

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

400 Vishnupriya July 31, 2024 [General](#) 2717

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@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
```

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 interface. On the left, a tree view of the LDAP directory is visible, with 'cn=jake j' highlighted by a green arrow. 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 several action buttons such as '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'. At the bottom, there are input fields for 'cn' (containing 'jake j') and 'gidNumber' (containing '500').

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

“ldapPublicKey” attribute.

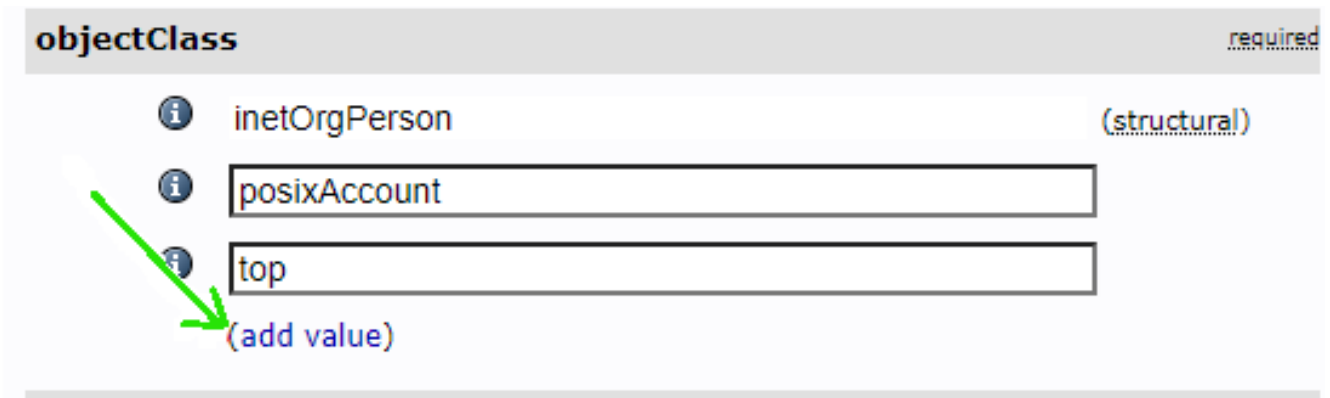
objectClass required

inetOrgPerson (structural)

posixAccount

top

[\(add value\)](#)

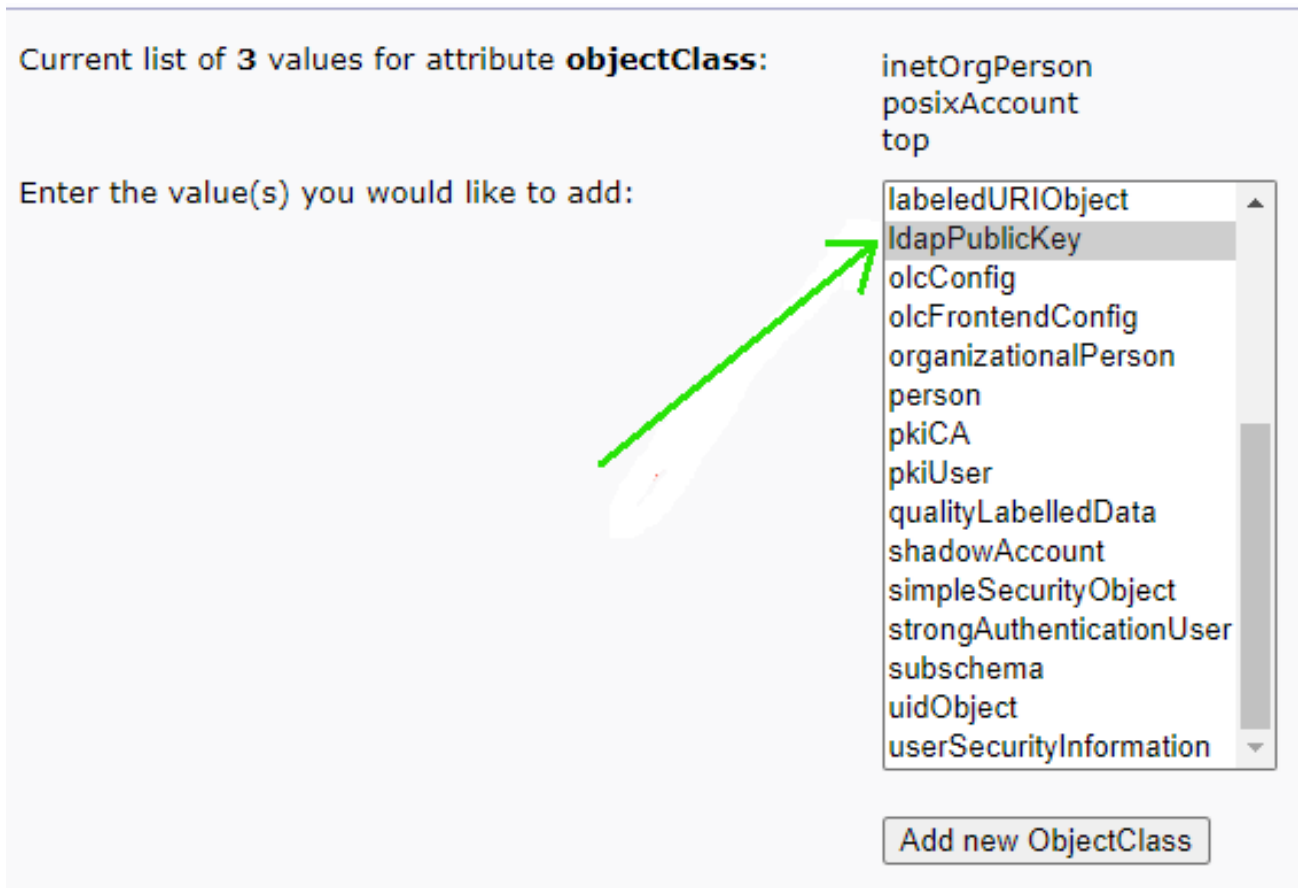


Current list of 3 values for attribute **objectClass**:

- 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



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 required, rdn

jake j

(add value)

(rename)

gidNumber required

500

ezeelogin ()

- postalAddress
- postalCode
- preferredDeliveryMethod
- preferredLanguage
- registeredAddress
- roomNumber
- secretary
- seeAlso
- sshPublicKey
- st
- street
- Telephone
- teletexTerminalIdentifier
- telexNumber
- title
- userCertificate
- userPKCS12
- userSMIMECertificate
- x121Address
- x500UniqueIdentifier
- sshPublicKey

- 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.

Add Attribute

cn required, rdn

jake j

(add value)

(rename)

gidNumber required

500

(add value)

sn required

(add value)

sshPublicKey

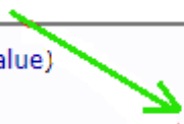
```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGcCn/BFoZ06UnCP
hJxG27PSj6IRdRho8hVib6EYNNvtSnt21aKmfPR80J7v
u2WJOMHXQVuNP0uw1HoGPdv0EsfdFpPX0NnT2SWfyKp
ngVQcJoTV94e6ZA45in+CtX+3ARngFd1jmjQmDT8ZK6
```

(add value)

uidNumber required

User Name alias, required

(add value)



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
```

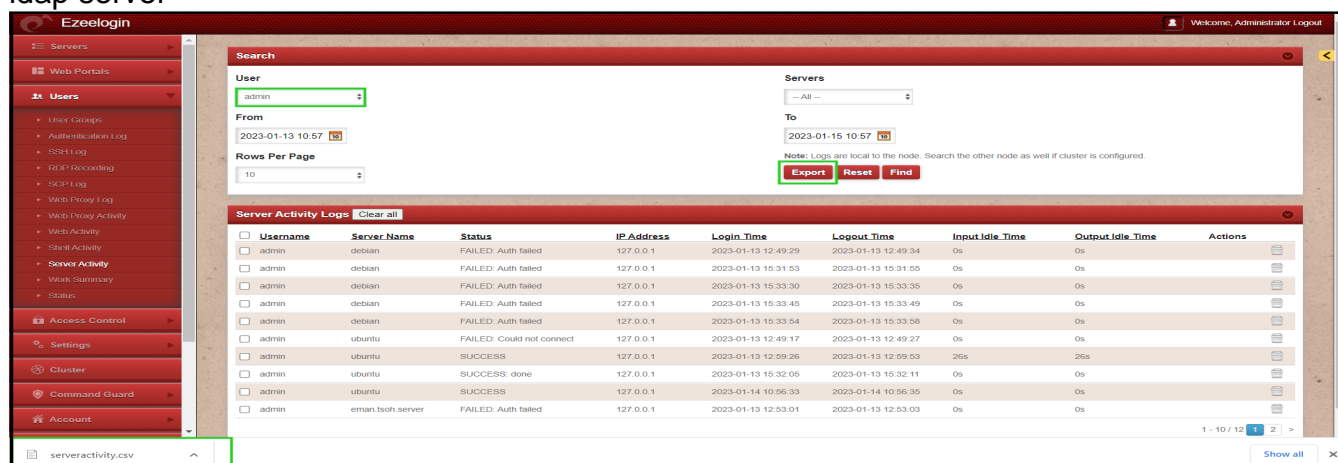
```
URI ldap:// ldap.example.com
```

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



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>