# Using LDAP as an SSH Public Key Store

## Create a Custom Schema

In the /opt/symas/etc/openldap directory create a new directory called custom-schema. This is necessary so the custom schema is not lost during software updates.

```
sudo -s

cd /opt/symas/etc/openldap

mkdir custom-schema
```

In the custom-schema directory create a file called openssh-lpk.schema and insert the following:

```
vi custom-schema/openssh-lpk.schema

attributetype: ( 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
    )
objectClass: ( 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 )
    )
```

## Update Slapd.conf

Add the custom schema to slapd.conf

```
vi custom-schema/openssh-lpk.schema

# Schema files. Note that not all of these schemas co-exist peacefully.
# Use only those you need and leave the rest commented out.
Include      /opt/symas/etc/openldap/schema/core.schema
Include      /opt/symas/etc/openldap/schema/cosine.schema
Include      /opt/symas/etc/openldap/schema/inetorgperson.schema
Include      /opt/symas/etc/openldap/custom-schema/openssh-lpk.schema
```

Restart slapd

```
service solserver restart
```

## Update Database

Add the ldapPublicKey objectClass to each user and then add the sshPublicKey attribute with the public key as the value for each user. This can be accomplished from the command line or by using an ldif.

```
ldapadd -x -H ldap://<producer's FQDN> -D <rootDN> -w <rootPW>
dn: cn=example user,ou=users,dc=example,dc=com
objectClass: ldapPublicKey
```

```
sshPublicKey: ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDpYZmRbgqEDhh+qUA+7LW960sVNjMdsJuEVfa8sBVO
1xGUwxy2kjweUKgLkc49GXQ6cJndwCHYhXzHiFuBalc4KdQTwgpIiJtxAH0BsBes3USWecVB
fPFHtr7K5PGKc+Dd/E0aH+7VdNG8abnRXUXroyd6DoUaIkN3rNq0aejq2pN0iuvfV65hAQLf
Rea3/uhMEFPSZmzcMdGGbd3Kq04X14BOxMpjICgtPTGByMrYjX2JzGKuJsHik8IwJxW8bga3
gRaPCY4eIyRA2IxwNYwJLP5ENvwz1rztBIMjTcasnk8N7Hy++nt8cbdNe1ZiLTLw3H6aHKns
MfAk1DLV/oZT example.user@example.com
```

## Create LDAP Query Script

Create a script containing an ldapsearch that will output the public keys for any user. You may need to tweak this command to get the desired result. (Note: Word wrapping is affecting the `result=` and `attrLine=` lines.)

```
vi /opt/symas/ssh/openssh-lpk
#!/bin/bash
set -eou pipefail
IFS=$'\n\t'

result=$(ldapsearch          '(&(objectClass=posixAccount)(uid='"$1"'))'
'sshPublicKey')
attrLine=$(echo "$result" | sed -n '/^ /{H;d};/sshPublicKey:/x;$g;s/\n
*//g;/sshPublicKey:/p')

if [[ "$attrLine" == sshPublicKey::* ]]; then
  echo "$attrLine" | sed 's/sshPublicKey:: //' | base64 -d
elif [[ "$attrLine" == sshPublicKey:* ]]; then
  echo "$attrLine" | sed 's/sshPublicKey: //'
else
  exit 1
fi
```

## Update SSH_Config

Add the following to /etc/ssh/sshd_config

```
vi /etc/ssh/sshd_config
AuthorizedKeysCommand /opt/symas/ssh/openssh-lpk
AuthorizedKeysCommandUser nobody
```

Restart the ssh service.

```
service ssh restart
```

Test connectivity.