Ezvoicetek
www.ezvoicetek.com

EZWEBPHONER-8200 WebRTC Phone Server Administrative Guide

Release 1.1 Mar. 2018

About EzVoiceTek

Ezvoicetek 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 Ezvoicetek solutions are provided to support both IPV4 and IPV6 dual stack simultaneously. We provides a painless migration path from IPV4 to IPV6 network.

EzVoiceTek Co., Ltd.
1F., No.16, Ln. 257, Yuantong Rd., Zhonghe Dist.,
New Taipei City 235, Taiwan (R.O.C.)
WEB: www.ezvoicetek.com
EMAIL: sales@ezvoicetek.com

Technical Support
Email: support@ezvoicetek.com

Copyright Notice and Disclaimer

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of Ezvoicetek.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. Ezvoicetek make no claim to these trademarks.

EzVoiceTek Co., Ltd. (EzVoiceTek) makes no representations or warranties with respect to the contents hereof. In addition, information contained herein are subject to change without notice. Every precaution has been taken in the preparation of this manual. Nevertheless, EzVoiceTek assumes no responsibility for errors or omissions or any damages resulting from the use of the information contained in this publication..

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 address to access GUI management interface by using popular browser such as Internet Explorer, Chrome or Firefox.

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 system.

Start the browse, and type http://xxx.xxx.xxx.xxx:8200 or https://xxx.xxx.xxx.xxx:8201 to login web manage where xxx.xxx.xxx.xxx is the IP address of the server.

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 Change Service Parameter Settings

The next step is to set the Service Parameters for working with SIP Proxy server or IP-PBX. Click ***SYSTEM -> Service Parameters*** and the following screen will appear.

Change the following parameters:

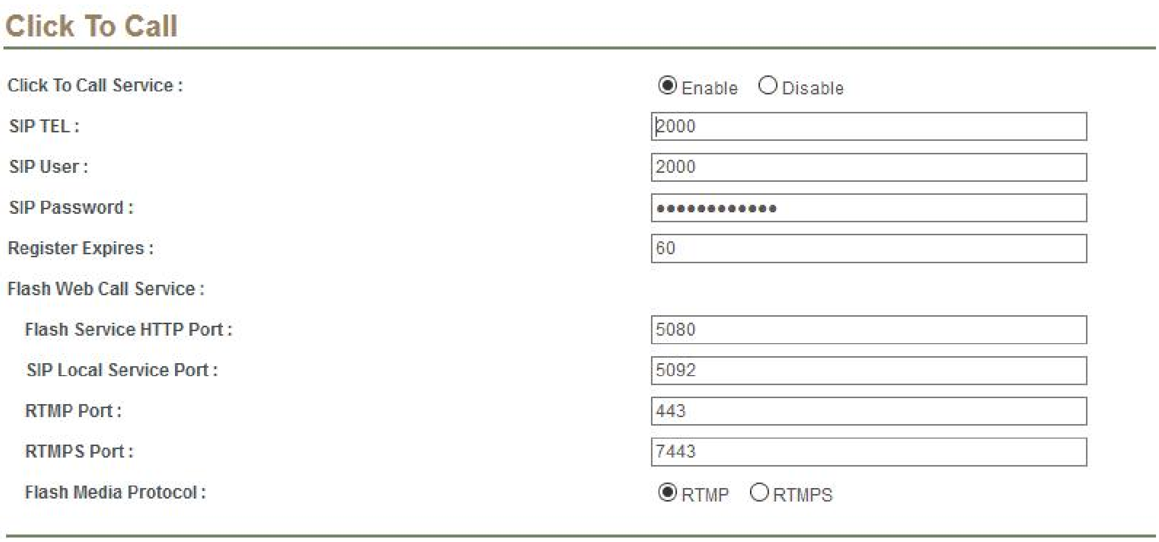
Parameter Name	Value
SIP Proxy Domain	SIP domain getting from SIP proxy or IP-PBX
SIP Proxy IP	SIP proxy IP

Parameter Name	Value
SIP Proxy Server UDP Port	SIP proxy IP UDP service port
Attached Network Interface	The Interface will be in binding for the WebRTC service
Using Secure Websocket	Whether use WSS (secure websocket) URL or not? It is recommended to enable in order to have browser to remember the mic phone or video permission. When it is enabled, it is need to use https instead of http to maximum the security protection.
Server Certificate	You need to use a real certificate (not self-signed certificate) because of the browser requirement. The certificate need dedicate for this server's domain or domain name.
Certificate Key	The private key file (unencrypted) together with the certificate.

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

1.4 Click to Call Settings

If the system has click to call license, you need create an account on SIP proxy server or IP-PBX and assigned here in order to use it. Click SYSTEM -> Click to Call and the following will appear:



Change the following values:

Parameter Name	Value
Click to Call Service	Enable
SIPTel	SIP Proxy or IP-PBX account number
SIP User	SIP User for authentication
SIP Password	SIP Password for authentication

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

1.5 Restart Service

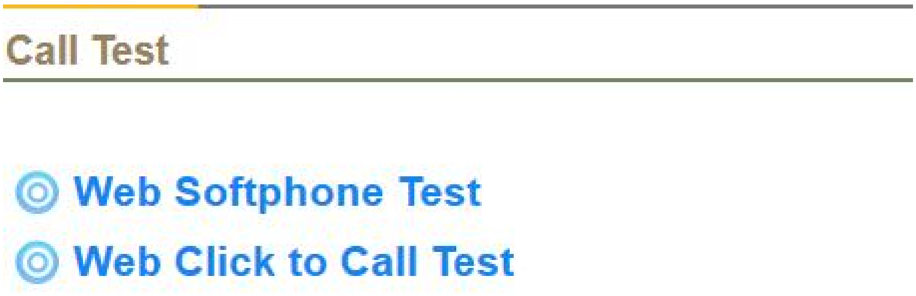
Before you can start the call test, you need restart the service in order to make sure your setting is taking effective.

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

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

1.6 Call Test

Click ***Diagnostic -> Call Test*** and the following will appear:



Click **Web Softphone Test** to test Webrtc feature
Click **Web Click to Call test** to test Click to Call features

2 Using the System

The administrator can logon the web GUI interface to manage the system service. It provides the service provisioning, real time system status monitor and system statistic report. The default login URL for administrator login is http://xxx.xxx.xxx.xxx:8200 or https://xxx.xxx.xxx.xxx:8201 and default login id is "admin" and password is "admin".

2.1 Home

The home page 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
Web Release	The current running web release

2.2 System

The system parameters including the Service, SIPTimer, system and license settings. Click the SYSTEM and will see the setting in the left panel as follows. Select the setting you need in left panel.

2.2.1 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:

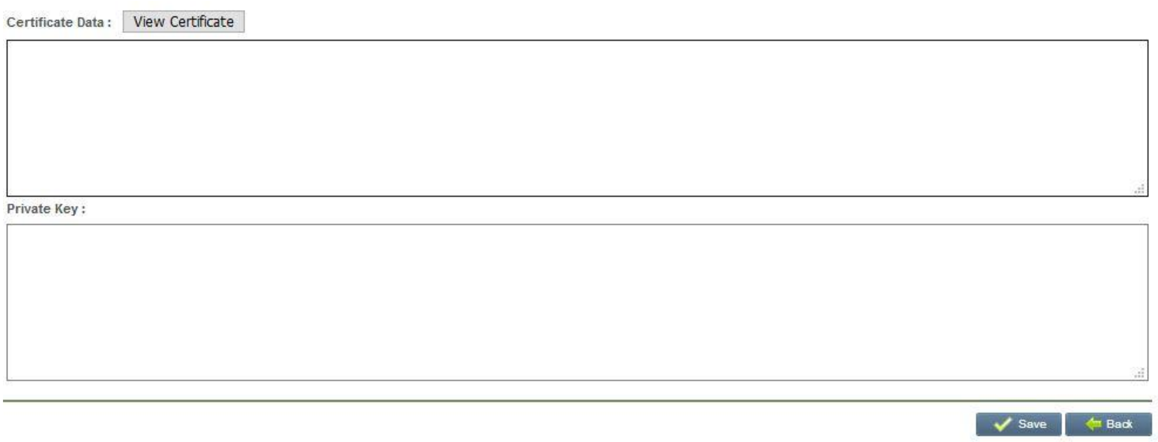
Parameter Name	Description
SIP Local Service Port	Local UDP port for SIP Service.
SIP Proxy Domain	The SIP Proxy server's domain name will be connected to.
SIP Proxy Server IP	The SIP Proxy Server IP Address

Parameter Name	Description
SIP Proxy Server UDP Port	The SIP Proxy Server UDP service port
Attached Network Interface	The attached Ethernet IP for the service
Media Starting Port	The media starting UDP port based on interval 20. For example, the system can support up-to 10 calls, it will required 200 (20*10) port reserved.
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 Timeout	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
Using Secure Websocket	Whether enable WSS (secure websocket) or not?
Server Certificate	The purchased server specified certificate. An self signed certificate is not accepted by most of browser.
Certificate Key	The private key file purchased (not encrypted format)
CDR keeping Days	How long the calling history will be kept for click to call service?
Behind NAT Mapped IP	If the system is seating behind a NAT server and would like to provide the service for those external Internet user with a IP mapped public address. This is the public IP address setup on NAT server to map to the system.
Phone Book URL	The system was fully integrated with our own IPPBX or VMS service. The extension just need input their own phone book and make it into a group. Then it could be access by webrtc softphone by using the Phone Book URL. You can input your phone book URL as the following format: https://XXX.XXX.XXX.XXX:9201/getpbook.jsp Normally, it is required to use https because of mixing https and http might not be allowed by the browser.

Parameter Name	Description
Video Call Resolution	The WebRTC video call resolution

2.2.1.1 WSS Certificate

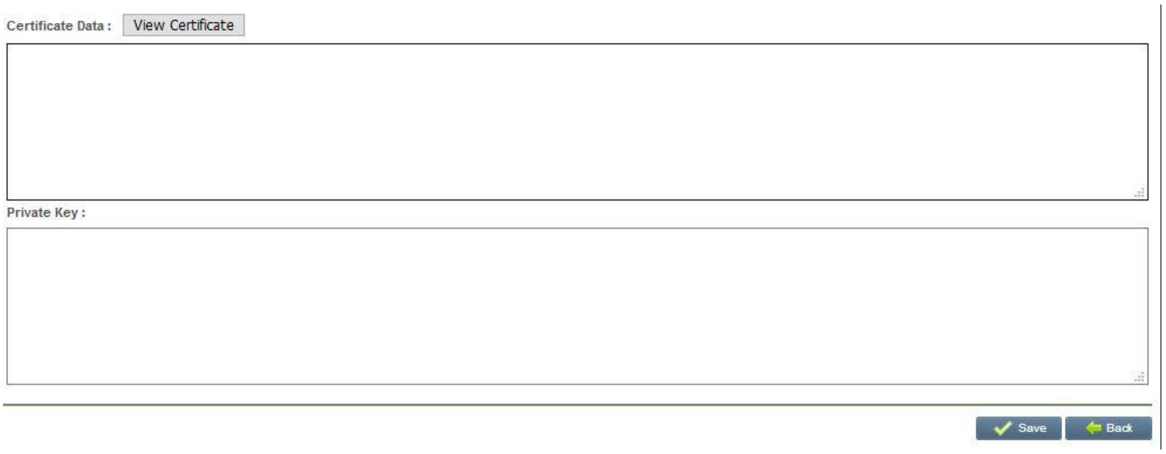
This is the place to configure secure websocket certificate. You might need to get the certificate from a supplier. Click Websocket Certificate and the following will appear:



Paste the purchased SSL certificate into the Certificate Data column and you can use view Certificate to check whether it is a correct certificate or not.
Paste the purchased SSL key into Private Key column and Click Save to make system need HTTPS SSL.

2.2.1.2 DTLS Certificate

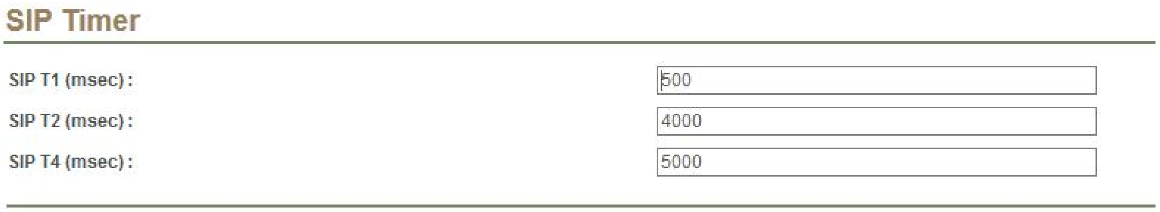
This is the place to configure secure DTLS certificate. You might need to get the certificate from a supplier. Click DTLS Certificate and the following will appear:



Paste the purchased SSL certificate into the Certificate Data column and you can use view Certificate to check whether it is a correct certificate or not.
Paste the purchased SSL key into Private Key column and Click Save to make system need HTTPS SSL.

2.2.2 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.

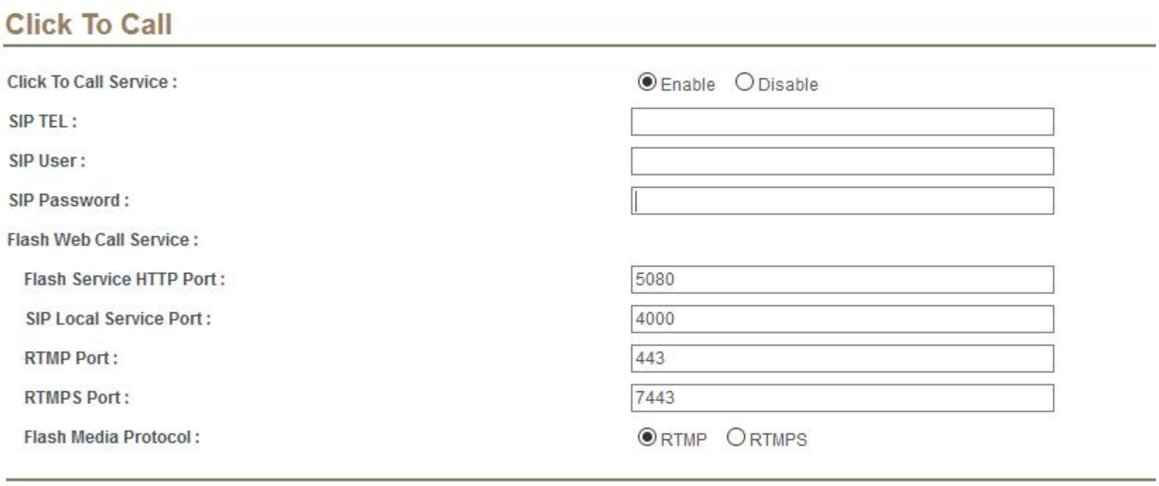


The detail of each parameter is described as below:

Parameter Name	Description
SIP 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.

2.2.3 Click to Call

The click to call service providing click to call on customer web. It support Flash + Webrtc auto detect and can be ran on any browsers which support Flash or Webrtc. Click ***SYSTEM -> Click to Call*** to view and change the settings.



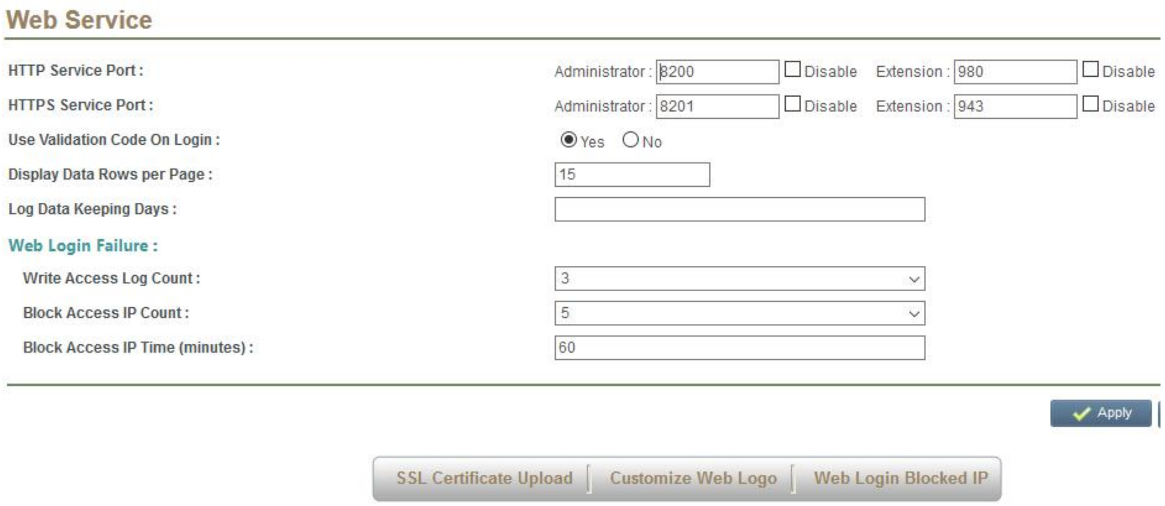
The detail of each parameter is described as below:

Parameter Name	Description
Click To Call Service	Whether enable click to call service or not?
SIP TEL	SIP account telephone number
SIP User	SIP account user id for authentication
SIP Password	SIP account password for authentication
Flash Web Call Service	The following parameters are based on the Flash based web call
Flash Service HTTP Port	Click to call's web service port
SIP Local Service Port	Starting port of SIP local service port. It will require local service port + license * 2 as a range.
RTMP Port	The flash used RTMP service port
RTMPS Port	The flash used RTMPS service port

Parameter Name	Description
Flash Media Protocol	The protocol will be used for flash media. It can be RTMP or RTMPS. RTMPS is based TLS.

2.2.4 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 login is 8200. The default value for extension login is 980.
HTTPS Service Port	The TCP service port for HTTPS (SSL) web GUI management. The default value for administrator login is 8201. The default value for extesnion SSL login is 943.
Display Data Rows per Page	Number of data rows will be displayed per page. The default is 15.
Log Data Keeping Days	How long in days that the system will keep the log data in the system.
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.

Parameter Name	Description
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 ***Web Login Blocked IP*** is able to view the current blocked IP and unlock if necessary as follows:

Parameter Name	Description
Blocked IP	The IP was blocked because of failed login
Login ID	The ID was tried for the failed login
Login time	The time was blocked
Time to unblock	The time will be unblocked

2.2.4.1 SSL Certificate

This is the place to configure secure HTTPS used SSL certificate. You might need to get the certificate from a supplier. Click SSL Certificate and the following will appear:

Paste the purchased SSL certificate into the Certificate Data column and you can use view Certificate to check whether it is a correct certificate or not.
Paste the purchased SSL bundle certificate CA data into Bundle CA column.
Paste the purchased SSL key into Private Key column and Click Save to make system need HTTPS SSL.

2.2.4.2 Customize Logo

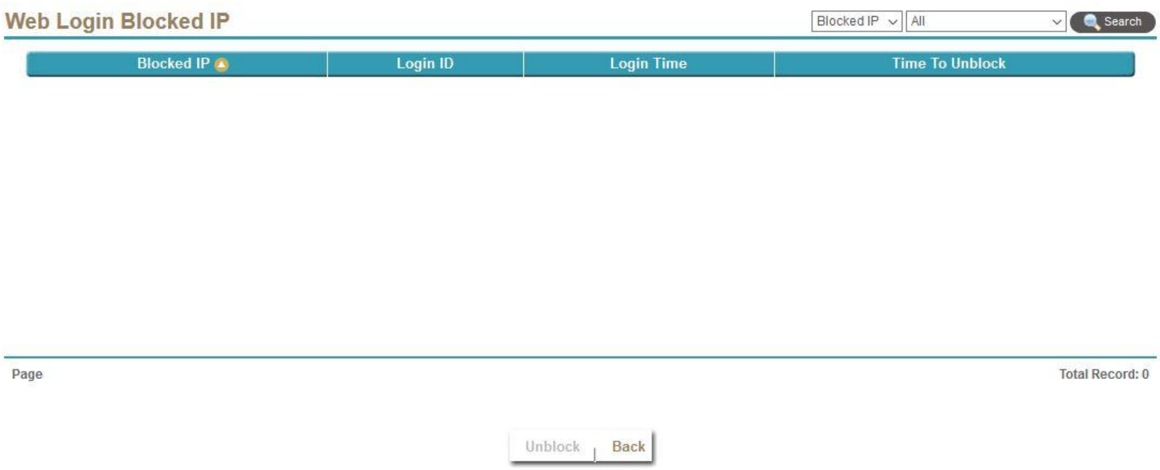
The administrator can change the customized logo as following:

Company Logo is a png format file which contains company name. The recommend resolution is around 180*60
Product Name Image File is a png format file which contains products name. The recommend resolution is around 500*40
Product Version Image File is a png format file which contains product ID or version.

It will be following after Product Name Image. The recommended resolution is around 150*20

2.2.4.3 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:

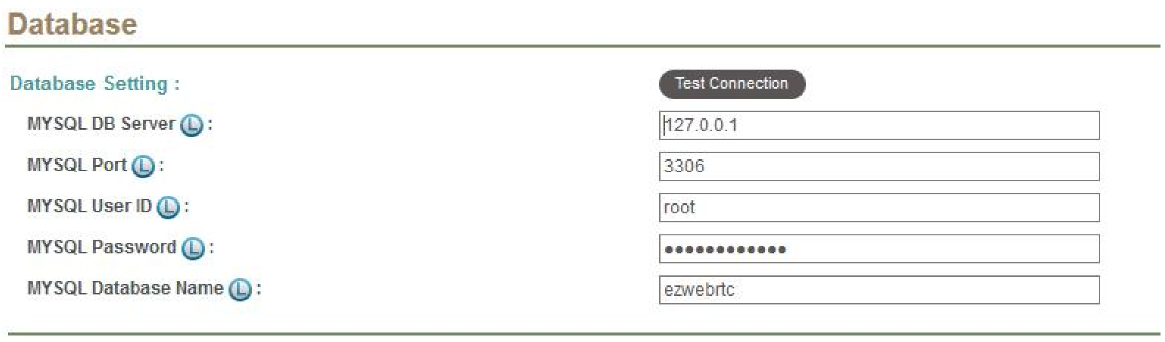


The detail of each parameter is described as below:

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

2.2.5 Database

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

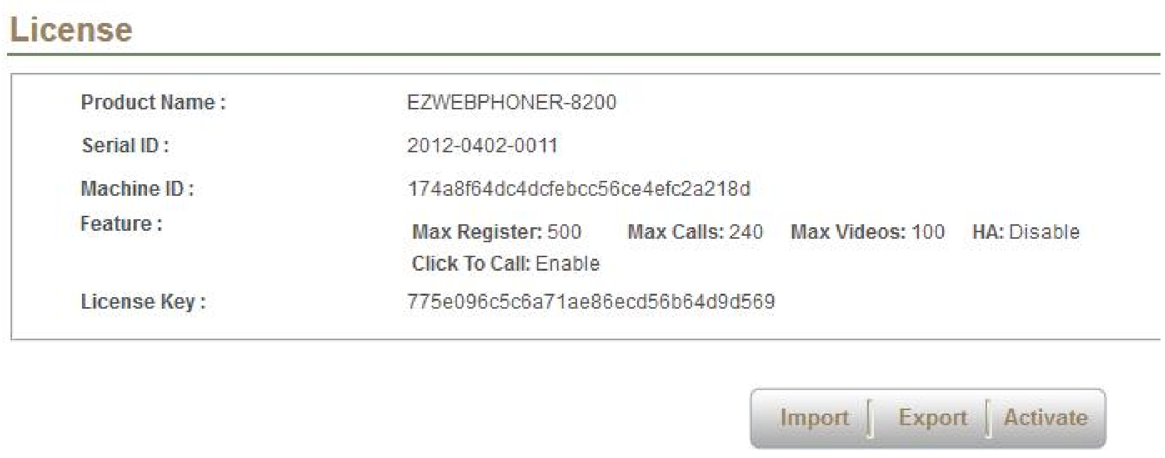


The detail of each parameter is described as below:

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

2.2.6 License

This the license granted for this dedicate server. It can only be used on this dedicate machine. There is no any responsibility 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
License Key	The license key granted
Expired Date	The expired date for the license (only for evaluation 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.

2.2.7 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.

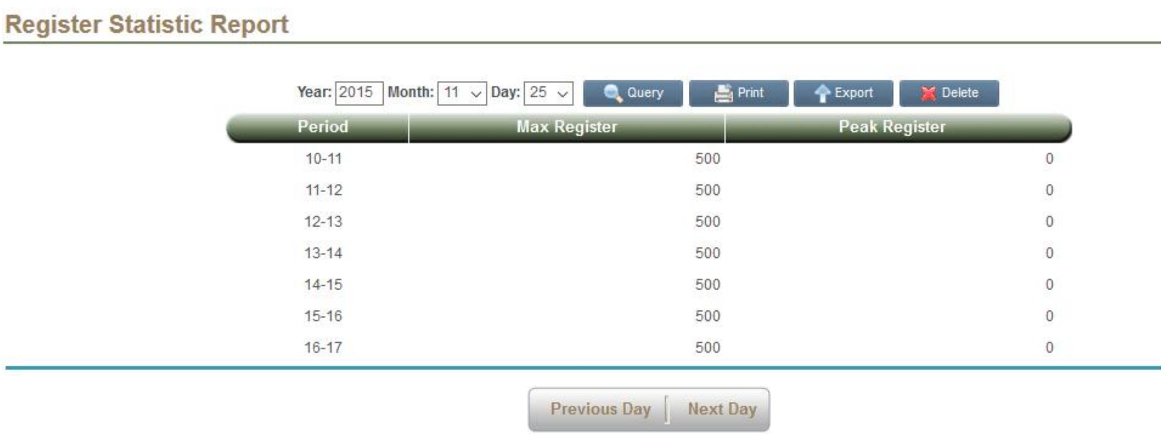
Parameter Name	Description
Trace Target	The target to be used for debugging. It could be the telephony number or IP address. You can combine it by using a semicolon to separate it. For example, you can have the trace target as "02123456;112.112.1.1" which indicates the debug message will contains the 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.

2.3 Report

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

2.3.1 Register Statistic Report

The Register Statistic Report provides the concurrent register user per hour. The administrator can use this report to know how many users are registered through this server. Click ***REPORT -> Register Statistic*** to view the report as follows.



Period	Max Register	Peak Register
10-11	500	0
11-12	500	0
12-13	500	0
13-14	500	0
14-15	500	0
15-16	500	0
16-17	500	0

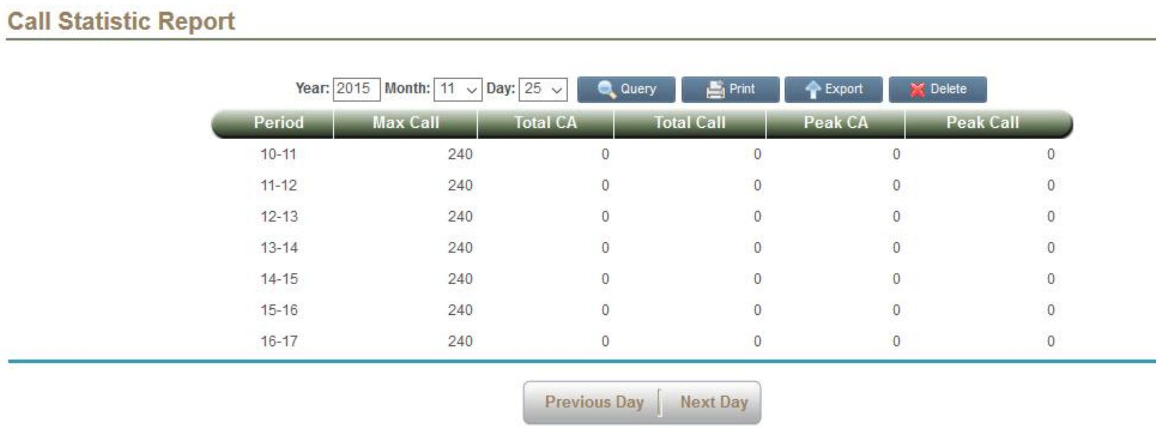
The detail of each report field is described as follows:

Field Name	Description
Period	The time period for this statistic

Field Name	Description
Max Register	The licensed concurrent register user
Peak Register	The peak number of user registered during this period

2.3.2 Call Statistic Report

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

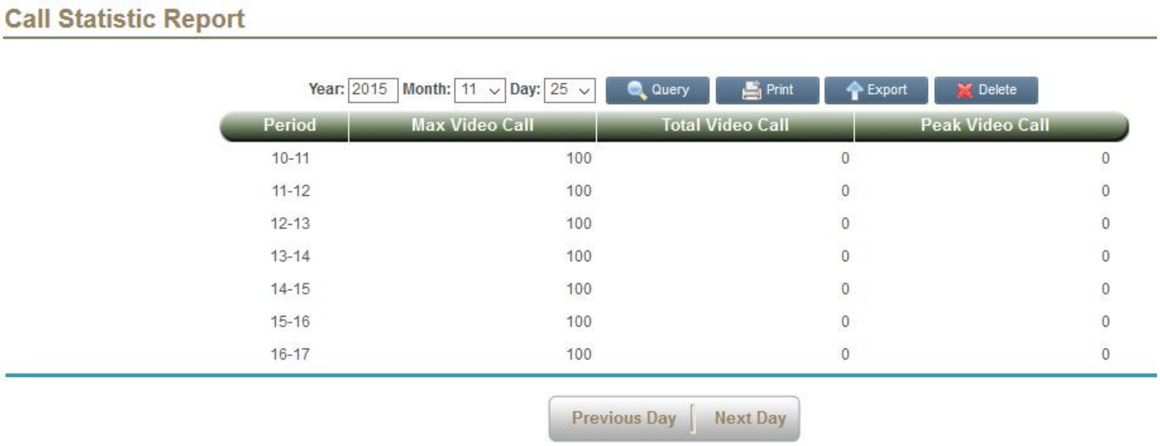


The detail of each report field is described as follows:

Field Name	Description
Period	The time period for this statistic
Max Call	Licensed concurrent calls
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

2.3.3 Video Call Statistic Report

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



Period	Max Video Call	Total Video Call	Peak Video Call
10-11	100	0	0
11-12	100	0	0
12-13	100	0	0
13-14	100	0	0
14-15	100	0	0
15-16	100	0	0
16-17	100	0	0

The detail of each report field is described as follows:

Field Name	Description
Period	The time period for this statistic
Max Video Call	The licensed concurrent video calls
Total Call	Total number of connected video calls during this period
Peak Call	The peak number of connected video calls during this period

2.3.4 Click to Call History Report

This report provides the detail history call report for click to call service. Click ***REPORT -> Click to Call History*** to view the report as follows:

CLICK TO CALL HISTORY REPORT

Search | Delete

Time	Caller	Called	Source IP	Call Type	Call Result	Talk Time
2015/11/17 14:18:49	1234	20012	61.220.196.228	Audio Call	Connected	14
2015/11/17 10:13:27	1234	20012	61.220.196.228	Audio Call	Connected	8
2015/11/17 10:02:51	1234	20012	61.220.196.228	Audio Call	Not Connect	0
2015/11/17 09:40:11	1234	20012	61.220.196.228	Audio Call	Not Connect	0
2015/11/16 21:47:16	1234	20012	36.230.111.32	Audio Call	Not Connect	0
2015/11/16 21:46:05	1234	20012	36.230.111.32	Audio Call	Connected	13
2015/11/16 21:45:19	1234	20012	36.230.111.32	Audio Call	Connected	9
2015/11/16 21:43:27	1234	20012	36.230.111.32	Audio Call	Not Connect	0
2015/11/16 21:40:29	1234	20012	36.230.111.32	Audio Call	Connected	60
2015/11/16 21:38:13	1234	20012	36.230.111.32	Audio Call	Not Connect	0
2015/11/16 21:38:03	1234	20012	36.230.111.32	Audio Call	Not Connect	0
2015/11/16 21:35:26	1234	20012	36.230.111.32	Audio Call	Not Connect	0
2015/11/16 17:25:38	1234	20012	61.220.196.228	Audio Call	Connected	7
2015/11/16 17:17:27	1234	20012	61.220.196.228	Audio Call	Connected	9
2015/11/16 17:15:39	1234	20012	61.220.196.228	Audio Call	Connected	42

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

Total Record: 157

Print | Export

The detail of each report field is described as follows:

Field Name	Description
Time	Starting Time of this call
Caller	Calling party number
Called	Called number
Source IP	The IP address of caller
Call Type	Whether this call is audio or video call?
Call Result	Whether this call is connected or not?
Talk Time	The connected period for this call

2.3.5 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

Search | Delete

Time	Target	Operation	Modifier	Login IP
2015/11/25 15:01:26	Click To Call	Modify	admin	122.116.144.66
2015/11/25 15:00:54	Click To Call	Modify	admin	122.116.144.66
2015/10/23 17:48:25	Restart Service	Execute	admin	61.220.196.228
2015/10/23 17:47:28	Click To Call	Modify	admin	61.220.196.228
2015/10/21 13:04:42	Click To Call	Modify	admin	61.220.196.228
2015/10/19 18:14:35	Restart Service	Execute	admin	114.32.60.152
2015/10/19 18:14:29	Service Parameter	Modify	admin	114.32.60.152
2015/10/19 18:13:01	Restart Service	Execute	admin	114.32.60.152
2015/10/19 18:12:53	Service Parameter	Modify	admin	114.32.60.152
2015/09/08 10:40:57	Restart Service	Execute	admin	61.220.196.223
2015/08/25 16:47:06	Restart Service	Execute	admin	61.220.196.228
2015/08/25 16:34:18	Restart Service	Execute	admin	114.32.60.152
2015/08/25 16:34:08	Service Parameter	Modify	admin	114.32.60.152
2015/08/25 16:33:39	Click To Call	Modify	admin	114.32.60.152
2015/08/25 15:02:36	Restart Service	Execute	admin	61.220.196.228

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

Total Record: 109

Detail

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

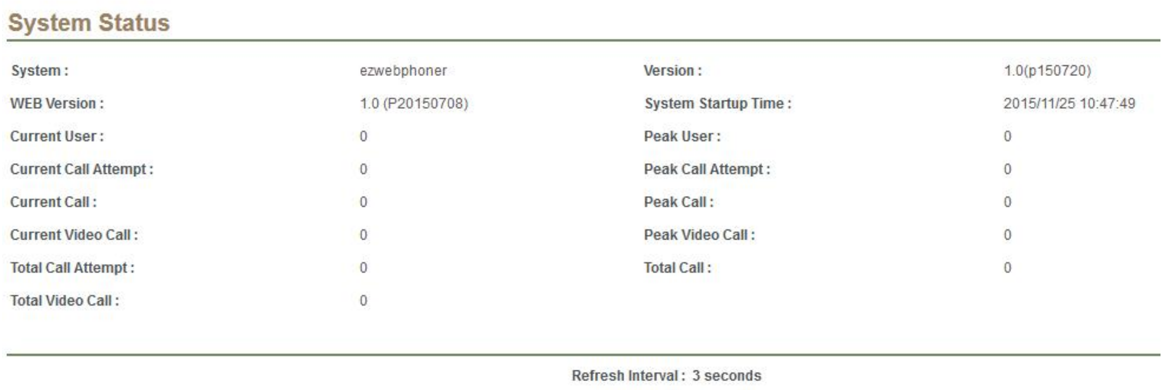
Select one of record and click the Detail button. You will able to see the detail for this provisioning record.

2.4 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.

2.4.1 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.



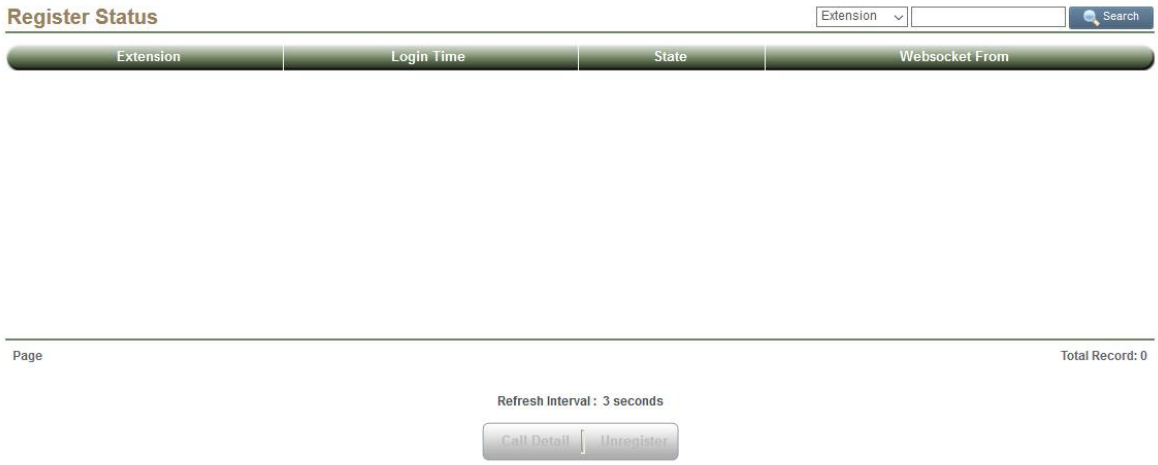
The detail of each filed is described as below:

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 to the system
Current Call Attempt	Current call attempt to the system
Current Call	Current connected call
Current Video Call	Current connected video calls
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 Video Call	The peak connected video call within this hour
Total Call Attempt	The total call attempt count for this hour
Total Call	Total count of connected call for this hour

Field Name	Description
Total Video Call	Total count of connected video call for this hour

2.4.2 Register Status

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



The detail of each filed is described as below:

Field Name	Description
Extension	The extension is currently registered
Login Time	The starting time to login to system
Status	The status of extension
Websocket From	Public IP and port where the extension is registered from using websocket

2.4.3 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
Extension	The calling party extension
Call Type	Incoming to Webrtc or outgoing to SIP
Remote	Remote party number. If it is incoming call, the remote is caller. If it is outgoing call, the remote is called.
State	The current call state
Setup Time	The starting time for the call
Ringing Time	The ringing time for the call
Connect Time	The connected time for the call

Select a call and click disconnect, you will able to disconnect the abnormal call.

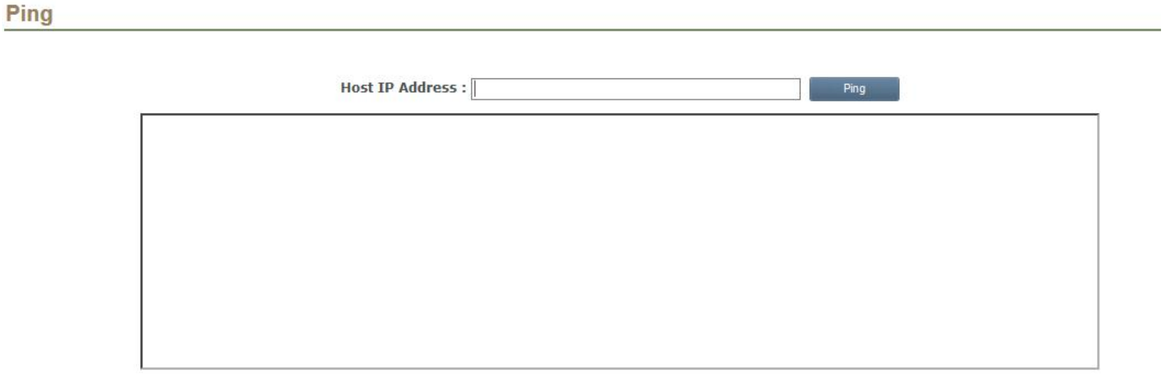
2.4.4 Call Capture

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 some big files in your system and eat all hard disk space. Click "Get Capture File" to download the captured file to analyze.

2.4.5 Ping

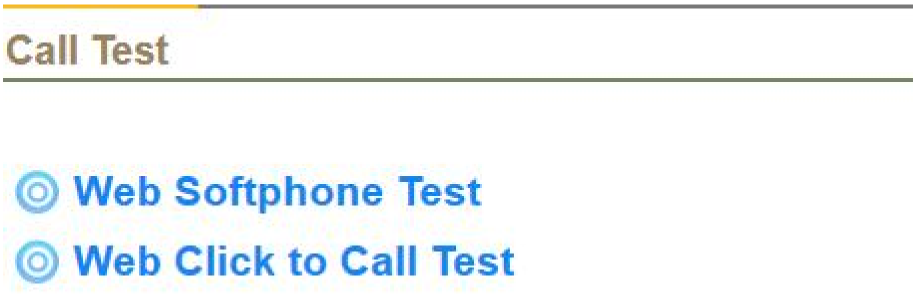
The administrator can ping a IP address from the host by clicking ***DIAGNOSTIC -> Ping.*** The following screen will appear.



Input the Host IP address and start the ping test.

2.4.6 Call Test

This call test is used to have easy way to test the system. Click ***Diagnostic -> Call Test*** and the following will appear:



Click **Web Softphone Test** to test Webrtc feature
Click **Web Click to Call test** to test Click to Call features

2.4.6.1 Web Softphone Test

After click Web Softphone Test URL, the following will appear:

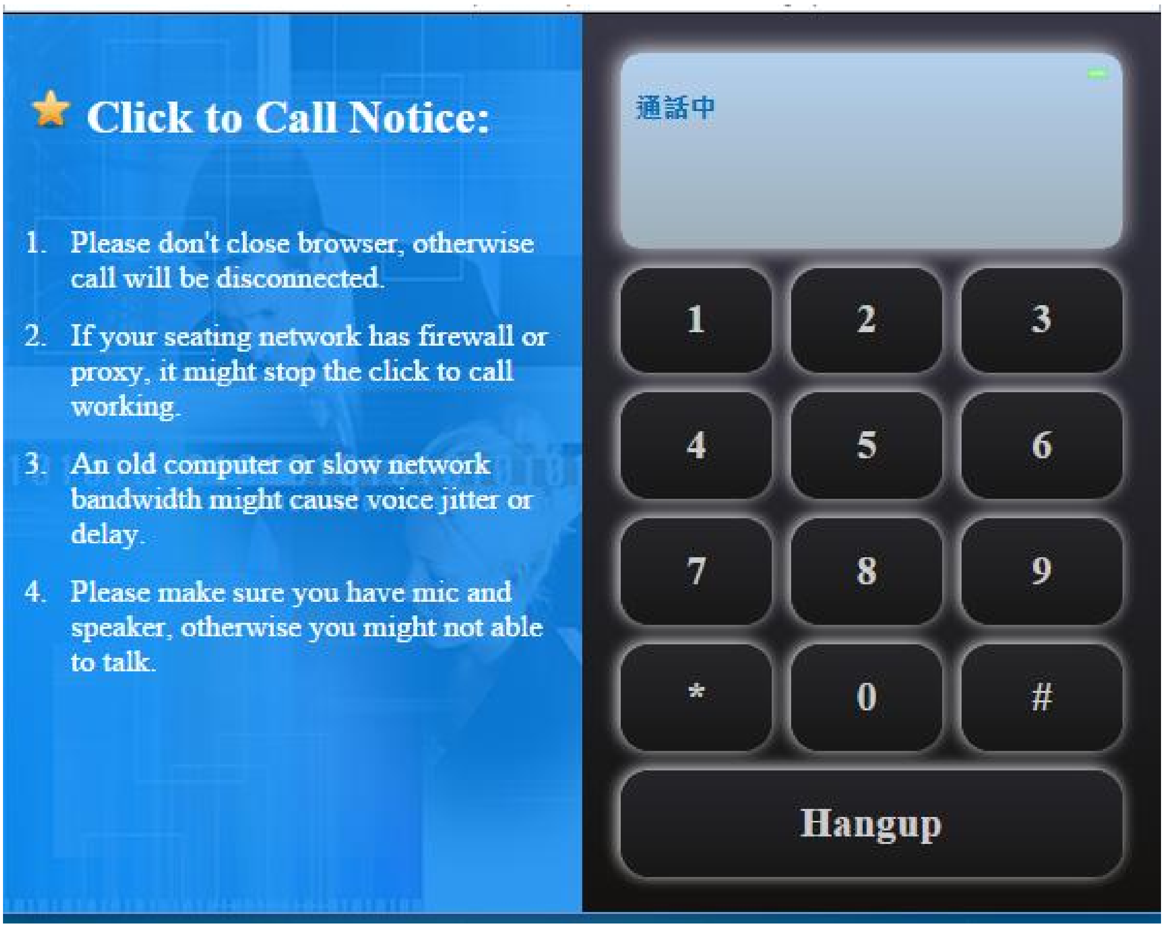
Using the SIP user ID and password to login and the following will appear:

The you will able to make audio or video webrtc calls. Please refer to WebRTC Websocket API for detail.

2.4.6.2 Click to Call Test

The demo page is used for testing click to call features. Click ***SYSTEM -> Click to Call*** Test and the following will appear:

Input Caller and Called Number, the click Make Call button. The call will be making through a popup window as following:



2.5 Administration

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

2.5.1 Restart Service

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

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

2.5.2 Reboot System

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

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

2.5.3 Account

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. If you need SOAP provisioning, you need create an account and give the authorization to "Provisioning".
Language	The web GUI language when the user login.

2.5.4 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.

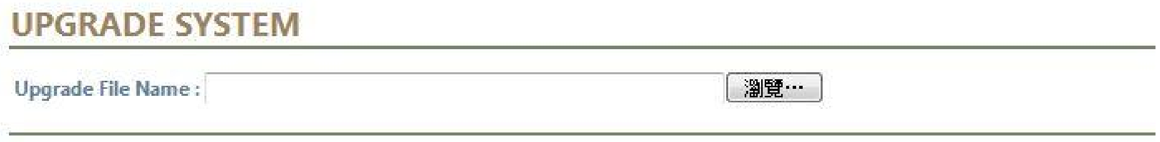
2.5.5 Backup/Restore

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.

2.5.6 Upgrade System

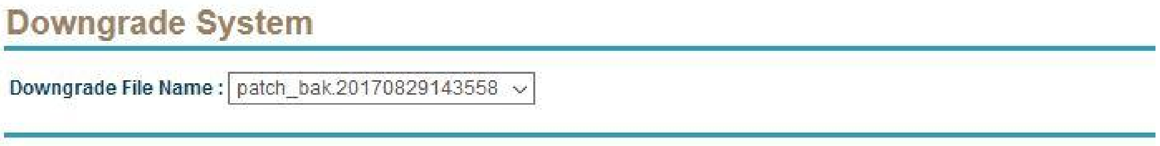
Use ***Upgrade System*** to do the application patch by clicking ***ADMINISTRATION -> Upgrade System***. Please only use the certificated patch file to do the upgrade. Otherwise, it will had problems.



After upgrade, reboot the machine to take effective.

2.5.7 Downgrade System

Use ***Downgrade System*** to restore the application to previous patch by clicking ***ADMINISTRATION -> Downgrade System***.



Select the downgrade file name which is backup by the upgrade automatically. Click Apply to downgrade. After downgrade, restart the service to take effective.

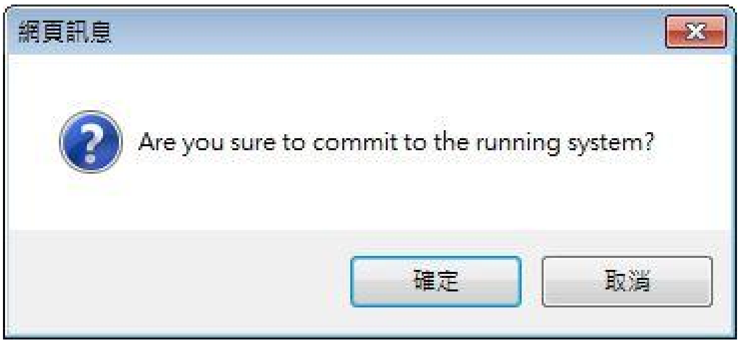
2.5.8 Logout

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

Click ***OK*** to logout.

2.6 Commit

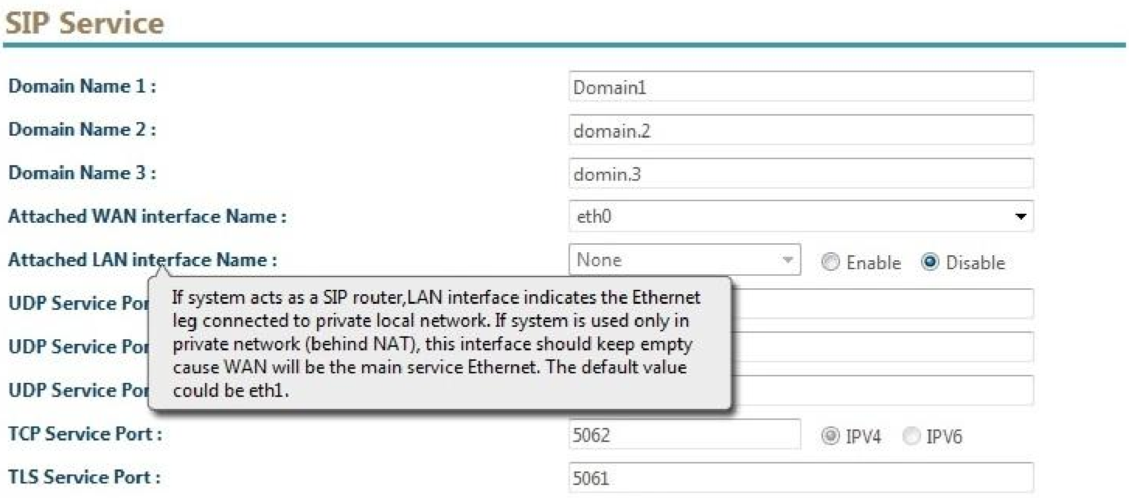
After you change the system settings, you need to apply it by clicking the ***COMMIT*** and the following popup screen will appear:



Select OK to commit the changes.

2.7 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 Built-in Web Phone

Ezwebphoner 8200 provides a built-in web softphone which can be use without any modifications. Use the following URL to login.

https://xxx.xxx.xxx.xxx:943 and the following will appear:

After login, you will see the following:


20006
Settings ▾
5
25
C
Redial
Hold
Mute
Start Record
Transfer
Phone Book
Call History
1
2
3
4
5
6
7
8
9
*
0
#

3.1 Settings

Click Settings and the following will appear:

Item Name	Description
Video Call	Whether enable or disable video call
MWI	Whether enable or disable Voice Mail MWI Service
Language	The GUI language
Exit	Quit this softphone

3.2 Feature Button

The WebRTC softphone contains the following feature buttons:

Item Name	Description
Redial	Redial the last called number
Hold	Hold the call and remote party will hear the music on hold if IP-PBX can support MOH.
Mute	Mute your microphone and your voice will not go to remote party. You can still hear the remote party voice.
Start Record	If IP-PBX can support recording on demand or disable recording feature. Click this button will enable or disable the recording.
Phone Book	Click this button will display the phone book with current status if BLF is enabled.
Call History	The history of incoming and outgoing call

The phone book will looking like the following:


Phone Book
同事
Alex 20009
Jim 20008
Friend Group 1
Jim 20008
Samuel 1 20007
王曉明 20002

4 Appendix

4.1 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
5066	UDP	Local SIP UDP service port	SYSTEM -> Service Parameter -> SIP Local Service Port
50000	UDP	RTP Media UDP port	SYSTEM -> Service Parameter -> Media Starting Port (This is the starting port address, the system will use "Media Starting Port" to "Service Parameter Port + Licensed Concurrent Call * 20)
4000-5000	UDP	Flash Used Local SIP UDP port	SYSTEM ->Click to Call -> SIP Local Service Port
55000-60000	UDP	Flash Local RTP Port	SYSTEM ->Click to Call -> SIP Local Service Port
2081	TCP	Secure Websocket Port (wss)	Only available when Using Secure Websocket is Enable
2082	TCP	Regulare Websocket Port (ws)	none
55000-60000	UDP	Flash Local RTP Port	These ports are used based on interval of 2. It starts on Flash Media Protocol to Flash Media Protocol+ Calls * 3.
1935	TCP	Flash RTMP Service Port	SYSTEM -> Click to Call -> RTMP Port
7443	TCP	Flash Secure RTMP Service Port	SYSTEM -> Click to Call -> RTMPS Port
5080	TCP	Flash Http service port	SYSTEM -> Click to Call -> Flash Web Service Port
8200	TCP	HTTP port for administrator	SYSTEM -> WEB Service -> HTTP Service Port -> Administrator Only be opened in firewall when necessary.

Default Ports	Protocol	Description	Configuration Path
8201	TCP	HTTPS port for administrator	SYSTEM -> WEB Service -> HTTPS Service Port -> Administrator Only be opened in firewall when necessary.
980	TCP	HTTP port for extension user	SYSTEM -> WEB Service -> HTTP Service Port -> Extension Only be opened in firewall when necessary.
943	TCP	HTTPS port for extension user	SYSTEM -> WEB Service -> HTTPS Service Port -> Extension Only be opened in firewall when necessary.

4.2 Customzied Phone Book URL

The system will always looking at the following for the phone book URL:

Phone Book URL: https://phonebook.demo.com:8080/getpbook.jsp
Extension: 1001

When system is querying the phone book will send the following to phone book web service:

https://phonebook.demo.com:8080/getpbook.jsp?pext=1001

And the web service get the 1001 is the target to be queried and output the following phone book XML to our system:

```
<EZPhoneDirectory>
        <PbookGroup>
                <GroupName>Company</GroupName>
                <DirectoryEntry>
                        <Name>Alex</Name>
                        <Telephone>20009</Telephone>
                        <Blf>No</Blf>
                </DirectoryEntry>
                <DirectoryEntry>
                        <Name>Jim</Name>
                        <Telephone>20008</Telephone>
                        <Blf>Yes</Blf>
                </DirectoryEntry>
```

```
        </PbookGroup>

        <PbookGroup>
                <GroupName>Friend Group</GroupName>
                <DirectoryEntry>
                        <Name>Jim</Name>
                        <Telephone>20008</Telephone>
                        <Blf>Yes</Blf>
                 </DirectoryEntry>
                <DirectoryEntry>
                        <Name>Samuel Tz</Name>
                        <Telephone>20007</Telephone>
                        <Blf>Yes</Blf>
                </DirectoryEntry>
                <DirectoryEntry>
                        <Name>Ming Wang</Name>
                        <Telephone>20002</Telephone>
                        <Blf>Yes</Blf>
                </DirectoryEntry>
        </PbookGroup>
</EZPhoneDirectory>
```

Please contact technical support for detail.

4.3 WebRTC Websocket API

The system provides a very easy interface to be implemented on web based technologies. It is based on HTML5 websocket and can be running under Windows, Linux, Mac, Andriod or ipad without any limitation. It frees the limitation for your agent OS and platform.

The websocket interface includes register and call control features.

The protocol URL could be one of the following:
ws://xxx.xxx.xxx.xxxx/2082 (regular websocket)
wss://xxx.xxx.xxx.xxxx/2081 (secure websocket)

xxx.xxx.xxx.xxx is the IP address of the server

Websocket Information:

websocket port: 2082
secure weboscket port: 2081

websocket protocol name: web-call-protocol

4.3.1 Command

This is the command API could be send to Webphoner server. The system will reply each command's ACK.

4.3.1.1 Connect to Server

This command start the AP level communication to WebRTC server after you successfully connect to webosocket server. The server will return an nonce value for authentication.

Connect to WebRTC Server
op= 1000
seq=xxx (Unique command sequence)

Connecting Authentication Response
op= 4001
seq=xxx (same as 3001)
nonce=xxx (nonce value for authentication)

4.3.1.2 Register

This command is used to ask to register to SIP Proxy server.

Register to SIP Proxy Server
op=1001
seq=xxx
tel=xxx (Register Telephone Number)
usr=xxx (SIP User ID)
mwi=x (0: disable, 1:enable mwi)
pwd=xxx (SIP User Password) (encrypted by des("***KEY***"+nonce+tel))
btype=xxx (0: Chrome (default), 1: Firefox, 2: Opera, 3: Edge, 4: Safari)

Please contact for real encryption key for ***KEY.***

Register ACK
op=2001
seq=xxx
code=xxx (0: Processing, -1: Stop Existing Register first, -2: Parameter Error)
pbook=xxxx (phone book access URL)
cid=xxxx (existing call-id)
cid=xxxx
cid=xxxx

You need wait Proxy Register Status Event (op=9001) in order to get real register status.

4.3.1.3 Unregister

This command is to ask to unregister from SIP proxy server.

Un-Register
op=1002
seq=xxx

Un-Register ACK
op=2002
seq=xxx
code=xxx (0: Processing, -1: No Existing Register, -2: Parameter Error)

4.3.1.4 Call Making

This command is used to making a call out.

Call Making:
op=1003
seq=xxx
disp=xxx (SIP Display Name)
from=xxx (SIP Calling Party Number)
to= xxx (SIP Called Number)
cdata=xxxxx (optional, CTI data)
skill=xxxx (optional, Skill data)
sdp=xxxxx (SDP getting from browser WebRTC)
(e.g. v=0\r\no=xxxx\r\n)

Call Making ACK
op=2003
seq=xxx
cid=xxxxx (SIP CALL-ID)
code=xxx
(0: Processing, -1: No Register for Proxy Call, -2: Parameter error, -3:Failed to get resource)

4.3.1.5 Incoming Call Answer

Answer incoming call when receive an **Incoming Call Event**.

Incoming Call Answer
op=1004
seq=xxx
cid=xxxxx(SIP CALL-ID)
sdp=xxxxx(v=0\r\no=xxxx\r\n)

Incoming Call Answer ACK

op=2004
seq=xxx
code=xxx (0: Processing, -1: No Register for Proxy Call, -2: Parameter error, -4: No such call)

4.3.1.6 Incoming Call Reject

Reject the incoming call with specified the SIP reason code.

Incoming Call Reject
op=1005
seq=xxx
cid=xxxxx(SIP CALL-ID)
rc=xxx (Reject Code)
mto=xxxx (Move to URL --- rc=302 only)

Frequently Used Code (rc=):
404 Not Found
415 Unsupported Media Type
486 Busy Here
480 Temporarily Unavailable
302 Moved Temporarily (Call Forward)

Incoming Call Reject ACK
op=2005
seq=xxx
code=xxx (0: Processing, -1: No such call, -2: parameter error)

4.3.1.7 Incoming Call Ringing

This command is used to make the caller get into ringing state by sending 180 Ringing.

Incoming Call Ringing
op=1006
seq=xxx
cid=xxxxx(SIP CALL-ID)

Incoming Call Ringing ACK
op=2006
seq=xxx
code=xxx (0: Processing, -4: No Such Call, -2: Parameter error)

4.3.1.8 Call Modify

This command is used to hold, unhold or retrieve it back when there is a 2nd call madden by call transfer.

Call Modify
op=1007
seq=xxx
cid=xxxxx(SIP CALL-ID)
type=x(0: unhold, 1:Hold 2:Retrieve, 3: Refresh Video Request)

2: retrieve is used to disconnect the call made by call transfer and back to 1st call.

Call Modify ACK
op=2007
seq=xxx
code=xxx (0: Processing, -4: No Such Call, -2: Parameter error)

4.3.1.9 Make 2nd Call for Transfer

This command is used to make 2nd call. If AP need transfer to it, just call Disconnect Call command.

Call Transfer (After Call Connected Only, this op will make second call)
op=1008
seq=xxx
cid=xxxxx (SIP CALL-ID)
rto=xxx (Number to be called)

Call Transfer ACK
op=2008
seq=xxx
code=xxx (0: Processing, -4: No such Call, -2: Parameter error)

4.3.1.10 Send Message

This command will send SIP message to remote party using MESSAGE method. It is a experimental feature, please contact for usage.

Send SIP Message
op=1009
seq=xxx
from=xxx (SIP From URL)
to=xxx (SIP TO URL)
mid=xxx (Message ID)
msg=xxx (SIP Message)

Send SIP Message ACK
op=2009
seq=xxx
code=xxx
(0: Processing, -2: Parameter error)

4.3.1.11 Disconnect Call

This command is use to hangup the call.

Call Disconnect: (After call Disconnect)
op=1010
seq=xxx
cid=xxxxx(SIP CALL-ID)

Call Disconnect ACK
op=2010
seq=xxx
code=xxx (0: Processing, -4: No such Call, -2: Parameter error)

4.3.1.12 Click to Call Guest Calling

This is only available when click to call module is enabled and will be used to making a call without register.

Guest Call Making
op=1011
seq=xxx
disp=xxx (DisplayName)
from=xxx (ANI)
to=xxx (DNIS)
nonce=xxxxxx (as same as session init)
cdata=xxxxx (cti data)
skill=xxxx (skill)
sdp=xxxxx (v=0\r\no=xxxx\r\n)

cdata has a special purpose that is used to carry Call Center CID (getting from chat) in order to bind this outgoing call into an existing chat. The format is "cdata=_cid=xxx".

Guest Call Making ACK
op=2011
seq=xxx
cid=xxxxx(SIP CALL-ID)

code=xxx (0: Processing, -1: No Register for Proxy Call, -2: Parameter error, -3: Failed to get resource)

4.3.1.13 Send DTMF

This command is used to send a DTMF digit to remote party.

Send DTMF
op=1012
seq=xxx
cid=xxxxx (SIP CALL-ID
dtmf=x (DTMF digit, one digit)

Send DTMF ACK
op=2012
seq=xxx
code=xxx (0: Processing, -4: No such Call, -2: Parameter error)

4.3.1.14 Voice Logging Control

This is working with voice recording on demand or disable recording on call features. It will send a SIP INFO to tell SIP Proxy to start the recording or stop recording based on the setting.

Voice Logging Control (recording on demand):
op=1013
seq=xxx
cid=xxxxx (SIP CALL-ID
rec=x (0: stop recording, 1: start recording)

Voice Logging Control Ack
op=2013
seq=xxx
code=xxx (0: Processing, -4: No such Call, -2: Parameter error)

4.3.1.15 BLF Monitor

This command is used to start or stop BLF monitor.

BLF Monitor:
op=1014
seq=xxx
blf=x (0: stop BLF, 1: start BLF, 2: Get BLF Extension)
ext=xxxx (optional monitor extension), if ext is empty or no ext and blf=0, mean clean ALL extension's BLF

BLF Monitor Ack
op=2014
seq=xxx

ext=xxxx,xxxx,xxxx,xxxx (if blf=2 for getting current BLF extension)
code=xxx (0: Processing, -1: over max BLF monitor count, -2: Parameter error)

4.3.2 Event

This is the Event will be received from Webphoner server. AP doesn't need reply ACK for Event.

4.3.2.1 Register Status Event

This is the Proxy Register Status Reporting event.

Proxy Register Status Event:
op=9001
seq=xxx
state=xxxx

(0: Registered, -1: Unregistered, -2: Request Timeout, -3: Contact Updated, -xxx: sip reason code)

4.3.2.2 Incoming Call Event

This event is to tell AP there is an incoming call arrived.

Incoming Call Event:
op=9002
seq=xxx
from=xxxxx (Calling Number)
disp=xxx (DislayName)
to=xxxx (Called Number)
cid=xxxxx (SIP CALL-ID)
ucid=xxxx (universal Call ID)
sdp=xxxx (caller's SDP)

4.3.2.3 Media Change Event

This event to tell AP that media was changed or established which could be IP, port or codec change. AP should receive this event after calling Call Making, Call Answer,Call Ringing or Call Modify.

Media Change Event:
op=9003
seq=xxx
cid=xxxxx (SIP CALL-ID)
sdp=xxxxx (Remote parties's SDP)

4.3.2.4 Call State Change Event

This event to tell AP there is a state changed for a existing call.

Call State Change Event:
op=9004
seq=xxx
cid=xxxxx(SIP CALL-ID)
ucid=xxxx (universal Call ID)
state=xxx (0: Disconnect 1: Ring 2: Connected, 3: Local Hold, 4:Remote Hold)
cause=xxx (xxx: SIP reject code)
aid=xxxx (ACD unique Call ID, this could be used for binding to chat or used for recording index).

4.3.2.5 Receive SIP Message Event

This event is to tell AP there is a message arrived. It is a experimental feature, please contact for usage.

Receive SIP Message: Notify to receive a SIP message.
op=9005
seq=xxx
from=xxx (SIP From URL)
to=xxx (SIP TO URL)
msg=xxx (SIP Message)

4.3.2.6 Message Sending Report Event

When calling Send Message and this event will tell AP whether the message was delivered or not. It is a experimental feature, please contact for usage.

SIP Message Sending Report
op=9006
seq=xxx
mid=xxx
code=xxx (0: Sent Successfully, -1: Request Timeout, -xxx: Other SIP error)

4.3.2.7 2nd Call State Change Event

This event reports second call's state change.

2nd Call State Change Event
op=9004
seq=xxx
cid=xxxxx(SIP CALL-ID)
state=xxx (0: Disconnect 1: Ring 2: Connected)
cause=xxx (xxx: SIP reject code)
aid=xxxx (ACD unique Call ID, this could be used for binding to chat or used for recording index).

4.3.2.8 Reset WebRTC Media Channel

This command to tell AP to reset WEBRTC channel. When receive this event, AP need reset WebRTC channel in order to get updated media.

Reset WEBRTC Channel:
op=9008
seq=xxx
cid=xxxxx (SIP CALL-ID)

4.3.2.9 Notify to Answer Event

This event is an event to tell AP to answer the call. When receive it, AP need answer immediately.

Notify to Answer Event
op=9009
seq=xxx
cid=xxxxx(SIP CALL-ID)

4.3.2.10 ACD Agent Answer Event

This event to tell AP that call center agent is answered. This agent telephone is required to bind this video with the chatting session. It will working only on the specified server. Please contact for detail usage.

ACD Agent Answer Event
op=9010
seq=xxx
cid=xxxx
agtel=xxx (Serviced agent telephone number)

4.3.2.11 Voice Mail Change Event

This will be only send when mwi is enabled for register command (op=1001). This event notice AP the changes of voice mail.

Voice Mail Change Event:
op=9011
seq=xxx
vm=1/1 (0/0) new/old (new_urgent/ old_urgent)

4.3.2.12 BLF Status Notify Event

This is the BLF Monitor Status Reporting event.

BLF Extension State Notice Event:
op=9012

seq=xxx
state=x (0:Success, <0 indicate error, e.g. -404 not found)
ext=xxx (reported extension)
blfxml=xxxxxxxxx (BLF dialog notice XML)

Example of blfxml

```
blfxml=<?xml version="1.0" encoding="UTF-8"?><dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="2" state="full" entity="sip:20002@61.220.196.224"><dialog id="20002" direction="recipient"><state>early</state><local><identity display="20002">sip:20002@61.220.196.224</identity></local><remote><identity display="20001">sip:20001@61.220.196.224</identity></remote></dialog></dialog-info>\r\n
```

How to parser the XML for BLF:

Called Party BLF Notify Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="2" state="full" entity="sip:20002@61.220.196.224">
<dialog id="20002" direction="recipient">
<state>early</state>
<local><identity display="20002">sip:20002@61.220.196.224</identity></local>
<remote><identity display="20001">sip:20001@61.220.196.224</identity></remote>
</dialog>
</dialog-info>\r\n
```

Calling Party BLF Notify Example:

```
<?xml version="1.0" encoding="UTF-8"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="2" state="full" entity="sip:20002@61.220.196.224">
<dialog id="20002" direction="initiator">
<state>terminated</state>
<local><identity display="20002">sip:20002@61.220.196.224</identity></local>
</dialog></dialog-info>\r\n
```

The BLF Extension Target:
<local><identity display="20002">sip:20002@61.220.196.224</identity></local>
retrieve between sip: and @
In this case, it is 20002

Calling or Called Indication:
Calling: direction="initiator"
Called: direction="recipient"

Extension Status:

<state>terminated</state>
void: unavailable
terminated: idle
early: Ringing
confirmed: Connected

Additional Caller ID:
When extension target is called party, caller ID can be retrieve from:
<remote><identity display="20001">sip:20001@61.220.196.224</identity></remote>