Synology®

Administrator's Guide for

Synology Directory Server

Based on

Synology Directory Server 4.4

Table of Contents

Chapter 1: Introduction

About Synology Directory Server

Synology Directory Server provides a centralized platform for account and resource management services powered by Samba schema. It supports commonly used Windows Active Directory® features, including user/group management, organizational units (OUs), group policies, Kerberos-based authentication, and the deployment of diverse client devices. With the domain service set up by Synology Directory Server, you can securely store a directory database, manage user accounts, and deploy devices based on your organization structure.

Synology Directory Essentials

This section provides an overview of Synology Directory service, which will help you clearly understand key knowledge required for performing administrative tasks via Synology Directory Server.

Directory Service

A directory is a repository containing individual persons, groups, locations, and various types of information. It is a tool for data storage and management, allowing users to easily find the information they want to access. In computer science, a directory service stores all account information in a centralized location. This service allows multiple resources to work together, which thus makes itself ideal for authorizing users' access, configuring identities, and managing the relationships among users and groups.

Active Directory® and Synology Directory Service

Active Directory® (AD) is a type of directory service that offers a centralized database of information with which IT administrators can securely manage accounts and resources, such as computers and printers. Synology Directory Server provides the AD-based **Synology Directory service**, allowing you to store and deploy resources on an intuitive interface.

Domain Name System (DNS)

Synology Directory service adopts the Domain Name System (DNS) to organize computers, printers, or other resources into a hierarchical structure.

A domain is a logical boundary set up for the creation and management of resources, while DNS is a standard Internet service that structures resources through domain names. In a domain (e.g., "syno.local"), devices are deployed through DNS, which helps resolve their easily readable hostnames (e.g., "pc1.syno.local") into IP addresses needed for locating and identifying devices with Internet protocols.

With a high dependency on DNS, it is necessary to set up a DNS server to maintain the functionality of domain when installing Synology Directory Server.

Domain Controller

A domain controller (DC) is a NAS that hosts a Synology Directory Server's domain. It is responsible for maintaining domain functionality, storing directory data, and managing user interactions within a domain.

In Synology Directory Server, the Synology NAS where a domain is created will be automatically promoted as a domain controller.

Domain Object

The domain database stored in Synology Directory Server is made up of information about objects, each of which represents a single and unique entry in the database. The following are the objects that can be managed in Synology Directory Server:

- **User**: A user account that can access resources deployed in a domain.
- **Group**: A manageable unit used to gather domain objects. All members in a group share the same access permissions to files, folders, applications, or devices within a domain.
- **Device**: A physical resource that can be accessed by domain users. It can be a computer, a printer, a NAS, etc.
- **Organizational Unit (OU)**: The smallest container in a domain to which administrative privileges and group policies can be assigned. You can put users, groups, computers in an OU for delegating the same authorities and policies to them. Besides, you can also add an OU to another OU, creating an OU hierarchy that corresponds with the real-world organization structure. In so doing, it will be more efficient to configure domain objects in Synology Directory Server.

Compatibility and Limitations

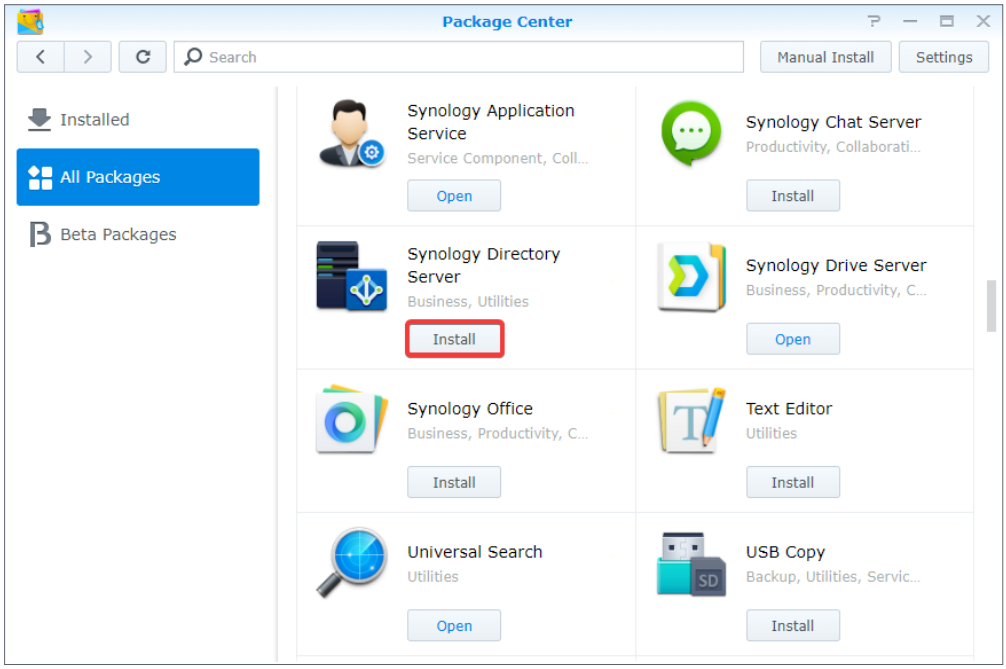
- DSM version requirement: DSM 6.2.2 or above.
- Domain functional level: Equal to Windows Server 2008.
- Synology Directory Server must work with the **DNS Server** package.
- Synology Directory Server is not compatible with configurations of other domain/LDAP services.
- Supported domain clients:
  - Windows 7 or above
  - macOS
  - Linux
- Applied Synology NAS models: See **this page** on the Synology official website.
- Limitations:
  - Synology Directory Server supports a single domain and a single domain controller only.
  - The hostname of the Synology NAS that functions as the domain controller cannot be changed after Synology Directory Server is activated on it.

Install Synology Directory Server

1. Before installing **Synology Directory Server** on the Synology NAS, please check the following:
   - The network connection of Synology NAS works properly.
   - The volume of Synology NAS is working well.
   - The DSM is updated to version 6.2.2 or above.
   - You are the **DSM** admin (or a user belonging to the **administrators** group) of the Synology NAS.
   - **The Synology NAS is using a static IP address**: To avoid clients from being disconnected because of IP address changes of the Synology NAS (domain controller), you need to set up a static IP address on your local area network for the Synology NAS.
   - **The Synology NAS is not a client of any domain or LDAP directory**: If the Synology NAS has already joined a domain or an LDAP directory, it must leave the domain or LDAP directory before using Synology Directory Server. This package is not compatible with configurations of other directory services.
   - **No domain name conflicts exist on the local area network**: Synology Directory Server will not be found by clients if more than one domain has the same name on the local network. To avoid this issue, please choose another name or remove the domains that have the same name.
2. Sign in to DSM as **admin** or a user belonging to the **administrators** group.

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

4. Click **Install** in the **Synology Directory Server** section and follow the onscreen instructions to complete the installation process.



Chapter 2: Get Started With Synology Directory Server

With Synology Directory Server, your Synology NAS can work as a domain controller that manages accounts, deploys devices, configures access permissions, and delegates authority in a domain. This chapter will help you get started with Synology Directory Server.

Set up Synology Directory Service

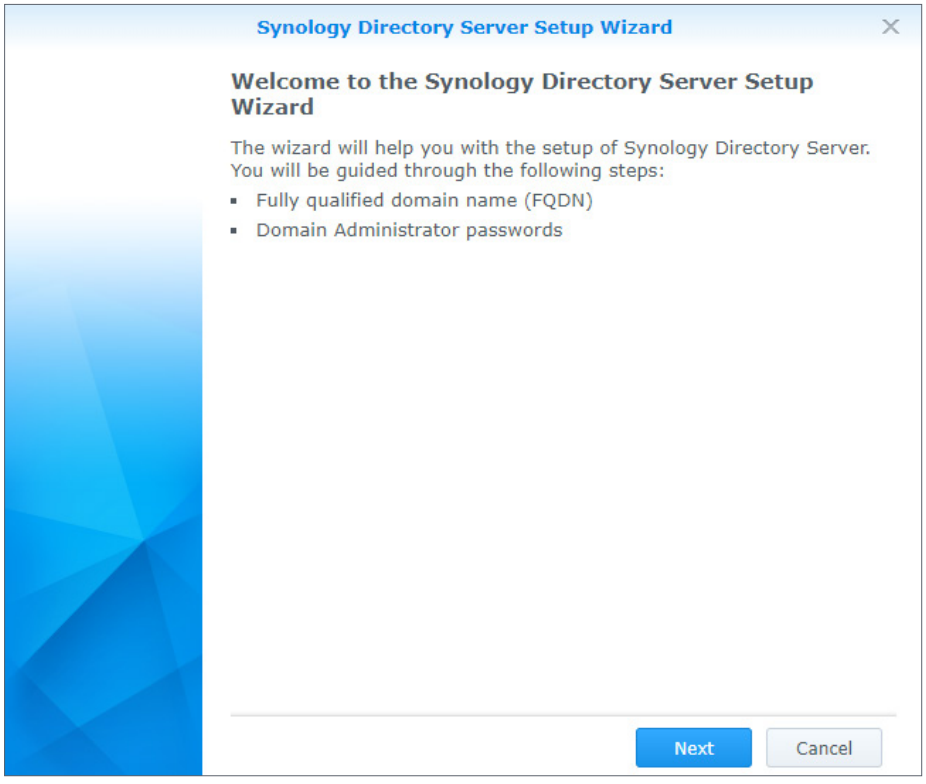
Once the installation is complete and there are no existing domains detected, you can start setting up Synology Directory service. In the section below, we will see how to create a domain and promote the Synology NAS as a domain controller.

Note:

- Before installing Synology Directory Server, you can set up a Synology High Availability cluster to secure an uninterrupted directory service (see the section **Ensure Uninterrupted Directory Service via Synology High Availability** for detailed instructions).

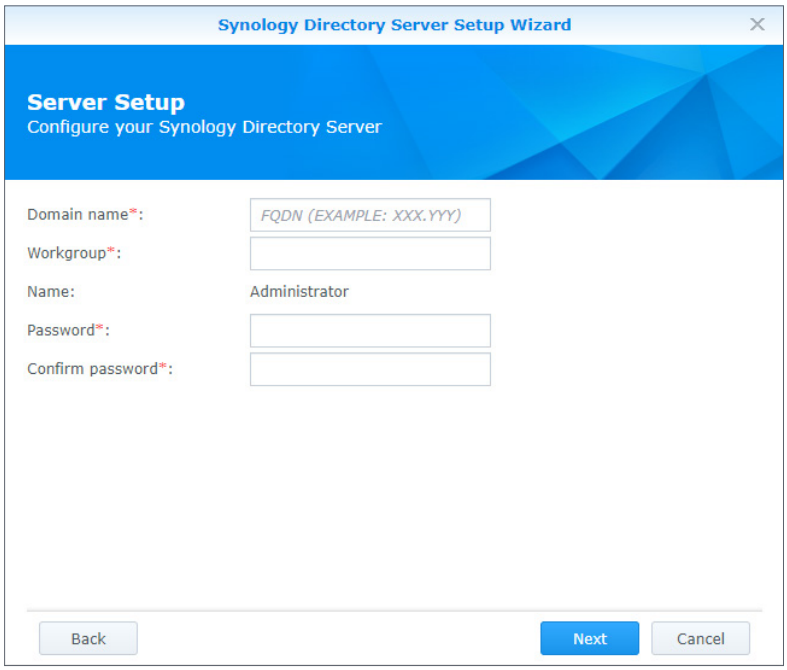
1. Launch **Synology Directory Server**.

2. Click **Next** to continue with the setup.

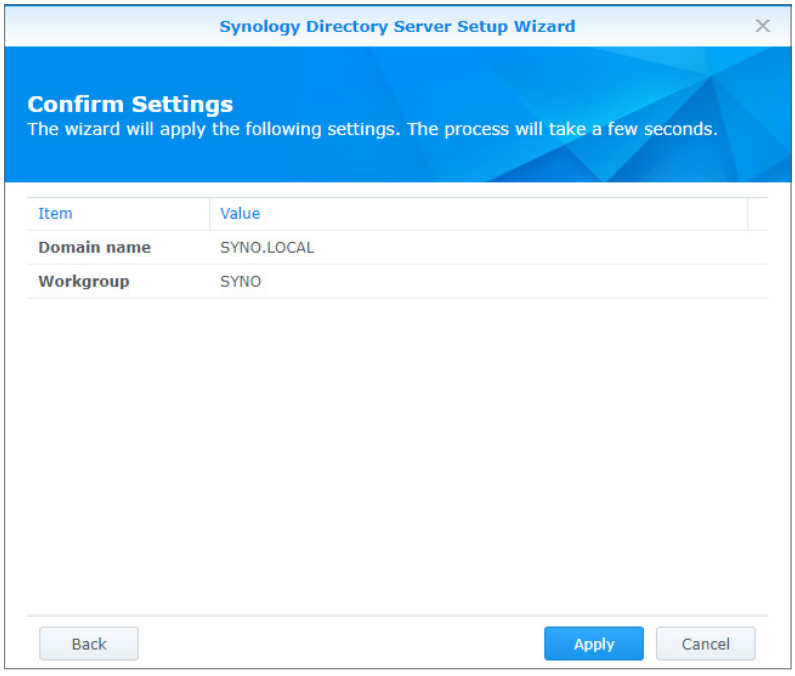


3. Enter the following information and click **Next**:

   - **Domain name**: Enter an FQDN (Fully Qualified Domain Name) for the domain, e.g., "syno.local".
   - **Workgroup**: The workgroup name (or the NetBIOS domain name) will be automatically filled in this field. For instance, if your domain name is "syno.local", the default workgroup name will be "syno".
   - **Password**: Enter a password for the administrator account of your domain.
   - **Confirm password**: Enter the password again.



4. Confirm the settings and click **Apply**. The system will now create the domain and promote the Synology NAS to be a domain controller.



Domain Naming Limitations:

- The domain name can only contain alphabetical characters, numeric characters, minus signs, and dots (only used as the delimiter of domain name's components).
- The domain name must contain at least two components. e.g., "syno.local".
- The domain name cannot start with a hyphen (-).
- The domain name cannot end with a hyphen (-) or a period (.).
- The maximum length is 255 characters.

Password Limitations:

To meet the password strength requirements, your password must comply with **at least three** of the following rules:

- Uppercase letters of the Latin (including A - Z with diacritic marks), Greek, and Cyrillic alphabets.
- Lowercase letters of the Latin alphabets (including a - z with diacritic marks), Greek, and Cyrillic alphabets.
- Numeric characters (0 - 9).
- Special characters, including #, $, !, etc.
- Unicode alphabets, including those in Asian languages.

About SMB Signing:

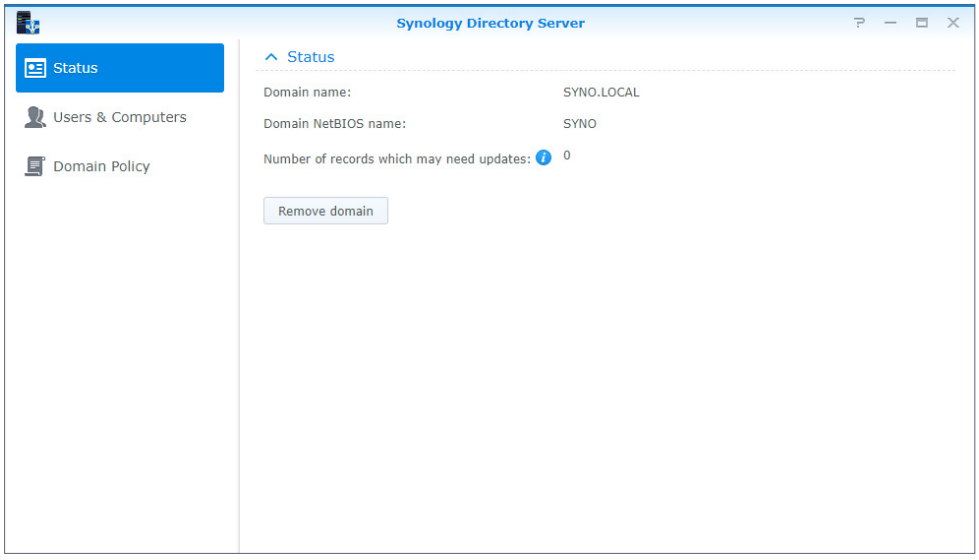
SMB Signing allows SMB communications to be digitally signed at the packet level. After a domain is created, this feature will be enabled automatically, which may reduce read/write performance during SMB file transfers. To enhance performance, please select **Auto** or **Disable** from the **Enable server signing** drop-down menu at **Control Panel** > **Domain/LDAP** > **Domain** > **Domain Options**.

Manage the Domain

On the **Status** page, you can check, edit, or remove your domain and the domain controller.

View Domain Information

Information about your domain can be viewed at any time on the **Status** page:



- **Domain name**: The full name of your domain.
- **Domain NetBIOS name**: The short name for the domain, which will be used by earlier versions of Windows (e.g., Windows 95 or Windows 98) to access Synology Directory resources.
- **Number of records which may need updates**: If the number shown is 0, then all DNS resource records in **DNS Server** correctly point to the IP address of the Synology NAS (domain controller). If the number shown is bigger than 0, then the resource records in **DNS server** require updating (see the section **Adjust A/AAAA Resource Records** for detailed instructions).

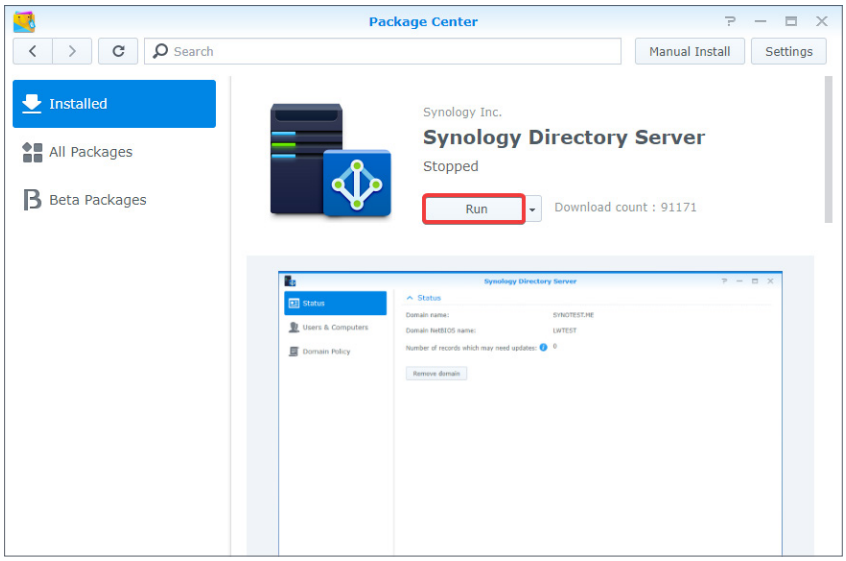
Remove the Domain

On the **Status** page, click **Remove Domain** to remove the domain currently managed by Synology Directory Server. Please note that removing the domain is **irreversible**.

Edit the IP Address of Domain Controller

Synology Directory Server is normally set up with a static IP address. For certain reasons, you may need to change the IP address of the Synology NAS that is running Synology Directory Server. Please follow the steps below:

1. Back up Synology Directory Server with **Hyper Backup** (see the section **Back up and Restore Directory Service via Hyper Backup** for more information).
2. Change the IP address of the Synology NAS.
3. Confirm and update the resource records in **DNS Server** (see the section **Adjust A/AAAA Resource Records** for more information).
4. Restart Synology Directory Server to update the network settings. Please do the following:
   a. Go to **Package Center** > **Installed** > **Synology Directory Server**.
   b. Click the inverted triangle and select **Stop**.
   c. After Synology Directory Server is stopped, click **Run** to restart the package.



Manage DNS Resource Records

Domain Name System (DNS) is a naming system that facilitates the exchange of data between computers over the Internet and other networks. It is mainly used to translate easy-to-memorize domain names (e.g., "pc1.syno.local") into corresponding IP addresses (e.g., "192.168.1.5"). This function is essential for the maintenance of Synology Directory Server's domain service.

The following will guide you through A/AAAA record configurations and the DNS auto-registering mechanism.

A/AAAA Resource Records

A and **AAAA** are both DNS resource records for resolution between domain names and IP addresses. While A records translate domain names into 32-bit IPv4 addresses, AAAA records resolve domain names into 128-bit IPv6 addresses.

DNS Auto Registering

After a client has successfully joined the domain created by Synology Directory Server, the server will automatically register or update an A resource record (and an AAAA resource record if IPv6 is enabled) to the DNS service on DSM, mapping the hostname of the client to an IP address.

Limitations:

- DNS auto registering cannot be disabled.
- **Naming rules of domain clients**: Only letters (a - z, A - Z), numbers (0 - 9) and hyphens (-) are allowed currently.
- **On Windows 7 or 10**: Re-login or restart will be necessary if the hostname or IP address has been changed.
- **On DSM or SRM**: Re-login or restart will **not** be necessary if the hostname or IP address has been changed, and the resource records will not be updated.

Adjust A/AAAA Resource Records

In order for Synology Directory Server to normally deliver services, all A/AAAA resource records in **DNS Server** must correctly point to the IP address of the Synology NAS. By default, all A/AAAA resource records will point to the IP address of the Synology NAS where a domain is created.

However, A/AAAA resource records may not properly point to the Synology NAS due to the following circumstances:

- The Synology NAS undergoes a change in its IP address after the domain has been created with Synology Directory Server.
- Synology Directory Server is restored through a backup task of **Hyper Backup** (see **Back up and Restore Directory Service via Hyper Backup** for more information).

When encountering the cases mentioned above, please follow the steps below:

1. Go to **DNS Server** > **Zones**.
2. Select the specific DNS zone in question such as ***domain name*@Active Directory** or _**msdcs.*domain name*@Active Directory**, and click **Edit** > **Resource record**.
3. Check the IP addresses configured in the A/AAAA resource records. Make sure all the records point to your Synology NAS.

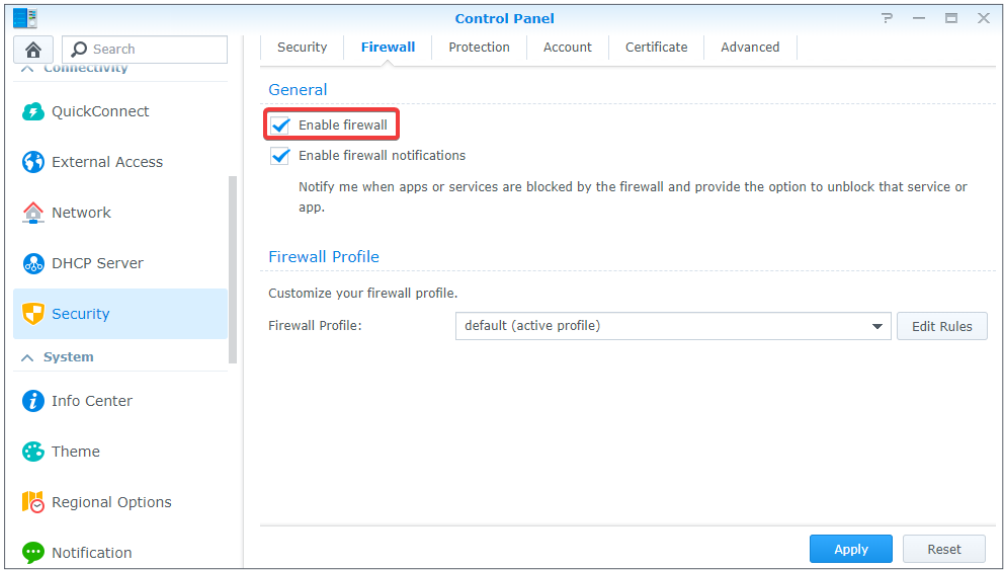
Note:

- To batch edit, you can press and hold **Ctrl** or **Shift** to select multiple resource records of the same type but with different names.

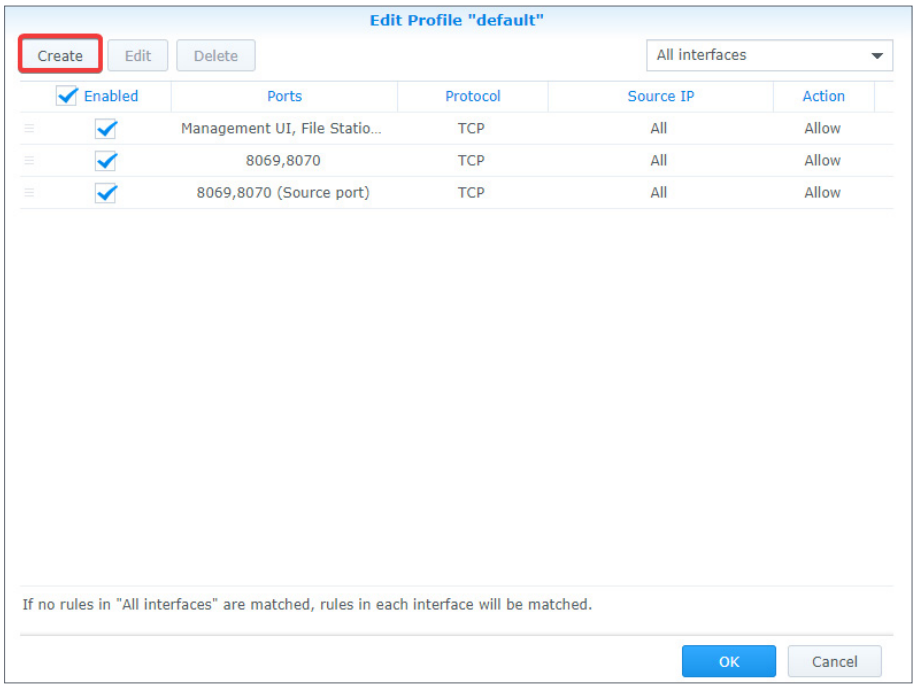
Add Firewall Rules to Secure Directory Service

Security is always one of the greatest concerns for Synology Directory administrators besides efficient management. To protect Synology Directory service, we suggest adding the following firewall rule to your Synology Directory Server:

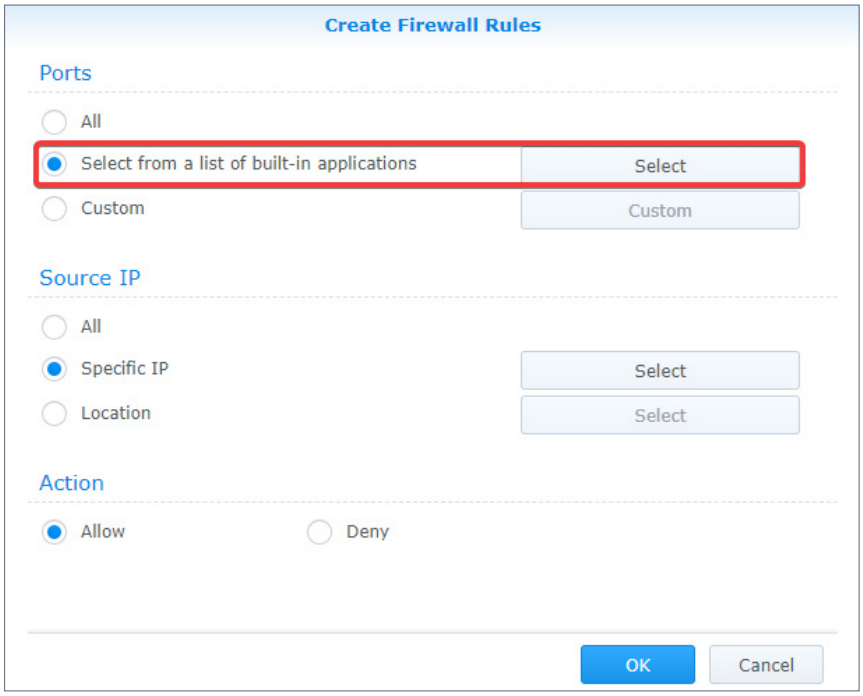
1. Go to **Control Panel** > **Security** > **Firewall**.
2. Tick the **Enable firewall** checkbox.
3. Under the **Firewall Profile** section, select a firewall profile from the drop-down menu and click **Edit Rules** on the right.



4. Click **Create**.

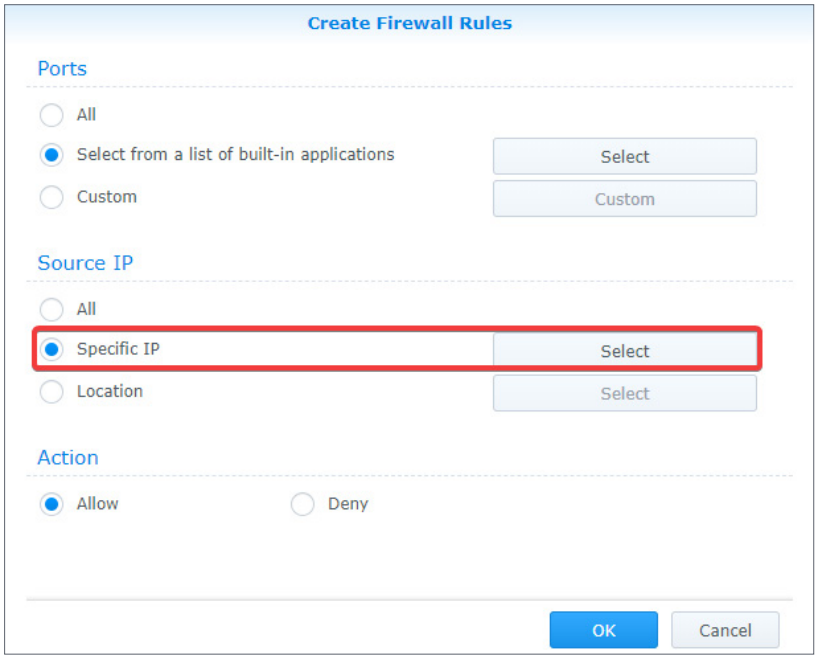


5. Under the **Ports** section, choose **Select from a list of built-in applications** and click **Select**.

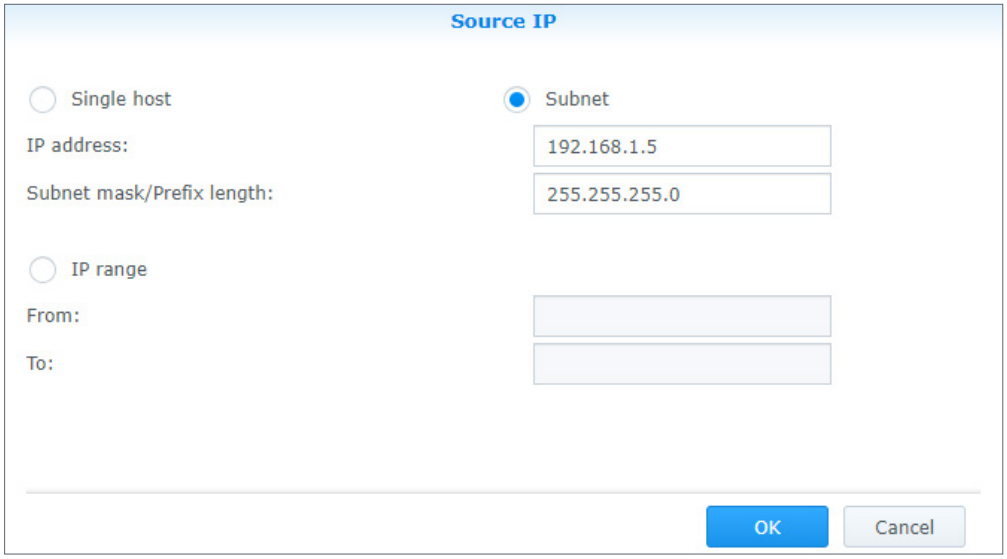


6. Select **DNS Server**, **Synology Directory Server**, and **Windows file server**. Click **OK** to confirm your selection.

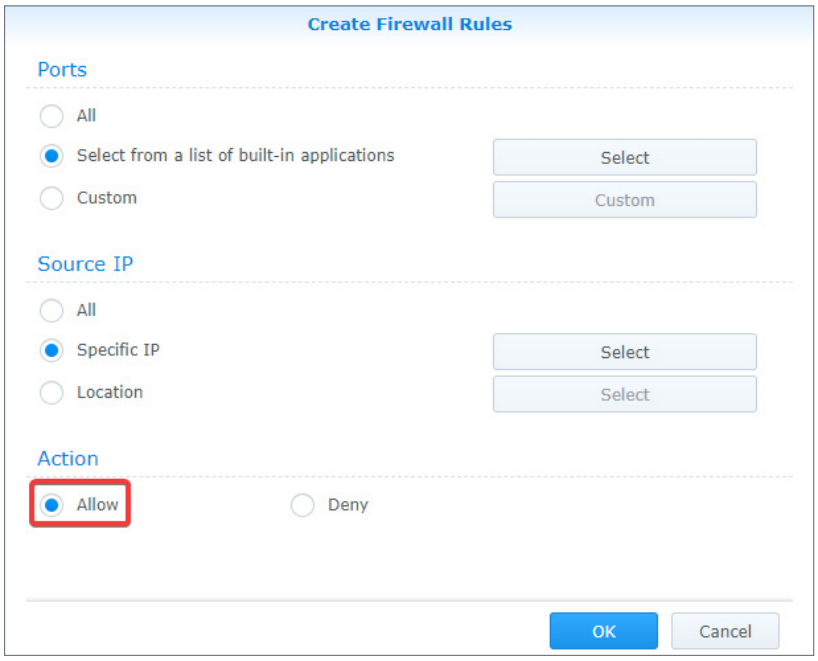
7. Under the **Source IP** section, choose **Specific IP** and click **Select**.



8. Specify the local area network where Synology Directory Server is running by entering an IP address or an IP range. Click **OK** after you confirm the information.



9. Under the **Action** section, select **Allow** to allow access by the ports and IP addresses you have specified.



10. Click **OK** to save the settings.

Note:

- For more information about the firewall settings on DSM, please refer to the **firewall help articles**.

Chapter 3: Manage OUs, Groups, Users, and Computers

In a domain hosted by Synology Directory Server, available resources are created and stored in the form of objects, such as organizational units (OUs), groups, users, and devices (e.g., computers or NAS).

This chapter will show you how to configure different types of domain objects in Synology Directory Server.

View the Status of Domain Objects

On the **Users & Computers** page, you can view the whole tree structure of the domain while object information is shown on the right panel:

- **Type**: The object's type is displayed. Objects can be organizational units, groups, users, or computers.
- **Name**: The name of an object (expect for OUs) will be represented in the following format:

```
Domain NetBIOS name\object name
```

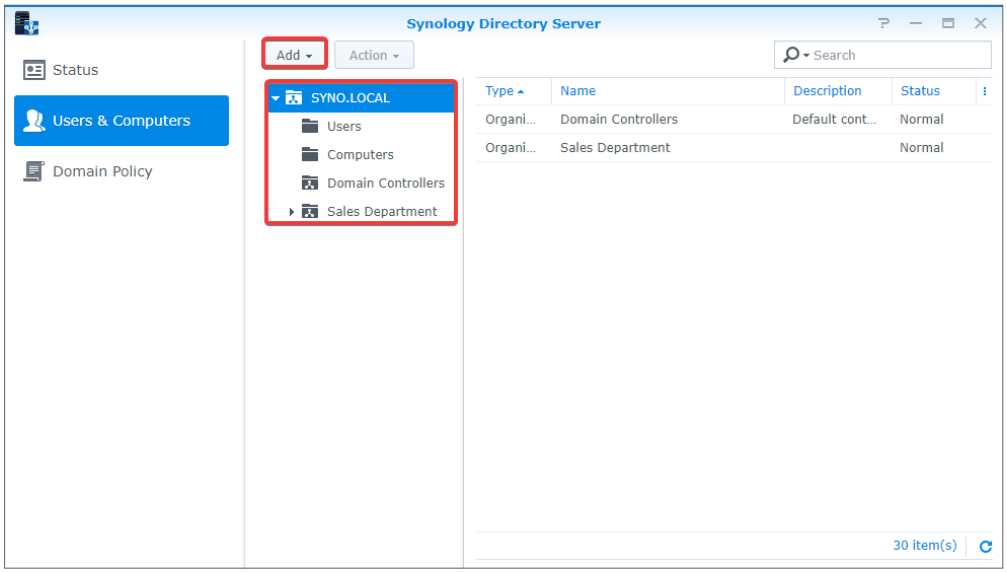
- **Description**: A note that describes the domain object.
- **DN**: The DN (distinguished name) is the path of an object in the domain database. For example, if a user's DN is "CN=bach,OU=sales,DC=syno,DC=local", you can analyze its elements as below:
  - **CN**=bach: The name of this user is "bach".
  - **OU**=sales: This user belongs to the organizational unit "sales".
  - **DC**=syno,**DC**=local: This user is in the domain "syno.local".
- **Status**: If a domain object is not deactivated, its status will be **Normal**. Otherwise, the status will be **Disabled**.

Manage Organizational Units (OUs)

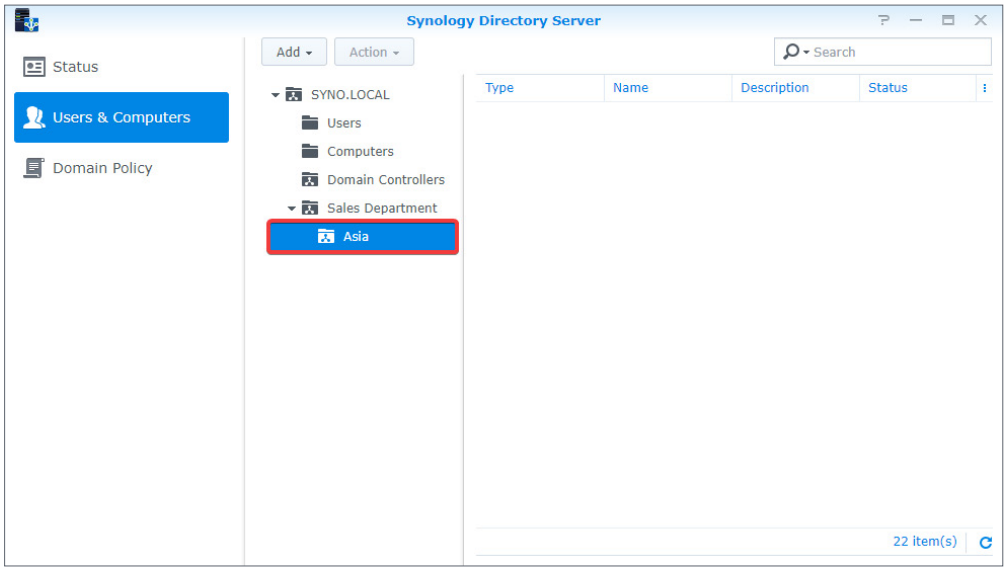
An organizational unit (OU) is a container object within a domain to which you can add all types of domain objects, including users, groups, computers, and other OUs. OUs organize domain objects into a hierarchy, which is helpful when there are a large number of users, computers, and groups. With a well-designed OU structure, IT administrators can easily link group policies and delegate administrative tasks to specific domain objects.

Add an OU

1. Go to the **Users & Computers** page.
2. Select the domain or an OU from the tree list, and click **Add** > **Organizational unit**.



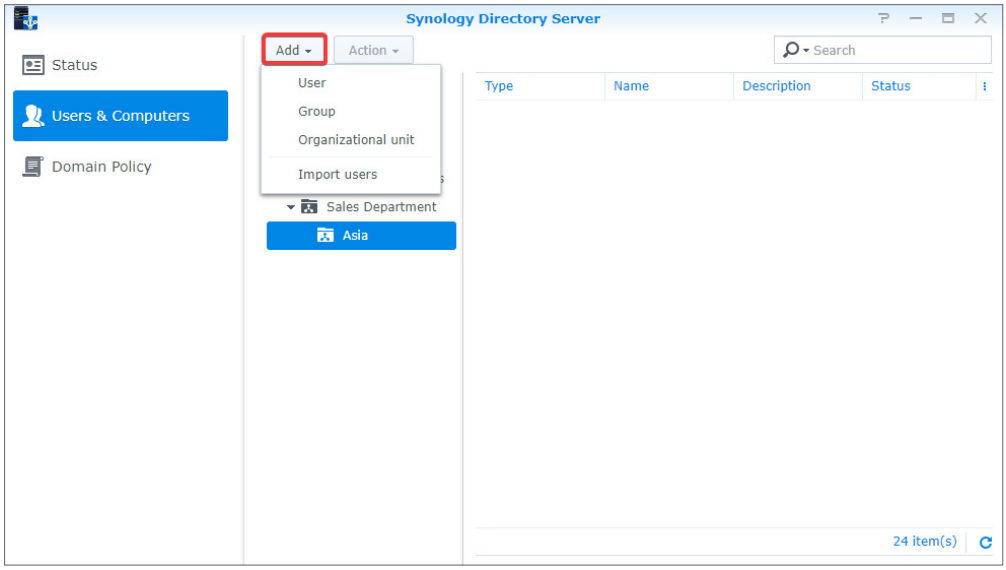
3. Specify a name for the new organizational unit in the field, and click **OK**.
4. Right-click the parent container of the newly added organizational unit, and click **Reload**. The newly added organizational unit will then show on the tree list.



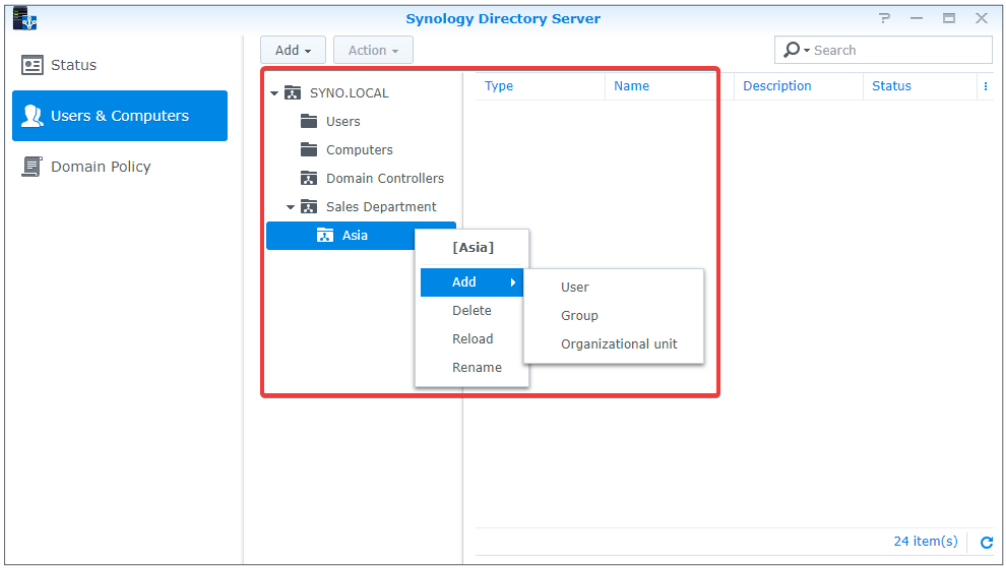
Add Objects to an OU

You can do the following to add objects to an OU:

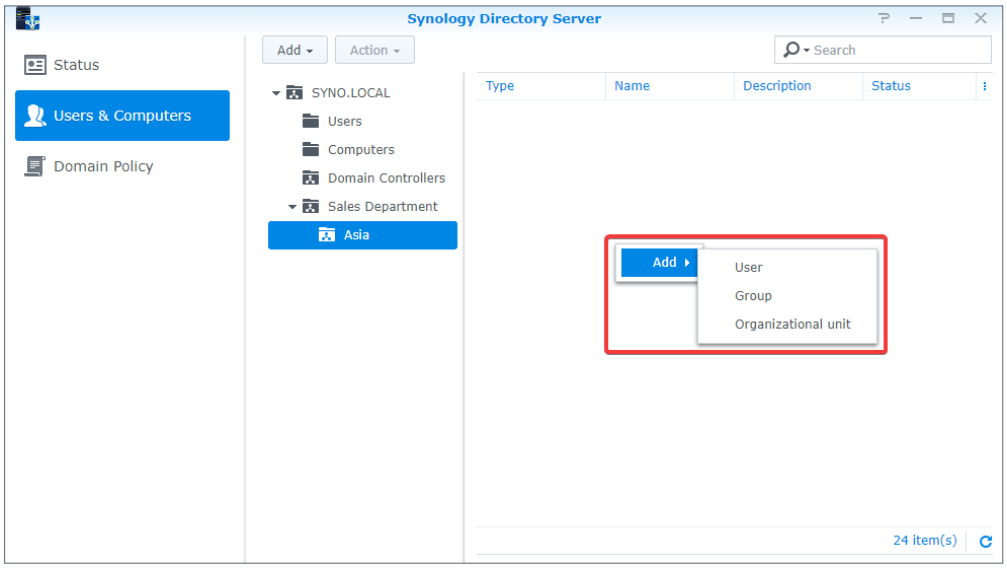
1. On the **Users & Computers** page, select an OU from the tree list.
2. Select one of the methods below to launch the creation wizard:
   - **Method 1**: Click **Add** and select a type of domain object from the drop-down menu.



   - **Method 2**: Right-click the specified OU on the tree list. Go to **Add** and select an object type.



- **Method 3**: Right-click the blank space of the specified OU and select an object type to add.



3. Follow the instructions in the creation wizard to add the object. Please go to the sections **Add an OU**, **Add a Group**, and **Add a User** for more operation guidelines.

Note:

- You can drag and drop one or more objects to an organizational unit listed on the tree list.
- The default view mode of directory only shows the objects not belonging to any organizational units. To view all users, groups, computers, and organizational units, select the root folder (named after your domain) from the tree list and click the magnifying glass icon on the upper-right corner. In the search bar, tick **All descendants** to display all objects.

Delete an OU

1. Right-click the OU you wish to delete from the tree list and click **Delete**.
2. Click **Delete** again in the pop-up message to confirm the deletion. Please note that the deletion of OUs is **irreversible**.

Manage Groups

Domain groups allow IT administrators to grant permissions to access devices, applications, or other services deployed in a domain. You can place domain users into a group and then apply an access control list (ACL) to the group for a specific service. This section will provide you the guidelines on how to manage domain groups in Synology Directory Server.

Default Groups

When you establish a domain, Synology Directory Server creates the following groups by default to help you manage the domain and configure access permissions:

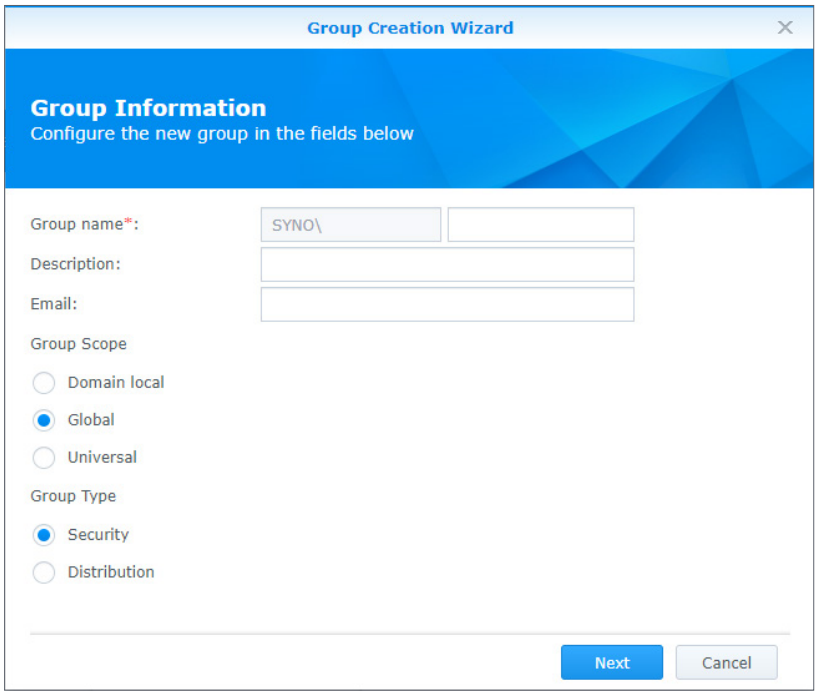
Group Name	Description
Domain Admins	Members of this group have administrative privileges to control all objects and settings in the domain.
Enterprise Admins	Members of this group have administrative privileges to control all objects and settings in the entire enterprise's domain structure.
Schema Admins	Members of this group can make changes to the domain schema.
Domain Guests	All domain guests are included in this group by default.
Domain Users	All domain users are included in this group by default.
Domain Computers	All workstations and servers are included in this group by default.
Domain Controllers	All domain controllers are included in this group by default.
Read-Only Domain Controllers	All read-only domain controllers (RODCs) are included in this group by default.
Enterprise Read-Only Domain Controllers	All read-only domain controllers (RODCs) in the entire enterprise's domain structure are included in this group by default.
Allow RODC Password Replication Group	Members of this group can replicate their passwords to all RODCs in the domain.
Denied RODC Password Replication Group	Members of this group cannot replicate their passwords to any RODCs in the domain.
Cert Publishers	Members of this group are given privileges to certificate publishing.
DnsAdmins	Members of this group can access domain name service in the domain.
DnsUpdateProxy	Members of this group are DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).
Group Policy Creator Owners	Members in this group can modify group policies for the domain.
RAS and IAS Servers	Members of this group are allowed to use remote access services.

Note:

- Synology Directory Server aligns with the functional level of Windows Server 2008 R2. Please refer to **this article** for more information about the built-in domain groups.

Add a Group

1. Click **Add** > **Group** on the **Users & Computers** page.
2. Enter a name in the **Group name** field, configure the following information for the new group, and click **Next**:
   - **Group Scope**
     - **Domain local**: Domain local groups are used for assigning permissions to resources in their home domain. This type of group can nest other domain local groups in the same domain. It can also contain user accounts, global groups, and universal groups from any domains or forests.
     - **Global**: Global groups are added for the management of user accounts. It can contain user accounts and other global groups in the same domain. In practice, we suggest placing global groups into domain local groups that are granted certain permissions instead of directly assigning permissions to them.
     - **Universal**: Universal groups are mainly used to nest global groups across domains. It can contain user accounts, global groups, and other universal groups from any domains in the forest where this universal group is located. In practice, we suggest placing universal groups into domain local groups that are granted certain permissions instead of directly assigning permissions to them.
   - **Group Type**
     - **Security**: Security groups are adopted to set up access permissions or rights to perform certain system tasks in the domain.
     - **Distribution**: Distribution groups are adopted for sending email messages to a collection of users. It can be used as an email alias.



3. Confirm the group information and click **Apply** to save the settings.

Edit Group Properties

1. Select the group you wish to edit, and click **Action** > **Edit**. The following group properties at the **General** tab are available for editing:
   - Group name
   - Description
   - Email
   - Group Scope
   - Group Type
2. Include or exclude members at the **Members** tab.
3. Click **OK** to save.

Note:

- You can also edit a group by right-clicking a group on the **Users & Computers** page and then clicking **Edit**.

Delete a Group

1. Select a group you wish to delete on the **Users & Computers** page, and click **Action** > **Delete**.
2. Click **Delete** in the pop-up message to confirm the deletion.

Note:

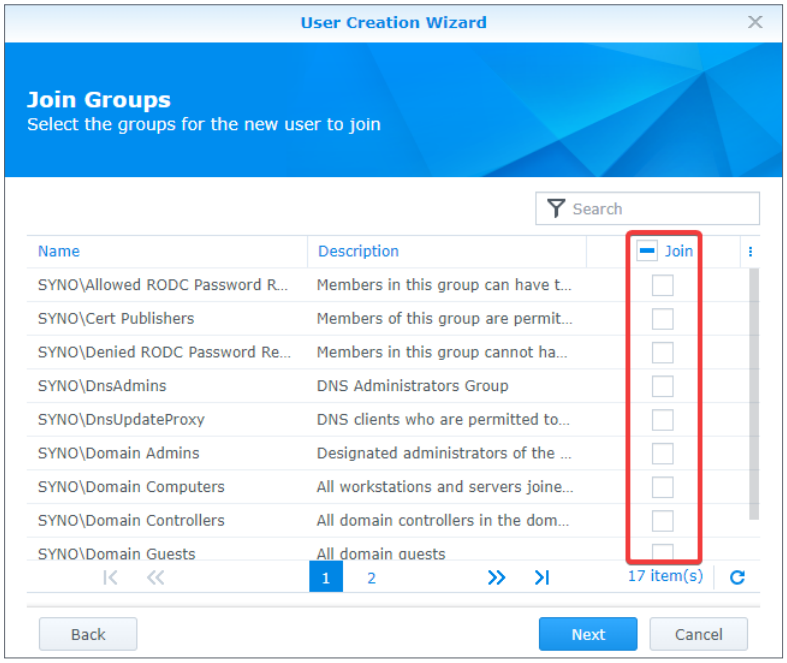
- You can also delete a group by right-clicking a group on the **Users & Computers** page and then clicking **Delete**.
- You can select multiple groups by pressing and holding the **Ctrl** or **Shift** key.
- The deletion of groups is **irreversible**.

Add Members to Groups

There are three methods to assign users to groups: by adding a user to groups during the user creation process, by editing a user's profile, and by editing group properties.

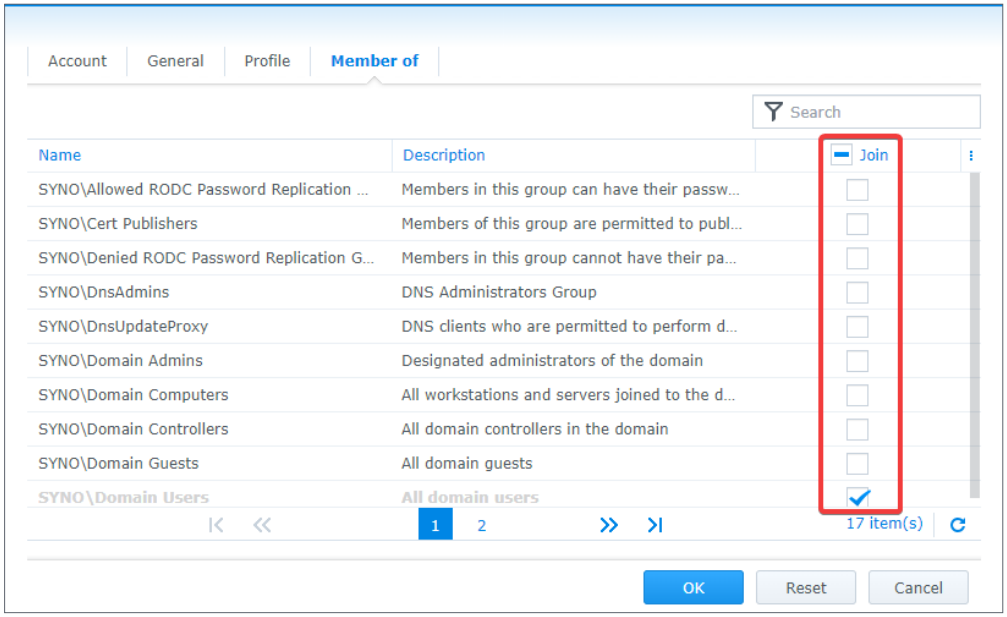
- **Add users to groups during the user creation process**

In the second step of the **User Creation Wizard**, tick the groups to which you wish to add this user and click **Next**. Follow the wizard to complete the user creation process.



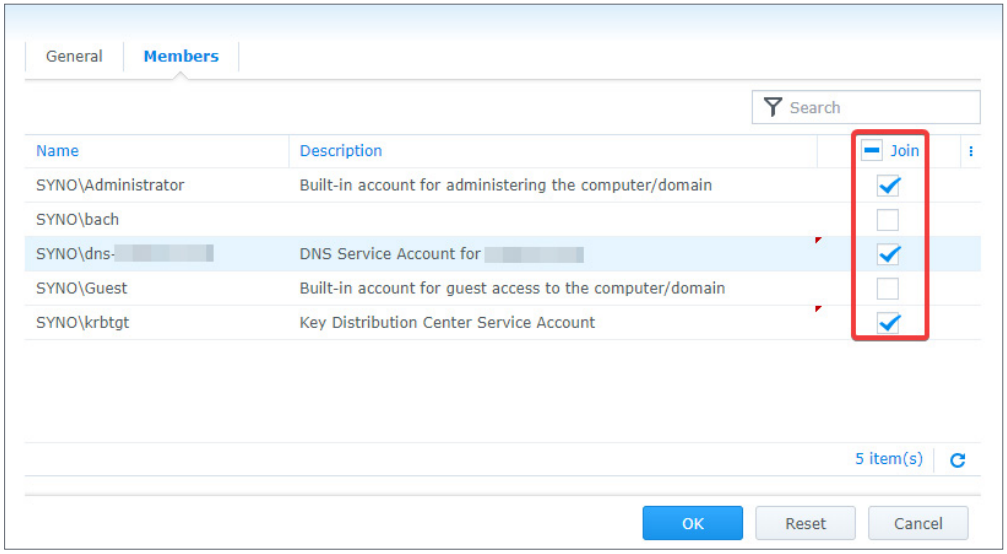
- **Add users to groups by editing user profiles**

Select the user you wish to edit on the **Users & Computers** page, and click **Action** > **Edit**. Switch to the **Member of** tab. Subsequently, tick the groups to which you wish to add this user and click **OK**.



- **Add users to groups by editing group properties**

Select the group you wish to edit, and click **Action** > **Edit**. Go to the **Members** tab and tick the users you wish to add to this group. Click **OK** to save and apply the settings.



Manage Users

Users in a domain are user accounts that can access resources in the domain. Members of your organization can use their user accounts to access domain-integrated resources according to their permissions and privileges.

This section will provide you the guidelines of managing domain users in Synology Directory Server.

Default Users

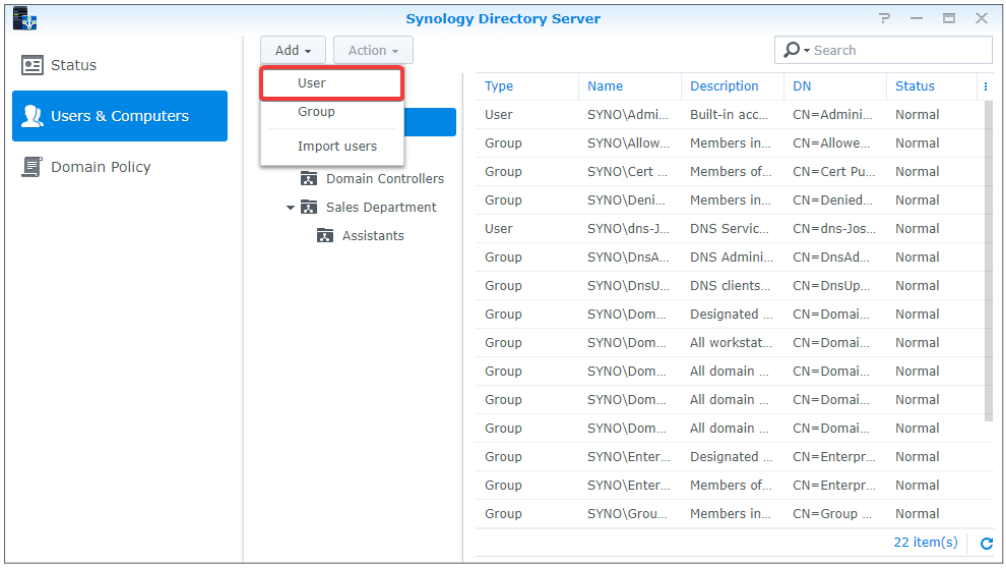
When you establish a domain, Synology Directory Server creates the following user accounts by default to help you manage the domain:

Username	Description
Administrator	The administrator account that has full control of Synology Directory Server. It is used for managing the domain and domain controller.
dns-*NAS hostname*	The DNS service account for the Synology NAS. It is named according to the hostname of the domain controller, e.g., "dns-MyNAS".
Guest	The account for guest access to the domain and deployed devices.
krbtgt	The account for the Kerberos Key Distribution Center service on the domain controller.

Add a User

1. On the **Users & Computers** page, click a container from the tree list you want to add users to. The container can be the container named after your domain (e.g., "SYNO.LOCAL"), the **Users** container, or an organizational unit.

2. Select **User** from the **Add** drop-down menu. The user creation wizard will be launched automatically.



3. In the **User Creation** wizard, configure the new user on the **Enter user Information** page. To enhance security, **Force this account to change password at next login** is automatically ticked by default. Kindly note that password strength requirements depend on the password policy configured at **Synology Directory Server** > **Domain Policy**.

4. Select the groups to which the user belongs on the **Join groups** page.

5. Confirm the settings and click **Apply** to add the domain user.

Note:

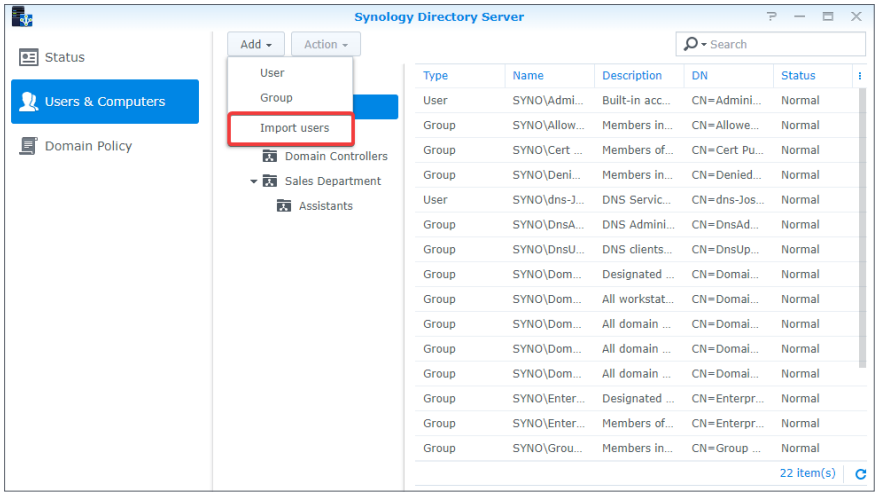
To meet the password strength requirements, your password must comply with **at least three** of the following rules:

- Uppercase letters of the Latin (including A - Z with diacritic marks), Greek, and Cyrillic alphabets.
- Lowercase letters of the Latin alphabets (including a - z with diacritic marks), Greek, and Cyrillic alphabets.
- Numeric characters (0 - 9).
- Special characters, including #, $, !, etc.
- Unicode alphabets, including those in Asian languages.

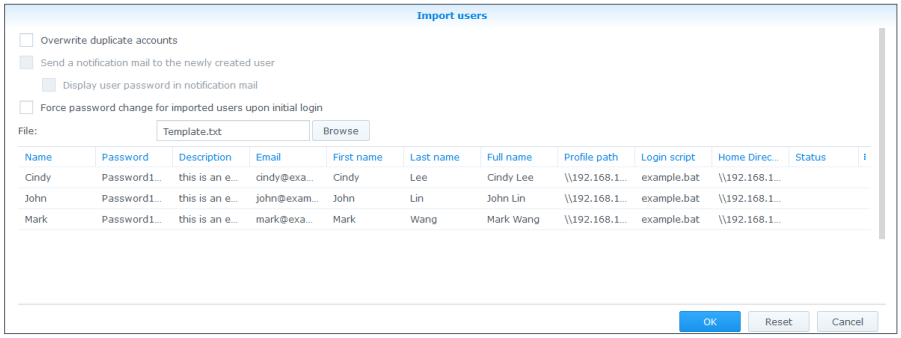
Import Multiple Users

Besides adding one user at a time, you may also import multiple user accounts by following the steps below:

1. On the **Users & Computers** page, click a container from the tree list you want to add users to. The container can be the container named after your domain (e.g., "SYNO.LOCAL"), the **Users** container, or an OU.
2. Click **Import users** from the **Add** drop-down menu.



3. Tick the following options according to your needs:
   - **Overwrite duplicate accounts**: Tick this option if you wish to replace the duplicate accounts with the ones existing in the user list.
   - **Send a notification mail to the newly created user**: Tick this option to send a notification mail to the user whose account is newly created. This option requires enabling system email notifications at **Control Panel** > **Notification** > **Email**.
   - **Display user password in notification mail**: This option is available when **Send a notification mail to the newly created user** is ticked. Tick this option if you wish to display the password in the notification message.
   - **Force password change for imported users upon initial login**: Tick this option if you wish to force imported users to change their password upon the initial login. This option adds extra protection to imported accounts.
4. Click **Browse** to select a .txt file to upload.
5. Confirm the preview is correct and click **OK** to import.



File Format:

When you prepare a file to import, place each user account on an individual row. Each piece of information should be separated by a **Tab** key in the following order:

1. Username 2. Password 3. Description 4. Email
5. First name 6. Last name 7. Full name
8. Profile path 9. Login script 10. Home directory

The format of an import file should meet the following requirements:

- The import file must be in UTF-8 format.
- The order of columns must be correct (from left to right).
- The imported passwords must comply with the password policy.
- Each line of information must contain nine tabs. If you want to skip a piece of information (e.g., **Description**), you still need to enter a **Tab** key to separate the empty value from the next value (e.g., **Email**).

Edit User Properties

1. Select the user you wish to edit on the **Users & Computers** page, and click **Action** > **Edit**. You can select multiple users by pressing and holding the **Ctrl** or **Shift** key.
2. Go to the **Account** tab in the editor window and the following user properties are available for editing:
   - **User login name**: You can rename this user in this field.
   - **Login Hours**: Click this button to customize logon hours of the user. In the configuration window, click **Deny** or **Allow** and select any grid cells. To select the entire day or hour in each day, click the day or hour. After arranging the schedule, click **OK** to save the settings.
   - **Usable Devices**: Click this button to select which computers this user can access.
   - **Lock out this account**: This option is enabled when an account is locked out because of account lockout policies. You can unlock the locked account by disabling this option.
   - **Force this account to change password at next login**: This account will be asked to change the password upon next login to Windows or Synology NAS.
   - **Disallow the user to change password**: This user will not be able to change the password on their own.
   - **Password never expires**: The user's password will never expire. We suggest enabling this option only for administrators.
   - **Store passwords using reversible encryption**: Enabling this option will compromise domain security. This option is not recommended unless demands of domain client services take higher priority over password security.
   - **Disable this account**
   - **Require smart card for interactive login**
   - **Disallow delegation of this sensitive account**: Services on client devices of the domain will not be able to access resources on behalf of this account.

- **Use DES encryption for this account**: The credentials of this account will be encrypted through DES (Data Encryption Standard) during Kerberos authentication.
- **Exempt this account from Kerberos preauthentication**

3. Go to the **Profile** tab and edit properties of **User Profile**, which allows the user to have a consistent desktop experience whenever they access a device deployed in the domain:
   - **Profile path**: The folder path which contains a user's profile, such as the **Desktop**, **Document**, and **Picture** folders.
   - **Login script**: A script is automatically executed when a user signs in to the Windows operating system. You can upload a Windows .bat file of 2 MB or less by clicking **Upload File**.
4. At the **Profile** tab, you can also add a **Home Directory** for the user:
   - **Local path**: Set a specific local folder as a home directory.
   - **Connect...to**: Set a specific remote shared folder on the Synology NAS as a home directory. The remote shared folder will be automatically mounted with a specific volume label of a drive by the Windows operating system if this option is selected.
5. Click **OK** to save the settings.

Note:

- You can also edit a user account by right-clicking a user on the **Users & Computers** page and then clicking **Edit**. The **Disable** option (for disabling a user account) is also available when you right-click the user.

Delete a User

1. Select a user you wish to delete on the **Users & Computers** page, and click **Action** > **Delete**.
2. Click **Delete** in the pop-up message to confirm the deletion.

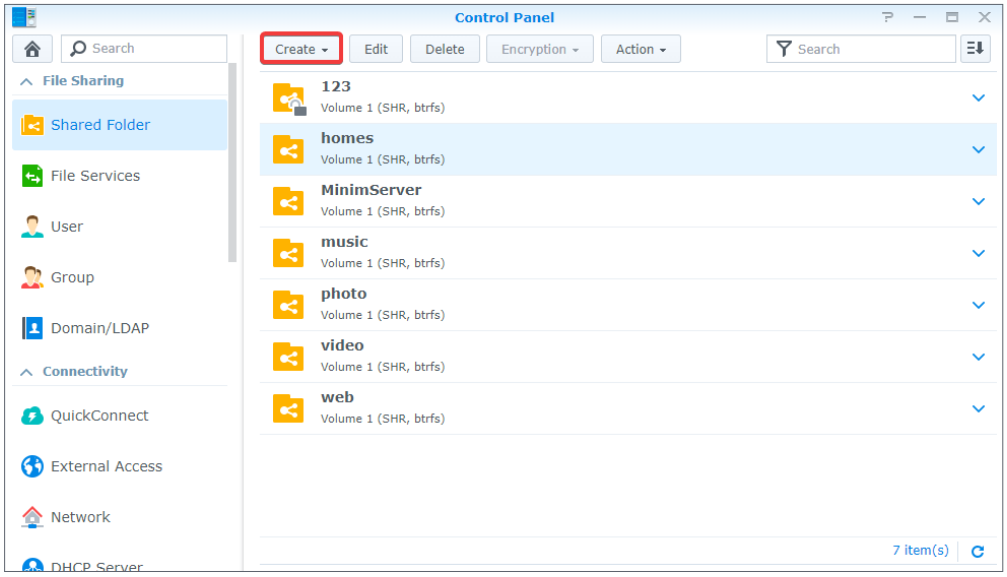
Note:

- You can also delete a user account by right-clicking a user on the **Users & Computers** page and then clicking **Delete**.
- You can select multiple users by pressing and holding the **Ctrl** or **Shift** key.
- The deletion of users is irreversible.

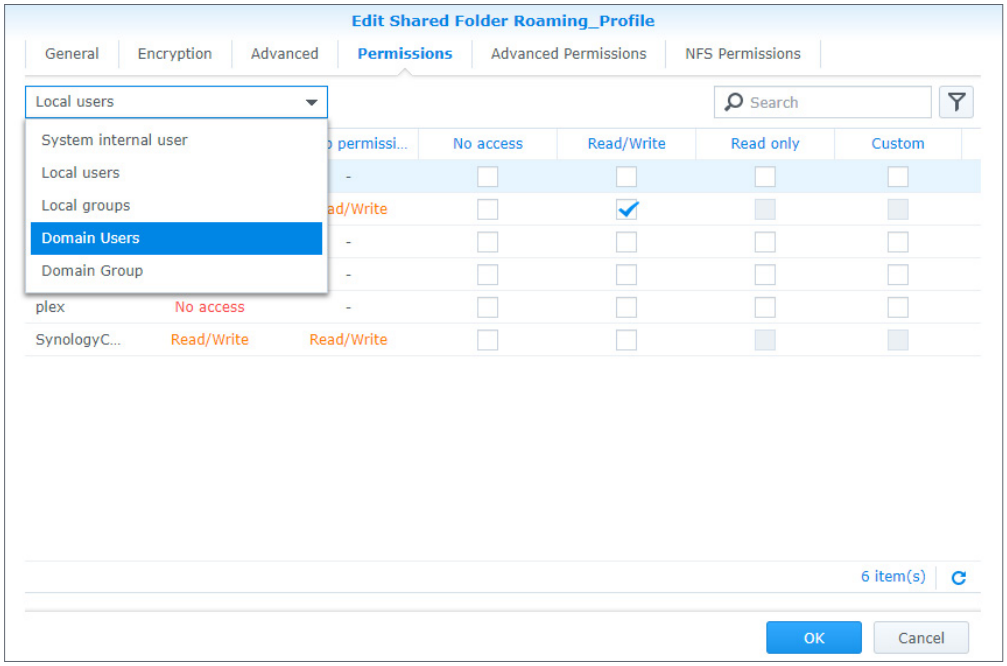
Assign a Roaming Profile for a Single User

Assigning roaming profiles allows domain users to access their files when they sign in to different computers joined to the domain. Before assigning a roaming profile to a user, you must create a shared folder and join at least one computer to the domain first. Please follow the steps below:

1. Join a computer to the domain (see the section **Join Windows PCs to a Domain**).
2. Go to DSM **Control Panel** > **Shared Folder** to create a shared folder. Please note that shared folders for a single user and for all users should not be the same.



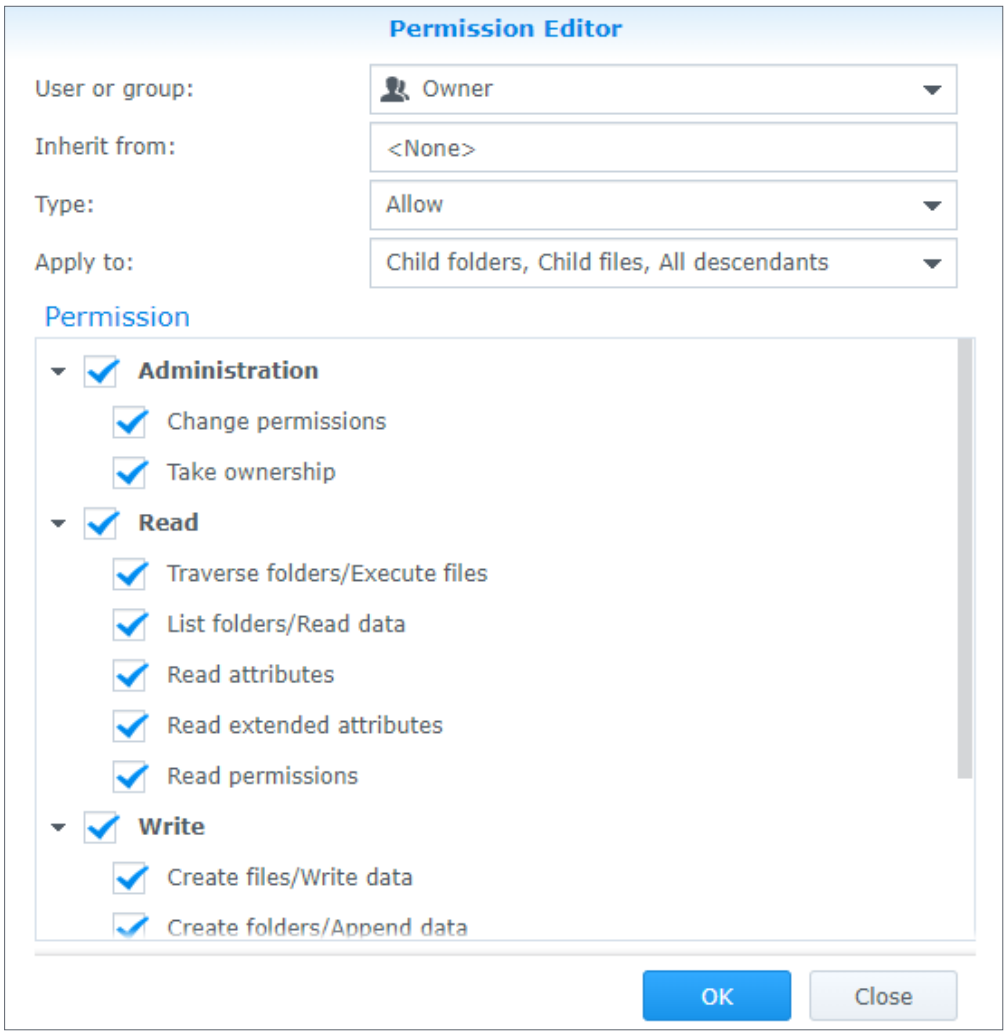
3. Right-click the created shared folder and click **Edit**.
4. At the **Permissions** tab, select **Domain Users.**



5. Tick the **Custom** checkbox, and the **Permission Editor** window will be displayed.

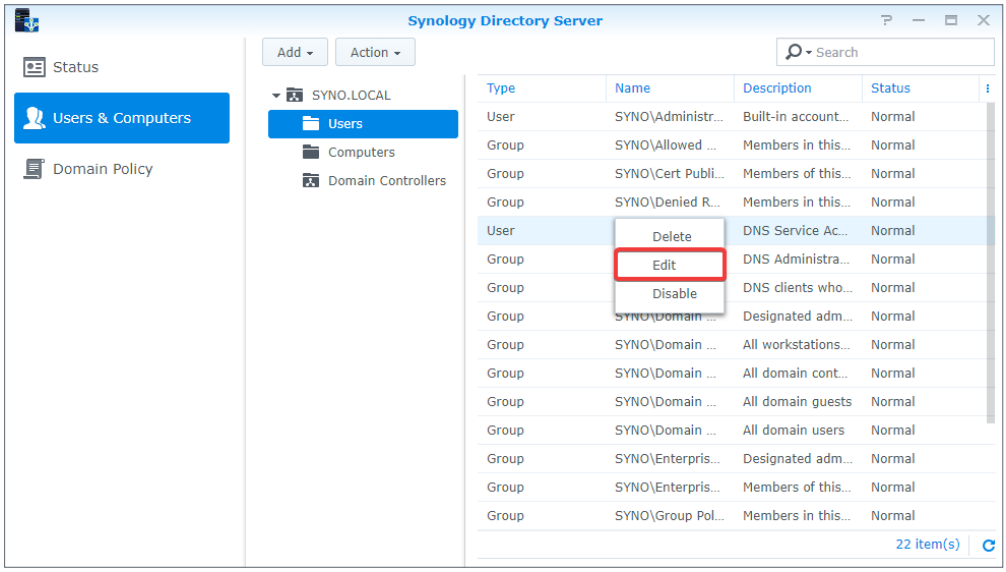
6. Select a target from the **User or group** drop-down menu, and set **Apply to** and **Permission** by following the settings in the table below. The image below is an example of how to set permissions for a user-defined group named "Owner".

User or group	Apply to	Permission
User-defined group (e.g., "Owner")	Tick **Child folders**, **Child files**, and **All descendants**.	Tick **Administration**, **Read**, and **Write** for full control.
Domain Admins	Select **All**.	Tick **Administration**, **Read**, and **Write** for full control.
Domain Users	Select **All**.	Tick **Read** for full read permissions and only **Create folders/Append data** under **Write**.



7. After setting up the shared folder, go to **Synology Directory Server** > **Users & Computers** > **Users**.

8. Right-click a domain user account and click **Edit**.

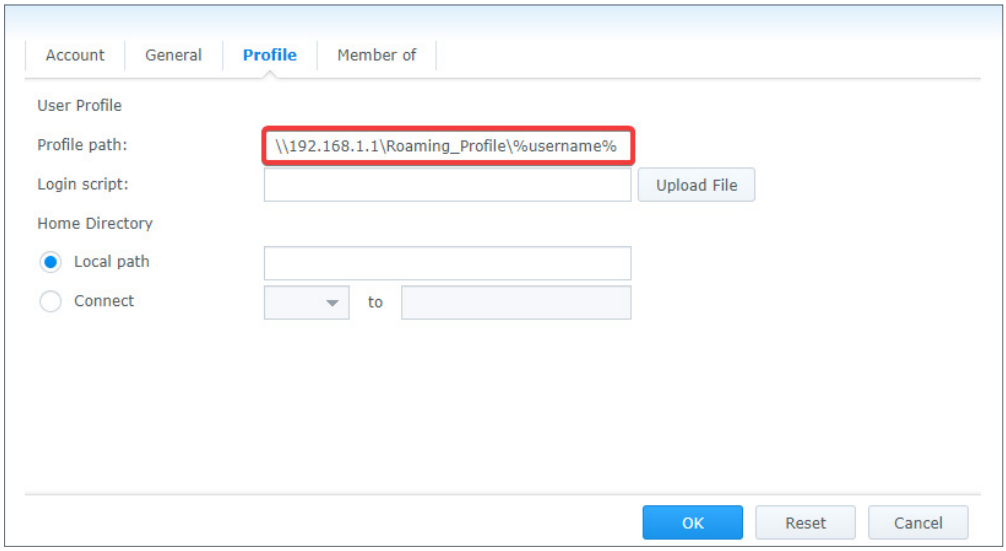


9. Switch to the **Profile** tab, enter a shared folder's path for the user's roaming profile in **Profile path** in the following format, and click **OK**:

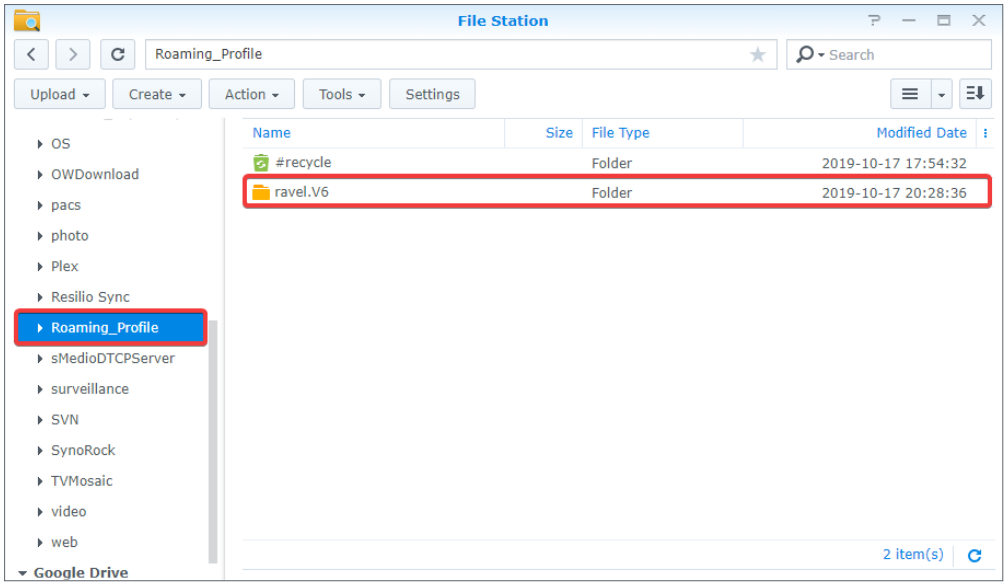
```
\\IP address of NAS\shared folder name\%username%
```

Note:

- Please do not modify "%username%", the environment variable that automatically points to the profile folder of the specified user.



10. Sign in to the domain-joined Windows PC with the specified domain user account. The domain controller will automatically create a corresponding roaming profile (the folder name will be "*username*.V6") in the remote shared folder on the NAS. When you sign out from the computer, the data will be synced back to the assigned path if you have created or modified data under the user's profile.



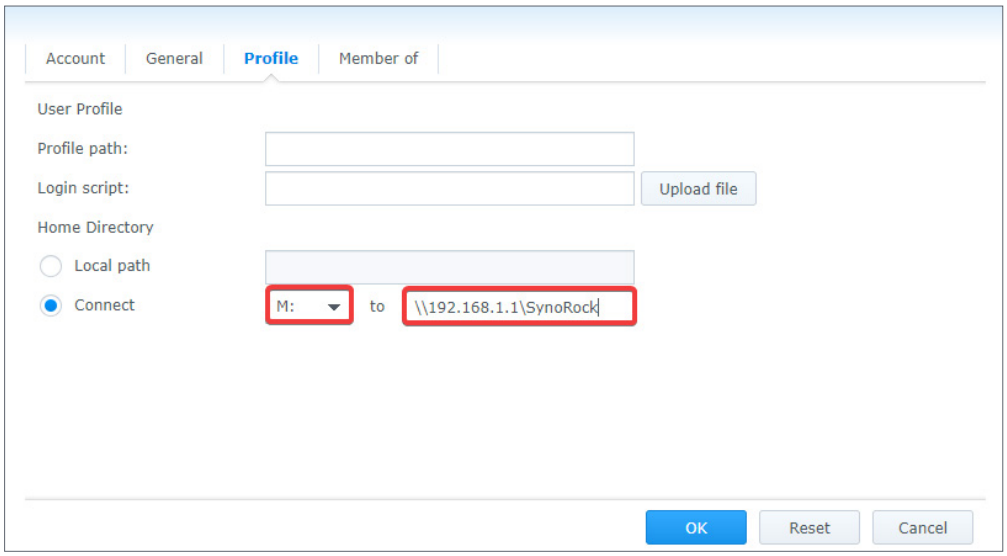
Mount a Network Drive for a Single User

In addition to setting roaming profiles, Synology Directory Server also allows you to mount a network drive for domain users. Please follow the steps below:

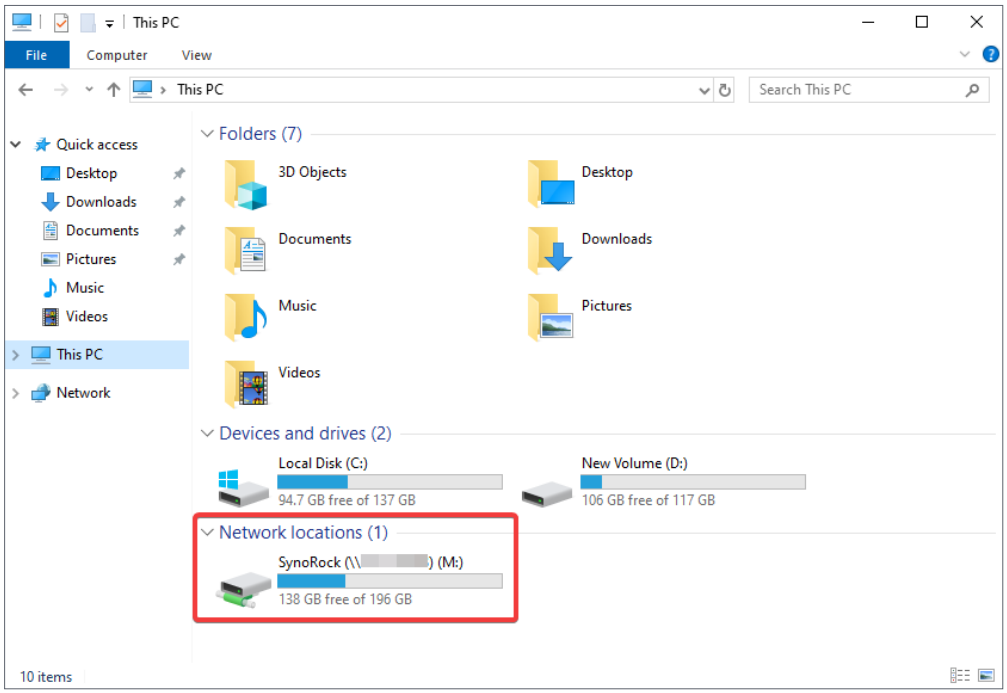
1. Join a user's computer to the domain (see the section **Join Windows PCs to a Domain**).
2. Create a shared folder and set sufficient permissions (at minimal read permissions required) to a domain user on the controller Synology NAS (see the section **Assign a Roaming Profile for a Single User**).
3. Go to **Synology Directory Server** > **Users & Computers**.
4. Right-click the specified user account and click **Edit**.
5. Switch to the **Profile** tab and click **Connect** under the **Home Directory** section.
6. Assign a drive letter for the network drive.
7. Enter the path of the shared folder (or a folder under the shared folder) you want to mount as a network drive.

```
\\IP address of NAS\(shared) folder name
```

8. Click **OK** to save the settings.



9. Sign in to the domain-joined Windows PC with this domain user account. You will see the mounted drive on the computer.



Note:

- The **Local path** option at the **Profile** tab is the path to a Windows local folder. Make sure this path has already been created on the computer you assigned. Otherwise, your settings will not be valid.
- If domain users have already signed in to the assigned Windows PC before a drive is mounted, they will need to sign in again to access the mounted drive.

Manage Computers

Computers in the domain created by Synology Directory Server can be workstations, servers, or NAS. This type of object can be deployed in the domain for users to access.

This section will briefly guide you through the management of computers in Synology Directory Server.

Note:

- To join computers or Synology NAS to the domain, see **Chapter 4** for detailed instructions.

Edit Computer Properties

1. Select the computer you wish to edit, and click **Action** > **Edit**.
2. Edit the **Description** for the computer.
3. Click **OK** to save the settings.

Note:

- You can also edit a computer by right-clicking a computer on the **Users & Computers** page and then clicking **Edit**.

Delete a Computer

1. Select a computer you wish to delete on the **Users & Computers** page, and click **Action** > **Delete**.
2. Click **Delete** in the pop-up message to confirm the deletion.

Note:

- You can also delete a computer by right-clicking the computer on the **Users & Computers** page and then clicking **Delete**.
- You can select multiple computers by pressing and holding the **Ctrl** or **Shift** key.
- The deletion of computers is **irreversible**.

Chapter 4: Join Devices to a Domain

Joining devices to a domain not only provides an efficient way to manage resources of an organization collectively, but also allows users to access them simply with one set of credentials.

This chapter will demonstrate how to join Windows clients and Synology NAS to a domain managed by Synology Directory service.

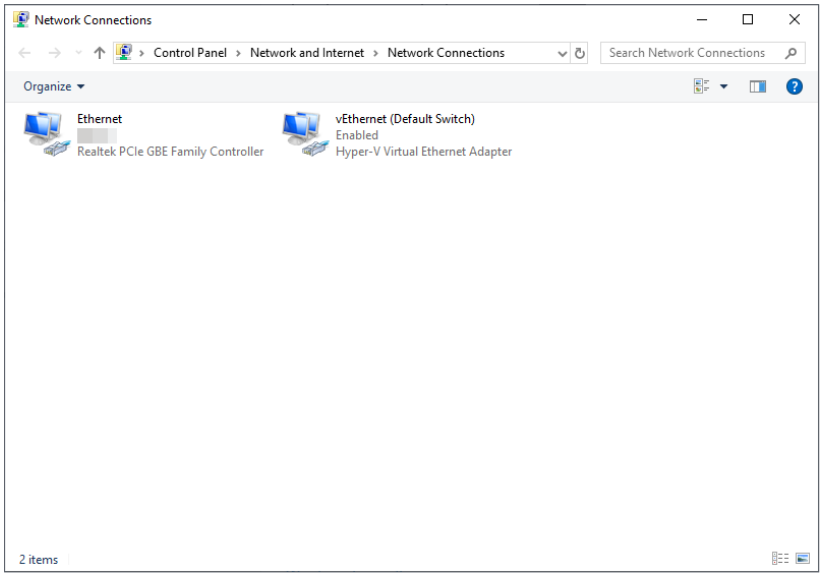
Join Windows PCs to a Domain

The following are the versions of Windows operating system that can be joined to the domain created by Synology Directory Server:

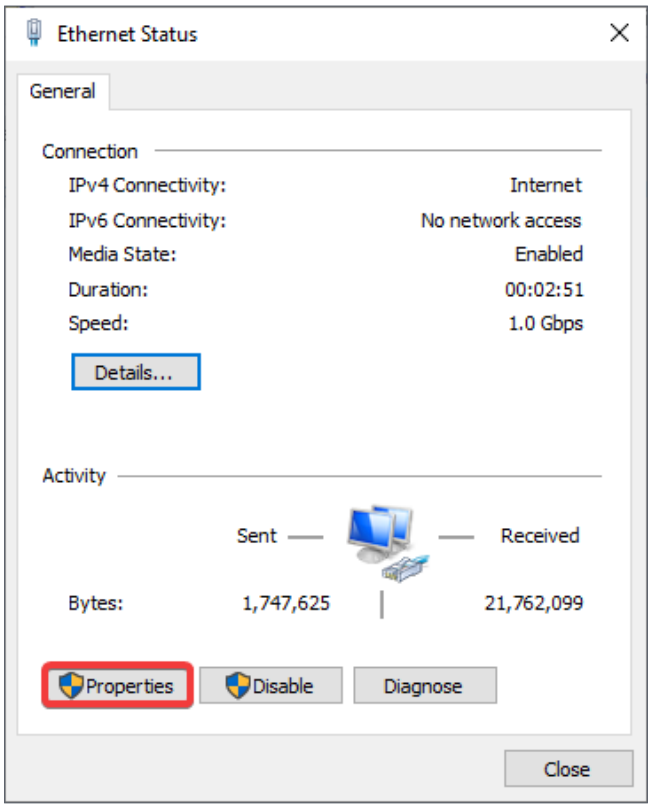
- Windows Server 2016 Datacenter/Standard
- Windows Server 2012 (R2) Datacenter/Standard
- Windows Server 2008 (R2) Datacenter/Enterprise/Standard
- Windows 10 Enterprise/Pro/Education
- Windows 8.1 (8) Enterprise/Pro
- Windows 7 Ultimate/Enterprise/Professional

The following steps will guide you to join a Windows 10 PC to a domain:

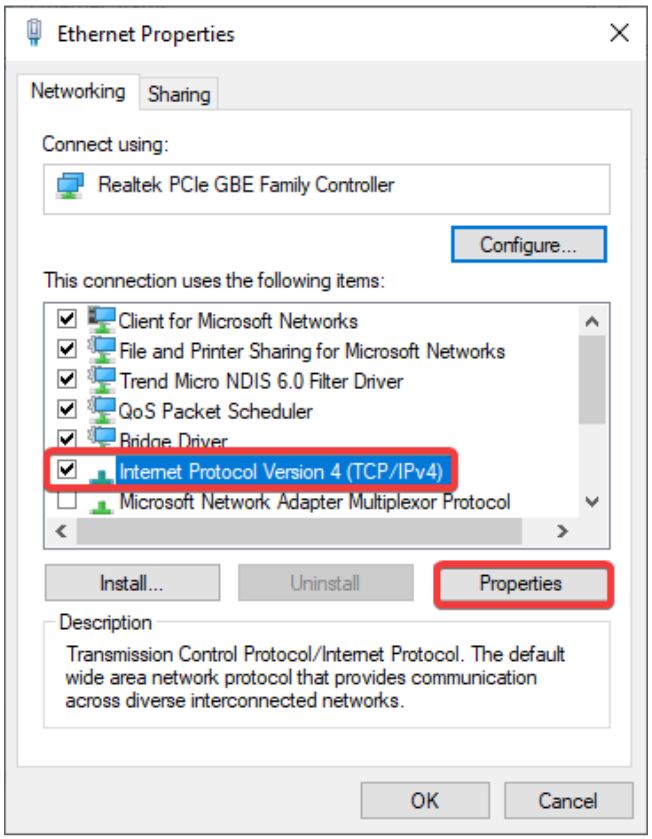
1. Go to Windows **Start** icon > **Settings** > **Network & Internet** > **Status** > **Change adapter options**, and double-click on the network interface the computer is currently using.



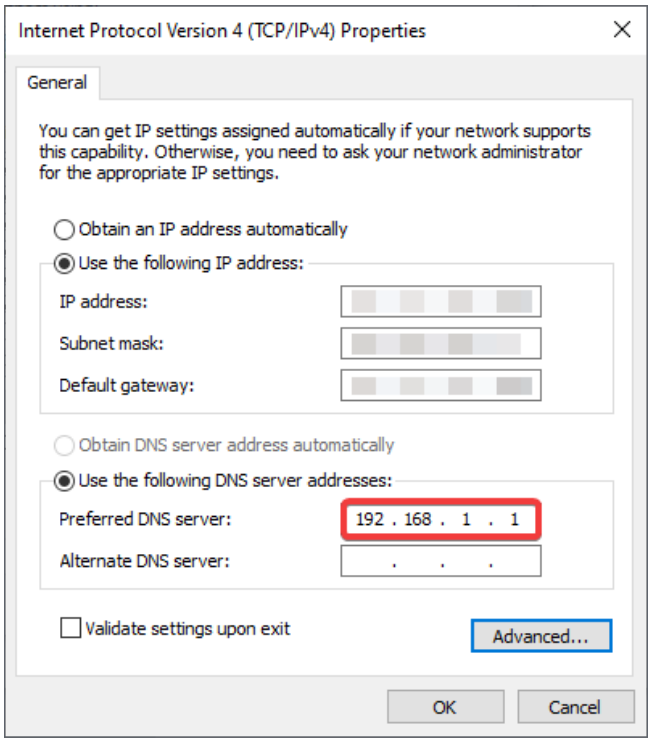
2. On the **Status** page, click **Properties**.



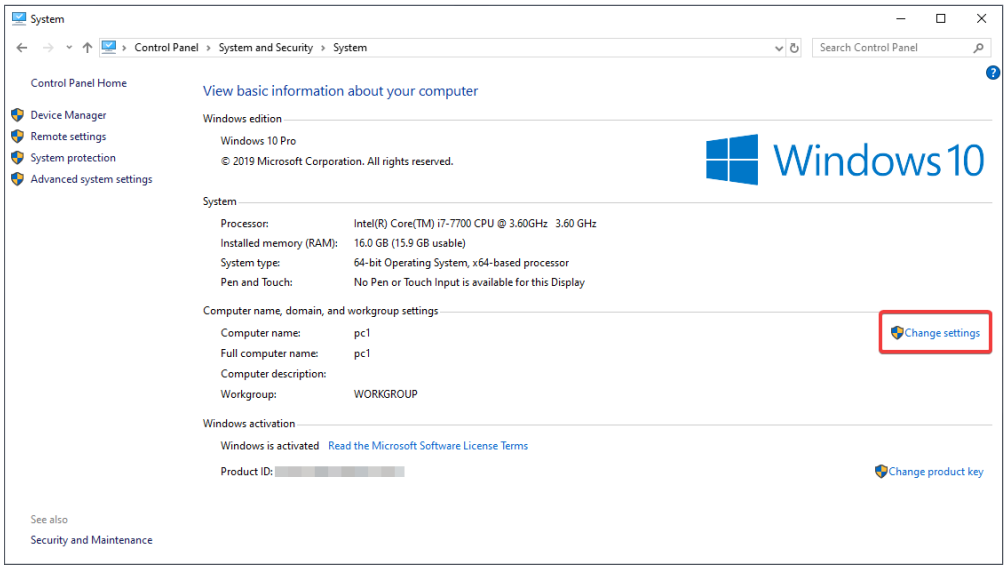
3. At the **Networking** tab, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



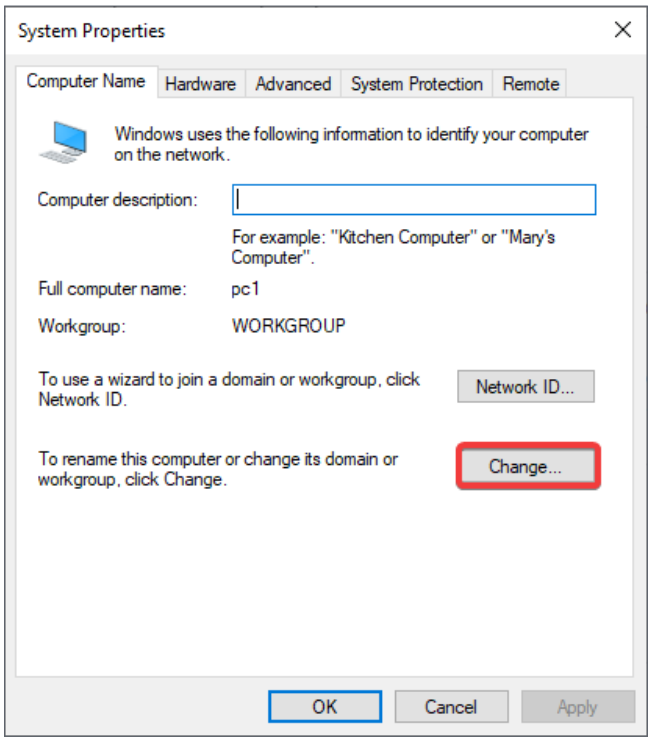
4. Tick **Use the following DNS server addresses**, enter the IP address of the domain controller in the **Preferred DNS server** field, and click **OK** to save the settings.



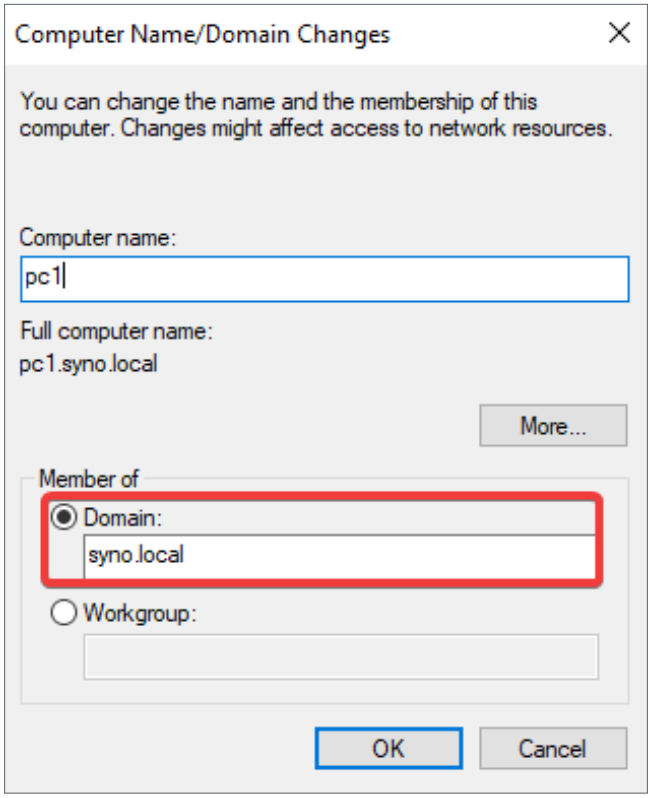
5. Go to Windows **Start** icon > **Settings** > **System** > **About** > **System info** and click **Change settings**.



6. At the **Computer Name** tab, click **Change...**



7. Under **Member of**, click **Domain** and enter the name of the domain you wish for this computer to join. Click **OK** after you have confirmed the settings.



8. Enter the domain administrator's credentials and click **OK**. Please refer to the following username format:

```
Domain NetBIOS name\administrator's username
```

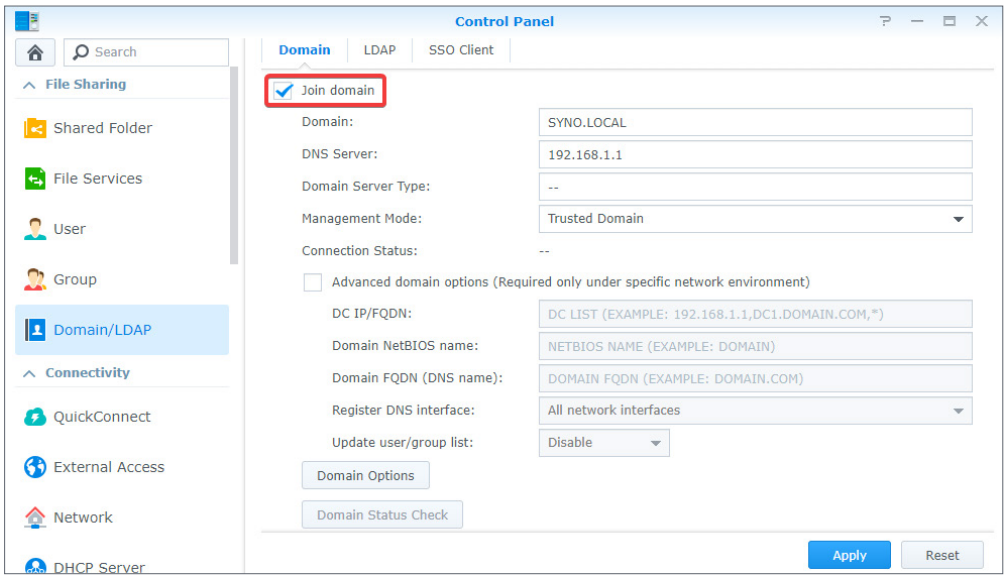
9. Restart the computer to complete the process of domain joining.

Join Synology NAS to a Domain

You can join Synology NAS to a domain as a domain client. After joining the domain, domain users can sign in to Synology NAS using their domain accounts and passwords, allowing them to access files and use DSM applications without the need to remember another set of username and password.

To join Synology NAS to your domain, please follow the steps below:

1. Go to **Control Panel** > **Domain/LDAP** > **Domain**.
2. Tick **Join domain**.



3. Enter the domain name and specify the DNS server in the appropriate fields.
4. If necessary, click **Domain Options** to configure advanced settings (see the following section **Advanced Options**).
5. Click **Apply**.
6. In the pop-up window, enter the domain administrator's credentials and click **OK**.

Advanced Options

This section covers the advanced options at **Control Panel** > **Domain/LDAP** > **Domain**:

Option Name	Description
Domain Server Type	This field shows the domain type of the Synology NAS after joining a domain. In this case, the domain type will be **AD Domain**.
Management Mode	This option will determine how you manage the privileges of domain users and groups. • **Trusted Domain**: You can manage users and groups in the domain that the NAS joins as well as other trusted domains. Users and groups can be filtered with the **Domain** drop-down menu. • **Single Domain with OU**: Only users and groups in the domain that the NAS joins will be displayed in this mode. This mode allows you to filter domain users/domain groups with the **OU** drop-down menu.
Advanced domain options	In most cases, you do not need to fill in any of the advanced domain options. Advanced domain options are needed only for specific domain environments. • **DC IP/FQDN**: Specify a domain controller's (DC) IP address or Fully Qualified Domain Name (FQDN), and the Synology NAS will try to communicate with it. • **Domain NetBIOS name**: Specify the NetBIOS name of the domain. • **Domain FQDN (DNS name)**: Specify the FQDN of the domain. • **Register DNS interface**: When joining a domain, the Network Interface Card (NIC) specified here will be registered with the DNS server. Please note that if the hostname of the Synology NAS includes an underscore (_), the registration will fail because underscores (_) cannot be used for DNS. • **Update user/group list**: Specify how often the Synology NAS automatically updates the domain user/group list. You can customize the period to perform updates daily, weekly, or monthly. In addition, domain user/group lists can be manually updated by going to the **Domain Users** tab and clicking **Update Domain Data**. Please note that automatic updates will affect system hibernation.
DiskStation will synchronize with an NTP server every time a domain user logs in	Enabling this option will force synchronize the time between the Synology NAS and the NTP server.

Option Name	Description
Get user/group lists with NT4-compatible mode	Enabling this option allows the system to obtain user/group lists using the NT4 RPC mode. This option can be enabled if certain domain user/group lists cannot be obtained using default settings.
Enable server signing	If users access the Synology NAS through SMB protocol on their computers with SMB client signing enabled, the server signing must also be enabled on the Synology NAS (i.e., the SMB file server) to ensure the functionality of file transfers.
Enumerate nested group levels	Specify the level number of nested domain group members that can be enumerated.
Domain Administrators	Specify up to ten groups of users to whom you wish to grant administrative privileges. Any user with administrative privileges will have full control of the Synology NAS and the files stored thereon.
Enable Integrated Windows Authentication	If this option is enabled, users who have already signed in to their computers using domain accounts can access DSM via an Internet browser without entering their credentials again.
Domain Status Check	Check the status of the connection between the DSM and the domain it has joined.

Using Integrated Windows Authentication

- The client computer must run Windows 7 or above.
- The client computer must be located in the same domain as Synology NAS.
- Go to Windows **Control Panel** > **Internet Options** > **Advanced** and make sure **Enable Integrated Windows Authentication** checkbox under the **Security** section is ticked.
- Integrated Windows Authentication works with all browsers. For Firefox, a few more steps are required for setup.
  1. Open a Firefox browser, enter "about:config" in the URL bar.
  2. Search for "network.automatic-ntlm-auth.trusted-uris".
  3. Double-click the **value** field and enter the IP address of the domain.
- For the Synology NAS joining a domain created by Synology Directory Server, additional configuration is required to use integrated Windows Authentication:
  1. Go to DSM **Control Panel** > **File Services** > **SMB/AFP/NFS**.
  2. Under the **SMB** section, click **Advanced Settings**.
  3. Select **SMB1** from the **Minimum SMB protocol** drop-down menu and click **Save**.
- Logins through Integrated Windows Authentication are only available on DSM 6.2.2 and above.

Chapter 5: Configure Group Policies

Group policies are the means of IT administrators to manage user experience within a domain. They can be used to define restrictions on common actions, deploy services on domain-integrated devices, manage updates, and ensure a consistent working environment for users. Good management of group policies will ease the burden of domain administration.

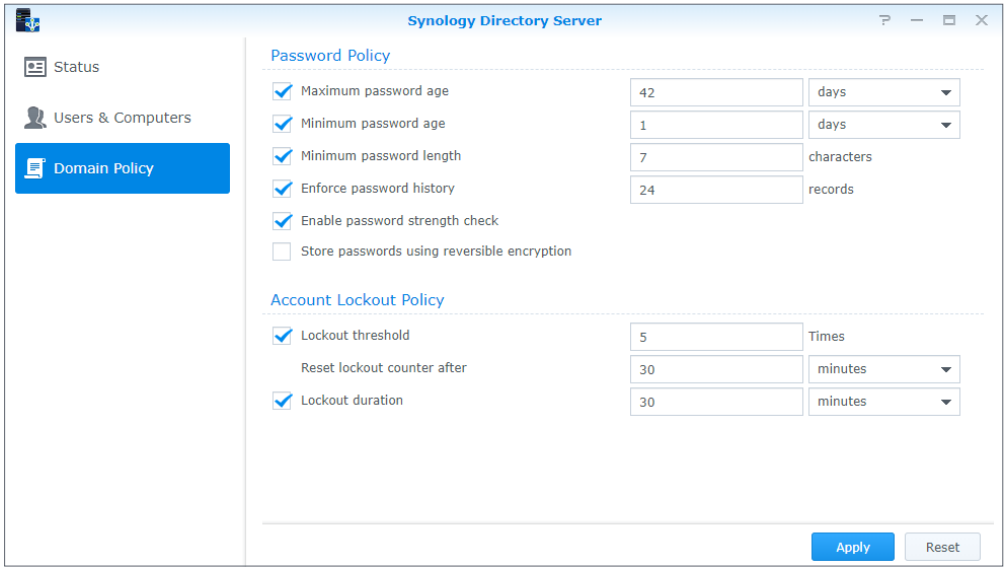
In this chapter, we will provide instructions on how to use Synology Directory Server and Windows Remote Server Administration Tools (RSAT) to configure group policies for your domain.

Configure Default Domain Policies

Default Domain Policy allows you to maintain account security on a domain level by setting up **password** and **account lockout** policies. You can click **Domain Policy** on the left panel to manage these two types of default domain policies.

Note:

- The settings on this page are applied to the group policy **Default Domain Policy** in Windows RSAT. If this group policy is deleted, this page cannot function normally.



Password Policies

The following are the available password policies on the **Domain Policy** page:

- **Maximum password age**: Specify the time after which the passwords expire. Passwords will never expire if the option is disabled.
- **Minimum password age**: Specify the time frame in which users are not allowed to change their passwords after their last password change. Passwords can be changed at any time if the option is disabled.
- **Minimum password length**: Specify the minimal length of new passwords.
- **Enforce password history**: Any new passwords must be different from the ones set previously, the number of which is to be specified here.
- **Enable password strength check**: Passwords must comply with the strength requirements. Please refer to the note below for more information.
- **Store password using reversible encryption**: Enabling this option will compromise domain security. This option is not recommended unless demands of domain client services take higher priority over password security.

Note:

To meet the password strength requirements, your password must comply with **at least three** of the following rules:

- Uppercase letters of the Latin (including A - Z with diacritic marks), Greek, and Cyrillic alphabets.
- Lowercase letters of the Latin alphabets (including a - z with diacritic marks), Greek, and Cyrillic alphabets.
- Numeric characters (0 - 9).
- Special characters, including #, $, !, etc.
- Unicode alphabets, including those in Asian languages.

Account Lockout Policies

The following are the available account lockout policies on the **Domain Policy** page:

- **Lockout threshold**: User accounts will be locked out when the number of failed login attempts is beyond your specified lockout threshold.
- **Reset lockout counter after**: The number of failed login attempts will be re-calculated after this specified time.
- **Lockout duration**: Locked-out user accounts will not be unlocked until the end of your specified lockout duration.

Use RSAT to Manage Group Policies

With Synology Directory Server, you can configure policies related to passwords and account lockout. To configure other types of group policies, however, you have to use Windows **Remote Server Administration Tools (RSAT)** on a domain-joined Windows PC (see **Chapter 4** to learn more on how to join Windows PCs to a domain).

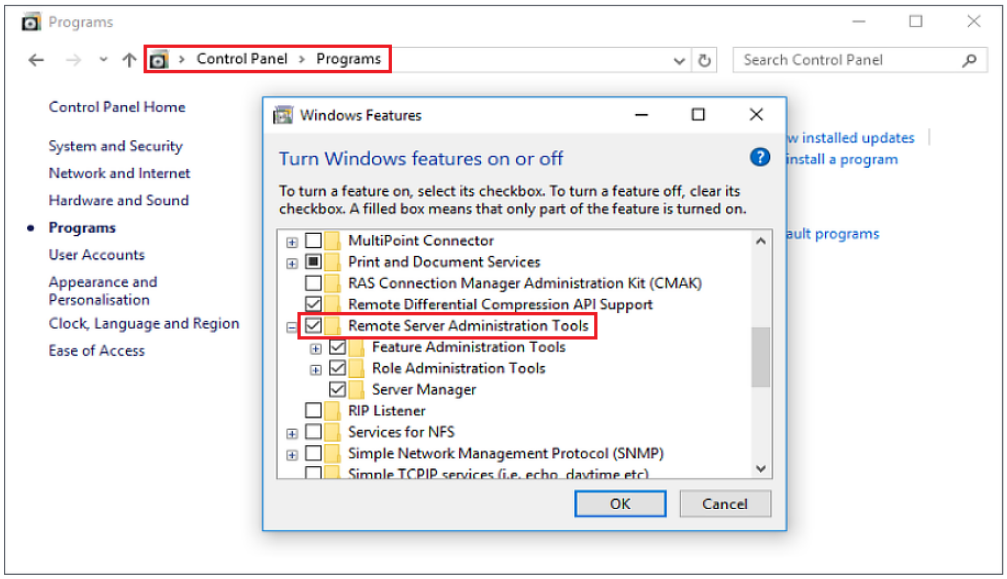
The following sections will guide you through group policy management via RSAT.

Install RSAT to a Windows PC

1. Download Windows RSAT from Microsoft Download Center to a Windows PC. Different Windows versions have separate RSAT installation files. You can refer to the following list to find an installation file corresponding to your version of Windows:

   - **Windows 8**
   - **Windows 8.1**
   - **Windows 10**

2. Run the downloaded file and follow the onscreen instructions in the wizard to install RSAT.
3. When the installation is complete, go to Windows **Control Panel** > **Programs** > **Turn Windows features on or off**, and tick the **Remote Server Administration Tools** checkbox.



4. Make sure you have joined the current computer to your domain and signed in as a domain administrator. You will find RSAT at **Control Panel** > **Administrative Tools**.

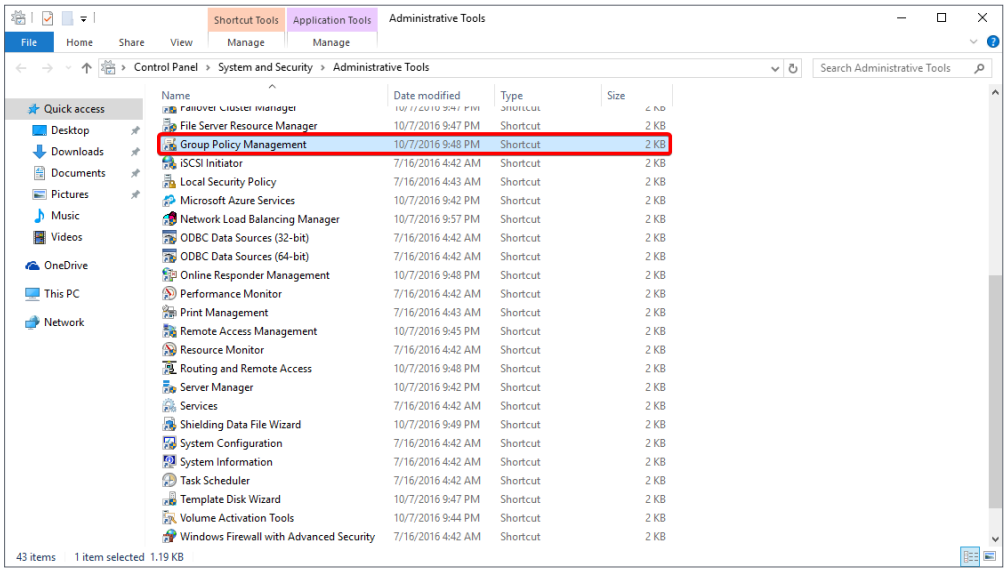
Note:

- Configurable options of RSAT depend on the Windows version of the computer where RSAT is installed. For instance, settings available in the Windows 8 RSAT may not cover all settings built in the Windows 10 RSAT.

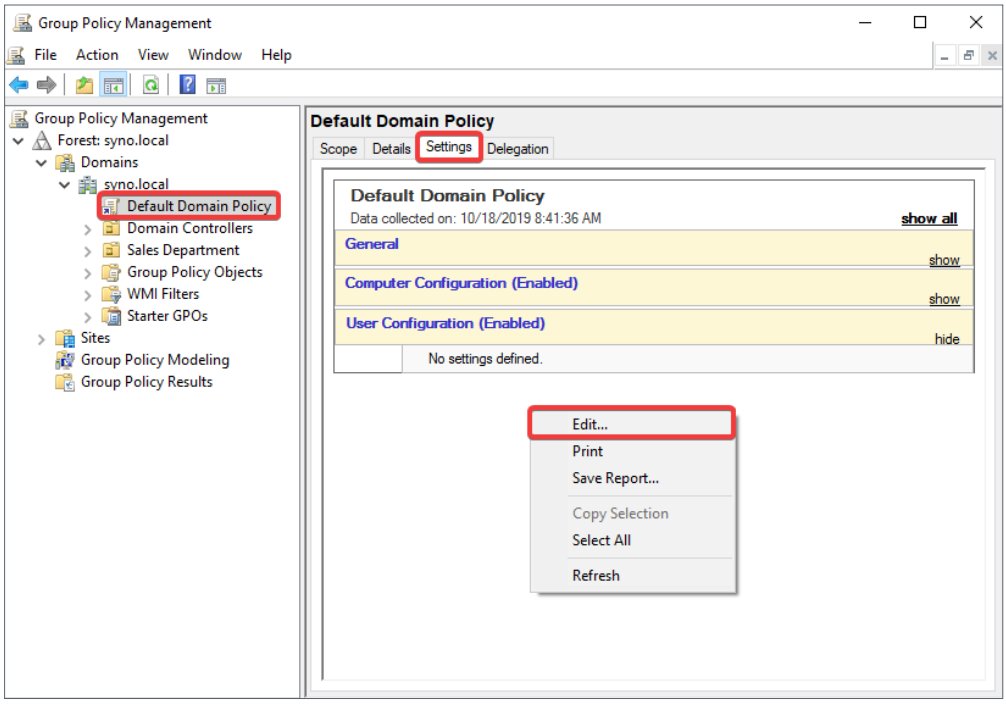
Assign a Roaming Profile for All Users

Roaming profiles allows domain users to access their files when they sign in to different computers that are joined to the domain. Please follow the steps below to assign profiles for all domain users via RSAT:

1. Make sure you have created a shared folder and granted sufficient permissions to all domain users on the domain controller.
2. Sign in to a domain-joined Windows PC as a domain administrator.
3. Go to Windows **Control Panel** > **System and Security** > **Administrative Tools** > **Group Policy Management**.

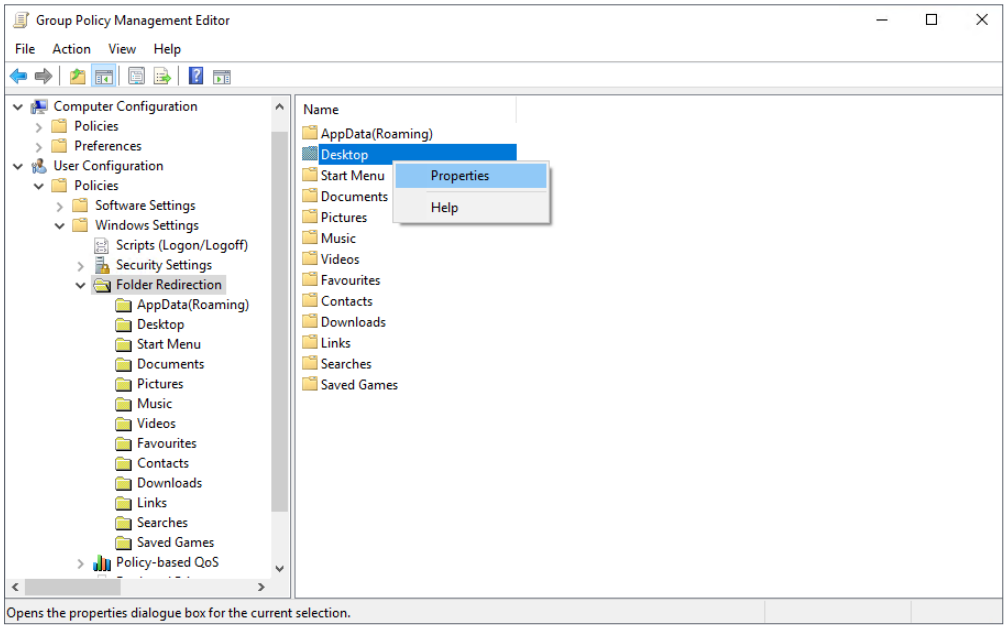


4. Go to **Forest: *domain name*** > **Domains** > ***Domain name*** > **Default Domain Policy**.
5. At the **Settings** tab, right-click to open the context menu, and click **Edit**.



6. Go to **User Configuration** > **Policies** > **Windows Settings** > **Folder Redirection**.

7. Right-click the folders you would like to redirect and click **Properties**.



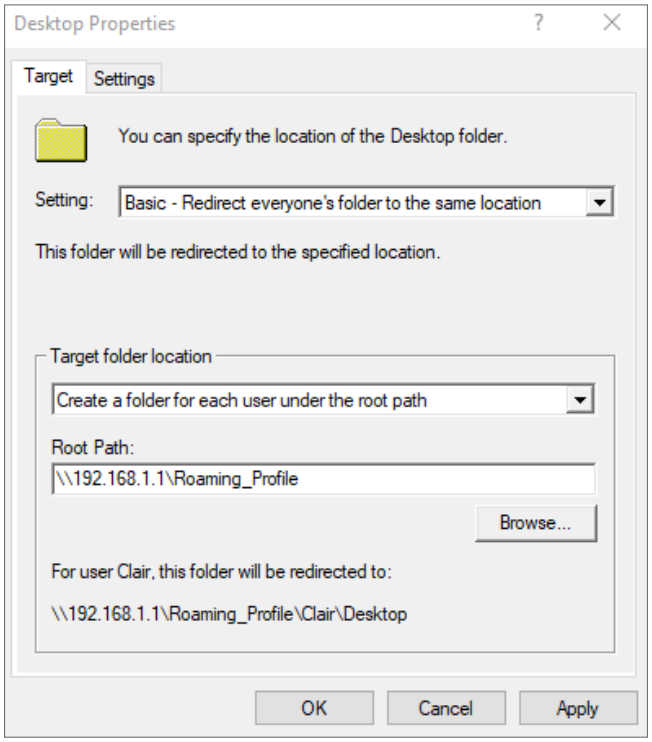
8. Configure the settings as below:

   a. Switch to the **Target** tab.

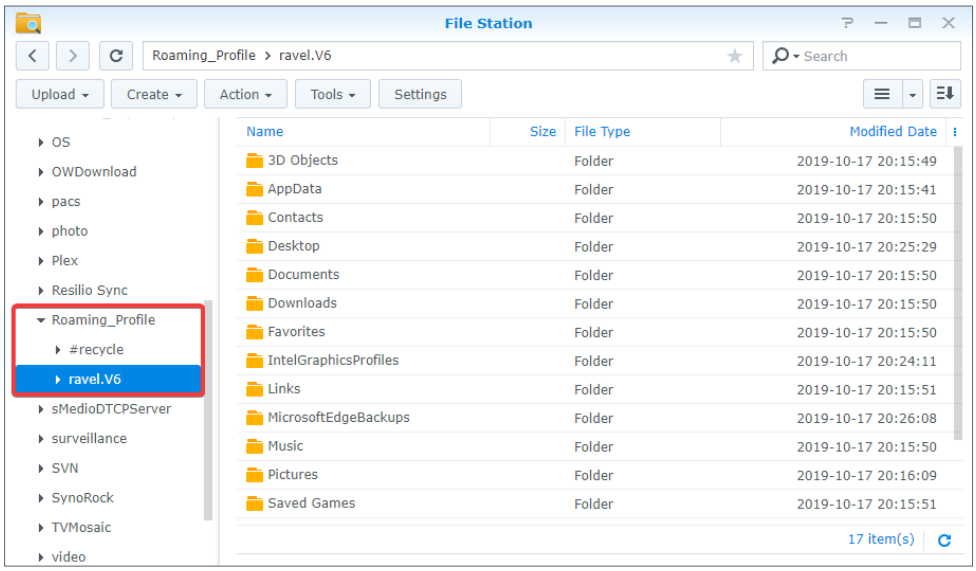
   b. Select **Basic - Redirect everyone's folders to the same location**.

   c. Enter the information needed in **Target folder location** and **Root Path**.

   d. Click **OK**.



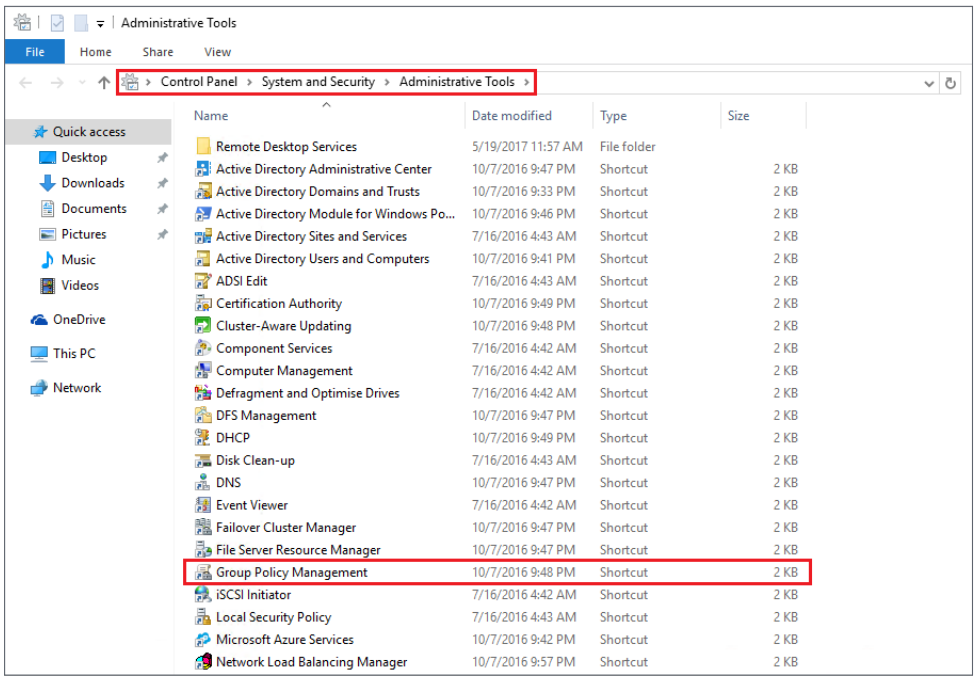
9. The roaming profiles of domain users will be directed to the path you assigned.



Mount a Network Drive for All Users

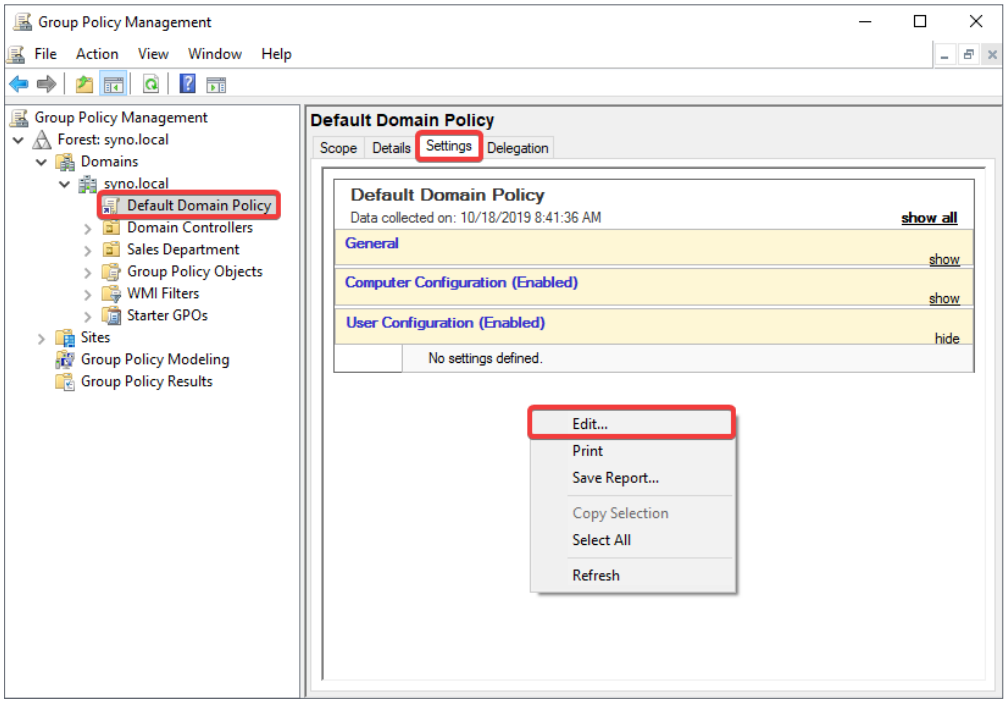
Besides setting roaming profiles, Synology Directory Server also allows you to mount a network drive for domain users. Please follow the steps below to mount a network drive for all users via RSAT:

1. Make sure you have created a shared folder and granted sufficient permissions (at minimal read permissions required) to all domain users on the controller Synology NAS.
2. Sign in to a domain-joined Windows PC as a domain administrator.
3. Go to Windows **Control Panel** > **System and Security** > **Administrative Tools** > **Group Policy Management**.

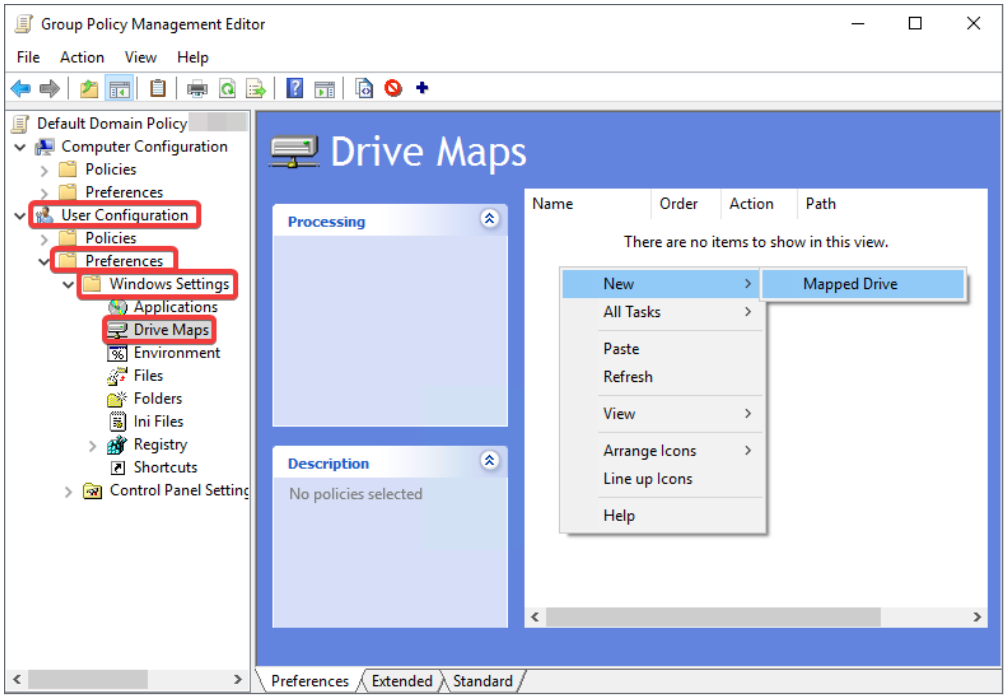


4. Go to **Forest: *domain name*** > **Domains** > ***Domain name*** > **Default Domain Policy**.

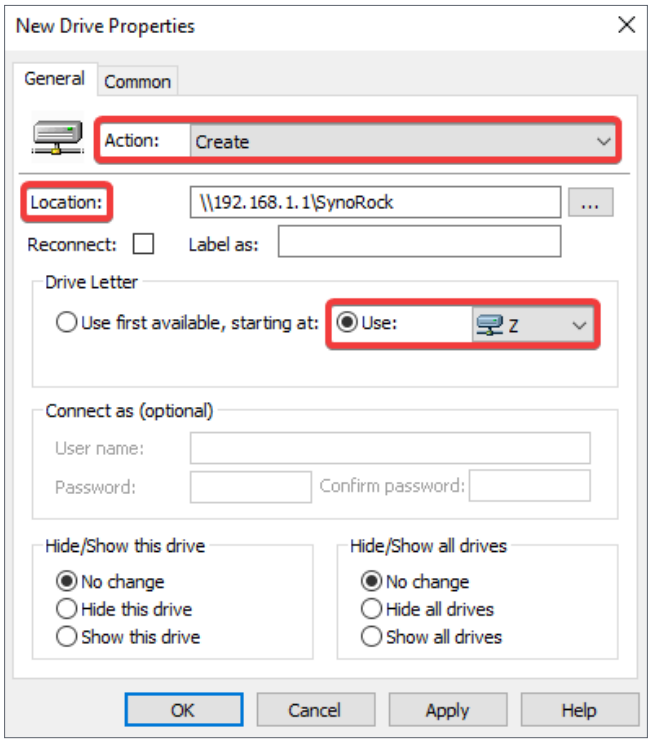
5. At the **Settings** tab, right-click to open the context menu, and click **Edit**.



6. In the console tree, go to **User Configuration** > **Preferences** > **Windows Settings** > **Drive Maps**. Right-click in the right-hand pane and click **New** > **Mapped Drive**.



7. Configure the following settings and click **OK**:
   - **Action**: Select **Create** from the drop-down menu.
   - **Location**: Enter the location of the network drive, e.g., "\\192.168.1.1\SynoRock".
   - **Drive Letter**: Under this section, click **Use** and choose a drive letter.



8. After the configuration, you will see the network drive mounted on this computer when you sign in via any domain user account.

Note:

- It is not necessary to enter a **User name** and **Password** under the **Connect as (optional)** section because Windows will attempt to mount the network drive for your account when the settings are completed. When a domain user signs in, Windows will automatically mount the network drive for that user's account.
- To make network drives work properly, please ensure that the destination of network drives exists and that users have access permissions.

Chapter 6: Maintain and Recover Directory Service

When working with Synology Directory Server, it is of vital importance that you make sure the directory service is securely maintained and backed up. Regular maintenance and backup become helpful when you lose data owing to accidental system failures or deletion of data.

In this chapter, we will cover tools and methods for setting up a high-availability cluster and backup tasks for Synology Directory Server.

Ensure Uninterrupted Directory Service via Synology High Availability

To secure the continuous availability of Synology Directory Server, we suggest protecting your directory database through the **Synology High Availability** package.

Synology High Availability uses two servers to form a "high-availability cluster" in which one server assumes the role of "active server" and another server acts as a standby "passive server". This server layout solution is designed to reduce interruptions of services caused by server malfunctions (See the **Synology High Availability help articles** for more information on essentials of high-availability clusters).

Please refer to the following for system requirements and a guideline on how to set up a high-availability cluster to ensure an uninterrupted Synology Directory service.

System Requirements

Synology High Availability requires two identical Synology NAS with the same system configurations to set up a cluster. Before starting, please pay extra attention to the following information and configure the pair of Synology NAS accordingly:

- **Applied models**: Both the active and passive servers should be identical models and support Synology High Availability. See **here** to learn more about models supporting this package.
- **DSM & package version**: The same version of DSM and Synology High Availability must be installed on both the active and passive servers. Please note that the service monitoring Synology Directory service is only supported by Synology Directory Server 4.4.5-0093 (and above) along with Synology High Availability 2.0.3-0140 (and above).
- **Identical storage and network settings**:
  - The number, capacity, and inserted slots of drives must be identical on both the active and passive servers.

- The total number of network interfaces and network settings must be identical on both the active and passive servers. In particular, please make sure each server has at least one static IP address belonging to the same subnet, and that you have set up a Heartbeat connection for internal communication between the two servers.

Note:

- For complete information on system requirements, please refer to **this article**.

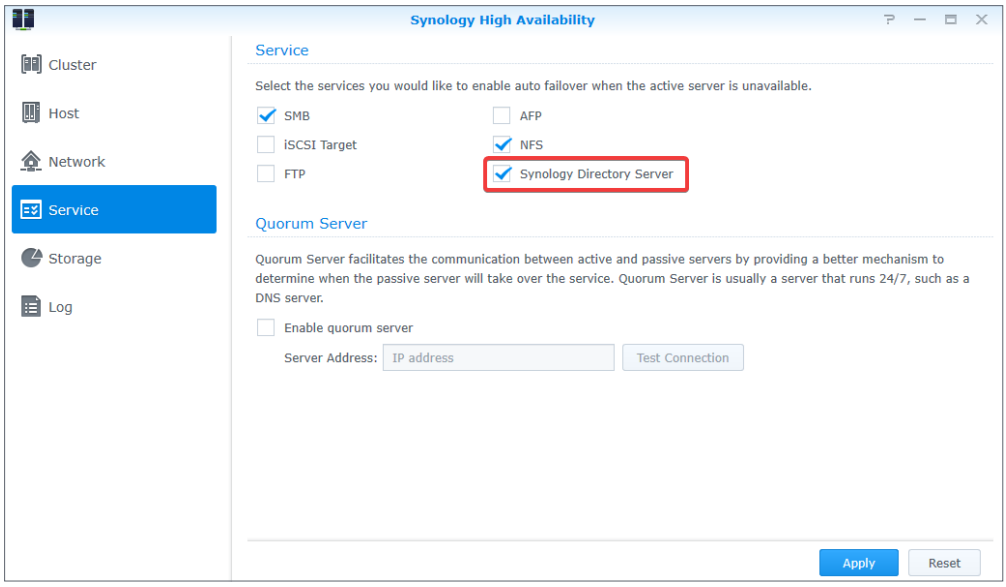
Set up a High-Availability Cluster

To set up a Synology High Availability cluster, please follow the steps below:

Note:

- To ensure that Synology Directory Server works properly, please set up the Synology High Availability cluster **before** activating Synology Directory service.

1. Launch **Synology High Availability**.
2. Click **Create high-availability cluster** and follow the wizard's instruction to complete the setup (see **this article** for detailed guidelines).
3. Install **Synology Directory Server** (see **this section**) and set up Synology Directory service (see **Chapter 2**).
4. Go to **Synology High Availability** > **Service**.
5. Tick **Synology Directory Server** and click **Apply** to save the settings.



Note:

- Besides the high-availability cluster, please also back up Synology Directory service periodically via **Hyper Backup** (see the section **Back up and Restore Directory Service via Hyper Backup** for detailed instructions).

Back up and Restore Directory Service via Hyper Backup

You may use the Synology **Hyper Backup** package to back up or restore the data and settings of Synology Directory Server. Hyper Backup offers the following features:

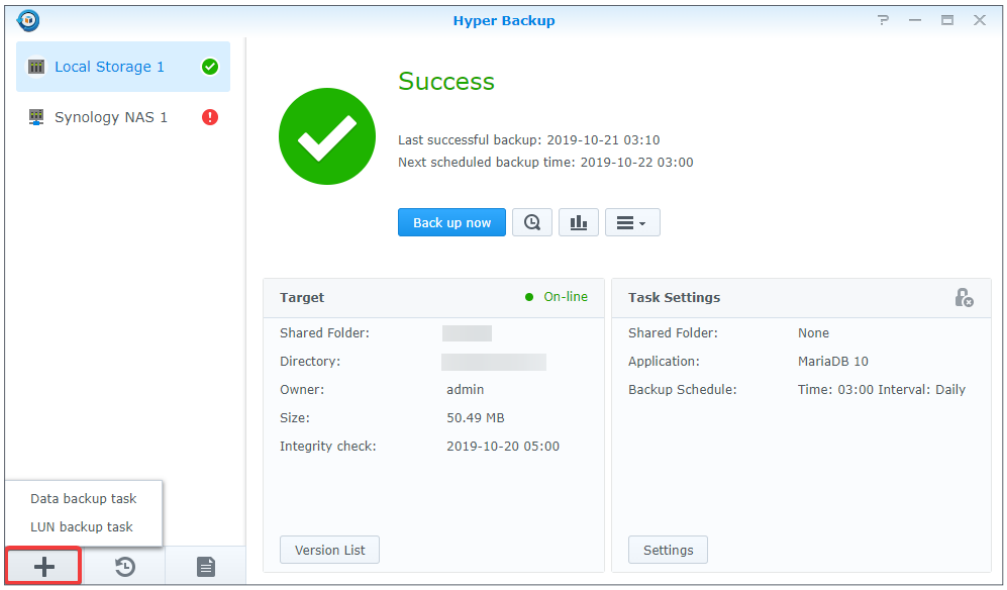
- Retain up to 65,535 versions of data while storage consumption is minimized with cross-version deduplication.
- Keep backed-up data in a proprietary database that can be easily browsed, downloaded, or restored with a multi-version explorer on the DSM, Windows, and Linux platforms.
- Back up various types of data (e.g., system configurations, shared folders, and applications/packages) manually or periodically.
- Store backup tasks in local shared folders, remote servers, or public clouds.
- Retain multiple backup versions for each task. Automatic backup rotation is optional and has three modes: deletion from the earliest backup version, **Smart Recycle**, and customized policies.

To back up Synology Directory Server, please go to **Package Center** to install Hyper Backup.

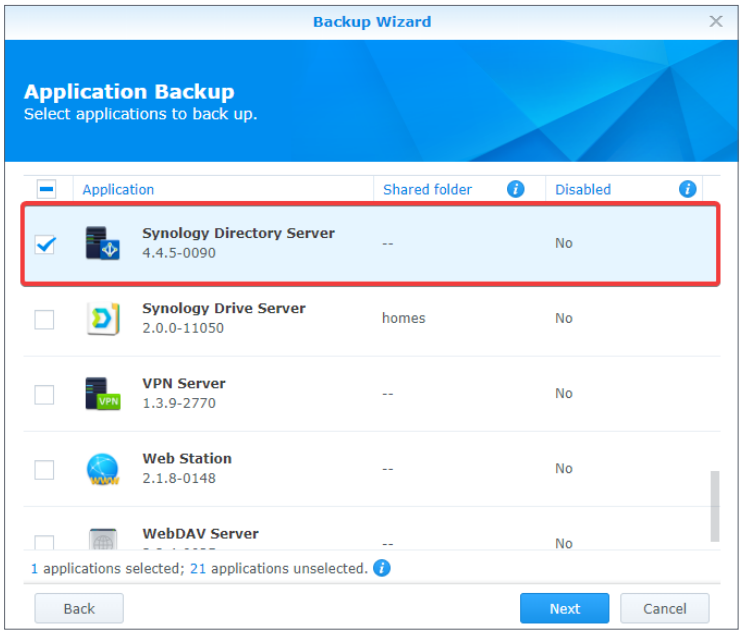
Create a Backup Task

Hyper Backup allows you to create, manage, and monitor data backup tasks. To back up your data, please follow the steps below:

1. Launch **Hyper Backup**.
2. Click **+** on the lower-left corner, and select **Data backup task** to launch the backup wizard.



3. Select the desired type of backup destination. We suggest not selecting the same device.
4. Select **Create backup task**.
5. Select the folders you wish to back up and click **Next**.
6. Tick **Synology Directory Server** and click **Next**.



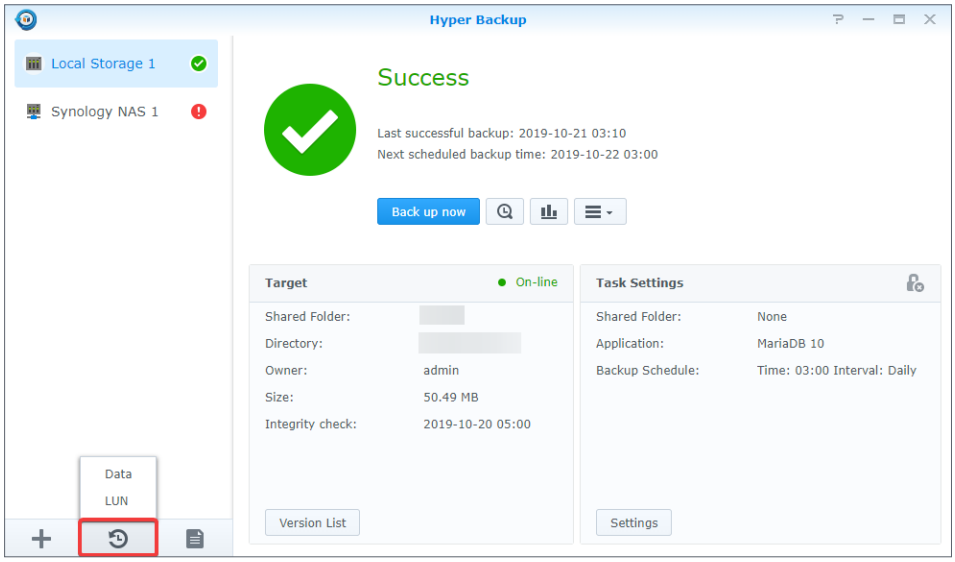
7. Follow the wizard's instructions to finish the backup task creation.

Restore a Data Backup

Hyper Backup allows you to recover your directory once errors occur in Synology Directory Server. Besides, you can also migrate Synology Directory service to another Synology NAS by service restoration in Hyper Backup.

To restore a data backup for Synology Directory Server, please follow the steps below:

1. Launch **Hyper Backup**. Click **Restore** > **Data** on the lower-left corner.



2. Select a backup task to restore.
3. You will be prompted to select system configurations, different versions of backup data, or more. It depends on which type of backup task you wish to restore.
4. If the backup task is encrypted, you will need the password/encryption key for successful restoration.
5. Follow the wizard to complete the restoration.

Note:

- For more details about the backup and restore functions, please refer to the **Hyper Backup help articles** on the Synology website.

Chapter 7: Troubleshooting and FAQs

This chapter provides some frequently asked questions on Synology Directory configurations.

Account Issues

Why can a newly-created user sign in to DSM using both the old/new passwords?

The issue arises from a Windows attribute **OldPasswordAllowedPeriod** (see **this article** for more information). This attribute determines how long the system will permit an NTLM login through the old password after a password change or reset.

When OldPasswordAllowedPeriod and the password settings are configured in the following way, domain users who have changed their passwords may be able to sign in to DSM using both the old and new passwords within a specified time (based on the value of OldPasswordAllowedPeriod):

- The password history function is enabled.
- NTLM (instead of Kerberos) is used to change passwords.
- OldPasswordAllowedPeriod is not set to zero (the default is 60 minutes).

To resolve the issue, please disable OldPasswordAllowedPeriod by following the steps below:

1. Open the terminal emulator on your computer (e.g., **PuTTY**).
2. Sign in to DSM with root permission via SSH/Telnet.
3. Enter the following command:

```
vi /var/packages/DirectoryServerForWindowsDomain/conf/etc/synoadserver.
conf.mustache
```

4. Change **old password allowed period** to **0** and save the settings.

What should I do if I receive the message "Account restrictions are preventing this user from signing in." when signing in to Windows with a domain user account?

The complete scenario of this issue is described below:

When you sign in to a domain-joined Windows PC with a domain user account, the login fails and you receive the message "Account restrictions are preventing this user from signing in. For example: blank passwords are allowed, sign-in times are limited, or a policy restriction has been enforced." However, you can still sign in to DSM through the user account. Accessing a shared folder with the same account over SMB is still available as well.

To resolve the issue, please do the following:

1. Go to DSM **Synology Directory Server** > **Users & Computers**.
2. Double-click the default user **krbtgt**.
3. At the **Account** tab, do either of the following:
   - Keep the **Lock out this account** checkbox unticked.
   - Tick the **Disable this account** checkbox.

How to list all disabled users in Synology Directory Server?

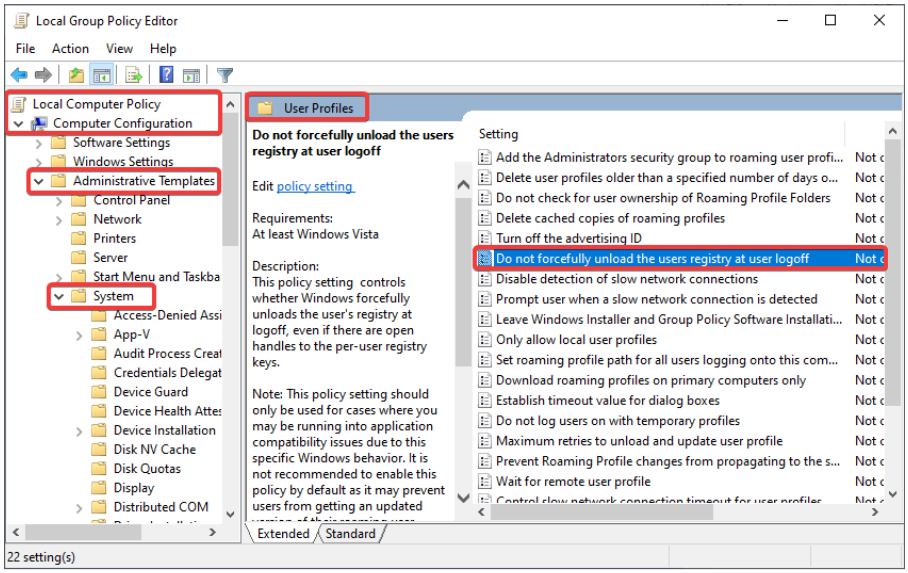
1. Open the terminal emulator on your computer (e.g., **PuTTY**).
2. Sign in to DSM with root permission via SSH/Telnet.
3. Enter the following command:

```
ldbsearch -H ldap://localhost '(&(objectCategory=Person)
(objectclass=user)(userAccountControl:1.2.840.113556.1.4.803:=2))' -P
```

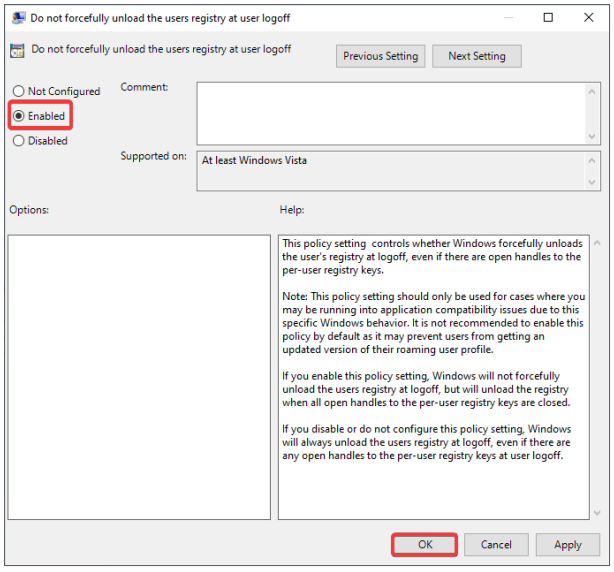
What should I do if roaming profiles are not synchronized to Synology Directory Server when OpLock is enabled? (Windows PC only)

If you enable OpLock (Opportunistic Locks) at DSM **Control Panel** > **File Services** > **SMB** > **Advanced Settings**, roaming profiles may not be successfully synced to Synology Directory Server when domain users shut down their computers. To resolve this issue, please do the following:

1. Run **Windows Powershell** as the administrator on a Windows PC.
2. At the command prompt, enter "gpedit.msc". You will see the window for **Local Group Policy Editor**.
3. Go to **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **System** > **User Profiles**.
4. Double-click **Do not forcefully unload the user registry at user logoff**.



5. In the resulting window, click **Enabled**.
6. Click **OK**.

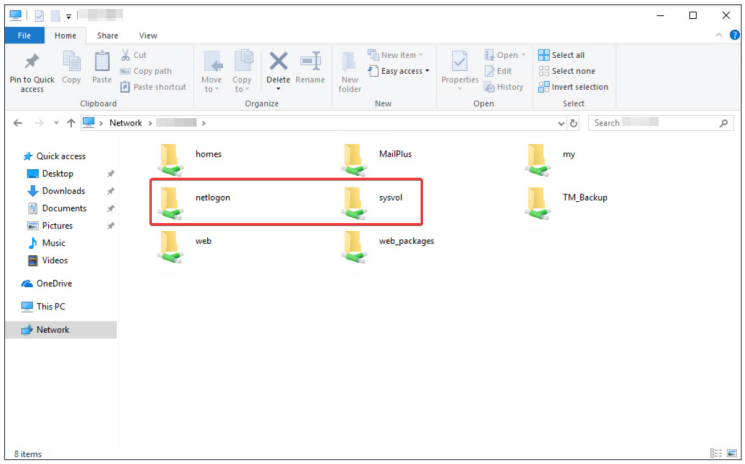


Directory Issues

Why are there "sysvol" and "netlogon" folders?

When using SMB protocol to connect your computer to a Synology NAS where a domain has been set up by Synology Directory Server, you will see **sysvol** and **netlogon** folders, which contain files required for Synology Directory Server.

The **sysvol** folder stores a domain's public files. The **netlogon** folder contains logon scripts and group policies that can be used by computers deployed within a domain.



Note:

- The **sysvol** and **netlogon** folders cannot be hidden or disabled.
- These two folders will not be displayed at DSM **Control Panel** > **Shared Folder**.
- These two folders will be displayed but cannot be accessed directly on Windows 10 computers.

How to expand nested groups for Synology Directory Server?

Nested groups provide flexibility in planning your group structure and applying access control lists (ACLs) to domain resources. To enable this function for the groups in Synology Directory Server's domain, please follow the steps below:

1. Open the terminal emulator on your computer (e.g., **PuTTY**).
2. Sign in to DSM with root permission via SSH/Telnet.
3. Enter "vi /etc/samba/smbinfo.conf".
4. Add the following parameter ("x" is the number of nested group levels. You can replace x with any numbers, such as 2 or 5.):

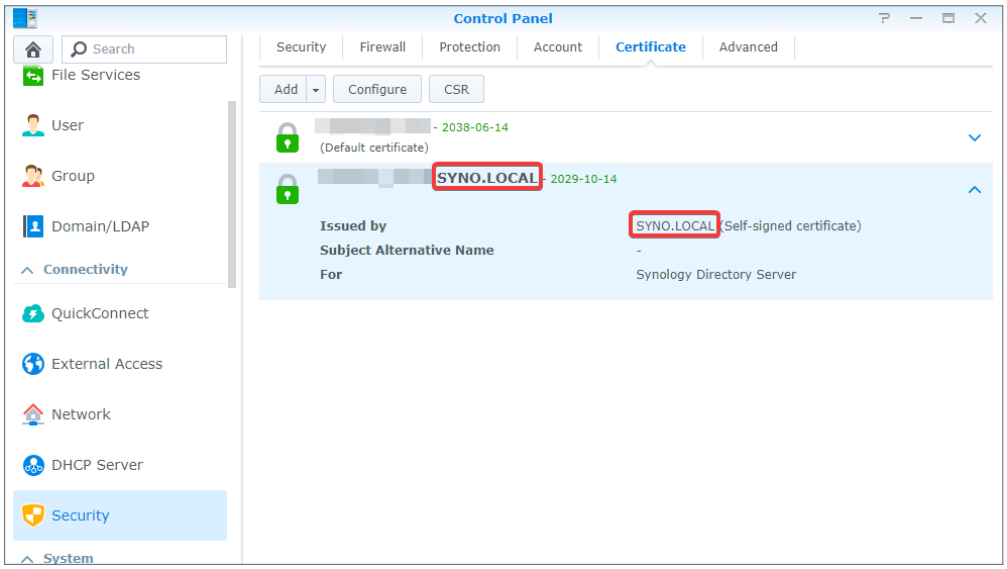
```
winbind expand groups=x
```

5. Enter "restart winbindd". We suggest executing this command during off-peak hours to reduce the performance impact on day-to-day activities.

What should I do if I receive the message "Strong authentication is required." when joining a computer to my domain through an LDAP-joining method?

Joining computers to the Synology Directory Server's domain through an LDAP-joining method is not officially supported by Synology Directory Server. However, you can still activate this function by following the steps below:

1. Go to DSM **Control Panel** > **Security** > **Certificate**, and make sure the name of the certificate used by Synology Directory Server matches your domain.



2. Open the terminal emulator on your computer (e.g., **PuTTY**).
3. Sign in to DSM with root permission via SSH/Telnet.
4. Enter "vi /etc/samba/smb.conf".
5. Add the following parameter and save the settings:

```
ldap server require strong auth = no
```

Note:

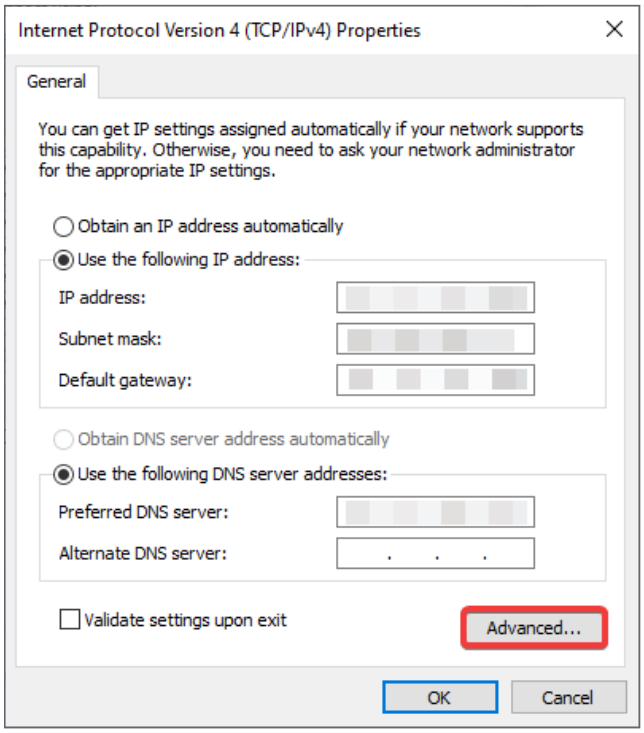
- To join your computer to a Synology Directory Server's domain, please identify Synology Directory Server by the FQDN (Fully Qualified Domain Name, e.g., "synol.local") during the LDAP-joining wizard on your computer.
- If you still cannot join your computer to the domain through an LDAP-joining method, we suggest setting up an LDAP directory through the **LDAP Server** package instead. For more information, see the **LDAP Server help articles** on the Synology website.

DNS Issues

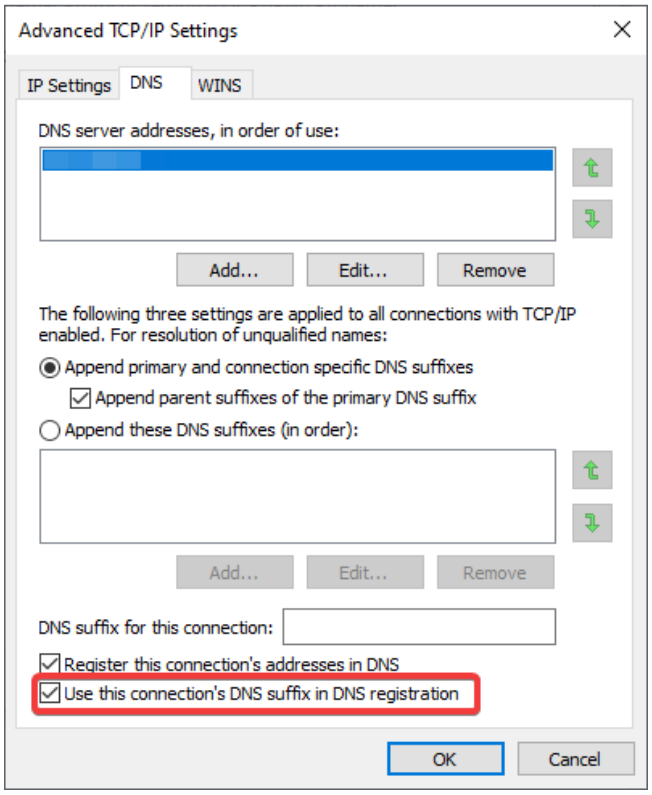
How to get domain clients registered to PTR records in DNS Server automatically? (Windows PC only)

A PTR record helps reverse DNS lookup, i.e., resolving an IP address back to a domain name or hostname. To make sure domain clients are registered to PTR records in **DNS Server** automatically, please follow the steps below:

1. **Enable "Use this connection's DNS suffix in DNS registration":**
    a. Use an account with administrator privileges to sign in to the domain-joined Windows PC that should register the PTR record.
    b. Go to the Windows **Start** icon > **Settings** > **Network & Internet** > **Status**> **Change adapter options**, and double-click on the network interface you are currently using.
    c. On the **Status** page, click **Properties**.
    d. At the **Networking** tab, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.
    e. Click **Advanced...**



    f. On the **Advanced TCP/IP Settings** page, go to the **DNS** tab.
    g. Tick **Use this connection's DNS suffix in DNS registration** and click **OK** to save the settings.



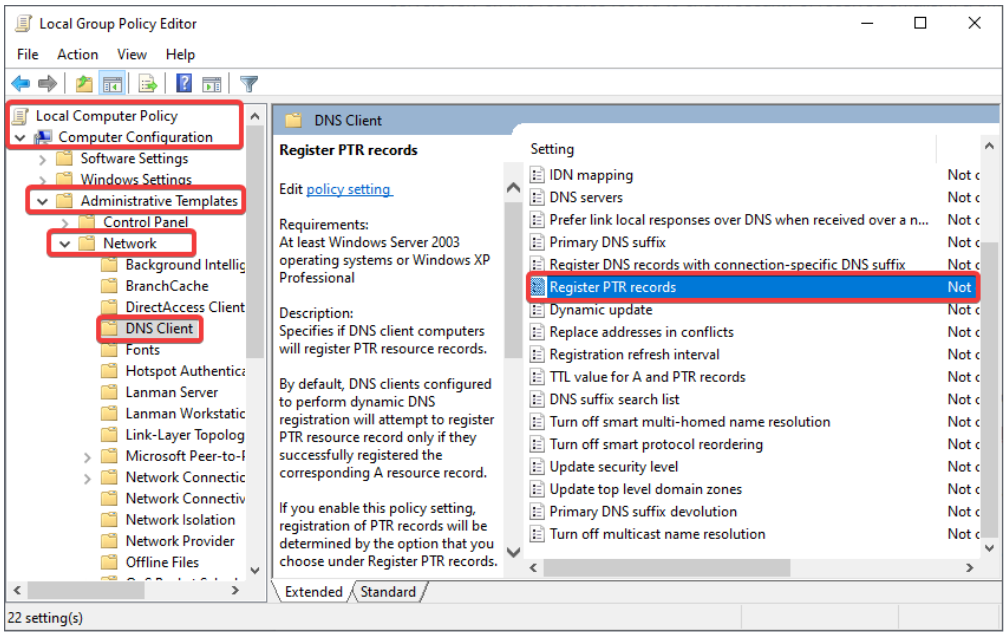
2. **Enable auto-registering PTR records:**

   a. On the same Windows PC, run **Windows Powershell** as the administrator.

   b. At the command prompt, enter "gpedit.msc". You will see the window for **Local Group Policy Editor**.

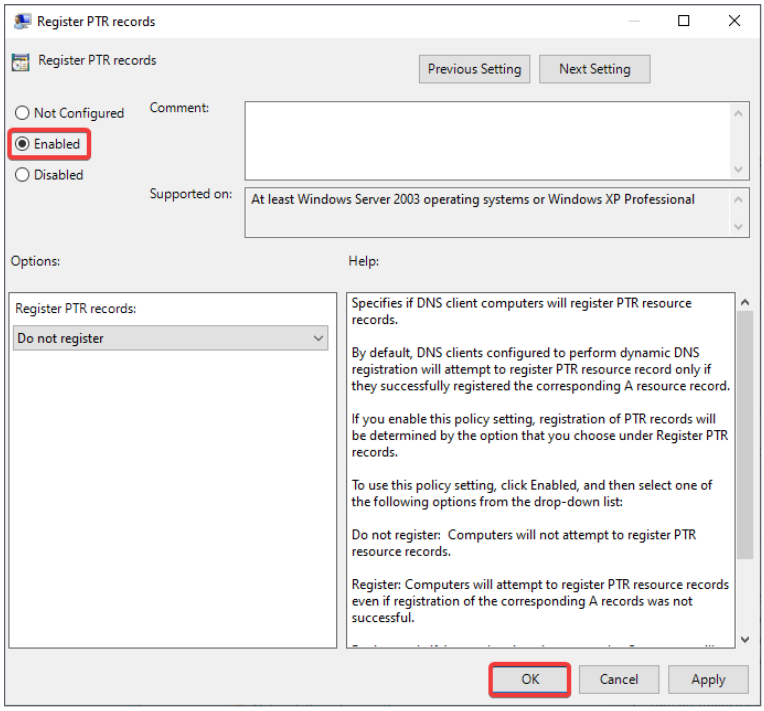
   c. Go to **Local Computer Policy** > **Computer Configuration** > **Administrative Templates** > **Network** > **DNS Client**.

   d. Double-click **Register PTR Records**.



e. In the resulting window, click **Enabled**.

f. Click **OK**.



How to force domain clients to register a new IP address to the AD zone in DNS Server? (Windows PC only)

1. Run **Windows PowerShell** as the administrator on a Windows PC.
2. Run the following command:

```
ipconfig /registerdns
```

SYNOLOGY INC.
9F, No. 1, Yuandong Rd.
Banqiao Dist., New Taipei City 220545
Taiwan
Tel: +886 2 2955 1814

SYNOLOGY AMERICA CORP.
3535 Factoria Blvd SE, Suite #200,
Bellevue, WA 98006
USA
Tel: +1 425 818 1587

SYNOLOGY UK LTD.
Unit 5 Danbury Court, Linford Wood,
Milton Keynes, MK14 6PL
United Kingdom
Tel.: +44 (0)1908048029

SYNOLOGY FRANCE
102 Terrasse Boieldieu (TOUR W)
92800 Puteaux
France
Tel: +33 147 176288

SYNOLOGY GMBH
Grafenberger Allee 295
40237 Düsseldorf
Deutschland
Tel: +49 211 9666 9666

SYNOLOGY SHANGHAI
200070, Room 201,
No. 511 Tianmu W. Rd.,
Jingan Dist., Shanghai,
China

SYNOLOGY JAPAN CO., LTD.
4F, No. 3-1-2, Higashikanda,
Chiyoda-ku, Tokyo, 101-0031
Japan

Synology®

synology.com