

## How to Configure MSAD Authentication Against Azure Active Directory

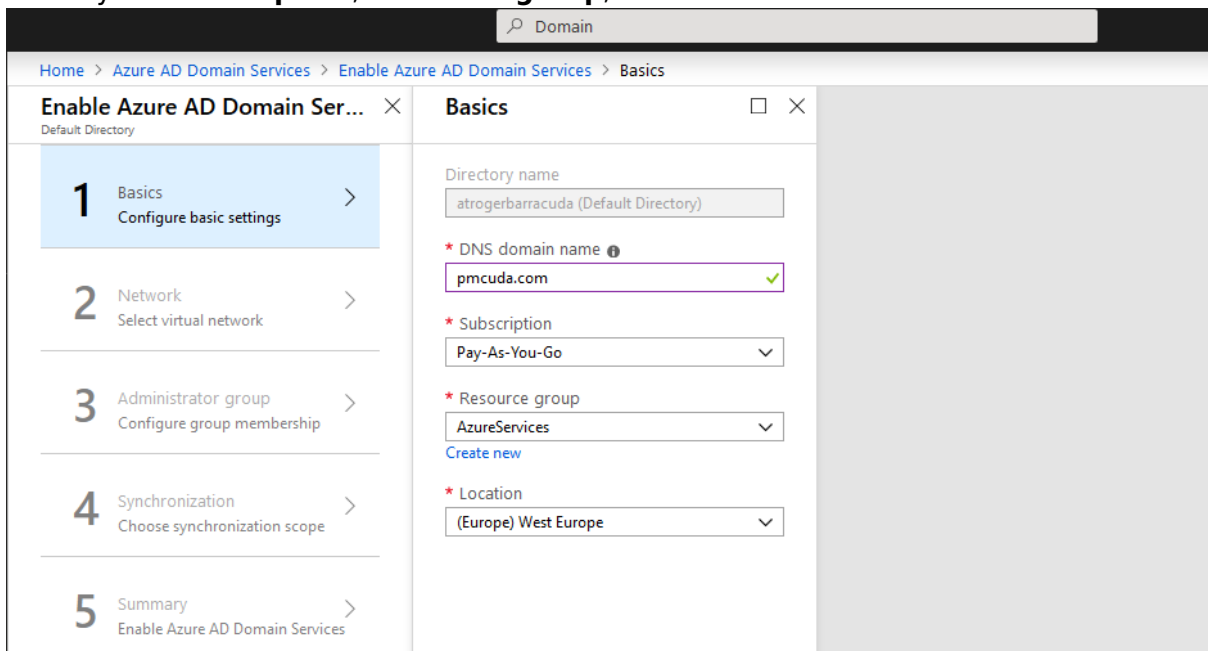
<https://campus.barracuda.com/doc/86542496/>

Azure Active Directory is a secure, cloud-based authentication store that lets you create users, groups, and applications that use authentication mechanisms such as MSAD. To configure MSAD authentication against Azure Active Directory, create your domain on the Azure Portal and define users who should be able to manage it. Then, activate Secure LDAP access over the Internet.

### Step 1. Add Your Domain to the Azure Portal

Enable Azure AD Domain Services and add your domain.

1. Log into the Azure Portal: <https://portal.azure.com>
2. In the left menu, click **Create a resource**.
3. In the search field, type domain and select **Azure AD Domain Services**.
4. Click **Create**. The **Azure AD Domain Services** configuration opens.
5. In the **Basics** blade:
  1. Enter the **DNS domain name** for your domain.
  2. Select your **Subscription, Resource group, and Location**.



The screenshot shows the 'Basics' blade in the Azure Portal for enabling Azure AD Domain Services. The blade is titled 'Enable Azure AD Domain Ser...' and has a search bar at the top with 'Domain' entered. The breadcrumb navigation is 'Home > Azure AD Domain Services > Enable Azure AD Domain Services > Basics'. The blade is divided into two sections: a left sidebar with numbered steps and a main content area with configuration fields.

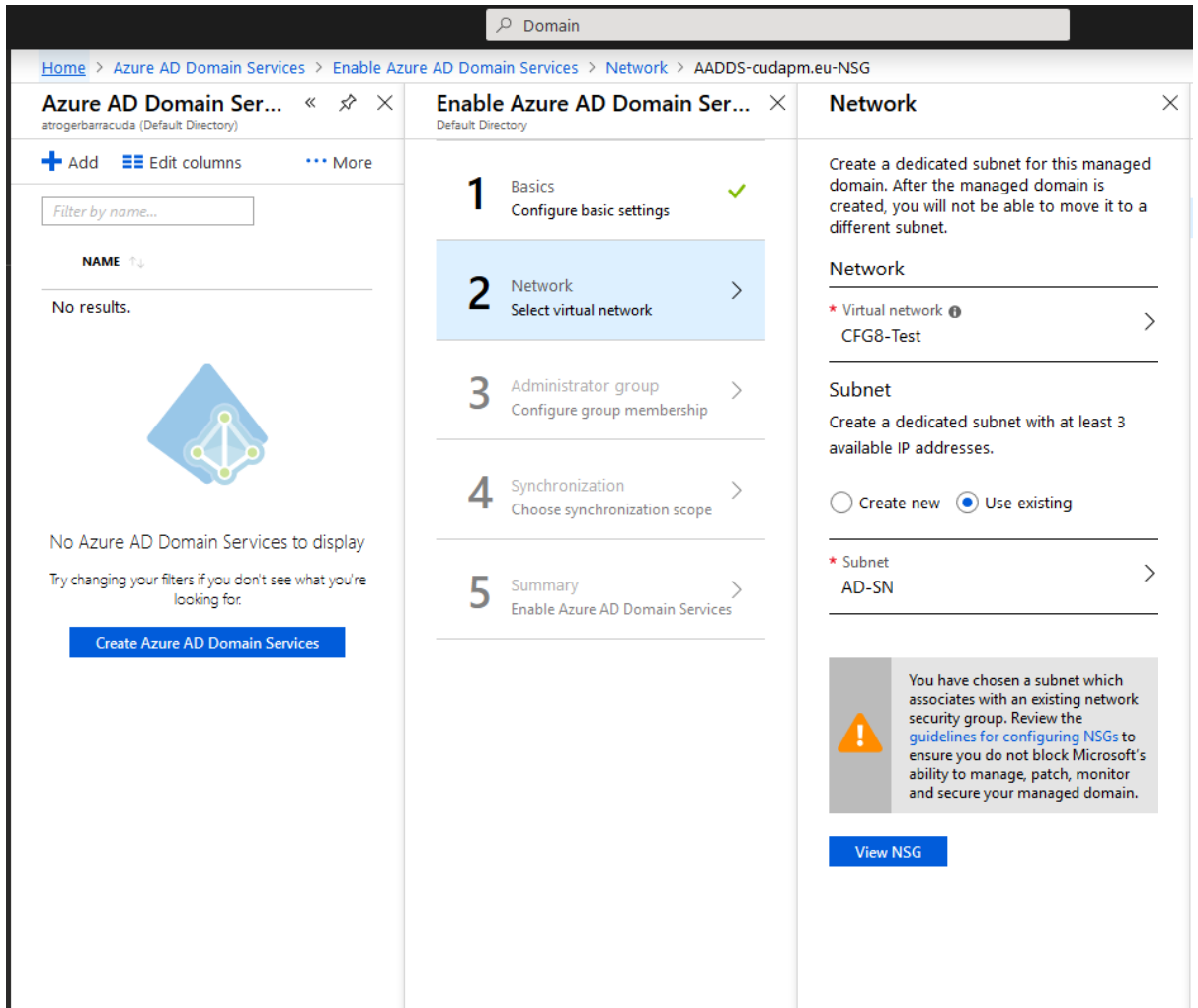
The left sidebar contains the following steps:

- 1 Basics: Configure basic settings
- 2 Network: Select virtual network
- 3 Administrator group: Configure group membership
- 4 Synchronization: Choose synchronization scope
- 5 Summary: Enable Azure AD Domain Services

The main content area contains the following configuration fields:

- Directory name: atrogerbarracuda (Default Directory)
- \* DNS domain name: pmcuda.com
- \* Subscription: Pay-As-You-Go
- \* Resource group: AzureServices
- \* Location: (Europe) West Europe

6. Click **OK**. In the **Network** blade:
  - Select or create the **Virtual network (VNET)**.
  - Select or create a **Subnet** for the service.



Domain

Home > Azure AD Domain Services > Enable Azure AD Domain Services > Network > AADS-cudapm.eu-NSG

**Azure AD Domain Ser...** atrogerbarracuda (Default Directory)

+ Add Edit columns More

Filter by name...

NAME

No results.

No Azure AD Domain Services to display  
Try changing your filters if you don't see what you're looking for.

Create Azure AD Domain Services

**Enable Azure AD Domain Ser...** Default Directory

- 1 Basics  
Configure basic settings ✓
- 2 Network  
Select virtual network
- 3 Administrator group  
Configure group membership
- 4 Synchronization  
Choose synchronization scope
- 5 Summary  
Enable Azure AD Domain Services

**Network**

Create a dedicated subnet for this managed domain. After the managed domain is created, you will not be able to move it to a different subnet.

Network

\* Virtual network  
CFG8-Test

Subnet

Create a dedicated subnet with at least 3 available IP addresses.

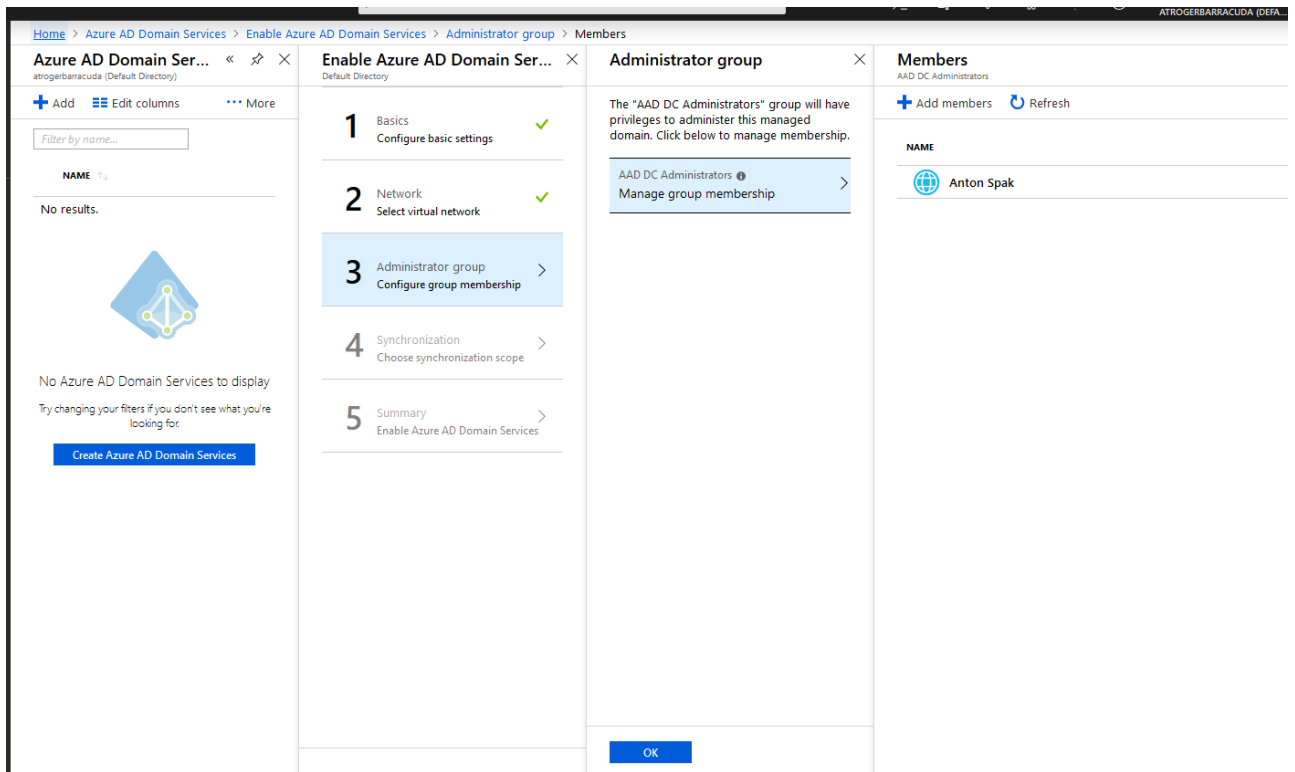
Create new  Use existing

\* Subnet  
AD-SN

You have chosen a subnet which associates with an existing network security group. Review the [guidelines for configuring NSGs](#) to ensure you do not block Microsoft's ability to manage, patch, monitor and secure your managed domain.

View NSG

7. Click **OK**. The group **AAD DC Administrators** will be automatically created.
8. Click **AAD DC Administrators**. The **Members** blade opens.
9. Click **+** to add the users and / or groups that should be able to manage the created domain.



10. Click **OK**. The **Synchronization** blade opens.
11. Select the scope of the users for domain synchronization.

Home > Azure AD Domain Services > Enable Azure AD Domain Services > Synchronization

### Enable Azure AD Domain Ser... ×


Default Directory

- 1** Basics ✓  
Configure basic settings
- 2** Network ✓  
Select virtual network
- 3** Administrator group ✓  
Configure group membership
- 4** Synchronization >  
Choose synchronization scope
- 5** Summary >  
Enable Azure AD Domain Services

### Synchronization □ ×

Synchronize all users and groups from Azure AD or synchronize scoped groups and their members. If you have a very large number of users and groups, you might want to consider starting with "scoped" synchronization which will improve the time to complete the synchronization.

**All** **Scoped**



Scoped synchronization can be modified with different group selections or converted to synchronize all users and groups. To change synchronization from "all" to "scoped", domain service instance needs to be deleted and re-created. [More information](#)

12. Click **OK**. The **Summary** blade opens.

Home > Azure AD Domain Services > Enable Azure AD Domain Services > Summary

**Enable Azure AD Domain Ser...** ×

Default Directory

- 1 Basics ✓  
Configure basic settings
- 2 Network ✓  
Select virtual network
- 3 Administrator group ✓  
Configure group membership
- 4 Synchronization ✓  
Choose synchronization scope
- 5 Summary >  
Enable Azure AD Domain Services

**Summary** □ ×

Basics

Name	pmcuda.com
Subscription	Pay-As-You-Go
Resource group	AzureServices
Location	(Europe) West Europe

Network

Virtual network	CFG8-Test
Subnet	AD-SN
Network security group	AADD5-cudapm.eu-NSG

Administrator group

Administrator group	AAD DC Administrators
Membership Type	Assigned

Synchronization

Synchronization scope	All
-----------------------	-----

**OK**

By enabling Azure AD Domain Services for this directory, you consent to storing credential hashes required for NTLM and Kerberos authentication in Azure AD.

13. Double-check your settings and click **OK** to finish the configuration. The Azure AD Domain Services will now be deployed.

It can take up to an hour until the deployment is completed.

## Step 2. Verify the Domain and Configure a Service User

After the deployment has succeeded, add and verify the domain to your Azure AD from the Azure **Default Directory - Custom domain names**.

1. Go to your domain.

Home > Default Directory - Custom domain names

### Default Directory - Custom domain names

Azure Active Directory

Search (Ctrl+V)

+ Add custom domain Refresh Troubleshoot Columns

Looking to move an on-premises application to the cloud and use Azure Active Directory Domain Services?

Status: Any Federated: All Primary: All

Apply Reset

Search

NAME	STATUS	FEDERATED	PRIMARY
atogerbarracuda.onmicrosoft.com	Available		✓
pmcuda.com	Unverified		

2. Configure a TXT or MX record on your domain register to verify the domain.

**test.com**  
Custom domain name

Delete

---

To use test.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

RECORD TYPE: **TXT** MX

ALIAS OR HOST NAME: @

DESTINATION OR POINTS TO ADDRESS: MS=ms50576124

TTL: 3600

Share these settings via email


Verify domain  
Verification will not succeed until you have configured your domain with your registrar as described above.


3. From **Users** on the left panel, add a service user to the domain.


Home > Default Directory > Users - All users > User > Profile


### User


Default Directory


\* Name 


 

\* User name 

Profile  Configured >

Properties  Default >

Groups  1 groups selected >

Directory role User >

Password

Show Password

### Profile

User

General

First name

Last name

Work info

Job title

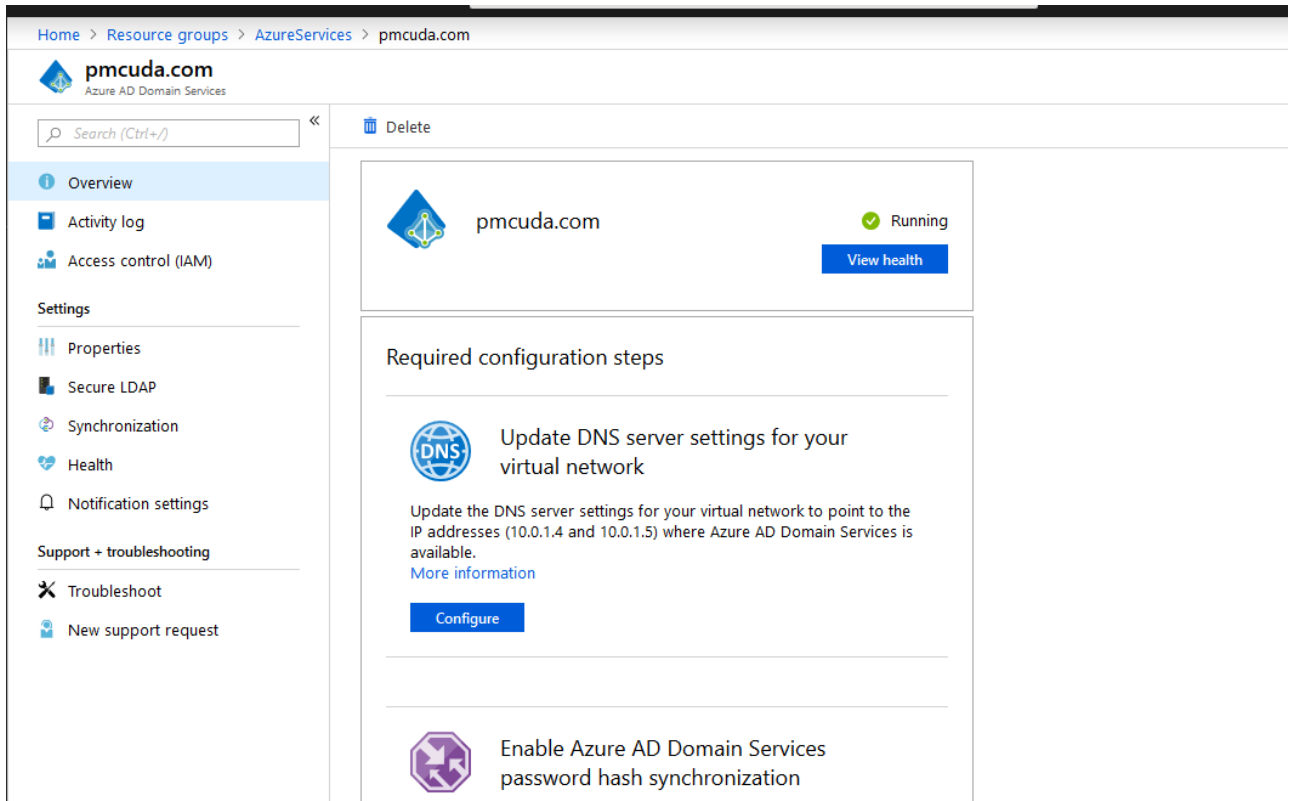
Department

4. Add the user to the Azure Admins Group.
5. After adding user login with this user, change the **Password**.

It is recommended to set the service user password not to expire.

### Step 3. Activate LDAPS

1. Go to **Azure AD Domain Services > your managed domain**.
2. Update / configure the DNS settings.



3. In the left menu, click **Secure LDAP**.
4. Enable **Secure LDAP**.
5. Enable **Allow Secure LDAP access over the internet**.

In this case, you will require a certificate for your domain. The certificate can be obtained from the root CA. Alternatively, a self-signed certificate can be used. For detailed information on how to create a self-signed certificate, refer to the Microsoft documentation:

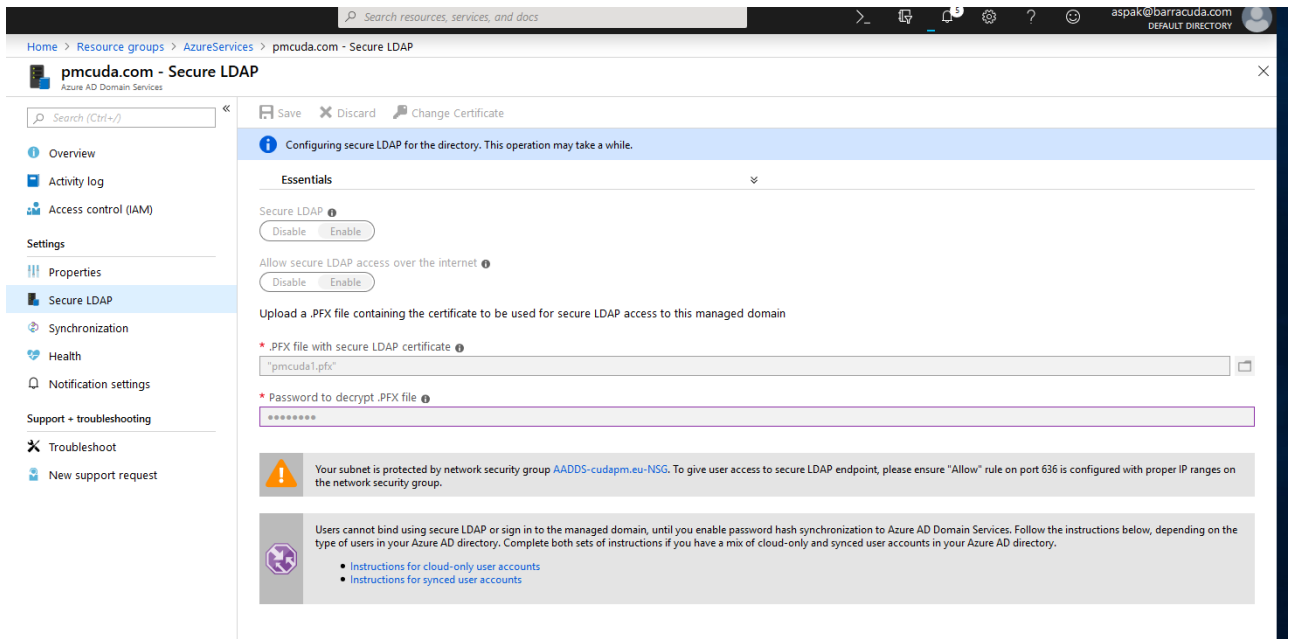
<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/configure-ldaps>

Recommendations:

- Use TripleDES-SHA1 encryption. Also make sure the password has at least 8 characters.
- The name should only include \*.pfx suffix. For example, do not use pmcuda.com.pfx. This will fail with incorrect password.

6. Add the certificate to activate LDAPs.





Home > Resource groups > AzureServices > pmcuda.com - Secure LDAP

**pmcuda.com - Secure LDAP**  
Azure AD Domain Services

Search (Ctrl+/)

Save Discard Change Certificate

Configuring secure LDAP for the directory. This operation may take a while.

**Essentials**

Secure LDAP

Allow secure LDAP access over the internet

Upload a .PFX file containing the certificate to be used for secure LDAP access to this managed domain

\* .PFX file with secure LDAP certificate

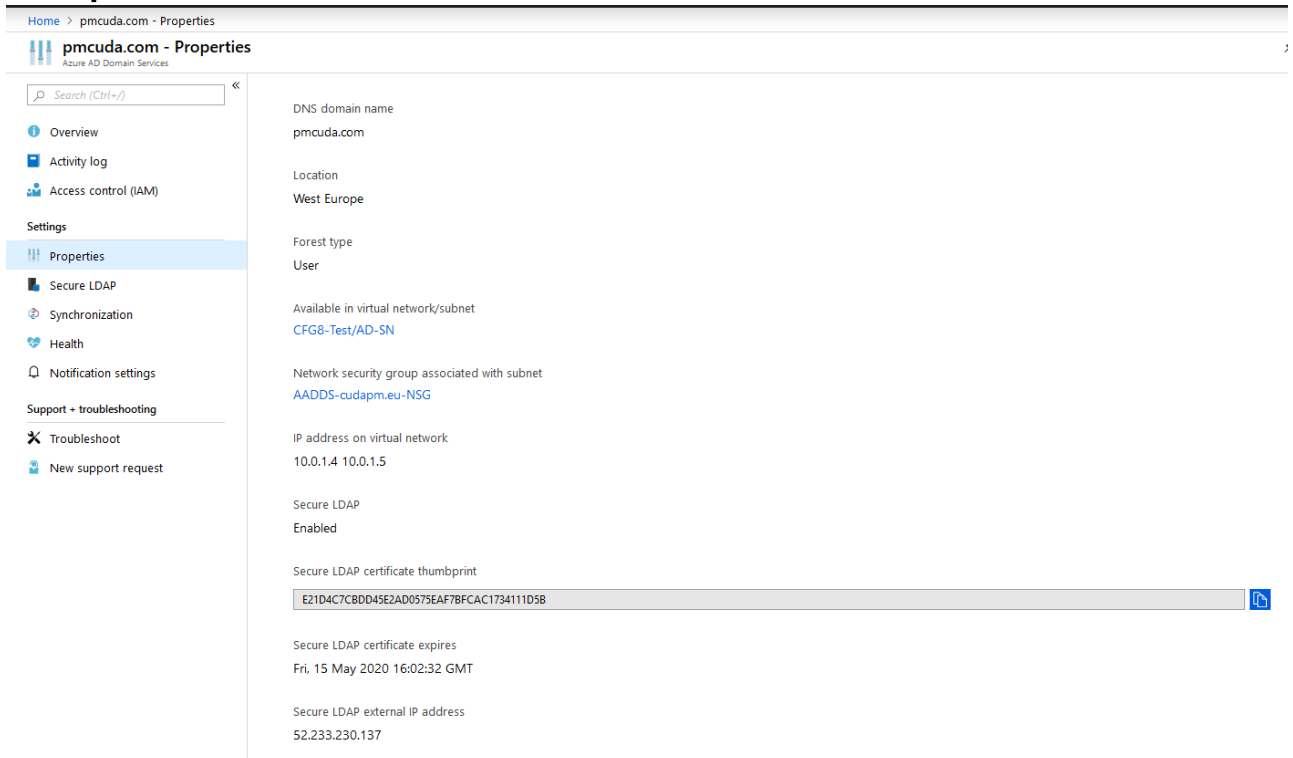
\* Password to decrypt .PFX file

**Warning:** Your subnet is protected by network security group AADD5-cudapm.eu-NSG. To give user access to secure LDAP endpoint, please ensure "Allow" rule on port 636 is configured with proper IP ranges on the network security group.

Users cannot bind using secure LDAP or sign in to the managed domain, until you enable password hash synchronization to Azure AD Domain Services. Follow the instructions below, depending on the type of users in your Azure AD directory. Complete both sets of instructions if you have a mix of cloud-only and synced user accounts in your Azure AD directory.

- Instructions for cloud-only user accounts
- Instructions for synced user accounts

7. The public IP and the associated NSG you need to point the CloudGen Firewall to can be found in **Properties**:



Home > pmcuda.com - Properties

**pmcuda.com - Properties**  
Azure AD Domain Services

Search (Ctrl+/)

Overview  
Activity log  
Access control (IAM)

Settings  
Properties  
Secure LDAP  
Synchronization  
Health  
Notification settings

Support + troubleshooting  
Troubleshoot  
New support request

DNS domain name  
pmcuda.com

Location  
West Europe

Forest type  
User

Available in virtual network/subnet  
CFG8-Test/AD-SN

Network security group associated with subnet  
AADD5-cudapm.eu-NSG

IP address on virtual network  
10.0.1.4 10.0.1.5

Secure LDAP  
Enabled

Secure LDAP certificate thumbprint  
E21D4C7CBDD45E2AD0575EAF7BFCAC1734111D58

Secure LDAP certificate expires  
Fri, 15 May 2020 16:02:32 GMT

Secure LDAP external IP address  
52.233.230.137

8. Set up the Network Security Group (NSG) according to your needs. Add at least port 636 to allow access via LDAPs for the on-premises CloudGen Firewall.

## Step 4. Configure LDAP Authentication on the CloudGen Firewall

1. On the CloudGen Firewall or Control Center, go to **Authentication Service > LDAP**

**Authentication.**

2. Configure the LDAPs using MSAD attribute settings according to this example:

Basic : 100000U=AADDC Users,DC=pmcuda,DC=com
— □ ×

<b>Basic</b>		
LDAP Base DN	<input type="text" value="OU=AADDC Users,DC=pmcuda,DC=com"/>	
LDAP Server	<input type="text" value="52.233.230.137"/>	
LDAP Server Port	<input type="text" value="636"/>	
LDAP User Field	<input type="text" value="sAMAccountName"/>	
LDAP Password Field	<input type="text" value="userPassword"/>	
Anonymous	<input type="text" value="No"/>	
LDAP Admin DN	<input type="text" value="SVC_LDAP@pmcuda.com"/>	
LDAP Admin Password	Current <input type="password"/> New <input type="password" value="•••••"/> Confirm <input type="password" value="•••••"/> Strength <input type="text"/>	
Group Attribute	<input type="text" value="memberOf"/>	
Cache LDAP Groups	<input type="text" value="No"/>	
Offline Sync [m]	<input type="text" value="60"/>	
Timeout [s]	<input type="text" value="3"/>	
<b>Mail Lookup</b>		
Additional Mail Fields	<input type="text"/>	
<b>Extended</b>		
Use SSL	<input checked="" type="checkbox"/>	
Log in to Authenticate	<input checked="" type="checkbox"/>	
Add User-DN as Group name	<input type="text" value="No"/>	

OK

Cancel

**LDAP Base DN**  
Enter the Base DN used for searching the directory.

**LDAP Server**  
Enter the IP address or hostname of the LDAP server.

**Note:**  
When using SSL, the server name should be used instead of the IP address.

**LDAP Server Port**  
Port of the LDAP server (default: 389).

**LDAP User Field**  
Name of the user identification attribute in the LDAP directory.

**LDAP Password Field**  
Name of the user password attribute in the LDAP directory.

**Anonymous**  
Enable this setting if no authentication is required.

**LDAP Admin DN**  
Enter the distinguished name for administrative rights.

**LDAP Admin Password**  
Set the password to authenticate on the LDAP server.

**Group Attribute**  
Enter the name of the attribute field on the LDAP server that contains group information.

**Note:**  
This is required when using services that process group information (e.g., URL Filter).

**Cache LDAP Groups**  
Enabling this setting causes the LDAP-authenticator to take group information out of the periodically synchronized database to reduce network traffic and server load on the LDAP server.

3. Click **OK**.
4. Click **Send Changes** and **Activate**.

For more information, please refer to the Microsoft documentation:  
<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-instance>

## Figures

1. az\_ad\_01.png
2. az\_ad02.png
3. az\_ad03.png
4. az\_ad04.png
5. az\_ad05.png
6. az\_ad06.png
7. az\_ad06a.png
8. az\_ad07.png
9. az\_ad08.png
10. az\_ad09.png
11. az\_ad10.png
12. az\_ad11.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.