Integrate azure AD with LDAP

627 Manu Chacko April 10, 2025 Getting Started 2998

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 <u>Integrate Azure AD</u> 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

E Microsoft Azure	 Search resources, services, and docs (G+/) 	≥_	Ŗ	Q	٢	?	ନ୍ଧ
All services							
All	Active Directory DomaX						
Favorites	▲ Azure Active Directory.						
Recents							
Recommended	Keywords: app service, mobile services, mobileservices						
Categories	Azure Database for MySQL servers App Service Domains Keywords: flexible server	ain,custor	n domain	domain	na		
AI + machine learning	FHIR service Service Bus Keywords: Health Data Services. MedTech service Keywords: Java Message Service; Resource	type: Mici	rosoft.Ser	viceBus/r	nam		
Analytics	Azure AD Domain Services Resource type: Microsoft AAD/domainServices Analysis Services/Resource type: Microsoft AnalysisServices/	servers					
Compute	Bot Services Communication Services						
Containers	Free services						
Databases	Keywords: free services, services Keywords: serverless; Resource type: Micros	soft.Conta	ainerServi	ice/mana	iged		
DevOps	Media Services Resource type: microsoft.media/mediaservices Resource type: microsoft.media/mediaservices	ervices					
General	Speech services Resource type: Microsoft.CognitiveServices/BrowseSpeechServices						
Hybrid + multicloud	Azure Al services multi-service account Resource type: Microsoft.CognitiveServices/BrowseAllnOne Azure Native New Relic Service						
Identity	SQL servers App Service Certificates Keywords: app service						
Internet of Things	App Service Environments Keywords: app service environment app service						
Management and governance	Integration Service Environments Resource type: MicrosoftLogic/integrationServiceEnvironments	sters					
Migration	Web PubSub Service API Management services Resource type Microsoft Signal RService/WebPubSub Resource type Microsoft ApiManagement/	service					
Mixed reality	Applied Al services						
Monitor	Resource type: Microsoft.CognitiveServices/BrowseAppliedAlHub	Microsof	ft.Cognitiv	veService	es/ac		
Networking	Azure Lab Services Azure Lab Services Azure Lab Services	EmailServ	ices				
https://portal.azure.com/#							

Step 2: Select your Managed Domain service



Step 3: Select Secure LDAP



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



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.

🚟 Console1 - [Console Root\Certificate	es (Local Computer)\Personal\Certificate	s]		_	
🚟 File Action View Favorites W	Vindow Help				- 8 ×
🗢 🔿 🗖 🗊 🗎 🗟 🔂					
Console Root	Issued To	Issued By	Expiration Date	Actions	
 Gertificates (Local Computer) Personal 	🔄 *. mydomain.com	*.mydomain.com	3/30/2021	Certificates	•
Certificates	Windows Azure CRP Certificate	Windows Azure CRP Certificate G	3/30/2021	More Actions	•
Irusted Koot Certification Autl					
> 🚞 Enterprise Trust					
> intermediate Certification Autl	1				
> Trusted Publishers					

- 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





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

🚮 Ldp			—		\times
Connection Bro	owse View	Options Utilities Help			
	Bind		×	OCOL_VE	RSION,
	User:	azureadmin			
	Password:	•••••			
	Domain:	mydomain.com			
	Bind type Bind as currently logged on user Bind with credentials Simple bind Advanced (DIGEST)				
	Encrypt	traffic after bind			
	Advanced	Cancel	ок		

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 Idap 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