KGateway Configuration Introduction

Revision History

Version	Date	Change Description	Author
V1.0	2018/7/1	initial	Ning

C O N F I D E N T I A L

Catalogue

1. Purpose

This document describes the basic functions and physical interfaces of the KGateway, which are mainly used to guide users to install and configure.

2. Introduction

The KGateway is made of PC material and is waterproof and dustproof. It supports outdoor installation and can be installed by wall mounting.

After the KGateway power on, it will Periodicly scanning the KBeacon advertisment pakcet then report the data through WiFi or Ethernet. Also it can accept data command from the cloud and forward the data to KBeacon, such as updating the KBeacon configruation. The KGateway using open MQTT + JSON API interface for third-party integration.

Specification

Power	POE or DC 5V
Scanning ability	> 200 beacon per 5 seconds
Wireless distance	BLE5.0: > 200 meters BLE4.0/4.1/4.2 > 100 meters (depends on environment)
Transmitting way	• ETH RJ45 • WiFi • WiFi hoppen • USB (For 3G/4G dongle)
API protocol	• HTTPS • MQTT
Installation way	Screw

Waterproof/Dustproof	IP54
Size	173*90*40
Material	ABS

3. External interface

3.1 Network interface

The KGateway supports following ways to connect to the internet:

1. through WiFi;

2.through the Ethernet interface;

3.throght 2G/3G/4G USB dongle (USB interface has been reserved, but need user to develop USB dongle driver)

4. The KGateway support WiFi Hopping, it means One KGateway can connect to internet by another KGateway.

3.2 Power supply interface

There are two interfaces for power supply: macro USB interface and Ethernet POE port;

- POE power supply, directly through the ethernet cable interface, using POE(802.3af) to supply power.
- Macro USB power supply, powered by the 5V/1A DC.

Warning: The KGateway can only use one of the two power supplies at the same time. Please don't insert two power supply at the same time, otherwise KGateway may be damaged.

3.3 LED indicator

The gateway has 2 LED indicators. The specific meanings are as follows:

1. Red indicator light:

If the red led flash, it means the gateway connect to the cloud fails.

2. green indicator light:

- 2-seconds or less frequency flash: indicates that the KGateway is successfully connected to the cloud and report KBeacon advertisment packet success.

- 10-second frequency flash: indicating that the KGateay connect to the cloud success, but it not found any KBeacon device.

4. Configuration

4.1 User name and password

- After power on, the KGateway will automatic broadcasting Wifi signal, and the default WiFi name is “blegw_mac address”

- The default WiFi connection password is “12345678”
- The default KGateway configruation IP address is 192.168.8.1
- The default web portal login name is “root”, and the default password is also “root”

4.2 Configuration

The KGateway is configured in web portal mode. You can using an web broswer to configure it. To ensure security, the configuration protocol uses https.It is recommended to use the chrome browser for configuration.

4.2.1 Log in to the KGateway

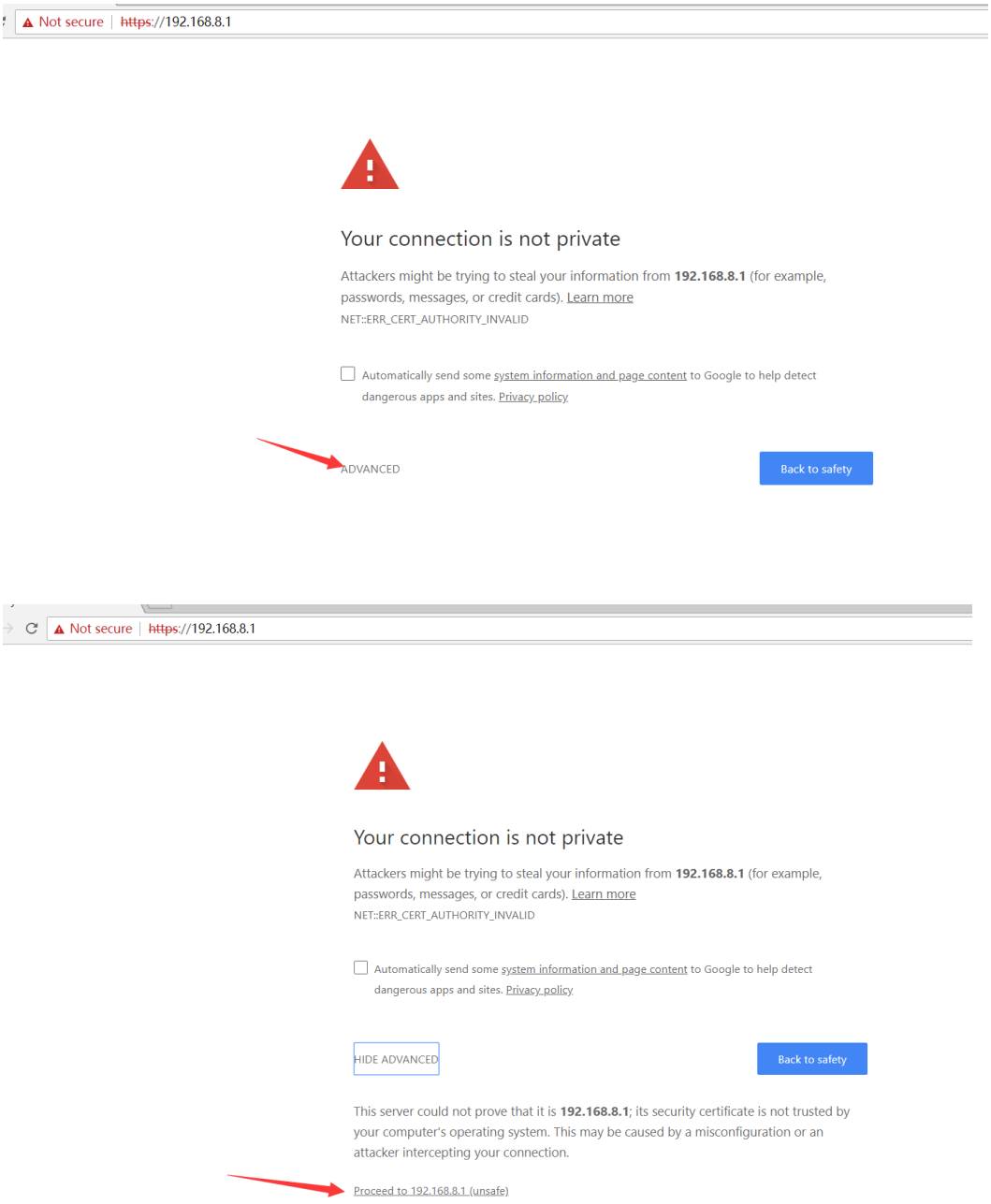
1. Power on the KGateway.

2. Using you PC with WiFi function to scan the WiFi signal of KGateway. If the device name is as follows, it indicates that it is an KGateway.

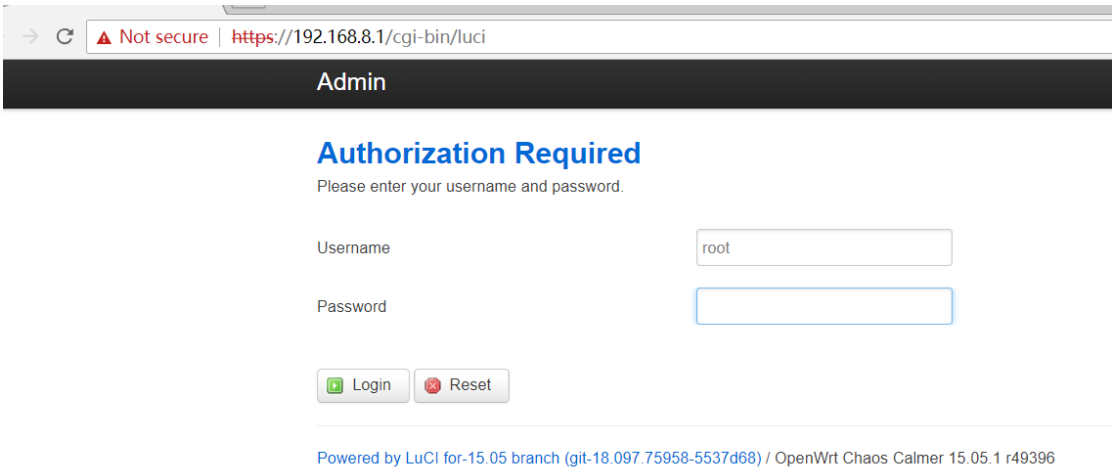
3. Input the WiFi password. The default is 12345678.

4. Log in to the gateway by typing https://192.168.8.1 in the browser. Due to the HTTPs login, the browser will pop up a warning. Click on "Advanced" and then click on "Continue to

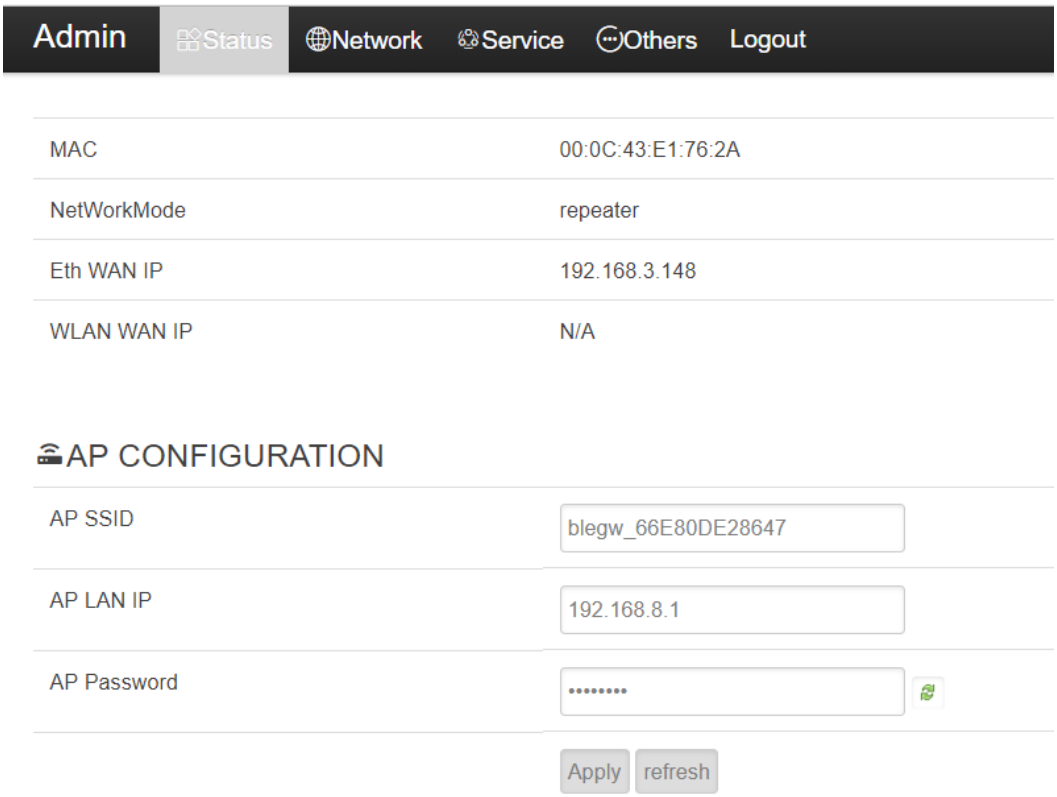
192.168.8.1" to enter the login page.



5. Enter the user name: root and password: root



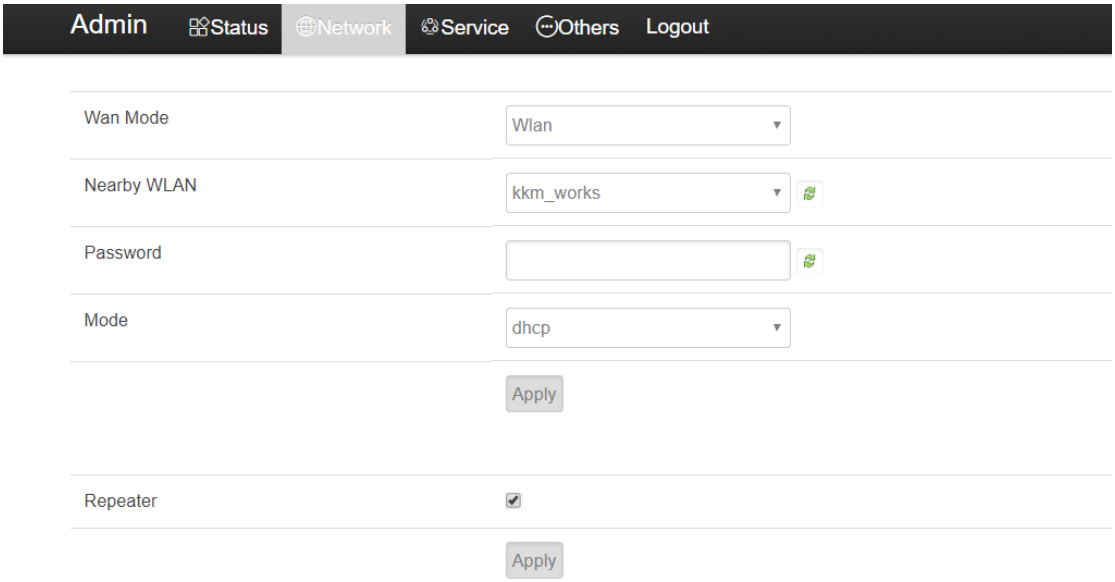
6. Check status about KGateway



4.2.2 Configure network connection

Tap on ***Network*** to go to the network configuration page. You can choose to connect to the network using WiFi or Ethernet connection.

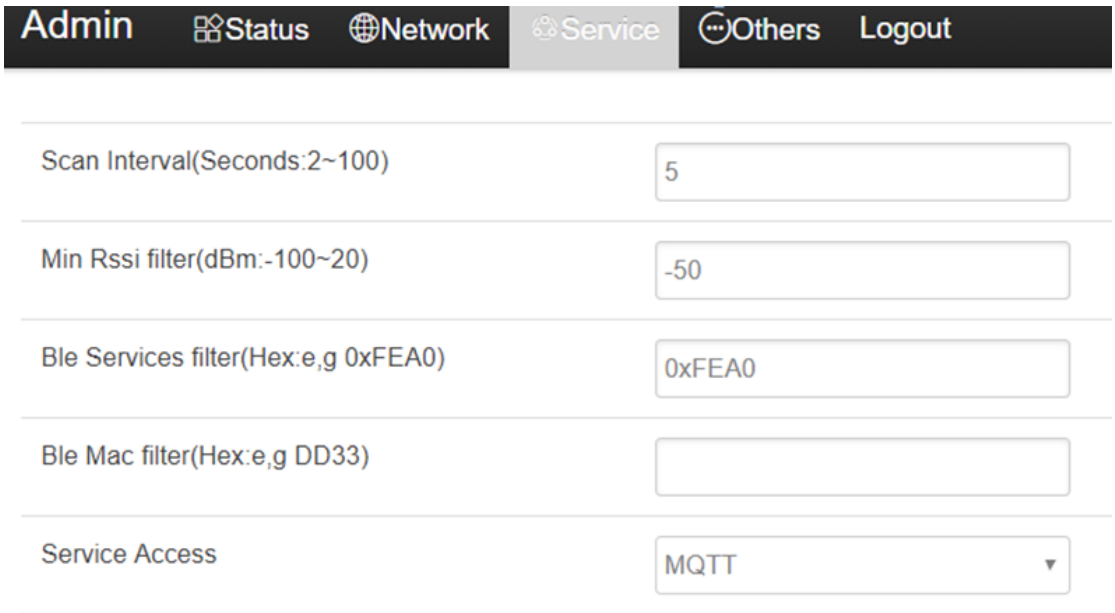
The IP address can be assigned in DHCP or static configuration.



4.2.3 Configuring Service Information

Click Services to go to the service configuration page, where each field is defined as follows:

4.2.3.1 Common configruation



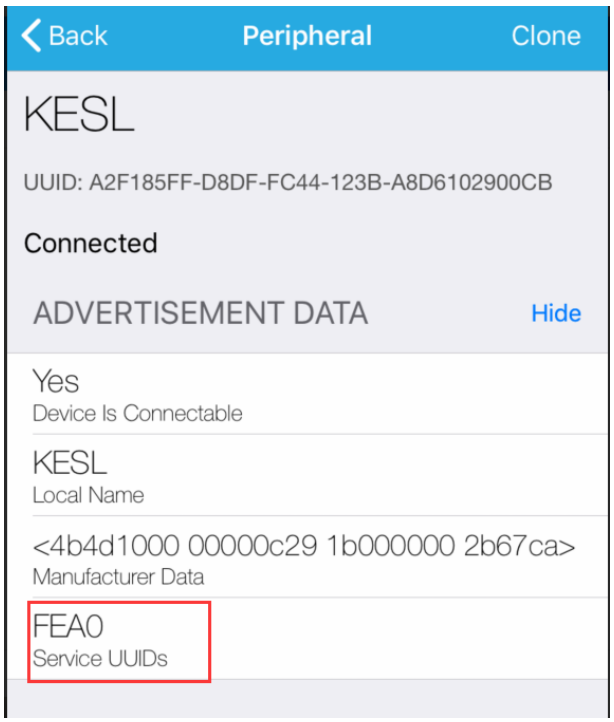
1. Scan Interval: This paramaters used for filter same Beacon report advertisment packet multi-time. the broadcast message of the same KBeacon will only be reported to HTTPs/MQTT

server once in one **Scan interval**.

2. Min Rssi filter: If this paramaters was set, the KGateway will only report the advertisement packet which signal > **Min Rssi** value.

3. Ble Services filter: If this paramaters was set, the KGateway will only report the advertisement packet which include the setting BLE services ID.

Following example is using Lightblue app on IOS to view the device service UUIDs, then you can set the services filter to 0xFEA0.



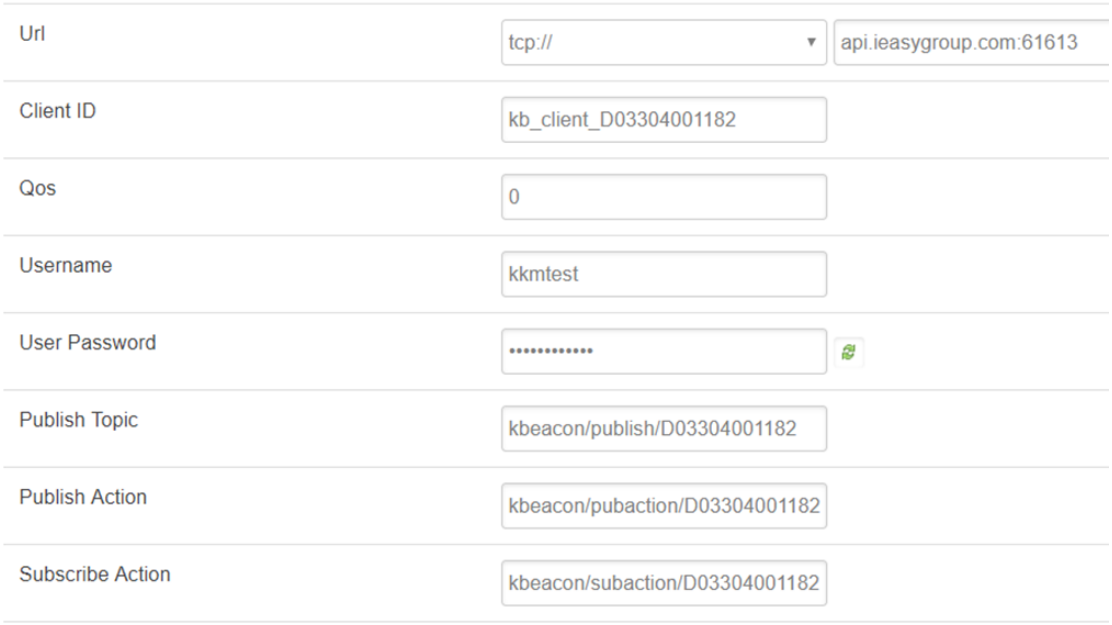
4. Ble Mac filter: If this paramaters was set, the KGateway will only report the Beacon advertisement packet which mac address include the filter value.

For example, if Ble Mac filter value set to 33DD, then following KBeacon advertisement packet will report to HTTPs cloud.

- KBeacon1: mac = 0x33DD01000002
- KBeacon2: mac = 0xA133DD010002
- KBeacon3: mac = 0xA10005033DD2

5. **Service Access:** MQTT or HTTPs.

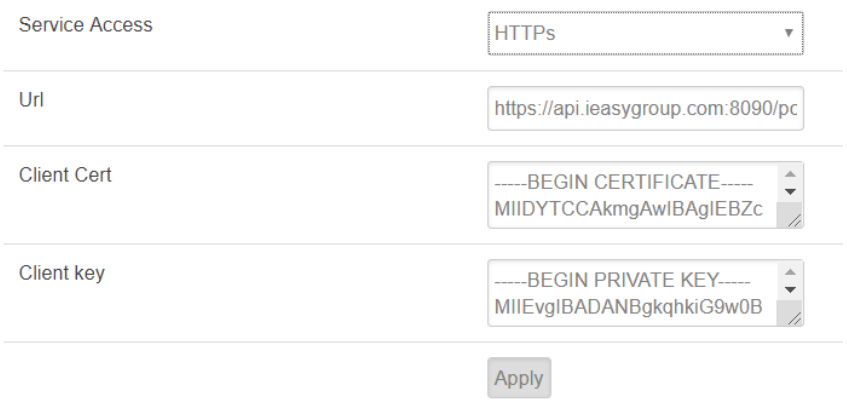
6. MQTT configuration



- **Url:** MQTT server address and port
- **Client ID:** Mqtt client id
- **Qos:** MQTT qos value for publish action and subscribe action topic. The publish Topic Qos is fixed to 0.
- **Username:** mqtt client user name
- **User Password**: mqtt client password
- **Publish Topic:** The status of the status release message, the status of the gateway scanning to each label, published through this topic.
- **Publish Action:** The response message of the gateway to the MQTT server, such as pictures and new response messages, is published through this topic.
- **Subscribe Action:** The gateway store will subscribe to the request from the MQTT server to listen to this topic. Such as pictures with new request messages.

Other MQTT parameters are basic MQTT information, which will not be detailed here.

7. HTTPs configuration



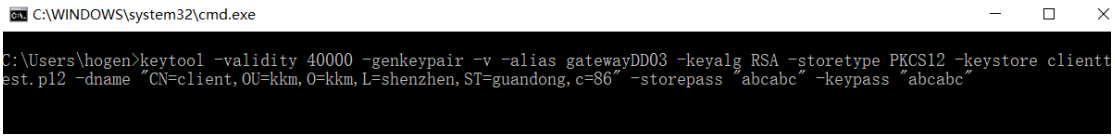
- **Url:** HTTPs server address and port
- **Client Cert:** certificate about HTTPs client
- **Client key:** private key about HTTPs client

The Client Cert and Client key need configured on HTTP server.

How to create client cert and client key? Following example was using keytool and openssl command on win10 to generate client key.

1) Create client p12 private key

keytool -validity 40000 -genkeypair -v -alias gatewayDD03 -keyalg RSA -storetype PKCS12 -keystore clienttest.p12 -dname "CN=client,OU=kkm,O=kkm,L=shenzhen,ST=guandong,c=86" -storepass "abcabc" -keypass "abcabc"



2) Export the client key to pem file

openssl pkcs12 -in clienttest.p12 -out clientcombine.pem -nodes

Then open clientcombine.pem file, you can see client cert key and client key, copy the content to web portal.

Bag Attributes

friendlyName: gatewaydd03

localKeyID: 54 69 6D 65 20 31 35 33 33 35 37 32 36 34 33 39 34

Key Attributes: <No Attributes>

-----BEGIN PRIVATE KEY-----

MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQC67ANsOFpfZg25

gUdcZE21/kKAnaZOxfg7YOgity69MzS6smrs9UWpu05ent7WbB2NmiXSBjkpLBhe

WtyIO8m1/lpZkc6hV33ArEVxwKqP+cTxMQA39mEwN9NKV9hTMaq8IPk5c1j/WcWL

eCVo+Dagl8jrAxWQaUPOO1S+vn8OdLoiZi+E+7vV+c3Nuv+04MmNweLjyGY38XlH

YRP2e/jXADvpjBw3PqvAZ0XQEBOrX00fu4zGRf7nAunvRYMz3yUGAVF4jYnGT9oj

2H04NWhtpRdvhbnc035NrxWlP2MGesxUmOyz4N/bpXp4/II+s8hwFoFEm1ESHMXC

5I2LgeNPAgMBAAECggEAVRmQcVuyoU4oH3WhFIpB6wKIKmAb0C9HVVlINk3pxI+k

iP8juR/tiFnTUzbHQx3T0p0EbPsSWRFPQt3hG1EFA4t6fN7qEQBxKyADOce6n3Pa

WuixLclI9BfmZSlbPn0VOzNT4/kE4rRvQJEBjym6TSDtgzlTPvz9ts3CRlkaJWzt

r7KIy7DMqdTo5X4HM1NLCNlevKi6tJJ/3cdflRjw3wEat/Q/xdnrTvfYqxDOTBb8

MSiz87t0KN460baXixkDCiernIHQh+peTpmKgi8hUWnd+SsbEEHqMLcXV7W8eWPO

rxL4o2EdNkU1i/jDPPpX5wWnSkbwY6G1vx1jn2InwQKBgQDn2fqZn/nzVsYio5Lv

uuVNgAoQPGQ196ADcXIwnW2KtxSIxwO+eulHqxoS7RHHIFg5/XuZwi2SDdBAZdFI

Du65X3Z+nUQguylr2TypLxBiqmgxaNUQZJWcdp1waJBM9fg2UlKxDi0x1vrlptli

5fAoNuPhLXOtjFHWsAh+tSU3oQKBgQDOZAu54H9UoLgCE30pNzaWujkb71siLXL6

eIM5R9cqvy6VNSAuoYG2rvEAcieDk2Y08jYomkaAHcHHTR/3EtkMK+LC9woMDDto

KmafgMcpgIb1FWmgZ/ltcGhLPC1SST0CsTAtKUtyCFFZ9fkWZDjUO2GA5yXmX2nq

yQLDrc507wKBgE36eFiW/6AiPT2FOnQ6rcilGb1gMmwcPsspqrhDGoafEN734IB+

IluiZoCbD3GjpUjLwnhyYJVQ5AvkssDDlPLv8pCfIDzJ9iJ5y/czBxXILob/tTlw

OwmGs2kNIgtgZv0OLxWxqO2sWnJG7bJfl6hO3dHsUY27NgM47YKANmZBAoGAJV2V

heRwCQlD5xRSL5kQZ/91AWq3LBvgWhphX4hzGwkbzOWeWvLgggtwFG2WW8re0S0c

wwMTSnSYtZVv+RJPe1WiqzuAdSftxXEPvUbaR9g+Frb2tZS9YqPcLerKJcCerBMa

LsLwJsf8unW+z9/7LelGQMkYYnnZuikEOBsKar8CgYAn0JYs3wVpEADUWB6jRLRf

DxpkLg0js5ie3q9ZQzlSMqR6Fa1DSSrhKwqBhiwuOFfOfuQEy5m430sULaF5BFuW

25gwAOWA9ksgpktFGzIZ4OiSFLKDJYlsO4s4N/28qVhUN/9CC4ZQWT0VJb/lCFnG

0owYolUCJJahWb5dp1HgGw==

-----END PRIVATE KEY-----

Bag Attributes

friendlyName: gatewaydd03

localKeyID: 54 69 6D 65 20 31 35 33 33 35 37 32 36 34 33 39 34

subject=/C=86/ST=guandong/L=shenzhen/O=kkm/OU=kkm/CN=client

issuer=/C=86/ST=guandong/L=shenzhen/O=kkm/OU=kkm/CN=client

-----BEGIN CERTIFICATE-----

MIIDYTCCAkmgAwIBAgIELNHwBTANBgkqhkiG9w0BAQsFADBgMQswCQYDVQQGEwI4

NjERMA8GA1UECBMIZ3VhbmRvbmcxETAPBgNVBAcTCHNoZW56aGVuMQwwCgYDVQQK

EwNra20xDDAKBgNVBAsTA2trbTEPMA0GA1UEAxMGY2xpZW50MCAXDTE4MDgwNDA0

MzQyNFoYDzIxMjgwMjA5MDQzNDI0WjBgMQswCQYDVQQGEwI4NjERMA8GA1UECBMI

Z3VhbmRvbmcxETAPBgNVBAcTCHNoZW56aGVuMQwwCgYDVQQKEwNra20xDDAKBgNV

BAsTA2trbTEPMA0GA1UEAxMGY2xpZW50MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A

MIIBCgKCAQEAuuwDbDhaX2YNuYFHXGRNtf5CgJ2mTsX4O2DoIrcuvTM0urJq7PVF

qbtOXp7e1mwdjZol0gY5KSwYXlrciDvJtf5aWZHOoVd9wKxFccCqj/nE8TEAN/Zh

MDfTSlfYUzGqvCD5OXNY/1nFi3glaPg2oJfl6wMVkGlDzjtUvr5/DnS6ImYvhPu7

1fnNzbr/tODJjcHi48hmN/F5R2ET9nv41wA76YwcNz6rwGdF0BATq19NH7uMxkX+

5wLp70WDM98lBgFRel2Jxk/aI9h9ODVobaUXb4W53NN+Ta8VpT9jBnrMVJjss+Df

26V6ePyCPrPIcBaBRJtREhzFwuSNi4HjTwIDAQABoyEwHzAdBgNVHQ4EFgQUG77U

oOu/oIlm+xxrbwk8FfPxDqkwDQYJKoZIhvcNAQELBQADggEBAAwfIJM8M7cZTEIb

x3kt20IdQizRf3jhA1hJuj5g0YDlNeAbZ7E2Ur+R9hWANQMFxz/QWQUH30twmEz9

dEt9e69ZNcUsREM5d4uBJmYhaSM3REOuOU1SiLY9gk9tEllyT5FVuubF4TJzyZ4s

mIHigKCcFuyijiQEiMlIABYw439KjyxtuOq+axsISOkrPPBEZanRC7VNehta000B

w4YCPU+8VdyufLb2ofZb1fvqj+KrD2BW735103olPG+RoFncMoG7FcoCKsQzyuZo

ylBA0wNmeVX9O/jdXctGCO+AN9gnszn7KgnJL9tXBj3t7NqA018ItFv5liE4CKvE

qmyJblA=

-----END CERTIFICATE-----

4.2.3.1.1 3. Import the client key to your HTTPs server

How to import the client's key to the HTTPs server is beyond the scope of this document. Different types of HTTPs servers have different methods.

Following example describe how to import client key file to an exist Apache tomcat HTTPs server.

Step1. Open the server.xml on Apache server. Folloing example Apache server using ***api.ieasygroup.com.jks*** as the key file.

```
    Define a non-SSL HTTP/1.1 Connector on port 8080
-->
<Connector port="8091" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />

<Connector port="8090" protocol="org.apache.coyote.http11.Http11Protocol" maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
           keystoreFile="${catalina.base}/conf/api.ieasygroup.com.jks" keystorePass="[redacted]" clientAuth="true" sslProtocol="TLS"
           truststoreFile="${catalina.base}/conf/api.ieasygroup.com.jks" truststorePass="[redacted]"/>
```

Step2. Output p12 file to certificate file.

keytool -export -v -alias gatewayDD03 -keystore clienttest.p12 -storetype PKCS12 -storepass "abcabc" -rfc -file clienttest.cer

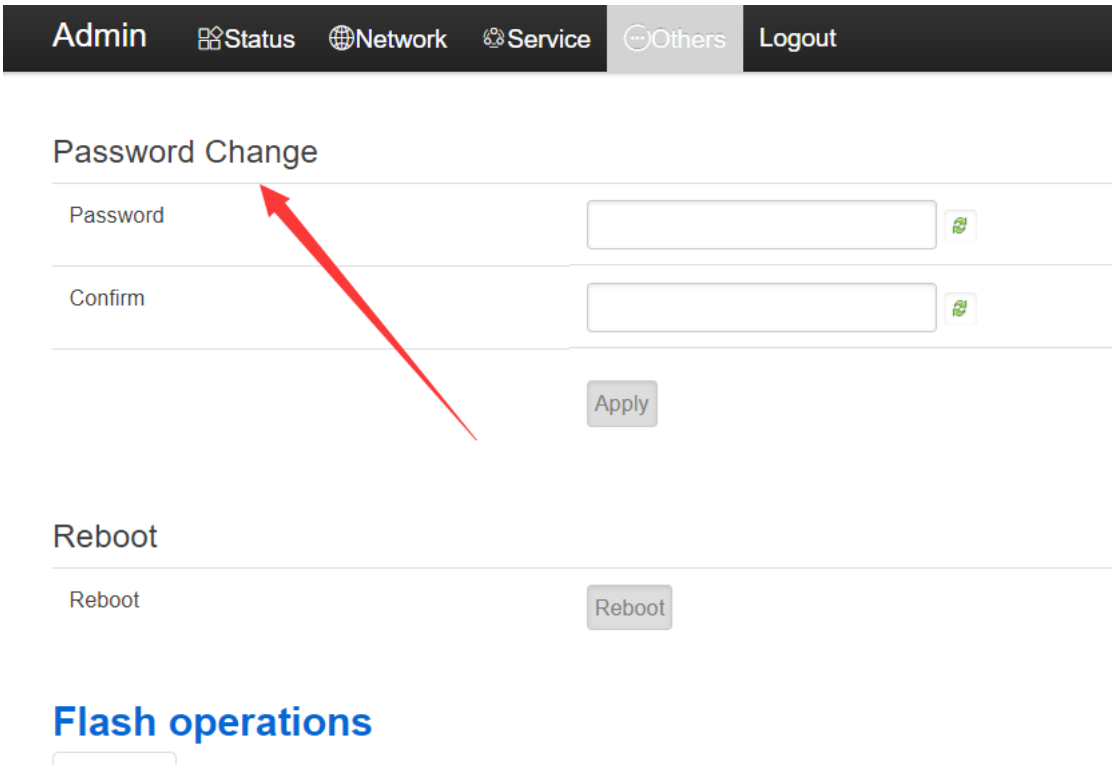
step3. Import the certificate file to HTTPs server key file(api.ieasygroup.com.jks).

keytool -import -v -alias gatewayDD03 -file clienttest.cer -keystore api.ieasygroup.com.jks -storepass xxxx

xxxx is the server key file password.

4.2.4 Modifying the Web Portoal Login Password

The login password defaults to “root” and the user can change it to another password.


Admin
Status
Network
Service
Others
Logout
Password Change
Password
Confirm
Apply
Reboot
Reboot
Reboot
Flash operations