Synology

LDAP Server User's Guide

Table of Contents

Introduction

Synology LDAP Server provides Lightweight Directory Access Protocol (LDAP) directory service that offers account integration and authentication support for LDAP-enabled applications. With LDAP integration, applications and services that previously required separate sets of user/group accounts now require users and groups to authenticate with the same account credentials.

LDAP Server simplifies the tasks of adding, modifying, and deleting user accounts among all LDAP-enabled applications. For example:

- If the password for a user is changed in LDAP Server, the change will be applied to the applications simultaneously, allowing the user to access all the applications with the new password.
- Likewise, with the help of LDAP Server, adding or removing users, or moving users between groups is just as easy. Therefore, if a company is undergoing corporate restructuring, IT professionals can add or remove employees' users or groups to cope with personnel changes, or move users between groups to allow or deny employees' access to individual department's resources. All privilege settings can be done in one convenient place and applied to all applications, saving IT professionals from the trouble of repeatedly making the same changes for each application.

The above examples demonstrate LDAP Server’s capability to centrally manage user/group accounts and simplify access control for applications and resources, which not only enhances network security but also reduces management costs.

LDAP Server can work seamlessly with multiple Synology NAS or Mac/Linux computers. IT administrators can join all Synology NAS or clients to LDAP Server to maximize IT efficiency by centralizing the account system of all Synology NAS or LDAP clients. Employees and departments can enjoy the convenience of using the same account credentials to access all resources, saving them from the trouble of remembering different usernames and passwords for different Synology NAS or computers.

This user's guide will guide you through the following:

- Chapter 1: Setting up LDAP Server and managing LDAP users and groups
- Chapter 2: Binding LDAP clients (including Synology NAS and client computers) to LDAP Server

Chapter

1

Set up LDAP Server

This chapter explains how to install and manage LDAP Server on your Synology NAS. When the setup is complete, LDAP clients (such as other Synology NAS and Mac computers) can join to LDAP Server for account integration.

Install and Launch LDAP Server

Before installing the LDAP Server package on your DiskStation Manager (DSM), please check the following:

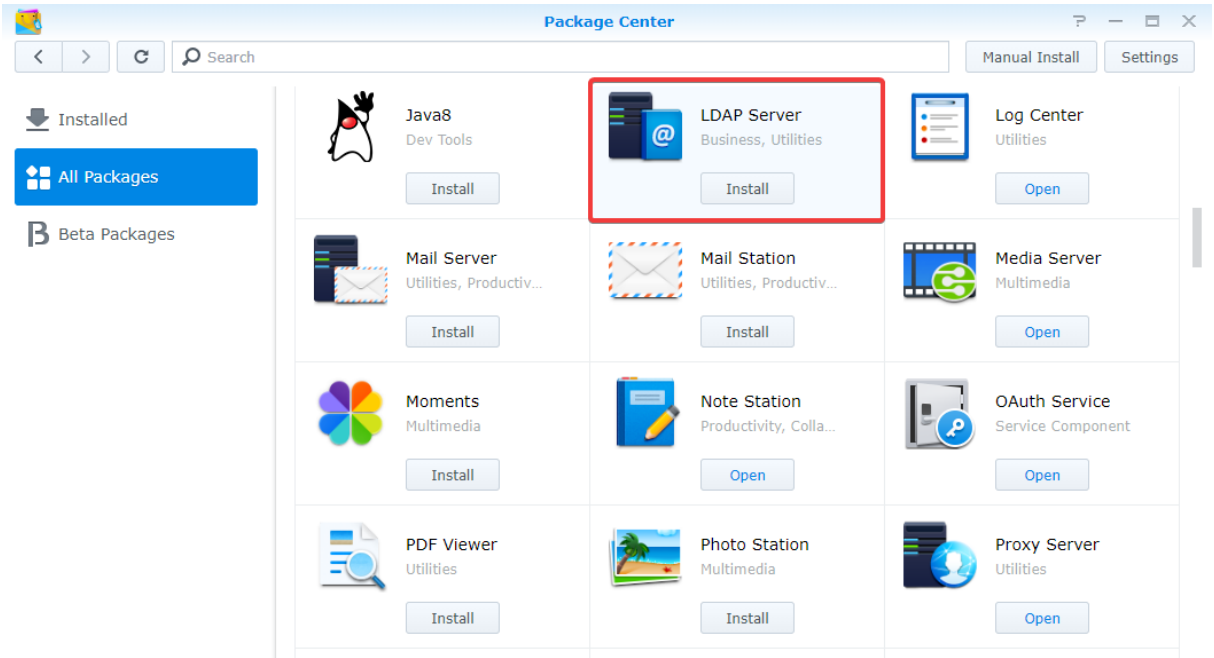
- Your Internet connection is working well.
- The volume of your DSM is healthy.
- Your DSM is updated to the latest version.
- You are the DSM **admin** (or a user belonging to the **administrators** group) for your Synology NAS.

To install and activate LDAP Server:

1 Log in to DSM as an **admin** or a user belonging to the **administrators** group.

2 Go to **Package Center** > **All Packages**.

3 Click the **Install** button in the **LDAP Server** section, and follow the onscreen instructions to complete the installation.



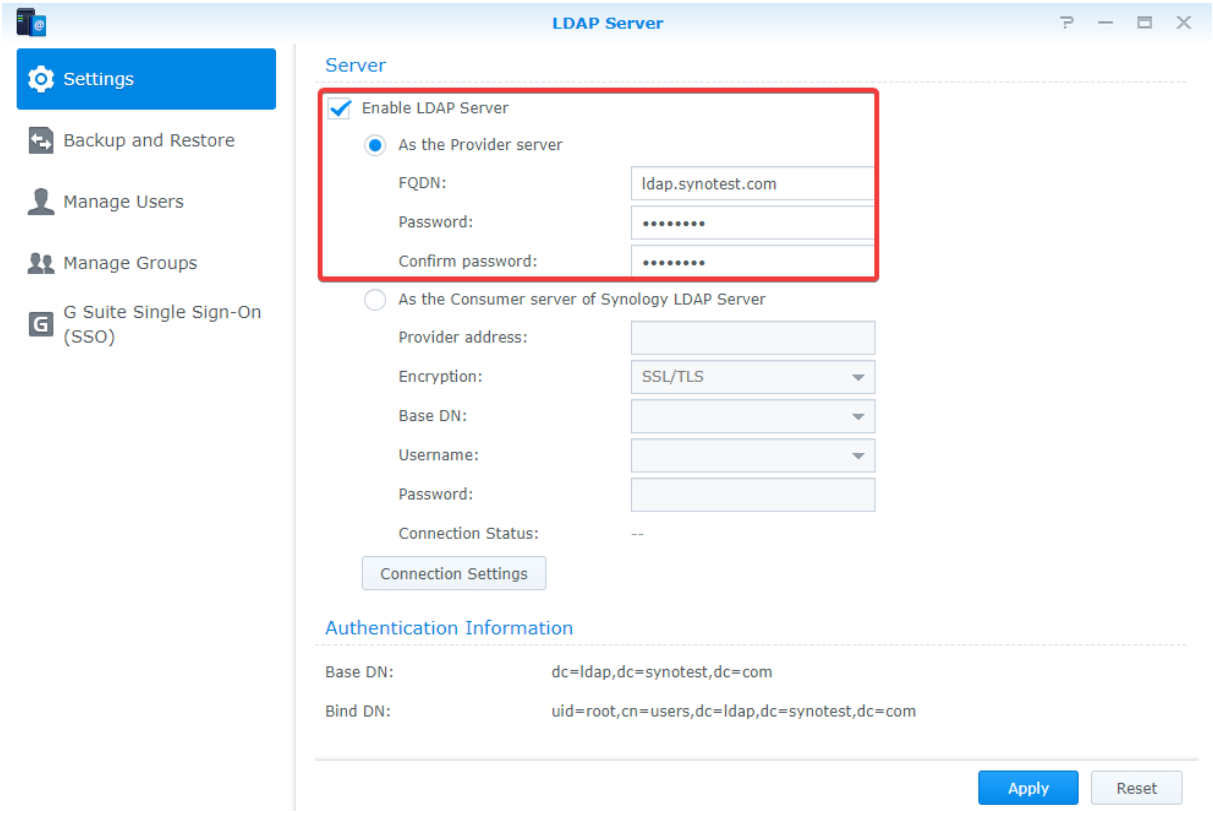
Enable LDAP Server

After the LDAP Server package is installed, go to **Main Menu** > **LDAP Server**.

> ***Note:*** If you have set up port forwarding or firewall rules for your Synology NAS, make sure port **389** (for LDAP connection) and **636** (for LDAP (SSL) connection) are properly configured at **Control Panel** > **External Access** > **Router Configuration** or **Control Panel** > **Security** > **Firewall**.

To enable LDAP Server:

1. Click **Settings** on the left panel, and then tick **Enable LDAP Server**.
2. In the **FQDN** (**Fully Qualified Domain Name**) field, specify the domain name for the LDAP database.
3. Enter the password of **Bind DN** (see below) in the **Password** field.
4. Click **Apply**.



When the setup is complete, you can see the following information of your LDAP Server in the **Authentication Information** section:

- **Base DN**: The distinguished name for LDAP Server's LDAP database. This is generated from the specified FQDN. For example, if the FQDN is *ldap.synology.com*, its Base DN will be *dc=ldap,dc=synology,dc=com*.
- **Bind DN**: The distinguished name for LDAP's **root**. For example, if the Base DN of the LDAP database is *dc=ldap,dc=synotest,dc=com*, then the Bind DN of **root** will be *uid=root,cn=users,dc=ldap,dc=synotest,dc=com*.

If LDAP clients want to bind to your LDAP Server, they should specify the Base DN to connect to the LDAP database, and then authorize with the Bind DN of **root** or an LDAP administrator account.

Manage LDAP Users/Groups with LDAP Server

You can create and manage LDAP users/groups with LDAP Server. To do so, go to **LDAP Server** and then click **Manage Users** or **Manage Groups** on the left panel. You will see several users and groups already created:

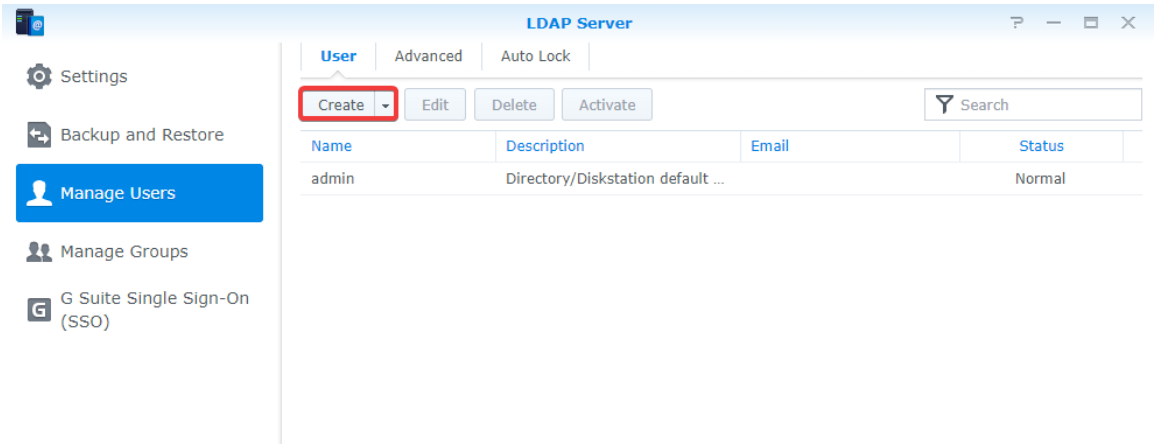
- **Default users**:
  - **admin**: The built in account for administration of the LDAP directory.
- **Default groups**:
  - **users**: This is the default group for all LDAP users. If users in this group are not added to the administrators or Directory Operators group, they will not have DSM or LDAP administrative privileges.
  - **administrators**: Users added to this group will have the same administrative privileges as DSM admin.
  - **Directory Operators**: Users added to this group will have administrative privileges of the LDAP database.
  - **Directory Clients**: Users belonging to this group will have the read permissions for users/groups in LDAP Server. For security purposes, it is recommended that an LDAP client that wishes to join an LDAP server is given a user in this group.
  - **Directory Consumers**: Users belonging to this group will have the read permissions for configurations and users/groups in LDAP Server. A Consumer server must belong to this group in order to replicate data from the Provider server. Members of this group should only be used in Bind DN of the Consumer server and should not belong to any other group. Otherwise, synchronization errors may occur due to incorrect permissions.

To create an LDAP user:

1 Click **Manage Users** on the left panel. Here you can see the built-in user account named **admin**. By default, LDAP **admin** has administrative privileges to the LDAP database.

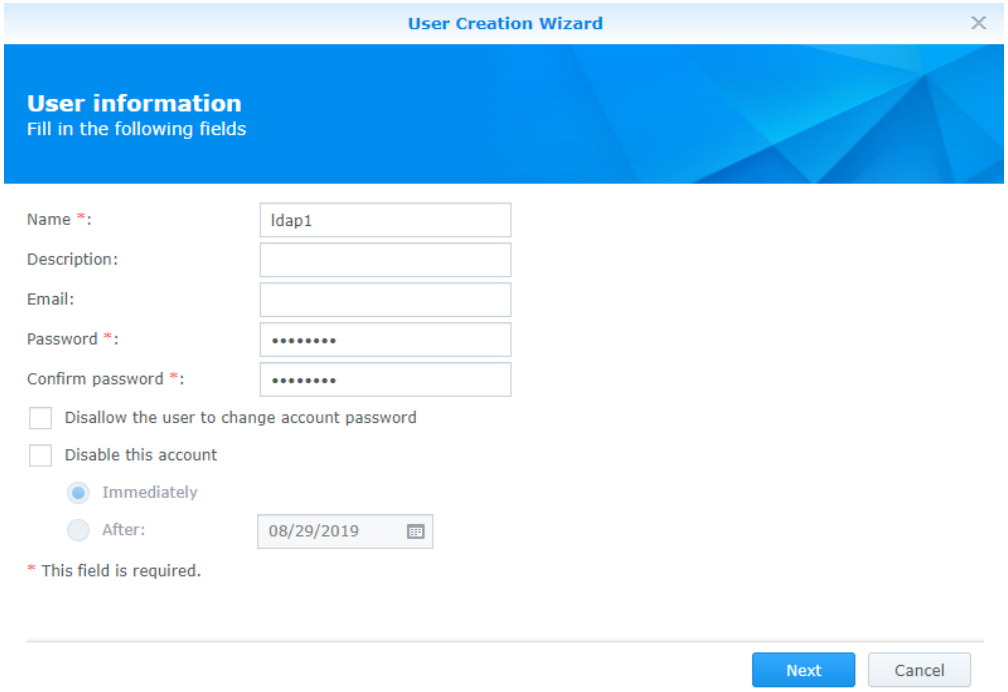
> ***Note:*** The password of **admin** is the one you specified on the **Settings** page. (See "Enable LDAP Server" on Page 5 for more information.)

2 Click **Create**.

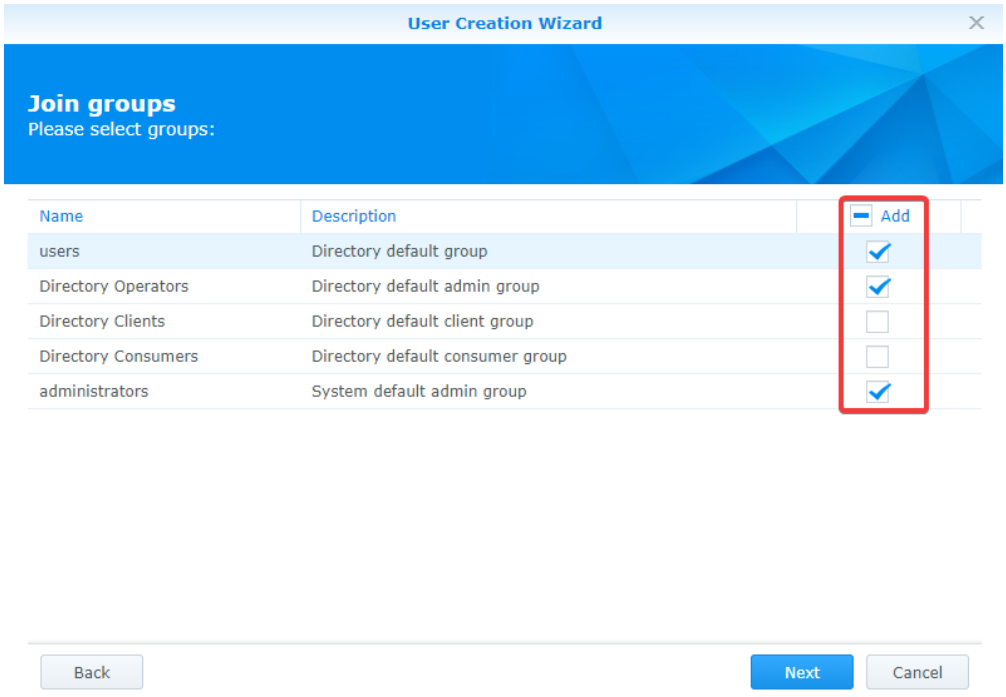


3 Specify the following information for the LDAP user and then click **Next**:

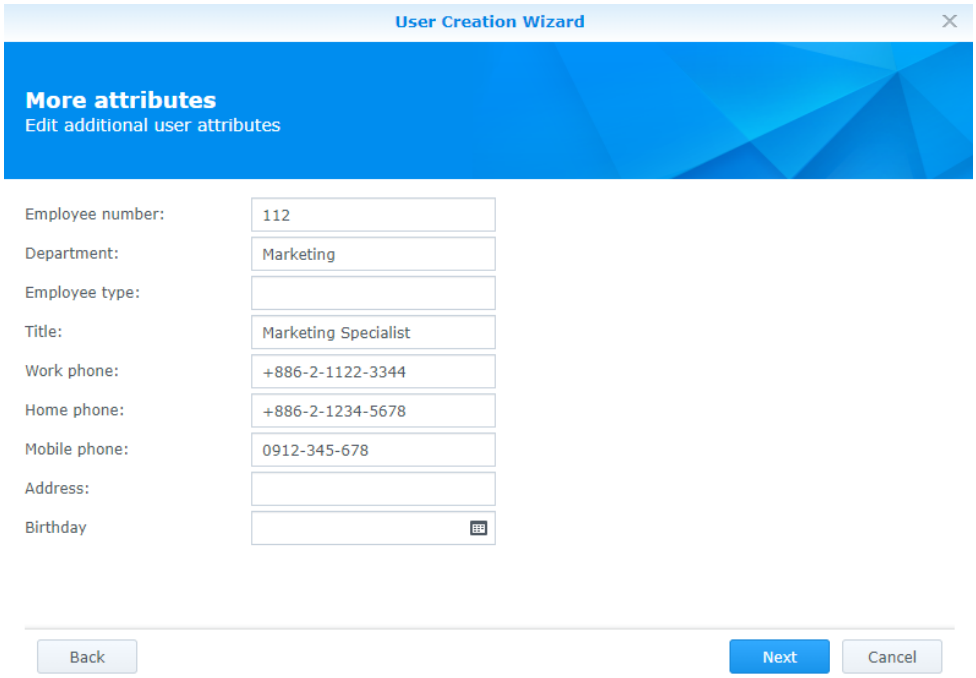
- **Name**: The name of the user will be stored as the **uid** attribute in the LDAP database.
- **Description** (optional): The description of the user will be stored as the **gecos** attribute.
- **Email** (optional): The email address of the user will be stored as the **mail** attribute.
- **Password**: The password of the user will be stored as the **userPassword** attribute.
- **Disallow the user to change account password** (optional): This information will be stored as the **shadowMin** attribute.
- **Disable this account** (optional): This information will be stored as the **shadowExpire** attribute.



4 Tick the checkboxes to add the user to the default or created groups, and click **Next**:



5 Add additional attributes for the user on the **More attributes** page, and click **Next**.



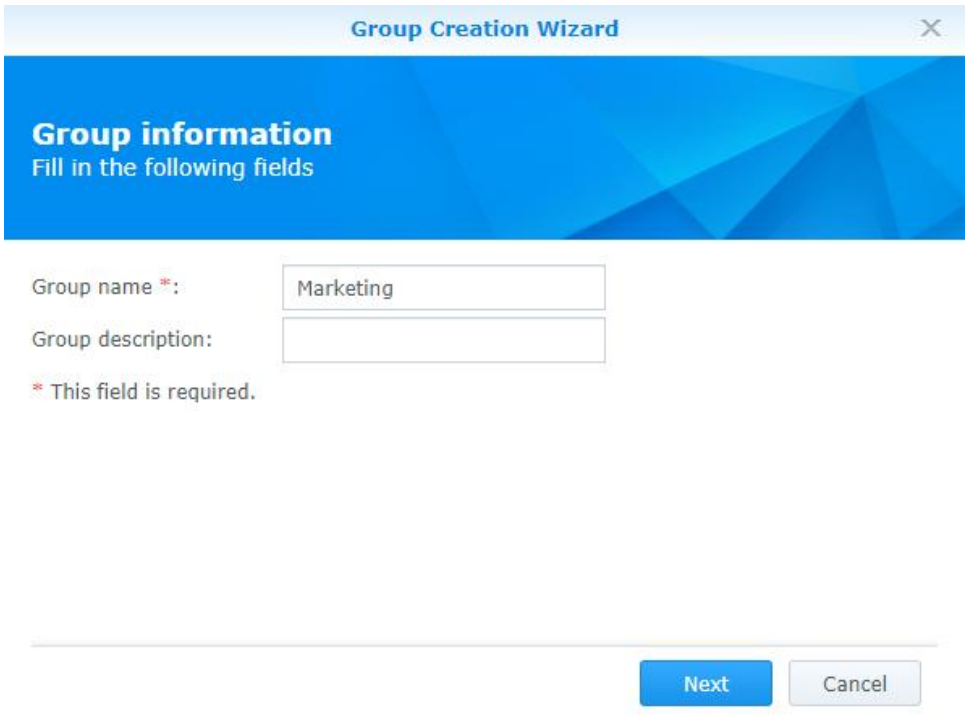
6 Click **Apply** to create the LDAP user. The distinguished name of the user in the LDAP database is **uid=[username],cn=users,[Base_DN]**.

To create an LDAP group and add group members:

1 Click **Manage Groups** on the left panel, and then click the **Create** button.

2 Specify the following information for the LDAP group and then click **Next**:

- **Group name**: The name of the group will be stored as the **cn** attribute in the LDAP database.
- **Group description** (optional): The description of the group will be stored as the **description** attribute in the LDAP database.



3 Click **Apply** to create the LDAP group. The distinguished name of the group in the LDAP database is **cn=[groupname],cn=groups,cn=[Base_DN]**.

4 Do the following to add group members:

a Select the group you want and click **Edit Members**.

b Click **Add**, select the users you want to add to the group from the user list (press and hold the Ctrl or Shift key for multiple selections), and then click **OK**. In the LDAP database, the **memberUid** attribute will be given to LDAP users added to this group.

c Click **Finish**.

> ***Note:*** You are not allowed to edit group members for the **users** group.

To edit or delete the LDAP users or groups:

1 Click **Manage Users** or **Manage Groups** on the left panel.

2 Click **Edit** or **Delete**, and follow onscreen instructions to complete the process.

Chapter 2

Join LDAP Clients to Directory Service

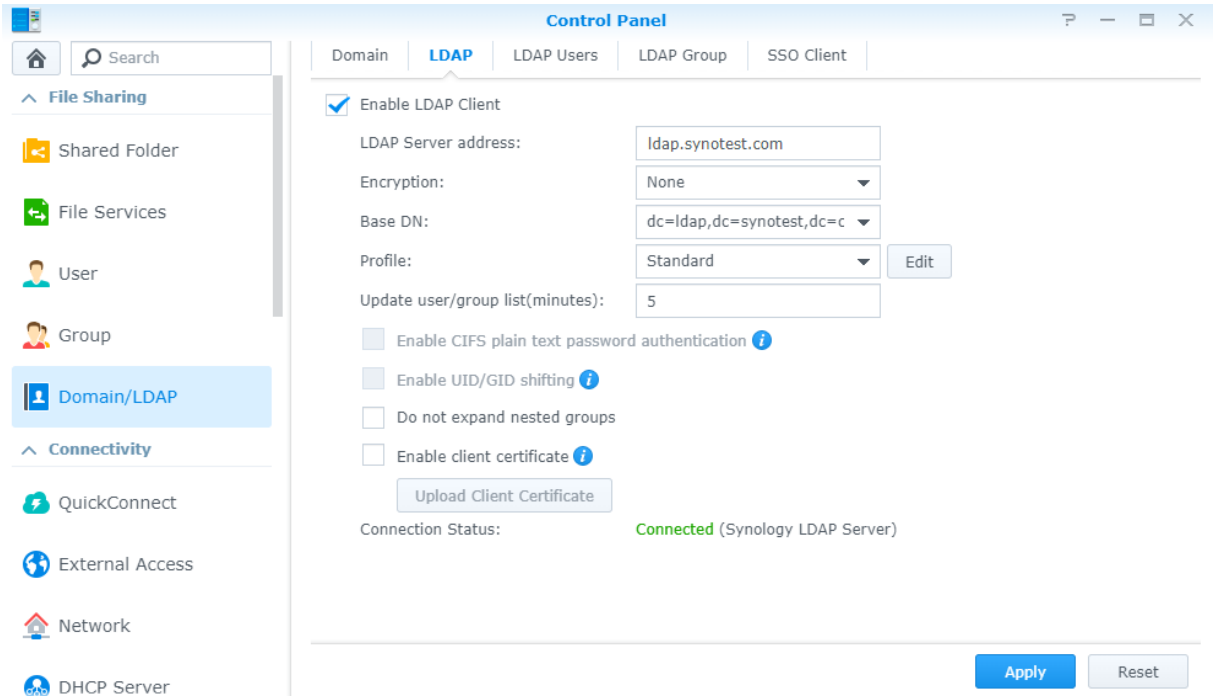
When the directory service is set up on the LDAP Server package or any other LDAP server, Synology NAS and other LDAP clients (such as Mac and Linux computers) can be bound to the server to join the directory service.

This chapter explains how to join Synology NAS and client computers to the directory service provided by the LDAP Server package or any other LDAP server.

Join Synology NAS to Directory Service

You can join your Synology NAS to Synology LDAP Server or other LDAP servers (such as Linux LDAP Server or Mac OpenLDAP Server) that contain the object class **posixAccount** for its users and groups.

When the joining process is complete, your Synology NAS will retrieve the information of LDAP users and groups from the LDAP server, allowing users with LDAP credentials to access files on Synology NAS via browser or file services (e.g., SMB, AFP, etc.). You can also manage LDAP users' and groups' access privileges to Synology NAS services and shared folders, just as you would with DSM local users or groups.



Support and Limitations:

- Your Synology NAS can be joined to only one LDAP server at a time.
- If you use the LDAP functionality mentioned in this section to join your Synology NAS to a server that don't contain the object class **posixAccount** for its users and groups (such as Windows Domain Controller or Microsoft Exchange Server), your Synology NAS will not be able to retrieve the information of LDAP users and groups from the server.

- If you want to join your Synology NAS to a Windows Domain Controller to retrieve the information of domain users and groups, go to **Control Panel** > **Domain/LDAP** > **Domain**. However, you are not allowed to join your Synology NAS to an LDAP directory and Windows domain at the same time.

To join your Synology NAS to an LDAP server:

1 Log in to DSM as **admin** (or a user belonging to the **administrators** group), go to **Control Panel** > **Domain/LDAP** > **LDAP**, and then tick **Enable LDAP Client**.

2 Enter the IP address or domain name of the LDAP server in the **LDAP Server address** field.

3 Choose an encryption type from the **Encryption** drop-down menu to secure LDAP connection with encryption mechanism.

4 Enter the Base DN of the LDAP server in the **Base DN** field, or choose an available Base DN from the **Base DN** drop-down menu.

> ***Note:*** For more information about Base DN, see "Enable LDAP Server" on Page 5.

5 If necessary, tick the checkboxes to configure advanced settings (see the **Advanced settings for joining an LDAP directory** subsection below for detailed instructions).

6 Confirm the entered information and click **OK**.

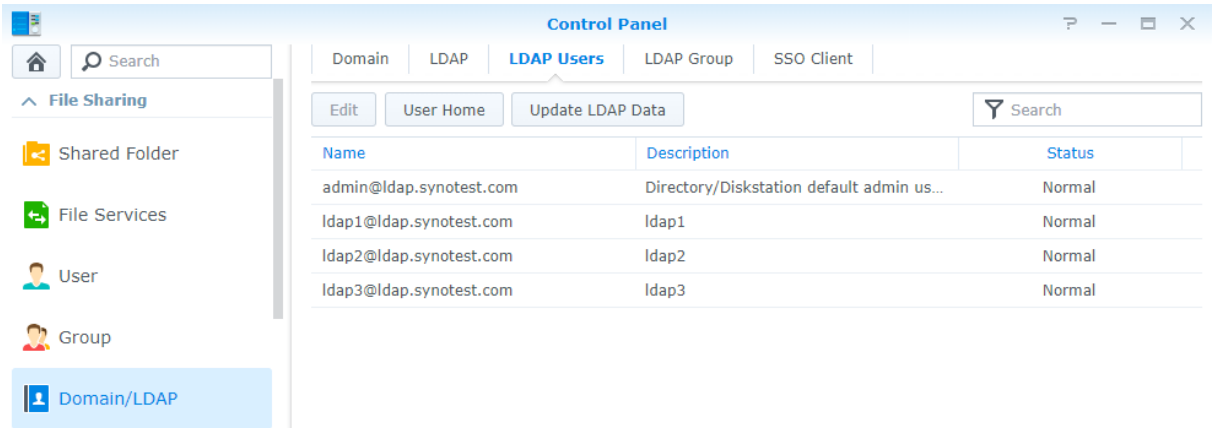
7 In the authentication window that appears, do the following:

a Enter the distinguished name (DN) or account name of an LDAP administrator (such as **root** or a user belonging to LDAP Server's **Directory Operators** group) in the **Bind DN or LDAP administrator account** field.

b Enter the password for the LDAP administrator in the **Password** field.

c Click **Apply**.

After your Synology NAS is joined to the LDAP server, it will start retrieving the information of LDAP users or groups from the server, and then display them under the **LDAP Users** or **LDAP Group** tab.



> ***Note:***
>
> - LDAP users are not allowed to access the following DSM applications: Photo Station, Audio Station, and Surveillance Station.
> - If LDAP users want to access Synology NAS files with their computer via the AFP protocol, they will need to authorize with the username **LDAP_Username@Suffix**. For example, if the name of the LDAP user is *ldap1*, and the Base DN of the LDAP database is *dc=ldap,dc=synology,dc=com*, then the suffix would be *ldap.synology.com*, and the user can authorize with the username ***ldap1@ldap.synology.com***.

Advanced settings for joining an LDAP directory:

The following will provide you detailed information on several advanced settings available during the LDAP joining process on your Synology NAS.

- **Profiles**

  Different LDAP servers might use different attributes for account names, group names, or to distinguish between accounts and groups. The Profile option allows you to specify or customize how user and group information is mapped to LDAP attributes. One of the following profiles can be selected depending on your LDAP server:

  - **Standard**: For servers running LDAP Server or Mac Open Directory.
  - **IBM Lotus Domino**: For servers running IBM Lotus Domino 8.5.
  - **Custom**: Allows you to customize mappings. Consult the section below for details.

  Before customizing LDAP attribute mappings, you will need some background knowledge. Synology DSM and the **Profile** editor both adhere to RFC 2307. For example, you can specify **filter > passwd** as **userFilter**, in which case the Synology NAS will interpret records with **objectClass=userFilter** on your LDAP server as LDAP accounts. If you specify **passwd > uid** as **username**, the Synology NAS will interpret **username** on your LDAP server as an account name. Leaving the mapping empty will apply RFC 2307 rules.

  Synology NAS requires a fixed integer to serve as an LDAP account identifier (**uidNumber**) or a group identifier (**gidNumber**). However, not all LDAP servers use integers to represent such attributes. Therefore, a keyword **HASH()** is provided to convert such attributes to integers. For example, your LDAP server might use the attribute **userid** with a hexadecimal value as the unique identifier for an LDAP account. In this case, you can set **passwd > uidNumber** to **HASH(userid)**, and then Synology NAS will convert it into an integer.

  The following is the summary of customizable attributes:

  - **filter**
    - **group**: required objectClass for group.
    - **passwd**: required objectClass for user.
    - shadow: required objectClass for user passwords.
  - **group**
    - **cn**: group name.
    - **gidNumber**: GID number of this group.
    - **memberUid**: members of this group.
  - **passwd**
    - **uidNumber**: UID number of this user.
    - **uid**: username.
    - **gidNumber**: primary GID number of this user.
  - **shadow**
    - **uid**: username.
    - **userPassword**: user password.

- **CIFS support and client computer's settings**:

  After CIFS plain text password authentication is enabled, LDAP users might need to modify their computers' settings to be able to access Synology NAS files via CIFS:

  If your Synology NAS joins to the directory service provided by a Synology LDAP server (or another Synology NAS that has installed and run the LDAP Server package) or the LDAP server that supports Samba schema and all LDAP users have correct sambaNTPassword attributes, LDAP users can access your Synology NAS files via CIFS without ticking Enable CIFS plain text password authentication or modifying their computers' settings. Otherwise, LDAP users will need to enable their computer's PAM support to be able to access Synology NAS files via CIFS. However, doing so will transfer LDAP users' password to Synology NAS in plain text (without encryption), thus lowering the security level.

  - **How to modify Windows settings:**

  1. Go to **Start** > **Run**, type **regedit** in the field, and then click **OK** to open **Registry Editor**.
  2. Depending on your Windows version, find or create the following registry:
     - **Windows 2000, XP, Vista, and Windows 7:**
       [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkStation\Parameters]
     - **Windows NT:**
       [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Rdr\Parameters]
     - **Windows 95 (SP1), 98 and Me:**
       [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\VNETSUP]
  3. Create or modify the DWORD value **EnablePlainTextPassword** and change its value data from **0** to **1**.
  4. Restart Windows for the change to take effect.

  - **How to modify Mac OS X's settings:**

  1. Go to **Applications** > **Utilities** to open **Terminal**.
  2. Create an empty file **/etc/nsmb.conf**:

```
sudo touch /etc/nsmb.conf
```

  3. Open **/etc/nsmb.conf** with vi:

```
sudo vi /etc/nsmb.conf
```

  4. Type ***i*** to insert text, and paste the following:

```
[default] >
minauth=none
```

  5. Press the Esc key and then type ***ZZ*** to save the changes and exit vi.

  - **How to modify Linux's settings:**

  If you're using smbclient, please add the following keys in the **[global]** section of **smb.conf**:

```
encrypt passwords = no
client plaintext auth = yes
client lanman auth = yes
client ntlmv2 auth = no
```

  If you're using **mount.cifs**, execute the following command:

```
echo 0x30030 > /proc/fs/cifs/SecurityFlags
```

  For more information, please refer to **this article**.

- **UID/GID shifting**

  To avoid UID/GID conflicts between LDAP users/groups and local users/groups, you can enable UID/GID shifting to shift the UID/GID of LDAP users/groups by 1000000. This option is only for LDAP servers which are non-Synology LDAP servers and have a unique numerical ID attribute for each user/group.

- **Nested group expansion**

  In a nested group, an LDAP group member belongs to another LDAP group, where the hierarchy of an organization is represented. When users look up which group a specific member belongs to, or the name list of a specific group, Synology NAS will expand a nested group according to the member attributes of the LDAP group, where the DN (Distinguished Name) of a child group is referenced by the attribute. The expansion of a nested group can be very time-consuming under different circumstances, e.g. where the server does not index the member attribute, or the group is deeply nested. You can choose not to expand a nested group to prevent such occurrence.

- **Client certificates**

  We support the usage of client certificate. Some specific LDAP Servers, e.g., Google LDAP, use certificates to authenticate clients. You can upload the client certificate after ticking the Enable client certificate option.

  > ***Note:*** This function is supported on DSM 6.2.2 or above.

Join Client Computer to Directory Service

This section explains how to join client computers to the directory service provided by LDAP Server, and configure the location of client computers' home folders for LDAP users. When the setup is complete, users can log in to client computers' operating system with their LDAP credentials, and then store documents, preference settings, and other information in their home folders.

Supported operating systems:

- **Mac:** Mac OS X 10.6 or later is recommended.
- **Linux:** Linux users can choose from a variety of open source LDAP solutions to bind their computers to LDAP Server. Refer to related documentation for detailed instructions.

> ***Note:*** LDAP Server does not support Windows domain, so you are not allowed to bind your Windows PC to LDAP Server to join Windows domain.

Bind Mac Clients to LDAP Server

If you are the administrator of your Mac, you can bind your Mac to LDAP Server at the **Users & Group** preference pane and **Directory Utility**.

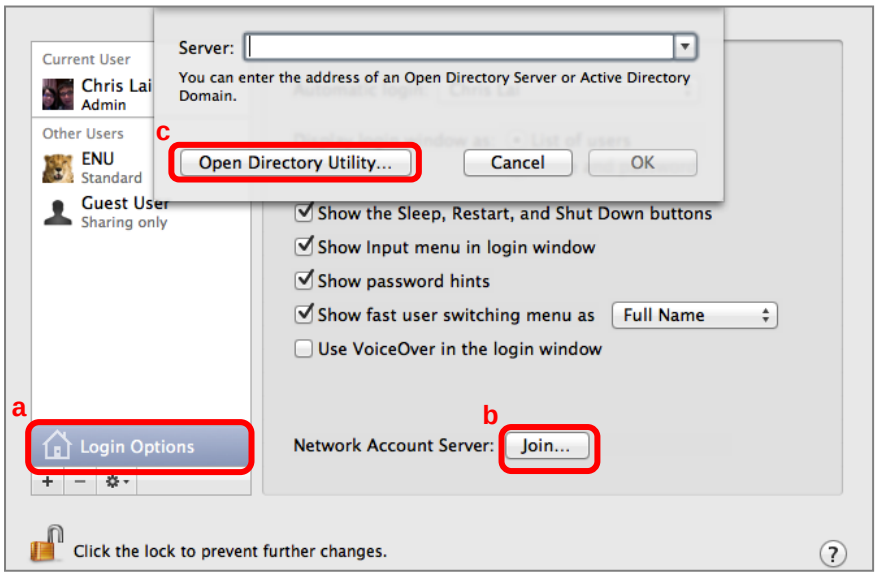
To bind your Mac to LDAP Server (using Mac OS X 10.7 for example):

1 Go to Apple menu > **System Preferences** > **Users & Groups**, and do the following:

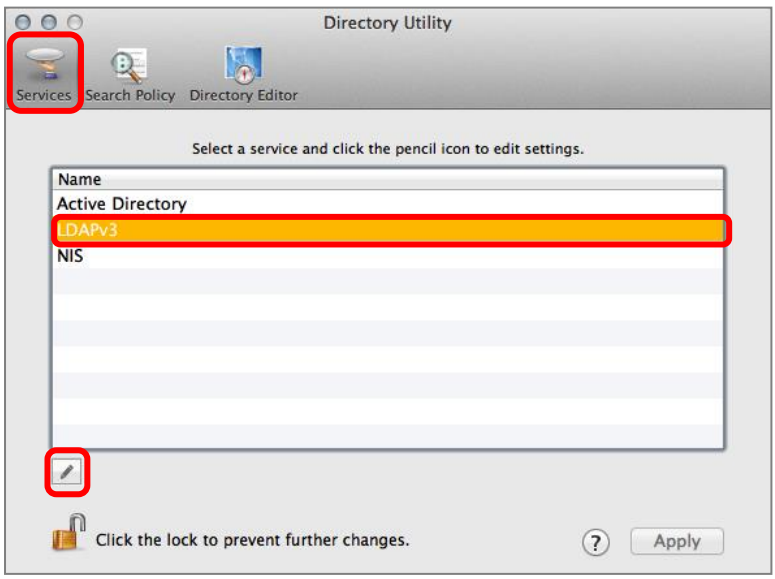
a Click **Login Options**. If the options appear to be grayed out, click the lock icon at the bottom-left corner, and then use Mac administrator's password to unlock the options.

b Click **Join**.

c In the dialog that appears, click **Open Directory Utility** to launch **Directory Utility**.



2 Under the **Services** tab, select **LDAPv3**, and then click the **Edit** button (with a pencil icon).

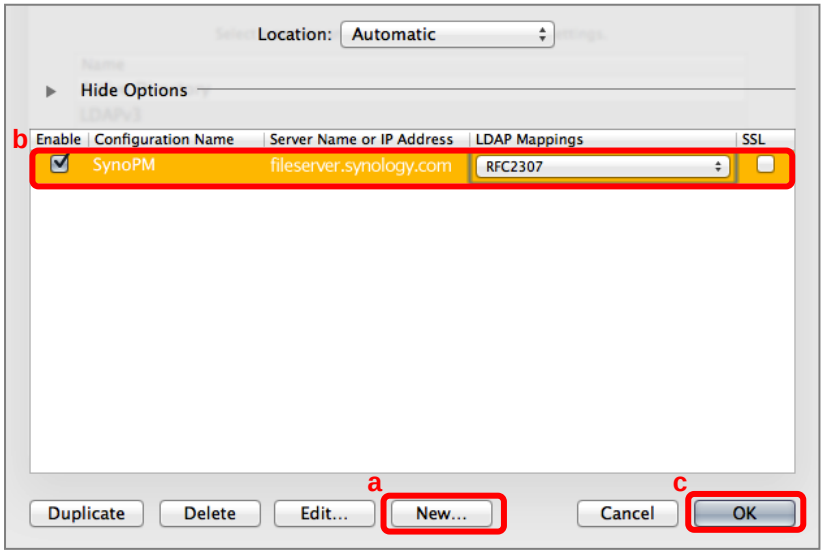


3 In the dialog that appears, do the following:

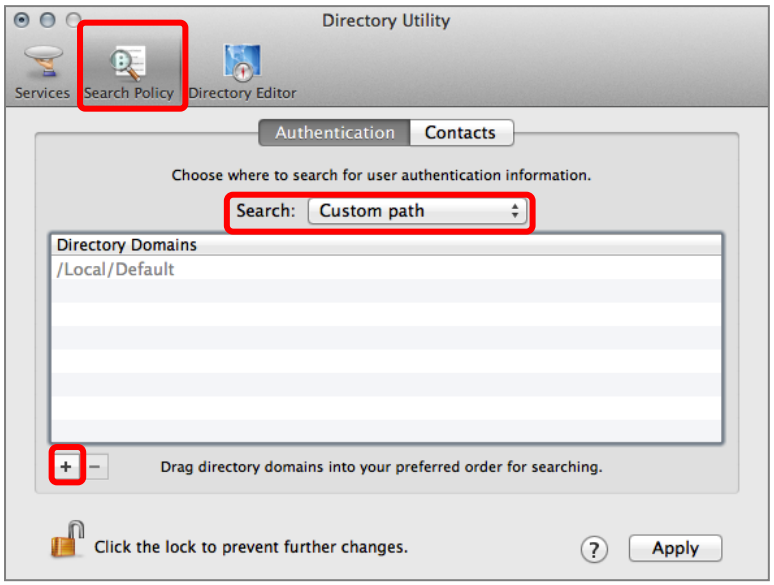
a Click **New**.

b In the expanded list of LDAP servers, enter the name or IP address of the Synology NAS that hosts LDAP Server, and then choose **RFC2307** from the drop-down menu. If you see a message prompting you to enter search DN suffix, click **OK** first.

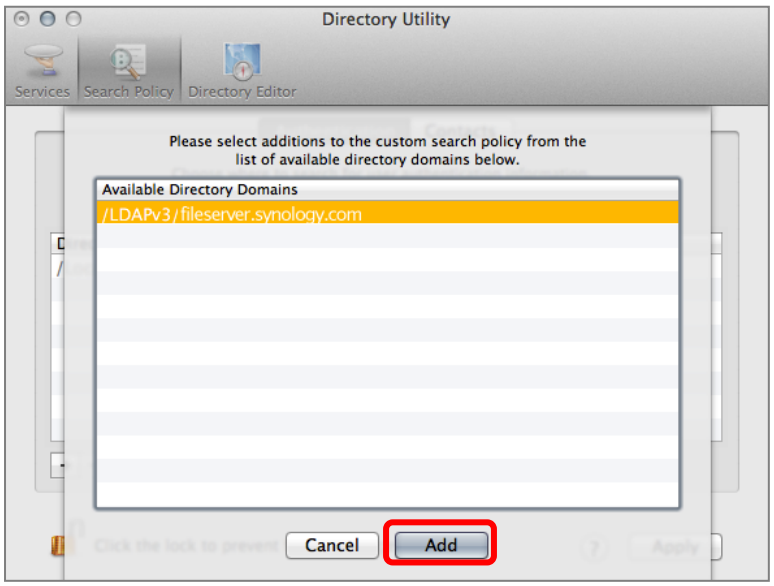
c Click **OK**.



4 Click the **Search Policy** tab, choose **Custom path** from the **Search** drop-down menu, and then click **+**.



5 Click **Add** to add the account system **/LDAPv3/Directory_Server_Address**. Your Mac's Directory Utility will use the account system to search and retrieve the information of LDAP users and groups from the LDAP database.



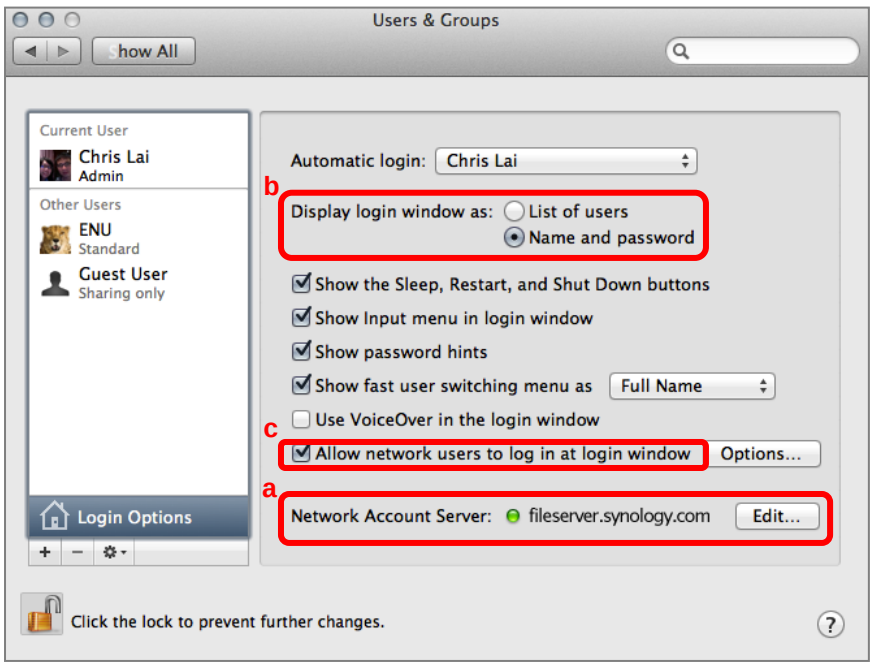
6 Click **Apply** in the Directory Utility window to apply the settings

7 Return to **Login Options** on the **Users & Group** preference pane, and then do the following:

a Check the green light next to the **Network Account Server** to make sure your Mac has successfully bound to LDAP Server. If your Mac has joined multiple network account servers, click **Edit** and check the green light next to your LDAP Server.

b Select **Name and password** in the **Display login window as** section.

c Tick **Allow network users to log in at login window**.



Create Mac Clients' Home Folders for LDAP Users

Your Mac is successfully bound to LDAP Server, and you should be able to log in to Mac OS X with your LDAP user credentials. However, since the home folder for the user is not created yet, you might see a window containing the following error message after login, indicating the home folder for the LDAP user is not created yet:

The home folder for user [LDAP_Username] isn't located in the usual place or can't be accessed.

Under the circumstances, unless the location of the home folder for your LDAP user account is properly configured, you might not be able to open Finder or modify any settings after login.

The location of the home folder could be the shared folder on any NFS server, such as the Synology NAS that hosts LDAP Server, any other Synology NAS with NFS enabled, or a Mac/Linux server.

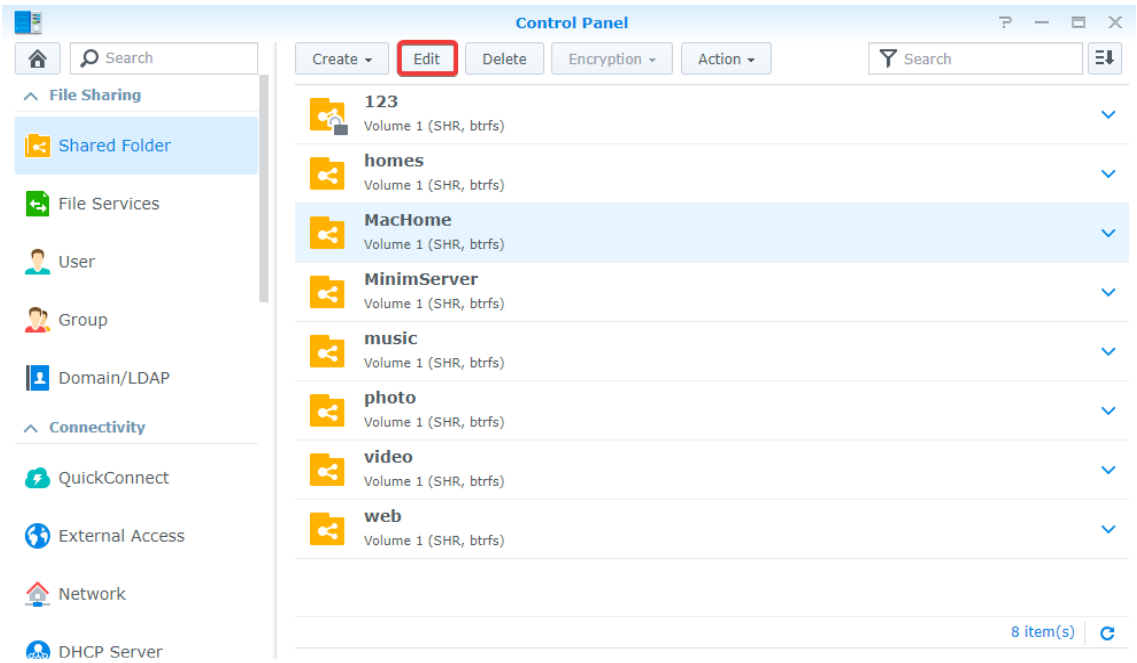
This section explains how to do the following:

- Setting up a Synology NAS as the location of Mac clients' home folders for LDAP users
- Setting up LDAP Server to access the Synology NAS via NFS to automatically create Mac clients' home folders

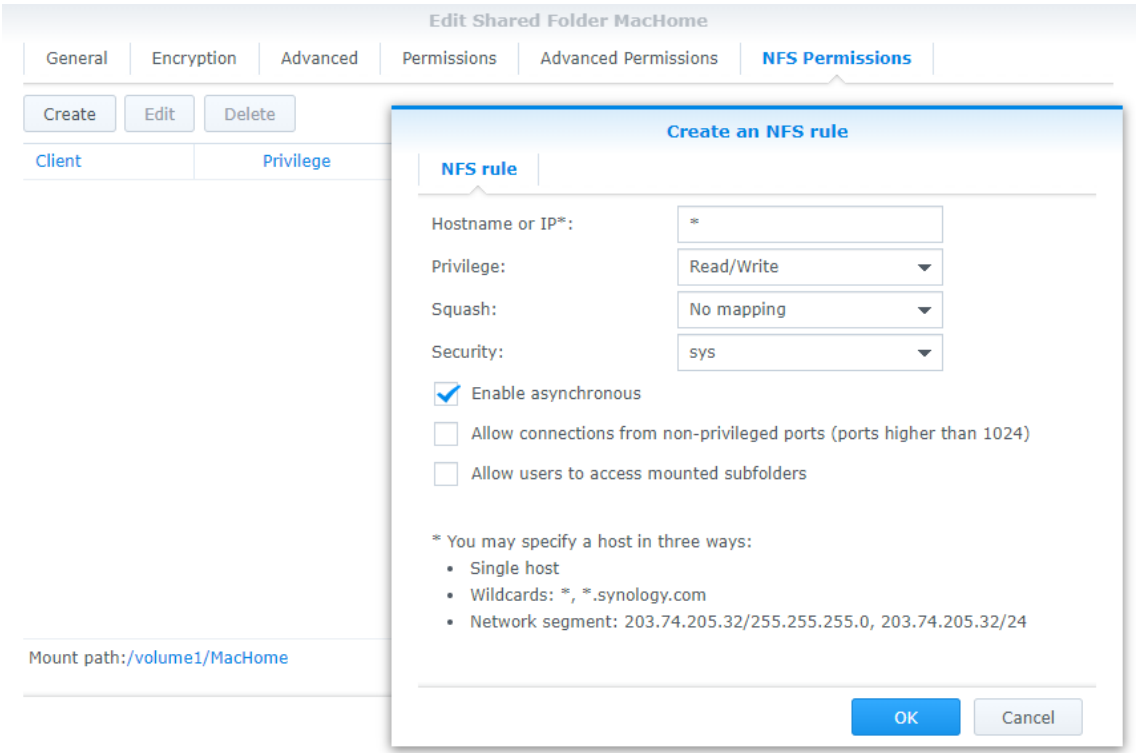
> ***Note:*** Since Mac clients' home folders will be used to contain all the files and preference settings for all LDAP users, it is recommended that you specify a Synology NAS (or NFS server) with storage space large enough to store the files for all LDAP users.

To configure the location of Mac clients' home folders for LDAP users:

1. Log in to the DSM of the Synology NAS that will be used to store the home folders (such as *fileserver.synology.com*) as DSM **admin** or a user belonging to the **administrators** group.
2. Go to **Control Panel** > **File Services** > **Win/Mac/NFS** to make sure the NFS service is enabled.
3. Go to **Control Panel** > **Shared Folder** to create a shared folder (such as *MacHome* on *Volume 1*).
4. Select the shared folder you just created, click **Edit**, and then go to the **NFS Permissions** page.



5 Click **Create** to create an NFS rule. Enter the hostname or IP address of NFS clients in the **Hostname or IP** field to specify which clients can access this shared folder. The hostname or address specified here should allow access from both LDAP Server and Mac clients. In our example, the asterisk ***** will be treated as a wildcard that allows access from all NFS clients. Keep other settings and click **OK**. Lastly, click **OK** again to save the rule and exit the **Edit Shared Folder** window.



6 Now we are going to add an NFS option that is not displayed in DSM's management UI, but is necessary for Mac clients to access the home folders. Use Telnet or SSH to log in to the Synology NAS that will be used to store home folders. Log in as **root** and authenticate using the password of DSM **admin**.

```
computername:~computerusername$ telnet fileserver.synology.com
...
fileserver login: root
Password: [DSM_admin's_password]
```

> ***Note:*** Make sure Telnet or SSH is enabled on your Synology NAS (at **Control Panel** > **Terminal & SNMP**) before logging in via Telnet/SSH.

7 Use the tool **vi** to edit the configuration file **/etc/exports**.

```
fileserver> vi /etc/exports
```

8 Find the NFS rule you just created for your shared folder (such as */volume1/MacHome*). Type ***i*** and then type ***insecure*****,** in the parentheses to add the **insecure** option to the NFS rule.

```
/volume1/MacHome *(rw,async,no_wdelay,no_root_squash,insecure,insecure_locks,
anonuid=0,anongid=0)
~
~
- /etc/exports [Modified] 0/0 100%
```

9 Press the Esc key and then type *ZZ* to save the changes and exit vi.

The configuration of the shared folder's NFS rule is complete. Now we need to set up LDAP Server to automatically mount Mac clients' home folders in this shared folder whenever an LDAP user is created.

To set up LDAP Server to automatically create Mac clients' home folders:

1 Use Telnet or SSH to log in to the Synology NAS that hosts LDAP Server. Log in as **root** and authenticate using the password of DSM **admin**.

```
computername:~computerusername$ telnet fileserver.synology.com
...
fileserver login: root
Password: [DSM_admin's_password]
```

> ***Note:*** Make sure Telnet or SSH is enabled on your Synology NAS (at **Control Panel** > **Terminal & SNMP**) before logging in via Telnet/SSH.

2 Use the tool **synoldapserver** to add the **automount** information.

```
synoldapserver --automount "[Hostname_OR_IP_address_of_NFS_Server]" "[Home_Folder_Path]"
```

For example, we have set up the Synology NAS *fileserver.synology.com* to store Mac clients' home folders in its shared folder */volume1/MacHome*. Therefore, we can use the following command to add the **automount** information:

```
fileserver> synoldapserver --automount "fileserver.synology.com" "/volume1/MacHome"
```

LDAP Server will automatically create the home folders for each LDAP user at the home folder path.

3 To confirm that the home folders are successfully created, use Telnet or SSH to log in to the Synology NAS which is set up to contain the home folders (such as *fileserver.synology.com*), navigate to the home folder path (using the *cd* command), and then browse its contents (using the *ls* or *ll* command). If you see the list of home folders named after the LDAP users, the home folders are successfully created.

```
computername:~computerusername$ telnet fileserver.synology.com
...
fileserver login: root
Password: [DSM_admin's_password]
...
fileserver> cd /volume1/MacHome
fileserver> ll
drwxrwxrwx  6 root    root      4096 Sep 25 17:47 .
drwxr-xr-x  34 root    root      4096 Sep 23 17:04 ..
drwx------  2 admin@19 users@19   4096 Sep 22 17:39 admin
drwx------  2 ldap1@19 users@19   4096 Sep 22 17:39 ldap1
drwx------  11 ldap2@19 users@19   4096 Sep 22 17:42 ldap2
drwx------  2 ldap3@19 users@19   4096 Sep 25 17:47 ldap3
```

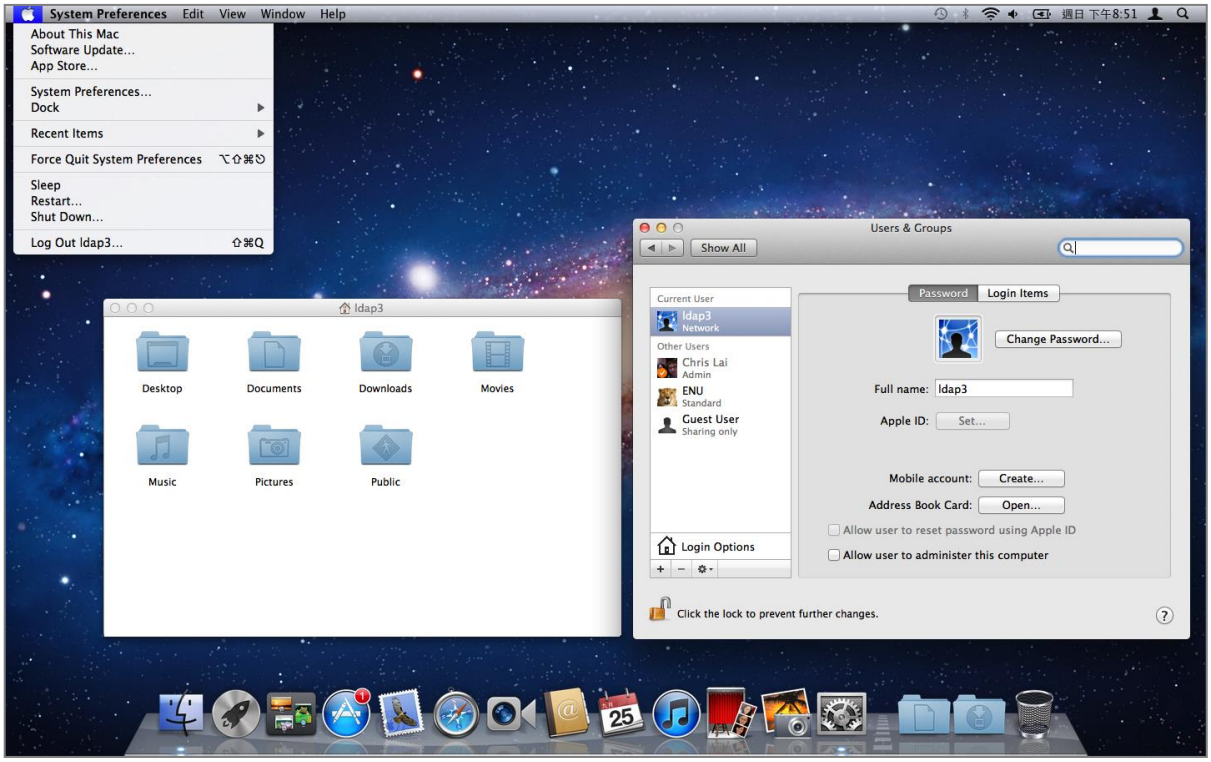
Log in to Mac OS X Using LDAP User Credentials

After Mac clients' home folders for LDAP users are properly mounted, your Mac will automatically mount the home folder for your LDAP user account upon login, and you can start storing documents, preference settings, and other information in your home folder.

To log in to Mac OS X using LDAP user credentials:

Start up your Mac. When you see the login window, enter your LDAP user's name (such as *ldap3*) and password in the fields, and then click to log in.

Now you can open Mac Finder to store files in your home folder and modify preference settings.



Learn More

For more information or online resources about your Synology NAS, please visit **www.synology.com**.