

Configure Ezeelogin to authenticate using Windows_AD(Pam-Ldap) in ubuntu?

187 Manu Chacko March 27, 2025 Tweaks & Configuration

14711



Configure Ezeelogin to authenticate using Windows_AD(Pam-LDAP) in Ubuntu 16.x, 18.x, 20.x, 22.x ?

Overview: This article provides steps to integrate Windows-AD (PAM-LDAP) in Ubuntu for SSH authentication via Ezeelogin. It includes PHP-LDAP installation, LDAP configuration through the web GUI, and setting up PAM_LDAP for SSH access, ensuring seamless LDAP user import and configuration verification.

Integration of WINDOWS-AD (PAM-LDAP) in Ubuntu

Install and set up the Active Directory

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

```
root@gateway:~# apt-get install php8.2-ldap
example :~# apt-get install php8.2-ldap
root@gateway:~# systemctl restart apache2
```

Step 1: Login to **Web-GUI** -> **open settings** -> **LDAP**

How to find base DN and bind RDN

Step 2: Add the details of LDAP configurations & enable **Windows Active Directory**.

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.)

The screenshot shows the 'LDAP Settings' configuration page in the Ezeelogin admin interface. The left sidebar contains a menu with 'Settings' expanded, showing options like General, Branding, Control Panels, Data Centers, API, LDAP, SAML, FIDO2, RADIUS, SIEM, and Server Fields. The main content area is titled 'LDAP Settings' and contains various input fields and checkboxes. The 'Name' field is set to 'windows2022' and the 'URI(s)' field is set to 'ldap://192.168.0.104'. The 'Start TLS' checkbox is unchecked. The 'Bind RDN' field is set to 'cn=Administrator,cn=users,dc=admod,dc=net'. The 'UID Attribute' is set to 'sAMAccountName'. The 'First Name Attribute' is set to 'givenName'. The 'Email Attribute' is set to 'mail'. The 'Timeout' is set to 10. The 'Active' checkbox is checked. The 'Verify Certificate' checkbox is unchecked. The 'Base DN' field is set to 'ou=ezeelogin,dc=admod,dc=net'. The 'Bind Password' field is masked with dots. The 'Filter' field is empty. The 'Last Name Attribute' field is empty. The 'Group Attribute' field is empty. The 'Rank' is set to 10. The 'Windows Active Directory' checkbox is checked. At the bottom right, there are 'Cancel' and 'Save' buttons.

Step 3: Open **Settings** -> **General** -> **Authentication** -> **Change web panel authentication to LDAP & enable External SSH Auth**

The screenshot shows the 'Authentication' settings page in the Ezeelogin admin interface. The left sidebar contains a menu with 'Settings' expanded, showing options like General, Branding, Control Panels, Data Centers, API, LDAP, SAML, FIDO2, RADIUS, SIEM, and Server Fields. The main content area is titled 'General Settings' and contains various input fields and checkboxes. The 'Web Panel Authentication' dropdown is set to 'LDAP'. The 'External SSH Auth' checkbox is checked. The 'Login captcha' dropdown is set to 'Disable'. The 'reCAPTCHA Sitekey' field is empty. The 'reCAPTCHA Secret' field is empty. The 'User Password Lifetime' is set to 0. The 'User SSH Key Lifetime' is set to 0. The 'Maximum Days Without Login' is set to 0. The 'Remote SSH Password Authentication' checkbox is checked. At the bottom right, there are 'Cancel' and 'Save' buttons.

Step 4: Select the LDAP users and **import** them to Ezeelogin.

The screenshot shows the 'Users' tab in the Ezeelogin admin interface. The left sidebar contains a menu with 'Users' expanded, showing options like User Groups, LDAP, Authentication Log, SSH Log, RDP Recording, SCP Log, Web Proxy Log, and Web Proxy Activity. The main content area is titled 'Users in LDAP' and contains a table with columns: Username, First Name, Last Name, Email, Status, User Group, LDAP, and Notes. The table has one row with the following data: Username: mike, First Name: mike, Last Name: , Email: , Status: New, User Group: Admins, LDAP: windows2022, Notes: . A green arrow points to the 'Import' button in the top right corner. Below the table, there is a section titled 'Users not in LDAP' with a similar table structure. The table has two rows with the following data: Row 1: Username: evan, First Name: evan, Last Name: geo, Email: qwertr@gmail.com, Status: Active, User Group: Developer, Actions: . Row 2: Username: mila, First Name: mira, Last Name: kii, Email: mira@gmail.com, Status: Active, User Group: Tester, Actions: . At the bottom right, there is a '1 - 2 / 2' indicator.

Step 5: You can confirm the imported LDAP users were listed in the Users tab. Now you can log in to ezeelogin with LDAP user in ezeelogin GUI

Note: When importing an LDAP user, they will be assigned to the default group or the mapped user group. After the import, if we change the LDAP user to another user group, we will receive a note saying "Group Mismatch." This is not an error.

Ezeelogin

Welcome, Administrator Logout

Servers

Web Portals

Users

User Groups

LDAP

Authentication Log

SSH Log

RDP Recording

SCP Log

Web Proxy Log

Web Proxy Activity

Web Activity

Shell Activity

Server Activity

Work Summary

Status

Access Control

Settings

Users in LDAP

find...

All

	Username ↓	First Name	Last Name	Email	Status	User Group	LDAP	Notes
☐	sa	Alex			New	groupldap	ldap1	
☐	achristy	Anu			Exists	groupldap	ldap1	Group mismatch
☐	lloyd	Lloyd			New	groupldap	ldap1	

1 - 3 / 3

Users not in LDAP

find...

All

Username ↓	First Name	Last Name	Email	Status	User Group	Actions
No item						

Note: 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**

Step 6: 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.

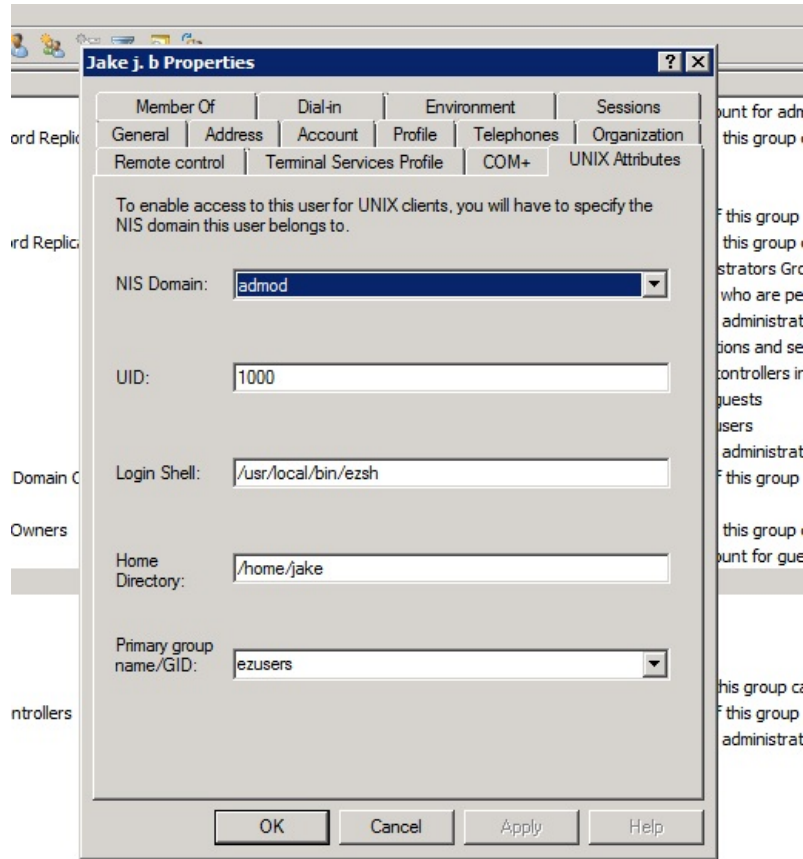
Login to the Windows server and open the Command Prompt. Enter the following command:

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

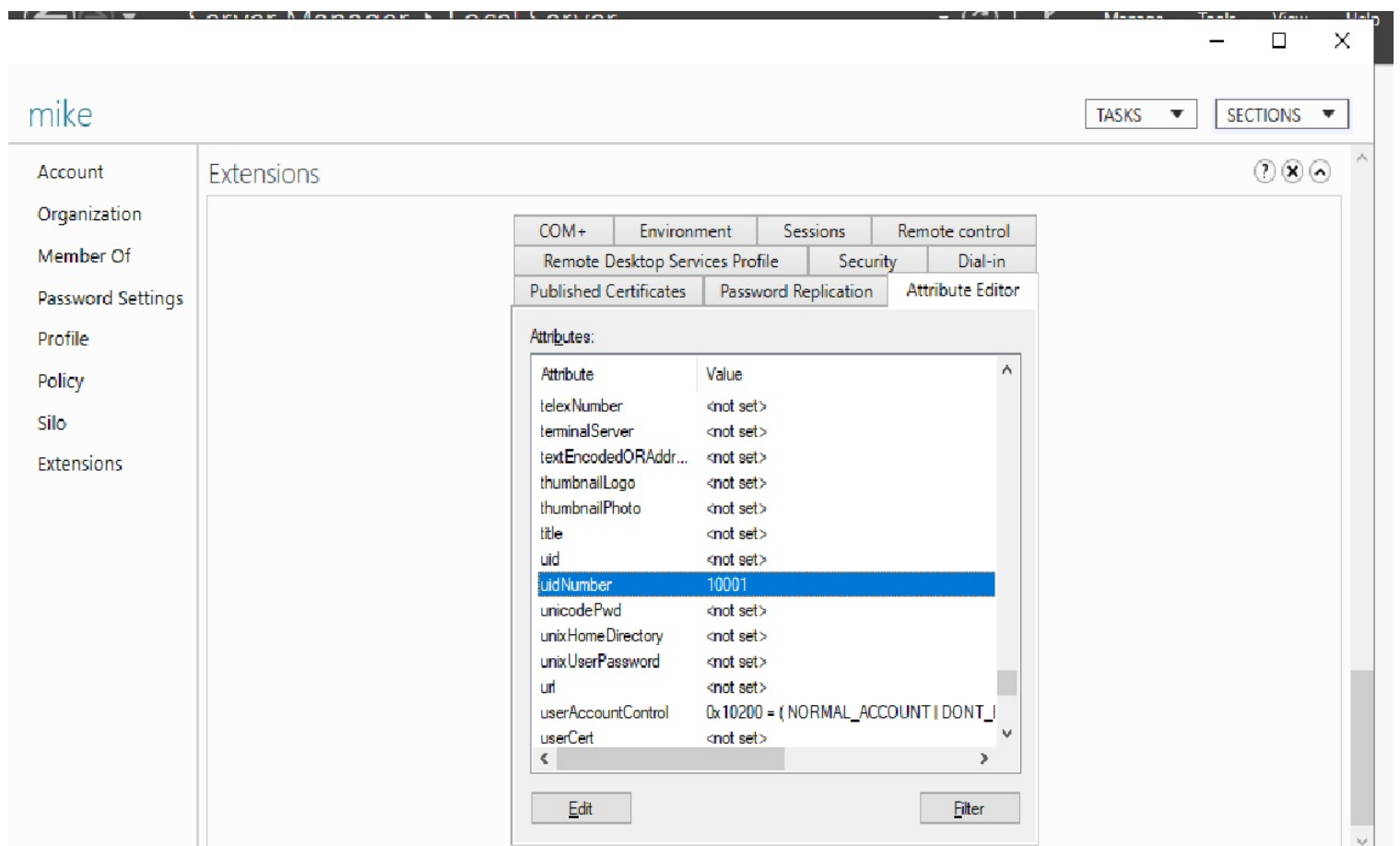
Reboot the server to complete the installation

Step 7: Make sure to add the values for UID, GID, Login Shell, Home Directory

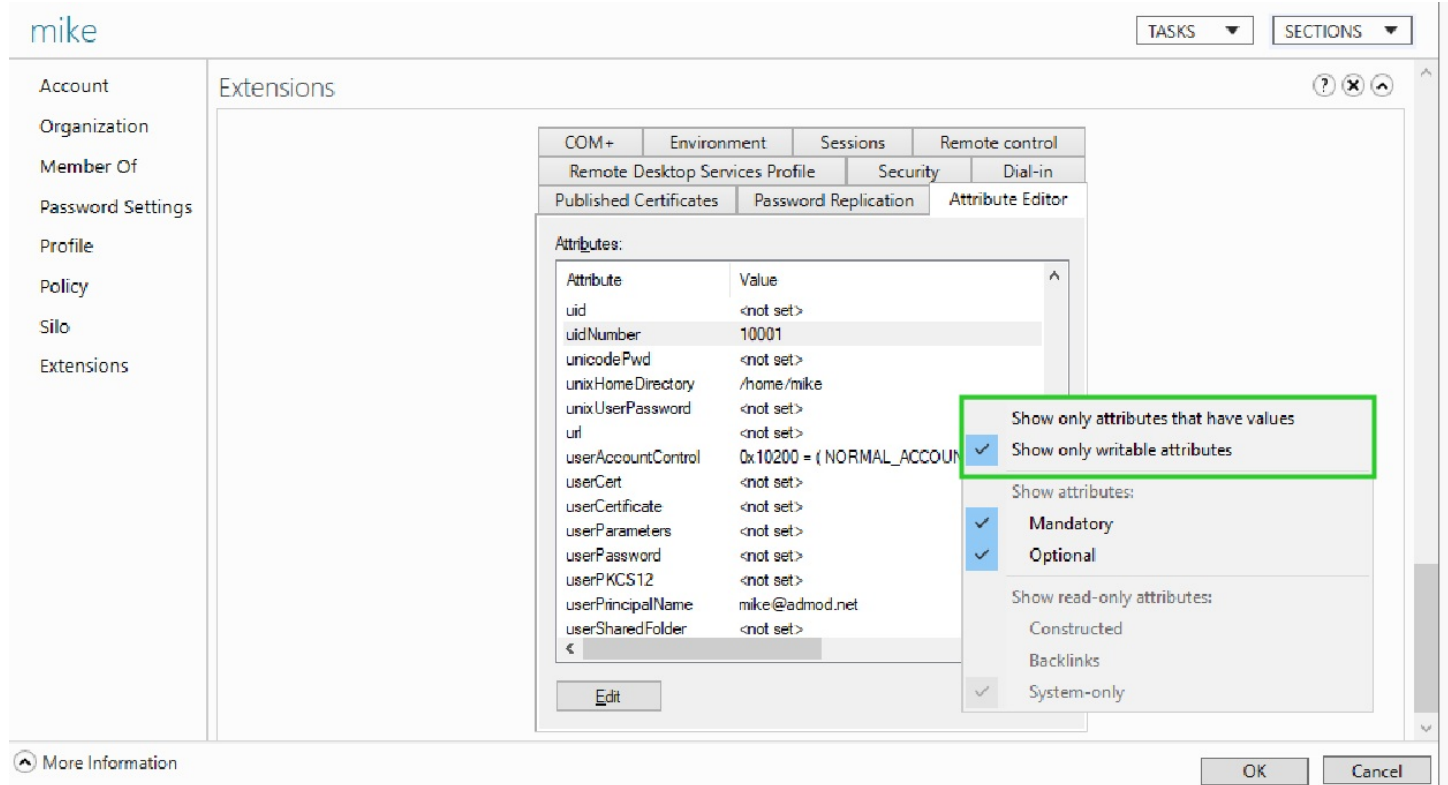
Win 2008 Unix Attributes



For Windows 2016 AD user set the attributes such as **uidNumber = 10001** , **gidNumber = 12001** , **unixHomeDirectory = /home/mike** , **loginShell=/usr/local/bin/ezsh**



Note: For the Unix Attributes uidNumber, gidNumber, and login shell 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

Step 1: Install the **pam-LDAP module** by the following command

```
root@gateway:~# apt-get install ldap-auth-client ldap-auth-config nscd
```

Step 2: Enter **LDAP URI, Base dn** & select **LDAP version 3**

Enter the details when it is prompted or you can add it later as follows.

Step 3: Add **Binddn, bind password** & Active Directory Mappings to **/etc/ldap.conf**

```
root@gateway:~# nano /etc/ldap.conf

base OU=developers,DC=adez,DC=com
uri ldap://192.168.1.15
binddn cn=admin,dc=eptest,dc=net
bindpw chaSD@#234JH56hj^7
```

Note: In Ubuntu 16.x, run the command "In -s /etc/ldap /etc/openldap" as well.

Step 4: Search for **RF 2307 (AD) mapping** & **add** or **uncomment** the following lines

```
nss_map_objectclass posixAccount user
nss_map_objectclass shadowAccount user
nss_map_attribute uid sAMAccountName
nss_map_attribute homeDirectory unixHomeDirectory
```

```
nss_map_attribute shadowLastChange pwdLastSet
nss_map_objectclass posixGroup group
nss_map_attribute uniqueMember member
pam_login_attribute sAMAccountName
pam_filter objectclass=User
pam_password ad

nss_override_attribute_value loginShell /usr/local/bin/ezsh
```

Step 5: Append 'ldap' to password, group & shadow in **/etc/nsswitch.conf**

```
root@gateway:~# 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:    compat ldap
group:     compat ldap
shadow:    compat ldap


hosts:     files mdns4_minimal [NOTFOUND=return] dns
networks:  files


protocols: db files
services:  db files
ethers:    db files
rpc:       db files


netgroup:  nis
```

Step 6: Enable auto-create home directory on login by adding the following to **/etc/pam.d/common-session** by the following command

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

Step 7: Edit **/etc/pam.d/common-password** and add the ldap entries.

```
root@gateway:~# vi /etc/pam.d/common-password

#look for the lines starting with the password and add the line below to enable authentication via LDAP.

password [success=1 user_unknown=ignore default=die] pam_ldap.so use_authok try_first_pass
```

Step 8: Restart nscd service

```
root@gateway:~# service nscd restart
```

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

Step 9: Now run the **id/finger** command and see whether you can get AD user details

```
root@gateway:~# 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.
:~# 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@gateway:~# 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:: AQUAAAAAAAAUVAAAAmhs/bgMv2mlWATm4VQAAAA==
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=

Troubleshooting Steps:

ERROR: [Could not authenticate with any LDAP server](#)

ERROR: [Could not bind to any LDAP server: 80090308](#)

[Error log file and configuration file to troubleshoot.](#)

Related Articles:

[How do I configure Ezeelogin to authenticate using Windows_AD\(Pam-LDAP\) in CentOS](#)

[Assigning user groups for LDAP users?](#)

[Can we map the existing user group in LDAP to ezeelogin as the ezeelogin user group?](#)

Online URL: https://www.ezeelogin.com/kb/article/configure-ezeelogin-to-authenticate-using-windows_ad-40;pam-ldap-41;-in-ubuntu-187.html