

# NSA210

*1-Bay Digital Media Server*

## *User's Guide*



### Default Login Details

Web Address	nsa210
User Name	admin
Password	1234

Firmware Version 3.20  
Edition 2, 7/2009

[www.zyxel.com](http://www.zyxel.com)

# ZyXEL



# About This User's Guide

## Intended Audience

This manual is intended for people who want to configure the NSA using the web configurator.

## Tips for Reading User's Guides On-Screen

When reading a ZyXEL User's Guide On-Screen, keep the following in mind:

- If you don't already have the latest version of Adobe Reader, you can download it from <http://www.adobe.com>.
- Use the PDF's bookmarks to quickly navigate to the areas that interest you. Adobe Reader's bookmarks pane opens by default in all ZyXEL User's Guide PDFs.
- If you know the page number or know vaguely which page-range you want to view, you can enter a number in the toolbar in Reader, then press [ENTER] to jump directly to that page.
- Type [CTRL]+[F] to open the Adobe Reader search utility and enter a word or phrase. This can help you quickly pinpoint the information you require. You can also enter text directly into the toolbar in Reader.
- To quickly move around within a page, press the [SPACE] bar. This turns your cursor into a "hand" with which you can grab the page and move it around freely on your screen.
- Embedded hyperlinks are actually cross-references to related text. Click them to jump to the corresponding section of the User's Guide PDF.

## Related Documentation

- Quick Start Guide

The Quick Start Guide is designed to help you get your NSA up and running right away. It contains information on setting up your network and configuring for Internet access.

- Web Configurator Online Help

The embedded Web Help contains descriptions of individual screens and supplementary information.

Note: It is recommended you use the web configurator to configure the NSA.

- Support Disc

Refer to the included CD for support documents.

## Documentation Feedback

Send your comments, questions or suggestions to: [techwriters@zyxel.com.tw](mailto:techwriters@zyxel.com.tw)

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,  
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

## Need More Help?

More help is available at [www.zyxel.com](http://www.zyxel.com).



- Download Library

Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the User Guide, Quick Start Guide and Command Line Interface Reference Guide in order to better understand how to use your product.

- Knowledge Base

If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.



## Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See [http://www.zyxel.com/web/contact\\_us.php](http://www.zyxel.com/web/contact_us.php) for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.

Brief description of the problem and the steps you took to solve it.

# Document Conventions

## Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

**Warnings tell you about things that could harm you or your device.**

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.




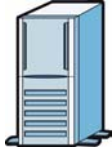

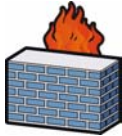



## Syntax Conventions

- The NSA may be referred to as the "NSA", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket ( > ) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

## Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The NSA icon is not an exact representation of your device.

Graphics in this book may differ slightly from the product due to differences in operating systems, operating system versions, or if you installed updated firmware/software for your device. Every effort has been made to ensure that the information in this manual is accurate.

NSA 	Computer 	Notebook computer 
Server 	Television 	Firewall 
Router 	Switch 	Internet 

# Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: RISK OF EXPLOSION IF BATTERY (on the motherboard) IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS. Dispose them at the applicable collection point for the recycling of electrical and electronic equipment. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.



# Contents Overview

**Introduction ..... 21**

    Getting to Know Your NSA ..... 23

    NAS Starter Utility ..... 29

    Web Configurator Basics ..... 39

    Tutorials ..... 59

**System Setting and Features ..... 133**

    Status Screen ..... 135

    System Setting ..... 139

    Storage ..... 145

    Network ..... 159

    Applications ..... 165

    Package Management ..... 211

    Auto Upload ..... 265

**Sharing ..... 281**

    Users ..... 283

    Groups ..... 289

    Shares ..... 293

**Maintenance and Protecting Data ..... 303**

    Maintenance Screens ..... 305

    Protecting Your Data ..... 329

**Troubleshooting and Specifications ..... 335**

    Troubleshooting ..... 337

    Product Specifications ..... 361

**Appendices and Index ..... 371**



# Table of Contents

<b>About This User's Guide .....</b>	<b>3</b>
<b>Document Conventions.....</b>	<b>6</b>
<b>Safety Warnings.....</b>	<b>8</b>
<b>Contents Overview .....</b>	<b>9</b>
<b>Table of Contents.....</b>	<b>11</b>
<b>Part I: Introduction.....</b>	<b>21</b>
<b>Chapter 1</b>	
<b>Getting to Know Your NSA .....</b>	<b>23</b>
1.1 Overview .....	23
1.2 Firmware .....	25
1.3 Hard Disk .....	25
1.4 LEDs .....	26
1.4.1 COPY/SYNC Button .....	27
1.4.2 RESET Button .....	27
<b>Chapter 2</b>	
<b>NAS Starter Utility.....</b>	<b>29</b>
2.1 Overview .....	29
2.2 What You Can Do .....	30
2.3 Starting the NAS Starter Utility .....	30
2.4 Network Interface Card List Screen .....	30
2.5 Device List Screen .....	31
2.6 The Network Configuration Screens .....	34
2.6.1 The Firmware Path Screen .....	36
<b>Chapter 3</b>	
<b>Web Configurator Basics .....</b>	<b>39</b>
3.1 Overview .....	39
3.2 Accessing the NSA Web Configurator .....	39
3.2.1 Access the NSA Via NAS Starter Utility .....	40
3.2.2 Web Browser Access .....	40
3.3 Login .....	41

3.4 User-level Screens Overview .....	42
3.5 My NSA Screens .....	43
3.5.1 My NSA Share Browsing Screen .....	44
3.5.2 My NSA Share Browsing Move or Copy Screen .....	47
3.5.3 My NSA Configuration Screen .....	48
3.5.4 My NSA Edit Share Screen .....	49
3.5.5 Share and Folder Names .....	50
3.5.6 Password Screen .....	51
3.6 Administration Screens .....	52
3.6.1 Global Administration Icons .....	52
3.6.2 Navigation Panel .....	53
3.6.3 Main Window .....	55
3.6.4 Status Messages .....	55
3.6.5 Common Screen Icons .....	55
3.6.6 Session Example (Windows) .....	56
<b>Chapter 4</b>	
<b>Tutorials.....</b>	<b>59</b>
4.1 Overview .....	59
4.2 Creating a Volume .....	59
4.2.1 Creating a RAID 1 Volume .....	60
4.2.2 Migrate Button .....	60
4.2.3 Create a SATA Volume Button .....	61
4.2.4 Creating a PC Compatible Volume .....	63
4.3 Deleting a Volume .....	66
4.4 File Sharing Tutorials .....	67
4.4.1 Creating a User Account .....	67
4.4.2 Creating a Share .....	70
4.4.3 Creating a Group .....	71
4.4.4 Accessing a Share From Windows Explorer .....	72
4.4.5 Accessing a Share Using FTP .....	74
4.4.6 Accessing a Share Through the Web Configurator .....	76
4.5 Download Service Tutorial .....	77
4.5.1 Copying/Pasting a Download Link .....	77
4.5.2 Installing the Link Capture Browser Plugin .....	80
4.5.3 Using the Link Capture Browser Plugin .....	85
4.5.4 Configuring the Download Service Preferences .....	87
4.5.5 Using Download Service Notification .....	89
4.6 Broadcatching Tutorial .....	93
4.7 Printer Server Tutorial .....	96
4.8 Copy and Flickr Auto Upload Tutorial .....	98
4.9 FTP Uploadr Tutorial .....	99
4.10 Web Configurator's Security Sessions .....	104



4.10.1 Customizing the NSA's Certificate .....	104
4.10.2 Downloading and Installing Customized Certificate .....	106
4.10.3 Turn on the NSA's Web Security .....	110
4.11 Using FTPES to Connect to the NSA .....	116
4.12 Using a Mac to Access the NSA .....	117
4.12.1 Finder .....	118
4.12.2 Go Menu .....	119
4.13 How to Use BackupPlanner .....	120
4.13.1 Creating an Archive Backup .....	121
4.13.2 Creating a Synchronization Backup .....	124
4.13.3 Restoring Archived Files by Backup Job .....	127
4.13.4 Restoring by Backup Files .....	129
 <b>Part II: System Setting and Features .....</b>	<b>133</b>
 <b>Chapter 5</b>	
<b>Status Screen .....</b>	<b>135</b>
5.1 Overview .....	135
5.2 The Status Screen .....	135
 <b>Chapter 6</b>	
<b>System Setting .....</b>	<b>139</b>
6.1 Overview .....	139
6.2 What You Can Do .....	139
6.3 What You Need to Know .....	139
6.4 The Server Name Screen .....	140
6.5 The Date/Time Screen .....	141
 <b>Chapter 7</b>	
<b>Storage .....</b>	<b>145</b>
7.1 Overview .....	145
7.2 What You Can Do .....	145
7.3 What You Need to Know .....	145
7.4 The Storage Screen .....	147
7.4.1 Creating a SATA Volume .....	148
7.4.2 Editing a Volume .....	151
7.4.3 Creating a USB Volume .....	152
7.5 Storage Technical Reference .....	153
7.5.1 Choosing a Storage Method for a Volume .....	153
7.5.2 Storage Methods .....	154
7.5.3 Volume Status .....	155

7.5.4 Volumes and RAID .....	156
7.5.5 Disk Replacement Restrictions .....	156
7.5.6 External Disks .....	157
<b>Chapter 8</b>	
<b>Network .....</b>	<b>159</b>
8.1 Overview .....	159
8.2 What You Can Do .....	159
8.3 What You Need to Know .....	159
8.4 The TCP/IP Screen .....	161
8.5 The PPPoE Screen .....	163
<b>Chapter 9</b>	
<b>Applications .....</b>	<b>165</b>
9.1 Overview .....	165
9.2 What You Can Do .....	165
9.3 What You Need to Know .....	165
9.4 The FTP Screen .....	167
9.5 The Media Server Screen .....	170
9.6 The Download Service Screen .....	171
9.6.1 Adding a Download Task .....	175
9.6.2 Configuring General Settings .....	177
9.6.3 Configuring the BitTorrent Settings .....	180
9.6.4 Edit IP Filter .....	181
9.6.5 Displaying the Task Information .....	183
9.7 The Web Publishing Screen .....	184
9.8 The Broadcatching Screen .....	186
9.8.1 Adding a Broadcatching Channel .....	188
9.8.2 Editing a Broadcatching Channel .....	192
9.9 The Print Server Screen .....	194
9.9.1 Print Server Rename .....	195
9.10 The Copy/Sync Button Screen .....	196
9.11 Technical Reference .....	197
9.11.1 Sharing Media Files on Your Network .....	197
9.11.2 Download Service .....	199
9.11.3 Link Capture Browser Plugin .....	199
9.11.4 Download Service Notification .....	200
9.11.5 BitTorrent Security .....	201
9.11.6 Web Publishing Example .....	203
9.11.7 Web Publishing .....	205
9.11.8 Channel Guides for Broadcatching .....	206
9.11.9 Printer Sharing .....	207
9.11.10 Copying Files .....	208

9.11.11 Synchronizing Files .....	209
<b>Chapter 10</b>	
<b>Package Management .....</b>	<b>211</b>
10.1 Overview .....	211
10.2 What You Can Do .....	211
10.3 What You Need to Know .....	211
10.4 Package Management Screen .....	212
10.4.1 Displaying the Package Information .....	215
10.5 eMule Screens .....	216
10.5.1 eMule Server Screen .....	216
10.5.2 Add Server .....	217
10.5.3 Edit Server .....	218
10.5.4 My Info .....	219
10.5.5 eMule Task Screen .....	220
10.5.6 Add Task .....	222
10.5.7 Preferences .....	224
10.5.8 Edit IP Filter .....	227
10.5.9 Share Browsing .....	228
10.5.10 Task Info .....	229
10.5.11 eMule Search Screen .....	231
10.6 DyDNS Screen .....	232
10.7 NFS Screen .....	233
10.7.1 Add/Edit NFS Share .....	235
10.7.2 NFS Session .....	236
10.8 SMART Screen .....	237
10.8.1 SMART Brief Summary .....	238
10.8.2 SMART Full Summary .....	239
10.9 Protect Screens .....	241
10.10 Backup Screens .....	241
10.10.1 Backup: Step 1 .....	243
10.10.2 Backup: Step 2 .....	245
10.10.3 Backup: Step 3 .....	248
10.10.4 Backup: Step 4 .....	249
10.10.5 Edit Job Screen .....	250
10.10.6 Edit Job: Step 1 .....	251
10.10.7 Edit Job: Step 2 .....	253
10.10.8 Restore Archive Screen .....	254
10.10.9 <b>Restore Archive: Step 1</b> .....	<b>254</b>
10.10.10 Restore Archive: Step 2 .....	255
10.10.11 Restore Archive: Step 3 .....	256
10.11 Restore Screen .....	257
10.11.1 Restore: Step 1 .....	257

10.11.2 Restore: Step 2 .....	258
10.11.3 Restore: Step 3 .....	259
10.11.4 Restore: Step 4 .....	260
10.12 Technical Reference .....	261
10.12.1 S.M.A.R.T Attributes .....	261
<b>Chapter 11</b>	
<b>Auto Upload.....</b>	<b>265</b>
11.1 Overview .....	265
11.2 What You Can Do .....	265
11.3 What You Need to Know .....	265
11.4 The Flickr/YouTube Screen .....	266
11.4.1 Configuring the Flickr Settings .....	267
11.4.2 Configuring the YouTube Settings .....	272
11.5 The FTP Uploadr Screen .....	276
11.5.1 Adding or Editing an FTP Server Entry .....	278
11.5.2 The FTP Uploadr Preferences Screen .....	279
 <b>Part III: Sharing .....</b>	 <b>281</b>
<b>Chapter 12</b>	
<b>Users .....</b>	<b>283</b>
12.1 Overview .....	283
12.2 What You Can Do .....	283
12.3 The Users Screen .....	284
12.3.1 User Icons .....	285
12.3.2 Adding or Editing an Account .....	286
12.3.3 Usernames .....	287
12.4 Displaying User Info .....	288
<b>Chapter 13</b>	
<b>Groups .....</b>	<b>289</b>
13.1 Overview .....	289
13.2 What You Can Do .....	289
13.3 The Groups Screen .....	289
13.3.1 Adding or Editing a Group .....	291
13.3.2 Group Names .....	292
<b>Chapter 14</b>	
<b>Shares .....</b>	<b>293</b>
14.1 Overview .....	293

14.2 What You Can Do .....	293
14.3 The Shares Screen .....	294
14.3.1 Adding or Editing Share .....	296
14.3.2 Configuring Advanced Share Access .....	297
14.3.3 Public and ANONYMOUS Share Access Rights .....	298
14.4 The Recycle Bin Configuration Screen .....	299
14.4.1 Recycle Bins .....	299
14.4.2 Configuring Recycle Bins .....	299
14.5 The Share Browser Screen .....	300
14.5.1 Moving or Copying Files .....	302
 <b>Part IV: Maintenance and Protecting Data.....</b>	<b>303</b>
 <b>Chapter 15</b>	
<b>Maintenance Screens .....</b>	<b>305</b>
15.1 Overview .....	305
15.2 What You Can Do .....	305
15.3 The Power Management Screen .....	306
15.3.1 Editing the Power Control Schedule Screen .....	308
15.4 The Log Screen .....	310
15.4.1 Report Config Screen .....	311
15.4.2 Email Setting .....	311
15.4.3 Report Setting .....	312
15.4.4 Syslog Server Setting .....	313
15.5 The Configuration Screen .....	314
15.6 SSL Certification .....	315
15.6.1 Modifying or Creating a Certificate .....	317
15.7 The Firmware Upgrade Screen .....	318
15.8 The Shutdown Screen .....	319
15.9 Technical Reference .....	319
15.9.1 Log Classes .....	320
15.9.2 Log Severity Levels .....	320
15.9.3 Log Messages .....	320
 <b>Chapter 16</b>	
<b>Protecting Your Data .....</b>	<b>329</b>
16.1 Overview .....	329
16.2 Protection Methods .....	329
16.3 Configuration File Backup and Restoration .....	330
16.4 Memeo Autobackup .....	330
16.4.1 Memeo Autobackup Installation and Setup .....	330

16.4.2 Using Memeo Autobackup After the Initial Setup .....	333
---	-----

## **Part V: Troubleshooting and Specifications ..... 335**

### **Chapter 17**

#### **Troubleshooting..... 337**

17.1 Troubleshooting Overview .....	337
17.2 Power, Hardware, Connections, and LEDs .....	338
17.3 NAS Starter Utility .....	341
17.4 NSA Login and Access .....	342
17.4.1 Reset the NSA .....	344
17.4.2 Enabling Scripting of Safe ActiveX Controls .....	344
17.5 I Cannot Access The NSA .....	346
17.6 Users Cannot Access the NSA .....	347
17.7 Storage Volumes .....	349
17.8 External USB Drives .....	350
17.9 Firmware .....	350
17.10 File Transfer .....	350
17.11 Networking .....	351
17.12 Some Features' Screens Do Not Display .....	352
17.13 Media Server Functions .....	353
17.14 Download Service and Broadcatching Functions .....	355
17.15 Web Publishing .....	356
17.16 Auto Upload .....	357
17.17 Package Management .....	358
17.18 Backups .....	359

### **Chapter 18**

#### **Product Specifications ..... 361**

18.1 Physical Features .....	361
18.2 Firmware Features .....	362
18.3 Specification Tables .....	364
18.4 Supported Media Server Content Formats .....	368
18.5 Supported iTunes Server Content Formats .....	369
18.6 Power Consumption .....	369

## **Part VI: Appendices and Index ..... 371**

Appendix A Setting up Your Computer's IP Address .....	373
--	-----

Appendix B Pop-up Windows, JavaScripts and Java Permissions .....	389
---	-----

Appendix C Common Services ..... 399

Appendix D Importing Certificates..... 403

Appendix E Open Source Licences..... 435

Appendix F Legal Information ..... 473

**Index..... 477**





---

# PART I

# Introduction

---

Getting to Know Your NSA (23)

NAS Starter Utility (29)

Web Configurator Basics (39)

Tutorials (59)



# Getting to Know Your NSA

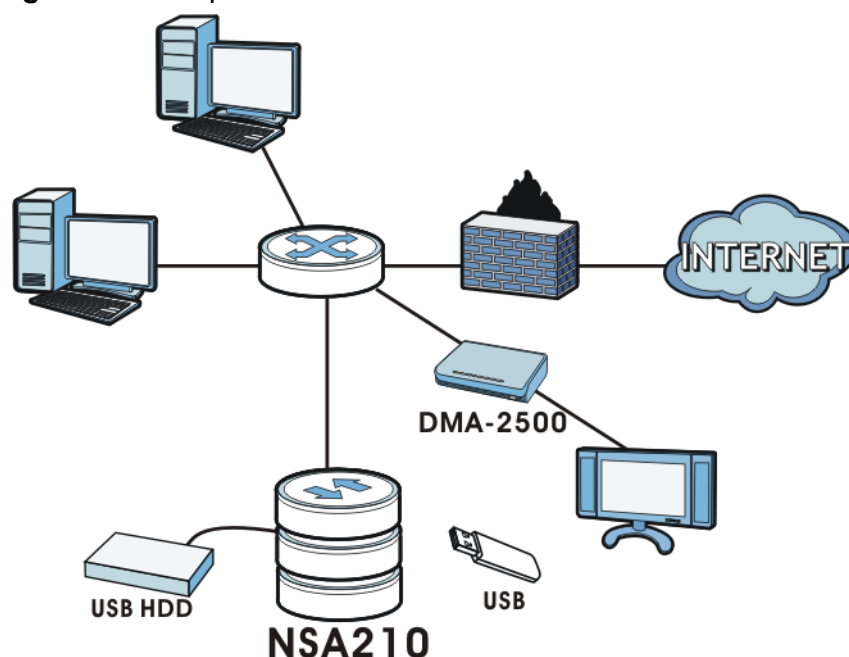
## 1.1 Overview

This chapter covers the main features and applications of the NSA.

Use the NSA210 to do the following.

- Share files between computers on your network.
- Back up files from your computers to the NSA.
- Use the **COPY/SYNC** button to copy or synchronize files between the NSA and USB devices like card readers, MP3 players, mass storage devices, and digital cameras without using a computer.
- Have the NSA handle large file downloads.
- Automatically download files from website feeds for convenient viewing.
- Play the NSA's video, music and photo files on your computers using the included media client software.
- Play the NSA's video, music and photo files on hardware-based media clients like the DMA-2500.
- Use the NSA's website to share files with remote users.
- Use iTunes on your computer to play video and music files stored on the NSA.
- Share printers.
- Automatically upload photo and video files to your FTP server, Flickr and YouTube accounts.

**Figure 1** Example of the NSA in a Home Network



Above is the NSA in a home network. Users back up and share data on the NSA. The DMA-2500 plays the NSA's media files on the TV. A USB hard drive provides extra storage space and files are copied directly from the USB mass storage device to the NSA.

Place the NSA behind a firewall and/or IDP (Intrusion Detection and Prevention) device to protect it from attacks from the Internet.

Note: See [Chapter 18 on page 361](#) for a more detailed list of NSA features and lists of compatible hard drives and USB devices.

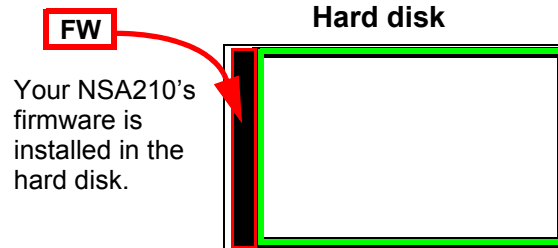
Refer to the Quick Start Guide for hardware connections and how to install and remove hard drives from the disk trays.

Note: Turn off and disconnect the NSA before you install or remove the internal hard disk.

## 1.2 Firmware

Before you can start using your NSA, you have to install the firmware on the hard disk. Use the NAS Starter Utility to do this. See [Chapter 2 on page 29](#) for more information on the NAS Starter Utility.

**Figure 2** NSA210 Hard Disk Partition



The firmware includes the features mentioned in [Section 3.6.2 on page 53](#). You can use the **Package Management** screen ([Chapter 10 on page 211](#)) to install more applications from a web location (specified in the firmware) to your NSA.

## 1.3 Hard Disk

Your NSA has one internal hard disk bay and one external SATA (eSATA) port. This allows you to connect one internal SATA (Serial Advanced Technology Attachment) hard disk and one eSATA hard disk (optional).

After installing the firmware on the internal hard disk, it is configured as a JBOD volume by default. JBOD stands for Just a Bunch Of Disk and in this storage method, all disk space is used for your data - none is used for backup. If you are not using an eSATA hard disk, JBOD is the only storage method you can use.

If you attach an eSATA (external SATA) hard disk, you can create a RAID 1 volume. RAID 1 allows data recovery in case your hard disk fails. To create a RAID 1 volume on the NSA, you must delete the JBOD volume created by the firmware. Refer to [Section 7.4 on page 147](#) for the **Storage** screen where you can create the RAID 1 volume.

The eSATA hard disk can also be configured as a JBOD or a PC Compatible Volume. See [Section 7.5.2 on page 154](#) for more information on these storage methods.

Note that both SATA and eSATA hard disks are treated as internal or SATA volumes in the **Storage** screen ([Section 7.4 on page 147](#)). Any hard disk connected to the USB port(s) is considered an external or USB volume.

# 1.4 LEDs

The NSA LEDs (lights) tell you important information.

**Figure 3** NSA Front Panel



This table describes the NSA’s LEDs.

**Table 1** LEDs

LED	COLOR	STATUS	DESCRIPTION
POWER	Blue	On	The NSA is turned on and receiving power.
		Off	The NSA is turned off.
SYSTEM	Green	On	The NSA has fully started and is operating normally.
		Blinking	The NSA is starting up or upgrading the firmware.
	Red	On	The NSA has failed.
HDD	Green	On	The hard disk drive is connected properly to the NSA.
		Blinking	The NSA is saving data to the hard disk drive.
	Red	On	The hard disk drive has failed and the NSA can no longer detect it.

**Table 1** LEDs (continued)

LED	COLOR	STATUS	DESCRIPTION
USB	Green	On	The hard disk drive is connected properly to the NSA.
		Blinking	The NSA is saving data to the hard disk drive.
	Red	On	The hard disk drive has failed and the NSA can no longer detect it.
		Off	No USB device connected to the USB port.
eSATA	Green	On	The hard disk drive is connected properly to the NSA.
		Blinking	The NSA is saving data to the hard disk drive.
	Red	On	The hard disk drive has failed and the NSA can no longer detect it.
		Off	No eSATA hard disk connected to the eSATA port.
COPY	Green	On	A USB device is connected to the NSA.
		Blinking	The NSA is copying or synchronizing files to or from the USB device.
	Red	On	Copying or synchronizing files to or from the USB device failed.
		Off	No USB device is connected.

## 1.4.1 COPY/SYNC Button

Use the **COPY/SYNC** button on the front panel to copy or synchronize files between a connected USB device and the NSA. See [Section 9.10 on page 196](#) for more details on how to configure the copy/sync settings.

## 1.4.2 RESET Button

Use the **RESET** button on the rear panel to restore the NSA's default settings.

**Figure 4** The RESET Button

- Press the **RESET** button until you hear one beep (after about two seconds), then release it. You will hear one more beep after you release the button.

This resets the NSA's IP address and password to the default values.

- Press the **RESET** button until you hear two beeps. After the second beep, continue pressing the button for five more seconds, then release it. You will hear three quick beeps after you release the button.

This resets the NSA to the factory default configuration. All settings you have configured on the NSA, including IP address, password, user accounts, groups, and so on will be reset to the factory defaults.

The reset process does NOT affect the volume settings, nor data stored on the NSA.

You should periodically back up your configuration file to your computer (see [Section 15.5 on page 314](#) for details about managing the NSA's configuration file). You could then restore your configuration in the event that you or someone else reset the NSA to the factory defaults.

**Note:** You should keep the NSA in a secure location in order to prevent unauthorized reset of the device.



# NAS Starter Utility

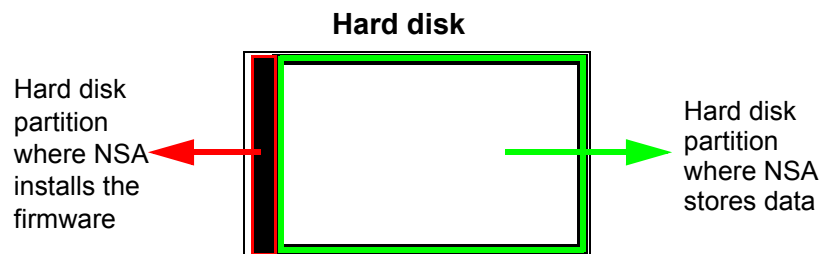
## 2.1 Overview

This chapter describes the NAS Starter Utility. You must use the NAS Starter Utility each time you install a new hard disk on the NSA. The NAS Starter Utility does the following:

- Discover and access the NSA's Web Configurator when you connect the NSA for the first time to your computer or your network
- Installs the firmware on the hard disk in your NSA so you can start configuring the NSA

The NAS Starter Utility formats the hard disk so that it installs the firmware on one partition and your data on another, as described in the following figure.

**Figure 5** NSA210 Hard Disk Partition



**Make sure you have a backup of any existing data in the hard disk before installing it in the NSA. The NSA installs its firmware on the hard disk and this may result to all data being deleted in the process.**

The NAS Starter Utility works on Windows platforms (Windows 2000, Windows XP, Windows Vista or Windows 7).

Note: Refer to the Quick Start Guide for for your NSA's hardware connections and the steps for installing the NAS Starter Utility.

## 2.2 What You Can Do

- Use the **Network Interface Card List** screen ([Section 2.4 on page 30](#)) to select the network interface that your computer is using to connect to the network where the NSA is on.
- Use the **Device List** screen ([Section 2.5 on page 31](#)) to view all hostnames, IP addresses and status of all NSAs in your network. If the NSA is initialized, you can also access the Web Configurator and map your NSA to your local computer in this screen.
- Use the **Network Configuration** screens ([Section 2.6 on page 34](#)) to configure NSA network settings such as host name (server name), IP address, subnet mask, default gateway, DNS and PPPoE settings.
- Use the **Firmware Path** screen ([Section 2.6.1 on page 36](#)) to initialize the hard disk and install the firmware.

## 2.3 Starting the NAS Starter Utility

- The NAS Starter Utility broadcasts a request packet when you first run it. Each NSA has an NAS Starter Utility Agent that always listens and responds to requests from the NAS Starter Utility. The NAS Starter Utility receives the response packet that contains information, such as host name, IP, MAC address, and so on.
- If you plan to use more than one NSA in your network, note down the MAC address of each device. The MAC address can be found printed on a sticker in the device housing. This enables you to identify each NSA when you start configuring them in the NAS Starter Utility screens.
- The NAS Starter Utility checks whether a hard disk is initialized or uninitialized. An initialized hard disk has the NSA firmware installed and can be used readily. An uninitialized hard disk can be a new hard disk or a used hard disk that has a different format than the NSA. In this case, the NSA has to initialize the hard disk by formatting it and installing the NSA firmware. All previous data is deleted so it is recommended that you back up all your files that are in the hard disk before installing it in the NSA.

You can initialize the hard disk in the **Firmware Path** screen ([Section 2.6.1 on page 36](#)). Note that if you select **Initialize Hard Disk** in this screen, you will lose all data in the hard disk.

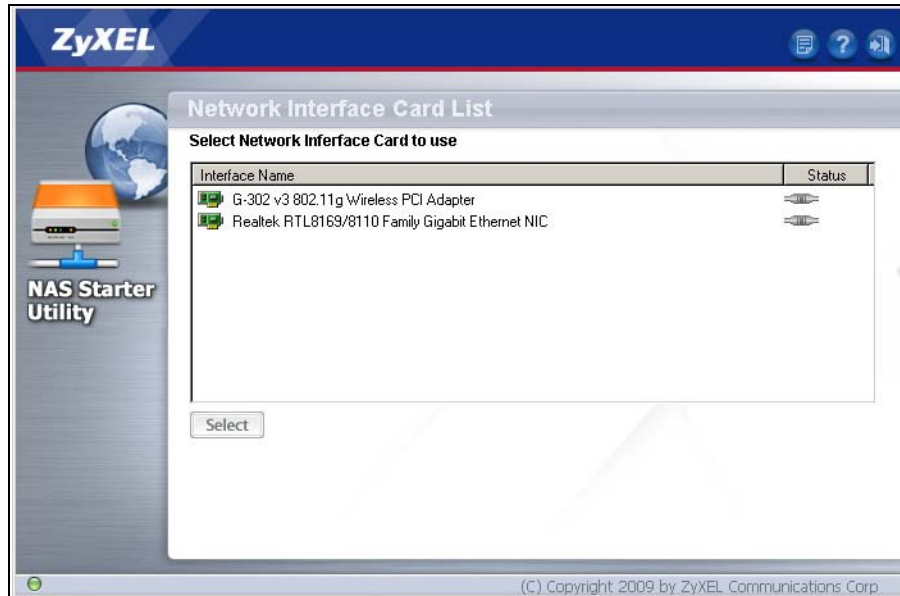
## 2.4 Network Interface Card List Screen

Use this screen to select the network interface on your computer to which your NSA is connected.

Start the NAS Starter Utility (click the icon in your Desktop or in **Start > Programs > ZyXEL > NAS Starter Utility**).

If the computer on which you are running the NAS Starter Utility has more than one active network interface, the **Network Interface Card List** screen appears as follows.

**Figure 6** Select Network Interface Card



Highlight one interface and then click **Select** to use that interface. The NAS Starter Utility will continue to use this interface until you exit the NAS Starter Utility and run it again.

**Note:** This screen does not show up if the computer on which you are running the NAS Starter Utility only has one active network interface. Skip this section and see the **Device List** screen ([Section 2.5 on page 31](#)).

## 2.5 Device List Screen

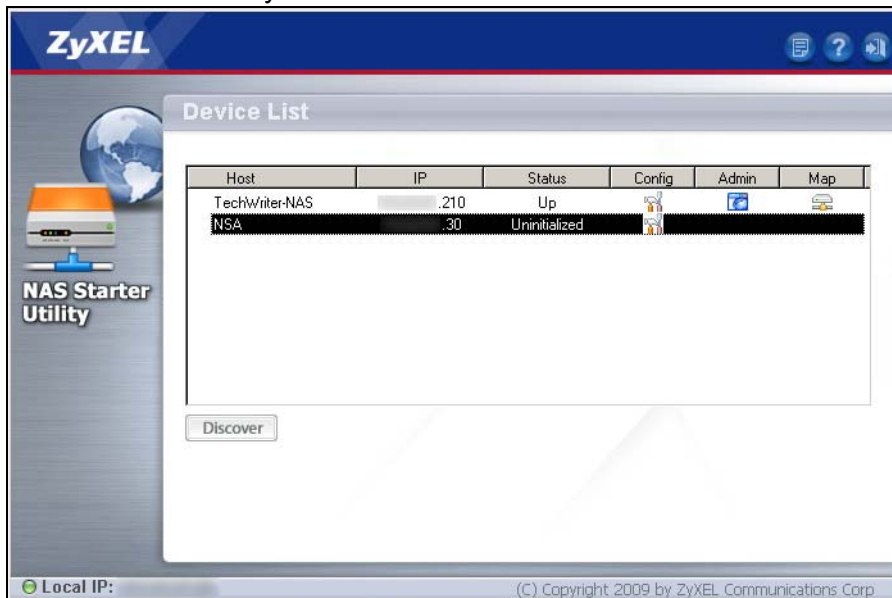
Use this screen to view all host names, IP addresses and status of all NSAs in your network. The host name is the **Server Name** of your NSA (default is '**NSA210**') that you can change (see [Section 2.6 on page 34](#)) to a more recognizable one in your network.

If the firmware is installed in your NSA, you can also access the Web Configurator and map your NSA to your local computer in this screen.

Start the NAS Starter Utility (click the icon in your Desktop or in **Start > Programs > ZyXEL > NAS Starter Utility**). The NAS Starter Utility main screen appears as follows.




Note: If the computer on which you're running the NAS Starter Utility has more than one active network interface, the **Network Interface Card List** screen ([Section 2.4 on page 30](#)) appears first so you can choose the network interface you want to use.

**Figure 7** NAS Starter Utility





The following table describes the labels in this screen.



**Table 2** NAS Starter Utility

LABEL	DESCRIPTION
	<b>About</b> Click this to view information about the NAS Starter Utility.
	<b>Help</b> Click this to open a web help page about the NAS Starter Utility screens.
	<b>Logout</b> Click this at any time to exit the NAS Starter Utility.

**Table 2** NAS Starter Utility

LABEL	DESCRIPTION
Host	<p>This is the server name you configured for the NSA. If you have more than one NSA in your network, it is recommended that you give each one a unique name for identification purposes.</p> <p>If you have several NSAs connected to your computer/network, hover your mouse over the host name to view the details of each device. A box pops up (see below) containing the details of each NSA. You can identify the device you want to configure by checking the MAC address.</p> <div data-bbox="570 506 1084 919" style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <pre> Hostname: NSA-Public MAC Address: 00:a0:c5:13:95:05 DHCP: Yes IP: .5 Mask: 255.255.255.0 Gateway: .254 DDNS: Yes Primary DNS: .2 Secondary DNS: .1 Firmware Version: V2009-06-15_04_38_14(AFD.0)b1 Model ID: NSA210 Status: Up URL: http://.5 Error: </pre> </div>
IP	This is the current IP address of the NSA.
Status	<p>This shows whether the NSA is <b>Uninitialized</b>, <b>Unreachable</b>, <b>Down</b>, <b>Config Failed</b> or <b>Up</b>.</p> <ul style="list-style-type: none"> <li>• This shows <b>Uninitialized</b> when the hard disk does not have the NSA firmware installed or the hard disk partitioning is not compatible with the NSA.</li> <li>• If the NAS Starter Utility fails to get a response or connect to the NSA web interface for any reason, the NSA is considered <b>Unreachable</b>. For example, the NSA may be unreachable if it's in a different subnet to the NAS Starter Utility.</li> <li>• If the NAS Starter Utility initially finds the NSA and then later the NSA is turned off or changed to a different subnet, it will show <b>Down</b>.</li> <li>• If you use the NAS Starter Utility to change NSA settings, but the NAS Starter Utility cannot apply the changes, it will show <b>Config Failed</b>.</li> <li>• When the NAS Starter Utility gets a response from an NSA and connects to the NSA web interface using its IP address, it shows <b>Up</b>.</li> </ul>
	<p><b>Config</b></p> <p>Click this to change the NAS Starter Utility's network settings and initialize and/or format the hard disk.</p>
	<p><b>Admin</b></p> <p>Click this to log into the web configurator. The default username is 'admin' and the password is '1234'.</p>

**Table 2** NAS Starter Utility

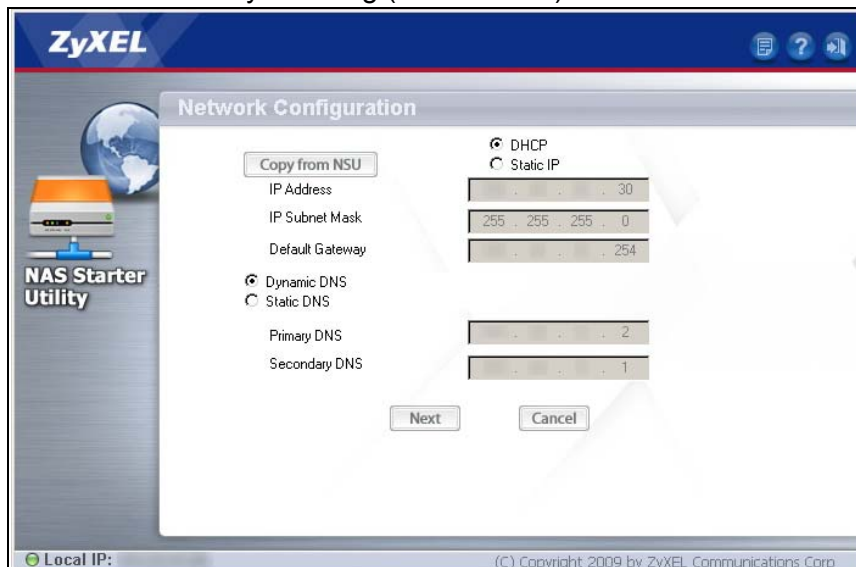
LABEL	DESCRIPTION
	<p><b>Map</b></p> <p>Click this to map the NAS Starter Utility to a Windows network drive. A pop-up screen appears. Enter the name of the share you want to map and then click <b>OK</b>.</p>
	<p><b>Discover</b></p> <p>Click this to refresh the screen.</p> <p>The NAS Starter Utility does not automatically refresh periodically.</p>

## 2.6 The Network Configuration Screens

Note: The Network Configuration screen that displays when you first use your NSA differs from the ones that shows when the NSA's hard disk has been initialized. Both screens are described in this section.

Use this screen to change the NSA network settings such as IP address, subnet mask, default gateway and DNS.

Click the icon under **Config** in the **Device List** screen. The following displays when the hard disk in the NSA not been initialized.

**Figure 8** NAS Starter Utility > Config (Uninitialized)

The following screen displays when the hard disk in the NSA has been initialized. It allows you to configure additional network settings such as host name (server name) and PPPoE settings.

**Figure 9** NAS Starter Utility > Config (Initialized)

**ZyXEL**

**Network Configuration**

Server Name: NSA

Device MAC: 00:a0:c5:13:

Device IP: 5

LAN

☒ DHCP ☐ Static IP

IP Address: 5

IP Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 254

☐ Dynamic DNS ☒ Static DNS

Primary DNS: 2

Secondary DNS: 1

Local IP: (C) Copyright 2009 by ZyXEL Communications Corp

The following table describes the labels in this screen. Some fields below do not apply to the **Device List** screen when the hard disk in the NSA is uninitialized.

**Table 3** NAS Starter Utility > Config

LABEL	DESCRIPTION
Server Name	The server name is a name that should uniquely identify the NSA in your network. You can enter up to 15 alphanumeric characters with minus signs allowed but not as the last character. The name must begin with an alphabetic character (a-z) and is NOT case sensitive.
Device MAC	This is the MAC address of your NSA.
Device IP	This is the current IP address of your NSA.
Copy from NSU	Click this if you want to manually assign the NSA an IP address that is in the same subnet as the computer to which your NSA is connected. When you click this, the IP address of the computer displays. Change the host ID part of the IP address. If your computer's IP address is AAA.BBB.CCC.XXX, change XXX to another number (for example, from 192.168.1.2 to 192.168.1.3.)  If the computer is connected to the network, use an IP address that is not yet taken by another computer.  If the computer is not connected to the network, note that the IP address you assign to the NSA may not work once you connect the computer or the NSA to the network.
DHCP	Select this if the NSA is automatically assigned an IP address from the ISP or a DHCP server in your network.

**Table 3** NAS Starter Utility > Config

LABEL	DESCRIPTION
Static IP	Select this if you want to assign the NSA a fixed IP address, subnet mask and default gateway.  <b>Note:</b> Do not configure an IP address that is already in use in your network. This results to a network IP address conflict and makes the NSA inaccessible.
Dynamic DNS	Domain Name System (DNS) is for mapping a domain name to its corresponding IP address and vice versa. Select this if the NSA is automatically given DNS information from the ISP or a DHCP server in your network.
Static DNS	If you were given specific IP address(es) of the DNS server(s), select this and enter the primary and secondary DNS in the corresponding fields.
Next	<b>Note:</b> This button shows when the hard disk in the NSA is uninitialized.  Click this to save your changes and go to the <b>Firmware Path</b> screen.
Apply	Click <b>Apply</b> to save your changes.  <b>Note:</b> The NSA does not need to restart when you change its IP address using the NAS Starter Utility, but please wait one minute for the change to take effect (after you click <b>Apply</b> ).
Cancel	Click this to return to the previous screen without saving.
PPPoE	Click this to check the current status of your PPPoE connection, enable or disable PPPoE and configure the PPPoE username and password as given by your ISP. If you use PPPoE to access the Internet, the NSA can be online when it turns on.

## 2.6.1 The Firmware Path Screen

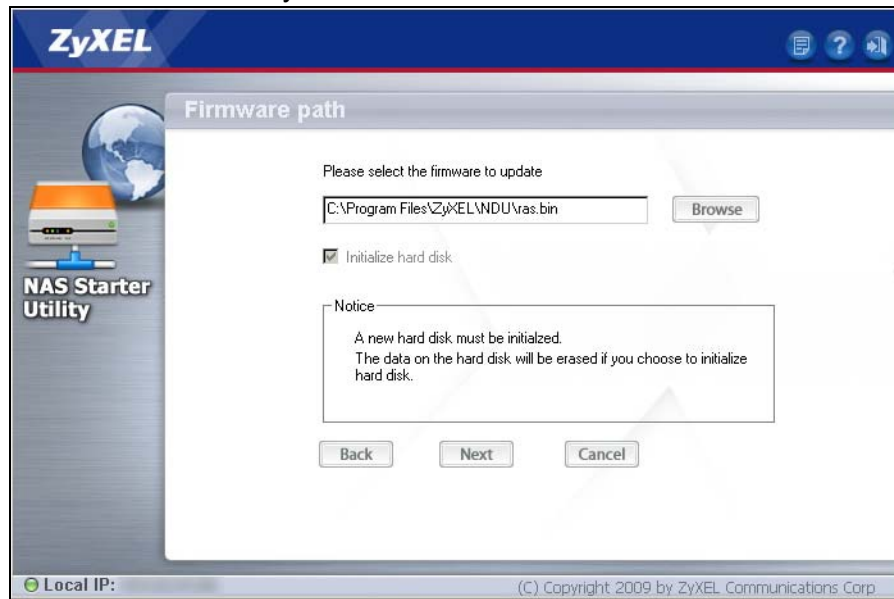
**Note:** Make sure you have installed the hard drive before configuring this screen.

Use this screen to initialize the hard disk and install the firmware. This screen only displays when the hard disk in the NSA is uninitialized. An uninitialized hard disk can be a new hard disk or a used hard disk that has a different format than the NSA or doesn't have the NSA firmware installed. The NSA needs to format the hard disk and install the firmware.



Click **Next** in the **Network Configuration** screen to initialize the hard disk and install the firmware.

**Figure 10** NAS Starter Utility > Firmware Path



The following table describes the labels in this screen.

**Table 4** NAS Starter Utility > Firmware Path

LABEL	DESCRIPTION
Browse	Click this and point to the location of the file provided by your administrator or that came on the CD-ROM.
Initialize hard disk	<p>This option is checked by default when the NAS Starter Utility detects that the hard drive does not have the firmware installed.</p> <p><b>Note:</b> The NSA formats the hard disk and installs the firmware. This deletes all existing data in the hard disk.</p> <p>Clear this if your hard disk has the NSA firmware installed and you want the NSA to retain the existing data in the hard disk. When you check this OR fail to clear this, you will lose all data in the hard disk even if the NSA recognizes the hard disk format and can retain all data.</p> <p><b>Note:</b> The checkbox can be checked or cleared only if the hard disk format is compatible with the NSA. If the hard disk format is not compatible with the NSA, this checkbox is checked by default and cannot be modified.</p>
Back	Click this to go back to the previous screen.
Next	Click this to go to the next screen to confirm your settings. The hard disk initialization and firmware installation starts. Please wait one minute for the process to finish. If the installation is successful, the NSA reboots.
Cancel	Click this to return to the previous screen without saving.



# Web Configurator Basics

## 3.1 Overview

This chapter describes how to access the NSA web configurator and provides an overview of its screens.

The web configurator is an HTML-based management interface that allows easy NSA setup and management using an Internet browser. Use Internet Explorer 5.0, Mozilla Firefox 1.03, Netscape Navigator 7.0 or later versions of these browsers. The recommended screen resolution is 1024 by 768 pixels or higher.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).

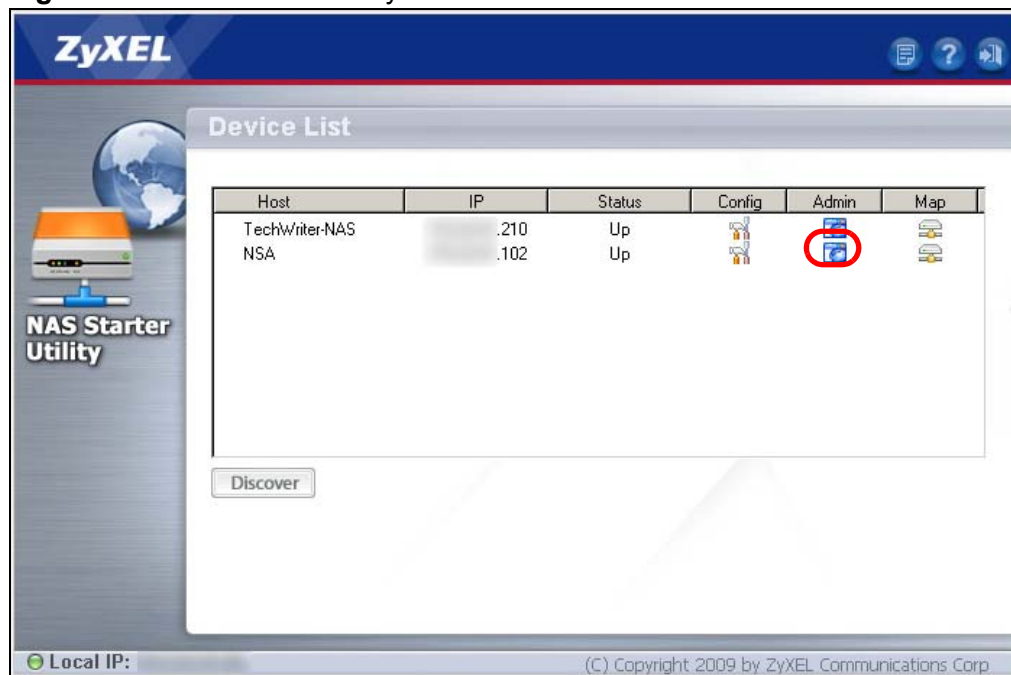
## 3.2 Accessing the NSA Web Configurator

Make sure your NSA is properly connected and that your computer is in the same subnet as the NSA (refer to the Quick Start Guide or the appendices).

### 3.2.1 Access the NSA Via NAS Starter Utility

If you don't know the IP address of the NSA, then use the NAS Starter Utility to find it. Refer to the Quick Start Guide for how to install and run the NAS Starter Utility. See [Chapter 2 on page 29](#) for more information on the NAS Starter Utility.

**Figure 11** NAS Starter Utility Main Screen



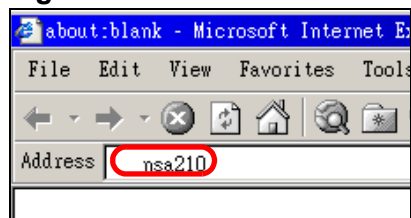
From the NAS Starter Utility main page click an icon under **Admin** to see the web configurator's login screen.

### 3.2.2 Web Browser Access

Note: You can access the NSA using your web browser only after the hard disk in the NSA has been "initialized" using the NAS Starter Utility (see [Chapter 2 on page 29](#)).

Configure the server name of your NSA using the **Network Configuration** screen ([Section 2.6 on page 34](#)) of the NAS Starter Utility. Open your browser and type in the server name of the NSA ("nsa210" by default).

**Figure 12** NSA URL



## 3.3 Login

The default username and password are 'admin' and '1234' respectively. Enter your username and password, then click **Login**. See [Chapter 12 on page 283](#) for how to create other user accounts.

**Figure 13** NSA Login Screen



The image shows the ZyXEL NSA login screen. At the top is a blue header with the 'ZyXEL' logo. Below the header, the text 'ZyXEL NSA' is centered. Underneath, it says 'Welcome to NSA' and 'Enter Username/password and click to login.' There are two input fields: 'Username:' with a smiley face icon and 'Password:' with a lock icon. Below the password field is a note in a yellow box: 'Note: Please turn on the Javascript and ActiveX control setting on Internet Explorer.' At the bottom are two buttons: 'Login' and 'Reset'.

You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

**Figure 14** Change Password Screen



The image shows the ZyXEL change password screen. At the top is a blue header with the 'ZyXEL' logo. Below the header, there is a padlock icon and the text 'Update Admin Info'. Underneath, it says 'As a security precaution, it is highly recommended that you change the admin password.' There are two input fields: 'New Password:' with a lock icon and 'Password (Confirm):' with a lock icon. Below the confirm field is a note in a yellow box: 'Note: (a maximum of 14 alphanumeric, printable characters, no single and double quotes)'. At the bottom are two buttons: 'Apply' and 'Ignore'.

## 3.4 User-level Screens Overview

All users (including the administrator) first see the user-level access **My NSA** screen after login.

**Figure 15** My NSA



Note: The web configurator management session automatically times out if it is left idle for 15 minutes. Simply log back into the NSA if this happens to you.

The icons and language label at the top-right of the screen ( **1** ) are visible from most screens. Use the tabs at the top of the screen to navigate between the user-level screens and menus. The following table describes the 'global' icons and tabs in the user-level screens.

**Table 5** User-level Global Labels and Icons

LABEL/ICON	DESCRIPTION
Language	Select the web configurator language from the drop-down list box.
Help	Click this to open a web help page specific to the screen you are currently configuring.
Logout	Click this at any time to exit the web configurator.
My NSA	Click this to go to screens where you can manage your shares and access the files on public shares. The administrator must go into the administration screens to manage other user's shares.
Password	Click this to go to a screen where you can change your password.

**Table 5** User-level Global Labels and Icons

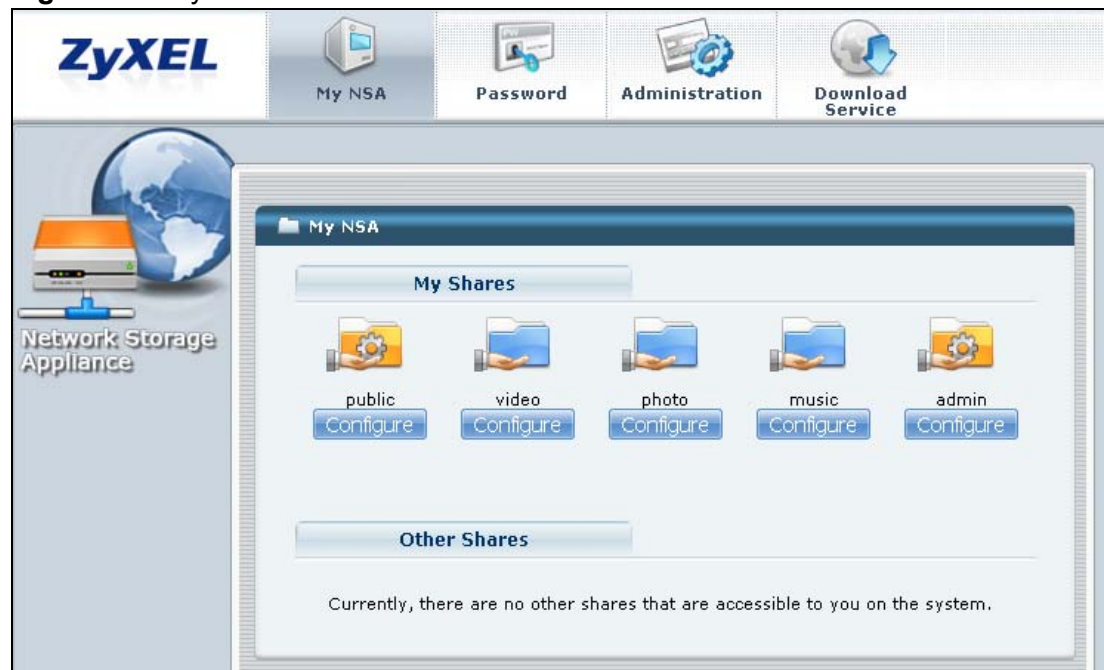
LABEL/ICON	DESCRIPTION
Administration	This tab displays when you log in as the administrator. Click this to go to screens where you can manage advanced configurations.
Download Service	This tab displays when you log in as the administrator. Click this to go to screens where you can have the NSA handle file downloads. See <a href="#">Section 9.11.2 on page 199</a> for more information.

## 3.5 My NSA Screens

Use the **My NSA** screens to manage your shares and access the files in folders to which you have access.




A share is a set of user access permissions for a specific folder on a volume (gives someone access to a folder). It is equivalent to the Windows concept of a shared folder, but the access rights are independent of the folder (you configure the share and the folder separately). You can map a share to a network drive for easy and familiar file transfer for Windows users.

The main **My NSA** screen displays the shares to which you have access.

**Figure 16** My NSA

The following table describes the labels in this screen.

**Table 6** My NSA

LABEL	DESCRIPTION
My Shares	<p>These are the shares that you own (and manage). The share icons are folder shaped. Click a share icon to access the share's contents.</p> <div data-bbox="565 415 646 489">  </div> <p>A plain share icon displays for a share on a volume on the internal hard drives.</p> <div data-bbox="565 548 646 621">  </div> <p>A USB symbol displays on the icon for a share on an external (USB) device. An external share's icon turns gray if the share is not currently available (because the USB device was removed for example).</p> <div data-bbox="565 680 646 753">  </div> <p>An orange icon displays a built-in system share created by the NSA.</p> <p>The administrator owns and manages the public shares.</p>
Configure	Click this to see and configure the management details for a share.
Other Shares	These are other shares on the internal hard drives or external (USB) devices that you can access (but not manage).

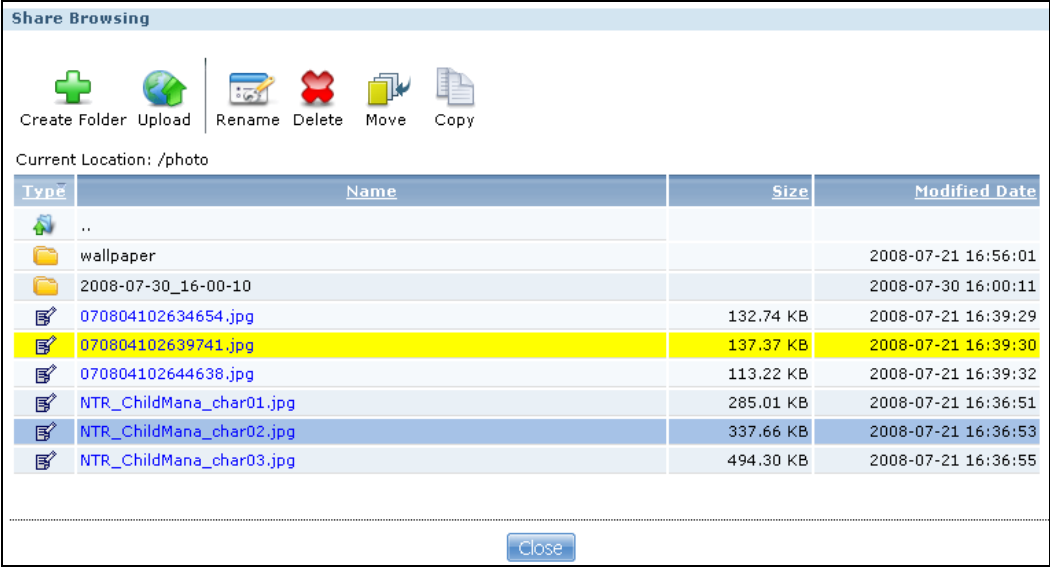
### 3.5.1 My NSA Share Browsing Screen

Click **My NSA** and then click a share to open the following screen. Use the **My NSA** share browsing screens to see and access share contents.

- Click a folder's name to go into the folder.
- Click a file's name to be able to save the file to your computer.
- Click the play icon to play the file. At the time of writing this is supported for MP3 files.
- Click to the right of a file or folder name to select it.
- Use the [SHIFT] key to select a range of entries. Hold down the [CTRL] key to select multiple individual entries.
- You can download up to a certain file size (per file) depending on the web browser you are using. If you are using Mozilla Firefox or Internet Explorer 7, you can download files up to 4 GB in size (per file). If you are using Internet Explorer 6, you can download files of up to 2 GB in size (per file).


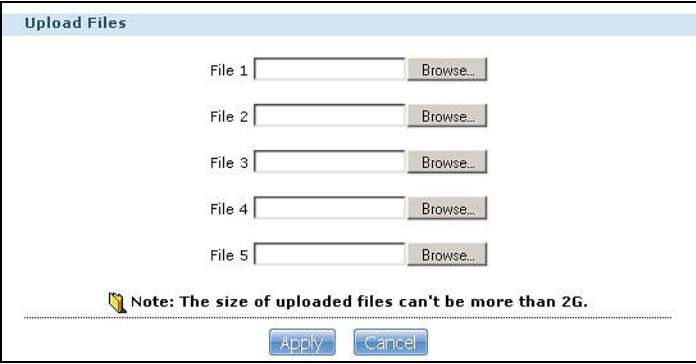


Figure 17 My NSA Share Browsing

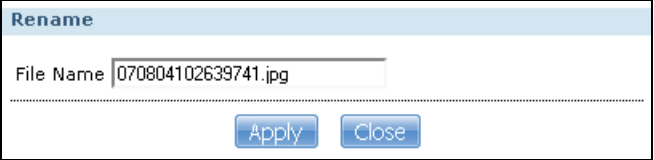



The following table describes the labels in this screen.

Table 7 My NSA Share Browsing

LABEL	DESCRIPTION
Create Folder	<p>Click this to open the following screen where you can create a new folder within the share.</p>  <p>Specify a name to identify the folder. See <a href="#">Section 3.5.5 on page 50</a> for more information on folder names. Click <b>Apply</b> to create a folder or click <b>Close</b> to exit this screen.</p>
Upload	<p>Click this to open the following screen where you can add files to the share.</p>  <p>Use the <b>Browse</b> button to locate your file/s and click <b>Apply</b> to upload the file. Click <b>Cancel</b> to close this screen.</p> <p>Note: Do not refresh the screen while an upload is going on.</p>

**Table 7** My NSA Share Browsing (continued)

LABEL	DESCRIPTION
Rename	<p>Select a folder or file and click this to open the <b>Rename</b> screen.</p>  <p>Enter the name you want and click <b>Apply</b> to make the changes. Click <b>Close</b> to exit this screen. See <a href="#">Section 3.5.5 on page 50</a> for more information on the number and types of characters you can use to name a folder or file.</p> <p><b>Note:</b> When you change a file name, make sure you keep the file extension unchanged.</p>
Delete	<p>Select a folder or file and click this to open the following warning screen.</p>  <p>Click <b>Yes</b> to delete the file, or click <b>No</b> to close the screen.</p>
Move	<p>Select a folder or file and click this to move it to another location within this share or another share that you can access. See <a href="#">Section 3.5.2 on page 47</a> for more details.</p>
Copy	<p>Select a folder or file and click this to create a copy of it in another location within this share or another share that you can access. See <a href="#">Section 3.5.2 on page 47</a> for more details.</p>
Current location	<p>This is the name of the share and folder path that you are in.</p>
Type	<p>The icon in this column identifies the entry as a folder or a file.</p> <p>The folder with an arrow pointing up is for the link that takes you to the next higher layer in the share's folder tree.</p>
Name	<p>This column identifies the names of folders and files in the share.</p> <p>Click <b>Up One Level</b> to go to the next higher layer in the share's folder tree.</p> <p>Click a file's file name to open the file or save it to your computer.</p> <p>Click a folder's name to display the folder's contents.</p>
Size	<p>This column displays a file's size in bytes.</p>

**Table 7** My NSA Share Browsing (continued)

LABEL	DESCRIPTION
Modified Date	This column displays the last time the file or folder was changed (in year-month-day hour:minute:second format).
Close	Click this to return to the <b>My NSA</b> screen.

### 3.5.2 My NSA Share Browsing Move or Copy Screen

Select a folder or file in the **My NSA** share browsing screens and click the **Move** button or the **COPY/SYNC** button to display a screen like the following. Use this screen to select the target path for moving or copying the folder or file.

**Figure 18** My NSA Share Browsing > Move (or Copy)

The following table describes the labels in this screen.

**Table 8** My NSA Share Browsing > Move (or Copy)

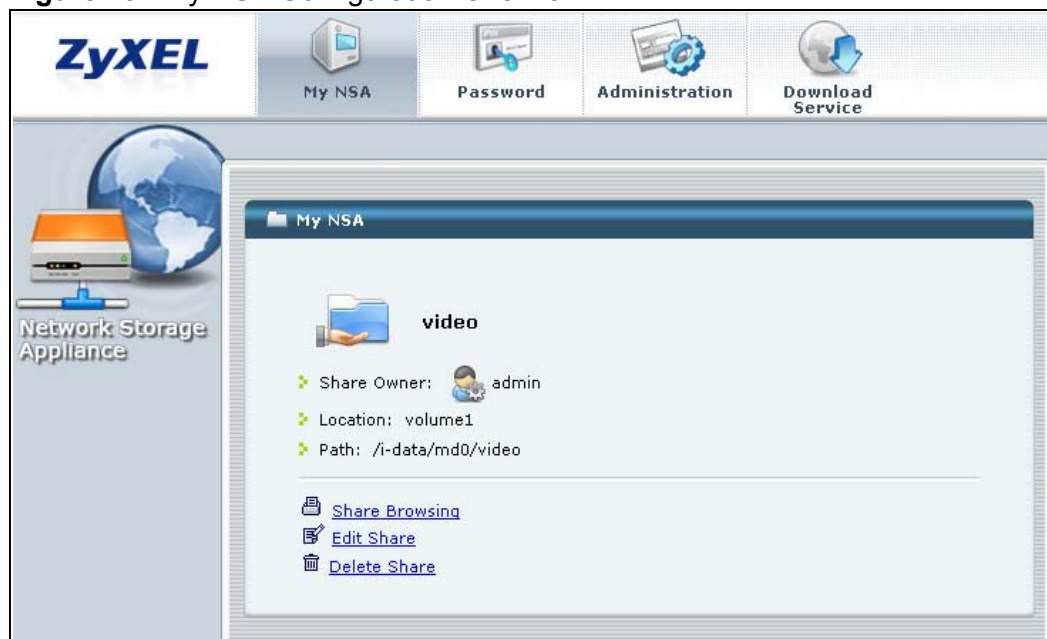
LABEL	DESCRIPTION
Shares	Select a target share from the drop-down list box.
Path	Select a folder on the NSA. You can also browse to find or create a folder on the NSA or type the location of the folder using forward slashes as branch separators.
Browse	<p>Click this to open the following screen where you can put the file in a specific folder.</p> <p>Select a folder and then click <b>Apply</b>. If you click <b>Apply</b> without selecting a folder, a forward slash displays in the <b>Path</b> field. All contents within the specified share are selected. Click <b>Cancel</b> to close this screen.</p>
Yes	Click this to move or copy the file.
Close	Click this to return to the <b>My NSA</b> share browsing screen without saving.

### 3.5.3 My NSA Configuration Screen

Use the **My NSA** configuration screens to see and configure share management details.

Click **My NSA** and then the **Configure** button of one of your shares to open the following screen. This screen displays a share's management details.

**Figure 19** My NSA Configuration Overview



The following table describes the labels in the this screen.

**Table 9** My NSA Management Overview

LABEL	DESCRIPTION
Share Owner	The share belongs to (and is managed by) this user account. The share owner controls access rights to the share.
Location	The share is for a folder on this volume.
Path	This is the share's file path.
Share Browsing	Click this to see and access the share's contents.
Edit Share	Click this to configure the share's management details.
Delete Share	Click this to permanently remove the contents associated with this share or to disable the share so that no users can access it.

### 3.5.4 My NSA Edit Share Screen

Use this screen to configure share management details.

Click **My NSA** and a share's **Configure** button. Then click **Edit Share** to open the following screen. This screen displays a share's management details.

**Figure 20** My NSA > Edit Share

The following table describes the labels in the this screen.

**Table 10** My NSA > Edit Share

LABEL	DESCRIPTION
Share Name	Configure a name to identify this share. Type a share name from 1 to 239 single-byte (no Chinese characters allowed for example) ASCII characters. The name cannot be the same as another existing local share. See <a href="#">Section 3.5.5 on page 50</a> for more information on share names.
Volume	You should have already created volumes (a single accessible storage area with a single file system) on the NSA.  Select the volume that you want to use with this share.
Make this share owned by	Select the administrator or user account that is to own (manage) this share. The share owner controls access rights to the share.
Enable This Share	Select this option to allow users to access this share. When this option is not selected, you cannot see and access this share.
Enable Recycle Bin	Select this option to keep deleted items in a recycle bin. When you delete an item, a recycle folder is created within the share, and the deleted item is stored in the recycle bin. Later if you want to retrieve a deleted item, you can select the item from the recycle folder and move/copy the item to another share.
Publish this share to Media Server	Select this option to make the share's files available to media clients.
Publish this share to Web	Select this option to let people use a web browser to access this share's files without logging into the My NSA screens.

**Table 10** My NSA > Edit Share (continued)

LABEL	DESCRIPTION
Share Access	<p>Select who can access the files in the share and how much access they are to be given. If you publish the share to the media server or the web, all users will have at least read-only access to the share, regardless of what you configure here.</p> <p>Select <b>Keep it private to owner</b> to allow only the share owner to read files in the share, delete files in the share and save files to the share.</p> <p>Select <b>Make it public</b> to allow anyone (with or without a user account on the NSA) to read files in the share, delete files in the share and save files to the share.</p> <p>Select <b>Advanced</b> to select which individual users can read the share's files, which users can delete the share's files, and which users are blocked from doing either.</p>
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

### 3.5.5 Share and Folder Names

The name can only contain the following characters:

- Alphanumeric (A-z, 0-9) and Unicode.

The NSA allows FTP access to shares, folders or files with names encoded in the UTF-8 (8-bit UCS/Unicode Transformation Format) format. So your FTP client must support UTF-8 in order to access shares, folders or files on the NSA with Unicode names.

- Spaces
- \_ [underscores]
- . [periods]
- - [dashes]

Other limitations include:

- All leading and trailing spaces are removed automatically.
- Multiple spaces within names are converted to a single space.
- Share names must be unique (they cannot be the same as other share names).
- The NSA creates automatic volume names for external (USB) disk volumes. These are a type of share, so the share name you configure cannot conflict with the external (USB) disk volume names. "ExtVol1" or "ExtVol2" are examples of external (USB) disk volume names.
- Folder names must be unique (they cannot be the same as other folder names).
- The minimum character length of a name is one character, that is a name cannot be blank.
- The maximum character length of share name is 239 characters.

- Unicode is supported for share names, although your FTP client must support UTF-8. Full support should be available in all Windows versions after Windows 2000.

### 3.5.6 Password Screen

Click **Password** to open the following screen. Use this screen to change an account's password. Enter a new password and confirm it by re-entering it.

**Figure 21** Password

The following table describes the labels in this screen.

**Table 11** Password

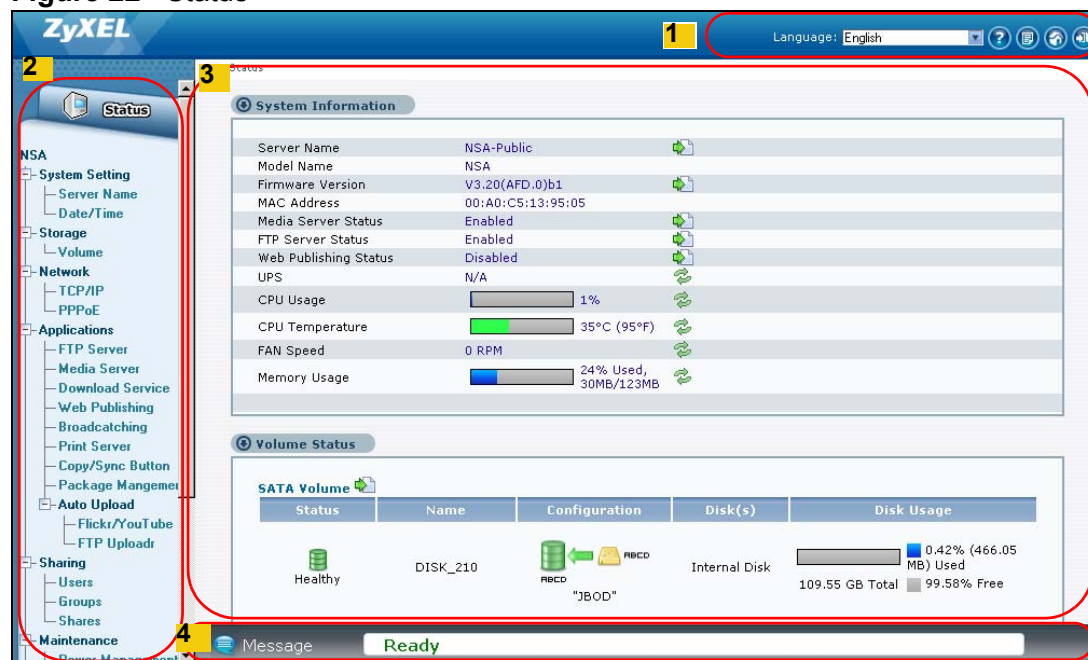
LABEL	DESCRIPTION
Account Name	Type the user name of the account for which you want to change the password.
Old Password	Type the user's current password.
New Password	Create a new password for the user. You can type from one to 14 single-byte (no Chinese characters allowed for example) ASCII characters.
Password (Confirm)	You must type the exact same password that you just typed in the above field.
Apply	Click this to save your changes.
Reset	Click this to refresh the screen.

## 3.6 Administration Screens

The **Administration** tab displays when you log in as the administrator. Click **Administration** in the **My NSA** screens to open the advanced administration screens.

The **Status** screen is the first advanced administration screen that displays.



**Figure 22** Status



### 3.6.1 Global Administration Icons



The icons and language label at the top-right of the screen ( **1** ) are visible from most of the administration screens. The following table describes the 'global' icons and labels.

**Table 12** Global Labels and Icons

LABEL/ICON	DESCRIPTION
Language	Select the web configurator language from the drop-down list box.
	<b>Help</b> Click this to open a web help page specific to the screen you are currently configuring.
	<b>About</b> Click this to view the model name, firmware version and copyright.



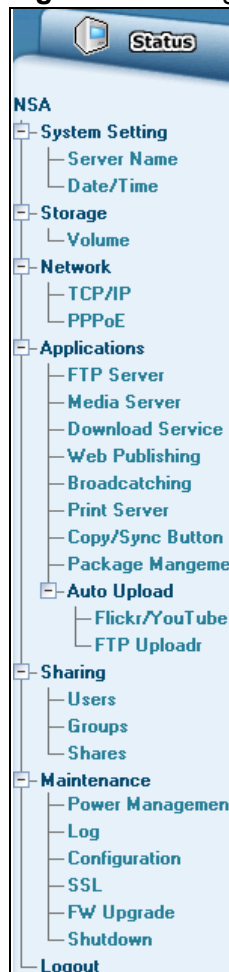
**Table 12** Global Labels and Icons

LABEL/ ICON	DESCRIPTION
	<b>Home</b> Click this to return to the user-level screens.
	<b>Logout</b> Click this at any time to exit the web configurator. This is the same as clicking the <b>Logout</b> link at the bottom of the Navigation panel.

## 3.6.2 Navigation Panel

The navigation panel on the left of the screen ( **2** ) contains screen links. Click a link to display sub-links. There are no sub-links for the **Status** screen. Certain screens also contain hyper links that allow you to jump to another screen.

The following screen shows the features listed in the navigation panel.

**Figure 23** Navigation Panel Links

The following table describes the navigation panel screens.


**Table 13** Screens Summary

LINK	SCREEN	FUNCTION
Status		This screen shows system information, the status of the volumes, and the users who are currently using the NSA.
System Setting	Server Name	Specify the NSA's server name and workgroup name.
	Date & Time	Chose a time zone and/or allow the NSA to synchronize with a time server.
Storage	Volume	View volume and disk information and create and edit volumes. A volume is a storage area that can span one or more internal disks or a single external (USB) disk.
Network	TCP/IP	Assign the NSA a dynamic or static IP address and DNS information.
	PPPoE	Configure PPPoE settings for a direct Internet connection.
Applications	FTP Server	Enable FTP file transfer to/from the NSA, set the number of FTP connections allowed, an FTP idle timeout, and the character set.
	Media Server	Enable or disable the sharing of media files and select which shares to share.
	Download Service	Have the NSA handle large file downloads.
	Web Publishing	Let people use a web browser to access files in shares without logging into the My NSA screens.
	Broadcatching	Subscribe the NSA to feeds to download frequently updated digital content like TV programs, radio talk shows, Podcasts (audio files), YouTube videos, or even BitTorrents.
	Print Server	View and manage the NSA's list of printers and print jobs.
	COPY/SYNC Button	Copy or synchronize files between a USB device and the NSA.
	Package Management	Set up more useful applications in your NSA. The NSA can download multiple packages/files at once and automatically goes through all the installation steps.
	Auto Upload - Flickr/YouTube	Upload files in selected shares to your Flickr and/or YouTube accounts.
	Auto Upload - FTP Uploadr	Upload files in selected shares to FTP servers.
Sharing	Users	View, create and edit administrator and user accounts to let people use the NSA.
	Groups	View, create and edit groups. Groups allow you to organize users into specific groups. You can create shares accessible only by the group members.
	Shares	View, create and edit shares. Shares are shared folders to which you can allow specific users read/write access rights.

**Table 13** Screens Summary (continued)


LINK	SCREEN	FUNCTION
Maintenance	Power Management	Configure power saving settings for the NSA and have the NSA turn itself off and on or reboot according to the schedules you configure.
	Log	View the NSA's logs and configure how you want to receive the log reports.
	Configuration	Back up and/or restore the NSA configuration file.
	SSL	Configure HTTPS and the NSA's SSL certificate.
	FW Upgrade	Upload/upgrade new firmware to your NSA.
	Shutdown	Restart the NSA or shut it down.
Logout		Click this to exit the web configurator. This is recommended to prevent unauthorized administrator access to the NSA.

### 3.6.3 Main Window

The main window (  ) shows the screen you select in the navigation panel. It is discussed in the rest of this document.

The **Status** screen is the first administration screen to display. See [Chapter 5 on page 135](#) for more information about the **Status** screen.




### 3.6.4 Status Messages

The message text box at the bottom of the screen (  ) displays status messages as you configure the NSA.












### 3.6.5 Common Screen Icons

The following table explains some icons that appear in several configuration screens.

**Table 14** Common Configuration Screen Icons

ICON	DESCRIPTION
	<b>Edit</b> Click this to go to a screen where you can change the configuration settings of an entry.
	<b>Delete</b> Click this to delete an entry from the list.
	<b>Edit</b> Click this to jump to related item's configuration screen.

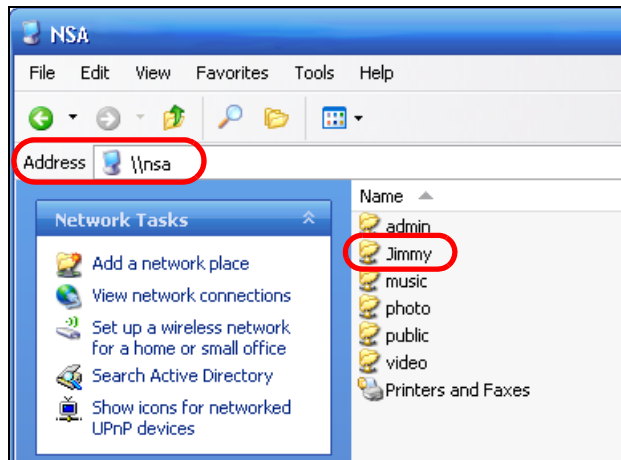
**Table 14** Common Configuration Screen Icons (continued)

ICON	DESCRIPTION
	<b>Refresh</b> Click this to refresh the data for the field or value with which it is associated.
	<b>User</b> See the chapter on user accounts for detailed information on variants of this icon.
	<b>Share</b> See the chapter on shares for detailed information on variants of this icon.
	<b>Healthy</b> This represents a healthy volume.
	<b>Degraded</b> This represents a degraded RAID 1 volume. Replace the faulty disk. If the replacement disk does not contain any partition, the NSA automatically restores the volume. If the replacement disk already contains a volume, you need to delete the volume and then click the <b>Repair</b> icon to fix the degraded RAID volume.
	<b>Down</b> This represents a down volume.
	<b>Scan Disk</b> Click this to scan a hard disk for file system errors.
	<b>Eject</b> Click this before you remove an external hard drive so that you do not lose data that is being transferred to or from that hard drive.
	<b>Locate</b> Click this to cause the LED on the external storage device to blink.
	<b>Repair</b> If you replace a faulty disk with a disk that contains a volume, you need to delete the volume and then click this to fix the degraded RAID volume.
	<b>Migrate</b> Click this to move data in a JBOD hard disk to a RAID 1 hard disk.

### 3.6.6 Session Example (Windows)

Open Windows Explorer and type two back slashes followed by the NSA name or IP address. Initially you can only read and write to the **Public**, **Video**, **Music**, and

**Photo** folders until you create other shares on the NSA. This session is then displayed as shown in the following figure.





# Tutorials

## 4.1 Overview

This chapter provides tutorials that show how to use the NSA.

- [Creating a Volume](#), see [page 59](#)
- [Deleting a Volume](#), see [page 66](#)
- [File Sharing Tutorials](#), see [page 67](#)
- [Download Service Tutorial](#), see [page 77](#)
- [Broadcatching Tutorial](#), see [page 93](#)
- [Copy and Flickr Auto Upload Tutorial](#), see [page 98](#)
- [FTP Uploadr Tutorial](#), see [page 99](#)
- [Web Configurator's Security Sessions](#), see [page 104](#)
- [Using FTPES to Connect to the NSA](#), see [page 116](#)
- [Using a Mac to Access the NSA](#), see [page 117](#)
- [How to Use BackupPlanner](#), see [page 120](#)

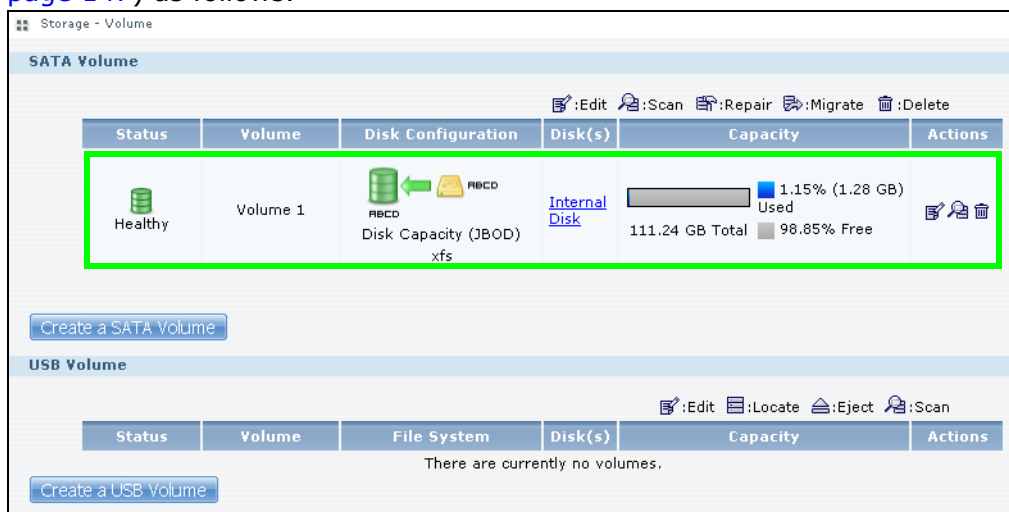
## 4.2 Creating a Volume

This section shows you how to create a volume on your NSA.

**Creating a volume deletes all existing data in the SATA or eSATA hard disk. Make sure you have a backup of your existing data before following the steps in this section.**

Your NSA has a single bay for a SATA (Serial Advanced Technology Attachment) hard disk. The firmware installed during hard disk initialization ([Chapter 2 on page 29](#)) automatically creates a JBOD volume on your SATA hard disk. JBOD is the default storage method if you are using a single hard disk for your NSA.

This JBOD volume shows up in the **Storage > Volume** screen ([Section 7.4 on page 147](#)) as follows.



When you attach an eSATA hard disk to your NSA, you can configure this volume as: 1) a backup to your SATA hard disk (**RAID 1**); or 2) as a separate storage drive (either another **JBOD** or a **PC Compatible Volume**).

## 4.2.1 Creating a RAID 1 Volume

This storage method allows recovery of data if your hard disk fails. To create a RAID 1 volume, you must connect an eSATA hard disk to your NSA. There are two ways to create a RAID 1 volume:

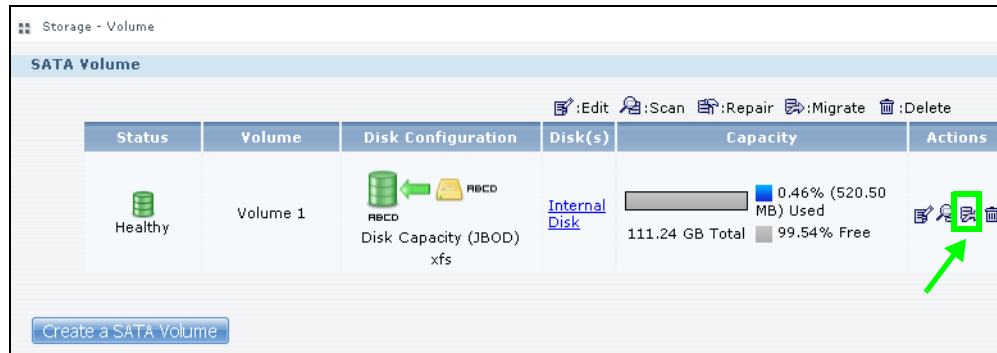
- Click the **Migrate** button - This is a quick way to create a RAID 1 volume. Use this to automatically synchronize data in the internal hard disk to the eSATA hard disk.
- Click the **Create a SATA volume** button - Use this if there are no existing volumes in your NSA.

## 4.2.2 Migrate Button

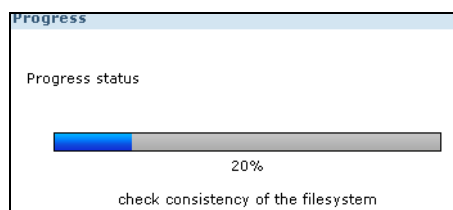
Do the following steps to create a RAID 1 volume.

- 1 Once you attach the eSATA hard disk to the NSA, the **Storage > Volume** screen shows the **Migrate** button.





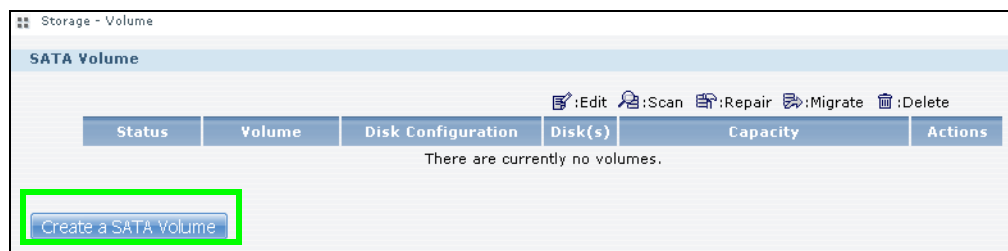
- 2 Click the **Migrate** button and you can see the following progress bar. Wait for up to 10 minutes for the RAID 1 volume to be created.



### 4.2.3 Create a SATA Volume Button

If you do not have an existing volume in the **Storage > Volume** screen, do the following steps to create a RAID 1 volume.

- 1 In the **Storage > Volume** screen, click **Create a SATA Volume**.



- 2 In the **Disk Configuration** screen, you can select the storage method.
  - Type in the **Volume Name** for your RAID 1 volume. The volume name can be 1 to 31 characters (a-z, 0-9, " " [spaces], "\_", and ".").
  - Choose **RAID 1** and click **Apply**.

**This deletes all existing data in the eSATA hard disk. Make sure you have a backup of any existing data in the hard disk.**

**Disk Configuration**

Volume Name

**JBOD** ABCD

A JBOD volume can be a single disk volume or can be made to span across several disks into a single larger volume. It does not provide any fault tolerance or performance benefits.

Volume will be created on ☒ Internal Disk ☐ External Disk

**PC Compatible Volume** ABCD

A primary partition will be created on the disk. It can be accessed by a PC if this disk is connected to a PC which supports the selected file system.

Volume will be created on ☒ External Disk File System

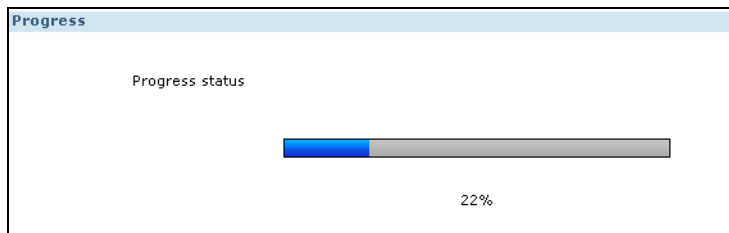
**RAID1** ABCD

Provides disk mirroring. Level 1 provides twice the read transaction rate of single disks and the same write transaction rate as single disks.

Volume will be created on ☒ Internal Disk ☒ External Disk

**Note:**  
When internal disk defect in RAID1 mode, NSA210 will be in "uninitialized" state. You can bring NSA210 to normal state by switching external disk to internal disk. After login WEB GUI, you can repair the degraded RAID1 by another external disk.

The NSA starts creating the volume and you can see the following progress bar. Wait for 2 minutes for the RAID 1 volume to be created.



3 The **Storage > Volume** screen displays with your RAID 1 volume.

**SATA Volume**

[Edit](#) [Scan](#) [Repair](#) [Migrate](#) [Delete](#)

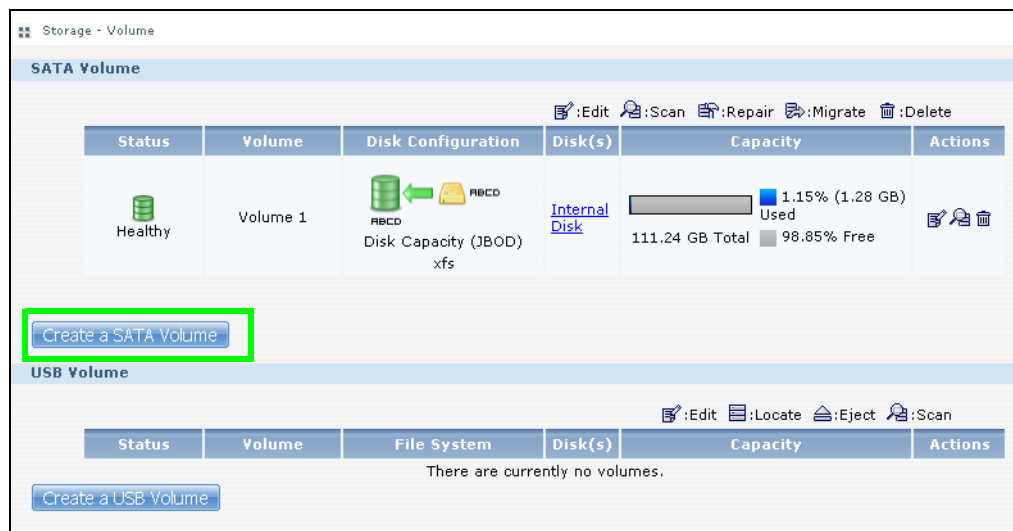
Status	Volume	Disk Configuration	Disk(s)	Capacity	Actions
Resync 0.1%	RAID1_Example	 Data Protection (RAID1) xfs	<a href="#">Internal Disk</a> <a href="#">External Disk</a>	<div style="width: 0.46%; height: 10px; background-color: blue;"></div> 0.46% (520.44 MB) Used 111.24 GB Total 99.54% Free	<a href="#">Edit</a> <a href="#">Scan</a> <a href="#">Repair</a> <a href="#">Migrate</a> <a href="#">Delete</a>

**Note:**  
When internal disk becomes defective while in RAID1 mode, the NSA210 will be in "uninitialized" state. You can bring the NSA210 to its normal state by using the external disk as the new internal disk. After login WEB GUI, you can repair the degraded RAID1 by another external disk.

## 4.2.4 Creating a PC Compatible Volume

You can use your eSATA hard disk as a separate storage volume. The following section shows you how to create a **PC Compatible Volume**. Use this storage method if you have an eSATA hard disk that will be connected to a Windows computer when it is not connected to the NSA. However, the computer's platform (for example, Windows XP SP2) should support the file system you selected for the eSATA hard disk.

- 1 Connect the eSATA hard disk to your NSA and go to the **Storage > Volume** screen. Click **Create a SATA Volume**.





- 2 In the **Disk Configuration** screen, you can select the storage method.
  - Type in the **Volume Name** for your PC Compatible volume. The volume name can be 1 to 31 characters (a-z, 0-9, " " [spaces], "\_", and ".").
  - Choose **PC Compatible Volume**.
  - Select the **File System** you want to use (**NTFS** in this example). Make sure this file system is supported by the Windows platform you are using in your computer. Refer to [Section 7.5.6 on page 157](#) for file systems supported by your NSA. Click **Apply**.


**This deletes all existing data in the eSATA hard disk. Make sure you have a backup of any existing data in the hard disk.**

**Disk Configuration**

Volume Name

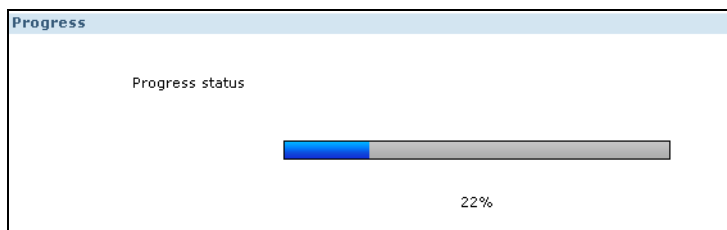
**JBOD** ABCD  
  
 A JBOD volume can be a single disk volume or can be made to span across several disks into a single larger volume. It does not provide any fault tolerance or performance benefits.  
 Volume will be created on ☐ Internal Disk ☐ External Disk

**PC Compatible Volume** ABCD  
  
 A primary partition will be created on the disk. It can be accessed by a PC if this disk is connected to a PC which supports the selected file system.  
 Volume will be created on ☒ External Disk File System

**RAID1** ABCD  
  
 Provides disk mirroring. Level 1 provides twice the read transaction rate of single disks and the same write transaction rate as single disks.  
 Volume will be created on ☒ Internal Disk ☒ External Disk

**Note:**  
 When internal disk defect in RAID1 mode, NSA210 will be in "uninitialized" state. You can bring NSA210 to normal state by switching external disk to internal disk. After login WEB GUI, you can repair the degraded RAID1 by another external disk.






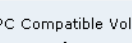




The NSA starts creating the volume and you can see the following progress bar. Wait for 2 minutes for the volume to be created.



### 3 The **Storage > Volume** screen displays with your **PC Compatible Volume**.

**SATA Volume**

[Edit](#) [Scan](#) [Repair](#) [Migrate](#) [Delete](#)

Status	Volume	Disk Configuration	Disk(s)	Capacity	Actions
Healthy	DISK	 Disk Capacity (JBOD) ext3	<a href="#">Internal Disk</a>	 0.63% (706.91 MB) Used 109.55 GB Total 99.37% Free	  
Healthy	Volume 2	 PC Compatible Volume fat32	<a href="#">External Disk</a>	 0% (64.00 KB) Used 76.68 GB Total 100.00% Free	  

### 4.2.4.1 Checking Your PC Compatible Volume

The files in the eSATA hard disk that you configured as a **PC Compatible Volume** should be accessible when you connect the eSATA hard disk to your computer.

You can configure the features of your NSA to save files to your eSATA hard disk. For example, you can refer to [Section 4.6 on page 93](#) to use the **Broadcatching** feature of your NSA to download files to your eSATA disk.

- 1 When asked for the **Location of Downloaded Files**, make sure you save the completed files to the eSATA hard disk (**Volume 2** in this example).

The screenshot shows the 'Settings' window with the following configuration:

- Channel Name: http://www.gcast.com/u/bluer...
- URL: http://www.gcast.com/u/blueritz/main.xml
- Download Policy: Download Only New Items
- Delete Policy: Manual
- Location of Downloaded Files: Put incomplete downloads in admin /download; Move completed downloads to Volume 2 /

The 'Move completed downloads to' row is highlighted with a green box. Buttons at the bottom include Edit, Apply, Reset, and Cancel.

- 2 The files downloaded by the NSA should be in the **Volume 2** folder. You can check this when you access the **Volume 2** folder from **My NSA > Share Browser** screen as follows.

The screenshot shows the 'Share Browsing' window with the following details:

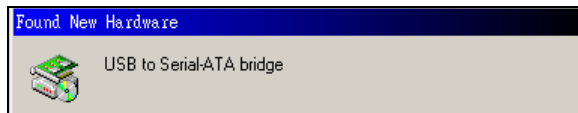
- Current Location: /Volume 2/C&D Top 10 Podcast (highlighted with a green box)
- Table of files:

Type	Name	Size	Modified Date
..	..		
Audio	01_May_21_2009_Thursday_Part_2.mp3	5.57 MB	2009-06-19 14:55:38
Audio	01_May_21_2009_Thursday_Part_1.mp3	9.20 MB	2009-06-19 14:53:14
Audio	01_May_20_2009_Wednesday_Part_4.mp3	4.93 MB	2009-06-19 14:53:51
Audio	01_May_20_2009_Wednesday_Part_3.mp3	6.39 MB	2009-06-19 14:53:38
Audio	01_May_20_2009_Wednesday_Part_2.mp3	5.14 MB	2009-06-19 14:53:26
Audio	01_May_20_2009_Wednesday_Part_1.mp3	6.35 MB	2009-06-19 14:54:35
Audio	01_May_19_2009_Tuesday_Part_4.mp3	7.91 MB	2009-06-19 14:54:26
Audio	01_May_19_2009_Tuesday_Part_3.mp3	6.93 MB	2009-06-19 14:54:15
Audio	01_May_19_2009_Tuesday_Part_2.mp3	6.43 MB	2009-06-19 14:54:11
Audio	01_May_19_2009_Tuesday_Part_1.mp3	7.37 MB	2009-06-19 14:54:02

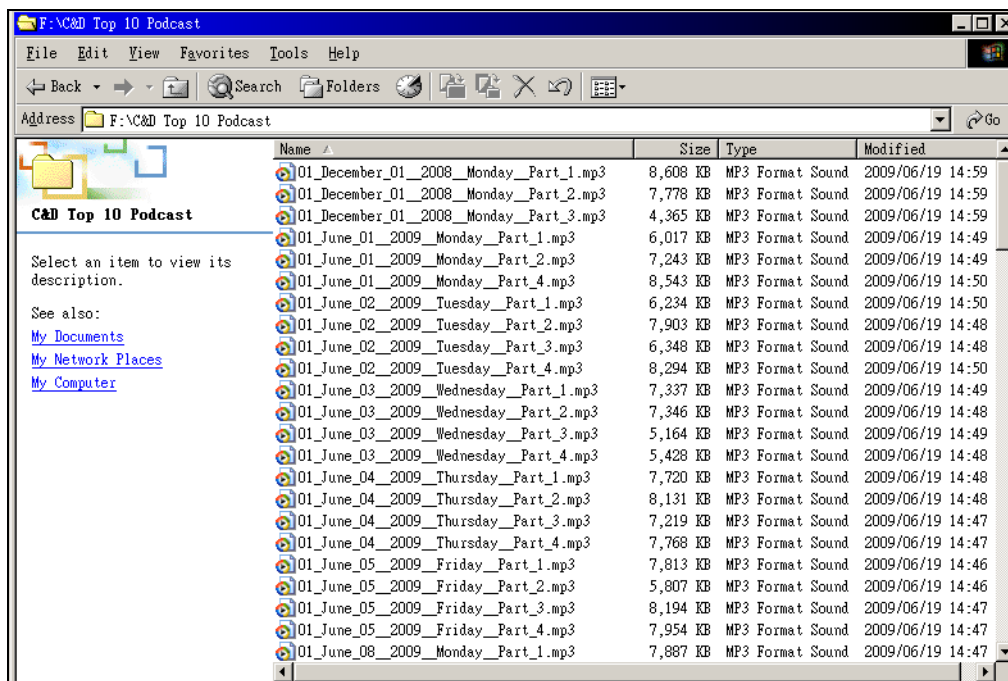
Page 1 Of 2    Next →

Close

- 3 Disconnect the eSATA hard disk from the NSA. Connect the eSATA hard disk to your computer. On some systems, you can see the following notification.



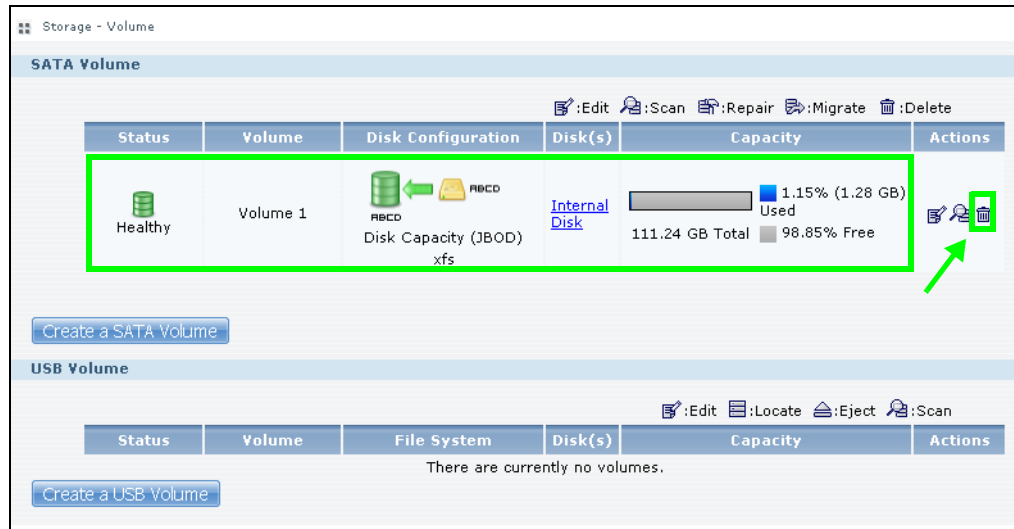
- 4 The computer assigns a letter to the eSATA hard disk (drive F in this example) that is accessible from the **My Computer** screen. Double click the eSATA drive and check your files. They should be the same files that are in the **My NSA > Share Browser** screen.



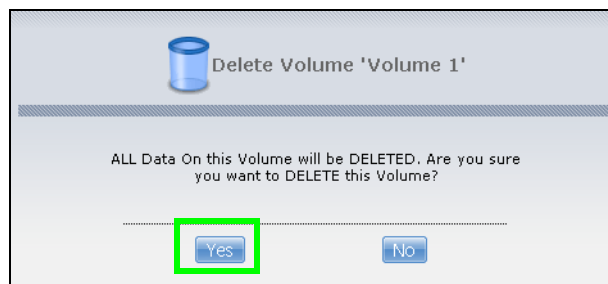
## 4.3 Deleting a Volume

Delete an existing volume in your NSA by doing the following steps.

- 1 In the **Storage > Volume** screen, select the volume you want to delete and click the delete icon.



- 2 A confirmation window appears as follows. Click **Yes**.



**This deletes all existing data in the volume. Make sure you have a backup of any existing data in the hard disk.**

## 4.4 File Sharing Tutorials

The following sections cover using the NSA for file sharing. This chapter assumes you have already followed the Quick Start Guide instructions to perform initial setup and configuration (so you have a working volume). See the rest of this User's Guide for details on configuring the NSA's various screens.

### 4.4.1 Creating a User Account

Bob wants to create accounts for his sons Jimmy and Kevin. This is how he would do it.

- 1 Log into the NSA web configurator (see [Section 3.3 on page 41](#)) and click **Administration** to go to the configuration screens.



- 2 Click **Sharing > Users** to open the **Users** screen. Then click **Add User**.





- 3 Configure the screen as follows and write down the username and password to give to Jimmy. If the username and password are the same as Jimmy's Windows login, Jimmy will not need to enter a username and password when he logs into his share from his computer. Set the **Account Type** to **User** so Jimmy doesn't get to configure the whole NSA. Click **Apply** to create the account.

**Add User**

Username: Jimmy

New Password: xxxx

Password (Confirm): xxxx

Account Type: ☒ Administrator ☒ User

**Available Group(s)**

- children
- family

**Group Membership**




Group Membership: (empty list)

Buttons: Add Selected Group(s) →, ← Remove Selected Group(s)

Buttons: Apply, Cancel

- 4 The account now displays in the **Users** screen.

Page 1 Of 1

User Type	Username
	Bob
	Jimmy
	admin

Page 1 Of 1

Now that Bob has created Jimmy's account, he can go through the steps again to create another account for Kevin. After both accounts are created, he can go to [Section 4.4.2 on page 70](#) to create shares for Jimmy and Kevin.

## 4.4.2 Creating a Share

Suppose Bob has already created separate accounts for his sons Jimmy and Kevin. Now Bob wants to create a share for each son. He also wants to make sure that each son can only access his own share (to keep them from deleting each other's files). This is how he would do it.

- 1 In the NSA's administration web configurator screens, click **Shares > Add Share**. Click **Add Share** to create a new share.



- 2 Specify a name for the share and select which volume it should be on. Configure the screen as follows. Then click **Edit**.

**Add Share**

Share Name:

Volume:

Make this share owned by:

☒ Enable This Share

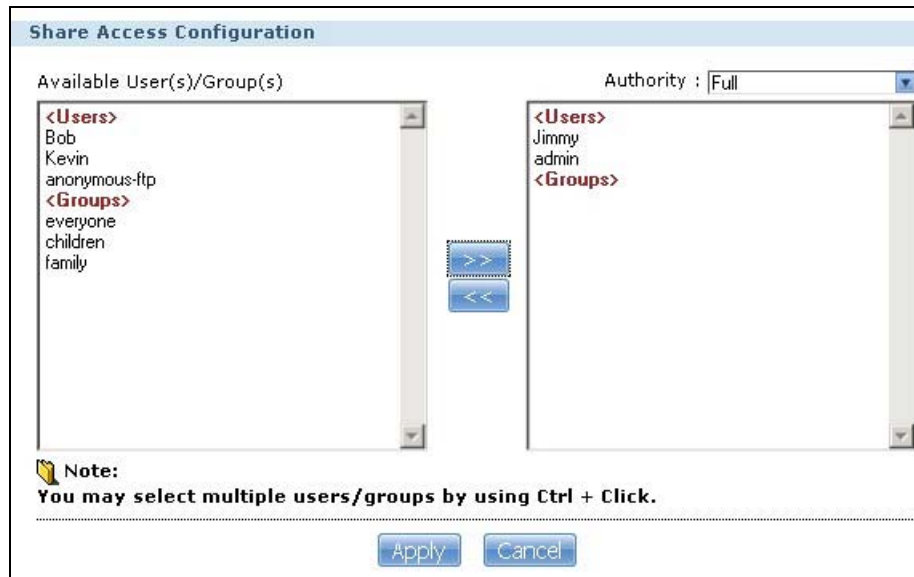
☒ Enable Recycle Bin

☐ Publish this share to Media Server

☐ Publish this share to Web

Share Access:

- 3 Configure the screen as follows to give Jimmy full access right to the share. Then click **Apply** to create the share.



Now that Bob has created Jimmy's share, he can go through the steps again to create another share for Kevin.

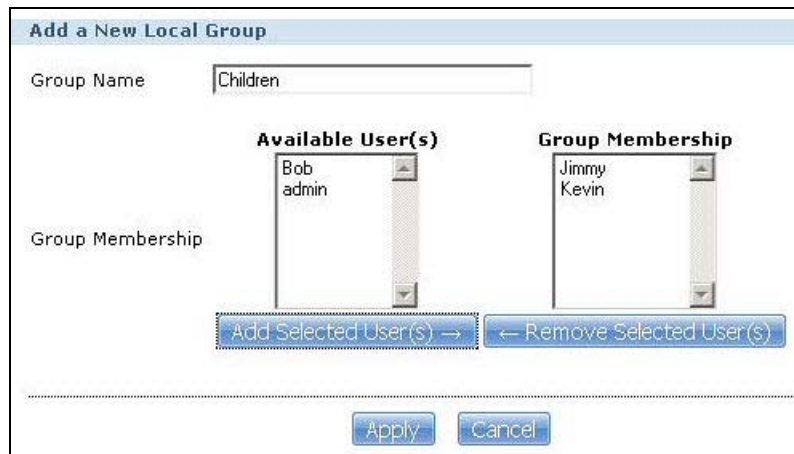
### 4.4.3 Creating a Group

After creating user accounts for Jimmy and Kevin, Bob wants to create a group for his sons and another one for the parents. Bob can assign access rights to his sons' group for certain shares such as a cartoons share and allow only the parents' group to access the scary movie share. This is how he would create the group.

- 1 In the NSA's administration web configurator screen, click **Groups > Add Group**.



- 2 Specify a name for the group. Select the user(s) you want to add to the group from the **Available User(s)** list and click **Add Selected User(s)**. Configure the screen as follows. Then click **Apply** to create the group.

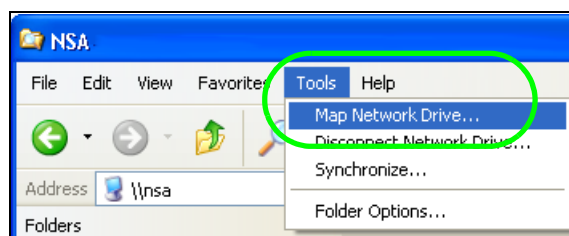


Now that Bob has created a group for Jimmy and Kevin, he can go through the steps again to create another group for the parents. Then he can see the rest of the tutorials for how to use the groups in assigning access rights to shares.

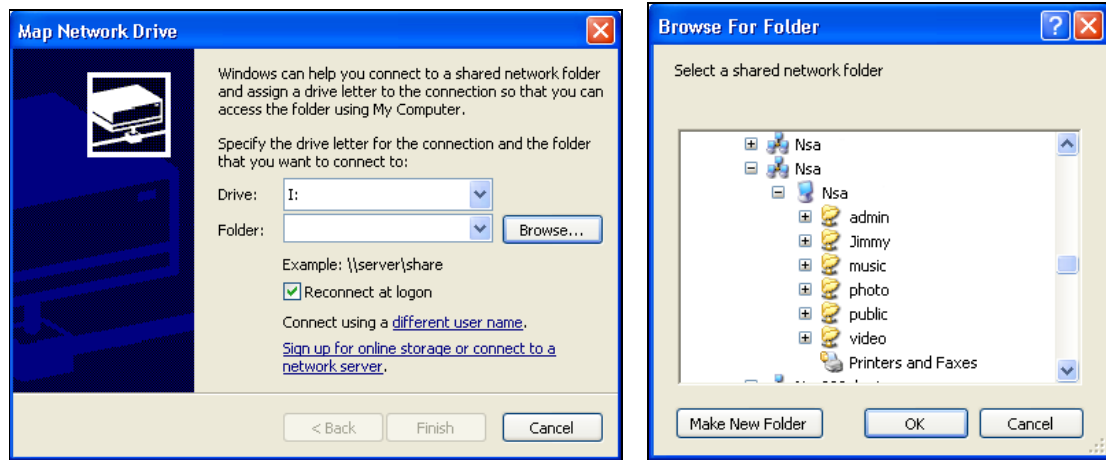
#### 4.4.4 Accessing a Share From Windows Explorer

If you map a NSA share (where data is stored) to a Windows network drive, you can use Windows Explorer to transfer files to and from the NSA as if it was another folder on your computer. Here he maps Jimmy's share to Jimmy's computer.

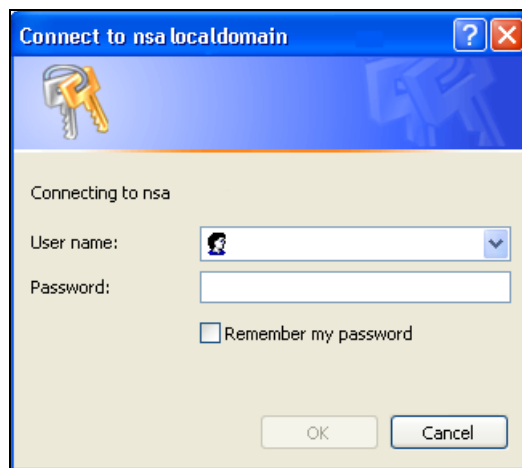
- 1 Start Windows Explorer and go to the NSA's server name ("nsa210" is the default) or IP address.
- 2 Click **Tools > Map Network Drive**.



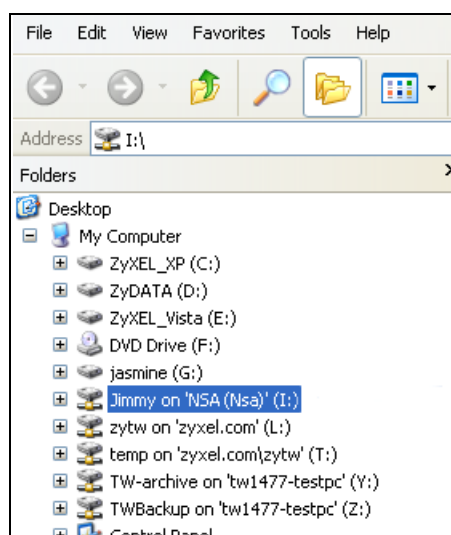
- 3 Select the network drive that you want to map the NSA to from the **Drive** list box. This example uses **I**. Then browse to and select the share on the NSA. Click **Finish**.



- 4 Enter the username and password for Jimmy's account and click **OK**. You do not need to do this if the username and password are the same as Jimmy's Windows login.



- 5 After the mapping is done, you can then simply copy and paste or drag and drop files from/to your local computer's drives to or from this network folder. Just like the NSA's share was another folder on your computer.

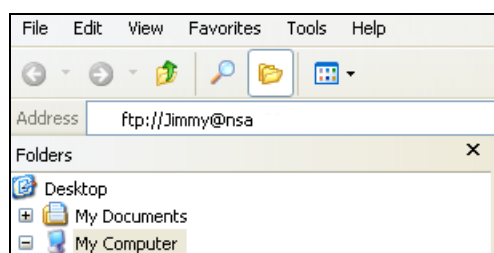


Now that Bob has mapped Jimmy's share to Jimmy's computer, he can go through the steps again to map Kevin's share to Kevin's computer.

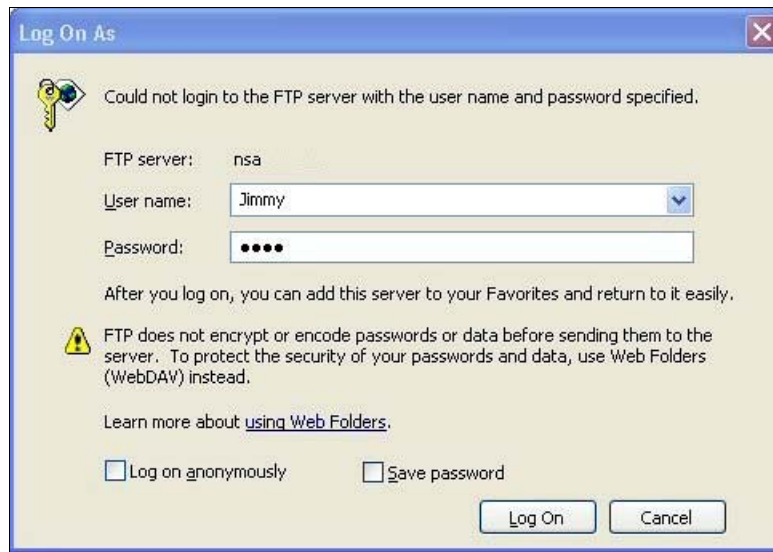
### 4.4.5 Accessing a Share Using FTP

You can also use FTP to access the NSA. Suppose Jimmy is temporarily using a different computer and wants to access his share without mapping it to the computer. This is how he would do it.

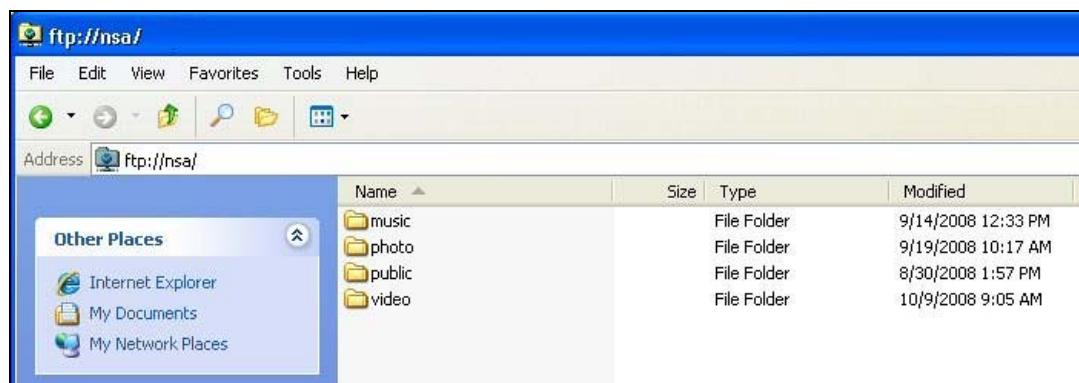
- 1 Open the FTP client (Windows Explorer is used here) and type "ftp://username@server" where "username" is the account's username and "server" is the NSA's IP address or server name.



- 2 Enter your password and click **Login**.



- 3 Now you can access files and copy files from/to your local computer's drives to or from this network folder.



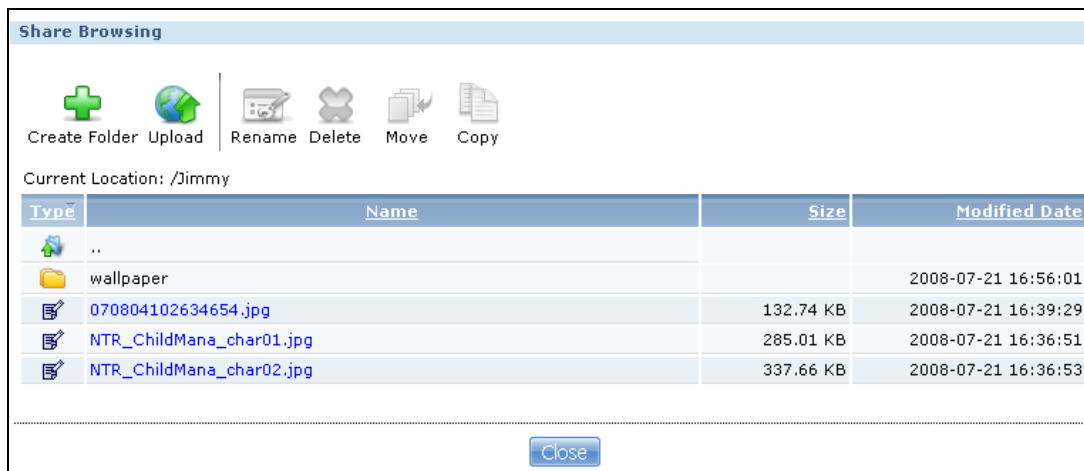
## 4.4.6 Accessing a Share Through the Web Configurator

You can browse and access files through the web configurator.

- 1 Log into the NSA web configurator (see [Section 3.3 on page 41](#)) using your username and password. Click a share to see the top level of the share's contents.



- 2 Here is the Jimmy share.



- 3 Click a folder's file name to browse the folder. You can open files or copy them to your computer. You can also create new folders and upload additional files to the share.
- 4 Click the logout icon when you are done.

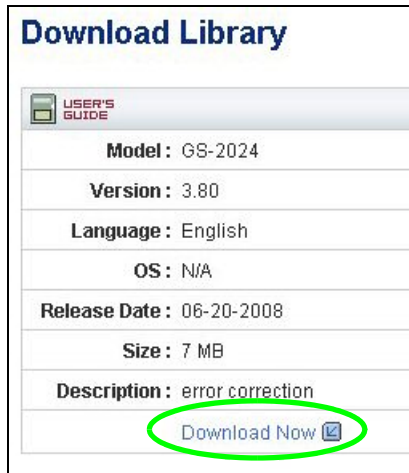


## 4.5 Download Service Tutorial

This tutorial covers using the NSA to download a file from the Internet. Use this same procedure for BitTorrent downloads as well as regular HTTP (web) and FTP downloads. See [Section 9.11.2 on page 199](#) for more on the download service.

### 4.5.1 Copying/Pasting a Download Link

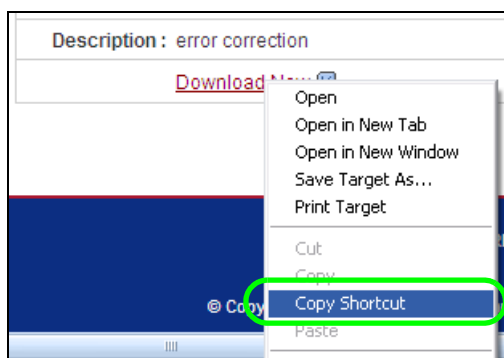
- 1 Open your Internet browser (this example uses Internet Explorer).
- 2 Find a download link for the file you want. In this example, [www.zyxel.com](#) has a **Download Now** link for downloading a datasheet for ZyXEL's GS-2024 (a device for making phone calls over the Internet).



Note: Make sure the link opens either the file you want or a pop-up window about how to handle the file.

Note: It is also OK for the link to open a .torrent file. If you are redirected to a screen that says the download should start in a few seconds, there may be a link to click if the download does not start automatically. See if that link opens the file or the pop-up window.

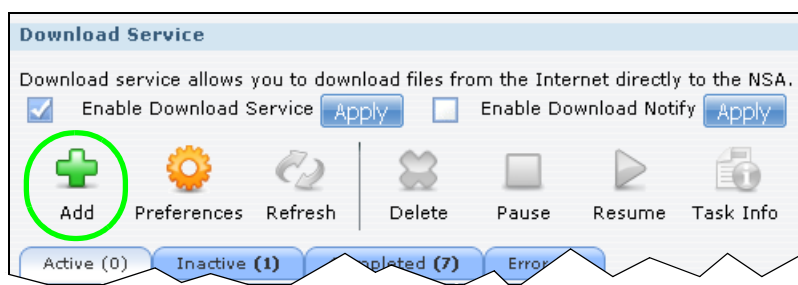
- 3 Right-click the download link and select **Copy Shortcut** in Internet Explorer (or **Copy Link Location** in Firefox).



- 4 Log into the NSA web configurator (see [Section 3.3 on page 41](#)) using the administrator account and click **Download Service**.



- 5 Click **Add**.



6 Right-click the **URL** field and select **Paste**.

**Add Download Task From URL**

**Source**

☒ URL ☐ Torrent File

**Location of Downloaded Files**

	Share	Path
Put incomplete downloads in	admin	/download
Move completed downloads to	public	/

**Note:**

1. BitTorrent jobs are stored in /public/incoming.
2. HTTP/FTP jobs are stored in /public.
3. All jobs triggered by RSS channels create the subfolder in /public using the channel name where it store all files downloaded from that channel.

**Caution:**

Do not use the NSA for illegal downloads. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws and will bear the consequences of any infringements thereof. ZyXEL takes NO responsibility or liability for your use of the download service feature.

7 The URL displays in the **URL** field. Click **Apply**.

**Add Download Task From URL**

**Source**

☒ URL ☐ Torrent File

**Location of Downloaded Files**

	Share	Path
Put incomplete downloads in	admin	/download
Move completed downloads to	public	/

**Note:**

1. BitTorrent jobs are stored in /public/incoming.
2. HTTP/FTP jobs are stored in /public.
3. All jobs triggered by RSS channels create the subfolder in /public using the channel name where it store all files downloaded from that channel.

**Caution:**

Do not use the NSA for illegal downloads. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws and will bear the consequences of any infringements thereof. ZyXEL takes NO responsibility or liability for your use of the download service feature.

8 After a few moments, the download task appears in the **Download Service** screen's **Active** tab.

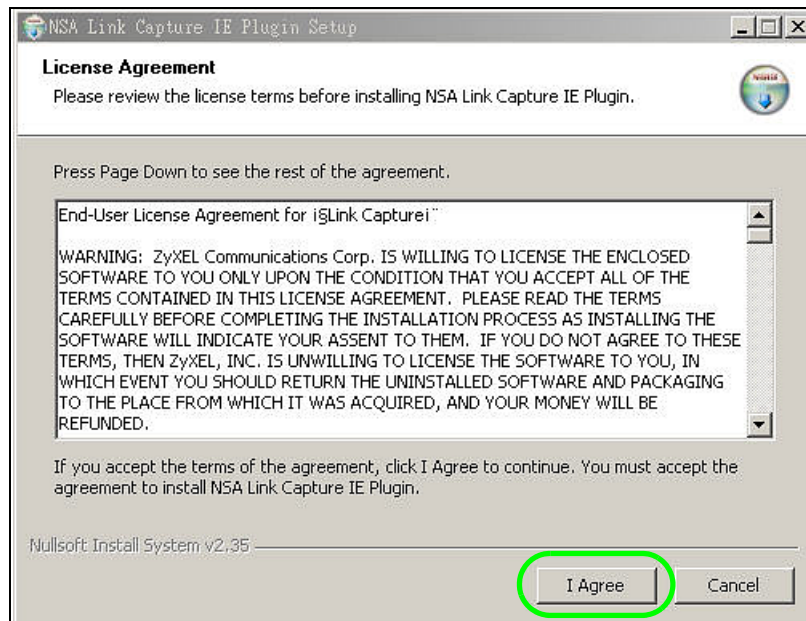
The download appears in the **Completed** tab when it is done. By default the NSA stores all downloads in the **admin** share's **download** folder. See [Section 4.4.4 on page 72](#), [Section 4.4.5 on page 74](#), or [Section 4.4.6 on page 76](#) for how to access a share.

## 4.5.2 Installing the Link Capture Browser Plugin

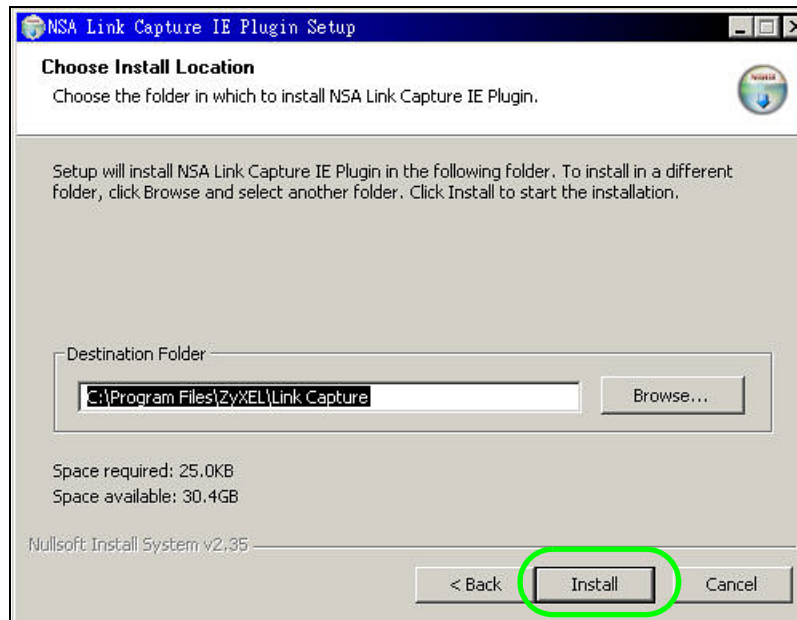
In addition to copying and pasting a download link to the **Download Service** screen, you can also install a link capture browser plugin in your web browser. Use the plugin to easily add a download link to the NSA's download service. See [Section 9.11.3 on page 199](#) for more on the link capture browser plugin.

### Internet Explorer

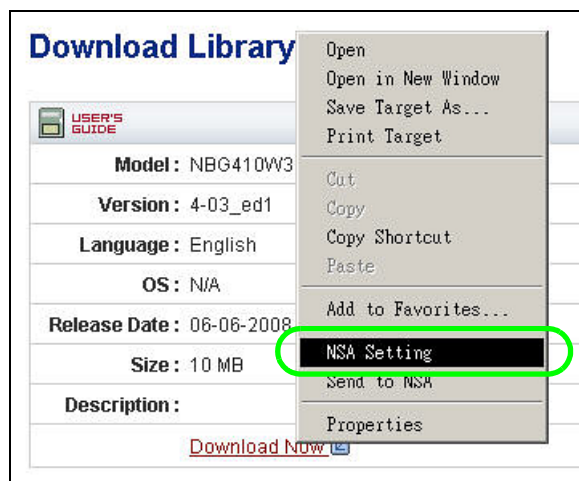
- 1 Open the folder containing the link capture browser plugin.
- 2 Double-click on the plugin to display the following screen. Click **I Agree** to begin installation.



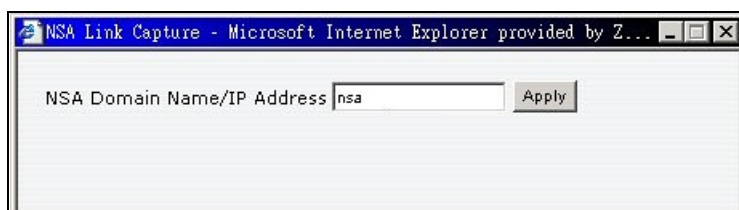
- 3 Select a location to save the plugin and click **Install**. Close the screen once the installation is complete.



- 4 Open Internet Explorer and locate a download link. In this example, [www.zyxel.com](http://www.zyxel.com) has a **Download Now** link for downloading a user's guide for ZyXEL's NBG410W3G (a 3G wireless router). Right-click on the download link and select **NSA Setting**.

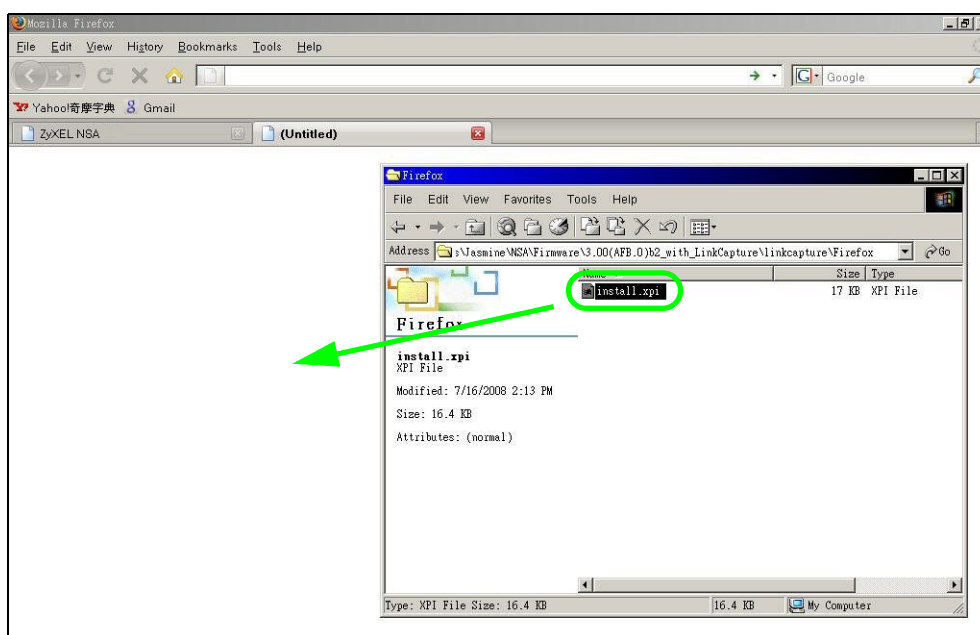


- 5 Enter the NSA's web address (nsa210 by default) and click **Apply**. A warning message displays asking for confirmation. Click **OK** to apply the setting.

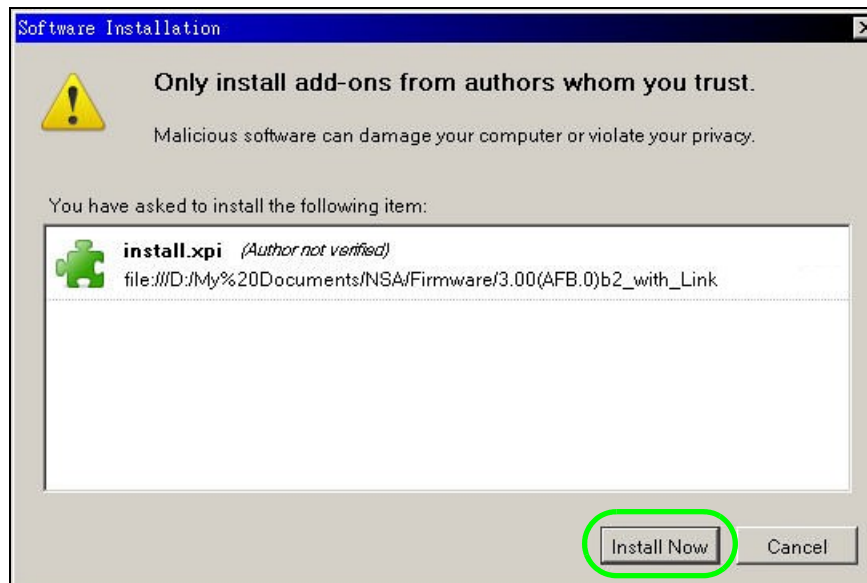


## Firefox

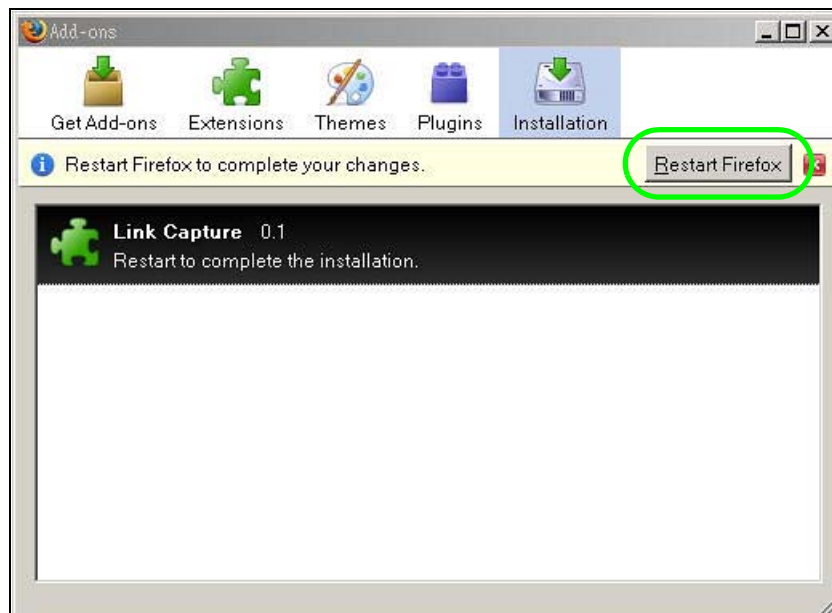
- 1 Open Firefox.
- 2 Open the folder containing the link capture browser plugin.
- 3 To install the plugin, drag and drop the plugin to Firefox.



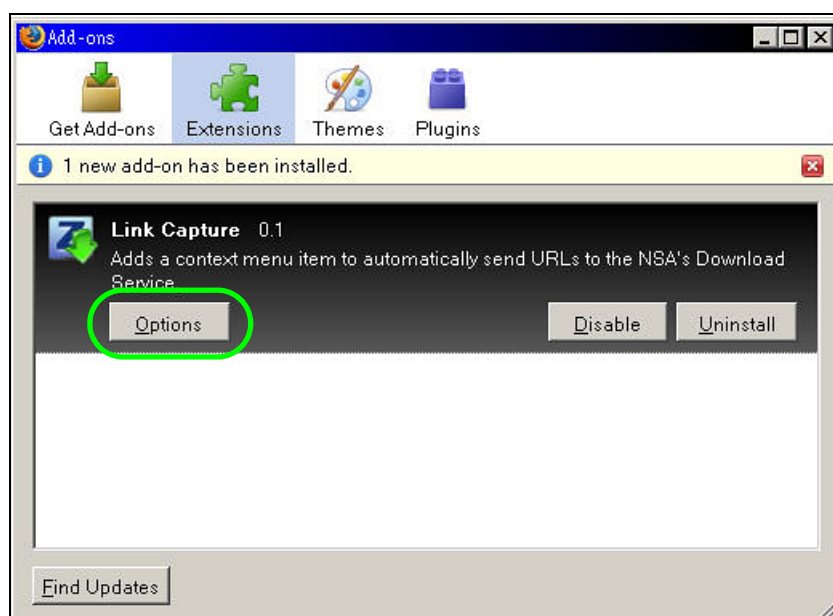
- 4 The following screen displays. Click **Install Now**.



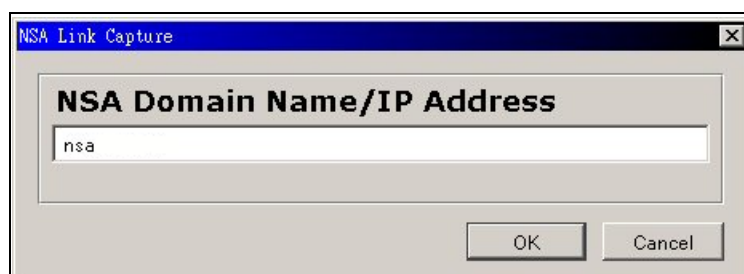
- 5 You need to restart Firefox after the installation.



- 6 When Firefox restarts, a message displays to show the installation succeeded. The plugin is installed as an extension in Add-ons. Click **Options** to configure the NSA's web address.



- 7 Enter the NSA's web address (nsa210 by default) and click **OK**.





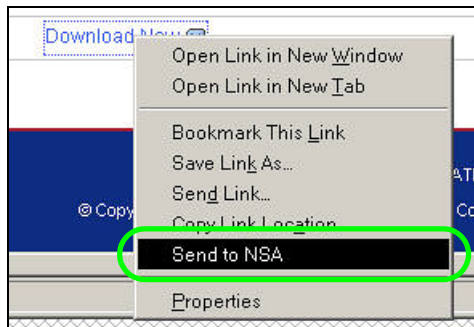
### 4.5.3 Using the Link Capture Browser Plugin

Once you install the plugin, you may begin sending download links to the NSA from your web browser. This example shows how to send a download link to the NSA's download service using the link capture browser plugin.

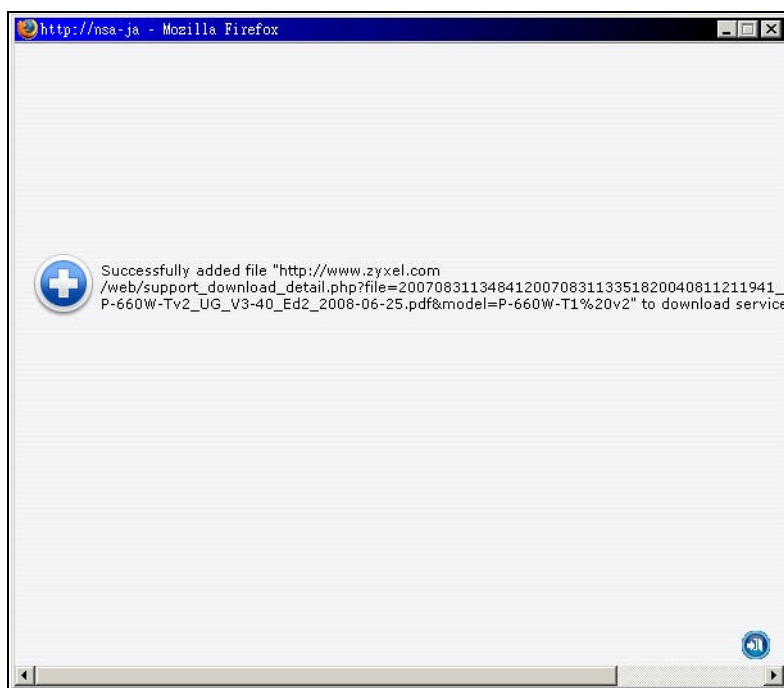
- 1 Open your Internet browser (this example uses Firefox).
- 2 Find a download link for the file you want. In this example, [www.zyxel.com](http://www.zyxel.com) has a **Download Now** link for downloading a user's guide for ZyXEL's P-660W-T1 (an ADSL router).



- 3 Right-click on the download link and select **Send to NSA**.



- 4 The login screen shows up. Enter your NSA's login information and click **Login** to send the link to the download service. A confirmation message displays.



- 5 Log into the NSA web configurator (see [Section 3.3 on page 41](#)) using the administrator account and click **Download Service**.



- 6 The download task appears in the **Download Service** screen's **Active** or **Queue** tab. It may appear in the **Completed** tab if the NSA already finished downloading the file or it may appear in the **Error** tab if the NSA failed to download the file.

By default the NSA stores all downloads in the **admin** share's **download** folder. See [Section 4.4.4 on page 72](#), [Section 4.4.5 on page 74](#), or [Section 4.4.6 on page 76](#) for how to access a share.

## 4.5.4 Configuring the Download Service Preferences

Once you added a list of download tasks to the NSA (see [Section 4.5.1 on page 77](#) and [Section 4.5.3 on page 85](#)), you can have the NSA download files during a specific time period of the day. You can also configure the BitTorrent settings to control bandwidth and optimize download efficiency.

Say you have the NSA turned on all the time, but you only want the NSA download files at night. Here is how you use the download period control feature to set the time range.

- 1 Click **Applications > Download Service > Preferences** to open the **General Settings** screen.
- 2 Select **Enable Download Period Control** and use the arrows to adjust the time period from 23:30 to 09:00. Click **Apply** to save your changes. The NSA only downloads files within this 9.5-hour period every day.

**Preferences**

General Settings BitTorrent

**Location of Downloaded Files**

	Share	Path
Put incomplete downloads in	admin	/download
Move completed downloads to	admin	/download

Edit

**Note:**

1. BT Jobs will be stored in /admin/download/incoming
2. HTTP/FTP Jobs will be stored in /admin/download
3. Jobs triggered by RSS Channel will create the Channel Name to /admin/download

**Download Period Control**

☒ Enable Download Period Control

Download Service is active in the specified time period (hh:mm - hh:mm)

23 :30 - 09 :00

Apply Reset Cancel

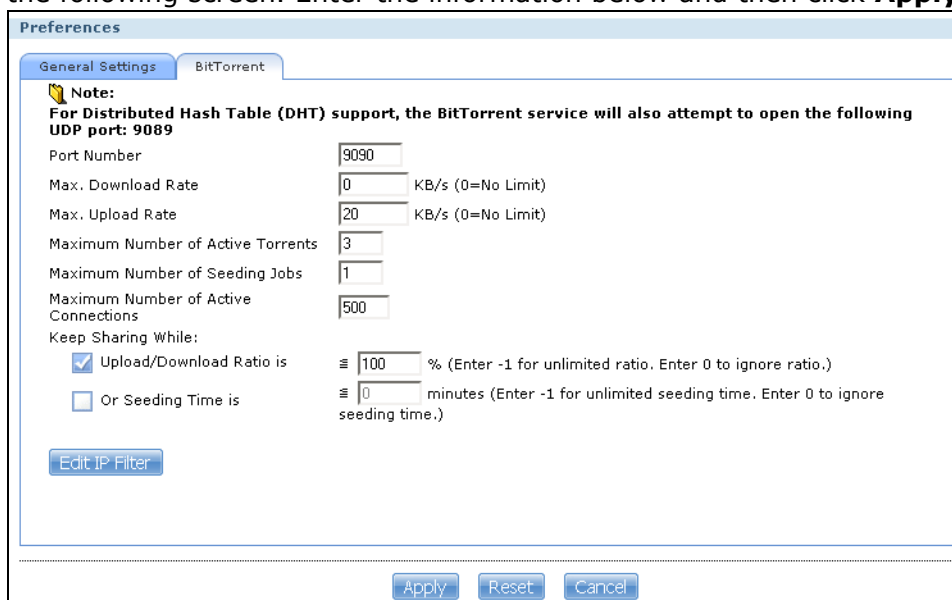
Note: If you configure the **Power On/Off Schedule** feature in the **Power Management** screen, make sure your active download period does not conflict with the power-off period.

Note: If power failure occurs during the active download period, the NSA will verify whether the downloaded files were damaged. If a file is corrupted, the NSA will download the file again. If the file is intact but not completely downloaded, the NSA will resume the download task after it restarts.

- 3 When it is not the download time, you see a message in the **Download Service** screen, indicating the active download period.



Click **Applications > Download Service > Preferences > BitTorrent** to open the following screen. Enter the information below and then click **Apply**.



Here is a list of BitTorrent settings you want to configure for your NSA:

- Limit the maximum upload rate to 20 KB/s.  
Enter this value in the **Max. upload rate** field.
- Actively download three torrent files but only upload one at a time.  
Enter 3 in the **Maximum Number of Active Torrents** field and enter 1 in the **Maximum Number of Seeding Jobs** field.
- Keep sharing until the NSA has shared equal or greater amount of the downloaded files.  
Select the check box and enter 100 in the **Upload/Download Ratio** field.

- Click **Edit IP Filter**. Use an online IP filter table from <http://www.bluetack.co.uk/config/level1.gz> for example to protect BitTorrent downloads.

Enter the URL in the **Update IP Filter from the Internet Every Week** field.

**Edit IP Filter**

☒ Enable IP Filter ( Last Update Time : N/A )

☒ Update IP Filter Table File from the Internet Every Week  
URL

☐ Upload IP Filter Table

**Note:** Please upload your list( \*.txt, \*.dat, \*.gz, \*.tgz or \*.tar.gz ) here. It will be saved as /admin/download/ipfilter.dat.

### 4.5.5 Using Download Service Notification

Use an RSS feed reader on your computer to keep track of files the NSA has downloaded. The following examples show how to subscribe to the NSA's download service notifications. See [Section 9.11.4 on page 200](#) for more on download service notifications.

Some RSS readers may not support the NSA's download service notifications. For example, Google Reader cannot support this feature if the NSA has a private IP address.

Note: It is recommended to subscribe to the download service notifications using the built-in reader in Internet Explorer 7 or higher, or Firefox.

You have to activate this feature in the **Download Service** screen. Click **Applications > Download Service** to open the following screen. Select **Enable Download Notify** and click **Apply**.

**Download Service**

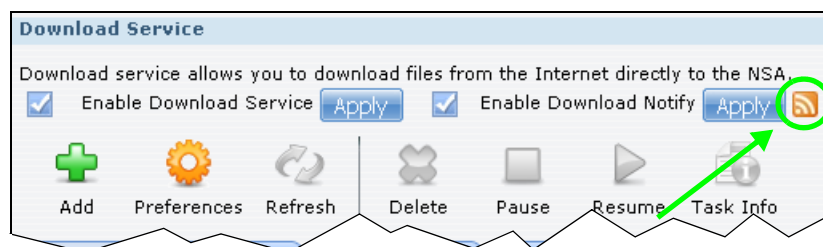
Download service allows you to download files from the Internet directly to the NSA.

☒ Enable Download Service

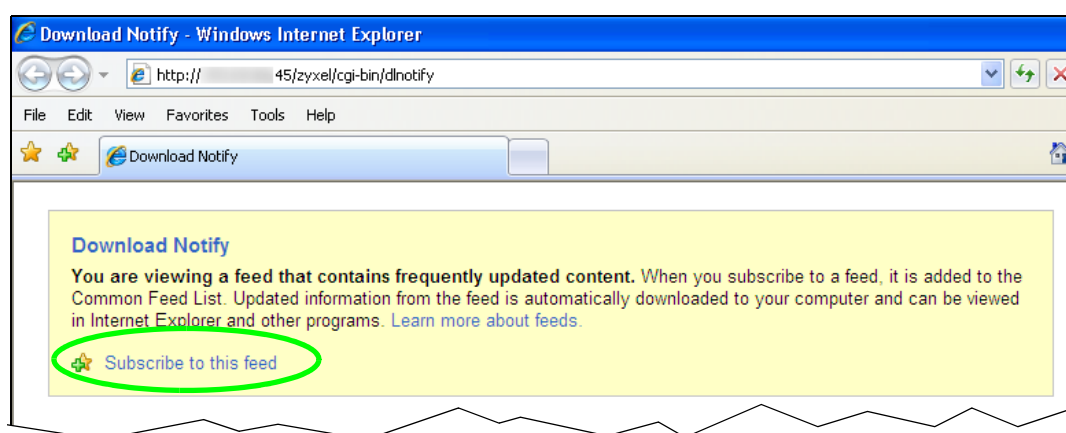
☒ Enable Download Notify

## Internet Explorer 7 Example

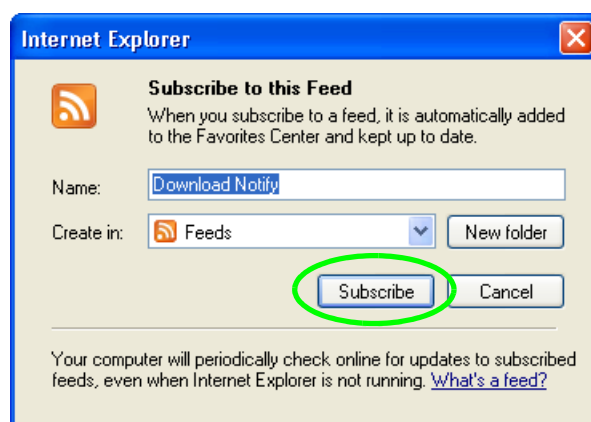
- 1 After you activate download service notification, click the **RSS** feed icon.



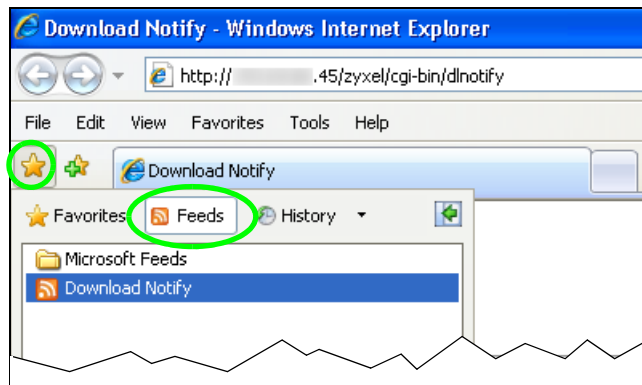
- 2 The following screen displays. Select **Subscribe to this feed**.



- 3 The following screen displays. Click **Subscribe**.

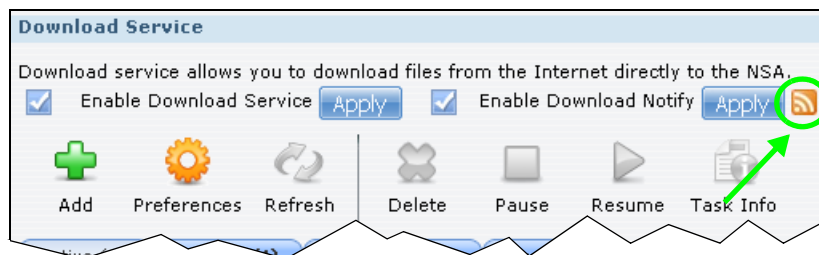


- 4 Click the **Favorite** icon on your browser and select the **Feeds** tab to check the updates of your NSA's download list.

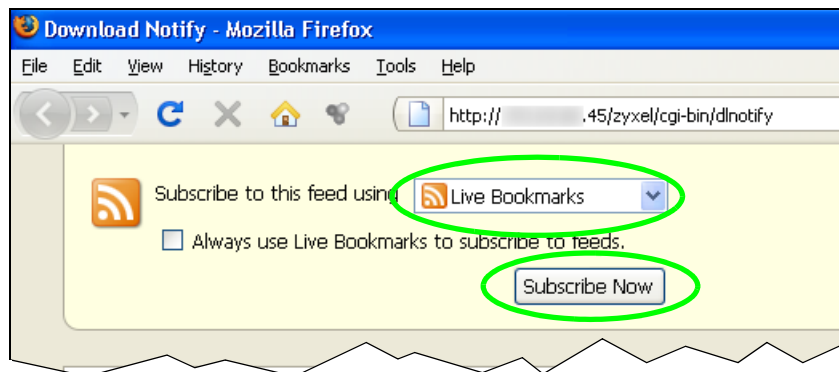


### Firefox Example

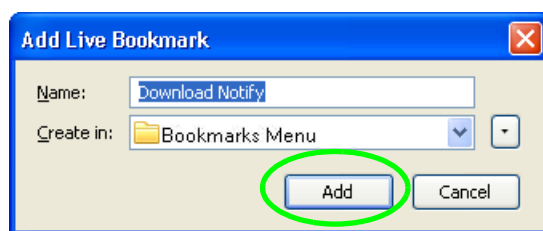
- 1 After you activate download service notification, click the **RSS** feed icon.



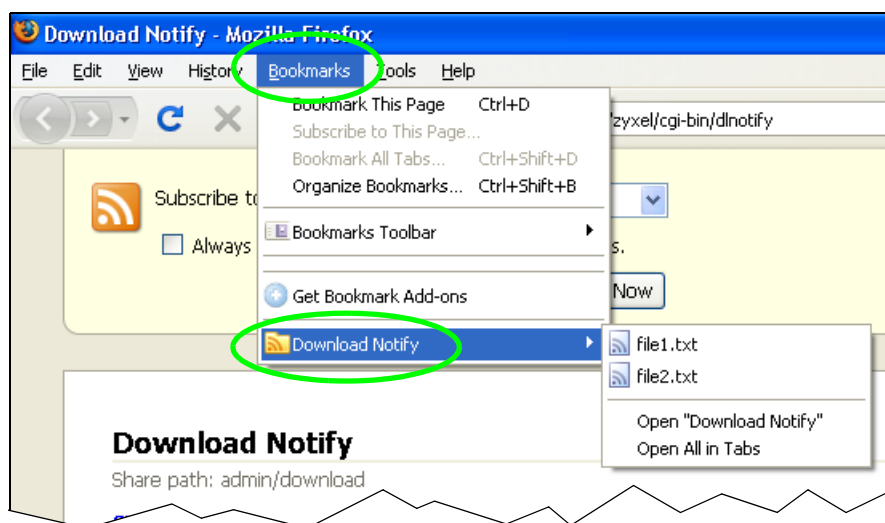
- 2 The following screen displays. Select **LiveBookmarks** from the drop-down list and click **Subscribe Now**.



- 3 The following screen displays. Select **Bookmarks Menu** and click **Add**.



- 4 From the Firefox's **Bookmarks Menu**, select **Download Notify** to check the updates of your NSA's download list.





## 4.6 Broadcatching Tutorial

Use broadcatching to have the NSA download frequently updated digital content like TV programs, radio talk shows, Podcasts (audio files), and blogs. This example shows how to subscribe the NSA to the CNET TV Internet television channel. See [Section 9.8 on page 186](#) for more on the broadcatching service.

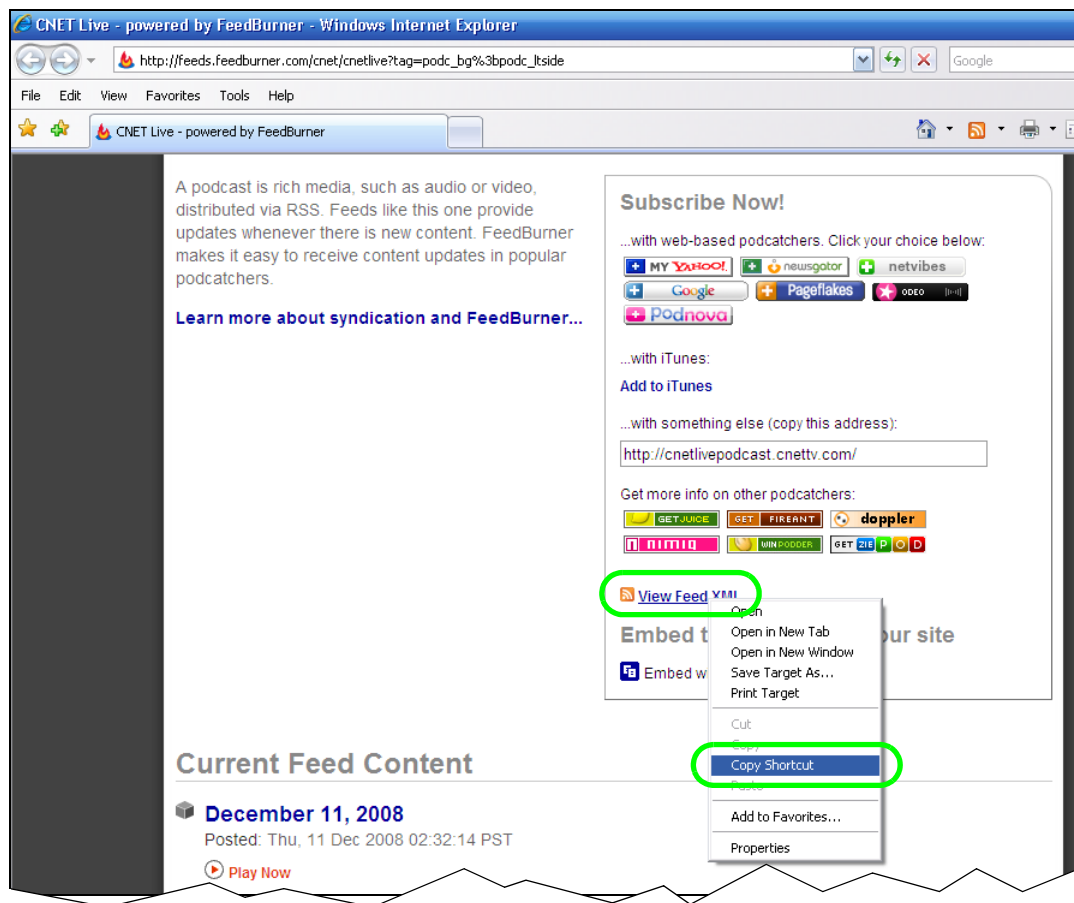
- 1 Open your Internet browser (this example uses Firefox).
- 2 Find the link for the RSS feed containing the channel you want to add. In this example, [http://reviews.cnet.com/4520-11455\\_7-6333605-1.html](http://reviews.cnet.com/4520-11455_7-6333605-1.html) has an **RSS** link for subscribing to the CNET Live podcast. However this is not the link for the actual RSS feed. Click the link to go to another screen that has RSS feed links.



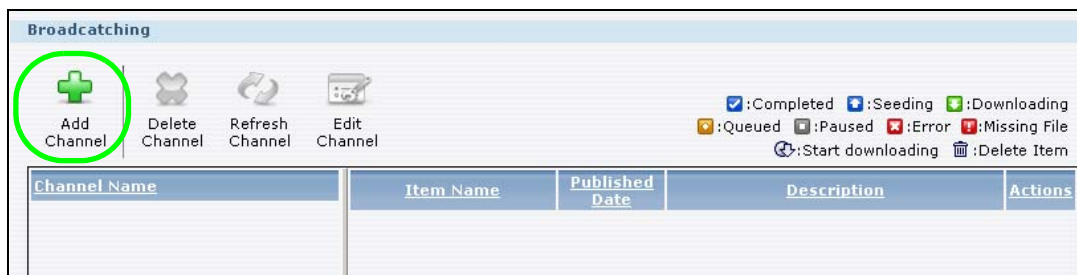
Note: Make sure the link goes to the actual RSS feed instead of to another list of links or information about the channel.

One way to test this is by clicking the link. Clicking an actual RSS feed link opens a screen of XML code (in browsers without an RSS feed aggregator) or a window where you can add the RSS feed (in browsers with an RSS feed aggregator).

- 3 Right-click the download link and select **Copy Link Location** in Firefox (or **Copy Shortcut** in Internet Explorer).



- 4 Log into the NSA web configurator (see [Section 3.3 on page 41](#)) using the administrator account and click **Administration > Applications > Broadcatching**.
- 5 Click **Add Channel**.



- 6 Right-click the URL field and select **Paste**.



- 7 The URL displays in the **URL** field.
- 8 Select a policy for what items to download. This example uses **Manually Choose Items for Download** so you will be able to select individual items to download later.
- 9 Select a policy for what items to delete. This example keeps the most recent 10 items.
- 10 Click **Apply**.

**Subscribe to Channel Feed**

Please enter the url address of the feed you want to subscribe to

Download Policy

Delete Policy  
☐ Manual  
☒ Keep last  of items

Location of Downloaded Files

	Share	Path
Put incomplete downloads in	admin	/download
Move completed downloads to	public	/

**Note:**

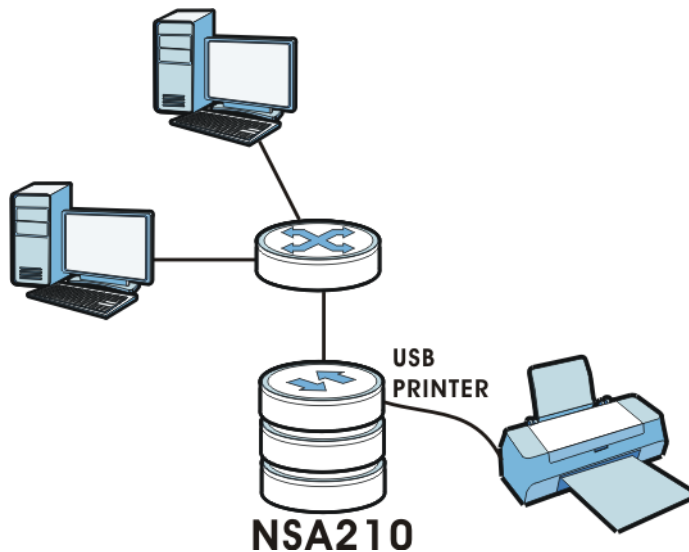
1. BitTorrent jobs are stored in /public/incoming.
2. HTTP/FTP jobs are stored in /public.
3. All jobs triggered by RSS channels create the subfolder in /public using the channel name where it store all files downloaded from that channel.

- 11 After a few moments, the channel appears in the **Broadcatching** screen where you can select items you want to download. The NSA saves the items you download in a folder named after the channel. By default, the channel folders are created in the **admin** share's **download** folder. The NSA's media server feature makes it easy for users on your network to play the broadcatching files you download. See [Section 9.11.1 on page 197](#) for more on the media server.

## 4.7 Printer Server Tutorial

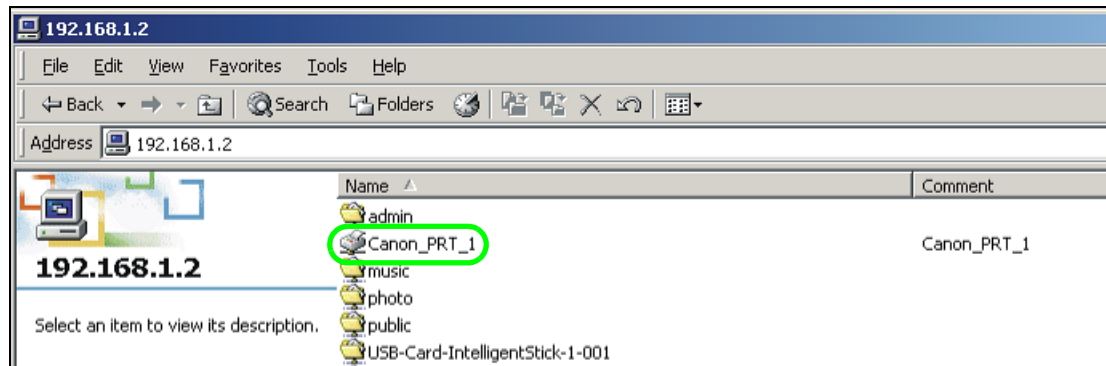
Do the following to have the NSA let computers on your network share a printer. See [www.zyxel.com](http://www.zyxel.com) for a list of compatible printers.

- 1 Make sure the NSA is on and the **SYS** light is on steady (not blinking).
- 2 Use a USB cable to connect the printer's USB port to one of the NSA's USB ports. Make sure the printer is also connected to an appropriate power source.

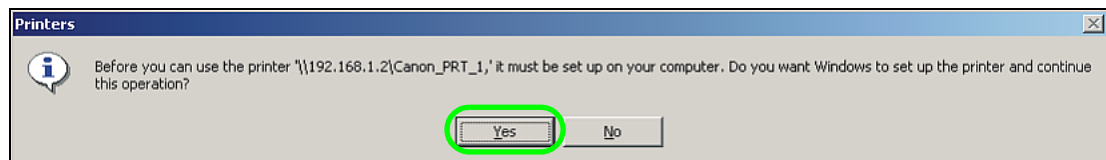


- 3 Turn on the printer.
- 4 The NSA detects the printer after a few moments.

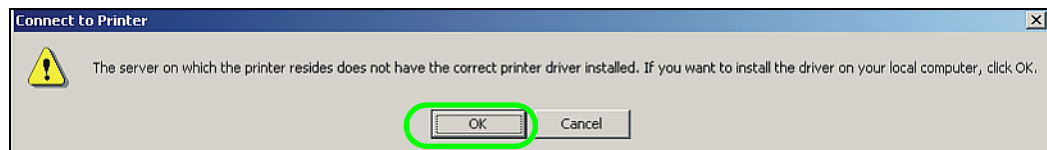
- 5 On your computer, open your CIFS file sharing program (Windows Explorer for example) and browse to the NSA. Double-click the printer's icon.



- 6 If you get a warning screen, click the option that lets you continue (**Yes** in this example).

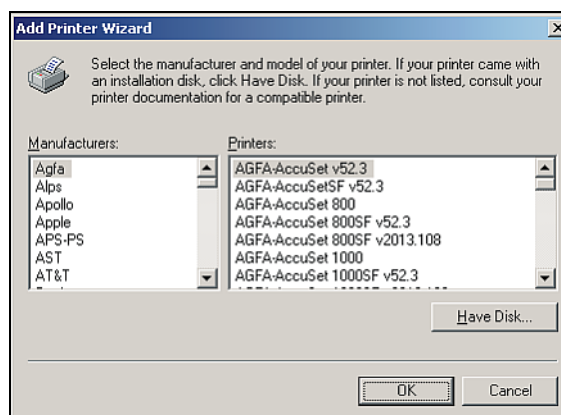


- 7 If your computer does not already have the printer's driver installed, you will need to install it. In this example, click **OK**.

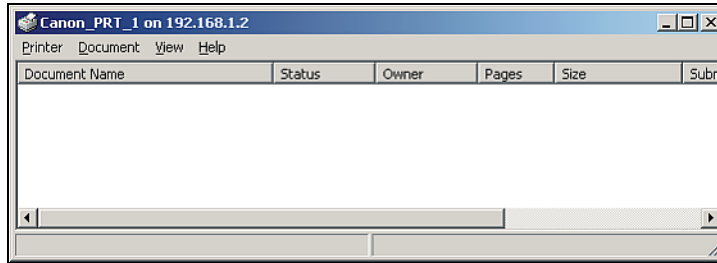


- 8 Use the wizard screens to install the printer driver on the computer. You may need to get the file from the printer's CD or the printer manufacturer's website (the driver is not installed on the NSA).

Note: You must install the printer driver on each computer that will use the printer.



After the driver installation finishes, the computer is ready to use the printer. Select the printer in an application to use it to print. Browse to the NSA using a CIFS program (like Windows Explorer) and double-click the printer's icon to open the printer's queue of print jobs.



Note: Repeat steps 5 to 8 on your other computers so they can also use the printer.

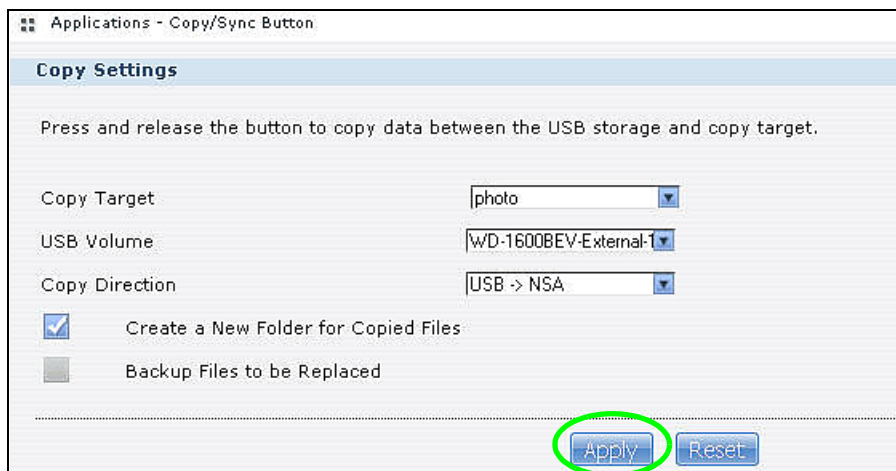
## 4.8 Copy and Flickr Auto Upload Tutorial

Amy received some photos taken during her best friend's wedding and saved the files on a USB disk. She wants to save a copy of the photos in the NSA and upload the photos to her Flickr account.

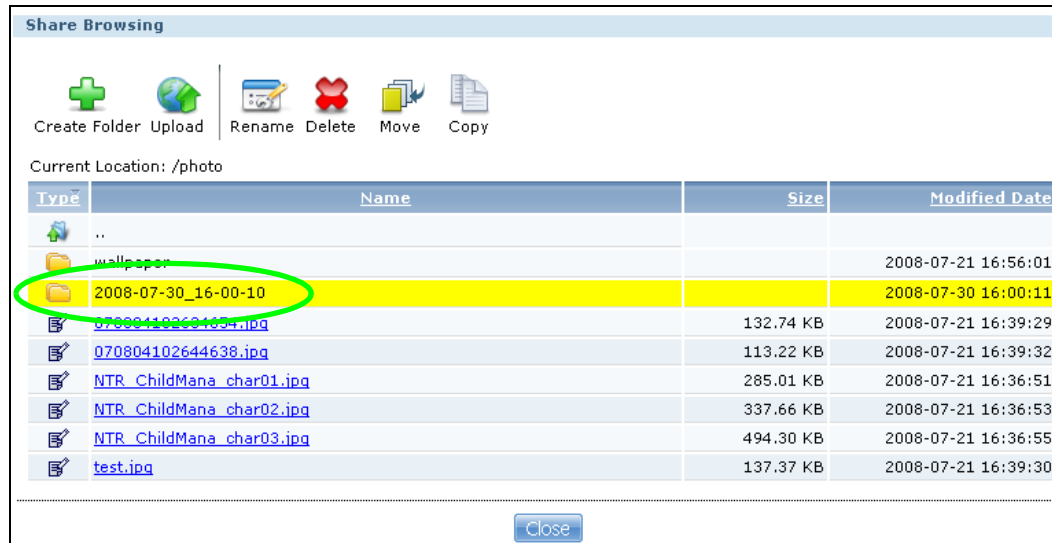
Amy has to activate the NSA's auto upload feature. See [Section 11.4 on page 266](#) for more details on setting up a Flickr account for auto upload. In this example Amy select the NSA's photo share for auto upload.

This is how Amy would transfer the files from her USB disk to the NSA.

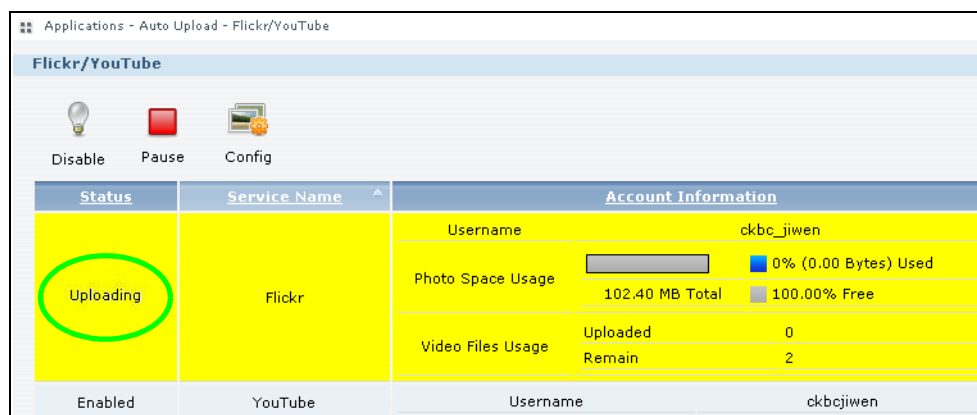
- 1 Click **Applications > Copy/Sync Button** in the navigation panel to open the screen.
- 2 Configure the copy settings as shown and click **Apply**.



- 3 Press and release the **COPY/SYNC** button on the NSA's front panel to start copying files.
- 4 The copied files can be found in a new folder in the photo share. The name of this folder is the date (yyyy-mm-dd) and time (hh:mm:ss) when the folder is created.



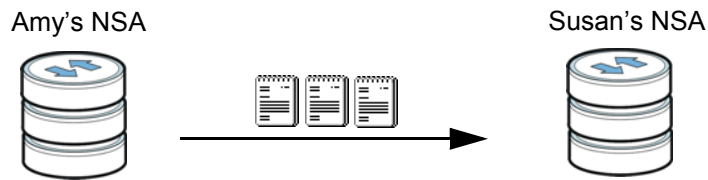
- 5 The NSA also automatically uploads the copied files to Flickr.



## 4.9 FTP Uploadr Tutorial

FTP Uploadr can automatically upload files saved on the NSA to a remote FTP server. Amy wants to share files on her NSA with Susan. They each have an NSA

at home, so Susan has to set her NSA as an FTP server for Amy to automatically send files using FTP Uploadr.



To set the NSA as an FTP server, click **Applications > FTP** to open the **FTP** screen. Select **Enable FTP** and click **Apply**.

The screenshot shows the 'FTP' configuration window. The 'Enable FTP' checkbox is checked and circled in green. Below it, the 'Connection Limit' is set to 10, 'Idle Timeout' is 15 minutes, and 'Port Number' is 21. To the right, default values are shown: 'Connection Limit: 20' and 'Max timeout: 300 minutes'. There are also checkboxes for 'Enable Anonymous FTP Access' and 'Customize the port range for data transfer', both of which are unchecked. A 'Note' section provides instructions on configuring shares for anonymous access. At the bottom, the 'Character Set' is set to '(UTF-8)'. The 'Apply' button is circled in green, along with a 'Reset' button.

Susan also has to create a user account and share on her NSA for Amy to upload files. The share is used for files uploaded from Amy's NSA. Amy will then use the following information to configure FTP Uploadr on her NSA.

**Table 15** FTP Uploadr Tutorial: FTP Server Information

FTP Domain Name or IP Address	example2.com
FTP User Name	Amy
FTP Password	xxxxx
Share (Remote Path)	Amy



This is how Amy would set up the NSA's FTP Uploadr.

- 1 Click **Applications > Auto Upload > FTP Uploadr** to open the **FTP Uploadr** screen. Select **Enable FTP Uploadr** and click **Apply** to turn on FTP Uploadr.

**FTP Uploadr**

☒ Enable FTP Uploadr **Apply**

Add Server
 Preferences
 Edit Server
 Delete Selected Server(s)
 Server Information

Domain Name/IP Address	Port Number	Remote Path	Account Name	Description
------------------------	-------------	-------------	--------------	-------------

- 2 Click **Add Server**.

**FTP Uploadr**

☒ Enable FTP Uploadr **Apply**

Add Server
 Preferences
 Edit Server
 Delete Selected Server(s)
 Server Information

Domain Name/IP Address	Port Number	Remote Path	Account Name	Description
------------------------	-------------	-------------	--------------	-------------

Currently, there are no servers.

- 3 Enter the information as describe in [Table 15 on page 100](#). Click **Apply** to add the server.

**Add Server**

Domain Name/IP Address: example2.com

Account Name: Amy

Password: XXXX

Port Number: 21

Remote Path: /Amy

Description: Send to Susan

**Test Connection**

**Apply** **Cancel**

- 4 In the **FTP Uploadr** screen, click **Preferences** to configure the auto upload settings.

FTP Uploadr

☒ Enable FTP Uploadr Apply

Add Server **Preferences** Edit Server Delete Selected Server(s) Server Information

Domain Name/IP Address	Port Number	Remote Path	Account Name	Description
example2.com	21	/Amy	Amy	Send to Susan

- 5 Amy wants to share video files with Susan. In the **Preferences** screen, click the **Add** button and select **video** from the **Shares** drop-down list box, enter a forward slash in the **Path** field and click **Apply** to add the share to the **Folder Watch List**.

Folder Watch List

Status	Share Name	Path	Action
There are currently no folders on the watch list.			

**Add Watch Folder**

Share: video

Path: / Browse ...

Add Apply Cancel

**Settings**

**Grace Period**  
The time the system will wait before a newly added file is saved in a watched folder.  
Grace Period: 15 minutes

**Bandwidth Limit**  
Max. upload rate: 0 KB/s (0=No Limit)

Apply

Reset Close

- 6 Amy also set the **Bandwidth Limit** to 20KB/s so that the upload doesn't slow down her Internet connection.

**Folder Watch List**

Status <sup>^</sup>	Share Name	Path	Action
	video	/	

[Add](#)

**Settings**

**Grace Period**  
The time the system will wait before a newly added file is saved in a watched folder.  
Grace Period  minutes

**Bandwidth Limit**  
Max. upload rate  KB/s (0=No Limit) [Apply](#)

[Reset](#) [Close](#)

Now Amy has set up FTP Uploadr to send files to Susan's NSA. Everytime Amy adds new files or renames files in the **video** share, these new or modified files will be uploaded automatically to the **Amy** share on Susan's NSA.

Similarly, Susan can go through the steps described above to configure FTP Uploadr on her NSA. Once Susan completes the setup, Amy can also receive files from Susan's NSA.



## 4.10 Web Configurator's Security Sessions

These tutorials show you how to configure security for the NSA's Web Configurator sessions. You will customize the NSA's self-signed SSL certificate and distribute it to your users.

### 4.10.1 Customizing the NSA's Certificate

- 1 Click **Maintenance > SSL** and then select **Edit a self-signed CA certificate** and click **Edit**.

Maintenance - SSL

**Force HTTPS (TLS/SSL) Connections**

**Caution:**  
Modifications of TLS/SSL certificate settings will restart network services.

☐ Force HTTPS

Apply

**Install System Default CA**

This action will install the system default CA in the trusted CA list of your browser

**Step1** Download the default CA file [Download](#)

**Step2** Double click on the CA file to install it into your browser

**Modify the Existing Certificate**

**Caution:**  
Modifications of TLS/SSL certificate settings will restart network services.

☒ Edit a self-signed CA certificate

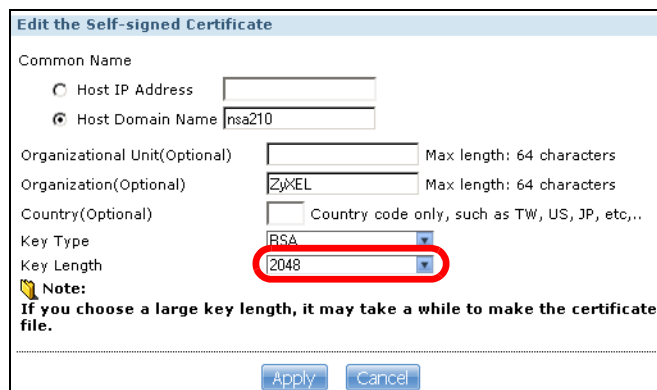
**Step1** Edit the Self-signed Certificate [Edit](#)

**Step2** Download the self-signed CA file [Download](#)

**Step3** Double click on the CA file to install it into your browser

☐ Create a Certificate To Be Authorized By My Own Certificate Authority

- 2 Next, let's modify the certificate by changing the **Common Name** to this NSA's host name of "nsa210", the **Organization** to "Test" and the **Key Length** to **2048**.



**Edit the Self-signed Certificate**

Common Name

☐ Host IP Address

☒ Host Domain Name

Organizational Unit(Optional)  Max length: 64 characters

Organization(Optional)  Max length: 64 characters

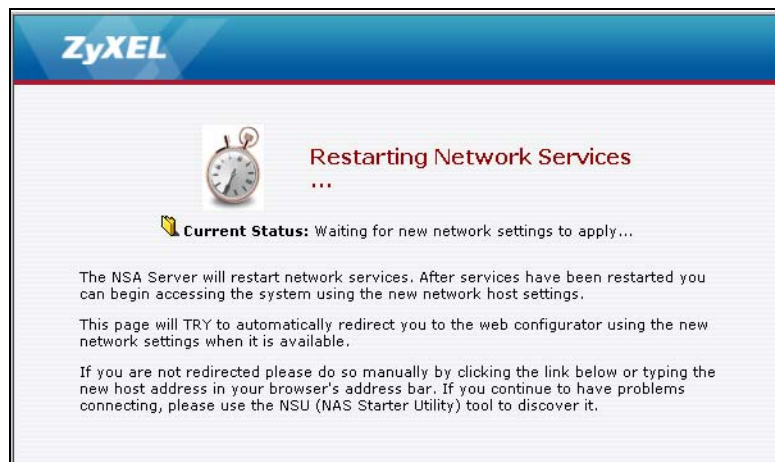
Country(Optional)  Country code only, such as TW, US, JP, etc,...

Key Type

Key Length

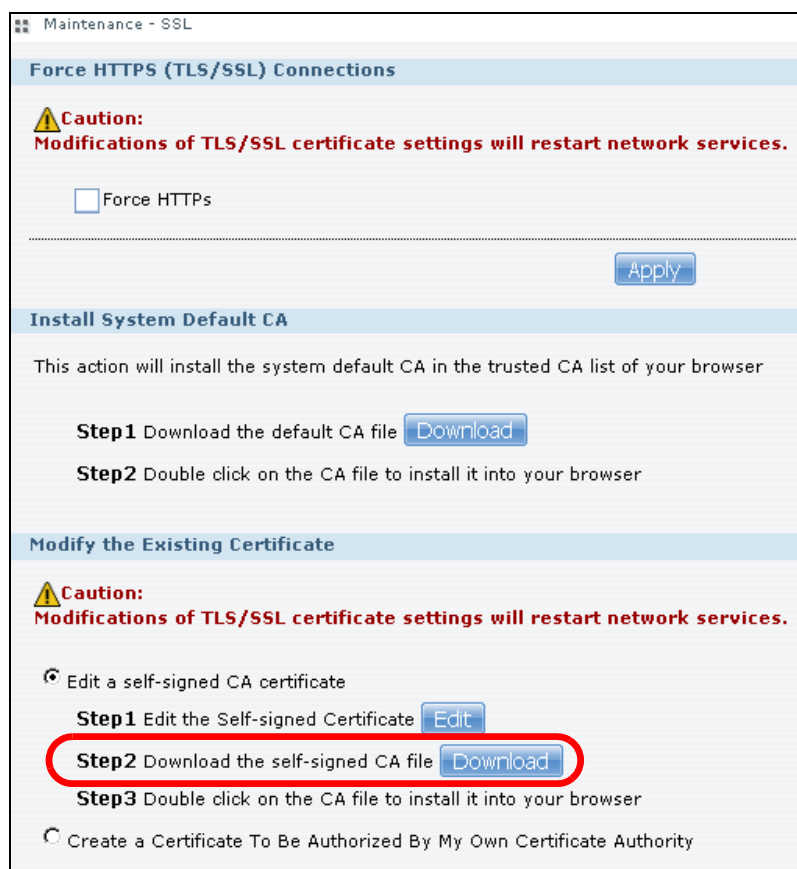
**Note:**  
If you choose a large key length, it may take a while to make the certificate file.

- 3 The NSA restarts its network services and returns you to the login screen.

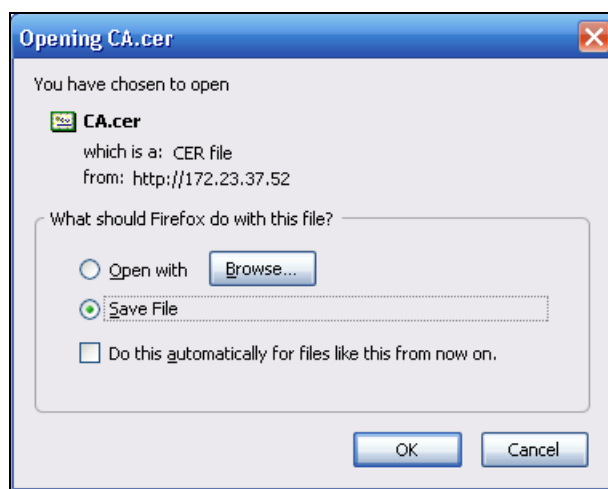


## 4.10.2 Downloading and Installing Customized Certificate

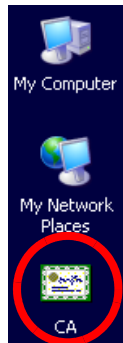
- 1 Log in and return to **Maintenance > SSL**. Under **Modify the Existing Certificate**, click **Download**.



- 2 Save the file to your computer.



- 3 Find the certificate file on your computer and double-click it.



- 4 Install the certificate. The rest of the steps in this section are an example of installing a certificate in Windows. See [Appendix D on page 403](#) for other examples. In the **Certificate** dialog box, click **Install Certificate**.



- 5 In the **Certificate Import Wizard**, click **Next**.

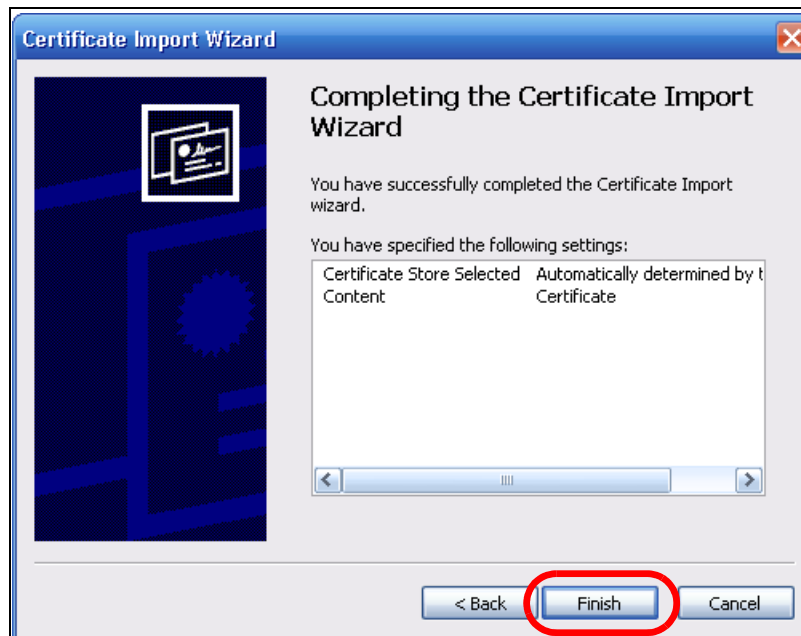


- 6 Leave **Automatically select certificate store based on the type of certificate** selected and click **Next**.

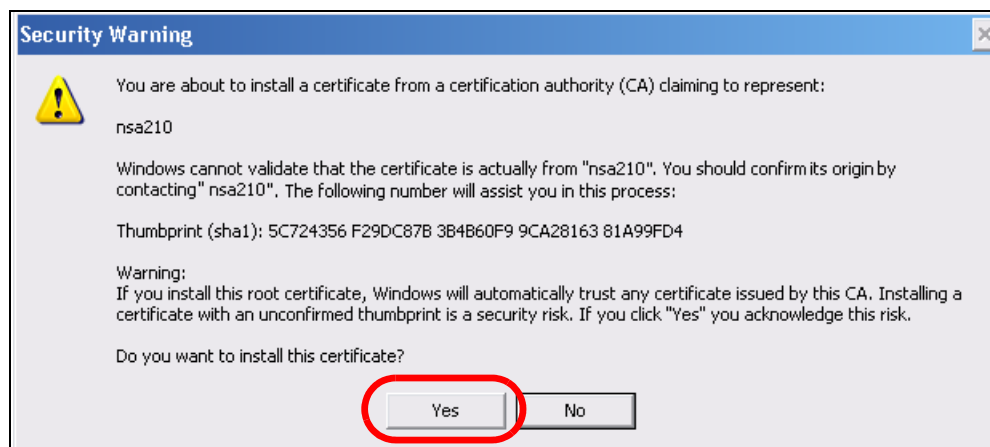




- 7 In the **Completing the Certificate Import Wizard** screen, click **Finish**.



- 8 If you are presented with another **Security Warning**, click **Yes**.



- 9 Finally, click **OK** when presented with the successful certificate installation message.



### 4.10.3 Turn on the NSA's Web Security

Now that you have customized the NSA's certificate and installed it in your computer, you can turn on security for your Web Configurator sessions. This example uses Firefox 3.0. See [Appendix D on page 403](#) for more information on browsers and certificates.

- 1 Close your web browser and open it again to reset its session with the NSA. Log in and click **Maintenance > SSL**. Select **Force HTTPS** and click **Apply**.

Maintenance - SSL

#### Force HTTPS (TLS/SSL) Connections

**Caution:**  
Modifications of TLS/SSL certificate settings will restart network services.

☒ Force HTTPS

Apply

#### Install System Default CA

This action will install the system default CA in the trusted CA list of your browser

**Step1** Download the default CA file [Download](#)

**Step2** Double click on the CA file to install it into your browser

#### Modify the Existing Certificate

**Caution:**  
Modifications of TLS/SSL certificate settings will restart network services.

☒ Edit a self-signed CA certificate

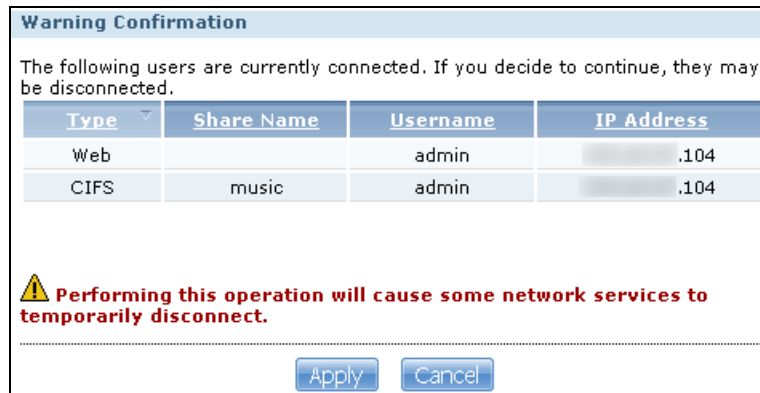
**Step1** Edit the Self-signed Certificate [Edit](#)

**Step2** Download the self-signed CA file [Download](#)

**Step3** Double click on the CA file to install it into your browser

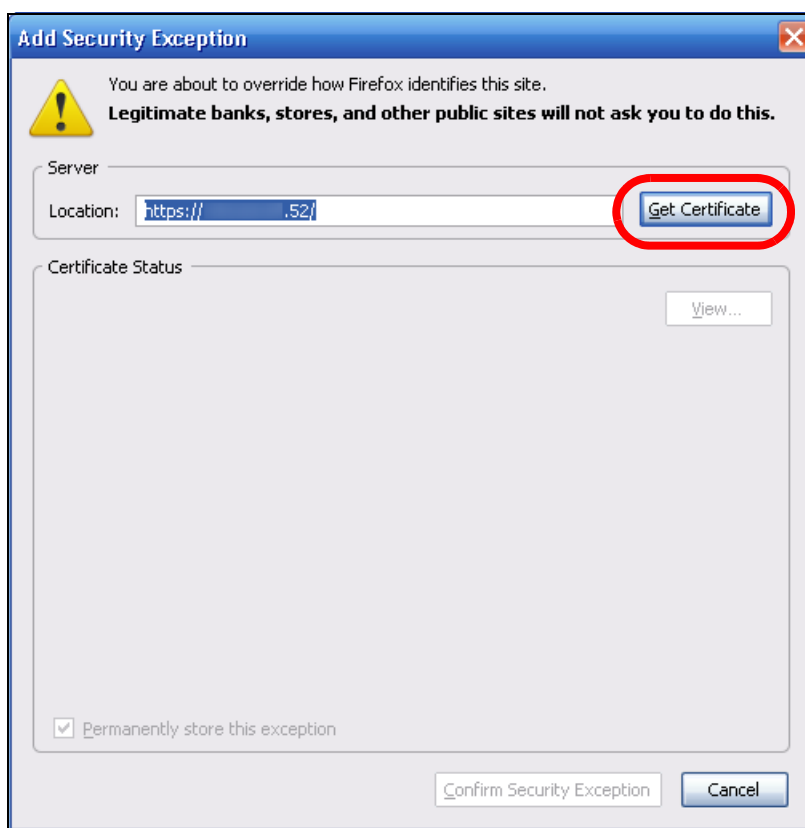
☐ Create a Certificate To Be Authorized By My Own Certificate Authority

- 2 A warning screen pops up if applying your change may disconnect some users. Click **Apply** to continue.

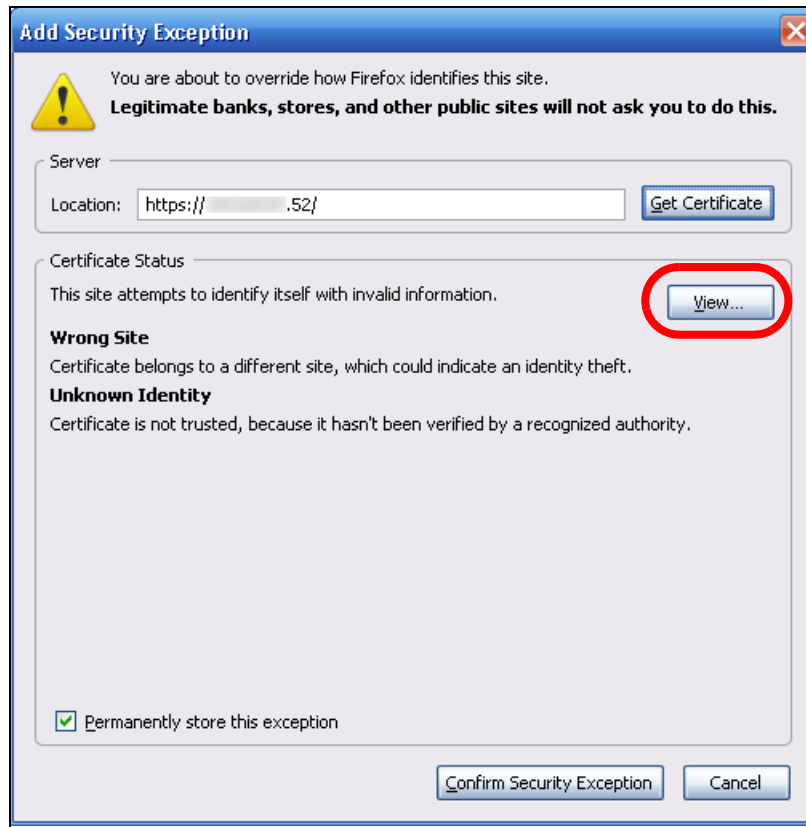


- 3 The NSA logs you out and automatically redirects your formerly non-secure (HTTP) connection to a secure (HTTPS) connection. Your browser may give you a warning about the device's public key certificate. Add an exception to allow your browser to bypass the warning.

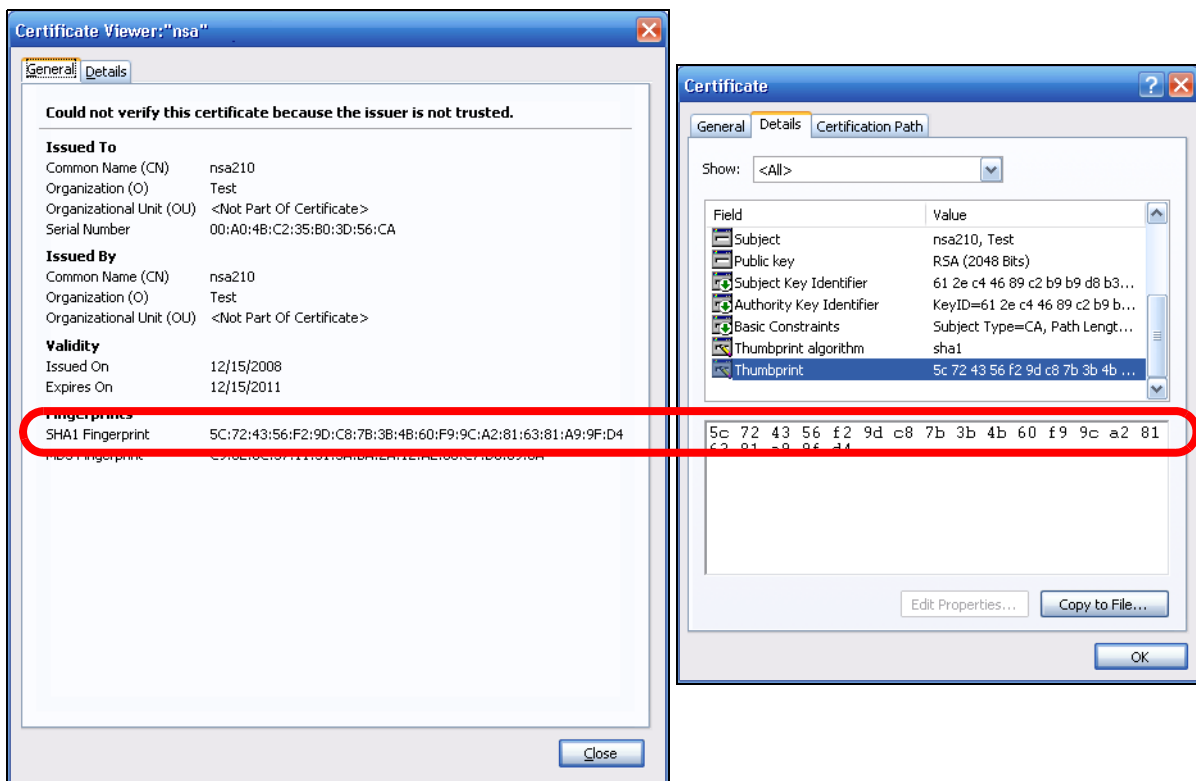


**4 Click Add Exception.****5 Click Get Certificate.**

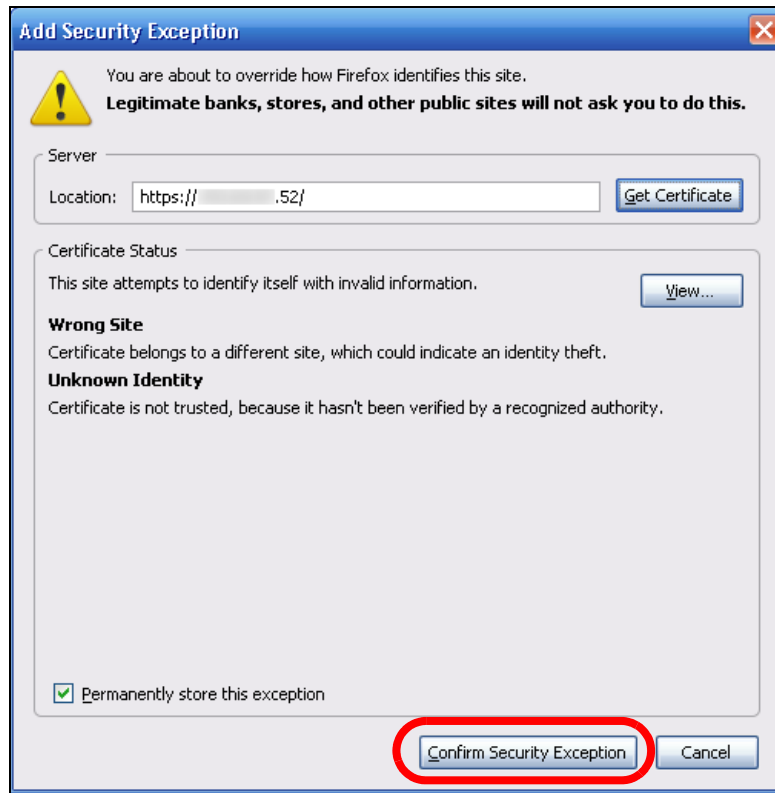
- 6 Before you add an exception, verify that the device to which you are trying to connect is providing the correct certificate. Click **View**.



- 7 The SHA1 fingerprint must match the NSA's certificate you downloaded from the NSA to your computer. (Double-click the NSA's certificate file and then click **Details** and look at the **Thumbprint**). Click **Close**.



- 8 If the certificate fingerprints match, click **Confirm Security Exception**, otherwise click **Cancel**.



- 9 The login screen displays.

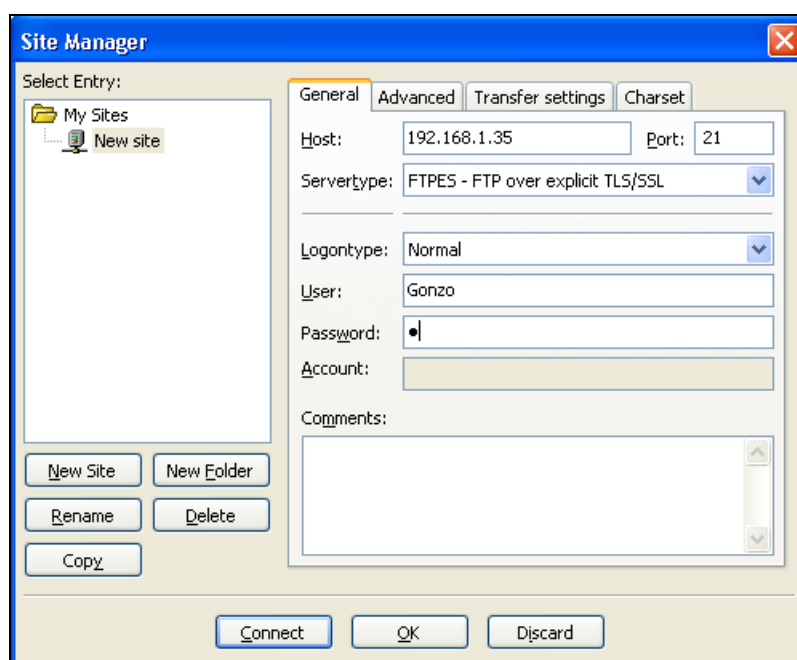


Now, anyone who connects to the NSA's Web Configurator screens will automatically do so by HTTPs. Use a secure method to let your users know the correct fingerprint for the NSA's certificate so they can check it before adding a security exception (as in steps 6 to 7 on pages 113 to 114). See the next section for how to use FTPES with the NSA for secure FTP transfers.

## 4.11 Using FTPES to Connect to the NSA

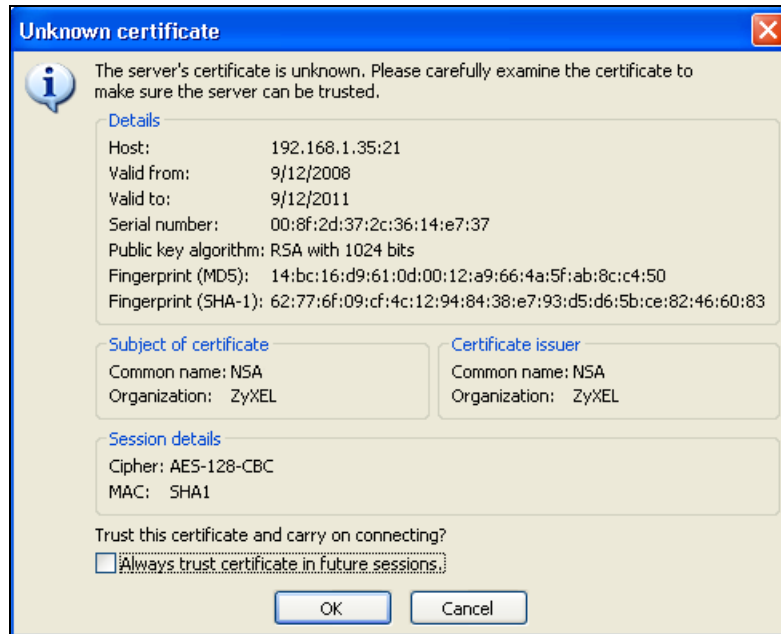
This section covers how to use FTP over Explicit TLS/SSL with the NSA for secure FTP transfers. Before you go through this section, read [Section 4.10 on page 104](#) to configure HTTPS. This example uses FileZilla.

- 1 Open FileZilla and click **File > Site Manager > New Site**.
  - Configure the **Host** field with the NSA's address.
  - Set the **Servertype** to **FTPES - FTP over explicit TLS/SSL**.
  - Configure the account name and password.
  - Click **Connect**.





- 2 A security warning screen displays. The SHA1 fingerprint must match the NSA's certificate you downloaded from the NSA to your computer. (Double-click the NSA's certificate file and then click **Details** and look at the **Thumbprint**). If they match, click **OK**.



The shares and folders to which Gonzo has access display. Now you can use FTP to securely transfer files to or from the NSA. Use a secure method to let your users know the correct fingerprint for the NSA's certificate so they can check it before adding a security exception.

## 4.12 Using a Mac to Access the NSA

This tutorial shows you how to find the NSA on Mac OS X 10.5 (Leopard).

You can access the NSA in two ways:

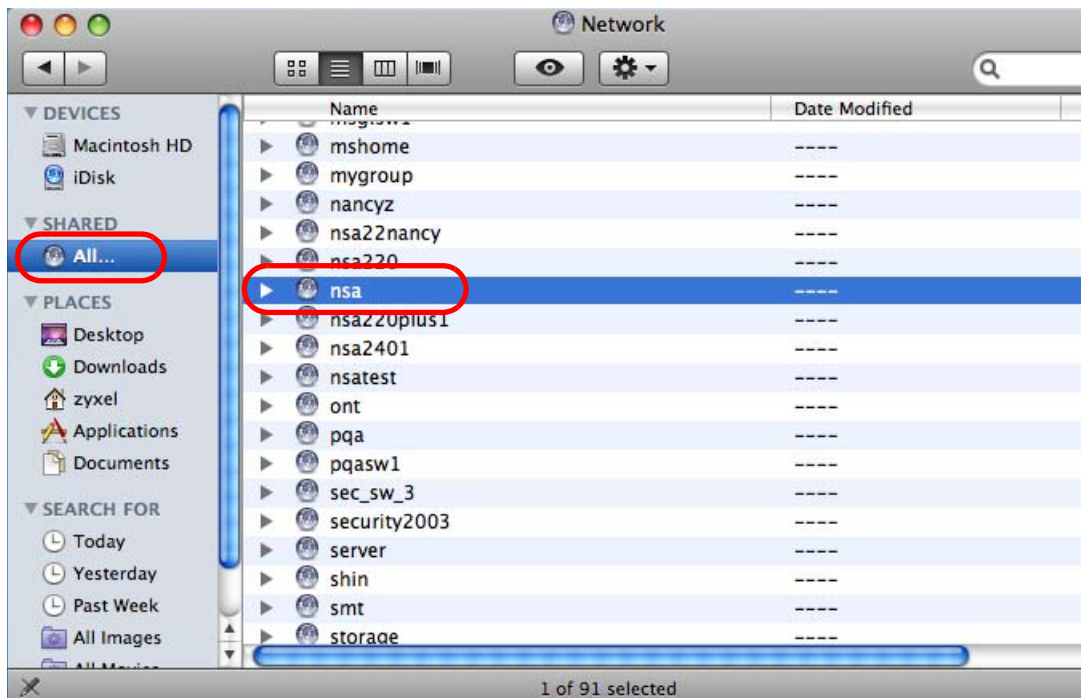
- Use the **Finder** to browse for the NSA, or
- Use the **Finder** > **Go** option to connect to the NSA.

## 4.12.1 Finder

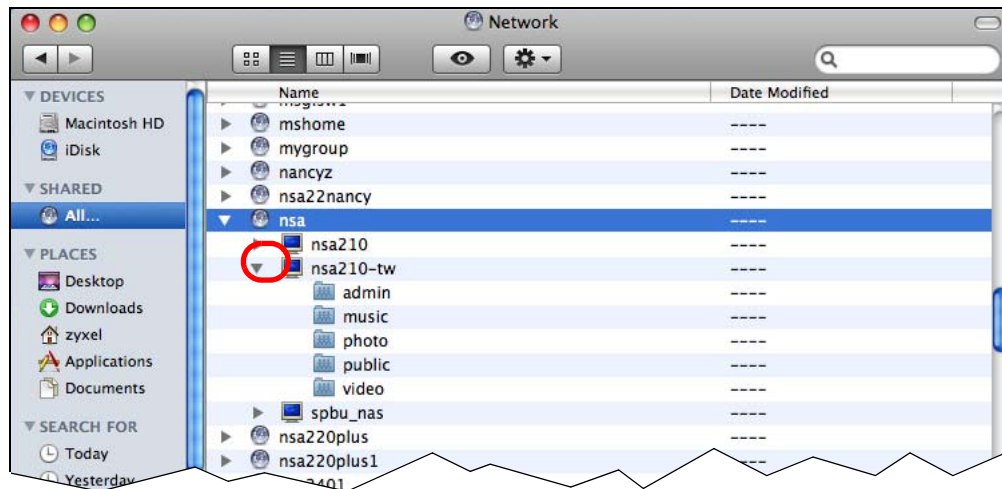
- 1 Open a new **Finder** window.



- 2 Select **All** under the **SHARED** sidebar. Look for the NSA from the **Network** list.

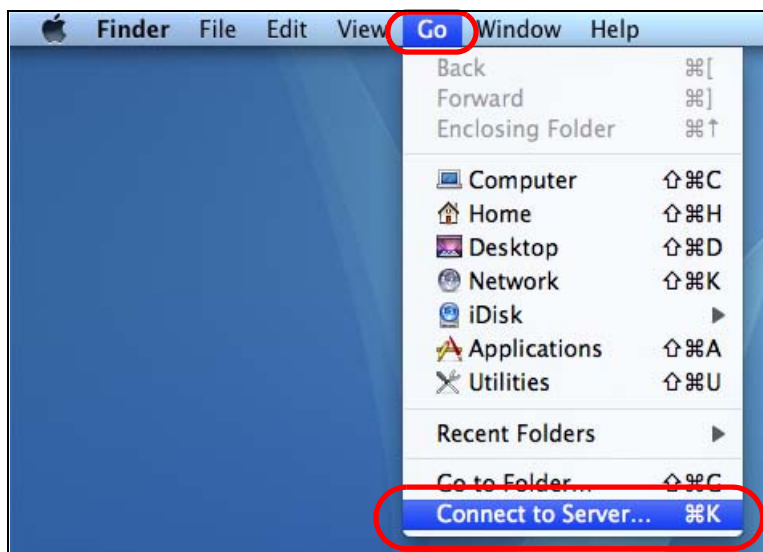


- 3 Expand the NSA to display the shares you may access.

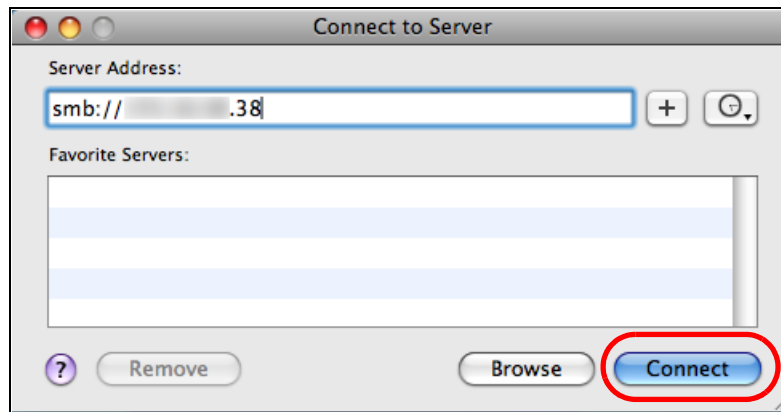


## 4.12.2 Go Menu

- 4 In the **Finder**, click **Go > Connect to Server**.



- 5 When the **Connect to Server** dialog box opens, enter `smb://` and the NSA's IP address in the **Server Address** field. You may also click **Browse** to have the Mac search for the NSA. Click **Connect**.



- 6 Once you establish the connection, you can access the NSA from the **Finder** or directly from the desktop.

## 4.13 How to Use BackupPlanner

Note: The screens and links in this section appear only after you have installed and enabled BackupPlanner. BackupPlanner is an application that you can install using Package Management (see [Chapter 10 on page 211](#).)

Use the NSA's BackupPlanner to have a backup of your files and folders.

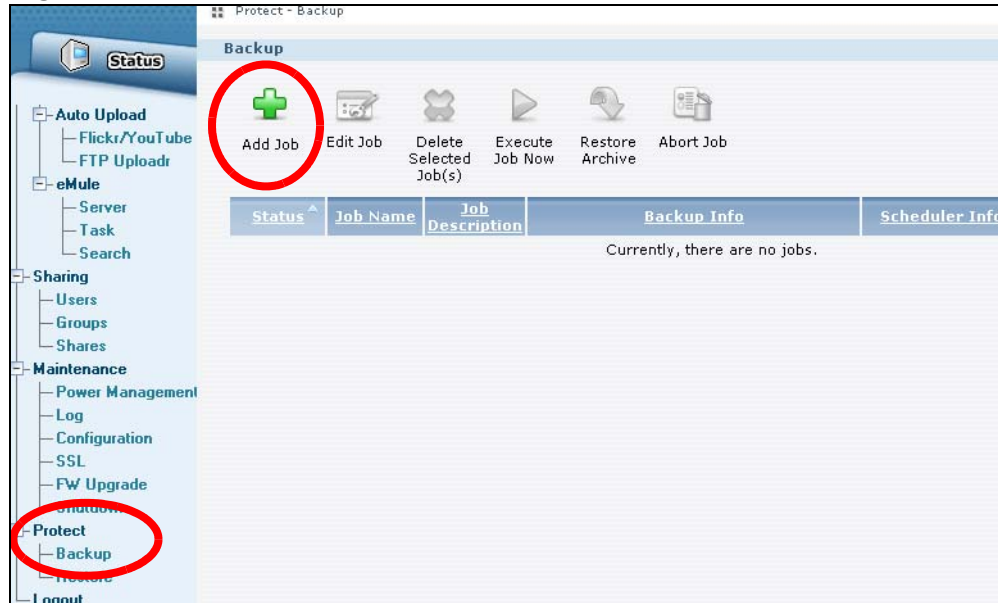
Schedule backups for times when the network is not busy (like at night or on weekends). For example, you might do daily backups of important individual files or folders and a weekly general archive. You can save backups to another location so your files can survive even if the original RAID or NSA fails.

### 4.13.1 Creating an Archive Backup

To backup the NSA every week to a remote NSA:

- 1 Click **Protect > Backup > Add Job**.

**Figure 24** Protect > Backup



- 2 Identify the backup job and select **Archive**.

New files are often added to the shares that you need to back up and existing files are not frequently changed so select **Incremental**. The NSA does a full backup first and later only copies source files that are new and/or modified since the last backup. This example sets the NSA to do another full backup after every four incremental backups.

**Figure 25** Protect > Backup > Add Job: Step 1

- 3 Select the **volume1** check box to select all the folders and files.

Select **Remote** and enter the other NSA's address, username, password, and share name.

If you want to make sure the remote NSA is reachable, click **Test Connection**.

**Figure 26** Protect > Backup > Add Job: Step 2

Protect - Backup

Add a new backup Job

Step 2

Backup Source

Volume 1

☒ Volume 1

- ☒ public
- ☒ video
- ☒ photo
- ☒ music
- ☒ admin
- ☒ Private

Selected Source Folders

Volume 1/

Backup Target

☒ Remote

Remote NSA Address: 192.168.3.2

Username: admin

Password: [masked]

Share Name: Backups

Test Connection

☐ Local

☒ External

Previous Next

- 4 In this example, the target NSA is on the LAN so leave the compression off.

Security is already configured on the target NSA so you can leave the encryption off, too.

Have the NSA keep 3 backups.

**Figure 27** Protect > Backup > Add Job: Step 3

Protect - Backup

Add a new backup Job

Step 3

**Compression**

☐ Yes

☒ No

**Encryption**

☐ Yes

☒ No

**Purge Policy**

☐ Keep All Old Backup files

☒ Keep Only the last  backup files(1-30)

☐ Keep Backups For  day(s)(1-3650)

Previous Next

- 5 Set the frequency to **Weekly**. Schedule the backup for 5:00 every Saturday morning.

Protect > Backup > Add Job: Step 4

Protect - Backup

Add a new backup Job

Step 4

**Scheduler**

Backup Frequency:

Start Time (hh:mm):  :

Every how many weeks?  (1-52)

on every ☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☒ Saturday

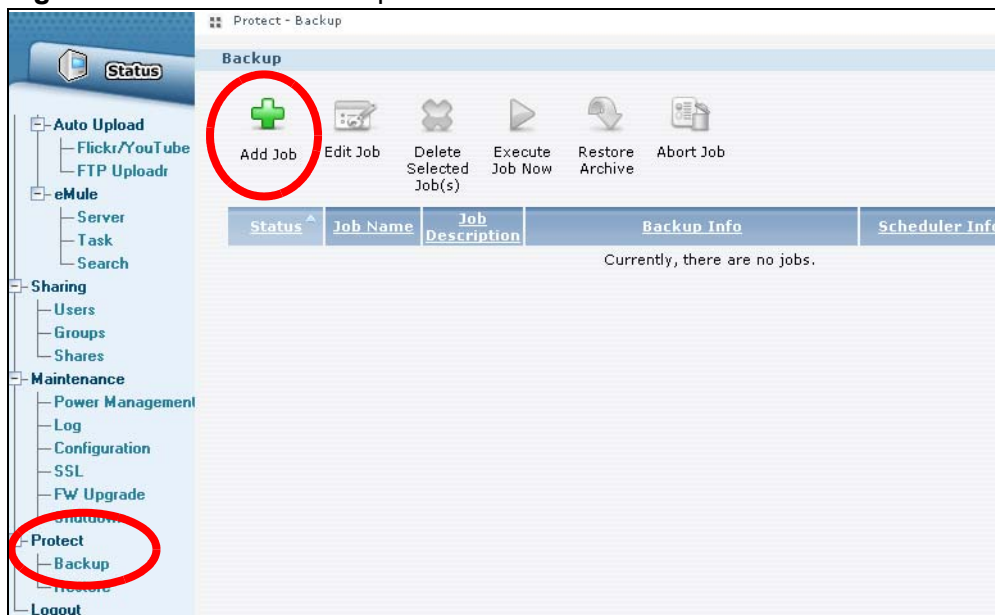
Previous Done

## 4.13.2 Creating a Synchronization Backup

To create a synchronization backup:

- 1 Click **Protect > Backup > Add Job**.

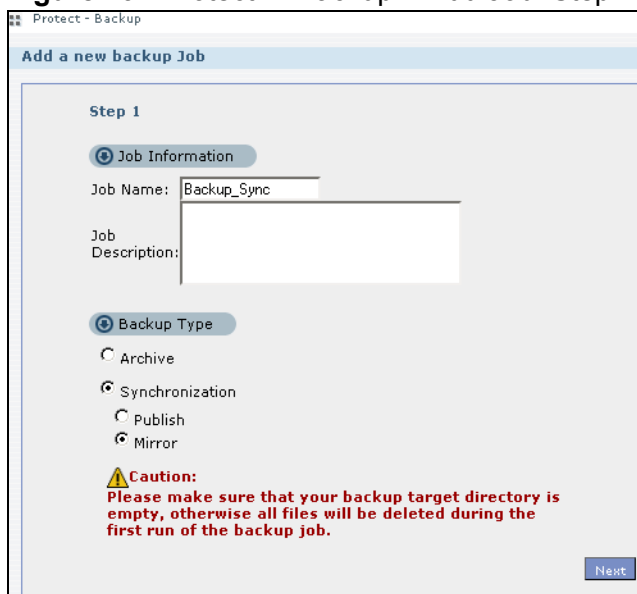
**Figure 28** Protect > Backup



Name the backup job and select **Synchronization**.

You want only your current set of files in the remote NSA's folder, so you select **Mirror** to make the target folder identical to the source folder. The NSA deletes any other files in the target folder.

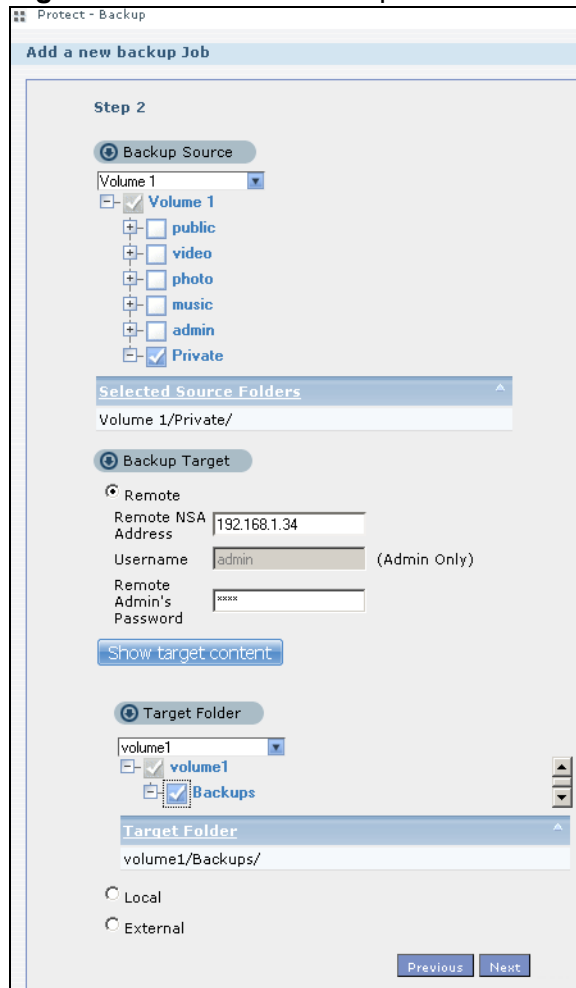
**Figure 29** Protect > Backup > Add Job: Step 1





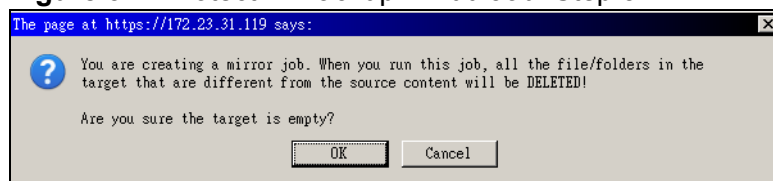
- 2 Select the folder that needs to be mirrored (your **Private** folder in this example) and **Remote**.
  - Enter the other NSA's address and administrator password.
  - Click **Show target content** to display the remote NSA's contents.
  - Select the destination on the remote NSA (**Backups** in this example).
  - Click **Next**.

**Figure 30** Protect > Backup > Add Job: Step 2



- 3 Click **OK** in the warning dialog box.

**Figure 31** Protect > Backup > Add Job: Step 3



- 4 For this example, assume the connection to the German branch office is a good one and not many files need to be backed up so leave the compression off.

- Turn on the encryption to protect these sensitive files during the transfer. The final files stored on the remote NSA will be unencrypted (usable).
- Restrict the bandwidth usage to 256 KB/s to stop the archives from using all of your network connection's available bandwidth.
- You don't have to configure a purge policy for a synchronization backup.
- Click **Next**.

**Figure 32** Protect > Backup > Add Job: Step 3

**Add a new backup Job**

Step 3

**Compression**

☐ Yes

☒ No

**Encryption**

Use Encrypted Connection

☒ Yes

☐ No

**Bandwidth**

256 KB/s (0 : No Limit)

**Purge Policy**

☐ Keep All Old Backup files

☐ Keep Only the last [ ] backup files(1-30)

☐ Keep Backups For [ ] day(s)(1-3650)

Previous Next

- 5 Schedule the backup to occur every morning at 3:00 and click **Done**.

**Figure 33** Protect > Backup > Add Job: Step 4

**Add a new backup Job**

Step 4

**Scheduler**

Backup Frequency: Daily

Start Time (hh:mm): 3:00

Every how many days? 1

Previous Done

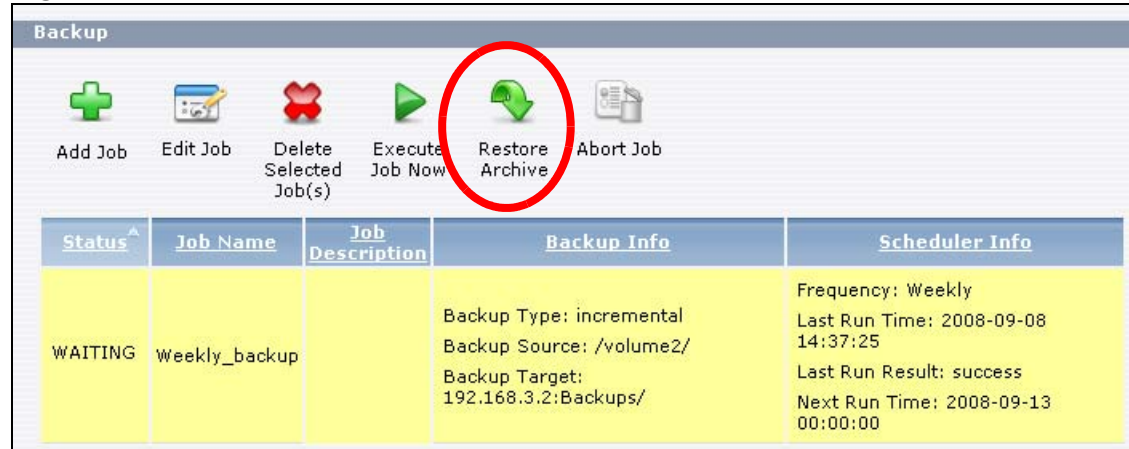
You do not need to use a special restore process to use the files a synchronization backup creates. The copy of files that the NSA creates on the other NSA's Backups share can be used directly by anyone with access to that share.

### 4.13.3 Restoring Archived Files by Backup Job

If you have backup jobs for which the NSA has already performed backups, you can restore the files based on the backup job. Do the following:

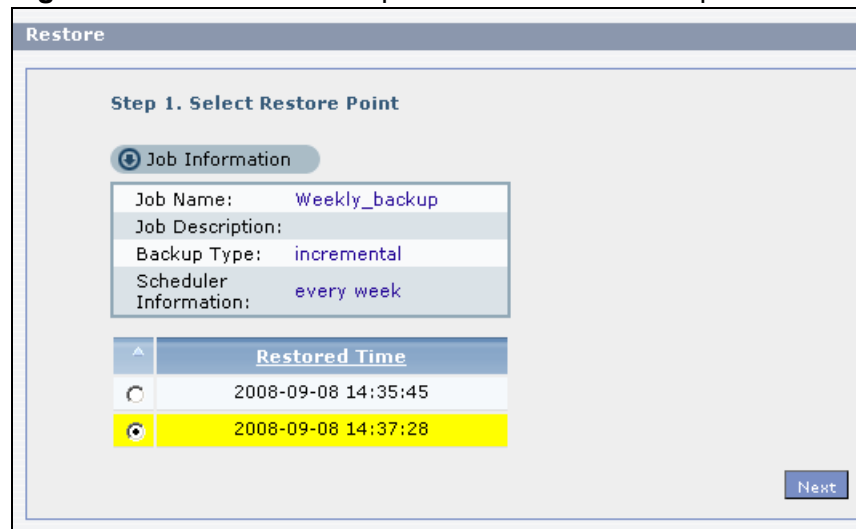
- 1 Click **Protect > Backup** screen, select a backup job and click **Restore Archive**.

**Figure 34** Protect > Backup



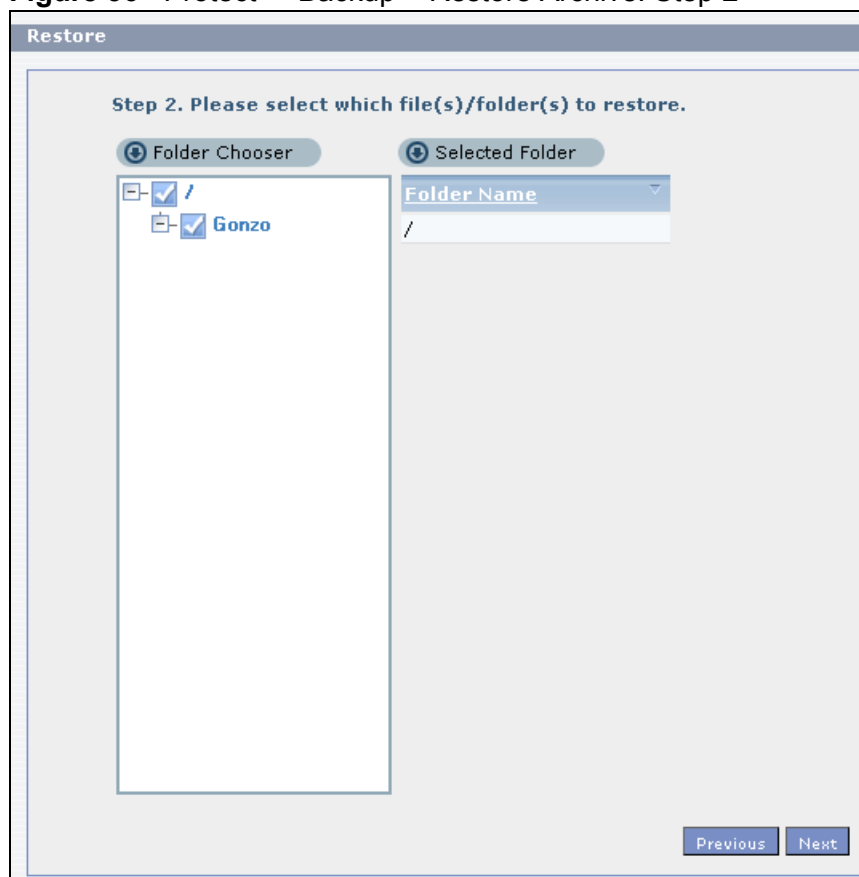
- 2 Select which backup to use and click **Next**.

**Figure 35** Protect > Backup > Restore Archive: Step 1



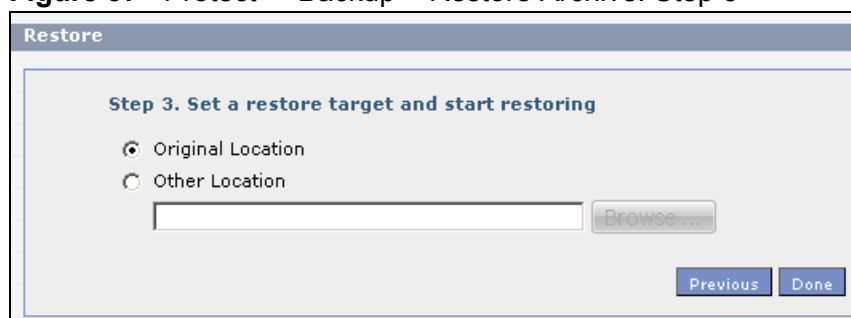
- 3 Select the share where you have stored your the backup you want to restore and click **Next**.

**Figure 36** Protect > Backup > Restore Archive: Step 2



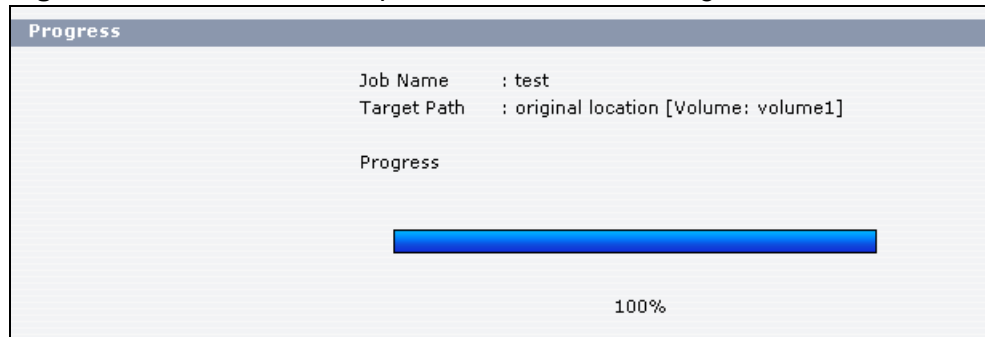
- 4 Select the original location and click **Done**.

**Figure 37** Protect > Backup > Restore Archive: Step 3



- 5 The NSA restores the files into the share. When it finishes you can access the files.

**Figure 38** Protect > Backup > Restore Archive: Progress

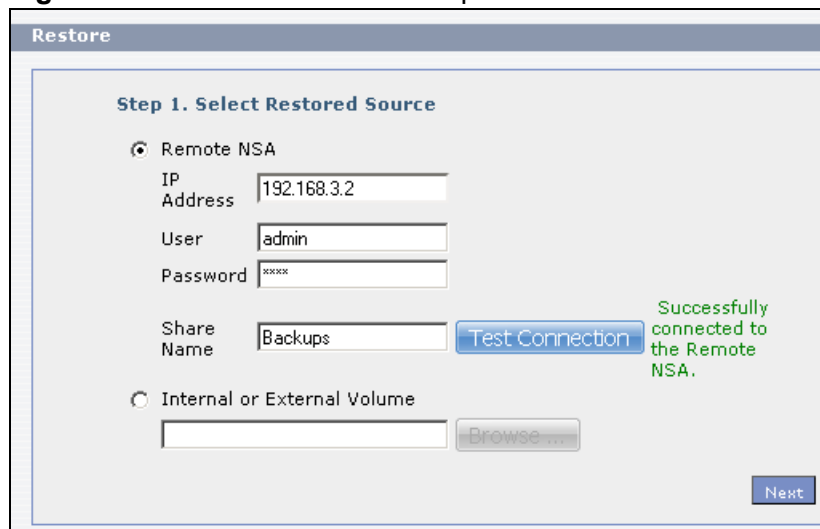


### 4.13.4 Restoring by Backup Files

If you deleted an archive backup job or the NSA or the RAID array containing the backup job failed you cannot restore archived files by the backup job. In this example, the NSA's RAID array failed. You've replaced the hard drives and re-configured the RAID. To restore by backup files:

- 1 Click **Protect > Restore**. Specify where the archive files are located. In this example, enter "192.168.3.2" as the IP address, "admin" as the account name, "1234" as the password, and "Backups" as the share name. Click **Test Connection**. Click **Next**.

**Figure 39** Protect > Restore: Step 1



- 2 Select the backup job and backup time and click **Next**.

**Figure 40** Protect > Restore: Step 2

Restore

Step 2. Select Restore Point

	Job Name
<input checked="" type="radio"/>	Weekly_backup
<input type="radio"/>	recycle

	Restored Time
<input type="radio"/>	2008-09-08 14:35:45
<input type="radio"/>	2008-09-08 14:37:28
<input checked="" type="radio"/>	2008-09-08 15:01:30

Previous Next

- 3 Select everything in the share except the recycle folder. Click **Next**.

**Figure 41** Protect > Restore: Step 3

Restore

Step 3. Please select which file(s)/folder(s) to restore.

Folder Chooser Selected Folder

Folder Name

/Gonzo/Planning/  
/Gonzo/Strategy/

Previous Next

- 4 Browse to the folder where you want to put the files. Click **Done**.

**Figure 42** Protect > Restore: Step 4

The screenshot shows a window titled "Restore". Inside, there is a section titled "Step 4. Set a restore target and start restoring". Below this title, there is a label "Path for restoring" followed by a text input field. To the right of the input field is a "Browse ..." button. Below the input field is a label "Please input encryption password if you have set to this backup job" followed by another text input field. In the bottom right corner of the dialog, there are two buttons: "Previous" and "Done".

- 5 The NSA restores the files and you can use them again.





---

# PART II

## System Setting and Features

---

System Setting (139)

Storage (145)

Network (159)

Applications (165)

Package Management (211)



# Status Screen

## 5.1 Overview

This chapter describes the **Status** screen, which is the first advanced administration screen that displays.

## 5.2 The Status Screen

Click **Administration** in the **My NSA** screens ([Section 3.5 on page 43](#)) to open the Web Configurator.

You can also view the status screen, by clicking **Status** on the top-left of the navigation panel.

**Figure 43** Status



The following table describes the labels in this screen.

**Table 16** Status

LABEL	DESCRIPTION
Status	Click this to refresh the status screen statistics.
System Information	
Server Name	This displays the name which helps you find the NSA on the network. Click the <b>Edit</b> icon to go to the screen where you can configure this.
Model Name	This displays which model this NSA device is.
Firmware Version	This is the NSA firmware version. Click the <b>Edit</b> icon to go to the <b>Maintenance &gt; FW Upgrade</b> screen from which you can upload/upgrade new firmware.
MAC Address	This displays the NSA's unique physical hardware address (MAC). You need the MAC address to register the product at myZyXEL.com. Customer support may also request it for troubleshooting purposes.
Media Server Status	This shows whether the media server function is enabled or disabled. It must be enabled for media clients to play content files stored on the NSA. Click the <b>Edit</b> icon to go to the screen where you can configure this.
FTP Server Status	This shows whether the FTP server function is enabled or disabled. It must be enabled to use FTP file transfer to/from the NSA. Click the edit icon to go to the screen where you can configure this.
Web Publishing Status	This shows whether the Web server function is enabled or disabled. It must be enabled to use HTTP to access shares on the NSA. Click the <b>Edit</b> icon to go to the screen where you can configure this.
UPS	This shows the Uninterruptible Power Supply (UPS) capacity. Click the <b>Edit</b> icon to go to the screen where you can configure this.
CPU Usage	<p>This displays a summary of CPU usage by all current processes.</p> <p>Click the <b>Refresh</b> icon to update this display. It also automatically updates itself every 10 seconds.</p> <p><b>Note:</b> If too many users are using the NSA then the NSA may appear sluggish.</p>
CPU Temperature	<p>This displays the current temperature near the NSA's CPU. The NSA generates an emergency log if the temperature goes out of the normal operating range. If the temperature goes even higher, the NSA shuts down automatically to avoid damage from overheating. If the NSA overheats, make sure the fans are working and it is in a well ventilated place.</p> <p>Click the <b>Refresh</b> icon to update this display. It also automatically updates itself every 60 seconds.</p>
Fan Speed	<p>This is the RPM (Rotations Per Minute) of the NSA's fans.</p> <p>Click the <b>Refresh</b> icon to update this display. It also automatically updates itself every 60 seconds.</p>

**Table 16** Status (continued)

LABEL	DESCRIPTION
Memory Usage	This shows how much of the NSA's total memory is being used.  Click the <b>Refresh</b> icon to update this display. It also automatically updates itself every 10 seconds.
Volume Status	A volume is a storage area on a single disk or spread across a number of disks within a single file system.
SATA Volume	This displays the volumes created on the hard drives installed in the NSA.  Click the <b>Edit</b> icon to open the <b>Storage</b> screen. You can create and edit the NSA's internal volume. See <a href="#">Chapter 7 on page 145</a> for more details.
USB Volume	This displays the volumes created on USB hard drives connected to the NSA. USB disks are numbered in the order that you insert USB devices.  Click the <b>Edit</b> icon to open the <b>Storage</b> screen. You can create and edit the external volume. See <a href="#">Chapter 7 on page 145</a> for more details.
Status	This icon indicates whether the volume is healthy, degraded, or down.
Name	This field shows the name for the volume. Read only displays for an external volume that uses Windows NTFS. This means the NSA can read the volume but can't save files on it.
Configuration	This field (also known as <b>Type</b> ) shows what type of data storage system (a RAID type or JBOD) an internal volume is using.
File System	This field shows what file system an external (USB) volume is using.
Disk(s)	For internal drives, this shows which hard drive bays are included in the volume. For external drives, this field shows <b>USB1</b> for the first external hard drive you connect to the NSA (regardless of which USB port) and <b>USB2</b> for the second.
Disk Usage	This field shows total disk size, the percentage of the disk being used and the percentage that is available.
Active Sessions	This shows how many users are currently connected to the NSA.
Type	This shows whether it's a Windows/CIFS, web (web configurator), or FTP connection to the NSA.
Share Name	This displays the shared folder name on the NSA that the user is connected to for CIFS sessions and is blank for FTP and web sessions.
Username	This displays the name of the user connected to the NSA if one is defined. <b>ANONYMOUS FTP</b> displays if a username is not defined for the user's connection.
Connected At	This displays the date and time the user last connected to the NSA in year, month, day, hour, minute, second format.
IP Address	This displays the IP address of the computer connected to the NSA.



# System Setting

## 6.1 Overview

This chapter gives an overview of the various features included in the system setting screens. You can identify your NSA on the network and set the time that the NSA follows for its scheduled tasks/logs.

## 6.2 What You Can Do

- Use the **Server Name** screen ([Section 6.4 on page 140](#)) to specify the NSA's server and workgroup names.
- Use the **Date/Time** screen ([Section 6.5 on page 141](#)) to set up date/time and choose a time zone for the NSA.

## 6.3 What You Need to Know

### Windows/CIFS

Common Internet File System (CIFS) is a standard protocol supported by most operating systems in order to share files across the network.

- CIFS is included by default in Windows operating systems.
- You can use Samba with Linux to use CIFS.
- CIFS transfers use security.

### Time Lag

Time lag occurs when the time on the NSA falls behind the time on the time server. This may happen if:

- the time server is no longer reachable
- if the NSA is shut down often (the NSA internal battery keeps time when the NSA is shut down and this may cause possible variance)

- power surges occur.

The NSA gives no warning if time lag occurs. You should resynchronize the time after a power surge or after you have shut down the NSA several times.

## 6.4 The Server Name Screen

Click **System Setting** > **Server Name** to open the following screen. Use this screen to configure your CIFS settings. In this screen you can set your server name and specify if your NSA is a part of a workgroup.

Note: CIFS cannot be disabled on the NSA.

**Figure 44** System Setting > Server Name

The following table describes the labels in these screens.

**Table 17** System Setting > Server Name

LABEL	DESCRIPTION
Server Name	Enter a name to identify your NSA on the network in this field.  You can enter up to 15 alphanumeric characters with minus signs allowed but not as the last character. The name must begin with an alphabet (a-z) and is NOT case sensitive.
Description	Add text here to describe the NSA if the <b>Server Name</b> field is not enough. Use up to 61 characters. You can use all characters except the following: / \ :   [ ] < > + ; , ? = * " ~ .
Workgroup Name	Type your workgroup name in this field. A workgroup is a group of computers on a network that can share files. These user accounts are maintained on the NSA.  You can enter up to 15 alphanumeric characters with minus signs allowed but not as the last character. The name must begin with an alphabet (a-z) and is NOT case sensitive.
Prevent NSA From Being Master Browser	Select this option if computers in your workgroup are named with non-English characters (such as Chinese and Russian). When you perform a search in the workgroup, this option allows you to locate computers named with non-English characters.



**Table 17** System Setting > Server Name (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Reset	Click this to restore previously saved settings.

## 6.5 The Date/Time Screen

Use this screen to select a time zone and a time server from which your NSA can get the time and date. This time is then used in NSA logs and alerts.

Click the **System Setting** link in the navigation panel and then click the **Date/Time** link to access the **Date/Time** screen.

**Figure 45** System Setting > Date/Time

The following table describes the labels in this screen.

**Table 18** System Setting > Date/Time

LABEL	DESCRIPTION
Current System Date Time Setting	
Current Time	This field displays the time used by your NSA for its logs and alerts.
Current Date	This field displays the date used by your NSA for its logs and alerts.
Date Time Setup	

**Table 18** System Setting > Date/Time (continued)

LABEL	DESCRIPTION
Manual	<p>Select this radio button to enter the time and date manually.</p> <p>When you enter the time settings manually, the NSA uses the new setting once you click <b>Apply</b>.</p> <p><b>Note:</b> If you enter time settings manually, they revert to their defaults when power is lost.</p>
New Date (yyyy-mm-dd)	<p>This field displays the last updated date from the time server or the last date configured manually.</p> <p>When you set <b>Time and Date Setup</b> to <b>Manual</b>, enter the new date in this field and then click <b>Apply</b>.</p>
New Time (hh:mm:ss)	<p>This field displays the last updated time from the time server or the last time configured manually.</p> <p>When you set <b>Time and Date Setup</b> to <b>Manual</b>, enter the new time in this field and then click <b>Apply</b>.</p>
Get from Time Server	<p>Select this check box to have the NSA get the time and date from the time server you select in the <b>Time Server Address</b> field.</p>
Time Server Address	<p>Select a time server from the drop-down list box or select <b>Specify my own time server</b> and enter the time server you wish to use in the field below. Check with your ISP/network administrator if you are unsure of this information.</p>
Synchronize Now	<p>Click this for the NSA to retrieve the correct time from the configured time server right away.</p>
Time Zone	
Time Zone	<p>Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).</p>
Enable Daylight Saving	<p>Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.</p> <p>Select this option if you use Daylight Saving Time.</p>
Start Date	<p>Configure the day and time when Daylight Saving Time starts if you selected <b>Enable Daylight Saving</b>. The hour field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would use <b>March, Second, Sunday</b>, at <b>2:00</b>.</p> <p>Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>March, Last, Sunday</b>. The time you specify depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>

**Table 18** System Setting > Date/Time (continued)

LABEL	DESCRIPTION
End Date	<p>Configure the day and time when Daylight Saving Time ends if you selected <b>Enable Daylight Saving</b>. The <b>o'clock</b> field uses the 24 hour format. Here are a couple of examples:</p> <p>Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select <b>November, First, Sunday</b>, at <b>2:00</b>.</p> <p>Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select <b>October, Last, Sunday</b>. The time you specify depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).</p>
Offset	Specify by how many hours to change the time for Daylight Saving Time.
Apply	Click this to save your changes. If you configured a new time and date, Time Zone and Daylight Saving at the same time, all of the settings take affect.
Cancel	Click this to restore your previously saved settings.



# Storage

## 7.1 Overview

Several NSA features require a valid internal volume. This chapter covers the management of volumes and disks (both internal and external).

## 7.2 What You Can Do

Use the **Storage** screen ([Section 7.4 on page 147](#)) to create and edit volumes in the NSA. You can view information on all volumes, create internal and external volumes, and configure the volume's properties.

## 7.3 What You Need to Know

### Disk

The NSA requires an initialized SATA (Serial Advanced Technology Attachment) hard disk to function. Refer to the Quick Start Guide for steps on how to initialize the hard disk.

SATA or Serial ATA (Advanced Technology Attachment) is a computer bus technology that allows high-speed data transfer to and from hard disks.

An eSATA (external SATA) hard disk has the same specifications as a SATA hard disk but is attached to the NSA using a cable. It can be used either to expand storage or backup data. The eSATA hard disk is optional.

You can attach one SATA and one eSATA to the NSA hard disk tray. Both SATA and eSATA hard disks are treated by the NSA as internal disks/volumes (refer to [Section 7.4.1 on page 148](#)).

The NSA can work with up to two USB hard disks. The USB-attached storage disks are treated by NSA as external disks/volumes (refer to [Section 7.4.3 on page 152](#)).

## Volume

A volume is a storage area on a disk or disks. You can create volumes on the internal disks and external disks attached to the USB port(s). You can spread a volume across internal disks but not between internal and external disks.

An internal disk/volume is the disk/volume that is physically installed in the NSA hard disk tray. The external disk/volume refers to disk drive(s) attached to NSA's USB port(s).

## Storage Methods

The NSA uses the following storage methods:

- RAID (Redundant Array of Independent Disks)
- PC Compatible Volume
- JBOD (Just a Bunch of Data)

The storage method you use depends on how many disks you have and how many volumes you want to create. It's important that you consider this carefully as all data is deleted when you re-create a volume. See [Figure 7.5.1 on page 153](#) for details on choosing a storage method.

Note: By default, the internal hard disk (SATA) you attach to the NSA is configured as JBOD and cannot be modified. You can attach a second internal hard disk (an eSATA hard disk) and configure the storage method of the internal hard disks (both SATA and eSATA).

## Finding Out More

See [Section 7.5 on page 153](#) for more technical background information on storage.

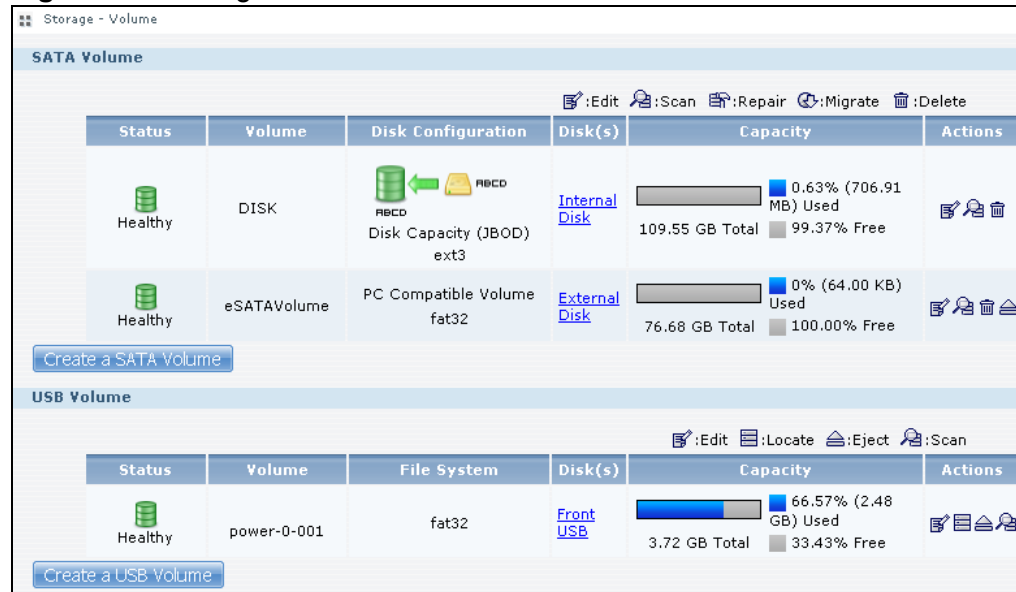
## 7.4 The Storage Screen

The **Storage** screen allows you to create and edit volumes in the NSA.

Click **Storage > Volume** in the navigation panel to display the following screen. Use this screen to display SATA (internal) and USB (external) volumes on the NSA.

Note: It is recommended to scan the volume every three months or 32 reboots.

**Figure 46** Storage > Volume



The following table describes the labels in this screen.

**Table 19** Storage > Volume

LABEL	DESCRIPTION
SATA/USB Volume	These tables display information on all internal SATA volumes (created on NSA internal disk drives) and external volumes (created on external disk drives attached to the NSA USB ports).
Create a SATA Volume	Click this to format internal hard drives and create a new volume. All data on the disk(s) will be lost.
Create a USB Volume	Click this to format an external hard drive and create a new volume. All data on the disk will be lost.
Status	This field shows whether the volume is <b>Healthy</b> , <b>Resync</b> , <b>Recovering</b> , <b>Degraded</b> , or <b>Down</b> . See <a href="#">Section 7.5.3 on page 155</a> for details on a volume's status.
Volume	The NSA creates the volume name automatically. You can edit it.
Disk Configuration	This field shows which disks and data storage system the volume is using.

**Table 19** Storage > Volume (continued)

LABEL	DESCRIPTION
File System	This field displays the file system that an external (USB) volume is using.
Disk(s)	<p>Click or roll your mouse over a link in this column to display the following details about the hard drive located in the corresponding hard drive bay.</p> <p>Type: Whether it is an internal or external (USB) hard drive.  Model Name: This is the hard disk number that identifies the disk.  File System: The file system that an external volume is using  Capacity: The total storage space on the disk.</p>
Capacity	This field shows total disk size, the percentage of the volume being used and the percentage that is available.
Actions	<p>This field displays icons allowing you to edit, scan, repair or delete a volume. You can also locate or eject an external volume.</p> <p>Note: If you delete a volume, all data in the volume disk(s) is erased.</p>

You see a warning screen before you delete a volume.

**Figure 47** Delete a Volume Warning Screen

## 7.4.1 Creating a SATA Volume

Note: An eSATA hard disk is required in order to create a SATA volume. Otherwise, the NSA shows an error “No disk is available for creating new volume.” The SATA hard disk is configured as a JBOD volume by default.





Click the **Create a SATA Volume** button in the **Storage > Volume** screen as shown in [Section 7.4 on page 147](#) to open the following screen. Use this screen to create a new NSA internal disk drive volume.

Note: Creating a volume formats the hard drive. All data on the disk will be lost.

**Figure 48** Storage > Volume > Create a SATA Volume

Disk Configuration



Volume Name  \*

**JBOD**

A JBOD volume can be a single disk volume or can be made to span across several disks into a single larger volume. It does not provide any fault tolerance or performance benefits.



Volume will be created on ☒ Internal Disk ☐ External Disk

**PC Compatible Volume**

A primary partition will be created on the disk. It can be accessed by a PC if this disk is connected to a PC which supports the selected file system.

Volume will be created on ☒ External Disk File System

**RAID1**

Provides disk mirroring. Level 1 provides twice the read transaction rate of single disks and the same write transaction rate as single disks.

Volume will be created on ☒ Internal Disk ☒ External Disk

**Note:**  
When internal disk defect in RAID1 mode, NSA210 will be in "uninitialized" state.  
You can bring NSA210 to normal state by switching external disk to internal disk.  
After login WEB GUI, you can repair the degraded RAID1 by another external disk.

The following table describes the labels in this screen.

**Table 20** Storage > Volume > Create a SATA Volume

Volume Name	<p>Type a volume name from 1 to 31 characters. To avoid confusion, it is highly recommended that each volume use a unique name.</p> <p>Acceptable characters are all alphanumeric characters, " " [spaces], "_" [underscores], and "." [periods].</p> <p>The first character must be alphanumeric (A-Z 0-9).</p> <p>The last character cannot be a space " ".</p> <p>For an external volume, type a volume name from 1 to 32 single-byte (no Chinese characters allowed for example) ASCII characters. The name cannot be the same as another existing external volume.</p>
JBOD	<p>Use this if you want maximum storage capacity and/or you have other means of protecting your data. JBOD is the only option if you only have one disk installed.</p> <p>Select which disks should make up this volume. A disk can only belong to one volume. You do not need to select anything if only one hard disk is installed.</p> <ul style="list-style-type: none"> <li>• <b>Internal Disk</b> - This refers to the hard disk you installed inside the NSA.</li> <li>• <b>External Disk</b> - This refers to the eSATA hard disk that you can attach as a second drive to your NSA.</li> </ul>
PC Compatible Volume	<p>This type is only available if you have attached an eSATA hard disk to your NSA.</p> <p>A primary partition is created on the eSATA hard disk.</p> <p>Use this to make your eSATA hard disk readable by other computer systems. However, the computer's platform (for example, Windows XP SP2) should support the file system you selected for the eSATA hard disk.</p> <ul style="list-style-type: none"> <li>• <b>External Disk</b> - This is checked automatically. It refers to the eSATA hard disk that you can attach as a second drive to your NSA.</li> <li>• <b>File System</b> - Select the file system you want the new volume to use.</li> </ul> <p>Windows file systems include:</p> <p><b>NTFS:</b> Recommended for volumes greater than 40 GB.</p> <p><b>FAT32:</b> Newer, and more efficient than FAT16. Supports a volume size of up to 32 GB (Giga Bytes) and individual file sizes of up to 4 GB.</p> <p><b>FAT16:</b> Compatible with older Windows operating systems. Supports volume and file sizes of up to 2 GB.</p> <p>Linux file systems include:</p> <p><b>EXT2:</b> Most commonly used on Linux platforms.</p> <p><b>EXT3:</b> The same as EXT2, but adds a journaled file system and is more robust.</p> <p><b>ReiserFS:</b> Offers better performance for small files.</p> <p><b>XFS:</b> Allows expansion for mounted volumes.</p>

**Table 20** Storage > Volume > Create a SATA Volume (continued)

RAID 1	Use this if you want to mirror all data on one disk to the other disk. This is only available when you have two hard disks installed (that is, the hard disk inside the NSA and an eSATA hard disk attached to the NSA.  The <b>External Disk</b> and <b>Internal Disk</b> boxes are automatically checked.
Apply	Click this to save your changes and create the volume.
Cancel	Click this to exit this screen without saving your changes or creating a volume.

Note: Once you create the first volume on the NSA, it is recommended to restart the NSA for better performance.

## 7.4.2 Editing a Volume

Click an internal volume's **Edit** icon in the **Storage > Volume** screen as shown in [Section 7.4 on page 147](#) to open the following screen. Use this screen to change the volume's name.

**Figure 49** Storage > Volume > Edit

The following table describes the labels in this screen.

**Table 21** Storage > Volume > Edit

LABEL	DESCRIPTION
Volume Name	For an internal volume, type a volume name from 1 to 31 characters. To avoid confusion, it is highly recommended that each volume use a unique name.  Acceptable characters are all alphanumeric characters and " " [spaces], "_" [underscores], and "." [periods].  The first character must be alphanumeric (A-Z, 0-9).  The last character cannot be a space " ".  For an external volume, type a volume name from 1 to 32 single-byte (no Chinese characters allowed for example) ASCII characters. The name cannot be the same as another existing external volume.
Apply	Click this to save your changes and rename the volume.
Cancel	Click this to close this screen without saving your changes.

### 7.4.3 Creating a USB Volume

Click the **Create a USB Volume** button in the **Storage > Volume** screen as shown in [Section 7.4 on page 147](#) to open the following screen. Use this screen to create a new NSA external disk drive volume.

Note: Creating a volume formats the drive. All data on the disk will be lost.

**Figure 50** Storage > Volume > Create a USB Volume

**Disk Configuration**

Volume Name  \*

Available Disk(s)

File System

**Warning: If there is any existing data on the Disk, it will be deleted to create this new Volume.**

The following table describes the labels in this screen.

**Table 22** Storage > Volume > Create a USB Volume

LABEL	DESCRIPTION
Volume Name	<p>Type a volume name from 1 to 31 characters. The name cannot be the same as another existing external volume.</p> <p>Acceptable characters are all alphanumeric characters and " " [spaces], "_" [underscores], and "." [periods].</p> <p>The first character must be alphanumeric (A-Z 0-9).</p> <p>The last character cannot be a space " ".</p>
Available Disk(s)	Select the external (USB) device upon which you want to create the volume.
File System	<p>Select the file system you want the new volume to use.</p> <p>Windows file systems</p> <p><b>NTFS:</b> Recommended for volumes greater than 40 GB.</p> <p><b>FAT32:</b> Newer, and more efficient than FAT16. Supports a volume size of up to 2 TB (Tera Bytes) and individual file sizes of up to 4 GB.</p> <p><b>FAT16:</b> Compatible with older Windows operating systems. Supports volume and file sizes of up to 2 GB.</p> <p>Linux file systems</p> <p><b>EXT2:</b> Most commonly used on Linux platforms.</p> <p><b>EXT3:</b> The same as EXT2, but adds a journaled file system and is more robust.</p> <p><b>ReiserFS:</b> Offers better performance for small files.</p> <p><b>XFS:</b> Allows expansion for mounted volumes.</p>

**Table 22** Storage > Volume > Create a USB Volume (continued)

LABEL	DESCRIPTION
Apply	Click this to save your changes and create the volume.
Cancel	Click this to exit this screen without saving changes.

## 7.5 Storage Technical Reference

This section provides some background information about the topics covered in this chapter.

### 7.5.1 Choosing a Storage Method for a Volume

The following is a guide to help you choose a storage method for the various number of disks supported on the NSA. See [Section 7.5.2 on page 154](#) for theoretical background on JBOD and the RAID levels used on the NSA. Typical applications for each method are also shown there.

#### One Disk

If you only have one disk, you must use JBOD. All disk space is used for your data - none is used for backup. If the disk fails, then you lose all the data on that volume (disk). You can add another disk to your one-disk JBOD volume later without having to re-create shares, access rights, and so on. Alternatively, you could create a different JBOD volume if you install a second disk. (and create new shares, access rights and so on).

#### Two Disks:

You may choose JBOD, PC Compatible Volume or RAID 1. With two disks you could create:

- up to two JBOD volumes
- one PC Compatible volume + one JBOD
- one RAID 1 volume
  - Choose JBOD for flexibility and maximum usage of disk space for data.
  - Choose RAID 1 if data security is more important than performance. Since RAID 1 mirrors data onto a second disk, you can recover all data even if one disk fails.

## 7.5.2 Storage Methods

This section contains theoretical background on JBOD, PC Compatible Volume and the RAID levels used on the NSA. Redundant Array of Independent Disks (RAID) is a method of storing data on multiple disks to provide a combination of greater capacity, reliability, and/or speed.

These are some terms that you need to know in order to understand storage systems.

- **Mirroring**

In a RAID system using mirroring, all data in the system is written simultaneously to two hard disks instead of one. This provides 100% data redundancy as if one disk fails the other has the duplicated data. Mirroring setups always require an even number of drives.

- **Duplexing**

Like in mirroring, all data is duplicated onto two distinct physical hard drives but in addition it also duplicates the hardware that controls the two hard drives (one of the drives would be connected to one adapter and the other to a second adapter).

### RAID 1

RAID 1 creates an exact copy (or mirror) of a set of data on another disk. This is useful when data backup is more important than data capacity. The following figure shows two disks in a single RAID 1 volume with mirrored data. Data is duplicated across two disks, so if one disk fails, there is still a copy of the data.

**Table 23** RAID 1

A1	A1
A2	A2
A3	A3
A4	A4
DISK 1	DISK 2

As RAID 1 uses mirroring and duplexing, a RAID 1 volume needs an even number of disks (two or four for the NSA).

RAID 1 capacity is limited to the size of the smallest disk in the RAID array. For example, if you have two disks of sizes 150 GB and 200 GB respectively in one RAID 1 volume, then the maximum capacity is 150 GB and the remaining space (50 GB) is unused.

Typical applications for RAID 1 are those requiring high fault tolerance without need of large amounts of storage capacity or top performance, for example, accounting and financial data, small database systems, and enterprise servers.

### RAID 1 and Data Protection

If a hard disk fails and you're using a RAID 1 volume, then your data will still be available (but at degraded speeds until you replace the hard disk that failed and resynchronize the volume). However, RAID cannot protect against file corruption, virus attacks, files incorrectly deleted or modified, or the NSA malfunctioning. Here are some suggestions for helping to protect your data.

- Place the NSA behind a hardware-based firewall. It should have stateful packet inspection, IDP (Intrusion Detection and Prevention), and anti-virus (like ZyXEL's ZyWALL UTM products for example).
- Use anti-virus software on your computer to scan files from others before saving the files on the NSA.

Keep another copy of important files (preferably in another location).

## 7.5.3 Volume Status

You (the administrator) can see the status of a volume in the **Status** or **Storage** screens.

The NSA has the following classifications for the status of a volume:

- **Healthy** if all disks in the volume are OK and the file system is functioning properly.
- **OK** means the USB connected device is functioning properly.
- **Resync** when you create a RAID 1 volume.
- **Recovering** appears when repairing a RAID 1 volume. (A RAID 1 volume was once degraded, but you have installed a new disk and the NSA is restoring the RAID 1 volume to a healthy state.)
- **Degraded** when a volume is currently down, but can be fixed. Data access may be slower from a degraded volume, so it's recommended that you replace the faulty disk and repair the volume as soon as you can.
- **Inactive** when a disk is missing from a two-disk JBOD volume. The volume is unusable. If you removed one of the disks you should be able to re-install it and use the volume again (as long as you did not change anything on the disk). If a disk has failed, you need to replace it and re-create the whole volume. All data will be lost. See page [339](#) for how to install or replace a hard drive.
- **Down** when a volume is down and can not be fixed.

A down RAID volume cannot be used until you repair or replace the faulty disk(s) in the volume. Degraded means one of the disks in the RAID volume is not

available but the volume can still be used. For a degraded volume, you should replace the faulty disk as soon as possible to obtain previous performance. See your Quick Start Guide for more information on replacing a disk.

If it's down, then the only indication is that you can no longer transfer files to/from the shares in the down volume.

Note: There is no explicit message from CIFS that tells users their volume is degraded or down.

## 7.5.4 Volumes and RAID

Note: Back up your data before deleting or re-creating a volume!

If you originally have one disk configured as JBOD, and you then install another disk and want to configure the two disks to use RAID 1, you should first back up all your data on the two disks (see the Memeo Autobackup utility on the included CD) and then restore your data later after you create the new volume type.

Below is a table that summarizes some attributes of RAID 1 as supported on the NSA. For capacity and storage efficiency, "S" is the size of the smallest drive in the array, and "N" is the number of drives in the array.

Performance rankings are approximations.

**Table 24** RAID 1 Quick Overview

RAID Level	1
Number of Disks	2
Capacity	$S \cdot N / 2$
Storage Efficiency	50%
Fault Tolerance	YYYY
Availability	YYYY
Read Performance	YYY
Write Performance	YYY

## 7.5.5 Disk Replacement Restrictions

Note: If you're using RAID 1 and the hard disk inside the NSA fails but the eSATA hard disk is still working, you can remove the hard disk inside the NSA and install the eSATA hard disk inside the NSA. Your NSA runs normally again, but you will need to have another eSATA hard disk attached to the NSA in order to employ RAID 1.



See the Quick Start Guide for information on replacing disks in the NSA. When replacing a disk in a degraded or down RAID volume, the new disk must be at least the same size or bigger than the other disks that are already in the RAID volume, so as all data in the volume can be restored.

For example, if you have RAID with 250 GB disks, you must put in a 250 GB or bigger disk as a replacement in order to restore all original data in that volume. If you put a bigger disk, the extra space on the disk will not be used.

Note: The NSA automatically repairs a degraded RAID if you insert an empty disk without an existing file system. Otherwise, when you replace a disk you must go to the **Storage > Internal Volume > RAID** screen, select the degraded array, and click **Repair**.

### Resynchronizing or Recovering a RAID 1 Volume

Resynchronizing or recovering a RAID 1 volume that was down is done block-by-block, so the time it takes depends more on the size of your hard drive(s) than the amount of data you have on them.

Note: Do not restart the NSA while the NSA is resynchronizing or recovering a volume as this will cause the synchronization to begin again after the NSA fully reboots.

You can access data on a RAID volume while it is resynchronizing or recovering, but it is not recommended.

## 7.5.6 External Disks

You may connect USB storage devices that support the following file systems to the NSA.

- Windows File Systems: NTFS, FAT32 and FAT16.
- Linux File Systems: ReiserFS, EXT2, EXT3, and XFS.



# Network

## 8.1 Overview

This chapter discusses the network configuration screens. The **Network** screens allow you to configure TCP/IP and PPPoE settings for the NSA.

## 8.2 What You Can Do

- Use the **TCP/IP** screen ([Section 8.4 on page 161](#)) to assign the NSA a dynamic or static IP address and DNS information
- Use the **PPPoE** screen ([Section 8.5 on page 163](#)) to configure PPPoE settings for a direct Internet connection.

## 8.3 What You Need to Know

### IP Address

The NSA needs an IP address to communicate with other devices on your network. The NSA can get an IP address automatically if you have a device on your network that gives them out. Or you can assign the NSA a static (fixed) IP address.

### DNS Server Address

A DNS (Domain Name System) server maps domain names (like [www.zyxel.com](http://www.zyxel.com)) to their corresponding numerical IP addresses. This lets you use domain names to access web sites without having to know their IP addresses. The NSA can receive the IP address of a DNS server automatically (along with the NSA's own IP address). You can also manually enter a DNS server IP address in the NSA.

### Jumbo Frames

Jumbo frames are Ethernet frames larger than 1500 bytes. They enable data transfer with less overhead. The bigger the frame, the better the network

performance. Your network equipment such as computers, switches and routers must be capable of supporting jumbo frames. You also need to enable jumbo frames in all related network devices.

## PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) allows the NSA to establish a direct Internet connection if you do not have a router. PPPoE is a dial-up connection. You need a username and password from your Internet Service Provider (ISP) to set up the connection.

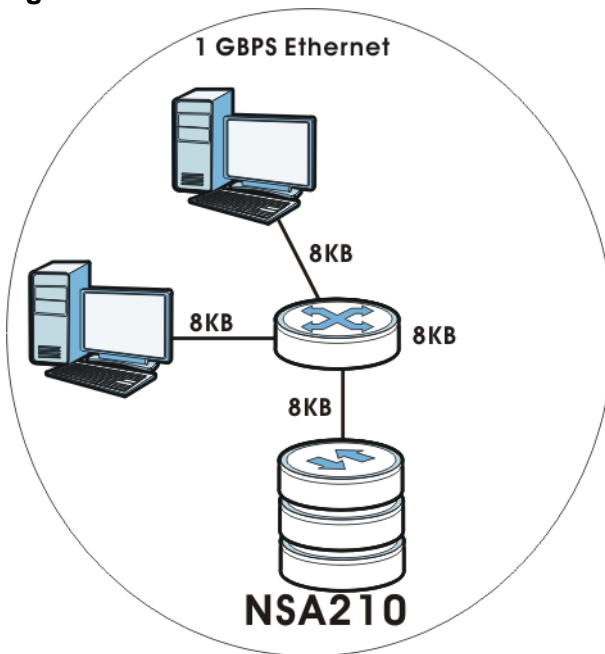
## Jumbo Frames

To use jumbo frames, your LAN must support 1 Gbps transmissions (Gigabit Ethernet). All of your network devices (computer Ethernet cards and switches, hubs, or routers) must also support the same size of jumbo frames that you specify in the NSA.

**Note:** If you enable jumbo frames on the NSA in a network that does not support them, you will lose access to the NSA. If this occurs, you will have to restore the factory default configuration. Push the **RESET** button on the NSA's rear panel and release it after you hear a beep.

In the following example, the NSA has jumbo frames enabled and set to 8KB frames. This means the computer, notebook computer, and switch must also have jumbo frames enabled and be capable of supporting 8KB frames.

**Figure 51** Jumbo Frames



## 8.4 The TCP/IP Screen

Use the **TCP/IP** screen to have the NSA use a dynamic or static IP address, subnet mask, default gateway and DNS servers.

Click **Network > TCP/IP** in the navigation panel to open the following screen.

Note: If you change the NSA's IP address, you need to log in again after you apply changes.

**Figure 52** Network > TCP/IP

**IP Address**

☒ Dynamic  
☐ Static

IP Address: 172.23.37.52  
 IP Subnet Mask: 255.255.255.0  
 Default Gateway: 172.23.37.254

**DNS**

☒ Dynamic  
☐ Static

Primary DNS Server: 172.23.5.2  
 Secondary DNS Server: 172.23.5.1

**HTTP (Web Configurator)**

☐ Enable Another HTTP Web Configuration Port  
 Port Number:

**Jumbo Frames**

☒ Disabled  
☐ Enabled  
☐ 4KB  
☐ 8KB  
☒ 9KB

**Caution:**  
 Jumbo Frame is supported in 1 Gbps and higher mode only. Please make sure your host, switch hub, and router support Jumbo Frames

**Network Diagnostic Tool**

Host: a.root-servers.net Ping...

Apply Reset

The following table describes the labels in this screen.

**Table 25** Network > TCP/IP

LABEL	DESCRIPTION
IP Address	
Dynamic	<p>Select this option to have the NSA get IP address information automatically.</p> <p>If no IP address information is assigned, the NSA uses Auto-IP to assign itself an IP address and subnet mask. For example, you could connect the NSA directly to your computer. If the computer is also set to get an IP address automatically, the computer and the NSA will choose addresses for themselves and be able to communicate.</p>
Static	Select this option for the NSA to use fixed TCP/IP information. You must fill in the following fields.
IP Address	Type an IP address in this field.
IP Subnet Mask	Type an IP subnet mask in this field.
Default Gateway	Type a default gateway address in this field.
DNS	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. If you have the IP address(es) of the DNS server(s), enter them.
Dynamic	Select the option to have the NSA get a DNS server address automatically.
Static	Select this option to choose a static DNS server address. Type the DNS server IP address(es) into the fields below.
Primary DNS Server	Type a primary DNS server IP address.
Secondary DNS Server	Type a secondary DNS server IP address.
HTTP (Web Configurator)	
Enable Another Web Configuration Port	Select this to configure an additional HTTP port for accessing the web configurator. Specify a number in the <b>Port Number</b> field.
Jumbo Frames	<p>Jumbo frames improve network performance. You must have a 1 Gbps (Gigabit Ethernet) network that supports jumbo frames. Select the largest size of frame that all of your network devices (including computer Ethernet cards and switches, hubs, or routers) support.</p> <p>When enabled, you can choose between <b>4 KB</b>, <b>8 KB</b>, and <b>9 KB</b> frame sizes.</p> <p>Note: If you enable jumbo frames on the NSA in a network that does not support them, you will lose access to the NSA. If this occurs, you will have to restore the factory default configuration. Push the <b>RESET</b> button on the NSA's rear panel and release it after you hear a beep.</p>

**Table 25** Network > TCP/IP (continued)

LABEL	DESCRIPTION
Network Diagnostic Tool	Use this section to test the network connection to a particular IP address or domain name. Select an address or type it into the field. Then click <b>Ping</b> to have the NSA send a packet to test the network connection. <ul style="list-style-type: none"> <li>• <b>Successfully pinged host</b> - The NSA is able to “ping” the host, the network connection is OK.</li> <li>• <b>Unable to ping host</b> - The NSA is able to “ping” the selected host.</li> </ul>
Apply	Click this to save your TCP/IP configurations. After you click <b>Apply</b> , the NSA restarts. Wait until you see the <b>Login</b> screen or until the NSA fully boots and then use the NAS Starter Utility to rediscover it.
Reset	Click this to restore your previously saved settings.

## 8.5 The PPPoE Screen

Use this screen to configure PPPoE settings for a direct Internet connection.

Click **Network > PPPoE** in the navigation panel to open the following screen.

PPPoE allows the NSA to establish a direct Internet connection.

**Figure 53** Network > PPPoE

Network - PPPoE

**Status**

Status	Disabled
IP Address	N/A
IP Subnet Mask	N/A

**Configuration**

Enable PPPoE to directly connect to the Internet.

☐ Enable PPPoE Connection

Username

Password

Password (Confirm)

Apply Reset

The following table describes the labels in this screen.

**Table 26** Network > PPPoE

LABEL	DESCRIPTION
Status	
Status	This field displays the status of PPPoE connection.
IP Address	This field displays the IP address of your PPPoE connection.
IP Subnet Mask	This field displays the IP subnet mask of your PPPoE connection.
Configuration	
Enable PPPoE Connection	Select this option to establish a direct Internet connection for the NSA. You need to enter the username and password as given by your ISP.
Username	Enter the username exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the username above.
Password (Confirm)	Retype the password for confirmation.
Apply	Click this to save your changes.
Reset	Click this to restore previously saved settings.



# Applications

## 9.1 Overview

This chapter discusses the features in the **Application** screens. The NSA contains various applications for file sharing and downloading.

## 9.2 What You Can Do

- Use the **FTP** screen ([Section 9.4 on page 167](#)) to configure settings for FTP file transfers to/from the NSA.
- Use the **Media Server** screen ([Section 9.5 on page 170](#)) to share files with media clients.
- Use the **Download Service** screen ([Section 9.6 on page 171](#)) to download files from the Internet.
- Use the **Web Publishing** screen ([Section 9.7 on page 184](#)) to publish shares for people to access files using a web browser.
- Use the **Broadcatching** screen ([Section 9.8 on page 186](#)) to download frequently updated digital content like TV programs, radio talk shows, Podcasts (audio files), and blogs.
- Use the **Print Server** screen ([Section 9.9 on page 194](#)) to share a printer.
- Use the **Copy/Sync Button** screen ([Section 9.10 on page 196](#)) to transfer files between a USB device and the NSA.

## 9.3 What You Need to Know

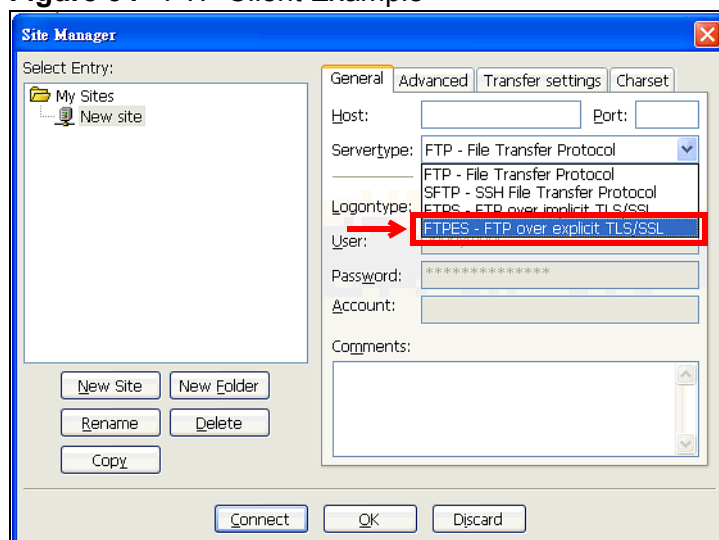
### FTP

File Transfer Protocol (FTP) is a file transfer service that operates on the Internet. A system running the FTP server accepts commands from a system running an FTP client. FTP is not a secure protocol. Your file transfers could be subject to snooping.

## FTPES (File Transfer Protocol over Explicit TLS/SSL)

File Transfer Protocol over Explicit TLS/SSL (FTPES) is a file transfer service that uses either TLS (Transport Layer Security) or SSL (Secure Sockets Layer) for secure transfers across the Internet. It requests for a mutual method of encryption from the FTP server for its file transfer sessions. Your FTP client must be set to use FTPES as in the following example.

**Figure 54** FTP Client Example



## Media Server

The media server feature lets anyone on your network play video, music, and photos from the NSA (without having to copy them to another computer). The NSA can function as a DLNA-compliant media server and/or an iTunes server. The NSA streams files to DLNA-compliant media clients or computers using iTunes. The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

## iTunes Server

The NSA iTunes server feature lets you use Apple's iTunes software on a computer to play music and video files stored on the NSA. You can download iTunes from [www.apple.com](http://www.apple.com).

## Download Service

The NSA's download service downloads files from the Internet directly to the NSA. You do not have to download to your computer and then copy to the NSA. This can free up your computer's system resources.

The NSA can download using these protocols.

- HTTP: The standard protocol for web pages.
- FTP: A standard Internet file transfer service.
- BitTorrent: A popular distributed peer-to-peer files sharing protocol.

### **BitTorrent**

The NSA includes a BitTorrent client for fast downloading and sharing of large files (such as educational public domain videos). With BitTorrent, you share while you're downloading the file. BitTorrent breaks up the file and distributes it in hundreds of chunks. You start sharing the file as soon as you have downloaded a single chunk.

### **Web Publishing**

Web publishing lets you "publish" shares (containing folders and files) on the NSA so people can access the files using a web browser without having to log into the My NSA screens. This way you can share files with others without them having to know and enter a username and password.

For example, if you want to share photos in a FamilyPhotos share, you could "web publish" it and others could use a web browser to access the photos at <http://my-NSA's-IP-Address/MyWeb/FamilyPhotos>.

### **Broadcatching**

Broadcatching is the downloading of digital content from Internet feeds. Use broadcatching to have the NSA download frequently updated digital content like TV programs, radio shows, podcasts (audio files), and blogs.

### **RSS**

RSS (Really Simple Syndication) is a format for delivering frequently updated digital content. A channel uses a feed to deliver its contents (items). Subscribe the NSA to a feed to be able to download the contents.

## **9.4 The FTP Screen**

Use FTP or FTPES (FTP over Explicit TLS/SSL) to upload files to the NSA and download files from the NSA. Click **Applications > FTP** to open the following screen.

**Figure 55** Applications > FTP

**FTP**

☒ Enable FTP

Connection Limit: 10 Connection Limit: 20

Idle Timeout: 15 minutes Max timeout: 300 minutes

Port Number: 21

☒ Enable Anonymous FTP Access

☒ Customize the port range for data transfer.

Starting Port:  \*

Ending Port:  \*

☒ Download / Upload Rate For All Users (include admin)

☐ Max. Download Rate: 0 KB/s (0=No Limit)

☐ Max. Upload Rate: 0 KB/s (0=No Limit)

☐ Download / Upload Rate For Anonymous Users

☐ Max. Download Rate: 0 KB/s (0=No Limit)

☐ Max. Upload Rate: 0 KB/s (0=No Limit)

**Note:**  
To configure a share to allow anonymous FTP access go to the configure shares page and modify a share's access rights to allow the user 'Anonymous FTP'.

**Character Set**

(UTF-8)

**Note:**  
The NSA uses UTF-8 format for FTP by default. If the NSA's folders or file names do not display correctly in your FTP client, select the appropriate character set here.

Apply Reset

The following table describes the labels in this screen.

**Table 27** Applications > FTP

LABEL	DESCRIPTION
FTP	
Enable FTP	You can use FTP to send files to the NSA or get files from the NSA. Select this check box to allow users to connect to the NSA via FTP; otherwise clear the check box.
Connection Limit	Enter the maximum number of concurrent FTP connections allowed on the NSA in this field. The connection limit is 20.
Idle Timeout	Enter the length of time that an FTP connection can be idle before timing out. The timeout limit is 300 minutes.
Port Number	This is the port number used by the NSA for FTP traffic.
Enable Anonymous FTP Access	Select this check box to allow any user to log into the NSA using 'FTP' or 'anonymous' as a username and no password. Any other name is considered a username, so must be valid and have a corresponding correct password.
Customize the port range for data transfer	<p>Select this check box to assign a port range for FTP clients to use when downloading files from the NSA using passive mode.</p> <p>The connection limit is restricted to half of the port numbers within the range if this value is smaller than the one configured in the <b>Connection Limit</b> field. For example, you specified a port range from 1024 to 1029 and configured 10 in the <b>Connection Limit</b> field. The FTP connection limit will only be 3 (6 ports in the range divided by 2) because it is the smaller value.</p>

**Table 27** Applications > FTP

LABEL	DESCRIPTION
Starting Port	Enter the first port number in the range. Choose from 1024 to 65535.
Ending Port	Enter the last port number in the range. Choose from 1024 to 65535.
Download/Upload Rate For All Users (include admin)	<p>Select this if you want to limit the download/upload bandwidth for all users who are logged into the NSA, including the administrator.</p> <ul style="list-style-type: none"> <li>• <b>Max. Download Rate</b> - Enter the download speed (in kilobytes/s) that the NSA allows for users who are logged into the NSA.</li> <li>• <b>Max. Upload Rate</b> - Enter the upload speed (in kilobytes/s) that the NSA allows for users who are logged into the NSA.</li> </ul>
Download/Upload Rate For Anonymous Users	<p>Select this if you want to limit the download/upload bandwidth for users who log into the NSA using 'FTP' or 'anonymous' as a username and no password.</p> <ul style="list-style-type: none"> <li>• <b>Max. Download Rate</b> - Enter the download speed (in kilobytes/s) that the NSA allows for users who are logged into the NSA.</li> <li>• <b>Max. Upload Rate</b> - Enter the upload speed (in kilobytes/s) that the NSA allows for users who are logged into the NSA.</li> </ul>
Character Set	<p>The NSA uses UTF-8 (8-bit UCS/Unicode Transformation Format) format for FTP by default. If the NSA's folders, or file names do not display correctly in your FTP client, select the appropriate language encoding here.</p> <p>This setting applies to all FTP client connections to the NSA. It does not affect your Windows/CIFS connections (it will not correct the character display in Windows Explorer).</p>
Apply	Click this to save your changes.
Reset	Click this to restore your previously saved settings.

## 9.5 The Media Server Screen

The **Media Server** screen allows you to share files with media clients.

Click **Applications > Media Server** to open the following screen. Use this screen to turn the media server and/or iTunes server on or off and select shares to publish (share with media clients like iTunes).

**Figure 56** Applications > Media Server



The following table describes the labels in this screen.

**Table 28** Applications > Media Server

LABEL	DESCRIPTION
Media Server	
Media Server Name	This is the name of the NSA media server on the network. It is the same as the NSA's server name. This name lets media clients distinguish between multiple media servers on your network.
Disable / Enable Media Server	Turn on the media server to let (DLNA-compliant) media clients on your network play media files located in the published shares. See <a href="#">Section 18.4 on page 368</a> for the multimedia file formats iTunes supports.
Rebuild Database	This option is available when you select <b>Enable Media Server</b> . Select this option to repair the files on the media server. For example, if the NSA got disconnected while downloading or uploading files, it might corrupt some files on the media server.
Unpublished Shares	This list box displays the shares that the NSA does not share with the media clients.
Publish Selected Share(s)	Select shares in the <b>Unpublished Shares</b> box and click this to share the shares with media clients. Use the [SHIFT] key to select a range of entries. Hold down the [CTRL] key to select multiple individual entries.

**Table 28** Applications > Media Server

LABEL	DESCRIPTION
Published Shares	This list box displays the shares that the NSA shares with the media clients.
Unpublish Selected Share(s)	Select shares in the <b>Published Shares</b> box and click this to not share the shares with media clients. Use the [SHIFT] key to select a range of entries. Hold down the [CTRL] key to select multiple individual entries.
Enable iTunes Server	Check this to let anyone on your network use iTunes to play music and video files in the published shares.
Enable SqueezeCenter	This is available if the <b>SqueezeCenter</b> application is installed using <b>Package Management</b> (see <a href="#">Section 10.4 on page 212</a> ).  Check this to enable <b>SqueezeCenter</b> .
Apply	Click this to save your changes.
Reset	Click this to restore your previously saved settings.

## 9.6 The Download Service Screen

The Download Service screen allows you to download files from the Internet.

Click **Applications > Download Service** to open the following screen. Use this screen to manage the NSA's file downloads.

Note: By default, the NSA saves downloads in the **admin** share's **download** folder.

**Figure 57** Applications > Download Service

**Download Service**

Download service allows you to download files from the Internet directly to the NSA.

☒ Enable Download Service  ☐ Enable Download Notify


■ :Downloading  
■ :Seeding  
 Total : ■ 39.61 KB / ■ --

Active (3) | Inactive (0) | Completed (1) | Error (0)

Status	Name	Complete(%)	Seeds	Peers	Download Speed	Upload Speed	Time Left	Priority
<span style="color: green;">■</span>	BR20090511.zip	0.06 %	3957(380)	0(0) [Downloading]	--	--	--	Auto
<span style="color: green;">■</span>	Anti-Diabetes (Type1) He...	0.54 %	531(55)	176(196) [81.9980]	39.61 KB/s	--	43:25:55	Auto


The following table describes the labels in this screen.

**Table 29** Applications > Download Service

LABEL	DESCRIPTION
Enable Download Service	Use this option (and click the <b>Apply</b> button) to turn the download service off or on. If you turn off the service, all downloads are paused. Files currently downloading are queued. Turning on the download service resumes downloads (or restarts them if they are not able to resume).
Enable Download Notify	Use this option (and click the <b>Apply</b> button) to turn the download service notification off or on. See <a href="#">Section 9.11.4 on page 200</a> for more details about this feature.
	At the time of writing, the NSA supports RSS 2.0 feeds.  Click this to get and subscribe to the NSA channel feed. This enables you to keep track and download the NSA's new contents (items).
Add	After you find a file to download, copy the file's URL. Then log into the NSA web configurator and go to the <b>Applications &gt; Download Server</b> screen and click this button. A screen opens where you create a new download task. You can paste the file's URL or use a BitTorrent file.
Preferences	Click this to open a screen where you can set the default location for saving downloads and configure your BitTorrent settings.
Refresh	Click this to update the information displayed on the screen.
Delete	To delete download tasks (or manually clear out completed download tasks), select a download task and click this to remove it from the list. A pop-up screen asks you to confirm. Click <b>Apply</b> to delete or <b>Cancel</b> to quit. When you delete a download task, you are given the option to delete the associated files. Selecting this option deletes a downloaded file and in the case of a BitTorrent download task, also deletes the related .torrent file.  Use your keyboard's [SHIFT] key to select a range of download tasks. Use the [CTRL] key and click individual download tasks to select multiple individual download tasks.
Pause	Select a downloading item and click this to temporarily stop the download. Paused downloads appear in the <b>Download Service</b> screen's <b>Inactive tab</b> .  Use your keyboard's [SHIFT] key to select a range of download tasks. Use the [CTRL] key and click individual download tasks to select multiple individual download tasks.
Resume	Select a paused item and click this to continue downloading the file.  Select a completed item and click this to re-seed a torrent file or download a file again. If you want to re-seed a BitTorrent task, keep the torrent file and the completed file in their original locations.
Task Info	Select an item on the list and click this to display information about the download task. See <a href="#">Section 9.6.5 on page 183</a> for more details.
The table lists your downloads. Click a column's heading to sort the entries by that criteria.	



**Table 29** Applications > Download Service (continued)

LABEL	DESCRIPTION
Active	<p>Click this to see the list of files the NSA is currently downloading or sharing with other BitTorrent users. The NSA handles a maximum of 10 active tasks at a time (or fewer depending on how much of the NSA's system memory is available). If you add more, they appear in the <b>Inactive</b> tab.</p> <p>BitTorrent downloads may appear in the <b>Inactive</b> tab for a while before showing in the <b>Downloading</b> tab. The NSA automatically moves completed tasks to the <b>Completed</b> tab.</p>
Inactive	Click this to see the list of files that are queued (waiting in line) for the NSA to download or the downloads that have been manually paused.
Completed	<p>Click this to see the list of files that the NSA has finished downloading.</p> <p>The <b>Location</b> column shows where a downloaded file is saved on the NSA. Click on the location link to open the share browser and access the file.</p>
Error	Click this to see the list of files that the NSA was not able to download. The NSA automatically retries unsuccessful download attempts. The download displays in the error tab when the re-attempts are also unsuccessful and the NSA stops trying to download the file. To try the download again, use the <b>Add</b> button to create a new download task.
Status	<p>The following icons show the download's status.</p>  <p><b>Completed:</b> The NSA has downloaded the whole file.</p> <p><b>Seeding:</b> The download is finished and the NSA is allowing other BitTorrent users to download it.</p> <p><b>Downloading:</b> The NSA is getting the file.</p> <p><b>Queued:</b> The download is waiting in line for the NSA to download it.</p> <p><b>Pause:</b> The download has been manually stopped. Select it and click <b>Resume</b> to continue it.</p> <p><b>Error:</b> The NSA was not able to complete the download. Select it and click <b>Resume</b> to reattempt the download.</p>
Name	This identifies the download file. A "... " indicates an abbreviated name. Hold your cursor over the name to display the full name.
Complete (%)	This is the percentage of the file that the NSA has downloaded.
Location	<p>This appears in the <b>Completed</b> tab.</p> <p>It displays the path for where the file is saved. Click on the location link to open the share browser and access the file.</p>

**Table 29** Applications > Download Service (continued)

LABEL	DESCRIPTION
Seeds	<p>Seeds apply to BitTorrent downloads. This is the number of computers that are sharing the complete file that you are downloading.</p> <p>This value is in the format "Leeches(Seeds)" where Leeches refer to peers that do not have a complete copy of the file yet and are still downloading; Seeds refer to peers that have the complete file.</p>
Peers	<p>Peers apply to BitTorrent downloads. This is the number of other computers that are also downloading (and sharing) the file you are downloading.</p> <p>This value is in the format "ConnectedPeers(AllPeers)[Health]" where Connected Peers is the number of computers to which the NSA is connected in order to download the file; AllPeers refer to the total number of computers to which the NSA can connect in order to download the file; Health indicates the availability of the file.</p>
Download Speed	<p>This is how fast the NSA is getting the file.</p> <p>It is normal for a BitTorrent download to start out with a slow download speed since it has to set up numerous connections. The speed should increase as the download progresses and decrease near the end of the download.</p>
Upload Speed	This is how fast the NSA is sending the file to other BitTorrent users.
Time Left	This is how much longer (in hours, minutes, and seconds) it should take to finish the download at the current download speed.
Priority	This is the download's priority on the NSA. You can set a currently downloading or queued download to high or automatic priority. You can set a download to high priority to have the NSA try to download it before the other files. However the actual download speed depends more on factors like the speed of you Internet connection, the speed of the download source's Internet connection, how many others are trying to download at the same time, the peers and seeds available and general network conditions.
Error Code	<p>This appears in the <b>Error</b> tab.</p> <p>This shows the tag for the error that occurred.</p>
Error Message	<p>This appears in the <b>Error</b> tab.</p> <p>This message states what went wrong with the download.</p>

## 9.6.1 Adding a Download Task

Click **Applications > Download Service > Add** to open the following screen. Use this screen to specify a file for the NSA to download. [Section 4.5 on page 77](#) provides a tutorial on adding a download task.

**Figure 58** Applications > Download Service > Add

**Add Download Task From URL**

**Source**

☒ URL  \*

☐ Torrent File

**Location of Downloaded Files**

	Share	Path
Put incomplete downloads in	admin	/download
Move completed downloads to	public	/

**Note:**

1. BitTorrent jobs are stored in /public/incoming.
2. HTTP/FTP jobs are stored in /public.
3. All jobs triggered by RSS channels create the subfolder in /public using the channel name where it store all files downloaded from that channel.

**Caution:**

Do not use the NSA for illegal downloads. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws and will bear the consequences of any infringements thereof. ZyXEL takes NO responsibility or liability for your use of the download service feature.

The following table describes the labels in this screen.

**Table 30** Applications > Download Service > Add

LABEL	DESCRIPTION
Source	
URL	<p>Paste the URL of the file you want to download into this field. The URL can be for an HTTP, FTP, or BitTorrent download.</p> <p>For a BitTorrent download, you can copy and paste the URL of the .torrent file. The NSA will automatically download the .torrent file and use it. You do not have to manually download the .torrent file or save it to your computer.</p> <p><b>Note:</b> Make sure the link opens either the file you want or a pop-up window about how to handle the file.</p> <p>It is also OK for the link to open a .torrent file. If you are redirected to a screen that says the download should start in a few seconds, there may be a link to click if the download does not start automatically. See if that link opens the file or the pop-up window.</p>
Torrent File	<p>A "torrent" file has information the NSA uses to do a BitTorrent download. A torrent file uses a .torrent extension. If you already have a torrent file saved on your computer, select the <b>Torrent File</b> option and specify its path or click <b>Browse</b> and look for its location.</p>

**Table 30** Applications > Download Service > Add

LABEL	DESCRIPTION
Location of Downloaded Files	<p>This shows where the NSA stores new downloads (<b>Put incomplete downloads in</b>) and where the NSA moves completed downloads (<b>Move completed downloads to</b>).</p> <p>The <b>Share</b> column shows the name of the share where the file is downloaded.</p> <p>The <b>Path</b> column points to the location in the share where the NSA will save the downloaded files.</p> <ul style="list-style-type: none"> <li>• BitTorrent jobs are stored in /*/incoming (where '*' is a folder that you have set.)</li> <li>• HTTP/FTP jobs are stored in /* (where '*' is a folder that you have set.)</li> <li>• All jobs triggered by RSS channels create the subfolder in /* using the channel name where it store all files downloaded from that channel (where '*' is a folder that you have set.)</li> </ul>
Edit	<p>Click this to open the following screen where you can set the default folder location where you "<b>Put incomplete downloads in</b>" and "<b>Move complete downloads to</b>".</p> <div data-bbox="760 835 1235 1146"> </div> <ul style="list-style-type: none"> <li>• <b>Share</b> - Select the share from the list.</li> <li>• <b>Path</b> - Type the folder location in the share directly or click <b>Browse</b> to open the following screen and navigate to the file's location.</li> </ul> <div data-bbox="607 1283 1421 1537"> </div> <ul style="list-style-type: none"> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Folder Name</b> - Enter a new folder name and click  to create it.</li> <li>• <b>Type</b> - This identifies the item as a folder or file.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Select a folder. If you don't select a folder, a forward slash (/) displays in the <b>Path</b> field. All contents within the specified share are automatically selected.</p> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>

**Table 30** Applications > Download Service > Add

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

## 9.6.2 Configuring General Settings

Click **Applications > Download Service > Preferences** to open the following screen. Use this screen to set the default location for saving downloads and configure the download period.

**Figure 59** Applications > Download Service > Preferences > General Settings

The screenshot shows the 'Preferences' dialog box with the 'General Settings' tab selected. The 'BitTorrent' sub-tab is also active. The 'Location of Downloaded Files' section contains a table with two rows: 'Put incomplete downloads in' and 'Move completed downloads to'. The first row has 'admin' for the share and '/download' for the path. The second row has 'public' for the share and '/' for the path. Below the table is an 'Edit' button. A 'Note' section follows, containing three numbered points: 1. BitTorrent jobs are stored in /public/incoming. 2. HTTP/FTP jobs are stored in /public. 3. All jobs triggered by RSS channels create the subfolder in /public using the channel name where it store all files downloaded from that channel. The 'Download Period Control' section has an unchecked checkbox 'Enable Download Period Control'. Below it, a text label says 'Download Service is active in the specified time period (hh:mm - hh:mm)'. There are two time pickers, each showing '00:00', separated by a minus sign. At the bottom of the dialog are 'Apply', 'Reset', and 'Cancel' buttons.

	Share	Path
Put incomplete downloads in	admin	/download
Move completed downloads to	public	/

**Note:**

1. BitTorrent jobs are stored in /public/incoming.
2. HTTP/FTP jobs are stored in /public.
3. All jobs triggered by RSS channels create the subfolder in /public using the channel name where it store all files downloaded from that channel.

**Download Period Control**

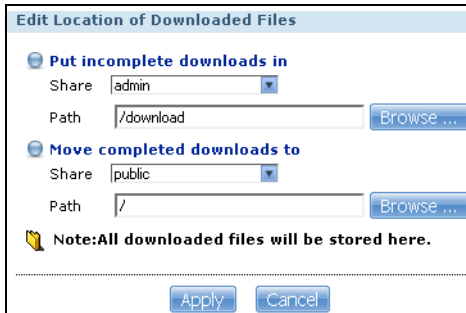
☐ Enable Download Period Control

Download Service is active in the specified time period (hh:mm - hh:mm)

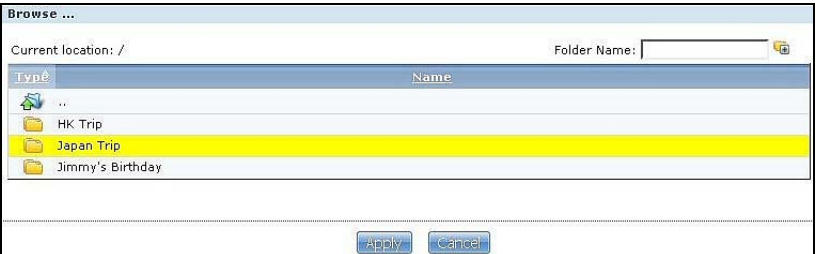

00:00 - 00:00

The following table describes the labels in this screen.

**Table 31** Applications > Download Service > Preferences > General Settings

LABEL	DESCRIPTION
Location of Downloaded Files	<p>This shows where the NSA stores new downloads (<b>Put incomplete downloads in</b>) and where the NSA moves completed downloads (<b>Move completed downloads to</b>).</p> <p>The <b>Share</b> column shows the name of the share where the file is downloaded.</p> <p>The <b>Path</b> column points to the location in the share where the NSA will save the downloaded files.</p> <ul style="list-style-type: none"> <li>• BitTorrent jobs are stored in /*/incoming (where '*' is a folder that you have set.)</li> <li>• HTTP/FTP jobs are stored in /* (where '*' is a folder that you have set.)</li> <li>• All jobs triggered by RSS channels create the subfolder in /* using the channel name where it store all files downloaded from that channel (where '*' is a folder that you have set.)</li> </ul>
Edit	<p>Click this to open the following screen where you can set the default folder location where you "<b>Put incomplete downloads in</b>" and "<b>Move complete downloads to</b>".</p> <div data-bbox="761 892 1224 1203">  </div> <ul style="list-style-type: none"> <li>• <b>Share</b> - Select the share from the list.</li> <li>• <b>Path</b> - Type the folder location in the share directly or click <b>Browse</b> to open the following screen and navigate to the file's location.</li> </ul>

**Table 31** Applications > Download Service > Preferences > General Settings

LABEL	DESCRIPTION
	 <ul style="list-style-type: none"> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Folder Name</b> - Enter a new folder name and click  to create it.</li> <li>• <b>Type</b> - This identifies the item as a file or folder.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Select a folder. If you don't select a folder, a forward slash (/) displays in the <b>Path</b> field. All contents within the specified share are automatically selected.</p> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>
Download Period Control	This feature sets the NSA to download files only within a specified time period.
Enable Download Period Control	Use the check box to turn the download period control on or off.
Download Service is active in the time period (hh:mm - hh:mm)	<p>Specify the time period for the NSA to download files.</p> <p><b>Note:</b> If you also configured the <b>Power On/Off Schedule</b> feature in the <b>Power Management</b> screen, make sure your active download period does not conflict with the power-off period.</p>
Apply	Click this to save your changes.
Reset	Click this to restore your previously saved settings.
Cancel	Click this to return to the previous screen without saving.

## 9.6.3 Configuring the BitTorrent Settings

Click **Applications > Download Service > Preferences > BitTorrent** to open the following screen. Use this screen to configure BitTorrent settings.

**Figure 60** Applications > Download Service > Preferences > BitTorrent

**Preferences**

General Settings BitTorrent

**Note:**  
For Distributed Hash Table (DHT) support, the BitTorrent service will also attempt to open the following UDP port: 9089

Port Number

Max. download rate  KB/s (0=No Limit)

Max. upload rate  KB/s (0=No Limit)

Maximum Number of Active Torrents

Maximum Number of Seeding Jobs

Maximum Number of Active Connections

Keep Sharing While:

☐ Upload/Download Ratio is  % (Enter -1 for unlimited ratio. Enter 0 to ignore ratio.)

☒ Or Seeding Time is  minutes (Enter -1 for unlimited seeding time. Enter 0 to ignore seeding time.)

Edit IP Filter

Apply Reset Cancel

The following table describes the labels in this screen.

**Table 32** Applications > Download Service > Preferences > BitTorrent

LABEL	DESCRIPTION
Port Number	Assign a port number for BitTorrent downloads. You can select a number from 2 to 65536. It is recommended to use a port number greater than 1025.
Max. download rate	You may need to limit the bandwidth the NSA uses for BitTorrent downloads if your network's other Internet applications are not getting enough downstream bandwidth. 0 has the NSA impose no restriction.
Max. upload rate	<p>You may need to limit the bandwidth the NSA uses to share files through BitTorrent if your network's other Internet applications are not getting enough upstream bandwidth. 0 has the NSA impose no restriction.</p> <p>If you do not allow any uploads, (for example, you set a limit of 1 KB/s) you will not have a good standing in the BitTorrent community.</p> <p>Note: The settings for maximum download/upload rates would not affect peers accessing the NSA from the same LAN.</p>
Maximum Number of Active Torrents	Specify how many simultaneous BitTorrent downloads are allowed on the NSA. You can enter a number from 1 to 10.
Maximum Number of Seeding Jobs	Specify how many simultaneous seeds are allowed on the NSA. Enter a number from 1 to 10. This value cannot exceed the one you configured in the <b>Maximum Number of Active Torrents</b> field.



**Table 32** Applications > Download Service > Preferences > BitTorrent

LABEL	DESCRIPTION
Maximum Number of Active Connections	Specify how many active connections are allowed on the NSA. Enter a number from 1 to 500. This specifies the number of computers that can connect to the NSA to download files being shared by the NSA.
Keep Sharing While	<p>With BitTorrent, the NSA starts sharing a file while you are downloading it. Set how long to continue sharing a file after the NSA finishes the download.</p> <p>Select <b>Upload/Download Ratio</b> to keep sharing a file until the NSA has uploaded a specific percent compared to the download.</p> <p>Select <b>Seeding Time</b> to keep sharing a file for a specific number of minutes after the download finishes.</p> <p>Continuing to share a file helps other BitTorrent users finish downloading it. Sharing out at least as much as you download helps keep you in good standing in the BitTorrent community.</p> <p>Enter -1 to share a file indefinitely. Leave both check boxes blank to have the NSA stop sharing the file as soon as the download finishes.</p> <p>If you select both options, the NSA keeps sharing a file until both conditions exceed the values you configure. For example, you entered 150% in the <b>Upload/Download Ratio</b> field and 120 minutes in the <b>Seeding Time</b> field. The NSA keeps sharing a file until it has shared 1.5 times the size of the file and has passed 120 minutes.</p>
Edit IP Filter	<p>Click this to enable or disable IP filtering for BitTorrent downloads.</p> <p>Refer to <a href="#">Section 9.6.4 on page 181</a> for information about the fields in this screen.</p>
Apply	Click this to save your changes.
Reset	Click this to restore your previously saved settings.
Cancel	Click this to return to the previous screen without saving.

## 9.6.4 Edit IP Filter

Use this screen to enable or disable IP filtering for BitTorrent downloads. IP filtering blocks IP addresses known to share fake files. You can either get an IP filter table from a website or use your own table.

Click **Enable IP Filter** in the **Applications > Download Service > Preferences > BitTorrent** screen.

**Figure 61** Applications > Download Service > Preferences > BitTorrent

The following table describes the labels in this screen.

**Table 33** Applications > Download Service > Preferences > BitTorrent > Edit IP Filter

LABEL	DESCRIPTION
Enable IP Filter	Click this to enable or disable IP filtering for BitTorrent downloads.
Update IP Filter Table File from the Internet Every Week	Select this option and enter a URL to use an online IP filter table. You can find an online IP filter table in websites such as <a href="http://www.bluetack.co.uk/config/level1.gz">http://www.bluetack.co.uk/config/level1.gz</a> .  When you change the URL of the online IP filter table, the NSA also performs an update after you click <b>Apply</b> .
Upload IP Filter Table	Select this option to upload your own IP filter table. Use the <b>Browse</b> button to locate the file and click <b>Upload</b> to save it on the NSA.  The NSA supports .txt, .dat, .gz, .tgz, and .tar.gz file extensions. The NSA saves the IP filter table as <b>/admin/download/ipfilter.dat</b> .
Download Current IP Filter Table	Click this to save a copy of the IP filter table on your computer.
Apply	Click <b>Apply</b> to update the IP filter table from the specified URL.
Cancel	Click this to return to the previous screen without saving.

## 9.6.5 Displaying the Task Information

Select an item on the list and click **Task Info**. Use this screen to check detailed information about the task.

**Figure 62** Applications > Download Service > Task Info

**Task Info**

**Detailed Information**

Status: Pause

Name: Christmas Adventure Screensaver (Christmas Adventure Screensaver [mininova].torrent) (BT)

Size: 3.42 MB

Uploaded/Downloaded Ratio: NaN (0.00 Bytes/0.00 Bytes)

Complete(%): 0.00 %

Seeds: --

Peers: --

Download Speed: --

Upload Speed: --

Health: 0.000000

Time Left: --

Priority: Auto

Comment: Auto-generated torrent by Mininova

Start Time: 2008-Dec-03 17:11:14

Completed On: 1970-Jan-01 08:00:00

Info-Hash: 52c15b1ba6daa21aac1516145e68c26a2be0c59f

Tracker: --

Close

The following table describes the labels in this screen.

**Table 34** Applications > Download Service > Task Info

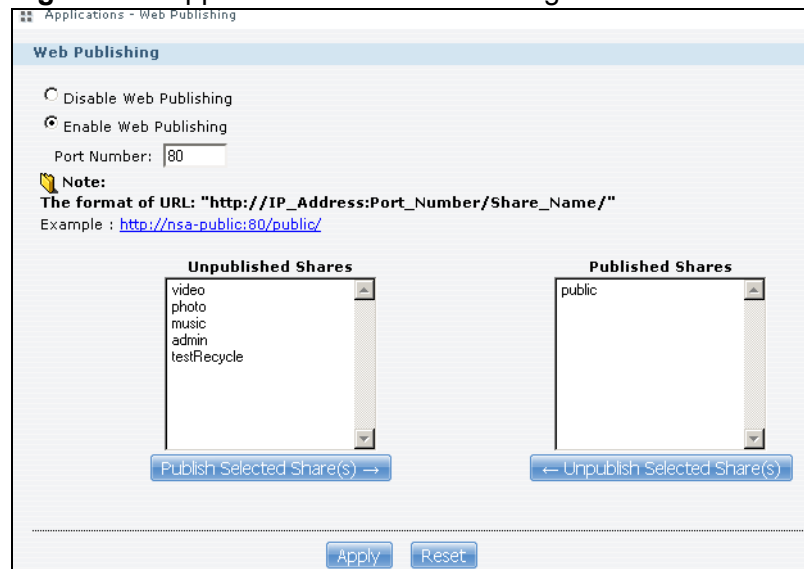
LABEL	DESCRIPTION
Status	This is the current status of the task.
Name	This is the name of the task.
Size	This is the size of the file to be downloaded.
Uploaded/ Downloaded Ratio	This is the ratio of total uploaded data to downloaded data.
Complete(%)	This field displays how much has been downloaded to the NSA.
Seeds	This is the number of computers that are sharing the complete file that you are downloading.
Peers	This is the number of other computers that are also downloading (and sharing) the file you are downloading.
Download Speed	This field displays how fast the NSA downloads the file.
Upload Speed	This field displays how fast the NSA uploads the file.
Health	This field displays how many full copies of the file are available for this task. The NSA can download a file with a higher health value more efficiently. If the health value is less than 1 (0.65 for example), there is no full copy of the file, and the NSA may not be able to complete downloading the file.

**Table 34** Applications > Download Service > Task Info

LABEL	DESCRIPTION
Time Left	This is the time remaining to complete the task.
Priority	Use this field to set the priority for downloading the task.  Select <b>Auto</b> to have the NSA automatically determine the task's priority.  Select <b>High</b> to have the NSA download this file before the other files.
Comment	Enter a description for this task. Click <b>Apply</b> to save the description.
Start Time	This field displays when the NSA started to download files.
Completed on	This field displays when the file was successfully downloaded to the NSA.
Info-Hash	This information is used to verify the torrent file.
Tracker	This field displays the tracker that NSA is currently connected to. A tracker is a server used for finding peers sharing the file.
Close	Click this to close the screen.

## 9.7 The Web Publishing Screen

Use this screen to turn web publishing on or off and select shares to publish. Click **Applications > Web Publishing** to open the following screen.

**Figure 63** Applications > Web Publishing

The following table describes the labels in this screen.

**Table 35** Applications > Web Publishing

LABEL	DESCRIPTION
Web Publishing	
Disable / Enable Web Publishing	Turn on web publishing to let people access files in the published shares using a web browser, without having to log into the My NSA screens.
Port Number	Specify a port number for accessing the published share websites hosted on the NSA. If you enter a number other than 80, make sure you include it when telling others how to access the web-published share. For example, say you specified port 8080, the NSA's IP address is 192.168.1.23, and the name of the web-published share is FamilyPhotos. You would have to enter "http://192.168.1.23:8080/MyWeb/FamilyPhotos/" in your browser's address bar to access the share's web page.
Unpublished Shares	This list box displays the shares that the NSA does not publish for web browser access.
Publish Selected Share(s)	Select shares in the <b>Unpublished Shares</b> box and click this to let people access files in the published shares using a web browser, without logging into the My NSA screens. Use the [SHIFT] key to select a range of entries. Hold down the [CTRL] key to select multiple individual entries.
Published Shares	This list box displays the shares people can access using a web browser, without logging into the My NSA screens.
Unpublish Selected Share(s)	Select shares in the <b>Published Shares</b> box and click this to not let people access using a web browser without logging into the My NSA screens. Use the [SHIFT] key to select a range of entries. Hold down the [CTRL] key to select multiple individual entries.
Apply	Click this to save your changes.
Reset	Click this to restore your previously saved settings.

Note: If you installed **php-MySQL-phpMyAdmin** through the **Package Management** screen ([Section 10.4 on page 212](#)) and enable it, you can use PHP and MySQL in your published web page.

## 9.8 The Broadcatching Screen

This screen displays the NSA's subscribed channels and the associated contents.

- The NSA saves a channel's downloaded items in a folder named after the channel.
- The NSA creates the channel folders in the same destination as the download service. See [Section 9.6.2 on page 177](#) to change the destination for saving downloads.
- The NSA's media server feature makes it easy for users on your network to play the broadcatching files you download. See [Section 9.11.1 on page 197](#) for more on the media server.
- If you add a channel that contains a torrent file, the NSA downloads the torrent file (.torrent) and transfers it to **Download Service** ([Section 9.6 on page 171](#)) and start the BitTorrent download task accordingly.





Click **Applications > Broadcatching** to open the following screen.



**Figure 64** Applications > Broadcatching










Applications - Broadcatching

### Broadcatching

Broadcatching has the NSA download frequently updated digital contents like TV programs, radio talk shows, Podcasts (audio files) and blogs with RSS feeds.


 Add Channel
  Delete Channel
  Refresh Channel
  Edit Channel

 :Start downloading  :Delete Item

Channel Name	Item Name	Published Date	Description	Actions
C&D Top 10 Podcast	<input checked="" type="checkbox"/> May 13, 2009 (...)	2009-05-13 15:03	Signs you're immature.	
Top 3 Results	<input checked="" type="checkbox"/> May 13, 2009 (...)	2009-05-13 15:02	Signs you're immature.	
	<input checked="" type="checkbox"/> May 13, 2009 (...)	2009-05-13 15:01	Signs you're immature.	
	<input checked="" type="checkbox"/> May 13, 2009 (...)	2009-05-13 15:00	Signs you're immature.	
	<input checked="" type="checkbox"/> May 12, 2009 (...)	2009-05-12 13:41	Signs that you partied too much, too long, too hard.	
	<input checked="" type="checkbox"/> May 12, 2009 (...)	2009-05-12 13:40	Signs that you partied too much, too long, too hard.	
	<input checked="" type="checkbox"/> May 12, 2009 (...)	2009-05-12 13:39	Signs that you partied too much, too long, too hard.	
	<input checked="" type="checkbox"/> May 12, 2009 (...)	2009-05-12 13:38	Signs that you partied too much, too long, too hard.	
	<input checked="" type="checkbox"/> May 11, 2009 (...)	2009-05-11 15:35	Taray quotes.	

The following table describes the labels in this screen.

**Table 36** Applications > Broadcatching

LABEL	DESCRIPTION
Add Channel	When you find a channel to subscribe to, copy the URL of the channel's feed and click this button. A screen opens for you to subscribe to the feed. When you are done, the feed's channel and contents display in the <b>Applications &gt; Broadcatching</b> screen.
Delete Channel	Select a channel and click <b>Delete Channel</b> to remove the channel from the NSA. Any of the channel's items that you have already downloaded stay in the channel's folder (in the <b>admin</b> share's <b>download</b> folder).
Refresh Channel	Select a channel and click <b>Refresh Channel</b> to check for new files.
Edit Channel	Select a channel and click <b>Edit Channel</b> to open a screen where you can set the channel's download and delete policies.
	The table lists channels and their files. Click a column's heading to sort the entries by that criteria.
Channel Name	This identifies the channel. A channel displays in red if there was an error the last time the NSA attempted to connect to it. When this happens, you can select the channel and click <b>Refresh Channel</b> to have the NSA reattempt to connect to it. Select a channel to see its available files. A "... " indicates an abbreviated name. Hold your cursor over the name to display the full name.
Item Name	<p>These are the downloadable files. The following icons show the file's status in the NSA.</p>  <p><b>Completed:</b> The NSA has downloaded the whole file. Double-click the item to go to the <b>Download Service</b> screen where you can see the file's name and location.</p> <p><b>Seeding:</b> The NSA downloaded the complete file and NSA is sharing it with other BitTorrent users. Double-click the item to go to the <b>Download Service</b> screen.</p> <p><b>Downloading:</b> The NSA is downloading the file. Double-click the item to go to the <b>Download Service</b> screen.</p> <p><b>Queued:</b> The file is waiting in line for the NSA to download it. Double-click the item to go to the <b>Download Service</b> screen.</p> <p><b>Pause:</b> The download has been manually stopped. Double-click the item to go to the <b>Download Service</b> screen.</p> <p><b>Missing File:</b> The NSA could not find the file.</p> <p><b>Error:</b> The NSA automatically retries unsuccessful download attempts. The status displays as error when the re-attempts are also unsuccessful and the NSA stops trying to download the file. To try the download again, use the <b>Add</b> button to create a new task.</p> <p>Note: A ... indicates an abbreviated file name. Hold your cursor over the name to display the full name.</p>

**Table 36** Applications > Broadcatching

LABEL	DESCRIPTION
Published Date	This is when the file was made available for download.
Description	This is the publishers introduction for the file.
Actions	<b>Start Downloading:</b> Click this to add the file to the NSA's download queue or check the file's status in the NSA's download service.  Click the <b>Delete</b> icon to remove the file from the channel's list.

## 9.8.1 Adding a Broadcatching Channel

At the time of writing, the NSA supports RSS 2.0 feeds. Websites with a feed usually display a feed icon (shown next). Copy and paste the feed's URL into the **Applications > Broadcatching > Add Channel** screen and you can download new files as they are added.

**Figure 65** Feed Icon

A channel uses a feed to deliver its contents (items). Subscribe the NSA to a feed to be able to download the contents.



Click **Applications > Broadcatching > Add Channel** to open the following screen. Use the **Add Channel** screen to subscribe the NSA to a channel's feed so you can view the channel. You also select policies for downloading and deleting the channel's items. [Section 4.6 on page 93](#) provides a tutorial on adding a broadcatching channel.

**Figure 66** Applications > Broadcatching > Add Channel

**Subscribe to Channel Feed**

Please enter the url address of the feed you want to subscribe to \*

Download Policy  
Download All Items

Delete Policy  
☒ Manual  
☐ Keep last  of items

Location of Downloaded Files

	Share	Path
Put incomplete downloads in	admin	/download
Move completed downloads to	public	/

Edit

**Note:**

1. BitTorrent jobs are stored in /public/incoming.
2. HTTP/FTP jobs are stored in /public.
3. All jobs triggered by RSS channels create the subfolder in /public using the channel name where it store all files downloaded from that channel.

Apply Cancel

The following table describes the labels in this screen.

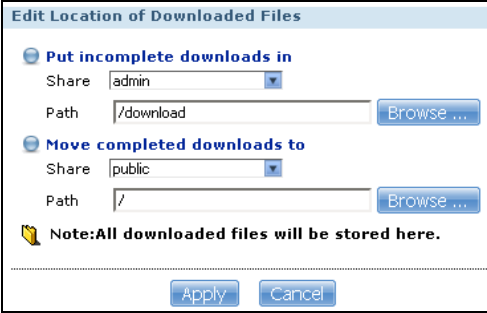
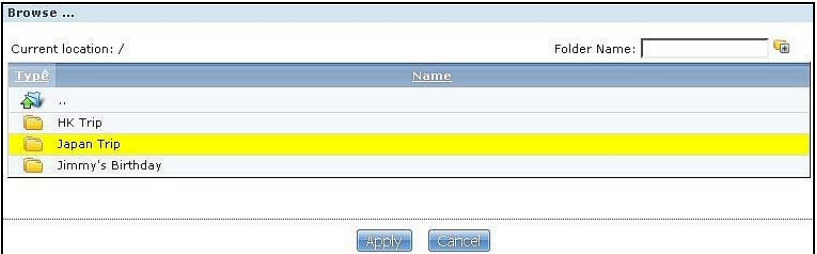

**Table 37** Applications > Broadcatching > Add Channel

LABEL	DESCRIPTION
Subscribe to Channel Feed	<p>Paste (or type) the URL of the feed for the channel to which you want to subscribe into this field. This is read-only in the <b>Preferences</b> screen.</p> <p>Note: Make sure the link goes to the actual RSS feed instead of to another list of links or information about the channel.</p> <p>One way to test this is by clicking the link. Clicking an actual RSS feed link opens a screen of XML code (in browsers without an RSS feed aggregator) or a window where you can add the RSS feed (in browsers with an RSS feed aggregator).</p>
Download Policy	<p>Set which of the channel's items the NSA downloads.</p> <p><b>Download All Items:</b> Download every file in the feed.</p> <p><b>Download Only New Items:</b> Download new files from today on.</p> <p><b>Manually Choose Items for Download:</b> Only download individual files you select later in the <b>Applications &gt; Broadcatching</b> screen.</p>

**Table 37** Applications > Broadcatching > Add Channel

LABEL	DESCRIPTION
Delete Policy	<p>Set how the NSA handles deleting the items downloaded from the channel.</p> <p><b>Manual:</b> Only delete individual files you select later in the <b>Applications &gt; Broadcatching</b> screen.</p> <p><b>Keep last N of items:</b> Select this to set the NSA to only keep a number of the channel's most recent files. When this number has been reached, if the NSA downloads another file from the channel, it deletes the oldest file from the NSA.</p>
Location of Downloaded Files	<p>This shows where the NSA stores new downloads (<b>Put incomplete downloads in</b>) and where the NSA moves completed downloads (<b>Move completed downloads to</b>).</p> <p>The <b>Share</b> column shows the name of the share where the file is downloaded.</p> <p>The <b>Path</b> column points to the location in the share where the NSA will save the downloaded files.</p> <ul style="list-style-type: none"> <li>• BitTorrent jobs are stored in /*/incoming (where '*' is a folder that you have set.)</li> <li>• HTTP/FTP jobs are stored in /* (where '*' is a folder that you have set.)</li> <li>• All jobs triggered by RSS channels create the subfolder in /* using the channel name where it store all files downloaded from that channel (where '*' is a folder that you have set.)</li> </ul>

**Table 37** Applications > Broadcatching > Add Channel

LABEL	DESCRIPTION
Edit	<p>Click this to open the following screen where you can set the default folder location where you “<b>Put incomplete downloads in</b>” and “<b>Move complete downloads to</b>”:</p>  <ul style="list-style-type: none"> <li>• <b>Share</b> - Select the share from the list.</li> <li>• <b>Path</b> - Type the folder location in the share directly or click <b>Browse</b> to open the following screen and navigate to the file's location.</li> </ul>  <ul style="list-style-type: none"> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Folder Name</b> - Enter a new folder name and click  to create it.</li> <li>• <b>Type</b> - This identifies the item as a file or folder.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Select a folder. If you don't select a folder, a forward slash (/) displays in the <b>Path</b> field. All contents within the specified share are automatically selected.</p> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

## 9.8.2 Editing a Broadcatching Channel

Click **Applications > Broadcatching**, then select a channel and click **Edit Channel** to open a similar **Edit** screen. Use the **Edit Channel** screen to change the download or delete policies.

**Figure 67** Applications > Broadcatching > Edit Channel

**Settings**

Channel Name

URL

Download Policy

Delete Policy ☒ Manual ☐ Keep last  of items

Location of Downloaded Files

	Share	Path
Put incomplete downloads in	admin	/download
Move completed downloads to	public	/

**Note:**


1. BitTorrent jobs are stored in /public/incoming.
2. HTTP/FTP jobs are stored in /public.
3. All jobs triggered by RSS channels create the subfolder in /public using the channel name where it store all files downloaded from that channel.

The following table describes the labels in this screen.

**Table 38** Applications > Broadcatching > Edit Channel

LABEL	DESCRIPTION
Channel Name	This is the name of the feed for the channel to which you want to subscribe into this field. This is read-only.
URL	This is the address of the channel.
Download Policy	Set which of the channel's items the NSA downloads.  <b>Download All Items:</b> Download every file in the feed.  <b>Download Only New Items:</b> Download new files from today on.  <b>Manually Choose Items for Download:</b> Only download individual files you select later in the <b>Applications &gt; Broadcatching</b> screen.
Delete Policy	Set how the NSA handles deleting the items downloaded from the channel.  <b>Manual:</b> Only delete individual files you select later in the <b>Applications &gt; Broadcatching</b> screen.  <b>Keep last N of items:</b> Select this to set the NSA to only keep a number of the channel's most recent files. When this number has been reached, if the NSA downloads another file from the channel, it deletes the oldest file from the NSA.

**Table 38** Applications > Broadcatching > Edit Channel

LABEL	DESCRIPTION
Location of Downloaded Files	<p>This shows where the NSA stores new downloads (<b>Put incomplete downloads in</b>) and where the NSA moves completed downloads (<b>Move completed downloads to</b>).</p> <p>The <b>Share</b> column shows the name of the share where the file is downloaded.</p> <p>The <b>Path</b> column points to the location in the share where the NSA will save the downloaded files.</p> <ul style="list-style-type: none"> <li>• BitTorrent jobs are stored in /*/incoming (where '*' is a folder that you have set.)</li> <li>• HTTP/FTP jobs are stored in /* (where '*' is a folder that you have set.)</li> <li>• All jobs triggered by RSS channels create the subfolder in /* using the channel name where it store all files downloaded from that channel (where '*' is a folder that you have set.)</li> </ul>
Edit	<p>Click this to open the following screen where you can set the default folder location where you "<b>Put incomplete downloads in</b>" and "<b>Move complete downloads to</b>".</p> <div data-bbox="760 835 1235 1148"> </div> <ul style="list-style-type: none"> <li>• <b>Share</b> - Select the share from the list.</li> <li>• <b>Path</b> - Type the folder location in the share directly or click <b>Browse</b> to open the following screen and navigate to the file's location.</li> </ul> <div data-bbox="620 1283 1429 1537"> </div> <ul style="list-style-type: none"> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Folder Name</b> - Enter a new folder name and click  to create it.</li> <li>• <b>Type</b> - This identifies the item as a file or folder.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Select a folder. If you don't select a folder, a forward slash (/) displays in the <b>Path</b> field. All contents within the specified share are automatically selected.</p> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>

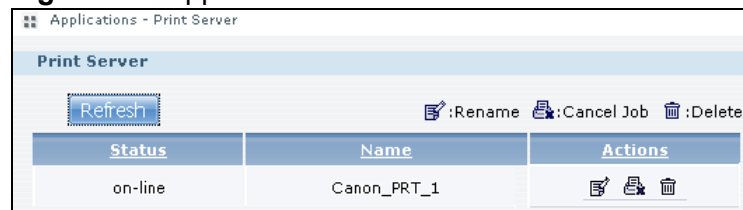
**Table 38** Applications > Broadcastching > Edit Channel

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

## 9.9 The Print Server Screen

Use the **Print Server** screen to view and manage the NSA's list of printers and print jobs.

Click **Applications > Print Server** to open the following screen.

**Figure 68** Applications > Print Server

The following table describes the labels in this screen.

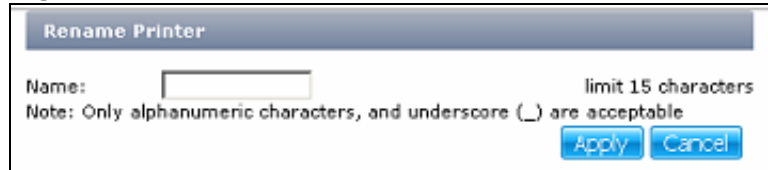
**Table 39** Applications > Print Server

LABEL	DESCRIPTION
Refresh	Click this to update the list of printers and print jobs.
	The table lists printers and their queued print jobs. Click a column's heading to sort the entries by that criteria.
Status	This field shows whether the printer is connected and turned on ( <b>on-line</b> ) or not ( <b>off-line</b> ).
Name	This identifies the printer. Each printer connected to the NSA must use a unique name.
Actions	<p><b>Rename:</b> Click this to change the name the NSA uses for the printer.</p> <p><b>Cancel Job:</b> Click this to remove all print jobs from the NSA queue for a particular printer. However, since the NSA sends print jobs to the printer as soon as it can, this button may only have an effect if there are very large or many print jobs in the queue. To stop a print job that has already started, you may have to turn off the printer.</p> <p><b>Delete:</b> Click this to remove a printer from the NSA's printer list. To add the printer back into the list, disconnect the printer from the NSA's USB port and reconnect it. If that does not work, disconnect the USB port and turn off the printer's power. Then reconnect the printer and turn it back on.</p>

## 9.9.1 Print Server Rename

Click **Applications > Print Server** and a printer's **Rename** icon to open the following screen. Use this screen to change the name the NSA uses for the printer.

**Figure 69** Applications > Print Server > Rename



Rename Printer

Name:  limit 15 characters

Note: Only alphanumeric characters, and underscore ( \_ ) are acceptable

Apply Cancel

The following table describes the labels in this screen.

**Table 40** Applications > Print Server > Rename

LABEL	DESCRIPTION
Name	Type a new name to identify the printer. The name must be unique from all the other names of printers connected to the NSA.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

## 9.10 The Copy/Sync Button Screen

The **COPY/SYNC** button on the front panel allows you to copy or synchronize files between a connected USB device and the NSA.

Click **Applications > Copy/Sync Button** to open the following screen.

**Figure 70** Applications > Copy/Sync Button

Applications - Copy/Sync Button

### Copy Settings

Press and release the button to copy data between the USB storage and NSA copy target.

NSA Copy Target: public

USB Volume:

Copy Direction: USB -> NSA

☐ Create a New Folder for Copied Files

☒ Backup Files to be Replaced

Backup Target:

Apply Reset

### Sync Settings

Press and hold the button until you hear a beep to synchronize data between the USB storage and NSA sync target.

NSA Sync Target: public

USB Volume:

Sync Direction: NSA <-> USB

☒ Backup Files to be Replaced or Removed

Backup Target:

Apply Reset

The following table describes the labels in this screen.

**Table 41** Applications > Copy/Sync Button

LABEL	DESCRIPTION
Copy Settings	
NSA Copy Target	Select the NSA share to use with the copy function.
USB Volume	If your USB device has multiple partitions, select which partition to use with the copy function.
Copy Direction	Select <b>USB -&gt; NSA</b> to copy files from your USB device to the NSA. Select <b>NSA -&gt; USB</b> to copy files from the NSA to your USB device.
Create a New Folder for Copied Files	Select this option to place the copied files in a new folder. The name of the folder created for the copied files consists of the date and time of the copy in year_month_day_hour_minute_second format.
Backup Files to be Replaced	This option is only available if you do not select <b>Create a New Folder for Copied Files</b> . Select this option to save the files that will be replaced by the source files.



**Table 41** Applications > Copy/Sync Button

LABEL	DESCRIPTION
Backup Target	Select a share in which to save the backup files.  Note: The NSA will not create a new folder to store the backup files. It is recommended to create a specific share (such as “backup”) for backup purposes.
Apply	Click this to save your changes.  The configuration file is saved on the USB device.
Reset	Click this to restore your previously saved settings.
Sync Settings	
NSA Sync Target	Select the NSA share to use with the synchronization function.
USB Volume	If your USB device has multiple partitions, select which partition to use with the synchronization function.
Sync Direction	Select <b>USB -&gt; NSA</b> to synchronize files from your USB device to the NSA.  Select <b>NSA -&gt; USB</b> to synchronize files from the NSA to your USB device.  Select <b>NSA &lt;-&gt; USB</b> to synchronize files in both directions simultaneously.
Backup Files to be Replaced or Removed	Select this option to save the files that will be replaced by the source files.
Backup Target	Select a share in which to save the backup files.  Note: The NSA will not create a new folder to store the backup files. It is recommended to create a specific share (such as “backup”) for backup purposes.
Apply	Click this to save your changes.  The configuration file is saved on the USB device.
Reset	Click this to restore your previously saved settings.

## 9.11 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

### 9.11.1 Sharing Media Files on Your Network

The media server feature lets anyone on your network play video, music, and photos from the NSA (without having to copy them to another computer). The NSA can function as a DLNA-compliant media server and/or an iTunes server. The

NSA streams files to DLNA-compliant media clients or computers using iTunes. The Digital Living Network Alliance (DLNA) is a group of personal computer and electronics companies that works to make products compatible in a home network.

- Publish shares to let others play the contained media files.
- The media server is a convenient way to share files you download using the broadcastcasting service (see [Section 9.8 on page 186](#)).
- Hardware-based media clients like the DMA-2500 can also play the files. See [Section 18.4 on page 368](#) for the supported multimedia file formats.

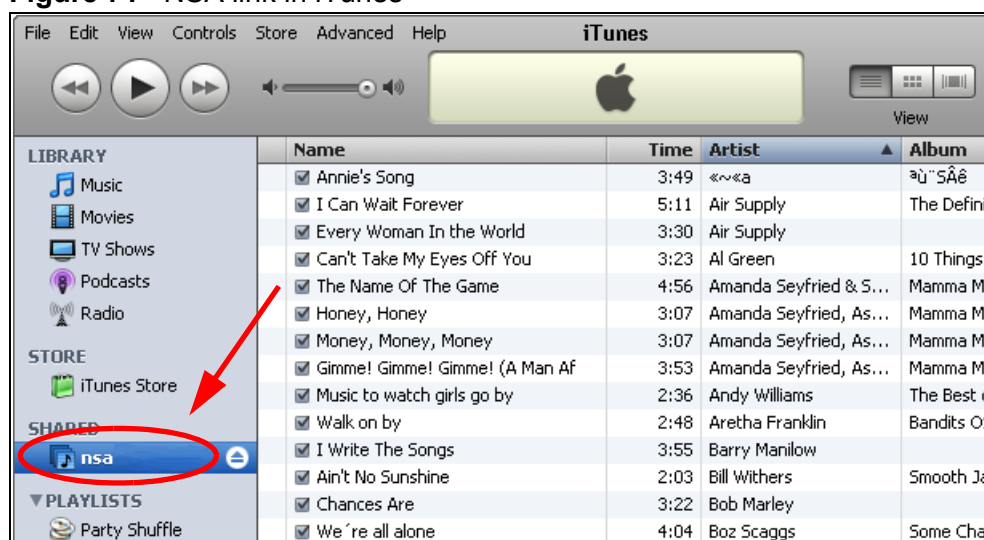
Note: Anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

## Songs and Videos from the iTunes Store

After using iTunes on your computer to download songs and videos from Apple's iTunes Store, you can copy them to the NSA. Many of these songs and videos have DRM (Digital Rights Management). At the time of writing, you can use your Apple account ID and password to authorize up to a total of five computers to play the files. To authorize a computer, open iTunes and click **Store > Authorize Computer**.

A link for the NSA in iTunes under **SHARED**. Click it to display the NSA's published media files as shown next.

**Figure 71** NSA link in iTunes



## 9.11.2 Download Service

The NSA's download service downloads files from the Internet directly to the NSA. You do not have to download to your computer and then copy to the NSA. This can free up your computer's system resources. The download service also handles your broadcatching downloads. See [Section 9.8 on page 186](#) for information on broadcatching.

The NSA can download using these protocols.

- HTTP: The standard protocol for web pages.
- FTP: A standard Internet file transfer service.
- BitTorrent: A popular distributed peer-to-peer files sharing protocol.

**Note:** Do not use the NSA for illegal purposes. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws and will bear the consequences of any infringements thereof. ZyXEL bears NO responsibility or liability for your use of the download service feature.

### Torrent Files

The NSA needs a ".torrent" file for BitTorrent to download a file. The torrent file gives the NSA information about the file to be downloaded (and shared) and the tracker(s) (computers) that coordinates the distribution of the file.

When you add a BitTorrent download task in the NSA's web configurator screens, you can copy and paste the URL of the torrent file. The NSA automatically downloads the torrent file and saves it in a **torrent** folder within the folder where the NSA stores downloaded files (the **admin** share's **download** folder by default).

If you already have the torrent file saved on your computer, you can just specify its location when adding a download task through the web configurator. Another method is to use FTP or a CIFS program (Windows Explorer for example) to copy the torrent file into the **torrent** folder. The NSA automatically uses the torrent file.

After your BitTorrent download and sharing are finished, you can go to the **incoming** folder within the destination share or folder and delete the .torrent file if you need to free up hard disk space.

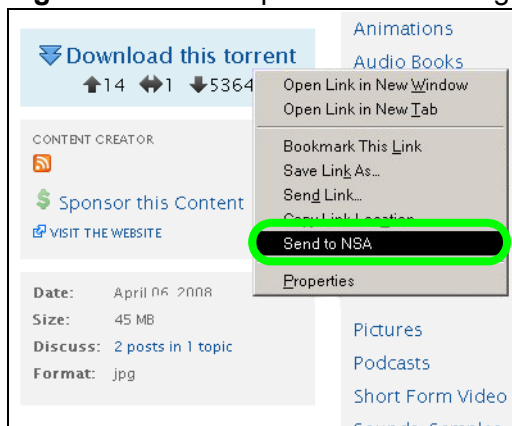
## 9.11.3 Link Capture Browser Plugin

The link capture browser plugin is an add-on feature for your web browser. Use the plugin to directly add a file's URL to the NSA's download service.

**Note:** The link capture browser plugin is located in the included CD.

The following screen displays how the plugin works.

**Figure 72** Link Capture Browser Plugin



Instead of copying and pasting a file's URL to the NSA's download service, you can right-click on the URL in the web browser and select **Send to NSA**. The URL is then added to the NSA's download service list.

See [Section 4.5.2 on page 80](#) and [Section 4.5.3 on page 85](#) for tutorials about installing and using the link capture browser plugin.

Note: At the time of writing, the plugin supports Internet Explorer 6.0/7.0 and Mozilla Firefox 2.0/3.0.

### 9.11.4 Download Service Notification

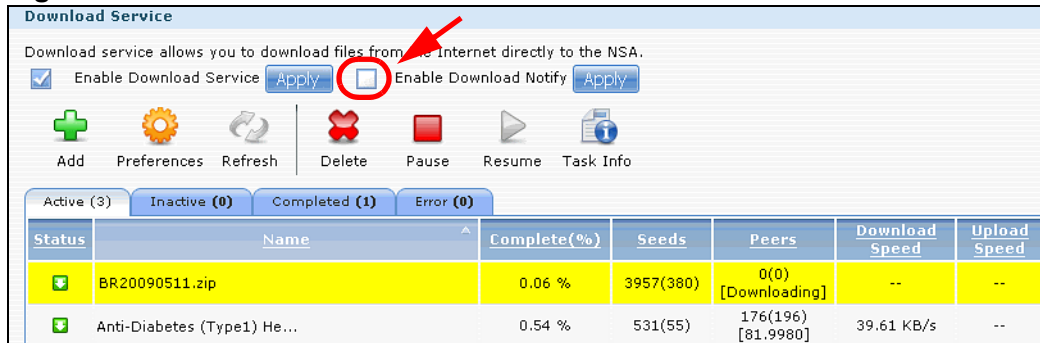
Use the download service notification to keep track of downloaded files on the NSA. You can subscribe to the NSA's download list on your computer. When the NSA finishes downloading new files, your RSS reader displays the information and links for the files. You can also download the files from the RSS reader to your computer.

See [Section 4.5.5 on page 89](#) for a tutorial about using the download service notification.

In the **Download Service** screen, select **Enable Download Notify** and click **Apply**. An RSS feed icon appears. Click the icon to subscribe to the NSA's download list.

Note: The download service notification only keeps track of files downloaded via BitTorrent.

**Figure 73** Download Service Notification



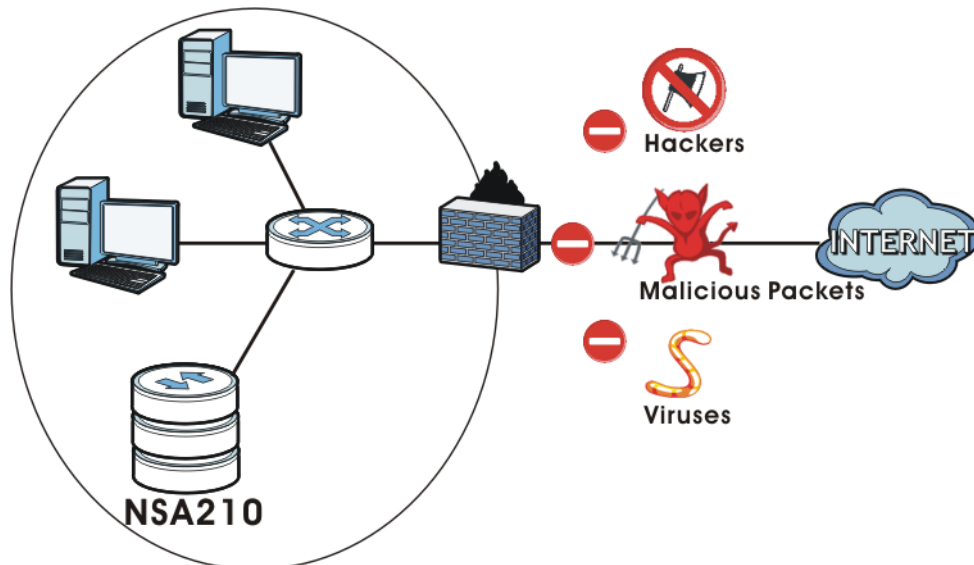
### 9.11.5 BitTorrent Security

When you download using BitTorrent, you reveal your IP address. This increases the risk of hacking attacks, which can be protected against by a good firewall.

#### Use a Hardware-based Firewall

Place a hardware-based firewall between your network and the Internet (a software-based firewall on your computer would just protect the computer itself, not the NSA since your computer is not between your NSA and the Internet).

**Figure 74** Firewall



Ideally your firewall should have the following:

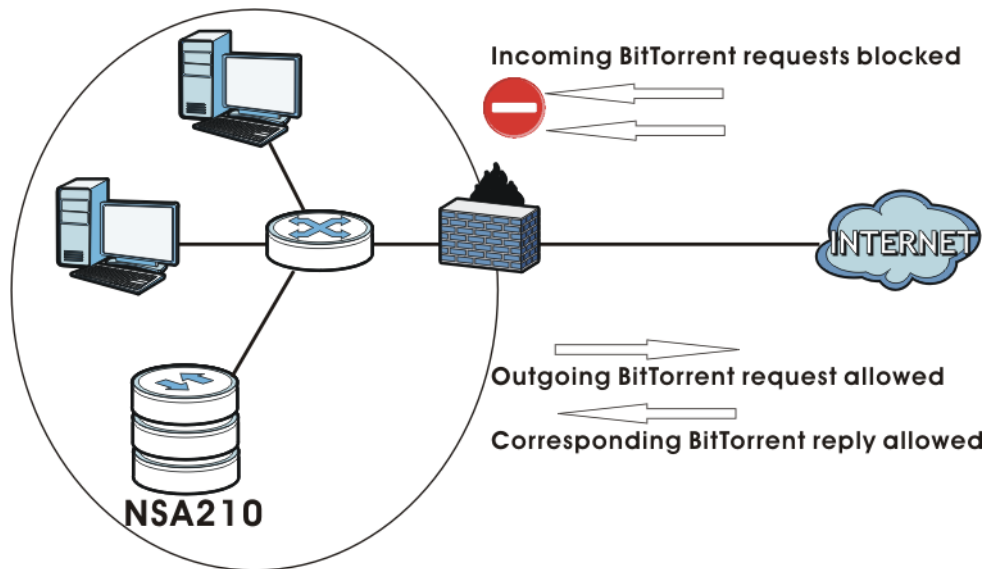
- Stateful packet inspection to control access between the Internet and your network and protect your NSA (and computers) from hacking attacks.
- IDP (Intrusion Detection and Prevention) to detect malicious packets within normal network traffic and take immediate action against them.
- Anti-virus to check files you download for computer viruses.

## BitTorrent and Your Firewall

The anti-virus feature on a firewall probably cannot check BitTorrent downloads for viruses, so use anti-virus software on your computer to scan the NSA for viruses.

When you download using BitTorrent, many other BitTorrent users are also trying to download the file from you. The firewall slows this down because by default, it only allows traffic from the Internet in response to a request that originated on the LAN (it lets you get files from the Internet and blocks those on the Internet from getting files from you).

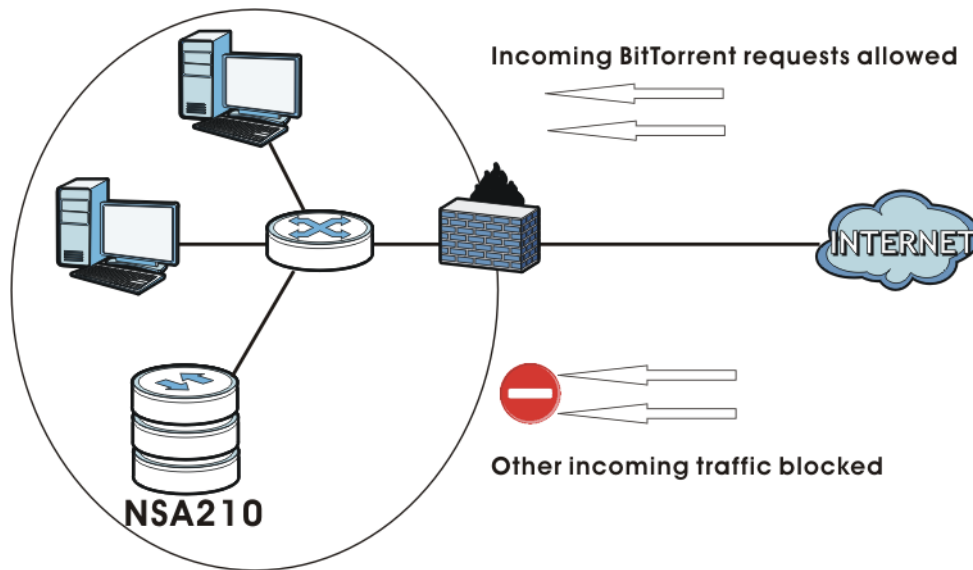
**Figure 75** Firewall Blocking Incoming BitTorrent Requests



To speed up BitTorrent file transfers, configure your firewall's port forwarding to send incoming TCP port 9090 and UDP port 9089 connections to the NSA. You probably need to use your firewall's HTML (web-based) configuration interface to

set this up (see the firewall's manual for details). You may also have to configure a corresponding firewall rule.

**Figure 76** Firewall Configured to Allow Incoming BitTorrent Requests

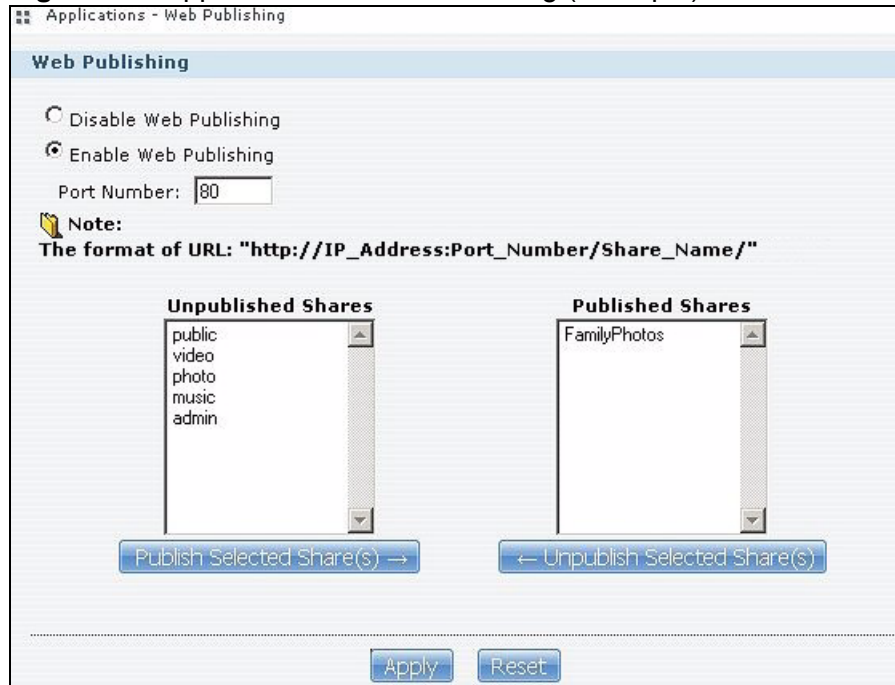


### 9.11.6 Web Publishing Example

This example covers how to configure the **Web Publishing** screen to let people use a web browser to access a share named FamilyPhotos without logging into the **My NSA** screens and shows how to access the share through the Internet.

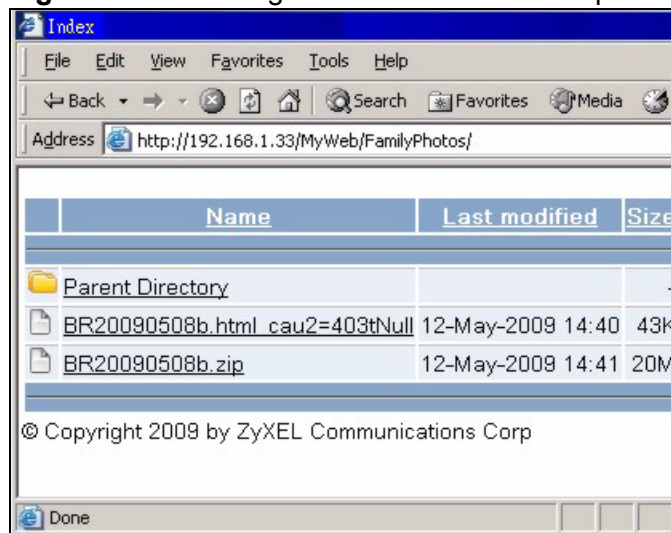
- 1 Click **Applications > Web Publishing** and configure the screen as shown (enable the web publishing and move **FamilyPhotos** over to **Published Shares**) and click **Apply**.

**Figure 77** Applications > Web Publishing (Example)



- 2 Now open your web browser and type in the address of the NSA's FamilyPhotos web page. In this example, the NSA's IP address is 192.168.1.33, and the name of the web-published share is FamilyPhotos. So you would enter "http://192.168.1.33/MyWeb/FamilyPhotos/" in your browser's address bar. Then press [ENTER] or click **Go**. A screen displays listing the share's files.

**Figure 78** Browsing to an NSA Share Example





- Click a file's link to open the file.
- Right-click a file's link and select **Save Target As..** (in Internet Explorer) to save a copy of the file.
- Click a label in the heading row to sort the files by that criteria.
- To customize how the page looks and works, create an index.html or index.htm file and store it in the share.

## 9.11.7 Web Publishing

Web publishing lets you "publish" shares (containing folders and files) on the NSA so people can access the files using a web browser without having to log into the My NSA screens. This way you can share files with others without them having to know and enter a user name and password.

For example, if you want to share photos in a FamilyPhotos share, you could "web publish" it and others could use a web browser to access the photos at `http://my-NSA's-IP-Address/MyWeb/FamilyPhotos`.

**Note:** The NSA does not use any security for the files in the published folders. It is not recommended to publish shares if you do not have the NSA behind a good hardware-based firewall. See [page 201](#) for more on firewalls.

Additionally, you can use HTML editing software (not included) to create an index.html or index.htm file to define and customize how your website works and looks.

### Accessing Web-published Shares from the Internet

You need to use a public address to access the NSA's web-published shares from the Internet. If your NSA uses a private IP address, you may need to use the public IP address of your Internet gateway and configure NAT or port forwarding on your Internet gateway and possibly firewall rules in order to let people access the NSA's web-published shares from the Internet.

### Web Publishing Port Number

If the web-published shares use a port number other than 80 (the normal port for web traffic), users must include it after the NSA's IP address in order to access the NSA's web-published shares. For example, say you specified port 8080, the NSA's IP address is 192.168.1.23, and the name of the web-published share is FamilyPhotos. You would have to enter "`http://192.168.1.23:8080/MyWeb/FamilyPhotos/`" in your browser's address bar to access the share's web page.

The NSA's web configurator uses port 80. To make the web configurator more secure, you can have the web-published shares use another port number. Then you can configure one set of firewall rules and NAT or port forwarding settings on

your Internet gateway specifically for allowing access to the web-published shares and another separate set of rules for accessing the NSA's web configurator.

### 9.11.8 Channel Guides for Broadcatching

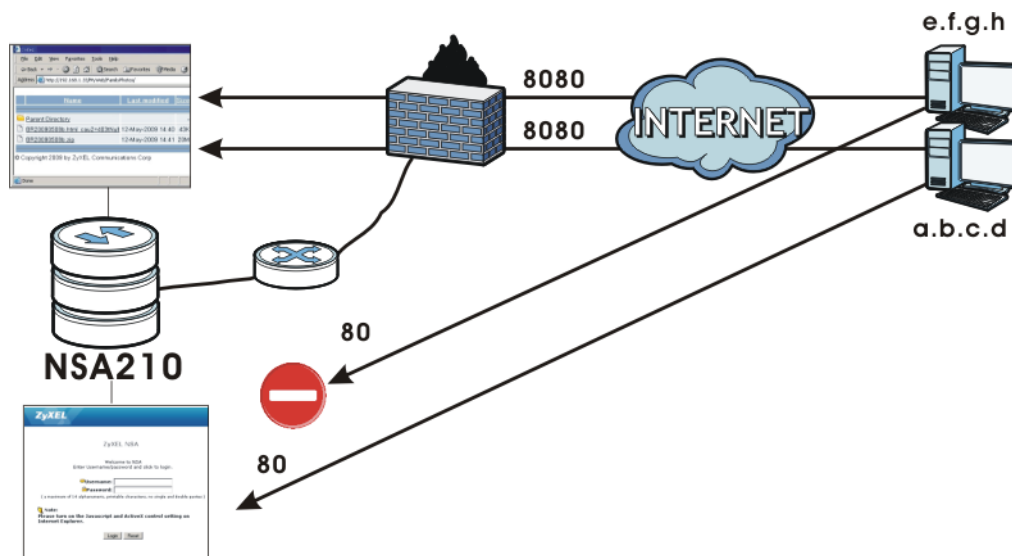
Here are some popular broadcatching channel guide web sites.

Note: ZyXEL does not endorse these web sites and is not responsible for any of their contents. Use these or any other web sites at your own risk and discretion.

- <http://www.zencast.com/>
- <http://www.miroguide.com/>
- <http://www.vuze.com/>
- <http://www.mefedia.com/>
- <http://www.vodstock.com/>
- <http://www.mininova.org>

In the following example, the Internet gateway's firewall is configured to allow anyone to access the NSA's web-published screens using port 8080. Web configurator access (port 80) however, is only allowed from IP address a.b.c.d.

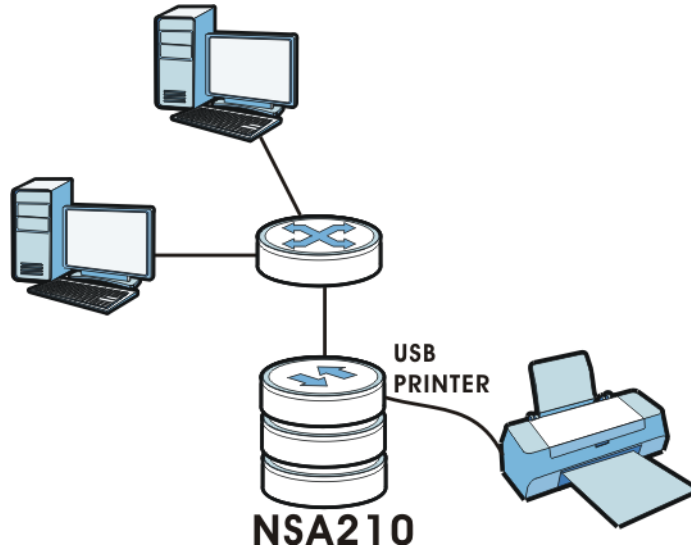
**Figure 79** Web Publishing Port Number Example



### 9.11.9 Printer Sharing

The NSA can act as a print server. A print server lets multiple computers share a printer. Connect a printer to the NSA's USB port to let multiple computers on your network use it. See [www.zyxel.com](http://www.zyxel.com) for a list of compatible printers.

**Figure 80** Printer Sharing



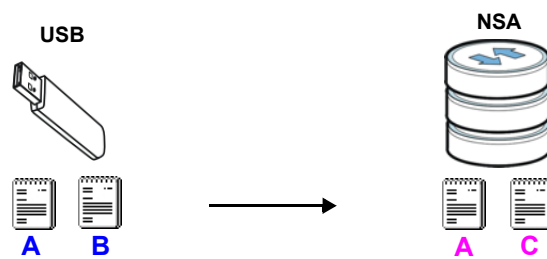
## 9.11.10 Copying Files

You can copy files from a USB device to the NSA or from the NSA to a USB device. Simply press and release the **COPY/SYNC** button to start copying files. See [Section 9.10 on page 196](#) for details about configuring the copy settings.

The following figure illustrates how copying files works when you copy files from a USB device to the NSA. The same concept applies when you copy files from the NSA to a USB device.

**Figure 81** Copying Files Example

**Before Copy**



**After Copy**



Both storage devices contain file A.

- A copy of files A and B from the USB device is transferred to the NSA.
- File A from the USB device replaces file A on the NSA.

### 9.11.11 Synchronizing Files

Synchronization makes the contents on the target device identical to the ones on the source device. You can synchronize files from a USB device to the NSA or from the NSA to a USB device. In addition, you may also synchronize files in both directions simultaneously.

Press and hold the **COPY/SYNC** button until you hear a beep to synchronize files. See [Section 9.10 on page 196](#) for details about configuring the synchronization settings.

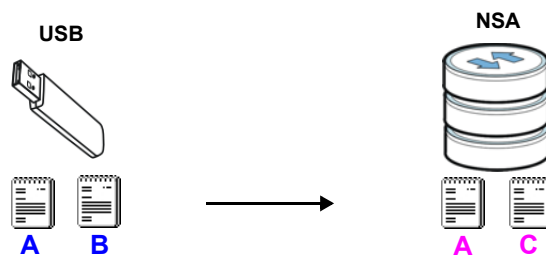
#### USB -> NSA or USB <- NSA

When you synchronize files in one direction, contents on the source device replace the files on the target device.

The following figure illustrates how synchronization works when you synchronize files from a USB device to the NSA. The same concept applies when you synchronize files from the NSA to a USB device.

**Figure 82** Synchronizing Files Example 1

#### Before Sync



#### After Sync



Both storage devices contain A.

- A copy of files A and B from the USB device is transferred to the NSA.
- File A from the USB device replaces file A on the NSA.
- File C on the NSA is deleted.

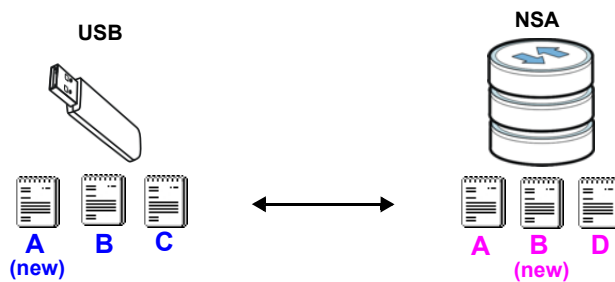
## USB <-> NSA

When you synchronize files in both directions simultaneously, both storage devices transfer unique files to one another. Files with the same file name are synchronized according to their modification date/time. The difference in modification time between the two files has to be greater than five minutes. More recently modified files overwrite the older ones during synchronization.

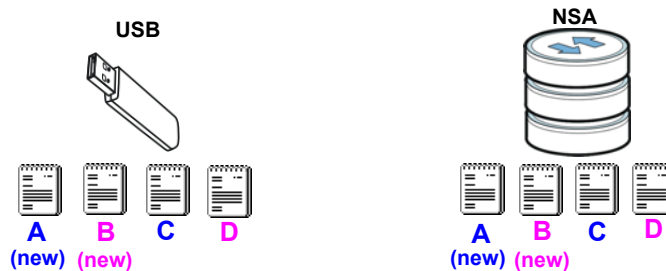
The following figure illustrates how synchronization works when you synchronize files in both directions simultaneously.

**Figure 83** Synchronizing Files Example 2

### Before Sync



### After Sync



A on the USB device and B on the NSA are modified more recently.

- File A from the USB device replaces file A on the NSA.
- File B from the NSA replaces file B on the USB device.
- A copy of file C from the USB device is transferred to the NSA.
- A copy of file D from the NSA is transferred to the USB device.

# Package Management

## 10.1 Overview

Package Management can be used to set up more useful applications in your NSA. The NSA can download multiple packages/files at once and automatically goes through all the installation steps.

## 10.2 What You Can Do

- Use the **Package Management** screen ([Section 10.4 on page 212](#)) to download and install applications from the web.
- Use the **eMule** screens ([Section 10.5 on page 216](#)) to configure the server, task and search settings for the eMule application.
- Use the **DyDNS** screen ([Section 10.6 on page 232](#)) to configure the domain name settings of your NSA.
- Use the **NFS** screen ([Section 10.7 on page 233](#)) to configure the Network File System (NFS) settings of your NSA.
- Use the **SMART** screens ([Section 10.8 on page 237](#)) to view your NSA hard disk(s) statistics and monitor their performance.
- Use the **Protect** screens ([Section 10.9 on page 241](#)) to configure and schedule the backup and restore jobs of your NSA.

## 10.3 What You Need to Know

This feature enables you to use the following applications:

- **eMule** - eMule is an open-source peer-to-peer (P2P) file-sharing application similar to eDonkey, which can be used to download files from the Internet. It uses the Kad protocol.
- **DyDNS** - This gives your NSA a domain name with a dynamic IP address. At the time of writing, this package supports accounts from the following service providers: DynDNS, NoIP, 3322, ZoneEdit, and DHS.

- **Gallery** - This web-based application allows your NSA to host pictures. You can upload images in your local computer or shares to this application. Use the administrator account of your NSA to log in to the Gallery console. The administrator can then create accounts for other users.
- **NFS** - NFS (Network File System) is a file-sharing protocol most commonly implemented on Unix-like systems.
- **PHP-MySQL-phpMyAdmin** - This tool can be used to manage MySQL through the web. Enter 'root' as the username and '1234' as the password to log in. This includes MySQL 5.1.30, PHP 5.2.8 and phpMyAdmin 3.1.1.
- **SMART** - Use S.M.A.R.T. (Self Monitoring, Analysis, and Reporting Technology) to monitor hard disks. It detects and reports the reliability of hard disks using standard indicators, enabling administrators to anticipate possible disk failures.
- **SqueezeCenter** - This enables you to manage a Logitech's Squeezebox device connected to the NSA.
- **Wordpress** - This allows you to create and manage a blog. Use the NSA administrator credentials to log in. The administrator can then create accounts for other users.
- **BackupPlanner** - Use this to schedule and run backup jobs for files stored in your NSA to an internal drive, external storage device or to another NSA in the network.

The following applications come with their own web configurator and documentation:

- Gallery
- PHP-MySQL-phpMyAdmin
- SqueezeCenter
- WordPress

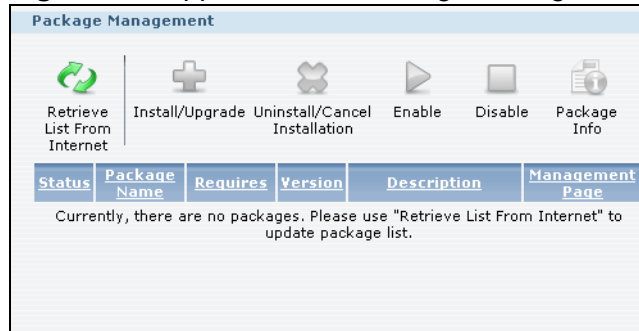
## 10.4 Package Management Screen

Use this screen to download and install applications from the web.



Click **Applications > Package Management** to open the following screen.

**Figure 84** Applications > Package Management




The following table describes the labels in this screen.

**Table 42** Applications > Package Management

LABEL	DESCRIPTION
Package Management	
Retrieve List From Internet	Click this to retrieve a list of available packages from the ZyXEL website.
Install/Upgrade	Choose the item(s) on the list and click this to install the selected application(s) on your system or upgrade to the latest version if you have previously installed the application.
Uninstall/Cancel Installation	Choose the item(s) on the list and click this to uninstall the selected application(s) from your system or cancel their active download(s) or install process/es.  This is only available if you have previously installed the package.
Enable	This option is only for non built-in packages.  Choose the item(s) on the list and click this to enable the application(s) on your system.  This is only available if you have previously installed the package.
Disable	This option is only for non built-in packages.  Choose the item(s) on the list and click this to disable the application on your system. You have to enable the application again in order to use it.  This is only available if you have previously installed the package.
Package Info	Select an item on the list and click this to display information about the package. See <a href="#">Section 10.4.1 on page 215</a> for more details.

**Table 42** Applications > Package Management

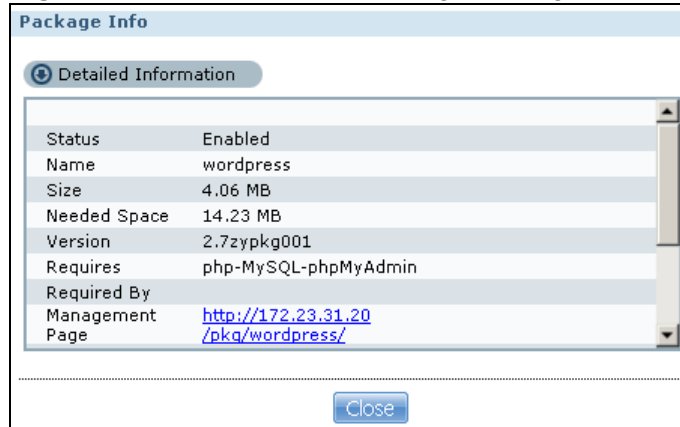
LABEL	DESCRIPTION
Status	<p>This is the current status of the application. It shows:</p> <ul style="list-style-type: none"> <li>• <b>Not Installed</b> - This displays for applications that have not been installed by the NSA.</li> <li>• <b>Installing (%)</b> - This displays when the application is being installed. It also shows the percent of the package already installed.</li> <li>• <b>Built-in</b> - This displays for applications installed by the NSA that you can configure in the NSA Web Configurator.</li> <li>• <b>Enabled</b> - This displays for applications installed and enabled by the NSA that have their own web configurators.</li> <li>• <b>Disabled</b> - This displays for applications installed and disabled by the NSA that have their own web configurators.</li> <li>• <b>Unknown</b> - It is possible to get this status if the web location for the application is unavailable.</li> </ul>
Package Name	This is the name of the application.
Requires	<p>This shows the other packages required in order to run this application.</p> <p>Note: A package would be disabled/enabled simultaneously if its prerequisite package(s) has been disabled/enabled. For example, when you enable WordPress, this also enables PHP-MySQL-phpMyAdmin automatically. However when you enable PHP-MySQL-phpMyAdmin, this does not automatically enable WordPress.</p>
Version	<p>This is the version number of the item.</p> <p>The  icon indicates that the application has a newer version available. Move your mouse over this icon to see the latest version number. Choose this item and click <b>Install/Upgrade</b>.</p>
Description	This shows a brief description of the application.
Management Page	This shows the location of the screens or web configurator where you can manage the application (after the package has been installed on the system).

Note: Once you install an application and enable it, additional links show up in the navigation panel. This applies to **eMule**, **DyDNS**, **NFS**, **SMART** and **BackupPlanner**. For **Gallery**, **PHP-MySQL-phpMyAdmin**, **SqueezeCenter** and **WordPress**, you can access the applications' web configurators through the **Package Management** screen.

## 10.4.1 Displaying the Package Information

Select an item on the list and click **Package Info**. Use this screen to check detailed information about the task.

**Figure 85** Applications > Package Management > Package Info



The following table describes the labels in this screen.

**Table 43** Applications > Package Management > Package Info

LABEL	DESCRIPTION
Status	<p>This is the current status of the application. It shows:</p> <ul style="list-style-type: none"> <li>• <b>Not Installed</b> - This displays for applications that have not been installed by the NSA.</li> <li>• <b>Installing (%)</b> - This displays when the application is being installed. It also shows the percent of the package already installed.</li> <li>• <b>Built-in</b> - This displays for applications installed by the NSA that you can configure in the NSA Web Configurator.</li> <li>• <b>Enabled</b> - This displays for applications installed and enabled by the NSA that have their own web configurators.</li> <li>• <b>Disabled</b> - This displays for applications installed and disabled by the NSA that have their own web configurators.</li> </ul>
Name	This is the name of the application.
Size	This is the size of the application at initial download.
Needed Space	This is the needed space to complete the installation of the application.
Version	This is the version number of the application.
Requires	This shows other package/s required to run this application.
Required By	This shows which other packages require this application in order to be usable.
Management Page	This shows the location of the screens, console or web configurator where you can manage the application (after the package has been installed on the system).
Source	This shows the location of the installed files of the application.

**Table 43** Applications > Package Management > Package Info

LABEL	DESCRIPTION
Description	This shows a brief description of the item.
Close	Click this to close the screen.

## 10.5 eMule Screens

Use these screens to manage the eMule application in your NSA. eMule is a peer-to-peer (P2P) file-sharing console that lets you download files from the Internet. It works with eDonkey and Kad networks.

### 10.5.1 eMule Server Screen

Use this screen to configure the eMule server.

Click **Applications > eMule > Server** to open the following screen.

**Figure 86** Applications > eMule > Server

Status	IP Address	Port Number	Name	Response	Number of Current Users	Max. User Number	Number of Files
Not connected	89.248.172.86	4500	Sharing Kingdom 3	312 ms	226.77 K	350 K	17.08 M
Not connected	89.248.172.50	4500	Sharing Kingdom 2	360 ms	140.84 K	350 K	10.89 M
Connecting	88.191.81.111	1111	PEERATES.NET	468 ms	68.30 K	250 K	13.43 K
Not connected	89.248.172.90	4500	Sharing Kingdom 4	469 ms	120.23 K	350 K	10.19 M

The following table describes the labels in this screen.

**Table 44** Applications > eMule > Server

LABEL	DESCRIPTION
Server	You can add multiple servers in this screen. However, the NSA can only connect to one eMule server at a time.
Enable eMule	Check this and click <b>Apply</b> to enable the eMule application.
Add Server	Click this to add an eMule server. A server provides a list of available files for download, users sharing them and other information.  Refer to <a href="#">Section 10.5.2 on page 217</a> for the <b>Add Server</b> screen.

**Table 44** Applications > eMule > Server

LABEL	DESCRIPTION
My Info	Select a server from the list and click this to view the details and connection status of the server.  Refer to <a href="#">Section 10.5.4 on page 219</a> for the <b>My Info</b> screen.
Connect	Click this to connect to the selected server or a random server if no server is selected.
Disconnect	Select a server from the list and click this to disconnect from the server.
Edit Server	Select a server from the list and click this to edit the server's information, including the server name and IP address.  Refer to <a href="#">Section 10.5.3 on page 218</a> for the <b>Edit Server</b> screen.
Delete Selected Server(s)	Select the server(s) from the list and click this to delete the server(s) from the list.
The table lists your servers. Click a column's heading to sort the entries by that criteria.	
Status	This shows the status of the NSA's connection to the server: <b>Connected, Connecting</b> or <b>Not Connected</b> .
IP Address	This shows the IP address of the server.
Port Number	This shows the port number used by the server for file-sharing.
Name	This shows the name of the server.
Response	This shows the length of time (in milliseconds) that the server took to reply to the NSA.
Number of Current Users	This shows the number of users currently connected to the server.
Max. User Number	This shows the total number of users that can connect to the server at the same time.
Number of Files	This shows the number of files available for download in the server.

You see a warning screen before you delete a server.

**Figure 87** Delete a Server

## 10.5.2 Add Server

Use this screen to add a server for the eMule application.

Click **Add** in the **Applications > eMule > Server** screen to add a server.

**Figure 88** Applications > eMule > Server: Add

The following table describes the labels in this screen.

**Table 45** Applications > eMule > Server: Add

LABEL	DESCRIPTION
Server IP	Select this if you know the server name, IP address and port number of the eMule server you want to add.
Server Name	Enter the server name.
IP Address	Enter the IP address of the server.
Port Number	Enter the port number used by the server for file-sharing.
ED2K Link	Select this and enter the ED2K link for the eMule server you want to add.  The ED2K link is used within the eMule network and contains information about the server.
Insert server.met from URL	Select this and enter the URL from which you want to download the server list that you want the NSA to use.
Apply	Click this to apply your changes.
Cancel	Click this to return to the previous screen without saving.

### 10.5.3 Edit Server

Use this screen to edit a server for the eMule application.

Click **Edit** in the **Applications > eMule > Server** screen to edit a server.

**Figure 89** Applications > eMule > Server: Edit

The following table describes the labels in this screen.

**Table 46** Applications > eMule > Server: Edit

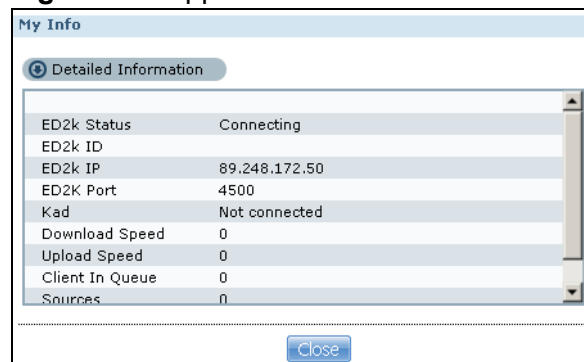
LABEL	DESCRIPTION
Server Name	Enter the server name.
IP Address	Enter the IP address of the server.
Port Number	Enter the port number of the server.
Apply	Click this to apply your changes.
Cancel	Click this to return to the previous screen without saving.

## 10.5.4 My Info

Use this screen to view the server details, including the status, IP address and download/upload speeds.

Click **MyInfo** in the **Applications > eMule > Server** screen to view the server details.

**Figure 90** Applications > eMule > Server: MyInfo



The following table describes the labels in this screen.

**Table 47** Applications > eMule > Server: MyInfo

LABEL	DESCRIPTION
ED2k Status	This shows the status of the NSA's connection to the server: <b>Connected, Connecting</b> or <b>Not Connected</b> .
ED2k ID	This is the identification given to the NSA by the eMule server. The ID comes in two types: <ul style="list-style-type: none"> <li>• <b>High ID</b> - The NSA connects to the server directly.</li> <li>• <b>Low ID</b> - The NSA connects to the server from behind a firewall.</li> </ul>
ED2k IP	This is the IP address of the eMule server to which the NSA is connected .
ED2k Port	This is the port number of the eMule server to which the NSA is connected.

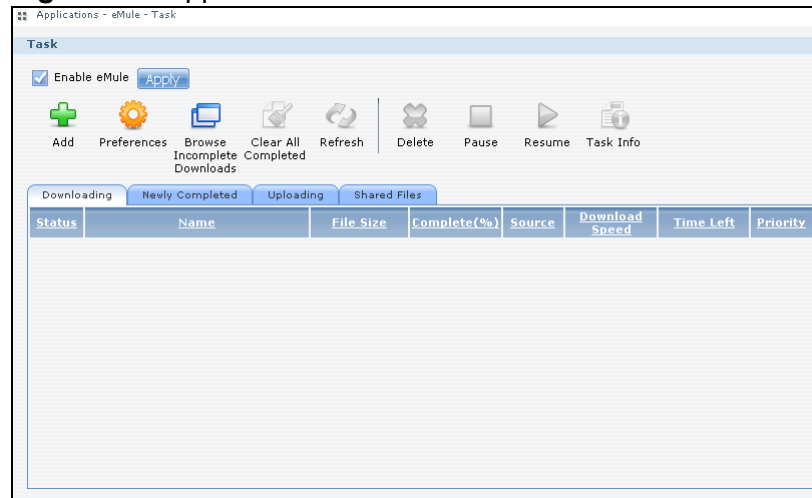
**Table 47** Applications > eMule > Server: MyInfo

LABEL	DESCRIPTION
Kad	This shows the status of the NSA's connection to the Kad network: <b>Connected</b> or <b>Not Connected</b> .  Kad is a shortcut for Kademlia network, which does not use servers to store files or user information in order to run a peer-to-peer network. Instead it employs peers/clients as small "servers" and runs queries through these peers.
Download Speed	This shows the current download speed of the eMule client.
Upload Speed	This shows the current upload speed of the eMule client.
Client in Queue	This shows the number of peers waiting to connect to the NSA to download its file (s).
Sources	This shows the total number of peers that can share the required files to the NSA eMule client.
Close	Click this to exit the screen.

## 10.5.5 eMule Task Screen

Use this screen to view tasks, including completed, downloading, uploading and shared tasks, that are being handled by the NSA.

Click **Applications > eMule > Task** screen to view the task details.

**Figure 91** Applications > eMule > Task

The following table describes the labels in this screen.

**Table 48** Applications > eMule > Task

LABEL	DESCRIPTION
Task	
Enable eMule	Check this and click <b>Apply</b> to enable the eMule application.



**Table 48** Applications > eMule > Task

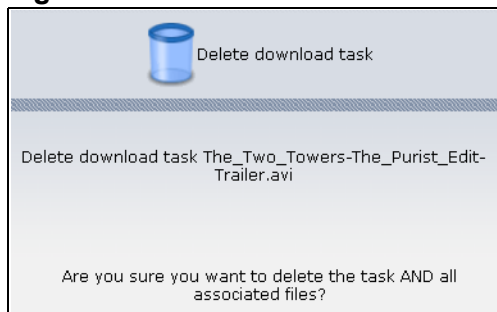
LABEL	DESCRIPTION
Add	Click this to add a download task (ED2K link) to the list. Refer to <a href="#">Section 10.5.6 on page 222</a> for the <b>Add Task</b> screen.
Preferences	Click this to open a screen where you can set the default location for saving downloaded files. You can also configure your eMule download settings. Refer to <a href="#">Section 10.5.7 on page 224</a> for the <b>Preferences</b> screen.
Browse Incomplete Downloads	Click this to open a screen where you can see a list of *.part.met files that the NSA is still in the process of downloading. Refer to <a href="#">Section 10.5.9 on page 228</a> for the <b>Share Browsing</b> screen.
Clear All Completed	Click this to remove all completed downloads from the task list. This only removes the newly completed task(s) in this session.
Refresh	Click this to refresh the task screen.
Delete	Select an item from the list and click this to delete the task.
Pause	Select an item from the list and click this to pause the task.
Resume	Select a paused item from the list and click this to resume the task.
Task Info	Select an item from the list and click this to view the details and status of the task.
The table lists your tasks. Click a column's heading to sort the entries by that criteria.	
Downloading	This table shows a list of download tasks that are still in progress.
Newly Completed	This table shows a list of tasks that have been completed but have not been cleared from the list.
Uploading	This table shows a list of upload tasks that are still in progress.
Shared Files	This table shows a list of files on the NSA that are available for download by other peers in the network.
Status	This shows the current status of the task: <b>Waiting</b> or <b>Downloading</b> .
Name/File Name	This shows the name of the file(s) associated to the task.
File Size/Size	This shows the size of the file(s) associated in the task.
Complete (%)	This shows the percentage of the file that has been downloaded by the NSA. It also indicates what percent of the file still needs to be downloaded.
Source	This shows the total number of peers that can share the required files to the NSA eMule client.
Download Speed	This shows the download speed of the NSA for the task.
Time Left	This shows how much more time the NSA needs to complete the file's download.
Priority	Use this field to set the priority for the task. Choose from <b>Auto</b> , <b>Low</b> , <b>Normal</b> or <b>High</b> .  Select <b>Auto</b> to have the NSA automatically determine the task's priority.  Select <b>High</b> to have the NSA complete this task before the others.

**Table 48** Applications > eMule > Task

LABEL	DESCRIPTION
Transferred	This shows what percent of the file the NSA has uploaded to other peers. This column is available in the <b>Uploading</b> tab.
Upload Speed	This shows the upload speed of the NSA. This column is available in the <b>Uploading</b> tab.
Requests	This shows the number of requests for a shared file. This column is available in the <b>Shared Files</b> tab.
Accepted Requests	This shows the number of file requests granted by the NSA. This column is available in the <b>Shared Files</b> tab.

Note: Download tasks initially appear in the **Downloading** tab of the eMule **Task** screen. Depending on its status, it can eventually show up in the other tabs (**Newly Completed**, **Uploading** or **Shared Files** tabs).

You see a warning screen before you delete a task.

**Figure 92** Delete a Task

## 10.5.6 Add Task

Use this to add a download task to the NSA.

Click **Add** in the **Applications > eMule > Task** screen to add a task.

**Figure 93** Applications > eMule > Task: Add

Add Download Task From ED2K Link

Source

ED2K Link 

Location of Downloaded Files

	Share	Path
Put incomplete downloads in	admin	/eMule/Temp
Move completed downloads to	admin	/eMule/Incoming

Edit

 **Caution:**

Do not use the NSA for illegal downloads. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws and will bear the consequences of any infringements thereof. ZyXEL takes NO responsibility or liability for your use of the download service feature.

Apply

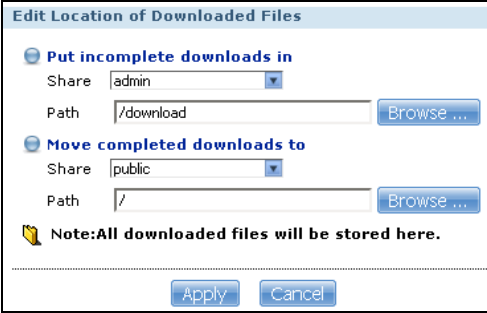


Cancel

The following table describes the labels in this screen.

**Table 49** Applications > eMule > Task: Add

LABEL	DESCRIPTION
Source	
ED2K Link	Paste the ED2K link of the file you want to download into this field.  The ED2K link identifies files in the eMule network. It starts with ed2k:// and may contain the name and size of the file you want to download.
Location of Downloaded Files	This shows where the NSA stores new downloads ( <b>Put incomplete downloads in</b> ) and where the NSA moves completed downloads ( <b>Move completed downloads to</b> ).  The <b>Share</b> column shows the name of the share where the file is downloaded.  The <b>Path</b> column points to the location in the share where the NSA will save the downloaded files.

**Table 49** Applications > eMule > Task: Add

LABEL	DESCRIPTION
Edit	<p>Click this to open the following screen where you can set the default folder location where you “<b>Put incomplete downloads in</b>” and “<b>Move complete downloads to</b>”:</p>  <ul style="list-style-type: none"> <li>• <b>Share</b> - Select the destination share from the drop-down list.</li> <li>• <b>Path</b> - This field displays the share folder’s path. You can use <b>Browse</b> to find or create a folder on the NSA or type the location of the folder using forward slashes as branch separators.</li> </ul>  <ul style="list-style-type: none"> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Folder Name</b> - Enter a new folder name and click  to create it.</li> <li>• <b>Type</b> - This identifies the item as a folder or file.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Select a folder. If you don’t select a folder, a forward slash (/) displays in the <b>Path</b> field. All contents within the specified share are automatically selected.</p> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

## 10.5.7 Preferences

Use this screen to configure your eMule settings, such as port numbers to use, its download/upload rates and the maximum number of peers allowed to connect to the NSA.

Click **Applications > eMule > Task > Preferences** to open the following screen.

**Figure 94** Applications > eMule > Task > Preferences

**Preferences**

**Username**  
Username

**Location of Downloaded Files**

	Share	Path
Put incomplete downloads in	admin	/eMule/Temp
Move completed downloads to	admin	/eMule/Incoming

**Port Number**  
UDP Port  The default port number is 4672  
TCP Port  The default port number is 4662

**Upload and Download Rate**  
Max. download rate  KB/s (0=No Limit)  
Max. upload rate  KB/s (0=No Limit)

**Connection**  
Maximum Number of Active Connections

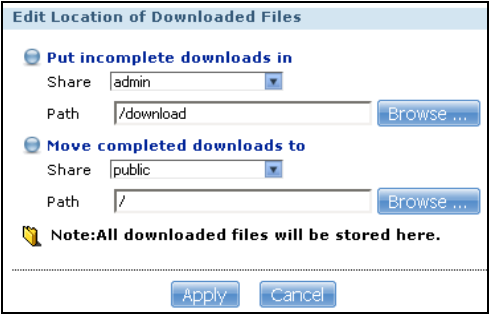
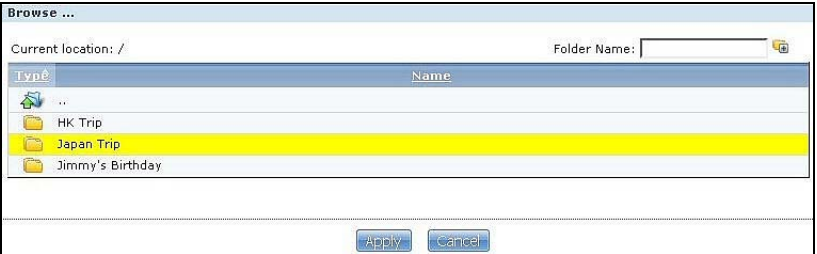

**IP Filter**

The following table describes the labels in this screen.

**Table 50** Applications > eMule > Task > Preferences

LABEL	DESCRIPTION
Username	
Username	Enter your user name that identifies the NSA in the eMule network.
Location of Downloaded Files	<p>This shows where the NSA stores new downloads (<b>Put incomplete downloads in</b>) and where the NSA moves completed downloads (<b>Move completed downloads to</b>).</p> <p>The <b>Share</b> column shows the name of the share where the file is downloaded.</p> <p>The <b>Path</b> column points to the location in the share where the NSA will save the downloaded files.</p>

**Table 50** Applications > eMule > Task > Preferences

LABEL	DESCRIPTION
Edit	<p>Click this to open the following screen where you can set the default folder location where you “<b>Put incomplete downloads in</b>” and “<b>Move complete downloads to</b>”:</p>  <ul style="list-style-type: none"> <li>• <b>Share</b> - Select the destination share from the drop-down list.</li> <li>• <b>Path</b> - This field displays the share folder’s path. You can use <b>Browse</b> to find or create a folder on the NSA or type the location of the folder using forward slashes as branch separators.</li> </ul>  <ul style="list-style-type: none"> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Folder Name</b> - Enter a new folder name and click  to create it.</li> <li>• <b>Type</b> - This identifies the item as a folder or file.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Select a folder. If you don’t select a folder, a forward slash (/) displays in the <b>Path</b> field. All contents within the specified share are automatically selected.</p> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>
Port Number	
UDP Port	Enter the UDP port number you want to use for file transfers.
TCP Port	Enter the TCP port number you want to use for file transfers.
Upload and Download Rate	
Max. download rate	Enter the maximum download rate for download tasks.
Max. upload rate	Enter the maximum upload rate for upload tasks.
Connection	
Maximum Number of Active Connections	Enter the maximum number of eMule peer-to-peer connections.
IP Filter	

**Table 50** Applications > eMule > Task > Preferences

LABEL	DESCRIPTION
Edit IP Filter	Click this to edit the IP Filter.  IP filtering prevents your NSA from accessing certain networks and IP addresses that may be hosting malicious programs.  Refer to <a href="#">Section 10.5.8 on page 227</a> to view and configure the <b>Edit IP Filter</b> screen.
Apply	Click this to save your changes.
Reset	Click this to clear the fields.
Cancel	Click this to return to the previous screen without saving.

## 10.5.8 Edit IP Filter

Use this screen to enable IP filtering which prevents your NSA from accessing certain networks and IP addresses that may be hosting malicious programs.

**Figure 95** Applications > eMule > Task > Preferences: Edit IP Filter

The following table describes the labels in this screen.

**Table 51** Applications > eMule > Task > Preferences: Edit IP Filter

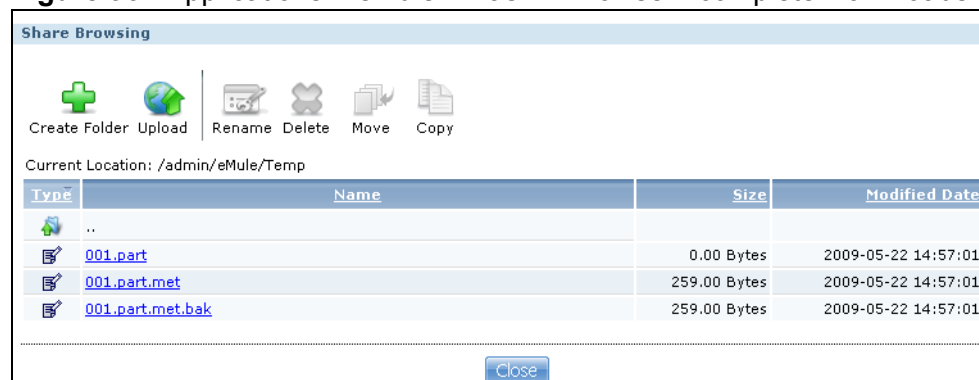
LABEL	DESCRIPTION
Enable IP Filter	Click this to enable IP filtering. This prevents your NSA from accessing certain networks and IP addresses that may be hosting malicious programs.  Select <b>Update IP Filter Table File from the Internet Every Week</b> if you know the web location of the IP filter table you want to use. Enter the link where your NSA can acquire the list of networks and IP addresses. The NSA checks this link every week and uses the latest IP filter table available.  Select <b>Upload IP Filter Table</b> if you want to use an IP filter table from your local computer.
Apply	Click this to save your changes.
Reset	Click this to return to the previous screen without saving.

## 10.5.9 Share Browsing

Use this screen to view a list of files that are still being downloaded by the NSA. The files are located in the eMule\Temp folder in the Admin share by default.

Click **Applications > eMule > Task > Browse Incomplete Downloads** to open the following screen.

**Figure 96** Applications > eMule > Task > Browse Incomplete Downloads



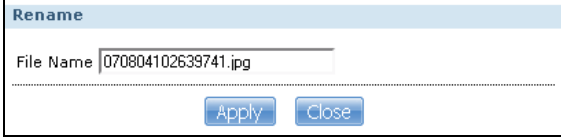

The following table describes the labels in this screen.

**Table 52** Sharing > Shares > Share Browser

LABEL	DESCRIPTION
Create Folder	Type a folder name and click <b>Apply</b> to make a new folder. The name can be 1 to 239 single-byte (no Chinese characters allowed for example) ASCII characters. The name cannot be the same as another existing folder in the same path. See <a href="#">Section 3.5.5 on page 50</a> for more information on folder names.
Upload	Click this to add files to the share. Use <b>Browse</b> to locate a file and click <b>Apply</b> to upload the file. Note that the size of each file should be less than 2 GB. <div data-bbox="540 1314 1125 1673"> <p>The 'Upload Files' dialog box contains five rows, each with a label 'File 1' through 'File 5', a text input field, and a 'Browse...' button. At the bottom, there is a note: 'Note: The size of uploaded files can't be more than 2G.' and two buttons: 'Apply' and 'Cancel'.</p> </div>



**Table 52** Sharing > Shares > Share Browser (continued)

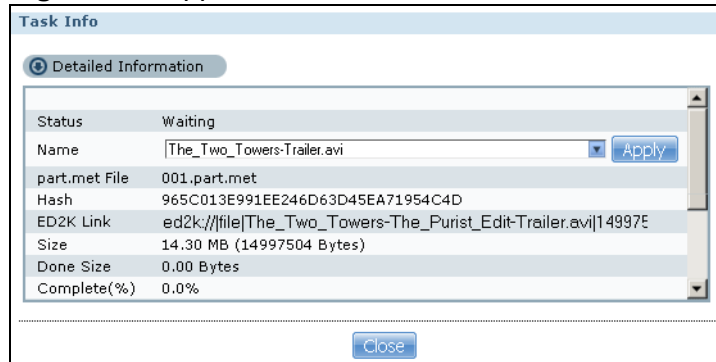
LABEL	DESCRIPTION
Rename	<p>Select a folder or file and click this to open a screen. Enter the name you want and click OK to make the changes.</p> <p>Note: When you change a file name, make sure you keep the file extension.</p> 
Delete	<p>Select a file/folder from the list and click this to open a warning screen. Click <b>Yes</b> to delete the file/folder, or click <b>No</b> to close the screen.</p> 
Move	Select a file/folder from the list and click this to relocate the file/folder to another share.
Copy	Select a file/folder from the list and click this to make a duplicate of the file/folder to another share.
Current location	This is the name of the share and folder path that you are in.
Type	<p>The icon in this column identifies the entry as a folder or a file.</p> <p>The folder with an arrow pointing up is for the link that takes you to the next higher layer in the share's folder tree.</p>
Name	This section lists the share's existing folders or files. Click to the right of the file/folder name to select the file/folder. You can also click the folder's name to navigate to a sub-folder within the folder.
Size	This field displays size of the file.
Modified Date	This field displays a file's latest modification date.
Close	Click this to close the screen.

## 10.5.10 Task Info

Use this screen to view eMule task details, such as status, file name, file size and its download progress.

Click **Task Info** in **Applications > eMule > Task** screen to open the following.

**Figure 97** Applications > eMule > Task: Task Info



The following table describes the labels in this screen.

**Table 53** Applications > eMule > Task: Task Info

LABEL	DESCRIPTION
Status	This shows the current status of the task - <b>Waiting</b> or <b>Downloading</b> .
Name	This shows the file name of the file associated with the task. You can change this file name by entering the new name and clicking <b>Apply</b> .
part.met File	This shows the temporary file name for an incomplete file.  Files in peer-to-peer networks can be divided into several parts for easier download. Once all the parts have been downloaded, you can run one part and the file automatically rebuilds itself. If the download of the file(s) is not completed, the file parts cannot open on their own.
Hash	This shows the hash value of the download file.  This is a text string that can be interpreted by eMule to check the downloaded file's integrity.
ED2K Link	This shows the ED2K link for this file.  The ED2K link identifies files in the eMule network. It starts with ed2k:// and may contain the name and size of the file you want to download.
Size	This shows the size of the file associated with the task.
Done Size	This shows the size of the file that has been downloaded so far.
Complete (%)	This shows what percent of the file has been downloaded so far.
Source	This shows the total number of peers that can share the required files to the NSA eMule client.
Download Speed	This shows the download speed for the task.
Time Left	This shows how much time is needed to complete the task.
Priority	This shows the priority of this task.  You can set this in <a href="#">Section 10.5.5 on page 220</a> .

**Table 53** Applications > eMule > Task: Task Info

LABEL	DESCRIPTION
Seen Complete	This shows the last time a source with the complete file was online.
Close	Click this to exit the screen.

### 10.5.11 eMule Search Screen

Use this screen to search for files available in an eMule server using keywords and other parameters, such as file type, file size and extension names.

Click **Applications > eMule > Search** to open the following screen.

**Figure 98** Applications > eMule > Search

The following table describes the labels in this screen.

**Table 54** Applications > eMule > Search

LABEL	DESCRIPTION
Search	
Enable eMule	Check this and click <b>Apply</b> to enable the eMule application.
Keyword(s)	Enter words that are related to the file you want to download.
File Type	Select the file type that you want to download.
Method	Select the search method you want eMule to employ.
Min Size	Enter the minimum file size you want included in the search results.
Max Size	Enter the maximum file size you want included in the search results.
Min Sources	Enter the minimum number of peers sharing the file you want to download.
Extension	Enter the file extensions separated by commas of files you want included in the search results.
Search	Click this to have the NSA search the eMule network for files that match the criteria you have set.
Clear	Click this to clear the fields.

**Table 54** Applications > eMule > Search

LABEL	DESCRIPTION
Download	Select a file from the results and click this to start downloading the file.
This table shows the results of the search.	
File Name	This shows the name of the file(s) that match the criteria you have set.
File Size	This shows the size of the file(s) that match the criteria you have set.
Source	This shows how many peers are currently available to share this file so that the NSA can download it.

## 10.6 DyDNS Screen

Use this to enable and configure DyDNS.

Dynamic DNS allows you to update your current dynamic IP address with a dynamic DNS service so that anyone can contact you (in NetMeeting, CUSeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.

Click **Network > DyDNS** to open the following screen.

**Figure 99** Network > DyDNS

Network - DyDNS

**Gateway Information**

Internal Address: unknown

External Address:

**Configuration**

Enable DyDNS support to allow users to access the server through a registered hostname.

☐ Enable DyDNS

Service Provider: DynDNS.com

Hostname:

Username:

Password:

Password (Confirm):

Apply Reset

The following table describes the labels in this screen.

**Table 55** Network > DyDNS

LABEL	DESCRIPTION
Gateway Information	
Internal Address	This shows the IP address assigned to the NSA by the gateway in your local network.
External Address	This shows the IP address of the NSA that can be accessed in the Wide Area Network (WAN). Note that this is not assigned by the DyDNS server.
Configuration	
Enable DyDNS	Select this to use dynamic DNS.  You need to have registered a dynamic DNS account with a service provider such as <a href="http://www.dyndns.org">www.dyndns.org</a> . The Dynamic DNS service provider will give you a password or key.
Service Provider	Select your Dynamic DNS service provider.
Hostname	Enter your host name provided by the Dynamic DNS service.
Username	Enter your user name for your DNS account.
Password	Enter the password assigned to your DNS account.
Password (Confirm)	Confirm the password you entered.
Apply	Click this to save your changes.
Reset	Click this to clear the fields.

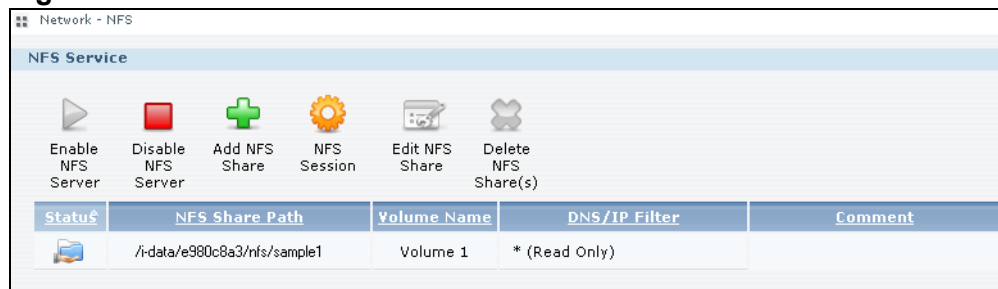
## 10.7 NFS Screen

Use this screen to enable and configure Network File System (NFS) settings on your NSA.

NFS is a client/server distributed file service that provides transparent file sharing for network environments. This allows shared folders in your NSA to be accessible like a local folder in a user's computer.

Click **Network > NFS** to open the following screen.

**Figure 100** Network > NFS



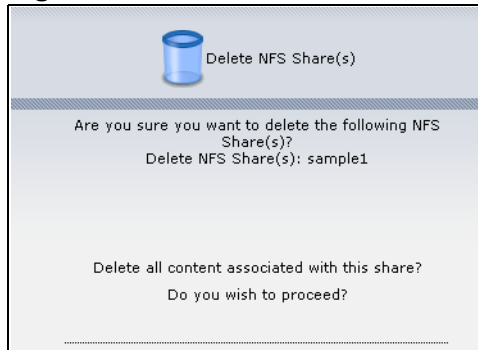
The following table describes the labels in this screen.

**Table 56** Network > NFS

LABEL	DESCRIPTION
NFS Service	
Enable NFS Server	Click this to employ NFS in your NSA. When you install the NFS application in your NSA, a read-only NFS share is automatically created as a sample.
Disable NFS Server	Click this to stop using NFS. This makes all NFS shares unavailable.
Add NFS Share	Click this to add an NFS share. Refer to <a href="#">Section 10.7.1 on page 235</a> for the <b>Add NFS Share</b> screen.
NFS Session	Click this to view active NFS sessions. You can see the list of users who have access to the NFS shares. Refer to <a href="#">Section 10.7.2 on page 236</a> for the <b>NFS Session</b> screen.
Edit NFS Share	Select an NFS share from the list and click this to edit it. Refer to <a href="#">Section 10.7.1 on page 235</a> for the <b>Edit NFS Share</b> screen.
Delete NFS Share (s)	Select an NFS share from the list and click this to delete it.
The table lists your NFS shares. Click a column's heading to sort the entries by that criteria.	
Status	This shows whether the share is active or not.
NFS Share Path	This shows the location of the share in the NSA.
Volume Name	This shows the volume where the NFS share is located.
DN/IP Filter	This shows which domain name(s) or IP address(es) have read/write access to the NFS shares. Refer to <a href="#">Section 10.7.1 on page 235</a> for the screen where you can configure this.
Comment	This shows a short description of the share.

You see a warning screen before you delete a volume.

**Figure 101** Delete an NFS Share



## 10.7.1 Add/Edit NFS Share

Use this screen to add or edit an NFS share.

Note: Some attributes of the NFS share cannot be edited.

Click **Add** or **Edit** in the **Network > NFS** screen to open the following:

**Figure 102** Network > NFS: Add/Edit

The following table describes the labels in this screen.

**Table 57** Network > NFS: Add/Edit

LABEL	DESCRIPTION
Volume Name	Select the volume where the folder you want to add as an NFS share is located.
NFS Share Name	Enter the name you want to give to the NFS share.
Full Path	This shows the location of the NFS share in the NSA. The NFS server assigns this path to the share folder you input.
Comment	Enter a short description for the share.

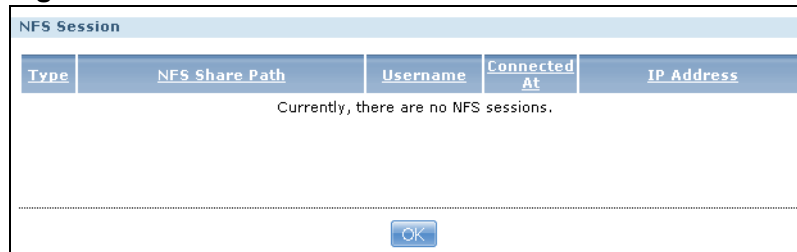
**Table 57** Network > NFS: Add/Edit

LABEL	DESCRIPTION
DN/IP Filter	<p>Enter the domain name(s) or IP address(es) that can have access to the NFS share.</p> <p>Enter '*' to make the share available to all users in the network. You can also enter a wildcard, such as '*.domain.com' to indicate that all users within that network have access to the share.</p> <p>Select the access rights you want to grant to each domain name or IP address you enter and click <b>Add</b>.</p> <ul style="list-style-type: none"> <li>• <b>Read Only</b> - Users with this access right can only view and copy files in the NFS share but cannot modify or delete them.</li> <li>• <b>Read/Write</b> - Users with this access right can view, edit or delete files in the NFS share.</li> </ul>
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

## 10.7.2 NFS Session

Use this screen to view a list of active NFS sessions. You can see which users are connected the NFS shares.

Click **NFS Session** in the **Network > NFS** screen to open the following.

**Figure 103** Network > NFS: NFS Session


NFS Session				
Type	NFS Share Path	Username	Connected At	IP Address
Currently, there are no NFS sessions.				
OK				

The following table describes the labels in this screen.

**Table 58** Network > NFS: NFS Session

LABEL	DESCRIPTION
Type	This shows if the NFS share is active or not.
NFS Share Path	This shows the location of the share in the NSA.
Username	This shows the username of the active user connected to the NFS share.
Connected At	This shows to which domain/IP address the user accessing the NFS share belongs.
IP Address	This shows the IP address of the user accessing the NFS share.
OK	Click this to close the window.



# 10.8 SMART Screen

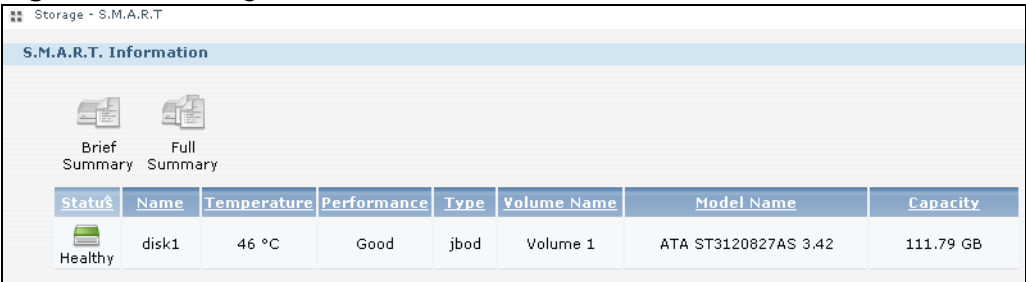
Use this screen to view indicators of your NSA’s hard disk(s) health.

Self Monitoring, Analysis, and Reporting Technology (S.M.A.R.T) detects and reports the reliability of hard disks using standard indicators (called “attributes”), to help you anticipate possible disk failures.

Note: The fields included the screens may vary depending on the hard disk that you use.

Click **Storage > S.M.A.R.T** to open the following screen.

**Figure 104** Storage > S.M.A.R.T



The following table describes the labels in this screen.

**Table 59** Storage > S.M.A.R.T

LABEL	DESCRIPTION
S.M.A.R.T. Information	
Brief Summary	Select a hard disk volume from the list and click this to display information about the volume, such as the hard disk vendor, specific model, hard disk capacity and so on.  See <a href="#">Section 10.8.1 on page 238</a> to view the <b>Brief Summary</b> screen.
Full Summary	Select a volume and click this to display more detailed information about the volume.  See <a href="#">Section 10.8.1 on page 238</a> to view the <b>Full Summary</b> screen.
The table lists your hard disks. Click a column’s heading to sort the entries by that criteria.	
Status	This shows the condition of the hard disk volume. Go to <a href="#">Section 7.5.3 on page 155</a> for more information.
Name	This shows the name assigned to the hard disk.
Temperature	This shows the temperature of the hard disk in degrees celsius.

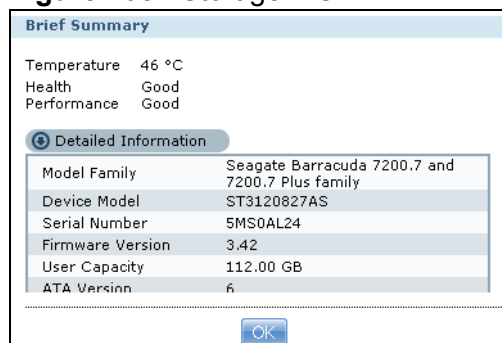
**Table 59** Storage > S.M.A.R.T

LABEL	DESCRIPTION
Performance	<p>This shows your hard disk's performance. Refer to <a href="#">Section 10.8.2 on page 239</a> for more information on how S.M.A.R.T determines your hard disk's condition. This displays:</p> <ul style="list-style-type: none"> <li>• <b>Good</b> - This shows when you compare each <b>Value</b> with the <b>Threshold Value</b> and all the <b>Value</b> is greater than the <b>Threshold Value</b>.</li> <li>• <b>Bad</b> - This shows when you compare each <b>Value</b> with the <b>Threshold Value</b> and at least one <b>Value</b> is less than or equal to the <b>Threshold Value</b>.</li> </ul>
Type	<p>This shows volume type or file system that the hard disk is using, such as <b>JBOD</b>, <b>PC Compatible Volume</b> and <b>RAID</b> or <b>FAT32</b>, <b>FAT16</b> and <b>NTFS</b>.</p> <p>See <a href="#">Section 7.5.2 on page 154</a> for descriptions of the volume types.</p>
Volume Name	This shows the name of the hard disk volume.
Model Name	This shows the factory model of the hard disk.
Capacity	This shows the total hard disk space of the hard disk volume.

## 10.8.1 SMART Brief Summary

Use this screen to display information about the volume, such as the hard disk vendor, specific model, hard disk capacity and so on.

Click **Brief Summary** in the **Storage > S.M.A.R.T** screen to display the following.

**Figure 105** Storage > S.M.A.R.T: Brief Summary

The following table describes the labels in this screen.

**Table 60** Storage > S.M.A.R.T: Brief Summary

LABEL	DESCRIPTION
Brief Summary	
Temperature	This shows the current temperature of the hard disk in degrees celsius.

**Table 60** Storage > S.M.A.R.T: Brief Summary

LABEL	DESCRIPTION
Health	This describes the overall health of the volume based on S.M.A.R.T diagnostics.
Performance	<p>This shows your hard disk's performance. Refer to <a href="#">Section 10.8.2 on page 239</a> for more information on how S.M.A.R.T determines your hard disk's condition. This displays:</p> <ul style="list-style-type: none"> <li>• <b>Good</b> - This shows when you compare each <b>Value</b> with the <b>Threshold Value</b> and all the <b>Value</b> is greater than the <b>Threshold Value</b>.</li> <li>• <b>Bad</b> - This shows when you compare each <b>Value</b> with the <b>Threshold Value</b> and at least one <b>Value</b> is less than or equal to the <b>Threshold Value</b>.</li> </ul>
Detailed Information	
Model Family	This shows the vendor and product family of the hard disk.
Device Model	This shows the factory model of the hard disk.
Serial Number	This shows the serial number of the hard disk.
Firmware Version	This shows the firmware version installed in the hard disk.
User Capacity	This shows the total hard disk space of the hard disk volume.
ATA Version	This shows the ATA version of the hard disk, which refers to an industry standard category for storage devices and connectors used.
ATA Standard	This field displays the Advanced Technology Attachment standard the hard drive supports.
Local Time	This field displays the local time that the hard drive is using.
SMART support	This field displays whether or not the hard drive is SMART-capable.
SMART support	This field displays whether or not the hard drive has SMART monitoring turned on.
OK	Click this to close the window.

## 10.8.2 SMART Full Summary

Use this screen to display more details information about the volume.

Click **Full Summary** in the **Storage > S.M.A.R.T** screen to display the following.

**Figure 106** Storage > S.M.A.R.T: Full Summary

Full Summary								
ID	Attribute Name ^	Flag	Value	Worst	Threshold	Type	Updated	When Failed
197	Current_Pending_Sector	0x0012	100	100	000	Old_age	Always	-
195	Hardware_ECC_Recovered	0x001a	063	045	000	Old_age	Always	-
200	Multi_Zone_Error_Rate	0x0000	100	253	000	Old_age	Offline	-
198	Offline_Uncorrectable	0x0010	100	100	000	Old_age	Offline	-
12	Power_Cycle_Count	0x0032	100	100	020	Old_age	Always	-
9	Power_On_Hours	0x0032	097	097	000	Old_age	Always	-
1	Raw_Read_Error_Rate	0x000f	063	045	006	Pre-fail	Always	-
5	Reallocated_Sector_Ct	0x0033	100	100	036	Pre-fail	Always	-
7	Seek_Error_Rate	0x000f	082	040	030	Pre-fail	Always	-

The following table describes the labels in this screen.

**Table 61** Storage > S.M.A.R.T: Full Summary

LABEL	DESCRIPTION
ID	This is the identification number used to tag a hard disk attribute.  This is standard across all S.M.A.R.T-enabled storage devices. However it depends on the storage vendor which attributes it will allow S.M.A.R.T to diagnose.
Attribute Name	This refers to an attribute of the hard disk that S.M.A.R.T can assess. Attributes describe the hard disk's physical state, performance, wear-and-tear, and so on.
Flag	This shows a code that S.M.A.R.T uses to determine the current state of the hard disk.
Value	This is a value that corresponds to the <b>Raw Value</b> . Compare this with the <b>Threshold Value</b> .  S.M.A.R.T compresses the raw value(s) into a digit from 1 to 253, where 1 indicates the worst scenario while 253 indicates the best scenario.  The values 100 or 200 usually represent the mean or normal value.
Worst	This is the lowest value attained by the hard disk since S.M.A.R.T started its assessment of the hard disk.
Threshold	This is the attribute's threshold value. If the attribute's current normalized value is less than or equal to the threshold, the attribute has failed. An attribute value close to or below the threshold indicates the hard drive is no longer reliable.
Type	This shows S.M.A.R.T's assessment of the hard disk.  <b>Old_age</b> indicates end-of-product life from old-age (normal wearing out) if the attribute value is less than or equal to the threshold.  <b>Pre-fail</b> indicate imminent hard drive failure if the attribute value is less than or equal to the threshold.  Note that just because an attribute is of the Pre-fail type does not mean your hard drive is ready to fail. It only means this if the current normalized value of the attribute is less than or equal to the threshold.
Updated	This indicates when the hard drive updates the value for this attribute.  <ul style="list-style-type: none"> <li>• <b>Always</b> means the hard drive updates this attribute during normal operation and during offline activities.</li> <li>• <b>Offline</b> means the hard drive only updates this attribute when no one is accessing the hard drive.</li> </ul>

**Table 61** Storage > S.M.A.R.T: Full Summary

LABEL	DESCRIPTION
When Failed	<p>This column indicates when (if ever) the attribute failed. An attribute has failed if the normalized value is less than or equal to the threshold.</p> <ul style="list-style-type: none"> <li>• <b>-:</b> This displays if the attribute is not failing now and has never failed in the past.</li> <li>• <b>FAILING_NOW:</b> This displays if the attribute's current normalized value is less than or equal to the threshold.</li> <li>• <b>In the past:</b> This displays if the attribute's current normalized value is greater than the threshold but the worst recorded value is less than or equal to the threshold.</li> </ul>
Raw Value	<p>This is the attribute's unprocessed raw data. These values show exact amounts of time or numbers of attempts or errors. The meaning to the raw values is specific to the hard drive manufacturer. Table 42 on page 156 has some information about whether a higher or lower individual raw S.M.A.R.T. attribute value is better.</p>
OK	Click this to close this window.

## 10.9 Protect Screens

The **Protect** screens include:

- **Backup** screens - These include steps to create and customize backup jobs.
- **Restore** screens - These include steps to restore previous backups made with the NSA.

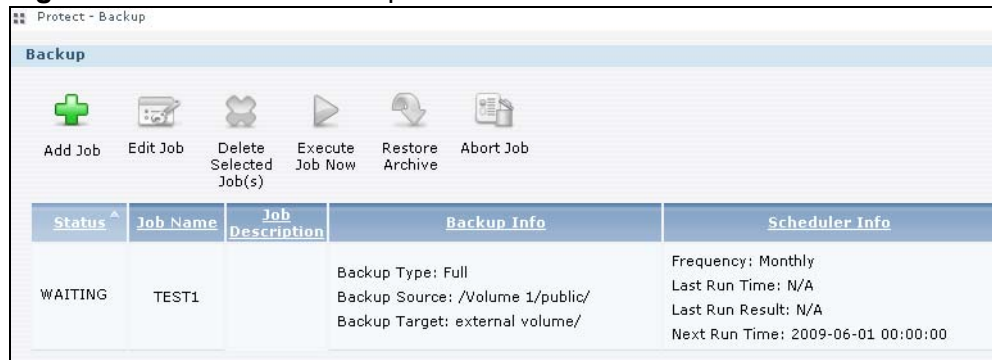
## 10.10 Backup Screens

Use this screen to create and customize scheduled backup jobs for your files.

You can have several backup jobs for specific folders and time periods.

Click **Protect > Backup** to open the following screen.

**Figure 107** Protect > Backup



The following table describes the labels in this screen.

**Table 62** Protect > Backup

LABEL	DESCRIPTION
Backup	
Add Job	Click this to create and customize a backup job.
Edit Job	Select a backup job in the list and click this to make some changes to it.
Delete Selected Job(s)	Select a backup job in the list and click this to delete it.
Execute Job Now	Select a backup job in the list and click this to run the backup job immediately.
Restore Archive	Select a backup job in the list and click this to restore the file(s) included in that backup job to the NSA.  This applies to Archive backups only. Refer to <a href="#">Section 10.10.8 on page 254</a> to see the screens.
Abort Job	Select a backup job in the list and click this to stop the process if the backup job is currently active.
Status	This shows the current state of the backup job. <ul style="list-style-type: none"> <li>• <b>Waiting</b> means the backup job is not active but is scheduled to run at some time.</li> <li>• <b>Running</b> indicates that the NSA is currently doing the backup job. When the backup job is running, you can also see a progress bar.</li> </ul>
Job Name	This identifies the backup job.
Job Description	This is a short description of the backup job.
Backup Info	This lists down the backup job details: type, source and target. Refer to <a href="#">Section 10.10.1 on page 243</a> and <a href="#">Section 10.10.2 on page 245</a> .
Scheduler Info	This shows the backup schedule, including the frequency, the time it was last run in (and whether or not it succeeded), and when it is scheduled to run again. The times use yyyy-mm-dd hh:mm:ss format.  Refer to <a href="#">Section 10.10.4 on page 249</a> .

### 10.10.1 Backup: Step 1

Use this screen to specify the job information and back up type.

Click **Add Job** in the **Protect > Backup** screen to open the following:

**Figure 108** Protect > Backup: Step 1

Protect - Backup

Add a new backup Job

Step 1

Job Information

Job Name: Test1

Job Description:

Backup Type

☒ Archive

☐ Full

☒ Incremental

Perform a full backup job after 30 increments (Max: 30)

☐ Synchronization

Next

The following table describes the labels in this screen.

**Table 63** Protect > Backup: Step 1

LABEL	DESCRIPTION
Job Information	
Job Name	Enter a name to identify the backup job.
Job Description	Enter a short description (up to 100 keyboard characters) for the backup job.

**Table 63** Protect > Backup: Step 1

LABEL	DESCRIPTION
Backup Type	<p>Choose the backup type that you want the NSA to implement for the backup job.</p> <p><b>Archive</b> - This is a backup of the source folder in an archive format. Once you backup your files in the target folder, you cannot access the files individually unless you have the extracting tool used by the NSA. If there are existing files in the target folder prior to the NSA's backup job, the files remain undisturbed. You can also choose between the following types of archive:</p> <ul style="list-style-type: none"> <li>• <b>Full</b> - The NSA does a fresh backup each time. This provides the most protection but also requires the most storage space.</li> <li>• <b>Incremental</b> - The NSA backs up new or modified files from the source folder since the last backup. The first backup is a full backup. You can also do a full backup after several incremental backups. Enter how many incremental backups the NSA runs before it performs a full backup of the source folder. You must keep the latest full backup to be able to restore the files later.</li> </ul> <p><b>Synchronization</b> - This does a backup of individual files. If you use this type, you cannot use the <b>Restore</b> feature of the NSA. You can also choose between the following types of synchronization:</p> <ul style="list-style-type: none"> <li>• <b>Mirror</b> - The NSA deletes all data in the target folder before running the backup. It makes a copy of the source files.</li> <li>• <b>Publish</b> - The NSA does a backup of individual files to the target folder without overwriting existing files in that folder. It makes the target folder identical to the source folder.</li> </ul>
Next	Click this to go to the next step.



## 10.10.2 Backup: Step 2

Use this screen to specify where the files you want to backup are located and set where you want the backup to be stored.

**Figure 109** Protect > Backup: Step 2

The screenshot shows a window titled "Protect - Backup" with a subtitle "Add a new backup Job". The main content area is labeled "Step 2".

**Backup Source:** A dropdown menu is set to "Volume 1". Below it is a section titled "Selected Source Folders" with an upward-pointing arrow.













**Backup Target:** The "Remote" radio button is selected. To its right are four input fields labeled "Remote NSA Address", "Username", "Password", and "Share Name". Below these fields is a "Test Connection" button.

At the bottom, there are two unselected radio buttons: "Local" and "External".

At the bottom right, there are two buttons: "Previous" and "Next".

The following table describes the labels in this screen.

**Table 64** Protect > Backup: Step 2

LABEL	DESCRIPTION
Backup Source	<p>Select an (internal) volume and the folders and files to back up using this tree interface.</p> <p>Click  to browse through folders, sub-folders and files.</p> <p>Click  to close a folder in the tree. This is useful if there are many folders or files that you wish to hide from view.</p> <p>Click  to select a folder or file to back up. This also selects all sub-folders and files.</p> <p>Click  to deselect the folder or file. This also de.selects all sub-folders and files.</p> <p><b>More ...</b>  and <b>More ...</b>  appear when there are too many folders/files to display. Click the arrows to scroll up or down through the folders/files.</p> <p> for a folder means all sub-folders and files and new folders/files added later will be backed up.</p> <p> for a file means the file will be backed up.</p> <p> (a grayed out check box) for a folder means that only some sub-folders and files under the folder will be backed up. Newly added folders/files will NOT be backed up.</p> <p> means the file structure is still loading. Please wait for the folders/files to display.</p> <p><b>Note:</b> If you select to back up an entire folder  and then de-select a sub-folder or file within that folder, the main folder icon will turn  and any new sub-folders and files added to this main folder after the initial backup configuration will <b>NOT</b> be backed up.</p> <p>A list of your select folders and files displays below the selection fields.</p>
Selected Source Folders	This shows the path of the backup source folder you selected.
Backup Target	Select the target folder where you want to place your backup.

**Table 64** Protect > Backup: Step 2

LABEL	DESCRIPTION
Remote	<p>Select this to back up to another device.</p> <p>For Archives:</p> <p>The remote device can be another NSA in the network. Fill in the following fields in order to be able to access it.</p> <ul style="list-style-type: none"> <li>• Remote NSA Address</li> <li>• Username</li> <li>• Password</li> <li>• Share Name</li> </ul> <p>Click <b>Test Connection</b> to see if your NSA can communicate with the remote device.</p> <p>For Synchronization:</p> <p>The remote device must be another NSA compatible with the NSA's synchronization feature. Fill in the following fields in order to be able to access it.</p> <ul style="list-style-type: none"> <li>• Remote NSA Address</li> <li>• Username</li> <li>• Remote Admin's Password</li> </ul> <p>Click <b>Show target content</b> to connect to the remote NSA so you can select the target share for the backup.</p>
Local	Select this if you want to place your backup in another volume in the NSA. Select the folder where you want to place the backup.
External	Select this if you have a USB hard disk connected to the NSA that you want to use for your backup. Select the folder where you want to place the backup.
Previous	Click this to go back to the previous screen.
Next	Click this to go to the next screen.

### 10.10.3 Backup: Step 3

Use this screen to specify compression, encryption and purge policies for the backup job. This step is only available if you are doing an archive backup or a synchronization backup to a remote target.

**Figure 110** Protect > Backup: Step 3

Protect - Backup

Add a new backup Job

Step 3

**Compression**

☐ Yes

☒ No

**Encryption**

☐ Yes

☒ No

Bandwidth :  KB/s (0 for no limitation)

**Purge Policy**

☒ Keep All Old Backup files

☐ Keep Only the last  backup files(1-30)

☐ Keep Backups For  day(s)(1-3650)

Previous Next

The following table describes the labels in this screen.

**Table 65** Protect > Backup: Step 3

LABEL	DESCRIPTION
Compression	<p>Select <b>Yes</b> if you want NSA to compress the files for your backup. Otherwise, choose <b>No</b>.</p> <p>In an <b>Archive</b> backup, compression is a method of packing computing files in a way that saves hard disk space.</p> <p>For a <b>Synchronization</b> backup (to a remote target), the source data will be compressed before the transmission to reduce the transmission time. It is used in slow networks only.</p>
Encryption	<p>Select <b>Yes</b> if you want NSA to encrypt the files for your backup. Otherwise, choose <b>No</b>.</p> <p>In an <b>Archive</b> backup, this means using a password to secure files.</p> <p>For a <b>Synchronization</b> backup (to a remote target), this means securing the file transfer session. However the final file stored on the remote NSA is unencrypted. This takes a long time. Make sure you really need this feature before enabling it.</p>
Bandwidth	<p>Restrict the bandwidth of synchronization backups to help stop them from using all of your network connection's available bandwidth. This is more important when backing up to a remote NSA or computer through the Internet.</p>

**Table 65** Protect > Backup: Step 3

LABEL	DESCRIPTION
Purge Policy	<p>The NSA maintains the files that have been included in your backups. However to save hard disk space, you can choose to delete files that have been included in previous backups.</p> <ul style="list-style-type: none"> <li>Select <b>Keep All Old Backup files</b> to store all files that have been included in previous backups.</li> <li>If you want to store a certain number of backup files, select <b>Keep Only the last n backup files (1-30)</b>. Enter a value (n) from 1 to 30 to specify how many backups the NSA stores. All backup files older than the last one are deleted. You will not be able to recover files that existed (only) in those previous backups. Select this if backup space is limited and recovery of old files is not important.</li> <li>If you want to store all backups for a certain time period, select <b>Keep Backups for n day(s) (1-3650)</b>. Enter a value (n) from 1 to 3650 to specify how many days the NSA stores all backup files. After this day has expired, all backup files will be deleted.</li> </ul>
Previous	Click this to go back to the previous screen.
Next	Click this to go to the next screen.

## 10.10.4 Backup: Step 4

Click this to specify the schedule for the backup job. The backup job automatically runs according to the schedule that you set in this screen.

**Figure 111** Protect > Backup: Step 4

Protect - Backup

Add a new backup Job

Step 4

**Scheduler**

Backup Frequency: Monthly

Start Time (hh:mm): 0:00

Step 1: Please select the month(s) of a year

☐ January ☐ February ☐ March ☐ April ☐ May ☐ June

☐ July ☐ August ☐ September ☐ October ☐ November ☐ December

Step 2: Please select the day of the month

☒ \* Day

☐ First Monday

Previous Done

The following table describes the labels in this screen.

**Table 66** Protect > Backup: Step 4

LABEL	DESCRIPTION
Scheduler	
Backup Frequency	Select from <b>Hourly</b> , <b>Daily</b> , <b>Weekly</b> and <b>Monthly</b> backup intervals. The screen changes depending on the item you select.

**Table 66** Protect > Backup: Step 4

LABEL	DESCRIPTION
Every how many hours?	This is only available if you selected <b>Hourly</b> as your backup frequency.  Select every how many hours the NSA performs the backup job.
On which minute of the hour?	This is only available if you selected <b>Hourly</b> as your backup frequency.  Select the minute (from 0 to 59) in an hour when the NSA performs the backup job.
Start Time (hh:mm)	This is available if you selected <b>Daily, Weekly</b> or <b>Monthly</b> as your backup frequency.  Select the time in hour:minute format when you want the NSA to perform the backup job.
Every how many days?	This is only available if you selected <b>Daily</b> as your backup frequency.  Enter the interval between days when the NSA performs the backup job.
Every how many weeks?	This is only available if you selected <b>Weekly</b> as your backup frequency.  Enter the interval between weeks when NSA performs the backup job.
Step 1: Please select the month(s) of a year	This is only available if you selected <b>Monthly</b> as your backup frequency.  Select the month(s) when you want the NSA to perform the backup job.
Step 2: Please select the day of the month	This is only available if you selected <b>Monthly</b> as your backup frequency.  Select the day in a month when you want the NSA to perform the backup job.
Previous	Click this to go back to the previous screen.
Done	Click this to close the screen.

## 10.10.5 Edit Job Screen

Use this screen to edit an existing backup job. Some attributes of the backup job cannot be changed, such as the name, backup type, source folder and so on.

## 10.10.6 Edit Job: Step 1

Click **Protect > Backup**. Select a backup job from the list and click **Edit Job** to open the following.

**Figure 112** Protect > Backup > Edit: Step 1

The screenshot shows a web-based configuration window titled "Protect - Backup". Inside, there's a section labeled "Step 1" with a sub-header "Job Settings". The settings are as follows:

- Job Name**: Example\_Backup
- Job Description**: This is an example.
- Backup Type**: incremental
- Source folder(s)/file(s)**: Volume 1/music/
- Backup Target**: External Volume
- Target Path**: silicon--power-0-001/
- Compression**: No
- Encryption**: No
- Bandwidth**: N/A KB/s (0 for no limitation)
- Purge Policy**:
  - ☒ Keep All Old Backup files
  - ☐ Keep Only the last [ ] backup files(1-30)
  - ☐ Keep Backups For [ ] day(s)(1-3650)

A "Next" button is located at the bottom right of the form.

The following table describes the labels in this screen.

**Table 67** Protect > Backup > Edit: Step 1

LABEL	DESCRIPTION
Job Settings	
Job Name	This field is read-only and shows the name of the backup job.
Job Description	Enter a short description for the backup job.
Backup Type	This field is read-only and shows the backup type.
Source folder(s)/file(s)	This is read-only and shows the path of the source folder for backup.
Backup Target	This field is read-only and shows on which volume (whether internal or external) the backup files are stored. If the target location is a remote NSA, this shows the remote IP address.
Target Path	This field is read-only and shows the target folder for the backup files.

**Table 67** Protect > Backup > Edit: Step 1

LABEL	DESCRIPTION
Compression	<p>This field is read-only and shows whether the backup employs compression.</p> <p>Compression reduces the size of the file that you want to back up. Backup is then faster, but restoring may be slower, so if backup space is not a concern and recovery speed is, then turn off compression.</p>
Encryption	<p>This field is read-only and shows whether the backup employs encryption.</p> <p>You can have the NSA use a password to encrypt the backup files.</p>
Bandwidth	<p>For backups to a remote NSA, you can restrict the bandwidth to help prevent the backups from using all of your network connection's available bandwidth. This is more important when backing up to a remote NSA or computer through the Internet.</p>
Purge Policy	<p>The NSA maintains the files that have been included in your backups. However to save hard disk space, you can choose to delete files that have been included in previous backups.</p> <ul style="list-style-type: none"> <li>• Select <b>Keep All Old Backup files</b> to store all files that have been included in previous backups.</li> <li>• If you want to store a certain number of backup files, select <b>Keep Only the last n backup files (1-30)</b>. Enter a value (n) from 1 to 30 to specify how many backups the NSA stores. All backup files older than the last one are deleted. You will not be able to recover files that existed (only) in those previous backups. Select this if backup space is limited and recovery of old files is not important.</li> <li>• If you want to store all backups for a certain time period, select <b>Keep Backups for n day(s) (1-3650)</b>. Enter a value (n) from 1 to 3650 to specify how many days the NSA stores all backup files. After this day has expired, all backup files will be deleted.</li> </ul>
Next	Click this to go to the next screen.



## 10.10.7 Edit Job: Step 2

Use this screen to edit the schedule for the backup job.

**Figure 113** Protect > Backup > Edit: Step 2

**Step 2**

**Scheduler Settings**

Backup Frequency: Monthly

Start Time (hh:mm) 1:00

Step 1: Please select the month(s) of a year

☐ January ☐ February ☐ March ☐ April ☐ May ☐ June

☐ July ☐ August ☐ September ☐ October ☒ November ☐ December

Step 2: Please select the day of the month

☐ \* Day

☒ First Sunday

Previous Done

The following table describes the labels in this screen.

**Table 68** Protect > Backup > Edit: Step 2

LABEL	DESCRIPTION
Scheduler Settings	
Backup Frequency	Edit this by selecting from <b>Hourly</b> , <b>Daily</b> , <b>Weekly</b> and <b>Monthly</b> backup intervals. The screen changes depending on the item you select.
Every how many hours?	This is only available if you selected <b>Hourly</b> as your backup frequency.  Select every how many hours the NSA performs the backup job.
On which minute of the hour?	This is only available if you selected <b>Hourly</b> as your backup frequency.  Select the minute (from 0 to 59) in an hour when the NSA performs the backup job.
Start Time (hh:mm)	This is available if you selected <b>Daily</b> , <b>Weekly</b> or <b>Monthly</b> as your backup frequency.  Select the time in hour:minute format when you want the NSA to perform the backup job.
Every how many days?	This is only available if you selected <b>Daily</b> as your backup frequency.  Enter the interval between days when the NSA performs the backup job.
Every how many weeks?	This is only available if you selected <b>Weekly</b> as your backup frequency.  Enter the interval between weeks when NSA performs the backup job.

**Table 68** Protect > Backup > Edit: Step 2

LABEL	DESCRIPTION
Step 1: Please select the month(s) of a year	This is only available if you selected <b>Monthly</b> as your backup frequency.  Select the month(s) when you want the NSA to perform the backup job.
Step 2: Please select the day of the month	This is only available if you selected <b>Monthly</b> as your backup frequency.  Select the day in a month when you want the NSA to perform the backup job.
Previous	Click this to go back to the previous screen.
Done	Click this to close the screen.

## 10.10.8 Restore Archive Screen

Use this screen to restore previous backups made with the NSA.

## 10.10.9 Restore Archive: Step 1

Click **Protect > Backup** screen ([Section 10.10 on page 241](#)). You can restore a previous backup job by selecting a backup job from the list and clicking **Restore Archive**.

**Figure 114** Protect > Backup > Restore Archive: Step 1

The screenshot shows a software interface titled 'Restore'. Under the heading 'Step 1. Select Restore Point', there is a tab labeled 'Job Information'. This tab contains a table with the following data:

Job Name:	Example F
Job Description:	Example F
Backup Type:	full
Scheduler Information:	every month

Below the table is a section titled 'Restored Time' which displays the date and time '2009-06-09 16:19:31'. A 'Next' button is located at the bottom right of the screen.

The following table describes the labels in this screen.

**Table 69** Protect > Backup > Restore Archive: Step 1

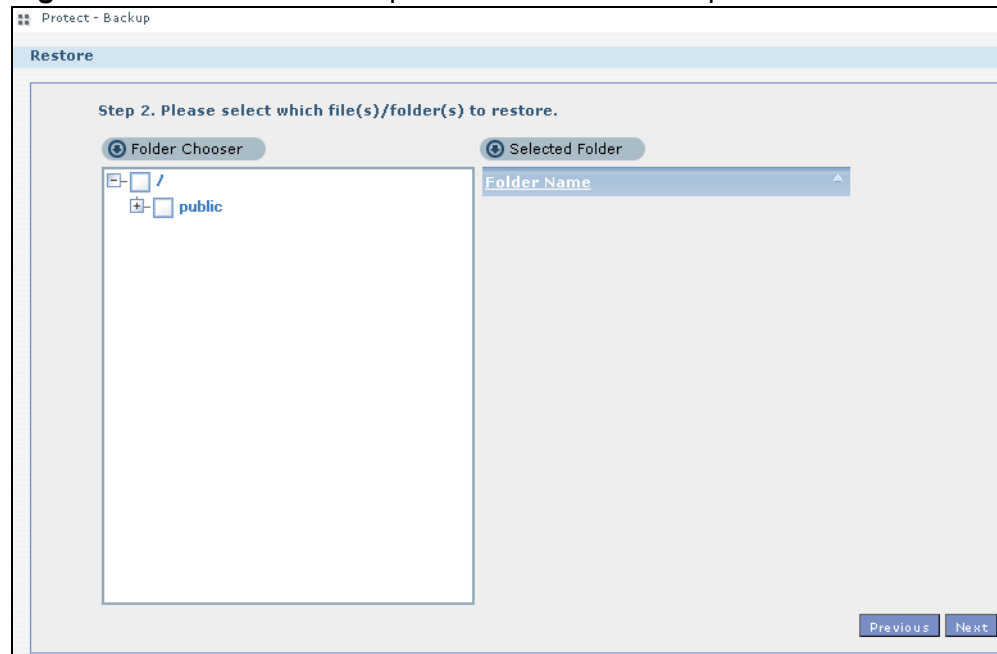
LABEL	DESCRIPTION
Step 1. Select Restore Source	Select a previous archive backup that you want to restore to the NSA.
Job Information	
Job Name	This is the name to identify the backup job.

**Table 69** Protect > Backup > Restore Archive: Step 1

LABEL	DESCRIPTION
Job Description	This is a short description (up to 100 keyboard characters) for the backup job.
Backup Type	This is the type of backup implemented for the backup job.
Scheduler Information	This field displays the backup's frequency.
Restored Time	Select a previous backup in the list that you want to restore to your NSA.
Next	Click this to go to the next screen.

## 10.10.10 Restore Archive: Step 2

Use this screen to select the folder where the archive you want to restore is located.

**Figure 115** Protect > Backup > Restore Archive: Step 2

The following table describes the labels in this screen.

**Table 70** Protect > Backup > Restore Archive: Step 2

LABEL	DESCRIPTION
Step 2. Please select which file(s)/folder(s) to restore.	
Folder Chooser	Select the folder where the backup you want to restore is located.
Selected Folder	This shows the path of the folder you selected.
Previous	Click this to go back to the previous screen.
Next	Click this to go to the next screen.

## 10.10.11 Restore Archive: Step 3

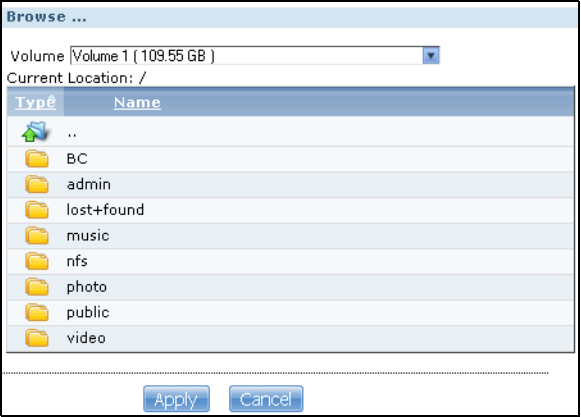
Use this screen to select the location in the NSA where you want to restore your backup.

**Figure 116** Protect > Backup > Restore Archive: Step 3



The following table describes the labels in this screen.

**Table 71** Protect > Backup > Restore Archive: Step 3

LABEL	DESCRIPTION
Step 3. Set a restore target and start restoring	
Original Location	Select this to restore the files to their original location in the NSA.
Other Location	<p>Click this to select a folder where you want to place the restored files. Click <b>Browse</b> to open the following screen.</p>  <ul style="list-style-type: none"> <li>• <b>Volume</b> - Select a volume from the list.</li> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Type</b> - This identifies the item as a file or folder.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>
Previous	Click this to go back to the previous screen.
Done	Click this to run the restore process and go back to the <b>Backup</b> screen.

## 10.11 Restore Screen

Use this screen to restore previous backups made with the NSA, including archives and folders from internal, external or remote NSAs to the NSA.

### 10.11.1 Restore: Step 1

You can access this screen by clicking **Protect > Restore**.

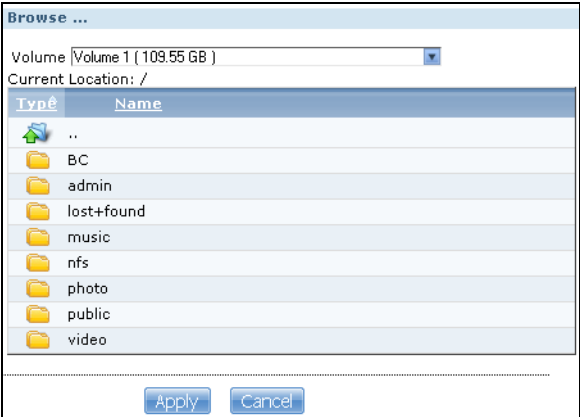
**Figure 117** Protect > Restore: Step 1

The following table describes the labels in this screen.

**Table 72** Protect > Restore: Step 1

LABEL	DESCRIPTION
Step 1. Select Restore Source	Select a previous archive backup that you want to restore to the NSA.  Select <b>Remote NSA</b> if the file is in another NSA in the network that you used for your backup. Fill in the fields below when you choose this option.  Select <b>Internal or External Volume</b> if you want to use another volume in the NSA or an attached USB hard disk for your backup. Click <b>Browse</b> to select the backup file.
IP Address	Enter the address of the NSA you want to use.
User	Enter the username you use to access the NSA.
Password	Enter the password of your NSA account.
Share Name	Enter the name of the share you want to use.
Test Connection	Click this to test your connection to the remote NSA that you have specified in the fields above.

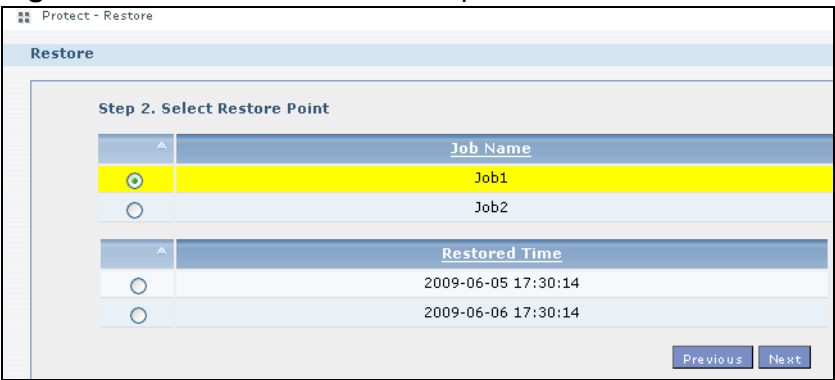
**Table 72** Protect > Restore: Step 1

LABEL	DESCRIPTION
Browse	<div>Click this to select where the previous backup that you want to restore is located.</div> <div></div> <div><ul style="list-style-type: none"><li>• <b>Volume</b> - Select a volume from the list.</li><li>• <b>Current Location</b> - This is the location of the selected folder.</li><li>• <b>Type</b> - This identifies the item as a file or folder.</li><li>• <b>Name</b> - This is the name of the folder/file.</li></ul><div>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</div></div>
Next	Click this to go to the next screen.

10.11.2 Restore: Step 2

Select a previous archive backup that you want to restore to the NSA.

**Figure 118** Protect > Restore: Step 2



The following table describes the labels in this screen.

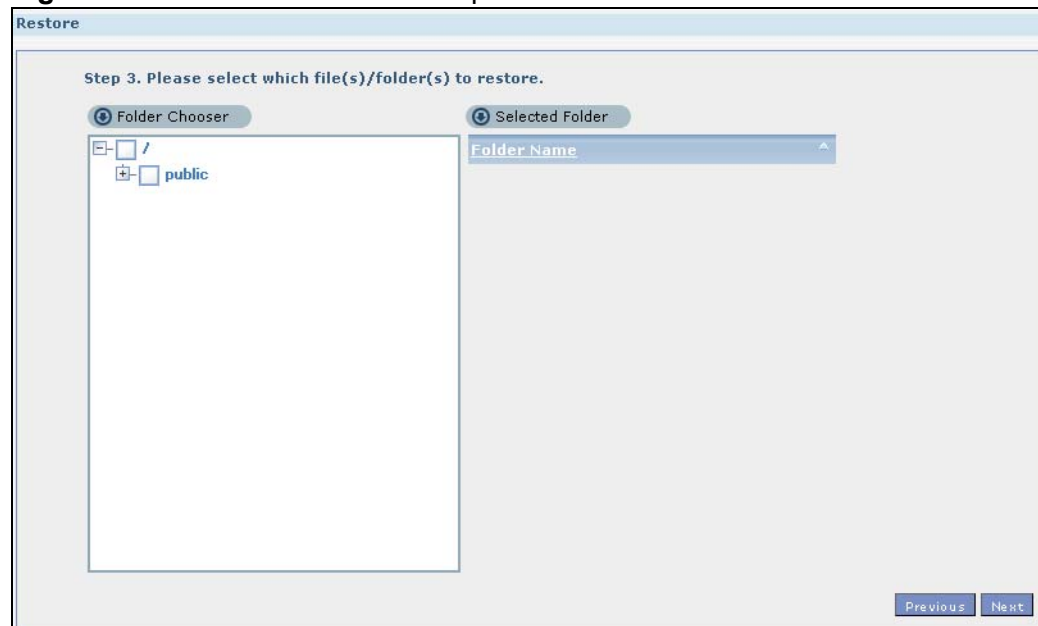
**Table 73** Protect > Restore: Step 2

LABEL	DESCRIPTION
Step 2. Select Restore Point	If you selected <b>Remote NSA</b> for the backup you want to restore, you can see a list of all the backups you performed in the <b>Job Name</b> table.  If you selected <b>Internal or External Volume</b> for the backup you want to restore, you can see a list of restore times for the backups you performed in the <b>Restored Time</b> table.
Job Name	Select a previous backup job in the list that you want to restore to your NSA. Once you choose a job name, all available restore times for that backup job shows in the <b>Restored Time</b> table.
Restored Time	Select a previous backup job in the list that you want to restore to your NSA.
Previous	Click this to go back to the previous screen.
Next	Click this to go to the next screen.

### 10.11.3 Restore: Step 3

Use this screen to select the folder where the archive you want to restore is located.

**Figure 119** Protect > Restore: Step 3



The following table describes the labels in this screen.

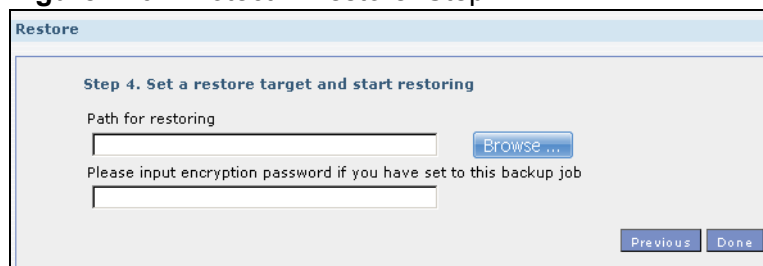
**Table 74** Protect > Restore: Step 3

LABEL	DESCRIPTION
Step 3. Please select which file(s)/folder(s) to restore.	
Folder Chooser	Select the folder where the backup you want to restore is located.
Selected Folder	This shows the path of the folder you selected.
Previous	Click this to go back to the previous screen.
Next	Click this to go to the next screen.

## 10.11.4 Restore: Step 4

Use this screen to select the location in the NSA where you want to restore your backup.

**Figure 120** Protect > Restore: Step 4



Restore

Step 4. Set a restore target and start restoring

Path for restoring

[Browse ...](#)

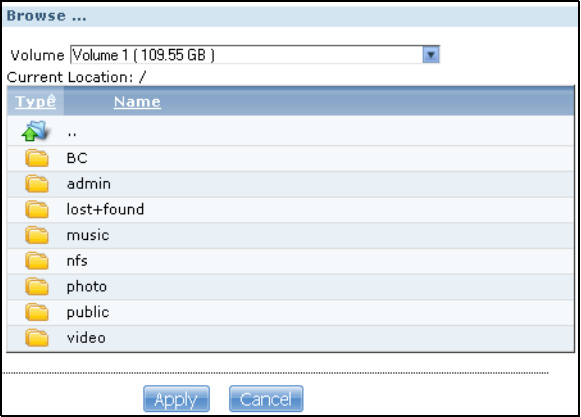
Please input encryption password if you have set to this backup job

[Previous](#) [Done](#)



The following table describes the labels in this screen.

**Table 75** Protect > Restore: Step 4

LABEL	DESCRIPTION
Step 3. Set a restore target and start restoring	
Browse	<p>Click this to select a folder where you want to place the restored files.</p>  <ul style="list-style-type: none"> <li>• <b>Volume</b> - Select a volume from the list.</li> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Type</b> - This identifies the item as a file or folder.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>
Previous	Click this to go back to the previous screen.
Done	Click this to run the restore process and go back to the <b>Backup</b> screen.

## 10.12 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

### 10.12.1 S.M.A.R.T Attributes

The following table describes some common S.M.A.R.T. attributes. If a higher or lower raw attribute value is better, it is indicated in the **BETTER** column. Since

S.M.A.R.T. attributes and their definitions vary by manufacturer, refer to the hard drive manufacturer for details about the attributes your hard drive supports.

**Table 76** S.M.A.R.T. Attributes

ID	ATTRIBUTE NAME	BETTE R	DESCRIPTION
01	Read Error Rate	Low	Shows the rate of hardware read errors. If this is not zero, there is a problem with the disk surface or the read/write heads.
02	Throughput Performance	High	This is the hard drive's general (overall) throughput performance. A decreasing value indicates a problem.
03	Spin-Up Time	Low	This is the average number of milliseconds the hard drive took for spindle spin up (from zero RPM to fully operational).
04	Start/Stop Count		The total number of spindle start and stop cycles.
05	Reallocated Sectors Count	Low	Total number of reallocated sectors on the hard drive. When the hard drive detects a read/write/verification error, it marks the sector as "reallocated" and transfers the data to a specially reserved (spare) area. The process is also known as remapping with "reallocated" sectors known as remaps. The more sectors the hard drive has to reallocate, the slower read and write speeds become.
06	Read Channel Margin		This is the margin of a channel when it reads data.
07	Seek Error Rate	Low	This is the rate of the magnetic heads' seek errors. A failure in the mechanical positioning system, such as servo damage or a thermal widening of the disk, results in seek errors. An increasing number of seek errors indicate the condition of the disk surface and the mechanical subsystem are worsening.
08	Seek Time Performance	High	This is an average performance indicator for the seek operations of the magnetic heads. Mechanical subsystem problems cause this value to decrease.
09	Power-On Hours (POH)	Low	This is how many hours the hard drive has been in a power-on state. The raw value lists the total number of hours (or minutes, or seconds depending on the manufacturer).
10	Spin Retry Count	Low	This is the total number of spin start retry attempts. This is the number of attempts to spin up to fully operational speed the hard drive has made when the first attempt did not succeed. An increase in this value is an indicator of hard disk mechanical subsystem problems.
11	Recalibration Retries	High	This is the number of times recalibration was requested when the first attempt did not succeed. A decrease in this value is an indicator of hard disk mechanical subsystem problems.
12	Device Power Cycle Count		This is the number of times the hard drive has gone through a full power on and power off.
13	Soft Read Error Rate	Low	This is the number of uncorrected read errors the hard drive has reported. If this is not zero, back up your data.

**Table 76** S.M.A.R.T. Attributes (continued)

ID	ATTRIBUTE NAME	BETTE R	DESCRIPTION
190	Airflow Temperature	Low	This indicates the temperature of the airflow measured by a Western Digital hard drive.
190	Temperature Difference from 100	High	This indicates the value of 100 - the temperature in degrees Celsius. Manufacturers can set a minimum threshold that corresponds to a maximum temperature.
191	G-sense error rate	Low	This is the number of mistakes caused by impact loads.
192	Power-off Retract Count	Low	This is how many times the heads are loaded off the media.
193	Load/Unload Cycle	Low	This is the number of load and unload cycles into head landing zone position.
194	Temperature	Low	This is the hard drive's internal temperature.
195	Hardware ECC Recovered	High	This is the time between ECC (Error Correction Code)-corrected errors.
196	Reallocation Event Count	Low	This is the total number of reallocation (remap) operations. The raw value is the total attempts to move data from reallocated sectors to a spare area. Successful and unsuccessful attempts are both included.
197	Current Pending Sector Count	Low	This is the number of unstable sectors awaiting reallocation. If the sector is later successfully written or read, this value decreases and reallocation is not performed. Only failed write attempts cause a reallocation, not read errors. This can be difficult to test since only direct I/O writes to the disk cause reallocations, not cached writes.
198	Uncorrectable Sector Count	Low	This is the number of errors reading or writing a sector that were not correctable. An increase in this value is an indicator of disk surface defects or mechanical subsystem problems.
199	UltraDMA CRC Error Count	Low	This is the number of data transfer errors through the interface cable according to the ICRC (Interface Cyclic Redundancy Check).
200	Write Error Rate / Multi-Zone Error Rate	Low	This is the total number of errors in writing sectors.
201	Soft Read Error Rate	Low	This is the number of read/write head off-track errors. If the value is not zero, make a backup.
202	Data Address Mark Errors	Low	This is the number of data address mark errors. This could also be a different, manufacturer-specific attribute.
203	Run Out Cancel	Low	This is the number of ECC (Error Correction Code) errors.
204	Soft ECC Correction	Low	This is the number of errors corrected by software ECC (Error Correction Code).

**Table 76** S.M.A.R.T. Attributes (continued)

ID	ATTRIBUTE NAME	BETTE R	DESCRIPTION
205	Thermal Asperity Rate (TAR)	Low	This is the number of thermal asperity errors. Thermal asperity is a read signal spike caused by sensor temperature rise due to touching the disk surface or contaminant particles.
206	Flying Height		This is the height of the hard drive's read/write heads above the disk surface.
207	Spin High Current		This is the quantity of high current used to spin up the drive.
208	Spin Buzz		This is the number of buzz routines to spin up the drive. When the arm holding the read/write heads is stuck, the motor driving it tries to oscillate the arm to free it. This causes an audible vibration.
209	Offline Seek Performance		This is the hard drive's seek performance during offline operations. Offline operations are tests the drive does itself as opposed to those that an external diagnostic tool has it do. Seek performance is how quickly the drive moves from track to track.
220	Disk Shift	Low	This is how far the disk has moved relative to the spindle (this kind of shift is usually due to shock).
221	G-Sense Error Rate	Low	This is the number of errors that have resulted from external vibration and shock.
222	Loaded Hours		This is how long the hard drive has operated under data load (this requires movement of the magnetic head armature).
223	Load/Unload Retry Count		This is how many time the magnetic head has changed position.
224	Load Friction	Low	This is resistance caused by friction in mechanical parts during operation.
225	Load/Unload Cycle Count	Low	This is the total number of load cycles.
226	Load 'In'-time		This is the total time that the magnetic heads actuator has had a load (not been in the parking area).
227	Torque Amplification Count	Low	This is the number of attempts to compensate for variations in platter speed.
228	Power-Off Retract Cycle	Low	This is how many times the magnetic armature was automatically retracted because the power was cut.
230	GMR Head Amplitude		This is the amplitude of thrashing (or the distance of repetitive forward and reverse head motion).
231	Temperature	Low	This is the hard drive's temperature.
240	Head Flying Hours		This is the total time that the head has been positioning.
250	Read Error Retry Rate	Low	This is the number of errors in reading from the disk.

# Auto Upload

## 11.1 Overview

This chapter discusses the features in the **Auto Upload** screens.

The auto upload feature uploads media files stored in the NSA to the Flickr and/or YouTube sharing websites. Besides web publishing and media server, auto upload is another convenient way to share media files with your friends and family. You can link the NSA to your Flickr and/or YouTube account and select shares for the NSA to upload. The NSA uploads the media files stored in the specified shares to your Flickr and/or YouTube account. When you add new files to the specified shares, the NSA also automatically uploads the new files to your Flickr and/or YouTube account.

## 11.2 What You Can Do

- Use the **Flickr/YouTube** screen ([Section 11.4 on page 266](#)) to upload photos and videos to your Flickr and YouTube accounts.
- Use the **FTP Uploadr** screen ([Section 11.5 on page 276](#)) to upload files to FTP servers.

## 11.3 What You Need to Know

### FTP

File Transfer Protocol (FTP) is a file transfer service that operates on the Internet. A system running the FTP server accepts commands from a system running an FTP client. FTP is not a secure protocol. Your file transfers could be subject to snooping.

## FTPES (File Transfer Protocol over Explicit TLS/SSL)

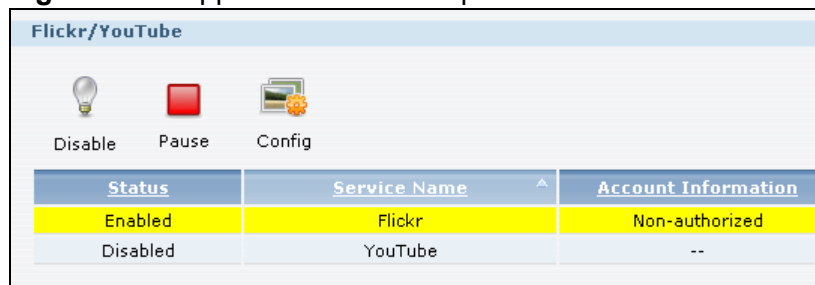
File Transfer Protocol over Explicit TLS/SSL (FTPES) is a file transfer service that uses TLS (Transport Layer Security) or Secure Socket Layer (SSL) for secure transfers across the Internet.

## 11.4 The Flickr/YouTube Screen

Use this screen to upload photos and videos to your Flickr and YouTube accounts.

Click **Applications > Auto Upload > Flickr/YouTube** to open the following screen.

**Figure 121** Applications > Auto Upload > Flickr/YouTube



The following table describes the labels in this screen.

**Table 77** Applications > Auto Upload > Flickr/YouTube

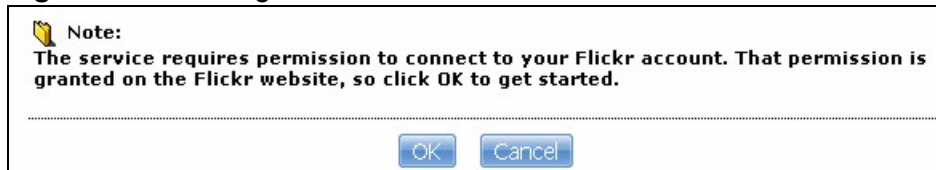
LABEL	DESCRIPTION
Flickr/YouTube	
Disable/Enable	Select a service from the list and click this to turn the service on or off.  If you disable the service and add more files to the watch folder(s), the NSA will not auto upload these files. However, the NSA still uploads any files added before you turned off the service.
Pause/Resume	Select a service from the list and click this to pause or resume the auto upload feature.
Config	Select a service from the list and click this to manage the service's settings.
Status	This field displays the service's status.  The service may be <b>Enabled</b> , <b>Disabled</b> , <b>Uploading</b> or <b>Paused</b> .
Service Name	This field displays the name of a sharing website to which the NSA can automatically upload files.
Account Information	This field displays the username and related information of the account to use with the auto upload feature.

## 11.4.1 Configuring the Flickr Settings

In the Applications > Auto Upload > Flickr/YouTube screen, select Flickr from the list and then click the Config button.

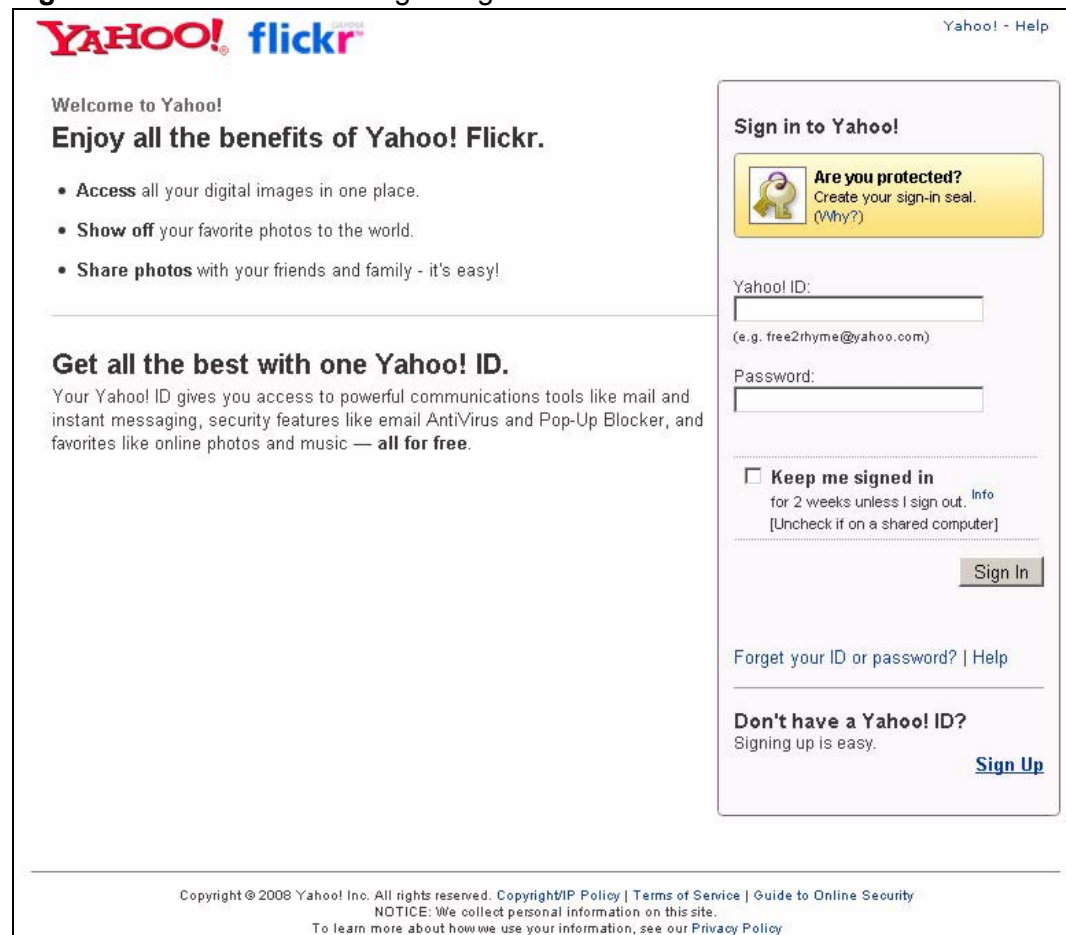
The following screen displays if you have not authorized the NSA to use a Flickr account. Click **OK** to continue the authorization process.

**Figure 122** Linking NSA to Flickr



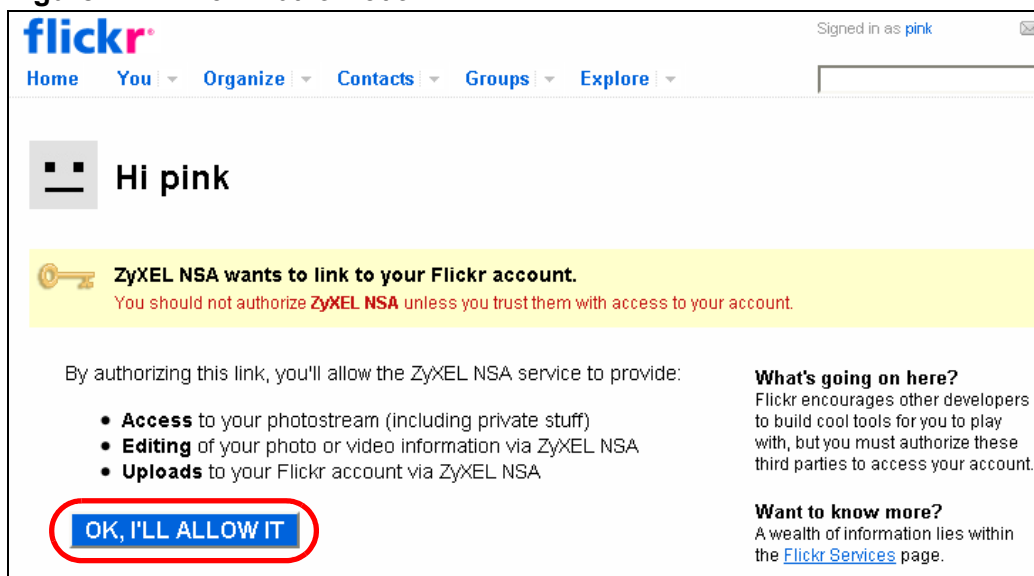
The web browser opens the Yahoo! Flickr login page. Enter your Yahoo account's information and click **Sign In**.

**Figure 123** Yahoo! Flickr Login Page



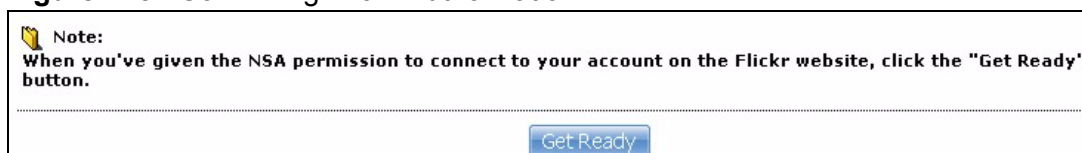
The following page displays asking for your authorization. Click **OK, I'LL ALLOW IT** to establish a link between the NSA and your Flickr account.

**Figure 124** Flickr Authorization



A confirmation page displays indicating successful authorization. Return to the NSA web configurator. Click **Get Ready** in the following screen to complete the authorization process.

**Figure 125** Confirming Flickr Authorization





Once the NSA is associated with your Flickr account, you can configure auto upload settings in the following screen.

**Figure 126** Applications > Auto Upload > Flickr/YouTube > Config (Flickr)

Applications - Auto Upload - Flickr/YouTube

### Flickr Account Configuration

Username: stopitswine

Photo Space Usage:  0% (0.00 Bytes) Used  
102.40 MB Total 100.00% Free

Video Files Usage: Uploaded: 0, Remain: 2

[Switch User](#)

### Folder Selection

#### Folder Watch List

Status	Share Name	Path	Action
	photo	/	

[Add](#)

**Note:**  
Only the following file formats will be automatically uploaded: bmp, gif, jpeg, jpg, png, tif, tiff, 3gp, 3g2, avi, mov, mpeg, mpg, wmv, mp4

### Grace Period

The time the system will wait before a newly added media file is saved in a watched folder.

Grace Period:  minutes

### Default Privacy

Who can see your media files on Flickr?

☒ Only You  
☐ Your friends  
☐ Your family  
☐ Anyone  
☒ Hide from public site area?

### Default Safety Level

☐ Safe  
☐ Moderate  
☒ Restricted

**Note:**  
Video on Flickr may only include "Safe" or "Moderate" content. "Restricted" video content is not allowed on Flickr and will be removed.



### Default Content Type

☒ Photos / Videos  
☐ Screenshots / Screencasts  
☐ Illustration / Art / Animation / CGI

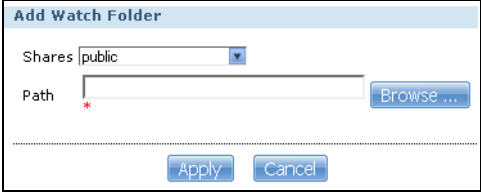
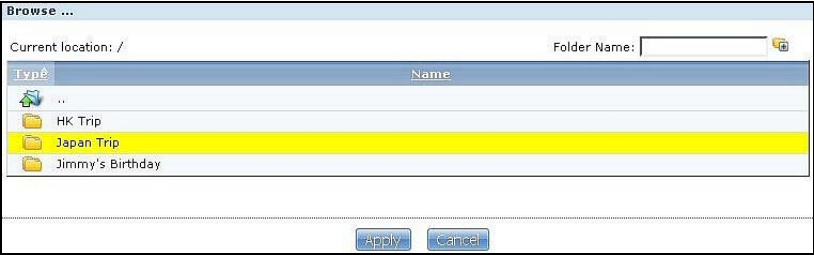

[Apply](#) [Reset](#)

The following table describes the labels in this screen.

**Table 78** Applications > Auto Upload > Flickr/YouTube > Config (Flickr)

LABEL	DESCRIPTION
Flickr Account Configuration	
Username	This field displays the Flickr account authorized for the auto upload feature.
Photo Space Usage	This shows how much storage space for photos (in size and percentage) you have used and how much space is still available on your Flickr account.
Video Files Usage	This shows how many videos you have uploaded and how many videos you can still upload to your Flickr account.
Switch User	Click this to use a different Flickr account for the auto upload feature.
Folder Selection	
Folder Watch List	This table displays a list of shares and folders selected for auto upload. Files stored in these locations are uploaded to your Flickr account.
Status	This indicates whether the folder or share is available.  represents a valid folder. The folder is available for auto upload.  represents a missing folder. The share may be deleted from the NSA, or the hard disk was removed from the NSA.
Share Name	This is the share selected for auto upload.
Path	This is the path of a folder selected for auto upload. The NSA only uploads files stored in the specified share or folder to your Flickr account.
Action	Use the <b>Remove</b> icon to remove a folder from the <b>Folder Watch List</b> .

**Table 78** Applications > Auto Upload > Flickr/YouTube > Config (Flickr) (continued)

LABEL	DESCRIPTION
Add	<p>Click this to open the following screen where you can set a folder that contains files you want the NSA to automatically upload.</p>  <ul style="list-style-type: none"> <li>• <b>Share</b> - Select the share from the list.</li> <li>• <b>Path</b> - Type the folder location in the share directly or click <b>Browse</b> to open the following screen and navigate to the file's location.</li> </ul>  <ul style="list-style-type: none"> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Folder Name</b> - Enter a new folder name and click  to create it.</li> <li>• <b>Type</b> - This is the type of the folder/file.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Select a folder. If you don't select a folder, a forward slash (/) displays in the <b>Path</b> field. All contents within the specified share are automatically selected.</p> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>
Grace Period	
Grace Period N minutes	Specify how long the NSA should wait when you add a new file for auto upload. For example, if you set the grace period to 5 minutes, the NSA uploads a new file after it has been in a watched folder for 5 minutes. You can choose from a range of 1 to 10080 minutes (up to one week).
Default Privacy	
Who can see your media files on Flickr?	<p>Determine who has the right to see files uploaded to your Flickr account.</p> <p>Select <b>Only You</b> if you do not want anyone else to see your files. You may also restrict the access to <b>Your friends</b> and/or <b>Your family</b>. You can set up a friend/family list in your Flickr account.</p> <p>Select <b>Anyone</b> to allow everyone to see your files.</p>
Hide from public site area	Check this option to prevent others from finding your files when they perform a search in the Flickr website.

**Table 78** Applications > Auto Upload > Flickr/YouTube > Config (Flickr) (continued)

LABEL	DESCRIPTION
Default Safety Level	Assign a safety level to your files.  Select <b>Safe</b> if the contents of your files are suitable for the general public.  Select <b>Moderate</b> if the contents of your files may be offensive to some people.  Select <b>Restricted</b> if the contents of your files are not suitable for certain people, such as children or your colleagues.
Default Content Type	Select a content type for your files. You can choose <b>Photo/Video</b> , <b>Screenshots/Screencasts</b> , or <b>Illustration/Art/Animation/CGI</b> .
Apply	Click this to save your changes.
Reset	Click this to restore previously saved settings.

## 11.4.2 Configuring the YouTube Settings

In the **Applications > Auto Upload > Flickr/YouTube** screen, select YouTube from the list and then click the **Config** button.

Note: Your YouTube account must be associated with a Google account.

Get a Google account and use it to log into YouTube. You can then merge the existing YouTube account to your Google account.

If you have not authorized a YouTube account on the NSA, the following screen displays. Enter your Google account's e-mail address and password in the fields and click **OK** to authorize the service.

**Figure 127** YouTube Account Settings

**YouTube Account Settings**

Email  \*

Password  \*

**Note:**  
To use this feature you must use a Google account that is linked to your YouTube account. Please create a Google account if you do not have one. Login to YouTube using your Google account and then link your existing YouTube account or create a new YouTube account.

OK Cancel

Once the NSA is associated with your YouTube account, you can configure auto upload settings in the following screen.

**Figure 128** Applications > Auto Upload > Flickr/YouTube > Config (YouTube)

Applications - Auto Upload - Flickr/YouTube

### YouTube Account Configuration

Username

### Folder Selection

#### Folder Watch List

Status	Share Name	Path	Action
	public	/C&D Top 10 Podcast	

**Note:**

- Only the following file formats will be automatically uploaded: 3gp, asf, asx, avi, dif, dl, dv, flv, gl, mov, movie, m4v, mp4, mpe, mpeg, mpg, ogv, qt, wm, wmv, wmx, wvx
- YouTube limits the file size allowed for an uploaded video. Files exceeding the file size limit may not be uploaded successfully.

### Grace Period

The time the system will wait before a newly added media file is saved in a watched folder.

Grace Period
minutes

### Video Category

Please select a category.

☒ Film & Animation
☐ Autos & Vehicles
☐ Music
☐ Pets & Animals
☐ Sports
☐ Travel & Events
☐ Comedy
☐ People & Blogs
☐ News & Politics
☐ Entertainment
☐ Education
☐ Howto & Style
☐ Nonprofits & Activism
☐ Science & Technology



### Default Privacy

Who can see your media files on YouTube?

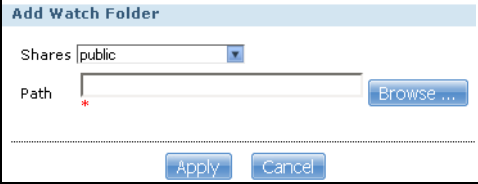


☒ Only You
☐ Anyone

The following table describes the labels in this screen.

**Table 79** Applications > Auto Upload > Config (YouTube)

LABEL	DESCRIPTION
Youtube Account Configuration	
Username	This field displays the Youtube account authorized for the auto upload feature.
Switch User	Click this to use a different YouTube account for the auto upload feature.
Folder Selection	
Folder Watch List	This table displays a list of shares and folders selected for auto upload. Files stored in these locations are uploaded to your YouTube account.
Status	<p>This field indicates whether the share or folder is available.</p> <p> represents a valid folder. The folder is available for auto upload.</p> <p> represents a missing folder. The share may be deleted from the NSA, or the hard disk was removed from the NSA.</p>
Share Name	This field displays the share selected for auto upload.
Path	This field displays the path of a folder selected for auto upload. The NSA only uploads the files stored in the specified share or folder to your YouTube account.
Action	Use the <b>Remove</b> icon to delete a folder from the <b>Folder Watch List</b> .

**Table 79** Applications > Auto Upload > Config (YouTube) (continued)

LABEL	DESCRIPTION
Add	<p>Click this to open the following screen where you can set a folder that contains files you want the NSA to automatically upload.</p>  <ul style="list-style-type: none"> <li>• <b>Share</b> - Select the share from the list.</li> <li>• <b>Path</b> - Type the folder location in the share directly or click <b>Browse</b> to open the following screen and navigate to the file's location.</li> </ul>  <ul style="list-style-type: none"> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Folder Name</b> - Enter a new folder name and click  to create it.</li> <li>• <b>Type</b> - This is the type of the folder/file.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Select a folder. If you don't select a folder, a forward slash (/) displays in the <b>Path</b> field. All contents within the specified share are automatically selected.</p> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>
Grace Period	
Grace Period N minutes	Specify how long the NSA should wait when you add a new file for auto upload. For example, if you set the grace period to 5 minutes, the NSA uploads a new file after it has been in a watched folder for 5 minutes. You can choose from a range of 1 to 10080 minutes (up to one week).
Video Category	Select the category that best describes the media files you want to upload.
Default Privacy	
Who can see your media files on YouTube?	<p>Determine who has the right to see files uploaded to your YouTube account.</p> <p>Select <b>Only You</b> if you do not want anyone else to see your files.</p> <p>Select <b>Anyone</b> to allow everyone to see your files.</p>
Apply	Click this to save your changes.
Reset	Click this to restore your previously stored settings.

## 11.5 The FTP Uploadr Screen

The FTP Uploadr feature uploads files stored in the NSA to FTP servers. Besides web publishing and media server, auto upload is another convenient way to share media files with your friends and family. You can link the NSA to the FTP server or the FTP server on another NSA and select shares or folders for the NSA to upload. The NSA uploads the files stored in the specified shares to the FTP server. When you add new files to the specified shares, the NSA also automatically uploads the new files to the FTP server.

Use this screen to configure the FTP Uploadr.

Click **Applications > Auto Upload > FTP Uploadr** to open the screen shown next.

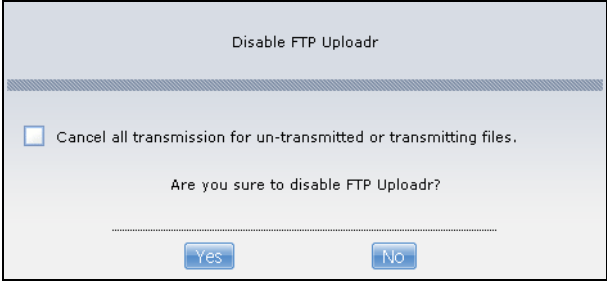

**Figure 129** Applications > Auto Upload > FTP Uploadr

Domain Name/IP Address	Port Number	Remote Path	Account Name	Description
ftp.example.com	21	/music	user	testing



The following table describes the labels in this screen.

**Table 80** Applications > Auto Upload > FTP Uploadr

LABEL	DESCRIPTION
Enable FTP Uploadr	<p>Use the check box to enable or disable the FTP Uploadr. Click <b>Apply</b> to save your changes.</p> <p>When you disable the FTP Uploadr, a screen opens requesting confirmation. Select the check box to stop any current or queued uploads. If you do not select the check box, the FTP Uploadr will finish uploading the files that are already in the queue list. Clicking <b>Yes</b> will disable the FTP Uploadr.</p> 
Add Server	Click this to add a target FTP server entry. See <a href="#">Section 11.5.1 on page 278</a> for more details.
Preferences	Click this to manage the settings of the FTP Uploadr.
Edit Server	Select a server from the list and click this to edit the FTP server entry.
Delete Selected Server(s)	<p>Select a server from the list and click this to remove the FTP server entry.</p> 
Server Information	Select a server from the list and click this to display the status and settings about the FTP server.
Domain Name/IP Address	This is the domain name or IP address of the FTP server.
Port Number	This is the port number used by the FTP server.
Remote Path	The NSA automatically uploads files to this location of the FTP server.
Account Name	This is the login account for the FTP server.
Description	This is the information related to the FTP server.

## 11.5.1 Adding or Editing an FTP Server Entry

Use this screen to add or edit an FTP server entry for auto upload.

In the **FTP Uploadr** screen, click the **Add Server** or **Edit Server** button to open the following screen.

**Figure 130** Applications > Auto Upload > FTP Uploadr > Add or Edit a Server

The following table describes the labels in this screen.

**Table 81** Applications > Auto Upload > FTP Uploadr > Add or Edit a Server

LABEL	DESCRIPTION
Domain Name/IP Address	Enter the domain name or IP address of the FTP server.
Account Name	Enter the account name used to access the FTP server.
Password	Enter the password associated with the account name.
Port Number	Enter the port number for the FTP server.
Remote Path	Enter the path to where the NSA automatically uploads files.
Description	Enter additional information about this FTP server.
Test Connection	Click this to test your settings and check whether you can use the settings to connect to the FTP server.
Apply	Click this to save your changes.
Cancel	Click this return to the previous screen without saving.

## 11.5.2 The FTP Uploadr Preferences Screen

Use this screen to configure the general settings for the FTP Uploadr.

In the **FTP Uploadr** screen, click the **Preferences** icon to open the following screen.

**Figure 131** Applications > Auto Upload > FTP Uploadr > Preferences

**Folder Watch List**

Status	Share Name	Path	Action
There are currently no folders on the watch list.			

[Add](#)

**Settings**

**Grace Period**  
The time the system will wait before a newly added file is saved in a watched folder.  
Grace Period  minutes

**Bandwidth Limit**  
Max. upload rate  KB/s (0=No Limit)

[Apply](#)

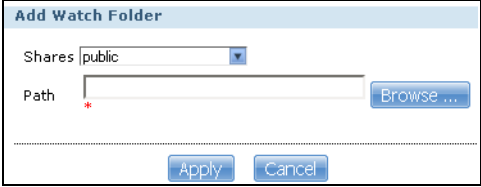


[Reset](#) [Close](#)

The following table describes the labels in this screen.

**Table 82** Applications > Auto Upload > FTP Uploadr > Preferences

LABEL	DESCRIPTION
Folder Watch List	
Status	This field indicates whether the share or folder is available. represents a valid folder. The folder is available for auto upload. represents a missing folder. The share may be deleted from the NSA, or the hard disk was removed from the NSA.
Share Name	This is the share selected for auto upload.
Path	This is the path of a folder selected for auto upload. The NSA only uploads files stored in the specified share or folder to your FTP server.
Action	Use the <b>Remove</b> icon to delete a folder from the <b>Folder Watch List</b> .

**Table 82** Applications > Auto Upload > FTP Uploadr > Preferences (continued)

LABEL	DESCRIPTION
Add	<p>Click this to open the following screen where you can set a folder that contains files you want the NSA to automatically upload.</p>  <ul style="list-style-type: none"> <li>• <b>Share</b> - Select the share from the list.</li> <li>• <b>Path</b> - Type the folder location in the share directly or click <b>Browse</b> to open the following screen and navigate to the file's location.</li> </ul>  <ul style="list-style-type: none"> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Folder Name</b> - Enter a new folder name and click  to create it.</li> <li>• <b>Type</b> - This is the type of the folder/file.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Select a folder. If you don't select a folder, a forward slash (/) displays in the <b>Path</b> field. All contents within the specified share are automatically selected.</p> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>
Settings	
Grace Period	Specify how long the NSA should wait when you add a new file for auto upload. For example, if you set the grace period to 5 minutes, the NSA uploads a new file after it has been in a watched folder for 5 minutes. You can choose from a range of 1 to 10080 minutes (up to one week).
Bandwidth Limit	<p>Enter the maximum upload rate for auto upload. You can choose from a range of 0 to 100,000 KB/s. Enter 0 if you do not want to set any limit.</p> <p>Use this to leave bandwidth on your network connection for other traffic, especially if your Internet connection has restricted upload speed.</p>
Apply	Click this to save your changes in this section.
Reset	Click this to restore previously saved settings.
Close	Click this to return to the previous screen without saving.

---

# PART III

## Sharing

---

[Users \(283\)](#)

[Groups \(289\)](#)

[Shares \(293\)](#)



## 12.1 Overview

This chapter introduces the **Users** screens of the NSA. Use the **Users** screens to create and manage administrator and user accounts.

Administrators can:

- Configure and manage the NSA.
- Create volumes, shares, and user accounts.
- Assign individual users specific access rights for specific shares.

Users are people who have access rights to the NSA and can store files there for later retrieval. A user can:

- Manage shares that he owns.
- Change his own password.
- Access the contents of other shares to which he is given access rights.

## 12.2 What You Can Do

- Use the main **Users** screen ([Section 12.3 on page 284](#)) to display a list of user accounts created on the NSA.
- Use the **Add User** screen ([Section 12.3.2 on page 286](#)) to create new user accounts.
- Use the **Edit User** screen ([Section 12.3.2 on page 286](#)) to edit the properties of an existing account.
- Use the **User Info** screen ([Section 12.4 on page 288](#)) to display the amount of volume space used by a selected account and the account's membership in any groups.

## 12.3 The Users Screen

Click **Sharing > Users** to display the screen shown next.

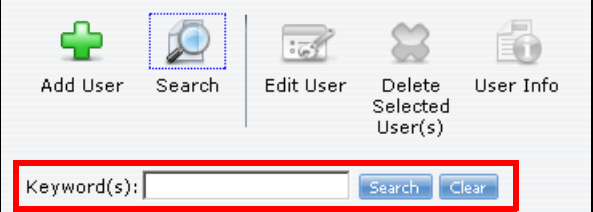
Use this screen to create and manage accounts for users who can store files on the NSA.

**Figure 132** Sharing > Users



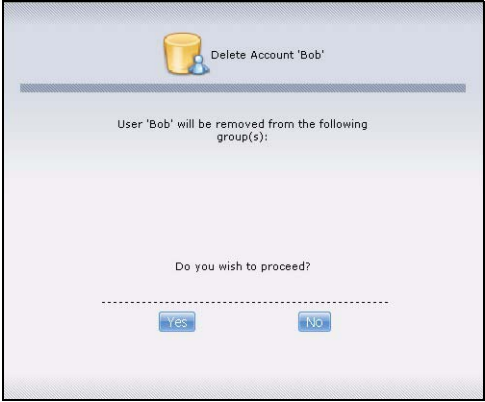
The following table describes the labels in this screen.

**Table 83** Sharing > Users

LABEL	DESCRIPTION
Add User	Click this to open a screen where you can configure a new user account.  Refer to <a href="#">Section 12.3.2 on page 286</a> to see the screen.
Search	Click this to display a search field. Type in the name of an account and then click <b>Search</b> to look up the account you specified. Click <b>Clear</b> to close the search function.  
Edit User	Select an account and click this to open a screen where you can edit the properties of the account.  Refer to <a href="#">Section 12.3.2 on page 286</a> to see the screen.





**Table 83** Sharing > Users (continued)

LABEL	DESCRIPTION
Delete Selected Users	<p>Select an account and click this to open a screen where you can delete the user account.</p> 
User Info	<p>Select an account and click this to open a screen displaying the amount of storage space used by the account. You can also check the account's membership in any groups.</p> <p>Refer to <a href="#">Section 12.4 on page 288</a> to see the screen.</p>
Display Number	Click the drop-down menu to set how many accounts you want to display in one screen.
Go to Page	Click the drop-down menu to display and access more user accounts.
User Type	This field displays whether the account is an administrator account or a user account.
Username	This field displays the username of each account.

### 12.3.1 User Icons

The following table describes the user icons.

**Table 84** User Icons

ICON	DESCRIPTION
	The blue icon is for an administrator account.
	The green icon is for a user account.

## 12.3.2 Adding or Editing an Account

Use this screen to create or edit a NSA user account with NSA access password.

Click the **Add User** button in the **Users** screen to open the following screen. Click the **Edit User** button in the screen shown previously to edit an existing account.

**Figure 133** Sharing > Users > Add or Edit a User

The following table describes the labels in this screen.

**Table 85** Users > Add or Edit a User

LABEL	DESCRIPTION
Username	Type a name from 1 to 32 single-byte (no Chinese characters allowed for example) ASCII characters. See <a href="#">Section 12.3.3 on page 287</a> for more details on usernames.
New Password	Create a password associated with this user. You can type from one to 14 single-byte (no Chinese characters allowed for example) ASCII characters.
Password (Confirm)	You must type the exact same password that you just typed in the above field.
Quota (per volume)	Select the volume in which you want the user's files to be stored.  Enter how much space (in megabytes) you want to allow for the user to store files.
Account Type	Select <b>Administrator</b> to give the account full configuration and management access to the NSA.  Select <b>User</b> to give the account basic access rights to the NSA and allow the user to manage his own shares, change his own password, and access the contents of other shares to which he is given access rights.
Group Membership	

**Table 85** Users > Add or Edit a User (continued)

LABEL	DESCRIPTION
Available Group(s)	This field lists the groups created on the NSA to which the selected account does not belong.
Group Membership	This field lists the groups that the selected account belongs to.
Add Selected Group(s)	Select a group from the <b>Available Groups</b> list and click this to add the account to that group.
Remove Selected Group(s)	Select a group from the <b>Group Membership</b> list and click this to remove the account from that group.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

### 12.3.3 Usernames

Enter a username from one to 32 characters. The first character must be alphabetical (case insensitive, [A-Z a-z]); numeric characters are not allowed as the first character.

The username can only contain the following characters:

- Alphanumeric A-z 0-9. Unicode usernames are supported with CIFS logins, but not FTP or web configurator logins.
- Spaces
- \_ [underscores]
- . [periods]
- - [dashes]

Other limitations on usernames are:

- All leading and trailing spaces are removed automatically.
- Multiple spaces within names are converted to a single space.
- Usernames are case insensitive. The username cannot be the same (no matter the letter case) as an existing user. For example, if a user exists with the name 'BOB', you cannot create a user named 'bob'. If you enter a user 'bob' but use 'BOB' when connecting via CIFS or FTP, it will use the account settings used for 'bob'.
- The username cannot be the same as a system username such as **ANONYMOUS-FTP** nor be the same as an existing user. Other reserved usernames that are not allowed are:
  - bin
  - daemon
  - ftp
  - anonymous-ftp

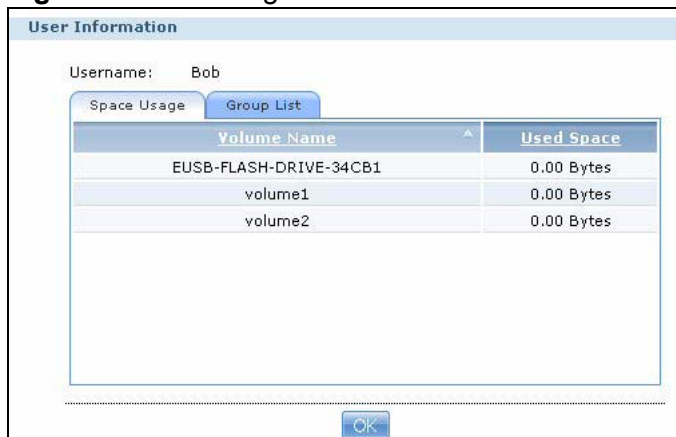
- anonymous
- nobody
- root
- pc-guest
- admin
- password

## 12.4 Displaying User Info

Use this screen to display a user's information.

In the **Users** screen, select an account and click **User Info** to open the following screen.

**Figure 134** Sharing > Users > User Info



The following table describes the labels in this screen.

**Table 86** Sharing > Users > User Info

LABEL	DESCRIPTION
Username	This field displays the selected username.
Space Usage	Click this to display the amount of volume space used by the selected account.
Group List	Click this to display the selected user's group membership.
Volume Name	This field displays the volume(s) created on the NSA.
Used Space	This field displays how much storage space the selected account is currently using. This only applies for files that the user saved onto the NSA while logged in with that username.
Group Name	This shows when you click the <b>Group List</b> tab. This displays the list of groups to which the selected user belongs.
OK	Click this to close the current screen.

# Groups

## 13.1 Overview

This chapter introduces the **Groups** screens. Use the **Groups** screens to create and manage groups. You can assign users to groups and grant individual groups access rights to specific shares.

## 13.2 What You Can Do

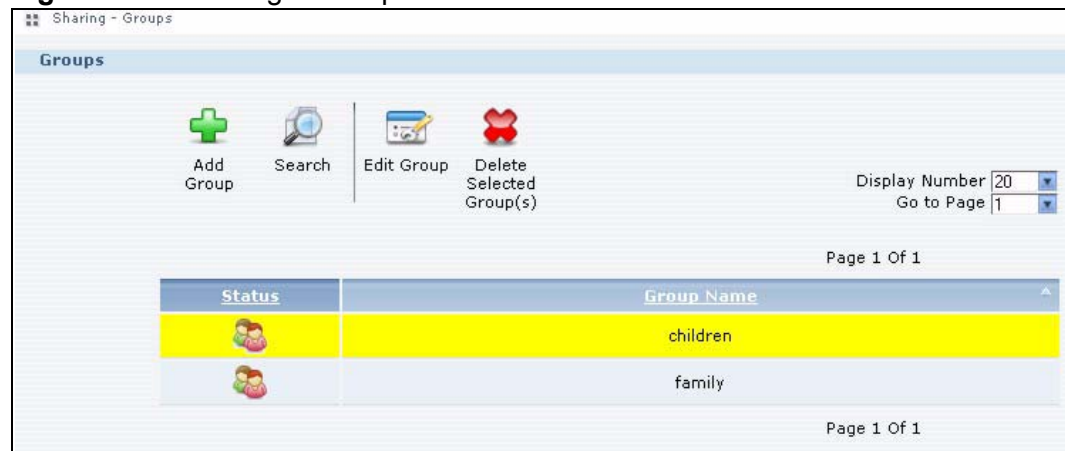
- Use the main **Groups** screen ([Section 13.3 on page 289](#)) to display and manage a list of groups created on the NSA.
- Use the **Add Group** screen ([Section 13.3.1 on page 291](#)) to create new groups.
- Use the **Edit Group** screen ([Section 13.3.1 on page 291](#)) to edit the properties of an existing group.

## 13.3 The Groups Screen

Use this screen to create and manage groups.

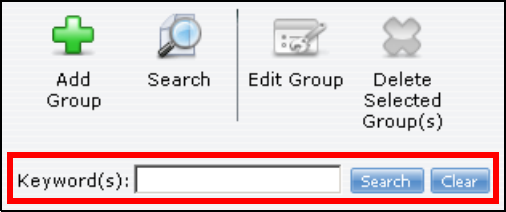
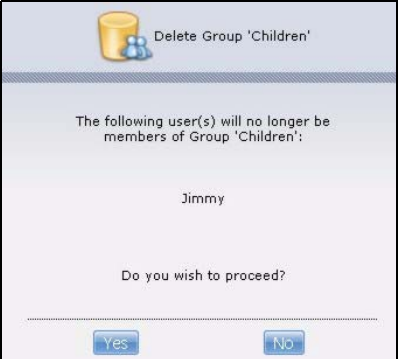
Click **Sharing > Groups** to display the screen shown next.

**Figure 135** Sharing > Groups




The following table describes the labels in this screen.

**Table 87** Sharing > Groups

LABEL	DESCRIPTION
Add Group	Click this to open a screen where you can configure a new group.
Search	Click this to display a search field. Type the name of a group and then click <b>Search</b> to look up the group you specified. Click <b>Clear</b> to close the search function. 
Edit Group	Select a group and click this to open a screen where you can edit the properties of the selected group.
Delete Selected Group(s)	Select a group and click this to open a screen where you can delete the group. 

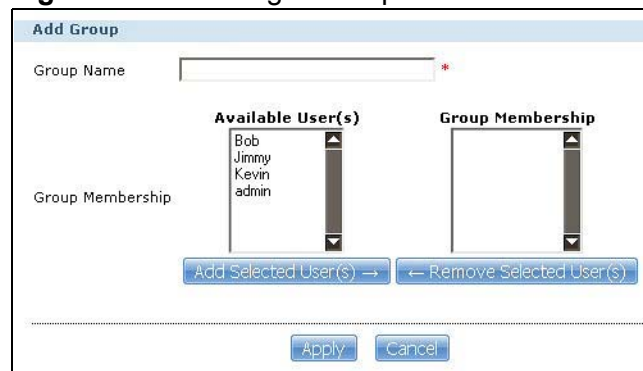
**Table 87** Sharing > Groups (continued)

LABEL	DESCRIPTION
Display Number	Click the drop-down menu to set how many groups you want to display in one screen.
Go to Page	Click the drop-down menu to select a page number. Jump to a different page to display and access more groups.
Status	 This field displays the group icon.
Group Name	This field displays the group names created on the NSA.

## 13.3.1 Adding or Editing a Group

Use this screen to create or edit a NSA group.

Click the **Add Group** button in the **Groups** screen to open the following screen. Click the **Edit Group** button in the screen shown previously to edit an existing group.

**Figure 136** Sharing > Groups > Add or Edit a Group


The following table describes the labels in this screen.

**Table 88** Sharing > Groups > Add or Edit a Group

LABEL	DESCRIPTION
Group Name	Type a name from 1 to 32 single-byte (no Chinese characters allowed for example) ASCII characters. See <a href="#">Section 13.3.2 on page 292</a> for more details on group names.
Group Membership	Use this field to assign group membership to individual users.
Available User(s)	This field lists the user accounts created on the NSA that are not members of the current group.
Group Membership	This field lists the user accounts added to the group.
Add Selected User(s)	Select a user account from the <b>Available Users</b> list and click this to add the account to the group.
Remove Selected User(s)	Select a user account from the <b>Group Membership</b> list and click this to remove the account from the group.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

## 13.3.2 Group Names

Enter a group name from 1 to 32 characters. The first character must be alphabetical (case insensitive, [A-Z a-z]); numeric characters are not allowed as the first character.

The group name can only contain the following characters:

- Alphanumeric A-z 0-9. Unicode usernames are supported with CIFS logins, but not FTP or web configurator logins.
- Spaces
- \_ [underscores]
- . [periods]
- - [dashes]

Other limitations on group names are:

- All leading and trailing spaces are removed automatically.
- Multiple spaces within names are converted to a single space.
- Group names are case insensitive. The group name cannot be the same (no matter the letter case) as an existing group. For example, if a group exists with the name 'FAMILY', you cannot create a group named 'family'.
- The group name cannot be the same as a system group name such as **EVERYONE** nor be the same as an existing group. Other reserved groups names that are not allowed are:
  - nobody
  - root
  - everyone



# Shares

## 14.1 Overview

A share is a set of access permissions mapped to a specific folder on a volume. It is equivalent to the Windows concept of a shared folder. You can map a share to a network drive for easy and familiar file transfer for Windows users.

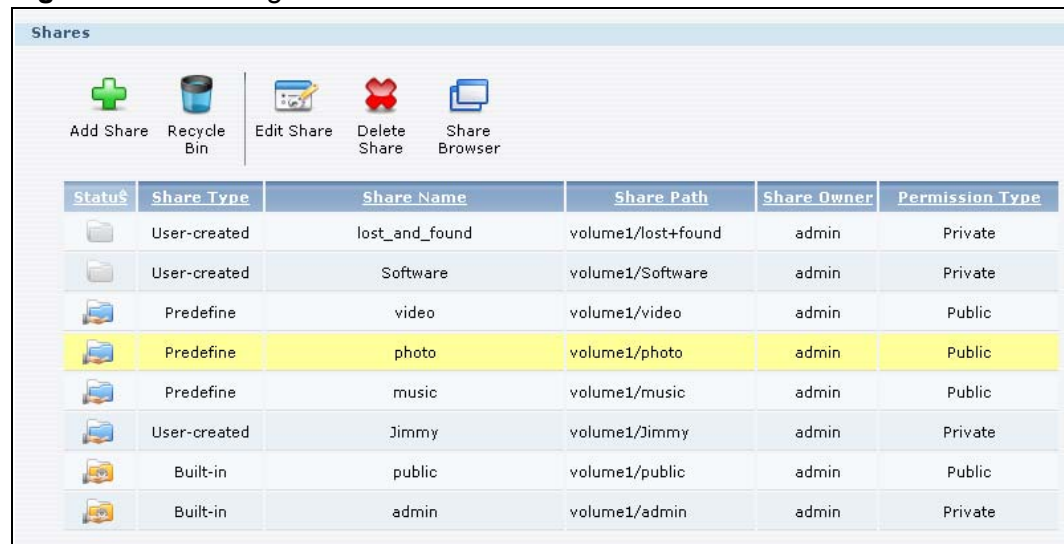
## 14.2 What You Can Do

- Use the **Shares** screen ([Section 14.3 on page 294](#)) to navigate a list of shares created on the NSA.
- Use the **Add Shares** screen ([Section 14.3.1 on page 296](#)) to create additional shares on the NSA.
- Use the **Recycle Bin** screen ([Section 14.4 on page 299](#)) to configure and clean up the recycle bins.
- Use the **Edit Share** screen ([Section 14.3.1 on page 296](#)) to edit a share's properties.
- Use the **Share Browser** screen ([Section 14.5 on page 300](#)) to navigate, add and edit the contents in a share.

## 14.3 The Shares Screen

Click **Sharing > Shares** in the navigation panel to open the following screen. This screen lists all shares created on the NSA.

**Figure 137** Sharing > Shares








The following table describes the labels in this screen.

**Table 89** Sharing > Shares

LABEL	DESCRIPTION
Add Share	Click this to create a new share.
Recycle Bin	Click this to configure recycle bins.
Edit Share	Select a share and click this to edit the share.
Delete Share	<p>Select a share and click this to remove or restrict access to the share.</p>
Share Browser	Select a share and click this to browse the share's contents.

**Table 89** Sharing > Shares (continued)

LABEL	DESCRIPTION
Status	<p>This field displays the share icons.</p> <p> represents a <b>Built-in</b> share on a volume on the internal hard drives.</p> <p> represents a <b>Predefined</b> or <b>User-Created</b> share on a volume on the internal hard drives.</p> <p> represents an <b>Auto</b> or <b>User-Created</b> share on a volume on the external (USB) devices.</p> <p> represents a disabled share that no user can access.</p> <p> represents a missing share. The NSA cannot find the hard disk associated with the share (the disk may be removed from the NSA for example). You may install the disk back to the NSA to recover the share, or you may delete the share from the NSA.</p>
Share Type	<p>This field displays <b>Built-in</b> for system shares. You cannot delete these shares (these are the public and admin shares).</p> <p>This field displays <b>Predefined</b> for default shares. You can delete these shares (these are the video, music, and photo shares).</p> <p>This field displays <b>User-created</b> for shares that an administrator has created. You can delete these shares.</p> <p>This field displays <b>Auto</b> for shares that are automatically created on an external (USB) device when a user plugs in the device.</p>
Share Name	This field displays the share's names.
Share Path	This field displays the share's file path, for example, volume1/music.
Share Owner	This is the name of the user account to which this share belongs.
Permission Type	<p>This field displays the access permission of a share.</p> <p>Everyone on the network can access a <b>Public</b> share.</p> <p>Only the share owner can access a <b>Private</b> share.</p> <p>An <b>Advanced</b> share allows you to assign specific access rights (read-only for example) to individual users/groups.</p>

## 14.3.1 Adding or Editing Share

Click **Add Share** to create a new share. In the **Shares** screen, select a share and click **Edit Share** to open the following screen. Use this screen to create or edit a share.

**Figure 138** Shares > Add Share (or Edit Share)

The following table describes the labels in this screen.

**Table 90** Shares > Add Share (or Edit Share)

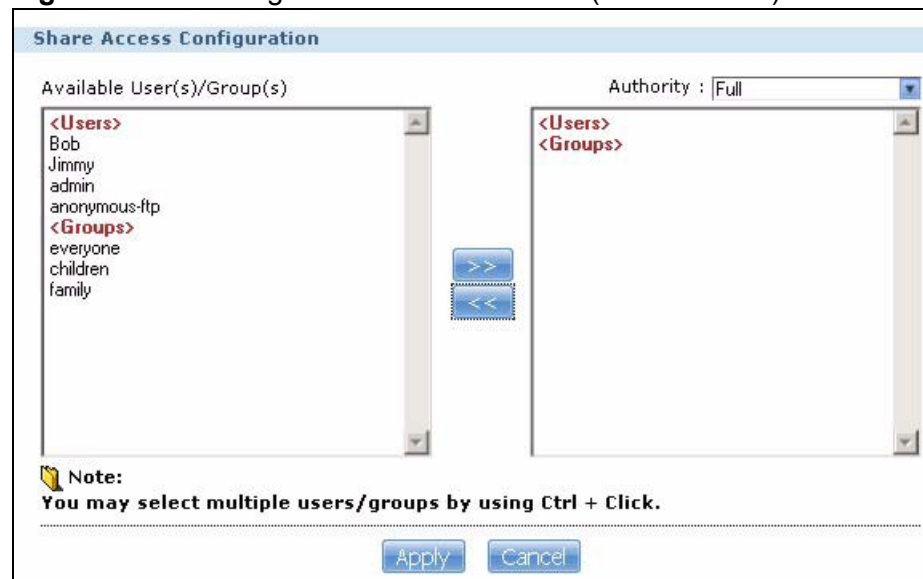
LABEL	DESCRIPTION
Share Name	Type a share name from 1 to 239 single-byte (no Chinese characters allowed for example) ASCII characters. The name cannot be the same as another existing share. See <a href="#">Section 3.5.5 on page 50</a> for more information on share names.
Volume	You should have already created volumes (a single accessible storage area with a single file system) on the NSA. Select the one that contains the folder that you want to share out.  You cannot modify this when editing a share.
Make this share owned by	Select the administrator or user account that can own (manage) this share. The share owner controls access rights to the share.
Enable this share	Click this to allow access to this share.
Enable Recycle Bin	Click this to activate the recycle bin. When you delete a file from this share, a recycle folder is created to store the deleted item.
Publish this share to Media Server	This shows only when you enable the <b>Media Server</b> ( <a href="#">Section 9.5 on page 170</a> ).  Select this option to have the NSA share files in this folder with media clients. The media clients do not have to use a password to play the shares you publish.
Publish this share to Web	This shows only when you enable the <b>Web Publish</b> ( <a href="#">Section 9.7 on page 184</a> ).  Select this option to let people use a web browser to access this share's files without logging into the My NSA screens.

**Table 90** Shares > Add Share (or Edit Share) (continued)

LABEL	DESCRIPTION
Share Access	<p>Assign access rights (full, read only or deny) to users or groups. If you publish the share to the media server or the web, all users will have at least read-only access to the share, regardless of what you configure here.</p> <p><b>Keep it private to owner</b> means only the share owner (selected above) can access the share.</p> <p><b>Make it Public</b> means every user (including people who do not have accounts on the NSA) can access the share.</p> <p><b>Advanced</b> allows you to assign specific access rights (full, read only or deny) to individual users/groups.</p>
Edit	This button is available only when you select <b>Advanced</b> share access. Click this to configure advanced share access rights.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.



## 14.3.2 Configuring Advanced Share Access

In the **Sharing > Shares > Add Share** or **Edit Share** screen, select **Advanced** from the **Share Access** drop-down list. Click **Edit** to open the following screen. Use this screen to configure share access rights for individual users and groups.

**Figure 139** Sharing > Shares > Add Share (or Edit Share) > Advanced

The following table describes the labels in this screen.

**Table 91** Sharing > Shares > Add Share (or Edit Share) > Advanced

LABEL	DESCRIPTION
Available Users/ Groups	This field lists the users/groups to which you can assign access rights.
Authority	<p>Use this field to assign access rights to users/groups.</p> <p><b>Full Control</b> gives users/groups full access (read, write and execute) to all files contained within this share.</p> <p><b>Read-Only</b> gives users/groups read-only access (they cannot modify nor execute) to all files contained within this share.</p> <p><b>Deny</b> blocks access (users/groups cannot read, modify, nor execute) to all files contained within this share.</p> <p>Among all access rights, <b>Deny</b> has the highest priority. For example, User A belongs to Group 1. You assign User A full access rights to the Music share but deny access rights to Group 1. Then User A cannot access the Music share.</p> <p>Note: If you deny access to all users, no-one can use the share, not even the administrator.</p>
 	Click an arrow button to move users/groups between the left and right fields. Use the arrow buttons to assign access rights to users/groups.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

### 14.3.3 Public and ANONYMOUS Share Access Rights

If you make a share public, users do not need to log in.

With **ANONYMOUS FTP**, you must enter either 'anonymous' or 'ftp' as the username. Any other name is considered a username, so must be valid and have a corresponding correct password.

## 14.4 The Recycle Bin Configuration Screen

Use this screen to periodically clean up items in all recycle bins.

### 14.4.1 Recycle Bins

Recycle bins in the NSA help users recover accidentally deleted files or folders in the shares. When you delete an item, a recycle folder is created within the share to hold the deleted item.

Every share can have its own recycle folder. You must enable the recycle-bin function to recycle deleted items. You can configure this setting when you add or edit a share. See [Section 14.3.1 on page 296](#) for details on activating the recycle bin in a share.

Later if you want to retrieve a deleted item, you can locate the item in the recycle folder. You may move or copy the deleted item to another share.

### 14.4.2 Configuring Recycle Bins

In the **Sharing > Shares** screen, click **Recycle Bin** to open the following screen.

**Figure 140** Sharing > Shares > Recycle Bin



The screenshot shows a 'Share Configuration' window. It has a title bar 'Share Configuration'. Below it, there is a text field 'Clean Recycle Bin every' followed by a numeric input field containing '0', and then 'days (0~31, 0 means not clean it automatically.)'. To the right of this is a button labeled 'Clean all recycle bins now'. At the bottom of the window are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

**Table 92** Sharing > Shares > Recycle Bin

LABEL	DESCRIPTION
Clean Recycle Bin every N days	Specify how often you want to clear the contents in all recycle bins. The specified days correspond to how long a file has been stored in a recycle bin. For example, if you set the interval to be 3 days, recycle bins will clean up items deleted or not accessed for 3 days.  Note: Cleaning up recycle bins permanently removes the files from the NSA.
Clean all recycle bins now	Click this to immediately remove contents from all recycle bins.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

## 14.5 The Share Browser Screen

Use this screen to create folders, upload files, and edit files within the share.

**Figure 141** Sharing > Shares > Share Browser



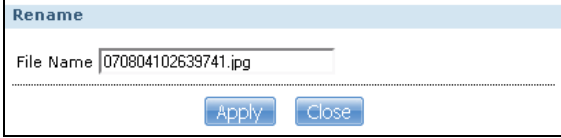

The following table describes the labels in this screen.

**Table 93** Sharing > Shares > Share Browser

LABEL	DESCRIPTION
Create Folder	Type a folder name and click <b>Apply</b> to make a new folder. The name can be 1 to 239 single-byte (no Chinese characters allowed for example) ASCII characters. The name cannot be the same as another existing folder in the same path. See <a href="#">Section 3.5.5 on page 50</a> for more information on folder names.
Upload	Click this to add files to the share. Use <b>Browse</b> to locate a file and click <b>Apply</b> to upload the file. Note that the size of each file should be less than 2 GB. <div data-bbox="540 1394 1125 1749"> <p>The 'Upload Files' dialog box contains five rows, each with a label 'File 1' through 'File 5', a text input field, and a 'Browse...' button. At the bottom, there is a note: 'Note: The size of uploaded files can't be more than 2G.' and two buttons: 'Apply' and 'Cancel'.</p> </div>



**Table 93** Sharing > Shares > Share Browser (continued)

LABEL	DESCRIPTION
Rename	<p>Select a folder or file and click this to open a screen. Enter the name you want and click OK to make the changes.</p> <p><b>Note:</b> When you change a file name, make sure you keep the file extension.</p> 
Delete	<p>Select a file/folder from the list and click this to open a warning screen. Click <b>Yes</b> to delete the file/folder, or click <b>No</b> to close the screen.</p> 
Move	Select a file/folder from the list and click this to relocate the file/folder to another share.
Copy	Select a file/folder from the list and click this to make a duplicate of the file/folder to another share.
Current location	This is the name of the share and folder path that you are in.
Type	<p>The icon in this column identifies the entry as a folder or a file.</p> <p>The folder with an arrow pointing up is for the link that takes you to the next higher layer in the share's folder tree.</p>
Name	This section lists the share's existing folders or files. Click to the right of the file/folder name to select the file/folder. You can also click the folder's name to navigate to a sub-folder within the folder.
Size	This field displays size of the file.
Modified Date	This field displays a file's latest modification date.
Close	Click this to close the screen.

## 14.5.1 Moving or Copying Files

Use this screen to move or copy files to another share.

In the **Share Browser** screen, select a file or folder and click **Move** or **Copy** to open the following screen.

**Figure 142** Sharing > Shares > Share Browser > Move (or Copy)

The following table describes the labels in this screen.

**Table 94** Sharing > Shares > Share Browser > Move (or Copy)

LABEL	DESCRIPTION
Shares	Select the destination share from the drop-down list.
Path	This field displays the share folder's path. You can use <b>Browse</b> to find or create a folder on the NSA or type the location of the folder using forward slashes as branch separators.
Browse	<p>Click this to open the following screen and navigate to the location of the file/folder.</p> <ul style="list-style-type: none"> <li>• <b>Current Location</b> - This is the location of the selected folder.</li> <li>• <b>Folder Name</b> - Enter a new folder name and click  to create it.</li> <li>• <b>Type</b> - This identifies the item as a folder or file.</li> <li>• <b>Name</b> - This is the name of the folder/file.</li> </ul> <p>Select a folder. If you don't select a folder, a forward slash (/) displays in the <b>Path</b> field. All contents within the specified share are automatically selected.</p> <p>Click <b>Apply</b> to save your settings and <b>Cancel</b> to close the screen.</p>
Yes	Click this to move or copy the file/folder to the designated share.
Close	Click this to return to the <b>Share Browser</b> screen.

---

# **PART IV**

## **Maintenance and Protecting Data**

---

Maintenance Screens (305)

Protecting Your Data (329)



# Maintenance Screens

## 15.1 Overview

This chapter discusses the **Maintenance** screens. The **Maintenance** screens allow you to manage system configurations.

## 15.2 What You Can Do

- Use the **Power Management** screen ([Section 15.3 on page 306](#)) to configure power settings for the NSA, including power saving, UPS, power on/off during power failure and power on/off schedule.
- Use the **Log** screen ([Section 15.4 on page 310](#)) to check the system's logs.
- Use the **Configuration** screen ([Section 15.5 on page 314](#)) to backup or restore the NSA configuration file.
- Use the **SSL** screen ([Section 15.6 on page 315](#)) to configure HTTPS and the NSA's SSL certificate.
- Use the **Firmware Upgrade** screen ([Section 15.7 on page 318](#)) to upload new firmware.
- Use the **Shutdown** screen ([Section 15.8 on page 319](#)) to restart or shut down your NSA.

## 15.3 The Power Management Screen

Use this screen to manage power settings for the NSA, including power saving, UPS, power on/off during power failure and power on/off schedule.

Click **Maintenance > Power Management** to display the following screen.

**Figure 143** Maintenance > Power Management

Maintenance - Power Management

**Power Management**

Turn off hard disk(s)  minutes

**Minimum UPS Capacity**

Minimum UPS Capacity  %

**Note: This feature will not work now because there is no UPS control cable connected.**

**Note: The NSA automatically shuts down if the UPS's remaining charge gets down to this level.**

**Power On After Power Failure**

☒ **Keep Former Status**  
If the system was on when the power failed, it restarts automatically when the power is restored. If it was off, it stays off.

☐ **Always Power On**  
The system restarts automatically when the power is restored.

☐ **Always Power Off**  
The system will not restart after power failure. You must press the power button manually to restart it.

**Power On/Off Schedule**

☐ **Enable Power Control Schedule**

The following table describes the labels in this screen.

**Table 95** Maintenance > Power Management

LABEL	DESCRIPTION
Power Management	
Turn off hard disk(s)	Enter the number of minutes the NSA will sit idle before spinning the hard disks down to sleep. The default power-off time is 3 minutes.
Apply	Click this to save your changes in this section.
Reset	Click this to restore your previously saved settings.
Minimum UPS Capacity	

**Table 95** Maintenance > Power Management (continued)

LABEL	DESCRIPTION
Minimum UPS Capacity	<p>When you use an APC Uninterruptible Power Supply (UPS) with a USB connection to the NSA, the NSA shuts itself down if the APC UPS's battery charge gets down to the percentage you specify in this field. This allows the NSA to shut down properly and avoid data loss caused by a power failure when the UPS stops supplying power.</p> <p>A setting around 50% is recommended. A setting close to 100% is not recommended since it would cause the NSA to shut down whenever the UPS is charging. A setting close to 0 is also not recommended since the UPS would not have enough power to allow the NSA to shutdown properly.</p>
Apply	Click this to save your changes in this section.
Power On After Power Failure	Select an option to set whether or not the NSA restarts when the power is restored after a power failure.
Keep Former Status	Select this option to have the NSA automatically restart only if it was operating when the power failed. The NSA remains off if it was already off when the power failed.
Always Power On	Select this option to keep the NSA operating as much of the time as possible. The NSA restarts automatically even if it was turned off when the power failed.
Always Power Off	Select this option to keep the NSA from automatically restarting when the power is restored after a power failure. This is a computer's "traditional" behavior. Select this if you have other servers such as a domain controller or DNS server that you want to start or check after a power failure before the NSA turns on.
Apply	Click this to save your changes in this section.
Power On/Off Schedule	
Enable Power Control Schedule	<p>Select this option to have the NSA turn itself off and on or reboot according to the schedules you configured.</p> <p>Click <b>Edit</b> to go to the screen where you can configure the power control schedules.</p> <p>Refer to <a href="#">Section 15.3.1 on page 308</a> for this screen.</p>
Apply	Click this to save your changes in this section.

## 15.3.1 Editing the Power Control Schedule Screen

Click **Maintenance > Power Management > Edit** to open this screen. Use this screen to configure power control schedules to have the NSA turn on, turn off, or reboot at specified times.

**Figure 144** Maintenance > Power Management > Edit

The screenshot shows the 'Power Control Schedule List' screen. At the top is a table with the following data:

Type	Frequency	Execute Time	Actions
Power On	Monthly : FirstMonday	00:00	
Power Off	Monthly : FourthFriday	00:00	

Below the table is a 'Note' section with a yellow icon and the text: 'You must click on the apply button for your power control schedule settings to apply.'

Below the note is the 'Add Power Control Schedule' section. It contains the following fields:

- Type: Power On (dropdown)
- Frequency: Monthly (dropdown)
- Execute Time (hh:mm): 0 : 0 (spinners)
- Please select the day of the month: ☐  \* Day (radio button and text input)
- ☒ First (radio button)
- Monday (dropdown)

At the bottom of the 'Add Power Control Schedule' section is an 'Add' button. At the bottom of the entire screen are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 96** Maintenance > Power Management > Edit

LABEL	DESCRIPTION
Power Control Schedule List	This table lists the power on, power off, and reboot schedules. For example, you could have one schedule to turn the NSA on every morning, at 8:00, another schedule to turn it off every evening at 18:00, and a third schedule to have it reboot every Friday at 14:00.  Click a column's heading cell to sort the schedules by that column's criteria. Click the heading cell again to reverse the sort order.
Type	This field displays whether the power control schedule has the NSA turn on, turn off, or reboot.
Frequency	This field shows how often (monthly, weekly, or daily) the NSA is to apply this power control schedule.
Execute Time	This field shows when the NSA is to use this power control schedule (when the NSA is to turn on, turn off, or reboot).
Actions	Click the <b>Delete</b> icon to remove a power control schedule from the list.
Add Power Control Schedule	Use this part of the screen to configure power on, power off, and reboot times.



**Table 96** Maintenance > Power Management > Edit (continued)

LABEL	DESCRIPTION
Type	Select whether this power control schedule has the NSA turn on, turn off, or reboot.
Frequency	Select whether the NSA is to apply this power control schedule entry on a monthly, weekly, or daily basis.
Execute Time (hh:mm)	<p>Enter the time, day, and/or day of the month as appropriate for this power control schedule entry. Leave more than 10 minutes between the execution times of the entries.</p> <p>If the NSA turns off or restarts while a user is transferring files to or from the NSA, the transfer fails. The user will need to restart the transfer.</p> <p>The NSA skips a scheduled restart or power off if the execution time comes while the NSA is doing any of the following:</p> <ul style="list-style-type: none"> <li>• Resynchronizing a RAID</li> <li>• Upgrading firmware</li> <li>• Replacing the configuration file</li> </ul> <p>If the NSA is turned off at the time when a restart or power off is scheduled, the NSA does not perform the restart or power off.</p> <p>If the NSA is turned on at the time when a power on is scheduled, the NSA does not perform the power on.</p>
Use this part of the screen to configure power on, power off, and reboot times.	
Please select the day of the month	<p>This is only available if you selected <b>Monthly</b> as your backup frequency.</p> <p>Choose the day of each month when NSA performs the backup job.</p>
Every how many weeks?	<p>This is only available if you selected <b>Weekly</b> as your backup frequency.</p> <p>Enter the interval between weeks and choose on which day in the week the NSA performs the backup job.</p>
Every how many days?	<p>This is only available if you selected <b>Daily</b> as your backup frequency.</p> <p>Enter the interval between days when the NSA performs the backup job.</p>
Add	Click this to add the power control schedule to the list.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

## 15.4 The Log Screen

Click **Maintenance > Log** to open the following screen.

Use this screen to display all NSA logs. There are at most 512 entries in the log. Older logs are removed by the system. You cannot download the log file via FTP or CIFS.

**Figure 145** Maintenance > Log

#	Time	Class	Severity	Message
1	2009-05-18 16:03:43	user	info	User admin has logged in from Web!
2	2009-05-18 16:02:14	user	info	User admin from Web has been logged out (lease timeout)!
3	2009-05-18 15:33:07	user	info	User admin has logged in from Web!
4	2009-05-18 15:30:09	user	info	User admin from Web has been logged out (lease timeout)!
5	2009-05-18 15:14:48	user	info	User admin has logged in from Web!
6	2009-05-18 15:00:31	user	info	User admin from Web has been logged out (lease timeout)!
7	2009-05-18 14:43:01	user	notice	Add new group crushes.
8	2009-05-18 14:41:24	user	info	User admin has logged in from Web!
9	2009-05-18 14:41:04	user	info	User admin from Web has been logged out (lease timeout)!
10	2009-05-18 14:36:32	built-in-service	info	Download service download http://www.garageband.com/mp3cat/.UZCMbCSD4a2n/01_April_17__2009__Friday__Part_3.mp3 error (0x20000012)
11	2009-05-18 14:36:31	built-in-service	info	Download service start to download http://www.garageband.com/mp3cat/.UZCMbCSD4a2n/01_April_17__2009__Friday__Part_3.mp3

The following table describes the labels in this screen.

**Table 97** Maintenance > Log

LABEL	DESCRIPTION
Refresh	Click this to update the log display.
Purge all Logs	Click this to erase all logs from the NSA.
Report Config	Click this to open a screen where you can configure email alerts for logs. Refer to <a href="#">Section 15.4.1 on page 311</a> to see the screens for this.
Display	The screen always shows all logs by default. Choose a specific log category to view logs for just that category.
#	This is the log entry's number in the list according to the currently selected sort order.
Time	This shows the date and time the log was created. Click the top of the column to sort by oldest or newest.
Class	This displays the log category; see <a href="#">Table 106 on page 320</a> for details.
Severity	This displays how serious the log is rated by the NSA. See <a href="#">Table 107 on page 320</a> for more information.
Message	This displays a description of the log. Click the top of the column to sort by alphabetical or reverse alphabetical order.

## 15.4.1 Report Config Screen

In the **Log** screen, click **Report Config** to do the following:

- Use the **Email Setting** screen ([Section 15.4.2 on page 311](#)) to enable and configure e-mail alerts from the NSA.
- Use the **Report Setting** screen ([Section 15.4.3 on page 312](#)) to select the type of alerts you want to receive through e-mail and schedule when the NSA e-mails the alerts.
- Use the **Syslog Server Setting** screen ([Section 15.4.4 on page 313](#)) to enable the syslog server and select the categories to include in the log report.

## 15.4.2 Email Setting

You can enable and configure e-mail alerts from the NSA. In the **Report Config** screen, click the **Email Setting** tab to open the following screen.

**Figure 146** Maintenance > Log > Report Config: Email Setting

The following table describes the labels in this screen.

**Table 98** Maintenance > Log > Report Config: Email Setting

LABEL	DESCRIPTION
Enable Log Email	Click this to have the NSA e-mail log alerts to your e-mail account.
Email To	Enter the e-mail address where you want to receive the log alerts.
Email From	Enter the e-mail address the NSA uses in the From field of the e-mail header for its log alerts.
Email Server	Enter the e-mail server address the NSA uses to send e-mail alerts,
Email Format	Select the e-mail format you want the NSA to use in its e-mail alerts.
Use SMTP Authentication	Click this if the e-mail server you want the NSA to use for its e-mail alerts requires a username and password.
User	Enter the username for the e-mail server.

**Table 98** Maintenance > Log > Report Config: Email Setting (continued)

LABEL	DESCRIPTION
Password	Enter the password for the e-mail server.
Password (Confirm)	Re-enter the password to confirm it.
After apply settings, send a test email	Click this to have the NSA send a test e-mail to the settings you have entered.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

### 15.4.3 Report Setting

You can select the type of alerts you want to receive through e-mail and schedule when the NSA e-mails the alerts. In the **Report Config** screen, click the **Report Setting** tab to open the following screen.

**Figure 147** Maintenance > Log > Report Config: Report Setting

The screenshot shows the 'Log Report Configuration' window with the 'Report Setting' tab selected. It contains two main sections: 'Email Alert' and 'Email Report'. Each section has a table of log categories with checkboxes. The 'Email Alert' section has a table with columns: All Logs, User, Shares, Services, System, Network, Storage, Applications, Backup, Auto Upload. The 'Email Report' section has a table with the same columns. Below the 'Email Report' table are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

**Table 99** Maintenance > Log > Report Config: Report Setting

LABEL	DESCRIPTION
Email Alert	Check the type of log alerts you want to receive in your e-mail. Select <b>All Log</b> to include all types of log alerts.
Email Report	Check the type of log alerts you want to receive in your e-mail. Select <b>All Log</b> to include all types of log alerts.
Report Time	Select how often ( <b>Weekly</b> , <b>Daily</b> or <b>Hourly</b> ), what day in the week (Monday to Sunday) and which time (hour:minutes) the NSA delivers its e-mail alerts.
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

## 15.4.4 Syslog Server Setting

You can enable the syslog server and select the categories to include in the log report. In the **Report Config** screen, click the **Syslog Server Setting** tab to open the following screen.

**Figure 148** Maintenance > Log > Report Config: Syslog Server Setting

The following table describes the labels in this screen.

**Table 100** Maintenance > Log > Report Config: Syslog Server Setting

LABEL	DESCRIPTION
Enable Syslog Server	Check this to enable syslog server.
Server Address	Enter the syslog server address you want the NSA to use for its log alerts.
In the table below, check the type of log alerts you want to receive in your e-mail. Select <b>All Log</b> to include all types of log alerts.	
Apply	Click this to save your changes.
Cancel	Click this to return to the previous screen without saving.

## 15.5 The Configuration Screen

Click **Maintenance > Configuration** to open the following screen. Use this screen to backup or restore the NSA configuration settings.

**Figure 149** Maintenance > Configuration

Maintenance - Configuration

**Backup Current Configuration Settings**

Click the "Backup" button to save the current configuration of our system to your local computer.

**Restore Configuration**

To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Restore.

Restore File:

**Reset MySQL Database Password**

Click the Reset MySQL Database Password button to reset the MySQL database password.

The following table describes the labels in this screen.

**Table 101** Maintenance > Configuration

LABEL	DESCRIPTION
Backup Current Configuration Settings	
Backup	Click this to save the current configuration of the NSA to your computer. A pop-up screen appears asking you to confirm. Click <b>OK</b> to continue or <b>Cancel</b> to quit.
Restore Configuration	<p>When you restore a file configuration, the NSA checks the volumes/share paths on the NSA and the configuration file.</p> <p>If the volume exists but the share path is missing in the NSA, the NSA automatically creates this share path.</p> <p>If the volume does not exist on the NSA, the <b>Status</b> of the share will show "missing share icon" in <b>Shares</b> screen (see <a href="#">Table 89 on page 294</a>).</p>
Browse	Click this to locate a previously-saved configuration file.
Restore	<p>Click this to load the previously-saved configuration file to the NSA. This replaces your current NSA configuration settings with the settings in the previously-saved configuration file.</p> <p>A pop-up screen appears asking you to confirm. Click <b>OK</b> to continue or <b>Cancel</b> to quit.</p>
Reset MySQL Database Password	Click this to reset the password for your MySQL database.

## 15.6 SSL Certification

Click **Maintenance > SSL** to open this screen, where you can turn on HTTPS, create a public key certificate, or upload a public key certificate that was issued by a known certificate authority.

**Figure 150** Maintenance > SSL

**Force HTTPS (TLS/SSL) Connections**

**⚠ Caution:**  
Modifications of TLS/SSL certificate settings will restart network services.

☐ Force HTTPS

[Apply](#)

---

**Install System Default CA**

This action will install the system default CA in the trusted CA list of your browser

Step1 Download the default CA file [Download](#)

Step2 Double click on the CA file to install it into your browser

---

**Modify the Existing Certificate**

**⚠ Caution:**  
Modifications of TLS/SSL certificate settings will restart network services.

☒ Edit a self-signed CA certificate

**Step1** Edit the Self-signed Certificate [Edit](#)


**Step2** Download the self-signed CA file [Download](#)

**Step3** Double click on the CA file to install it into your browser

☐ Create a Certificate To Be Authorized By My Own Certificate Authority

The following table describes the labels in this screen.

**Table 102** Maintenance > SSL

LABEL	DESCRIPTION												
Force HTTPS	<p>Select the <b>Force HTTPS</b> option to turn on the NSA’s web browser security. Anyone who connects via HTTPS to the NSA must install the public key certificate associated with it.</p> <p>Note: The NSA will restart the web configurator after you click <b>Apply</b>.</p> <p>The NSA displays a warning screen if applying your change may disconnect some users. Click <b>Apply</b> if you want to continue.</p> <div><p><b>Warning Confirmation</b></p><p>The following users are currently connected. If you decide to continue, they may be disconnected.</p><table><tr><th>Type</th><th>Share Name</th><th>Username</th><th>IP Address</th></tr><tr><td>Web</td><td></td><td>admin</td><td>172.23.37.104</td></tr><tr><td>CIFS</td><td>music</td><td>admin</td><td>172.23.37.104</td></tr></table><p> <b>Performing this operation will cause some network services to temporarily disconnect.</b></p><div><input type="button" value="Apply"/> <input type="button" value="Cancel"/></div></div>	Type	Share Name	Username	IP Address	Web		admin	172.23.37.104	CIFS	music	admin	172.23.37.104
Type	Share Name	Username	IP Address										
Web		admin	172.23.37.104										
CIFS	music	admin	172.23.37.104										
Install System Default CA	<p>Click <b>Download</b> button to save a copy of the NSA’s public key certificate to your local computer. This is useful for installing the certificate without having to connect to the NSA, or for sending by email to other users for them to install prior to logging into the NSA for the first time. After saving the certificate to your computer, double-click it to install it.</p> <p>Note: Each web browser handles certificate installation differently. See <a href="#">Appendix D on page 403</a> for more information.</p>												
Modify the Existing Certificate	<p>Select <b>Edit a self-signed CA certificate</b>, then follow the on-screen instructions for creating a public key certificate signed by the NSA as the local certificate authority.</p> <p>Note: Use certificates created and signed by the NSA if the device is not open to external access.</p> <p>Select <b>Create a certificate authorized by other CA</b>, then follow the on-screen instructions to install a certificate that has been authorized by a third-party certificate authority.</p> <p>Note: Use this method if the device is open to external access, such as allowing users to connect through the Internet using FTP over TLS or HTTPS.</p>												



## 15.6.1 Modifying or Creating a Certificate

When you select the **Edit a self-signed CA certificate** option, then click the **Edit** button, a screen opens to allow you to make adjustments to the NSA's public key certificate.

The screen is also the same for the **Create a certificate authorized by other CA** option.

**Figure 151** Maintenance > SSL > Create or Edit a Certificate

The following table describes the labels in this screen.

**Table 103** Maintenance > SSL > Create or Edit a Certificate

LABEL	DESCRIPTION
Common Name	This name describes the certificate's origin, either in the form of an IP address or a domain name.
Host IP Address	Select this option and enter the NSA's IP address if you want to use this for the common name.
Host Domain Name	Select this option and enter the NSA's domain name if you want to use this for the common name
Organizational Unit (Optional)	Enter this name of the organizational unit which owns or maintains the NSA. This is an optional field.
Organization (Optional)	Enter this name of the organization or company which owns or maintains the NSA. This is an optional field.
Country (Optional)	Enter this name of the country in which the NSA is located. This is an optional field.
Key Type	Select the certificate's key type, either <b>RSA</b> or <b>DSA</b> . RSA is a public-key encryption and digital signature algorithm, while DSA is only a digital signature algorithm.
Key Length	Select the encryption key length. The longer the key, the better the encryption security. The only drawback to having a long key is that the file encrypted with it swells in size as well.

**Table 103** Maintenance > SSL > Create or Edit a Certificate

LABEL	DESCRIPTION
Apply	Click this to save your changes.
Cancel	Click this to discard changes and close the window.

## 15.7 The Firmware Upgrade Screen

Use this screen to upgrade the NSA firmware. You should first have downloaded the latest firmware files from the ZyXEL website.

Click **Maintenance > FW Upgrade** to open the following screen.

**Figure 152** Maintenance > FW Upgrade

The following table describes the labels in this screen.

**Table 104** Maintenance > FW Upgrade

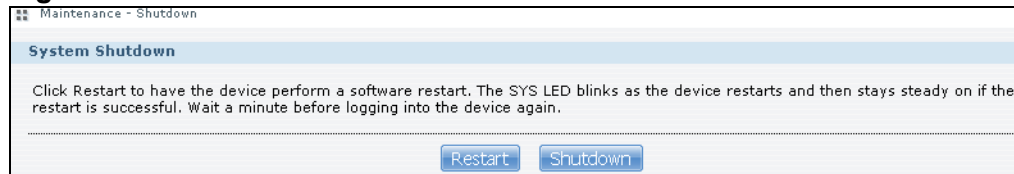
LABEL	DESCRIPTION
Firmware File	Type the location of the firmware file you want to upload
Browse	Click this to find the file on your computer
Upload	Click this to upload the new firmware. The NSA automatically restarts after you upgrade. Wait until the restart completes before accessing the NSA again. If you interrupt the upgrade, then the NSA may become unusable.
Reset	Click this to refresh the screen.

## 15.8 The Shutdown Screen

Use this screen to turn off the NSA or perform a software restart. A software restart is faster than turning the NSA off and then turning it on again. Before shutting down or restarting, check the **System Status > Active Sessions** screen to make sure that no one is logged into the NSA or transferring files to or from the NSA.

Click **Maintenance > Shutdown** to open the following screen.

**Figure 153** Maintenance > Shutdown



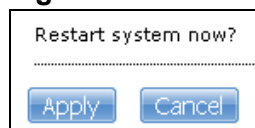
The following table describes the labels in this screen.

**Table 105** Maintenance > Shutdown

LABEL	DESCRIPTION
Restart	Click this to have the device perform a software restart.
Shutdown	Click this to shut down the system and restart it again later.

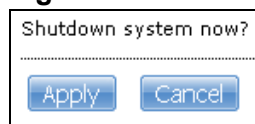
When you click the **Restart** button a pop-up screen will appear asking you to confirm. Click **OK** to continue or **Cancel** to quit the restart.

**Figure 154** Maintenance > Shutdown > Confirm Restart



When you click the **Shutdown** button a pop-up screen will appear asking you to confirm. Click **OK** to continue or **Cancel** to quit the shutdown.

**Figure 155** Maintenance > Shutdown > Confirm Shutdown



## 15.9 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

## 15.9.1 Log Classes

The following table shows information on log classes.

**Table 106** Log Classes

LOG CATEGORY	DESCRIPTION
Users	This log class shows information on user access to the NSA.
Shares	This log class shows information on shares being created or deleted.
Services	This log class shows information on the operation of the NSA's built-in services.
System	This log class shows all other system related messages.
Network	This log class shows information on network configuration, setting changes and so on.
Storage	This log class shows information on the NSA's internal and external storage activities.
Backup	This log class shows information on all backup-related activities.
Auto Upload	This log class shows information on automatic uploads done by the NSA.

## 15.9.2 Log Severity Levels

The following table shows information on log severity levels. Levels range from 0 to 6 with 0 being the most severe level log and 6 being an informational log only. Log levels are not displayed in the logs and are for your reference only.

**Table 107** Log Severity Levels

LEVEL	DESCRIPTION
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Info

## 15.9.3 Log Messages

Here are some example log messages.

**Table 108** Log Messages

CLASS	SEVERITY	MESSAGE
Auto upload	INFO	%s is queued.
Auto upload	INFO	%s uploaded (Flickr or YouTube Upload).

**Table 108** Log Messages (continued)

CLASS	SEVERITY	MESSAGE
Auto upload	WARNING	error uploading "%s" (%s): %s
Auto upload	INFO	%s will not be uploaded to %s for there is already a duplicate file.
Auto upload	INFO	Failed to upload %s to %s (FTP Upload) : %s
Auto upload	INFO	Successfully upload %s to %s (FTP Upload)
Copy/Sync Button	ERROR	[USB %s] Backup Folder Does Not Exist.
Copy/Sync Button	ERROR	[USB %s] Target Folder Does Not Exist.
Copy/Sync Button	ERROR	[USB Sync] Failed at %s: It is a Folder in Internal Volume. But It is not a Folder in USB.
Copy/Sync Button	ERROR	[USB Sync] Failed at %s: It is a Folder in USB. But It is not a Folder in Internal Volume.
Copy/Sync Button	ERROR	[USB Sync] Failed at File %s.
Copy/Sync Button	ERROR	[USB Sync] Sync Failed at Folder %s.
Copy/Sync Button	ERROR	Modify COPY/SYNC Button Configuration: %s
Copy/Sync Button	ERROR	Please Change Your Folder Name. Invalid Path: %s
Copy/Sync Button	INFO	[USB Sync] Copying %s from Internal Volume to Backup Folder.
Copy/Sync Button	INFO	[USB Sync] Copying %s from Internal Volume to USB.
Copy/Sync Button	INFO	[USB Sync] Copying %s from USB to Backup Folder.
Copy/Sync Button	INFO	[USB Sync] Copying %s from USB to Internal Volume.
Copy/Sync Button	INFO	[USB Sync] Deleting %s from Internal Volume.
Copy/Sync Button	INFO	[USB Sync] Deleting %s from USB.
Copy/Sync Button	INFO	[USB Sync] Deleting %s from USB Recursively.
Copy/Sync Button	INFO	[USB Sync] Finished. Elapsed Time %s Seconds.
Copy/Sync Button	INFO	[USB Sync] Moving %s from Internal Volume to Backup Folder.
Copy/Sync Button	INFO	[USB Sync] Moving %s from USB to Backup Folder
Copy/Sync Button	INFO	[USB Sync] Skip %s: File not Exist
Copy/Sync Button	INFO	[USB Sync] Skip %s: Not a Regular File.

**Table 108** Log Messages (continued)

CLASS	SEVERITY	MESSAGE
Copy/Sync Button	INFO	[USB Sync] Start Pre-Processing: Generating File Lists.
Copy/Sync Button	NOTICE	[USB Sync] Start Copying Files.
Download Service	ERROR	Download service cannot find a volume
Download Service	ERROR	Download service failed to find ipfilter.dat
Download Service	INFO	Download service add a URL download job %s
Download Service	INFO	Download service delete %s by user
Download Service	INFO	Download service download %s error (0x%08x)
Download Service	INFO	Download service download %s finished in %s
Download Service	INFO	Download service found a new torrent file %s
Download Service	INFO	Download service initialized
Download Service	INFO	Download service pause %s by user
Download Service	INFO	Download service set %s to %s priority by user
Download Service	INFO	Download service set default download location to %s
Download Service	INFO	Download service set max BT download rate to %d KB/s by user
Download Service	INFO	Download service set max BT upload rate to %d KB/s by user
Download Service	INFO	Download service set max download slot to %d
Download Service	INFO	Download service set seeding time to %d minutues
Download Service	INFO	Download service set TCP port to %d and UDP port to %d
Download Service	INFO	Download service set torrent monitor location to %s
Download Service	INFO	Download service start to download %s
Download Service	INFO	Download service stopped
Download Service	INFO	Download service suspend %s because of no data income detected or to limit max download slot

**Table 108** Log Messages (continued)

CLASS	SEVERITY	MESSAGE
Download Service	INFO	Download service add comment %s to %s by user
Download Service	INFO	Download service set min upload/download ratio to %d%
Download Service	INFO	Download service set max seed slot to %d
Download Service	INFO	Download service start loading ipfilter.dat
Download Service	INFO	Download service clear all ipfilter rules
Download Service	INFO	Download service blocked peer removed from peer list
Download Service	INFO	Download service disconnected blocked peer
Download Service	INFO	Download service incoming connection blocked by IP filter
Download Service	INFO	Download service peer from tracker blocked by IP filter
Download Service	INFO	Download service abort loading ipfilter.dat
Download Service	INFO	Download service will update ipfilter.dat from %s after %d day(s)
Download Service	INFO	Download service added %d rules from ipfilter.dat
Download Service	INFO	Download service detected invalid ip range %s in ipfilter.dat
Download Service	WARNING	Download service default location does not exist. Load default
Download Service	WARNING	Download service default torrent location does not exist. Load default
Groups	NOTICE	Add new group %s.
Groups	NOTICE	Delete group %s.
Network	NOTICE	%s is active because of changing Port Group. Enable DHCP client.
Network	NOTICE	%s is inactive because of changing Port Group. Disable DHCP client.
Network	NOTICE	%s MTU > (%s MTU - 8), %s may not work correctly.
Network	NOTICE	(%s MTU - 8) < %s MTU, %s may not work correctly.
Network	NOTICE	Add interface %s.
Network	NOTICE	Because %s link down. Default route will not apply until %s link up.
Network	NOTICE	Because base interface %s will be disabled.Interface %s is disabled now., base_ud_iface
Network	NOTICE	Network Config setting is changed

**Table 108** Log Messages (continued)

CLASS	SEVERITY	MESSAGE
Network	NOTICE	Interface %s was disabled.
Network	NOTICE	Interface %s was enabled.
Network	NOTICE	Port Group on %s is changed. Renew DHCP client.
Network	NOTICE	Account pppoe was changed
Network	NOTICE	Add account pppoe
Network	NOTICE	ADD interface ppp0
Network	NOTICE	Interface ppp0 will reapply because Device-Ha become active status.
Network	NOTICE	Interface ppp0 will reapply because Device-Ha is not running.
Network	NOTICE	Network port is disabled
Network	NOTICE	Network port is enabled
Services	INFO	HTTP management port has changed to %s
Services	INFO	Clock timezone is set to GMT%s
Services	INFO	Clock timezone is set to default
Services	INFO	Clock daylight saving is enabled
Services	INFO	Clock daylight saving is disabled
Services	INFO	Clock has disable daylight saving
Services	INFO	MyClock has enable daylight saving
Services	INFO	MyClock has set timezone to %s
Services	INFO	MyClock has set timezone to default
Services	INFO	The date and time are updated from NTP server.
Services	INFO	The date and time are updated manually.
Services	INFO	The time is updated manually.
Services	NOTICE	FTP server stops
Services	NOTICE	FTP server starts
Services	NOTICE	MyClock has changed daylight saving interval
Services	NOTICE	MyClock has disabled daylight saving interval
Services	NOTICE	NTP server has set to '%s'
Services	NOTICE	NTP server has set to null
Services	NOTICE	The NTP service is disabled.
Services	NOTICE	The NTP service is enabled.
Services	WARNING	Reaching Maximum Allowed Rules
Services	WARNING	Rule is empty
Services	WARNING	The Rule Does Not Exist
Shares	INFO	Expire recycle-bin finish for share %s, process time: %s seconds, remove %s file (%s bytes)
Shares	NOTICE	Add new disabled share %s for unshared folder: %s in volume: %s.



**Table 108** Log Messages (continued)

CLASS	SEVERITY	MESSAGE
Shares	NOTICE	Add new share %s.
Shares	NOTICE	Delete share %s.
Shares	NOTICE	Purge all files in recycle-bin folder in share: %s.
Shares	NOTICE	Recycle-bin disabled. Remove recycle-bin folder in share: %s.
Storage	ERROR	Eject External Disk (%s): FAILED
Storage	INFO	Eject External Disk (%s): SUCCESS
Storage	ERROR	Relabel Raid to [%s]: FAILED
Storage	ERROR	Start Repairing Degraded Raid by disk%s: FAILED
Storage	INFO	Relabel Raid to [%s]: SUCCESS
Storage	INFO	Start Repairing Degraded Raid by disk%s: SUCCESS
Storage	NOTICE	Auto Repair Degraded RAID by disk%s.
Storage	NOTICE	There is a RAID Degraded.
Storage	ERROR	Cancel External Volume Scan: FAILED
Storage	ERROR	Cancel Internal Volume Scan: FAILED
Storage	ERROR	Cannot Unmount Volume and RAID. System Busy Using Volume and RAID: Please Reboot and Try Again
Storage	ERROR	Create External Normal Volume [%s] (%s): FAILED
Storage	ERROR	Create Internal Volume [%s] (%s): FAILED
Storage	ERROR	Rename External Volume to [%s]: FAILED
Storage	ERROR	Scan External Volume: FAILED
Storage	ERROR	Scan Internal Volume (%s operation): FAILED
Storage	INFO	Cancel External Volume Scan: SUCCESS
Storage	INFO	Cancel Internal Volume Scan: SUCCESS
Storage	INFO	Create External Normal Volume [%s] (%s): SUCCESS
Storage	INFO	Create Internal Volume [%s] (%s): SUCCESS
Storage	INFO	Rename External Volume to [%s]: SUCCESS
Storage	INFO	Scan External Volume: SUCCESS
Storage	INFO	Scan Internal Volume (%s operation): SUCCESS
System	INFO	NTP update failed
System	INFO	NTP updates successfully from %s
System	INFO	NTP fails to update from %s
System	INFO	Device is rebooted by administrator!
System	INFO	Device is shutdown by administrator!
System	NOTICE	DNS server is changed.
System	NOTICE	Hostname is cleared.
System	NOTICE	Hostname is set to '%s'.
System	NOTICE	System description is changed.
System	NOTICE	System description is empty now.

**Table 108** Log Messages (continued)

CLASS	SEVERITY	MESSAGE
System	NOTICE	DNS server setting is changed
System	NOTICE	DNS server address is changed to be given from DHCP server
System	NOTICE	DNS server address is changed to be assigned by user
System	NOTICE	Name server is changed.
USB	NOTICE	An external APC UPS device is plugged/unplugged.
USB	NOTICE	An external Mass Storage device is plugged/unplugged.
USB	NOTICE	An external Printer device is plugged/unplugged.
USB	NOTICE	An external USB hub device is plugged/unplugged.
Users	ALERT	Failed %s login attempt (incorrect password or inexistent username)
Users	ALERT	Failed %s login attempt (incorrect password or inexistent username)
Users	INFO	User %s has logged in from %s!
Users	INFO	User %s has logged out from %s!
Users	INFO	User %s from %s has been logged out (re-auth timeout)!
Users	INFO	User %s from %s has been logged out (lease timeout)!
Users	NOTICE	Add new user %s by %s from %s.
Users	NOTICE	User %s password has been changed.
Users	NOTICE	Delete user %s by %s from %s.
Users	NOTICE	The user %s from %s has attempted to change the user %s password but old password verification fail.
Users	NOTICE	User %s on %u.%u.%u.%u has been denied access from %s
Users	NOTICE	User %s password has been changed by %s from %s.
Backup/ Restore	ERROR	When query remote target [%s]: %s
Backup/ Restore	INFO	Backup job [%s] successfully
Backup/ Restore	ERROR	When backup [%s]: %s
Backup/ Restore	ERROR	When backup [%s], error happens: %s
Backup/ Restore	INFO	Start to restore backup job [%s].
Backup/ Restore	INFO	Restore backup job [%s] successfully.
Backup/ Restore	ERROR	Restore backup job [%s] failed: %s
Backup/ Restore	INFO	Start to restore backup job [%s] from [%s].
Backup/ Restore	INFO	Restore from [%s] successfully.

**Table 108** Log Messages (continued)

CLASS	SEVERITY	MESSAGE
Backup/ Restore	ERROR	Restore from [%s] failed: %s
Backup/ Restore	ERROR	When restore [%s]: %s
Backup/ Restore	ERROR	When restore job [%s], error happens: %s
Power Management	INFO	Job [%s] is triggered by schedule
Power Management	INFO	Job [%s] is triggered by user
Power Management	ERROR	Job [%s] is resulted as failed
Power Management	INFO	Job [%s] is finished successfully
Power Management	INFO	Job [%s] is pending because other job is running
Power Management	INFO	Job [%s] is canceled by user
Power Management	INFO	Restore job [%s] is triggered by user
Power Management	INFO	[Power On] schedule is triggered.
Power Management	INFO	[Power Off] schedule is triggered.
Power Management	INFO	[Reboot] schedule is triggered.



# Protecting Your Data

## 16.1 Overview

This chapter compares the different ways of protecting data on the NSA and explains how to use backup management software included on the CD.

## 16.2 Protection Methods

There are a variety of ways to protect your data on the NSA. Below is a summary table of what can be done in each situation.

**Table 109** Overview of Protection Methods

SITUATION	ACTION
Unexpected NSA behavior after configuration changes	Back up the NSA configuration file before you make major configuration changes.
Need to transfer data from your computer to the NSA after volume(s) have been created	Use the Memeo Autobackup program.
Data infected by virus	Use anti-virus software on your computer to scan files before saving them onto the NSA. Although this may be slow so you may want to schedule it to occur while no one is using the NSA.  Use a firewall with anti-virus capability on your network.
Hard drive malfunction.	Use RAID.
NSA malfunction Network down  Natural disaster such as a fire or earthquake occurs where your NSA is located	Back up data to another NSA or external USB hard drive.

The following sections describe these methods in more detail. See [Section 7.5.2 on page 154](#) for more information on RAID.

## 16.3 Configuration File Backup and Restoration

Use the **Maintenance > Configuration** menus to create a file of your NSA configurations such as passwords, shares and volumes created, network settings and so on. If you're going to do some major configuration changes, then it is advisable to create a configuration backup file. If things go wrong after you make the configuration changes, you can always go back to the previous configuration by restoring an earlier configuration file.

If you forgot the NSA password, then use the **RESET** button (see [Section 17.4.1 on page 344](#)) to return the NSA to the factory default configuration.

Note: Configuration File Backup and Restoration does not affect data (your files and folders), volumes on the NSA.

## 16.4 Memeo Autobackup

Use the Memeo Autobackup software (included on the CD) on your computer to schedule and manage backups. You can backup from your computer to the NSA. You can also backup from one NSA on your network to another. You can set the Memeo Autobackup software to automatically back up files from your computer to the NSA whenever you modify the files.

Install the included DLNA-compliant Memeo Autobackup software on your Windows 2000 or later computers to let them browse and play files stored on the NSA.

Note: The Memeo Autobackup program uses the same network port as the NAS Starter Utility to discover the NSA. To avoid a port conflict, do not run the Memeo Autobackup program at the same time as the NAS Starter Utility.

Use the Memeo Autobackup software included on the CD to automatically back up selected files from your computer to the NSA whenever you modify the files.

Memeo Autobackup works with Windows 2000 Workstation with Service Pack 6, Windows XP Pro, or Windows XP Home Edition.

### 16.4.1 Memeo Autobackup Installation and Setup

Note: The Memeo Autobackup program uses the same network port as the discovery utility to discover the NSA. To avoid a port conflict, turn off the discovery utility before using Memeo Autobackup.

- 1 Since a computer restart is required, close your other files and programs before installing the Memeo Autobackup software.
- 2 Insert the included CD into your CD-ROM drive. Click the **Tools** icon in the screen that displays. Then click **Memeo Instant Backup Software**.

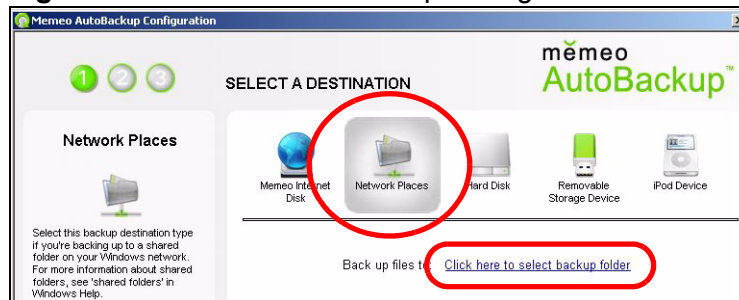
Note: If this screen does not display, use Windows Explorer (My Computer) to go to the CD-ROM (commonly drive D). Double-click **setup.exe**.

- 3 Follow the instructions to install the software.

Note: Memeo Autobackup requires Microsoft.NET version 1.1. The wizard installs it for you if it is not already on your computer.

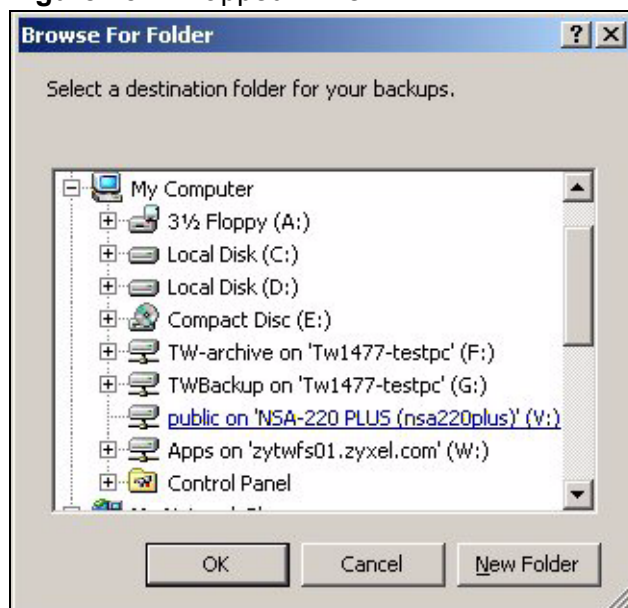
- 4 When you see the following screen, select **Network Places** and click the link to select your backup folder.

**Figure 156** Memeo Autobackup Configuration



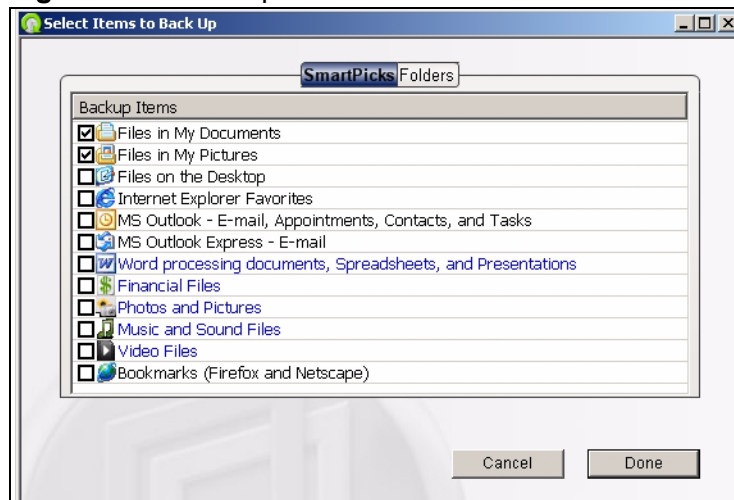
- 5 Select the NSA's mapped drive and click **OK**.

**Figure 157** Mapped Drive



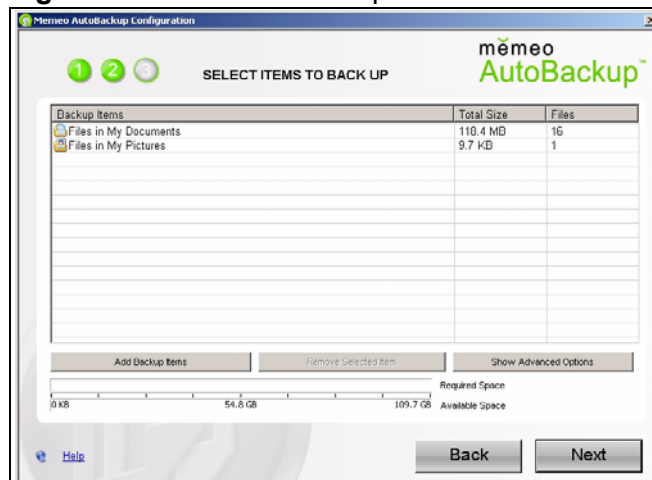
- 6 In this screen, select the items that you want to back up.

**Figure 158** Backup Items



- 7 This screen lists the items you selected for backup. Confirm your selections and click **Next**.

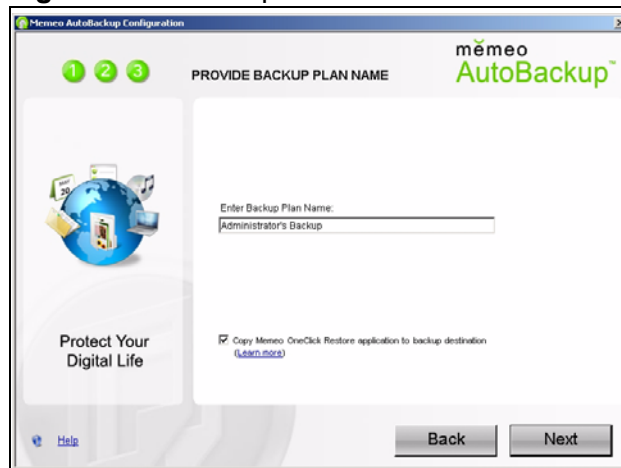
**Figure 159** Confirm Backup Items






- 8 Specify a name for your backup plan (or just use the default). Click **Next** and then **Done**.

**Figure 160** Backup Plan Name

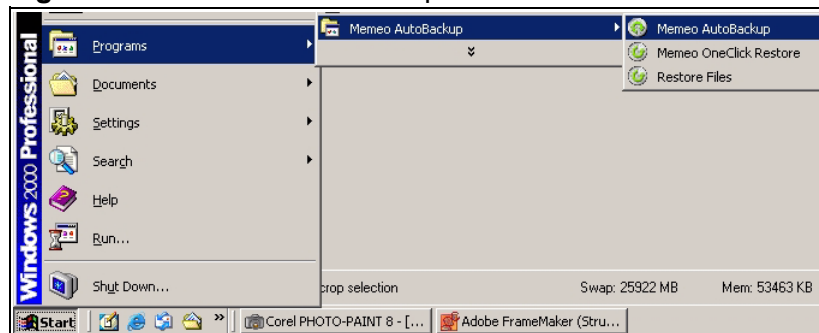


## 16.4.2 Using Memeo Autobackup After the Initial Setup

After you have installed and configured Memeo Autobackup, double-click the  icon in the system tray to open the program's start screen.

If the icon is not displayed, you can click **Start > Programs > Memeo Autobackup > Memeo Autobackup** to start it.

**Figure 161** Memeo Autobackup





---

# **PART V**

# **Troubleshooting and Specifications**

---

Troubleshooting (337)

Product Specifications (361)



# Troubleshooting

## 17.1 Troubleshooting Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- [Power, Hardware, Connections, and LEDs](#)
- [NAS Starter Utility](#)
- [NSA Login and Access](#)
- [I Cannot Access The NSA](#)
- [Users Cannot Access the NSA](#)
- [Storage Volumes](#)
- [External USB Drives](#)
- [Firmware](#)
- [File Transfer](#)
- [Networking](#)
- [Some Features' Screens Do Not Display](#)
- [Media Server Functions](#)
- [Download Service and Broadcatching Functions](#)
- [Web Publishing](#)
- [Auto Upload](#)
- [Package Management](#)
- [Backups](#)

## 17.2 Power, Hardware, Connections, and LEDs

---

The NSA **PWR** LED does not turn on (no LEDs are on).

---

- Make sure the NSA is turned on.
- Make sure you are using the power adaptor or cord included with the NSA.
- Make sure the power adaptor or cord is connected to the NSA and plugged in to an appropriate power source. Make sure the power source is turned on.
- Turn the NSA off and on.
- If the problem continues, contact the vendor.

---

The **HDD** LED is off.

---

The **HDD** LED is off when the NSA cannot detect a hard drive in the drive bay. Replace or install a hard drive. See [Installing or replacing a hard drive](#).

---

The **HDD** LED is orange.

---

Orange means that the NSA detected an error on the hard drive (like a bad sector for example). The NSA automatically tries to recover a bad sector, but the LED stays orange until the NSA restarts. Even if the hard drive still functions, it is recommended that you replace it since errors are a sign that the hard drive may fail soon. See [Installing or replacing a hard drive](#).

---

The **HDD** LED is red.

---

Red means the hard drive has failed and the NSA can no longer detect it. Replace the hard drive. See [Installing or replacing a hard drive](#). If you are using a RAID I volume, you may still be able to use the volume but you should replace the faulty drive as soon as possible.

---

### I want to install another hard disk in my NSA.

---

- The NSA has one internal hard disk bay. It can only support one internal hard disk.
- You can attach an external (SATA) hard disk to your NSA. Use the eSATA port in the rear panel of the device. The hard disk can be configured as an internal volume in the **Storage > Volume** screen. See [Section 7.4 on page 147](#) for more details.

---

### Installing or replacing a hard drive.

---

**Do not remove or install the hard drive while the NSA is turned on. The NSA must be turned off before you remove or install the hard drive.**

- 1 Turn the NSA off, remove the front panel and the drive tray and make sure:
  - there is a SATA I or SATA 3.0 Gbit/s compatible hard drive installed.
  - the hard drive is installed correctly in the drive tray. Push the tray back into NSA drive bay until the screw hole at the top of the drive tray is flush with the drive bay (see the NSA Quick Start Guide and [Section 7.5.5 on page 156](#)).
  - the hard drive could be faulty. Try a different hard drive or test the original hard drive in a different NSA or computer.
- 2 If you had to replace the drive, turn on the NSA and go to the **Storage** screen.

---

### I want to install my internal (SATA) hard disk and access the data inside it.

---

The NSA needs to install its firmware on the internal (SATA) hard disk. It formats the hard disk and creates partitions such that the firmware is installed on one partition, and data is stored on another. In the process, the NSA deletes all existing data in the hard disk.

---

### I want to connect my external (SATA) hard disk and access the data inside it.

---

You need to turn the external (SATA) hard disk into a volume using the **Storage > Volume** screen before the NSA can use it. In the process, all existing data in the hard disk is deleted.

---

The LAN LED (by the **LAN** port) is off.

---

- Make sure the Ethernet cable is connected properly to the NSA and connected to another (Ethernet) device. Make sure the other device is turned on. If it's connected directly to a computer, make sure that the computer network card is working (ping 127.0.0.1 on the computer).
- Use another Ethernet cable. If you're connecting to a Gigabit Ethernet, make sure you're using an 8-wire Ethernet cable.
- If the problem continues, contact the vendor.

See [Section 1.4 on page 26](#) for a description of NSA LEDs.

---

My NSA turns off or reboots by itself.

---

Check the **Power Management** screen. This is where you configure power settings for the NSA, including power saving, UPS, power on/off during power failure and power on/off schedule. The NSA may be set to turn off under certain conditions.

---

A power failure occurred while the NSA is downloading files.

---

- If power failure occurs during the active download period, the NSA will verify whether the downloaded files were damaged.
- If a file is corrupted, the NSA will download the file again.
- If the file is intact but not completely downloaded, the NSA will resume the download task after it restarts.



## 17.3 NAS Starter Utility

---

The NAS Starter Utility cannot discover my NSA.

---

- Close the NAS Starter Utility and reopen it.
- Check your hardware connections and make sure they are set up correctly.
- Only one instance of the NAS Starter Utility can run on your computer. Make sure you close any duplicate windows for this application.
- Wait for the **SYS** LED to stop blinking before clicking **Discover**.
- Confirm that the computer running the NAS Starter Utility has a network connection. See the section on the NSA's LAN connection for related information.
- The computer running the NAS Starter Utility can only discover NSAs in the same subnet. NSAs connected to the same switch or router as your NAS Starter Utility computer are usually in the same subnet unless the router is doing subnetting or the switch is implementing VLAN.
- The Memeo Autobackup program uses the same network port as the NAS Starter Utility to discover the NSA. To avoid a port conflict, do not run the Memeo Autobackup program at the same time as the NAS Starter Utility.

---

I was able to access the NSA on a previous attempt but I cannot access the NSA anymore.

---

If you enable jumbo frames on the NSA in a network that does not support them, you will lose access to the NSA. If this occurs, you will have to restore the factory default configuration. The reset process does NOT affect the volume settings, nor data stored on the NSA. Push the **RESET** button on the NSA's rear panel and release it after you hear a beep ([Section 17.4.1 on page 344](#)).

---

I want to initialize my internal (SATA) hard disk again.

---

**Initializing the hard disk deletes all existing data in it! Back up your files before doing this procedure.**

If you want to initialize an internal (SATA) hard disk that has been initialized by the NSA previously, you will need to reformat the hard disk using your computer. To do this:

- 1 Connect the hard disk to your Windows computer (follow the instructions of your hard disk manufacturer on how to do this). Go to **My Computer > Manage > Disk Management**. Locate the hard disk (on some systems, the hard disk shows up as the disk without a drive letter assigned to it).
- 2 Right-click on all partitions in the hard disk and click **Format**.

**Make sure you select the correct hard disk. Otherwise, all data in the formatted hard disk will be gone.**

---

I don't want to initialize my hard disk but I cannot clear the **Initialize Hard Disk** check box in the **Firmware Path** screen.

---

The checkbox in the **Firmware Path** screen can be cleared only if the hard disk format is compatible with the NSA. If the hard disk format is not compatible with the NSA, this checkbox is checked by default and cannot be modified.

---

I have at least two NSAs in my network, how do I identify which one I want to configure in the NAS Starter Utility screens.

---

If you have several NSAs connected to your computer/network, you can do the following to identify the NSA you want to configure:

- 1 Go to the **Device List** screen.
- 2 Hover your mouse over the host name under **Host** until a box pops up. This shows the details of each NSA device.
- 3 You can identify the device you want to configure by checking the MAC addresses of the NSAs. You can check the MAC address of your NSA by checking the attached sticker in the device housing.

## 17.4 NSA Login and Access

---

I forgot the server name of the NSA.

---

- The default server name is **nsa210**.

- Use the NAS Starter Utility to discover your NSA. If you have admin privileges, you can directly change the IP address of the NSA using the NAS Starter Utility.
- If the server name has changed and you don't have the NAS Starter Utility, see [Section 17.4.1 on page 344](#) to use the **RESET** button to return the default setting.

---

### I cannot get to the NSA login screen.

---

- Use the NAS Starter Utility to discover your NSA. If you have admin privileges, you can directly change the IP address of the NSA using the NAS Starter Utility.
- Make sure you have used the NAS Starter Utility to initialize your NSA. The hard disk has to have the firmware installed before the NSA can be used.
- If you used the **RESET** button, the NSA may have a new IP address. Close and reopen the NAS Starter Utility to discover the NSA.
- Make sure the NSA is turned on.
- If you are trying to login directly by typing the server name into your web browser's address field, make sure you are using the correct server name as the web site address.
  - The default server name is **nsa210**, if you have changed the server name, use the new one.
  - If the server name has been changed and you do not know the new server name, see the troubleshooting suggestions for [I forgot the server name of the NSA](#).
  - If it still doesn't work, try using the NAS Starter Utility.
- Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and [Section 1.4 on page 26](#).
- By default, the NSA gets an IP address automatically. The NSA assigns itself an IP address if no device assigns one. If your computer is also set to get an IP address automatically, the computer and the NSA can both assign themselves IP addresses and communicate. See [Section 8.4 on page 161](#) if you need to configure the NSA with a static IP address.
- Make sure your computer's IP address is in the same subnet as the NSA's IP address. You can use the NAS Starter Utility to find the NSA's IP address. See [Appendix A on page 373](#) for how to change your computer's IP address. Skip this if you know that there are routers between your computer and the NSA.
- Ping the NSA from your computer. Make sure your computer's Ethernet adapter is installed and functioning properly. In a (Windows) computer, click **Start, (All) Programs, Accessories** and then **Command Prompt**. In the **Command Prompt** window, type "ping" followed by the NSA's IP address (use the NAS Starter Utility to find the NSA's IP address if you don't know it) and then press [ENTER].
- Make sure you are using Internet Explorer 6.0 (and later) or Firefox 1.07 (and later).

- Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See [Appendix B on page 389](#). With Internet Explorer 6, you may also have to enable scripting of safe ActiveX controls. See [Section 17.4.2 on page 344](#).

## 17.4.1 Reset the NSA

If you forget your password or cannot access the web configurator, use the **RESET** button at the rear of the NSA. When you use the following reset procedure, the system name and admin password are returned to the factory defaults.

You may need to close and re-open the NAS Starter Utility to discover the NSA. This is because the NSA automatically re-acquires IP address information, so its IP address may change since. If no IP address information is assigned, the NSA uses Auto-IP to assign itself an IP address and subnet mask. For example, you could connect the NSA directly to your computer. If the computer is also set to get an IP address automatically, the computer and the NSA will choose addresses for themselves and be able to communicate.

- 1 Press and hold the **RESET** button (for about two seconds) until you hear a beep, and then release it.
- 2 The NSA automatically restarts to complete the reset.

---

[I forgot the password.](#)

---

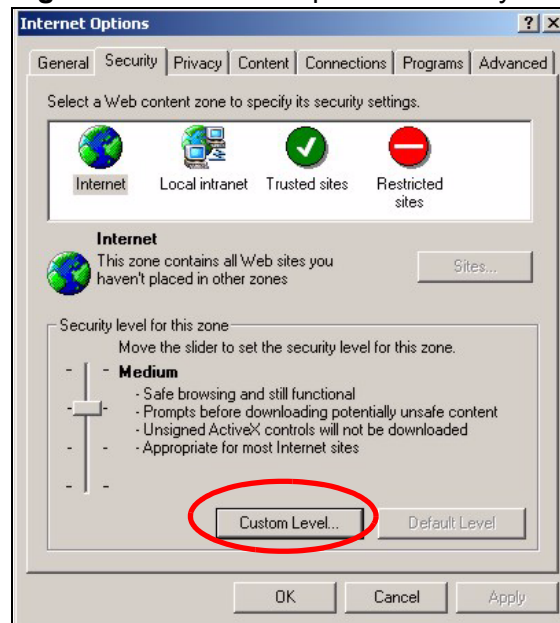
- The default password is **1234**.
- If you have changed the password and forgotten it, you will have to reset the NSA.

## 17.4.2 Enabling Scripting of Safe ActiveX Controls

If pages of the web configurator do not display properly in Internet Explorer, check that scripting of safe ActiveX controls is enabled.

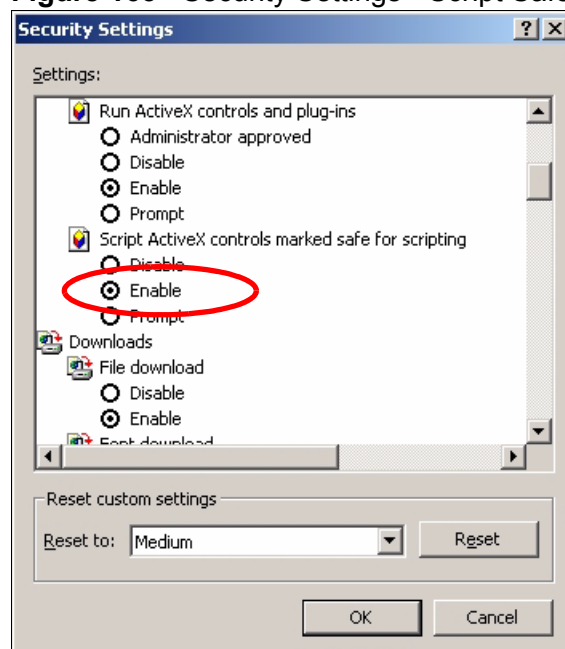
- 1 In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

**Figure 162** Internet Options: Security



- 2 Click the **Custom Level...** button.
- 3 Under **Script ActiveX controls marked safe for scripting**, make sure that **Enable** is selected (the default).
- 4 Click **OK** to close the window.

**Figure 163** Security Settings - Script Safe ActiveX Controls



---

I can see the login screen, but I cannot log in to the NSA.

---

- Make sure you have entered the username and password correctly. The default username is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- Turn the NSA off and on.
- If this does not work, see [Section 17.4.1 on page 344](#) to reset the device.

---

I cannot see the multi-language web configurator screens while using Internet Explorer.

---

Use [Section 17.4.2 on page 344](#) to enable the scripting of safe ActiveX controls.

---

The Web Configurator logs out by itself.

---

The web configurator management session automatically times out if it is left idle for 15 minutes. Simply log back into the NSA if this happens to you.

## 17.5 I Cannot Access The NSA

---

I cannot access a share.

---

- Check that the NSA is turned on and connected to the network. Try to ping the NSA or use the NAS Starter Utility to discover it.
- Make sure you have used the NAS Starter Utility to initialize your NSA. The hard disk has to have the firmware installed before the NSA can be used. See [Chapter 2 on page 29](#) for more information.
- Check that you entered your login name and password correctly.
- Check that the share exists and check its access settings.
- Check if the shared folder is a subfolder of another (parent) share. Check that the parent share's access rights do not conflict with the subfolder share. It is recommended that you do not create subfolder shares.

- Check if there are any existing mapped network drives to the NSA. You may need to disconnect existing mapped network drives as a new mapped network drive connection may use (different) previously-saved login information. To do this, open Windows Explorer and click **Tools > Disconnect Mapped Network Drives**.
- Check that the volume in which the share resides, exists and is not down or degraded. If it is down or degraded, see [Section 17.2 on page 338](#).
- Make sure you have the client for Microsoft networks installed and enabled in your network connection's properties.
  - In Windows XP or 2000, click **Start > Settings > Control Panel > Network Connections (Network and Dial-up Connections in Windows 2000/NT) > Local Area Connection > Properties**.
  - Check that **Client for Microsoft Networks** is in the list of components and has its check box selected.

## 17.6 Users Cannot Access the NSA

---

### A local user cannot access a share

---

- Check that the NSA is turned on and connected to the network. The local user should try to ping the NSA or use the NAS Starter Utility to discover it.
- The local user should check that he entered his login name and password correctly.
- Check if the share exists and has the correct access settings for this user.
- Check the Access Control List (ACL) of read/write permissions associated with specific files and/or folders. Account names added to the list are linked to the files and folders that they are allowed to access, along with what kinds of actions they are allowed to perform with those files and folders (delete, move, rename, and so on).
- The user's computer may already be connected to another of the NSA's shares using a different user name and/or password. This can happen without the user realizing it if the user's computer automatically connects to a share at logon. Right-click any other connected shares and click **Disconnect**. Then re-attempt to connect to the desired share.
- Check if the share has an ANONYMOUS or EVERYONE access right. If the user is already logged into a share using her username and password, she will NOT be able to access a share that has ANONYMOUS FTP only access rights (as these require 'no login'). In this case she should log out and try to access the share again without logging in. See [Section 9.4 on page 167](#) for more details.
- Check if the shared folder is a subfolder of another (parent) share. Check that the parent share's access rights do not conflict with the subfolder share. It is recommended that you do not create subfolder shares.

- Check if the user belongs to a group with conflicting access rights. **DENY** always takes precedence. If you allow a user **FULL** access to a share but set his group to **DENY**, then he will NOT be able to access the share.
- The local user should check if there are any existing mapped network drives to the NSA. He may need to disconnect existing CIFS connections as new CIFS connection may use previously-saved login information that may be different to NSA login.
- Check that the array in which the share resides, exists and is not down or degraded. If the array is down or degraded, see [Section 17.2 on page 338](#).
- If the user is using DFS links, then he can only access the NSA using CIFS and not FTP.
- Check that the share has not been disabled.

---

I cannot import domain user or user group information even though testing of the connection to the domain controller is OK.

---

- Check the NSA's DNS setting. The DNS server the NSA is using must be able to resolve the domain controller's address. If the domain controller uses a private IP address, the NSA needs to use a private DNS server. If the domain controller uses a public IP address, the NSA needs to use a public DNS server.
- Leave the domain and re-join it.

---

A domain user can't access a share.

---

In addition to the checks listed previously for local users, check that the domain controller is turned on and connected to the network.

---

A user can access a share but cannot access individual folders or files within the share.

---

- Check the Access Control List (ACL) of read/write permissions associated with the share's specific files and/or folders. Account names added to the list are linked to the files and folders that they are allowed to access, along with what kinds of actions they are allowed to perform with those files and folders (delete, move, rename, and so on).



## 17.7 Storage Volumes

---

I want to use my external (SATA) hard disk to create a RAID 1 volume but I cannot see **RAID 1** in the list when I click **Create a SATA volume**.

---

- Refer to [Section 4.2.1 on page 60](#) for a tutorial on how to create a RAID 1 volume.
- Make sure that the eSATA hard disk is connected to the NSA's eSATA port located in the device's rear panel. The **eSATA** LED's light should be on.
- The capacity of your eSATA hard disk must be equal to or greater than the internal (SATA) hard disk capacity.
- If the eSATA hard disk is detected by the NSA but you still do not see RAID 1 in the list, check if the internal hard disk is already configured as a JBOD volume. Note that after installing the firmware on the internal hard disk, the internal hard disk is configured as a JBOD volume by default. If this is the case, create a RAID 1 volume by clicking the **Migrate** button ([Section 4.2.2 on page 60](#)) in the **Storage > Volume** screen.
- The **RAID 1** option when you click the **Create a SATA volume** button is only visible when there are no existing volumes in your NSA.

---

I want to choose another storage method for my internal (SATA) hard disk/ external (SATA) hard disk.

---

- If you are not using an eSATA hard disk, **JBOD** is the only storage method you can use for your internal hard disk.
- If you are using an eSATA hard disk, you can configure the internal hard disk and the external hard disk as a **RAID 1** volume.
- For the eSATA hard disk alone, you can configure it as a **JBOD** or **PC Compatible Volume**.
- If you want to change an existing storage method for your hard disk, go to the **Storage > Volume** screen. Delete the volume you want to configure again.

**Deleting an existing volume in the NSA deletes all data in that volume.**

---

One of the hard disks (in a RAID 1 volume) failed.

---

- If you are using RAID 1 and the hard disk inside the NSA fails but the eSATA hard disk is still working, you can remove the hard disk inside the NSA and install the eSATA hard disk inside the NSA. Your NSA runs normally again, but you will need to have another eSATA hard disk attached to the NSA in order to employ RAID 1.
- If the eSATA hard disk in the RAID 1 volume fails, the NSA automatically repairs a degraded RAID if you connect an empty eSATA hard disk without an existing file system. If you connect an eSATA hard disk that is already formatted, you must manually to turn it into a volume in the **Storage > Volume** screen. All data in the hard disk is deleted.

## 17.8 External USB Drives

---

The **COPY** LED is red.

---

Copying files from a USB device failed. The USB device may not be compatible with the NSA. Try save the files onto a computer and then from the computer to the NSA (through the network connection).

## 17.9 Firmware

---

I want to know the firmware version of my NSA.

---

Go to the **Status** screen. The **Firmware** field shows you the current firmware version running.

## 17.10 File Transfer

---

I want to transfer my file(s) from my local computer or storage device to the NSA.

---

- After you initialize your hard disk, you can directly access the folders in your NSA and transfer files in the same way you transfer files in your local computer:

- 1 On your Windows computer, click **Start > Run** or open a web browser.
- 2 Enter **\\nsa210** (default) or the **Server Name** you assigned the NSA. This shows you the folders in the NSA.
- 3 Use drag-and-drop or copy-and-paste to transfer files over to your NSA.
  - Use the **COPY/SYNC** button to transfer files from an external (USB) storage device to the NSA.
  - If the file you want to transfer is less than or equal to 2GB, you can use the **My NSA** screen (see [Section 3.5.1 on page 44](#)).

---

I want to transfer my file(s) from the NSA to my local computer or storage device.

---

- After you initialize your hard disk, you can directly access the folders in your NSA and transfer files in the same way you transfer files in your local computer:
- 1 On your Windows computer, click **Start > Run** or open a web browser.
  - 2 Enter **\\nsa210** (default) or the **Server Name** you assigned the NSA. This shows you the folders in the NSA.
  - 3 Use drag-and-drop or copy-and-paste to transfer files from your NSA to your local computer's folder or your storage device.
    - You can download the files from your NSA. Just click on the file(s) in the **Share Browsing** screen ([Section 3.5.1 on page 44](#)). Your computer will prompt you for the location where you want to save the file.

## 17.11 Networking

---

I want to control who can access my folder(s)/file(s).

---

- If you are an administrator, you can configure a user's access rights. Use the **Shares** screen ([Section 14.3 on page 294](#)) to do this.
- If you enabled **Web Publishing** for a folder, anyone on your network can play the media files in the published shares. No user name and password or other form of security is used. The media server is enabled by default with the video, photo, and music shares published.

---

One of the computers in my network cannot use the printer I connected to the NSA.

---

- You must install the printer driver on each computer that will use the printer.
- Check [Section 17.4 on page 342](#) and check for related connectivity issues.

## 17.12 Some Features' Screens Do Not Display

---

Many NSA features require a valid internal volume.

---

Features like the print server, download service, broadcatching, FTP and Windows/CIFS access will not work without a valid internal volume. Make sure you have a volume on an internal disk and that the volume is in the healthy state.

- Install an internal disk if one is not installed yet or has failed. See the Quick Start Guide for how to install an internal disk.
- Create a new volume if you do not have one on the internal disk yet.
- Make sure the volume on the installed internal disk is in a healthy state.

---

I cannot use some applications in the Web Configurator.

---

- The firmware installed in your NSA includes the features mentioned in [Section 3.6.2 on page 53](#). This does not include the applications you can install using the **Package Management** screen.
- You can use the **Package Management** screen ([Chapter 10 on page 211](#)) to install more applications from a web location (specified in the firmware) to your NSA.
- If you have installed the application and can see the application's configuration screen but still cannot use it, check that you have **Enabled** the application.

## 17.13 Media Server Functions

---

I set the media server function to publish a folder, but some of the files in the folder do not display in the list on the media client.

---

Files with formats that are not supported on the media server may not display in the list. See [Appendix on page 368](#) for the file formats that the media server supports.

---

I published a folder with the media server function, but the media client does not play some of the files (or does not play them properly).

---

- 1 Files with formats that are not supported on the media server may not display in the list. See [Section 18.4 on page 368](#) for the file formats that the media server supports.
- 2 If you are using media client software, you may need to install codecs on your computer. Since the media client software uses your computer's installed codecs, files do not play if the required codec is not installed on your computer.
- 3 The media client may not support the file's format.

---

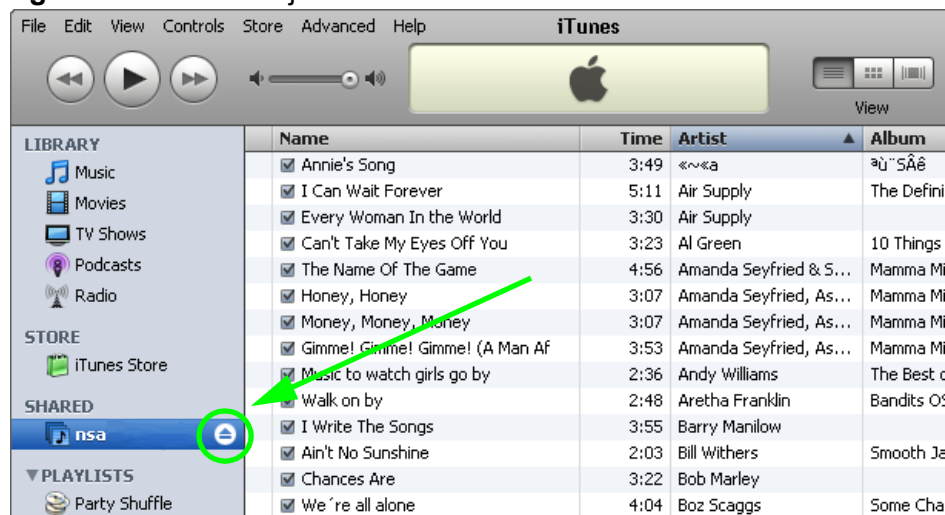
iTunes does not display the names of all the music or video files I just put on the NSA.

---

- 1 Make sure the files are a format supported by iTunes. See [Section 18.5 on page 369](#).
- 2 Go to **Applications > Media Server**. Make sure the share containing the music and video files is published and the iTunes server option is enabled.

- 3 If an iTunes client is connected, the NSA's iTunes server function scans the published media server folders for files every three minutes. Leave iTunes connected to the NSA for three minutes. Then use the NSA's eject button (as shown next) to disconnect.

Figure 164 iTunes Eject Button



- 4 Then click the NSA's link to reconnect.

Figure 165 iTunes Reconnected



- 5 Another way to get the NSA's iTunes server function to scan the published media server folders for files is to go to **Applications > Media Server** and disable and re-enable the iTunes server option. If you uploaded many files, it may take awhile for the NSA to find and list all of them. Then try reconnecting your iTunes client.

---

I cannot use iTunes to play files located on my NSA.

---

- 1 Make sure the files are a format supported by iTunes. See [Section 18.5 on page 369](#).
- 2 If you have files from the iTunes Store that use DRM, you need to use your Apple account ID and password to authorize other computers to play the files. Apple permits you to authorize up to five computers at a time. To authorize a computer, open iTunes and click **Store > Authorize Computer**.
- 3 If you are connecting through a NAT router, make sure that TCP port 3689 and UDP port 5353 are open for traffic on both the server and the client and all points in between (especially the NAT router). If your router includes a firewall, make sure it also allows TCP port 3689 and UDP port 5353 traffic.

## 17.14 Download Service and Broadcatching Functions

---

The download list or broadcatching items are missing after I removed a hard drive.

---

The NSA's download and broadcatching lists are stored on the system volume. If you have two JBOD volumes, it is possible to remove one and still use the other. However if you remove the system volume, you may lose the download and broadcasting lists. With two JBOD volumes, the hard disk that was installed first is usually the system volume.

---

The channel I added in the **Broadcatching** screen is active but no files are downloaded to the NSA.

---

Check the **Download Policy** for that channel (see [Section 9.8.1 on page 188](#)). It may be set to manual download. You can configure your NSA to download all items or only new items automatically once the channel is updated.

---

I cannot find the download files.

---

By default, the **Download Service** and **Broadcatching** features store downloaded files as follows:

- BitTorrent jobs are stored in /\*/incoming (where '\*' is a folder that you have set.)
- HTTP/FTP jobs are stored in /\* (where '\*' is a folder that you have set.)
- All jobs triggered by RSS channels create the subfolder in /\* using the channel name where it store all files downloaded from that channe (where '\*' is a folder that you have set.)

Check your **Preferences** in the **Download Service** ([Section 9.6 on page 171](#)) and **Broadcatching** ([Section 9.8 on page 186](#)) screens to know or configure where downloaded files are stored.

## 17.15 Web Publishing

---

A web-published share cannot be accessed by web browser from the Internet.

---

- Make sure the person trying to access the share is using the correct web address (and port number if the NSA's web publishing feature is not using port 80). See [page 205](#) for details.
- Make sure the publishing feature is turned on and the share is in the list of published shares.
- Make sure the person trying to access the share is using Internet Explorer 6.0 (and later) or Firefox 1.07 (and later).
- You need to use a public address to access the NSA's web-published shares from the Internet. If your NSA uses a private IP address, use the public IP address of your Internet gateway (firewall) and configure NAT or port forwarding on your Internet gateway and possibly firewall rules in order to let people access the NSA's web-published shares from the Internet.
- Make sure the firewall's public IP address is static or that the firewall uses a Dynamic Domain Name (DDNS).
- Web publishing uses TCP protocol and the port number you specify. Make sure there is not another service using TCP protocol with the same port number. See [Appendix C on page 399](#) for a list of common services and their associated protocols and port numbers.
- If Firefox access to the share does not work, check that you did not set the Web publishing feature to use one of the following ports. (Firefox blocks these ports by default.)

**Table 110** Ports Blocked By Default in Firefox

POR T	SERVICE
1	tcpmux
7	echo

POR T	SERVICE
95	supdup
101	hostriame

POR T	SERVICE
513	login
514	shell



**Table 110** Ports Blocked By Default in Firefox

POR T	SERVICE
9	discard
11	systat
13	daytime
15	netstat
17	qotd
19	chargen
20	ftp data
21	ftp control
22	ssh
23	telnet
25	smtp
37	time
42	name
43	nicname
53	domain
77	priv-rjs
79	finger
87	ttyslink

POR T	SERVICE
102	iso-tsap
103	gppitnp
104	acr-nema
109	POP2
110	POP3
111	sunrpc
113	auth
115	sftp
117	uucp-path
119	NNTP
123	NTP
135	loc-srv epmap
139	netbios
143	IMAP2
179	BGP
389	LDAP
465	SMTP+SSL
512	print exec

POR T	SERVICE
515	printer
526	tempo
530	courier
531	chat
532	netnews
540	uucp
556	remotefs
563	NNTP+SSL
587	submission
601	syslog
636	LDAP+SSL
993	IMAP+SSL
995	POP3+SSL
2049	nfs
4045	lockd
6000	X11

- Make sure your ISP allows you to run a server and is not blocking the port number of the NSA's web publishing feature.

## 17.16 Auto Upload

---

The NSA does not automatically upload files to Flickr or YouTube.

---

- 1 Make sure the NSA is connected to the Internet. See [Section 8.4 on page 161](#) for details about testing network connections.
- 2 Click **Maintenance** > **Log** to check the NSA's log for a message about the file.
  - 2a If the log message displays "no such file or directory", the file may have been removed from the NSA. Make sure the file still exists in the watch folder.

- 2b** If the log message displays “filename is queued”, the file may still be waiting for auto upload. Check the grace period setting in the service’s **Configuration** screen. You can set a smaller grace period to shorten the queue time.
- 2c** If you cannot find any log messages about the file:

  - Make sure the **Folder Watch List** includes the folder containing the file. You can upload the file to the watch folder again.
  - Make sure the file’s format is supported by Flickr or YouTube. You can find the supported file extensions in the **Folder Watch List**.
- 2d** If the log message displays “not authorized yet”, check if you can enter the NSA’s **Configuration** screen for the service. If you changed the password of your Flickr or YouTube account, you cannot access the service’s **Configuration** screen, and the NSA cannot auto upload files. Make sure you also update the account information in the NSA.
- 3** Make sure the file size does not exceed the limit imposed by the service. At the time of writing, Flickr restricts the file size to 10 MB, and YouTube restricts the file size to 100 MB.
- 4** Make sure you did not exceed the service’s upload quota. Flickr and YouTube have different policies about how much you can upload within a certain period, for example, 100 MB/week.
- 5** The NSA may have temporarily failed to connect to the service. You can upload the file to the watch folder again.

## 17.17 Package Management

---

The NSA won’t install the package(s) I selected in the **Package Management** screen.

---

- The web location of the package may be undergoing maintenance. Try again at a later time. Upgrade the firmware of the NSA.
- If a new firmware is available, do an upgrade and try installing the package(s) again.

---

The eMule **Search** screen does not work.

---

You need to be connected to an eMule server before you can use the **Search** screen. Wait for the NSA to connect to a server before configuring the **Search** screen.

---

I want to know how my hard disk is performing.

---

Use S.M.A.R.T. (Self Monitoring, Analysis, and Reporting Technology) to monitor hard disks. It detects and reports the reliability of hard disks using standard indicators, enabling administrators to anticipate possible disk failures. Go to the **Package Management** screen to install the S.M.A.R.T. application.

## 17.18 Backups

---

I cannot make a backup.

---

- Check that enough space is available on the external disk. If there isn't you may need to purge older backups or delete other files on the backup USB disk or NSA (see [Section 10.9 on page 241](#)).
- If you are using **BackupPlanner** ([Section 10.10 on page 241](#)):
  - You can look at the **Backup** screen's **Last Run Result** display.
  - If you're backing up to another NSA, another NSA, or a computer, check that it allows the NSA to write files to it. For a synchronization backup, the target must be another NSA or another compatible model.
  - Check that the NSA is not performing another backup job. **Scheduler** queues backups when a different backup is already going on at the time a backup is scheduled.

---

The backup does not run at the time configured.

---

- Check that the correct time is configured on the NSA.
- Check that the NSA is able to access the time server from which it gets the time; see [Section 6.5 on page 141](#).



# Product Specifications

See also [Chapter 1 on page 23](#) for a general overview of the key features.

## 18.1 Physical Features

These are the main external physical features.

**Table 111** Physical Features

USB Ports	<p>2 USB (version 2) ports.</p> <p>Copy or sync files directly from the NSA to compatible USB devices like card readers, MP3 players, mass storage devices, and digital cameras without using a computer. Copy or sync files directly from a USB device to the NSA.</p> <p>Expand the NSA's storage capacity with compatible USB devices (like hard drives).</p>
Gigabit Ethernet Port	<p>The 10/100/1000 Mbps auto-negotiating Ethernet port allows the NSA to detect the speed of incoming transmissions and adjust appropriately without manual intervention. It allows data transfer of either 100 Mbps or 1000 Mbps in either half-duplex or full-duplex mode depending on your Ethernet network. Use an 8-wire Ethernet cable for Gigabit connections. The port is also auto-crossover (MDI/MDI-X) meaning it automatically adjusts to either a crossover or straight-through Ethernet cable.</p> <p>Actual data throughput varies depending on the network conditions and environmental factors, including volume of network traffic, network overhead and building materials.</p>
SATA Interface	<p>Serial ATA is a low cost interface technology that allows high speed data transfer. Serial ATA also allows more efficient internal airflow and also smaller chassis design.</p>
eSATA Interface	<p>eSATA is the "external" counterpart of the SATA interface. It has all of SATA's features but with the added advantage of being mobile.</p>

**Table 111** Physical Features

Power Button	<p>Press the <b>Power</b> button for one second to turn it on.</p> <p>Turn off the NSA before unplugging the device.</p> <p>Press the <b>Power</b> button for 3 seconds until you hear one beep, then release it. The NSA goes starts to shutdown its software and turns off.</p> <p>Press the <b>Power</b> button for 5 seconds until you hear two beeps, then release it. This NSA turns off immediately.</p>
COPY/SYNC Button	<p>The <b>COPY/SYNC</b> button is used to copy or sync data from the NSA to a compatible external (USB) storage device or from the external (USB) storage device to the NSA.</p> <p>Press the <b>COPY/SYNC</b> button to copy data from Public folder (default) of the NSA. Use the Web Configurator to configure the folder locations for the <b>COPY/SYNC</b> function. During the data transfer, the <b>COPY</b> LED blinks and stops when the transfer is complete.</p> <p>If you want to sync the data in the NSA with the external (USB) storage device, press the <b>COPY/SYNC</b> button until you hear one beep.</p> <p>If the <b>COPY</b> LED turns red, an error has occurred and the transfer is stopped. Press the <b>COPY/SYNC</b> button once and the <b>COPY</b> LED turns green.</p>
RESET Button	<p>Press the <b>RESET</b> button for 2 seconds to restart the NSA.</p> <p>If you forget your (admin) password, press the <b>RESET</b> button for 10 seconds to restore the factory default password to "1234" (with username "admin"), and auto-IP address (DHCP client).</p>

## 18.2 Firmware Features

These are some of the main firmware features of the NSA.

**Table 112** Firmware Features

DLNA Server	The NSA is a DLNA-compliant media server that lets DLNA-compliant media clients play video, audio, and photo content files stored on the NSA.
RAID File Storage	Use RAID 1 if you have two drives and want to mirror primary data to the second drive. If one drive fails, replace it and then re-synchronize to recover all data.
User Passwords	Configure a password for an individual <b>User</b> to restrict access to the NSA.

**Table 112** Firmware Features

Client Support	<p>Data can be shared among all Windows, Mac, Linux, and UNIX users that have FTP client software or CIFS file sharing support (such as Samba for Linux and UNIX users).</p> <p>The NSA is also a DLNA-certified media server that lets DLNA-compliant media clients play video, audio, and photo content files stored on the NSA.</p>
HTTP	Access the NSA using a regular web connection (HTTP).
DHCP (Dynamic Host Configuration Protocol)	DHCP (Dynamic Host Configuration Protocol) allows the NSA to obtain an IP address and subnet mask at start-up from a centralized DHCP server. Alternatively, you can give the NSA a static IP address and subnet mask.
Full Network Management	The embedded web configurator is an platform-independent web-based utility that allows you to easily access the NSA's management settings.
Hard Disk Drive Power Saving	If a hard disk inside the NSA is idle for six minutes, the NSA puts it to sleep until you use it again.
Firmware Upload and Configuration File Management	Upload new firmware to the NSA using the web configurator. You can also back up and restore the NSA configuration file containing all its settings to/from your computer.
NAS Starter Utility	Use the NAS Starter Utility from a Windows computer to find NSA(s) in your network, access the NSA login page, change its IP address configuration or map to a Windows network drive.
Memeo Autobackup	Memeo Autobackup is a tool for Windows users to create backups of data stored on their Windows computers to an NSA. This software is included on the CD.
Time and Date	Configure a time server and set a time zone for your NSA to show the correct times in logs.
Auto Upload	The auto upload feature uploads media files stored in the NSA to the Flickr and/or YouTube sharing websites. It is a convenient way to share media files with your friends and family. You can link the NSA to your Flickr and/or YouTube account and select shares for the NSA to upload. The NSA uploads the media files stored in the specified shares to your Flickr and/or YouTube account. When you add new files to the specified shares, the NSA also automatically uploads the new files to your Flickr and/or YouTube account.
iTunes Server	The NSA can mimic the iTunes application and download content from the iTunes server.
Package Management	Package Management can be used to set up more useful applications in your NSA, including eMule, DyDNS, NFS, SMART, BackupPlanner, Gallery, PHP-MySQL-phpMyAdmin, SqueezeCenter and WordPress. The NSA can download multiple packages/files at once and automatically goes through all the installation steps.

**Table 112** Firmware Features

DyDNS	Dynamic DNS allows you to update your current dynamic IP address with a dynamic DNS service so that anyone can contact you (in NetMeeting, CUSeeMe, etc.). You can also access your FTP server or Web site on your own computer using a domain name (for instance myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives will always be able to call you even if they don't know your IP address.
Download Service	The NSA's download service downloads files from the Internet directly to the NSA. You do not have to download to your computer and then copy to the NSA. This can free up your computer's system resources. The download service also handles your broadcastcatching downloads.
Power Schedule	Use this screen to manage power settings for the NSA, including power saving, UPS, power on/off during power failure and power on/off schedule.

## 18.3 Specification Tables

The NSA hardware specifications are shown in the following table.

**Table 113** NSA Hardware Specifications

Default IP Address	DHCP client. If no DHCP server is found, the NSA uses Auto-IP to choose an IP address in the 169.254.X.X subnet (where X is a number from 1 to 254).
Default Subnet Mask	DHCP client by default. If no DHCP server is found, the subnet mask defaults to 255.255.255.0 (24 bits).
Default Username	admin
Default Password	1234
Dimensions	195.5 (D)* 58 (W)* 130 (H) mm
Weight	0.66 kg (without hard drives)
Drive Trays	One
Compatible Hard Disks	SATA I and SATA II 3.0 Gbit/s (Serial Advanced Technology Attachment) compatible hard drives.
Maximum Number of Folders Per Share	The NSA's media server function can detect up to 8,000 folders within a single published share.  After 8,000 folders have been created, new folder contents will not be added to the media server's list. However you can still access the folders using Samba.
Ports	
Ethernet	One auto-negotiating, auto MDI/MDI-X 10/100/1000 <sup>A</sup> Mbps RJ-45 Ethernet port (1000BASE-T)



**Table 113** NSA Hardware Specifications (continued)

USB v2.0 Storage	One port in the back panel and one port in the front panel. Windows: NTFS (read only), FAT32 and FAT16 Linux: ReiserFS, XFS, EXT2, and EXT3.
eSATA port	One port in the back panel.
LEDs	PWR, SYSTEM, HDD, eSATA, USB and COPY.
Operating Temperature	0° C ~ 40° C
Power Supply	Input: 100 - 240 V AC, 0.9 A, 50-60 Hz Output: 12 V DC, 2.5 A
Storage Temperature	-30° C ~ 70° C
Operating Humidity	0% ~ 95% RH (non-condensing)
Storage Humidity	0% ~ 95% RH (non-condensing)
Certifications	Device: CE, FCC Part 15B, C-Tick, BSMI Power Adapter: CE, FCC, CUL, TUV/GS, RCM, BSMI, Efficiency Level V (CEC regulation)

A. Use an 8-wire Ethernet cable for Gigabit connections.

The NSA firmware specifications are shown in the following table

**Table 114** NSA Firmware Specifications

File Storage System	JBOD, RAID 1
Network Protocols	TCP/IP, UDP/IP DHCP Client FTP HTTP
File Management	Create/Delete System Volume
Network File Sharing Protocol	CIFS/SMB for Windows and Mac OSX HTTP for web browser FTP
Network Security	Authentication Share level
Supported Clients	Windows 2000 (SP4) Windows XP (SP2) Windows Vista (32 bit) Windows 7 Windows Server 2003 Mac OS X 10.3 and later versions

**Table 114** NSA Firmware Specifications (continued)

Maximum Number of Users Allowed	64 <sup>A</sup>
Maximum Number of Concurrent FTP Sessions	32 <sup>A</sup>
Maximum Number of Concurrent CIFS Sessions	32 <sup>A</sup>
System Management	Remote Management via Web Configurator (HTTP) NAS Starter Utility
Logging/Monitoring	Centralized Logs
Firmware Upgrade	Web Configurator
Web Browsers Supported	Internet Explorer 6.0 and later versions Firefox 1.03 and later versions Safari 1.22 and later versions

A. Limits may vary depending on user-share resource usage.

The following list, which is not exhaustive, illustrates the standards and recommendations supported in the NSA.

**Table 115** Supported Standards and Recommendations

CSS level 1	Cascading Style Sheets.
CSS level 2 revision 1 ("CSS 2.1")	Cascading Style Sheets.
DATETIME	"Date and Time Formats", W3C (World Wide Web Consortium) Note, M. Wolf and C. Wicksteed, 15 September 1997. Revised 27 August 1998. See <a href="http://www.w3.org/TR/1998/NOTE-datetime-19980827">http://www.w3.org/TR/1998/NOTE-datetime-19980827</a>
DLNA v1.5 Server	The DLNA (Digital Living Network Alliance) group of companies works to make products compatible and able to work in a home network in order to make digital living easy and seamless. DLNA clients play files stored on DLNA servers.
ECMA-262	The original ECMAScript standard, also known as JavaScript.
ECMA-262 Edition 2	The ECMAScript standard's second revision; also ISO standard 16262.
ECMA-262 Edition 3	The ECMAScript standard's third revision; corresponds to JavaScript 1.5.
ECMA-357	ECMAScript for XML (E4X). See also the E4X errata.
HTML 3.2 Reference Specification	The HyperText Markup Language (HTML).
HTML 4.01 Specification	Defines the HyperText Markup Language (HTML), the publishing language of the World Wide Web.
ISO 3166-1	Country names (official short names in English) in alphabetical order as given in ISO 3166-1 and the corresponding ISO 3166-1-alpha-2 code elements.
ISO 639-2	Two-letter and three-letter language code sets.

**Table 115** Supported Standards and Recommendations

MIMETYPES	IANA registered content types (MIME types). See the IANA web site ( <a href="ftp://ftp.isi.edu/in-notes/iana/assignments/media-types/">ftp://ftp.isi.edu/in-notes/iana/assignments/media-types/</a> ).
ISO 15740	Picture Transfer Protocol (PTP) from the International imaging Industry Association allows you to transfer pictures from digital cameras or other devices without needing additional device drivers.
RFC 1001	(STD-19) - Protocol standard for NetBIOS service on a TCP/UDP transport: Concepts and methods
RFC 1002	(STD-19) - Protocol standard for NetBIOS service on a TCP/UDP transport: Detailed specifications
RFC 1034	(STD-13) - Domain names - concepts and facilities
RFC 1035	(STD-13) - Domain names - implementation and specification
RFC 1305	Network Time Protocol (NTP version 3)
RFC 1415	FTP-FTAM Gateway Specification
RFC 1510	The Kerberos Network Authentication Service (V5)
RFC 1738	Uniform Resource Locators (URL)
RFC 1808	Relative Uniform Resource Locators
RFC 1945	The Hypertext Transfer Protocol (HTTP) 1.0.
RFC 2131	Dynamic Host Configuration Protocol
RFC 2396	Uniform Resource Identifier (URI)
RFC 2396	Uniform Resource Identifiers (URI): Generic Syntax
RFC 2616	Hypertext Transfer Protocol (HTTP) 1.1.
RFC 2854	History of HTML development, and lists the relevant W3C (World Wide Web Consortium) recommendations for the "text/html" MIME type.
RFC 3066, BCP 47 (Best Current Practice)	Language tags
RFC 3282	"Content-language:" headers.
RFC 3986	(STD-66) - Uniform Resource Identifier (URI): Generic Syntax
RFC 4120	The Kerberos Network Authentication Service (V5)
RFC 4248	The telnet URI Scheme
RFC 793	(STD-7) - Transmission Control Protocol
RFC 959	(STD-9) - File Transfer Protocol
SATA	SATA I and SATA II 3.0 Gbit/s (Serial Advanced Technology Attachment) compatible hard drives.
UPnP	Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices.
USB 2.0	USB (Universal Serial Bus) version 2.0 allows for interfacing devices with data transfers rates of up to 480 Mbps.
XHTML 1.0	Extensible HyperText Markup Language (Second Edition)
XHTML 1.1	Module-based XHTML

## 18.4 Supported Media Server Content Formats

The following describes the details about the files that the NSA media server can publish.

**Table 116** Supported Media Server Content Formats

CATEGORY	FILE TYPE	EXTENSION
Video	MPEG-1/MPEG-2	dat, dvr-ms, iso, m1v, m2p, m2t, m2v, mp2, mpe, mpeg, mpeg2, mpg, mpg2, ts, vob, m2ts, tts
	MPEG-4	m4v, mp4
	AVI	avi
	DivX	divx , avi
	Motion JPEG	mjpeg, mjpg
	Quick Time Video	mov
	RealMedia	rmvb, rm
	Ogg	ogm
	Matroska	mkv
	ASF	asf
	Windows Media Video	asf, wmv
	Subtitle	srt, ssa, idx, sub

**Table 116** Supported Media Server Content Formats

CATEGORY	FILE TYPE	EXTENSION
Music	MP3	mp3, mpa
	Ogg Vorbis	ogg
	RealMedia	ra, ram
	WAVE	wav
	Windows Media Audio	wma
	Matroska	mka
	Monkeys Audio	ape
	MP1	mp1
	MP4	mp4, m4a, m4p
	PCM	pcm
	LPCM	lpcm
	DTS	dts
	AC3	ac3
	Free Lossless Audio Codec	flac
	Au	au
	AAC	aac
	3GPP	3gp, 3g2
	AIFF	aif, aiff
	Playlist	wpl, pls, m3u
Photo	Bitmap	bmp
	JPEG	jpe, jpeg, jpg
	PNG	png

Note: Not all published file types can be viewed by all client applications.

## 18.5 Supported iTunes Server Content Formats

At the time of writing, the NSA's supports iTunes 7.4.1.2, publishing AAC (MPEG-4), MP3, AIFF, WAV, and Apple Lossless files.

## 18.6 Power Consumption

The NSA was tested using the specified power sources with the external power adapter and with two hard drives installed.

Note: This table is a laboratory test of NSA power consumption for your reference only.

**Table 117** Full loading Power consumption in Watts(W)\*

POWER SOURCE	SYSTEM READ/ WRITE
240V/50Hz	26.4W (max)
100V/60Hz	25.2W (max)

\*Full loading test condition: 1.5 TB internal hard drive with 2 x USB storage and 1 x eSATA storage.

---

# PART VI

## Appendices and Index

---

Setting up Your Computer's IP Address  
(373)

Pop-up Windows, JavaScripts and Java  
Permissions (389)

Common Services (399)

Importing Certificates (403)

Open Source Licences (435)

Legal Information (473)

Index (477)





# Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

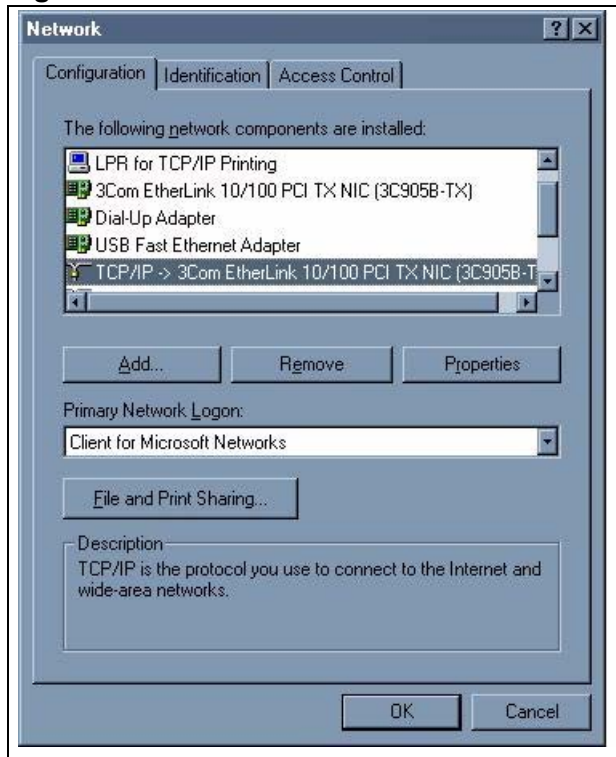
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

## Windows 95/98/Me

Click **Start, Settings, Control Panel** and double-click the **Network** icon to open the **Network** window.

**Figure 166** WIndows 95/98/Me: Network: Configuration



### Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.

- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

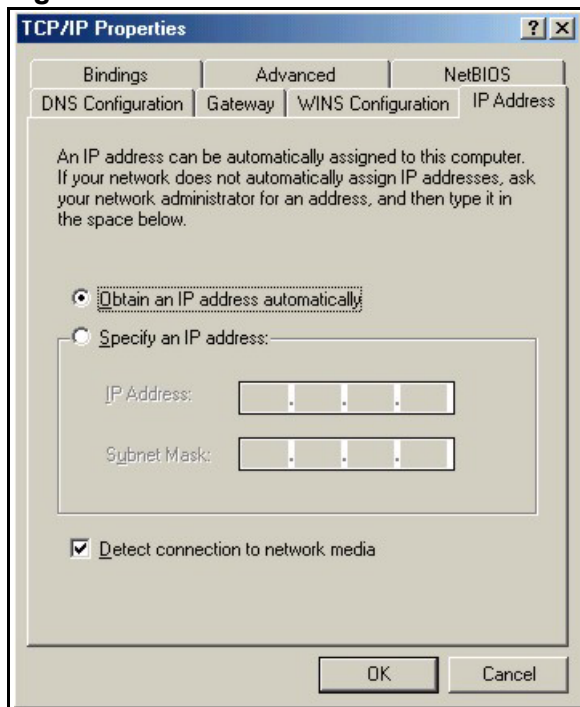
If you need Client for Microsoft Networks:

- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.
- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

## Configuring

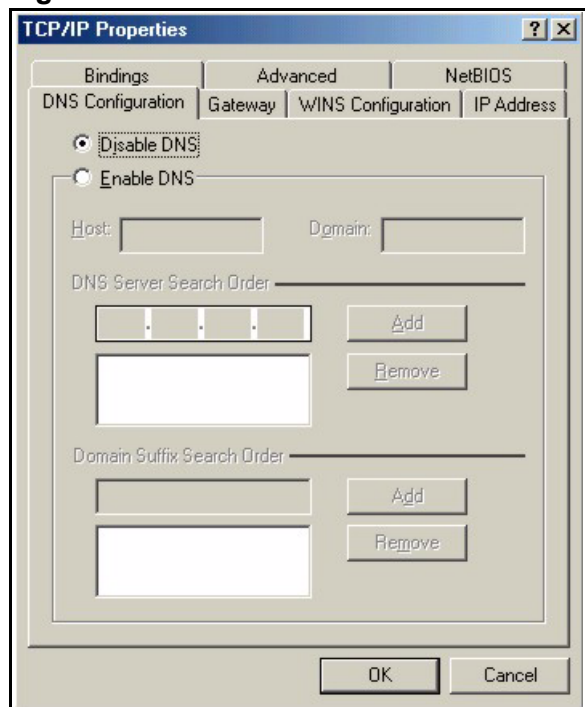
- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 Click the **IP Address** tab.
  - If your IP address is dynamic, select **Obtain an IP address automatically**.
  - If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

**Figure 167** Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 Click the **DNS** Configuration tab.
  - If you do not know your DNS information, select **Disable DNS**.
  - If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

**Figure 168** Windows 95/98/Me: TCP/IP Properties: DNS Configuration



- 4 Click the **Gateway** tab.
  - If you do not know your gateway's IP address, remove previously installed gateways.
  - If you have a gateway IP address, type it in the **New gateway field** and click **Add**.
- 5 Click **OK** to save and close the **TCP/IP Properties** window.
- 6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.
- 7 Restart your computer when prompted.

## Verifying Settings

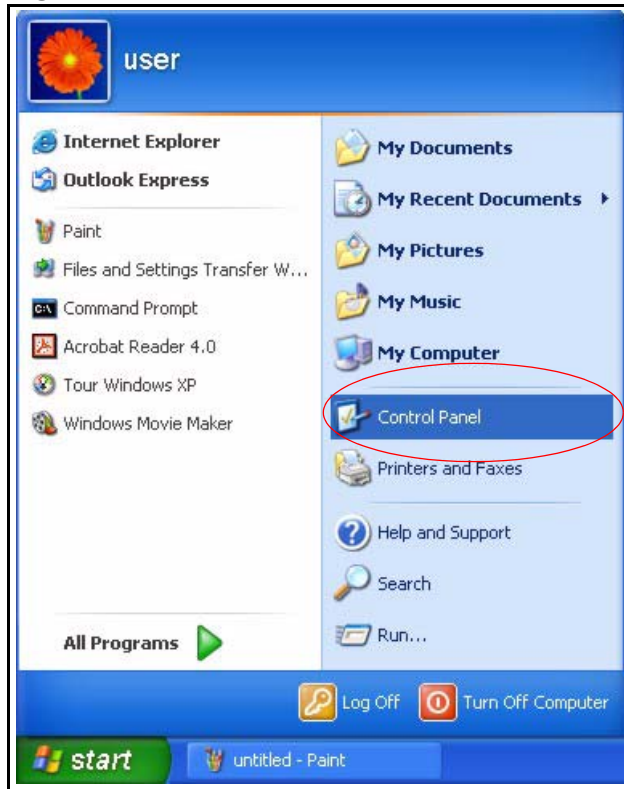
- 1 Click **Start** and then **Run**.
- 2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
- 3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

## Windows 2000/NT/XP

The following example figures use the default Windows XP GUI theme.

- 1 Click **start** (**Start** in Windows 2000/NT), **Settings**, **Control Panel**.

**Figure 169** Windows XP: Start Menu



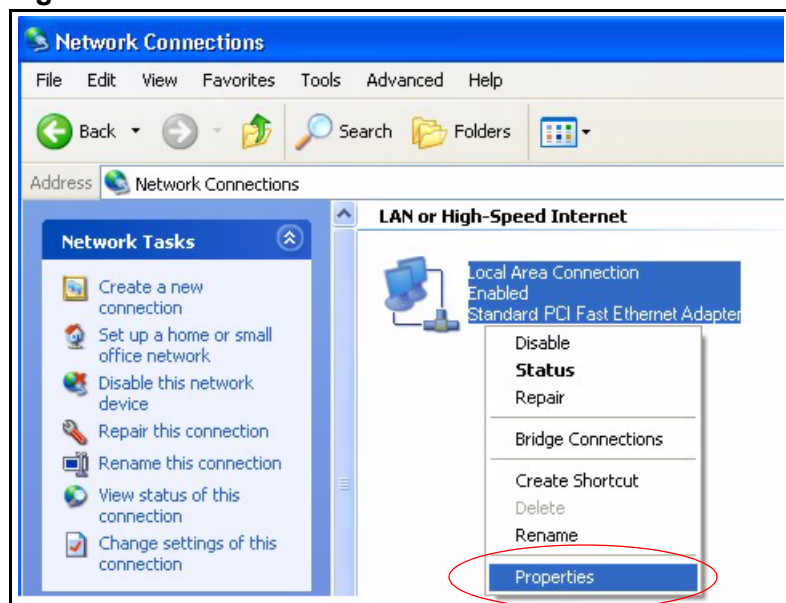
- 2 In the **Control Panel**, double-click **Network Connections** (**Network and Dial-up Connections** in Windows 2000/NT).

**Figure 170** Windows XP: Control Panel



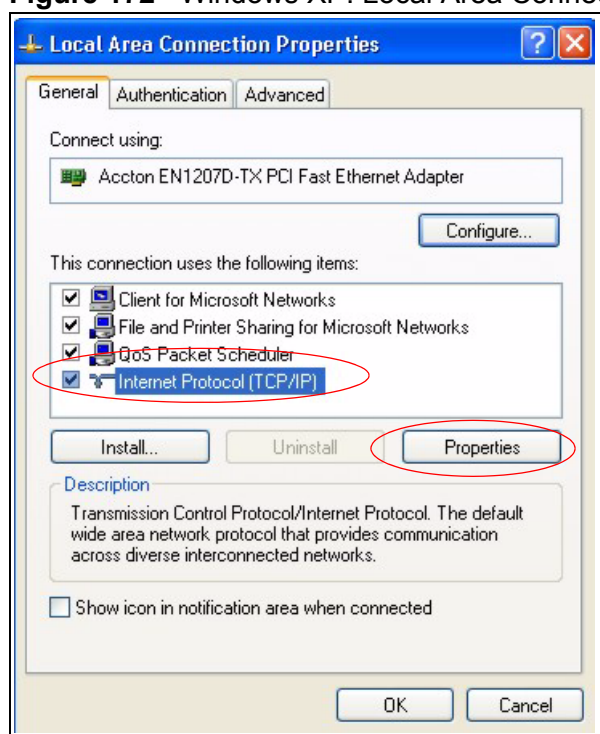
- 3 Right-click **Local Area Connection** and then click **Properties**.

**Figure 171** Windows XP: Control Panel: Network Connections: Properties



- 4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and then click **Properties**.

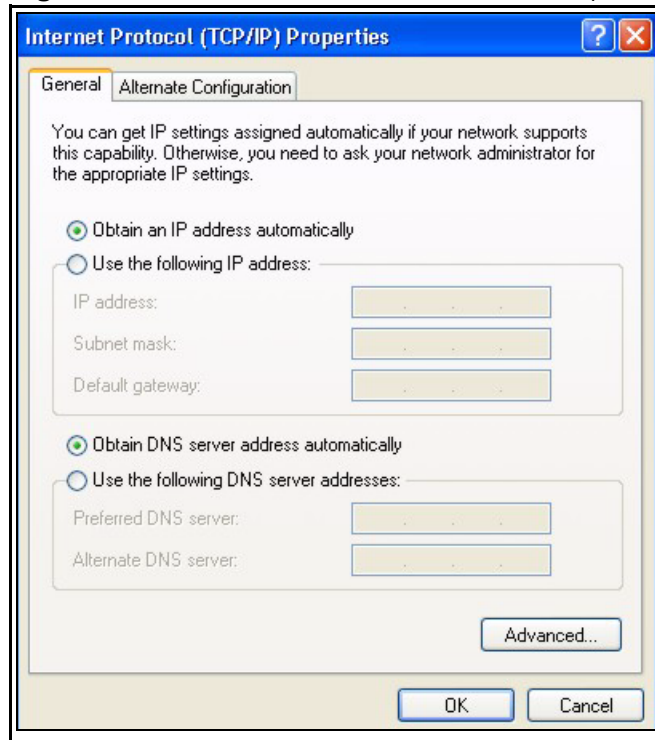
**Figure 172** Windows XP: Local Area Connection Properties



- 5 The **Internet Protocol TCP/IP Properties** window opens (the **General** tab in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.
- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.
- Click **Advanced**.

**Figure 173** Windows XP: Internet Protocol (TCP/IP) Properties



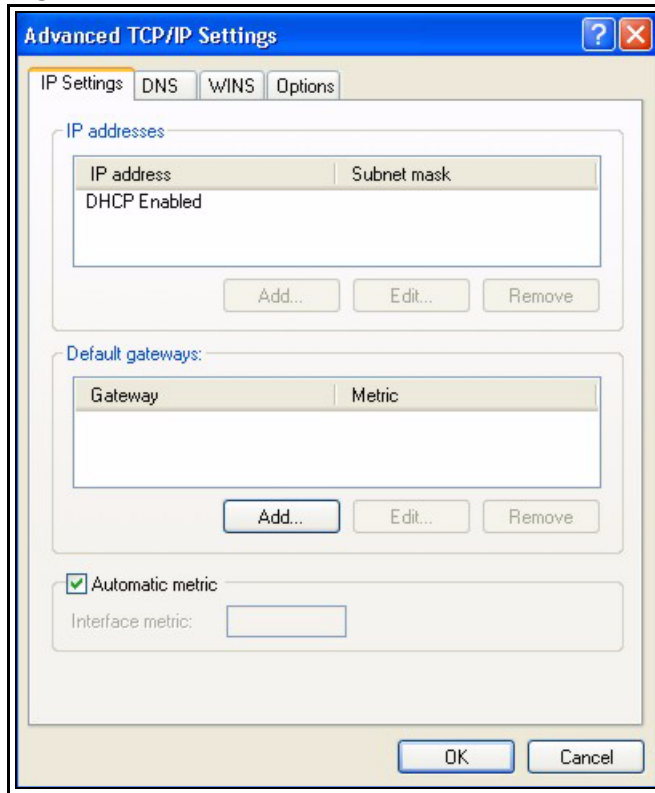
- 6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settings** tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.

- Click **OK** when finished.

**Figure 174** Windows XP: Advanced TCP/IP Properties

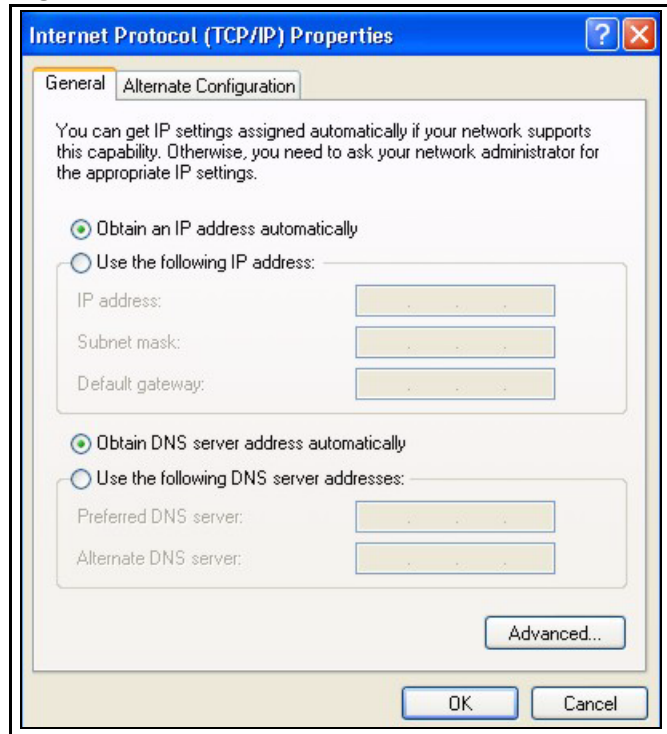


- 7 In the **Internet Protocol TCP/IP Properties** window (the **General** tab in Windows XP):
- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
  - If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.



If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

**Figure 175** Windows XP: Internet Protocol (TCP/IP) Properties



- 8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.
- 9 Click **Close (OK** in Windows 2000/NT) to close the **Local Area Connection Properties** window.
- 10 Close the **Network Connections** window (**Network and Dial-up Connections** in Windows 2000/NT).
- 11 Restart your computer (if prompted).

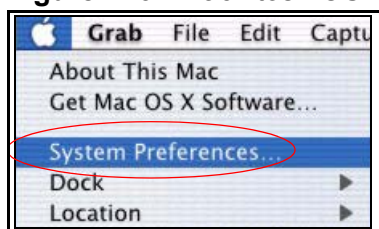
## Verifying Settings

- 1 Click **Start, All Programs, Accessories** and then **Command Prompt**.
- 2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

## Macintosh OS X

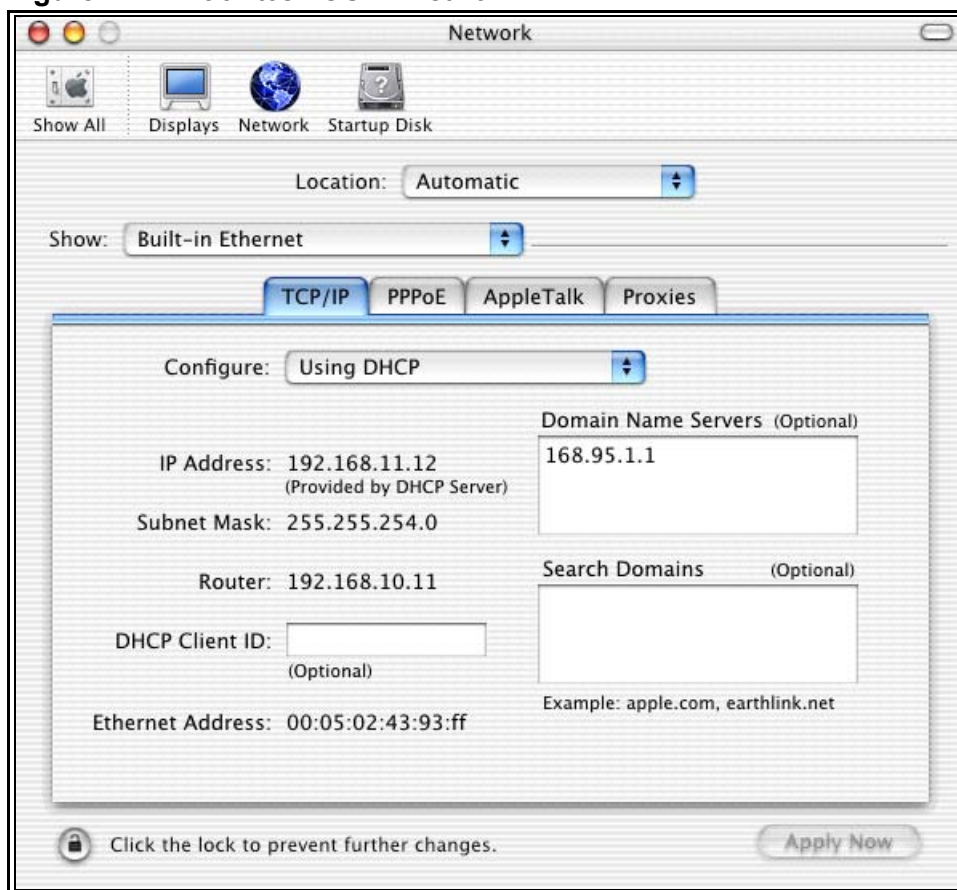
- 1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

**Figure 176** Macintosh OS X: Apple Menu



- 2 Click **Network** in the icon bar.
  - Select **Automatic** from the **Location** list.
  - Select **Built-in Ethernet** from the **Show** list.
  - Click the **TCP/IP** tab.
- 3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

**Figure 177** Macintosh OS X: Network



- 4 For statically assigned settings, do the following:
  - From the **Configure** box, select **Manually**.
  - Type your IP address in the **IP Address** box.
  - Type your subnet mask in the **Subnet mask** box.
  - Type the IP address of your gateway in the **Router address** box.
- 5 Click **Apply Now** and close the window.
- 6 Restart your computer (if prompted).

## Verifying Settings

Check your TCP/IP properties in the **Network** window.

## Linux

This section shows you how to configure your computer's TCP/IP settings in Red Hat Linux 9.0. Procedure, screens and file location may vary depending on your Linux distribution and release version.

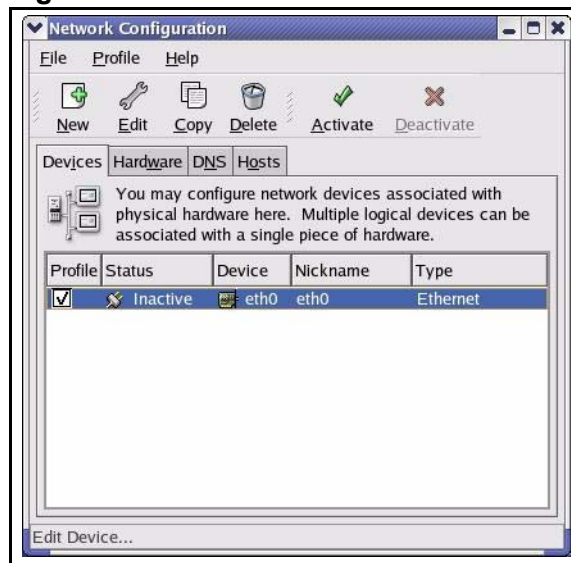
Note: Make sure you are logged in as the root administrator.

## Using the K Desktop Environment (KDE)

Follow the steps below to configure your computer IP address using the KDE.

- 1 Click the Red Hat button (located on the bottom left corner), select **System Setting** and click **Network**.

**Figure 178** Red Hat 9.0: KDE: Network Configuration: Devices



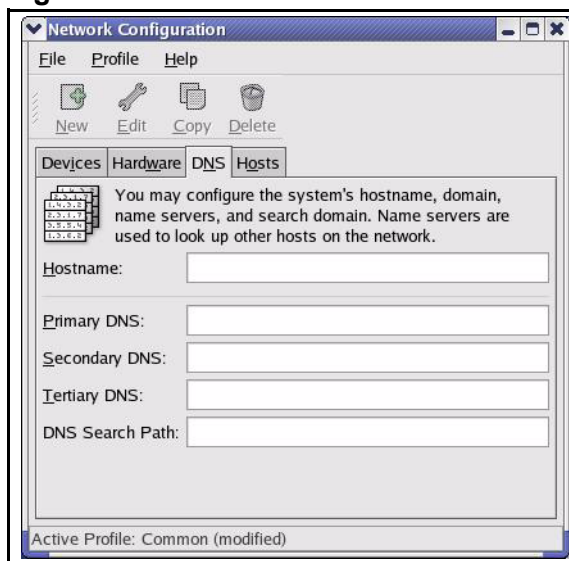
- 2 Double-click on the profile of the network card you wish to configure. The **Ethernet Device General** screen displays as shown.

**Figure 179** Red Hat 9.0: KDE: Ethernet Device: General



- If you have a dynamic IP address, click **Automatically obtain IP address settings with** and select **dhcp** from the drop down list.
  - If you have a static IP address, click **Statically set IP Addresses** and fill in the **Address**, **Subnet mask**, and **Default Gateway Address** fields.
- 3 Click **OK** to save the changes and close the **Ethernet Device General** screen.
  - 4 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Configuration** screen. Enter the DNS server information in the fields provided.

**Figure 180** Red Hat 9.0: KDE: Network Configuration: DNS



- 5 Click the **Devices** tab.
- 6 Click the **Activate** button to apply the changes. The following screen displays. Click **Yes to save the changes in all screens**.

**Figure 181** Red Hat 9.0: KDE: Network Configuration: Activate



- 7 After the network card restart process is complete, make sure the **Status** is **Active** in the **Network Configuration** screen.

## Using Configuration Files

Follow the steps below to edit the network configuration files and set your computer IP address.

- 1 Assuming that you have only one network card on the computer, locate the `ifconfig-eth0` configuration file (where `eth0` is the name of the Ethernet card). Open the configuration file with any plain text editor.
  - If you have a dynamic IP address, enter `dhcp` in the `BOOTPROTO=` field. The following figure shows an example.

**Figure 182** Red Hat 9.0: Dynamic IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- If you have a static IP address, enter **static** in the `BOOTPROTO=` field. Type `IPADDR=` followed by the IP address (in dotted decimal notation) and type `NETMASK=` followed by the subnet mask. The following example shows an example where the static IP address is 192.168.1.10 and the subnet mask is 255.255.255.0.

**Figure 183** Red Hat 9.0: Static IP Address Setting in `ifconfig-eth0`

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.10
NETMASK=255.255.255.0
USERCTL=no
PEERDNS=yes
TYPE=Ethernet
```

- 2 If you know your DNS server IP address(es), enter the DNS server information in the `resolv.conf` file in the `/etc` directory. The following figure shows an example where two DNS server IP addresses are specified.

**Figure 184** Red Hat 9.0: DNS Settings in `resolv.conf`

```
nameserver 172.23.5.1
nameserver 172.23.5.2
```

- 3 After you edit and save the configuration files, you must restart the network card. Enter `./network restart` in the `/etc/rc.d/init.d` directory. The following figure shows an example.

**Figure 185** Red Hat 9.0: Restart Ethernet Card

```
[root@localhost init.d]# network restart

Shutting down interface eth0:           [OK]
Shutting down loopback interface:       [OK]
Setting network parameters:             [OK]
Bringing up loopback interface:         [OK]
Bringing up interface eth0:             [OK]
```

## Verifying Settings

Enter `ifconfig` in a terminal screen to check your TCP/IP properties.

**Figure 186** Red Hat 9.0: Checking TCP/IP Properties

```
[root@localhost]# ifconfig
eth0      Link encap:Ethernet HWaddr 00:50:BA:72:5B:44
          inet addr:172.23.19.129 Bcast:172.23.19.255 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:730412 (713.2 Kb) TX bytes:1570 (1.5 Kb)
          Interrupt:10 Base address:0x1000
[root@localhost]#
```





# Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

## Internet Explorer Pop-up Blockers

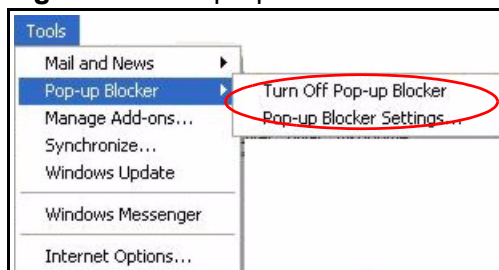
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

### Disable Pop-up Blockers

- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

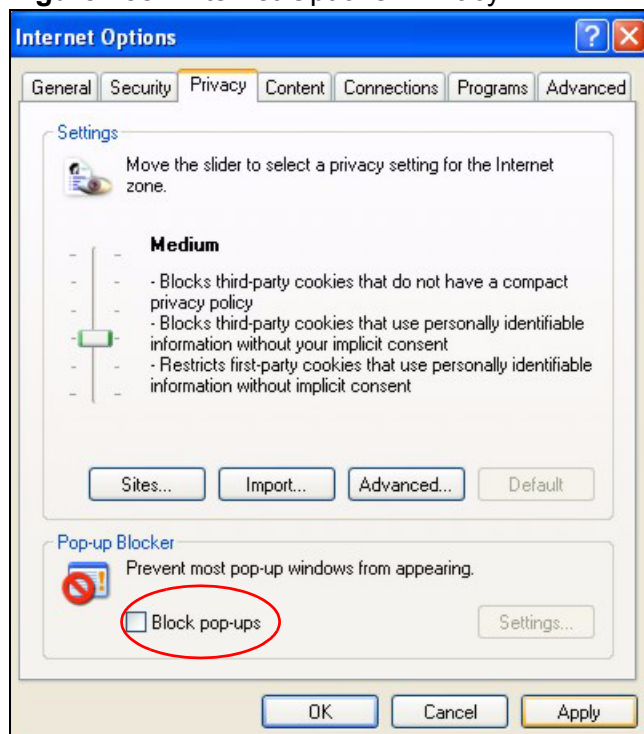
**Figure 187** Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

**Figure 188** Internet Options: Privacy



- 3 Click **Apply** to save this setting.

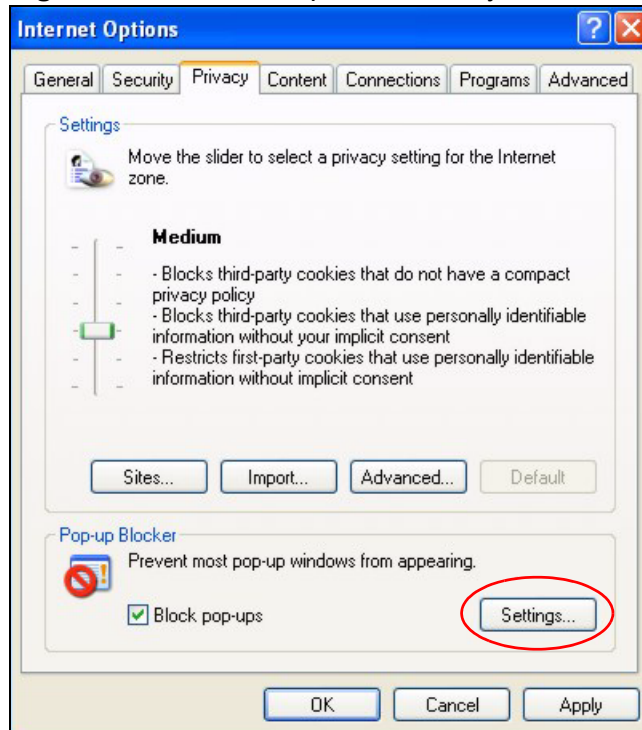
## Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

- 1 In Internet Explorer, select **Tools, Internet Options** and then the **Privacy** tab.

- 2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

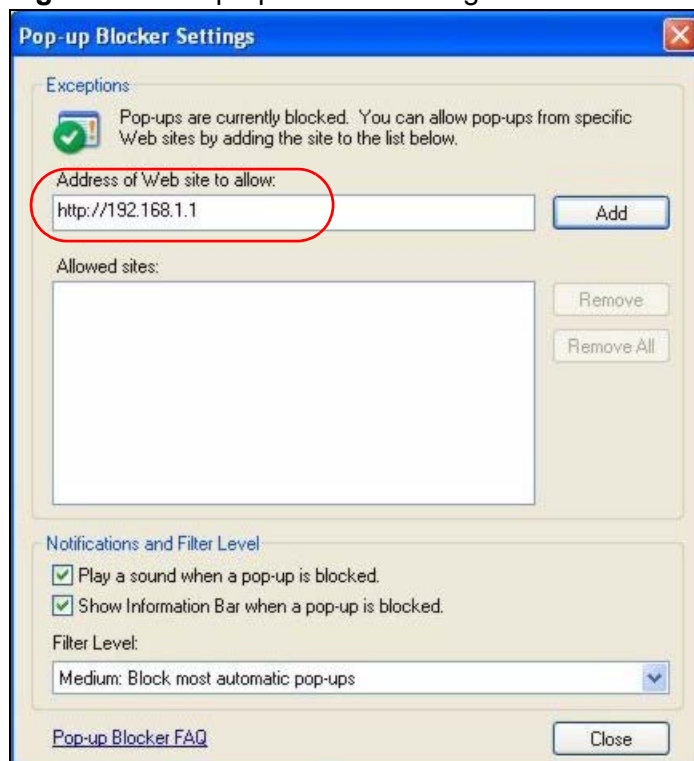
**Figure 189** Internet Options: Privacy



- 3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

- Click **Add** to move the IP address to the list of **Allowed sites**.

**Figure 190** Pop-up Blocker Settings



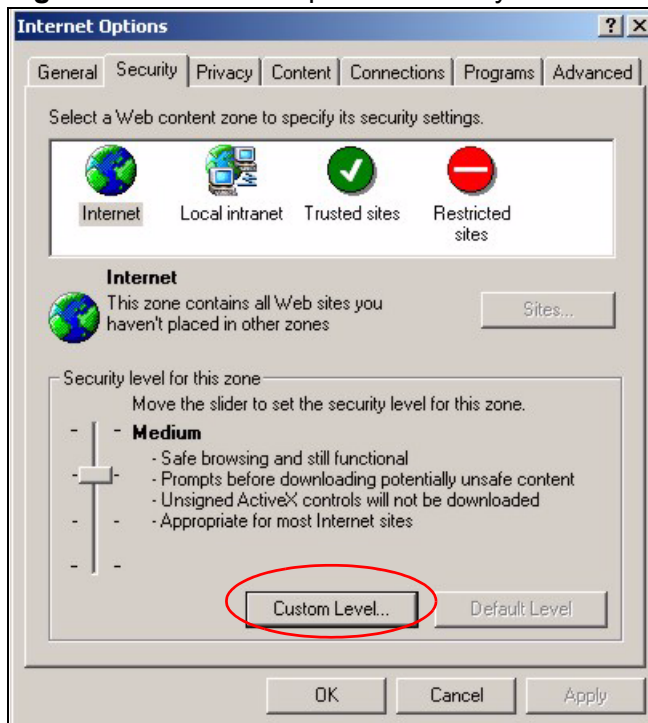
- Click **Close** to return to the **Privacy** screen.
- Click **Apply** to save this setting.

## JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

- 1 In Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.

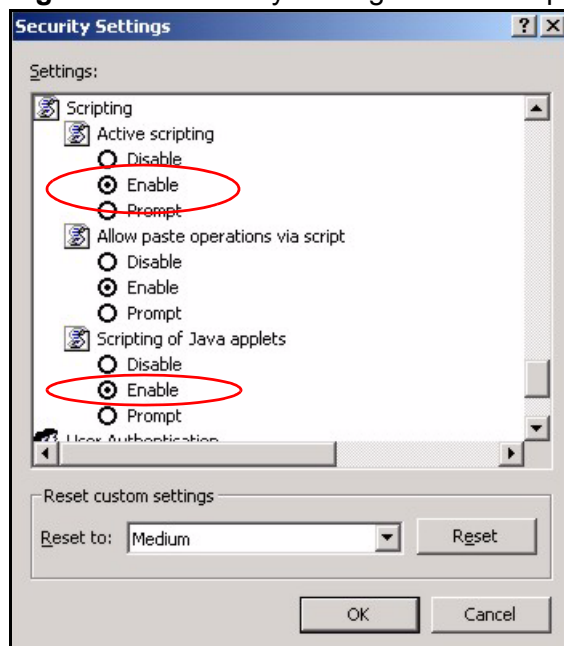
**Figure 191** Internet Options: Security



- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

- 6 Click **OK** to close the window.

**Figure 192** Security Settings - Java Scripting

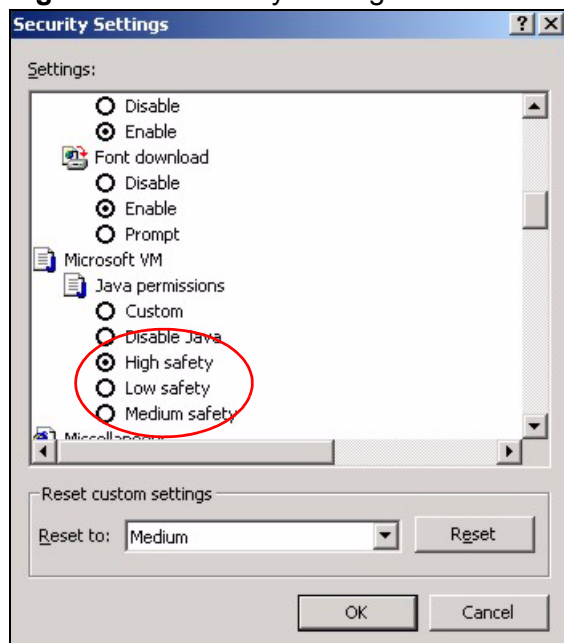


## Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.

- 5 Click **OK** to close the window.

**Figure 193** Security Settings - Java

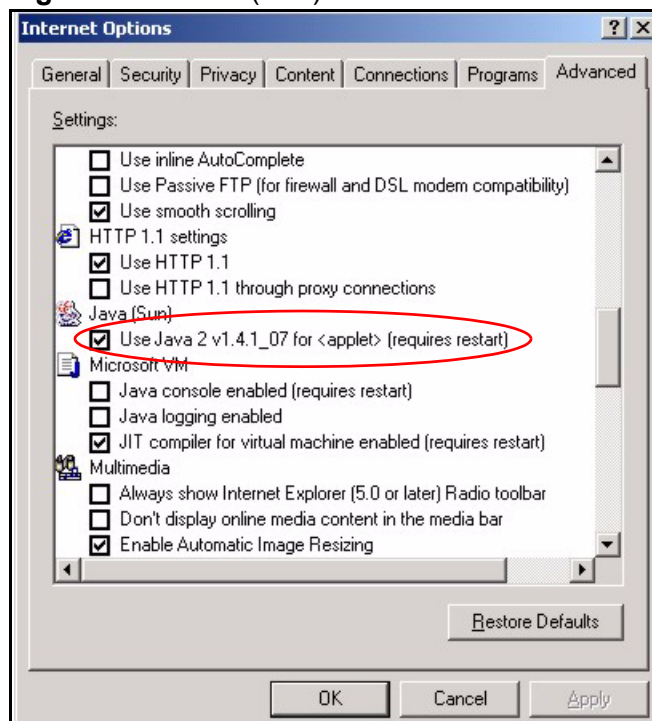


## JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options** and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

- 3 Click **OK** to close the window.

**Figure 194** Java (Sun)

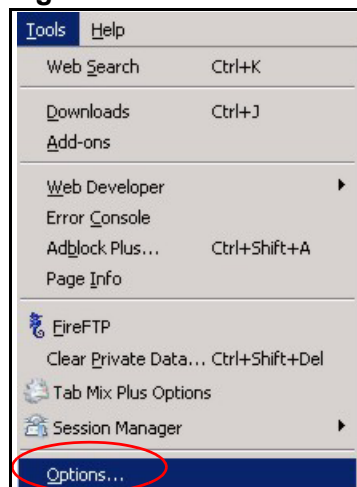


## Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

You can enable Java, Javascripts and pop-ups in one screen. Click **Tools**, then click **Options** in the screen that appears.

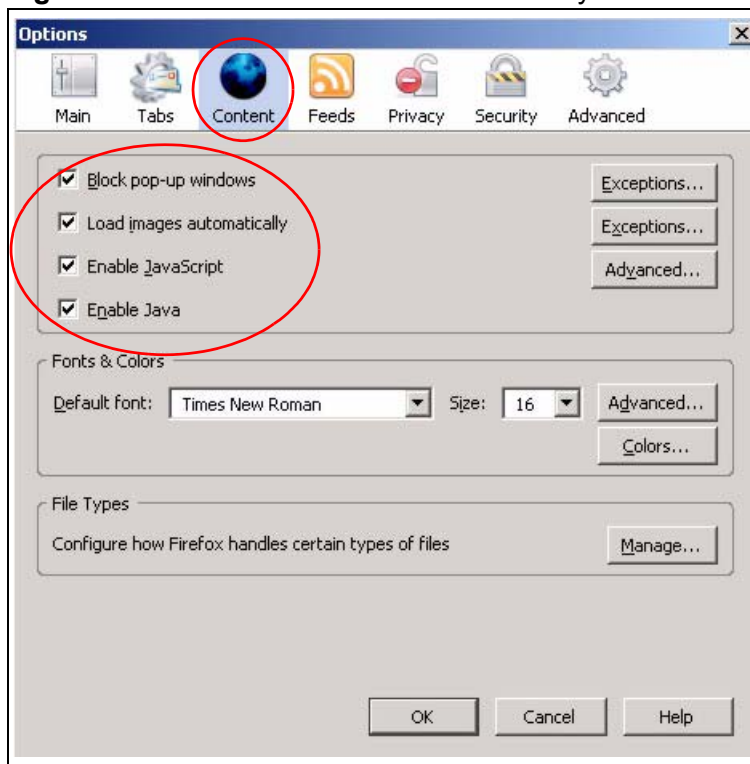
**Figure 195** Mozilla Firefox: Tools > Options





Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

**Figure 196** Mozilla Firefox Content Security





# Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

**Table 118** Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example <a href="http://www.zyxel.com">www.zyxel.com</a> ) to IP numbers.

**Table 118** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).

**Table 118** Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

**Table 118** Commonly Used Services (continued)


NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

# Importing Certificates

This appendix shows you how to import public key certificates into your web browser.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the site to be issued to all visiting web browsers to let them know that the site is legitimate.

Many ZyXEL products, such as the NSA-2401, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the ZyXEL-created certificate into your web browser and flag that certificate as a trusted authority.

Note: You can see if you are browsing on a secure website if the URL in your web browser's address bar begins with `https://` or there is a sealed padlock icon (  ) somewhere in the main browser window (not all browsers show the padlock in the same location.)

In this appendix, you can import a public key certificate for:

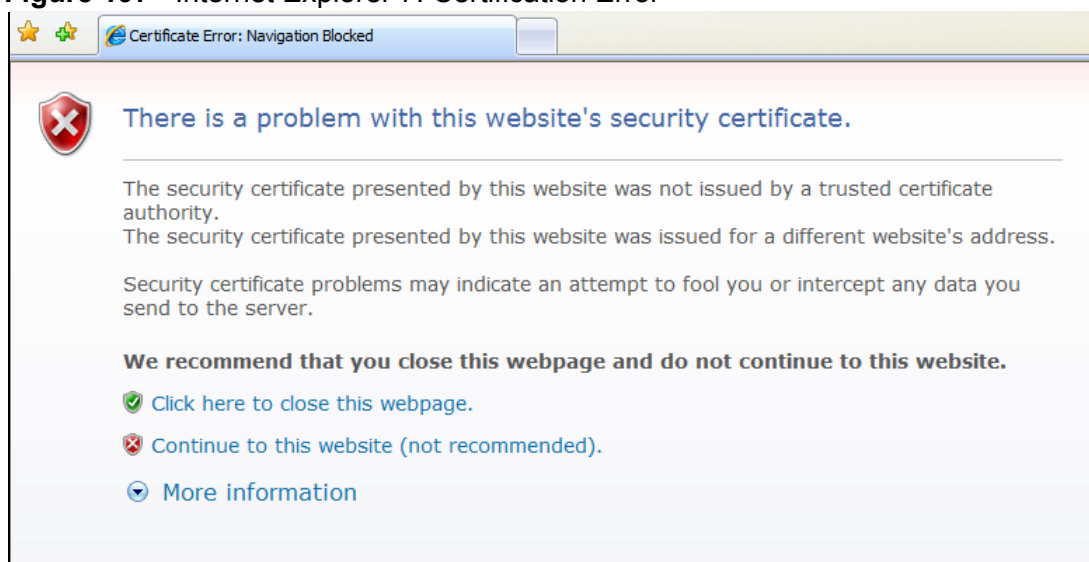
- Internet Explorer on [page 404](#)
- Firefox on [page 414](#)
- Opera on [page 420](#)
- Konqueror on [page 428](#)

## Internet Explorer

The following example uses Microsoft Internet Explorer 7 on Windows XP Professional; however, they can also apply to Internet Explorer on Windows Vista.

- 1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.

**Figure 197** Internet Explorer 7: Certification Error



- 2 Click **Continue to this website (not recommended)**.

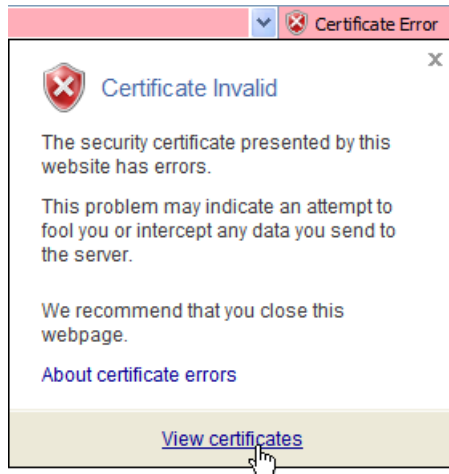
**Figure 198** Internet Explorer 7: Certification Error





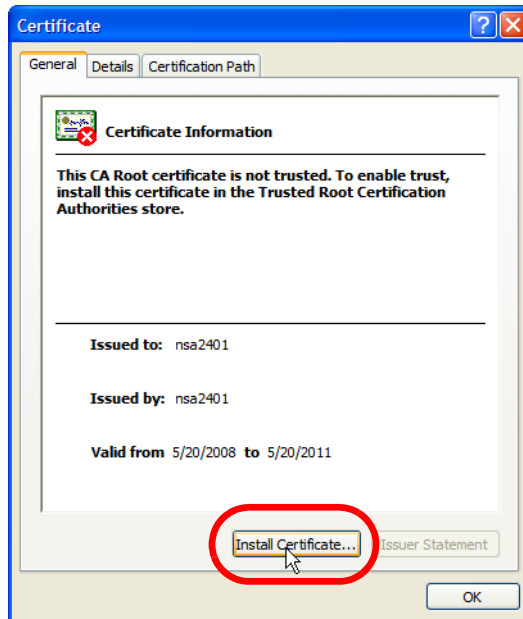
- 3 In the **Address Bar**, click **Certificate Error** > **View certificates**.

**Figure 199** Internet Explorer 7: Certificate Error



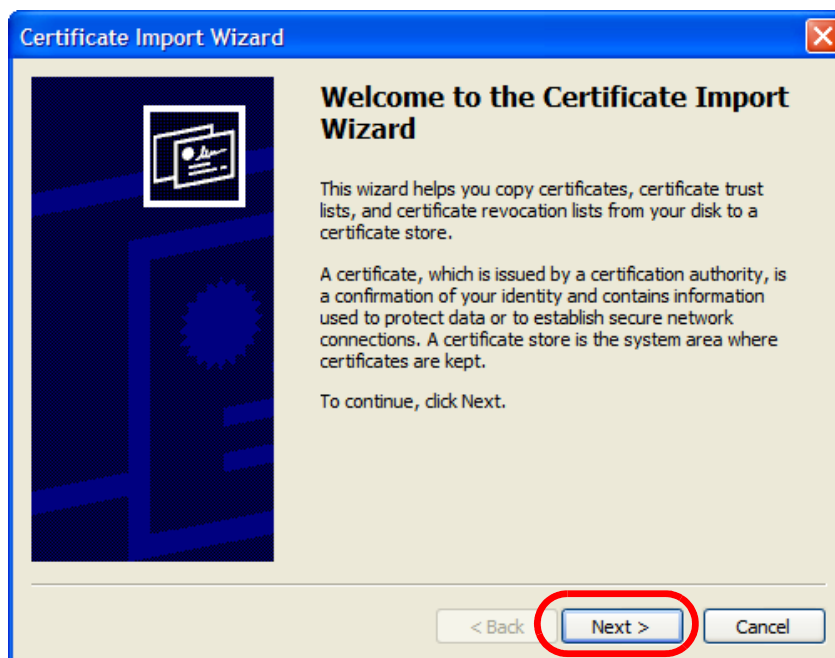
- 4 In the **Certificate** dialog box, click **Install Certificate**.

**Figure 200** Internet Explorer 7: Certificate



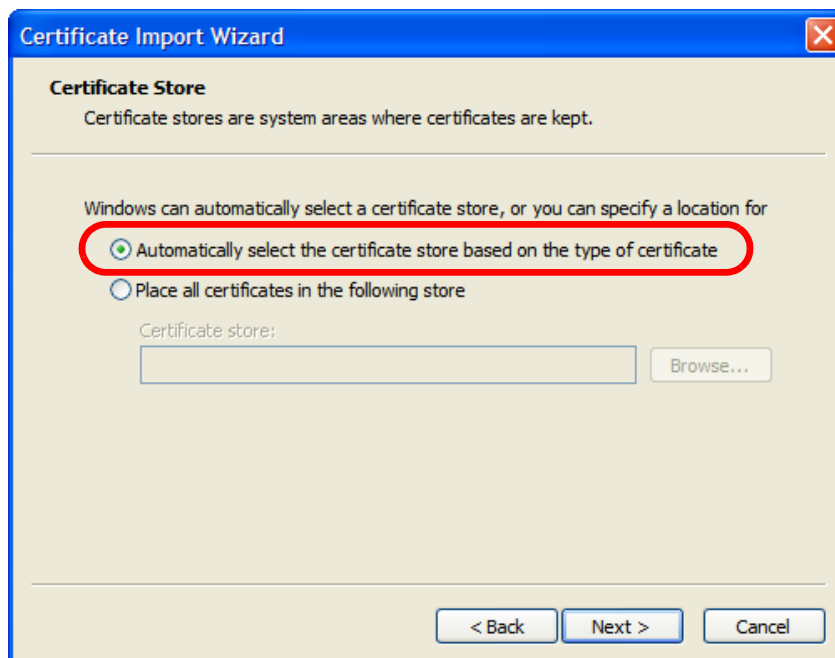
- 5 In the **Certificate Import Wizard**, click **Next**.

**Figure 201** Internet Explorer 7: Certificate Import Wizard



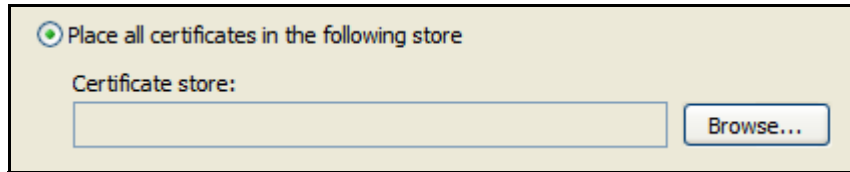
- 6 If you want Internet Explorer to **Automatically select certificate store based on the type of certificate**, click **Next** again and then go to step 9.

**Figure 202** Internet Explorer 7: Certificate Import Wizard



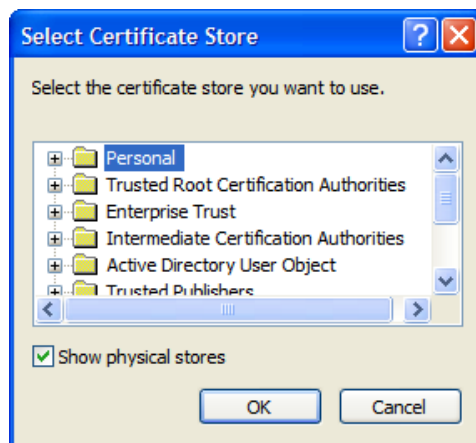
- 7 Otherwise, select **Place all certificates in the following store** and then click **Browse**.

**Figure 203** Internet Explorer 7: Certificate Import Wizard



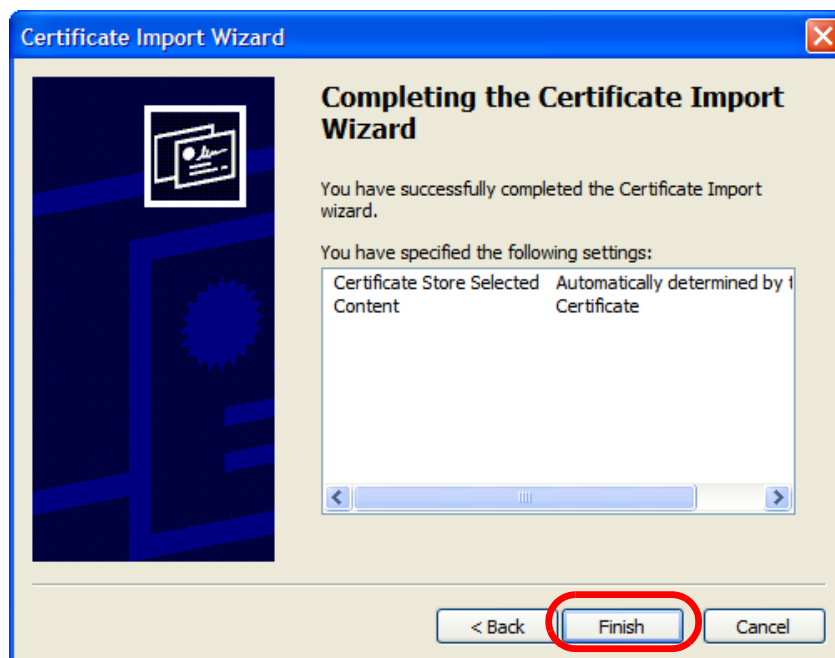
- 8 In the **Select Certificate Store** dialog box, choose a location in which to save the certificate and then click **OK**.

**Figure 204** Internet Explorer 7: Select Certificate Store



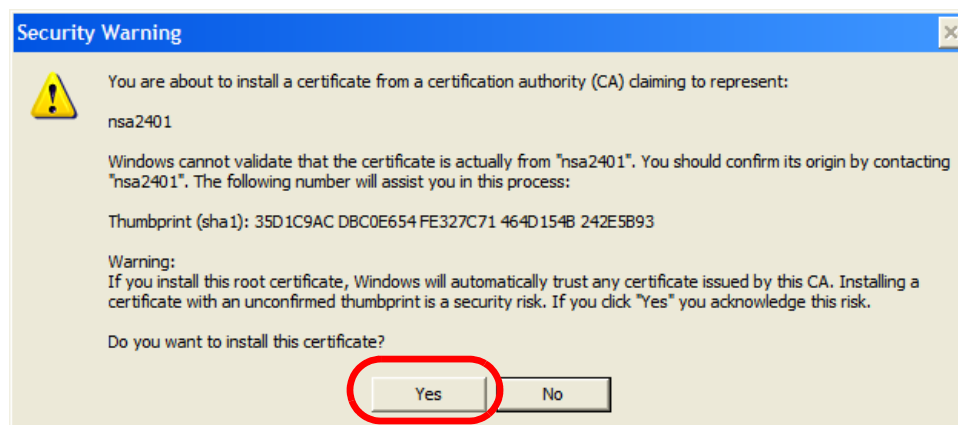
- 9 In the **Completing the Certificate Import Wizard** screen, click **Finish**.

**Figure 205** Internet Explorer 7: Certificate Import Wizard



- 10 If you are presented with another **Security Warning**, click **Yes**.

**Figure 206** Internet Explorer 7: Security Warning



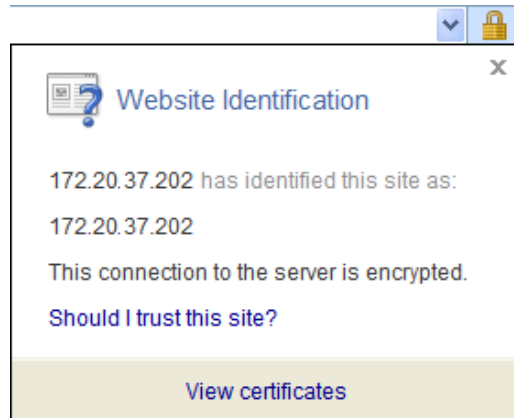
- 11 Finally, click **OK** when presented with the successful certificate installation message.

**Figure 207** Internet Explorer 7: Certificate Import Wizard



- 12 The next time you start Internet Explorer and go to a ZyXEL Web Configurator page, a sealed padlock icon appears in the address bar. Click it to view the page's **Website Identification** information.

**Figure 208** Internet Explorer 7: Website Identification



## Installing a Stand-Alone Certificate File in Internet Explorer

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

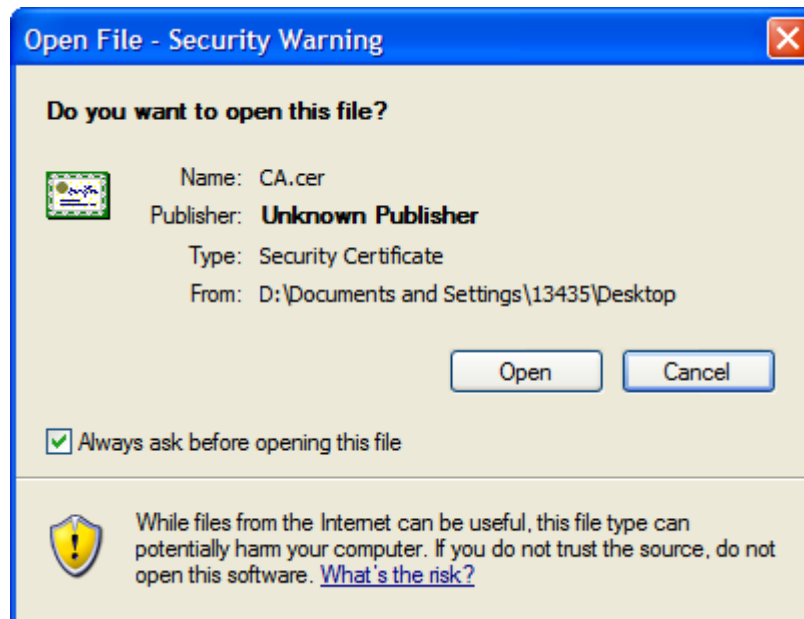
- 1 Double-click the public key certificate file.

**Figure 209** Internet Explorer 7: Public Key Certificate File



- 2 In the security warning dialog box, click **Open**.

**Figure 210** Internet Explorer 7: Open File - Security Warning



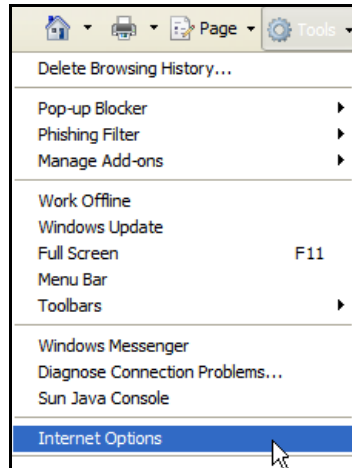
- 3 Refer to steps 4-12 in the Internet Explorer procedure beginning on [page 404](#) to complete the installation process.

## Removing a Certificate in Internet Explorer

This section shows you how to remove a public key certificate in Internet Explorer 7.

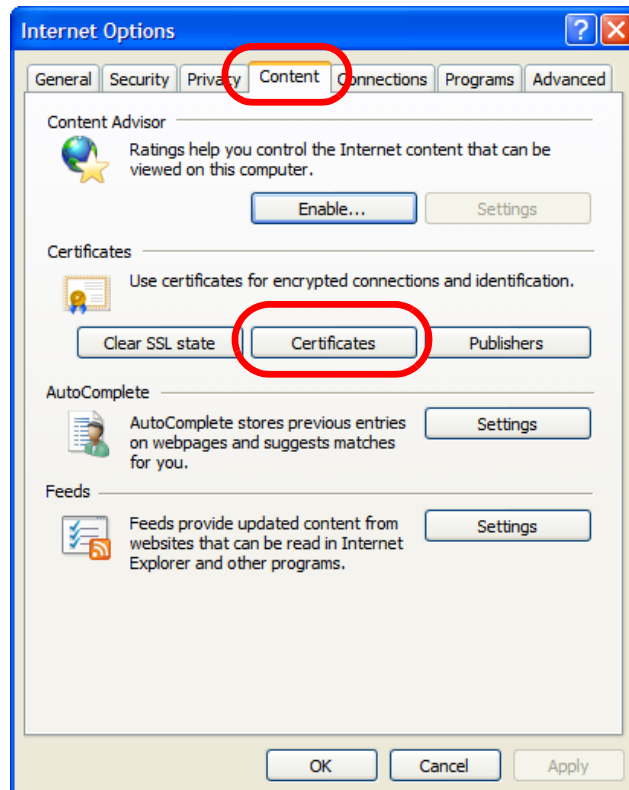
- 1 Open **Internet Explorer** and click **Tools > Internet Options**.

**Figure 211** Internet Explorer 7: Tools Menu



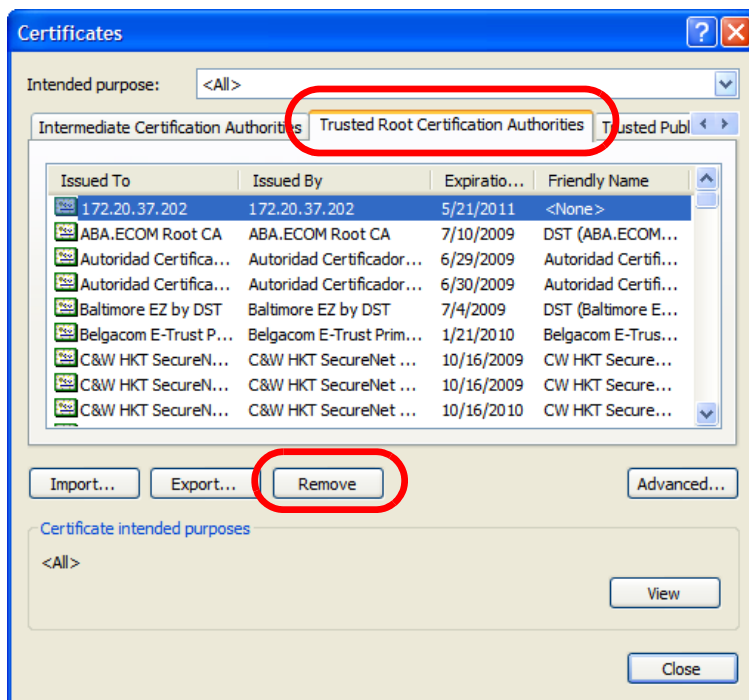
- 2 In the **Internet Options** dialog box, click **Content > Certificates**.

**Figure 212** Internet Explorer 7: Internet Options



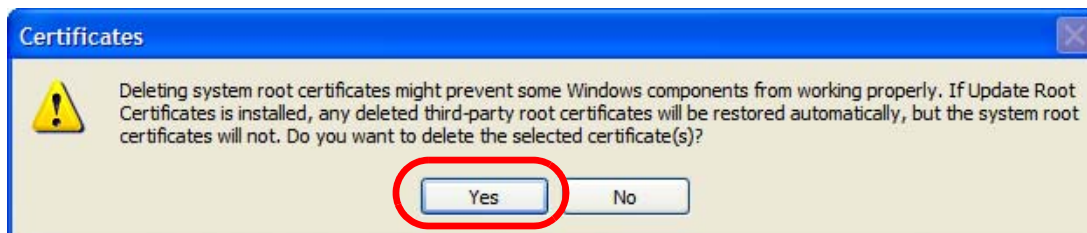
- 3 In the **Certificates** dialog box, click the **Trusted Root Certificates Authorities** tab, select the certificate that you want to delete, and then click **Remove**.

**Figure 213** Internet Explorer 7: Certificates



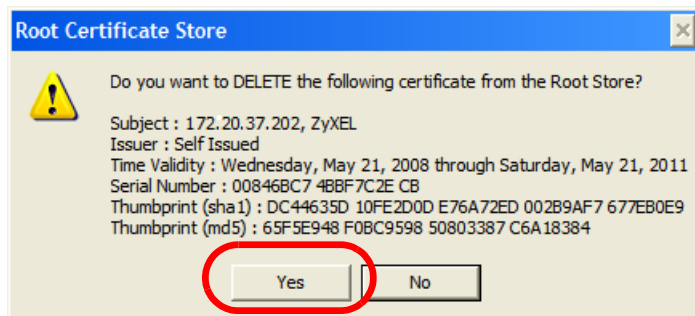
- 4 In the **Certificates** confirmation, click **Yes**.

**Figure 214** Internet Explorer 7: Certificates



- 5 In the **Root Certificate Store** dialog box, click **Yes**.

**Figure 215** Internet Explorer 7: Root Certificate Store





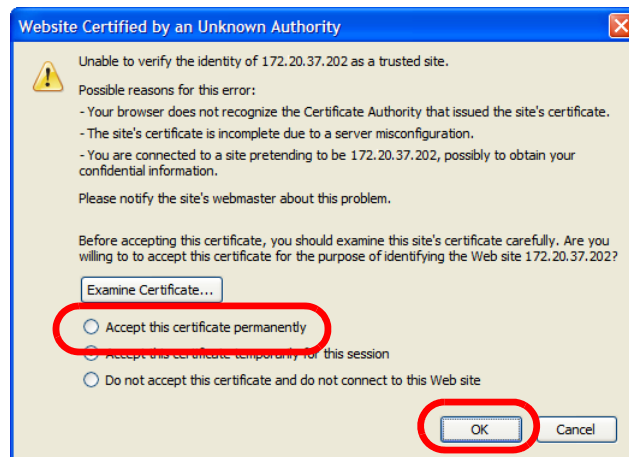
- 6 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

## Firefox

The following example uses Mozilla Firefox 2 on Windows XP Professional; however, the screens can also apply to Firefox 2 on all platforms.

- 1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
- 2 Select **Accept this certificate permanently** and click **OK**.

**Figure 216** Firefox 2: Website Certified by an Unknown Authority



- 3 The certificate is stored and you can now connect securely to the Web Configurator. A sealed padlock appears in the address bar, which you can click to open the **Page Info > Security** window to view the web page's security information.

**Figure 217** Firefox 2: Page Info

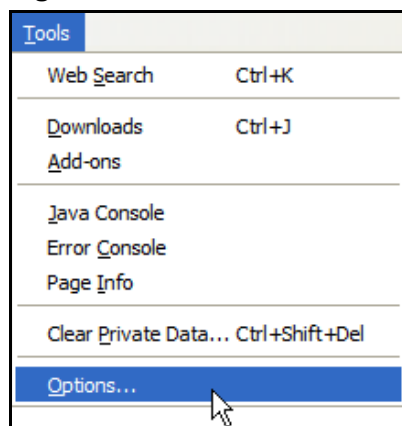


## Installing a Stand-Alone Certificate File in Firefox

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

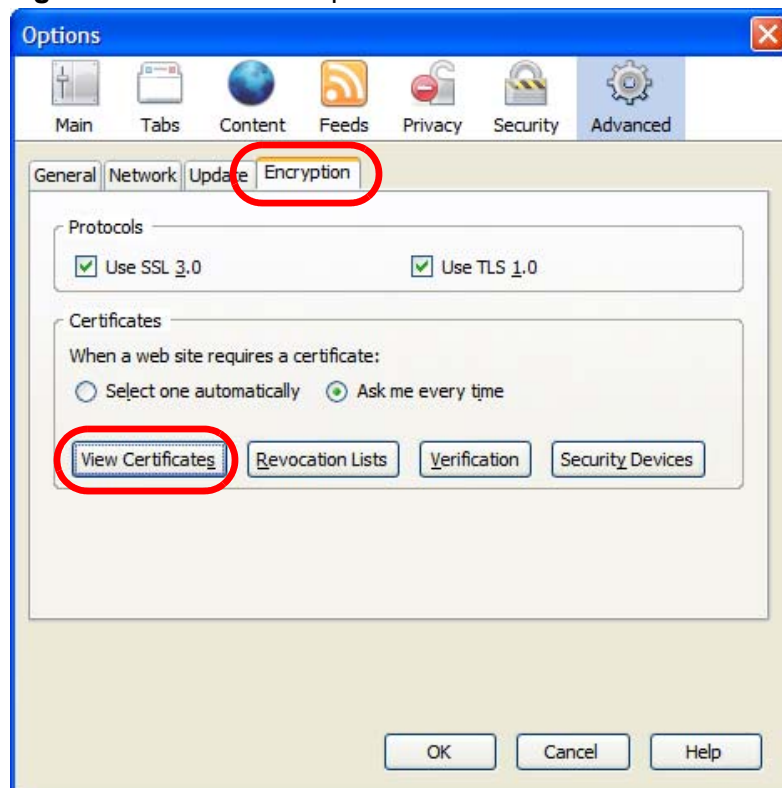
- 1 Open **Firefox** and click **Tools > Options**.

**Figure 218** Firefox 2: Tools Menu



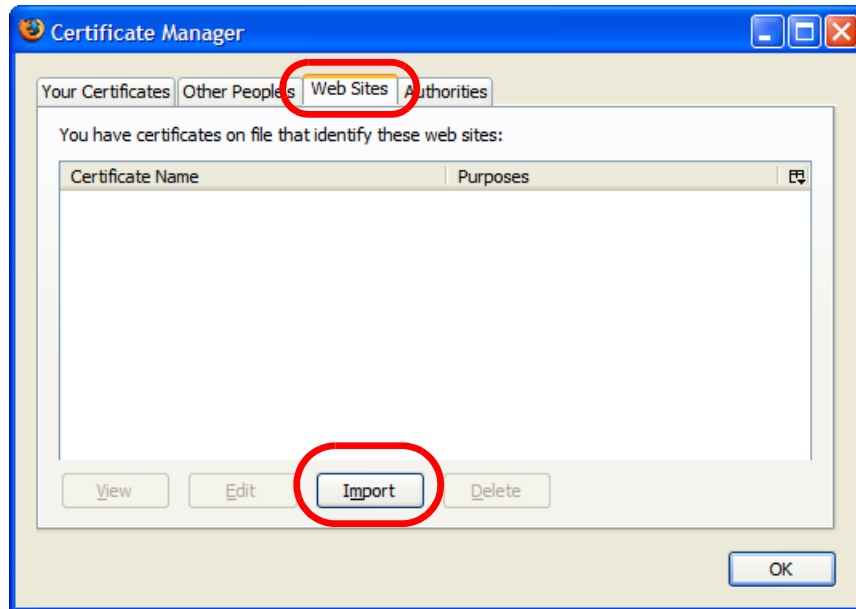
- 2 In the **Options** dialog box, click **Advanced > Encryption > View Certificates**.

**Figure 219** Firefox 2: Options



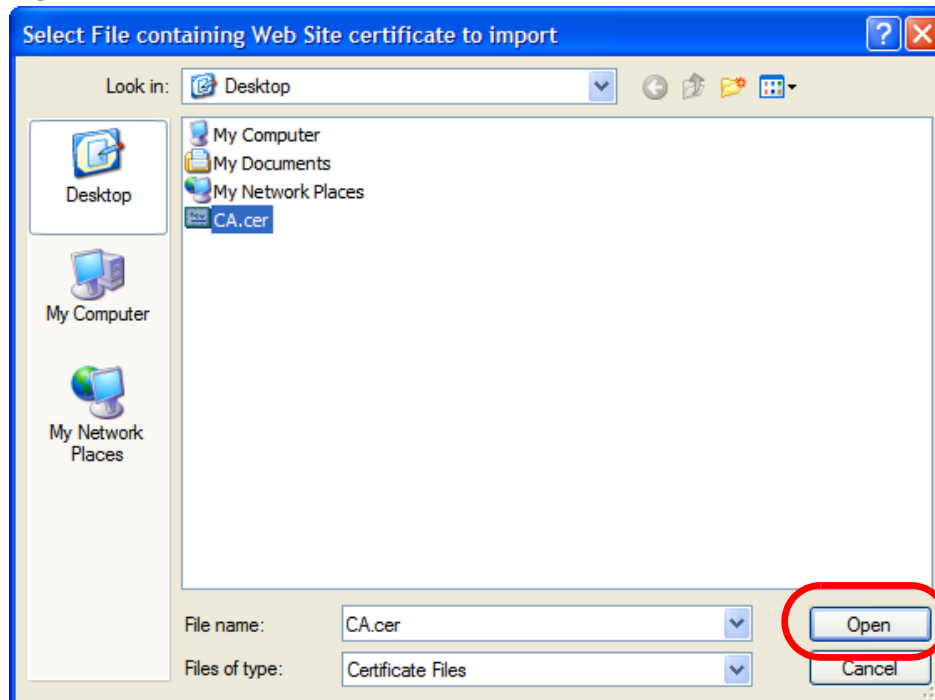
- 3 In the **Certificate Manager** dialog box, click **Web Sites** > **Import**.

**Figure 220** Firefox 2: Certificate Manager



- 4 Use the **Select File** dialog box to locate the certificate and then click **Open**.

**Figure 221** Firefox 2: Select File



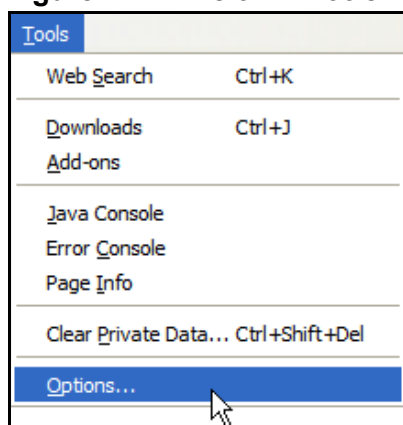
- 5 The next time you visit the web site, click the padlock in the address bar to open the **Page Info** > **Security** window to see the web page's security information.

## Removing a Certificate in Firefox

This section shows you how to remove a public key certificate in Firefox 2.

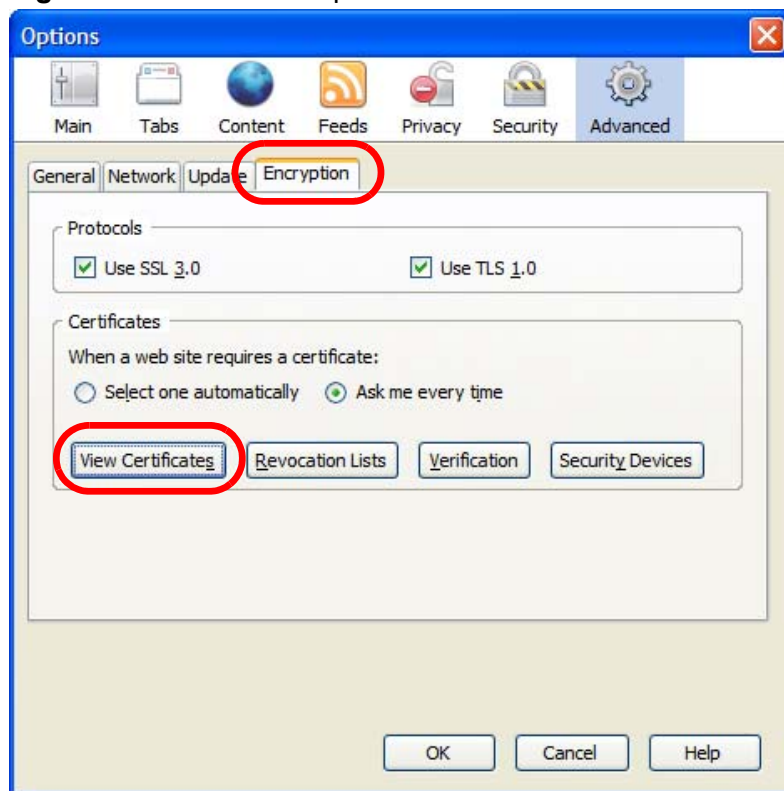
- 1 Open **Firefox** and click **Tools > Options**.

**Figure 222** Firefox 2: Tools Menu



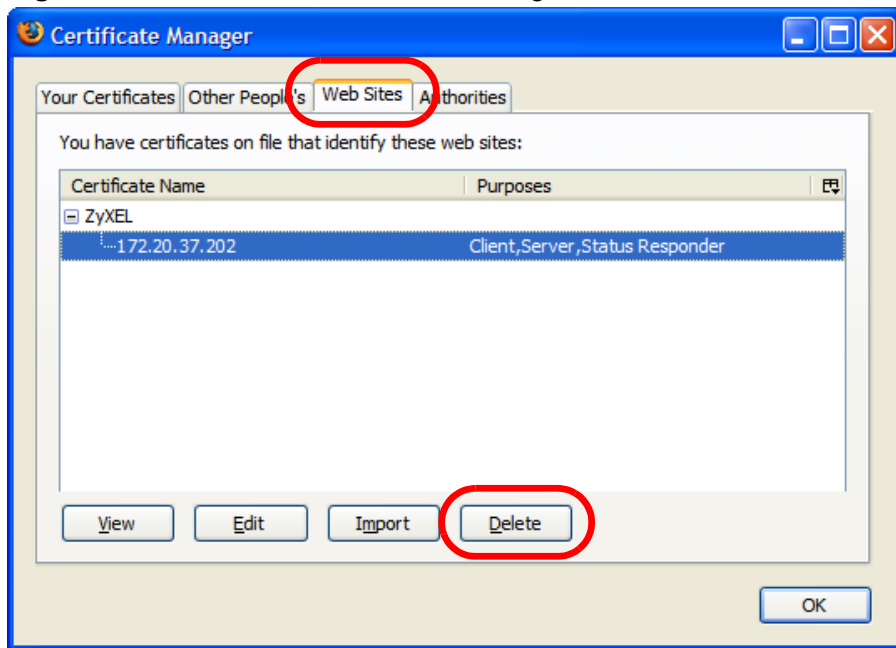
- 2 In the **Options** dialog box, click **Advanced > Encryption > View Certificates**.

**Figure 223** Firefox 2: Options



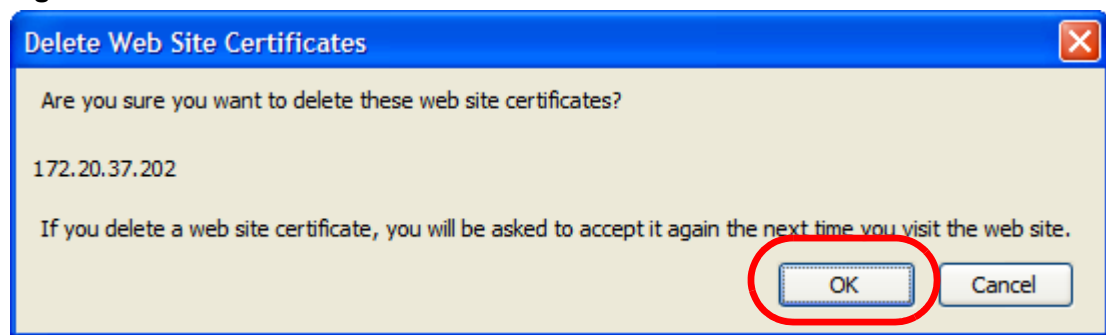
- 3 In the **Certificate Manager** dialog box, select the **Web Sites** tab, select the certificate that you want to remove, and then click **Delete**.

**Figure 224** Firefox 2: Certificate Manager



- 4 In the **Delete Web Site Certificates** dialog box, click **OK**.

**Figure 225** Firefox 2: Delete Web Site Certificates



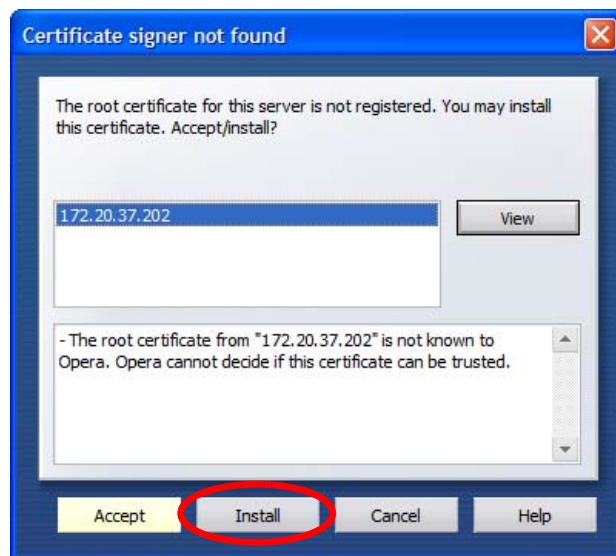
- 5 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

## Opera

The following example uses Opera 9 on Windows XP Professional; however, the screens can apply to Opera 9 on all platforms.

- 1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
- 2 Click **Install** to accept the certificate.

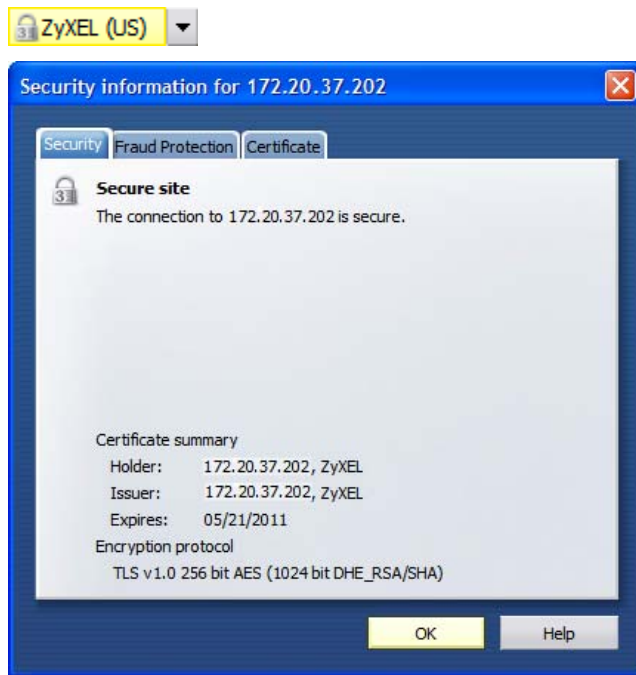
**Figure 226** Opera 9: Certificate signer not found





- 3 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

**Figure 227** Opera 9: Security information

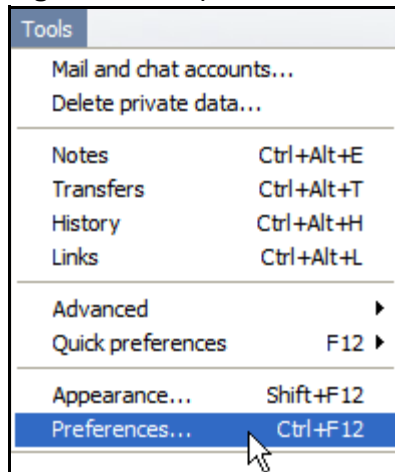


## Installing a Stand-Alone Certificate File in Opera

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

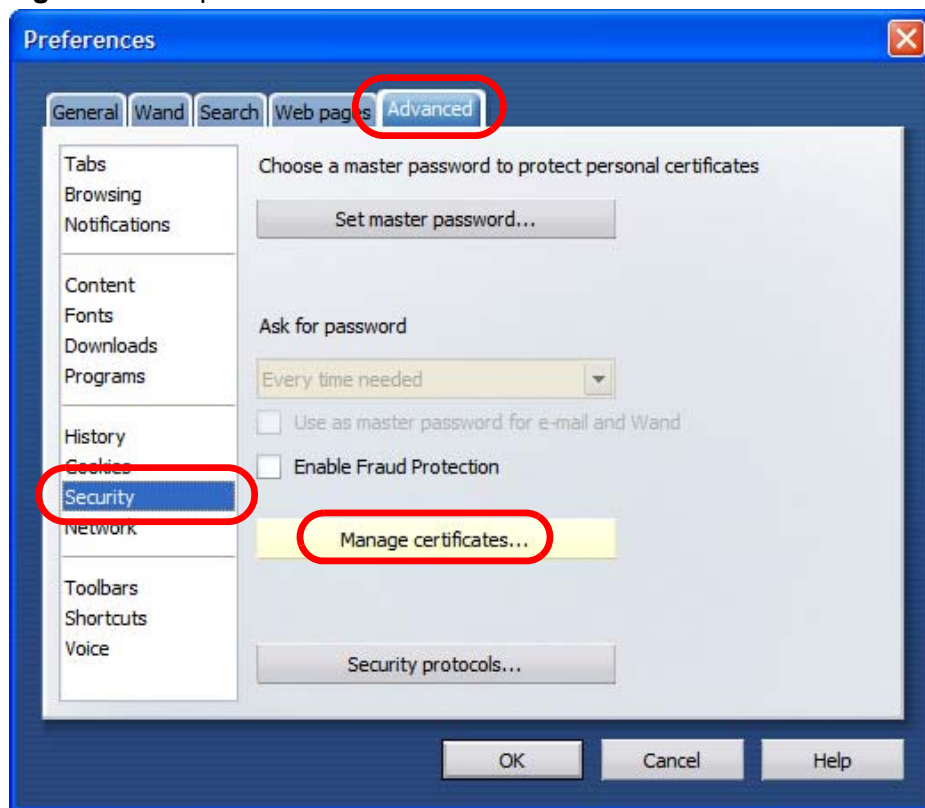
- 1 Open **Opera** and click **Tools > Preferences**.

**Figure 228** Opera 9: Tools Menu



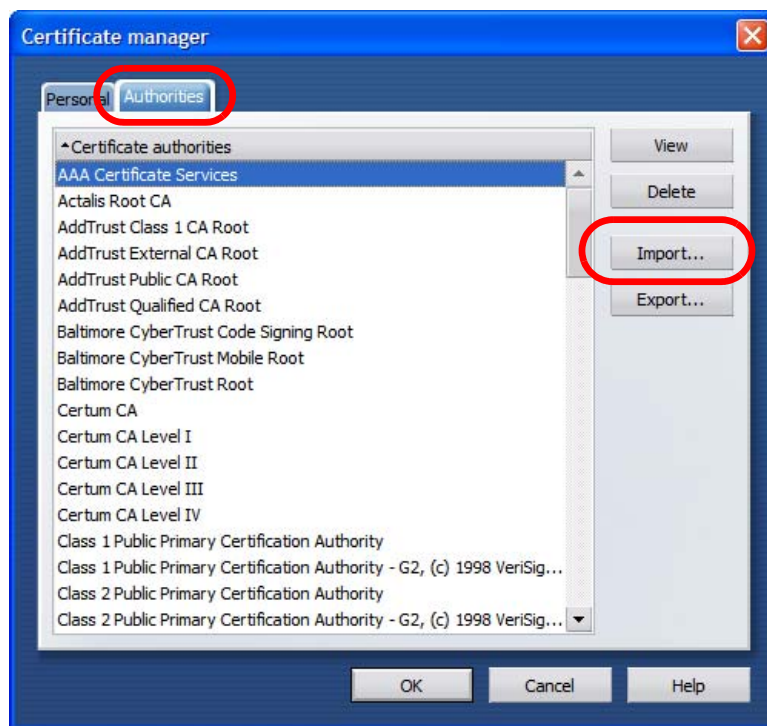
- 2 In **Preferences**, click **Advanced** > **Security** > **Manage certificates**.

**Figure 229** Opera 9: Preferences



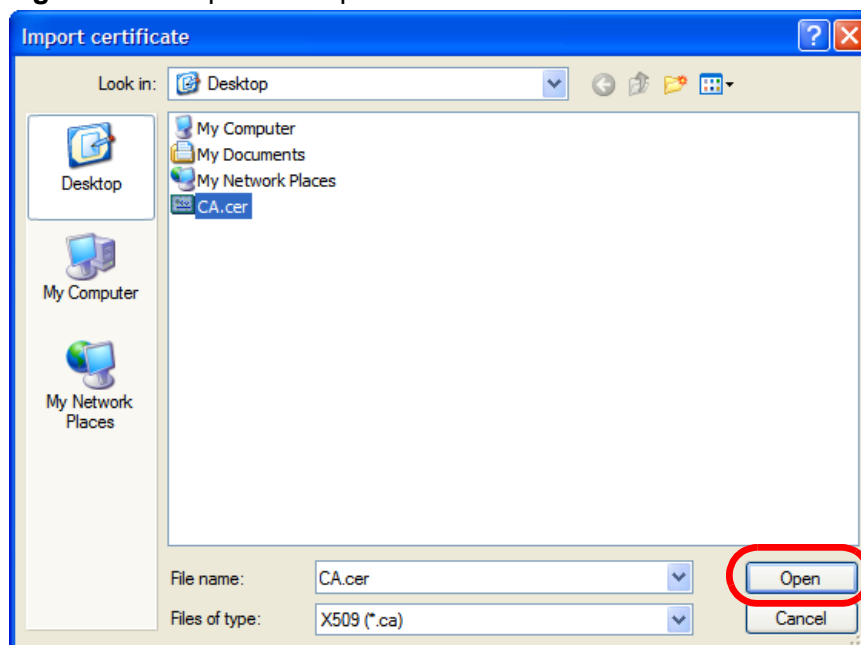
- 3 In the **Certificates Manager**, click **Authorities > Import**.

**Figure 230** Opera 9: Certificate manager



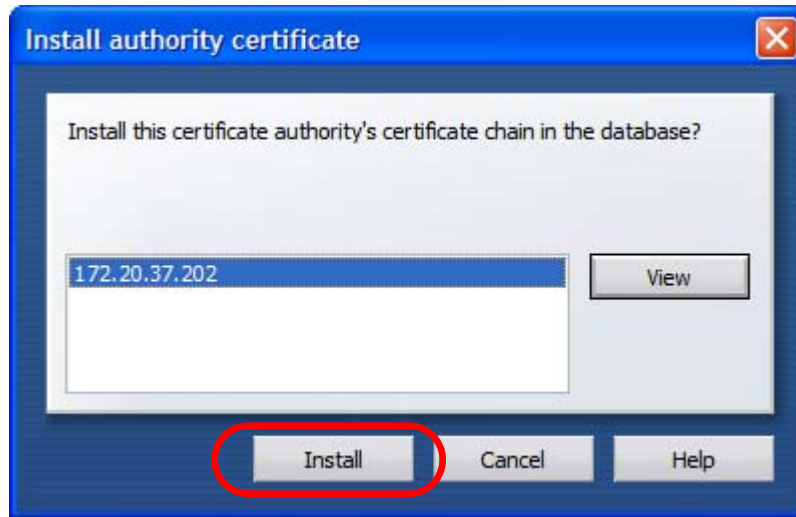
- 4 Use the **Import certificate** dialog box to locate the certificate and then click **Open**.

**Figure 231** Opera 9: Import certificate



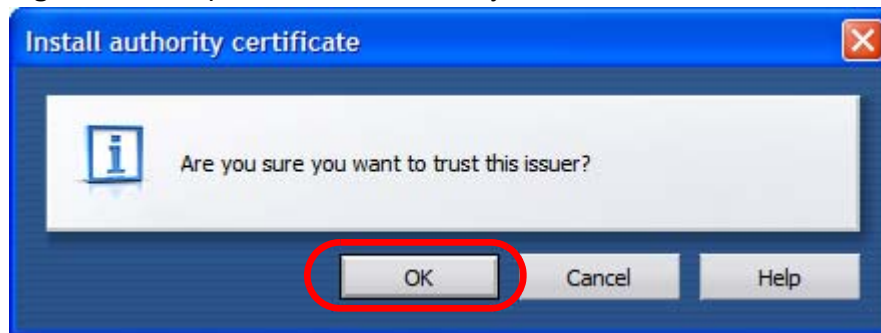
- 5 In the **Install authority certificate** dialog box, click **Install**.

**Figure 232** Opera 9: Install authority certificate



- 6 Next, click **OK**.

**Figure 233** Opera 9: Install authority certificate



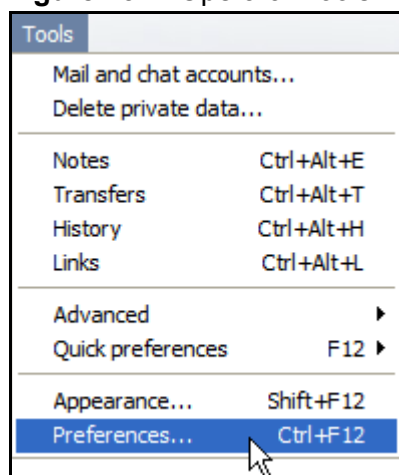
- 7 The next time you visit the web site, click the padlock in the address bar to open the **Security information** window to view the web page's security details.

## Removing a Certificate in Opera

This section shows you how to remove a public key certificate in Opera 9.

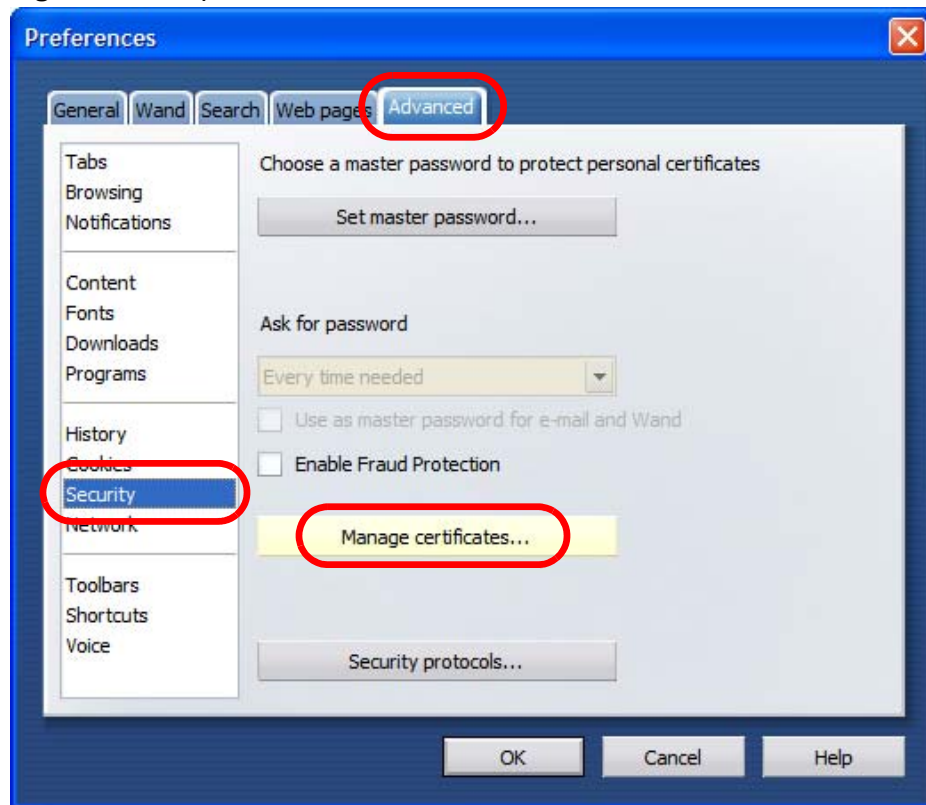
- 1 Open **Opera** and click **Tools > Preferences**.

**Figure 234** Opera 9: Tools Menu



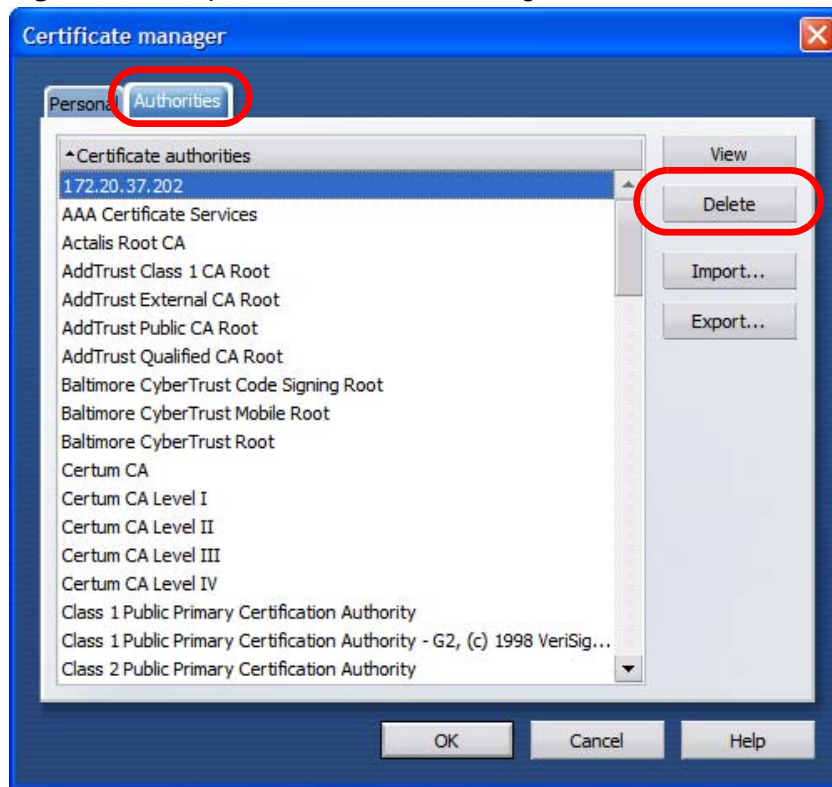
- 2 In **Preferences, Advanced > Security > Manage certificates**.

**Figure 235** Opera 9: Preferences



- 3 In the **Certificates manager**, select the **Authorities** tab, select the certificate that you want to remove, and then click **Delete**.

**Figure 236** Opera 9: Certificate manager



- 4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

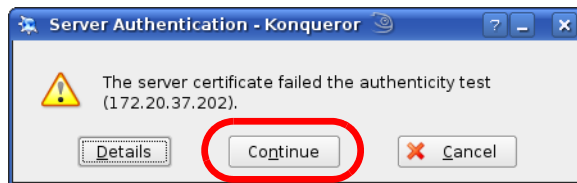
Note: There is no confirmation when you delete a certificate authority, so be absolutely certain that you want to go through with it before clicking the button.

## Konqueror

The following example uses Konqueror 3.5 on openSUSE 10.3, however the screens apply to Konqueror 3.5 on all Linux KDE distributions.

- 1 If your device's Web Configurator is set to use SSL certification, then the first time you browse to it you are presented with a certification error.
- 2 Click **Continue**.

**Figure 237** Konqueror 3.5: Server Authentication



- 3 Click **Forever** when prompted to accept the certificate.

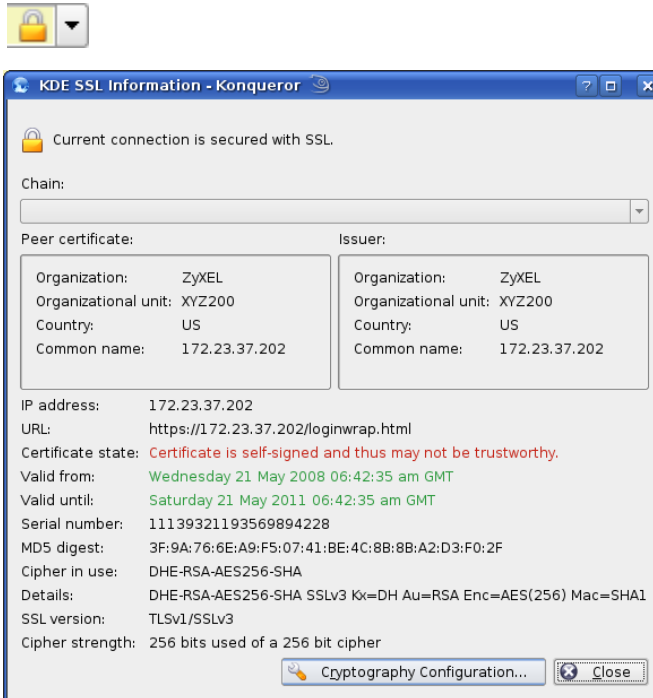
**Figure 238** Konqueror 3.5: Server Authentication





- 4 Click the padlock in the address bar to open the **KDE SSL Information** window and view the web page's security details.

**Figure 239** Konqueror 3.5: KDE SSL Information



## Installing a Stand-Alone Certificate File in Konqueror

Rather than browsing to a ZyXEL Web Configurator and installing a public key certificate when prompted, you can install a stand-alone certificate file if one has been issued to you.

- 1 Double-click the public key certificate file.

**Figure 240** Konqueror 3.5: Public Key Certificate File



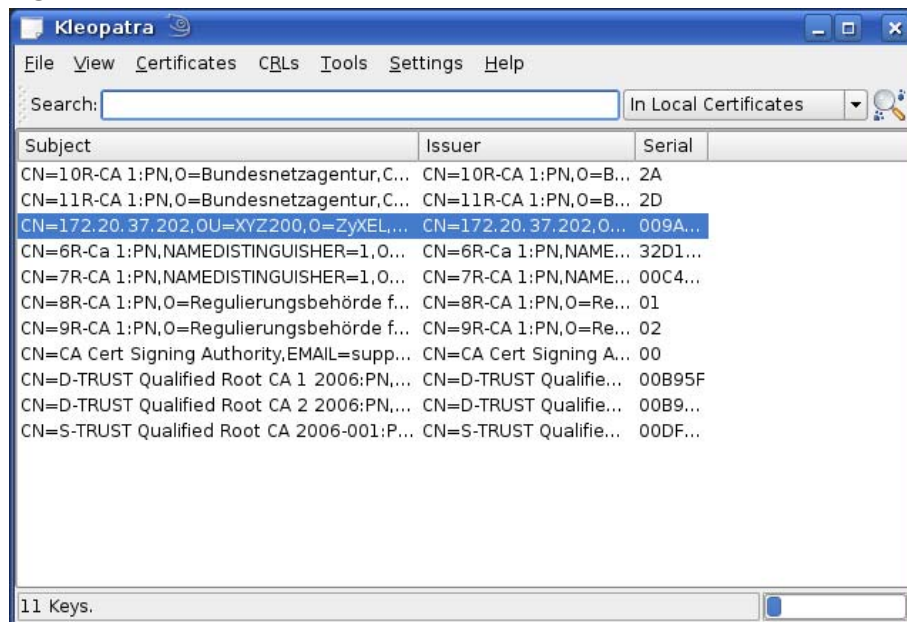
- 2 In the **Certificate Import Result - Kleopatra** dialog box, click **OK**.

**Figure 241** Konqueror 3.5: Certificate Import Result



The public key certificate appears in the KDE certificate manager, **Kleopatra**.

**Figure 242** Konqueror 3.5: Kleopatra



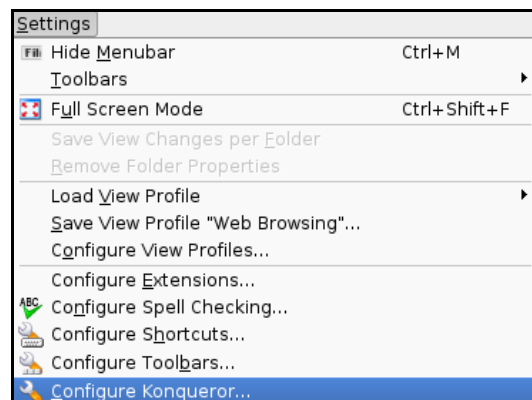
- 3 The next time you visit the web site, click the padlock in the address bar to open the **KDE SSL Information** window to view the web page's security details.

## Removing a Certificate in Konqueror

This section shows you how to remove a public key certificate in Konqueror 3.5.

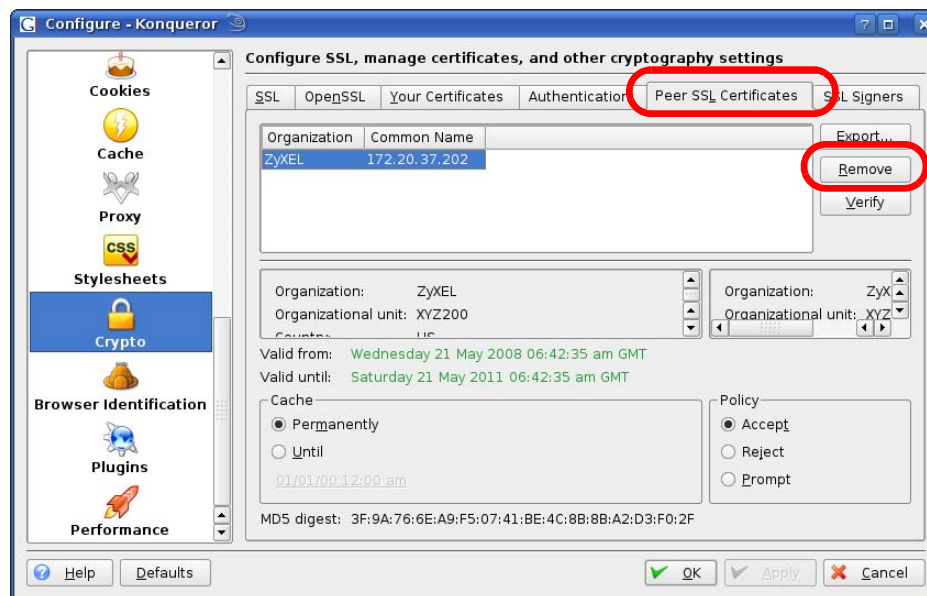
- 1 Open **Konqueror** and click **Settings > Configure Konqueror**.

**Figure 243** Konqueror 3.5: Settings Menu



- 2 In the **Configure** dialog box, select **Crypto**.
- 3 On the **Peer SSL Certificates** tab, select the certificate you want to delete and then click **Remove**.

**Figure 244** Konqueror 3.5: Configure



- 4 The next time you go to the web site that issued the public key certificate you just removed, a certification error appears.

Note: There is no confirmation when you remove a certificate authority, so be absolutely certain you want to go through with it before clicking the button.



# Open Source Licences

## Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes software developed by the Apache Software Foundation under Apache License.

## Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

### TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

#### 1. Definitions.

“License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

“Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

“Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition,

“control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-



charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works hereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any

additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Version 1.1

Copyright (c) 1999-2003 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).<sup>1</sup>" Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [apache@apache.org](mailto:apache@apache.org).

Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please see <http://www.apache.org/>.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

This Product includes phpmvc software under LGPL license.

## **GNU LESSER GENERAL PUBLIC LICENSE**

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts

as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

#### Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get

it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can re-link them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License. In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library

has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a “work based on the library” and a “work that uses the library”. The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

#### GNU LESSER GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called “this License”).

Each licensee is addressed as “you”.

A “library” means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The “Library”, below, refers to any such software library or work which has been distributed under these terms. A “work based on the Library” means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term “modification”.)

“Source code” for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library. Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) The modified work must itself be a software library. b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change. c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License. d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote

it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy. This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-

readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange. If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not

compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables. When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law. If such an object file uses only numerical parameters, data structure layouts and accessories, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.) Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications. You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things: a) Accompany the work with the complete corresponding

machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-



readable “work that uses the Library”, as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.) b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a

copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with. c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution. d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place. e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the “work that uses the Library” must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things: a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above. b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received

copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to

refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or

among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing

and reuse of software generally.

#### NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS.

This Product includes apcid, apcupsd, autofs, device-mapper, evms, exim. Lm\_sensors, mdadm, pam\_mount, raidtools, samba, sg\_utils, smartmontools, vsftpd, xfsprogs and Linux kernel software under GPL license.

## **GNU GENERAL PUBLIC LICENSE**

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### **Preamble**

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to

know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that re-distributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

#### TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on)

of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent

application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

#### NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL



OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

#### END OF TERMS AND CONDITIONS

All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product includes OpenLDAP software under the OpenLDAP Public License

### **The OpenLDAP Public License**

Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted

This Product includes open SSL under the Open SSL License

## Open SSL License

### LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

### OpenSSL License

=====

Copyright (c) 1998-2004 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

-----

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related:-).

If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

This Product include mod\_ssl software under BSD license

## **BSD**

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This Product includes php software under the PHP License

### **The PHP License, version 3.0**

Copyright (c) 1999 - 2006 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"

5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes PHP, freely available from <<http://www.php.net/>>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via E-mail at group@php.net. For more information on the PHP Group and the PHP project, please see <<http://www.php.net/>>.

This product includes the Zend Engine, freely available at <<http://www.zend.com/>>.

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND

NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This Product includes Sablotron software under MPL License

## **Mozilla Public License Version 1.1**

### 1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

## 2. Source Code License.

### 2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof) the licenses granted in this Section 2.1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

Notwithstanding Section 2.1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3)



for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

## 2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination) the licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

Notwithstanding Section 2.2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

## 3. Distribution Obligations.

### 3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

### 3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution

Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

### 3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

### 3.4. Intellectual Property Matters

#### (a) Third Party Claims

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or unscrupulous) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

#### (b) Contributor Apes

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the legal file.

#### (c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4 (a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

### 3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

### 3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Sections 3.1, 3.2, 3.3, 3.4 and 3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

### 3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

### 4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the legal file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

#### 5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

#### 6. Versions of the License.

##### 6.1. New Versions

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

##### 6.2. Effect of New Versions

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

##### 6.3. Derivative Works

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

#### 7. Disclaimer of warranty

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose

or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

## 8. Termination

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/ or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

#### 9. Limitation of liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall you, the initial developer, any other contributor, or any distributor of covered code, or any supplier of any of such parties, be liable to any person for any indirect, special, incidental, or consequential damages of any character including, without limitation, damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to you.

#### 10. U.S. government end users

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

#### 11. Miscellaneous

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

## 12. Responsibility for claims

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

## 13. Multiple-licensed code

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

Exhibit A - Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at <http://www.mozilla.org/MPL/>

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is \_\_\_\_\_.

The Initial Developer of the Original Code is \_\_\_\_\_.

Portions created by \_\_\_\_\_ are Copyright (C) \_\_\_\_\_  
\_\_\_\_\_. All Rights Reserved.

Contributor(s): \_\_\_\_\_.

Alternatively, the contents of this file may be used under the terms of the \_\_\_\_\_ license (the "[\_\_\_\_\_] License"), in which case the provisions of [\_\_\_\_\_] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [\_\_\_\_\_] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [\_\_\_\_\_] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [\_\_\_\_\_] License."

NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit

A rather than the text found in the Original Code Source Code for Your Modifications.

This Product includes expiate and krb5 software under the MIT License

## The MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

NOTE: Some components of the NSA incorporate source code covered under the Apache License, GPL License, LGPL License, BSD License, Open SSL License, OpenLDAP License, PHP License and MIT License. To obtain the source code covered under those Licenses, please contact ZyXEL Communications Corporation at: ZyXEL Technical Support.

## End-User License Agreement for "NSA"

**WARNING:** ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.



### 1. Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

### 2. Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

### 3. Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

### 4. Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. You may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing.

### 5. Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least

as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

#### 6.No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyxEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyxEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERRUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

#### 7.Limitation of Liability

IN NO EVENT WILL ZyxEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyxEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyxEL'S AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED \$1,000. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

#### 8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE

IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

#### 9.Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

#### 10.Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

#### 12.General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.



# Legal Information

## Copyright

Copyright © 2009 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

## Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Do not use the NSA for illegal purposes. Illegal downloading or sharing of files can result in severe civil and criminal penalties. You are subject to the restrictions of copyright laws and any other applicable laws and will bear the consequences of any infringements thereof. ZyXEL bears NO responsibility or liability for your use of the download service feature.

Make sure all data and programs on the NSA are also stored elsewhere. ZyXEL is not responsible for any loss of or damage to any data, programs, or storage media resulting from the use, misuse, or disuse of this or any other ZyXEL product.

## Certifications

### Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

### **Notices**

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

### **Viewing Certifications**

- 1 Go to <http://www.zyxel.com>.
- 2 Select your product on the ZyXEL home page to go to that product's page.
- 3 Select the certification you wish to view from this page.

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

### **Note**

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or

implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at [http://www.zyxel.com/web/support\\_warranty\\_info.php](http://www.zyxel.com/web/support_warranty_info.php).

## **Registration**

Register your product online to receive e-mail notices of firmware upgrades and information at [www.zyxel.com](http://www.zyxel.com) for global products, or at [www.us.zyxel.com](http://www.us.zyxel.com) for North American products.





# Index

## A

access rights [50](#)  
     Flickr [271](#)  
     shares [297](#), [298](#)  
     YouTube [275](#)  
 activation  
     download service [172](#)  
     Flickr/YouTube [266](#)  
     FTP [168](#)  
     FTP Uploadr [277](#)  
     media server [170](#)  
     recycle bins [49](#), [296](#)  
     web publishing [185](#)  
 ANONYMOUS FTP [347](#)  
 anonymous FTP access [168](#)  
 applications [165](#), [265](#)  
     auto upload  
         Flickr/YouTube [265](#)  
         FTP Uploadr [276](#)  
     broadcasting [167](#), [186](#)  
         adding channels [172](#), [187](#), [188](#)  
         channel guides [206](#)  
         RSS [167](#)  
     COPY/SYNC button [196](#)  
         configuration [196](#)  
         example [208](#)  
         synchronization [209](#)  
     download service [166](#), [199](#), [364](#)  
         activation [172](#)  
         adding a task [175](#)  
         BitTorrent [167](#), [175](#), [199](#)  
         configuration [171](#)  
         link capture browser plugin [199](#)  
         notifications [200](#)  
         preferences [177](#)  
         protection [201](#), [202](#)  
         status [173](#)  
         URL [175](#), [223](#)  
     FTP [165](#), [167](#), [265](#)  
         activation [168](#)  
         anonymous access [168](#)  
         passive mode transfer [168](#)

media server [166](#), [170](#)  
     activation [170](#)  
     configuration [170](#)  
     iTunes server [166](#), [197](#), [198](#)  
     rebuilding database [170](#)  
 print server [207](#)  
     configuration [194](#)  
     name [195](#)  
 web publishing [167](#), [184](#), [205](#)  
     activation [185](#)  
     example [203](#)  
     port number [205](#)  
 archive [121](#)  
 authorization  
     Flickr [267](#), [268](#)  
     YouTube [272](#)  
 auto upload  
     Flickr/YouTube [265](#)  
         activation [266](#)  
         authorization [267](#), [272](#)  
         configuration [270](#), [272](#)  
     FTP Uploadr [276](#)  
         activation [277](#)  
         bandwidth limit [280](#)  
         configuration [279](#)  
         server entry [278](#)  
     grace period [271](#), [275](#), [280](#)

## B

backup [120](#), [121](#)  
     archive [121](#)  
     synchronization tutorial [124](#)  
     tutorial [124](#)  
 backup files  
     restoring files by [129](#)  
 backup job  
     restoring files by [127](#)  
 backup settings [314](#)  
 bandwidth limit [280](#)  
 BitTorrent [167](#)

- IP filtering [181](#), [182](#)
- protection [201](#), [202](#)
- re-seeding [172](#)
- settings [180](#)
- torrent files [175](#), [199](#)
  - health [183](#)
  - info-hash [184](#)
  - trackers [184](#)
- broadcatching [167](#), [186](#)
  - adding channels [172](#), [187](#), [188](#)
  - channel guides [206](#)
  - RSS [167](#)
- browser plugin, capturing link [199](#)
- browsing shares [44](#)

## C

- capturing download links [199](#)
- certificate [316](#)
  - editing [317](#)
  - tutorial [104](#)
  - verifying [114](#)
- changing password [41](#), [42](#)
- channel guides [206](#)
- CIFS [139](#)
- configuration
  - COPY/SYNC button [196](#)
  - download service [171](#)
  - Flickr [270](#)
  - FTP Uploadr [279](#)
  - print server [194](#)
  - recycle bins [299](#)
  - shares [48](#), [49](#)
  - YouTube [272](#), [273](#)
- COPY/SYNC button [27](#), [196](#)
  - configuration [196](#)
  - example [208](#)
  - synchronization [209](#)
- copying contents [46](#), [47](#), [302](#)
- CPU
  - temperature [136](#)
  - usage [136](#)
- creating
  - groups [290](#), [291](#)
  - shares [45](#), [294](#), [296](#)
  - users [284](#), [286](#)

- volumes [149](#), [152](#)

## D

- data protection [155](#)
- database, rebuilding [170](#)
- date [141](#)
- deleting shares [46](#)
- diagnostic tools [163](#)
- disk
  - S.M.A.R.T. attributes [261](#)
- disk replacement [157](#)
- displaying user information [288](#)
- DLNA [166](#), [197](#)
- DNS [159](#), [162](#)
- Domain Name System, see DNS
- domain user
  - troubleshooting [348](#)
  - troubleshooting share access [348](#)
- download period control [179](#)
- download service [166](#), [199](#), [364](#)
  - activation [172](#)
  - adding a task [175](#)
  - BitTorrent [167](#)
    - IP filtering [181](#), [182](#)
    - protection [201](#), [202](#)
    - re-seeding [172](#)
    - settings [180](#)
    - torrent files [175](#), [199](#)
  - configuration [171](#)
  - download period control [179](#)
  - link capture browser plugin [199](#)
  - notifications [200](#)
    - activation [172](#)
  - preferences [177](#)
  - status [173](#)
  - URL, download service [175](#), [223](#)
- duplexing [154](#)

## E

- explicit TLS/SSL [116](#)
- external volumes [152](#)

## F

fan speed [136](#)

file

troubleshooting access [348](#)

File Transfer Protocol over Explicit TLS, see FTPES

File Transfer Protocol over TLS, see FTPS

files, uploading [45](#)

FileZilla [116](#)

fingerprint [114](#)

firmware, upgrading [318](#)

Flickr [265](#)

access rights [271](#)

activation [266](#)

authorization [267](#), [268](#)

grace period [271](#)

safety level [272](#)

folder

troubleshooting access [348](#)

FTP [116](#), [165](#), [167](#), [265](#)

activation [168](#)

anonymous access [168](#)

over TLS [116](#)

passive mode transfer [168](#)

FTP Uploadr [276](#)

activation [277](#)

bandwidth limit [280](#)

configuration [279](#)

grace period [280](#)

server entry [278](#)

FTPES [166](#)

FTPES - FTP over explicit TLS/SSL [116](#)

FTPS [116](#), [266](#)

## G

global icons [42](#), [52](#)

GMT [142](#)

grace period [271](#), [275](#), [280](#)

groups [289](#)

adding [290](#), [291](#)

editing [291](#)

membership [286](#), [291](#)

names [292](#)

searching [290](#)

## H

HTTP port [162](#)

HTTPS [110](#), [315](#)

## I

icons [42](#), [52](#), [55](#)

global [42](#), [52](#)

shares [44](#)

users [285](#)

IP address [159](#)

IP filtering [181](#), [182](#)

iTunes server [166](#), [197](#), [198](#)

## J

JBOD [150](#), [153](#)

jumbo frames [159](#), [160](#), [162](#)

## L

lag, time [139](#)

language selection [42](#)

LEDs [26](#)

link capture browser plugin [199](#)

login [41](#)

logs [310](#)

## M

maintenance [305](#)

backup settings [314](#)

logs [310](#)

power management [306](#), [364](#)

failure [307](#)

resume [307](#)

- schedule [308](#)
  - UPS [307](#)
- reset [314](#)
- restoring settings [314](#)
- shutdown [319](#)
- upgrading firmware [318](#)
- master browser [140](#)
- media server [166](#), [170](#)
  - activation [170](#)
  - configuration [170](#)
  - iTunes server [166](#), [198](#)
  - rebuilding database [170](#)
- membership [286](#)
  - groups [286](#), [291](#)
- mirroring [154](#)
- moving contents [46](#), [47](#), [302](#)
- My NSA [42](#), [43](#)
  - configuring shares [48](#), [49](#)
  - creating shares [45](#)
  - icons [42](#)
  - language selection [42](#)
  - share browser [44](#)

## N

- naming
  - server [140](#)
  - shares [50](#)
  - volumes [151](#)
  - workgroup [140](#)
- NAS Starter Utility, see NSU
- navigation panel [53](#)
- network [159](#)
  - diagnostic tools [163](#)
  - DNS [159](#), [162](#)
  - HTTP port [162](#)
  - IP address [159](#)
  - jumbo frames [159](#), [160](#), [162](#)
  - PPPoE [160](#), [163](#)
    - activation [164](#)
  - TCP/IP [161](#)
- notifications
  - download service
    - activation [172](#)
- notifications, download service [200](#)
- NSU [40](#)

## P

- passive mode transfer [168](#)
- password [41](#), [42](#), [51](#)
- port, HTTP [162](#)
- power management [306](#), [364](#)
  - failure [307](#)
  - resume [307](#)
  - schedule [308](#)
  - UPS [307](#)
- PPPoE [160](#), [163](#)
  - activation [164](#)
- preferences, download service [177](#)
- print server [207](#)
  - configuration [194](#)
  - name [195](#)
- protect [121](#)
  - backup [120](#)
  - backup tutorial [124](#)
- protection, download service [201](#), [202](#)
- public key certificate [316](#)
  - editing [317](#)

## R

- RAID
  - degraded [155](#)
  - RAID 0 [153](#)
  - RAID 1 [153](#), [154](#), [155](#)
  - recovering [157](#)
  - replacing disks [157](#)
  - resynchronization [157](#)
- rebuilding database [170](#)
- recycle bins [299](#)
  - activation [49](#), [296](#)
  - configuration [294](#), [299](#)
- related documentation [3](#)
- replacing disks [157](#)
- reset [27](#), [314](#)
- restoring
  - by backup files tutorial [129](#)
  - by backup job tutorial [127](#)
  - files [127](#)
- restoring settings [314](#)
- RSS [167](#)

download service notifications [200](#)

## S

S.M.A.R.T.

attributes [261](#)

safety level, Flickr [272](#)

schedule, power management [308](#)

scheduling, download service [179](#)

secure connections [110](#)

selecting language [42](#)

server entry, FTP Uploadr [278](#)

server name [140](#)

setup

BitTorrent [180](#)

COPY/SYNC button [196](#)

download service [171](#)

Flickr [270](#)

FTP Uploadr [279](#)

media server [170](#)

print server [194](#)

YouTube [272, 273](#)

share

troubleshooting local user access [347](#)

shares [43, 293](#)

access rights [50, 297, 298](#)

adding [294, 296](#)

browser [44](#)

configuration [48, 49](#)

copying contents [46, 47, 302](#)

creation [45](#)

deletion [46](#)

editing [296](#)

icons [44](#)

moving contents [46, 47, 302](#)

names [50](#)

recycle bins [294, 299](#)

activation [296](#)

configuration [299](#)

share browser [294, 300](#)

status [295](#)

types [295](#)

uploading files [45, 228, 300](#)

shutdown [319](#)

SSL [116, 315](#)

certificate [316](#)

editing [317](#)

tutorial [104](#)

status [52, 136](#)

download service [173](#)

shares [295](#)

volume [147, 155](#)

storage [145](#)

creating volumes [149](#)

disk replacement [157](#)

JBOD [146, 150, 153](#)

methods [153](#)

duplexing [154](#)

mirroring [154](#)

naming volumes [151](#)

RAID [146](#)

degraded [155](#)

RAID 0 [153](#)

RAID 1 [153, 154, 155](#)

recovering [157](#)

resynchronization [157](#)

status [147, 155](#)

USB devices [152, 157](#)

volumes [146](#)

synchronization [196, 209](#)

configuration [196](#)

directions [197](#)

single direction [209](#)

tutorial [124](#)

two directions [210](#)

system

date/time [141](#)

login [41](#)

master browser [140](#)

password [41, 42, 51](#)

reset [27](#)

server name [140](#)

settings [139](#)

status [136](#)

time lag [139](#)

workgroup name [140](#)

## T

TCP/IP [161](#)

temperature

CPU [136](#)

thumbprint [114](#)

- time [141](#)
  - lag [139](#)
  - server [142](#)
  - zone [142](#)
- TLS [116](#), [166](#), [266](#)
- torrent files [175](#), [199](#)
  - health [183](#)
  - info-hash [184](#)
  - trackers [184](#)
- Transport Layer Security, see TLS
- troubleshooting
  - domain user [348](#)
  - domain user share access [348](#)
  - file access [348](#)
  - folder access [348](#)
  - forgot password [342](#), [343](#)
  - LED indicators [338](#)
    - LAN [340](#)
  - local user share access [347](#)
  - login [346](#)
  - media files [353](#)
  - NAS Starter Utility [341](#)
  - overview [337](#)
  - user share access [346](#)
  - web configurator access [343](#)

## U

- upgrading firmware [318](#)
- uploading files [45](#), [228](#), [300](#)
- UPS [307](#)
- URL [175](#), [223](#)
- USB devices [152](#), [157](#)
- User Name [233](#)
- usernames [287](#)
- users [283](#)
  - adding an account [284](#), [286](#)
  - displaying information [285](#), [288](#)
  - editing an account [286](#)
  - group membership [286](#), [291](#)
  - icons [285](#)
  - search [284](#)
  - usernames [287](#)

## V

- video category, YouTube [275](#)
- volumes [146](#)
  - creation [149](#), [152](#)
  - JBOD [146](#), [150](#), [153](#)
  - names [151](#)
  - RAID [146](#)
    - degraded [155](#)
    - RAID 0 [153](#)
    - RAID 1 [153](#), [154](#), [155](#)
    - recovering [157](#)
    - resynchronization [157](#)
  - status [147](#), [155](#)
  - storage methods [153](#)
    - duplexing [154](#)
    - mirroring [154](#)

## W

- web configurator [39](#)
  - icons [42](#)
  - language selection [42](#)
  - login [41](#)
  - My NSA [42](#), [43](#)
  - navigation panel [53](#)
  - password [41](#), [42](#), [51](#)
  - status [52](#)
- web publishing [167](#), [184](#), [205](#)
  - activation [185](#)
  - example [203](#)
  - port number [205](#)
  - troubleshooting [356](#)
- web security [110](#)
- workgroup name [140](#)

## Y

- YouTube [265](#)
  - access rights [275](#)
  - activation [266](#)
  - authorization [272](#)
  - configuration [272](#), [273](#)
  - grace period [275](#)
  - video category [275](#)