



ioSafe 214 User's Guide

Powered by Synology DSM 4.3

Table of Contents

Chapter 1: Introduction

Chapter 2: Getting Started with ioSafe's 214 and DiskStation Manager

Install ioSafe 214 and DSM	8
Log in to DiskStation Manager	8
DiskStation Manager Appearance	11
Manage DSM with the Main Menu	13
Manage Personal Options	15

Chapter 3: Modify System Settings

Change DSM Settings	17
Change Network Settings	19
Modify Regional Options	20
Use Energy Saving Features	21

Chapter 4: Manage Storage Space

Volumes and Disk Groups	23
Repair Volumes or Disk Groups	25
Expand Volumes or Disk Group	25
iSCSI Targets and LUNs	25
Manage Hard Disks	26
SSD Cache	27
Manage External Disks	27

Chapter 5: Access your 214 from the Internet

Use the EZ-Internet Wizard	28
Set Up Port Forwarding Rules for Router	29
Register DDNS for 214	30
Access DSM Services via QuickConnect	31
Set up VPN Connection	32

Chapter 6: Enhance Internet Security

Prevent Unauthorized Connection with Firewall	33
Control the Outgoing Traffic of Services	34
Prevent Attacks over the Internet	35
Automatically Block Suspicious Login Attempts	36

Chapter 7: Set Up File Sharing

Enable File Sharing Protocols for All Platforms	37
Join 214 to Directory Service	38
Host LDAP Service with Directory Server	39
Manage Users and Groups	39
Set Up Shared Folders	42

Define Windows ACL Privileges for Shared Folder.....	44
Index Shared Folder Contents	45

Chapter 8: Access Files from Anywhere

Access Files within the Intranet.....	46
Access Files via FTP	49
Access Files via WebDAV	50
Sync Files via Cloud Station.....	51
Access Files via File Station.....	52

Chapter 9: Back Up Data

Back Up Computer Data	55
Back up Data or iSCSI LUN on the ioSafe 214	57
Sync Shared Folder Contents between 214s	59
Back up 214 Data with Time Backup	59
Back up Data on USB Device	60
Back up Data to Amazon Glacier.....	60

Chapter 10: Host Websites, Email Server, and Print Server

Use Web Station to Host Websites	61
Host Mail Server.....	62
Install Mail Station to Enable Webmail Service	63
Set ioSafe 214 as Print Server.....	64

Chapter 11: Discover Various Applications with Package Center

What Package Center Offers	65
Install or Buy Packages.....	65

Chapter 12: Share Photos, Videos, and Blogs with Photo Station

Install Photo Station.....	66
Enable Personal Photo Station	67
Photo Station Features.....	67

Chapter 13: Play Music with Audio Station

Install Audio Station.....	69
Manage Audio Station Settings.....	70
Audio Station Features.....	70

Chapter 14: Organize Videos and Record TV Programs with Video Station

Install Video Station	72
Before You Start.....	73
Video Station Features.....	73

Chapter 15: Download Files with Download Station

Install Download Station.....	75
Download Station Features	76

Chapter 16: Safeguard Your Environment with Surveillance Station

Install Surveillance Station.....	79
Manage Surveillance Station Settings	80

Watch Live View.....	81
Work with Timeline.....	83

Chapter 17: Create a Domain Name Server with DNS Server

Install DNS Server	84
Before You Start.....	84
DNS Server Features	85

Chapter 18: Manage Media Server and iTunes Service

Install DLNA Media Server	86
Manage DLNA Media Server	86
Install iTunes Server	87
Manage iTunes Server	87

Chapter 19: Perform Advanced Management Tasks

Check System Information.....	89
View System Logs	91
Monitor System Resources.....	92
Manage Bluetooth Devices.....	93
Automate Tasks	93
Update DSM	93
Receive Event Notifications.....	94
Access Applications with Independent Login.....	95
Index Multimedia Files for Applications.....	95
Reset Admin Password.....	96
Restore ioSafe 214 to Factory Defaults	96
Reinstall ioSafe 214.....	97
Enable SNMP Service	97
Enable Terminal Services.....	97

Chapter 20: Communicate with Mobile Devices

Manage DSM Settings with DSM mobile.....	98
Use iOS, Android, and Windows Apps	98
Use Other Mobile Devices	99

Introduction

Important Note: The ioSafe 214 is based on the Synology DS214 Motherboard and Synology DSM OS. Certain configuration settings may require you to select “Synology DS214” or “Synology” as an option. Contact techsupport@iosafe.com if you get stuck.

Congratulations on your purchase of the ioSafe 214 powered by Synology's DiskStation Manager (DSM). The ioSafe 214 is a Network Attached Storage (NAS) device designed to protect your private cloud data against loss from fire and water. When used correctly, the ioSafe 214 can be an integral part of your data protection, security and sharing strategy.

Redundant Disks (RAID 1)

Your ioSafe 214 is equipped with the ability to instantaneously replicate data between the two installed hard drives (RAID 1: Mirrored Drives) to protect against hard drive failure. You can also combine the capacities of the drives (RAID 0: Striped Drives) but you should be aware that RAID 0 offers no redundancy and if either of the hard drives fail, you could lose data from the entire volume! RAID 0 happens to be even less reliable than using a single drive. As with all data storage, we at ioSafe recommend you follow 3-2-1 Backup as a **minimum** rule: Keep at least 3 complete copies of all your data. Keep the copies on at least 2 different devices. Keep at least 1 copy protected against natural disaster – either on an ioSafe device, offsite or online.

Data Recovery Service (DRS)

Your ioSafe 214 may or may not include our Data Recovery Service (DRS) option. The diskless version of the ioSafe 214 does not include DRS. Consider this service as a safety net in case of any disaster events which may cause your data to be at risk. If you are under the terms of our DRS, you can simply contact ioSafe and we will begin the process of recovery. There are various levels, restrictions and limitation so contact your ioSafe sales representative (sales@iosafe.com) or visit <http://iosafe.com/products-2baynas-drs> for the terms of our Data Recovery Service.

Store and Share Files over the Internet

Windows users, Mac users, and Linux users can easily share files within the Intranet or through the Internet. Unicode language support makes sharing files in different languages from the ioSafe 214 simple.

Manage Files with Web-Based File Station

One of DiskStation Manager's applications, File Station, can make it possible for users to manage their files on the ioSafe 214 easily through a web interface. You can also access the files stored on ioSafe 214 with a mobile device.

Transfer Files via FTP

The ioSafe 214 provides FTP service with bandwidth restriction and anonymous login. To transfer data safely, FTP over SSL/TLS and uninvited IP auto-block are also available.

Sync Files with Cloud Station

Cloud Station is a file sharing service that allows your 214 to become a file sync center to sync files between multiple client computers. With the Cloud Station application installed on your computers, you can simply drop your office file to a folder on your office computer, and then open the same file automatically synced to your laptop.

Share Storage Capacity as iSCSI LUNs

You can designate portion of your ioSafe 214 volume space to be an iSCSI LUN, which will allow the iSCSI initiator to access the space like a local disk.

Back Up Files on Computer and Server

The ioSafe 214 provides various backup solutions to back up computer data to ioSafe 214, back up ioSafe 214 data or iSCSI LUN to an external hard drive, another ioSafe 214, an rsync-compatible server, Amazon S3 server, HiDrive backup server, etc.

Enjoy Entertainment Content on the Server

Download Station allows you to download files from the Internet through BT, FTP, HTTP, eMule and NZB to ioSafe 214. The Media Server and iTunes support allows computers or DMA devices within LAN to playback multimedia files on ioSafe 214¹.

With the USBCopy function, you can press the Copy button on your 214 to instantly copy files from a camera to ioSafe 214.

Organize Videos with Video Station

Video Station allows you to organize your collection of movies, TV shows, and home videos into a media platform on which you can watch and play video clips, live stream and record digital TV programs with a USB DTV dongle plugged into your ioSafe 214, view and edit video metadata whose information is retrieved automatically from the Internet. You can also stream videos to your iPhone or iPad for playback.

Share Photos, Videos, and Blogs with Photo Station

Photo Station gives you the freedom to share photos and videos over the Internet without complicated upload steps. Album control ensures the content is shared with the right persons. Visitors can leave comments for your photos. Furthermore, a brand new blogging system is integrated for you to easily share your life and thoughts over the Internet.

Enjoy Music Anytime and Anywhere

Audio Station allows you to listen to music stored on the ioSafe 214, from a connected iPod, or even stream Internet Radio stations. In addition, you can stream music from the ioSafe 214 with a web browser over the Internet.

Host Websites

The Virtual Host feature allows you to host up to 30 websites using Web Station, with PHP and MySQL supported.

Record Videos with IP Cameras

Surveillance Station allows you to manage, view, and record videos from multiple IP cameras over the network. By accessing the web-based management interface of Surveillance Station, you can watch the real-time image the camera is monitoring, and record videos continuously, in motion-detection mode, or in alarm-recording mode.

Discover More Apps with Package Center

Package Center brings intuitiveness and convenience for users to easily install and update a variety of applications (which are packed into packages). Just browse all available applications and select the ones that best suit your needs. All can be done with just a few clicks.

¹ For recommended peripheral models, including hard drive, USB printer, DMA, and UPS, please visit www.iosafe.com.

Print Server

USB or network printers connected to your 214 can be shared by client computers over the local area network. AirPrint support allows you to print to the printer from an iOS device, while Google Cloud Print support allows you to print to the printer when you are using Google products and services.¹

Online Resources

If you cannot find what you need here, please see **DSM Help** or take a look at Synology's online resources below.

- **FAQ:** www.iosafe.com/support or www.synology.com/support/faq.php
- **Wiki:** forum.synology.com/wiki
- **Forum:** forum.synology.com
- **Download Center:** www.synology.com/support/download.php
- **Technical Support:** www.iosafe.com/support or www.iosafe.com/contact

¹ For recommended peripheral models, including hard drive, USB printer, DMA, and UPS, please visit www.iosafe.com/support.

Getting Started with ioSafe's 214 and DiskStation Manager

This chapter explains how to log in to ioSafe 214 web-based management User Interface, **Synology DiskStation Manager (DSM)**, customize your own desktop, manage its taskbar and widgets, and use the **Main Menu** to access DSM settings and applications. For more detailed instructions, please see **DSM Help**.

Install ioSafe 214 and DSM

You should have already installed and connected your ioSafe 214 through your network using the **Quick Start Guide** included on this CD. If you have not completed the set-up using the Quick Start Guide, Please close this document and open the Quick Start Guide.

Log in to DiskStation Manager

You can log in to DSM with Synology Assistant or with a web browser.

Use Synology Assistant

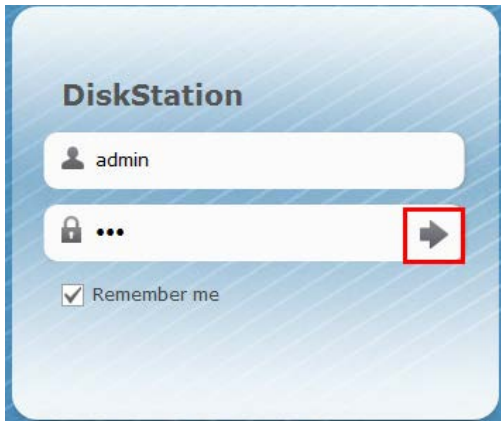
Windows User:

- 1 Insert the installation disc into your computer, and click **Start**. Follow the onscreen instructions to complete the setup process.



- 2 Synology Assistant will be installed and launched on your computer.

- 3 Choose the server you want to manage. Click **Connect** or double-click the selected server to go to DSM's login screen.
- 4 Enter your user name and password, and click **Login**. The default password for **admin** is empty. If you want to save your login information and log in automatically next time, tick **Remember me** before logging in.



Mac OS X User:

- 1 Insert the installation disc into your computer, and then double-click the **SynologyInstall** icon on the desktop.



- 2 In the window that appears, double-click the **MacOSX** folder, and then double-click **Synology Assistant-[number].dmg**.
- 3 Double-click the **Synology Assistant.app** in the window that appears.



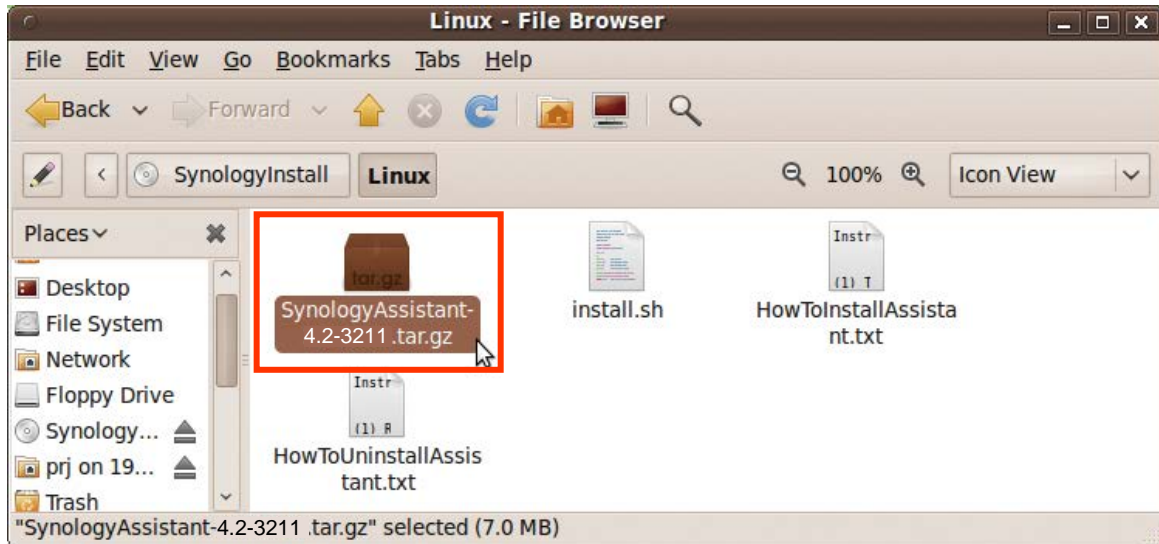
- 4 Follow step 3 to 4 of the "Windows User" section to log in to DSM.

Linux (Ubuntu) User:

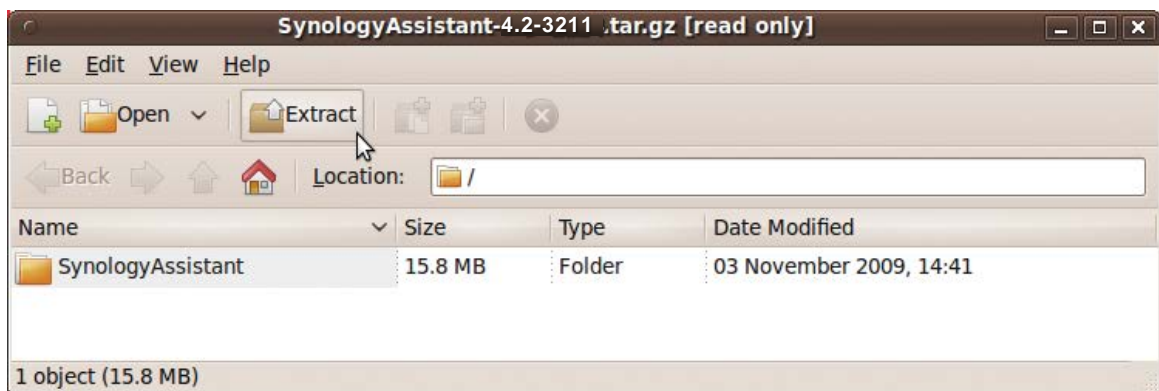
- 1 Insert the installation disc into your computer, and then double-click the **SynologyInstall** icon on the desktop.



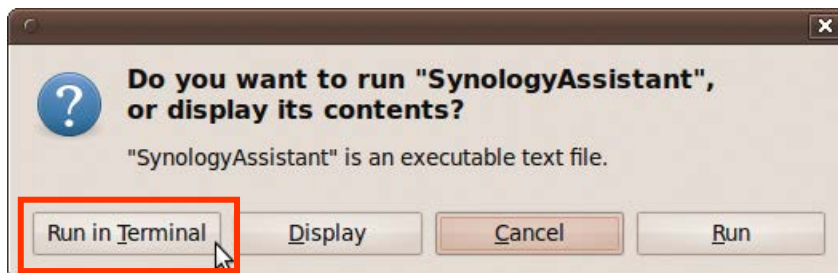
- 2 In the **File Browser** window that appears, double-click the Linux folder, and then double-click **Synology Assistant-[number].tar.gz**.



- 3 Click **Extract**, and then extract the **SynologyAssistant** directory to the path **/usr/local** or any other path.



- 4 Go to the path **/usr/local/SynologyAssistant** (or **[the path you just specified]/SynologyAssistant**), double-click **SynologyAssistant**, and then select **Run in Terminal** in the dialog box that appears.



- 5 Follow step 3 to 4 of the "Windows User" section to log in to DSM.

Use a Web Browser

- 1 Open a web browser window, enter any of the following in the address field, and then press Enter on your keyboard:

- `http://ioSafe_Server_IP:5000`
- `http://ioSafe_Server_Name:5000/` (or `http://ioSafe_Server_Name.local:5000/` on a Mac)

`ioSafe_Server_Name` should be replaced with the name you set up during the setup process. If you choose **One-step Setup** during the setup process, the `ioSafe_Server_Name` will be **ioSafe**.



- 2 Enter your user name and password, and click **Login**. The default password for **admin** is empty. If you want to save your login information and log in automatically next time, tick **Remember me** before logging in.

Note: To ensure your connection to DSM runs smoothly, please use the following browsers.

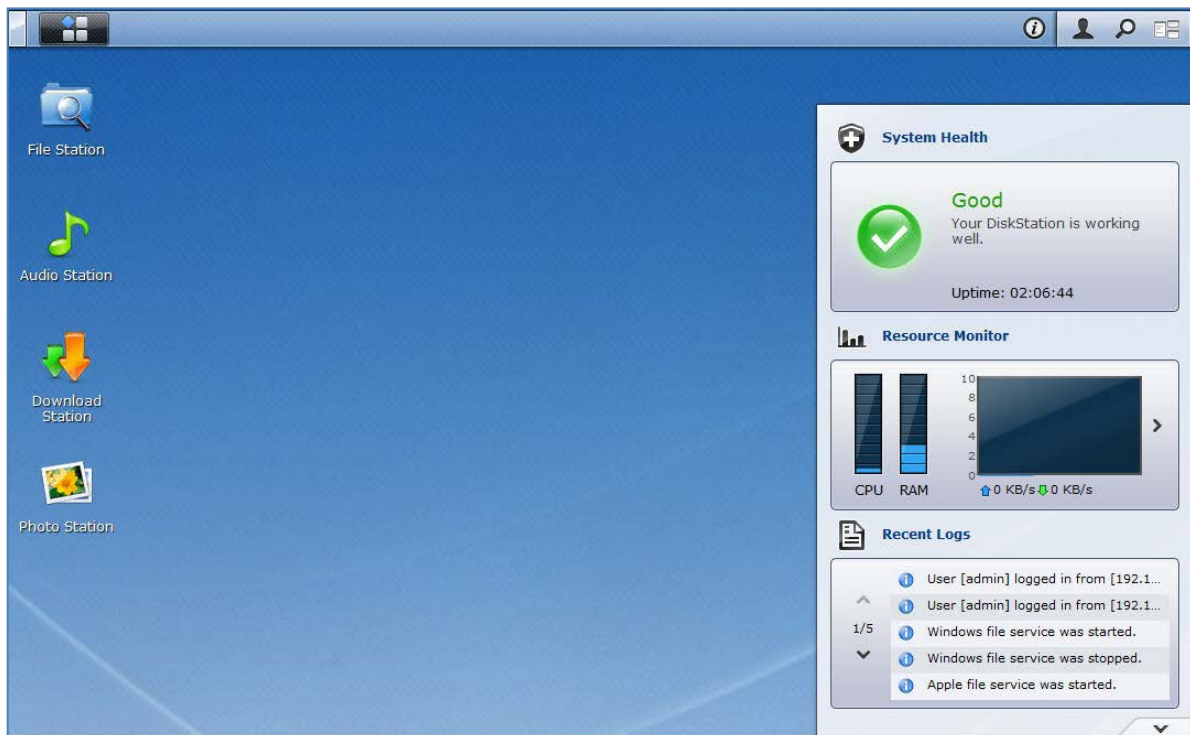
- **Chrome**
- **Firefox**
- **Safari:** 5.0 or later
- **Internet Explorer:** 8.0 or later

DiskStation Manager Appearance

When you log in to DiskStation Manager (DSM), you can see the desktop, taskbar and widgets.

Desktop and Shortcuts

The desktop is where your application windows are displayed. You can also create desktop shortcuts to frequently used applications.



To create a desktop shortcut to an application:

Drag its thumbnail from the **Main Menu** to the desktop.

To remove a desktop shortcut to an application:

Right-click the shortcut and choose **Remove shortcut**.

To open Synology-designed or third-party applications (available at Package Center) in a new browser window:

Right-click the applications' **Main Menu** thumbnail or desktop shortcut and choose **Open in New Window**.

Note: You can also customize your desktop background color or wallpaper with the **Desktop** function. See "Desktop" for more information.

Taskbar

The taskbar at the top of the desktop contains the following functions:



1 The Show Desktop button: Click to clear your application windows and reveal the desktop. Click again to bring the windows back to the desktop. For more information about application windows, see "Open Application Windows".

2 The Main Menu button: Click to reveal the **Main Menu**. See "Manage DSM with the Main Menu" for more information.

3 The icons of open applications:

- Click the icon of an application to show or hide its window on the desktop.
- Right-click the icon and choose from the shortcut menu to manage the application window (**Maximize**, **Minimize**, **Restore**, **Close**) or its taskbar icon (**Pin to Taskbar**, **Unpin from Taskbar**).

4 The Notifications button (with an exclamation mark): Click to check the logs of important events.

- **Clear All:** Click to remove all events and hide the **Notification** button.
- **Show All:** Click to see all notifications in another window.
- **(Number) unread:** If there are more than 30 unread notifications, **(Number) unread** will appear instead of **Show All** to notify you of how many notifications have not been read. Click to see all notifications in another window.

Note: For more information about system log, see "View System Logs".

5 The Options menu: Click to manage your user account settings or leave DSM.

- **Options:** Click to manage personal options for your DSM users. See "Manage Personal Options".
- **Logout:** Click to exit your current account and return to login screen.

6 The Search icon: Click to enter keywords in the search field to quickly find a list of relevant applications and **DSM Help** articles.

7 The Pilot View button: Click to have an instant preview of all open applications and hover your mouse over the application windows for quick navigation.

Note: **Pilot View** is not supported by Internet Explorer.

Widgets

The widgets at the bottom-right corner of the desktop contain the system information of your ioSafe 214.

To open/close the widget panel:

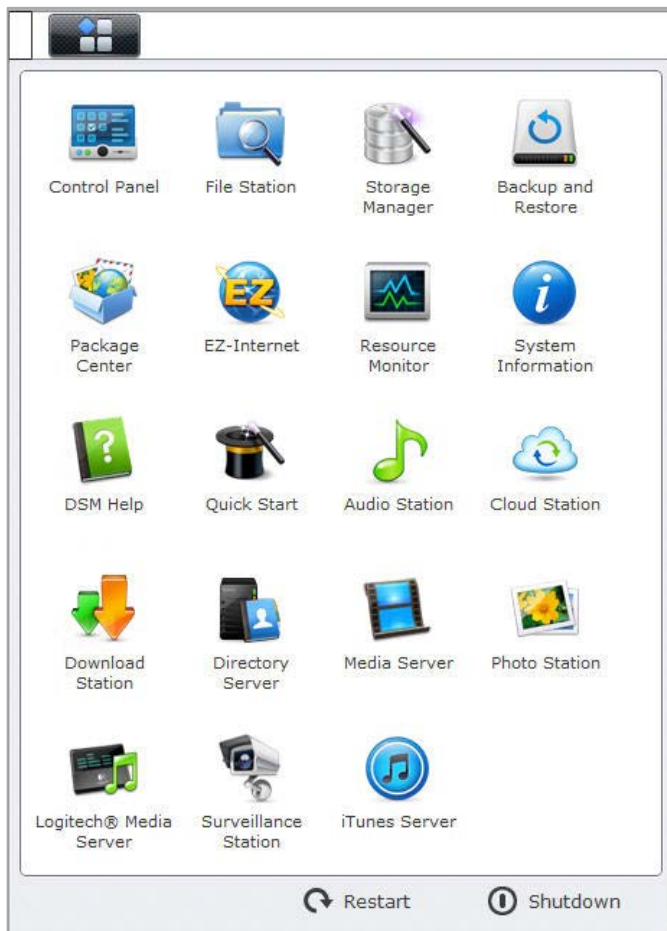
Click the upward/downward triangle to reveal/close the panel.

You can choose any three of the following subject to be displayed on the widget panel. More information can be acquired by clicking the icon at the top-left corner of each corresponding subject panel.

- **Current Connections:** See a list of users who are currently accessing the ioSafe 214 resources.
- **File Change Log:** View the file change log records of the ioSafe 214 services.
 - **No active logs:** Appears when none of the logs (Samba, WebDAV, FTP, File Station) is enabled.
 - **No logs available:** Appears when any one of the logs (Samba, WebDAV, FTP, File Station) is enabled.
- **Recent Logs:** View the log records of the ioSafe 214 services.
- **Resource Monitor:** Monitor the CPU usage, memory usage, and network flow.
- **Scheduled Backup:** View the status of your backup tasks.
- **Storage:** View your ioSafe 214's volume usage and disk status.
- **System Health:** Obtain an overall status of your ioSafe 214 and all connected devices (if any). You will be advised to take corrective action when system error occurs.

Manage DSM with the Main Menu

The **Main Menu** is where you can find all the applications and settings provided by DiskStation Manager. Not all icons below will appear until you install those applications from the package center.



Restart and Shutdown

Click **Restart** or **Shutdown** at the bottom-right corner of the **Main Menu** to restart the ioSafe 214 or turn it off, just like using any other operating systems.

Reorder Main Menu's Thumbnails

Open **Main Menu** and drag any thumbnail to any position you want.

Open Application Windows

In addition to the **Control Panel**, the **Main Menu** contains the thumbnails of all the other DSM applications. With DSM's multitasking ability, now you can open multiple application windows at the same time.

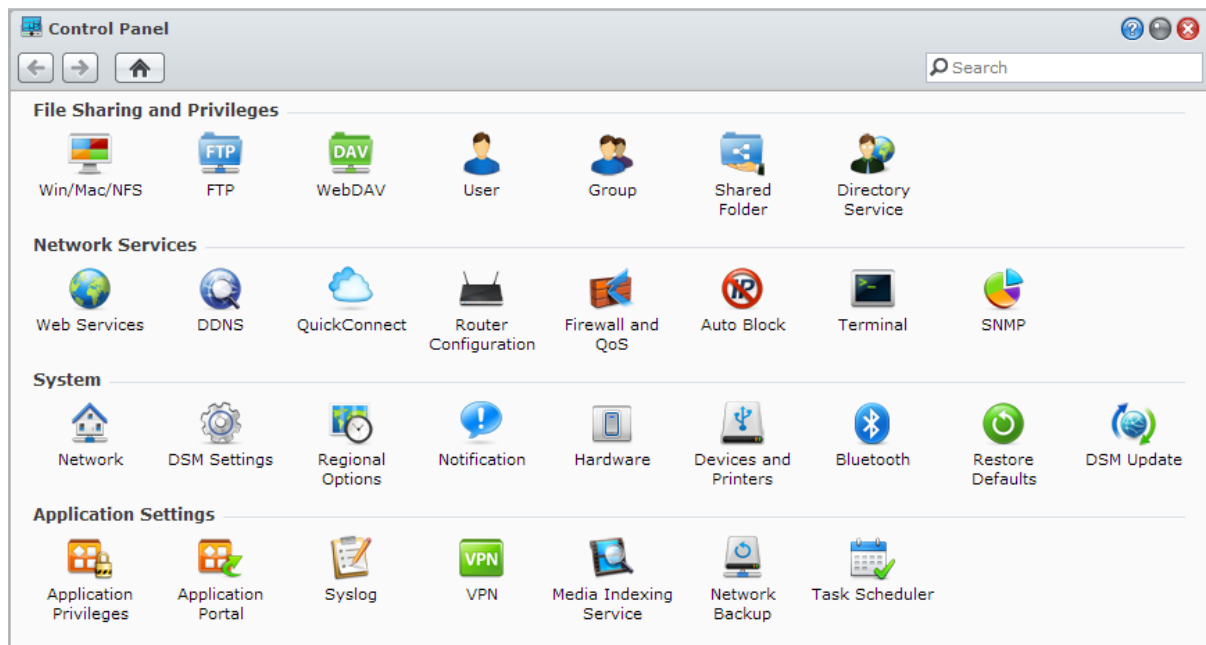
To open an application window:

Click any thumbnail of an application from the **Main Menu** to open the application window on the desktop and the application icon on the taskbar.

Note: You can also open application windows through desktop shortcuts. See "Desktop and Shortcuts" for more information.

Use the Control Panel

Choose **Control Panel** from the **Main Menu** to see the thumbnails of DSM settings.



The DSM settings on the Control Panel are grouped into the following categories:

- **File Sharing and Privileges:** Set up file sharing for Win/Mac/NFS, as well as application privileges for different user accounts.
- **Network Services:** Manage and edit the settings for network services and Internet connection.
- **System:** Edit the basic settings on your ioSafe 214.
- **Application Settings:** Assign application privileges for user accounts, enable the services of built-in applications, create a VPN connection, and index multimedia files stored on your ioSafe 214 for applications.

Note: Control Panel is accessible only to users belonging to the **administrators** group. See "Create Groups" for more information.

Manage Personal Options

Click the **Options** menu (with a figure icon) at the top-right corner of your DSM desktop to manage your user account settings or log out of DSM.

The screenshot shows the 'Options' window with the 'Account' tab selected. The window has a title bar with a question mark, a close button, and a maximize button. Below the title bar are four tabs: 'Account', 'Volume Usage', 'Desktop', and 'Others'. The 'Account' tab is active, showing the following fields and controls:

- Name:** Hector
- Description:** [Empty text box]
- Password:** [Masked text box with 6 dots]
- Confirm password:** [Masked text box with 6 dots]
- Email:** [Empty text box]
- Display language:** English (dropdown menu)
- ☐ **Enable 2-step verification**
- 2-Step Verification** (button)
- View your account activity, including current connections and login history.**
- Account Activity** (button)

At the bottom of the window are 'OK' and 'Cancel' buttons.

Account

Under **Account**, you can edit your account settings, enable 2-step verification, and view recent login activity of your DSM account.

Limitations:

- The user description is case sensitive and can be 0 to 64 displayable Unicode characters.
- The password is case sensitive and should be 0 to 127 displayable characters, including letters, numbers, signs, and space.

2-Step Verification

2-step verification provides improved security for your DSM account. If 2-step verification is enabled, you will need to enter your password in addition to a one-time verification code when logging into DSM. Verification codes are obtained from authenticator apps installed on your mobile device. Therefore, if someone wants to access your account, he will not only need your username and password, but also your mobile device.

Requirements:

2-step verification requires a mobile device and an authenticator app which supports the Time-based One-Time Password (TOTP) protocol. Authenticator apps include Google Authenticator (Android/iPhone/BlackBerry) or Authenticator (Windows Phone).

Account Activity

Account activity displays recent login activity of your DSM account, such as the time your account was accessed or from what IP address.

Volume Usage

Under **Volume Usage**, you can view your quota on all ioSafe 214 volumes set by DSM **administrators**, as well as the amount of capacity you have used on each volume.

Desktop

Under **Desktop**, you can customize the appearance of your desktop by changing the background and text color of the desktop, or uploading images to be used as the desktop wallpaper.

Photo Station

This tab is viewable only when users belonging to the **administrators** group enable Personal Photo Station service in Photo Station. ioSafe's 214 provides the **home/photo** folder for you to store photos and videos that you want to share. The system will create index thumbnails of the photos and videos automatically, and then people can view photo albums via a web browser. See "Enable Personal Photo Station" for more information.

Others

Under **Others**, you can customize other personal options. For more information about personal options, please see **DSM Help**

Modify System Settings

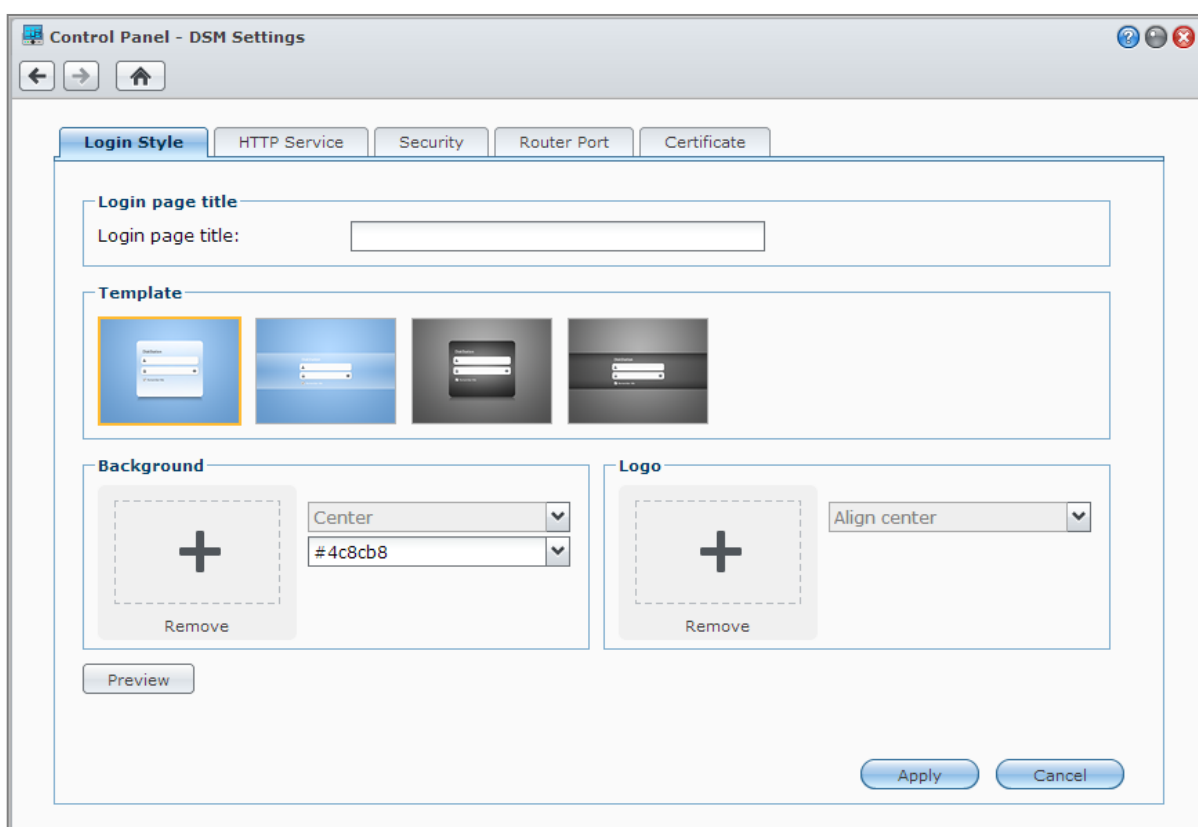
After you have connected to the ioSafe 214 through DiskStation Manager (DSM) and learned how to access its functions and customize its appearance, users belonging to the **administrators** group can begin to modify basic settings.

This chapter explains the basics of modifying network settings, display languages, time, and energy saving features. For more detailed instructions, please see [DSM Help](#).

Change DSM Settings

DSM provides options to change the style of the login screen, customize the ports used for HTTP service, enhance the security of browsing sessions, configure ports for sharing files with Internet services, and validate the identity of a server and the administrator with a certificate.

Go to **Main Menu > Control Panel > DSM Settings** to change the following DSM settings. For more detailed instructions, please see [DSM Help](#).



Login Style

The **Login Style** tab provides options to change the layout of the DSM login screen, allowing you to choose from a variety of templates or upload custom logos or background images.

HTTP Service

Click the **HTTP Service** tab to change the port number for accessing DSM or configure HTTPS settings. When the HTTPS connection function is enabled, any connection to the ioSafe 214 via the HTTPS protocol will be encrypted with the SSL/TLS encrypting mechanism.

More Information

About redirecting to HTTPS connection:

When the option **Automatically redirect HTTP connections to HTTPS** is checked, you will be redirected to port 5001 while trying to access the web DSM through port 5000.

Ports used for HTTPS connection:

- **DSM:** The port number is 5001, so you can access the DSM through the secure channel:
https://ioSafe_Server_IP:5001/
- **Web Station:** The port number is 443, so you can access Web Station through the secure channel:
https://ioSafe_Server_IP:443/ or https://ioSafe_Server_Name:443/

Security

Click the **Security** tab to modify the security settings for each DSM login session. The following options are available here:

- **Logout timer:** An automatic logout occurs if you are inactive for the time period you specified in the logout timer.
- **Enhance browser compatibility by skipping IP checking:** If you access the ioSafe 214 through a HTTP proxy and encounter random logouts, you can skip IP checking. However, skipping IP checking will lower the security level.

Router Port

Click the **Router Port** tab to configure router port settings. To open files on the ioSafe 214 with Internet services (such as Google Docs or Pixlr Editor), please enter the hostname or public static IP address of the 214, as well as the public port number. These settings only need to be modified if different port numbers were specified for the router port (assigned on your router) and the local port (assigned on your ioSafe 214) during setup.

Certificate

A certificate can be used for SSL secured services of the ioSafe 214, such as web, mail, or FTP. Having a certificate allows users to validate the identity of a server and the administrator before sending any confidential information. Click the **Certificate** tab to manage and view the status of 214 certificates, allowing you to create, import/export, or renew certificates. The certificate setup wizard helps create self-signed certificates or download certificate signing requests (CSR) for registration with certificate authorities (CA).

For more information regarding managing certificates, please see **DSM Help**.

Change Network Settings

Go to **Main Menu** > **Control Panel** > **Network** to modify the following network settings of your ioSafe 214. For more detailed instructions, please see **DSM Help**.

The screenshot shows the 'Control Panel - Network' window with the 'General' tab selected. The window has a title bar with standard OS controls and navigation buttons. Inside, there are three tabs: 'General', 'Network Interface', and 'Tunnel'. The 'General' tab contains the following fields and options:

- Instruction: "Enter the server name, DNS server and default gateway information."
- Server Name: Text box containing "DiskStation".
- Default gateway: Text box containing "192.168.31.254".
- ☐ Manually configure DNS server
 - Preferred DNS Server: Text box containing "192.168.252.254".
 - Alternative DNS Server: Text box.
- ☐ Connect via a proxy server
 - Address: Text box.
 - Port: Text box containing "80".
- Advanced Settings: Button.
- ☒ Bypass proxy server for local addresses.

At the bottom right of the window are 'Apply' and 'Cancel' buttons.

General

The **General** tab provides options to edit the name and default gateway of the ioSafe 214, as well as configure domain name server or proxy server settings.

Network Interface

The **Network Interface** tab provides options to connect your ioSafe 214 to the network via the following network interfaces.

LAN

If your 214 is connected to a local area network, you can click **LAN** on the left side to configure network interface settings, such as choosing whether to automatically obtain network configurations with DHCP or to manually set the IP address of the 214.

Wireless

Click **Wireless** on the left side to connect the ioSafe 214 to a wireless network. Wireless network is available only when a wireless dongle is plugged into the USB port of your ioSafe 214.

IPv6 Setup

When you are configuring the **LAN** or **Wireless Network** interface, click the **IPv6 Setup** button to change the IPv6 settings.

ioSafe 214 supports IPv4/IPv6 dual stack scheme. This means that both IPv4 and IPv6 can work simultaneously on ioSafe 214. The default setting for IPv6 is **Auto**.¹

¹ IPv6 service is only supported on 08-series models or later (excluding 108j, 109j).

PPPoE

Click the **PPPoE** on the left side if your ioSafe 214 is connecting to a DSL or cable modem, and your Internet Service Provider (ISP) uses PPPoE (Point to Point Protocol over Ethernet).

Hotspot

If a wireless dongle¹ is connected to the USB port of your ioSafe 214, you can enable hotspot on your 214 to turn it into a wireless access point that can share its wireless connection with computers or mobile devices within the range of the Wi-Fi network.

Tunnel

Tunnel is a technique that encapsulates IPv6 packets within IPv4 packets, allowing isolated IPv6 host or network to be compatible with IPv4 network backbone.

Click the **Tunnel** tab to allow your 214 to gain Internet access via IPv6 under the IPv4 environment.

Modify Regional Options

Go to **Main Menu > Control Panel > Regional Options** to configure the following regional options. For more detailed instructions, please see **DSM Help**.

Control Panel - Regional Options

Time | Language | NTP Service

Current Time
Wed Aug 8 08:12:26 2012

Time Zone
Time zone: (GMT+08:00) Taipei

Time Setting

☒ Manually
Date: 2012/8/8
Time: 08 : 12 : 26

☐ Synchronize with a NTP server
Network time server:
Update Now

Apply Cancel

¹ For a complete list of supported wireless dongles, visit <http://iosafe.com/support>.

Set Up Time

Click the **Time** tab to set up the system time settings of the 214. You can check the current time, manually set the server's date and time, or automatically set the time using a network time server.

Language

Click the **Language** tab to set the language for DiskStation Manager, notifications, and specify the codepage for Unicode filename conversion.

- **Display Language:** Choose your preferred display language, or have it the same as your default browser setting.
- **Notification Language:** Set your preferred language for email and instant messaging notifications from ioSafe 214.
- **Codepage:** ioSafe 214 uses Unicode to avoid file inaccessibility from computers using different languages. But for the following devices or applications to use ioSafe 214 services without problem, you need to choose the appropriate codepage for them:
 - Computers without Unicode support
 - Applications that convert non-Unicode strings to Unicode, such as FTP service, UPnP support, music metadata indexing

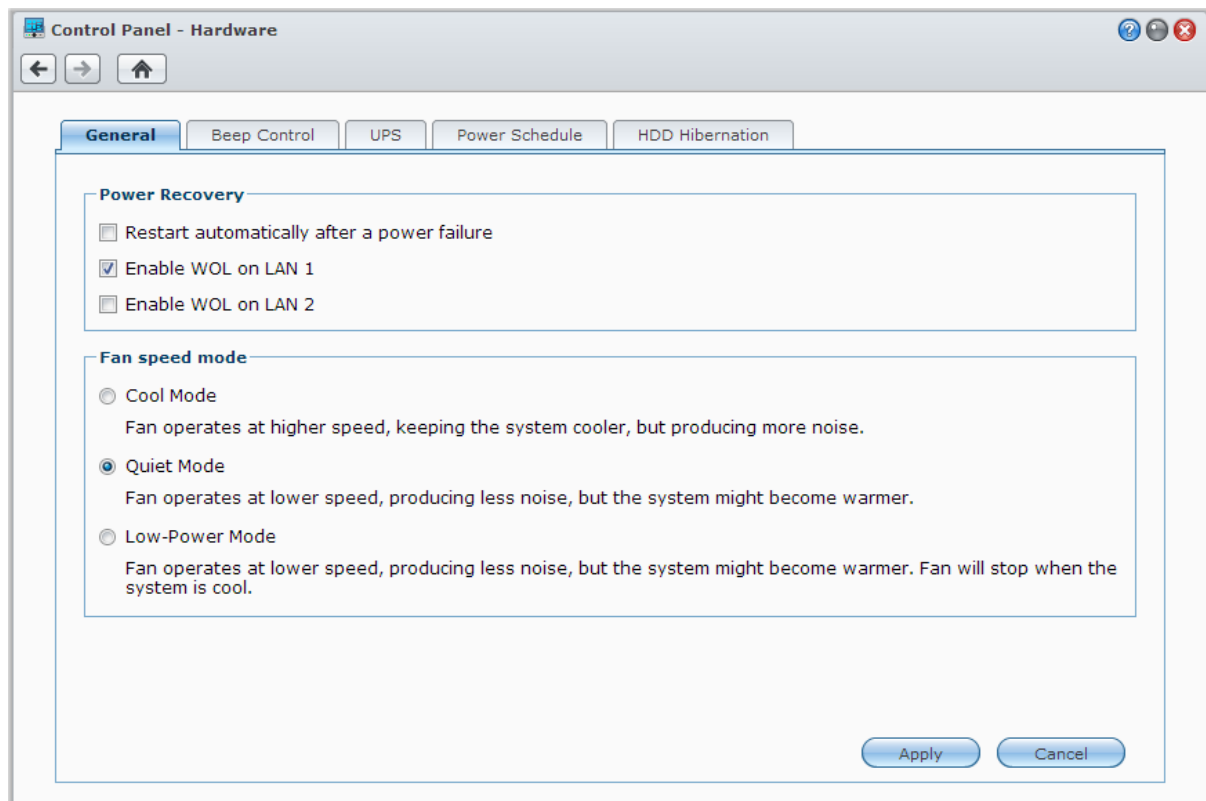
NTP Service

Click the **NTP Service** tab to have your ioSafe 214 serve as a network time server to synchronize time between different network devices and the 214 over network.

Note: The NTP service is required for Surveillance Station and Synology High Availability. Therefore, if you have Surveillance Station installed and run on your 214, the service cannot be disabled while the package is running.

Use Energy Saving Features

Go to **Main Menu > Control Panel > Hardware** to manage the following energy saving features provided by DSM. For more detailed instructions, please see **DSM Help**.



General

Click the **General** tab to modify power recovery, Wake on LAN (WOL), or fan speed settings.

- **Restart automatically after a power failure:** If the system shuts down due to unexpected power failure, the power recovery function allows the system to boot up automatically once power has been restored.
- **Enable Wake on LAN:** Enable Wake on LAN for the specified network interface.
- **Fan Speed Mode:** Modify the fan speed according to your environment and preferences.

More Information

About Wake on LAN: After Wake on LAN is enabled for your 214, you can turn on ioSafe 214 over the local area network or the Internet by using a WOL (Wake on LAN) application. Activate the function by entering 214's IP address (or DDNS hostname) and MAC address.

Wake on LAN works only after ioSafe 214 is shut down properly by pressing the **Power** button or selecting **Shutdown** from DSM's Main Menu, and its power cord is plugged into a working power outlet.

Beep Control

Click the **Beep Control** tab to have 214 play beep sounds under certain circumstances.

UPS

Under the **UPS** tab, you can modify UPS-related settings. UPS (Uninterruptible Power Supply) is a backup power device that allows the ioSafe 214 to continue operating for a short time if power failure occurs. This function helps prevent data loss by giving the 214 enough time to save data and unmount volumes before losing power and shutting off. The 214 supports connecting to local or SNMP UPS devices.

Power Schedule

Click the **Power Schedule** tab to start up or shut down automatically at a specified time.

HDD Hibernation

Click the **HDD Hibernation** tab to manage disk hibernation for all internal or external disks on your 214.

When a disk enters HDD hibernation mode, it will stop spinning and become inactive, which not only saves energy but also extends the disk's lifespan.

Manage Storage Space

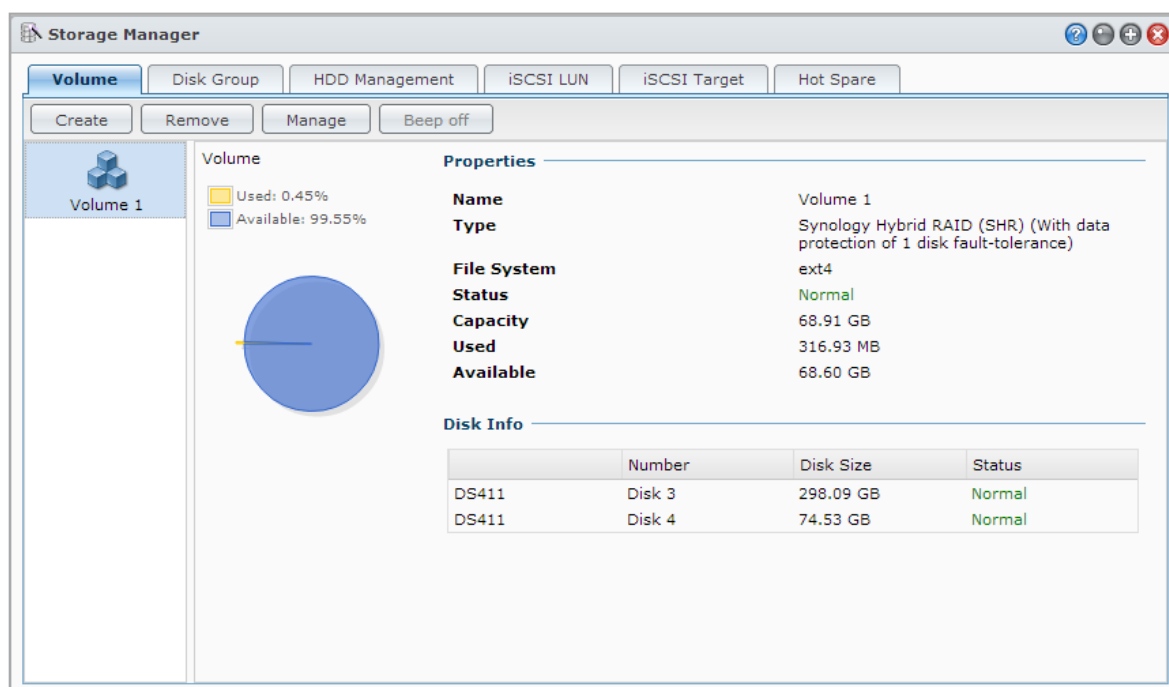
Before taking advantage of the various features of your ioSafe 214, you need to set up storage spaces. This chapter explains how Storage Manager can help you manage storage spaces, such as volumes, Disk Groups, iSCSI Targets, or iSCSI LUNs, as well as view the status of hard drives. For more detailed instructions, please see [DSM Help](#).

Volumes and Disk Groups

Volumes are the basic storage spaces on your ioSafe 214. Before you start storing or serving any data on your 214, you will need to create at least one volume. With DSM's Storage Manager, volumes can be created with various options, such as different RAID types or customized capacity allocation. For detailed instructions, please see [DSM Help](#).

Create Volumes

To create a volume, go to [Main Menu](#) > [Storage Manager](#) > [Volume](#) and click [Create](#). This action launches a setup wizard which helps create a volume based on your individual needs.



Quick or Custom Volumes

When creating a new volume, the following options are available:

Method	Features
Quick	Creates an SHR (Synology Hybrid RAID) volume. Automatically optimizes volume capacity and performance based on member hard disks. Recommended for saving time and simplifying storage management.
Custom	Supports different RAID types. Supports creating single or multiple volumes on Disk Groups. Provides options to allocate specific amounts of capacity for each volume (only when creating multiple volumes on RAID) Recommended for users who want to precisely control storage management on your 214.

Single or Multiple Volumes on RAID

When creating a custom volume, the following options are available:

Option	Feature
Single Volume on RAID	Uses all of the available capacity of the selected disks to create a single volume. Provides better speed and performance. Supports different RAID types.
Multiple Volumes on RAID	Allows you to create multiple volumes on a Disk Group. Supports allocating specific amounts of capacity to each volume. Provides greater storage management flexibility. Supports different RAID types.

RAID Types

Depending on your model and number of installed hard disks, the below RAID types can be implemented when creating custom volumes or Disk Groups.

RAID Type	HDD #	Allowed Failed HDD #	Description	Capacity
SHR	1	0	A Synology Hybrid RAID volume optimizes storage capacity and performance when combining hard drives of different sizes. SHR volumes consisting of two provide 1-disk fault tolerance.	1 x (HDD size)
	2	1		Optimized by the system
Basic	1	0	A Basic volume is created with one hard drive as an independent unit. When creating a Basic volume, you can select only one hard drive at a time.	1 x (HDD size)
JBOD	2	0	JBOD is a collection of hard drives.	Sum of all HDD sizes
RAID 0	2	0	Combining multiple disks to build a storage space, RAID 0 offers Striping , a process of dividing data into blocks and spreading the data blocks across several hard drives, but without safety measures.	(HDD #) x (Smallest HDD size)
RAID 1	2	1	The system will write identical data to each hard drive at the same time, so data integrity is protected when at least one disk is normal.	Smallest HDD size

Create Disk Groups

As stated above, creating Disk Groups provides more flexibility when managing storage spaces. Disk Groups can be created within the volume creation setup wizard, or you can go to **Main Menu > Storage Manager > Disk Group** and click **Create**.

Repair Volumes or Disk Groups

The repair function is available for RAID 1 and SHR volumes or Disk Groups. Depending on your RAID types, when one of the hard drives in the volume or Disk Group fails, it will be in the **degraded** mode. You can repair the volume or Disk Group by replacing the crashed disk(s) to keep the data on the volume or Disk Group protected. For more detailed instructions, please see **DSM Help**.

Expand Volumes or Disk Group

The storage capacity of volumes or Disk Groups can be gradually expanded by installing more or larger hard disks. This feature allows you to expand the capacity of your volume or Disk Group according to your budget and with no need to worry about losing any existing data.

The sections below provide basic information regarding expanding volumes and Disk Groups. For more detailed instructions, please see **DSM Help**.

Expand a Volume by Changing Volume Size

When creating multiple volumes on RAID, specified amounts of Disk Group storage capacity can be allocated to each volume. If you want to change the amount of allocated storage capacity for a volume, please select the volume and click **Edit**.

Expand a Volume or Disk Group by Replacing Hard Disks

For SHR or RAID 1, the storage capacity of volumes and Disk Groups can be expanded by replacing smaller hard disks with larger ones. When expanding storage capacity with this method, please be careful to replace each hard disk one-by-one. After replacing one hard disk, the volume or Disk Group must be repaired before the next hard disk is replaced. For more detailed instructions, please see **DSM Help**.

Please see the following table to see which hard disk should be replaced first.

RAID Type	Minimum Hard Disk Size
SHR (Synology Hybrid RAID)	If the capacity of all member hard disks is equal, then you should replace at least two hard disks. Otherwise, the capacity of your volume will not expand.
	If the capacity of member hard disks is different, then the new, replacement hard disks should be equal to or larger than the largest existing hard disk. In addition, you should replace smaller member hard disks first in order to optimize capacity usage.

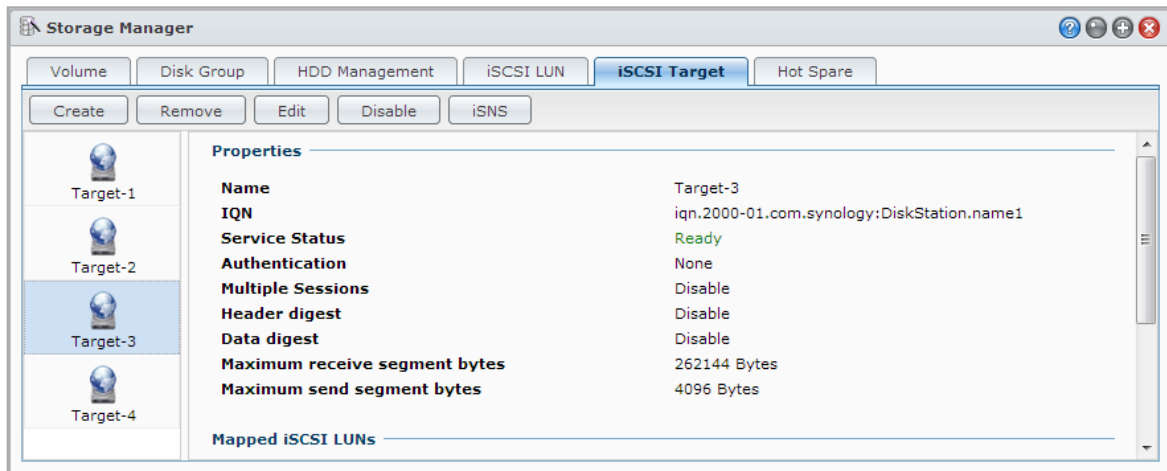
iSCSI Targets and LUNs

iSCSI (Internet Small Computer System Interface) is a type of storage area networking (SAN) service that provides access to consolidated, block level data storage. The main use of iSCSI is to facilitate data transfers over intranets, allowing users to manage storage over long distances.

The sections below provide basic information regarding iSCSI Targets and LUNs. For more detailed instructions, please see **DSM Help**.

Manage iSCSI Targets

Go to **Main Menu > Storage Manager** and click the **iSCSI Target** tab to manage iSCSI Targets on your ioSafe 214. The maximum number of iSCSI Targets on the 214 is 10. For more information, please refer to "Manage iSCSI LUNs".



Manage iSCSI LUNs

An iSCSI LUN (logical unit number) represents an individually addressable portion of an iSCSI Target. An iSCSI LUN can be mapped to multiple iSCSI Targets to perform storage operations such as read or write.

Go to **Main Menu > Storage Manager** and click the **iSCSI LUN** tab to manage iSCSI LUNs on your ioSafe 214. The maximum number of iSCSI LUNs on the 214 is 10. For detailed product specifications, please refer to www.ioSafe.com.



Manage Hard Disks

The **HDD Management** tab allows you to monitor the status of the hard disks installed in your 214, providing options to manage and analyze hard disk performance and health. To see this tab, go to **Main Menu > Storage Manager** and click **HDD Management**. For more detailed instructions, please see **DSM Help**.

Enabling Write Cache Support

Enabling write cache support enhances the performance of your 214. Only certain hard disk models support this feature. To ensure data protection while using write cache support, usage of a UPS device is strongly recommended. We also suggest the system be shut down properly every time after use. Disabling write cache will reduce the chances of data loss caused by abnormal power outages, but system performance will decline.

Running S.M.A.R.T. Test

Disk S.M.A.R.T. tests examine and report the status of your hard disk, alerting you to possible disk failures. We recommend promptly changing your disk if any errors are detected. S.M.A.R.T. tests can also be scheduled to run automatically by creating tasks.

Checking Disk Info

The **Disk Info** section displays a hard disk's model name, serial number, firmware version, and total size.

SSD Cache

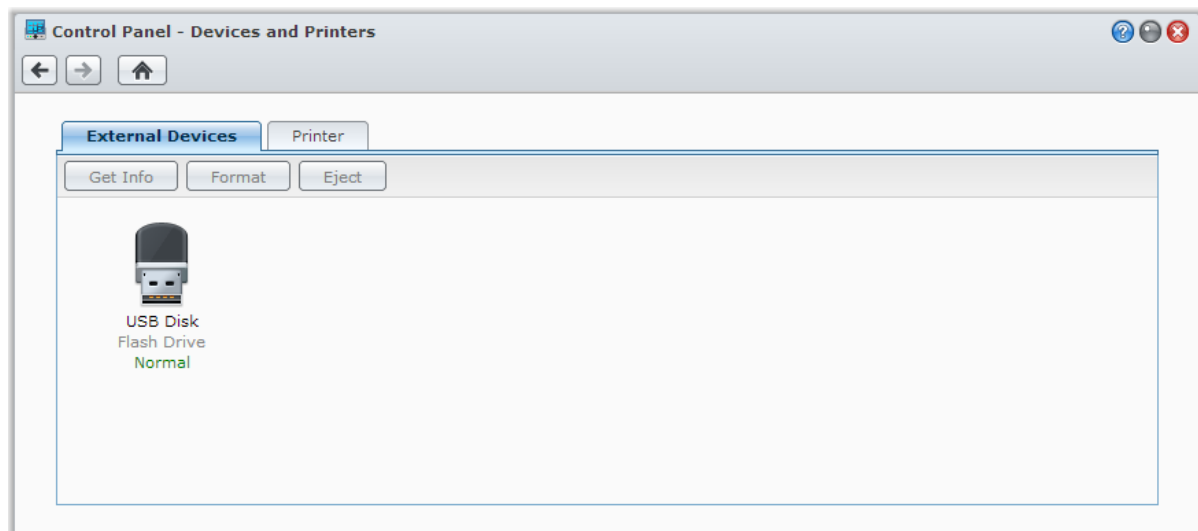
SSD cache¹ drives can be installed and mounted in a RAID 0 configuration to boost the read speed of a volume, including iSCSI LUN (Regular Files) on a volume, or iSCSI LUN (Block-Level) on your ioSafe server. You can mount, check SSD compatibility, and view related information by going to **Main Menu > Storage Manager > SSD Cache**.

Please refer to your ioSafe Quick Installation Guide for information regarding SSD installation. For more detailed information regarding SSD management, please see **DSM Help** or **Synology SSD Cache White Paper**.

Manage External Disks

External USB disks can be attached to the USB port of your ioSafe 214 for backup or file sharing purposes.

Go to **Main Menu > Control Panel > Devices and Printers > External Devices** to manage attached external disks or setup printers. The **External Devices** tab provides options to view device information, change formats, or eject the device. The **Printer** tab provides options to setup USB or network printers. For more detailed instructions, please see **DSM Help**.



¹ SSD cache is supported on specific models only. Visit www.synology.com for more information

Access your 214 from the Internet

You can connect to your ioSafe 214 over the Internet, allowing its services to be accessible from anywhere and anytime.

This chapter explains the basics regarding using the Synology EZ-Internet wizard, advanced port forwarding functions, and DDNS hostname registration to connect your ioSafe 214 to the Internet. For more detailed instructions, please see [DSM Help](#).

Use the EZ-Internet Wizard

The **EZ-Internet** Wizard can set up 214 access via the Internet with an easy-to-use wizard, without going through the complicated firewall settings, PPPoE setup, DDNS registration, and router port forwarding configuration. Go to **Main Menu > EZ-Internet** and follow the wizard to complete the setup.

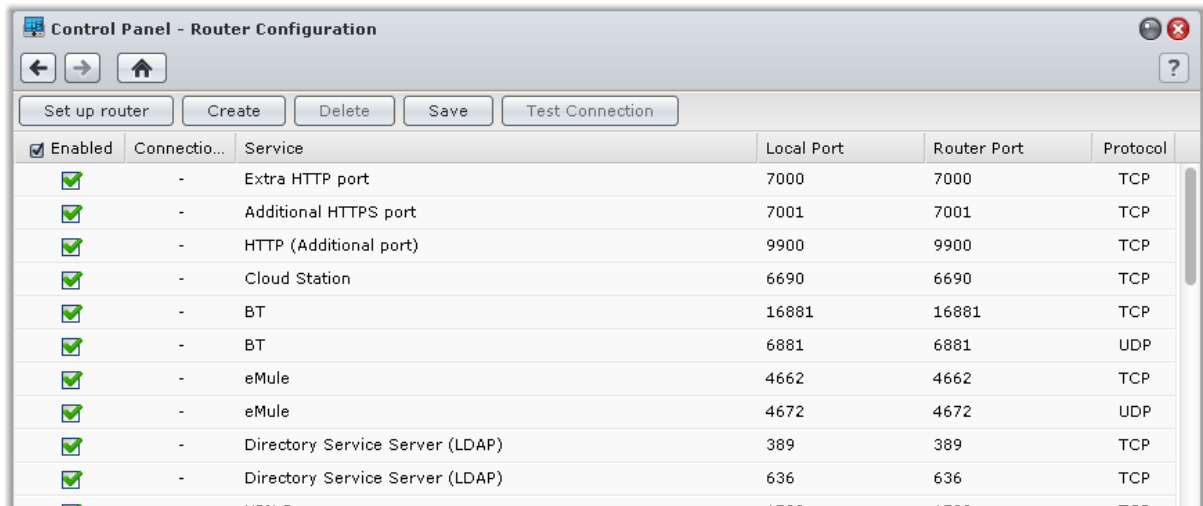


Set Up Port Forwarding Rules for Router

If your ioSafe 214 is within the Intranet, you can set up port forwarding rules for the router to allow your ioSafe 214 to be accessible over the Internet.

Note: Before you start, make sure you have manually assigned a static IP address for your ioSafe 214. See "Network Interface" for more information.

Go to **Main Menu > Control Panel > Router Configuration** to set up your router and port forwarding rules. For more detailed instructions, please see **DSM Help**.



Note: To configure port forwarding rules and assign static IP address, you must have the administrative permission to the router.

Set up Router

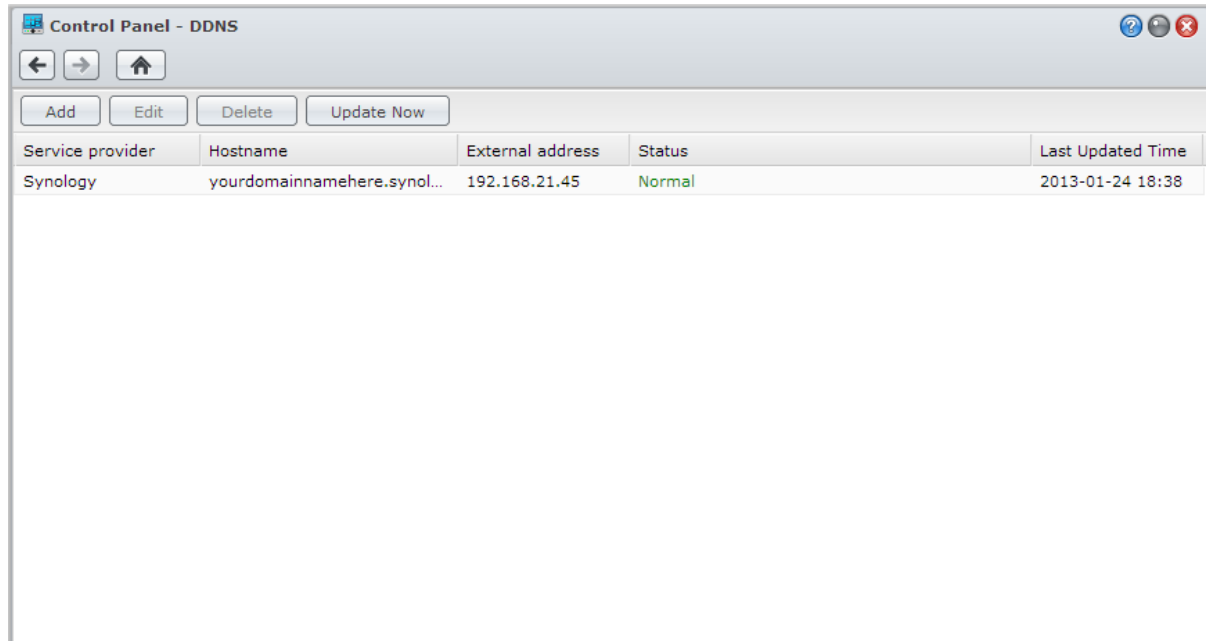
Before adding port forwarding rules with DSM, you need to set up 214's connection to the router. To begin, please click the **Set up router** button.

Add Port Forwarding Rules

Add port forwarding rules to specify the destination ports of your ioSafe 214 that will receive packages from specific router ports. Click **Create** to start creating port forwarding rules.

Register DDNS for 214

DDNS (Dynamic Domain Name Service) simplifies connecting to your 214 over the Internet by mapping a hostname to its IP address. For example, DDNS allows you to access your 214 using a domain name (e.g. www.john.synology.me), with no need to remember an IP address (e.g. 172.16.254.1).



Service Requirement

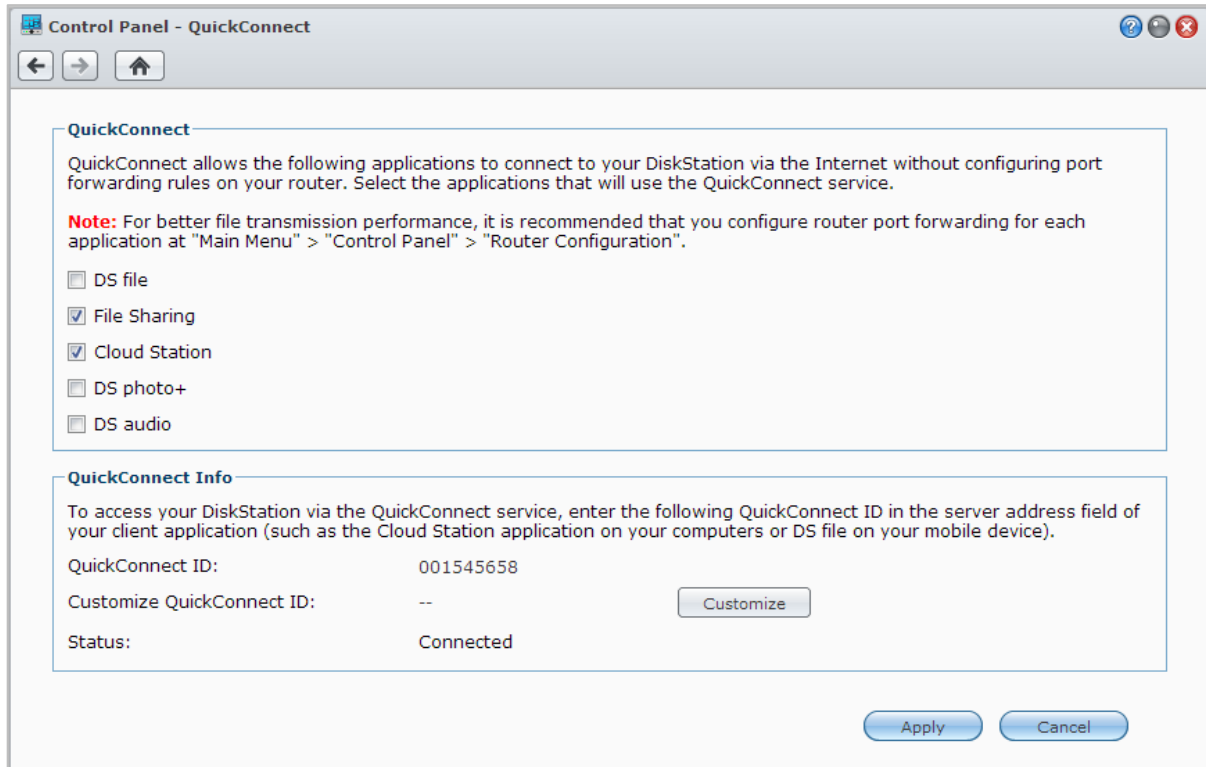
- The servers of the DDNS service provider are working normally.
- The 214 is able to connect to the Internet.
- DDNS will only run in a network environment where there is no proxy server required.
- You can only enter one hostname for each DDNS provider.

Register a DDNS hostname for your ioSafe 214

Go to **Main Menu** > **Control Panel** > **DDNS**. You can point an existing hostname at the IP address of your 214, or register for a new one provided by Synology or several other DDNS providers. Please consult each provider for more details regarding hostname registration.

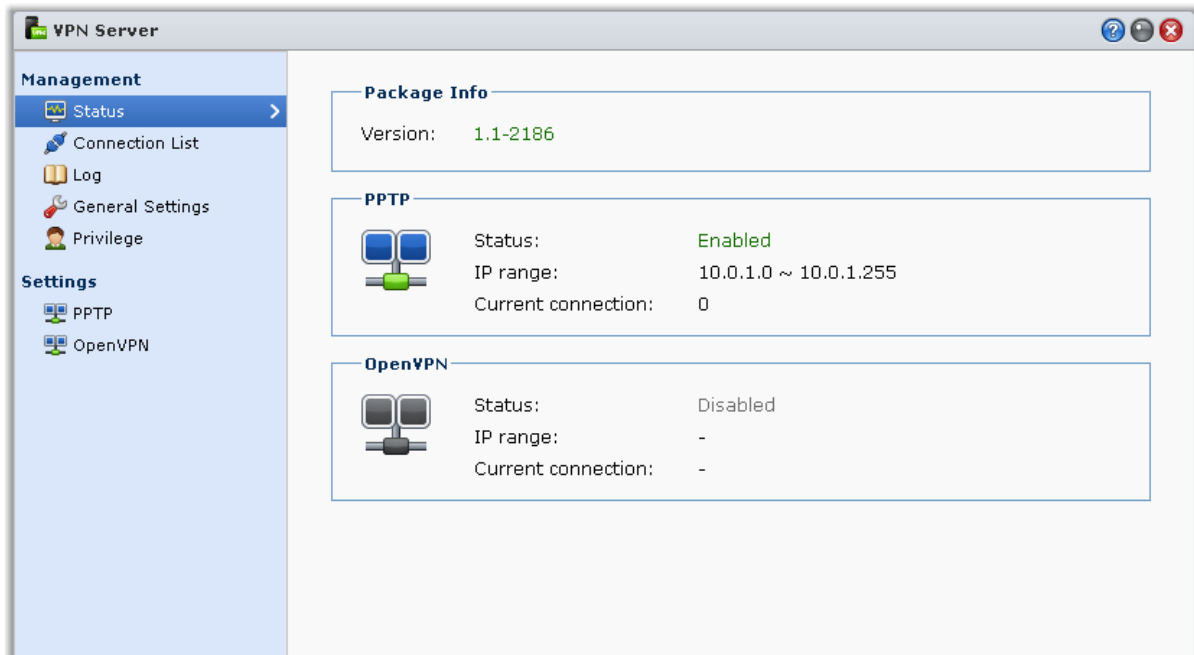
Access DSM Services via QuickConnect

QuickConnect is a solution that helps client applications (such as DS file, Cloud Station, DS audio, etc.) connect to your 214 via the Internet without setting up port forwarding rules. Go to **Main Menu > Control Panel > QuickConnect** to manage the QuickConnect service. For more details regarding QuickConnect, please see **DSM Help**.



Set up VPN Connection

VPN Server is an add-on package that enables your 214 to become a PPTP/OpenVPN VPN (virtual private network) server, allowing DSM local users over the Internet to access resources shared within 214's local area network. For more information about VPN, refer to [here](#).



Set up your 214 as a VPN Server

To install VPN Server on your 214, go to **Main Menu > Package Center**. For more information about VPN Server, run and launch the package, and then click its **Help** button (with a question mark) at the top-right corner. To learn more about how to access 214's VPN Server with a VPN client, refer to the **VPN Server User's Guide** available at Synology's [Download Center](#).

Connect your ioSafe 214 to a VPN Server

Go to **Main Menu > Control Panel > VPN** to set your 214 as a VPN client to connect to a VPN server, and then gain access to the virtual private network. For each VPN server, you can create or modify its connection profile, and then use the profile to connect to the server with a simple click. For more information about how to set your 214 as a VPN client, click the **Help** button (with a question mark) at the top-right corner.

Note: You are not allowed to set your 214 as a VPN server and client at the same time.

Enhance Internet Security

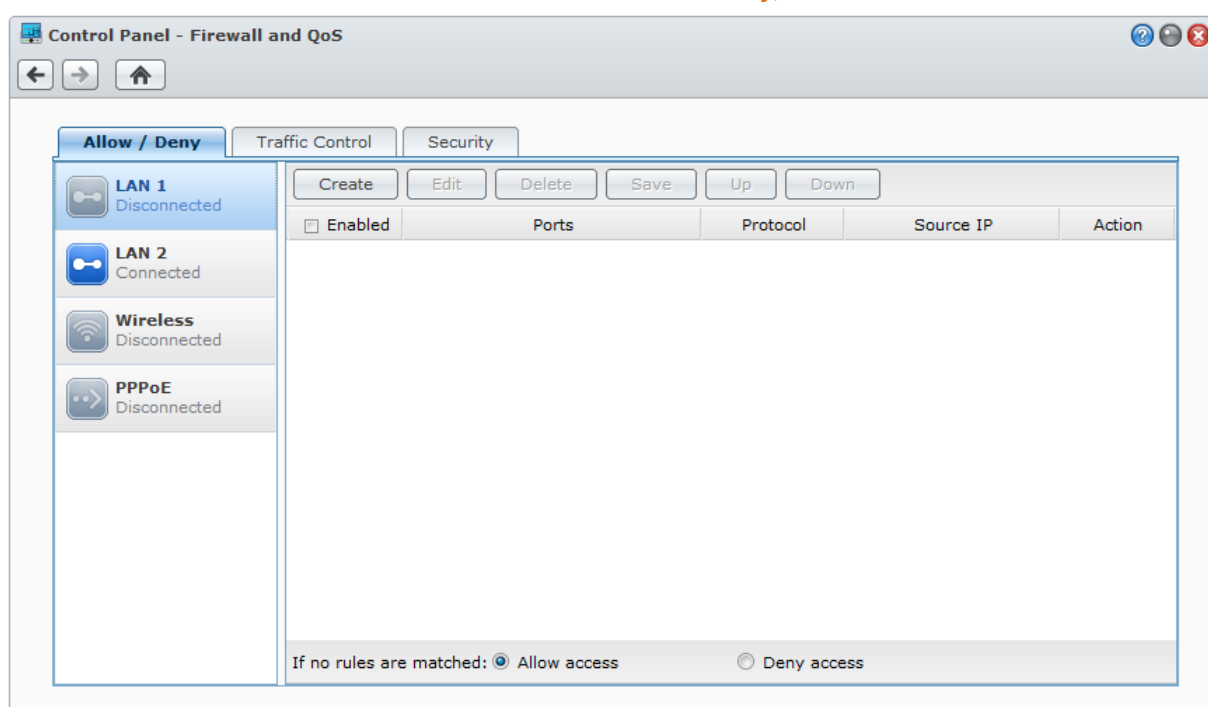
After your ioSafe 214 is available on the Internet, you will need to safeguard it against any attacks from Internet hackers.

This chapter explains how to set up firewall, control outgoing traffic, enable DoS protection and enable auto block. For more detailed instructions, please see [DSM Help](#).

Prevent Unauthorized Connection with Firewall

The built-in firewall can prevent unauthorized logins, and control which services can be accessed. In addition, you can choose to allow or deny access to certain network ports from specific IP addresses.

Go to **Main Menu > Control Panel > Firewall and QoS > Allow / Deny**, and click **Create** to create firewall rules.



Apply Firewall Rules to Ports

In the **Ports** section, apply firewall rules to all ports or selected ports using one of the following options:

- **All:** Choose this option to apply the rule to all ports on ioSafe 214.
- **Select from a list of built-in applications:** Tick the system services that will be included in the rule.
- **Custom:** Specify the type and protocol of the port, and enter the custom port number.

You can enter up to 15 ports separated with comma, or by specifying a port range.

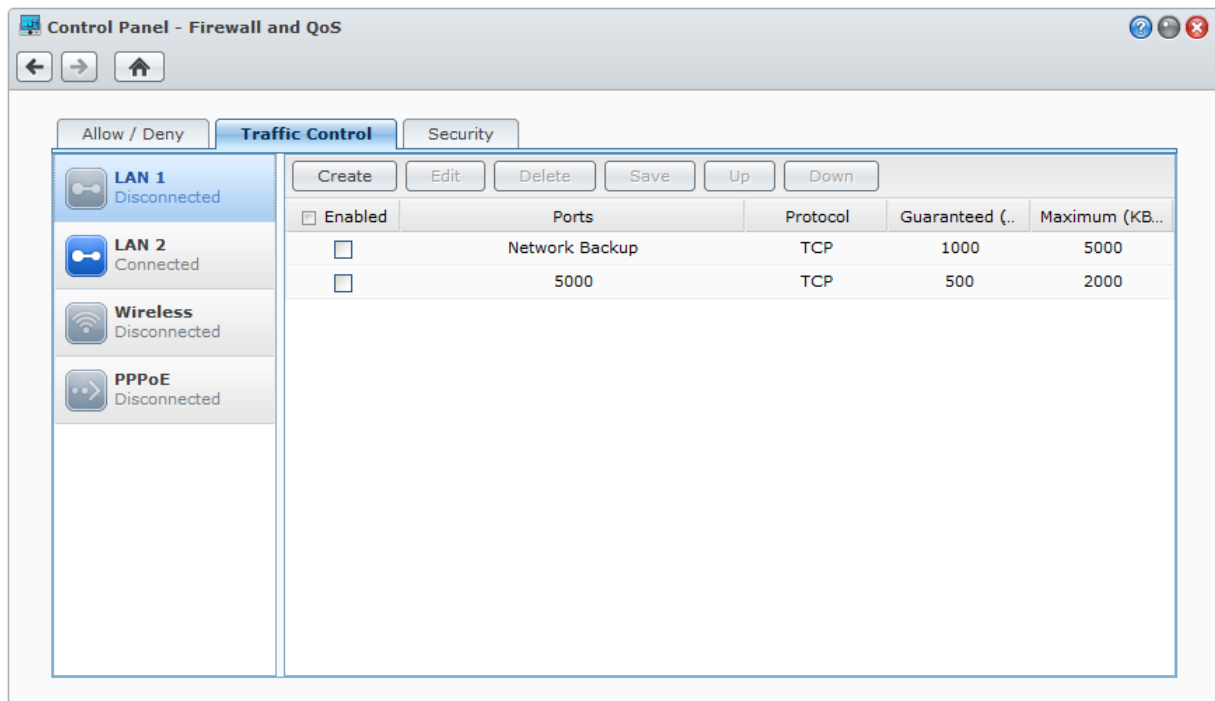
Apply Firewall Rules to Source IP Addresses

In the **Source IP** section, choose to allow or deny access from a source IP addresses using one of the following options:

- **All:** Choose this option to apply the rule to all source IP addresses.
- **Single host:** Choose this option to apply the rule to an IP address.
- **Subnet:** Choose this option to apply the rule to a subnet.

Control the Outgoing Traffic of Services

Traffic control aims to control the outgoing traffic of services running on 214. Go to **Main Menu > Control Panel > Firewall and QoS > Traffic Control**, and click **Create** to create traffic control rules.



Apply Traffic Control Rules to Ports

In the **Ports** section, apply firewall rules to all ports or selected ports using one of the following options:

- **All:** Choose this option to apply the rule to all ports on ioSafe 214.
- **Select from a list of built-in applications:** Tick the system services that will be included in the rule.
- **Custom:** Specify the type and protocol of the port, and enter the custom port number.

You can enter up to 15 ports separated with comma, or by specifying a port range.

Configure Bandwidth Settings

After selecting a service, you will need to set **Guaranteed Bandwidth** and **Maximum Bandwidth** to limit its outgoing traffic.

- **Guaranteed Bandwidth**

Defines the outgoing traffic a service guarantees to serve when the whole system bandwidth is wide enough.

- **Maximum Bandwidth**

Defines the outgoing traffic this service can borrowed when the whole system bandwidth is enough and there is **System Remaining Bandwidth**. It is suggested that the system manager calculate **System Output Bandwidth** first and then make sure the sum of **Guaranteed Bandwidth** for each service is not greater than **System Output Bandwidth**, or the setting may not work correctly.

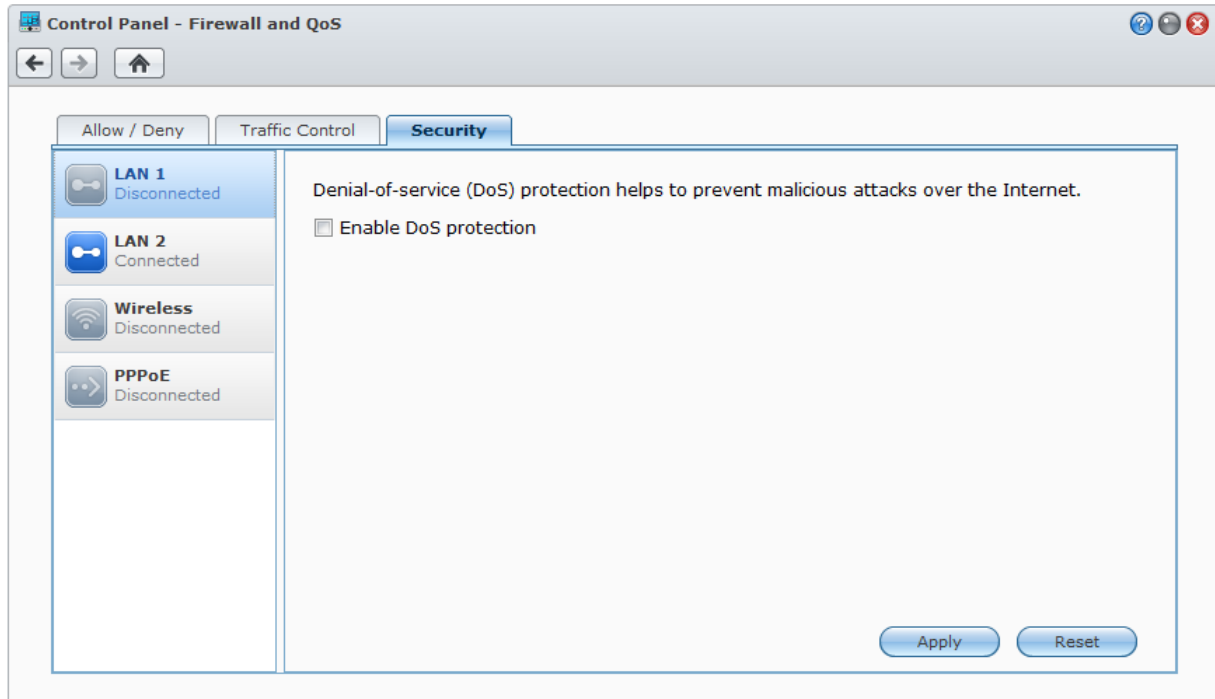
Setting Formula

System Output Bandwidth = Sum of **Guaranteed Bandwidth** of each service + **System Remaining Bandwidth**

Guaranteed Bandwidth for each service \leq **Maximum Bandwidth** for each service

Prevent Attacks over the Internet

Denial-of-service (DoS) protection helps to prevent malicious attacks over the Internet. Go to **Main Menu** > **Control Panel** > **Firewall and QoS** > **Security** to enable DoS protection and improve network security.



Automatically Block Suspicious Login Attempts

Auto block allows you to prevent unauthorized login. After enabling the service, an IP address will be blocked if it has too many failed login attempts. Go to **Main Menu > Control Panel > Auto Block** to create and manage your block list and allow list.

Control Panel - Auto Block

General Block List Allow List

Enable this option to block IP addresses with too many failed login attempts, including logins via SSH, Telnet, rsync, Network Backup, Shared Folder Sync, FTP, WebDAV, Synology mobile apps, File Station, and DSM.

☐ Enable auto block

An IP address will be blocked if it reaches the number of failed login attempts within the time period entered below.

Login attempts:

Within (minutes):

☐ Enable block expiration

When block expiration is enabled, blocked IP addresses will be unblocked after the number of days entered below.

Unblock after (days):

Apply Cancel

Set Up File Sharing

ioSafe 214 can become the file sharing center within the Intranet or over the Internet, allowing users to access its files anytime and anywhere. For more detailed instructions, please see [DSM Help](#).

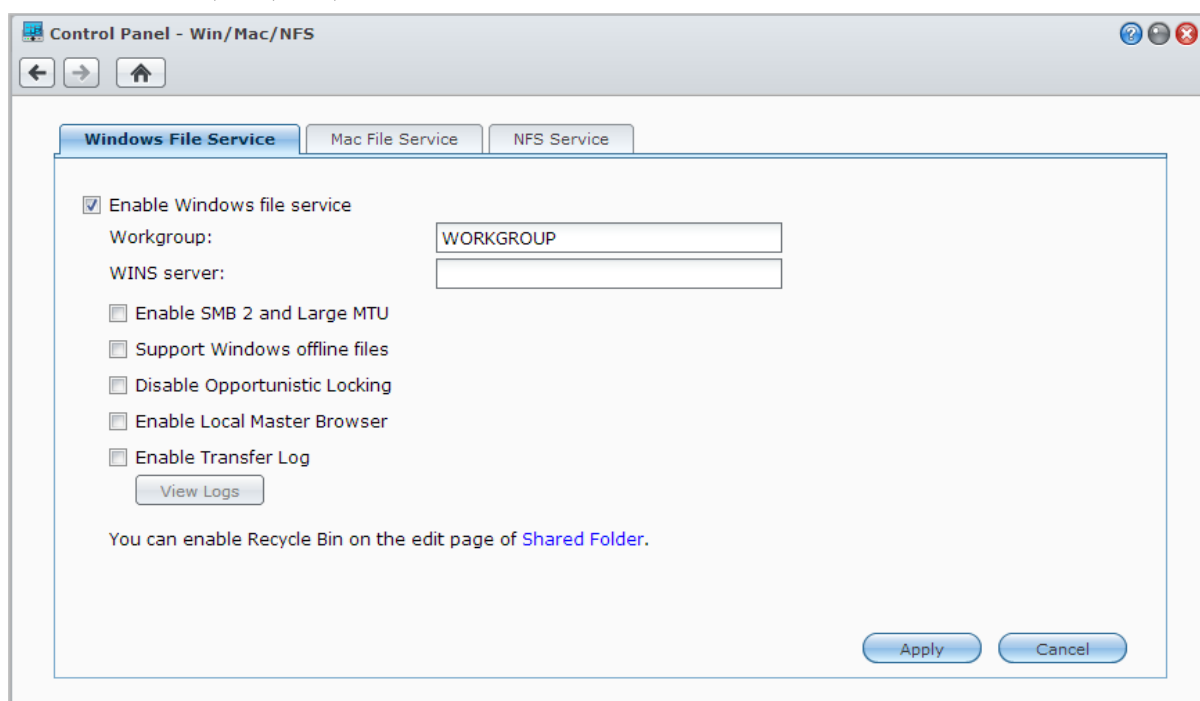
This chapter explains how to enable the support for file sharing protocols for all platforms, create and manage users and groups, set up shared folders, and allow or deny access to the shared folders, applications or subfolders from specific users or groups.

Enable File Sharing Protocols for All Platforms

This section tells you how to enable the ioSafe 214 to support file sharing protocols for all platforms.

ioSafe 214 supports the following file sharing protocols:

- **For Windows:** SMB/CIFS (My Network Places), FTP, WebDAV
- **For Mac:** SMB, FTP, AFP, WebDAV
- **For Linux:** SMB, FTP, NFS, WebDAV



Manage Windows File Service

Click the **Windows File Service** tab at **Main Menu > Control Panel > Win/Mac/NFS** to enable ioSafe 214 to be the Windows file server (CIFS server).

Manage Mac File Service

Click the **Mac File Service** tab at **Main Menu > Control Panel > Win/Mac/NFS** to make ioSafe 214 a Mac file server (AFP Server).

Tick **Enable Bonjour Printer Broadcast** to allow Mac clients to browse and locate the printer connected to the ioSafe 214.

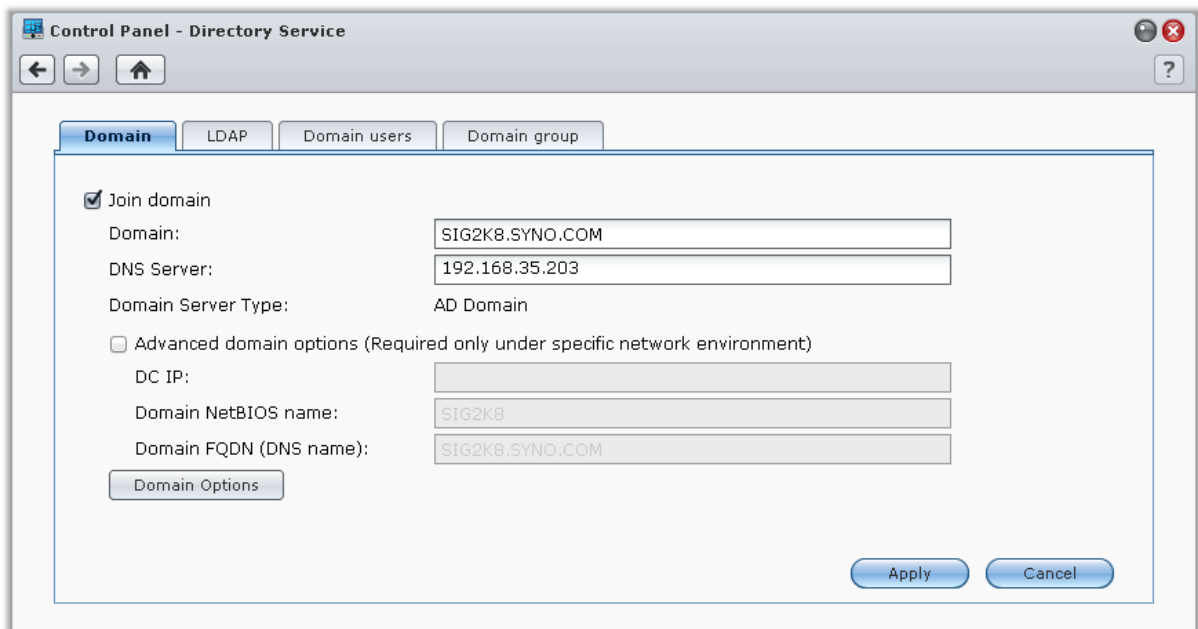
Enable NFS Service for Linux Clients

Click the **NFS Service** tab at **Main Menu** > **Control Panel** > **Win/Mac/NFS** to allow Linux client to access 214 data.

If you want to configure Linux client's NFS access privileges to the shared folders, see "Allow Users or Groups to Access Shared Folders" for more information.

Join 214 to Directory Service

Go to **Main Menu** > **Control Panel** > **Directory Service** to join your ioSafe 214 to a directory service as a Windows domain or LDAP client. When 214 is joined to a directory service, you can manage domain/LDAP users' access privileges to shared folders and DSM applications and enable their home service.



Joining a Windows Domain

Click the **Domain** tab, and enter domain name and DNS server (optional) to join the 214 to a Windows ADS domain. In the window that appears, enter the user name and password for the administrator of the domain server.

After the ioSafe 214 joins the domain, domain users can log in to 214 with their domain account and password.

Note:

- If your domain user name includes "%" and "\$", you might not be able to access your home folder. Please ask your domain administrator to give you a new user name.
- Domain groups **Domain Admins** and **Enterprise Admins** will be added to the local group **administrators** automatically. In other words, domain users in these groups have administrative right on the 214, including performing DSM/CIFS/FTP/AFP/WebDAV applications.
- You can also configure domain users' access privileges to the shared folders on ioSafe 214. See "Allow Domain Users or Groups to Access Shared Folders" for more information.

Binding to an LDAP Server

LDAP allows your 214 to join an existing directory service as an LDAP client, and then retrieve user or group information from an LDAP server (or "directory server"). You can manage LDAP users' or groups' access privileges to DSM applications and shared folders, just as you would with DSM local users or groups.

Host LDAP Service with Directory Server

Directory Server is an add-on package based on LDAP version 3 (RFC2251) that allows your 214 to become an account administration center to centralize the account management of all connecting clients, and provides authentication service for them.

To install Directory Server on your 214, go to **Main Menu > Package Center**. For more information about Directory Server, please refer to **DSM Help**. To learn more about how to access 214's Directory Server with a LDAP client, refer to the **Directory Server User's Guide** available at Synology's **Download Center**.

Manage Users and Groups

Go to **Main Menu > Control Panel > User** or **Group** to create users or groups, and allow or deny their access to different shared folders.

Name	Description	Email	Status
admin	System default user		Normal
chrislai			Normal
Darren			Normal
gmbh			Normal
guest	Guest		Disabled
Jocelyn	Test		Normal
mk1			Normal
mk2			Normal
nvrdemo			Normal
sac			Normal
calact1			Normal

Create Users

Click **Create** to create a user account. The user can log in to edit his/her account info after the user account has been established. You can also choose to set an account expiration date or disallow the user to change account password.

Creating User Accounts by Importing User List

Additionally, you can create multiple user accounts by importing a user list. Create a text file which contains the following tab-delimited information in each line:

- Username
- Password
- Description
- Email
- Quota (MB) in volume 1
- Quota (MB) in volume 2 (and so on)

Note:

- All fields are optional except **Username**.
 - An example of the text file is shown as follows:
- | | | | | |
|--------|------|---------|----------------|-------|
| eddy | 1234 | father | eddy@abc.com | 80000 |
| rosy | 5678 | mother | rosy@abc.com | 80000 |
| chaddy | 8901 | brother | chaddy@abc.com | 20000 |
| eric | 2345 | cousin | eric@abc.com | 20000 |

Save the text file in UTF-8 encoding. Go to **Main Menu > Control Panel > User** and choose **Create > Import Users**.

Apply Password Strength Rules

You can enable password strength service to make sure DSM users' passwords are secure enough to withstand malicious login attempts. Click **Password Strength** to configure this measure of the effectiveness of a password.

Note:

- Password Strength rules only work for passwords created or modified after the Password Strength service is enabled. Existing passwords won't be affected by the rules.
- The rules won't apply to the passwords of users created by importing user list.

Create User's Home Folder

Each DSM user (except for guest) can have his/her own folder called the **home** folder, which is accessible only by the user and the system administrator. Click **User Home** to enable user home service.

For users belonging to the **administrators** group, DSM users' home folders are here: **homes/[Username]**

Note:

- When the user home service is disabled, the **homes** folder will be kept but accessible by users belonging to the **administrators** group only. Users can access their home folders again if the user home service is enabled again.
- To delete the **homes** folder, the user home service must be disabled first.

Create Domain/LDAP User's Home Folder

If you have joined your 214 to a directory service as a Windows domain or LDAP client, you can go to **Main Menu > Control Panel > Directory Service > Domain users** or **LDAP user** to create domain/LDAP users' home folder. Click **User Home** and tick **Enable home service for domain users** or **Enable home service for LDAP users**.

Like local users, all domain/LDAP users can access their own home folder via CIFS, AFP, FTP, WebDAV, or File Station. Users belonging to the **administrators** group can access all personal folders located in the **homes** default shared folder. For users belonging to the **administrators** group, domain/LDAP users' home folders are in the folder named **@DH-domain name** (for domain users) or **@LH-FQDN name** (for LDAP users). The name of the user's home folder is the user account plus a unique number.

Note:

- To delete the **homes** shared folder, user home service must be disabled first.
- Enabling domain/LDAP user home service will also enable the local user home service if it's not enabled yet.
- The domain user home service would be disabled if the local user home service is disabled.

Create Groups

Go to **Main Menu > Control Panel > Group** to create and edit a group, add users to the group, and then edit the group's properties, saving you the trouble of editing users one by one.

Groups created by default include the following:

- **administrators:** Users belonging to the **administrators** group have the same administrative privilege as **admin**.
- **users:** All users belong to the **users** group.

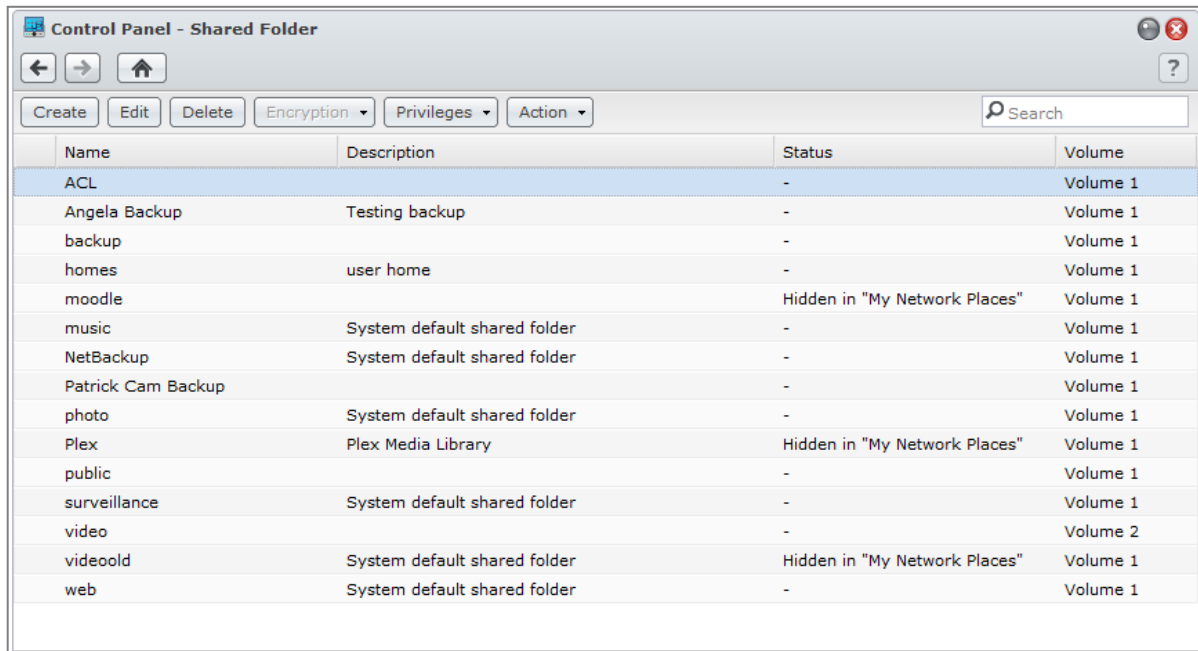
Note: For more information about editing a group's access privileges to shared folders or applications, see "Allow Users or Groups to Access Shared Folders" and "Allow Users to Access Applications" for more information.

Allow Users to Access Applications

Go to **Main Menu > Control Panel > Application Privileges** to decide which applications could be accessed by a user.

Set Up Shared Folders

Go to **Main Menu > Control Panel > Shared Folder** to manage the shared folders, which are the root folders of ioSafe 214. (Folders within the shared folders are called **subfolders**.) You can store data in the shared folders and share them with users or groups with access privileges.



Built-in Shared Folders Created by the System

System built-in shared folders are created when the services or applications requiring the folders are enabled.

Name	Description
public	The public folder will be created automatically after the first time you set up ioSafe 214.
web	The web folder contains contents of your website. It will be created automatically when Web Station is enabled. For more information about Web Station, see "Use Web Station to Host Websites".
photo	The photo folder contains photos and videos you want to share on Photo Station. It will be created automatically when Photo Station or DLNA/UPnP Media Server is enabled. For more information about Photo Station and Media Server, see "Chapter 12: Share Photos, Videos, and Blogs with Photo Station" and "Manage DLNA Media Server".
music	The music folder contains music you want to share on Audio Station. It will be created automatically when Audio Station is enabled. For more information about Audio Station, see "Chapter 13: Play Music with Audio Station".
video	The video folder contains videos you want to browse through DLNA/UPnP DMA. It will be created automatically when Media Server is enabled. For more information about Media Server, see "Manage DLNA Media Server".
surveillance	The surveillance folder contains Surveillance Station recordings. It will be created automatically when Surveillance Station is enabled. It is read-only and can only be accessed by the system administrator. For more information about Surveillance Station, see "Chapter 16: Safeguard Your Environment with Surveillance Station".
home	The home folder provides a private space for each user to store data where only the user can access. It will be created automatically when User Home is enabled. For more information about User Home, see "Create User's Home Folder".
homes	The homes folder contains the home folders of all users. It will be created automatically when User Home is enabled. Only system administrator can access and manage all users' home folders. For more information about User Home, see "Create User's Home Folder".
NetBackup	The NetBackup folder is created automatically when Network Backup Service is enabled. For more information about network backup, see "Network Backup".

Name	Description
usbshare	The usbshare[number] folder is created automatically when you connect an USB disk to ioSafe 214's USB port. For more information about external USB disks, see "Manage External Disks".

Create a Shared Folder

If you are a user belonging to the **administrators** group, you can click **Create** to create shared folders and assign access privileges to the folders.

Remove a Shared Folder

If you are a user belonging to the **administrators** group, you can click **Delete** to remove any shared folder created by yourself.

Important: Removing any shared folder also removes all data within it. If you still need the data, back them up first.

Allow Users or Groups to Access Shared Folders

Go to **Main Menu > Control Panel > Shared Folder**, click **Privileges** and choose **Privileges Setup** to allow or deny users' or groups' access to the shared folders.

Note:

- To set the access privileges to subfolders, you can use File Station. See "Edit the Properties of Files and Subfolders" for more information.
- When you encounter privilege conflicts, the privilege priority is as follows: **No access > Read/Write > Read only**.
- When you create a new shared folder, if the access privilege of users belonging to the **administrators** group to the folder is set as **No access**, then users belonging to the **administrators** group will only be able to see the folder by going to **Main Menu > Control Panel > Shared Folder**.

Allow Linux Clients to Access Shared Folders

Select a shared folder from the shared folder list, click **Privileges** and choose **NFS Privileges** to assign NFS privileges.

Term Explanation

Asynchronous: NFS servers will reply to requests before the changes on the file are completed.

Allow Domain Users or Groups to Access Shared Folders

If you have joined your 214 to a directory service as a Windows domain or LDAP client, you can go to **Main Menu > Control Panel > Directory Service > LDAP User, LDAP Group, Domain users**, or **Domain Group** to set up and modify the shared folder privileges of a domain/LDAP user or group.

Note: In the event of privilege conflicts, the privilege priority will be: No access (NA) > Read/Write (RW) > Read only (RO).

Encrypt a Shared Folder

Go to **Main Menu > Control Panel > Shared Folder** and click **Edit** to encrypt your shared folder. After a folder is encrypted, you can use the **Encryption** drop-down menu to edit the folder.

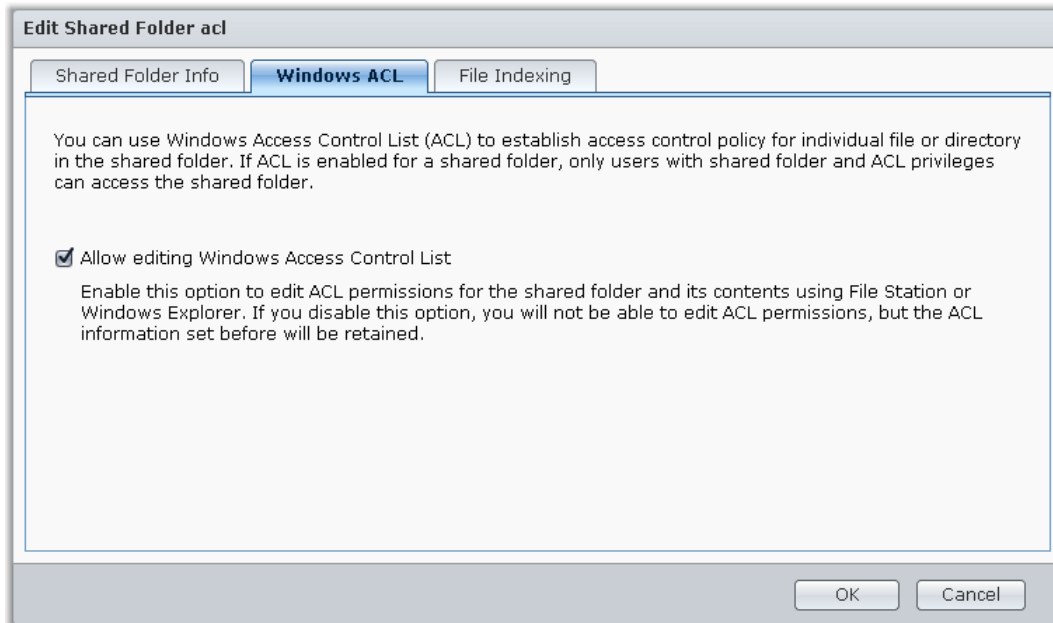
The AES 256-bit encryption can block off all unauthorized access attempts. Without the encryption key, other people will not be able to use the encrypted data even if they remove the hard drives from your ioSafe 214 and mount it on their device.

Note: Tick **Mount automatically on startup** to mount the encrypted folder automatically after the ioSafe 214 starts up next time. By default, encrypted shared folder will be unmounted automatically on startup for security reasons.

Define Windows ACL Privileges for Shared Folder

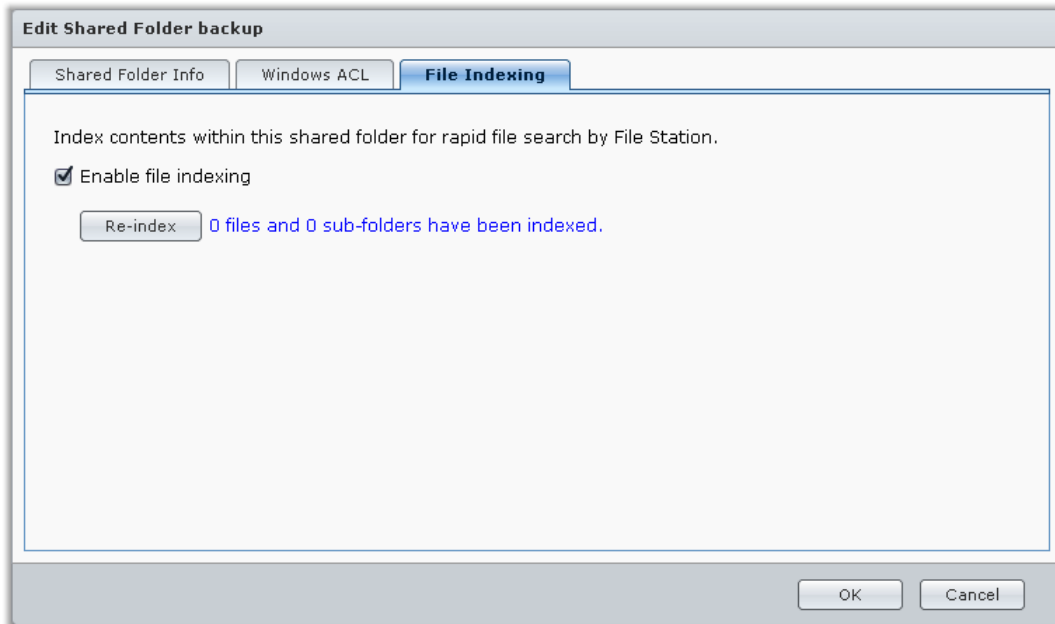
Go to **Main Menu > Control Panel > Shared Folder** to define ACL privileges for a shared folder. Windows Access Control List (ACL) is a list of privileges or permissions that determine specific access rights under the Windows environment. This can help administrator define access control rules for an individual file or a directory, and give different access rights for individual user or group.

Through Windows ACL, you can assign different privileges to local and domain users in the system. The privileges apply to all file-related applications, such as FTP, File Station, NFS, AFP, WebDAV, etc.



Index Shared Folder Contents

Indexing the contents of a shared folder can help you find files or folders more quickly during file search.



Note: See "Search for Files or Folders" for more information about searching files with File Station.

Access Files from Anywhere

When you have set up users or groups with proper access privileges to the shared folders, they can share their files with your ioSafe 214 from anywhere.

This chapter explains the ways to access the ioSafe 214 shared folders within the Intranet or over the Internet. For more detailed instructions, please see [DSM Help](#).

Access Files within the Intranet

This section explains how to allow users to use Windows, Mac, or Linux computer to access shared folders on ioSafe 214 within the Intranet.

Note: Before accessing, make sure the relative file sharing protocols have been enabled for your ioSafe 214. See "Enable File Sharing Protocols for All Platforms" for more information.

Access Shared Folders from Windows

To access shared folders from Windows, you can use any of the following methods.

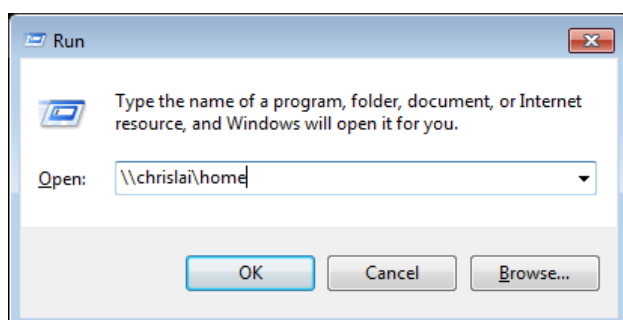
Method 1: Use Synology Assistant to map the shared folders as network drives.

Run Synology Assistant and select the server from the server list. Click **Map Drive** and follow the onscreen steps to finish the setup.

Upon completion, you can access the mapped shared folder directly in Windows Explorer.

Method 2: Use the Run window.

Press Windows-R to open the **Run** window. Enter `\\ioSafe_Server_Name\\Shared_Folder_Name` in the **Open** field.



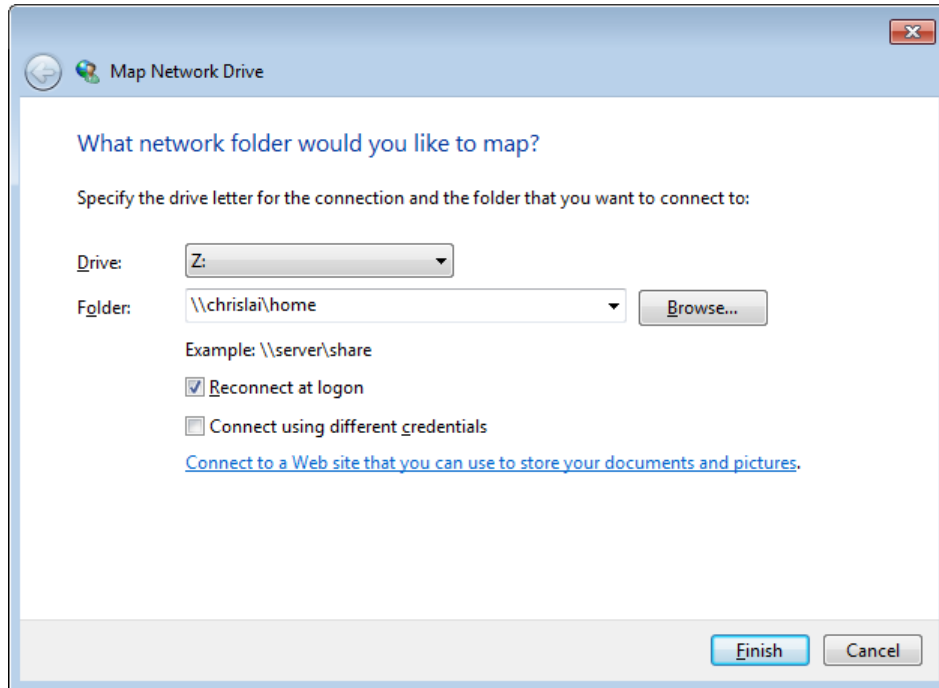
Method 3: Use Windows Explorer.

Open a Windows Explorer window and choose **Tools > Map network drive** to show the **Map Network Drive** window. Choose a drive number from the **Drive** drop-down menu.

Locate the shared folder by doing one of the following:

- Enter **\\ioSafe_Server_Name\Shared_Folder_Name** in the **Folder** field.
- Click **Browse** to locate the shared folder, and then click **OK**.

Enter your user name and password for ioSafe 214 and click **OK**. Upon completion, you can access the mapped shared folder directly in Windows Explorer.

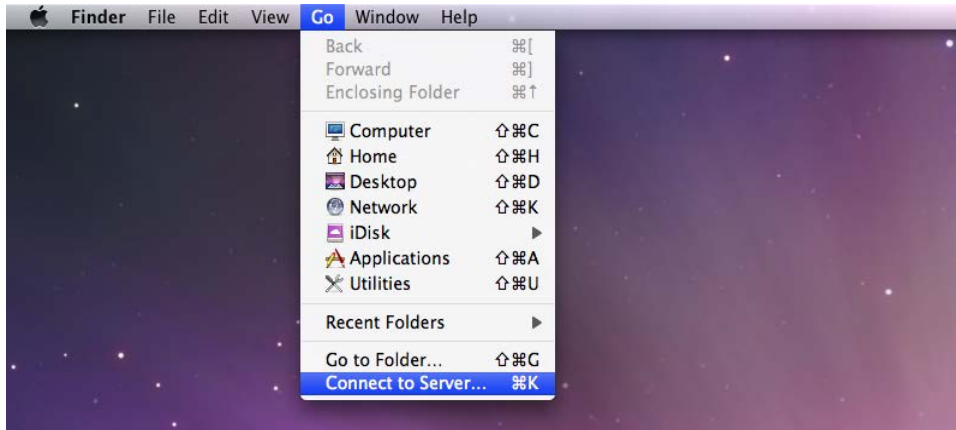


Access Shared Folders from Mac

Choose **Go > Connect to Server** from the menu bar. Type ioSafe 214's IP address or server name (appended with **.local**) preceded by **smb://** or **afp://** in the **Server Address** field and click **Connect**. (e.g. **smb://EricaWang.local** or **afp://192.168.0.2**)

Note: For better performance, it is recommended that you connect to the shared folders via SMB.

Select the shared folder you want to access. Upon completion, you can access the shared folder in the Finder window.



Access Shared Folders from Linux

In DiskStation Manager, Go to **Main Menu > Control Panel > Shared Folder**. Select the shared folder you want to access, click **NFS Privileges**, and find the mount path at the bottom of the window that appears.

On a Linux computer, enter the mount path to mount the shared folders.

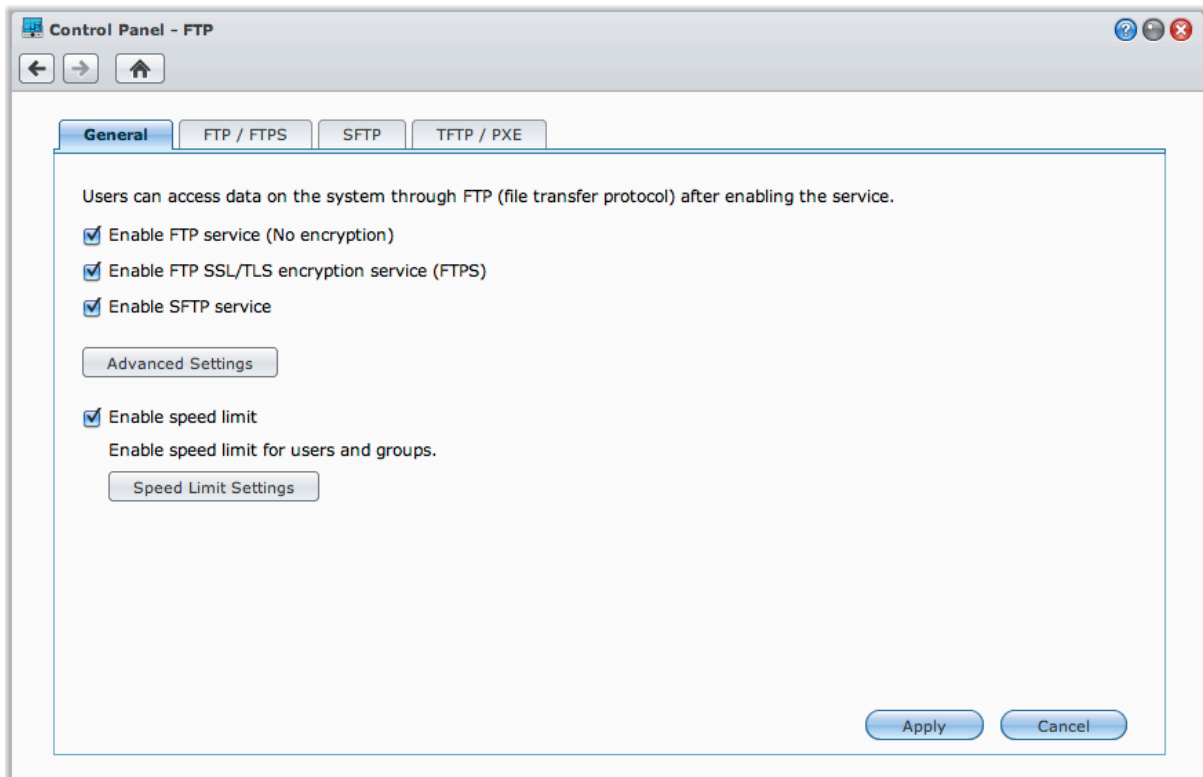
Note: For more information about NFS Privileges, see "Allow Users or Groups to Access Shared Folders".

Access Files via FTP

If your ioSafe 214 is accessible over the Internet, you can use a FTP application to access the shared folders.

Note: For more information about making ioSafe 214 accessible over the Internet, see "Chapter 5: Access your 214 from the Internet".

Go to **Main Menu > Control Panel > FTP** to enable FTP service, allowing users to upload or download ioSafe 214 data via FTP.



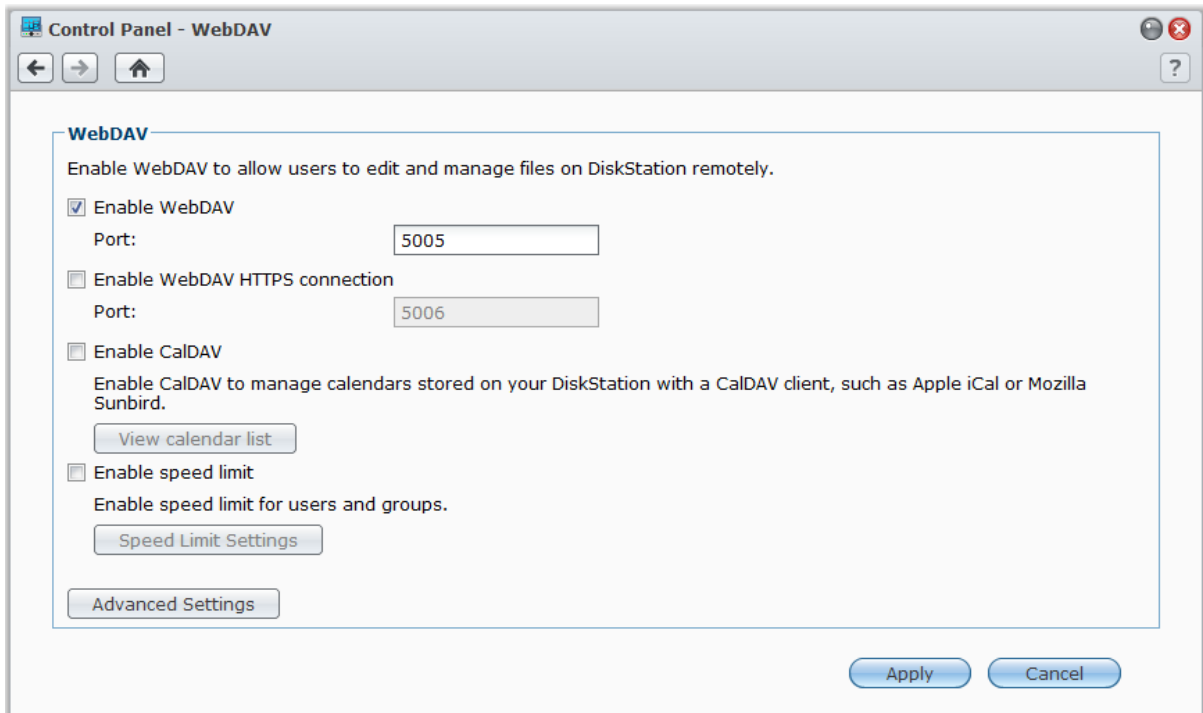
Connect to ioSafe 214 Using a FTP Application

Open any FTP application on your computer and enter the following information to connect to ioSafe 214:

- ioSafe 214's IP address or domain name
- Your user account and password
- The port number (The default number is 21)

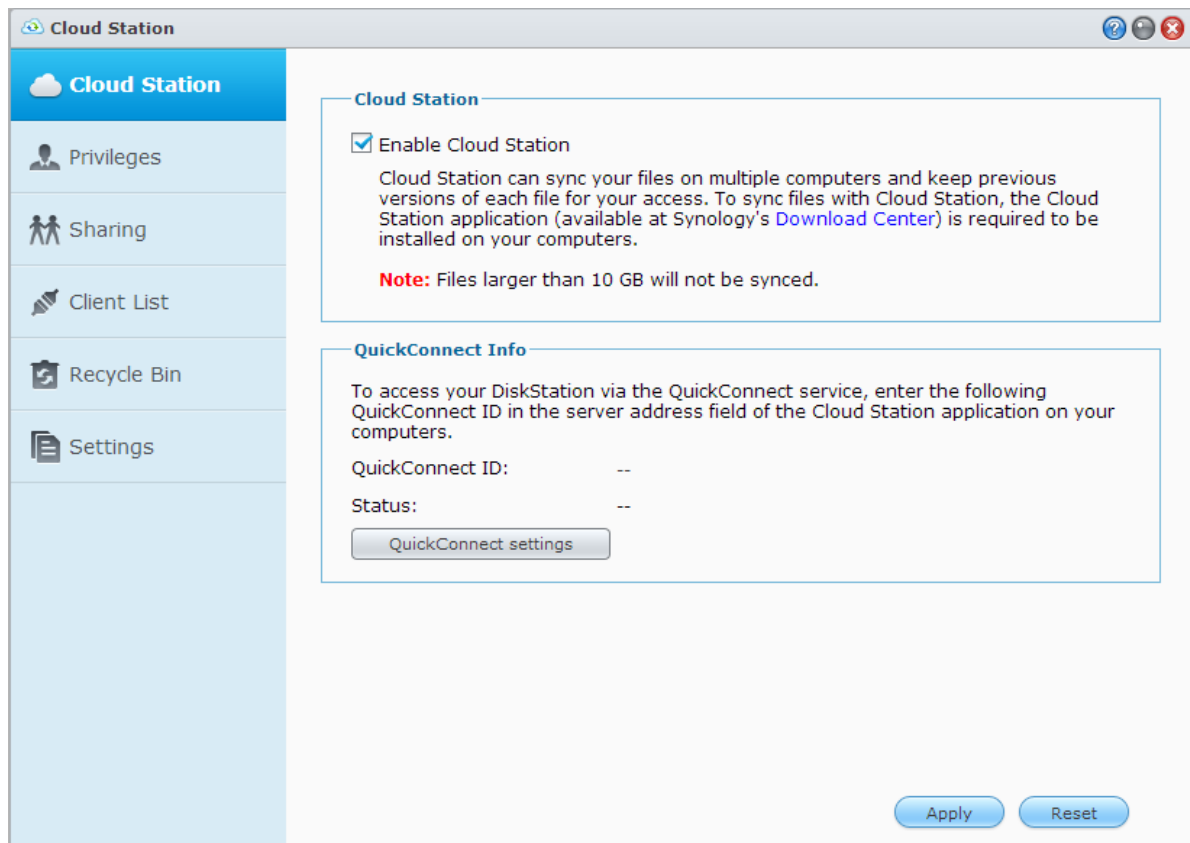
Access Files via WebDAV

By enabling WebDAV or CalDAV (at **Main Menu > Control Panel > WebDAV**), you can remotely manage and edit files or calendars stored on the 214.



Sync Files via Cloud Station

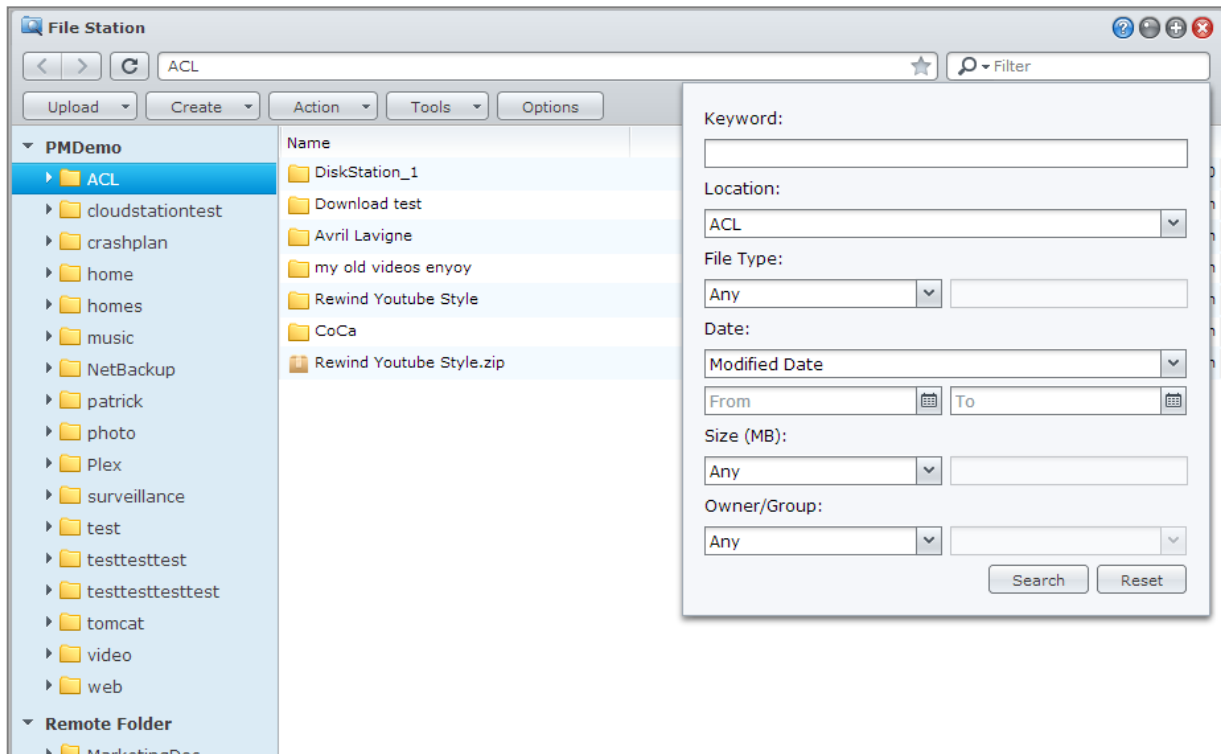
Cloud Station is a file sharing service that allows your 214 to become a file sync center to sync files between multiple client computers. Go to **Main Menu > Package Center** to install and run the Cloud Station package.



Note: A client application (Cloud Station for computer clients, available at Synology's [Download Center](#)) is required to be installed on client computers before syncing files with 214.

Search for Files or Folders

You can type keywords in the **Filter** field at the top-right corner of File Station to filter through files or folders in the current folder. Additionally, you can also perform advanced search in the **Advanced Search** panel for more refined search results.



Note: For quicker search result, it is recommended that you index shared folder contents. See "Index Shared Folder Contents" for more information.

Set File Station in Action

With the **Action** menu, right-clicking, and dragging-and-dropping, you can easily download, upload, copy, move, rename, delete, extract, and compress files or folders, and more.

Edit the Properties of Files and Subfolders

You can edit the access privileges to files and subfolders (meaning folders and their subfolders in a shared folder), copy download links and open file in a new browser window in the **Properties** window. Select the files and folders for which you want to set access privileges. Right-click one of the files or folders, or choose the **Action** menu, and then choose **Properties**.

Note:

- To set access privileges to shared folders, please see "Allow Users or Groups to Access Shared Folders" for more information.
- You are not allowed to edit the access privileges to files and subfolders in the **photo** shared folder here. To set access privileges to photo albums for Photo Station users, open Photo Station, go to the **Settings** page, and click the **Help** tab for more information.
- With File Station, you can only perform the upload action for files and folders on your computer. All the other File Station actions and properties setting are available for files and folders on the ioSafe 214 only.

Share File Links

With File Station, you can generate URLs for 214 files, which could be used by people without DSM user credentials to download the shared files. For more information, click the **Help** button (with a question mark) at the top-right corner, and then go to **File Station > Share File Links**.

Mount Remote Folders or Virtual Drives

File Station allows you to mount remote folders to access contents shared by network computers or other 214s, or virtual drives to access contents within disc images. That way, you can easily navigate all available network resources or disc images with File Station. For more information about remote folders or virtual drives, click the **Help** button (with a question mark) at the top-right corner, and then go to **File Station > Mount Remote Folders** or **Mount Virtual Drives**.

Edit Music Information

With File Station's Music Information Editor, you can view or edit the information of music files. Simply right-click the music files and choose **Edit music information**.

View Documents, Photos, or Videos

With File Station, you can view documents, videos or photos. For more information, click the **Help** button (with a question mark) at the top-right corner, and then go to **File Station > Read and Move Files > View Documents, Photos, or Videos**.

Edit Photos

With File Station, you can edit photos with web-based editors, such as Pixlr Editor or Pixlr Express. For more information, click the **Help** button (with a question mark) at the top-right corner, and then go to **File Station > Read and Move Files > Edit Photos**.

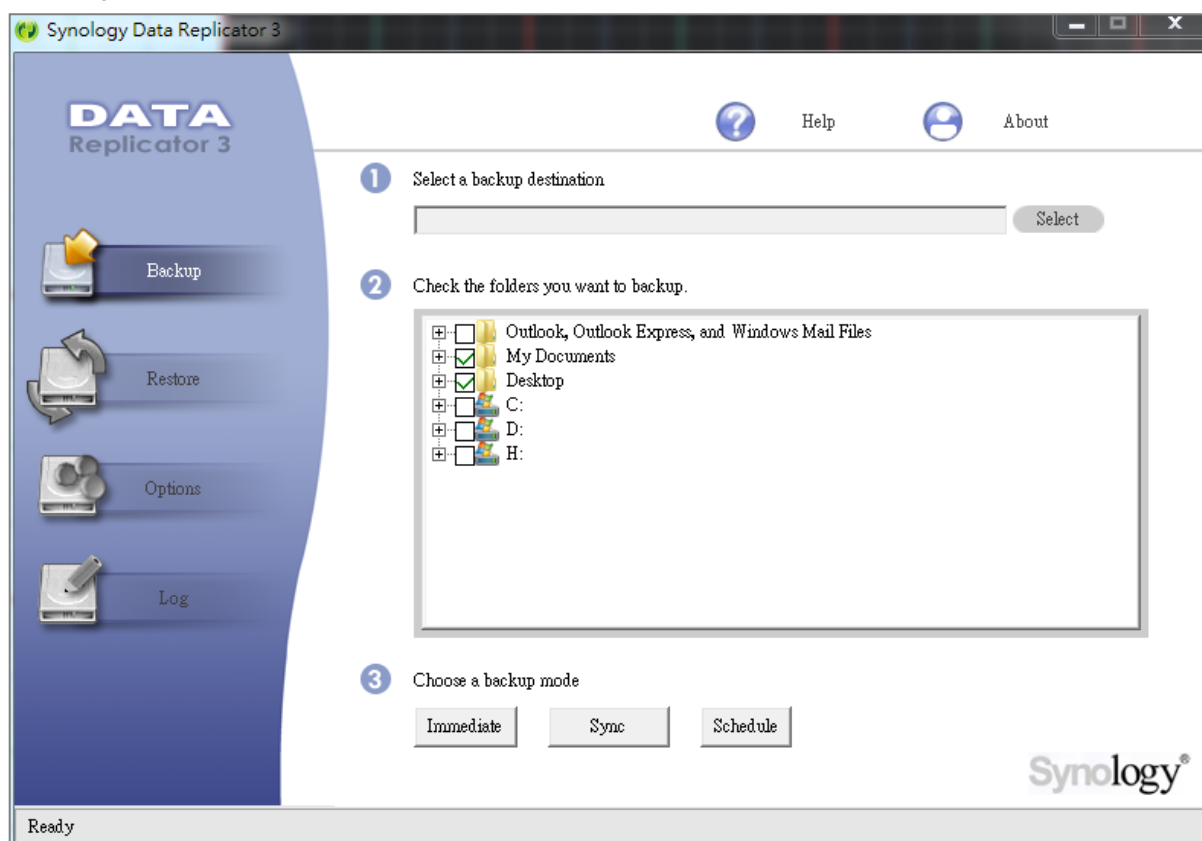
Back Up Data

ioSafe offers comprehensive backup solutions for your computer and ioSafe 214, allowing you to back up data on your computer to ioSafe 214. If you are a user belonging to the **administrators** group, you can also back up 214 data with local or network backup, or sync shared folder contents between 214s. The creative Copy button simplifies external storage devices backup with One-touch design. The support for the Amazon S3 backup service and the innovative Time Backup package give you other choices for server backup.

This chapter explains how the various backup solutions of DSM can help protect your data. For more detailed instructions, please see [DSM Help](#).

Back Up Computer Data

Synology-designed Data Replicator 3 allows you to back up data from a Windows computer to ioSafe 214. If you are using a Mac or Linux, ioSafe 214 can also serve as their backup destination.



Use Data Replicator for Windows

The Synology Data Replicator installation package can be found on the Installation disc and Synology's Download Center at: <http://www.synology.com/support/download.php>

What Can Data Replicator Do?

- Monitor specific folders on your Windows computer and perform real-time backup when any modification to the contents within a monitored folder is made.
- Adjust backup versions and restore points.
- Restore backup data from ioSafe 214 to your Windows computer according to your preference.

Important:

- Your computer and ioSafe 214 should use the same encoding. See "Language" for more information.
- Synology Data Replicator 3 is the next generation of Synology Data Replicator. It can only restore the data on ioSafe 214 that was backed up after Data Replicator 3 was installed. If users have backed up data on ioSafe 214 using Synology Data Replicator, we recommend restoring data on ioSafe 214 to PC first before using Synology Data Replicator 3.

Data Replicator Requirement:

- **Free HDD Space:** 5MB
- **Operating System:** Windows 2000 or later
- **Best Screen Resolution:** 1024 x 768 or above
- **Network Environment:** Microsoft Networking over TCP/IP enabled and has network connection with ioSafe 214

To install Data Replicator:

- 1 Insert the Installation disc into the optical drive of your computer.
- 2 Click **Data Replicator 3**, and follow the onscreen instructions to finish installation.

To use Data Replicator:

For detailed instructions on how to use Data Replicator, see its Help by clicking the **Help** button.

Use Time Machine for Mac

ioSafe 214 provides compatibility for backup with Apple Time Machine. Mac users can back up their data to ioSafe 214's shared folder without problem. Go to **Main Menu > Control Panel > Win/Mac/NFS**, tick **Enable Mac file service**, and choose a shared folder from the **Time Machine** drop-down menu. The chosen shared folder will become Time Machine's backup destination

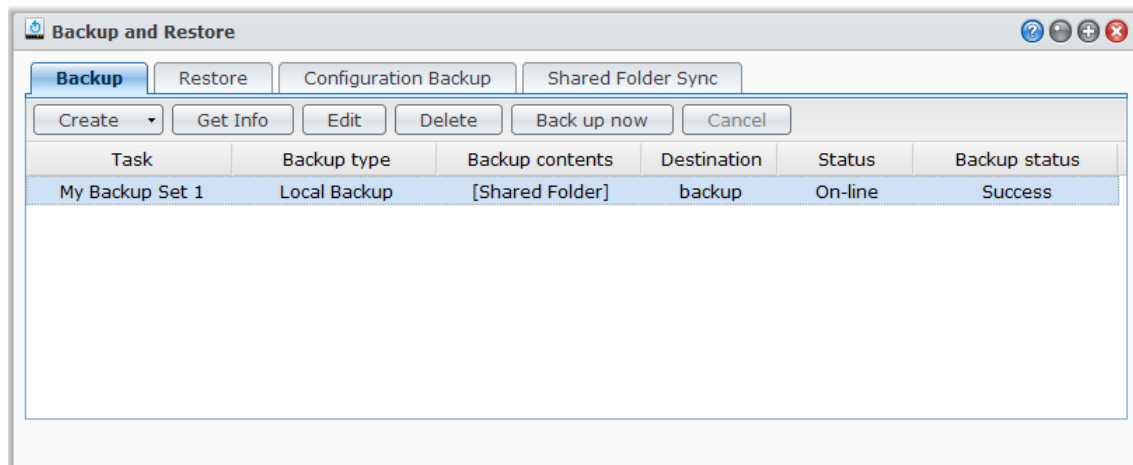
Note: For more information about using Time Machine, see the help on your Mac computer.

Use rsync for Linux

You can use rsync to back up Linux data to ioSafe 214.

Back up Data or iSCSI LUN on the ioSafe 214

Other than backing up computer data to ioSafe 214, users belonging to the **administrators** group can back up data or iSCSI LUN on the 214.



Ways to Back Up ioSafe 214 Data

Local Backup and Network Backup are ways you can choose to back up data or iSCSI LUN on your ioSafe 214. Plus, ioSafe 214 also supports Amazon S3 Backup, allowing you to back up data to the Amazon S3 Server. Go to **Main Menu > Backup and Restore > Create** to take advantage of the below backup methods. For more detailed instructions, please see **DSM Help**.

Local Backup

Local Backup allows backing up data from the ioSafe 214 to a system shared folder or an external disk via USB interface. The backups will be saved in a sub-folder named "LocalBackup" under the destination shared folder.

Note: You may need to format the external disk before performing Local Backup to the disk for the first time.

Network Backup

Network Backup allows backing up data from the ioSafe 214 to another ioSafe server or an rsync-compatible server. There are two modes available for Network Backup: **non-encrypted** and **encrypted**. Encrypted mode provides better security, while non-encrypted mode provides better performance. To ensure backup efficiency, it is recommended that you choose encrypted backup for important files.

Note: For more information about enabling Network Backup Service to set up your 214 as a backup destination, go to **Main Menu > Control Panel > Network Backup**, and click the **Help** button (with a question mark) at the top-right corner.

Amazon S3 Backup

Amazon S3 Backup allows backing up data from the ioSafe 214 to an Amazon S3 server. After you perform an Amazon S3 Backup task, a single backup file will be stored in a **Bucket** on Amazon S3 Server, which is identified by a unique **Set KEY Value** that begins with **SourceServerName_MAC address**, and ends with the complete file path of this file.

With Amazon S3 Backup, backing up to Amazon S3 RRS (Reduced Redundancy Storage) is also supported.

Note:

- There are also encrypted and non-encrypted modes for Amazon S3 Backup.
- Fees may apply to use the Amazon S3 Backup service.
- For more information about backing up 214 data, go to **Main Menu > Backup and Restore** and click the **Help** button (with a question mark) at the top-right corner.

Perform Backup Tasks on the ioSafe 214

Go to **Main Menu > Backup and Restore** to perform backup tasks on ioSafe 214.

Before you start, do the following:

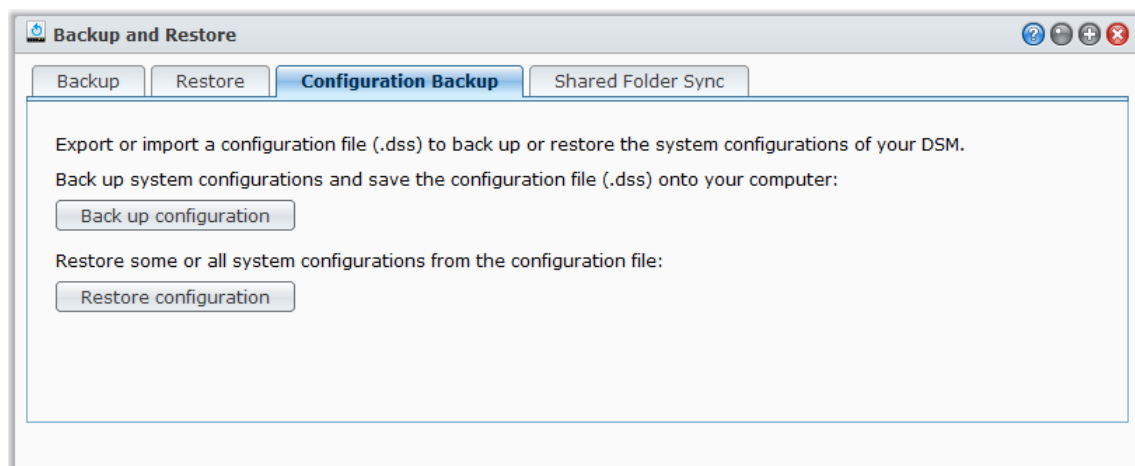
- **For Network Backup to another ioSafe 214:** Log in to the DSM of the target ioSafe 214, and then go to **Main Menu > Control Panel > Network Backup > Network Backup**. Make sure **Enable network backup service** is ticked and **Use customized rsync configuration** is deselected to make the target 214 available for backup.
- **For Local Backup to external disks:** Go to **Main Menu > Control Panel > External Devices** and click **Format** to format the external disk.

To perform data or LUN backup or restoration:

For detailed instructions, click the **Help** button at the top-right corner, and then go to **Backup and Restore > Backup**.

Backup and Restore System Configurations

Go to **Main Menu > Backup and Restore > Configuration Backup** to back up and restore the system configurations of your ioSafe 214. You can back up system configurations to a configuration file (.dss) and then restore the configurations at a later time.



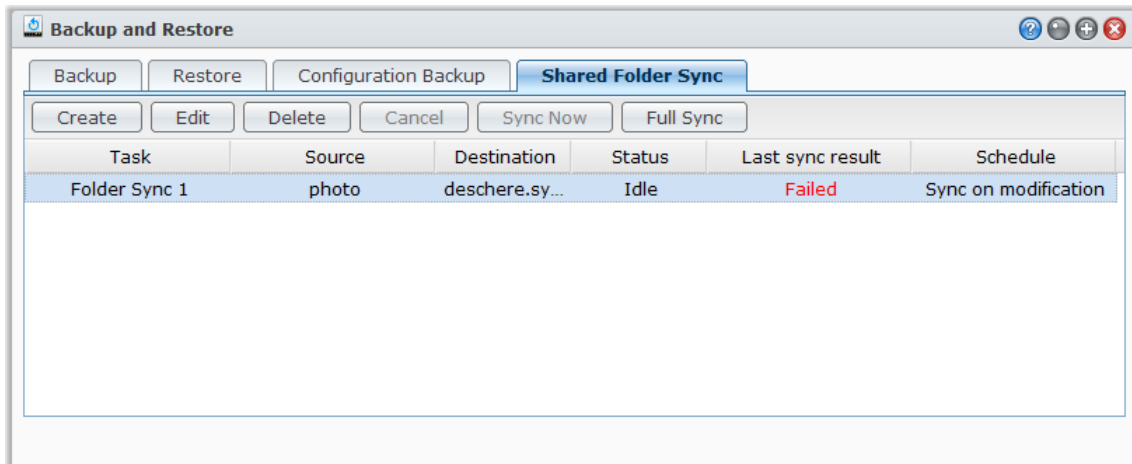
More Information

The configurations that will be backed up include the following:

- Users, Groups, and Shared Folders
- Workgroup, Domain, and LDAP
- File Sharing Services (such as Windows File Service, Mac File Service, NFS Service, FTP, and WebDAV),
- Web Services
- Network Backup Services (such as Network Backup (or Rsync) Service, Shared Folder Sync Service, and Time Backup Service)
- Other Services (such as User Home and Password Strength)

Sync Shared Folder Contents between 214's

Shared Folder Sync allows you to sync shared folder contents from a source 214 (or "client") to a destination 214 (or "server") over the network. Shared Folder Sync backup tasks can be viewed and managed by going to **Main Menu > Backup and Restore > Shared Folder Sync**. For detailed instructions regarding how to enable Shared Folder Sync, please see **DSM Help**.

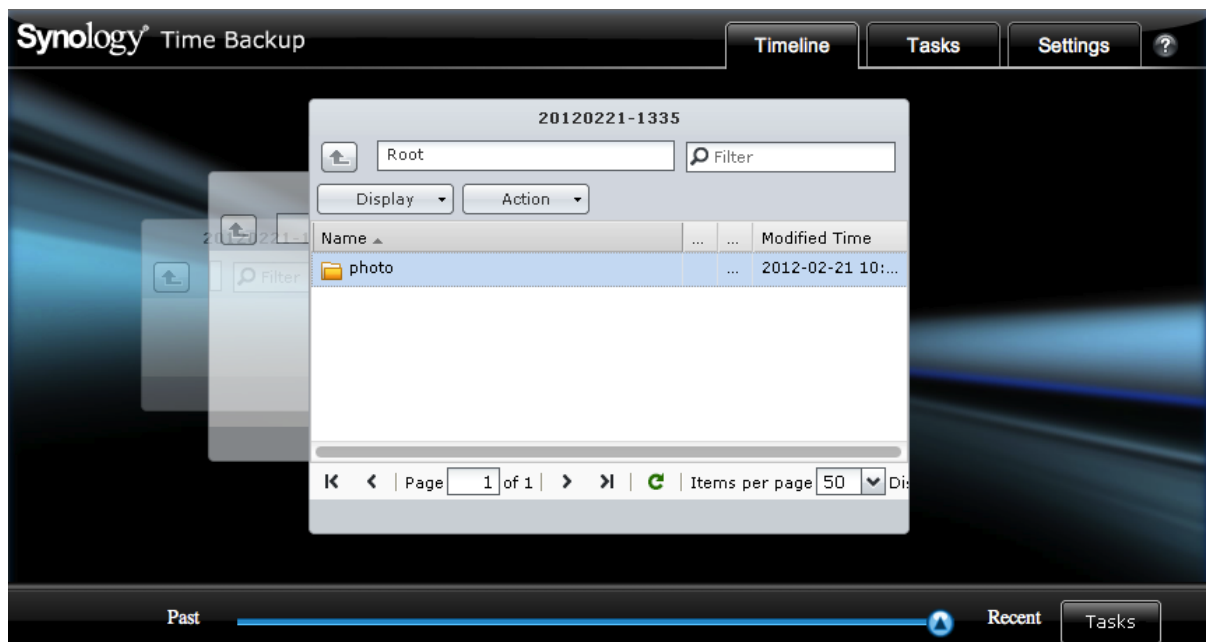


Backup 214 Data with Time Backup

Synology Time Backup is a quick and flexible way to back up and restore shared folders on 214. You can back up the data locally onto another volume, or onto an external hard disk. You can set up multiple **tasks** and create more than one **version** for each task.

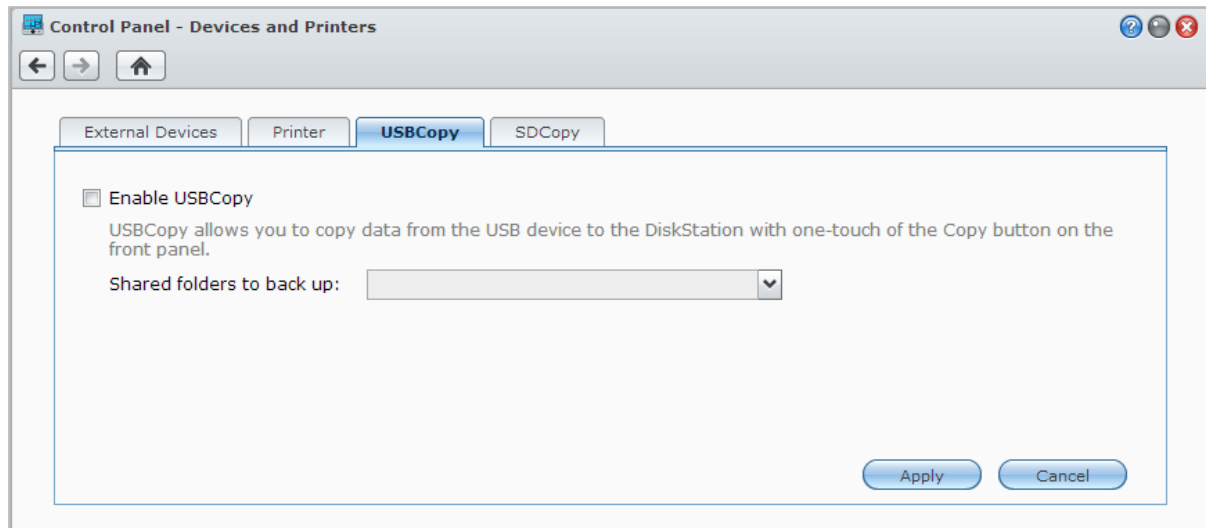
Time Backup features snapshot function. When creating a version, the system will take a **snapshot** and capture the condition of the data within the specified moment. The system will create a version entry within seconds. You can access the newly created version and edit the files you've just backed up with no time delay.

Time Backup can be installed by going to **Main Menu > Package Center**.



Backup Data on USB Device

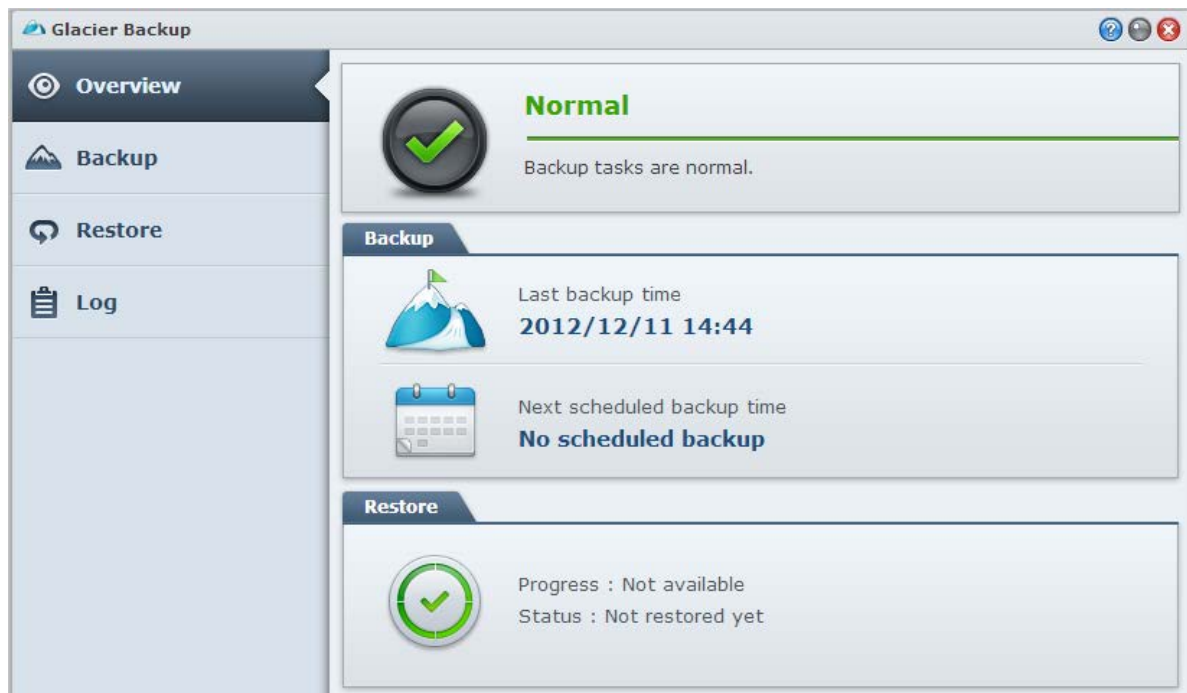
You can go to **Main Menu > Control Panel > Devices and Printers** to specify a shared folder for use with USBCopy, and then use the **Copy** button on the front panel of your 214 to copy data from a USB device to the shared folder.



Backup Data to Amazon Glacier

Synology's Glacier Backup is a backup management tool which facilitates backing up data on the 214 to Amazon Glacier, a cloud storage service which provides secure and durable data storage at extremely low costs. By backing up files to your Amazon Glacier account, Glacier Backup helps save space on your 214 and provides a contingency plan to avoid data loss.

Glacier Backup can be installed by going to **Main Menu > Package Center**. For more detailed instructions regarding Glacier Backup, please see **DSM Help**.

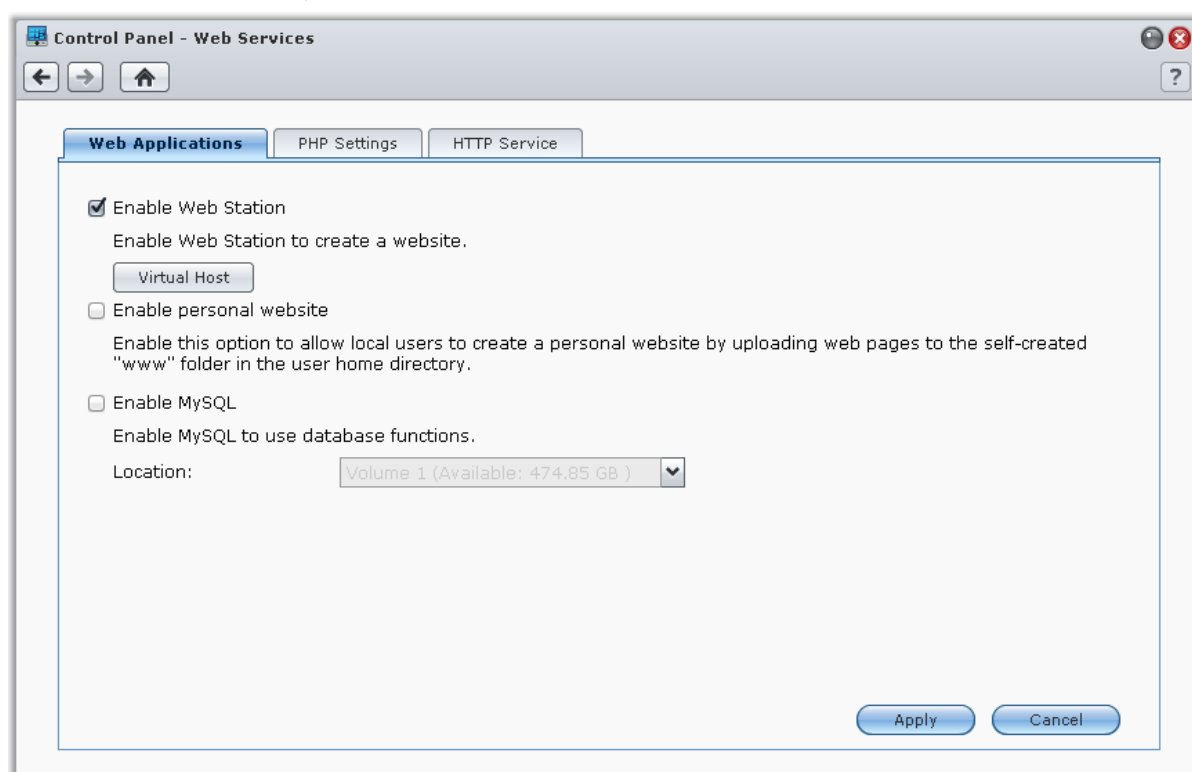


Host Websites, Email Server, and Print Server

ioSafe 214 is designed for small and medium businesses (SMB), providing the ability to set up web, email, and print servers on a single ioSafe 214 without spending extra money. This chapter provides basic information regarding these features. For more detailed instructions, please see [DSM Help](#).

Use Web Station to Host Websites

Go to **Main Menu > Control Panel > Web Services** to set up your website with Web Station, which is integrated with support for PHP and MySQL. For detailed instructions, please see [DSM Help](#).



Enable Web Station

With the Web Station feature, you can create a website with web pages on the ioSafe 214. With built-in PHP and MySQL support, you can create dynamic, database-driven website for your business. There is also a variety of 3rd party packages such as Content Management, Customer Relationship Management & e-Commerce system in Package Center, so that you can install them with a few clicks. The default shared folder, "web" will store the web page files for your website.

Enable Virtual Host to Host Websites

You can host multiple websites on a single server with virtual host feature. Each website can have different port numbers or even different hostnames.

Enable Personal Website

The personal website function is a convenient way to allow ioSafe 214 users to host their own personal websites. Each local user, domain user and LDAP user will have a unique website address.

Enable MySQL

You can enable MySQL to use the MySQL database function for your website. After MySQL is enabled, you can install the **phpMyAdmin** package available at Synology's **Download Center** to manage the MySQL database.

Manage PHP Settings

After you have enabled Web Station, you can click the **PHP Settings** tab to configure PHP related settings. For more detailed instructions, please see **DSM Help**.

More Information

Install Featured Applications

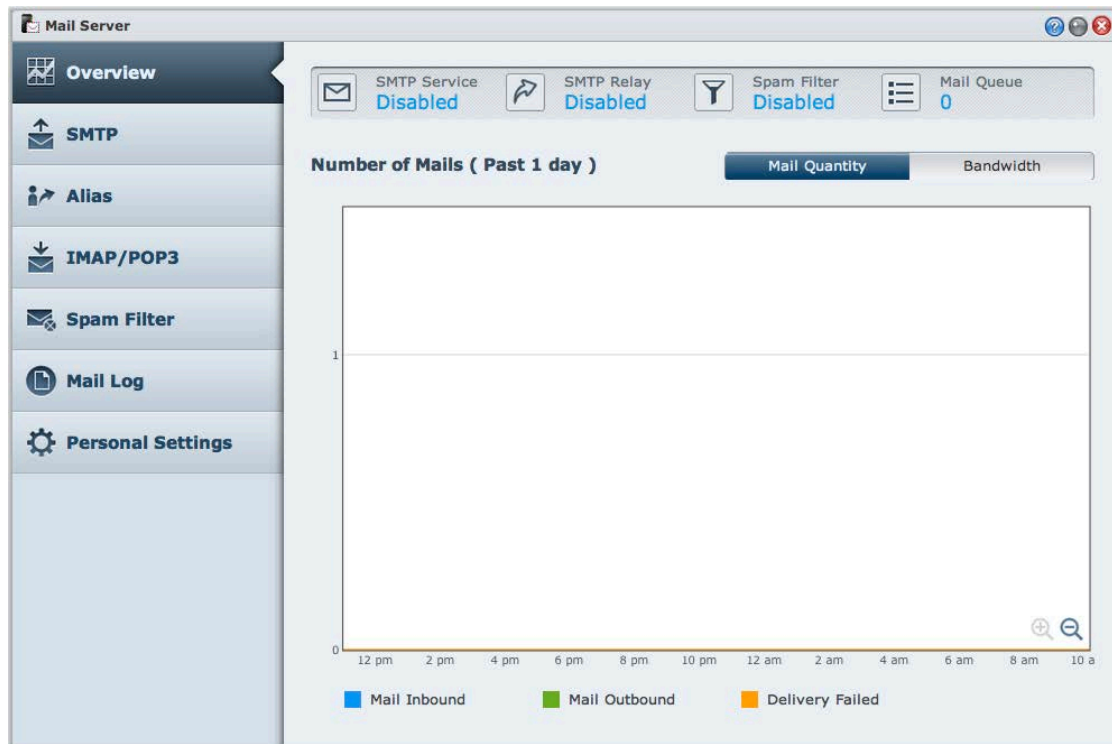
- After you have finished setting up your web environment, you can install applications to enhance the features of your website using many of the free Open Source applications.
- For a list of featured applications tested to be compatible with ioSafe 214, visit http://www.synology.com/support/faq_show.php?q_id=404. For the download links and installation instructions of those applications, visit their official websites.

Modify HTTP Service Options

Click the **HTTP Service** tab at **Control Panel > Web Services**. In addition to the default port number 80, you can add another port for the use of Photo Station and Web Station. For more detailed instructions, please see **DSM Help**.

Host Mail Server

You can turn your ioSafe 214 into a mail server, allowing ioSafe 214 users to receive and deliver mail messages using their mail client programs.



Before you start

Register a domain name for your IP, or apply for a DDNS hostname.

Note: For more information about registering a DDNS account for ioSafe 214, see "Register a DDNS hostname for ioSafe 214."

- When applying for a domain name or dynamic domain name, please fill the MX (Mail eXchanger) record of mail domain with your mail server (that is the FQDN of ioSafe 214).
For example, if the mail server is **mail.synology.com**, then fill the MX record with **mail.synology.com**.
- Go to **Main Menu > Control Panel > User** and enable **User Home** service to allow users to store their mail messages in their home folders. Otherwise, they will not be able to send or receive mails.

Note: For more information about User Home, see "Create User's Home Folder."

Confirm the port forwarding settings:

You should follow the table below to setup port forwarding if NAT is required.

Protocols	SMTP	POP3	IMAP	IMAPS	POP3S
Port	25	110	143	993	995
Note	IMAPS: IMAP over SSL/TLS POP3S: POP3 over SSL/TLS				

Set up Mail Server

Go to **Main Menu > Package Center** to install and run the Mail Server package. For more detailed instructions regarding Mail Server, please see **DSM Help**.

Install Mail Station to Enable Webmail Service

With the Mail Station package up and running, 214 users can send and receive mails via DSM's webmail service.

To install and run Mail Station:

Go to **Main Menu > Package Center** to install and run the Mail Station package.

Note: For more information about installing packages for DiskStation Manager, see "Chapter 11: Discover Various Applications with Package Center."

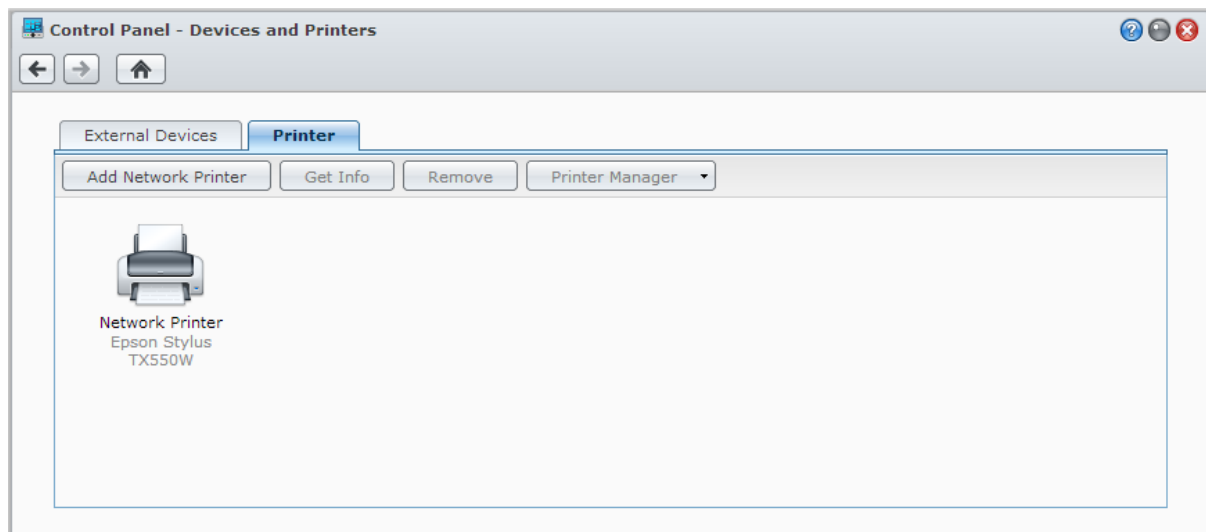
To connect to Mail Station:

Type the following web address in the address bar of your web browser, and then press Enter on your keyboard:
http://ioSafe_Server_IP_Address/mail/

Note: For more information about using the webmail service, see **Mail Station 2 User's Guide** from Synology's Download Center at: <http://www.synology.com/support/download.php>

Set ioSafe 214 as Print Server

Go to **Main Menu** > **Control Panel** > **Devices and Printers** > **Printer** to set the 214 as a print server over your local area network, allowing client computers or mobile devices to access printers connected to the 214. The 214 can connect to USB printers or network printers. In addition, AirPrint support allows you to print from an iOS device, and Google Cloud Print support allows you to print using Google products and services.¹ For more detailed instructions, please see **DSM Help**.



Note: One 214 can be connected by up to 2 USB printers.

Set up Computer to Access Print Server

After the print server is set up on your 214, Windows, Mac, and Linux clients within the local area network can connect to the print server and access its print/fax/scan service.

Access Print Server with iOS Devices

If you have enabled DSM's AirPrint support, any iOS devices running on iOS 4.2 or later can print to the printer connected to your 214.¹

¹ For recommended peripheral models, including hard drive, USB printer, DMA, and UPS, please visit www.iosafe.com/support.

Discover Various Applications with Package Center

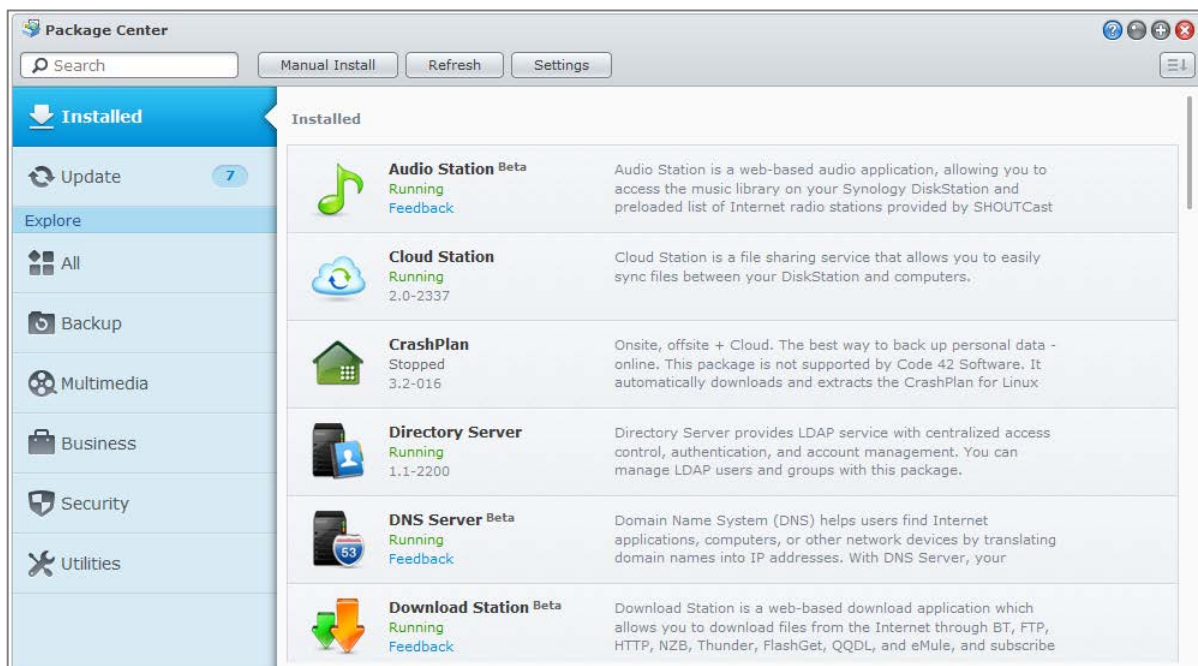
Synology has integrated third party or Synology-designed applications into packages that can be installed on the ioSafe 214 and managed with Package Center.

Coming with full-featured applications, ioSafe 214 provides you with a variety of privileges to enjoy multimedia contents, share photos, videos, and blogs, access files anytime and anywhere, monitor live actions from cameras, live stream and record digital TV programs, search and download files from the Internet, back up precious data, and build your own cloud.

This chapter introduces packages available at Package Center and how to install packages. For more detailed instructions, please see [DSM Help](#).

What Package Center Offers

Go to **Main Menu** > **Package Center** to find out what Package Center has to offer.



Install or Buy Packages

On the left panel, you will see a group of package categories listed under **Explore**. Choose any category to view a complete collection of packages classified under this category. Click **Install** or **Buy**, and follow the onscreen instructions to install the package. You can also click **Manual Install** and follow the wizard to install a package by uploading .spk file (available at Synology's [Download Center](#) or third party websites).

Share Photos, Videos, and Blogs with Photo Station

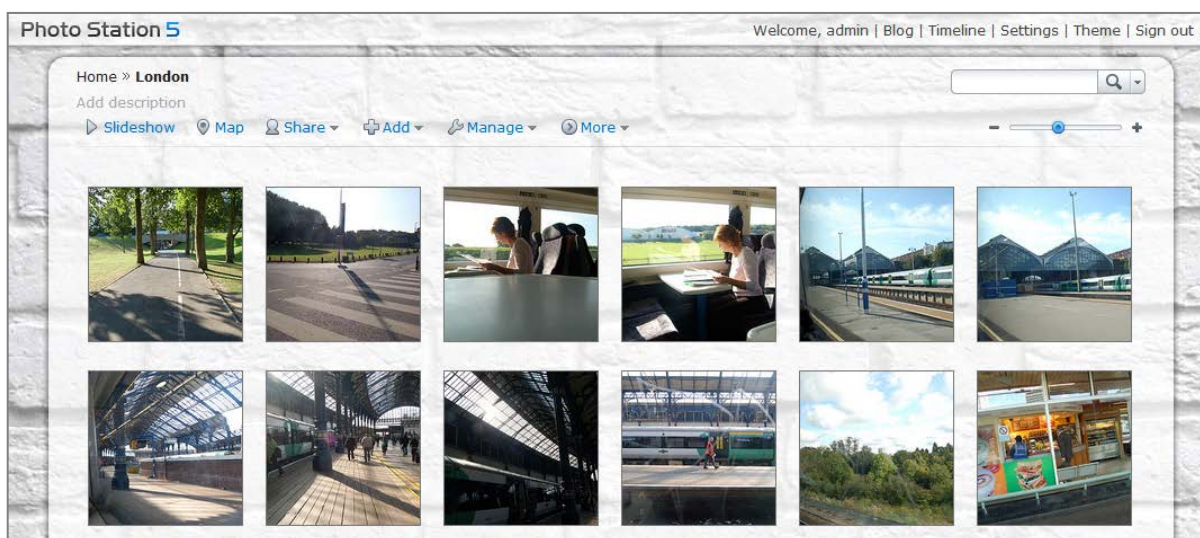
Photo Station is an online photo album integrated with a blog for you to easily share photos, videos, and blog over the Internet. It features Timeline on which photos and videos can be presented with Google Maps displaying where they are taken. Face recognition allows you to have Photo Station find faces on photos for you. With this experimental feature, you can take memorable notes to mark your precious moments by tagging photos with people, places and descriptions.

Moreover, you can download DS photo+ from Apple's App Store, Android Market, or Windows Marketplace to browse photos and watch videos saved on your 214 with your iOS/Android devices or Windows Phone on the go. For more information about DS photo+, see "Chapter 21: Communicate with Mobile Devices".

This chapter provides a brief overview of Photo Station's features. For more detailed instructions, please see [DSM Help](#), or go to the [Settings](#) page and click the [Help](#) tab in Photo Station.

Install Photo Station

Go to [Main Menu](#) > [Package Center](#) to install Photo Station owned by DSM users belonging to the **administrators** group. Once Photo Station is installed, the **photo** shared folder will be created automatically to contain Photo Station data.



Support and Limitations

- **Supported image formats:** BMP, JPEG, GIF, RAW (arw, srf, sr2, dcr, k25, kdc, cr2, crw, nef, mrw, ptx, pef, raf, raw, 3fr, erf, mef, mos, orf, rw2, dng, x3f), TIFF, PNG
- **Supported video formats:** 3G2, 3GP, ASF, AVI, DAT, DivX, FLV, M4V, MOV, MP4, MPEG, MPG, MTS, M2TS, M2T QT, WMV, XviD, RM¹, RMVB¹, VOB¹
- **Browser requirement:** JavaScript enabled
- **Microsoft Internet Explorer requirement:** ActiveX controls and plug-ins and Active scripting enabled
- **Upload limit:** If you upload contents with Photo Station, you can only upload up to 2GB of contents at a time.

¹ Users can download files of the specified formats, but cannot play them in Photo Station as a compressed Flash video.

Enable Personal Photo Station

Users belonging to the **administrators** group (if Photo Station's account system is set as **DSM accounts**) can enable Personal Photo Station service to allow all DSM users to have their own Personal Photo Station.

To enable Personal Photo Station, you need to enable the following services first:

- Enable user home service (Go to **Main Menu** > **Control Panel** > **User** > **User Home**). See "Create User's Home Folder" for more information.)
- Enable Personal Photo Station service in Photo Station (Go to **Settings** > **General** > **Personal Photo Station**)
- Enable Personal Photo Station in DSM (Go to **Options** > **Photo Station**). See "Manage Personal Options" for more information.

Photo Station Features

Once properly installed and setup, Photo Station provides the below features. For more detailed instructions regarding these and other features, please see **DSM Help**, or go to the **Settings** page and click the **Help** tab in Photo Station.

Choose Photo Station User Accounts

When Photo Station or Personal Photo Station is enabled by DSM **administrators** or DSM users, they become their Photo Station's administrator, who can choose to integrate DSM user accounts into Photo Station, or manage independent user accounts. To choose and manage user accounts, go to **Settings** > **General** > **User Accounts**.

Create Albums

Users belonging to the **administrators** group can create albums and upload photos via various methods depending on which suits you best, manage albums with different functions, view uploaded files with quality thumbnail for better browsing experience, and edit photos and videos on the **Photos** page. Go to the **Settings** page and click the **Help** tab for more information.

Share with Social Networks

When you browse your albums, you can share links and upload photos and videos from Photo Station to your social network accounts, or sync Photo Station albums with Facebook. To manage settings related to social networks, go to **Settings** > **General** > **Social Network Settings**.

Browse Photos and Videos with Timeline

Browsing photos and videos with Timeline is intuitive and easy. You can navigate the files by scrolling up or down the mouse wheel to quickly find photos or videos of a specific period of time, and simultaneously view where they are taken or recorded with Google Maps displayed below.

The Timeline function needs to be enabled at **Settings** > **Photos** > **Basic Settings** before you can browse files with Timeline. To configure the Timeline settings and play with Timeline, go to **Timeline**.

Manage Tags for Photos

You can tag your photos with people, locations, and descriptions, and manage people tags, geotags, and descriptive tags with the add, edit, delete, and confirm functions.

To add tags, go to the **Photos** page, select any album to which you want to add tags to enter the thumbnail view, and click **Manage**.

To batch edit or delete tags, go to **Settings** > **Photos** > **Basic Settings** and click **Tag**.

Perform Face Recognition

By enabling face recognition function, you can not only configure Photo Station to detect faces and perform auto recognition, but also identify faces yourselves manually. Without enabling the face recognition function, you are

not allowed to configure Photo Station to auto recognize faces for you. To enable the function, go to **Settings** > **Photos** > **Face Recognition**.

Customize Album Layout

You can customize the layout of Photo Station by changing template, background image, background color, font color, and logo image at **Settings** > **Photos** > **Basic Settings** > **Theme**, as well as choose how thumbnails and the number of thumbnails are displayed within an album at **Settings** > **Photos** > **Thumbnail Settings**.

Use the Blog

If you are a Photo Station administrator, you can sign in to enable, manage and back up your personal blog. Moreover, you can also personalize your blog space by adjusting its settings and layout.

The blog function needs to be enabled at **Settings** > **Blog** > **Basic Settings** before you can post articles on your blog. To manage the blog, go to **Blog**.

Play Music with Audio Station

Audio Station is a web-based audio application, allowing you to access the music library on your ioSafe 214, choose available audio sources on the local area network, and add your favorite music to playlists for playback. You can also browse and play songs on the DLNA-certified Digital Media Servers, and listen to Internet radio.

Audio Station can play music with live lyrics display through USB or Bluetooth speakers connected to your ioSafe 214, on your computer, DLNA-certified Digital Media Renderers, iOS/Android devices, Windows Phone, AirPlay compatible devices¹, or external speakers or home stereo equipment connected to the audio dock of Synology Remote (sold separately).

You can download DS audio from Apple's App Store, Android Market, or Windows Marketplace to play the music in Audio Station with your iOS/Android device or Windows Phone. For more information about DS audio, see "Chapter 21: Communicate with Mobile Devices".

This chapter provides a brief overview of Audio Station's features. For more detailed instructions, please see [DSM Help](#).

Install Audio Station

Go to **Main Menu** > **Package Center** to install Audio Station. Once Audio Station is installed, the **music** shared folder will be created automatically to contain music you want to share on Audio Station.



¹ AirPlay is supported on specific models only. Visit www.synology.com for more information.

Manage Audio Station Settings

Users belonging to the **administrators** group need to do the following before enjoying music or allowing users to listen to music on Audio Station:

- **Enable personal music library:** You can enable personal library to allow 214 users to have their own personal music library. Once users' personal library is enabled, they can choose to browse and play either their own personal music or both shared and personal music. To enable personal music library, click **Settings > Personal Library**.
- **Enable optional settings:** You can enable related settings to allow 214 users to download songs, enjoy high-quality audio output, record diagnostic log, or restrict users from accessing UPnP devices listed under **Media Server**.
- **Assign access privileges:** Users can access the following only when their privileges are granted by users belonging to the **administrators** group. To assign privileges, click **Settings > Privileges**.
 - **USB/UPnP Renderer:** Users with this privilege can play music through USB devices or UPnP renderers.
 - **UPnP Browsing:** Users with this privilege can play media server contents.
 - **Manage Playlist:** Users with the privilege can edit or add shared playlists.
 - **Edit Music Tag:** Users with this privilege can edit music information.
- **Manage lyrics plugins:** Users can search lyrics from the Internet when lyrics plugins added to Audio Station are enabled by users belonging to the **administrators** group. To enable lyrics plugins, click **Settings > Lyrics Plugins**.
- **Manage transcoder¹:** You can manage transcoder to allow Audio Station to support more audio formats under streaming mode. To manage transcoder, click **Settings > Transcoder**.

Audio Station Features

Once properly installed and setup, Audio Station provides the below features. For more detailed instructions regarding these and other features, please see **DSM Help**.

Choose Audio Source

You can choose below audio sources shown on the left panel to play its contents at the bottom of Audio Station or with the mini player.

- **Library:** The library contains music in the **music** shared folders or any other indexed folders of your ioSafe 214, which will be organized into the categories shown in the main area of Audio Station.
- **Playlist:** You can organize your songs into playlists to categorize and access your favorite music more easily. There are three types of playlists: **Personal playlist** (viewable by the 214 user who creates the playlist), **shared playlist** (viewable by all 214 users with access to Audio Station), and **smart playlist** (in which songs are exclusively selected based on specific rules). Smart playlists can also be edited at **Main Menu > iTunes Server**.
- **Internet Radio:** Audio Station comes with lists of Internet radio stations provided by SHOUTCast(TM) and RadiolO. You can also create your own radio lists or add radio stations to your favorites for quick access. Click **Internet Radio > Create** to create new radio stations or right-click the radio stations to add them to the pre-defined lists.
- **Media Server:** Audio Station can browse and play media contents on DLNA-certified Digital Media Servers or other ioSafe 214s on the local area network. Click **Media Server** to see media servers and ioSafe 214s found in the local area network.

¹ The ioSafe 214 supports Type 2 video Transcoding which handles videos in MP4 or MKV format. The video quality will remain as the original (H.264 video stream), and only the audio quality will be transcoded based on the audio stream of the source file and the 214's computing power. In this case, the video can be played on your device, but it requires enough bandwidth to stream if the bit-rate of your video is high. In addition, video transcoding type 2 is required (or necessary) if you wish to display subtitles on devices like Apple TV.

Change Browsing Views

By clicking the three buttons on the right side of the control bar, you can browse your songs or media contents in three different views: **List**, **Artwork**, **Playing Queue**.

Edit Music Information

You can view and edit the information of music files and song lyrics. To view and edit music information or song lyrics, right-click a music file and choose **Song information**.

Choose Output Devices

You can select your desired output device from the **My computer/USB speakers/[Media renderer name]** (indicating the device you have been streaming music to) drop-down menu on the control bar, and add songs to individual devices to play music via different devices. The output devices include the following:

- **My computer:** Stream music to your computer for playback via the speakers of your computer.
- **USB speakers:** Play music via the USB speakers connected to the USB port of your video Transcoding, or via external speakers or home stereo equipment connected to the audio dock of Synology Remote (sold separately).
- **Media renderer:** Play music via a Digital Media Renderer (DMR), an AirPlay¹ compatible device, or Bluetooth speakers within your local area network. Once they are found, their device name will appear in the drop-down menu, like Apple TV, Sonos. To connect Bluetooth devices to your 214, see "Manage Bluetooth Devices".

¹ AirPlay is supported on specific models only. Visit www.synology.com for more information.

Organize Videos and Record TV Programs with Video Station

Video Station is an ideal video organizer of your collection of movies, TV shows, home videos, and TV recordings, allowing you to watch videos on your computer, DLNA/UPnP-compliant DMAs, AirPlay devices¹, iOS/Android devices, and Windows Phone. You can also live stream and record digital TV programs with a USB DTV dongle or **HDHomeRun** with DVB-T standard (sold separately) plugged into your ioSafe 214, view and edit video metadata whose information is retrieved automatically from the Internet, and create your own watchlist or favorite collection list for quick access.

You can download DS video from Apple's App Store, Android Market, or Windows Marketplace to play videos in Video Station with your iOS/Android device or Windows Phone. For more information about DS video, see "Chapter 21: Communicate with Mobile Devices".

This chapter provides a brief overview of Video Station's features. For more detailed instructions, please see **DSM Help**.

Install Video Station

Go to **Main Menu** > **Package Center** to install Video Station.



¹ AirPlay is supported on specific models only. Visit www.synology.com for more information.

Before You Start

Users belonging to the **administrators** group need to do the following before watching videos or streaming live TV programs with Video Station:

- **Create video folders:** Users belonging to the **administrators** group need to create video folders for movie, TV show, home video, and TV recording first to store your videos before managing files with Video Station. While placing video files, please make sure they are stored by corresponding type. To create video folders, click **Settings > Video Folder** (for movie/TV show/home video) or **TV Recording** (for TV recording).
- **Plug in a USB DTV dongle¹ to the 214:** Users belonging to the **administrators** group can record digital TV programs and watch digital TV programs broadcast live with the streaming service provided by Video Station with a USB DTV dongle or **HDHomeRun** with DVB-T standard (sold separately) plugged into your 214.

More Information

Tips for naming video files:

When placing videos in respective folders, it is recommended you follow the distinctive naming rules for different types of video files in addition to storing them by type. In doing so, not only files can be properly indexed, metadata can also be correctly retrieved from the Internet to update the video info. Naming guidelines for movies and TV episodes are as below:

- **Movie** - It should follow the format: **Movie name (Release year).ext**. For example, Avatar was released in 2009. According to the formula, the best file name is "Avatar 2009.avi".
- **TV Show** - It should follow the format: **TV show name.SXX.EYY.ext**. For example, if you are compiling a video clip, say episode 4 of season 3 for Gossip Girl, the best file name is "Gossip Girl.S03.E04.avi".

Video Station Features

Once properly installed and setup, Video Station provides the below features. For more detailed instructions regarding these and other features, please see **DSM Help**.

Categorize Your Videos

Users belonging to the **administrators** group can categorize video collections into movie, TV show, home video, and TV recording as shown on the left panel of Video Station. You can browse videos of each category by different classifications, and manage your videos by adding them to favorites, watchlist, or custom collection for quick access.

Manage Video Metadata

By the time your video files are placed in the respective video folders, metadata and poster image of the videos are collected automatically from the Internet, except for home videos whose metadata must be edited from scratch on your own. Users belonging to the **administrators** group can edit and correct video information; non-admin users can only view video and media information.

Record TV Programs

Users belonging to the **administrators** group can record digital TV programs by setting up a recording schedule; non-admin users can only watch programs which have already been recorded.

Live Stream TV Programs

Users belonging to the **administrators** group can choose which digital TV programs broadcast live to stream; non-admin users can only watch programs which have already been streamed with the streaming service

¹ For the complete list of supported DTV dongles, please visit [Synology's website](#).

provided by Video Station. Once the channel scan is completed, you can stream programs for playback with Video Station's embedded Video Player.

Play Videos

Video Station comes with an embedded player which allows you play videos with once the package is installed on your ioSafe 214. In addition to playing videos on your local computer, you can also stream multimedia contents to DLNA/UPnP-compliant DMAs or AirPlay compatible devices for video playback.

For better viewing quality and faster transcoding speed, it is recommended you install [VLC media player \(Windows, Linux\)](#) on your local computer for video playback.

Download Files with Download Station

Download Station is a web-based download application which allows you to download files from the Internet through BT, FTP, HTTP, NZB, Thunder, FlashGet, QQDL, and eMule, and subscribe to RSS feeds to keep you updated on the hottest or latest BT. It offers the auto unzip service to help you extract compressed files to your ioSafe 214 whenever files are downloaded.

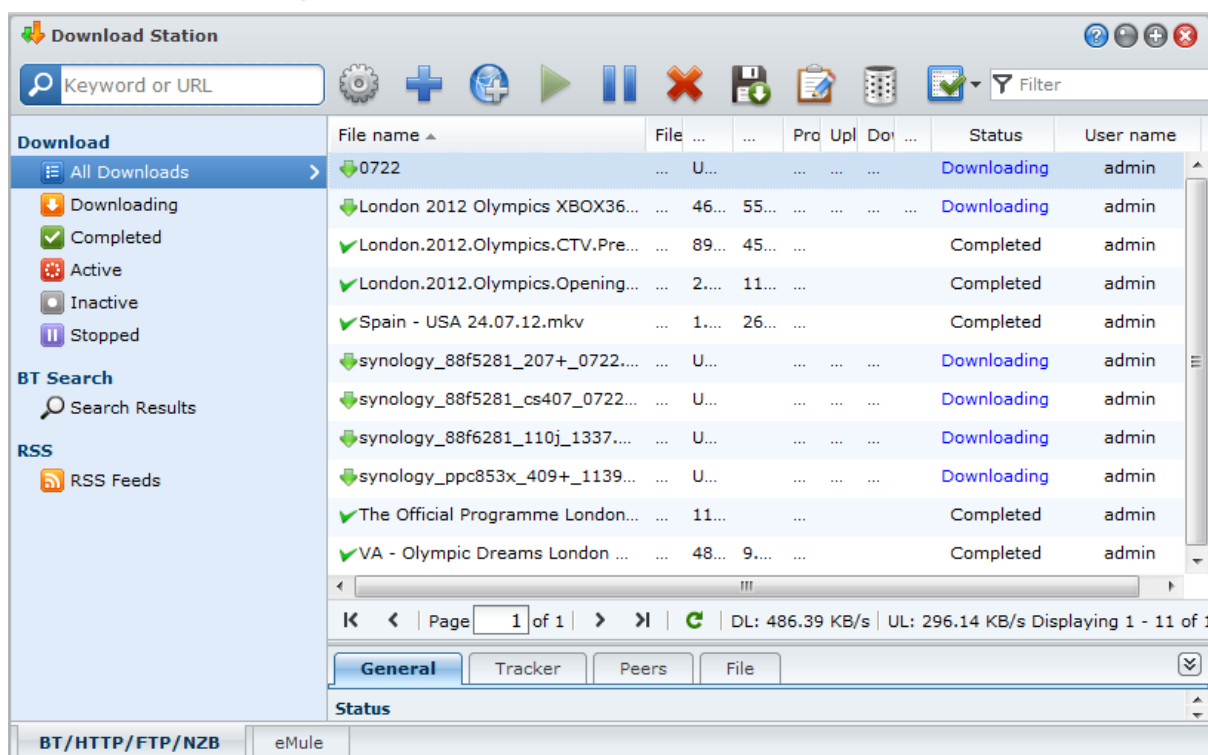
With Download Station, you can download files from multiple file hosting sites, and search for torrent files via system default search engines as well as self-added engines with the BT search function.

You can download DS download from Apple's App Store or Android Market to manage your download files in Download Station with your iOS/Android device. For more information about DS download, see "Chapter 21: Communicate with Mobile Devices".

This chapter provides a brief overview of Download Station's features. For more detailed instructions, please see [DSM Help](#).

Install Download Station

Go to [Main Menu](#) > [Package Center](#) to install Download Station.



Important: You must comply with all applicable laws and regulations when using Download Station. **DO NOT** download or share copyrighted files or software!

Download Station Features

Once properly installed and setup, Download Station provides the below features. For more detailed instructions regarding these and other features, please see [DSM Help](#).

Manage Auto Extract Service

Auto Extract service optimizes download task by unzipping downloaded archives automatically to your specified location. Password can be created to extract compressed files if needed.

Click **Settings** (the gear icon) next to the search field at the top and click the **Auto Extract** tab on the left side to manage the settings for Auto Extract.

Set up BT/HTTP/FTP/NZB

By using Download Station to download files, it will automatically detect the protocol your download link is using, and start the download for you.

Click the **BT/HTTP/FTP/NZB** tab at the bottom of Download Station to download files using BT/HTTP/FTP/NZB protocols, and click **Settings** (the gear icon) next to the search field at the top to manage the following BT/HTTP/FTP/NZB settings. For more detailed instructions, please see [DSM Help](#).

- **General:** Set download schedule, prioritize process order, and enable notification.
- **Location:** Specify download destination folder and torrent/NZB watched folder.
- **File Hosting:** Manage online file hosting and media sharing websites, where users can upload and share the files or multimedia contents with other people.
- **BT:** Edit settings for downloading BT files.
- **BT Search:** Use the BT Search function to search for torrent files with a list of default BT search engines.
- **FTP/HTTP:** Set the number of simultaneous connections to one FTP server, and limit the maximum download rate of each FTP task.
- **NZB:** Set up a news server to download NZB files.
- **RSS:** Shorten the update interval from 24 hours to your preferred time period for RSS download tasks.

Term Explanation

What is BitTorrent?

BitTorrent (BT) is a peer-to-peer file sharing protocol used for distributing data over the internet. It is one of the most common protocols for transferring large files. To share a file or group of files, a small file containing the metadata and the tracker of the original files (called "torrent") is created. Users can download "torrent" files and open them with specific software and connect to other users to start file downloads.

What is NZB?

NZB is an XML-based file format for retrieving posts from Usenet servers. The file includes information that your newsreader can use to start downloading. You need to join a newsgroup before you can start downloading files on Usenet.

Create BT/HTTP/FTP/NZB Download Tasks

You can create BT/HTTP/FTP/NZB download tasks by choosing any of the following methods.

- **Create by uploading files:** Upload any of the following files from your local computer to Download Station:
 - Torrent files (.torrent) contain information for downloading files being shared over the BT network.
 - NZB files (.nzb) contain information for retrieving posts from news servers.
 - URL files (.txt) contain a list of HTTP/FTP URLs for downloading the linked files.
- **Create by entering URLs:** You can create download tasks by entering URLs. Click **Add**. In the window that appears, enter the URLs of the file you want to download.

- **Create via BT search:** You can search for torrent files with BT search engines to help you find your favorite downloads more easily. To create download tasks via BT search, enter a keyword in the search field at the top-left corner of BT/HTTP/FTP/NZB.

Create Download Tasks for RSS Feeds

You can use Download Station to download RSS feeds that links to files instead of web pages, such as your favorite audio broadcasts.

More Information

What is RSS?

RSS (Really Simple Syndication, also known as RSS feed) is an alternative way of web browsing. Web publishers often use RSS feeds to publish frequently-updated works, such as blog entries, news headlines, podcasts, photo albums, or audio/video clips.

Can Download Station download all kinds of RSS feeds?

RSS files on the website of BT search engines and iTunes podcasts are generally supported by Download Station.

Some download links in the RSS file are links to a web page rather than the actual file. This kind of RSS files will not be supported. To view and update their RSS feeds, you can use a RSS reader (such as Google Reader) instead.

Manage BT/HTTP/FTP/NZB Download Tasks

You can check the download tasks you just created by clicking any of the following on the left panel, and use the buttons along the top of download queue and the tabs below the queue to manage your tasks. For more detailed instructions, please see [DSM Help](#).

- **All Downloads** lists all download tasks.
- **Downloading** lists download tasks that are currently downloading.
- **Completed** lists download tasks that are completely downloaded.
- **Active Downloads** lists download tasks that are currently downloading or seeding.
- **Inactive Downloads** lists download tasks that are erroneous, waiting, or paused by you.
- **Stopped** lists download tasks that are paused by you.

Set up eMule

eMule downloading is not enabled by default. You will need to enable eMule before configuring its settings. To enable eMule, click **Settings** (the gear icon) next to the search field at the top of Download Station, go to **Download Station > General** on the left panel.

Now you can click the **eMule** tab at the bottom-left corner of Download Station, and then click the gear icon next to the search field at the top of Download Station to manage the following settings of eMule. For more detailed instructions, please see [DSM Help](#).

- **General:** Manage the settings of ED2K server, notification, and protocol obfuscation.
- **Location:** Set the default destination folder for eMule, and share your files on the ED2K network.
- **Connection:** Set up connection for eMule downloads.
- **Bandwidth:** Set upload and download rates and download schedule to limit download and upload bandwidths.

Term Explanation

What is eMule?

eMule is a free peer-to-peer file sharing application which connects to both the eD2k network and the Kad network. Although the transfer speed is usually slow, eMule has a very large user base, and an even larger file sharing base which makes it excellent for finding rare content.

Create eMule Download Tasks

You can create eMule download tasks by choosing any of the following methods.

- **Create by uploading files:** Upload a text file (.txt) containing ED2K links from your local computer to Download Station. To create download tasks by uploading a file, click **Download Queue** on the left panel. Click the **Create** button, choose **Open a file**, and click the button to browse to the text file for upload.
- **Create by entering URLs:** To create download tasks by entering URLs, click **Create**. In the window that appears, choose **Enter URL**, and enter the URLs of the file you want to download.
- **Create via eMule search:** Click **Search** on the left panel to search and download the files you are looking for. To create download tasks, do either of the following.
 - **General search:** Enter a keyword in the search field at the top-left corner of eMule, select a file type and search method.
 - **Advanced search:** Click on the down arrow to the right of the **Start/Stop search** button.

Manage eMule Download Tasks

You can manage the download tasks you just created by clicking **Download Queue** on the left panel, and check your shared files currently uploaded to other eMule clients by clicking **Uploading**.

Safeguard Your Environment with Surveillance Station

Surveillance Station is a professional Network Video Recording (NVR) software bundled with DiskStation Manager (DSM), allowing you to remotely record and monitor video footages from IP cameras which are paired with your 214, watch live view videos, set up scheduled recording, playback recorded events via web browser or mobile device for remote monitoring so as to safeguard your home or office environment.

With Surveillance Station, you can set up VisualStation within LAN to live view managed cameras without the help of a PC.

Additionally, you can download DS cam from Apple's App Store or Android Market to live view your IP cameras and play recorded events from Surveillance Station with your iOS/Android device. For more information about DS cam, see "Chapter 21: Communicate with Mobile Devices".

This chapter explains how to install Surveillance Station, manage IP cameras, watch and record live view videos, set up scheduled recording, playback recorded events, and use all the other comprehensive features provided by Surveillance Station. For more detailed instructions, please see [DSM Help](#).

Install Surveillance Station

Go to **Main Menu > Package Center** to install Surveillance Station. After installation, the **surveillance** shared folder will be created automatically to contain your Surveillance Station data. This shared folder is read-only and can be accessed only by users belonging to the **administrators** group.

The screenshot displays the Surveillance Station Management interface. The left sidebar contains a navigation menu with categories: Camera, Device, Event, and System. The main area shows a table of cameras with columns for Preview, Name, IP address, Status, Occupied, Limit to, and Rotation. The table lists seven cameras, including Warehouse1, Warehouse2, 6F_Hallway, 6F_Entrance, Brickcom, Axio P3344, and Axio. The status of the last two cameras is 'Unrecognized'.

Preview	Name	IP address	Status	Occupied	Limit to	Rotation
	Warehouse1	192.168.31.39	Normal	68 (GB)	-- (GB) / 30 (days)	Yes
	Warehouse2	192.168.31.38	Normal	44 (GB)	-- (GB) / 30 (days)	Yes
	6F_Hallway	192.168.34.74	Disabled	2 (GB)	-- (GB) / 30 (days)	Yes
	6F_Entrance	192.168.34.75	Disabled	3 (GB)	-- (GB) / 30 (days)	Yes
	Brickcom	192.168.22.206	Normal	9 (GB)	10 (GB) / -- (days)	Yes
	Axio P3344	--	Unrecognized	0 (GB)	-- (GB) / -- (days)	--
	Axio	--	Unrecognized	0 (GB)	-- (GB) / -- (days)	--

At the bottom of the interface, there is a pagination bar showing 'Page 1 of 1' and a status bar indicating 'Displaying 1 - 7 of 7'.

Manage Surveillance Station Settings

Click the **Management** tab to configure the following Surveillance Station settings.

Add and Edit Cameras

Go to **Camera > Camera List** under **Management** to add and edit cameras, set up recording schedule, and set up the advanced settings: **Motion Detection**, **Liveview Analytics**, **Camera Optimization**, **Patrol Settings**, **Fisheye Dewarping**.

To organize multiple cameras into camera groups for easier deployment, go to **Camera > Camera Group**.

Note: If you are not a user belonging to the **administrators** group, you may have limited access due to the privilege settings. To learn more about this, go to "Assign Privileges" or contact your administrator.

Play and Manage Events

Go to **Event > Event List** under **Management** to browse all events, play them with the Event Player, and delete, lock, filter, or download the video files.

Note: Your IP camera must support alarm recording to be able to use **Alarm Recording**. Alarm recording often relates to the IP camera's digital input and output pin, or DIDO. Refer to its datasheet for pin configuration detail. Alarm recording will begin when the IP camera detects an input pin is triggered.

Export Events

Go to **Event > Export** under **Management** to export the events to any shared folder or to an external storage device via USB or eSATA interface.

Mount Events

Go to **Event > Mount** under **Management** to mount exported events. You can mount exported archives onto Surveillance Station. The events in mounted archives can be played on the **Event** and **Timeline** pages.

Use E-Map

You can add, edit, and delete e-maps at **System > E-Map** under **Management**. After the e-map is created, you can go to **Live View** and click **Configure** to assign the e-map to a live view layout. When the setup is complete, you can click the **E-Map** button on the **Live View** page to open the map and quickly pinpoint the location of a camera.

Manage Notification Settings

Under the **Management** tab, go to **System > Notification** to have Surveillance Station send you notification messages via email, SMS, mobile devices or instant messaging programs whenever important events occur. You can decide which types of events to be notified at **System > Notification > Filter** and configure notification settings at **System > Notification > Settings**.

Manage Advanced Settings

Go to **System > Advanced** under **Management** to manage the advanced settings for Surveillance Station. You can choose from the drop-down menu to set the initial page after logging in to Surveillance Station. You can also enable centralized management, which allows you to set your 214 as a host server, and then add multiple 214s as clients to form a larger Surveillance network. Furthermore, you can manage a VisualStation within LAN and connect a TV set or LCD monitor to the VisualStation, and then watch live views and recordings of IP cameras managed by your 214 on the TV/LCD screen without using a computer.

Assign Privileges

Go to **System** > **Privilege** under **Management** to manage and assign access privileges to IP cameras for DSM users.

Install Camera License

Go to **System** > **License** under **Management** to manage camera license. With **Default License**, your 214 can manage one camera within LAN. You can purchase additional **Synology Camera License Packs** and then add the license key here to manage additional cameras.

View Logs

Go to **System** > **Log** under **Management** to view and manage log records of critical events such as camera disconnection or changes on the camera settings.

Watch Live View

On the **Live View** page, you can watch live feeds up to 49 channels, take snapshot and adjust camera angle via PTZ (Pan/Tilt/Zoom), e-map, manual recording, video analytics, or analytics history. You can also customize your own channel layout to fit your different surveillance scenarios and deployment.

Liveview Analytics lets you track targets during live viewing and recording. You can choose from several analytic types for your IP cameras, and track suspicious events intelligently to trigger smart recording on-the-fly. Each recorded session is archived in an organized fashion for analysis. A simulation mode ensures accurate tuning so you can adjust sensitivity, detection zone, and object size to deliver the best result for individual cameras.

For more detailed instructions, please see **DSM Help**.

Configure Layout

DSM users belonging to the **administrators** group and users with the **manager** privilege can configure layout setting. To customize the layout of camera live views and apply an e-map to a specific layout, click the **Configure** button.

Use PTZ Control

If your camera has PTZ (pan/tilt/zoom) support, you can select a camera and use the **Controller** panel to adjust the camera's direction. Clicking on the home button will restore the camera back to its original position. If you have selected a camera with partial PTZ support, the unsupported functions on the **Controller** panel will be grayed out.

Use Other Functions

On the **Live View** page, you can also use the following functions.



- 1 To digitally zoom in and out, drag the zoom bar or place the mouse over the live view of a selected camera and then scroll the mouse. You can also zoom digitally by using the scroll button on your mouse, and move by dragging the picture.
- 2 To adjust volume, drag the volume bar.
- 3 To pause or resume the playback, click this button.
- 4 To save the current image, click **Snapshot**.
- 5 To start manual recording, click **Manual Recording**.
- 6 To configure layout setting, click **Configure**.
- 7 Click **Show information**, and the status for each camera will be displayed on the corner of each live view window.
- 8 To see the corresponding E-Map, click **E-Map**.
- 9 To see the live view in full screen mode, click **Full screen**.
- 10 Click **Toggle** to enable Liveview Analytics on the cameras you want for live viewing.

Note: Only cameras whose Liveview Analytics settings have been configured at **Camera List > Advanced > Liveview Analytics** under the **Management** tab can be enabled here. For detailed instructions on Liveview Analytics settings, click the figure icon at the top-right corner and then click **Help**.

- 11 To playback and see the frequency of Liveview Analytics events, click **Analytics History**.
- 12 To see the corresponding preset or patrol, click the **Preset Position** or **Patrol** list.

Note: Non-Internet Explorer browsers support limited functions only.

Work with Timeline

Surveillance Station allows you to locate the actual recorded footage via Timeline and calendar support. The calendar lets you pick any date to show the day's recording. Using Event Timeline, you can easily identify events recorded in different modes, labeled by color on the timeline.

During an event playback, you can activate Smart Search to track down suspicious targets. Smart Search is an intelligent feature that helps you analyze past event effectively and eliminate any potential false alarms. For more detailed instructions, please see [DSM Help](#).

Play Events with Timeline

Click the **Timeline** tab to see the timeline page, which offers the Multiple-Event Playback function, which allows you to simultaneously watch events recorded on one day or at the same time by different cameras. All event videos are lined up in the timeline. You can easily find the event you are looking by clicking a specific time on this day or during the hour, and play it with the event player on this page.

Search for Specific Situations with Smart Search

Click the search icon at the bottom-left corner of the timeline page to enter the **Smart Search** mode. With Smart Search, you can search events for specific situations such as general movement or missing/foreign objects on the screen. If the camera lens was occluded or lost its focus by people trying to avoid surveillance, Smart Search can also help you find out when the situations happened.

Create a Domain Name Server with DNS Server

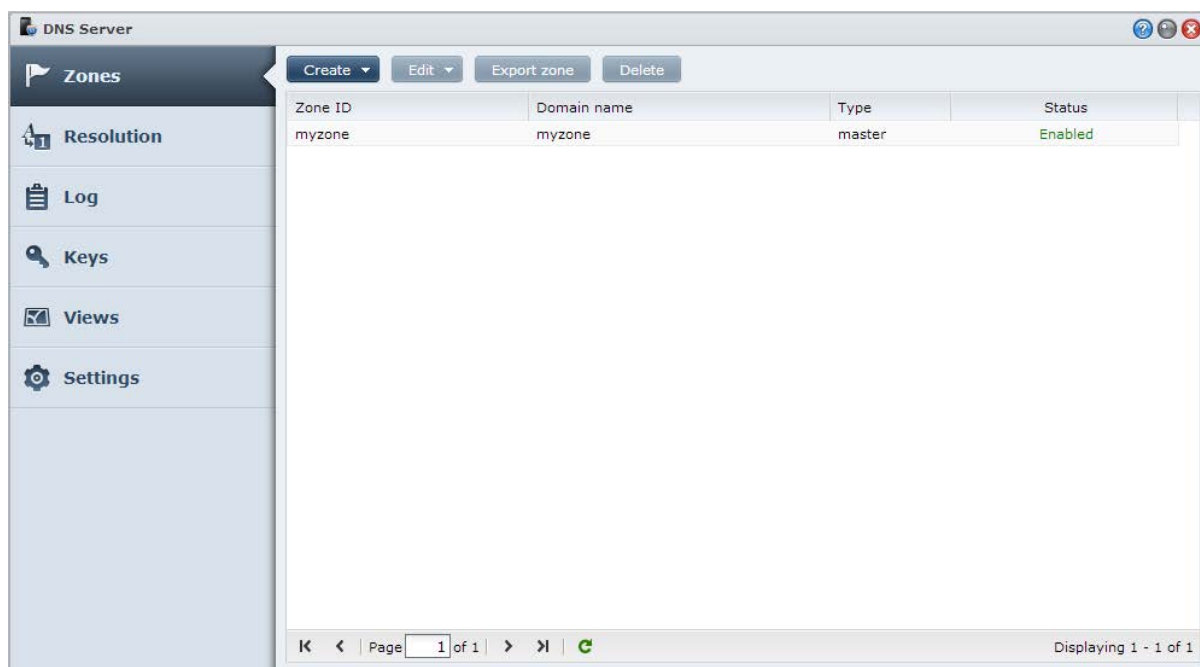
DNS (Domain Name System) is a naming system that facilitates the exchange of data between computers over the Internet and other networks. Its main function is to translate user-friendly domain names (e.g. www.ioSafe.com) into corresponding fixed, public IP addresses (e.g. 120.89.71.100). This function allows users to easily find web pages, computers, or other devices over the Internet or local network.

Synology's DNS Server allows your 214 to become a domain name server, host multiple zones, as well as provide name and IP address resolution services.

This chapter provides a brief explanation of the features of DNS Server. For more details instructions, please see [DSM Help](#).

Install DNS Server

DNS Server can be installed by going to [Main Menu](#) > [Package Center](#).



Before You Start

Please see the following notes before using DNS Server:

- **Obtain a fixed, public IP address:** To run DNS Server, you need to acquire a fixed IP address for your 214.
- **Register a domain name:** Setting up authoritative server functions requires registering your domain name with a domain name provider. For example, if you want to use a domain called example.com, you need to register the domain [example](http://example.com) with the domain provider of [.com](http://example.com) domain names.
- **Check firewall or port forwarding settings:** DNS services require the use of TCP and UDP port 53. If your 214 uses a firewall, this port must be opened. If the 214 connects to the Internet through a router, set up port forwarding rules and open TCP and UDP port 53.

- **Register your device:** After you set up DNS Server, remember to register the IP address and other required information of your 214 with the provider of your domain name. Otherwise, clients will be unable to query your 214 over the Internet. Consult your domain name provider for more information.

DNS Server Features

Once properly installed and setup, DNS Server provides the below features. For more detailed instructions regarding these and other features, please see [DSM Help](#).

Zones

This page provides options to manage your domain names by creating and modifying zones. A zone refers to a portion of the domain name space for which a domain name server is authoritative and possesses complete information. With DNS Server, zone files can be created, stored, and managed on the 214.

Zones are divided into two types: master zones and slave zones. Master zones possess information for zone files. Slave zones synchronize zone files from master zones (an operation called zone transfer).

Resolution

You can enable resolution services to allow the 214 to resolve recursive queries. A recursive query occurs when the 214 is not authoritative for a requested domain. In this case, the 214 queries other domain name servers until the information is found, or until the query fails.

For example, if a client queries your 214 for the address of "iosafe.com," but your 214 is not authoritative for this domain (i.e. you do not own iosafe.com), it will query other domain name servers or forward the request to specified forwarder servers, and then relay the result back to the sender of the query.

Keys

TSIG (Transfer Signature) keys limit what hosts are allowed to synchronize zone files from the master server. This page displays the keys currently used by DNS Server.

Views

A domain name server can present different information to different clients by implementing views. This function, sometimes called spilt-horizon DNS, can improve security and privacy management of DNS zone records. For example, you have one domain name, but wish to provide different responses to queries from external and internal sources. In such cases, you can create different views with separate resource records.

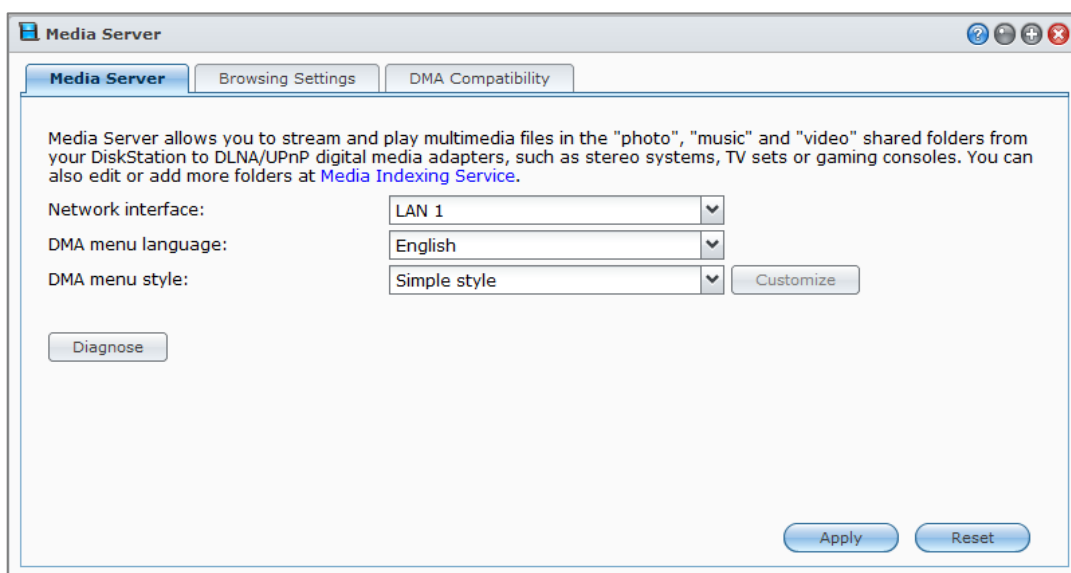
Manage Media Server and iTunes Service

The ioSafe 214 can become a multimedia server on the local area network, allowing computers (using Windows Media Player or iTunes) and DLNA/UPnP home devices (such as stereo system or TV set) to play its multimedia contents.

This chapter explains how to stream multimedia contents from ioSafe 214 to your computer or other DLNA/UPnP home devices. For more detailed instructions, please see [DSM Help](#).

Install DLNA Media Server

Go to **Main Menu > Package Center** to install Media Server.



Manage DLNA Media Server

Go to **Main Menu > Media Server** to browse and play the multimedia contents on the ioSafe 214 via DLNA/UPnP home devices, also known as **Digital Media Adapter (DMA)**. With Media Server, you can easily connect those devices such as TV sets and stereo systems to your home network, and stream multimedia files stored on the 214 to the devices to enjoy music, photos, and videos. More indexed folders can be added for sharing at Media Indexing Service. See "Manage Indexed Folder" for more information.

Note: You can play the following multimedia file formats on ioSafe 214 with DLNA/UPnP enabled DMA¹:

- **Audio:** AAC, FLAC, M4A, MP3, Ogg Vorbis, PCM, WAV, WMA, WMA VBR, WMA PRO, WMA Lossless
- **Image:** BMP, JPG (jpe, jpeg), GIF, ICO, PNG, PSD, TIF (tiff), UFO, RAW (arw, srf, sr2, dcr, k25, kdc, cr2, crw, nef, mrw, ptx, pef, raf, 3fr, erf, mef, mos, orf, rw2, dng, x3f)
- **Video:** 3GP, 3G2, ASF, AVI, DAT, DivX, DVR-MS, ISO, M2T, M2TS, M4V, MKV, MP4, MPEG1, MPEG2, MPEG4, MTS, MOV, QT, SWF, TP, TRP, TS, VOB, WMV, XviD, RV30, RV40, AC3, AMR, WMA3, RMVB
- **Playlist:** M3U, WPL

¹ The actual playback capabilities may vary depending on the DLNA/UPnP client.

Manage Indexed Folder

By default, media files within the **photo**, **video**, and **music** shared folders are indexed by Media Indexing Service. If you want DMA devices and DSM's photo, video, or music applications to access more files on your 214, you can add more indexed folders at **Main Menu > Control Panel > Media Indexing Service > Indexed Folder**.

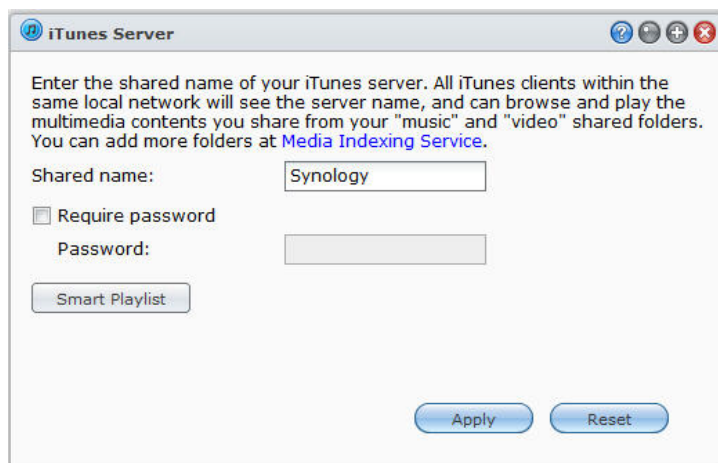
Play Multimedia Contents with DMA Devices

ioSafe 214 can pair up perfectly with Sony PS3, Xbox 360, and many other DMA devices. You can use those devices to browse and stream multimedia contents from your 214 to your stereo system and TV set.¹

Note: For information about browsing media server's contents with DMA devices, see the documentation that came with your multimedia device.

Install iTunes Server

Go to **Main Menu > Package Center** to install iTunes Server.



Manage iTunes Server

Go to **Main Menu > iTunes Server** to use iTunes service. After it is enabled, all iTunes clients on the same local area network can browse and play songs or videos in the **music** and **video** shared folders on the server. The server will be listed below **Shared** in the iTunes window after the service is enabled.

Note: For privacy reasons, iTunes clients are not allowed to view videos in the **photo** shared folder.

Launch iTunes Server

Enter your **Shared name**. Tick **Require password** and enter a password if you want iTunes users to enter a password before accessing your shared folders.

¹ For recommended peripheral models, including hard drive, USB printer, DMA, and UPS, please visit www.iosafe.com/support.

Use Smart Playlist

Click **Smart Playlist** to open the **Smart Playlist** window, where you can create and edit smart playlists on your ioSafe 214.

A smart playlist can automatically include certain types of songs that match specific rules. iTunes clients will be able to play the smart playlist you created.

Note: You can also create and edit smart playlists with Audio Station. See "**Choose Audio Source**" for more information.

Re-index Media Files

Click **Re-index** at **Main Menu > Control Panel > Media Indexing Service** to reconstruct the index structure of the audio files if you find missing files while browsing through ioSafe 214 with iTunes. The process will be executed in the background.

For more information about the index function provided by Media Indexing Service, click the **Help** button (with a question mark) at the top-right corner at **Main Menu > Control Panel > Media Indexing Service**, or see "Index Multimedia Files for Applications".

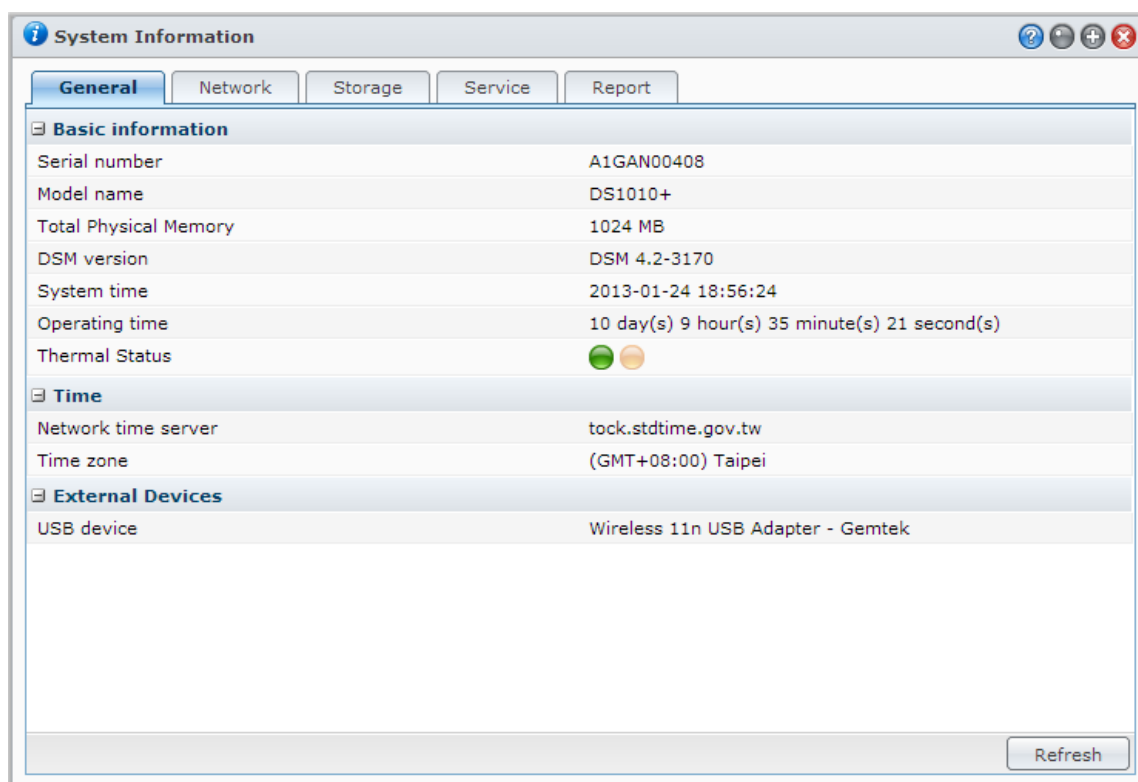
Perform Advanced Management Tasks

DiskStation Manager comes with a variety of management functions, allowing you to check system information, monitor system resources, manage notification services, restore or upgrade DSM, access applications with independent login, index multimedia files for applications and more.

This chapter explains how to comprehend advanced management functions to make sure your ioSafe 214 is providing the best performance. For detailed instructions, please see [DSM Help](#).

Check System Information

System Information provides an overview of the status of the 214 and other connected devices. Go to [Main Menu](#) > [System Information](#) to check the below information. For more detailed instructions, please see [DSM Help](#).



General

Under the **General** tab, you can see the basic information about your 214, including serial number, model name, amount of physical memory, DSM version, time information, thermal status, or external devices.

The 214's thermal status is represented by green or orange lights:

- **Green:** Thermal status is normal.
- **Orange:** 214's thermal temperature is high. You need to cool down your 214, or it will shut down to prevent system overheat.

The system's general information includes the following:

- **Basic Information:** You can see the detailed information about your ioSafe 214 here, including serial number, model name, memory size, DSM version, system time, operating time, and thermal status.
- **Time:** You can see the time setting of your ioSafe 214 here, including time server and time zone. To set up your time server, see "Set Up Time."
- **External Devices:** You can see the model name of your external USB devices here.

Network

Under the **Network** tab, you can view the status of network configuration and network interfaces.

The network status includes the following:

- **Basic information:** See the basic information of your 214's network configuration.
- **[Interface Name]:** See the detailed information of the network interface(s) currently configured on your 214.

Storage

Under the **Storage** tab, you can check the free or used space of your 214 volumes and check the status of the hard disks.

To check volume usage:

From the pie charts, you can see the free or used space of 214 volumes.

Following are the possible status types of an internal hard disk:

- **Normal:** System partition and volume are available for use on the hard drive.
- **Initialized:** System partition is established, but no volume has been created.
- **Not Initialized:** System partition and volume are not established on the hard drive.
- **No Disk Installed:** No disk is installed in the corresponding hard drive slot.
- **System Partition Failed:** System partition on the hard drive is unavailable. We recommend that you replace the hard drive.
- **Crashed:** Failed to access volume on the hard drive. We recommend that you replace the hard drive.

Note: For the system to function normally, there should be at least one disk in **Normal** or **Initialized** status.

Service

Under the **Service** tab, you can see the list of DSM services, which can be enabled or disabled by clicking **Enable** or **Disable** under the **Action** column. The checkmarks under the **Status** column indicate whether the services are enabled.

Report¹

Under the **Report** tab, you can collect data and generate reports that provide information about disk usage trends. You can select report types, set a schedule to receive periodic storage reports or generate reports on demand. For more detailed instructions, please see **DSM Help**.

View System Logs

Go to **Main Menu > System Logs** to view the log records of 214 services. General system, connection, file transfer (Windows file service, FTP, WebDAV, File Station), and backup (backup, network backup, USBCopy) logs are displayed here. This section also provides options to delete or save logs. For detailed instructions, please see **DSM Help**.

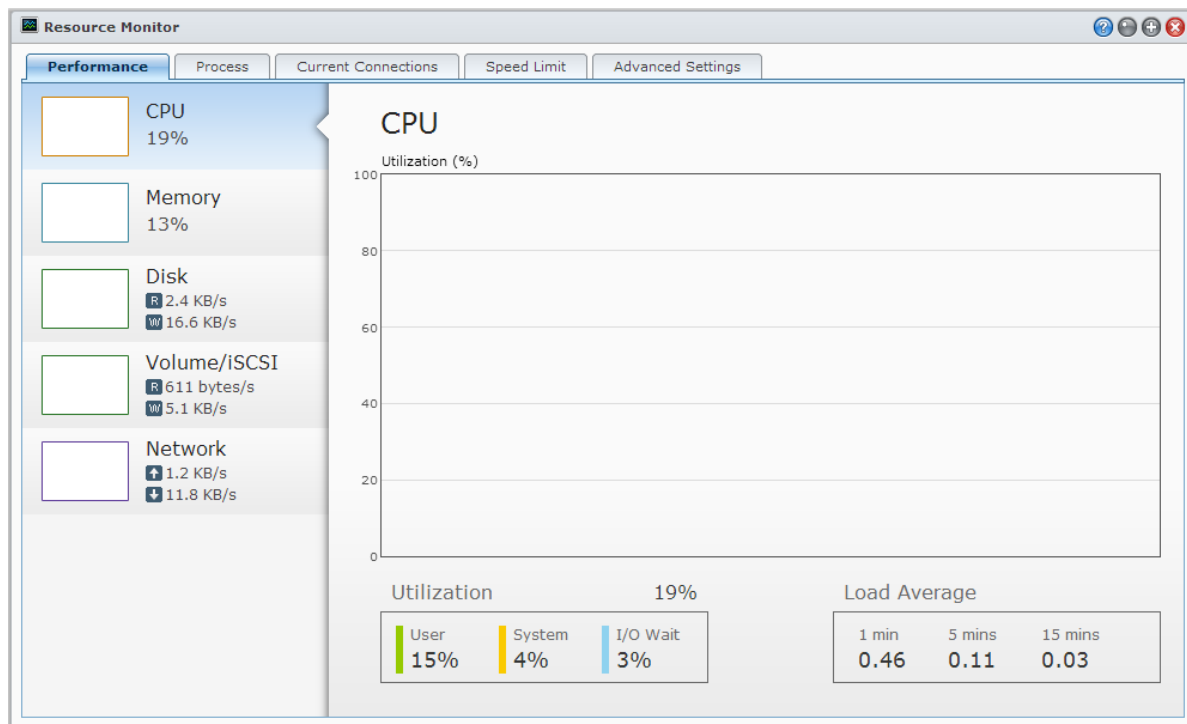
Log	Date & Time	User	Event
System	2012/08/01 17:56:13	admin	User [admin] logged in from [192.168.24.246]
System	2012/08/01 17:41:40	admin	User [admin] logged in from [192.168.21.253]
System	2012/08/01 17:00:29	admin	User [admin] logged in from [192.168.21.253]
System	2012/08/01 16:12:28	admin	User [admin] logged in from [192.168.22.183]
System	2012/08/01 15:49:03	admin	User [admin] logged in from [192.168.21.253]
System	2012/08/01 14:57:17	admin	User [admin] logged in from [192.168.22.181]
System	2012/08/01 14:28:34	admin	User [admin] logged in from [192.168.21.253]
System	2012/08/01 14:20:04	admin	User [admin] logged in from [192.168.20.247]
System	2012/08/01 14:05:13	admin	User [admin] logged in from [192.168.21.253]
System	2012/08/01 14:03:02	SYSTEM	Windows file service was started.
System	2012/08/01 14:02:59	SYSTEM	Apple file service was started.
System	2012/08/01 14:02:59	SYSTEM	Windows file service was stopped.
System	2012/08/01 14:02:57	SYSTEM	Apple file service was stopped.

K < | Page 1 of 23 | > > | Info:1116 | Warning:2 | Error:19 | Displaying 1 - 50 of 1137

¹ Only available on specific models.

Monitor System Resources

Go to **Main Menu > Resource Monitor** to monitor system resources, such as CPU usage, memory usage, disk utilization and network flow. You can choose to monitor the below tabs in real time or view the previous data. For more detailed instructions, please see **DSM Help**.



Performance

Click on **Performance** tab to view the resource utilization data, including CPU, memory, disk, and network. Detailed date, time and information of the chart will be shown upon mouse-over.

Process

Click on the **Process** tab to view the CPU and memory usage of each process in the order of decreasing CPU load. The process status includes **Running**, **Sleeping** and **Stopped**. Linux equivalents of process status are **running**, **stopped/tracing**, **sleeping**.

Current Connections

Under the **Current Connections** tab, you can view a list of users who are currently accessing 214 resources. You can export the current list, kill connections of specific users, or disable user.

Speed Limit

Under the **Speed Limit** tab, you can view and manage the list of file transfer processes that applied speed limit. You can update the lists or kill connections of specific file transfers.

Advanced Settings

Click on **Advanced Settings** tab to set up additional options, including real time duration and usage settings.

Manage Bluetooth Devices

Go to **Main Menu** > **Control Panel** > **Bluetooth** to manage Bluetooth adapters and connect Bluetooth devices to your 214. Once connected, some Bluetooth devices, such as speakers or headphones, can be selected as the audio output for Audio Station, allowing you to easily listen to music stored on your 214. For more detailed instructions, please see **DSM Help**.

Automate Tasks

Go to **Main Menu** > **Control Panel** > **Task Scheduler** to schedule and run services or scripts at pre-defined times. You can create and manage tasks to automatically run user-defined scripts, empty shared folder recycle bins, or start and stop certain services. For more detailed instructions, please see **DSM Help**.

Update DSM

Periodically, Synology releases free DSM updates. Updates may include new features, function improvements, and performance enhancements. Go to **Main Menu** > **Control Panel** > **DSM Update** to keep your ioSafe 214 up to date.

Important: The data saved on the ioSafe 214 will not be erased during the updating process. However, for security reason, we recommend that you back up the data first.

Checking for Updates

Every time you go to **DSM Update**, the system will check with Synology to see if a new DSM version is available for download, and then display the result in green or red text. In addition, you can manually install updates obtains from Synology's **Download Center** or have the system automatically check for updates. For more detailed instructions, please see **DSM Help**.

Troubleshooting

If you cannot update DSM, the following suggestions might help solve your problem:

- Check if the upgrading process was interrupted by users, or other unexpected events, such as a power failure.
- Check the DSM version. You can only update the system with a newer DSM version.
- Download the DSM update again because the update file might be corrupted.

If the problem remains, please contact ioSafe's **Technical Support**.

Receive Event Notifications

Go to **Main Menu > Control Panel > Notification** and set up ioSafe 214 to notify you via e-mail, SMS, mobile devices, Windows Live Messenger, or Skype, when status changes or errors occur to the system, for example: connection loss, fan behavior change, power failure, storage volume running out of space, or back and restoration failure, etc.

For more information about how to select notification event types and edit notification messages, click the **Help** button (with a question mark) at the top-right corner, and then go to **Control Panel > System > Notification > Advanced**.

Manage E-mail Notification Service

Click the **E-mail** section to set up email notifications. You can enter your SMTP server information and e-mail addresses to receive notification messages when status changes or errors occur to the system, such as connection loss, fan behavior change, power failure, storage volume running out of space, or back and restoration failure, etc.

More Information

About SMTP server's domain name:

The SMTP server can be an IP address or a domain name. If it is a domain name, please make sure a valid DNS server IP has been entered at **Main Menu > Control Panel > Network**, and make sure the server is on the Internet.

Manage SMS Notification Service

Click the **SMS** section to set up SMS notifications. You can enable SMS notifications in order for ioSafe 214 to send you notification messages via SMS when status changes or errors occur to the system, such as connection loss, fan behavior change, power failure, storage volume running out of space, or back/restoration failure, etc.

More Information

SMS URL: case sensitive and must be between 1 and 500 Unicode characters. The number of parameters must be between 4 and 10. This SMS URL is only for setup purposes. No SMS message will be sent after setup is completed. The format of this URL is provided by the SMS service provider, and the URL must include the following parameters: username, password, destination phone, and message content.

Using Clickatell as an example, a sample URL would be the following (reference only):

`https://api.clickatell.com/http/sendmsg?user=TestUser&password=TestPassword&api_id=3148203&to=886123456789&text=Hello+world`

Please note that in "message content" parameter, the space between "Hello" and "world" will be replaced by the particular character defined by the service provider.

Manage Mobile Devices and Instant Messaging Notifications

Click the **Push Service** section to set up mobile device and instant messaging notifications. You can enable push service to send notification messages to your mobile devices and instant messaging programs (Windows Live Messenger and Skype) via Synology's push service server when status changes or errors occur to the system.

Access Applications with Independent Login

Go to **Main Menu > Control Panel > Application Portal** to configure connection settings of applications, which allows you to run the applications in an independent browser window without logging in to DSM. These connection settings include customizing portal aliases, HTTP and HTTPS ports.

Note: Applications whose connection settings can be configured via Application Portal are: Audio Station, Download Station, Surveillance Station, Video Station, File Station.

Customized Alias

Applications can be opened in an independent browser window at **[http(s)://DSM server address:DSM server port number [HTTP(S)]/alias name/]** once the portal alias is set up.

Customized HTTP(S) Ports

Applications can be opened in an independent browser window at **[http(s)://DSM server address:customized port number]** once the HTTP(S) port is set up.

Index Multimedia Files for Applications

Go to **Main Menu > Control Panel > Media Indexing Service** to have Media Indexing Service automatically scan multimedia files, such as photos, music, and videos stored on your 214, and compile them into the media library to be indexed by multimedia applications: Media Server, Audio Station, Photo Station, and iTunes Server. For more detailed instructions, please see **DSM Help**.

Re-index Media Files

Multimedia data within the installed applications can be scanned and re-indexed for applications. Click **Re-index** to re-construct the index structure of all media files in the indexed folders, both default folders and the ones created by you. The process will be executed in the background.

Reset Admin Password

If you forgot the password for **admin** and are therefore unable to log in to DSM, you can reset the password to blank and set a new password.

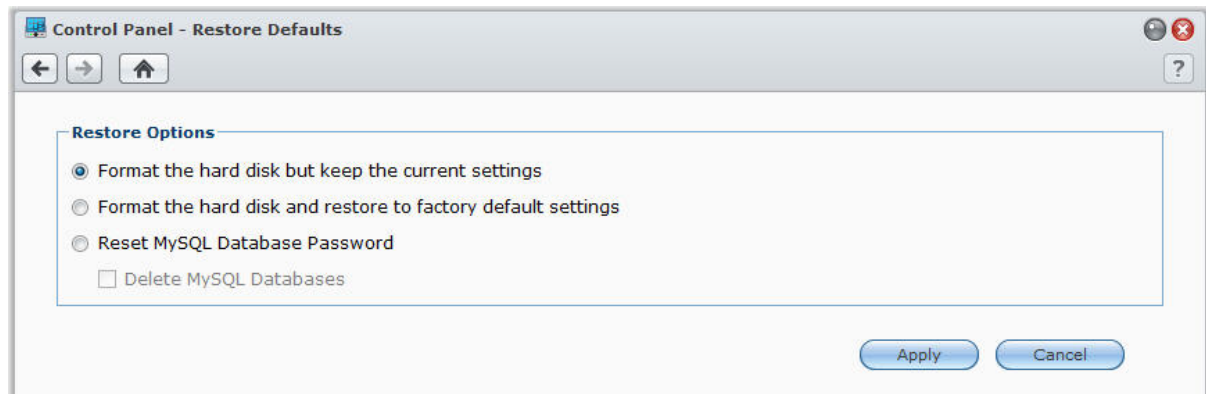
To reset admin's password:

Press and hold the **RESET** button on the back panel of your ioSafe 214 for 4 seconds until you heard a beep sound.

Note: Other than resetting administrator's password, using the **RESET** button will also restore ioSafe 214's IP and DNS to the default value.

Restore ioSafe 214 to Factory Defaults

Go to **Main Menu > Control Panel > Restore Defaults** if you want to restore your ioSafe 214 to factory defaults.



There are three restore options:

- **Format the hard disk but keep the current settings:** All user data in the hard drive will be deleted; whereas the system configurations will remain.
- **Format the hard disk and restore to factory default settings:** All user data in the hard drive will be deleted and the entire system will be restored to default.
- **Reset MySQL Database Password:** The password of the MySQL database will be reset.

If you wish to delete your MySQL databases, check the **Delete MySQL Databases** checkbox and click **Apply**.

Reinstall ioSafe 214

If you want to reinstall your ioSafe 214 without losing its data, you can use the **RESET** button on the back panel.

To reinstall ioSafe 214:

- 1 Press and hold the **RESET** button for about 4 seconds until the ioSafe 214 emits a beep sound.
- 2 Within the next 10 seconds, press and hold **RESET** button for about 4 seconds until the ioSafe 214 emits a beep sound.
- 3 Run Synology Assistant and follow the installation instructions in the **Quick Installation Guide** that came with your installation disc to set up the ioSafe 214.

Important: The data saved on the ioSafe 214 will not be erased during the reinstallation. However, for security reason, we strongly recommend that you back up the data first.

Enable SNMP Service

Go to **Main Menu > Control Panel > SNMP** to enable SNMP service, which allows users to monitor ioSafe 214 network flow with the network management software.

Currently, SNMPv1, SNMPv2c and SNMPv3 protocols are supported.

Enable Terminal Services

Go to **Main Menu > Control Panel > Terminal** to enable Terminal service, allowing you to use Telnet or SSH to log in to ioSafe 214 and modify its settings.

Important: Use the Terminal service with caution. Improper manipulation or modification to ioSafe 214 may result in system malfunction or data loss.

Communicate with Mobile Devices

As Internet access grows popular on mobile devices, Synology provides you with several creative alternatives to communicate with your ioSafe 214 using iOS/Android, Windows Phone, or other mobile devices.

Manage DSM Settings with DSM mobile

DSM mobile allows DSM users belonging to the **administrators** group to manage DSM settings and check DSM information with the web browser of an iOS (iPhone, iPad or iPod touch), Android device, or Windows Phone.

To log in to DSM mobile:

- 1 Use the web browser of your iOS/Android device or Windows Phone to connect to **http://ioSafe_Server_IP:5000**.
- 2 Enter your DSM user credentials and tap **Login**.

Note: For more information about DSM mobile, tap **Help** on the home page.

Use iOS, Android, and Windows Apps

The Synology mobile apps are now available on Apple's App Store, Android Market, and Windows Marketplace, allowing you to communicate with your ioSafe 214 wherever Wi-Fi access is available. You can manage your 214 files, music, photos, videos, even the surveillance videos, sync folders between your mobile devices and 214, download files, and watch videos on the go.

DS audio

DS audio allows you to access Audio Station with an iOS/Android device or Windows Phone and listen to your favorite music on the go. Besides, the remote controller feature allows you to control Audio Station's music playback when there is an audio output device connected to the USB port of your 214, such as a USB speaker, or an external speakers or home stereo equipment connected to the audio dock of Synology Remote (sold separately).

DS cam

DS cam allows users who own an iOS/Android device to live view their IP cameras, take snapshots, and view recorded events from your Surveillance Station whenever a network connection is available.

DS cloud

DS cloud is the mobile counterpart to Synology's Cloud Station and allows you to easily sync folders between an iOS/Android device and your 214.

DS download

DS download allows you to access Download Station and download files directly with an iOS/Android device. You can create download tasks by adding a URL, via a built-in mini browser of the application, or the integrated Safari browser for user convenience. Managing basic settings such as transfer speed limits or activating the advanced schedule is also possible.

DS file

DS file allows you to access and manage 214 files with an iOS/Android device or Windows Phone.

DS finder

DS finder allows you to monitor or email the status of your 214, and request it to perform wake on LAN (WOL), restart, shut down, or play beep sounds (to help you quickly find the its location) with an iOS/Android device or Windows Phone.

DS photo+

DS photo+ allows you to access Photo Station with an iOS/Android device or Windows Phone and share your precious moments on the go. Download and save photos from Photo Station to your mobile device so you can enjoy the flashbacks anytime anywhere. You can also use DS photo+ to upload snapshots or videos from your camera phone straight to Photo Station. Besides, you and your friends can interact by leaving comments on any photos, adding more fun to your photo sharing experiences.

DS video

DS video allows you to access Video Station and watch videos both at home and on the move with an iOS/Android device or Windows Phone. You can browse and organize your collections of videos, record digital TV programs available at the place you are located with a USB DTV dongle (sold separately) plugged into your 214, and manage your recording tasks and schedules.

Note: For more information about those mobile Apps, refer to the Help files that come with the Apps.

Use Other Mobile Devices

If you have a mobile device running on Windows Mobile 6.0 (with Internet Explorer Mobile or Opera 9.0 or later), Symbian OS 9.1 (with S60 3rd Edition or later), or iPhone OS 2.3.1 or later, you can use the device to log in to ioSafe 214 to view photos with Mobile Photo Station and read supported file formats with Mobile File Station around the world where Internet access is available.

Troubleshooting

For any questions about managing your DSM, go to **Main Menu > DSM Help** or click the **Help** button (with a question mark) at the top-right corner of every window. For any questions other than that, please visit ioSafe Inc. website www.iosafe.com/support for further assistance.