



FCM5600 IPPBX Admin Guide

Related to Software Version v4.0.4.p6

FIBERME Communications LLC

1749 Old Meadow Rd. Suite 401

McLean, VA 22102, USA

1. Preface

1.1 Audience

This manual is intended to provide clear operating instructions for those responsible for configuring and managing the FCM5600 IP-PBX. By carefully reading and consulting this manual, to help the audience solve the setting and deployment issues.

1.2 Safety Notice

Please read the following safety notices before installing or using this IPPBX. They are crucial for the safe and reliable operation of the device. Failure to follow the instructions contained in this document may result in damage to your IPPBX and avoidance of the warranty.

- 1- Please use the external power supply which is included in the package. Any other power supply may cause damage to the unit, affecting performance or inducing noise.
- 2- Before using the external power supply in the package, please check your building power voltage. Connecting to inaccurate power voltage may cause fire or damage.
- 3- Please do not damage the power cord. If the power cord or plug is impaired, do not use it. Connecting a damaged power cord may cause fire or electric shock.
- 4- Ensure the plug-socket combination is accessible even after the unit is installed. In order to maintain the unit, it will need to be disconnected from the power source.
- 5- Do not drop, knock, or shake the unit. Rough handling can break internal circuit boards.
- 6- Do not install the unit in places where there is direct sunlight. Also do not place the unit on carpets or cushions. Otherwise, it may cause the unit to malfunction or cause fire.
- 7- Avoid exposing the unit to high temperature (above 40°C), low temperature (below -10°C) or high humidity. Otherwise, it could cause damage and will void the warranty.
- 8- Avoid letting the unit in contact with water or any other liquid which would damage the unit.
- 9- Do not attempt to open the device. Non-expert handling of the device could cause damage and will void the warranty.
- 10- Consult your authorized dealer for assistance if any issues or questions you may have.
- 11- Do not use harsh chemicals, cleaning solvents, or strong detergents to clean the unit.
- 12- Clean the unit with a soft cloth that has been slightly dampened in a mild soap and water solution.

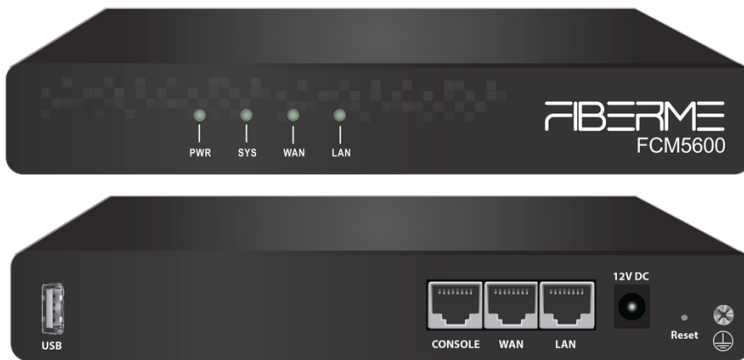
-
- 13- If you suspect the unit has been struck by lightning, do not touch the unit, power plug or phone line. Call your authorized dealer for assistance to avoid the possibility of electric shock.
 - 14- Ensure the unit is installed in a well-ventilated room to avoid overheating.
 - 15- Before you work on any equipment, be aware of any hazards involved in electrical circuitry and be familiar with standard practices for preventing accidents if you are in a situation that could cause physical injury.

2. Overview

2.1 Brief Introduction

FIBERME FCM5600 IPPBX is the most innovative solution for VoIP telecommunications in the SMB (Small and Medium-sized Business) market. They provide not only traditional PBX functionality such as automated attendant and voicemail, but also offer many advanced telephony features, including remote extensions, remote office connection, IVR, call recording, and call detail records (CDR). All of these can greatly enhance business operations while reducing operating costs.

FCM5600 IPPBX



2.2 Mechanical Design

- 1x Power Interface (DC 12V 1x 1x Reset Button)
- 1x USB Interface (For USB keyboard or USB storage)
- 1x Console Interface (For connecting to a monitor and debug purpose)
- 2 * Ethernet Interface (WAN/LAN:10/100Mbps)

Identification	Indication	Status	Specification
PWR	Power Status	On	Power on
		Off	Power off
SYS	System Status	On	System initiating
		Blink	System is functioning
		Off	System failure
WAN	WAN Status	On	Connected but no data transmitting
		Blink	Data transmitting

		Off	Disconnected
LAN	LAN Status	On	Connected but no data transmitting
		Blink	Data transmitting
		Off	Disconnected

2.3 Key Feature

- ✓ BLF(Busy Lamp Field)
 - ✓ Caller ID
 - ✓ DND(Do Not Disturb)
 - ✓ WebRTC
 - ✓ Extension User Portal
 - ✓ Call Detail Records (500,000 records)
 - ✓ Call Center Queues
 - ✓ Call Parking
 - ✓ Call Forward
 - ✓ Call Transfer
 - ✓ Call Waiting
 - ✓ Call Recording
 - ✓ One Touch Recording
 - ✓ Video Call
 - ✓ Voicemail
 - ✓ Virtual Fax
 - ✓ Conference Bridge (10 Conferences)
 - ✓ DISA (Direct Inward System Access)
 - ✓ Paging and Intercom
 - ✓ Direct Inbound Routing
 - ✓ Blacklist (blacklist the last caller)
 - ✓ Smart DID
 - ✓ Quick Setup Wizard
 - ✓ Flexible Dial Permissions
 - ✓ Feature Codes
 - ✓ Wakeup Call
 - ✓ One Number Stations
 - ✓ Music On Hold
 - ✓ Phonebook/LDAP(10,000 contacts)
 - ✓ Department (ring group, pickup group)
 - ✓ Phone Provisioning
 - ✓ Expansion Box Provisioning
 - ✓ Speed Dial
 - ✓ Time Conditions
 - ✓ SIP/IAX Extension Registration
 - ✓ Static/DHCP Network Access
 - ✓ System Backup
 - ✓ T.38 Fax Pass-through
 - ✓ USB Extended Storage (Scalable)
 - ✓ GeoIP Security Policy
-
- ✓ Audio Codec: G.722/ G.711-Ulaw/ G.711-Alaw/ G.726/ G.729/ GSM/ SPEEX/Opus
 - ✓ Video Codec: H.261/ H.263 / H.263+ /H.264/VP8
 - ✓ VPN Server (PPTP/OpenVPN, support 10 VPN clients)
 - ✓ VPN Client (PPTP/OpenVPN)
 - ✓ IP Phone Provisioning (FIBERME, Cisco, Fanvil, Htek, Yealink, Grandstream)

2.4 Environmental Requirements

Operating Temperature: 0 °C ~40 °C Storage Temperature: -20 °C ~ 55 °C Humidity: 5~95%

3. Getting Started

3.1 Hardware Installation

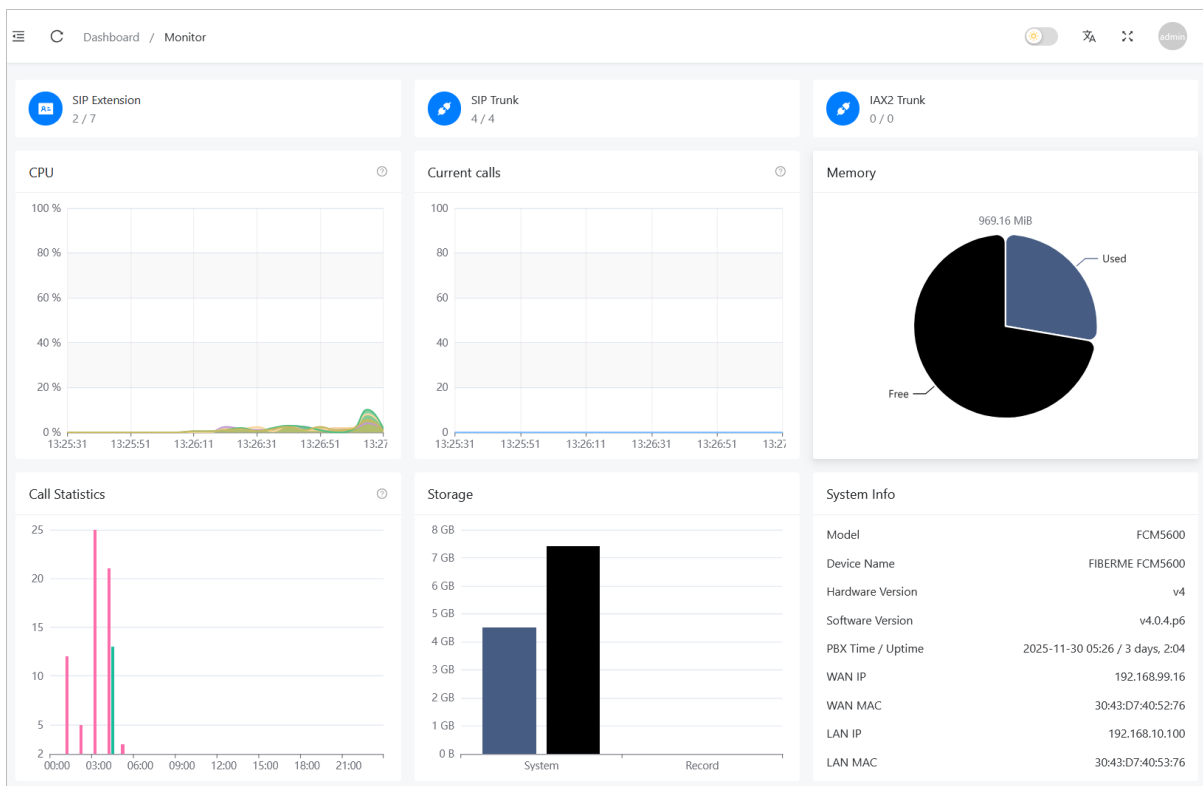
Hardware installation of each model is documented in the “Quick Installation Guide”, and the guide was packed with each of the IPPBX packages. Please refer to the guide to install the unit into your local LAN.

Please pay attention to the safety notices during the hardware installation process.

4. Dashboard

4.1 Monitor

The index interface is the system status page, which mainly displays system information and system resource information, such as the number of trunks, call statistics, system storage, etc.



- **SIP Extension:** The number of registered SIP extensions and the total number of SIP

extensions in the system.

- **SIP Trunk:** The number of registered SIP trunks and the total number of SIP trunks in the system.
- **IAX2 Trunk:** The number of registered IAX2 trunks and the total number of IAX2 trunks in the system.
- **CPU:** Display the current usage of the CPU.
- **Current Calls:** The number of concurrent calls in the system.
- **Memory:** Display the current usage of memory.
- **Call Statistics:** Statistics of the current day's call type and number of calls of the device.
- **Storage:** Display the current usage of storage.

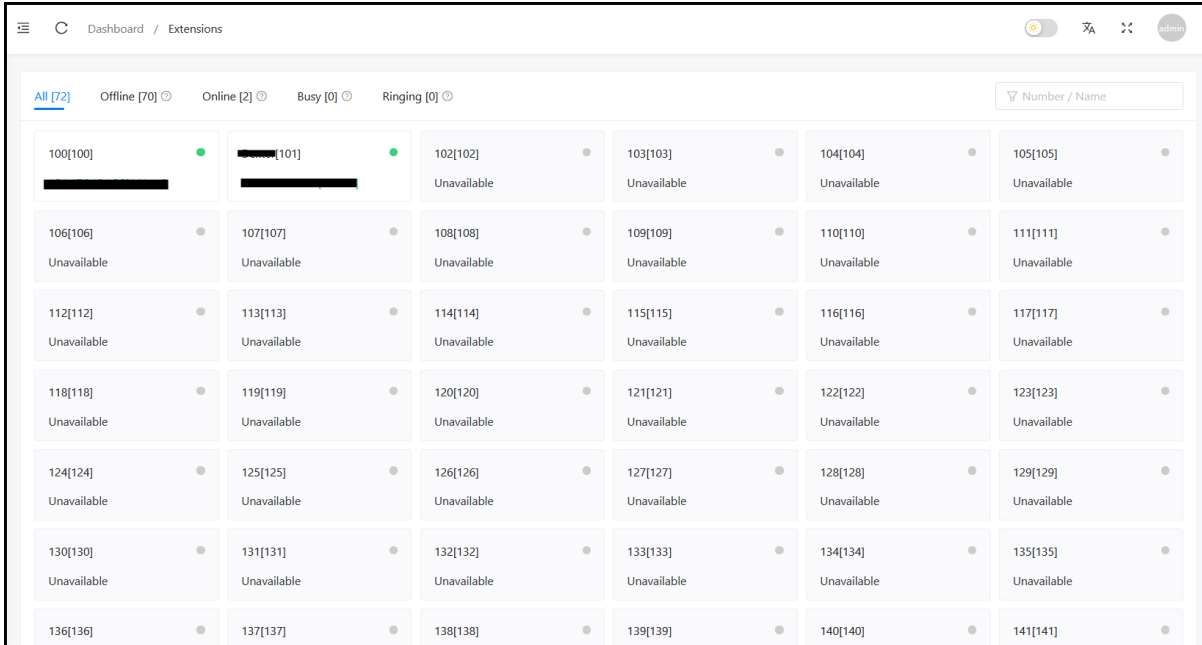
System Info

- **Model:** The model of the current device.
- **Device Name:** The given name of the current device. You may change the Device name under path: *system-Settings-Web-Web Customization*
- **Hardware Version:** The hardware version number of the current device
- **Software Version:** The software version number of the current device
- **PBX Time / Uptime:** The system time and the duration of uptime operation of the current device
- **WAN IP:** WAN port IP address
- **WAN MAC:** WAN port Mac address
- **LAN IP:** LAN port IP address
- **LAN MAC:** LAN port Mac address

4.2 Extensions

On the Extensions page, you can see all extensions' real-time statuses, such as online, offline, busy, and ringing.

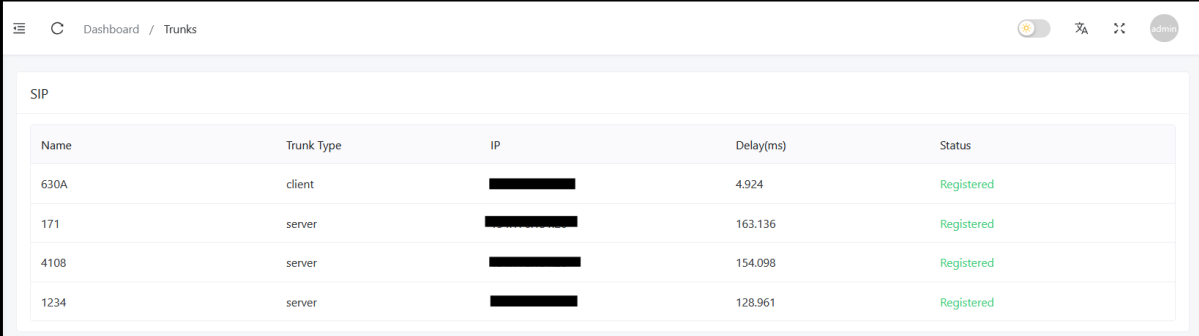
The IP address is displayed below the registered extension number corresponding to the registered terminal's IP address.



Dashboard / Extensions						
All [72] Offline [70] Online [2] Busy [0] Ringing [0]						
Number / Name						
100[100] ● [REDACTED]	[REDACTED][101] ● [REDACTED]	102[102] ● Unavailable	103[103] ● Unavailable	104[104] ● Unavailable	105[105] ● Unavailable	
106[106] ● Unavailable	107[107] ● Unavailable	108[108] ● Unavailable	109[109] ● Unavailable	110[110] ● Unavailable	111[111] ● Unavailable	
112[112] ● Unavailable	113[113] ● Unavailable	114[114] ● Unavailable	115[115] ● Unavailable	116[116] ● Unavailable	117[117] ● Unavailable	
118[118] ● Unavailable	119[119] ● Unavailable	120[120] ● Unavailable	121[121] ● Unavailable	122[122] ● Unavailable	123[123] ● Unavailable	
124[124] ● Unavailable	125[125] ● Unavailable	126[126] ● Unavailable	127[127] ● Unavailable	128[128] ● Unavailable	129[129] ● Unavailable	
130[130] ● Unavailable	131[131] ● Unavailable	132[132] ● Unavailable	133[133] ● Unavailable	134[134] ● Unavailable	135[135] ● Unavailable	
136[136] ● Unavailable	137[137] ● Unavailable	138[138] ● Unavailable	139[139] ● Unavailable	140[140] ● Unavailable	141[141] ● Unavailable	

4.3 Trunks

On the Trunks page, you can view the status of all SIP trunks, IAX trunks, analog trunks, and E1/T1 trunks. The status of analog trunks and E1/T1 trunks depend on the trunk's sound card. You may click on the "Free Line" in the analog trunk list to free the current busy channel.



Name	Trunk Type	IP	Delay(ms)	Status
630A	client	[REDACTED]	4.924	Registered
171	server	[REDACTED]	163.136	Registered
4108	server	[REDACTED]	154.098	Registered
1234	server	[REDACTED]	128.961	Registered

SIP/IAX

- **Name:** Trunk Name
- **Trunk Type:** Type of trunk (Server or Client)
- **IP:** IP address of the trunk
- **Delay:** Delay in trunk's data
- **Status:** Registration status of trunk

5. PBX Settings

5.1 Extensions/Trunks

5.1.1 Departments

Path: **PBX Settings** -> **Extensions/Trunks** -> **Departments**



Department concept is an extremely useful feature of IPPBX system. Extensions are grouped by your company's actual organizational structure.

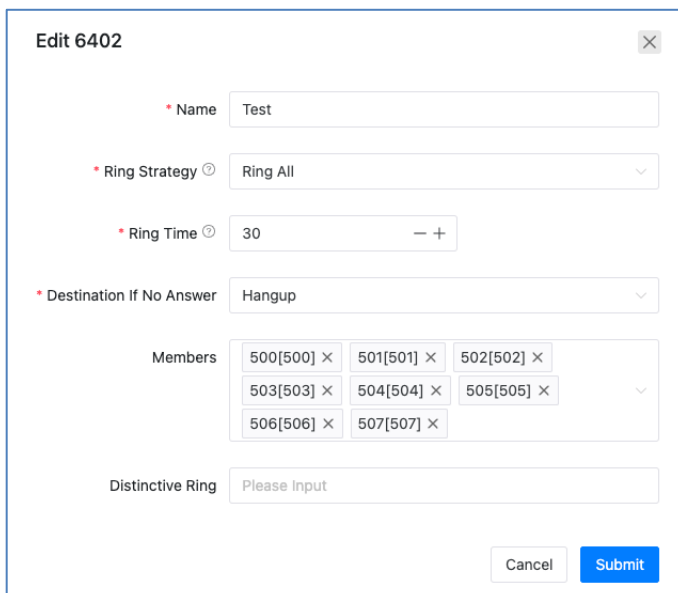
Existing Departments created must be listed here.

If you wish to create a new department, please click on the **Add** button. Specify the department name and select member extensions then submit.



Name	Extension	Members	Operation
6401-	6401	899[899]	[Edit] [Delete]
Test	6402	500[500] 501[501] 502[502] 503[503] 504[504] 505[505] 506[506] 507[507]	[Edit] [Delete]

If you wish to Modify/Delete a department, please click on  button to edit, or click on the  button to remove a department.



Edit 6402 ✕

* Name

* Ring Strategy

* Ring Time - +

* Destination If No Answer

Members

Distinctive Ring

- **Name:** You may change the department name from the textbox.
- **Ring Strategy:** In the dropdown list select a desired ring strategy of how to ring the

department (Ring Group) extensions upon incoming calls.

- **Ring All:** Ring all available member extensions until one answers (default).
- **Linear:** Starting with the first member, ring the extension of each member in turn until the call is answered.
- **Ring Time:** You may adjust the ring time of each extension upon department ring group incoming calls from the textbox.
- **Destination if no answer:** In the dropdown list select a call destination for the inbound calls when no one answers the call.
- **Members:** You may add/remove members of your department.
- **Distinctive Ringtone:** It can ring the phones with specific ringtone upon inbound calls to this department.

5.1.2 IP Extensions


Path: **PBX Settings -> Extensions/Trunks -> IP Extensions**

IP Extensions will list any existing extensions, as well you can add, edit or delete extensions for this page.

IP extensions are user extensions including desktop IP phones, softphones for Windows/Android/iPhone/Linux and other endpoints that support SIP/IAX2 protocol.

Add Bulk Add Import Export Bulk Edit Delete Selected Delete All							<input type="text" value="Name / Number"/> <input type="button" value="Q"/>
<input type="checkbox"/>	Name	Extension Number	Outbound CID 1	Outbound CID 2	Department Name	Dial Permission	Operation
<input type="checkbox"/>	220	220				DialPlan1	
<input type="checkbox"/>	221	221				DialPlan1	
<input type="checkbox"/>	222	222				DialPlan1	
<input type="checkbox"/>	223	223				DialPlan1	
<input type="checkbox"/>	224	224				DialPlan1	
<input type="checkbox"/>	225	225				DialPlan1	
<input type="checkbox"/>	226	226				DialPlan1	
<input type="checkbox"/>	227	227				DialPlan1	

Total 477 items

This page will list all created extensions, to check or modify the extension properties please click  button.

Edit 312
✕

Profiles
Features
Advanced

Enable

Mobile Number

Dial Permission

Language

Outbound CID 1

Music On Hold

* Name

* Password Medium

Email

Outbound CID 2

- **Mobile Number:** Note the mobile phone number of the extension.
- **Dial Permission:** Defines which type of numbers the extension can dial.
- **Language:** Choose a specific system voice prompts.
- **Outbound CID (1/2):** Outbound CID will be passed to the called party while calling through the VoIP or digital trunk (E1/T1/BRI) lines, you can define 2 CIDs for each extension and choose which to be used by dial rules. By default, Outbound CID1 will be used by the dial rules. There's another Outbound CID option in the trunk settings, it has higher priority than the extension Outbound CID.
- **Music On Hold:** When the user is on hold, the caller will hear the music on hold, and it can be selected here.
- **Name:** Alias of this extension which can be the name of the extension user.
- **Password:** The password is used for phone registration or extension web portal logging. The password can be set manually or automatically generated by the IPPBX system. The auto-generated password consists of numbers, letters and special characters.
- **Email:** The email address of the extension user, can be used to receive extension QR code and voicemail to email notifications.

Add
✕

Profiles
Features
Advanced

Voicemail

Remote Extension

Video Call

WebRTC

Call Spy

Web Login

* Pickup Group

* Voicemail Password

Number Of Simultaneous Registrations

Video Codecs

Call Recording

* Register Expiration

Whitelist

- **Voicemail:** If this option is enabled, when an inbound call is not answered or the extension user is busy, the caller will be forwarded to voicemail.
- **Remote Extension:** If this option is enabled, users can remotely register extensions out of the LAN. For security reasons, users cannot enable this option with a weak password.
- **Video Call:** Enable/Disable the Video Call, it will be effective only when the endpoint supports video.
- **WebRTC:** If this option is enabled, the extension user will be able to make or receive calls via the Web (WebRTC technology) without any browser plug-in support.
- **Call Spy:** If this option is enabled, the Call Spy feature will allow the phone calls of this extension to be monitored by other extensions. please refer to Call Spy Feature Codes for how to monitor phone calls. And the dial permission used by the other extension needs to be enabled with Call Spy feature in the **Internal Permissions** section, otherwise call spy won't work.
- **Web Login:** If this option is enabled, the extension user can enter the extension number and password on the IPPBX's management address to login to the extension web portal. Users can view call records, check contact lists and send faxes, etc.
- **Voicemail Password:** Set the voicemail password. The extension user needs to enter the password when dialing *97 or *98 to enter the voice mailbox to check the voice message.
- **Number of Simultaneous Register:** The extensions could be registered on up to 5 different SIP endpoints at the same time, by default the value is 2. When there are already 2 registers, the 3rd register will be responded with a 403 error.
- **Video Codecs:** Only if two extensions with video call enabled use the same video codec can they establish a video call. Supported video codecs are H.261, H.263, H.263+, H.264, VP8.

- **Call Recording:** This is an auto-recording option, you can choose to record the inbound, outbound, or both inbound and outbound calls.
- **Register Expiration:** Registration Expiration can change the default registration expiration time of the endpoints, the default time is 1800 seconds.
- **Whitelist:** After setting the whitelist policy for incoming or outgoing calls, you can let the extension implement the specified whitelist policy.
- **Pickup Group:** Setting for extension pickup group. If several extensions are set under the same pickup group, when a certain extension is ringing but no one answers, other member extensions in the group can use the pickup feature to help him answer this call. The default value is 1 (1-64), please use ‘,’ to separate each group for multiple groups use.

Edit 312
✕

Profiles
Features
Advanced

* Transport Protocol 🔗

SRTP 🔗

NAT Support 🔗

Permit IP 🔗

Send PAI 🔗

* RTP Timeout 🔗 -- +

* DTMF Mode 🔗

* Qualify(sec.) 🔗 -- +

IAX2 Extension 🔗

* Qualify Timeout(sec.) 🔗 -- +



Send RPID 🔗


Inband Progress 🔗

Optional Codes	Selected Codes
Select all Total 8 items <input checked="" type="checkbox"/> Ulaw <input checked="" type="checkbox"/> Alaw <input checked="" type="checkbox"/> G.729 <input type="checkbox"/> GSM <input type="checkbox"/> G.722 <input type="checkbox"/> G.726 <input type="checkbox"/> Speex <input type="checkbox"/> G.723	Clear 3 items selected Alaw Ulaw G.729

- **Transport Protocol:** The transport protocol to be used by SIP signaling. By default, it uses UDP protocol, if you choose to use TCP or TLS please make sure the SIP IP phone or softphone uses the same protocol. Otherwise, you'll get "403" error on SIP register.
- **DTMF Mode:** Defines how the system detects DTMF tones, the default setting is RFC4733, it can be changed if necessary.

- **SRTP:** Secure Real-time Transport Protocol (SRTP) encrypts the RTP traffic to secure your VoIP phone calls. Before enabling this option you need to ensure the SIP endpoint can also support SRTP.
- **Qualify(S):** The IPPBX system sends a SIP OPTIONS command regularly to check if the device is still online.
- **NAT Support:** Enable this option if extension user or the phone is behind a router.
- **IAX Extension:** Enable this option to activate IAX protocol support.
- **Permit IP:** Defines which IP address or network address (either private IP or public IP) is allowed to register to this extension, register coming from other addresses will be dropped.
- **Qualify Timeout (S):** If a qualify message is not responded by the SIP endpoint within the “Qualify Timeout”, IP PBX system will consider the endpoint offline.
- **Send PAI:** Send the P Asserted Identity header. The P-Asserted-Identity contains the caller id information for the call on the INVITE SIP packet. Send the remote Party ID header. PAI and RPID are mutually exclusive you can set one or the other but not both.
- **Send RPID:** Send the Remote Party ID header. PAI and RPID are mutually exclusive you can set one or the other but not both.
- **RTP Timeout:** RTP timeout can be used to automatically hangup the call if no RTP traffic is received within 60 (default) seconds.
- **Inband Progress:** Set whether to send the ring tone via voice streaming.
- **Available Codec:** FCM5600 IPPBX system supports the following audio codecs G.711 (ulaw, alaw), G.722, G.726, G.729, GSM, Opus and Speex. You may choose the appropriate audio codecs from the **Available Codec** column and click to add to **Selected Codec** column.
- **Selected Codec:** Audio codecs you chose will be added here. The sequence of the audio codecs listed here is the sequence of the audio codecs to be used for negotiating the media of a phone call to be established.

If you want to create more extensions or if no extensions have been created because you skipped the quick setup wizard, you can click the  button to add a new extension or click the  button to create a batch of extensions.

 and  options are available for backup using MS xlsx file or adding extensions of the IPPBX system in bulk.

Batch Add
✕

Profiles
Features
Advanced

Enable

<p>* Start Extension Number <input type="text" value="104"/></p> <p>Start Outbound CID 1 <input type="text" value="Please Input"/></p> <p>Start Outbound CID 2 <input type="text" value="Please Input"/></p> <p>Password <input type="text" value="Please Input"/></p> <p>Language <input type="text" value="Default"/></p>	<p>* Count <input type="text" value="2"/> - +</p> <p>CID Calculation 1 <input type="text" value="+ 1"/></p> <p>CID Calculation 2 <input type="text" value="+ 1"/></p> <p>Dial Permission <input type="text" value="DialPlan1"/></p> <p>Music On Hold <input type="text" value="default"/></p>
---	--

- Define a **Start Extension Number** and the number of extensions to be created in the **Count** field.
- If you want to associate outbound CID numbers to the extensions, you'll need to specify the first CID number in the **Start Outbound CID (1/2)** field and in the **CID Calculation** field specify the calculating of the following CID numbers. Otherwise leave these fields blank.
- In the **Password** field you may leave it blank so the created extensions will use random passwords or you can define a password so the created extensions will share the same password.

As for other options, you may configure them accordingly per your demands. The features/options configured will be applied to all newly created extensions.

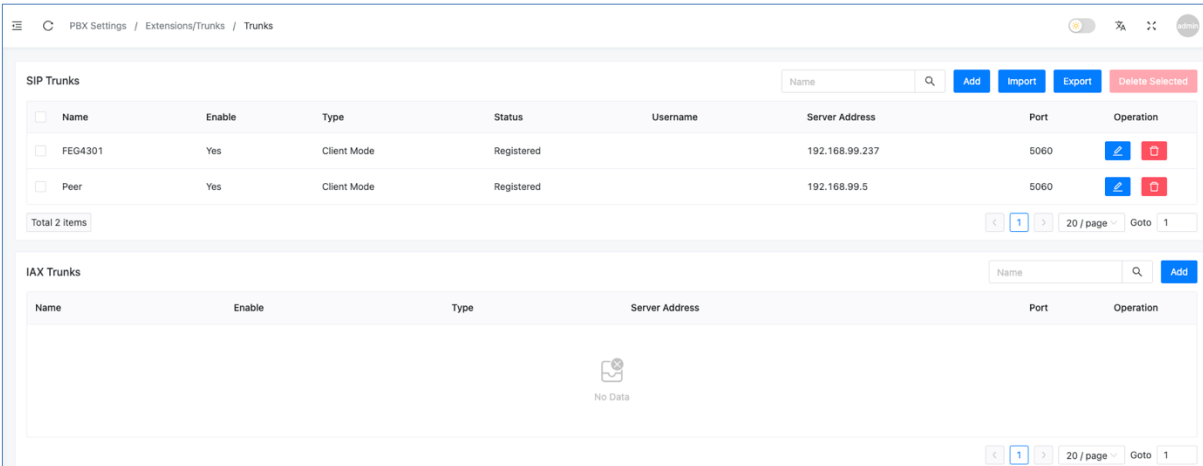
5.1.3 Trunks

SIP Trunks

Path: **PBX Setting -> Extensions/Trunks -> Trunks**

FCM5600 IPPBX can be registered as a SIP user agent to a SIP proxy (provider). If you have subscribed to a VoIP service from an ITSP (Internet Telephony Service Provider), then with the account details provided by them you can configure a SIP trunk on your FIBERME IPPBX system for the user extensions to share and make outbound phone calls.

To implement your SIP trunk account on the IPPBX system, you'll need to create a SIP trunk.



The screenshot shows the 'Trunks' configuration page in the FCM5600 IPPBX Admin interface. It is divided into two main sections: 'SIP Trunks' and 'IAX Trunks'.

SIP Trunks Section:

- Search bar: Name
- Buttons: Add, Import, Export, Delete Selected
- Table with columns: Name, Enable, Type, Status, Username, Server Address, Port, Operation
- Table content:

Name	Enable	Type	Status	Username	Server Address	Port	Operation
FEG4301	Yes	Client Mode	Registered		192.168.99.237	5060	[Edit] [Delete]
Peer	Yes	Client Mode	Registered		192.168.99.5	5060	[Edit] [Delete]
- Total 2 items
- Page controls: 1 / 20 / page, Goto 1

IAX Trunks Section:

- Search bar: Name
- Button: Add
- Table with columns: Name, Enable, Type, Server Address, Port, Operation
- Table content: No Data
- Page controls: 1 / 20 / page, Goto 1

Most of the trunk settings will be given by the service provider, settings that are not mentioned by the provider you may leave them blank or use default values.

- **Enable:** The trunk will be active and usable only if it's enabled.
- **Authentication:** If the service provider doesn't require a username and password for this account to register to their server then you can disable this option.
- **Server Address:** The SIP server domain or IP address.
- **Out Proxy Server:** SIP trunk proxy server's IP address.
- **Out Proxy Port:** SIP trunk proxy server's port number.
- **User Name:** Username provided by SIP Provider.
- **AuthUser:** AuthUser is the optional authorization user for the SIP server.
- **Password:** Password provided by SIP Provider.
- **Contact:** Contact user to use in an outbound call request through this trunk.
- **Retry Interval:** Once registration expired, retry interval is the number of seconds system will wait before attempting to send another register request to the server.
- **Identify By:** Identify by the user name and domain or the Authorization username.

- **Type:** In practical applications, client mode SIP trunks are the most commonly used to connect to the SIP providers for low cost, long distance and international phone calls, while server mode is only used when users want to do SIP trunking between IPPBXs.
- **Registration Expiration:** Expiration time of registration in seconds.
- **Max Retry:** Defines how many times the IPPBX system will attempt to register to the server before permanently giving up.

Edit FEG4301
✕

Basic
Other

Fax Detect

SRTP

Client URI

Server URI

AOR Contact

* Call Recording

From User

From Domain

* DTMF Mode

Send PAI

RTP Timeout

Fax DST

NAT Support

* Transport Protocol

* Prompts Language

Simultaneous Call

* Preferred Outbound CID

Outbound CID

Dial Permission

* Video Codecs

Send RPID

Qualify

Available codes	Selected codes
<input checked="" type="checkbox"/> Ulaw <input checked="" type="checkbox"/> Alaw <input checked="" type="checkbox"/> G.729 <input type="checkbox"/> GSM	Alaw Ulaw G.729

- **Fax Detect:** Enable/disable fax detection on this trunk.
- **SRTP:** Secure Real-time Transport Protocol (SRTP) encrypts the RTP traffic to secure your VoIP phone calls. Before enabling this option, you need to ensure the end point can also support SRTP.
- **Client URI:** Client SIP URI used when attempting outbound registration (e.g. SIP:1234567890@sip.example.com:5060).
- **Server URI:** SIP URI of the server to register against (e.g. sip:sip.example.com:5060).
- **AOR Contact:** Address of records, it uses the same format as the client URI.

- **Call Recording:** Enable/disable call recording on this trunk. If enabled, all phone calls going in or out will all be recorded.
- **From User:** Username to use in “From” header for sending outbound call requests to this trunk.
- **From Domain:** Your service provider’s domain name.
- **DTMF Mode:** Used to inform the system how to detect the DTMF key press. Choices are Inband, rfc4733, SIP info and Auto.
- **Send PAI:** Send the P Asserted Identity header. The P-Asserted-Identity contains the caller id information for the call on the INVITE SIP packet. PAI and RPID are mutually exclusive you can set one or the other but not both.
- **RTP Timeout:** RTP Timeout can be used to automatically hangup the call if not RTP traffic is received within 60 (default) seconds.
- **Qualify:** Qualify will cause the server sending SIP OPTIONS command regularly to check that the device is still online.
- **NAT Support:** With this option enabled, Asterisk may override the address/port information specified in the SIP/SDP messages, and use the information (sender address) supplied by the network stack instead. This feature is often required when there is a firewall located between the PBX and the service provider.
- **Transport Protocol:** To set the VoIP trunk to use UDP, TCP or TLS as the transport protocol, in most cases the providers use UDP as default transport protocol.
- **Prompts Language:** You can choose a desired language of the system voice prompts to play for the incoming calls from this trunk. For example, if the call is not answered or the user is busy, the IPPBX system will notify the caller to leave a voice message in the language you set.
- **Simultaneous Calls:** This option will limit the number of simultaneous outbound calls can be made through this trunk, leave it blank as not limited.
- **Preferred Outbound CID:** To set preferred outbound CID of this trunk of the extensions.
- **Outbound CID:** The number you want to display to the called party while dialing out through this trunk. It depends on the service provider whether it works or not.
- **Dial Permission:** Custom dial permission for this trunk, by default it uses the “default” dial permission. Configure only if this trunk is for branch office integration, so calls coming from the other side can dial out from this IPPBX trunk directly. DO NOT change unless you fully understand how this feature works.
- **Video Codecs:** If the ITSP supports video calls then you can enable compatible video codecs here for video phone calls.
- **Send RPID:** Send the Remote Party ID header. PAI and RPID are mutually exclusive you can set one or the other but not both.

- **Available Codec:** FCM5600 IPPBX system supports the following audio codecs G.711 (ulaw, alaw), G.722, G.726, G.729, GSM, Opus and Speex. You may choose the appropriate audio codecs from here and click to add to Selected Codec.
- **Selected Codec:** Audio codecs you chose will be added here. The sequence of the audio codecs listed here is the sequence of the audio codecs to be used for negotiating the media of a phone call to be established.

IAX Trunks

Path: **Telephony -> Outbound Control -> Trunks**

IAX trunks can be used to interconnect 2 IPPBXs in remote locations. You have to create a “Server Mode” IAX trunk on one IPPBX and a “Client Mode” on the other IPPBX. The server mode IAX trunk should define username and password, the username and password should be applied on the client mode IAX trunk.

- **Trunk Name:** It should be the username of the IAX trunk account.
- **Authentication:** If the “Server Mode” trunk hasn’t enabled this option, then it doesn’t require a username and password for this account, you can disable this option and specify the Server Address for authentication.
- **Server Address:** The IAX server domain or IP address.
- **User Name:** Username provided by IAXserver.
- **Password:** Password provided by IAXserver.
- **Outbound CID:** The number you want to display to the called party while dialing out through this trunk.
- **Dial Permission:** Custom dial permission for this trunk, by default it uses the “default” dial permission. Configure only if this trunk is for remote IPPBX integration, so calls coming from the other side can dial out from this IPPBX trunk directly. DO NOT change unless you fully understand how this feature works.
- **Call Recording:** Enable/disable call recording on this trunk. If enabled, all phone calls going in or out will all be recorded.
- **Type:** Server Mode IAX trunk provides username and password for the Client Mode IAX trunk to register.
- **Preferred Outbound CID:** To set preferred outbound CID of this trunk of the extensions.
- **Prompts Language:** You can choose a desired language of the system voice prompts to play for the incoming calls from this trunk. For example, if the call is not answered or the user is busy, the IPPBX system will notify the caller to leave a voice message in the language you set.
- **Available Codec:** FCM5600 IPPBX system supports audio codecs such as G.711 (ulaw, alaw),

G.722, G.726, G.729, GSM, Opus and Speex. You may choose the appropriate audio codecs from here and click to add to Select Codec.

- **Selected Codec:** Audio codecs you choose will be added here. The sequence of the audio codecs listed here is the sequence of the audio codecs to be used for negotiating the media of a phone call to be established.

5.2 Inbound Control

Path: *PBX Setting -> Inbound Control*

The Inbound Control section is where you define how FIBERME FCM5600 IPPBX system handles incoming calls. Typically, you determine the phone number that outside callers have called (DID Number) and then indicate which extension, Ring Group, Voicemail, or other destination to which the call should be directed.

5.2.1 IVR

Path: *PBX Settings -> Inbound Control -> IVR*

IVR, or Interactive Voice Response, is responsible for the menus people hear and respond to when they call up a company or business and hear the words for example: "press 1 for sales, press 2 for marketing, press 0 to speak to the operator,".

Before configuring IVR menus you will first need to create inbound call destinations, for example, **Extensions**, **Departments** (ring groups), **IVR prompts**, **Call Queues**, etc.

If you want to create multi-layer IVR menus, you may need to create the sub-layers at first. In order to create an IVR menu, please click on the **Add** button, you'll see a popup dialog as below:

Add
✕


<p>* Name <input type="text" value="Please Input"/></p> <p>* Voice Prompts <input type="text" value="Please Select"/></p> <p>Dial Extension <input checked="" type="checkbox"/></p> <p>Language <input type="text" value="Default"/></p> <p>Events <input type="text" value="No Press"/> <input type="text" value="Hangup"/></p> <p><input type="text" value="Invalid Key"/> <input type="text" value="Hangup"/> <input style="margin-left: 10px;" type="button" value="+"/></p>	<p>* Number <input type="text" value="7000"/></p> <p>Loop Count <input type="text" value="1"/></p> <p>Dial Permission <input type="text" value="Extension"/></p> <p>* Press Key Timeout(s) <input type="text" value="3"/> <input type="button" value="-"/> <input style="margin-left: 5px;" type="button" value="+"/></p>
--	---

- In the **Name** field a name is required to identify this IVR menu.
- In the **Number** field a number had been created for this IVR menu for user being able to dial this number and test the IVR options.
- In **Voice Prompts** drop-down list, select a pre-recorded voice prompt for this IVR menu. The prompts will be played to the callers as they enter the IVR. The voice prompts must be uploaded or recorded from the **PBX Settings -> Voice Prompts -> IVR Prompts** page.
- In **Loop Count** drop-down list, select the number of times to playback this IVR prompts before callers pressing a key.
- **Dial Extension** switch could be enabled for callers to dial specific numbers upon this IVR menu if they already knew which number should be dialed, so the callers don't have to listen to all the options of this IVR.
- If **Dial Extension** is enabled a default **Dial Permission** named **Extension** will be applied for callers being able to dial internal extensions upon this IVR menu, if you wish callers could dial some more numbers you may select another dial permission here. (Not Recommended)
- **Language** option determines which language of the system voice prompts the callers will hear if they landed on some inbound destinations that will play system voice prompts via this IVR menu, voicemail for example.
- **Press Key Timeout(s)**: The maximum interval time in seconds between pressing two keys.
- **Events** are the IVR options to be configured according to the instructions you have specified in the selected IVR prompts. Available key presses could be set from **0** to **9**, ***** and **#**. If the caller presses the key which are not specified, and it will be handled by the "Invalid Key" option. And if the caller didn't press any key during the whole IVR process, the call will be handled by the "No Press" option.

5.2.2 Call Queue

Path: **PBX Settings -> Inbound Control -> Call Queue**

A call queue places incoming calls in line to be answered while extension users are busy with other calls. The queued calls are distributed to the next available extension user in the order received. Once a call queue has been created, it can be assigned to specific extensions and configured to feature greetings, messages, and hold music.

To create a call queue, please click on the  button, a popup window will show up as below:

Add ✕

[General Settings](#)
 [Advanced Settings](#)
 [Announcements](#)

* Name

* Number

* Ring Strategy

* Music On Hold

Static Agents

Dynamic Agents

* Destination If No Answer

First please complete the **General Settings**.

- In **Call Queue Name** field specify a name to identify this queue.
- In **Queue Number** field a default number is given. The number could be changed within the Paging Group Extension Number Range listed on **Telephony -> Preferences -> Global PBX Options** page, Extension Ranges section.
- **Ring Strategy** sets the method how you wish the queue agent extensions to ring when there's incoming call to this queue.
- **Ring All**: Ring all available agents until one answers(default).
- **Leastrecent**: Ring the extension of the Agent who has least recently received a call.
- **Fewestcalls**: Ring the extension of the Agent who has taken the fewest number of calls.
- **Random**: Ring the extension of a random Agent.
- **RRMemory**: The system remembers which agent was last called and begins the round robin with the next agent.
- **Linear**: Starting with the first agent, ring the extension of each agent in turn until the call is answered.
- **RROrdered**: Same as RRMemory, except the queue member order is preserved.
- In the **Music On Hold** drop-down list select a music folder as hold music when callers are waiting in the queue.

- After **Agent Penalty** is enabled, and the Ring Strategy is on the Linear mode, the incoming calls in the queue will ring the agents in the order of the static agent extension numbers list.
- **Static Agents** are extensions that are assumed to always be in the queue. Static agents do not need to “log in” to the queue, and cannot “log out” of the queue.
- **Dynamic Agents** are extensions that can log in and out of the queue. Extensions selected here will NOT automatically be logged in to the queue.
- **Destination if no answer** sets the final destination for the callers if no one answers the call when they were in the queue.

More advanced options for call queue is available, please click on “Advanced Settings” to show advanced options, they are optional but might be useful to improve the callers’ experiences.

Add
✕

General Settings
Advanced Settings
Announcements

Auto Fill

* Agent Timeout(sec.) -- +

* Auto Pause ▾

* Wrap Up Time(sec.) -- +

Report Hold Time

* Max Callers -- +

Add Queue Name Caller ID

Max Wait Time(sec.)

Join Empty

Leave When Empty

- **Auto Fill** if it's set to be Yes, and multiple agents are available, the PBX will send one call to each waiting agent (depending on the ring strategy). Otherwise, it will hold all calls while it tries to find an agent for the top call in the queue, making the other callers wait.
- **Agent Time Out** specifies the number of seconds to ring an agent's extension before sending the call to the next Agent (based on Ring Strategy).
- If an agent's extension rings and the agent fails to answer the call, **Auto Pause** option can automatically pause that agent to stop them receiving further calls from the queue.
- **Wrap Up time** is the amount of time in seconds that an agent has to complete work on a call after which the call is disconnected.
- If **Report Hold Time** is enabled, it will report to the agent about how long the caller had been waiting in the queue.
- The value of **Max Callers** limits the maximum amount of callers can wait in the queue (Default is 0 -- unlimited). When the maximum number of callers in the queue is reached, subsequent callers will be sent to the **If no answer** destination.
- If **Add Queue Name Caller ID** option is enabled, when an incoming call is distributed to an agent the queue name will be displayed on the phone screen along with the caller ID. So a call queue agent knows which call queue the call is coming from. This feature is helpful if an agent belongs to multiple call queues.
- Calls that have been waiting in the queue for **Max Wait Time (Sec)** will be sent to the **If no answer** destination. If left blank, there will not be any time limitation of waiting time.
- **Join Empty** option allows callers to enter the queue when no agents are available. If this option is not enabled, callers will not be able to enter the queue without available agents.
- callers will be sent to the **If no answer** destination.
- **Leave When Empty** option if it's enabled and calls are still in the queue when the last agent logs out, the remaining callers in the Queue will be transferred to the If no answer destination. This option cannot be used with Join Empty at the same time.

You may set the system to playback announcements to the callers while they are waiting in the queue. Please click on the "Announcements" to setup customized announcements.

Add
✕

General Settings
Advanced Settings
Announcements

Caller Position Announcements

* Announce Hold Time ⓘ

Announce Position ⓘ

* Broadcast Frequency(sec.) ⓘ -- +

Periodic Announcements

* Repeat Frequency(sec.) ⓘ -- +

Announcements Prompts ⓘ

- **Caller Position Announcements** is used to tell the callers how they've been waiting and the position in the queue.
- **Announce Hold Time:** Announce to the callers of the time they have been waiting, the first minute callers waiting in the queue will not hear such announcements.
- **Announce Position:** If set to be Yes, the system will announce the position of the caller is currently waiting in the queue.
- **Broadcast Frequency (Sec):** To defines how often to announce queue position and estimate hold time.
- **Periodic Announcements** can be used to periodically playback voice prompts to the callers waiting in the queue.
- Repeat Frequency (Sec): The time interval to repeat this periodic announcements.
- Announcements Prompts: To select a voice prompt to be periodically played to the waiting callers.

After setting up call queue, you may use internal extensions (non-agent extensions) to call the queue number to verify the queue settings.

5.2.3 Time Conditions

Path: **PBX Settings -> Inbound Control -> Time Conditions**

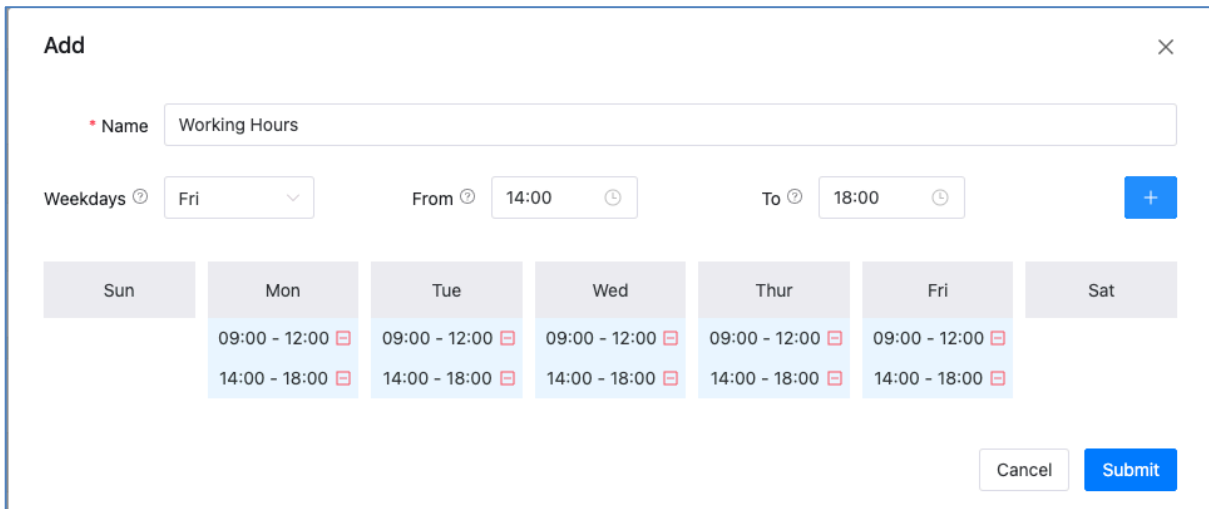
Time conditions in FCM5600 IPPBX allow you to control what happens to inbound calls both during and outside (weekends/holidays) normal business hours.

Time condition settings include Time Rule, Weekday and Holiday settings.

- Time Rule:
- Weekdays:
- Holidays:

To create a time rule you need first set up weekdays and holidays.

To set up weekdays you may modify the default one or create a new one by clicking on **Add** button.



Add [Close]

* Name: Working Hours

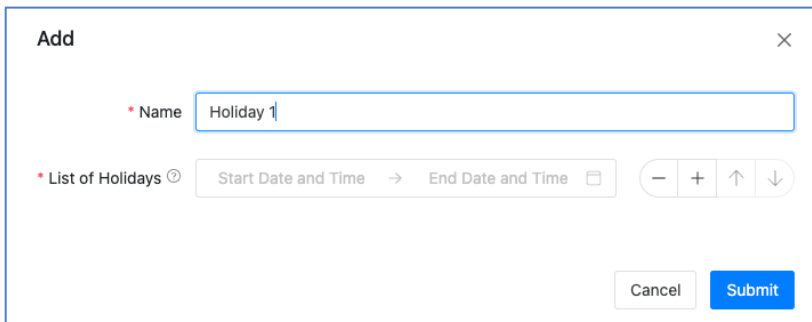
Weekdays: Fri [Dropdown] From: 14:00 [Dropdown] To: 18:00 [Dropdown] [Add]

Sun	Mon	Tue	Wed	Thur	Fri	Sat
	09:00 - 12:00 [Edit]	09:00 - 12:00 [Edit]	09:00 - 12:00 [Edit]	09:00 - 12:00 [Edit]	09:00 - 12:00 [Edit]	
	14:00 - 18:00 [Edit]	14:00 - 18:00 [Edit]	14:00 - 18:00 [Edit]	14:00 - 18:00 [Edit]	14:00 - 18:00 [Edit]	

[Cancel] [Submit]

This example shows the company opens from Monday to Friday. On each weekday, it opens from 9 am to 12 pm, after a 2-hour break then opens from 2 pm to 6 pm. Any other time duration unspecified will be considered as non-business hours.

In order to exclude holidays from the weekdays, you'll also have to set up holidays.



Add [Close]

* Name: Holiday

* List of Holidays [Info]

Start Date and Time	End Date and Time	
		[Add] [Remove] [Up] [Down]

[Cancel] [Submit]

Please ensure you add all upcoming holidays to the holiday list. Now you have all

prerequisites to set up a time rule.

Now you could apply this time rule to the **Inbound Routes**.

In the above example, there are only business hours and non-business hours for inbound calls. If you want inbound calls during your holidays to be handled by a holiday IVR, you could setup another IVR dedicated for holidays.

5.2.4 Inbound Routes

Path: **PBX Setting -> Inbound Control -> Inbound Routes**

The Inbound Routes settings tell your IPPBX system where to send those inbound calls coming in from the trunks. Calls can be sent to a variety of destinations, including extensions, departments (ring groups), call queues, IVRs, DISAs, conferences, paging groups, voicemail, fax, etc.

Office Closed ⓘ

• Destination Type ⓘ

• Inbound Destination ⓘ

Status ⓘ

Office Closed is an extending of time conditions, you can manually activate Office Closed by feature code. This feature allows much more flexible time conditions to be temporarily applied for the offices which may have some unscheduled businesses and activities off the time table of the time conditions. For the Office Closed feature codes and instructions, please refer to Feature Codes.

The Inbound Routes are configured per each trunk. You may set different inbound destinations for different trunks.

<input type="checkbox"/> Trunk Name	Destination Type	Inbound Destination	Distinctive Ringtone	Operation
<input type="checkbox"/> FEG4301	Queue	Test Queue[6500]		<input type="button" value="Edit"/>
<input type="checkbox"/> Peer	Extension	899[899]		<input type="button" value="Edit"/>

Total 2 items < 1 > 20 / page Goto 1

Please click on  button to configure inbound routes for each trunk,

Edit FEG4301
✕

* Destination Type

* Inbound Destination

Distinctive Ringtone

In the Inbound Destination field select a desired inbound destination for inbound calls from this trunk.

Distinctive Ringtone is optional, if needed, you may specify the ringtone name of the phone, so when the callers call in from this trunk the phone will ring this specific ringtone. It requires the phone support distinctive ringtone feature.

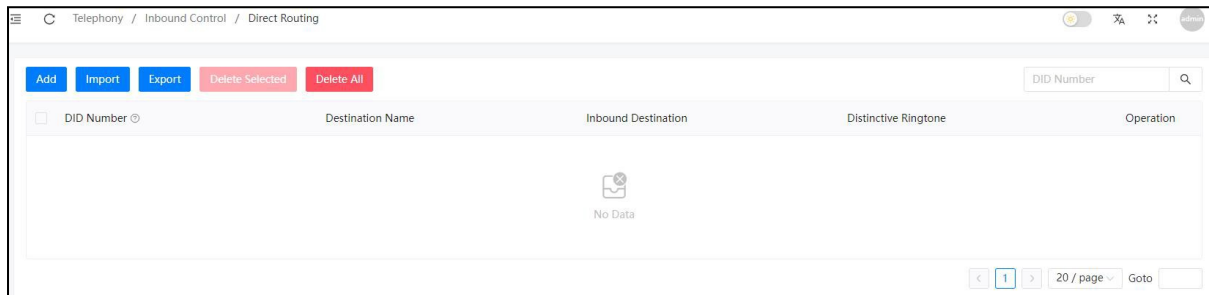
This is how you configure inbound routes for a trunk, you may configure the same inbound routes for other trunks or use different inbound route settings per your requirements.

5.2.5 CID/DID Routing

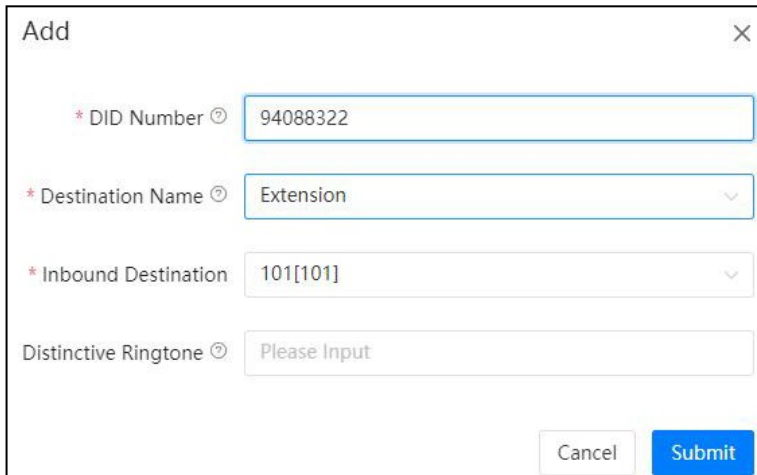
Path: **PBX Setting -> Inbound Control -> CID/DID Routing**

You may set up CID/DID Routing based on the DID numbers of your trunk lines and the phone numbers of the external callers. CID/DID Routing has higher priority than time conditions (unless the inbound destination is a time rule) and other general inbound routes.

CID/DID Routing based on DID numbers will cause the inbound calls which dialed the specified DID number to a specific call destination without the limitation of any other inbound settings. To add a CID/DID Routing rule based on DID number, please click on the "Add" button as shown below.



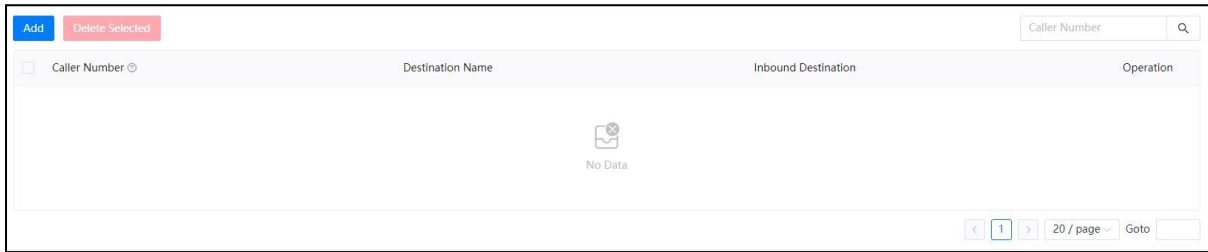
In the popup window, specify one of your DID numbers, and assign a call destination for all inbound calls by calling this DID number.



In the above example, 94088322 is one of your DID numbers, you may configure it with an extension number, when someone calls this number, the call will then directly go to the selected extension.

In the **Distinctive Ringtone** field you may specify the ringtone name of the phone, so when the callers call the DID number and the call goes to this extension the phone will ring this specific ringtone. It requires the phone support distinctive ringtone feature.

To add a CID/DID Routing rule base on the caller's number, please click "Add" button as shown below.



In the popup window, specify the caller’s number, and assign a call destination for inbound calls from this external phone number.

Once this Direct Routing is created, all phone calls coming from the number 85337096 will then all go to extension 101, no matter when and from which trunk the call is coming in.

Add ✕

* Caller Number

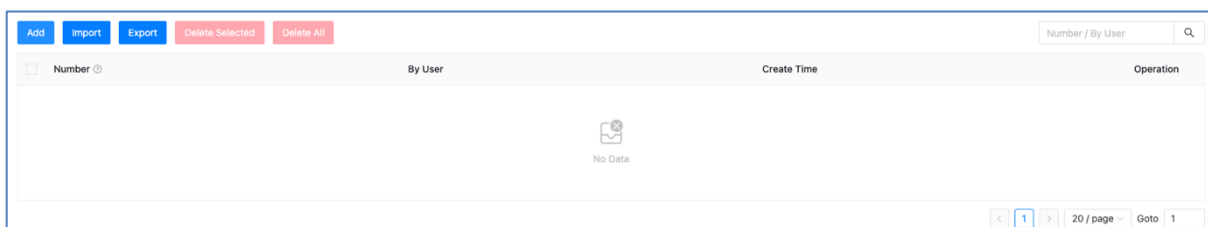
* Destination Name

* Inbound Destination

5.2.6 Blacklist

Path: **PBX Setting -> Inbound Control -> Blacklist**

Blacklist feature allows you to create a list of numbers that are not allowed to call in to the IPPBX system. Blacklist could be managed by both the admin user and operator user. The extension user could also add numbers to the system blacklist by using Blacklist Feature Codes.



By specifying a number in the top right number blank, you may add a number to the system blacklist.

If you want to share the blacklist numbers on other IPPBX systems, you may download it by clicking the **Export** button to download all blacklist numbers in a file and upload on other IPPBX systems.

5.3 Outbound Control

By default if you've not configured any outbound control settings, the extension users are not able to make outbound phone calls yet. Please follow the instructions of this chapter to configure the IPPBX system for outbound phone calls.

5.3.1 Dial Rules

Path: **PBX Settings -> Outbound Control -> Dial Rules**

On the FIBERME FCM5600 IPPBX system you can setup different dial rules, for users to dial numbers in different format/pattern and cause the IPPBX system to call out through different trunk lines. For example, users dial the numbers with a prefix 9 to call out through the CO lines (land lines). Or dial the numbers with a prefix 00 to call out through the VoIP lines (SIP trunks).

Click on **Add** button to create a dial rule name, below is an example dial rule.

Edit ✕

* Name

Click on the “+” button to create new dialing rules.

Strip	Dial Pattern	Via Trunk/Trunks	Operation
E1			+ ↶ ✕

Add
✕

Time Rule ⊙

Strip ⊙

PIN Sets ⊙

Call Time limit(sec.) ⊙ − +

Prepend ⊙

Dial Pattern ⊙

Outbound CID ⊙

Via Trunk/Trunks


Call Method ⊙

Available Trunks Select all Total 2 items

FEG4301

Peer

Selected Trunks 0 items selected



No Data

- In the **Time Rules** dropdown list, you may select a time condition for this dial rule, so this dial rule will only be available to be used at business hours.
- **Prepend** option is used to always add specific digit/digits in front of the actual dialed number after the **STRIP** is deleted. These extra digits will be sent along with the actual number to the service provider to exchange. For example, if you want to always add an area code in front of the dialed number, you can specify the area code in front of the dialed number, you can specify the area code here, otherwise, leave this field blank.
- **Strip** is the first digit users have to dial while they want to make calls through the trunk/trunks selected in this dial rule. The system will strip the prefix from the number that is sent to the trunk.
- **Dial Patterns** act like a filter for matching numbers dialed with trunks. The various patterns you can enter are similar to Asterisk's definition of them:
 - **X** — Refers to any digit between 0 and 9
 - **N** — Refers to any digit between 2 and 9
 - **Z** — Any digit that is not zero. (E.g. 1 to 9)
 - **.** — Wildcard. Match any number of anything. Must match *something*.
- **Pin Set** is a collection of PIN codes for granting outbound phone calls.
- **Outbound CID:** Choose between Outbound CID1 and Outbound CID2 to send to the called

party. When the extension user make outbound phone calls by using this dial rule, the chosen outbound CID number will be used. So in the below **Selected Trunks** field, select the trunks need to be used, and the service provider need to support users passing outbound CIDs.

- **Call Time Limit:** The limited time of call conversation can be made while using this dial rule. The limitation can be set from 60 to 3600 seconds.
- **Call Method** sets how to use the selected trunks for outbound phone calls.
- **Linear:** Always take the first available trunk, if the first trunk is busy it will try the second trunk, if the second trunk is busy it will try the third, and so on.
- **Linear Cycle:** Always take the next trunk, the trunk which the last had taken will not be used, it will call out through the next one directly.
- Double click one of the trunks or drag-and-drop to move the trunks from **Available Trunks** field to **Selected Trunks** field. The selected trunks will be used by this dial rule for outbound phone calls.

Note: If you want all users to use the same dial rule for outbound phone calls, a dial prefix may not be necessary. But please make sure all available trunks should be included in the Selected Trunks field, otherwise unselected trunks will never be used.

If you want to set different dial rules please make sure the dial rules use different dial prefixes.

5.3.2 Dial Permissions

Path: **Telephony -> Outbound Control -> Dial Permissions**

A dial permission consists of outbound dial permissions (dial rules) and internal dial permissions. Each extension number had been assigned with a dial permission. Dial rules are created for dial outbound phone calls, internal dial permissions are used for controlling extension numbers by using local phone system features.

You may create several different dial permissions. By assigning the extension numbers with different dial permissions you may limit the extension users to dial certain outbound phone calls and use certain local phone system features.

Click on **Add** button to create a new dial permission or you may use the default dial permission.

Edit
✕

* Name

Dial Rules

Available Rules Unselect all Total 1 items

DialOut

Selected Rules Clear 1 items selected

DialOut

Internal Permissions

Extension

Department

Conference

DISA

Feature Codes

IVR

Paging & Intercom

Call Parking

Call Pickup

Call Queue

Call Spy

Seize CO Line

In the **Dial Rules** section by moving the dial rules from the **Available Rules** field to the **Selected Rules** field to enable the dial rules in this dial permission. In the above-given example, 2 dial rules had been enabled. The “call-pstn” rule is used to make phone calls through CO lines (land lines). The “call-voip” rule is used to make phone calls through the SIP trunk. So if you assign this dial permission to the extension users, they will be able to make outbound phone call both through CO lines and the SIP trunk.

In the **Internal Permissions** section by switching the internal call features on/off to enable/disable the call features.

- **Extension:** Allow/Disallow dialing other extension numbers.
- **Paging & Intercom:** Allow/Disallow dialing paging & intercom group numbers.
- **Department:** Allow/Disallow dialing other department numbers.
- **Call Parking:** Allow/Disallow answering the parked calls.
- **Conference:** Allow/Disallow using conference feature.
- **Call Pickup:** Allow/Disallow pickup phone calls on other extensions.
- **DISA:** Allow/Disallow using DISA feature.
- **Call Queue:** Allow/Disallow dialing the call queue numbers.
- **Feature Codes:** Allow/Disallow using feature codes.
- **Call Spy:** Allow/Disallow spying on other extensions' phone calls.
- **IVR:** Allow/Disallow dialing IVR extensions.
- **Seize CO Line:** Allow/Disallow the extension user to dial the FXO trunk BLF code to seize the line and make outbound phone calls directly.

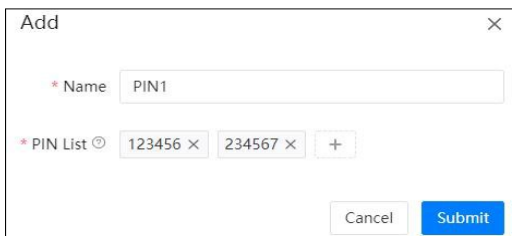
By default, all extensions use the default dial permission "DialPlan1", if you have created new dial permissions, please don't forget to assign them to the extensions from **PBX Settings -> Extensions/Trunks -> IP Extensions**

5.3.3 PIN Sets

Path: **PBX Settings -> Outbound Control -> PIN Sets**

Pin sets can be used to secure your IPPBX system phone services and in particular for outbound dial rules and DISA.

Each PIN Set consists of a series of PIN Codes.



The PIN codes could be any digits that you want, but usually recommended it to be 3 to 5 digits meaningless numbers.

You could distribute these PIN codes out to each of the extension users or several of them to share a same PIN per your demand. If the PIN set is implemented on a dial rule or DISA, the IPPBX system will ask them to enter one of those PIN codes before they can call out.

The PIN codes also can be used to query call logs and recordings, so even if the extension user

dialed a number from another extension if PIN code is used you'll know who actually made that call.

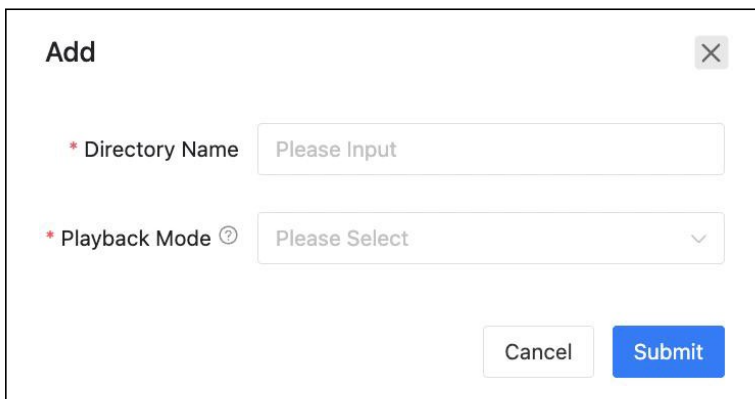
5.4 Voice Prompts

5.4.1 Music On Hold


Path: **PBX Settings -> Voice Prompts -> Music On Hold**

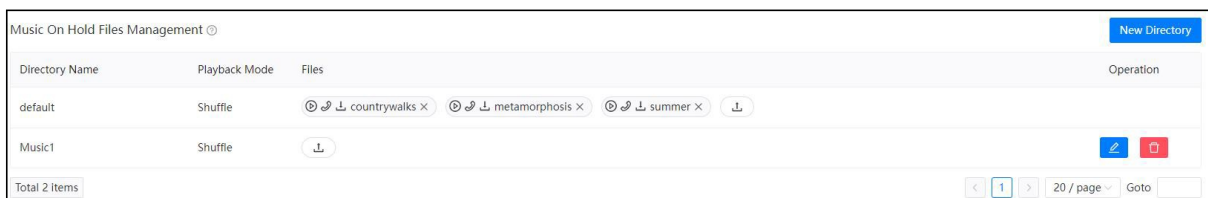
Music On Hold (MOH) is commonly known on an IPPBX system allows audio files (such as WAV or MP3 files) to be uploaded to the IPPBX system and played back when a caller is placed on hold or is waiting in a queue.

Audio files are managed by folder basis. You may use the system default MOH folder as on hold music or you may create new folders and upload your custom music files. Please first click on **New Directory** to create a new MOH folder.



Give this folder a name and set the playback mode as shuffle (random playback) or in turn (playback in order). Once done click on "Submit".

Now click on  button to upload audio files to the newly created folder one by one. Supported File Format: MP3, WAV (8KHz, 16bit, Mono)



Directory Name	Playback Mode	Files	Operation
default	Shuffle	countrywalks x metamorphosis x summer x	
Music1	Shuffle		

5.4.2 IVR Prompts

Path: **PBX Settings -> Voice Prompts -> IVR Prompts**

To configure an IVR menu on FCM5600 IPPBX system you'll first need to record your IVR prompts, these IVR prompts will communicate with the callers about the menu options that

they have e.g. press one for sales.

Always be sure that the recorded IVR prompts will match the options to be set up in the IVR. If you change your IVR options, don't forget to change your recording!

The IVR prompts are pre-recorded and then uploaded to the FCM5600 IPPBX system.



Files	Format	Play	Operation
closed	wav		
closed_cn	wav		
welcome	wav		
welcome_cn	wav		

The pre-recorded audio could be MP3 or WAV (16bit, 8KHz, Mono) format.

After uploading, you may playback on the web by clicking button or playback on a phone by clicking on the button.

If you want to record the voice prompts by using an IP phone extension, please click on the **Recording** button, in the pop-up dialog, please define a name for the audio file to be recorded and select an extension which will be used to do the recording.



When done, click on Submit and the selected extension will ring. After the user pick up the phone, after the peep record your message and hang-up. When recording is done, the newly recorded audio will be listed on this page and ready to be used for setup IVR.

5.4.3 Custom Prompts

Path: **PBX Settings -> Voice Prompts -> Other Custom Prompts**

Custom prompts are to be used by call queue, call forward and some other advanced features, where customized voice prompts required.

You could record the voice prompts in MP3 or WAV (16bit, 8000Hz, mono) format and upload here. Then when you setup call queue periodic announcements you could select the

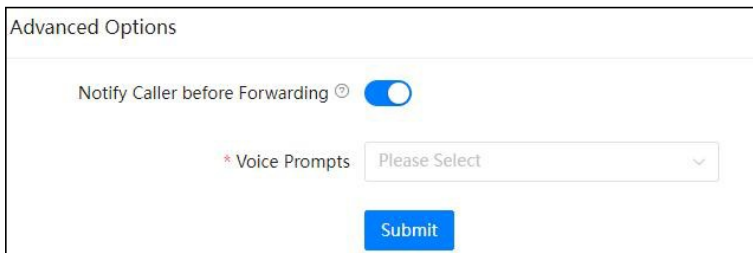
customized voice prompts, or when you setup call forward notify message you could set the IPPBX system to notify callers before forwarding their calls.

5.5 Advanced Features

5.5.1 Call Forward

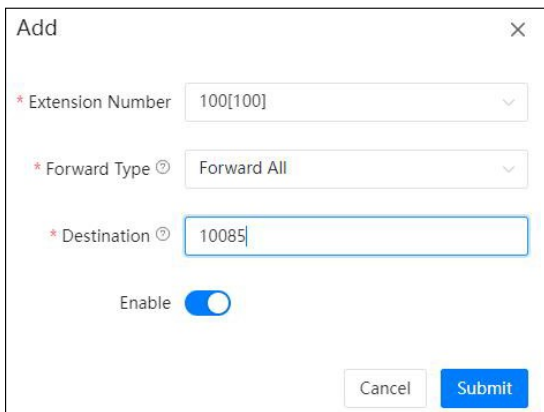
Path: **PBX Settings -> Advanced Features -> Call Forward**

Call forward allows calls to an extension to be forwarded to a specific internal extension number or an external phone number. According to different application scenario, the forward type can be set as Forward All, Forward on Busy, Forward When Unavailable, No Answer and Busy, or No Answer and Unavailable.



- **Notify Caller before Forwarding** option allows you to choose a voice prompt to be played to the caller to notify caller that the call will be forwarded. The voice prompts is uploaded from **PBX Settings -> Voice Prompts -> Other Custom Prompts** page. If this option is not enabled, the call will be forwarded without notifying the caller.

To configure call forward please click on the **Add** button. And follow the explanations to complete the configurations as below.



- In the **Extension Number** drop-down list select the extension to be configured with call forward.
- In **Forward Type** drop-down list select the condition of when to forward the incoming calls.
- In the **Destination** field specify the number to receive the forwarded phone calls. If it's another internal extension number, just fill in with that extension number. If it's an external number, you'll have to specify the dial prefix in front of the actual number. In this case, the actual number is 65302385, the dial prefix is 9.

In the forward list, you may disable or enable items based on requirements.

<input type="checkbox"/>	Extension Number	Forward Type ⓘ	Timeout(sec.)	Destination	Enable	Operation
<input type="checkbox"/>	101	Forward All	0	965302385	<input checked="" type="checkbox"/>	✎ ✖
<input type="checkbox"/>	100	Forward All	0	10085	<input checked="" type="checkbox"/>	✎ ✖

Total 2 items

Call forward could be configured by Admin user and the operator user, and even by extension user from the extension user web portal or by extension users from their phones by feature codes, please refer to Call Forward feature codes.

5.5.2 Follow Me

Path: **PBX Settings** -> **Advanced Features** -> **Follow Me**

Click on [Add](#) add a follow me feature like below.

Add ✕

* Extension Number

* Ring Duration(sec.) ⓘ - +

* Follow Me List ⓘ

<input type="text" value="101"/>	<input type="text" value="10"/> - +	- + ↑ ↓
<input type="text" value="921432368"/>	<input type="text" value="10"/> - +	- + ↑ ↓

- Select the **Extension** which will be configured with Follow Me.
- **Ring Duration (Sec)**: To set the time in seconds to ring the extension before Follow Me process starts.
- **Follow Me List**: The list of numbers to be reached in order.
- **Number and Timeout (Sec)**: The number to be reached and the time to ring this number before trying the next one. If the number is an external number, don't forget to add a dial prefix in front of it.

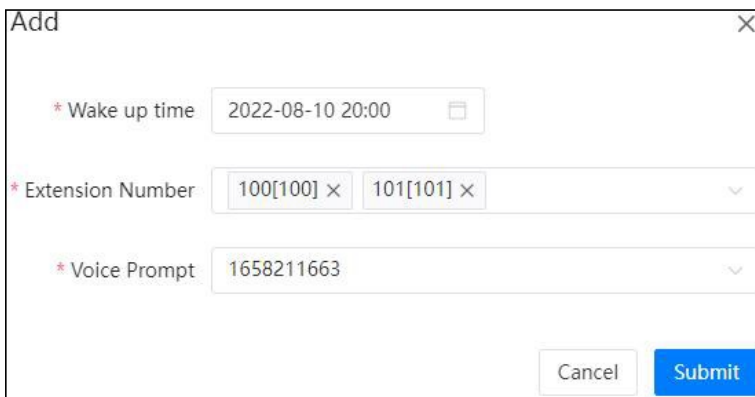
Take the above settings as example, when extension 100 gets an incoming call, if it's not answered in 15 seconds, the call will be forwarded firstly to 101 and ring this extension for 10 seconds, if still not answered, it will try number 921432368 (9 is the dial prefix, not part of the number) for another 10 seconds. If extension 101 answered the call then 921432368 will not be called. If the call didn't answer by any of the numbers listed in **Follow Me List**, the Follow Me process will end and the caller will be disconnected.

5.5.3 Wake Up Call

Path: **PBX Settings -> Advanced Features -> Wake Up Calls**

Wake Up Call feature could be used to schedule reminders to the user extensions. Wakeup calls could be scheduled by admin user from admin Web interface, by operator user from operator Web interface, or could be scheduled by extension users by dialing Wake Up Call feature codes.

To schedule a wakeup call from admin user Web interface, please click on **Add** button, in the popup window set the time of the wakeup call and select the extension/extensions to be called at the scheduled time point.





















- Click on **Wake up time** field to schedule the date and time for the wakeup call.
- In **Extension Number** field you could select one or more extensions as you want.
- In **Voice Prompt** please choose the voice file to be played in the wake-up call. If Default is selected, then the it will play the current time in the wake-up call.

If a wakeup call is not answered, system will try to ring back in the next minute, and will retry 2 times, after which system will consider the wakeup call completed.

5.5.4 Conference

Path: **PBX Settings -> Advanced Features -> Conference**

Conferences allow two or more callers to be joined together so that all parties on the call can hear one another. Conferences are also referred as Conference Bridges or Conference Rooms. There are 10 conference numbers for internal extension users to dial to join conference calls. You can also set conference as a destination in inbound routes to allow outside callers to reach the conferences.

Conference Number	Guest Password	Admin Password	Leader Wait	Announce Caller	Conference Recording	Operation
0900	1234	2345	No	No	No	 
0901	1234	2345	No	No	No	 
0902	1234	2345	No	No	No	 
0903	1234	2345	No	No	No	 
0904	1234	2345	No	No	No	 
0905	1234	2345	No	No	No	 
0906	1234	2345	No	No	No	 
0907	1234	2345	No	No	No	 
0908	1234	2345	No	No	No	 
0909	1234	2345	No	No	No	 

Total 10 items < 1 > 20 / page Goto

Only users who dial the same conference number could hear one another. Please click the **Add** to add a conference.

Add ✕

* Conference Number

* Guest Password

* Admin Password


* Dial Permission

* Hold Music

Leader Wait

Announce Caller

Conference Recording

There are options for each conference for you to customize the conference feature. Please click the  button to change the options if needed.

Edit 0900 ✕

* Guest Password ⊙

* Admin Password ⊙

* Dial Permission ⊙

* Hold Music ⊙

Leader Wait ⊙

Announce Caller ⊙

Conference Recording ⊙

- **Guest Password** is for ordinary conference users, only the users who enter the correct password can join in the conference.
- **Admin Password** is for conference admin, only the user/users who enter the admin password will become the conference administrator. Conference admin can invite other numbers to join in the conference by using Conference feature codes.
- **Dial Permission** could be used by the conference admin user to dial other numbers and invite them to join in the conference. By default, all conferences use Internal dial permission, which means by default the conference admin could only invite internal extension numbers to join in the conference, if inviting an external number is necessary, please select a valid dial permission which could be used to dial external numbers.
- **Leader Wait**, if enabled, the conference will start when the conference admin entered. Before the conference admin joining in, all other participants will be waiting with background music on.
- **Announce Callers** option causes the IPPBX system to notify all conference participants about new participants join-in. Before a new participant joining in the conference, the IPPBX system will ask the participant to say his/her name, once done, the system playback the recorded name to other participants and at the same time, new participant joins in.
- **Call Recording** option determines whether the conferences to be held in this “conference room” should be recorded or not.

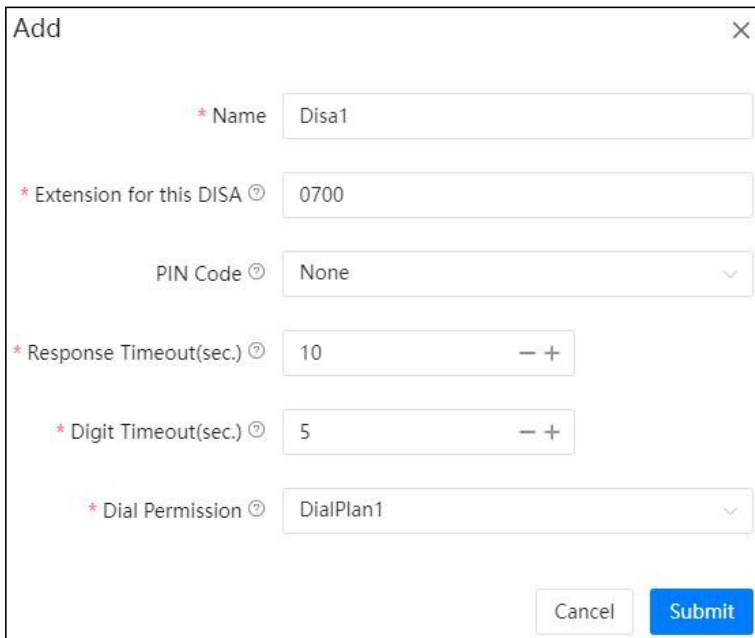
5.5.5 DISA

Path: **PBX Settings -> Advanced Features -> DISA**

Direct inward system access (DISA) allows an outside caller to dial directly into the PBX system and access the system's features and facilities remotely.

It's useful if you want people to be able to, for example, take advantage of the low rate for international calls that you have available on your system, or to allow outside callers to be able to use the paging or intercom features of the system. Always protect this feature with strong password/passwords, the passwords need to be set on PIN Sets page.

To add a DISA feature, follow the explanations below.



The screenshot shows a web form titled "Add" with a close button (X) in the top right corner. The form contains the following fields:

- Name:** A text input field containing "Disa1".
- Extension for this DISA:** A text input field containing "0700".
- PIN Code:** A dropdown menu currently set to "None".
- Response Timeout(sec.):** A numeric input field with a spinner, set to "10".
- Digit Timeout(sec.):** A numeric input field with a spinner, set to "5".
- Dial Permission:** A dropdown menu currently set to "DialPlan1".

At the bottom of the form, there are two buttons: "Cancel" and "Submit".

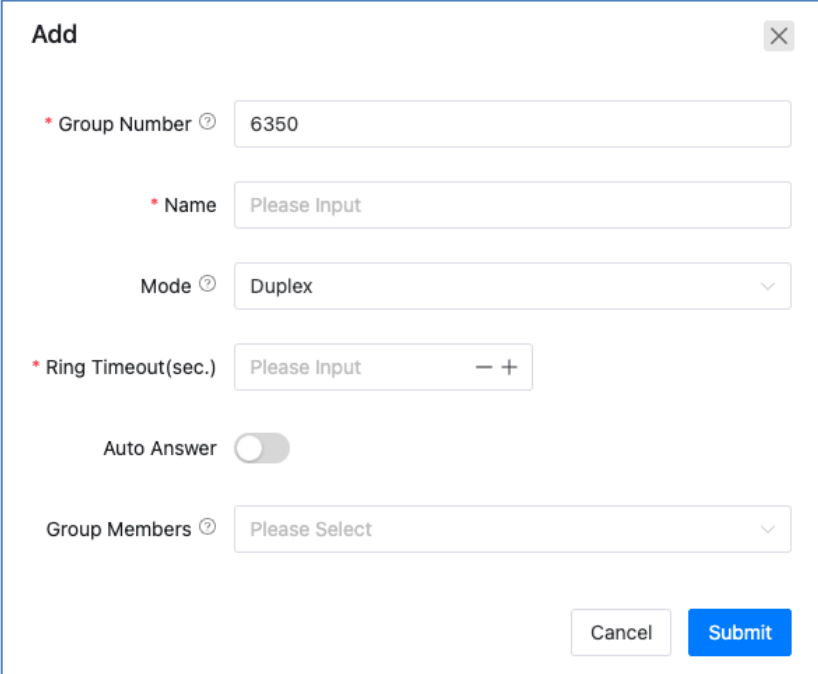
- In the **PIN Code** drop-down list select a valid PIN Set. The PIN codes of this PIN set will be used to authorize all callers using the system features and facilities.
- **Response Timeout(sec):** The maximum waiting duration before hanging up if the dialed number is incomplete or invalid. Defaulted 10 seconds
- **Digit Timeout(sec):** The maximum interval time between digits when typing extension number. Defaulted 5 seconds.
- **Extension for this DISA:** If you want to access DISA by dialing an extension, you can define an extension number for this DISA.
- **Dial Permission:** Select a dial permission for this DISA so callers will be able to make outbound phone calls using the trunks on the IPPBX system.

5.5.6 Paging & Intercom

Path: **PBX Settings -> Advanced Features -> Paging & Intercom**

The Paging and Intercom feature allows you to use your phone system as an intercom system, provided that your endpoints (phone devices) support this functionality. The Paging and Intercom feature allows you to define an extension number that by calling the number will simultaneously page/intercom a group of phones.

To create a **Paging & Intercom** group, please click on the **Add** button, a popup window will show up as below.



The screenshot shows a modal window titled "Add" with a close button (X) in the top right corner. The form contains the following fields and controls:

- * Group Number**: Text input field containing "6350".
- * Name**: Text input field containing "Please Input".
- Mode**: Dropdown menu with "Duplex" selected.
- * Ring Timeout(sec.)**: Spin box with "Please Input" and minus/plus buttons.
- Auto Answer**: Toggle switch, currently turned off.
- Group Members**: Dropdown menu with "Please Select".

At the bottom of the form are two buttons: "Cancel" and "Submit".

- In the **Name** field a name should be given to identify this paging group.
- In the **Mode** dropdown list, if "Simplex" is selected, calling the group number will page on the group members, if "Duplex", the group members are able to talk back to the caller (intercom); If "Multicast" is selected, the system will use the multicast method to send the paging data.
- **Ring Timeout (sec)** : Device's ringing timeout duration.
- **Auto Answer** Enable/Disable automatic answer feature of the terminal device. (It requires the terminal to support the SIP header auto answering tag).
- In the **Group Members** field, select the desired user extensions, make sure all extensions you selected are desktop based IP phones, otherwise if the phone is an analogone, paging/intercom will not work.

Except group paging and intercom, extension users could also paging/intercom an individual extension by using feature codes, please refer to introductions in Other feature codes section.

5.5.7 Smart DID

Path: **PBX Setting -> Advanced Features -> Smart Routes**

With Smart Routes feature, the IPPBX system has the ability to route an inbound call directly to an extension if the extension had previously called or tried to call the external number. It

is convenient for the called party to make a call back and be directly routed to the extension that called them without going through the IVR menu or reception desk.

For example, extension 100 called external number 1234567, no matter this number answered or not, when the number tries to ring back, the call will go directly to extension 100.

If you want this to happen, please use the **Enable Smart Routes** switch to turn on this feature.

Smart DID ⓘ

Enable

Time of Validation ⓘ

Apply to Trunk/Trunks ⓘ

In **Time of Validation** dropdown list choose how long the system to save these outbound call records. When the records expired, the inbound calls will be routed according to you inbound routes settings.

In **Apply to Trunk/Trunks** field, you have to select the trunk/trunks Smart Routes feature will be applied to.

5.5.8 Phonebook

Path: **PBX Settings -> Advanced Features -> Phonebook**

LDAP Server Info ⓘ

Username cn=user,dc=ippbx,dc=com Password password Directory Node dc=ippbx,dc=com

Activate Sync Extension Numbers ⓘ Contacts Sorting ⓘ Phone Number

<input type="checkbox"/>	Contact Name ↓	Phone Number	E-mail	Company / Department	By User	Speed Dial Number ⓘ	Operation
No Data							

< 1 > 20 / page Goto 1

Phonebook feature for FCM5600 IPPBX is just like a contact list on the mobile phones. You may add contacts to the IPPBX system, when the contacts calling in, on the ringing user extension phone screen will display the caller number and the contact name you have

added before. If the number didn't match any contacts in the phonebook, then only caller number will be displayed on the ringing phone screen.

You may click on the  button to add a new contact from the popup window.


Add ✕

* Contact Name

* Phone Number

E-mail

Company / Department

Speed Dial Number 

Or you may export the phonebook template file to add the contacts by MS Excel and then upload the file to generate contacts.

Contacts could be added by admin user from admin web interface, by operator from operator web interface and by extension user from extension user web portal.

A contact added by admin user and operator user is visible to all extension users, but a contact added by an extension user is only visible to the user who added it and the admin and operator user, other extensions won't be able to see it.


5.5.9 Callback


Path: **PBX Settings -> Advanced Features -> Callback**


Callback is to allow a company employee who needs to make a call from their personal phone to call the IPPBX, the IPPBX calls them back and the cost of any future outbound calls are at the company's expense.

Options

Enable

Strip Prefix 

Add Prefix 

* Dial Permission 

- **Enable:** Enable Call Back feature by switching the button on.
- **Strip Prefix:** The received caller ID might have some additional digits in front of it and it will not be possible for you to call back directly, you can specify here to remove some digits before calling back.
- **Add Prefix:** Define digits added before calling out the numbers.

Add ✕

* Number

* Destination Type

* Destination

- **Dial Permission:** Choose an appropriate dial plan to make sure the IPPBX system has the permissions for outbound calling.
- **Number:** The number which will be used to call into the IPPBX system and handled by the Callback feature.
- **Destination:** An extension or another call destination which will be used to call the callback number.


In the above example, if the caller 85337096 called the IPPBX system, IPPBX will disconnect this call and make a call back to this number using extension 100.

In the call back destination field you can even set the destination to a conference, call queue or DISA, so the callers can access these functionalities all at the companies expense.

5.5.10 Whitelist

Path: **PBX Settings -> Advanced Features -> Whitelist**

An extension user can set up a whitelist, only the numbers in the whitelist can dial that extension number, otherwise the call will be rejected. After establishing the whitelist, user can select the association in the 'IP Extension'.

Name	Type	Number List	Operation
 No Data			

Add
✕

* Name

* Type

* Number List

- **Name:** the name of the white list.
- **Type:** call in or out white list.
- **Number List:** the system would check whether the incoming call number match with any one number on the number list. Please use ' , ' to separate multiple numbers.

5.6 Preferences

5.6.1 Global PBX Options

Path: *PBX Settings -> Preferences -> Global PBX Options*

PBX Global Settings

<p>Early Media <input type="checkbox"/></p> <p>Outbound Call Transfer <input type="checkbox"/></p> <p>Music On Ringback <input type="checkbox"/></p> <p>Auto Answer <input type="checkbox"/></p> <p>Block Anonymous Calls <input type="checkbox"/></p> <p>Call Forward CID <input type="checkbox"/></p> <p>Press 0 to Operator <input type="checkbox"/></p> <p>Indicate Line Busy <input type="checkbox"/></p> <p>Diversion <input type="checkbox"/></p> <p>Abandoned Call Logs <input type="checkbox"/></p> <p>PPI <input type="checkbox"/></p>	<p>* Global Ring Time(sec.) <input type="text" value="30"/></p> <p>Operator Extension <input type="text" value="101[101]"/></p> <p>Music On Hold Folder <input type="text" value="Please Select"/></p> <p>Auto Answer Time(sec.) <input type="text" value="Please Select"/></p> <p>Jitter Buffer <input type="checkbox"/></p> <p>Blind Transfer Callback <input type="checkbox"/></p> <p>Operator File <input type="text" value="Default"/></p> <p>Busy File <input type="text" value="Default"/></p> <p>Recording Files Format <input type="text" value="wav"/></p> <p>SIP Header Type <input type="text" value="sip"/></p> <p>Internal Callback <input type="checkbox"/></p>
--	--

- **Operator Extension:** Choose an extension to be operator extension. When an incoming call has been directed to voicemail, then by pressing '0' the caller will be put through to the operator extension.
- **Global Ring Time:** If it's not specifically configured, an incoming call will ring the extension for the time given here.

-
- **Outbound Call Transfer:** Allow outbound phone calls to be transferred, if enabled it might cause phone call problem in certain situations. For example, an outbound phone call had been placed to another IVR system, the keypress might be recognized as transfer request on your own IPPBX system.
 - **Early Media:** Early media is the ability of two user agents to communicate before a call is actually established.
 - **Music On Ringback:** If enabled, callers will hear music instead of ringback tone when calling extensions.
 - **Music On Hold Folder:** To select the music folder.
 - **Auto Answer:** Auto-answer enables the IPPBX to automatically answer the inbound calls from analog ports.
 - **Auto Answer Time:** The time in second after the call is auto answered.
 - **Block Anonymous Calls:** If enabled, all anonymous (without caller ID) calls will be blocked by the phone system.
 - **Jitter Buffer:** Jitter buffer can be used to resolve the sound distortion caused by network congestion, timing drift or route changes.
 - **Call Forward CID:** The incoming call numbers are allowed to be transmitted through other digital trunks.
 - **Press 0 to Operator:** Calls that are unanswered due to the disable of extension's voice mailbox, it will prompt a 'Press 0 to speak with an operator'.
 - **Operator File:** Calls that are unanswered due to the disable of extension's voice mailbox, the selected prompt will be played to the caller.
 - **Indicate Line Busy:** Whether to enable the announcement of 'Line Busy' when the outgoing line cannot be connected.
 - **Busy File:** After the outgoing call fails, the selected prompt will be played to the caller.
 - **Blind Transfer Callback:** Enable the blind transfer for unanswered call to be transferred.
 - **Diversion:** While forwarding/transferring a call out through SIP trunk, the actual caller number can be passed to the forwarded number with diversion option enabled, but requires the SIP trunk service provider support this feature, otherwise please disable this option.
 - **PPI:** The P-Preferred-Identity (PPI) header is used among trusted SIP entities (typically intermediaries) to carry the identity of the user sending a SIP message as it was verified by authentication.
 - **Abandoned Call Logs:** Whether to record the abandoned call that are in the queue into logs.
 - **SIP Header Type:** The header type for PPI and Diversion.
 - **Internal Callback:** When an internal extension dials another internal extension that is unanswered or busy, the caller can press 1 to activate callback, and the called extension will

automatically call back the extension that activated callback when the next hang-up occurs. If callback is activated multiple times, the most recent activation is used.

The user extension number and system extension number ranges are defined here to avoid any conflicts within the IPPBX system. You can modify these number ranges as per your requirements. The user extension number could be 2 to 11 digits. And **Call Retrieve Number** range need to be modified from the **Feature Codes** screen.

5.6.2 VoIP Advanced

Path: **PBX Settings -> Preferences -> VoIP Advanced**

Global SIP settings allow you to configure some general and advanced options for the IPPBX system global SIP preferences.

SIP Settings

- * UDP Port -- +
- * TCP Port -- +
- * TLS Port -- +
- ICE Enable
- STUN Server Address
- * RTP Port Range -
- * User Agent
- * Endpoint Identifier Order
- External Media Address
- External Signaling Address
- External UDP Signaling Port
- External TCP Signaling Port
- External TLS Signaling Port
- Local Net(IP/Netmask Length) 1
- Local Net(IP/Netmask Length) 2
- Local Net(IP/Netmask Length) 3

- **UDP Port:** SIP over UDP service port. By default, FIBERME FCM5600 IPPBX system uses UDP as SIP transmission protocol. Port number can be changed here if required. If changed on the IPPBX system, you'll also have to change on the SIP clients.
- **TCP Port:** If the phones support TCP protocol, you can register SIP extensions over TCP protocol on port 5061.
- **TLS Port:** If the phones support TLS protocol, you can register SIP extensions over TLS protocol on port 5062.
- **ICE Enable:** This is specific to clients that support NAT traversal for media via ICE, STUN, TURN. By default, please keep it enabled, otherwise WebRTC won't work, **STUN Server Address** can be left blank.
- **STUN Server Address:** By default, please keep it blank, if you got available STUN server,

please specify the valid server address, otherwise an invalid STUN server address will cause phone system exception.

- **RTP Port Range:** The UDP ports used by the IPPBX system to carry RTP voice stream. Do not change the port range or you may encounter audio issue with phone calls.
- **User Agent:** The default user agent string also contains the Asterisk version. If you don't want to expose it, change the user agent string here.
- **Endpoint Identifier Order:** The priority of SIP signaling user authentication type (non-professional users are not recommended to modify).
- **External Media Address:** If you want to map your IPPBX system to the Internet, you should specify the static public IP address or domain name here.
- **External Signaling Address:** This is similar to External Media Address except that the External Signaling Address is looked up regularly (every 10s).
- **External UDP Signaling Address Port:** Port number of SIP signaling with UDP transport protocol on the public network.
- **External TCP Signaling Address Port:** Port number of SIP signaling with TCP transport protocol on the public network.
- **External TLS Signaling Address Port:** Port number of SIP signaling with TLS transport protocol on the public network.
- **Local Net (IP/Netmask Length):** Your local network address/addresses. *Note: If you are going to map your IPPBX system to the Internet, the following configurations should be done.*
 1. SIP port mapping on your router (one of the following: UDP: 5060; TCP: 5061; TLS: 5062).
 2. RTP port mapping on your router (UDP: 10001 to 10500).
 3. Specify External Media Address and External Signaling Address.
 4. Specify your local network address/addresses.
 5. For extensions remote registration, enable "Remote Extension" on extension edit popup window.

Mapping your IPPBX to the Internet will be risky, for security precautions please always use strong passwords.

IAX Settings ⓘ

* UDP Port -- +

IAX2 extension support had been enabled by default for all extensions. And IAX2 works on

UDP port 4569, you may modify the port number if required.

Asterisk supports different QoS settings at the application level for various protocols on both signaling and media. The Type of Service (TOS) byte can be set on outgoing IP packets for various protocols. The TOS byte is used by the network to provide some level of Quality of Service (QoS) even if the network is congested with other traffic.

Type of Service ?

TOS for Signaling packets

TOS for RTP audio packets

TOS for RTP video packets

COS Priority for Signaling packets

COS Priority for RTP audio packets

COS Priority for RTP video packets

5.6.3 Voicemail Settings

Voicemail settings can be used to configure global voicemail options for all extension users.

Voicemail Settings

Mailbox Options

Max Greeting Time(sec.) Dial '0' for Operator

Delete Voicemail

Voice Message Options

Message Format Maximum Messages

Max Message Time(min.) Min Message Time(sec.)

Playback Options

Say Message CallerID Say Message Duration

Play Envelope Allow Users to Review

- **Max Greeting Time** sets the max greeting message duration the extension users can record in their mailbox to greet the callers when they entering voicemail.
- **Dial '0' for Operator:** option if enabled, the callers can press 0 to call the operator extension.

- **Delete Voicemail:** When this option is enabled, the voicemail in the IPPBX system will be automatically deleted after the voicemail is sent out by email (regardless of whether the email is sent successfully or not).
- **Message Format:** sets the voicemail audio file format to be saved in the IP PBX system.
- **Maximum Messages** sets the maximum number of messages can be saved in the system for each extension user.
- **Max Message Time** sets the maximum duration of a single voice message can be accepted by IP PBX system.
- **Min Message Time** sets the minimum duration of a single voice message can be accepted by the IP PBX system, message duration less than the Min Message Time will be discarded by IP PBX system.
- **Say Message Caller ID:** Announce caller ID when listening to the message on user extension.
- **Say Message Duration:** Announce message duration when listening to the message on user extension.
- **Play Envelope:** Announce date time and caller ID when listening to the message on user extension.
- **Allow Users to Review:** Allow callers to review their message before saving.



5.7 Feature Codes

Path: *PBX Settings* -> *Feature Codes*

Feature codes can be dialed from user extensions to enable and disable certain features or to achieve some call features. For example, enable and disable call forward, transfer incoming calls, check voice messages, etc.

Feature codes could be modified if necessary but please ensure all feature codes you wish to change will not conflict with other existing ones.

5.7.1 Voicemail Feature Code



Voicemail 	
Dial Voicemail	*98
My Voicemail	*97

Dial *98 and you will enter the main menu of voicemail feature, by specifying the extension number and voicemail password of the required extension then you can check its voicemail and you can do this for any extension by following the system voice guidance.

By dialing *97 from an extension and entering the voicemail password for this extension you can follow the voice guidance to check voicemail of your own extension. Or alternatively, you can configure some advanced options for your voicemail box.

5.7.2 Call Pickup Feature Code

Call pickup feature codes allow users to pickup calls that are not directed to them by dialing a feature code *8 or **.



Call Pickup 	
General Call Pickup	*8
Direct Call Pickup	**

If there's an incoming call ringing on an extension that belongs to your department, you may dial the general call pickup feature code *8 (end with #) to pick up the call. While if there are 2 ringing extensions in your department, by dialing *8 will pick up the first incoming call. If you need to pick up the second incoming call or if you don't know which call came first, you may use direct call pickup feature code.

Direct call pickup feature code could be used to pick up an incoming call on a specific extension, no matter the extension is from the same department or from another department. Just dial ** following by the extension number (end with #) you'll be able to pick up the incoming call on that specific extension.

5.7.3 Call Parking Feature Codes

Call parking feature allows anyone who has received a call to park the call on an extension, allowing any other user to access the parked call.

Call Parking 		
Parking Number	#72	
Call Retrieve Number	41-49	

To park a call, extension user could dial #72 during a live call, and then listen as the system tells you where you can retrieve the call (usually extension 41). The second call will be parked on 42, and it continues to park on orderly.

To retrieve the parked calls, user should dial the retrieve number given by the IPPBX system.



And this could be done by any extension.

A call could be parked for maximally 120 seconds before it goes back to the extension which parked it. And the parking lot (call retrieve numbers) could be monitored by BLF. It's helpful if the operator wants to know if there are calls parked on the IPPBX system.

5.7.4 Call Transfer Feature Code

Call Transfer is used to transfer a call in progress to some other destinations. There are two types of call transfer.

- Attended call transfer - Where the call is placed on hold, a call is placed to another party, and a conversation can take place privately before the caller on hold is connected to the new destination. It is also referred to "Supervised Call Transfer".
- Blind call transfer - Where the call is transferred to the other destinations without intervention (the other destination could ring out and may not be answered for instance).

Call Transfer 		
Blind Transfer	#1	
Attended Transfer	*2	
Abort Transfer	*0	

In a live call, you can press #1 key and the IPPBX system prompts "Transfer", you then enter the number to transfer to, this call will be transferred instantly and the user can hangup. If

the transferred number doesn't answer this call then it will go to voicemail.


If blind transfer sometimes seems inappropriate, you may use attended transfer feature. In a live call, you can press *2 and the IPPBX system prompts "Transfer", you then enter the number to transfer to, after someone answers your call, you can introduce this call and hang-up at which point the call is transferred.

In an attended transfer, if the third party rang for 15 seconds without answering, the extension user will go back to the caller and the transfer is terminated. You may also manually abort the transfer by pressing *0 when the third party is still ringing.

5.7.5 Blacklist Feature Code

Blacklist feature codes allow the extension users to add external phone numbers to IPPBX system blacklist from their phones, consequently the numbers added will not be able to dial in to the IPPBX system.

Adding blacklist numbers from phone by using feature codes is the same as adding blacklist numbers from admin and operator UI.

Blacklist ⓘ	
Blacklist the Last Caller	*76
Blacklist a Number	*40
Whitelist a Number	*41


Blacklist the last caller allows you to dial *76 to directly add the last caller's number to the IPPBX blacklist.

You may also dial *40 (end with #) and follow the voice prompts to specify the number you wish to blacklist to add numbers to the IPPBX system blacklist.

To remove numbers from blacklist (whitelist a number), you can dial *41 (end with #) and follow the voice prompts to specify the number you wish to whitelist.

5.7.6 Call Spy Feature Code

Call Spy allows users to dial the spy feature codes following by an extension number to listen to the call conversation in real-time.


Call Spy ⓘ	
Normal	*54
Whisper	*55
Barge	*56

- **Normal Spy:** For example, extension 410 is talking to someone on the phone, you can dial *54410 (end with #) to listen to their conversation, however, neither speaker will be able to hear you.
- **Whisper Spy:** Whisper spy is also known as coaching. For example, a new employee is talking to the customer on the phone, their supervisor can dial *55 following by the employee's extension number (end with #) to listen to their conversation. The supervisor can talk to the new employee only without the customer hearing the conversation.
- **Barge Spy:** Barge spy is similar to an instant 3-way conference call. While an extension user is talking to someone else on the phone, you can dial *56 following by their extension number (end with #) to talk to both of the speakers.

Note: Before you can spy on an extension, please enable "Call Spy" option on the extension edit popup window.

5.7.7 Call Queue Feature Code

Call queue feature codes are for call queue agent extensions only. They are meaningless to the non-agent extensions.

Call Queue ⓘ	
Agent Pause	*95
Agent Unpause	*095
Agent Login	*62
Agent Logout	*062

Agent Login and **Agent Logout** are for dynamic agents to login or out of the call queue. And for both static agents and dynamic agents, they can dial *95 to suspend their extensions temporarily, new calls will not be distributed to their extensions, until they dial *095 to resume.

5.7.8 Conference Feature Code

Conference feature codes are used by conference admin for inviting participants to join in a conference or for creating a conference during a normal phone call.

Conference ?	
Invite Participant	0
Return with Participant	**
Return without Participant	*#
Create Conference	*0

When in a conference room, if the conference admin user presses 0 they will get a dial tone for inviting others to participate in this conference.

If the invited party agrees to join in the conference, conference admin user can dial ** to return to the conference with invited party.



If the invited party doesn't want to join in the conference, conference admin user can press *# to return to the conference without the invited party.

During a live call the extension user can press *0 to create a dynamic conference room. The other side will automatically enter the conference as an ordinary participant while the extension user who created this conference will be requested to enter the conference password to enter. Usually, the user needs to enter the conference admin user password as the user needs to invite others to join in the conference.

Note: After a dynamic conference is created, in reality you have entered a static conference room (by default 90 is the first available conference room). You are able to use conference admin menu to invite others to the conference and also others can dial 90 to enter this conference.

5.7.9 Wakeup call Feature Code



Except configuring Wakeup Calls from admin and operator web user interface, extension users could request wakeup calls from their phones directly by feature codes.

Wake Up Call 		
Wake Up Call Main Menu		*55
Direct Wake Up Call Request		*55*
Cancel All Wakeup Calls		*055

- **Cancel All Wakeup Calls:** By dialing this code to cancel all requested wakeup calls.
- **Direct Wakeup Call Request:** Add a wakeup call directly by dialing this feature code followed by a specific date and time in 8-digit number format, for example, feature code is *55*, you can dial *55*08010730 to add a wakeup call of 7:30am on August 1st.
- **Wakeup Call Main Menu:** Advanced wakeup call menu for adding, viewing and canceling wakeup calls.

5.7.10 Call Forward Feature Code

Call forward could be configured from admin and operator web user interface. With the following feature codes, extension users can activate or deactivate call forward directly from their phones without configuration on the Web GUI.

Call Forward 		
Forward All Activate		*72
Deactivate All		*73
Activate Forward on Busy		*90
Deactivate Forward on Busy		*91
Activate Forward on No Answer		*92
Deactivate Forward on No Answer		*93



For example, a FCM5600 IPPBX requires prefix 9 to call outbound, and the number you want to forward the calls to is 85337096.

- **Forward All Activate:** Dial *72985337096, press 1 to confirm.
- **Deactivate Forward All:** Dial *73 .

- **Activate Forward on Busy:** Dial *90985337096, press 1 to confirm.
- **Deactivate Forward on Busy:** Dial *91.
- **Activate Forward on No Answer:** Dial *72985337096, press 1 to confirm.
- **Deactivate Forward on No Answer:** Dial *93.

5.7.11 DND Feature Code

DND (Do Not Disturb) could be set on the IP phones from the phone level, if the phone doesn't have DND feature you may use the DND feature code to set DND from IPPBX system level. Any phone connected to the FCM5600 IPPBX system can use the DND feature code, no matter it's IP phone, analog phone or softphone.



DND 		
DND Activate		*77
DND Deactivate		*78

Simply dial *77 to enable DND, if you hear a beep sound that means DND is on. Once DND enabled, the extension will only be able to make calls, and inbound calls will be rejected.

Make sure when you are ready to receive inbound calls, dial *78 to deactivate DND.


5.7.12 Office Closed Feature Code

Office Closed could be set on the IP phones from the phone level. Any phone connected to the FCM5600 IPPBX system can use the Office Closed feature code, no matter it's an IP phone, analog phone or softphone.

Office Closed 		
Office Closed On		*81
Office Closed Off		*081

By dialing the Office Closed On feature code you may disable all inbound control settings, all inbound calls will be forwarded to a specific destination. By dialing the Office Closed Off feature code to resume all inbound control settings.

5.7.13 Other Feature Codes

Others	
One Touch Recording	*1
Intercom	*50
Paging	*51
Announce WAN Port IP	**11
Announce LAN Port IP	**12
Announce Extension Number	**13
Speed dial	*99
Switch Phone	*3
Meet Me Page	*52

- **Announce WAN Port IP:** By dialing this code you'll hear the system announce the IP address of the IPPBX WAN interface.
- **Announce LAN Port IP:** By dialing this code you'll hear the system announce the IP address of the IPPBX LAN interface.
- **Announce Extension Number:** By dialing this code you can check the extension number of your phone, either it's an IP phone or analog phone.
- **One Touch Recording:** One Touch Recording is also known as Record on Demand. It allows users to record phone calls selectively. In a live call conversation, an extension user can use feature code *3 to record this call. With this feature, you don't have to configure recording all calls for the extensions which may cause heavy system resource use if some call recordings are not required.
- **Intercom:** The intercom feature code allows you to intercom one extension only. You don't have to create a "Paging and Intercom" group for only one extension if you intend to intercom with only that extension.
- **Paging:** The paging feature code allows you to page one extension only. It's the same as the intercom feature code, the only difference between paging feature code and intercom feature code is by using intercom feature code both sides can talk to each other but using paging feature code, only the caller can talk to the called party.

- **Speed Dial:** Use speed dial feature code with contact speed dial number to call a contact instead of dial the contact's actual number.
- **Meet Me Page:** Meet Me Page can be used to page someone over the phones/speakers. The paged person can use this feature code to terminate the paging and establish an intercom call with the initiator.
- **Switch Phone:** When the extension is registered on several different endpoints, you may dial *3 from an idle endpoint to switch the call to the idle endpoint.

6. Reports

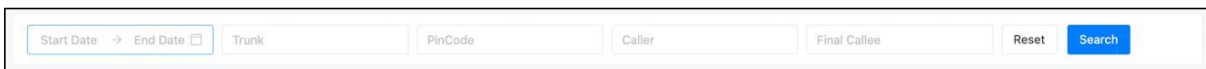
6.1 Records

6.1.1 Call Record

Path: **Reports** -> **Records** -> **Call Record**

Call recordings to be checked here are for those extensions which had enabled call recording from the extension edit page.

Search criteria can be used to search call recordings are as follows.



- **Start-End Date** could be used to search the recording within the specific time range (require).
- **Trunk** could be used to search according to the inbound/outbound trunk's name (optional).
- **PIN Code** could be used only for those calls which are dialed out with PIN codes define in PIN Set (optional).
- **Caller** could be used to search according to a specific caller's number (optional).
- **Final Callee** could be used to search according to a specific callee's number (optional). The searched recordings will be displayed in a list with some detailed information.

Start time	Caller	Callee	Final Callee	Duration	Trunk	PinCode	Type	Status	Operation
2022-09-01 04:17:17	877	866	866	01:32			Internal	Answered	 
2022-09-01 04:11:45	866	887	887	00:28			Internal	Answered	 
2022-09-01 04:10:47	866	887	887	00:23			Internal	Answered	 
2022-08-31 21:42:34	802	809	809	00:17			Internal	Answered	 

Total 4 items

< 1 > 20 / page Goto

You may playback the recording by built-in web player by clicking on the  button.



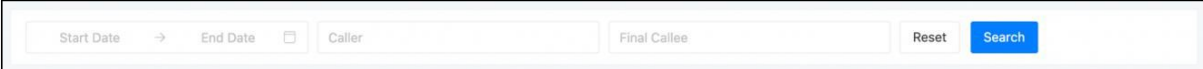
Or you may click on the  button to download or Click  to delete.

Call recordings can be managed only by the admin user from admin web UI. Operator user can only query and review the recordings but cannot delete them.

6.1.2 Conference Recordings

Path: **Reports -> Records -> Conference Recordings**

If the Conferences had call recording enabled, the conference held will be recorded and conference recordings could be found for review here.



Start Date → End Date Caller Final Callee Reset

In the Start-End Date fields you may specify to search for recordings of the specific time period.

The searched recordings will be listed with detailed information of when the conference calls were started, the conference number and the call/record duration. There are also the same options to playback, download and delete the recording files.

Start time	Caller	Callee	Final Callee	Duration	Type	Status	Operation
2022-09-01 04:20:34	800	0900	CONFERENCE(0900)	00:32	Internal	Answered	<input type="button" value="Play"/> <input type="button" value="Download"/>
2022-09-01 04:14:24	887	0900	CONFERENCE(0900)	01:16	Internal	Answered	<input type="button" value="Play"/> <input type="button" value="Download"/>

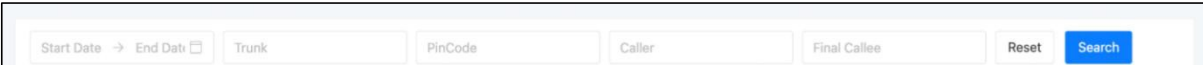
Total 2 items < 1 > 20 / page Goto

6.1.3 One Touch Recordings

Path: **Reports -> Records -> One Touch Recordings**

One touch recording is for those extensions that are not enabled call recording, when the user wants to record the call, by pressing *3 will start recording.

The recordings of once touch recording could be found here. Search criteria and recording list options are the same as “normal” call recordings, except one touch recording could not be found on the **Call Recording** page.



Start Date → End Date Trunk PinCode Caller Final Callee Reset

Start time	Caller	Callee	Final Callee	Duration	Trunk	PinCode	Type	Operation
2022-09-01 04:21:54	877	800	800	00:19			Internal	<input type="button" value="Play"/> <input type="button" value="Download"/>

Total 1 items < 1 > 20 / page Goto

6.2 Log

6.2.1 CDR

Path: **Reports -> Logs -> CDR**

Call logs are also known as CDR (Call Detailed Records), on the call logs page you can check records for any call that went through the IPPBX system.

To query call logs, you need to first specify the searching criteria. After querying the records, you can click the download button to export.

Start time	Caller	Callee	Final Callee	Duration	Trunk	PinCode	Type	Status
2023-05-30 17:28:17	fax[101]	102	102	00:00			Internal	No Answer
2023-05-26 14:10:47	101	103	102	00:07			Internal	Answered
2023-05-26 14:10:33	101	102	102	00:00			Internal	Answered
2023-05-26 14:10:06	101	103	102	00:04			Internal	Answered
2023-05-26 14:09:53	101	102	102	00:00			Internal	Answered
2023-05-26 14:09:10	101	103	102	00:07			Internal	Answered
2023-05-26 14:09:03	101	102	102	00:00			Internal	Answered
2023-05-26 14:06:23	101	103	102	00:11			Internal	Answered
2023-05-26 14:06:09	101	102	102	00:00			Internal	Answered
2023-05-26 14:02:01	103	102	102	00:00			Internal	No Answer
2023-05-25 17:39:16	101	103	102	00:07			Internal	Answered

Total 84 items

- In **Start** and **End Date** fields set the start and end date to search call logs within this period of time.
- By specifying the name of a trunk in the **Trunk** field to search the inbound or outbound calls came in or sent out through this specific trunk only.
- In the **PIN Code** field specify a PIN code of a PIN Set to search outbound calls made by using this PIN code.
- The time when this call took place will be listed in the **Start Time** column.
- In the **Caller** column lists the original caller of the calls.
- In the **Final Callee** column lists the first callee but might not be the last.
- The **Final Callee** column lists the extension/destination where the call finally ends.
- In the **Duration** column lists the call duration of each phone calls, this might not be the exact talk time, as when calling though the FXO ports, IPPBX system will auto answer the inbound calls so IVR works, and it will auto answer the outbound calls, so the IPPBX could send the numbers out through the PSTN lines.
- In the **Trunk** column lists the trunks used by those phone calls. Internal call will not take any trunk so this blank will be blank for internal calls.
- In the **PIN Code** column, only those outbound calls made out with a PIN code will list the PIN code used here. This is a good idea to tell which user/users made the call, as the PIN codes

are not shared by every extension user. Every extension may have a PIN different than others or several extension users share a PIN code that is different than others.

- In the **Type** column it indicates the type of each phone call, inbound, outbound or internal.
- In the **Status** column you could tell if the calls are successfully made or failed for any reason.

6.2.2 Fax Log

All fax records of the IPPBX system can be queried on the Fax Log page, select the start and end dates, and also specify the sender and receiver information to query all fax records that meet the conditions within a certain period of time. If no other query conditions are specified except the time period, all fax records in the IPPBX system within the time period will be directly queried.

Start time	Sender	Receiver	Type	Status
2022-08-30 11:19:10	003	85337096	Send	OK
2022-08-29 17:19:40	85337096	003	Receive	OK

Total 2 items

< 1 > 20 / page Goto

7. Addons

7.1 API

7.1.1 AMI

Path: *Value Added Features -> API ->AMI*

This section defines the information of the AMI interface. If the AMI Account Settings is empty, it will consider that the AMI interface is closed. The AMI interface is mainly used for the connection of third-party systems and send commands to control traffic and obtain relevant data in the device.

AMI Account Settings

Username ⓘ

Password ⓘ

Allow IP/Subnet Mask ⓘ

- **Username:** AIM interface authentication username.
- **Password:** AMI interface password
- **Allow IP/Subnet Mask:** the segment of IP addresses that are allowed to access.


7.1.2 Push Event


Path: *Value Added Features -> API ->Push Event*

The Push Event is a data sending method based on HTTP POST, which can be used to connect with a third-party system to obtain call pop-up data or call recording data. When the Push Event is enabled, the device will push the selected event data to the specified URL.

Therefore, the URL is required to fill out.

Push

URL 

Event 

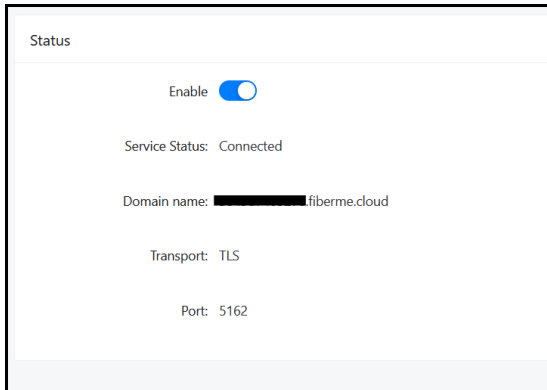
- **URL:** The destination address of the push event.
- **Event:** The AMI event type that needs to be pushed to the destination address.

7.2 FRC

7.2.1 Status

Path: *Value Added Features* -> *FRC*

FRC status information



- **Enable:** Enable/Disable the FRC.
- **Service Status:** Connection status between IPPBX and FRC.
- **Domain Server:** The external domain name used for extensions registration and WebRTC access to the IPPBX.
- **Transport :** The protocol used between IPPBX and FRC.
- **Port:** The port number used for extensions registration to the IPPBX.

7.3 Hot Standby

Path: *Value Added Features -> Hot Standby*

The hot-standby function is using two same model of IPPBX server with the same software version, one as the primary server and the other one work as secondary server. When the primary fails, all current calls can be automatically switched to the secondary server in a short time. It requires configuration on both primary server and secondary server. When the status of the secondary server is “Connected”, that means configuration data of the primary server has been synchronized to the secondary server. The secondary server will not load the data in real time, it will be loaded only after it’s status change from secondary to primary or the system restarts.

Hot Standby

Enable

Username

Password

Mode

SlaveIP

Virtual IP Address

NIC

Notification Email

Phone Call Notification

- **Enable:** Enable/Disable Hot-standby function.
- **Username/Password:** The username and password used by the primary server and secondary server to verify the heartbeat data. The primary and secondary servers must be configured with the same username and password for authentication.
- **Mode:** Primary Mode/Secondary Mode. The primary server indicates the currently working server.
- **Master/Slave IP:** The IP address of the Primary server or Secondary server.
- **Virtual IP Address:** The IP address of the hot-standby function to provide external services, which the IP address can be registered by the extensions.
- **Network Interface:** The network interface for sending the heartbeat data, eg: WAN/LAN.

- **Email Notification:** Email address for sending notification when the state is switched. (SMTP service is required)
- **Phone Call Notification:** Phone number for calling notification when the state is switched. (Internal and external numbers are support. Please make sure DialPlan1 has the authority to dial this number).

7.4 Remote Management

Path: *Value Added Features ->Remote Management*

Enabling the Remote Management function to connect the device to the official remote management platform. Technicians can use the authorized device's login credentials to access the device system through the remote management platform.

Remote Management

Enable 

Invitation Code

Host

- **Enable:** Enable/Disable the Remote Management function.
- **Invitation Code:** Obtain the invitation code from the FIBERME Support Team or distributors. Using this invitation code to connect to the remote management platform.
- **Host:** It is used for third-party remote management server connection. If you use the FIBERME RemoteConnect server, you do not need to fill in this parameter.

7.5 AutoConfig

7.5.1 Devices

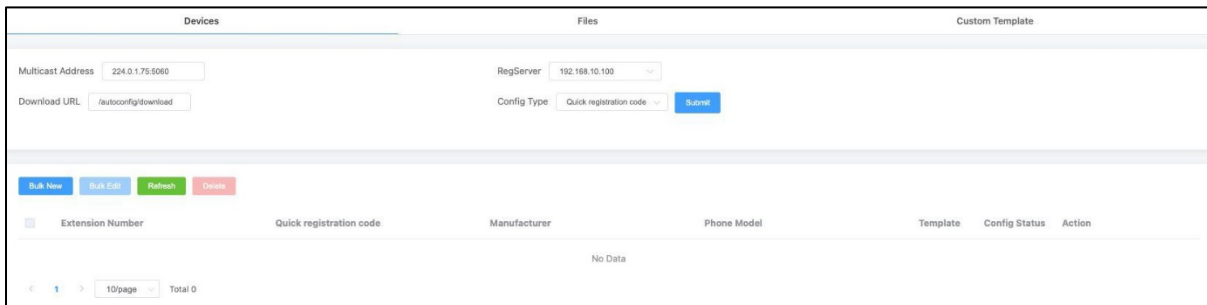
Path: **Value Added Features** ->**AutoConfig** ->**Devices**

The AutoConfig function helps to realize the automatic discovery and configuration of IP phones in the LAN. It supports pnp and option66 methods.

Step-1: Scan or Add a new phone. Simply click on the **Scan** button, it can automatically discover the phone in the same LAN, or discover the phone through pnp subscription feature. You can also click the **New** button to manually adding a supported manufacturer and model of IP phone.

Step-2: For configuring the IP phone, please click on the **Edit** button on each phone to assign an extension number and modify other configuration to the phone.

Step-3: Send configuration, select the phone that needs to send configuration data and click the **Reboot** button (the phone must support sip check-sync restart), and the phone should automatically restart and download the configuration file generated by the IPPBX. If the phone does not support automatic restart, you can manually restart the phone for the phone to download the configuration file.



- **Multicast Address:** The multicast address for monitoring PNP data. Default address is 224.0.1.75:5060.
- **RegServer:** The server address for generating the phone auto-configuration file, you may choose the IPPBX's WAN port or LAN port.
- **Download URL:** The download path required when downloading the configuration file in static mode.
- **Config Type:** Choose to use PNP for configuration or quick registration code
- **MAC:** MAC address of IP phone
- **IP:** IP address of IP Phone
- **Status:** The status of IP phone. (Green -> online, Red -> Offline)
- **Type:** phone registration method, it helps to distinguish whether the phone is discovered by

PNP subscription, manually added or scan added.

- **Manufacturer:** Brand of the IP Phone
- **Phone Model:** IP Phone model
- **Template:** The configuration template applied on the phone
- **Config Status:** IP Phone configuration status
- **Action:** Edit and delete operations can be performed on the phone

7.5.2 Files

Path: *Value Added Features ->AutoConfig->Files*

This is a HTTP file server which used to store phone configuration files. The phone configuration file can be obtained from the IPPBX by setting up static auto provisioning sever address on the IP phone side and realize automatic configuration function. The complete URL should be in the format of http://IP + Download URL + File name. For example, <http://192.168.17.147/autoconfig/download/68692e0250f2.cfg>.



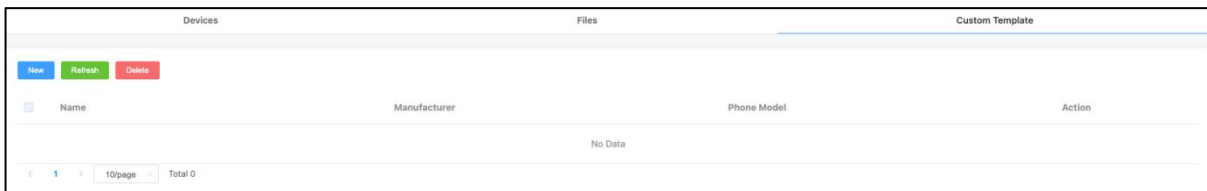
Name	Action
68692e0250f2.cfg	Delete
ptz	Delete

< 1 > 10条/页 共 2 条

7.5.3 Custom Template

Path: *Value Added Features ->AutoConfig->Custom Template*

Click the "New" button on the "Custom Template" page to create and edit a new template and apply it on the "Devices" page.



Name	Manufacturer	Phone Model	Action
No Data			

< 1 > 10/page Total 0

8. System

8.1 Reboot /Reset

8.1.1 Cron Reboot

Path: *System -> Cron Reboot*

To periodically restart the driver or asterisk service.

Cron Reboot

Asterisk

DAHDI


Interval(days) - +

Reboot Time ⌚

- **Asterisk:** Enable/Disable restart Asterisk service.
- **DAHDI :** Enable/Disable restart DAHDI service.
- **Interval (days):** The time period between each restart.
- **Reboot Time:** The specific time of restarting the device.

8.1.2 Reboot

Path: *System -> Reboot and Reset*


By clicking on the  button you may restart your FCM5600 IPPBX from the web UI. Restart the IPPBX system will terminate all active phone calls, please make sure there're no phone calls going on before restarting the IPPBX system.

8.1.3 Reset

Path: **System -> Reboot and Reset**

To reset FCM6500 please refer to below 3 reset methods (**Method 1, Method 2 and Method 3**).

Method 1: Reset from web UI Resetting the IPPBX system

Click on  button and confirm with the popup window, reset process will begin. During the reset process the IPPBX system will restart and the whole process will take around 4 to 5mins.

Before resetting you may enable options “I’d like to keep the network profiles” and “I’d like to keep the call logs and recordings”, so after resetting you may still access the IPPBX system web UI from the same IP with all your call logs and recordings remain untouched. If network profiles had been reset too, you’ll need to access the IPPBX system via the default IP address.

WAN default IP: 192.168.1.100 / LAN Default IP: 192.168.10.100

Note: Reset from web UI will clear all system configurations, except if you have enabled “I’d like to keep the network profiles” and “I’d like to keep the call logs and recordings” options which will keep the network configurations and the call logs and call recordings.

By default backups will be kept, so after resetting from web UI you may restore backup directly from the IPPBX system.

Method 2: Reset by RST button at system running stage, the SYS LED indicator winks once every 2 seconds. Now you may press and hold the RST button on the back panel of the IPPBX for about 7 seconds, then the SYS LED will go off, the IPPBX system will reboot and start the reset process.

Reset FCM5600 IPPBX this way is the same as resetting from the web UI. Only difference would be you cannot choose to keep the network profiles, call logs and recordings, and you will need to access the IPPBX system via the default IP.

Method 3: Reset by RST button at system booting stage.

Reset the FCM5600 IPPBX system by RST button at the system booting stage will erase everything on the IPPBX system, including backups will be erased as well. Resetting this way will fully recover the IPPBX system to factory defaults.

So if you wish to restore the IPPBX configurations with a previous backup, please download it to your operating system first before resetting.

To reset the FCM5600 IPPBX system at system booting stage, you need to first cut off the power supply. Press and hold the RST button then power it on. 4 to 5 seconds later when SYS LED goes on release the RST button.

Around 5mins later access the IPPBX system via the default IP address. You'll first be directed to the quick setup wizard page, you may start configuring a fresh new phone system or you may skip and upload offline backup to restore previous configurations.

8.2 Region /Time

Path: *System -> Region / Time*

System time is very important for the IPPBX system, especially when the IPPBX system handles inbound phone calls according to time conditions, then only if the system time is correct will calls be handled properly. Also, call logs and call recordings files are named with system time. If time's not correct on the system, the phone system will not work properly.

At the initial setup while you going through the quick setup wizard your location would be set. If you had skipped the quick setup wizard or you want to change the time zone, you may do it here.

Location

Country / Region ⊙ ▼

[Submit](#)

Time Settings

Current PBX Time 2022-08-10 02:47

Sync [NTP Time Settings](#) [Manual Time Settings](#)

Time Zone ▼

* NTP Server

[Submit](#)

Location and time may be configured separately. Both modifying location and time settings requires rebooting the IPPBX system.

The location settings will determine the type of tone (Dial tone, Busy, Congestion tone, etc.) you heard on the phones, the time zone and also the opermode on the **Analog Settings** page. So you may not change the location settings here but adjust the time settings only.

You may set the Time Zone and NTP Server to let the IPPBX system synchronize time from the NTP server. This is by default how the system time works.

Or you may manually configure the system time.

Time Settings

Current PBX Time 2022-08-10 02:47

Sync [NTP Time Settings](#) [Manual Time Settings](#)

Set Current PBX Time 📅

[Submit](#)

In the Set Current PBX Time blank, you may manually input the date and time to set it as the current PBX time. Then click on “Submit” button to save the manually set time to the IPPBX hardware.

8.3 Storage

Data storage allows you to upload your recording files, log files and voicemail messages to an FTP server through the Ethernet. Or you may attach an external USB drive to the IPPBX USB interface for saving the above mentioned files.

8.3.1 USB Storage

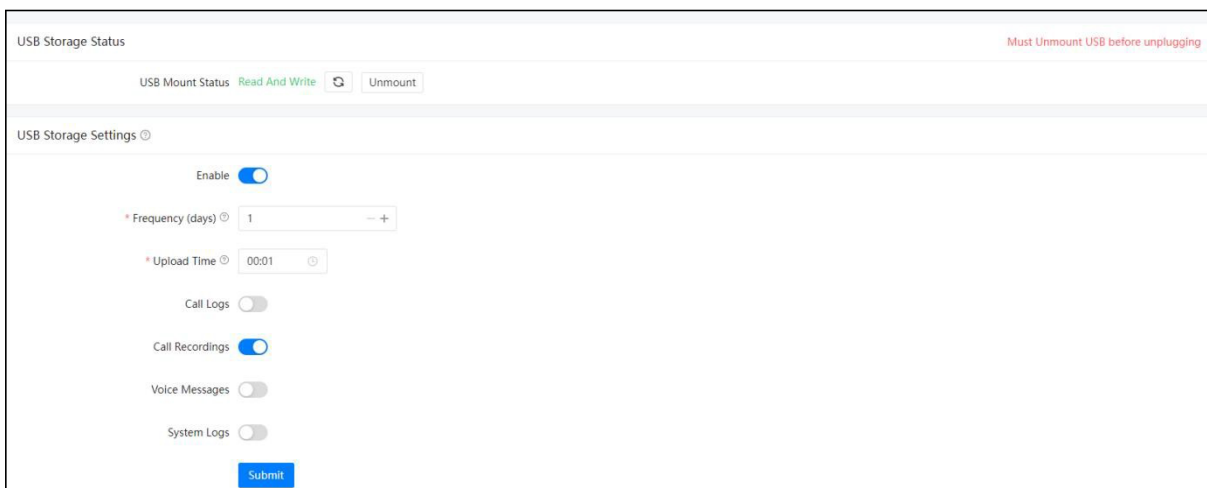
Path: **System -> Storage -> USB Storage**

FCM5600 comes with 1 USB interface,

Supported USB file system formats are: FAT16, FAT32, exFAT, NTFS, EXT3 and EXT4. If it's a portable USB hard drive, please make sure it uses external power supply. And please make sure the USB drive only has a single partition otherwise it won't be detected by the IPPBX system.

Before attaching the USB drive and configuring data storage settings please make sure no one else is signed in the IPPBX web UI and there's no phone call going on in the system. Because during the configuration process of USB data storage, the recordings, logs and voicemails generated would be lost.

Once a USB drive is detected, you'll see the **USB Mount Status** changed to **Read And Write**.



USB Storage Status Must Unmount USB before unplugging

USB Mount Status: Read And Write Unmount

USB Storage Settings

Enable

* Frequency (days) – +

* Upload Time

Call Logs

Call Recordings

Voice Messages

System Logs

Submit

- **Frequency (days):** The time interval between each data backup operation.
- **Upload Time:** The specific time when the data backup operation is performed.

- **Call Logs:** Whether to backup the call log data to the USB storage.
- **Call Recordings:** Whether to backup the call recording data to the USB storage.
- **Voice Messages:** Whether to backup the voice message data to the USB storage.
- **System Logs:** Whether to backup the system log data to the USB storage.

As the example shown above, the system will backup the call recording data only to the USB storage at 00:01AM every day. The system will perform the backup operation at the configured time point until there is no remaining space in the USB storage. Before removing the USB storage, please click the “Unmount” button to unmount the USB, otherwise data loss may occur.

Note: If your USB drive could not be detected by the IPPBX system, please use USB disk format tool to delete all partitions on the USB drive and create a single new partition and try again. Before doing this please backup the data in your USB drive as doing this will erase all data on the drive.

8.3.2 FTP Storage

Path: **System -> Storage -> FTP Storage**

Utilizing your existing FTP server, you can configure the IPPBX system to upload call recordings, voicemails and call log files to your FTP server. If you don't have one you can even use your Windows PC to setup an FTP server for the IPPBX system to connect to. You must however ensure that your PC is always turned on or at least available at the times when your IPPBX is going to upload files.

FTP storage should not be configured to work at the same time with USB data storage. Otherwise the data on the USB will all be migrated to your FTP server.

To configure FTP storage, enable it and configure the FTP server credentials and the file uploading options.

FTP Storage Settings

FTP Uploading

* FTP Server Address

* FTP Server Path

* Username

* Password

* Frequency (days) -- +

* Upload Time

Call Logs

Call Recordings

Voice Messages

System Logs

System Backup

- In the **FTP Server Path** field you may specify the directory of where to store the uploading files.
- In the **Frequency** dropdown list select the number of days of each uploading.
- In the **Upload Time** field specify the exact time of the uploading.

Once configurations done, click on button to connect the IPPBX system with the FTP server. Once connected, you'll see the **FTP Connect Status** changed to **Connected**.

Each time after uploading, the call recordings, voicemails, system logs and system backup will be removed from the IPPBX internal storage, call logs will be kept on the IPPBX system and will make a duplicate on the FTP server.

Enabling the FTP server service, you need to create an FTP user first, then you the FTP client software on your desktop to connect to the IPPBX's FTP server to manage all the files.

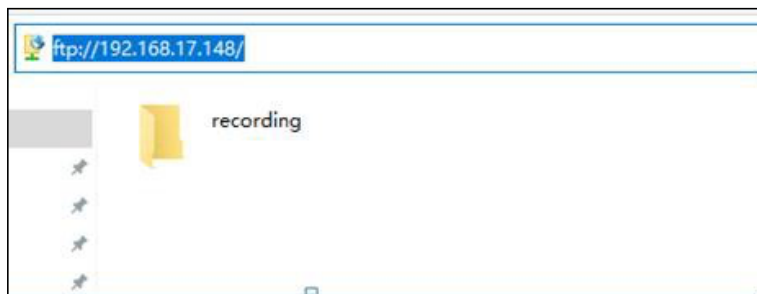
FTP Server

Enable Service

Allow Write

* Username

* Password



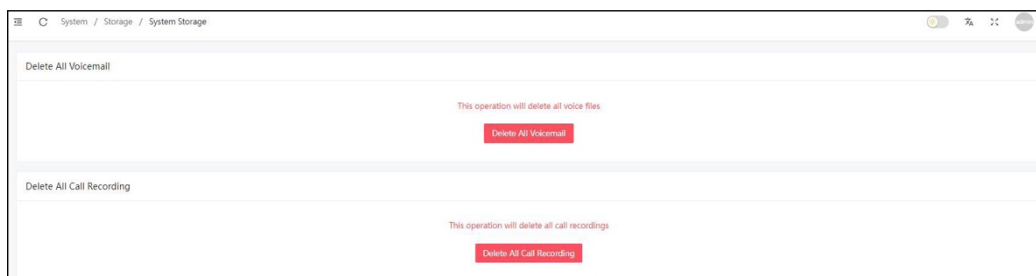
- **Enable Service:** Enable/Disable FTP server service.
- **Allow Write:** Whether to allow the client user to modify the data on the server after logging in.
- **Username:** FTP client login username.
- **Password:** FTP client login password.

8.3.3 System Storage

Path: **System -> Storage -> System Storage**

Storage management of recording files and voice data in the system.

When the system storage is full, you can clear the recording files and voice data files in the system storage.



8.4 Network Settings

8.4.1 Network Profiles

Path: *System -> Network Settings -> Network Profiles*

WAN

Network Mode [?]

* IP Address

* Netmask

Gateway

Primary DNS

Alternative DNS

Enable Virtual IP [?]

The WAN network interface of FCM5600 IPPBXs could be configured to work in Static IP, DHCP or PPPoE mode. In most cases assign a static IP would be the best practice. As all the IP phones will communicate with the IPPBX through this IP address.

On WAN port, gateway and DNS could be configured so the IPPBX could have Internet access, as a result, SIP trunking and remote extensions could work.

As for LAN, it's only used when you don't want the IPPBX system to have Internet access.

LAN

* IP Address

* Netmask

Enable Virtual IP [?]

Default IP on LAN port is 192.168.10.100, you may change this IP but LAN IP should NOT be in the same network segment as WAN port.

8.4.2 VLAN

Path: **System -> Network Settings -> VLAN**

With a layer-3 switch you can configure VLAN on FCM5600 IPPBX system to divide the VoIP and data traffic. Voice VLAN can ensure that phones remain working even when the data network is congested.

To set VLAN, navigate to web menu Network Settings->Network->VLAN. As you can see here on this page, you are able to configure 4 VLANs, 2 each for WAN or LAN port.

VLAN

WAN Port VLAN 1

Enable

* VLAN ID

* IP Address

* Netmask

WAN Port VLAN 2

Enable

* VLAN ID

* IP Address

* Netmask

LAN Port VLAN 1

Enable

LAN Port VLAN 2

Enable

Ensure VLAN IPs for VLAN1 and VLAN2 of WAN and LAN interfaces are in several different network segments.

8.4.3 VPN

Path: **System -> Network Settings -> VPN**

VPN (Virtual Private Network) is mainly used for setting up long-distance and/or secured network connections. When used on the IPPBX system, all phone calls made and received



are encrypted so it secures your remote offices/extensions' phone services. Built-in VPN Server on the FCM5600 IPPBX system is an easy way to set up a secured connection between other FCM5600 IPPBXs or IP phones. You don't need to build a dedicated VPN server or buy a VPN router. This is also a workaround to avoid firewall issues when configuring remote VoIP client such as SIP protocol which is notoriously difficult to pass through a firewall due to its random port numbers to establish connection.

OpenVPN Server

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. It is capable of traversing network address translators (NATs) and firewalls.

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

To configure OpenVPN server, please click on the **OpenVPN Server** button to show the configurations.



Configure the VPN server before turning it on.

In the **Certificate** field click on **Create** button to create the OpenVPN certificate .

Specify your customized information and click on [Submit](#) button to continue. Click on [Configure](#) button to setup the OpenVPN server.

OpenVPN Server configuration ✕

Stealth

* Port

Protocol

Device Node

Cipher

Compress LZO

TLS Server

Remote Network IP

Remote Network Netmask

Route IP

Route Netmask

Client to Client

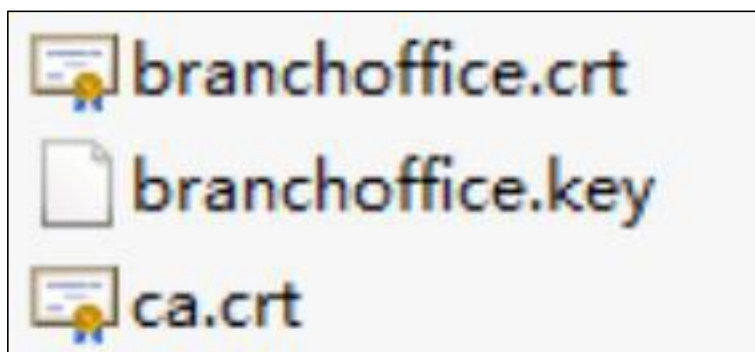
- **Stealth:** Certain deep packet inspection firewalls might not allow OpenVPN traffic, stealth SSL tunneling can disguise your OpenVPN traffic under the HTTPS traffic which is often seen as HTTPS traffic by the DPI.
- **Port:** OpenVPN service port, the default port is 1194. You will need to forward this port on your router for the clients being able to connect to the server.
- **Stealth Port:** OpenVPN service port, the default is 1194.
- **Protocol:** You can choose either UDP or TCP. But the port forwarding (1194) on your router should be using the same protocol.
- **Device Node:** TUN or TAP; A TAP device is a virtual Ethernet adapter, while a TUN device is a virtual point-to-point IP link.

- **Cipher:** Cipher (or cypher) is an algorithm for performing encryption or decryption.
- **Compress LZO:** LZO is an efficient data compression library which is suitable for data de-compression in real-time.
- **TLS-Server:** TLS is an excellent choice for authentication and key exchange mechanism of OpenVPN.
- **Remote Network:** The OpenVPN client network, VPN server uses the first available IP of the client network.
- **Route:** The route entries adjust the local routing table, telling it which network to route over the VPN.
- **Client-to-Client:** Client-to-Client can enable intercommunication between clients.

Once configurations done, click on [Submit](#) button to save the configurations and you may create certificates for the OpenVPN clients now. Each VPN client needs a certificate to be able to connect to the server. OpenVPN server on FCM5600 IPPBX system can connect up to 20 clients.



Each certificate entry created here is for an OpenVPN client. Download the certificate and extract files inside the package, 3 files you'll get and they should be uploaded on a client to be able to connect to this server.



Finally turn on the enable switch to enable OpenVPN server.

OpenVPN Client

To configure OpenVPN client, please click on the “Open VPN Client” button to show the configurations.

VPN Settings

PPTP Client
OpenVPN Client

Enable

CA Certificate [?]	Done	Upload	Delete
Client Certificate [?]	Done	Upload	Delete
Client Key [?]	Done	Upload	Delete

[Configure](#)

The certificate files downloaded from the OpenVPN server should be uploaded here. In the **CA Certificate** field upload the ca.crt file.

In the **Client Certificate** field upload the xxxx.crt file. In the **Client Key** field upload the xxxx.key file.

When done, click on the [Configure](#) button to configure the OpenVPN client to connect to the server.

OpenVPN Client Configuration ✕

* Server IP [?]

Stealth

* Port [?]

Protocol [?] ▼

Device Node [?] ▼

Cipher [?] ▼

Compress LZO [?]

Default Gateway [?]

[Cancel](#) [Submit](#)

- In the **Server Address** field you should specify the OpenVPN server address, which can be a public IP or a domain name.
- Enable **Stealth** if the OpenVPN server has enabled it.
- The **Port** number should be exactly the same as on the OpenVPN server. By default it's 1194.
- Please use the same **Stealth Port** as the OpenVPN server.
- The transport **Protocol** should be exactly the same as on the OpenVPN server. By default UDP is used.
- **Device Node** could be set to TUN or TAP, a TAP device is a virtual Ethernet adapter, while a TUN device is a virtual point-to-point IP link.
- **Cipher** (or Cypher) is an algorithm for performing encryption or decryption.
- Either toenable **Compress LZO** or not, depends on if you have enabled it on the server.
- If **Default Gateway** enabled, it will use VPN connection as default gateway, data which should be sent to the default gateway will now be sent though VPN connection.

Once done, click on submit to save the configurations. Finally click on Enable switch to switch on the VPN client connection.

VPN Settings

PPTP Client
OpenVPN Client

Enable

CA Certificate ⓘ	Done	Upload	Delete
Client Certificate ⓘ	Done	Upload	Delete
Client Key ⓘ	Done	Upload	Delete

[Configure](#)

VPN Client Status

Address
Mode
Status

And you may check the VPN connection status in the **VPN Client Status** section.

VPN Client Status	
Address	172.16.0.6
Mode	openvpn
Status	Connected

In the VPN client status section the VPN client IP, the VPN type and the connection status will be displayed.

PPTP VPN Server

PPTP (The Point-to-Point Tunneling Protocol) uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products.

Click on “PPTP Server” button to show the configurations.



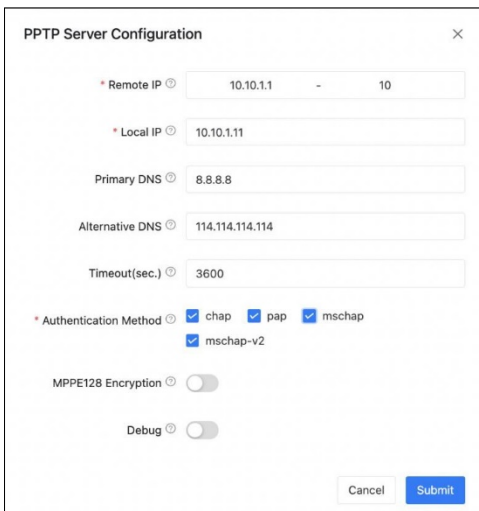
VPN Settings Please configure VPN server/client before enabling it

PPTP Client
 OpenVPN Client
 PPTP Server
 OpenVPN Server

Enable

[Configure](#)

Configure the PPTP VPN server before enabling it.



PPTP Server Configuration [X]

* Remote IP -

* Local IP

Primary DNS

Alternative DNS

Timeout(sec.)

* Authentication Method chap pap mschap
 mschap-v2

MPPE128 Encryption

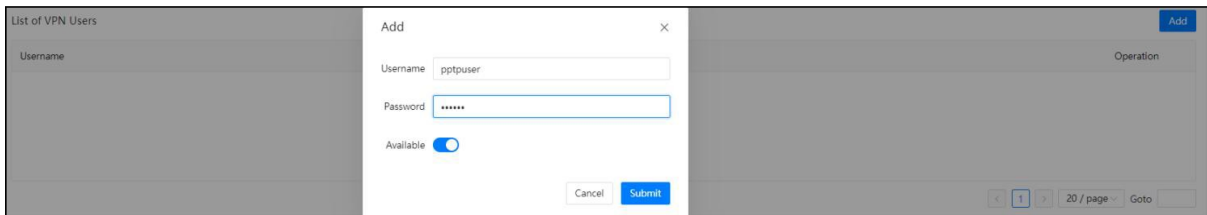
Debug

[Cancel](#) [Submit](#)

- **Remote IP:** PPTP VPN remote network IP range, there must be 10 or less available IP addresses between start IP and end IP.

- **Local IP:** PPTP VPN local server IP address.
- **Primary DNS:** Primary DNS for VPN connection.
- **Alternative DNS:** Secondary DNS for VPN connection.
- **Timeout(S):** Session timeout for PPTP tunnels.
- **Authentication Method:** Choose method/methods for the authentication of the VPN clients.
- **chap:** Challenge Handshake Authentication Protocol, CHAP takes a more sophisticated and secure approach to authentication by creating a unique challenge phrase (a randomly generated string) for each authentication.
- **pap:** Password Authenticate Protocol PAP works like a standard login procedure; it uses static username and password to authenticate the remote system.
- **mschap:** MS-CHAP is the Microsoft version of the Challenge-Handshake Authentication Protocol.
- **mschap-:** Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP), this provides stronger security for remote access connections.
- **Enable MPPE128 Encryption:** Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol (PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections with 128-bit key.
- **Debug:** Enable debug for PPTP VPN connection, debug information will be written into system logs.

Once server configurations done, you may create PPTP client users, each user created is for a VPN client to connect. PPTP VPN server on FCM5600 IPPBX can connect up to 20 PPTP VPN clients.



Remember to set the Availability to Yes, when you don't want this user to connect, just set Availability to No or you may remove the user from the VPN user list.



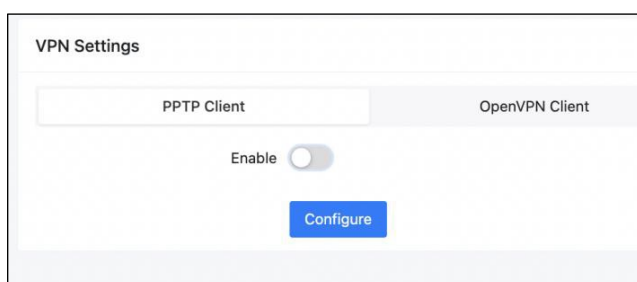
Username	Available	Operation
pptpuser	Yes	 

Finally click on the Enable switch to turn the PPTP VPN server on.

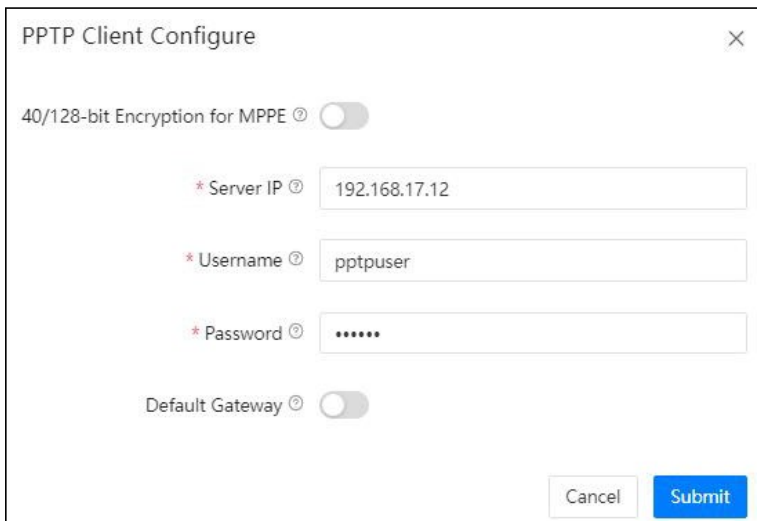


PPTP VPN Client

To configure PPTP VPN client, please click on the “PPTP Client” button to show the configurations.



Configure PPTP VPN client settings before enabling it.



- **Enable 40/148-bit encryption for MPPE:** Tick to enable 40-bit key (standard) or 128-bit key (strong) MPPE encryption schemes.
- **Server Address:** PPTP VPN server public IP.
- **Username:** PPTP VPN username given by the VPN server.
- **Password:** PPTP VPN user password given by the VPN server.
- **Default Gateway:** If enabled, all network traffic will go through the PPTP VPN connection.

Once done, click on [Submit](#) button to continue, and now you may click on Enable switch to turn on PPTP VPN client.



The screenshot shows the 'VPN Settings' page. At the top right, there is a red warning message: 'Please configure VPN server/client before enabling it'. Below this, there are four tabs: 'PPTP Client', 'OpenVPN Client', 'PPTP Server', and 'OpenVPN Server'. The 'PPTP Client' tab is active. Under this tab, there is an 'Enable' toggle switch which is currently turned on. Below the toggle is a blue 'Configure' button. At the bottom of the page, there is a section titled 'VPN Client Status' with fields for 'Address', 'Mode', and 'Status'.

Later it should be connected to the PPTP VPN server, and the connection status will be displayed in the **VPN Client Status** section.



The screenshot shows the 'VPN Client Status' section. It displays the following information:

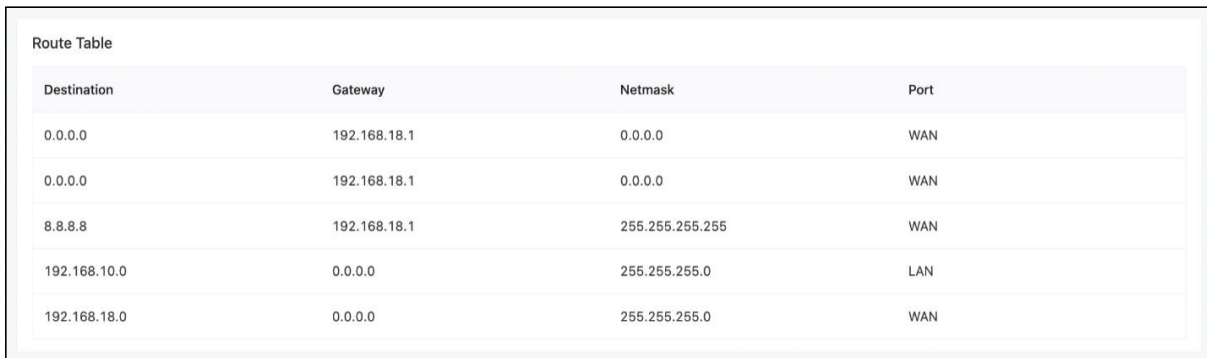
VPN Client Status	
Address	172.16.0.2
Mode	pptp
Status	Connected

In the VPN client status section the VPN client IP, the VPN type and the connection status will be displayed.

8.4.4 Static Routing

Path: **System -> Network -> Static Routing**

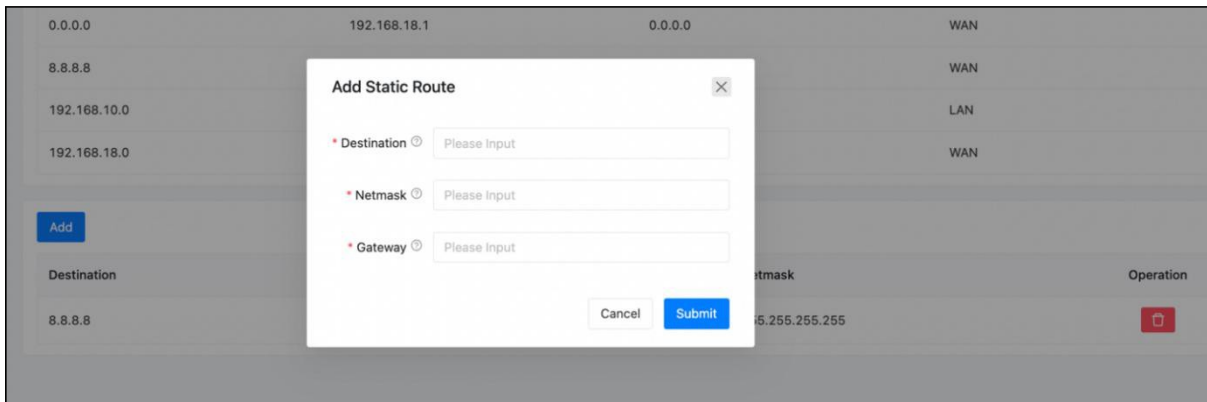
Static Routing is a form of routing that occurs when a router uses a manually configured routing entry, rather than information from a dynamic routing protocol to forward traffic.



The screenshot shows the 'Route Table' section. It displays a table with the following data:

Destination	Gateway	Netmask	Port
0.0.0.0	192.168.18.1	0.0.0.0	WAN
0.0.0.0	192.168.18.1	0.0.0.0	WAN
8.8.8.8	192.168.18.1	255.255.255.255	WAN
192.168.10.0	0.0.0.0	255.255.255.0	LAN
192.168.18.0	0.0.0.0	255.255.255.0	WAN

When needed you may click on the [Add](#) button to add a manual static route.



- **Destination** is the IP address of the destination host or network address.
- If the packets are to be sent to the **Destination** specified above, then send them to the **Gateway** address.

After the new record has been manually created you will see it listed in the **route** table.

8.4.5 DHCP Server

Path: *System -> Network -> DHCP Server*

DHCP (Dynamic Host Configuration Protocol) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

With DHCP, computers/IP phones request IP addresses and networking parameters automatically from FCM5600 IPPBX WAN/LAN port which saves administrators a lot of time when compared with having to configure these settings manually.

Before activating DHCP services, please ensure there's no other DHCP server running in your LAN, otherwise, there will be a collision between servers.

Set the DHCP server network parameters and turn it on.

DHCP Services

Enable

Port

* Start IP Address

* End IP Address

* Netmask

Gateway

DNS

TFTP

* Address Lease Time(hour) -- +

The DHCP clients which obtained IP addresses from the IPPBX system DHCP server will be listed on the right side of the page, in the **DHCP Clients** section. If you want some host or client to always get the same IP address, **IP Address Reservation**

will help. Click on the button.

Add ×

* Name

* MAC Address

* IP Address

Just simply specify the MAC address of the client device and associate an IP address with it, and this IP will always be reserved for this specific client device.

8.4.6 SNMP

Path: **System -> Network -> SNMP**

SNMP Settings

Read Only

Enable

* Community

* Network

* Subnet Length

Read Write

Enable

* Community

* Network

* Subnet Length

- **Enable:** Turn On/OFF SNMP
- **Community:** Community tag
- **Network:** The working network of SNMP
don't have to add them to the IP whitelist.

8.5 Email Services

8.5.1 Mail Server Settings

Path: **System -> Email Services -> Mail Server Settings**

Various kinds of Emails could be sent from the FCM5600 IPPBX system. The Emails could be automatically sent by the IPPBX system in certain circumstances or manually sent by admin and operator users.

To configure the IPPBX system being able to send out emails, mail (SMTP) server needs to be configured at first priority.

We have built-in some popular Email service providers' SMTP configuration templates for users to quickly deploy their mail server.

Mail Server Settings ⊙

Mail Service Provider ⊙

* SMTP Server ⊙

* Port ⊙

SSL ⊙

* Email ⊙

* Password ⊙

- In the **Mail Service Provider** dropdown list select your Email service provider. If it's not included here, please choose **Other**.
- Once you have selected the mail service provider the **SMTP Server** field will be auto filled. Otherwise you'll have to manually input the SMTP Server address.
- Default SMTP service **Port** is 25, but with SSL/TLS it would be 465. Otherwise you'll have to input the actual port number your mail service provider uses.
- **SSL** encrypts a communication channel between the IPPBX system and the SMTP server. Most of the mail service providers have implemented SSL support.
- In the **Email** field input the Email account to be used by the IPPBX system, all mails from the IPPBX system will be sent out by this mail account.
- In **Password** field input the password of the Email account you have specified.

Once done the above settings, click on button to make configurations effective. And you may click on "Test" button and input an Email address to send a test email to verify if the mail server is successfully deployed.

Note: You may need to activate SMTP service from your Email web portal before you can successfully configure SMTP server on the IPPBX system.

8.5.2 Voicemail to Email Settings

Path: **System -> Email Services -> Voicemail to Email Settings**

Voicemail to Email is a very useful feature for the extension users, as the IPPBX system has the ability to send received new voicemail messages of their extensions to their Email box. It could be an Email notification or administrator could set the IPPBX system to send Email with voice messages attached in the Email notifications.

Email Templates

Voicemail to Email

Mail Subject: IPPBX New Voicemail Notification

Mail Body: Hi \${VM_NAME} \nYou have got a new voicemail from phone number (\${VM_CALLERID}) at \${VM_DATE}.\nSent by IP Phone System.

Variables: \${VM_NAME} \${VM_DUR} \${VM_MAILBOX} \${VM_CALLERID} \${VM_MSGNUM} \${VM_DATE}

Deliver Message as Attachment

- The **Mail Subject** field you can set customized Email subject which will be received by the extension users when they have new messages.
- The **Mail Body** is also customizable, you may use variables in the mail body to describe the new voice messages they got. The format of the variables must be the same as listed in the **Variables** section.
- **Variables** could be used in the mail body to indicate the extension users about their new voice message details.
- With **Deliver Message as Attachment** option enabled the voice message will be attached to the notify Email, users may playback the voice messages when they got the notify Email.

With Voicemail to Email enabled and Mail Server configured, the extension users will get Email notifications when new voice message received on their extensions, just make sure the extensions have their Email addresses specified.

8.6 Diagnostic

8.6.1 PING

Path: **System -> Diagnostic -> PING**

The ping command is a very common method for troubleshooting the accessibility of devices. It uses a series of Internet Control Message Protocol (ICMP) Echo messages to determine:

- Whether a remote host is active or inactive.
- The round-trip delay in communicating with the host.
- Packet loss.

Specify the domain or IP of the host you want to contact, then click on **Submit** button, and then the command begins to process. You will receive results output from the system indicating the reachability of the destination.

Ping

IP Address / Domain * **Submit**

```

PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=49 time=61.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=49 time=61.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=49 time=61.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=49 time=61.3 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 5ms
rtt min/avg/max/mdev = 61.314/61.397/61.443/0.252 ms
          
```

8.6.2 Trace Route

The traceroute command is used to discover the routes that the packets actually took while traveling to their destination.

Path: **System -> Diagnostic -> Traceroute**

In the IP Address/Domain Name field specify the IP or domain name that you want to lookup and click on **Submit** button to begin tracing.

Trace Route

IP Address / Domain * Submit

```

tracert to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 * * *
 2 192.168.7.1 (192.168.7.1)  0.889 ms  1.522 ms  2.045 ms
 3 183.221.89.129 (183.221.89.129)  5.718 ms  6.511 ms  7.279 ms
          
```

During the whole process each step will output in the Results field, you can view which routes the packets have taken before reaching their final destination.

8.6.3 TCP Dump

Ethernet capture uses TCPDUMP which is a common packet analyzer that allows users to capture TCP/IP and other packets being transmitted or received over a network to which the FCM5600 IPPBX is attached. The captured packets can be downloaded from the IPPBX system and been analyzed on your Windows PC to display the SIP traffic details. It can be used to debug a VoIP call problem.

Path: **system -> Diagnostic -> Ethernet Capture**

To capture the network traffic, you need to select the network interface according to on which the IPPBX system is working on. Then click on Start button to start capturing the network traffic.

TCP Dump

Interface * Stop Start

Once the process begins, the Start button will change to Stop. At this moment, you should make a call to recur the phone call problem or ensure some other problem had recurred, so the captured network traffic could content errors that are helpful for troubleshooting. Once done click on Stop button, and the captured network traffic will be automatically downloaded.

The downloaded file could be analyzed by Wireshark or you could send the file to FIBERME support team for help.

8.7 Security Center

FCM5600 IPPBX system has been preconfigured with a built-in firewall which prevents your IP phone system from unauthorized access, malicious users and some other attackers.

You may not need to specifically configure the firewall settings but for security precautions please always keep it on.

8.7.1 Firewall

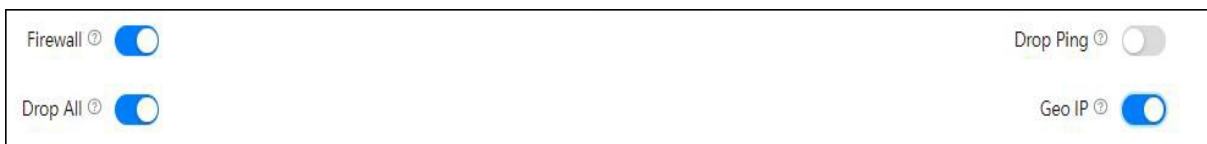
Path: **System** -> **Security Center** -> **Firewall**

FCM5600 IPPBX system uses Fail2Ban to perform intrusion detection and uses iptables to block any attack attempts.



- First of all make sure the **Firewall** option is enabled. Only consider disabling your firewall if your FCM5600 IPPBX is behind a router/firewall without any port forwarding from the Internet.
- **Drop Ping** will cause the system to ignore ping request. If enabled, you cannot ping the IPPBX system.
- **Drop All** will cause all packets sent to the IPPBX system being dropped, this will cause FCM5600 IPPBX system to block all communication with the outside world. Except web UI still works in local network, other services will all be terminated.
- **Geo IP** is a security policy which can be used to grant access of IP addresses from certain countries/regions, all IP addresses from other countries/regions which are not specified will all be blocked. By default, web UI will still be accessible. Enabling **Geo IP** requires **Drop All** to be enabled too. To implement Geo IP please follow the steps below.

Step 1: Enable Geo IP and Drop All



Step 2: Select trusted countries/regions

Geo IP

Please Select ▼

Submit

Geo IP can be used to grant access of IP addresses from certain countries/regions, all IP addresses from other countries/regions which are not specified will all be blocked. You will also need to add a common rule to grant access of the local IP addresses.

Besides selecting the trusted IP addresses from certain countries/regions, you'll still need to add a common rule in the **Common Rules** section to grant access or the local network hosts/devices.

Step 3: Add a common rule to grant access of your local LAN.

Add ×

* Name

* Action

* Protocol

IP Address

Netmask

Port

Mac Address

- The **Action** of this rule needs to be set as **Accept**.
- **Protocol** should be set as **TCP/UDP**.
- **IP** should be the local network address instead of a single IP address.
- **Netmask** should be the subnet mask of the network address.
- The **Port** range determines which kind of services to be granted. In this case you may leave it blank to grant local network all access to the IPPBX system.
- **Mac Address** determines the action to be taken according to the Mac address of a device instead of its IP address, it only works with devices within the same local network because Mac addresses are not routable. In this case you are going to grant access of all the local network hosts/devices, so you may leave it blank.

By now, Geo IP security policy should work. The private IP addresses from your local network and the public IP addresses from the countries/regions you've selected should be able to access your IPPBX system. Other IP addresses will all be blocked.

Common Rules can be used to configure the firewall to grant or deny an IP address or a network from communicating with the IPPBX system. Even the service port number can be specified so it can grant or deny a specific IP or network to access a specific service. The priority from high to low of the firewall rules is from the top of the list to the bottom.

If you are going to grant access of some kind of services to specific IP address or network, add the grant rule/rules first then add the deny rules. If the order of the rules is not correct you may use the arrows in the **Priority** column to adjust the order of the rules.

Priority	Name	Action	Protocol	IP Address	Port	Mac Address	Operation
↓ ↑	AcceptAMI	Accept	TCP/UDP	192.168.17.0	5038 - 5038		 
↕ ↑	BlockAMI	Drop	TCP/UDP		5038 - 5038		 

In the above given example, the 2 rules “AcceptAMI” and “BlockAMI” limited that only the IP addresses from network 192.168.17.0 can have AMI access. Except IP from this network others will all be denied to access. In this case, if the “AcceptAMI” rule is moved beneath the “BlockAMI” rule, then the AMI port will be totally lockdown, no one can access it.

Note: If you are going to add rules to block some IP addresses from accessing some kind of services on the IPPBX system, be sure you add the correct IP/network address (if not defined, the firewall will consider as ALL), and the correct service port number (if not define, the firewall will consider as ALL), otherwise misconfiguration of a deny rule might cause the IPPBX system total lockdown, only way would be using Console to unlock the IPPBX from command lines.

Auto Defense will help with the prevention of DDOS attacks.

Add
✕

* Name

* Port -- +

* Protocol ▾

* Packet -- +

* Interval -- +

You may specify the service port number and the maximum packets to be accepted on this port number in a certain time interval. Except the specified number of packets, more packets sent within the time interval will be dropped by the IPPBX system.

8.7.2 Intrusion Detection and Prevention

Path: **System -> Security Center -> Intrusion Prevention**

FCM5600 IPPBX system uses Fail2Ban to perform intrusion detection. Fail2Ban is an intrusion prevention framework written in the Python programming language. It works by reading Asterisk logs and some other logs in the IPPBX system, and uses iptables profiles to block brute-force attempts.

There are 4 default intrusion detection and prevention rules to secure SIP, IAX2, Web and SSH services on your IPPBX system. And by default all of them are activated to keep your IPPBX system safe.

SIP Intrusion Detection and Prevention

Intrusion Detection and Prevention

* Illegal Attempts -- +

* Observation(sec.) -- +

* Ban for(sec.) -- +


Each of the intrusion detection and prevention rule is configured with a maximum **Illegal Attempts** and the **Observation** time duration, once the **Illegal Attempts** reached the given value in the given **Observation** time duration, the source IP address of where the illegal attempts coming from will be banned by the firewall for the given time duration specified in Ban for field. Banned IP will be listed on the **IP Blacklist** page.

Besides the 4 default rules, if you want to add more rules you can do it on the **Firewall** page **Auto Defense** section.


8.7.3 IP Blacklist

Path: **System** -> **Security Center** -> **IP Blacklist**

IP Blacklist will list all suspected intruders/attackers' IP addresses. The list is automatically generated by the system firewall if possible intrusion/attacking had been detected. And the list will show the IP address of the banned hosts, as well as what kind of service intrusion was detected.



Type	IP Address	Operation
 No Data		

If an IP address appears incorrectly in the list of rejected IP, you can click on the  button to remove it from the IP blacklist.

8.7.4 IP Whitelist

Path: **System** -> **Security Center** -> **IP Whitelist**

IP Whitelist allows you to add IP addresses and network addresses to the IPPBX system as a trusted. The IP addresses in the whitelist will always be treated as trusted IP and will not be regulated by the firewall rules.

Add
✕

* Name

* IP Address

* Netmask

Protocol SIP IAX HTTPS SSH

Enable

Adding a trusted IP to the IP whitelist, you may also define which kind of services it could access.

- **SIP** allows the IP to be able to register SIP extensions.
- **IAX** (IAX2) allows the IP to be able to register IAX extensions.
- **HTTPS** allows the IP to access the web UI of the IPPBX system.
- **SSH** allows the IP to access the IPPBX system command lines through SSH.

Note: You'll only need to add trusted IP addresses to the IP Whitelist when you have configured Drop All or Geo IP security policies. And in the policies these IP addresses are not included as trusted IP addresses. Otherwise you don't have to add them to the IP whitelist.

8.8 Backup/Upgrade

8.8.1 Upgrade

Path: **System-> Backup/Upgrade -> Upgrade**

System / Backup/Upgrade / Upgrade

Version

Version v4.0.0.beta3

Update Time 2022-01-14/09:26:33

Upgrade

File

Please click on the **Upload** button and select the corresponding firmware for the upgrade process. If an incorrect model of device firmware is uploaded, the upgrade will fail. After the upgrade is successful, the system will automatically restart.

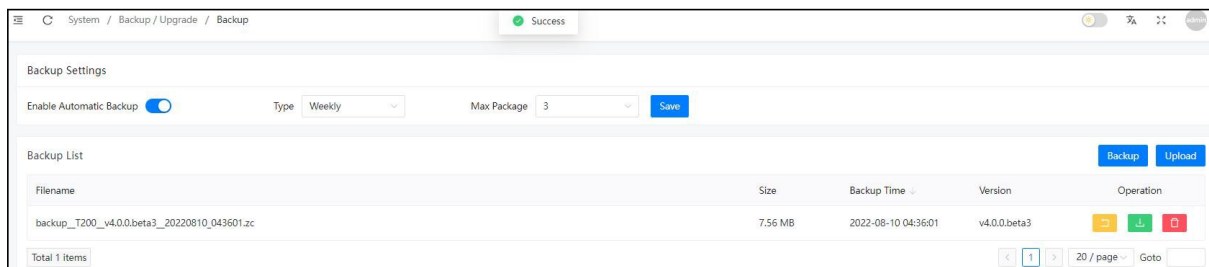
8.8.2 Backup

Taking a backup on FCM5600 IPPBX system is the same as when you create a recovery point on your Windows system. By restoring the backup you can recover the FCM5600 IPPBX system configurations to the time point when it was still functioning well.

Normally the first backup should be taken when you have finished configuring the IPPBX to work for the very first time. Also, when you have applied new changes to your configuration is always a good time to take another backup.

Path: **System->Backup/Upgrade -> Backup**

You may click on **Backup** button to take a backup of your system when necessary. A backup file will be generated.



- **Enable Auto Backup:** Enable/Disable auto backup service
- **Type:** Frequency of auto backup, such as daily, weekly, etc.
- **Max Package:** The maximum number of backup packages can be reserved in the system

File name is generated according to the software version, date and exact time when the backup is performed. You may click on **Download** button to download the backup to your operating system. Or click on **Delete** button to delete it from the IPPBX system.

When you want to restore the backup, you may click on the **Restore** button. Restoring a backup will cause the system reboot, so please make sure there are no phone calls going on in the IPPBX system before you doing this.

If you are going to restore an offline backup (backup downloaded to your operating system) please click on the **Upload** button.

Note: Backups will not be cleared after a system reset. So you may not need to download the backup to your operating system. And after a system reset, you may skip the quick setup wizard and go to the backup page to restore a backup directly to recover your previous configurations.

8.9 System Logs

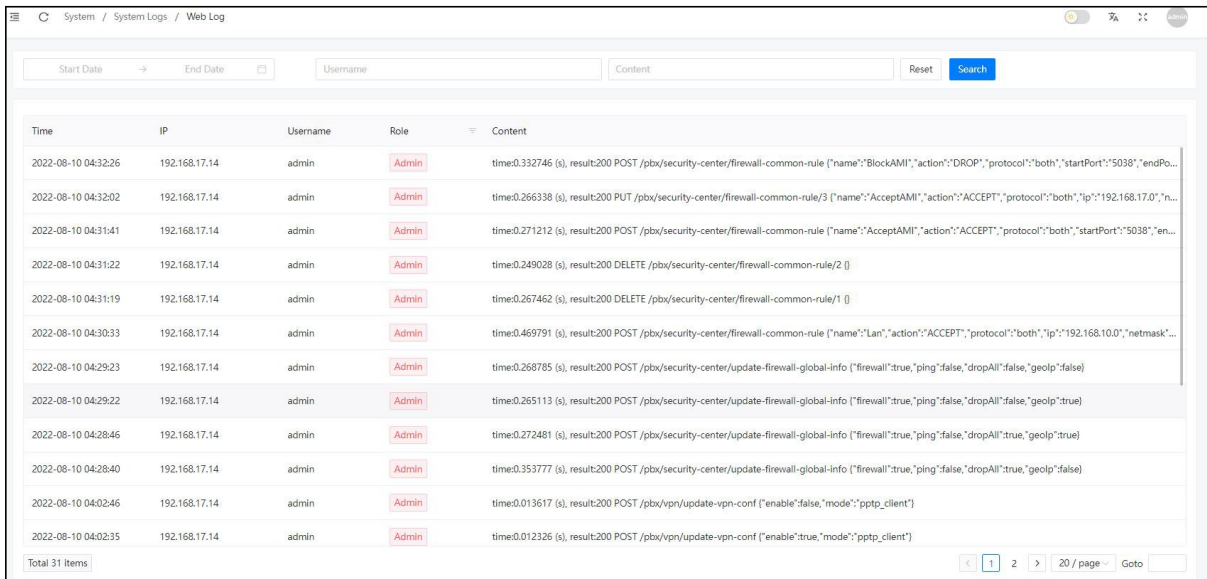
8.9.1 Web Log

Path: **System-> System Logs -> Web Log**

On Web Access Logging page you may check all the logs of the web access records, including admin user, operator user and extension users.

In the **From** and **To** fields set the start and end date, in User dropdown list select the user role if you want to search per the type of users, optionally if you want to search according to the user's IP address you may also specify the IP address in the **IP Address** field then finally click on **Search** button.

The searching results are as below.



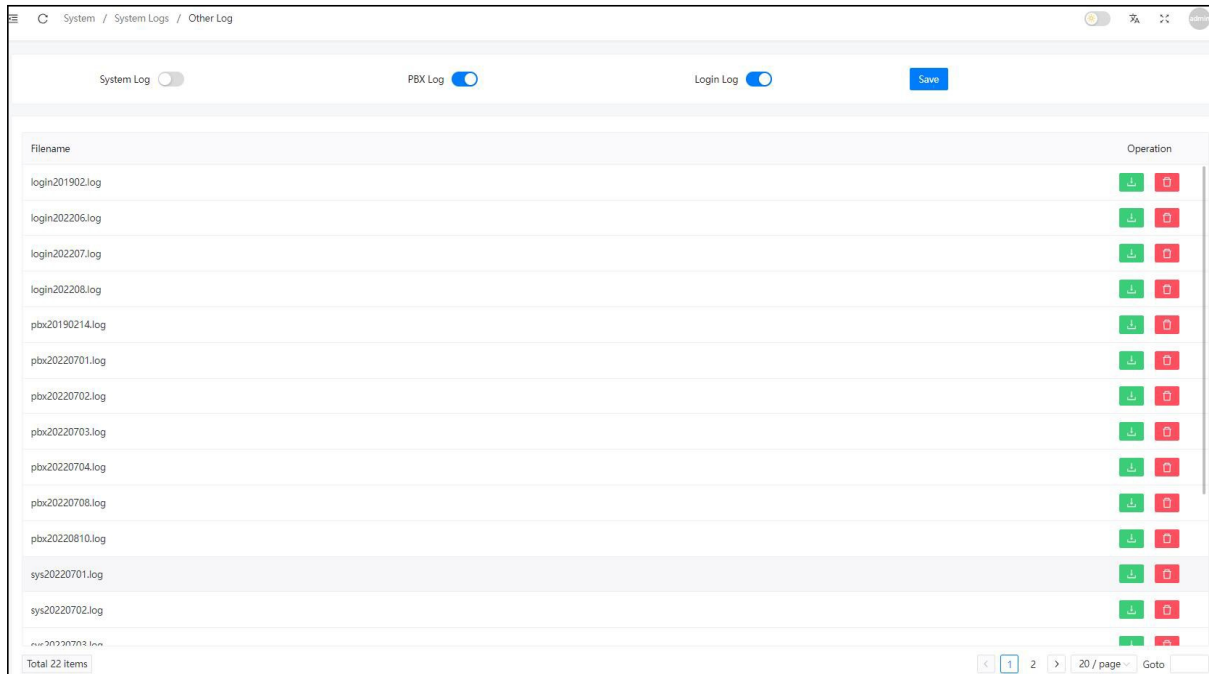
Time	IP	Username	Role	Content
2022-08-10 04:32:26	192.168.17.14	admin	Admin	time:0.332746 (s), result:200 POST /pbx/security-center/firewall-common-rule {"name":"BlockAMI","action":"DROP","protocol":"both","startPort":"5038","endPo...
2022-08-10 04:32:02	192.168.17.14	admin	Admin	time:0.266338 (s), result:200 PUT /pbx/security-center/firewall-common-rule/3 {"name":"AcceptAMI","action":"ACCEPT","protocol":"both","ip":"192.168.17.0","n...
2022-08-10 04:31:41	192.168.17.14	admin	Admin	time:0.271212 (s), result:200 POST /pbx/security-center/firewall-common-rule {"name":"AcceptAMI","action":"ACCEPT","protocol":"both","startPort":"5038","en...
2022-08-10 04:31:22	192.168.17.14	admin	Admin	time:0.249028 (s), result:200 DELETE /pbx/security-center/firewall-common-rule/2 []
2022-08-10 04:31:19	192.168.17.14	admin	Admin	time:0.267462 (s), result:200 DELETE /pbx/security-center/firewall-common-rule/1 []
2022-08-10 04:30:33	192.168.17.14	admin	Admin	time:0.469791 (s), result:200 POST /pbx/security-center/firewall-common-rule {"name":"Lan","action":"ACCEPT","protocol":"both","ip":"192.168.10.0","netmask"...
2022-08-10 04:29:23	192.168.17.14	admin	Admin	time:0.268785 (s), result:200 POST /pbx/security-center/update-firewall-global-info {"firewall":true,"ping":false,"dropAll":false,"geolp":false}
2022-08-10 04:29:22	192.168.17.14	admin	Admin	time:0.265113 (s), result:200 POST /pbx/security-center/update-firewall-global-info {"firewall":true,"ping":false,"dropAll":false,"geolp":true}
2022-08-10 04:28:46	192.168.17.14	admin	Admin	time:0.272481 (s), result:200 POST /pbx/security-center/update-firewall-global-info {"firewall":true,"ping":false,"dropAll":true,"geolp":true}
2022-08-10 04:28:40	192.168.17.14	admin	Admin	time:0.353777 (s), result:200 POST /pbx/security-center/update-firewall-global-info {"firewall":true,"ping":false,"dropAll":true,"geolp":false}
2022-08-10 04:02:46	192.168.17.14	admin	Admin	time:0.013617 (s), result:200 POST /pbx/vpn/update-vpn-conf {"enable":false,"mode":"pptp_client"}
2022-08-10 04:02:35	192.168.17.14	admin	Admin	time:0.012326 (s), result:200 POST /pbx/vpn/update-vpn-conf {"enable":true,"mode":"pptp_client"}

The time of when the login action took place, by which user, the source IP address and the actions taken will all be listed.

8.9.2 Other Log

Path: **System-> System Logs -> Other Log**

Advanced logging can be used for higher level of the IPPBX system troubleshooting.



- **SSH Access Logging** can be used to trace the SSH login records.
- **PBX Logging** can be used to analyze the phone services related issues.
- **The OS Logging** can be used to analyze the IPPBX system OS level issues.

Enable the desired type of logging if you are qualified to analyze such kind of logs or if our support team asked for these kinds of logs for troubleshooting, otherwise please keep them disabled.

8.10 Settings

8.10.1 Account

The Account page is for managing different user roles and login accounts within the entire IPPBX system. Please click on the “Add” button to create a new user account and select the corresponding user role for this account. When the user role is “Panel User”, an extension number is required to be bound to the user. In addition, the Administrator account can only change the password but cannot be deleted.

Username ↓	Password	Role	Extension	Operation
admin	*****	Admin		
cgg	*****	Panel User	809	
lookingsea	*****	Panel User	808	
接线员	*****	Operator User		
cg	*****	Billing Manager		
admin1	*****	Admin		
zy	*****	Panel User	855	

Total 7 items

< 1 > 20 / page Goto

- **Username/password:** Account username/password
- **Role:** User roles correspond to the their own landing page/software.
- Administrator -> main configuration system web page.
- PBX Panel -> Desktop-based PBX Panel software login.
- Billing -> web-based billing system login.
- Operator -> web-based operator login.
- **Extension:** The extension number that associated to the PBX Panel user.

8.10.2 SSL

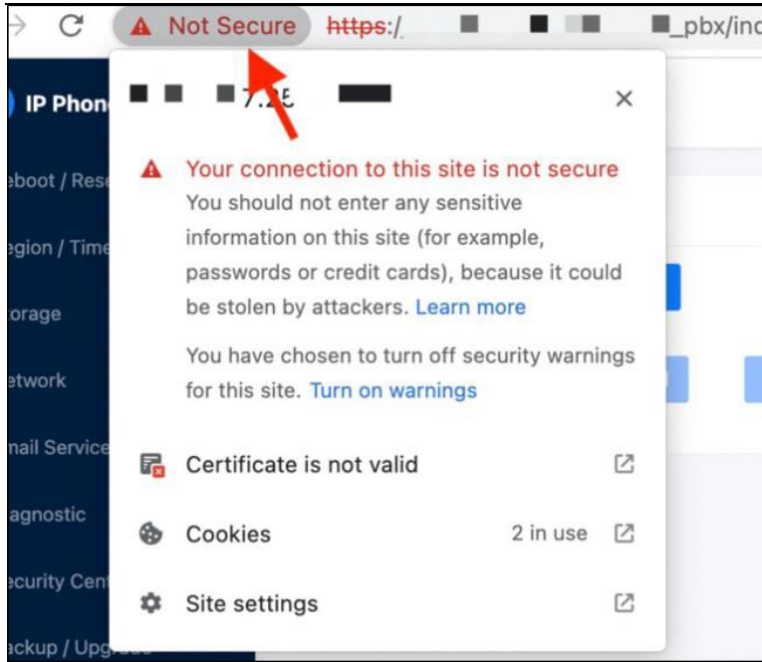
First, click the “Select” button to select the corresponding .key and .pem files. Then, click on the “Upload” button to these files to the system. Last, click on the “Replace Certificate” button will use the new files to replace the old ones. Operation failure if the certificate file is incorrect.

SSL Configuration

Key/Pem File [?] Select

[?] Upload Replace Certificate

You can check from the browser whether or not the certificate file is replaced successfully.



8.10.3 SSH

The IPPBX system disabled the SSH function by default. When the SSH is enabled, user can use the root credential to log in the system via command-line interface. The root user is generally used for system maintenance, and it is recommended to close it after use. You can change the SSH port number or root user's password on this SSH page.

SSH

Enable

Port — +

Change password

* Password 👁

* New Password 👁

* Confirm Password 👁

8.10.4 HTTP

By setting up the relevant parameters of the HTTP service of the web, you can modify the access port of the page.

HTTP Settings

Type ▼

Port 80 redirection

Host 🔗

Port — +

- **Type:** For system security purpose, only HTTPS is allowed.
- **Port 80 redirect:** To facilitate access, directly enter the IP address into the browser and it will be automatically directed to the corresponding protocol and port.
- **Host:** Allowed IP address segment. Default opens all addresses to access.
Non-professionals do not recommend modifying this setting.
- **Port:** Port number



FCM5600 IPPBX Admin Guide

FIBERME Communications LLC

1749 Old Meadow Rd. Suite 401
McLean, VA 22102, USA

sales@fiberme.com | www.fiberme.com