

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

400 Vishnupriya July 31, 2024 [General](#) 2834

## Integrating SSH Public Key Authentication with OpenLDAP on Ezeelogin

**Overview:** This article describes how to integrate SSH public key authentication on an Ezeelogin gateway server by exporting the public key from an OpenLDAP server. It includes steps for updating the LDAP schema, adding user attributes, creating a fetching script, and configuring SSH to use the public keys retrieved from LDAP.

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

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

```
root@ldapservr:~# 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

```

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

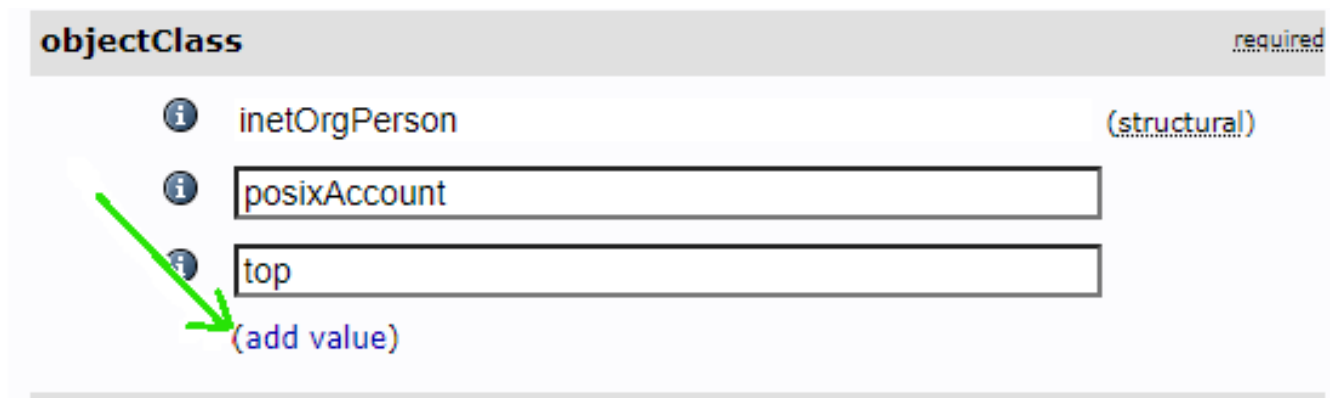


**Step 3.** Login to the GUI of your ldap server. Create a user with the “Generic: User Account” template. Select the user "jake" as shown below




The screenshot shows the phpLDAPadmin web interface. On the left, a tree view of the LDAP directory is shown, with 'cn=jake j' highlighted under the 'ou=people' container. A green arrow points to this entry. The main panel displays the details for 'cn=jake j', including the server name 'My LDAP Server', the distinguished name 'cn=jake j,ou=people,dc=example,dc=com', and the template 'Default'. Below this, there are two attribute sections: 'cn' with the value 'jake j' and 'gidNumber' with the value '500'. The 'cn' attribute has a 'required: rdn' label, and the 'gidNumber' attribute has a 'required' label. There are also links for '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'. A hint at the bottom says: 'Hint: To delete an attribute, empty the text field and click save. Hint: To view the schema for an attribute, click the attribute name.'

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

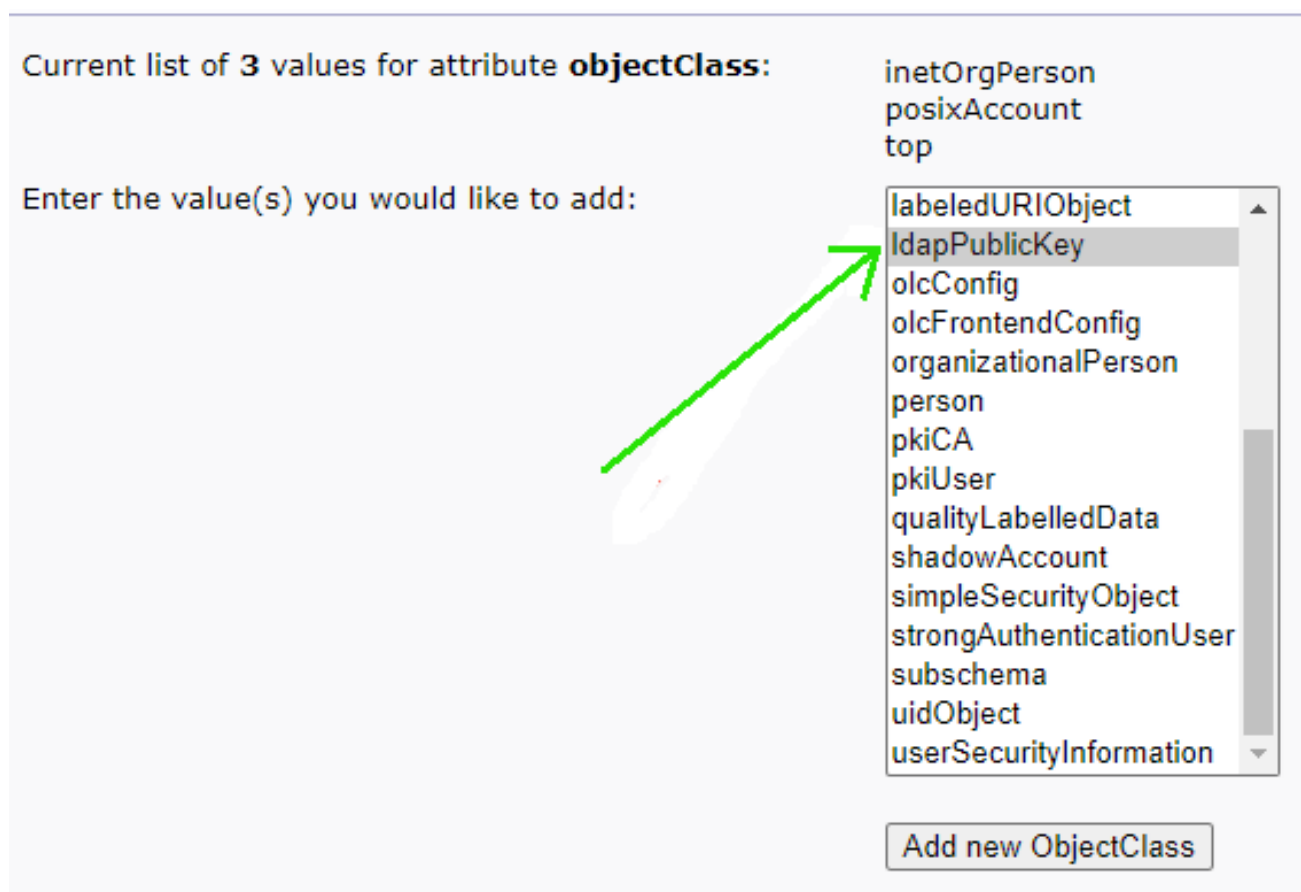
“ldapPublicKey” attribute.



**objectClass** required

-  inetOrgPerson (structural)
-  posixAccount
-  top

[\(add value\)](#)



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

- inetOrgPerson
- posixAccount
- top

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

- labeledURIObject
- ldapPublicKey**
- olcConfig
- olcFrontendConfig
- organizationalPerson
- person
- pkiCA
- pkiUser
- qualityLabelledData
- shadowAccount
- simpleSecurityObject
- strongAuthenticationUser
- subschema
- uidObject
- userSecurityInformation

[Add new ObjectClass](#)

**Step 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

jake j

(add value)

(rename)

gidNumber

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.

sshPublicKey

Add Attribute

sshPublicKey

cn

jake j

(add value)

(rename)

gidNumber

500

(add value)

**sn** required

j

(add value)

**sshPublicKey**

ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQgCn/BFoZ06UnCP  
hJxG27PSj6IRdRho8hVib6EYNVtSnt21aKmfPR80J7v  
u2WJOMHXQVuNP0uw1HoGPdv0EsfFpPX0NnT2SWfyKp  
ngVQcJoTV94e6ZA45in+CtX+3ARngFd1jmjQmDT8ZK6

(add value)

**uidNumber** required

1011

**User Name** alias, required

jake

(add value)

Update Object

**Step 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'
```

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

**Step 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
```

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

```
AuthorizedKeysCommand /usr/local/fetchsshkeys
```

```
AuthorizedKeysCommandUser root
```

**Step 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 menus: Servers, Web Portals, Users, Access Control, Settings, Cluster, Command Guard, and Account. The main area is titled 'Server Activity Logs' and includes a search bar with fields for User (set to 'admin'), Servers (set to 'All'), From (2023-01-13 10:57), and To (2023-01-15 10:57). Below the search bar is a table of activity logs. The table has columns: Username, Server Name, Status, IP Address, Login Time, Logout Time, Input Idle Time, Output Idle Time, and Actions. The logs show several failed authentication attempts for the 'admin' user on 'debian' servers and successful logins for 'admin' on 'ubuntu' servers.

| 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               |         |

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?](#)

[How to use the LDAP password as the security code on user login in SSH?](#)

Online URL:

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