How to Setup Azure AD Domain Services for MXvirtual

Administrator Guide

Version 1.0

August 2018

How to setup Azure AD Domain Services for MXvirtual
Version 1.0
August 2018

1 Setup Azure AD Domain Services

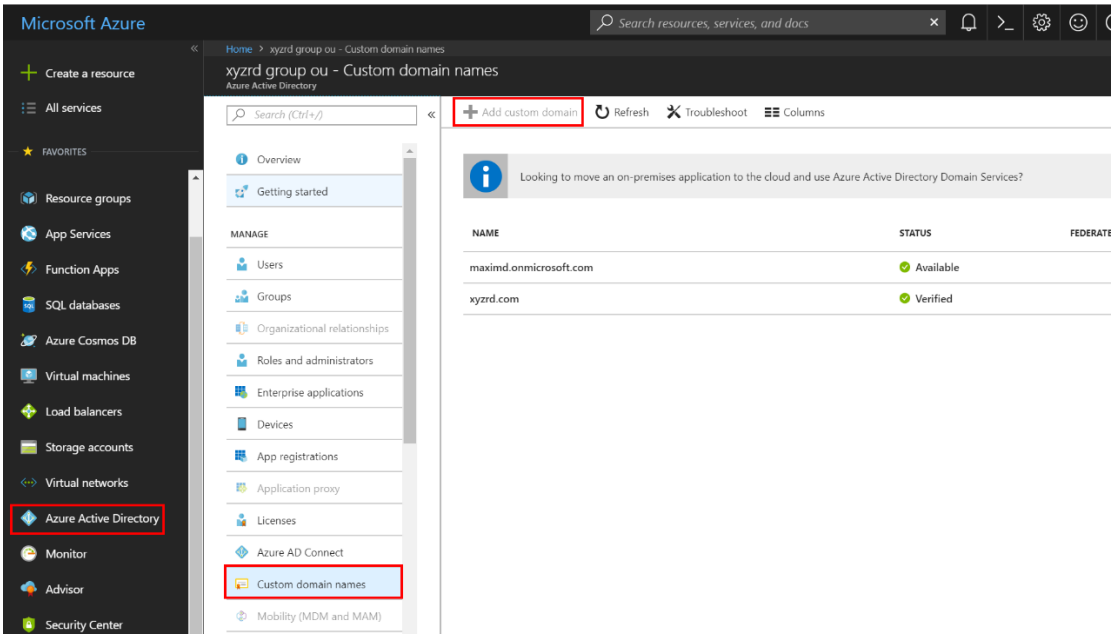
Azure Active Directory (Azure AD) is Microsoft's multi-tenant, cloud-based directory, and identity management service that combines core directory services, application access management, and identity protection into a single solution. To set up MXvirtual work with Azure AD services please follow the steps below. Before you begin, you need:

- A valid **Azure subscription**.
- An **Azure AD directory** - either synchronized with an on-premises directory or a cloud-only directory.
- The **Azure subscription** must be associated with **the Azure AD directory**.
- You **need global administrator** privileges in your Azure AD directory to enable Azure AD Domain Services.
- A **certificate** to be used to enable secure LDAP.

1.1 Add a custom domain name to your directory

This step is not required for "Azure AD Domain Service" to work. But domain name must be the same for registered users and "Azure AD Domain Service".

1. Sign in to the **Azure portal** with an account that's a global admin for the directory.
2. On the left, select **Custom domain names**.
3. Select **Add custom domain**.
4. Get domain name **verified**.

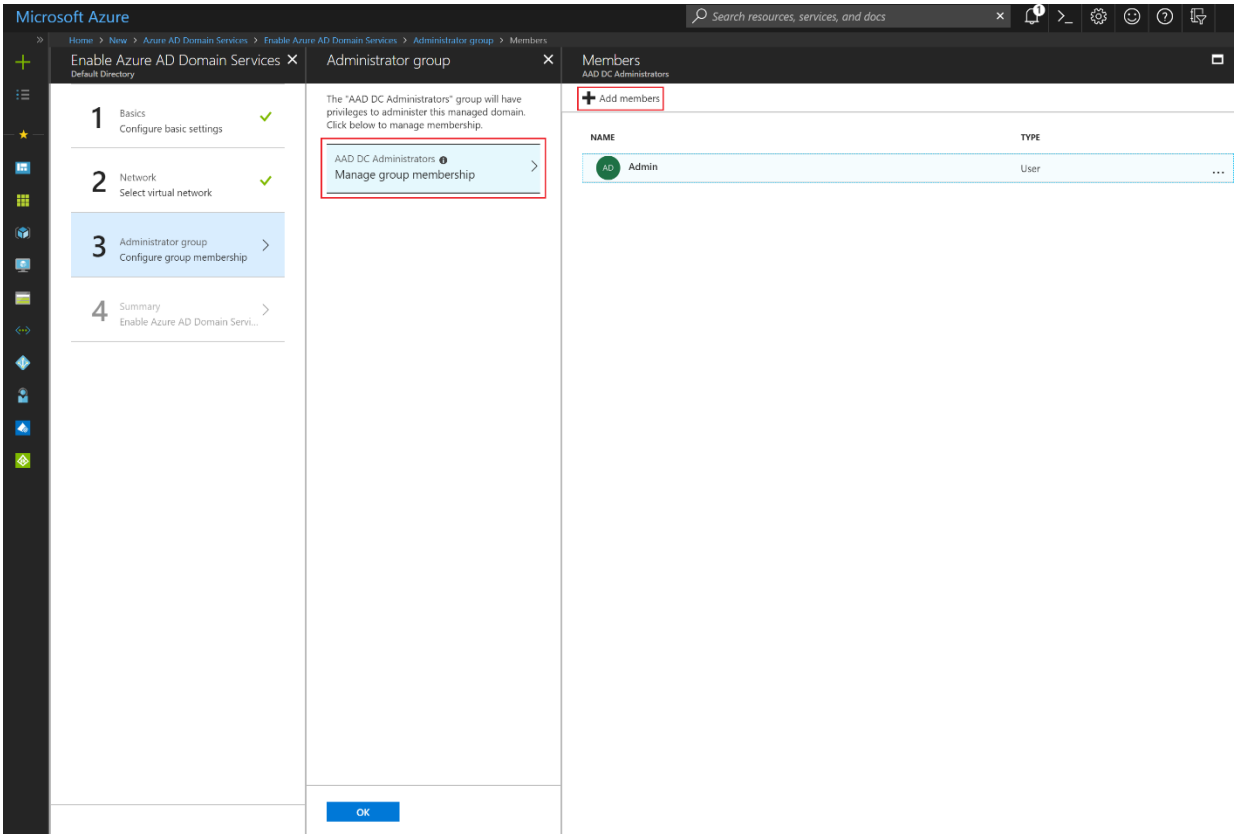


➲ **Whole process documentation here.**

1.2 Deploy Azure AD Domain Services

To launch the **Enable Azure AD Domain Services** wizard, complete the following steps:

5. In the left pane of Azure portal, click **Create a resource**.
6. In the **New** page, type **Domain Services** into the search bar.
7. Click to select **Azure AD Domain Services** from the list of search suggestions. On the **Azure AD Domain Services** page, click the **Create** button.
8. The **Enable Azure AD Domain Services** wizard is launched.
9. Configure **Basic**, **Network** and **Administrative Group** settings.
10. Deployment takes around 30 min.



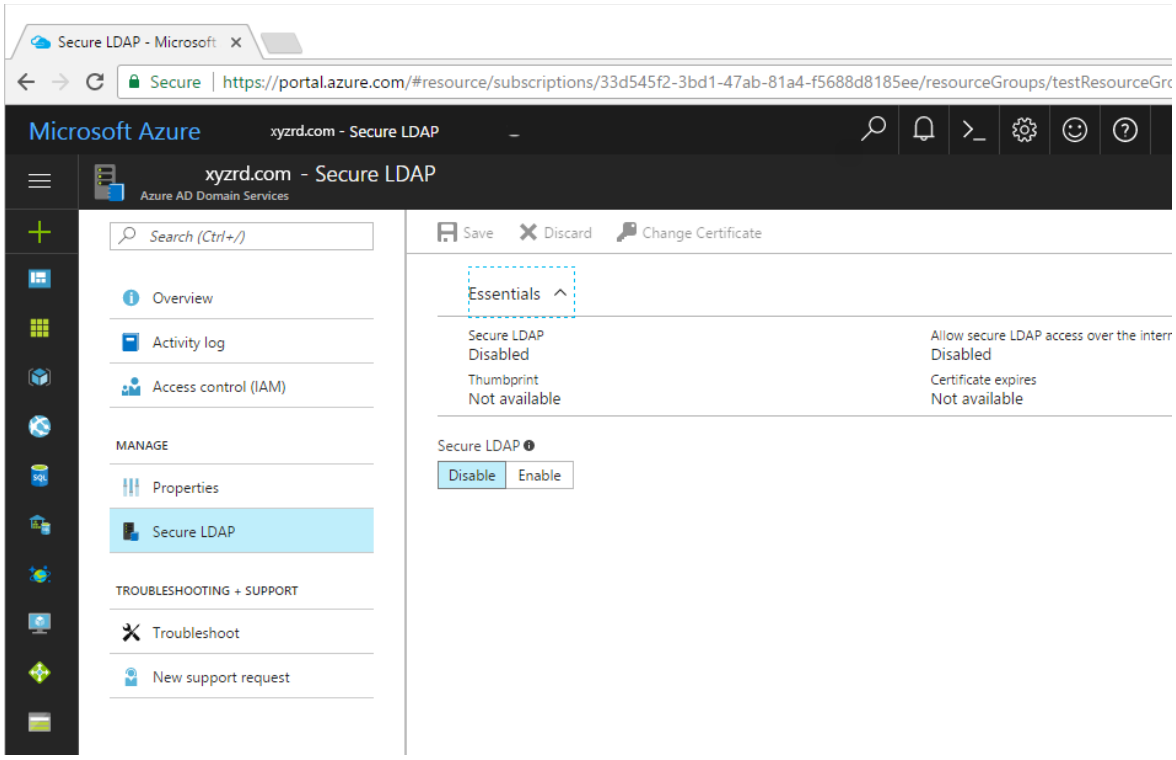
➲ **Whole process documentation here.**

Note:

** Domain name should be the same as custom domain name in "Azure AD". For example: Custom domain name in Azure AD is "xyzrd.com". Azure AD Domain Services should be deployed for "xyzrd.com". ** It is advised to put the domain services in different subnet than **Other Resources** *** To configure group membership, click **AAD DC Administrators**. Members of this group are granted administrative permissions on machines that are domain-joined to the managed domain.*

1.3 Enable LDAPS

11. Navigate to the **Azure portal**.
12. Search for **'domain services'** in the Search resources search box. Select Azure AD Domain Services from the search result. The Azure AD Domain Services page lists your managed domain.
13. Click the name of the **managed domain** (for *example*, 'xyzrd.com') to see more details about the domain.
14. Click **Secure LDAP** on the navigation pane.
15. **Enable** secure LDAP for the managed domain.
16. **Enable** secure LDAP access over the internet**.**
17. Click the folder icon following **.PFX file with secure LDAP certificate**. Specify the path to the PFX file with the certificate for secure LDAP access to the managed domain.
18. Create a network security group (NSG) and **add inbound rules for ports 389 and 636.**



➲ **Whole process documentation here.**

Note:
When you enable LDAPS access over the internet to your managed domain, it creates a security threat. The managed domain is reachable from the internet at the port used for secure LDAP (that is, port 636). You can choose to restrict access to the managed domain to specific known IP addresses that MXvirtual resides on. **Get an **SSL certificate that is used for secure LDAP access to the managed domain. **SSL Certificate** has to be for *. <domain>.<name>(i.e., **Domain** is xyzrd.com, then **Certificate** is *.xyzrd.com).*

2 Configure MXV LDAP

Zultys MXvirtual adds the ability to include authentication through integration with an LDAP (Lightweight Directory Access Protocol) server. With LDAP authentication, users can login using the same password whether by local area network, intranet, e-mail, etc. To use LDAP authentication, LDAP service first must be enabled on each MX phone system. To configure follow the steps below:

2.1 LDAP Configuration

1. Go to: **System Settings** -> LDAP configuration.
2. Tick **Enable** Authentication.
3. **Search Base** i.e., OU=AADDC Users,DC=xyzrd,DC=com
4. **Domain** i.e., xyzrd.com
5. Credentials to access LDAP server: User that is in "**AAD DC Administrators**" group, i.e., ldap@xyzrd.com
6. LDAP Servers. **Add Public IP or DNS name** of "Azure AD Domain Service". IP can be found in Properties of "Azure AD Domain Service" under "Secure LDAP external IP address".
7. Switch security to **"SSL/TLS"**.
8. Be sure that **SSL certificate** is **trusted** in MXV. SSL Certificate CN name and DNS name have to be correct. For above example: certificate for *.xyzrd.com. DNS name should be ldap.xyzrd.com or similar. In case of CN name and DNS are incorrect, MXV won't connect to LDAP server.
9. To add certificate as trusted, **upload certificate** file to Maintenance -> Security Certificate Management -> Trusted Certificates

2.2 Configure Users

10. Go to: Configure -> **Users**.
11. **Edit users** that will have LDAP authentication. User's "username" has to be the same as registered in Azure AD.
    Example:
12. User in Azure AD = user1@xyzrd.com
13. Username in MXV = user1
14. Users with **LDAP authentication** can use their Azure AD username and password for **MXV, MXIE, ZAC, ZMC** authentication.

➲ **Whole process documentation here.**