

# CONFIGURING ACTIVE DIRECTORY IN LIFELINE

## CONTENTS

Introduction	1
Audience	1
Terminology	1
Test Environment	2
Joining a Lenovo network storage device to an AD domain	3
Importing Domain Users and Groups	6
Managing Local and Active Directory Users (Hybrid Authentication)	8
Best Practices	9
Frequently Asked Questions	12



## INTRODUCTION

Active Directory (AD) is a technology created by Microsoft to provide a variety of network services, including LDAP directory access, Kerberos authentication, DNS-based naming and network information, and information security for user access to networked resources. Active Directory also allows administrators to assign policies, deploy software, and apply critical updates in Windows environments. Active Directory was first released with Windows 2000 Server edition, and revised to extend functionality and improve administration in Windows Server 2003. Additional improvements were made in Windows Server 2003 R2. In Windows Server 2008 and Windows Server 2008 R2, AD was further refined and renamed Active Directory Domain Services.

The Active Directory framework that holds all objects can be viewed at different levels. At the top of the structure is the forest, a collection of every object and its attributes and rules. A forest can contain trees, and a tree is a collection of one or more domains. All Lenovo® network storage products support both Active Directory domain mode and peer-to-peer Windows workgroup mode for Common Internet File System (CIFS) file sharing.

A Lenovo network storage device offers great reliability, ease of use, and ease of management that are designed specifically for the needs of Small Businesses (SMBs) and Remote Office/Branch Office (ROBOs). The Active Directory support enables the device to be deployed in a domain infrastructure, regardless of the size of the domain and the location of the domain controller (DC). After joining the network storage device to an AD domain, users can take advantage of the many AD benefits, such as centralized user account management and authentication for storage administration.

This paper describes the Active Directory support and integration on Lenovo network storage, using a Lenovo EMC px6-300d network storage device as an example. Some instructions and procedures are presented to illustrate common administrative tasks, including joining a storage device to AD, managing domain users and groups, and granting device administrator permission to a domain user. An FAQ about the AD support and integration is included at the end of the paper.

## AUDIENCE

Information contained in this paper is intended for Lenovo customers, partners, and service personnel involved in planning, deploying, or administering a Lenovo network storage device in an Active Directory environment.

## TERMINOLOGY

**Active Directory (AD):** a technology created by Microsoft to provide a variety of network services including LDAP directory access, Kerberos authentication, DNS-based naming and network information, and information security for user access to networked resources. Active Directory also allows administrators to assign policies, deploy software, and apply critical updates in Windows environments.



**Lightweight Directory Access Protocol (LDAP):** an application protocol for querying and modifying data using directory services running over TCP/IP.

**Domain:** a logical group of computers that share a central directory database that contains the user accounts and security information for the resources in the domain.

**Organizational Unit (OU):** an AD container into which users, groups, computers, and other organizational units are placed for logical organization of domain objects. An OU cannot contain objects from other domains.

**Domain Controller (DC):** a server that manages all security-related aspects between user and domain interactions and responds to security authentication requests within a Windows domain.

**Server Message Block (SMB):** an application layer network protocol that was later renamed to CIFS by Microsoft.

**Common Internet File System (CIFS):** A distributed file system providing transparent access to remote file systems. Whether you are a small business without dedicated IT resources, or a medium-sized business with a small IT staff that is already stretched thin, continuously managing your corporate network can be a difficult, expensive proposition. For businesses with multiple sites, the task is even more daunting, since the equipment is typically physically separated from those who are required to manage it effectively.

**Samba:** a free software re-implementation of the SMB/CIFS networking protocol. It runs mostly on UNIX and Unix-like operating systems, such as Linux, to provide file and print services for Microsoft Windows clients and can integrate with Active Directory as part of a domain.

**Windows File Sharing:** the practice of distributing or providing access to files using the CIFS protocol.

**Domain Name System (DNS):** a hierarchical naming system for resources connected to the Internet or a local network. It associates various information with domain names assigned to each of the participants.

**Folder:** on a Lenovo network storage device, a folder is a file system directory that can be accessed by hosts using file sharing protocols, including NFS and CIFS. In addition to the IT resource constraints, the hardware and software required to achieve and maintain a highly available infrastructure can easily cost hundreds of thousands of dollars well out of reach for small-and medium-sized businesses.

### TEST ENVIRONMENT

The Active Directory configuration for this white paper is performed with a Lenovo EMC px6-300d. The following Active Directory domain infrastructure was used:

- Domain name: MIXED2K8.COM



- Preferred Server IP: 172.30.2.20

### JOINING A LENOVO NETWORK STORAGE DEVICE TO AN AD DOMAIN

When you join your Lenovo network storage device to your existing Active Directory user organization, your network storage device can work in a high availability environment, which means it can work with multiple AD servers, should one server fail or go offline.

#### Configuring DNS Information

A DNS server is required for the Lenovo network storage device to join a domain and function correctly in a domain mode. Depending on your network, you may have to manually add your storage device to your DNS server. Or your domain controller may also be your DHCP and DNS server, in which case you don't have to change your network settings, and your device has configured the DNS server automatically. Contact your AD system administrator to learn how your network is configured.

To manually configure the DNS server on your storage device, perform the following procedure:

1. Access the Network feature page on your Lenovo network storage device.
2. On the Network page, click Modify network settings.
3. In the Network Settings box, uncheck "Automatically configure DNS, WINS, and all IP addresses".
4. Enter the IP address of the DNS Server in the text box and click Apply.

In this example, the IP address of the DNS server is 172.30.2.19.

**Network Settings**

Configure network settings that apply to all network interfaces. [Overview](#)

☒ Automatically configure DNS, WINS, and all IP addresses (DHCP)

DNS Servers:

WINS Servers:

Bonding Mode:  ▼

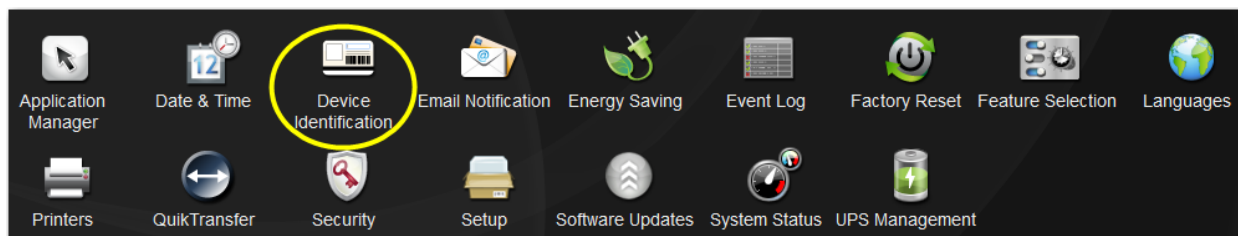
☐ Use proxy settings

#### Configuring AD Domain Information

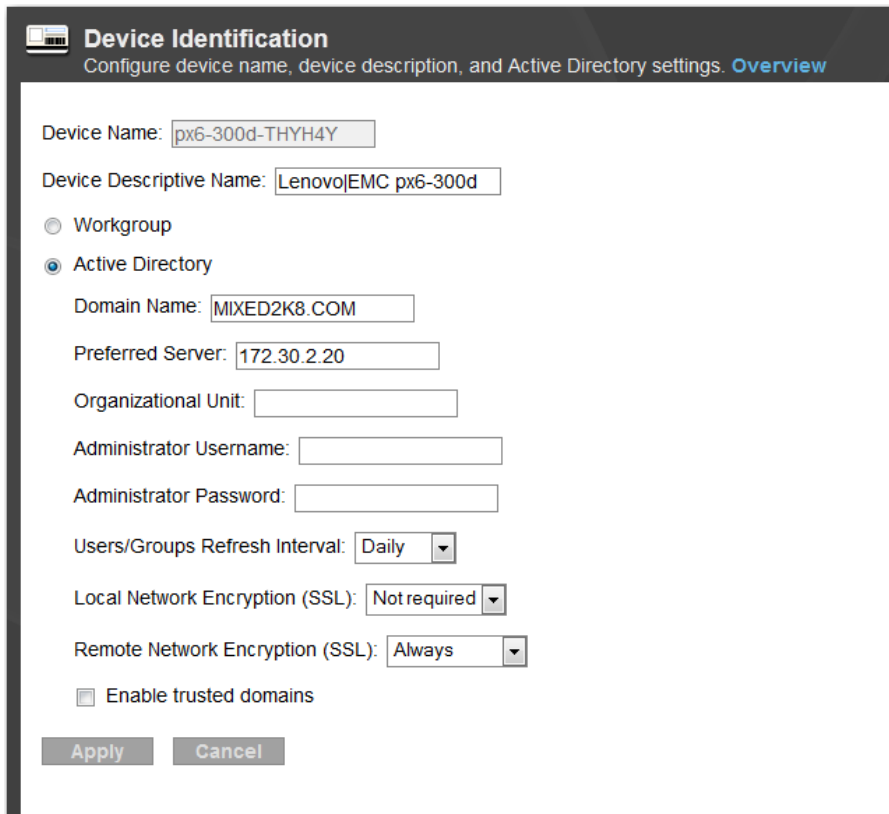


Currently Lenovo network storage devices can join and function in a Windows NT domain, Windows Server 2000 domain, Windows Server 2003 domain, Windows Server 2003 R2 domain, Windows Server 2008 domain, and Windows Server 2008 R2 domain.

1. Access the Device Identification feature in your storage device's management console.



2. On the Device Identification page, select **Active Directory**.
3. Enter **Domain Name** and **Preferred Server** information, MIXED2K8.COM and 172.30.2.20, respectively, in this example.
4. Optionally enter **Organizational Unit** information to place the network storage device as part of a domain OU if desired.
5. You must use a domain account that has permission to join computers into the domain. Enter the **Administrator Username** and **Administrator Password** for the domain join operation.
6. Choose how often the network storage device should refresh users and groups from the domain controller. By default, it is **Daily**.
7. Optionally set **Local Network Encryption**. By default, it is not required.
8. Optionally set **Remote Network Encryption**. By default, it is always set.
9. Optionally check **Enable trusted domains**. This allows your storage device to access other trusted domains.



**Device Identification**  
Configure device name, device description, and Active Directory settings. [Overview](#)

Device Name:

Device Descriptive Name:

☐ Workgroup

☒ Active Directory

Domain Name:

Preferred Server:

Organizational Unit:

Administrator Username:

Administrator Password:

Users/Groups Refresh Interval:

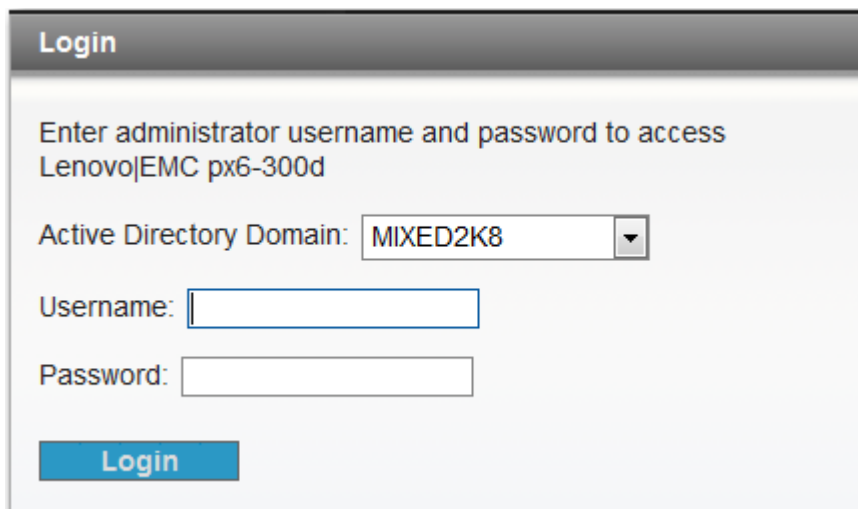
Local Network Encryption (SSL):

Remote Network Encryption (SSL):

☐ Enable trusted domains

10. Click **Apply** to join the storage device into the domain. This operation will take awhile to complete. After it completes successfully, your storage device automatically redirects to the login page.

11. Log in to your storage device using the administrator credentials you entered in step 5.



**Login**

Enter administrator username and password to access  
Lenovo|EMC px6-300d

Active Directory Domain:

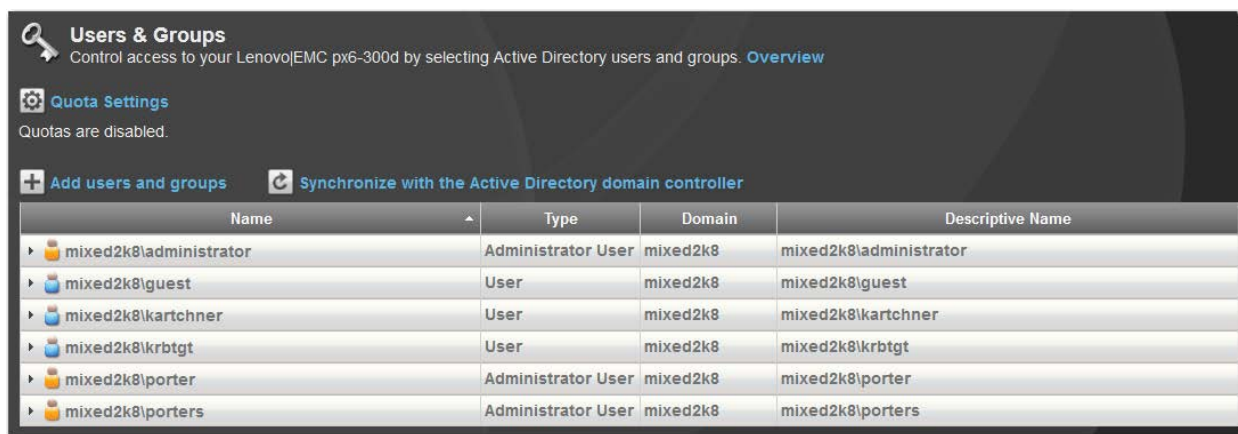
Username:

Password:

## IMPORTING DOMAIN USERS AND GROUPS

You can import domain users and groups onto the Lenovo network storage device. Only the users and groups that have been imported can be granted permissions to shared storage and log in through the management console.

1. Click the **Users & Groups** feature in the device console. All users and groups that have been imported onto the network storage device are listed here.



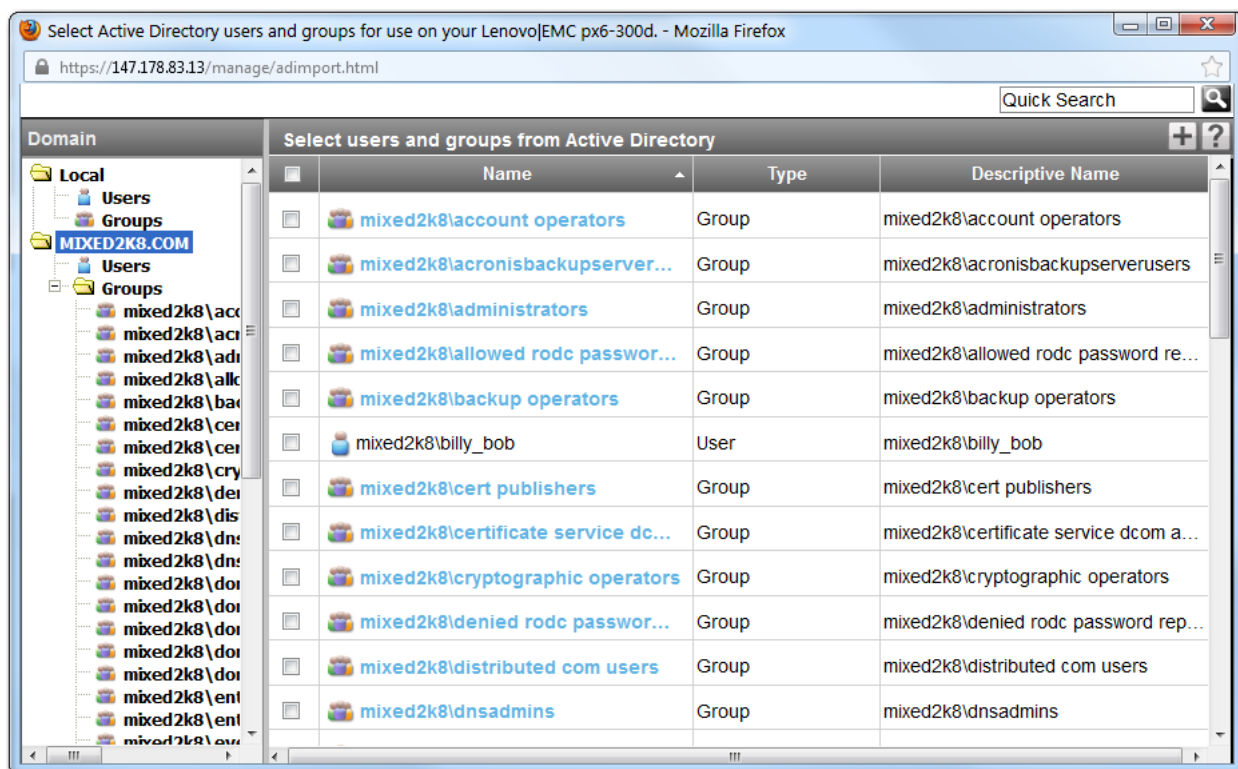
2. Click the **Synchronize with the Active Directory domain controller** link to synchronize domain users and groups with the DC. Wait until the refresh finishes before performing any user/group related operations.

**Note:** the Synchronize operation does not import new or additional domain users and groups automatically. Follow step 3 to import new or additional users and groups.

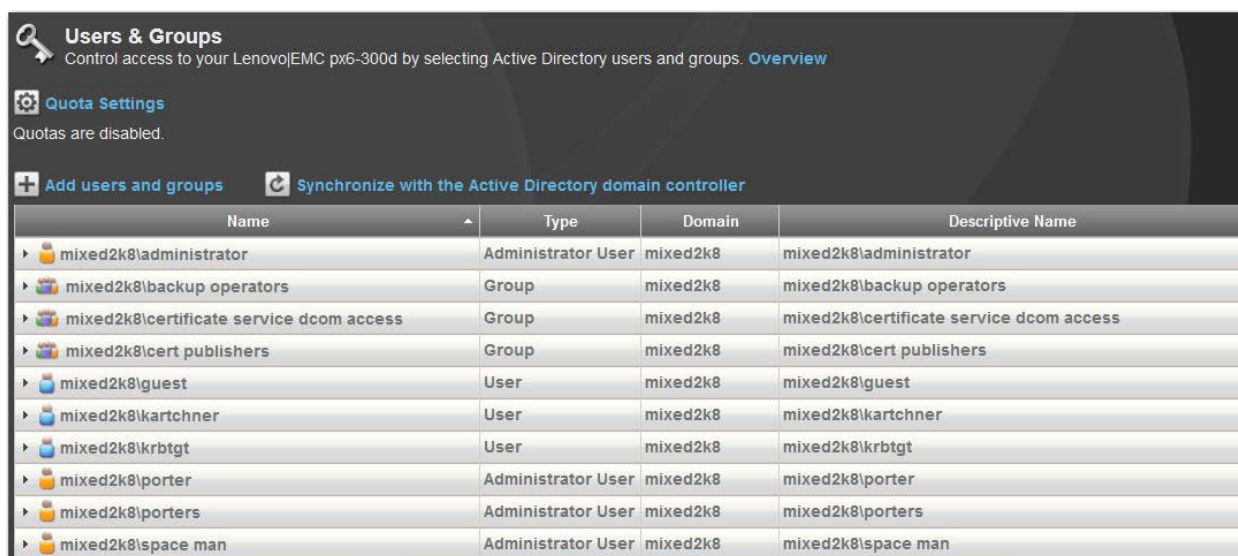
3. Click **Add users and groups** to import domain users and groups. All the domain users and groups that have not already been imported to the device are listed in this page.

**Note:** this GUI page only displays up to 3,000 users and groups. If there are more than 3,000 users and groups, you could click the **Find** link to search for a user or group that you want to import but do not see in the list.





4. Check the users and groups that you want to add to the px6-300d device and click the plus button. These selected users and groups are imported onto the device.



## Deleting Users and Groups

To delete an imported user or group from the network storage device:

1. To delete an existing user or group, expand the user or group name.
2. In the Information section, click **Delete**.



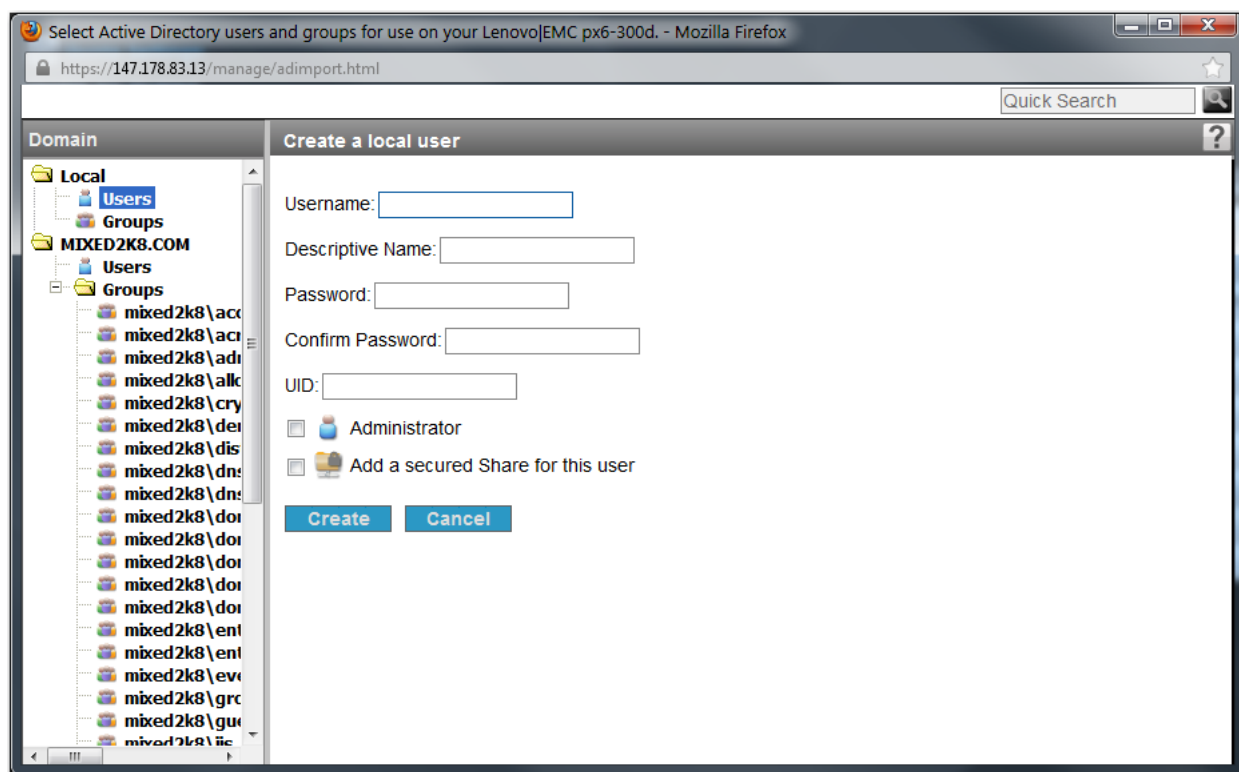
**Note:** Deleting a user or group does not delete any Shares to which the user or group has access. Click the checkbox if you want to delete all Shares that only this user can access.

3. In the confirmation pop-up window, click **Yes**.
4. If you do not wish to delete a user or group, click **No** to return to the Users & Groups page.

### MANAGING LOCAL AND ACTIVE DIRECTORY USERS (HYBRID AUTHENTICATION)

After you have enabled Active Directory and added AD users and groups, you may want users and groups that are local to the storage device. You can configure your Lenovo network storage device 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 in to and manage the storage device. This allows hybrid authentication on your storage device and, if desired, you can switch between AD mode and Workgroup mode.

1. Access the Users & Groups page.
2. On the Users & Groups page, 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 users to any local groups you create.
4. Enter the necessary credentials for the user or the group name, and click **Create**.



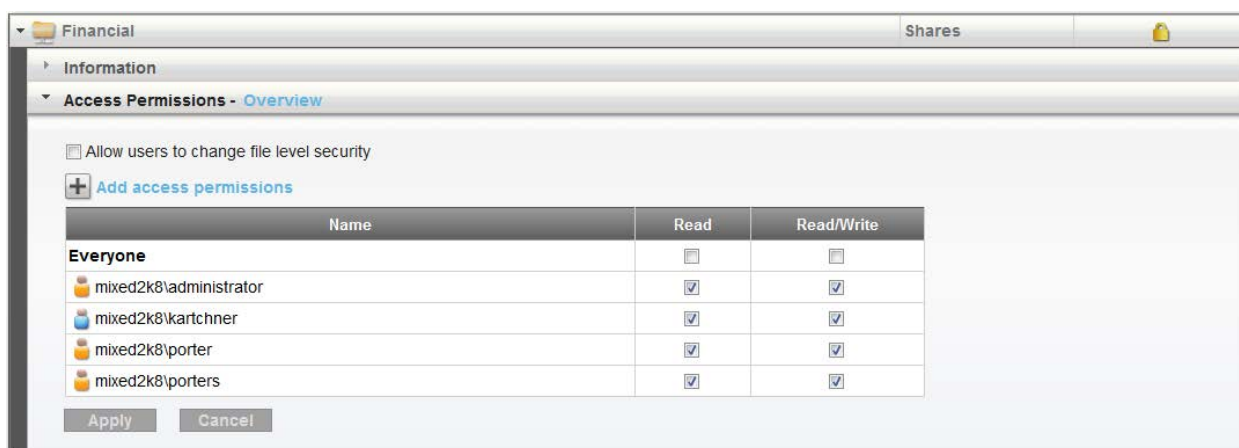
## BEST PRACTICES

The following are best practices you should use when you deploy Active Directory in your system environment.

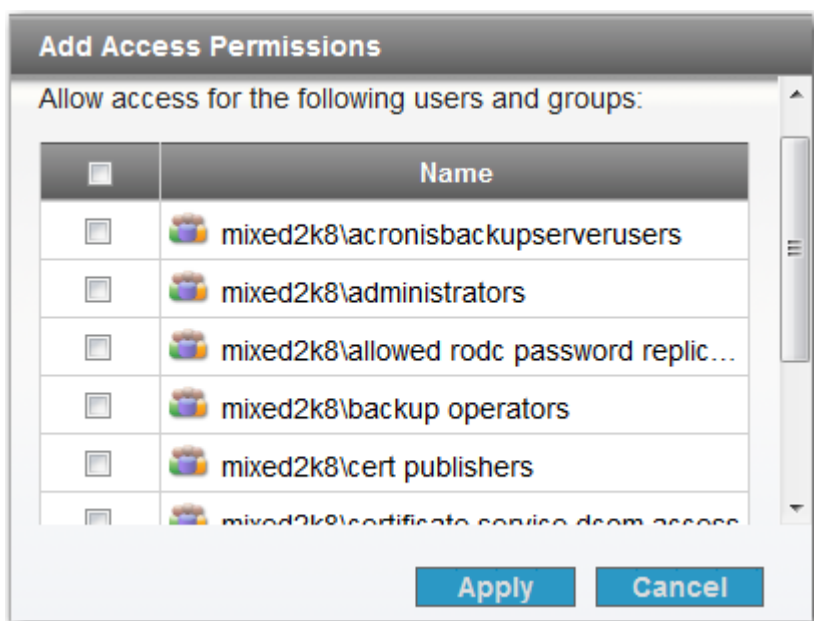
### Creating Secured Shares in AD Mode

To accelerate the progress of adding a large number of secured Shares in AD mode, the following practices are recommended:

- Create Shares first and then import users from the domain
  - Aggregate users in groups and grant access control to the groups if a large number of users need access to the Shares
1. Access the Shares page to create a new Share. Set Access Permissions for users and groups.



2. Repeat step 1 to create all the secured Shares you plan to add before the next steps.
3. Create groups on the domain controller to aggregate users that share the same level of access control to secured Shares on the Lenovo network storage device.
4. Import the groups onto the Lenovo network storage device.
5. Grant access permissions to the groups. All the users that belong to a group inherit from the group the same permissions to access secured Shares.
6. Configure access permissions to all secured folders for the group.

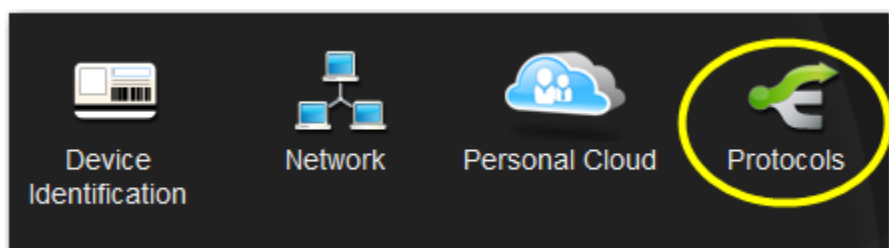


## Using NFS in AD Mode

NFS permissions on Unix/Linux are based on User IDs (UIDs). For a user to access a secured Share with NFS, the user must have a UID on the Lenovo network storage device matching its corresponding UID on the host. When a Lenovo network storage device is in AD mode, the user accounts are imported from the domain and therefore do not have UIDs unless a user mapping service is in place to map Windows users to Unix/Linux users. Lenovo network storage devices do not have a user mapper running to provide such a service. Consequently, in AD mode, NFS access control is only enforced at the host level. Whereas in Workgroup mode, NFS access control is enforced at both the user level and host level.

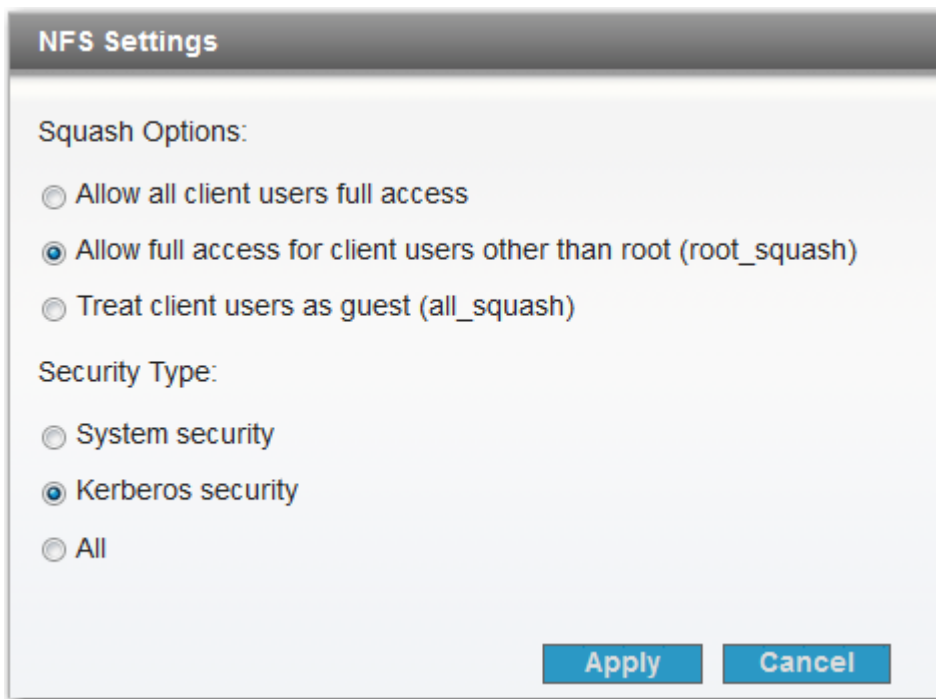
To set NFS access control on secured Shares:

1. Access the Protocols page in the storage device's console.



2. Turn on the NFS protocol.
3. Apply the NFS security setting for Active Directory.
  - 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.



**NFS Settings**

Squash Options:

- ☐ Allow all client users full access
- ☒ Allow full access for client users other than root (root\_squash)
- ☐ Treat client users as guest (all\_squash)

Security Type:

- ☐ System security
- ☒ Kerberos security
- ☐ All

**Apply** **Cancel**

4. On the Shares page, expand a Share name to display the NFS section.
5. Expand the NFS section, enter an NFS rule for the Share, and click **Apply**.



Financial Shares

Information

Access Permissions

**NFS - Overview**

Location: /nfs/Financial

Set NFS host access to secured Share 'Financial'.

[+ Add an NFS rule](#)

**Apply** **Cancel**

Active Folders

## FREQUENTLY ASKED QUESTIONS

**Q: What are the recommended numbers of users, groups, and folders to configure in the AD mode on a Lenovo network storage device?**

A: Different Lenovo platforms have different numbers. Note that these are not hard limits — they merely indicate a level of configuration that may result in the best overall system performance.

Platform	# of users	# of groups	# of folders
ix2-200	50	10	50
ix4-200d	50	10	50
ix4-200r	100	20	50
ix12-300r	1024	128	50

**Q: Can I create a local user account on the Lenovo device when it is in AD mode?**

A: Yes. Your Lenovo device offers hybrid authentication which allows the creation of local users while the device is in AD mode.

**Q: What happens if my DC is down or my network connection to the DC is lost?**

A: Your Lenovo network storage device can work in a high availability environment, which means it can work with multiple AD servers should one server fail or go offline. Your storage device can automatically switch authentication services to other domain controllers in the network, if there are any.

**Q: When using an administrator user account to log in to the device console, why does the admin account appear turned into a normal user and the Lenovo network storage device console presents only limited functions accordingly?**

A: Occasionally, the status of a user becomes incorrect during authentication with the DC. You may reboot the Lenovo network storage device to resolve this problem.

**Q: When clicking the Synchronize or Add commands on the Users & Groups page, why does the updating progress stall?**

A: Occasionally data synchronization with the DC can time out. You may retry the operation or reboot the device to resolve this problem.

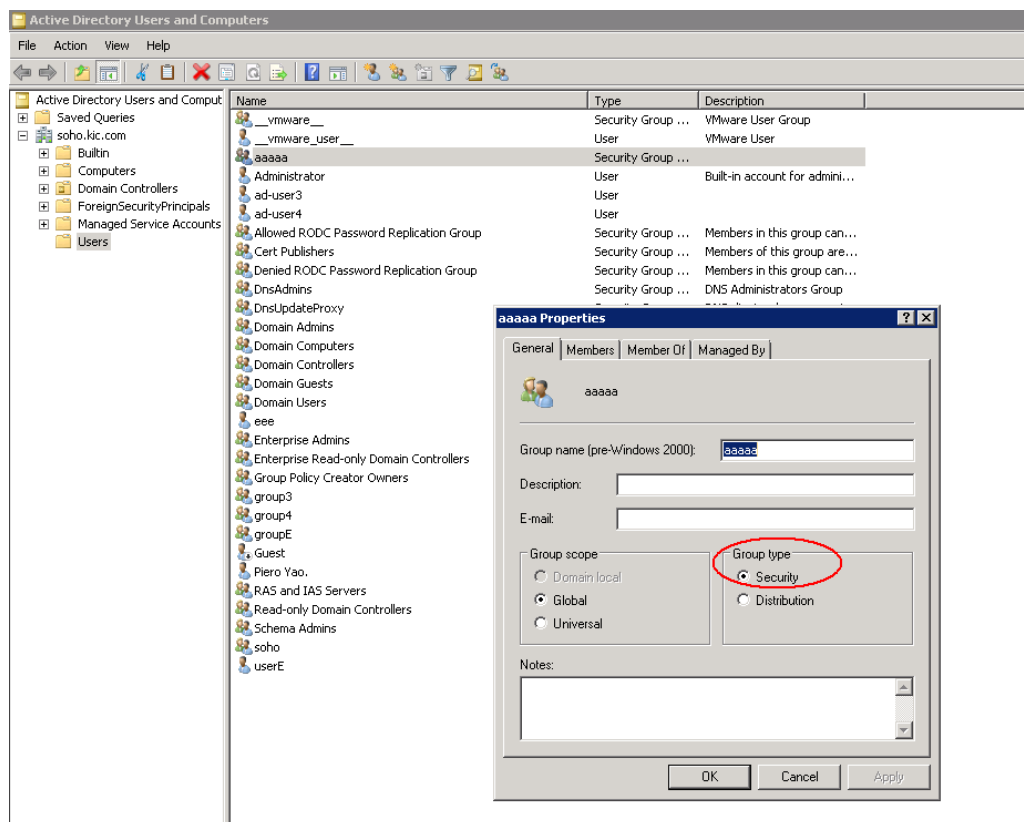
**Q: If a group is a system built-in group in the domain, after importing this group to the Lenovo network storage device, why is no member user shown out of this group?**

A: Currently domain built-in groups are not supported on Lenovo network storage devices.



**Q: Can I import domain groups that are categorized as Distribution groups, such as a mail group?**

**A:** All imported groups must be of the Security Group type. If the type is Distribution Group, it won't be imported onto the Lenovo network storage device, so you need to change the group type to Security. You may find the group type on the DC.



**Q: I have a user named “Aaa” in the domain. Why can’t I find this user when I search in the “Select users and groups from Active Directory” dialog box?**

**A:** The DC converts all NetBIOS names to lowercase for the Samba server, so you should use all lowercase to search for names, as in “aaa” in this case.

**Q: How do I make sure AD authentication is not impacted by other I/O activities on a network with very limited bandwidth, such as VPN over WAN?**

**A:** You can set the Quality of Service (QoS) settings as following:

- Set the VPN tunnel from the Lenovo network storage device to the DC on ports 137, 138, 139, 445, 389, 445 and 901.
- Set the VPN tunnel from the client PC to the Lenovo network storage device on port 139.

**Q: What kind of domain users could be used to join a Lenovo network storage device into the domain?**

A: Any domain user having authority to join PCs into the domain could also be used to join the Lenovo network storage device into the domain.

**Q: When a Lenovo network storage device is joined into a domain, is a DNS record created automatically for the device in the DNS server?**

A: Yes, a DNS record for the Lenovo network storage device is created automatically.

**Q: What Microsoft domains do Lenovo network storage devices support?**

A: Lenovo network storage devices support Windows NT domain, Windows 2K domain, W2K3 domain, W2K3R2 domain, W2K8 domain, and W2K8R2 domain.

**Q: How large a domain can Lenovo network storage devices support?**

A: There is no maximum size for the domain. Lenovo network storage devices have been tested in a domain with as many as 10,000+ groups and 100,000+ users. Keep in mind, the larger the domain, the slower the performance on user/group operations, such as syncing to the AD controller and importing members.

**Q: Do Lenovo network storage devices support domain names that contain an underscore?**

A: No, Lenovo network storage devices do not support domain name that contain an “\_”. According to Microsoft’s best practices, it is illegal to use the character. Check out <http://support.microsoft.com/kb/909264> for more details.

**Q: What are the restrictions on using special characters in domain user names and passwords?**

A: There is no known restriction on special characters being used in passwords. According to Microsoft, the following characters are invalid in user names and should not be used:

/ \ [ ] : ; | = , + \* ? < > @ “



[www.lenovo.com](http://www.lenovo.com)