

Chapter 5

Managing Your NAS server

If you are the Administrator of the NAS server, you can use your Web browser to connect to the server and perform administrative tasks such as checking who is using the server, checking the disk status, and changing configuration options. This chapter gives you a brief introduction to these administrative tools. It also covers special concerns for backing up the data stored on your NAS server and using the NAS server in different network environments.

Language Support For File And Folder Names

Documents saved on a NAS server may be written in any language that the operating system supports. File and folder name support is provided only for languages that are compatible with Code Pages 437 (US English, Indonesian¹, Basque¹, Catalan¹), 850 (Western Europe including Afrikaans, Basque, Catalan, Dutch, English, French, German, Italian, Indonesian¹, Icelandic², and Spanish) and 865 [Northern Europe including Danish, Finnish, Norwegian (Bokmål), Norwegian (Nyorsk), and Swedish].



Warning: Use of file and folder names in other languages not listed above may not be fully supported. Thus, files and folders may be impossible to open or delete if named using unique characters in unsupported languages. Cyrillic characters are an example of characters that are not supported for use in file or folder names.

If you are running Microsoft Windows you can find the active code page currently used by the client. To find the code page, open a shell prompt and type `chcp`, then press Enter. The active code page is displayed.

For details about language support and code pages, see the Technical Reference.

-
1. The primary and secondary code pages for Indonesian (437, 850), Basque (850, 437), and Catalan (850, 437) are all supported.
 2. The primary Icelandic code page (850) is supported, but the secondary page (861) is not supported.

Using the Home Page

To display the NAS server **Home** page, start your Web browser, enter the server's name or IP address in the Address or Location box, and press **Enter** or **Return**.

On the **Home** page, you can:

- Access the folders and files within that share by clicking a share icon.
- See who is currently using the server by clicking the **Active Users** link.
- Change the password for a local user by clicking the **Change Password** link. (Local users are described in “Defining Users” on page 11.)
- Access additional server management features by clicking the **Administration** link to display the **Administration** menu.

Using the Administration Menu

From the **Administration** menu you can:

- Click **Quick Configure** if you would like step-by-step instructions to help you customize your NAS server and to change basic configuration settings from its factory defaults. (See “Using Quick Configure” on page 17.)
- Click **Server Settings**, **Network Settings**, **Security**, or **Disk Utilities** to review your server's configuration settings, make configuration changes as needed, and monitor your server's operation.



For example, you can use **Disk Utilities** to check a disk or change its description.

- View information about users (click **Active Users**), files (click **Open Files**), and the server log (click **Server Log**).

To learn more about the links and buttons on the **Administration** menu, click **Help** at the top of the page.

Using the Virtual Machine

Your NAS Server comes with a virtual machine already installed. This lets applications based on Java technology be run on the NAS server. The virtual machine is a software module that converts the platform independent code based on Java technology into code that is specific to the NAS server's microprocessor. Once the code is converted, the virtual machine executes the converted code.

What is a NASExtension?

A NAS Extension is an application designed to run on the NAS server. NASExtensions are integrated using the framework created specially for them. The NAS server framework allows you to access an application based on Java™ technology from the NAS server Web Administration tool. Only applications developed and integrated for the NAS server can be accessed this way.

To find other NASExtensions on your NAS Server, open the Web Administration tool and click NASExtensions. A list of all installed NASExtensions is displayed.

Enabling the Virtual Machine

By default, the virtual machine is turned off. To turn it on and begin using NASExtensions and other applications based on Java technology:

1. Start the NAS server Web Administration tool and click **NASExtensions**.
2. Click **Start Java** to start the virtual machine. You are then prompted to confirm that you want to start Java™.
3. Click **Yes** to restart the NAS server with the virtual machine enabled.

What is Secure Server?

Secure Server uses Secure Sockets Layer (SSL) to let you transmit private data over TCP/IP. The data is encrypted using a private key prior to transmitting the data. By encrypting the data prior to transmission, it will be secure and can only be read by the user requesting the data via a Web browser. The secure server is supported by all major browsers and by conventional Web pages using SSL will begin with *https*: instead of *http*:

Enabling Secure Server

To enable Secure Server, the virtual machine must be enabled. Use the NAS server Web Administration tool's advanced administration features to start SSL.

1. If Java is not already active, start Java and restart the machine as described in "Enabling the Virtual Machine" on page 31.
2. Open the Web Administration tool in your Web browser and click **Network Settings**.
3. Click **Web**, then **Secure Server (SSL)**.
4. Click **Enable/Disable SSL**, then click **OK** and log in again.

Backing Up the NAS Server

The easiest way to maintain an automatic backup on your NAS Server is with the Server-to-Server NASExtension. This NASExtension uses Java-based technology to synchronize two NAS Servers. The synchronization can be fully automated and works with all NAS Servers running OS v3.4 with a virtual machine installed. For details, see your NAS Server Sales team.

If you choose not to use this NASExtension, you should back up files stored on the NAS server in the same manner that you back up any other file server. You can use any of several commercial backup programs to copy the data stored on your server to backup media such as tape, another disk drive, another NAS server, or CD-ROM. Most backup programs store the data in a special format and include a restore function for retrieving files from backups.

Some special considerations for backing up from different operating systems are detailed in this section.

Windows Systems

The NAS server is compatible with all major backup software for Microsoft Windows NT, 200, and XP, and Microsoft Windows 2000 servers that do not require a software agent to be installed on the server to be backed up.

UNIX Systems

You can back up your NAS server using UNIX[®] backup applications, such as **tar** and **cpio**. However, you must use backup software that supports remote volumes without requiring remote system agent support.

Macintosh Systems

To back up data on your NAS server from a Macintosh computer, you must first mount the appropriate network shares (volumes) on the desktop. Doing so allows Macintosh backup programs to operate without a remote agent running on the NAS server.

Novell Networking Systems

You can back up a NAS server using applications that are compatible with the Novell[®] SMS (Storage Management System) and TSA (Target Service Agent) protocols. Supported network backup programs include Computer Associates[®] ARCserve[™] IT and Veritas Backup Exec[™] for NetWare.

When using Novell-based networking backup applications with a NAS server, you need to be aware of the following issues:

- If the NAS server does not appear on the list of servers available for backup, you may need to reconfigure the backup software to recognize the server. With some software packages, the only way to do this is to reinstall the backup program.
- Some backup applications do not operate if your server supports more users than allowed by your backup software license. By default, the NAS server is configured for 250 Novell networking users. You may need to reduce this number to match your license restrictions.

For example, if you purchased a 25-user version of Computer Associates ARCserveIT, you need to change the number of Novell networking users to 25 or fewer. (From the **Novell Networking** page, click **Advanced**, then change the **Number of user licenses**. This setting has no effect on other networking environments.)

- The NAS server does not currently support data compression. Therefore, you cannot back up data from a NetWare 4.x or 5.x volume with data compression enabled and restore it to a NAS server. (Compressed files are restored as zero length files to the NAS server volume.) If you want to transfer your data to a NAS server, you must decompress it on the NetWare server before you perform the backup.

For more detailed information about your NAS server see the Technical Reference. To access this document, use your Web browser to open the Intro.html file in the Technical Reference subdirectory of the NAS server CD-ROM.

Tips for Specific Network Environments

This section contains additional tips for using your NAS server in specific network environments. See the NAS server Technical Reference for additional information on this topic. To access this document, use your Web browser to open the Intro.html file in the Technical Reference subdirectory of the NAS server CD-ROM.

Microsoft Networks

The NAS server operates like a Microsoft Windows NT 4.0 file server.

By default, the NAS server is configured as part of **Workgroup**. You can reconfigure the server for a different workgroup or domain through **Quick Configure** or **Network Settings** (see “Using the Administration Menu” on page 30).

If you configure your NAS server to use Microsoft domain security (as described in “Configuring Microsoft Domain Security” on page 22), you do not need to set up all your network users as local NAS server users.

UNIX NFS Networks

The NAS server supports version 2.0 and 3.0 of the NFS protocol. The NAS server preserves the case of file names, but is case insensitive when comparing file names. Therefore, the server cannot have two files with the same name.

For example, a file saved as “FOO,” another saved as “Foo,” and a third saved as “foo” are considered the same file to the server.

A network share on a NAS server is equivalent to an exported file system on an NFS server. NFS users can mount NAS server shares and access their content directly or mount a subdirectory of a share. They can use dynamic mounting (with auto-mount) or static mounting (with automatic remount when the server restarts after being shut down). To perform a static mount, you must be logged into your UNIX system as root. Mount a NAS server exported file system with the following commands:

```
mount NAS_server:/share_name/local_dir
```

where `NAS_server` is the NAS Server name or IP address, `share_name` is the name of the exported file system, and `local_dir` is the local directory to which the file system is mounted. Below are two examples of a mount:

```
mount NAS30286:/share1/workdir
or
mount 192.168.1.1:/share1/workdir
```

The NAS server uses mount points (network shares) to control access. Files and directories (folders) accessible through the mount point have the access rights of the network share combined with any file and folder security.

You can configure NAS server users and grant them rights for selected network shares. (NAS server user names, such as `ROOT` and `GUEST`, are not case sensitive.) You can then associate user accounts from one or more UNIX systems to a NAS server user.

To configure NFS users first click **Users** on the **Security** menu and then click **New** to create a new, local user. (For more information about local users, see “Defining Snap Server Users” on page 21.) Select the user you have created and then click **NFS**. On the **NFS Settings for User** page, click **New**. On the **New NFS Settings for User** page, enter the user ID (UID), IP address, and Address Mask. Click **OK** to apply your changes. For more information, refer to the online Help.

Macintosh Networks

The server operates like an AppleShare® 6.0 file server. The interoperability with Windows clients is equivalent to that of a Windows NT 4.0 or Windows 2000 server with **Services for Macintosh** enabled.

If you use Microsoft networking, you can enable domain support for Macintosh networking users by configuring the NAS server to use Microsoft domain security (see “Configuring Microsoft Domain Security” on page 22). In this configuration, you do not need to set up Macintosh networking users (and groups) as local NAS server users.

Security settings for files or folders cannot be changed from a user’s computer which uses native Macintosh tools. Any changes made will have no effect.

The NAS server supports cross-platform access to application-specific files, thus allowing Macintosh-based and Windows-based applications to interoperate transparently. The NAS server keeps the resource forks in a hidden folder. To maintain compatibility with Apple programs, it is strongly recommended to copy, delete, or move these shared files using a Macintosh computer. (If working on a Windows computer, copy, delete, or move the entire folder containing the shared files.)

Novell Networks

The NAS server operates in a manner similar to a Novell NetWare 3.12 file server.

The NAS server is pre-configured to operate with other NetWare servers on a Novell network. If you want to use the NAS server as the only server for a network of Windows computers, use Microsoft networking instead.

You can link the NAS server security to that of another NetWare server, meaning that all of the users (and groups) on the existing NetWare server are automatically accepted as remote users (or groups). (See “Defining Snap Server Users” on page 21.) The external NetWare server used for this purpose must be a 3.x NAS Server or have both bindery emulation and IPX support enabled. (NDS users can take advantage of this feature to connect to the NAS server using bindery authentication.)

A network share on a NAS server is equivalent to a volume on a NetWare server.

Operating the NAS server as a Web Server

In addition to providing administration functions through the Web, the NAS server can also operate as a Web server, providing Web access to files and folders.

The NAS server supports direct read-only Web access to its files using the HTTP protocol. The NAS server is not intended for use as an all-purpose Web server, as it does not support PERL or Java scripting, animations, streaming video, or anything that would require a special application or service running on the server.

Place all HTML files you want displayed under the **webroot\$** share. To access these files as Web pages, type in the URL in your Web browser. For example:

```
http://NAS_server/Index.html
```

where *NAS_server* is the NAS server’s name or IP address, and *Index.html* is the name of the file you want to access.

To access a NAS server share (see “Assigning User Access to Network Shares” on page 23), enter the following address in a Web browser’s Address or Location box:

```
http://NAS_server/share_name
```

where *NAS_server* is the NAS server’s name or IP address and *share_name* is the name of the share. Your share should look similar to the ones on the following page.

```
http://NAS30286/share1  
or  
http://192.168.1.1/share1
```

By default, when you connect to a share from the Web, you see a list of files and folders contained in that share. How your browser displays a file depends on the file type and browser settings. To set up a Web “home” page for a share, create an HTML file named `index.html` and store it in the root of the `webroot$` share.

You can enable or disable Web access to network shares. From the **Administration** menu, click **Network Settings, Web**, and then **Enable or Disable Web**. When Web access is disabled, only administrators can access shares from the Web. When Web access is enabled, access is based on the security settings you defined. See “Setting Up Security” on page 20.



Tip: You can use the Web settings to customize the server’s Home page.

Operating the NAS server as an FTP Server

Your NAS server can also be used as an FTP server, allowing users to access to the server’s files and directories via FTP clients.

To access the NAS server share (see “Assigning Users Access to Files and Folders” on page 24), enter the following address in a Web browser’s or FTP program’s Address or Location box:

```
ftp://NAS_server/share_name
```

where `NAS_server` is the NAS server’s name or IP address and `share_name` is the desired share. It should look similar to the examples below.

```
ftp://NAS30123/share1  
or  
ftp://192.168.1.1/share1
```

You now have standard FTP access to all files and directories within the share.

You can enable or disable FTP access to network shares. From the **Administration** menu, click **Network Settings, FTP**, and then **Enable FTP Server**. When FTP access is enabled, access is based on the security settings you defined. See “Setting Up Security” on page 20.

Managing the NAS server with SNMP

Your NAS server can be managed using SNMP.

SNMP is enabled by default. To disable SNMP access:

1. Go to the server’s **Home** page and open the **Administration** menu.

2. Select **Network Settings** and then select **SNMP**.
3. Disable the SNMP access.

UPS Support

Your NAS Server can be used with uninterruptible power supplies (UPS). NAS Servers communicate with the UPS via the network, not via a serial cable.

You can configure the NAS Server to automatically shut down upon receiving a low battery message from your network-based uninterruptible power supply (UPS).

Your NAS Server can interact with two UPS devices; messages from either or both can be configured to trigger an automated shutdown.

To enable automated shutdown on low battery:

1. From the Web Administration tool, select **Server Settings** and then select **UPS Support**. The page changes to show you available UPS settings.
2. Enable UPS support.
3. Enter the IP address and administrator information for the primary UPS device.
4. If using a second device, enter the information for the secondary device.
5. Define the UPS device to use when determining that a shutdown is needed.
6. Click **OK** to complete the configuration.

Hot Swappable Items

The NAS server has three hot swappable features: the disk drives, the fans, and the power supplies. If you should need to replace a part of the NAS server, you will be able to purchase replacement components through your NAS server retailer.



Tip: The server can be configured to send e-mail or SNMP failure notification to the administrator if one of the drives, fans or power supplies fails. See “Failure Notification via E-mail” on page 20.