

# configure jump server to use SSL for MySQL

206 Manu Chacko October 11, 2024 [Tweaks & Configuration](#) 10389

## How to configure Ezeelogin jump server to use SSL for MySQL database connections on centos?

**Overview:** This article explains configuring SSL for MySQL on the Ezeelogin jump server using CentOS 7 and MySQL 5.5. It includes checking SSL status, generating certificates, updating MySQL and Ezeelogin configurations, and verifying the connection to ensure secure database access.

### Mysql-SSL setup on Centos 7, Mysql server 5.5 version

#### Step 1. Check the Current SSL/TLS Status

Log into a MySQL session

```
root@gateway:~# mysql -u root -p -h 127.0.0.1
```

Show the state of the SSL/TLS variables by typing:

```
mysql> SHOW VARIABLES LIKE '%ssl%';
```

Output

```
+-----+-----+
| Variable_name | Value |
+-----+-----+
| have_openssl | DISABLED |
| have_ssl | DISABLED |
| ssl_ca | |
| ssl_capath | |
| ssl_cert | |
| ssl_cipher | |
| ssl_crl | |
| ssl_crlpath | |
| ssl_key | |
+-----+-----+
9 rows in set (0.01 sec)
```

The **have\_openssl** and **have\_ssl variables** are both marked as DISABLED. This means that SSL functionality has been compiled into the server, but that it is not yet enabled.

## Step 2. Generate SSL/TLS Certificates and Keys

Create a clean environment

```
root@gateway:~# mkdir /etc/certs && cd /etc/certs
```

Create the CA certificate

```
root@gateway:~# openssl genrsa 2048 > ca-key.pem
```

```
root@gateway:~# openssl req -new -x509 -nodes -days 3600  
-key ca-key.pem -out ca.pem
```

Create the server certificate, remove passphrase, and sign it

```
root@gateway:~# openssl req -newkey rsa:2048 -days 3600  
-nodes -keyout server-key.pem -out server-req.pem
```

```
root@gateway:~# openssl rsa -in server-key.pem -out server-key.pem
```

```
root@gateway:~# openssl x509 -req -in server-req.pem -days 3600  
-CA ca.pem -CAkey ca-key.pem -set_serial 01 -out server-cert.pem
```

Create the client certificate, remove passphrase, and sign it

```
root@gateway:~# openssl req -newkey rsa:2048 -days 3600  
-nodes -keyout client-key.pem -out client-req.pem  
  
root@gateway:~# openssl rsa -in client-key.pem -out client-key.pem  
  
root@gateway:~# openssl x509 -req -in client-req.pem -days 3600  
-CA ca.pem -CAkey ca-key.pem -set_serial 01 -out client-cert.pem
```

After generating the certificates, verify them:

```
root@gateway:~# openssl verify -CAfile ca.pem server-cert.pem client-cert.pem  
  
output  
  
server-cert.pem: OK  
client-cert.pem: Ok
```

## Enable SSL for MySQL

We have to edit the MySQL configuration file `'/etc/my.cnf'`

In the `'[mysqld]'` section, paste the configuration below.

```
root@gateway:~# vi /etc/my.cnf  
  
ssl-ca=/etc/certs/ca.pem  
  
ssl-cert=/etc/certs/server-cert.pem  
  
ssl-key=/etc/certs/server-key.pem
```

Restart the MySQL service

```
root@gateway:~# systemctl restart mysql
```

After restarting, open up a new MySQL session using the same command as before.

```
root@gateway:~# mysql -u root -p -h 127.0.0.1
```

Check state of the SSL/TLS variables by typing:

```
mysql> SHOW VARIABLES LIKE '%ssl%';
```

Output

```
+-----+-----+
| Variable_name | Value |
+-----+-----+
| have_openssl | YES |
| have_ssl | YES |
| ssl_ca | Ca.pem |
| ssl_capath | |
| ssl_cert | server-cert.pem |
| ssl_cipher | |
| ssl_crl | |
| ssl_crlpath | |
| ssl_key | server-key.pem |
+-----+-----+
9 rows in set (0.01 sec)
```

The **have\_openssl** and **have\_ssl** variables read **"YES"** instead of **"DISABLED"** this time.

Check the connection details by the following command :

```
root@gateway:~# mysql -u ezlogin_database_username -p -h hostname or ip --ssl-ca=/etc/certs/ca.pem  
--ssl-cert=/etc/certs/client-cert.pem --ssl-key=/etc/certs/client-key.pem
```

example :

```
root@gateway:~# mysql -u ezlogin_xxxx -p -h 10.11.1.11 --ssl-ca=/etc/certs/ca.pem --ssl-  
cert=/etc/certs/client-cert.pem --ssl-key=/etc/certs/client-key.pem
```

In Case the certificate verification has been failed, refer [SSL certificate failed with MYSQL SSL](#)

```
mysql> s
```

```
-----
```

```
...
```

```
SSL: Cipher in use is DHE-RSA-AES256-SHA
```

```
...
```

```
Connection: 127.0.0.1 via TCP/IP
```

```
...
```

SSL cipher is displayed, indicating that SSL is being used to secure our connection.

### Step 3. Configure ezeelogin jump server to use SSL for Mysql 5.5

Add `mysql_ssl_key`, `mysql_ssl_cert`, `mysql_ssl_ca` to **`/usr/local/etc/ezlogin/ez.conf`**

Edit the **`/usr/local/etc/ezlogin/ez.conf`** file add the following

```
root@gateway:~# vi /usr/local/etc/ezlogin/ez.conf
```

```
#Add the following
```

```
system_folder /var/www/ezlogin/  
force_https no  
uri_path /ezlogin/  
db_host 10.10.1.11  
db_port 3306  
db_name ezlogin_qzms  
db_user ezlogin_edcjwz  
db_pass dsH)$s5xAE[QgFms  
db_prefix aqvo_  
cookie_encryption_key ASvs8^pnu^^X9  
cookie_name lcrfs  
cookie_path /ezlogin/  
www_folder /var/www/html/ezlogin/  
admin_user admin  
mysql_encrypt yes  
mysql_ssl_key /etc/certs/client-key.pem  
mysql_ssl_cert /etc/certs/client-cert.pem  
mysql_ssl_ca /etc/certs/ca.pem  
mysql_ssl_cpath /etc/certs/  
mysql_ssl_verify no
```

**Note:** Make sure that you have changed db\_port to 3306 & db\_host to IP Address of your host

**Step 4.** Change the bind address & allow the Ezeelogin jump server user to access the database.

Edit the /etc/mysql/mysql.conf.d/mysqld.cnf & change bind-address

```
root@gateway:~# vi /etc/mysql/mysql.conf.d/mysqld.cnf
```

Change bind-address to host ip(server ip)

```
bind-address x.x.x.x (Host ip)
```

Restart the MySQL service

```
root@gateway:~# systemctl restart mariadb
```

you can find out Ezeelogin jump server **dbname** and Ezeelogin Mysql **username** from the **ez.conf** file

```
root@gateway:~# cat /usr/local/etc/ezlogin/ez.conf
```

```
system_folder /var/www/ezlogin/
```

```
force_https no
```

```
uri_path /ezlogin/
```

```
db_host 10.10.1.11
```

```
db_port 3306
```

```
db_name ezlogin_qzms
```

```
db_user ezlogin_edcjwz
```

```
db_pass dsH)$s5xAE[QgFms
```

```
db_prefix aqvo_
```

```
cookie_encryption_key ASvs8^pnu^^X9
```

```
cookie_name lcrfs
```

```
cookie_path /ezlogin/  
www_folder /var/www/html/ezlogin/  
admin_user admin  
mysql_encrypt yes  
mysql_ssl_key /etc/certs/client-key.pem  
mysql_ssl_cert /etc/certs/client-cert.pem  
mysql_ssl_ca /etc/certs/ca.pem  
mysql_ssl_capath /etc/certs/  
mysql_ssl_verify no
```

## Login to mysql

```
root@gateway:~# mysql -u root -p  
  
[Enter password]  
  
mysql> grant all on ezlogin_databasename.* to 'mysql_username'@'%' identified by 'password';  
  
example : mysql > grant all on ezlogin_xxx.* to 'ezlogin_xxxx'@'%' identified by  
'dsH)$s5xAE[QgFmfsfgg';  
  
mysql > flush privileges;  
  
mysql > exit
```

## Check if you can log in to MySQL using Ezeelogin databases

```
root@gateway:~# mysql -u ezeelogin_databasename_username -h 10.11.1.11 -p  
  
Enter Password:
```



```
mysql >
```

```
mysql > exit
```

**Note:** If you have any difficulties please [contact support](#)

### **Related Articles:**

[Configure Ezeelogin to use SSL for MySQL version 8 on Ubuntu](#)

[Configure ssh jump server to use SSL for Mariadb](#)

[Increase script execution time in Ubuntu and CentOS](#)

[configure jump server to use SSL for MySQL server 5.7 version](#)

[Basic MySQL commands for troubleshooting database related issues in Ezeelogin](#)

[Unable to access GUI while using MySQL SSL](#)

[failed to connect to database: Error: TLS/SSL error: Permission denied](#)

Online URL: <https://www.ezeelogin.com/kb/article/configure-jump-server-to-use-ssl-for-mysql-206.html>