



**TerraMaster TNAS**

# **Operation Instruction**

Model:F2-NAS 2/F4-NAS

## Contents

1. System Settings	3
1.1 General Settings	3
1.2 Network Setting	4
1.3 Hardware Setting	5
1.4 Startup Tasks	5
1.5 Security Setting	5
1.6 Notification Setting	6
1.7 Power Manager	6
1.8 System Logs	6
1.9 Software Update	7
1.10 Restore to Factory Default	8
2. Authority Setting	8
2.1 Users	8
2.2 User Groups	9
2.3 Hardware Setting	9
2.4 Quota	10
3. Network Service	10
3.1 Samba	10
3.2 Apple Networking	10
3.3 LNFS Service	10
3.4 FTP	11
3.5 Telnet/SSH	11
3.6 SNMP Setup	11
3.7 Web Server	12
3.8 Virtual host	13
3.9 Discovery Service	13
4. Applications	14
4.1 iTunes Server	14
4.2 MySQL Server	14
4.3 Backup Server	15
4.4 UPnP Media Server	15
5. File Manager	15
5.1 File Management via Tcloud	15
5.2 File Management via web browser	16
6. Tcloud	16
6.1 Cloud User List	16
6.2 Create Cloud Users	17
6.3 Enable Cloud Functions for Existing Users	17
6.4 TCloud Login	18

7. Storage Manager .....	19
7.1 Disk Manager .....	19
7.1.1 Hard Disk Information .....	19
7.1.2 Hard Disk Group .....	20
7.1.3 Encrypt File System .....	20
7.1.4 iSCSI Storage .....	21
7.2 Virtual Disk .....	23
7.3 External Storage Device .....	24
8. Backup .....	25
8.1 Rsync Backup .....	25
8.2 Time Machine .....	27
8.3 Backup to External Devices .....	27
9. Download Center .....	28
9.1 BT/PT Download .....	28
9.2 Thunder Remote Download .....	28
10. System Information .....	29
10.1 Hardware Information .....	29
10.2 Service Status .....	29
10.3 Resource Monitor .....	29

# 1. System Settings

This paper introduces the operations and settings of TNAS. In many cases, an administrator account is required to log into TOS. Default factory administrator name: admin; initial password: admin.

**You can log into TOS via the following means:**

1. Log in via Tcloud desktop application. To run Tcloud on a PC, search TNAS device in the network, select found TNAS, click "Log in", and input a user name and password; an operator can log into the system.
2. To log in via TNAS IP address: input IP address of TNAS at the URL field of the webpage browser, e.g., <http://192.163.1.100>, an operator can log into TOS. The IP address of TNAS can be obtained via the

## 1.1 General Settings

To log into TOS via an administrator account and go to "Control Panel"> "System Setting">"General Setting", a user can set the device name, time and language.

### Device name:

Users can name TNAS according to their preferences, with letters (a-z, A-Z), numbers (0-9), and dash (-) only.

### Communication port:

A port number for system connection shall be assigned to TNAS, which is 8181 by default.

### Secure Sockets Layer (SSL):

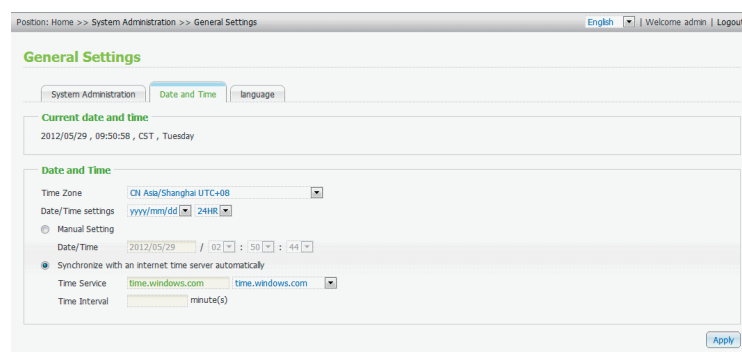
If the Administrator allows other users to login TNAS by means of SSL, please enable the SSL function and input the communication port number. When the option of "Use SSL Only" is enabled, users can only access TNAS via HTTPS.

Note: If a user wants to remotely log in to TNAS by SSL on Internet, but TNAS is connected to the back-end of a NAT router, then the port 443 has to be opened and linked to the IP address of TNAS.

### Date and Time

Please select the correct time zone, then set the right date and time for TNAS. If the date and time setting is incorrect, the following problems may occur:

- The file access time may be inconsistent with the actual time.
- The time of the event may not be accurately displayed when checking the event log of the system.



The screenshot shows the 'General Settings' page in the TOS interface. The breadcrumb path is 'Position: Home >> System Administration >> General Settings'. The page has tabs for 'System Administration', 'Date and Time', and 'Language'. The 'Date and Time' tab is active, showing the 'Current date and time' as '2012/05/29, 09:50:58, CST, Tuesday'. Below this, the 'Date and Time' section includes a 'Time Zone' dropdown set to 'CN Asia/Shanghai UTC+08', a 'Date/Time settings' dropdown set to 'yyyy/mm/dd' with a '24HR' time format, and a 'Manual Setting' section with 'Date/Time' set to '2012/05/29' and '02:50:44'. There is also a 'Synchronize with an internet time server automatically' section with 'Time Service' set to 'time.windows.com' and 'Time Interval' set to 'minute(s)'. An 'Apply' button is at the bottom right.

### Synchronize with an internet time server automatically:

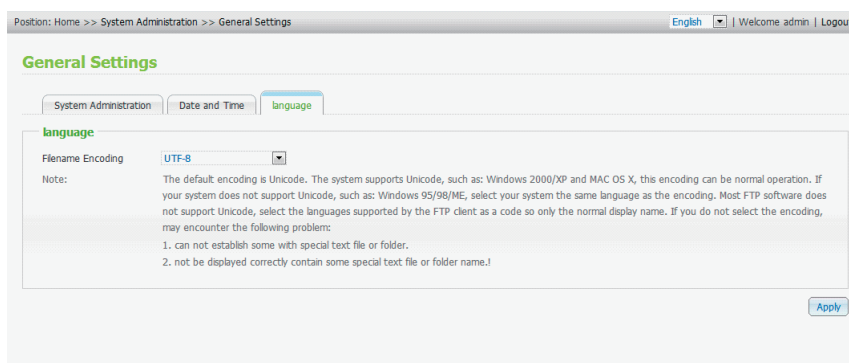
TNAS will automatically synchronize the date and time with a specified NTP (Network Time Protocol) time server if “Synchronize with an internet time server automatically” is enabled. You need to enter the IP address of NTP server and the time interval here. TNAS shall be connected to the Internet so as to make this function work.

Note: It may take a few minutes for the time synchronization to finish the first time.

### Language:

Please choose the language code for the display of files and folders in TNAS.

Note: The default code of TOS is Unicode. If your system does not support Unicode, select the same language code as that of your system. Most FTP software does not support Unicode, so please select the language code supported by FTP software. If the language code is incorrect, the names of some files or folders may not be displayed correctly.



## 1.2 Network Setting

To log into TOS with an administrator account and go to “Control Panel” > “System Settings” > “Network Setting”, a user can set TCP/IP address, Wi-Fi network and DDNS parameters.

### TCP/IP Setting:

To go to “Control Panel” > “System Settings” > “Network Setting” > “TCP/IP”, a user can select the type of IP address and set the sub-mask and gateway information here.

### Wi-Fi Network:

Users can connect TNAS with the Internet using a USB wireless network card. To do this, please insert a USB wireless network card into the USB port of TNAS and go to “Control Panel” > “System Settings” > “Network Setting” > “Wi-Fi Network” for Wi-Fi network setting.

Note: TNAS supports only one USB wireless network card at one time.

TNAS only supports the Wi-Fi dongle officially supplied by TerraMaster. Please visit the TerraMaster official website for details.

### DDNS Settings:

DDNS is a way to allow users remote access to TNAS through the Internet. Before setting DDNS, users need to register a web address on the DDNS service provider’s platform.

Here are DDNS service providers that TNAS supports:

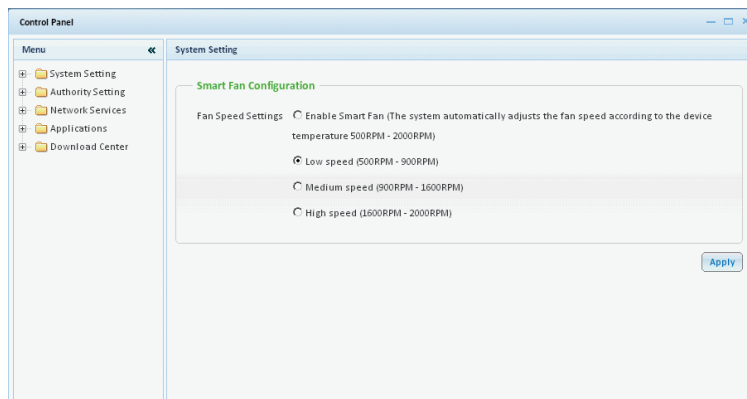
<http://www.dyndns.com>

<http://www.no-ip.org>

To set DDNS, go to “Control Panel” > “System Settings” > “Network Setting” > “DDNS”, fill in the information you got from the DDNS service registration in the form, then click “Apply” to finish. To perform remote access to TNAS via DDNS, please input the web address you got from the DDNS provider in the address bar of the web browser, and go to the TNAS remote login page, where users can go to the user name and password for remote login.

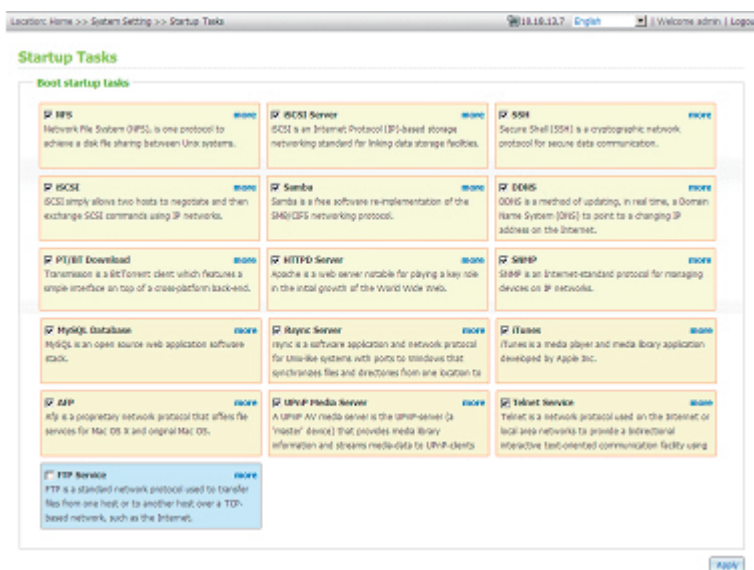
### 1.3 Hardware Setting

To set the fan speed of TNAS, go to “Control Panel” > “System Settings” > “Hardware Setting”. The available options include Enable Smart Fan, Low Speed, Medium Speed and High Speed. Smart fan is recommended.



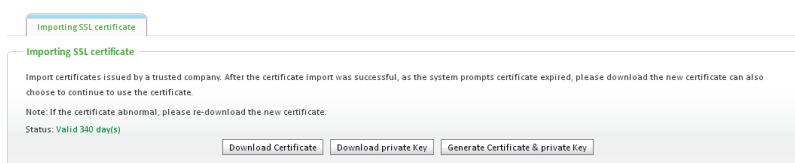
### 1.4 Startup Tasks

Users can choose to boot startup tasks upon TNAS booting. Please go to “Control Panel” > “System Setting” > “Startup Tasks” and check the required startup tasks. Note: too many startup tasks may influence the boot speed of TNAS.



### 1.5 Security Setting

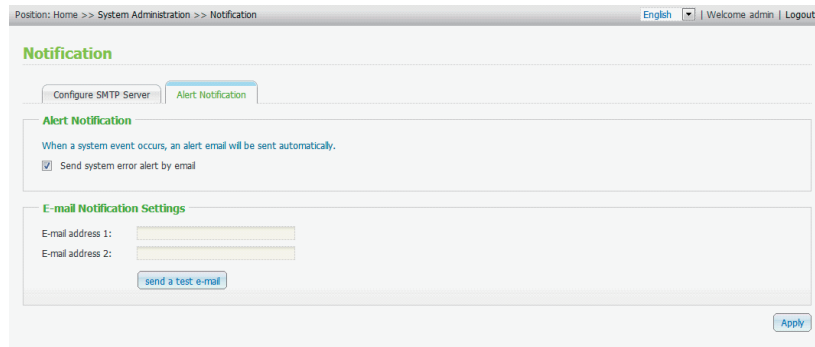
The SSL is a secure communication protocol and can encrypt data to transfer. The SSL secure certificate and key has a use time period. After the certificate expires, you should update the SSL certificate and key. Please go to “Control Panel” > “System Setting” > “Security Setting” to view the time period or import a new security certificate.



**Note:** If user imports an incorrect security certificate, it will result in a failure in login via SSL.

## 1.6 Notification Setting

When the administrator enables the “Alert Notification” function and TNAS has a system error, the system will send the alarm or notification to the user via email. To use this function, please go to “Control Panel” > “System Settings” > “Notification Setting” > “Alert Notification” and check “Enable” and fill the in email address of the receiver. Please go to “Control Panel” > “System Settings” > “Notification Setting” > “SMTP server setup” and set the email-sending server.



The screenshot shows the 'Notification' settings page. At the top, there are two tabs: 'Configure SMTP Server' and 'Alert Notification'. The 'Alert Notification' tab is active. Below the tabs, there is a section titled 'Alert Notification' with a description: 'When a system event occurs, an alert email will be sent automatically.' There is a checkbox labeled 'Send system error alert by email' which is checked. Below this, there is a section titled 'E-mail Notification Settings' with two input fields for 'E-mail address 1' and 'E-mail address 2'. There is a 'send a test e-mail' button and an 'Apply' button at the bottom right.

## 1.7 Power Setting

By going to “Control Panel” > “System Settings” > “Power Setting”, users can restart or shut down TNAS, and set the schedule for system power. Users can also set up the power handling method when the power is restored from an abnormal power outage, for example, the power cord is removed.

### Start/Shutdown:

Restart or shut down TNAS immediately.

### Buzzer Control:

While the buzzer alert is switched on, the buzzer will sound in case of startup, shutdown, software update, error, warning prompt, etc.

### Power Resumption Settings:

Configure TNAS to resume to the previous power-on or power-off status, turn on, or remain off when the AC power resumes after a power outage.

### Power On/Power Off/Restart Schedule Setting:

Specify a schedule for automatic system power on, power off or restart at certain time on any day in a week or every day. Unlimited schedules can be set.

## 1.8 System Logs

### System Event Logs :

NAS can store 10,000 event logs, including warning, error and information messages. If system does not function correctly, please go to “Control Panel” > “System Settings” > “System Logs” > “System Event Logs” to check event logs for more details, which can be used as reference for troubleshooting.

Note: Right click a log with mouse to delete or clear the record.

Position: Home >> System Setting >> System Logs

10.18.13.25 English Welcome admin Logout

### System Logs

System event logs System connection logs On-line users

All services Clear Apply

Type	Time	User	Server IP	Server Port	Client IP	Client Port	Hostname	Information
http	2013-11-29 15:29:25	admin	10.18.13.25	8600	10.18.6.150	57070	Tnas-941029	Login System Manage Successful
http	2013-11-28 09:03:50	admin	10.18.13.25	8600	10.18.13.121	49856	Tnas-Qin	Login System Manage Successful
http	2013-11-26 14:34:50	admin	192.168.1.106	8600	192.168.1.116	62160	Tnas-Qin	Login System Manage Successful
http	2013-11-26 10:43:01	admin	10.18.13.25	8600	10.18.13.112	3142	Tnas-Qin	Login System Manage Successful
http	2013-11-25 17:50:52	admin	10.18.13.25	8600	27.44.208.67	1332	Tnas-Qin	Login System Manage Successful
http	2013-11-22 09:48:38	admin	10.18.13.25	8600	10.18.13.104	50423	Tnas-Qin	Login System Manage Successful
http	2013-11-21 11:37:27	admin	10.18.13.25	8600	112.228.7.88	56952	Tnas-Qin	Login System Manage Successful
http	2013-11-20 15:02:32	admin	10.18.13.25	8600	10.18.13.155	4473	Tnas-Qin	Login System Manage Successful
http	2013-11-19 14:19:29	admin	10.18.13.25	8600	61.142.7.36	60981	Tnas-Qin	Login System Manage Successful
http	2013-11-19 14:19:24	admin	10.18.13.25	8600	10.18.9.46	1860	Tnas-Qin	Login System Manage Successful

Total: 18 | Display 10 | Per Page

### System Connection Logs:

By going to “Control Panel” > “System Setting” > “System Logs” > “System Event Logs”, it’s available to view the record of TNAS connection through HTTP, FTP, Telnet, SSH, AFP and Samba.

Position: Home >> System Setting >> System Logs

10.18.13.25 English Welcome admin Logout

### System Logs

System event logs System connection logs On-line users

All services Clear Apply

Type	Time	User	Server IP	Server Port	Client IP	Client Port	Hostname	Information
http	2013-11-29 15:29:25	admin	10.18.13.25	8600	10.18.6.150	57070	Tnas-941029	Login System Manage Successful
http	2013-11-28 09:03:50	admin	10.18.13.25	8600	10.18.13.121	49856	Tnas-Qin	Login System Manage Successful
http	2013-11-26 14:34:50	admin	192.168.1.106	8600	192.168.1.116	62160	Tnas-Qin	Login System Manage Successful
http	2013-11-26 10:43:01	admin	10.18.13.25	8600	10.18.13.112	3142	Tnas-Qin	Login System Manage Successful
http	2013-11-25 17:50:52	admin	10.18.13.25	8600	27.44.208.67	1332	Tnas-Qin	Login System Manage Successful
http	2013-11-22 09:48:38	admin	10.18.13.25	8600	10.18.13.104	50423	Tnas-Qin	Login System Manage Successful
http	2013-11-21 11:37:27	admin	10.18.13.25	8600	112.228.7.88	56952	Tnas-Qin	Login System Manage Successful
http	2013-11-20 15:02:32	admin	10.18.13.25	8600	10.18.13.155	4473	Tnas-Qin	Login System Manage Successful
http	2013-11-19 14:19:29	admin	10.18.13.25	8600	61.142.7.36	60981	Tnas-Qin	Login System Manage Successful
http	2013-11-19 14:19:19	Tnas-Qin	10.18.13.25	8600	10.18.9.46	1860	Tnas-Qin	Username not exist!

Total: 45 | Display 10 | Per Page

### On-line Users :

Go to “Control Panel” > “System Settings” > “System Logs” > “On-line Users”, and the information of the on-line users connecting to TNAS is shown on this page.

Position: Home >> System Administration >> System Logs

English Welcome admin Logout

### System Logs

System event logs System connection logs On-line users

Type	Time	User	Server IP	Server Port	Client IP	Client Port	Hostname	Information
Total: 0 Records								

## 1.9 Software Update

Go to “Control Panel” > “System Settings” > “Software Update”, and a user can update TOS software of TNAS on this page.

Position: Home >> System Administration >> Firmware Update

English Welcome admin Logout

### Firmware Update

Software update

Software update

Current version: FINAS\_S1\_0\_V1.244

Before updating system software, please make sure the product model and software version are correct. Follow the steps below to update software:

Step 1: Download the release notes of the same version as the software from terramaster website <http://www.terramaster.com/> Read the release notes carefully to make sure you need to update the software.

Step 2: Before updating system software, back up all disk data on the server to avoid any potential data loss during system update.

Step 3: Click the [Browse...] button to select the correct software image for system update. Click the [UPDATE SYSTEM] button to update the software.

Please select an upgrade package!

Users can select “update online”, and TNAS will detect the available new version of TOS software and update automatically. TNAS should keep a connection with the Internet during the update. Users can also visit the “Download Center” of the TerraMaster website to select a proper TOS version for downloading and updating manually.



## 1.10 Restore to Factory Default

To restore the factory settings of TNAS, go to “Control Panel” > “System Settings” > “Restore to Factory Default” and click “RESET” to restore the system configurations of TNAS to factory default.

Warning: When “RESET” is pressed on this page, all the user accounts, network disk and system settings will be cleared and restored to default.

# 2. Authority Setting

Go to “Control Panel” > “Authority Setting”, and then users can set the user, user group, shared folder and capacity limit.

## 2.1 Users

The following user accounts have been created by default in the system:

- **Admin**

Admin is defaulted administrator, a member of the administrator user group with the highest authority. It cannot be deleted.

- **Guest**

Guest is a guest account, a system default user that would not be displayed on the user listing. Guest does not belong to any user group. User can't delete it or set a password.

- **All users**

“All users” is a guest account, a system default user that would not be displayed on the user listing. This account is used if users visit TNAS through FTP. User can't delete it or set a password.

A new user account can be created by the administrator; the following information is required to create a new user:

- **User name**

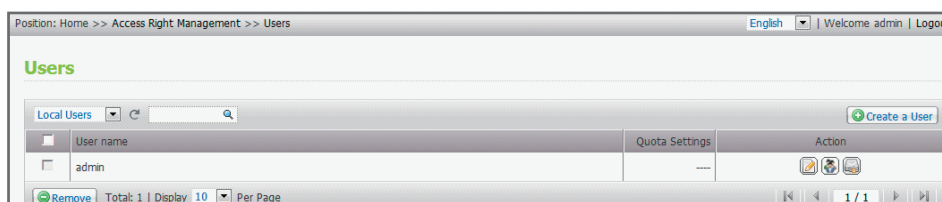
The user name can contain a maximum of 32 characters, is not case-sensitive but cannot contain such characters as: " / \ [ ] : ; | = , + \* ? < > ` ' .

- **Password**

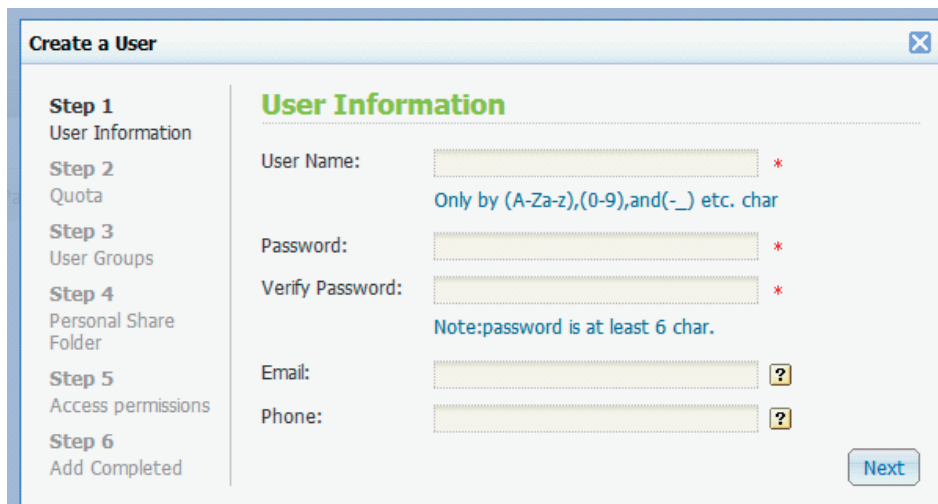
The password is case-sensitive and supports a maximum of 16 characters. It is recommended to use a password of at least 6 characters.

### Create a User

To create a user account, please go to “TOS” > “Control Panel” > “Authority Setting” > “Users” and click “Create a User”.



Follow the instructions to complete the user information, and click “OK” to create a user account



Note: users can remote login TNAS via Internet from anywhere only when “Enable Remote Access” is

## 2.2 User Groups

User group is a group of users with the same access rights to files or folders. TOS has created the following user groups by default:

- **Admin**

All the members in this group have the administration rights of TNAS. This group cannot be deleted.

- **All users**

All the registered users belong to the “All users” group. This group cannot be deleted.

Administrator can add user groups. To add user groups, users should go to “TOS” > “Control Panel” > “Authority Setting” > “User Group” page, click “Create a group”, fill in information according to the prompt and click “OK” to add. A group name can contain a maximum of 256 characters, not case-sensitive but cannot contain such characters as: “ / \ [ ] : ; | = , + \* ? < > ` ”

## 2.3 Shared Folders

Shared folder is a network disk space where users can create a couple of different shared folders for storing data of a different nature, or for different users or user groups to access files.

Log in to TOS, and go to “Control Panel” > “Authority Setting” > “Shared Folders”, where users can view the information and status of a shared folder or edit it.

Administrator or user can add new shared folders. To add new shared folders, go to “Control Panel” > “Authority Setting” > “Shared Folders” page, click “Add share folder”, fill in information according to the prompt, and finally click “OK”.

Users can set the read/write access for the shared folder and its sub-folder. To set the read/write access for the shared folder, please go to “TOS” > “Control Panel” > “Authority Setting” > “Shared Folders” page, select a network folder, and then click “Edit”.

### ISO Shared Folders

Users can mount the ISO image files on TNAS as an ISO image shared folder. TNAS supports mounting up to 256 ISO image files.

To mount an IOS image file, please log in to TOS with an administrator account, go to “Control Panel” > “Authority Setting” > “Shared Folders” > “ISO Shared Folders”, click “Mount an ISO file”, select the ISO image file and click “Mount”.

## 2.4 Quota

Administrator can set quota for all users in “Control Panel” > “Authority Setting” > “Quota”. When user has reached the quota size, the user cannot add any more date. By default, no quota is set for the users.

# 3. Network Service

## 3.1 Samba

Log in to TOS with an administrator account, go to “Control Panel” > “Network Service” > “Samba”, and enable “samba service” so that users can access and store the files on TNAS via a LAN.

### Workgroup:

Workgroup of TNAS by default. Administrator can also rename workgroups which belong to TNAS.

### SAMBA recycle bin:

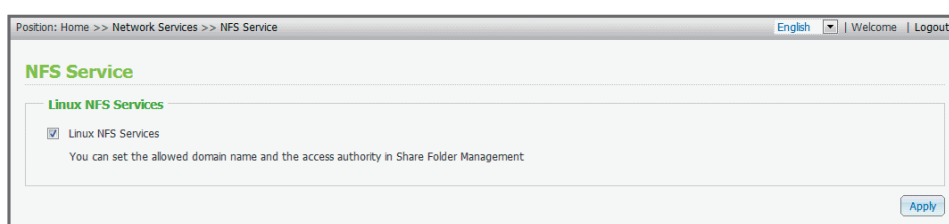
When the Samba recycle bin is enabled, the deleted data will be moved to recycle bin for temporary storage. To enable this function, please click “Apply” after checking this option. “Empty Samba recycle bin” means to empty the data in the recycle bin.

## 3.2 Apple Networking

Enable this service if on MAC OS Apple computer. To do this, go to “Control Panel” > “Network Services” > “Apple Networking” and click “Enable Apple Networking”.

## 3.3 NFS Service

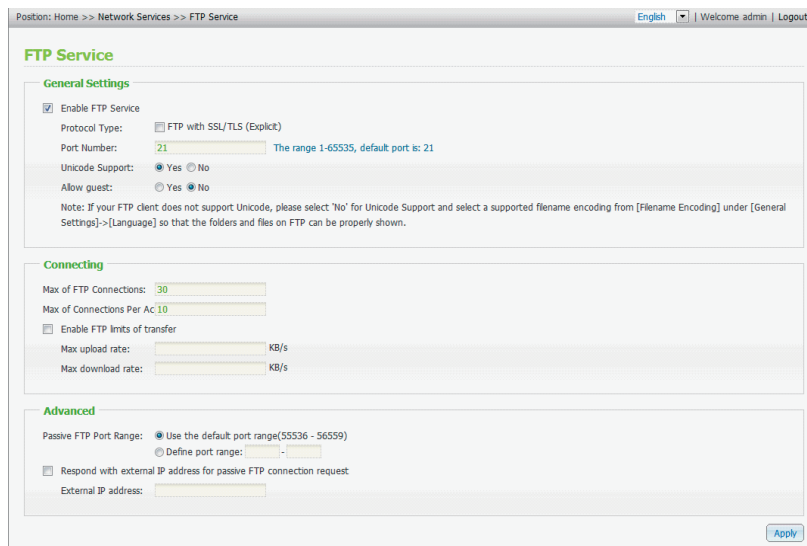
If for Linux OS, please enable NFS service. To do this, go to “Control Panel” > “Network Services” > “NFS Service” and enable “Linux NFS Services”.



### 3.4 FTP

To use the FTP service of TNAS, go to “Control Panel” > “Network Services” > “FTP Service” and check “Enable FTP Service”.

When FTP service is enabled, users can set the maximum of FTP connections and the maximum upload and download rate.



#### Unicode Support:

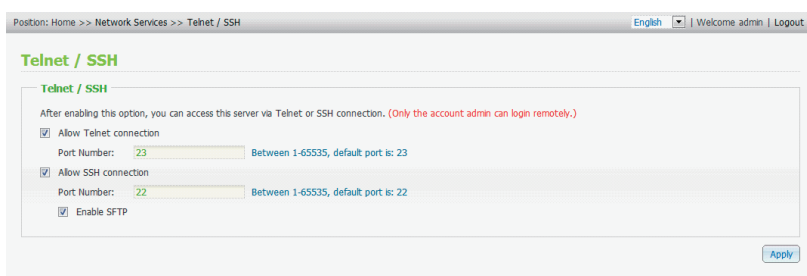
Users can set whether to support Unicode. Generally, “No” is set by default.

#### Passive FTP Port Range:

Users can use the default port range (55536-56559) or define a port range above 1024. If this option is checked, make sure the specified communication port is enabled on router or firewall.

### 3.5 Telnet/SSH

Users can log in to TNAS via Telnet or SSH connection, but only the administrator account can login remotely. Go to “Control Panel” > “Network Services” > “Telnet/SSH” to enable this option. User are advised to download a Telnet or SSH connection application; for example, Putty. Make sure the specified ports have been enabled on the router or firewall.

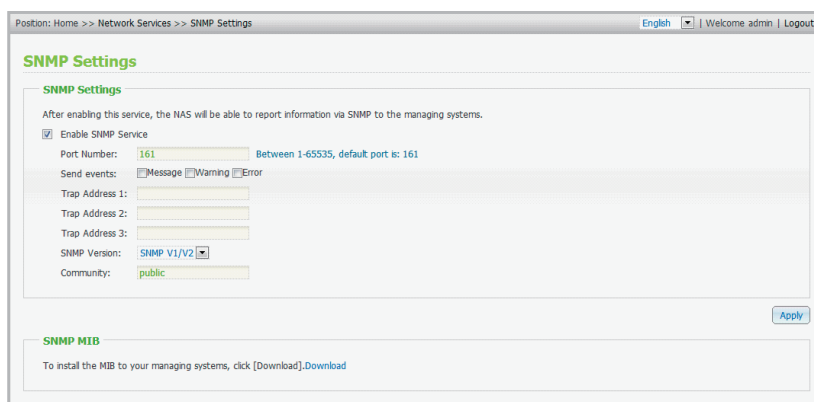


### 3.6 SNMP Setup

With SNMP (Simple Network Management Protocol) service enabled, if there is any event, warning or error message, it will be sent by TNAS (SNMP agent) to the SNMP manager immediately. To enable SNMP service, please go to “Control Panel” > “Network Services” > “SNMP Settings”, check “Enable SNMP Service”, input IP address of SNMP manager, and click “Apply”.

The fields are described as below:

Field	Description
Send Events	Select the type of events to be sent.
Trap Address	The IP address of SNMP manager (3 at most).
SNMP MIB (Management Information Base)	The MIB is a database in ASCII text format used to provide the status of TNAS to the SNMP manager in the SNMP network. Users can download the MIB files and view it with any word processor or text editor.
Community (SNMP V1/V2)	An SNMP community string is a text string that acts as a password. It is used to authenticate messages that are sent between the SNMP server and TNAS. The community string is included in every packet that is transmitted between the SNMP manager and TNAS.
SNMP V3	TNAS supports SNMP version 3. Specify the authentication and privacy settings (if available).



### 3.7 Web Server

TNAS Web Server allows users to upload web pages and manage their own website easily. It also supports Joomla!, PHP and MySQL/SQLite to establish a social networking site or build interaction.



To use Web Server functions, please refer to the following steps:

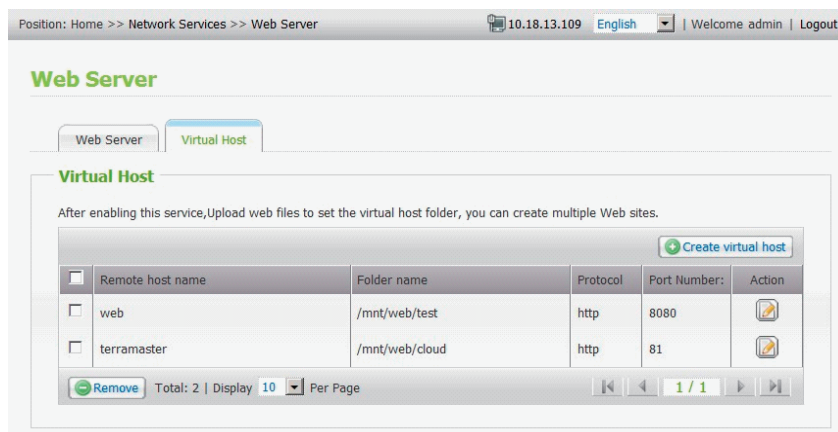
1. Go to "Control Panel" > "Network Services" > "Web Server", check "Enable Web Server", and input port number (default is 8800). To use secure connection (SSL), please check it and input the port number.
2. Upload the HTML files to the shared folder named "web" on TNAS. The file index.html, index.htm or index.php will be the home page files.
3. When everything is set, users can then enter http://NAS IP:8080 (for example, http://192.168.5.100:8080) in the address bar of the web browser to log in to the page.

### 3.8 Virtual Host

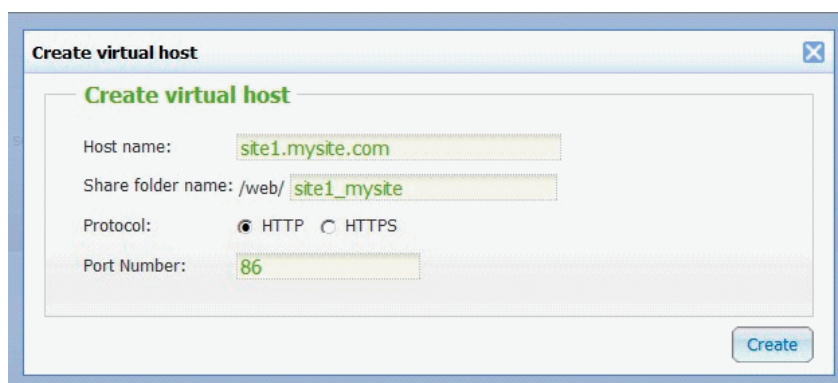
To use this function, please go to “Control panel” > “Authority Setting” > “Shared Folders”, but first users shall create a shared folder in TNAS to store the web page.

The steps for creating the virtual host are described as follows:

1. Select “Enable Virtual Host” and then click “Save”.
2. Click “Create Virtual Host”.



3. Enter the host name and specify the directory path where the web files will be uploaded.
4. Specify the protocol (HTTP or HTTPS) for connection. If HTTPS is selected, please click “Enable Secure Connection (SSL)” on “Control Panel” > “Network Services” > “Web Server” page.
5. Specify the port number for connection. Then, click “Create” to create the virtual host.



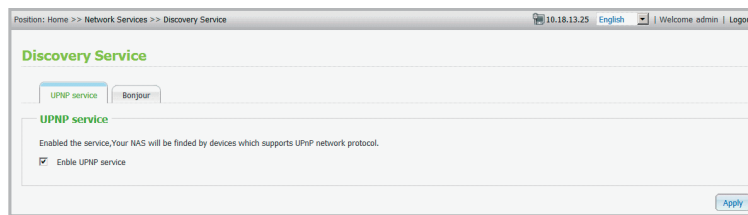
After the virtual host is created, the user can upload the HTML files to the designated shared folder. To access to virtual host, users just need to input domain name http://NAS IP\_or https://NAS IP in web browser on the computer.

### 3.9 Discovery Service

#### UPnP Discovery Service:

As per UPnP protocol, when a UPnP device is added to the network, such device will inform other UPnP devices within the network. When UPnP Discovery Service is enabled, TNAS can be discovered by any operating systems that support UPnP within the network.

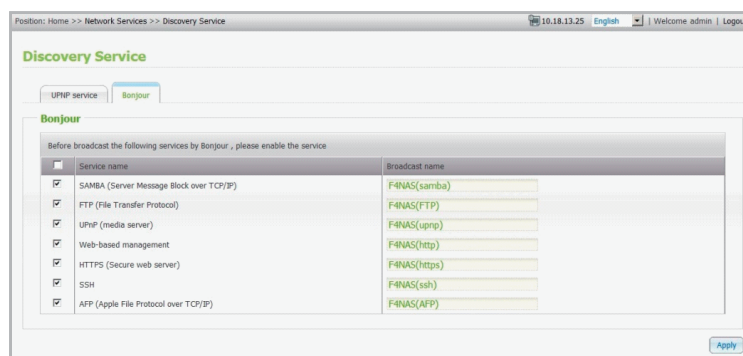
Go to “Control Panel” > “Network Services” > “Discovery Service” > “UPNP”, check “Enable UPNP Service”, and click “Apply”.



### Bonjour:

By Bonjour service(s), Mac computer will automatically discover the TNAS network connection in the local area network, such as FTP, without the need to enter the IP addresses or configure the DNS servers. To enable Bonjour service, please go to “Control Panel” > “Network Services” > “Discovery Service” > “Bonjour”, select the network connection services, and click “Apply”.

Note: before using this service, Bonjour shall be enabled.



## 4. Applications

### 4.1 iTunes Server

The audio files in shared folder “media” in TNAS can be shared to iTunes by using this application. All the computers with iTunes installed in the local area network are able to find, scan and play the shared audio files on TNAS.

To use the iTunes server, go to “Control Panel” > “Applications” > “iTunes Server”, check “Enable iTunes server” and click “Apply”.

### 4.2 MySQL Server

Users can enable MySQL Server as a website database. Before this function is used, please go to “Control Panel” > “Applications” > “MySQL Server” and check “Enable MySQL Server”.

Users can enable this option to allow other servers to connect to MySQL server of TNAS as a database server through their Internet connection. When users disable this option, MySQL server will only be configured as a local database server for the web server of TNAS. After enabling remote connection, assign a port for the remote connection service of MySQL server. The default port is 3306.

A directory called phpMyAdmin will be automatically created in “Web” shared folder. Users can input the link: <http://NAS IP/phpMyAdmin/> to enter the phpMyAdmin page and manage the MySQL database.

Note: Do not delete the phpMyAdmin directory. Users can rename this directory. To connect to the renamed directory, users can enter the link <http://NAS IP/renamed directory> in the web browser.

### Database Maintenance

- “Reset the root password”: Execute this function to reset the password of MySQL root as “admin”.
- “Database re-initialize”: Execute this function to delete all the data on MySQL database.

## 4.3 Backup Server

Enable Rsync server to configure TNAS as a backup server for data backup from a remote Rsync server to TNAS server. Go to “Control Panel” > “Applications” > “Backup Server” to enable this function. The default port number for remote backup via Rsync is 873 and the default user name is rsync. Set the password and click “Apply”.

## 4.4 UPnP Media Server

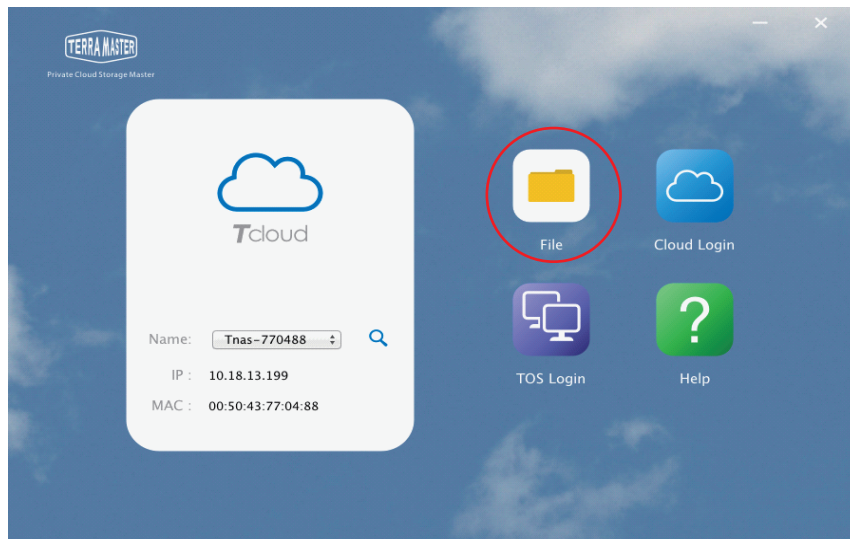
To access and play TNAS multimedia contents via UPnP multimedia server, please check “Enable UPnP Media Server” and click “Apply”.

# 5. File Manager

## 5.1 Manage File Via Tcloud Application

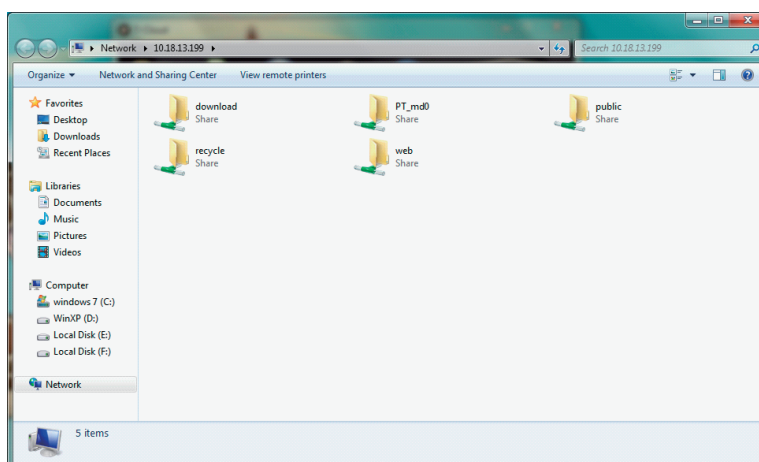
The files in LAN can be managed via the Tcloud application via the following methods: .

1. Open the Tcloud application on your computer. As soon as a TNAS is found, click “File manager”.



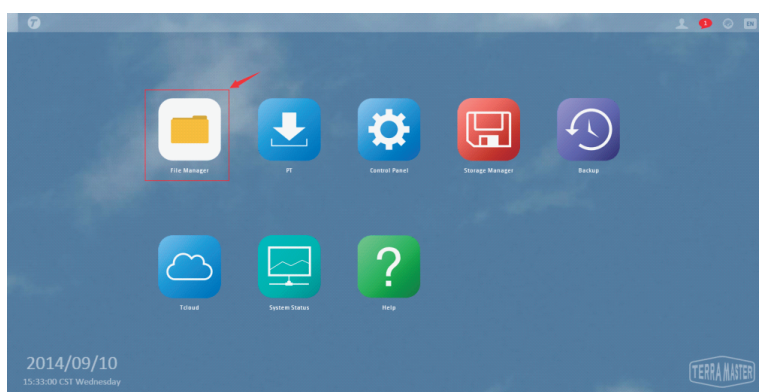
2. Enter the login user name and password (as the case may be), and the computer will list shared folders on TNAS.





## 5.2 Manage File Via Web Browser

Log in to TOS, click “File Manager” on the home page to manage the file through a web browser on TNAS. If TNAS is connected to the Internet, users can access TNAS via the web from anywhere.

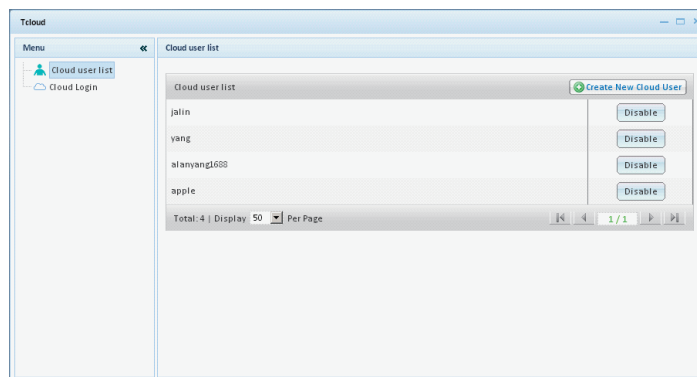


# 6. Tcloud

Tcloud (TerraMaster Cloud) is TerraMaster’s exclusive private cloud storage service. With this service, users can find remote access to TNAS via internet and manage the files in TNAS.

## 6.1 Cloud User List

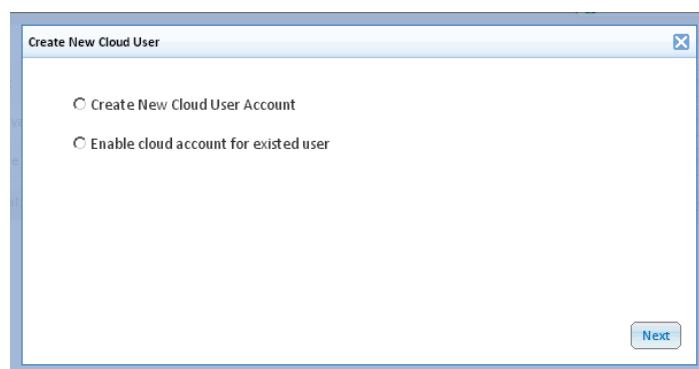
Log in to TOS with your administration account, and go to “Tcloud” > “cloud user list”, which lists all users who have enabled the remote access permission.



## 6.2 Create Cloud Users

By clicking “Create cloud user”, the administrator can create a user account to remotely log in to TNAS. Please log in to TOS with the administrator account and go to “Control Panel” > “Authority Setting” > “User”. The cloud users are created via the following methods:

1. Click "Create NewCloud User" and the following dialog box will appear. Select either “Create New Cloud User Account” or “Enable cloud account for existed user”

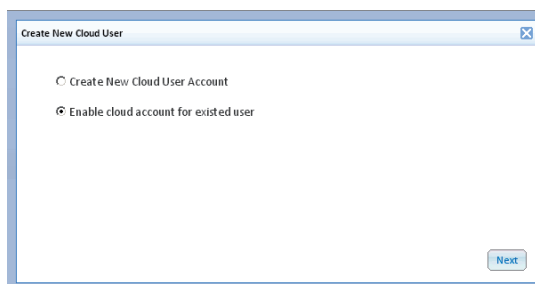


2. If users select “Create New Cloud User Account”, the administrator will be able to create a new user account . Follow the prompts to operate.

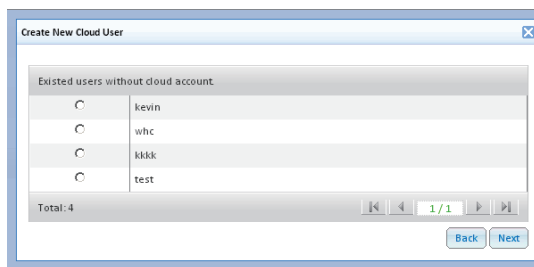
## 6.3 Enable Cloud Account For Existing User

If some users do not enable the remote access privileges in creation, the administrator can enable this privilege for this user at any time. The method for enabling the remote access privilege for existing users is described as follows:

1. Log in to TOS with your administration account, go to “Tcloud” > “Cloud User List”, click “Enable cloud account for existed user” and click “Next”.

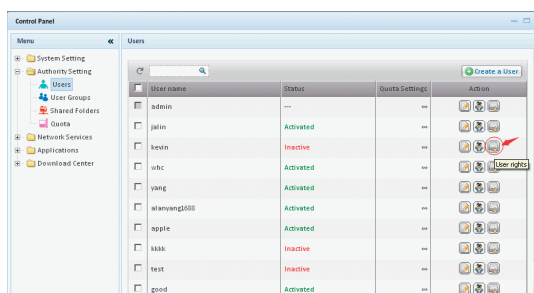
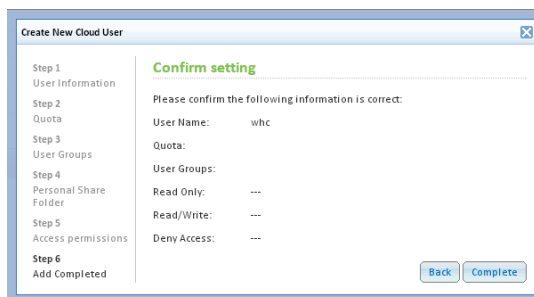


2. All local users that have not enabled cloud functions will be listed.



3. Select the user name and click “Next”.

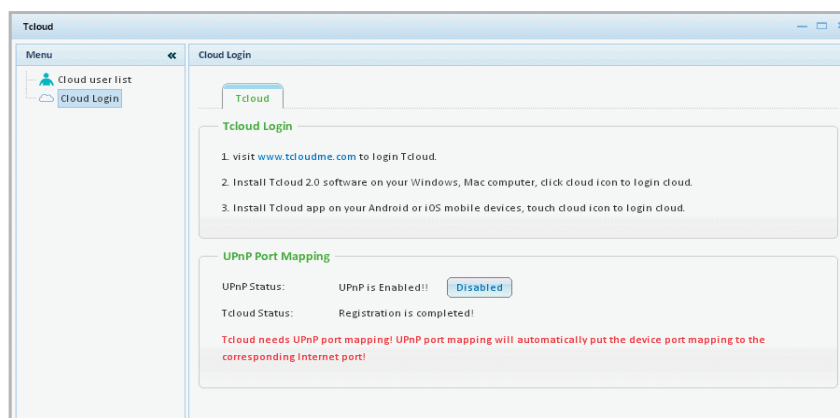
4. Click “Complete” after confirming the user’s information.



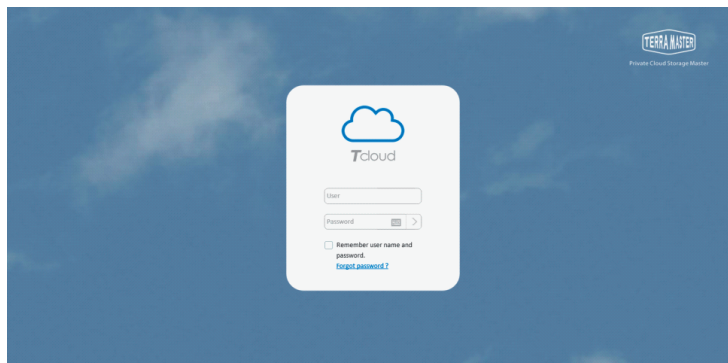
## 6.4 Cloud Login

This page introduces methods of Tcloud remote login to TNAS.

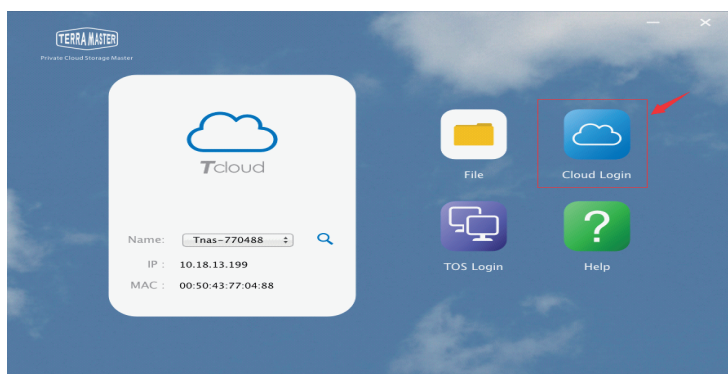
Users can remotely log in to Tcloud via the following method:



1..Users can enter the remote login interface by inputting <http://tcloudme.com> on the PC browser address bar. At this time, input the name and password to remotely log in to TNAS.



2. Users can click “Cloud Login” on the Tcloud desktop application to enter the TNAS remote login interface. At this time, enter the user name and password to remotely log in to TNAS.



## 7. Storage Manager

### 7.1 Disk Manager

#### 7.1.1 Hard Disk Information

Go to “Control Panel” > “Storage Manager” > “Disk Manager” > “Disk Information”, information like model, size and current status of the hard disk is shown here. Users can check the hard disk, and scan the bad track on the hard disk here.

After TNAS initialization finishes, the following default shared folders will be created in TNAS:

Public: The default shared folder for all users.

Download: The folder for Download Center.

USB: The folder for data copy from USB ports.

Web: The folder for Web Server.

Recycle: the folder of network recycle bin.

Note: The default shared folders of TNAS are created on the first hard disk of the hard disk group and the directory path cannot be changed.

### Bad Track Scanr

Click “Scan Now” to check the bad track of

### Hard Disk S.M.A.R.T.

You can check the hard disk information by HDD S.M.A.R.T. (Self-Monitoring

## 7.1.2 Hard Disk Group

Users can create a hard disk group by using a different RAID mode for hard disks:

2-disk TNAS: RAID 0, RAID 1 and single disk and JBOD.

4-disk TNAS: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, single disk and JBOD.

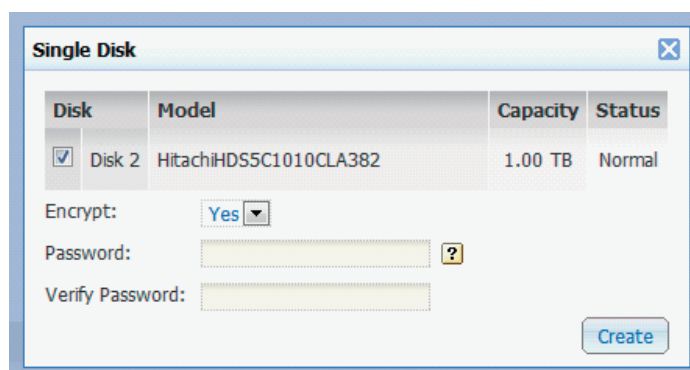
5-disk TNAS: RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, single disk and JBOD.

You can visit the official TerraMaster website or via the Internet to find out the work principle and features of different hard disk groups.

Note: A user can use the external hard disk connected with TNAS via e-SATA as the hard disk to create the hard disk group.

## 7.1.3 Encrypt File System

TNAS encrypt file system provides users a solution for protection of sensitive data. Before disk group creation has finished, click “YES” to the option of “Encrypt”, then the disk group is given the file encryption function.



The data encryption functions may not be available due to the legislative restrictions of some countries.

## How to Use Data Encryption

TNAS protects the disk groups with 256-bit AES encryption standard. The encrypted disk groups can only be mounted for normal read/write access with the authorized password. The encryption function protects the confidential data from unauthorized access even if the hard disk or the entire NAS was stolen.

### Please be aware of the following before using the data encryption function.

The encryption function works for the whole hard disk group, which can be a single disk, JBOD or other RAID disk group.

Select yes or no to encrypt a new hard disk group before it is finally created on TNAS. User will not be able to encrypt a hard disk group if he/she chooses not to, unless the group is initialized again. Note that initializing will clear all data in hard disk group.

The encryption cannot be removed unless the hard disk group is initialized; to do this, all the data will be deleted.

Keep the encryption password safe. If user forgot the password, the data cannot be accessed anymore. Before user starts, read the instructions carefully.

## Encrypt hard disk on TNAS

### Create a new encrypted hard disk group with new hard disks

If TNAS has been installed, to create a new encrypted hard disk group by installing new hard disks on TNAS, follow the steps below.

1. Install the new hard disk(s) on TNAS.
2. Log in to TOS with your admin account. Go to "Disk Manager" > "Hard Disk Group".
3. Select the disk group the user wants to configure according to the number of new hard disks installed.
4. Select the hard disk(s) for creating the hard disk group. In this example, we choose to create a single disk. The procedure also applies to other types of hard disk groups.
5. Select "Yes" for the "Encrypt" option and enter the encryption settings.
6. Then click "Create" to create the new encrypted group. Note that all the data on the selected disks will be DELETED! Please back up the data before creating the encrypted group.

### Confirm if hard disk group is encrypted

To confirm whether the hard disk group is encrypted, log in to TOS with your admin account. Turn to "Disk Manager" > "Encrypted File System". The hard disk group is encrypted when "Encrypted" is viewed in the status column.

## 7.1.4 iSCSI Storage

iSCSI: Internet Small Computer System Interface

The iSCSI technology is a new storage technology which combines the SCSI interface with Ethernet technology to enable the server to exchange documents with the storage device using IP network. TNAS supports the iSCSI storage function.

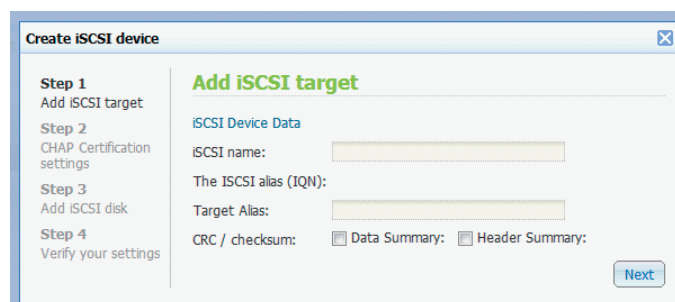
When the server is connected to the storage device via the iSCSI bus, the server is called an initiator and the storage device is called a target.

Follow the steps below to configure the iSCSI target service on TNAS.

Note: It is suggested NOT to connect to the same iSCSI target with two or more different iSCSI initiators at the same time because this may result in conflicts and data corruption.

**A maximum of 10 iSCSI targets can be created. However, the maximum number of concurrent connections to the iSCSI targets supported by TNAS varies depending on the network infrastructure and the application performance. Too many concurrent connections may slow down the performance of TNAS.**

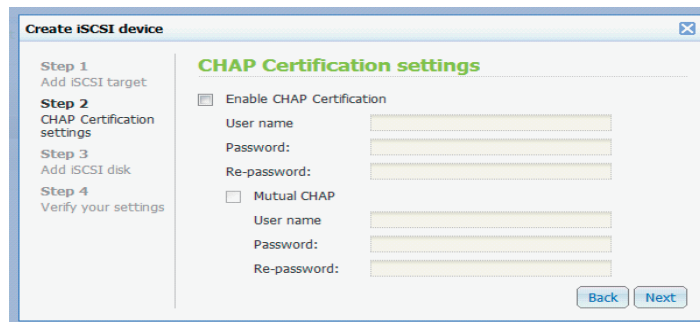
1. Please log in to TOS with an admin account, go to "Storage Manager" > "Disk Manager" > "iSCSI storage" > "Portal Management", check "Enable iSCSI target service" and click "Save".
2. Go to "Storage Manager" > "Disk Manager" > "iSCSI storage" > "Target Management" and click "Create iSCSI targets".
3. Enter the target name and target alias. User may check the options "Data Summary" and/or "Header Summary" (optional). These are the parameters that the iSCSI initiator will be verifying when it attempts to connect to the iSCSI target.



4. Enable CHAP Certification: enter the user name and password, which are required when initiator tries to access the iSCSI target of TNAS.

Mutual CHAP: Enable this option for mutual authentication between the iSCSI target and the initiator. The target will authenticate the initiator using the first set of user name and password. The initiator will authenticate the target using the “Mutual CHAP” settings.

Field	User name limitation	Password limitation
CHAP authentication	Valid characters: 0-9, a-z, A-Z Maximum length: 256 characters	Valid characters: 0-9, a-z, A-Z Maximum length: 12-16 characters
Mutual CHAP	Valid characters: 0-9, a-z, A-Z, : (colon), (dot), and - (dash) Maximum length: 12-16 characters	Valid characters: 0-9, a-z, A-Z, : (colon), (dot), and - (dash) Maximum length: 12-16 characters



**Create iSCSI device**

Step 1: Add iSCSI target  
Step 2: CHAP Certification settings  
Step 3: Add iSCSI disk  
Step 4: Verify your settings

**CHAP Certification settings**

☒ Enable CHAP Certification

User name:   
Password:   
Re-password:

☐ Mutual CHAP

User name:   
Password:   
Re-password:

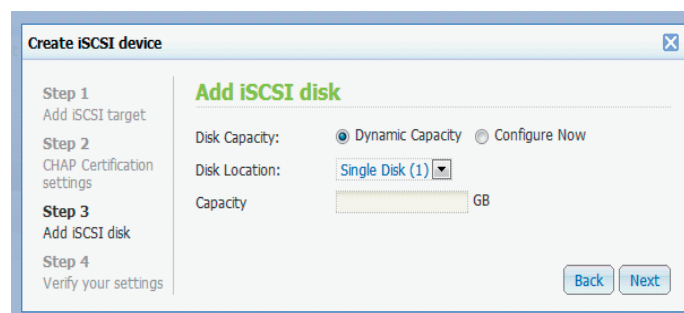
[Back](#) [Next](#)

#### 5. Create an iSCSI LUN.

An iSCSI LUN is a logical disk mounted to the iSCSI target. Select one of the following modes to allocate the disk capacity to the LUN:

- Thin Provisioning: Allocate the disk capacity in a flexible manner. User can allocate the disk capacity to the target regardless of the current storage capacity available on TNAS. Over-allocation is allowed, as the storage capacity of TNAS can be expanded in future.
- Instant Allocation: Allocate the iSCSI disk capacity immediately. This option guarantees the disk capacity assigned to the LUN, but this may take more time to create the LUN.

Specify the LUN location. Enter the capacity for the LUN. Click “Next”.



**Create iSCSI device**

Step 1: Add iSCSI target  
Step 2: CHAP Certification settings  
Step 3: Add iSCSI disk  
Step 4: Verify your settings

**Add iSCSI disk**

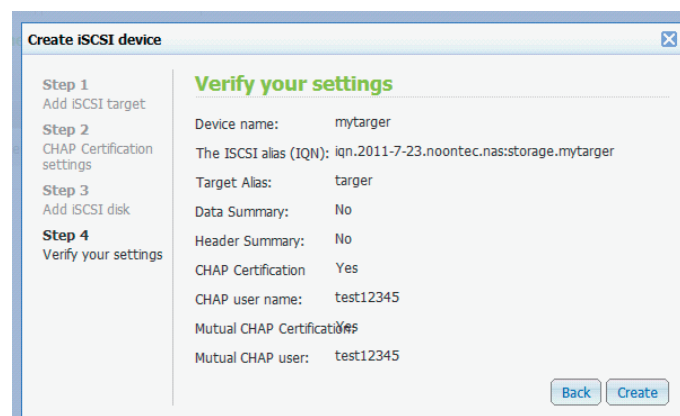
Disk Capacity: ☒ Dynamic Capacity ☐ Configure Now

Disk Location:

Capacity:  GB

[Back](#) [Next](#)

#### 6. Verify the configuration. Click “Create” to complete the setup.



**Create iSCSI device**


Step 1: Add iSCSI target  
Step 2: CHAP Certification settings  
Step 3: Add iSCSI disk  
Step 4: Verify your settings

**Verify your settings**

Device name: mytarget  
The iSCSI alias (IQN): iqn.2011-7-23.noontec.nas:storage.mytarget  
Target Alias: target  
Data Summary: No  
Header Summary: No  
CHAP Certification: Yes  
CHAP user name: test12345  
Mutual CHAP Certification: No  
Mutual CHAP user: test12345

[Back](#) [Create](#)

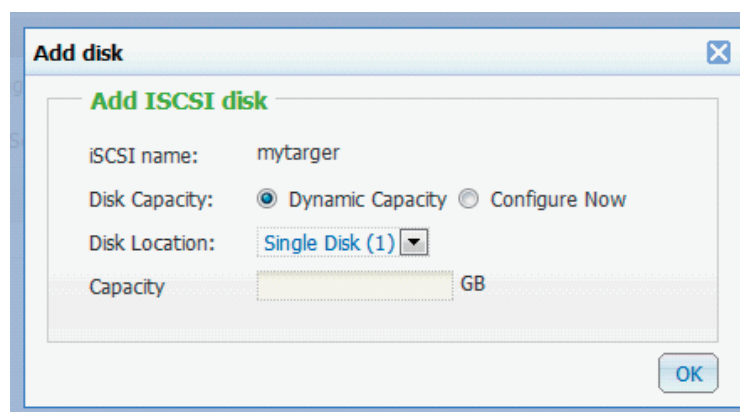
## iSCSI LUN Capacity Expansion

To expand iSCSI disk capacity, go to “Storage Manager” > “Disk Manager” > “iSCSI Storage” > “Target Management”, select iSCSI disk target and press .



Input capacity value and click “OK” to complete setting. The disk capacity can be increased many times up to the maximum limit, but it cannot be decreased.

Disk Configuration Mode	Disk capacity upper limit
Dynamic Capacity	32TB
Configure Now	Free size available on the disk group



To learn how to use and set the starter on the server running Windows OS, please visit [www.microsoft.com](http://www.microsoft.com).

To learn how to use and set the starter on the PC running MAC OS, please visit

<http://www.attotech.com/products/product.php?sku=INIT-MAC0-001>.

To learn how to use and set up the starter on PC running Linux OS, please refer to <http://www.open-iscsi.org/>.

## 7.2 Virtual Disk

User can use this function to add the iSCSI targets of other network storage or storage servers to TNAS as the virtual disks for storage capacity expansion. TNAS supports maximum 8 virtual disks.

Note: The maximum size of a virtual disk TNAS supports is 16TB.

Add virtual disks via the following steps:

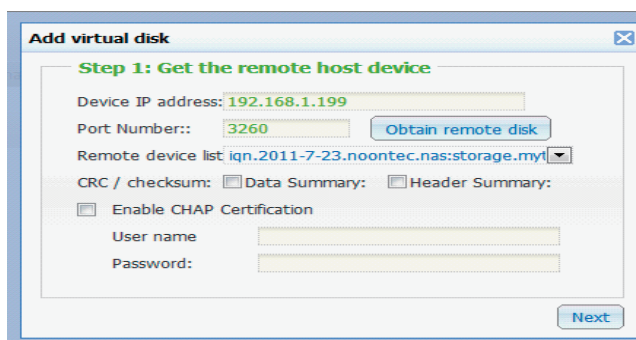
### Step 1:

To add a virtual disk to TNAS, please go to “Control Panel” > “Storage Manager” > “Virtual Disk”, click “Add Virtual Disk”. Make sure an iSCSI target has been created.



**Step 2:**

Enter the target server IP and port number (default: 3260). Click “Obtain Remote Disk”. Select a target from the target list. If authentication is required, enter the user name and the password. Users may select the options “Data Summary” and/or “Header Summary” (optional). These are the parameters that the iSCSI initiator will be verifying when it attempts to connect to the iSCSI target. Then click “Next”.

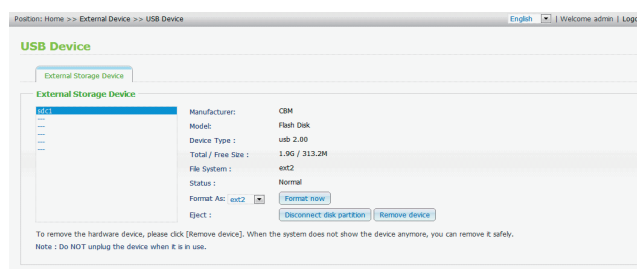
**Step 3:**

Enter a name for the virtual disk. If the target is mapped with multiple iSCSI disks, select a disk from the list. The target disk can only connect to not more than one host or server. TNAS supports mounting EXT3, EXT4, FAT32, NTFS, HFS+ hard disk. If the format of the virtual disk is “Unknown”, select “Format virtual disk now”. User can format the virtual disk as EXT3, EXT4, FAT 32, NTFS, or HFS+. Click “OK” to finish, and all data on the virtual disk will be cleaned.

## 7.3 External Storage Device

TNAS supports external USB and e-SATA storage devices for storage expansion. Go to “Control Panel” > “Storage Manager” > “External Device” > “External Storage Device”. Once an external storage device is connected to a USB or an e-SATA interface of TNAS, the details will be shown on this page.

It may take tens of seconds for TNAS to detect the external USB or e-SATA device successfully. Please wait patiently.



Please set the use mode for the external storage devices connected to TNAS:

- Share documents: the external storage device can be used as expanded storage capacity of TNAS via this mode, which is a frequent manner.
- RAID 1 disk group: the external storage device and TNAS will compose a RAID 1 hard disk group, and the data in TNAS will be backed up to the external device. When the hard disk group is created, the hard disk on the external storage device will be formatted. After the hard disk group is created successfully and as soon as the external storage device connects TNAS, the data in TNAS will be automatically backed up to the external storage device.

## 8. Backup

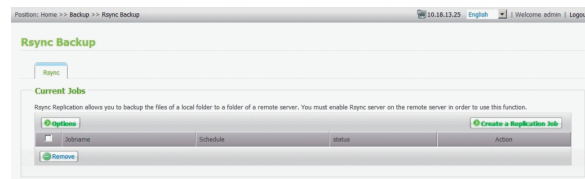
### 8.1 Rsync Backup

By the Rsync backup function, the data on TNAS can be backed up to other NAS device or server. If the backup destination is other NAS device, you need to set that NAS device to be Rsync backup server.

Add virtual disks via the following steps:

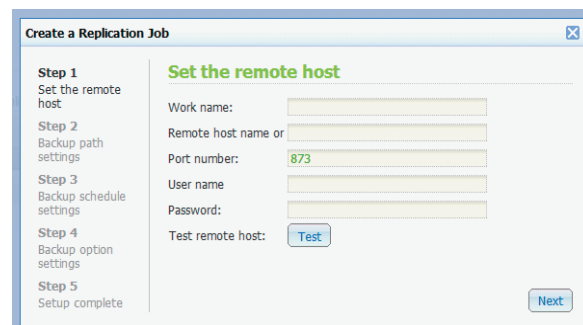
#### Step 1:

Log in to TOS as administrator, go to "Control Panel" > "Storage Manager" > "Backup" > "Rsync backup"; to create a remote backup job, click "create a remote backup job".



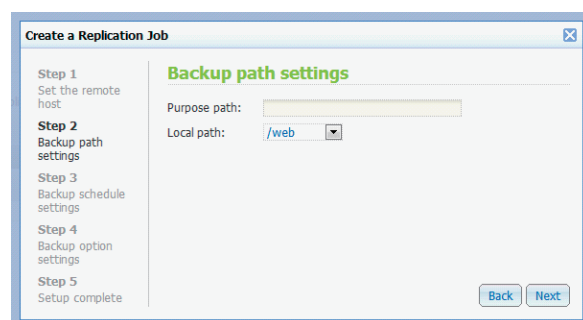
#### Step 2:

Enter the remote host name or IP address, port number, user name and password. The default port number is 873. Note that the user name must have the read/write permissions and sufficient capacity quotas. Click "Test" to confirm the successful connection, and then click "Next".



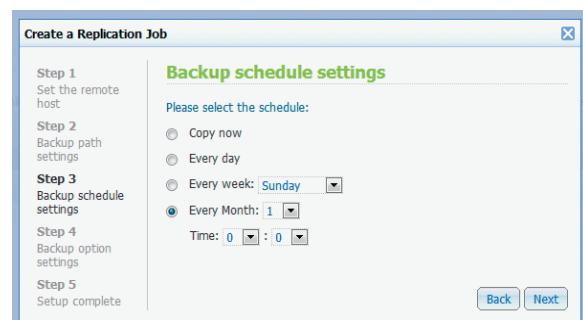
#### Step 3:

Specify the destination path. Input the destination path. Once successfully connected, click the pull-down button and shared list will be obtained, Backup path: where the data will be replicated to.



#### Step 4:

Step 4: Set the backup schedule.



**Step 5:**

Specify other options for the backup.

**Enable encryption:** Select this option to execute encrypted remote backup. Note that user must enable “Allow SSH connection” in “Network Services > “Telnet/SSH” and specify the same port number for SSH and encrypted remote backup.

**Activate file compression:** Enable this option to allow file compression during the data transfer process to decrease the data size. This option is recommended for a low bandwidth environment or remote backup over WAN.

**Stop network file services before backup:** Stop all connections to the NAS via Samba (SMB), AFP and FTP before remote backup is in process.

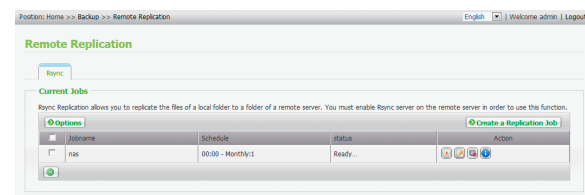
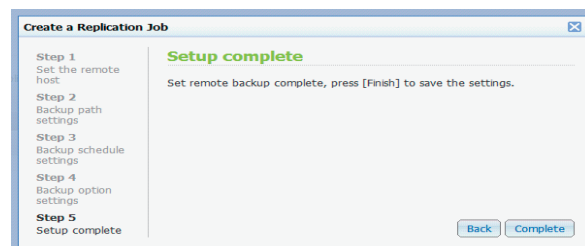
**Backup changed documents or files:** When this option is enabled, after the first-time backup, TNAS will only back up the files that have been changed since the last backup. User is recommended to enable this option for the backup to shorten the backup time.

**Delete extra files on remote destination:** Select this option to synchronize the source data with the destination data (one-way synchronization). Extra files on the destination will be deleted. Source data will remain unchanged.

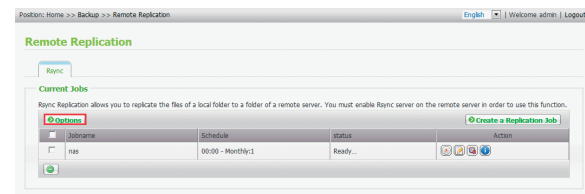
**Sparse files backup:** Sparse file is a type of file that takes up less disk space than its actual size and contains large blocks of zero-byte data. Enabling this option may reduce the time required for remote backup.

**Step 6:**

Click “Finish”



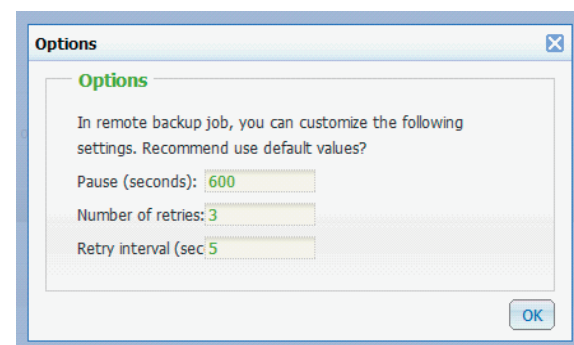
To configure the pause and retry settings of the backup, click “Options”.



- **Pause (seconds):** Specify a timeout value for each backup. This is the maximum number of seconds to wait until backup is cancelled if no data has been received.

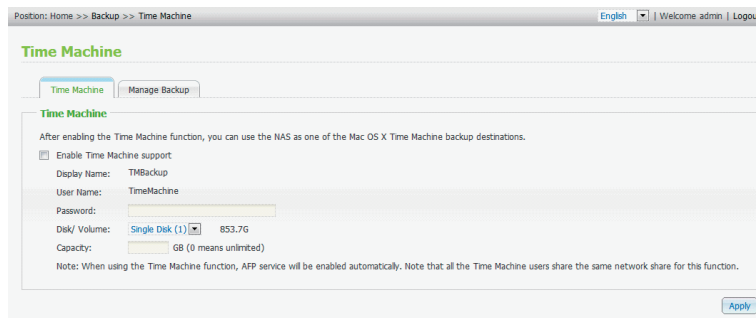
- **Number of retries:** Specify the number of times device should try to execute backup when it fails.

- **Retry intervals (second):** Specify the number of seconds to wait in between each retry.



## 8.2 Time Machine

User can enable Time Machine to make TNAS as a backup destination for more than one Mac computer.

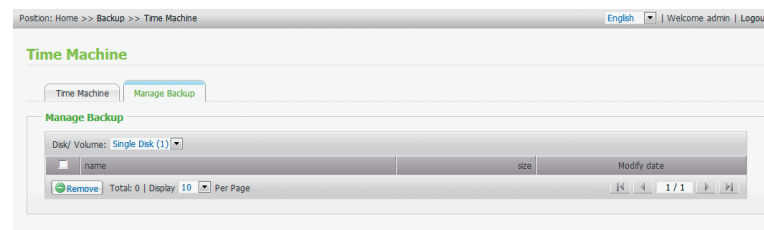


To use the Time Machine, go to "Control Interface" > "Storage Manager" > "Backup" > "Time Machine" page, and follow the steps below.

1. Check "Enable Time Machine".
2. Enter the Time Machine password.
3. Select a hard disk group on TNAS as the backup destination.
4. Enter the storage capacity that Time Machine backup is allowed to use. The maximum value is 4095GB. To specify a larger capacity, please enter 0 (unlimited).
5. Click "Save" to save the settings.

To know learn how to use the time machine on MAC PC, please view the Apple website <http://www.apple.com> and read the operation instruction.

### Management Backup



To manage the Time Machine, go to "Control Panel" > "Storage Manager" > "Backup" > "Time Machine" > "Management Backup". User can then check the Time Machine backup, its data size, backup date and time and delete the backup file.

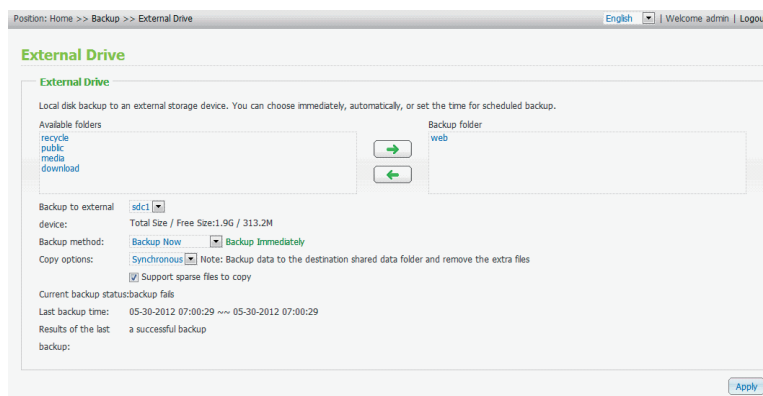
## 8.3 Backup to External Storage

TNAS supports real-time and scheduled data backup from the internal disks group to USB or e-SATA external storage devices. To use this function, please turn to "Control Panel" > "Storage Manager" > "Backup" > "Backup to External storage", follow the steps below.

Note: If an external storage device is encrypted by TNAS, make sure it is unlocked in "External device" > "External Storage device" before creating any backup.

1. Connect external storage devices to the USB interfaces or e-SATA interface of TNAS. The storage format of the external storage device should be in the same format with that of the hard disk in TNAS.

If there is any discrepancy, TNAS will inform to format external storage device, please turn to "Control Panel" > "Storage Manager" > "External device" > "external storage device" to format the external storage device.



2. Select the folder that needs to be backed up.
3. Select the external destination device for backup.
4. Select real-time or scheduled backup.
  - Real-time backup: Real-time backup copies files that are new, changed and renamed from the source folder to the target folder as soon as the changes are made after the first-time backup.
  - Scheduled backup: Copy files that are new, changed and renamed from the source folder to the target folder according to the schedule.
  - Auto-backup: Execute data backup automatically every time device is connected to TNAS.
5. Click “Save” and the setting is completed.

## 9. Download Center

### 9.1 BT/PT Download

TNAS supports BT/PT download. User can add the download task to list and TNAS will automatically complete the download.

**Important Note:** Do not download any copyrighted material illegally. The Download Center provides the authorized files download only. Download of any unauthorized data may result in civil or criminal penalties. Users shall comply with Copyright Ordinance and bear all the consequences arising from violation of the Copyright Ordinance.

To enable download function, go to “Download Center” > “BT/PT Download” and check “Enable BT/PT Download Center”. After that, close the page, log into “download center” again, and the user can now enter the download page.

## 10. System Information

### 10.1 Hardware Information

Log in to TOS via an admin account and go to “System Information” > “Hardware Information” and the user can view the working conditions of hardware, including boot time, usage of network port, usage of processor and memory, operating temperature of CPU, frame and hard disk.

Position: Home >> System Status >> System Information English | Welcome admin | Logout

### System Information

Server Name	F4NAS
Firmware Version	F4NAS_S1.0_V1.244
System Up Time	5 day(s) hour(s) minute(s)

### Port Status

Port number	Status	IP Address	MAC Address	Packets Received	Packets Sent	Error Packets
eth0	<span style="color: green;">●</span>	192.168.1.199	00:50:43:00:02:02	13327689	2739044	0

### Hardware Information

CPU Usage	0%
Total Memory	495.02 MB
Free Memory	353.91 MB
CPU Temperature	45 °C
System Temperature	40 °C
HDD 1 Temperature	43 °C
HDD 2 Temperature	42 °C
HDD 3 Temperature	---
HDD 4 Temperature	---
System Fan Speed	533 RPM

### 10.2 Service Status

Log in to TOS via an admin account and go to “System Information” > “Service Status” and the user can view the current status of several services and port usage.

Position: Home >> System Status >> System Service English | Welcome admin | Logout

### System Service

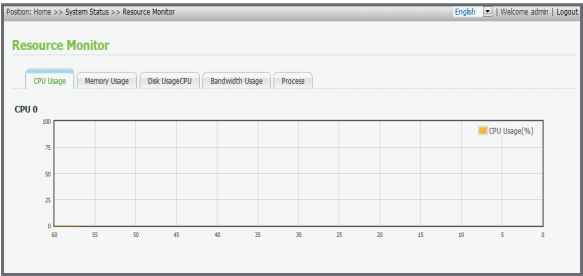
<b>Samba service</b> Service status <span style="color: green;">●</span> Workgroup soft Server Type Standalone Server Enable WINS server <span style="color: red;">●</span> Enable Local Master Browser <span style="color: red;">●</span>	<b>Web Server</b> Service status <span style="color: green;">●</span> Port number 80 <b>DDNS Service</b> Service status <span style="color: red;">●</span> <b>MySQL Server</b> Service status <span style="color: green;">●</span> Enable TCP/IP Networking <span style="color: red;">●</span>
<b>Apple Networking</b> Service status <span style="color: green;">●</span> <b>Unix/Linux NFS</b> Service status <span style="color: green;">●</span> Download Station Service status <span style="color: green;">●</span> <b>System Port Management</b> Port number 8080 <b>Disk Management</b> Enable iSCSI Target Service <span style="color: green;">●</span> Port number 3260	<b>FTP server settings</b> Service status <span style="color: green;">●</span> Port number 21 Maximum Connections 30 <b>Multimedia Station</b> Enable iTunes Server <span style="color: green;">●</span> Enable UPnP Media Server <span style="color: green;">●</span>

### 10.3 Resource Monitor

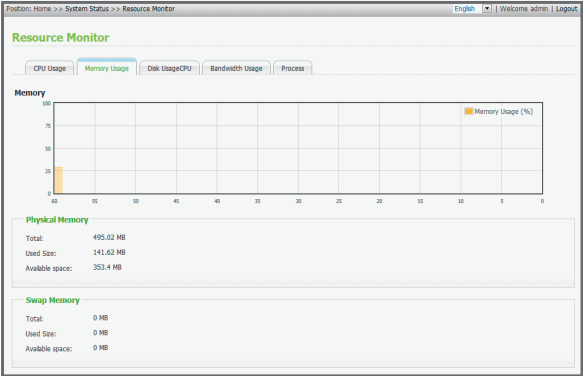
Log in to TOS via an admin account and go to “System Information” > “Resource Monitor” and the user can view the CPU usage, disk usage, and bandwidth transfer statistics of TNAS on this page.



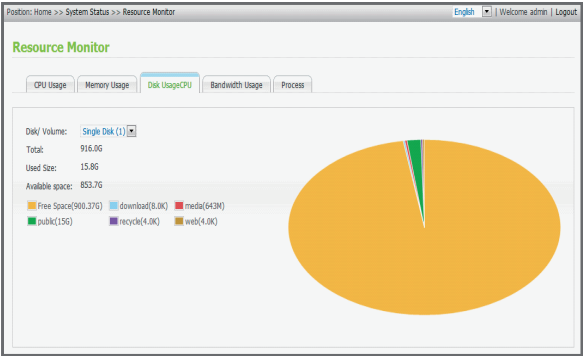
CPU Usage: This tab shows the CPU usage of TNAS.



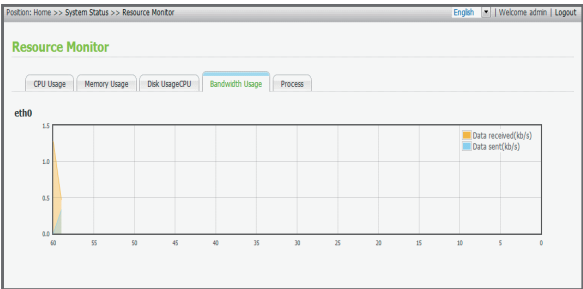
Memory Usage: This tab shows the memory usage of TNAS by real-time dynamic graph.



Disk Usage: This tab shows the disk space usage of each disk group and its network folders.



Bandwidth Usage: This tab provides information about bandwidth usage of each available LAN port of TNAS.



Process: This tab shows information about the processes running on TNAS.

Process name	User	PID	CPU Usage	Memory Usage
medatomb	root	18954	0.0%	23.0%
unraid	root	19280	0.0%	15.3%
transmission-daemon	root	19229	0.0%	10.1%
myaidd	root	18942	0.0%	5.3%
php-cgi	root	19291	0.0%	4.6%
php-cgi	root	11837	0.0%	4.6%
php-cgi	root	1392	0.0%	4.5%
php-cgi	root	12072	0.0%	4.5%
php-cgi	root	1387	0.0%	4.5%
php-cgi	root	1047	0.0%	4.5%
php-cgi	root	12026	0.0%	4.5%
php-cgi	root	1142	0.0%	4.2%
php-fpm	root	19125	0.0%	4.1%
mysqld	root	1294	0.0%	4.0%
smbd	root	19128	0.0%	3.4%
smbd	root	19152	0.0%	2.4%
rmbd	root	19143	0.0%	3.3%
mt-daapd	root	19076	0.0%	2.7%
httd	daemon	19323	0.0%	2.1%
httd	daemon	19325	0.0%	2.1%
httd	daemon	19327	0.0%	2.1%
httd	daemon	19324	0.0%	2.1%
httd	daemon	19326	0.0%	2.1%