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

Synology provides a single-sign-on (SSO) solution to integrate all your web applications and services. Once users sign in to any one of your web applications and services with their credentials, they can access any other ones without signing in again.

Aside from the benefits mentioned above, with your existing subscription to Microsoft Azure[™], you can also join your Synology NAS as an SSO client to Microsoft Azure Active Directory Domain Services. This exempts you from the need to deploy and manage domain controllers on premises.

This tutorial will guide you through how to join your Synology NAS to Azure AD Domain Services, and how to enable Azure SSO service.

Contents

- 1. Before you start
- 2. Enable Microsoft Azure AD Domain Services
- 3. Join Synology NAS to Azure AD Domain
- 4. Enable Azure SSO service on Synology NAS

1. Before you start

Before you proceed with the setup, please make sure you have already had an adequate environment as described below.

- The operating system of your Synology NAS has been updated to **DiskStation Manager (DSM)** 6.2 or above.
- An IPSec VPN tunnel has been set up between Microsoft Azure virtual network and the network where your Synology NAS is located. We recommend setting up your local network with a Synology Router. For detailed steps, please refer to this <u>tutorial</u>.

Note:

- The domain join function is not available on Synology Embedded DataStation and Network Video Recorder products.
- Visit <u>Microsoft Azure AD Domain Services</u> website to learn more on their pricing details.

2. Enable Microsoft Azure AD Domain Services

1. Log in to your <u>Microsoft Azure</u> account.

2. Click New > Security + Identity > Azure AD Domain Services.



3. <u>Configure the basic settings.</u>

E	nable efault Dire	Azure AD Domain Serv	ices	s 🗙 Basics	×
	1	Basics Configure basic settings	>	Directory name 群暉科技股份有限公司	
	2	Network Select virtual network		Subscription	
	3	Administrator group Configure group membership		QC4 ✓ ★ Resource group Create new Use existing	
	4	Summary Enable Azure AD Domain Servi		Synology	
				ОК	

4. In the Network step, select the Virtual network and Subnet for your Azure AD Domain services.



Note:

For the configuration of Azure Virtual Network, you may refer to the **tutorial** on how to set up

Site-to-Site VPN between Synology Router and Microsoft Azure.

5. In the **Administrator group** step, specify the members who are given the privileges to manage the domain.

Enable Default Dir	Azure AD Domain Sen	vices ×	Administrator group	×	Members AAD DC Administrators		×
1	Basics Configure basic settings	~	The "AAD DC Administrators" group will have privileges to administer this managed domain. Click below to manage membership.	1	+ Add members 2		
2	Network		AAD DC Administrators 0 Manage group membership	>	NAME AD administrator	түре User	
	Select virtual network			_	QC QC4	User	
3	Administrator group Configure group membership						
4							
			ОК				

6. Check the summary of your setup, and click **OK** to enable Azure AD Domain Services.



7. Once the deployment of your newly created Azure AD Domain is complete, find the domain's IP addresses on the

virtual network, which will later be used in the configuration on Synology NAS.

≡	All resources 群晖科技股份有限公司	* ×	synology.com - Properties	
+ New	Add 📑 Columns	••• More		
🗉 Dashboard 🛛 🚺	Filter by name			
	10 items		Overview	synology.com
	NAME		Activity log	LOCATION
Resource groups			Access control (IAM)	East Asia
🔇 App Services	aadds-3cf3b06dc2ae4e8…			AVAILARLE IN VIRTUAL NETWORK/SUBNET
	aadds-3cf3b06dc2ae4e8…		MANAGE	Syno_VNet/AD_Domain
Function Apps	aadds-4b1f8c309bae463f…		Properties	
👼 SQL databases	aadds-6eea2934ed38493…		Secure LDAP	IP ADDRESS ON VIRTUAL NETWORK
🦉 Azure Cosmos DB	Azure_to_RT2600ac			10.237.1.5 10.237.1.4
_	GatewayIP			SECURE LDAP
Virtual machines	🚸 Sean_RT2600ac		🗙 Troubleshoot	Disabled
🚸 Load balancers	<↔ Syno_VNet		New support request	
	Syno_VNet_Gateway			RESOURCE GROUP
	synology.com	2		synology
↔ Virtual networks				ADMIN GROUP
4 Azure Active Directory				AAD DC Administrators

8. You may need to update DNS server and set up password synchronization on Azure Portal. For detailed steps, please follow the instructions on Azure Portal.

3. Join Synology NAS to Azure AD Domain

1. Sign in as administrator to DSM on the Synology NAS that you wish to join to Azure AD Domain.

2. Go to **Control Panel > Domain/LDAP > Domain**, and configure the following settings:

	Control Pa	nel ? – 🗖 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:				
👤 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			
🔝 DHCP Server		Apply Reset			

- a. Tick the **Join domain** checkbox.
- b. **Domain**: Here, we enter *SYNOLOGY.COM*.
- c. **DNS Server**: Enter the Azure AD domain's IP address. If you have more than one address, simply separate them with comma.
- d. Click **Apply**.
- 3. Enter the credentials of Azure AD domain's administrator, and click **Next**.

Domain	×
Join Windows Domain	

Please enter an administrator user name and its password of the Windows domain you want to join.

Name:	@synology.com	
Password:	•••••	
Specify OU		

Cancel

4. Read the notes, and click **OK** to start joining.

	Domain	
Join Wine	dows Domain	
Note: Back	 System time will be changed according to the to on the Windows domain server when joining do and to serve Saving become the NTP serve Saving System DNS server settings will be changed if specify a DNS server IP. Network service will restart when these setting applied. 	time omain, you s are ncel
hen the domain ic	nin is complete click Finish	
hen the domain jo	pin is complete, click Finish . Domain	
hen the domain jo	Domain Status Check	
hen the domain jo Domain S Check Items	Domain Status Check St	atus
hen the domain jo Domain S Check Items Check if the c	Domain Domain Status Check St connection works properly between Synology	atus Q
ben the domain jo Domain S Check Items Check if the c Check if confli	Domain Domain Status Check St connection works properly between Synology icting hostnames exist in the subnet	atus Q
ben the domain jo Domain S Check Items Check if the c Check if confli Check if the c	Domain Domain Ctatus Check Status Check St connection works properly between Synology icting hostnames exist in the subnet connection works properly between Synology	atus O O O
Domain S Check Items Check if the c Check if the c Check if the c Check if the c	Domain Domain Status Check St connection works properly between Synology icting hostnames exist in the subnet connection works properly between Synology connection works properly between Synology	atus O O O O O
Domain S Check Items Check if the c Check if the c Check if the c Check if the c Check if the c	Domain Domain Ctatus Check Status Check St connection works properly between Synology icting hostnames exist in the subnet connection works properly between Synology Connection works properly between Synology TU is configured correctly to ensure the con	atus O O O O O O O O O O O O

6. You can now view the users and groups managed on Azure Active Directory.

8 0		Control Panel			? -
Search	Domain LDAP	Domain Users	omain Group SSO Cl	ient	
 File Sharing 	Edit User Home	Update domain dat	a OU:	🔻 🍸 Se	arch
 Shared Folder 	Name	Full name	Email	Description	Status
	SYNOLOGY				Normal
🕁 File Services	SYNOLOGY				Normal
•	SYNOLOGY				Normal
Vser User	SYNOLOGY				Normal
Group	SYNOLOGY				Normal
Group	SYNOLOGY				Normal
Domain/LDAP	SYNOLOGY				Normal
	SYNOLOGY				Normal
Connectivity	SYNOLOGY				Normal
3 OuickConnect	SYNOLOGY				Normal
	SYNOLOGY				Normal
😚 External Access	SYNOLOGY				Normal
	SYNOLOGY				Normal
🟠 Network	SYNOLOGY				Normal
•					22 item(s)

4. Enable Azure SSO service on Synology NAS

1. On Azure Portal, go to **Azure Active Directory > App registrations**, and click **New application registration**.

		egistrations <u>3</u>
+ New	Overview	+ New application registration 🗄 Endpoints 🗙 Troubleshoot
🖪 Dashboard	🗹 Quick start	To view and manage your registrations for converged applications, please visit the Microsoft Application Console.
All resources	MANAGE	Search by name or AppID My apps V
📦 Resource groups	я ^q Users and groups	DISPLAY NAME APPLICATION TYPE APPLICATION ID
🚫 App Services	Enterprise applications	No results.
Function Apps	Devices 2	
👼 SQL databases	Registrations	
🤵 Azure Cosmos DB	Application proxy	
Virtual machines	🔓 Licenses	
🚸 Load balancers	Azure AD Connect	
Storage accounts	Custom domain names	
	Mobility (MDM and MAM)	
	📍 Password reset	
Azure Active Directory	Company branding	
Monitor	🔅 User settings	
Advisor	Properties	
Security Center	Notifications settings	
Oost Management + Billing	SECURITY	
Help + support	Conditional access	
More services >	MFA Server	
	🍟 Users flagged for risk 🛛 🗸	

2. <u>Configure the following settings, and then click **Create**:</u>

Create	
* Name 0	
AzureSSO	~
Application type 0	
Web app / API	~
* Sign-on URL €	
https://118.165.158.46:5001/webman/	login. 🧹
Create	

- **Name**: Enter the application's name.
- Application type: Select Web app / API.
- **Sign-on URL**: Enter the URL of your application's login page.
- 3. You will see the just now created application in the list, click on it to get essential information.

o view and manage your regist	trations for converged appli	rations please visit the Microso	off Application Console
Search by name or ApplD	My apps		Application console.
DISPLAY NAME		APPLICATION TYPE	APPLICATION ID

4. Copy the **Application ID**. Then, click **Settings** > **Keys**.

Note: You may skip to steps 7 and 8 to paste the copied value first.

AzureSSO Registered app 2 The Settings Manifest The Delete		* :	×	Settings	×
Display name AzureSSO	Application ID b93708d0-5d87-43f7-9477-aa03a0df560d	1		GENERAL	
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	
				API ACCESS	
				🔏 Required permissions	
			3	🕈 Keys	,
				TROUBLESHOOTING + SUPPORT	
				🗙 Troubleshoot	
				New support request	

5. Follow the steps below to generate the application's key:

Keys				
R Save X Discard	⊼ Upload Public Key			
3 Passwords				
DESCRIPTION	EXPIRES	VALUE		4
AzureSSOkey 1	Never expires 2	✓ Value will be displayed on save		
Key description	Duration	✓ Value will be displayed on save		
Public Keys				
THUMBPRINT		START DATE	EXPIRES	
No results.				

- . Set up the key's **DESCRIPTION** and duration of validity (**EXPIRES**).
- a. Click Save.
- b. The key will show at the **VALUE** column. You must copy it right away before leaving this page.

Note: You may skip to steps 7 and 8 to paste the copied value first.

6. Go to **Azure Active Directory** > **Properties** to copy the **Directory ID**.

≡	群暉科技股份有限公司 - Azure Active Directory	司 - Properties	
+ New	 Overview 	Save X Discard	
🔚 Dashboard	🥑 Quick start	* Name 群碼設持股份有限公司	
All resources	MANAGE	Country or region	
📦 Resource groups	g ^q Users and groups	Taiwan	
🔇 App Services	Enterprise applications	Location Asia, United States, Europe datacenters	
🦘 Function Apps	Devices	Notification language	
👼 SQL databases	App registrations	中文(新聞) Global admin can manage Anure Subscriptions	~
💓 Azure Cosmos DB	Application proxy	Yes No	3
Virtual machines	Licenses	Directory ID	
💠 Load balancers	Azure AD Connect	b0c81ce5-4ea8-4a64-b1b4-26/69fa2d492	
Storage accounts	Custom domain names		
🖘 Virtual networks 🛛 🚺	Mobility (MDM and MAM)		
Azure Active Directory	Password reset		
A Monitor	Company branding		
Monitor	User settings		
🌳 Advisor	Properties		
Security Center	Notifications settings		
Oost Management + Billing	SECURITY		
🎴 Help + support	Conditional access		
More services >	MFA Server		
	Users flagged for risk		

7. Go to DSM **Control Panel > Domain/LDAP > SSO Client**, and do the following steps:

		Control Panel	? - O X
Search	Domain LDAP Dom	ain Users Domain Group SSO Client	
V Group	Enable Synology SSO se	rvice	
Domain/LDAP	SSO server URL:	http://nas.example.com:5000	
∧ Connectivity	Application ID:	Register now	
🤣 QuickConnect	Enable OpenID Connect	SSO service	
😚 External Access	Profile:	3 azure	Edit 4
1 Network		websphere	
👧 DHCP Server			
🛜 Wireless			
😌 Security			
∧ System			
i Info Center			Apply Reset

- . Tick Enable OpenID Connect SSO service.
- a. Select **azure** in the **Profile** drop-down list.
- b. Click Edit.

8. Paste the copied values of Application ID, Keys, and Directory ID, as well as enter the Redirect URI of your

application's login page.

	Control Panel P - D X
Search	Domain LDAP Domain Users Domain Group SSO Client
💥 Group	Enable Synology SSO service
Domain/LDAP	SSO server URL: http://nas.example.com:5000
∧ Connectivity	Profile
	Application ID: b93708d0-5d87-43f7-9477-aa03a0df560d
QuickConnect	Keys:
😚 External Access	Directory ID: b0c81ce5-4ea8-4a64-b1b4-26769fa2d492
1 Network	Redirect URI: https://11846:5001/webman/login.cgi
👧 DHCP Server	
🛜 Wireless	Apply Cancel
당 Security	
∧ System	
i Info Center	Apply Reset

9. Remeber to click **Apply** when the configuration is complete.

		Control Panel	7 - E X
Search	Domain LDAP Dom	ain Users Domain Group SSO Client	
K Group	Enable Synology SSO ser		
Domain/LDAP	SSO server URL:	http://nas.example.com:5000	
∧ Connectivity	Application ID:	Register now Ilt on the login page	
💋 QuickConnect	Fnable OpenID Connect	SSO service	
G External Access	Profile:	azure	Edit
	Application ID:	b93708d0-5d87-43f7-9477-aa03a0df560d	
1 Network	OAuth 2.0 Token Endpoint:	https://login.microsoftonline.com/b0c81ce5-4ea8-4a64- b1b4-26769fa2d492/oauth2/token	
\delta DHCP Server	OAuth 2.0 Authorization	https://login.microsoftonline.com/b0c81ce5-4ea8-4a64-	
🛜 Wireless	Endpoint:	b1b4-26769fa2d492/oauth2/authorize	
Security	Redirect URI:	https://118. 46:5001/webman/login.cgi	
∧ System			
🧃 Info Center			Apply Reset

10. Valid users managed by your Azure Active Directory can now sign in to your Synology NAS hosting web application with their original credentials. To sign in with SSO, select **Azure SSO Authentication** from the drop-

Seán					
Azure SSO Authentication	- 1				
Stay signed in					
Next	2				
		Synolo	ov ne	SM 6	2 RC

)	https://login.microsoftonline.com/b0c81ce5-4ea8-4a64-b1b4-26769fa2d492/
	Microsoft
	Pick an account
	@synology.com
	+ Use another account

12. Users will then see a confirmation. Just click **Accept** to sign in.



©2018 Microsoft Terms of use Privacy & cookies