Configure Ezeelogin to authenticate using Windows_AD / OpenLDAP in Debian?

362 Manu Chacko July 23, 2025 Features & Functionalities, Tweaks & Configuration 6831

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**

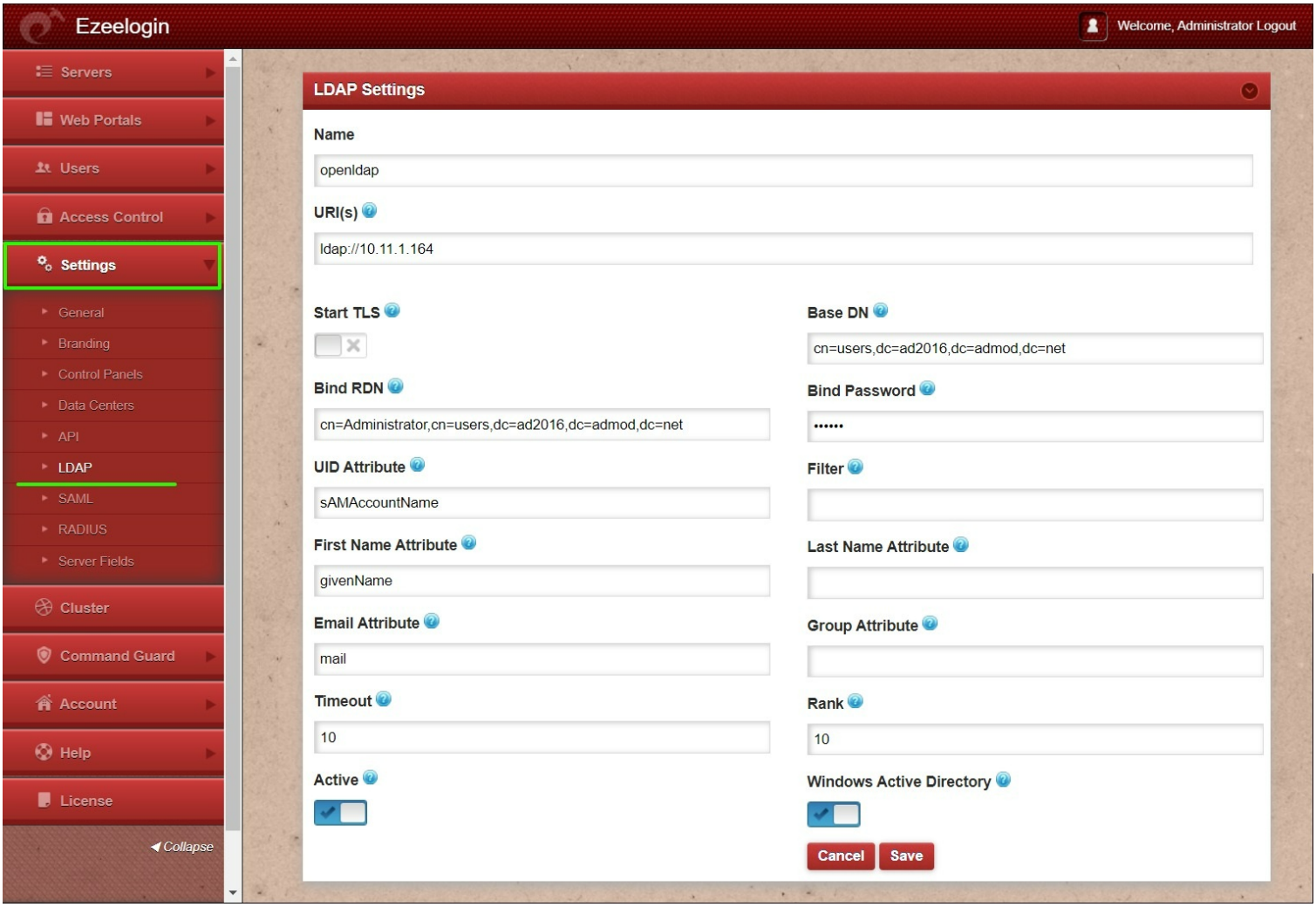
How to find base DN and bind RDN

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

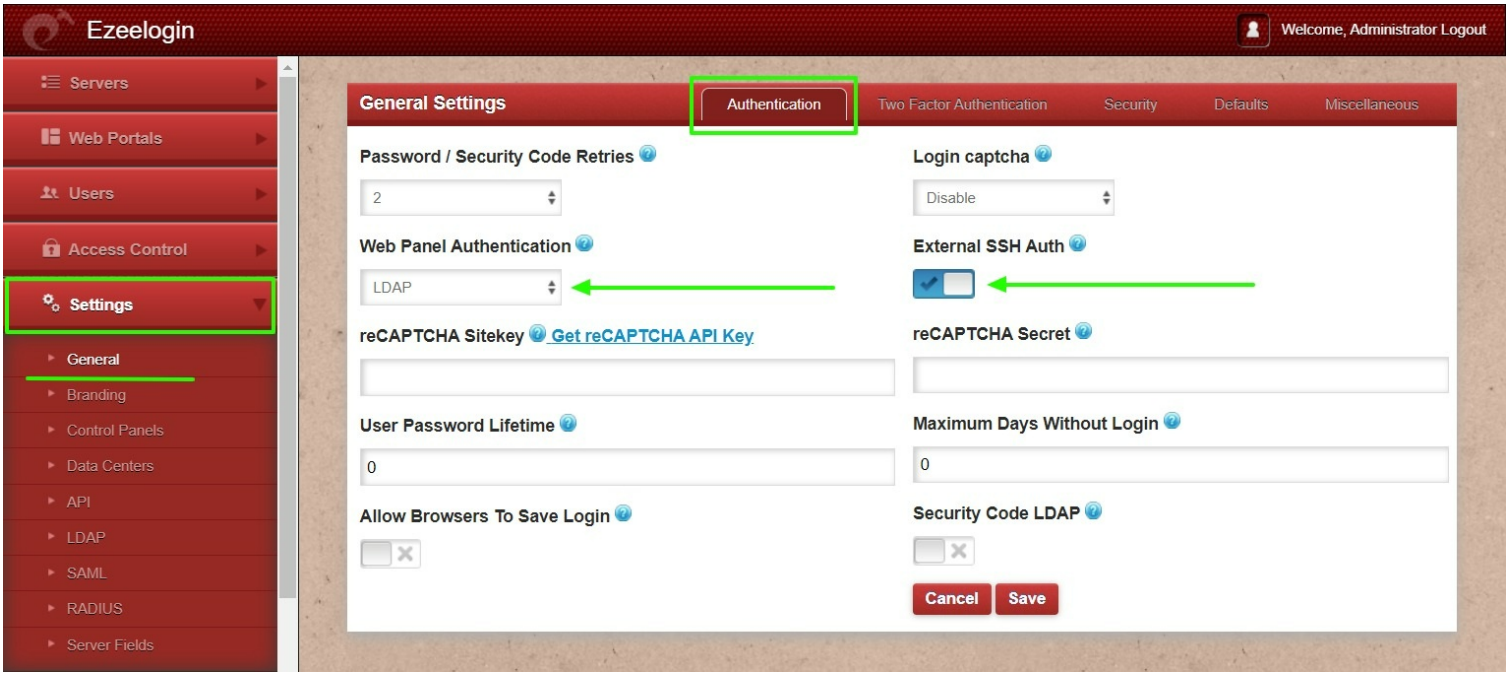
Multiple URIs or a list of URIs can be specified in the format:

- ldaps://host.com:636/ ldaps://host.com:636/

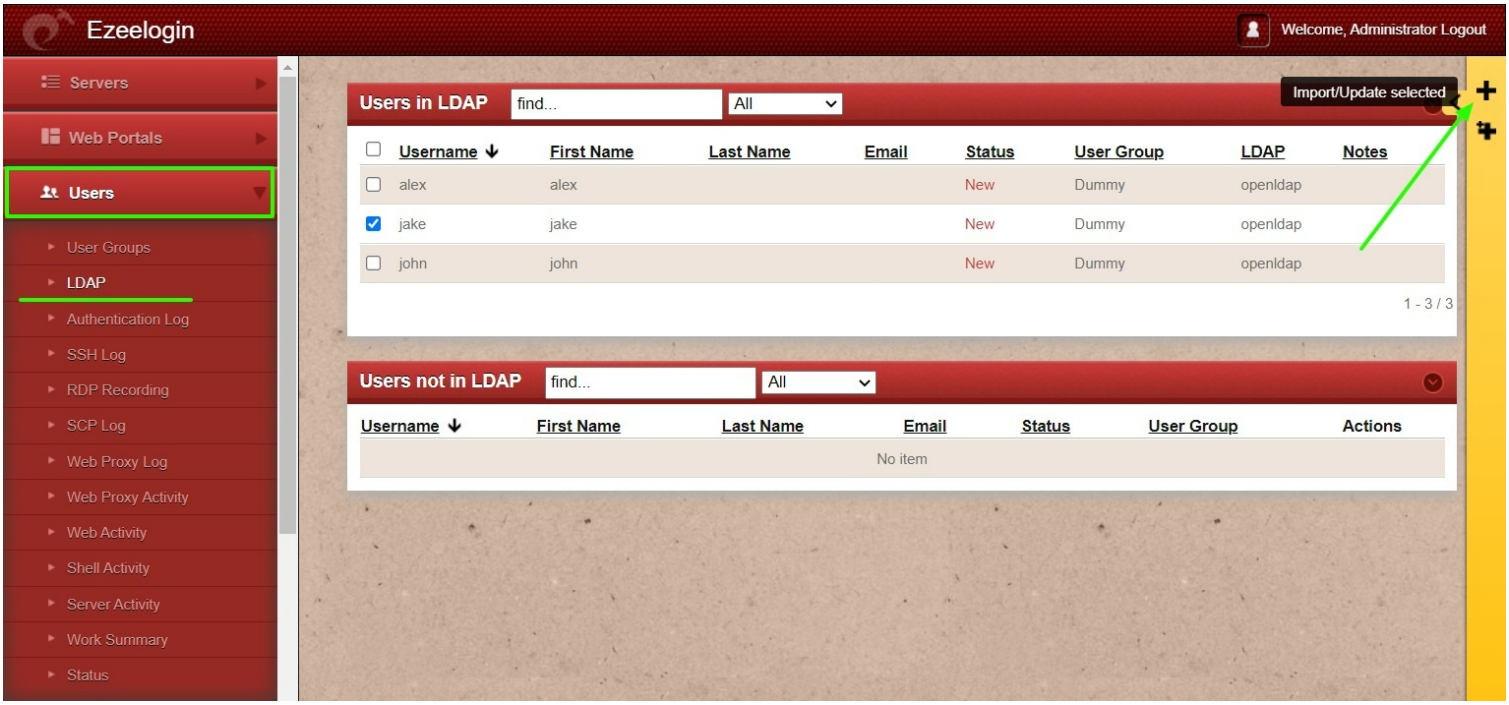
(Only the protocol, hostname, and port fields are allowed.)



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



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



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.

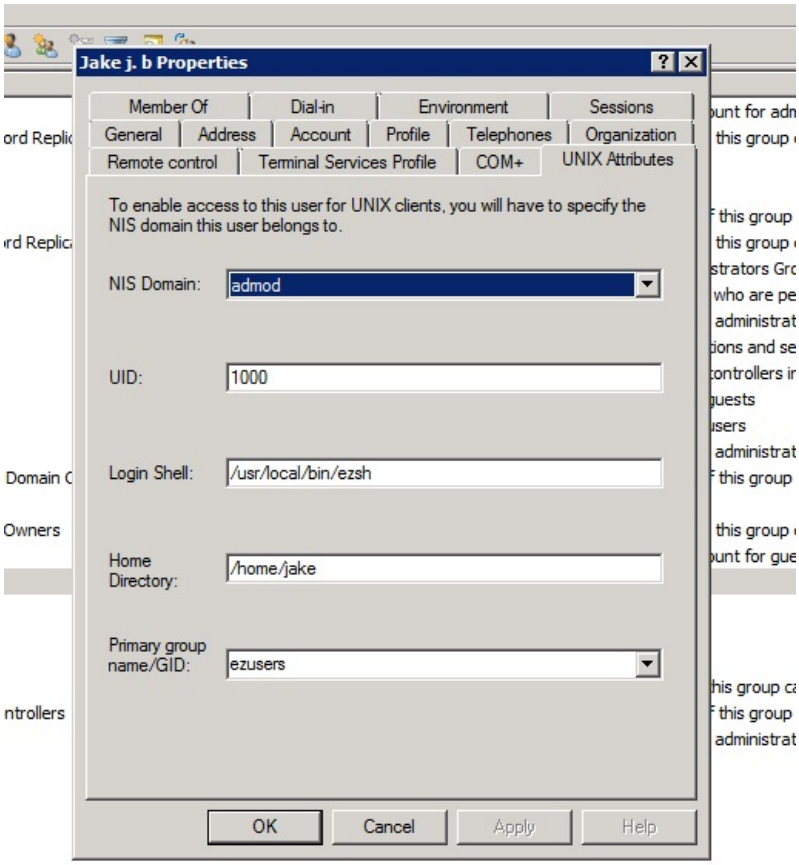
Log in to the Windows server & open the command prompt.
Enter the below command:

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

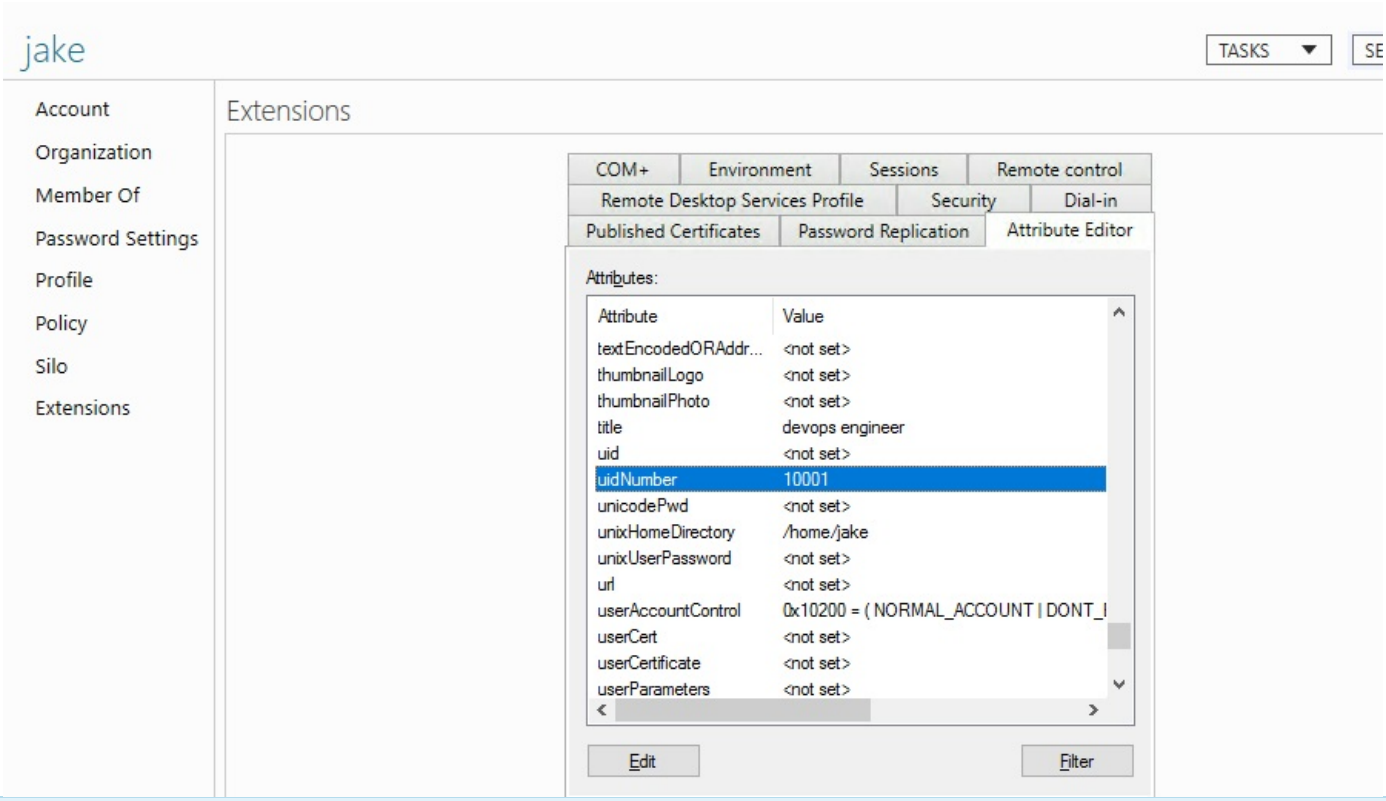
Reboot the server to complete the installation

5. Make sure to add the values for UID, GID, Login Shell, and Home Directory.

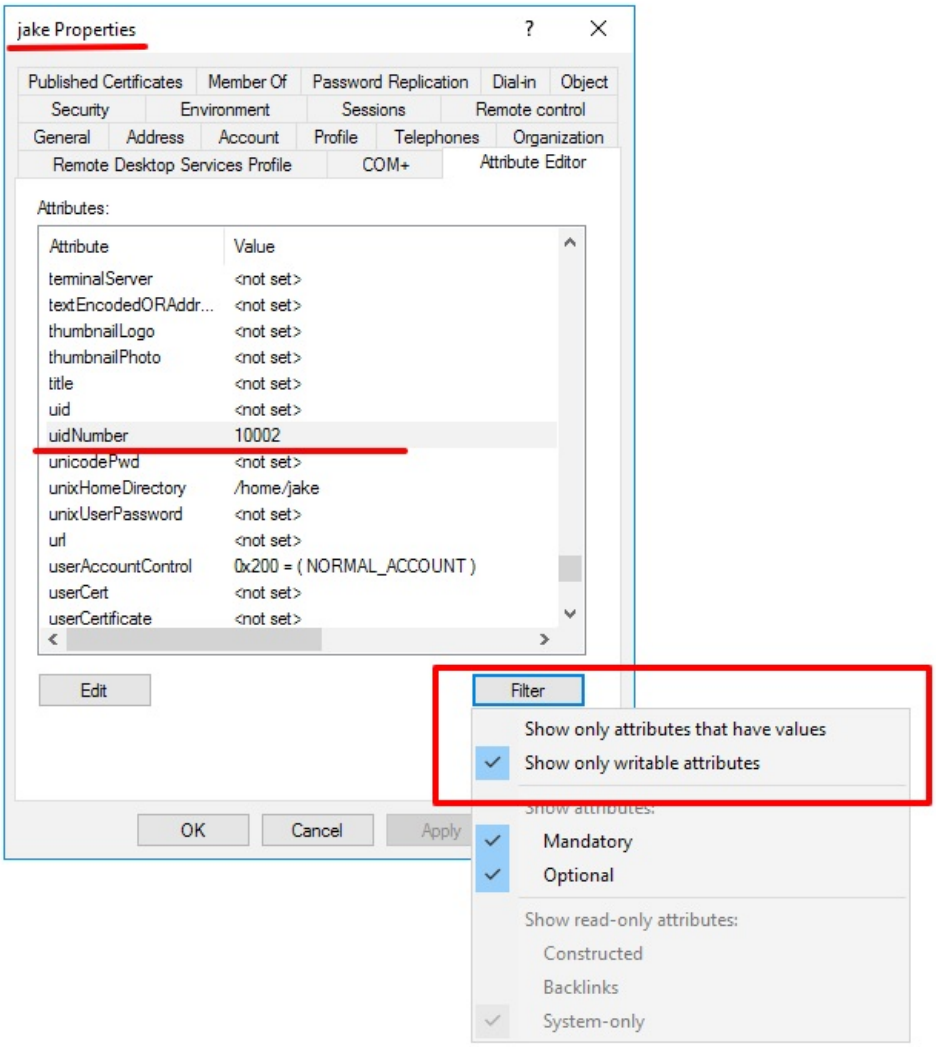
Win 2008 Unix Attributes



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.



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
gshadow: 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
```

5. 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)

Note: Run an LDAP search to check the values returned from your AD server as follows. This is used for troubleshooting. Ensure that it returns the values of uid, gid, home directory, and login shell.

[root@jumpserver]# **ldapsearch -x -LLL -E pr=200/noprompt -h 10.11.1.164 -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: 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:: ldpkFlnRs0O6irphlTq1AA==

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: 16010101000000.0Z
uidNumber: 10001
gidNumber: 12000
unixHomeDirectory: /home/jake
loginShell: /usr/local/bin/ezsh
# pagedresults: cookie=
```

Related Articles:

Record and download RDP recordings.

Record RDP sessions.

Map existing user group in ldap to Ezeelogin as Ezeelogin user group

Online URL: https://www.ezeelogin.com/kb/article/configure-ezeelogin-to-authenticate-using-windows_ad-openldap-in-debian-362.html