

# Authentication of Ezeelogin gateway users using Public keys fetched from Open LDAP server

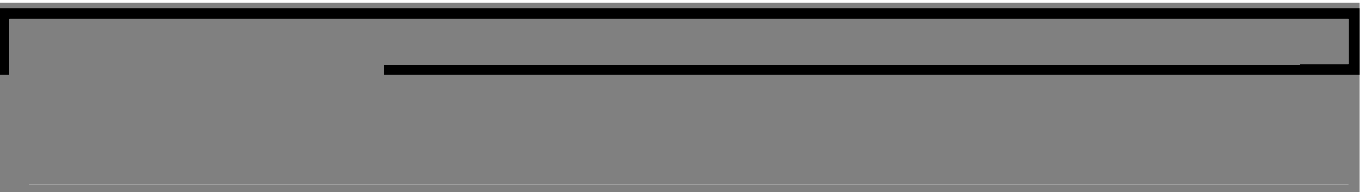
400 Vishnupriya May 3, 2024 [General](#) 2117

Integrate SSH Public key authentication on Ezeelogin gateway server by exporting the Public Key from Openldap server for a centralized ssh key based authentication

1. First you need to update Openldap LDAP server with a schema to add the sshPubicKey attribute for users:

```
__root@ldapservers:~__ cat << EOL >~/openssh-lpk.ldif
dn: cn=openssh-lpk,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: openssh-lpk
olcAttributeTypes: ( 1.3.6.1.4.1.24552.500.1.1.1.13 NAME
'sshPublicKey'
DESC 'MANDATORY: OpenSSH Public key'
EQUALITY octetStringMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
olcObjectClasses: ( 1.3.6.1.4.1.24552.500.1.1.2.0 NAME
'ldapPublicKey' SUP top AUXILIARY
DESC 'MANDATORY: OpenSSH LPK objectclass'
MAY ( sshPublicKey $ uid )
)
EOL
```

2. You need to run the following command to add ldif :



3. Login to the GUI of your ldap server. Create a user with the “Generic: User Account” template. Select the user "jake" as shown below

The screenshot displays the phpLDAPadmin web interface. On the left, a sidebar titled "My LDAP Server" shows a tree structure of the LDAP directory. A red arrow points to the entry "cn=jake j" under the "ou=people (7)" container. The main panel on the right shows the details for the selected user "cn=jake j". At the top, it indicates the server is "My LDAP Server" and the distinguished name is "cn=jake j,ou=people,dc=example,dc=com". Below this, there are several action buttons: Refresh, Switch Template, Copy or move this entry, Rename, Create a child entry, Show internal attributes, Export, Delete this entry, Compare with another entry, and Add new attribute. Two hints are provided: "Hint: To delete an attribute, empty the text field and click save." and "Hint: To view the schema for an attribute, click the attribute name." The "cn" attribute is shown with the value "jake j" and options to "(add value)" or "(rename)". The "gidNumber" attribute is shown with the value "500" and a link to "ezeelogin ()".

4. Go to the “objectClass” attribute section, click “add value”, and choose the “ldapPublicKey” attribute.

**objectClass** required


i

inetOrgPerson

(structural)

i


i

 [\(add value\)](#)

Current list of 3 values for attribute **objectClass**:

inetOrgPerson  
posixAccount  
top

Enter the value(s) you would like to add:



labeledURIObject

**IdapPublicKey**

olcConfig

olcFrontendConfig

organizationalPerson

person

pkiCA

pkiUser

qualityLabelledData

shadowAccount

simpleSecurityObject

strongAuthenticationUser

subschema

uidObject

userSecurityInformation

[Add new ObjectClass](#)

5. After you submit, go back to the user edit page, click “Add new attribute” on the top part, and choose “sshPublicKey”, paste the public key into the text area, and finally click “Update Object”.

cn=jake j

Server: My LDAP Server Distinguished Name: cn=jake j,ou=people,dc=example,dc=com Template: Default

Refresh

Switch Template

Copy or move this entry

Rename

Create a child entry

Hint: To delete an attribute, empty the text field and click save.

Hint: To view the schema for an attribute, click the attribute name.

Show internal attributes

Export

Delete this entry

Compare with another entry

Add new attribute

cn

required, rdn

jake j

(add value)

(rename)

gidNumber

required

500

ezeelogin ()

Server: My LDAP Server Distinguished Name: cn=jake j,ou=people,dc=example,dc=com Template: Default

Refresh

Switch Template

Copy or move this entry

Rename

Create a child entry

Hint: To delete an attribute, empty the text field and click save.

Hint: To view the schema for an attribute, click the attribute name.

postalAddress

postalCode

preferredDeliveryMethod

preferredLanguage

registeredAddress

roomNumber

secretary

seeAlso

sshPublicKey

st

street

Telephone

teletexTerminalIdentifier

telexNumber

title

userCertificate

userPKCS12

userSMIMECertificate

x121Address

x500UniqueIdentifier

sshPublicKey

Add Attribute

cn

required, rdn

jake j

(add value)

(rename)

gidNumber

required

500

ezeelogin ()

(add value)

**sn**

required

j

(add value)

**sshPublicKey**

ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQGCn/BFoZ06UnCP  
hJxG27PSj6IRdRho8hVib6EYNVtSnt21aKmfPR80J7v  
u2WJOMHXQVuNP0uw1HoGPdv0EsfdFpPX0Nnt2SWfyKp  
ngVQcJoTV94e6ZA45in+CtX+3ARngFd1jmjQmDT8ZK6

(add value)

**uidNumber**

required

1011

**User Name**

alias, required

jake

(add value)

Update Object

6. Create a script on your Ezeelogin server that queries LDAP for a user's public key under /usr/local/fetchsshkeys

## TROUBLESHOOTING

Ensure that the public key is fetched for the user jake from the Openldap server by running the following command:

```
root@jumpserver:~ ldapsearch -x '(&(objectClass=ldapPublicKey)(uid="jake j"))' 'sshPublicKey' | sed -n '/^/{H;d};sshPublicKey:/x;$g;s/n */g;s/sshPublicKey: //gp'
```

Install the script on your system and make it executable by running: `chmod 0500 /usr/local/fetchsshkeys`

7. Make sure your `/etc/ldap/ldap.conf` or `/etc/openldap/ldap.conf` file is configured to point to the right Open LDAP server. For example:

```
BASE dc=example,dc=com

URI ldap:// ldap.example.com
```

8. Add the following lines on the gateway server to your `sshd_config` file to point to the script

9. Now, the user "jake" will be authenticated using the public key fetched from the Open ldap server

The screenshot displays the Ezeelogin web interface. On the left is a sidebar with navigation links: Servers, Web Portals, Users, Access Control, Settings, Cluster, Command Guard, and Account. The main area shows a search filter for 'User: admin' and a date range from '2023-01-13 10:57' to '2023-01-15 10:57'. Below this is a table of 'Server Activity Logs'.

Username	Server Name	Status	IP Address	Login Time	Logout Time	Input Idle Time	Output Idle Time	Actions
admin	debian	FAILED: Auth failed	127.0.0.1	2023-01-13 12:49:29	2023-01-13 12:49:34	0s	0s	
admin	debian	FAILED: Auth failed	127.0.0.1	2023-01-13 15:31:53	2023-01-13 15:31:55	0s	0s	
admin	debian	FAILED: Auth failed	127.0.0.1	2023-01-13 15:33:30	2023-01-13 15:33:35	0s	0s	
admin	debian	FAILED: Auth failed	127.0.0.1	2023-01-13 15:33:45	2023-01-13 15:33:49	0s	0s	
admin	debian	FAILED: Auth failed	127.0.0.1	2023-01-13 15:33:54	2023-01-13 15:33:58	0s	0s	
admin	ubuntu	FAILED: Could not connect	127.0.0.1	2023-01-13 12:49:17	2023-01-13 12:49:27	0s	0s	
admin	ubuntu	SUCCESS	127.0.0.1	2023-01-13 12:59:26	2023-01-13 12:59:53	26s	26s	
admin	ubuntu	SUCCESS: done	127.0.0.1	2023-01-13 15:32:05	2023-01-13 15:32:11	0s	0s	
admin	ubuntu	SUCCESS	127.0.0.1	2023-01-14 10:56:33	2023-01-14 10:56:35	0s	0s	
admin	eman.tsoh server	FAILED: Auth failed	127.0.0.1	2023-01-13 12:53:01	2023-01-13 12:53:03	0s	0s	

At the bottom of the interface, there is a link to 'serveractivity.csv' and a 'Show all' button.

Make sure that you have installed ldapsearch on your Ezeelogin server.

## Related Articles

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

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

Online URL:

<https://www.ezeelogin.com/kb/article/authentication-of-ezeelogin-gateway-users-using-public-keys-fetched-from-open-ldap-server-400.html>