

## Prohibit Non-Certificated CPE from Registering the Service

### Target Objective:

For a service provider, it is required to prohibit the customer to use a non-certificated device from your service platform. It is not only for protecting your investment but also minimize the service level which caused by the non-certificated CPE devices. WellSIP 6500 allow to using the SIP standard header User Agent to validate whether it is a certificate CPE device or not. Only the certificated CPE devices (matched user agent) are allowed to register to your service platform. You can also limit the CPE device used for each subscriber.

### Recommendations:

**Step 1:** Setup the all system certificated devices' user agent here. Please click system>Device ACL to add a new certificate device as follows:



**Create Device ACL**

Device : 3804

User Agent : FXO\_WG

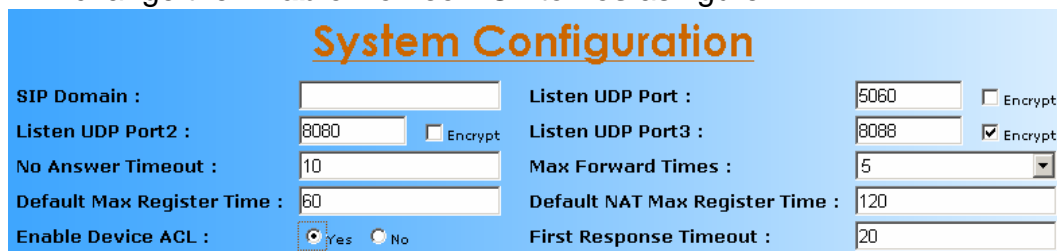
Desc : ACL for 3804

Apply Cancel Back

- Device: 3804
- User Agent: FXO\_WG
- Desc: Welltech FXO 4 port gateway 3804A

Repeat Step 1 to add all certificated devices.

**Step 2:** Enable the Device ACL features by click **Configuration>System** to change the **Enable Device ACL** to **Yes** as figure 1-1.



**System Configuration**

SIP Domain :

Listen UDP Port : 5060  Encrypt

Listen UDP Port2 : 8080  Encrypt

Listen UDP Port3 : 8088  Encrypt

No Answer Timeout : 10

Max Forward Times : 5

Default Max Register Time : 60

Default NAT Max Register Time : 120

Enable Device ACL :  Yes  No

First Response Timeout : 20

Figure 1-1

Step 3: If you want to restrict a subscriber's CPE device to ensure the granted service, click **Configuration > Subscriber > Subscriber** to enable the subscriber allowed CPE devices as follows:

**Create Subscriber**

Active Mode :  Active  InActive

TEL NO : 1001

User Password : ●●●●

User Group : 1 - CLS1 Servi

DNIS Screening Group : None

Emergency Group : None

Device Type : Subscriber

Preferred RTP Group : None

RTP Proxy : Auto

NAT Group : None

Max Register Time : 0

First Reponse Time : 0

Max Contact Allowed : 1

Device 1 : 3804

Max Concurrent Call : 0

Over Max Contact Rule : Use Global Setting

Effective Period

Disallow register from NAT

User Account : 1001

Web Password : ●●●●

Authentication Mode : Register Only

Call Authorization Mode : None

Caller ID Mode : Transparent

Hunting Method : Sequential

Register Type : Dynamic

Predefine URI 1 :

Predefine URI 2 :

Max NAT Register Time : 0

No Answer Timer : 0

Pickup Group : none

Device 2 : None

Call Validation : Invite

AAA Sending Stage : Use Global Setting

Remove Tag For Cancel

Sync Web Password

Description :

Each device can have up-to 2 different device type to be used. Just select the device type defined in System -> Device ACL for “device 1” and “device 2”.

Device 1: 3804

Device 2: none

Apply Change to take effective.

After the above settings, all subscribers are allowed to use the defined CPE devices in “System -> Device ACL” (STEP 1). The user “1001” will allow to use 3804 only no matter how many devices are set in global device ACL.

It ensures the customers can use only certificated devices to register to your service platform. Protecting your investment and reduce the supporting cost.