onbon仰邦科技

User Manual

YQ software authentication and encryption

Version：V1.0　Release Date：2020.4.17

CATALOG

Y series controller supports authentication and encryption function, as to encrypt for resource.

Create Certificate

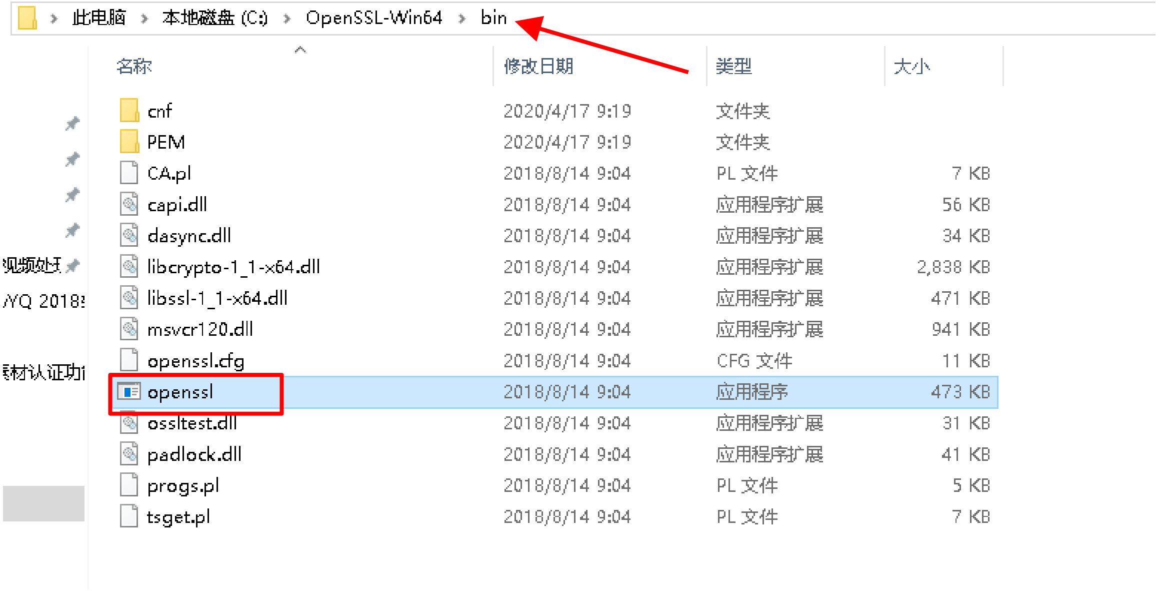
1. Install software

Create certificate by OpenSSL.

Firstly, download OpenSSL tool according to your PC system, here is the link：
https://oomake.com/download/openssl

For example, for windows 64: (install package is : Win64OpenSSL-1_0_2p)

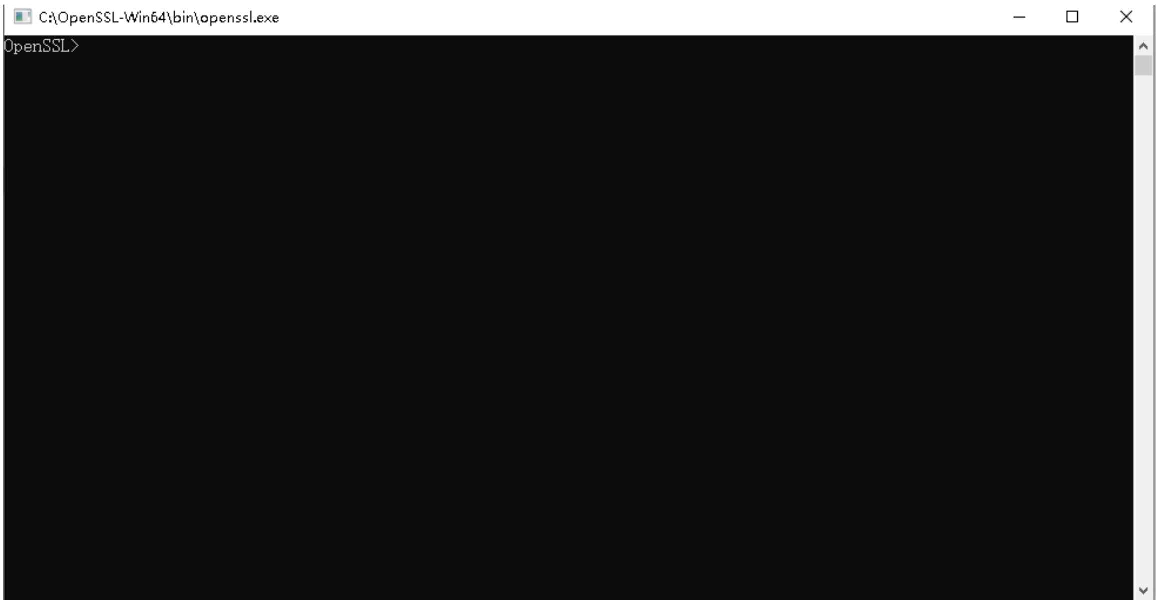
After install, open the file, enter into bin, find OpenSSL application program)



此电脑 › 本地磁盘 (C:) › OpenSSL-Win64 › bin

名称	修改日期	类型	大小
cnf	2020/4/17 9:19	文件夹	
PEM	2020/4/17 9:19	文件夹	
CA.pl	2018/8/14 9:04	PL 文件	7 KB
capi.dll	2018/8/14 9:04	应用程序扩展	56 KB
dasync.dll	2018/8/14 9:04	应用程序扩展	34 KB
libcrypto-1_1-x64.dll	2018/8/14 9:04	应用程序扩展	2,838 KB
libssl-1_1-x64.dll	2018/8/14 9:04	应用程序扩展	471 KB
msvcr120.dll	2018/8/14 9:04	应用程序扩展	941 KB
openssl.cfg	2018/8/14 9:04	CFG 文件	11 KB
openssl	2018/8/14 9:04	应用程序	473 KB
ossltest.dll	2018/8/14 9:04	应用程序扩展	31 KB
padlock.dll	2018/8/14 9:04	应用程序扩展	41 KB
progs.pl	2018/8/14 9:04	PL 文件	5 KB
tsget.pl	2018/8/14 9:04	PL 文件	7 KB

Double click "openssl", enter into openssl command window, input openssl command, as below:

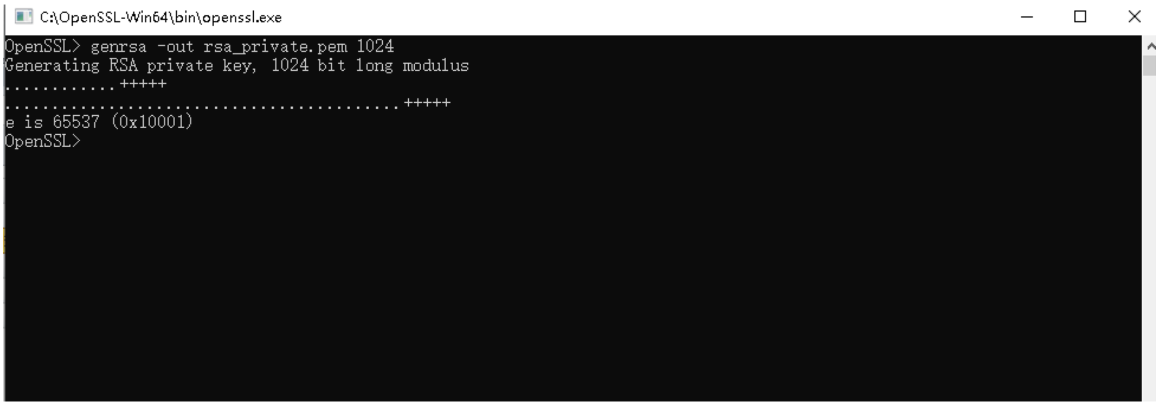


C:\OpenSSL-Win64\bin\openssl.exe

```
OpenSSL>
```

2. Create private key:

genrsa -out rsa_private.pem 1024



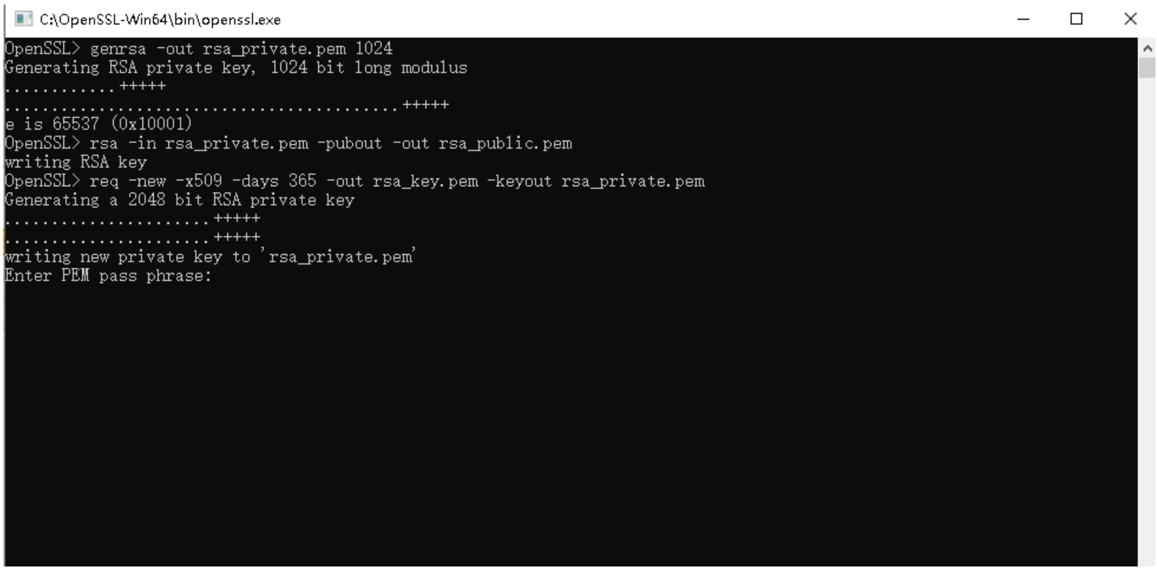
```
OpenSSL> genrsa -out rsa_private.pem 1024
Generating RSA private key, 1024 bit long modulus
...........+++++
..........................................+++++
e is 65537 (0x10001)
OpenSSL>
```

3. Create public key and certificate:

rsa -in rsa_private.pem -pubout -out rsa_public.pem

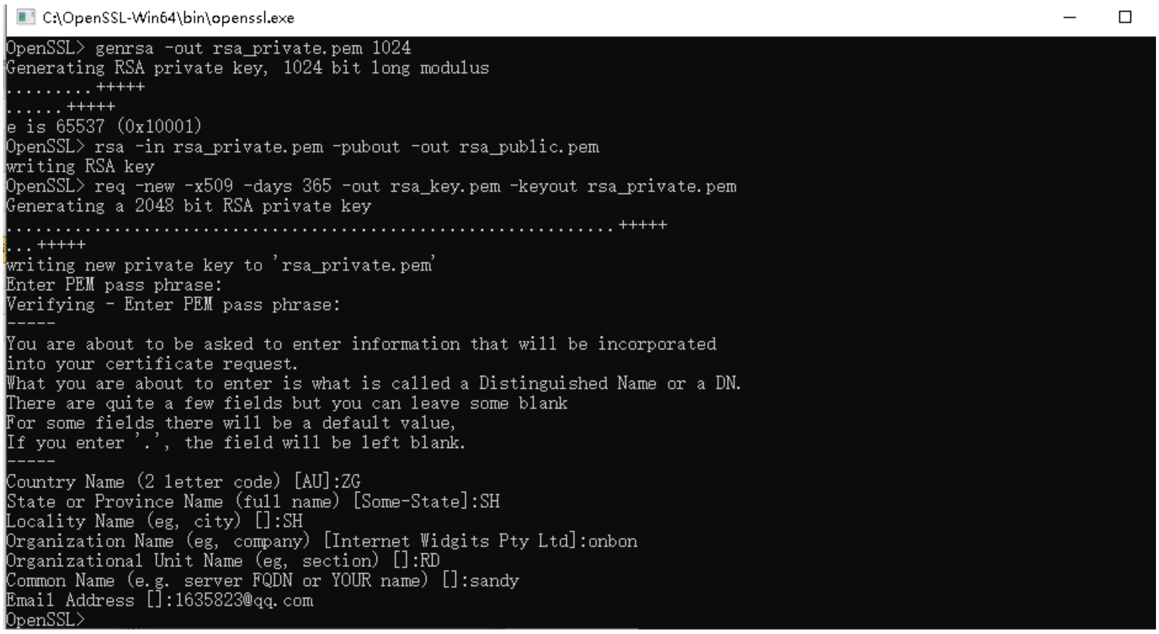
req -new -x509 -days 365 -out rsa_key.pem -keyout rsa_private.pem

After input command, you need to input passwords, first time, input numbers passwords at least 6 digits, then click “Enter” , second, input passwords again, click “Enter” .



```
OpenSSL> genrsa -out rsa_private.pem 1024
Generating RSA private key, 1024 bit long modulus
...........+++++
..........................................+++++
e is 65537 (0x10001)
OpenSSL> rsa -in rsa_private.pem -pubout -out rsa_public.pem
writing RSA key
OpenSSL> req -new -x509 -days 365 -out rsa_key.pem -keyout rsa_private.pem
Generating a 2048 bit RSA private key
.....................+++++
.....................+++++
writing new private key to 'rsa_private.pem'
Enter PEM pass phrase:
```

And then input country name(two digits), province, city, company, department, name, email.



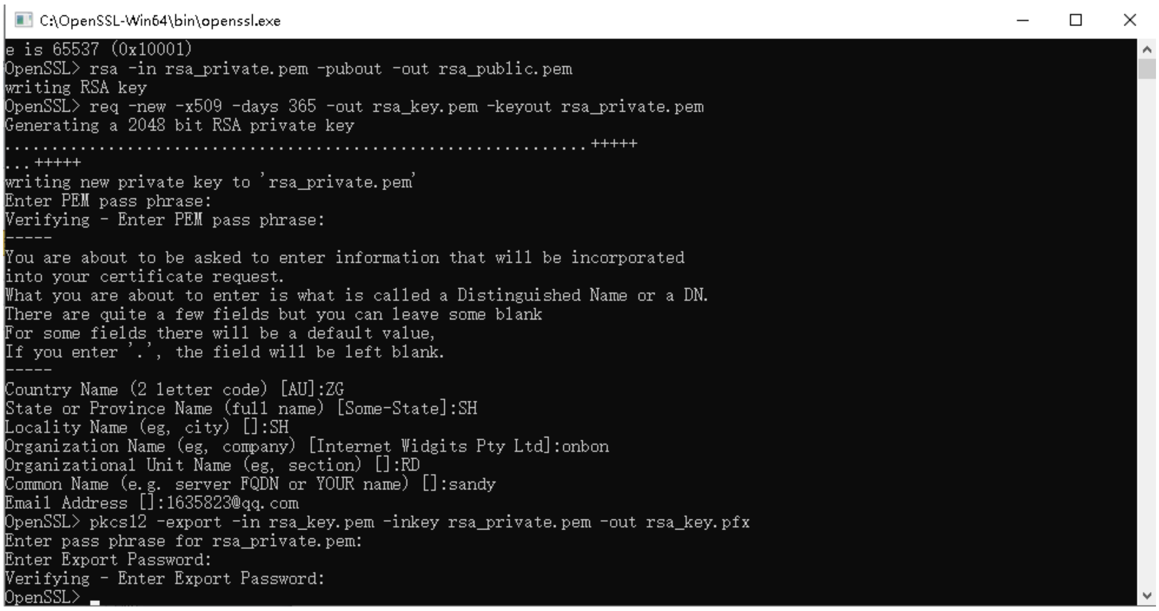
C:\OpenSSL-Win64\bin\openssl.exe

```
OpenSSL> genrsa -out rsa_private.pem 1024
Generating RSA private key, 1024 bit long modulus
.........+++++
......+++++
e is 65537 (0x10001)
OpenSSL> rsa -in rsa_private.pem -pubout -out rsa_public.pem
writing RSA key
OpenSSL> req -new -x509 -days 365 -out rsa_key.pem -keyout rsa_private.pem
Generating a 2048 bit RSA private key
.............................................................+++++
...+++++
writing new private key to 'rsa_private.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ZG
State or Province Name (full name) [Some-State]:SH
Locality Name (eg, city) []:SH
Organization Name (eg, company) [Internet Widgits Pty Ltd]:onbon
Organizational Unit Name (eg, section) []:RD
Common Name (e.g. server FQDN or YOUR name) []:sandy
Email Address []:1635823@qq.com
OpenSSL>
```

4. **Export public key:**

pkcs12 -export -in rsa_key.pem -inkey rsa_private.pem -out rsa_key.pfx

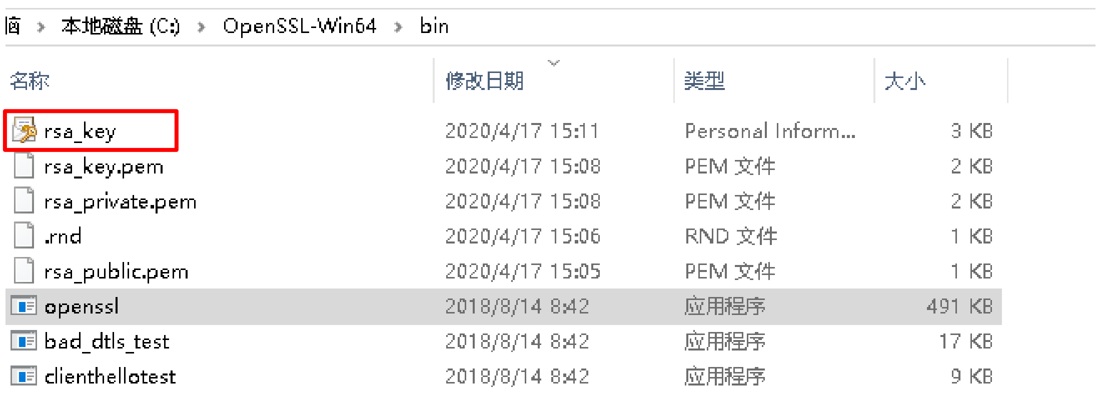
Need to input certificate password when you export (same with the second time passwords), and then need to input pfx certificate password (same with the second time passwords).



C:\OpenSSL-Win64\bin\openssl.exe

```
e is 65537 (0x10001)
OpenSSL> rsa -in rsa_private.pem -pubout -out rsa_public.pem
writing RSA key
OpenSSL> req -new -x509 -days 365 -out rsa_key.pem -keyout rsa_private.pem
Generating a 2048 bit RSA private key
.............................................................+++++
...+++++
writing new private key to 'rsa_private.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ZG
State or Province Name (full name) [Some-State]:SH
Locality Name (eg, city) []:SH
Organization Name (eg, company) [Internet Widgits Pty Ltd]:onbon
Organizational Unit Name (eg, section) []:RD
Common Name (e.g. server FQDN or YOUR name) []:sandy
Email Address []:1635823@qq.com
OpenSSL> pkcs12 -export -in rsa_key.pem -inkey rsa_private.pem -out rsa_key.pfx
Enter pass phrase for rsa_private.pem:
Enter Export Password:
Verifying - Enter Export Password:
OpenSSL> _
```

The certificate you create is just like below:



画 › 本地磁盘 (C:) › OpenSSL-Win64 › bin

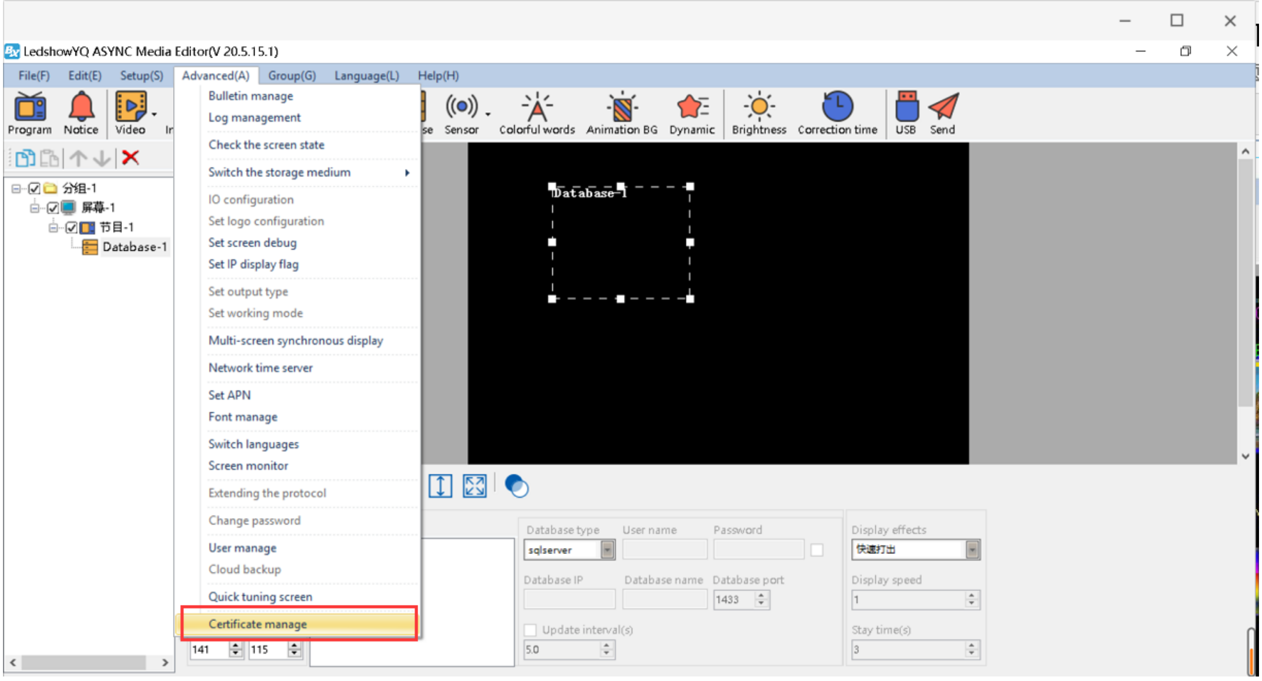
名称	修改日期	类型	大小
rsa_key	2020/4/17 15:11	Personal Inform...	3 KB
rsa_key.pem	2020/4/17 15:08	PEM 文件	2 KB
rsa_private.pem	2020/4/17 15:08	PEM 文件	2 KB
.rnd	2020/4/17 15:06	RND 文件	1 KB
rsa_public.pem	2020/4/17 15:05	PEM 文件	1 KB
openssl	2018/8/14 8:42	应用程序	491 KB
bad_dtls_test	2018/8/14 8:42	应用程序	17 KB
clienthellotest	2018/8/14 8:42	应用程序	9 KB

Note: when you do the third step “3. Create public key and certificate” , this command, you will get notices as below: “ [Unable to load config info from /usr/local/ssl/openssl.cnf] **”**

Please search “openssl.cnf” , create a new folder “c:/usr/local/ssl” in your computer, and put openssl.cnf file into ssl folder.

Software Configuration

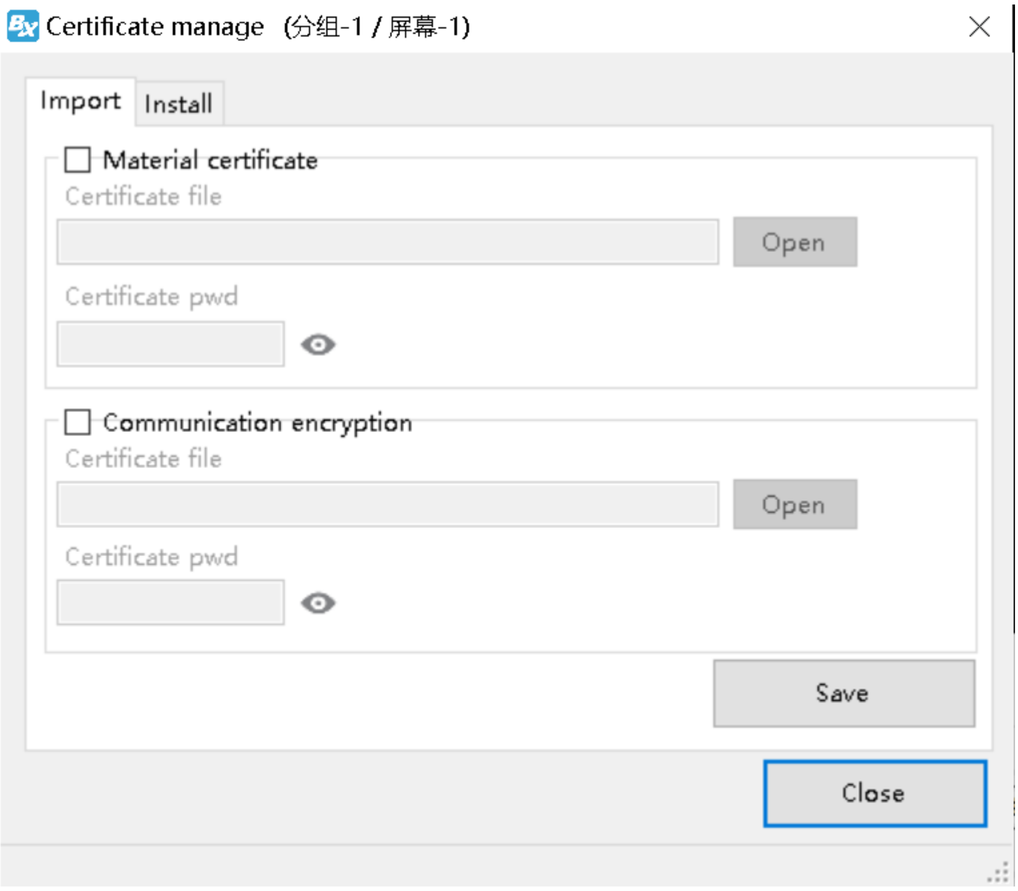
After communicate with Y series controller, please open LedshowYQ software. Click “Advanced” – “certificate management” .



LedshowYQ ASYNC Media Editor(V 20.5.15.1)

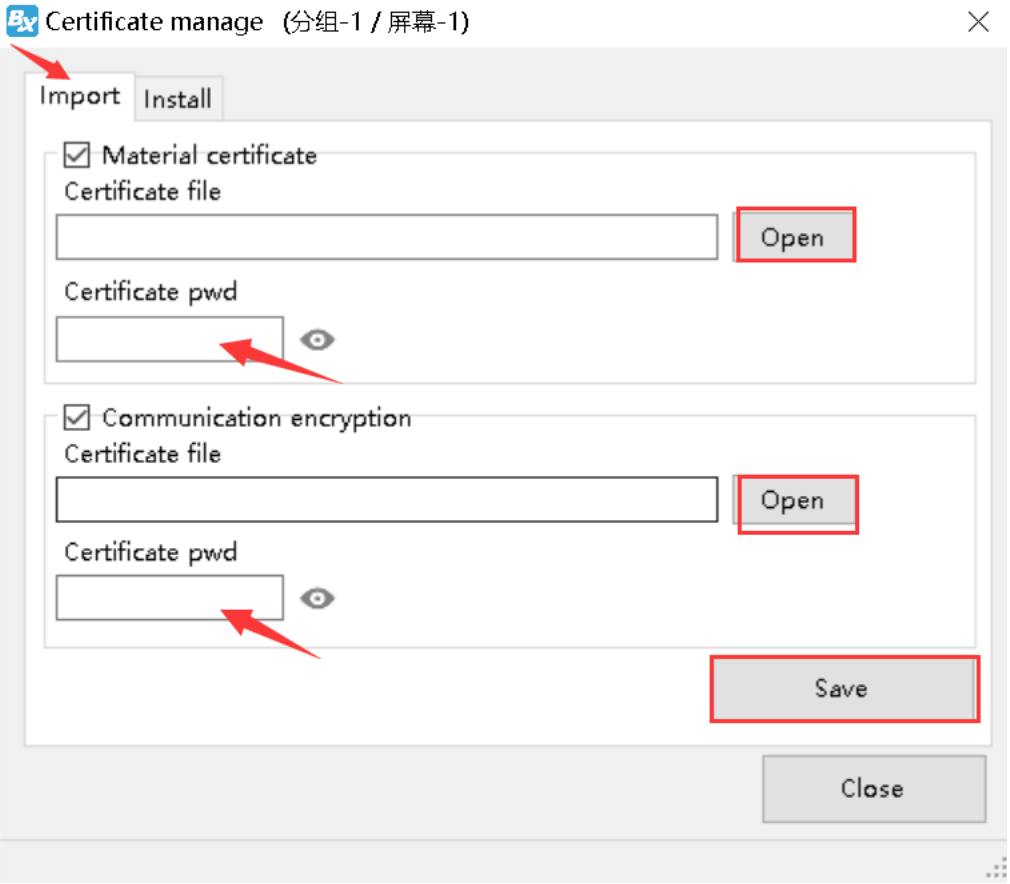
Database type: sqlserver
User name
Password
Database IP
Database name
Database port: 1433
Update interval(s): 5.0
Display effects: 快速打出
Display speed: 1
Stay time(s): 3

Input passwords “888”, enter into “certificate manage” page, as below:



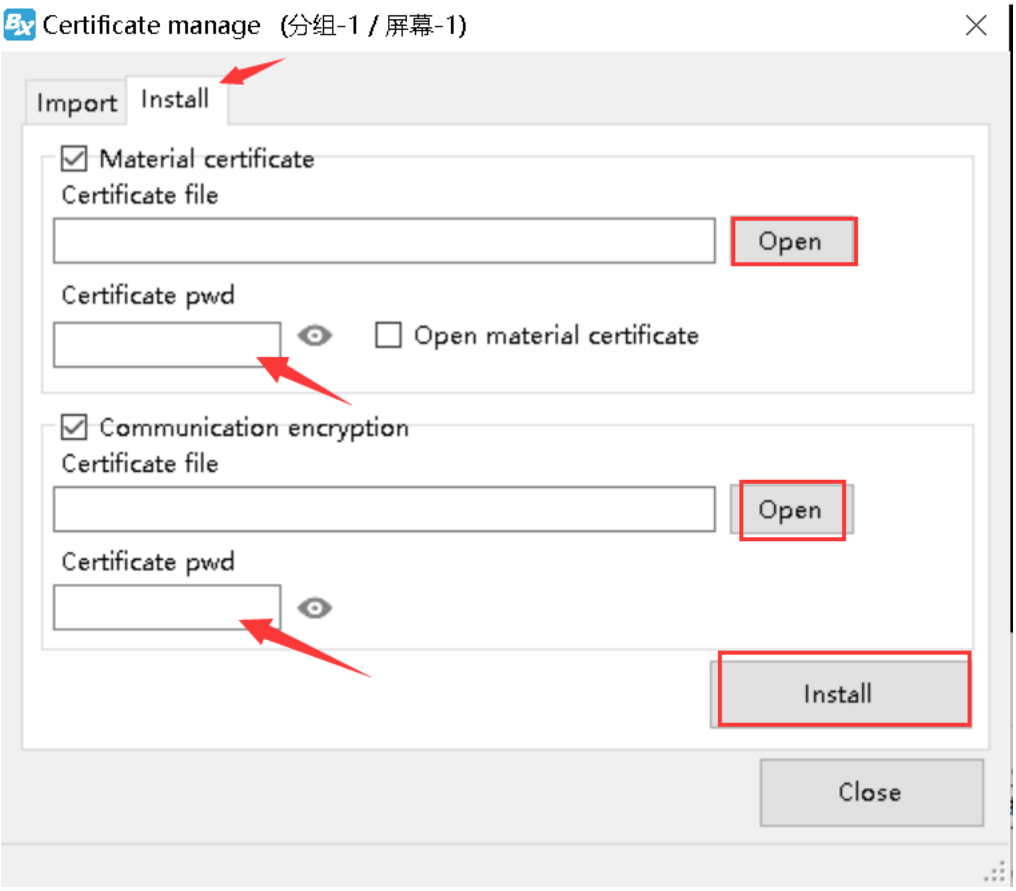
1. Import certificate

Click “Import” – check “Material certificate” and “Communication encryption” - click “open” as to select the relative files in “Material certificate” and “Communication encryption” - input certificate passwords. After finish these settings, click “save”, and then “Close”. As below:



2. Install certificate

Click “install” – check “Material certificate” and “Communication encryption” – click “open”, as to select relative files in “Material certificate” and “Communication encryption”, input certificate passwords – check “Open material certificate”. After finish these settings, click “install”, and lastly click “Close”. As below:



After install certificate file, means the certificate file is installed in controller. LedshowYQ software and controller you used are authenticated and encrypted. So, when you use LedshowYQ software and controller, need to be verified first, then, can get communication and send programs.

Shanghai ONBON Technology Inc.

Address: 7 Floor, Tower 88, 1199#, North Qinzhou Road,
Xuhui District, Shanghai City, China
Website: www.onbonbx.com

ONBON Wechat number

ONBON (Jiangsu) Optoelectronic Industrial Co.,LTD

Address: 1299#, Fuchun Jiang Road, Kunshan City,
Jiangsu Province, China