# Configure Ezeelogin to authenticate using Windows\_AD / OpenLDAP in Debian?

362 Manu Chacko March 27, 2025 Features & Functionalities, Tweaks & Configuration 3440

# Configure Ezeelogin to authenticate using Windows\_AD / OpenLDAP (Pam-Ldap) in Debian.

**Overview**: This article describes the steps to configure Ezeelogin to authenticate using Windows Active Directory or OpenLDAP (PAM-LDAP) on Debian, including installing necessary PHP and PAM-LDAP modules, adjusting configuration files, and validating the setup.

**Note:** Make sure that the PHP-LDAP extension is installed on the server. Replace the PHP version in the below command.

```
root@jumpserver:~# apt-get install phpx.x-ldap
```

eg: -----> :~# apt-get install php8.2-ldap

root@jumpserver:~# systemctl restart apache2

1. Login to Web-GUI > open settings > Ldap

Iow to find base DN and bind RDN

• Add the details of LDAP configurations & Check **WINDOWS ACTIVE DIRECTORY** if you are authenticating with <u>Windows</u> **AD** & **Save.** 

Multiple URIs or a list of URIs can be specified in the format:

Idaps://host.com:636/ Idaps://host.com:636/

(Only the protocol, hostname, and port fields are allowed.)

Ezeelogin		Le Velcome, Administrat
Servers	LDAP Settings	
Web Portals	Name	
. Users 🕨 🕨	openIdap	
Access Control	URI(s) @	
Settings	ldap://10.11.1.164	
General	Start TLS 🞯	Base DN 🐵
Branding	- X	cn=users,dc=ad2016,dc=admod,dc=net
Control Panels	Pind PDN (2)	Direct Deserver of @
Data Centers		
API	cn=Administrator,cn=users,dc=ad2016,dc=admod,dc=net	
LDAP	UID Attribute 🕑	Filter 🞯
SAML	sAMAccountName	
RADIUS	First Name Attribute @	Last Name Attribute
Server Fields	aivonNamo	
Cluster	givenivanie Email Attribute @	Croup Attribute @
Command Guard	mail	
Account ►	Timeout @	Rank @
Help	10	10
License	Active @	Windows Active Directory @
		1

2. Open **Settings > General > Authentication >** change web panel **authentication to LDAP** & Check **External SSH Auth.** 

Ezeelogin						Welcome, Administrato	or Logout
E Servers	Ceneral Settings	Authentication	Two Eactor Authoritication	Socurity	Dofaulte	Miscollanoous	
Ueb Portals	Password / Security Code Retries	Authentication	Login captcha @	Security	Delauits	Wiscenarieous	
1. Users	2		Disable	\$			
Access Control	Web Panel Authentication @		External SSH Auth				
°₀ Settings 🗸	LDAP 🛊 ┥		Image: A state of the state				
General	reCAPTCHA Sitekey @ <u>Get reCAPTCHA</u>	<u>API Key</u>	reCAPTCHA Secret	0			
Control Panels	User Password Lifetime @		Maximum Days With	out Login 💿			
► Data Centers	0		0				
► API	Allow Browsers To Save Login @		Security Code LDAF	0			
► LDAP			×				
► SAML							1
► RADIUS			Cancel Save				
Server Fields							

3. Select the LDAP users and import them to Ezeelogin.

Ezeelogin								Velco	ome, Administrator I
≣ Servers ►	^ 	sers in LDAP	find	All	-			Imp	ort/Update selected
Web Portals		Username ↓	First Name	Last Name	Email	Status	User Group	LDAP	Notes
t Users		) alex	alex			New	Dummy	openIdap	_/
		jake	jake			New	Dummy	openIdap	
User Groups	C	) john	john			New	Dummy	openIdap	1
Authentication Log									1 - 3 /
	1.0			1	ANT STORE STORE	N. Contraction	The Artist	1	
	U	sers not in LDAP	find	All	~				۲
	U	sername 🗸	First Name	Last Name	Email	Sta	tus User	Group	Actions
	1.1				No item				
				No. No. Contraction	C. P. C. C. C. C. C.	ANTE STO	100 Mar 100		
		•	19. 3. 5° 1. 8/ 3.				•	1	
		C. Anna Star							
	A .		a start and		57.	and ha		in the second	

- You can confirm the imported LDAP users were listed in Users.
- Now you can log in to Ezeelogin with LDAP users in Ezeelogin GUI.
- After importing the users to Ezeelogin, log in with the user and set up the security code for the user under Account > Password > New Security Code.
- Skip the 4th & 5th steps if you are configuring OpenLDAP.

## 4. Make sure that UNIX ATTRIBUTES is enabled on WINDOWS(2003,2008,2012) SERVER.

Note: You do not need to install unix attributes on Windows 10 and Windows 2016 server OS.

- Log in to the Windows server & open the command prompt.
- Enter the below command:

Dism.exe/online/enable-feature /featurename:nis /all

- Reboot the server to complete the installation
- 5. Make sure to add the values for UID, GID, Login Shell, and Home Directory.

Win 2008 Unix Attributes

<b>2</b> 🔥 🤇	ka 📟 📼 🗛					
<u> </u>	Jake j. b Propert	ties			?	×
ord Replic	Member Of General Add Remote control	Dial-i dress   Acco   Terminal	n   Env ount   Profile Services Profile	ironment Telephones COM+	Sessions Organization UNIX Attributes	ount for adn this group (
rd Replici	To enable acce NIS domain this	ess to this user s user belongs t	for UNIX clients, to.	you will have t	o specify the	<sup>F</sup> this group this group
	NIS Domain:	admod				who are pe administrat
	UID:	1000				controllers in juests isers
Domain C	Login Shell:	/usr/local/bir	n/ezsh			<sup>E</sup> this group
Owners	Home Directory:	/home/jake				this group ( ount for gue
	Primary group name/GID:	ezusers			•	his group ca
ntrollers						<sup>F</sup> this group administrat
		ОК	Cancel	Apply	Help	

• For Window 2016 AD user set the attributes such as uidNumber = 10001, gidNumber = 12001, unixHomeDirectory = /home/jake, loginShell=/usr/local/bin/ezsh



For the Unix Attributes uidNumber, gidNumber, and loginShell to be visible, make sure to click on the Filter button and select ONLY " Show Only Writable Attributes" as shown below.

ke Propertie	s					?	$\times$	
ublished Cer	tificates	Member Of	Passwor	rd Replication	n Dia	l-in	Object	
Security	Envi	ironment	Ses	sions	Remo	te cor	ntrol	
General	Address	Account	Profile	Telephon	es (	Organi	ization	
Remote D	esktop Serv	rices Profile	C	:OM+	Attrib	ute Eo	ditor	
Attributes:								
Attribute		Value					^	
terminalSer	ver	<not set=""></not>						
textEncode	edORAddr	<not set=""></not>						
thumbnailL	ogo	<not set=""></not>						
thumbnailP	hoto	<not set=""></not>						
title		<not set=""></not>	•					
uid		<not set=""></not>						
uidNumber		10002		_				
unicodePw	/d	<not set=""></not>						
unixHomeL	Directory	/home/ja	ke					
unixUserPa	assword	<not set=""></not>	•					
un	ntControl	0/200 - (			5			
userCert	ricontrol	<not set=""></not>	NOT MA		,			
userCertific	ate	<not set=""></not>					~	
<						>		
<b>E</b> 10				<b>_</b>			_	
Edit					1	liter		I
						Sho	w only at	tributes that have values
					$\checkmark$	Show	w only w	ritable attributes
							-	
	OK		ancel	Apply		31101	w attribu	tes:
	UN		ancei	νфріγ	$\sim$	M	andatory	/
					$\checkmark$	0	ptional	
						Show	w read-o	nly attributes:
						C	onstructe	ed
						Ba	cklinks	
						0.	- the second second	l.
					$\sim$	Sy	stem-on	ny

# Let's configure PAM\_LDAP Authentication for SSH

• Login to Ezeelogin SSH server to configure pam-LDAP.

1. Install the pam-LDAP module by the following command:

root@jumpserver:~# apt install libnss-ldap libpam-ldap ldap-utils nscd

2. Enter LDAP URI, Base dn, select Ldap version 3, Bindpassword, and BInddn on prompts.

• You can reconfigure the settings with the following command

root@jumpserver:~# dpkg-reconfigure libnss-ldap

**Note:** Skip the 3rd step if you are configuring OpenLDAP.

### 3. Add Active Directory Mappings to /etc/libnss-ldap.conf

• Search for RF 2307 (AD) mapping & add or uncomment the following lines.

root@jumpserver:~# nano /etc/libnss-ldap.conf

nss\_map\_objectclass posixAccount user

nss\_map\_attribute uid sAMAccountName

nss\_map\_attribute homeDirectory unixHomeDirectory

nss\_override\_attribute\_value loginShell /usr/local/bin/ezsh

4. Append 'ldap' to password, group & shadow in /etc/nsswitch.conf

```
root@jumpserver:~# cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages
installed, try:
# `info libc "Name Service Switch"' for information about this file.
passwd: files systemd ldap
group: files systemd
                      ldap
shadow: files ldap
qshadow: files
hosts: files mdns4_minimal [NOTFOUND=return] dns myhostname
networks: files
protocols: db files
services: db files
ethers: db files
rpc: db files
netgroup: nis
```

<sup>5.</sup> Enable auto-create home directory on login by adding the following to **/etc/pam.d/common-session** by the following command

```
root@jumpserver:~# echo "session optional pam_mkhomedir.so
skel=/etc/skel umask=077" >> /etc/pam.d/common-session
```

6. Edit /etc/pam.d/common-password and Remove the option '**use\_authtok**' on the password '**pam\_ldap**' module configuration as below.

root@jumpserver:~# vi /etc/pam.d/common-password # Remove the option 'use\_authtok' on the password 'pam\_ldap' module configuraiton as below. password [success=1 user\_unknown=ignore default=die] pam\_ldap.so try\_first\_pass

7. Restart nscd service

root@jumpserver:~# service nscd restart

Note: Ensure the login shell of the LDAP user is /usr/local/bin/ezsh

• Now run the id/finger command and see whether you are able to get AD user details

```
[root@jumpserver ~]# finger jake
Login: jake Name: jake t
Directory: /home/jake Shell: /usr/local/bin/ezsh
Last login Wed Jun 13 05:02 (EDT) on pts/1 from 10.1.1.13
No mail.
No Plan.
[root@jumpserver ~]# id jake
uid=10001(jake) gid=120001(domain users) groups=1547600513(domain
users)
```

logiasher. Houbleshooking: Ensure inatur rekking the values of und, gid, home directory; and is

```
[root@jumpserver]# ldapsearch -x -LLL -E pr=200/noprompt -h
l0.11.1.164 -D "administrator@ad2016.admod.net" -w admod_2016 -b
"cn=jake,cn=users,dc=ad2016,dc=admod,dc=net"
dn: CN=jake,CN=Users,DC=ad2016,DC=admod,DC=net
objectClass: top
objectClass: person
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: jake
givenName: jake
```

distinguishedName: CN=jake,CN=Users,DC=ad2016,DC=admod,DC=net instanceType: 4 whenCreated: 20180703063304.0Z whenChanged: 20180703063554.0Z displayName: jake uSNCreated: 45128 uSNChanged: 45136 name: jake objectGUID:: ldpkFlnRs006irphlTq1AA== userAccountControl: 512 badPwdCount: 0 codePage: 0 countryCode: 0 badPasswordTime: 0 lastLogoff: 0 lastLogon: 0 pwdLastSet: 131750731848783837 primaryGroupID: 513 objectSid:: AQUAAAAAAAUVAAAAmhs/bgMv2mlWATm4VQQAAA== accountExpires: 9223372036854775807 logonCount: 0 sAMAccountName: jake sAMAccountType: 805306368

```
userPrincipalName: jake@ad2016.admod.net
objectCategory:
CN=Person,CN=Schema,CN=Configuration,DC=ad2016,DC=admod,DC=net
dSCorePropagationData: 160101000000.0Z
uidNumber: 10001
gidNumber: 12000
unixHomeDirectory: /home/jake
loginShell: /usr/local/bin/ezsh
# pagedresults: cookie=
```

#### **Related Articles:**

Record and download RDP recordings.

Record RDP sessions.

Online URL: <u>https://www.ezeelogin.com/kb/article/configure-ezeelogin-to-authenticate-using-windows\_ad-openldap-in-debian-362.html</u>