



My Cloud™ Pro Series

User Manual

- My Cloud PR2100
- My Cloud PR4100



WD Service and Support

Should you encounter any problem, please give us an opportunity to address it before returning this product. Most technical support questions can be answered through our knowledge base or email support service at <http://support.wdc.com>. If the answer is not available or if you prefer, please contact WD at the best telephone number shown below.

Your product includes 30 days of free telephone support during the warranty period. This 30-day period starts on the date of your first telephone contact with WD Technical Support. Email support is free for the entire warranty period and our extensive knowledge base is available 24/7. To help us keep you informed of new features and services, remember to register your product online at <http://register.wd.com>.

Accessing Online Support

Visit our product support website at <http://support.wdc.com> and choose from these topics:

- **Downloads**—Download drivers, software, and updates for your WD product.
- **WD Support Portal**—Register your WD products and get support information customized to your needs.
- **Warranty & RMA Services**—Get warranty, product replacement (RMA), RMA status, and data recovery information.
- **Knowledge Base**—Search by keyword, phrase, or Answer ID.
- **Documentation**—Get manuals, installation guides, and documentation for your WD product.
- **WD Community**—Share your thoughts and connect with other WD users
- **Online Learning Center**—Start here to get the most out of your My Cloud device (<http://www.mycloud.com/learn/>).

Contacting WD Technical Support

When contacting WD for support have your WD product serial number, system hardware, and system software versions available.

North America		Europe (toll free)*	00800 ASK4 WDEU (00800 27549338)
English	800.ASK.4WDC (800.275.4932)	Europe	+31 880062100
Spanish	800.832.4778	Middle East	+31 880062100
Mexico	001 8002754932	Africa	+31 880062100
South America		Russia	8 10 8002 335 5011
Chile	1230 020 5871	Asia Pacific	
Colombia	009 800-83247788	Australia	1800 429 861 / 0011 800 2275 4932
Venezuela	0800 100 2855	China	800 820 6682 / 400 627 6682
Peru	0800 54003	Hong Kong	3057 9031
Uruguay	00 413 598 3787	India	1800 200 5789 / 1800 419 5591
Argentina	0800 4440839	Indonesia	001 803 852 3993
Brazil	0800 7704932 0021 800 83247788	Japan	0800 805 7293
		Korea	02 2120 3415
		Malaysia	1800 817 477
		New Zealand	0508 555 639 / 00800 2275 4932
		Philippines	1800 1855 0277
		Singapore	1800 608 6008
		Taiwan	0800 225 593
		Thailand	00 1800 852 5913
		Other countries	+86 21 2603 7560

* Toll free number is available in the following countries: Austria, Belgium, Czech Republic, Denmark, France, Germany, Ireland, Italy, Netherlands, Norway, Poland, Slovakia, Spain, Sweden, Switzerland, United Kingdom.

Registering Your WD Product

Register your WD product to get the latest updates and special offers. You can easily register your drive online at <http://register.wd.com> or by using My Cloud device software.

Table of Contents

WD Service and Support	ii
Registering Your WD Product	iii
1 Important User Information	1
Important Safety Instructions	1
Recording Your WD Product Information	2
2 Product Overview	3
Package Contents	3
Requirements	3
Product Components	4
Pre-installation Instructions	8
Handling Precautions	8
3 Getting Started	9
Preparing your My Cloud Device for Use	9
Getting Started with My Cloud Online Setup	11
Getting Started without My Cloud Online Setup	11
Accessing Content	14
4 The Dashboard at a Glance	16
Launching the Dashboard	16
The Dashboard Home Page	17
Common Tasks	27
5 Managing Users and Groups	29
About Users	29
About Groups	34
6 Managing Shares	37
About Shares	37
7 Accessing Your Cloud Remotely	40
Enabling Cloud Access for the My Cloud Device	40
Configuring Cloud Access for a User	40
Access Your Files with iOS and Android Mobile Apps	41
8 Backing Up and Retrieving Files	43
About Backups	43
Managing a USB Device and USB Backups	43

Remote Backups	46
Internal Backups	47
Viewing Backup Details	48
Modifying a Backup Job	48
Deleting a Backup Job	48
Cloud Backups	49
Camera Backups	51
9 Managing Storage	53
About Storage	53
RAID Storage	53
Disk Status	55
iSCSI Storage	56
Volume Virtualization	58
10 Managing Apps	60
About Apps	60
Managing Apps	60
11 Playing/Streaming Videos, Photos, & Music	62
Media Servers	62
Media Storage	64
Enabling DLNA and iTunes	64
Accessing Your My Cloud Device Using Media Players	66
Accessing Your My Cloud Device Using iTunes	67
12 Configuring Settings	68
General	68
Network	75
Media	84
System Diagnostics	86
Notifications	91
Firmware Update	93
13 Regulatory Information	96
Regulatory Compliance	96
14 Appendices	98
Appendix A: My Cloud Quick User Guide	98
Appendix B: Safe Mode Firmware Update Procedures	101
Appendix C: My Cloud Action Icons	102
Appendix D: My Cloud Device URLs and Names	104
Appendix E: Creating a User Import File	105

Appendix F: Replacing the SO-DIMM Memory Module 107

15 Index 109

Important User Information

[Important Safety Instructions](#)
[Recording Your WD Product Information](#)

Important Safety Instructions

This device is designed and manufactured to assure personal safety. Improper use can result in electric shock or fire hazard. The safeguards incorporated into this unit will protect you if you observe the following procedures for installation, use, and servicing.

- Follow all warnings and instructions marked on the product.
- Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
- Do not use this product near any liquids.
- Do not place this product on an unstable surface. The product may fall, causing serious damage to the product.
- Do not drop the product.
- Do not block the slots and openings on the top and bottom of the chassis; to ensure proper ventilation and reliable operation of the product and to protect it from overheating, these openings must not be blocked or covered. Making sure the drive is standing upright also helps prevent overheating.
- Operate this product only from the type of power indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- Do not allow anything to rest on the power cord. Do not locate this product where persons will walk on the cord.
- If an extension cord is used with this product, make sure that the total ampere rating of the equipment plugged into the extension cord does not exceed the extension cord ampere rating. Also, make sure that the total rating of all products plugged into the wall outlet does not exceed the fuse rating.
- Never push objects of any kind into this product through the chassis slots as they may touch dangerous voltage points or short out parts that could result in a fire or electric shock.
- Unplug this product from the wall outlet and refer servicing to qualified service personnel under the following conditions:
 - When the power cord or plug is damaged or frayed.
 - If liquid has been spilled on the product.
 - If the product has been exposed to rain or water.
 - If the product does not operate normally when the operating instructions are followed. Adjust only those controls that are covered by the operating instructions since improper adjustment may result in damage and require extensive work to the product by a qualified technician to restore the product to normal condition.
 - If the product has been dropped or the chassis has been damaged.
 - If the product exhibits a distinct change in performance, contact WD Customer Support at <http://support.wdc.com>.

Recording Your WD Product Information

Remember to write down the following WD product information, which is used for setup and technical support. Your WD product information is found on the label on the back of the device.

- Serial Number
- Model Number
- Purchase Date
- System and Software Notes

2

Product Overview

- [Package Contents](#)
- [Requirements](#)
- [Product Components](#)
- [Pre-installation Instructions](#)
- [Handling Precautions](#)

Package Contents

- My Cloud device
- Shielded Ethernet cable
- AC power adapter
- Quick Install Guide

For information on additional accessories for this product, visit:

US	www.shopwd.com or www.wdstore.com
Europe	www.shopwd.eu or www.wdstore.eu
All others	Contact WD Technical Support at http://support.wdc.com/contact.aspx , and click on Change country for technical contacts in your region.

Requirements

Operating System

Windows®

- Windows 10
- Windows 8.1
- Windows 8
- Windows 7

Mac OS X®

- El Capitan (Mac OS 10.11)
- Yosemite (Mac OS 10.10)
- Mavericks (Mac OS 10.9)
- Mountain Lion (Mac OS 10.8)

Note: Compatibility may vary depending on your computer's hardware configuration and operating system.

Web Browsers

- Internet Explorer 10.0 and later on supported Windows computers.
- Safari 6.0 and later on supported Windows and Mac computers.
- Firefox 30 and later on supported Windows and Mac computers.
- Google Chrome 31.0 and later on supported Windows and Mac computers.

Local Network

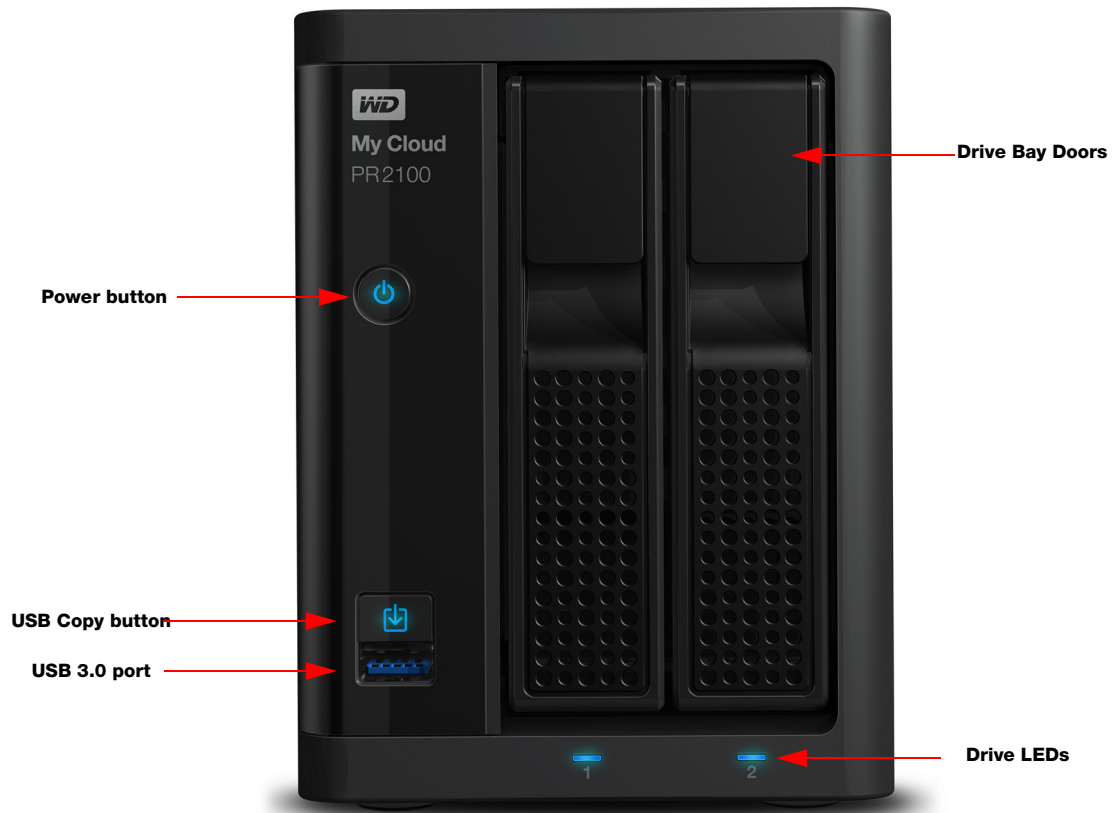
- Router/switch (Gigabit is recommended to maximize performance.)

Internet

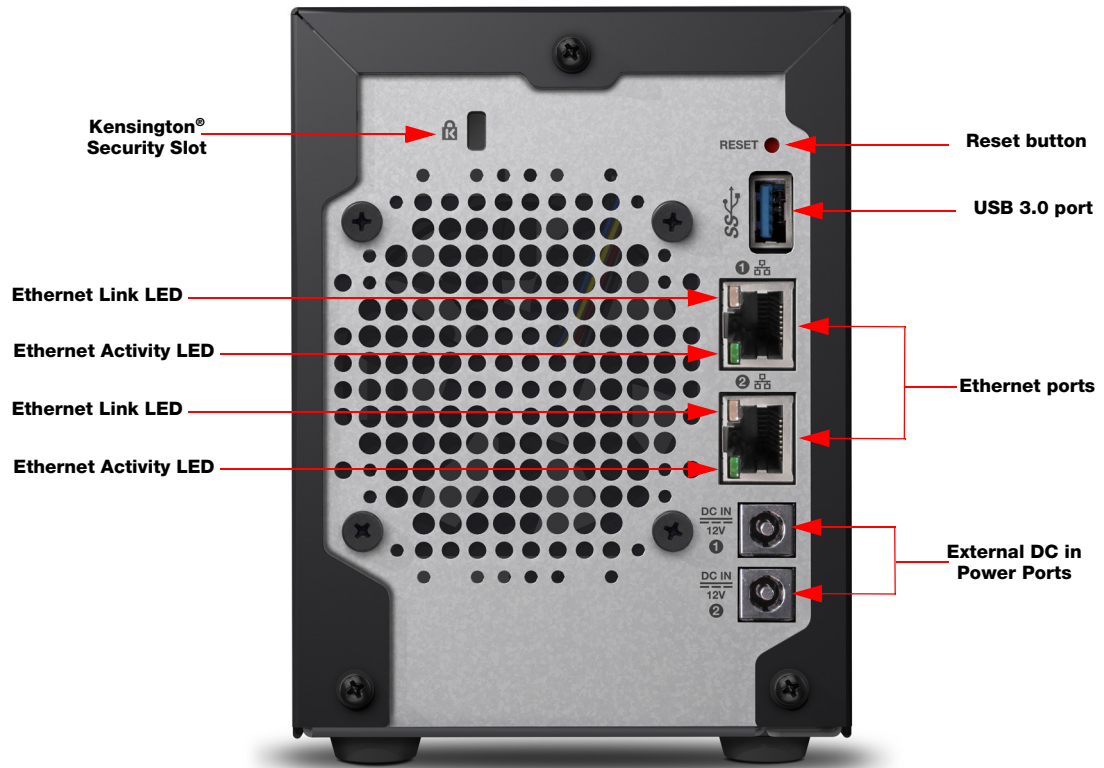
- Broadband Internet connection is required for initial setup and software downloads, as well as for remote access and mobile apps.

Product Components

2-Bay Front View (My Cloud PR2100)



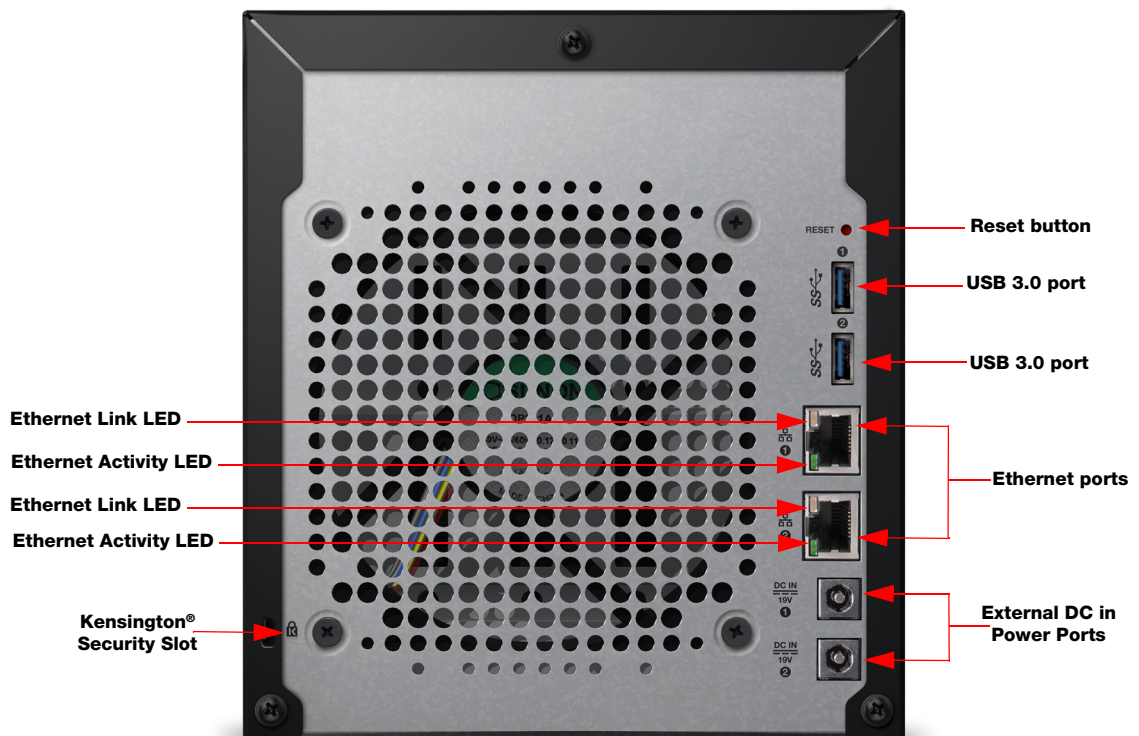
2-Bay Back View (My Cloud PR2100)







4-Bay Front View (My Cloud PR4100)



4-Bay Back View (My Cloud PR4100)



Back View Icons

Component	Icon	Description
Ethernet port		Connects the device to a local network.
USB 3.0 port		Connects to a USB hard drive for additional storage.
Reset button	()	Restores settings and administrator password for the device. Visit http://support.wdc.com , and see Knowledge Base Answer ID 10432.
Power port		Connects the device to an AC adapter and the power outlet.
Kensington security slot		For device security, the device is equipped with a security slot that supports a standard Kensington security cable. Visit http://www.kensington.com/ for more information.

LEDs

Front Panel Power LED

The following table describes the front panel power LED behavior.

State	Color	Appearance	State Description
Power Down	Not lit	N/A	Device is off.
Standby	Blue	Pulsing	Device is in standby mode.
Powering Up	Blue	Blinking	Device is powering on or in the process of updating the firmware.
Power Up	Blue	Solid	Device is in a powered up state.
Device at fault	Red	Blinking	Device at fault, such as system hang.
Action required	Red	Solid	A condition, such as a network cable having become unplugged, which requires you to act.

Back Panel Ethernet (Network) LEDs

The following table describes the network and activity LEDs:

Note: Looking at the Ethernet port with the cable latch on top, the top-right LED is the Link LED, and the top-left LED is the Activity LED.

State	LED	Appearance	State Description
Link down	Link	Off	Cable or device is not plugged in, or other end of link is not operational.
Link up – 10/100 Mbps connection	Link	Yellow	Cable is plugged in, and both ends of the link have successfully established communications. 10/100 Mbps network connection.
Link up – 1000 Mbps connection	Link	Green	Cable is plugged in, and both ends of the link have successfully established communications. 10/100/1000 Mbps network connection.
Link idle	Activity	Solid	Active communication is not in progress.
Link busy	Activity	Green - Blinks	Active communication is in progress.

Pre-installation Instructions

Before beginning installation, select a suitable location for your device to obtain maximum efficiency. Place it in a location that is:

- Near a grounded power outlet.
- Clean and dust free.
- On a stable surface free from vibration.
- Well ventilated, with nothing blocking or covering the slots and openings.
- Away from fields of electrical devices such as air conditioners, radio, and television receivers.

Handling Precautions

WD products are precision instruments and must be handled with care during unpacking and installation. Rough handling, shock, or vibration can damage the device drives. Observe the following precautions when unpacking and installing your external storage product:

- Do not drop or jolt the device.
- Do not move the device while it is powered on.
- Do not use this product as a portable device.
- Do not remove both data drives at the same time. This will cause your device to become unresponsive.

3

Getting Started

- [Preparing your My Cloud Device for Use](#)
- [Getting Started with My Cloud Online Setup](#)
- [Getting Started without My Cloud Online Setup](#)
- [Accessing Content](#)

It's easy to set up the My Cloud device—just unpack your device, connect it, and wait for the Power LED on the front of your device to turn a solid blue. Then setup your device from your web browser.

Note: For information about safely shutting down and disconnecting the device, see “Logging Out and Shutting Down your Device” on page 27.

Preparing your My Cloud Device for Use

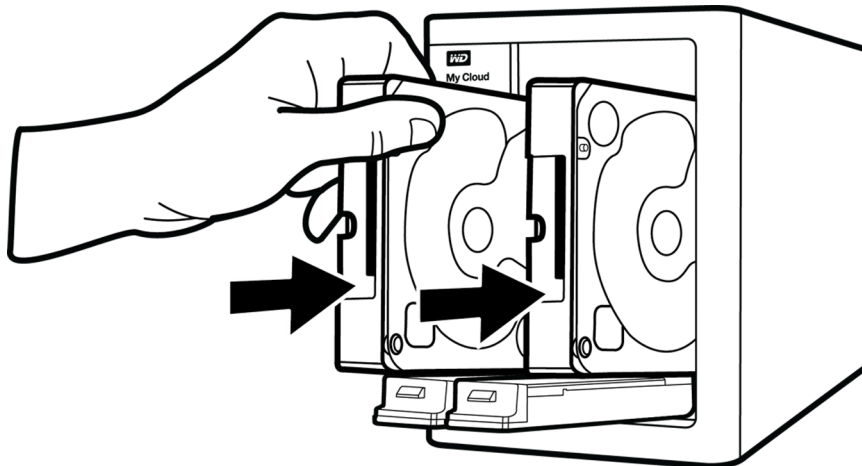
There are a few steps you need to take in order to get your My Cloud device up and running. Follow the steps outlined below to prepare your device for use.

Adding a Hard Disk Drive to your Device (Diskless Drives)

Use the following steps to install the hard disk drive(s) in your My Cloud device.

Note: If your My Cloud device came with the drive(s) pre-installed, continue to “Physically Connecting your Device” on page 10.

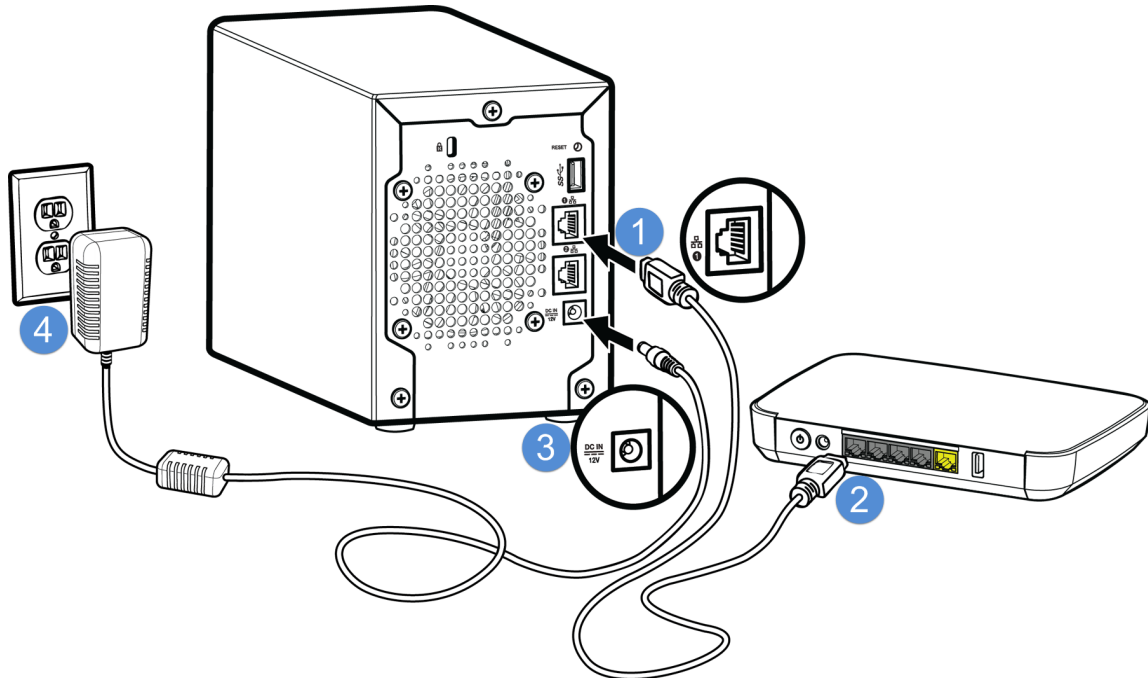
1. Pull the handle on the front of the hard disk drive toward you.
2. Slide the approved hard disk drive into the drive bay, making sure that it is properly seated and is facing the correct direction.



3. Using some force, snap the hard disk drive handle shut.
4. Follow steps 1 through 3 for all hard disk drives on your device.

Note: After the My Cloud device is physically connected, the drive LEDs on the front of the device will be solid red until new volumes are created. For more information, see “Physically Connecting your Device” on page 10 and “RAID Storage” on page 53.

Physically Connecting your Device



Follow the steps below to connect the My Cloud device to a home or small office network.

Important: To avoid overheating, make sure the device is upright as shown in the illustration above and nothing is blocking or covering the slots and openings on the top and bottom of the device. In the event of overheating, the device will perform a safe shutdown, interrupting all processes currently being performed. If this occurs, data may be lost.

Important: The provided shielded Ethernet cable must be used between the unit and network connection to comply with FCC Part 15 Class B and EN-55022/EN-55024 Class B.

1. Using the Ethernet cable, connect one end of the Ethernet cable to the Ethernet port located on the back of the device.
2. Connect the other end of the Ethernet cable directly into a router or network switch port.
3. Connect one end of the power adapter into the power supply socket on the back of the device.
4. Plug the other end of the power adapter into a power outlet. The unit powers up automatically.

Important: Wait for the My Cloud device to finish powering up (approximately three minutes) before configuring it. You will know it is ready when the power LED stops blinking and turns a solid blue.

5. When the power LED on your device turns a solid blue, continue to Getting Started with My Cloud Online Setup.

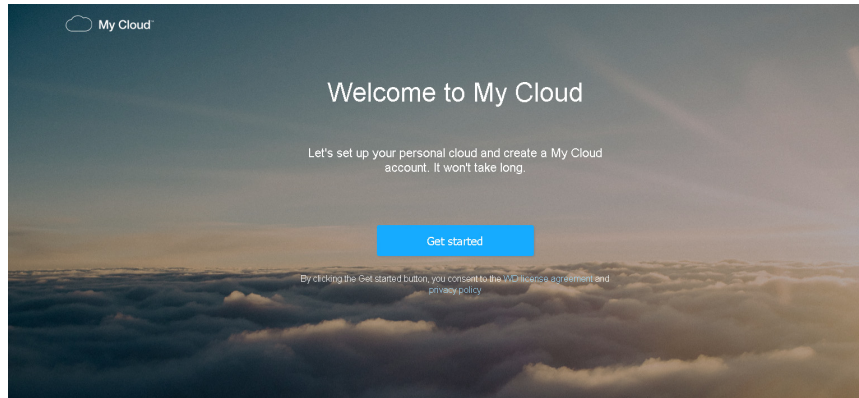
Getting Started with My Cloud Online Setup

The online setup process walks you through the steps necessary to easily connect your My Cloud device to your home or small office network. Use the following steps to run the online setup process, discover the device, and get started using your device.

My Cloud Device Online Setup

After connecting your device:

1. Open a web browser and type <http://mycloud.com/setup> to display the welcome page.



2. On the Welcome page, click Get Started.
The setup function begins searching for your My Cloud device.
3. Follow the on-screen instructions to complete the setup process.

Note: To keep all of your My Cloud content synchronized to your network-attached devices, download the WD Sync app at http://www.mycloud.com/learn/#mc_download.

Getting Started without My Cloud Online Setup

Use the following steps to set up your device using your web browser (for browser requirements, see “Web Browsers” on page 3).

If you choose not to set up the network attached storage (NAS) for your device, you can still:

- Configure the device using the My Cloud dashboard. (See “The Dashboard at a Glance” on page 16.)
- Use your My Cloud device as an external hard drive, dragging and dropping files to and from it. (See “Accessing Content” on page 14.)
- Back up files using USB, Remote, Internal, Cloud, and Camera backup. (See “Backing Up and Retrieving Files” on page 43.)

1. Open a browser and enter your device URL as listed below, then click **Enter**.

Note: If you changes your device name at any time, the URL also change to the new name.

If your device name is...	Your Windows URL is...	Your Mac URL is...
My Cloud PR2100	http://mycloudPR2100	http://mycloudPR2100.local
My Cloud PR4100	http://mycloudPR4100	http://mycloudPR4100.local

The login page appears:

2. Click **Login**. You do not need to enter a password because you haven't set one up yet. The Choose your language screen appears:

3. From the drop-down list, select the language you'd like to use for the user interface.
4. Click the Western Digital End User License Agreement link to read the Western Digital End User License Agreement.
 - If you agree, click **I accept** or return to the previous page and click the **I agree** check box.
5. Click **Continue**. The Getting Started screen appears.

6. Enter a password in both the Password and Confirm Password fields.
 - If you do not wish to create a password at this time, leave both fields blank.

7. Click **Next**. The Setup Cloud Access page appears.

The screenshot shows a dialog box titled "Getting Started" with the following content:

WD My Cloud PR2100 lets you create your personal cloud. Store your photos, videos, music, and files in one place, and access your content anywhere. Access requires a MyCloud.com account, and each user needs one.

Setup Cloud Access

admin First Name Last Name Email Address

If you do not wish to add other users now, click **Next** to continue.

Back Cancel Next

8. Enter your first name, last name, and email address, then click **Save**. The email address is needed if you want to create an account with remote access capability.

- If you'd like to enter additional user accounts:
 - Enter the user name, first name, last name, and email address for the new user account, then click **Save**.

Note: If you entered an email address, ensure that the user checks their email account. They will receive an email with instructions on how to set up and activate a password for cloud access.

- Continue the above step for all user accounts you'd like to add.

Note: The My Cloud app provides free remote access to your personal cloud device. Once you create your account, you can access your device using your mobile devices with Internet access and from the My Cloud desktop app.

9. Click **Next**. The following Getting Started screen appears:

The screenshot shows a dialog box titled "Getting Started" with the following content:

Enhance your WD Experience

Auto Update Firmware **ON** [Info]

Product Improvement Program **ON** [Info]

Register your Product

Registering your product helps register your warranty & sets you up to receive updates about your product.

First Name* Last Name* Email Address*

Back Cancel Next

10. Do the following:

- To have your device's firmware updated automatically, set the **Auto Update Firmware** toggle button to ON (optional).
- To participate in the Product Improvement Program, set the Product Improvement Program toggle button to ON (optional).
- To register your device, enter your First Name, Last Name, and Email Address.


11. Click **Finish** to display the My Cloud dashboard. For instructions on using the dashboard, see "The Dashboard Home Page" on page 17.

Accessing Content

The My Cloud device's Public folder contains Shared Music, Shared Pictures, and Shared Videos subfolders. The existing content of the subfolders are files that you dragged and dropped or files that have been backed up from your computer or an attached USB drive.

Note: Any of the folders can hold any file type.

Once you've physically connected your My Cloud device (see "Preparing your My Cloud Device for Use" on page 9), use the following steps to access the contents of your device.

If your operating systems is...	Then...
Windows 8 / Windows 8.1 / Windows 10	<ol style="list-style-type: none"> 1. On the Start page, type Computer. 2. Click Computer. 3. In the left pane, click Network. 4. Double-click the My Cloud device (see "Appendix D: My Cloud Device URLs and Names" on page 104 for a list of device names) and locate the device's Public folder. 5. Double-click the Public folder to display the Shared Music, Shared Pictures, and Shared Videos subfolders. You can now drag and drop files into (and from) the shared media folders using Windows Explorer.
Windows 7	<ol style="list-style-type: none"> 1. Click  or Start > Computer > Network > My Cloud device (see "Appendix D: My Cloud Device URLs and Names" on page 104 for a list of device names) and, if required, enter your share credentials. The device's Public and private folders (shares) appear. 2. Double-click the Public folder to display the Shared Music, Shared Pictures, and Shared Videos subfolders. You can now drag and drop files into (and from) the shared media folders using Windows Explorer.

If your operating systems is...	Then...
Mac OS X (El Capitan, Yosemite, Mavericks, Mountain Lion)	<ol style="list-style-type: none"> 1. In a Finder window, click the My Cloud device (see “Appendix D: My Cloud Device URLs and Names” on page 104 for a list of device names) under the shared items in the side bar. 2. If presented with an authorization page, enter your Username and password or select Guest and click Connect to display the Public share. 3. Double-click the Public folder to display the subfolders: Shared Music, Shared Pictures, and Shared Videos. You can now drag and drop files into the shared folders using Finder. 4. If you want to create a shared drive icon permanently on your desktop, create an alias. There are two ways to do this: <p>Note: Before creating an alias, click Finder > Preferences > General and make sure Connected Servers is checked.</p> <ul style="list-style-type: none"> - Click the item you wish to alias (e.g., Shared Music), hold down the mouse button, hold down the Cmd and Option keys simultaneously, then drag the item to where you’d like to make an alias. Instead of moving the original item, this action creates an alias at the new location. <p style="text-align: center;">- OR -</p> <ul style="list-style-type: none"> - Right-click the item you want to alias (e.g., Shared Music) and click File > Make Alias.

Mapping the Public Folder (Windows)

To map the My Cloud Public folder for quick access in the future:

1. In Windows Explorer, under Network, click the My Cloud device (see “Appendix D: My Cloud Device URLs and Names” on page 104 for a list of device names).
2. Right-click the Public folder and select **Map Network Drive** from the menu.
3. Select an available letter from the **Drive** drop-down list.
4. Select the **Reconnect at login** check box.
5. Click **Finish**. Your Public drive is now mapped.

4

The Dashboard at a Glance

[Launching the Dashboard](#)
[The Dashboard Home Page](#)
[Common Tasks](#)




Use the My Cloud dashboard to configure settings and to manage the device. For example, you can set up user accounts and restrict access to the files on your My Cloud device, set up folders for storing files, enable remote access, and customize the device to suit your needs.

Note: If this is the first time you are opening the dashboard, see “Getting Started without My Cloud Online Setup” on page 11.

Launching the Dashboard

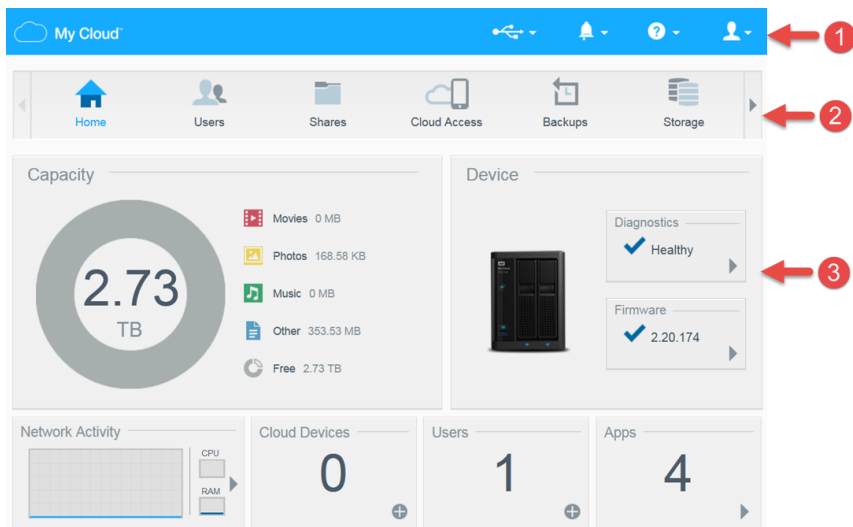
Use one of the following methods to launch the dashboard.

IF you want to launch from . . .	THEN . . .
A web browser or Windows Explorer	<p>Using Device Name:</p> <ol style="list-style-type: none"> Enter the name of your My Cloud device in the browser’s address field (see “Appendix D: My Cloud Device URLs and Names” on page 104 for a list of device names): <ul style="list-style-type: none"> http://<device name> (Windows) (Example: http://mycloudPR2100) http://<device name>.local (Mac) (Example: http://mycloudPR4100.local) Click Go. <p>Using IP Address:</p> <ol style="list-style-type: none"> Enter the IP address of your My Cloud device in the browser’s address field: http://<IP Address>. <ul style="list-style-type: none"> For My Cloud PR2100, click Settings, then click Network. The IP address is displayed in the Network Profile area. For My Cloud PR4100, on the front of the device, click the down button to the right of the Status LCD display. The IP address appears in the Status LCD display. Or, click Settings, then click Network. The IP address is displayed in the Network Profile area. Click Go.

IF you want to launch from . . .	THEN . . .
Windows 8 / Windows 8.1 / Windows 10	<ol style="list-style-type: none"> 1. On the Start page, type Computer. 2. Click Computer. 3. In the left pane, click Network. 4. In the right panel, locate your My Cloud device under Storage. 5. Double-click the device, or right-click and select View device webpage from the resulting menu.
Windows 7	<ol style="list-style-type: none"> 1. Click  > Computer. 2. In the left panel, select Network. 3. In the right panel, locate your My Cloud device under Storage. 4. Double-click the device, or right-click and select View device webpage from the resulting menu.
Mac OS X	<ol style="list-style-type: none"> 1. Click the Safari icon  > bookmark icon  > Bonjour. 2. Double-click the My Cloud device on the network.
Mobile Devices	<p>iOS Devices:</p> <ol style="list-style-type: none"> 1. Open a browser. 2. In the Address bar, enter http://<device name>.local. <p>Android Devices:</p> <ol style="list-style-type: none"> 1. Open a browser. 2. In the Address bar, enter http://<device name>.

The Dashboard Home Page

The My Cloud Home page has an information bar at the top, a navigation icon bar across the page, and an instant overview of the status of the device's main functions with links for updating settings.






-
- 1 Information Icons
 - 2 Navigation Icons
 - 3 Status and Update Panels
-

Information Icons

The Information Icons, at the top of the page, provide quick access to:








- Attached USB device(s)
- Device alerts
- Online Help and Support
- User information.

Icon	Name	Actions
	USB device attached to the My Cloud device	Click to display the USB device(s) connected.
	Alert Notifications	Click to display recent alerts about new firmware and network issues.
	Help	Click to access the My Cloud Getting Started Wizard, Help, Support, and About information.

Icon	Name	Actions
	User	Click to see the user name of the user currently logged into the My Cloud device. You can also Hibernate (Shutdown), Reboot, or Logout of the

Navigation Icons

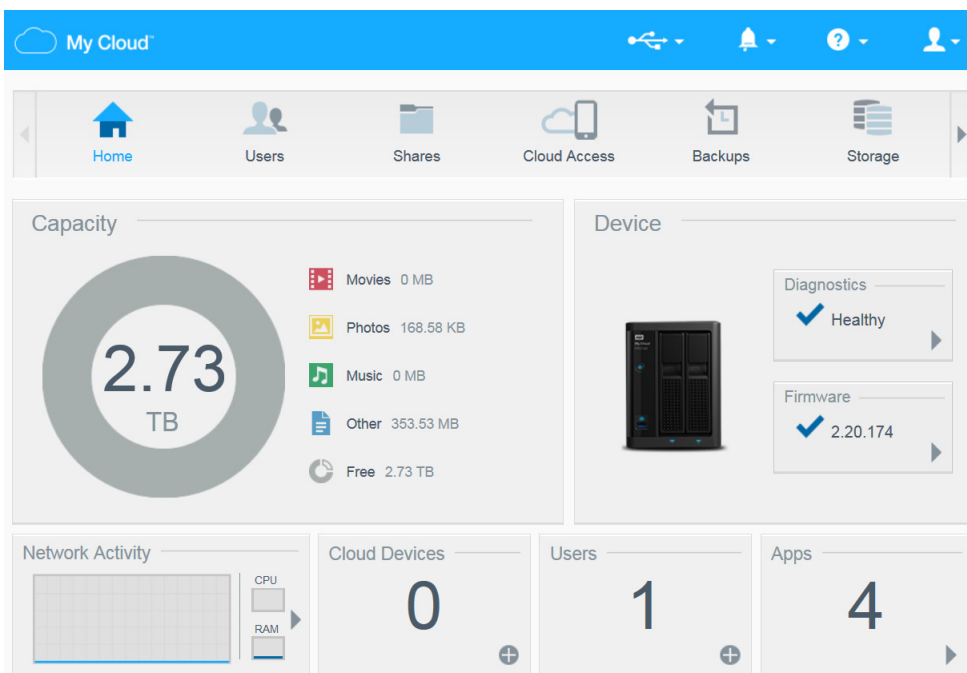
The Navigation Icons provide access to the various features and settings of your My Cloud device.

Icon	Name	Actions
	Home	An instant overview of the status of the device's main functions and provides links for updating those settings.
	Users	Create, change, and delete user accounts. Grant users full or limited access to particular shares.
	Shares	Create, change, and delete shares and grant specific user accounts full, limited, or no access to particular shares.
	Cloud Access	Set up, change, and remove remote cloud access to particular shares. Monitor remote access status.
	Backups	Create backups to: <ul style="list-style-type: none"> • A USB drive. • Another My Cloud device on or outside of your network. • Another location on your My Cloud device. • Your My Cloud device from a camera.
	Storage	Select and specify how you want the My Cloud device to store your data.
	Apps	Add or remove various apps that allow you to use your device more productively.

Icon	Name	Actions
	Settings	Configure advanced settings for your My Cloud device, including: <ul style="list-style-type: none"> • General device settings. • Network configurations. • Media options. • Device utility tasks. • Notification settings. • Firmware update settings.

Viewing Device Status and Making Updates on the Home Page

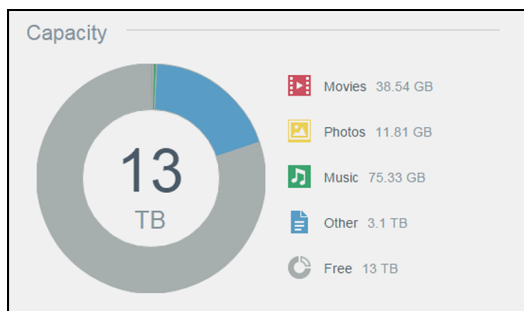
The main body of the Home page shows the status of the device and its functions and provides shortcuts to the most necessary tasks.



Capacity

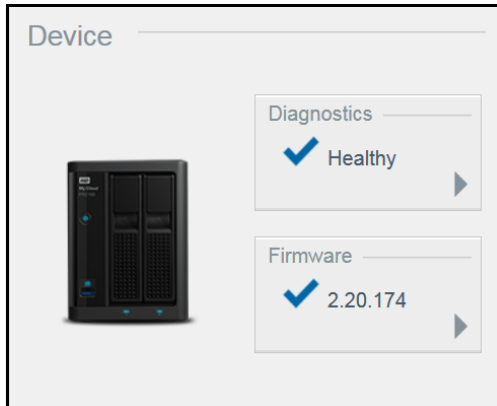
The Capacity panel displays the amount of storage remaining on your My Cloud device and how the storage is allocated.

Note: Storage allocation information only appears when the Cloud Services option is ON. See “Cloud Access” on page 71 for steps to enable Cloud Services.



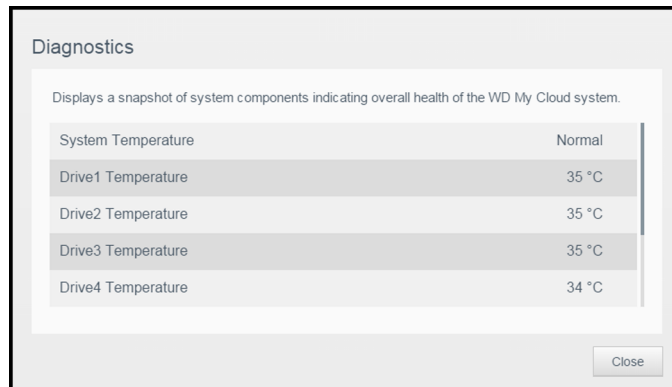
Device

The Device section identifies the overall health of the system, indicates the current version of your firmware, and informs you when firmware updates are available.



Diagnostics

The Diagnostics section displays a snapshot of the system's components and identifies the overall health of the My Cloud device.



1. To see details about the status of system's components, click the arrow in the Device area.
2. To return to the Home page, click **Close**.

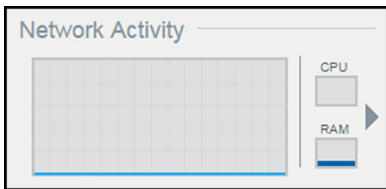
Firmware

The Firmware section displays the current firmware version loaded on your My Cloud device. A green check mark indicates that your firmware is up-to-date.

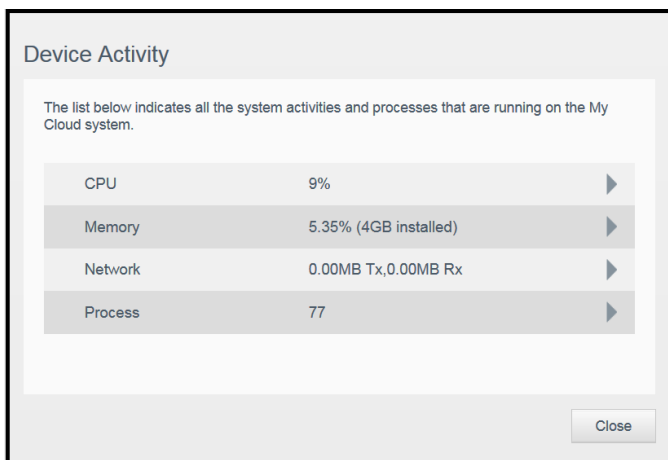
1. To view whether an updated version of the firmware is available, click the arrow to the right of Firmware to display firmware availability.
2. If an update is available, click **Install and Reboot** to update your device.
3. To return to the Home page, click **OK**.

Network Activity

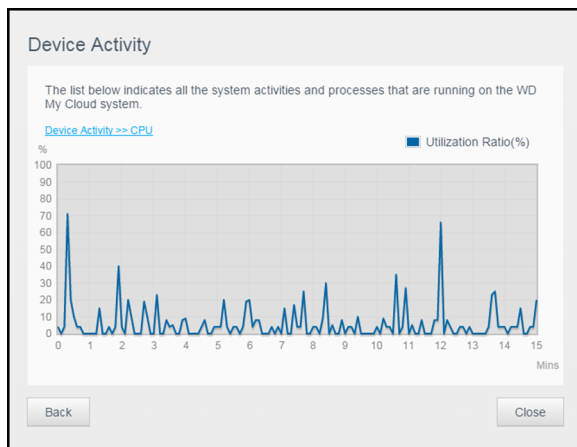
The Network Activity panel displays the system activities and processes that are running on your My Cloud device. At a glance, you can see the network, CPU, and RAM activity.



To view a list of all device activities and processes running on your My Cloud device, click the arrow in the Network Activity area.

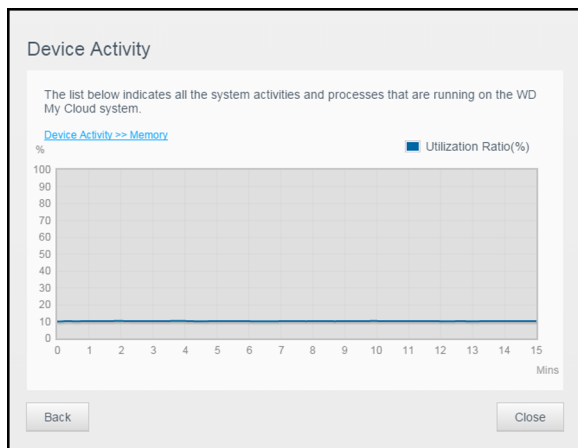


- **CPU:** In the Device Activity window, click the right arrow to view the CPU activity. Click **Back** to return to the Device Activity pane. Click **Close** to return to the Home

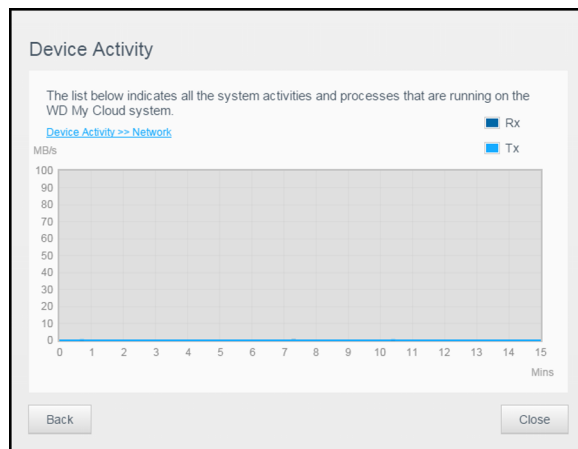


page.

- Memory:** In the Device Activity window, click the right arrow to view Memory activity. Click **Back** to return to the Device Activity pane. Click **Close** to return to the Home page.



- Network:** In the Device Activity window, click the right arrow to view the network activity. Click **Back** to return to the Device Activity pane. Click **Close** to return to the Home page.



- Process:** In the Device Activity window, click the right arrow to view the process information, including the list of active processes and the amount of CPU and Memory usage for each process. Click **Back** to return to the Device Activity pane. Click **Close** to return to the Home page.

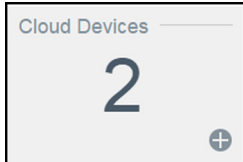
The screenshot shows the 'Device Activity' window with the 'Process' view selected. The text above the table states: 'The list below indicates all the system activities and processes that are running on the WD My Cloud system.' Below this is a link 'Device Activity >> Process'. The table below shows the following data:

Process	CPU%	Memory Usage
upnp_nas_device	0.0	6.8
httpd	0.0	4.5
httpd	0.0	4.5
httpd	0.0	4.5
httpd	0.0	4.5
httpd	0.0	4.5

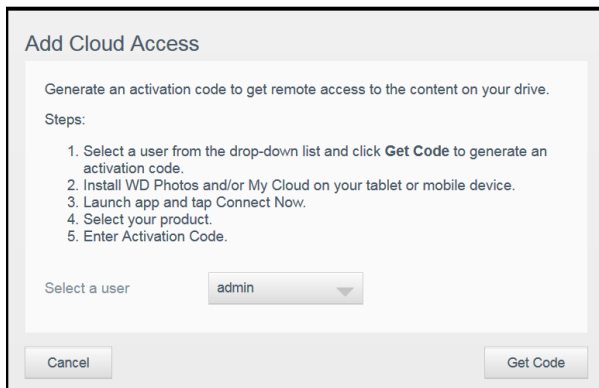
There are 'Back' and 'Close' buttons at the bottom of the window.

Cloud Devices

The Cloud Devices panel displays the number of cloud and smart devices currently accessing the My Cloud device remotely.



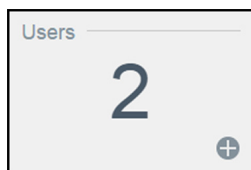
1. To add cloud access for a user, click the plus sign (+) in the lower-right area of the panel.



2. Select a user from the drop-down menu.
3. To generate an activation code for the selected user, click **Get Code**.
4. Follow the page instructions to connect your tablet or mobile device to the My Cloud device. Click OK to close.

Users

1. The Users panel displays the number of users currently set up to use the My Cloud device.



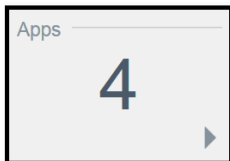
2. To add a user, click the plus (+) sign in the lower-right area of the panel.

Note: When you enter the email address on the Add User screen, a new cloud access account is created. Once created, the new user receives an email with instructions on how to set up and activate a password for cloud access.

3. Enter the required information and click **Apply**.

Apps

The Apps panel displays the apps currently installed on your My Cloud device.



To view the installed apps, click the arrow in the lower-right corner of the panel.

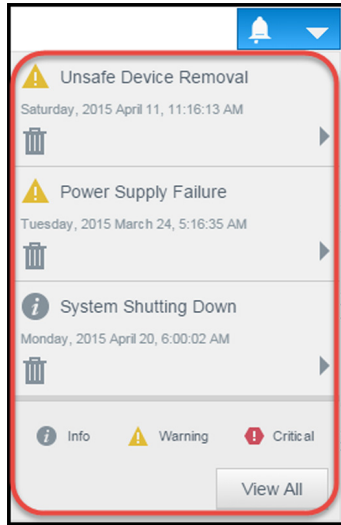
Managing Alerts

Alerts display system messages containing pertinent information about the status of your My Cloud device. Three types of alerts appear on the upper-right area of the dashboard.

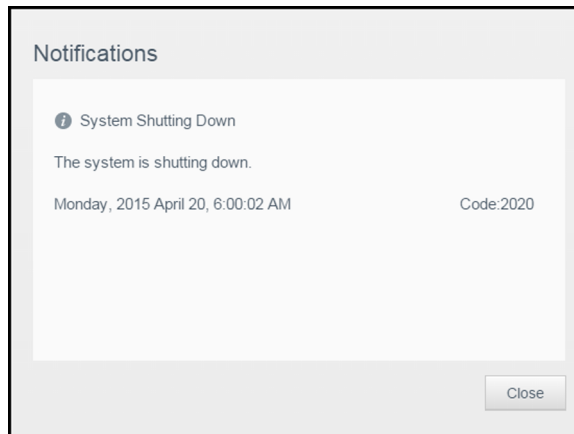
Alert Icon	Type of Alert	Description
	Informational	Informational alerts keep you updated on non-vital system information. Example: Reboot Required
	Warning	Warnings present a condition that might cause a problem in the future. Example: Network Disconnected
	Critical	This alert presents an error or problem that has occurred, usually a system failure. Example: Drive Overheating

Viewing Alert Details

1. Click the Alert icon in the upper-right corner of the screen.
2. From the Alert list, click the arrow next to the alert you'd like to view, or click **View All** to review details for all of your alerts.



- To view alert details, click the arrow next to the alert.



- To close the alert message, click **Close**.

Dismissing an Alert

1. Click the Alert icon in the upper-right corner of the screen.
2. Select the Delete icon to the left of the alert you want to dismiss.
3. To dismiss all alerts, click **View All**, then click **Dismiss All**.

Obtaining Customer Support

To open the Support page:

1. Click the **Help** icon on any page to display the Help menu.

2. Click **Support** to display the following page:

If a problem occurs with the My Cloud device, WD Technical Support needs information about your device to troubleshoot and determine the best solution. There are two ways to get your device information and request support:

- Run a system report and send it to WD automatically.
- Create a system report manually and send it to WD.

The Support page is also where you can help improve WD products by participating in the Product Improvement Program.

Requesting Automated Support

In the Request Automated Customer Support section:

1. Click the **Privacy Policy** link to review WD's privacy policy.
2. Click the **Attach my device's diagnostic report and request support** check box.
3. Click the **Request Support** button.

Creating and Saving a System Report

1. In the Create and Save System Report section, click **Create and Save**. This saves the file to your computer.
2. If desired, email the report to WD Technical Support.

Product Improvement Program

Participating in WD's Product Improvement Program helps us improve our products. Use the following steps to participate in the Product Improvement Program.

1. In the Product Improvement Program area, review the information on the screen.
2. Click the toggle button to turn on the Product Improvement Program.

Obtaining Other Support

The Support Resources section contains links to additional resources.

- To obtain the most recently updated user manual, click the **Product Documentation** link.
- To see answers to frequently asked questions and instructions, click the **FAQs** link.
- To discuss your My Cloud device with other users, click the **Forum** link.
- To see WD phone numbers and other contact information, click the **Contacts** link.

Logging Out and Shutting Down your Device

Shutting down the Device

Use the following steps to safely shut down your My Cloud device.

1. Click the User icon in the upper-right corner of the screen.
2. Click **Hibernate**.
3. Review the confirmation message, then click **OK**. Your My Cloud safely shuts down.

Note: You can also shut down your My Cloud device by holding the power button on the front of the device for approximately 4 seconds and then releasing it.

Rebooting the Device

1. Click the User icon in the upper-right corner of the screen.
2. Click **Reboot**.
3. Review the confirmation message, then click **OK**. Your My Cloud safely reboots.

Logging Off of your Device

1. Click the User icon in the upper-right corner of the screen.
2. Click **Logout**. Your My Cloud logs you out of the device.

Common Tasks

The next few chapters step you through the procedures for configuring and using the My Cloud device. The following table provides shortcuts to instructions for some common tasks.

How do I ...	See ...
Set up the My Cloud device on my network	page 11
Use media servers	page 62
Enable DLNA (Digital Living Network Alliance) and iTunes	page 64
Shut down or reboot the My Cloud device	page 28 & 88
Update firmware	page 94
Access content from the device (public and private shares)	page 14
Add users	page 29
Create shares	page 38
Upload and back up content to the device	page 43

How do I ...	See ...
Back up the device	page 43
Enable or disable remote access for you and people you want to share with	page 40
Download WD mobile apps	page 41
Manage storage within your device	page 53

5

Managing Users and Groups

[About Users](#)
[About Groups](#)

About Users

The Administrator, normally the device owner, is the person in charge of setting up the device. As the My Cloud device owner, you have a special user account (admin) that provides you with admin privileges. With these privileges, you can set up and configure the device to your specific needs and add other users to your personal cloud. You also have the power to determine exactly what users can access on the device.

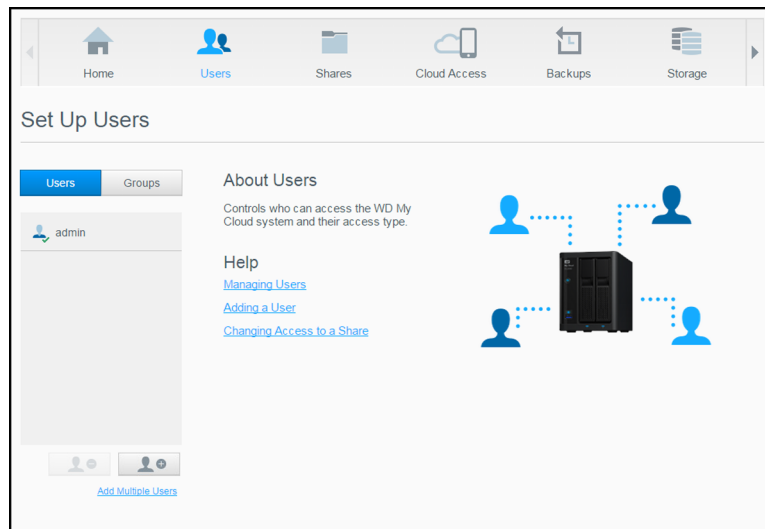
As a default, admin user name does not have a password. You can create one at anytime (see “Updating a User Password” on page 32).

Note: Only one individual at a time can use the Admin logon ID to log into the web browser app. Because of this, ensure that you log out of the My Cloud device web browser app when you are not using it. This allows other users authorized to use the Admin logon ID to access the web browser app. See “Energy Saver” on page 72 to automatically log out of the app after a set amount of time.

The Users screen displays a list of the current users and allows the Administrator to view user details, create new users, create groups, and grant a user access to existing shares and groups.

Viewing Users

1. On the Navigation bar, click **Users** to display the Set Up Users screen.



2. To view user details, click a user name in the left pane. The user’s profile and share access information appear. A user can have read only, read/write, or no access privileges assigned to a share. See “About Shares” on page 37 for additional information on shares.

Note: In the Share Access section, the shares that don’t require access permission are grayed out. Once you make a share private, the share appears in the list and you can be edited. (See “Editing Share Settings” on page 38.)

Adding a Single User

The Admin adds user accounts and sets the parameters of the shares that a user can access. Use the following steps to add a single user account.

Note: You can add up to 512 users to your device.

1. To add a user, click the **Add User** icon in the lower-left side of the screen.
2. Enter the user information on the screen, then click **Apply**.

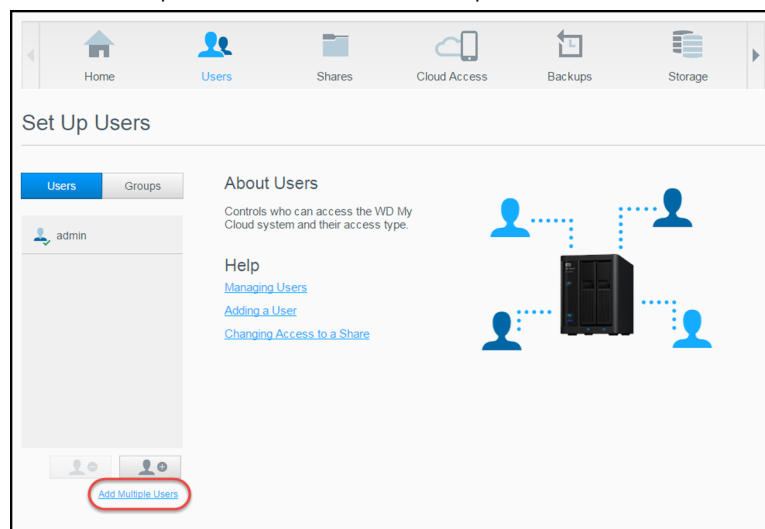
The system updates, and the new user account is created and appears on the screen.

Note: When you enter the email address on the Add User screen, a new cloud access account is created. Once created, the new user receives an email with instructions on how to set up and activate a password for cloud access.

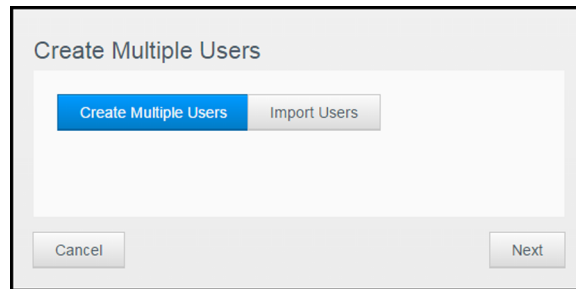
Adding Multiple Users

Use the following steps to add multiple user accounts.

1. To add multiple users, click Add Multiple Users in the lower-left side of the screen.



2. Select an option, then click **Next**.
 - **Create Multiple Users:** Allows you to enter users manually. See “Creating Multiple Users” on page 31.
 - **Import Users:** Allows you to import a list of users into the device. Continue to “Import Multiple Users” on page 31.



Creating Multiple Users

1. Enter the following information on the Create Multiple Users screen, then click **Next**:
 - **User Name Prefix:** Enter a prefix for your user name. This will be added to the Account Prefix to create the User Name (Example: HR).
 - **Account Prefix:** Enter a numeric account prefix. This will be added to the User Name Prefix to create the User Name (Example: 143).
 - **Number of Users:** Enter the number of user accounts you’d like to create. The maximum number you can add appears to the right.
 - **Password:** Enter a password for the user accounts.
 - **Confirm New Password:** Confirm the password for the user accounts.
 - **Overwrite Duplicate Accounts** (optional): Select this check box to overwrite any existing duplicate accounts on your device.
2. To assign the new users to a group, click the check box next to a group, then click **Next**.
3. Enter the Quota Amount or leave the value blank for unlimited space, then click **Next**. (See “User Quotas” on page 32.)
4. Your new user accounts appear on screen. Click **Apply** to save them to your device.

Import Multiple Users

1. Click **Download** to download a .txt file identifying the format you’ll need to set up your user import file.
2. Create and save your import file. For details on how to create and format your user import file, see “Appendix E: Creating a User Import File” on page 105.
3. Select Overwrite Duplicate Accounts to exclude user list duplications.
4. Click **Import User List** and select the import file you created.
5. Click **Next**.
6. Review your imported user list, then click **Apply**.
Your new user accounts save to your personal cloud.

Editing User Settings

1. On the Set Up Users screen, select the user whose information you want to edit. The User Profile and Share Access panels appear.
2. Modify the required and optional settings, as desired.
3. Assign an access level for private shares in the Share Access area. (See “Making a Share Private” on page 39 for information on creating a private share.)

Updating a User Password

When viewing details about a user, the Admin can add or change the user’s password (no password is the default setting).

Use the following steps to update a user password.

1. On the Set Up Users screen, select a user from the list in the left pane.
2. In the User Profile area, click the toggle button if no password has been previously created, then continue to Step 4 below.
3. Click **Configure** to the right of the toggle button if you’d like to edit an existing password.
4. Enter the new password in both the Password and Confirm Password fields.

The screenshot shows a dialog box titled "Edit Password". It has two text input fields: "New Password *" and "Confirm Password *". Below the fields, there is a small asterisk and the text "* Password required". At the bottom of the dialog, there are two buttons: "Cancel" on the left and "Apply" on the right.

5. Click **Apply**.

Assigning a User to a Group

Use the following steps to assign a user account to a user group. See “About Groups” on page 34 for information about User Groups.

1. On the Set Up Users screen, select a user from the left pane.
2. In the Group Membership field, click **Configure**.
3. Select the check box next to the group you’d like the user to join, then click **Apply**.

User Quotas

A quota determines the amount of disk space allocated to the user on the My Cloud device. Provided below are the rules for assigning user quotas and the steps to assign a quota to a user account.

Quota Rules

Assigning user quotas allows you to better control the disk space allocated to a user or a group. There are various rules dictating which quota takes precedence over another.

Note: If user permissions and group permissions differ, the most restrictive permission takes precedence.

- A User quota must be less than or equal to the group quota (e.g., if your group has a 20 GB quota and you try to set the user quota to 30 GB quota, you will be prompted to reduce your user quota to be equal to or less than the group quota).
- If the user quota is not set, the group quota is assigned to the user.
- When a user quota is set prior to the user joining a group and a group is assigned:
 - If the user quota is more than the group quota, the individual user's quota is automatically reduced to the group quota amount.
 - If the user quota is less than or equal to the group quota, the individual user quota remains unchanged.

Assigning User Quotas

1. On the Set Up Users screen, select a user from the left pane.
2. In the Quotas field, click **Configure**.
3. Enter the amount of space to assign to the user on the My Cloud device.
 - To assign unlimited space, leave the Quota Amount field blank.

4. Click **Apply**.

Removing a User

Use the following steps to delete users from the My Cloud device.

Note: The Admin account cannot be deleted.

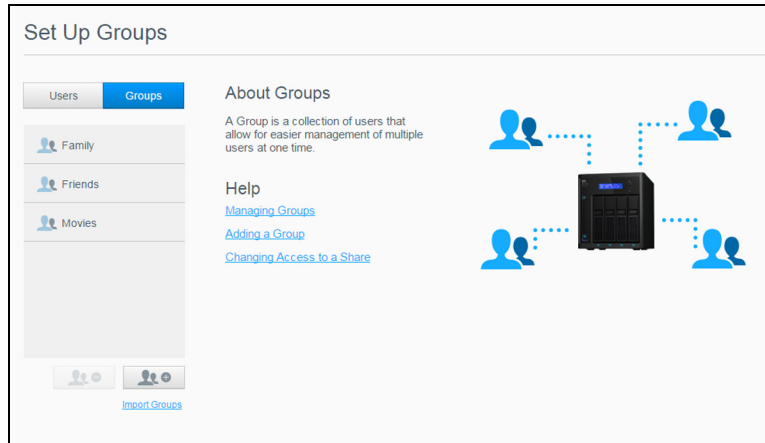
1. On the Set Up Users screen, select the user you'd like to delete.
2. Click the **Remove User** icon.
3. In response to the confirmation message, click **OK**. The user account is removed from the device and no longer appears in the user account list.

About Groups

A group allows easier management of multiple users. The permissions and privileges you assign to group accounts determine the actions that can be taken by that group.

Viewing Groups

1. On the Navigation bar, click **Users** to display the Set Up User screen.
2. Click **Groups**.



3. To view group details, click a group name on the left pane. The group profile appears.

Adding a Group

1. To add a group, click the **Add Group** icon on the lower-left side of the Set Up Groups screen.
2. Enter a Group Name.
3. Click the check box next to the users you'd like to add to your new group, then click **Apply**.

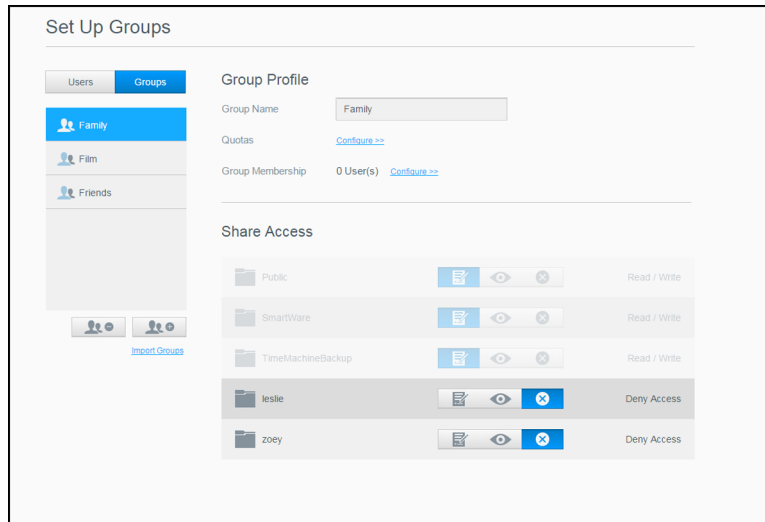
Editing Group Settings

1. On the Set Up Groups screen, select the group whose information you'd like to edit. The Group Profile and Share Access panel appears.
2. Modify the required and optional settings as desired then click **Apply**.
 - To update the group's access to shares, see "Assigning Share Access to Groups" on page 35.

Assigning Share Access to Groups

Once a group account is created, you can assign access to the various shares on your My Cloud device using the following steps.

1. On the Set Up Groups screen, select the group for which you'd like to assign a share.



Note: A share must first be made private on the Shares screen. All public shares are grayed out. See “About Shares” on page 37 for additional information.

2. In the Share Access area, click one of the following option icons to indicate the type of access to the share:
 - **Read/Write Access:** Select this option to provide the group account with read/write access to the selected share. The group members can view and update the share.
 - **Read Only Access:** Select this option to provide the group account with read only access to the selected share. The group member can view the share but can't update it.
 - **Deny Access:** The group has no access to this share.

The group is updated with your share access selection.

Assigning Quotas to a Group

Use the following steps to assign a quota to a Group. A quota determines the amount of space assigned to the user on the My Cloud device. (See “User Quotas” on page 32 for information on quotas.)

1. On the Set Up Groups screen, select the group from the left pane.
2. In the Quotas field, click **Configure**.
3. Enter the amount of space you'd like to assign to the group on the My Cloud device.
 - To assign unlimited space, leave the Quota Amount field(s) blank.
4. Click **Apply**.

Removing a Group

Use the following steps to delete a group from the My Cloud device.

Note: User accounts are returned to their individual settings when a group to which they belonged is deleted.

1. On the Set Up Group screen, select the group you'd like to delete in the left pane.
2. Click the **Remove Group** icon.
3. In response to the confirmation message, click **OK**. The Group account is removed from the device and no longer appears in the Group account list.

6

Managing Shares

About Shares

About Shares

A share is an area on the My Cloud device for storing files (similar to a folder or directory).

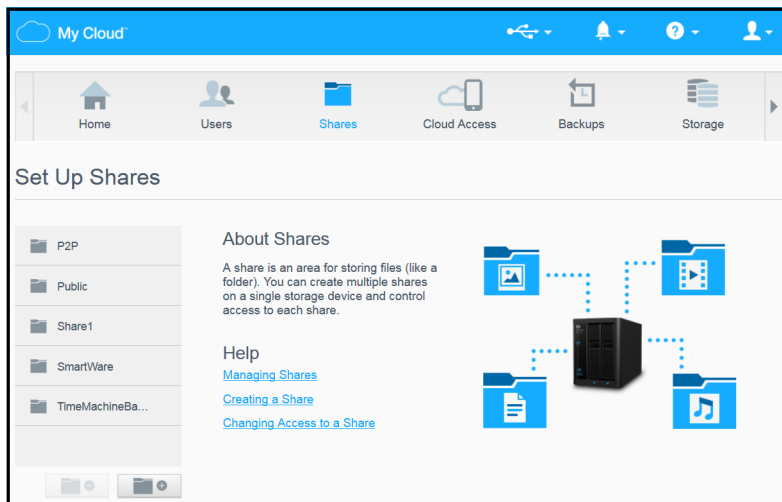
A share can be public so that all users can access the contents, or private to limit access to selected users. The **Shares** icon on the Navigation bar displays a list of shares on the My Cloud device and enables the Admin to manage shares and user access.

Viewing a List of Shares

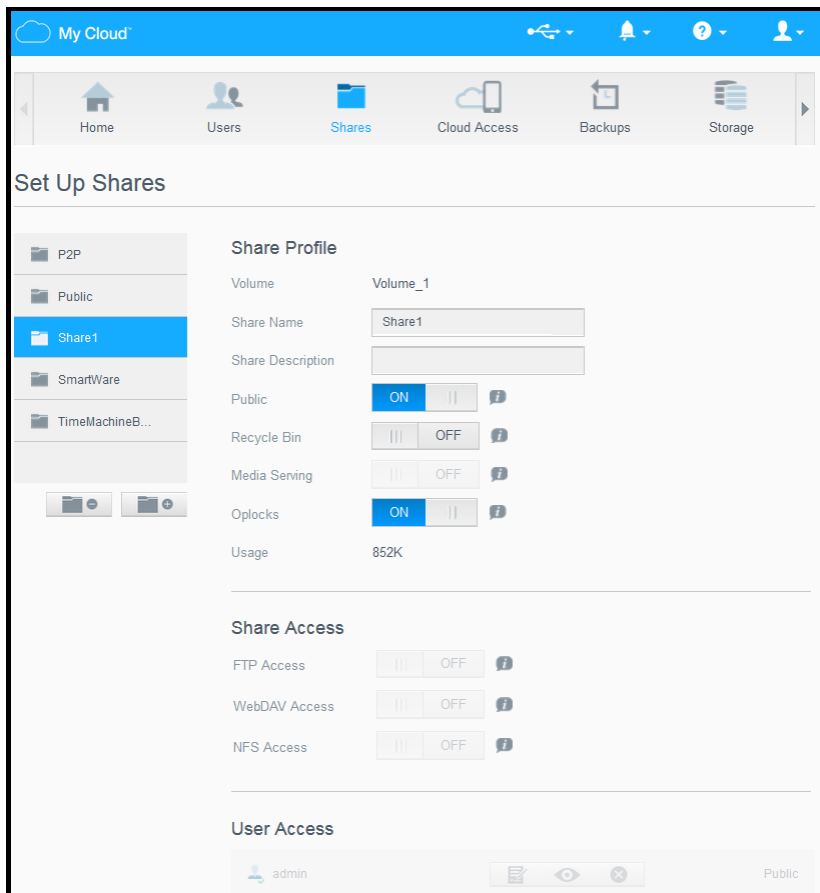
Click the **Shares** icon on the Navigation bar to display a list of shares on the My Cloud device. For each share name, the description, media serving, and public access status display.

Use the following steps to view a list of shares.

1. On the Navigation bar, click **Shares** to display the About Shares page.



2. Click a share to display its profile and share access information.



Note: You can only configure permissions if a share is private. Public shares always have read/write access and are grayed out.

Creating a New Share

You can create a share and designate it as public or private. For example, if the share contains financial information, you might want to make that share private. Or, if there are photos you would like a friend to see, you can make the share public for that friend.

1. Click the **Shares** icon on the Navigation bar.
2. Click the **Add Share** icon.
3. Enter the Share Name and Share Description (optional), then click **Apply**.

Editing Share Settings

1. On the Set Up Shares screen, select the share you'd like to edit. The Share Profile panel appears.
2. Modify the fields you'd like to edit as desired.
3. Click **Apply** to save your change, if prompted.

Making a Share Private

If you decide there is a reason to limit access to a public share, use the following steps to make a share private.

1. On the Set Up Shares screen, select the share you'd like to make private.
2. In the Share Profile area, click the **Public** toggle button to **OFF**.
3. For each user listed in the **User Access** section, select their level of access by clicking the appropriate icon for the share (e.g., read/write, read only, or no access).

Deleting a Share

WARNING! Deleting a share erases all files and folders on that share.



1. On the Set Up Shares screen, select the share you would like to delete.
2. Click the **Delete Share** icon in the left panel.
3. In response to the confirmation message, click **OK**.

Accessing the Contents of a Share Locally

Note: For information on accessing the contents of a share remotely, see “Accessing Your Cloud Remotely” on page 40.

For a private share, the user must have:

- A user name and password assigned to the share name.
- Read-only or Read/Write access to the share.

IF you want to open a share using . . .	THEN . . .
Windows 8 / Windows 8.1 / Windows 10	<ol style="list-style-type: none"> 1. In the task bar, click the File Explorer icon . 2. In the left panel, select Network and double-click the My Cloud device name (see “Appendix D: My Cloud Device URLs and Names” on page 104 for a list of device names). 3. Double-click a public or private share on your device.
Windows 7	<ol style="list-style-type: none"> 1. Click  or Start > Computer. 2. In the left panel, select Network. 3. Click the My Cloud device name (see “Appendix D: My Cloud Device URLs and Names” on page 104 for a list of device names). 4. Double-click the public or private shares on your device.
Mac OS X	<ol style="list-style-type: none"> 1. Open a Finder window and locate your My Cloud device under the Shared heading in the side bar. <ul style="list-style-type: none"> - If presented with an authorization page, either enter your user name and password or select Guest, then click Connect. 2. Click the device to display the public or private shares on your device.
WD Access	Go to the My Cloud Learning Center to download WD Access at http://www.mycloud.com/learn/ .

7

Accessing Your Cloud Remotely

- [Enabling Cloud Access for the My Cloud Device](#)
- [Configuring Cloud Access for a User](#)
- [Access Your Files with iOS and Android Mobile Apps](#)

This chapter explains how to set up the My Cloud device for remote access and describes some of the ways you can take advantage of its many capabilities.

Enabling Cloud Access for the My Cloud Device

Before you can use your My Cloud device remotely, the device must be enabled for cloud access. To verify that your My Cloud device is enabled for remote access and to check the status of its remote connection(s), see “Cloud Access” on page 71.

There are three ways to enable the cloud for your smart devices:

- **Discovery on your Local Area Network (LAN):** If you are on your LAN, cloud access software will automatically discover and list your device. Once discovered, you can complete the steps necessary to connect to the cloud.
- **Email:** If you include an email address when you add a new user to your My Cloud device, the new user will receive an email with instructions on setting up and activating a password for cloud access (see “My Cloud Access” on page 40).
- **Activation Code:** If you or your users are not on your LAN, you can generate an Activation Code to provide access to the cloud (see “Cloud Device Access” on page 41),

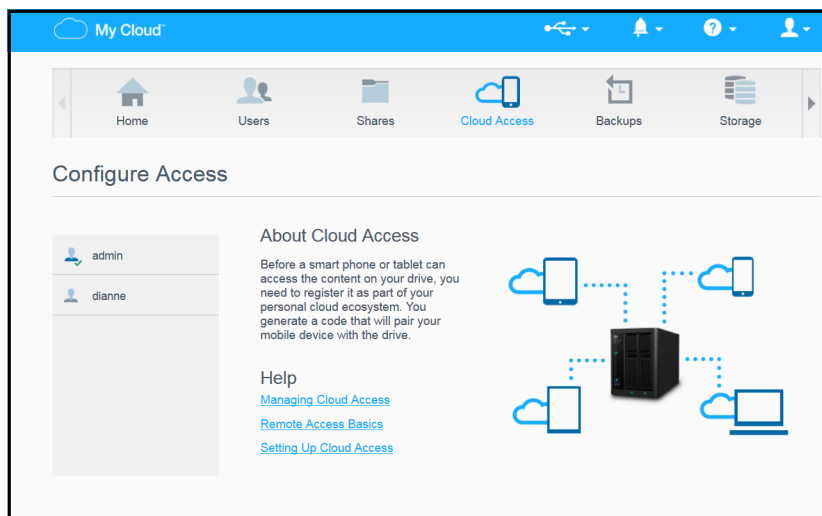
Configuring Cloud Access for a User

Once you’ve enabled cloud access on the My Cloud device, use the following steps to give remote access capability to your device users.

My Cloud Access

Use the following steps to set-up access to the My Cloud device.

1. On the Navigation bar, click the **Cloud Access** icon.



2. In the left pane, select the user you'd like to configure for My Cloud access.
3. In the My Cloud.com Login for <user name> area, click **Sign Up**.
4. On the Update My Cloud Login dialog, enter the user's email address. This email address is used to send the user confirmation information and instructions on setting up and activating a password for cloud access.
5. Click **Save**.

Cloud Device Access

Use the following steps to generate an activation code for a user's mobile device(s) and My Cloud Desktop app.

Important: Codes are valid for 48 hours from the time of the request and can be used only once.

1. On the Navigation bar, click the **Cloud Access** icon.
2. In the left pane, select the user you'd like to configure for cloud device access.
3. In the Cloud devices for <user name> area, click **Get Code**.
You'll need to generate one code for each mobile device and app you want to activate. You also need a code to activate the My Cloud for desktop app. A dialog box displays the user's activation code and its expiration date and time.
Note: Make sure to write down the access codes you generate.
4. Click **OK**. The Cloud devices for <user name> area displays your generated code and its expiration date. Once you use the code(s), this area displays the cloud devices to which the user now has access.

Access Your Files with iOS and Android Mobile Apps

The My Cloud mobile apps allow you to access all of the content on your personal cloud from any device.

My Cloud Mobile App

Save valuable space on your mobile devices with easy photo and video uploads directly to your personal cloud, then securely access and share your memories.

The My Cloud mobile app also allows you to easily transfer files between your personal cloud, Dropbox™, and other public cloud accounts. These free apps are available for iOS and Android.

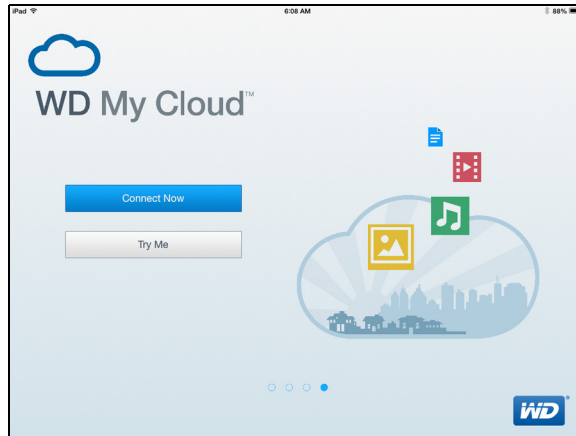
For features and instructions, see the Help, Guide Me page, and Quick Tips within the My Cloud mobile app, or visit the My Cloud Learning Center at <http://www.mycloud.com/learn/>.


Requirements

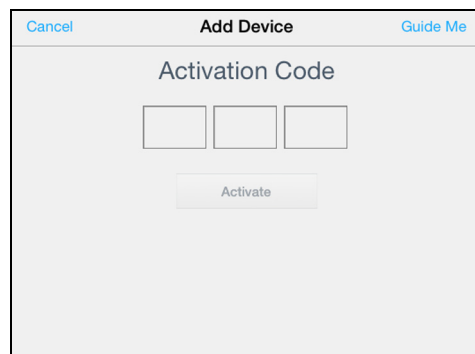
- My Cloud device with the most recent firmware, connected to the Internet.
- Access to cloud services requires the My Cloud app.
- A Smart device running one of the following operating systems:
 - iOS iPhone or iPad running versions 7.0 or later software.
 - Android smartphone or tablet running versions 4.0 or later software.

Installing the My Cloud Mobile App

1. Download the My Cloud mobile app from the Apple App Store, Google Play store, or Amazon Appstore for Android, and install it on your mobile device.
2. Launch the app.
3. Review the Western Digital End User License Agreement, then click **Accept**.
4. Tap **Connect Now**.



5. Select one of the following My Cloud device connection options:
 - **Cloud Sign in:** Tap  and sign into your personal cloud using your My Cloud or other public cloud accounts.
 - **Add Manually:** If the mobile device is not on the same LAN or Wi-Fi network as the My Cloud device:
 - In the Add Manually section, tap WD Device.
 - Enter the activation code generated on you My Cloud and tap **Activate**. (For information on obtaining an activation code, see “Configuring Cloud Access for a User” on page 40.)



Note: You must generate one code for each device you want to activate. Codes are valid for 48 hours from the time of request and can be used one time only.

8

Backing Up and Retrieving Files

- [About Backups](#)
- [Managing a USB Device and USB Backups](#)
- [Remote Backups](#)
- [Internal Backups](#)
- [Viewing Backup Details](#)
- [Modifying a Backup Job](#)
- [Deleting a Backup Job](#)
- [Cloud Backups](#)
- [Camera Backups](#)

About Backups

There are various ways to back up your data on the My Cloud device. These include:

- **USB Backup**—Allows you to back up your My Cloud device data to a USB device or to backup your USB device data to your My Cloud device.
- **Remote Backup**—Allows you to back up My Cloud device data to another My Cloud device.
- **Internal Backup**—Allows you to back up data from one share to another on your My Cloud device.
- **Cloud Backup**—Allows you to backup My Cloud device data to an external cloud backup service.
- **Camera Backup**—Allows you to backup your camera to the My Cloud device.

Managing a USB Device and USB Backups

When you attach a USB drive to the My Cloud device, you turn the USB drive into a shared network drive. Once connected, the USB drive has the following capabilities:

- When you connect an external USB drive such as a My Passport®, a memory stick, or a camera to the My Cloud device, you can access it with Windows Explorer or Mac Finder.
- The USB drive can serve as a target for backups.
- You now have the option of mapping the drive as a user share drive.
- If a WD external drive has been locked, when it is attached to the My Cloud device, it maintains that security. Using the Dashboard, you can unlock or re-lock it as desired.

Connecting a USB Drive

Connect a USB hard drive to a USB port on your My Cloud device for additional storage and backup capabilities. The USB drive appears as a share on the My Cloud dashboard. You can view details of the USB drive at anytime by clicking the USB icon at the top of the page.

The My Cloud device supports the following formats for externally attached USB drives while performing file transfer:

- FAT32
- NTFS
- HFS+J

WARNING! Mounting or ejecting a USB drive while performing a file transfer will interrupt the file transfer process.

Creating a USB Backup

There are two ways to create a USB backup with your My Cloud device:

- **Back USB port backups:** Use the ports on the back of your My Cloud device to backup the data on your USB port to your My Cloud device, or to backup data on your My Cloud device to the inserted USB port. (See “Creating USB Port Backups” on page 44.)
- **Front USB port with USB Copy button:** Backs up all of the information on inserted USB device to your My Cloud device. (See “Creating Front USB Port Backups with the USB Copy Button” on page 45.)

Creating USB Port Backups

Use the following steps to back up your data on your My Cloud device to a USB device or to backup your USB device data to your My Cloud device.

Note: This information is applicable only for the USB ports on the back of your My Cloud device. See “Creating Front USB Port Backups with the USB Copy Button” on page 45 for information on creating a USB backup copy using the USB port on the front of your device.

1. On the Navigation bar, click **Backups** to display the Backups screen.



2. Click **USB Backups**, if not already selected.
3. Click **Create Job**.

4. Enter the following information to create a USB backup job:

Job Name	Enter a Job Name for your backup.
Direction	Indicate the direction of your backup from the drop-down menu. Options include: <ul style="list-style-type: none"> • USB to NAS: Backs up the data on your USB device to the My Cloud device. • NAS to USB: Backs up the data on your My Cloud device to a USB device.
Source Folder	Click Browse , and select the folder you'd like to back up, then click OK .
Destination Folder	Click Browse , and select the destination folder for your backup, then click OK .
Backup Type	Indicate the type of backup you'd like to perform. <ul style="list-style-type: none"> • Copy: Copies files from the source to the destination. • Synchronize: Copies files from the source to the destination. This option will overwrite duplicate files. • Incremental: Creates up to 10 copies of the incremental source file changes to the destination.
Auto Start When Connected	This option automatically starts the job when the device is connected. Click the toggle button to turn the option on or off.

5. Click **Create**.
6. In the USB Backup Jobs area, click the **Start Backup** icon to begin your backup. The progress of the backup appears in the USB Backup Jobs area.

Creating Front USB Port Backups with the USB Copy Button

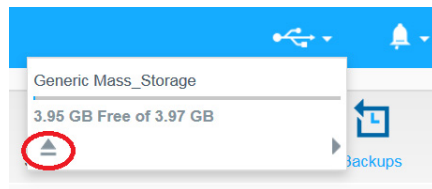
Use the following steps to create a backup job and copy the contents of a USB drive to your My Cloud device.

1. Insert your USB device into the front USB port (port 1) of your device.
2. Press the USB Copy button above the USB port for approximately 5 seconds. This creates a backup job for your USB device.
3. On the Navigation bar, click **Backups** to display the Backups screen.
4. Click **USB Backups**, if not already selected.
5. In the USB Backup Jobs area, the backup job for your device displays (USB_Port_1).
6. Click the **Start Backup** button to copy the contents of the USB device to your My Cloud device. The progress of the backup appears in the USB Backup Jobs area. Once copied, you can access your backed up content in the **Public > USB Import** folder.

Ejecting a USB Drive

Use the following steps to eject a USB drive from your My Cloud device.

1. Click the USB icon at the top of the page.
2. Click the **Eject USB drive** button.



Remote Backups

This option allows you to back up your My Cloud device to another My Cloud device.

Before you proceed with a remote backup, ensure the following:

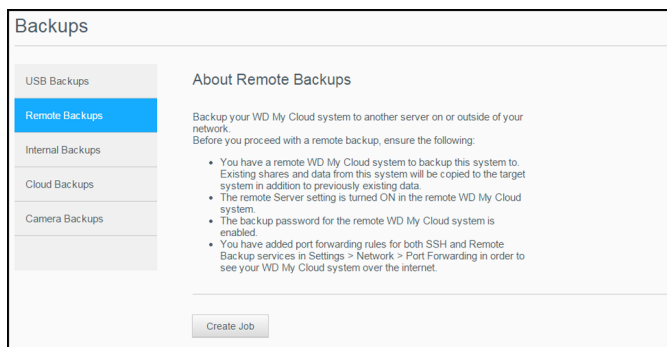
- You have a remote My Cloud device to which to back up this device. Existing shares and data from this device will be copied to the target device in addition to previously existing data.
- The remote Server setting is turned ON in the remote My Cloud device.
- The backup password for the remote My Cloud device is enabled.
- You have enabled port forwarding to see the remote My Cloud device over the Internet.

For additional information on remote backups, see Knowledge Base Answer ID 11807.

Creating a Remote Backup

Use the following steps to back up your My Cloud to a remote device.

1. On the Navigation bar, click Backups to display the Backups screen.
2. Click Remote Backups.



3. Click Create Job.
4. Enter the following information to create a Remote backup job:
 - Job Name: Enter a Job Name for your backup.
 - Remote Server: Select the type of remote server.
 - NAS Server (a My Cloud device on your local network), OR
 - My Cloud <device name> (a My Cloud device that is not on your local network).
 - Remote IP Address: Enter the IP address of the server (example: 192.168.1.16).

- Password: Enter the password for the remote backup server.
 - SSH User Name: Enter the Secured Shell protocol (SSH) user name for the remote device.
 - SSH Password: Enter the SSH password for the remote device.
 - Source Folder: Click **Browse** and select the folder you'd like to back up, then click **OK**.
 - Destination Folder: Click **Browse** and select the destination folder for your backup, then click **OK**.
 - Backup Type: Indicate the type of backup you'd like to perform.
 - **Copy**: Copies files from the source to the destination, OR
 - **Synchronize**: Copies files from the source to the destination. This option will overwrite duplicate files
 - Recurrence:
 - Click the toggle button to enable the Recurrence feature.
 - Select the frequency of the backup: Daily, Weekly, Monthly.
 - Select a time (hour, AM/PM) from the drop-down menu.
5. Click Create.
 6. In the USB Backup Jobs area, click the Start Backup icon to begin your backup. The progress of the backup appears in the USB Backup Jobs area.

Recovering a Remote Backup

Use the following steps to recover the data you saved on your remote server. This process recovers the data you saved on the remote server to your local server.

1. On the Remote Backup screen, under Remote Backup Jobs, click the **Job Detail** icon next to the job you'd like to view.
2. On the Job Detail screen, click **Recover Backup**. Your data recovery begins.

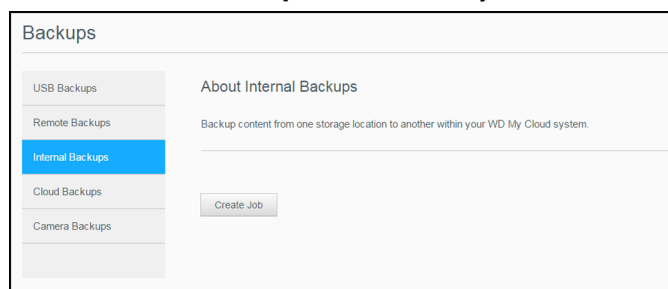
Internal Backups

Internal backups allow you to make backups of the existing content from one storage location to another on your My Cloud device.

Creating an Internal Backup

Use the following steps to back up your My Cloud internally.

1. On the Navigation bar, click **Backups** to display the Backups screen.
2. Click **Internal Backups**, if not already selected.



3. Click **Create Job**.
4. Enter the following information to create a Internal backup job:

- Job Name: Enter a Job Name for your internal backup.
 - Source Folder: Click **Browse** and select the folder you'd like to back up, then click **OK**.
 - Destination Folder: Click **Browse** and select the destination folder for your backup, then click **OK**.
 - Backup Type: Indicate the type of backup you'd like to perform.
 - **Copy**: Copies files from the source to the destination, OR
 - **Synchronize**: Copies files from the source to the destination. This option will overwrite duplicate files, OR
 - **Incremental**: Creates up to 10 copies of the incremental source file changes to the destination.
 - Recurrence:
 - Click the toggle button to enable the Recurrence feature.
 - Select the frequency of the backup: Daily, Weekly, Monthly.
 - Select a time (hour, AM/PM) from the drop-down menu.
5. Click **Create**. Your job appears in the Internal Backup Queue and will begin backing up at the indicated time.

Initiating an Immediate Internal Backup

- On the Internal Backups screen, under Internal Backup Queue, select the job you'd like to modify, then click the **Begin Now** button. The internal backup begins.

Viewing Backup Details

Use the following steps to view the details of a USB, Remote, and Internal Backup job.

1. On the Backups screen, select either USB, Remote, or Internal Backups, if not already selected.
2. In the Backup Job/Backup Queue section, select the job you'd like to view, then click the **Job Detail** icon.
3. Review the details of your Backup job, then click **Close**.

Modifying a Backup Job

Use the following steps to modify a USB, Remote, or Internal Backup job.

1. On the Backups screen, select either USB, Remote, or Internal Backups, if not already selected.
2. In the Backup job/Backup Queue section, select the job you'd like to modify, then click the **Modify Job** icon.
3. On the Modify Job dialog, make the necessary changes to your job, then click **Apply**.

Deleting a Backup Job

Use the following steps to delete a USB, Remote, or Internal Backup job.

Note: You can not delete a backup job created by using the USB Copy Button on the front of your device.

1. On the Backups screen, select either USB, Remote, or Internal Backups, if not already selected.

2. In the Backup job/Backup Queue, select the job you'd like to delete, then click the **Delete Job** icon.
3. In response to the confirmation message, click **OK**. The selected Backup job is now deleted and removed from the Backup Jobs list.

Cloud Backups

My Cloud device uses the following cloud services to create remote backups:

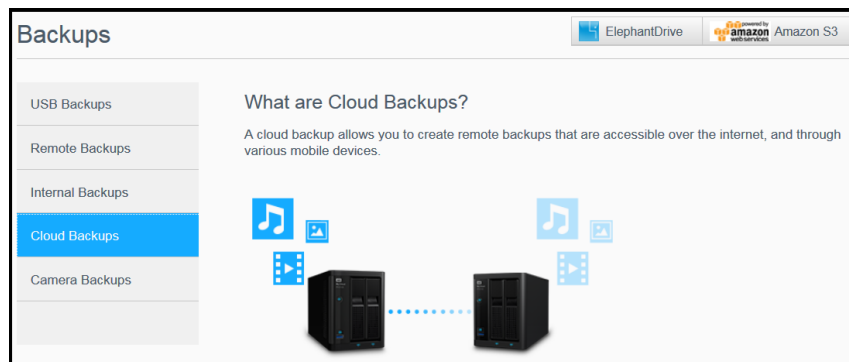
- **ElephantDrive:** ElephantDrive is a cloud backup service that provides secure and automatic backups to your files remotely.
- **Amazon S3:** Amazon Simple Storage Service (S3) is an online file storage web service that can be used to store and retrieve any amount of data, at any time, from anywhere on the web.

Enabling ElephantDrive Cloud Backup

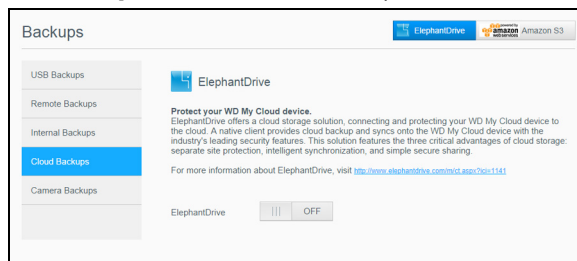
ElephantDrive is a cloud backup service that provides secure and automatic backups to your files remotely. Once set up, ElephantDrive automatically syncs with your device. For additional information see <http://home.elephantdrive.com/welcome/wdc/>.

Use the following steps to enable a cloud backup using ElephantDrive.

1. On the navigation bar, click **Backups** to display the Backups screen.
2. Click **Cloud Backups**, if not already selected.



3. Click **ElephantDrive** at the top of the screen.



4. In the ElephantDrive field, click the toggle button to turn on your ElephantDrive cloud backup.
5. Click **Register**. The Register screen displays.
6. Enter the following information and click **Register**:
 - **Email address:** Enter the email address you'll use to receive information from ElephantDrive.
 - **Password:** Enter a password for your new account
 - **Verify Password:** Reenter your password.

- You've now enabled your ElephantDrive cloud backup.

Backing Up with ElephantDrive

Once you've enabled ElephantDrive, use the following steps to create a cloud backup.

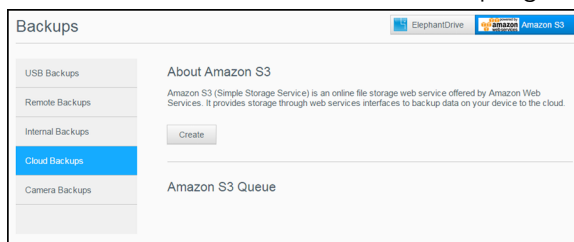
- On the Navigation bar, click **Backups** to display the Backups screen.
- Click **Cloud Backups**, if not already selected.
- Click **ElephantDrive** in the top-right area of the screen.
- In the Access Backups field, click **Login**.
- Enter the email and password used when you registered in step 6 of "Enabling ElephantDrive Cloud Backup" on page 49, then click **Login**.
- In the ElephantDrive field, click the **New device backup wizard** link.
- Log in to ElephantDrive using the email and password used when you registered with ElephantDrive in step 6 of "Enabling ElephantDrive Cloud Backup" on page 49.
- Follow the steps outlined in the ElephantDrive backup wizard to create your cloud backup.

Enabling an Amazon S3 Cloud Backup

Note: Before creating your Cloud backup, sign up for the Amazon S3 service at <http://aws.amazon.com/s3>.

Once your Amazon S3 account is set up, use the following steps to create a cloud backup.

- On the navigation bar, click **Backups** to display the Backups screen.
- Click **Cloud Backups**, if not already selected.
- Click the **Amazon S3** button in the top-right area of the screen.



- Click **Create**.
- Enter a Job Name for your cloud backup and click **Next**.
- Enter the following information supplied by Amazon S3:
 - Region:** Select the region used for your cloud from the drop-down menu.
 - Access Key:** Enter the access key supplied to you by Amazon S3.
 - Private Key:** Enter the private key supplied to you by Amazon S3.
 - Remote Path:** Enter the remote path for your cloud. This is normally your bucket name.
- Click **Next**.

8. Enter the following information, then click **Next**:

Type	Select one of the following options: <ul style="list-style-type: none"> • Upload: Backs up your My Cloud data to your Amazon S3 bucket. • Download: Backs up your Amazon S3 bucket to your My Cloud device.
Backup Type	From the drop-down menu, select the type of backup you'd like to perform. Options include: <ul style="list-style-type: none"> • Overwriting existing file(s): Overwrites files in the target folder that have the identical name as your source file. • Full Backup: Creates a separate folder containing all of the backup data each time the backup is performed. • Incremental Backup: Overwrites files with source files that are newer than the target files.

9. In the Local Path field, enter a path for your backup on your My Cloud server.
- Click **Browse** to browse to a location for your backup on the device. (Example Volume_1/backup)
10. Click the toggle button to activate the Autoupdate feature. This automatically updates your backup based on a schedule you create.
- If you activate the Autoupdate feature:
 - Select the Autoupdate schedule: Daily, Weekly, or Monthly
 - Select the Autoupdate Time from the drop-down menu (Daily option).
 - Select Autoupdate Date and Time from the drop-down menus (Weekly or Monthly option).
11. If you don't select Autoupdate, in the Backup Now field, indicate whether you want to begin the backup now.
- Select **Yes** to begin your backup now.
12. Click **Next**.
13. Review your settings and click **Finish**. Your Amazon S3 Cloud backup is created. The new job displays in the Amazon S3 Queue section of the Amazon S3 Backup page.
14. Access your Amazon S3 Cloud backup bucket to view your device backups.

Camera Backups

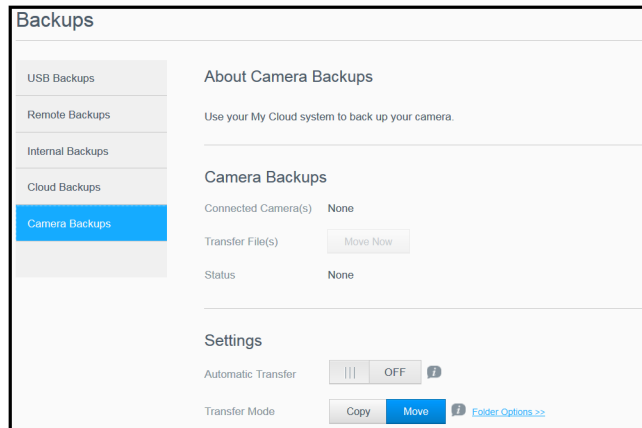
Camera backups allow you to backup the data on your camera to the My Cloud device. Once downloaded, users can navigate to the location where the camera data was saved to access the data, if they have access to that share.

Creating a Camera Backup

Use the following steps to back up your camera to the My Cloud device.

1. Ensure that your camera is connected to your My Cloud device.
2. On the Navigation bar, click **Backups** to display the Backups screen.

3. Click **Camera Backups**, if not already selected.



4. Ensure that the Connected Camera(s) area identifies your camera.
5. In the Settings area, enter the following information to backup the data on your camera:
 - **Automatic Transfer:** Click the toggle button to automatically transfer data from a camera that is connected to the My Cloud device.
 - **Transfer Mode:** Select how you'd like the camera data to be transferred. Options are:
 - **Copy:** Duplicates the information from your camera to the My Cloud device. This will leave the original data on your camera, OR
 - **Move:** Transfers the files on your camera to the My Cloud device, deleting the files from your camera.
 - **Folder Options:** Select this option to identify a destination for the transferred camera files. On the Camera Folder Options screen:
 - **Transfer Folder:** Click **Browse** to enter the location on your device where you'd like to transfer your data, then click **OK**.
 - **Folder Name:** Select a Folder Name type from the pull-down menu. If you select Custom Folder Name, enter a folder name in the Enter Folder Name field.
 - Click Save.
6. In the Transfer File(s) field, click **Copy/Move Now** to begin the file transfer, if Automatic Transfer is off.
7. Once complete, the Status field indicates that the backup is complete for the connected device and the day, date, and time of the completed download.

9

Managing Storage

- [About Storage](#)
- [RAID Storage](#)
- [Disk Status](#)
- [Viewing S.M.A.R.T Data Information](#)
- [Volume Virtualization](#)

About Storage

The Storage page allows you to configure the storage within your device and view the status and capacity of its disks. This chapter provides details on managing the storage on your My Cloud device.

Storage				
RAID	RAID Profile			
Disk Status	RAID Health: Healthy			
iSCSI	All RAID Volumes are active and healthy.			
Volume Virtualization	RAID Volume			
	Volume_1	JBOD	3.93 TB	Good
	Volume_2	JBOD	3.93 TB	Good
	Volume_3	JBOD	3.93 TB	Good
	Volume_4	JBOD	3.93 TB	Good
	Change RAID Mode			

RAID Storage

RAID (Redundant Array of Independent Disks) allows you to store the same data in different places on multiple hard drives, providing necessary redundancy, greater performance, and data integrity. There are several different levels of RAID, each one providing a different method of sharing or distributing data among the drives. Your My Cloud device allows you to select from the following storage modes:

Note: The difference between a drive and a volume is that a volume can be a single drive or multiple drives.

RAID Mode	Description
JBOD	The use of one or more drives not in a RAID configuration but managed as separate logical volumes.
Spanning	Combination of drives in a linear fashion to create one large logical volume.

RAID Mode	Description
RAID 0	RAID 0 mode provides disk striping across all drives in the RAID drive group. RAID 0 does not provide data redundancy but does provide the best performance of any RAID level. RAID 0 breaks up data into smaller segments and stripes the data segments across each drive in the drive.
RAID 1	In RAID 1 mode, the RAID controller duplicates all data from one drive to a second drive in the drive group. RAID 1 provides complete data redundancy, but cuts the required storage capacity in half.
RAID 5	RAID 5 mode offers superior performance and protection by striping data across 3 or more drives and dedicating a quarter of each drive to fault tolerance. This option is only available for 4-bay My Cloud devices.
RAID 10	RAID 10 mode is a RAID protocol in which data is written in stripes across primary disks that have been mirrored to the secondary disks. This option is only available for 4-bay My Cloud devices.

Viewing the Current RAID Mode

Use the following steps to view the RAID mode currently used on your device.

1. On the Navigation bar, click **Storage** to display the Storage screen.
2. Click **RAID**, if not already selected.
3. In the RAID Profile and RAID Volume areas, the following information displays:
 - RAID Health.
 - Auto-Rebuild status (whether or not Auto Rebuild is turned on).
 - RAID Volume which shows the number of volumes for which RAID or JBOD are configured.

Changing the RAID Mode

Use the following steps to change the current RAID mode on your My Cloud device.

WARNING! Changes made to your RAID mode will delete all of your data and your user settings. See “Saving a Configuration File” on page 88 for information on saving your user settings.

1. On the Navigation bar, click **Storage** to display the Storage screen.
2. Click **RAID**, if not already selected.
3. Click **Change RAID Mode** at the bottom of the screen.
4. Review the warning message and click **OK**.
5. Select the RAID mode you'd like to use for your My Cloud device.
Options include:

JBOD	The use of one or more drives not in a RAID configuration but managed as separate logical volumes.
Spanning	Combination of drives in a linear fashion to create one large logical volume.

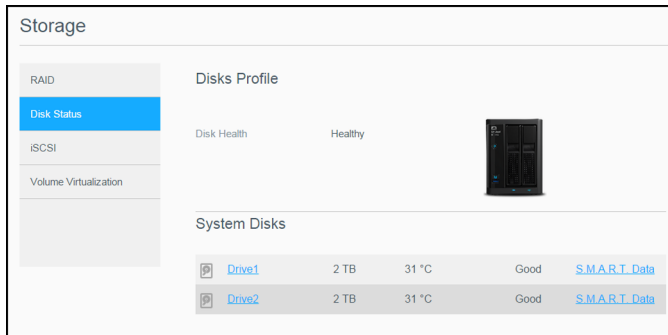
RAID 0	Data is striped across multiple hard drives, enabling accelerated reading and recording of data by combining the work of two or more drives to increase performance. However, if one drive fails, all of your data will be lost.
RAID 1	Two instantaneous copies of the data are recorded on separate hard drives so if one of them fails, other(s) continue to read/write data until the faulty hard drive is replaced.
RAID 5	Offers superior performance and protection by striping data across 3 or more drives and dedicating a quarter of each drive to fault tolerance. If one of the drives fails, the other(s) continue to read/write data until the faulty hard drive is replaced. This option is only available on 4-bay My Cloud devices.
RAID 10	RAID protocol in which data is written in stripes across primary disks that have been mirrored to the secondary disks. If one of the drives fails, the other(s) continue to read/write data until the faulty hard drive is replaced. This option is only available on 4-bay My Cloud devices.

6. Review and select the Storage option you'd like to use, select the **Switch to <Storage Mode>** check box, then click **Next**. A drive self-test is performed.
7. Review the warning at the top of the screen.
8. Once the test is complete, Review the status of your volumes and click **Next**.
9. If the Volume slider displays, select the amount of space you'd like to dedicate to the selected RAID mode.
 - If you choose not to use the entire volume for your RAID selection, you can configure the remaining disk space as Spanning by selecting the **Configure the remaining disk space as Spanning** check box.
10. Click **Next** to continue.
11. If you'd like to automatically rebuild the RAID configuration once the disk is recognized, click the Auto Rebuild toggle button to **ON**, then click **Next**.

Note: This screen does not display for JBOD, Spanning, and RAID 0 modes.
12. If you'd like to encrypt a volume, click the **Locked** icon, then click **Next**.
13. Review the summary of your selections, and click **Next**.
14. Review the warning screen and click **Finish**. The requested hard drive changes begin. Do not turn off your My Cloud device while these changes are in progress.
15. When the process is complete, click **Finish** again.

Disk Status

The Disk Status screen identifies the health of the disk drives as well as the status and information on each drive used in your My Cloud device.



The Disk Status screen consists of the following areas:

- **Disks Profile:** This area displays the general status of all of the disk drives on your device.
- **System Disks:** This area identifies the drives in your device, the status of each drive, and the amount of space on that drive.

Note: If a drive is not supported, the status is **not compatible**.

Viewing Hard Disk Drive Information

Use the following steps to view status of the disks on your My Cloud device.

1. On the Storage page, click **Disk Status**, if not already selected.
2. In the System Disks area, select **Drive <drive #>** next to the disk for which you'd like to view information.
3. Review the hard drive information and click **Close**. The Hard Drive Information screen displays the following data:

Vendor	The vendor from whom the hard drive was obtained.
Model	The model number of the hard drive selected.
Serial Number	The serial number of the hard drive selected.
Capacity	The capacity of the hard drive selected.
Firmware Version	The current firmware version used on the drive selected.

Viewing S.M.A.R.T Data Information

Self-Monitoring, Analysis and Reporting Technology (S.M.A.R.T.) data detects and reports on various indicators of drive reliability with the intent of anticipating hardware failures.

Use the following steps to view S.M.A.R.T data information concerning your My Cloud device drives.

1. On the Storage page, click **Disk Status**, if not already selected.

2. In the System Disks area, select **S.M.A.R.T Data** next to the disk for which you'd like to view information.
3. Review the S.M.A.R.T drive information, then click **Close**.

iSCSI Storage

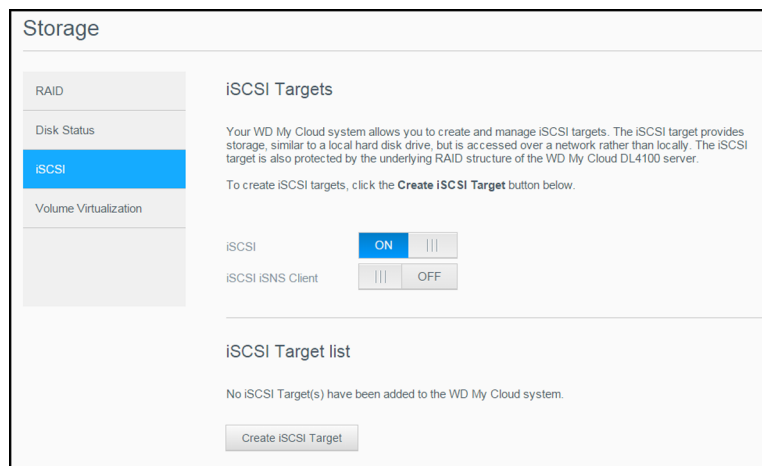
Internet SCSI (iSCSI) is an industry standard developed to enable transmission of iSCSI block storage commands and data over an existing IP network by using the TCP/IP protocol. The encapsulated iSCSI commands and data can be transmitted over a local area network (LAN) or a wide area network (WAN). As with traditional iSCSI, an iSCSI storage solution requires at least one “initiator” residing on the client computer and at least one “target” residing on the storage server.

Once the connection is established between the iSCSI initiator and the iSCSI target, the operating system on the iSCSI initiator sees the storage as a local storage device that can be formatted, read, and written in the usual manner.

Your My Cloud device allows you to create and manage iSCSI targets. The iSCSI target provides storage, similar to a local hard disk drive, but is accessed over a network rather than locally. The iSCSI target is protected by the underlying RAID structure of the My Cloud device.

iSCSI Roles

- **Initiator:** A client computer that accesses storage devices using iSCSI commands over an IP network.
- **Target:** A network-attached storage device that provides access to logical disks (which can be created on the My Cloud device).



Creating an iSCSI Target

Use the following steps to create an iSCSI target

1. On the Storage page, click **iSCSI**, if not already selected.
2. Under iSCSI Targets, click the toggle button to **ON** to enable iSCSI.
3. Click **Create iSCSI Target** at the bottom of the screen.
4. On the Create iSCSI Target screen, enter the following information:
 - **Alias:** The alias should be a descriptive name for your target.
 - **Created On:** Select the Volume where you'd like the iSCSI target to reside.

- **Size:** The size of your target and the unit of information for that size (e.g. GB, TB). Click **Next**.
 - If you'd like to assign security for your target, click **CHAP**.
 - Enter an existing User Name and Password, then confirm the Password.
5. Click **Apply**. Your new iSCSI target is created and displays in the iSCSI Target List.

Enabling / Disabling an iSCSI Target

Use the following steps to enable or disable an iSCSI target.

Enabling an iSCSI Target

1. On the Storage page, click **iSCSI**.
2. Under iSCSI Target list, click **Details** next to the target you'd like to enable.
3. Click **Enable**. The selected target is now enabled.

Disabling an iSCSI Target

1. On the Storage page, click **iSCSI**.
2. Under iSCSI Target list, click **Details** next to the target you'd like to disable.
3. Click **Disable**. The selected target is now disabled.

Modifying an iSCSI Target

Use the following steps to modify an iSCSI target.

1. On the Storage page, click **iSCSI**.
2. Under iSCSI Target list, click **Details** next to the target you'd like to modify.
3. Make all of your necessary changes, then click **Save**.

Enabling iSCSI iSNS Client

The Internet Storage Name Service (iSNS) protocol is used for interaction between iSNS servers and iSNS clients. iSNS clients are computers, also known as initiators, that are attempting to discover storage devices, also known as targets, on an Ethernet network. Use the following steps to configure the iSCSI iSNS client.

Note: iSNS is primarily used to connect to a Windows server.

1. Click **iSCSI**, if not already selected.
2. Click the toggle button to enable iSCSI.
3. In the iSCSI iSNS Client field, click the toggle button to **ON**.
4. Click **Configure**.
5. Enter the iSNS client server address (normally the IP address of your Windows server), then click **Apply**.

Deleting an iSCSI Target

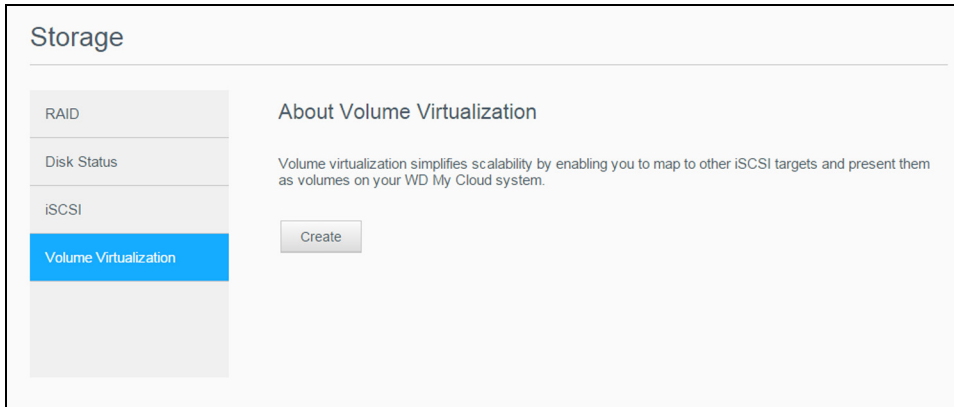
Use the following steps to delete an iSCSI target.

1. On the Storage page, click **iSCSI**.
2. Under iSCSI Target list, click **Details** next to the target you'd like to delete.

3. Ensure that this is the target you want to delete, then click **Delete**.
4. Review the warning message, then click **OK**. The selected target is deleted and removed from the iSCSI Target list.

Volume Virtualization

Volume Virtualization simplifies scalability by allowing you to map iSCSI targets on other network storage devices and present them as volumes on your My Cloud device.



Creating a Virtualized Volume

Use the following steps to create a virtualized volume on your device.

1. On the Storage page, click **Volume Virtualization**, if not already selected.
2. Click **Create**.
3. In the Device IP field, enter the IP address of the device where the iSCSI target resides, then click **Next**.
4. Select an iSCSI target from the retrieved list, then click **Next**.
5. To add authentication to the target, click the toggle button to **ON**, enter a User Name and Password, then click **Next**.
 - Disabled authentication is the default. To keep the default, ensure that the Authentication toggle button is Off, then click **Next**.
6. Select a LUN (Local Unit Number) from the list, then click **Next**.
7. Enter a name for the share folder, then click **Next**.
8. Review the Volume Virtualization summary to ensure that your settings are correct, then click **Apply**. A virtual volume is created.

Connecting a Virtualized Volume to a Target

Use the following steps to connect a virtualized volume on your device.

1. On the Storage page, click **Volume Virtualization**, if not already selected.
2. Click **Job Details** next to the virtual volume you'd like to connect.
3. Click **Connect**. Once connected to the target, the system automatically formats the LUN, if it hasn't been done before.
4. Once your virtual volume is formatted, click **Close**. The state of the volume is changed to Connected. Your new virtual volume is now available on your My Cloud device.

Modifying a Virtualized Volume

Use the following steps to modify a virtualized volume on your device.

1. On the Storage page, click **Volume Virtualization**, if not already selected.
2. Select the virtual volume you'd like to modify, then click **Modify**.
3. Make the necessary changes to the volume, then click **Apply**. When the modified settings are saved, the virtual volume is connected again.

10

Managing Apps

[About Apps](#)
[Managing Apps](#)

About Apps

Apps are small, self-contained programs used to enhance the existing functions of your My Cloud device or service. The

My Cloud device provides various apps that allow you to use your device more productively.

Note: WD recommends that you fully understand the nature of any app before you install it on your device.

Note: Obtain support for each app through the individual vendor.

My Cloud comes with various apps pre-installed.

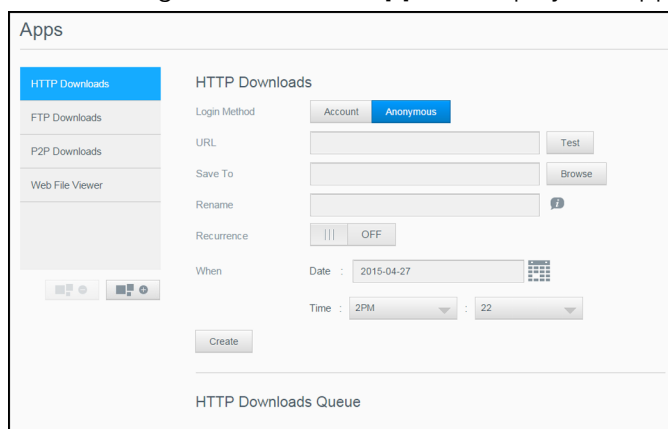
Managing Apps

The Apps screen displays a list of the currently installed apps. From this screen, you can use your installed apps, add new apps, or remove apps you no longer want to use.

Note: You cannot remove pre-installed apps.

Viewing Apps

1. On the Navigation bar, click **Apps** to display the Apps screen.



2. To select an app, click the name of the app in the left pane. The app appears in the right pane.

Adding an App

Use the following steps to add an app to your My Cloud device.

1. On the Navigation bar, click **Apps** to display the Apps screen.
2. Click the **Add an App** icon in the lower-left side of the screen. The first time you add an app, the Terms of Service screen appears. Read and accept the agreement.
3. For details about the app, click **Details**. Close the Details screen.

4. Place a check next to the app(s) you'd like to add to your device, then click **Install**. The selected apps are added to your device.

Manually Adding an App

If you have an app you'd like to add that is not listed on the Add an App screen, use the following steps to manually add that app to your My Cloud device.

Note: WD recommends that you fully understand the nature of any app before you install it on your device.

1. On the Navigation bar, click **Apps** to display the Apps screen.
2. Click the **Add an App** icon on the lower-left side of the screen.
3. Click the **To install an app manually, click here** link.
4. Navigate to the app you'd like to install on your device.
5. Select the app you'd like to install, then click **Open**.
The selected app installs and is added to your device.

Deleting an App

Use the following steps to delete an app from your My Cloud device.

Note: You cannot delete pre-installed apps.

1. On the Navigation bar, click **Apps** to display the Apps screen.
2. From the Apps list in the left pane, select the app that you'd like to delete from the device.
3. Click the **Remove an App** icon on the lower-left side of the screen.
4. In response to the confirmation message, click **OK**. The app is removed from the device and no longer appears in the user account list.

Updating an App

Use the following steps to update an app that you've added to your My Cloud device.

1. On the Navigation bar, click **Apps** to display the Apps screen.
2. If there is an update for one of the apps you've added to your device, an Updates available link appears at the top-right area of the screen.
3. Click the **Updates Available** link to display the Updates Available screen.
4. Select the app you'd like to update from the list and click **Update**.
 - If you'd like to view the details of the update, click **Details**.
 - Click **Back** to return to the Update screen.

Playing/Streaming Videos, Photos, & Music

[Media Servers](#)

[Media Storage](#)

[Enabling DLNA and iTunes](#)

[Accessing Your My Cloud Device Using Media Players](#)

[Accessing Your My Cloud Device Using iTunes](#)

Media Servers

The My Cloud device is designed to serve as your home's media server. It enables you to stream photos, music, and videos to your DLNA-compatible devices and music to your iTunes-compatible devices.

Both DLNA-compatible and iTunes-compatible devices search for media stored in any Public share that has media serving enabled. By default, DLNA Media is disabled. Once you enable it on the Settings > Media Server page, media serving for the Public share is also automatically enabled. For all other shares, media serving remains off.

If you do not want DLNA to display specific media files, place them in a private share that is set to disable media sharing. (See “Editing Share Settings” on page 38.)

Media Server Overview

The My Cloud device uses TwonkyMedia as its DLNA media server. It streams your music, photos, and videos to compatible devices in your home. Playing media on a compatible device is easy.

The media server searches for all the media stored in the Public share on the My Cloud device connected to your home network. After enabling media serving for the device (see “Enabling DLNA and iTunes” on page 64), you can just transfer your multimedia content to the Public share on your My Cloud device, and you are ready to stream and view content on your home entertainment center, game consoles (such as Xbox 360® or PlayStation® 3), WD TV® Live media player, or DLNA® 1.5 digital media adapters), and other PC computers on your home or office network. Visit <http://www.dlna.org> for further information on DLNA.




iTunes Overview

You or anyone connected to the My Cloud device can use iTunes to play stored music files. iTunes creates a virtual music library on the device and treats it as an iTunes repository, making it possible to stream music files from the My Cloud device to Windows or Mac computers running iTunes.

iTunes scans any shares that have the Media Serving setting enabled, including the Public share by default.

Media Types Supported

Note: Some devices may not support playback of all these files. Please refer to your device's user manual to see which formats are supported.

 Audio files	 Video files	 Image Files
3GP	3GP	BMP
AAC	ASF	JPEG
AC3	AVI	PNG
AIF	DivX	TIF
ASF	DV	
FLAC	DVR-MS	
LPCM	FLV	
M4A	M1V	
M4B	M2TS	
MP1	M4P	
MP2	M4V	
MP3	MKV	
MP4	MOV	
MPA	MP1	
OGG	MP4	
WAV	MPE	
WMA	MPEG1	
	MPEG2	
	MPEG4	
	MPG	
	MTS	
	QT	
	QTI	
	QTIF	
	RM	
	SPTS	
	TS	
	VDR	
	VOB	
	WMV	
	Xvid	

Media Types Supported by iTunes

Note: iTunes 10.4 or later only supports music files. See Knowledge Base Answer ID 8412 for additional information on iTunes-supported versions.

The iTunes Media Server supports the following file extensions: FLAC, M4A, MP3, MP4A, and WAV.

Note: Some devices may not support playback of all these files. Please refer to your device's user manual to see which formats are supported.

Media Storage

You can access and store media content on the My Cloud device by means of network shares.

The device comes preconfigured with the Public network share, which contains the following folders for media storage:

- **Shared Music**—Stores music files you want to share with other users.
- **Shared Pictures**—Stores image files you want to share with other users.
- **Shared Videos**—Stores video files you want to share with other users.

Note: You will notice that the Public share's Shared Music and Shared Pictures shares contain mirrored and uploaded subfolders. These folders are needed by Twonky 7.2. You can now upload all media types to the uploaded subfolder from a DLNA client with "upload" capability.

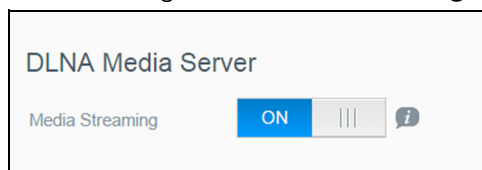
Go to the Twonky configuration site (NAS_IP:9000) to aggregate content from all NAS devices with DLNA capability on your network to the mirrored folder. Uploading and mirroring are best left to expert users, as these features are not supported by WD customer support.

Enabling DLNA and iTunes

The Media page of the Settings Screen allows you to enable or disable the DLNA and iTunes media servers. Media server utilities for rescanning the NAS or fully rebuilding the DLNA database are also on the Media page.

Enabling DLNA

1. On the Navigation bar, click **Settings** and in the left panel click **Media**.

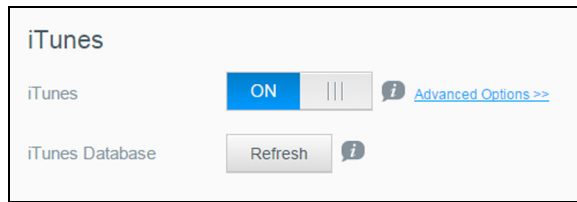


2. In the DLNA Media Server area, Media Streaming field, click the toggle button to **ON**.

Note: Media Streaming is OFF by default. The media server must be enabled before you can provide media serving for a share. (See "Creating a New Share" on page 38 for instructions on how to enable media serving on a share.)

Enabling iTunes

1. On the Navigation bar, click **Settings** and then click **Media** in the left panel.



2. In the iTunes area, iTunes field, click the toggle button to ON to enable iTunes (if not already enabled).
 - Note:** iTunes is ON by default. To disable it, click the toggle button to OFF.
3. Click **Advanced Options** to display additional options for iTunes.
 - Note:** If iTunes is OFF, this field does not display on your screen.
 - If you'd like to use a password when accessing your My Cloud device on iTunes, in the Password field:
 - Click the toggle button to **ON**.
 - Enter a password.
4. For Auto Refresh, select the frequency of the media refresh for iTunes from the drop-down menu.
5. Click **Apply** to save your settings.

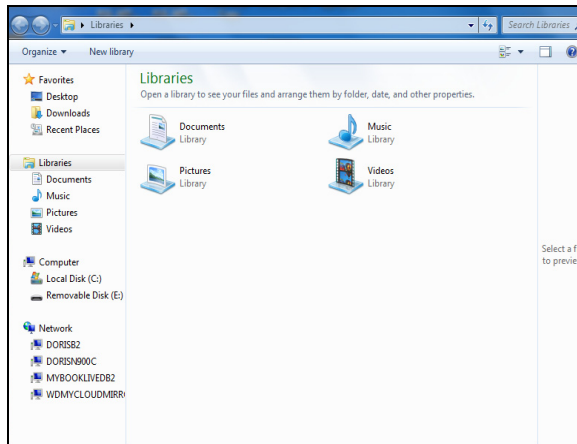
Refreshing iTunes

Use the following steps to refresh the iTunes directory. This allows iTunes to pick up any new media.

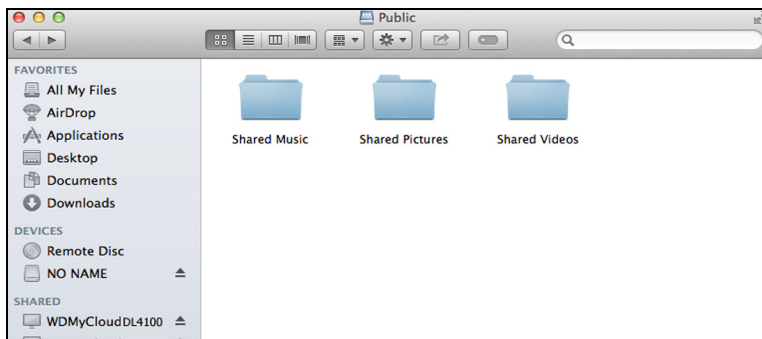
1. On the Navigation bar, click **Settings** and then click **Media** in the left panel.
2. In the iTunes Database field, click **Refresh**.

Adding Media Content to the Folders

1. Open **Windows Explorer** or **Mac Finder**.



Windows Explorer



Mac Finder

2. Navigate to the Shared Music folder on your My Cloud device, then copy your music files to the Shared Music folder.
3. Follow the same process to place your videos and pictures into their respective Shared Pictures and Shared Video folders.

Accessing Your My Cloud Device Using Media Players

Now that you have copied your files to one of the Shared folders, you can use a variety of media players to stream media. The following types are supported:

- WD TV® Live Media Players
- Windows Media Player
- Xbox 360
- PlayStation 3
- Other media players:
 - BluRay Players
 - Network Connected TVs
 - Digital Picture Frames
 - Network Music Player
- DLNA Devices

Note: For specific information on using and updating the media player, go to the appropriate support site.

WD Media Players

You can connect the various WD TV and WD Media Players to your home network for access to media content stored in a network drive such as the My Cloud device. For details on using a WD Media Player to access files on your device, see Knowledge Base Answer ID 9769 or refer to your WD Media Player User Guide.

Other Media Players

Following are general steps for setting up devices such as digital picture frames, Blu Ray players, network-connected TVs, and digital media adapters.

1. Make sure that your My Cloud device is connected to your home's local network and is powered on.
2. Follow the user instructions provided with your media player to proceed through any initial setup or installation of drivers.
3. Using the navigation feature on your player, scan and detect your My Cloud device on your network.
4. Depending on the player, you may need to access a Settings/Network Setup page in the user interface to establish connection so that your player can link to your My Cloud device. Please refer to your player's user guide for specific instructions.

DLNA Devices

See specific DLNA media device user manuals for instructions on connecting a DLNA device to your local area network so you can access content on the My Cloud device. Go to <http://www.dlna.org> for a list of DLNA-certified devices and for further information.

Accessing Your My Cloud Device Using iTunes

You or anyone connected to the My Cloud device can use iTunes to play stored music files. This service creates a virtual music library on the device and treats it as an iTunes repository, making it possible to stream music files from the My Cloud device to Windows or Mac computers running iTunes. For a list of supported media types, See "Media Types Supported" on page 63.

Note: iTunes 10.4 or later only supports music files. See Knowledge Base Answer ID 8412 for additional information on iTunes supported versions.

Note: iTunes scans any shares that have the Media Serving setting enabled, including the Public share by default.

You can drag and drop media files into the corresponding folders in the Public share (e.g., music files into the My Cloud/Public/Shared Music default share).

Streaming Media in iTunes

iTunes is enabled by default in the dashboard. See "Enabling iTunes" on page 65 for more information on configuring iTunes.

1. Launch iTunes on your computer.
2. Click **WDMMyCloud<model#>** under the Shared section of the left pane. If you have copied music to the /Public/Shared Music folder or a video to /Public/Shared Videos, and it is in a format supported by iTunes, it is listed in the right pane.

3. Double-click a media file you'd like to play.

12

Configuring Settings

[General](#)
[Network](#)
[Media](#)
[Utilities](#)
[Notifications](#)
[Firmware Update](#)

The Settings option on the Navigation bar allows the Administrator to view and customize the My Cloud device's system, network, media, utilities, notifications, and firmware settings. This chapter explains how to configure the various settings for your My Cloud device.

General

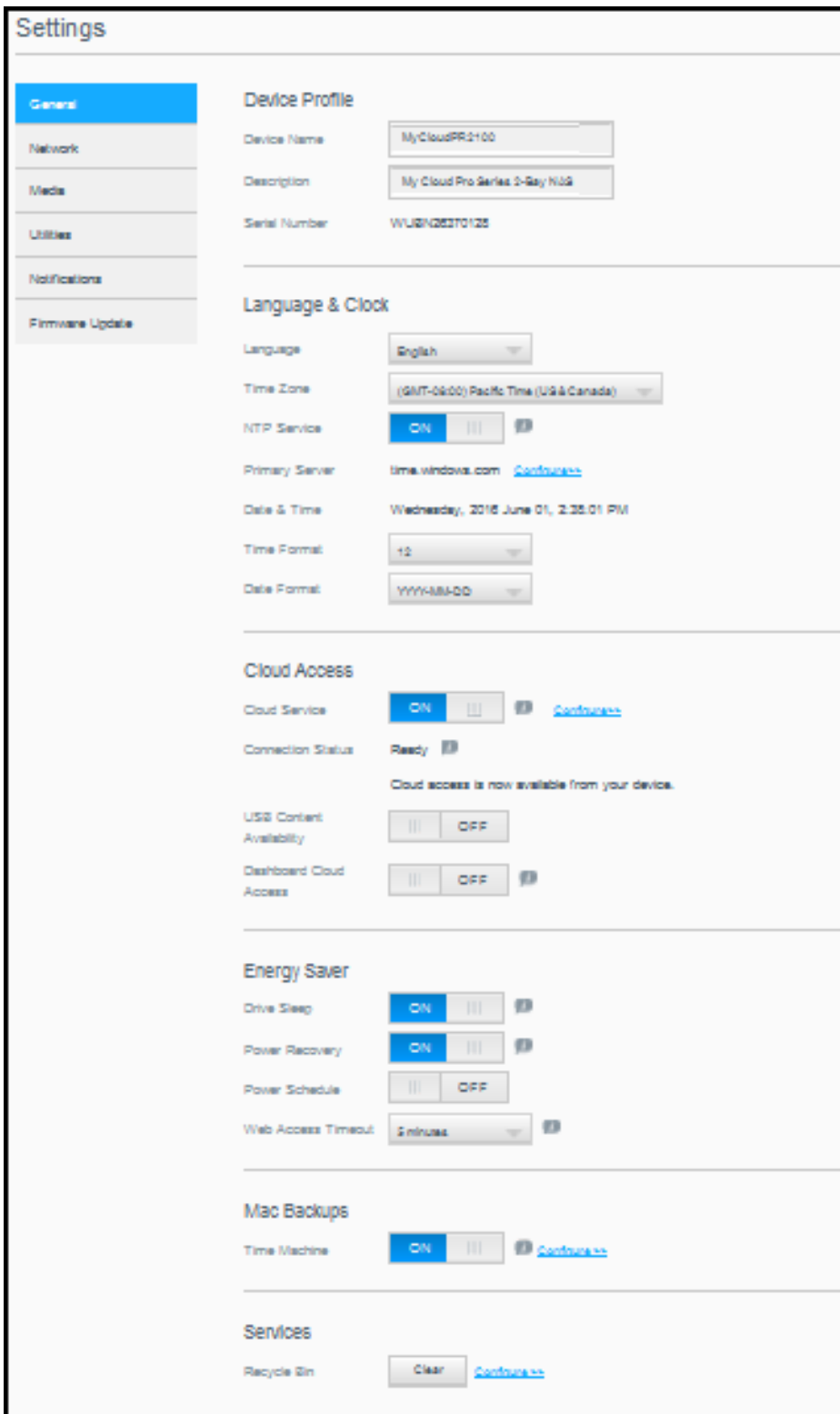
On the General page you can:

- View and modify the device name and description.
- Select the language in which the web pages should display.
- Set the date, time, and time zone for the device.
- Enable cloud access for your device.
- Set energy saving options.
- Enable and configure Time Machine backups for your Mac.
- Clear the Recycle Bin.
- Enable various services for your device.

WARNING! Renaming the My Cloud device forces all the network computers to remap their shared network resources, and will cause issues with any backup job in progress (such as Time Machine). Change the device name only when necessary.

Accessing the General Screen

On the Navigation bar, click **Settings**. The General page appears.



Device Profile

1. In the Device Profile section of the General page, view or modify the following settings:

Device Name	Enter a unique name for your device to identify it on the network. The device name can be up to 15 characters long and cannot include special characters (e.g., @, #, \$ etc.).
Description	The default description is MyCloud<model# >. If desired, enter a different description for your device. The device description can be up to 32 characters long and cannot include special characters (e.g., @, #, \$ etc.).
Serial Number	Displays the WD-assigned number that identifies the specific unit. This field cannot be updated.

2. If you made any changes, click **Apply** (appears next to the updated field once a change is made).

Note: Throughout the My Cloud dashboard, the **Apply**, **Save** and **Cancel** buttons display only if you make changes.

Language and Clock

In this section of the General screen, you can change the language that appears in the My Cloud device's interface and set the date and time. The date and time are synchronized to the NTP (Network Time Protocol) server by default. You have the option of setting the date and time manually or allowing the NTP to access the Internet and automatically set the time. If you are not connected to the Internet, you must enter the date and time manually.

1. In the Language & Clock section, you can view or modify the following settings:

Language	From the drop-down list, select the language you'd like to display on your My Cloud device web pages. The default language is English.
----------	--

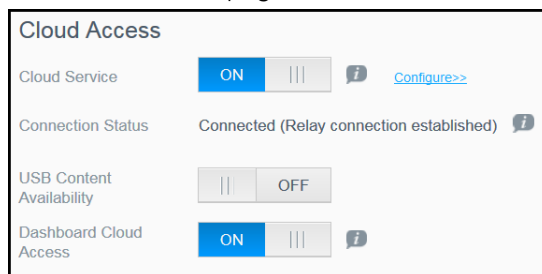
Time Zone	From the drop-down list, select the time zone where your device is located.
NTP Service	Enable or disable the Network Time Protocol (NTP) service, which automatically synchronizes your device to update the time and date.
Primary Server	Change the primary server used for your NTP service. <ul style="list-style-type: none"> To change the primary server used for your NTP service, click Configure, Click Add User NTP and enter the URL address of the new primary server. Click Save.
Date & Time	Displays the device date and time. This information is synchronized to the NTP server by default.
Time Format	From the drop-down list, select 12 (12-hour clock) or 24 (24-hour clock).
Date Format	From the drop-down list, select the date format you'd like to use to display the date on your device.

- Click **Save** for each change you make.

Cloud Access

Use the following steps to turn cloud access on or off for all users (i.e., control whether computers and mobile devices can access the content on the My Cloud device).

Note: This action turns on/off cloud access for the entire My Cloud device. To turn on access for an individual user, see “Configuring Cloud Access for a User” on page 40.



- Scroll down to the Cloud Access area of the General screen.
- In the Cloud Service field, ensure that the toggle button is set to ON. The Connection Status changes to Connected (<Current status of cloud access connection>).
- Click **Configure** to change the type of connection you use for your cloud access.

On the Cloud Access Connection Options screen, there are three access options:

- Auto:** Auto uses UPnP (Universal Plug and Play) to attempt to open ports on your router. If successful, a direct connection is established between your device and your apps.
- Manual:** Establishes a connection through the two selected ports. If either port is unavailable, a relay connection is established. A manual router configuration is required for this option. For more information, refer to your router manufacturer's guidelines.

- **Win XP:** Establishes a connection through ports 80 and 443. If these ports are unavailable, a relay connection is established. This option is required if you are using Windows XP.

Note: By default, the My Cloud device automatically establishes a direct connection between your mobile devices and router.

4. In the Content Database field, click **Rebuild** to rebuild your My Cloud database.

Note: Only perform this option to troubleshoot if you suspect database corruption.
5. Click **Apply**. The Connection Status field indicates that your device is connected.

USB Content Availability

This option allows you to turn on My Cloud device access to USB content.

- In the USB Content Availability field, click the toggle button to ON.

Dashboard Cloud Access

This option allows you to turn on remote access to the Dashboard from the cloud.

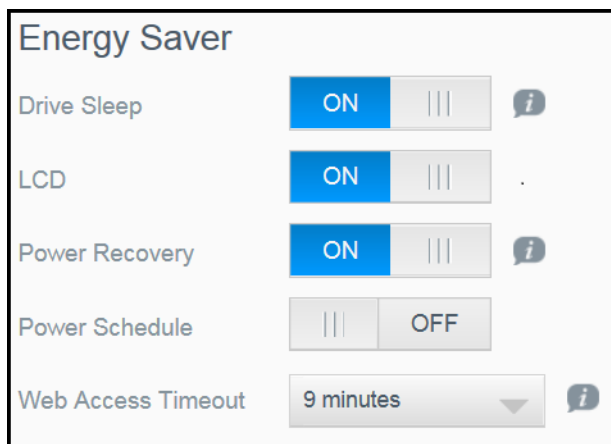
1. In the Dashboard Cloud Access field, click the toggle button to turn on access to the Dashboard from the cloud remotely.

Note: Selecting this option allows you to perform administrator functions remotely.
2. Review the information on the screen, enter and reenter a password for your administrator account, then click **Apply**.
 - If your administrator account already has a password associated with it, review the Dashboard Cloud Access screen, then click **OK**.

Note: If you set your Cloud Setting to Manual, you will have to access your device remotely using the ports you selected during the manual cloud setup. Example: If you setup your manual HTTP port as 5040, you'd use the following address to access your device: `http://<Device IP Address>:5040`.

Energy Saver

The Energy Saver fields allow you to reduce the energy required to run your My Cloud device. Use the following information to configure the energy saving options on your My Cloud device.

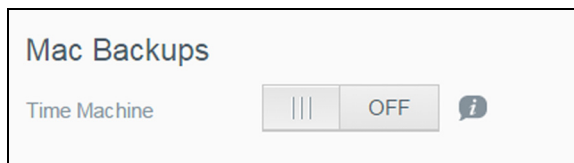


View or change the following settings:

Drive Sleep	<p>Enabling this function allows the hard drives to go into standby mode to save power after a designated period of inactivity. Drive Sleep is enabled to sleep after approximately 10 minutes by default.</p> <ul style="list-style-type: none"> To enable/disable Drive Sleep, click the toggle button.
LCD	<p>Enabling this function allows the device LCD to go into standby mode to save power after a designated period of time. LCD is enabled to go into standby mode after 10 minutes by default.</p> <ul style="list-style-type: none"> To enable/disable LCD, click the toggle button. <p>This option is only available for 4-bay My Cloud devices.</p>
Power Recovery	<p>Automatically restarts your device from a previously unexpected shutdown due to power failure. Power Recovery is enabled by default.</p> <p><i>Note:</i> If you disable this feature, your device will not automatically power on after an unexpected shutdown.</p> <ul style="list-style-type: none"> To enable/disable Power Recovery, click the toggle button.
Power Schedule	<p>The Power Schedule allows you to schedule shutdowns for your My Cloud device.</p> <ol style="list-style-type: none"> To enable/disable Power Schedule, click the toggle button. Click Configure to customize your power schedule. Click on the day of the week and time(s) to schedule shutdowns for your device. Click Save.
Web Access Timeout	<p>Automatically logs you out of the system after a designated amount of time.</p> <ul style="list-style-type: none"> From the Web Access Timeout drop-down menu, scroll down to select the amount of time you'd like to use for your system timeout. The system updates automatically.

Mac Backups

This section of the General screen enables or disables Time Machine backups of Mac computers.



Important: You must set a password for your Admin account in order to restore your Time Machine backups.

To configure backup settings:

1. In the Mac Backups area, click the toggle button to ON to enable Time Machine backups, if not previously enabled.
2. Click the **Configure** link to display the Time Machine Settings dialog.
3. From the **Select a Share** drop-down list, select a share you'd like to use to back up your Mac data.
4. In the Maximum Size field, move the slider to indicate the maximum value you'd like to use for your backup.

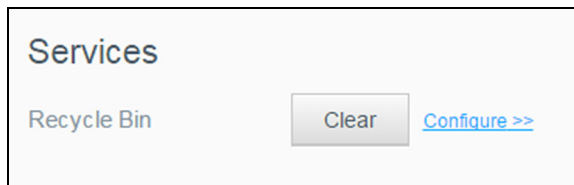
Note: Increasing the maximum backup value after the initial backup has no effect on existing backups. WD recommends leaving this setting at the maximum value for your initial backup. After the first backup is complete, you can change the backup size by dragging the Maximum Size slider.

5. Click **Save**.

Important: Once Time Machine begins to back up your files to a selected share, we recommend that you continue to back up to that share. Switching shares generates a new backup file which will not contain your previously saved information.

Services

This section of the General screen enables or disables the Recycle service available on your My Cloud device.



Clearing your Recycle Bin

Use the following steps to clear your device's Recycle Bin.

Automatically Clear Recycle Bin:

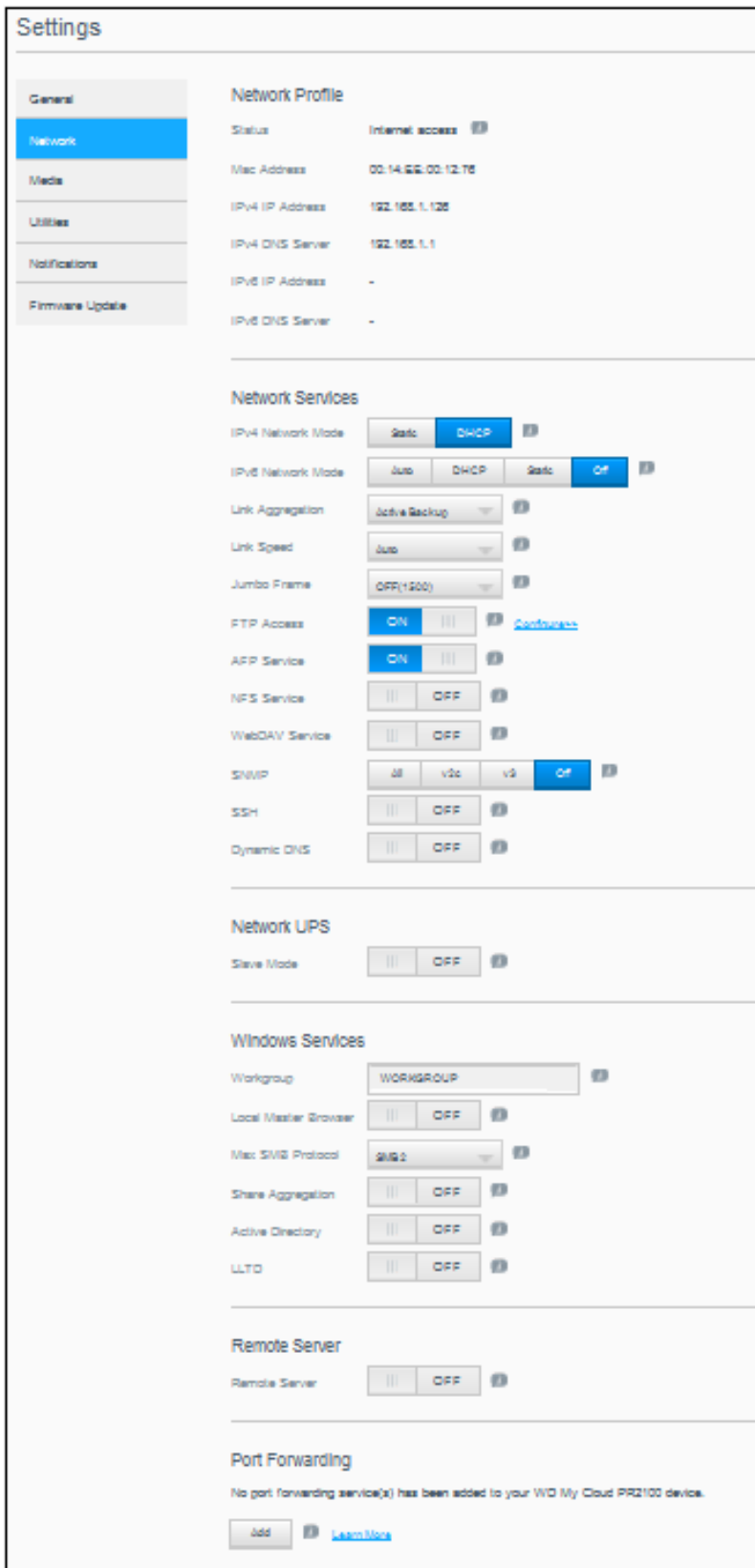
1. In the Services > Recycle Bin area, click **Configure**.
2. In the Auto clear Recycle Bin field, click the toggle button to turn ON the Auto clear function.
3. In the File retention time field, enter the number of days you'd like to retain your data before it is cleared.
4. Click **Save**.

Manually Clear Recycle Bin:

1. To manually clear the Recycle Bin on your device, click **Clear**.
2. Click OK to confirm.

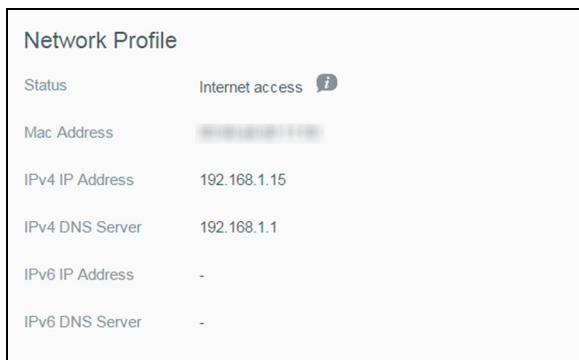
Network

The **Network** screen displays the device’s MAC and IP addresses and allows you to set network options such as FTP access, remote servers, and workgroups.



Network Profile

The Network Profile section of the Network screen displays network information for the My Cloud device.

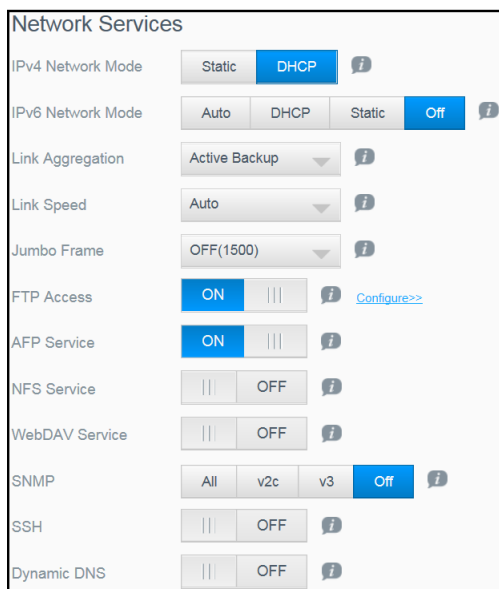


The Network Profile section displays the following information:

Status	The current status of Internet connectivity.
MAC Address	The Media Access Control (MAC) address for this device.
IPv4 IP Address	The IP version 4 address for this device.
IPv4 DNS Server	The IP version 4 DNS server address for this device.
IPv6 DNS IP Address	The IP version 6 address for this device.
IPv6 DNS Server	The IP version 6 DNS server address for this device.

Network Services

The Network Services section of the Network screen allows you to enable or disable the services available on your My Cloud device.



You can review or update the following fields:

IPv4 Network Mode	<p>By default, the network mode is set to DHCP, which means the My Cloud device automatically gets the IP address and other settings from your network.</p> <ol style="list-style-type: none"> Select the method of assigning the device's unique IPv4 address: <ul style="list-style-type: none"> Static: Static IP address allows you have the same IP address every time you connect. You will be prompted for IP Address, Subnet mask, Gateway IP address, and DNS Server. (If you don't know this information, please check your router settings.) DHCP: DHCP Client causes the My Cloud device to obtain an IP address and associated settings automatically from the local DHCP server. <p><i>Note:</i> When configuring Static or DHCP, record your Subnet mask, Gateway IP address, and DNS Server in a safe location for future reference. This information will not be displayed once it is entered into the My Cloud server.</p> Complete the LAN Setup Wizard to setup your network mode.
-------------------	---

IPv6 Network Mode	<p>The IPv6 format is a new IP standard that specifies the formats of packets and the addressing scheme across multiple IP networks. By default, this option is set to Off. Select the method of assigning the device's IPv6 address:</p> <ul style="list-style-type: none"> Auto DHCP Static Off <p>Once selected, complete the following fields on the associated screen, then click Apply:</p> <ul style="list-style-type: none"> IP Address Prefix Length Default Gateway DNS Server1 DNS Server2 <p>When configuring the Static or DHCP, record your Subnet mask, Gateway IP address, and DNS Server in a safe location for future reference. This information will not be displayed once it is entered into the My Cloud server.</p>
-------------------	--

Link Aggregation	<p>This is also called Bonding and refers to the use of two LAN cards, present in your NAS, and two cables connected to your router simultaneously. This improves performance and reliability.</p> <p>Select the type of link aggregation you'd like to use for your device from the pull-down menu, or select OFF to cancel Link Aggregation. Click Apply to save your selection.</p>
------------------	--

Link Speed	<p>Select the link speed for your network from the pull-down menu, then click Apply. Options Include:</p> <ul style="list-style-type: none"> Auto 100 1000
------------	--

Jumbo Frames	<p>Jumbo frames are large IP frames used to increase performance over supported networks. Select the Jumbo Frame option for your network from the pull-down menu, then click Apply.</p> <p><i>Note:</i> All devices on your network (e.g., router, computer) must support and be configured for this option in order to maximize performance.</p>
FTP Access	<p>File Transfer Protocol (FTP) enables the transfer of data from one computer to another through a network.</p> <p>To enable FTP Access:</p> <ol style="list-style-type: none"> 1. Click the toggle button to ON. 2. Review the Note about Shares settings, then click OK. 3. Click Configure. 4. On the FTP Settings screen, enter the following information: <ul style="list-style-type: none"> • Maximum Users: From the drop-down menu, select the maximum number of users you'd like to have FTP access. • Idle Time: Enter the amount of time, in minutes, you'd like the FTP to be idle before it times out. • Port: Enter the port to be used for FTP access. • Flow Control: Select either Unlimited or Customize. If you select Customize, enter a Flow Control value. 5. Click Next. 6. In the Passive Mode field, select either Default or Customize. If you select Customize, enter Passive Mode values. 7. Select the check box if you'd like to report external IP in PASV (Passive) mode: <ul style="list-style-type: none"> • Click Get IP to enter the External IP address. • Click Next. 8. Enter the following information: <ul style="list-style-type: none"> • Client Language: Select the client language from the drop-down menu. • TLS: Select the Transport Layer Security (TLS) check box next to either Implicit TLS or Explicit TLS connections, if applicable. • FXP: To enable File eXchange Protocol (FXP), click the toggle button to ON. 9. Click Next. 10. Enter any IP addresses that you want to block from FTP access. then select either Permanent or Temporary from the drop-down menu. Click Apply to save your entries. 11. Click Finish.
AFP Service	<p>Apple File Protocol (AFP) Service is automatically enabled if you are set up for Time Machine backups.</p> <ul style="list-style-type: none"> • To enable/disable AFP Service, click the toggle button. <p>WARNING! Mounting or ejecting a USB drive while performing an NFS or AFP file transfer will interrupt the file transfer process.</p>

NFS Service	<p>Network File System. Select this option to enable NFS Service for your network, which allows a user to access files over a network.</p> <ul style="list-style-type: none"> To enable/disable NFS Service, click the toggle button. <p>WARNING! Mounting or ejecting a USB drive while performing a file transfer will interrupt the file transfer process.</p>
WebDAV Service	<p>Select this option to enable Web Distributed Authoring and Versioning (WebDAV) service to enable web access to content within the same network.</p> <ul style="list-style-type: none"> To enable/disable WebDAV Service, click the toggle button. <p><i>Note:</i> In order to connect to the WebDAV service, use the following IP address: <code>http://<server ip address>:8080/Public</code></p>
SNMP	<p>Simple Network Management Protocol (SNMP) manage devices over IP networks. Select from the following to choose all, or a specific SNMP version:</p> <ol style="list-style-type: none"> Click All to enable v2c and v3 SNMP versions. <ul style="list-style-type: none"> Location: Contact Information Notifications: Click the toggle button to set Notifications to ON, and enter the Notification IP Address. User Management (SNMPv3): Click Users, and then click Add User. Enter the User Name. Select the Security Level from the drop-down menu to set authentication and encryption levels. Click the View drop-down menu to allow queries at the System level and Network level, or select All to allow queries to all device information. Click Apply. Click v2c. <ul style="list-style-type: none"> Location Contact Information Notifications: Click the toggle button to set Notifications to ON, and enter the Notification IP Address. Click Apply. Click v3. <ul style="list-style-type: none"> Location Contact Information Notifications: Click the toggle button to set Notifications to ON, and enter the Notification IP Address. To add Users, click Users, and then click Add User. Enter the User Name. Select the Security Level from the drop-down menu to set authentication and encryption levels. Click the View drop-down menu to allow queries at the System level and Network level, or select All to allow queries to all device information. Click Apply. Click Off to turn off SNMP service. <p>See the WD Tech Support Downloads page at http://support.wdc.com to download the MiB configuration file.</p>

SSH	<p>Select this option to securely access your personal cloud and perform command-line operations via the Secured Shell (SSH) protocol. SSH is disabled by default. Use the toggle button to turn ON or OFF.</p> <ol style="list-style-type: none"> To enable SSH, click the toggle button to ON. Review the SSH message, select the I accept check box, and click OK. <p>WARNING! Please note that modifying or attempting to modify this device outside the normal operation of the product voids your WD warranty.</p> <ol style="list-style-type: none"> Create a password, and click Save. <p><i>Note:</i> The SSH login User Name is sshd.</p>
Dynamic DNS	<p>Select the Dynamic Domain Name System (DNS) to host a server (Web, FTP, Game server, etc.) using a domain name.</p> <ol style="list-style-type: none"> To enable Dynamic DNS, click the toggle button to ON. Click Configure. On the DDNS Settings screen, enter the following information: <ul style="list-style-type: none"> Server Address: Select a server address from the drop-down menu. Host Name: Enter a Host Name for the server. User Name or Key: Enter a User Name or Key for the server. Password or Key: Enter a password or key for the server. Verify Password or Key: Re-enter the password or key for the server. Click Save.

Network UPS

An Uninterruptible Power Supply (UPS) is a device that works off of a battery and keeps devices that are connected to the UPS port running, for at least a short time, if the main power source goes out. When a My Cloud device is connected to a UPS, the drive will automatically shut down when the UPS is drained to a specified percentage. See Knowledge Base Answer ID 11852 for a list of supported UPS devices.

UPS Connection for a Single My Cloud Device

For a single My Cloud device, the connection to a UPS is accomplished through a USB connection from the My Cloud device to the UPS.

UPS Connection for Additional My Cloud Device(s)

Additional My Cloud devices on the same local area network (LAN) can be added to the single, My Cloud-to-UPS scenario mentioned above using a master/slave protocol. The UPS Master device (the first, or single, My Cloud device connected to the UPS) controls the additional, slave My Cloud device(s).

The slave My Cloud device(s) communicates with the UPS Master device via IP address. If the UPS is discharged to the specified percentage, all of the My Cloud slave devices will automatically shut down properly.

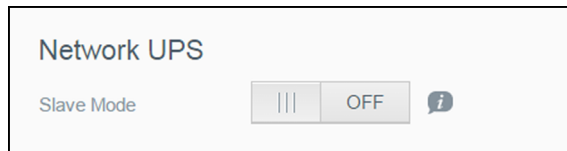
Use the following procedure to set up a UPS Master and Slave Connection.

Setting up a UPS Master and Slave Connection

This procedure is performed from an additional, slave My Cloud device(s), using the IP address of the UPS Master My Cloud device.

Note: Record the IP address of the UPS Master My Cloud device before starting this procedure. The Master UPS IP address can be found in “Network Profile” on page 76.

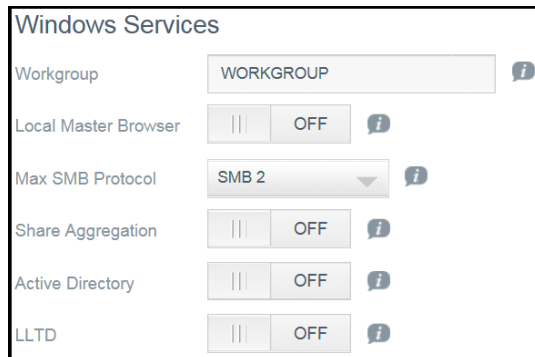
1. Connect the slave My Cloud device to your LAN via Ethernet cable (for details, see “Preparing your My Cloud Device for Use” on page 9).
2. On the slave My Cloud device, go to **Settings > Network > Network UPS** and click the Slave Mode toggle button to **ON**. The Network UPS Slave Mode screen appears.



3. Enter the IP address of the UPS Master My Cloud device. An “In progress” screen appears, and when the setting is updated the Network UPS Slave Mode is set to ON.
4. Repeat this procedure for each slave My Cloud device to be linked to the UPS device.

Windows Services

The Windows Services section of the Network screen allows you to configure Window Services applications on your My Cloud device.



Workgroup

The Workgroup feature allows devices in the same workgroup to access one another. This option is only available for Windows operating systems. Each time you add a device to your network, assign it the same workgroup name to enable access.

1. Enter the name of the WORKGROUP.
2. Click **Apply**.

Local Master Browser

The Local Master Browser feature allows you to collect and record resource and/or service information across multiple subnets.

- To enable/disable the Local Master Browser, click the toggle button to ON.

Max SMB Protocol

The Max SMB Protocol feature allows you to select the maximum Server Message Block (SMB) protocol you'd like to use for your device.

- Select the Max SMB Protocol from the drop-down menu.

Share Aggregation

Share aggregation (similar to Distributed File System [DFS]) consolidates shares from other My Cloud devices, or network devices that support the SMB protocol. Enabling this function allows you to improve data availability. Distributed File System is disabled by default.

1. To enable Share Aggregation, click the toggle button to ON.
2. In the Share Aggregation Settings window, enter the Root Folder Name to create a container for the linked, remote shares. Click Apply.
3. Click Add Link to connect to add links to aggregate remote shares.
 - Enter the Local Folder Name for the folder displayed under the Root Folder.
 - Enter the Remote Host hostname, or, the IP address of the target device.
 - Manually enter the Remote Share name, or, click Get Remote Share Folder to display Remote Host shares.
 - Click Apply.

Active Directory

Enabling this function allows your My Cloud device to join an existing Windows domain. Active Directory is disabled by default.

1. To enable/disable Active Directory, click the toggle button. The Active Directory Settings screen appears.
2. Enter the following information:

User Name	Enter the Active Directory server account name.
Password	Enter the Active Directory server password.
Domain Name	Enter the fully qualified name (FQDN) of the Active Directory to join.
DNS Server	Enter the Domain Name System (DNS) Server IP address.

3. Review the information on the screen, then click **Apply**.

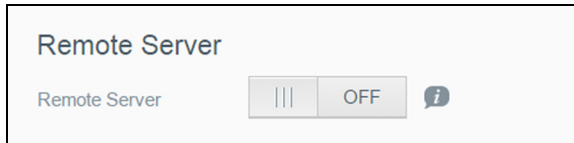
LLTD

This enables/disables the Link Layer Topology Discovery (LLTD) protocol. Select this option to enable LLTD on your network for enhanced network discovery and diagnostics on Microsoft Windows machines.

- To enable/disable LLTD, click the toggle button.

Remote Server

The Remote Server section of the Network screen allows you to enable your My Cloud device to act as a remote server, allowing you to back up shares from another compatible My Cloud on the LAN or WAN.



Note: To see your My Cloud device over the Internet, ensure that you've added port forwarding rules for both SSH and Remote Backup services. (See "Network Services" on page 76.)

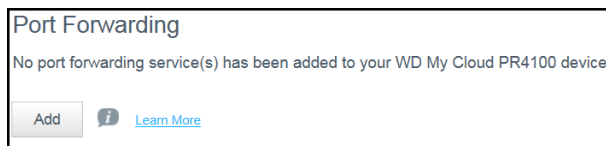
To enable Remote Server:

1. Click the toggle button to **ON**. The Remote Server screen appears.
2. Enter a backup Password to enable remote backups.
3. Click **Apply**. The system updates and the Remote Server is enabled.

Port Forwarding

The Port Forwarding section of the Network screen allows you to manage your connections to particular services by assigning default or custom port numbers.

For additional information on Port Forwarding, click Learn More to see Knowledge Base Answer ID 8526.



Adding Port Forwarding Services

1. Click **Add** to add port forwarding service(s) to your My Cloud device.
2. On the Port Forwarding Settings screen, click either **Select the default service scan** or **Customize a port forwarding service**, and then click **Next**.
 - If you chose the Select the default service scan: Choose the default service scan you'd like to use for port forwarding, and then click **Finish**.
 - If you selected Customize a port forwarding service, complete the following fields:
 - **Service:** Enter a service for your port forwarding.
 - **Protocol:** Select a protocol from the drop-down menu.
 - **External Port:** Enter an external port number for your port forwarding.
 - **Internal Port:** Enter the internal port number for your port forwarding.
 - Click **Finish**.

Modifying Port Forwarding Services

1. Click **Details** next to the port forwarding service you'd like to modify.
2. Make all necessary changes, and then click Finish.

Deleting Port Forwarding Services

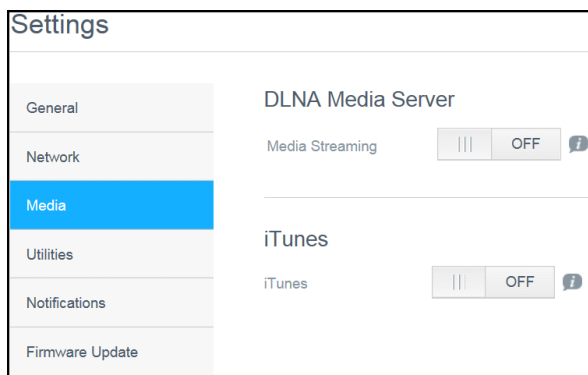
1. Click **Details** next to the port forwarding service you'd like to delete.
2. Click **Delete**. Your Port Forwarding service is deleted and removed from the Port Forwarding list.

Media

On the Media screen, you can enter DLNA (Digital Living Network Alliance) media server and iTunes media player settings, so that you can enjoy media in every room in your house.

- On the Navigation bar, click the **Settings** icon, then click **Media** in the left panel.

Note: DLNA and iTunes only work on your local network.

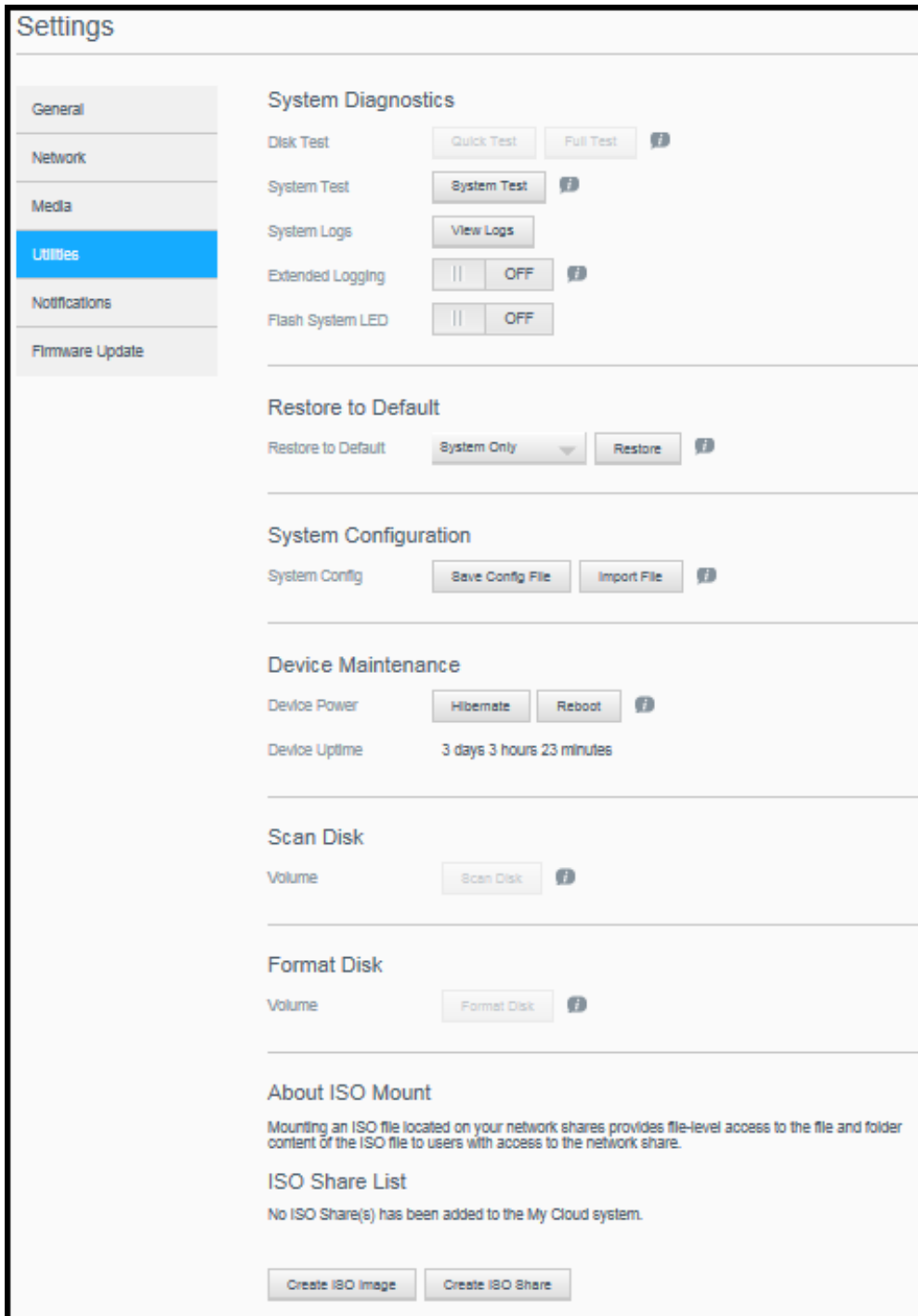


For instructions on entering media settings on this page and then displaying or streaming media, see “Playing/Streaming Videos, Photos, & Music” on page 62.

Utilities

On the Utilities page, you can test the My Cloud device and get diagnostic information, restore the device to factory defaults, reboot or shut down the device, and import or export a configuration file.

To access the Utilities screen, click the **Settings** icon and then click **Utilities** in the left pane.



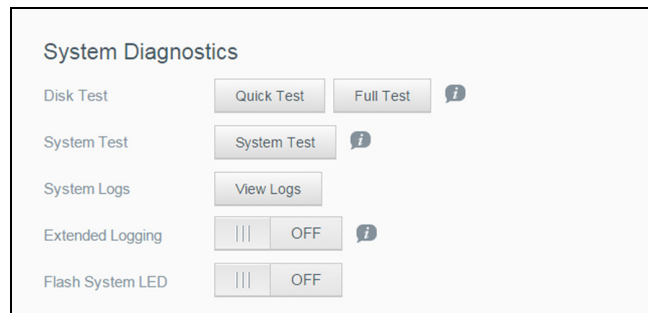
System Diagnostics

Run system diagnostic tests if you are having problems with your device. You can also view your system logs, and enable extended logging for your diagnostics.

Diagnostic Tests

There are three types of diagnostic tests:

- **Quick Test:** The quick test checks the hard drives for major performance problems. The result of a quick test is a pass or fail evaluation of the hard drive's condition. The quick test can take several minutes to complete.
- **Full Test:** The full test is a more comprehensive drive diagnostic. It methodically tests each and every sector of the hard drives. You will be informed of the condition of the hard drive once the test is performed. The full test may take hours to complete, depending on the size and data configuration of the hard drives.
- **System Test:** The system test reviews the health of your device hardware (hard drives, fan, system clock, and device temperature). On the Utilities page, click **Quick Test**, **Full Test**, or **System Test**. Test progress and test results appear.



Running a Diagnostic Test:

- Review the test results and click **Close**.
 - If the device fails the test, click the Help icon at the top of the page, then click **Support** to get assistance.

Viewing System Logs

System logs provide a list of the events occurring on your device. Use the following steps to view your system logs.

1. In the System Diagnostics area, click **View Logs**.
2. On the View Logs dialog, review the device log entries. To customize the log:
 - Select the Log Level from the pull-down menu.
 - Select Filter By option from the pull-down menu.
 - To clear the log, click **Clear**.
3. Once you've reviewed the log, click **Close**.

Extended Logging

To capture extended logs in your diagnostics. Ensure that there are no backups, file activity, or file transfers being performed prior to extending your logging capability.

1. Click the toggle button to ON to turn on extended logging.

CAUTION! System reboot is required to turn extended logging on or off. Backups, file activity and transfers may be interrupted.

2. Read the Extended Logging message, and click OK. The My Cloud device reboots.

Flash System LED

The Flash System LED option flashes the device Power LED. This option is useful when you need to identify a specific device when you have more than one My Cloud device.

1. Click the toggle button to turn ON flash system LED.
2. Click the toggle button to the OFF position when the LED flash is no longer required.

Restore to Default

The Restore to Default area allows the Administrator to perform a restore on the My Cloud device.



Perform one of the following options to restore your system:

- **System Only:** Reverts system settings to their default values, but retains user data and shares.
- **Quick Restore:** Reverts all settings to their default values, erases all user data and shares, and retains default shares. Quick Restore creates a new file table on the device, but does not fully overwrite or erase the drive, so data recovery programs can be used to restore user data and shares.
- **Full Restore:** Reverts all settings to their default values, deletes all user data and shares permanently, and retains default shares. Data recovery programs cannot be used to restore data; all user data and shares, with the exception of the default shares, are permanently deleted.

Important: Before doing a factory restore or a system update, you may choose to save your device's current configuration. At a later time, you can import a previously saved configuration. Keep in mind that importing a configuration after restoring factory defaults does not restore shares or users. See "Saving a Configuration File" on page 88," to create or restore a configuration file.

Note: To erase all of the data on your device, see "Format Disk" on page 89.

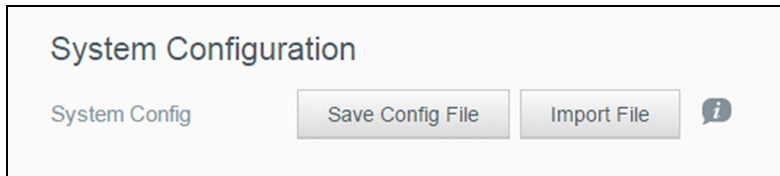
Restoring your System

Use the following steps to restore your system to one of the three available options.

1. In the Restore to Default area, click either **System Only**, **Quick Restore**, or **Full Restore**.
2. Click **Restore**.
3. Review the confirmation message and click **OK**. The device reboots. Don't unplug the device during this rebooting process. Once the reboot is complete, launch the dashboard.

System Configuration

The system configuration area allows you to save a configuration file or import an existing configuration file. This is useful if you perform a system restore and want to maintain your current configurations.



Saving a Configuration File

Use the following steps to save a configuration file.

- In the System Configuration area, click **Save Config File**. The configuration file saves to your desktop.

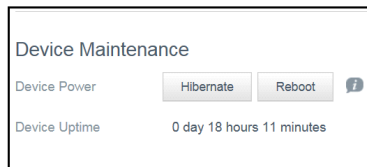
Importing a Configuration File

Use the following steps to save a configuration file.

1. In the System Configuration area, click **Import File**.
2. Navigate to the location of your saved configuration file and select it. The configuration file is loaded. The device reboots. Don't unplug the device during this rebooting process. Once the reboot is complete, launch the dashboard.

Device Maintenance

The Device Maintenance area allows you to shut down and reboot your My Cloud device. This area also displays the amount of time the device has been up and running.



Shutting down the Device

Use the following steps to safely shut down your My Cloud device.

1. In the Device Maintenance area, click **Hibernate**.
2. Review the confirmation message and then click **OK**. Your My Cloud safely shuts down.

Rebooting the Device

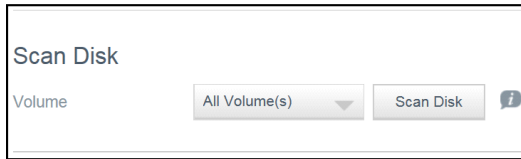
1. In the Device Maintenance area, click **Reboot**.
2. Review the confirmation message and then click **OK**. Your My Cloud safely reboots.

Viewing Device Uptime

The Device Uptime area displays the amount of time your device has been up and running.

Scan Disk

The Scan Disk area allows you to scan your device's hard disks for any errors.



Scanning Your Disk

Use the following steps to run a disk scan on your My Cloud device.

1. In the Volume area, select the volume you'd like to scan from the drop-down menu.
2. Click **Scan Disk**.
3. Review the confirmation message and click **OK**. Your My Cloud is scanned for disk errors.

Format Disk

The Format Disk area allows you to format your device's hard disk(s).



Formatting Your Disk

WARNING! The Format Disk option erases all of the user data and shares permanently, retaining default shares. Data recovery programs cannot be used to restore data; all user data and shares are permanently deleted.

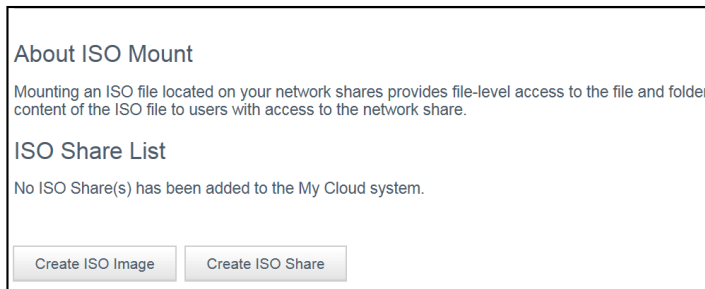
Formatting your disk will take several hours to complete.

Use the following steps to format the disks on your My Cloud device.

1. In the Volume area, select the volume(s) you'd like to format from the drop-down menu.
2. Click **Format Disk**.
3. Review the confirmation message, select the check box, and click **OK**. Your My Cloud begins formatting.

ISO Mounting

Mounting an ISO file located on your network shares provides file-level access to the file and folder content of the ISO file to users with access to the network share.



Creating an ISO Image

An ISO image is a file that is an exact copy of an existing file system. Use the following steps to create an ISO image.

1. In the About ISO Mount area, click **Create ISO Image**.
2. In the Image Size field, select the image size for the ISO image.
3. In the Image Path field, click **Browse** to select the folder you'd like to image, or enter the path for the data you'd like to image then click **OK**.
4. In the Image Name field, enter a name for your ISO image.
5. Click **Next**.
6. In the Select field, click **Overwrite** or **Skip**.
 - **Overwrite:** When overwrite is selected, files with the same name will be overwritten.
 - **Skip:** When skip is selected, files with the same name will be skipped.
7. Select the folders and files you'd like to add to your image file in the left column, then click **Add>>**.
8. Select the folders and files that you'd like to remove from the ISO image, then click **<<Remove**.
9. Click **Next**. Review the message.
10. Click **Finish**.

Creating an ISO Share

Use the following steps to create an ISO share.

1. Click **Create ISO Share**.
2. Browse to the ISO file you'd like to include in your ISO share and place a check next to the file.
3. Enter the share description, then click **Next**.
4. Click **Next**.
5. Complete the following fields:
 - **Media Serving:** To enable Media Serving for the ISO Share, click the toggle button to ON.
 - **FTP Access:** To enable FTP Access for the ISO Share, click the toggle button to ON.

- **WebDAV Access:** To enable WebDAV Access for the ISO Share, click the toggle button to ON.

Note: If FTP Access or WebDAV access are disabled for the device, the FTP Access and WebDAV Access fields will be grayed out.

6. Click **Next**.
7. Click the toggle button to ON to enable NFS Access for the ISO Share.
 - Note:** If NFS Access is disabled for the device, the NFS Access fields will be grayed out.
8. Enter the host IP address.
9. Click **Apply**.
10. Click **Save**. The new ISO share is displayed in the ISO Share List.

Viewing the Details of an ISO Share

Use the following steps to modify an ISO share.

1. In the ISO Share area, click the **Details** icon next to the ISO share you want to view.
2. Review the ISO share details, then click **Close**.

Modifying an ISO Share

Use the following steps to modify an ISO share.

1. On the ISO Mount screen, click the Modify icon next to the ISO share that you'd like to modify.
2. The Edit ISO Share dialog box appears. Click **Next**.
3. Complete the following fields:
 - **Media Serving:** To enable Media Serving for the ISO Share, click the toggle button.
 - **FTP Access:** To enable FTP Access for the ISO Share, click the toggle button.
 - **WebDAV Access:** To enable WebDAV Access for the ISO Share, click the toggle button.
 - Note:** If FTP Access or WebDAV access are disabled for the device, the FTP Access and WebDAV Access fields will be grayed out.
 - **Public:** To enable public access to the share.
4. Click **Next**.
5. Click the toggle button to enable NFS Access for the ISO Share.
 - Note:** If NFS Access is disabled for the device, the NFS Access fields will be grayed out.
6. Enter the Host IP address.
7. Click **Apply**.
8. Click **Save**. The modified ISO share is displayed in the ISO Share List.

Deleting an ISO Share

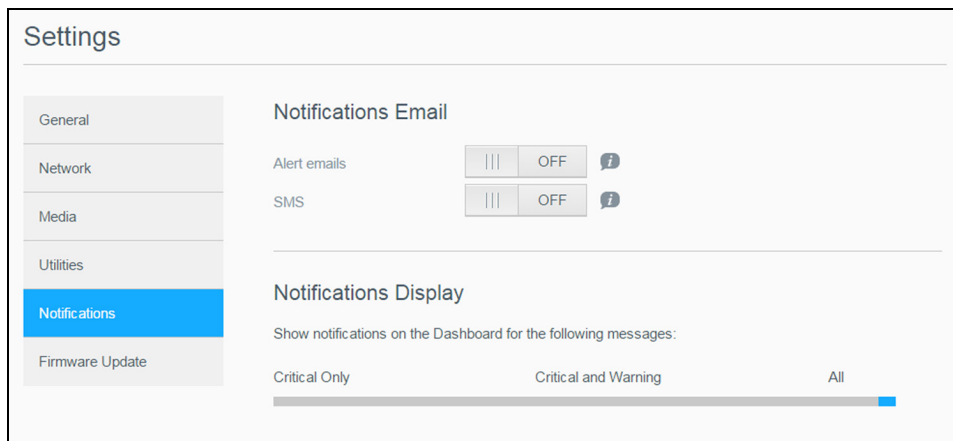
Use the following steps to delete an ISO share.

1. On the ISO Mount screen, select the Delete icon next to the ISO share that you'd like to delete.
2. Review the confirmation message, then click **OK**. The ISO share is deleted and removed from the ISO Share List.

Notifications

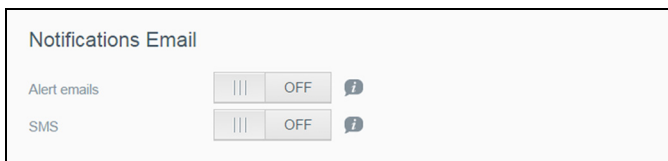
The My Cloud device provides notifications about various events, such as firmware updates, the success of firmware installations, and system shutdowns. Notifications display in the Alert area at the top of the screen and are also available by email, depending on how your device is configured (for additional information on Alerts, see “Managing Alerts” on page 25).

The Notification page allows you to set up email addresses for up to five users who will receive notifications, set up SMS alert messages for mobile devices, and set the level of alert for which you will be notified.



Notifications Email

The Notification Email area allows you to set up email alerts and SMS notifications for specified users.



Enabling Email Alerts

1. On the Navigation bar, click the **Settings** icon and click **Notifications** on the left pane.
2. To enable Alert emails, click the toggle button to **ON**.
3. Click **Configure**.
4. On the Notification screen, click on the slider bar to select the level of alerts you'd like to receive by email:
 - **Critical Only**: Send only critical alerts to the specified email address.
 - **Critical and Warning**: Send both critical and warning alerts to the specified email address.
 - **All**: Send all alerts (Informational, Critical, Warning) to the specified email address.
5. Click **New Email**.
6. Enter the email address where you'd like to receive alert emails and click **Save**.

7. Repeat step 5 and step 6 to enter up to five email addresses.
8. Click **Send Test Email** to validate the email addresses you entered.
9. Click **OK** and then check your email for a validation email.

Enabling SMS Notifications

Note: Check with your SMS service provider to obtain their requirements for sending SMS messages. Certain carriers may require you to send SMS/text messages by email.

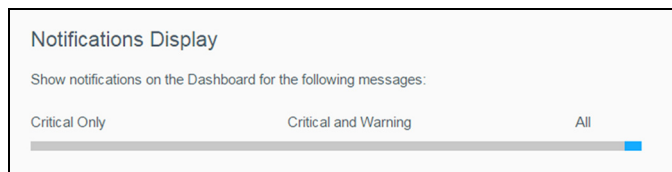
1. On the Navigation bar, click the **Settings** icon and click **Notifications** from the left pane.
2. To enable SMS, click the toggle button to **ON**.
3. Click **Configure**.
4. On the SMS Settings screen, enter the Provider Name.
5. Enter the SMS URL with the message content set to be “Hello world.”

Note: This SMS URL is used only for setup. No SMS message will be sent after setup is completed. Obtain the URL format requirements from your SMS service provider. They should contain the following parameters: username, password, destination phone, and message content.

6. Click **Next**.
7. Select the corresponding category for each SMS parameter from the drop-down menu.
8. Click **Finish**. Your SMS notification is now set up.

Notifications Display

The Notifications Display allows you to select the type of notifications that are sent to you.

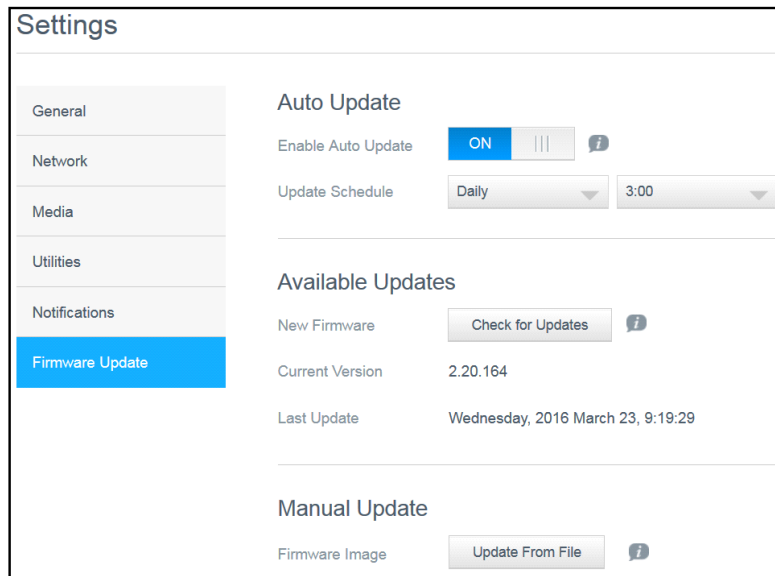


1. On the Notification Display screen, click on the slider bar to select the level of notifications:
 - **Critical Only:** Send only critical alerts.
 - **Critical and Warning:** Send both critical and warning alerts.
 - **All:** Send all alerts (Informational, Critical, Warning).

The system updates with your selection.

Firmware Update

The Firmware Update page allows you to set up the device to update the My Cloud firmware automatically or to manually check for an update file. The current version number and the date of last update of the firmware also display on this screen.

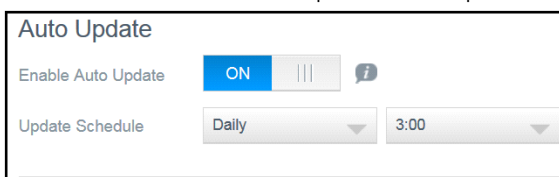


Auto Update

Auto Update allows you to schedule your My Cloud device to conveniently check for available software updates and install them automatically. This is the easiest way of ensuring the My Cloud firmware is current.

Note: After a firmware update installs, the My Cloud device may reboot. Since a reboot affects users' ability to access the cloud, schedule the updates to occur at times when the likelihood of users accessing the cloud are minimal.

Note: If you enable Auto Update, you are asked to manually reboot your system when the update is completed.

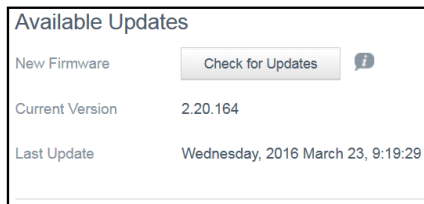


Updating Firmware Automatically

1. To enable Auto Update, click the toggle button to **ON**.
2. In the Update Schedule field, from the drop-down lists, specify the frequency (e.g., daily) and the time at which the device should look for an update on the WD website.
3. Click **Save**. Once saved, your device will check for firmware updates at the specified time and day. If an update is available, it will automatically install and prompt you for a reboot.

Available Updates

You can check for available updates at any time in the Available Updates area. This area also displays the current version of the firmware and indicates when the last firmware update was made.



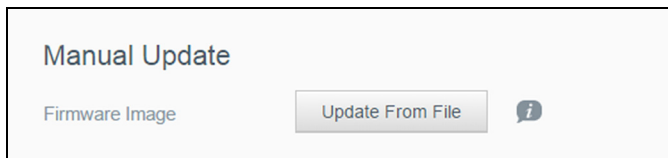
Checking for Available Firmware Updates

1. In the New Firmware field, click **Check for Updates**.
2. Review the Update Firmware screen and click **OK**.
 - If an update is available, click **Install and Reboot**.

Manual Update

Follow this procedure to perform a manual update.

Note: Ensure that you've downloaded the firmware file you need to install on your device from the WD Tech Support Downloads page at <http://support.wdc.com/product/download.asp>.



Manually Installing a Firmware Update

1. In the Manual Update section, click **Update From File**.
2. Navigate to the firmware update file and click **Open**.
3. Review the confirmation message and click **OK**.
The update installs on your device. When the update is complete, your My Cloud device reboots.

13

Regulatory Information

Regulatory Compliance

Regulatory Compliance

Federal Communications Commission (FCC) Class B Information

Operation of this device is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Requirements, Part 15

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause interference with radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, you are encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the retailer or an experienced radio/television technician for help.

Any changes or modifications not expressly approved by WD could void the user's authority to operate the equipment.

ICES/NMB-003 Compliance

Cet appareil DE la classe B est conforme à la norm NMB-003 de Canada.

This device complies with Canadian ICES-003 Class B.

Safety Compliance

Approved for US and Canada. CAN/CSA-C22.2 No. 60950-1, UL 60950-1: Safety of Information Technology Equipment.

Approuver pour els Etas-Units et el Canada. CAN/CSA-C22.2 No. 60950-1: Secret equipment DE technologie de l'information.

This product is intended to be supplied by a listed limited power source, double insulated, or direct plug-in power unit marked "Class 2."

Product Model	Network Standby Power Consumption	Off Mode Power Consumption
My Cloud PR4100	N/A*	<0.5 W
My Cloud PR2100	N/A*	<0.5 W

*Small-scale server. Network standby power consumption not applicable.

CE Compliance for Europe

Verified to comply with EN55022 for RF emission; EN-55024 for Generic Immunity, as applicable; and EN-60950 for Safety.

GS Mark (Germany only)

Machine noise - regulation 3. GPSGV: Unless declared otherwise, the highest level of sound pressure from this product is 70db(A) or less, per EN ISO 7779. Maschinenlärminformations-Verordnung 3. GPSGV: Der höchste Schalldruckpegel beträgt 70 db(A) oder weniger gemäß EN ISO 7779, falls nicht anders gekennzeichnet oder spezifiziert.

KC Notice (Republic of Korea only)

기종별	사용자 안내문
B 급기기 (가정용방송통신기자재)	이기는가정용(B 급) 전자파적합기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다

Class B Device Please note that this device has been approved for non-business purposes and may be used in any environment, including residential areas.

Korean KCC certification ID: MSIP-REM-WDT-D8C

VCCI Statement

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 VCCI-B

Environmental Compliance (China)

部件编号	铅 (Pb)	Mercury (Hg)	Cadmium (Cd)	六价铬 (Cr (VI))	多溴联苯(PBB)	多溴联苯醚(PBDE)
PCBA	X	○	○	○	○	○
适配器主体	X	○	○	○	○	○
电缆	○	○	○	○	○	○
螺丝	○	○	○	○	○	○
脚垫	○	○	○	○	○	○
金属	○	○	○	○	○	○
塑料	○	○	○	○	○	○
木箱	○	○	○	○	○	○
标签	○	○	○	○	○	○

○：表示元件构成同种材料不含有杂质或所含杂质符合 SJ/T 11363-2006 规范所规定的最大允许搀杂范围。

X：表示元件所含物质超出 SJ/T 11363-2006 规范

HEVC Advance



14

Appendices

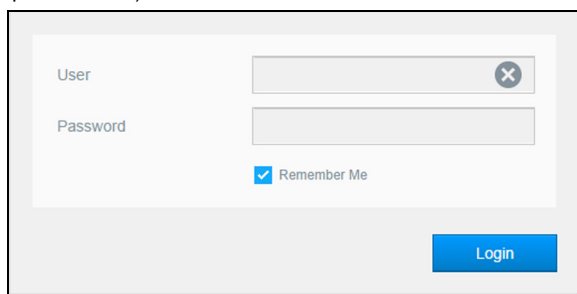
- [Appendix A: My Cloud Quick User Guide](#)
- [Appendix B: Safe Mode Firmware Update Procedures](#)
- [Appendix C: My Cloud Action Icons](#)
- [Appendix D: My Cloud Device URLs and Names](#)
- [Appendix E: Creating a User Import File](#)
- [Appendix F: Replacing the SO-DIMM Memory Module](#)

Appendix A: My Cloud Quick User Guide

This guide is primarily for My Cloud users, rather than the administrator.

Logging into My Cloud

1. Enter the name of your My Cloud device with applicable model number PR2100 or PR4100 (default name: mycloudPR<x100>) in the browser's address field:
 - **http://<device name>** (Windows) (Example: http://mycloudPR2100)
 - **http://<device name>.local** (Mac) (Example: http://mycloudPR4100.local)
2. Click **Go**.
3. On the My Cloud Login page, enter your User name and Password (the default is no password).



4. Click **Login**. The My Cloud dashboard home page appears.

The Dashboard Home Page

The My Cloud Home page has an information bar at the top-right area of the screen, a navigation icon bar across the page, an instant overview of the status of the device's main functions and links for updating settings.

Viewing the Home Page

The Home page is your gateway to the My Cloud device. From this page you can find:

- The capacity of the device
- Status and links to My Cloud device diagnostics, firmware information, and network activity
- Status and links to configure cloud access, users, and built-in applications to make your My Cloud device more productive

Capacity

The Capacity panel displays the amount of free storage left on your My Cloud device.

Quick Status

Note: Appears for users not the administrator.

The Quick Status area displays the total number of FTP, HTTP, P2P downloads performed.

Cloud Access Links

Note: These links only display for user accounts.

The Cloud Access Links allow you to access the software necessary to gain access to the My Cloud device from your desktop and mobile apps.

Downloads and Apps Information

Note: These links only display for user accounts.

The Downloads and Applications area displays information on the number of downloads and apps available on your device.

- To access the page associated with each download or applications, click the plus sign.
- To download files to your location, enter the information required for each download method.

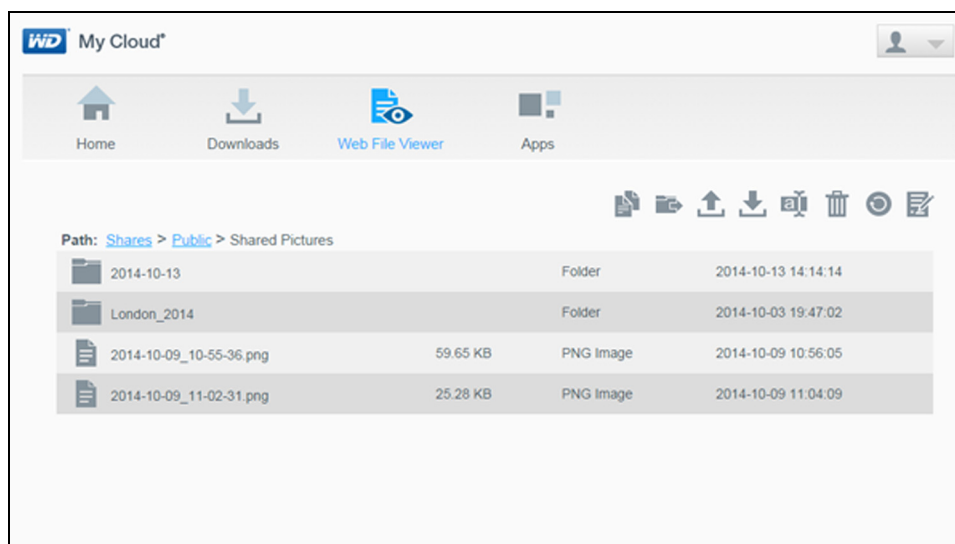
Downloads

The Downloads page allows you to download files using the following methods:

- HTTP (Hypertext Transfer Protocol)
 - FTP (File Transfer Protocol)
 - P2P (Peer-to-Peer)
1. In the left pane, click a download method.
 2. To download files to your location, enter the information required for each download method.

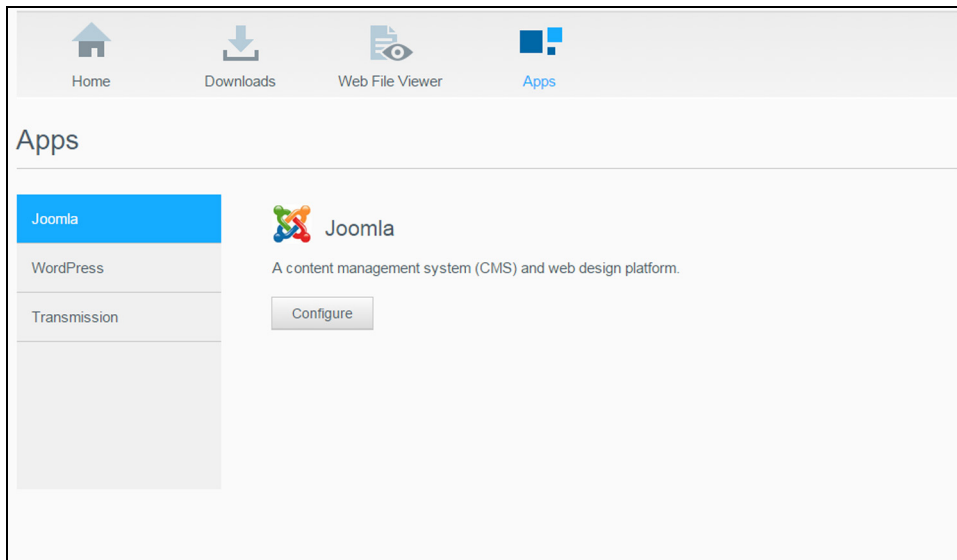
Web File Viewer

The Web File Viewer page provides access to the various files contained the My Cloud device for which you have access. On this screen you can see and manage files on the device.



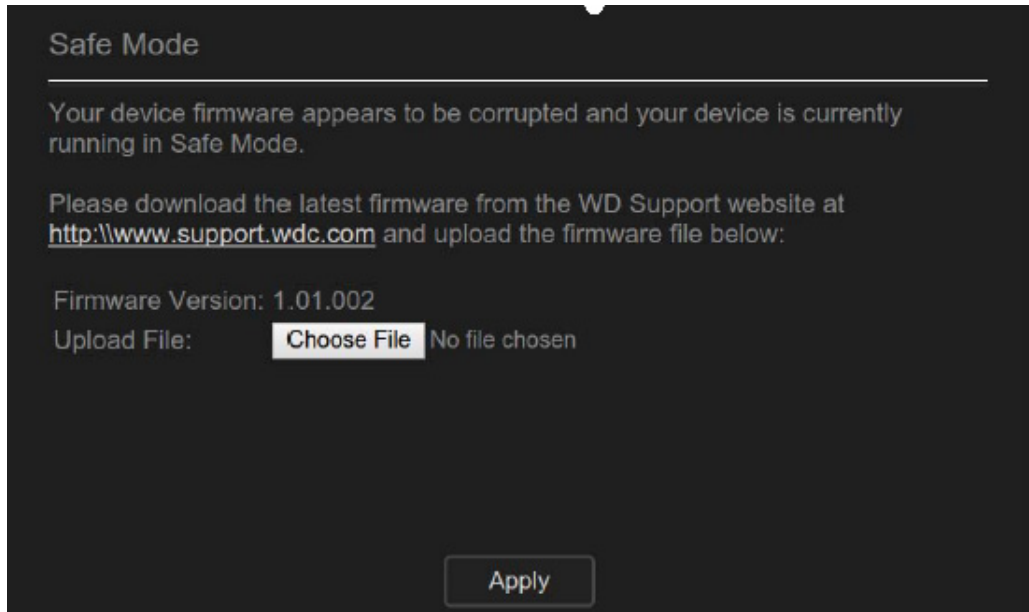
Apps

The Apps page provides access to the various apps available for your use on the My Cloud device. Available apps vary depending on what your administrator has implemented.



Appendix B: Safe Mode Firmware Update Procedures













If you see the following screen, use the steps outlined below to recover your device from safe mode.













Note: Before performing these steps, download My Cloud firmware from the WD support website (<http://support.wdc.com>) and save it to a location to which you can browse from your computer. Make sure to unzip the firmware file.

1. Log on to your router's DHCP LAN/Device Client Table to obtain the IP address for your device.
2. Type the device IP address in a browser window. The Safe Mode UI appears.
3. Browse to the location where you saved the downloaded firmware.
4. Click **Apply** to load the firmware.
5. On the dialog box, click **OK**. **The device reboots.**
6. Once your reboot is completed, ensure that you clear your browser's cache. Check your browser's help to determine the best way to clear the cache.
7. Once your device has completed the reboot, we recommend that you do a system restore ("Restore to Default" on page 87).

Appendix C: My Cloud Action Icons

Icon	Button Name	Actions
	Add App	Select this option to add an app to your My Cloud device.
	Add Group	Select this option to open the Add a Group dialog and add a group to your device.
	Add Shares	Select this option to open the Add Share dialog and add a share to your device.
	Add User	Select this option to open the Add User dialog and add a user to your device.
	Cloud Access	Set up, change, and remove remote cloud access to particular shares. Monitor remote access status.
	Delete	Select this to delete an alert.
	Delete Job	Select this option to delete the selected job.
	Delete Shares	Select this option to delete a share. WARNING! Deleting a share erases all files and folders on that share.
	Encrypted RAID Volume	Select this option if you'd like your RAID volume to be encrypted.
	Job Detail	Select this option to view the job.
	Job Detail	Select this option to view the details of the backup job.
	Modify Job	Select this option to modify a backup job.

Icon	Button Name	Actions
	My Cloud Dashboard Desktop Icon	Click this icon to open the My Cloud Dashboard.
	Read Only Access	Provides the user/group account with read only access to the selected share. The user/group member can view the share but can't update it.
	Read/Write Access	Provides a user or group account with read/write access to the selected share. The user/group members can view and update the share.
	Recover	Select this option to recover a remote backup.
	Remove an App	Select this option to delete an app from your My Cloud device.
	Remove Group	Select this option to remove a group from your device
	Remove User	Select this option to remove a user from your device.
	Start Backup	Select this option to start a device backup.
	Toggle	Allows you to turn a feature on or off.
	Unencrypted RAID Volume	Select this option if you'd like your RAID volume to be unencrypted.

Appendix D: My Cloud Device URLs and Names

Device URL

Use the device URL to access your device from a web browser.

Note: If you changes your device name at any time, the URL also change to the new name.

If your device name is...	Your Windows URL is...	Your Mac URL is...
My Cloud PR2100	http://mycloudPR2100	http://mycloudPR2100.local
My Cloud PR4100	http://mycloudPR4100	http://mycloudPR4100.local

Device Name

The device name appears in the Mac Finder and Windows Explorer.

Device Name	Window / Mac Name
My Cloud PR2100	MyCloudPR2100
My Cloud PR4100	MyCloudPR4100

Appendix E: Creating a User Import File

The User Import file is designed to quickly enter multiple users into your device. Provided below is the file format used to import your user information and examples of how each field works. See “Adding Multiple Users” on page 30 for steps on how to create multiple users with your User Import file.

User Import File format

Use the following format when entering your data into the User Import file.

- username/password/group/rw/ro/deny:quota

All fields are required. If you would like to leave a field blank, leave a space between the forward slashes (/) for that field.

Field Definitions

Provided below is a list of user import file fields, their definitions and an data example.

Required Fields	Definition	Example
username	User Name. Enter the name for your new user.	Joe Jones
password	User Password: Enter a password for your new user.	password
group	Group Name: Enter the name of the group to which you would like to add the new user. Note: The Group must exist before you can add a user to it. See “Adding a Group” on page 34 to create a new group.	Family
RW	Read/Write Shares: Enter the shares you would like the user to view and update. If you would like to provide Read/Write access to more than one share, separate the share names with an “:”	Public
RO	Read Only Shares: Enter the shares you would like the user to view only. If you would like to provide Read Only access to more than one share, separate the share names with an “:”	TimeMachineBackup
deny	Deny Access: Enter those shares to which the user will have no access.	financial;jill_video
quota	Quota Amount (TB:GB:MB): Enter the quota amount for the new user. To assign unlimited space, leave this field blank.	0:0:0:0

Sample User Import File

```
Joe/password/test/Public:SmartWare:TimeMachineBackup/  
Public:SmartWare:TimeMachineBackup/Test/0:0:0:0/  
Anne/yellow!/anne///0:0:0:0/  
Donald///SmartWare///0:0:0:0/  
Zoey/blue!807///0:0:0:0/  
Astra////anne/0:0:0:2/
```

Appendix F: Replacing the SO-DIMM Memory Module

Note: This procedure is applicable for the My Cloud PR4100 only.

The SO-DIMM memory module in the My Cloud device is upgradeable. The My Cloud device must be powered off prior to module replacement.

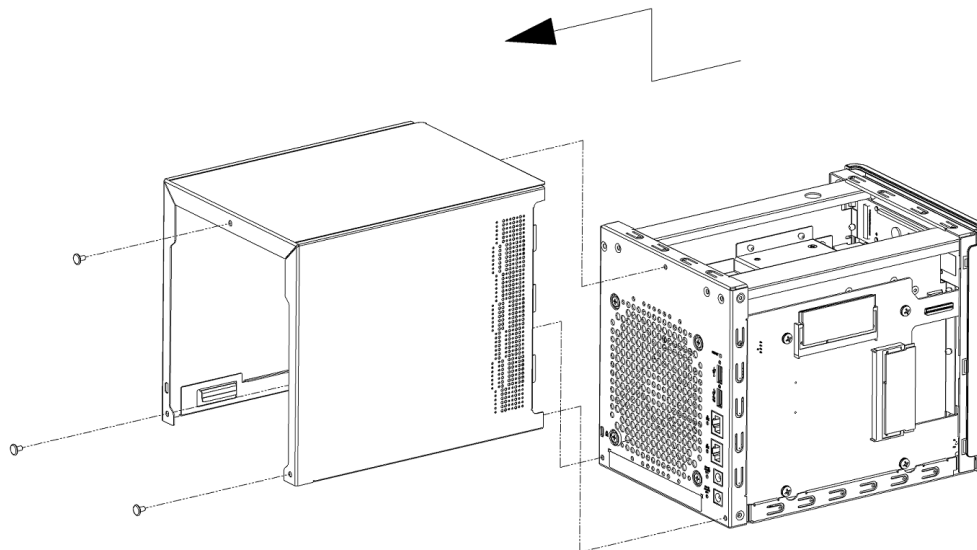
For details about the supported memory module, refer to <http://support.wdc.com>.

What you'll Need:

- Phillips screwdriver
- Replacement SO-DIMM Memory module

Replacing a SO-DIMM Memory Module

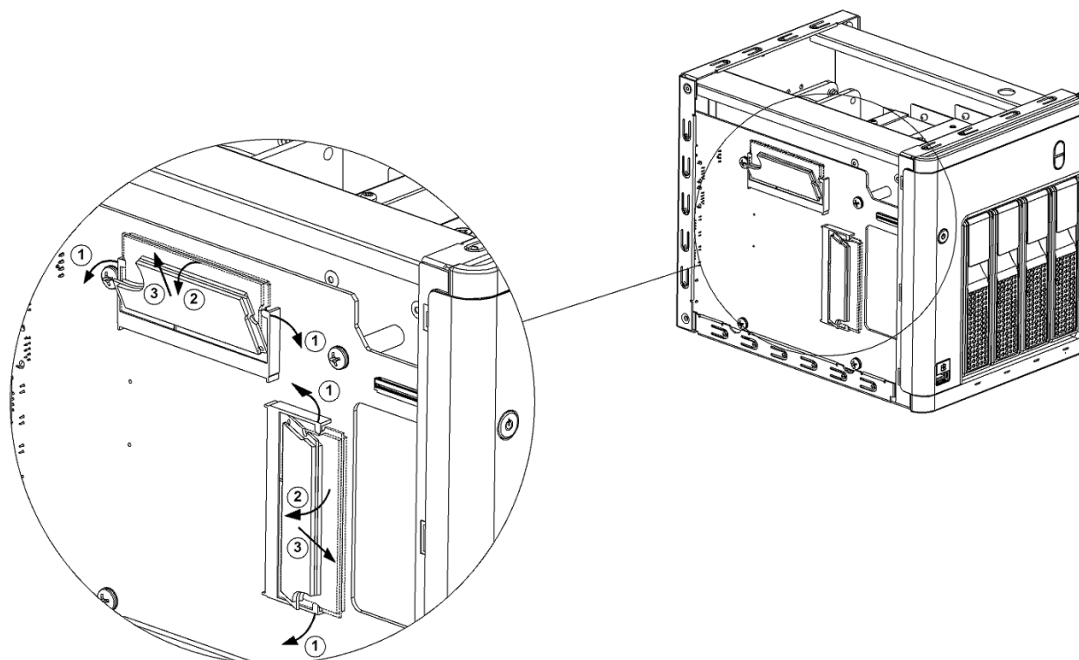
1. Before getting started, shut down the My Cloud device and disconnect all external connections.
2. Place the unit on a clean and stable surface, with the back of the unit facing you.
3. Release three (3) screws on the back of the unit.



4. Pull the unit cover toward you and up to release the cover.

5. Remove and replace the SO-DIMM memory module.

Note: This device uses memory modules in coordinated pairs. For a list of supported memory modules, refer to <http://support.wdc.com>.



6. Once the pair of SO-DIMM memory modules have been changed, replace the unit cover and replace and tighten the three (3) exterior screws.

Note: When replacing the cover back to the unit, be careful not to touch or damage the components on the PCBA.

Note: Do not over-tighten the PCBA screws.

7. Connect all external connections.
8. Restart the device.

Index

A

- about
 - apps 60
 - camera backups 51
 - disk status 55
 - DLNA 67
 - internal backups 47
 - iSCSI 56
 - media servers 62
 - shares 37
 - Volume Virtualization 58
 - WD Media Players 67
- accessing
 - content 14
 - general settings 69
 - iTunes on My Cloud device 67
 - online support ii
 - personal cloud using media players 66
 - remote cloud access 40
- accessories 3
- action icons 102
- Active Directory settings 82
- adding
 - a hard disk drive 9
 - a single user 30
 - apps 60
 - groups 34
 - media content to a folder 66
 - multiple users 30
 - port forwarding services 83
- AFP Services 78
- alerts
 - details 25
 - dismissing 25
 - email 92
 - icons 24
 - managing 24
 - viewing 25
- Amazon S3 Cloud
 - backing up to 50
 - enabling a backup 50
- apps
 - about 60
 - adding 60
 - deleting 61
 - managing 60
 - My Cloud Mobile 41

- updating 61
 - viewing 60
- Apps Panel 24
- assigning
 - a group to a user 32
 - quotas to a group 35
 - quotas to users 32
 - share access to groups 35
- audio files, supported 63
- automated support, requesting 26
- available updates, firmware 94

B

- backups
 - about 43
 - Amazon S3 Cloud 50
 - camera 51
 - cloud 49
 - deleting 48
 - ElephantDrive 50
 - internal 47
 - Mac 73
 - modifying 48
 - remote 46
 - USB 43
 - using USB Copy Button 45
- box contents 3

C

- camera backups
 - about 51
 - creating 51
- capacity
 - panel 20
 - storage 20
- changing the RAID mode 54
- Class B Device Notice, Korea 97
- cloud access
 - enabling on your device 40
 - settings 71
- cloud backups
 - about 49
 - Amazon S3 50
 - using Amazon S3 Cloud Backup 50
 - using ElephantDrive 49
- Cloud Devices Panel 22, 23
- common tasks 27
- compliance
 - Europe 96
 - machine noise, Germany 97
 - regulatory 96
 - safety 96

- configuration files
 - importing 88
 - saving 88
- connecting
 - a USB drive 43
 - a virtualized volume to a target 59
 - My Cloud device 10
- contacting WD Technical Support ii
- creating
 - a USB backup 44
 - a virtualized volume 59
 - an iSCSI target 57
 - an ISO Share 90
 - camera backups 51
 - internal backups 47
 - multiple users 31
 - new shares 38
 - remote backups 46
 - user import file 105
- customer support
 - documentation 27
 - FAQs 27
 - Forum 27
 - obtaining 25
 - WD contacts 27
- D**
- dashboard
 - at a glance 16
 - end user 98
 - home page 17
 - information icons 18
 - launching 16
 - navigation icons 18
- default settings, restore 87
- deleting
 - an app 61
 - an iSCSI target 58
 - an ISO Share 91
 - backups 48
 - port forwarding 83
 - shares 39
- device
 - activity 21
 - health 20
 - logging off 27
 - maintenance 88
 - processes 21
 - rebooting 27, 88
 - section 20
 - shutting down 88
 - status 19
 - viewing uptime 88
- diagnostics
 - section 20
 - tests 86
- disabling
 - an iSCSI target 57
 - DLNA 64
 - iTunes 65
- disk
 - adding to diskless drive 9
 - scanning 89
 - status,about 55
- diskless device, adding hard disk drives 9
- dismissing a system alert 25
- DLNA
 - about 67
 - devices 67
 - disabling 64
 - enabling 64
- drive sleep mode 73
- Dynamic DNS 80
- E**
- editing
 - group settings 34
 - shares 38
 - user settings 32
- ElephantDrive Cloud Backup
 - backing up to 50
 - enabling a backup 49
- emails
 - alerts 92
 - notification 92
- enabling
 - Amazon S3 Cloud backups 50
 - an iSCSI target 57
 - cloud access for a user 40
 - DLNA 64
 - ElephantDrive Cloud backup 49
 - iSCSI iSNS Client 58
 - iTunes 65
 - SMS notifications 92
- End User Guide 98
- Energy Saver
 - drive sleep mode 73
 - LCD 73
 - power recovery 73
 - power schedule 73
 - settings 72
 - web access timeout 73

- environmental compliance, China 97
- Ethernet cable, Important notice 10
- extended logging 86
- F**
- firmware
 - auto updates 94
 - dashboard section 21
 - updates 93
- Flash System LED 87
- front USB port, backups 45
- FTP Access 78
- G**
- general settings 68
 - accessing 69
 - Active Directory settings 82
 - cloud access 71
 - Energy Saver 72
 - language and clock settings 70
 - Local Master Browser 81
 - Mac backup 73
 - Network Profile 76
 - Network Services 76
 - Network settings 75
 - services settings 74
 - share aggregation 82
 - workgroup 81
- groups
 - about 34
 - adding 34
 - assigning a user 32
 - assigning quotas 35
 - assigning share access 35
 - assigning shares 35
 - editing settings 34
 - quota rules 33
 - removing 35
 - viewing 34
- H**
- handling precautions 8
- hard disk
 - viewing information 56
- hard disk, viewing information 56
- hibernate, shutting down the device 18, 27
- I**
- ICES/NMB-003 compliance, Canada 96
- icons
 - action 102
- alert 24
- Help menu 25
- information 17
- navigation (end user) 98
- navigation bar, home page 17, 18
- on back of device 7
- image files, supported 63
- importing
 - configuration files 88
 - multiple users 31
- initiating an internal backup 48
- installing
 - iOs and Android mobile apps 41
 - mobile apps 42
 - My Cloud mobile app 42
- internal backups
 - about 47
 - creating 47
 - initiating 48
 - viewing 48
- Internet requirements 4
- IPv4 Network Mode 77
- IPv6 Network Mode 77
- iSCSI
 - about 56
 - roles 57
- iSCSI iSNS Client, enabling 58
- iSCSI target
 - creating 57
 - deleting 58
 - disabling 57
 - enabling 57
 - modifying 58
- ISO Shares
 - creating 90
 - deleting 91
 - modifying 91
 - viewing 91
- iTunes
 - accessing on My Cloud device 67
 - disabling 65
 - enabling 65
 - media types supported 64
 - overview 62
 - refreshing 65
 - streaming media 67
- J**
- Jumbo Frames 78
- L**
- LAN, requirements 3

- language and clock settings 70
- LED
 - Back Panel Ethernet (Network) 8
 - description 7
 - Front Panel Power 7
- link
 - aggregation 77
 - bonding 77
 - LAN cards 77
 - speed 77
- LLTD 82
- Local Area Network, LAN 3
- Local Master Browser 81
- logging off of your device 27
- M**
- Mac
 - backups 73
 - creating an alias for shared drive 14
 - OS X, access contents 14
- Machine noise compliance, Germany 97
- managing
 - alerts 24
 - apps 60
 - USB backups 43
 - users and groups 29
- manual updates 95
- manually adding an app 61
- mapping public folders 15
- Max SMB Protocol 81
- media
 - content, adding 66
 - settings, about 84
 - storage, about 64
 - streaming in iTunes 67
 - supported by iTunes 64
 - types supported 63
- media players
 - accessing in My Cloud device 66
 - accessing your personal cloud using 66
 - media
 - types supported 63
 - other 67
 - WD 67
- media servers
 - about 62
 - overview 62
- mobile apps
 - installing 42
- modifying
 - a virtualized volume 59
 - an iSCSI target 58
 - an ISO Share 91
 - backups 48
 - multiple users 30
 - creating 31
 - importing 31
- music
 - iTunes 62
 - playing 62
- My Cloud
 - accessing contents of shares locally 39
 - deleting a share 39
 - home page (end user) 98
 - managing users 29
 - remote access 40
 - system report 26
 - URLs 104
 - user settings 29
- My Cloud device
 - access 41
 - action icons 102
 - dashboard (end user) 98
 - device activity 21
 - device URLs and names 104
 - logging in (end user) 98
 - online setup 11
 - quick user guide 98
 - registration iii
 - storage capacity 20
- My Cloud Mobile App
 - installing 42
 - requirements 41
- N**
- navigation icons
 - admin 18
 - end user 98
- network
 - activity panel 21
 - profile settings 76
 - settings 75
 - UPS 80
- network services
 - IPv4 Network Mode 77
 - IPv6 Network Mode 77
 - settings 76
- NFS Service 79
- noise compliance
 - Germany 97
- notifications 91

- display 93
 - email 92
 - SMS 92
- O**
- obtaining customer support 25
 - online setup 11
 - operating system compatibility 3
- P**
- package contents, list 3
 - password
 - updating 32
 - updating user 32
 - photos, viewing 62
 - port forwarding 83
 - adding 83
 - deleting 83
 - power button, shutdown 27
 - precautions, handling 8
 - pre-installation instructions 8
 - preparing your device 9
 - private shares, creating 39
 - product components
 - 2-bay back view 5
 - 2-bay front view 4
 - 4-bay back view 6
 - 4-bay front view 6
 - Product Improvement Program 26
 - product registration iii
 - public folders, mapping 15
 - public share
 - opening with a Mac OS 14
 - opening with Windows OS 14
- Q**
- quotas
 - assigning to a group 35
 - assigning user 33
 - assigning users to user 32
- R**
- RAID mode
 - changing 54
 - viewing 54
 - RAID storage
 - about 53
 - changing 53
 - types 53
 - rebooting the device 27, 88
 - recording WD product information 2
 - recovering remote backups 47
 - refreshing iTunes 65
 - registration, product iii
 - regulatory compliance 96
 - remote backups 46, 47
 - remote cloud access 40
 - remote server
 - enable 83
 - removing
 - groups 35
 - users 33
 - requirements
 - FCC 96
 - Internet 4
 - local network 3
 - My Cloud Mobile App 41
 - operating system 3
 - web browsers 3
 - restore
 - device to default settings 87
 - system 87
 - RF emission compliance 96
 - RoHS environmental compliance, China 97
 - Running a Diagnostic Test 86
- S**
- S.M.A.R.T. data 56
 - safe mode
 - firmware update procedures 101
 - recovering from 101
 - safety
 - compliance, U.S. and Canada 96
 - instructions 1
 - saving, configuration file 88
 - scan disk
 - for errors 89
 - scanning 89
 - secure access, SSH 80
 - services settings 74
 - settings
 - firmware update 93
 - general 68
 - media 84
 - network 75
 - notifications 91
 - utilities 85
 - shared drive, creating a Mac alias 14
 - shares
 - about 37
 - accessing contents locally 39

- accessing locally 39
 - aggregation settings 82
 - assigning group access 35
 - creating new 38
 - deleting 39
 - editing 38
 - making them private 39
 - viewing a list of 37
 - viewing content 14
 - shutting down the device
 - Hibernate 27, 88
 - power button 27
 - single user, adding 30
 - SMS notifications 92
 - SNMP 79
 - SSH, secure access 80
 - streaming
 - media in iTunes 67
 - videos, photos, and music 62
 - system
 - activity 21
 - alerts, dismissing 25
 - alerts, icons 24
 - configuration 88
 - configuration, about 88
 - diagnostics, about 20, 86
 - health 20
 - logs, viewing 86
 - restoring 87
 - system report 26
 - creating and saving 26
 - sending to Technical Support 26
- T**
- tests, diagnostic 86
- U**
- updates
 - firmware 94
 - firmware, automatic 94
 - making on the Home Page 19
 - manual 95
 - updating
 - apps 61
 - user password 32
 - UPS
 - network connection 80
 - USB
 - backups, creating 44
 - backups, managing 43
 - copy button 45
 - Copy Button backups 45
 - front port backups 45
 - USB drive
 - connecting 43
 - drive details 43
 - user import file
 - creating 105
 - format 105
 - users
 - about 29
 - adding a single 30
 - adding multiple 30
 - assigning a group to 32
 - assigning quotas 33
 - assigning quotas to 32
 - creating multiple 31
 - enabling remote cloud access 40
 - group quota rules 33
 - importing multiple 31
 - panel 23
 - password, updating 32
 - quotas 32
 - removing 33
 - settings, editing 32
 - viewing 29
 - viewing list of 29
- V**
- video files, supported 63
 - videos
 - playing and streaming 62
 - streaming 62
 - viewing
 - a list of shares 37
 - alert details 25
 - apps 60
 - backup details 48
 - details of an ISO Share 91
 - device share content 14
 - device uptime 88
 - groups 34
 - hard disk drive information 56
 - hard disk information 56
 - System Logs 86
 - the current RAID mode 54
 - users 29
 - virtualized volume
 - about 58
 - connecting to a target 59
 - creating 59
 - modifying 59

W

Warning

- changing RAID mode 54
- deleting a share 39
- formatting disk erases data 89
- mounting a USB drive 44
- mounting/ejecting a USB drive 78
- renaming the My Cloud device 68
- SSH, modifying the device 80

WD

- product registration iii
- service and support ii
- technical support, contacting ii

WD Media Players, about 67

web

- access timeout 73
- compatible browsers 3
- file viewer 99

WebDAV Service 79

Windows

- accessing content 14
- mapping a public folder 15
- services 81
- workgroup feature 81

workgroups 81

Information furnished by WD is believed to be accurate and reliable; however, no responsibility is assumed by WD for its use nor for any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of WD. WD reserves the right to change specifications at any time without notice.

Western Digital, WD, the WD logo, My Book, My Cloud, My Passport, WD Red and WD TV are registered trademarks of Western Digital Corporation or its affiliates in the U.S. and other countries, and My Cloud, WD Quick View, WD SmartWare, WD Photos, and WD TV Live are trademarks of Western Digital Corporation or its affiliates in the U.S. and other countries. Other marks may be mentioned herein that belong to other companies.

© 2020 Western Digital Corporation or its affiliates.

Western Digital
5601 Geat Oaks Parkway
San Jose, California 95119 U.S.A.

4779-705142-A03 March 2020