# Azure Active Directory SSO (More Common than ADFS)

|  |  |  |
| --- | --- | --- |
|  | **File** | **Modified** |

No files shared here yet.

 Drag and drop to upload or browse for files 

Top of Form

Upload file

File description

Bottom of Form

“ **Prepared by Mohamed Ghayaty - Incorta SysOps Team Email :** [**mohamed.ghayaty@incorta.com**](mailto:mohamed.ghayaty@incorta.com)”

This Document contains detailed steps of how to integrate Incorta with Azure Active Directory SSO online subscription and how to synchronize users between Incorta and Azure Active Directory SSO online subscription.

**Important Hints about Sync-users part:**

Azure Active Directory Enterprise applications Can't be treated as LDAP, While LDAP is the only way Incorta uses to Sync Users.

Instead, Azure Portal itself can be treated as LDAP via Azure AD domain services and that's what we use plus workarounds to perform sync users part.

**First Part : SSO Integration,**  
**Create Azure AD SSO application and Integrate Incorta with it**

Please refer to below URL  
Author : Ahmed Eissa - Dev Team Email : [ahmed.eissa@incorta.com](mailto:ahmed.eissa@incorta.com) Azure ADFS SSO Integration

**Second Part : Sync Users,**  
**Configure Azure Portal Account as LDAP Create LDAP Authentication user:**

1. From All Services, Go to "Users",
2. Then Click on " New User",
3. Fill in Fields, Make sure that new user has Email configured in its profile,
4. Azure will give Initial password for the new user, save this password, then navigate to below link:

<https://account.activedirectory.windowsazure.com/r/#/profile>

Sign in to the above link using newly created user/pass.  
It'll ask you to enter new credentials after first login.  
Change the password, and Wait for 20 Mins, Until Sync Happened in Azure.

**Enable Azure Active Directory Domain Services using the Azure portal:**

Follow Steps Mentioned in below Link : <https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-getting-started>

**Add User to Domain Service Admin Group:**

**Note:** User added to this group will has the authority to Authenticate LDAP.  
1.Open your "Azure AD Domain Services", and select domain name, in our example it's "[mohamedkhaledincorta.onmicrosoft.com](http://mohamedkhaledincorta.onmicrosoft.com)",

2.Then Select Properties,

3.From the opened page, Search for "Admin Group", its name is "AAD DC Administrators" and click on it,

1. Click on members and add your user that should authenticate LDAP and add it to owners too,

5.Still in Properties page, Take a note from following fields ( Location , IP Address on virtual network, Security LDAP external Address ),

**Add Azure AD Domain Service IPs to the Virtual network DNS servers :**

1. From Azure AD Domain Service, Click on the domain name and select "Properties", Then search for "Available Virtual Network /SUBNET" and click on it , in our example its "incorta-vnet/default",
2. Click on "DNS Servers" then in Custom, Add the 3 IPs of the newly created Domain service ( internal and external ):

**Note:** Those IPs will be used to discover the LDAP in the following steps.

**[ Validation ] – Connect to LDAP Via Windows LDP.exe:**

Now, Azure is LDAP, Below steps will help you to see the tree from windows VM Machine,

1. Using Azure Virtual Machines Service, Create Windows VM and make sure it's in same Resource Group and Area like pre-configured AD Domain service.
2. Login to the machine via Remote Desktop Connection.
3. Make Windows VM join Domain we configured in the above sections,  
   From "This PC", right click and select Manage, In "Computer name, domain, workgroup settings" Click on "Change Settings",

Click on Change,

Then, Click on "Member Of" and select "Domain", then type the created Domain name in previous sections, in our example it's "[mohamedkhaledincorta.onmicrosoft.com](http://mohamedkhaledincorta.onmicrosoft.com)"

1. Open IE browser or chrome and Download LDP tool using below link: <https://www.computerperformance.co.uk/w2k3/utilities/ldp.htm>
2. After successfull download, Click on LDP.exe
3. LDP tool will be empty like below Snaptshot,

**Note** : To View the tree of any LDAP we should go through 3 steps ( Connect, Bind, and View ), All steps will be shown in detail within the below steps:

1. From Connection, Select "Connect",
2. In Server Type Domain Name and in Port Type "389",
3. Now, Let's Bind .. From Connection Select Bind,

10. Enter User Name we created in previous Section and password then make sure you checked the Domain Field.

10.

11. Now, We're ready to View the tree, From View, Select Tree,

12. Click on Drop Down icon and select our Domain Name in the shown format,

13. Nice, Now you can see the tree and this is an Excellent Validation to the previous work.

**[ Validation ] – Connect to LDAP Via Linux "ldapsearch":**

1. Using Azure Virtual Machines Service, Create Linux VM in the Same Zone and resource group like AD Domain service.
2. Installing "ldapsearch","ldapsearch" exists in many ldap clients packages, Let's search for one of them using below command,

yum whatprovides \*/ldapsearch

1. Based on the result, run the below command,

yum install <package\_name>

1. Now, "ldapsearch" is installed, Run the below command on your linux terminal,

ldapsearch -x -H 'ldap://10.0.0.17:389' -b 'DC=mohamedkhaledincorta,DC=onmicrosoft,DC=com' -s base -D 'mohamed.abdullah@m [ohamedkhaledincorta.onmicrosoft.com](http://ohamedkhaledincorta.onmicrosoft.com)' -w 'password'

**where,**  
**IP** Internal IP of the Domain Service.  
**Domain Name** [mohamedkhaledincorta.onmicrosoft.com](http://mohamedkhaledincorta.onmicrosoft.com) DC=mohamedkhaledincorta,DC=onmicrosoft,DC=com **User** User We created previously [mohamed.abdullah@mohamedkhaledincorta.onmicrosoft.com](mailto:mohamed.abdullah@mohamedkhaledincorta.onmicrosoft.com)  
**Password** Enter User Password

Now, You've a Successfully configured Azure AD Domain Service and it's accessible. If Any issues appeared, Revisit the steps or open ticket against Azure support team.

**Create Azure Group:**

1. From Azure All Services, Select Groups.
2. Create New Group.
3. Configure Azure Group and Add all members you need to login to incorta to this group.
4. Add This group to pre-created Azure AD SSO application in Part 1.

From All Services, Select "Azure Active Directory",

Select "Enterprise Applications", Then Click on APP created in Part 1.

Select "Users and groups", And add the group we created.

Now, We're ready to sync Azure users from Incorta.

**Configure Incorta to Sync Azure user in SSO group related to Azure AD SSO app:**

**Notes :**

1. Edit file <Incorta\_Installation\_Dir>/bin/ldap-config.properties Notice Lines in Red.

**# Provide ldap url**  
**# Example: ldap://HOST\_NAME:PORT\_NUM**  
**ldap.base.provider.url=ldap://10.0.0.17:389**  
**# Distinguished Name to connect with**  
**ldap.base.dn=OU=AADDC Users,DC=mohamedkhaledincorta,DC=onmicrosoft,DC=com # Distinguished Name and password of a user in the ldap to authenticate with** [**ldap.user.dn=mohamed.abdullah@mohamedkhaledincorta.onmicrosoft.com**](mailto:ldap.user.dn=mohamed.abdullah@mohamedkhaledincorta.onmicrosoft.com) **ldap.user.dn.password=Password**  
**# The attributes that will map login name, mail and name of Incorta user ldap.user.mapping.login=mail**  
**ldap.user.mapping.name=cn**  
**ldap.user.mapping.mail=mail**  
**# The attributes that will map name and attached users of Incorta group ldap.group.mapping.name=cn**

**Make sure that Linux VM Contains Incorta is located in same zone and Resource Group like Azure AD Domain Service. Incorta is on HTTPS**

**ldap.group.mapping.member=member**

**# a filter to search users with given example**

**ldap.user.search.filter=(&(objectCategory=user)(memberOf=cn=SSOGROUP3,OU=AADDC Users, DC=mohamedkhaledincorta,DC=onmicrosoft,DC=com))**  
**# a filter to search groups with given example ldap.group.search.filter=(&(objectCategory=Group)(cn=SSOGROUP3))**

**#user.type is optional with default (ldap) and indicates the user type, possible values are: internal, sso, and ldap user.type=ldap**  
**#ldap.follow.referral is optional with default (false) and indicate that it does not have a copy of a requested object and giving the client a location that is more likely to hold the object,**

**#which the client uses as the basis for a DNS search for a domain controller.**  
**#Ideally, referrals always reference a domain controller that indeed holds the object.**  
**# If set to true ,the search will be slower So Please don't use it unless you have multiple reference Site! ldap.follow.referral=false**

**Explanation:**  
**ldap.base.provider.url** ldap://<local\_ip\_of\_domain\_service>:389 **ldap.base.dn**=OU=AADDC Users,DC=mohamedkhaledincorta,DC=onmicrosoft,DC=com

Where,

**AADC Users** is the group contains users of Azure Domain Service. **DC=mohamedkhaledincorta,DC=onmicrosoft,DC=com** [mohamedkhaledincorta.onmicrosoft.com](http://mohamedkhaledincorta.onmicrosoft.com) domain Name.

**ldap.user.dn User Created in Part 2, should be member of Admin Group of Domain Service "AAD DC Administrators"**

**ldap.user.dn.password User password**

**ldap.group.mapping.member should be "member"**

**ldap.user.search.filter=(&(objectCategory=user)(memberOf=cn=SSOGROUP3,OU=AADDC Users, DC=mohamedkhaledincorta,DC=onmicrosoft,DC=com))**

**Where cn Group we created earlier "Create Azure Group/Part2" ldap.group.search.filter=(&(objectCategory=Group)(cn=SSOGROUP3))**

**Where cn Group we created earlier in "Create Azure Group/Part2"**

1. Edit below line in file <Incorta\_Installation\_Dir>/sync\_directory\_with\_ldap.sh

session=`$incorta\_cmd login https://incorta\_url:port/incorta <tenant\_name> incorta\_user incorta\_password False`

1. Run Script sync\_directory\_with\_ldap.sh , notice and validate results.

How to validate ?  
exported Group -> Should be the group which is member of Azure AD SSO app that we created in "Create Azure Group/Part2"  
exported Users -> Members we added to this group.

Important Notes:  
All users should have Email configured.  
Any Change in Azure Part will take min 20 mins to Reflect in the system.