Documentation : Ambience/Repertoire 202x LDAP Configuration

Additional notes can be found here : https://support.elixirtech.com/t/configure-ambience-repertoire-202x-server-to-use-ldap-authentication

For Ambience/Repertoire 202x LDAP Configuration (/etc/application.conf), set ldap-sso enabled to 'true', e.g.:

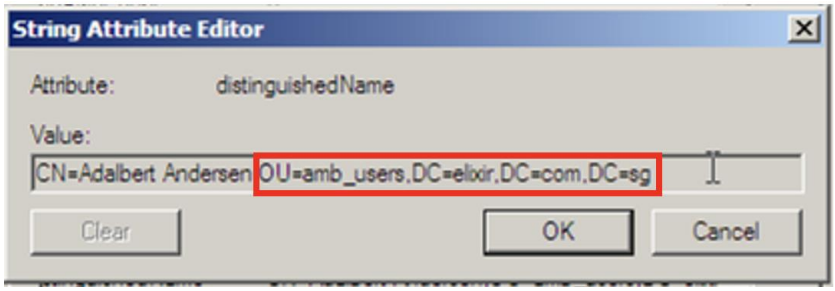
choose either simple-sso (default) or ldap-sso or federated-sso
ambience.modules.simple-sso.enabled = false
ambience.modules.ldap-sso.enabled = **true**
ambience.modules.federated-sso.enabled = false

Refer to the following table for **points 1,2,3,4,6,7**		
1	host	Refers to the hostname or IP address of your Active Directory (AD) Server
2	port	Refers to the port number your AD uses for LDAP protocol
3	protocol	Set 'default' for LDAP or 'ldaps' for LDAPS
4	method	Set 'simple' for username/password authentication, 'none' for anonymous
6	user	For example, in Ambience/Repertoire 202x, it should be written as follows: `user = "CN=admin,CN=user,DC=elixir,DC=com,DC=sg"`

		The bind user should have the rights to traverse through the Active Directory.
7	password	Please encrypt your plain-text password for use in Ambience/Repertoire 202x. For more reference, do refer to the following support entry: https://support.elixirtech.com/t/encrypting-using-ambience-repertoire-202x/540

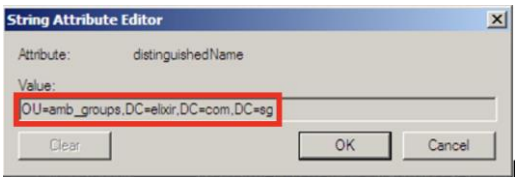
Refer to the following table for **point 5**		

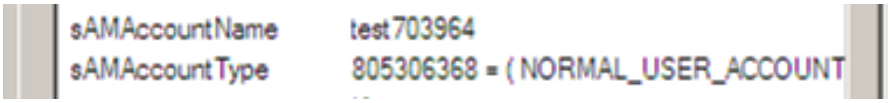
5	users	In Ambience/Repertoire 202x, it should be written as follows:
		`users = "ou=users1,DC=elixir,DC=com,DC=sg"`
		
		If you have an array of users from different OU's,
		`users = ["ou=users1,DC=elixir,DC=com,DC=sg",`
		`"ou=users2,DC=elixir,DC=com,DC=sg"]`

	From the Active Directory, (for e.g.,)	
	users	1/ From the "Active Directory Users and Computers", select an LDAP user. 2/ Right-click and select "Properties". 3/ Click on the "Attribute Editor" tab. 4/ Scroll down and refer to "distinguishedName". 5/ From the example below, the required information would be the highlighted portion.  - If you're not able to view "Attribute Editor", please refer to the following documentation: https://docs.secureauth.com/0902/en/enable-active-directory-advanced-features.html

Refer to the following table for **point 8**		

8	root, filter	In Ambience/Repertoire 202x, it should be written as follows:
		
		`root="OU=group1,DC=elixir,DC=com,DC=sg"`
		`filter="member=CN=${username},OU=group1,DC=elixir,DC=com,DC=sg"`
		
		If you have an array of groups from different OU's,
		
		`groups: [{`
		`enabled = true`
		`root = "OU=group1,DC=elixir,DC=com,DC=sg"`
		`filter =`
		`"member=CN=${username},OU=group1,DC=elixir,DC=com,DC=sg"`
		`},{`
		`enabled = true`
		`root = "OU=group2,DC=elixir,DC=com,DC=sg"`
		`filter =`
		`"member=CN=${username},OU=group2,DC=elixir,DC=com,DC=sg"`
		`}]`

	From the Active Directory, (for e.g.,)	
	root, filter	1/ From the “Active Directory Users and Computers”, select the LDAP group used. 2/ Right-click and select “Properties”. 3/ Click on the “Attribute Editor” tab. 4/ Refer to “distinguishedName”. 5/ From the example below, the required information would be the highlighted portion.  - If you’re not able to view “Attribute Editor”, please refer to the following documentation: https://docs.secureauth.com/0902/en/enable-active-directory-advanced-features.html

Refer to the following table for **point 9**		
9	uidAtrribute	- “uidAttribute” is a unique identifier for an LDAP user. - Commonly used attributes includes: “uid”, “sAMAccountName” Shown below is an example on how to check the uidAttribute used in a Microsoft Active Directory. 1/ From the “Active Directory Users and Computers”, select an LDAP user. 2/ Right-click and select “Properties”. 3/ Click on the “Attribute Editor” tab. 4/ Scroll down and you should be able to observe the following which suggests that the attribute used in this AD is “sAMAccountName”.  - If you’re not able to view “Attribute Editor”, please refer to the following documentation: https://docs.secureauth.com/0902/en/enable-active-directory-advanced-features.html