晶捷數位股份有限公司

Jing Jie System Integration Co.,Ltd.

UniPBX-2000 IPV4/V6 Dual IP-PBX
Administrative Guide

Release 1.5.1 June., 2016

About Jing Jie

Jing Jie Co., Ltd. concentrates to provide the IPV6+IPV4 SIP server farm solution including SIP proxy server, IP-PBX, SIP surveillance server and QoS Monitor to our partner, system integrator and value added reseller. All Jing Jie solutions are provided to support both IPV4 and IPV6 dual stack simultaneously. We provides a painless migration path from IPV4 to IPV6 network.

Jing Jie Co., Ltd.
14F., No.669, Bannan Rd.,
Zhonghe Dist.,
New Taipei City 235, Taiwan (R.O.C.)
WEB: www.jinjsi.com
EMAIL: info@jinjsi.com

Technical Support
Email: support@jinjsi.com

Copyright Notice and Disclaimer

Table of Contents

1 Getting Start

After successfully installed the system , first of all is to login to the web management interface. You can either using IPv4 or IPv6 address to access GUI management interface by using popular browser such as Internet Explorer or Firefox.

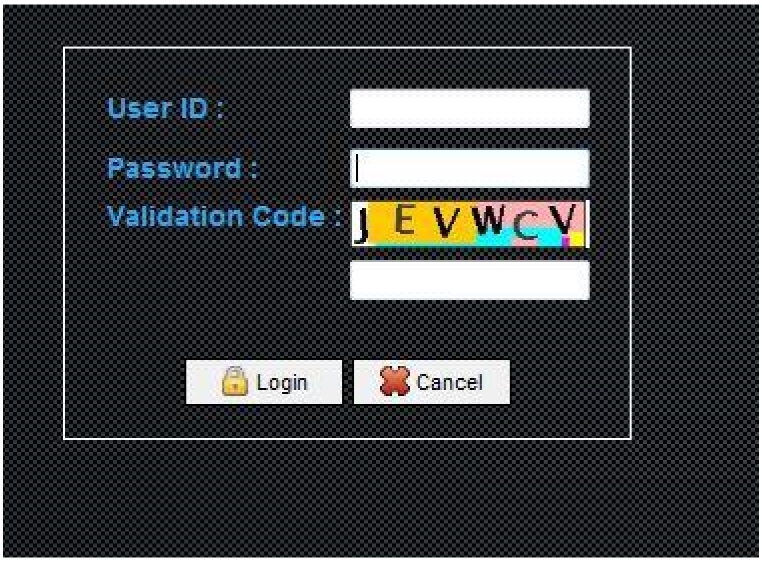
If you are installing a HA version, make sure that MYSQL database replication service is working correctly and both server is running to make the setting simplified.

1.1 Logon the system

After connect the Ethernet cable into the server machine, administrator need to use a computer which had Firefox or IE installed and network connected in order to connect to system GUI. For convenience, configuration computer is recommended to have same subnet as the server.

Start the browse, and type http://xxx.xxx.xxx.xxx:9200 or https://xxx.xxx.xxx.xxx:9201 to login the web manage where xxx.xxx.xxx.xxx is the IP address. If the system is using 2 ethernet leg, it might be easier to use LAN IP for connection.

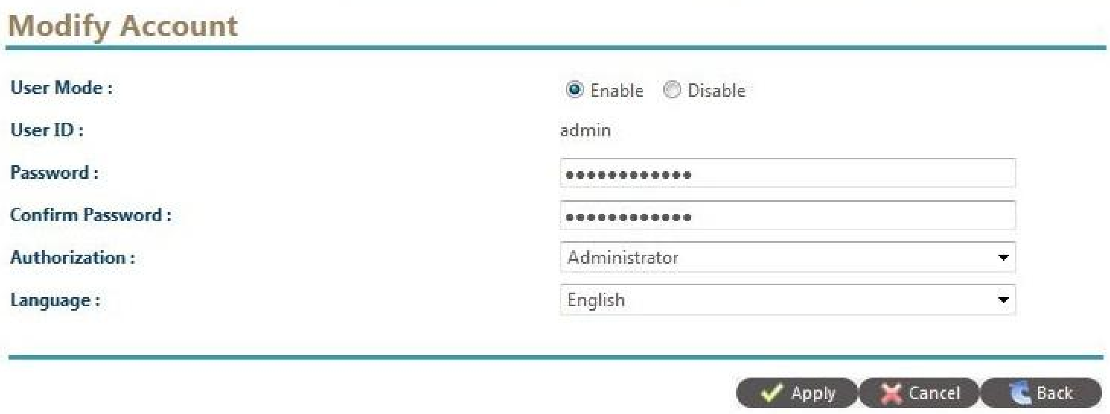
After connected, you should able to see th following login page. Input the default user ID "admin" and password "admin" and the validation code (CAPTCHA) to logon the system.



1.2 Change Default Password

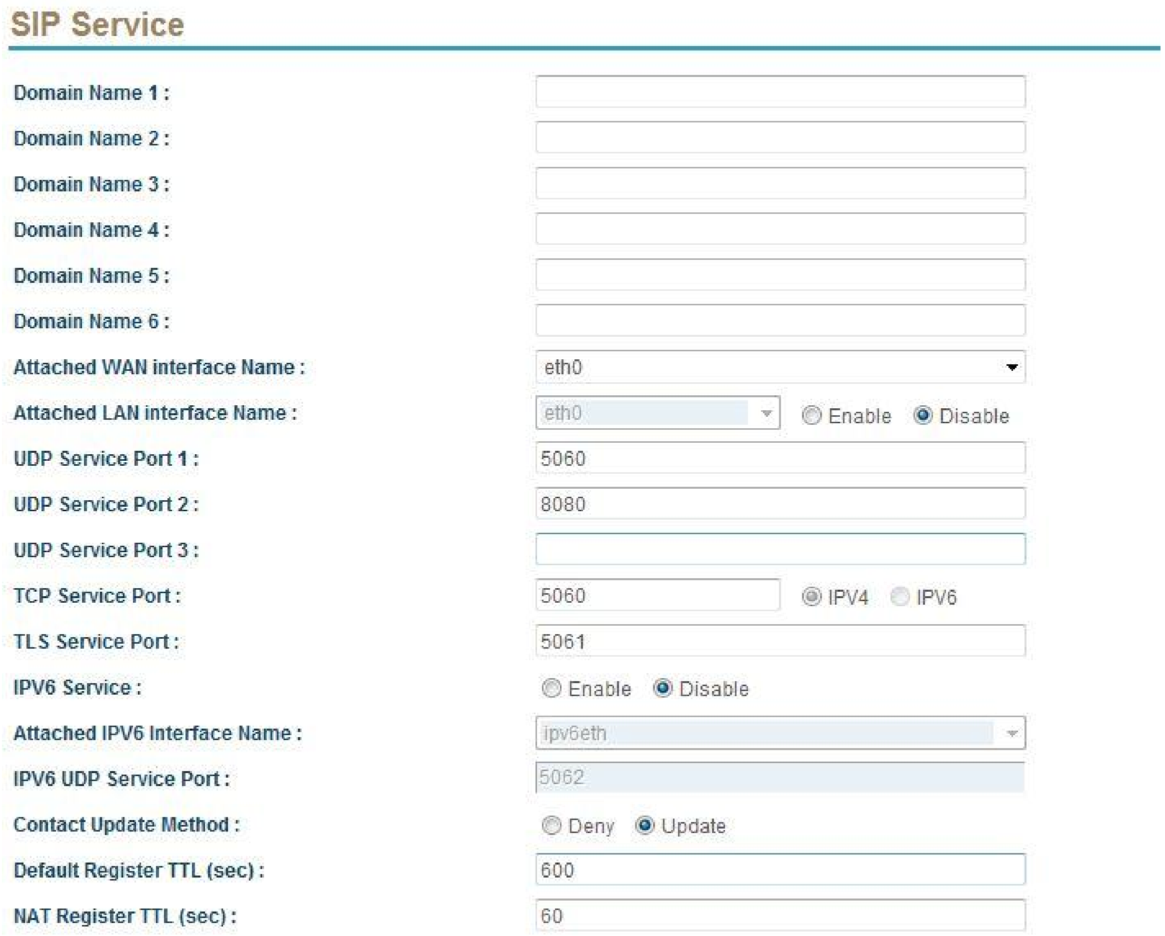
The default password of "admin" is madden for easy to remember. To secure the system access, it is recommended to change the default password as the follows.

Click ***ADMINISTRATION -> Account -> admin*** and the following screen will appear. Input the new password at the Password and Confirm Password fields and click the ***Apply*** button to take effective. Click logout to quit the system UI and relogin by new password for confirmation.



1.3 Setting SIP Service

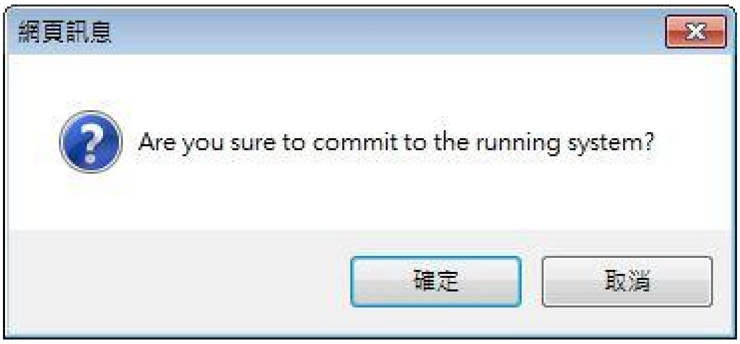
The next step is to set the SIP service parameters for providing service. Click ***SYSTEM -> SIP service*** and the following screen will appear.



Click ***Default*** button to get the default setting of SIP service and change the following settings:

Parameter Name	Value
Attached WAN interface Name	eth0
Attached LAN interface Name	eth1 (for 2 Ethernet Leg Mode), none (for 1 Ethernet Leg Mode)
UDP Service Port 1	5060
UDP Service Port 2	8080
UDP Service Port 3	
TCP Service Port	
TLS Service Port	

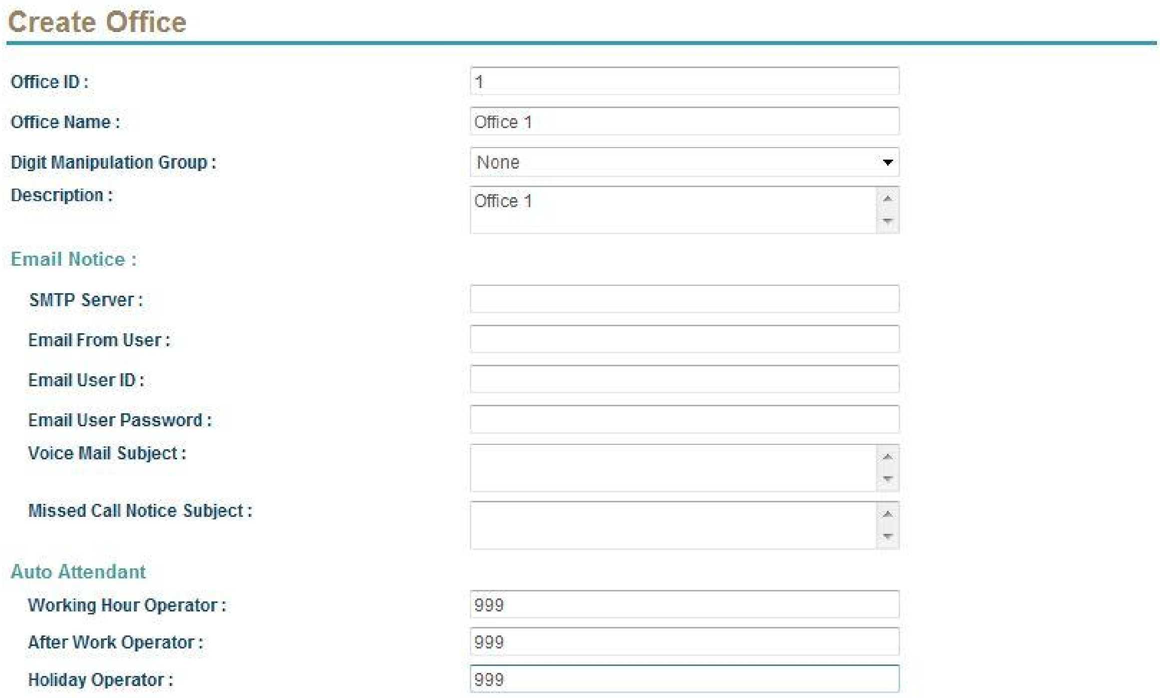
Parameter Name	Value
IPV6 Service	disable
IPV6 UDP Service Port	
Contact Update Method	overwrite
Default Register TTL	600
NAT Register TTL	60

Click 

button and ***COMMIT*** to take effect.

1.4 Create Office

Before we can create the required SIP extensions, the administrator need create an office which includes the SIP extensions. Click ***EXTENSION -> Office -> New*** to create a extension as follows:



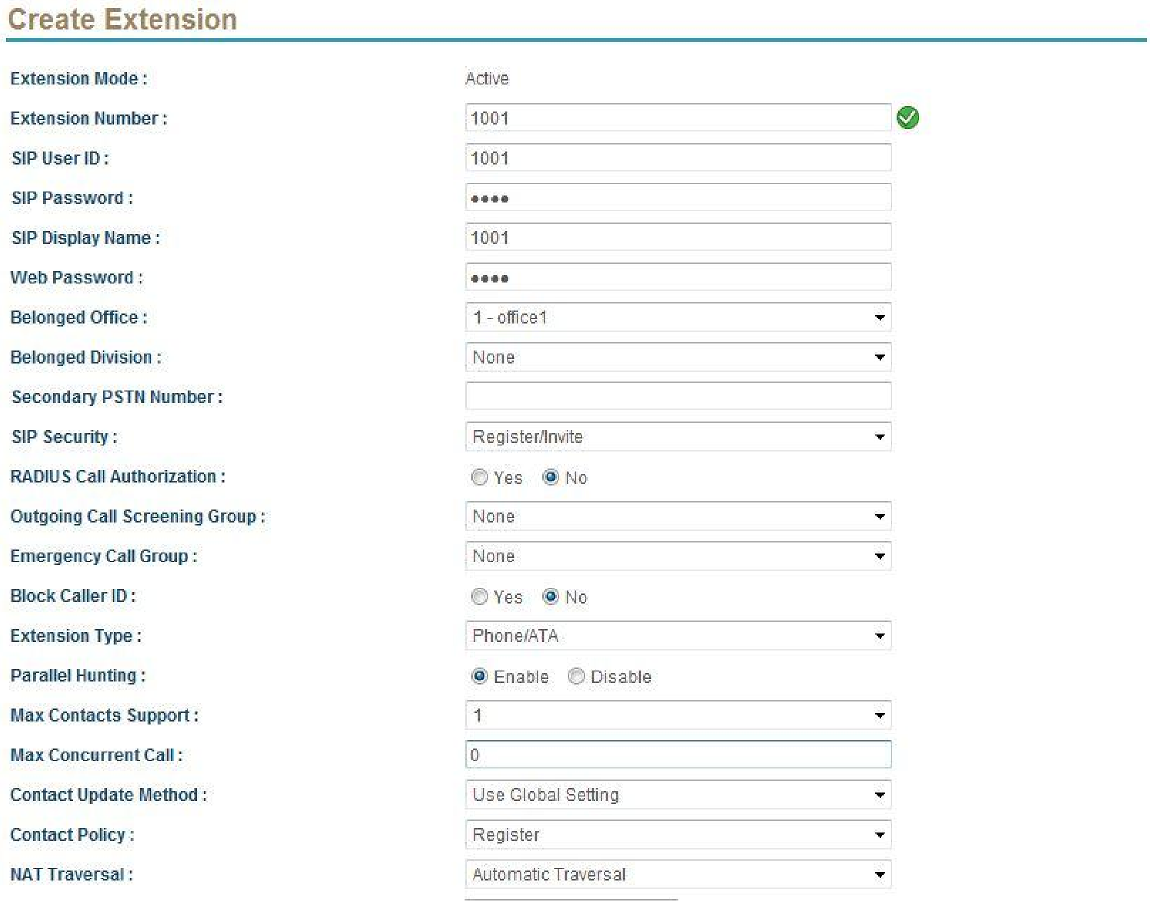
Click the ***default*** button to set those access to a default value and enter the following values:

Parameter Name	Value
Office ID	1
Office Name	office 1
Auto Attendant Operator	set operator number (e.g. 999) for working hour operator, after work operator and holiday operator
Description	office 1

Click ***Apply*** to save it.

1.5 Create Extensions

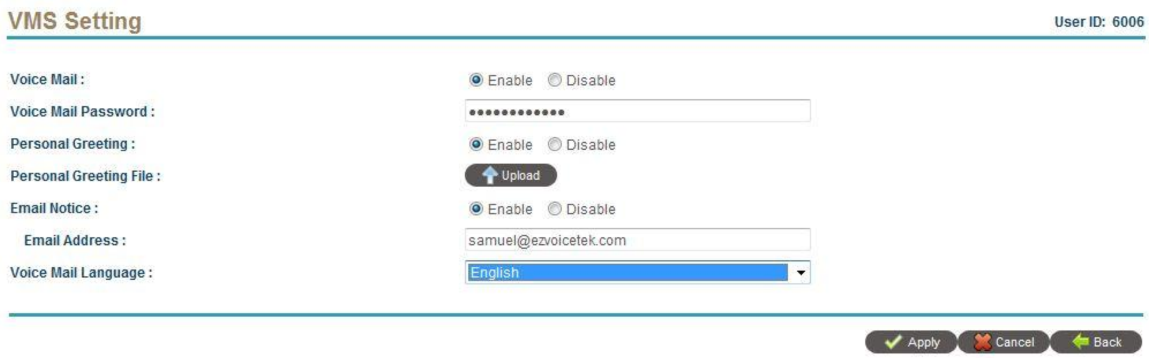
The next is to create 2 SIP extensions and operator console for calling and called.
Click ***EXTENSION -> Extension -> New*** to create a extension as follows:



Create extension 1001 based on the following values:

Parameter Name	Value
Extension Mode	enable
Extension Number	1001
SIP User ID	1001
SIP Password	1001
Belonged User Group	Select group 1 "Office 1"
Name	1001

And setup the ***AA/VMS*** as follows:



Enable the Voice Mail for 1001:

Parameter Name	Value
Voice Mail	enable
Voice Mail Password	1001
Voice Mail Language	English

Click ***Apply*** to save it.

Create extension 1002 based on the following values:

Parameter Name	Value
Extension Mode	enable
Extension Number	1002
SIP User	1002
SIP Password	1002
Belonged User Group	Select group 1 "Office 1"
Name	10012

And setup the ***AA/VMS*** as follows

Parameter Name	Value
Voice Mail	enable
Voice Mail Password	1001
Voice Mail Language	English

Click ***Apply*** to save it.

Create operator as following:

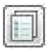
Parameter Name	Value
Extension Mode	enable
Extension Number	999
SIP User	999
SIP Password	999
Belonged User Group	Select group 1 "Office 1"
Name	999

Click ***Apply*** to save it.

Click ***COMMIT*** to take effective.

1.6 Create AA Flow from Template

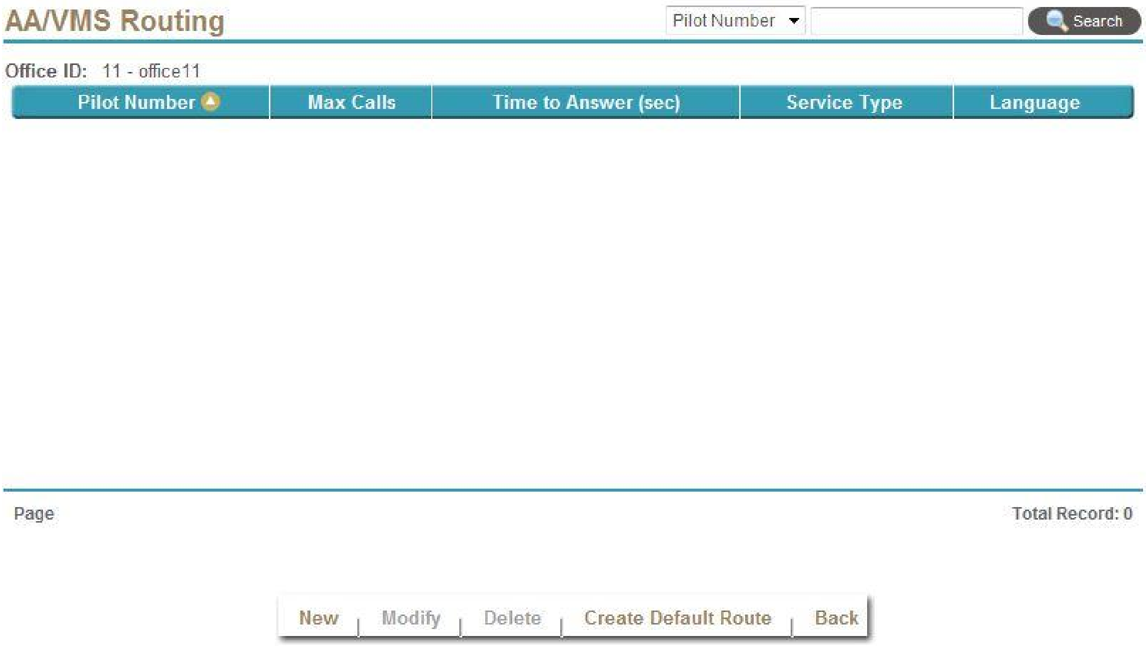
In order to quick enable the AA service for the office, the quickest way to test it is to copy a existing template into the office. The copy will create the template call flow for the office and also copy the required prompt files. Click ***EXTENSION -> Office -> Menu Designer*** and the following screen will appear.

Click  to prepare the copy from a template and the following popup screen will appear.

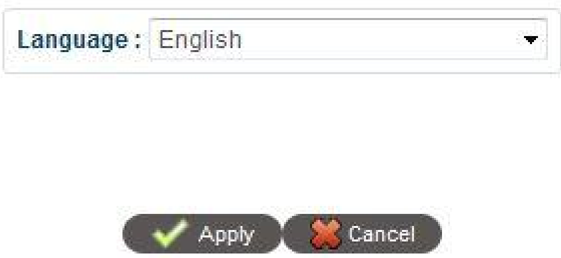
Select 'Copy Menu From Template' and select a suitable template to apply. After apply it, the system will duplicate the call flow and voice prompt into this office. It will become like as below.

1.7 Create AA/VMS Access Key

In order to have Auto Attendant and Voice Mail services enabled for your company. You need create the corresponding routing to be associated to it. Click ***Office -> Office 1 -> VMS Routing*** and the following will appear.



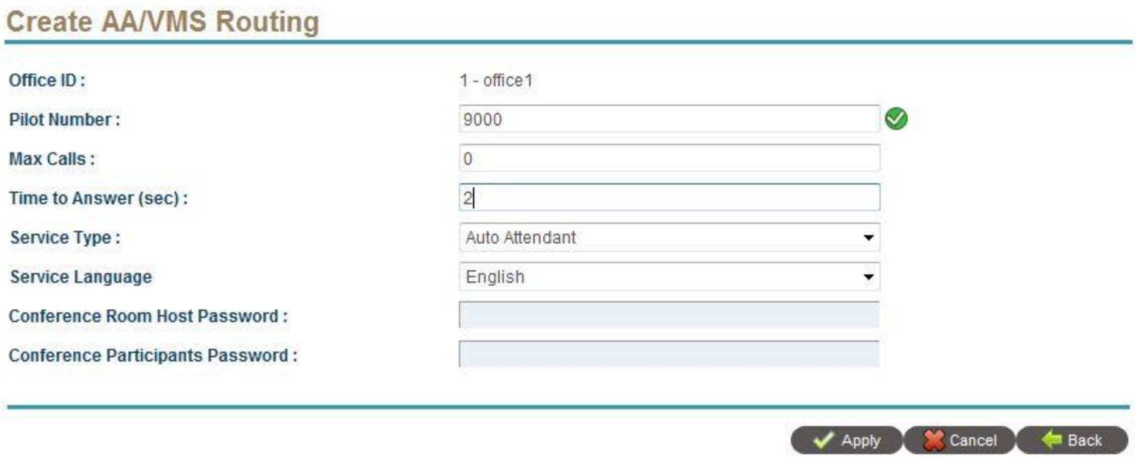
Click ***Create Default Route*** to have the system to create the default routing for the created office. The following will appear:



Click ***Apply*** and the default routing will be generated as follows:

Pilot Number	Max Calls	Time to Answer (sec)	Service Type	Language
*50	Unlimit	1	VMS Main Menu	English
*51	Unlimit	1	VMS From Extension	English
*52	Unlimit	1	Direct to Voice Mail	
*56	Unlimit	1	Call Park	English
*59		1	Music On Hold	
*60	Unlimit	1	Adhoc Conference	English

The next is to create the auto attendant incoming routing number. Click ***New*** to add the routing number for AA as follows.



Enter the following example for the auto attendant service:

Parameter Name	Value
Pilot Number	9000
Max Calls	0
Time to Answer (sec)	2

Parameter Name	Value
Service Type	Auto Attendant
Service Language	English

Click ***Apply*** to save it.

Click ***COMMIT*** to take effective.

1.8 Verify the Device Register

After create extension 1001,1002 and operator 999, you need to configure the SIP phone, gateway or soft-phone to register to the system. To confirm whether those two extensions are registered correctly or not, click ***DIAGNOSTIC -> Extension Status*** and the following screen will appear.

Input 1001 and 1002 as above for the search criteria, click ***Search*** button. You should see both 1001 and 1002 are in the list and registered. If you don't see 1001 and 1002 are in the list, there are some other issues need to be resolved.

1.9 Make a Extension Call

Use extension 1001 calls extension 1002. 1002 should ring and you should able to answer it and talk. To confirm the calls status from the system, click DIAGNOSTIC -> Call Status and the following screen will appear.

Input 1001 and 1002 as above for the search criteria, click ***Search*** button. You should see a call which is calling from 1001 and called to 1002 in the list. If you don't see the call in the list, there are some other issues need to be resolved.

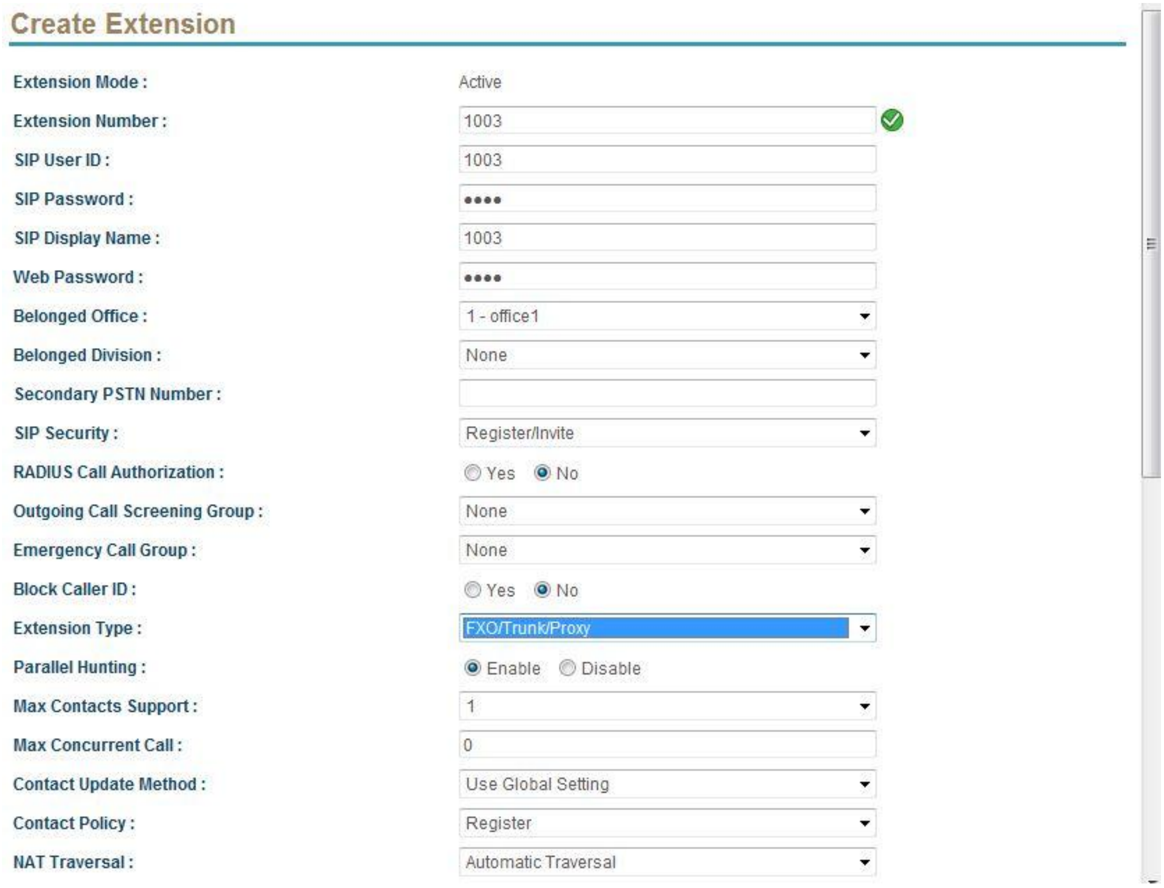
1.10 Maka Calls to AA/VMS

Use extension 1001 calls auto attendant number 9000 . 1001 should hear the auto attendant greeting and you should able to dial to extension 1002 and talk. If the 1002 is not answer the call, you should able to leave a message to 1002.

If you CPE device can support SIP WMI, you should see a new voice mail arrived. 1002 can dial the *50 to get into voice mail main menu and retrieve email.

1.11 Add a PSTN Gateway

The next is connecting to PSTN gateway which is normally a FXO gateway. To start with it, click ***EXTENSION -> Extension*** to create a gateway account for FXO/E1/T1 gateway as follows.



Create a extension 1003 for FXO gateway. Please use the following values for the gateway.

Parameter Name	Value
Extension Mode	enable
Extension Number	1003
SIP User ID	1003
SIP Password	1003
Extension Type	FXO/Trunk/Proxy
Max Concurrent Call	0 means unlimited
Contact Policy	Permanent Contact
Permanent Contact 1	sip:1003@xxx.xxx.xxx.xxx:5060 (SIP URI for the gateway). If you are using Register for the gateway, you don't need

Parameter Name	Value
	setup this field.
Belonged Office	Select group 1 "Office 1"
Name	1003

Click ***Apply*** to save it.

Click ***COMMIT*** to take effective.

Then you need to configure the FXO gateway to register to the system. Verify the FXO is registered or not by using the extension status as the description in "Verify the Device Register".

1.12 Add a VOIP Carrier

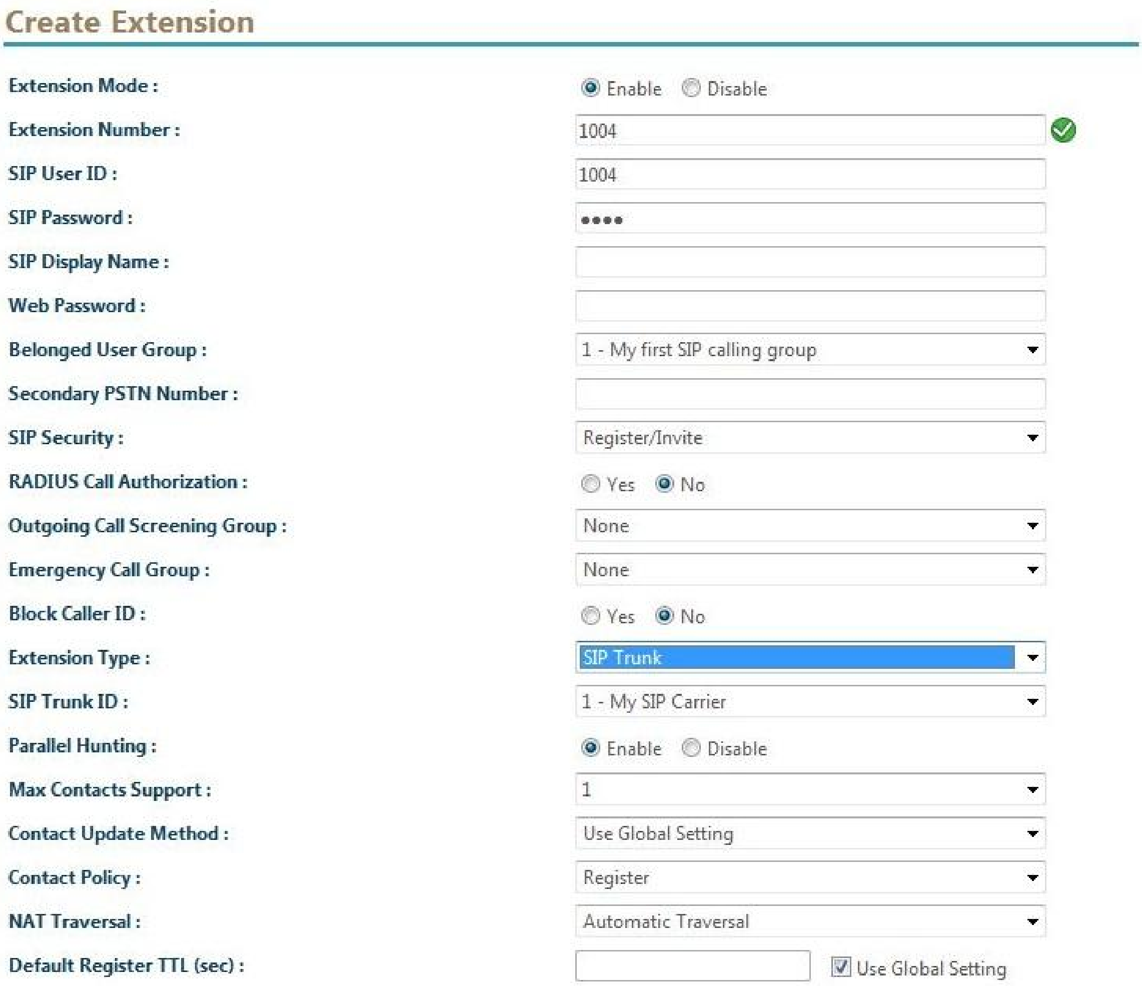
If you are using a VOIP carrier instead of using a PSTN gateway, you can use the following steps to connect to your VOIP carrier. At first is to create a SIP trunk by click ***FEATURE -> SIP Trunk -> New*** and the following screen will appear.

Input the following values for the SIP trunk as an example. You should get those value from your VOIP carrier.

Parameter Name	Value
SIP Trunk ID	1
SIP Domain	sip.carrier.com
Register TEL	9900
Registrar Server	112.3.3.1
Registrar Port	5060
Outbound Proxy Server	112.3.3.1
Outbound Proxy Port	5060
SIP Register User ID	9900
SIP Register Password	9900
Register Expires Time	600
Description	My SIP Carrier

Click ***Apply*** to save it.

The next is to create a extension to associate the SIP trunk together. Click ***EXTENSION -> Extension -> New*** to create the extension 1004 as follows.



Input the following values for extension 1004.

Parameter Name	Value
Extension Mode	enable
Extension Number	1004
SIP User ID	1004
SIP Password	1004
Extension Type	SIP trunk
SIP Trunk ID	Select ID "1 -My SIP Carrier"
Belonged User Group	Select group 1 "My first calling group"

Parameter Name	Value
Name	1004
Description	My VOIP Carrier Extension

Click ***Apply*** to save it.

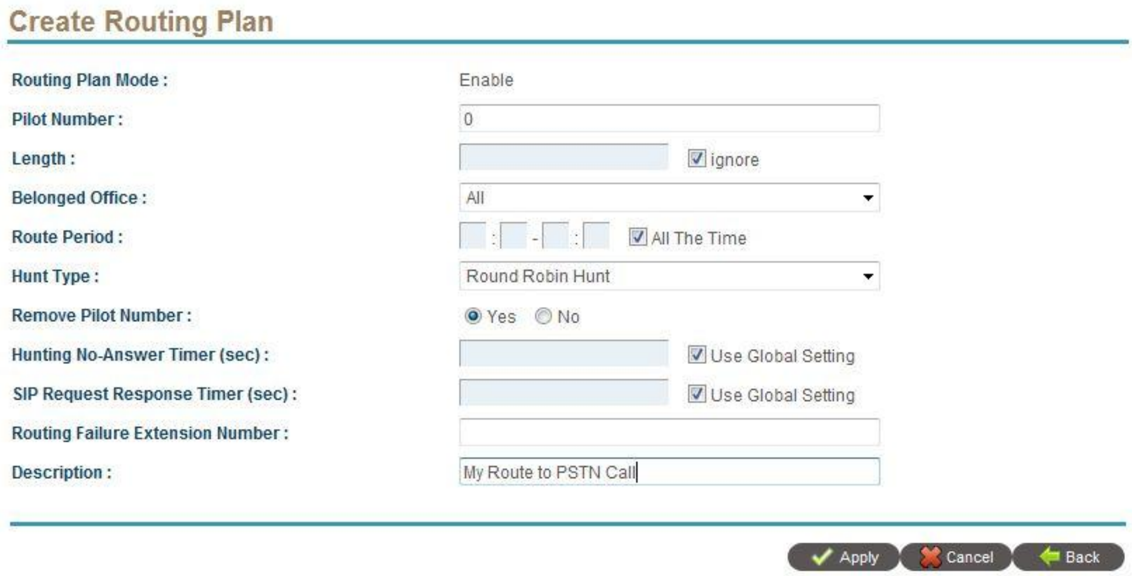
Click ***COMMIT*** to take effective and verify the FXO is registered or not by using the extension status as the description in "Verify the Device Register".

1.13 Create Routing Plan

Assume the following is the dialing rule for PSTN gateway or VOIP Carrier
Leading 0 is used to indicate this call is to PSTN gateway or VOIP carrier.
Leading 0 need to be removed before send to PSTN gateway or VOIP Carrier.

The calling example is described as below:
Extension 1001 dialed 0023123456. System will route the call to extension 1003 (PSTN gateway) or 1004 (SIP trunk). Before the system send the call out, the system will remove the leading 0 and change the called number to 02123456.

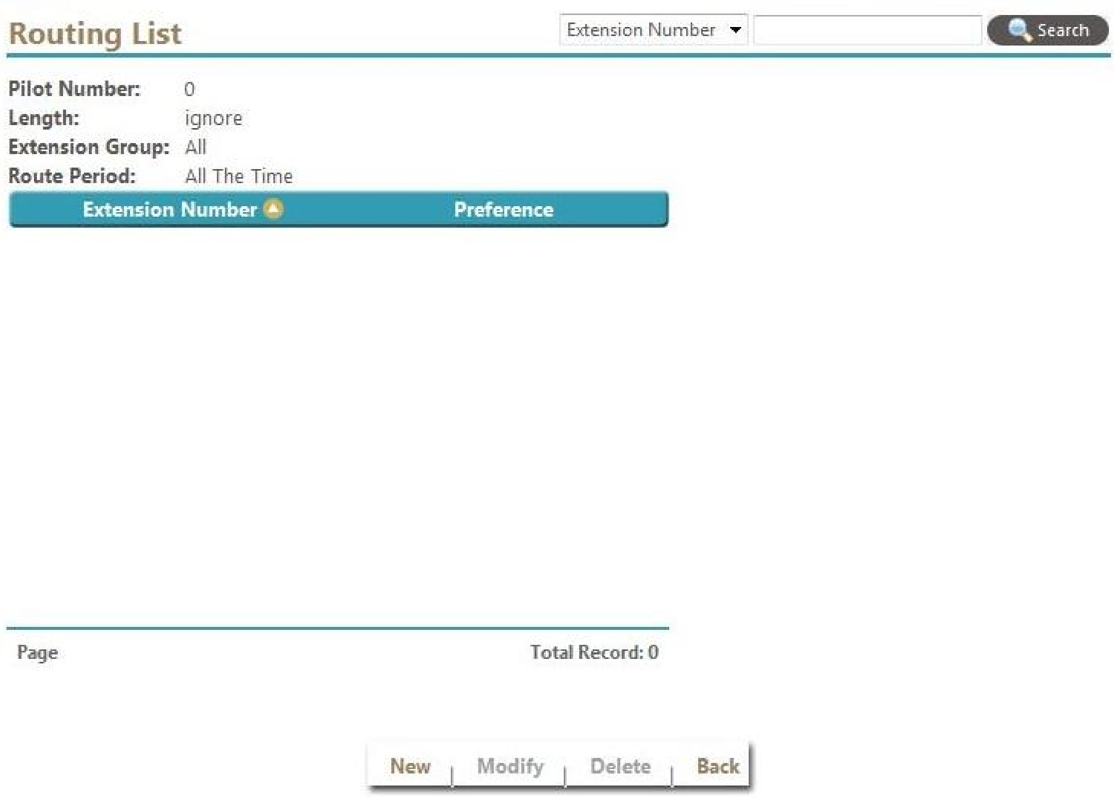
Click ***FEATURE -> Routing Plan -> New*** to create a routing plan as follows:



Input the following values to create the routing plan.

Parameter Name	Value
Routing Plan Mode	enable
Pilot Number	0
Length	ignore
Belonged Office	all
Route Period	All the time
Hunt Type	Round Robin Hunt
Remove Pilot Number	Yes

Click ***Apply*** to save it. Click ***Back*** to return the ***Routing Plan*** page. Select the created route plan and click the ***routing list*** button below. The following screen will appear.



Select ***New*** to add a routing list as below.

Input the following value to add the routing list.

Parameter Name	Value
Extension Number	1003 (PSTN gateway), 1004 (VOIP Carrier)

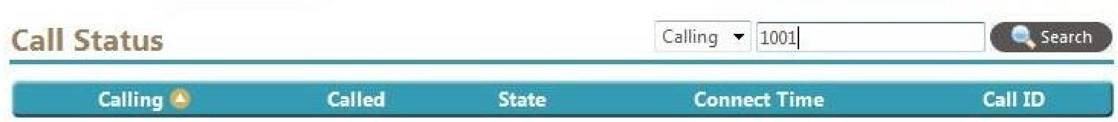
Parameter Name	Value
Preference	0

Click ***Apply*** to save it.

Click ***COMMIT*** to take effective.

1.14 Make a PSTN Call

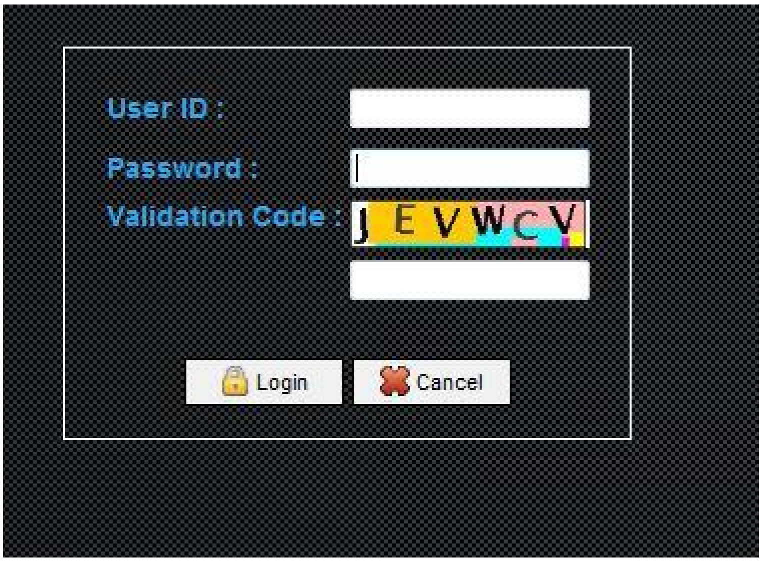
Use extension 1001 or extension 1002 to dial the 002123456 (this number should be replaced to your own telephone number). If everything is getting smoothly, your phone should ring and you should able to answer it and talk. To confirm the calls status from the system, click DIAGNOSTIC -> Call Status and the following screen will appear.



Input 1001 and 1002 as above for the search criteria, click ***Search*** button. You should see a call which is calling from 1001 or 1002 and called to your telephone number in the list. If you don't see the call in the list, there are some other issues need to be resolved.

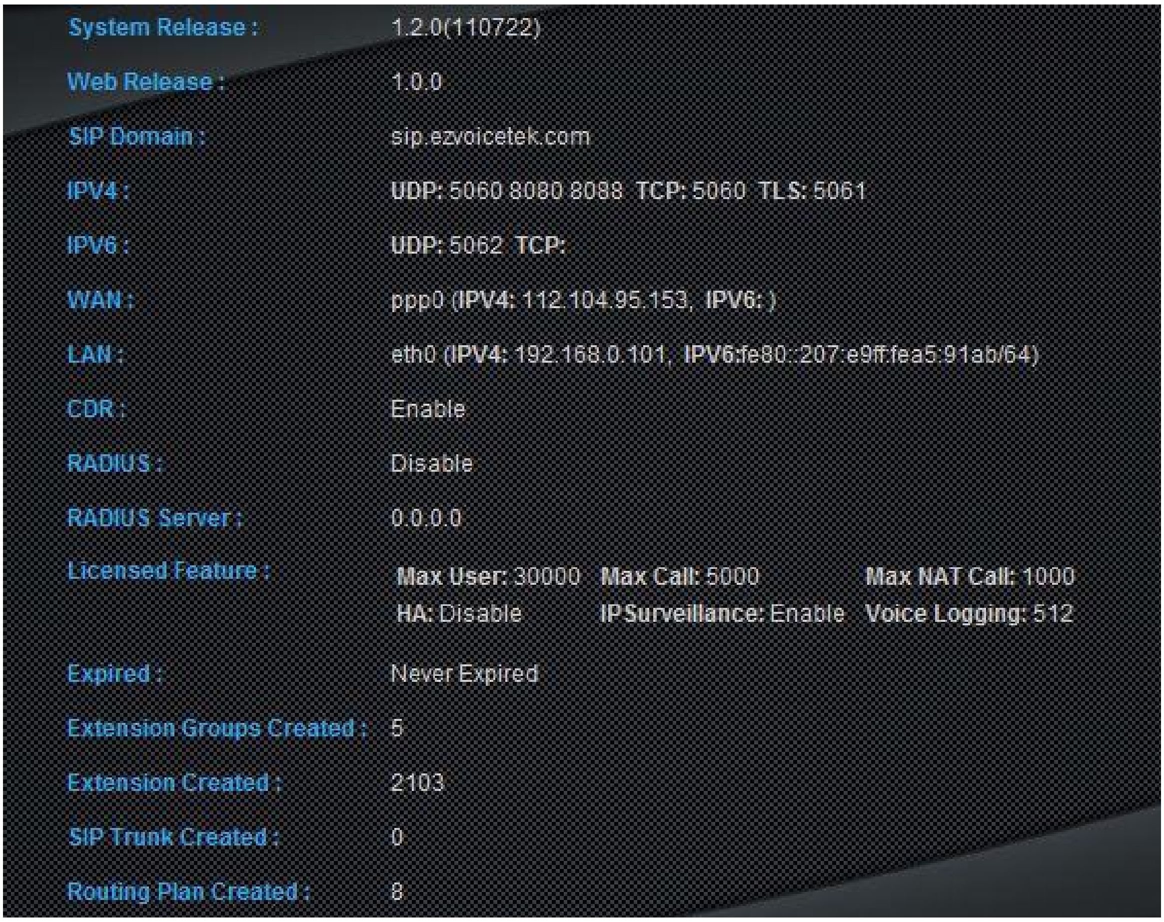
2 Using the System

The administrator can logon the web GUI interface to manage the system service. It provides the sip service provisioning, real time system status monitor and system statistic report. The default login URL for administrator login is http://xxx.xxx.xxx.xxx:9200 (or https://xxx.xxx.xxx.xxx:9201) and default login id is "admin" and password is "admin".



2.1 Home

The home page of the system, provides the system summary information. The administrator can have a quick way to view the major system settings.



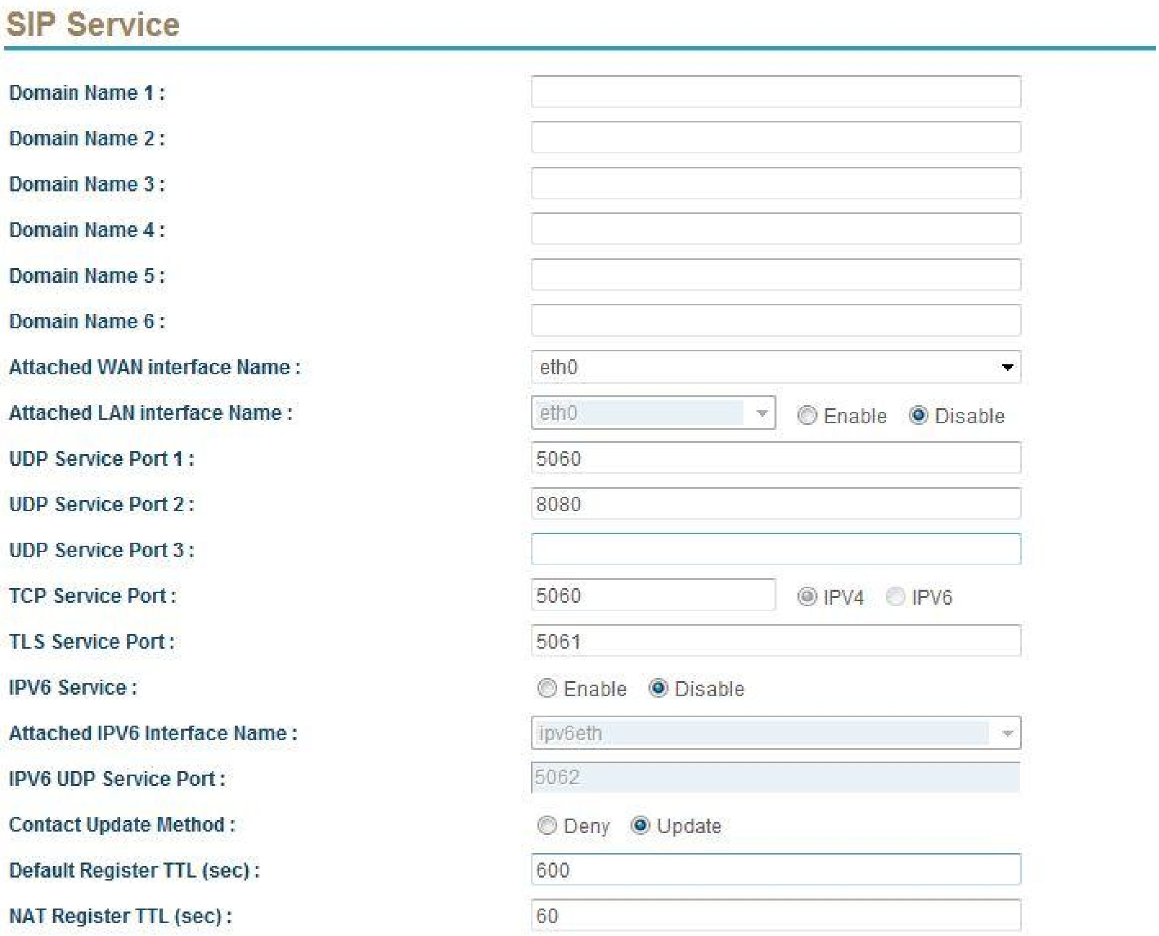
The detail of each parameter are described as below:

Parameter Name	Description
Product Name	The product name
System Release	The current running system release
Web Release	The current running web release
Sip Domain	Accepted SIP domain or FQDN of the system
IPV4	IPV4 SIP service status
IPV6	IPV6 SIP service status
WAN	WAN interface name and current IP
LAN	LAN interface name and current IP
CDR	Call Detail Record Status

Parameter Name	Description
RADIUS	RADIUS Settings
RADIUS Server	RADIUS Server
Licensed Feature	Licensed Feature
Expired	License Expires Date
Extension Groups Created	Current created Extension Group
Extension Created	Current created Extension
Sip Trunk Created	Current created SIP Trunk
Routing Plan Created	Current created Routing Plan

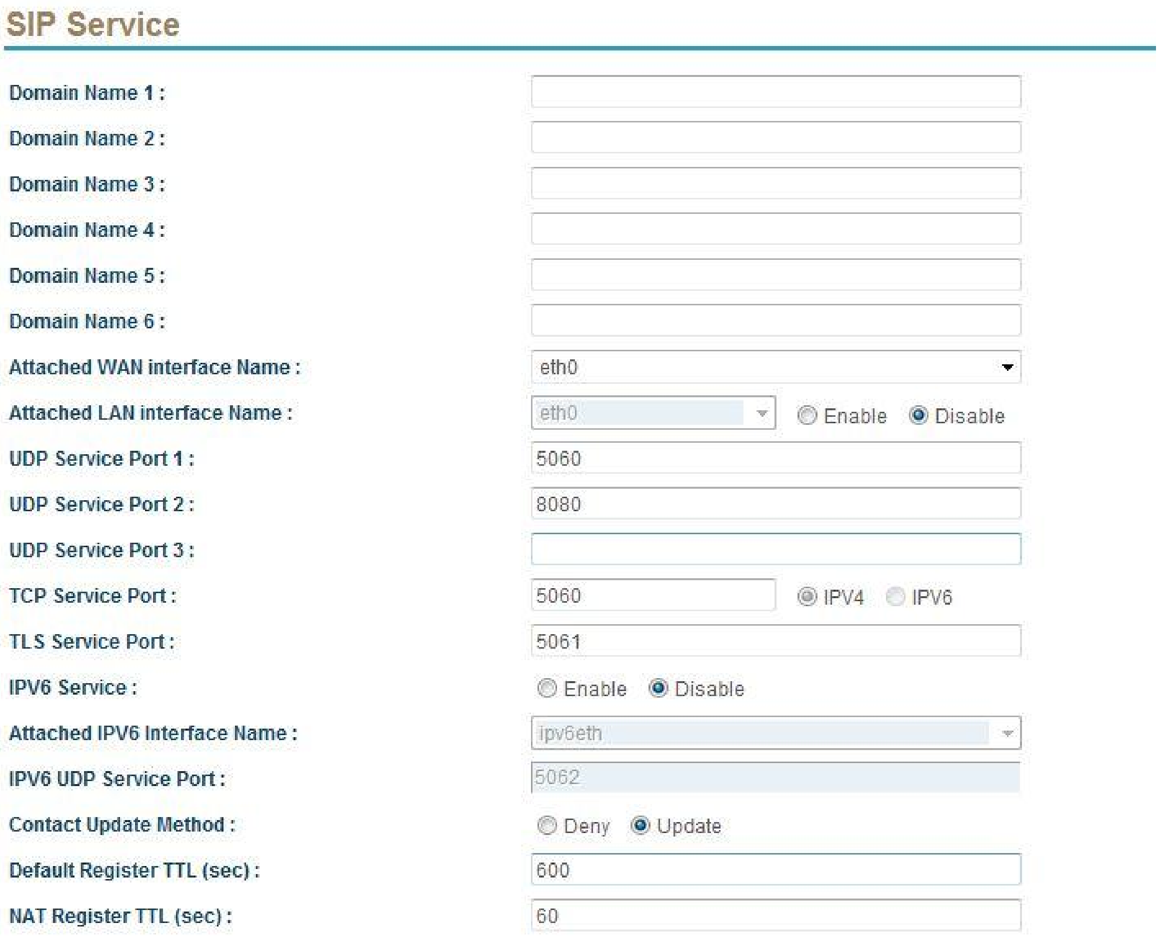
2.2 System

The system parameters including the SIP, RADIUS, system and license settings. Click the SYSTEM and will see the setting in the left panel as follows.



2.2.1 SIP Service

The SIP Service page is the main configuration for SIP core. Click ***SYSTEM -> SIP Service*** to view and change the settings.



The detail of each parameter is described as below:

Parameter Name	Description
Domain Name 1-6	Accepted SIP domain or FQDN of the system
Attached WAN interface Name	If system acts as a SIP router, WAN interface indicates the Ethernet leg connected to public IP network. If system is used only in private network (behind NAT), this interface indicate the service Ethernet leg. The default value could be eth0.
Attached LAN interface Name	If system acts as a SIP router,LAN interface indicates the Ethernet leg connected to private local network. If system is used only in private network (behind NAT), this interface should keep empty cause WAN will be the main service Ethernet. The default value could be eth1.

Parameter Name	Description
UDP Service Port 1	IPV4 UDP port used for SIP service. The default value is 5060.
UDP Service Port 2	IPV4 UDP port used for SIP service. The default value is 8080.
UDP Service Port 3	IPV4 UDP port used for SIP service
TCP Service Port	TCP port used for SIP service. It could be either IPV4 or IPV6. The default value is 5060.
TLS Service Port	IPV4 TCP port used for SIP TLS service. The default value is 5061.
IPV6 Service	Enable IPV6 SIP service or not
Attached IPV6 Interface Name	The Ethernet interface will be used or IPV6 service.
IPV6 UDP Service Port	IPV6 UDP port used for SIP service.
Contact Update Method	Choose "deny" to reject the new register request when the account reached the max allowed contact. Choose "update" to accept the new register request and remove the oldest one. The default value is "update".
Default Register TTL	The default register time to live (expires) in seconds for a user coming from public network. The default value is 600 seconds.
NAT Register TTL	The default register time to live (expires) in seconds for a user coming from behind IP sharing box. The default value is 60 seconds.
Default TCP Register TTL	The default register time to live (expires) in seconds for a user coming from public network by using SIP TCP. The default value is 1800 seconds.
NAT TCP Register TTL	The default register time to live (expires) in seconds for a user coming from behind IP sharing box using SIP TCP. The default value is 600 seconds.

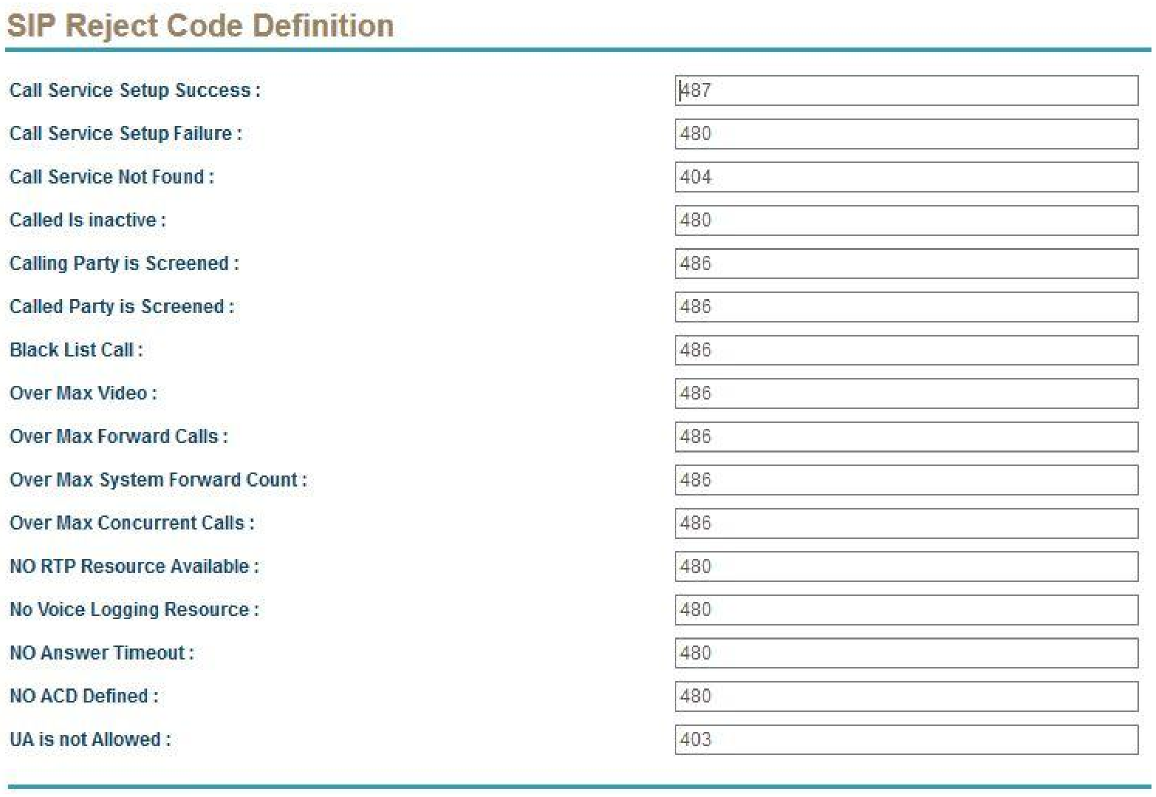
Parameter Name	Description
Max Forward Count	The max forward counts for a call to be forwarded. When it reach the count, the forward setting will be ignored. The default value is 5.
Max Forward/ Transferred Call	The system wide max allowed forward or transferred calls. It is recommended to set it to 2 or 5 instead of unlimited.
SIP User for a Forwarded Call	SIP user part of "FROM" header for a forwarded call. When select "original caller", the SIP user part of "FROM" header will be caller's user. Or the forwarded user will be used. The default value is "forward user".
SIP Display Name for a Forward Call	SIP Display Name of "FROM" header for a forwarded call. When select "original caller", the SIP Display Name of "FROM" header will be caller's user. Or the forwarded user will be used for the SIP display name. The default value is "original caller".
Send 423 Interval Too Brief	Whether to send 423 "interval too brief" when receive a register which expires is smaller than the default time to live. The default value is "disable".
INVITE-Initiated Dialog Event Pattern	The RFC 4235 Dialog Event Package Status Notify Code
Unavailable	Notify State code when the user is not registered. The default value is "void".
Idle	Notify State code when the user is not registered and has no calls. The default value is "terminated"
Ringing	Notify State code when the user is not registered and is ringing. The default value is "early".
Connect	Notify State code when the user is not registered and is talking. The default value is "confirmed"
SIP Service Socket Receive Buffer	The maximum sending buffers in bytes for the SIP service socket.
SIP Service Socket Send Buffer	The maximum receiving buffers in bytes for the SIP service socket.

2.2.1.1 TLS Certficate Upload

This is used to upload the SIP required TLS certificate. Click TLS Certificate Upload button to upload the certificate for SIP TLS service.

2.2.1.2 SIP Reject Code

This is a mapping table for SIP Proxy reject reason code.

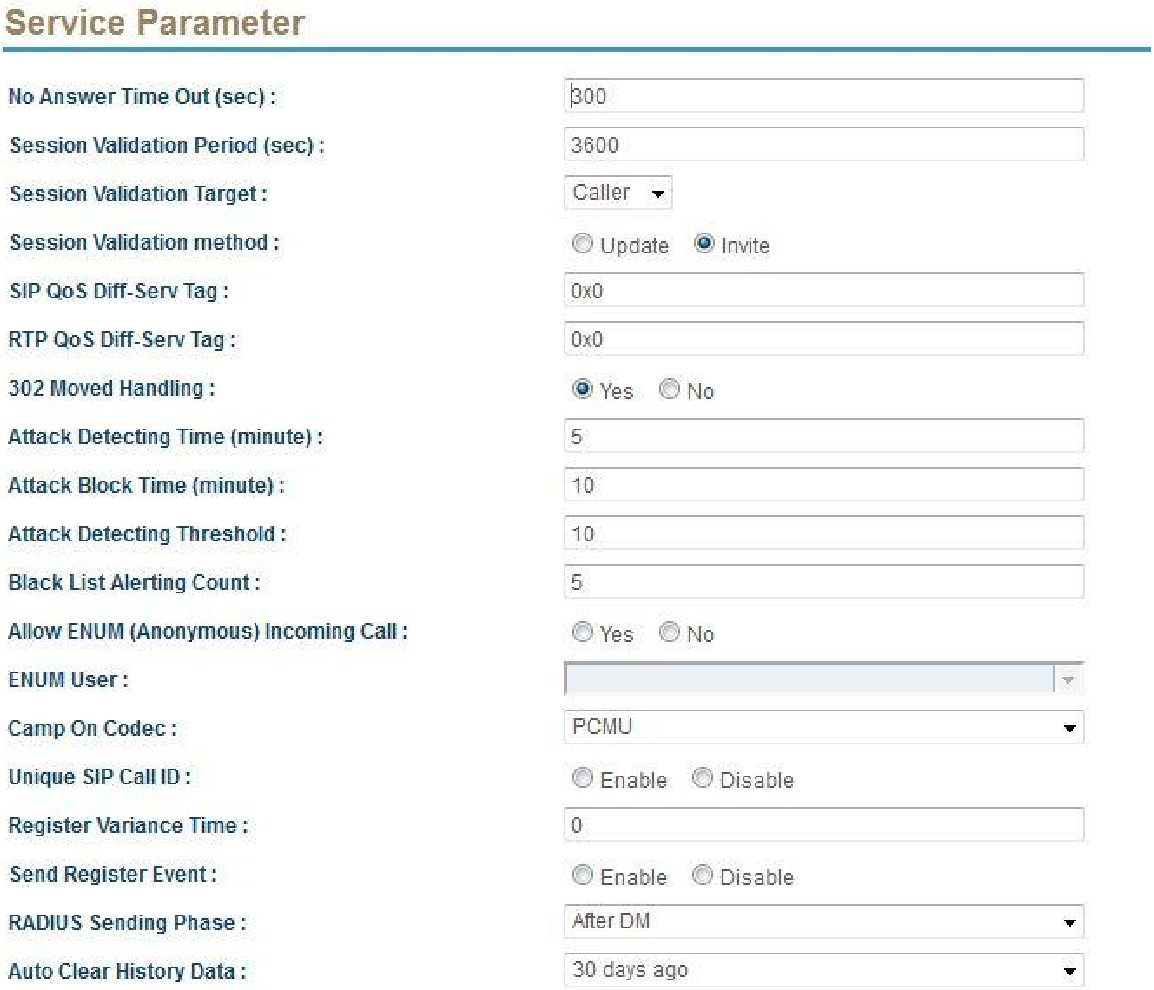


The detail of each parameter is described as below:

Parameter Name	Description
Description for SIP Reject Reason	The description of SIP reject reason. Please contact FAE if need more inmation
SIP Reason Code	Which reason code will be return to CPE

2.2.2 Service Parameter

The Service Parameters including some default setting of SIP service. Click ***SYSTEM -> Service Parameter*** to view and change the settings.



The detail of each parameter is described as below:

Parameter Name	Description
No Answer Time Out	The default time to wait for the called party to answer. The recommended value is 300.
Session Validation Period	The time to check whether the call is still connected or not. The default value is 3600 seconds which will check the call around 30 minutes.
Session Validation Target	The calling or called party will be checked for the call existence. The default value is caller.
Session Validation method	The SIP request method to be used for checking the call existence. The default value is "Invite".

Parameter Name	Description
SIP QoS Diff-Serv Tag	The DiffServ tag used for SIP signaling. The default value is 0 which means no QOS tag is used.
RTP QoS Diff-Serv Tag	The DiffServ tag used for RTP packets. The default value is 0 which means no QOS tag is used.
302 Moved Handling	When system receive a 302 moved response, send it back to original caller if it is set to "No". When it is set to "Yes', the system will initiate a call to the moved target. The default value is "Yes".
Attack Detecting Time (minute)	The system will detect the SIP attack by using the "Attack Detecting Time" as a period. Within this period, if the SIP attacks were found and the count is more than the "Attack Detecting Threshold", this attacking IP address will be add to the blocked IP address until "Attack Block Time" is reached. The default value is 5 minutes. The recommended value is 3-5 minutes.
Attack Block Time (minute)	The system will detect the SIP attack by using the "Attack Detecting Time" as a period. Within this period, if the SIP attacks were found and the count is more than the "Attack Detecting Threshold", this attacking IP address will be add to the blocked IP address until "Attack Block Time" is reached. The default value is 10 minutes. It is recommended not shorter than 10 minutes.
Attack Detecting Threshold	The system will detect the SIP attack by using the "Attack Detecting Time" as a period. Within this period, if the SIP attacks were found and the count is more than the "Attack Detecting Threshold", this attacking IP address will be add to the blocked IP address until "Attack Block Time" is reached. The default value is 10.
Black List Alerting Count	If call to a blocked black list in routing plan and over the count defined here within a day, a system alert will be written to system alert report and send to administrator.
Allow ENUM (Anonymous) Incoming Call	Whether allow to accept anonymous calling? This need to be enabled if you are using ENUM and want to accept the ENUM calls. Also it is necessary to setup

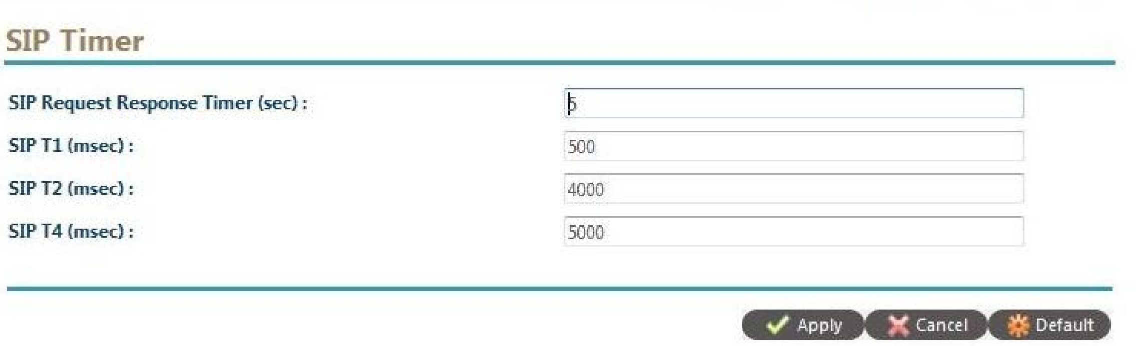
Parameter Name	Description
	the ENUM user and its DNIS screening in order to protect your network will not be attacked by any SIP caller.
ENUM User	This is the user will be used for ENUM incoming call in order to protect the system against the sip attack by taking the advantage of ENUM. You should set the proper DNIS screening for this user.
Camp On Codec	This is the codec will be used for camp on. The system will use this codec to call both parties.
Unique SIP Call ID	Whether enable the Unique SIP call ID for each call or not. It is related to parallel ringing case. The device might reject the second call when using same SIP call ID. Please contact FAE for usage. The default is OFF.
Register Variance Time	The max time in second to remove the extension from registered table after register expired. The register should normally be refreshed before expires.
Send Register Event	Whether to send register status through system alert sub-system or not when the feature of Monitor Register Status was turned on for an extension. When it is enabled, the event will be write to system alert and send to administrator by settings.
RADIUS Sending Phase	Whether to send RADIUS authorization or billing message based on original digits (before DM) or modified digits (after DM).
Black List DNIS Screening Group	When a black list calls was called and over the Black List Alerting Count, this DNIS screening group will be applied if you select. Normally, when a black list was called, it might be a SIP attack and it is recommended to use a more restricted DNIS screening group to have more protection on your service from fraud calls.
Disconnect Existing Calls when Black List was Detected	When a black list calls was called and over the Black List Alerting Count, whether disconnect all existing calls for this user or not. To enable this can avoid the SIP attacker to call those expensive calls but not in your black list.

Parameter Name	Description
Send New Replaced Invite to Transferee	Whether to send a new replaced Invite to transferee or not?
Use Global No Answer Timeout When No Answer Services were not Set	When it enabled and no answer forward was not enabled, the global no answer forward will be used, otherwise user's no answer forward will be used.
Disconnect Call When Reinvite Failed	Whether to disconnect the call when reinvite is failed or not?
Enable Talk Time Roundup	Whether to enable the rounding for talking time or time. If it is enabled, the talking time will be round-up which means 1.01 will become 2.
Server Transfer SDP	SDP will be used when starting a server based transfer.
Find Extension Before DM	Whether enable to find extension before DM or not? If it is enabled, the system will try to find extension before DM and after DM.
IP Look Up Server	The server URL to be used to look-up the IP belonged country.
Match String	The matched keyword from server's response.
Look up Mode	The supported IPV4 or IPV6 look up mode for this server.
Enhanced Password	When it was enabled, the system will ask more higher level of security password. It will require to have the following.To avoid the SIP attack from your system, it is recommended to turn it option ON. 1. minimum password length is 8 2. at least one symbol (except digit password) 3. at least one digit 4. at least one alphabet (except digit password)
Hide Charge Amount In Billing Report	Whether show Charge Amount in billing report or not? If it is enable, the charge amount will be hided.
Auto Clear History Data	Whether to enable the automatic database cleanup or not. It is enabled, the system will clean those historical data (except call detail record) automatically based on your setting.

Parameter Name	Description
Talking RTP Timeout	The RTP Timeout for voice calls. If system doesn't receive any RTP for any side, the call will be dropped.
Video Talk RTP Time Out	The RTP timeout for video calls. If system doesn't receive any RTP for any side, the call will be dropped.
On-Hold RTP Timeout	The RTP timeout for on-hold call state
Video RTP Socket Receive Buffer	The socket receiving buffer for video calls
Video RTP Socket Send Buffer	The socket sending buffer for video calls
Internal Call Alert-Info Value	Distinct ringing used Alert-Info header value for internal extension call
External Call Alert-Info Value	Distinct ringing used Alert-Info header value for non-internal extension call

2.2.3 SIP Timer

There are some SIP related timer in this page for system tuning purpose. Click ***SYSTEM->SIP Timer*** to view and modify the settings.



The detail of each parameter is described as below:

Parameter Name	Description
SIP Request Response Timer	The time to wait for a response when send out a SIP request. The default value is 5 seconds.

Parameter Name	Description
SIP T1	The T1 timer, which is defined in milliseconds, specifies the amount of round trip time (RTT), that the client will attempt to send a SIP Request and expect a response. By default, the T1 timer is set to 500ms.
SIP T2	Maximum retransmission interval for non-INVITE requests and INVITE responses. The default value is 4000 ms.
SIP T4	Maximum duration that a message can remain in the network. The default value is 5000 ms.

2.2.4 RADIUS

To enable RADIUS authorization and accounting message for prepaid/postpaid billing service, it is required to setup the RADIUS service parameter here. Please note that the RADIUS authorization request will be sent after caller DM and before called DM. The RAIDUS start/stop billing request will also send the same calling/ called number as RADIUS authorization request to make it consisted.

Click ***SYSTEM -> RADIUS*** to view and change the settings.

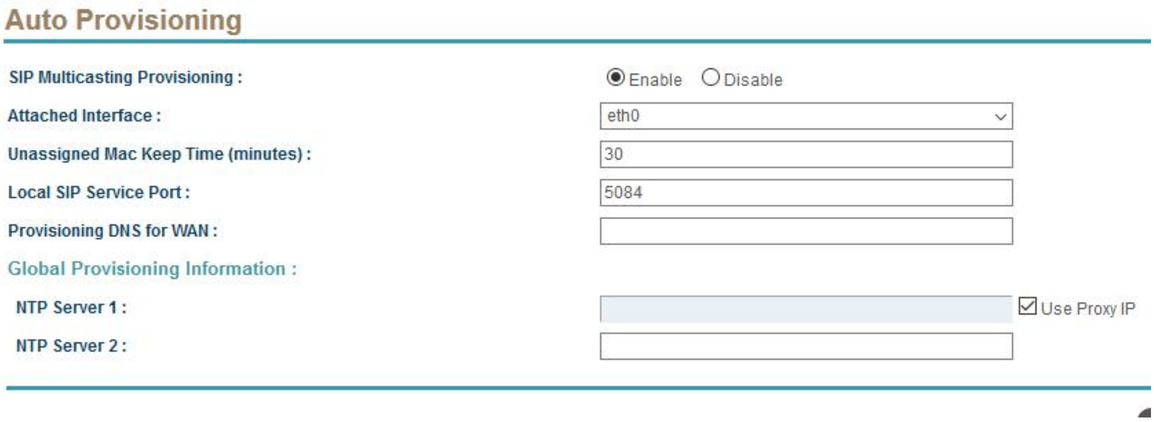
The detail of each parameter is described as below:

Parameter Name	Description
RADIUS	Enable RADIUS authorization and accounting or not. Administrator need also turn on RADIUS call authorization from extension in order to let system send the RADIUS authorization to RADIUS server when the extension calling. The default value is disabled.
RADIUS Server	RADIUS Server to be used for sending authorization and accounting message.
RADIUS Server Authorization Service Port	The UDP port of RADIUS Server to receive the RADIUS authorization request. The default value is 1812.
RADIUS Server Accounting Service Port	The UDP port of RADIUS Server to receive the RADIUS accounting request. The default value is 1813.
Local RADIUS Binding Port	The local binding port for RAIDUS server. The default value is 1812.
RADIUS Vender ID	The RADIUS vender attribute . The default value is 9 (CISCO).
Shared Secret Key	The share secret to be used in between RADIUS server and system.
RADIUS Server Response Time out (sec)	The time in seconds to wait the response from RADIUS server when send out a RADIUS request. The default value is 10 seconds.
Inter-Extension Call Authorization	If it is set to "No", the system will not send out a RADIUS authorization when a extension calls to another extension. The default value is "No".
RADIUS Billing	Enable to send RADIUS billing out to server or not. The default is "Disable".
Send Unconnected Call	Whether to send a RADIUS accounting message for a unconnected call or not. The default is "Yes".
Inter-Extension Call Billing	Whether to send a RADIUS accounting message When a extension calls to another extension. The default is "No".
RADIUS Start Billing	If it is set to "No", the system will not send out the RADIUS billing start when a call is connected. Only RADIUS billing stop will be send after the call is disconnected. The default value is "No".

Parameter Name	Description
Database CDR	If it is enabled, the system will do the local billing calculation. It will store call detail into local database and use the tariff plan to calculate the charge amount. And you will able to see the top usage or division report from the Billing.

2.2.5 Auto Provisioning

The system can support CPE auto provisioning. Please contact technical support for supported model. Click SYSTEM -> Auto Provisioning and the following will appear:



Parameter Name	Description
SIP Multicasting Provision	Whether to enable SIP multicasting (SIP pnP) for searching SIP provisioning server or not.
Attached Interface	Which interface will be serviced for SIP multicasting service. Because normally multicasting package cannot over layer 3 network. Thus this is normally service at LAN interface.
Unassigned Mac Keep Time (minutes)	How long the unassigned mac address will be kept in the system for assignment? Within this period, the unassigned mac with line ID will be found in the Diagnostic -> Unassigned Mac List
Provisioning DNS for WAN	When this parameter was set, the provisioned config URL will be used for this DNS name instead of IP address.
NTP Server 1/2	The NTP server 1 will be used for CPE. Check User Proxy IP if SIP proxy or PBX do provide NTP service.

2.2.6 CDR

Call detail record (CDR) can be turn on or off here. Click ***SYSTEM -> CDR*** to view and change the settings.

The detail of each parameter is described as below:

Parameter Name	Description
CDR Logging	Whether to enable the CDR recording or not. The default value is Yes.
CDR Keeping Days	How long the CDR will be kept int he system.
Syslog CDR	Whether to turn on to send real time CDR record to syslog server or not?
Syslog Server IP	The syslog server to be send for real time CDR record. Empty means not send.

2.2.7 Web Service

This page come with web GUI service settings. Click ***SYSTEM -> WEB Service*** to view and change the settings.

The detail of each parameter is described as below:

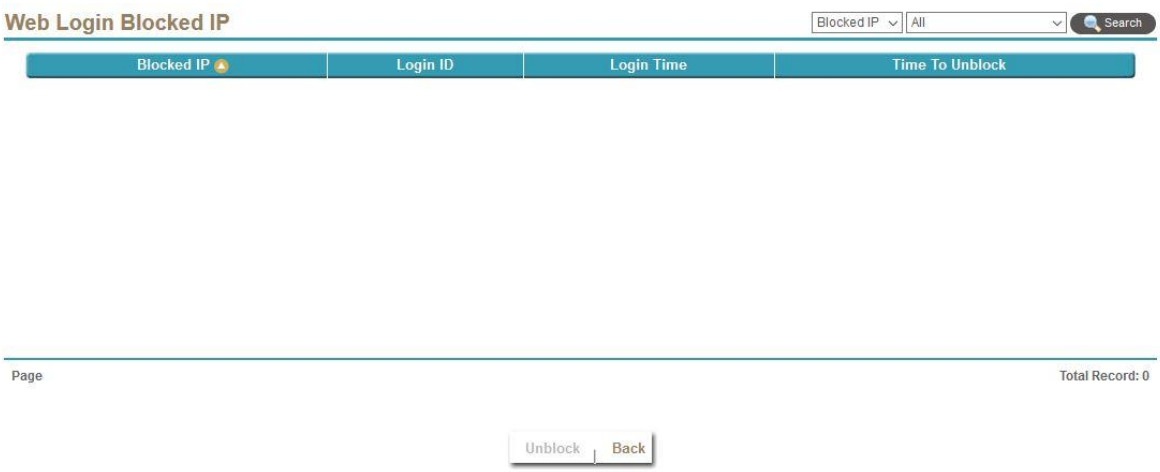
Parameter Name	Description
HTTP Service Port	The TCP service port for web GUI management. The default value for administrator and supervisor login is 9000. The default value for extension login is 80.
HTTPS Service Port	The TCP service port for HTTPS (SSL) web GUI management. The default value for administrator and supervisor login is 9001. The default value for extesnion SSL login is 443.
Display Data Rows per Page	Number of data rows will be displayed per page. The default is 15.
SOAP Provisioning Service	The HTTP or HTTPS interface for SOAP provisioning for extension and call features. It is recommended to use HTTPS for security reason. The default service port is TCP 8080.
Log Data Keeping Days	How long the system log data will be clean automatically in days?
Auto Provision Service Port	The service port for auto provisioning URL. The default port is 9999.

Parameter Name	Description
Use Validation Code on Login	Use CAPTCHA to against the response is not generated by a computer or not for logon. It is recommended to enable it for security reason.
Extension Web Language	The default web language will be used when a extension is login.
Write Access Log Count	Number of authentication failure will be written to Web provisioning report.
Block Access IP Count	Number of authentication failure will block this IP address.
Block Access IP Time (minutes)	How long the IP address will be blocked.

Click SSL Certificate Upload to upload the HTTPS certificate.
Click Reset Web to restart web service.
Click Customize Web Logo to have customer required logo or others.

2.2.7.1 Web Login Blocked IP

Here show the blocked IP for the web. When the system blocked an IP for attempting login, you can unblock here. Click Web Service -> Web Login Blocked IP and the following will appear:



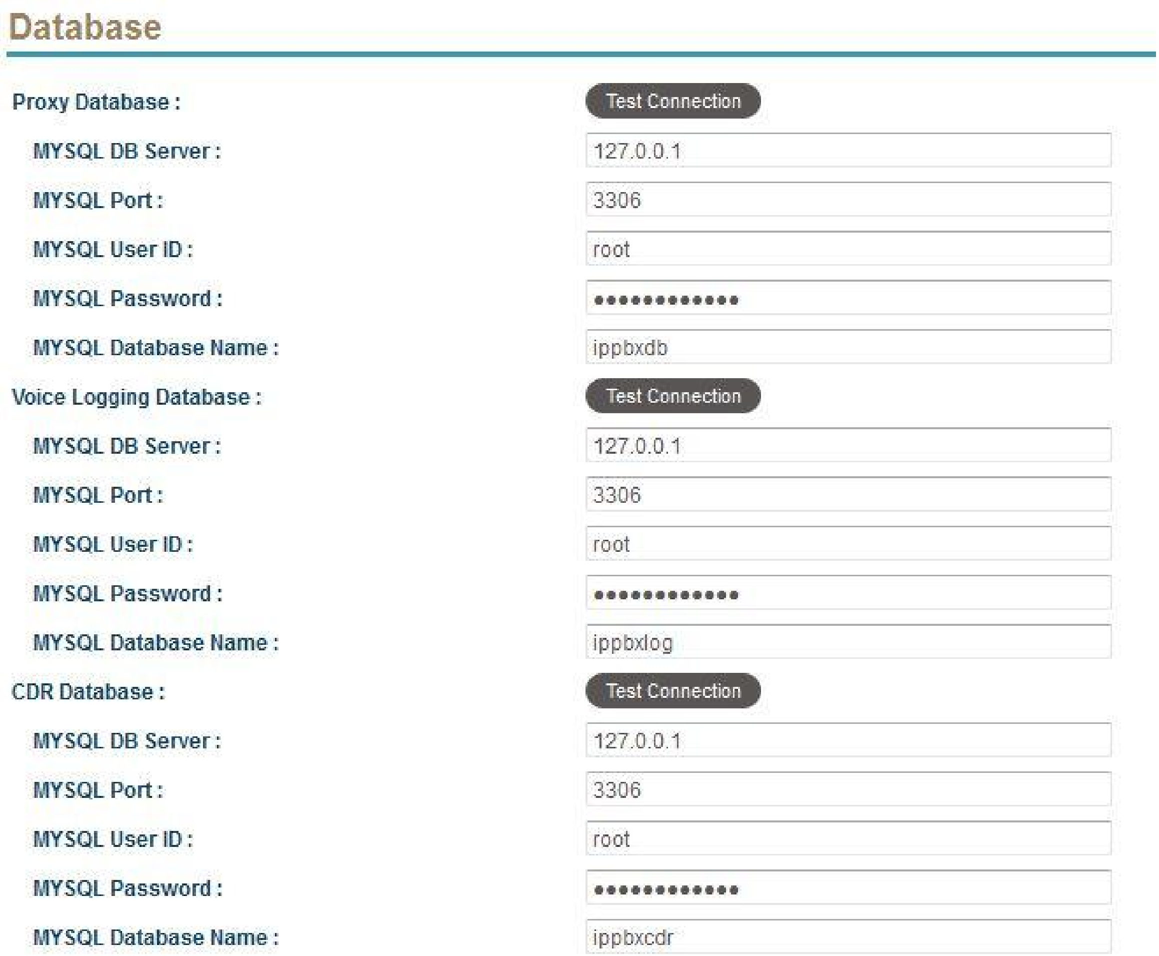
The detail of each parameter is described as below:

Parameter Name	Description
Blocked IP	The IP was blocked because of failed login

Parameter Name	Description
Login ID	The ID was tried for the failed login
Login Time	The time was blocked
Time to Unblock	The time will be unblocked

2.2.8 Database

This is for system database settings. Click ***SYSTEM -> Database*** to view and change the settings.

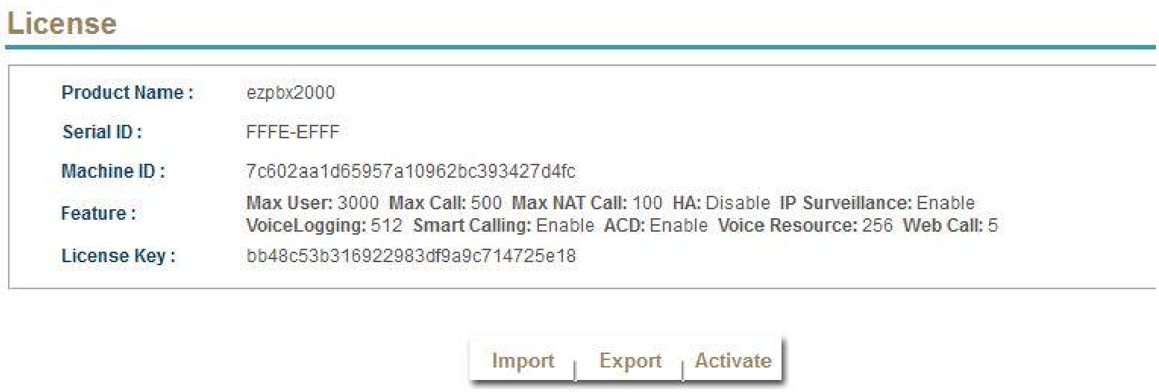


The detail of each parameter is described as below:

Parameter Name	Description
MYSQL DB Server	MYSQL database server IP address. The default value is 127.0.0.1
MYSQL Port	MYSQL database connection port. The default port is 3306.
MYSQL User ID	MYSQL access user ID
MYSQL Password	MYSQL access password
MYSQL Database Name	MYSQL Database Name

2.2.9 License

This the license granted for the system. It can only be used on this dedicate machine. There is no any responsibilities for error, omissions or any damages resulting from the wrong use of the license. Click ***SYSTEM -> License*** to view or import/export the license.



The detail of each parameter is described as below:

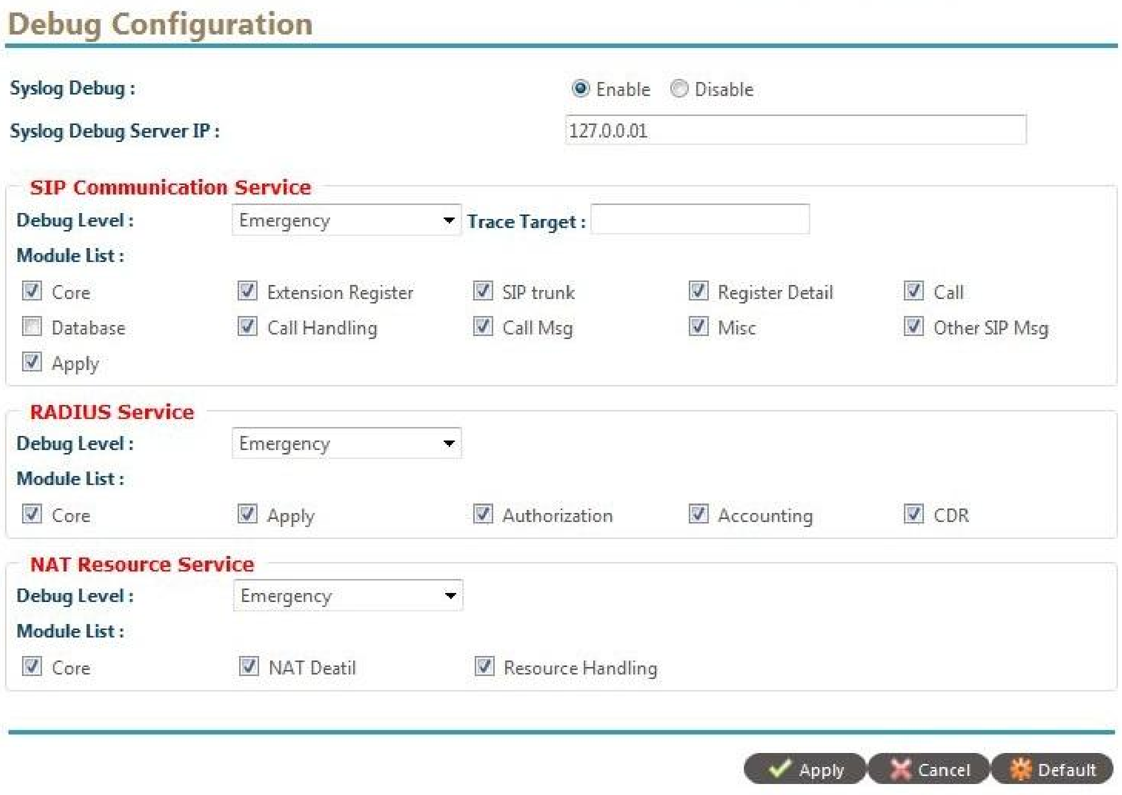
Parameter Name	Description
Product Name	The licensed product name
Serial ID	The serial ID generated for each license
Machine ID	The machine ID used for the license
Feature	The feature list of this license

Parameter Name	Description
License Key	The license key generated
Expired Date	The expired date for the license

Click Import to upload a granted license, Export to download a existing license. Click Activate to active a granted serial number license. Click Deactivate to deactivate a serial number in order to move to other server.

2.2.10 Debug

The Debug Configuration page is used to manage the debug level and modules. Please only turn on the debug level under the recommendation from supporting FAE. Or the system performance might be greatly affected. In order to receive the system debug log, the administrator need prepare a PC which installed a SYSLOGD server. It is recommended that both server and syslogd PC stay at same network because of the large packet might be send over the network. Click ***SYSTEM -> Debug*** to view and change the debug settings.



The detail of each parameter is described as below:

Parameter Name	Description
Syslog Debug	Enable syslog debug or not
Syslog Debug Server IP	The syslogd server to receive the debug information. The port to receive the syslog is 514.
Trace Target	The target to be used for debugging. It could be the telephony number or IP address. You can combine it by using a semicolon to separate it. For example, you can have the trace target as "02123456;112.112.1.1" which indicates the debug message will contains the calling or called number is 02123456 or IP address is 112.112.1.1.
Debug Level	This parameter is the detail level of generating debug information. The default level is "Warning". When you change it to debug, the system will generate hug log and might greatly affect the system performance. Please only change it under the supervision of FAE.
Module List	The target module to be debug. Please only change it under the supervision of FAE.

2.2.11 System Alert

The system can be set to automatically send the system event notice to administrator through syslog or email. Click ***SYSTEM -> System Alert*** to view and change the settings.

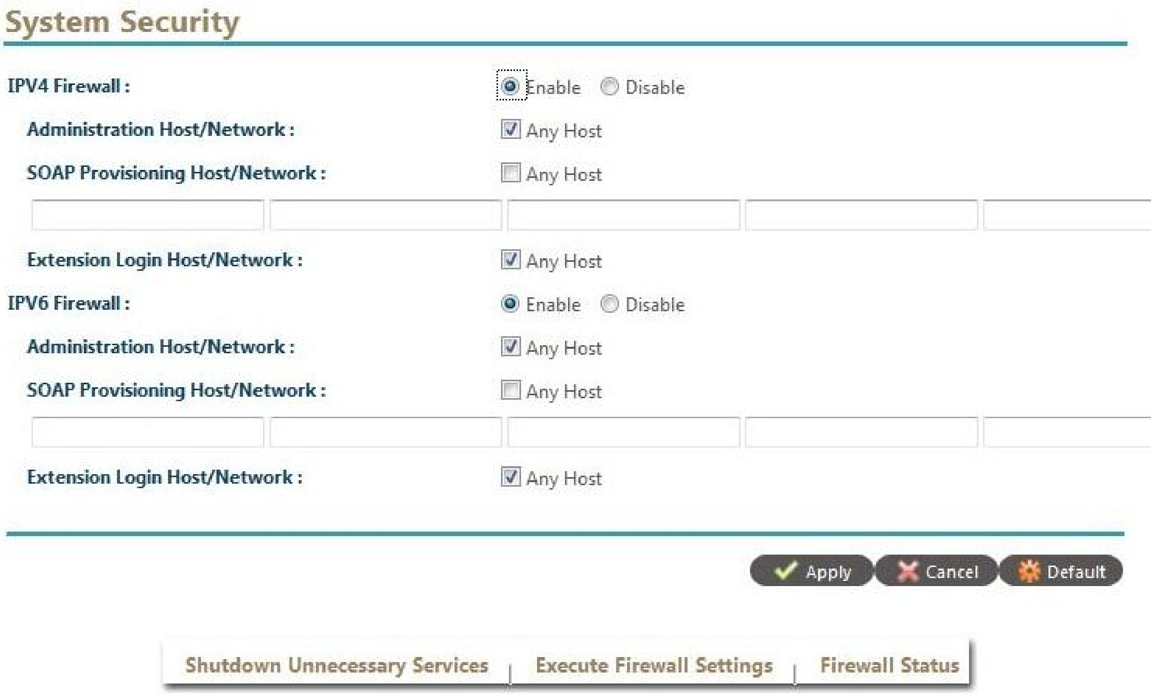
The detail of each parameter is described as below:

Parameter Name	Description
System Alert Threshold	The filter level to send the alert out. The default is level of "Notice".
Alert to Syslog	Whether to send the system alert to syslogd server or not.
Syslog Receiver IP	The syslogd server to receive the system alert.
Alert to Email	Whether to send the system alert to the listed email account or not.
SMTP Server	The SMTP server for sending the system alert mail notice.
SMTP Port	The SMTP server port. For SSL the default is 465 and for StartSSL or none, the default is 25.
SSL Type	The SMTP server supported SSL Type, it can be none, STARTTLS or SSL.
Email From	The email sending account (FROM)
Email To List	The email addresses to receive the system alert email.

Parameter Name	Description
Email Subject	The email subject for the system alert notice. The variable "$HOSTIP$", Host IP address, could be used in the subject to make the subject easy to be read (e.g. System Alert Notice from $HOSTIP$).
Email User ID	The email sending account ID
Email User Password	The email sending account password

2.2.12 System Security

The system integrated with Linux firewall in order to protect your system from the hacker. After input the trusted managed host and execute the firewall settings, the system will automatically create the necessary setting. Click ***SYSTEM -> System Security*** to view and change the settings.

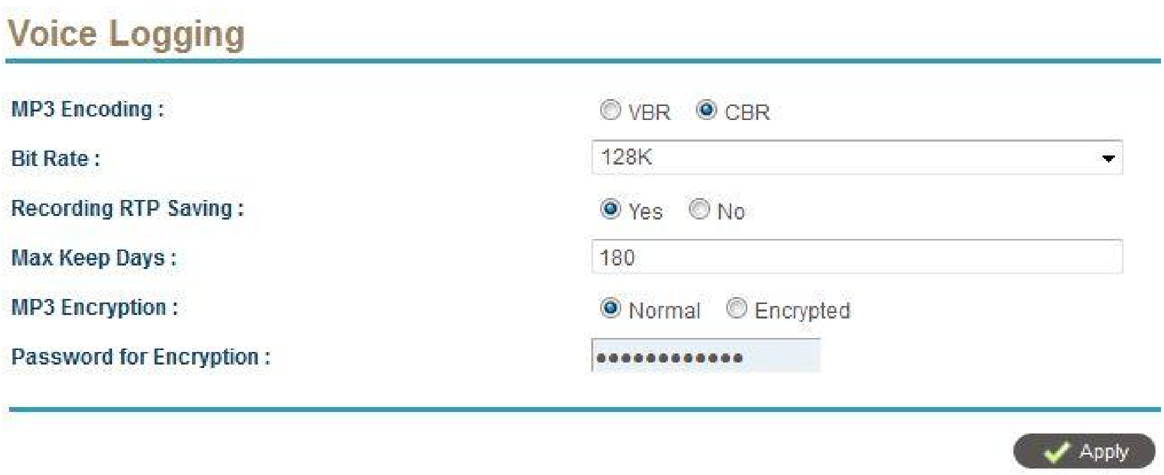


The detail of each parameter is described as below:

Parameter Name	Description
IPV4 Firewall	Enable or disable IPV4 firewall settings.
Administration Host/ Network	The trusted IP address (xxx.xxx.xxx.xxx e.g. 192.168.1.2) or network (xxx.xxx.xxx.xxx/xxx e.g. 10.0.0.1/24) to manage the server. Check Any Host to allow any host to access the administration web.
SOAP Provisioning Host/Network	The trusted IP address (xxx.xxx.xxx.xxx e.g. 192.168.1.2) or network (xxx.xxx.xxx.xxx/xxx e.g. 10.0.0.1/24) to use SOAP to provision the server. Check Any Host to allow any host to use the provisioning interface. Keeping all host blank will disallow any host to connect.
Extension Login Host/Network	The trusted IP address (xxx.xxx.xxx.xxx e.g. 192.168.1.2) or network (xxx.xxx.xxx.xxx/xxx e.g. 10.0.0.1/24) allowed to access extension login web page. Check Any Host to allow any host to use the provisioning interface. Keeping all host blank will disallow any host to connect.
IPV6 Firewall	Enable or disable IPV6 firewall settings.
Shutdown Unnecessary Services	Close those unnecessary Linux services to have maximum security. Please only used when you are very familiar to Linux system.
Execute Firewall Settings	After you set those parameters for firewall and apply it, you need to execute it to make it working. However, before you execute the firewall settings, please make sure your have applied all the settings to the system (either soft-reset or commit based on the prompt), especially for the administration HTTP and HTTPS ports. Otherwise, you might not able to access the system after execute the firewall settings.
Firewall Status	To show the current running firewall status

2.2.13 Voice Logging

The voice logging service requires additional license for running it. Please contact "Jing Jie" when you need it. The system support MP3 compression for voice logged files including VBR and CBR coding. Click ***SYSTEM -> Voice Logging*** to view and change the settings.



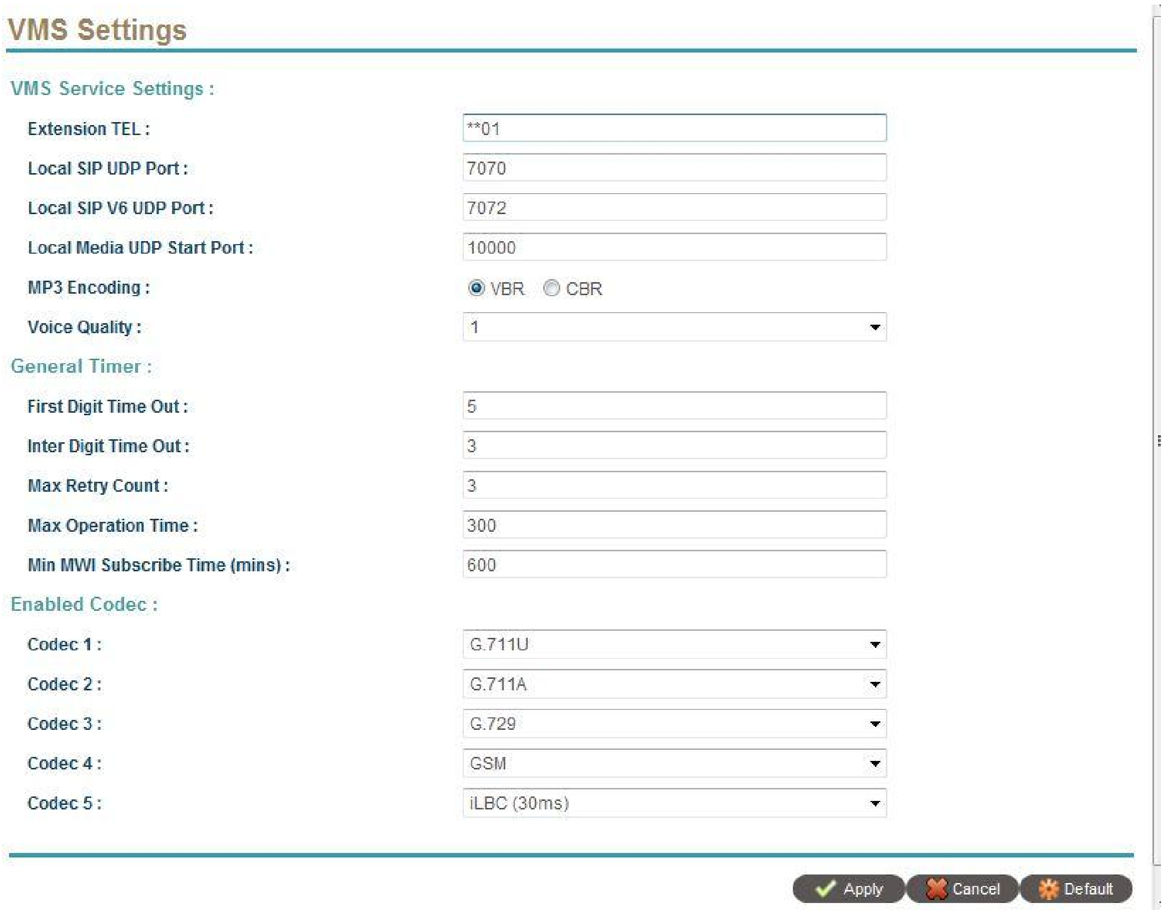
The detail of each parameter is described as below:

Parameter Name	Description
MP3 Encoding	MP3 encoding method, it could be CBR (Constant Bit Rate) or VBR(Variable Bit Rate) depending on the compression ration and quality.
Bit Rate	The selected bit rate will be used when CBR is selected.
Voice Quality	Selected voice quality when VBR is used. 0: best quality (220-260K), 9: best compress ration (45-85K)
Recording RTP Saving	Whether to save the recording RTP for future tracking or not? Turn on this feature will increase the disk usage and system performance. Please only turn on it under FAE's instruction.
Max Keep Days	The max days for storing the recorded file which is depending on the system storage capacity.
MP3 Encryption	Whether to encrypted the MP3 file or not? You can select to use system internal password or customized password.
Password for Encryption	Input encryption password when use customized password.
Recording File By Extension Group ID	Whether store voice recording files into different directory for each extension group (office)?

Parameter Name	Description
Mixed Mono Channel	Whether enable mix calling and called parties' voice into a mono channels for MP3 or not.
Recording RTP Keeping Days	The maximum keeping days for recording voice logging files.

2.2.14 VMS Settings

The VMS Settings includes the settings of voice mail system, auto attendant and conference. Click ***SYSTEM -> VMS Settings*** to view and change the settings:



The detail of each parameter is described as below:

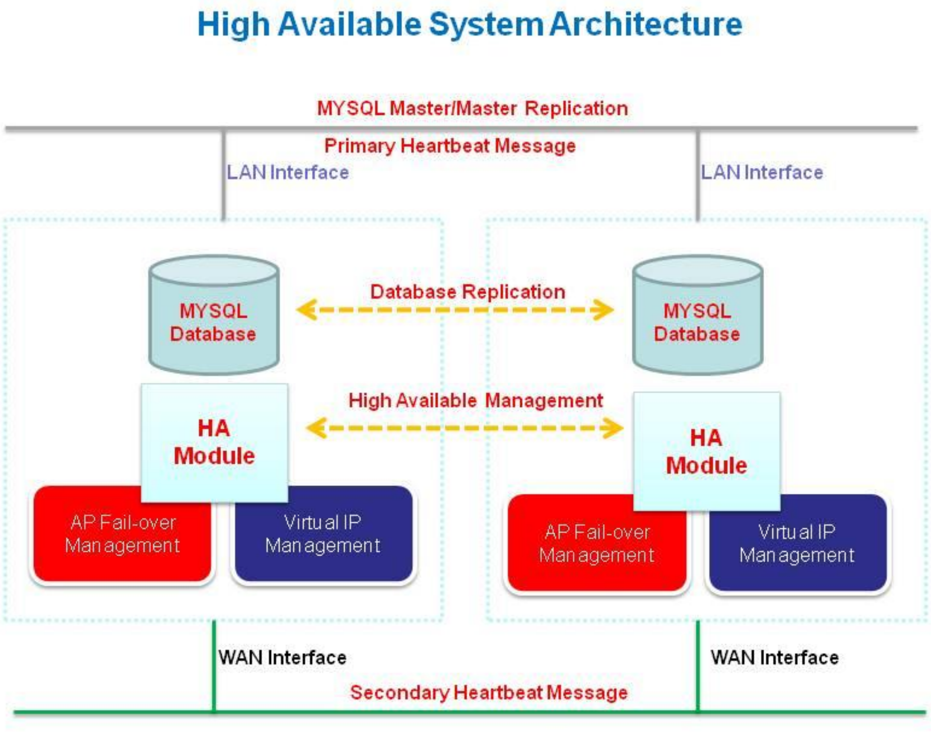
Parameter Name	Description
Extension Tel	The extension number will be used for AA, VMS and conference. It need to be an uniqe number in the system.
Local SIP UDP Port	This is local IPV4 SIP UDP port will be used for AA, VMS and conference service.

Parameter Name	Description
Local SIP V6 UDP Port	This is local IPV6 SIP UDP port will be used for AA, VMS and conference service.
Local Media UDP Start Port	The is the media UPD starting port will be used for AA, VMS and conference service. The default is 10000. It means the UDP ports will be used will be 10000 to 10000+ (Max service channel * 4).
MP3 Encoding	MP3 encoding method, it could be CBR (Constant Bit Rate) or VBR(Variable Bit Rate) depending on the compression ration and quality.
Voice Quality	Selected voice quality when VBR is used. 0: best quality (220-260K), 9: best compress ration (45-85K)
Bit Rate	The selected bit rate will be used when CBR is selected.
Call Queuing Music Prefix	The prefix need to be used to access call queuing music when you are using the call queue feature. The default value is **4.
VMS Default Office	The AA/VMS will use the default group for DM and Routing.
Outgoing Call Using Transfer	This is only for smart office feature. When it is enabled, the outgoing call from small calling will use transfer instead of bridge.
VMS Personal Greeting Max Recording Time	The maximum time in seconds for personal greeting voice file.
Voice Mail Keeping Days	The maximum voice mail file keeping days.
First Digit Time Out	After complete the playing of announcement, this is the time to wait the first digit. The recommended value is 6-10 seconds.
Inter Digit Time Out	After first digit was received, this the time to wait the incoming digit. The default is 3 seconds.
Max Retry Count	The max retry time for VMS and conference when doing the input. The default value is 3.
Max Operation Time	This is the max operation time for AA and VMS. When the user are playing AA or VMS over this time, the call will be disconnected. The recommended value is 600 seconds.

Parameter Name	Description
Min MWI Subscribe Time (mins)	The minimum time for MWI SUBSCROBE request. The recommended value is 30 minutes.
Codec 1-5	The codec will be used for AA, VMS and conference.

2.2.15 High Available

The system supports active/standby redundant mode. It relies on MYSQL database replication and high available software to build the system redundant as follows:



To make the redundant working smoothly, you need to the following to be prepared:

1. Two Ethernet network interface and use different VLAN or physical switch to separate the network traffic.
2. For each service interface and IP protocol (V4 or V6), you need to have a dedicate IP address for the server.
3. The virtual IP addresses to be used.

It supports the following high available modes:

Active/Standby Redundant for 1 Ethernet Leg

Active/Standby Redundant for 2 Ethernet Legs
Above case but IPV4 only

Some system architecture examples will be showing in the following topic. For high available, if the fail-over is happened, the call will be continue for 2-5 second silence and voice recording will became 2 separate recorded file. However, the HA will try to keep the server running on the same server as long as possible, it will only failed to the standby node when the following is happened:

1. System is crashed several times (3 times in default) without continues working for 30 seconds.
2. The machine is crashed or had hardware failure.
3. If the virtual IP cannot be added into the node.

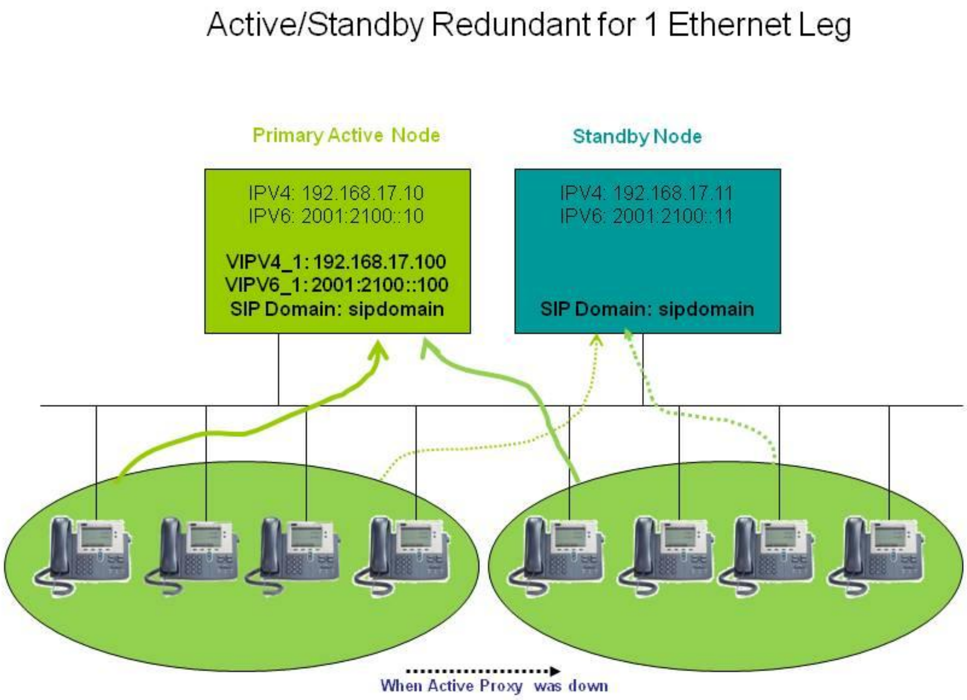
Each cluster need had an identifier which is Cluster ID. It is recommended to use different UDP broadcasting port to reduce the CPU usage for verifying each heartbeat message. You can use the default port which is port number 654 or higher than port number 60000 to avoid some port conflicts.

The following is the system requirements before you can install or start the HA service:
1. Both servers need to have 2 Ethernet interfaces which need connect to a separate Ethernet switch for redundant purpose.
2. If you are using CISCO switch, please make sure the Ethernet port's is set to become a fast port (turn off spanning tree).
3. Both servers need use NTP to synchronize the time. Otherwise the HA service will not working correctly.

Please check the above requirements before you can move on.

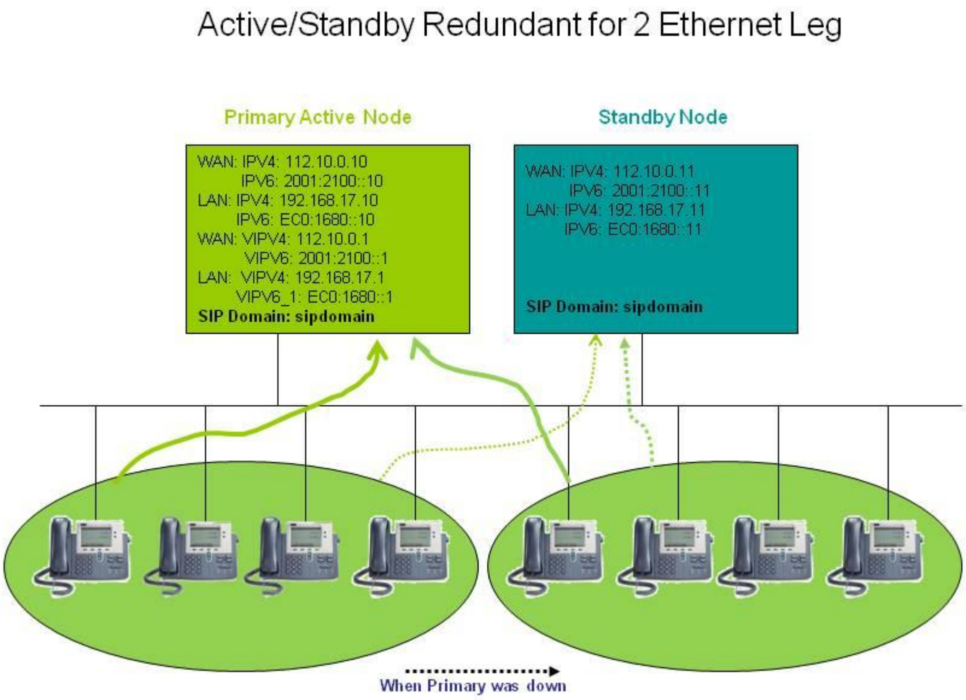
2.2.15.1 Active/Standby (1 Ethernet)

In this mode, the system is serving for WAN interface and another node is a standby node. In the normal case, the SIP CPE is register to their server through VIP. If one of the machine is down, the another peering node will taking over the VIP and continue the service.



2.2.15.2 Active/Standby (2 Ethernet)

In this mode, the system is serving for both WAN and LAN interface and another node is a standby node. In the normal case, the SIP CPE is register to their server through either WAN's VIP or LAN's VIP. If one of the machine is down, the another peering node will taking over the VIP and continue the service.



2.2.15.3 IPV4 Only Redundant

IPV4 only redundant is a simplified architecture for described above. In this mode, IP V6 is disabled.

2.2.15.4 High Available Settings

Click ***SYSTEM -> High Available*** to change the HA settings. Some other parameters might also affect the HA settings such as IPV6 enabled and Attached LAN Interface Enable/Disable. When change these parameters, you are required to change corresponding HA settings. The following is the screen of settings.

Parameter Name	Description
Cluster ID	Cluster ID is used to identify the cluster. Different Cluster ID will not able to working together. For different Cluster ID, it is required to use different Cluster Service Port. The maximum length of ID is 6 bytes.
Cluster Service Port	The UDP port will be used for intra-cluster communication to send and receive heartbeat message. It is required to have different Cluster Service Port for each Cluster ID. The default value is 694.
Primary Heartbeat Device	The broadcasting of heartbeat message will be send through this primary network device and then secondary one. The default value is "eth1" which is dedicated for heartbeat.
Secondary Heartbeat Device	The broadcasting of heartbeat message will be send through this primary network device and then secondary one. The default value is "eth0" which is the backup network device.

Parameter Name	Description
Heartbeat Keep Alive Interval	The interval to send the heartbeat message. This value will decide how long the failure can be detected. The minimum value is 300ms and maximum is 3000ms. The default value is 700ms.
Heartbeat Keep Alive Dead Time	The time to detect a node in the cluster is dead or not. Normally, it will be the multiple of keep alive interval. The default value is 4 seconds which is around 4 keep alive heartbeat packets lost will be consider a node failure.
Cluster Type	The following types are supported to meet different requirements: Active/Active Cluster: Both servers are acting as an independent server and backup for each other. The register information will be forwarded to backup node to speed up the fail over timing. Once the active one is failed to service, it will switch over to backup node. Active/Standby Cluster: One of cluster server will become active while another one is a backup server. The register information will be forwarded to backup node to speed up the fail over timing. Once the active one is failed to service, it will switch over to backup node.
Cluster Member 1	The cluster member's host name which is get from uname ? □n. Please note that both server settings need the same order. This cluster member will start and service HA Group 1 by default in Active/Active mode
Member IPV4 Address	The IPV4 address for Cluster Member 1. The system might acting strange is you set a wrong IP address.
Cluster Member 2	The cluster member's host name which is get from uname ? □n. Please note that both server settings need the same order. This cluster member will start and service HA Group 2 by default in Active/Active mode.
Member IPV4 Address	The IPV4 address for Cluster Member 2. The system might acting strange is you set a wrong IP address.
HA Group 1	High Available Group 1. It is required for both AA and AS mode.
IPV4 VIP for WAN	Virtual IP V4 address for WAN interface.
Netmask Prefix Length	VIP Network Prefix Length. For example, 24 is means 255.255.255.0.

Parameter Name	Description
IPV4 VIP for LAN	Virtual IPV4 address for LAN interface.
IPV6 VIP for WAN	Virtual IP V6 address for WAN interface. The IPV6 address must be a global unicast addressed, not a link-local or site-local address. IPV6 VIP for WAN is only available when 1 Ethernet leg mode is used (Attached LAN Interface is disabled).
IPV6 VIP for LAN	Virtual IP V6 address for WAN interface. Virtual IP V6 address for WAN interface. The IPV6 address must be a global unicast addressed, not a link-local or site-local address. It could be use fc00:xxxx:xxx:xxx as the private IP V6 address. IPV6 VIP for LAN is only available when 2 Ethernet legs mode is used (Attached LAN interface is enabled).
HA Group 2	High Available Group 2. It is only required for AA mode.

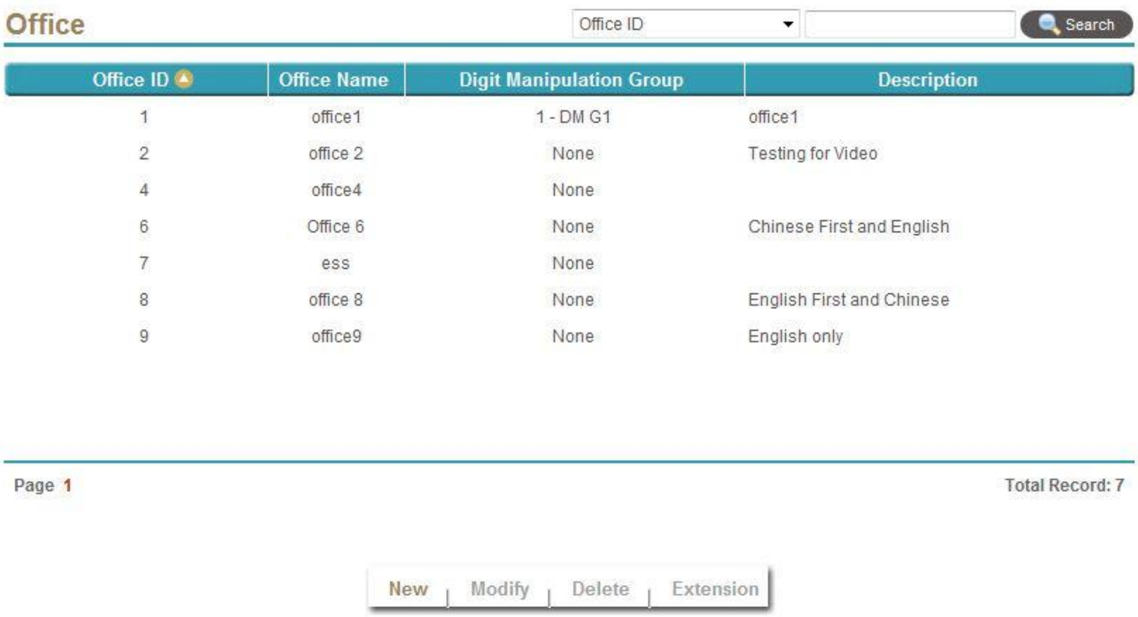
2.3 Extension

Each connected SIP phone, gateway or carrier requires to create a extension in the system in order to accept the register or call from it. Each extension (SIP device/ client) should belong to a extension group which define the digit manipulation rule, access code and mail server settings. Also each extension group can have multiple call pickup group and extension could be assigned to a pickup group for group pickup service.

Also each extension could enable the extension call service based on its requirement such as follow me here, incoming call or outgoing call blocking.

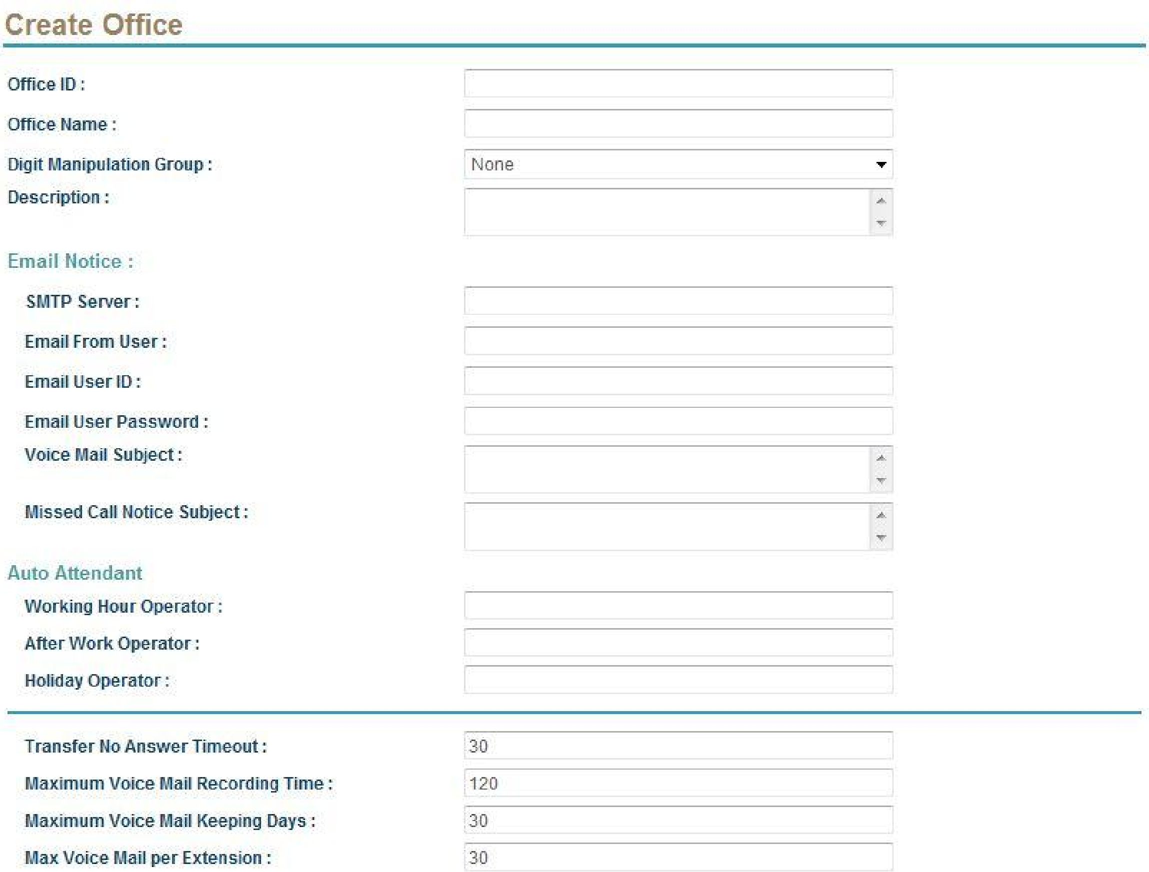
2.3.1 Office

For each office you need create here. Click ***EXTENION-> Office*** view and create the settings.



Office ID	Office Name	Digit Manipulation Group	Description
1	office1	1 - DM G1	office1
2	office 2	None	Testing for Video
4	office4	None	
6	Office 6	None	Chinese First and English
7	ess	None	
8	office 8	None	English First and Chinese
9	office9	None	English only

Select New, Modify, Delete to change the office settings. The following web page will appear:



The detail of each parameter is described as below:

Parameter Name	Description
Office ID	Office ID
Office Name	The name of office
Digit Manipulation Group	The Digit Manipulation Group ID will be used for this group.
Time Zone	The time zone will be used for this office's extension. It need to be set if using CPE auto provisioning feature.
Description	The description for this office.
Email Notice	The email notice setting for SMTP server will be used for missed call or voice mail notice.
SMTP Server	The SMTP server IP address
SMTP Port	The SMTP server port. For SSL the default is 465 and for StartSSL or none, the default is 25.
SSL Type	The SMTP server supported SSL Type, it can be none, STARTTLS or SSL.
Email Form User	The email sending email address for SMTP server.
Email User ID	The email sending account ID for SMTP server
Email User Password	The email sending account password for SMTP server
Voice Mail Subject	The email subject for sending new voice mail notice. The administrator can input the system variable to make the subject easy to be read:
Voice Mail Body	The customizable email body for new voice mail notice. The administrator can input the system variable to make the subject easy to be read.
Missed Call Notice Subject	The email subject for sending missed call notice. The administrator can input the system variable to make the subject easy to be read.
Missed Call Email Body	The customizable email body for missed call mail notice. The administrator can input the system variable to make the subject easy to be read.

Parameter Name	Description
Voice Mail Subject	The email subject for sending a new voice mail notice. The administrator can input the system variable to make the subject easy to be read.
Voice Mail Body	The email body for sending a new voice mail notice. . The administrator can input the system variable to make the subject easy to be read.

The Auto Attendant parameters can be defined as follows:

Parameter Name	Description
Working Hour Operator	The operator number for working hour
After Work Operator	The operator number for off hours
Holiday Operator	The operator number for holiday
Work Hour Menu	The call flow menu for working hour
After Work Hour Menu	The call flow menu for off hours
Holiday Menu	The call flow menu for holiday
Priority Menu	Highest priority call flow will be used. When this call flow menu is enabled, auto attendant will run this call flow instead of others setting. This is useful when office is off for some reasons such as company tours.
Black List Menu	When the caller ID met the black list and black list call flow was enabled, auto attendant will run the black list call flow. Normally, it will reject the calls.
Manual Working Mode Switch	Whether enable to use VMS Main Menu access code (in VMS route) to set the AA working mode or not. For example VMS main menu access code is *50, the following mode can be selected: *500: Use Time based routing *501: working hour *502: After call work mode *503: Holiday Mode *504: Priority Announcement Mode

Parameter Name	Description
	*505: Toggle working hour and after call work mode. (This will be also the BLF to subscribe in order to get the working hour (LED is OFF or Green) or not (LED is ON or Red).
Hold Tone Music Prompt	The music will be used for music on hold and transferring music in AA. The file format is 8K * 16 bits linear PCM Mono Wav.
Transfer No Answer Timeout	The time to wait the called party answer for transferring.
Use Separate No Answer Timeout	Whether to use different no answer timeout for different working time.
Maximum Voice Mail Recording Time	The max recording time for each voice mail.
Maximum Voice Mail Keeping Days	The maximum keep days for voice mail messages.
Max Voice Mail per Extension	This the maximum number of voice mail allowed to each extension. Over this number, the oldest voice mail message will be overwritten.
Meet Me Conference Access Key	The access key to get into meet me conference with AA.
Outgoing Call Access Key	The access key to get into the outgoing call service with AA.
Voice Mail Access Key	The access key to get into the voice mail access within AA.
Outgoing Call No Answer Timeout	The time to wait the called party answer for outgoing call within AA.
Working Time	The working time setting for the office.
Period 1-3	The working period to be defined for each week day. The format is hh:mm-hh:mm, such 09:00-12:00.
Menu ID 1-3	The Menu ID is the menu ID (call flow) to be ran for this working hour period.

2.3.1.1 Access Code

The Access Code parameters are used to define those service activation or deactivation from telephone set. Once the feature access code is accepted by the system, the system will send SIP "180 ring" and user will hear ring back tone. If it is rejected by the system, the will send "406 Not Acceptable" instead and user should hear a busy tone. Click ***Access Code*** button below the ***Office*** modification screen. The following screen will appeared.

Each access code filed are defined as following:

Parameter Name	Description
Enable Call Forward Always	The access code to enable "Call Forward Always". The default value is *01. Dialing Rule: ACCESS_CODE+FORWARD_TEL or ACCESS_CDOE (using the existing setting).
Disable Call Forward Always	The access code to disable "Call Forward Always". The default value is *02. Dialing Rule: ACCESS_CODE.
Enable Call Forward No-Answer	The access code to enable "Call forward" for no answer. The default value is "*05". Dialing Rule: ACCESS_CODE+FORWARD_TEL or

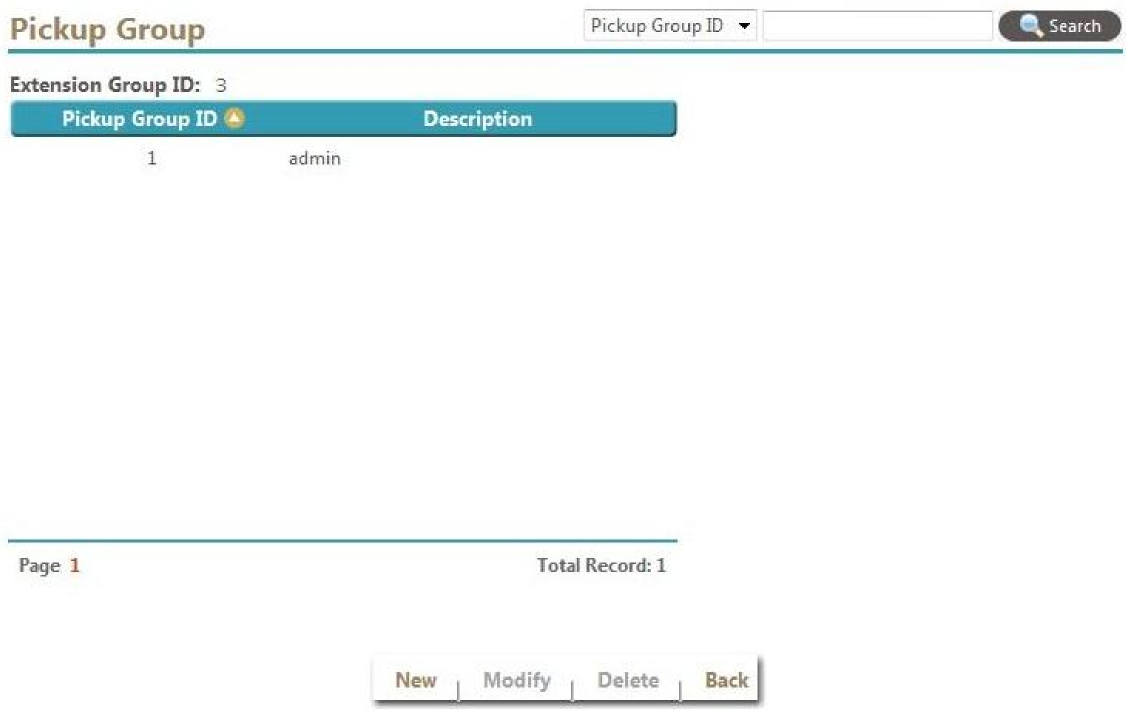
Parameter Name	Description
	ACCESS_CDOE (using the existing setting).
Disable Call Forward No-Answer	The access code to disable "Call Forward for no answer". The default value is "*06". Dialing Rule: ACCESS_CODE.
Enable Call Forward Busy	The access code to enable "Call Forward" for busy. The default value is "*03". Dialing Rule: ACCESS_CODE+FORWARD_TEL or ACCESS_CDOE (using the existing setting).
Disable Call Forward Busy	The access code to disable "Call Forward" for busy. The default value is "*04". Dialing Rule: ACCESS_CODE.
Enable Call Forward Unavailable	The access code to enable call forward for unregistered. The default value is "*10". Dialing Rule: ACCESS_CODE+FORWARD_TEL ACCESS_CDOE (using the existing setting).
Disable Call Forward Unavailable	The access code to disable call forward for unregistered. The default value is "*11". Dialing Rule: ACCESS_CODE.
Enable Do Not Disturb	The access code to enable "Do Not Disturb". The default value is "*08". Dialing Rule: ACCESS_CODE+HHMMHHMM (DND time period 1) ACCESS_CODE+HHMMHHMMHHMMHHMM(time period1 and period2) ACCESS_CODE (using the existing setting).
Disable Do Not Disturb	The access code to disable "Do Not Disturb". The default value is "*09". Dialing Rule: ACCESS_CODE.
Enable Follow Me	The access code to enable follow me. This service requires to use web to setup first. The default value is "*12". Dialing Rule: ACCESS_CODE.
Disable Follow Me	The access code to disable follow me. The default value is "*13". Dialing Rule: ACCESS_CODE.

Parameter Name	Description
Calling with Caller ID	The access code to enable calling ID for this call. The default value is "*15". Dialing Rule: ACCESS_CODE+DIAL_TEL.
Calling without Caller ID	The access code to disable calling ID for this call. The default value is "*16". Dialing Rule: ACCESS_CODE+DIAL_TEL.
Group Pickup	The access code to pick a call within a pickup group. The default value is "*31". Dialing Rule: ACCESS_CODE.
Global Any Pickup	The access code to pick any calls. The default value is "*30". Dialing Rule: ACCESS_CODE.
Dedicate Pickup	The access code to pick a dedicated extension's call. The default value is "*32". Dialing Rule: ACCESS_CODE+EXTENSION_TEL.
Enable Privilege Calling	The access code to unblock those outgoing privilege call screening. The default value is "*33". Dialing Rule: ACCESS_CODE+WEB PASSWORD
Disable Privilege Calling	The access code to block those outgoing privilege call screening. The default value is "*34". Dialing Rule: ACCESS_CODE++WEB PASSWORD
Privilege Calling	Privilege Calling is used to call a privilege screened prefix once. The default value is "*35". Dialing Rule: ACCESS_CODE+WEB_PASSWORD+* +CALLED_NUMBER.
Camp On	To enable system to make the call for the extension when the called party is become to idle. It can be applied only when the called party is in busy state. The default value is "*28". Dialing Rule: ACCESS_CODE.
Permanent Block Caller ID	The access code to permanently block the caller ID sending. The default value is "*17". Dialing Rule: ACCESS_CODE
Permanent Send Caller ID	The access code to permanently enable the caller ID sending. The default value is "*18". Dialing Rule: ACCESS_CODE
Group BLF URI	The RFC 4235 Dialog Event Package URI for whole extension group. Subscribe this number for BLF, whole group's status will be sent. The default value is NULL

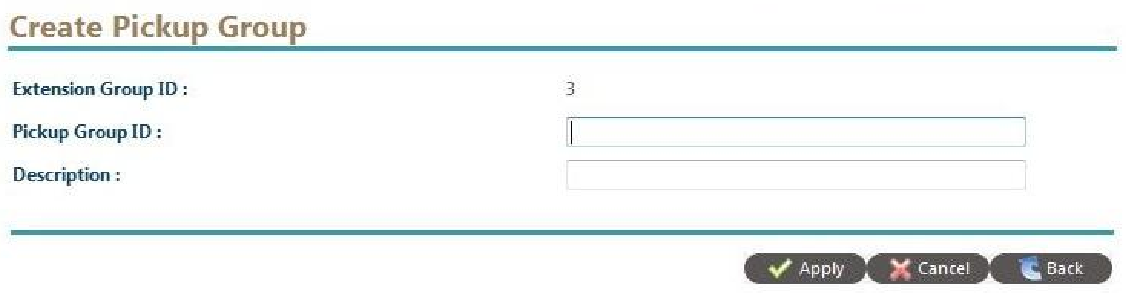
Parameter Name	Description
	which means disble this feature.
Set Call Forward Always for Extension	The access code to set Call Forward Always for an unregistered extension. Dialing Rule: ACCESS_CODE+Extension+*+web_password+*+forwarded number.

2.3.1.2 Pickup Group

The pickup group is used for pickup the ring call within the same office. Each pickup group cannot cross the office. After select the specified office, click ***Pickup Group*** button to add or remove the pickup group settings.



Select New, Modify or Delete to modify the pickup group settings. The following web page will appear:

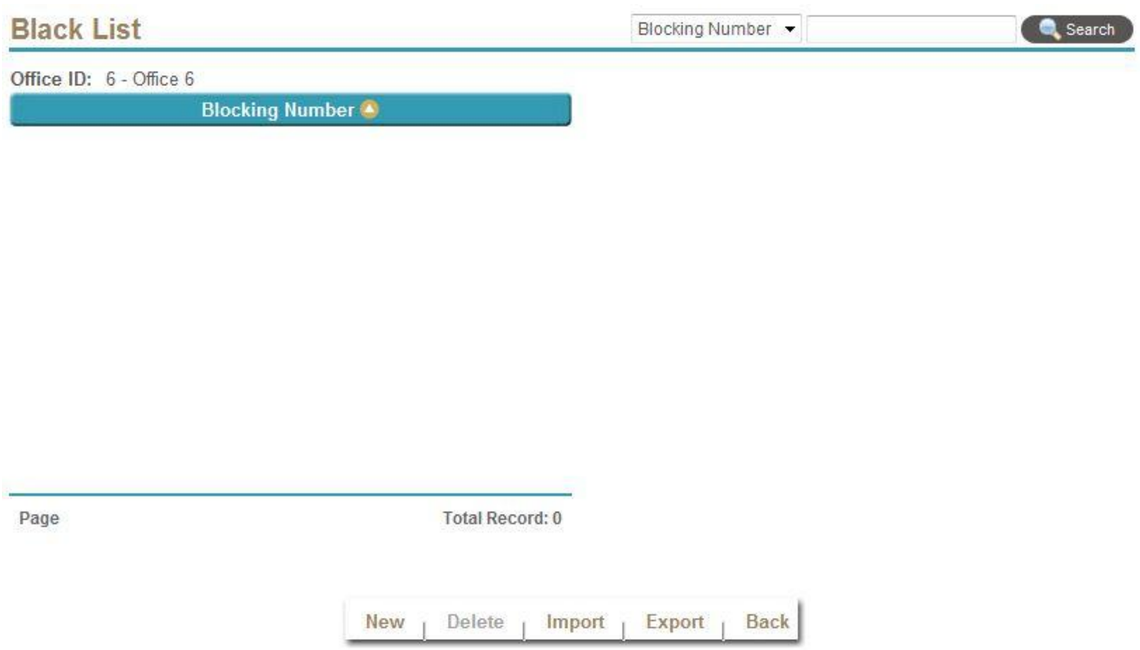


The detail of each parameter is described as below:

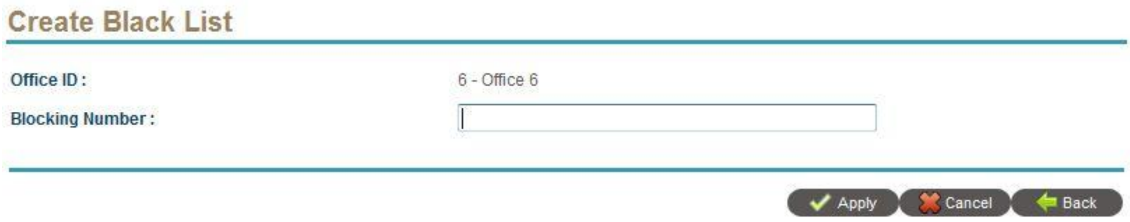
Parameter Name	Description
Pickup Group ID	Pickup group ID for call pickup
Description	Description for this group

2.3.1.3 Black List

Black List can be used for auto attendant service to filter those unwanted calls. When auto attendant receive a call, it will try to map the incoming caller ID against the black list. If it is mapped and black list menu was selected, the system will start the back list call flow instead of normal call flow. Click ***Black List*** button to view and modify the black list as follows:



Click ***New*** to add a new black list ID as follows:

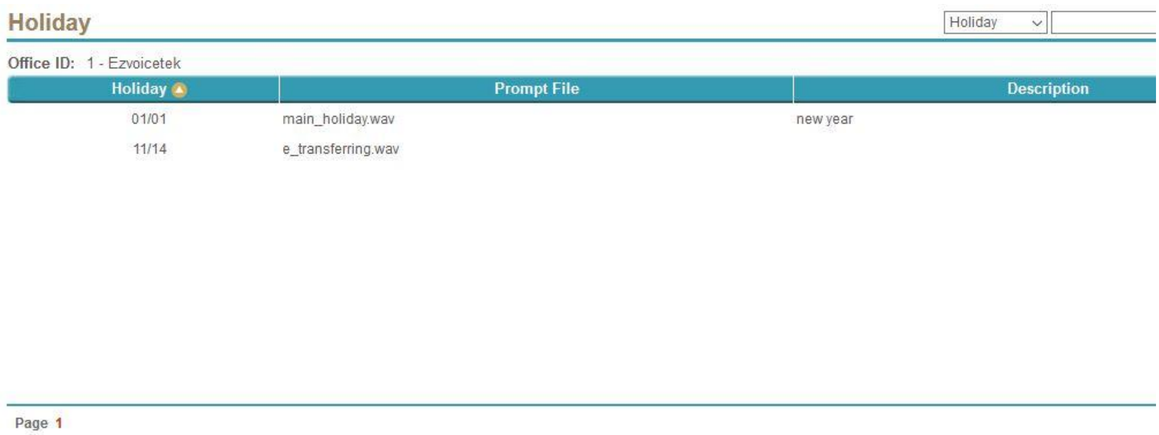


The detail of each parameter is described as below:

Parameter Name	Description
Office ID	Office ID for this black list
Blocking Number	The number will be in black list.

2.3.1.4 Holiday

The holiday definition for the office. If today is one of date in holiday list, the holiday flow will be executed. Click ***Holiday*** button to view the current holiday settings. The following screen will appeared.



Click ***New*** to add the a new holiday or use Import/Export to update whole holiday list. The following is the add or modify screen:

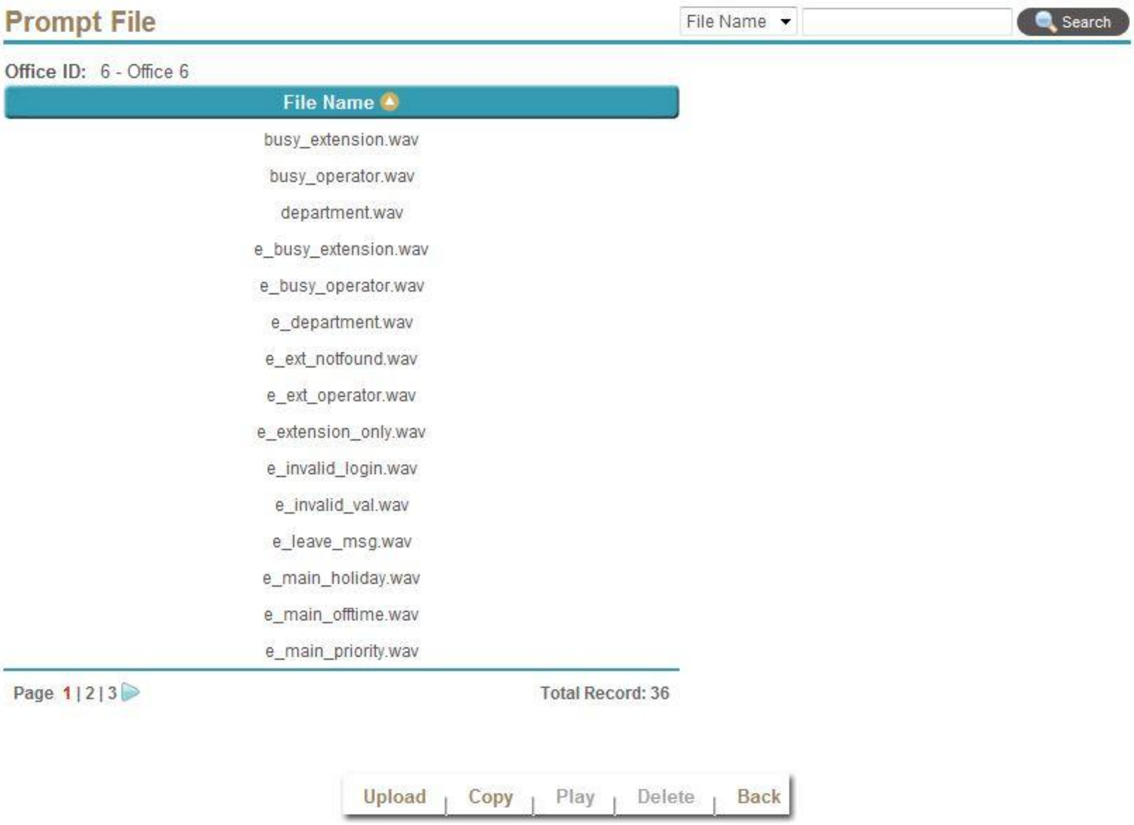
The detail of each parameter is described as below:

Parameter Name	Description
Office ID	Office ID
Holiday	The holiday date in formation of MM/DD.
Description	The holiday name or description for this holiday.
Holiday Prompt	The holiday prompt could be used for this specified holiday in menu editor.

2.3.1.5 Prompt File

To manage the office's prompt file, click ***Prompt*** button for this office and the office belonged to this office will be listed. Once you click a prompt file name, you can play to hear the voice or delete it. Click ***Upload*** and you will able to upload your own recorded file into this office. The file format is showed as follows:
- 8K Sample Rate
- 16 bits
- Linear PCM (signed)
- Mono
- Wav format

Click Copy and you will able to copy prompts from a existing office. The prompt file management page are showed as below:



2.3.1.6 VMS Routing

The AA/VMS Routing is used to define those AA and VMS related service call routing number. For each service, you need create a service routing number in order to use it. Each service type was defined as follows:

Service Type	Description
Auto Attendant	This is the service for auto attendant service.
VMS Main Menu	To enter the voice mail access menu. This service can be also used as manual working mode switch. And subscribe to this prefix + 5 (e.g VMS main menu is *50, subscribe to *505) is the BLF for working hour mode. BUSY indicates now is working hour and IDLE indicates others mode.
VMS from Extension	To access voice mail from through its own extension. Using this prefix, the system will use the calling extension as the default extension.
Music on Hold	You need set this in order to enable music on hold service.

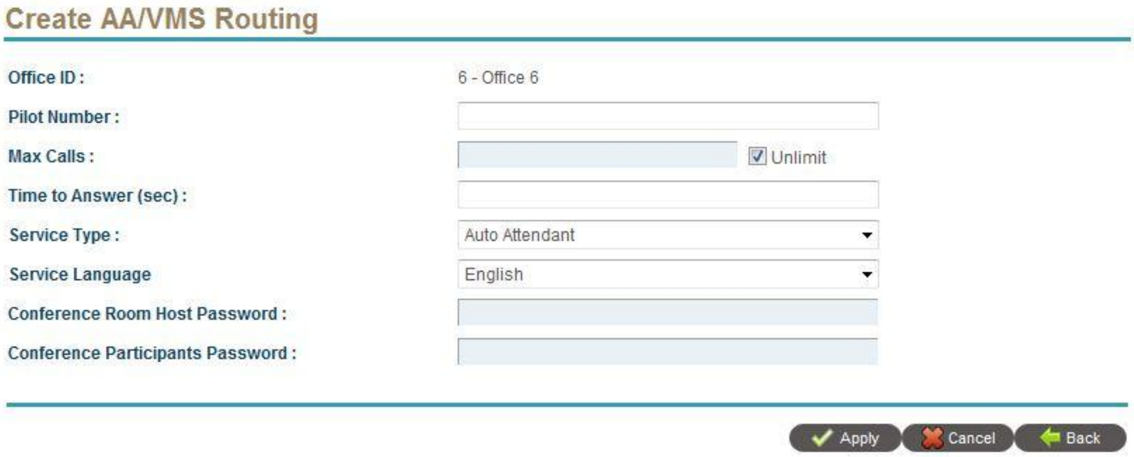
Service Type	Description
Meeting Me Conference	The dial in conference service. You need create each conference room here.
Call Park	The call park room will be created. If you create it, total 10 room will be created. For example, the pilot number is 812, thus you will have park room from 8120 to 8129. To park a call to a park room, you can have the following ways: 1. Make the second call to the pilot number (e.g. 812 in this case) and you will hear the park number to be used. Then you can do the consultant transfer to it. It could be used for IP phone or gateway. 2. If you are using the attendant console and able to know the park room (e.g. 8120 to 8129), you can do subscribe the BLF for the status of parking room and blind transfer to the dedicate park room (e.g. 8121).
Adhoc Conference	The dialing out conference service.
Direct to voice mail	This can be used when you want to transfer a call to a dedicated voice mail in order to leave a message. You need put extension number following by the defined pilot number.
Outgoing Calling	This can be used to dialing a privilege dialing prefix by entering extension and VMS password. An IVR will guide the caller to input it. It is useful when you want to dial a privilege screened prefix from another extension.
Meeting Me Conference Global	This is a global meeting me conference which allow PSTN number to call into this meeting me conference room directly. It is different from the Meeting Me Conference which only allow PSTN user to call through company auto attendant.
Service Setting	This is the announcement service for this office.
Dial Out Conference	The is conference room which is configure to have predefined participant list and once the conference host was dialed in with host password, the system will automatically call all the participant list number to invite them to join it.
Broadcasting Service	This is the announcement broadcasting service. The participant list the number to be dialed for this broadcast and the pilot number is the dialing entry point. The broadcasting target need have auto answer feature for this broadcasting. And the broadcasting start and stop notice

Service Type	Description
	will be played.

The interface to manage ***AA/VMS routing*** is showed as below:

Pilot Number	Max Calls	Time to Answer (sec)	Service Type	Language
*50	Unlimit	1	VMS Main Menu	English
*51	Unlimit	1	VMS From Extension	Chinese
*52	Unlimit	1	Direct to Voice Mail	
*56	Unlimit	1	Call Park	English
*59		1	Music On Hold	
26629087	Unlimit	1	Auto Attendant	Chinese
26629088	1	2	Auto Attendant	English
8130	Unlimit	2	Meet Me Conference	Chinese
8131	Unlimit	2	Meet Me Conference	English
814	Unlimit	2	Adhoc Conference	English
815	Unlimit	2	Adhoc Conference	Chinese

Click ***New*** to add a new routing plan as follows:

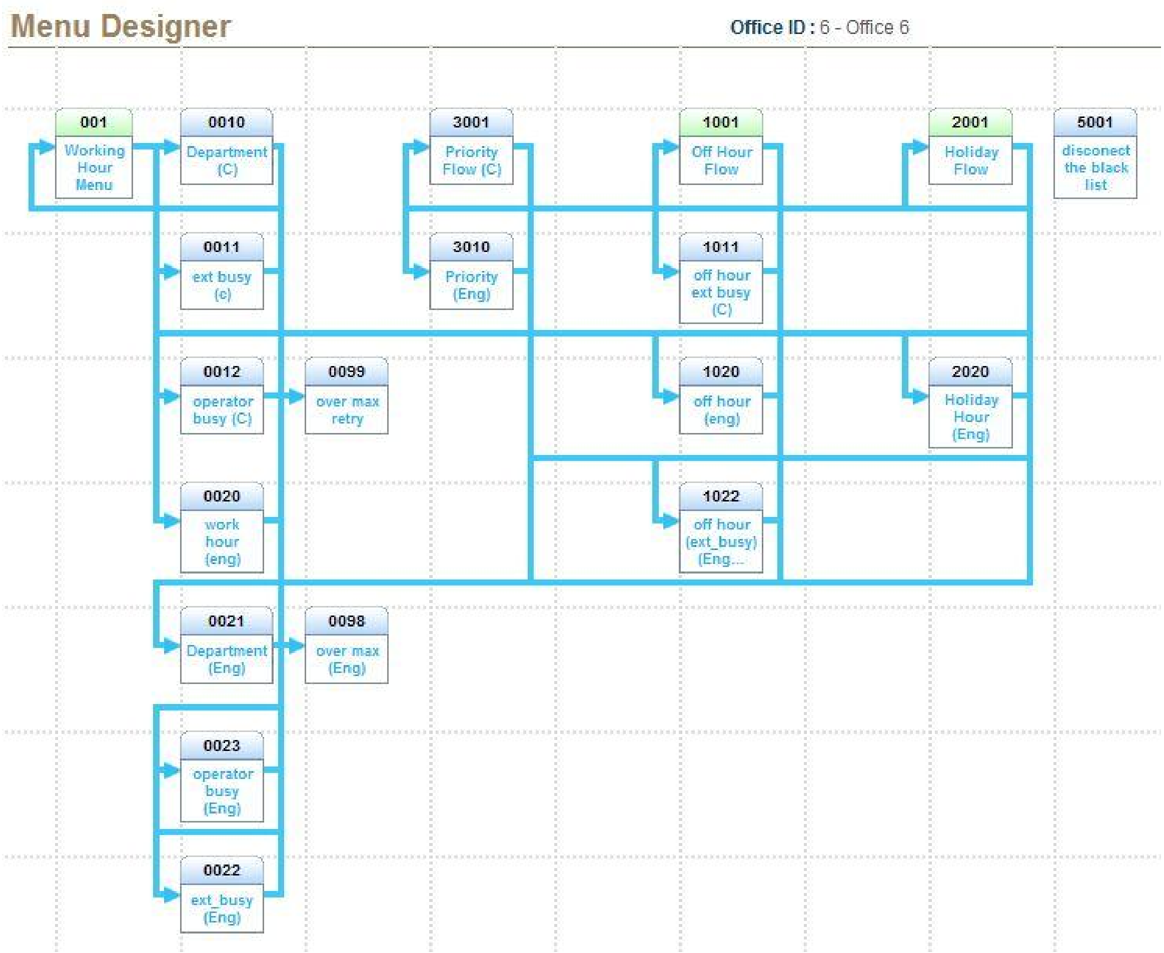


The detail of each parameter is described as below:

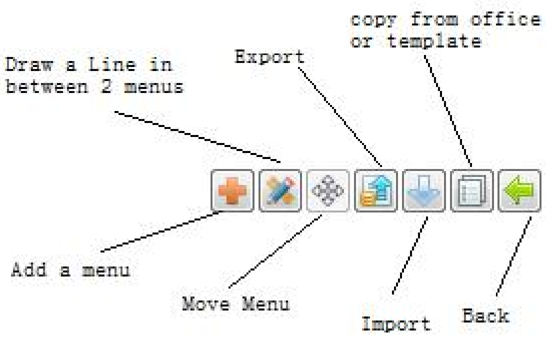
Parameter Name	Description
Office ID	Office ID
Pilot Number	The AA/VMS service routing number
Max Calls	Maximum allowed calls for this service
Time to Answer	The time to wait before answer this service call.
Service Type	The AA/VMS service type described above
Service Language	The language will be used for those AA service such as voice mail main menu, meet me conference or outgoing calling.
Language	AA & VMS service prompt language
Conference Room Host Password	Conference room's hosting password. Only after hosting person get into the meeting conference, the conference can be started. This is also the password to initial the adhoc conference room if the service type is adhoc conference.
Conference Participants Password	The password allow the participant to join into the conference.
Conference Join Access Key	The access key used for adhoc conference service. It allowed to quit the current on-going conference and invite new person to join the conference. An IVR will be started after press the access key.

2.3.1.7 Menu Designer

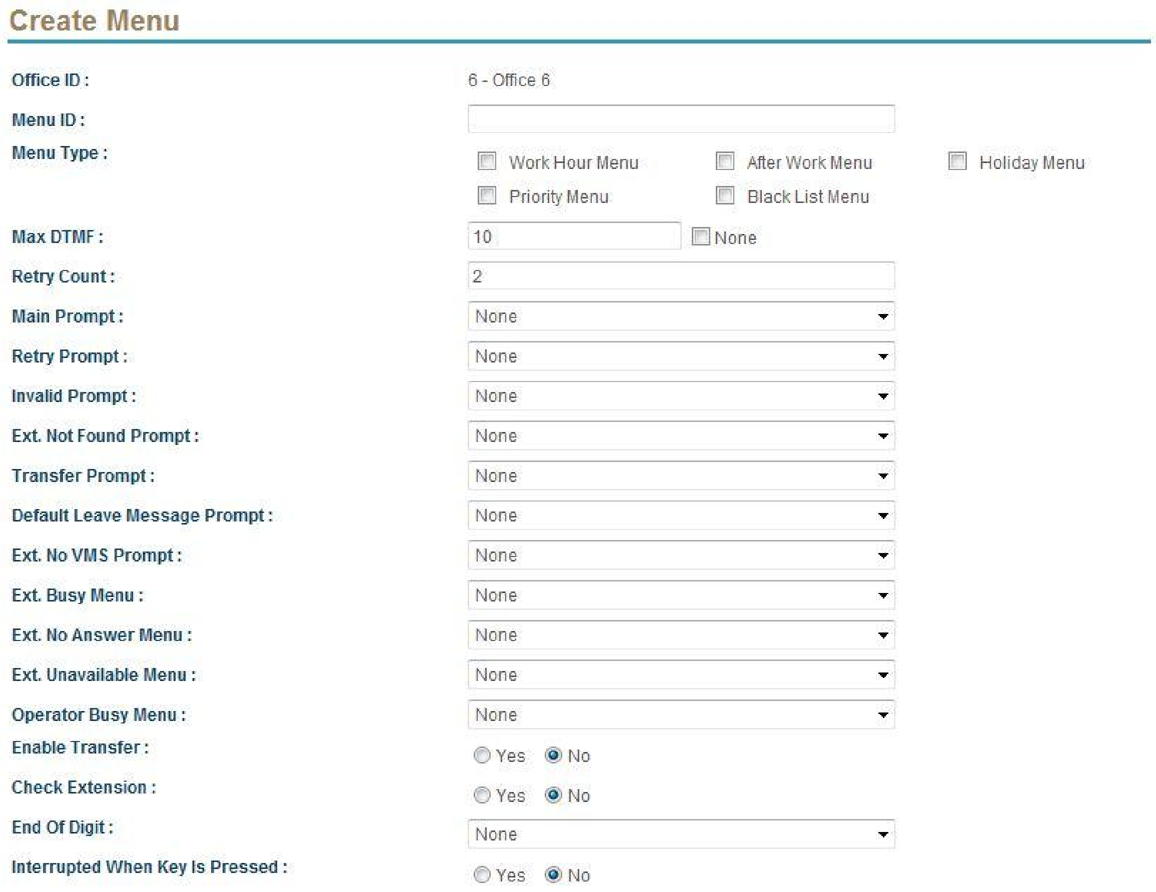
For each office you need create his own call flow for auto attendant service.The quickest way to build your own call flow is copying a existing office or from a template and edit it.Click ***Menu Designer*** and you will able to start your call flow design as follows:



In the top left, you will able to see the menu icon as .



For each menu, click right key and your will see the ***Modify*** action for reviewing and modify the menu parameters. To create a new menu, click ***add*** icon and you will see the following:



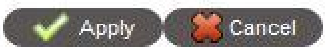
The detail of each parameter is described as below:

Parameter Name	Description
Office ID	Belonged office ID
Menu ID	The call flow menu ID
Menu Type	The menu type to indicate this menu is the entry point for difficult call flow. Each type can have only 1 entry point to be selected. The old one will be unchecked automatically.
Use Holiday Prompt if Set	This is only available for holiday menu, the system will use the holiday prompt if it is set instead of main prompt. If there is no holiday prompt is set, the main prompt will be played.
Redirect Call Immediately	When it is enable, the system will send 302 moved to tell the caller to move the specified number set in the Default Action. This call will not be answered

Parameter Name	Description
Max DTMF	Maximum DTMF digits to be received.
Retry Count	The max retry count within this call flow menu
Main Prompt	The prompt will be played when execute the call flow menu.
Retry Prompt	The prompt will be played for retrying this call flow menu. It could be played such as no DMTF received, not a extension, invalid input etc.
Invalid Prompt	When the inputted DTMF was an invalid value, this prompt will be played.
Ext. Not Found Prompt	The prompt will be played when the inputted extension does not existed.
Transfer Prompt	The prompt will be played before transferring.
Default Leave Message Prompt	The default prompt to indicate caller to leave a voice mail when called extension doesn't enable personal greeting.
Ext. No VMS Prompt	The prompt will be played when the transferred extension doesn't had a voice mail and the caller request to leave a message.
Ext. Busy Menu	The call flow menu will be executed when called extension is busy.
Ext. No Answer Menu	The call flow menu will be executed when called extension is not answer.
Ext. Unavailable Menu	The call flow menu will be executed when called extension is not available.
Operator Busy Menu	The call flow menu will be executed when operator doesn't answer.
Enable Transfer	When it is enabled, call transfer to extension will be executed.
Check Extension	If it is enabled, the system will check whether the inputted digits is in the extension list before the call transfer to be executed.
End Of Digit	End of Digit to indicate the end of input. Normally, it will be #.
Interrupted When Key Is Pressed	Whether stop the playing when a DTMF was received. Normally, it should be enabled.

Parameter Name	Description
Description	The description of this menu.
Key Action	The action will be executed when this key was matched. The following actions can be selected: Transfer to operator: will try to transfer this call to operator. Repeat Prompt: Will repeat the Main prompt. Disconnect: Disconnect the call. Jump to Menu: Execute the call flow menu in value filed. Transfer to Extension: The call will be transferred to a dedicate number in value field. Jump to Voice Mail: Get into this extension's voice mail.
Retry Fail Action	When max retry is reached the retry count, the action should be taken.
Default Action	The default action when there is no DTMF will be received (max DTMF is equal to 0).

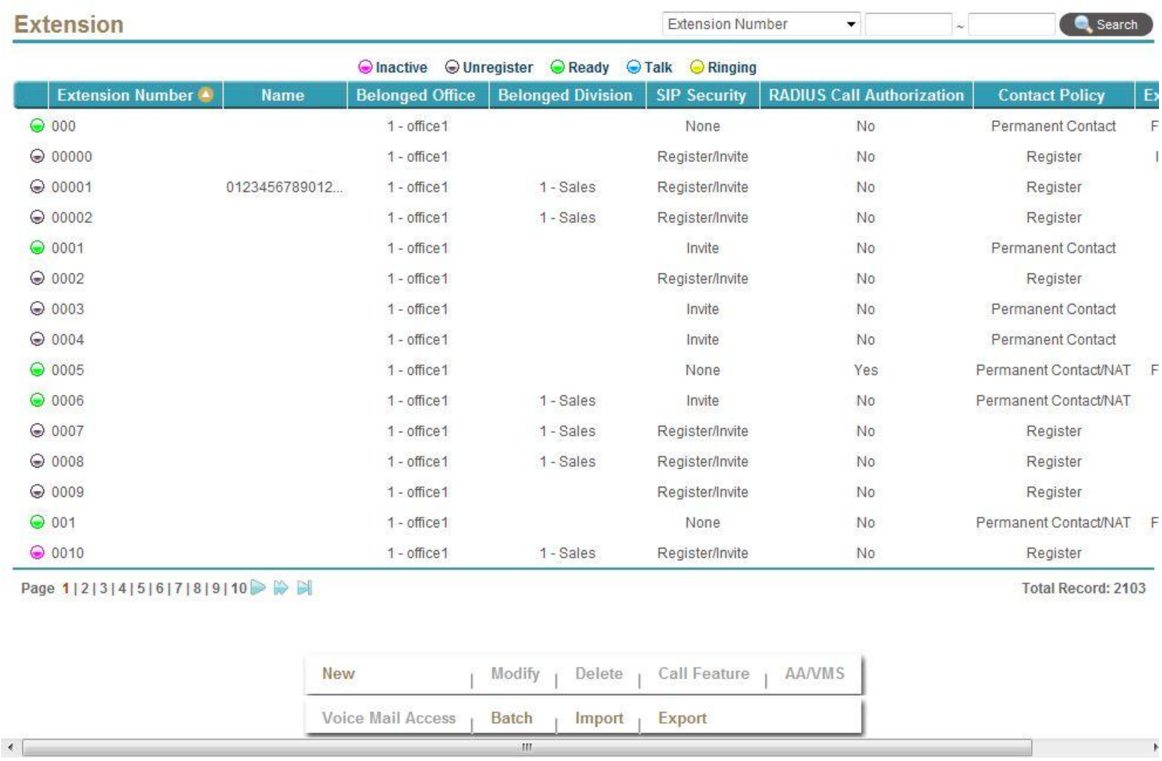
By using the menu to build you call flow, you can create the AA call flow very quick. The system also provide the template to be copied for your needs. Click ***Copy*** and you will see the following:



You can use the copy to copy from a existed working office or from a template which including voice prompt and call flows.

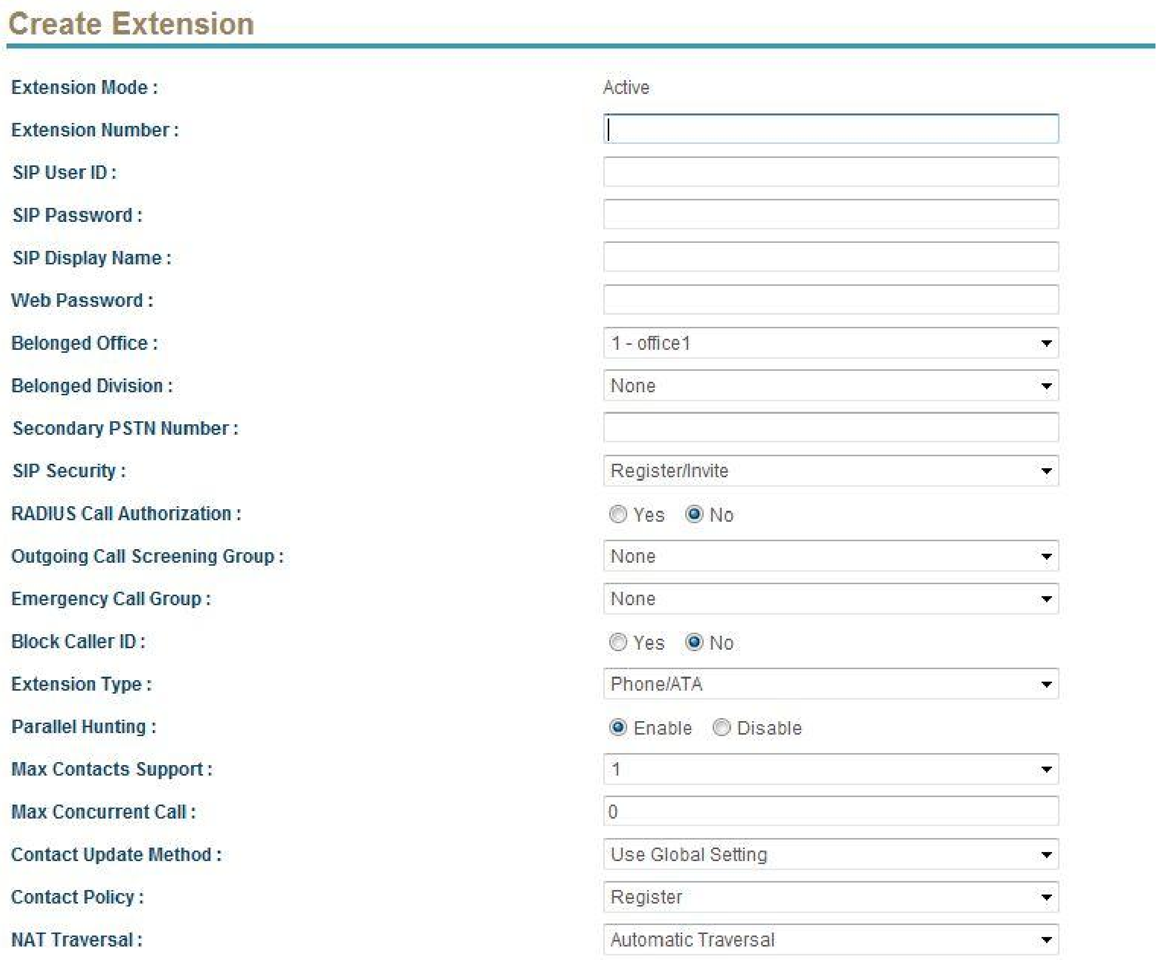
2.3.2 Extension

No matter the connected device is a SIP gateway, ATA, IP phone or Proxy, the administrator must create an extension for it in order to allow it to register or call. For the type of "FXO/Gateway/Proxy", it normally can allow multiple call simultaneously. Click ***EXTENSION -> Extension*** to view or modify the extension settings. Or you can click ***EXTENSION -> Office -> Extension*** to see the office owned extension only.



Click Rebuild can rebuilt this mac's device configuration if auto provisioning is enabled.

Select New, Modify, Delete to change the extension settings. The following web page will appear:



The detail of each parameter is described as below:

Parameter Name	Description
Extension Mode	Whether to activate this extension or not.
Extension Number	The extension telephone number for SIP registration (from/ to header).
SIP User ID	The SIP user ID for authentication
SIP Password	The SIP user password for authentication
SIP Display Name	The display name used for SIP FROM header. If it is NULL, it indicates use the CPE's setting.
Web Password	The password for extension owner to login the extension web for service settings. In order to allow extension login, the "SYSTEM->WEB Service->Allow Extension Logon"

Parameter Name	Description
	need to be set to enable. The web password can only allow digits (0-9), since it will be used for "outgoing call privilege access" as a password.
Belonged Office	An extension should be only belong to a office. Please select the office here.
Belonged Division	An extension can belong to a charged division which is used to manage and billing purpose.
Secondary PSTN Number	When an extension has set the PSTN number, the system will try to match it for a incoming call. If the called number was matched, the call will derived to the matched extension. And for outgoing call to a non-extension target, the caller ID will be changed to this PSTN number.
SIP Security	The level of SIP security. When set to register/invite, it means the extension will be authenticated for register and call. For set to "Register Only", the extension will only be authenticated for register request. The default value is "Register/Invite".
RADIUS Call Authorization	Whether to enable the RADIUS call authorization or not. Please only enable it when you have a RADIUS server connected and set the corresponding parameters in "SYSTEM-> RADIUS". The default value is "No".
Outgoing Call Screening Group	The group ID of outgoing call screening.
Abbreviated Dialing Group	The group ID of abbreviated dialing.
Emergency Call Group	The group ID of emergency call.
Block Caller ID	Whether to enable caller ID sending (CLIP) or not (CLIR). The default value is "No".
Extension Type	The type of the extension. The following is the guide line for the settings: ATA/Phone: It is used normally for IP phone or FXS/ATA gateway. FXO/Trunk/Proxy: It is normally be used for gateway such as FXO/E1 gateway or SIP proxy.

Parameter Name	Description
	SIP Trunk: It is used for connecting to another VOIP carrier. In this case, VOIP carrier will give you a SIP account for calling and you need to set it on SIP trunk then associate it here. Voice Mail Server: The external voice mail server which support MWI and diversion header. ENUM: This is a ENUM peering which will need set a restricted security. CTI Phone: It will be only available when ACD license is turned on. It is required to set ACD extension to this type in order to work with ACD Server. Web Caller: It will be only available when web call license is turned on. This type indicate this account is a web call server.
SIP Trunk ID	The SIP trunk ID associated to.
Parallel Hunting	Whether to fork (send) SIP request to all registered contacts or by sequence. The default value is "enable".
Max Contacts Support	How many ATA/Phone can register to this account. The default value is 1.
Max Forward/ Transferred Call	The extension wide max allowed forward or transferred calls. It is recommended to use global or set it to 2 or 5 instead of unlimited.
Contact Update Method	If the number of register for an account is more than the max contact supported, the system can be set to reject it (Deny) or remove the oldest one and accept it (overwrite). The default value is "overwrite".
Contact Policy	The extension contact type, it could be: Register: The SIP client will register to the system. This is the typical type for most of SIP client. Permanent Contact: The user need define where is the SIP client and interface connected. Permanent Contact/NAT: This is same as the Permanent Contact but the SIP client is located in behind NAT. You need to setup a DMZ or port mapping in order to use it.

Parameter Name	Description
Permanent Contact 1	When the contact policy is permanent contact, this is the defined contact URI and the target interface. The SIP URI is used for the contact address. For example: sip:1001@112.25.26.3:5060 or sip: 1030@113.111.222.333:9099.
Permanent Contact 2	When the contact policy is permanent contact, this is the defined contact URI and the target interface. The SIP URI is used for the contact address. For example: sip:1001@112.25.26.3:5060 or sip: 1030@113.111.222.333:9099.
Public TA	Public IP address and port for the DMZ server when Permanent Contact/NAT is selected. The format is IP:Port, for example, 112.35.23.11:9000.
NAT Traversal	The type of NAT traversal. If it is set to "Automatic Traversal", the system will automatically detect whether need to use NAT resource or not. If it is set to "Always ON", NAT resource will always be used. This mode could be used if you would like to do the call logging or interception. When it is set to "Always OFF", the system will never use the NAT resource and it might lead the silence issue. If you have voice logging license activated, you will see the "Voice Logging" item here. Select it, every call to or from this extension will be recorded. Record on Call will be use when CPE can support recording on demand feature.
Default Register TTL	The default register time (SIP UDP only) to live (expiries) in seconds for a user coming from public network. The default value is to use the global setting in SYSTEM-> SIP Service -> Default Register TTL. If you assign another value, the system will use it instead.
NAT Register TTL	The default register time (SIP UDP only) to live (expiries) in seconds for a user coming from private network (behind NAT). The default value is to use the global settings in SYSTEM-> SIP Service -> Default Register TTL. If you assign another value, the system will use it instead.
SIP Request Response Timer	The time to wait in seconds for a response when send out a SIP request. The default value is to use the global settings in SYSTEM->SIP Timer->SIP Request Response Timer.

Parameter Name	Description
No Answer Time Out	The time to wait in seconds for the called party to answer. The default value is to use the global settings in SYSTEM->Service Parameter->No Answer Time Out.
Dedicate Device 1	The allowed device to be used for this extension. The system will check the SIP "user-agent" header to validate. The comparing method is prefix match. It doesn't require a fully match.
Dedicate Device 2	The allowed device to be used for this extension. The system will check the SIP "user-agent" header to validate. The comparing method is prefix match. It doesn't require a fully match.
Session Validation method	he SIP request method to be used for checking the call existence. The default value is "Use Global" which means to use the setting in SYSTEM-> Service Parameters -> Session Validation method.
Max Concurrent Call	The allowed max concurrent calls including connecting and connected calls.
SIP Privacy	The outgoing SIP privacy policy (according to RFC 3325): Remove: Remove all RFC 3325 privacy header. It could be used for a un-trusted network or device type is phone/ata. By-Pass: No change for privacy header for compatible reason Adaptive: The system will according to incoming call's privacy header or caller information to add the necessary privacy header. Only use it for a trusted peering network. The default value is remove.
Inter-Extension Call Billing	Whether to send intra company billing message to RADIUS server or not. It only applied when work with IP Centrex Server.
RADIUS Sending Phase	Whether to send RADIUS authorization or billing message based on original digits (before DM), modified digits (after DM) or use global settings.
Enable Talk Time Roundup	Whether to enable the rounding for talking time or time. If it is enabled, the talking time will be round-up which means 1.01 will become 2.
Register IP Check	Whether check SIP register IP or not? This feature can select IP/netmask to check or use IP lookup service to verify the belonged country.

Parameter Name	Description
Not Matched Policy	The way to handle when IP network or country is not matched the defined network. Send Alert Only: enable this if administrator need receive an alert only Send Alert and Unregister: This option will send alert message and unregister this unmatched contact. Send Alert, Unregister and Disconnect Call: This option will send alert, unregister this contact and disconnect all existing calls.
Limited Network 1-2	The allowed IP network in this format: xxx.xxx.xxx.xxx/ prefix_length (e.g. 192.168.10.100/24).
Limited Country 1-2	The allowed country for this account
Auto Provisioning	Whether enable auto provisioning for this account for not?
MAC Address	The assigned mac address for this account. You can use SIP PnP to get the device's MAC address if CPE can support SIP PnP Multicasting.
Device Name	The provisioned device type
Device Line ID	The device line (if it have multiple lines) will be used for this account.
Register Interface	The interface will be used to register to SIP.
Register TTL	Which register will be set as default.
Extension Owner	The is the contact information for this extension. It could be WAN or LAN interface based on customer's requirement.
Name	The extension owner's name
Mobile	The extension owner's mobile number
TEL	The extension owner's home/office telephone number
Email	The extension owner's email address. This will also be the email address to receive the "Missed Call Email" and voice mail notice.
Address	The extension owner's address.
Description	Description for this extension

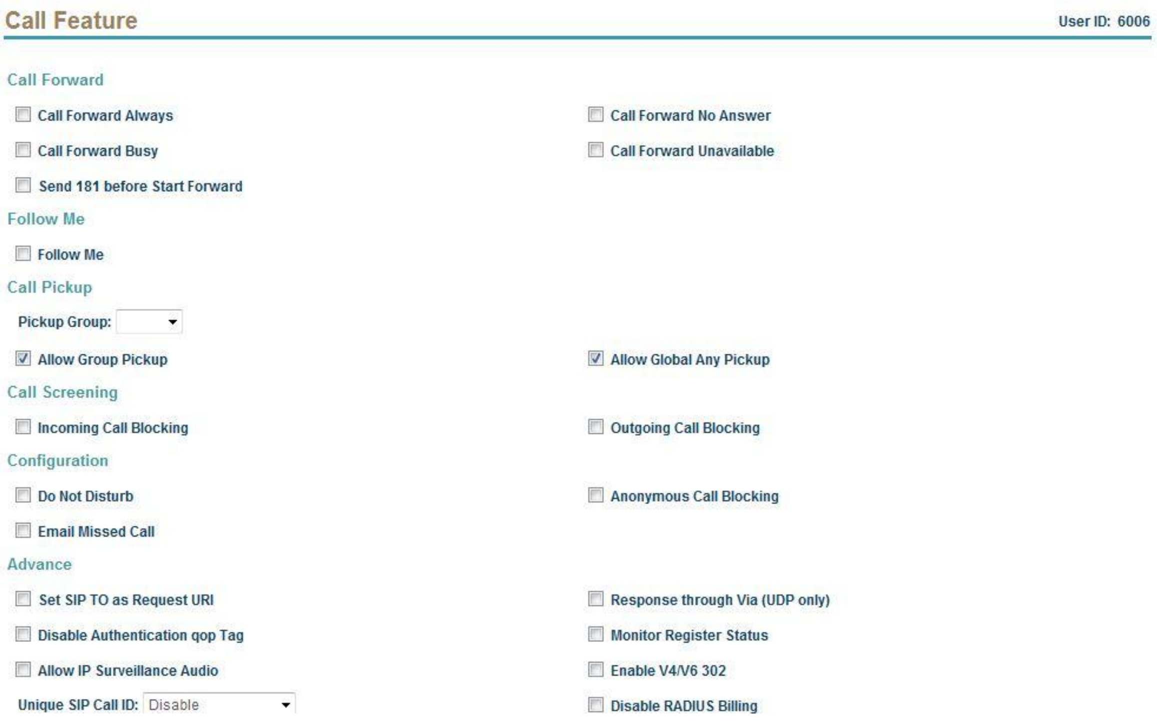
The detail of AA/VMS Setting parameters are described as below:

Parameter Name	Description
Voice Mail	Whether enable or disable the voice mail.
Voice Mail Password	The password to access the voice mail.
Outgoing Call within AA	Whether allow to dial out to PSTN (not extension) within AA.
Personal Greeting	The personal greeting when get into the extension's voice mail.
Personal Greeting File	The wav file for personal greeting. The file format is 8K * 16 bits linear PCM Mono Wav. You can upload your own by clicking upload button.
Disable Voice Mail Recording	Whether disable voice mail recording or not. When it is enable, you need to have your own personal greeting.
SIP Notice	SIP WMI Notify when voice mail changes.
Notify without Subscribe	Enable to send NOTIFY without SUBSCRIBE. This is un-usual. Normally, this should be disabled.
Email Notice	Email Notify when a new voice mail arrived.
Email Address	The mail address for send notice
Delete Email after send it to email	Delete the original voice mail after send the email notice with attachment out.
Marked as Read	Marked the original voice mail become old after send the email notice with attachment out.
Voice Mail Language	The default voice mail language for this extension
My Phone	It is available for smart calling feature only. This field will be used to set the default call back phone number such as mobile number.
Notify to Answer for Outgoing Call Request	It is only available for smart calling feature. When it is enabled and use outgoing call (Call To) or click to call feature, the system will send SIP NOTIFY to ask this extension answer and then start to calling out to the Call To

Parameter Name	Description
	number.

2.3.2.1 Call Feature

Each extension can enable or disable the call feature individually by click ***Call Feature*** button. The following screen will appear.



The detail of each parameter is described as below:

Parameter Name	Description
Call Forward Always	Enable call forward always.
Always Forward Number	The telephone number to be forwarded

Parameter Name	Description
Call Forward No Answer	Enable call forward for no answer call.
No Answer Forward Number	The telephone number to be forwarded
Call Forward Busy	Enable call forward for a busy call.
Busy Forward Number	The telephone number to be forwarded
Call Forward Unavailable	Enable call forward when SIP client is not registered.
Unavailable Forward Number	The telephone number to be forwarded
Send 181 before Start Forward	Enable to send 181 (call is being forwarded) before start forward.
Follow Me	Enable Follow Me here service or not. When enable follow me, the Follow Me number should be defined.
Follow Me Hunting First	When follow me is enabled and "Follow Me Hunting First" is check, the system will try to call the follow me matched entries and then try extension (if Hunting Extension is checked). If "Follow Me Hunting First" is not checked, the system will call the extension first and then hunt the follow me matched entries. The normal case will be enable all follow me options.
Hunting Extension	Enable to hunt extension after follow me entries cannot be reached.
Pickup Group	The belonged pickup group for picking up the group's phone calls.
Allow Group Pickup	Enable to allow the same group extension to pickup the call. If it is unchecked, other extension at the same pickup group will not able to pick this extension.
Allow Global Any Pickup	Enable to allow the any extension to pickup the call. Both extensions do not require at the same pick group. If it is unchecked, there is no any extension can pick up the call by using Global Any Pickup access code.

Parameter Name	Description
Incoming Call Blocking	When it is checked, the incoming call will be filtered by matching the "calling party number" with "Incoming call blocking list". If it is matched, the call will be rejected.
Outgoing Call Blocking	When it is checked, the dialed number will be filtered by "Outgoing Call Blocking List". If the leading pattern was matched the list, the call will be rejected.
Do Not Disturb	Enable Do Not Disturb or not. When DND is enabled, the desired period for DND should be defined.
Anonymous Call Blocking	When the incoming call doesn't include the caller ID, whether to reject it or not.
Email Missed Call	If the extension is unable to take the call, whether to send a email to extension owner or not.
Set SIP TO as Request URI	Make sure to set the SIP TO header is same as Request URI if it is checked.
Response through Via (UDP only)	Send the SIP response message back to the top via instead of using the registered ports.
Disable Authentication qop Tag	Whether to send qop tag for SIP authentication (401/407) or not.
Monitor Register Status	If it is check, the system will report the device status. If it is not registered or re-registered, a record will be written to Extension Status Detail for tracking. It is useful if administrator would like to keep the watch of this extension.
Allow IP Surveillance Audio	Allow 2 way voice (audio) to SIP surveillance camera or not. This option is only available when surveillance module is installed.
Enable V4/V6 302	Whether enable v4/v6 302 moved or not? This can be applied only for a V4/V6 dual stack CPE device. The default is disabled since the system will do the V4/V6 traversal automatically.
Unique SIP Call ID	Whether enable the Unique SIP call ID for each call or not. It is related to parallel ringing case. The device might reject the second call when using same SIP call ID. Please contact FAE for usage. The default is OFF.

Parameter Name	Description
Disable RADIUS Billing	Whether to disable the RADIUS Billing send or not. If it is set to yes, the system will not send any RADIUS billing out and this number will not be billing. Normally, it should be set to No.
Server Transfer SDP	SDP will be used when starting a server based consultant transfer. The following option can be set: 1. Full Codec SDP: Use full caller SDP to invite the transferred party. 2. Negotiated Codec: Use first call's negotiated SDP (only 1 codec) to invite the transferred party.
Contact as TO for 200 OK	Whether to set Contact as TO header for 200 OK response message or not.
Set Diversion to User	Whether always add Diversion header no matter it is a diverted call or not.
Called Number(DNIS) From	Which header will be used to get DNIS (called number)? It could be TO header (default) or Request URI.
Disable Over Max Call Notice	Whether disable the system alert when this extension is over max call or not.
Send to Existing TCP Connection	Whether to send SIP request to the existing register TCP connection no matter it is coming from NAT or not. The default system behavior is that when the called party is seating in a public IP network, the system will send to its TCP contact instead of using existing TCP connection. Enable this, the system will overwrite the rule and send the SIP request through the existing TCP connection.
Add RFC-2833 if not in SDP	Added RFC 2833 into SDP if RFC2833 DTMF event is not found in SDP. It is useful for those SIP trunk doesn't support RFC2833 in SDP offer but can use it when answer to have it.
Copy Display to ANI	Whether copy Display name into SIP user part (ANI) or not? This is a special usage, please contact technical support for using it.
Set Refer-by to ANI	Use SIP Refer-by user to become an SIP user part (ANI) for newly created outgoing call leg.
Webrtc SIP Hack	reserved only

Parameter Name	Description
Disable Video Call	Whether to allow video call to be madden or not?
Enable Distinctive Ringing	Whether enable or disable distinctive ringing feature? This feature need a compatible SIP phone to support this feature.

2.3.2.1.1 Follow Me

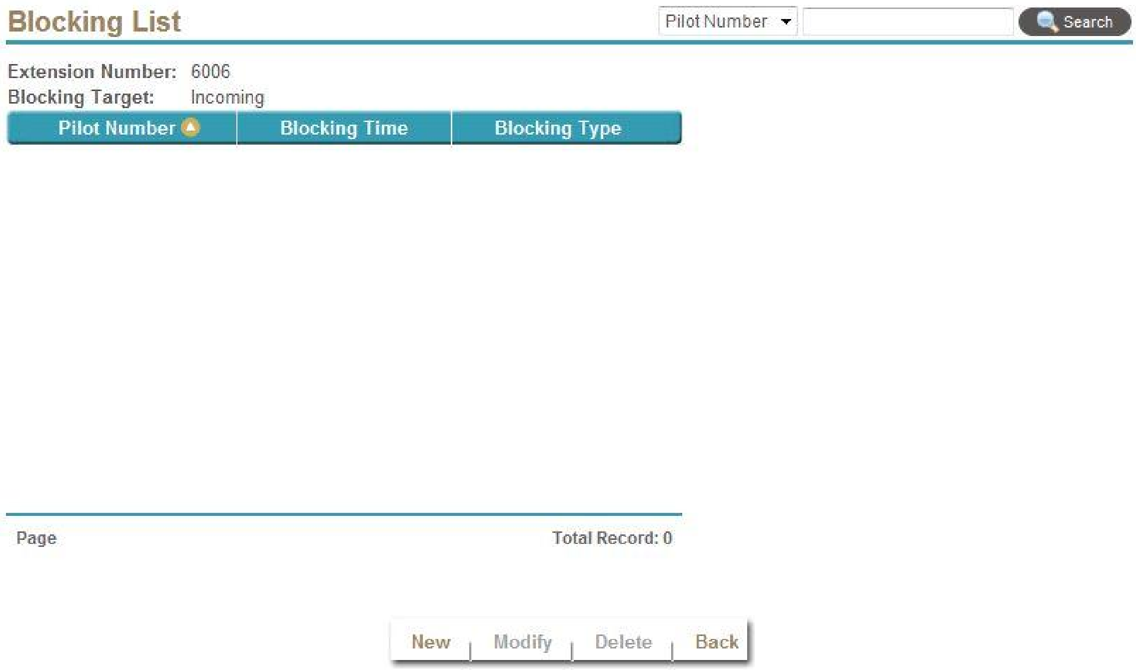
The follow me time should be defined here when ***Follow Me*** service was enabled in ***Call Feature***. Click ***Follow Me*** button to set the following me period and number as follows:

The detail of each parameter is described as below:

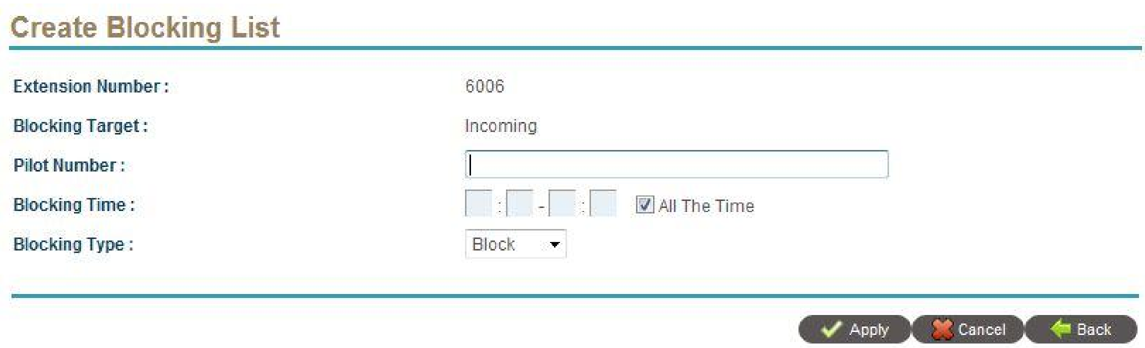
Parameter Name	Description
Start Time	The start time (24 hours format) to enable this follow me number. Earlier than this time, this follow me number will be ignored. You can also click the "All the Time" for whole day service.
Stop Time	The stop time (24 hours format) to enable this follow me number. Over this time, this follow number will be ignored. You can also click the "All the Time" for whole day service.
Weekday	The applied weekday for this following me number.
Follow Number	The telephone number to be followed when the time is in between start and stop time.

2.3.2.1.2 Incoming Call Blocking List

When enabled the incoming call block feature in call feature screen. The calling party number defined here will be filtered based on the blocking type.



Select New, Modify, Delete to change the screening setting. The following web page will appear:



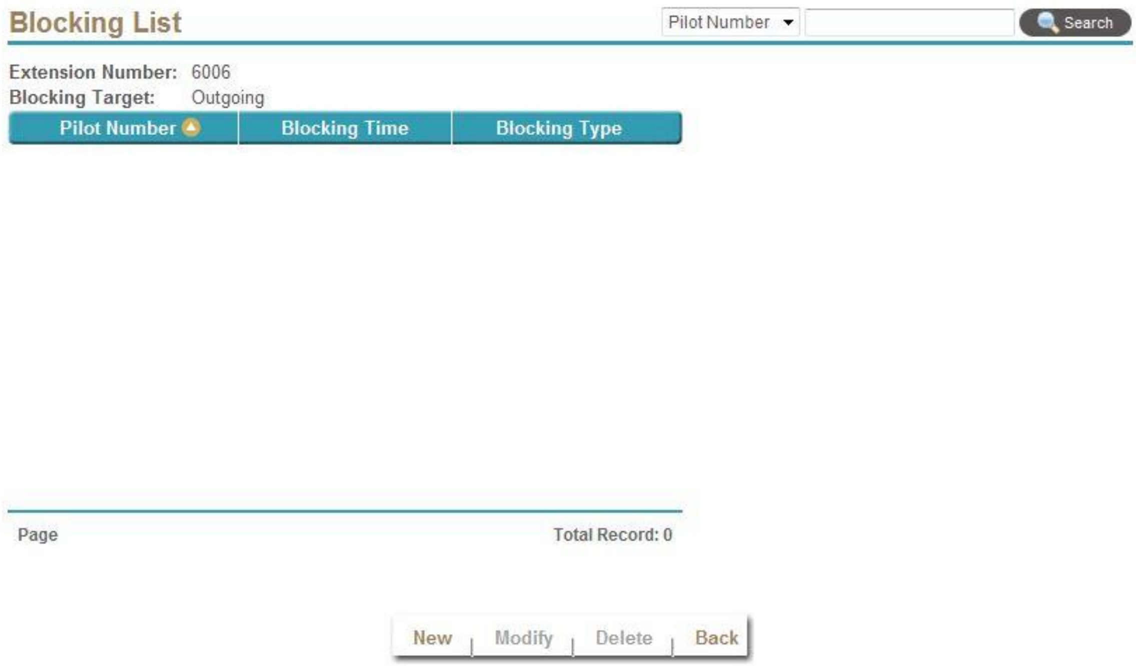
The detail of each parameter is described as below:

Parameter Name	Description
Blocking Target	Incoming call or outgoing call to be screened.

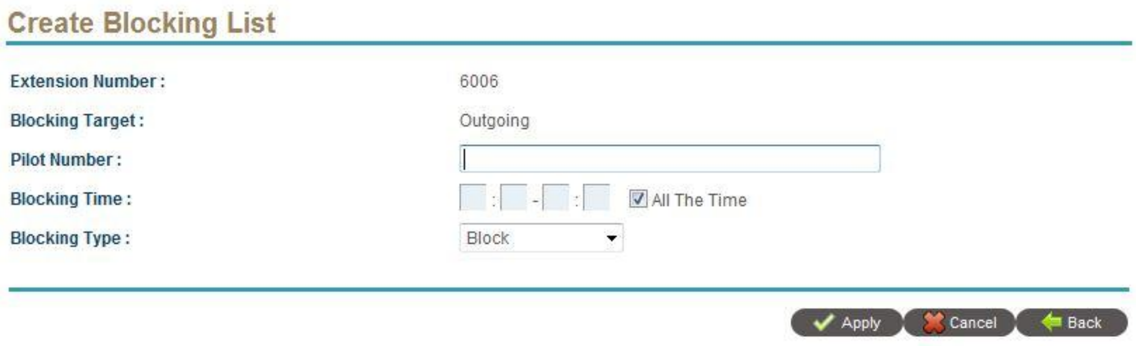
Parameter Name	Description
Pilot Number	The calling number used to be matched. If incoming calling number (SIP user part) is matched, the call might be rejected or accepted based on the "Blocking Type".
Blocking Time	The system allow to have time restricted screening feature. When you enter the blocking time for a screening list, this screen will only affected by this certain period.
Blocking Type	Whether to block or unblock it. When all entries in the same group are set to "block", it means all call can be passed unless those listed pilot number. When all entries are set to "unblock", only those calls matched the entry will able to get through. If some of entries are set to "block" and some are set to "unblock", the call matched "blocked" list will be rejected first and the call matched "unblock" list will able to get through.

2.3.2.1.3 Outgoing Call Blocking List

When enabled the outgoing call block feature in call feature screen. The called number prefix defined here will be filtered based on the blocking type.



Select New, Modify, Delete to change the screening setting. The following web page will appear:



The detail of each parameter is described as below:

Parameter Name	Description
Blocking Target	Incoming call or outgoing call to be screened.
Pilot Number	The called number prefix used to be matched. If the outgoing number prefix is matched the pilot number, the call might be rejected or accepted based on the "Blocking Type".
Blocking Time	The system allow to have time restricted screening feature. When you enter the blocking time for a screening list, this screen will only affected by this certain period.
Blocking Type	Whether to block, unblock or privilege access for the pilot number prefix. When all entries in the same group are set to "block", it means all call can be passed unless those listed pilot number. When all entries are set to "unblock", only those calls matched the entry will able to get through. If some of entries are set to "block" and some are set to "unblock", the call matched "blocked" list will be rejected first and the call matched "unblock" list will able to get through. For those entries are set to "privilege access", it will able to get through when you use "Enable Privilege Access" access code to turn it on to call and use "Disable Privilege Access" access code to turn it off.

2.3.2.2 Voice Mail Access

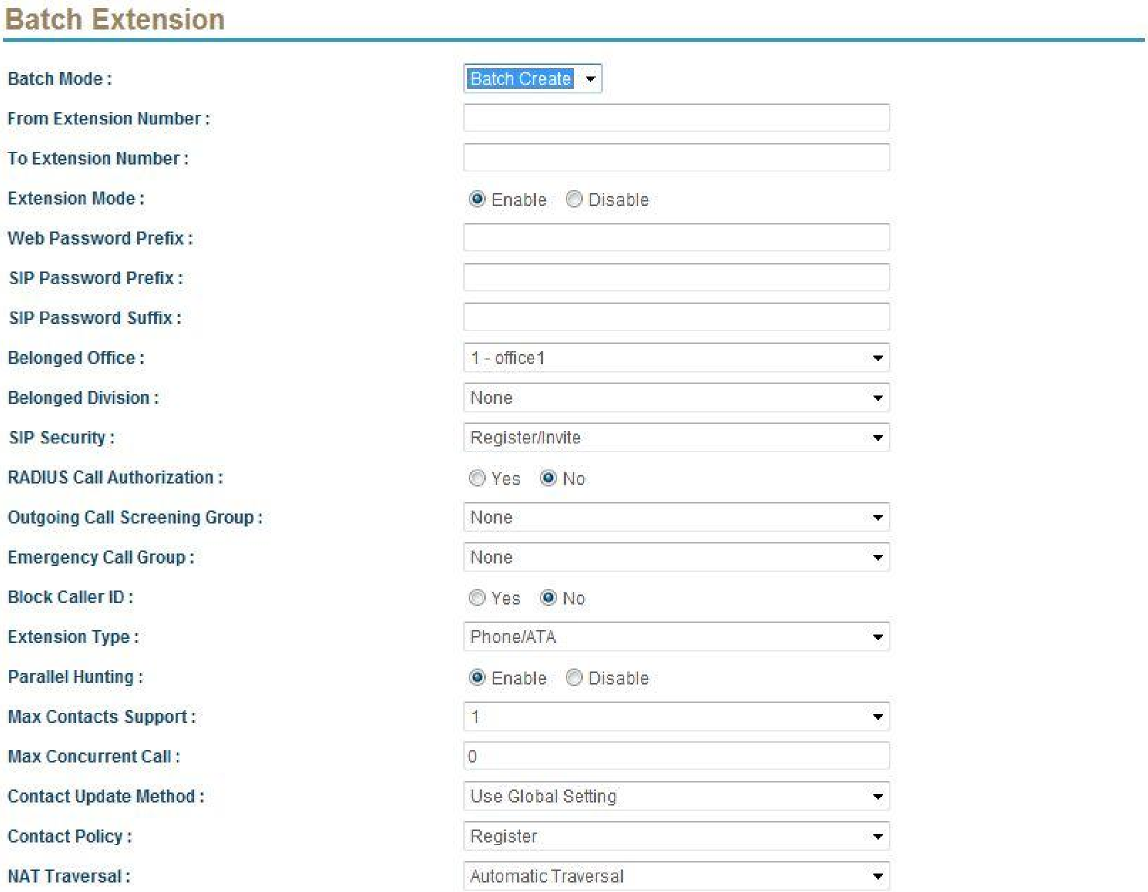
The extension users can access their owned voice mail either by web or phone. To check voice mail by web, click ***EXTENSION -> Extension -> Voice Mail Access*** and the following screen will be displayed.

You can double click the item to hear the voice mail. The detail of each parameter is described as below:

Parameter Name	Description
Calling Time	The time to start the call
Calling From	The calling party number
Status	Whether the voice mail was read or not?

2.3.2.3 Batch Create

Batch create is mainly used for creating testing data. Click ***EXTESNION -> Extension -> Batch*** and the following screen will appear.



The detail of each parameter is described as below:

Parameter Name	Description
Batch Mode	The way to batch create extension: Batch Create: Create extension numbers in between "From Extension Number" and "To Extension Number". The existing number will be ignored. Batch Modify: Replace the existing record by using the current settings in between "From Extension Number" and "To Extension Number". Only existing extension will be replaced. Batch Delete: Delete the extension in between "From Extension Number" and "To Extension Number".
From Extension Number	Beginning extension of batch creating
To Extension Number	Ending extension of batch creating

Parameter Name	Description
Web Password Prefix	The prefix for the web password. The system will set the default web password as "Web Password Prefix"+"Extension Number". For security reason, it is recommended to set a prefix instead of keeping blank.
SIP Password Prefix	The prefix for SIP password. The system will set the default SIP password as "SIP Password Prefix"+"Extension Number"+"SIP Password Suffix". For security reason, it is recommended to set a prefix and suffix instead of keeping blank.
SIP Password Suffix	The suffix for SIP password. The system will set the default SIP password as "SIP Password Prefix"+"Extension Number"+"SIP Password Suffix". For security reason, it is recommended to set a prefix and suffix instead of keeping blank.
Others Parameters	Please refer to Extension parameters for detail

2.3.2.4 Phone Book

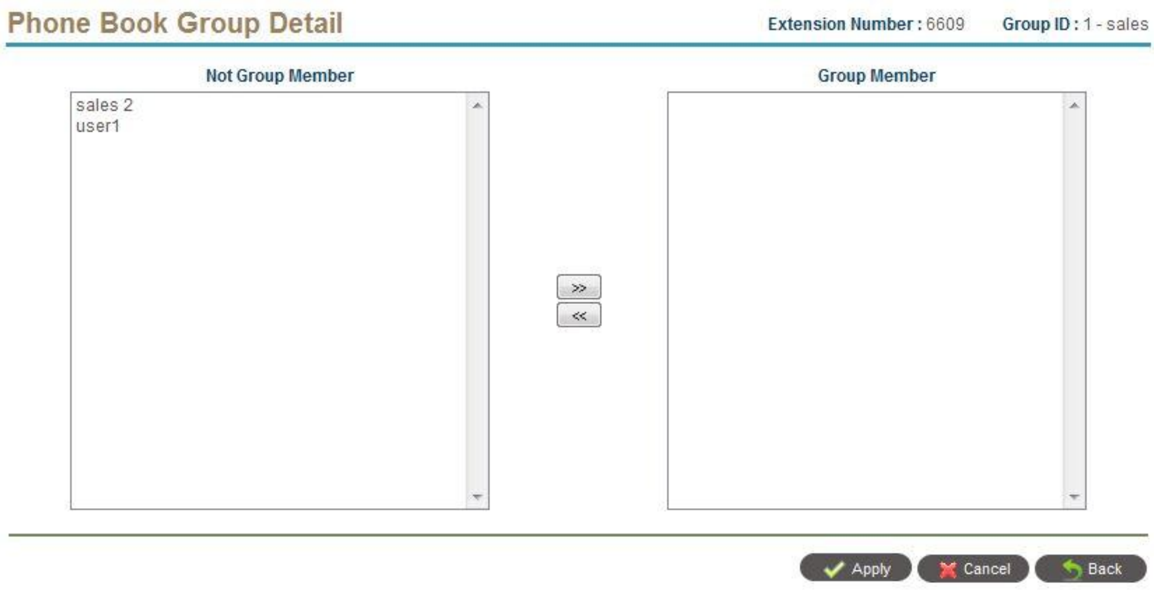
The phone book will be used when smart calling feature was purchased. It can speed up the smart phone user to start a conference or a out call easily. Click EXTENSION -> Extension -> Phone Book and the following will appear.

Click New to add a new phone book entry as follows.

Input the name and telephone number to create an entry of phone book.

If you want to create a group to be used later, click Phone Book Group -> New and the following will appear.

Input the group ID and Group name to create a phone book group. Then click Phone Book Group -> Detail and select the extension into the group as follows.



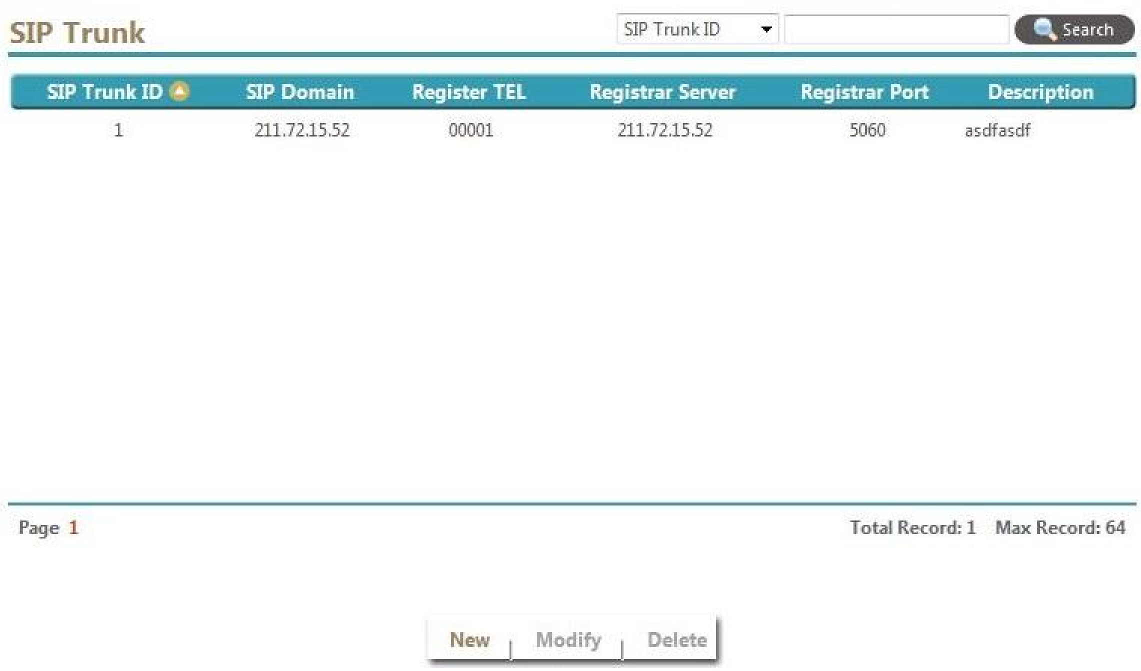
Click >> to assign the extension to the group or << to un-assign it.

2.4 Feature

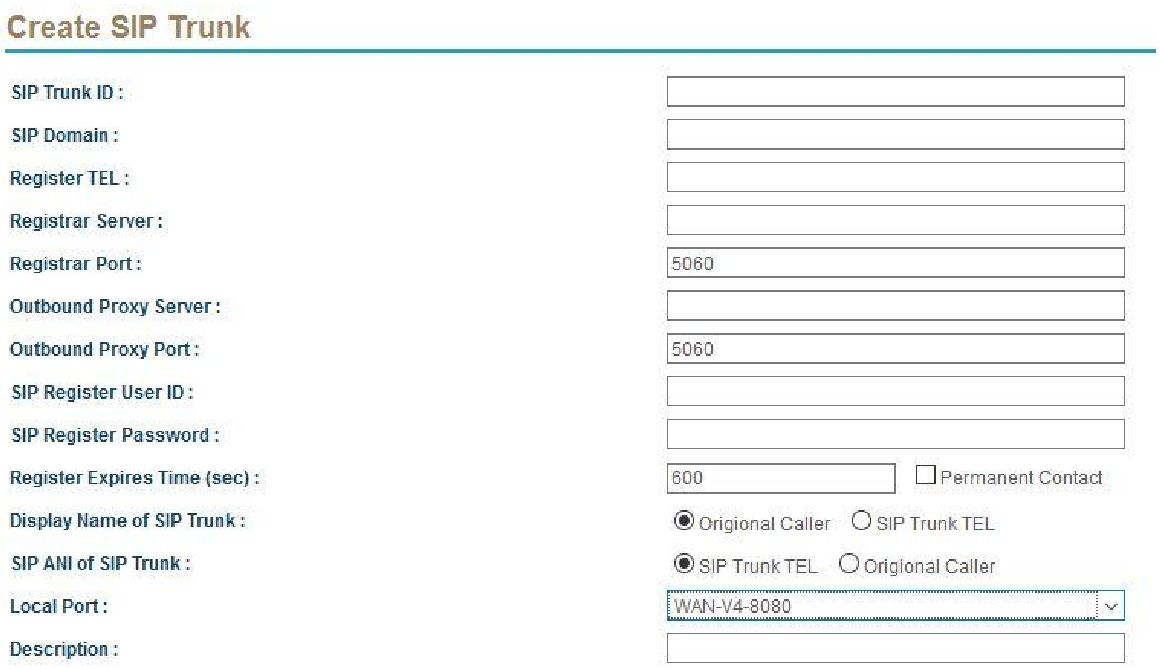
The system provides the flexible SIP trunking, digit manipulation, routing plan, DNIS screening group and others can be defined here. Those features is core for providing required services for customers.

2.4.1 SIP Trunk

The SIP trunk is used to register to a VOIP carrier or another SIP proxy server. After input the SIP register or calling information here, you need to create a extension to associate it together in order to making a call. The maximum SIP trunk could be created is 64. Click ***FEATURE-> SIP Trunk*** to view the created SIP trunk.



Select New, Modify, Delete to change the SIP Trunk setting. The following web page will appear:

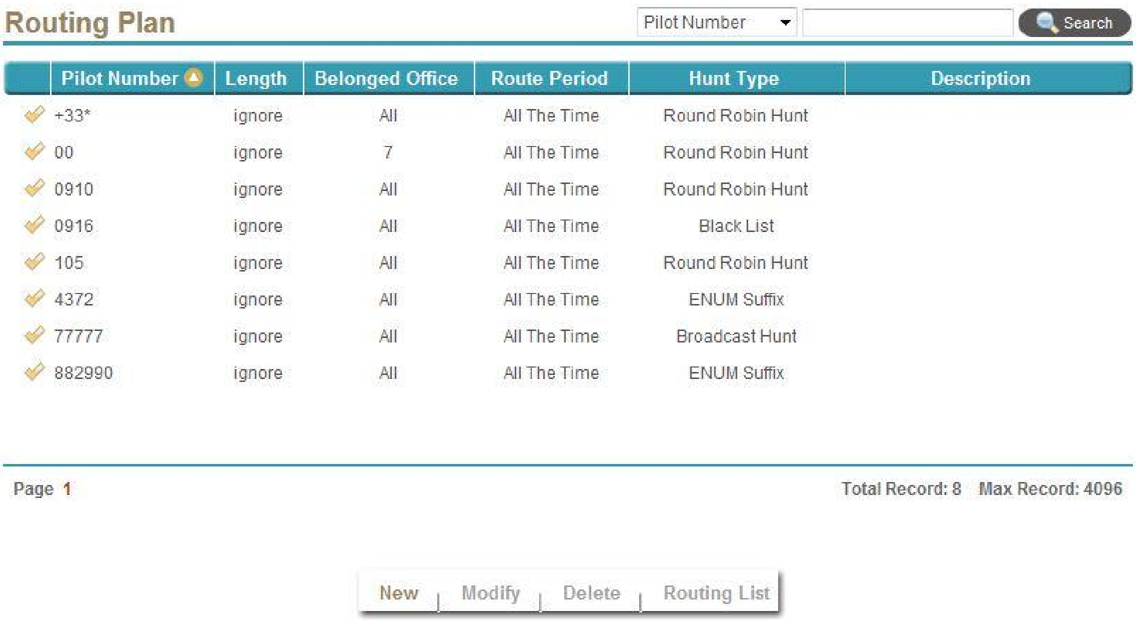


The detail of each parameter is described as below:

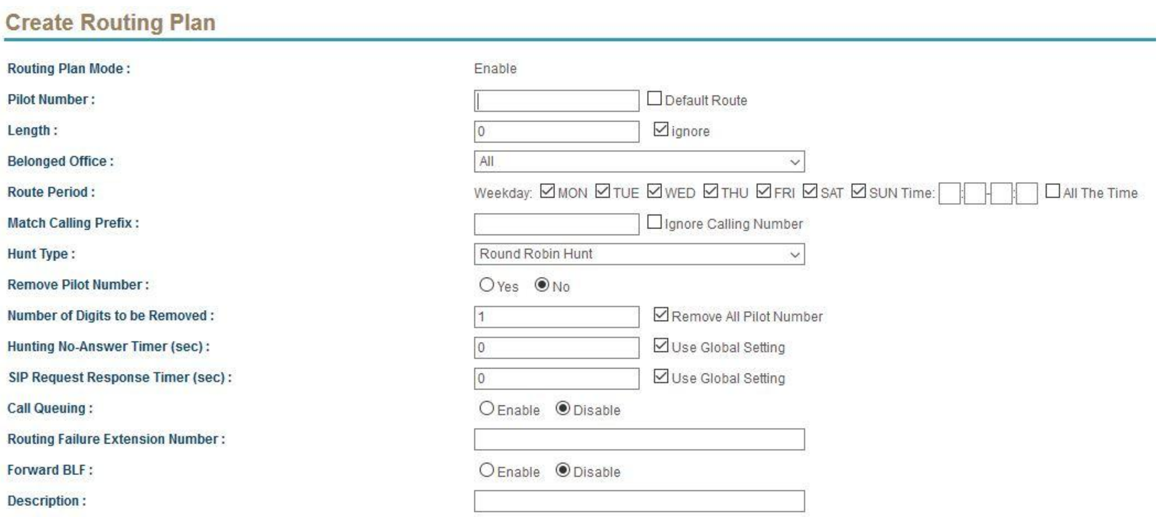
Parameter Name	Description
SIP Trunk ID	SIP trunk ID
SIP Domain	The SIP register domain for SIP trunk user
Register TEL	The SIP User (normally, it is TEL number) for register
Registrar Server	The SIP registrar proxy server IP address or DNS name.
Registrar Port	The SIP service port to register (default value is 5060)
Outbound Proxy Server	The SIP outbound proxy IP address or DNS name
Outbound Proxy Port	The outbound proxy service port (default value is 5060)
SIP Register User ID	The SIP user ID for authentication
SIP Register Password	The SIP password for authentication
Register Expires Time	The register expires in seconds for SIP register. The default is 600 seconds.
Permanent Contact	If this is checked, this SIP trunk will no register and use peering instead.
Display Name of SIP Trunk	The SIP Display Name will be used when this SIP trunk is calling. The default is original caller's SIP TEL.
SIP ANI of SIP Trunk	The SIP TEL will be used when this SIP trunk is calling. The default is SIP trunk's TEL.
Local Port	The local SIP port will be used for this SIP trunk. For most of case, it will be 5060 port.
Description	The description for this SIP trunk

2.4.2 Routing Plan

The routing plan is used to provides different routing based on prefix, time of day, dialed length and hunting type to decide where the call should be called. The maximum Routing Plan could be created is 4096. Click ***FEATURE -> Routing Plan*** to view the current created routing plans as follows:



Select New, Modify, Delete to change the routing plan. The following web page will appear:



The detail of each parameter is described as below:

Parameter Name	Description
Routing Plan Mode	Activate this routing plan or not
Pilot Number	The leading number (prefix) used to be matched with the called number.

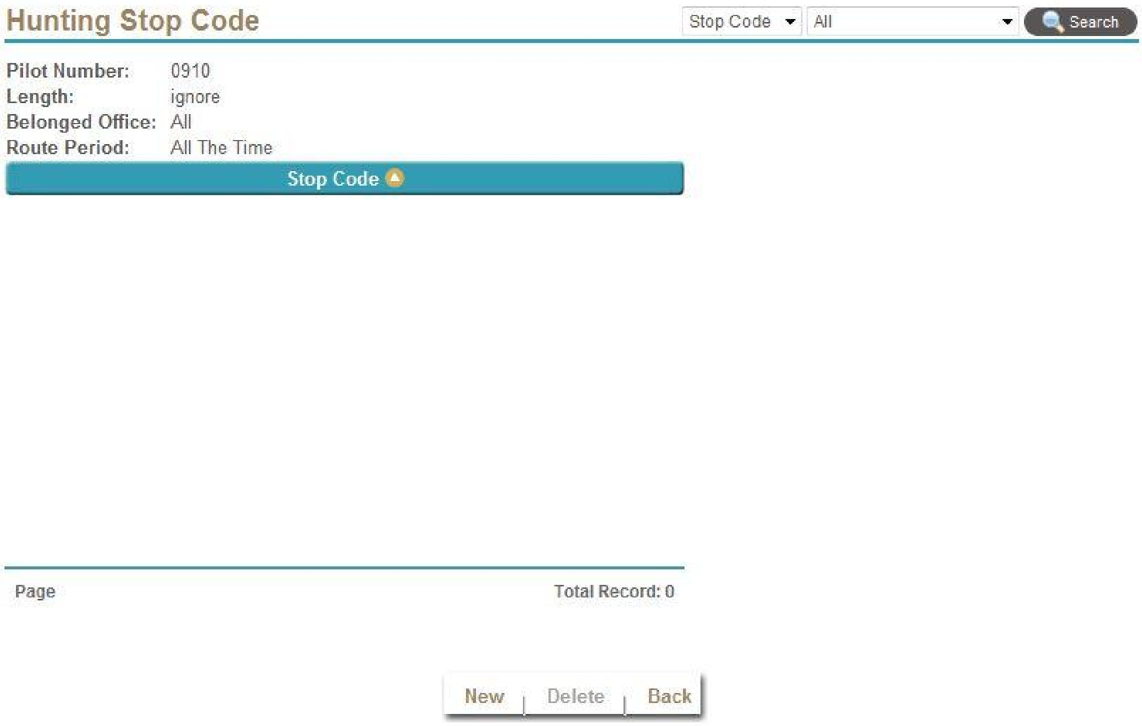
Parameter Name	Description
Length	The length to be matched for the called number length. If "ignore" is checked, the length matching is ignored.
Belonged Office	The selected office will be applied to this routing. Select "All" if don't need group filter.
Route Period	The time of day and weekday to execute this route. You can also specified a time such as 20:00-0800 for overnight setting or check the "All the Time" button to have whole day service.
Match Calling Prefix	Whether to match calling party number (ANI) prefix for this routing or not.
Hunt Type	The hunting type of this route: Round Robin Route: call is hunted rotary until one is answered. Preference Hunt: The highest preference priority will be hunt first and then lower one until one is answered. (0 is lowest and 9 is highest) Broadcast Hunt: the system will call all the entries of routing list simultaneously until one of them is answered. Round Robin Hunt (Load Balance): The call is hunted rotary until one is answered or the response reason code is matched the Hunting Stop Code. Preference Hunt (Load Balance): The highest preference priority will be hunt first and then lower one until one is answered or the SIP response reason code is matched the Hunting Stop Reason (0 is lowest and 9 is highest). Black List: Call to this route (matched pilot number prefix) will be rejected. It could be used to protect the system for calling those expensive countries and avoid the VOIP attack. ENUM Hunt: Using ENUM query to get the called party's SIP url and call to it. The ENUM suffix need to be specfied in order to make the correct ENUM DNS query. Customized Route: Internal used only.
ENUM Suffix	The ENUM NAPTR queried DNS domain suffix. It could be "e164.arpa" or others.
Remove Pilot Number	Check it to remove the pilot number before calling.

Parameter Name	Description
Hunting No-Answer Timer	No answer time out in seconds for this route. The default value is " Use Global Setting" which means use the global setting in SYSTEM-> Service Parameter.
SIP Request Response Timer	SIP Request response time out for this route. The default value is " Use Global Setting" which means use the global setting in SYSTEM-> SIP Timer.
Call Queuing	Whether enable call queue feature or not? If it is enabled and all extensions are not able to answer the call, the call will be put on queue and call queue music will be played. There are 2 prompts will be played. The first prompt is xxx_0.wav which will be played once and repeat play the xxx_1.wav after it. xxx is the queuing music ID.
Queuing Music ID	There are 2 prompts will be played for each queue. The first prompt is xxx_0.wav which will be played once and repeat play the xxx_1.wav after it. xxx is the queuing music ID.
Forward BLF	Whether to forward BLF to this routing prefix if it is matched. It is used only when this routing is to VMS and is for call park and working hour BLF.
Routing Failure Extension Number	If all of entries for route cannot be reached or stopped, here is the last destination to be routed. This is normally to route to an voice mail such *521234 or a a mobile such as 092322221111.
Description	The description for this route

2.4.2.1 Hunting Stop Code

For the routing plan which hunt type is "load balance" mode, the ***Hunting Stop Code*** is used to quit the hunting. It is typical be used when the system had multiple gateway or carrier. Normally, when a gateway return with the reason code of busy or gone, the system should normally stop the hunting. It indicates the user might be busy or cannot be reached, route to next gateway or carrier will not help also. Hunting Stop Code could be changed to meet the different hunting requirements:

Click ***Hunting Stop Code*** button after enter the modification page of a routing plan. The following web page will appear:



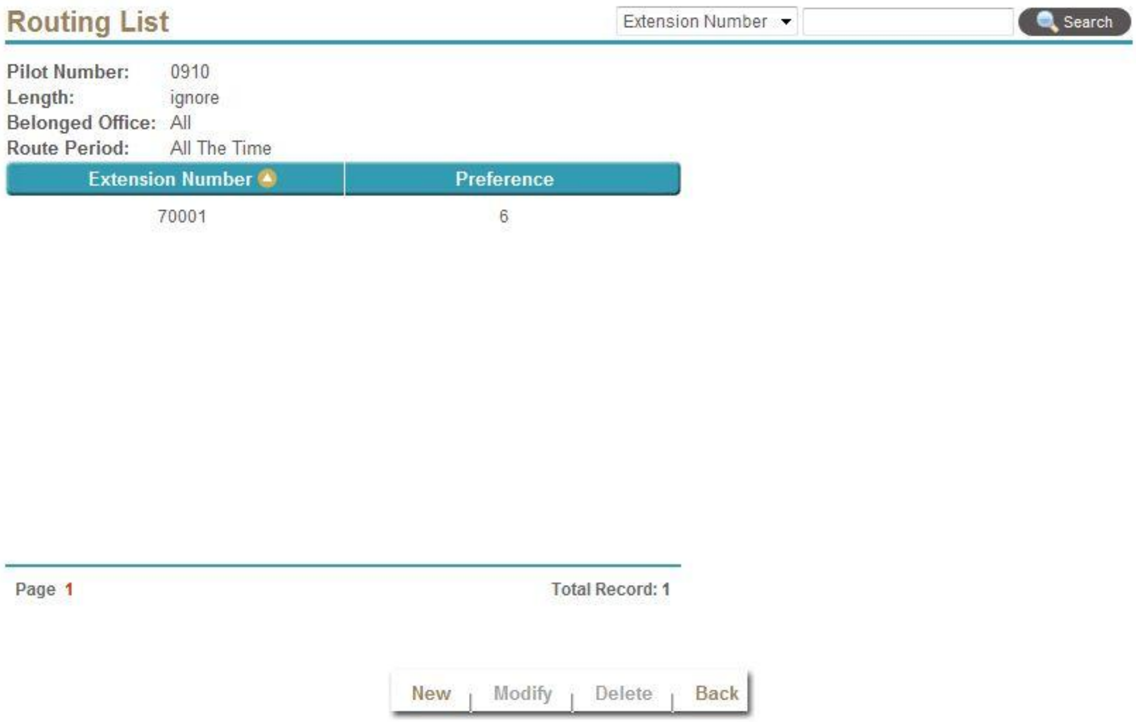
Select New, Modify, Delete to change the Hunting Stop Code. The following web page will appear:

The detail of each parameter is described as below:

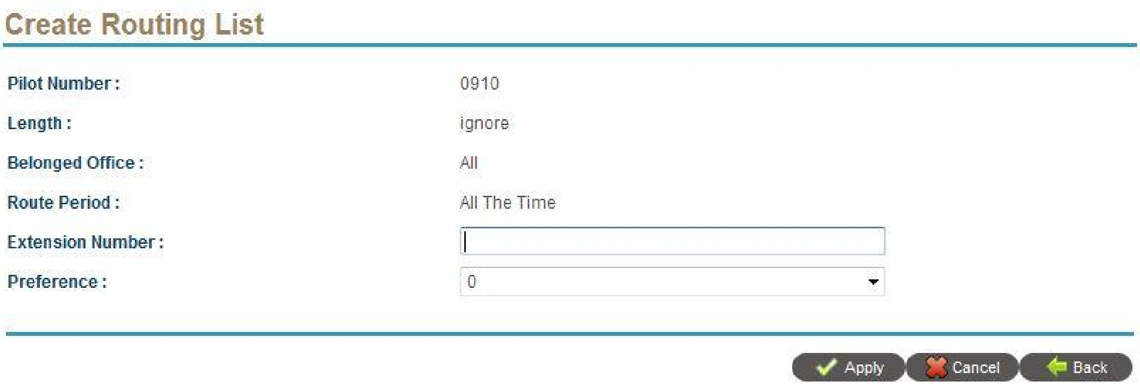
Parameter Name	Description
Stop Code	The reason code to be used for stopping the hunting. If the reason code are not listed, you can enter the SIP response code here to stop the hunting.

2.4.2.2 Routing List

Each routing plan contains multiple routing devices, such as gateway, VOIP carrier or extension. Here is the place to define where to be routed. Click ***Routing List*** button after select a routing plan. The following screen will appear:



Select New, Modify, Delete to change the Routing List setting. The following web page will appear:



The detail of each parameter is described as below:

Parameter Name	Description
Extension Number	The extension to be added to this routing plan.
Preference	The preference priority number: 0 is lowest and 9 is highest. The higher value indicate higher preference for preference route.

2.4.3 Digit Manipulation

Digit Manipulation is used to manipulate the calling or called number. The administrator can insert, delete or change some digits from original number. The digit manipulation can be place on caller, called or both for flexible usage. The maximum Digit Manipulation could be created is 4096.

Click ***FEATURE -> Digit Manipulation*** to view the current settings. The following web page will appear.

Select New, Modify, Delete to change the Digit Manipulation Group setting. The following web page will appear:

The detail of each parameter is described as below:

Parameter Name	Description
Group ID	Digit Manipulation Group ID
Description	The description for this Digit Manipulation Group

2.4.3.1 DM Group List

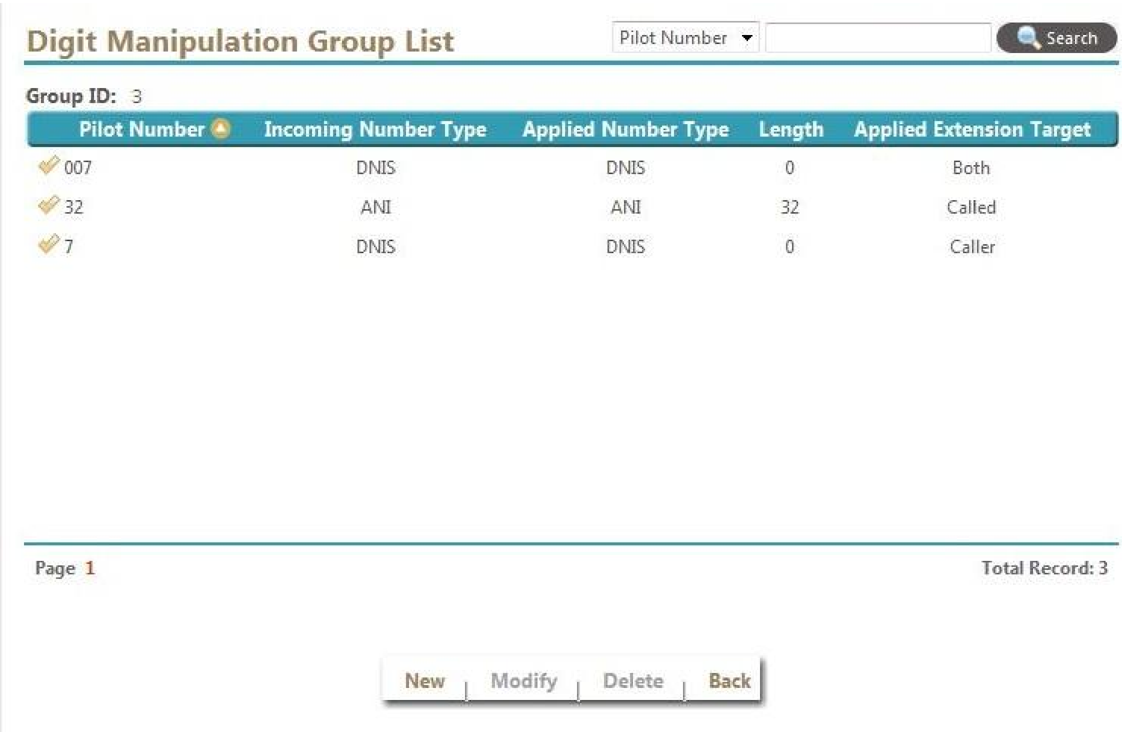
The detail operation list for the digit manipulation group. The process policy of digit manipulation list within the group is showing as below:

Step 1. Search "Incoming number Type" is equal to "ANI" and pilot number is matched incoming ANI. If found, do the following:
- Change ANI based on the DM list when "Applied Number Type" is equal to ANI.
- Change DNIS based on the DM list when "Applied Number Type" is equal to DNIS.

Step 2: Search "Incoming number Type" is equal to "DNIS" and pilot number is matched incoming DNIS. If found, do the following:
- Change ANI based on the DM list when "Applied Number Type" is equal to ANI.
- Change DNIS based on the DM list when "Applied Number Type" is equal to DNIS.

The caller DM will be done before RADIUS authorization and called DM is after RADIUS authorization. It indicates that called DM will not affect the RADIUS billing.

Click ***Group List*** button after select a Digit Manipulation Group. The following web page will appear.



Select New, Modify, Delete to change the Digit Manipulation List. The following web page will appear:

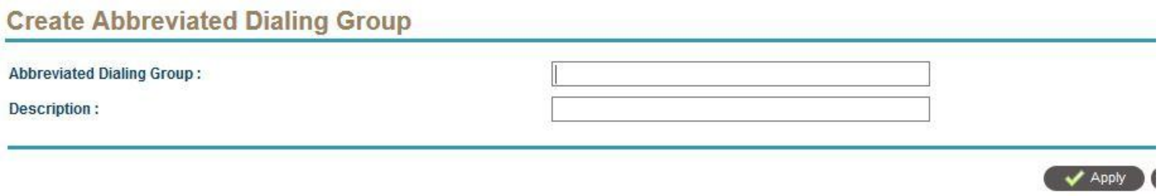
The detail of each parameter is described as below:

Parameter Name	Description
Mode	Activate this digit manipulation group or not
Pilot Number	The leading number (prefix) to be matched
Incoming Number Type	The incoming number type to be matched. It could be calling number (ANI) or called number (DNIS). For most of case, the DM incoming type will be DNIS.
Applied Number Type	The target to be manipulated. It could be calling number (ANI) or called number (DNIS). For most of case, the applied number type is DNIS.
Length	If the length is greater than 0, it means the incoming number requires to have the same length. If it is equal to 0, length mating will be ignored.
Applied Extension Target	When it is set to "caller", this DM will be applied when the extension is making the call out. When it is set to "called", the DM will be applied when the extension has been selected to be called. When it is set to "Both", the DM will be applied when the extension is calling and called. For normal case, it should be set to "caller".
Start Position	The start position to be replaced. Before the first digit, the position is 0. Between digit 1 and digit 2, the position is 1 and so on. If the position is greater than the digit length, it indicates after last digit.
Stop Position	The stop position to be replaced. Before the first digit, the position is 0. Between digit 1 and digit 2, the position is 1 and so on. If the position is greater than the digit length, it indicates after last digit.
Replace Value	The value to be placed after remove the digit in between start and stop position. You can keep it empty if only required to delete those digits in between start and stop. The following are the examples of the DM rule: Number to be DM: 1234567, Start position: 0, stop position: 0, Replaced value: "002", DM result: 0021234567. Number to be DM: 1234567, start position: 2, stop position: 6, replaced value: "002", DM result:120027 Number to be DM: 1234567, start position: 24, stop position: 24, replace value: "002", DM result: 1234567002. Number to be DM: 1234567, start position: 1, stop position: 2, replaced value: "", DM result:134567.

2.4.4 Abbreviated Dialing

The abbreviated dialing group is used to replace the dialed abbreviated number to the real telephone number. Click ***FEATURE -> Abbreviated Dialing Group*** to view the current groups of emergency call as follows:

Select New, Modify, Delete to change the Abbreviated Dialing Group setting. The following web page will appear:



The detail of each parameter is described as below:

Parameter Name	Description
Abbreviated Dialing Group	The Abbreviated Dialing Group ID
Description	The description for this Abbreviated Dialing Group

2.4.4.1 Abbreviated Dialing Group List

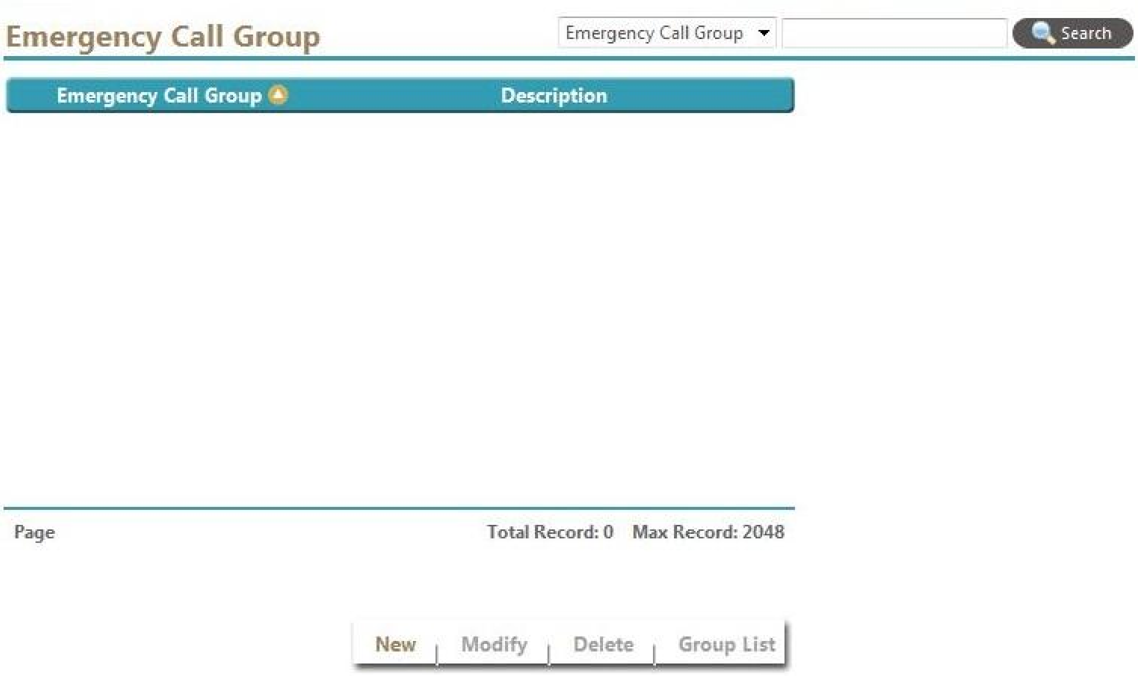
Here is the place to define the replacement of abbreviated number call. Click the ***Group List*** after select a created ***Abbreviated Dialing Group*** as follows:

The detail of each parameter is described as below:

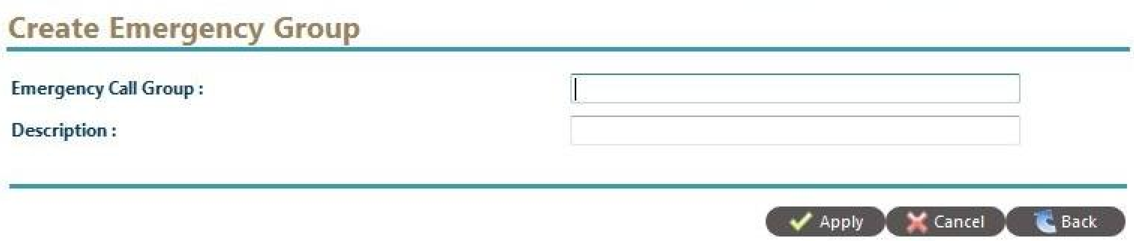
Parameter Name	Description
Abbreviated Dialing Number	The abbreviated dialing number such as *95.
Actual Called Number	The real number to be called for this abbreviated number

2.4.5 Emergency Call Group

The emergency call group is used to replace the dialed emergency call to the real telephone number in order to call the corresponding government office based on the users information. Click ***FEATURE -> Emergency Call Group*** to view the current groups of emergency call as follows:



Select New, Modify, Delete to change the Emergency Group setting. The following web page will appear:

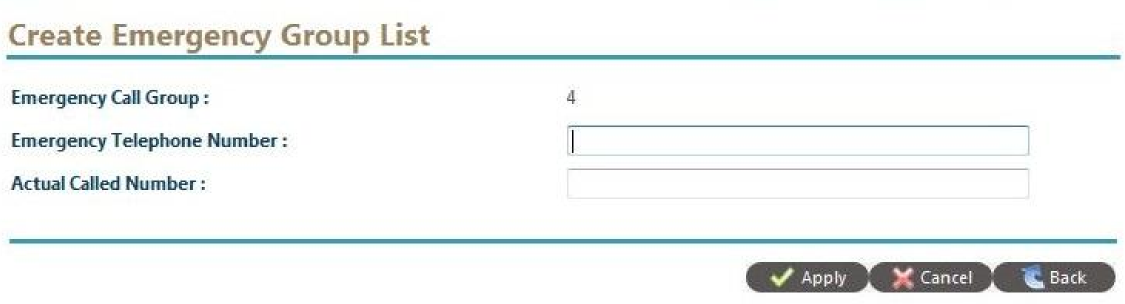


The detail of each parameter is described as below:

Parameter Name	Description
Emergency Group ID	The Emergency Call Group ID
Description	The description for this Emergency Call Group

2.4.5.1 Emergency Group List

Here is the place to define the replacement of emergency call. Click the ***Group List*** after select a created ***Emergency Group*** as follows:

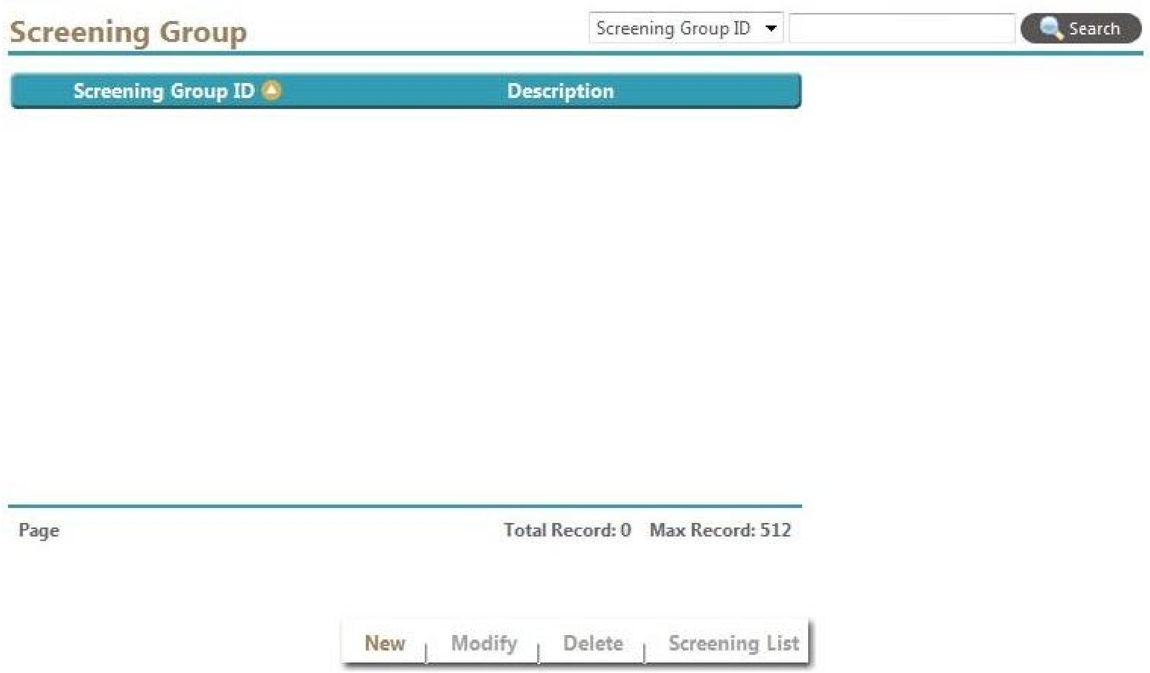


The detail of each parameter is described as below:

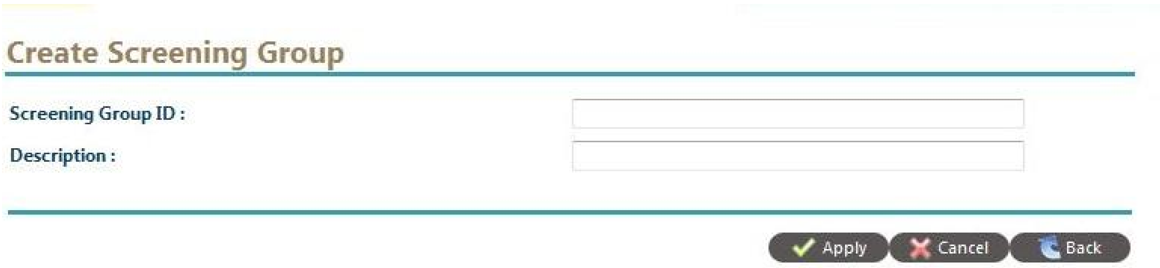
Parameter Name	Description
Emergency Telephone Number	The called emergency number, such as 911, 119, 110 etc.
Actual Called Number	The real number to be called for the emergency call.

2.4.6 Screening Group

There are two outgoing call blocking list could be used. The first is in the ***Extension -> Outgoing Call Screening Group*** and another is personal call screening in ***Extension -> Call Feature -> Outgoing Call Screen***. The ***Outgoing Call Screening Group*** is normally used for system based screening while call feature's outgoing call screen is dedicated for the extension. For the system based screening, you need define the DNIS screening group and the relate detail here. The maximum screen group could be created is 512. Click ***FEATURE -> DNIS Screening Group*** to view the current DNIS screening group as follows:



Select New, Modify, Delete to change the Screening Group setting. The following web page will appear:

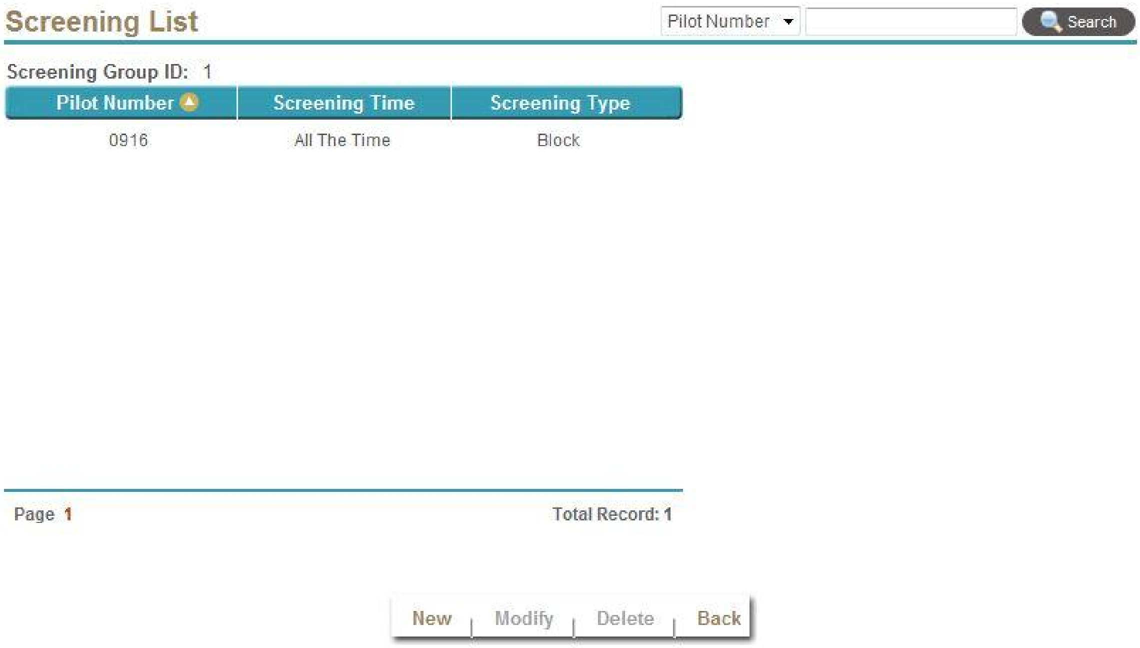


The detail of each parameter is described as below:

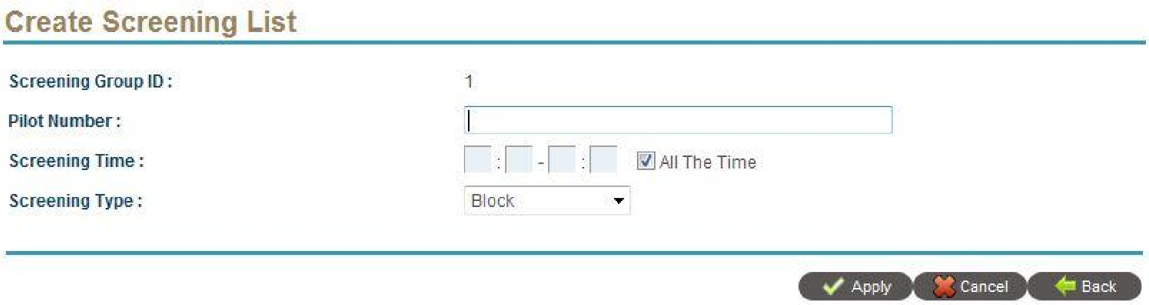
Parameter Name	Description
Screening Group ID	DNIS (called number) screening group ID
Description	The description for this DNIS screening group

2.4.6.1 Screening List

The detail of telephone number to be blocked or un-blcoked for the selected DNIS screening group should be defined here. Click ***Screening List*** button after select a created DNIS Screening Group to view the screening list as below:



Select New, Modify, Delete to change the Screening List setting. The following web page will appear:



The detail of each parameter is described as below:

Parameter Name	Description

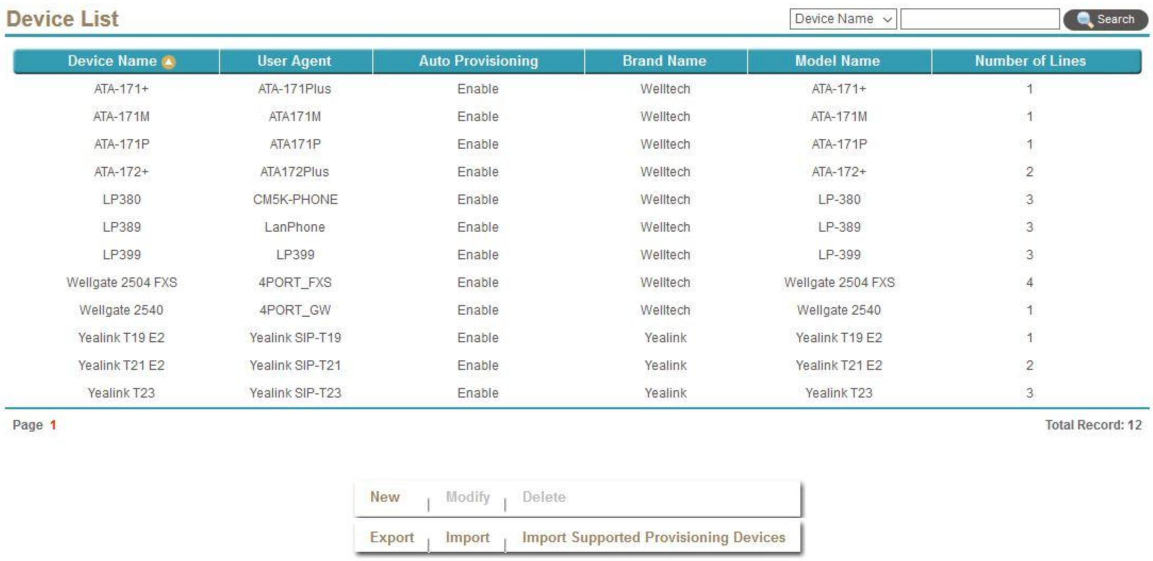
Pilot Number	The called number prefix used to be matched. If the outgoing number prefix is matched the pilot number, the call might be rejected or accepted based on the "Blocking Type".
Screening Time	The system allow to have time restricted screening feature. When you enter the blocking time for a screening list, this screen will only affected by this certain period.
Blocking Type	Whether to block, unblock or privilege access for the pilot number prefix. When all entries in the same group are set to "block", it means all call can be passed unless those listed pilot number. When all entries are set to "unblock", only those calls matched the entry will able to get through. If some of entries are set to "block" and some are set to "unblock", the call matched "blocked" list will be rejected first and the call matched "unblock" list will able to get through. For those entries are set to "privilege access", it will able to get through when you use "Enable Privilege Access" access code to turn it on to call and use "Disable Privilege Access" access code to turn it off.

2.4.7 Device List

Device List is used as a list selection when an extension is using the dedicate device feature and used for CPE auto provisioning. To use CPE auto provisioning, you need to first to click "Import Supported Provisioning Devices" and import all supported device list into the system in order to provisioning them.

For using it only for dedicate device, you will only create a device list first and then can be selected from an extension. If that device has changed its User Agent to others, you can change here and don't need to change all over the extension. The system is using SIP "User-Agent" header to distinct the different device.

Click ***FEATURE -> Device List*** to view the current settings. The following web page will appear.



Device List

Device Name	User Agent	Auto Provisioning	Brand Name	Model Name	Number of Lines
ATA-171+	ATA-171Plus	Enable	Welltech	ATA-171+	1
ATA-171M	ATA171M	Enable	Welltech	ATA-171M	1
ATA-171P	ATA171P	Enable	Welltech	ATA-171P	1
ATA-172+	ATA172Plus	Enable	Welltech	ATA-172+	2
LP380	CM5K-PHONE	Enable	Welltech	LP-380	3
LP389	LanPhone	Enable	Welltech	LP-389	3
LP399	LP399	Enable	Welltech	LP-399	3
Wellgate 2504 FXS	4PORT_FXS	Enable	Welltech	Wellgate 2504 FXS	4
Wellgate 2540	4PORT_GW	Enable	Welltech	Wellgate 2540	1
Yealink T19 E2	Yealink SIP-T19	Enable	Yealink	Yealink T19 E2	1
Yealink T21 E2	Yealink SIP-T21	Enable	Yealink	Yealink T21 E2	2
Yealink T23	Yealink SIP-T23	Enable	Yealink	Yealink T23	3

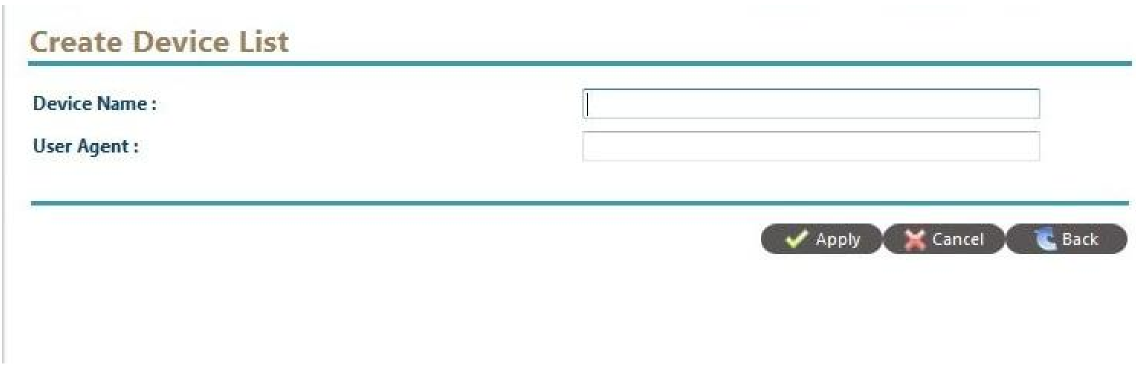
Click Import Supported Provisioning Devices if you don't see any provisioned device was here. You can view the supported provisioning device as follows by click an item and modify. The following will appear:

Modify Device List

Device Name :	LP380
User Agent :	CM5K-PHONE
Auto Provisioning :	Enable
Brand Name :	Welltech
Model Name :	LP-380
Number of Lines :	3
Model Template :	LP380.mod Download
Device Template :	LP380.mac Download
Model Configuration File :	firmware/PHONE_ver.dat
Device Configuration File Format :	$_CAP_MAC_$.dat
Customized Command :	enc_welltech_380.sh
Applied Firmware :	ip380_1512090.ssh Upload Download Clear

Click Rebuild Configuration will rebuild all device configuration files for this device model. If you have many devices, it might take long time.

For dedicate device, select New, Modify, Delete to change the Device List setting. The following web page will appear:



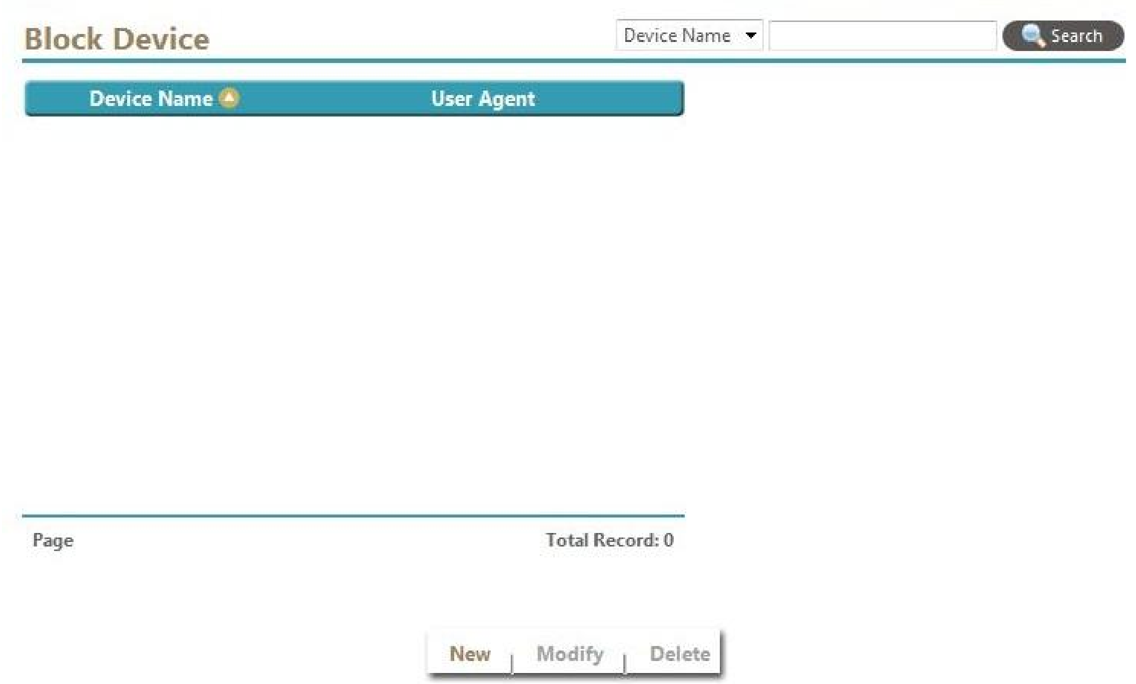
The detail of each parameter is described as below:

Parameter Name	Description
Device Name	The name to be selected in the dedicate device of extension.
User Agent	The SIP "User Agent" header used to be filtered for dedicate device.
Auto Provisioning	Whether enable auto provisioning feature for this device or not. (1.4 or above only)
Brand Name	The brand name of this device
Model Name	The model name of this device
Number of Lines	Number of lines supported for this device. The default is 1.
Model Template	The model template will be used for this device
Device Template	The device template will be used for this device
Model Configuration File	The model configuration file for this device if it is supported.
Device Configuration File Format	The file naming format for this device
Customized Command	Special command required to generate configuration file for this device
Conf Check Interval (mins)	The interval for the device to refresh or get the new configuration.
Latest Model Firmware	Newest firmware will be used for this device

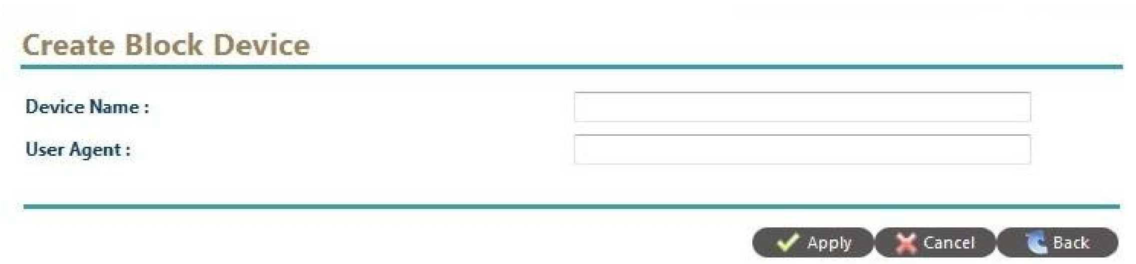
2.4.8 Block Device

Block Device is used to filter the incoming request. If the incoming SIP request's "SIP User Agent" header match the defined block device by using prefix matching, the incoming SIP request will be ignored silently.

Click ***FEATURE -> Block Device*** to view the current settings. The following web page will appear.



Select New, Modify, Delete to change the Block Device setting. The following web page will appear:

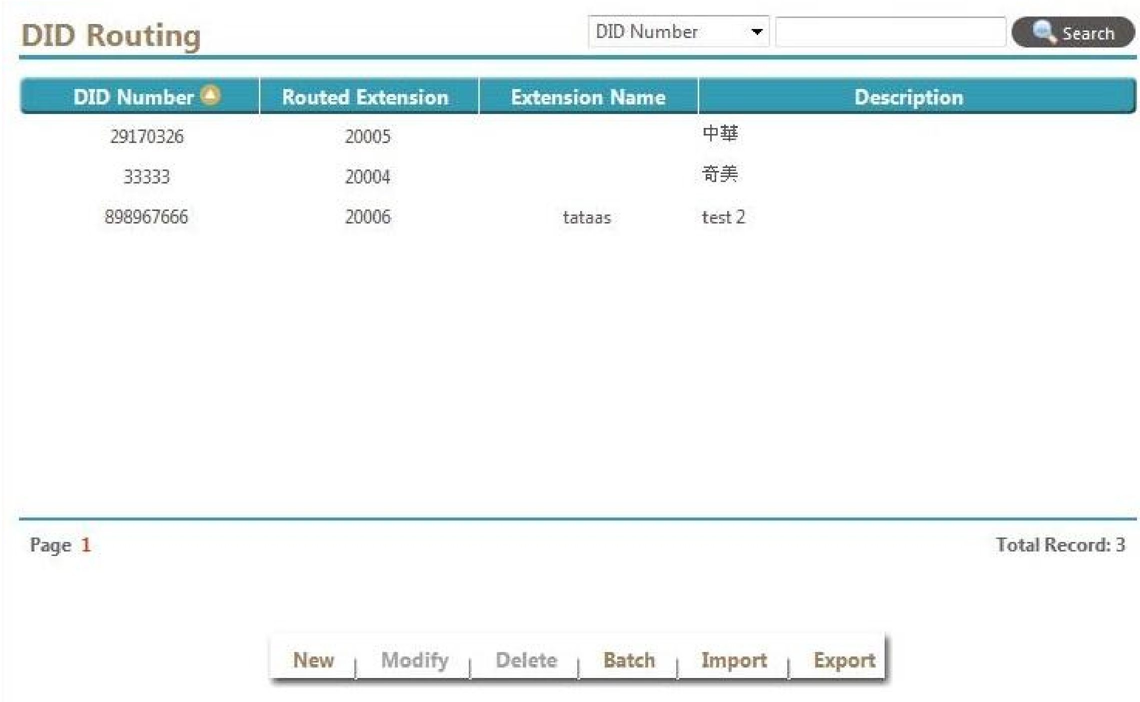


The detail of each parameter is described as below:

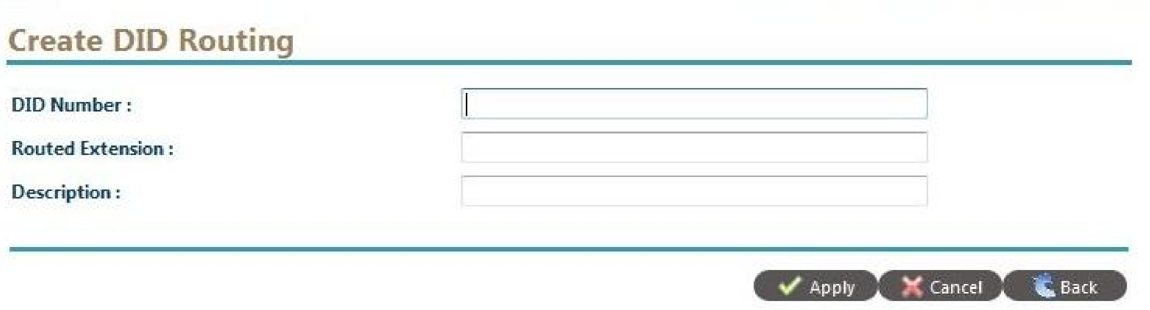
Parameter Name	Description
Device Name	The name to be blocked by the system. The request from this type of agent will be ignored.
User Agent	The SIP "User Agent" header used to be filtered for blocking.

2.4.9 DID Routing

This service is used to have a central management for your DID number routing. You can use to route your DID number to any extension, gateway or proxy. When system receive the call, it will check this DID number first to decide where to send the call out. Click ***FEATURE -> DID Routing*** to view the current settings.



Select New, Modify, Delete to change the DID Routing. The following web page will appear:



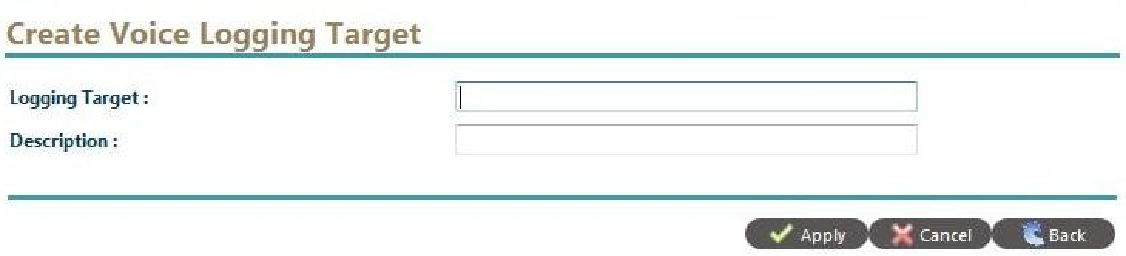
The detail of each parameter is described as below:

Parameter Name	Description
DID Number	DID number to be routed
Routed Extension	When system receive this DID number, which extension is going to be routed. If the routed extension type is phone/ ATA, the called will be replaced to the extension tel number in order to reach the phone or ATA. Or the original called number (DID) will be used for call.
Description	The description for this DID number

2.4.10 Voice Logging Target

The voice logging service requires additional license to run. Please contact "Jing Jie" for detail. You can define an extension to do the recording or record by using a calling or called number. Here is the place to define which telephone number will be recorded. Click ***FEATURE -> Voice Logging Target*** to view the current settings.

Select New, Modify, Delete to change the Voice Logging Target. The following web page will appear:



The detail of each parameter is described as below:

Parameter Name	Description
Logging Target	The target to be recorded. If caller number or called number matched the logging target, this call will be recorded.
Description	The description for this logging target.

2.4.11 Queue Prompt

The system support call queue feature. The max call queue can be supported is 1000, starting from 000 to 999. You need config call queuing feature in Routing Plan to enable call queuing feature. Here is the place to put the required queue prompts. There are 2 prompts for each call queue. The "Play Once Prompt" will be play once at first and play the "Continue Play Prompt" till the call is connected or disconnected. Click FEATURE-> Queue Prompt and the following screen will appear.

The file format is showed as follows:
- 8K Sample Rate
- 16 bits
- Linear PCM (signed)
- Mono
- Wav format

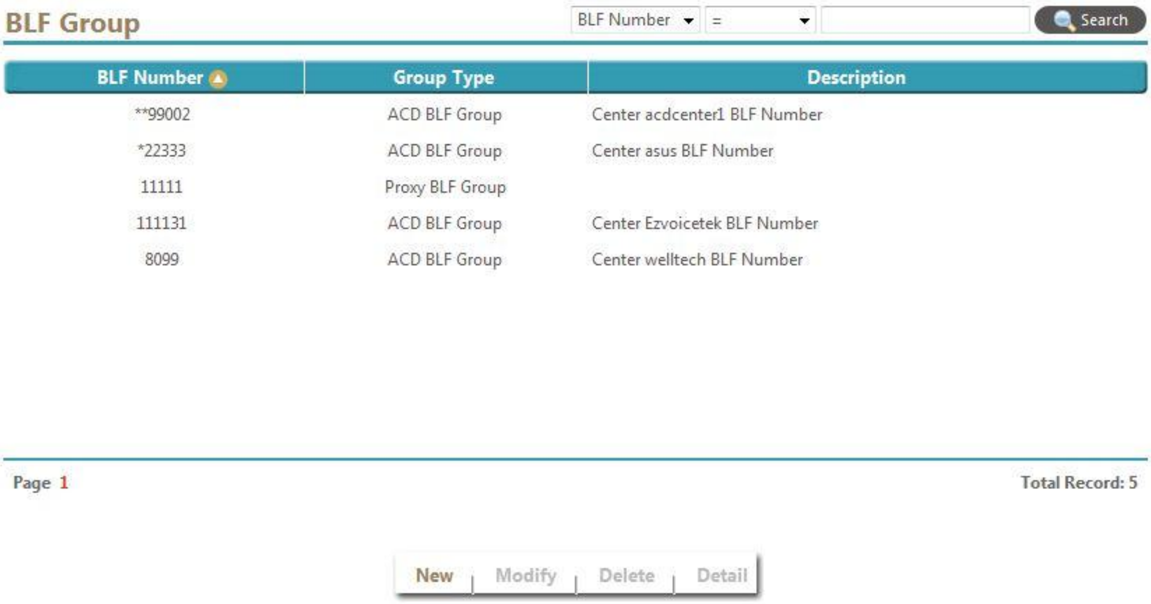
Click New to add a new queuing prompt and the following screen will appear.

The detail of each parameter is described as below:

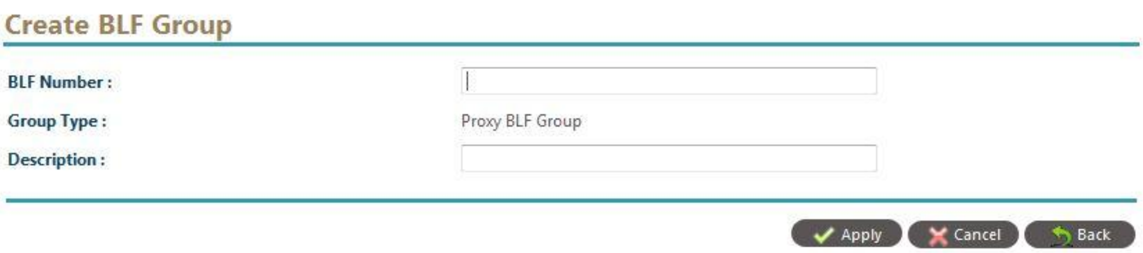
Parameter Name	Description
Prompt ID	There are 2 prompts will be played for each queue. The first prompt is xxx_0.wav which will be played once and repeat play the xxx_1.wav after it. xxx is the queuing music ID.
Play Once Prompt	This file will be play continues after play once prompt.
Continue Play Prompt	This file will be play once when first get into the queue.

2.4.12 BLF Group

The BLF group is used for ACD to get the extension status or some attendant console will use it for getting extension status. Each group contains multiple extension and once a device subscribe this BLF representative number, all extensions' status will be notified to the device. Click FEATURE -> BLF Group to view the current settings as follows:



Select New to add a new BLF group as follows:

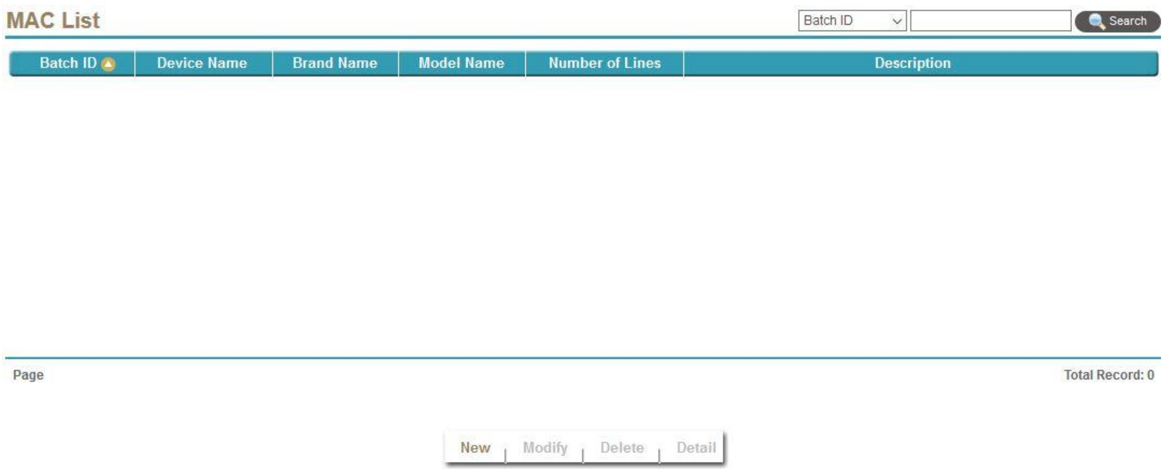


The detail of each parameter is described as below:

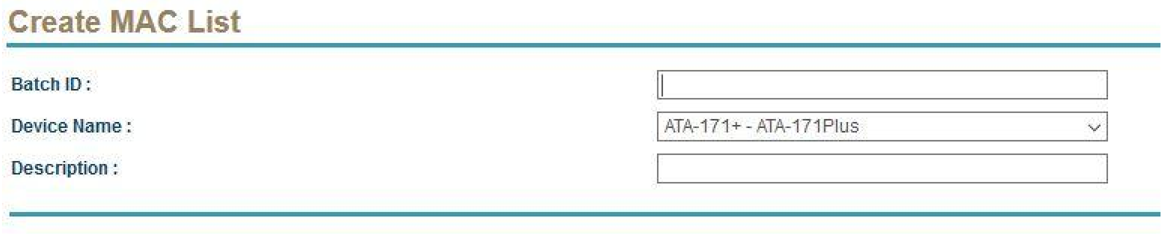
Parameter Name	Description
BLF Number	BLF group representative number
Group Type	Only Proxy BLF group can be created here. ACD BLF group need to be created in ACD module.
Description	The description for this BLF group

2.4.13 MAC List

Mac list is use for batch processing the devices. Administrator can get MAC list from supplier or input manually. The MAC List is based on batch concept, each batch contains one device model type. For different model, please create separate batch for it. Click FEATURE -> MAC List and the following will appear:



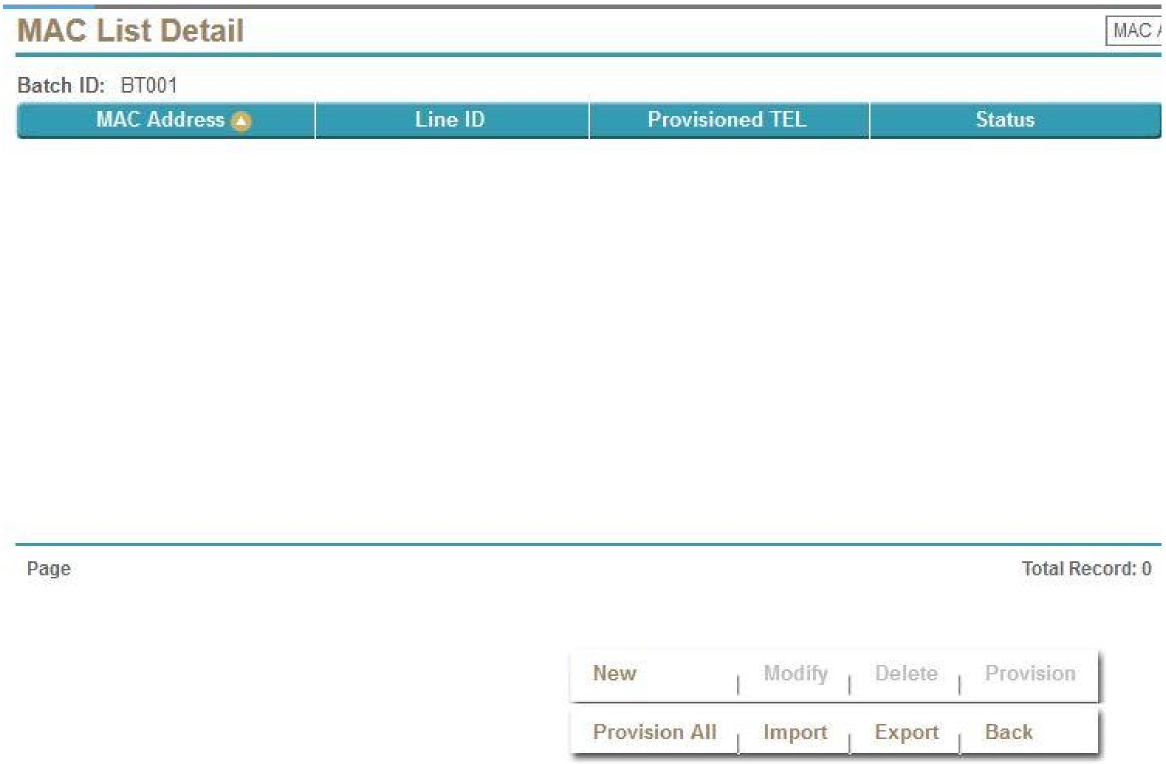
Select New, Modify, Delete to change the MAC List setting. The following web page will appear:



The detail of each parameter is described as below:

Parameter Name	Description
Batch ID	The ID for this batch
Device Name	The device model will be applied for this provisioning batch
Description	The description for this batch

Click Detail to view and edit the detail of this batch provisioning list and the following will appear:



It will be easier to export to Excel, edit and Import to system. Click Provision All to provision all MAC list in this batch. Otherwise, you can select a line and click

Provision to provision it.

2.5 Report

The system provides system statistic and status reports for management purpose.

2.5.1 Call Statistic Report

Daily call statistic report provides the administrator to understand the call attempts, connected call and access success ration for each hour. Click ***REPORT -> Call Statistic*** and select the day to view the daily report as follows.

The detail of each report field is described as follows:

Field Name	Description
Extension	The extension number currently registered
Period	The time period for this statistic
Total CA	Total number of calls attempts during this period
Total Call	Total number of connected calls during this period
Peak CA	The peak number of call attempts during this period
Peak Call	The peak number of connected calls during this period

Field Name	Description
Access Success Ratio	The average ASR (access success ratio) for this period

2.5.2 Extension Statistic Report

The extension statistic report provides the current register user per hour. The administrator can use this report to know whether all user are registered or not. Click ***REPORT -> Extension Statistic*** to view the report as follows.

The detail of each report field is described as follows:

Field Name	Description
Period	The time period for this statistic
User	The number of user registered by end of this period
Peak User	The peak number of user registered during this period

2.5.3 Extension Status Detail Report

When you enable the "Monitor Register Status" service from extension call feature, the system will record down the extension status for the following state:

- register to system
- register time out
- send call without response
- response back

Click ***REPORT -> Extension*** Status Detail to view the report as follows:

Extension Status Detail Report

Year: 2013 Month: 11 Day: 12 Extension : Query Print Export Delete

Time	Extension	User Name	State	Private IP	Private Port	Public IP	Public Port
13:28:36	601	601	Registered	100.86.63.158	8080	27.241.166.83	47116
13:18:33	601	601	Unregistered	100.86.63.158	8080	27.241.166.83	46681
12:48:37	601	601	Registered	100.86.63.158	8080	27.241.166.83	46681
12:38:33	601	601	Unregistered	100.86.63.158	8080	27.241.166.83	46455
11:49:11	601	601	Registered	100.86.63.158	8080	27.241.166.83	46455
11:49:10	601	601	Unregistered	100.86.63.158	8080	27.241.166.83	46315
11:19:13	601	601	Registered	100.86.63.158	8080	27.241.166.83	46315
11:09:11	601	601	Unregistered	100.86.63.158	8080	27.241.166.83	45725
10:39:12	601	601	Registered	100.86.63.158	8080	27.241.166.83	45725
10:39:11	601	601	Unregistered	100.86.63.158	8080	27.241.166.83	41217
10:29:11	601	601	Registered	100.86.63.158	8080	27.241.166.83	41217
10:29:11	601	601	Unregistered	100.86.63.158	8080	27.241.166.83	41217
09:49:11	601	601	Registered	100.86.63.158	8080	27.241.166.83	41217

The detail of each report field is described as follows:

Field Name	Description
Time	The time for the event
Extension	The extension number for the event
User Name	The SIP user name for the event
State	The extension status changed which could be registered or unregistered
Private IP	The private IP address from SIP contact address
Private Port	The private port from SIP contact address
Public IP	The public IP address received from
Public Port	The public port received from

2.5.4 NAT Resource Statistic Report

This report provides the utilization of NAT resource. The administrator can verify how many NAT resource are used. Click ***REPORT -> NAT Resource Statistic*** to view the report as follows:

NAT Resource Statistic Report

Year: 2011 Month: 3 Day: 24 Query Print Export Delete

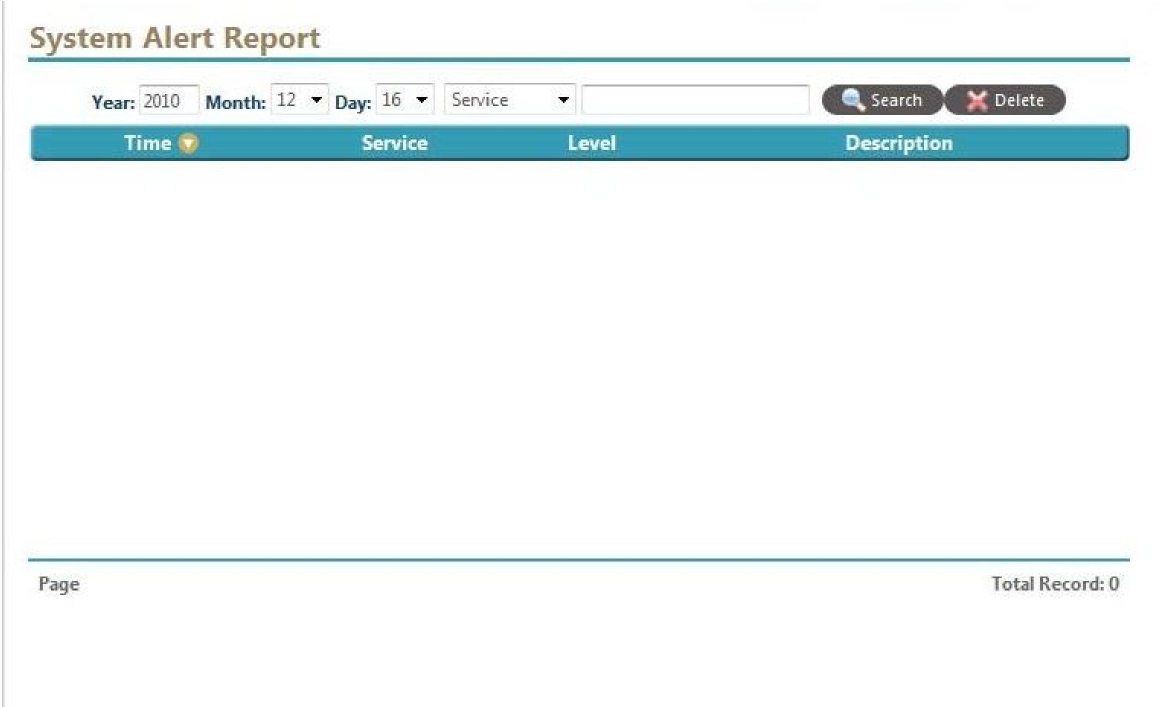
Period	NAT Resource	Peak NAT Req	NAT Utilization (%)	NAT Serviced	NAT Req Failure	NAT Failure Rate (%)
00-01	1000	0	0.00%	0	0	0.00%
01-02	1000	0	0.00%	0	0	0.00%
02-03	1000	0	0.00%	0	0	0.00%
03-04	1000	0	0.00%	0	0	0.00%
04-05	1000	0	0.00%	0	0	0.00%
05-06	1000	0	0.00%	0	0	0.00%
06-07	1000	0	0.00%	0	0	0.00%
07-08	1000	0	0.00%	0	0	0.00%
08-09	1000	0	0.00%	0	0	0.00%
09-10	1000	0	0.00%	0	0	0.00%
10-11	1000	0	0.00%	0	0	0.00%
11-12	1000	0	0.00%	0	0	0.00%
12-13	1000	0	0.00%	0	0	0.00%
13-14	1000	0	0.00%	0	0	0.00%
14-15	1000	0	0.00%	0	0	0.00%
15-16	1000	0	0.00%	0	0	0.00%
16-17	1000	1	0.10%	13	0	0.00%

The detail of each report field is described as follows:

Field Name	Description
Period	The time period for this statistic
NAT Resource	The licensed NAT resource
Peak NAT Req	The peak number of NAT resource request during this period
NAT Utilization (%)	The utilization for NAT resource
NAT Serviced	The NAT request serviced during this period
NAT Req Failure	The count of failed NAT request during this period
NAT Failure Rate (%)	The NAT request failure rate for this period

2.5.5 System Alert Report

This report provides system alert notice report. The administrator can use it to understand when and which service had problem. Click ***REPORT -> System Alert*** to view the report.

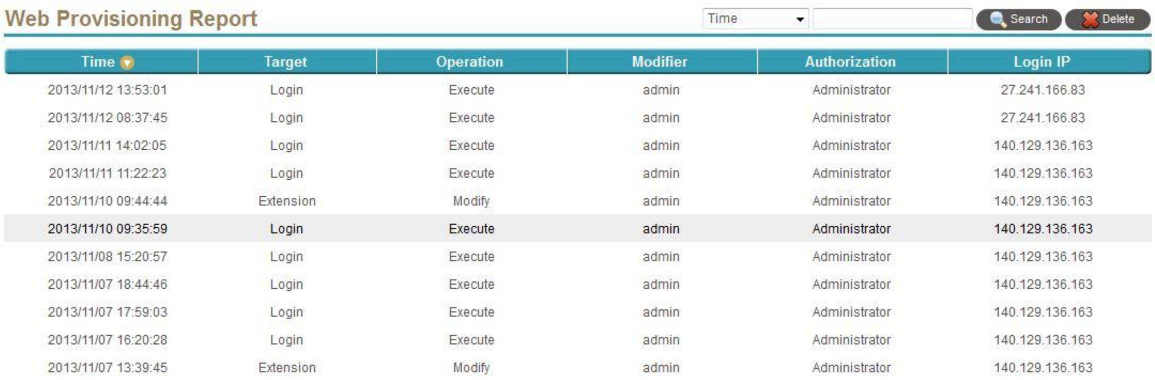


The detail of each report field is described as follows:

Field Name	Description
Time	The system alert notice event time
Service	The service which generated the event
Level	The level of this event
Description	The system alert notice content

2.5.6 Web Provisioning Report

The system will record down all the access to the system from web. The administrator can use it to audit the system and tracking the changes. Click ***REPORT -> Web Provisioning*** to view the report as follows:


Web Provisioning Report

Time | Search | Delete

Time	Target	Operation	Modifier	Authorization	Login IP
2013/11/12 13:53:01	Login	Execute	admin	Administrator	27.241.166.83
2013/11/12 08:37:45	Login	Execute	admin	Administrator	27.241.166.83
2013/11/11 14:02:05	Login	Execute	admin	Administrator	140.129.136.163
2013/11/11 11:22:23	Login	Execute	admin	Administrator	140.129.136.163
2013/11/10 09:44:44	Extension	Modify	admin	Administrator	140.129.136.163
2013/11/10 09:35:59	Login	Execute	admin	Administrator	140.129.136.163
2013/11/08 15:20:57	Login	Execute	admin	Administrator	140.129.136.163
2013/11/07 18:44:46	Login	Execute	admin	Administrator	140.129.136.163
2013/11/07 17:59:03	Login	Execute	admin	Administrator	140.129.136.163
2013/11/07 16:20:28	Login	Execute	admin	Administrator	140.129.136.163
2013/11/07 13:39:45	Extension	Modify	admin	Administrator	140.129.136.163

The detail of each report field is described as follows:

Field Name	Description
Time	The time to access web
Target	The web target to be accessed
Operation	The operation madden by user
Modifier	The user who made the change
Authorization	The authorization right of this account
Login IP	The login IP address

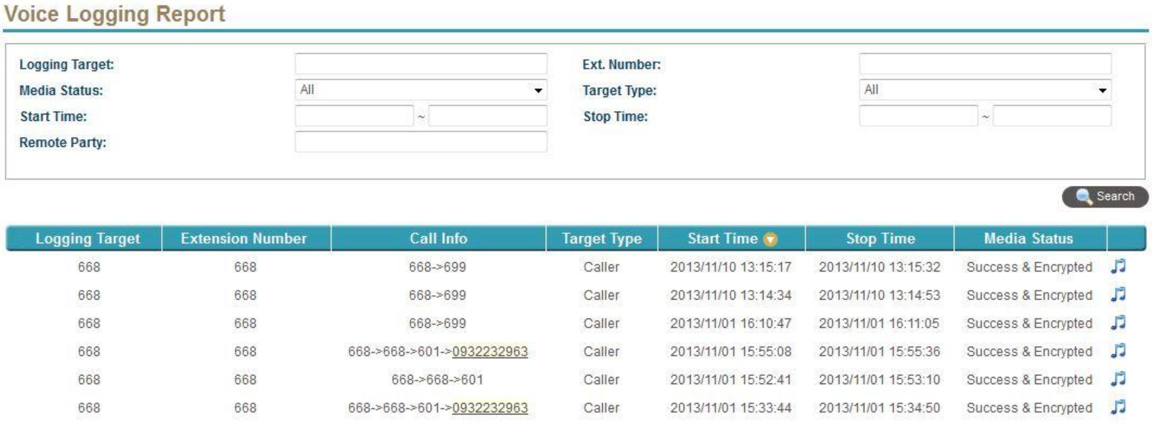
Select one of record and click the Detail button. The following detail for such record will appear.


Web Provisioning Detail Report

Time :	2013/11/10 09:35:59
Target :	Login
Operation :	Execute
Modifier :	admin
Authorization :	Administrator
Login IP :	140.129.136.163
Update Value :	

2.5.7 Voice Logging Report

The voice logging service requires additional license to run. Please contact "Jing Jie" for detail. If a target was recorded, you can query and listen the recorded prompt here. Click ***REPORT -> Voice Logging*** to view the report as follows:

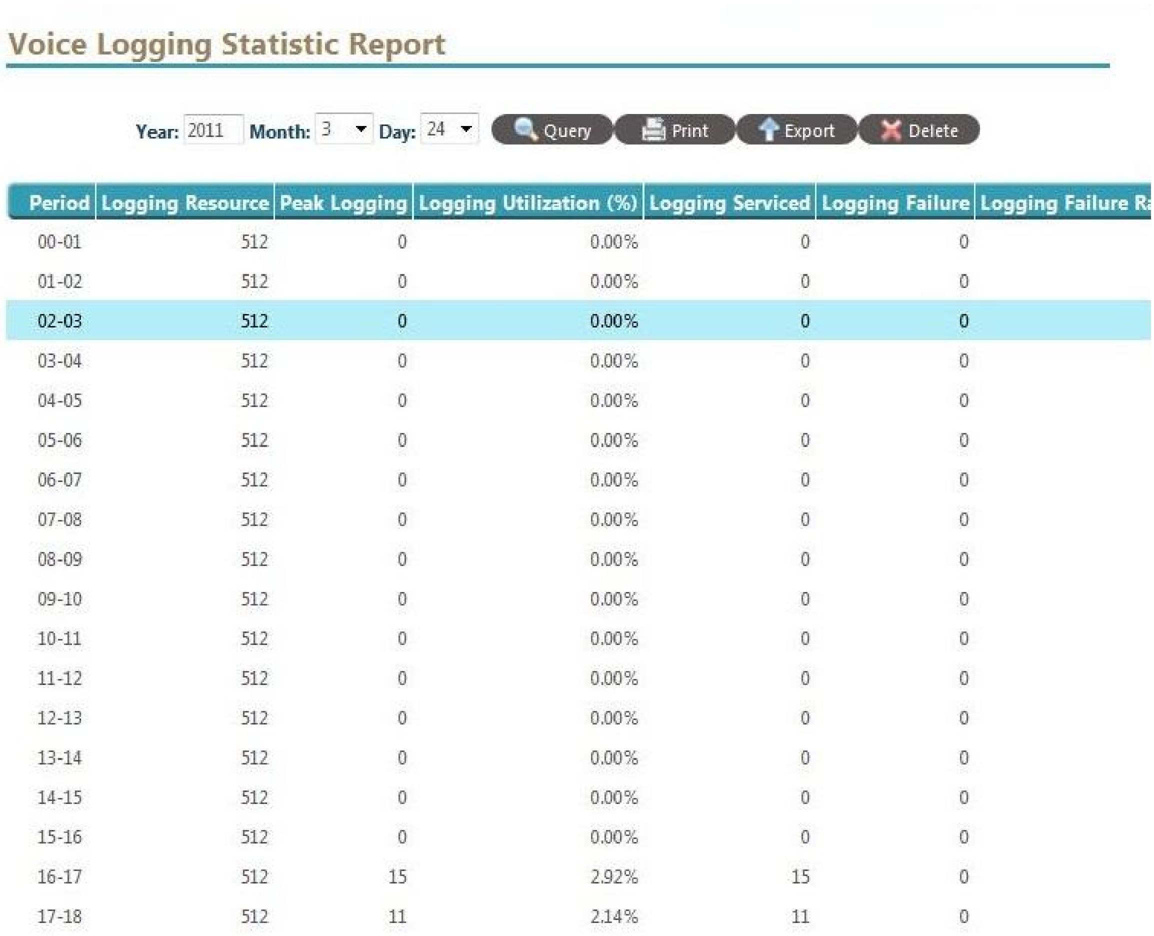


Click ***Detail***, can see the detail information for this logged call. Click ***Play*** can play the logged voice file (MP3 format).

Field Name	Description
Logging Target	The voice logging target
Extension Number	The voice logging recorded extension number. It could be a gateway or SIP phone etc.
Media Status	The recorded and encryption status for this call
Target Type	The type (caller, called or forwarder) for the recorded target
Start Time	The start time of this call
Stop Time	The stop time of this call
Call Info	The detail of this call including forwarding history.
SIP Call-ID	SIP Caller ID for reference
Caller Media Info	The caller party's RTP source IP and port
Called Media Info	The called party's RTP source IP and port
Multi Target	Whether this recording file contains multiple recording target or not?

2.5.8 Voice Logging Statistic

This report provides the utilization of Voice Logging resource. The administrator can verify how many Voice Logging resource are used. Click ***REPORT -> Voice Logging Statistic*** to view the report as follows:



Period	Logging Resource	Peak Logging	Logging Utilization (%)	Logging Serviced	Logging Failure	Logging Failure R
00-01	512	0	0.00%	0	0	
01-02	512	0	0.00%	0	0	
02-03	512	0	0.00%	0	0	
03-04	512	0	0.00%	0	0	
04-05	512	0	0.00%	0	0	
05-06	512	0	0.00%	0	0	
06-07	512	0	0.00%	0	0	
07-08	512	0	0.00%	0	0	
08-09	512	0	0.00%	0	0	
09-10	512	0	0.00%	0	0	
10-11	512	0	0.00%	0	0	
11-12	512	0	0.00%	0	0	
12-13	512	0	0.00%	0	0	
13-14	512	0	0.00%	0	0	
14-15	512	0	0.00%	0	0	
15-16	512	0	0.00%	0	0	
16-17	512	15	2.92%	15	0	
17-18	512	11	2.14%	11	0	

Field Name	Description
Period	The time period for this statistic
Logging Resource	The licensed logging resource
Peak Logging	The peak number of logging resource request during this period
Logging Utilization (%)	The utilization for logging resource

Field Name	Description
Logging Serviced	The logging request serviced during this period
Logging Failure	The count of failed logging request during this period
Logging Failure Rate (%)	The logging request failure rate for this period

2.5.9 AA/VMS Statistic

Daily AA/VMS statistic report provides the administrator to understand the AA/VMS and conference resource usage for each hour. Click ***REPORT -> AA/VMS Statistic*** and select the day to view the daily report as follows.


AA/VMS Statistic Report

Year: 2013 Month: 11 Day: 12 Office ID : All Query Print Export Delete

Period	Total AA/VMS Resource	Peak AA/VMS Resource	Total Conference Resource	Peak Conference Resource	Auto Attendant	Peak Auto Attendant
00-01	0	0	0	0	0	0
01-02	0	0	0	0	0	0
02-03	0	0	0	0	0	0
03-04	0	0	0	0	0	0
04-05	0	0	0	0	0	0
05-06	0	0	0	0	0	0
06-07	0	0	0	0	0	0
07-08	0	0	0	0	0	0
08-09	0	0	0	0	0	0
09-10	0	0	0	0	0	0
10-11	0	0	0	0	0	0
11-12	0	0	0	0	0	0
12-13	0	0	0	0	0	0
13-14	0	0	0	0	0	0
14-15	0	0	0	0	0	0

Previous Day | Next Day

The detail of each report field is described as follows:

Field Name	Description
Period	The time period for this statistic
Total AA/VMS Resource	Total service count for AA/VMS service
Peak AA/VMS Resource	Peak service count for AA/VMS service

Field Name	Description
Total Conference Resource	Total service count for conference service
Peak Conference Resource	Peak service count for conference service
Auto Attendant	Service count of auto attendant
Peak Auto Attendant	Peak service count for auto attendant
Total Auto Attendant	The total service count for auto attendant within this period
VMS	Voice Mail service count
Peak VMS	Peak service count for VMS service
Total VMS	The total service count for voice mail within this period
VMS From Ext.	The service count for VMS from extension service.
Peak VMS From Ext.	The peak service count for VMS from extension service.
Total VMS From Ext.	The total service count for VMS from extension within this period.
Music on Hold	Service count for Music on Hold service.
Peak Music On Hold	The peak service count for Music on Hold service.
Total Music On Hold	The total service count for music on hold service within this period.
Meeting Me Conference	The service count for meet me conference service.
Peak Meet Me Conference	The peak service count for meet me conference service.
Total Meet Me Conference	The total service count for meet me conference within this period.
Call Park	The service count for call park service
Peak Call Park	The peak service count for call park service
Total Call Park	The total service count for call park service within this period.
Adhoc Conference	The service count for adhoc conference service.

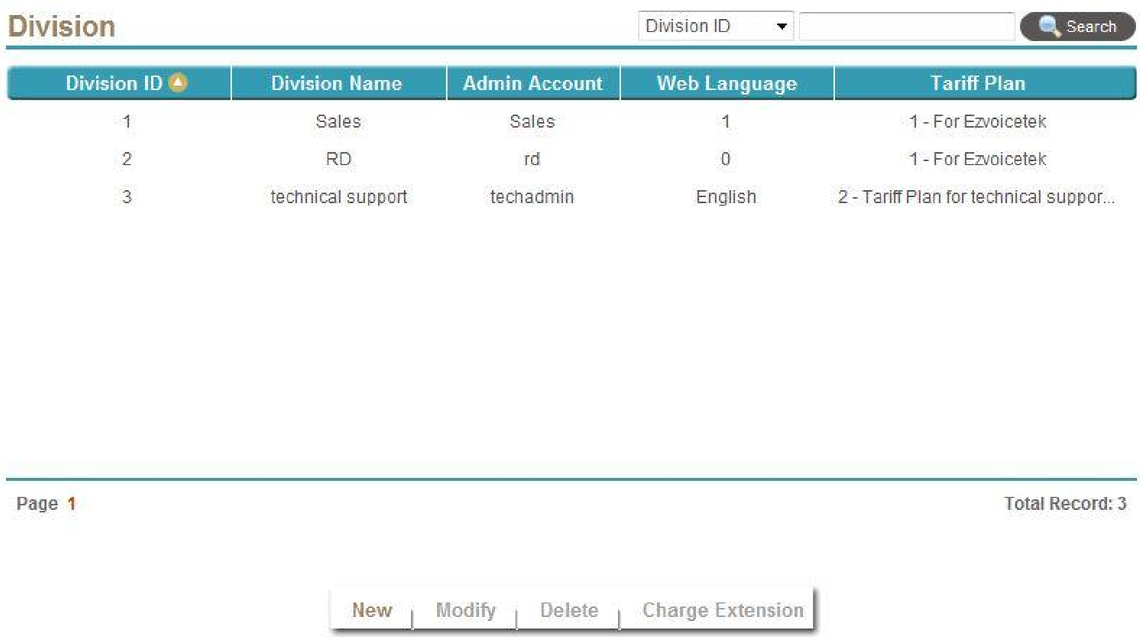
Field Name	Description
Peak Adhoc Conference	The peak service count for adhoc conference service.
Total Adhoc Conference	The total service count for adhoc conference service within this period.
Voice Message	The service count for extension to extension voice mail or direct to voice mail service.
Peak Voice Message	The peak service count for extension to extension voice mail or direct to voice mail service.
Total Voice Message	The total service count for extension to extension voice mail or direct to voice mail service.

2.6 Billing

The system has built-in billing to enterprise charge purpose. First, you need to create a division and assign extension to it. Then you can you have enterprise, division and extension level of billing report.

2.6.1 Division

Division is the managing and charging unit for enterprise. To have correct charge for each division, you need assign extensions to it. Click ***BILLING -> Division*** to view and change the division settings as follows:

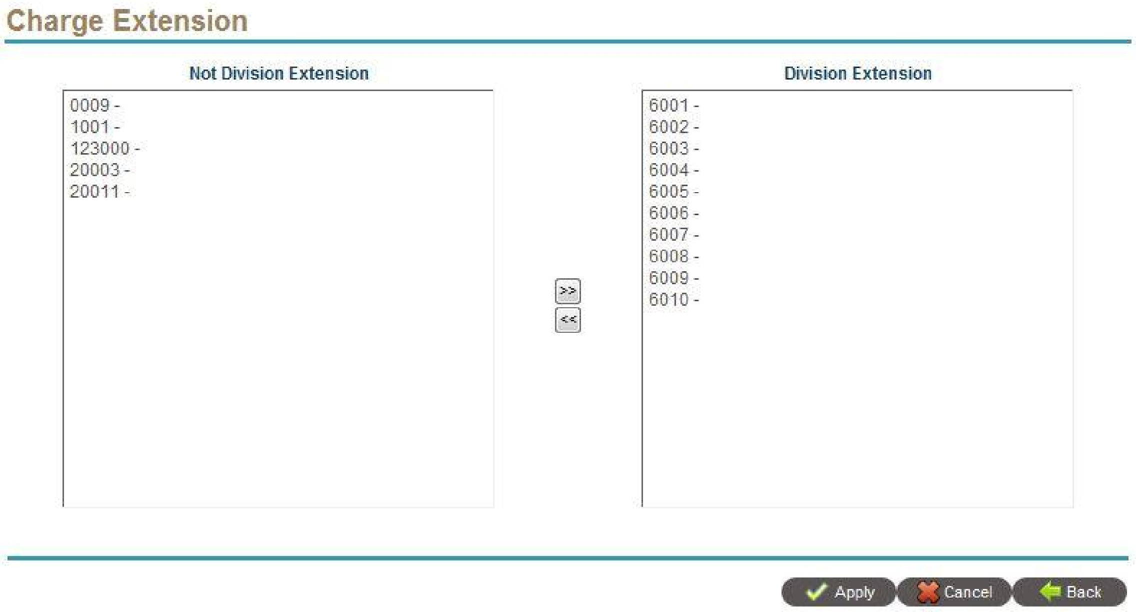


Select New, Modify, Delete to change the division. The following web page will appear:

The detail of each parameter is described as below:

Parameter Name	Description
Division ID	The charge division ID.
Division Name	The name of the division
Admin Account	The administration account for this division.
Admin Password	The password for the division administration account.
Web Language	Web language when login.
Tariff Plan	The tariff plan for billing purpose.

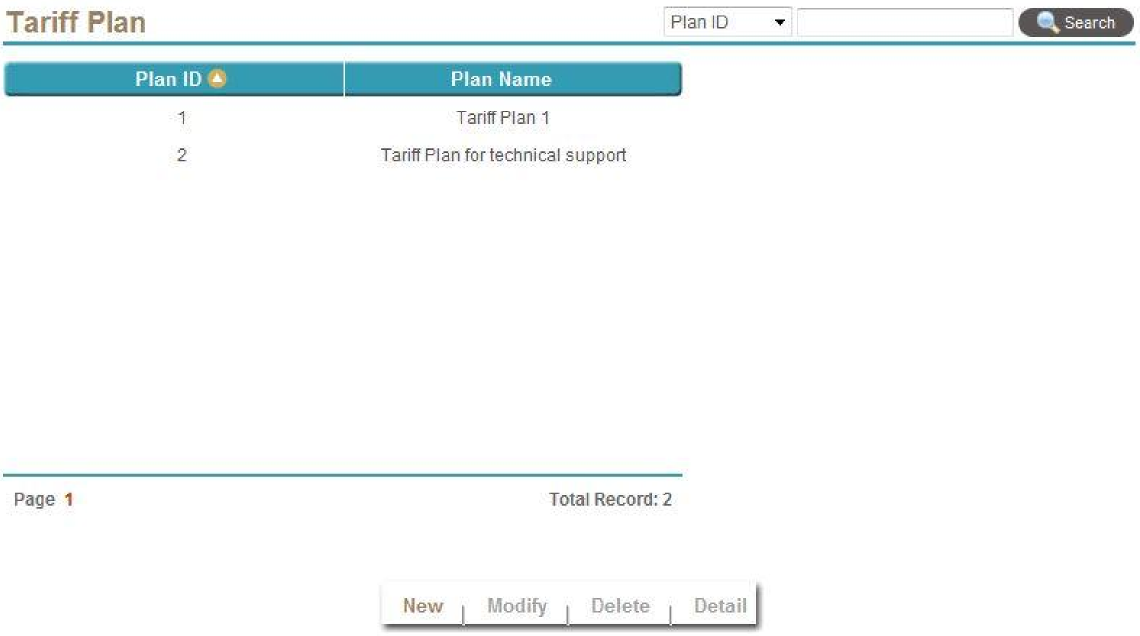
To assign the extension to a division, click ***Charge Extension*** and the following will displayed.



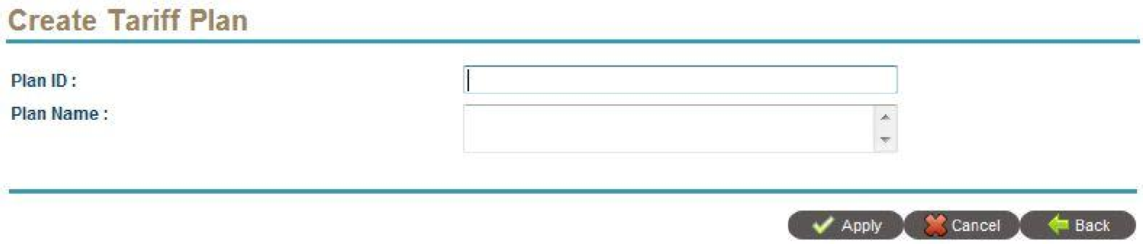
You can select extension from left window (no charged extension) and click >> to be assigned to this charge division.

2.6.2 Tariff Plan

The tariff plan is used to calculate the charge amount based on the charge unit. It is recommended to assign a default rate for those undefined prefix. Click ***BILLING -> Tariff Plan*** to view and change the tariff plan as follows:



Select New, Modify, Delete to change the Tariff Plan. The following web page will appear:

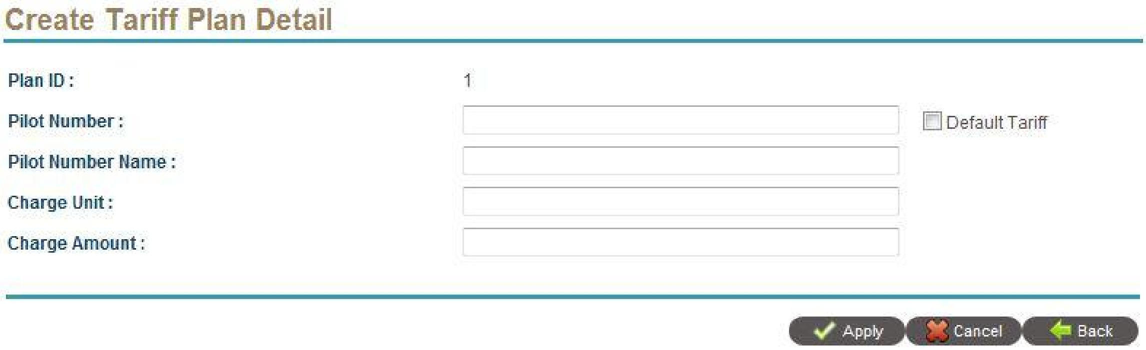


The detail of each parameter is described as below:

Parameter Name	Description
Plan ID	The tariff plan ID
Plan Name	The tariff plan name

Click ***Detail*** to view and modify the tariff rate plan. The following screen will appear.

Select New, Modify, Delete to add the Tariff Detail. The following web page will appear:

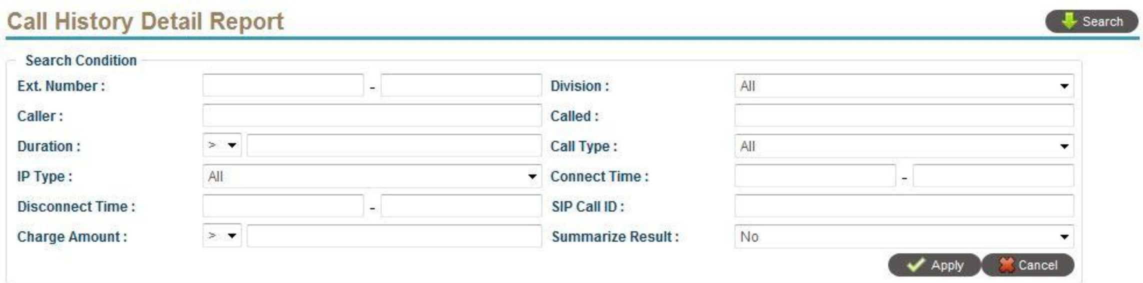


The detail of each parameter is described as below:

Parameter Name	Description
Plan ID	The tariff plan ID
Pilot Number	The prefix to be matched the called number. Check default tariff to set a default rate for this plan.
The prefix name	The name of this prefix
Charge Unit	The charge unit in seconds.
Charge Amount	The charge amount based on this unit.

2.6.3 Call History Detail Report

Call History Detail Report is used to show call list based on search condition. Click ***BILLING -> Call History Detail Report*** to list the filtered calls. The search condition will appear as follows:



You can select the search condition as above and click search to start the query. The filtered Call History Detail Report will appear as follows:

Call History Detail Report

Search Delete

Ext. Number	Division	Caller	Called	Duration	Amount	Call Type	IP Type	Connect Time	Disconnect Time	Cause	Sour
6009	3 - technical support	6009	6006	7	2.000	Extension	V4 To V4	2011-08-04 14:46:12	2011-08-04 14:46:19	200	140.129
6009	3 - technical support	6009	*56	6	18.000	Extension	V4 To V4	2011-08-03 11:24:59	2011-08-03 11:25:05	200	140.129
6006	3 - technical support	6006	26629090	4	1.800	Extension	V4 To V4	2011-08-03 10:39:57	2011-08-03 10:40:01	200	140.129
6006	3 - technical support	6006	26629090	13	4.500	Extension	V4 To V4	2011-08-03 09:52:20	2011-08-03 09:52:33	200	140.129
6006	3 - technical support	6006	26629090	21	6.300	Extension	V4 To V4	2011-08-03 09:51:50	2011-08-03 09:52:11	200	140.129
6006	3 - technical support	6006	26629090	3	0.900	Extension	V4 To V4	2011-08-03 09:18:21	2011-08-03 09:18:24	200	140.129
6006	3 - technical support	6006	26629090	2	0.900	Extension	V4 To V4	2011-08-03 09:17:22	2011-08-03 09:17:24	200	140.129
20010	1 - Sales	20010	20016	95	8.440	Extension	V4 To V4	2011-08-02 15:33:02	2011-08-02 15:34:37	200	192.16
20010	1 - Sales	20010	*91	19	3.800	Extension	V4 To V4	2011-08-02 15:31:15	2011-08-02 15:31:34	200	114.32.
20010	1 - Sales	20010	20016	41	4.220	Extension	V4 To V4	2011-08-02 15:25:39	2011-08-02 15:26:20	200	192.16
20010	1 - Sales	20010	*92	371	74.200	Extension	V4 To V4	2011-08-02 15:24:57	2011-08-02 15:31:08	200	114.32.
20010	1 - Sales	20010	20016	44	4.220	Extension	V4 To V4	2011-08-02 15:08:04	2011-08-02 15:08:48	200	192.16
20010	1 - Sales	20010	*92	1,049	209.800	Extension	V4 To V4	2011-08-02 15:07:25	2011-08-02 15:24:54	200	114.32.
20010	1 - Sales	20010	20016	31	4.220	Extension	V4 To V4	2011-08-02 14:52:29	2011-08-02 14:53:00	200	192.16
20010	1 - Sales	20010	20017	69	6.040	Extension	V4 To V4	2011-08-01 20:48:27	2011-08-01 20:49:36	200	192.16

Page 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

Total Record: 1117

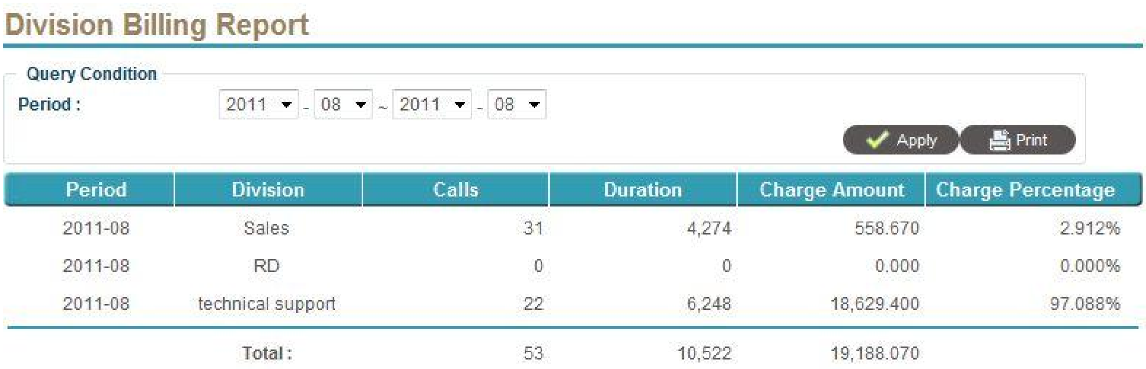
The detail of each report field is described as follows:

Field Name	Description
Ext. Number	Extension Number
Division	belonged division
Caller	calling party number
Called	called party number
Duration	call duration
Amount	charged amount
Call Type	Call type could be the following: Extension: extension to extension calls Outgoing: Extension outgoing call Incoming: Incoming call to extension Misc: Others call type
IP Type	The IP address type which could be IPV4 or IPV6
Connect Time	The call connect time
Disconnect Time	The call disconnecting time
Cause	The SIP disconnecting cause for this call.
Source IP	The IP address for the calling party

Field Name	Description
Destination IP	The IP address for the called party
SIP Call ID	SIP Call ID for this call which could be used for tracking.
Universal Call ID	Universal Call ID for tracking purpose

2.6.4 Division Billing Report

Division Billing Report shows the charge amount and percentage for each division. It could be used for enterprise easy to do the telephony charge for each division. Click ***BILLING -> Division Billing Report*** and select the queried period to see the following report.



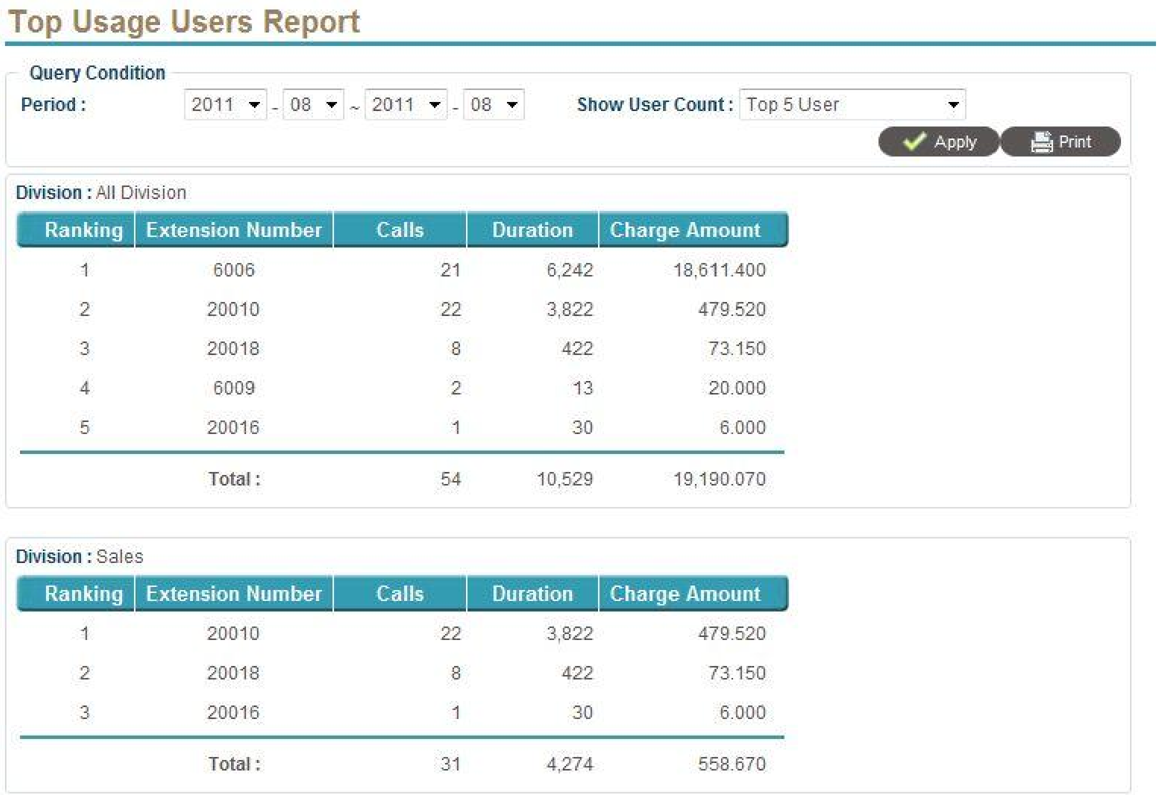
Period	Division	Calls	Duration	Charge Amount	Charge Percentage
2011-08	Sales	31	4,274	558.670	2.912%
2011-08	RD	0	0	0.000	0.000%
2011-08	technical support	22	6,248	18,629.400	97.088%
	Total :	53	10,522	19,188.070	

The detail of each report field is described as follows:

Field Name	Description
Period	Charged Month
Division	Charged division name
Calls	Total calls of this month
Duration	Total call duration of this month
Charge Amount	Total charged charged amount of this month
Charge Percentage	Charged percentage against over all charge of this month

2.6.5 Top Usage User Report

Top Usage User Report show the top usage user for whole company or division for administrator. Click ***BILLING -> Top Usage User Report*** and select the queried period to see the following report.

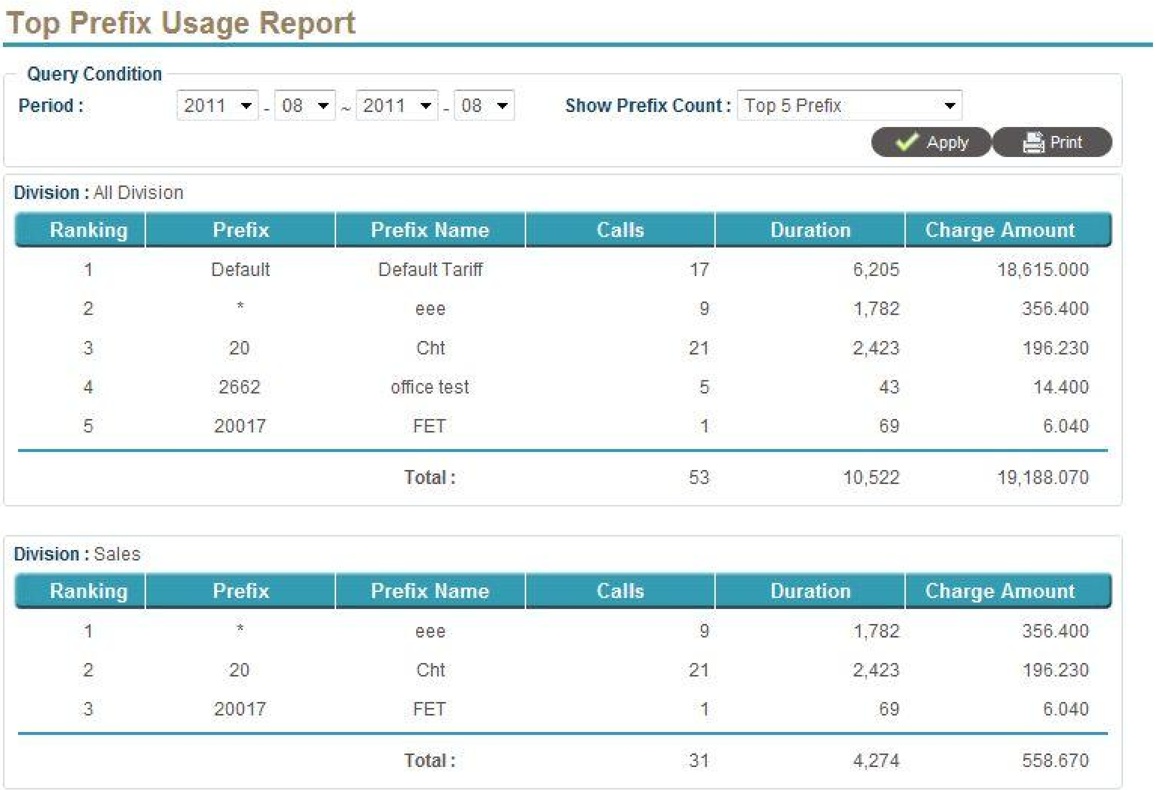


The detail of each report field is described as follows:

Field Name	Description
Ranking	The ranking of top users
Extension Number	Extension number
Calls	Total calls of this month
Duration	Total call duration of this month
Charge Amount	Total charged charged amount of this month

2.6.6 Top Prefix Usage Report

Top Prefix Usage Report show the top usage user for whole company or division for administrator. Click ***BILLING -> Top Prefix Usage Report*** and select the queried period to see the following report.



Ranking	Prefix	Prefix Name	Calls	Duration	Charge Amount
1	Default	Default Tariff	17	6,205	18,615.000
2	*	eee	9	1,782	356.400
3	20	Cht	21	2,423	196.230
4	2662	office test	5	43	14.400
5	20017	FET	1	69	6.040
		Total :	53	10,522	19,188.070

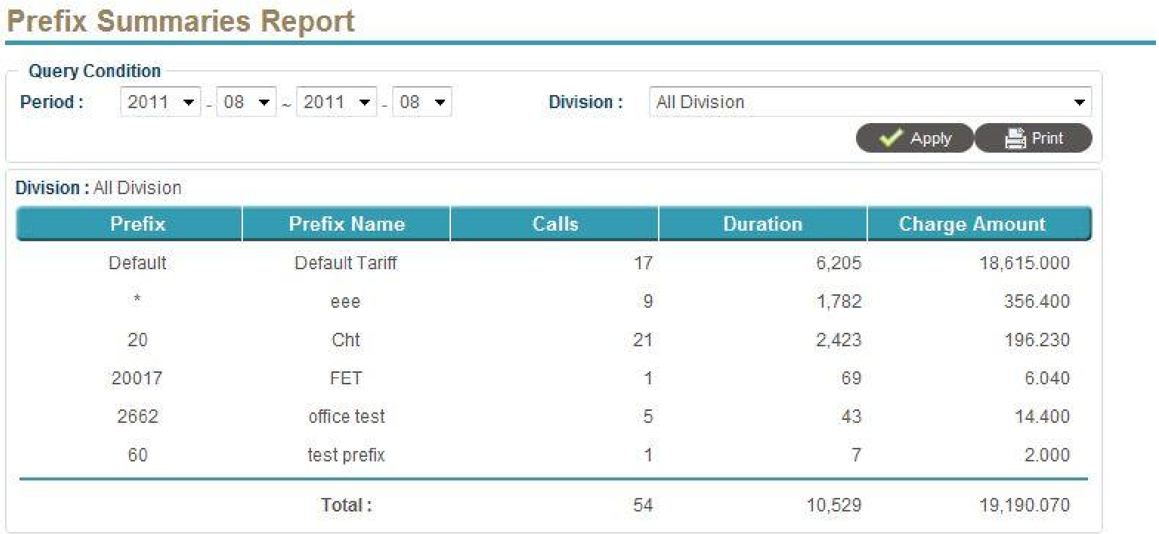
Ranking	Prefix	Prefix Name	Calls	Duration	Charge Amount
1	*	eee	9	1,782	356.400
2	20	Cht	21	2,423	196.230
3	20017	FET	1	69	6.040
		Total :	31	4,274	558.670

The detail of each report field is described as follows:

Field Name	Description
Ranking	The ranking of top users
Prefix	Prefix
Prefix Name	Prefix Name
Calls	Total calls of this month
Duration	Total call duration of this month
Charge Amount	Total charged charged amount of this month

2.6.7 Prefix Summaries Report

Prefix Summaries Report show the status of each defined prefix for selected period based on the selected divsion. Click ***BILLING -> Prefix Summaries Report*** and select the queried period to see the following report.



Prefix	Prefix Name	Calls	Duration	Charge Amount
Default	Default Tariff	17	6,205	18,615.000
*	eee	9	1,782	356.400
20	Cht	21	2,423	196.230
20017	FET	1	69	6.040
2662	office test	5	43	14.400
60	test prefix	1	7	2.000
	Total :	54	10,529	19,190.070

The detail of each report field is described as follows:

Field Name	Description
Prefix	Prefix
Prefix Name	Prefix Name
Calls	Total calls of this month
Duration	Total call duration of this month
Charge Amount	Total charged charged amount of this month

2.7 Diagnostic

The Diagnostic page provides real time monitoring for system, extension, call and system log tracking. It could be very good tools to help administrator to identify the root cause of problems.

2.7.1 System Status

The ***System Status*** provides the current status of system status. You can see whether the system is up and the resource usage. Click ***DIAGNOSTIC -> System Status*** to view the current system status. The following screen will appear.

System Status

System :	ezpbx2000	Version :	1.3.2(P131018)
WEB Version :	1.4 (P20130925)	System Startup Time :	2013/11/01 15:08:12
Current User :	14	Peak User :	14
Current Call Attempt :	0	Peak Call Attempt :	0
Current Call :	0	Peak Call :	0
Current NAT Used :	0	Peak NAT Used :	0
Total NAT Used :	0	Failed NAT Request :	0
Total Call Attempt :	0	Total Call :	0
Max Transaction :	1260	Used Transaction :	2
Max Memory Pool :	3281	Used Memory Pool :	0
Current Voice Logging :	0	Peak Voice Logging :	0
Total Voice Logging :	0	Failed Voice Logging :	0
Current Web Call :	0	Peak Web Call :	0
Total Web Call :	0		

Refresh Interval : 3 seconds

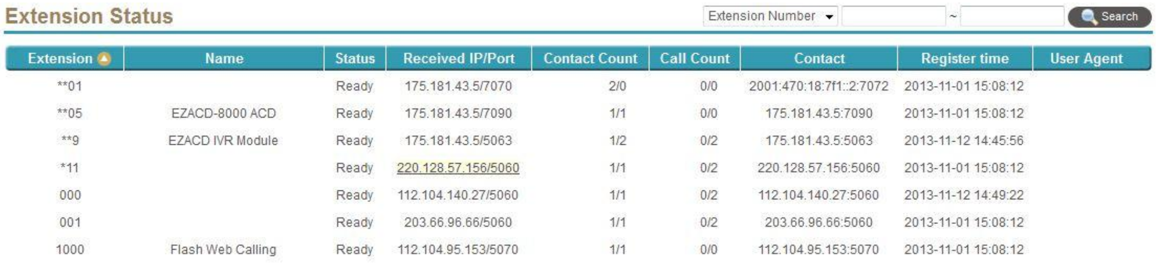
The detail of each filed is described as below:

Field Name	Description
System	The system core name
Version	The major system release
Web Version	The web service release
System Startup Time	The system started time
Current User	Current user is registered in the system
Current Call Attempt	Current call attempt to the system
Current Call	Current connected call (talking calls)
Current NAT Used	Current calls that use NAT resource which means the rap will be route to the center
Total NAT Used	Total count of NAT resource is used within this hour. It will be cleared on the sharp of each hour.

Field Name	Description
Peak User	The peak of user registered to the system within this hour
Peak Call Attempt	The peak call attempt to the system within this hour
Peak Call	The peak connected call within this hour
Peak NAT Used	The Peak NAT resource used within this hour
Failed NAT Request	The count of NAT resource request failure
Total Call Attempt	The total call attempt count for this hour
Total Call	Total count of connected call for this hour
Max Transaction	The transaction allocated for the system
Used Transaction	The current used transaction
Max Memory Pool	The memory pool allocated for the system
Used Memory Pool	The current used memory pool
Current Voice Logging	The current voice logging resource are used
Peak Voice Logging	The peak voice logging resource were used
Total Voice Logging	The total voice logging resource were used for this hour
Failed Voice Lgging	The total voice logging resource were unable to be gotten for this hour.
Current Web Call	The current web calls are used
Peak Web Call	The peak web calls are used
Total Web Call	The total web calls are used

2.7.2 Extension Status

The administrator can query the current registered extension by clicking ***DIAGNOSTIC -> Extension Status***. The following screen will appear.



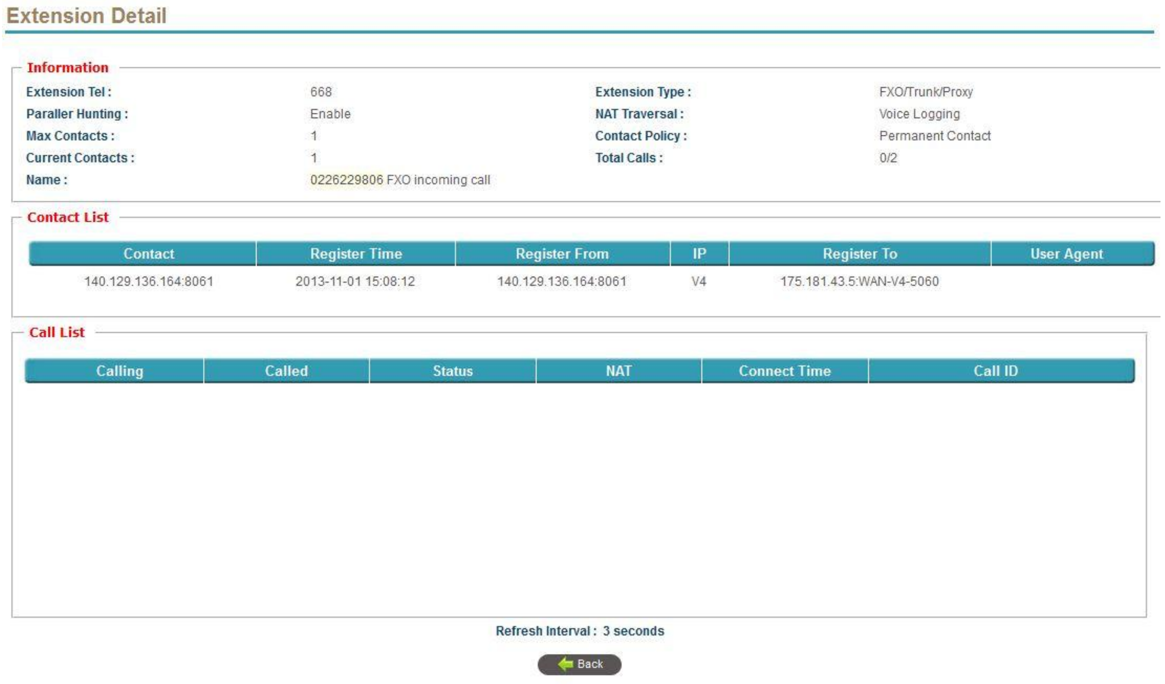
Extension	Name	Status	Received IP/Port	Contact Count	Call Count	Contact	Register time	User Agent
**01		Ready	175.181.43.5/7070	2/0	0/0	2001:470:18:7f1::2:7072	2013-11-01 15:08:12	
**05	EZACD-8000 ACD	Ready	175.181.43.5/7090	1/1	0/0	175.181.43.5:7090	2013-11-01 15:08:12	
**9	EZACD IVR Module	Ready	175.181.43.5/5063	1/2	0/2	175.181.43.5:5063	2013-11-12 14:45:56	
*11		Ready	220.128.57.156/5060	1/1	0/2	220.128.57.156:5060	2013-11-01 15:08:12	
000		Ready	112.104.140.27/5060	1/1	0/2	112.104.140.27:5060	2013-11-12 14:49:22	
001		Ready	203.66.96.66/5060	1/1	0/2	203.66.96.66:5060	2013-11-01 15:08:12	
1000	Flash Web Calling	Ready	112.104.95.153/5070	1/1	0/0	112.104.95.153:5070	2013-11-01 15:08:12	

The detail of each filed is described as below:

Field Name	Description
Extension	The extension is currently registered
Name	The name of this extension
Status	The status of extension
Received IP/Port	Public IP and port where the extension is registered from.
Contact Count	Number of contact registered and max contact allowed
Calls Count	Current call and max calls allowed (0 means no limits)
Contact	The newest registered contact
Register Time	The latest register time
User Agent	The SIP User Agent of this registered device

Click Add User Agent will add this SIP User Agent into the selected account's settings.

Double click the selected extension, you can see the detail status of it. The following screen will appear.

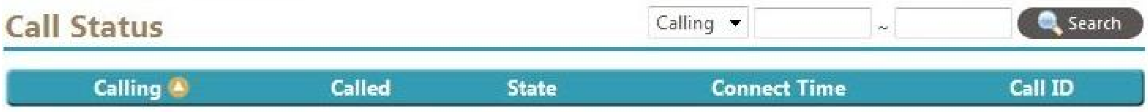


The contact list will show the current registered devices. Click it and it will allow you to unregister if need.

The call list show the current calls for this extension number. Click it and it will allow you to disconnect the call.

2.7.3 Call Status

The real time call status can be checked here. It can show all the activated calls or selected extension's call. Click ***DIAGNOSTIC -> Call Status*** to enter the call status monitor screen as follows:



The detail of each filed is described as below:

Field Name	Description
Calling	The calling party number
Called	The called party number
State	The current call state
Connect Time	The connected time for the call
Call ID	The SIP call ID

2.7.4 High Available Status

The HA status can be checked by click ***DIAGNOSTIC -> High Available Status***. If both server are working correctly, you could see that the status of each HA member is "online" as follows:

The detail of each filed is described as below:

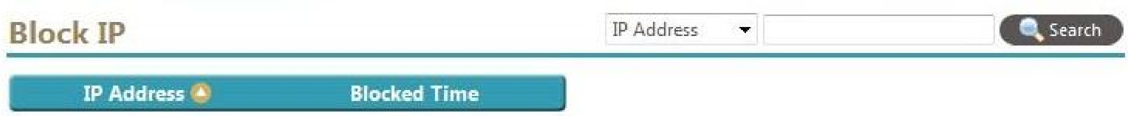
Field Name	Description
Cluster ID	Cluster ID is used to identify the cluster. Different Cluster ID will not able to working together. For different Cluster ID, it is required to use different Cluster Service Port. The maximum length of ID is 6 bytes.
Cluster Service Port	The UDP port will be used for intra-cluster communication to send and receive heartbeat message. It is required to have different Cluster Service Port for each Cluster ID. The default value is 694.
Cluster Type	The following types are supported to meet different requirements:

Field Name	Description
	Active/Active Cluster: Both servers are acting as an independent server and backup for each other. The register information will be forwarded to backup node to speed up the fail over timing. Once the active one is failed to service, it will switch over to backup node. Active/Standby Cluster: One of cluster server will become active while another one is a backup server. The register information will be forwarded to backup node to speed up the fail over timing. Once the active one is failed to service, it will switch over to backup node.
HA Member 1	The cluster member's host name which is get from uname ? □n. Please note that both server settings need the same order. This cluster member will start and service HA Group 1 by default in Active/Active mode
HA Member 2	The cluster member's host name which is get from uname ? □n. Please note that both server settings need the same order. This cluster member will start and service HA Group 2 by default in Active/Active mode.
HA Group 1 Resource Status	The status of High Available Group 1. It is required for both AA and AS modes.
IPV4 VIP for WAN	Virtual IP V4 address for WAN interface.
IPV4 VIP for LAN	Virtual IPV4 address for LAN interface.
IPV6 VIP for WAN	Virtual IP V6 address for WAN interface. The IPV6 address must be a global unicast addressed, not a link-local or site-local address. IPV6 VIP for WAN is only available when 1 Ethernet leg mode is used (Attached LAN Interface is disabled).
IPV6 VIP for LAN	Virtual IP V6 address for WAN interface. Virtual IP V6 address for WAN interface. The IPV6 address must be a global unicast addressed, not a link-local or site-local address. It could be use fc00:xxxx:xxx:xxx as the private IP V6 address. IPV6 VIP for LAN is only available when 2 Ethernet legs mode is used (Attached LAN interface is enabled).
Service Controller	It is a internal status for HA resource status controlling.
Status	Resource status and which server is servicing now.
Failcount	If there is a problem to start the resource, HA will try to restart it and add 1 for the Failcount. Normally, it will be 0.
HA Group 2	High Available Group 2. It is only required for AA mode.

Field Name	Description
IPV4 VIP for WAN	Virtual IP V4 address for WAN interface for HA Group 2.
IPV4 VIP for LAN	Virtual IP V4 address for LAN interface for HA Group 2.
IPV6 VIP for WAN	Virtual IP V6 address for WAN interface for HA Group 2. The IPV6 address must be a global unicast addressed, not a link-local or site-local address. IPV6 VIP for WAN is only available when 1 Ethernet leg mode is used (Attached LAN Interface is disabled).
IPV6 VIP for LAN	Virtual IP V6 address for WAN interface for HA Group 2. Virtual IP V6 address for WAN interface. The IPV6 address must be a global unicast addressed, not a link-local or site-local address. It could be use fc00:xxxx:xxx:xxx as the private IP V6 address. IPV6 VIP for LAN is only available when 2 Ethernet legs mode is used (Attached LAN interface is enabled).
Service Controller	It is a internal status for HA resource status controlling.

2.7.5 Blocked IP

The system will detect the SIP attack such as "friendly scanner" or other potential attack by the attacking behavior and blocked it automatically. A system alert event will be written to system alert for auditing purpose. After the defined "Attack Block Time" in Service Parameter is reached, the blocked IP will be released. The administrator can query the current blocked IP address by clicking ***DIAGNOSTIC -> Blocked IP***. The following screen will appear.



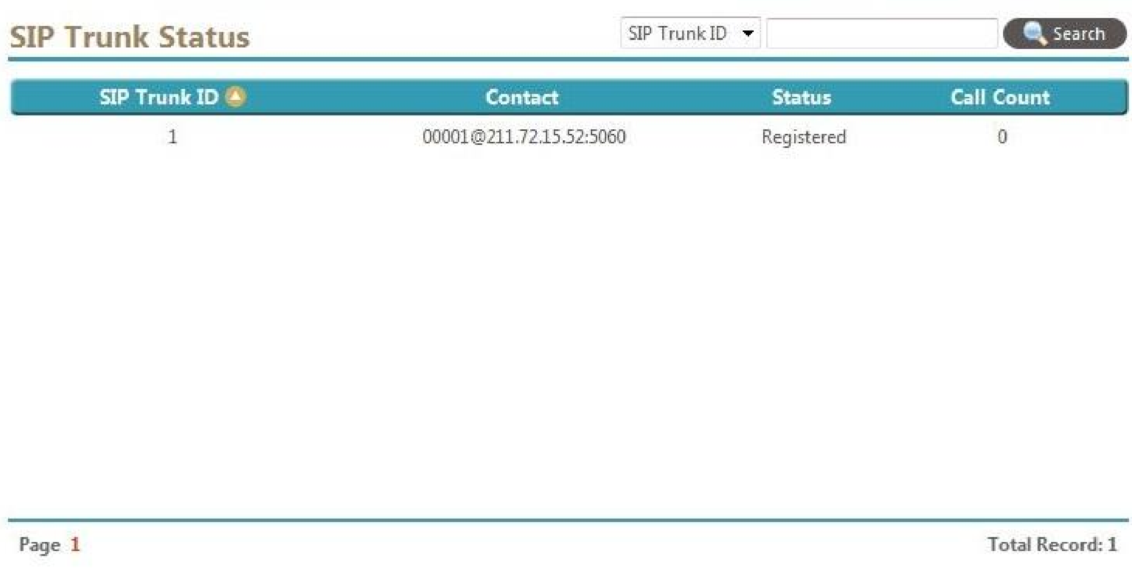
The detail of each filed is described as below:

Field Name	Description
IP Address	The IP address was blocked by the system because of SIP attack detected.

Field Name	Description
Block time	The time to block this IP address.

2.7.6 SIP Trunk Status

The administrator can query the current SIP trunk status by clicking ***DIAGNOSTIC -> SIP Trunk Status.*** The following screen will appear.

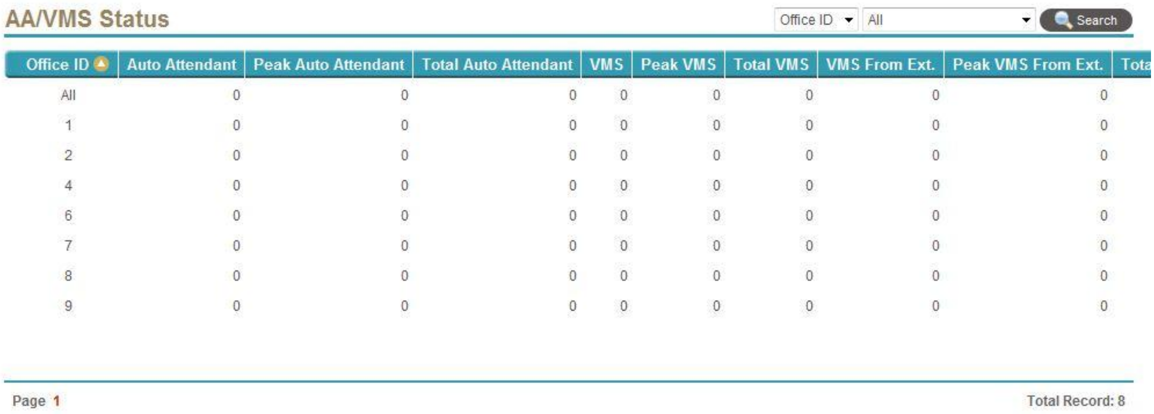


The detail of each filed is described as below:

Field Name	Description
SIP Trunk ID	SIP trunk ID
Contact	SIP trunk register contact
Status	Register status for this SIP trunk
Call Count	Number of concurrent call for this trunk

2.7.7 AA/VMS Status

AA/VMS Status show the current status of service. Click ***DIAGNOSTIC -> AA/VMS Status*** to check the resource status as follows.



Office ID	Auto Attendant	Peak Auto Attendant	Total Auto Attendant	VMS	Peak VMS	Total VMS	VMS From Ext.	Peak VMS From Ext.	Tota
All	0	0	0	0	0	0	0	0	
1	0	0	0	0	0	0	0	0	
2	0	0	0	0	0	0	0	0	
4	0	0	0	0	0	0	0	0	
6	0	0	0	0	0	0	0	0	
7	0	0	0	0	0	0	0	0	
8	0	0	0	0	0	0	0	0	
9	0	0	0	0	0	0	0	0	

The detail of each filed is described as below:

Field Name	Description
Office ID	Office ID for this statistic
Auto Attendant	Service count for auto attendant
Peak Auto Attendant	Peak service count for auto attendant
Total Auto Attendant	The total service count for auto attendant within this period
VMS	Voice Mail service count
Peak VMS	Peak service count for VMS service
Total VMS	The total service count for voice mail within this period
VMS From Ext.	The service count for VMS from extension service.
Peak VMS From Ext.	The peak service count for VMS from extension service.
Total VMS From Ext.	The total service count for VMS from extension within this period.
Music on Hold	Service count for Music on Hold service.
Peak Music On Hold	The peak service count for Music on Hold service.
Total Music On Hold	The total service count for music on hold service within this period.
Meeting Me Conference	The service count for meet me conference service.

Field Name	Description
Peak Meet Me Conference	The peak service count for meet me conference service.
Total Meet Me Conference	The total service count for meet me conference within this period.
Call Park	The service count for call park service
Peak Call Park	The peak service count for call park service
Total Call Park	The total service count for call park service within this period.
Adhoc Conference	The service count for adhoc conference service.
Peak Adhoc Conference	The peak service count for adhoc conference service.
Total Adhoc Conference	The total service count for adhoc conference service within this period.
Ext2Ext VMS	The service count for extension to extension voice mail or direct to voice mail service.
Peak Ext2Ext VMS	The peak service count for extension to extension voice mail or direct to voice mail service.
Total Ext2Ext VMS	The total service count for extension to extension voice mail or direct to voice mail service.

2.7.8 Ping

The administrator can ping a IP address from the host by clicking ***DIAGNOSTIC -> Ping.*** The following screen will appear.

Input the Host IP address and start the ping test.

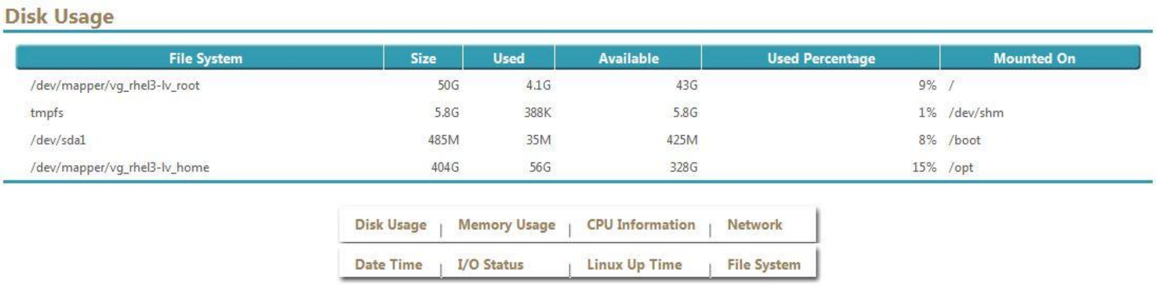
2.7.9 Call Capture

Call capture is a debug tool for tracking a call and suitable for low traffic mode. If you need large traffic capture and analyse, you need have a qos monitor product to do it. Click DIAGNOSTIC -> Call Capture and following will appear:

Select an network interface to capture and required packet filter, click Start Capture to start the capture. Please make sure you stop the capture after you get required packets. Otherwise, the capture might create a big file in your system and eat all hard disk space. Click "Get Capture File" to download the captured file to analyze.

2.7.10 System Information

Click DIAGNOSTIC -> System Information, you will able to see the current system related setting,s including up time, hard disk, cpu, network information as follows:



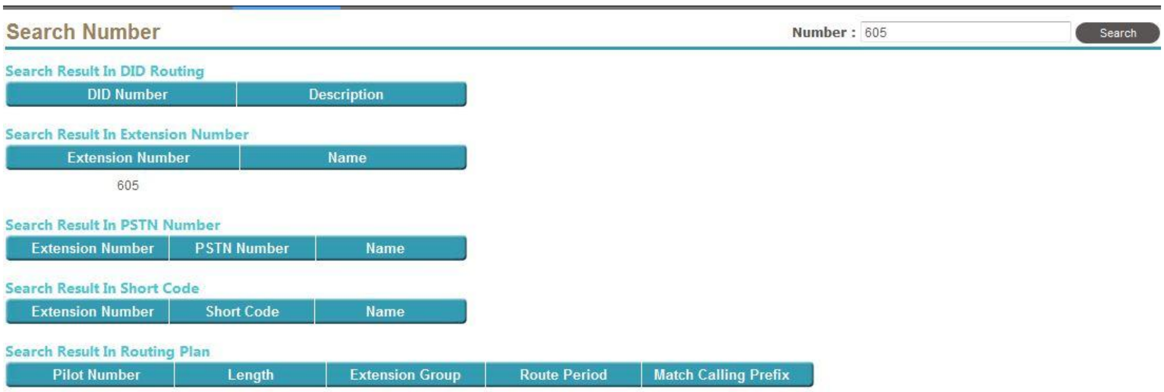
Disk Usage

File System	Size	Used	Available	Used Percentage	Mounted On
/dev/mapper/vg_rhel3-lv_root	50G	4.1G	43G	9%	/
tmpfs	5.8G	388K	5.8G	1%	/dev/shm
/dev/sda1	485M	35M	425M	8%	/boot
/dev/mapper/vg_rhel3-lv_home	404G	56G	328G	15%	/opt

Click each button to see the different status. For detail, please refer to Linux administration guide.

2.7.11 Search Number

Search number can be used to search matched number in DID routing, Extension number, PSTN number, short code or routing plan and display the result for your reference. Click DIAGNOSTIC -> Search Number and the following will appear:



2.7.12 Unassigned Mac List

When CPE can support SIP PnP mutlicasting to find the provisioning server, when CPE turned on, Administrator can find the unassigned line on here. Click DIAGNOSTIC -> Unassigned Mac List and the following will appear:

Select a line and click Assign Extension Number, the following will appear:

Choice the extension and register interface and click Apply. This MAC's CPE will automatically use it without touching to it.

2.8 Administration

The ***Administration*** setting includes the user account management, restart or reboot the service.

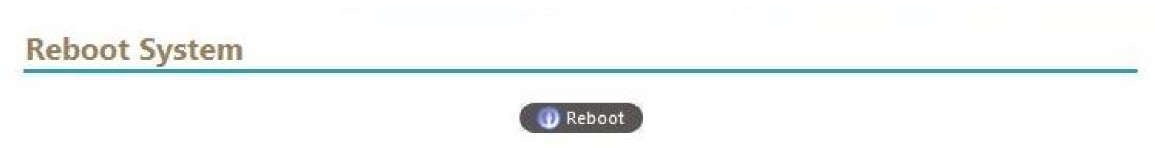
2.8.1 Restart Service

Click ***ADMINISTRATION -> Restart Service*** and the following pop screen will appear.

Click ***restart*** button to restart the whole service.

2.8.2 Reboot System

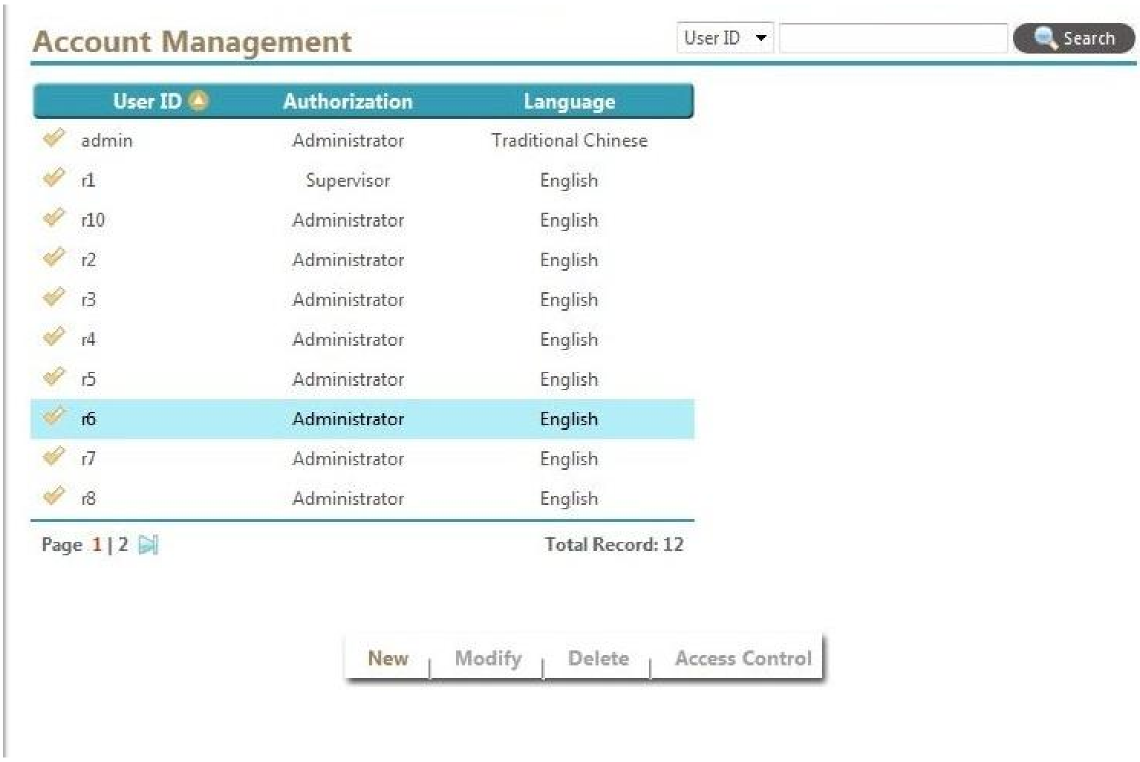
Click ***ADMINISTRATION -> Reboot System*** and the following screen will appear.



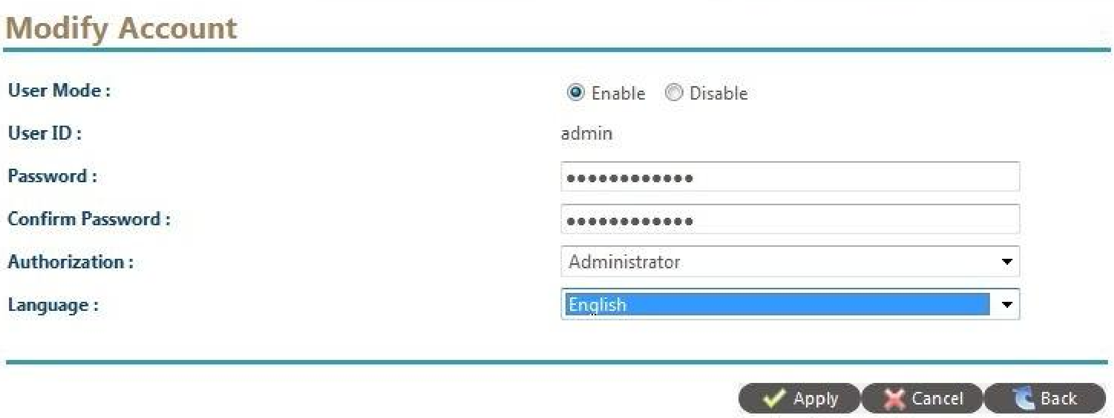
Click ***Reboot*** button to reboot the whole machine.

2.8.3 Account

The system provides 3 different level of user to login the web, Administrator, Supervisor and Extension. The extension login has its own separate port (default is 80/443) in order to make the system secure. Administrator has all access right to manage the system while Supervisor can be customize the access right base on the customer's management requirements. Click ***ADMINISTRATION -> Account*** to view the current settings of user account. The following screen will appear.



Click ***New*** to add a new user and the following screen will appear.



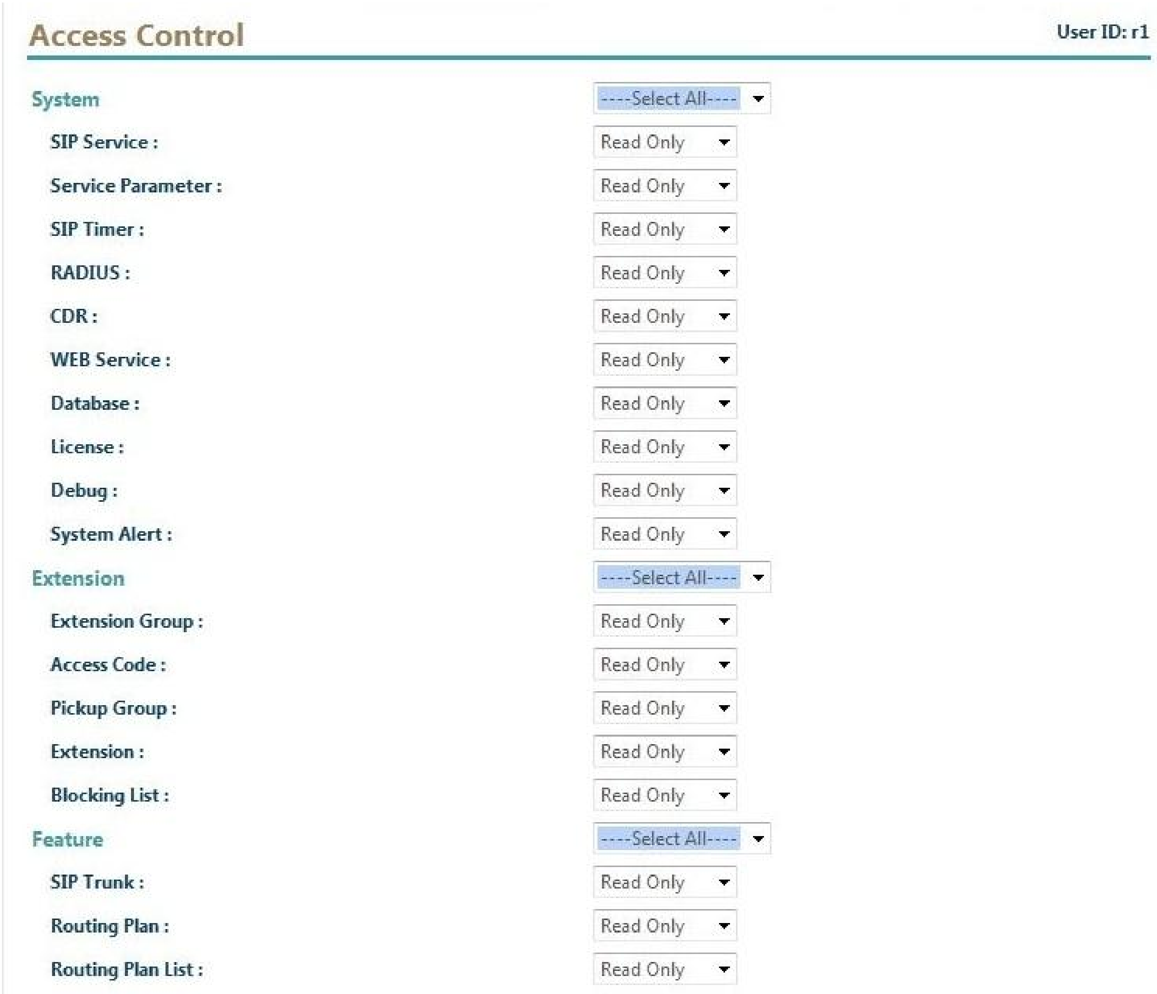
The detail of each parameter is described as below:

Field Name	Description
User Mode	Activate or de-activate the user

Field Name	Description
User ID	The user ID to login
Password	The user password
Authorization	The authorized role for the user. As an administrator, it could do anything while supervisor can be customized to have different access right.
Language	The web GUI language when the user login.

2.8.3.1 Supervisor Access Right

For supervisor, the administrator can define the access list to limit the access of web page by module. Select a existing account which authorization is set to "supervisor" and click the ***Access Control*** to view the current access right of each module as follows.



The administrator can set access deny, read only or full access right for each module. Click ***Apply*** to save.

2.8.4 Clear Hitory Data

It is recommended to clean the unnecessary historical data periodically. Here is the place to clean those historical data. Click ***Administration -> Clear History Data*** to clean those historical data.

Select those data you want to delete, click apply to delete it.

2.8.5 Backup/Restore

Backup/Restore is used to backup the system configuration or restore it back. All the configuration will be saved. Click ***ADMINISTRATION -> Backup/Restore*** to do the backup to restore.

Select Backup System Configuration to backup the system configuration.
Select Restore System Configuration to restore it back.

2.8.6 Upgrade System

Use ***Upgrade System*** to do the application patch by clicking ***ADMINISTRATION -> Upgrade System***. Please only use the certificated patch file to do the upgrade. Otherwise, it will had problems.

After upgrade, reboot the machine to take effective.

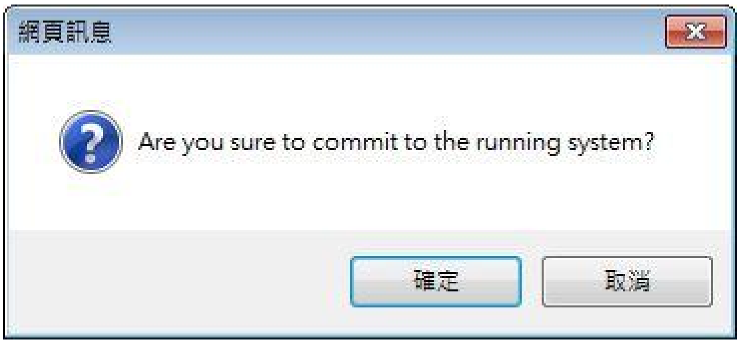
2.8.7 Logout

To quit the management web for the current user, click ***ADMINISTRATION -> Logout*** and the following pop screen will appear.

Click ***OK*** to logout.

2.9 Commit

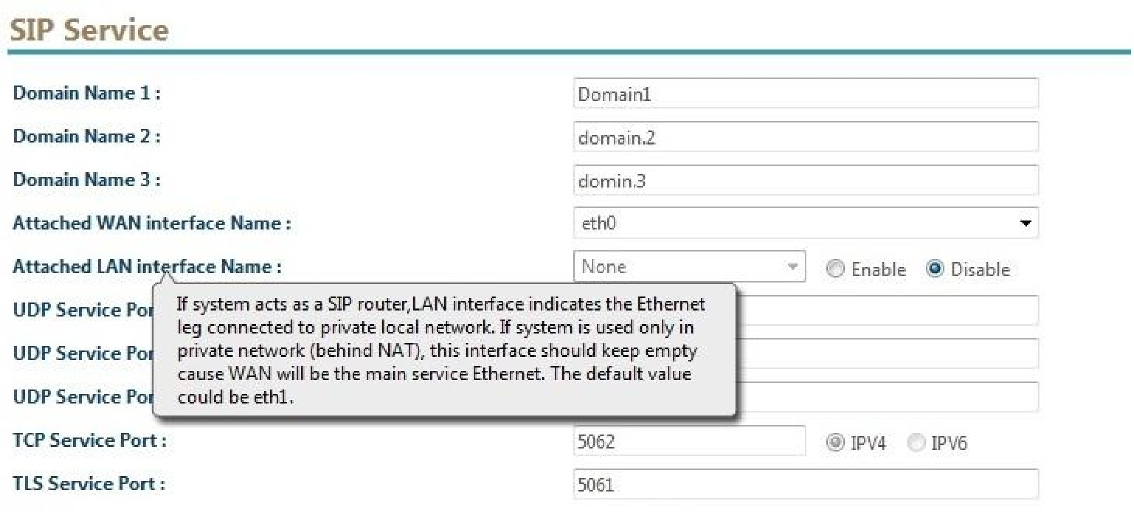
After you change the system settings, you need to apply it by clicking the ***COMMIT*** and the following popup screen will appear:



Select OK to commit the changes.

2.10 Help

The system provides pop up help hint when you move the cursor to the filed as follows.



Also you can click ***HELP*** to see on line help which provides the same information as this guide.

3 Division Manger Login

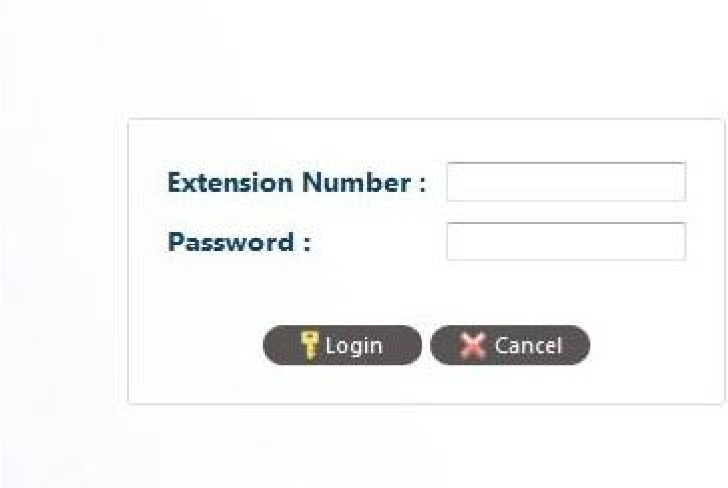
The division manager use the same login URL as administrator. After login, it can only access to those division owned extension. Each division can only have 1 division manager. After login the following screen will appear.

Please refer to ***Billing*** and ***Extension*** settings for detail. Please don't forget to click ***COMMIT*** to apply the configuration to running system.

4 Extension Login

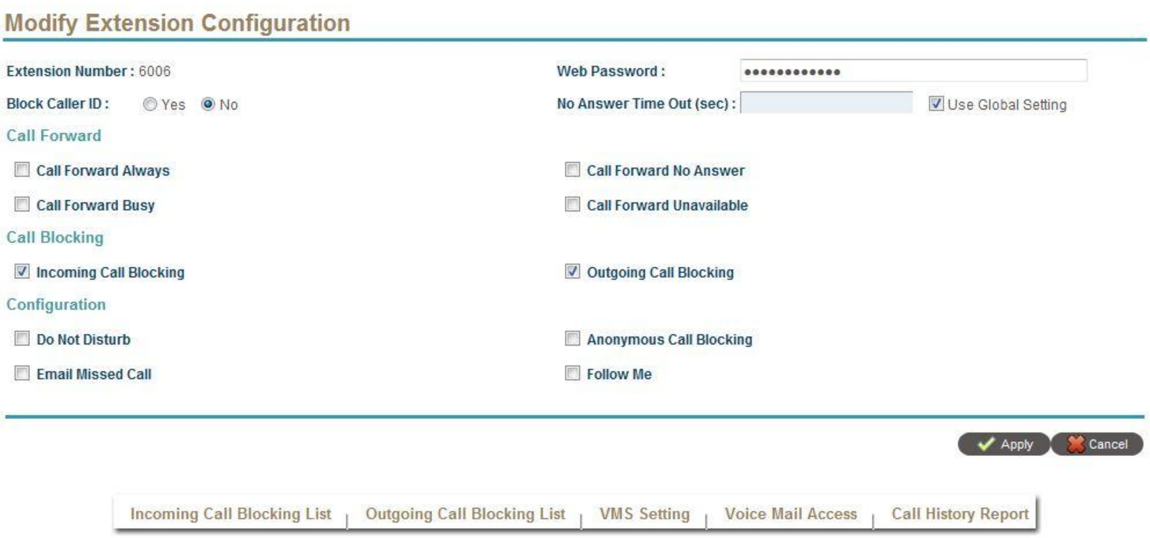
In order to make the system more secure, the system provides a separate port for extension login. The default login for http port is 80 and the default SSL login port is 443. Both are de-fact port for web access and make the customer easily to remember. It can be changed on ***SYSTEM -> Web Service***.

By using the default settings, the user should able to type http://xxx.xxx.xxx.xxx or https://xxx.xxx.xxx.xxx to login. The following screen will appear. Input Extension Number and Web password to login the extension page.



4.1 Extension Settings

After extension login, the extension setting pages will appear as follows:



The detail of each parameter is described as below:

Parameter Name	Description
Extension Number	The extension telephone number for SIP registration (from/ to header).
Web Password	The password for extension owner to login the extension web for service settings. In order to allow extension login, the "SYSTEM->WEB Service->Allow Extension Logon" need to be set to enable. The web password can only allow digits (0-9), since it will be used for "outgoing call privilege access" as a password.
Block Caller ID	Whether to enable caller ID sending (CLIP) or not (CLIR).
No Answer Time Out	The time to wait in seconds for the called party to answer. The default value is to use the global settings in SYSTEM->Service Parameter->No Answer Time Out.
Call Forward Always	Enable call forward always.
Always Forward Number	The telephone number to be forwarded
Call Forward No Answer	Enable call forward for no answer call.
No Answer Forward Number	The telephone number to be forwarded
Call Forward Busy	Enable call forward for a busy call.
Busy Forward Number	The telephone number to be forwarded
Call Forward Unavailable	Enable call forward when SIP client is not registered.
Unavailable Forward Number	The telephone number to be forwarded
Incoming Call Blocking	When it is checked, the incoming call will be filtered by matching the "calling party number" with "Incoming call blocking list". If it is matched, the call will be rejected
Outgoing Call Blocking	When it is checked, the dialed number will be filtered by "Outgoing Call Blocking List". If the leading pattern was matched the list, the call will be rejected

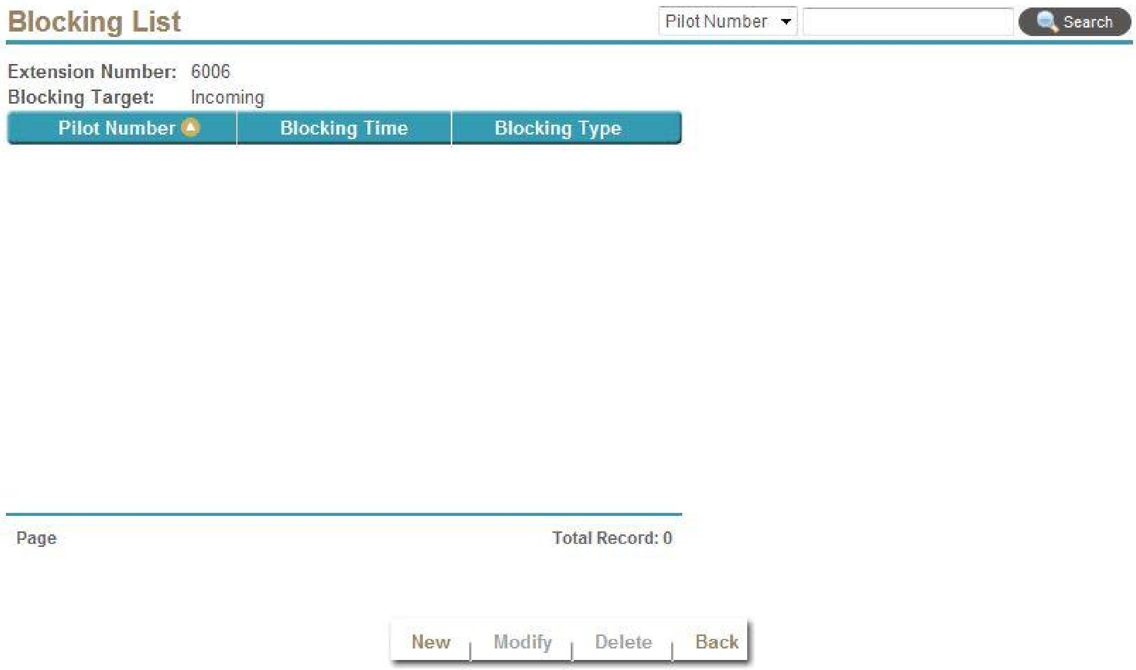
Parameter Name	Description
Anonymous Call Blocking	When the incoming call doesn't include the caller ID, whether to reject it or not.
Email Missed Call	If the extension is unable to take the call, whether to send a email to extension owner or not.
Do Not Disturb	Enable Do Not Disturb or not. When DND is enabled, the desired period for DND should be defined.
Follow Me	Enable Follow Me here service or not. When enable follow me, the Follow Me number should be defined.

The Follow Me parameters are described as follows:

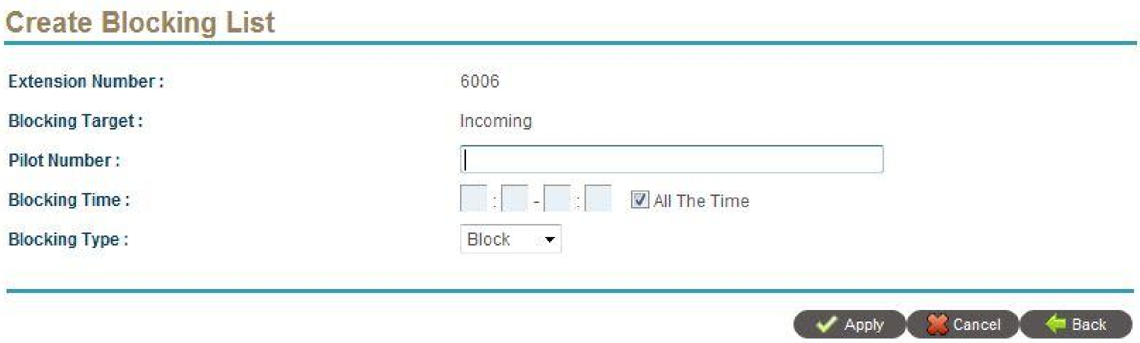
Parameter Name	Description
Start Time	The start time (24 hours format) to enable this follow me number. Earlier than this time, this follow me number will be ignored. You can also click the "All the Time" for whole day service.
Stop Time	The stop time (24 hours format) to enable this follow me number. Over this time, this follow number will be ignored. You can also click the "All the Time" for whole day service.
Follow Number	The telephone number to be followed when the time is in between start and stop time.

4.2 Incoming Call Blocking List

When enabled the incoming call block feature in ***Extension Setting***. The calling party number defined here will be filtered based on the blocking type.



Select New, Modify, Delete to change the screening setting. The following web page will appear:



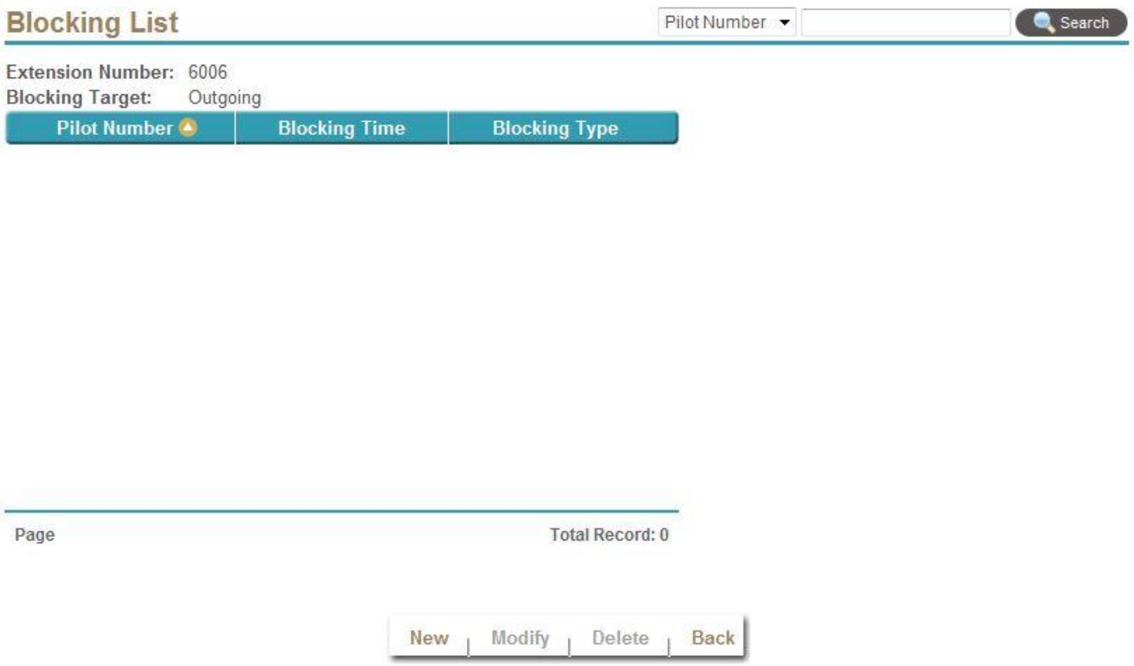
The detail of each parameter is described as below:

Parameter Name	Description
Blocking Target	Incoming call or outgoing call to be screened.
Pilot Number	The calling number used to be matched. If incoming calling number (SIP user part) is matched, the call might be rejected or accepted based on the "Blocking Type".

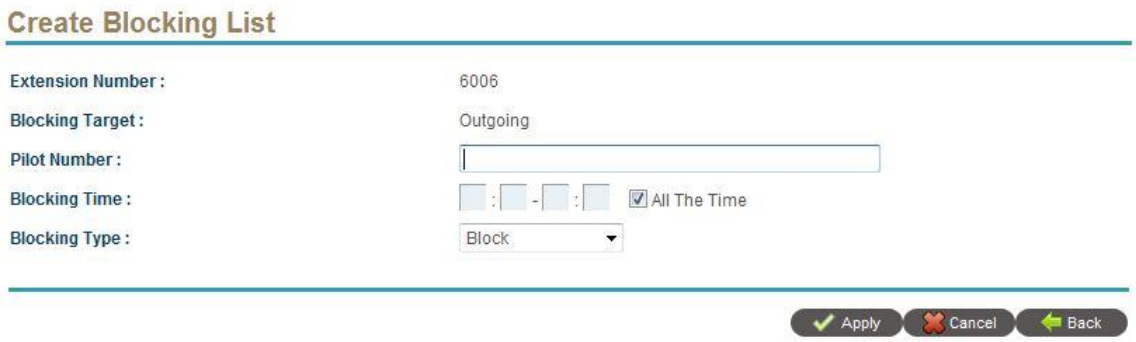
Parameter Name	Description
Blocking Time	The system allow to have time restricted screening feature. When you enter the blocking time for a screening list, this screen will only affected by this certain period.
Blocking Type	Whether to block or unblock it. When all entries in the same group are set to "block", it means all call can be passed unless those listed pilot number. When all entries are set to "unblock", only those calls matched the entry will able to get through. If some of entries are set to "block" and some are set to "unblock", the call matched "blocked" list will be rejected first and the call matched "unblock" list will able to get through.

4.3 Outgoing Call Blocking List

When enabled the outgoing call block feature in ***Extension Setting***. The called number prefix defined here will be filtered based on the blocking type.



Select New, Modify, Delete to change the screening setting. The following web page will appear:

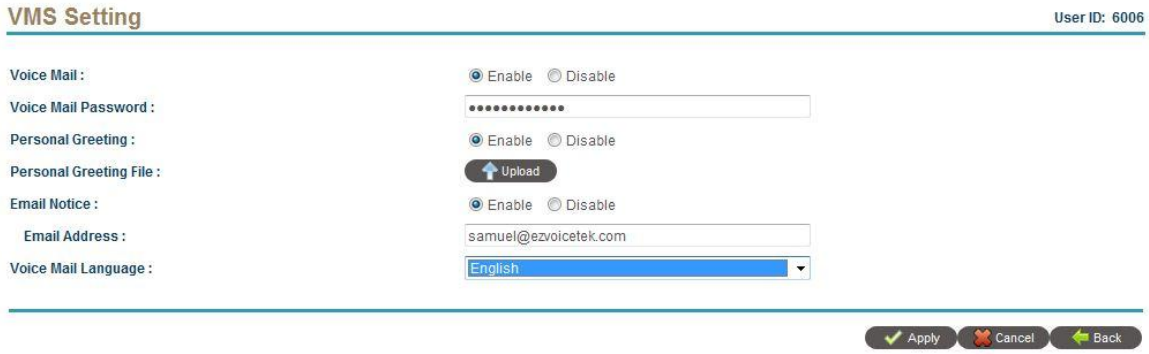


The detail of each parameter is described as below:

Parameter Name	Description
Blocking Target	Incoming call or outgoing call to be screened.
Pilot Number	The called number prefix used to be matched. If the outgoing number prefix is matched the pilot number, the call might be rejected or accepted based on the "Blocking Type".
Blocking Time	The system allow to have time restricted screening feature. When you enter the blocking time for a screening list, this screen will only affected by this certain period.
Blocking Type	Whether to block, unblock or privilege access for the pilot number prefix. When all entries in the same group are set to "block", it means all call can be passed unless those listed pilot number. When all entries are set to "unblock", only those calls matched the entry will able to get through. If some of entries are set to "block" and some are set to "unblock", the call matched "blocked" list will be rejected first and the call matched "unblock" list will able to get through. For those entries are set to "privilege access", it will able to get through when you use "Enable Privilege Access" access code to turn it on to call and use "Disable Privilege Access" access code to turn it off.

4.4 VMS Setting

This is the setting for VMS setting. You can turn on and off for your voice mail or ask to send to email as follows:

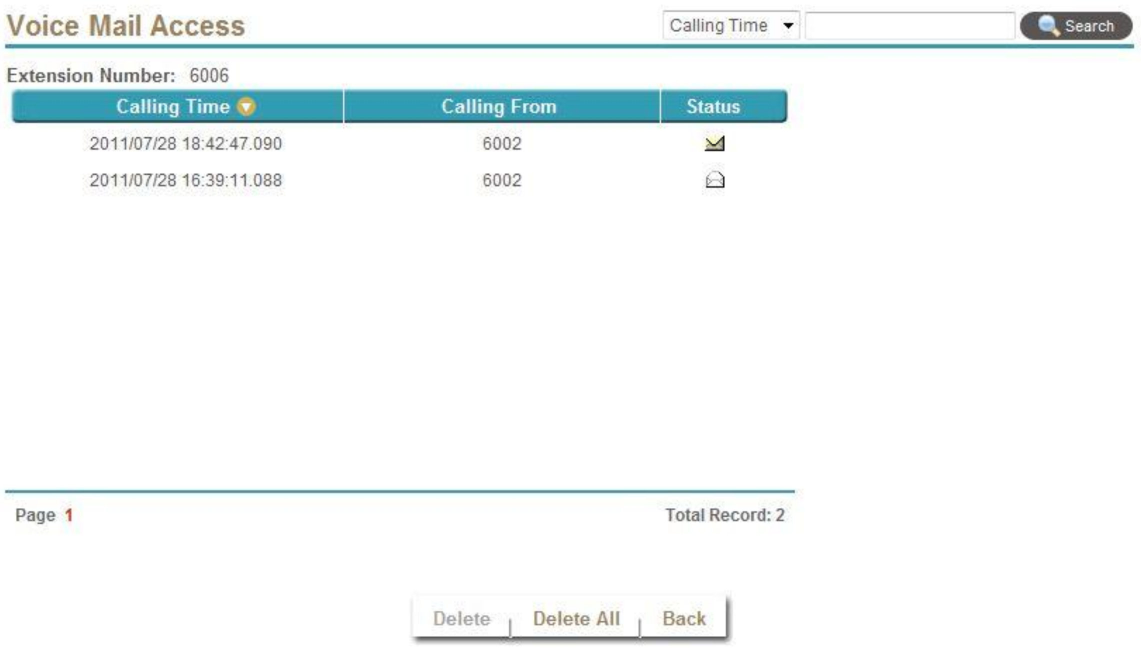


The detail of each parameter is described as below:

Parameter Name	Description
Voice Mail	Whether enable or disable the voice mail.
Voice Mail Password	The password to access the voice mail.
Personal Greeting	The personal greeting when get into the extension's voice mail.
Personal Greeting File	The wav file for personal greeting. The file format is 8K * 16 bits linear PCM Mono Wav. You can upload your own by clicking upload button.
Email Notice	Email Notify when a new voice mail arrived.
Email Address	The mail address for send notice
Voice Mail Language	The default voice mail language for this extension

4.5 Voice Mail Access

To check voice mail by web, click ***Voice Mail Access*** and the following screen will be displayed.

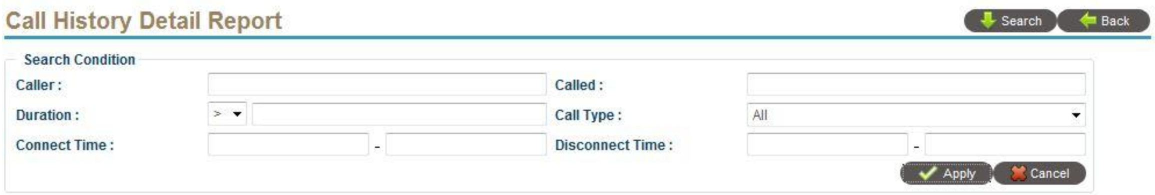


You can double click the item to hear the voice mail. The detail of each parameter is described as below:

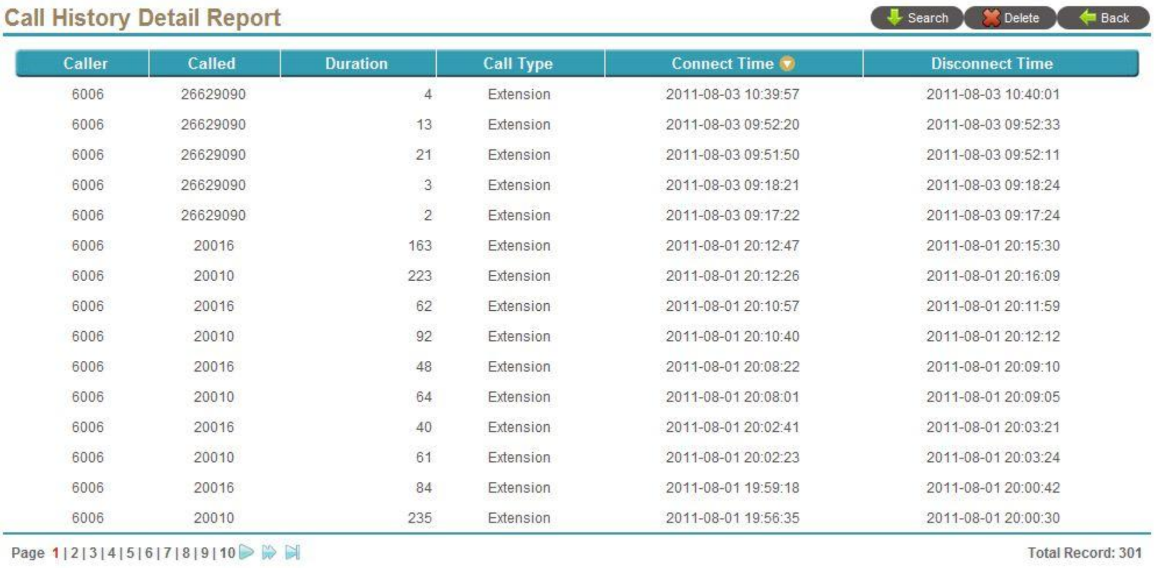
Parameter Name	Description
Calling Time	The time to start the call
Calling From	The calling party number
Status	Whether the voice mail was read or not?

4.6 Call History Report

Extension can query hist own call history list by clicking ***Call History Report***. A search criteria will appear for query as follows:



After apply the search criteria, the following report will appear.



Call History Detail Report

Search | Delete | Back

Caller	Called	Duration	Call Type	Connect Time	Disconnect Time
6006	26629090	4	Extension	2011-08-03 10:39:57	2011-08-03 10:40:01
6006	26629090	13	Extension	2011-08-03 09:52:20	2011-08-03 09:52:33
6006	26629090	21	Extension	2011-08-03 09:51:50	2011-08-03 09:52:11
6006	26629090	3	Extension	2011-08-03 09:18:21	2011-08-03 09:18:24
6006	26629090	2	Extension	2011-08-03 09:17:22	2011-08-03 09:17:24
6006	20016	163	Extension	2011-08-01 20:12:47	2011-08-01 20:15:30
6006	20010	223	Extension	2011-08-01 20:12:26	2011-08-01 20:16:09
6006	20016	62	Extension	2011-08-01 20:10:57	2011-08-01 20:11:59
6006	20010	92	Extension	2011-08-01 20:10:40	2011-08-01 20:12:12
6006	20016	48	Extension	2011-08-01 20:08:22	2011-08-01 20:09:10
6006	20010	64	Extension	2011-08-01 20:08:01	2011-08-01 20:09:05
6006	20016	40	Extension	2011-08-01 20:02:41	2011-08-01 20:03:21
6006	20010	61	Extension	2011-08-01 20:02:23	2011-08-01 20:03:24
6006	20016	84	Extension	2011-08-01 19:59:18	2011-08-01 20:00:42
6006	20010	235	Extension	2011-08-01 19:56:35	2011-08-01 20:00:30

Page 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10   Total Record: 301

The detail of each report field is described as follows:

Field Name	Description
Caller	calling party number
Called	called party number
Duration	call duration
Call Type	Call type could be the following: Extension: extension to extension calls Outgoing: Extension outgoing call Incoming: Incoming call to extension Misc: Others call type
Connect Time	The call connect time
Disconnect Time	The call disconnecting time

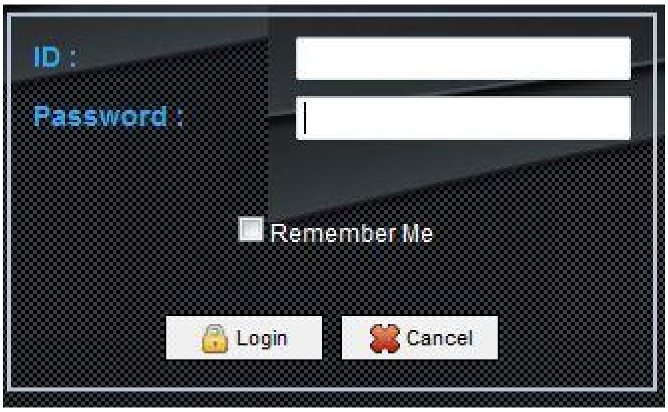
4.7 Smart Calling

The Smart Calling feature enable you to make your smart phone becomes a small office center. It provides the following unique features:

1. Allow to enable call forward to your smart phone to receive calls.

2. Allow to call your customers using office extension
3. Allow to create a 16-parties conference
4. Allow to monitor the meeting me conference room

To enable you to use smart calling feature, the extension need have "Outgoing Call within AA" enabled. And then you can use your smart phone or smart pad to login the extension office (default URL is http://xxx.xxx.xxx.xxx:81/). And the following login screen will appear. If you are login from the PC, you should able to click Smart Calling button after you login.



After login, you should see the following.

4.7.1 Settings

Click Settings and the following will appear.

The detail of each parameter is described as below:

Parameter Name	Description
Forward to My Phone	Whether to forward my extension to "My Phone" or not.
My Phone	The telephone number will be used as my phone number for forward, calling out and conference.
Language	The service language will be used for IVR prompt.

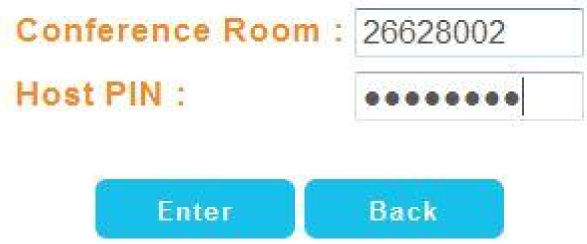
4.7.2 Call To

Click Call To and the following will appear to allow to call out to some one by using office's PBX.

Click  to add a user from users phone book or type the outgoing call number as above. Then click  to start the calling. The system will call you "MY Phone" first and start the calling.

4.7.3 Meet Me Conference

By using your smart phone, you can manage the meeting me conference from anywhere. Click Meet Met Conference and the following will appear.

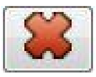


Enter the monitored meet me conference room number and host PIN code, press Enter and the following will appear.

The above had 2 participants are joined, you can use the following to control the conference room.

 Mute the participant or whole conference room.

 Un-mute the participant or whole conference room.

 Disconnect the user from the conference room.

 Quit the meet me conference control and back to menu.

4.7.4 Create Conference

You can create a conference on demand from your smart phone or pad anywhere. Click Create Conference and the following will appear.

Click  to add a phone book group into conference room.

Click  to add a contact from phone book into conference room.

Click  to add telephone numbers into conference room.

After you select the participants need to be joined the conference, click Create to start the conference room. The following screen will appear.

You can use the following to control the conference room.

 Add a new contact from phone book into conference room.

 Add a new telephone number into conference room.

 Mute the participant or whole conference room.

Un-mute the participant or whole conference room.

 Disconnect the user from the conference room.

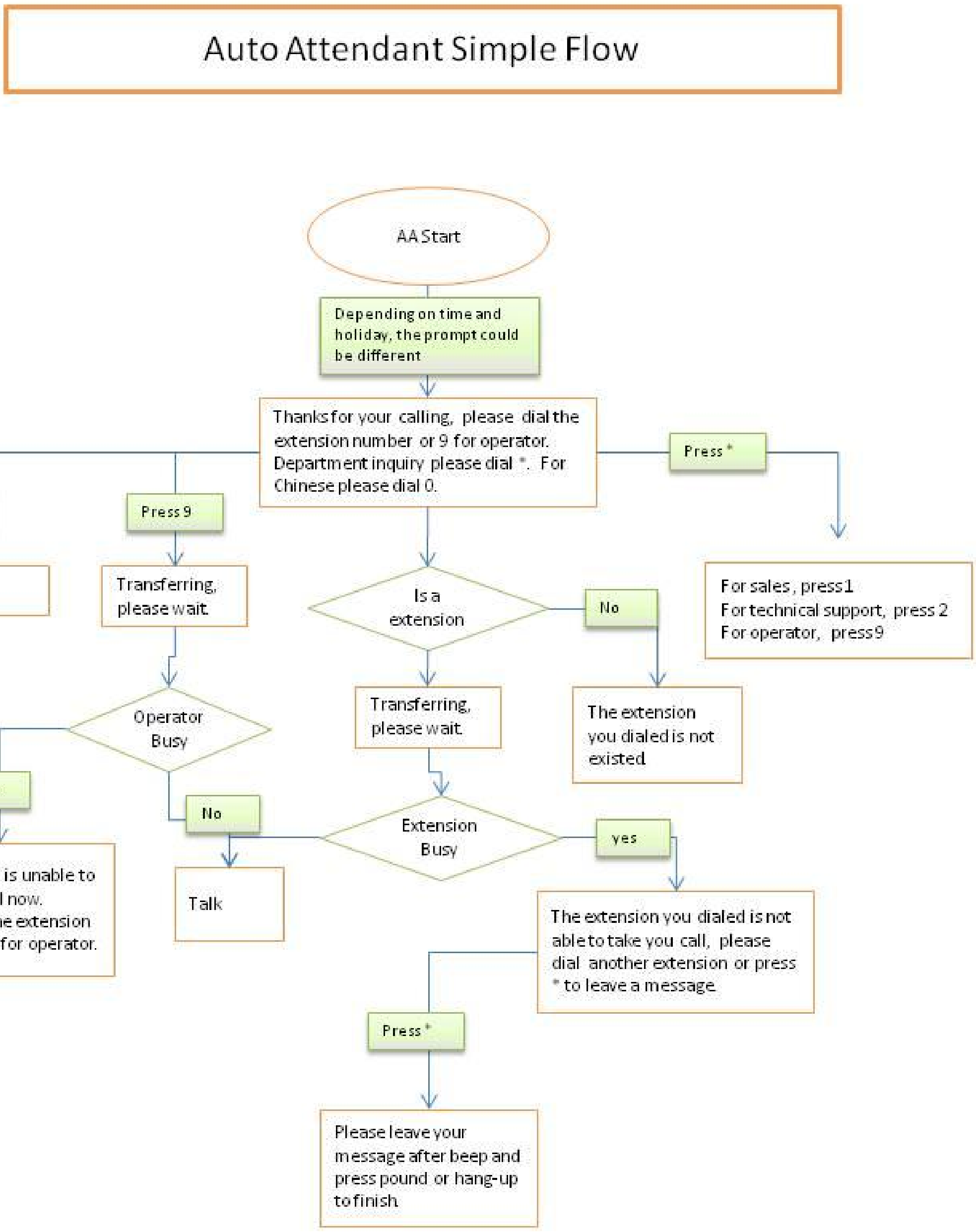
 The participant was disconnect, click to redial to invite him to join again.

Quit the meet me conference control and back to menu.

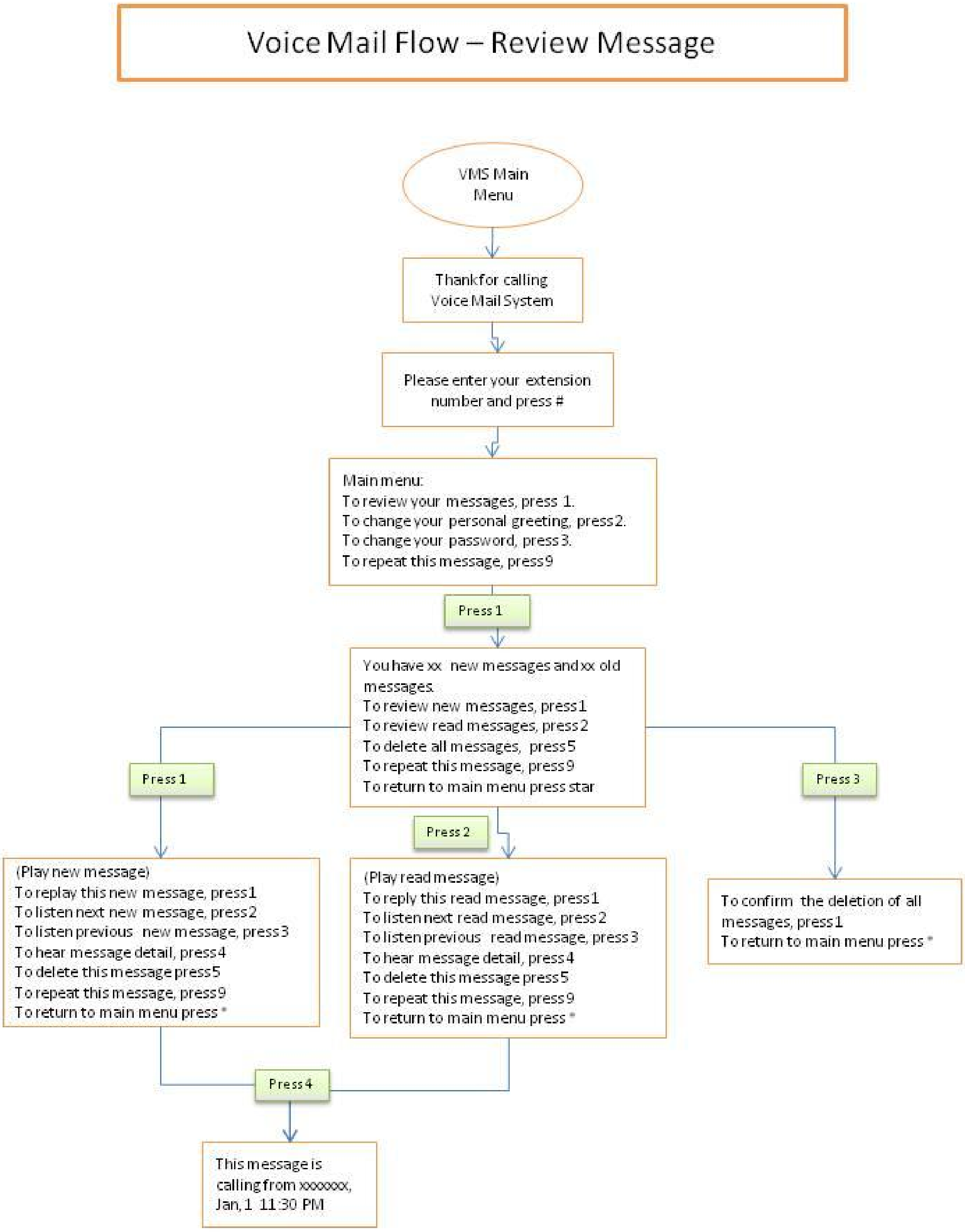
5 Appendix

5.1 Call Flow Reference

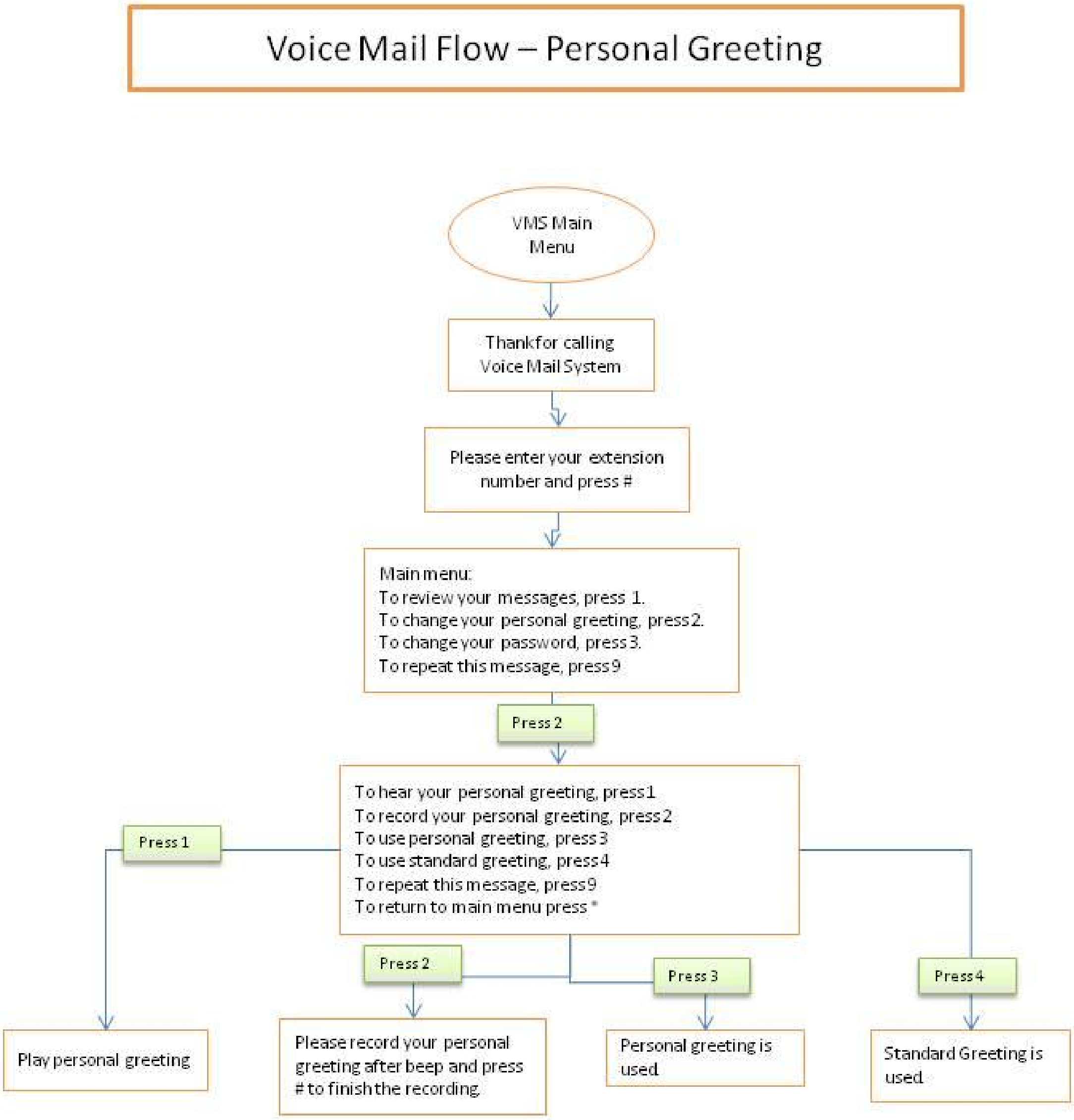
5.1.1 AA Call Flow Sample



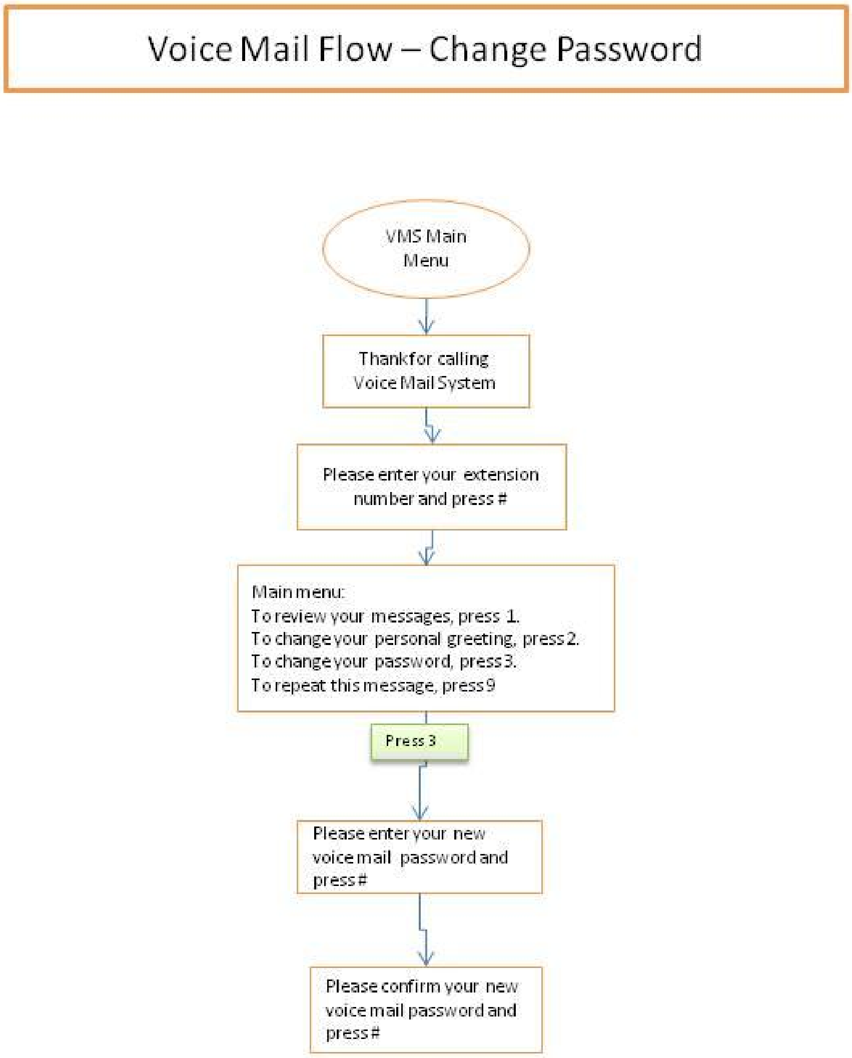
5.1.2 VMS Flow - Review Message



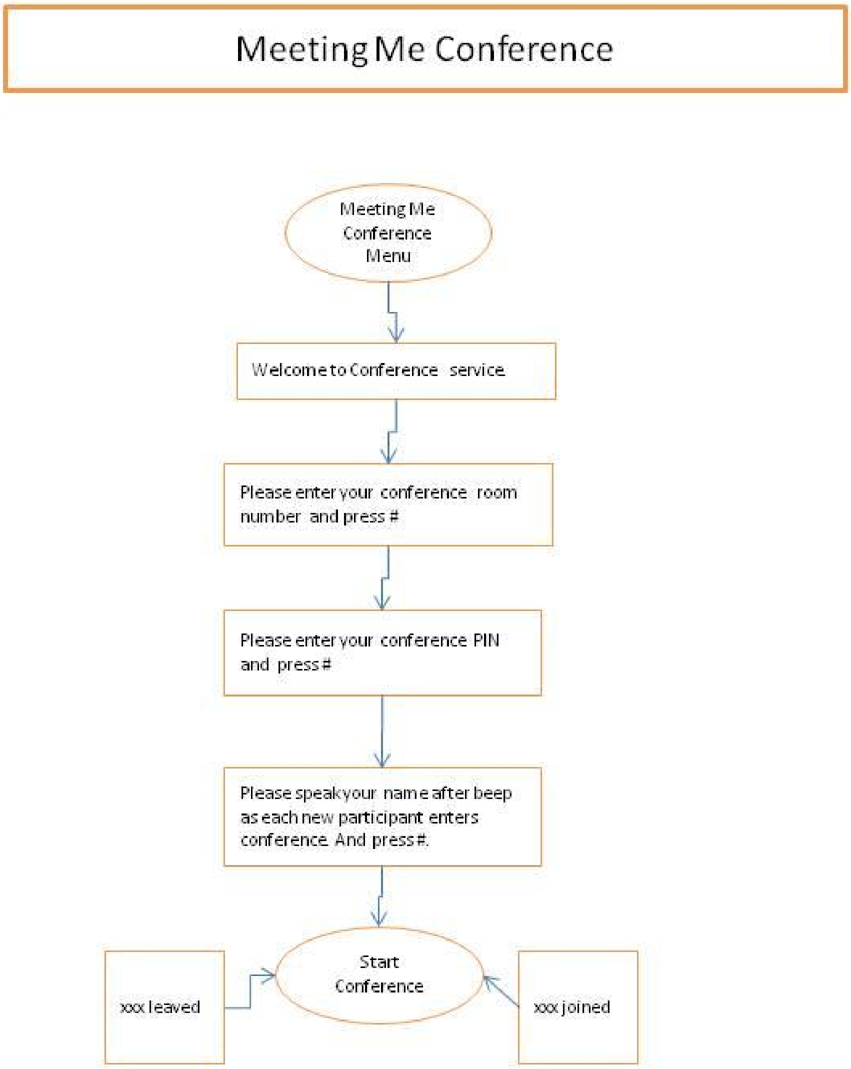
5.1.3 VMS Flow - Personal Greeting



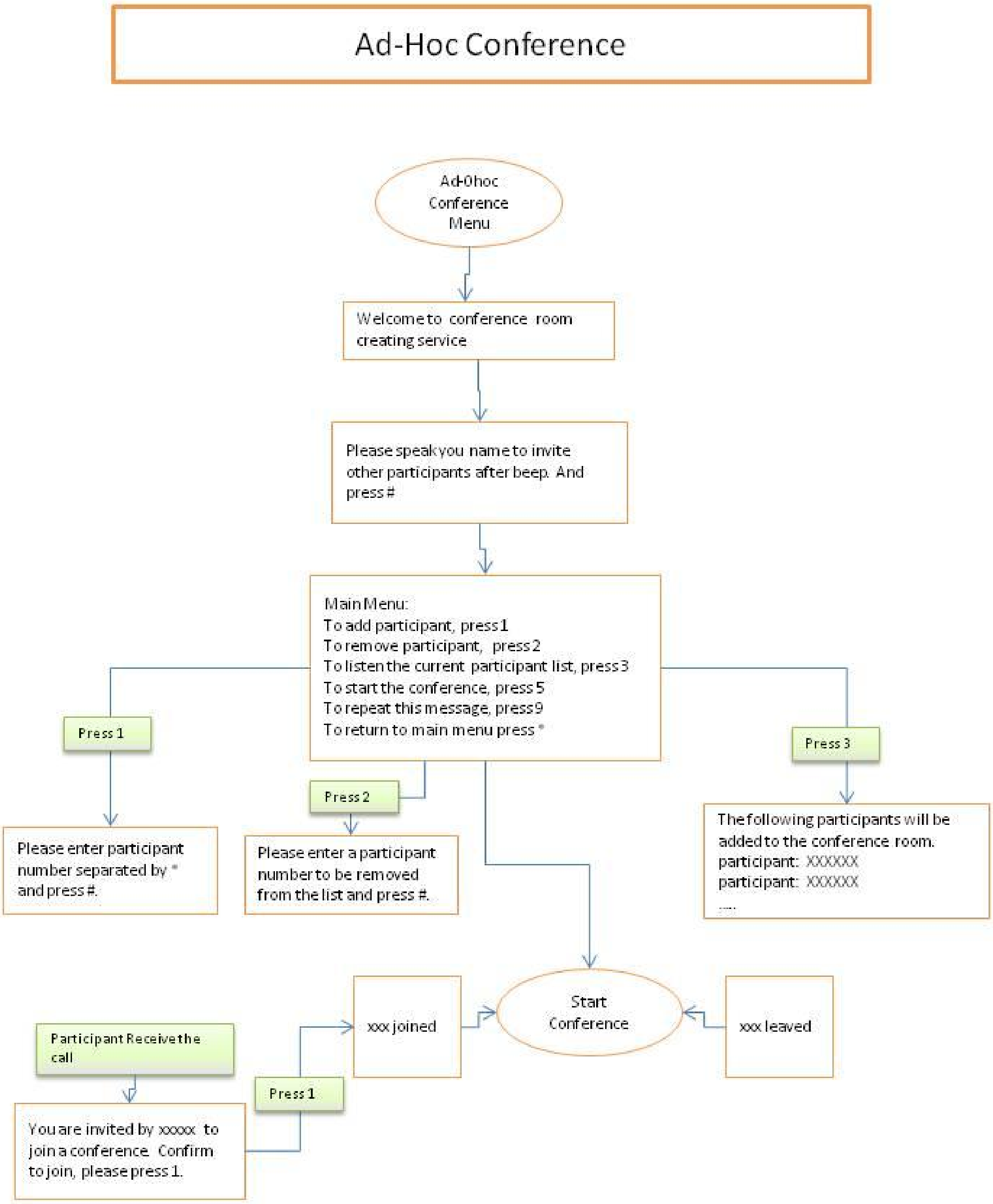
5.1.4 VMS Flow - Change Password



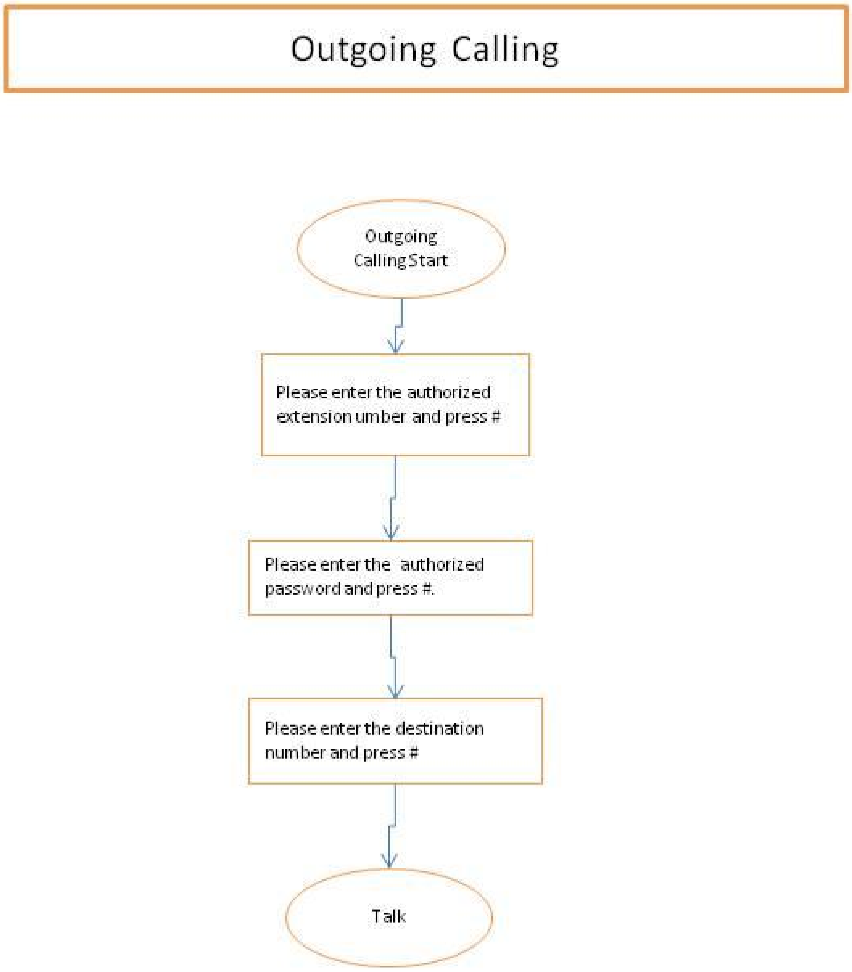
5.1.5 Meeting Me Conference



5.1.6 Ad-Hoc Conference



5.1.7 Outgoing Calling



5.2 RADIUS Attribute List

This appendix including the system provides RADIUS attribute list for connecting to a RADIUS server.

5.2.1 Authorization Request Message

The authorization message will be send if RADIUS service is turn on and RADIUS Call Authorization is check in Extension. If the RADIUS return failed, the call will be rejected.

Attribu te	Attribute Name	VS A	Description	Form at	Example
4	NAS-IP-Address		IP Address of the In-Bound gateway	Nume ric	4 bytes unsigned long
61	NAS-Port-Type		Physical port type	Nume ric	0: Asynchronous
6	Service-Type		Type of service requested	Nume ric	5: Outbound
1	User-Name		Account number	String	1001
30	Called-Station-Id		Destination phone number	String	1001
31	Calling-Station-Id		Calling Party Number (ANI)	String	1002
26	h323-conf-id	24	GUID	String	xxxx
26	call-origin-endpt	152	calling remote address (public IP if appliable)	String	112.1.1.1:5060
26	h323-call-type	27	Protocol type or family used on this leg of the call	String	VOIP
26	gw-rxd-cdn	153	The called number as received by the gateway in the incoming signalling message before any translation rules are applied.	String	1002
26	incoming-req-uri	151	Incoming call leg request URI SIP: sip:user@ip:port	String	sip:1002@192.168.1.1:5060
26	outgoing-req-uri	154	outgoinh call leg request URI	String	sip:1002@192.168.1.1:5060

Attribute	Attribute Name	VSA	Description	Format	Example
			SIP: sip:user@ip:port		
2	User-Password		16 octets user password	String	

5.2.2 Authorization Response Message

The RADIUS server could response the following attributes for authorization request.

Attribute	Attribute Name	VSA ID	Description	Format	Example
26	h323-return-code	103	The reason for failing authentication	Sting	0: Authenticated 1: Invalid Account 2: Invalid pin number 3: Account in use 4: Zero Balance 5: Account Expired 6. Over Credit Limit 7: Denied User 9: Called Number Blocked 10: Number of Retries Exceeded 11: Invalid argument 12: Insufficient Balance
26	h323-credit-time	102	Number of seconds for which the call is authorized. It has higher priority than session time out.	String	900
27	session-timeout		Allowed session time (ignored if h323-credit-time found)	Numeric	4 bytes unsigned long -- 900

5.2.3 Start Accounting Message

When a call is connected, the RADIUS billing start could be set to send to RADIUS server. The following is the Start Accounting Message which will be sent out.

Attri bute	Attribute Name	SA ID	Description	For mat	Example
4	NAS-IP-Address		IP Address of the In-Bound gateway	Num eric	4 bytes unsigned long
61	NAS-Port-Type		NAS port type	Num eric	0: Asynchronous
1	User-Name		User Account	Strin g	1001
31	Calling-Station-Id		Calling Party Number (ANI)	Strin g	1001
30	Called-Station-Id		Called Party Number (DNIS)	Strin g	1002
40	Acct-Status-Type		Message Request Type	Num eric	1: Start Accounting
6	Service-Type		Type of Service Requested	Num eric	5: Outbound
26	H323-gw-id	33	Name of the SIP Proxy Server	Strin g	SIP Proxy Name or IP
26	call-origin-endpt	152	calling remote address (public IP)	Strin g	112.3.1.3:5060
26	h323-remote-address	23	called remote address (public IP)	Strin g	112.4.1.1:8080
26	h323-conf-id	24	GUID	Strin g	xxxxx-xxxxx
26	h323-call-type	27	Protocol type or family used on this leg of the call	Strin g	VOIP
26	h323-call-origin	26	‘Originate’ or ‘Answer’	Strin g	Originate
26	h323-setup-time	25	Setup time	Strin g	yyyy/mm/dd hh:mm:ss
26	outgoing-setup-time	171	Outgoing setup time	Strin g	yyyy/mm/dd hh:mm:ss
26	call-alert-time	168	Alter time	Strin g	yyyy/mm/dd hh:mm:ss

Attribute	Attribute Name	SA ID	Description	Format	Example
26	h323-connect-time	28	Connect time	String	yyyy/mm/dd hh:mm:ss
26	gw-rxd-cdn	153	The called number as received by the gateway in the incoming signalling message before any translation rules are applied.	String	1002
26	call-id	173	SIP call ID kept for whole call	String	
26	fdcnt	174	Forward Count	String	0: normal call, 1: 1st forward
26	incoming-req-uri	151	Incoming call leg request URI SIP: sip:user@ip:port	String	sip:1002@112.3.3.3:5060
26	outgoing-req-uri	154	outgoing call leg request URI (after DM) SIP: sip:user@ip:port	String	sip:1002@112.3.3.3:5060
44	Acct-Session-Id		A unique accounting identifier	String	8 bytes, like 12345678
41	Acct-Delay-Time		No of seconds tried	Numeric	3

5.2.4 Stop Accounting Message

When a call is disconnected, the RADIUS billing stop could be set to send to RADIUS server. The following is the StopAccounting Message which will be sent out.

Attribute	Attribute Name	VSA ID	Description	Format	Example
4	NAS-IP-Address		IP Address of the In-Bound gateway	Numeric	4 bytes unsigned long
61	NAS-Port-Type		Physical port type	Numeric	0: Asynchronous
1	User-Name		Account number	String	1001
30	Called-Station-Id		Destination phone number	String	1001
31	Calling-Station-		Calling Party Number (ANI)	String	1002

Attribute	Attribute Name	VSA ID	Description	Format	Example
	Id				
40	Acct-Status-Type		Account Request Type	Numeric	2: Stop Accounting
6	Service-Type		Type of service requested	Numeric	5: Outbound
26	h323-gw-id	33	Name of gateway	String	SIP Proxy IP
26	h323-conf-id	24	GUID	String	xxxx
26	h323-call-type	27	Protocol type used on this leg of the call - Telephony or VOIP	String	VOIP
26	h323-setup-time	25	Setup time	String	yyyy/mm/dd hh:mm:ss
26	outgoing-setup-time	171	Outgoing setup time	String	yyyy/mm/dd hh:mm:ss
26	call-alert-time	168	alert time in	String	yyyy/mm/dd hh:mm:ss
26	h323-connect-time	28	Connect time	String	yyyy/mm/dd hh:mm:ss
26	h323-disconnect-time	29	Disconnect time	String	yyyy/mm/dd hh:mm:ss
26	h323-disconnect-cause	30	SIP Disconnect Cause Code	String	200
26	h323-call-origin	26	‘Originate’ or ‘Answer’	String	Originate
26	call-origin-endpt	152	calling remote address (public IP)	String	112.3.3.3
26	h323-remote-address	23	called remote address (public IP)	String	112.3.3.5
26	gw-rxd-cdn	153	The called number as received by the gateway in the incoming signalling message before any translation rules are applied.	String	1002
26	call-id	173	SIP call ID kept for whole call	String	

Attribute	Attribute Name	VSA ID	Description	Format	Example
26	fdcnt	174	Forward Count	String	0: normal call, 1: 1st forward
26	incoming-req-uri	151	Incoming call leg request URI SIP: sip:user@ip:port	String	sip:1001@192.168.1.1:5060
26	outgoing-req-uri	154	outgoing call leg request URI (after DM) SIP: sip:user@ip:port	String	sip:1001@192.168.1.1:5060
44	Acct-Session-Id		A unique accounting identifier-match start & stop	String	8 bytes, like 12345678
46	Acct-Session-Time		For how many second the user receive the service	Numeric	320
41	Acct-Delay-Time		No of seconds tried	Numeric	3

5.3 Call Detail Record Description

Call Detail Record format is described as follows. The billing start and stop are saved at one file.

Field Index	Field Name	Description
1	RADIUS Client IP	RADIUS Client (NAS) IP address (NAS-IP-Address)
2	SIP Proxy IP	SIP Proxy IP address (h323-gw-id)
3	Account Type	Accounting Type: 1. Billing Start, 2: Billing Stop (Acct-Status-Type)
4	User	SIP User Name to be Charged (User-Name)
5	Called Number	Called Number (Called-Station-Id)
6	Calling Number	Calling Number (Calling-Station-Id)
7	Call Type	Call Type: "VOIP" (h323-call-type)
8	Service Type	RADIUS Service Type: outbound (Service-Type)
9	Call ID	RADIUS Conference ID which is globally unique (h323-conf-id)

Field Index	Field Name	Description
10	Account Session ID	A unique accounting identifier-match start & stop (Acct-Session-Id)
11	Talk Time	Call Duration (Acct-Session-Time)
12	Disconnect Cause Code	The SIP caused code for a disconnected call (h323-disconnect-cause)
13	Incoming Leg Setup Time	incoming call leg INVITE received time (h323-setup-time)
14	Outgoing Leg Setup Time	outgoing call leg INVITE sending time (outgoing-setup-time)
15	Call Alerting Time	Call alerting (ring) time (call-alert-time)
16	Call Connected Time	Call connected time (h323-connect-time)
17	Call Disconnect Time	Call disconnect time (h323-disconnect-time)
18	SIP Call ID	SIP call ID which can be used for call tracking. It will be the same for a whole call. (call-id)
19	Forward Count	call forward count (0 means no forward, 1 means first forward and so on) (h323-disconnect-time)
20	Calling Public IP	calling device's public IP address (call-origin-endpt)
21	Called Pubic IP	called devices' public IP address (h323-remote-address)
22	Original Called Number	The original called number before any digit manipulation (gw-rxd-cdn)
23	Incoming SIP URI	incoming call leg SIP request URI(incoming-req-uri)
24	Outgoing SIP URI	outgoing call leg SIP request URI (outgoing-req-uri)
25	PBX Call Type	0: extension to extension calls, 1: extension outgoing calls 2: extension incoming calls, 3: others

Field Index	Field Name	Description
26	IP Type	0: IPv4 o IPV4 calls, 1: IPv4 to IPV6 calls 2: IPv6 to IPv4 calls, 3: IPv6 to IPV6 calls
27	Additional Parameters	reserved

If you have turned on enhanced CDR, you will have more fields to descript the quality of calls as follows:

Field Index	Field Name	Description
27	RTP Audio Status	-1: no RTP receive, 0:both voices, 1: one way voice from caller, 2: one way voice from called
28	RTP Video Status	-1: no RTP receive, 0:both video, 1: one way video from caller, 2: one way video from called
29	Negotiated Audio Payload	payload type negotiated
30	Negotiated Audio Ptime	payload size time from SDP
31	Caller Audio Packet Count	Caller Audio Packet Count
32	Caller Audio Octet Count	Caller Audio Octet Count
33	Caller Audio Payload Size	Caller Audio Payload Size
34	Caller Audio Lost Packets	Caller Audio Lost Packets
35	Caller Audio Mean Jitter	Caller Audio Mean Jitter
36	Caller Audio lost Rate	Caller Audio lost Rate
37	Caller Peak Jitter	Caller Peak Jitter
38	Called Audio Packet Count	Called Audio Packet Count

Field Index	Field Name	Description
39	Called Audio Octet Count	Called Audio Octet Count
40	Called Audio Payload size	Called Audio Payload size
41	Called Audio Lost Packets	Called Audio Lost Packets
42	Called Audio Mean Jitter	Called Audio Mean Jitter
43	Called Audio lost Rate	Called Audio lost Rate
44	Called Peak Audio Jitter	Called Peak Audio Jitter
45	Negotiated Video Payload	Negotiated Video Payload
46	Negotiated Video Ptime	Negotiated Video Ptime
47	Caller Video Packet Count	Negotiated Video Ptime
48	Caller Video Octet Count	Caller Video Octet Count
49	Caller Video Payload Size	Caller Video Payload Size
50	Caller Video Lost Packets	Caller Video Lost Packets
51	Caller Video Mean Jitter	Caller Video Mean Jitter
52	Caller Video lost Rate	Caller Video lost Rate
53	Caller Peak Video Jitter	Caller Peak Video Jitter
54	Called Video Packet Count	Called Video Packet Count
55	Called Video	Called Video Octet Count

Field Index	Field Name	Description
	Octet Count	
56	Called Video Payload size	Called Video Payload size
57	Called Video Lost Packets	Called Video Payload size
58	Called Video Mean Jitter	Called Video Payload size
59	Called Video lost Rate	Called Video Payload size
60	Called Peak Video Jitter	Called Video Payload size
61	Additional Parameters	

5.4 System Alert List

The system provides the following system alerting notice to email or syslogd server.

Module	Level	Event
SIP	CRITICAL	Stopping SIP communication Service: (failed to create required transaction)
SIP	CRITICAL	Stopping SIP communication Service: (failed to create required call handler)
SIP	CRITICAL	Failed to start SIP communication service: (Failed to connect to database to load initial parameters)
SIP	CRITICAL	Failed to start SIP communication service: (Failed to initialize SIP stack)
SIP	WARN	The IP x.x.x.x(User-Agent) has been blocked temporarily.
SIP	WARN	NAT resource service WARNING: (failed to get NAT resource)
SIP	WARN	User ID: xxx is making a black list call

Module	Level	Event
SIP	NOTICE	The IP x.x.x.x has been removed from blocking IP list.
SIP	NOTICE	SIP communication service NOTICE: (database connection resumed)
SIP	NOTICE	01:35:47 (Registered) Extension: xxxx was registered from x.x.x.x:5060 (x.x.x.x:5060)
SIP	NOTICE	SIP communication service NOTICE: (service started)
SIP	INFO	User ID: XXX call attempt had over the max concurrent calls
SIP	INFO	Loop Detected: Calling: xxx from (x.x.x.x) to Called: xxx
SIP	INFO	Changes applied to the running system
RTP	NOTICE	Failed to create required sockets port=xxx
RTP	NOTICE	NAT resource service NOTICE: (service(v120206) started)
RTP	INFO	Changes applied to the running system
RADIUS	WARN	Failed to start RADIUS service: (failed to bind required sockets port:xxx)
RADIUS	WARN	Failed to start RADIUS service: (failed to get initial parameters to start)
RADIUS	NOTICE	RADIUS service NOTICE: (service started)
RADIUS	INFO	Changes applied to the running system
RADIUS	WARN	Failed to receive response from RADIUS Server [xxx.xxx.xxx.xxx].
RADIUS	NOTICE	Received RADIUS response from Server [xxx.xxx.xxx.xxx]
HA	CRITICAL	This node is set to STANDBY mode by administrator. You need activate it manually to rejoin the HA cluster.
HA	CRITICAL	This node is failed-over to standby node (A/A mode). Please check the system and reactive it.
HA	CRITICAL	This node is failed-over to standby node (A/S mode) and the system will start tried to clean-up.
HA	CRITICAL	Resetting this node, because of no available note can be failed over.

Module	Level	Event
HA	WARN	HA Group 1 stopped at xxx
HA	NOTICE	This node is set to ON-LINE by administrator.
HA	NOTICE	HA Group 1 started at xxx (xxx is hostname)

5.5 Digit Manipulation Example

This appendix includes some digit manipulation examples for reference. Assumed that the following is the digit manipulation defined in the system.

Group ID	Pilot Number	Incoming Number Type	Applied Number Type	Length	Applied Ext. Target	Start Position	Stop Position	Replace Value	Description
1	0	DNIS	DNIS	0	caller	0	0	002	Insert 002 in DNIS when leading digit is 0
2	0	DNIS	DNIS	10	caller	0	0	009	Insert 009 to DNIS if DNIS leading digits is 0 and length is equal 10
3	002	DNIS	DNIS	0	caller	0	3	886	Remove leading 3 digits and add 886 in DNIS when leading digit is 002.
4	1	ANI	ANI	4	caller	32	32	0001	Append 0001 for ANI when ANI's leading digit is 1 and length is 4.
5	2	DNIS	DNIS	0	caller	3	3	008	Insert 008 after third digits when DNIS's leading digit is 2
6	3	ANI	ANI	0	called	0	0	+0	Add +0 for ANI when called to this extension and ANI's leading digit is 3
7	009	DNIS	DNIS	0	called	0	1	+	Remove leading 1 digits and add + in front of DNIS when DNIS's leading digit is 009.

Group ID	Pilot Number	Incoming Number Type	Applied Number Type	Length	Applied Ext. Target	Start Position	Stop Position	Replace Value	Description
8	5	ANI	DNIS	4	caller	3	5	00	Change 4th to 5th digit to 00 for DNIS when ANI's leading digit is 5 and length is 4.

Here comes the digit manipulation result based on the above digit manipulation rules.

Calling Number (ANI)	Called Number (DNIS)	ANI Applied DM Group ID	DNIS Applied DM Group ID	ANI After DM	DNIS After DM
2001	0886232342663	n/a	1	2001	0020886232342663
1001	0232342663	4	2	10010001	0090232342663
1001	002232342663	4	3	10010001	886232342663
3001	2113	6	5	+03001	2110083
3001	4001	6	n/a	+03001	4001
4001	009886232342663	n/a	7	4001	+009886232342663
5001	32342663	n/a	8	5001	32340063

5.6 Outgoing Scrrening Policy

When the system had both outgoing call screening group based on the feature's setting and the personal screening are specified, the personal outgoing screening setting got higher priority to run if they are conflict. The following is the example to explain it.

Case 1:

Assumed the following outgoing call screening group setting are assigned to extension 1001.

Pilot Number	Screening Type
002	block

Pilot Number	Screening Type
0204	block

Extension 1001 had the following personal outgoing call screening group:

Personal Pilot Number	Personal Screening Type
00286	unblock

The following is the calling example and result

Called Number	Result
002132342663	block the call
00286123456	allow to call
0091234567	allow to call
0204123456	block the call
12345678	allow to call

Case 2:

Assumed the following outgoing call screening group setting are assigned to extension 1002.

Pilot Number	Screening Type
002	unblock
0204	unblock

Extension 1001 had the following personal outgoing call screening group:

Personal Pilot Number	Personal Screening Type
009	unblock

The following is the calling example and result

Called Number	Result
002132342663	allow to call
00286123456	allow to call
0091234567	allow to call
0204123456	allow to call
12345678	block the call

Case 3:

Assumed the following outgoing call screening group setting are assigned to extension 1003.

Pilot Number	Screening Type
002	block
0204	block
0021	unblock

Extension 1001 had the following personal outgoing call screening group:

Personal Pilot Number	Personal Screening Type
00286	unblock

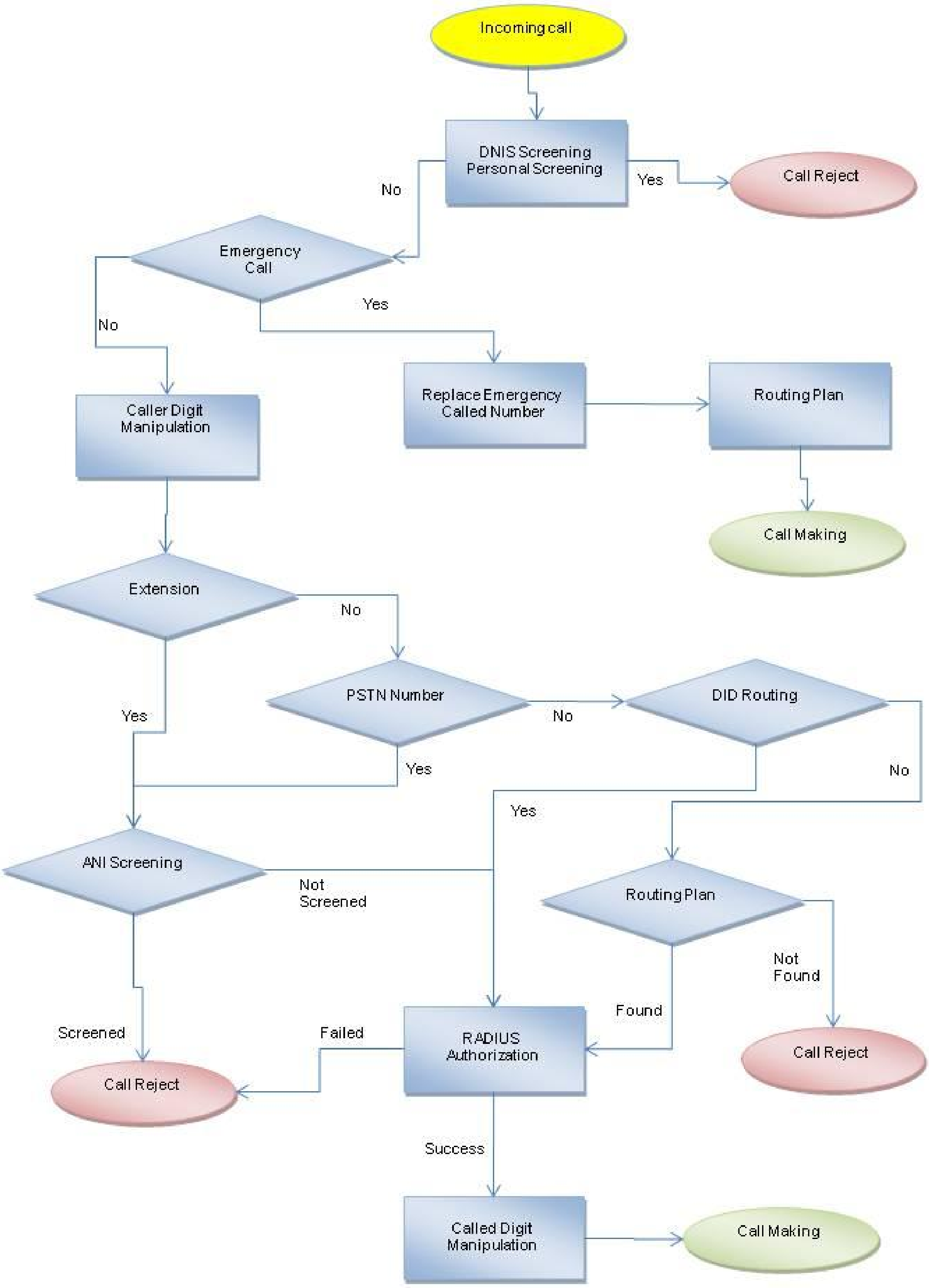
The following is the calling example and result

Called Number	Result
002132342663	allow to call
00286123456	allow to call
0091234567	block the call
0204123456	block the call
12345678	block the call

Although the system provides very flexible outgoing screening block feature, it is recommend to only use block or unblock only, not both, in order to keep the screening easy to be predicted.

5.7 Call Processing Policy

The system call processing policy helps administrator to understand the handling procedure on system point of view.



Incoming call
DNIS Screening
Personal Screening
Yes
Call Reject
No
Emergency
Call
Yes
No
Replace Emergency
Called Number
Routing Plan
Caller Digit
Manipulation
Call Making
Extension
No
PSTN Number
No
DID Routing
Yes
Yes
No
Yes
ANI Screening
Not
Screened
Routing Plan
Not
Found
Found
Screened
Failed
RADIUS
Authorization
Call Reject
Call Reject
Success
Called Digit
Manipulation
Call Making

5.8 Extension Import Description

The appendix is described the imported CSV file format. The tab is used to be used as a separator.

The following is the field description for extension.

[SIPPD_UserM]

Field Index	DB Field Name	Description
1	UGroup_ID	Extension Group ID
2	User_ID	Extension Number
3	Active_Fg	Enable or disable the extension (0: Disable, 1:Enable)
4	Screen_GID	Outgoing call screening ID (-1: none)
5	Password	User password
6	Device_Type	Extension Type (0: Phone/ATA, 1: FXO/Trunk/ Proxy, 2:SIP Trunk, 3: Voice Mail Server)
7	Register_Type	Contact Policy (0: register, 1:Permanent Contact 2:Permanent Contact/NAT)
8	Enabled_Servi ce	Service Bit Mask, each bit indicate the following service (0: disable, 1:enable) 0: personal incoming call screening 1. personal outgoing call screening 2. Enable/Disable Call Forward Always 3. Enable/Disable Call Forward No Answer 4. Enable/Disable Call Forward Busy 5. Enable/Disable Call Forward Unavailable 6. Enable/Disable Fine Me 7. Enable/Disable Do Not Disturb 8. Enable/Disable Email Missed Call 9. Enable/Disable Allow Group Pickup 10. Enable/Disable Allow Global Any Pickup 11. Enable/Disable Response to Sending Port (UDP port) 12. Reserved (set to 0) 13. Follow Me Hunting First

Field Index	DB Field Name	Description
		14. Hunting Extension 15. Send 181 before Start Forward 16. set SIP TO as request URI 17. Enable/Disable VMS 18. Enable/Disable "Disable Authentication qop tag" 19. Enable/Disable Anonymous Call Blocking 21. Enable/Disable Privilege Access 22. Monitor Register Status
9	First_ResponseT	SIP Request Response Timer (sec)
10	No_Ans_Timer	No Answer Time Out (sec)
11	RTP_Proxy	NAT Traversal (0:Automatic Traversal, 1: Always ON, 2: Always OFF)
12	Auth_mode	SIP Security (0: Register Only, 1:Register Invite)
13	Authority_Mode	RADIUS Authorization (0: No - RADIUS is not used, 1: Yes - RADIUS authorization is ON)
14	Hunting_Method	Parallel Hunting (0: disable parallel hunting, 1:enable parallel hunting)
15	CallID_Mode	Block Caller ID (0: Not block caller ID, 1: block caller ID)
16	Predefine_URI	Permanent Contact 1
17	Predefine_URI2	Permanent Contact 2
18	Uncond_URI	Forward Number for Call Forward Always
19	NoAns_URI	Forward Number for Call Forward No Answer
20	Busy_URI	Forward Number for Call Forward Busy
21	UnAval_URI	Forward Number for Call Forward Unavailable
22	Max_RegTime	Default Register TTL (sec)
23	Max_NATRegTime	NAT Register TTL (sec)
24	Locate_URI1	Follow Me's follow number for time period 1

Field Index	DB Field Name	Description
25	Locate_T1	Follow Me time period 1 (format: hhmm-hhmm)
26	Locate_URI2	Follow Me's follow number for time period 2
27	Locate_T2	Follow Me time period 2 (format: hhmm-hhmm)
28	Locate_URI3	Follow Me's follow number for time period 3
29	Locate_T3	Follow Me time period 3 (format: hhmm-hhmm)
30	Locate_URI4	Follow Me's follow number for time period 4
31	Locate_T4	Follow Me time period 4 (format: hhmm-hhmm)
32	Locate_URI5	Follow Me's follow number for time period 5
33	Locate_T5	Follow Me time period 5 (format: hhmm-hhmm)
34	DoNot_Distrib T1	DND time period 1 (format: hhmm-hhmm)
35	DoNot_Distrib T2	DND time period 2 (format: hhmm-hhmm)
36	Replace_ANI	Secondary PSTN Number
37	Replace_Type	reserved (always set to 1)
38	Miss_Call_URI	Email address of Missed Call (also it is owner's email address)
39	UAC_ID	SIP Trunk ID (only available for SIP trunk extension type)
40	Max_Contact	Max Contacts Support (1-5)
41	Emg_GID	Emergency Call Group ID (-1: none)
42	Web_Password	Web password
43	Login_ID	SIP User ID
44	Display_Name	SIP Display Name
45	Pickup_GID	Pickup Group ID (-1: none)
46	Transport_Type1	Permanent contact address 1 transportation address 0: WAN/UDP Port 1 1: WAN/UDP port 2

Field Index	DB Field Name	Description
		2: WAN/UDP port 3 3: LAN/UDP port 1 4: LAN/UDP port 2 5. LAN/UDP port 3 6. IPV6 UDP port 7. TCP Port 8. TLS Port
47	Transport_Type2	Permanent contact address 2 transportation address, refer to Transport_type1
48	Device_1	Dedicate Device 1
49	Device_2	Dedicate Device 2
50	Call_Validation	Session Validation method (0: None, 1: Update, 2: Invite, 3: Use Global Setting)
51	Max_Call	reserved (set to 0 always)
52	Description	Description of this extension
53	Over_Max_Contact_Rule	Contact Update Method (0: Use Global Setting, 1: Deny 2: Update)
54	AAA_Sending_Stage	reserved (set to 0)
55	Enabled_Service_Mask	reserved (set to 2147483647)
56	F_User_Name	Extension Owner's Name
57	F_Mobile	Extension Owner's Mobile
58	F_Contact_tel	Extension Owner's Telephone number
59	F_Address	Extension Owner's Address

The following is for personal incoming and outgoing call screening.

[SIPPD_Screening]

Field Index	DB Field Name	Description
1	User_ID	Extension Number

Field Index	DB Field Name	Description
2	Screen_Prefix	Pilot Number
3	Screen_Target	Blocking Target (0: incoming call, 1:outgoing call)
4	Screen_Type	Blocking Type (0: Block, 1:Unblock, 2: Privilege Access)

5.9 List of Used Network Ports

The following is the list of used TCP/IP ports. The network administrator can use it to set the firewall when necessary.

Default Ports	Protocol	Description	Configuration Path
5060	UDP	SIP UDP service port	SYSTEM -> SIP Service -> UDP Service Port 1
8080	UDP	SIP UDP service port	SYSTEM -> SIP Service -> UDP Service Port 2
n/a	UDP	SIP UDP service port	SYSTEM -> SIP Service -> UDP Service Port 3
n/a	UDP	SIP IPV6 UDP service port	SYSTEM -> SIP Service -> IPV6 UDP Service Port
7070	UDP	AAVMS UDP SIP Port	SYSTEM -> VMS Settings -> Local SIP UDP Port
7072	UDP	AAVMS UDP IPV6 SIP Port	SYSTEM -> VMS Settings -> Local IPV6 SIP UDP Port :
1810	UDP	RADIUS local port	SYSTEM -> RADIUS -> Local RADIUS Binding Port
20000-39999	UDP	NAT Resource Port	These ports are used based on interval of 10. The n-th NAT resource will use the port from 20000+10*n to 20000+10*n+3, total 4 UDP ports. For example, the 9-th port will use ports from 20090 to 20093.
10000-19999	UDP	AA/VMS RTP port	These ports are used based on interval of 10. The n-th AA/VMS resource will use the port from 10000+4*n to 10000+4*n+3, total 4 UDP ports.

			SYSTEM -> VMS Settings -> Local Media UDP Start Port
694	UDP	HA heartbeat broadcasting port	SYSTEM -> High Available -> Cluster Service Port
5060	TCP	SIP TCP service port	SYSTEM -> SIP Service -> TCP Service Port
5061	TCP	SIP TLS service port	SYSTEM -> SIP Service -> TLS Service Port
9200	TCP	HTTP port for administrator	SYSTEM -> WEB Service -> HTTP Service Port -> Administrator Only be opened in firewall when necessary.
9201	TCP	HTTPS port for administrator	SYSTEM -> WEB Service -> HTTPS Service Port -> Administrator Only be opened in firewall when necessary.
80	TCP	HTTP port for extension user	SYSTEM -> WEB Service -> HTTP Service Port -> Extension Only be opened in firewall when necessary.
443	TCP	HTTPS port for extension user	SYSTEM -> WEB Service -> HTTPS Service Port -> Extension Only be opened in firewall when necessary.
8080	TCP	SOAP Provisioning Port	SYSTEM -> Web Service -> SOAP Service Port Only be opened in firewall when necessary.
514	TCP	Log Service Port	none
3306	TCP	MYSQL Service Port	SYSTEM-> Database -> MYSQL Port

5.10 Debug Logging

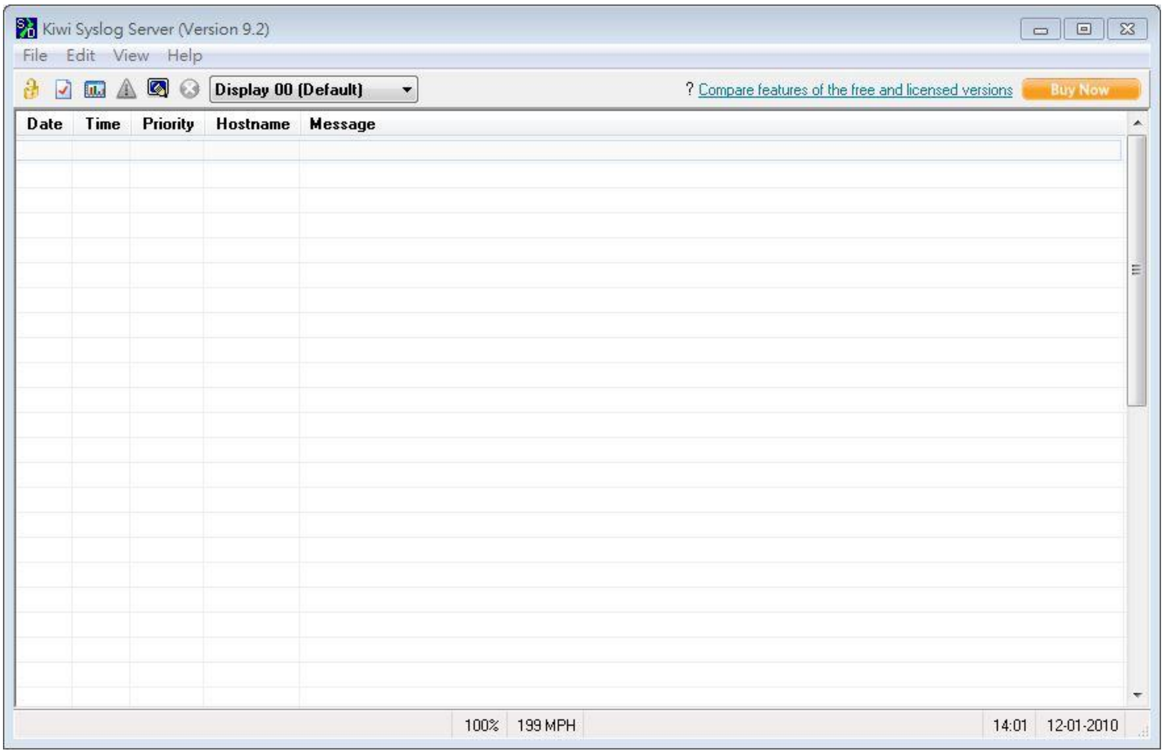
This appendix descript the step by step of debug information logging for troubleshooting as follows:

Step 1: Create a directory in C:\logs will be used for log file.

Step 2: Download the free version of kiwi syslog server from http://www.kiwisyslog.com

Step 3: Install it on your computer as a stand along application

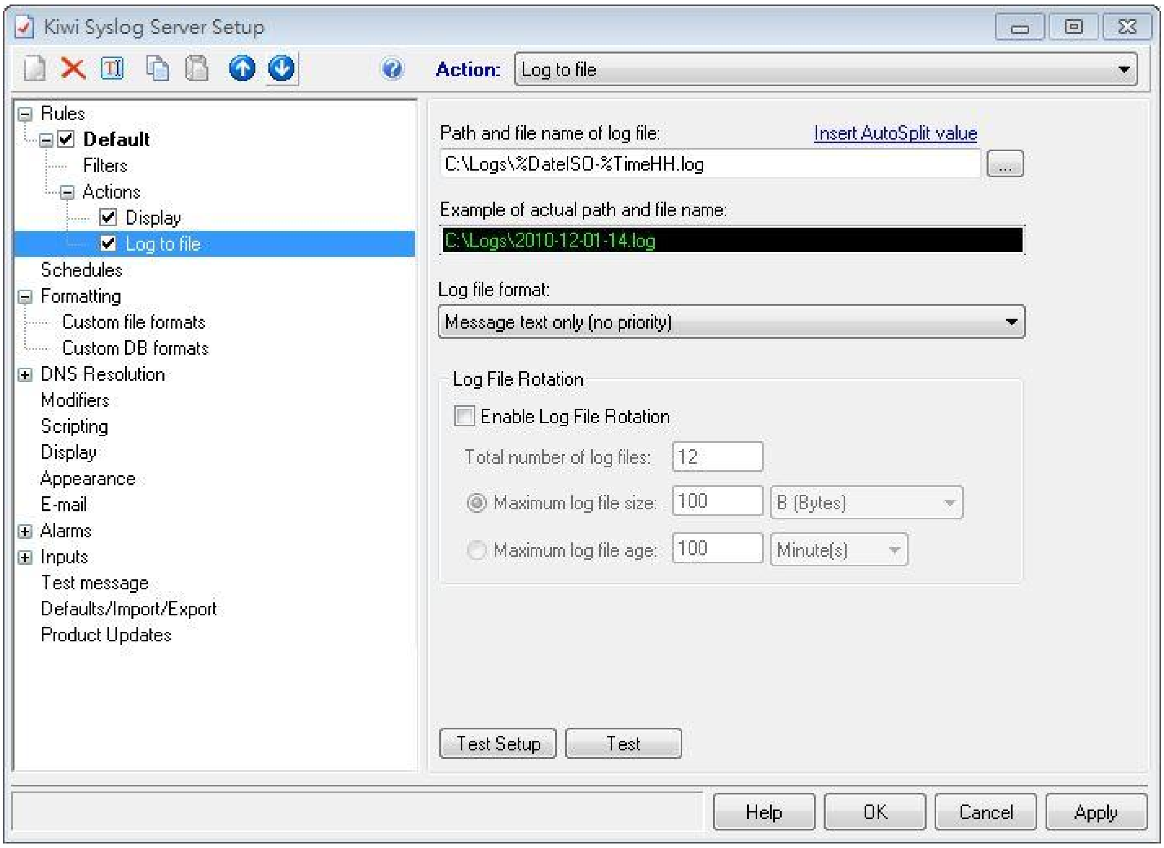
Step 4: Start up the Kiwi Syslog Server, you will see the following main screen:



Step 5: Click ***File -> Setup*** and you should see the setup screen. Do the following settings:

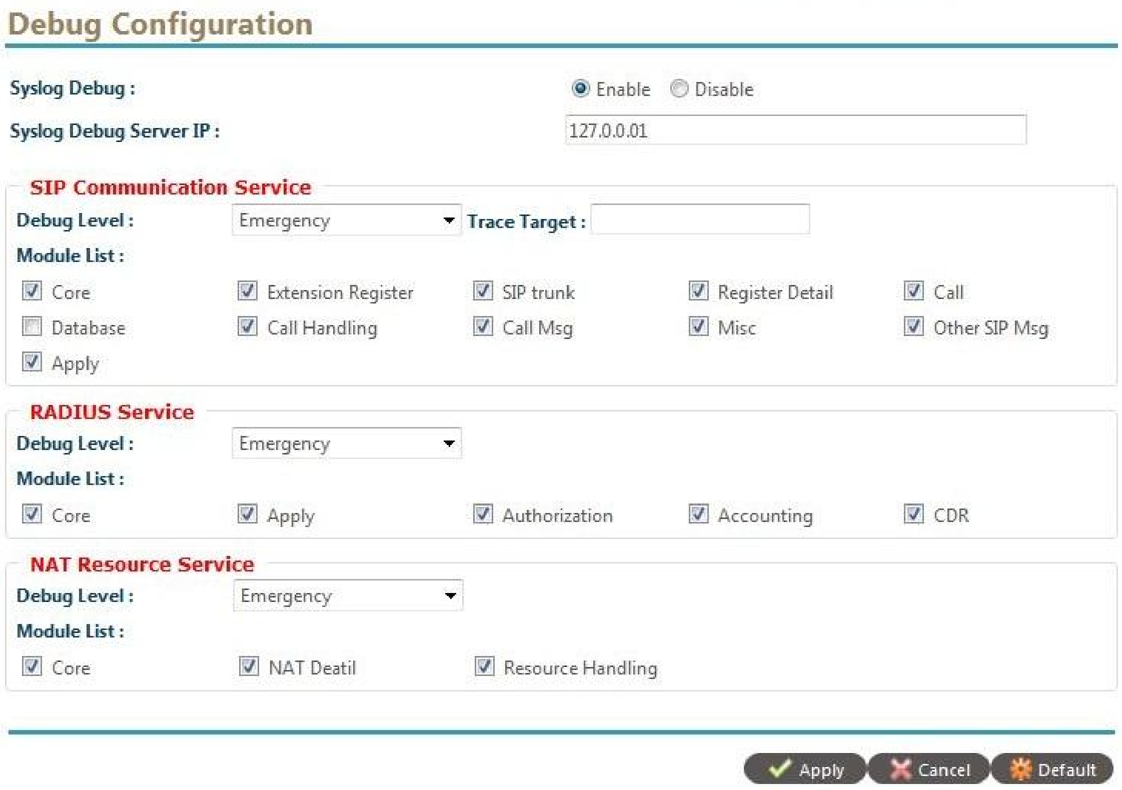
1. Choose Rules -> Default -> Actions ->Log to file to change
   - Path and file name of log file to "C:\Logs\l%DateISO-%TimeHH.log"
   - Log file format: Message Text Only (no priority)
   - Click Apply and OK

After this settings, you will able to see your log file in c:\Logs directory.



Step 6: Right click in main windows and select Show/High columns, uncheck all items except 'message'.

Step 7: Login to the system and click SYSTEM -> Debug. The following screen will display.



Change the following:

Syslog Debug: Enable

Syslog Debug Serve IP: xxx.xxx.xxx.xxx (IP address you have installed syslog server)

Change the required module's debug level to "Debug"

Check the required module list for debug.

Click Apply to save it.

Step 9: Click COMMIT to start the syslog sending and start your testing.

Step 10: You should able to see the debug log in the kiwi syslog screen. And the hourly log file can be found in the C:\logs or the directory you set. The file name will be YYYY-MM-DD-HH.log.

Step 11: Send the log and problem and environment description to supporting FAE.