Enabling LDAPv3 for OS X 10.2 at the University of Michigan

PDF version of this page

1. Log in to the computer using an account with administrative privileges.

2. Open the **Directory Access** utility from the **Utilities** folder inside the **Applications** folder. You'll need to authenticate by clicking on the lock icon.



Authenticate	
Directory Access requires that you type your passphrase.	
Name: admin	
Password or phrase:	
Details	
? Cancel OK	
	Configure

3. **LDAPv3** should already be enabled; if not, check the checkbox. It 's pretty likely that you won't need any of the other services selected, so deselect them now. Select the **LDAPv3** line and click the **Configure...** button.

Enable	Name	Version
	AppleTalk	1.0
	BSD Configuration Files	1.1
	LDAPv2	1.5
. ∡	LDAPv3	1.5.4
	NetInfo	1.5.1
	NIS	1.0
	Rendezvous	1.0.1
	SLP	1.0
	SMB	1.0
	Configure	

4. Select the location you want to configure, deselect **Use DHCP-supplied LDAP Server**, and click on the **Show Options** button.

	Location: Automatic	•
	Use DHCP-supplied LD	AP Server
Show Options —	Talk onfiguration Files	1.0
		Cancel OK

5. Click on the **New...** button. Double-click on **Untitled 0**, and change it to **umichIdap.v3**,. Double-click on **unknown.domain.com** and change it to **Idap.itd.umich.edu.** Leave **LDAP Mappings** set to **Custom**. Currently, SSL is not supported (it will be soon); so for now, **don't** select the SSL checkbox. With the entire line highlighted, click on the **Edit...** button.

▲ +	L (lide Options	ocation: Automatic Use DHCP-supplied LD	AP Server	
Enable	Configuration Name	Server Name or IP Address	LDAP Mappings	SSL
\checkmark	Untitled 0	unknown.domain.com	Custom	

6. Under the **Connection** tab, you shouldn't need to make any changes, so click on the **Search** & **Mappings** tab. Under the **Record Types & Attributes** box,click on the **Add** button.

umichldap.v3				
Connection	Searc	h & Mappings		
Configuration Name:	umic	hldap.v3		
Server Name or IP Address: Idap.itd.umich.edu				
Open/close times out in	120	seconds		
Connection times out in	120	seconds		
Use authentication when connecting				
Distinguished Name:				
Password:				
Encrypt using SSL				
Use custom port	389			
		Cancel OK		

Access this LDAPv3 server using	Custom
Record Types and Attributes	Map to any 🛟 items in list
▶ Default Attribute Types	
Delete Add	Delete Add
Search base:	
Search in: 🔘 all subtrees	O first level only
	Write to Server

7. Make sure the **Record Types** radio button is selected, select **Users** and then click the **OK** button.

PresetGroups	
PresetUsers	
PrintService	
PrintServiceUser	
Printers	
Protocols	
RPC	
Server	1
Services	1
UserAliases	
Users	
WebServer	*
Select an item to add t to select multiple item	to the list. Shift or command-click is.

8.Click inside the Search base text box. Type in ou=people, dc=umich, dc=edu.

um	ichidap.vs
Connection	Search & Mappings
Access this LDAPv3 server using	Custom
Record Types and Attributes	Map to any 📫 items in list
▶ Default Attribute Types	
►Users	
Delete Add	Delete Add
Search base: ou=people, dc=u	mich, dc=edu
Search in: 💽 all subtrees	first level only
	Write to Server
	(Cancel) OV
	Cancer

9. Back in the **Record Types & Attributes** box, make sure **Users** is selected and click the **Add** button again. Make sure the **Attribute Types** radio button is selected. Select **RecordName** and click the **OK** button. Again, back to the **Map to** box and click the **Add** button. Type in **uid**.

	Attribute Types	-
Access 1	PrintServiceUserData Protocols	•
Record	RealName	n list
_	RecordName	L
► Defa ► User	SetupAssistantAdvertising SetupAssistantAutoRegister SetupAssistantLocation State URL URLForNSL UniqueID UserShell Select an item to add to the list. Shift or command-click	Ð
Searc	Cancel OK	er)

Access this LDAPv3 ser	rver using Custom
Record Types and Attri	ibutes Map to any 🛊 items in lis
► Default Attribute Ty ▼Users	ypes uid
Delete	dd Delete Add
Search base:	
Search in: 🔵 all sub	otrees 🔘 first level only

10. Repeat the same steps using the following information:



Make sure to include AuthenticationAuthority mapping; it's a recent addition for security!

Attribute Type:	Maps to:
RecordName	uid
RealName	cn
UniqueID	uidnumber
PrimaryGroupID	gidnumber
NFSHomeDirectory	homedirectory
UserShell	loginshell

EmailAddress	mail
AuthenticationAuthority	loginshell

11. When you are finished, click the **OK** button. At the next screen, click the **OK** button there as well.

	Connection	Search & Mappings
Access this LDAP	/3 server using	Custom
Record Types and	Attributes	Map to any 🛟 items in list
UniquelD PrimaryGrou NFSHomeDi UserShell EMailAddres Authenticat	upID rectory is ionAuthority	loginshell
Delete	Add	Delete Add
earch base:		
Search in: 🔘 a	ll subtrees	first level only
		Write to Server

▲ +	Li Iide Options	ocation: Automatic	AP Server	
Enable	Configuration Name	Server Name or IP Address	LDAP Mappings	SSL
	umichldap.v3	ldap.itd.umich.edu	Custom	•
Dupl	icate Delete	Edit New.	Cancel	ОК

12.Click on the **Authentication** tab. You can remove any previous custom paths by selecting them and clicking the **Remove** button. Then click the **Add** button, and select **/LDAPv3/Idap.itd.umich.edu**. Then click the **Add** button. Nothing under the **Contacts** tab needs to be configured, so you can click on the **Apply** button. Click on the red close-window button **Save** the changes, and you are done!

0	Directory Access
	Services Authentication Contacts
	Choose where to search for user authentication information.
	Search: Custom path
Directory	Node
/NetInfo	/root
/LDAPv2	/ldap.itd.umich.edu
	Drag directory nodes into your preferred order for searching.
	Remove Add
en 1 - 2	

c	oose where to s	earch for user aut	hentication information	
	Search: C	ustom path	•	
Directory N	lode			
/NetInfo/I	oot dap.itd.umich	n.edu		
D	ag directory noc	les into your prefe	rred order for searching	g.
	R	emove Ad	d	

13. Start the **Terminal** application from the **Utilities** folder in the **Applications** folder.

14. Type id *uniquename* <Enter>, where uniquename is a "Michigan Person" who does not have a local user account on the computer. The reply will come back id: uniquename: No such user until the changes come through; then you should get the uid, gid, and groups values for that unquename. That indicates that everything is working correctly.

00 /usr/bin/login (ttyp1) [localhost:~] jhstew% id wes id: wes: No such user [localhost:~] jhstev% id wes id: wes: No such user [localhost:~] jhstev% id wes id: wes: No such user [localhost:~] jhstev% id wes id: wes: No such user [localhost:~] jhstev% id wes id: wes: No such user [localhost:~] jhstev% id wes id: wes: No such user [localhost:~] jhstev% id wes id: wes: No such user [localhost:~] jhstev% id wes id: wes: No such user [localhost:~] jhstev% id wes uid=5386(wes) gid=10 groups=10

Additional sites for your UM OS X Configurating pleasure:

http://www.umich.edu/~arosenbl has pages on configuring both MIT Kerberos and OpenAFS http://www.itd.umich.edu/macos/macosx_more.html The "more" page has all the good stuff. Well, more is **MORE**, isn't it? Reloading a lab? You need Radmind...<u>http://rsug.itd.umich.edu/software/radmind/macosx.html</u> Running logout scripts, or other scripts that want a gui? <u>http://rsug.itd.umich.edu/software/ihook</u> Setting up a lab in the first place? <u>http://www.macosxlabs.org</u> is where you need to go. No, trust me; you need to go there.

How about a free secure ftp client? http://rsug.itd.umich.edu/software/fugu