

A red decorative graphic consisting of a vertical rectangle with a diagonal cut on the right side, creating a triangular shape.

px4-300r Network Storage Array

with LifeLine 4.1

User Guide

© 2014 LenovoEMC, Ltd. All rights reserved.

Lenovo and the Lenovo logo are registered trademarks of Lenovo in the United States, other countries, or both. The EMC logo is a registered trademark of EMC Corporation in the United States and/or other countries. LenovoEMC and LifeLine are registered trademarks or trademarks of LenovoEMC, Ltd. in the United States, other countries, or both. Windows is a trademark of the Microsoft group of companies. Mac is a trademark of Apple Inc., registered in the United States and other countries. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. Certain other product names, brand names, and company names may be trademarks or designations of their respective owners.

CONTENTS

Setting up Your px4-300r Network Storage Array	1
Setup Overview	2
About the px4-300r Device Components	3
Front Panel	3
Drive Bay Detail	4
Rear Panel	4
Default Settings	5
Connecting the px4-300r Network Storage Array to Your Network	6
Check Package Contents	6
Connecting the px4-300r	7
Safety Information	8
Accessing Your Device If It's Not Discovered	9
Direct Access Using the Device IP Address or Model Name	9
Discovery Using LenovoEMC Storage Manager	9
Discovering the px4-300r Using Your Computer OS	9
Setting Up Favorite Features	11
Setting Up Additional Features	12
Device Setup	13
 Device Configuration Options	 15
Network Settings	16
Manually Configuring Network Settings	17
Bonding NICs	18
VLAN Settings	19
Naming Your px4-300r Network Storage Array	20
Configuring Your px4-300r Network Storage Array to Use Active Directory	21
Enabling Active Directory Trusted Domains	22
Customizing Access to Features on Your px4-300r Network Storage Array	23
Enabling the Display of Features	23
Enabling Access Permissions to Features	23
Non-Administrator User Log In	24
Obtaining Alerts About Your px4-300r Network Storage Array	25
Tracing Events on Your px4-300r Network Storage Array	26
Downloading the complete event log file	26

Obtaining System Status for Your px4-300r Network Storage Array	27
Space Usage	27
Control Panel	27
Device Information	27
Using Your px4-300r Network Storage Array in Various Time Zones	29
Setting the Display Language for Your px4-300r Network Storage Array	30
Printing Documents	31
Securing Your px4-300r Network Storage Array and Contents	32
How Do I Secure My px4-300r Network Storage Array?	33
Security Settings	34
Users and Groups	35
Users and Groups Overview	36
Users	36
Groups	36
How Access Rights Are Granted Using Groups in Workgroup Mode	36
Adding Users	37
Managing Users	38
Changing User Information	38
Changing User Access Permissions	39
Setting Quotas	39
Deleting Users	39
Adding Groups	40
Managing Groups	41
Removing a User from the Group	41
Changing Group Access Permissions	41
Deleting Groups	42
Using Active Directory Domain	43
Active Directory Users and Groups Overview	44
Managing Active Directory Users and Groups	45
Importing Users and Groups from Active Directory	45
Synchronizing with the Active Directory Controller	45
Changing Access Permissions	46
Setting Quotas	46
Deleting an Active Directory User or Group	46

Managing Your px4-300r Network Storage Array with Local and Active Directory Users	47
Enabling Active Directory after Creating Users in Workgroup Mode	47
Logging in to Your px4-300r	47
Creating Local Users and Groups in Active Directory Mode	47
Creating Share Permissions for AD Users and Local Users	48
Switching to Workgroup Mode from Active Directory	48
Sharing Files	49
Sharing Overview	50
Interfaces for Sharing	50
Shares	51
What are Shares and How Do I Organize Content with Them?	51
Adding Shares	52
Managing Shares	53
Deleting Shares	55
Using Protocols to Share Files	56
What Are Protocols and How Do I Use Them to Share Files?	56
AFP File Sharing for Macs	56
Bluetooth File Sharing	56
FTP File Sharing	57
TFTP	57
NFS File Sharing	57
rsync: Synchronizing Files with Another Storage Device or Other Computers	58
Monitoring Your Device with an SNMP Management Tool	59
Managing File Sharing with Web Access (http/https)	60
WebDAV: Managing Files Using HTTP or HTTPS	60
Windows DFS: Creating a Distributed Windows File System	60
Windows File Sharing	61
Sharing Content through the Home Page	62
Sharing Your Content with the World	62
Adding a Custom Home Page	62
Automatically Sending Content to Multiple People at Once	64
How to Set Up an Email Distribution Active Folder	64
Sharing Content Using Social Media: Overview	65
Managing Your Content	66
Transferring Content to and from Your px4-300r Network Storage Array with Copy Jobs	67
Copy Jobs Limitations	67

Getting Content from a USB External Storage Device	68
Safely removing external storage	68
One-touch Transferring of Content from a USB Device	69
Setting QuikTransfer	69
Drive Management	70
Managing Drives	71
Write Caching	71
Global Drive Management Settings	71
Storage Pool Information	72
Drive Status	72
Adding New Drives to Your px4-300r Network Storage Array	73
Storage Pool Management	75
Understanding How Your Content Is Stored	76
Storage Pools	76
Volumes	76
Adding and Managing Storage Pools	77
Adding a Data Storage Pool	77
Improving Performance with a Cache Storage Pool	79
Creating a Cache Storage Pool	79
Assigning a Cache Pool to a Volume	80
Volumes	81
Snapshots	81
Exposing/Unexposing the Snapshot	82
Restoring a Snapshot	82
Deleting a Snapshot	82
Displaying Shares in the Snapshot	82
Make the Snapshot Read-only	82
Changing Expose Mode	82
Adding and Managing Volumes	83
Deleting a Storage Pool	85
Changing RAID Protection Types	86
iSCSI: Creating IP-Based Storage Area Networks (SAN)	87
iSCSI Overview	88
Adding iSCSI Drives	89

Enabling iSCSI Drives	89
Connecting to iSCSI Drives	89
Managing iSCSI Drives	90
Adding CHAP User Access to an iSCSI Drive	90
Deleting iSCSI Drives	91
Backing up and Restoring Your Content	92
Backup and Restore Overview	93
Backup of Data through RAID Protection	93
Backing up to and Restoring from Your px4-300r Network Storage Array	94
Backing up Macs with Time Machine	94
One-touch Transferring of Content from a USB Device	94
Copy Jobs Overview	95
Backing up Your px4-300r Network Storage Array	96
Copy Jobs	96
From: Settings	97
To: Settings	98
Setting a Schedule	98
Registering with Avamar for Backup and Restore	100
Backing up with Amazon S3	101
Restoring Files with Amazon S3	101
Backing up with LenovoEMC Personal Cloud	102
Restoring Files with Personal Cloud	102
Remote Access: Accessing Your px4-300r Network Storage Array From Anywhere in the World	103
Remote Access Overview	104
Enabling Remote Access	105
Basic Option: Completing the Enable Remote Access Process	105
Premium Option: Completing the Enable Remote Access Process	105
Accessing Your px4-300r Network Storage Array Remotely	107
Personal Cloud: Accessing Your LenovoEMC Personal Cloud From Anywhere in the World	108
What Is LenovoEMC Personal Cloud ?	109
LenovoEMC Personal Cloud Key Terms	109
Is My Content Secure?	110

Creating a LenovoEMC Personal Cloud	111
Configuring Router Port Forwarding for Personal Cloud	112
Router Port Forwarding	112
Configuring Your LenovoEMC Personal Cloud	113
Enabling Internet Access to the px4-300r	113
Changing Personal Cloud Settings	113
Inviting People onto Your LenovoEMC Personal Cloud	114
Joining a Trusted Device to LenovoEMC Personal Cloud	115
Managing Trusted Devices on a Personal Cloud	116
Disconnecting Trusted Devices	116
Deleting Trusted Devices	116
Using Copy Jobs with a LenovoEMC Personal Cloud	117
Disabling or Deleting Your LenovoEMC Personal Cloud	118
Accessing Content Using Your LenovoEMC Personal Cloud	119
Informing Users What to Do with LenovoEMC Personal Cloud	120
Sharing Content Using Social Media	121
Sharing Content Using Social Media: Overview	122
Facebook	123
Flickr	124
YouTube	125
Share Content through LenovoEMC Personal Cloud	126
Media Management	127
Media Management Overview	128
Scanning for Media Content	128
Media Services Capabilities and Limitations	129
Sharing Media Content over the Internet	130
Enabling Internet Access from the Media Server Page	130
Media Aggregation	131
Enabling Media Aggregation	131
Social Media Sharing	132
Streaming Music, Movies, and Pictures	133
Example: Setting up iTunes	133
Example: Setting up Xbox 360	133
Photos	134
Photos Overview	134

Streaming Pictures	134
Creating a Slideshow on the Device Home Page	134
Automatically Resizing Your Photos	134
Getting Pictures from Your Camera	135
Music	136
Music Overview	136
Streaming Music	136
Videos	137
Video Capabilities Overview	137
Streaming Movies	137
Adding Applications to Your px4-300r Network Storage Array	138
Application Overview	139
Application Installation	140
Application Manager	141
Starting or stopping an application	141
Adding applications	141
Removing applications	141
Software Updates	142
Auto-update process: installing a device software update	142
Manual update process: installing a device software update	142
Backing up and Recovering Your px4-300r Network Storage Array Settings	144
Backing Up Your px4-300r Network Storage Array Settings	145
Backing up Device Configuration	145
Restoring a Configuration Backup	145
Hardware Management	146
Energy Saving	147
Power Down Drives	147
Brightness	147
Wake On LAN	147
Creating a Power Schedule	147
Factory Reset	148
UPS Management	149
Troubleshooting Routers	150
Enabling the DMZ	150

Configuring Port Forwarding on Double NAT Networks	151
Bridging the Secondary Router	151
Bridging the Primary Router	151
Additional Support	153
How to Get Help	154
Support	155
Legal	156
Open Source	157
Warranty Information	158
Limited Warranty Notice	158
Limited Warranty for Iomega Products	158
Regulatory Information	159
Federal Communication Commission Interference Statement	159
Canadian Verification	159
European Union conformity	159
Important WEEE Information	160
European Union RoHS	160
India RoHS	160
California Perchlorate Information	160
Polyvinyl Chloride (PVC) Cable and Cord Notice	160
Recycling and environmental information	161
Export classification notice	161
Copyright and Trademark Information	162

CHAPTER 1

Setting up Your px4-300r Network Storage Array

Setup Overview

It's easy to set up your px4-300r Network Storage Array:

- Remove it from the box, connect it to your network switch or hub, and then power it up.
- Launch a web browser and either enter the Setup URL, <http://setup.lenovoemc.com>, or use the device IP address or model name to access the device directly.
- **Device Setup** launches automatically the first time you access your device and guides you through selecting the configuration options that best meet your needs.

Refer to the following sections for information on the device components and connection instructions.

[About the px4-300r Components](#)

[Connecting the px4-300r to Your Network](#)

[Safety Information](#)

[Accessing Your Device If It Is Not Discovered](#)

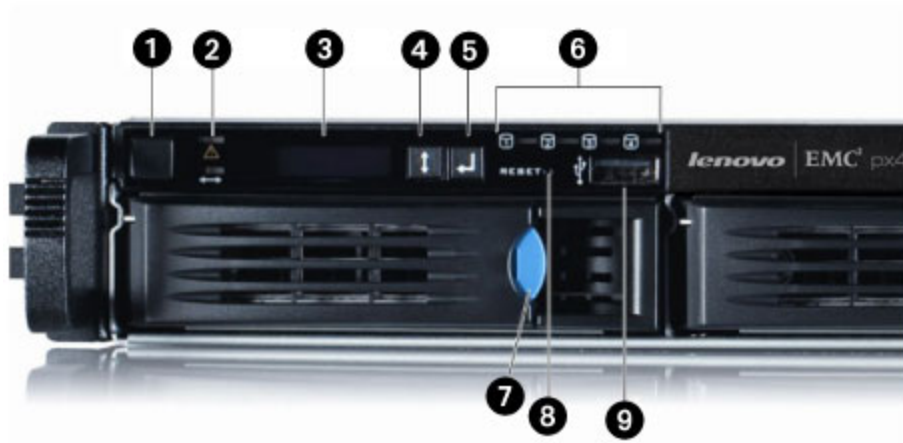


By default, the px4-300r will attempt to acquire an IP address from DHCP. If there is not a DHCP server available on the network, the px4-300r will use an IP address in the self-assigned APIPA range (169.254.x.x).

About the px4-300r Device Components

Front Panel

Status Indicators, Buttons and Ports



1. Power Button and Indicator – Press and release to power the px4-300r on or off. The power button is illuminated when the px4-300r is running.



Holding the power button for 4 seconds will result in a forced shutdown and could cause data loss if data transfers are in process.

2. System Status Indicator – Displays the current operational status of the px4-300r Network Storage Array.

The top LED light displays the current operational status of the px4-300r.

- Off – Powered up and ready.
- Flashing White – px4-300r is rebuilding the RAID array.
- Flashing Red – System or drive error – LCD or system software indicates error.
- Solid Red – System error during boot.

The bottom LED light displays the status of a QuikTransfer Copy Job.

- Off: No QuikTransfer Copy Jobs are running or defined.
- Solid Blue – Copy Jobs are configured – also applies to external USB drives that are plugged in and have a Copy Job configured.
- Flashing Blue – Data transfer in progress.
- Pattern Flashing Blue – Indicates an error with the data transfer – LED or system software indicates error.

3. LCD Display – Scroll through the display screen to view the device name, free disk space, IP address, and date and time. You can initiate a QuikTransfer Copy Job from the LCD and view or dismiss any errors or warnings on the px4-300r without having to turn on your computer.

4. Select or Cancel Button – Push the Select or Cancel button to select a menu option on the LCD display, or dismiss the current message.

5. Next Button – Push the Next button to scroll to the next px4-300r info screen.

6. Drive Activity Indicators – Displays the current status of drives in the px4-300r.

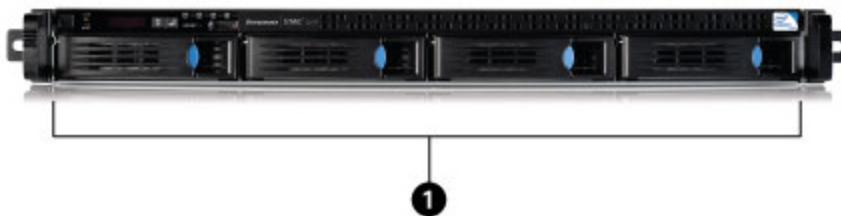
- Solid Blue – Powered up and ready.
- Flashing Blue: Data transfer in progress.
- Pattern Flashing Blue: Data transfer in progress.

7. Drive Sled Release Latch – Press the release button and pull the latch to release the drive sled.

8. Reset Button – Hold the RESET button for four seconds to reset security and network settings. This allows you to regain access if network settings are incorrect or you've forgotten your password.

9. USB Connector – Supports devices such as USB storage devices and printers.

Drive Bay Detail



Drive Bays – The px4-300r has four user-serviceable drive bays.

Rear Panel



1. Power Connector – Plug the power cable into this connector.

2. High-Speed USB 2.0 connectors – Supports devices such as USB storage devices and printers.

3. Gigabit Ethernet Ports – High-speed Ethernet connectors that automatically detect your network speed (10/100/1000Base-T).

4. Serial Connector – The serial connector is used for troubleshooting only.

Default Settings

- **IP Address** — If no DHCP server is found on your network the px4-300r will get a self-assigned IP address in the 169.254.x.x range.
- **Device Name** — The default name for your px4-300r Network Storage Array is px4-300r. If there is more than one px4-300r on your network, a number is added to the name, such as px4-300r-1 px4-300r-2, and so on.
- **Default Shares** — Device setup will create default Shares on your px4-300r. The specific default Shares will vary depending on the options you select during device setup. You can [create additional Shares](#) as desired.

Connecting the px4-300r Network Storage Array to Your Network

Check Package Contents

Verify that the box contains the following items:

1. px4-300r (models may vary)



2. Power Cables



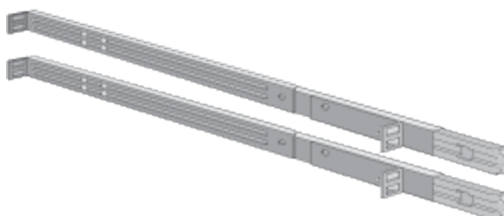
3. Quick Start Guide



4. Ethernet Cable



5. Rail Kit (models may vary)



Package contents may vary.

Connecting the px4-300r

If you have purchased more than one px4-300r, complete all steps on one device before setting up additional devices.

1. Make sure at least one hard drive is installed in the px4-300r. Refer to <http://support.lenovoemc.com> for a list of drives approved for use with the px4-300r.
2. Use the included network cable to connect the px4-300r to your network hub or switch.
3. Connect the included power cord to the back of the px4-300r and to an Uninterruptible Power Supply (UPS).
4. Power on the px4-300r.
5. Your px4-300r should power on automatically.
6. To set up your px4-300r, open a web browser and go to <http://setup.lenovoemc.com>, or enter the device IP address or the model name "px4-300r" in your computer's web browser. Device Setup will launch automatically the first time you access your px4-300r and guide you through configuring basic setup options.



On a Mac use "local.px4-300r" to access Device Setup using the model name. For best results, use a computer that is connected to the same subnet or network segment as the px4-300r. If Device Setup doesn't launch, see [Accessing Your Device If It's Not Discovered](#).

7. **OPTIONAL:** if desired, install the LenovoEMC Storage Manager and Twonky Media Server software.

LenovoEMC Storage Manager will automatically scan your network and connect to available Shares on the px4-300r.

Installing the Twonky Media Server software enables you to manage media aggregation on your client computer.

Mac Users: When you install LenovoEMC Storage Manager, its icon will appear on the Menu Bar. Shares on the px4-300r will mount and appear on the Mac Desktop.

NOTE: If the px4-300r Shares do not appear on the Mac Desktop, open **Finder Preferences** and check **Connected Servers** under "Show these items...". You can also find the Shares listed under **Shared** when you open a Finder window.

PC Users: When you install LenovoEMC Storage Manager, its icon will appear in the System Tray. Shares on the px4-300r will automatically be assigned a drive letter and will be available in the **Network** section in Windows Explorer or under **Computer Network Locations**.



If you receive a message from your operating system's firewall alerting you of network activity while installing the software, be sure to unblock communications.

If you do not install the LenovoEMC Storage Manager, see [Discovering the px4-300r Using Your Computer OS](#) for information on how to manually connect Shares on the device.

Safety Information

Observe the following guidelines when using your px4-300r Network Storage Array:

- Follow all instructions marked on the px4-300r and in the documentation.
- Use only the power supply cable provided with the px4-300r. Always use the appropriate power supply cable for your country.
- Unplug the px4-300r before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- Do not use the px4-300r near water. Do not spill liquid on or into the px4-300r.
- Do not place the px4-300r on an unstable surface.
- Do not place the px4-300r near or on a radiator or heat register.
- Openings in the px4-300r are provided for fans and air ventilation and should not be blocked or covered. Make sure the px4-300r has ample ventilation (at least 6 inches or 127 mm) in front and behind the unit.
- Do not walk on the power cord or allow anything to rest on it.
- There is a danger of explosion if the coin cell lithium battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the equipment manufacturer. Dispose of used batteries according to local, state, regional, and federal regulations.

Under any of the following conditions, unplug the px4-300r from the wall outlet and contact technical support:

- The power cord or plug is damaged.
- Liquid has been spilled into the device.
- The device does not function properly when the operating instructions are followed.
- The device was dropped or the exterior enclosure is damaged.

Accessing Your Device If It's Not Discovered

If your px4-300r is not discovered when you enter the Setup URL, you can use one of the following options to access it. Device Setup will launch automatically the first time you access your device.

Direct Access Using the Device IP Address or Model Name

You can access the device management interface directly using your computer's web browser by entering either the device IP address or the model name in the URL bar.

- The default name for your px4-300r Network Storage Array is px4-300r. If there is more than one px4-300r on your network, a number is added to the name, such as px4-300r-1 px4-300r-2, and so on.

If you have updated your px4-300r from an earlier version of LifeLine, the device name might include an additional alphanumeric identifier following the model name. This will not change when you install LifeLine 4.1.

Discovery Using LenovoEMC Storage Manager

You can install LenovoEMC Storage Manager from the [LenovoEMC web support site](#). Select your px4-300r from the LenovoEMC products on the support home page, and then look for LenovoEMC Storage Manager under **Downloads and Updates**.

Installing LenovoEMC Storage Manager on your client computer helps you discover the px4-300r on your network. It also makes it allows multiple computers on your network to interact with the px4-300r.

Discovering the px4-300r Using Your Computer OS

You can access the management interface for your px4-300r using your client computer's operating system as described by these methods for Windows PCs or Macs.

Windows 8:

1. Click **File Explorer** on the task bar.
2. You should see your px4-300r listed under **Other Devices**.
3. Right-click on the icon for your px4-300r and select **View device webpage** to launch the web-based device management interface.
4. You can also select **Properties** from the right-click menu to see the device webpage URL. Click the URL to launch the device management interface.



The webpage URL shows the IP address assigned to your px4-300r.

Windows 7 and Vista:

1. Click **Start > Computer > Network**.
2. You should see your px4-300r listed under **Other Devices**.
3. Double-click the device icon to access the px4-300r device management console.

Windows XP:

1. If you have not enabled UPnP Discovery, click **Start > Help and Support**.
2. In the Help and Support browser, search for **UPnP** and follow the steps from “Install the UPnP framework”.
3. After UPnP is enabled, open Windows Explorer and in the **Folders** view, expand **My Network Places**.
4. You should see your px4-300r listed.
5. Double-click the device icon to access the px4-300r device management console.

Mac:

1. Open a new Finder window.
2. Select **All...** under **Shared** on the left side of the Finder window,
3. Double-click your px4-300r to login to the device management console.



After you complete setup for your px4-300r, you can connect to device Shares by selecting **Go > Connect to Server** and entering either **afp://<device IP address>** or **smb://<device IP address>**.

Setting Up Favorite Features

After you complete device setup, the px4-300r management console will open and display default **Favorite Features** based on options you selected during setup.

Select **All Features** to see additional features available on your px4-300r. If you want to add any of these to your Favorites, just click and drag the icon from the All Features screen to the **Favorite Features** tab.

You can access the user interface, setup options, and help information for any feature by clicking its icon under either Favorite Features or All Features. You can find information in this user guide on any available feature by searching for the feature name using the PDF Find feature:

1. If your PDF Reader doesn't display a Find box by default, press Ctrl-F under Windows or Apple-F on a Mac.
2. Enter a feature name, keyword, or text string for the information you want to find.
3. Select Next or use the drop-down menu for advanced search options.

Setting Up Additional Features

After completing device setup, you may want to configure additional features of your px4-300r. Refer to the sections under **Device Configuration Options** for information on configuring many basic features. More complex features are covered by other sections of this manual.

LenovoEMC Personal Cloud

You can set up a Personal Cloud to allow invited users access to content on your px4-300r. This content can be in private Shares that are exclusive to the users who join the Personal Cloud, which adds an additional layer of security. In addition, you may want to join other trusted devices to the Personal Cloud, so that content on those devices can be made available to Personal Cloud users. For more information about Personal Cloud, refer to the [Personal Cloud overview](#).

File Sharing

Setting up File Sharing enables you to add content to your px4-300r and make it available in a wide variety of ways, including content features such as Active Folders and media sharing. For more information, refer to the [Sharing Overview](#).



Security is automatically enabled when you setup your px4-300r and all Shares are secured by default. You can create users on your device and set access privileges as desired to limit data access to Shares. You can also make Shares public if you want them to be accessible by everyone. See [Securing Your Device](#) for more information.

Device Setup

Device Setup runs automatically when you first access the px4-300r and steps you through configuring basic device options. If you want to change these configuration settings later on, you can run setup again by selecting the **Device Setup** icon under **All Features** in the px4-300r device management console.

You can also manually configure options for any feature on your px4-300r by selecting that feature's icon. Other sections in this manual provide information on settings options for the features available on your px4-300r.



If you run Device Setup after completing initial setup, it will not affect any content stored on your px4-300r or change other configuration options you have set.

Some processes on your px4-300r also use the setup steps to confirm administrator authorization and configure basic storage options, such as file system and RAID protection. This will not affect other settings or data on your px4-300r.

CHAPTER 2

Device Configuration Options

Network Settings

The **Network** feature enables you to view and change the network configuration settings on your px4-300r. You can use Network to identify your DNS servers and WINS servers and how your system's IP address is determined. Most system IP addresses and other network settings can normally be configured automatically.

If you want to change the default network settings for your px4-300r, refer to [Manually Configuring Network Settings](#).

You can also use the Network feature to configure the following features on your px4-300r.

Bonded NICs

If your px4-300r has multiple network interface cards (NICs), you can bond those NICs. Refer to [Bonding NICs](#).

VLAN

Each NIC in your px4-300r can be added to up to four Virtual LANs (VLAN). For information on adding a NIC to a VLAN, refer to [VLAN Settings](#).


Enabling Jumbo Frame Support

You can enable jumbo frames for each NIC in your px4-300r by expanding the **Information** section for a NIC and entering a jumbo frame size in the **Jumbo Frame** field. If you do not want jumbo frame support, leave the field blank. Jumbo frame support is useful for transferring large files, such as multimedia files, over a network. Jumbo frame support increases transfer speed by placing large files in fewer data packets. It also reduces the demand on the device hardware by having the CPU process more data in fewer data packets.

Jumbo frame support should only be enabled if you are sure your network is jumbo-frame compatible and all network devices have been configured to support jumbo frames. It is recommended that you confirm all network interface cards (NICs) are configured to support jumbo frames before enabling this feature.

Manually Configuring Network Settings

Changing Network Configuration Settings

1. Click the **Network** icon to open the Network feature.
2. Click  **Modify network settings** to manually configure settings that apply to all network interfaces.
3. To manually set static IP addresses, remove the check mark for **Automatically configure DNS, WINS, and all IP addresses (DHCP)**.
DNS Servers – enter the IP addresses of the DNS (Domain Name System) servers. DNS is used for translating the domain name to IP addresses.
WINS Servers – enter the IP addresses of the WINS server.
4. **Bonding Mode** applies if you want to bond two or more network interfaces on your px4-300r. The default setting is Adaptive Load Balance. Refer to [Bonding NICs](#) for additional information on bonding modes.
5. To connect your px4-300r to a proxy server, check **Use proxy settings** and enter proxy IP address, port number, and the proxy username and password.
6. Click **Apply** to save your settings.
7. To set a static IP address, expand the Network Interface section and remove the check mark for **Automatically acquire network addresses (DHCP)**.



If this box is checked and a DHCP server is not available on the network, the device will auto-assign an IP address in the 169.254.x.x range.

8. Complete the following settings to assign a static IP address for the selected network interface:
 - **IP Address** – the static IP address for the px4-300r. Use an available IP address in the range used by the LAN.
 - **Subnet Mask** – the subnet that the IP address belongs to. The default value is 255.255.255.0.
 - **Gateway** – enter the gateway IP address in this field.
9. Click **Apply** to save your settings.

Additional Network Configuration Options

For information on adding a NIC to a VLAN (Virtual LAN), refer to [VLAN Settings](#).


For information on bonding multiple network interface cards (NICs), refer to [Bonding NICs](#).

Bonding NICs

Bonding network interface cards (NICs) is a way to provide redundancy for your px4-300r on the network. If one NIC should fail, your px4-300r will remain accessible on the network if that NIC is bonded to others. Depending on the bonding mode selected, it can also increase bandwidth.

You can bond the built-in NICs in your px4-300r.

Use the following procedure to bond NICs:

1. Open the Network feature and click  **Modify network settings**.
2. Use the drop-down menu to select the Bonding Mode you want to use:
 - **Adaptive Load Balance:**
This mode increases bandwidth by distributing the load across the bonded NICs. Adaptive Load Balance does not require any switch or router support because the bonding is done by the px4-300r, and LifeLine's bonding driver takes care of network traffic to support the bonding. Adaptive Load Balance is the default bonding mode.
 - **Link Aggregation:**
This mode increases bandwidth by distributing the load across multiple ports in a switch. Link Aggregation requires an 802.3ad compatible network switch.
 - **Failover:**
Failover mode protects network connectivity for your px4-300r in case a NIC fails. In Failover mode, only one NIC in the bond is active; other NICs in the bond are passive. If the active NIC fails, another NIC in the bond becomes active and maintains network connectivity. Failover mode does not require any switch support, and it does not provide any bandwidth increase.
3. Click **Apply** to save your setting.
4. In the Network Interface table, expand the number for one of the NICs you want to bond, and then expand the **Bond Network Interface** section.
5. Check the box under **Bond** next to each NIC you want to bond to the selected NIC. For example, if you expanded NIC 1, and your configuration includes four NICs, you could bond NIC 1 to NIC 2, 3, and/or 4.
6. Click **Apply** to save your settings.

The section updates and displays the NICs that are bonded to the selected NIC.

Unbonding NICs


1. To unbond a NIC, uncheck the box next to the bonded NIC.
2. Click **Apply** to save your settings.

VLAN Settings

A VLAN (Virtual Local Area Network) is a network of devices that are joined into one broadcast domain, even if the devices are not physically connected to each other. VLANs are useful for creating smaller networks within a larger LAN; for example, a legal department in a company might be on its own VLAN because it has sensitive documents that only certain personnel should have access to. The smaller networks that VLANs create do not require any additional physical resources, such as additional cabling. Your px4-300r Network Storage Array can be configured to support VLANs by connecting the corresponding physical NIC to the trunk port of an L2/L3 switch.

VLAN is configured for each NIC, but it is not supported on bonded NICs. If a NIC is bonded, you must unbind it first to configure it for a VLAN.

Adding a VLAN

1. To add a VLAN, expand the **VLAN Settings** section of a NIC.
2. Click  **Add VLAN**.
3. Enter a VLAN ID value between 2 and 4094. You can enter up to 4 VLAN IDs for each NIC. A VLAN can obtain its network settings from DHCP, or you can uncheck DHCP and enter the IP address, subnet mask, and gateway manually.
4. Refer to [Network Settings](#) on page 16 for information about jumbo frames.
5. Click **Apply** to save your changes.

Deleting a VLAN

In the **VLAN Settings** section click **Delete** to delete the VLAN.

Naming Your px4-300r Network Storage Array

You can provide a meaningful name for your px4-300r using the Device Identification feature. This feature enables you to change the Storage Device Name, the Storage Device Descriptive Name, and the Workgroup Name.

Change any of these by editing the text fields. Click **Apply** to save your changes.

- **Device Name:** Enter a name for the px4-300r device. Use a name that will help you identify it on your network.
- **Device Descriptive Name:** Enter a descriptive name for the px4-300r device. This name can provide additional detail that identifies the device. If you leave this field blank, the default device name is used.
- **Workgroup Name:** Enter a workgroup name for the px4-300r device if you need to change the default name. The workgroup name identifies a group of computers that share information with each other. Change the workgroup name only if you explicitly define a workgroup on your network. Most users won't need to change the workgroup name, unless they have explicitly defined a different workgroup on their other computers.



Renaming the px4-300r will require a device restart.

Configuring Your px4-300r Network Storage Array to Use Active Directory

If you have an existing Active Directory user organization, you can incorporate it into the px4-300r device management interface. Your px4-300r can work in a high availability environment, which means it can work with multiple AD servers should one server fail or go offline.

Follow the instructions below to configure your px4-300r to use Active Directory.

1. Manually set the DNS server for the px4-300r:
Open the **Network** feature. Uncheck **Automatically configure all network settings**, type the IP address of your DNS Server in the text box, and click **Apply** to save your settings.
2. Configure the px4-300r to join the Active Directory domain:
Open the **Domain Management** feature and click **ON** to enable Active Directory.
3. Provide the following connectivity information for the existing AD user organization that you want to incorporate into the px4-300r:
 - **Domain Name** – the fully qualified domain name of your Active Directory domain, for example, sohead.com.
 - **Preferred Server** – optionally enter the actual name or IP address of your Active Directory Server, for example, ad-server.sohoad.com or 10.14.50.12. If this field is left blank, the px4-300r will use the DNS setting (step 1) to resolve the AD Server (also called "Domain Controller").
 - **Organizational Unit** – an optional predefined subset of directory objects within an Active Directory domain, where the computer object for the px4-300r will be created in the domain.
 - **Administrator Username** – the Active Directory username with domain administrator privilege, or enough privilege to join client computers to the domain.
 - **Administrator Password** – the Active Directory password for the specified Active Directory username.
 - **Users/Groups Refresh Interval** – how often the px4-300r should refresh the list of available users and groups from the Active Directory server.
 - **Local Network Encryption (SSL)** – enforces encryption on your local network.
 - **Remote Network Encryption (SSL)** – enforces encryption outside your local network, such as through the internet. Choices for both encryption types are Not required and Always (encryption is always enforced). Always encrypting communication is safest, but can impact performance.
 - **Enable trusted domains** – enables your px4-300r to allow access to other domains.
4. Click **Apply** to save your settings.

Enabling Active Directory Trusted Domains

By enabling Active Directory trusted domains on your px4-300r, you enable the importing of users and groups from other trusted domains to your px4-300r device. Those users and groups from other domains will then have access to features on your px4-300r, including accessing folders and documents in Shares.

Now that you have enabled access to all trusted domains, you can add users and groups from those trusted domains to your px4-300r. For more information, refer to [Managing Users and Groups with Active Directory](#).

Customizing Access to Features on Your px4-300r Network Storage Array

Feature Selection (FS) enables an administrator user to customize the device management console for non-admin users. Using FS, an admin can enable the display of certain features and disable others. In addition, an admin can provide non-administrator users access to certain features by setting permissions for those users.



Access permission to a feature can be given only to non-administrator users, since admin users always have access to all features.

Enabling the Display of Features


1. Click the **Feature Selection** icon to open the interface page.
All the features of your px4-300r display on the page with a status that indicates whether the feature is enabled or disabled.
2. To enable a feature, expand the desired feature name, and click the switch to **On**. For example, to enable Amazon S3, expand the Amazon S3 feature, and click the switch to **On**.
3. To disable a feature, click the switch to **Off**.



You can set the display of applications on the Feature Selection page, provided an application has that capability. For more information on installing features, refer to the [Application Manager](#).

Enabling Access Permissions to Features

You can configure access permissions for non-administrator users with certain features. Expand the feature on the Feature Selection page to determine if it supports feature access permissions.

1. If you have not already done so, create users and groups on your px4-300r.
2. Open the Feature Selection page.
3. To enable access to an enabled feature, expand the desired feature name, and click  **Add access permissions**.
4. In the pop-up window, select one or more users to provide them access. If you have created groups, you can also limit access for them in this way.
5. Click **Apply** to save your changes.
The list of users with access is displayed under the feature. To remove user access, uncheck the access box next to the user, and click **Apply** to save your changes.



You can enable access permissions for applications on the Feature Selection page, provided an application has that capability. For more information on installing features, refer to the [Application Manager](#).

Non-Administrator User Log In

Non-administrator users can log in to a px4-300r with feature access enabled. When these non-admin users access the device, they first see the Login screen where they enter their login credentials. After logging in, the device management console displays with those features to which the non-admin user has access.

Obtaining Alerts About Your px4-300r Network Storage Array

You can configure your px4-300r to send email alerts when problems are detected. This is done through the **Email notification** feature, which enables you to set up a destination for emails sent by the px4-300r when problems are detected.

Click the **Email** icon to open the Email notification feature. To provide a destination email address, enter the following information:

- **Destination Email Addresses** – enter a valid email address or addresses. This email address provides a destination for messages sent by the px4-300r when problems are detected by the system. You can add multiple email addresses by separating them with commas, spaces or semicolons.
- Check **Send a test email message** to confirm that email notification is working properly.
- Check **Configure custom SMTP settings** only if your network blocks SMTP traffic, requiring additional credentials, such as a corporate firewall.

Most users will not need to check this option. If checked, enter the following additional information to identify your SMTP server:

- **Email Server (SMTP)** – enter the address of your SMTP server.
- **Sender Email Address** – enter an email address for the px4-300r to use as the From address when it creates messages.
- **Email Login** – enter the username used to log into the email account you entered above.
- **Email Password** – enter the password for the email account.
- **Confirm Password** – confirm the password for the email account. It must match the password provided above.



If your email application uses a SPAM blocker, it is recommended that you add a sender email address to your safe list. If you do not define additional credentials, the default sender email is: `alertnotification@lenovoemc.com`

Click **Apply** to save your changes.

Tracing Events on Your px4-300r Network Storage Array

The **Event Logs** feature displays only the 1000 most recent events logged to the px4-300r. A complete event log, however, is available for download.

The following icons indicate the severity of each status message:

- **INFORMATION**
Identifies that a change has been made to the state of your px4-300r device, usually by a user, such as attaching a peripheral.
- **WARNING**
Identifies that there is a problem with your px4-300r device that requires your attention, but your device will continue to operate normally for now.
- **ERROR**
Identifies an urgent problem with your px4-300r device that may result in data loss and requires your immediate attention.

You can sort the displayed list by Date, User, or Event by clicking the column headers.

Downloading the complete event log file

Click **Download** to download a comma-separated event log file. A new page is opened with a link to the event log file. Click the event log file link to download or open the file.

The downloaded file contains 5 columns: Number, Date, User, Severity, Message.

Obtaining System Status for Your px4-300r Network Storage Array

The device management console displays overall system health and space usage information. The System Status feature provides additional status details and a control panel that enables you to:

- Blink the lights
- Restart
- Shut down

Click the **System Status** icon to open the feature page.

Space Usage

The Space Usage section graphically represents the amount of space used by Shares on the px4-300r. The exact space used displays in a ToolTip when you mouse over each Share.

Control Panel

The Control Panel displays commands for the px4-300r:

- **Blink the lights**
To help identify a specific px4-300r when there is more than one device configured on your network, blink the lights on the front of the px4-300r by clicking:
- **Restart**
Restart the px4-300r.
- **Shut down**
Shut down the px4-300r.



Before shutting down the px4-300r, be sure you have access to the physical device to turn it on. It is recommended that you always use the power button to shut down the device.

Device Information

The Device Information section displays various hardware, software, and status details.

Status

The Status Information section displays changes to or issues with your px4-300r. If an issue requires user action to resolve, such as a warning or error message, the px4-300r management console displays a link in the status message.

The following types of messages can display:

INFORMATION	Identifies that a change has been made to the state of your px4-300r, usually by a user, such as attaching a peripheral.
WARNING	Identifies that there is a problem with your px4-300r that requires your attention, but your device will continue to operate normally for now.
ERROR	Identifies an urgent problem with your px4-300r that may result in data loss and requires your immediate attention.

Using Your px4-300r Network Storage Array in Various Time Zones

You can set the date and time used on your px4-300r, so that it can appear to be in one time zone, when it actually may be in a different one. This can help your users have the correct date and time if they live and work in a location different from your px4-300r. You can set the date, time, and time zone through the **Date & Time** feature.



When an Active Directory Domain is in use, the px4-300r synchronizes time with the domain controller.

1. To change time zones, select a Time Zone from the drop-down menu, and then select how time will be set for the px4-300r:
 - **Internet Time Server** — By default, Automatically synchronize with an internet time server and Use the default time server are selected. To specify a time server, select Specify the time server and type the URL of the internet time server you wish to use in the text box that displays.
 - **Manual** — Select Manually set date and time. To set the current date and time, click the appropriate icon for calendar and clock settings.
2. Click **Apply** to save your changes.

Setting the Display Language for Your px4-300r Network Storage Array

You can set the display language for your px4-300r through the **Languages** feature.

The Languages page allows you to change the language used in email notification messages.

The language used by the px4-300r management interface is based on the preferences configured in your browser. You can change the language used in this program by modifying your browser's preferred language settings.

Click **Apply** to save your changes.

Printing Documents

Printing documents from your px4-300r is simple after you have attached a compatible printer. The **Printers** feature displays a table of printers that are attached to the px4-300r. For each attached printer, the table shows the name, model, status, and number of documents waiting.

To attach a printer, simply plug a supported printer's USB cable to a USB port on the px4-300r. Once attached, the printer will appear in the table. When the cable is unplugged, the printer will be removed from the table.



The Print feature is a one-way print spooler only and does not support two-way communication with the printer. For best results, use a printer without multi-function features (for example, scanner, copier, fax, modem), as these normally require bi-directional communication.

CHAPTER 3

Securing Your px4-300r Network Storage Array and Contents

How Do I Secure My px4-300r Network Storage Array?

Your px4-300r is automatically secured during [Device Setup](#). This creates an administrator user login, secures all Shares to protect content stored on your device from unauthorized access, and encrypts communications when using the web-based device management interface.

The administrator has full access to the device management interface and can create additional admin users as desired. All admin users on the device can modify security settings, create non-admin users and groups, join the device to an Active Directory domain, assign user access privileges to device Shares, and customize feature access for non-admin users.

You control access to content stored on your px4-300r by adding users and groups and assigning access permissions to device Shares. If you want to allow public access to a Share on your px4-300r, you must explicitly provide permissions for Everyone to that Share. See [Adding Users](#) and [Changing Access Permissions](#) for more information.



Updating from an earlier version of LifeLine where an administrator login was not required will run the device setup sequence to force creation of an administrator user. Updating a device with security enabled will not change existing security settings other than to remove the option to disable security.

Security Settings

Only administrator users can view or change settings on the px4-300r. To change any security settings, you must login to the device management interface as an admin user.

1. Click the **Security** icon to open the Security settings page.
2. Set the encryption options you want to use.

Local Encryption enforces encryption on your local network.

Remote Encryption enforces encryption outside your local network, such as through the internet,

Choices for both encryption types are **Not required** and **Always** (encryption is always enforced). Always encrypting communication is safest, but can impact performance.

Encryption is always available when you access your px4-300r using https.

3. If you have your own security certificate, you can load it by selecting **Use an imported certificate** and browsing to the certificate to load it.



Browser communications with the px4-300r are encrypted as part of the built-in security on the device. If you do not have your own security certificate, each computer that attempts to access the px4-300r may encounter a security warning, which can be safely ignored. In addition, you may be asked to accept a signed certificate for the px4-300r, which you should accept. If you change the device name at a later date, these warnings may appear again.

4. Click **Apply** to save your changes.
5. [Click here](#) to learn how to create users on the device.
6. [Click here](#) to learn how to change access permissions for device Shares.

CHAPTER 4

Users and Groups

Users and Groups Overview

The **Users & Groups** feature displays all users and groups on the px4-300r and enables administrators to add and modify users and groups.

Users

Non-administrator users can be added to enable controlled access to Share content. Additional administrator users can be added to allow specific users to configure the px4-300r.

The table on the Users & Groups interface page displays the Username and Descriptive Name for each user and group. Click in a row of the table to view or modify details about a user or group.

Groups

Groups consist of one or more users, and administrators can grant each group rights to Shares on the px4-300r. Users can belong to more than one group. The Groups feature enables administrators to create one or more groups and set access privileges for them.

By default, there are no groups defined. Once an administrator defines one or more groups, the Groups functionality is dynamically available when creating, modifying, and viewing users, Shares, and groups.

How Access Rights Are Granted Using Groups in Workgroup Mode


When groups are defined in Workgroup mode, a user's access rights are the most rights granted to the user and all groups to which the user belongs.

For example, assume 3 Shares exist (SF1, SF2, and SF3), two users (UserA and UserB), and three groups (Group1, Group2, Group3). When created, UserA was not granted access rights to any Share, and UserB was granted Read rights to SF3. Group1 has Read/Write rights to SF1, Group2 has Read/Write rights to SF2, and Group3 has Read/Write rights to SF3. If UserA is added to Group1, UserB is added to Group2, and Group1 is added to Group3, the table below shows the resulting access rights for each user and group defined:

Name	Member of Group	Access Rights
UserA	Group1, Group3	SF1 - Read/Write SF3 - Read/Write
UserB	Group2	SF2 - Read/Write SF3 - Read
Group1	Group3	SF1 - Read/Write SF3 - Read/Write
Group2	none	SF2 - Read/Write
Group3	none	SF3 - Read/Write

Adding Users

To add a user on your px4-300r:

1. Click the **Users & Groups** icon to open the feature page.
2. Click  **Add a user**.
3. Enter the following information:
 - **Username** – enter the username of the user to be created. This is the username for logging into the px4-300r. There is a maximum of 32 characters, and spaces are not allowed. The following are not valid usernames: root, daemon, bin, sys, sync, mail, proxy, www-data, backup, operator, sshd, postfix, nobody, unuser, guest, and rsync.
 - **Descriptive Name** – add a descriptive name to identify the user. For example, if you created a user with a Username of jsmith, you may want to add the Descriptive Name Joe Smith.
 - **Password** – create a password for the user. The password should be at least 8 to 12 characters, and spaces are not allowed. The maximum password length is 32 characters.
 - **Confirm Password** – confirm the password. If the text in this field does not match the text in the Password field, an error will be returned.
 - **Quota Size** – set a quota size by entering a value in gigabytes. This limits the amount of storage space this user can have. To have no quota, leave this field blank. You see this option only if you have [enabled quotas](#).
 - **Administrator** – check this box to allow this user to manage the px4-300r.
 - **Add a secured Share for this user** – check this box to create a secured Share for this user. This Share will have the new user's name, and allows access only to that user.
 - **Send a Personal Cloud invitation** – click this link to invite a user to join your Personal Cloud on the px4-300r. This opens the Send a Personal Cloud Invitation dialog box where you create an invitation by entering a user's email address along with any additional comments. A user then receives the invitation, which contains the Personal Cloud name and username and password. A user enters that information from LenovoEMC Storage Manager. For more information on this, refer to the online help with LenovoEMC Storage Manager. You see this option only if a [Personal Cloud has been created](#) on the px4-300r.
 - **Allow this user to add trusted devices to my Personal Cloud** – check this box to allow a user to [join a trusted device](#) to a Personal Cloud. A trusted device is a machine, either a computer or another px4-300r, that belongs to an added user. Only trusted devices that belong to users that have been added to the px4-300r can join the LenovoEMC Personal Cloud. This option displays only if a [Personal Cloud has been created](#) on the px4-300r.
4. Click **Create**.
5. Expand **Access Permissions** for the new user and set the desired access to Shares on the px4-300r. See [Changing Access Permissions](#) for detailed instructions.

Managing Users

The section describes how to:

- [Change User Information](#)
- [Change User Access Permissions](#)
- [Set Quotas](#)
- [Delete a User](#)

Changing User Information

You can change user information for existing users on the px4-300r, but you cannot change the username. If you want to change a username, delete the existing user and create a new user with the new username.

1. Expand the user list and click a user to modify the following information:
 - **Descriptive Name** – add a descriptive name to identify the user. For example, if you created a user with a Username of jsmith, you may want to add the Descriptive Name Joe Smith.
 - **Password** – create a password for the user. The password should be between 8 and 12 characters, and spaces are not allowed.
 - **Confirm Password** – confirm the password. If the text in this field does not match the text in the Password field, an error will be returned.
 - **Send a Personal Cloud invitation** – click this link to invite a user to join your Personal Cloud on the px4-300r. This opens the Send a Personal Cloud Invitation dialog box where you create an invitation by entering a user's email address along with any additional comments. A user then receives the invitation, which contains the Personal Cloud name and username and password. A user enters that information from LenovoEMC Storage Manager. For more information on this, refer to the online help with LenovoEMC Storage Manager. You see this option only if a [Personal Cloud has been created](#) on the px4-300r.
 - **Allow this user to add trusted devices to my Personal Cloud** – check this box to allow a user to [join a trusted device](#) to a Personal Cloud. A trusted device is a machine, either a computer or another px4-300r, that belongs to an added user. Only trusted devices that belong to users that have been added to the px4-300r can join the LenovoEMC Personal Cloud. You see this option only if a [Personal Cloud has been created](#) on the px4-300r.
 - **Quota Size** – set a quota size by entering a value in gigabytes. To have no quota, leave this field blank. You see this option only if you have enabled quotas.
 - **Administrator** – check this box if you would like to allow this user to manage the px4-300r.
2. Click **Apply**.

Changing User Access Permissions

1. Expand **Access Permissions** to change Share access permissions for the selected user.
2. To give this user access to a specific set of Shares, click **Add access permissions**.
3. In the Add Access Permissions pop-up window, select which Shares this user can access, and click **Apply**.
4. Uncheck **Read** or **Read/Write** to limit access permission to each Share for this user.
5. Click **Apply** to save your changes. If both Read and Read/Write are unchecked, the Share is removed from the list.




Access to default Shares must be granted explicitly to all added users, including administrator users. Only the administrator created during device setup has default access to the initial Shares. When new Shares are added, all existing administrator users will have default access to those Shares.

Setting Quotas

You can limit the amount of space allocated to one or more users by applying quotas.



If your px4-300r has multiple Storage Pools and you define a quota for users, that quota is applied to all Storage Pools.



1. Click  **Quota Settings** to enable quotas, and set a default quota for each user.
2. In the **Quota Settings** pop-up window, check **Enable quotas** to turn on quotas for each user.
3. If desired, enter a **Default Quota**. This quota applies to new users only.
4. Check **Set default quota for all users** to apply the default quota to all users.
5. Click **Apply** to save your changes.
6. To set individual user quotas, expand the **Information** section for a user and enter a value in **Quota size**. If you leave the box blank, there is no quota for that user.
7. Click **Apply** to save your changes.

Deleting Users

To delete an existing user:

1. Click the **Users & Groups** icon.
2. Click the username to expand the user.
3. In the User Information section, click **Delete**.
4. In the **Delete User** pop-up window, click **Yes**.
5. The user is removed from the user list.

Adding Groups


1. Click the **Users & Groups** icon to add or manage groups on the px4-300r.
2. Click  **Add a group**. The Information section opens.
3. From the Information section, give the new group a name.
4. To add users to the group, click  **Add users**. Select a user or users to include in the group. Select the checkbox in the title bar to add all listed users.
5. Click **Apply** to save your changes.

Managing Groups



This section describes how to:

- [Remove a User from a Group](#)
- [Change Group Access Permissions](#)
- [Delete a Group](#)

Removing a User from the Group

1. Open a group to display the users belonging to it.
2. To remove a user from the group, click the  next to that user. When the **Remove user** pop-up window appears, click **Yes** to remove the user.

Changing Group Access Permissions

1. To refresh the list of users, click  above the table.
2. Expand **Access Permissions** to change group permissions to a secured Share. If iSCSI is enabled, you can also change group permissions to secured iSCSI drives.
3. To add permissions to a Share, click  **Add access permissions**.
4. From the **Add Access Permissions** pop-up window, select a Share or Shares for the group to access. If iSCSI is enabled, select iSCSI drives for the group to access. Select the checkbox in the title bar to select all the Shares listed. If iSCSI is enabled, select the checkbox in the title bar to also select all the iSCSI drives listed.
5. Click **Apply** to save your changes.
6. In the table listing the Shares, check **Read** or **Write** for each Share. If iSCSI is enabled, check **Read** or **Write** for each iSCSI drive. The group can have full access by checking both **Read** and **Write**. To grant only read access, check only **Read**.
NOTE: A group must have read access at a minimum. A group cannot have only write access.
7. Uncheck **Read** to remove all access to a Share and remove the Share from the table. If iSCSI is enabled, uncheck **Read** to remove all access to an iSCSI drive and remove the iSCSI drive from the table.
8. Click **Apply** to save your changes.
9. If NFS is enabled, the **GID** field is visible. The GID value must be the same on both the Linux client and the px4-300r Network Storage Array for the client to access files. To modify the GID, type a new GID value.

Deleting Groups

To delete an existing group:

1. Click the **Users & Groups** icon.
2. Click the group name to expand the group.
3. In the Information section, click **Delete** to delete the group.
4. In the **Delete Group** confirmation pop-up window, click **Yes**.
5. If you do not wish to delete the group, click **Cancel** to return to the Groups page.

CHAPTER 5

Using Active Directory Domain

Active Directory Users and Groups Overview


When the px4-300r is connected to an Active Directory domain, administrator users can import users and groups from an Active Directory (AD) server and grant them access rights to Shares on the px4-300r. You can have both local and AD users on your px4-300r. See [Managing Your px4-300r Network Storage with Local and Active Directory Users](#) for more information. For information on enabling AD on the px4-300r, refer to [Configuring Your px4-300r to Use Active Directory](#).

Managing Active Directory Users and Groups

The section describes how to:

- [Import Users and Groups from Active Directory](#)
- [Synchronize with the Active Directory Controller](#)
- [Change Access Permissions for AD Users or Group](#)
- [Set Quotas](#)
- [Delete an AD User or Group](#)

Importing Users and Groups from Active Directory

1. Click the **Domain Management** icon to join your px4-300r to an Active Directory domain. See [Configuring Your px4-300r for Active Directory](#) for more information.
2. With Active Directory enabled, click the **Users & Groups** icon to open the management interface for adding users and groups.
3. Click  **Import Users and Groups from Active Directory**.
4. The pop-up window for **Import Users and Groups from Active Directory** is searchable, and you can sort by name, descriptive name, or type. You can filter the list of users and groups by selecting a specific user or group from the domain tree.
5. Select the checkbox next to a user or group to import that user or group to your px4-300r Network Storage Array from the Active Directory domain. Select the checkbox in the title bar to select all the users and groups in the Active Directory domain.
6. Click **Apply** to save your changes.


Synchronizing with the Active Directory Controller

You can poll the Active Directory controller at any time to check for new users and groups on the controller, so you can add them to your px4-300r. This keeps your px4-300r up to date with any group changes on the controller and indicates if any users on the controller were deleted or promoted.

- Click  **Synchronize with the Active Directory Controller**.

Changing Access Permissions

Expand **Access Permissions** to change user or group permissions to a secured Share. When the px4-300r is in AD mode, AD and local users can have access to a secured Share. See [Managing Your Device with Local and Active Directory Users](#).


1. To add permissions to a Share, click  **Add access permissions**.
2. From the **Add Access Permissions** pop-up window, select a Share or Shares for the user or group to access. Select the checkbox in the title bar to select all the Shares listed.
3. Click **Apply** to save your changes.
4. In the table listing the Shares, check **Read** or **Write** for each Share. A user or group can have full access by checking both **Read** and **Write**. To grant only read access, check only **Read**.



A user or group must have read access at a minimum. A user or group cannot have only write access.

5. Uncheck **Read** to remove all access to a Share and remove the Share from the table.
6. Click **Apply** to save your changes.

Setting Quotas

1. Click  **Quota settings** to enable quotas and set a default quota. Quotas are only set for individual users, and not groups.
2. In the **Quota Settings** dialog, click **Enable quotas** to turn on quotas for each user. Quotas can be set for each user individually or set as a default value.
3. Enter a **Default Quota** in gigabytes. When you set a default quota, this becomes the quota size for all new users.
4. Check **Set default quota for all users** to globally set the same quota size to all users. You may overwrite this default value for individual users by setting their quota size separately in the user's Information section.
5. Click **Apply** to save your changes.

Deleting an Active Directory User or Group

To delete a user or a group:

1. Click the **Users & Groups** icon to open the feature management page.
2. To delete an existing user or group, click to expand that user or group.
3. In the Information section, click **Delete**. Deleting a user or group does not delete any Shares to which the user or group has access.
4. In the confirmation pop-up window, click **Yes**.
5. If you do not wish to delete a user or group, click **No** to return to the Users & Groups interface page.

Managing Your px4-300r Network Storage Array with Local and Active Directory Users

You can configure your px4-300r to allow both local users and groups and Active Directory (AD) users and groups on the device simultaneously. While in AD mode, you can have existing local users and groups and also create new ones. In addition, both AD and local administrator users can log into and manage the px4-300r. This allows hybrid authentication on your px4-300r and, if desired, you can switch between AD mode and Workgroup mode.

Enabling Active Directory after Creating Users in Workgroup Mode

After you create users in Workgroup mode, you can switch your px4-300r to AD mode. This enables support for both Active Directory users and groups and local users and group.

1. On the Domain Management page, select **Active Directory**.
2. Configure your AD settings. See [Configuring your px4-300r for Active Directory](#) for more information.
3. Click **Apply**.

After changing to AD mode, you are required to log back in to the px4-300r. Your px4-300r is now configured to allow both local administrators and AD administrators to log in.


Logging in to Your px4-300r

When an administrator logs in to the px4-300r, the admin chooses between the device name or the AD domain name.

1. At the Login screen, choose what type of user is logging in from the Active Directory Domain drop-down:
 - to log in as a local user, choose the device name from the drop-down menu and enter the username and password
 - to log in as an Active Directory user, choose the Active Directory domain name from the drop-down menu and enter the username and password
2. Click **Login**.

Creating Local Users and Groups in Active Directory Mode

After an AD or local administrator logs in to the px4-300r, that admin user can create additional local users and groups on the px4-300r. The **Users & Groups** feature lists all local and AD users and groups on the px4-300r.

1. Click the **Users & Groups** icon to open the management interface for adding users and groups.
2. Click  **Add users and groups...**
3. In the Import Users and Groups from Active Directory page, under Local, click **Users** to create a local user or **Groups** to create a group. You can add AD members to any local groups you create.
4. Enter the necessary credentials for the user or the group name, and click **Create**.

Creating Share Permissions for AD Users and Local Users

You can create access permissions for both AD and local users on any new or existing Shares on your px4-300r. For more information, see [adding Shares](#) and [managing Shares](#).

Switching to Workgroup Mode from Active Directory

Switching your px4-300r from AD mode to Workgroup mode will remove all AD users and groups, including AD admin users, from the px4-300r.

1. Click the **Domain Management** icon to open the feature management page.
2. Click the switch to turn off Active Directory.
3. Click **Apply**.
4. If you are an AD administrator making this change, you will be required to log back into the device as a local user. If there isn't a local administrator account on the px4-300r, device setup will run to enable you to create a new administrator user.



Creating a new local administrator user through device setup will not affect other configuration settings or content stored on the px4-300r. Local users and groups will not be changed.

CHAPTER 6

Sharing Files

Sharing Overview

Your px4-300r Network Storage Array is set up for storing, retrieving, and accessing files among users, client computers, and applications.


File sharing is accomplished by:

- [Creating Shares](#)
- [Creating users and groups and setting access permissions](#)
- [Setting up media services](#)
- [Configuring Active Folders](#)

This section on Sharing Files also provides information on advanced file sharing options, including network protocols and customizing the device home page.

Interfaces for Sharing

Your px4-300r has three separate interfaces for file sharing:

- **px4-300r Device Management Console**
You manage the creation of Shares and set user access to Shares through the device management console (web-based management interface).
- **LenovoEMC Storage Manager**
Optionally installed on your local computer, LenovoEMC Storage Manager discovers any LifeLine-based network storage devices on your subnet, maps device Shares to computers, and provides local access to your content. It provides access to Shares through your computer's file management program, such as Windows Explorer or Mac Finder, allowing you to drag and drop many files between your computer and your px4-300r device. Installing LenovoEMC Storage Manager is optional.
- **Home Page**
The Home page serves as a web-accessible interface to your px4-300r device. The Home page content is configured using the device management console. The Home page displays any Shares that have been made accessible to everyone (public Shares). It can also display secured Shares accessible only to users who log in to the px4-300r device from the Home page. You can access the Home page of your px4-300r device by entering the device name or IP address directly in your browser. If you are an administrator user, you can access the device management console from the Home page by clicking  .

Shares

What are Shares and How Do I Organize Content with Them?

Shares are folders that contain all types of content, including documents, pictures, and music files. Shares are secured by default, which means access to content in them is limited to users and groups with specified privileges. If you want Shares on your device to be publicly accessible, which means they can be accessed by anyone who has access to your network, you must set Read and/or Write permissions for Everyone to that Share.



When Media Sharing is enabled, all media content on that Share will be available to all DLNA media-capable devices on the network, including computers and web browsers. This makes your media content available to everyone who has access to your network, even if specific user access privileges are set for that Share. If you do not want your media files to be publicly available, do not enable the media sharing option.

All Shares on the px4-300r are displayed on the Shares page. The Shares page displays a table that contains folders, connected drives, and any cloud storage to which your px4-300r is connected. The Properties column displays the features that are enabled for each Share.

Share Information

The Information section on the Shares page displays the Share name, graphically displays the space usage of the Share, and allows you to view the content using the web-based content viewer.

To view the content of a Share, click **View Content** to open the Content Viewer.



You can also use the standard file browser on your client computer to view the content of Shares. You must have user access permissions for the Share. If you have installed LenovoEMC Storage Manager, it will map drive letters for px4-300r Shares under Windows or mount Shares on a Mac. Look for the px4-300r device under Network locations in Windows Explorer. On a Mac, open a new Finder window and look under Shared. See [Discovering the px4-300r Using Your Computer OS](#) for additional information.

To learn how to modify your Share information, refer to [Managing Shares](#).

Access Permissions

The Access Permissions section contains a list of users who currently have access to that Share. If you give permissions for Everyone to a Share, access to the Share is unrestricted, and content on the Share can be viewed by anyone with access to your network.


To learn how to modify Access Permissions on a Share, refer to [Managing Shares](#).

Active Folders

Follow the link to the Active Folder options for information on configuring each:

- [Email Distribution](#)
- [Facebook](#)
- [Flickr](#)
- [Photo Resize](#)
- [YouTube](#)

Adding Shares

1. Click the **Shares** icon to open the feature management page.
2. To add a new Share, click  **Add a Share**. Type a name for the Share. All Shares must have a name. Names cannot exceed 32 characters. The following are not valid Share names: global, homes, printers.
3. Click **Create**. To modify an existing Share, click the Share row to expand the Share.

Managing Shares


You can change Share information, change access permissions, make a Share an Active Folder, use Share volumes, and modify a Share volume.

If available, you can also enable NFS secured access.



The **Application Data** share is created automatically when you install an application that requires data storage on the px4-300r network storage device. Do not change or delete this share.

Changing Share Information


1. Modify the existing name for the Share.
2. Choose whether to enable media sharing. When Media sharing is enabled, the media server scans this Share for any media content and makes it available to anyone with access to your network, even if this Share is secured. If you do not want media content made available to anyone, do not check this option. When Media sharing search is enabled,  displays in the Properties for that Share.
3. To view the content of a Share, click the **View Content** link to open the Content Viewer.
4. Click **Apply** to save your changes.


Changing Access Permissions

1. Expand **Access Permissions** to change user permissions to a Share. You can provide specific access privileges to users or groups, or you can make a Share public by setting Read and Write permissions for Everyone.



All Shares are secured by default, so they will be accessible only by the device administrator unless additional access permissions are set. The administrator created during device setup has default access to initial Shares; access permissions to these Shares must be explicitly set for all other users, including added administrator users. When new Shares are added to the px4-300r, all existing administrator users will have default access to those Shares.




The security icon  displays in the Share's properties to indicate that the Share is secured.

2. Check **Allow users to change file level security** to allow file and folder permissions to be set through other programs, such as Windows Explorer, independent of the px4-300r. Setting this option allows users to put additional access restrictions on individual files and folders.
3. To limit access to this Share to a specific set of users, click  **Add access permissions** and choose one or more users from the pop-up window. If you have created groups, you can select one or more groups.
4. In the **Access Permissions** section, check Read, Write, or both to set access to this Share for each user. To remove a user, leave both Read and Write unchecked for that user. If you grant Read and Write permissions for Everyone, the list of users is also cleared since all users will have access to this Share. If you have created groups, you can also set Share access by specifying

group permissions.

5. Click **Apply** to save your changes.

Enabling NFS Secured Access


1. To enable **NFS**, first click the switch on from the Protocols page.
2. On the Shares page, select a secure Share and expand the NFS section. You cannot apply a rule to an unsecured Share.
3. Click  **Add an NFS rule** to add a **Host Name** for the rule. Rules are added to specify the hosts that are allowed to access Shares using NFS. Use this table to add NFS rules to specify access for hosts. For example, *.cs.foo.com matches all hosts in the domain cs.foo.com. To export a Share to all hosts on an IP address or local network simultaneously, specify an IP address and netmask pair as address/netmask where the netmask can be in dotted-decimal format, or as a contiguous mask length. For example, either /255.255.252.0 or /22 will result in identical local networks.
4. When the rule is added, read access is automatically set to the Share. Select **Write** to allow users to write to that Share. Use  and  to modify the rule priority for NFS access.
5. Click **Apply** to save your changes.

Making a Share an Active Folder


1. You can optionally enable Active Folders on a Share to allow you to associate this Share with a specific feature that will happen automatically when files are copied to the Share. For example, you can enable a Share as a social media active folder to upload a file to a social media site. Refer to [Sharing Content with Social Media Overview](#). You can only set one Active Folder option per Share.
2. Expand the **Active Folder** section and check **Enable**. Select one of the following Active Folder options and follow the link for details on configuring each:
 - [Email Distribution](#)
 - [Facebook](#)
 - [Flickr](#)
 - [Photo Resize](#)
 - [YouTube](#)
3. Click **Apply** to save your changes.

Using Share Volumes

When you create a Share, you can use an existing volume or create a new one for that Share. After that Share is created, you cannot move it to a different volume. You can modify the volume by changing its size.

1. To set the volume for a Share as you are creating it, click  **Change volume allocation** in the **Information** section.
2. Choose whether to use an existing volume or to create a new one. For more information on existing volumes, refer to [Adding and Managing Volumes](#).
3. Select an existing Storage Pool in which to place the volume.
4. If you are selecting from more than one existing volume, select a volume from the **Volume** drop-down menu.
5. If you are creating a new volume, enter a name for the volume in the **Volume** text box.
6. Enter a size for the volume. You cannot reduce this size later.
7. Click **OK**.
8. In the Information section, click **Apply** to save your changes.

Modifying a Share Volume

1. Click  **Change volume allocation** in the **Information** section.
2. Enter a new size for the volume.
3. Click **OK**.
4. In the Information section, click **Apply** to save your changes.

Deleting Shares

To delete a Share:

1. Click the **Shares** icon to open the feature management page.
2. To delete an existing Share, click to expand the Share.
3. In the Information section, click **Delete** to delete the Share.
4. In the **Delete Share** confirmation pop-up window, click **Yes**.
5. If you do not wish to delete the Share, click **Cancel** to return to the Shares page.



Do not delete the Application Data share if it appears on your px4-300r network device. It is required by applications that store data on the px4-300r.

Using Protocols to Share Files

What Are Protocols and How Do I Use Them to Share Files?

Your px4-300r Network Storage Array uses communication protocols to mount file systems and allow files to be transferred between client computers and the px4-300r.

The px4-300r includes the following protocols for file sharing:

- [Apple Filing Protocol / Time Machine](#)
- [Bluetooth](#)
- [FTP](#)
- [TFTP](#)
- [NFS](#)
- [rsync](#)
- [SNMP](#)
- [Web Access \(HTTP/HTTPS\)](#)
- [WebDAV](#)
- [Windows DFS](#)
- [Windows File Sharing](#)

AFP File Sharing for Macs


The Apple Filing Protocol (AFP) enables Apple file sharing, which is the preferred method for Mac users to access Shares on the px4-300r. When AFP is enabled, you can use Time Machine to back up a Mac client computer to your px4-300r Network Storage Array. See [Backing up Macs with Time Machine](#).

AFP is on by default. If AFP has been disabled, click the switch on to re-enable it.

Bluetooth File Sharing

Once a Bluetooth adapter is detected, files can be uploaded from a Bluetooth device to a configurable destination Share on the px4-300r.

Configuring Bluetooth settings


1. To enable Bluetooth, click the switch on.
2. Once Bluetooth Transfer is enabled, check the box **Require a PIN for access** if you want to require Bluetooth users to supply a unique PIN to allow file transfers to the destination Share on the px4-300r. When using this option, you must define a unique PIN number for each device attempting to upload data using Bluetooth.
3. To set the destination Share, click .
4. Click **Apply** to save your settings.



To change any Bluetooth settings, click .

FTP File Sharing

On the Protocols page, click the switch to turn on FTP (File Transfer Protocol) and allow access to your px4-300r Network Storage Array.

Click  to select either FTP or secure FTP (SFTP) or both. If you select and enable SFTP, you cannot have the [secure rsync protocol](#) enabled.

When you turn on FTP, you can send files to your px4-300r.

TFTP

On the Protocols page, click the switch to turn on TFTP (Trivial File Transfer Protocol) and allow access to your px4-300r Network Storage Array. When you turn TFTP on, you can send files to your px4-300r using FTP.

NFS File Sharing

On the Protocols page, click the switch to turn on NFS (Network File System). This protocol allows remote hosts to mount file systems over a network and interact with them as though they were mounted locally to your px4-300r. Your px4-300r Network Storage Array uses NFS version 4, which improves security and performance.



Select an option to choose how users on client computers are mapped to the px4-300r:

Set the squashing options for NFS:

- To have all users, including root, map as guest, select **Treat client users as guest (all_squash)**. All files are owned by user guest, and all users accessing the px4-300r have the same access rights. If you have enabled Active Directory on your px4-300r, this is the only option available for mapping client computers.
- To have all users map as themselves but root maps as guest, select **Allow full access for client users other than root (root_squash)**.
- To have all users map as themselves, including root, select **Allow all client users full access**.

If the px4-300r is using Active Directory mode, you see the following NFS version 4 security settings:

- **System security** - This uses Linux system security.
- **Kerberos security** - Kerberos is a protocol that uses secret key cryptography for authentication between client and server applications.
- **All** - Combines system security and Kerberos security.

Once enabled, add NFS access rules for each secure Share from the [Managing Shares](#) page. NFS provides another protocol for sharing storage data with Linux hosts. When NFS is enabled, you can configure rules for host-based access to secure Shares.

Rules can be added to secure Shares to specify the hosts that are allowed to access Shares using NFS. For example, *.cs.foo.com matches all hosts in the domain cs.foo.com. To export a Share to all hosts on an IP address or local network simultaneously, specify an IP address and netmask pair as address/netmask where the netmask can be in dotted-decimal format, or as a contiguous mask length. For example, either /255.255.252.0 or /22 will result in identical local networks.

To change any NFS settings, click .

Access to Shares through NFS and User Permissions

When you access your px4-300r through NFS, the access permissions to content on the px4-300r are controlled by Host-Based Access Control rules on your client computer, not by user access permissions on your px4-300r. This means that any valid user on the Linux computer who has access to the host (the storage device) can access Shares on the px4-300r, even if not given specific user permission to those Shares on the device.

rsync: Synchronizing Files with Another Storage Device or Other Computers

When you turn on this protocol, you enable the px4-300r Network Storage Array as an rsync server. It can then be used as a source and/or destination device for rsync Copy Jobs. Because of the fast and efficient nature of rsync, an rsync Copy Job can be faster than a Windows File Sharing Copy Job. For more information on Copy Jobs, refer to [Backing Up Your px4-300r](#).

If you enable the px4-300r as an rsync server, you can optionally set up a user account on the px4-300r for secure rsync Copy Jobs.

Configuring rsync server settings

1. To enable rsync server, click the switch on.
2. To create a secure user account, check **Configure secure rsync credentials**.
3. The username is preset as rsync. You can change this to a more meaningful user account name. Enter a password and confirm it for the rsync user account name. When you create a secure rsync user account on the px4-300r, you allow other devices to securely copy to or from it.
4. By default, rsync uses TCP port 873 for accepting requests. You can change this value to a different port number, if desired.
5. Click **Apply** to save your settings.



To change any rsync server settings, click . You cannot enable rsync server if you have already enabled [SFTP](#).

Monitoring Your Device with an SNMP Management Tool

SNMP (Simple Network Management Protocol) provides information about the state of the px4-300r Network Storage Array to various administrative computers, known as managers. When the SNMP protocol is enabled on a device, SNMP agent software on the device reports information to the managers, and an administrator user can perform some configuration of the px4-300r through the manager. Information that comes from the px4-300r is called a trap. Managers and the px4-300r must be running on the same network.

SNMP should be disabled unless you are specifically providing information to a management system that requires this information.

Configuring SNMP settings

1. To enable SNMP, click the switch on.
2. Enter a unique username and password to define the community.
3. Confirm your password.
4. Enter the IP address of the host in the **Trap Receivers** text box. To grant access to multiple receivers, list all of them in the text box, separating each entry with a space.
5. Click **Apply** to save your settings.

To change any SNMP settings, click  .

SNMP Traps

A px4-300r can provide various traps to a manager. These traps provide information on the current state of the px4-300r.

Traps include:

- A drive may have either failed or been removed
- Multiple drives may have either failed or been removed
- The device encountered a file system corruption

SNMP MIB File for the px4-300r

The management information base (MIB) file is a database of various device object types, which a manager can change. Examples of MIB objects are:

deviceName – the name of the px4-300r network storage device

diskName – the name of drives on the px4-300r network storage device

conTable – a table for the connected client count

raidStatus – a description of the RAID status. Values are Normal, Rebuilding, Degraded, RebuildFS, and Faulted.

The MIB file is available for downloading by entering the following URL in your browser:

`http://<devicename>/manage/mibs/lenovoemcmib.txt`

where <devicename> is the model name for your px4-300r unless you have [set a custom device name](#).

Managing File Sharing with Web Access (http/https)

The Web Access protocol enables or disables the link to the [Content Viewer](#) from the Shares page. When the Content Viewer is disabled, you cannot browse any Share content from the px4-300r management interface.

If you disable the Web Access protocol, you also disable the display of the home page on your px4-300r. Refer to [Sharing Your Content with the World](#) for additional information on displaying the home page for your px4-300r.

WebDAV: Managing Files Using HTTP or HTTPS

WebDAV (Web-based Distributed Authoring and Versioning) is a protocol that provides web-based access to Shares on the px4-300r. With WebDAV enabled on the px4-300r, you can view, add, or delete files through your WebDAV client using either HTTP for unencrypted access or HTTPS for encrypted access. HTTP offers faster performance, but is not secured. Access Shares using a URL such as `http://devicename/WebDAV/Foldername`. Refer to your operating system's documentation to learn how to access files through WebDAV.

Configuring WebDAV settings

1. To enable WebDAV, click the switch on.
2. To enable WebDAV for HTTP, check **Enable WebDAV Over HTTP**.
3. To enable WebDAV for HTTPS, check **Enable WebDAV Over HTTPS**.
4. Click **Apply** to save your settings.

Windows DFS: Creating a Distributed Windows File System

Windows DFS (Distributed File System) organizes Shares and files on a network, such that they appear to be all in one directory tree on a single network storage device, even if the Shares reside on many devices.


Windows DFS terms

There are several terms to understand with Windows DFS.

- **Namespace:** A virtual Share containing other folders that are located on different devices throughout a network.
- **DFS root:** An object that consolidates all the folders in your network and makes them available through a single entry point. An example of a DFS root is `\\DeviceName\DFSRootName`.
- **DFS link:** A folder under the DFS root.

Configuring Windows DFS settings

To enable Windows DFS, click the switch on.

1. Enter a DFS root name. The DFS root name is the starting point of a DFS namespace.
After entering a DFS root name, you add DFS links, which map to folders on other devices.
2. Click  **Click to add a DFS link target** to begin adding DFS links.
3. Enter the DFS link name, which includes the name of the host and Share to which you are linking.

4. Click **Apply** to save your settings, or click **Cancel** to discard your changes.

Windows File Sharing

Windows File Sharing allows you to work in Workgroup mode, using the px4-300r device management console to create users and manage access. To enable Windows File Sharing, click the switch on.

Sharing Content through the Home Page


Sharing Your Content with the World

When you set up the Home Page for your px4-300r Network Storage Array, you are presenting content to anyone who accesses your px4-300r from an internet browser. That content includes a slideshow and Shares where you have set access permissions for Everyone.

You can manage the look of the Home Page by using the **Home Page Settings** feature. This allows you to display a slideshow, display public Shares, name the Home Page, and turn the Home Page on or off.

1. Click the **Home Page Settings** icon.
2. Click the slider switch to **On** to enable the Home Page on your px4-300r.
3. Select **Default home page settings**.
4. Enter a title for the Home Page. This title displays in the top banner of the Home Page when users access the px4-300r. If you leave this field blank, the default device name is used.
5. Check **Display Shares** to display publicly accessible Shares. When you select to display Shares, users will see all Shares where you have set access permissions for Everyone.
6. Check **Display slideshows** to display picture slideshows that are in folders on the px4-300r. Click **Manage slideshows** to configure any slideshows you want to display. The slideshow location can be any folder attached to the px4-300r, including a USB drive or [DFS location](#).
7. Click **Apply** to save your changes, or click **Cancel** to discard your changes.

Deleting a Slideshow

To delete a slideshow from the list of available slideshows, click . After you delete a slideshow, you can configure a different one.

Custom Home Page Content


For information on custom home page content, refer to [Adding a Custom Home Page](#) below

Adding a Custom Home Page

You can customize the look of the home page for your px4-300r Network Storage Array to include html pages and client-side scripting, such as Javascript. This customized home page replaces the default home page on the px4-300r. In addition, there are applications available on www.lifelineapps.com that can enhance your home page content.

You add your custom html content to a Share on your px4-300r and then specify its location on the Home Page Settings page.

Applying the Customized Home Page

1. Click the **Home Page Settings** icon to access the feature settings.
2. Select **Customized home page settings**.
3. In the Home Page Name field, enter the name of the start page of your custom home page. By default, the name is index.html.
4. Specify the destination Share where the start page and your html content exists on your px4-300r by clicking  and navigating to the Share.



You cannot access the destination Share through the [WebDAV](#) interface. Access through WebDAV is permanently disabled.

5. Select the Share name and click **Apply**.
6. Click **Apply** to save your settings.



When you apply a custom home page for your px4-300r, the icon for opening the px4-300r management console is no longer visible. To return to the management console, you must explicitly enter the URL to the management console in your browser:
IP address/manage/management.html

Automatically Sending Content to Multiple People at Once

You can send content to multiple people at once using an email distribution active folder. You can configure a [Share](#) as an Email Active Folder so that when you add files to that Share, they are automatically sent to the recipients on the email distribution list. To configure a Share as an Email Active Folder, access the Shares feature from the px4-300r device management console, select or create a Share, and expand the Active Folders section to enable and configure email distribution.

How to Set Up an Email Distribution Active Folder



Email Distribution lets you email your files to friends and family directly from your px4-300r device management console. Use Email Distribution to share files with an email list. To prevent email distribution list spamming, the px4-300r allows lists of 250 or fewer email recipients and sends a maximum of six emails in a 24-hour period.

Refer to [Managing Shares](#) for more information on managing Shares and Active Folders.

Configuring an Email Distribution Active Folder

1. Click the **Shares** icon to access the feature page.
2. Select a Share to use as an Email Distribution Active Folder, and click to expand the Active Folder section.
3. Check **Enable**.
4. Select **Email Distribution** from the drop-down menu.
5. Include an email address in the **Sender Email Address** text box. Distribution is sent from this email address.
6. You can add multiple email addresses in the **Email To:** text box by separating them with commas, spaces, or semicolons.
7. Add a subject and email message for your recipients.
8. Check **Send the file as an attachment**, **Send a link to the file**, or both.
9. Click **Apply** to save your changes.
10. Once configured, all files in this Share are sent by email to your recipients. Click **View Transfer History** to see the transfer activity from this Share to your account.

Sharing Content Using Social Media: Overview

If you have an account with social media services such as Facebook, Flickr, or YouTube, you can share content on your px4-300r Network Storage Array with your friends and family using one or more of these social media sites. To share your content using social media sites, create Shares called [Active Folders](#), and connect each Active Folder with a social media account. Refer to the help topic links below for more information on these procedures. When you add photos and movies to an Active Folder, those files are automatically uploaded to the social media site associated with that Active Folder. If you have photos or movies you want to share with others, this is a great way to make your content available to people who may not have access to your px4-300r.

If you have configured a Personal Cloud on your px4-300r, you can grant Personal Cloud users access to Shares and Active Folders. This is useful if you want to allow users to add files to your social media sites. For example, if your px4-300r has a Flickr Active Folder, you can grant Personal Cloud users access to that Active Folder. In this manner, when photos are added to the Flickr Active Folder, either by you or by Personal Cloud users, those photos are uploaded automatically to your Flickr account.

Note that an Active Folder can only be associated with one social media account. For example, if you want Active Folders for your Facebook and YouTube accounts, create two Active Folders, and assign one Active Folder to Facebook, and one to YouTube. Using this example, any photos you add to your Facebook Active Folder are automatically uploaded to your Facebook page, and any movies you add to your YouTube Active Folder are automatically uploaded to your YouTube page. Not only is this a fast and easy way to share content, but uploading content to your social media sites provides an additional backup of your content, as the content is stored both on your px4-300r and at your social media accounts.

Managing Your Content

You manage content on your px4-300r Network Storage Array using the Content Viewer. The Content Viewer is a graphical file browser that lets you view and manage content in the Shares on your px4-300r from the device management console or the LenovoEMC Storage Manager.

The Content Viewer is divided into two panes. The left pane lists the Shares on the px4-300r and allows you to delete or add a Share. If you select a Share that contains pictures, you can start a slideshow of the pictures in that Share. The right pane lists the files and folders in a Share and allows you to delete content or upload a file to the Share.

To delete multiple files simultaneously, hold the Ctrl key on your keyboard and select each file, or drag your mouse over the filenames. Share content can be sorted, and you can switch between a list view and a thumbnail view of the files. When you are looking at content in a list view and you hover your mouse over an image, a thumbnail view of the image displays next to your mouse. If all the content cannot fit on one page, there are pagination controls that allow you to continue browsing the content.

Transferring Content to and from Your px4-300r Network Storage Array with Copy Jobs

You can transfer content to and from your px4-300r using the Copy Jobs feature. Copy Jobs copies files from one storage device to another, either by a set schedule or immediately by the user. An example of a Copy Job scenario is if you keep pictures from your digital camera on a separate USB drive, but you also want to maintain a backup of these pictures on your px4-300r. Using Copy Jobs, you can create a task that copies your photos on the USB drive to a Share on your px4-300r, and you can set that task to a schedule so the images automatically copy at a specific time. This ensures that your photos are always safely backed up to your px4-300r in the event your USB device ever fails or is lost.



While a Copy Job copies all data from one NAS device to another, it does not copy permissions or access rights from one NAS device to another.

All saved Copy Jobs display on the Copy Jobs page. From there, you can manually start and stop a Copy Job, view Copy Job information, modify a Copy Job, check its last run status, and, if applicable, view when the Copy Job is next scheduled to run.

When defining a Copy Job, you can copy data from or to any of the following:

- Any NAS device automatically discovered on the same subnet as your px4-300r
- Any NAS device that you manually add to the subnet using the LenovoEMC Storage Manager
- Any external storage device, such as a USB device, connected to your px4-300r
- A Windows computer that is automatically discovered on the same subnet as your px4-300r

When selecting what data to copy on the source storage device, you can choose a specific folder or all folders. You can also copy from a folder on an external storage device mounted to your px4-300r.

When selecting the destination device, you can copy files to the top-level folder on the destination device (the default option), or to an existing folder on this device, which adds the copied files into folders.

You can manually start or stop a Copy Job by clicking start or stop buttons on the Copy Jobs page. You can schedule a Copy Job to run automatically at a set day and time.


Copy Jobs Limitations

- Copy Jobs does not establish a continuous replication or mirroring relationship between the source and destination devices. You should not set up Copy Jobs for disaster recovery.
- Copy Jobs does not support transferring content from iSCSI drives.

Getting Content from a USB External Storage Device

You can transfer content to your px4-300r Network Storage Array from external USB storage devices. The External Storage page displays a list of externally connected storage devices. You can connect supported external storage to your px4-300r using one of the provided USB ports. When you connect external storage to your px4-300r, that device content is accessible from the **Shares** page.

Safely removing external storage

Click  to safely remove the external storage. A confirmation dialog will display. Click **Yes** to remove the external storage. When the external storage has been removed from the **External Storage** table, it is safe to remove, and you may unplug it from the px4-300r. When the external storage is safely removed, its associated Share is removed as well.

One-touch Transferring of Content from a USB Device


One touch transfer of content is created on the QuikTransfer page. On the QuikTransfer page, you can set the default destination Share for any automatically created QuikTransfer Copy Jobs.

QuikTransfer automatically copies all files from any USB external storage device plugged into your px4-300r Network Storage Array to the destination Share when the QuikTransfer button is pressed.



You must have a USB external storage device connected to the px4-300r before using this feature.

Setting QuikTransfer

1. Select a destination folder for the default QuikTransfer Copy Job by clicking  and selecting a folder in the file browser. The file browser provides a way to select a Share and all its folders, or just some of the folders under a Share.
2. Click **Apply** to save your setting.

CHAPTER 7

Drive Management

Managing Drives

The Drive Management feature provides settings for managing storage and lets you apply global settings for drives on your px4-300r Network Storage Array. The Drive Management feature also enables you to [add and manage Storage Pools](#) on your px4-300r.

Write Caching

Write Caching is a global setting that applies to all drives in your px4-300r. To set the disk write caching value, click the Settings icon and select an option from the drop-down menu. The settings options are **Always disabled**, **Enabled with UPS**, or **Always enabled**.



Enabling Disk Write Caching is not the same as creating an SSD Cache. See [Improving Performance with a Cache Pool](#) for information on how to create and use an SSD Cache.

Understanding Disk Write Caching


Write caching is a mechanism that attempts to separate the fast processing speed of the px4-300r from the relatively slow mechanics of actually writing data to drive.

When write caching is disabled, every write to drive causes the px4-300r to wait while the data is written to drive, which can slow performance. When write caching is enabled and the px4-300r sends a write request to the drive, it writes the data to cache (which is much faster) and sends an immediate acknowledgment to the px4-300r saying the write is complete. The system proceeds without waiting for the data to actually get written to drive, which occurs in the background.

While write caching does improve performance, there are some risks. The system responds that the data is written to drive when in fact it has only been written to cache. Should the px4-300r lose power, any data not completely written to drive is lost forever.

This is because cache memory is volatile. If you lose power, the contents of the cache are lost. Therefore, if there were any pending writes in the cache that were not written to the drive, they will be lost forever. Using a UPS (Uninterrupted Power Supply) can mitigate the risk associated with write caching, which is why it is recommended to only enable this feature when a UPS is connected.

Global Drive Management Settings

1. Click  **Settings** to access the global drive management settings available on your px4-300r.
2. Select the link **Perform an offline file system check then reboot** if any of the following conditions exist on your px4-300r:
 - Data is unavailable
 - Data is missing after an unclean shutdown
 - You are concerned about the integrity of the file system



This option will take the volume offline for some time. The check could take up to several hours, depending on the size of the volume and other factors. During the check, data will be inaccessible. When the check is completed, it will reboot the device.

3. Select a value for **Disk Write Caching**. See [Understanding Disk Write Caching](#) for more information on the options.

4. Check **Use available drives as hot spares** to allow unused drives to become part of a RAID-protected storage pool. If a drive in a Storage Pool fails, all the data on that drive can be mirrored to the hot spare drive.
5. Click **Apply** to save your changes.

Storage Pool Information

The Drive Management page displays a table that provides the following information about existing Storage Pools.

- **Name** – The name of the Storage Pool.
- **Protection** – The type of protection assigned to the Storage Pool.
- **Capacity** – The total amount of storage in the Storage Pool.
- **Allocated/Available** – Allocated is the space allocated to share volumes and iSCSI volumes. Available is the difference between capacity and used.

See [Storage Pool Management](#) for more information.

Drive Status

An image on the Drive Management page provides information on the drive status of your px4-300r. The image displays the physical layout of drives and the drive slot numbers. If a drive has a circled letter, it is a member of a Storage Pool. If you hover your mouse over a drive in the image, the ToolTip displays the drive model, size, and status, including if the drive is failing.

If you hover your mouse on either a Storage Pool name in the table or on a drive in the Storage Pool image, all drives in the Storage Pool are highlighted.

Adding New Drives to Your px4-300r Network Storage Array

The px4-300r can be powered on or off when installing or replacing hard drives. If you have purchased a diskless device, you might want to install all of the hard drives at once (steps 1-4 below). In this case, it is recommended that you power off the px4-300r while installing the drives. If you are replacing a drive that has failed, it will be easiest to do so while the px4-300r is powered up. This will enable you to use the px4-300r management interface to confirm that you are removing the correct drive.



Make sure you are installing drives qualified for use with your px4-300r. Refer to <http://support.lenovoemc.com> for a list of approved drives.

The following instructions cover installing new hard drives (HDDs) or SSDs in your px4-300r while the device is powered on:

1. Access the drive bays for your px4-300r and pull out an empty drive tray.
2. Mount the drive on the drive tray using the screws included with the drive.
3. Insert the drive tray containing the new drive back into the empty slot.



If the first drive installed in the px4-300r contains data, a dialog box will appear asking for confirmation to overwrite the drive. Click **Yes** to proceed. Any existing data will be deleted. If the px4-300r is unable to overwrite the existing data, refer to the LenovoEMC support site for instructions for cleaning a hard drive (see https://lenovo-na-en.custhelp.com/app/answers/detail/a_id/30456). After cleaning the disk, re-install it in your px4-300r.

You will not see the confirmation dialog for additional drives even if they contain data.

4. If this is the first drive installed in your px4-300r, you will be re-directed to Device Setup. If you are not re-directed to Device Setup, see [Accessing Your Device If It's Not Discovered](#).
5. If your px4-300r is already set up, you will be re-directed to the management console.
6. From the px4-300r management console, select the **Drive Management** icon under **All Features**.
7. Your px4-300r displays the new hard drives in the bays where they are mounted.
8. To create a RAID Array, you must install a minimum of two hard drives. You can remain on the Drive Management page while mounting the second drive.



If you are installing drives that contain data, they will be overwritten when you select them on the Drive Management page. If you encounter issues overwriting a drive, refer to https://lenovo-na-en.custhelp.com/app/answers/detail/a_id/30456 for instructions on how to clean the drive.

9. When all new drives have been detected, click  **Add a Storage Pool**.



You can create a Storage Pool using one drive if desired. You will not have any RAID protection options and can only select **None** from the RAID dropdown list while configuring your Storage Pool.

10. Complete the [Storage Pool configuration options](#) and select the desired drives on which to build the Storage Pool by checking the boxes next to them. All drives in a Storage Pool must be the same model, manufacturer, and capacity.



The image will vary depending on the specific network storage device and the installed drives.

11. Allow a few minutes for the RAID array and Storage Pool to build. When complete, the Storage Pool status displays on the Drive Management page:

ID		Protection	Capacity	Allocated/Available
▼ A	Work	Mirror (RAID 1)	1.8 TB	829.36 GB / 0.99 TB

CHAPTER 8

Storage Pool Management

Understanding How Your Content Is Stored

Content on your px4-300r Network Storage Array is stored in [Shares](#) and iSCSI volumes. To access content in Shares, your client computer uses network [protocols](#), such as AFP and Windows File Sharing. The px4-300r's file system maintains the physical location of content that resides in volumes used for Shares. Block-level data is stored in iSCSI drives. File systems for iSCSI volumes are maintained by the connected host computer and not the px4-300r.

Shares reside on volumes, which along with iSCSI volumes, reside in Storage Pools. Volumes allow you to partition space in Storage Pools, and Storage Pools group multiple physical drives together into a single logical unit to provide redundancy, availability and capacity. All the drives in a Storage Pool must be the same size and should have the same protection (for example, RAID 5).



All disks within a single Storage Pool must meet the following requirements:

- Same manufacturer
- Same rotational speed
- Same capacity

Mixed disk configurations may result in unpredictable device behavior and will not be supported. If you need technical assistance, please be prepared to backup your data and remove any unsupported drives or configurations.

Storage Pools

A Storage Pool is a grouping of drives with a certain storage size and an assigned data protection. A Storage Pool has a minimum of one drive. By default, your px4-300r has one Storage Pool.

Storage Pool Data Protection

For each Storage Pool, you can select its type of protection. Protection type determines how data is replicated across a Storage Pool and determines the amount of space used for data protection and storage. The drives in your px4-300r are protected using a built-in, pre-configured technology that redundantly stores data across the drives, so that if a single drive fails, in most cases, you will not lose any data. This technology, known as RAID (Redundant Array of Independent Disks), enables a series of drives to act together as a single storage system. If you create multiple Storage Pools, you can assign different [RAID types](#) to each Storage Pool.

For more information on selecting RAID types, refer to [Changing RAID Protection Types](#).

Volumes

A Volume is a single storage area. A volume can be comprised of one or more hard drives. In a single-volume system, the volume consists of the entire storage space. Shares reside in volumes. iSCSI drives also reside in volumes.


Adding and Managing Storage Pools

A Storage Pool is a grouping of drives with a certain storage size and an assigned data protection. A Storage Pool has a minimum of one drive. By default, your px4-300r Network Storage Array has one Storage Pool. If you add drives to your px4-300r, you can create additional Storage Pools. If your px4-300r includes different capacity drives, you will need to create additional Storage Pools as all drives in a single Storage Pool must be the same capacity.

If your px4-300r has one or more SSD drives installed, you can create a Cache Storage Pool, which is a grouping of solid-state drives that helps increase read and write performance to [volumes](#) in a data Storage Pool. See [Creating a Cache Storage Pool](#), for more information on this option.

Adding a Data Storage Pool

Adding a new Storage Pool requires available drives, that is drives that are not already incorporated into an existing Storage Pool. If you want to use multiple Storage Pools and all drives are already included in an existing Storage Pool, you will need to delete the existing Storage Pool before proceeding with the steps below.

1. Open the **Drive Management** feature and click  **Add Storage Pool**.
2. In the **Information** section, enter a name for the Storage Pool.
3. To set the RAID protection, choose a value from the drop-down menu:
 - **Parity (RAID 5)**: Uses the space corresponding to one drive-size for protection, leaving remaining space for storing actual data.
 - **Mirror Stripe (RAID 10)**: Uses half of the storage space for protection, leaving half for actual data. Protects data in the event of a single drive failure. Requires at least four drives.
 - **None (RAID 0)**: Uses all of the storage space for data. Does not protect against data loss in the event of drive failure; however, the drive are striped for better performance.
 - **None**: Uses all of the storage space for data, providing contiguous storage space by concatenating all member drives. Does not protect against data loss in the event of drive failure.
4. Select the checkbox of the drive or drives you want to add to the Storage Pool. All drives in a Storage Pool must be the same size. If your px4-300r includes different capacity drives, you will need to create a Storage Pool for each capacity grouping.
5. Check **Enable periodic consistency check** to enable a monthly parity or mirror consistency check.



The check helps to prevent a single drive failure from becoming a two-drive failure, resulting in data loss. The check runs for several hours and can affect performance of the px4-300r. If you do not want to run the check, remove the check mark for this option.

6. If commonly used Shares, Backups, Documents, Movies, Music, Pictures, and SharedMedia do not already exist on the px4-300r device, check **Create commonly used Shares** to create these Shares and add them to the Storage Pool.

7. If your px4-300r includes one or more SSD drives that are not already incorporated into a Storage Pool, you will see the option **Use for SSD Cache**. See [Creating a Cache Pool](#) for more information.



You cannot create commonly used Shares on an SSD Cache Pool.

8. Click **Create** to add the new Storage Pool.
9. Click **Cancel** to discard any changes.

Improving Performance with a Cache Storage Pool

A cache Storage Pool is a pool of solid-state drives designed to increase read and write performance on your px4-300r Network Storage Array. You create a cache Storage Pool and then associate a [volume](#) on a data Storage Pool to the cache pool.




You can create only one cache Storage Pool on your px4-300r. You can associate a cache pool with multiple data storage volumes and allocate specific portions of the cache to each storage volume.

Creating a Cache Storage Pool

To create a cache Storage Pool, there must be one or more SSD drives installed in your px4-300r that are not part of an existing Storage Pool.



Typically, you create a cache Storage Pool with one solid-state drive. However, if you want to use the fastest cache policy (Write-back) with your cache volumes, it is recommended that you create a cache pool with at least two SSD drives and apply a redundant RAID protection to help prevent data loss in the event one of the SSDs fails.

1. Open the **Drive Management** feature and click  **Add Storage Pool**.
2. In the **Information** section, enter a name for the cache Storage Pool.
3. To set the RAID protection, choose a value from the drop-down menu:
 - **Parity (RAID 5)**
Uses the space corresponding to one drive-size for protection, leaving remaining space for storing actual data.
 - **Mirror Stripe (RAID 10)**
Uses half of the storage space for protection, leaving half for actual data. Protects cached write data in the event one SSD fails.
 - **None (RAID 0)**
Uses all of the storage space for data. Does not protect against data loss in the event of drive failure; however, the SSDs are striped for better performance.
 - **None**
Uses all of the storage space for data, providing contiguous storage space by concatenating all member drives. Does not protect against data loss in the event of drive failure.



If you plan to use the Write-back policy for any cache volume, the cache pool should use the same level of drive protection as the data pool to prevent data loss in case of loss of the cache pool. If you will be using only Write-through or Write-around cache volumes, the cache pool can be unprotected. See the following section on [Assigning a Cache Pool to a Volume](#) for more information on setting cache policy options.

4. Select the checkbox of the solid-state drive or drives you want to add to the cache pool. You can only designate SSDs as cache pool drives if they have not already been assigned to an existing Storage Pool. All drives in a Storage Pool must be the same size.

5. Check **Enable periodic consistency check** to enable a monthly parity or mirror consistency check.



The check helps to prevent a single drive failure from becoming a two-drive failure. The check runs for several hours and can affect performance of the px4-300r. If you do not want to run the check on your cache pool, remove the check mark for this option.

6. Check **Use for SSD Cache**.
7. Click **Create** to add the cache Storage Pool.
8. Click **Cancel** to discard any changes.

Assigning a Cache Pool to a Volume

After creating a cache Storage Pool, you assign a volume from a data Storage Pool to use a specified portion of the cache pool. A cache pool can be assigned to a new or existing volume. You can also assign multiple storage volumes to use the cache pool by managing the cache size for each volume.

1. On the Drive Management page, begin [creating a volume](#) or expand an existing volume in a data Storage Pool.
2. In the information section for the volume, check **Use cache for this volume**.
3. Enter a value for the **Cache Size (GB)** to specify the amount of cache space for the volume. This value cannot exceed the total size of the cache pool.
4. Select the **Cache Policy** to use with this volume.
 - **Write-through** - This is the safest cache policy. All writes are cached to the SSD pool and are also written to disk immediately. Write-through caches are not persistent through a drive removal or device reboot. All disk reads are cached.

If your SSDs have slower write performance than your non-SSD drives, this policy may limit write performance; however, this is likely only when using early generation SSDs. You can avoid this issue by using only SSDs qualified for use with your px4-300r. Refer to <http://support.lenovoemc.com> for a list of approved SSDs.
 - **Write-back** - This is the fastest cache policy, but is less safe. All writes go to the cache pool initially and then are written to disk later. Data loss can occur if the cache pool is lost before disk write is completed (for example, if an SSD fails on an unprotected cache pool). Write-back caches are persistent across drive removal or device reboot. All disk reads are cached.
 - **Write-around** - This is a safe policy that improves read performance, but not write performance. Writes are not written to the cache pool. They are written directly to disk. Write-around caches are not persistent across drive removal or device reboot. All disk reads are cached.
5. Click **Apply** to save your settings for an existing volume, or click **Create** to create a new storage volume.



It is possible to create user data volumes or iSCSI drives in an SSD cache pool; however, this can affect the performance of the cache pool and is not recommended.

Volumes

Snapshots

Snapshots Overview

A snapshot is a backup of a source volume at a certain point in time. The snapshot can be taken while the px4-300r is actively writing to the source volume, which means you do not have to stop your px4-300r from writing to the volume. After a snapshot is taken, you have the option of restoring it to the source volume and reverting the source volume to its state at the time the snapshot was taken.

Snapshots can be created on demand, or they can be scheduled. You can create a snapshot on an [encrypted volume](#). Any Shares in the source volume are added to the snapshot with a date stamp appended to their name, for example, Documents_2012_09_22_11_22_35. You can add content to these snapshot Shares.



You cannot create a snapshot of a volume that has SSD cache enabled.

Creating a Snapshot on Demand

1. On the Drive Management page, in an existing non-cache Storage Pool, expand the Volumes section, expand the Volume name and then expand the Snapshots section.




You must have already created a [Share](#) on this volume to see the Snapshots section.

2. Click **Create a snapshot of this volume now**.
3. In the Create a Snapshot dialog box, specify the following and click **Apply**:
 - Enter a size for the snapshot as a percentage of the source volume.
 - Choose whether to expose or unexpose the snapshot. If you unexpose the snapshot, no content on the snapshot is available for access. If the snapshot is exposed, you can view the contents of the snapshot. With either unexposed or exposed snapshots, you can restore files from them.
 - If you do not want to write any content to the snapshot, check **Make snapshot read-only**.
 - If you select to expose the snapshot, you can check **Expose for previous version only**. Previous versions is a feature in Windows only. Previous versions are copies of files and folders that Windows automatically saves as part of a restore point. You can use previous versions of files to restore files that you accidentally modified or deleted, or that were damaged. To access previous versions, right-click a file or folder in Windows Explorer and click **Restore Previous Versions**.

Creating Snapshots with a Schedule

1. On the Drive Management page, in an existing non-cache Storage Pool, expand the Volumes section, expand the Volume name and then expand the Snapshots section.
2. Click **Create snapshots of this volume on a schedule**.
3. In the Manage Snapshot Schedule dialog box, specify the following and click **Apply**:
 - Check **Enable snapshot schedule**
 - Specify when to take a snapshot, for example, every hour, four hours, or once a day.


- Enter a start time, or click  to use the sliders.
- Select the days you want to take a snapshot, or select **All Days** to take a snapshot every day.
- Enter the number of snapshots to save.
- Enter a size for the snapshots as a percentage of the source volume.
- Choose whether to expose or unexpose the snapshot.
- If you do not want to write any content to the snapshot, check **Make snapshot read-only**.
- If you unexpose the snapshot, you can make it read-only.
- If you select to expose the snapshot, you can check **Expose for previous version only**.

Managing Snapshots


Snapshots display in a table under the source volume. Snapshots are named with the source Share name and an appended date and time stamp, for example, Shares_2012_08_17_10_10_32. You cannot change the name of a snapshot.

After a snapshot is created, you can modify it in several ways.

Exposing/Unexposing the Snapshot

Click  to alternate the snapshot between exposed and unexposed.

Restoring a Snapshot

This feature overwrites any changes in the source volume and returns it to its state at the time the snapshot was taken. Click  to restore a snapshot. After you click this button, you are prompted to confirm the restore. Click **Yes**. After you click **Yes**, an additional confirmation displays. The message indicates that the source volume will be briefly unavailable, and the snapshot will be deleted. Check the checkbox and click **OK**.

Deleting a Snapshot

Click  to delete a snapshot. When prompted to confirm the deletion, click **Yes**.

Displaying Shares in the Snapshot

Expand the snapshot Information section, and click **View snapshot Shares**. This opens a window that displays all the Shares in the volume. When you list the shares, you can determine if this is a snapshot you want to restore. Click **OK** to close the window. You can view the Shares in an exposed or unexposed snapshot.

Make the Snapshot Read-only

Check **Read-only** to alternate snapshot between writeable and read-only.

Changing Expose Mode

In an exposed Share snapshot, you can set the expose mode for "Expose all Shares" and "Expose for previous versions." Expose for previous versions exposes content so that you can access it through Windows Explorer. Expose all Shares not only allows you to access old content through the previous versions mechanism, it also creates Shares with the backup time in their name so you can access content on computers that are not running Windows.


Adding and Managing Volumes

A volume is a single accessible storage area with an allocated size. You can create volumes after creating Storage Pools.

Shares in Volumes

All Shares on the px4-300r Network Storage Array are added to volumes, and the size of the Share is limited by the free space of the volume. When you create a Share, you can add it to a volume at the same time. This is the simplest method for adding a Share to a volume. For more information on adding Shares to volumes, refer to [Using Share Volumes](#). All iSCSI drives on the px4-300r are added to volumes, and the size of the iSCSI drive is limited by the free space of the volume. When you create an iSCSI drive, you can add it to a volume at the same time. This is the simplest method for creating iSCSI drives. For more information on adding iSCSI drives, refer to [Managing iSCSI Drives](#).

To add a new volume:

1. On the **Drive Management** page, expand a Storage Pool, expand the **Volumes** section, and click  **Add a Volume**.
2. In the **Information** section, enter a name for the volume in the **Volume** field.
3. In the **Size (GB)** field, enter a size in gigabytes (GB) for the volume. Note that both the allocated and available space for the volume displays.
4. When you create a new volume, you can optionally enable encryption to protect your data if your px4-300r is lost or stolen. You can only enable encryption when you create a volume. Enabling encryption can reduce performance since information transferred to and from the drives must be processed using the 256-bit Advanced Encryption Standard (AES) protocol. To apply encryption to a volume, click the **Enable encryption** checkbox. There are two options for encryption: allowing the system to generate a passphrase, or creating one yourself. The passphrase is not a 256-bit encryption key.
 - **Generate and save passphrase on the system** – Select this option to allow the system to store a passphrase for the volume. This type of encryption works only when the px4-300r is powered down. If any drives are removed while your system is powered down, data on the encrypted volume will not be accessible. When the px4-300r is rebooted, the system-generated passphrase is automatically applied to the encrypted volume, unlocking it and enabling data access.
 - **Enter a passphrase** – This is a more secure type of encryption and is the recommended option. Click the **Enter a passphrase** option; then enter and verify a passphrase for the volume. You can change the passphrase at any time. After restarting the px4-300r, an encrypted volume is unavailable until you re-enter the passphrase. Note that the passphrase must consist of eight or more characters.

After you create a passphrase, a new section for the volume appears called **Volume Encryption**. When you want to unlock a volume, enter the passphrase in this section.



It is recommended that you save a backup of the master key file in a secure location, separate from your px4-300r. You should not save the backup master key to a drive that is connected to your px4-300r. If a system failure occurs, the passphrase stored on your px4-300r may be lost, and your backup master key file is required to recover and access your data. Also, if you forget



your passphrase, you can reset it using the backed-up master key. Click **Back up master key** to back up the master key file. To reset the passphrase, click **Reset passphrase with master key**, then enter a new passphrase and verify it.

5. If you are adding a volume in a [cache pool](#), there is an option to associate the volume with a cache pool. Check **Use a SSD cache for this Volume**.
6. Click **Create** to save your changes.
7. Click **Cancel** to discard any changes.

Deleting a Storage Pool

1. On the **Drive Management** page, expand the **Information** section of the Storage Pool you want to delete.
2. Click **Delete**.
3. The **Delete Storage Pool** window displays.
4. Select **Check this box if you want to delete the Storage Pools**.
5. Click **Yes** to delete the Storage Pool.
6. Click **No** to cancel the operation and retain the Storage Pool.



Deleting a Storage Pool deletes all Shares and data contained within the Storage Pool.

Changing RAID Protection Types

You can change the RAID protection of existing Storage Pools. You can also set the RAID protection type when you [add drives](#) to your px4-300r Network Storage Array and [create new Storage Pools](#). Protection type can be changed only when the Storage Pool is in a normal (healthy) state. If you are unfamiliar with RAID protection, it is recommended that you do not change this setting.



Most changes to protection type will delete all data on the Storage Pool. You can make the following protection type changes without deleting data:

- Expanding a RAID 5 configuration by adding one or more drives.
 - Migrating from RAID 1 with two disks to a RAID 5 configuration with three or more disks.
 - Migrating from JBOD with one disk to RAID 1 with two disks.
-

To change the RAID type, expand the Information section of a Storage Pool on the Drive Management page, and choose a value from the Protection drop-down menu:

- Parity (RAID 5)
- Mirror Stripe (RAID 10)
- None (RAID 0)

For additional explanation on these RAID types, refer to [Adding and Managing Storage Pools](#).

Note that the displayed available capacity changes as you select different RAID types from the Protection drop-down menu. RAID array capacity is based on drive use, which differs for some RAID types.

Click **Apply** to change the RAID protection.

Click **Cancel** to retain your previous RAID configuration.

CHAPTER 9

iSCSI: Creating IP-Based Storage Area Networks (SAN)


iSCSI Overview

The iSCSI page allows you to create iSCSI drives on your px4-300r Network Storage Array and allows the LenovoEMC Storage Manager to communicate with those drives over a network. An iSCSI drive provides a single place for all your storage, which you can divide as needed to support all computers in your enterprise business. iSCSI is useful for transmitting large blocks of data over a network at a high speed.

Only one client computer can connect to an iSCSI drive at a time, so iSCSI drives are not for shared data. If your business is clustering clients, then a cluster can access iSCSI drives. Also, you must create a list of users who can access an iSCSI drive. These are not users who have access to other features on your px4-300r.

Adding iSCSI Drives

To add an iSCSI drive:

1. Click the **iSCSI** icon to open the feature management page.
2. When the iSCSI page opens, click the switch to enable the feature.
3. Click  **Add an iSCSI drive**.
4. If your px4-300r has multiple Storage Pools, select the desired Storage Pool from the drop-down menu.
5. Enter a name for the iSCSI drive.
6. Enter a size for the iSCSI drive. The size must be smaller than the free space available on your px4-300r.
7. Click **Create** to create the iSCSI drive.

Enabling iSCSI Drives

1. Click **Settings** to begin configuring an iSCSI drive.
2. To set the discovery of the iSCSI drive using iSNS, check **Enable discovery with iSNS**.
3. Choose one of the following options:
 - **Use local iSNS server** – the device acts as an iSNS server for the iSCSI drives.
 - **Use external iSNS server** – you supply the IP address or host name of the external iSNS server for the iSCSI drives.
4. To enable the Challenge Handshake Authentication Protocol (CHAP), check **Enable two-way authentication (Mutual CHAP)**. With Mutual CHAP enabled, the client performs an additional check to confirm that it is using the correct device.
5. Enter an initiator secret (password) for Device Secret and then enter it again in the confirm box.
6. Click **Apply** to save your changes.

Connecting to iSCSI Drives

You can connect iSCSI drives on your px4-300r to your computer using LenovoEMC Storage Manager or the Microsoft software initiator. If you are using another type of software or hardware initiator, you must use the native tools provided with your initiator to connect your iSCSI drives. Do not connect more than one iSCSI initiator at a time to an iSCSI drive.




Attempting to connect two iSCSI initiators to the same iSCSI drive at the same time may result in data corruption or drive damage. The px4-300r management console prevents you from connecting two iSCSI initiators to the same iSCSI drive at the same time, but if you connect to an iSCSI drive using native tools, you may encounter this issue. You can use the **Connected Clients** section to view a list of client computers connected to your px4-300r that are running iSCSI initiator software. On the iSCSI page, expand an iSCSI drive, then expand the Connected Clients section. If the iSCSI drive is in use, you will see a list of connected client computers running initiator software.

Managing iSCSI Drives

Adding CHAP User Access to an iSCSI Drive

After you add an iSCSI drive, you create a list of CHAP users that have access to an iSCSI drive. These users are independent from the [users you create](#) on your px4-300r.

1. On the iSCSI page, expand an iSCSI drive, and expand **iSCSI CHAP Users** to add user access to an iSCSI drive.
2. Click  **Add a CHAP user** and enter a CHAP username and password.
3. Click **Create**. Continue adding as many users as needed to access the drive.
4. To delete a user, expand the user section and click **Delete**.

Deleting iSCSI Drives

To delete an iSCSI drive:

1. Click the **iSCSI** icon to open the feature management page.
2. Click the iSCSI name to expand the iSCSI drive.
3. In the iSCSI Information section, click **Delete** to delete the iSCSI drive.
4. Click **Yes** in the confirmation pop-up window.
5. If you do not wish to delete the iSCSI drive, click **Cancel** to return to the iSCSI page.

CHAPTER 10

Backing up and Restoring Your Content

Backup and Restore Overview

Your px4-300r Network Storage Array provides many ways to back up and restore content.

To back up content to and restore content from your px4-300r, you can use:

- Time Machine
- Copy Jobs

To back up and restore your px4-300r, you can use the following features and applications:

- Copy Jobs
- Avamar
- Amazon S3
- LenovoEMC Personal Cloud features

Backup of Data through RAID Protection

The drives in your px4-300r are protected using a built-in, pre-configured technology that redundantly stores data across the drives. This technology, known as RAID (Redundant Array of Independent Disks), enables a series of drives to act together as a single storage system. RAID configurations that provide data redundancy preserve data integrity on the system if a drive fails and is replaced.



While RAID technology provides fault tolerance, it is not a true backup. It is strongly recommended to always have another copy of your data that is not stored on the px4-300r.

For more information, refer to [Understanding How Your Content Is Stored](#).

Backing up to and Restoring from Your px4-300r Network Storage Array

Backing up Macs with Time Machine

You can use Time Machine to back up a Mac client computer to the px4-300r network storage device.

Follow the instructions below to set up Time Machine backups to your px4-300r:

1. Connect your Mac to your px4-300r using Apple File Protocol (AFP). You can do this using LenovoEMC Storage Manager for Mac or Bonjour.
2. Mount the Backup Share from the px4-300r network device.



If you want to create a new Share for Time Machine backups, you can do so using the px4-300r management console. Mount the Share you want to use before proceeding to the next step.

3. Select **System Preferences...** from the Apple Menu.
4. Select **Time Machine** (listed under System).
5. Click **ON** to enable Time Machine.
6. From the list of available drives, choose the desired Share on your px4-300r, then click **Use for Backup**.
7. Time Machine will automatically create the sparsebundle image under the selected Share and begin backing up your computer to your network storage device. After the initial backup, Time Machine backs up files every hour.



Time Machine uses a single destination drive for backups. If you have previously set up another drive for Time Machine backups and want to change to use the px4-300r network device, click **Select Disk**, then choose the desired Share on your px4-300r.

One-touch Transferring of Content from a USB Device


One touch transfer of content is created on the QuikTransfer page. On the QuikTransfer page, you can set the default destination Share for any automatically created QuikTransfer Copy Jobs.

QuikTransfer automatically copies all files from any USB external storage device plugged into your px4-300r Network Storage Array to the destination Share when the QuikTransfer button is pressed.



You must have a USB external storage device connected to the px4-300r before using this feature.

Setting QuikTransfer

1. Select a destination folder for the default QuikTransfer Copy Job by clicking  and selecting a folder in the file browser. The file browser provides a way to select a Share and all its folders, or just some of the folders under a Share.
2. Click **Apply** to save your setting.

Copy Jobs Overview

You can back up content to and from your px4-300r Network Storage Array using the Copy Jobs feature. Copy Jobs copies files from one storage device to another, either by a set schedule or immediately by the user. An example of a Copy Job scenario is if you keep pictures from your digital camera on a separate USB drive, but you also want to maintain a backup of these pictures on your px4-300r. Using Copy Jobs, you can create a task that copies your photos on the USB drive to a Share on your px4-300r, and you can set that task to a schedule so the images automatically copy at a specific time. This ensures that your photos are always safely backed up to your px4-300r in the event your USB device ever fails or is lost.

For more information, refer to [Backing up Your px4-300r Network Storage Array](#) on the facing page.

Backing up Your px4-300r Network Storage Array

Copy Jobs

Transferring Content to and from Your px4-300r Network Storage Array with Copy Jobs

You can transfer content to and from your px4-300r using the Copy Jobs feature. Copy Jobs copies files from one storage device to another, either by a set schedule or immediately by the user. An example of a Copy Job scenario is if you keep pictures from your digital camera on a separate USB drive, but you also want to maintain a backup of these pictures on your px4-300r. Using Copy Jobs, you can create a task that copies your photos on the USB drive to a Share on your px4-300r, and you can set that task to a schedule so the images automatically copy at a specific time. This ensures that your photos are always safely backed up to your px4-300r in the event your USB device ever fails or is lost.



While a Copy Job copies all data from one NAS device to another, it does not copy permissions or access rights from one NAS device to another.

All saved Copy Jobs display on the Copy Jobs page. From there, you can manually start and stop a Copy Job, view Copy Job information, modify a Copy Job, check its last run status, and, if applicable, view when the Copy Job is next scheduled to run.

When defining a Copy Job, you can copy data from or to any of the following:

- Any NAS device automatically discovered on the same subnet as your px4-300r
- Any NAS device that you manually add to the subnet using the LenovoEMC Storage Manager
- Any external storage device, such as a USB device, connected to your px4-300r
- A Windows computer that is automatically discovered on the same subnet as your px4-300r

When selecting what data to copy on the source storage device, you can choose a specific folder or all folders. You can also copy from a folder on an external storage device mounted to your px4-300r.

When selecting the destination device, you can copy files to the top-level folder on the destination device (the default option), or to an existing folder on this device, which adds the copied files into folders.

You can manually start or stop a Copy Job by clicking start or stop buttons on the Copy Jobs page. You can schedule a Copy Job to run automatically at a set day and time.

Copy Jobs Limitations


- Copy Jobs does not establish a continuous replication or mirroring relationship between the source and destination devices. You should not set up Copy Jobs for disaster recovery.
- Copy Jobs does not support transferring content from iSCSI drives.

Adding Copy Jobs



The page describes how to:

- [Add Copy Jobs](#)
- [Set From Information](#)
- [Set To Information](#)
- [Set a Schedule](#)

Adding Copy Jobs



1. On the Copy Jobs page, click . A Copy Job is added to the top of the list and the Information section displays.
2. Enter a name for the Copy Job.
3. The **Overwrite Setting** determines what happens to files in the destination location if they have the same name as those in the source location. Select one of the following values from the Overwrite Setting drop-down menu:
 - **Overwrite and don't delete** – Files in the destination location are overwritten with files from the source location. Any files in the destination location that are not in the source location are preserved.
 - **Overwrite and delete** – Files in the destination location are overwritten with files from the source location. Any files in the destination location that are not in the source location are deleted. The destination location becomes an exact copy of the source location.
 - **Don't overwrite** – Only files in the source location that are not in the destination location are copied. No files are overwritten in the destination location.

From: Settings


1. In the **From:** section, click  to select a source location. This is the location of the files you want to copy. In the dialog, enter the Device Name or IP address in the text box, or select a device from the list. If a connected device is not listed, click the **Refresh** button.
2. Click **OK** to save your selection or click **Cancel**.
3. The **Protocol** drop-down menu displays if the source device is different from the device you are currently accessing; for example, it could be a separate NAS device on your network. From the **Protocol** drop-down menu, choose one of the following:
 - **Windows File Sharing** – The default value in the menu is Windows File Sharing and in most cases you should accept the default value. For more information, refer to [Windows File Sharing](#) on page 61.
 - **rsync** – The rsync protocol can provide faster copying, but may not be available on all devices. If you are able to select the rsync protocol, and you want the rsync Copy Job to be secure, select the **Use secure rsync (SSH)** option. Enter the rsync username and password for the rsync server to or from which you are copying. The rsync username and password is set up on a different device than the device on which you are creating the Copy Job. For more information on creating an rsync user, refer to [rsync: Synchronizing Files with Another Storage Device or Other Computers](#) on page 58.
4. Enter a valid username and password, if applicable, for the device to provide access to its folders.
5. To select a specific folder, click  to select a source location for the **What to copy:** section. In the Copy dialog box, select all Shares or a folder, and select one of the following options for the Copy Job from the drop-down menu:
 - **The selected folder and its contents** – copies the selected folder and its contents. If the destination is a folder, a new folder will be created for each source folder. If the destination is Top Level, a new top-level folder is created on the destination device for each source folder.

- **Only the contents of the selected folder** – copies the contents of the selected folder; not the folder itself. If the destination is a folder, the files and folders in the selected folder are copied directly to it (the source folder name is not copied). If the destination is Top Level, a new top-level folder is created on the destination device for each folder in the source folder.
6. By selecting Shares, you choose to copy All Shares, in which all files on the px4-300r are copied. Any files not contained in a folder are not copied. If the destination is a folder, a new folder will be created for each source folder. If the destination is Top Level, a new top-level folder is created on the destination device for each source folder.
 7. Click **OK** to save your selection or click **Cancel**.
 8. Click **Apply** to save your changes.

To: Settings

1. In the **To:** section, click  to select a destination location. This is the location where you want your files copied. In the dialog, enter the Device Name or IP address in the text box. Or, from the drop-down menu, select a device in the list. If a connected device is not listed, click the **Refresh** button.
2. Click **OK** to save your selection or click **Cancel**.
3. The Protocol drop-down menu displays if the source device is different from the device you are currently accessing; for example, it could be a separate NAS device on your network. From the **Protocol** drop-down menu, choose one of the following:
 - **Windows File Sharing** – The default value in the menu is Windows File Sharing and in most cases you should accept the default value. For more information, refer to [Windows File Sharing](#) on page 61.
 - **rsync** – The rsync protocol can provide faster copying but, may not be available on all devices. If you are able to select the rsync protocol, and you want the rsync Copy Job to be secure, select the **Use secure rsync (SSH)** option. Enter the rsync username and password for the rsync server you are copying from or to. The rsync username and password is set up on a different device than the device on which you are creating the Copy Job. For more information on creating an rsync user, refer to [rsync: Synchronizing Files with Another Storage Device or Other Computers](#) on page 58.
4. Enter a valid username and password, if applicable, for the device to provide access to its folders.
5. To select a specific folder, click  to select a destination location for the **Copy to here:** section. In the Copy to here dialog, select a Share or a folder from a Share to copy your files.
6. Click **OK** to save your selection or click **Cancel**.
7. Click **Apply** to save your changes.

Setting a Schedule

1. To set a schedule, expand the Schedule section.
2. In the Schedule section, select **Enable Schedule for Copy Job**.
3. Select the days you want the Copy Job to run, or select **All Days** to run the Copy Job every day.
4. Click  to select a start time. Click **Done** to save your time selection.
5. Click **Apply** to save your changes. The new Copy Job displays on the Copy Jobs page.

Managing Copy Jobs

From the Copy Jobs page, you can add, start, stop, delete, or monitor Copy Jobs.


After you have added Copy Jobs, the Copy Jobs page displays a list of Copy Jobs. The information section includes the name of each Copy Job, date and time it last ran, and its next scheduled time.

From the Copy Jobs list, you can perform the following actions:

Modifying Copy Jobs

1. In the list on the Copy Jobs page, find the Copy Job you want to modify, and click it to expand the **Information** section.
2. Refer to [From: Settings](#) on page 97 for information about revising the Copy Job fields.

Deleting Copy Jobs

1. In the list on the Copy Jobs page, find the Copy Job you want to delete.
2. Click  from the **Actions** column of the table to delete the Copy Job.
The Delete Copy Job pop-up window opens.
3. If you are sure that you want to delete the Copy Job, click **Yes**.



If you do not wish to delete the Copy Job, click **Cancel** to return to the Copy Jobs page.

Restoring Files with Copy Jobs

To restore files with Copy Jobs, create a new Copy Job that reverses the back-up Copy Job. Modify the From and To settings to copy files from the backup location to the original source location, specify what to restore, set overwrite settings, and choose the protocol for the Copy Job.

Refer to [From: Settings](#) on page 97 for detailed information on Copy Job settings.

Registering with Avamar for Backup and Restore

Avamar is backup and recovery server software that uses deduplication to eliminate redundant copies of data, reducing the required storage space. For example, your px4-300r Network Storage Array might have 100 email messages with the same 1 MB attachment. If all those emails are backed up, that same attachment is backed up 100 times, requiring 100 MB of storage space. With Avamar and data deduplication, only one copy of the attachment is actually stored, so 100 MB of storage is effectively reduced to 1 MB.



When you enable Avamar on your px4-300r, you are registering with an Avamar server. You cannot back up and restore from your px4-300r. Backup and restore operations are executed from the Avamar server.

Registering Your px4-300r with the Avamar Server

1. On the Avamar page, click the switch on.
The Avamar Settings pop-up window opens.
2. In the Avamar Settings pop-up window, enter the following information and click **Apply** to save your settings:
 - **Server Address** – the Avamar server IP address or hostname.
 - **Client Domain** – the registered domain name from the Avamar server.

Backing up with Amazon S3

The Amazon S3 online storage service allows you to back up your px4-300r Network Storage Array to the cloud.

Enabling the Amazon S3 Feature

1. On the Amazon S3 page, click the switch on.
If you do not have an Amazon S3 account, click the link to create an account.
2. Enter a valid access key, secret key, and bucket name from your Amazon S3 account information.
You can create a bucket at account setup, or you can enter a new bucket for your px4-300r. Your content lives in this bucket on your Amazon S3 account.
3. Select an existing Share on your px4-300r in which to copy files that are then backed up to Amazon S3.
4. Click **Apply** to save your changes.

Backing up Files to the Amazon S3 Cloud

After you copy files to the selected Share on your px4-300r, the files are automatically backed up to the Amazon S3 cloud service. File uploads are limited to 5 GB in size. If you delete files from the selected Share on your px4-300r, they are not automatically deleted from the cloud service. You can manually delete those files from the cloud service by clicking a command on the Amazon S3 page.

Restoring Files with Amazon S3

When you want to restore files from the Amazon S3 cloud service to your px4-300r Network Storage Array, you can choose to restore all files or select individual files to restore.

Backing up with LenovoEMC Personal Cloud

You can back up content on your px4-300r Network Storage Array by creating a Copy Job from the LenovoEMC Personal Cloud hosted on the device to another LifeLine-based network storage device that is a member of the same Personal Cloud.

Refer to LenovoEMC Personal Cloud help for additional information.

Restoring Files with Personal Cloud

You can restore content on your px4-300r by creating a Copy Job from the LenovoEMC Personal Cloud on it to another px4-300r that is a member of the Personal Cloud.

Refer to LenovoEMC Personal Cloud help for additional information.

CHAPTER 11

Remote Access: Accessing Your px4-300r Network Storage Array From Anywhere in the World

Remote Access Overview

This section describes how to use TZO remote access to access your device's data from any web-enabled computer in the world.



If TZO remote access was enabled when you upgraded your px4-300r to LifeLine version 4.0 or higher, the feature will continue to function as it did before. Otherwise this feature no longer appears. We recommend you use Personal Cloud for remote access. See [LenovoeEMC Personal Cloud](#) for more information.

Review the following prerequisites prior to enabling remote access:

- **Enable Security** – Before you can enable remote access, you must have security enabled on your px4-300r Network Storage Array.

If security is already enabled, you are ready to enable remote access. If not, a pop-up window is provided to enable security and create an administrator user to manage your secured px4-300r.
- **Check the internet connection** – Your px4-300r requires internet connectivity.
- **Automatically configure the router** – Prior to enabling remote access, ensure that your router is UPnP enabled. If you have more than one router on your network, you must only have one router used as a DHCP Server. Refer to your router documentation for more information. Your px4-300r attempts to automatically configure your router. However, if it cannot, a warning displays, and you must manually configure your router to forward a specific port to your px4-300r. Most routers refer to this as port forwarding or application access, and it is recommended that you refer to your router's documentation to learn how to set these values.

The following information is needed to manually configure your router:

- **Device IP Address**
- **Port Name** – HTTPS
- **Port Number** – 443
- **Protocol** – TCP
- **Choose a subscription service level** – Basic or Premium.
 - **Basic** – Allows you to define a sub-domain name and choose from a list of domains (Domain Name) to create your web address. A complimentary subscription period with TZO is included with your purchase of your px4-300r. Once your complimentary subscription period expires, you must renew your subscription with TZO to continue accessing your px4-300r remotely.
 - **Premium** – Requires you to pay for your registration subscription by following a link before you can complete the enabling remote access process. It allows you to define a top-level domain name (Domain Name), or use one that you already own, such as yourname.com
- **Create a Web Address for your Device** – You create a web address to access your px4-300r by specifying a Domain Name.

Enabling Remote Access

Follow this procedure to enable remote access:

1. [Enable security](#) if it is not yet enabled.
2. On the Remote Access page, click the switch to Enable.

Your px4-300r begins to automatically configure remote access. First, your internet connection is tested. If the connection is successful, a green checkmark displays on the px4-300r image. If there is a problem, an error message displays. After resolving the error, you can click the provided link to retest the connection.

If the configuration is successful, a green checkmark displays on the image of your router.



See ["Remote Access Overview "](#) on page 104 for information on manually configuring your router if your router cannot be automatically configured.

3. Once the router is configured, click **Register with TZO** to choose a subscription level (basic or premium) and follow the associated procedure below to complete the enabling remote access process.

See ["Remote Access Overview "](#) on page 104 for more information on the subscription levels.

Basic Option: Completing the Enable Remote Access Process

1. The registration fields display. Enter the following information in the pop-up window to create a web address for your px4-300r and define an email address:
 - **Sub-domain Name** – Enter a unique sub-domain name in the first text box.
 - **Domain Name** – Select a domain name from the drop-down list. It is recommended that you choose a domain name that you can easily remember and will help you identify your px4-300r.

The web address is created by combining the sub-domain and domain name. This will ultimately be the address that will be registered and you can use to access your px4-300r remotely.
 - **Email Address** – The email address will be registered with TZO to notify you about domain name renewals.
2. Click **Apply** to save your settings.



If the domain name you selected is already in use, you will need to define a new one and click **Apply** again.

If your registration is successful, the pop-up window closes, and the Remote Access page provides your account information under the TZO logo.

Premium Option: Completing the Enable Remote Access Process

1. The registration fields display. Enter the following information in the pop-up window to create a web address for your px4-300r and define an email address:
 - **Domain Name** – Enter a domain name. It is recommended that you choose a domain name that you can easily remember and will help you identify your px4-300r.

This will ultimately be the address that will be registered and you can use to access your px4-300r remotely.

- **Email Address** – Enter a valid email address. The email address will be registered with the DDNS server to notify you about domain name renewals.
2. Click **Apply** to register your domain name.



If the domain name you selected is already in use, you will need to define a new one and click **Apply** again.

3. If your domain name is valid, a new browser window opens and you will be redirected to the TZO site where you can register your web address and purchase your registration at special rates.

The Remote Access page provides your account information under the TZO logo.

Accessing Your px4-300r Network Storage Array Remotely

Once you have enabled remote access and created your web address, you can access files stored on your px4-300r Network Storage Array from any internet-capable computer in the world.

When you access your px4-300r remotely, you can access files from any Share to which you are granted access. However, accessing your px4-300r from a remote location will not provide all the same functionality provided by a computer in your local network.

The following procedure describes how to access your px4-300r remotely.

Open a web browser and type your px4-300r unique web address, which can be found on the Remote Access page. The Home page of the px4-300r displays. Administrator users can log in. Non-administrator users can access only the content available from the Home page.

CHAPTER 12

Personal Cloud: Accessing Your LenovoEMC Personal Cloud From Anywhere in the World

What Is LenovoEMC Personal Cloud ?

LenovoEMC Personal Cloud turns your px4-300r Network Storage Array into a hub for sharing files and backing up data among computers anywhere in the world. A Personal Cloud can exist on your px4-300r Network Storage Array, or on another LenovoEMC network device. When you create a Personal Cloud, you gain access to your px4-300r from anywhere on the internet. You can also share with friends and family by inviting users to join your Personal Cloud.

You manage Personal Cloud users the same way you manage other users on your px4-300r, so you control the storage and content they can access through the Personal Cloud. Trusted devices can be added to your Personal Cloud to connect them through the internet as if they are on a common home network with your px4-300r.

People who join your Personal Cloud can access data, perform Copy Job operations, stream media from your px4-300r over the internet, and use remote desktop to access computers on the local network for your px4-300r. If you allow a user to join their trusted devices to the Cloud, those devices become part of the Cloud and can be accessed by other users on the Cloud.

LenovoEMC Personal Cloud Key Terms

The following are a few key terms to help get you started with a Personal Cloud:

- **LenovoEMC Personal Cloud**— This is a feature you can configure from your px4-300r device management interface that allows you to securely share storage and media capabilities with computers around the world.
- **Web Access** – You can use Personal Cloud to access your px4-300r from the web. Enter myCloudName.mylenovoemc.com in a web browser, and when prompted, enter a valid username and password for your px4-300r. You can also use the LenovoEMC Link, which is an application that runs on mobile devices, by entering the Personal Cloud name and then a valid username and password. For more information on the LenovoEMC Link, refer to its documentation.
- **My Personal Cloud** – When you are the administrator of your px4-300r, you can create a Personal Cloud through the device management console, and then invite people to join it. You create and manage the Personal Cloud using the **Personal Cloud** feature interface. The Personal Cloud that you administer is called My Personal Cloud.
- **Other Personal Cloud** – If you want to have your px4-300r join a Personal Cloud hosted on another LenovoEMC network storage device instead of administering your own, select the option for **Other Personal Cloud**. Enter the Personal Cloud name, username, and password you received when you were invited to join your px4-300r as a Trusted Device on the other Personal Cloud.
- **Joining LenovoEMC Personal Cloud as a Trusted Device** – To connect your computer or your px4-300r as a trusted device to a Personal Cloud, use the username and password given to you for that Personal Cloud. The person managing the Personal Cloud has to create you as a user on the device hosting the Personal Cloud and give you permission to add trusted devices. You can connect your px4-300r to only one Personal Cloud at any given time, so you must select between either My Personal Cloud or Other Personal Cloud.

An administrator should complete the following tasks to set up or join a Personal Cloud:

- [Creating a Personal Cloud](#)
- [Inviting People onto Your Personal Cloud](#)
- [Joining a Trusted Device to a Personal Cloud](#)

Is My Content Secure?

Your content is always secure using LenovoEMC Personal Cloud. Each user on a Personal Cloud is required to enter a valid username and password when accessing your px4-300r.

You can use your Personal Cloud to share content with the people you choose. For example, you have photos of your new baby you want to share with your sister, your brother, and your sister-in-law. To share your baby photos with these family members, create a Personal Cloud, and then invite your sister, your brother, and your sister-in-law to join your Personal Cloud.

Your px4-300r Network Storage Array provides an easy way to send email invitations and instructions to the people you select as Personal Cloud users. In this way, your content is never exposed and remains private. It is visible only to the individuals you invite to be Personal Cloud users. Content of the Personal Cloud is determined by you as the Personal Cloud owner. Refer to the help topic links below for more information on Personal Cloud.



People added to your Personal Cloud as users are not required to own a LenovoEMC network storage device or have access to your px4-300r. The process of adding someone as a Personal Cloud user grants them access to your Personal Cloud from any computer.

Creating a LenovoEMC Personal Cloud

Before you can work with your LenovoEMC Personal Cloud, you first create a Personal Cloud and configure the settings.


1. Click the **Personal Cloud** icon to open the feature page.
2. Expand the **Configure** section.
3. Click the button for **My Personal Cloud** to open the portal that lets you create your Personal Cloud.
4. After you click the My Personal Cloud button, a new website containing the portal opens. You create a Personal Cloud on this website. After you create the Personal Cloud, you return to the px4-300r device management console.
5. After your Personal Cloud is ready and connected to the internet as indicated by the status images, you can [create Shares](#), [invite people to join your Personal Cloud](#), or configure [Copy Jobs](#).



You control access to content on your Personal Cloud the same way you control access to your px4-300r by users and groups on your network. If you have content on your px4-300r that you do not want to share with members of your Personal Cloud, you should put that content in secured Shares that are not accessible to anyone invited to your Personal Cloud.

Configuring Router Port Forwarding for Personal Cloud

In most cases, your px4-300r attempts to automatically configure your router. However, if it cannot, a message displays that your router is not configured for port forwarding, and you must manually configure your router to forward a specific port to your px4-300r. Most routers refer to this as port forwarding, application access, or virtual server. It is recommended that you refer to your router's documentation for setting these values. When you set up port forwarding, you are allowing data to travel through your Personal Cloud between your px4-300r and trusted devices.

When you have selected a port value to forward for Personal Cloud, click  **Settings** on the Personal Cloud page, and enter your selected port number in the Personal Cloud settings dialog box. If you have more than one Personal Cloud, you can enter a range of port values for your Personal Clouds. The range of port values is 50500-50599. You must also port forward port 443 to enable https access to your px4-300r.

Router Port Forwarding

Some routers have a UPnP option. If you have a UPnP router, enabling this option allows the px4-300r software to automatically configure the correct forwarding ports. Otherwise, you must perform additional steps by manually enabling port forwarding on your home network router. Port forwarding allows invited users to connect remote computers or other px4-300r devices outside of your local area network (LAN) as trusted devices to the Personal Cloud on your network.



Port forwarding must be configured for both the network router on which the Personal Cloud is configured, and any remote network from which trusted devices are accessing the Personal Cloud.

The following steps are generic router settings. If you have never logged into your router before, consult the manufacturer's documentation to find specific details such as default IP address, default administrator account, and password.

1. Log in to your router by entering its IP address in the URL field on your computer's browser. If prompted, enter the router's administrator account name and password.
2. Navigate to the Port Forwarding configuration page. This is often related to Port Mapping, Application, Virtual Server, or Gaming configuration options.
3. Type in the desired application or service name. This is typically a blank or drop-down field where you can type or choose a user-specified application or service name for the port you are forwarding. Create a new entry with a value like "LenovoEMC Personal Cloud" in this field.
4. Enter a port number for the Personal Cloud service in the range 50500-50599 in both the port start and port end fields. Port number 50500 is the default. It should not be necessary to change this value, but if you do, choose the next available port; for example, 50501. If you decide to choose a port in the higher range, note that the Media Server uses the same range of ports, numbering backwards from 50599.
5. Repeat the previous step, using port 443 to enable https communication with your px4-300r.
6. Enter the IP address of the LenovoEMC network storage device that is hosting the Personal Cloud (for example, your px4-300r). The IP address displays in the system status section of the device management interface.
7. Save the changed settings.
8. Reboot the router if required.

Configuring Your LenovoEMC Personal Cloud

As a LenovoEMC Personal Cloud administrator, you can manage various settings on your Personal Cloud to ensure that it functions as efficiently as possible. Settings include specifying an email address when sending invitations. When data is traveling through the Personal Cloud, you can control the security of that information by specifying a Secure Communication level. Note that data stored on your px4-300r through the Personal Cloud is not encrypted, and using encryption can slow down communications.

Enabling Internet Access to the px4-300r

You can grant internet users, including LenovoEMC Link users, secure access to the px4-300r web interface and unrestricted access to media content on your px4-300r. LenovoEMC Link is an application that runs on mobile devices, and allows access to content on your px4-300r.

Before enabling secure access, you must first [create users](#) on your px4-300r and [set access permissions](#) to Shares. After enabling secure access, any internet users can access your px4-300r home page, and view any unsecured content (that is content in Shares you have explicitly made public by setting access permissions for Everyone). Content on secured Shares is restricted to users who have valid usernames and passwords for the px4-300r.



If you enable media sharing for any Shares on your px4-300r, media files in those Shares become available to all internet users.

Changing Personal Cloud Settings

1. In the Configure section of the Personal Cloud page, click **Settings**.
2. In the Personal Cloud Settings dialog box, configure the following:
 - **Administration Email Address** – This is the sender email address used on the email invitations.
 - **Port Number** – Your router forwards this specific port for your Personal Cloud. This value is automatically filled in, and you do not have to change it, unless you have more than one Personal Cloud on your network. Refer to [Configuring Router Port Forwarding for Personal Cloud](#) for more information.
 - **Secure Communication** – This setting controls the security of information traveling through the Personal Cloud.



You can also specify a Secure Communication level setting with LenovoEMC Storage Manager. The Secure Communication setting in the px4-300r device management console sets the minimum value. You cannot specify a setting lower than this value using LenovoEMC Storage Manager. For information on using LenovoEMC Storage Manager, refer to its online help.

- **Enable unrestricted access to media content**– This setting makes all media files in media-enabled Shares available to anyone on the internet accessing your px4-300r, even if those media files are in secured Shares. For more information on making a Share media-enabled, refer to [changing Share information](#).
3. Click **Apply** to save your changes.

Inviting People onto Your LenovoEMC Personal Cloud

When you invite people to join your LenovoEMC Personal Cloud, you are actually selecting from existing users on your px4-300r, or adding people as users on your px4-300r. In addition, you are optionally allowing them to [join a trusted device to your Personal Cloud](#). Computers are added as trusted devices through LenovoEMC Storage Manager. Refer to its online help for more information.

The invited users receive an email invitation that includes the username and password they must provide when connecting to your Personal Cloud from the LenovoEMC Storage Manager on their computer.

1. From either the Personal Cloud Quick Setup dialog box or the Personal Cloud feature page, click **Invite Users**.



You can also send an invitation to join a Personal Cloud when you are adding users to your px4-300r. Refer to [Adding Users](#) on page 37 for more information.

2. In the Invite Users dialog box, select the name of an existing user or click **Create New User** to [add a new user](#).
3. If the email address field is not already completed, enter an email address for the user.
4. Click **Apply** to send the invitation.

Joining a Trusted Device to LenovoEMC Personal Cloud

You can join your px4-300r as a trusted device on the Personal Cloud hosted on another LenovoEMC network storage device if you have been given permission by the Personal Cloud administrator.



You cannot join your trusted device to a Personal Cloud if you have not been added as a user on the Personal Cloud.

1. Click the **Personal Cloud** icon to open the feature page.
2. Select the **Other Personal Cloud** command to join another LenovoEMC Personal Cloud.
3. In the **Add Trusted Device to Personal Cloud** dialog box, enter the Personal Cloud name, username, and password you received in the email invitation.
4. Enter a descriptive name for your trusted device in the **Description** field.
5. Click **Apply**.

After applying this information, you are automatically connected to the Personal Cloud.

Managing Trusted Devices on a Personal Cloud

As administrator of a LenovoEMC Personal Cloud hosted on your px4-300r, you can manage trusted devices on your Personal Cloud. Trusted devices can be disconnected, or you can completely delete a trusted device from the Personal Cloud.


Disconnecting Trusted Devices


1. Click the **Personal Cloud** icon to open the feature page.
2. Click **My Personal Cloud**, and expand the trusted device section.
3. To disconnect a trusted device from the Personal Cloud, select the device and click the switch to **Disabled**.
4. Click **Yes** in the confirmation pop-up window.



The trusted device is not deleted and can be re-enabled at a later time.

Deleting Trusted Devices

To delete a trusted device from the Personal Cloud, click  next to the device's name. The trusted device is deleted and can only be added again by a user with trusted device privileges.

1. On the **Personal Cloud** page, expand the Trusted Devices section.
2. Click  next to the trusted device you want to remove from the Personal Cloud.
3. Confirm the deletion.

Using Copy Jobs with a LenovoEMC Personal Cloud

You can create [Copy Jobs](#) that can transfer data from one [trusted device](#) to another through the Personal Cloud. When you add a trusted device to your Personal Cloud, a Copy Jobs icon displays next to that device in the trusted device table. Clicking the Copy Jobs button opens the Copy Jobs page to help you configure a Copy Job between the LenovoEMC network storage device that is hosting the Personal Cloud and the trusted device. For more information on setting up Copy Jobs, refer to [Adding Copy Jobs](#).

Disabling or Deleting Your LenovoEMC Personal Cloud

When you disable your Personal Cloud, you eliminate access to your Personal Cloud without deleting the account information you created when you set up the Personal Cloud. Later, if you want to re-enable your Personal Cloud, you can do so without re-entering all the account information.

To completely stop the Personal Cloud and eliminate any account information with it, delete it. If you delete your Personal Cloud and later decide you want to recreate it, you must start the creation process again and re-invite all users. When you delete a Personal Cloud, you lose your ownership of its name.

To disable a Personal Cloud, open the feature page and click **Disable**.

To delete a Personal Cloud, click **Settings** and then click **Delete** in the Personal Cloud Settings dialog box.

Accessing Content Using Your LenovoEMC Personal Cloud

You can share content on your px4-300r through your Personal Cloud. You can [set access permissions to Shares](#) on your px4-300r to make content accessible to all users of your Personal Cloud, or you can restrict access to specific users or groups. Access permissions control whether users are only allowed to read files in Shares, or if they can also write (upload) files to Shares.

You can also use your Personal Cloud for remote access to content on your px4-300r from anywhere in the world. Enter the name of your Personal Cloud in a web browser, followed by ".mylenovoemc.com". For example, to access a Personal Cloud named "tomscloud1", enter the URL:

```
tomscloud1.mylenovoemc.com
```

When prompted, enter your username and password to login to the px4-300r. You will be able access all Shares on the px4-300r where you have access permissions set.

Other users on your Personal Cloud can also use the remote access feature. They must enter the URL with the name of your Personal Cloud, followed by ".mylenovoemc.com". Only users with valid usernames and passwords for the px4-300r can access the px4-300r through your Personal Cloud. Users will be able to access only the Shares where they have been explicitly granted access permissions.

Informing Users What to Do with LenovoEMC Personal Cloud

LenovoEMC Personal Cloud enables invited users to access your px4-300r from the web. They enter the Personal Cloud URL, myCloudName.mylenovoemc.com, in a web browser, using the name of your Personal Cloud in place of "myCloudName", and when prompted, enter a valid username and password for your px4-300r.

When users access your px4-300r through your Personal Cloud, they can view Shares, upload and download content, and stream content. Optionally, they can install LenovoEMC Storage Manager on their computers, and then join their computers as trusted devices to the Personal Cloud. When users join their computer as a trusted device to the Personal Cloud, they are making their machine and its files available to other users of the Personal Cloud, creating a large virtual network.

CHAPTER 13

Sharing Content Using Social Media

Sharing Content Using Social Media: Overview

If you have an account with social media services such as Facebook, Flickr, or YouTube, you can share content on your px4-300r Network Storage Array with your friends and family using one or more of these social media sites. To share your content using social media sites, create Shares called [Active Folders](#), and connect each Active Folder with a social media account. Refer to the help topic links below for more information on these procedures. When you add photos and movies to an Active Folder, those files are automatically uploaded to the social media site associated with that Active Folder. If you have photos or movies you want to share with others, this is a great way to make your content available to people who may not have access to your px4-300r.

If you have configured a Personal Cloud on your px4-300r, you can grant Personal Cloud users access to Shares and Active Folders. This is useful if you want to allow users to add files to your social media sites. For example, if your px4-300r has a Flickr Active Folder, you can grant Personal Cloud users access to that Active Folder. In this manner, when photos are added to the Flickr Active Folder, either by you or by Personal Cloud users, those photos are uploaded automatically to your Flickr account.

Note that an Active Folder can only be associated with one social media account. For example, if you want Active Folders for your Facebook and YouTube accounts, create two Active Folders, and assign one Active Folder to Facebook, and one to YouTube. Using this example, any photos you add to your Facebook Active Folder are automatically uploaded to your Facebook page, and any movies you add to your YouTube Active Folder are automatically uploaded to your YouTube page. Not only is this a fast and easy way to share content, but uploading content to your social media sites provides an additional backup of your content, as the content is stored both on your px4-300r and at your social media accounts.

Facebook

Facebook is a social network to connect with friends and family. You can configure a [Share](#) as a Facebook Active Folder so that photos and movies added to that Share are automatically uploaded to your Facebook account.

Refer to [Managing Shares](#) on page 53 for more information on managing Shares and Active Folders.



If you do not have a Facebook account, go to the Facebook website to open an account.

Configuring a Facebook Active Folder

1. Click the **Shares** icon.
2. Select a Share to use as a Facebook Active Folder, and click to expand the Active Folder section.
3. Check **Enable**.
4. Select **Facebook** from the drop-down menu.
5. Click **Configure Facebook account access** to configure your Facebook account. You will be taken to a Facebook page to configure your account. Follow the instructions provided by Facebook.
6. Check **Delete files after upload** to delete images or movies from the Share once they are transferred to your Facebook account.
7. Images can also be resized prior to upload. Check 800x600, 1024x768, or enter a custom resolution for resizing images.
8. Click **Apply** to save your changes.
Once configured, all your images in this Active Folder will upload to your Facebook account.
9. Click **View Transfer History** to see the transfer activity from this Share to your account.

Flickr

Flickr is a photo sharing network for sharing photos with friends and family. You can configure a Share as a Flickr Active Folder so that images and albums added to that Share are automatically uploaded to your Flickr account.

Refer to [Managing Shares](#) on page 53 for more information on managing Shares and Active Folders.



If you do not have a Flickr account, go to the Flickr website to open an account.

Configuring a Flickr Active Folder

1. Click the **Shares** icon.
2. Select a Share to use as a Flickr Active Folder, and click to expand the Active Folder section.
3. Check **Enable**.
4. Select **Flickr** from the drop-down menu.
5. Click **Configure Flickr account access** to configure your Flickr account. You are taken to a Flickr page to configure your account. Follow the instructions provided by Flickr.
6. Check **Delete files after upload** to delete images from the Share once they are transferred to your Flickr account.
7. Click **Apply** to save your changes.
8. Once configured, all images added to this Active Folder are uploaded to your Flickr account. Click **View Transfer History** to see the transfer activity from this Share to your account.

YouTube

YouTube is a social media site to share video content. You can configure a Share as a YouTube Active Folder so that videos added to that Share are automatically uploaded to your YouTube account.

Refer to [Managing Shares](#) on page 53 for more information on managing Shares and Active Folders.



If you do not have a YouTube account, go to the YouTube website to open an account.

Configuring a YouTube Active Folder

1. Click the **Shares** icon.
2. Select a Share to use as a YouTube Active Folder, and click to expand the Active Folder section.
3. Check **Enable**.
4. Select **YouTube** from the drop-down menu.
5. Check **Delete files after upload** to delete videos from the Share once they are transferred to your YouTube account.
6. Click **Apply** to save your changes.
7. Once configured, all videos added to this Active Folder automatically upload to your YouTube account.
8. Click **View Transfer History** to see the transfer activity from this Share to your account.

Share Content through LenovoEMC Personal Cloud

You can share your multimedia content with friends and family through a LenovoEMC Personal Cloud. Refer to the [LenovoEMC Personal Cloud](#) section for more information.

CHAPTER 14

Media Management

Media Management Overview

The px4-300r has a built-in Media Server feature. When this feature is turned on, the Media Server scans for media content in all Shares that have media sharing enabled. Media content contained in these Shares is then accessible from the px4-300r to any media player on your network, even if the Share is secured. For information on enabling media sharing, refer to [Managing Shares](#) on page 53.

Scanning for Media Content

The Media Server automatically scans for media content on a regular basis. However, you can click **Scan now** at any time to force the media server to perform an immediate scan for media content. This is especially useful after you have created new Shares with media sharing enabled and copied a large amount of media content to them.

Media Services Capabilities and Limitations

One important consideration when using the Media Server feature is that it can share media content on your px4-300r with anyone on the internet. When media sharing is enabled, internet users, including those users on mobile devices running the LenovoEMC Link, can access media content on your px4-300r.



When you enable internet access to your media content, all media content is available to any user on the internet, regardless of any security you may have applied to a media file. All your pictures, movies, and music are available to anyone accessing your px4-300r. You should be sure you want to make all your media content this accessible before enabling media sharing.


Sharing Media Content over the Internet

There are two methods for sharing media content on your px4-300r with anyone on the internet. You can enable internet access on the Media Server page. Alternatively, you can enable internet access by [configuring your LenovoEMC Personal Cloud](#).

Enabling Internet Access from the Media Server Page



You can only enable internet access from the Media Server page if you have already created and [configured a Personal Cloud](#). If a Personal Cloud is not set up, you do not see the Enable internet access option.

1. Click the **Media Server** icon to open the feature management page.
2. Click  **Settings**.
3. In the dialog box, check **Enable internet access**.
4. Click **Apply** to save your changes.
5. In the confirmation dialog box, check **Check this box to continue**.
6. Click **OK** to save your selection or click **Cancel**.


With this setting enabled, LenovoEMC Link users can access media content directly from the px4-300r. Refer to your LenovoEMC Link documentation for details.

For additional information on enabling internet access, refer to [Media Services Capabilities and Limitations](#).

Media Aggregation

If you have multiple Digital Living Network Alliance (DLNA) servers in your network that have media content, you can combine all media content into one view by enabling aggregation on your px4-300r. When you enable aggregation, all media content on DLNA servers is available for playback using a DLNA player, such as Playstation®, Windows Media Player®, or Xbox®. In addition, you can optionally copy all media content from your network servers to your px4-300r.

Enabling Media Aggregation

1. Click the **Media Server** icon to open the feature management page.
2. Click  **Settings**.
3. Check **Enable media aggregation**.
This enables aggregation for media servers already discovered in your network.
4. Choose the default aggregation setting.
The default aggregation setting sets the default value for media servers as they are added to your network.

The default aggregation settings are as follows:

- **None** – Media aggregation is off.
- **Show Common View** – This enables media aggregation and allows all media content from computers on the network to be played back by a DLNA player. All your movies, music, and pictures are linked from various computers and can be played back from one view. All aggregated media files remain on their original device, and can only be played while that device is powered on and connected to the network.
- **Copy Files** – This enables media aggregation and automatically copies all media content from computers, both networked and local, to your px4-300r. All your movies, music, and pictures from various computers can be played back from one view, and they are copied into Shares on your px4-300r. Because all media files are copied to the px4-300r, they can be played even if the original device they were on is powered off or not connected to the network.
- **Copy on Request** – This enables media aggregation but does not automatically copy all media content from computers, both networked and local, to your px4-300r. Computers on the network will have to enable media aggregation individually and then media files are copied to the px4-300r. If a computer is running the LenovoEMC Storage Manager, media aggregation is automatically enabled.



When you enable media aggregation, the media server restarts, and any media you are currently streaming stops playing. You can begin streaming your media after the media server has restarted.

Social Media Sharing

You can share media content, such as movies and pictures, using social media sites like Facebook, Flickr, or YouTube. Refer to the [Sharing Content Using Social Media](#) section for more information.

Streaming Music, Movies, and Pictures

The Media Server supports playback of videos, music and pictures from any UPnP AV (Universal Plug and Play Audio Visual) network media players, such as Playstation, Windows Media Player, or Xbox.

You can play back all your media files from your individual home computers by enabling [media aggregation](#) on your px4-300r. You can also connect USB mass storage devices (such as your iPod, mp3 player, or USB drive) to your px4-300r and directly stream files through the device, or access media files through a networked media player. Below are two examples of how to set up the following media players:

- [iTunes](#)
- [Xbox 360](#)



The procedures shown below are intended as examples. Your media player or version may operate differently. It is recommended that you refer to your media player documentation for instructions on how to add a network device.

Example: Setting up iTunes

1. Locate the source directory of your iTunes media content.
2. Drag, or copy, your existing media content to a Share that has media sharing enabled.
3. When you open the iTunes Library, iTunes will display all of the media content from the px4-300r.

Example: Setting up Xbox 360

1. Connect your Xbox 360 to your TV and to the same local network as your px4-300r.
2. Navigate to the **Media** Tab in Xbox 360 and select a media-enabled Share.
3. Select **Computer** from the options menu.
4. Click **Yes, Continue** when asked if you have downloaded and installed media sharing software on your computer, since the px4-300r device comes preconfigured with this software.
5. Select px4-300r from the list of names. You should now see all the unsecured media content on your device.

Photos

Photos Overview

Your px4-300r has multiple ways to manage your pictures.

Your px4-300r can:

- Stream pictures that are in Shares with media sharing enabled
- Display pictures on the Home Page in a slideshow
- Automatically resize pictures
- Transfer pictures from your digital camera
- Upload pictures to social media sites like Flickr or Facebook

Streaming Pictures

The px4-300r has a built-in media server that, when turned on, can scan for pictures in specific folders that have media sharing enabled. Any pictures contained in these specific folders will then be accessible to any user on your network with a media player. For information on enabling a folder as a media folder, refer to [Managing Shares](#) on page 53.

Scanning for Pictures

The Media Server automatically scans for media content on a regular basis. However, you can click **Scan now** at any time to force the media server to perform an immediate scan for pictures. This is especially useful after you have created new folders with media sharing enabled and copied a large amount of media content to them.

Creating a Slideshow on the Device Home Page

Your px4-300r can display a slideshow on its home page.

On the Home Page Settings feature page, check **Display slideshows** to display picture slideshows from folders on the px4-300r. Click **Manage slideshows** to configure any slideshows you want to display. The slideshow location can be any folder attached to the px4-300r, including a USB drive or DFS location.

Automatically Resizing Your Photos

A Photo Resize Active Folder automatically changes the size of photos in that Share to a set size. You can choose to keep the original photos added to this Share, while a resized copy is created. The resized photos are saved to a folder on the Share named by the photo size you choose, such as 800x600. To configure a Share as a Photo Resize Active Folder, access Shares from the px4-300r management console, select a Share, and expand the Active Folders section to enable and configure it.


Refer to [Managing Shares](#) on page 53 for more information on managing Shares and Active Folders.

Configuring a Photo Resize Active Folder

1. Click the **Shares** icon.
2. Select a Share to use as a Photo Resize Active Folder, and click to expand the Active Folder section.
3. Check **Enable**.
4. Select **Photo Resize** from the drop-down menu.
5. You can set a size for your pictures. Select 640x480, 800x600, 1024x768, or enter a Custom Resolution for resizing images. The resized photos are saved to a folder on the Share named by the photo size you choose, such as 800x600.
6. You can keep a copy of the original by selecting **Keep the original files after resizing**.
7. To add a watermark to your photo, select **Add a watermark to the photos**. Click the Watermark file icon to apply a watermark image to your file.
8. Click **Apply** to save your changes.
9. Once configured, all photos added to this Active Folder are resized to your settings. Click **View Content** to see the files in this Share.

Getting Pictures from Your Camera

The Picture Transfer Protocol (PTP) allows pictures to be automatically copied from a USB camera connected directly to the px4-300r. When Picture Transfer is turned on, and your camera is connected to your px4-300r, the pictures are copied to the configured destination folder.

1. Open the Picture Transfer page, click the switch on.
2. Optionally, if you want to automatically delete the pictures from your camera once they have been safely copied to your LenovoEMC storage device, check **Remove Copied Pictures From Camera** to automatically delete the pictures from your camera once they have been safely copied to your px4-300r.
3. Click  to open the Select Folder pop-up window, and select a Share as the destination for your pictures.

Music

Music Overview

If you have music files in media-sharing enabled folders on your px4-300r, those music files can be streamed by a DLNA player running on a computer on the network.

Streaming Music

The px4-300r has a built-in media server that, when turned on, scans for music in specific folders that have media sharing enabled. Any music contained in these specific folders is then accessible to any user on your network with a media player. For information on enabling a folder as a media folder, refer to [Managing Shares](#) on page 53.

Scanning for Music

The Media Server automatically scans for media content on a regular basis. However, you can click **Scan now** at any time to force the media server to perform an immediate scan for media content. This is especially useful after you have created new folders with media sharing enabled and copied a large amount of media content to them.

Videos

Video Capabilities Overview

Your px4-300r Network Storage Array has multiple ways to manage your videos.

Your px4-300r can:

- Stream movies that are in Shares with media sharing enabled
- Upload videos that are added to Shares associated with social media sites

Streaming Movies

The px4-300r Network Storage Array has a built-in media server that, when turned on, scans for movies in specific folders that have media sharing enabled. Any movies contained in these specific folders are accessible to any user on your network with a media player. For information on enabling a folder as a media folder, refer to [Managing Shares](#) on page 53.

Scanning for Movies

The Media Server automatically scans for media content on a regular basis. However, you can click **Scan now** at any time to force the media server to perform an immediate scan for movies. This is especially useful after you have created new folders with media sharing enabled and copied a large amount of media content to them.

CHAPTER 15

Adding Applications to Your px4-300r Network Storage Array

Application Overview

You can install supported applications on your px4-300r using the Application Manager page. For each application installed you may have the option to uninstall, start, and stop the application.

Application Installation

Certain applications on your px4-300r must be installed before you can use them. When you click on an uninstalled application in the px4-300r management console, you open the feature page of the application. To install the application, click the install link. The application is downloaded to the px4-300r, and you can start the application from the Application Manager page.

You can also download applications from www.LifeLineApps.com.



Some applications require data storage on the px4-300r network device. Installing one of these applications automatically creates the Application Data share on the px4-300r device. Do not modify or delete this share.



Application Manager

The Application Manager page allows you to add applications to your px4-300r from an installation file located on your computer. For each application installed you may have the option to uninstall, start, and stop the application. This page shows the applications which came preinstalled with your px4-300r; as well as applications that you have manually installed.



Only valid applications built using the LenovoEMC SDK can be installed on your px4-300r.

Starting or stopping an application

When available, click  in the Action column to stop an application. Click  to start it again.

Adding applications

1. Click the **Add application** link. The Add application window displays.
2. Enter the path and name of the application file, or click **Browse**, and select the application file located on your computer.
3. Click **Upload** to install the application.





Removing applications

When available, click  in the Action column to uninstall an application.

Software Updates

The Software Updates page identifies the px4-300r software status and provides the ability to update the software for the px4-300r.





Auto-update process: installing a device software update

1. In the table listing the current software installed on your px4-300r, click  in the Action column to check for updates.
2. The Status column will state whether the software is up to date or if an update is available. To copy an update file to your px4-300r, click . The software update file is downloaded directly to your px4-300r.
3. If multiple updates are ready, you may install all the updates at the same time. Click  **Apply all pending updates** to install the available updates. The software updates are applied to your px4-300r.
4. Once the software is installed, the px4-300r will reboot. If you are applying multiple updates, you only need to reboot once. Do not power down the px4-300r during this time.
5. If you want to remove the update without applying changes, click  in the Action column.



Do not shut down the px4-300r during the update process as this can damage the px4-300r. The px4-300r will be temporarily inaccessible during the software update. Be sure no critical files are being accessed.

Manual update process: installing a device software update

1. In the table listing the current software installed on your px4-300r, click  in the Action column to check for updates.
2. If an update is available, the Status column will state that a software update is available with a link. Download the update file to your local computer.
3. To retrieve the update, click  **Add Software**.
4. In the **Add Software** pop-up window, if an update is available, there will be a link to download the appropriate update for your px4-300r. Click the link, follow the instructions on the download site page, and download the software update to your local computer.
Once downloaded, click **Browse** to select the update, and then click **Upload** to continue.
5. When the update is uploaded to the px4-300r, the Status column will say **Ready to apply**.
6. Click  **Apply all pending updates** to apply the update or updates. The software updates will be applied to your px4-300r. If you want to remove the update without applying changes, click  in the Action column.

The px4-300r restarts once the software is installed. You should not power down the px4-300r during the installation process as this can damage the px4-300r. If multiple updates are ready, all of them will be applied, requiring only one reboot.



The px4-300r will be temporarily inaccessible during the software update. Be sure no critical files are being accessed.

CHAPTER 16

Backing up and Recovering Your px4-300r Network Storage Array Settings


Backing Up Your px4-300r Network Storage Array Settings

The Configuration Backup and Restore page allows you to back up and restore system configuration information. Backing up a configuration saves various system properties, including users, groups, device identification, and Share names and permissions. Configuration information is saved to a file, and you can save as many versions of the file as you want. After backing up the configuration, you can restore it to your px4-300r at any time. You can also apply the configuration backup to other px4-300r devices, effectively using the configuration as a template.




Configuration Backup and Restore does not back up or restore any data files on your px4-300r.

Backing up Device Configuration

1. On the Configuration Backup and Restore page, click  **Back up configuration** to select a name and location for your configuration backup.
2. Save the configuration file to an external device, such as your computer or a USB drive. You can save as many configuration backups as you want.

Restoring a Configuration Backup

1. On the Configuration Backup and Restore page, click  **Restore configuration** to select a saved configuration backup.
2. In the Restore Configuration dialog box, click **Browse** to locate a previously saved configuration backup stored on your computer or USB device.
3. Select one of the following options:
 - **Restore settings** – overwrites any existing settings, such as device identification and Share names. When you select this option, existing data on the px4-300r is not deleted, and the configuration restore operation starts automatically after you click Apply in the Restore Configuration dialog box.
 - **Restore settings and drive configuration** – deletes all data, users, and settings from the target px4-300r. If you select this option, a confirmation dialog box displays and informs you that restoring the configuration will delete all data and overwrite any existing users or settings on the target px4-300r. Check **Check this box to continue** to confirm this dialog box or click **Cancel** to stop the configuration restore process.
4. Click **Apply** to save your changes. After you click Apply, the restore process starts.
5. If your source px4-300r had Active Directory enabled, you are prompted to enter the administrator name and password of an account that has the rights to join the domain.
6. Click **OK**.

CHAPTER 17

Hardware Management

Energy Saving

The Energy Saving feature provides power settings for the px4-300r.

Power Down Drives

Click the **Power Down Drives** drop-down menu to select how much idle time should be allowed to elapse before the px4-300r powers down the drives. Drives automatically power back up when the px4-300r accesses them. You may notice a slight delay when the drives are accessed.

Brightness

To adjust the brightness of the lights on the px4-300r, set the **Indicator Brightness** to High, Medium, or Low.

Wake On LAN

Wake On LAN powers on your px4-300r when a specific signal is sent over the network. Additional software may be required to send the Wake On LAN signal to your device.

1. Check the **Wake On LAN** checkbox to enable Wake On LAN.
2. Click **Apply** to save your changes.

Creating a Power Schedule

You can create a power schedule for your px4-300r. This allows you to set daily times to automatically power off and/or power on the device.

1. Check the box next to **Enable device power schedule**.
2. Check the boxes for **Power Off** and/or **Power On**.
3. Set the power schedule time in both hours and minutes (HH:MM), and specify AM or PM.
4. Click **Apply** to save your changes.

Factory Reset

Factory Reset returns the px4-300r to its original state. This feature is useful if you give your px4-300r to someone else.

Factory Reset provides two options for returning your px4-300r to its original state:

- **Quickly delete all data** – permanently deletes all record of existing or deleted data, users, and passwords.
- **Securely delete all data** – this option takes significantly longer, but provides an added security benefit by overwriting all drives with random data in addition to permanently erasing all data on the drives to prevent recovery of existing or deleted data, users, and passwords. The secure delete operation renders all data irrecoverable.



You can use the factory reset feature only to erase the drives internal to the px4-300r. You cannot use this feature to reset any external storage devices that may be connected.

1. Click the **Factory Reset** icon to open the management interface.
2. Choose one of the following options:
 - Quickly delete all data
 - Securely delete all data
3. From the **After Reset** drop-down menu, choose to **Restart** or **Power off** the px4-300r after the factory reset completes.
4. Click **Apply**.
5. In the pop-up confirmation, click **Yes** to perform the factory reset. After the factory reset completes, the px4-300r powers down or restarts depending on your selection.
6. Device Setup will launch automatically when the px4-300r restarts, so you can configure basic settings.



When you quickly delete or securely delete all data on your px4-300r, any installed applications, as listed on the [Application Manager](#) page, are also deleted. Go to www.lifelineapps.com to download and reinstall your applications. In addition, you should visit the LenovoEMC support web site for specific information on reinstalling applications that came preloaded with your px4-300r.

UPS Management

The LenovoEMC UPS Management page allows you to monitor the status of an attached Uninterruptible Power Supply.

If your px4-300r is connected to a UPS battery backup unit, it is listed on this page. The battery status of the backup unit is also indicated, displaying how much of a charge is left in the battery. To monitor the battery status of your UPS unit, connect your px4-300r to it with a USB cable.

If the px4-300r is running from the UPS battery, it automatically shuts down to preserve data as the battery charge gets low.

Troubleshooting Routers

If you encounter a problem while connecting or using your px4-300r, check the topics listed below for possible solutions.

If you have properly set port forwarding on your router and remote access still does not work, you may have multiple routers on your network. In this situation, you will most likely have two NAT (Network Address Translation) firewalls.

1. One of the easiest ways to identify this issue is to log in to the router to which the px4-300r is connected.
2. Once you have logged in, go to the page that shows the router's WAN IP address, usually Status or Network Info.
3. If the WAN IP address begins with 192.168, 10, or 172, you may have a NAT Firewall between the router and internet connection.

There are several options for resolving double NAT situations. The sections below explore the pros and cons of each resolution:



These instructions will refer to the router that is connected directly to the internet as the Primary Router. The cascaded router or router to which your px4-300r is connected is referred to as the Secondary Router.

- Use the primary router's DMZ
- Port forward the primary router to the secondary router
- Put the secondary router in bridging mode
- Put the primary router in bridging mode

Enabling the DMZ

Most routers have a feature called DMZ or Default Server. DMZ stands for Demilitarized Zone, Data Management Zone, Demarcation Done, or Perimeter Network. The DMZ allows you to enter an IP address that will exist outside the router's NAT Firewall.

This is the easiest way to configure your network to handle double NAT situations; however, it is dependent upon DMZ functionality within your primary router.

To enable the DMZ:

1. Log in to the primary router.
2. Navigate to the settings page for DMZ or Default Server. Refer to the documentation that came with your router for information on where this feature is found.
3. Enter the secondary router's IP address.
4. Save your settings.

Your secondary router is no longer behind your primary router's firewall. If port forwarding is correctly configured, remote access should now be working properly. Moving your secondary router into the DMZ should not have any effect on the security of the network, since it is still protected by the secondary router's firewall.

Configuring Port Forwarding on Double NAT Networks

If for some reason the network configuration cannot be changed and your setup requires the double NAT, you must perform the port forwarding steps twice. On the primary router, set the port forwarding to the cascaded router's external IP address. On the cascaded router, set the port forwarding to the px4-300r's IP address.

Bridging the Secondary Router

Make sure that the primary router (usually the one connected to or acting as the DSL/Cable modem) is the only one with DHCP (Dynamic Host Configuration Protocol) and NAT (Network Address Translation) enabled. The secondary should be changed to bridging mode. Ensure that the secondary router connects to the primary router using a standard port rather than the port labeled Uplink or internet. This turns your secondary router into a switch; however, you can still enable its Wireless Access Point if so equipped.

Refer to the documentation that came with your router for configuration information and settings.

Bridging the Primary Router

If none of the above options are available, you must enable transparent bridging on your primary router. This may require contacting your ISP (Internet Service Provider) to configure the DSL or Cable Modem/NAT into bridge mode, which then disables the first NAT/Firewall. After this first firewall in the modem is disabled, the secondary router handles all the network traffic, Port Forwarding, and allows Remote Access to work.



You should not attempt bridging without help from the ISP. If bridge mode is attempted by the customer and not configured properly, it can render the customer's internet connection inoperable. Primary router bridging may also require special configuration information and settings on the secondary router.

If you configured your px4-300r using DHCP, you may not be able to reconnect to it via Remote Access after a reboot. DHCP automatically receives an IP address from the server whenever the px4-300r restarts. This is a very simple way to configure the px4-300r but can cause problems with your router's port forwarding settings. The router does not dynamically update port forwarding settings and cannot port forward to your px4-300r if its IP address changes.

To resolve this problem, try one of the following processes:

- Increase the length of the DHCP lease: Your router attempts to remember all DHCP clients and assigns them the same IP address every time they request an IP address; however, the router forgets clients if they do not request an IP address for a certain amount of time. Your router has a setting for the duration of the validity of the DHCP lease. If your network requires DHCP, this may be a good solution; however, it is not always guaranteed to work. Occasionally updating your router's port forwarding settings may be required.
- Use Static DHCP: Some routers allow you to assign Static IP addresses through the DHCP system based on the MAC address of the device. This ensures that the px4-300r always gets the same IP address, and your port forwarding settings are always correct. Static DHCP allows you to leave your px4-300r in DHCP mode. Refer to your router's documentation for more information on configuring DHCP settings.
- Use a Manual IP Address: Changing the Manual IP address reduces the reliance of your px4-300r on the DHCP server; however, you must perform additional configuration for it to work properly.
 1. Log in to your router and write down the DHCP range it is using.

2. Refer to your router's documentation for more information on configuring DHCP settings.
3. Navigate to the IP address settings interface page on your px4-300r . For more information, check the Network Settings section of this manual.
4. Enter a new IP address that is outside of your router's DHCP range. For example, if your router is distributing IP addresses in the range of 192.168.14.2 through 192.168.14.50, you must assign the px4-300r a number between 192.168.14.51 and 192.168.14.255. Make sure you are assigning the px4-300r an IP address that is not in use by another device.
5. Enter a subnet mask. The subnet mask describes the size of your network. For most networks this is 255.255.255.0 which allows for 256 network devices. If you are on a larger network or are using the self-assigned APIPA range (169.254.x.x), you must use a 255.255.0.0 or larger subnet mask.
6. For best results, enter the IP address(es) for your DNS Server(s).
7. If necessary, enter the IP address(es) for your WINS server(s).
8. Enter a gateway address. In most cases, this is the IP address of your router.
9. If necessary, update your router's port forwarding information with the new static DHCP IP address.

CHAPTER 18

Additional Support

How to Get Help

LenovoEMC is committed to providing excellent customer support. To meet this goal, Lenovo Customer Support offers a variety of support options designed to meet the needs of a wide range of users. For complete information on the support options available for your product, visit the web support site at <http://support.lenovoemc.com>.

Here's just some of what is available on LenovoEMC's award-winning web support site, 24 hours a day, 7 days a week:

- Answers to frequently asked questions (FAQs)
- Online help pages with troubleshooting or basic how to information
- Up-to-date LenovoEMC software
- Advanced online support options, such as 1-on-1 live chat and email
- Electronic copies of product manuals
- Information on telephone support options
- Information on advanced technical service options, such as data recovery
- Warranty information and product return instructions

Support options available may vary depending on your region and language of choice. LenovoEMC's specific customer support policies (including fees for services) and procedures change as technology and market conditions dictate. To obtain information about LenovoEMC's current policies, select the **Support Policy** link from the top banner on the web support site or write to:

LenovoEMC Customer Service
4059 South 1900 West
Roy, UT 84067, USA

Support

The Support feature opens the LenovoEMC web site where you can get more information about your px4-300r. The Support page provides access to content for learning more about using and supporting your px4-300r.

Refer to the LenovoEMC Support site for more information.

CHAPTER 19

Legal

Open Source

The software included in this product contains copyrighted software that is licensed under open source agreements. Components of this software covered under GPL or other open source licenses are fully documented as to license and redistribution requirements in the ReadMe file available with the source code. The corresponding source code package is available for download from the LenovoEMC web site at <http://support.lenovoemc.com>. To locate the download page for open source code, select your network storage product and your operating system. Scroll down the page to the search field and enter “open source”. In addition, you can also obtain a copy of the applicable open source code on CD by sending a money order or check for \$10 (USD) to:

LenovoEMC, Ltd. • ATTN: Source Code • 4059 South 1900 West • Roy, UT 84067 USA

Please include the model name for your network storage product with the request.

Warranty Information

Limited Warranty Notice

Lenovo Network Storage products are covered by the terms of the Lenovo Limited Warranty, version L505-0010-02 08/2011. Read the Lenovo Limited Warranty (LLW) at http://www.lenovo.com/warranty/llw_02/. You can view the LLW in a number of languages from this Web site. If you cannot view the LLW from the Web site, contact your local Lenovo office or reseller to obtain a printed version of the LLW.

Warranty Period

The warranty period for px4-300r Network Storage Array products is 3 years for product purchased in all regions.

Applicable Types of Warranty Service (as described in the Lenovo Limited Warranty):

1. Customer Replaceable Unit ("CRU") Service
7. Product Exchange Service

For network storage products, coverage for product exchange transportation may differ by region. For additional information on this coverage, please contact a local Lenovo service provider.

For a full explanation of the types of warranty service, refer to the full warranty available at http://www.lenovo.com/warranty/llw_02/.

NOTE: Lenovo Network Storage products are manufactured solely to standard commercial grade levels of reliability and are not intended for use in any systems that require the products to conform to the higher grades of reliability, such as critical safety systems, life-support systems, medical devices, nuclear facilities, military devices, satellites, or aviation equipment. Lenovo shall not be liable for any damages incurred if Lenovo products are used in such capacities, and no warranty shall apply.

Limited Warranty for Iomega Products

Iomega network storage products are covered by a limited 3 year warranty. Iomega warranties are now serviced by Lenovo Customer Support. See the LenovoEMC web support site at <http://support.lenovoemc.com> for complete warranty terms and conditions.

Regulatory Information

This topic provides regulatory information for various countries.

Manufacturer/Responsible Party

LenovoEMC, Ltd., 4059 South 1900 West, Roy, UT 84067

EU Representative

Lenovo, Einsteinova 21, 851 01 Bratislava, Slovakia

Federal Communication Commission Interference Statement

This equipment complies with Part 15 of the FCC Rules. Operation is subject to the following conditions:

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

NOTE: This equipment has been tested and found to comply with the limits for a Class A 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 instructions, may cause harmful interference to 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, the user is 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 receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.



Lenovo is not responsible for any radio or television interference caused by using other than specified or recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

Canadian Verification

This Class A digital apparatus complies with Canadian ICES-003.

European Union conformity

Lenovo declares that this network storage product conforms to all applicable European Directives and Standards, including by way of example, 2004/108/EC and 2006/95/EC.

The Declaration of Conformity is available at www.lenovo.com/social_responsibility/us/en/ec_doc_servers.html

Important WEEE Information



The WEEE marking on Lenovo products applies to countries with WEEE and e-waste regulations (for example, European Directive 2002/96/EC, India E-Waste Management & Handling Rules, 2011). Appliances are labeled in accordance with local regulations concerning waste electrical and electronic equipment (WEEE). These regulations determine the framework for the return and recycling of used appliances as applicable within each geography. This label is applied to various products to indicate that the product is not to be thrown away, but rather put in the established collective systems for reclaiming these end of life products.

Users of electrical and electronic equipment (EEE) with the WEEE marking must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to them for the return, recycle, and recovery of WEEE and to minimize any potential effects of EEE on the environment and human health due to the presence of hazardous substances. For additional WEEE information go to: www.lenovo.com/social_responsibility/us/en/product_recycling_program.html

European Union RoHS

Lenovo products sold in the European Union, on or after 3 January 2013 meet the requirements of Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment ("RoHS recast" or "RoHS 2").

For more information about Lenovo progress on RoHS, go to:

www.lenovo.com/social_responsibility/us/en/RoHS_Communication.pdf

India RoHS

RoHS compliant as per E-Waste (Management & Handling) Rules, 2011.

California Perchlorate Information

This product contains a manganese dioxide lithium coin cell battery which may contain perchlorate material. Special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate.

Polyvinyl Chloride (PVC) Cable and Cord Notice

WARNING: Handling the cord on this product or cords associated with accessories sold with this product will expose you to lead, a chemical known to the State of California to cause cancer, and birth defects or other reproductive harm. Wash hands after handling.

Recycling and environmental information

Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. For information on recycling Lenovo and LenovoEMC products, go to: www.lenovo.com/social_responsibility/us/en/product_recycling_program.html

Dispose of the coin cell lithium battery as required by local ordinances or regulations.

Export classification notice

This product is subject to the United States Export Administration Regulations (EAR) and has an Export Classification Control Number (ECCN) of 5A992.c It can be re-exported except to any of the embargoed countries in the EAR E1 country list.

Copyright and Trademark Information

© 2014 LenovoEMC, Ltd. All rights reserved.

Lenovo and the Lenovo logo are registered trademarks of Lenovo in the United States, other countries, or both. The EMC logo is a registered trademark of EMC Corporation in the United States and/or other countries. LenovoEMC and LifeLine are registered trademarks or trademarks of LenovoEMC, Ltd. in the United States, other countries, or both. Windows is a trademark of the Microsoft group of companies. Mac is a trademark of Apple Inc., registered in the United States and other countries. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. Certain other product names, brand names, and company names may be trademarks or designations of their respective owners.