] [Add User] [Delete]
everyone	[Search] [Add User] [Delete]
testgroup	[Search] [Add User] [Delete]

---

To view the user groups:

- 
- STEP 1** Click **Administration > User Groups** from the Navigation menu. The *User Groups* window opens and displays the following information.
- **Group Name**—A list of the user groups assigned to this NAS.
  - **Action**—An action to perform for this user group. Options are Details, Edit Group Users, and Private Network Share.
- STEP 2** From the drop-down list, you can select to view:
- **Local Groups**—Select to view the local groups assigned to this NAS.
  - **Domain Groups**—Select to view the domain groups assigned to this NAS.
- STEP 3** Type a user group name in the search field to search for a specific group.
- STEP 4** From the drop-down list, **Displays entries per page**, select the number of entries to display.
- STEP 5** Click the arrows in the lower right to navigate forward and back on the User window.

---

To create a user group:

- 
- STEP 1** Click **Administration > User Groups** from the Navigation menu. The *User Groups* window opens.
- STEP 2** Click **Create a User Group**. The *Create a User Group* wizard window opens to guide you through the new group settings.
- **User Group Name**—Enter the User Group name.  
A group name must not exceed 256 characters. It is case-sensitive and supports double-byte characters, such as Chinese, Japanese, and Korean. The following characters are not supported:  
" / \ [ ] : ; | = , + \* ? < > ` ' %
- STEP 3** Click **Next** to continue to the *Assign Users* window.
- **Yes**—Click to assign users to the user group. Continue to Step 4.
  - **No**—Click to exit the wizard and add users to the user group at a later time.
- STEP 4** Click **Next** to continue to the user name list.

- 
- STEP 5** Click the check box next to the user name that you want to add to the group.
- STEP 6** Click **Next** to continue and **Finish** to complete the process of creating a group. You are returned to the *User Group* window and the new group is displayed in the *Group Name* list.
- 

To delete a user group:

---

- STEP 1** Click **Administration > User Groups** from the Navigation menu. The *User Groups* window opens.
- STEP 2** Click the check box next to the user group name that you want to delete.
- STEP 3** Click **Delete**.
- STEP 4** Click **OK** to continue or **Cancel** to exit.
- 

## Disk Management

This section describes the functions under Disk Management that let you configure the disks and view disk status. The following topics are included:

- **Volume Management**
- **RAID Management**
- **HDD SMART**
- **Encrypted File System**
- **iSCSI**
- **Virtual Disk**

## Volume Management

The *Disk Management > Volume Management* window shows the model, size, and current status of the disks in the NAS. You can format volumes, check disks, and scan bad blocks on the disk.

The screenshot displays the 'Volume Management' interface for a Cisco Small Business NSS 326 Smart Storage device. The interface includes a navigation menu on the left and a main content area with several options for creating disk volumes:

- Single Disk Volume:** Create single disk volume(s).
- RAID 1 Mirroring Disk Volume:** Create mirroring disk volume(s).
- RAID 0 Striping Disk Volume:** Create one striping disk volume.
- JBOD Linear Disk Volume:** Create one linear disk volume.
- RAID 5 Disk Volume:** Combine 3 or more disks to create a disk volume with data protection (1 failed disk is allowed).
- RAID 6 Disk Volume:** Combine 4 or more disks to create a disk volume with data protection (2 failed disks are allowed).

Below these options, there are two tables showing the current disk volume configurations:

**Current Disk Volume Configuration: Physical Disks**

Disk	Model	Capacity	Status	Bad Blocks Scan	SMART Information
Drive 1	WDC WD2500AAJS-65M0A01.0	232.89 GB	Ready	SCAN NOW	GOOD
Drive 2	WDC WD2500AAJS-65M0A01.0	232.89 GB	Ready	SCAN NOW	GOOD
Drive 3	WDC WD2500AAJS-65M0A01.0	232.89 GB	Ready	SCAN NOW	GOOD
Drive 4	WDC WD2500AAJS-65M0A01.0	232.89 GB	Ready	SCAN NOW	GOOD
Drive 5	WDC WD2500AAJS-65M0A01.0	232.89 GB	Ready	SCAN NOW	GOOD
Drive 6	WDC WD2500AAJS-65M0A01.0	232.89 GB	Ready	SCAN NOW	GOOD

**Current Disk Volume Configuration: Logical Volumes**

Volume	File System	Total Size	Free Size	Status
RAID 6 Disk Volume: Drive 1 2 3 4 5 6	EXT4	911.03 GB	910.81 GB	Ready

At the bottom of the logical volumes table, there are buttons for **FORMAT NOW**, **CHECK NOW**, and **REMOVE NOW**.



Depending on the NAS model that you own, volumes can be created in the following volume types:

Volume Type	Description
Single Disk Volume	Each disk will be used as a standalone disk. However, if a disk is damaged, all data will be lost.
RAID 1 Mirroring Disk Volume	RAID 1 (mirroring disk) protects your data by automatically backing up the contents of one drive onto the second drive of a mirrored pair. This protects your data if one of the drives fails. Unfortunately, the storing capacity is equal to a single drive, as the second drive is used to automatically back up the first. Mirroring Disk is suitable for personal or corporate use to store important data.
RAID 0 Striping Disk Volume	RAID 0 (striping disk) combines 2 or more drives into one larger disk. It offers the fastest disk access but it does not have any protection of your data if the striped array fails. The disk capacity equals the number of drives in the array times the size of the smallest drive. Striping disk is usually used to maximize your disk capacity or for fast disk access but not for storing important data.
Linear Disk Volume (JBOD)	JBOD is also defined as “Just a Bunch of Disks.” You can combine two or more disks into one larger disk. When a file is saved, it will be saved on physical disks sequentially, but does not have a disk failure file protection function. The overall capacity of linear disk is the sum of all disks. Linear disk is generally used for storing large data and is not appropriate to use for file protection of sensitive data.

Volume Type	Description
<p>RAID 5 Disk Volume</p>	<p>RAID 5 disk volume is ideal for organizations running databases and other transaction-based applications that require storage efficiency and data protection.</p> <p>To create a RAID 5 disk volume, a minimum of 3 hard disks are required. The total capacity of RAID 5 disk volume equals the size of the smallest capacity disk in the array x (number of hard disks -1). It is recommended that you use the same brand and same capacity hard drive to establish the most efficient hard drive capacity.</p> <p>Additionally, if your system contains four disk drives, three of them can be used to implement RAID 5 data disks and the fourth drive can be used as a spare disk. When a physical disk failure occurs, the system will automatically rebuild the data with the spare disk.</p> <p>RAID 5 can survive 1 disk failure and the system can still operate properly. When a disk fails in RAID 5, the disk volume will be in “degraded mode.” There is no more data protection at this stage. If one more disk fails, all data will be lost. Therefore, you must replace a new disk immediately. You can install a new disk after turning off the server or hot swap the new disk when the server is on. The status of the disk volume will be “rebuilding” after installing a new disk. When rebuilding completes, your disk volume resumes to normal status.</p> <p>To install a disk when the server is on, make sure the disk volume is in “degraded” mode. Or wait for two long beeps after the disk crash, then insert the new disk.</p>

Volume Type	Description
RAID 6 Disk Volume	<p>RAID 6 disk volume is ideal for important data protection.</p> <p>To create a RAID 6 disk volume, a minimum of 4 hard disks are required. The total capacity of RAID 6 disk volume equals the size of the smallest capacity disk in the array x (number of hard disks -2). It is recommended that you use same brand and same capacity hard drive to establish the most efficient hard drive capacity.</p> <p>RAID 6 can survive 2 drives failure and system can still operate properly.</p> <p><b>NOTE</b> To install a disk when the server is on, make sure the disk volume is in “degraded” mode. Or wait for two long beeps after the disk crash, and then insert the new disk.</p>
RAID 5, RAID 6 Read-only Mode	<p>The drive configuration enters read-only mode in the following occasions:</p> <ul style="list-style-type: none"> <li>▪ 2 drives are damaged in RAID 5</li> <li>▪ 3 drives are damaged in RAID 6</li> </ul> <p>The drives in the above configurations are read-only. It is recommended to re-create new drive configuration in such case.</p>

To create a volume type:

- STEP 1** Choose **Disk Management > Volume Management** from the Navigation menu. The *Volume Management* window opens.
- STEP 2** Click on a desired volume type that is supported by your NAS.
- STEP 3** Choose parameters for your selected volume type.
- STEP 4** Click **Create**.

---

To scan for bad blocks on a disk:

- 
- STEP 1** Choose **Disk Management > Volume Management** from the Navigation menu. The *Volume Management* window opens.
- STEP 2** Click **Scan Now** for the drive that you want to scan. The status of the scan is shown in the Status column.
- 

To format a volume:

- 
- STEP 1** Choose **Disk Management > Volume Management** from the Navigation menu. The *Volume Management* window opens.



---

**CAUTION** Formatting a volume will remove all data from it.

---

- STEP 2** Click **Format Now** on the volume that you want to format.
- STEP 3** Choose a file system type and click **OK**.
- 

When the disk is formatted, the NAS will create the following default share folders:

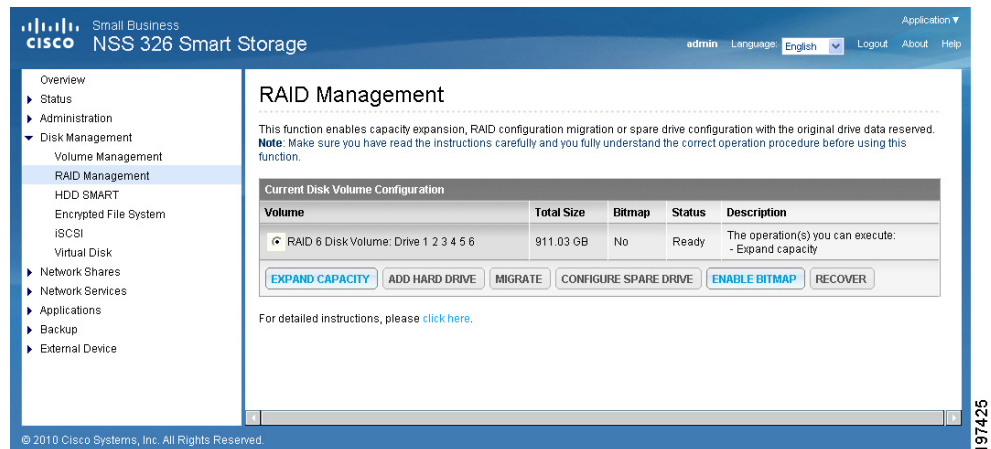
- **Public**—Network share for file sharing.
- **Download**—Network share for Download Station.
- **Multimedia**—Network share for Multimedia Station.
- **Usb**—Network share for data copy function via USB ports.
- **Web**—Network share for Web Server.
- **Network Recycle Bin 1**—Default network recycle bin share for deleted files. You need to enable the network recycle bin from the *Administration > Network Recycle Bin* window.

To check a volume:

- STEP 1** Choose **Disk Management > Volume Management** from the Navigation menu. The Volume Management window opens.
- STEP 2** Click **Check Now** on the volume that you want to check.

## RAID Management

The RAID Management function enables capacity expansion, RAID configuration migration, or spare drive configuration while preserving the original drive data.



The following actions are available in the *Disk Management > RAID Management* window:

Action	Description
Expand capacity	This action enables drive capacity expansion by replacing the drives in an array one by one. Expand capacity is supported for the following drive configurations: RAID 1 expansion, RAID 5 expansion, RAID 6 expansion.
Add hard drive	This action enables adding new drive member to a drive configuration. Add hard drive is supported by the following drive configurations: RAID 5 and RAID 6 expansion.

Action	Description
Migrate	This action enables a drive configuration to be migrated to a different RAID configuration. Migrate is supported for the following drive configurations: Migrate single drive to RAID 1, 5, or 6, Migrate RAID 1 to RAID 5 or 6, Migrate RAID 5 to RAID 6.
Configure spare drive	This action allows you to add or remove a RAID 5 spare drive.
Start BITMAP/Stop BITMAP	Bitmap improves the time for rebuilding after a crash, or removing/re-adding a device. It does not improve normal read/write performance, and might even cause a small degradation in performance. However, if an array has a bitmap a device can be removed and re-added and only blocks changes need to be made since the removal (as recorded in the bitmap) can be resynced. Bitmap support is only available for RAID 1, 5, and 6.
Recover	This action can recover a failed RAID disk volume from “inactive” status to the normal state (RAID 1, 5, and 6 will be recovered to the degrade mode, RAID 0 and JBOD will be recovered to the normal state). Before recovering the failed disk volume, confirm that all hard disks of the disk volume are properly seated in the NAS drive bay. Once recovery is completed, back up your disk data immediately in case the disk volume fails again. Not all inactive RAID disk volumes can be recovered.

To expand the capacity of a disk volume:



**CAUTION** Do not turn off power to the NAS during this process.

- STEP 1** Choose **Disk Management > RAID Management** from the Navigation menu. The *RAID Management* window opens.
- STEP 2** Click on the volume that you want to expand.
- STEP 3** Click **Expand Capacity**. The *Expand capacity* window opens.
- STEP 4** On the drive that you want to expand capacity, click **Change**.

- 
- STEP 5** After the text in the Description field says “You can replace this drive,” then replace with specified drive with one that has more capacity.
  - STEP 6** Wait for the NAS to beep twice after removing the hard drive.
  - STEP 7** After the text in the Description field says “Please insert the new drive,” then insert the drive into the drive slot.
  - STEP 8** After inserting the hard drive, wait for the NAS to beep. The NAS will then start rebuilding the RAID array.
- 

To add a hard drive:

- 
- STEP 1** Choose **Disk Management > RAID Management** from the Navigation menu. The *RAID Management* window opens.
  - STEP 2** Select the hard drive to add to the RAID configuration.
  - STEP 3** Click **Add Hard Drive**.
  - STEP 4** Select the hard drive to add to the RAID and click **Add Hard Drive**. All data on the selected drive will be deleted during this process. Click **OK** to confirm. The NAS will beep twice.



- 
- CAUTION** This process may take as little as a few hours or more than 24 hours to complete depending on the number and size of the drives being replaced. Please wait patiently for the process to finish. Do not turn off power to the NAS during this process.
- 

After drive expansion, the number of drives in the configuration and the total capacity will reflect the changes implemented. You can use the larger capacity.

---

To migrate a disk configuration to a higher RAID level:

- 
- STEP 1** Prepare a hard drive of the same format and same capacity (or larger) as an existing drive in the RAID configuration. The drive configuration status must be “Ready.”
  - STEP 2** Choose **Disk Management > RAID Management** from the Navigation menu. The *RAID Management* window opens.

---

**STEP 3** Select an available drive and click **Migrate**.

**STEP 4** Select one or more available drives. The drive capacity after migration is displayed. Click **Migrate**.

When migration is in process, the required time and total drive capacity after migration are displayed in the “Description” field. After migration completes, the new drive configuration is displayed and the status is Ready. You can use the new drive configuration.

---

To configure a spare drive:

---

**STEP 1** Prepare a drive of the same format and same capacity (or larger) as an existing drive in the RAID configuration. The drive configuration status must be Ready.

**STEP 2** Choose **Disk Management > RAID Management** from the Navigation menu. The *RAID Management* window opens.

**STEP 3** Select a volume to have a spare drive added to it and click **Configure Spare Drive**.

**STEP 4** Select a drive to be added to the volume that you previously selected and click **Configure Spare Drive**. When you add a spare drive, all the data on the selected drive will be deleted during this process. Click **OK** to proceed.

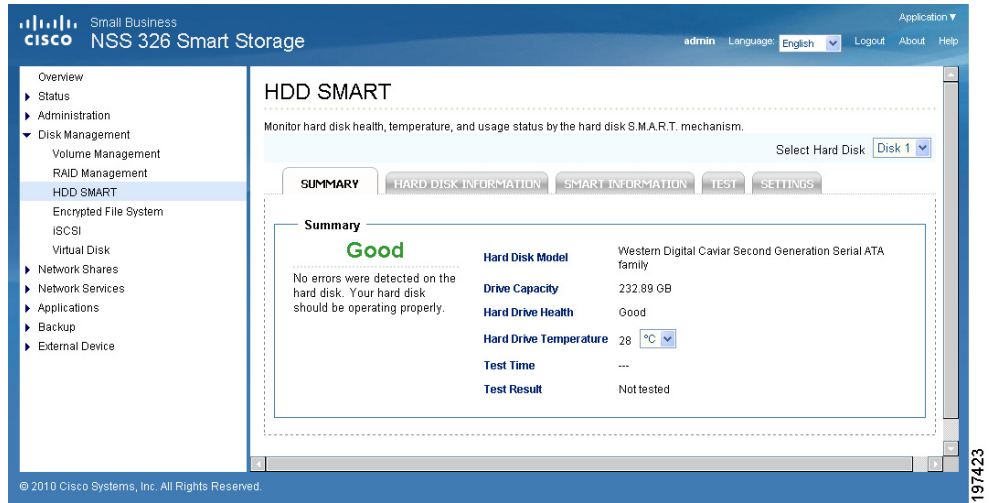
After the configuration completes, the drive configuration is updated and the status is Ready. You can use the drive configuration.

---

## HDD SMART

The *Disk Management > HDD SMART* windows enables users to monitor hard drive health, temperature, and usage status by the hard disk S.M.A.R.T. mechanism.





Tab	Description
Summary	Shows the hard disk SMART summary and the latest test results.
Hard disk information	Shows hard disk model, number, serial number, disk capacity, firmware, and ATA information.
SMART information	Shows the hard disk SMART summary and the latest test results.
Test	Select to execute the a rapid or complete SMART test for the hard disk. The test result will be shown.
Settings	Select to enable temperature alarm. When the hard disk temperature exceeds the configured limit, the system records an error message. The rapid and complete test schedules can be configured. The latest test results can be viewed on the Summary window.

To view a summary of hard disk health:

- Choose **Disk Management > HDD SMART > Summary** from the Navigation menu. The *Summary* window opens.

---

To view hard disk information:

- Choose **Disk Management > HDD SMART > Hard Disk Information** from the Navigation menu. The *Hard Disk Information* window opens.
- 

To view hard disk SMART information:

- 
- STEP 1** Choose **Disk Management > HDD SMART > SMART Information** from the Navigation menu. The *SMART Information* window opens.
- STEP 2** Select the hard disk that you want to view SMART information. The window display SMART information on the selected drive.
- 

To test a hard disk:

- 
- STEP 1** Choose **Disk Management > HDD SMART > Test** from the Navigation menu. The *Test* window opens.
- STEP 2** Select the hard disk that you want to test.
- STEP 3** Choose either **Rapid Test** or **Complete Test** to test the hard disk. The Complete Test is more thorough, but will take longer to test.
- STEP 4** Click **Test**.
- 

To set temperature alarm settings and schedule hard disk tests:

- 
- STEP 1** Choose **Disk Management > HDD SMART > Settings** from the Navigation menu. The *Settings* window opens.
- STEP 2** Select the hard disk that you want to configure.
- STEP 3** Click **Enable Temperature Alarm** and choose an alarm temperature value to enable a temperature alarm.
- STEP 4** Click **Enable Rapid Test** and choose a time period to schedule a rapid test.
- STEP 5** Click **Enable Complete Test** and choose a time period to schedule a complete test.
- STEP 6** Click **Apply**.
-

---

## Encrypted File System

From the *Disk Management > Encrypted File System* window, you can manage the encrypted disk volumes on the NAS. Each encrypted disk volume is locked by a particular key. The encrypted volume can be unlocked by the following methods:

- **Encryption Password**—Enter the encryption password to unlock the disk volume. The default password is “admin.”
- **Encryption Key File**—You can upload the encryption file to the server to unlock the disk volume. The key can be downloaded from “Encryption Key Management” window after you have unlocked the disk volume successfully.

You can create encrypted volumes in *Disk Management > Volume Management* window and encrypted volumes can only be configured when creating a disk volume.

To manage disk volume encryption:

- 
- STEP 1** Choose **Disk Management > Encrypted File System** from the Navigation menu. The *Disk Volume Encryption Management* window opens.
  - STEP 2** Click **Encryption Key Management**. The *Encryption Key Management* window opens.
  - STEP 3** Choose encryption options and click **Apply**.
- 

## iSCSI

The NAS supports built-in Internet Small Computer System Interface (iSCSI) service which allows the transmission of SCSI commands over an IP network. From the *Disk Management > iSCSI* window, you can enable iSCSI, view or create a iSCSI target list.



To enable iSCSI for the NAS:

- STEP 1** Install an iSCSI initiator on your computer (Windows PC, Mac, or Linux).
- STEP 2** Choose **Disk Management > iSCSI** from the Navigation menu. The *iSCSI/Configuration* window opens.
- STEP 3** Click **Enable iSCSI Target Service** and enter an iSCSI Service Port number.
- STEP 4** Optionally, click **Enable iSNS** to enable Internet Storage Name Service (iSNS) and enter the iSNS Server IP address.
- STEP 5** Click **Apply** to save the settings.

To create a new iSCSI target:

- STEP 1** Choose **Disk Management > iSCSI > iSCSI Target List** from the Navigation menu. The *iSCSI Target List* window opens.
- STEP 2** Click **Create New iSCSI Target**.
- STEP 3** Enter the iSCSI target parameters.

#### iSCSI Target Profile

- **Target Name**—Enter the target name for the iSCSI storage resource.

#### iSCSI Target LUN (Logical Unit Number)

- **Allocate the disk space now**—Check to allocate disk space.

**NOTE** If you select not to allocate the disk space now, the disk space can be more flexibly used. However, it is not guaranteed that the iSCSI target has enough disk space as specified. You may increase the physical disk capacity by “Online RAID Capacity Expansion” (available in RAID 1, 5, 6).

- **Volume**—From the drop-down list, select the disk volume.
- **Capacity**—Move the slider to increase or decrease the capacity.

#### Type

- **None**—Click to use no authentication between the iSCSI initiator and targets. The default is None.
- **CHAP**—Click to use the CHAP authentication protocol.
  - **User Name**—Enter the user name for CHAP authentication.
  - **Password**—Enter the password.
  - **Re-enter Password**—Re-enter the password for verification.
- **Mutual CHAP**—Click to use the CHAP authentication protocol between the iSCSI initiator and targets.
  - **Initiator Name**—Enter the initiator name for the mutual CHAP authentication.
  - **Password**—Enter the password.
  - **Re-enter Password**—Re-enter the password for verification.

#### CRC/Checksum (Optional)

- **Data Digest**—Click to use the data digest procedure when identifying and verifying the checksum.
- **Header Digest**—Click to use the header digest procedure when identifying and verifying the checksum.

**STEP 4** Click **Apply** to save the iSCSI target parameters.

**STEP 5** Run the iSCSI initiator (Windows PC, Mac, or Linux) and connect to the iSCSI target (NAS).

After successful logon, format the iSCSI target (disk volume). You can start to use the disk volume on the NAS as a virtual drive on your computer.

**NOTE** The NAS supports a maximum of 8 iSCSI devices.

---

## Virtual Disk

The Virtual Disk (VD) is based on iSCSI technology, which makes it become the stack master and can connect to the other stack targets. With the VD, you can expand the capacity of your NAS and use it as the system disk volume(s). In addition, you can create disk shares and use them for data exchange, storage and backup, just like the local disk shares.

**NOTE** This function and its content is only applicable on some NAS models.

Each virtual disk drive will be recognized as a single logical volume in the local system.

To add a virtual disk:

- 
- STEP 1** Choose **Disk Management > Virtual Disk** from the Navigation menu. The *Virtual Disk* window opens.
  - STEP 2** Click **Add Virtual Disk**.
  - STEP 3** Enter the target server IP and port number (default: 3260). Click **Get Remote Disk**. If authentication is required, enter the user name and password. Then, click **Apply**.
  - STEP 4** When the status of the virtual disk is “Ready,” you can start to use the virtual disk as a disk volume of the NAS.
- 

The NAS supports a maximum of eight virtual disks.

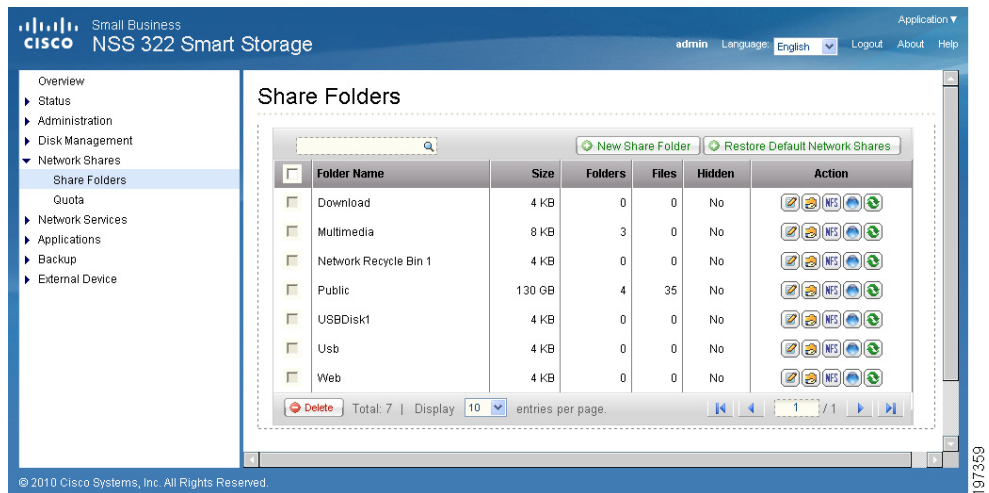
## Network Shares

This section describes creating network share folders and editing the access rights of users and user groups. The following topics are included:

- **Share Folders**
- **Quota**

## Share Folders



The primary purpose of a network share is for sharing files over a network. Under a standard operating environment you can create different network shares for various file types and provide different access rights to users or user groups to shared folders. Several default network shares are created during system initialization and installation.



## Action Buttons

In the Share Folders window there are a number of actions that you can perform on each share folder as described below.

Action Name	Icon	Description
Property		Click this icon to edit the share folder property, including disk volume, hide network drive, lock file, path, comment, and enable write-only FTP access.
Access Control		Click this icon to edit the access right of the users and user groups to the share folder.
NFS Access Control		Click this icon to edit the NFS access right of the share folder.

Action Name	Icon	Description
WebDAV Access Control		Click this icon to edit the WebDAV (Web-based Distributed Authoring and Versioning) access control of the share folder. You can edit the WebDAV access right of the local users and local groups, and edit the access rights of guests who could remotely access the share folders by web browser. To use this function, you must enable WebDAV and Web server from the <i>Network Services &gt; Web Server</i> window.
Refresh		Click this icon to refresh the information of the share folder.  <b>NOTE</b> Share Folder status does not update dynamically. You must click <b>Refresh</b> for the latest status. By default, the system will automatically refresh all shares by 2:00 a.m. (0200) based on the NAS system clock.

### NFS Access Control

You can set the NFS access rights for a network share as described below.

Field	Description
No Limit	Unlimited access allows the user to create, read, write, and delete files or folders in the network share and any subfolders.
Read Only	Read Only access allows the user to read files in the network share and any subfolders but denies functions to write, create, or delete.
Deny Access	Denies all access to files and folders in the network share.

The format of an allowed IP address or domain name is shown below:

- **Single server**—A valid domain name, IP address, or host name that can be resolved by a DNS server.
- **Use wildcard characters to specify a series of servers**—Use “\*” or “?” to specify the string criteria. When you use wildcard characters in a valid host name, dot (.) is not included in wildcard characters. For example, when you enter \*.example.com, one.example.com is counted while one.two.example.com is not counted.



- **IP network**—Can be specified in two formats. The first format is a.b.c.d/x, where a.b.c.d refers to the network and x refers to number of bits of the network mask. For example, the IP configuration can be specified as 192.168.0.0/24. The second valid format is a.b.c.d/network mask. In this case, a.b.c.d refers to the network and the following value refers to the network mask setting. For example, the same IP configuration can be specified as 192.168.100.8/255.255.255.0.
- **Network group**—Represented as @group-name; group-name refers to the name of NIS network group.

**NOTE** Make sure the format you enter is correct. An incorrect format can lead to access errors.

### WebDAV Access Control

You can set up WebDAV folder access controls. WebDAV is a set of extensions to the HTTP or HTTPS protocol that allows the users to edit and manage files on remote World Wide Web servers. Users and User Group rights can be set to Full Access, Deny Access or Read Only. WebDAV access right settings applied to a folder will be granted to all users who are given access this share folder; they will share the same access right settings.

To create a new share folder:

- 
- STEP 1** Choose **Network Shares > Share Folders** from the Navigation menu. The *Share Folders* window opens.
  - STEP 2** Click **New Share Folder**. The *Create a Share Folder Wizard* opens. Click **Next** to continue.
    - Enter a folder name for the share folder.
    - Choose a disk volume for the share folder.
    - Choose whether you want to hide the share folder in My Network Places.
    - Choose whether to lock open files (oplocks) in the share folder.
    - Choose whether to automatically specify a path for the share folder or you can manually enter a path.
    - Enter a description for the share folder.
    - Click **Next**.
  - STEP 3** Select a privilege level and guest access rights for the share folder and click **Next**.

- STEP 4** Select read/write access by user and click **Next**.
- STEP 5** A confirm settings window opens, click **Next** if you agree with the settings or click **Back** to change any settings.
- STEP 6** Click **Finish** to exit the Share Folder Wizard.

To restore default network shares:

- STEP 1** Choose **Network Shares > Share Folders** from the Navigation menu. The *Share Folders* window opens.
- STEP 2** Click **Restore Default Network Shares**. A dialog asks if you are sure that you want to restore default network shares. Click **OK** to continue.

## Quota

From the *Network Shares > Quota* window, you can enable the quota settings for all the users and specify the quota size they are allowed to use on each disk volume of the NAS. This function is disabled by default.

Small Business  
cisco NSS 322 Smart Storage

admin Language: English Logout About Help

Overview  
 ▶ Status  
 ▶ Administration  
 ▶ Disk Management  
 ▶ Network Shares  
     Share Folders  
     **Quota**  
 ▶ Network Services  
 ▶ Applications  
 ▶ Backup  
 ▶ External Device

### Quota

**Quota**

Enable quota for all users

Quota size on the disk: 1000 MB

**Note:** Individual user quota size can be changed in [Users - Quota Settings \[Users\]](#)

APPLY SHOW QUOTA

Striping Disk Volume: Drive 1 2 (Free Size : 332612 MB)			
Users	Quota Size	Used Size	Status
admin	--	0.03 MB	No size limitation
guest	1000.00 MB	0.00 MB	Available 1000.00 MB
User	1000.00 MB	0.00 MB	Available 1000.00 MB

© 2010 Cisco Systems, Inc. All Rights Reserved. 197358

---

Field	Description
Enable Quota for all users	The Quota function is disabled by default. You can activate this function to manage or allocate disk space for each user.
Quota size on the disk	Set quota size for each user's access authorization to the disk. A user is denied the right to create new files or directories once the quota size is exceeded. This integer number entered in the quota field must be greater than 0 and cannot exceed the supported limit up to 2,000,000 MB (2 TB).

To enable quota for all users:

- 
- STEP 1** Choose **Network Shares > Quota** from the Navigation menu. The *Quota* window opens.
  - STEP 2** Click **Enable quota for all users** to enable a quota size to be applied to all users.
  - STEP 3** Enter a quota size in MB.
  - STEP 4** Click **Apply**. Your Quota settings are updated to the NAS.

**NOTE** You can change the individual user quote size in *Administration > Users > Edit Account Profile*.

---

---

## Network Services

This section describes the following network services that are supported on the NAS.

- **Microsoft Networking**
- **Apple Networking**
- **NFS Service**
- **FTP Service**
- **Telnet/SSH**
- **SNMP Settings**
- **Web Server**

### Microsoft Networking

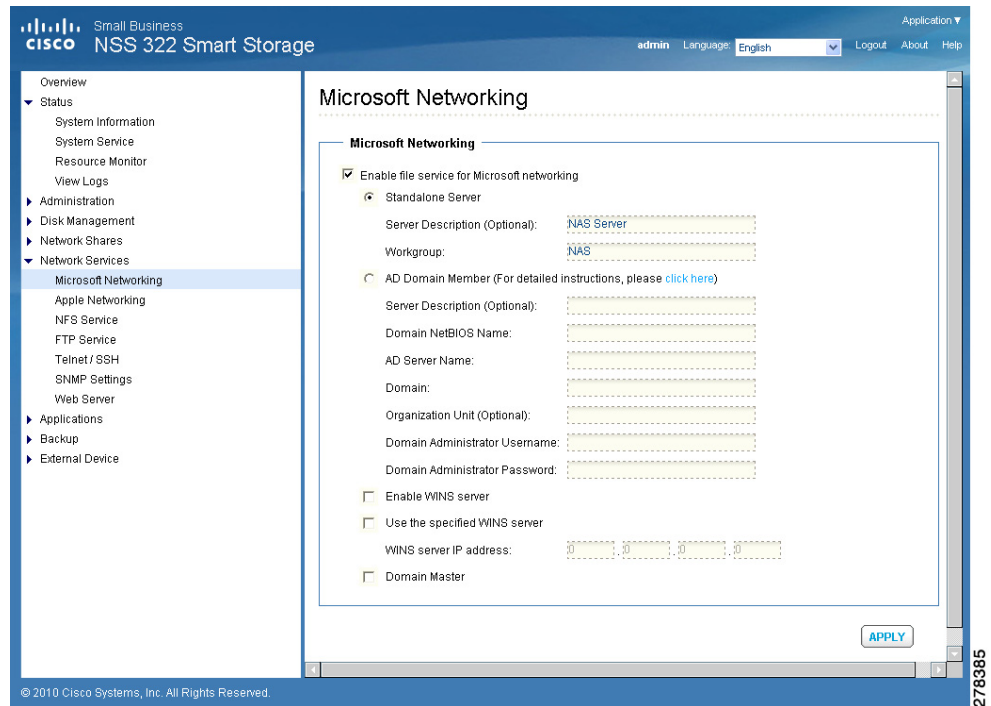
The NAS device supports Microsoft networking protocols used with home and business LANs.

Microsoft Windows users must enable Microsoft networking in order to access the files on network share folders. After enabling this option, you must assign a workgroup name. The workgroup name must not exceed 15 characters. The following characters are not supported:

" / \ [ ] : ; | = , + \* ? < > ` ' %

**NOTE** The first character cannot be a period (.).

The NAS device can be configured as a standalone server or member of the Windows Active Directory® (AD). AD can centralize the information about users, groups of users, and computers and manage them in a more advanced network. Through the network, AD Server can offer other computers and network devices within the same domain correct account information so that the information system of the organization can be safer and more convenient.



To enable Microsoft networking:

- STEP 1** Choose **Network Services > Microsoft Networking** from the Navigation menu. The *Microsoft Networking* window opens.
- STEP 2** Click **Enable file service for Microsoft networking** to enable Microsoft networking.
- STEP 3** Select either **Standalone Server** or **AD Domain Member** networking type and enter the appropriate parameters according to the the networking type that you choose.
  - **Standalone Server**—Use local Users for user authentication.

Field	Description
Server Description (Optional)	Describe the NAS so that users can easily identify the server. For example, the name of the administrator or department, or the location of the server.
Workgroup	Specify the workgroup to which the NAS belongs.

—OR—

- **AD Domain Member**—Use a Microsoft AD domain to authenticate users.

Field	Description
Server Description (Optional)	Describe the NAS so that users can easily identify the server. For example, the name of the administrator or department, or the location of the server.
Domain NetBIOS Name	Enter the NetBIOS domain name from the AD Domain server. To identify the name, from the AD server open a window from <i>Control Panel &gt; System Properties</i> . The name that displays in the Domain field is the domain name. The NetBIOS domain name is the first occurrence of the domain name. For example, if the domain name is “Cisco.com,” the NetBIOS domain name is “Cisco” without “.com.”
AD Server Name	The name of the AD server. To identify the name, from the AD server open a window from <i>Control Panel &gt; System Properties</i> . <ul style="list-style-type: none"> <li>▪ A name displays in the title computer name as the AD server name (Windows 2008 only).</li> <li>▪ For Windows 2003, the format display from the server is different. The AD server name is part the computer name. Example in Windows 2003: computer name displays “aaaaaa.bbbbbbb.com” where “aaaaaa” is the AD server name and “bbbbbb.com” is the domain name.</li> </ul>
Domain	Enter the AD server domain name. To identify the name, from the AD server open a window from <i>Control Panel &gt; System Properties</i> . The name that displays in the Domain field is the domain name.
Organization Unit (Optional)	Organization Unit provides a unique way to classify users, groups of users, or computers located in the AD domain directories. The purpose of Organization Unit is to differentiate between objects (users, groups of users, or computers) with the same name, primarily to parcel out authority to manage objects.
Domain Administrator Username	Enter the AD domain administrator username to login to the AD domain server for NAS to import AD user and group profiles.

Field	Description
Domain Administrator Password	Enter the AD domain administrator password for AD domain server authentication.

- STEP 4** Click **Enable WINS server** to allow the NAS AD configuration to support WINS server functionality.
- STEP 5** If there is an existing WINS server on your network and your workstation is configured to use that WINS server for name resolution, you must specify your WINS server IP address on the NAS. Click the check box **Use the specified WINS server** to enable the specified WINS server and enter the WINS server IP address.
- STEP 6** Click **Domain Master** to make the NAS responsible for keeping track of computers available on the network or the computers that have announced themselves as master browser for offering services.

**NOTE** Do not set this NAS to be the domain master if a Windows system is already set as the domain master within your network.

- STEP 7** Click **Apply**. Your Microsoft networking settings are updated to the NAS.

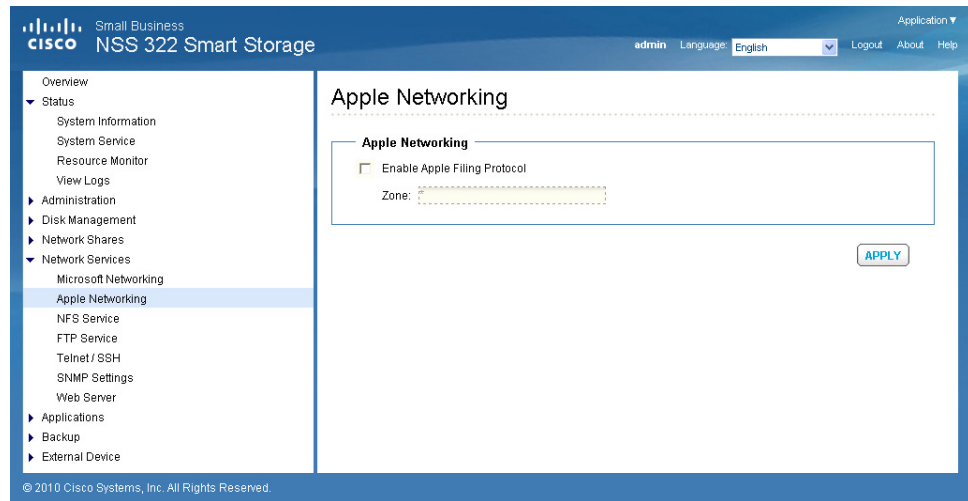
## Apple Networking

From the *Network Services > Apple Networking* window, Apple Macintosh users can enable Apple Networking in order to access network shares via the Apple File Protocol (AFP).

If your NAS is a member of an AppleTalk network that includes an extended network assigned with multiple zones, assign a zone name. The zone name must not exceed 15 characters. The following characters are not supported:

" / \ : | ? < > . %

If you do not wish to assign a network zone, enter an asterisk (\*). The asterisk (\*) is the default setting.



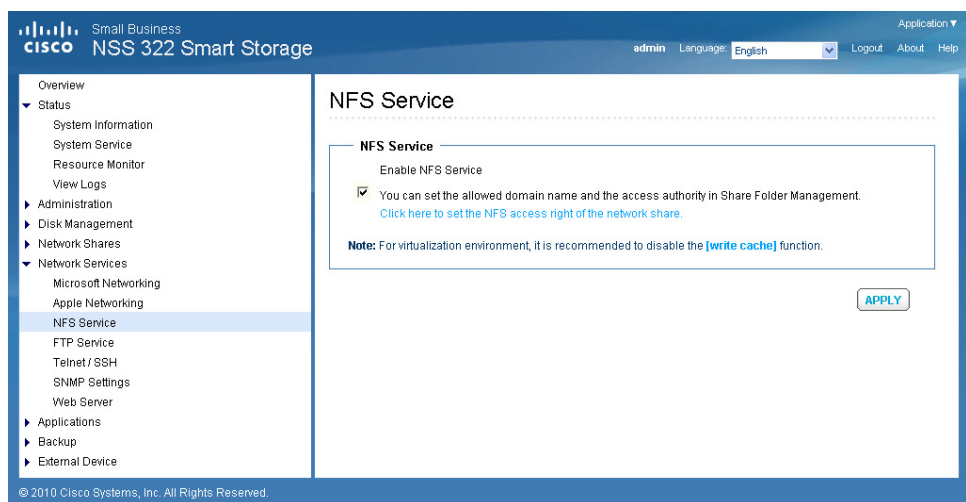
To enable Apple networking:

- STEP 1** Choose **Network Services > Apple Networking** from the Navigation menu. The *Apple Networking* window opens.
- STEP 2** Click **Enable Apple Filing Protocol** to enable Apple networking.
- STEP 3** Click **Apply**. Your Apple networking settings are updated to the NAS.

## NFS Service

From the Network Services, NFS Service window, Linux users can enable NFS Service to support file access by Linux servers.





To enable NFS service:

**STEP 1** Choose **Network Services > NFS Service** from the Navigation menu. The *NFS Service* window opens.

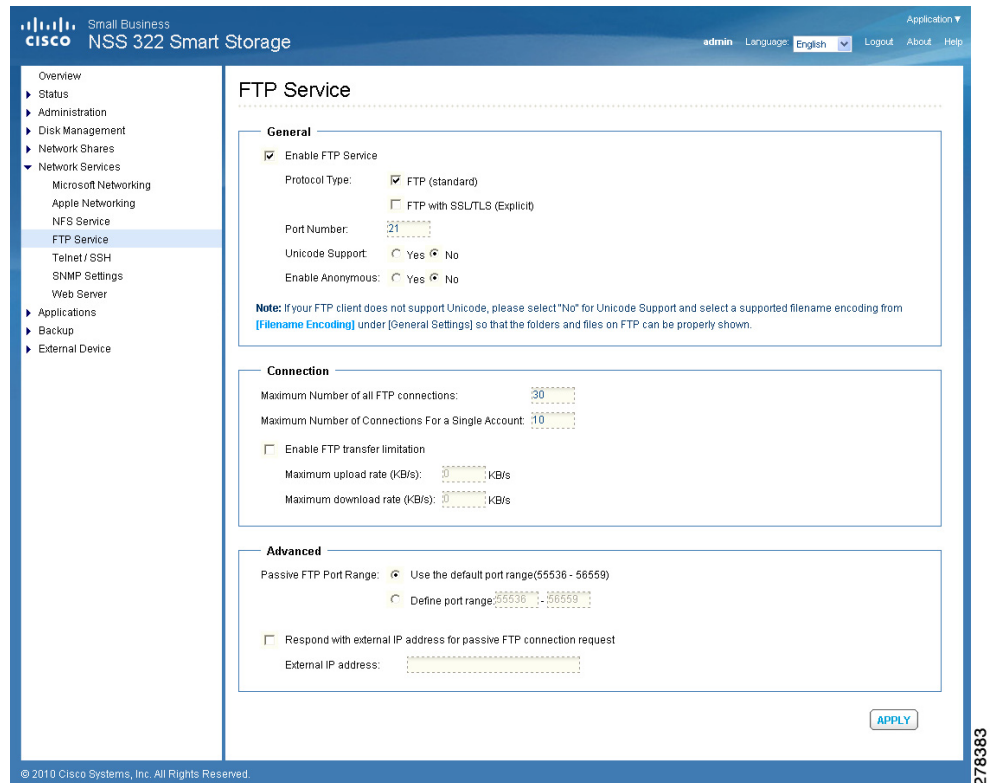
**STEP 2** Click **Enable NFS Service** to enable NFS service.

**NOTE** For virtualization environment, it is recommended that you disable the **write cache** function in the **Administration > Hardware** dialog box. Default is disabled.

**STEP 3** Click **Apply**. Your NFS service settings are updated to the NAS.

## FTP Service

FTP clients can have access to network share folders on the NAS device.



To enable FTP service:

- STEP 1** Choose **Network Services > FTP Service** from the Navigation menu. The *FTP Service* window opens.
- STEP 2** Click **Enable FTP Service** to enable FTP service.
- STEP 3** Select at least one FTP transfer protocol type:
  - **FTP (standard)**—Use general FTP protocol.
  - **FTP with SSL/TLS (Explicit)**—Use SSL or TLS Explicit encryption protocol.
- STEP 4** Enter a port number for FTP service. The default is 21.
- STEP 5** You can enable or disable Unicode Support by clicking **Yes** (enabled) or **No** (disabled) in the **Unicode Support** field. The default setting is **No**. If your FTP client does not support Unicode, select **No** for Unicode Support and select a supported filename encoding from *Administration > General Settings* so that folders and files can be displayed correctly.

**STEP 6** You can enable or disable anonymous login to the FTP site by clicking **Yes** (enabled) or **No** (disabled) in the **Enabled Anonymous** field. The default setting is **No**.

**STEP 7** Enter the FTP Connection parameters:

- **Maximum number of all FTP connections**—Maximum number of clients that can be connected at the same time. The upper limit is 256.
- **Maximum Number of Connections for a Single Account**—Maximum number of connections for a single account. The upper limit is 256.
- **FTP transfer limitation**—You can set the maximum upload and download rates. Click **Enable FTP transfer limitation** to set these parameters then enter upload and download maximum values.

**STEP 8** Enter Advanced FTP parameters:

- **Passive FTP Port Range**—You can use the default port range (55536-56559) or define a port range higher than 1024.
- **Respond with external IP address for passive FTP connection request**—You can enable this function when a remote computer is not able to connect to the FTP server using a WAN connection where the FTP server is behind a router/firewall. When this function is enabled the FTP server returns the manually specified IP address or automatically detects the external IP address so that the remote computer can connect to the FTP server successfully.

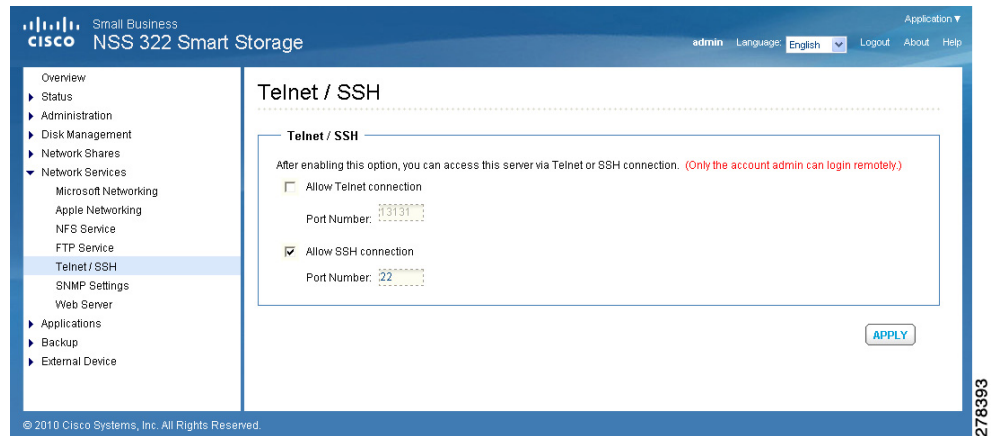
**STEP 9** Click **Apply**. Your FTP service settings are updated to the NAS.

---

## Telnet/SSH

From the *Network Services > Telnet/SSH* window, you can allow access to the NAS using a Telnet or SSH connection.

**NOTE** Only the “admin” account can login remotely. User with administrator privileges is not allowed to login remotely.

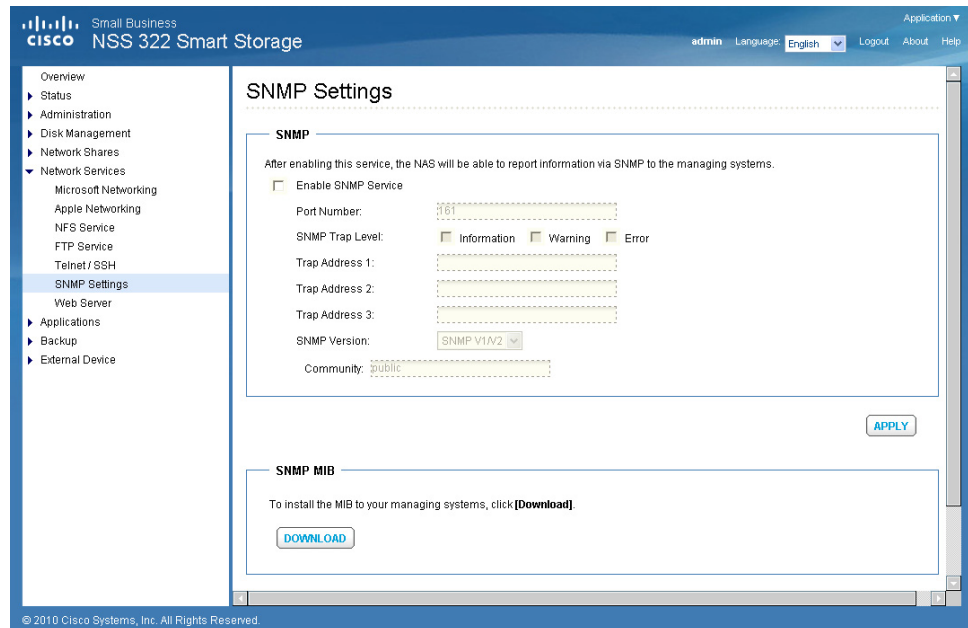


To enable Telnet/SSH remote login:

- STEP 1** Choose **Network Services > Telnet/SSH** from the Navigation menu. The *Telnet/SSH* window opens.
- STEP 2** Click **Allow Telnet connection** to enable Telnet/SSH remote login.
- STEP 3** Enter a Port Number for Telnet. The default port is 23.
- STEP 4** Click **Allow SSH connection** to enable SSH connection.
- STEP 5** Enter a Port Number for SSH connection. The default value is 22.
- STEP 6** Click **Apply**. Your Telnet/SSH settings are updated to the NAS.

## SNMP Settings

From the *Network Services > SNMP Settings* window, you can configure Simple Network Management Protocol (SNMP), which is widely used in network management systems to monitor appliances attached to a network such as a NAS. You can set up SNMP traps to be alerted via SNMP. You can enter up to three SNMP trap addresses. In addition, you can also select the system event log level in SNMP.



To enable SNMP service:

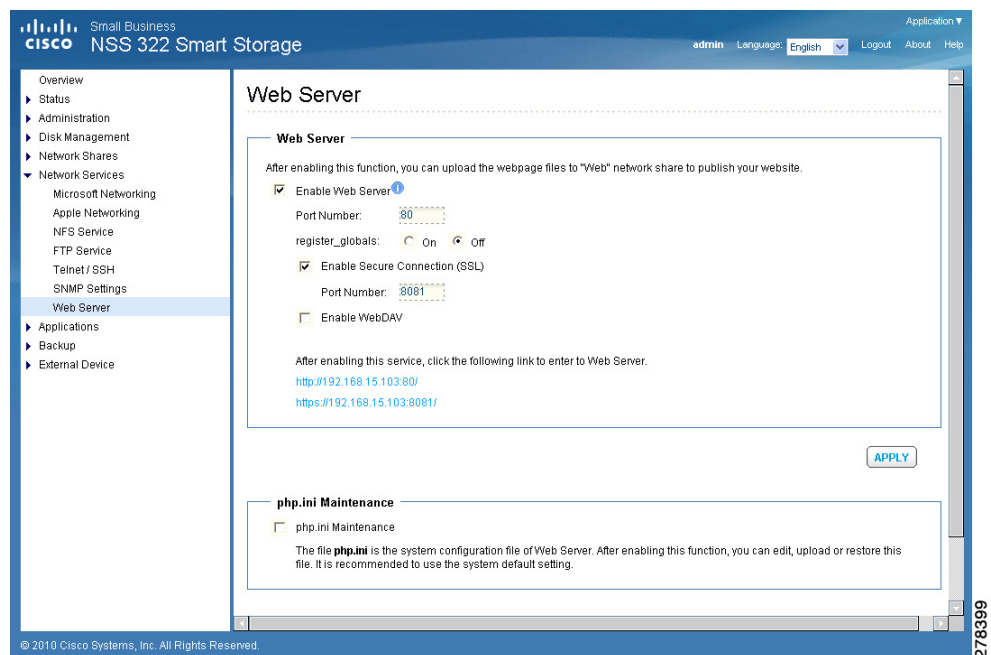
- STEP 1** Choose **Network Services > SNMP Settings** from the Navigation menu. The *SNMP Settings* window opens.
- STEP 2** Click **Enable SNMP Service** to enable SNMP service.
- STEP 3** Enter a Port Number for SNMP service. The default value is 161.
- STEP 4** Click SNMP Trap Level types. You can choose from **Information**, **Warning**, and **Error** event log types.
- STEP 5** Specify up to three SNMP trap addresses in the **Trap Address** fields.
- STEP 6** Select an SNMP version. You can choose from SNMP V1/V2 or SNMP V3.
- STEP 7** Specify an SNMP community in **Community** field.
- STEP 8** Click **Apply**. Your SNMP settings are updated to the NAS.

**STEP 9** To install the SNMP MIB to your managing systems, click **Download** and save the file.

The MIB is a type of database in ASCII text format that is used to manage the NAS in the SNMP network. The SNMP manager uses the MIB to determine the values or understand the messages sent from the agent (NAS) within the network. You can download the MIB and view it with any word processor or text editor.

## Web Server

From the *Network Services > Web Server* window, you can enable Web Server and create a web page that is viewable either locally or on a public network. To access the NAS using a web browser, enable Web File Manager. See **Web File Manager, page 136**.



To enable web server:

- STEP 1** Choose **Network Services > Web Server** from the Navigation menu. The *Web Server* window opens.
- STEP 2** Click **Enable Web Server** to enable the web server.
- STEP 3** Enter a Port Number for the web server. The default value is 80.

- 
- STEP 4** Enable or disable `register_globals` by clicking **On** (enable) or **Off** (disable). The setting is disabled by default. When the web program asks to enable PHP `register_globals`, enable `register_globals`. However, for system security concerns, it is recommended that this option be disabled when possible.
- STEP 5** Enable SSL if a secure connection is needed by clicking **Enable Secure Connection (SSL)**. After enabling this option, users can access websites which are hosted on the NAS over SSL. The concept of HTTPS is a combination of the HTTP with the SSL/TLS to create a secure channel over the network.
- STEP 6** Enable WebDAV (Web-based Distributed Authoring and Versioning) if needed by clicking **Enable WebDAV**. WebDAV is a set of extensions to HTTP that allows users to edit and manage files collaboratively on remote World Wide Web servers. After enabling this function you can access shared folders remotely through a client application.
- NOTE** Go to **Access Right Management > Share Folders** for detailed privilege settings.
- STEP 7** Enable `php.ini` if necessary by clicking **php.ini Maintenance**. The `php.ini` file is the system configuration file for the Web Server. After enabling this function, you can edit, upload or restore this file. It is recommended that you use the system default setting.
- STEP 8** Click **Apply**. Your web server settings are updated to the NAS.
- 

## Applications

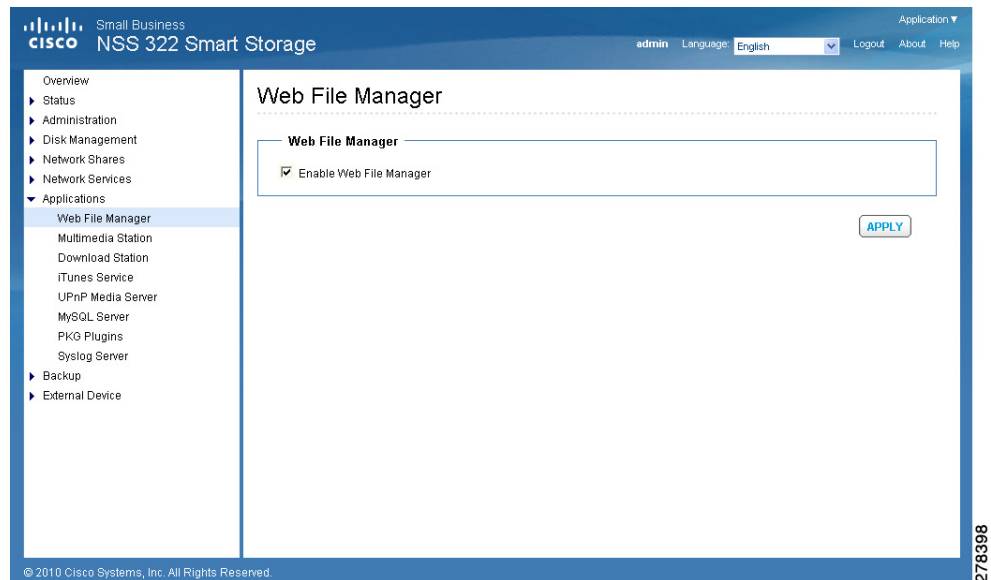
This section describes the numerous applications available that expand the NAS capabilities.

- **Web File Manager**
- **Multimedia Station**
- **Download Station**
- **iTunes Server**
- **UPnP Media Server**
- **MySQL Server**
- **PKG Plugins**

- Syslog Server

## Web File Manager

You have the option of using a web browser to access your files on this NAS. If your system is connected to the Internet and uses a public IP address, the Web File Manager allows you to access your files on the NAS using a web browser.



To enable the Web File Manager:

- STEP 1** Choose **Applications > Web File Manager** from the Navigation menu. The *Web File Manager* window opens.
- STEP 2** Click **Enable Web File Manager** to enable the Web File Manager.
- STEP 3** Click **Apply**. Your Web File Manager settings are updated to the NAS.

**NOTE** You must first create a network share before using Web File Manager. After the web file manager is enabled, it can be accessed from *Applications > Web File Manager*. If your NAS is using SSL, you can access Web File Manager from the URL **https://NAS IP:8080/cgi-bin/filemanager/**. The default port is 8080. If your NAS is configured with a different port, you need to use that port value for access to the Web File Manager application. You need a valid user account to log into the Web File Manager management GUI.



---

## Accessing the Web File Manager

This section describes how to use the Web File Manager which allows you to manage the files on your NAS from the Internet.

There are three ways to access the Web File Manager:

- Directly using the Web File Manager URL.
- From the NAS main login window.
- From the administration window.

**NOTE** You must know the IP address of your NAS to login to the Web File Manager.

To access the Web File Manager from a URL:

---

**STEP 1** From your browser, go to URL `http://<IP Address>:8080/cgi-bin/filemanager/`.

**STEP 2** Enter your Username and Password. The Web File Manager opens.

---

To access the Web File Manager from the NAS login window:

---

**STEP 1** Enter your Username and Password.

**STEP 2** From the Application drop-down list, select **Web File Manager**.

**STEP 3** Click **Login**. The *Web File Manager login* window opens.

**STEP 4** Enter your Username and Password for the Web File Manager. The *Web File Manager* opens.

---

To access the Web File Manager from the Administration window:

---

**STEP 1** Login to the Administration window.

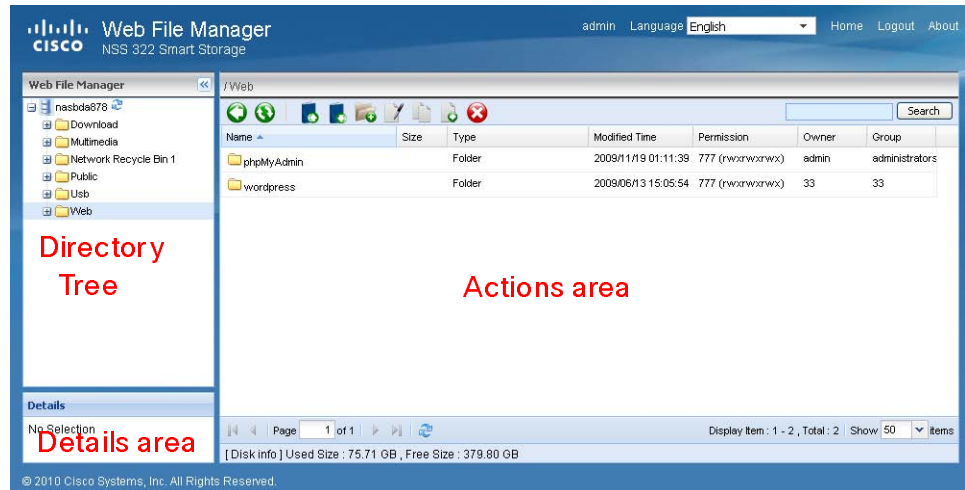
**STEP 2** Choose **Web File Manager** from the Application drop-down list, located in the top right corner of the window. The *Web File Manager* opens.

**STEP 3** If a login window appears, login to the Web File Manager.

---

## Using the Web File Manager

The Web File Manager window is composed of three areas: Directory Tree (labeled Web File Manager), Details, and the Actions area. These are explained in more detail below.










- **Directory Tree**—The Directory Tree shows a visual representation of the files and directories of your NAS. You can expand and collapse the structure by clicking on the plus (+) and minus (-) icons.
- **Details Area**—The Details area shows information on the selected file or directory such as name, size, and permissions.
- **Actions Area**—The Actions Area is the largest part of the Web File Manager where you can perform numerous actions on files and directories on your NAS. These actions are described below.

### Action Buttons

In the Web File Manager window there are a number of actions that you can perform on files as described below.

Action Name	Icon	Description
Parent Folder		Click to move to the parent folder of the currently selected file.
Refresh		Click to refresh the contents of the current directory.

Action Name	Icon	Description
Upload		Click to upload a file into the current directory.
Download		Click to download a file or directory from the current directory.
Create Folder		Click to create a new folder in the current directory.
Rename		Click to rename the currently selected file or directory.
Copy		Click to copy the currently selected file or directory.
Move		Click to move the currently selected file or directory.
Delete		Click to delete the currently selected file or directory.

To upload a file to the current directory:

**STEP 1** Click the **Upload** icon. The *Upload* window opens.

**STEP 2** Click **Browse** and select a file. Click **Open**.

**NOTE** If Skip is chosen for the Mode, the file will not be copied if another file exists with the same filename. If Overwrite is chosen for the Mode and if there is a file with the same filename, then that file will be overwritten.

**STEP 3** Click **Start**. Your files are copied to your NAS.

**STEP 4** Click the **Refresh** icon if you want to see the file in the Actions area.

To download a file from the NAS:

**STEP 1** Click the **Download** icon. The *File Download* dialog opens.

**STEP 2** Click **Save** and specify a location for the file. Click **Save**.

---

To create a new folder on the NAS:

- 
- STEP 1** Using the Directory Tree, go to the location where you want the new folder.
  - STEP 2** Click the **Create Folder** icon. The *Create folder* dialog opens.
  - STEP 3** Enter a name for the new folder and click **Ok**.
- 

To rename a file or folder on the NAS:

- 
- STEP 1** Select the file or folder that you want to rename.
  - STEP 2** Click the **Rename** icon. The *Rename* dialog opens.
  - STEP 3** Enter a new name for the file or folder and click **Ok**.
- 

To copy a file or folder on the NAS:

- 
- STEP 1** Select the file or folder that you want to copy.
  - STEP 2** Click the **Copy** icon. The *Copy to* dialog opens.
    - NOTE** If Skip is chosen for the Mode, the file will not be copied if another file exists with the same filename. If Overwrite is chosen for the Mode and if there is a file with the same filename, then that file will be overwritten.
  - STEP 3** Enter a new name for the file or folder and click **Ok**.
- 

To move a file or folder on the NAS:

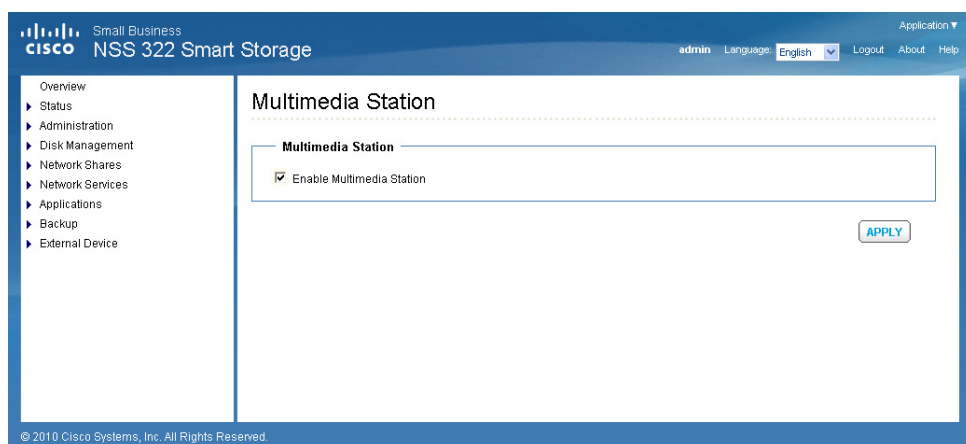
- 
- STEP 1** Select the file or folder that you want to move.
  - STEP 2** Click the **Move** icon. The *Move to* dialog opens.
    - NOTE** If Skip is chosen for the Mode, the file will not be moved if another file exists with the same filename. If Overwrite is chosen for the Mode and if there is a file with the same filename, then that file will be overwritten.
  - STEP 3** Enter a new name for the file or folder and click **Ok**.
-

To delete a file on the NAS:

- STEP 1** Select the file that you want to delete.
- STEP 2** Click the **Delete** icon. The Rename dialog opens.
- STEP 3** Click **Yes** to verify that you want to delete the file.

## Multimedia Station

From the *Applications > Multimedia Station* window, you can configure the NAS to share photos, music, or video files over the network. The Multimedia Station is a web interface that allows you to manage your multimedia files including videos, music, and photos.



To enable the Multimedia Station:

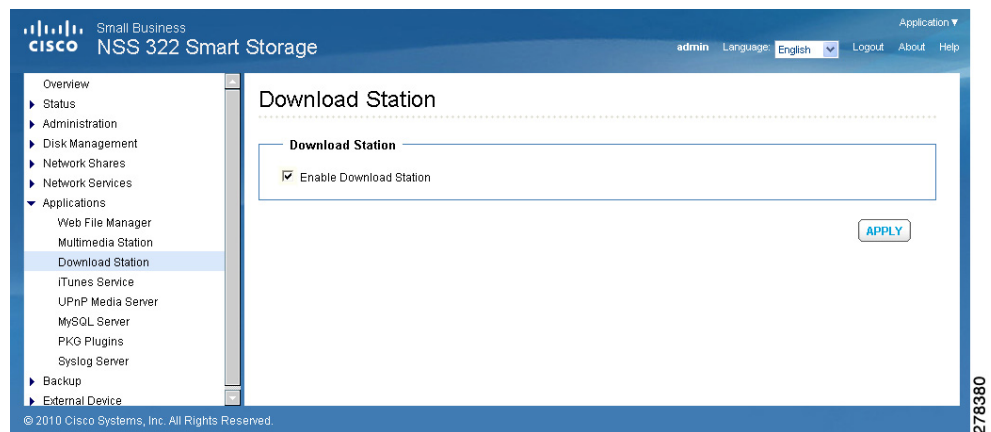
- STEP 1** Choose **Applications > Multimedia Station** from the Navigation menu. The *Multimedia Station* window opens.
- STEP 2** Click **Enable Multimedia Station** to enable the Multimedia Station.
- STEP 3** Click **Apply**. Your Multimedia Station settings are updated to the NAS.

**NOTE** After the Multimedia Station is enabled, it can be accessed by selecting *Applications > Multimedia Station* from the top right corner of the Administration window. If your NAS is using SSL, you can access Multimedia Station from the URL

<https://NAS IP:8080/Qmultimedia/>. The default port is 8080. If your NAS is configured with a different port, use that port value for access to the Multimedia Station application. You need a valid user account to log in to the main management GUI.

## Download Station

The NAS supports Bit Torrent (BT), HTTP, and FTP download. To use the download function of the NAS, you must enable the Download Station application.



**CAUTION** It is illegal to download of copyrighted materials. The Download Station functionality is provided for downloading authorized files only. Downloading or distribution of unauthorized materials may result in severe civil and criminal penalty. Users are subject to the restrictions of the copyright laws and should accept all the consequences.

To enable the Download Station:

**STEP 1** Choose **Applications > Download Station** from the Navigation menu. The *Download Station* window opens.

**STEP 2** Click **Enable Download Station** to enable Download Station.

**NOTE** After the Download Station is enabled, it can be accessed by selecting *Applications > Download Station* from the top right corner of the Administration window.

---

**STEP 3** Click **Apply**. Your Download Station settings are updated to the NAS.

---

## Accessing the Download Station

This section describes how to use the Download Station which supports BT, HTTP, and FTP download.

There are three ways to access the Download Station: directly using the Download Station URL, from the NAS main login window, or from the administration window.

**NOTE** You must know the IP address of your NAS to login to the Download Station.

To access the Download Station from a URL:

---

**STEP 1** From your browser, go to URL `http://<IP Address>:8080/cgi-bin/downloadstation/`.

**STEP 2** Enter your Username and Password. The Download Station opens.

---

To access the Download Station from the NAS login window:

---

**STEP 1** Enter your Username and Password.

**STEP 2** From the Application drop-down list, select **Download Station**.

**STEP 3** Click **Login**. The *Download Station* login window opens.

**STEP 4** Enter your Username and Password for the Download Station. The Download Station opens.

---

To access the Download Station from the Administration window:

---

**STEP 1** Login to the Administration window.

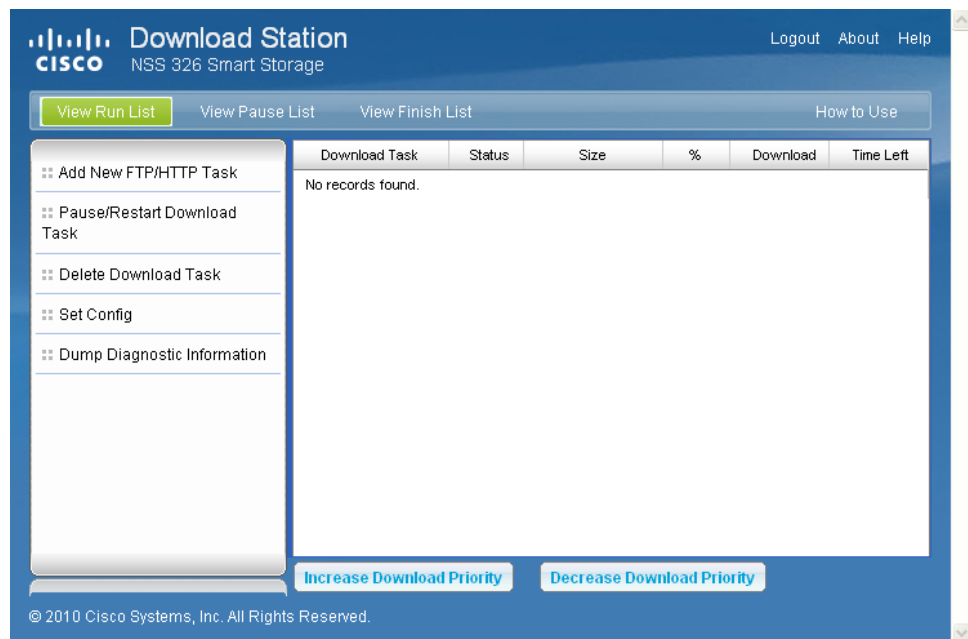
**STEP 2** Choose **Download Station** from the Application drop-down list, located in the top right corner of the window. The Download Station opens.

**STEP 3** If a login window appears, login to the Download Station.

---

## Using the Download Station

To use the download function of the NAS, you must enable the Download Station application from *Applications > Download Station*.



- **Download Task**—File name of the task.
- **Status**—Download status of the task, such as Run or Wait.
- **Size**—Total size of the task.
- **%**—Download percentage of the task.
- **Time Left**—Estimated download time of the download task.

To add a new FTP/HTTP task:

- STEP 1** Click **Add New FTP/HTTP Task**.
- STEP 2** Enter the FTP or HTTP URL of the download task and select the share folder to save the files.
- STEP 3** Enter the user name and password to access the URL of the download task (if necessary).



- 
- STEP 4** Click **Ok** to start downloading. After uploading a download task, the task will appear on the View Run List.
- 

To configure download tasks:

---

- STEP 1** Click **Set Config** and enter the number of the maximum tasks you want to download at the same time. The default is 3.
- STEP 2** Enter the maximum download rate. The default is 0, which indicates unlimited.
- STEP 3** Enter the download time settings. Select continuous download or set the daily download time. If the end time value is smaller than the start time, the end time will be treated as the time on the next day.
- 

To pause a running download task:

---

- STEP 1** Select the task in the View Run List.
- STEP 2** Click **Pause/Restart Download Task**.

You can view tasks that are paused or finished in the View Pause List and View Finish List respectively.

- STEP 3** To restart a paused task, select the task in the View Pause List and click **Pause/Restart Download Task**.
- 

To delete a running, paused, or finished task:

---

- STEP 1** Select the task from the View Run List, View Pause List, or View Finish List.
- STEP 2** Click **Delete Download Task**.

You can select to remove the download task only and retain the downloaded files, or remove the task and downloaded files.

---

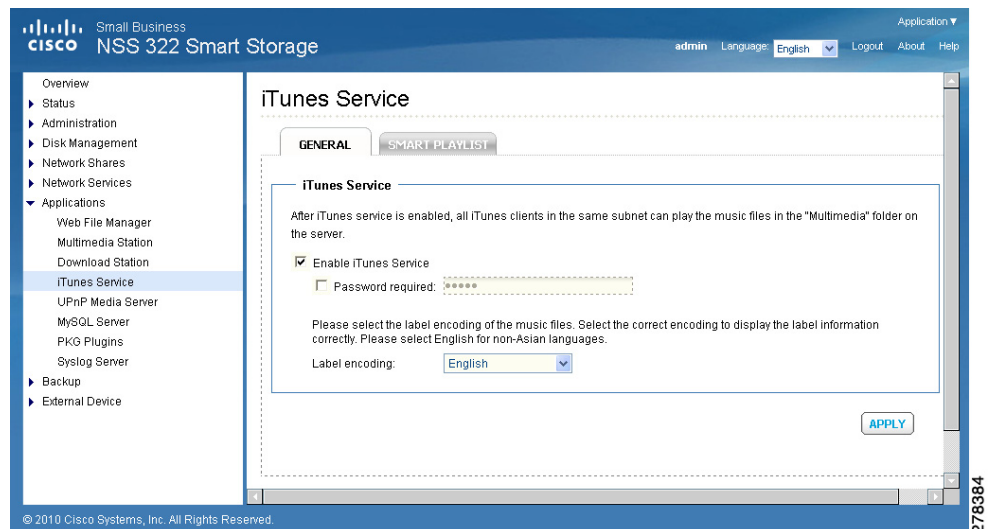
**NOTE** To access the folders you have downloaded, go to the NAS “Download” share folder.

To view diagnostic information of a download task:

- STEP 1** Select a task on the list
- STEP 2** Click **Dump Diagnostic Information**.

## iTunes Server

From the *Applications > iTunes Service* window, you can enable the iTunes Server service. When enabled, this service lets you share mp3 files that are in the Multimedia folder on the NAS. You can find, browse, and play all the music files on the NAS using computers that are on the network by using iTunes.



**NOTE** To use the iTunes Service, iTunes must be installed on your computer and music files must be uploaded to the Multimedia folder of NAS. You can download the latest iTunes software from the Apple website at <http://www.apple.com>.

To enable the iTunes Service:

- STEP 1** Choose **Applications > iTunes Service** from the Navigation menu. The *iTunes Service* window opens.
- STEP 2** Click **Enable iTunes Service** to enable iTunes Service.
- STEP 3** If you want to require the users to access the data only by entering the correct password, click **Password required** and enter a password.
- STEP 4** To display the label information correctly, select the label encoding for the music files from the **Label Encoding** drop-down list.

- STEP 5** You can define Smart playlist rules to categorize the songs into different playlists. If there is no song that matches the rules in the playlist, the iTunes client will not show the playlist. If you want to create a Smart playlist, click the **Smart Playlist** tab, click **Add**, and enter a Smart playlist. Click **Apply** to save the Smart playlist.
- STEP 6** Click **Apply**. Your iTunes Service settings are updated to the NAS.

## UPnP Media Server

The NAS offers a DLNA compatible UPnP media server called TwonkyMedia. Enable this function and the NAS will share particular music, photos, or video files to DLNA network. You can use DLNA compatible digital media player, to play the multimedia files from the NAS to your TV, or to any PC with the DLNA application, or to an acoustic sound system.

Universal Plug and Play (UPnP) is a set of computer network protocols promulgated by the UPnP Forum. UPnP allows devices to connect seamlessly and allows simplification of networks at home and in a corporate environment. UPnP achieves this by defining and publishing UPnP device control protocols built on open, Internet-based communication standards. The term UPnP comes from the term Plug-and-Play, a technology for dynamically attaching devices to a computer.



To enable the UPnP Media Server:

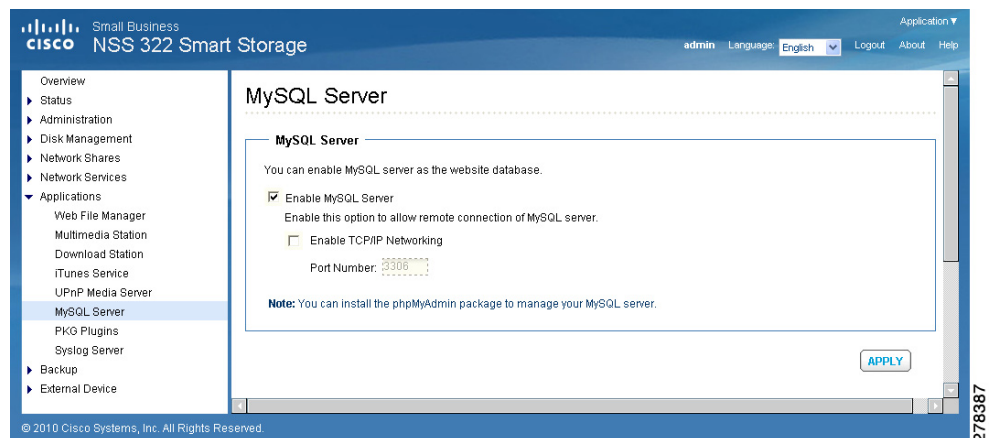
- STEP 1** Choose **Applications > UPnP Media Server** from the Navigation menu. The *UPnP Media Server* window opens.
- STEP 2** Click **Enable UPnP Media Server** to enable UPnP Media Server.

- STEP 3** If you want to view the UPnP Media Server configuration window with your browser, click **After enabling this service, click the following link to enter UPnP Media Server configuration page**. You can access the configuration page directly from **http://NAS IP:9000/** if SSL is enabled.j
- STEP 4** Click **Apply**. Your UPnP Media Server settings are updated to the NAS.

## MySQL Server

You can enable this option to configure MySQL Server of the NAS as a database server of another web server in remote site through Internet connection. When you disable this option, your MySQL Server will only be configured as local database server for the web server of the NAS.

After enabling remote connection, you can assign a port for the remote connection service of MySQL Server.



To enable MySQL Server:

- STEP 1** Choose **Applications > MySQL Server** from the Navigation menu. The *MySQL Server* window opens.
- STEP 2** Click **Enable MySQL Server** to enable MySQL Server.
- STEP 3** To enable TCP/IP Networking, click **Enable TCP/IP Networking** and specify a port number. The default port is 3306.
- STEP 4** Click **Apply**. Your MySQL Server settings are updated to the NAS.

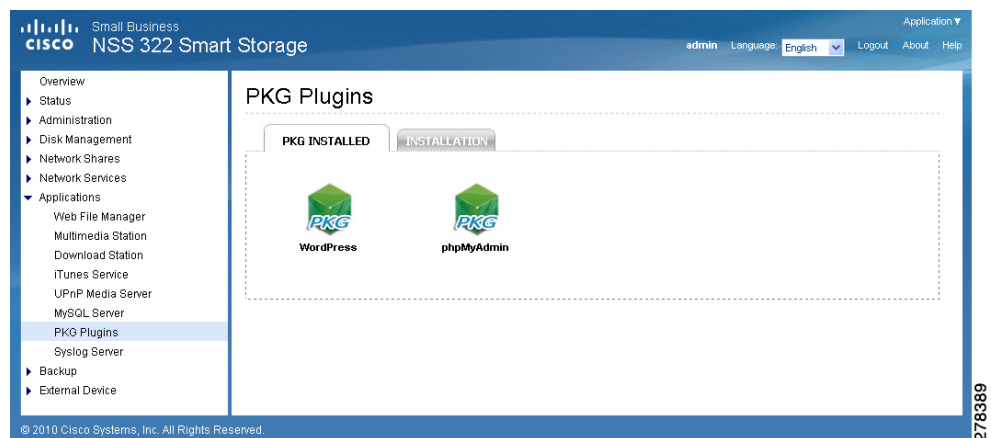
**NOTE** You can install the phpMyAdmin package to manage your MySQL server.

You can reset the root password by clicking **Reset Root Password**. The password of MySQL root will be reset to “admin” after executing this function.

You can re-initialize the MySQL database by clicking **Re-Initialize Database**. All the data on MySQL database will be cleared after executing this function.

## PKG Plugins

From the *Applications > PKG Plugins* window, you can install PKG packages to add more functions to the NAS. Before you install the packages, make sure the files are correct, read the instructions carefully, and back up all important data on the NAS. Download the software package that you want to install on NAS to your computer.



To install a previously installed PKG package:

- STEP 1** Choose **Applications > PKG Plugins** from the Navigation menu. The *PKG Plugins* window opens.
- STEP 2** Click the PKG application that you want to install. The *PKG Plugins* window opens.
- STEP 3** Click the web page link for the application. The web page for the application opens.
- STEP 4** Follow the instructions on the application web page to continue installing the package.

---

To install a new PKG package:

- STEP 1** Choose **Applications > PKG Plugins > Installation** from the Navigation menu. The *PKG Plugins INSTALLATION* window opens.
  - STEP 2** Click **Browse** to locate a PKG file.
  - STEP 3** Click **Install**. The PKG Plugin is installed to the NAS.
- 

To remove a PKG package:

- STEP 1** Choose **Applications > PKG Plugins > PKG Installed** from the Navigation menu. The *PKG Plugins PKG INSTALLED* window opens.
  - STEP 2** Click on the package that you want to remove.
  - STEP 3** Click **Remove**. The PKG Plugin is removed from the NAS.
- 

## Syslog Server

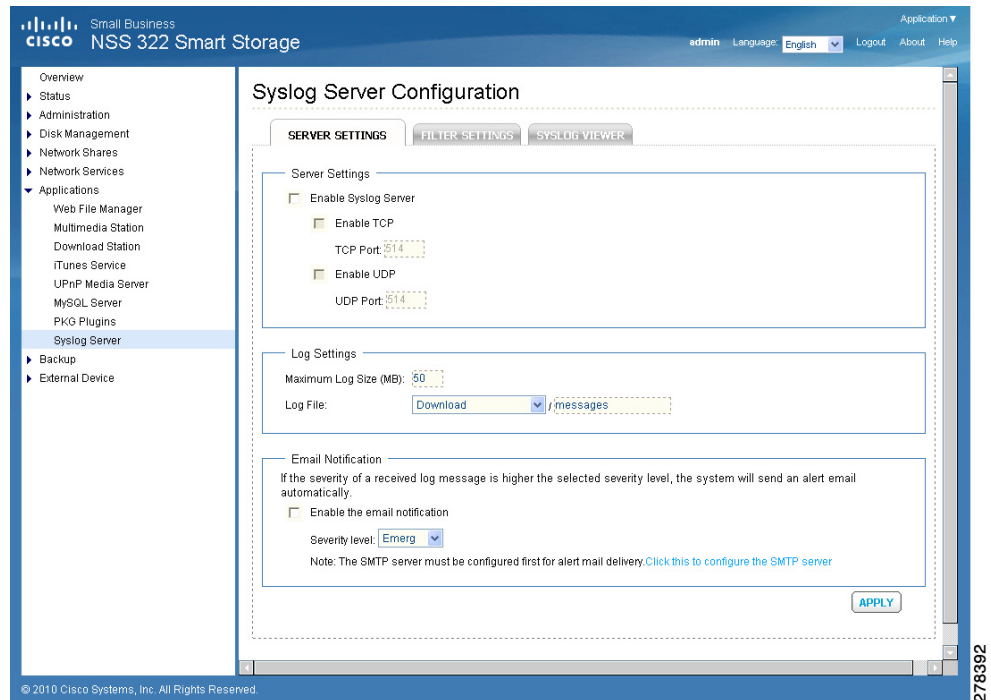
This section describes how to configure the syslog server settings for the NAS.

- **Server Settings**
- **Filter Settings**
- **Syslog Viewer**

### Server Settings

From the *Applications > Syslog Server > Server Settings* window, you can configure the server settings, log settings, and email notification.

After enabling the Syslog Server, the NAS can receive and store system log messages based on the syslog settings. Users can also define the maximum size, the stored path, and the name of the log file. Once the log file has reached its maximum size, it will be archived and renamed automatically. For example: *MyLogFile\_2010\_06\_06*. The date format follows the user-defined date format in *Administration > General Settings*.

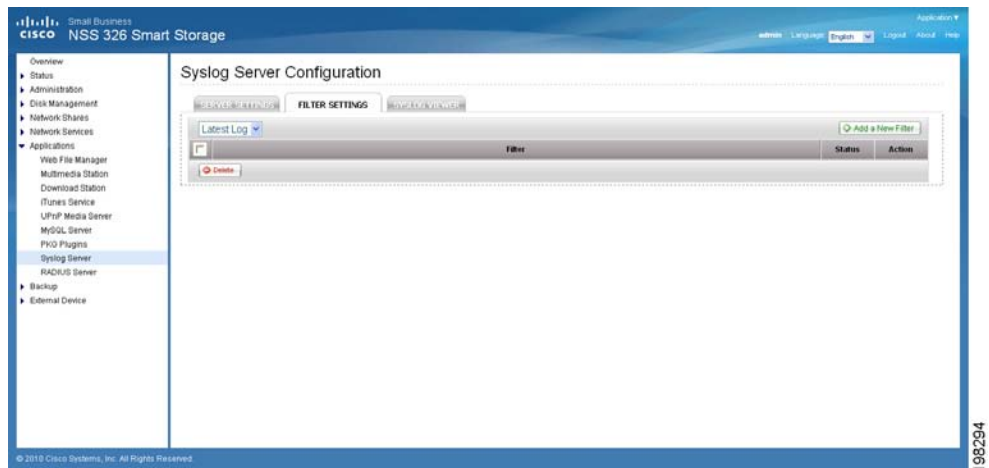


To enable the syslog server:

- STEP 1** Choose **Applications > Syslog Server** from the Navigation menu. The *Syslog Server Configuration* window opens.
- STEP 2** Click **Enable Syslog Server** to enable the Syslog Server.
- STEP 3** **Enable UDP** is automatically activated on port 514. You can change this to a different port by entering a different port number. You can also enable TCP by clicking on **Enable TCP** which uses TCP port 514 by default. You can change this to a different port by entering a different port number.
- STEP 4** Enter a maximum size (in MB) for the logs in **Maximum Log Size**.
- STEP 5** In **Log File**, specify a directory location for the logs to be saved.
- STEP 6** If you would like email notification of log messages, click **Enable the email notification** and specify the severity level of the logs you wish to receive.
- STEP 7** Click **Apply**. The syslog server settings are updated to the NAS.

## Filter Settings

The *Applications > Syslog Server > Filter Settings* window displays the filter settings and status. From this window, you can also add or delete a filter.

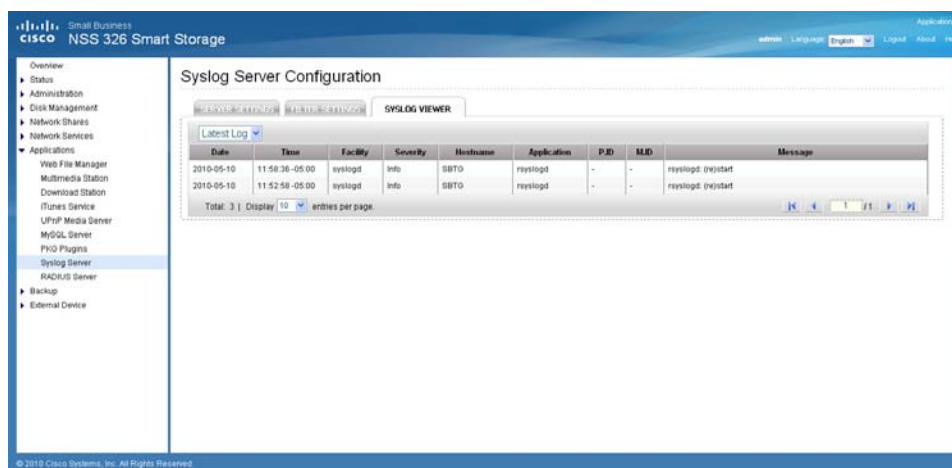


- **Filter**—Lists the filters that are currently defined.
- **Status**—Shows the status of each filter.
- **Action**—The type of action.
- **Add a New Filter**—Click to define different filters and the expressions of each filter in the Filter Settings. The filter wizard helps you create the filters easily. You can also select to use the manual editing mode to create and edit the filters.
- **Delete**—Click to delete a filter.

## Syslog Viewer

The *Applications > Syslog Server > Syslog Viewer* window displays the log file.





- **Date**—Date that the log occurred.
- **Time**—Time that the log occurred.
- **Facility**—Program that logged the message.
- **Severity**—Severity level of the log.
- **Hostname**—Name of the host that originated the log.
- **Application**—Name of the application that originated the log.
- **P.ID**—Process ID of the log.
- **M.ID**—Message ID of the log.
- **Message**—Message content of the log.

## RADIUS Server

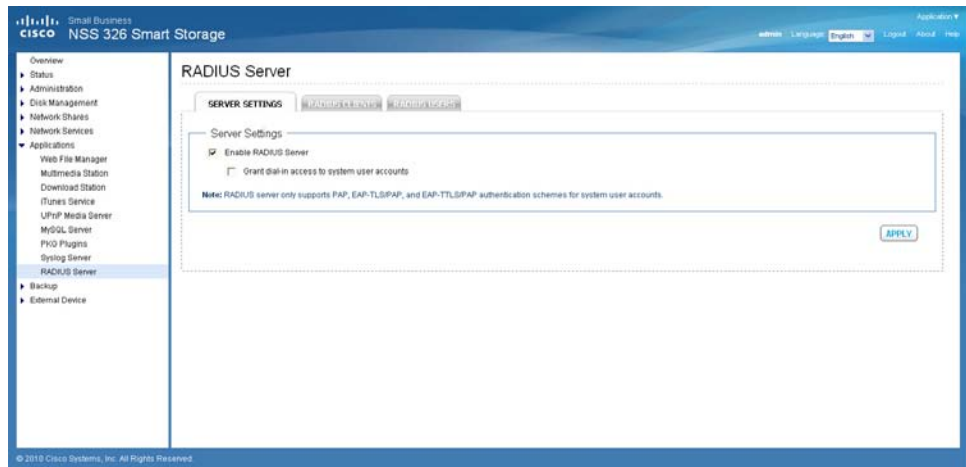
This section describes how to configure the RADIUS server settings, such as:

- **Server Settings**
- **RADIUS Clients**
- **RADIUS Users**

## Server Settings

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting management for computers to connect and use a network service. It is often used to manage access to the Internet or internal networks which may incorporate modems, access points, and web servers. The built-in RADIUS Server monitors UDP ports 1645, 1812 (for RADIUS authentication) and 1646, 1813 (for RADIUS accounting) for RADIUS requests.

From the *Applications > RADIUS Server > Server Settings* window, you can enable the RADIUS server.



To enable the RADIUS server:

**STEP 1** Choose **Applications > RADIUS Server > Server Settings** from the Navigation menu. The *Server Settings* window opens.

**STEP 2** Click **Enable RADIUS Server**.

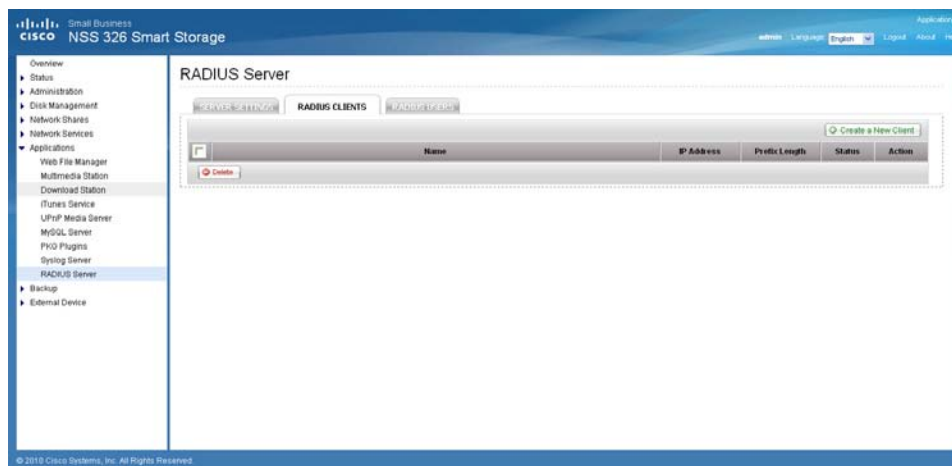
- **Grant dial-in access to system user accounts**—Click the check box to enable dial-in access to existing users.

**NOTE** RADIUS server supports PAP, EAP-TLS/PAP, and EAP-TTLS/PAP authentication for system user accounts.

**STEP 3** Click **Apply** to save the server settings.

## RADIUS Clients

From the *Applications > RADIUS Server > RADIUS Clients* window, you can view the existing RADIUS clients or configure the settings for a new RADIUS client.



The following parameters are displayed in the RADIUS Clients window:

- **Name**—Lists the names of the existing RADIUS clients.
- **IP Address**—IP address of the RADIUS client.
- **Prefix Length**—Prefix length of the RADIUS client.
- **Status**—RADIUS client status. You can enable or disable the RADIUS client from the Action field.
- **Action**—You can enable, disable, or edit the RADIUS client from the Action field.
- **Delete**—Click to delete the selected RADIUS client.
- **Create a New Client**—Click to create a new RADIUS client.

To create a new RADIUS client:

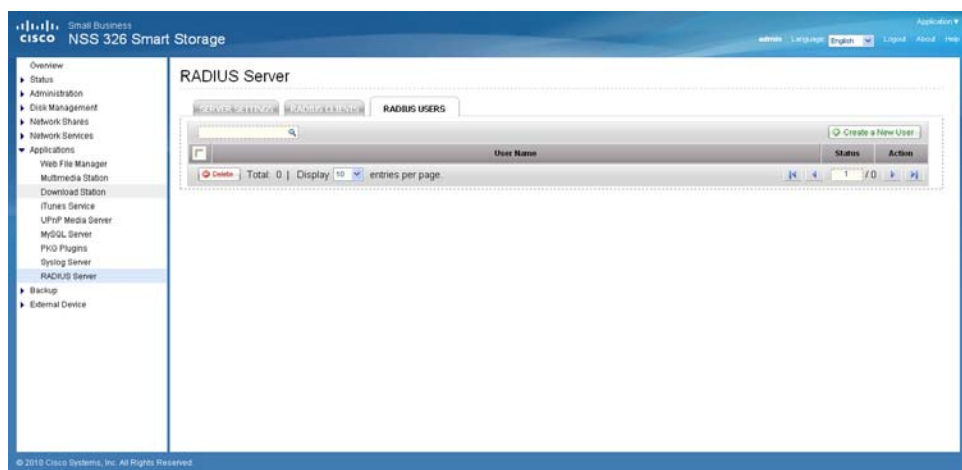
- STEP 1** Choose **Applications > RADIUS Server > RADIUS Clients** from the Navigation menu. The *RADIUS Clients* window opens.
- STEP 2** Click **Create a New Client** to create a new RADIUS client, such as a wireless access point. Enter the following parameters:
  - **Name**—Name of the new RADIUS client.

- **IP Address**—IP address for the new RADIUS client.
- **Prefix Length**—Prefix length for the new RADIUS client.
- **Secret Key**—Secret key for the new RADIUS client.

**STEP 3** Click **Apply** to save the new client settings.

## RADIUS Users

From the *Application > RADIUS Server > RADIUS Users* window, you can configure the RADIUS user settings.



To configure RADIUS user settings:

**STEP 1** Choose **Applications > RADIUS Server > RADIUS Users** from the Navigation menu. The *RADIUS Clients* window opens.

**STEP 2** Enter the following parameters:

- **Search**—Type a username in the search box to search for a specific user.
- **Create a New User**—Click to create a new RADIUS user.
  - **Name**—Enter the new username.
  - **Password**—Enter the password for the new RADIUS user.
  - **Verify Password**—Re-enter the password for the new RADIUS user.
- **User Name**—Lists the existing RADIUS users.

- 
- **Status**—Displays the user account status. You can enable or disable the user account in the Action field.
  - **Action**—You can enable, disable, or edit the RADIUS user from the Action field.
  - **Delete**—Click to delete the selected RADIUS user.
- 

## Backup

The NAS allows numerous ways to backup the data on its internal drives. This section includes the following topics regarding backing up your data:

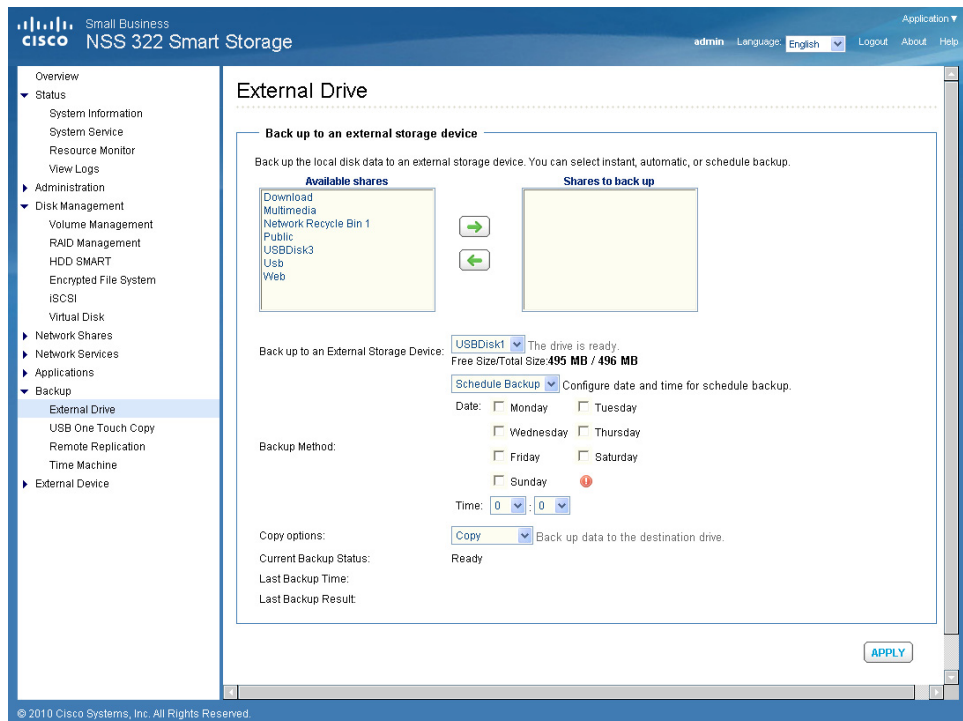
- **External Drive**
- **USB One Touch Copy**
- **Remote Replication**
- **Time Machine**

## External Drive

You can back up the local drive data to an external storage device. From the *Backup > External Drive* window, you can select to execute instant, automatic, or schedule backup methods, and configure the relevant settings.

- **Backup Now**—To back up data to the external storage device immediately.
- **Schedule Backup**—To back up data by schedule. You can select the week day and time to execute the backup.
- **Auto-backup**—To execute the backup automatically once the storage device is connected to the NAS.

You can select “Copy” or “Synchronize” for the copy options. When “Copy” is selected, files are copied from the NAS to the external device. By selecting “Synchronize,” the data on the internal drives of the NAS and the external storage device are synchronized. Any different files from the same folder name on the external device are deleted.



---

To backup to an external storage device:

- 
- STEP 1** Choose **Backup > External Drive** from the Navigation menu. The *External Drive* window opens.
- STEP 2** Select one or more network shares from the **Available shares** box.
- STEP 3** Click the Right Arrow to move the selected network shares to the **Shares to back up** box.
- STEP 4** Select an external storage device in **Back up to an External Storage Device**.
- STEP 5** Select a backup method in **Backup Method**. If you selected **Schedule Backup**, click days and specify a time to backup.
- STEP 6** Select a copy option in **Copy options**.



---

**CAUTION** If you select “Synchronize”, all data on the destination folders will be DELETED and then synchronized with the source folders.

---



---

**CAUTION** Do not remove an external drive from the NAS while backup is in progress.

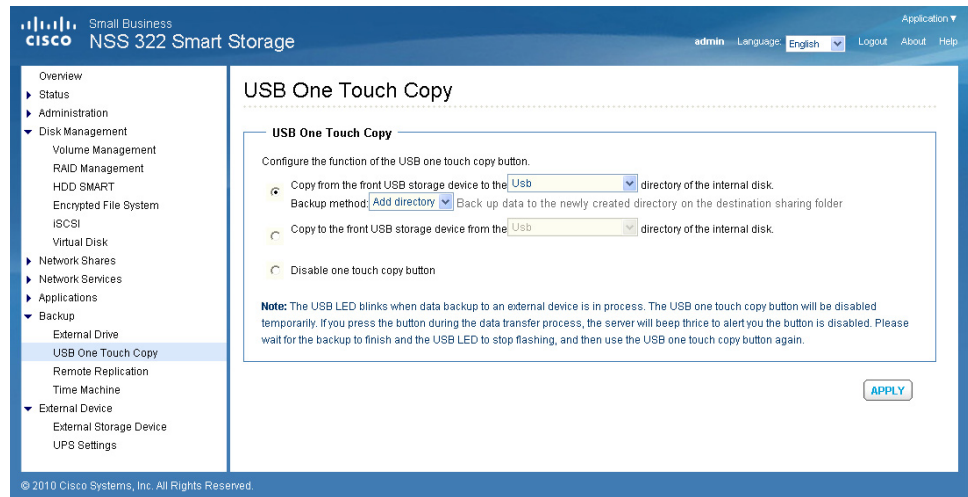
---

- STEP 7** Click **Apply**. Back up to an external device begins.
- 

## USB One Touch Copy

From the *Backup > USB One Touch Copy* window, you can configure the function of the USB one touch copy button. The following three functions are available:

- Copy from the front USB storage to a specified directory of the internal drive of the NAS.
- Copy to the front USB storage from a specified directory of the internal drive of the NAS.
- Disable the one touch copy button.



To configure the USB One Touch Copy feature:

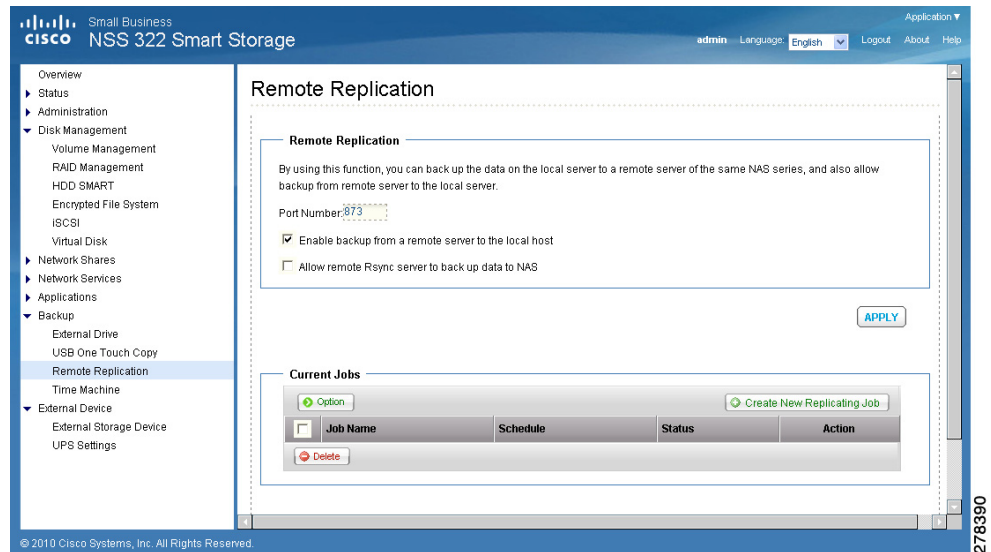
- STEP 1** Choose **Backup > USB One Touch Copy** from the Navigation menu. The *External Drive* window opens.
- STEP 2** Click one of the behaviors of the USB One Touch Copy button.
- STEP 3** Click **Apply**. Your USB One Touch Copy settings are updated to the NAS.

**NOTE** The USB LED blinks when the data transfer to an external device is in progress. After the data transfer is completed, the USB LED will stop flashing and the USB One Touch Copy button will be temporarily disabled. To perform another data transfer using USB One Touch Copy, unplug the USB cable from the port and re-insert prior to starting the data transfer.

## Remote Replication

From the *Backup > Remote Replication* window, you can configure the remote replication feature. The Remote Replication feature lets you replicate your local files to a remote folder on another server. You can perform immediate replication job or schedule a replication job to be executed at a specified time periodically. In order to reduce the network bandwidth usage as well as the time consumed, your files can be compressed before transferring over the network.





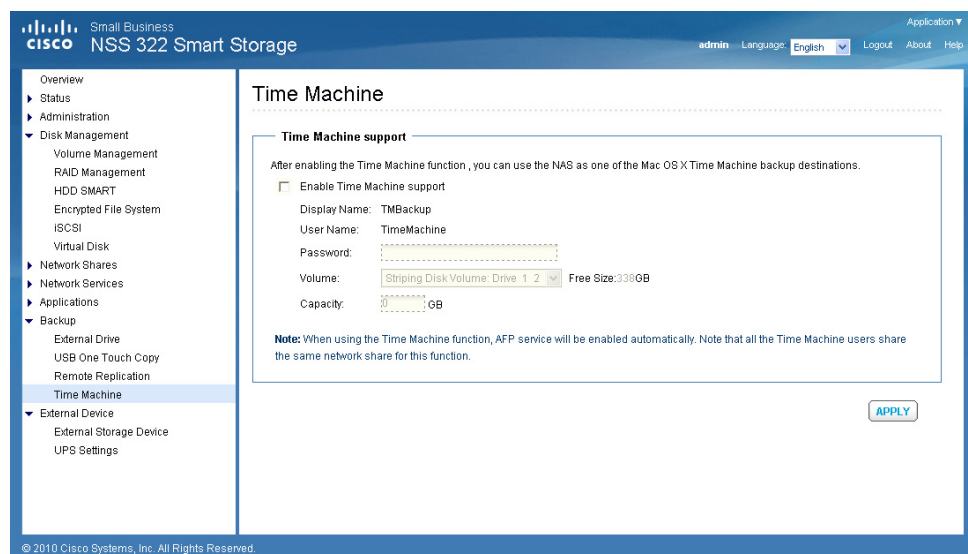
To create a new replication job:

- STEP 1** Choose **Backup > Remote Replication** from the Navigation menu. The *Remote Replication* window opens.
- STEP 2** Enter the parameters in Remote Replication:
  - **Port Number**—Specify a port number for remote replication. The default port number is 873.
  - **Enable backup from a remote server to the local host**—Check this option to allow the remote server to back up data to the local host via remote replication.
  - **Allow remote Rsync server to back up data to NAS**—Check this option to allow the remote server to back up data to the local host via remote replication.
- STEP 3** From Current Jobs, you can configure the following settings:
  - a. Click **Options** to change the advance settings for backup timeout, number of retries, and retry intervals.
  - b. Click **Create New Replicating Job** to launch the *Remote Replication Wizard*.

- STEP 4** Enter the parameters in the *Remote Replication Wizard*. Click **Next** after entering the parameters for each step in the *Remote Replication Wizard*.
- Select a server type and enter a Remote Replication Job Name. Click **Next**.
  - Enter the IP address or name of the remote server, the Port Number for remote backup, the User Name, and Password with write access to the remote server. Click **Test** to check the connection. Click **Next**.
  - Enter the destination path. The share folder name (network share or directory) is case-sensitive. Click **Next**.
  - Enter the source path. You can select to back up the whole network share and a folder in the share. Click **Next**.
  - Define a replication schedule. Click **Next**.
  - Set up other options for the remote replication job. Click **Finish**. A new replicating job appears in the Current Jobs list.
- STEP 5** Click **Apply**. Your Remote Replication settings are updated to the NAS.

## Time Machine

From the *Backup > Time Machine* window, you can configure your NAS as a Mac OS X Time Machine backup destination.



On your Apple computer, you must use Mac OS X 10.5.6 or later.

**NOTE** When using the Time Machine function, Apple Filing Protocol (AFP) service will be enabled automatically. Note that all the Time Machine users share the same network share for this function.

To enable Time Machine support:

- 
- STEP 1** Disable the Time Machine function in the System Preferences on your Apple computer.
  - STEP 2** Choose **Backup > Time Machine** from the Navigation menu. The *Time Machine* window opens.
  - STEP 3** Enter a Password for the Time Machine destination. The User Name is **TimeMachine**.
  - STEP 4** Select a Volume for the Time Machine destination.
  - STEP 5** Select a capacity to be assigned to the Time Machine destination.  
**NOTE** Time Machine will eventually utilize all the disk space allocated to it.
  - STEP 6** Click **Apply**. Your Time Machine settings are updated to the NAS.  
**NOTE** For more information on Time Machine, refer to Apple Support at <http://www.apple.com/support/leopard/timemachine/>.
  - STEP 7** From your Apple computer, enable Time Machine and select the NAS as a destination for Time Machine.
- 

## External Device

This section describes the external devices supported by NAS and includes the following topics:

- **External Storage Device**
- **UPS Settings**

## External Storage Device

The NAS is designed with external ports to support eSATA drives, USB drives, and thumb drives for extended storage. From the *External Device > External Storage Device* window, you can perform numerous functions on these external devices such as formatting the device, removing the disk partition, and removing the device from the NAS.

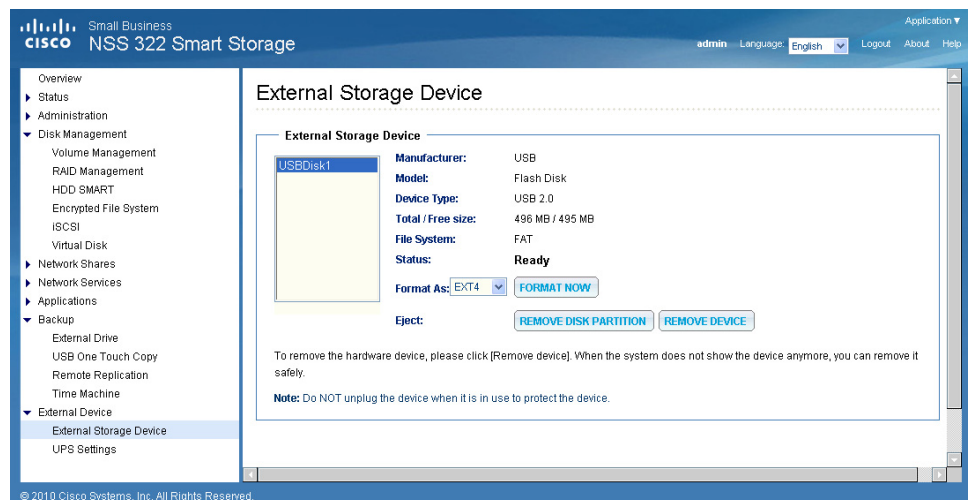
**NOTE** External devices are accessible to everyone who has network access to the NAS. Therefore, all users on the NAS can read and write data to these devices.



**CAUTION** Do not unplug an external device when it is in use to protect it and the data on it.



**CAUTION** Formatting or removing a disk partition from an external device will delete all data from the external device.



To format an external device:

- STEP 1** Connect an external device to the NAS.
- STEP 2** Choose **External Device > External Storage Device** from the Navigation menu. The *External Storage Device* window opens.
- STEP 3** Select the external storage device from the window.

---

**STEP 4** Choose a format type.

**STEP 5** Click **Format Now**. The external device is formatted in the selected format.

**NOTE** The NAS can format the external drive for a FAT32, NTFS, EXT3, or EXT4 file system. If you are formatting your external drive for EXT3 or EXT4, it cannot be recognized if you are using a Windows operating system. The NAS will recognize each partition existing on the external drive as one disk. If a single drive with multiple partitions is connecting to the NAS port, it will appear as multiple USB disks. For example, if you are using an external disk drive with four partitions, the NAS will recognize each partition as USBdisk1, USBdisk2, USBdisk3, and USBdisk4. To format a complete clean for external drives, you need to format each partition.

---

To remove a partition from an external device:

---

**STEP 1** Connect an external device to the NAS.

**STEP 2** Choose **External Device > External Storage Device** from the Navigation menu. The *External Storage Device* window opens.

**STEP 3** Select the external storage device from the window.

**STEP 4** Click **Remove Disk Partition**. The disk partition is removed from the selected external device.

---

To remove an external device from the NAS:

---

**STEP 1** Choose **External Device > External Storage Device** from the Navigation menu. The *External Storage Device* window opens.

**STEP 2** Select the external storage device from the window.

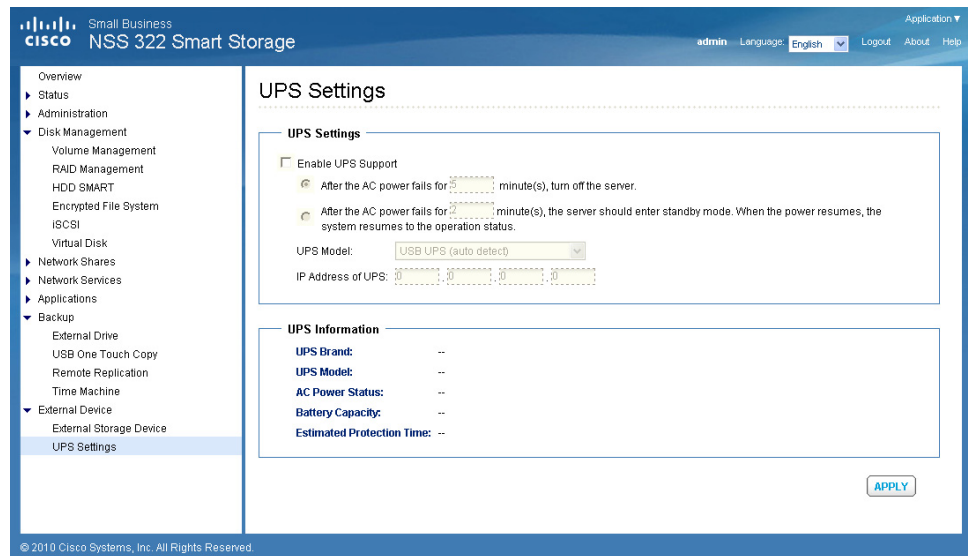
**STEP 3** Click **Remove Device**. The selected external device is removed from the NAS.

---

## UPS Settings

The NAS supports connection to an Uninterruptible Power Supply (UPS) to protect your system from abnormal system shutdown caused by a power outage. From the *External Device > UPS Settings* window, you can enable UPS support and configure the UPS settings, model and IP address.

The UPS Information area shows the UPS brand, model, AC power status, battery capacity, and estimated protection time for your UPS. If these fields are not filled, either the UPS is not communicating with the NAS or it does not provide this information to the NAS.



To enable UPS support:

- STEP 1** Ensure that the UPS is connected to your NAS according to the instructions from the UPS manufacturer.
- STEP 2** Choose **External Device > UPS Settings** from the Navigation menu. The *UPS Settings* window opens.
- STEP 3** Click **Enable UPS Support**.
- STEP 4** To turn off the NAS after a specified amount of time after power has failed, click **After the AC power fails for x minute(s), turn off the server**, and specify a time in minutes.
- STEP 5** To put the server in standby mode after the power has failed, click **After the AC power fails for x minute(s), the server should enter standby mode**, and specify a time in minutes. When the power resumes, the system resumes to the operation status.

---

**STEP 6** In **UPS Model**, choose a connection method:

- a. Choose **USB UPS (auto detect)** if your UPS is connected to the NAS via USB.
- b. Choose **APC UPS with SNMP Management** if your UPS is connected to the NAS via IP SNMP. Enter the IP address of the UPS in the address area.

**STEP 7** Click **Apply**. Your UPS settings are updated to the NAS.

---

# Configuring the NAS for Active Directory Authentication

The NAS supports Microsoft Active Directory Domain Services (AD DS). This chapter describes how to configure your NAS to join Microsoft Active Directory Services.

**NOTE** The NAS supports Windows Server 2000 and above.

## Before You Begin

Before you configure NAS for Active Directory authentication, ensure the following:

- You have access to an Active Directory domain.
- You have access to a properly configured DNS server.
- You have the following information:
  - An Active Directory domain administrator account for authentication.
  - The fully Qualified Domain Name (FQDN) of the Active Directory domain.
  - The NetBIOS domain name for the Active Directory domain.
  - The hostname or IP address (hostname is preferred) of the domain controller running the Active Directory domain.

The domain controller is a Windows Server 2000 or above computer running Active Directory Services.

  - (Optional) The name of the Organizational Unit (OU) the NAS belongs to.
- The IP address of your NAS.

**NOTE** It is important to note the time and date settings of your NAS device. A time deviation of more than 5 minutes between the NAS and your Domain Controller causes Kerberos Authentication to fail and you cannot join your domain.



**NOTE** We recommend that you configure your NAS to use your Domain Controller for time synchronization.

## Joining the NAS to Your Domain

This section describes how to join your NAS to your domain.

- [Configuring Date and Time, page 169](#)
- [Configuring DNS Settings, page 170](#)
- [Configuring Microsoft Networking, page 171](#)

### Configuring Date and Time

To configure NAS to use an NTP server:

**STEP 1** Start the web-based configuration utility of your NAS device.

To start the web-based configuration utility, open a web browser and enter the following in the URL field:

**http://<IP Address>:8080**

Where <IP Address> is the IP address of your NAS device.

**STEP 2** Click **Administration > General Settings > Date and Time**.

**STEP 3** To get the date and time from an NTP server, check **Synchronize with an internet time server automatically**.

**STEP 4** To specify an NTP server in the Server field, check **Input Manually**.

**STEP 5** In the Server field, enter the hostname or IP address of the NTP server.

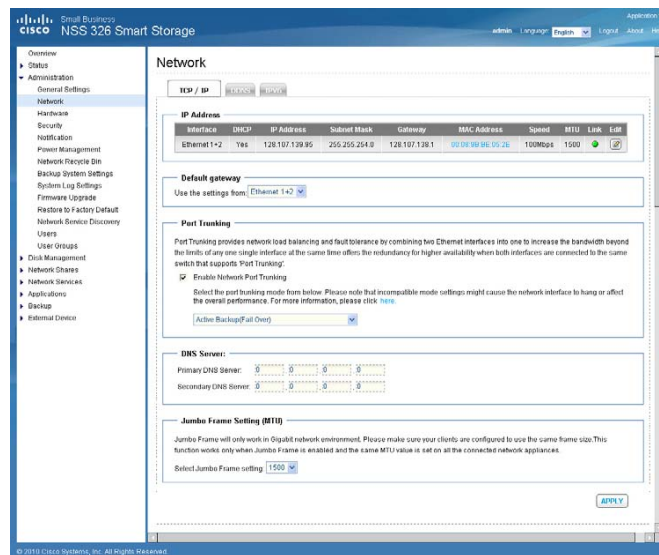
Make sure the time difference between the NAS and the domain controller is less than five minutes. If time difference is greater than five minutes, Kerberos Authentication fails and you cannot join the domain. To avoid this possibility, we recommend you use the domain controller as the NTP server.

**STEP 6** To save your settings, click **Apply**.

## Configuring DNS Settings

To configure DNS settings for your NAS, follow these steps.

**STEP 1** From the web-based configuration utility of your NAS, click **Administration > Network > TCP / IP**.



**STEP 2** In the **Primary DNS Server** field, enter the IP address of the primary DNS server.

We recommend that you use the domain controller as the primary DNS server.

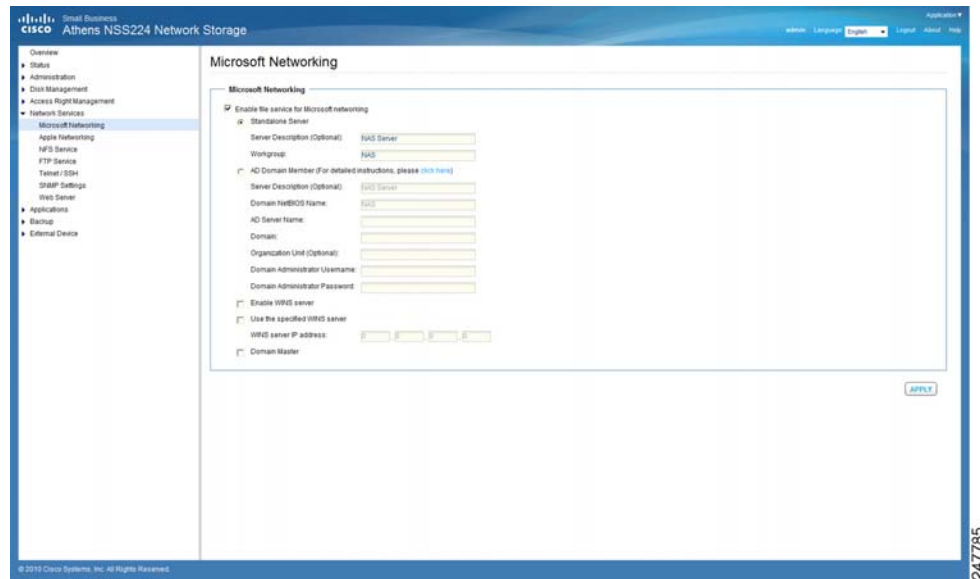
**STEP 3** In the **Secondary DNS Server** field, enter the IP address of the secondary DNS server.

**STEP 4** To save your settings, click **Apply**.

## Configuring Microsoft Networking

To configure your NAS to be an Active Directory domain member, follow these steps.

- STEP 1** From the web-based configuration utility of your NAS device, click **Network Services > Microsoft Networking**.



- STEP 2** Click the **AD Domain Member** radio button.

- STEP 3** (Optional) In the **Server Description** field, enter a description of your NAS.

**STEP 4** In the **Domain NetBIOS Name** field, enter the name of your NetBIOS domain.

You can find the name of your NetBIOS domain from a domain computer or a domain controller.

To find the name of the NetBIOS domain for your organization from a domain computer, follow these steps:

- a. Choose **Start > Run**.
- b. In the **Open** field, enter **CMD** and click **OK**.
- c. At the command prompt, enter the following:

```
nbtstat -A <IP_address_of_domain_controller>
```

The output of the command should be similar to the following:

```
C:\Users\a_user>nbtstat -A 192.168.52.250
Local Area Connection 2:
Local Area Connection:
Node IpAddress: [192.168.52.39] Scope Id: []
    NetBIOS Remote Machine Name Table
    Name                Type                Status
    -----
    MY_DC                <00>    UNIQUE            Registered
    NSS                  <00>    GROUP             Registered
    NSS                  <1C>    GROUP             Registered
    MY_DC                <20>    UNIQUE            Registered
    NSS                  <1B>    UNIQUE            Registered

    MAC Address = 00-0C-29-E2-ED-5E
```

In the NetBIOS Remote Machine Name Table, the first row contains the hostname of the domain controller (in this example, **MY\_DC**) and the second row contains the NetBIOS name (in this example, **NSS**), as indicated by the text in bold.

To find the name of the NetBIOS domain for your organization from a domain controller, follow these steps:

- a. Open “Active Directory Users and Computers” Snap-In.
- b. Right-click on you fully qualified domain name and choose **Properties**.

In the Properties window, the Domain Name (Pre-Windows 2000) field displays the NetBIOS name.

**STEP 5** In the AD Server Name field, enter the hostname of your domain controller.

To find the hostname of your domain controller:

- a. Log in to your domain controller.
- b. Click **Start**, right-click **My Computer**, and choose **Properties**.
- c. In the **Properties** window, click **Computer Name**.

In the *Properties* window, the *Full computer name* field displays the hostname.

For example, if the full computer name is mydc.example.com, the hostname of the domain controller is mydc.

You can also follow these steps to find the hostname of your domain controller:

- a. Click **Start > Run**, enter **CMD** in the **Run** window, and click **OK**.
- b. In the **command** window, type **Hostname** and press **Enter**.

The returned text is the hostname of your domain controller.

**STEP 6** In the **Domain** field, enter the fully qualified domain name (for example, mycompany.local).

**STEP 7** (Optional) In the **Organizational Unit (OU)** field, enter the path of the OU containment.

**STEP 8** In the **Domain Administrator Username** field, enter the username of the domain controller administrator.

**STEP 9** In the **Domain Administrator Password** field, enter the password of the domain controller administrator.

**STEP 10** To save your settings, click **Apply**.

A window appears displaying a message indicating whether your NAS has successfully joined the domain controller. In addition, the web-based utility adds an entry to the system log.

If your NAS failed to join the domain controller, check your settings and try again.

**STEP 11** Confirm that your NAS successfully joined the domain controller.

- a. Click **Administration > Users**.
- b. From the drop-down menu, choose **Domain Users**.
- c. Verify that you see the list of all the Active Directory domain users.
- d. Click **Administration > User Groups**.
- e. From the drop-down menu, choose **Domain Groups**.
- f. Verify that you see the list of all the Active Directory domain user groups.

---

If your NAS successfully joined the Active Directory domain, you can access the NSS shared folders from any computer in the domain.

To open a shared folder, open a Windows Explorer window and enter the following in the Address field:

`\\<NSS_Name>\<Shared_Folder_Name>`

To access NAS shared folders from a computer which is not part of the Active Directory domain, use a Windows Explorer window to open the shared folder and then provide your credentials as follows:

`<NetBios_Domain_Name>\<domain_username>`

For example, mydomain\nssuser1.

# NAS Maintenance

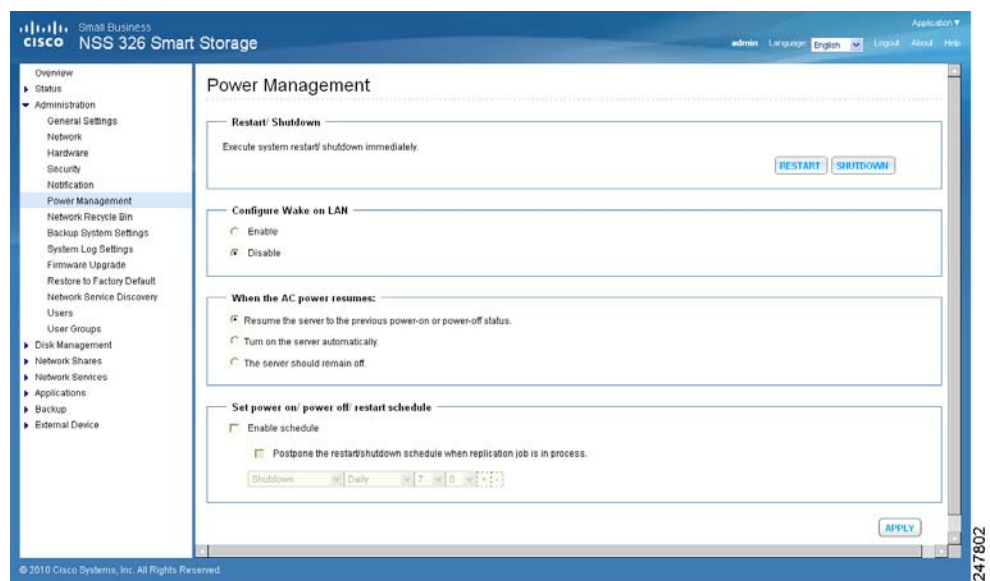
This chapter describes how to restart or shut down the NAS, reset the NAS system hardware, the steps to take to replace a hard disk, what to do in the event of a power outage, and how your system temperature is protected. The following sections are included:

- **Restart or Shut Down the NAS**
- **Hardware System Reset**
- **Disk Failure or Malfunction**
- **Power Outage or Abnormal Shutdown**
- **System Software Abnormal Operation**
- **System Temperature Protection**

## Restart or Shut Down the NAS

Follow the steps below to restart or shut down the NAS.

- STEP 1** Click **Administration > Power Management** from the Navigation menu. The *Power Management* window opens.
- STEP 2** To restart the NAS immediately, click **RESTART**. To shutdown the NAS immediately, click **SHUTDOWN**.



You can also press the power button for 5 seconds to turn off the NAS. The NAS beeps once and shuts down immediately.

## Hardware System Reset

There are two ways to reset the NAS system hardware: basic and advanced.

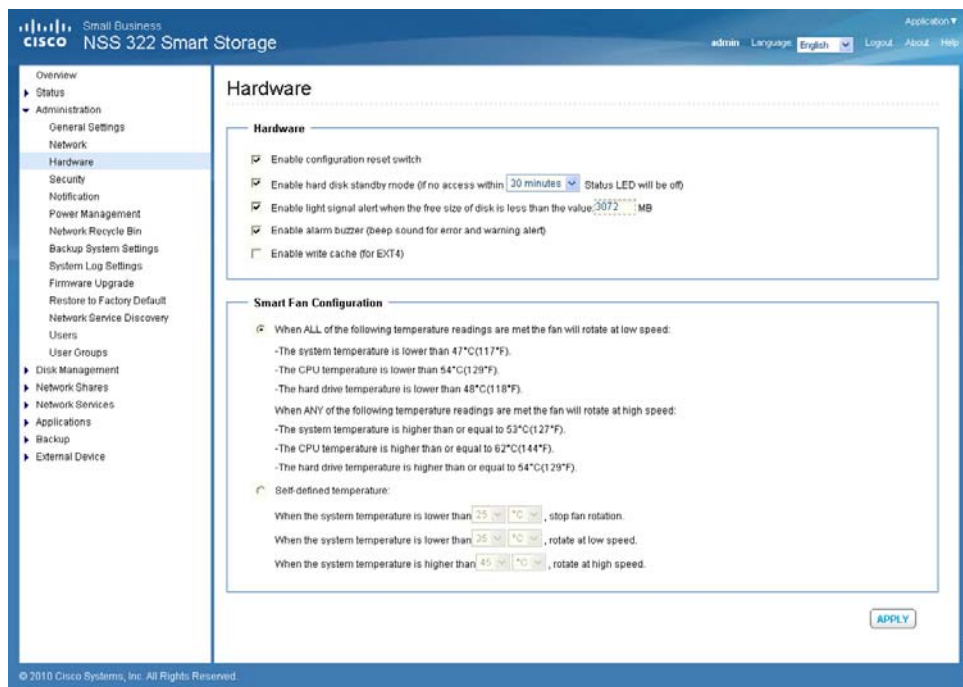
- NOTE** Hardware system reset as described in this chapter is different from the **Administration > Restore to Factory Default** command. See [Restore to Factory Default, page 91](#) more details regarding the **Restore to Factory Default** command.





**CAUTION** To prevent the unintentional loss of NAS system settings, be sure to read and understand the basic and advanced descriptions of the hardware system reset function before performing a system hardware reset.

**NOTE** To reset the system by the reset button, the option **Enable configuration reset switch** in **Administration > Hardware** must be activated.



System	Basic System Reset (1 beep)	Advanced System Reset (2 beeps)
All NAS models	Press the reset button for 3 seconds.	Press the reset button for 10 seconds.

### Basic System Reset (3 seconds)

The following settings are reset to their default value during a basic system reset:

Feature/Function	Setting after 3 Second Reset
System administration password	admin
Administration > Network > TCP/ IP	Obtain IP address settings automatically via DHCP
Administration > Network > TCP/ IP	Disable Jumbo Frame
General Settings > System Administration > System Port	8080 (system service port)
Administration > Security > Security Level	Low (Allow all connections)
LCD panel password (only applicable to models with LCD panel)	No Password

To perform a basic system reset:

- STEP 1** Press and hold the reset button for 3 seconds, a beep will sound.
- STEP 2** Wait for the NAS to reboot.

---

## Advanced System Reset (10 seconds)



**CAUTION** Users, User Groups, and Network Share folders will be cleared during an advanced system reset.

---

During an advanced system reset, the NAS will reset all system settings to their default values just as it does by web-based system reset in **Administration > Restore to Factory Default** except that all data remains on the disk. However, to retrieve the data after an advanced system reset, you will need to create the same network share folders on the NAS to access the data. Use the “specify path” when creating the network share folders, in order to access the data.

To perform an advanced system reset:

- 
- STEP 1** Press and hold the reset button for 10 seconds, you will hear two beeps at the third and the tenth seconds.
  - STEP 2** Wait for the NAS to reboot.
  - STEP 3** Adjust NAS system settings as necessary.
- 

## Disk Failure or Malfunction

If one of your disks fail, the status indicator on the NAS will blink red; you can verify that a disk failure has occurred by viewing the system logs.

**NOTE** When configuring your NAS using RAID, be sure to select the proper RAID level for adequate data protection. Refer to **Disk Management, page 103** for more details on RAID.

Perform the following steps to replace a failed disk.

- 
- STEP 1** Click **Administration > System Log Settings** from the Navigation menu. The *System Logs* window opens.
  - STEP 2** If a disk failure has occurred, the log will specify which disk has failed.
  - STEP 3** Locate the failed disk on the NAS and remove it. The failed disk can be identified by a red indicator over the failed disk.



---

**CAUTION** Be especially careful to pull out the disk from the correct drive slot. An improperly removed disk in a RAID array can cause catastrophic failure to the remaining degraded RAID array, including total data loss.

---

**STEP 4** Remove the failed drive from the drive sled by removing the screws that attach it.

**STEP 5** Connect a new disk into the drive sled using the appropriate screws for the disk.

**STEP 6** Insert the drive assembly into the NAS.

**STEP 7** If you are using a mirroring RAID disk configuration, the NAS will configure the drive and place it into the RAID array. This operation may take several minutes or hours depending on the size of the disk and RAID array.

**STEP 8** If you are using a non-RAID disk configuration, you may need to reformat and reconfigure the new disk. You can change disk configuration from **Disk Management > Volume management**.

**NOTE** You can view the System Logs to verify that the NAS has returned to normal operation.

---

If you experience any other malfunction or failure with the NAS, do the following:

---

**STEP 1** Record the malfunction status or error messages shown in system logs.

**STEP 2** Stop using the failed NAS and turn it off.

**STEP 3** Contact customer service for technical support.

**NOTE** The NAS must be repaired by professional technicians, do not try to repair the server yourself. Back up any important files or folders to avoid potential data loss due to disk failure.

---

## Power Outage or Abnormal Shutdown

In case of a power outage or improper shutdown of the NAS, it will resume to the state before it is shut down.

**NOTE** Other power outage options are available from the **External Device > UPS Settings** window.

If your NAS does not function properly after restart, do the following:

- 
- STEP 1** If the system configuration is lost, configure the system again.
- STEP 2** In the event of abnormal operation of the NAS, contact customer service for technical support.

## System Software Abnormal Operation

If the system software does not operate properly, the NAS automatically restarts to resume normal operation. If you find that the system restarts continuously, it may fail to resume normal operation. In this case, contact technical support.

## System Temperature Protection

The system shuts down automatically for hardware protection if any of the following criteria is met:

- The system temperature exceeds 70°C (158°F)
- The CPU temperature exceeds 85°C (185°F)
- The hard drive temperature exceeds 65°C (149°F)

---

## Product Battery Replacement

This product contains a permanently affixed battery, so for product safety and data integrity reasons such battery should only be removed or replaced professionally by a repair technician or waste management professional. Please contact Cisco or an authorized service agent if the product fails to perform due to malfunction of the permanently affixed battery.



---

**CAUTION** There is the danger of explosion if the battery is replaced incorrectly.

---

# Troubleshooting Abnormal RAID Operation

This chapter describes steps to troubleshoot abnormal RAID operation of your Cisco NAS.

**NOTE** If the NAS administration interface cannot be accessed due to an improperly configured port trunking mode, improperly configured Jumbo Frame setting, or an incompatible switch, reset the network settings by pressing the reset button on the back panel of the NAS for 3 seconds.

## Before You Begin the Troubleshooting Process



---

**CAUTION** Before troubleshooting the RAID configuration of your NAS, back up the important data on the NAS to avoid any potential data loss.

---



---

**CAUTION** Insert or remove only one drive from the NAS at a time.

---



---

**CAUTION** After inserting or removing a hard drive, wait until you hear two beeps from the NAS before inserting or removing the next hard drive.

---

## Troubleshooting Abnormal RAID Operation of Your NAS

To troubleshoot abnormal RAID operation of your NAS, follow these steps:

**STEP 1** Check whether the RAID rebuilding has failed.

When the RAID rebuilding fails:

- The Status LED of the NAS blinks red.
- In the *Disk Management > Volume Management* window of the web-based configuration utility of the NAS, the status of the disk volume configuration is “In degraded mode.”

**STEP 2** Determine which hard drives caused the RAID rebuilding failure.

In the web-based configuration utility of your NAS, open the **System Administration > System Logs** window and search for error messages similar to the following sample message:

```
Error occurred while accessing Drive 2.  
Drive 2 has been removed.
```

This message indicates that the hard drive in slot 2 has failed.

**STEP 3** Replace the failed drives with new drives.

After inserting the new hard drives, the RAID rebuilding should start.

**STEP 4** If the rebuilding succeeds, the NAS will return to normal operation. Skip the remaining steps.

If the rebuilding fails again due to a read/write error, continue the troubleshooting.

**STEP 5** Determine which hard drives caused the error.

- If the error is caused by one of the new drives, go back to **STEP 3**.
- If the error is caused by an old drive, go to **STEP 4**.

**STEP 6** If the RAID configuration is RAID 1, do one of the following:

Reinstall and set up the NAS:

- a. If you haven't done so already, back up the drive data to another storage device.
- b. Reinstall and set up the NAS.



---

**Execute RAID 1 migration:**

- a. Format one of the new drives as a single drive.
- b. Back up the data on the NAS to the new drive using Web File Manager.
- c. Unplug the drive with errors and insert a new drive in its place.
- d. Execute a RAID 1 migration.

**STEP 7** If the RAID configuration is RAID 5 or 6, back up the data and run system installation and configuration again.

---

## Using the LCD Display

This chapter describes the LCD display on the front panel of the NSS 324 and NSS 326 Smart Storage devices. Using the LCD display, you can configure the disks and view the system information. The following sections are included:

- [System Configuration Using the LCD Display](#)
- [Viewing System Information Using the LCD Display](#)
- [System Messages](#)

### System Configuration Using the LCD Display

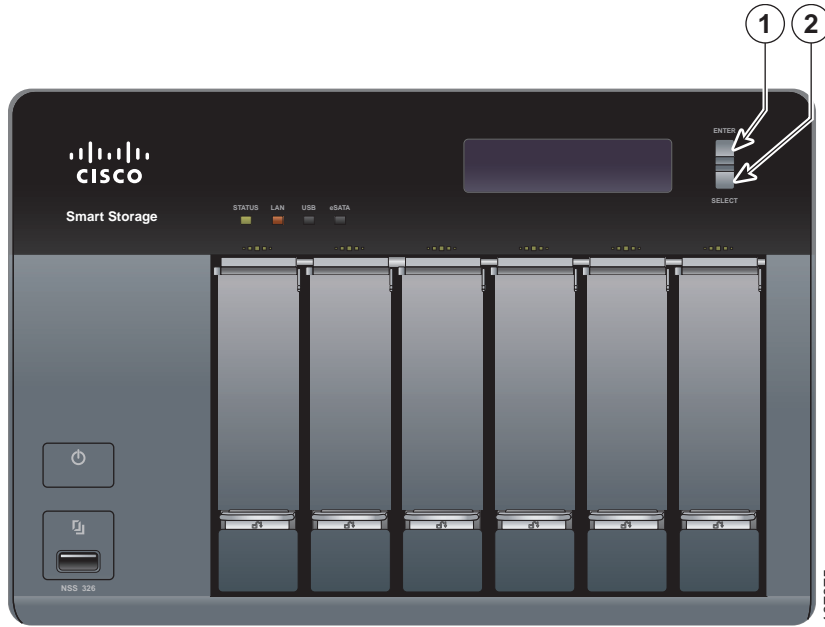
When the NAS is configured and the device is powering up, you can view the NAS name and IP address. For example:

N	A	S	B	E	4	5	E	2								
1	2	7	.	2	1	0	.	1	3	9	.	1	5	2		

For the initial or first-time installation, the LCD display shows the number of hard drives detected and the IP address.

Number of Disks Detected	Default Disk Configuration	Available Disk Configuration Options
1	Single	Single
2	RAID 1	Single, JBOD, RAID 0, RAID 1
3	RAID 5	Single, JBOD, RAID 0, RAID 5
4 or more	RAID 5	Single, JBOD, RAID 0, RAID 5, RAID 6

Use the Select and Enter button when configuring the disks using the LCD display. The following shows the location of the Select and Enter button on the NSS 326. The location is the same on the front panel of the NSS 324.



Number	Item	Description
1	Enter	Displays options for configuration or status such as bootup progress, disk configuration, and volume. After configuration, you can view the hostname and IP address.
2	Select	Press Select to confirm a configuration or menu option.

To configure the disks using the LCD display:

- STEP 1** At the prompt **Config Disks?** in the LCD display, press **Select** to choose the disk configuration.

For example, when you power on the NAS with five disks installed, the LCD display shows:



The following options are available:

- **Single Disk**—Uses the disk drives as single disk volumes. When a drive failure occurs, all data is lost.
- **JBOD (Linear)**—JBOD lets you combine multiple disks of mixed capacities into a single logical storage device. The capacity of the JBOD array is the sum of the total capacities of the individual component disks (that is, it does not have the limitation of RAID 1 where you lose some capacity when using mixed sized disks). JBOD offers no performance increase compared to the component disks. It has lower reliability than the component disks, as the failure of a single disk results in the failure of the whole array.
- **RAID 0**—Distributes data across several disks in a way which that improves speed and full capacity. All data on all disks will be lost if any single disk fails.
- **RAID 1**—Uses two disks (mirrored disks) which each store the same data, so that data is not lost as long as one disk survives. Total capacity of the array equals the capacity of the smaller disk.
- **RAID 5**—Combines three or more disks in a way that protects data against loss of any single disk.
- **RAID 6**—Combines four or more disks in a way that protects data against loss of any two disks.

**STEP 2** After choosing the disk configuration, press **Enter**. The LCD display shows the configuration that you selected. For example:

C	h	o	o	s	e		R	A	I	D	5	?			
	Y	e	s				N	o							

Yes is the default disk configuration.

When you select RAID 1, RAID 5, or RAID 6 configuration, the system initializes the disks, creates the RAID device, formats the RAID device, and mounts it as a volume on the NAS. The progress is shown on the LCD display. When the progress reaches 100 percent, you can access the RAID volume, create share folders, and upload files to the folders on the NAS. In the interim, to ensure that the stripes and blocks in all the RAID component devices are ready, the NAS will execute RAID synchronization. The synchronization progress can be monitored from the *Disk Management > Volume Management* window. The synchronization rate is approximately 30-60 MB/s. This number can vary by disk models, system resource usage, and other factors.

**NOTE** If any disk of the RAID array fails during the synchronization, the RAID device will enter degraded mode. The volume data is still accessible. If you replace a failed disk with a new disk to the RAID device, it will start to rebuild. You can check the status from the *Disk Management > Volume Management* window.

**STEP 3** Press **Enter** to continue. The LCD display shows:

E	n	c	r	y	p	t		V	o	l	u	m	e	?
	Y	e	s			N	o							

No is the default. If you choose yes, the disk volume is encrypted with a password and provides an extra layer of security against the theft of data. The default encryption password is a password of the “admin” account.

**NOTE** To change the encryption password, choose *Disk Management > Encrypted File System* from the Navigation menu. See [Encrypted File System, page 115](#).

**STEP 4** Press **Enter** to continue. The system configuration progress is displayed. When the configuration is complete, you will receive an IP address and default NAS device name that is shown in the LCD display.

**STEP 5** Start a web browser. You can access the management GUI from a web browser using either the NAS IP address or NAS device name.

- In the Address bar, enter the IP address of the device that is shown in the LCD display:

**http://<NAS IP address>:8080**

Or

- In the Address bar, enter the NAS device name that is shown in the LCD display:

**http://<NAS device name>:8080**

**STEP 6** When the login window opens, enter the administrator account username and password.

The default username is **admin**. The default password is **admin**. Username and password are case sensitive.

**STEP 7** Click **Login**.

**STEP 8** Follow the prompts to change the admin password.

**STEP 9** Click **Submit**.

**STEP 10** When the login window opens, enter the administrator account username **admin** and the new administrator password that you created in **STEP 8**.

## Viewing System Information Using the LCD Display

When the LCD display shows the NAS name and IP address, press the **Enter** button for two seconds to enter the Main Menu. Press the **Select** button to move forward through the options.

From the Main Menu you can view system information, shut down or reboot the NAS, or modify the password for the LCD display.

The Main Menu displays the following items:

- **TCP/ IP**
- **Physical Disk**
- **Volume**
- **System**
- **Shut Down**
- **Reboot**
- **Password**
- **Back**

### TCP/ IP

From the TCP/IP menu, press the **Select** button to move forward through the options. In TCP/ IP, you can view the following options:

- **LAN IP Address**—IP address of this interface.
- **LAN Subnet Mask**—Subnet mask of this interface.
- **LAN Gateway**—IP address of the network gateway device.
- **LAN PRI. DNS**—IP address of the Domain Name System (DNS) server. This address is typically provided by your Internet Service Provider (ISP).

- **LAN SEC. DNS**—Second DNS server.

In Network Settings, press the **Enter** button to enter the Network Settings. Press the **Select** button to move forward through the options.

- **Network Settings:**
  - **Network Settings – DHCP**—Specifies whether this interface uses Dynamic Host Configuration Protocol (DHCP).
  - **Network Settings – Static IP**—If a static IP address is configured, shows static IP address, subnet mask, gateway, and DNS of LAN 1 and LAN 2.
  - **Network Settings – BACK**—Move back in the menu options.
- **Back to Main Menu**—Return to the Main Menu.

## Physical Disk

In Physical disk, you can view the following options:

- Disk Info
- Back to Main Menu

To view the physical disk:

- 
- STEP 1** From the Main Menu, press the **Select** button until the Physical disk option is displayed.
- STEP 2** Press the **Enter** button. The Disk Info shows the temperature and the capacity of the first disk.

D	i	s	k	:	1		T	e	m	p	:	5	0	°	C
S	i	z	e	:		2	3	2		G	B				

- STEP 3** Press the **Select** button to view each disk.
- STEP 4** When Back to Main Menu is displayed, press the **Enter** button to return to the Main Menu.
-

## Volume

The Volume option shows the disk configuration of the NAS.

To view the volume:

- STEP 1** From the Main Menu, press the **Select** button until the Volume option is displayed.
- STEP 2** Press the **Enter** button. The first line shows the RAID configuration and storage capacity. The second line shows the member drive number of the configuration.

```

R A I D 5      7 5 0 G B
D r i v e     1 2 3 4
  
```

- STEP 3** If there is more than one volume, press the **Select** button to view the information.
- STEP 4** When Back to Main Menu is displayed, press the **Enter** button to return to the Main Menu.

The following table shows the description of the LCD messages for RAID 5 configuration.

LCD Display	Drive Configuration
RAID 5+S	RAID 5 + spare
RAID 5 (D)	RAID 5 degraded mode
RAID 5 (B)	RAID 5 rebuilding
RAID 5 (S)	RAID 5 re-synchronizing
RAID 5 (U)	RAID 5 is unmounted
RAID 5 (X)	RAID 5 non-activated



## System

The System option shows the system temperature and the rotation speed of the system fan.

To view the system option:

**STEP 1** From the Main Menu, press the **Select** button until the System option is displayed.

**STEP 2** Press the **Enter** button. The CPU and system temperatures are displayed.

C	P	U		T	e	m	p	:		5	0	°	C		
S	y	s		T	e	m	p	:		5	5	°	C		

**STEP 3** Press the **Select** button to view the rotation speed of the system fan. The NSS 326 displays FAN1 and FAN2.

S	y	s		F	A	N	1	:		8	6	5	R	P	M		
S	y	s		F	A	N	2	:		8	6	5	R	P	M		

**STEP 4** Press the **Select** button. When Back to Main Menu is displayed, press the **Enter** button to return to the Main Menu.

## Shut Down

Use the Shut down option to power off the NAS.

To power off the NAS:

**STEP 1** From the Main Menu, press the **Select** button until the Shut down option is displayed.

**STEP 2** Press the **Select** button to select **Yes**.

**STEP 3** Press the **Enter** button to confirm.

---

## Reboot

Use the Reboot option to restart the NAS.

To reboot the NAS:

- 
- STEP 1** From the Main Menu, press the **Select** button until the Reboot option is displayed.
  - STEP 2** Press the **Select** button to select **Yes**.
  - STEP 3** Press the **Enter** button to confirm.
- 

## Password

The default password of the LCD display is blank. Enter the Password option to change the password of the LCD display.

**NOTE** The LCD password is not the same as the “admin” account password.

To change the password of the LCD display:

- 
- STEP 1** From the Main Menu, press the **Select** button until the Password option is displayed. The following is shown:

C	h	a	n	g	e		P	a	s	s	w	o	r	d	
					Y	e	s			N	o				

- STEP 2** Select **Yes** to continue.
- STEP 3** Enter a password with a maximum of eight numeric characters (0-9).
- STEP 4** When the cursor moves to OK, press the **Enter** button. To confirm the changes, verify the password.

N	e	w		P	a	s	s	w	o	r	d	:			
														O	K

---

## Back

Select the Back option to return to the main menu.

## System Messages

When the NAS encounters system errors, an error message is shown on the LCD display. Press the **Enter** button to view the message. Press the **Enter** button again to view the next message.

```
S y s t e m   E r r o r !
P l s .   C h e c k   L o g s
```

System Message	Description
Sys. Fan Failed	System fan failed.
Sys. Overheat	System is overheated.
HDD Overheat	Disk overheated.
CPU Overheat	CPU is overheated.
Network Lost	Both LAN 1 and LAN 2 are disconnected in Failover or Load-Balancing mode.
LAN1 Lost	LAN 1 is disconnected.
LAN2 Lost	LAN 2 is disconnected.
HDD Failure	Disk has failed.
HDD Ejected	Disk is ejected.
Vol1 Full	Volume is full.
Vol1 Degraded	Volume is in degraded mode.
Vol1 Unmounted	Volume is unmounted.
Vol1 Nonactivate	Volume is not activated.



## Specifications

This appendix lists the specifications for the Cisco Small Business NSS 322, NSS 324, and NSS 326 Smart Storage devices.

Feature	NSS 322	NSS 324	NSS 326
<b>Physical Specifications</b>			
Form	Desktop	Desktop	Desktop
Dimensions (H x W x D)	5.91 x 4.02 x 8.5 in. 150 x 102 x 216 mm	6.97 x 7.09 x 9.25 in. 177 x 180 x 235 mm	6.89 x 10.12 x 9.25 in. 175 x 257 x 235 mm
Net Weight	3.84 lbs 1.74 kg	8.04 lbs 3.65 kg	11.46 lbs 5.2 kg
Gross Weight	11.02 lbs 5 kg	18.43 lbs 8.36 kg	22.35 lbs 10.14 kg
<b>Hardware Specifications</b>			
Network	2 Gigabit LAN ports	2 Gigabit LAN ports	2 Gigabit LAN ports
eSATA	2 (back)	2 (back)	2 (back)
Memory	1GB DDRII RAM	1GB DDRII RAM	1GB DDRII RAM
Flash	512 MB	512 MB	512 MB
USB 2.0 x 5	1 (front) 4 (back)	1 (front) 4 (back)	1 (front) 4 (back)
<b>Power</b>			
Type	External power adaptor	Internal power supply	Internal power supply
Input	100-240V~, 47~63Hz, 7A	100-240V~, 47~63Hz, 3.5A	100-240V~, 47~63Hz, 3.5A

Feature	NSS 322	NSS 324	NSS 326
Certificate	CE, FCC, VCCI, BSMI	CE, FCC, VCCI, BSMI	CE, FCC, VCCI, BSMI
<b>Browser Support</b>			
	Internet Explorer 7 & 8, Safari 3 & 4, Firefox 3	Internet Explorer 7 & 8, Safari 3 & 4, Firefox 3	Internet Explorer 7 & 8, Safari 3 & 4, Firefox 3
<b>Environmental</b>			
Operating Temperature	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)
Storage Temperature	-4 to 158°F (-20 to 70°C)	-4 to 158°F (-20 to 70°C)	-4 to 158°F (-20 to 70°C)
Operating Humidity	0 to 80 percent relative humidity	0 to 80 percent relative humidity	0 to 80 percent relative humidity
Storage Humidity	0 to 95 percent relative humidity	0 to 95 percent relative humidity	0 to 95 percent relative humidity
Operating Altitude (from mean sea level)	-52 ft to 10,000 ft -16 m to 3,048 m	-52 ft to 10,000 ft -16 m to 3,048 m	-52 ft to 10,000 ft -16 m to 3,048 m
Storage Altitude (from mean sea level)	-52 ft to 34,777 ft -16 m to 10,600 m	-52 ft to 34,777 ft -16 m to 10,600 m	-52 ft to 34,777 ft -16 m to 10,600 m

## Where to Go From Here

Cisco provides a wide range of resources to help you obtain the full benefits of the Cisco Small Business Smart Storage.

Support	
Cisco Small Business Support Community	<a href="http://www.cisco.com/go/smallbizsupport">www.cisco.com/go/smallbizsupport</a>
Online Technical Support and Documentation (Login Required)	<a href="http://www.cisco.com/support">www.cisco.com/support</a>
Phone Support Contacts	<a href="http://www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html">www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html</a>
Software Downloads (Login Required)	Go to <a href="http://tools.cisco.com/support/downloads">tools.cisco.com/support/downloads</a> , and enter the model number in the Software Search box.
Product Documentation	
NSS 322, NSS 324, and NSS 326 Smart Storage (Datasheets, Firmware, Quick Start Guides, FAQs, Application Notes, Release Notes, Approved Vendor List, Regulatory Compliance and Safety Information)	<a href="http://www.cisco.com/go/smallbizsmartstorage">www.cisco.com/go/smallbizsmartstorage</a>
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	<a href="http://www.cisco.com/web/partners/sell/smb">www.cisco.com/web/partners/sell/smb</a>
Cisco Small Business Home	<a href="http://www.cisco.com/smb">www.cisco.com/smb</a>
Marketplace	<a href="http://www.cisco.com/go/marketplace">www.cisco.com/go/marketplace</a>

