

How to implement an SSO solution on Synology NAS with Microsoft Azure AD Domain Services

Synology, as a single-sign-on (SSO) solution, allows users to sign in to any one of your web applications and services while, simultaneously, being able to access any other by that initial sign-in. Thus, Synology acts as the ultimate merge of all your web applications and services in a single sign-in.

Considering the benefits, your subscription to Microsoft Azure allows you to join your Synology NAS as an SSO client to Microsoft Azure Active Directory Domain Services. By this means, you can consider the need of domain controllers on premises' deployment and management done.

This tutorial will provide you all the information and the step that you will need to join your Synology NAS to Azure AD Domain Services, and how to enable Azure SSO service.

Before you start make sure the operating system of your Synology NAS has been updated to DiskStation Manager (DSM) on the latest version. Make sure an IPSec (Internet Protocol security) VPN (Virtual Private Network) tunnel has been set up between Microsoft Azure Virtual Network and the network where you located your Synology NAS.

A. Firstly, you need to Enable Microsoft Azure AD Domain Survives

- 1. Log in to your *Microsoft Azure Account*
- 2. On Azure Portal Click New \rightarrow Security + identity \rightarrow Azure AD Domain Services





3. Configure the Basic settings

| Enable Default Dire | Enable Azure AD Domain Services × | | | 1 | Basics | | | × |
|------------------------|---|---|--|---|--|-----------------------|----|---|
| 1 | Basics Configure basic settings | > | | [| Directory name 群暉科技股份存 | 有限公司 | | |
| 2 | Network Select virtual network | | | | Subscription | | | |
| 3 | Administrator group Configure group membership | | | | QC4 Resource grou Create new | ip ⊕ O Use existir | ng | |
| 4 | Summary Enable Azure AD Domain Servi | | | | Synology Location East Asia | | | • |
| | | | | | ОК | | | |



4. Configure the Network Settings. Select the Virtual Network and Subnet for **YOUR** Azure AD Domain Services

| Enable Azure AD Domain Serv Default Directory | ices X | × Network × |
|---|--------|--|
| Basics Configure basic settings | ~ | It is recommended that you create a dedicated subnet for use with this domain service. After the domain service is created you will not be able to modify the subnet. To manage your existing |
| 2 Network Select virtual network | > | Virtual network Virtual network Virtual network Virtual network |
| Administrator group Configure group membership | | Synology_VPN * Subnet AD |
| 4 Summary Enable Azure AD Domain Servi | | |
| | | |
| | | ОК |

5. Configure Administrator group settings. Add the members who will manage the specific domain.

| Enable Default Dir | Azure AD Domain Serv | vices × | Administrator group | × | Members AAD DC Administrators | | × |
|-----------------------|---|---------|---|---|----------------------------------|------|---|
| 1 | Basics | ~ | The "AAD DC Administrators" group will have privileges to administer this managed domain. Click below to manage membership. | | + Add members 2 | | |
| | Conligure basic settings | | | | NAME | ТҮРЕ | |
| 2 | Network | , | AAD DC Administrators AAD DC Administrators | > | administrator | User | |
| 2 | Select virtual network | | | - | QC4 | User | |
| 3 | Administrator group Configure group membership | | | | | | |
| 4 | Summary Enable Azure AD Domain Servi. | | | | | | |
| | | | З | | | | |



- 6. Lastly, Check the summary, if all the settings are correct click **OK** to enable Azure AD Domains Services.
- 7. Once you complete the setup of Azure AD Domain, find your Domain IP address on the virtual network to start the configuration on Synology NAS.
 - a) On Azure Portal click → all resources → sunology.com → Properties → Look for IP ADDRESS
 ON VIRTUAL NETWORK

| ≡ | All resources 群暉科技設份有限公司 | * × | synology.com - Properties | |
|--|---|----------|---------------------------|--|
| + New | ➡ Add III Columns Filter by name | ••• More | Search (Ctrl+/) | DNS DOMAIN NAME |
| All resources | 10 items NAME 11 | | Overview Activity log | |
| Resource groups App Services | aadds-3cf3b06dc2ae4e8 aadds-3cf3b06dc2ae4e8 | | Access control (IAM) | East Asia AVAILABLE IN VIRTUAL NETWORK/SUBNET |
| Function Apps | aadds-4b1f8c309bae463f··· | | | Syno_VNet/AD_Domain |
| Azure Cosmos DB | Azure_to_RT2600ac GatewavIP | | TROUBLESHOOTING + SUPPORT | 10.237.1.5 10.237.1.4 |
| Virtual machines | Sean_RT2600ac | | X Troubleshoot | SECURE LDAP Disabled |
| Load balancers Storage accounts | Syno_VNet Syno_VNet_Gateway | | New support request | RESOURCE GROUP |
| ↔ Virtual networks | synology.com | 2 | | ADMIN GROUP |
| Azure Active Directory | | | | AAD DC Administrators |

b) Save the IP Address.

Note: You might need to update DNS Server and set up password synchronization on Azure Portal.

B. Secondly, Join your Synology NAS to Azure AD Domain.

- 1) Sign into your DSM on Synology NAS as an administrator.
- 2) Go to **Control Panel** → **Domain/LDAP** → **Domain**



| | Control P | anel ? – E X | | | | |
|-------------------|--|---|--|--|--|--|
| Search | Domain 2 LDAP SSO Client | | | | | |
| ∧ File Sharing | 🧹 Join domain | | | | | |
| Shared Folder | Domain: | SYNOLOGY.COM | | | | |
| | DNS Server: | 10.237.1.5,10.237.1.4 | | | | |
| File Services | Domain Server Type: | | | | | |
| 9 User | Management Mode: | Trusted Domain 💌 | | | | |
| | Advanced domain options (Required only under specific network environment) | | | | | |
| 🙎 Group | DC IP/FQDN: | DC LIST (EXAMPLE: 192.168.1.1,DC1.DOMAIN.COM,*) | | | | |
| | Domain NetBIOS name: | NETBIOS NAME (EXAMPLE: DOMAIN) | | | | |
| | Domain FQDN (DNS name): | DOMAIN FQDN (EXAMPLE: DOMAIN.COM) | | | | |
| ∧ Connectivity | Register DNS interface: | All network interfaces | | | | |
| QuickConnect | Update user/group list: | Disable 💌 | | | | |
| | Domain Options | | | | | |
| 😚 External Access | Domain Status Check | | | | | |
| 🚖 Network | | 3 | | | | |
| | | Apply Reset | | | | |

- a) Tick the *Join Domain* Checkbox.
- b) Domain: Here, always type SYNOLOGY.COM
- c) **DNS Server**: Enter the Azure AD Domain IP Address.
- d) Click **APPLY**.
- 3) Once A Window will pop up.
 - a) Enter the credentials of Azure AD Domain's Administrator and click Next.
 - b) Once you read the notes, click **OK** to start Joining.
 - c) When the Domain Join is complete, click **Finish**.
 - d) Now you can view all the users and groups managed on Azure Active Directory.

| 1 | | Control Panel | | | 7 - 0) |
|-------------------|----------------|--|----------------------|-------------|------------|
| Search | Domain LDAP | Domain Users | Domain Group SSO Cli | ent | |
| ∧ File Sharing | Edit User Home | Update domain dat | a OU: | 🔻 🏹 Se | arch |
| Shared Folder | Name | Full name | Email | Description | Status |
| | SYNOLOGY | 100 | | | Normal |
| File Services | SYNOLOGY | | | | Normal |
| • | SYNOLOGY\ | | | | Normal |
| User | SYNOLOGY\ | | | | Normal |
| Group | SYNOLOGY\ | | | | Normal |
| Group | SYNOLOGY\ | | | | Normal |
| Domain/LDAP | SYNOLOGY\ | | | | Normal |
| | SYNOLOGY\ | | | | Normal |
| Connectivity | SYNOLOGY\ | | | | Normal |
| OuickConnect | SYNOLOGY | | | | Normal |
| | SYNOLOGY\ | | | | Normal |
| S External Access | SYNOLOGY\ | | | | Normal |
| | SYNOLOGY\ | | | | Normal |
| Network | SYNOLOGY | the second s | | | Normal |
| DHCP Server | | | | | 22 item(s) |



C. Lastly, Enable Azure SSO Service on Synology NAS.

- 1) Log in to your Microsoft Azure Account.
- On Azure Portal, go to Azure Active Directory → App Registrations, and click New Application Registration.
- 3) Once you click on New Application Registration, a window will pop up.
 - a) Configure the setting and then click **Create**.
 - b) Name: Enter the Application's Name.
 - c) Application Type: select Web app / API.
 - d) **Sing-on URL:** Enter the URL of your Application's login page. (Synology URL)

| Create | × |
|---|---|
| * Name 0 | |
| AzureSSO 🗸 | |
| Application type 🖲 | |
| Web app / API 🗸 🗸 🗸 | |
| * Sign-on URL 🛛 | |
| https://118.165.158.46:5001/webman/login. 🗸 | |
| | |
| | |
| | |
| | |
| | |
| Create | |

4) Once the application is created, it will appear in the list. Then click on it to get all the details you might need.



| New application registration 🗄 El | ndpoints 🗙 Troubleshoot | |
|---|---|--------------------------------------|
| To view and manage your registrations fo Search by name or AppID | r converged applications, please visit the My apps ~ | Microsoft Application Console. |
| DISPLAY NAME | APPLICATION TY | PE APPLICATION ID |
| AZ AzureSSO | Web app / API | b93708d0-5d87-43f7-9477-aa03a0df560d |

- 5) Below Settings, Copy and save the Application ID.
- 6) Click Settings \rightarrow Keys.

| AzureSSO Registered app 2 | | * × | S | ettings O Filter settings | × |
|--|--|-----|---|------------------------------|---|
| Display name AzureSSO | Application ID b93708d0-5d87-43f7-9477-aa03a0df560d | 1 | (| SENERAL | |
| Application type Web app / API | Object ID 44e0745d-ef62-4fa3-b886-f7a3a9cf2eeb | | | Properties | > |
| Home page https://118.165.158.46:5001/webman/logi | Managed application in local directory AzureSSO | | | 📃 Reply URLs | > |
| | * | | | 🞦 Owners | > |
| | | | | IPI ACCESS | |
| | | | | Required permissions | > |
| | | | 3 | 🕈 Keys | > |
| | | | | | |

- 7) Once you click on Key button, follow the bellow instruction to generate the application key:
 - a) Set up the key's **Description** and duration of validity (expires).
 - b) Click Save.
 - c) The key will appear at the VALUE column. Make sure you copy and save the value before exiting the specific page.



| Keys | | | | □ × |
|-------------------------------|---------------------------|-----|---------------------------------|-----|
| R Save X Discard | \Lambda Upload Public Key | | | |
| 3 Passwords description | EXPIRES | | VALUE | 4 |
| AzureSSOkey 1 | V Never expires | 2 ~ | Value will be displayed on save | |
| - | | | | |

- 8) On Azure Portal go to Azure Active Directory \rightarrow Properties and copy the Directory ID.
- 9) Go to DSM **Control Panel** → **Domain/LDAP** → **SSO Client**, then follow the bellow instruction:
 - a) Tick Enable OpenID Connect SSO Services.
 - b) Select Azure in the Profile Drop-Down list.
 - c) Click Edit.

| | Control Panel | ? — E X |
|------------------------|-----------------------------------|---------|
| Domain LDAP Dom | ain Users Domain Group SSO Client | |
| Enable Synology SSO se | rvice | |
| SSO server URL: | http://nas.example.com:5000 | |
| Application ID: | Register now | |
| 2 Select SSO by defa | ult on the login page | |
| Enable OpenID Connect | SSO service | |
| Profile: | 3 ~ | Edit 4 |
| | azure | |
| | websphere | |

d) Paste the values of Application ID, Keys and Directory ID and enter the Redirect URL of your application's login page.

| | Profile | |
|-----------------|--------------------------------------|--|
| Application ID: | b93708d0-5d87-43f7-9477-aa03a0df560d | |
| Keys: | | |
| Directory ID: | b0c81ce5-4ea8-4a64-b1b4-26769fa2d492 | |
| Redirect URI: | https://118 | |
| | | |
| | | |
| | | |
| | Apply Cancel | |



- 10) Click **Apply** when the configuration is complete.
- 11) All the active members managed by your Azure Active Directory can now sign into your Synology NAS hosting Application with their credentials. To Sign in with SSO, select Azure SSO Authentication from the drop-down list.

| \leftarrow \rightarrow \circlearrowright \pitchfork https://118 | □ ☆ | 7⁄≡ | l~ | Ŀ | |
|---|-----|-----|----|---|--|
| | | | | | |
| Seán | | | | | |
| Azure SSO Authentication \sim | 0 | | | | |
| Stay signed in | | | | | |
| Next | 2 | | | | |

12) Users will see a pop-up window requiring their account credentials.





13) Lastly, users will see a confirmation. Press Accept to sing in.



The implementation has been successfully completed.