

TERANAS INSTANT STORAGE

Quick Installation Guide

SnaZio*
TERANAS HD



Table of Contents

Step 1	Detect TeraNAS with RAIDar	3
Step 2	Connect to Frontview Setup Wizard	7
Step 3	Setup Clock	10
	System Time	10
Step 4	Configure Networking	11
	Ethernet	
	DNS	
	DHCP	
Step 5	Select Security Level	14
	Windows	
	Workgroup	
Step 6	Setup File Sharing	16
	Services	
	Share List	
	Share Options	
	Add Share	
Step 7	Setup Print Sharing	21
Step 8	Configure System Settings	22
	Alerts Contacts	
	Password	
Step 9	All Done!	25



Step

1

Detect TeraNAS with RAIDar

The TeraNAS Installation CD contains RAIDar, a utility used for discovering the TeraNAS on your network.. This is useful in environments where the TeraNAS obtains a random DHCP IP address.

Note

RAIDar runs only on Windows. If you are using Mac OS X or Linux, you will need to discover the TeraNAS using your Terminal or Console session. Type


nmblookup -R VOLUME

to return the IP address of the TeraNAS, and enter **https://*ipaddr*/admin** in your browser to connect to the FrontView Setup Wizard. Then skip to **Step 2**.

On a Windows PC residing on the same network, install RAIDar from the CD. You will need approximately 40MB of disk space. Load the CD and double-click on **Setup.exe** to start the installation.

Note

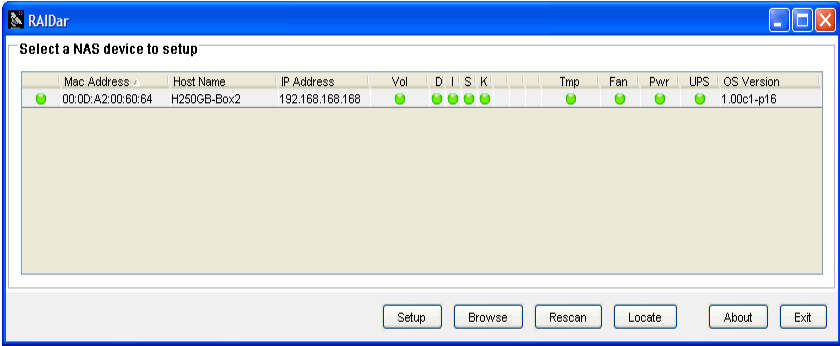
If your client has a static IP address, make sure it is on the same subnet as the TeraNAS device. You can do this by



configuring your client to obtain its IP address via DHCP. Even if your network does not have existing DHCP service, the TeraNAS device will assure that you will get an IP address.

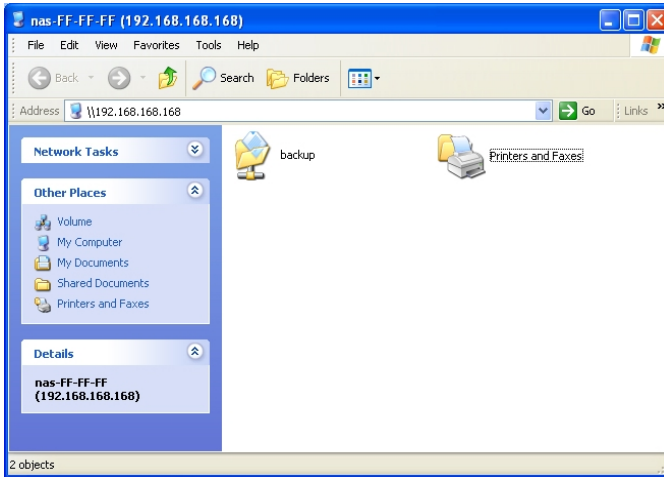


When you invoke RAIDar, your TeraNAS device will be detected when the device is in a ready state. If you have multiple TeraNAS devices on your network, match the MAC Address of the system to the address listed on the back of your system.





You can select the device and click **Browse** to access the default share called **backup**. The **backup** share can be used as a big repository for your data and backups.



The TeraNAS configures itself for anonymous guest access unless specified otherwise. Access to the backup share is granted to anyone but this can be changed in the security setup page of the Setup Wizard.

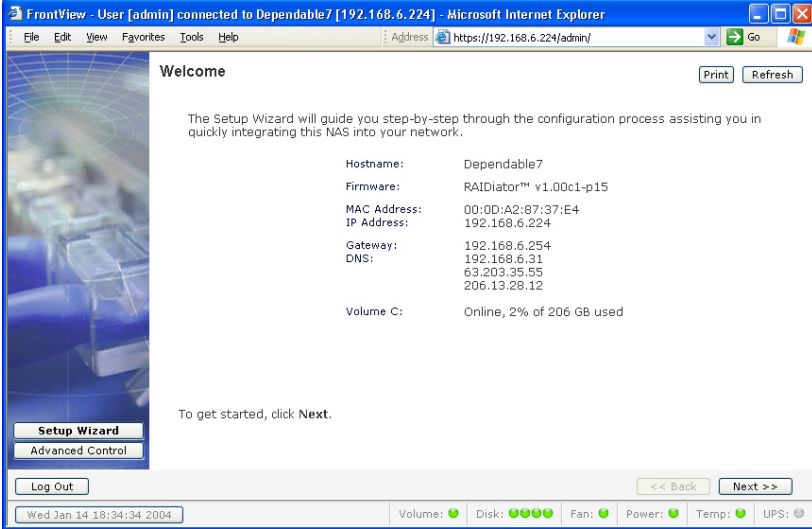
Step 2

Connect to FrontView Setup Wizard

Click **Setup** in RAIDar and you will be prompted to enter the login and password of the administrative user for the Setup Wizard. Use user name **admin** and password **infrant1** to log in.



A successful login will bring up the FrontView Setup Wizard.

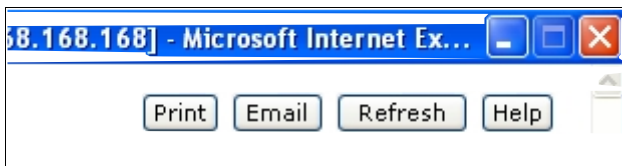


Most options in the FrontView Setup Wizard are pre-selected to fit most environments, so the wizard should not take too long to complete. It is highly recommended that you go through this wizard, especially if this is your first TeraNAS.

In a typical Setup Wizard process, you will set the clock, configure the networking, select the security mode, create shares, and set up an alert notification contact.

As you traverse through the setup pages, you will notice a familiar theme – a command bar in the upper right corner, navigation and status bar at the bottom, and the menu bar on the left.

The command bar typically provides options to print or email the page, refresh the browser window, and display help where available.



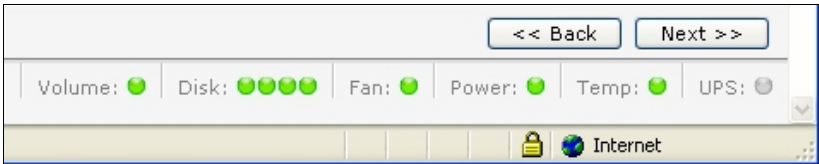


The navigation bar allows you to traverse through the wizard. Clicking **Next** implies that you have accepted the changes in the current window and wish to apply these changes. If an **Apply** button exists, you must click on the **Apply** button to save your changes before pressing **Next**. If multiple tabs exist in the menu page, clicking **Next** traverses through the tabs before continuing to the next menu page.

If you wish to log out of FrontView at any time, the **Logout** button will remind you to close all browser windows to securely log out.

The status bar right below the navigation bar provides instant health status of individual devices in the TeraNAS. Green LED indicates things are working normally and amber indicates a warning or failure condition. Refer to the TeraNAS User Guide for more information on other LED indications.

The menu bar on the left provides the option to switch between **Setup Wizard** and **Advanced Control** modes. More menus are available once you enter the advanced mode.



Step 3

Setup Clock

System Time

Clicking the **Next** button in the Welcome page brings up the Clock page. Here, you can set the date, time, and time zone. Set appropriately to ensure files maintain proper timestamp.

Clock Print Refresh

System Time

Proper clock setup is recommended to ensure proper file time-stamping. Please enter the current date and time.

Date:

Time: : :

Timezone:

Click **Next** to set up networking.

Step 4

Configure Networking

Ethernet

You can accept the default Ethernet settings if the TeraNAS is installed in a network environment where DHCP service is used. Otherwise, specify a static address.

If you assign static IP addresses, beware that the browser will lose connection to the TeraNAS device after the IP address has been changed. If you encounter this, you can click **Rescan** in RAIDar to rediscover the device and reconnect from there.

Click **Next** to display the **DNS** tab.

The screenshot shows the 'Network' configuration page with the following details:

- Buttons: Print, Email, Refresh
- Tabs: Ethernet (selected), DNS, DHCP
- Instructions: Enter the hostname and IP address information for this network interface. If your network utilizes a DHCP server to hand out IP addresses, select the DHCP option for your IP assignment method. Otherwise, enter the IP address, netmask, and gateway values accordingly.
- MAC address: 00:00:A2:00:40:90
- Status: Online / 100 Mbit / Full-Duplex
- Hostname: Dependable7
- IP assignment: Use values from a DHCP server (dropdown menu)
- IP address: 192.168.6.168
- Netmask: 255.255.255.0
- Default gateway: 192.168.6.254
- Buttons: Renew now

DNS

If you had selected the DHCP option in the Ethernet tab, the domain name server fields will be automatically filled based on the settings from your DHCP server. If you had selected the Static option, you can manually enter the entries here.

Network

DNS, or Domain Name Service, provides a means to translate hostnames to IP addresses. Enter the DNS IP addresses here.

Domain name server 1:	<input type="text" value="192.168.6.31"/>
Domain name server 2:	<input type="text" value="63.203.35.55"/>
Domain name server 3:	<input type="text" value="206.13.28.12"/>
Domain name:	<input type="text" value="dependable7.com"/>

Click **Next** to display the **DHCP** tab.



DHCP

The DHCP tab allows this device to act as a DHCP server. This is convenient in networks where DHCP service is not available, automating the task of assigning IP addresses to new clients.

The DHCP option is available only if this device is not already using a DHCP address. Enabling DHCP service on a network already utilizing a DHCP server will introduce conflicts. If you wish to use this device as a DHCP server, make sure to specify static addresses in the Ethernet and DNS tabs.

Network Print Email Refresh

Ethernet DNS **DHCP**

DHCP, or Dynamic Host Configuration Protocol, service provides a way for individual computers on the IP network to automatically obtain an IP address along with other network parameters to help reduce network administration.

Enable DHCP service.

Starting IP Address: 192.168.6.

Ending IP Address: 192.168.6.

Lease Time (min):

Click **Next** to configure the TeraNAS security.

Step 5

Select Security Level

Windows

Next, you need to select the Windows security mode that's appropriate for your environment. The default **Home or small office** mode (also referred to as **Share mode**) is appropriate for the home or smaller office environments where everyone on the network will be using this device as a big repository for shared data. Shares in this mode can be protected with a password.

The other options may be more appropriate for a larger office or corporate environment and are covered in the **User Guide**.

Security

Windows Workgroup

Select the Windows network environment where this NAS will be deployed.

- Home or small office.** Select this option if you would like to restrict share access with the use of an optional share password. Each user accesses the shares on the device as a common guest user and will have the same read/write privilege as other users. This option supports setting disk quotas on a per-share basis.
- Medium-size office or workgroup.** Select this option if you would like to control access to shares based on user or group accounts and your network does not utilize a domain controller for authentication. If you select this option, you will need to create a user account for anyone accessing this device. This option supports setting disk quotas on a per-user or per-group basis.
- Department or corporate environment.** Select this option if you would like to control access to shares based on user and group accounts and your Windows network utilizes a centralized domain controller or active directory service (ADS) for login authentication. This option supports setting disk quotas on a per-user or per-group basis. Do not select this option otherwise or if you are unsure.



Workgroup

Click **Next** and you will be prompted to enter the workgroup name. Enter a workgroup name of up to 15 characters. You can elect to keep the default name.

Security Print Email Refresh

Windows **Workgroup**

Enter the Windows network workgroup name.

Workgroup/Domain:

Click **Next** to configure file sharing.

Step 6

Setup File Sharing

Services

After selecting the security model, you can create shares. A share is simply a network folder on the TeraNAS that clients communicating in various file access protocols from different operating systems can access.

You'll first need to select the file protocols you wish to enable in the Services tab. CIFS for Windows clients, NFS for Unix/Linux, AFP for Macs, HTTP for browser, and FTP for anonymous file uploads and downloads.

For our example, we'll enable all services to show how shares will be accessed using each protocol. For your environment, only enable the services you plan to use. CIFS and HTTPS cannot be disabled.

When you click **Next**, you are presented with the share list for Volume C. Volume C is the initial volume pre-configured on the TeraNAS.

Shares Print Email Refresh Help

Services Volume C Printer

Select the file sharing protocol you wish to enable. In general, disable the protocols you do not intend to use. You can always enable them later. Click **Help** for more information.

- CIFS**, or Common Internet File System, used by Windows and Mac OS X clients.
- NFS**, or Network File System, used in Unix or Linux environments.
- AFP**, or AppleTalk Filing Protocol, used by Mac OS 9 and earlier.
- FTP**, or File Transfer Protocol, used extensively for basic file upload and downloads.
- HTTP**, or Hypertext Transfer Protocol, used everywhere web browsers exist.
- HTTPS**, or HTTP with SSL encryption, used where secure web access is desired.



Note

The default volume configuration is a redundant RAID level setting that provides the best capacity. A two-disk configuration is configured as a RAID level 1 volume. A three or more disk configuration is configured as a RAID level 5 volume. With these settings, in case a disk fails, the TeraNAS device will continue to function in degraded mode until the failed disk is replaced.



Share List

The Share List tab lists the shares currently available on the TeraNAS. As an example, the share, **backup**, has been pre-configured with default access.

You'll notice share icons representing the access privilege for each file access protocol. You can hover the mouse pointer over the access icons to get a quick glimpse of the access settings.

If more advanced access control is desired, click on an icon to manage the share access options.

Shares Print Email Refresh Help

Services **Volume C** Printer

Disk space: 1% of 206 GB used
Additional 10 GB reserved for snapshots

Share List Add Share

Click on a document icon to customize the access control. Place the mouse cursor over the icon to display the current access level in the status bar. Quota values of 0 disables quota enforcement. For instruction on how to access the shares, click [Help](#).

Share Name	Description	Password	Disk Used	Quota (MB)	Win	Unix	Web	Delete
backup	Backup Share		0 MB	0				

- Disabled
- Read-only Access
- Read/Write Access
- Read Access with exceptions
- Write Access with exceptions




Share Options

In the **Share Options** tab, you can list hosts you wish to limit share access to. When you specify a host in the allow list, no other hosts will be able to access the share using the selected file protocol. Hosts can be listed as IP addresses or valid DNS names separated by commas.

For more information on share access setup, please refer to the **User Guide**.

Shares Print Email Refresh Help

Services **Volume C** Printer

Disk space:  5% of 206 GB used
Additional 10 GB reserved for snapshots

Share List Add Share **Share Options**

Windows [CIFS] Unix [NFS] Web [HTTP/HTTPS]

Share Name: **backup** Default Access: Read/write ▼

Hosts allowed access:




Add Share

To add more shares, click on the **Add Share** tab. You can enter up to five share names with share descriptions. In the **Share** security mode, you can optionally assign a share password and disk quota. The disk quota feature allows you to limit disk usage on a share-by-share basis.

Shares Print Email Refresh Help

Services **Volume C** Printer

Disk space:  5% of 206 GB used
Additional 10 GB reserved for snapshots

Share List **Add Share**

Enter the share names and descriptions you wish to add. You can optionally specify a share password and share-level disk quota. Disk quota value of 0 disables quota enforcement.

Share Name	Description	Password (optional)	Disk Quota	
Brochure	Marketing Brochures	••••••••	2000	MB
Finance	Company Finance	••••••••••	10000	MB
Spec	Engineering Specs	••••••••	2000	MB
Drawings	Design Drawings	••••••••	3000	MB
Music	Shared Music		0	MB

In the figure above, five shares are being added, with a password and disk quota specified for the first four shares.

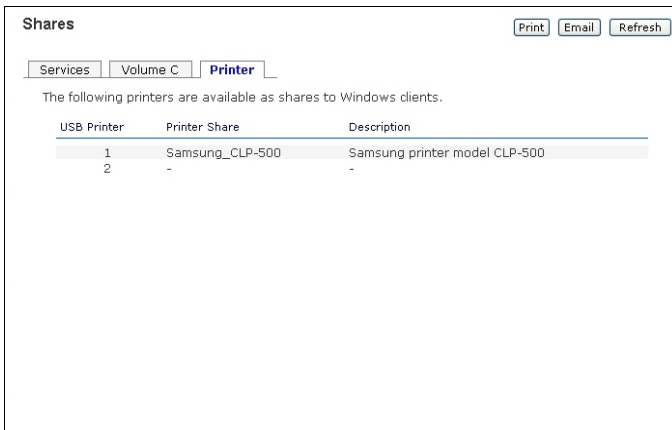
When you are done adding shares, click **Next** to setup print shares.

Step

7

Setup Print Sharing

If you have not already done so, you can connect up to two USB printers to the TeraNAS now. Wait a few seconds, and click Refresh to view it in the Printer tab list. The print share name will automatically reflect the manufacturer and model of your printer. To assign a printer driver to a print share, click **Browse** in RAIDar or simply enter `\\hostname` in the Explorer address bar, and double-click the printer icon.



Click **Next** to set up alert contacts.

Alerts Contacts

In the **Contacts** tab, enter one or more email addresses you wish to use as the system alert contact. Email alerts are the most effective way for the TeraNAS device to notify you of various system status, warnings, and fatal system errors.

Use the **Send Test Message** option to verify that alert messaging is working. If you do not receive the test message, check the network gateway and DNS settings. Also, some network firewalls prevent unknown message transfer agents (MTA), such as that used by the TeraNAS, from working. If this is the case, you will need to specify a remote SMTP server in Advanced Control mode when you are done with the Setup Wizard. This method is covered in the TeraNAS User Guide.

System Print Email Refresh

Alerts

Contacts

In case of disk failure, enclosure problems, quota violations, low disk capacity, and other system warnings and error events, alert messages will be sent to the email addresses listed below. This is the preferred way that this device communicates its status with you, so please make sure to fill out primary and secondary contacts here.

Enter email address(es)

Alert Contact 1: Send Test Message

Alert Contact 2:

Alert Contact 3:



Note

Various email services may filter out the test message and actual email alerts sent by the TeraNAS. Verify that the test message arrives at the email destination before continuing.



Password

The password tab allows you to change the default password assigned for the **admin** user. You are required to change the password before continuing. Please keep the password in a safe place.

In addition, you will need to specify a password recovery question and the expected answer, along with your email address. This allows you to reset the password on the TeraNAS in case the password is lost. You can refer to the User Guide for information on how this is done.

System Refresh

To change a password you will need to additionally specify a password recovery question, the expected answer, and an email address. In case you forget the admin password, you can reset the password by answering the password recovery question correctly and specifying the email address where the new admin password will be sent. **There is no other way to recover a lost password without setting the device back to factory default.**

New admin password:

Retype admin password:

Password recovery question:

Password recovery answer:

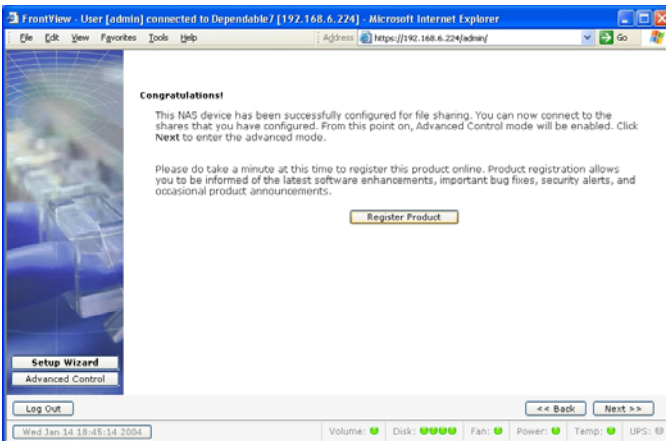
Password recovery email address:

All Done!

At this point, register your TeraNAS by clicking on **Register Product**. This puts your TeraNAS into our warranty and support database and allows us to inform you of the latest software enhancements, bug fixes, and security alerts.

Click **Next** to continue with the **FrontView Advanced Control** mode. Advance Control options are documented in the TeraNAS User Guide.

If you wish, you can now start accessing the shares that you have just created using the Windows Explorer. For instructions on how to access the shares from Windows or other operating systems, refer to the Accessing Shares chapter in the User Guide.





Copyright © 2005 **V One Multimedia**. All rights reserved.

<http://www.snazio.com>

TeraNAS, FrontView, RAIDar, RAIDiator, Network Storage Processor, and NSP are trademarks or registered trademarks of V One Multimedia. All other product names are the property of their respective owner.