

Thecus VisoGuard

NVR22/42/46/55/77/88/120/160

The term " VisoGuard NVR " in this user manual represents NVR22/42/46/55/77/88/120/160.

User's Manual

Copyright and Trademark Notice

Thecus and other names of Thecus products are registered trademarks of Thecus Technology Corp. Microsoft, Windows, and the Windows logo are registered trademarks of Microsoft Corporation. Apple, iTunes and Apple OS X are registered trademarks of Apple Computers, Inc. All other trademarks and brand names are the property of their respective owners. Specifications are subject to change without notice.

Copyright © 2011 Thecus Technology Corporation. All rights reserved.

About This Manual

All information in this manual has been carefully verified to ensure its correctness. In case of an error, please provide us with your feedback. Thecus Technology Corporation reserves the right to modify the contents of this manual without notice.

Product name: Thecus VisoGuard NVR

Manual Version: 1.1

Release Date: July 2011

Limited Warranty

Thecus Technology Corporation guarantees all components of Thecus VisoGuard NVR products are thoroughly tested before they leave the factory and should function normally under general usage. In case of any system malfunctions, Thecus Technology Corporation and its local representatives and dealers are responsible for repair without cost to the customer if the product fails within the warranty period and under normal usage. Thecus Technology Corporation is not responsible for any damage or loss of data deemed to be caused by its products. It is highly recommended that users conduct necessary back-up practices.

Safety Warnings

For your safety, please read and follow the following safety warnings:

-  Read this manual thoroughly before attempting to set up your Thecus VisoGuard NVR.
-  Your Thecus VisoGuard NVR is a complicated electronic device. DO NOT attempt to repair it under any circumstances. In the case of malfunction, turn off the power immediately and have it repaired at a qualified service center. Contact your vendor for details.
-  DO NOT allow anything to rest on the power cord and DO NOT place the power cord in an area where it can be stepped on. Carefully place connecting cables to avoid stepping or tripping on them.
-  Your Thecus VisoGuard NVR can operate normally under temperatures between 5°C and 40°C, with relative humidity of 20% – 85%. Using Thecus VisoGuard NVR under extreme environmental conditions could damage the unit.
-  Ensure that the Thecus VisoGuard NVR is provided with the correct supply voltage (AC 100V ~ 240V, 50/60 Hz). Plugging the Thecus VisoGuard NVR to an incorrect power source could damage the unit.
-  Do NOT expose Thecus VisoGuard NVR to dampness, dust, or corrosive liquids.
-  Do NOT place Thecus VisoGuard NVR on any uneven surfaces.
-  DO NOT place Thecus VisoGuard NVR in direct sunlight or expose it to other heat sources.
-  DO NOT use chemicals or aerosols to clean Thecus VisoGuard NVR. Unplug the power cord and all connected cables before cleaning.
-  DO NOT place any objects on the Thecus VisoGuard NVR or obstruct its ventilation slots to avoid overheating the unit.
-  Keep packaging out of the reach of children.
-  If disposing of the device, please follow your local regulations for the safe disposal of electronic products to protect the environment.

Table of Contents

Copyright and Trademark Notice	2
About This Manual.....	2
Limited Warranty	2
Safety Warnings.....	3
Table of Contents	4
Chapter 1: Introduction.....	6
Overview	6
Package Contents	7
Front Panel.....	8
Hard Disk Trays	16
Rear Panel.....	17
Chapter 2: Hardware Installation	23
Overview	23
Before You Begin	23
Cable Connections	23
Chapter 3: First Time Setup.....	30
Overview	30
Thecus Setup Wizard	30
LCD Operation (NVR55/NVR46/NVR77/NVR88)	33
OLED Operation (NVR42/NVR120/NVR160)	36
Typical Setup Procedure	36
Chapter 4: System Administration	38
Overview	38
Web Administration Interface	38
My Favorite.....	39
Menu Bar.....	41
Message Bar	42
System Information.....	43
General Information.....	43
System/Service Status	43
Logs.....	44
System Management	45
Date and Time: System Date and settings	45
Notification configuration	46
Firmware Upgrade	47
Administrator password	47
Config Mgmt	48
Factory default	49
Reboot & Shutdown	49
File System check.....	49
UI Login Configuration.....	51
System Network	52
WAN/LAN1.....	52
LAN2.....	53
DHCP Server Configuration	54
Storage Management.....	54
Disks Information	54
RAID Information.....	57
Space Allocation(NVR46R/NVR46S/NVR55)	61
Share Folder	62

Folder and sub-folders Access Control List (ACL).....	66
User and Group Authentication.....	67
Local User Configuration	67
Local Group Configuration.....	69
Network Service	71
Samba / CIFS.....	71
FTP	72
Application Server	73
Module Installation.....	73
Chapter 5: Using Thecus VisoGuard NVR.....	74
Overview	74
Login Page.....	74
Using the Web Disk	75
Photo Server	78
Windows XP Publishing Wizard	78
Managing Albums and Photos	84
Creating Albums	85
Password Protecting Albums.....	85
Uploading Pictures to Albums	85
EXIF Information	85
Slide Shows	86
Mapping a Client PC to the Thecus VisoGuard NVR	86
Windows.....	86
Chapter 6: Tips and Tricks	87
USB and eSATA Storage Expansion.....	87
Replacing Damaged Hard Drives.....	87
Hard Drive Damage	87
Replacing a Hard Drive	87
RAID Auto-Rebuild	87
Chapter 7: Troubleshooting	88
Forgot My Network IP Address	88
Can't Map a Network Drive in Windows XP	88
Restoring Factory Defaults	88
Problems with Time and Date Settings.....	89
Dual DOM Supports for Dual Protection	89
Appendix A: Customer Support.....	90
Appendix B: RAID Basics	91
Overview	91
Benefits	91
Improved Performance	91
Data Security	91
RAID Levels.....	91
Appendix C: Licensing Information	94
Overview	94
Source Code Availability	94
CGIC License Terms.....	95
GNU General Public License.....	95

Chapter 1: Introduction

Overview

Thank you for choosing the Thecus VisoGuard NVR Networking Surveillance + Storage Server. The Thecus VisoGuard NVR is an easy-to-use Surveillance storage server that allows a dedicated approach to storing and distributing data on a network. Surveillance data reliability is ensured with RAID features that provide data security and recovery—over multi Terabyte of storage is available using RAID 5 and RAID 6. Gigabit Ethernet ports enhance network efficiency, allowing the VisoGuard NVR to take over file management functions, increase application and data sharing and provide faster data response.

Package Contents

The thecus VisoGuard NVR should contain the following common items:

- System Unit x1
- QIG (Quick Installation Guide) x1
- CD-Title x1 (Universal CD)
- Ethernet Cable x1
- Accessory bag x1
- HDD Compatibility list Card x1
- Multiple Languages Warranty Card x1
- Power cord x1

Your **NVR22/NVR42** package should contain additional items:

- Power adapter

Your **NVR46R/S** package should contain the additional items:

- Power Cord
 - NVR46R +1
- USB Cable (A-B Type) x1

Your **NVR55** package should contain additional items:

- USB Cable (A-B Type) x1

Your **NVR88/NVR120/NVR160** package should contain additional items:

- Power Cord x1

Please check to see if your package is complete. If you find that some items are missing, contact your dealer.

Front Panel

NVR22:

The Thecus NVR22's front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	Description
Power Button	<ul style="list-style-type: none"> • Powers the NVR22 on/off.
USB Port	<ul style="list-style-type: none"> • USB 2.0 port for compatible USB devices, such as digital cameras, USB disks.
USB Copy Button	<ul style="list-style-type: none"> • Copies USB storage contents to NVR22.
Card reader	<ul style="list-style-type: none"> • Supports SD/SDHC/MMC cards via USB interface.
HDD1 led	<ul style="list-style-type: none"> • Blinking white: HDD activity
HDD2 led	<ul style="list-style-type: none"> • Blinking white: HDD activity
WAN led	<ul style="list-style-type: none"> • Solid white: WAN Cable link • Blinking white: Network activity
LAN led	<ul style="list-style-type: none"> • Solid white: LAN Cable link • Blinking : Network activity
USB Copy led	<ul style="list-style-type: none"> • Blinking white: USB copy activity
Card reader led	<ul style="list-style-type: none"> • Blinking white: Card reader copy activity

NVR42:

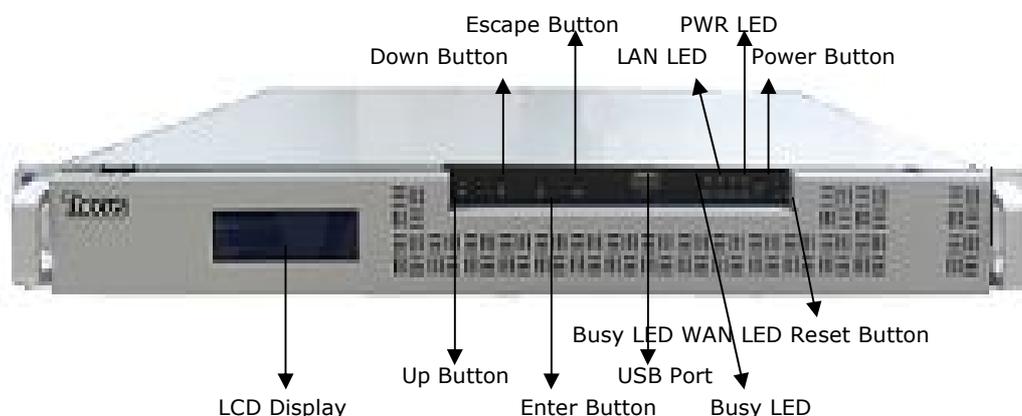
The Thecus NVR42's front panel has the device's controls, indicators, and hard disk trays:



Front Panel		
Item	Description	
Power Button	<ul style="list-style-type: none"> Power on/off NVR42 	
OLED	<ul style="list-style-type: none"> Displays current system status and messages OLED screen saver will be enabled after screen is left idle for more than 3 mins OLED screen will be disabled after it is left idle for more than 6 mins 	
OLED	HDD 1 LED	<ul style="list-style-type: none"> Yellow: HDD activity Red: HDD failure
	HDD 2 LED	<ul style="list-style-type: none"> Yellow: HDD activity Red: HDD failure
	HDD 3 LED	<ul style="list-style-type: none"> Yellow: HDD activity Red: HDD failure
	HDD 4 LED	<ul style="list-style-type: none"> Yellow: HDD activity Red: HDD failure
	WAN LED	<ul style="list-style-type: none"> Blinking green: network activity
	LAN LED	<ul style="list-style-type: none"> Blinking green: network activity
	USB Copy	<ul style="list-style-type: none"> Blue: USB Copy activity Red: USB Copy failure
HDD Tray	<ul style="list-style-type: none"> Four HDD trays support 4x 3.5" or 4 x 2.5" HDDs 	
USB Copy Button	<ul style="list-style-type: none"> Copy USB storage contents to NVR42 	
USB Port	<ul style="list-style-type: none"> USB 2.0 port for compatible USB devices, such as USB disks. 	

NVR46:

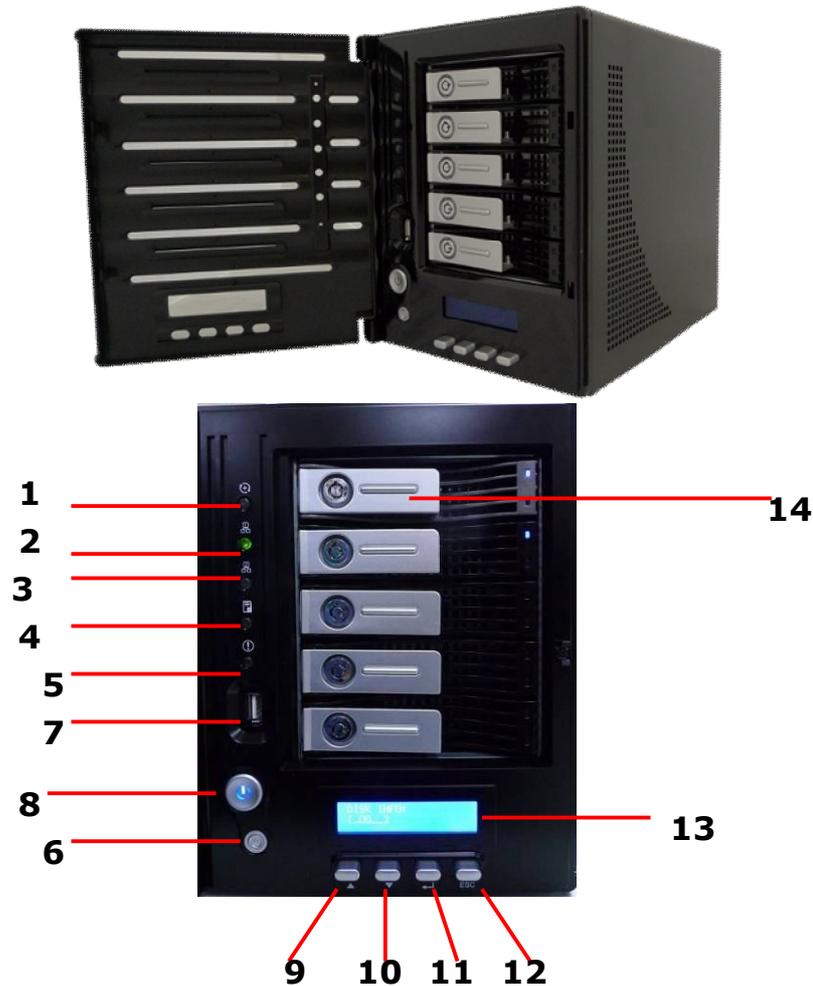
The Thecus NVR46's front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	Description
WAN LED	<ul style="list-style-type: none"> • Solid green: network link • Blinking green: network activity
LAN LED	<ul style="list-style-type: none"> • Solid green: network link • Blinking green: network activity
Busy LED	<ul style="list-style-type: none"> • Blinking orange: system startup or system maintenance; data currently inaccessible
USB Port	<ul style="list-style-type: none"> • USB 2.0 port for compatible USB devices, such as digital cameras, USB disks
Power Button	<ul style="list-style-type: none"> • Power on/off NVR46 • Solid blue: Device is powered on • Blinking blue: eSATA hard disk is connected and active
Reset Button	<ul style="list-style-type: none"> • Resets the NVR46 • Press for five seconds during boot process to reset IP address and admin password
HDD Trays	<ul style="list-style-type: none"> • Four 3.5" SATA HDD trays • Locks are provided for added security
LCD Display	<ul style="list-style-type: none"> • Displays current system status and warning messages • Displays hostname, WAN/LAN IP address, RAID status, and current time
Up Button ▲	<ul style="list-style-type: none"> • Push to scroll up when using the LCD display
Down Button ▼	<ul style="list-style-type: none"> • Push to scroll down when using the LCD display
Enter Button ↵	<ul style="list-style-type: none"> • Push to confirm information entered into the LCD display
Escape Button ESC	<ul style="list-style-type: none"> • Push to leave the current LCD menu

NVR55:

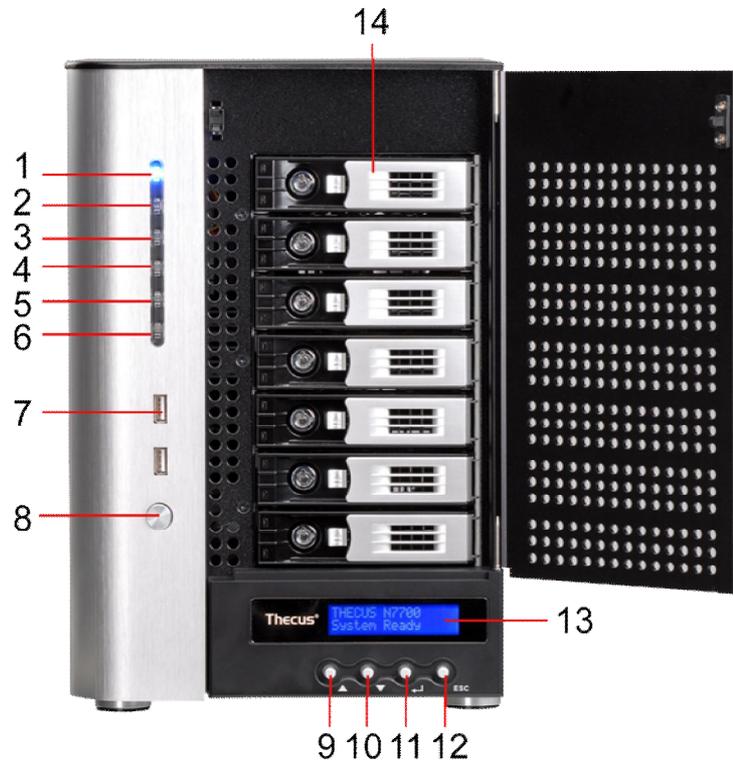
The Thecus NVR55's front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	Description
1.System LED	<ul style="list-style-type: none"> • Blinking orange: System is being upgraded or ;is starting up; data currently inaccessible
2.WAN/LAN1 LED	<ul style="list-style-type: none"> • Solid green: Network link • Blinking green: Network activity
3.LAN2 LED	<ul style="list-style-type: none"> • Solid green: Network link • Blinking green: Network activity
4.USB Copy LED	<ul style="list-style-type: none"> • Solid blue: Files are being copied from a USB storage device
5.Syetem Warning LED	<ul style="list-style-type: none"> • Solid RED: System error
6.Reset Button	<ul style="list-style-type: none"> • Resets system configuration to default value.
7.USB Port	<ul style="list-style-type: none"> • USB 2.0 port for compatible USB devices, such as USB disks.
8.Power Button/ Power LED	<ul style="list-style-type: none"> • Power on/off NVR55 and Power LED. • Solid blue: System is power on.
9.Up Button ▲	<ul style="list-style-type: none"> • Push to scroll up when using the LCD display.
10.Down Button ▼	<ul style="list-style-type: none"> • Push to enter the USB copy operation screen.
11.Enter Button ↵	<ul style="list-style-type: none"> • Push to enter LCD administrator password to access basic system setting.
12.Escape Button ESC	<ul style="list-style-type: none"> • Push to leave the current LCD menu.
13.LCD Display	<ul style="list-style-type: none"> • Displays current system status and warning messages.
14.HDD Trays	<ul style="list-style-type: none"> • Five 3.5" SATA HDD trays. • Locks are provided for added security.

NVR77:

The Thecus NVR77's front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	Description
1.Power LED	<ul style="list-style-type: none"> • Solid blue: System is power on.
2.System LED	<ul style="list-style-type: none"> • Solid orange: system is being upgraded or system startup; data currently inaccessible
3.WAN LED	<ul style="list-style-type: none"> • Solid green: network link • Blinking green: network activity
4.LAN LED	<ul style="list-style-type: none"> • Solid green: network link • Blinking green: network activity
5.USB Copy LED	<ul style="list-style-type: none"> • Solid blue: files are being copied from a USB storage device
6.eSATA link LED	<ul style="list-style-type: none"> • Solid blue: external eSATA device has connected
7.USB Port	<ul style="list-style-type: none"> • USB 2.0 port for compatible USB devices, such as USB disks.
8.Power Button	<ul style="list-style-type: none"> • Power on/off NVR77
9.Up Button ▲	<ul style="list-style-type: none"> • Push to scroll up when using the LCD display
10.Down Button ▼	<ul style="list-style-type: none"> • Push to enter USB copy operation screen
11.Enter Button ↵	<ul style="list-style-type: none"> • Push to enter LCD operate password for basic system setting
12.Escape Button ESC	<ul style="list-style-type: none"> • Push to leave the current LCD menu
13.LCD Display	<ul style="list-style-type: none"> • Displays current system status and warning messages
14.HDD Trays	<ul style="list-style-type: none"> • Seven 3.5" SATA HDD trays • Locks are provided for added security

NVR88:

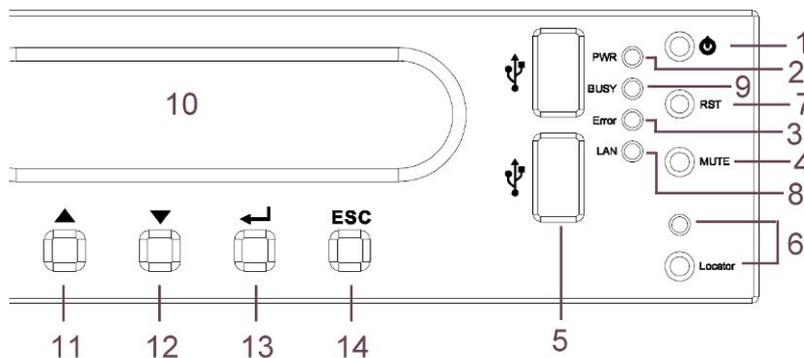
The Thecus NVR88's front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	Description
1.Power Button	• Power on/off NVR88
2.Power LED	• Solid green: System is power on.
3.Reboot Button	• Press to system reboot
4.System fan alarm LED	• Solid red: system fan failure notification
5. Mute button	• Mute the system fan alarm.
6.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks.
7.Up Button ▲	• Push to scroll up when using the LCD display
8.Down Button ▼	• Push to enter USB copy operation screen
9.Enter Button ↵	• Push to enter LCD operate password for basic system setting
10.Escape Button ESC	• Push to leave the current LCD menu

NVR120:

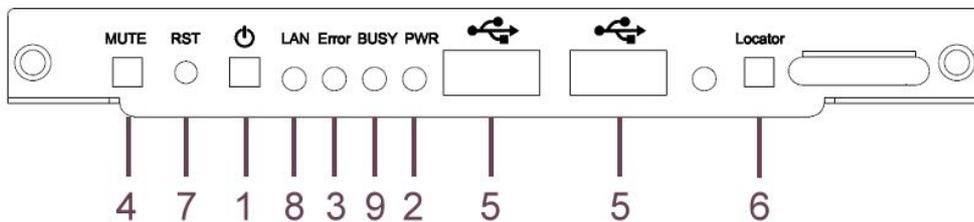
The Thecus NVR120's front panel has the device's controls, indicators, and hard disk trays:



Front Panel	
Item	Description
1.Power Button	• Power on/off NVR120
2.Power LED	• Solid green: System is power on.
3.System error LED	• Solid RED: System error.
4.Mute button	• Mute the system fan alarm.
5.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks
6. Locator button / LED	• Press the button, the back led will light up to identify the system position of the rack
7. RST	• Reboot system.
8. LAN	• Blinking green: network activity • Solid green: network link
9. BUSY	• Blinking orange: system startup or system maintenance; data currently inaccessible
10.OLED	• Displays current system status and messages • OLED screen saver will be enabled after screen is idle for more than 3 minutes • OLED screen will be turn off after idle for more than 6 minutes
11.Up Button ▲	• Push to scroll up when using the OLED display
12.Down Button ▼	• Push to enter USB copy operation screen
13.Enter Button ↵	• Push to enter OLED operate password for basic system setting
14.Escape Button ESC	• Push to leave the current OLED menu

NVR160 series:

The Thecus NVR160's front panel has the device's controls, indicators, and hard disk trays:



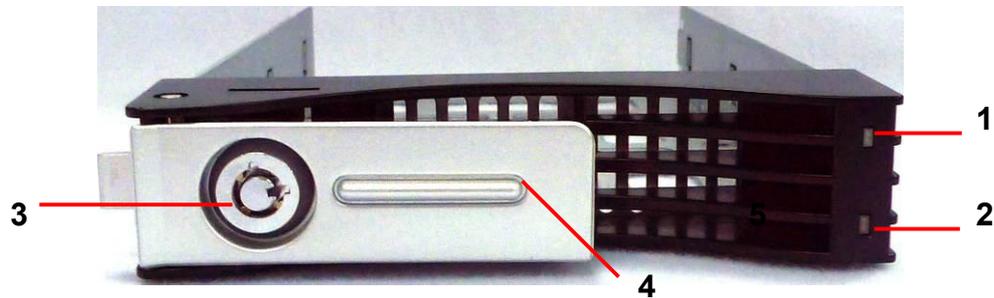
Front Panel	
Item	Description
1.Power Button	• Power on/off NVR160
2.Power LED	• Solid green: System is power on.
3.System error LED	• Solid RED: System error.

4.Mute button	<ul style="list-style-type: none"> • Mute the system fan alarm.
5.USB Port	<ul style="list-style-type: none"> • USB 2.0 port for compatible USB devices, such as USB disks.
6. Locator button / LED	<ul style="list-style-type: none"> • Press the button, the back led will light up to identify the rack position of the system
7. RST	<ul style="list-style-type: none"> • Reboot system.
8. LAN	<ul style="list-style-type: none"> • Blinking green: network activity • Solid green: network link
9. BUSY	<ul style="list-style-type: none"> • Blinking orange: system startup or system maintenance; data currently inaccessible
10.OLED	<ul style="list-style-type: none"> • Displays current system status and messages • OLED screen saver will be enabled after screen is idle for more than 3 minutes • OLED screen will be turn off after idle for more than 6 minutes
11.Up Button ▲	<ul style="list-style-type: none"> • Push to scroll up when using the OLED display
12.Down Button ▼	<ul style="list-style-type: none"> • Push to enter USB copy operation screen
13.Enter Button ↵	<ul style="list-style-type: none"> • Push to enter OLED operate password for basic system setting
14.Escape Button ESC	<ul style="list-style-type: none"> • Push to leave the current OLED menu

Hard Disk Trays

NVR22/NVR42/NVR55:

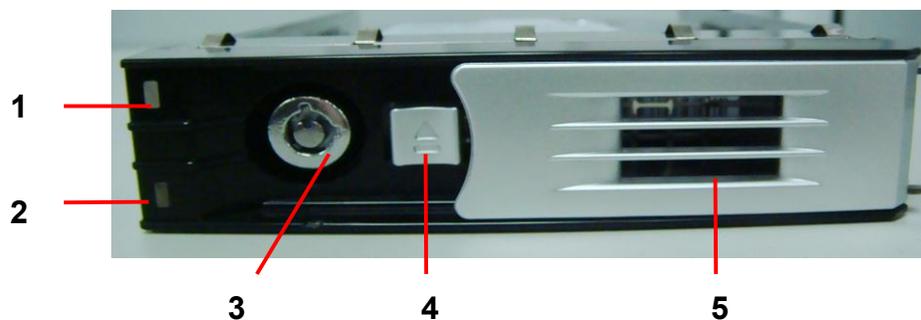
Each of mentioned above models hard disk trays has a lock, a latch, and two LED indicators:



Hard Disk Trays	
Item	Description
1.HDD Power LED	• Solid blue: Hard disk is powered on(No function on NVR42)
2.HDD Access/Error LED	• Blinking green: System is accessing data on the hard disk • Solid red: HDD fail(No function on NVR42)
3.Lock	• Use the lock to physically secure the hard disk to the unit.
4.Handle	• Pull to remove the HDD tray.

NVR46/NVR77/NVR88/NVR120/NVR160:

Each of mentioned above models hard disk trays has a lock, a latch, and two LED indicators:

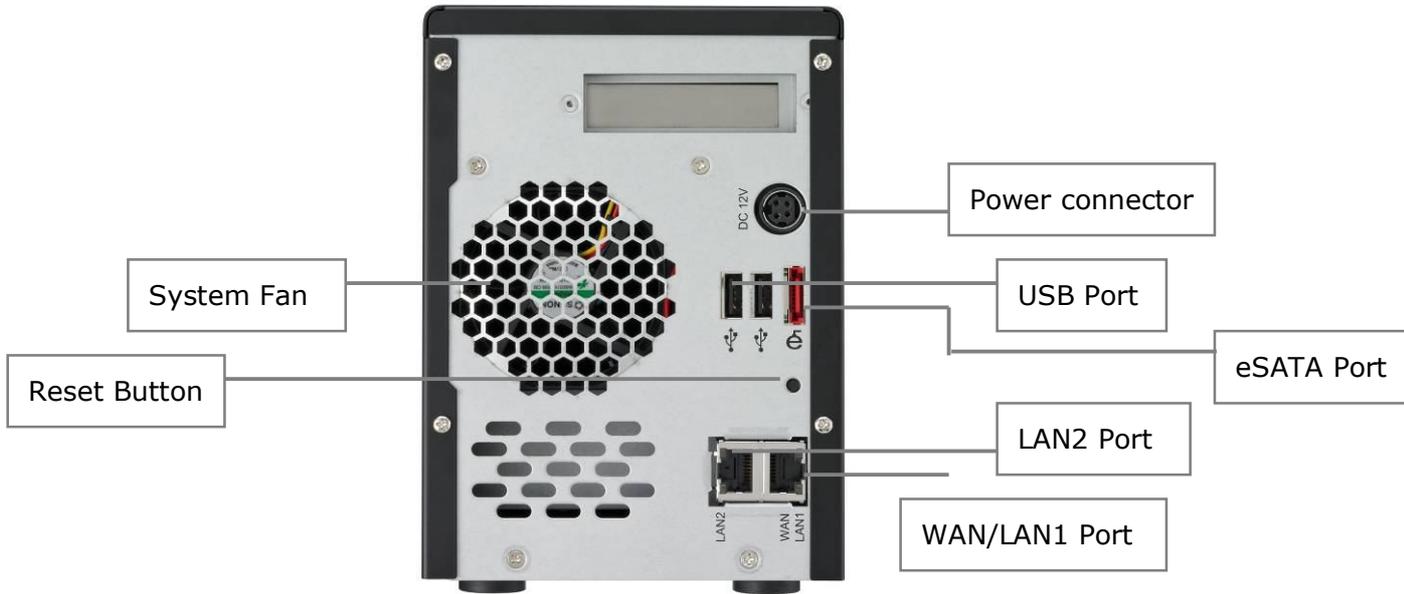


Hard Disk Trays	
Item	Description
1.HDD Power LED	• Solid blue: Hard disk is powered on
2.HDD Access/Error LED	• Blinking green: System is accessing data on the hard disk • Solid red: HDD fail
3.Lock	• Use the lock to physically secure the hard disk to the unit.
4.Latch	• Use to open and remove or close and secure the tray.
5.Handle	• Pull to remove the HDD tray.

Rear Panel

NVR22:

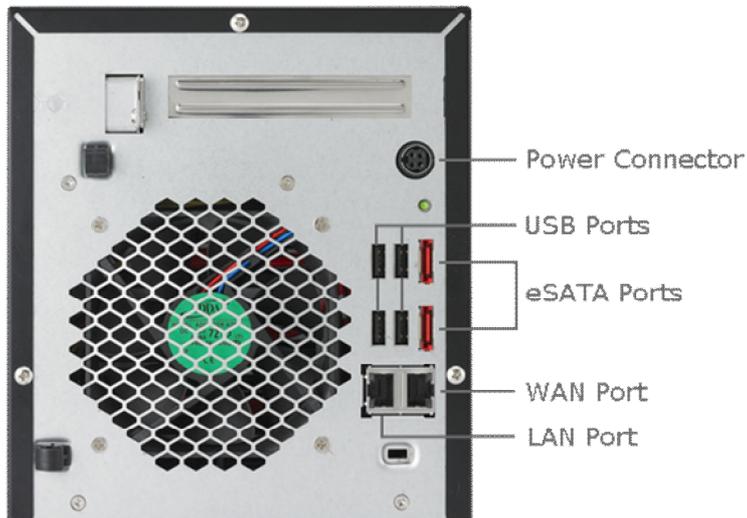
The NVR22 rear panel features ports and connectors.



Back Panel	
Item	Description
eSATA Port	<ul style="list-style-type: none"> eSATA port for high-speed external storage expansion.
USB Port	<ul style="list-style-type: none"> USB 2.0 port for compatible USB devices, such as digital cameras, USB disks.
WAN/LAN1 Port	<ul style="list-style-type: none"> WAN/LAN1 port for connecting to an Ethernet network through a switch or a router.
LAN2 Port	<ul style="list-style-type: none"> LAN2 port for connecting to a local Ethernet network through a switch or a router.
System Fan	<ul style="list-style-type: none"> System fan that exhausts heat from the unit.
Power Connector	<ul style="list-style-type: none"> Connect the included power cords to this connector.
Reset Button	<ul style="list-style-type: none"> Resets the NVR22. Pressing and holding the Reset button on the back for 5 seconds will reset your network setting and password, and turn off Jumbo Frame Support.

NVR42:

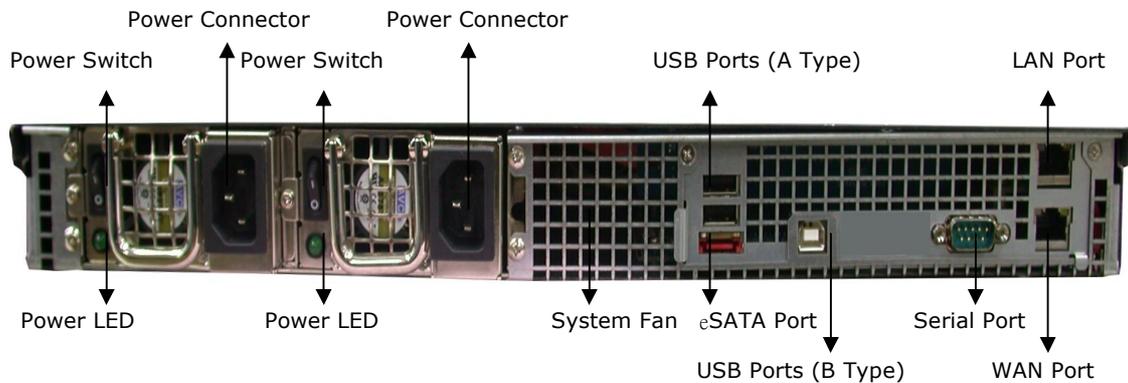
The NVR42 rear panel features ports and connectors.



Item	Description
Power Connector	<ul style="list-style-type: none"> For connect the power adaptor
WAN Port	<ul style="list-style-type: none"> WAN port for connecting to an Ethernet network through a switch or router
LAN Port	<ul style="list-style-type: none"> LAN port for connecting to an Ethernet network through a switch or router
USB Ports	<ul style="list-style-type: none"> USB 2.0 ports for storage expansion
eSATA Ports	<ul style="list-style-type: none"> eSATA port for high-speed storage expansion

NVR46R:

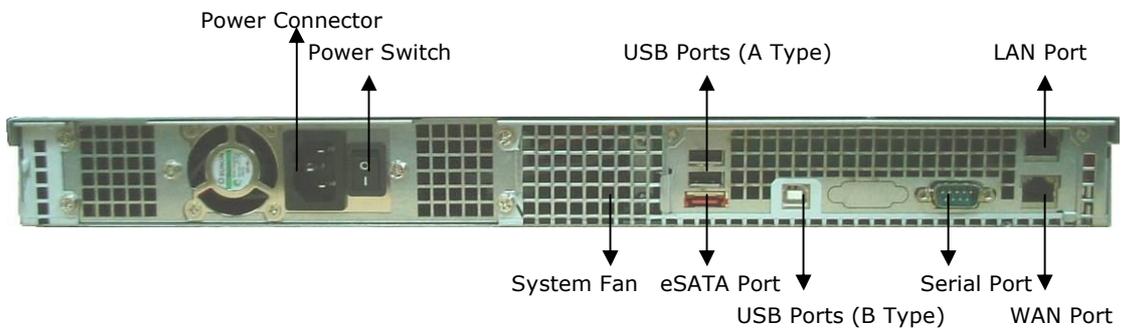
The rear panel of the NVR46R houses most of the USB and Ethernet connections, as well as the eSATA port, system fan, and power connector. See the table below for descriptions of each:



NVR46 Back Panel	
Item	Description
eSATA Port	• eSATA port for high-speed storage expansion
USB Ports	• USB 2.0 ports for compatible USB devices, such as digital cameras, and USB disks
WAN Port	• WAN port for connecting to an Ethernet network through a switch or router
LAN Port	• LAN port that can be used for connection sharing
Power Switch	• Switch for power supply
System Fan	• System fan that exhausts heat from the unit
Serial Port	• This port is for factory use only
Power Connector	• Connect the included power cords to these connectors

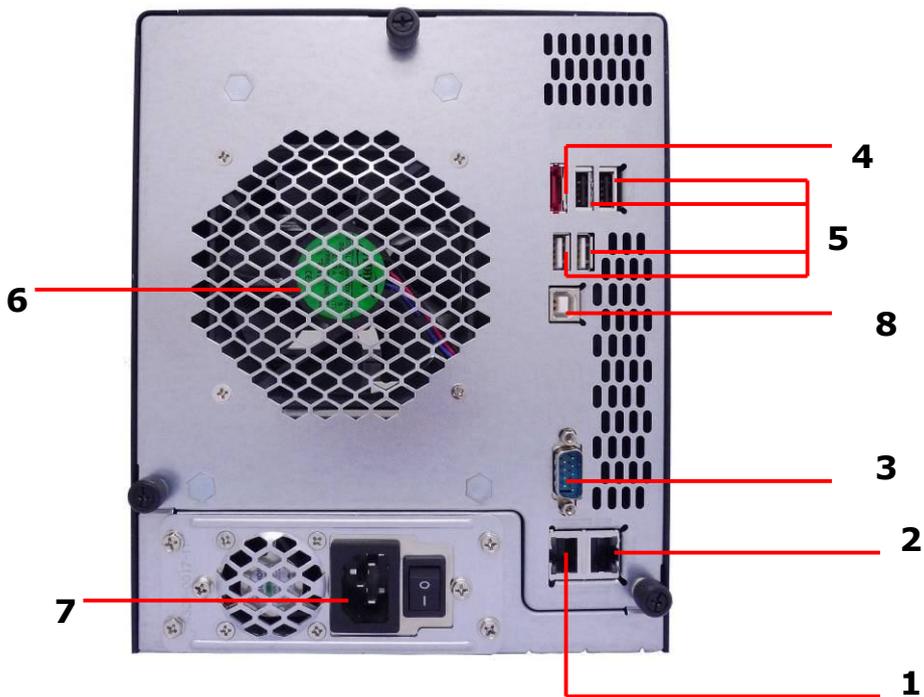
NVR46S:

The rear panel of the NVR46S is similar to the NVR46R, but with a single power connector:



NVR55:

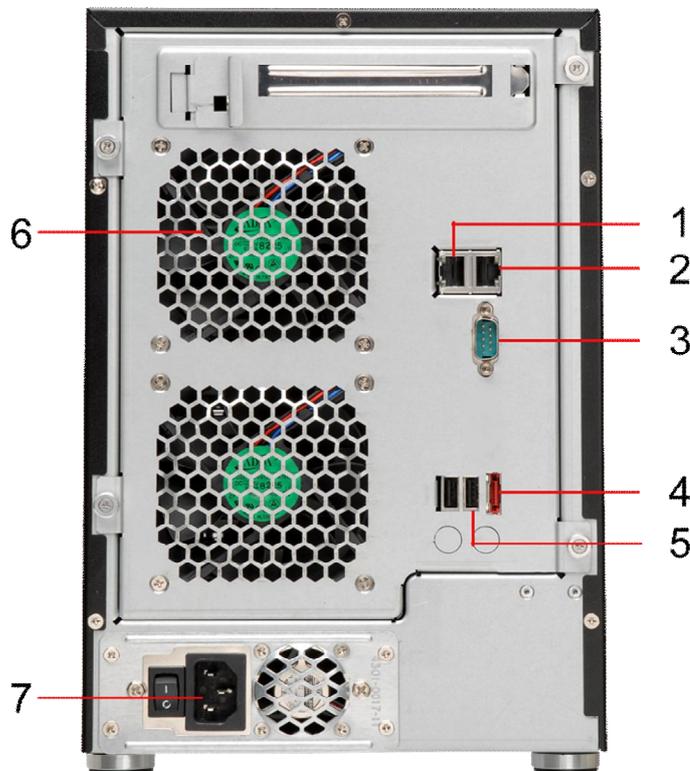
The NVR55 rear panel features ports and connectors.



Back Panel	
Item	Description
1.WAN Port	• WAN port for connecting to an Ethernet network through a switch or router
2.LAN Port	• LAN port for connecting to an Ethernet network through a switch or router
3.Serial Port	• This port is for external UPS device
4.eSATA Port	• eSATA port for high-speed storage expansion
5.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks.
6.System Fan	• System fan that exhausts heat from the unit
7.Power Connector	• Connect the included power cords to these connectors
8.USB Port	• USB 2.0 port to connect PC (Type B of target mode)

NVR77:

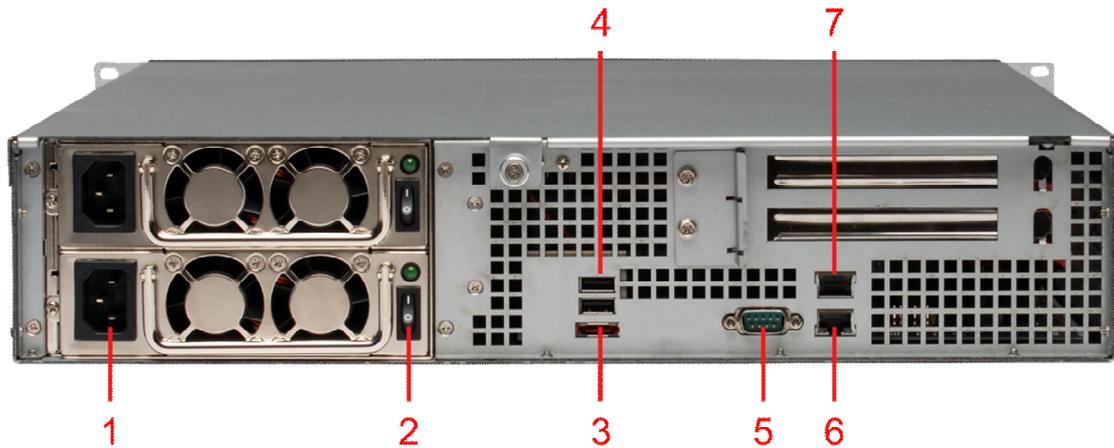
The NVR77 rear panel features ports and connectors.



Back Panel	
Item	Description
1.LAN Port	• LAN port for connecting to an Ethernet network through a switch or router
2.WAN Port	• WAN port for connecting to an Ethernet network through a switch or router
3.Serial Port	• This port is for external UPS device
4.eSATA Port	• eSATA port for high-speed storage expansion
5.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks.
6.System Fan	• System fan that exhausts heat from the unit
7.Power Connector	• Connect the included power cords to these connectors

NVR88:

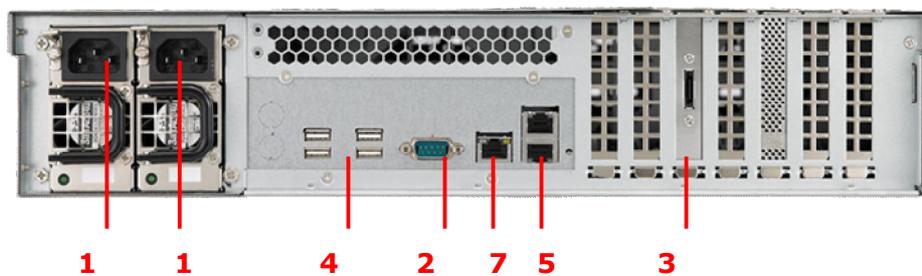
The NVR88 rear panel features ports and connectors.



Back Panel	
Item	Description
1.Power Connector	• Connect the included power cords to these connectors
2.Power Switch	• Switch for power supply
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks.
5.Serial Port	• This port is for external UPS device
6.WAN Port	• WAN port for connecting to an Ethernet network through a switch or router
7.LAN Port	• WAN port for connecting to an Ethernet network through a switch or router

NVR120:

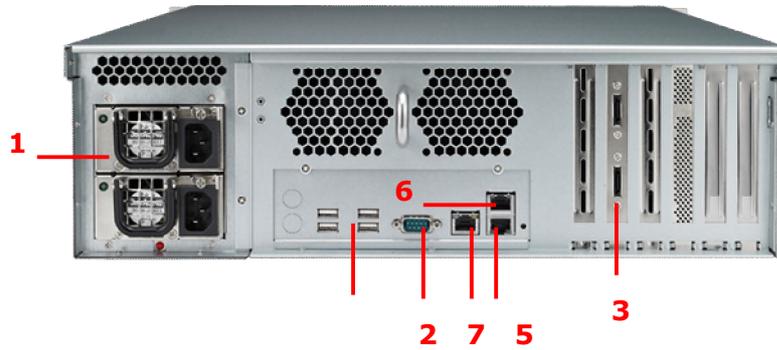
The NVR120 rear panel features ports and connectors.



Back Panel	
Item	Description
1.Power Connector	• Connect the included power cords to these connectors
2.Serial Port	• This port is for external UPS device
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks
5.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
6.LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
7.LAN3 Port	• LAN3 port .(No function)

NVR160:

The NVR160 rear panel features ports and connectors.



Back Panel	
Item	Description
1.Power Connector	• Connect the included power cords to these connectors
2.Serial Port	• This port is for external UPS device
3.eSATA Port	• eSATA port for high-speed storage expansion
4.USB Port	• USB 2.0 port for compatible USB devices, such as USB disks
5.WAN/LAN1 Port	• WAN/LAN1 port for connecting to an Ethernet network through a switch or router
6.LAN2 Port	• LAN2 port for connecting to an Ethernet network through a switch or router
7.LAN3 Port	• LAN3 port . (No function)

Chapter 2: Hardware Installation

Overview

Your Thecus VisoGuard NVR is designed for easy installation. To help you get started, the following chapter will help you quickly get your Thecus VisoGuard NVR up and running. Please read it carefully to prevent damaging your unit during installation.

Before You Begin

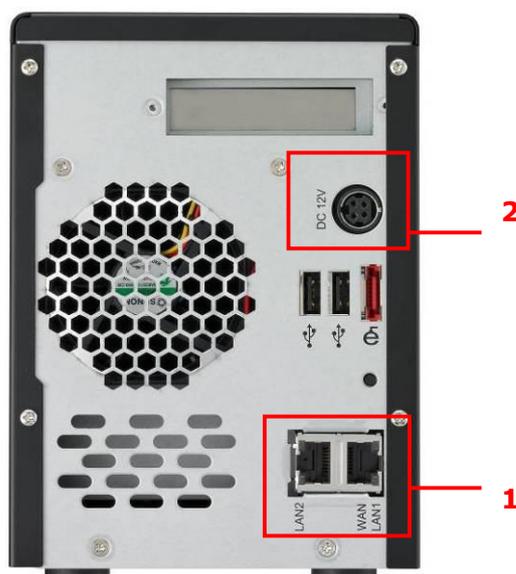
Before you begin, be sure to take the following precautions:

1. Read and understand the **Safety Warnings** outlined in the beginning of the manual.
2. If possible, wear an anti-static wrist strap during installation to prevent static discharge from damaging the sensitive electronic components on the Thecus VisoGuard NVR.
3. Be careful not to use magnetized screwdrivers around the Thecus VisoGuard NVR's electronic components.

Cable Connections

NVR22:

To connect the NVR22 to your network, follow the steps below:



1. Connect an Ethernet cable from your network to the WAN/LAN1 port on the back panel of the NVR22.
2. Connect the provided power cord into the power socket on the back panel. Plug the other end of the cord into a surge protected socket.



3. Press the power button to boot up the NVR22.

NVR42:

To connect the NVR42 to your network, follow the steps below:

1. Connect an Ethernet cable from your network to the WAN port on the back panel of the NVR42.



2. Connect the provided power cord into the universal power socket on the back panel. Plug the other end of the cord into a surge protector socket.



3. Press the power button on the Front Panel to boot up the NVR42.



NVR46:

The NVR46 supports four standard 3.5" Serial ATA (SATA) hard disks. To install a hard disk into the NVR46, follow the steps below:

1. Remove a hard disk tray from the NVR46.
2. Slide the new SATA hard disk into the tray and fasten the screws.
3. Insert the hard disk and tray back into the NVR46 until it snaps into place and lock it with a key if desired.
4. The LED blinks green when the hard disk is accessed. If the Error LED flashes red it signals a problem.

To connect the NVR46 to your network, follow the steps below:

1. Connect an Ethernet cable from your network to the WAN port on the back panel of the NVR46.



2. Connect the provided power cord into the universal power socket on the back panel. Plug the other end of the cord into a surge protector socket. Press the power supply switch to turn on the power supply.

NOTE

If you are installing the NVR46R, be sure to connect both power cables. If you do not, the system will assume one power supply has failed, and an alarm will sound. For more information, refer to Chapter 8: Troubleshooting.



Press the power button on the Front Panel to boot up the NVR46.

NVR55:

The NVR55 supports five standard 3.5" Serial ATA (SATA) hard disks. To install a hard disk into the NVR55, follow the steps below:

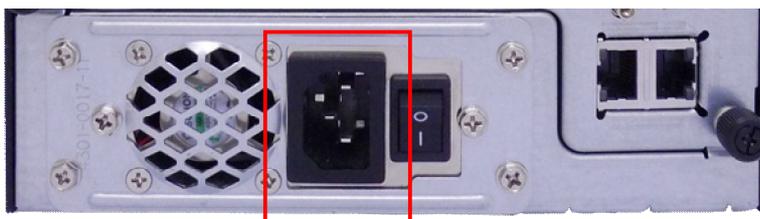
1. Remove a hard disk tray from the NVR55.
2. Slide the new SATA hard disk into the tray and fasten the screws.
3. Insert the hard disk and tray back into the NVR55 until it snaps into place and lock it with a key if desired.
4. The LED blinks green when the hard disk is accessed.

To connect the NVR55 to your network, follow the steps below:

1. Connect an Ethernet cable from your network to the WAN port on the back panel of the NVR55.



2. Connect the provided power cord into the universal power socket on the back panel. Plug the other end of the cord into a surge protector socket. Press the power supply switch to turn on the power supply.



3. Press the power button on the Front Panel to boot up the NVR55.



NVR77:

The NVR77 supports seven standard 3.5" Serial ATA (SATA) hard disks. To install a hard disk into the NVR77, follow the steps below:

1. Remove a hard disk tray from the NVR77.
2. Slide the new SATA hard disk into the tray and fasten the screws.
3. Insert the hard disk and tray back into the NVR77 until it snaps into place and lock it with a key if desired.
4. The LED blinks green when the hard disk is accessed.

NOTE

If your HDD was part of a RAID 1, RAID 5 or RAID 6 array previously, it automatically rebuilds. If you replace all the drives with higher capacity drives, you will need to go to Administrator login and format the drives.

To connect the NVR77 to your network, follow the steps below:

1. Connect an Ethernet cable from your network to the WAN port on the back panel of the NVR77.



2. Connect the provided power cord into the universal power socket on the back panel. Plug the other end of the cord into a surge protector socket. Press the power supply switch to turn on the power supply.



3. Press the power button on the Front Panel to boot up the NVR77.



NVR88:

The NVR88 supports eight standard 3.5" SATA hard disks. To install a hard disk into the NVR88, follow the steps below:

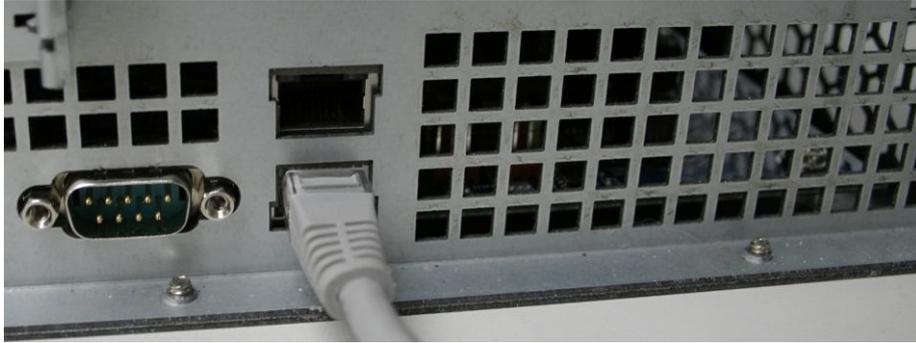
1. Remove a hard disk tray from the NVR88.
2. Slide the new SATA hard disk into the tray and fasten the screws.
3. Insert the hard disk and tray back into the NVR88 until it snaps into place and lock it with a key if desired.
4. The LED blinks green when the hard disk is accessed.

NOTE

If your HDD was part of a RAID 1, RAID 5 or RAID 6 array previously, it automatically rebuilds. If you replace all the drives with higher capacity drives, you will need to go to Administrator login and format the drives.

To connect the NVR88 to your network, follow the steps below:

1. Connect an Ethernet cable from your network to the WAN port on the back panel of the NVR88.



2. Connect the provided power cord into the universal power socket on the back panel. Plug the other end of the cord into a surge protector socket. Press the power supply switch to turn on the power supply.



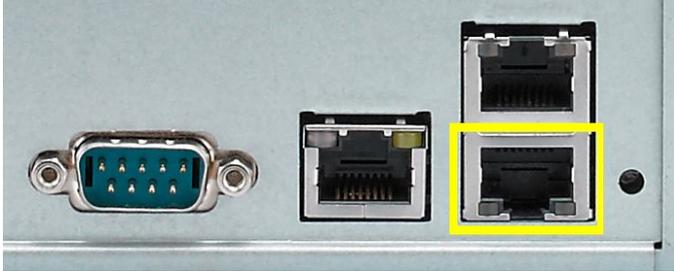
3. Press the power button on the Front Panel to boot up the NVR88.



NVR120/NVR160:

To connect the NVR120/NVR160 products to your network, follow the steps below:

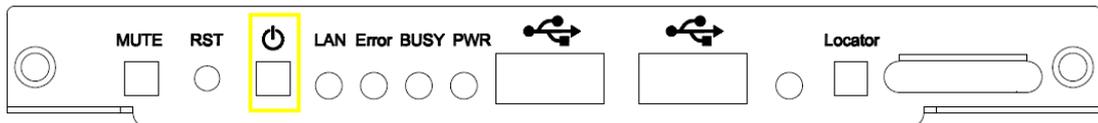
1. Connect an Ethernet cable from your network to the WAN/LAN1 port on the back panel of the NVR120/NVR160.



2. Connect the provided power cord into the universal power socket on the back panel. Plug the other end of the cord into a surge protector socket.



3. Press the power button on the Front Panel to boot up the NVR120/NVR160.



Chapter 3: First Time Setup

Overview

Once the hardware is installed, physically connected to your network, and powered on, you can configure the Thecus VisoGuard NVR so that it is accessible to your network users. There are two ways to set up your Thecus VisoGuard NVR: using the **Thecus Setup Wizard** or the **LCD display**. Follow the steps below for initial software setup.

Thecus Setup Wizard

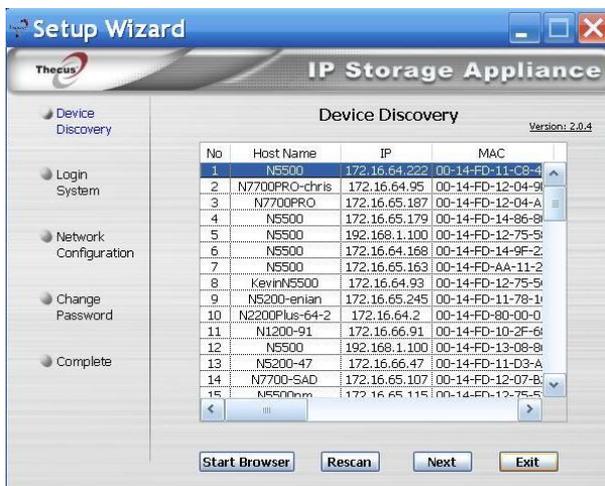
The handy Thecus Setup Wizard makes configuring Thecus VisoGuard NVR a snap. To configure the Thecus VisoGuard NVR using the Setup Wizard, perform the following steps:

1. Insert the installation CD into your CD-ROM drive (the host PC must be connected to the network).

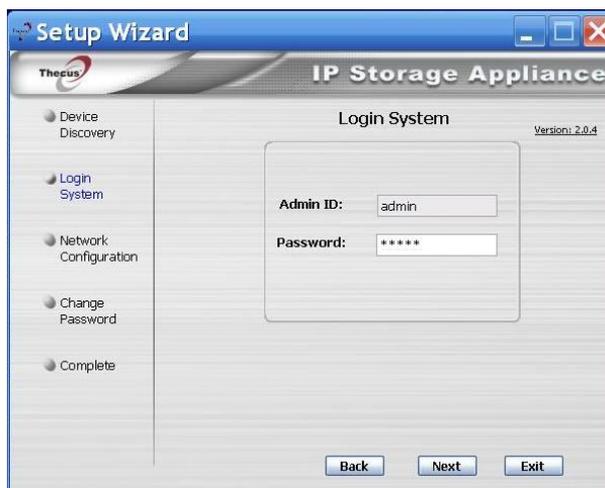
- The Setup Wizard should launch automatically. If not, please browse your CD-ROM drive and double click on **Setup.exe**.



- The Setup Wizard will start and automatically detect all Thecus storage devices on your network.



- Select the Thecus VisoGuard NVR that you like to configure.
- Login with the administrator account and password. The default account and password are both "admin".



- Name your Thecus VisoGuard NVR and configure the network IP address. If your switch or router is configured as a DHCP Server, configuring the Thecus VisoGuard NVR to automatically obtain an IP address is recommended. You may also use a static IP address and enter the DNS Server address manually.



7. Change the default administrator password.



8. Finished! Access the Thecus VisoGuard NVR Web Administrator Interface by pressing the **Start Browser** button. You can also configure another Thecus VisoGuard NVR at this point by clicking the **Setup Other Device** button. Press **Exit** to exit the wizard.



NOTE

The Thecus Setup Wizard is designed for installation on systems running Windows XP/2000/vista/7. Users with other operating systems will need to install the Thecus Setup Wizard on a host machine with one of these operating systems before using the unit.

LCD Operation

The Thecus VisoGuard NVR is equipped with an LCD on the front for easy status display and setup. There are four buttons on the front panel to control the LCD functions.

NVR42:

OLED Operation

The NVR42 is equipped with an OLED on the front for easy status display and setup. There are four buttons on the front panel to control the OLED functions.

OLED Controls

Use the **Up** (▲), **Down** (▼), **Enter** (↵) and **Escape** (ESC) keys to select various configuration settings and menu options for NVR42 configuration.

The following table illustrates the keys on the front control panel:

OLED Controls

Icon	Function	Description
▲	Up Button	Select the previous configuration settings option.
▼	Down Button	USB copy confirmation display.
↵	Enter	Enter the selected menu option, sub-menu, or parameter setting.
ESC	Escape	Escape and return to the previous menu.

There are two modes of operation for the OLED: **Display Mode** and **Management Mode**.

Display Mode

During normal operation, the OLED will be in **Display Mode**.

Display Mode	
Item	Description
Host Name	Current host name of the system.
WAN	Current WAN IP setting.
LAN	Current LAN IP setting.
Link Aggregation	Current Link Aggregation status
System Fan	Current system fan status.
CPU Fan	Current CPU fan status
2009/05/22 12:00	Current system time.
RAID	Current RAID status.

The NVR42 will rotate these messages every one-two seconds on the OLED display.

NVR55/NVR46/NVR77/NVR88:

LCD Controls

Use the **Up** (▲), **Down** (▼), **Enter** (↵) and **Escape** (ESC) keys to select various configuration settings and menu options for Thecus VisoGuard NVR configuration.

The following table illustrates the keys on the front control panel:

LCD Controls		
Icon	Function	Description
▲	Up Button	Select the previous configuration settings option.
▼	Down Button	USB copy confirmation display.
↵	Enter	Enter the selected menu option, sub-menu, or parameter setting.
ESC	Escape	Escape and return to the previous menu.

There are two modes of operation for the LCD: **Display Mode** and **Management Mode**.

Display Mode

During normal operation, the LCD will be in **Display Mode**.

Display Mode	
Item	Description
Host Name	Current host name of the system.
WAN/LAN1	Current WAN/LAN1 IP setting.
LAN2	Current LAN2 IP setting.
Link Aggregation	Current Link Aggregation status
System Fan1	Current system fan1 status.
System Fan2	Current system fan2 status.
CPU Fan	Current CPU fan status
2009/05/22 12:00	Current system time.
Disk Info	Current status of disk slot has been installed
RAID	Current RAID status.

The Thecus VisoGuard NVR will rotate these messages every one-two seconds on the LCD display.

USB Copy

The USB Copy function enables you to copy files stored on USB devices such as USB disks and digital cameras to the Thecus VisoGuard NVR by press button. To use USB copy, follow the steps below:

1. Plug your USB device into an available USB port on the Front end.
2. In **Display Mode**, press the **Down Button** (▼).
3. The LCD will display "USB Copy?"
4. Press **Enter** (↵) and the Thecus VisoGuard NVR will start copying USB disks connected to the front USB port.
5. All of data will be copied into system folder named "USB copy".

Management Mode

During setup and configuration, the LCD will be in **Management Mode**.

To enter into Management Mode, press **Enter (↵)** and an "Enter Password" prompt will show on the LCD.

At this time, the administrator has to enter the correct LCD password. System will check whether the correct LCD password has been entered. The default LCD password is "0000". If correct password is entered, you will enter into the **Management Mode** menu.

Management Mode	
Item	Description
WAN Setting	IP address and netmask of your WAN ports.
LAN Setting	IP address and netmask of your LAN ports.
Link Agg. Setting	Select Disable or Failover .
Change Admin Passwd	Change administrator's password for LCD (OLED) operation.
Reset to Default	Reset system to factory defaults.
Exit	Exit Management Mode and return to Display Mode .

NOTE

You can also change your LCD password using the Web Administration Interface by navigating to **System Management > Administrator Password**. For more on the Web Administration Interface, see **Chapter 4: System Management**.

NVR120/NVR160:

OLED Operation

The NVR120/NVR160 is equipped with an OLED on the front for easy status display and setup. There are four buttons on the front panel to control the OLED functions.

OLED Controls

Use the **Up (▲)**, **Down (▼)**, **Enter (↵)** and **Escape (ESC)** keys to select various configuration settings and menu options for NVR120/NVR160 configuration.

The following table illustrates the keys on the front control panel:

OLED Controls		
Icon	Function	Description
▲	Up Button	Select the previous configuration settings option.
▼	Down Button	USB copy confirmation display.
↵	Enter	Enter the selected menu option, sub-menu, or parameter setting.
ESC	Escape	Escape and return to the previous menu.

There are two modes of operation for the OLED: **Display Mode** and **Management Mode**.

Display Mode

During normal operation, the OLED will be in **Display Mode**.

Display Mode	
Item	Description
Host Name	Current host name of the system.
WAN/LAN1	Current WAN/LAN1 IP setting.
LAN2	Current LAN2 IP setting.
Link Aggregation	Current Link Aggregation status
System Fan	Current system fan status.
CPU Fan	Current CPU fan status
2009/05/22 12:00	Current system time.
RAID	Current RAID status.

The NVR120/NVR160 will rotate these messages every one-two seconds on the OLED display.

Typical Setup Procedure

From the Web Administration Interface, you can begin to setup your Thecus VisoGuard NVR for use on your network. Setting up the Thecus VisoGuard NVR typically follows the five steps outlined below.

For more on how to use the Web Administration Interface, see **Chapter 4: Web Administration Interface**.

Step 1: Network Setup

From the Web Administration Interface, you can configure the network settings of the Thecus VisoGuard NVR for your network. You can access the **Network** menu from the menu bar.

For details on how to configure your network settings, refer to **Chapter 4: System Network**.

Step 2: RAID Creation

Next, administrators can configure their preferred RAID setting and build their RAID volume. You can access RAID settings from the menu bar of the Web Administration Interface by navigating to **Storage Management > RAID Configuration**.

For more information on configuring RAID, see **Chapter 4: System Management > RAID Configuration**.

Don't know which RAID level to use? Find out more about the different RAID levels from **Appendix B: RAID Basics**.

Step 3: Create Local Users or Setup Authentication

Once the RAID is ready, you can begin to create local users for Thecus VisoGuard NVR.

For more on managing users, go to **Chapter 4: User and Group Authentication**.

Step 4: Create Folders and Set Up ACLs

Once users are introduced into your network, you can begin to create various folders on the Thecus VisoGuard NVR and control user access to each using Folder Access Control Lists.

More information on managing folders, see **Chapter 4: Storage Management > Share Folder** .

To find out about configuring Folder Access Control Lists, see **Chapter 4: Storage Management > Share Folder > Folder Access Control List (ACL)**.

Step 5: Start Services

Finally, you can start to setup the different services of Thecus VisoGuard NVR for the users on your network. You can find out more about each of these services by clicking below:

[SMB/CIFS](#)

[File Transfer Protocol \(FTP\)](#)

Chapter 4: System Administration

Overview

The Thecus VisoGuard NVR provides an easily accessible **Web Administration Interface**. With it, you can configure and monitor the Thecus VisoGuard NVR anywhere on the network.

Web Administration Interface

Make sure your network is connected to the Internet. To access Thecus VisoGuard NVR **Web Administration Interface**:

1. Type the Thecus VisoGuard NVR IP address into your browser. (Default IP address is `http://192.168.1.100`)



NOTE

Your computer's network IP address must be on the same subnet as the Thecus NVR. If the Thecus NVR has default IP address of 192.168.1.100, your managing PC IP address must be 192.168.1.x, where x is a number between 1 and 254, but not 100.

NOTE

This page can be displayed with Flash or with HTML. Choose **Flash** for Flash (shown in the top figure) and **Traditional** for HTML (shown in the bottom figure).

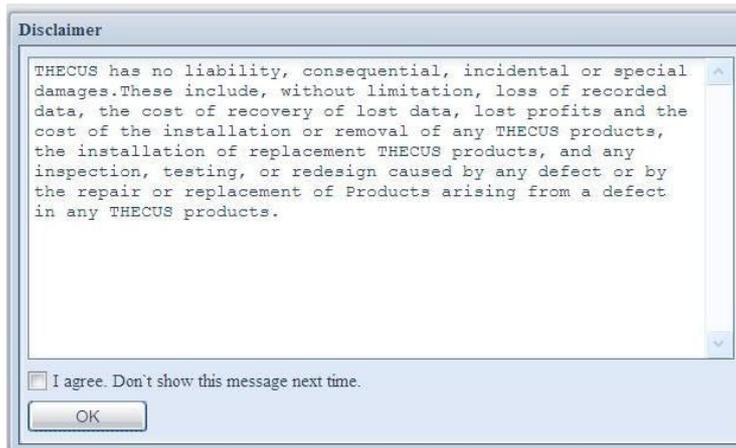
2. Login to the system using the administrator user name and password. The factory defaults are:

User Name: admin

Password: admin

- ※ If you changed your password in the setup wizard, use the new password.

Once you are logged in as an administrator disclaimer page will appear as below. Please click the check box if you do not want to have this page displayed during the next login.



Following by disclaim page, you will see the **Web Administration Interface**. From here, you can configure and monitor virtually every aspect of the Thecus VisoGuard NVR from anywhere on the network.

My Favorite

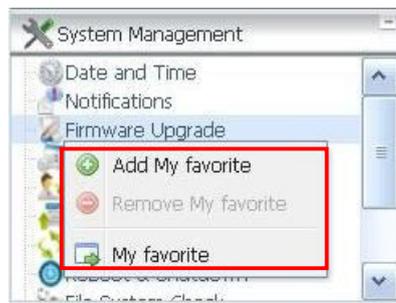
The user interface with "My Favorite" shortcut is allowed user to designate often used items and have them display on the main screen area. The figure below displays 12 default favorite functions.



Administrators can add or remove favorite functions to My Favorites by right clicking the mouse on the menu tree.



The other way administrators can add favorite functions is by clicking the "Add Favorite" icon in each function screen. Please refer figure below in red circuit icon.

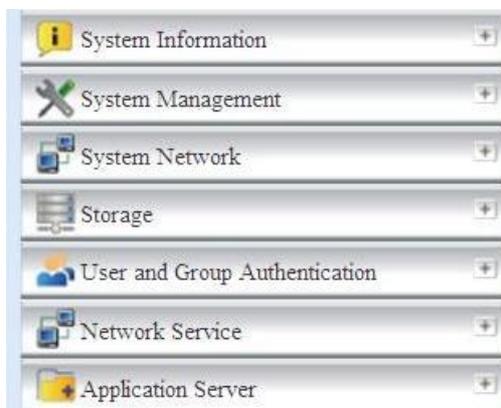


To return to the favorite screen, simply click "Home" located at the left hand corner of the main screen.



Menu Bar

The **Menu Bar** is where you will find all of the information screens and system settings of Thecus VisoGuard NVR. The various settings are placed in the following groups on the menu bar:



Menu Bar	
Item	Description
System Information	Current system status of the Thecus VisoGuard NVR.
System Management	Various Thecus VisoGuard NVR system settings and information.
System Network	Information and settings for network connections, as well as various services of the Thecus VisoGuard NVR.
Storage	Information and settings for storage devices installed into the Thecus VisoGuard NVR.
User and Group Authentication	Allows configuration of users and groups.
Network Service	Setup and manage protocols such as Samba/CIFS and FTP.
Application Server	Module Installation of the Thecus VisoGuard NVR.

Moving your cursor over any of these items will display the dropdown menu selections for each group.

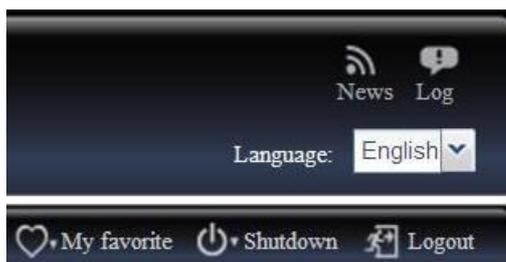
In the following sections, you will find detailed explanations of each function, and how to configure your Thecus VisoGuard NVR.

Message Bar

You can get information about system status quickly by moving mouse over.



Message Bar		
Item	Status	Description
	RAID Information.	Display the status of created RAID volume. Click to go to RAID information page as short cut.
	Disks Information.	Display the status of disks installed in the system. Click to go to Disk information page as short cut.
	FAN.	Display system FAN Status. Click to go to System Status page as short cut.
	Network.	Green: The system is connected to the Internet. Red: The system is unable to connect to the Internet.



- **News**

Accesses online registration and the latest release news.

- **Log**

Accesses the system log. New logs will be displayed with an icon here.

- **Language Selection**

The Thecus VisoGuard NVR supports multiple Languages, including:

English,Japanese,Traditional Chinese,Simplified Chinese,French,German,Italian, Korean,Spanish,Russia,Polish,Portugal

On the menu bar, click Language and the selection list appears. This user interface will switch to selected Language for Thecus VisoGuard NVR.

- **My Favorite**

Add/Remove the current page from the Home page.

- **Shutdown**

Choose **Shutdown** or **Reboot** from the dropdown menu to shutdown or reboot your VisoGuard NVR.

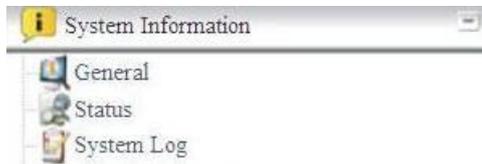
- **Logout**

Click to log out of Web Administration Interface.

System Information

Information provides viewing on current Product info, System Status, Service Status and Logs.

The menu bar allows you to see various aspects of the Thecus VisoGuard NVR. From here, you can discover the status of the Thecus VisoGuard NVR, and also other details.



General Information

Once you login, you will first see the basic **Product Information** screen providing **Manufacturer**, **Product No.**, **Firmware Version**, and **System Up Time** information.

Product Information	
Manufacturer	Thecus
Product No.	NVR160
Firmware Version	5.0.3
Up Time	20 minutes

Product Information	
Item	Description
Manufacturer	Displays the name of the system manufacturer.
Product No.	Shows the model number of the system.
Firmware version	Shows the current firmware version.
Up time	Displays the total run time of the system.

System/Service Status

From the **Status** menu, choose the **System** item, **System Status** and **Service Status** screens appear. These screens provide basic system and service status information.

System Status	
CPU Activity	15%
CPU Fan Speed	OK
System Fan 1 Speed	OK
Up Time	3 Days 9 Hours 11 Minutes

Service Status	
AFP Status	Stopped
NFS Status	Stopped
SMB/CIFS Status	Running
FTP Status	Stopped

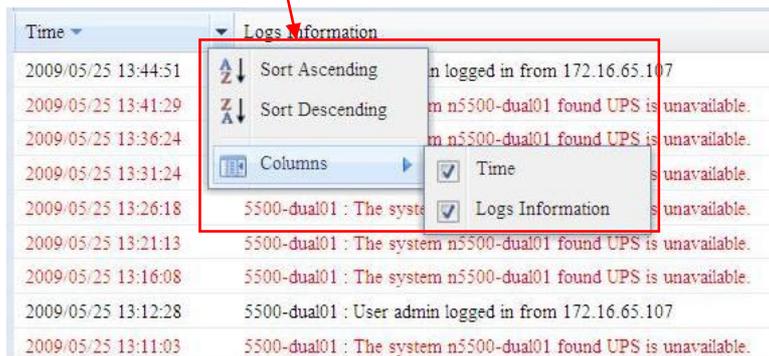
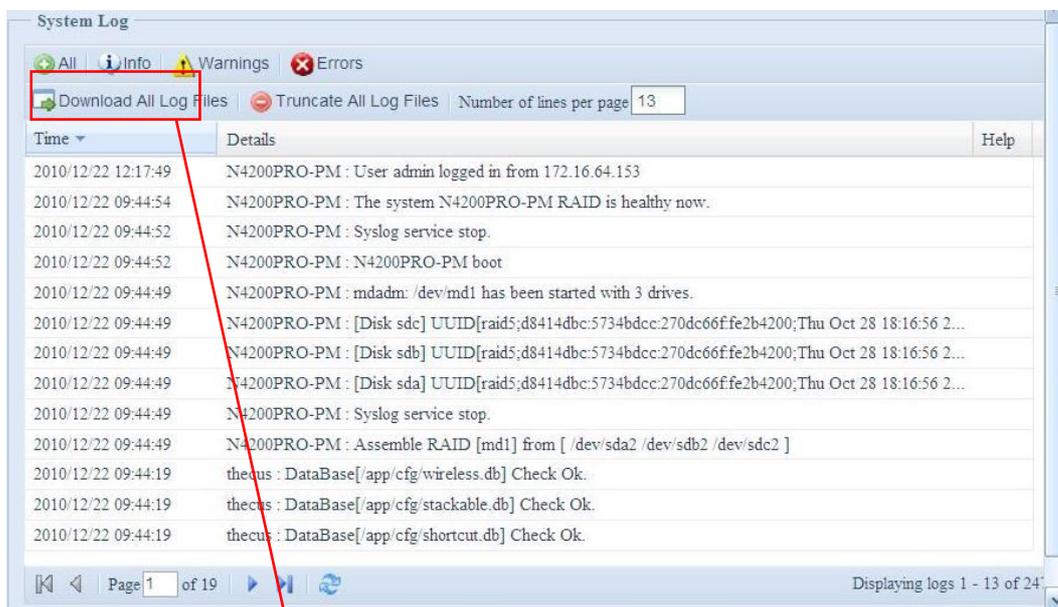
System Status	
Item	Description
CPU Activity (%)	Displays current CPU workload of the Thecus VisoGuard NVR.

CPU Fan Speed	Displays current CPU fan status.
System Fan Speed	Displays the current status of the system fan.
Up Time	Shows how long the system has been up and running.

Service Status	
Item	Description
SMB/CIFS Status	The status of the SMB/CIFS server.
FTP Status	The status of the FTP server.

Logs

From the **System Information** menu, choose the **Logs** item and the **System Logs** screen appears. This screen shows a history of system usage and important events such as disk status, network information, and system booting. See the following table for a detailed description of each item:



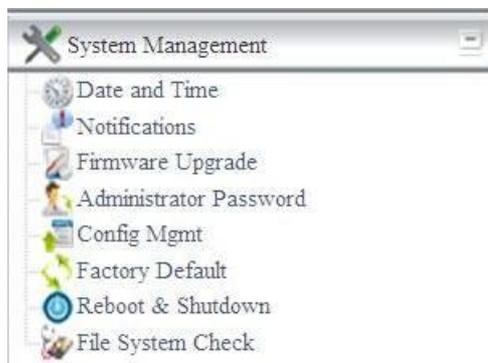
See the following table for a detailed description of each item:

System Logs	
Item	Description
All	Provides all log information including system messages, warning messages and error messages.
INFO	Records information about system messages.
WARN	Shows only warning messages.
ERROR	Shows only error messages.

Download All Log File	Export all logs to an external file.
Truncate All Log File	Clear all log files.
The number of lines per page <input type="checkbox"/>	Specify desired number of lines to display per page.
Sort Ascending	Shows logs by date in ascending order.
Sort Descending	Shows logs by date in descending order.
<< < > >>	Use the forward (> >>) and backward (<< <) buttons to browse the log pages.
	Re-loading logs.

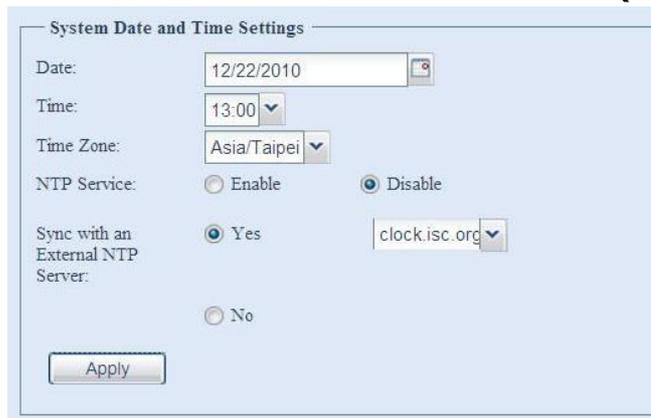
System Management

The **System Management** menu gives you a wealth of settings that you can use to configure your Thecus VisoGuard NVR system administration functions. You can set up system time, system notifications, and even upgrade firmware from this menu.



Date and Time: System Date and settings

From the **Date and time** menu, choose the item and the screen appears. Set the desired **Date**, **Time**, and **Time Zone**. You can also elect to synchronize the system time on Thecus VisoGuard NVR with an **NTP (Network Time Protocol) Server**.



See the following table for a detailed description of each item:

Time	
Item	Description
Date	Sets the system date.
Time	Sets the system time.
Time Zone	Sets the system time zone.
NTP Server	Select Enable to synchronize with the NTP server. Select Disable to close the NTP server synchronization.

Sync with external NTP Server	Select YES to allow Thecus VisoGuard NVR to synchronize with an NTP server of your choice. Press Apply to change.
-------------------------------	---

WARNING If an NTP server is selected, please make sure your Thecus VisoGuard NVR has been setup to access the NTP server.

Notification configuration

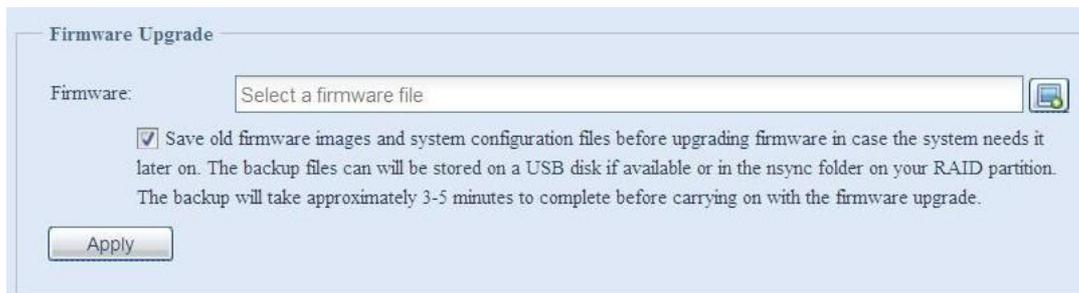
From the menu, choose the **Notification** item, and the **Notification Configuration** screen appears. This screen lets you have Thecus VisoGuard NVR notify you in case of any system malfunction. Press **Apply** to confirm all settings. See following table for a detailed description of each item.

Notification Configuration	
Item	Description
Beep Notification	Enable or disable the system beeper that beeps when a problem occurs.
Email Notification	Enable or disable email notifications of system problems.
SMTP Server	Specifies the hostname/IP address of the SMTP server.
Port	Specifies the port to send outgoing notification emails.
Auth Type	Select the SMTP Server account authentication type.
SMTP Account ID	Set the SMTP Server Email account ID.
Account Password	Enter a new password.
E-mail From	Set email address to send email.
Receiver's E-mail Address (1,2,3,4)	Add one or more recipient's email addresses to receive email notifications.

NOTE Consult with your mail server administrator for email server information.

Firmware Upgrade

From the menu, choose the **Firmware Upgrade** item and the **Firmware Upgrade** screen appears.



Follow the steps below to upgrade your firmware:

1. Use the **Browse** button  to find the firmware file.
2. Press **Apply**.
3. The beeper beeps and the Busy LED blinks until the upgrade is complete.

NOTE

- The beeper only beeps if it is enabled in the System Notification menu.
- Check Thecus website for the latest firmware release and release notes.
- Downgrading firmware is not permitted.

WARNING

Do not turns off the system during the firmware upgrade process. This will lead to a catastrophic result that may render the system inoperable.

NOTE

- Save old firmware images and system configuration files before upgrading firmware in case the system needs it later on. The backup files can will be stored on a USB disk if available or in the nsync folder on your RAID partition. The backup will take approximately 3-5 minutes to complete before carrying on with the firmware upgrade.

Administrator password

From the menu, choose the **Administrator Password** item and the **Change Administrator Password** screen appears. Enter a new password in the **New Password** box and confirm your new password in the **Confirm Password** box. Press **Apply** to confirm password changes.

There is also **password** for enter **LCD** setting you could setup here. Enter a new password in the **New Password** box and confirm your new password in the **Confirm Password** box. Press **Apply** to confirm password changes.

See the following table for a detailed description of each item.

Change Administrator and LCD Entry Password	
Item	Description
New Password	Type in a new administrator password.
Confirm Password	Type the new password again to confirm.
Apply	Press this to save your changes.

Config Mgmt

From the menu, choose the **Config Mgmt** item and the **System Configuration Download/Upload** screen appears. From here, you can download or upload stored system configurations.

See the following table for a detailed description of each item.

System Configuration Download/Upload	
Item	Description
Download	Save and export the current system configuration.
Upload	Import a saved configuration file to overwrite current system configuration.

NOTE

Backing up your system configuration is a great way to ensure that you can revert to a working configuration when you are experimenting with new system settings. The system configuration you have backup can be only restore in same firmware version. And the backup details have excluded user/group accounts.

Factory default

From the menu, choose the **Factory Default** item and the **Reset to Factory Default** screen appears. Press **Apply** to reset Thecus VisoGuard NVR to factory default settings.



WARNING

Resetting to factory defaults will not erase the data stored in the hard disks, but **WILL** revert all the settings to the factory default values.

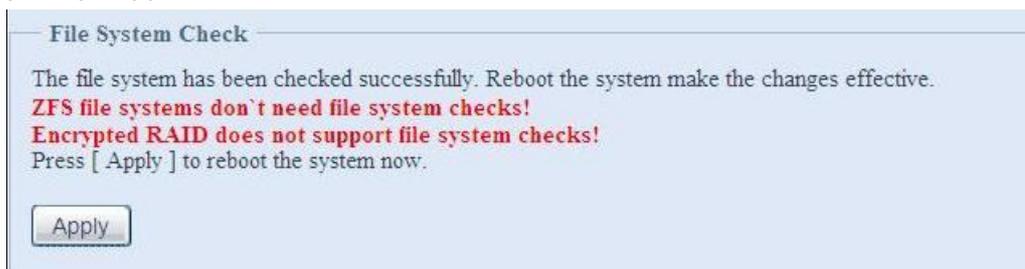
Reboot & Shutdown

From the menu, choose **Reboot & Shutdown** item, and the **Shutdown/Reboot System** screen appears. Press **Reboot** to restart the system or **Shutdown** to turn the system off.



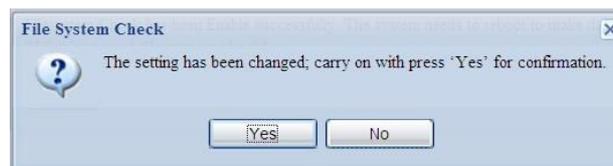
File System check

The File System Check allows you to perform a check on the integrity of your disks' file system. Under the menu, click **File system Check** and the **File System Check** prompt appears.

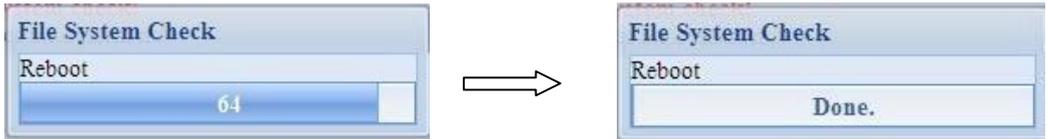


To perform a file system check, click **Apply**.

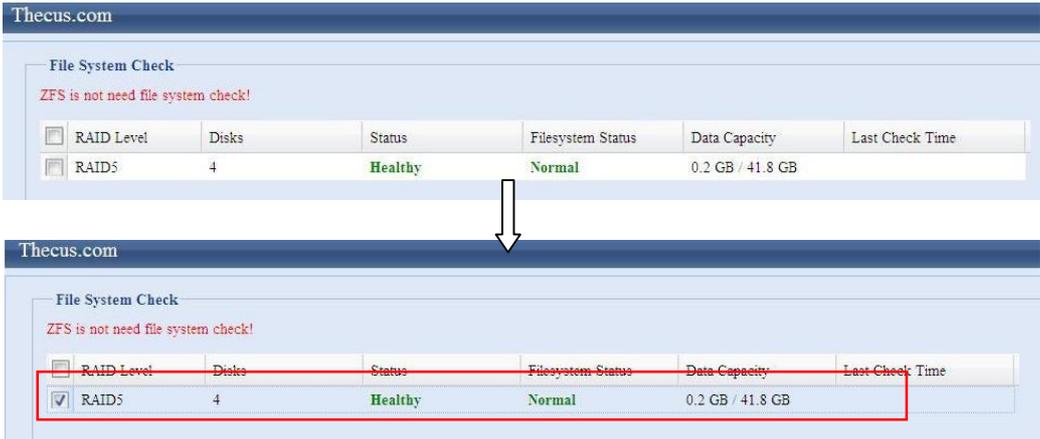
Once clicked, the following prompt will appear:



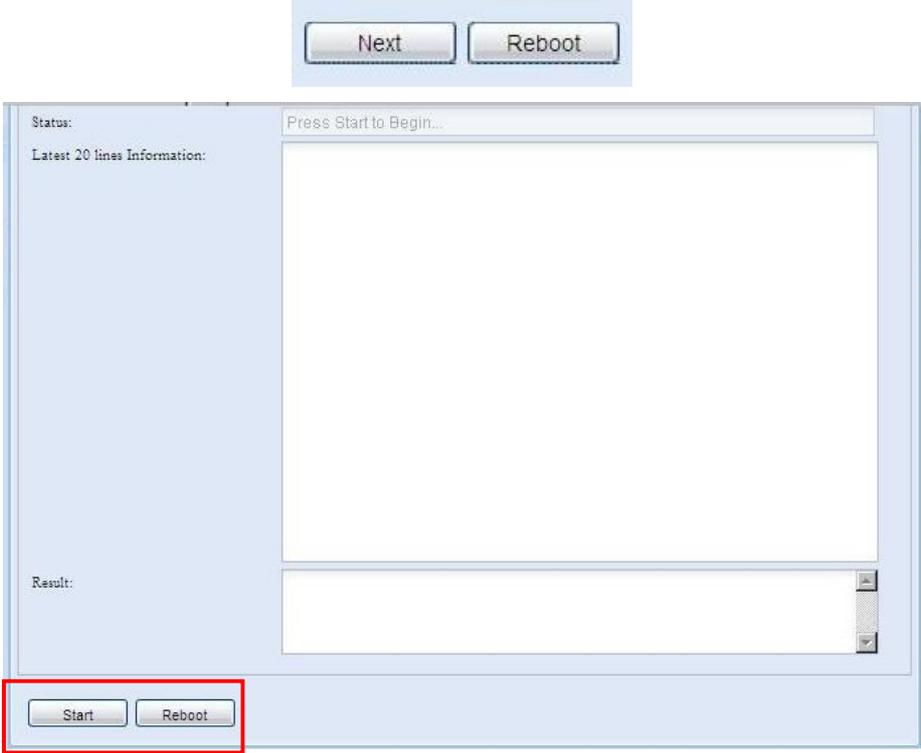
Click **Yes** to reboot the system.



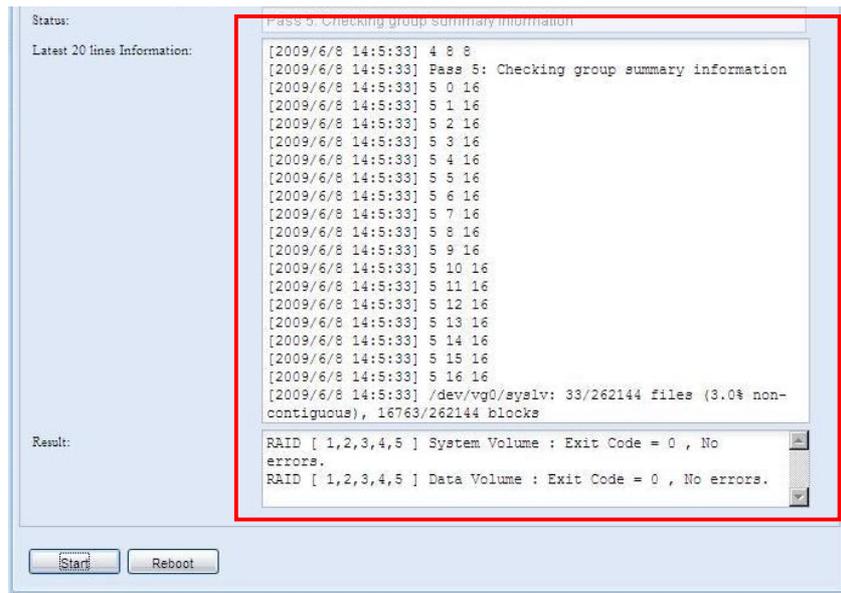
Once the system has rebooted, you will be returned to the **File System Check** prompt. There you will see the available RAID volumes to run the file system check on except ZFS volume, ZFS has no need to perform file system check. Check the desired RAID volumes and click **Next** to proceed with the file system check. Click **Reboot** to reboot without running the check.



Once you click **Next**, you will see the following screen:



Click **Start** to begin the file system check. Click **Reboot** to reboot the system. When the file system check is run, the system will show 20 lines of information until it is complete. Once complete, the results will be shown at the bottom.



NOTE

The system must be rebooted before Thecus VisoGuard NVR can function normally after file system check complete.

UI Login Configuration

Adjusts UI Login Configuration settings. You can enable/disable the Web Disk, Photo Server functions, and VisoGuard according to your needs.

For the Thecus VisoGuard NVR, users need to install the photo server module or web disk module to access these functions.

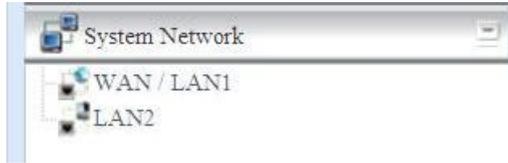


NOTE

Factory default:
 Web Disk and Photo Server are disabled.
 VisoGuard is enabled.

System Network

Use the **System Network** menu to make network configuration settings as well as service support settings.



WAN/LAN1

WAN/LAN1 Configuration

From the **System Network** menu, choose **WAN/LAN1**, and the **WAN/LAN1 Configuration** screen appears. This screen displays the network parameters of the WAN/LAN1 connection. You may change any of these items and press **Apply** to confirm your settings. See a description of each item in the following table:

The screenshot shows the WAN/LAN1 Configuration window with the following fields and values:

- Host Name: NVR160
- Domain Name: thecus.com
- WINS Server 1: (empty)
- WINS Server 2: (empty)
- MAC Address: 00:14:FD:15:59:84
- Link Detected: yes
- Link Speed: 1000Mb/s
- Jumbo Frame Support: Disable (Note: Select from drop down list or input manually, 1501-9018)
- IP Sharing Mode: Enable Disable
- Link Aggregation: Disable
- IP Address Setup:
 - Static (selected) / Dynamic
 - IP: 172.16.64.81
 - Netmask: 255.255.252.0
 - Gateway: 172.16.66.135
 - DNS Server 1: 172.16.66.244
 - DNS Server 2: 168.95.1.1
 - DNS Server 3: (empty)

An Apply button is located at the bottom of the window.

WAN/LAN1 Configuration	
Item	Description
Host name	Host name that identifies the Thecus VisoGuard NVR on the network.
Domain name	Specifies the domain name of Thecus VisoGuard NVR.
WINS Server	To set a server name for NetBIOS computer.
MAC Address	MAC address of the network interface.
Jumbo Frame Support	Enable or disable Jumbo Frame Support of the WAN/LAN1 interface on your Thecus VisoGuard NVR.
IP Sharing Mode	When enabled, PCs connected to the LAN2 port will be able to access the WAN/LAN1.
Link Aggregation	Specifies whether WAN/LAN1 and LAN2 ports will be aggregated and act as one port. There are 1 modes can be choose from: Fail-over
Set IP Address by: Static / Dynamic	You can choose a static IP or Dynamic IP, and input your network configuration
IP	IP address of the WAN/LAN1 interface.
Netmask	Network mask, which is generally: 255.255.255.0

Gateway	Default Gateway IP address.
DNS Server	Domain Name Service (DNS) server IP address.

NOTE

- Only use Jumbo Frame settings when operating in a Gigabit environment where all other clients have Jumbo Frame Setting enabled.
- If you are only using the WAN/LAN1 port, we suggest that you disable IP Sharing Mode. This will result in higher throughput.
- A correct DNS setting is vital to networks services, such as SMTP and NTP.

WARNING

Most Fast Ethernet (10/100) Switches/Routers do not support Jumbo Frame and you will not be able to connect to your Thecus VisoGuard NVR after Jumbo Frame is turned on. If this happens, turn off the Thecus VisoGuard NVR. Then, insert USB disk with factory reset utility included and power on the Thecus VisoGuard NVR. Till the system power on complete then it will bring your system settings back to factory default.

LAN2

LAN2 Configuration

The Thecus VisoGuard NVR supports two Gigabit Ethernet ports for higher service availability. To configure these ports, choose **LAN2** from the **System Network** menu, and the **LAN2 Configuration** screen appears. Press **Apply** to save your changes.

LAN2 Configuration	
Item	Description
MAC Address	Displays the MAC address of the LAN2 interface.
Jumbo Frame Support	Enable or disable Jumbo Frame Support on the LAN2 interface.
IP	Specifies the IP address of the LAN2 interface.
Netmask	Specifies the Network Mask of the LAN2 interface.
Gateway	When Thecus VisoGuard NVR as a DHCP server from LAN2, it can have another route to balance traffic bandwidth for its DHCP clients
Link Detected	Specifies the LAN2 port link status
Link Speed	Specifies the LAN2 port link speed

NOTE

Before enabling Jumbo Frame Support, please make sure your network equipment supports Jumbo Frame. If your equipment is incompatible, you might not be able to connect to your Thecus VisoGuard NVR.

NOTE

If the IP sharing mode setting is set to "Enable" under WAN/LAN1 port, then this 2nd gateway cannot be configured.

DHCP Server Configuration

A DHCP server can be configured to assign IP addresses to devices connected to the LAN2 port. To configure these ports, choose **LAN2** from the **System Network** menu.

DHCP Configuration	
Item	Description
DHCP Server	Enable or disable the DHCP server to automatically assign IP address to PCs connected to the LAN2 interface.
Start IP	Specifies the starting IP address of the DHCP range.
End IP	Specifies the ending IP address of the DHCP range.
DNS Server	Displayed the DNS server IP address.

NOTE

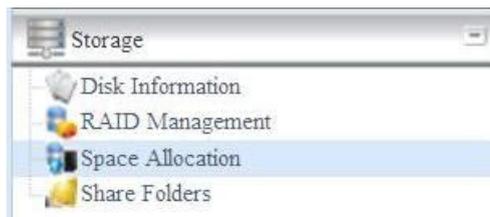
The IP Segment of WAN/LAN1 and LAN2 should not overlap.

WARNING

The IP address of the LAN2 interface should not be in the range of the Start IP address and End IP address.

Storage Management

The **Storage** menu displays the status of storage devices installed in the Thecus VisoGuard NVR, and includes storage configuration options such as RAID and disk settings, folder configuration and space allocation.



Disks Information

From the **Storage** menu, choose the **Disks** item and the **Disks Information** screen appears. From here, you can see various items about installed SATA hard disks. Blank lines indicate that a SATA hard disk is not currently installed in that particular disk slot.

NOTE

- The screen shot below just example from Thecus IP Storage. The disk slots can from 2 to 16 depend on the model of Thecus VisoGuard NVR.

Disks Information

Disk No.	Capacity (MB)	Model	Firmware	Status	Bad Block Scan
1	476,940	WDC WD5003ABYX-0	01.0	Detected	Click to start
2	476,940	WDC WD5003ABYX-0	01.0	Detected	Click to start
3	476,940	WDC WD5003ABYX-0	01.0	Detected	Click to start
4	N/A	N/A	N/A	N/A	N/A

Total Capacity: 1430820 (MB)

Disk Power Management

Disk Power Management: Minute

Disks Information	
Item	Description
Disk No.	Indicates disk location.
Capacity	Shows the SATA hard disk capacity.
Model	Displays the SATA hard disk model name.
Firmware	Shows the SATA hard disk firmware version.
Status	Indicates the status of the disk. Can read OK , Warning , or Failed .
Bad Block scan	Yes to start scan Bad Block.
Total Capacity	Shows the total SATA hard disk capacity.
Disk Power Management	The administrator can set the disk to power down after a period of inactivity.

NOTE

When the Status shows Warning, it usually means there are bad sectors on the hard disk. It is shown only as a precaution and you should consider changing the drives.

S.M.A.R.T. Information

On the **Disks Information** screen, the status of each disk will be displayed in the **Status** column. Clicking on an **OK** or **Warning** link will display the **S.M.A.R.T Information** window for that particular disk.

You may also perform disk SMART test, simply to click "Test" to start with. The result is only for reference and system will not take any action from its result.

SMART INFO

Info

Tray Number: 5

Model: WDC WD2002FYPS-0

Power On Hours: 529 Hours

Temperature Celsius: 35

Reallocated Sector Count: 0

Current Pending Sector: 0

Test

Test Type: short long

Test Result: Click to start

Test Time: --

S.M.A.R.T. Information	
Item	Description
Tray Number	Tray the hard disk is installed in.
Model	Model name of the installed hard disk.
Power ON Hours	Count of hours in power-on state. The raw value of this attribute shows total count of hours (or minutes, or seconds, depending on manufacturer) in power-on state.
Temperature Celsius	The current temperature of the hard disk in degrees Celsius
Reallocated Sector Count	Count of reallocated sectors. When the hard drive finds a read/write/verification error, it marks this sector as "reallocated" and transfers data to a special reserved area (spare area). This process is also known as remapping and "reallocated" sectors are called remaps. This is why, on a modern hard disks, you can not see "bad blocks" while testing the surface - all bad blocks are hidden in reallocated sectors. However, the more sectors that are reallocated, the more a decrease (up to 10% or more) can be noticed in disk read/write speeds.
Current Pending Sector	Current count of unstable sectors (waiting for remapping). The raw value of this attribute indicates the total number of sectors waiting for remapping. Later, when some of these sectors are read successfully, the value is decreased. If errors still occur when reading sectors, the hard drive will try to restore the data, transfer it to the reserved disk area (spare area), and mark this sector as remapped. If this attribute value remains at zero, it indicates that the quality of the corresponding surface area is low.
Test Type	Set short or long time to test.
Test Result	Result of the test.
Test Time	Total time of the test.

NOTE

If the Reallocated Sector Count > 32 or Current Pending Sector of a hard disk drive > 0, the status of the disk will show "Warning". This warning is only used to alert the system administrator that there are bad sectors on the disk, and they should replace those disks as soon as possible.

Bad Block Scan

On the **Disks Information** screen, you may also perform disk bad block scan, simply to click "Click to start" to start with. The result is only for reference and system will not take any action from its result.

Disk No.	Capacity (MB)	Model	Firmware	Status	Bad Block Scan
1	1,907,729	WDC WD2002FYPS-0	04.0	OK	▶ Click to start
2	1,907,729	WDC WD2002FYPS-0	04.0	OK	▶ Click to start
3	1,907,729	WDC WD2002FYPS-0	04.0	Warning	▶ Click to start
4	1,907,729	WDC WD2002FYPS-0	04.0	OK	▶ Click to start
5	1,907,729	WDC WD2002FYPS-0	04.0	OK	▶ Click to start
6	1,907,729	WDC WD2002FYPS-0	04.0	OK	▶ Click to start
7	1,907,729	WDC WD2002FYPS-0	04.0	OK	▶ Click to start
8	1,907,729	WDC WD2002FYPS-0	04.0	OK	▶ Click to start

Total Capacity: 15261832 (MB)

The testing result will be stay till system reboot with "Yet to start" displayed as default.

RAID Information

From the **Storage** menu, choose the **RAID** item and the **RAID Information** screen appears.

This screen lists the RAID volumes currently residing on the Thecus VisoGuard NVR. From this screen, you can get information about the status of your RAID volumes, as well as the capacities allocated for data, and target USB (depend on Model).

Mas.. RAID	ID	RAID Level	Status	Disks Used	Total Capacity	Data Capacity	VisoGuard Capacity
*	RAID	N/A		5	929 GB	N/A GB	N/A

RAID Information	
Item	Description
Master RAID	The RAID volume currently designated as the Master RAID volume.
ID	ID of the current RAID volume. NOTE: All RAID IDs must be unique.
RAID Level	Shows the current RAID configuration.
Status	Indicates status of the RAID. Can read either Healthy , Degraded , or Damaged .
Disks Used	Hard disks used to form the current RAID volume.
Total Capacity	Total capacity of the current RAID.
Data Capacity	Indicates the used capacity and total capacity used by user data.
VisoGuard Capacity	Indicates the capacity allocated to VisoGuard.

Create a RAID

On the **RAID Information** screen, press the **create** button to go to the **CREATE RAID** screen. In addition to RAID disk information and status, this screen lets you make RAID configuration settings.

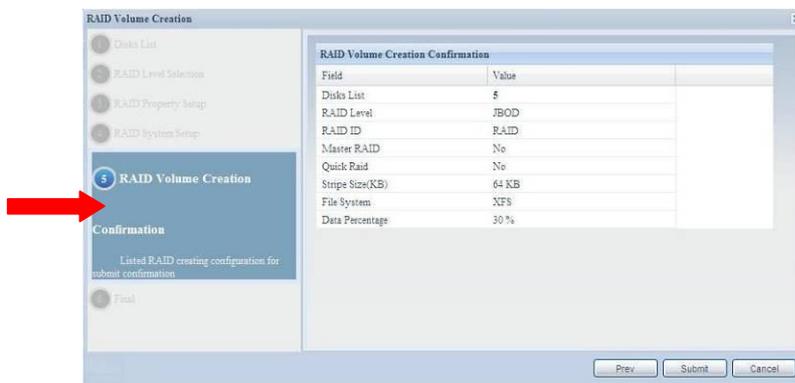
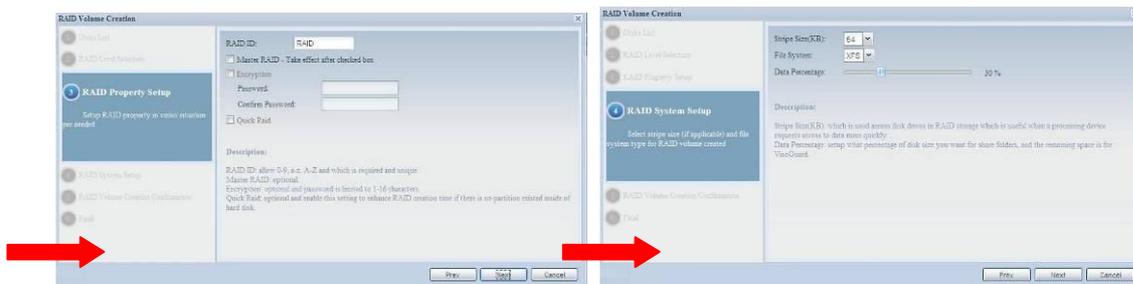
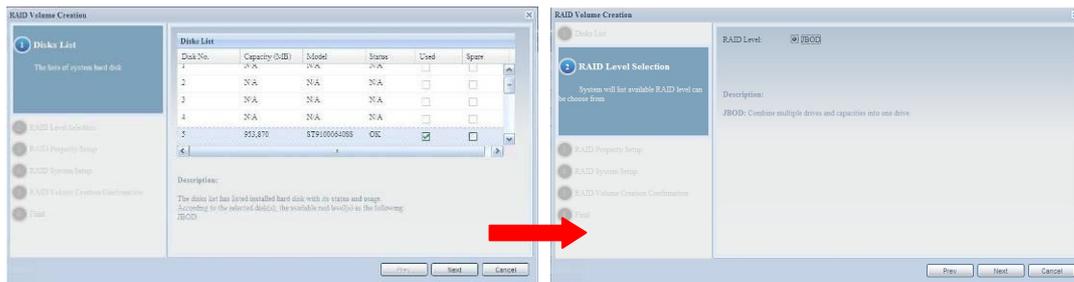
Using **Create RAID**, you can select stripe size, choose which disks are RAID disks or the Spare Disk.

RAID Configurations	
Item	Description
Disk No.	Number assigned to the installed hard disks.
Capacity (MB)	Capacity of the installed hard disks.
Model	Model number of the installed hard disks.
Status	Status of the installed hard disks.
Used	If this is checked, current hard disk is a part of a RAID volume.
Spare	If this is checked, current hard disk is designated as a spare for a RAID volume. 1. NVR 22/42/77/88/120/160: RAID space default 30%, VisoGuard space default 70% 2. NVR46/55: RAID space default 30%, USB Target space default 5%, VisoGuard space default 65% 3. Setting options in the UI can be modified
Master RAID	Check a box to designate this as the Master RAID volume.
Stripe Size	This sets the stripe size to maximize performance of sequential files in a storage volume. Keep the 64K setting unless you require a special file storage layout in the storage volume. A larger stripe

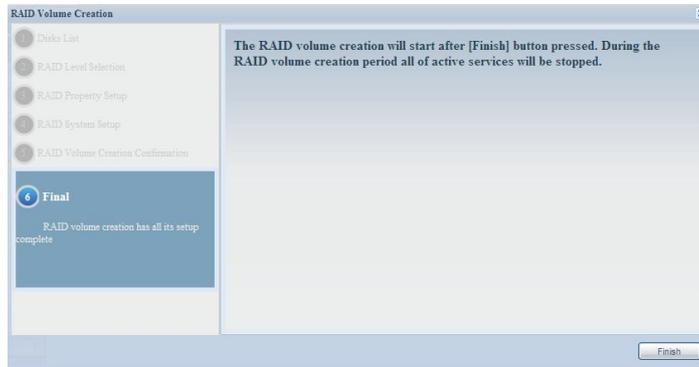
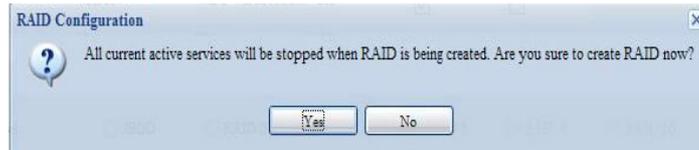
	size is better for large files.
Data Percentage	The percentage of the RAID volume that will be used to store data.
Create	Press this button to configure a file system and create the RAID storage volume.

To create a RAID volume, follow the steps below:

1. On the **RAID Information** screen, click **create**.
2. On the **RAID Configuration** screen, set the RAID storage space as **JBOD**, **RAID 0**, **RAID 1**, **RAID 5**, **RAID 6**, or **RAID 10** — see **Appendix B: RAID Basics** for a detailed description of each.
3. Specify a RAID ID.
4. Specify a stripe size — 64K is the default setting.
5. Specify the percentage allocated for user data by drag the horizontal bar.
6. Selected the file system you like to have for this RAID volume. The selection is available from **XFS**.



7. Press **Submit** to build the RAID storage volume.



NOTE Building a RAID volume may take time, depending on the size of hard drives and RAID mode. In general, while the RAID volume building process is up to "RAID Building" then the data volume is capable to be accessed.

WARNING Creating RAID destroys all data in the current RAID volume. The data is unrecoverable.

RAID Level

You can set the storage volume as **JBOD**, **RAID 0**, **RAID 1**, **RAID 5**, **RAID 6** or **RAID 10**. RAID configuration is usually required only when you first set up the device. A brief description of each RAID setting follows:

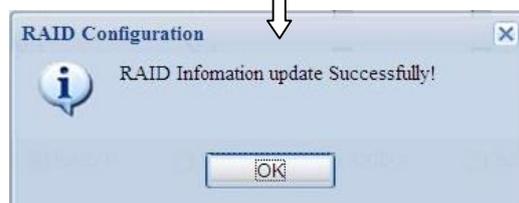
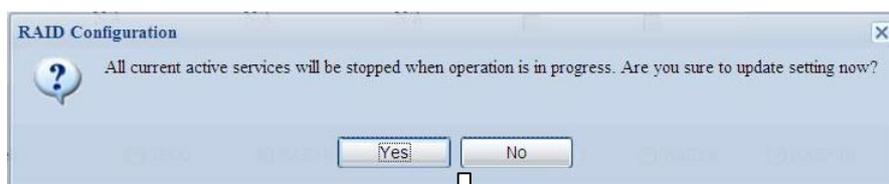
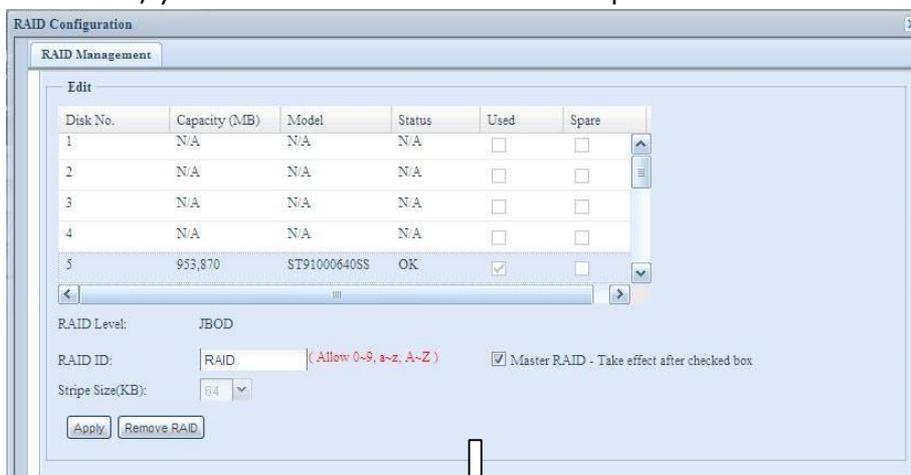
RAID Levels	
Level	Description
JBOD	The storage volume is a single HDD with no RAID support. JBOD requires a minimum of 1 disk.
RAID 0	Provides data striping but no redundancy. Improves performance but not data safety. RAID 0 requires a minimum of 2 disks.
RAID 1	Offers disk mirroring. Provides twice the read rate of single disks, but same write rate. RAID 1 requires a minimum of 2 disks.
RAID 5	Data striping and stripe error correction information provided. RAID 5 requires a minimum of 3 disks. RAID 5 can sustain one failed disk.
RAID 6	Two independent parity computations must be used in order to provide protection against double disk failure. Two different algorithms are employed to achieve this purpose. RAID 6 requires a minimum of 4 disks. RAID 6 can sustain two failed disks.
RAID 10	RAID 10 has high reliability and high performance. RAID 10 is implemented as a striped array whose segments are RAID 1 arrays. It has the fault tolerance of RAID 1 and the performance of RAID 0. RAID 10 requires 4 disks. RAID 10 can sustain two failed disks.

WARNING If the administrator improperly removes a hard disk that should not be removed when RAID status is degraded, all data will be lost.

Edit RAID

On the **RAID Information** screen, press the **Edit** button to go to the **RAID Configuration** screen.

Using **Edit RAID**, you can select RAID ID and the Spare Disk.

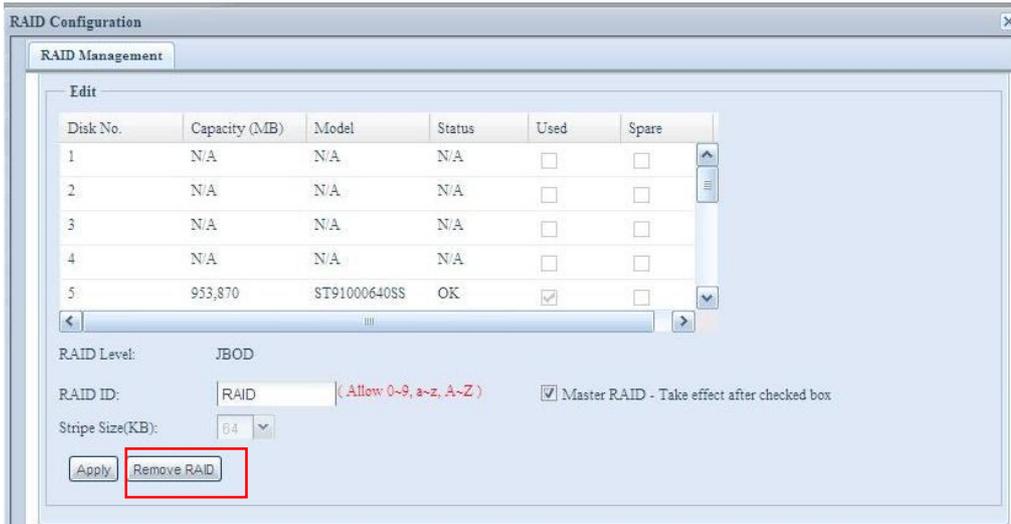


Remove RAID

Click to remove the RAID volume. All user data has been created in selected RAID volume will be removed.

To remove a RAID volume, follow the steps below:

1. On the RAID List screen, select the RAID volume by clicking on its radio button, and click **RAID Information** to open the **RAID Configuration** screen.
2. On the **RAID Configuration** screen, click **Remove RAID**.
3. The confirmation screen appear, you will have to input "Yes" with exactly wording case to complete "**Remove RAID**" operation



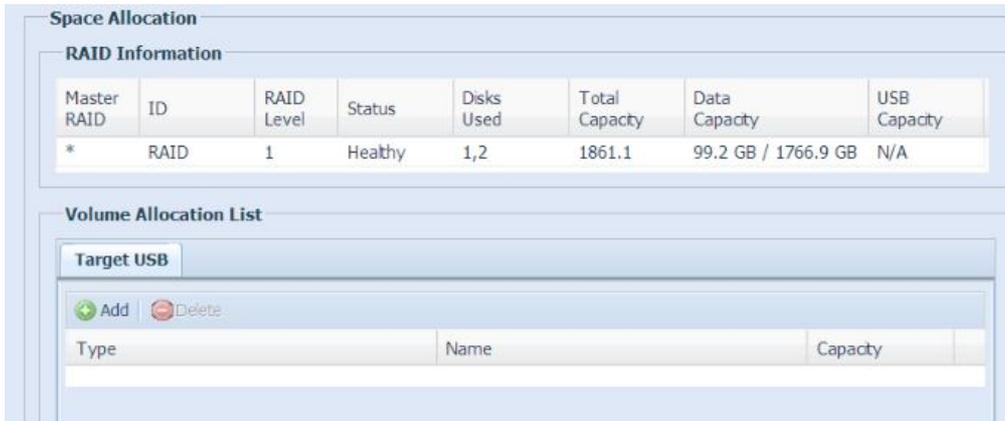
WARNING Remove RAID destroys all data in the current RAID volume. The data is unrecoverable.

Space Allocation (NVR55/NVR46R/NVR46S only)

You may specify the space allocated for Target USB volumes.

To do this, under the **Storage** menu, click **RAID** and the **RAID List** window appears. Select the RAID volume you wish to reallocate by clicking on its radio button, and click **Space Allocation**. The **RAID Information** and **Volume Allocation List** windows will appear.

The Volume Allocation List displays the space allocated for **Target USB** volumes on the current RAID volume.

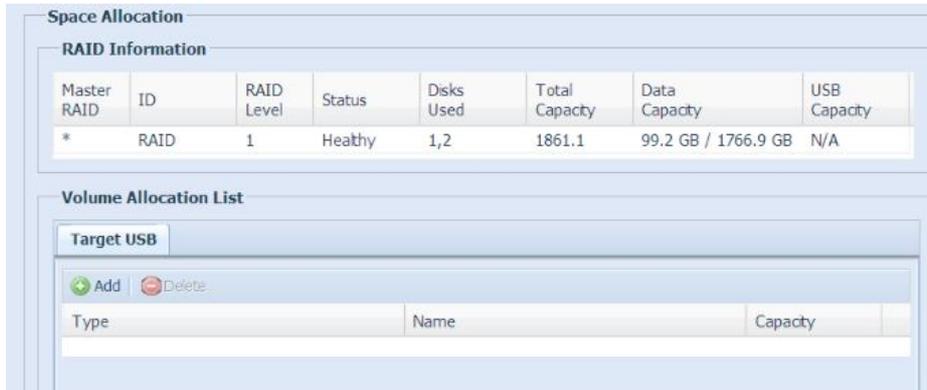


Volume Allocation List	
Item	Description
Modify	Click this to modify the allocated space.
Delete	Click this to delete the allocated space.

Target USB	Click to allocate space to USB volume.
Type	Type of volume.
Name	Name assigned to the volume.
Capacity	Capacity of the allocated space.

Allocating Space for Target USB Volume

1. Under the **Volume Allocation List**, click **Target USB**.
The **Create Target Volume** screen appears.



2. Designate the percentage to be allocated from the **Allocation** drag bar.
3. Click **OK** to create the USB volume.

Create USB Volume	
Item	Description
RAID ID	ID of current RAID volume.
Unused	Percentage and amount of unused space on current RAID volume.
Allocation	Percentage and amount of space allocated to USB volume.

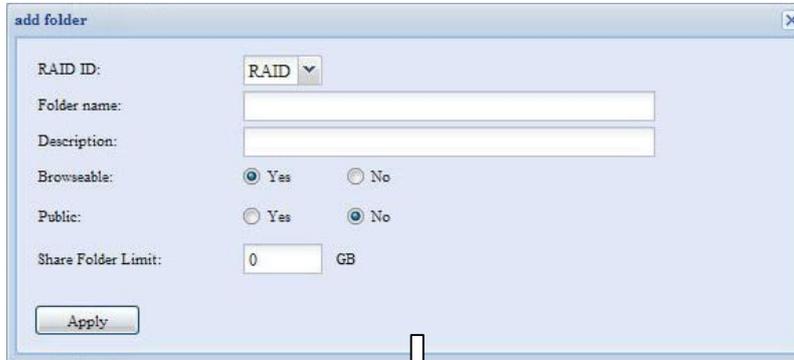
Share Folder

From the **Storage** menu, choose **Share Folder**, and the **Folder** screen appears. This screen allows you to create and configure folders on the Thecus VisoGuard NVR volume.



Adding Folders

On the **Folder** screen, press the **Add** button and the **Add Folder** screen appears. This screen allows you to add a folder. After entering the information, press **Apply** to create new folder.



Add Folder	
Item	Description
RAID ID	RAID volume where the new folder will reside.
Folder Name	Enter the name of the folder.
Description	Provide a description the folder.
Browseable	Enable or disable users from browsing the folder contents. If Yes is selected, then the share folder will be browseable.
Public	Admit or deny public access to this folder. If Yes is selected, then users do not need to have access permission to write to this folder. When accessing a public folder via FTP, the behavior is similar to anonymous FTP. Anonymous users can upload/download a file to the folder, but they cannot delete a file from the folder.
Share Folder Limit	Enter the maximum size of the folder in Gigabytes (GB). The folder cannot grow beyond this limit. You can enter a 0 to turn off the share folder limit. This option did not apply while XFS file system selected.
Apply	Press Apply to create the folder.

NOTE

Folder names are limited to 60 characters. Systems running Windows 98 or earlier may not support file names longer than 15 characters.

Modify Folders

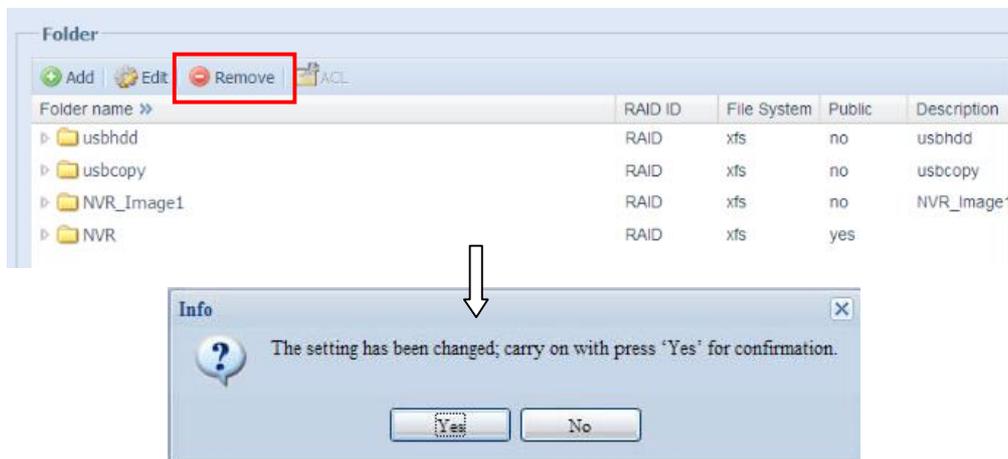
On the **Folder** screen, press the **Edit** button and the **Modify Folder** screen appears. This screen allows you to change folder information. After entering the information, press **Apply** to save your changes.



Modify Folder	
Item	Description
RAID ID	RAID volume where the folder will reside.
Folder Name	Enter the name of the folder.
Description	Provide a description the folder.
Browseable	Enable or disable users from browsing the folder contents. This setting will only apply while access via SMB/CIFS and web disk.
Public	Admit or deny public access to this folder.
Share Limit	Enter the maximum size of the folder. The folder will not grow beyond this limit. You can enter a 0 to turn off the share folder limit.

Remove Folders

To remove a folder, press the **Remove** button from the specified folder row. The system will confirm folder deletion. Press **Yes** to delete the folder permanently or **No** to go back to the folder list.



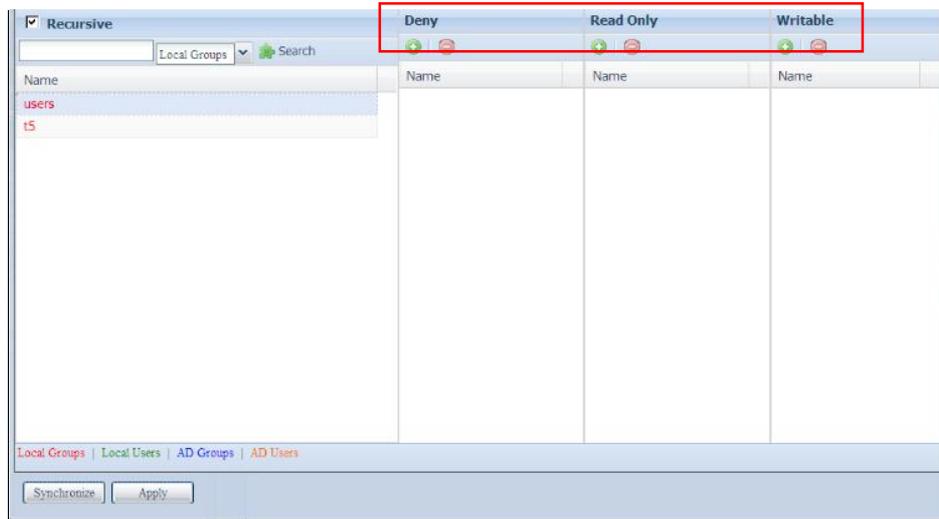
WARNING

All the data stored in the folder will be deleted once the folder is deleted. The data will not be recoverable.

Folder and sub-folders Access Control List (ACL)

On the Folder screen, press the **ACL** button, and the **ACL setting** screen appears. This screen allows you to configure access to the specific folder and sub-folders for users and groups. Select a user or a group from the left hand column and then

choose **Deny**, **Read Only**, or **Writable** to configure their access level. Press the **Apply** button to confirm your settings.



ACL setting	
Item	Description
Deny	Denies access to users or groups who are displayed in this column.
Read Only	Provides Read Only access to users or groups who are displayed in this column.
Writable	Provides Write access to users or groups who are displayed in this column.
Recursive	Enable to inherit the access right for all its sub-folders.

To configure folder access, follow the steps below:

1. On the **ACL** screen, all network groups and users are listed in the left hand column. Select a group or user from this list.
2. With the group or user selected, press one of the buttons from the three access level columns at the top. The group or user then appears in that column and has that level of access to the folder.
3. Continue selecting groups and users and assigning them access levels using the column buttons.
4. To remove a group or user from an access level column, press the **Remove**  button in that column.
5. When you are finished, press **Apply** to confirm your ACL settings.

NOTE

If one user has belonged to more than one group but different privilege than the priority Deny > Read Only > Writable

To setup sub-folders ACL, click on "►" symbol to extract sub folders list as screen shot shows below. You may carry on with same steps as share level ACL setting.

Folder name >>	RAID ID	File System	Public	Description
usbhdd	RAID	xfs	no	usbhdd
usbcopy	RAID	xfs	no	usbcopy
NVR_Image1	RAID	xfs	no	NVR_Image1
NVR	RAID	xfs	yes	
test1			yes	
test2			yes	

NOTE

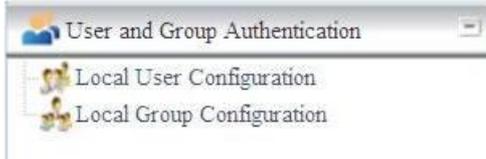
The ACL can be set for share and sub-folders level, not for files.

The ACL screen also allows you to search for a particular user. To do this, follow the steps below:

1. In the blank, enter the name of the user you would like to find.
2. From the drop down select the group you would like to search for the user in.
3. Click **Search**.

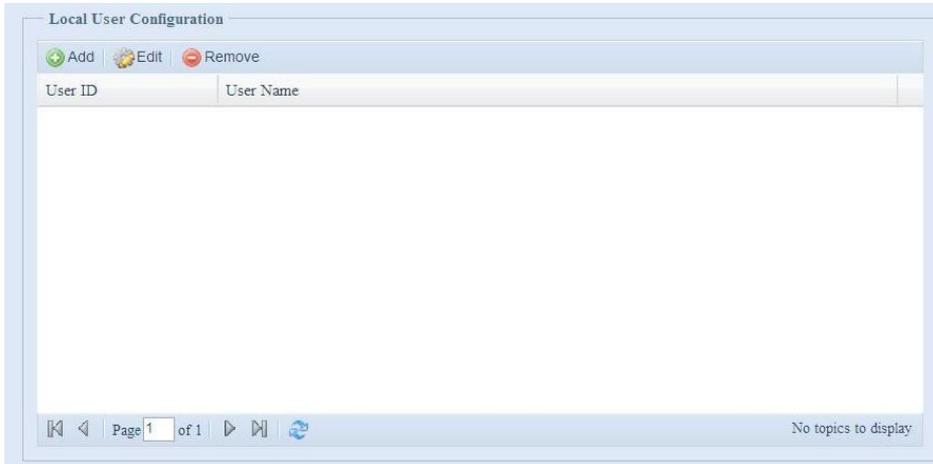
User and Group Authentication

The Thecus VisoGuard NVR has built-in user database that allows administrators to manage user access using different group policies. From the **User and Group Authentication** menu, you can create, modify, and delete users, and assign them to groups that you designate.



Local User Configuration

From the **Accounts** menu, choose the **User** item, and the **Local User Configuration** screen appears. This screen allows you to **Add**, **Edit**, and **Remove** local users.



Local User Configuration	
Item	Description
Add	Press the Add button to add a user to the list of local users.
Edit	Press the Edit button to modify a local user.
Remove	Press the Remove button to delete a selected user from the system.

Add Users

1. Click on the **Add** button on **Local User Configuration** screen, and **Local User Setting** screen appears.
2. On the **Local User Setting** screen, enter a name in the **User Name** box.
3. Enter a **User ID** number. If left blank, the system will automatically assign one.
4. Enter a password in the **Password** box and re-enter the password in the **Confirm** box.
5. Select which group the user will belong to. **Group Members** is a list of groups this user belongs to. **Group List** is a list of groups this user does not belong to. Use the << or >> buttons to have this user join or leave a group.

6. Press the **Apply** button and the user is created.

GroupID	Group Name
102	users

NOTE

All users are automatically assigned to the 'users' group.

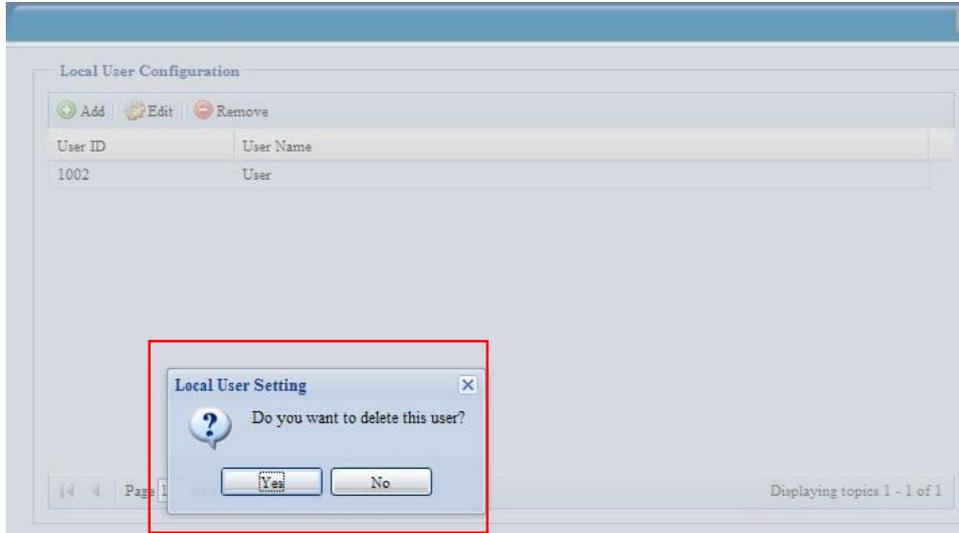
Edit Users

1. Select an existing user from the **Local User Configuration** screen.
2. Click on the **Edit** button, and **Local User Setting** screen appears.
3. From here, you can enter a new password and re-enter to confirm, or use the **<<** or **>>** buttons to have this user join or leave a group. Click the **Apply** button to save your changes.

GroupID	Group Name
102	users

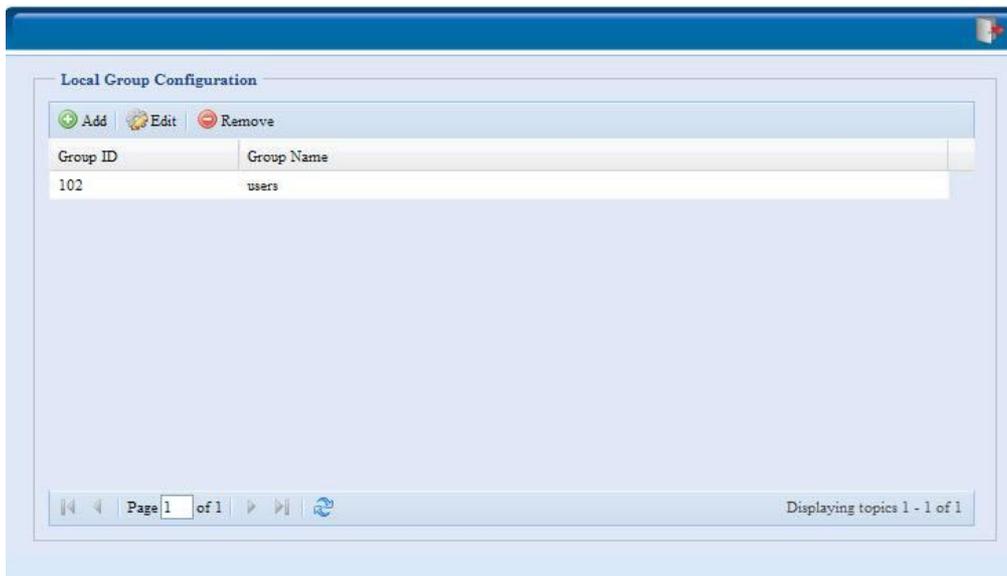
Remove Users

1. Select an existing user from the **Local User Configuration** screen.
2. Click on **Remove** button and the user is deleted from the system.



Local Group Configuration

From the **Accounts** menu, choose the **Group** item, and the **Local Group Configuration** screen appears. This screen allows you to **Add**, **Edit**, and **Remove** local groups.



Local Group Configuration	
Item	Description
Add	Press the Add button to add a user to the list of local groups.
Edit	Press the Edit button to modify a selected group from the system.
Remove	Press the Remove button to delete a selected group from the system.

Add Groups

1. On the **Local Group Configuration** screen, click on the **Add** button.
2. The **Local Group Setting** screen appears.
3. Enter a **Group Name**.
4. Enter a **Group ID** number. If left blank, the system will automatically assign one.
5. Select users to be in this group from the **Users List** by adding them to the **Members List** using the << button.
6. Click the **Apply** button to save your changes.

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. It is divided into two main sections: "Local Group Setting" on the left and "Users List" on the right. At the bottom, there is an "Apply" button.

Local Group Setting

Group Name:

Group ID:

Members List

UserID	User Name
--------	-----------

Users List

Search:

UserID	User Name
1002	User

Edit Groups

1. On the **Local Group Configuration** screen, select a group name from the list.
2. Press the **Edit** button to modify the members in a group.
3. To add a user into a group, select the user from the **Users List**, and press the << button to move the user into the **Members List**.
4. To remove a user from a group, select the user from **Members List**, and press the >> button.
5. Click the **Apply** button to save your changes.

The screenshot shows a dialog box titled "Edit" with a close button (X) in the top right corner. It is divided into two main sections: "Local Group Setting" on the left and "Users List" on the right. At the bottom, there is an "Apply" button.

Local Group Setting

Group Name:

Group ID:

Members List

UserID	User Name
--------	-----------

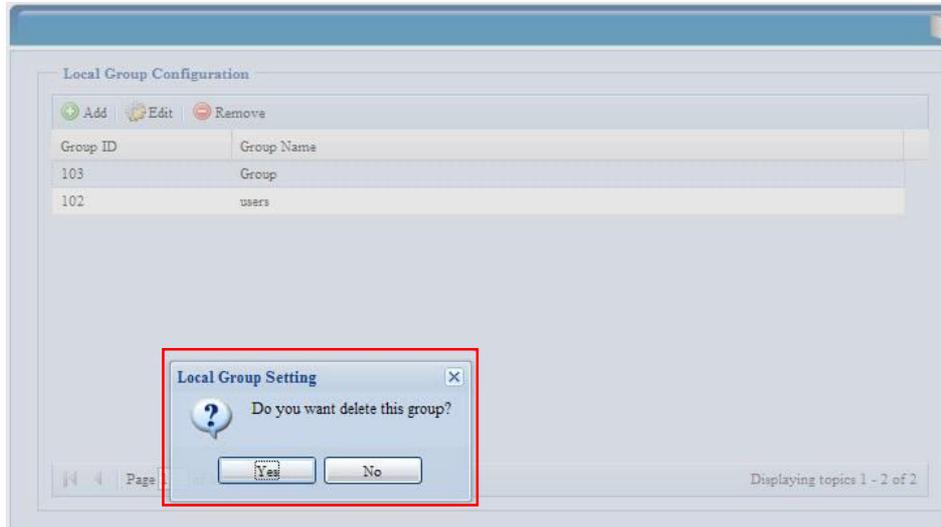
Users List

Search:

UserID	User Name
1002	User

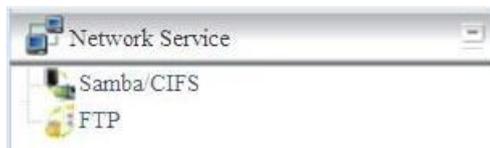
Remove Groups

1. On the **Local Group Configuration** screen, select a group name from the list.
2. Press **Remove** to delete the group from the system.



Network Service

Setup and manage protocols such as Samba/CIFS, and FTP.



Samba / CIFS

There are 7 options is currently allow Admin to Enable/Disable to operate Thecus VisoGuard NVR associated with Samba / CIFS protocol. With the option changed, it will need to reboot system to activate.



Samba Service

Used for letting the operating system of UNIX series and SMB/CIFS of Microsoft Windows operating system (Server Message Block / Common Internet File

System). Do the link in network protocol. Enable or Disable SMB/CIFS protocol for Windows, Apple, Unix drive mapping.

NOTE

- In some environments, due to security concerns, you may wish to disable SMB/CIFS as a precaution against computer viruses.

File Access Cache

File Access Cache is default **Enable**. This option will help to increase the performance while single client access share folder in writing under SMB/CIFS protocol.

Samba Recycle Bin

The Thecus VisoGuard NVR is supported recycle bin via SMB/CIFS protocol. Simply enable it then all of deleted files/folders will reside in the ".recycle" folder with hidden attribution in each share.



In general, Windows has default to invisible all of hidden folders/files. So please enable this option to view ".recycle" folder.

Samba Anonymous Login Authentication

To enable this option, no matter there is share folder has been created in public access. The user account and password is needed from system to access under SMB/CIFS protocol. On the other hand, no more anonymous login is allowed.

Samba is Native mode

The Thecus IP storage is supported Samba mode options. In the ADS environment with "Native" mode selected then Thecus IP storage is capable to become local master position.

FTP

Thecus VisoGuard NVR can act as a FTP server, enabling users to download and upload files with their favorite FTP programs. From the **Network Service** menu, choose the **FTP** item, and the **FTP** screen appears. You can change any of these items and press **Apply** to confirm your settings.

A screenshot of the 'FTP' configuration screen in the Thecus VisoGuard NVR interface. The screen has a light blue background and contains the following settings:

- FTP: Enable Disable
- Secure FTP (Explicit): Enable Disable
- Port: 21
- Passive Port Range(30000-32000): 30000 ~ 32000
- FTP ENCODE: UTF-8
- Allow Anonymous FTP Access: Upload/Download
- Auto Rename:
- Upload Bandwidth: Unlimited
- Download Bandwidth: Unlimited

At the bottom left, there is an 'Apply' button.

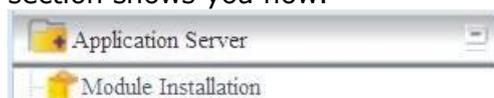
A description of each item follows:

FTP	
Item	Description
FTP	Enable FTP Service on Thecus VisoGuard NVR.
Security FTP	Enable or disable Security FTP, be sure the client FTP software has also security FTP setting enabled.
Port	Specifies the port number of an incoming connection on a non-standard port.
FTP ENCODE	If your FTP client or operating system does not support Unicode (e.g. Windows® 95/98/ME or MAC OS9/8), select the same encoding as your OS here in order to properly view the files and directories on the server. Available options are BIG5, HZ, GB2312, GB18030, ISO, EUC-JP, SHIFT-JIS and UTF-8.
Allow Anonymous FTP Access	Upload/Download: Allow anonymous FTP users to upload or download files to/from public folders. Download: Allow anonymous FTP users to download files from public folders. No access: Block anonymous FTP user access.
Auto Rename	If checked, the system will automatically rename files that are uploaded with a duplicate file name. The renaming scheme is [filename].#, where # represents an integer.
Upload Bandwidth	You may set the maximum bandwidth allocated to file uploads. Selections include Unlimited, 1, 2, 4, 8, 16 and 32 MB/s.
Download Bandwidth	You may set the maximum bandwidth allocated to file downloads. Selections include Unlimited, 1, 2, 4, 8, 16 and 32 MB/s.

To access the share folder on Thecus VisoGuard NVR, use the appropriate user login and password set up on the **Users** page. Access control to each share folder is set up on the **ACL** page (**Storage Management > Share Folder > ACL**).

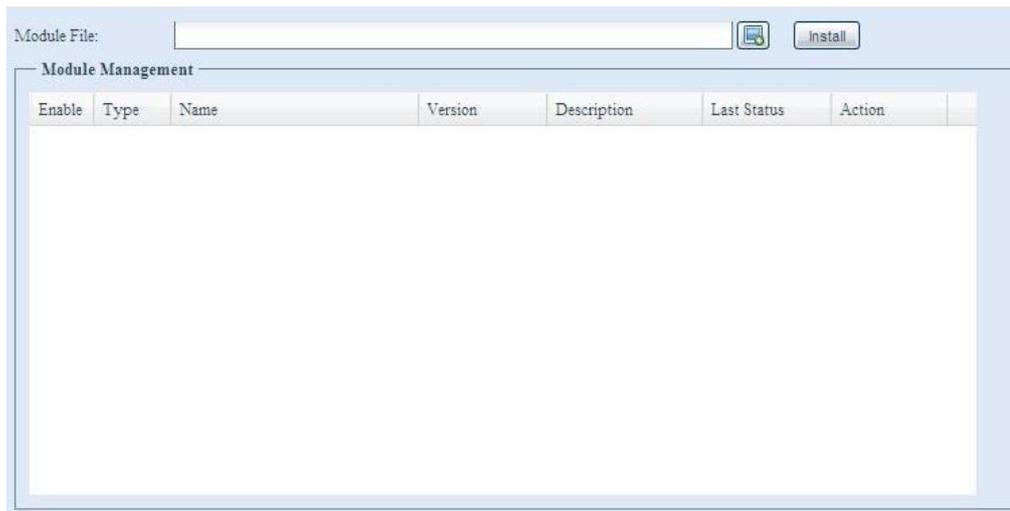
Application Server

Thecus VisoGuard NVR support Module Installation functionality. The following section shows you how.



Module Installation

From the **Application Server** menu, choose the **Module Installation** item and the **Module Management** screen appears. From here, you can install separate software modules to extend the functionality of your Thecus VisoGuard NVR.



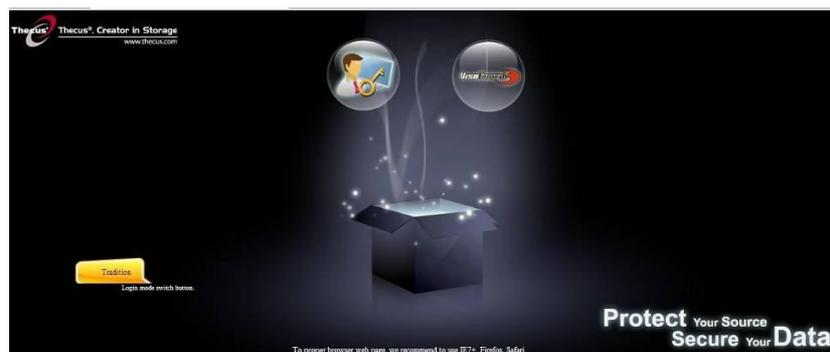
Chapter 5: Using Thecus VisoGuard NVR

Overview

Once the Thecus VisoGuard NVR is setup and operating, users on the network may manage all varieties of digital music, photos, or files by simply using their web browsers. To manage your personal files or access public files on the Thecus VisoGuard NVR, just enter its IP address into your browser (default IP address is <http://192.168.1.100>), and you will be taken to the **Thecus VisoGuard NVR Login** page.

Login Page

To login to the system, enter your user name and password, then click **Login** to log into the system. You will be taken to the **selected** interface.



NOTE

※ A RAID volume must be created in the Thecus admin UI before the VisoGuard UI can be accessed.

NOTE

※ For this function, must install the Web Disk module first.

Using the Web Disk

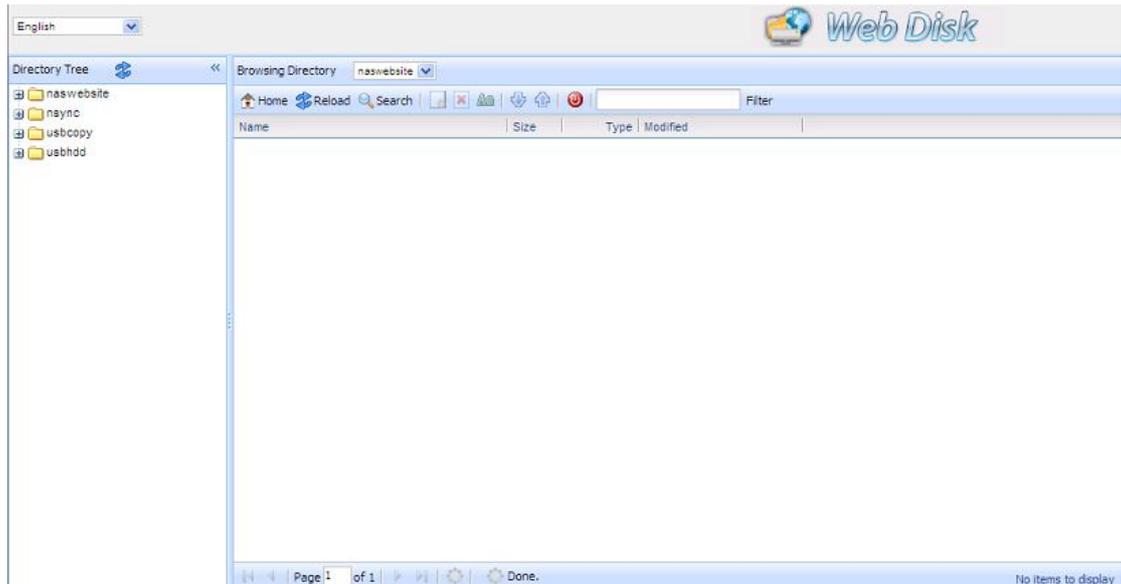
Thecus VisoGuard NVR provide a Web Disk function that allows you to access the system over the Internet from any browser.



1. In the Login page, type in the User ID and password that were previously set for you in the Accounts menu. See **Chapter 4: User and Group Authentication > Local User Configuration**.
2. The Web Disk page appears showing folders currently available to you, this is controlled via the **Access Control List (ACL)**.
3. Click on a folder name to enter the folder.
4. The folder's page appears displaying files and folders. Click on a file to download the file.
5. Buttons on the folder page allow you to create new folders, upload files, and delete files in the folder.
6. To create a new folder within the current folder, press the New Folder button. When the screen appears enter a name for the folder. Press OK to create the folder.
7. To upload a file from your computer to the current folder, press the New File (upload) button. When the screen appears, press **Browse** and locate the file to upload. Press **OK** and the file will be uploaded to the current folder.
8. To delete a file or folder, select the file or folder's check box. Press Delete button. You can also click the Select All button to select all files and folders in this folder.

To access folders with access control, you must first login with a local user account.

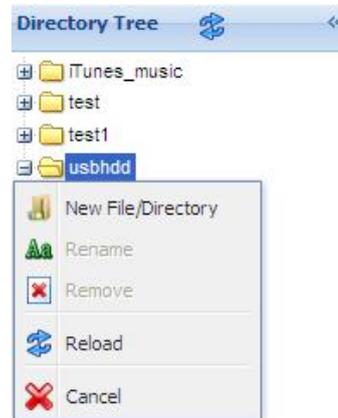
For more information on how to setup user rights to the folders, please check **Chapter 4: Storage Management > Share Folder > Folder Access Control List (ACL)**.



Folder Page Button	
Button	Description
Directory Tree	List all directory trees per login user's privilege.
Browsing Directory	Browsing selected directory of its folders and files.
Home	Go back to the web disk directory layer.
Reload	Re-load the current list.
Search	Search files in the current web disk directory. (Must input the complete file name.)
(new file/Directory)	Creates a new folder or directory.
(delete)	Deletes selected files or folders.
(Rename)	Rename a directory or file.
(download)	Download a file to current folder of your computer.
(upload)	Upload file from your computer to current web disk folder.
(Admin)	Change password and confirm new password.
(logout)	To logout of the web disk interface.
Show Directories	Show the files and folders in the directory.
Filter	Search files in the directory. (You can only input some word string.)
Name	Displays the names of folders and files.
Size	Shows the size of folders and files.
Type	Displays the type of folders and files.

Modified	Shows the time of most recent modification of folders and files.
owner	Owner of the file.

There is also the way by using right click button to bring up context windows as short cut to operate what you needed.



NOTE

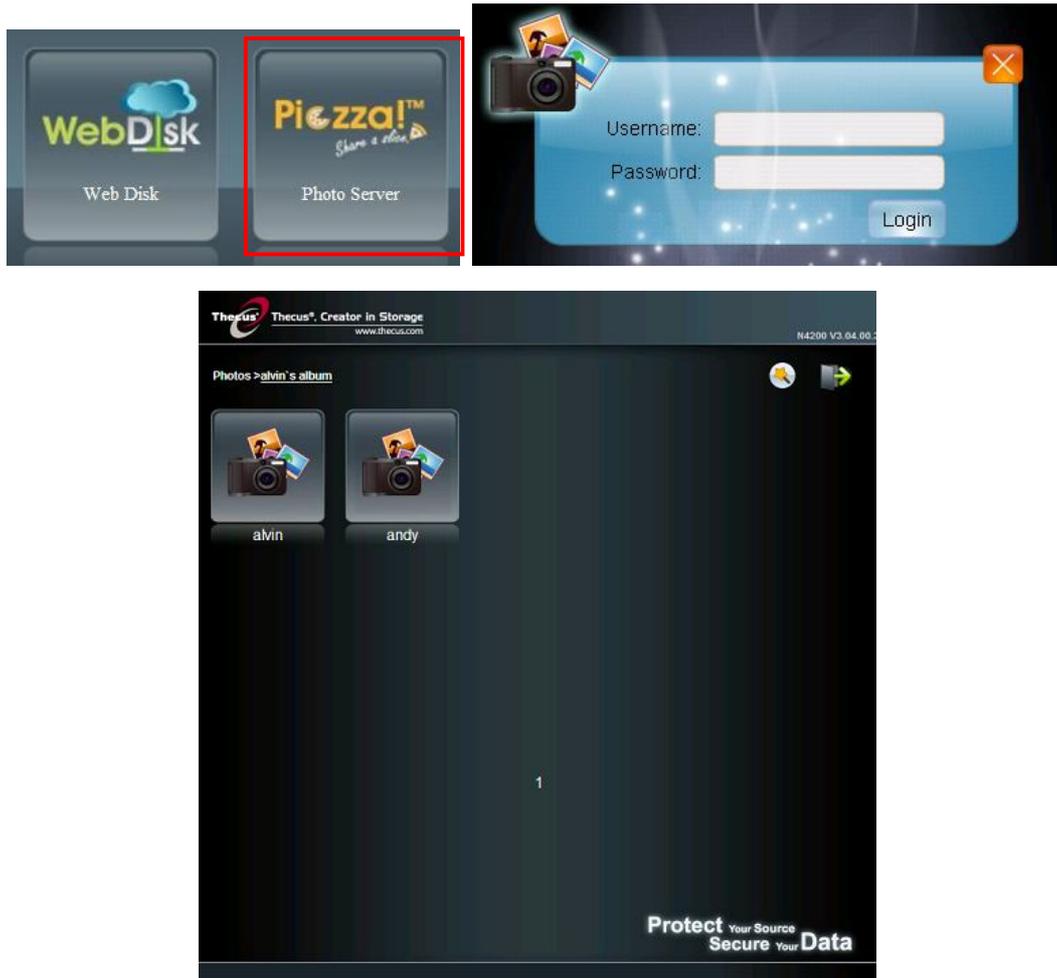
✘ For this function, must install Piczza module first.

Photo Server

Using the Photo Server, users can view and share photos, and even create their own albums right on the Thecus VisoGuard NVR.

You will see your own photo gallery and all public photo albums on the network.

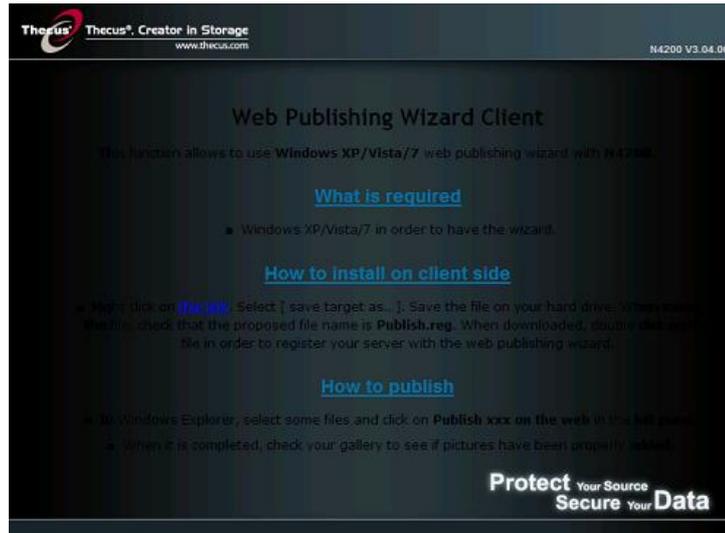
To manage any picture files, you must first select the item by clicking the box then entering your user name and password to log in to the photo server.



Windows XP Publishing Wizard

There are many ways for a local user to upload pictures into their photo album. Users of Windows XP can upload their pictures using the Windows XP Publishing Wizard.

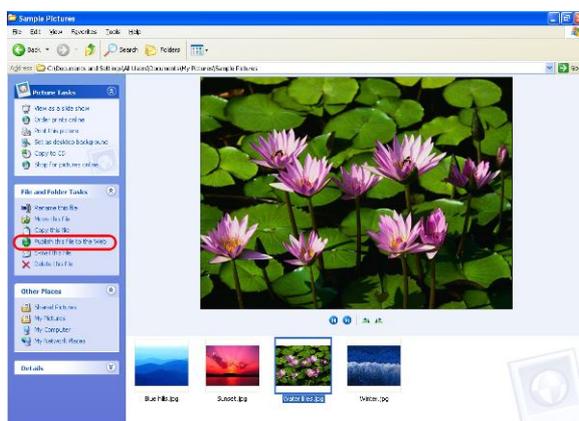
1. Click on the **XP Publishing Wizard** icon on top right corner. 
2. The **XP Web Publishing Wizard Client** screen appears. Click on the link to install the Publishing Wizard.



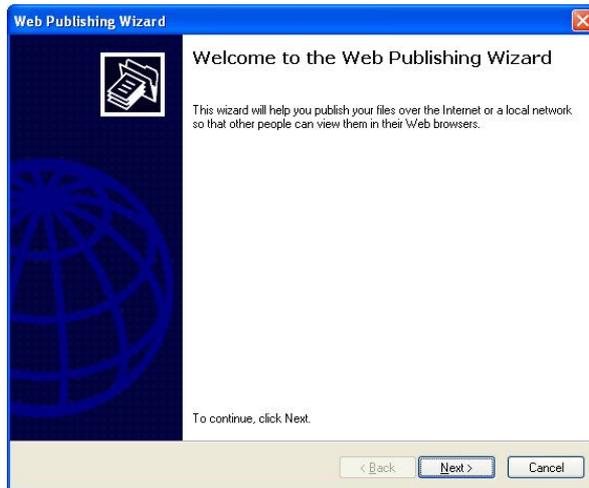
3. Windows XP will ask whether you want to run or save this file. Click **Save** to save the register file.



4. Once the register file is installed, use the Windows file manager to browse the folder that contains the picture you want to publish. On the left pane, there will be an icon labeled **"Publish this folder to the Web"**.



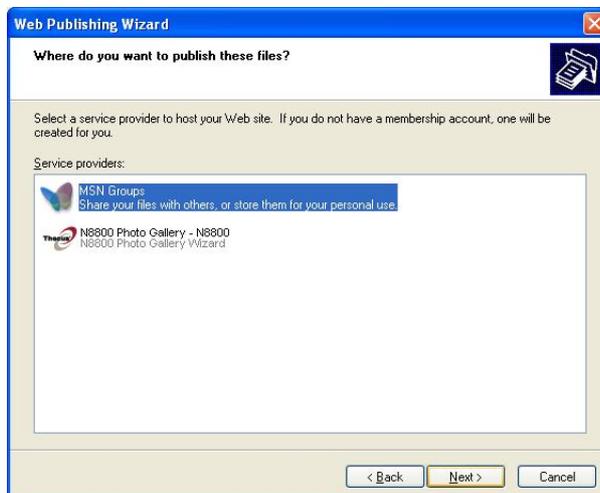
5. Click on this icon and **Web Publishing Wizard** will start.



6. Select the pictures you want to publish to the Photo Web Server by placing a check mark on the top left hand corner of the picture. Click **Next**.



7. Your PC will start to connect to the Photo Web Server.
8. Select **Thecus VisoGuard NVR Photo Gallery Wizard** to publish your pictures to Thecus VisoGuard NVR.



9. Login into Thecus VisoGuard NVR with your local user name and password.



10. Create your album by entering an album name and clicking on the **Create Album** button.

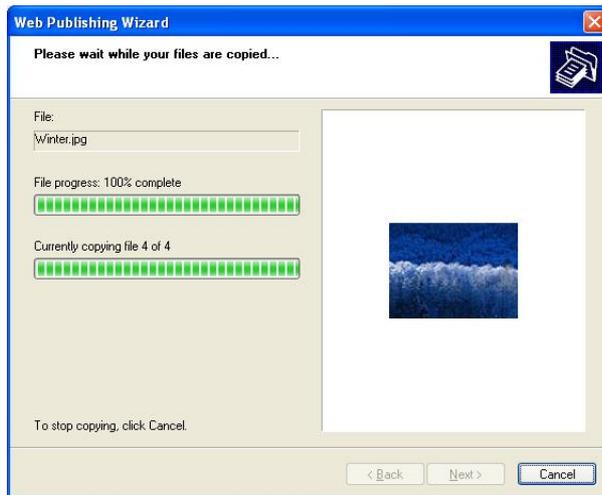


11. Select the album you want to upload your pictures to.

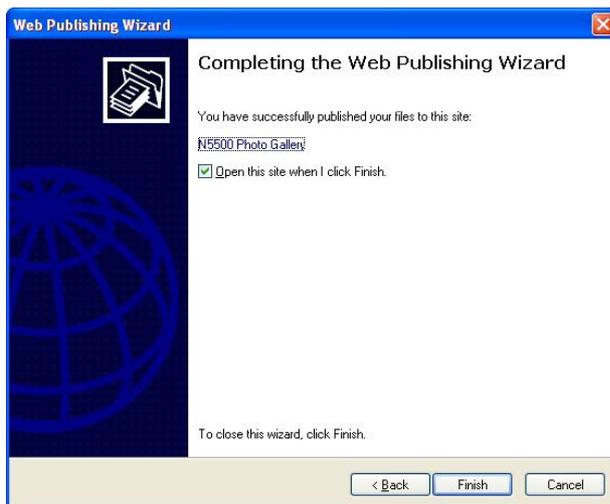
12. Confirm the target album.



13. Windows will show you that the picture upload is in progress.



14. When the upload is finished, the Wizard will ask you whether if you want to go to the website. Click **Finish** to go to your Photo Web Server.



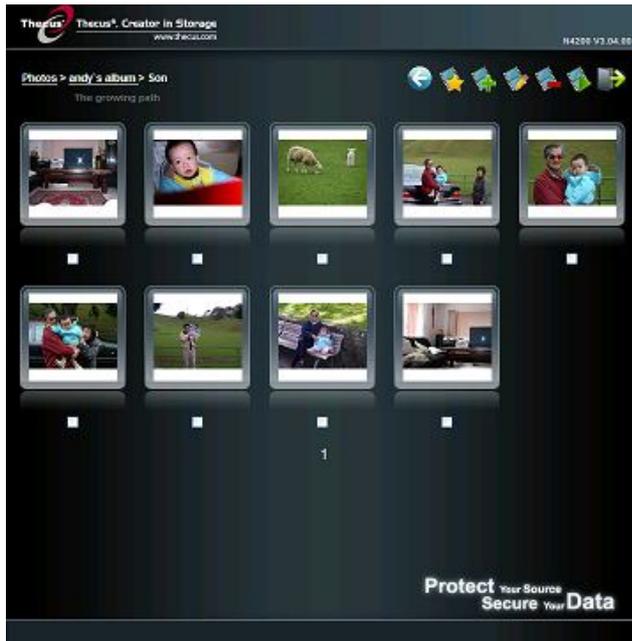
15. Click on the user's icon to go to that user's album.



16. You will see the user's album list. Click on **Album**.



17. Finished! You will see the pictures just selected in the album.



Managing Albums and Photos

Icon	Function	Description
	Make Cover	Make selected photo your cover picture.
	Back	Return to the previous screen.
	Add	Add a new album or photos.
	Modify	Edit the name and description of the selected album or photo. Each name is limited to 20 characters and each description is limited to 255 characters.
	Delete	Delete the selected albums or photos.

NOTE

- Only logged in users will see these icons.
- To prevent system errors, Thecus VisoGuard NVR sets the following limitations on photo files:
 - Each file upload is limited to a size of 8MB. Files exceeding 8MB will NOT be uploaded and no error message will appear.
 - Only these photo file types will be uploaded: *.jpg, *.gif, *.bmp, *.png, *.pcx, *.psd, *.bmp.
 - If duplicate file names exist during upload process, system will add a number in front of the original file name (abc → 1abc).

Creating Albums

To create a photo album, follow the steps below:

1. Click the **Add** button to create a new album.
2. Enter a name for the album, and enter a description if you wish. Then, click on the **Create Album** button.

Password Protecting Albums

If you would like to put a password on a particular album, follow these steps:

1. Select the album to be protected, click on the **Edit** button, and the **Album Edit** screen will appear.
2. The owner of the album can enter an album password to protect the album, so that only people with the correct password can view the album.

Uploading Pictures to Albums

Uploading pictures to albums using the Web User Interface is easy:

1. When the album is created, click the album icon to enter the album. Initially the album is empty.
2. Click the **Add** button to upload pictures into the album. The **Upload Photos** screen will appear. Users can select and upload up to 8 pictures at a time.
3. Once the picture is uploaded, you can view it in the album. The owner of the album can delete or modify the pictures with the **Delete** or **Modify** buttons on the top right hand corner

EXIF Information

While viewing pictures, you can also have Thecus VisoGuard NVR display the EXIF information for each photo.



Simply click the **EXIF** button to display EXIF information. To hide this information, click the **EXIF** button again.

Slide Shows

Slide shows are a great way to enjoy pictures stored on your Thcus VisoGuard NVR.

You can click on the **Start Slide Show** icon on the top right hand corner to start the slide show.



To stop the slide show, click on the **Stop Slide Show** icon on the top right hand corner.

Mapping a Client PC to the Thcus VisoGuard NVR

You can map share folders on Thcus VisoGuard NVR so that you can access them as if they were drives on your computer. You can connect to the shared network folders on Thcus VisoGuard NVR as follows:

Windows

1. Go to the **My Computer** folder in Windows.
2. In the menu bar, select **Tools** and then **Map Network Drive...**
3. The **Map Network Drive** window appears.
4. Assign a drive letter for the share folder.
5. Click the **Browse** button to find the folder over your network. Alternatively, you may enter the folder name you wish to connect to or enter its IP address. (i.e. \\192.168.1.100\share)
6. Click **Finish**. When the **Connect As...** window appears, enter your user name and password.
7. Click **OK**. The share folder appears as the drive you assigned. You can now access this folder as though it were a drive on your computer.

.Chapter 6: Tips and Tricks

USB and eSATA Storage Expansion

The Thecus VisoGuard NVR supports external USB hard disks through its USB ports. Once a USB hard disk has successfully mounted, the entire volume will be linked automatically to the default USB HDD folder. The Thecus VisoGuard NVR supports USB external storage devices. All file names on the USB disk volume are case sensitive.

The Thecus VisoGuard NVR also supports eSATA hard disks with its eSATA port.

Before attaching an eSATA or USB disk drive to Thecus VisoGuard NVR, you have to partition and format it on a desktop computer or a notebook first. The attached device will be located at `\\192.168.1.100\usbhdd\sd(x)1` where 192.168.1.100 means the IP address of Thecus VisoGuard NVR and `sd(x)1` stands for the first partition on the eSATA or USB disk drive.

Replacing Damaged Hard Drives

If you are using RAID 1, RAID 5, or RAID 6 you can easily replace a damaged hard drive in the Thecus VisoGuard NVR while keeping your data secure with the system's automatic data recovery.

Hard Drive Damage

When a hard drive is damaged and data in the RAID volume, the system LCD will display warning message also the system beeps.

Replacing a Hard Drive

To replace a hard disk drive in Thecus VisoGuard NVR:

1. Remove the tray with the damaged hard disk.
2. Unscrew the damaged hard disk and remove it from the tray.
3. Slide a new hard disk into the tray and fasten the screws.
4. Insert the hard disk tray back into Thecus VisoGuard NVR until it snaps into place. You can also lock it with a key if desired.
5. The LED blinks green when the HDD is accessed.

RAID Auto-Rebuild

When using RAID 1, 5, 6, or 10 on Thecus VisoGuard NVR, you can use the auto-rebuild function when an error is detected.

1. When a hard disk fails the system beeps and/or an email notification is sent to specified receivers.
2. Check the LCD to see which disk has failed.
3. Follow the steps mentioned above to replace the failed hard disk.
4. The system automatically recognizes the new hard disk and starts the auto-rebuild sequence to resume its status before the hard disk crash.

Chapter 7: Troubleshooting

Forgot My Network IP Address

If you forget your network IP address and have no physical access to the system, you can find out the IP address by either looking directly onto Thecus VisoGuard NVR LCD panel, or by using the setup wizard to retrieve the IP of your Thecus VisoGuard NVR.

1. Start the Setup Wizard, and it will automatically detect all Thecus VisoGuard NVR products on your network.
2. You should be able to find the IP address of Thecus VisoGuard NVR which you have forgotten in the **Device Discovery** screen.

Can't Map a Network Drive in Windows XP

You may have problems mapping a network drive under the following conditions:

1. The network folder is currently mapped using a different user name and password. To connect using a different user name and password, first disconnect any existing mappings to this network share.
2. The mapped network drive could not be created because the following error has occurred: **Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed.** Disconnect all previous connections to the server or shared resource and try again.

To check out existing network connections, type `net use` under the DOS prompt. You may refer the URL below for more network mapping information.

http://esupport.thecus.com/support/index.php?_m=downloads&_a=viewdownload&downloaditemid=57&nav=0

Restoring Factory Defaults

From the **System** menu, choose the **Factory Default** item and the **Reset to Factory Default** screen appears. Press **Apply** to reset Thecus VisoGuard NVR factory default settings.

WARNING

Resetting to factory defaults will not erase the data stored in the hard disks, but WILL revert all the settings to the factory default values.

Problems with Time and Date Settings

The administrator is able to select an NTP Server to keep Thecus VisoGuard NVR time synchronized. However, if Thecus VisoGuard NVR can not access the Internet, you may encounter a problem when setting the Time and Time Zone. If this happens:

1. Login to the Web Administration Interface.
2. Navigate to **System Management>Time**.
3. Under **NTP Server**, select **No**.
4. Set the **Date**, **Time**, and **Time Zone**.
5. Click **Apply**.

In addition, if Thecus VisoGuard NVR is able to access the Internet and you want to keep the NTP Server clock.isc.org by default, please make sure the DNS Server is correctly entered, thereby allowing the NTP Server name to correctly resolve. (See **System Network > WAN/LAN1 > DNS Server**)

Appendix A: Customer Support

If your Thecus VisoGuard NVR is not working properly, we encourage you to check out **Chapter 7: Troubleshooting**, located in this manual. You can also try to ensure that you are using the latest firmware version for your Thecus VisoGuard NVR. Thecus is committed to providing free firmware upgrades to our customers. Our newest firmware is available on our Download Center:

<http://www.thecus.com/download.php>

If you are still experiencing problems with your Thecus VisoGuard NVR, or require a Return Merchandise Authorization (RMA), feel free to contact technical support via our Technical Support Website:

http://www.thecus.com/support_tech.php

Customers in the US should send all technical support enquiries to the US contact window included in the following web page:

http://www.thecus.com/support_tech.php

For Sales Information you can e-mail us at:

sales@thecus.com

Thank you for choosing Thecus!



Appendix B: RAID Basics

Overview

A Redundant Array of Independent Disks (RAID) is an array of several hard disks that provide data security and high performance. A RAID system accesses several hard disks simultaneously, which improves I/O performance over a single hard disk. Data security is enhanced by a RAID, since data loss due to a hard disk failure is minimized by regenerating redundant data from the other RAID hard disks.

Benefits

RAID improves I/O performance, and increases data security through fault tolerance and redundant data storage.

Improved Performance

RAID provides access to several hard disk drives simultaneously, which greatly increases I/O performance.

Data Security

Hard disk drive failure unfortunately is a common occurrence. A RAID helps prevent against the loss of data due to hard disk failure. A RAID offers additional hard disk drives that can avert data loss from a hard disk drive failure. If a hard drive fails, the RAID volume can regenerate data from the data and parity stored on its other hard disk drives.

RAID Levels

The Thecus VisoGuard NVR supports standard RAID levels 0, 1, 5, 6, 10, and JBOD. You choose a RAID level when you create a system volume. The factors for selecting a RAID level are:

- Your requirements for performance
- Your need for data security
- Number of hard disk drives in the system, capacity of hard disk drives in the system

The following is a description of each RAID level:

RAID 0

RAID 0 is best suited for applications that need high bandwidth but do not require a high level of data security. The RAID 0 level provides the best performance of all the RAID levels, but it does not provide data redundancy.

RAID 0 uses disk striping and breaking up data into blocks to write across all hard drives in the volume. The system can then use multiple hard drives for faster read and write. The stripe size parameter that was set when the RAID was created determines the size of each block. No parity calculations complicate the write operation.

RAID 1

RAID 1 mirrors all data from one hard disk drive to a second one hard disk drive, thus providing complete data redundancy. However, the cost of data storage capacity is doubled.

This is excellent for complete data security.

RAID 5

RAID 5 offers data security and it is best suited for networks that perform many small I/O transactions at the same time, as well as applications that require data security such as office automation and online customer service. Use it also for applications with high read requests but low write requests.

RAID 5 includes disk striping at the byte level and parity information is written to several hard disk drives. If a hard disk fails the system uses parity stored on each of the other hard disks to recreate all missing information.

RAID 6

RAID 6 is essentially an extension of RAID level 5 which allows for additional fault tolerance by using a second independent distributed parity scheme (dual parity) Data is striped on a block level across a set of drives, just like in RAID 5, and a second set of parity is calculated and written across all the drives; RAID 6 provides for an extremely high data fault tolerance and can sustain two simultaneous drive failures.

This is a perfect solution for mission critical applications.

RAID 10

RAID 10 is implemented as a striped array whose segments are RAID 1 arrays. RAID 10 has the same fault tolerance as RAID level 1. RAID 10 has the same overhead for fault-tolerance as mirroring alone. High I/O rates are achieved by striping RAID 1 segments. Under certain circumstances, RAID 10 array can sustain up to 2 simultaneous drive failures

Excellent solution for applications that would have otherwise gone with RAID 1 but need an additional performance boost.

JBOD

Although a concatenation of disks (also called JBOD, or "Just a Bunch of Disks") is not one of the numbered RAID levels, it is a popular method for combining multiple physical disk drives into a single virtual one. As the name implies, disks are merely concatenated together, end to beginning, so they appear to be a single large disk.

As the data on JBOD is not protected, one drive failure could result total data loss.

Stripe Size

The length of the data segments being written across multiple hard disks. Data is written in stripes across the multiple hard disks of a RAID. Since multiple disks are accessed at the same time, disk striping enhances performance. The stripes can vary in size.

Disk Usage

When all disks are of the same size, and used in RAID, Thecus VisoGuard NVR disk usage percentage is listed below:

RAID Level	Percentage Used
RAID 0	100%
RAID 1	$1/n \times 100\%$
RAID 5	$(n-1)/n \times 100\%$
RAID 6	$(n-2)/n \times 100\%$
RAID 10	50%
JBOD	100%

n : HDD number

Appendix C: Licensing Information

Overview

This product included copyrighted third-party software licensed under the terms of GNU General Public License. Please see THE GNU General Public License for extra terms and conditions of this license.

Source Code Availability

Thecus Technology Corp. has exposed the full source code of the GPL licensed software. For more information on how you can obtain our source code, please visit our web site, <http://www.thecus.com>.

Copyrights

- This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
- This product includes software developed by Mark Murray.
- This product includes software developed by Eric Young (eay@cryptsoft.com).
- This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).
- This product includes PHP, freely available from (<http://www.php.net/>).
- This product includes software developed by the University of California, Berkeley and its contributors.
- This product includes software developed by Winning Strategies, Inc.
- This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>).
- This product includes software developed by Softweyr LLC, the University of California, Berkeley, and its contributors.
- This product includes software developed by Bodo Moeller.
- This product includes software developed by Greg Roelofs and contributors for the book, "PNG: The Definitive Guide," published by O'Reilly and Associates.
- This product includes software developed by the NetBSD Foundation, Inc. and its contributors.
- This product includes software developed by Yen Yen Lim and North Dakota State University.
- This product includes software developed by the Computer Systems Engineering Group at Lawrence Berkeley Laboratory.
- This product includes software developed by the Kungliga Tekniska Högskolan and its contributors.
- This product includes software developed by the Nick Simicich.
- This product includes software written by Tim Hudson (tjh@cryptsoft.com).
- This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

CGIC License Terms

Basic License

CGIC, copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004 by Thomas Boutell and Boutell.Com, Inc.

Permission is granted to use CGIC in any application, commercial or noncommercial, at no cost. HOWEVER, this copyright paragraph must appear on a "credits" page accessible in the public online and offline documentation of the program. Modified versions of the CGIC library should not be distributed without the attachment of a clear statement regarding the author of the modifications, and this notice may in no case be removed. Modifications may also be submitted to the author for inclusion in the main CGIC distribution.

GNU General Public License

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 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 redistributors 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