

# Release Note for MyPBX Standard/Pro 2.18.0.X

===Firmware Version: V2.18.0.22===

Applicable Model: MyPBX Standard/Pro

Release Date: November 7th, 2013

## 1. New Features

1. Added "Office Hours" option on outbound route.
2. Added "alwaysauthreject" option on "SIP Settings" page. Once enabled, when registering with invalid username or password, MyPBX will always return "403 Forbidden" response message.
3. Added TLS certificate settings for SIP.
4. Added "Security Center", including Firewall, Service and Port settings.
5. Added "NIC" option in "System Logs" page to choose NIC (Network Information Center) when using packet capture tool on MyPBX.
6. Added detection of new password complexity when you try to change password.
7. Added "Remote Party ID" option on "SIP Settings" page to analyze DID.

## 2. Drive Update

1. Supports new S2 module. After drive update, both old and new S2 module can be used on the device.

Below are pictures of old and new S2 module.



Old S2 Module



New S2 Module

Figure 2-1

## 3. Optimization

1. Enhance the security of MyPBX.
  - 1) Web GUI login: Optimize the encryption algorithm of web login using

MD5+BASE64.

- 2) If the default password of "user", one level of the web GUI admin access, was never changed, the "user" account will be disabled after firmware upgrade. A strong enough password is required when enabling "user" administrator.
  - 3) AMI security: AMI can be enabled or disabled on AMI page. The AMI password is separated from web GUI login password.
  - 4) Basic protection for the SIP registration: Even if the firewall is disabled on MyPBX, the SIP client which failed to register extension for 8 times in a minute will be locked. There is no need to reboot MyPBX after enabling or disabling Firewall.
  - 5) Compulsory password complexity requirement for remote extensions: a password with digits, both uppercase and lowercase letters is required when enabling a remote extension.
  - 6) Encrypt password fields in configuration files "users.conf" and "siptrunk.conf" using MD5.
2. Change the default value of "Register Attempts" on "SIP Settings" page to "0".
  3. After uploading IP phone configuration file to MyPBX "Phone provision" page, one more step of manually rebooting the IP phone will make it work. There is no need to add the IP phone on "Configured Phone" page before uploading IP phone configuration file to MyPBX.
  4. Allow to create a call queue without any permanent agents.
  5. Compatible with IE 10 browser.
  6. Number of IP in Blacklist is unlimited. Pagination display is supported.

## 4. Bug Fixed

1. Fixed the bug that caller ID numbers which starts with digit 0 cannot be evicted by the conference administrator.
2. Fixed the bug that the "Delete" button doesn't work in "inbound route" page if you choose Portuguese to log in MyPBX.
3. Fixed the bug that "Programkeys Configuration" on "General Settings for Aastra" phone provision page didn't work.
4. Fixed the bug that DOD setting would be ignored if PIN user is used when making a call.
5. Fixed the bug that firewall page cannot be accessed if there are many IP listed in IP Blacklist.
6. Fixed the bug that "Skip Greeting" for voicemail doesn't work if users call in MyPBX through SIP trunk.
7. Fixed the bug that Distinctive Ring Tone would not work if Callback is enabled.
8. Fixed the bug that "DID number" on "Inbound route" set as "+500-+600" would not work.
9. Fixed the bug that the alert call from MyPBX through GSM trunk will

disconnect automatically with only one ring tone.

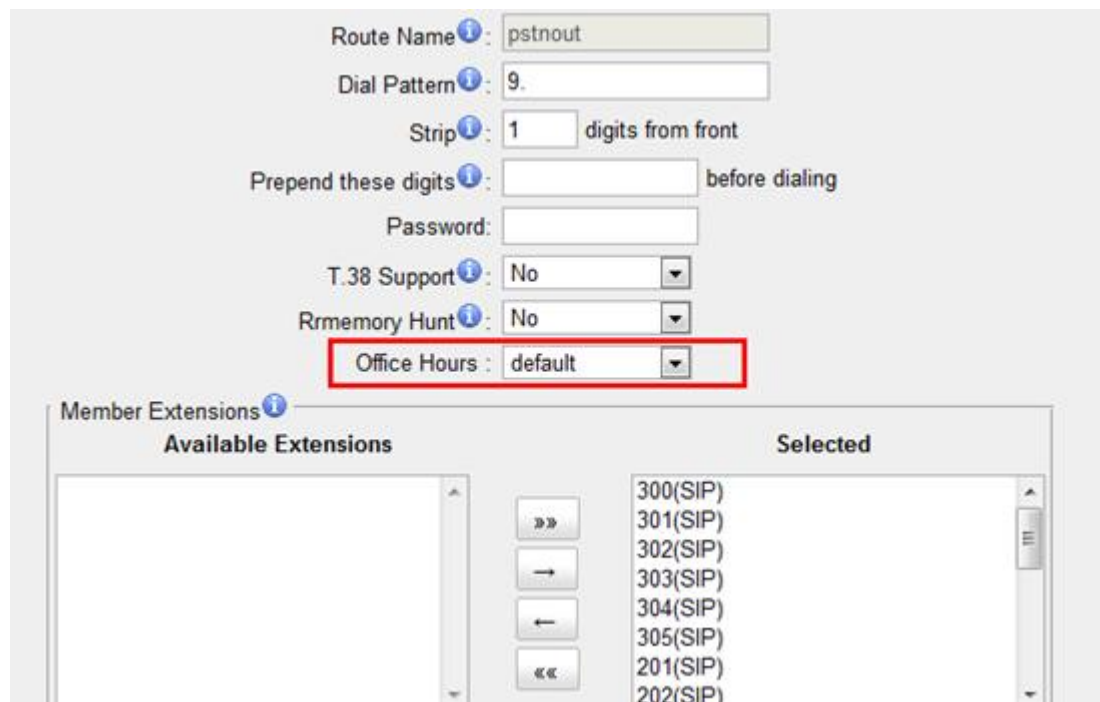
## 5. Instruction (New Features)

### 1. Added "Office Hours" option on outbound route.

**Path:** Basic → Outbound Routes

**Instruction:**

Users can choose "Office Hours" on the outbound route to limit outgoing calls from MyPBX according to the business hours.



The screenshot shows the configuration page for an outbound route named 'pstrout'. The 'Office Hours' dropdown menu is highlighted with a red box and is set to 'default'. Other settings include Dial Pattern: 9, Strip: 1 digits from front, Password: (empty), T.38 Support: No, and Rmemory Hunt: No. Below the settings is a 'Member Extensions' section with two columns: 'Available Extensions' and 'Selected'. The 'Selected' column contains a list of extensions: 300(SIP), 301(SIP), 302(SIP), 303(SIP), 304(SIP), 305(SIP), 201(SIP), and 202(SIP).

Figure 5-1

### 2. Added "Alwaysauthreject" option on "SIP Settings" page.

**Path:** Internal Settings → SIP Settings → Advanced Settings

**Instruction:**

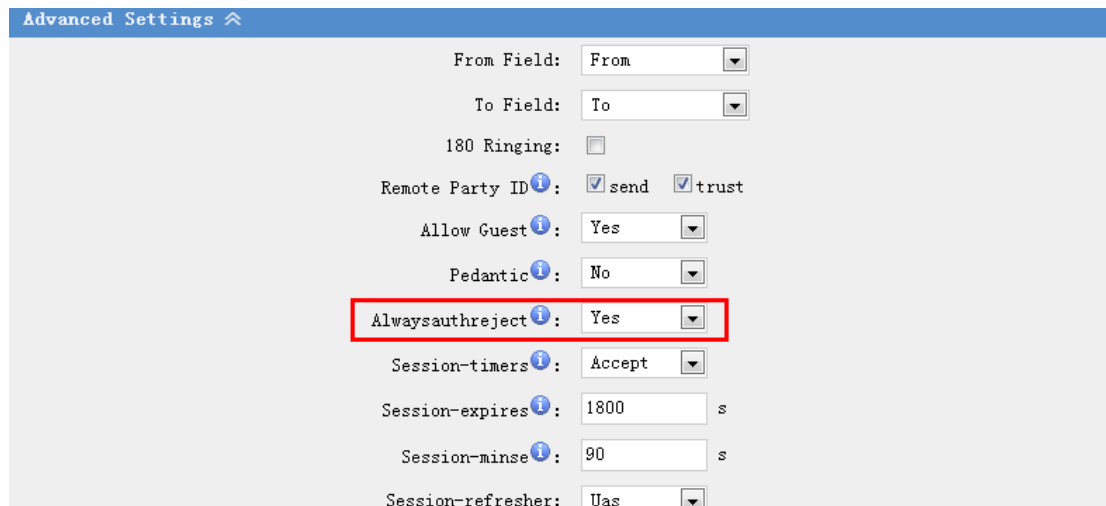


Figure 5-2

### 3. Added more TLS options.

**Path:** Internal Settings → SIP Settings → General

**Instruction:**

In order to enhance the security of call, more TLS options are available. The packages of call will not be captured if TLS is enabled. Users can find options "TLSDontVerifyServer", "TLSVerifyClient", "TLSIgnoreCommonName", "TLSClientMethod" in "SIP Settings" page.

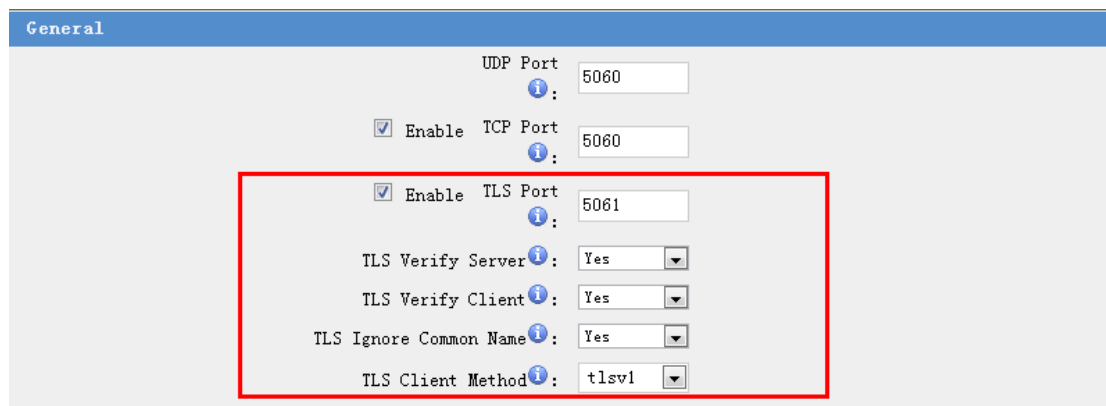


Figure 5-3

The certificates including CA certificate and server certificate can be uploaded to MyPBX in "Certificates". The CA certificate should choose type "Trusted Certificate" and server certificate choose "PBX Certificate."

**Path:** System Settings → Certificate

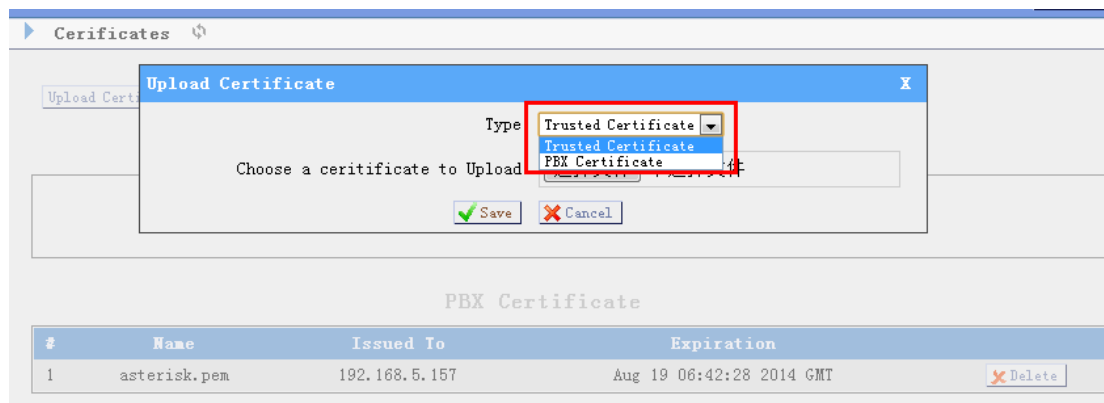


Figure 5-4

#### 4. Added "Security Center", including Firewall, Service, Port.

**Path:** System Settings → Security Center

**Instruction:**

The Security Center includes Firewall, Service and Port. With this center, the administrator can check and configure MyPBX security quickly.

Function	Status	Note	Setting
Firewall Switch	Enabled	The number of firewall rule is:5,Please check if the rule is effective.	Setting
Drop All	Disabled		Setting
Blacklist Rules	Configured	The number of blacklist rules is:3	IP Blacklist
Alert Settings	Not Configured	It is recommended that you configure Alert Settings.	Alert Settings

Figure 5-5 Firewall

Name	Status	Note	Setting
AMI	Disabled		Setting
SSH	Enabled		Setting
TFTP	Enabled		Disabled

Figure 5-6 Service

Name	Port	Setting
SIP UDP Port	5060	Setting
SIP TCP Port	5060	Setting
SIP TLS Port	5061	Setting
HTTP Bind Port	80	Setting

Figure 5-7 Port

#### 5. Added "NIC" option in "System Logs" page to choose NIC

**(Network Information Center) when using packet capture tool on MyPBX.**

**Path:** Reports→System Logs→Packet Capture Tool

**Instruction:**

Users can choose the NIC to capture log.

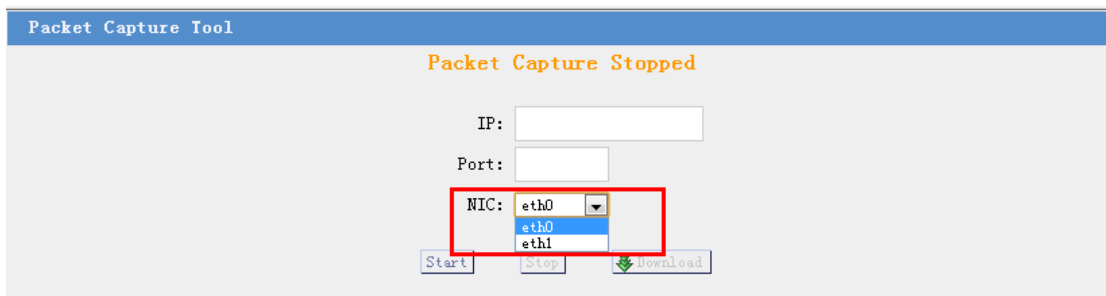


Figure 5-8

**6. Added detection of new password complexity when you try to change password.**

**Path:** System Settings → Password Settings

**Instruction:**

When users need to set new password on MyPBX, the password complexity will be detected, which will help users to set a strong password and make MyPBX safer. A strong password is comprised of letters, numbers and characters.

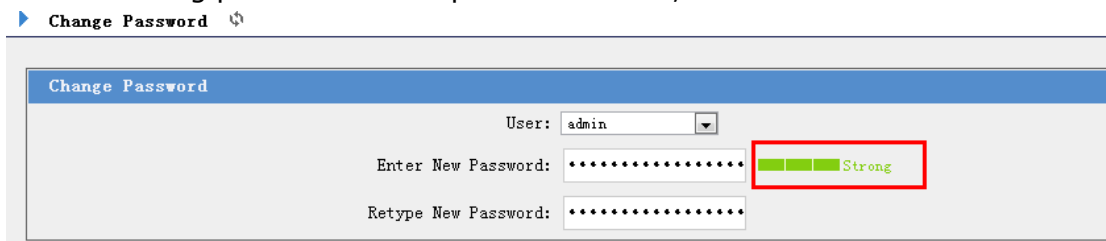


Figure 5-9

**7. Added "Remote Party ID" option on "SIP Settings" page to analyze DID.**

**Path:** Internal Settings →SIP Settings →Advanced Settings→Remote Party ID

**Instruction:**

This option is to setup where to get the DID from SIP invite header. If set to Remote-Party-ID, when there is a SIP incoming INVITE request, MyPBX will resolve the DID from Remote-Party-ID header.

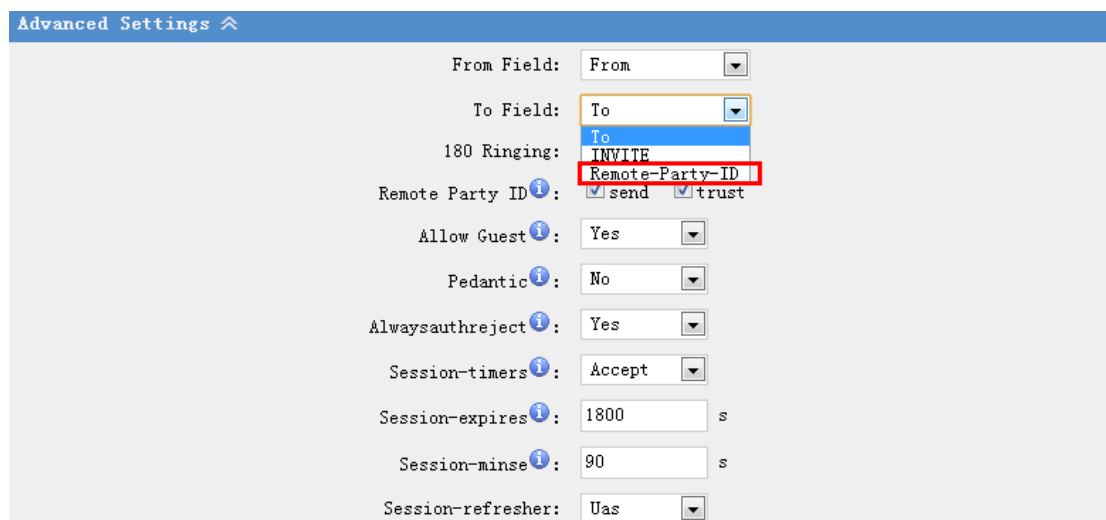


Figure 5-10

## 6. Instruction (Optimization)

### 1. Enhance the security of MyPBX.

#### 1) Web GUI login.

**Instruction:**

Foreground-background communication uses web MD5+BASE64 encryption, which will enhance system security. In the new version, we added BASE64 encryption, the password is well protected and will not be seen in captured log.

#### 2) AMI security.

**Path:** System Settings→ AMI Settings

**Instruction:**

AMI security: AMI can be enabled or disabled on AMI page. The AMI password is separated from web GUI login password.

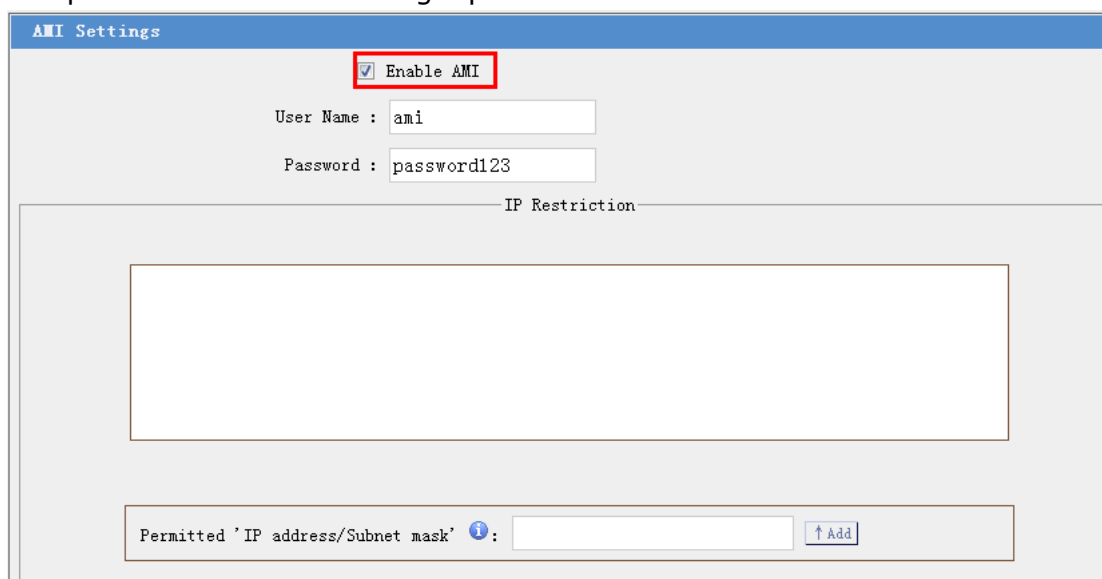


Figure 6-1



### 3) Firewall.

- a. Basic protection for the SIP registration: Even if the firewall is disabled on MyPBX, the SIP client which failed to register extension for 8 times in a minute will be locked.
- b. There is no need to reboot MyPBX after enabling or disabling Firewall.

### 4) Remote extension password.

Compulsory password complexity requirement for remote extensions: a password with digits, both uppercase and lowercase letters is required when enabling a remote extension.



**Edit Extension - 200**

**General**

Type: SIP    Extension: 200    Password: PinSET19

Name: 200    Caller ID: 200

**Voicemail**

Enable Voicemail    Voicemail Access PIN #: 200

**Mail Setting**

Enable Send Voicemail

Email Address:

**Note:** Please ensure that the section 'SMTP Settings for Voicemail' (in the 'Voicemail Settings') have been properly configured before using this feature.

**Group**

Pickup Group: 1

**Follow me**

Follow me:  Always     No answer     When Busy

Transfer to:  Voicemail     Number

**Other Options**

Call Waiting     DND     User Web Interface    Ring Out: 30

**Spy Settings**

Allow Being Spied    Spy Modes: General Spy

**Optional Settings**

**VoIP Settings**

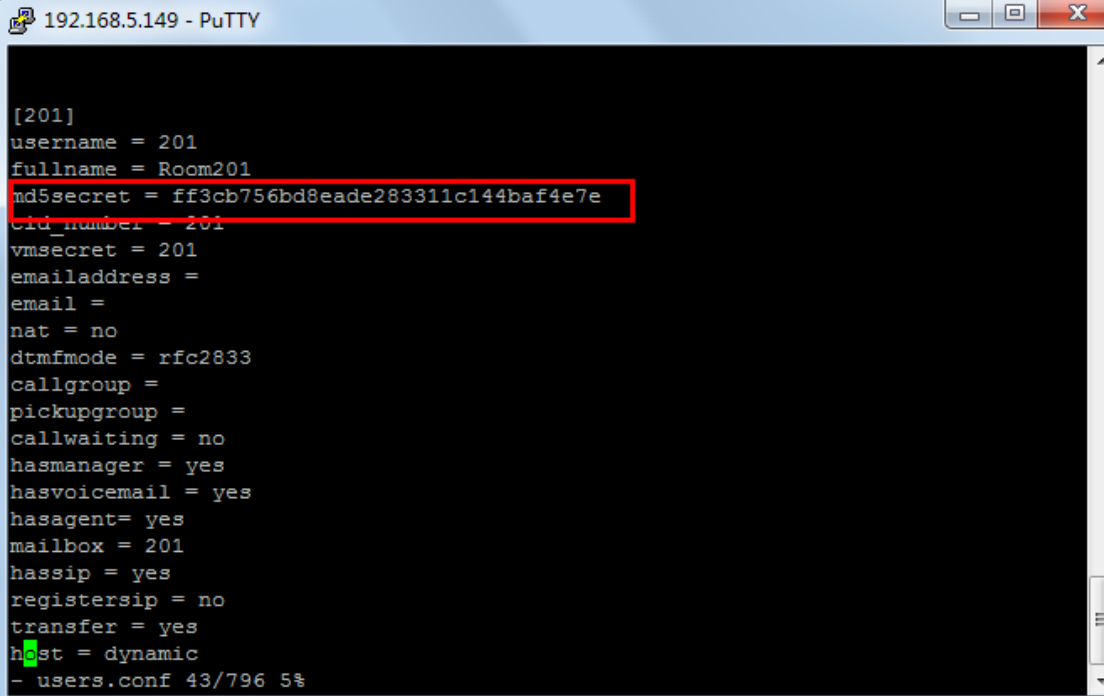
NAT:     Qualify:     Enable SRTP:

Transport: UDP    DTMF Mode: RFC2833    Register Remotely:

Figure 6-2

## 5) Encrypt configuration files "users.conf" and "siptrunk.conf" using MD5.

In the following picture, we can see that passwords in users.conf are encrypted by MD5.

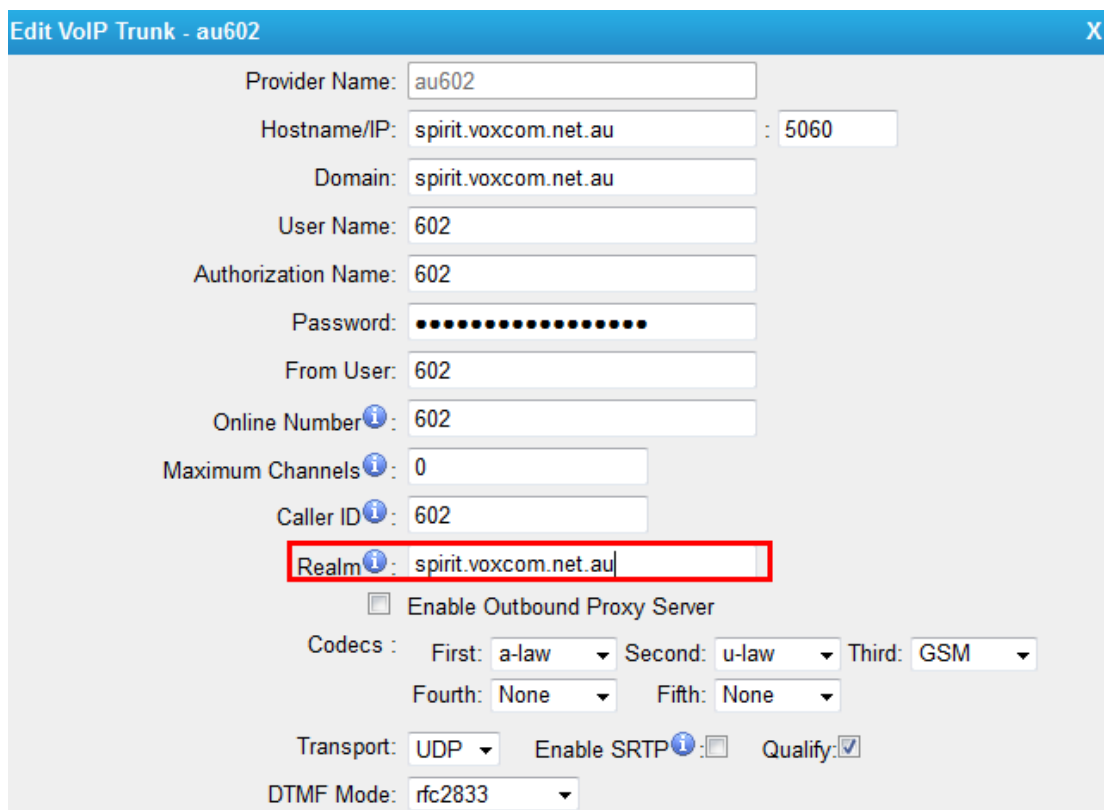


```
192.168.5.149 - PuTTY

[201]
username = 201
fullname = Room201
md5secret = ff3cb756bd8eade283311c144baf4e7e
cid_number = 201
vmsecret = 201
emailaddress =
email =
nat = no
dtmfmode = rfc2833
callgroup =
pickupgroup =
callwaiting = no
hasmanager = yes
hasvoicemail = yes
hasagent = yes
mailbox = 201
hassip = yes
registersip = no
transfer = yes
host = dynamic
- users.conf 43/796 5%
```

Figure 6-3

For encryption of "siptrunk.conf", "Realm" needs to be filled in on VOIP trunk so that the password will be encrypted in the configuration file "siptrunk.conf".



Provider Name:   
 Hostname/IP:  :   
 Domain:   
 User Name:   
 Authorization Name:   
 Password:   
 From User:   
 Online Number:   
 Maximum Channels:   
 Caller ID:   
**Realm:**   
 Enable Outbound Proxy Server  
 Codecs : First:  Second:  Third:   
 Fourth:  Fifth:   
 Transport:  Enable SRTP:  Quality:   
 DTMF Mode:

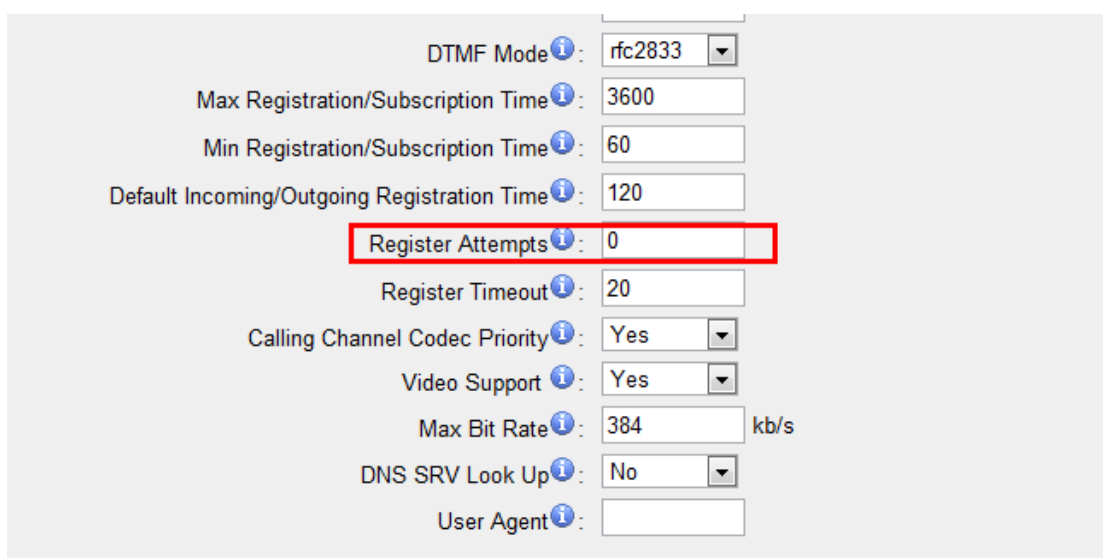
Figure 6-4

**6) User Administrator.**

If the default password of “user”, one level of the web GUI admin access, was never changed, the “user” account will be disabled after firmware upgrade. A strong enough password is required when enabling “user” administrator.

**2. Change the default value of “Register Attempts” on “SIP Settings” page to “0”.**

**Path:** Internal Settings →SIP Settings →General



DTMF Mode:   
 Max Registration/Subscription Time:   
 Min Registration/Subscription Time:   
 Default Incoming/Outgoing Registration Time:   
**Register Attempts:**   
 Register Timeout:   
 Calling Channel Codec Priority:   
 Video Support:   
 Max Bit Rate:  kb/s  
 DNS SRV Look Up:   
 User Agent:

Figure 6-5

### 3. Allow to create a call queue without any permanent agents.

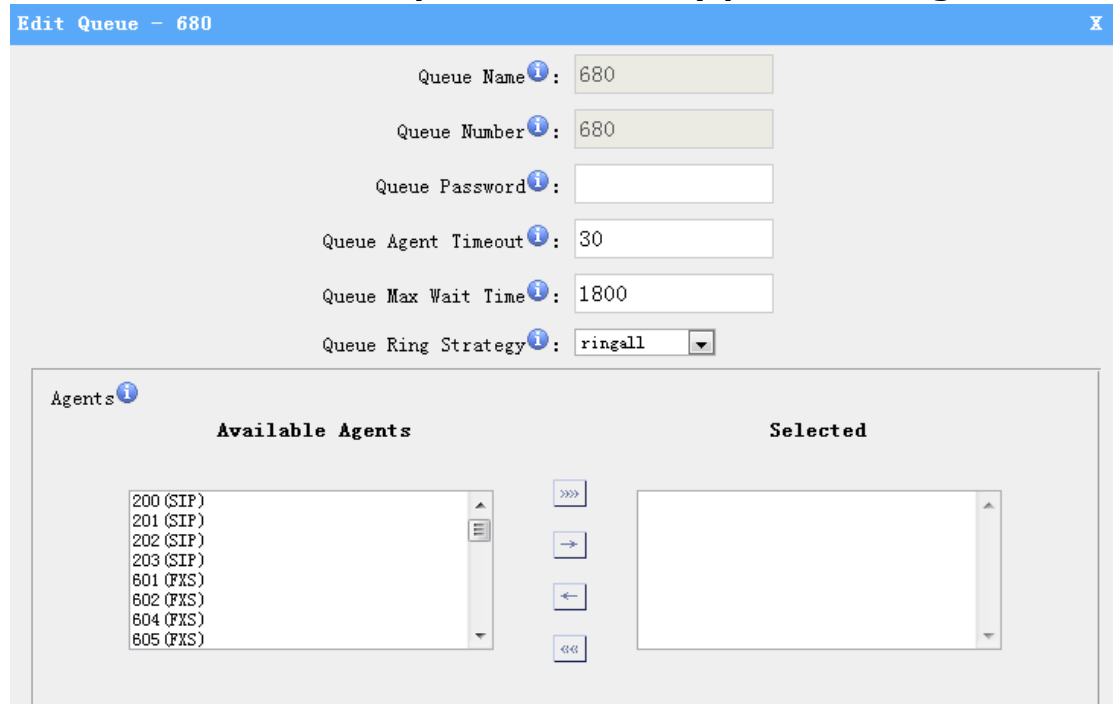


Figure 6-6

### 4. Compatible with IE 10 browser.

### 5. Number of IP in Blacklist is unlimited. Pagination display is supported.



Figure 6-7

<The End>