

Integrate azure AD with LDAP

627 Manu Chacko April 10, 2025 [Getting Started](#) 2274

Configure secure LDAP for Azure Active Directory Domain Services and integrate it into your application.

Overview: This article helps to enable LDAPS (Secure LDAP) on Azure Active Directory and integrate it into your application. It guides you through configuring secure LDAP for Azure Active Directory Domain Services to ensure secure, encrypted communication between your application and the directory service.

Refer to this article to [Integrate Azure AD](#) in Ezeelogin jump server

Make your Azure Active Directory Domain Service more secure and connect external systems easily with LDAPS. Follow the steps to enable LDAPS and test LDAP queries from an external system.

Step 1: Log into the Azure portal, Search, and Select Azure AD Domain Services

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar with the text "Search resources, services, and docs (G+/I)". Below the search bar, the results are displayed under the heading "All services". On the left, there's a sidebar with "Categories" including AI + machine learning, Analytics, Compute, Containers, Databases, DevOps, General, Hybrid + multcloud, Identity, Integration, Internet of Things, Management and governance, Migration, Mixed reality, Monitor, and Networking. The search results are filtered by "Active Directory DomaX". The results list includes:

- Azure Active Directory
- App Services (Keywords: app service, mobile services, mobileservices)
- Azure Database for MySQL servers (Keywords: flexible server)
- FHIR service (Keywords: Health Data Services, MedTech service)
- Azure AD Domain Services (Resource type: Microsoft.AAD/domainServices) - This item is highlighted with a red bar.
- Bot Services (Resource type: Microsoft.BotService/botServices)
- Free services (Keywords: free services, services)
- Media Services (Resource type: microsoft.media/mediaservices)
- Speech services (Resource type: Microsoft.CognitiveServices/BrowseSpeechServices)
- Azure AI services multi-service account (Resource type: Microsoft.CognitiveServices/BrowseAllInOne)
- SQL servers
- App Service Environments (Keywords: app service environment, app service)
- Integration Service Environments (Resource type: Microsoft.Logic/IntegrationServiceEnvironments)
- Web PubSub Service (Resource type: Microsoft.SignalRService/WebPubSub)
- Applied AI services (Resource type: Microsoft.CognitiveServices/BrowseAppliedAIHub)
- Azure Lab Services
- Service Health
- Activity log
- App Service Domains (Keywords: app service domain, vanity domain, custom domain, domain na...)
- Service Bus (Keywords: Java Message Service, Resource type: Microsoft.ServiceBus/nam...)
- Analysis Services (Resource type: Microsoft.AnalysisServices/servers)
- Communication Services (Keywords: azure communication services)
- Kubernetes services (Keywords: serverless, Resource type: Microsoft.ContainerService/managed...)
- Peering Services (Resource type: Microsoft.Peering/peeringServices)
- Azure Native Dynatrace Service
- Azure Native New Relic Service
- App Service Certificates (Keywords: app service)
- App Service plans (Keywords: app service)
- Service Fabric clusters (Resource type: Microsoft.ServiceFabric/clusters)
- API Management services (Resource type: Microsoft.ApiManagement/service)
- Azure AI services (Keywords: Azure AI services, Resource type: Microsoft.CognitiveServices/ac...)
- Email Communication Services (Resource type: Microsoft.Communication/EmailServices)

The URL at the bottom of the page is <https://portal.azure.com/#>.

Step 2: Select your Managed Domain service

Microsoft Azure

Search resources, services, and docs (G+/I)

All services >

Azure AD Domain Services

Default Directory (oktaezezeelogin.onmicrosoft.com)

+ Create

⚙️ Manage view

🔄 Refresh

⬇️ Export to CSV

🔗 Open query

🏷️ Assign tags

Filter for any field...

Subscription equals all


Resource group equals all

Location equals all

+ Add filter

Showing 1 to 1 of 1 records.

No grouping

<input type="checkbox"/> Name ↑↓	Type ↑↓	Resource group ↑↓	Location ↑↓
<input type="checkbox"/>  mydomain.com	Azure AD Domain Services	cloudweg.com	East US

Step 3: Select Secure LDAP

Microsoft Azure Search resources, services, and docs (G+/I)

All services > Azure AD Domain Services >

Azure AD Domain ...

Default Directory (oktaezezeelogin.onmicrosoft.co...

+ Create Manage view ...

Filter for any field...

Name ↑

mydomain.com

mydomain.com Azure AD Domain Services

Search Refresh Delete

Overview

- Activity log
- Access control (IAM)
- Tags

Settings

- Properties
- Secure LDAP**
- Synchronization
- Custom Attributes (Preview)
- Replica sets
- Trusts
- Health
- Notification settings
- SKU
- Security settings
- Locks

Monitoring

- Metrics
- D diagnostic settings

Configuration issues for your managed domain were detected. Run configuration diagnostics to see a de

mydomain.com

Running

View health

Azure AD Domain Services SKUs

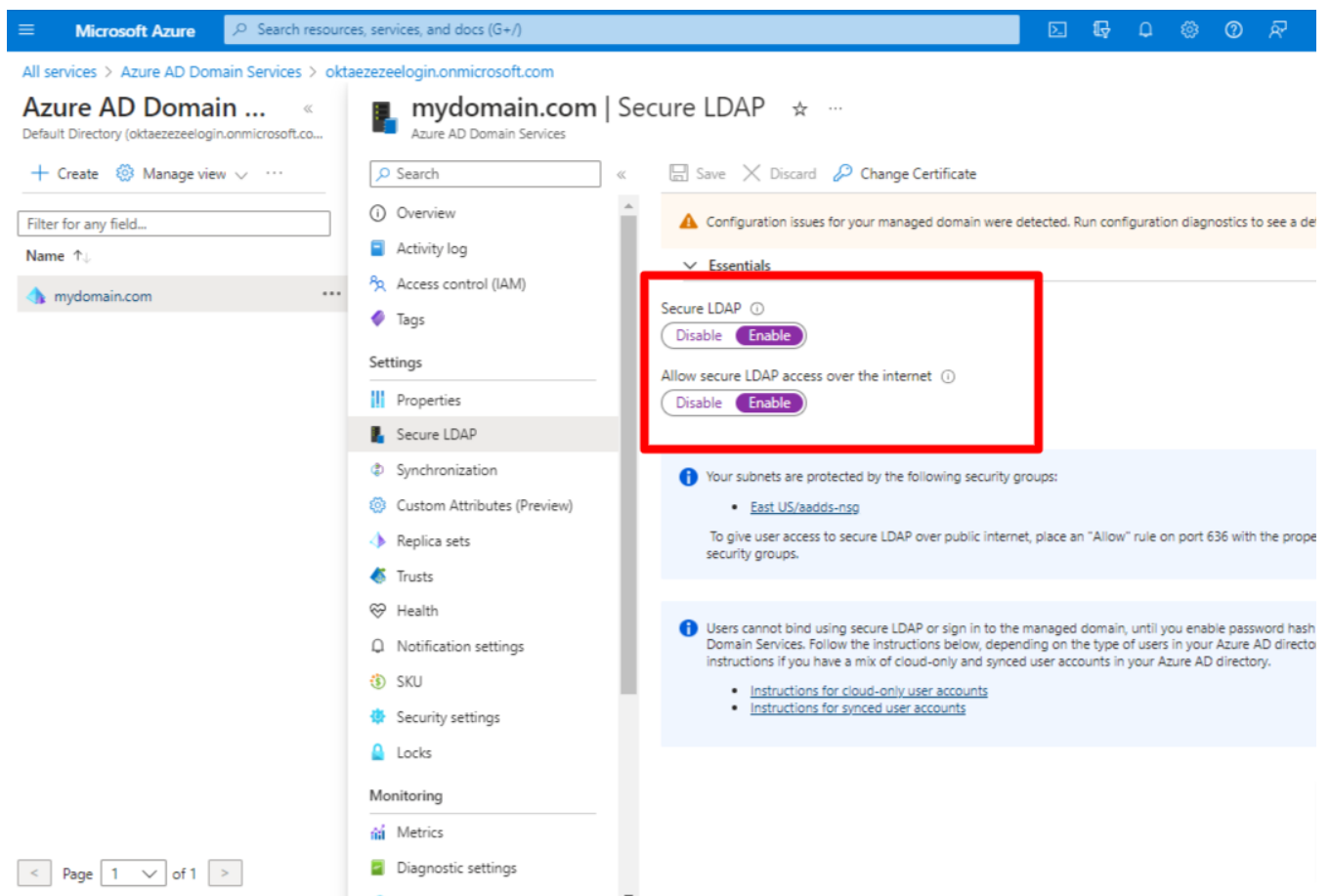
Choose Azure AD Domain Services SKU for your organization

Azure AD Domain Services is available in multiple service tiers, known as SKUs. These SKUs provide predictable pricing, varying performance levels, and selectable enterprise and premium features.

More information

Choose SKU

Step 4: Enable secure LDAP and Allow secure access over the Internet



A digital certificate is required to encrypt the communication to use secure LDAP. The certificate can be obtained from a public certificate authority (CA) or an enterprise CA or a self-signed certificate

Step 5: Follow the instruction to create and export a self-signed certificate

Step 5(A): Open a PowerShell window as Administrator and run the following commands. Replace the **\$dnsName** variable with your managed domain, For example mydomain.com

```
#Define your own DNS name used by your managed domain
$dnsName="mydomain.com"
#Get the current date to set a one-year expiration
$lifetime=Get-Date
#Run the command to generate the certificate

New-SelfSignedCertificate -Subject *.$dnsName `
-NotAfter $lifetime.AddDays(365) -KeyUsage DigitalSignature,
KeyEncipherment `
-Type SSLServerAuthentication -DnsName *.$dnsName, $dnsName
```

You can view the following output if the certificate was successfully created

```

PS C:\WINDOWS\system32> New-SelfSignedCertificate -Subject *.$dnsName `
>> -NotAfter $lifetime.AddDays(365) -KeyUsage DigitalSignature, KeyEncipherment `
>> -Type SSLServerAuthentication -DnsName *.$dnsName, $dnsName.com

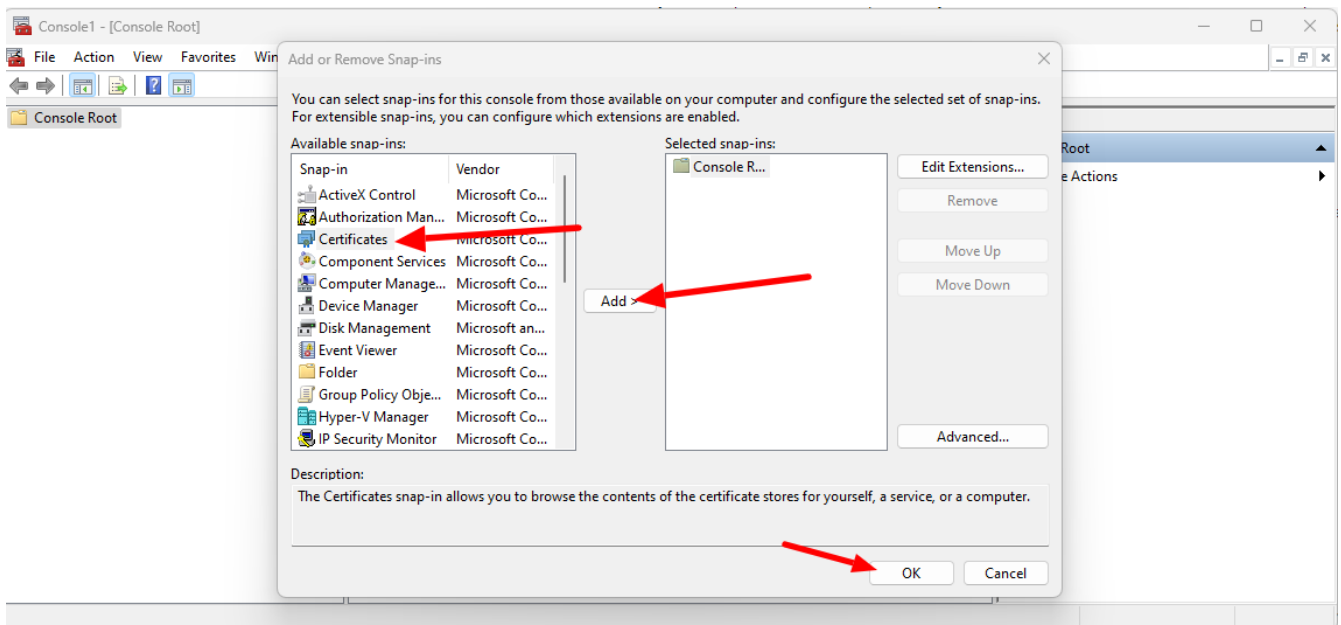
PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\MY

Thumbprint                                     Subject
-----
959BD1531A1E674EB09E13BD8534B2C76A45B3E6    CN=mydomain.com

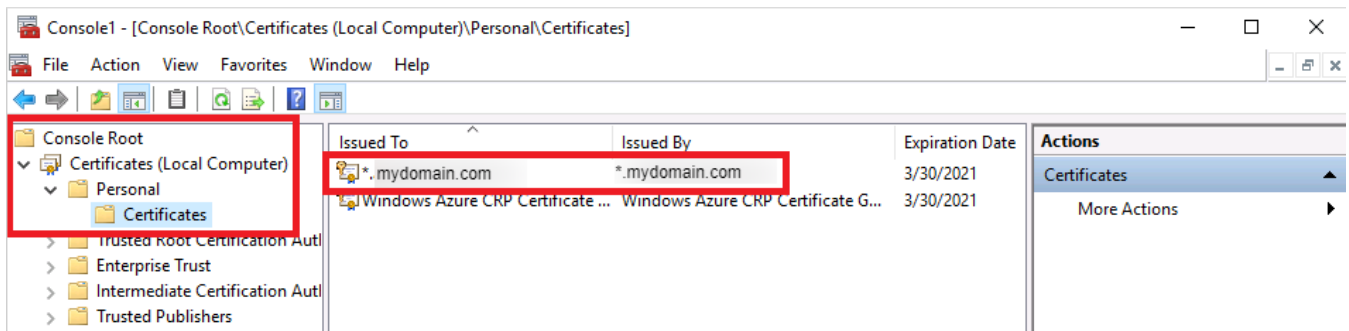
```

Step 5(B): Export a certificate for Azure AD DS

- Open run on windows machine and enter **mmc** , press ok
- Click on the **File** and select **Add/Remove Snap-in**
- Select certificates and click on Add , click ok



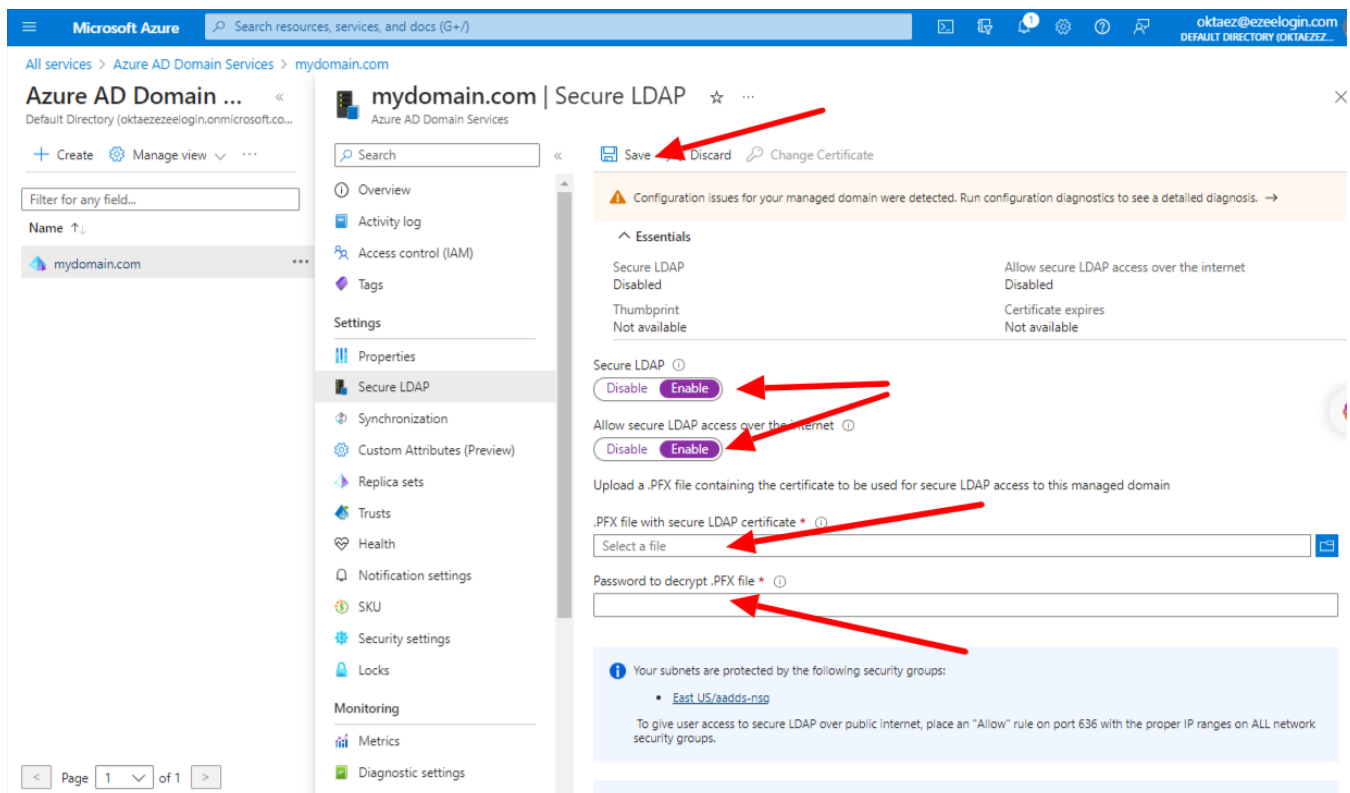
- Then select Local computer: (the computer this console is running on) , then click Finish .
- In the MMC window, expand Console Root. Select Certificates (Local Computer), then expand the Personal node , followed by the Certificates node.



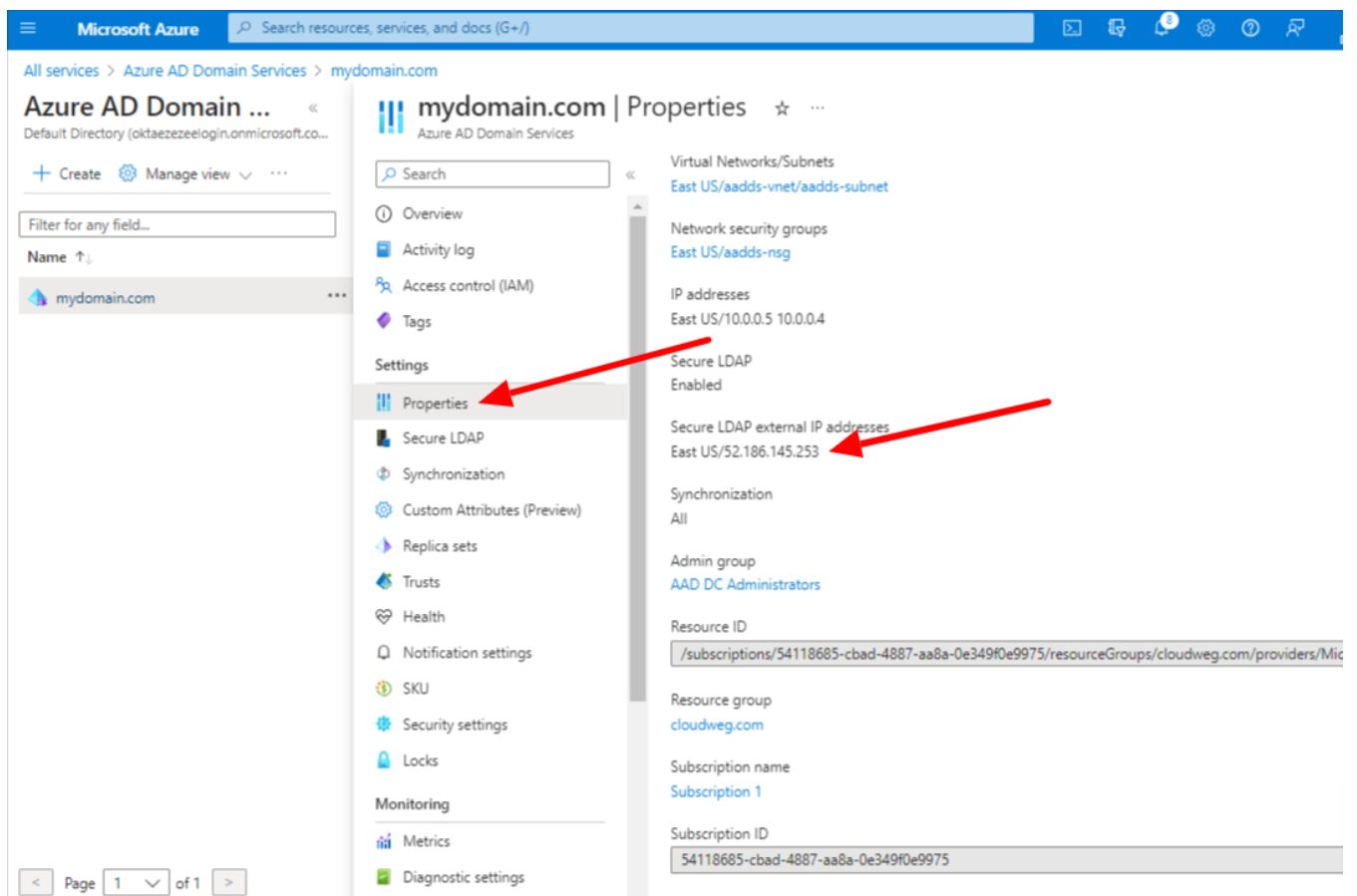
- Right-click on this certificate, then choose All Tasks > Export
- Export Private Key page, choose Yes, export the private key, then select Next .
- Select Personal Information Exchange - PKCS #12 (.PFX) as the file format for the certificate. Check the box for Include all certificates in the certification path if possible
- Click Next and type a password and follow the prompts

You will get the certificate exported in pfx format. Now you can continue on Azure portal

Step 6: Select the folder icon next to .PFX file with secure LDAP certificate. Browse to the path of the .PFX file you exported in the previous step and enter the password to decrypt which you have used while exporting and save.



Step 7: Click on **Properties** and configure your DNS provider to create a host record to resolve to this **Secure LDAP external IP address**. You can configure this to your Local DNS forwarder or to your system host to resolve locally for testing.

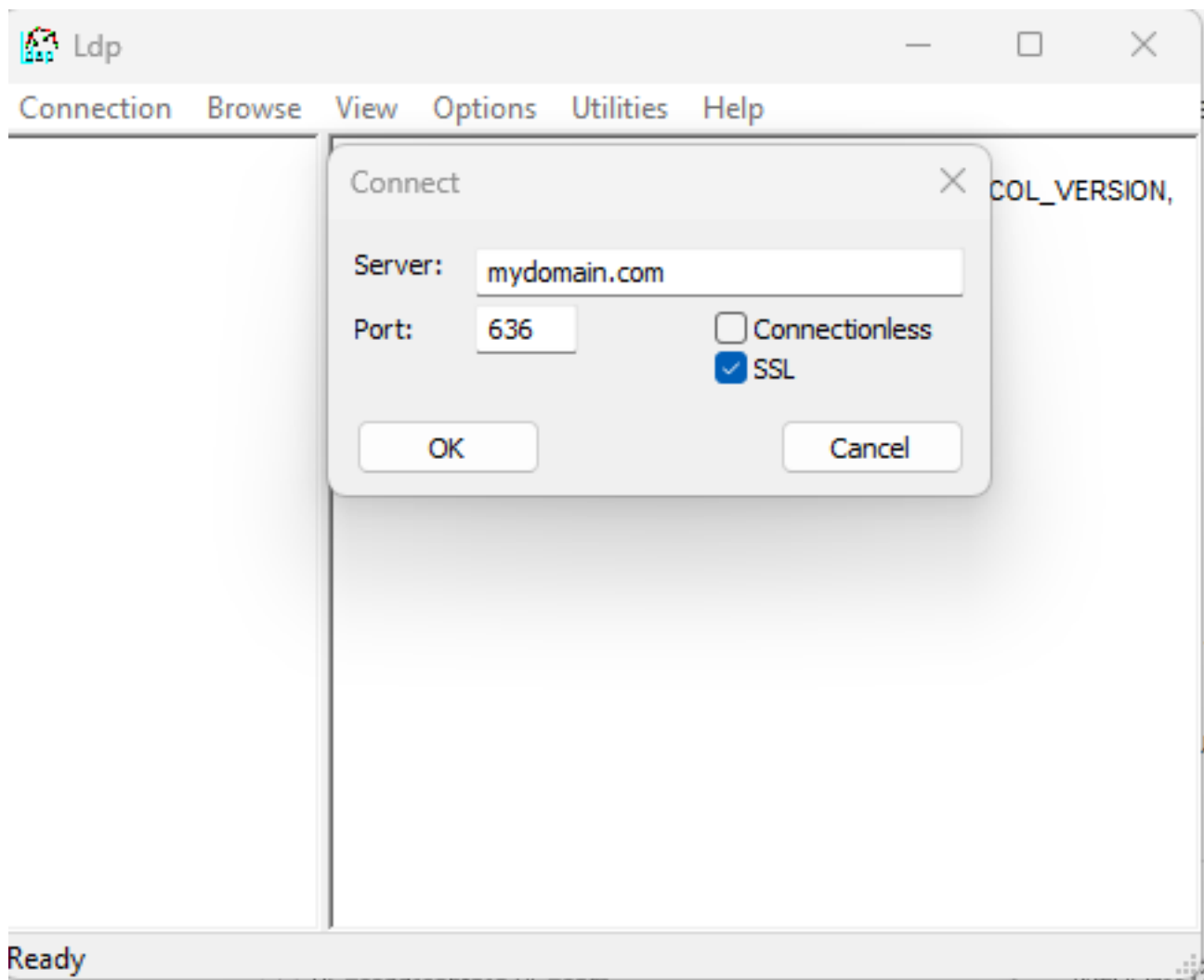


Test the LDAPS queries from an external system

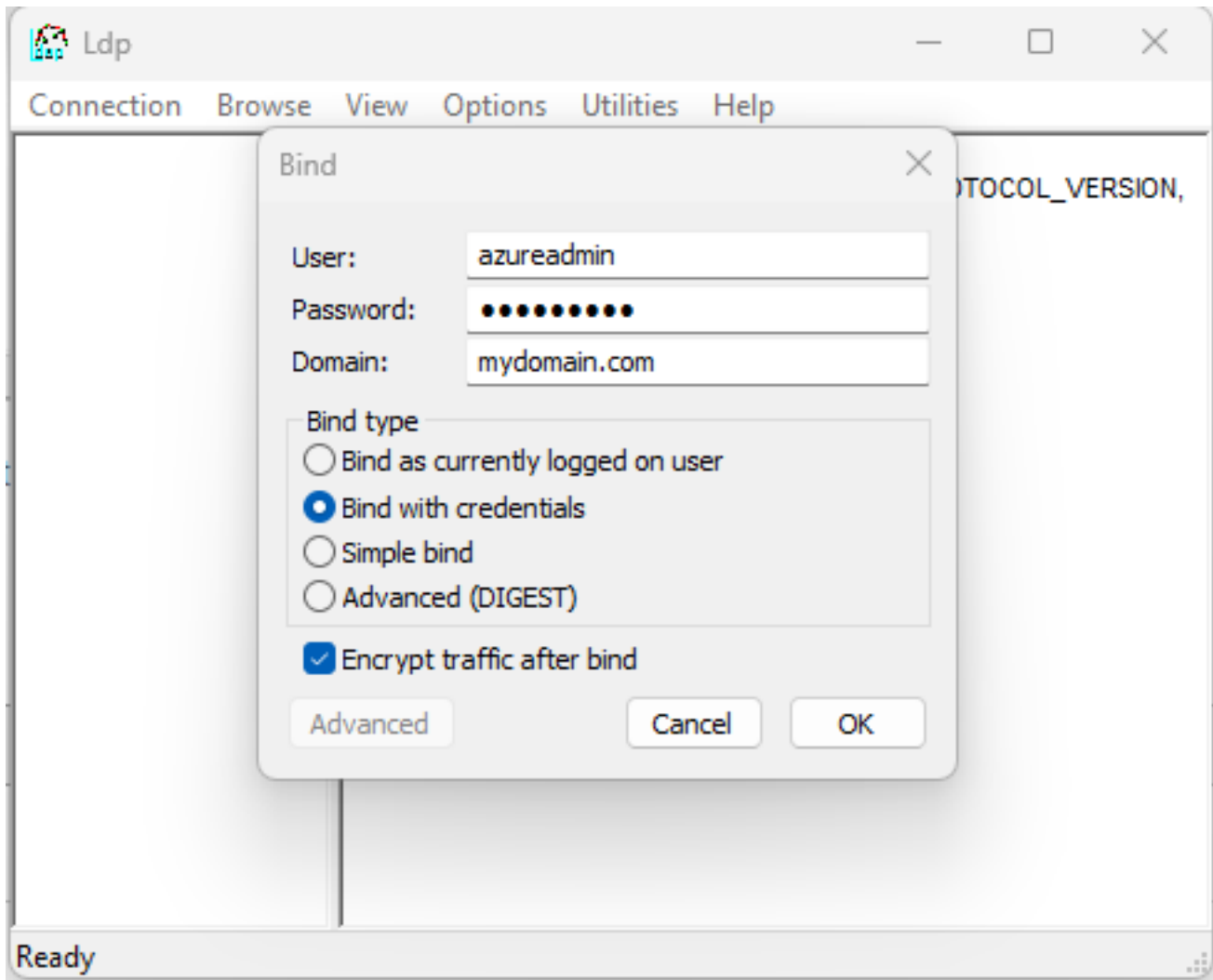
Step 1: Add the following **Secure LDAP external IP address** to your host file on the system

```
52.186.145.253 mydomain.com
```

Step 2: Open LDP.exe tools and enter the domain name, Port 636, select **SSL** and click **ok**



Step 3: Open **Connection > Bind**, Select **Bind with credentials** and input your **Username**, **Password**, and **Domain** of the **Azure Bind User**



Step 4: Open **View** -> **Tree** will list the entire Active Directory Tree.

Step 5: You can also run LDAPSEARCH from your terminal as follows. Use "LDAPTLS_REQCERT=never" if you are using a self-signed certificate.

```
john@dellpc:~# LDAPTLS_REQCERT=never ldapsearch -H  
ldaps://mydomain.com:636 -D "john@mydomain.com" -W -b  
"DC=mydomain,DC=com"
```

Related Articles:

[Can we map existing user group in ldap to ezeelogin as ezeelogin user group ?](#)

[Assigning user group for LDAP users?](#)

[Integrate Azure AD in Ezeelogin jump server](#)

Online URL: <https://www.ezeelogin.com/kb/article/integrate-azure-ad-with-ldap-627.html>