How to Configure MSAD Authentication Against Azure Active Directory

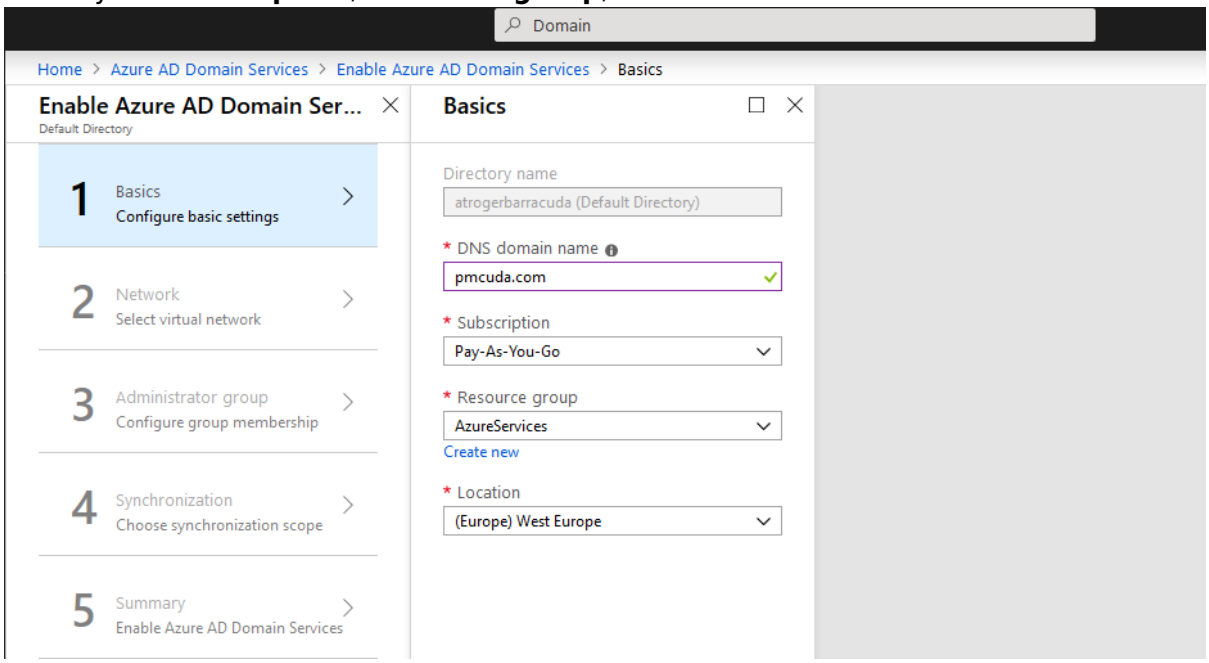
https://campus.barracuda.com/doc/86542123/

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.

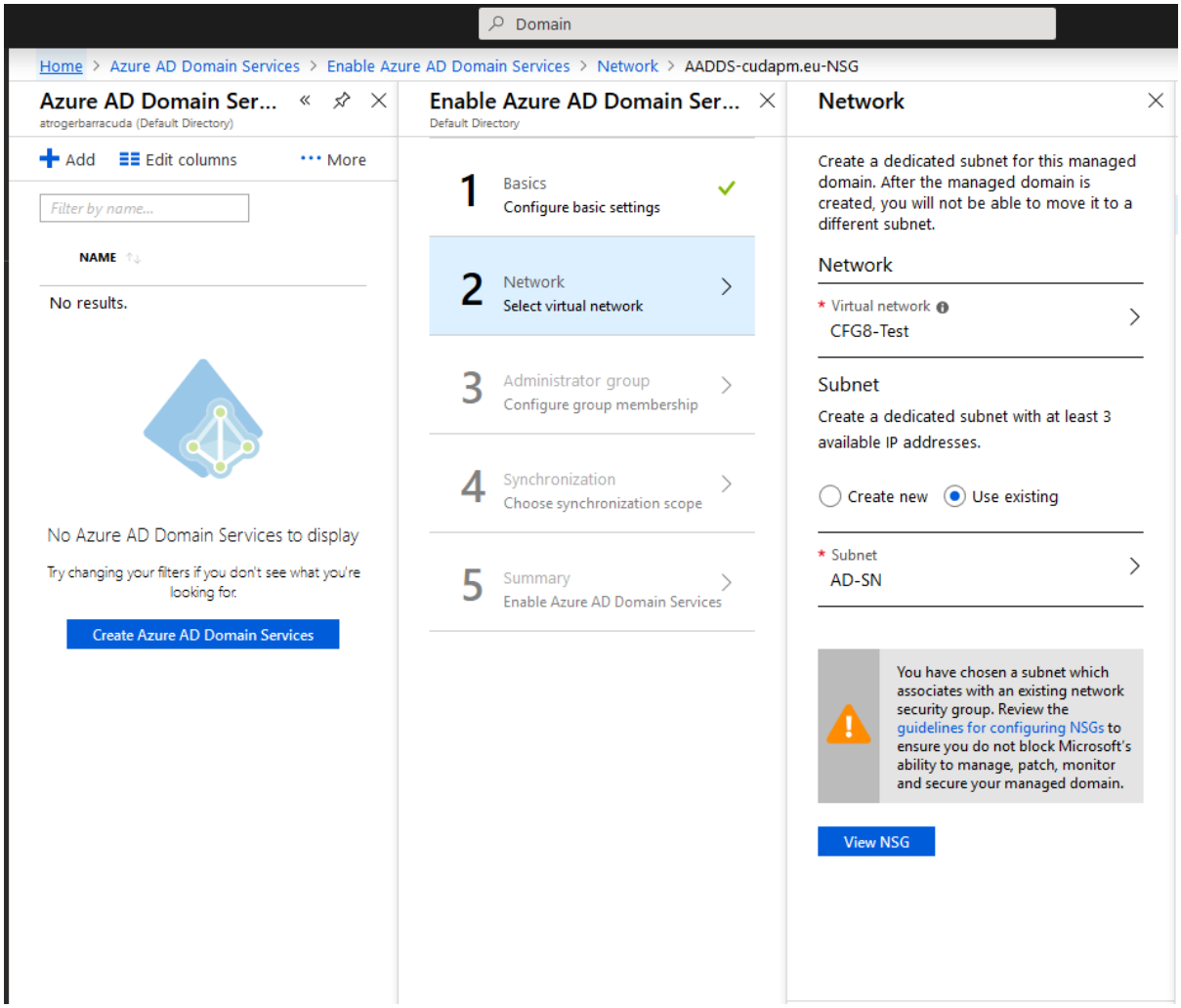
Step 1. Add Your Domain to the Azure Portal

Enable Azure AD Domain Services and add your domain.

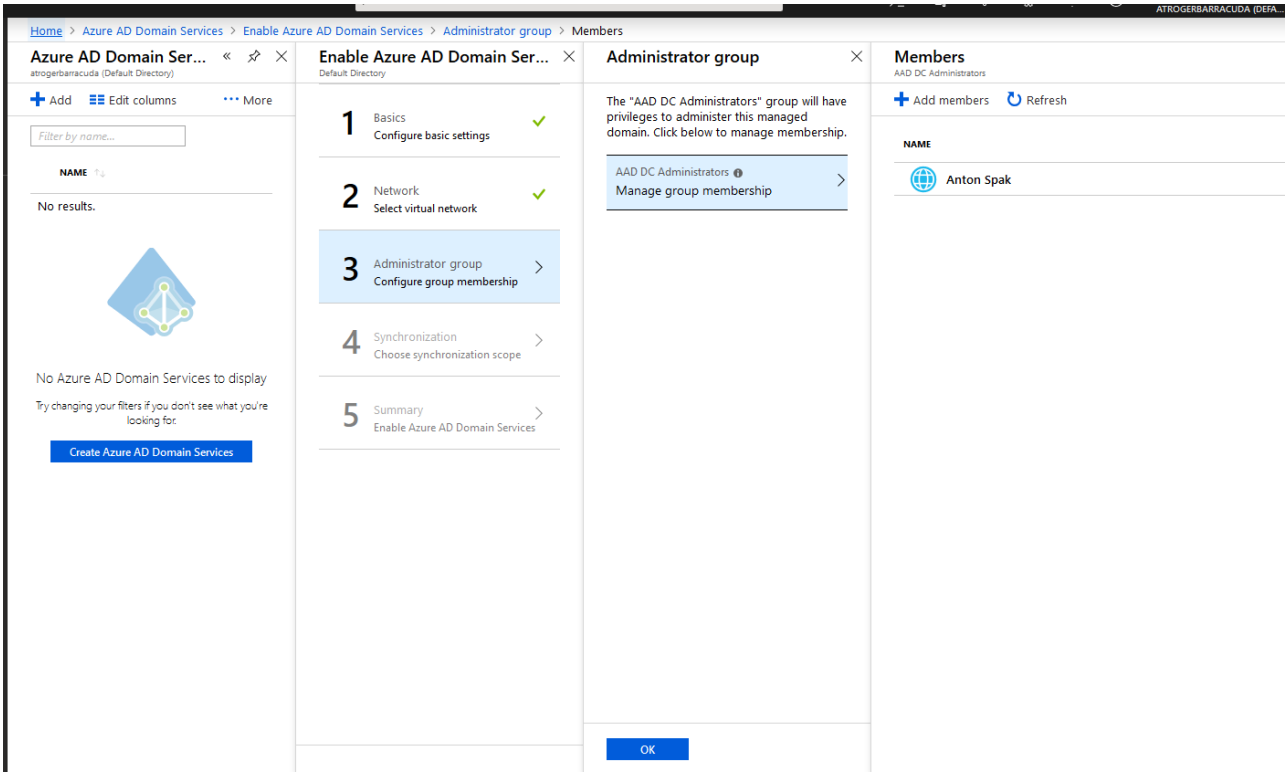
1. Log into the Azure Portal: https://portal.azure.com
2. In the left menu, click **Create a resource**.
3. In the search field, type `domain` and select **Azure AD Domain Services**.
4. Click **Create**. The **Azure AD Domain Services** configuration opens.
5. In the **Basics** blade:
    1. Enter the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



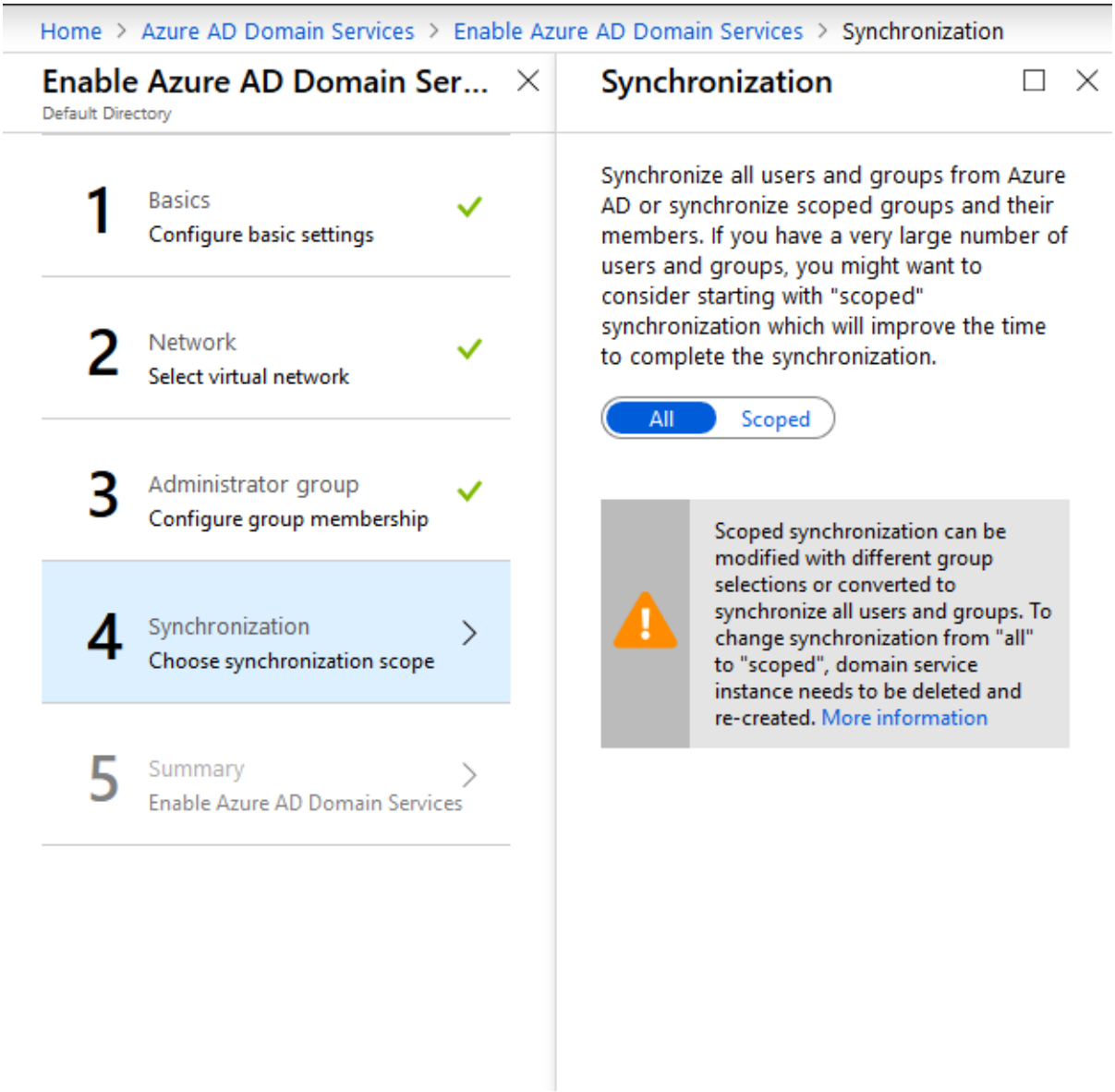
6. Click **OK**. In the **Network** blade:
    - Select or create the **Virtual network** (VNET).
    - Select or create a **Subnet** for the service.



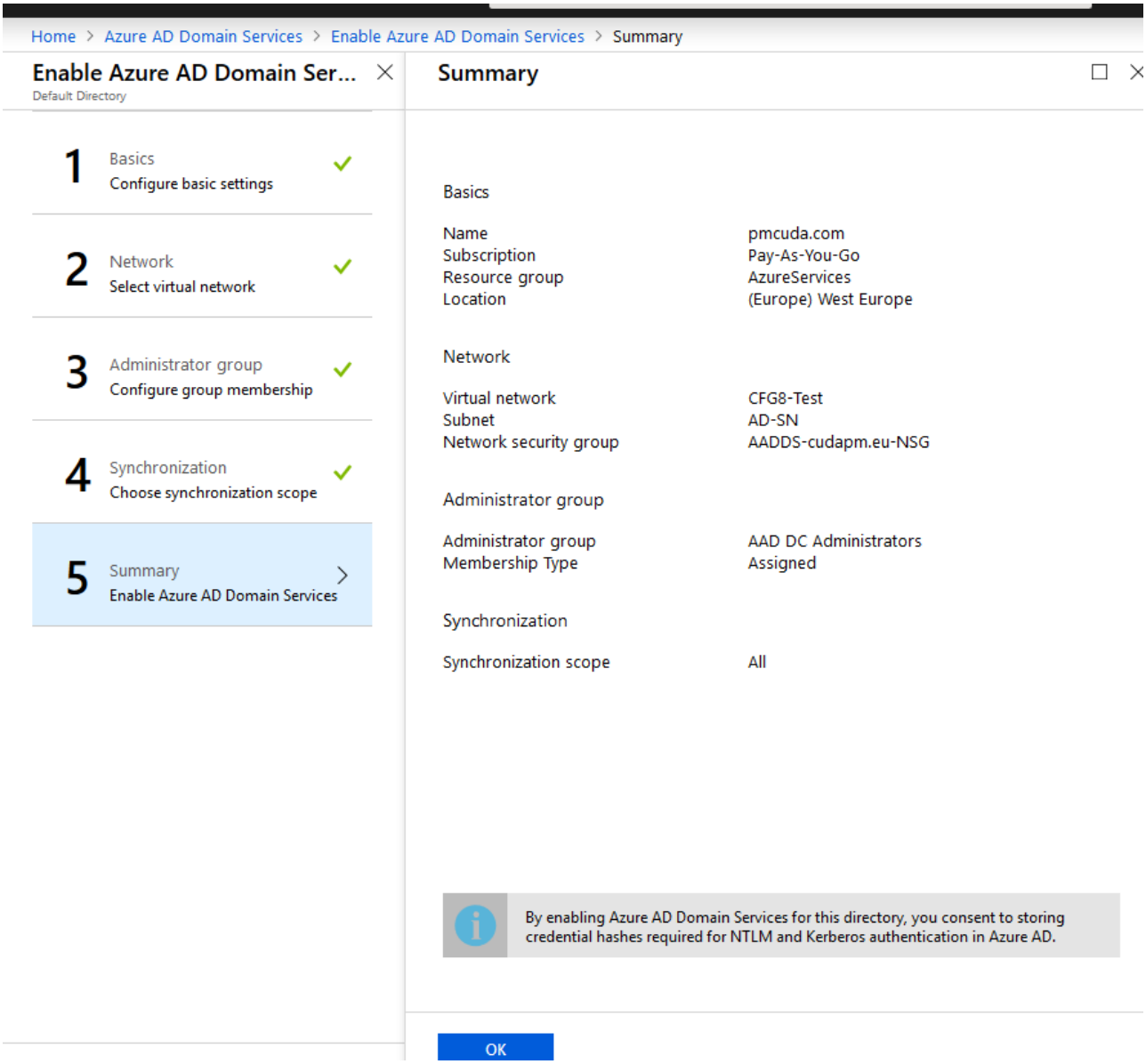
7. Click **OK**. The group **AAD DC Administrators** will be automatically created.
8. Click **AAD DC Administrators**. The **Members** blade opens.
9. Click **+** to add the users and / or groups that should be able to manage the created domain.



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



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



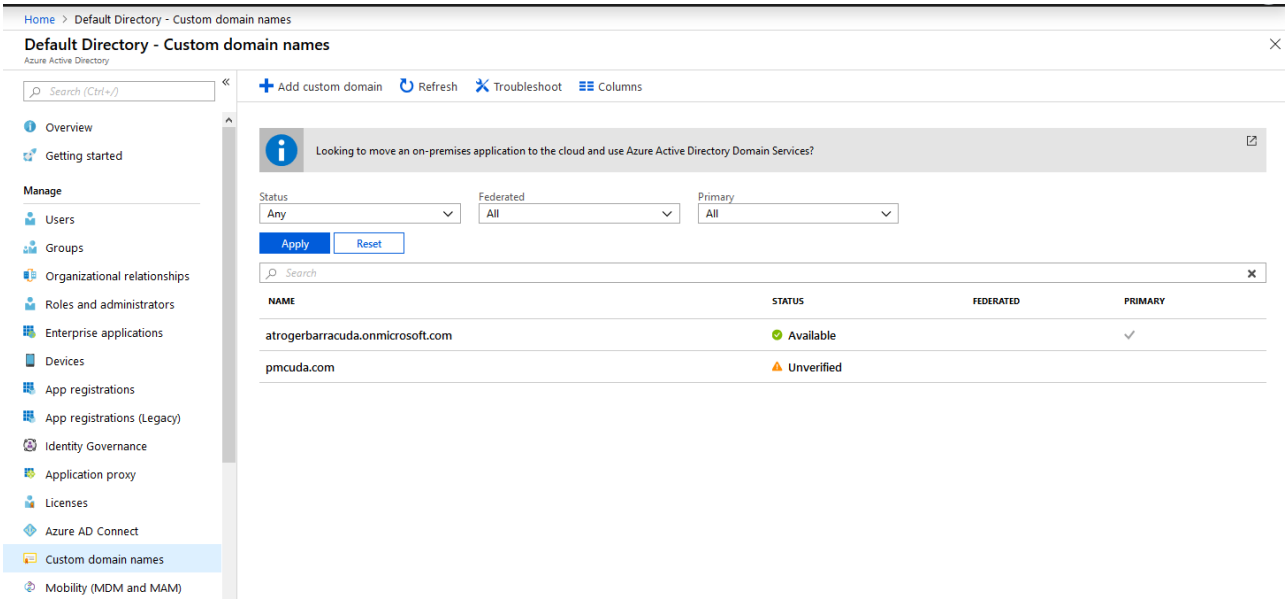
13. Double-check your settings and click **OK** to finish the configuration. The Azure AD Domain Services will now be deployed.

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

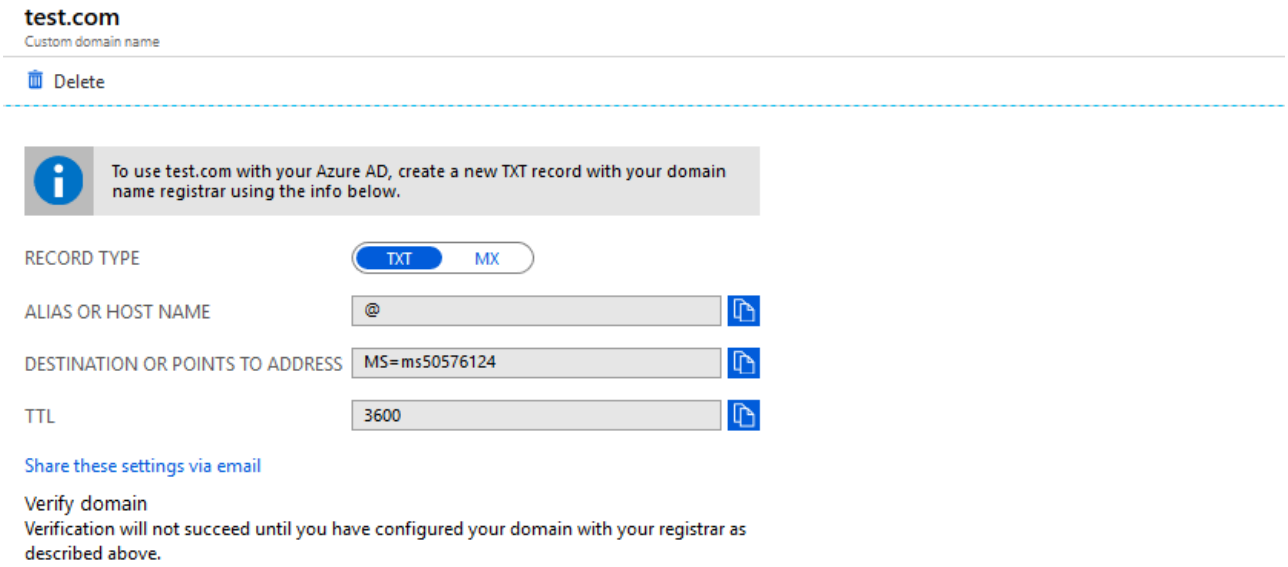
Step 2. Verify the Domain and Configure a Service User

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

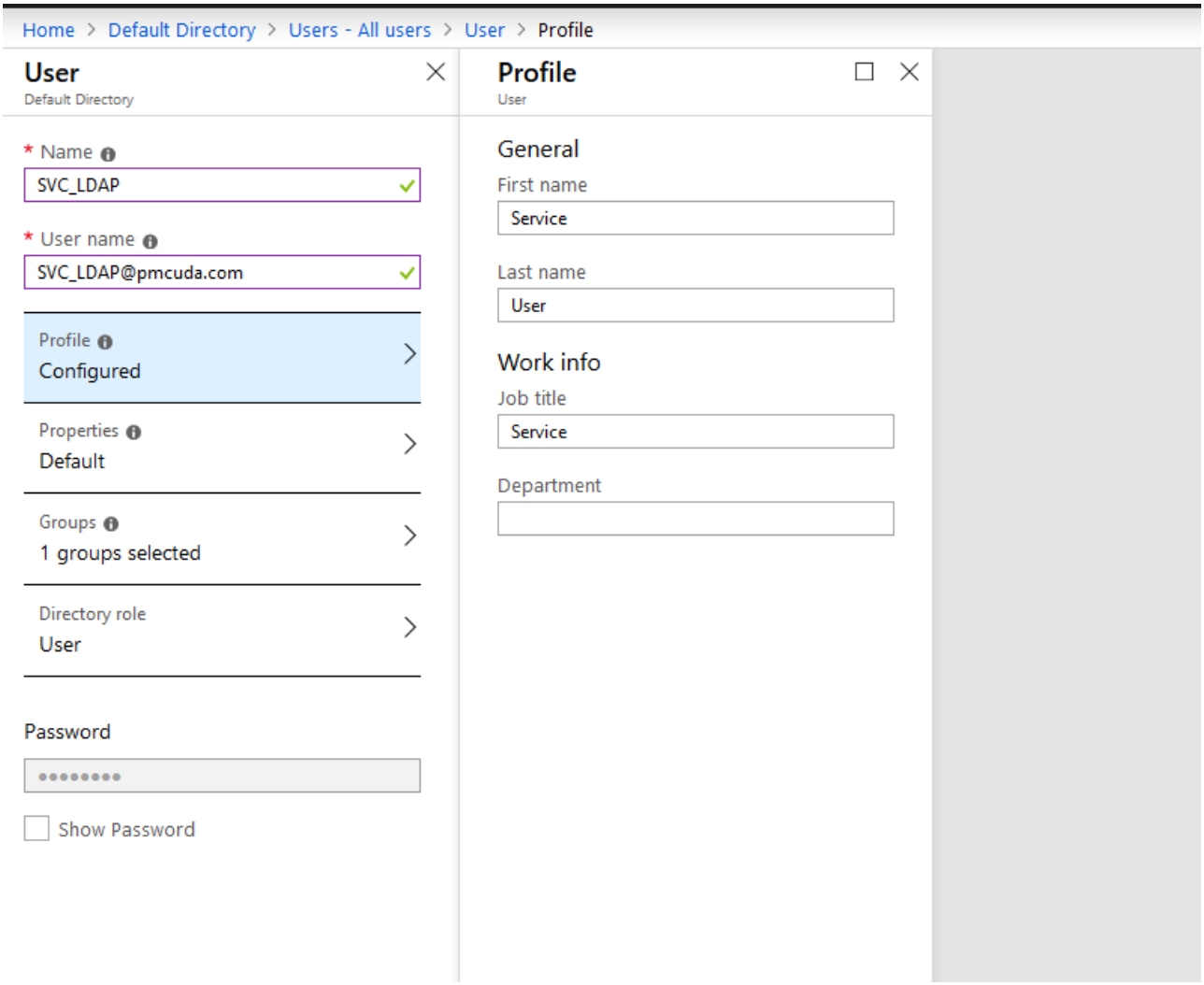
1. Go to your domain.



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



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

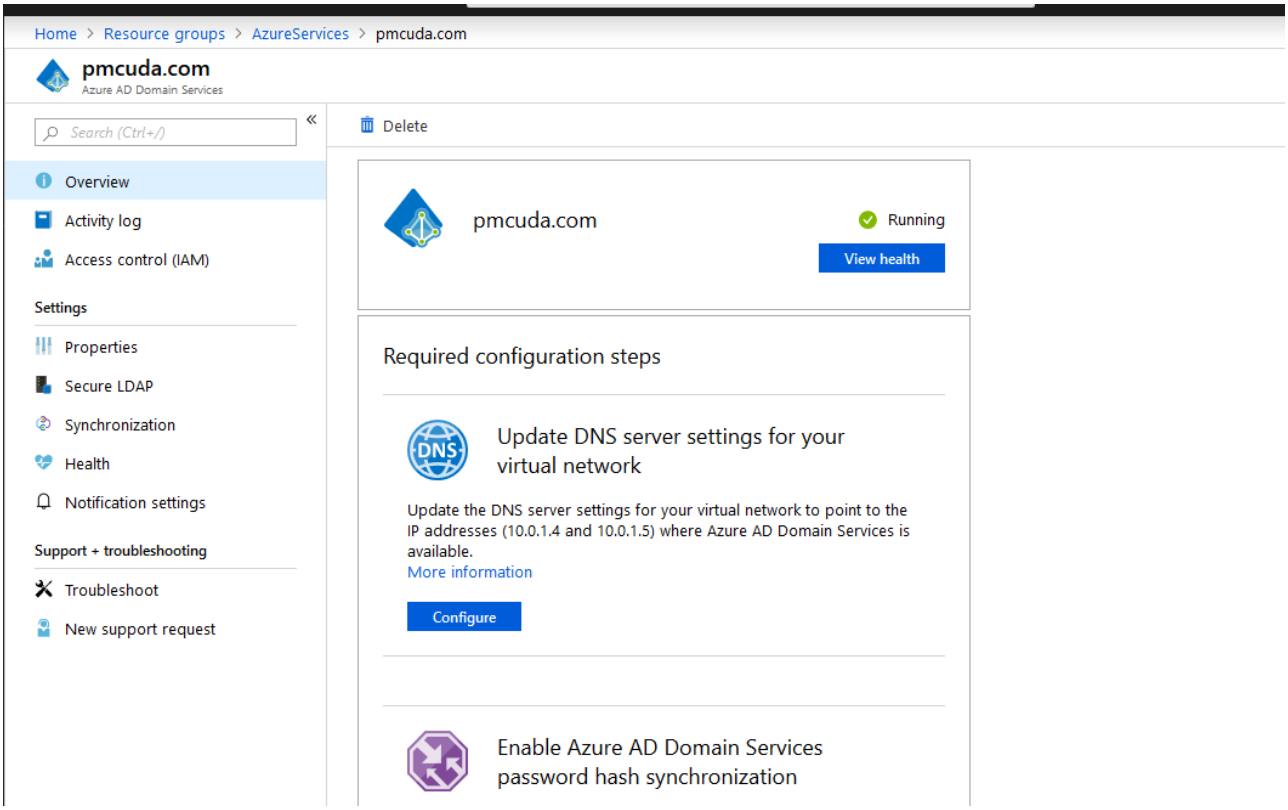


4. Add the user to the Azure Admins Group.
5. After adding user login with this user, change the **Password**.

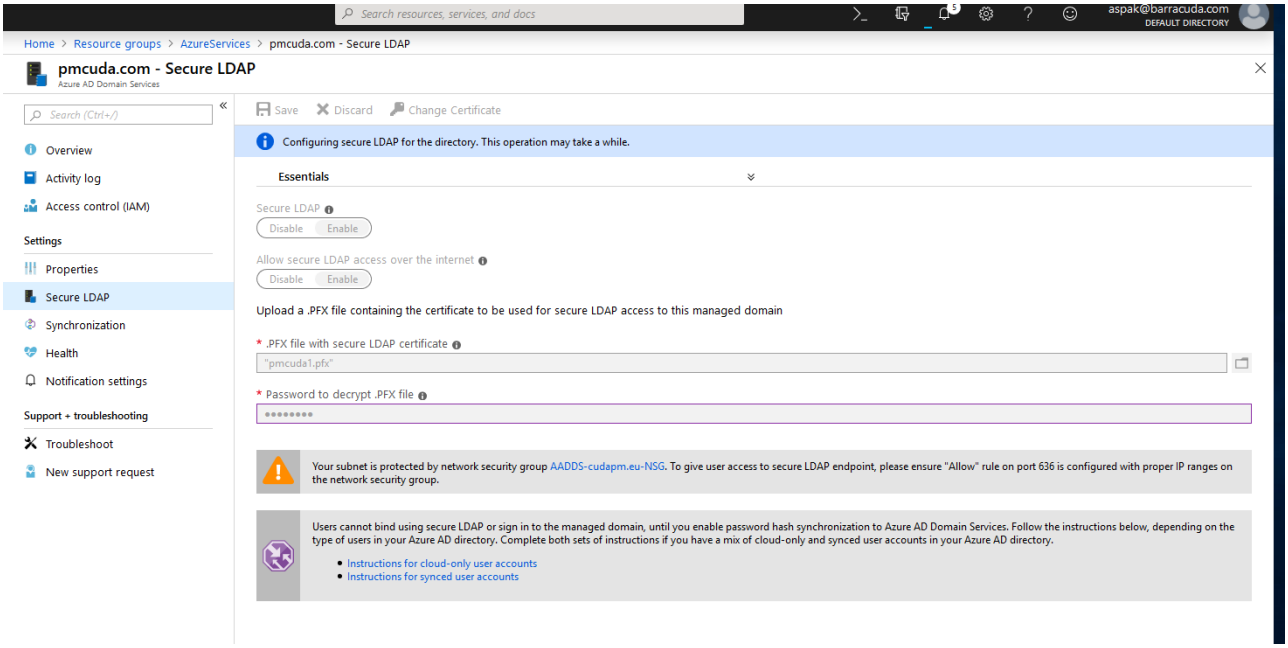
It is recommended to set the service user password not to expire.

Step 3. Activate LDAPs

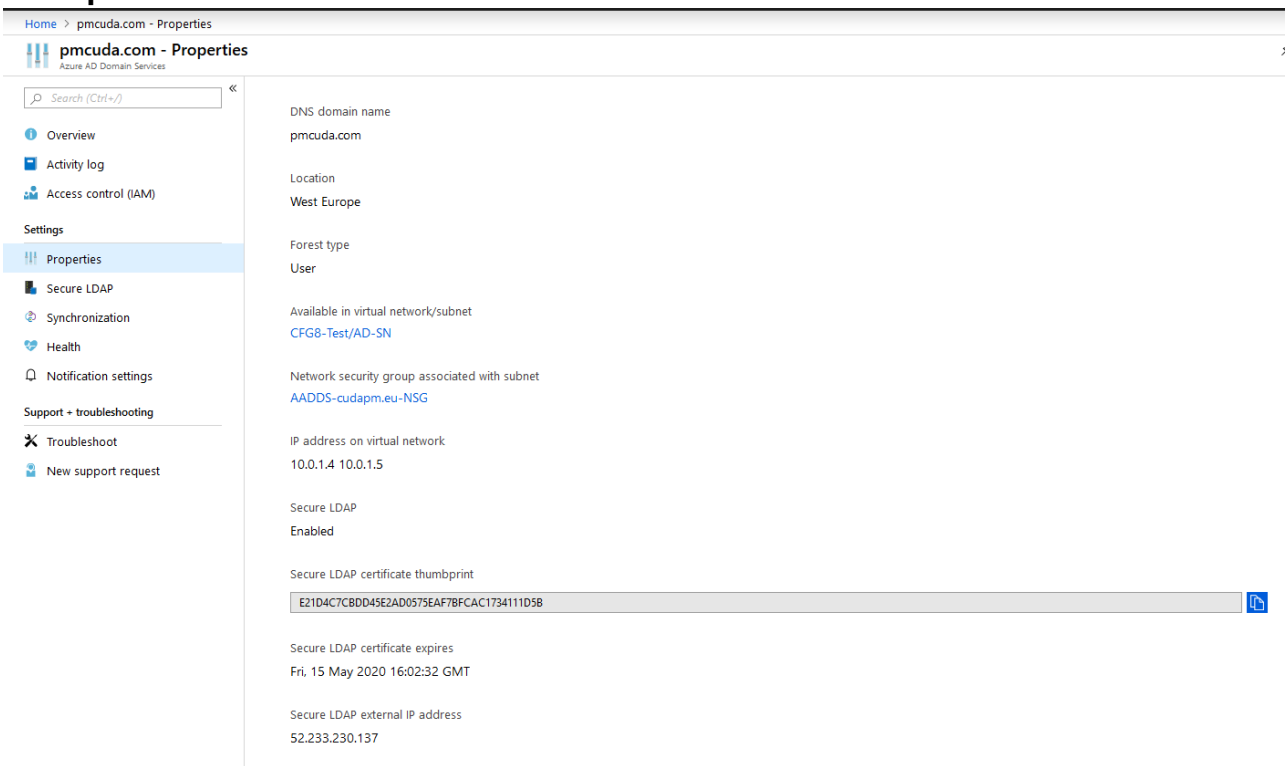
1. Go to **Azure AD Domain Services > *your managed domain***.
2. Update / configure the DNS settings.



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.



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



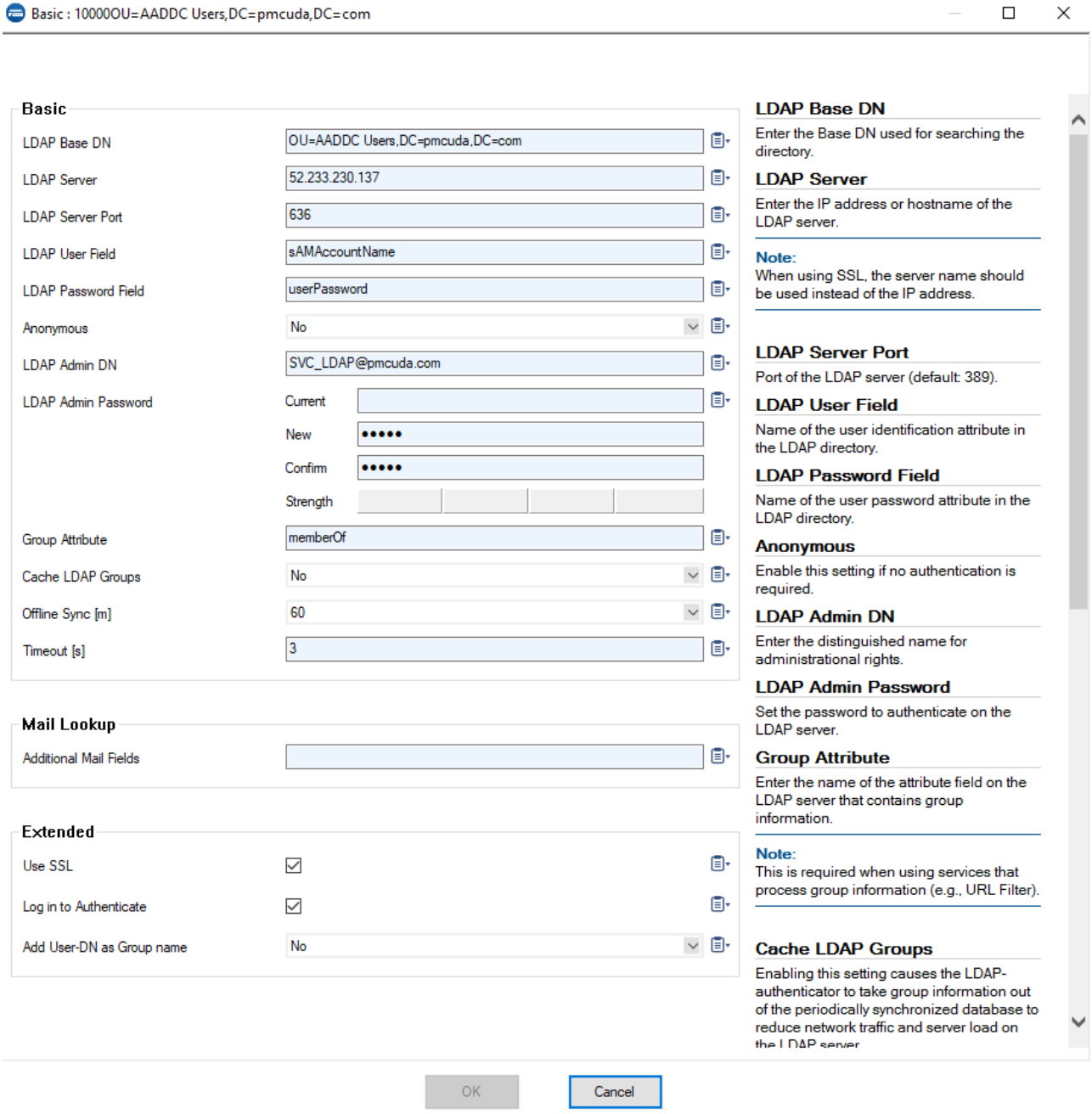
8. Set up the Network Security Group (NSG) according to your needs. Add at least port 636 to allow access via LDAPs for the on-premises CloudGen Firewall.

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:



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