

User's Manual

Internet Telephony PBX System

- ▶ **IPX-1100 / IPX1102**
- ▶ **IPX-2200**



Copyright

Copyright (C) 2024 PLANET Technology Corp. All rights reserved.

The products and programs described in this User's Manual are licensed products of PLANET Technology. This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means by electronic or mechanical including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If user finds information in this manual that is incorrect, misleading, or incomplete, we would appreciate user comments and suggestions.

CE Mark Warning

This device is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Energy Saving Note of the Device

This power required device does not support Standby mode operation. For energy saving, please remove the DC-plug or push the hardware Power Switch to OFF position to disconnect the device from the power circuit.

Without removing the DC-plug or switching off the device, the device will still consume power from the power circuit. In view of Saving the Energy and reducing the unnecessary power consumption, it is strongly suggested to switch off or remove the DC-plug from the device if this device is not intended to be active.

WEEE Warning



To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Trademarks

The PLANET logo is a trademark of PLANET Technology. This documentation may refer to numerous hardware and software products by their trade names. In most, if not all cases, their respective companies claim these designations as trademarks or registered trademarks.

Revision

User's Manual of PLANET Internet Telephony PBX System

Model: IPX-1100/IPX-1102/IPX-2200v3

Release: Feb. 2024

Table of Contents

1. Overview	9
1.1 Introduction.....	9
1.1.1 Package Contents.....	15
1.2 Mechanical Design	16
1.2.1 IPX-1100/IPX-1102/IPX-2200	16
1.2.2 IPX-2200	19
1.3 Plug-in Modules for IPX-2100/IPX-2200/IPX-2500	21
1.4 Specifications	24
1.5 Key Features	30
2. Getting Started	31
2.1 Hardware Installation.....	31
2.2 Accessing the Web GUI.....	31
2.3 Configuration Wizard.....	32
3. Dashboard	42
3.1 Monitor	42
3.2 Extensions	44
3.3 Trunks.....	45
4. Telephony	47
4.1 Extensions	47
4.1.1 Departments	47
4.1.2 IP Extensions.....	49
4.1.3 Analog Extensions.....	55
4.2 Inbound Control.....	57
4.2.1 IVR.....	57
4.2.2 Call Queue.....	59
4.2.3 Time Conditions.....	64
4.2.4 Inbound Routes	66

4.2.5 Direct Routing.....	68
4.2.6 Blacklist	70
4.3 Outbound Control.....	71
4.3.1 Trunks.....	71
4.3.2 Dial Rules.....	80
4.3.3 Dial Permissions	82
4.3.4 PIN Sets.....	84
4.4 Audio Library	85
4.4.1 Music On Hold.....	85
4.4.2 IVR Prompts	86
4.4.3 Custom Prompts.....	87
4.5 Advanced Features.....	88
4.5.1 Call Forward	88
4.5.2 Follow Me	90
4.5.3 Wake Up Call	91
4.5.4 Conference	92
4.5.5 DISA	94
4.5.6 Paging & Intercom.....	95
4.5.7 Smart DID	96
4.5.8 Phonebook.....	97
4.5.9 LDAP	99
4.5.10 Callback	100
4.5.11 Whitelist.....	101
4.6 Preferences	102
4.6.1 Global PBX Options	102
4.6.2 VoIP Advanced	105
4.6.3 Analog Settings	108
4.6.4 Voicemail Settings.....	110
4.7 Feature Codes.....	111
4.7.1 Voicemail Feature Code	111
4.7.2 Call Pickup Feature Code	112

4.7.3	Call Parking Feature Codes.....	113
4.7.4	Call Transfer Feature Code	114
4.7.5	Blacklist Feature Code	115
4.7.6	Call Spy Feature Code	116
4.7.7	Call Queue Feature Code	117
4.7.8	Conference Feature Code.....	118
4.7.9	Wakeup Call Feature Code.....	119
4.7.10	Call Forward Feature Code.....	120
4.7.11	DND Feature Code.....	121
4.7.12	Office Closed Feature Code.....	122
4.7.13	Other Feature Codes	123
5.	Reports.....	124
5.1	Records	124
5.1.1	Call Record	124
5.1.2	Conference Recordings	126
5.1.3	One Touch Recordings.....	127
5.2	Log.....	128
5.2.1	Call Log.....	128
5.2.2	Fax Log	129
6.	Addons.....	130
6.1	API	130
6.1.1	AMI	130
6.1.2	Push Event.....	131
6.1.3	PMS.....	132
6.2	Control Panel	133
6.2.1	Group	133
6.2.2	Settings.....	134
6.3	Hot Standby	135
6.4	AutoConfig	136
6.4.1	Devices.....	136

6.4.2 Files	138
6.4.3 Custom Template	139
7. System	140
7.1 Reboot /Reset	140
7.1.1 Cron Reboot	140
7.1.2 Reboot	141
7.1.3 Reset.....	142
7.2 Region /Time	144
7.3 Storage	146
7.3.1 USB Storage.....	146
7.3.2 FTP Storage.....	148
7.3.3 System Storage.....	150
7.4 Network Settings	151
7.4.1 Network Profiles	151
7.4.2 VLAN.....	152
7.4.3 VPN.....	153
7.4.4 Static Routing.....	165
7.4.5 DHCP Server.....	166
7.4.6 SNMP.....	168
7.5 Email Services	169
7.5.1 Mail Server Settings.....	169
7.5.2 Voicemail to Email Settings.....	171
7.6 Diagnostic	172
7.6.1 PING	172
7.6.2 Trace Route	173
7.6.3 TCP Dump.....	174
7.6.4 Channel Monitor	175
7.6.5 Asterisk CLI.....	176
7.7 Security Center	177
7.7.1 Firewall	177

7.7.2 Intrusion Detection and Prevention.....	181
7.7.3 IP Blacklist.....	182
7.7.4 IP Whitelist.....	183
7.8 Backup/Upgrade	184
7.8.1 Upgrade.....	184
7.8.2 Backup	185
7.9 System Logs	186
7.9.1 Web Log	186
7.9.2 Other Log	187
7.10 Settings	188
7.10.1 Account	188
7.10.2 Plug-in.....	189
7.10.3 Web	190
7.10.4 SSL.....	191
7.10.5 SSH.....	192
7.10.6 HTTP	193

1. Overview

1.1 Introduction

Model	IPX-1100	IPX-1102	IPX-2200
			
Extension User	100	100	200
Concurrent Call	50	50	80
Room Concurrent Call	30	30	60
Recording/Voicemail	400 hours	400 hours	15,000 hours
Module	0	2 Built-in FXO Modules	1/2 Slot(s) for Analog and GSM Module

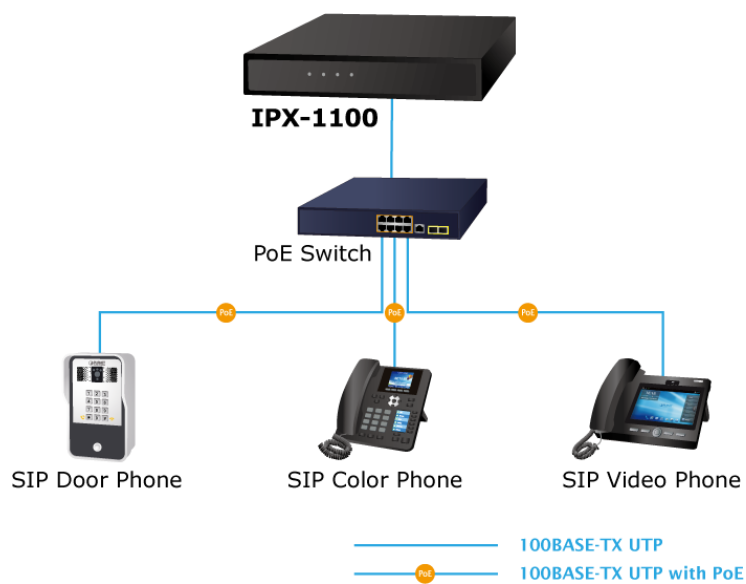
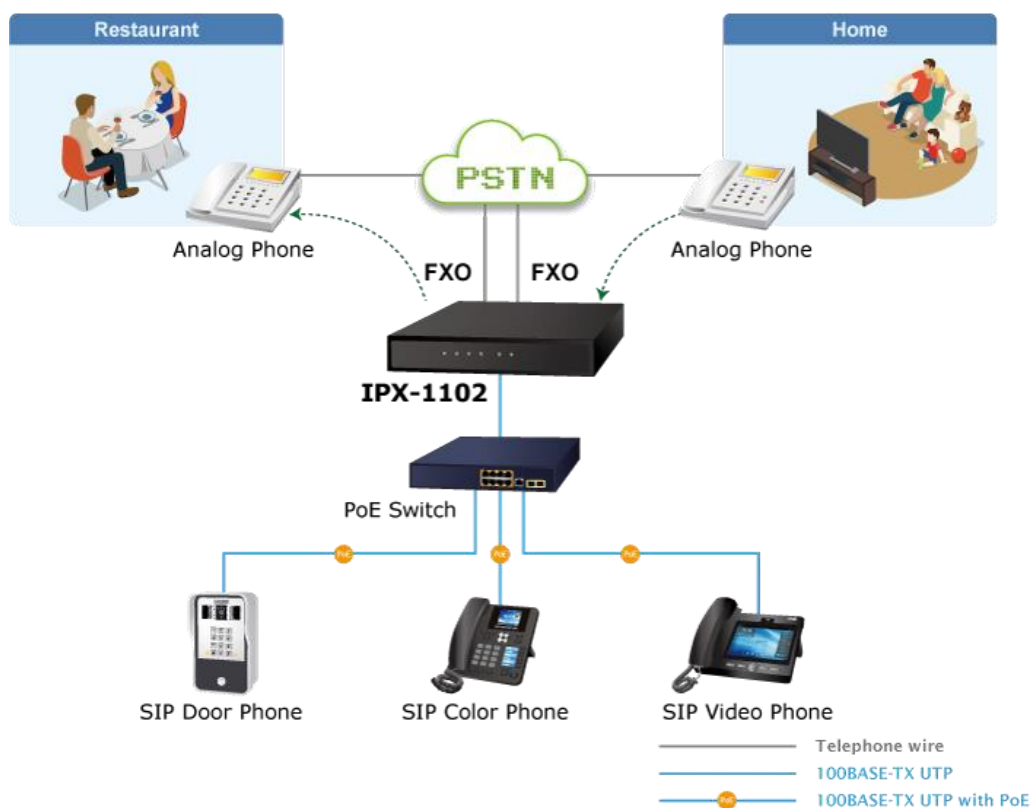
Intuitive, Ease-of-Use IP PBX Management

PLANET next-generation Internet Telephony PBX system is easy to set up and manage thanks to a perceptive web-based user interface and quick setup wizard. Since it is an asterisk-based equipment, the entire benefits of the pre-loaded SIP can be had as any other enterprise-level appliance would come equipped with the feature. The Internet Telephony PBX system is able to accept 100 or 200 user registrations, and easy to manage a full voice over IP system with the convenience and cost advantages. The equipment is best paired with PLANET color IP phones to get the function going smoothly and to have a seamless connection between the software and hardware.

Off-net Calling Capability, Call Restriction, Call Access Control

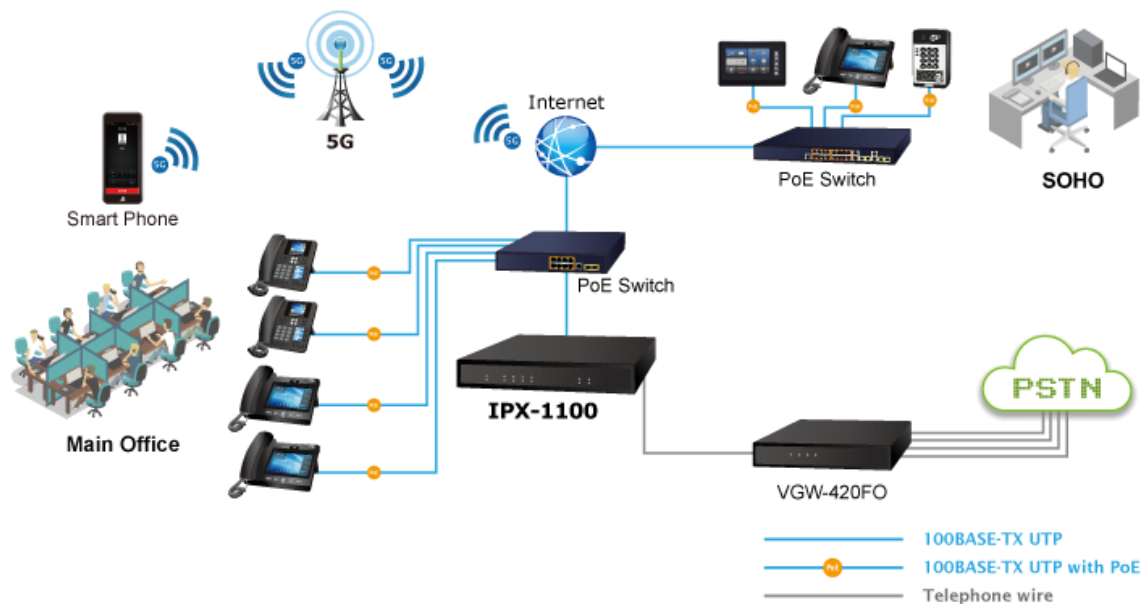
The IPX-1102 comes with 2 FXO ports and the IPX-2200 integrates up to 8 calls via the IPX-21FO (4 FXO), IPX-21SL (2 FXO + 2 FXS) and IPX-21GS (4 GSM) modules to form a feature-rich PBX system that supports seamless communications between the existing PSTN calls, analog phones, IP phones and SIP-based endpoints.

The IPX-1100 is a simplified version of IPX-1102 and is instrumental in establishing a robust VoIP system for small- and medium-sized businesses (SMBs). When seamlessly integrated with PLANET VoIP gateways (VGW-series), the IPX-1100 extends support for analog connections. This integration guarantees seamless communication encompassing the existing PSTN calls, analog phones, IP phones, and SIP-based endpoints.



Replacing Old PBX Easily without New Wiring

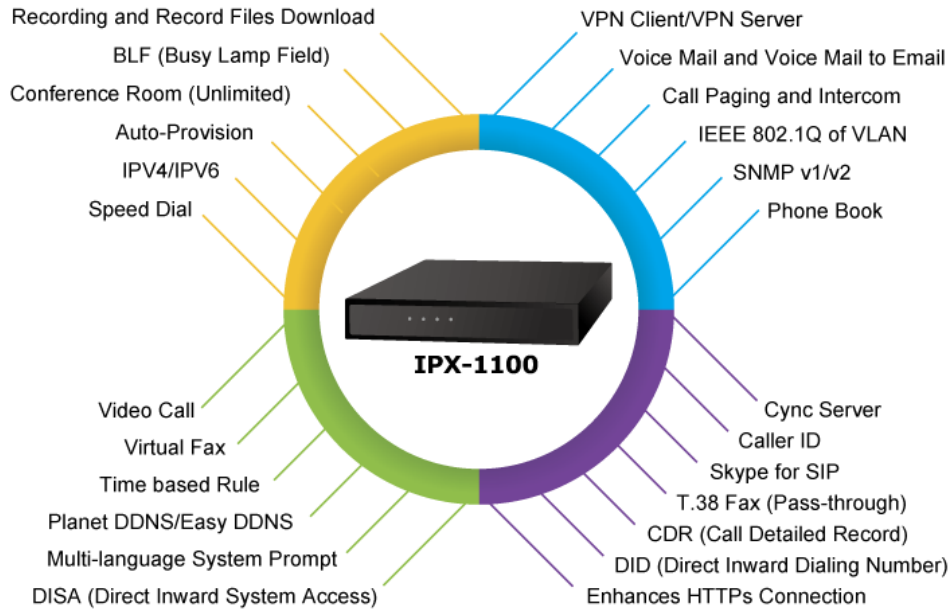
Cost-effective, easy-to-install and simple-to-use, the Internet Telephony PBX system converts standard telephones into IP-based networks. It enables the service providers and enterprises to offer users traditional and enhanced telephony communication services via the existing broadband connection to the Internet or corporation network.



With the Internet Telephony PBX system, home users and companies are able to save the installation cost and extend their past investments in telephones, conferences and speakerphones. The Internet Telephony PBX system can be the bridge between the traditional analog system and IP network without having to invest heavily.

Distributed VoIP Network Infrastructure

In the new-generation communication age, the Internet Telephony PBX system supports IPv6 and VPN (client/server) connection to provide users with more flexible and advantageous communications products. With PLANET DDNS function, the Internet Telephony PBX system also helps users to apply and remember the login information easier. Its multiple-language feature helps user to quickly and easily manage the system. Moreover, the Internet Telephony PBX system supports Lync server to which smart phone (using third-party app) and analog phone are connected via its communication with other devices of Lync server.



Standard Compliance

Compliant with the Session Initiation Protocol 2.0 (RFC 3261), the Internet Telephony PBX system is able to broadly interoperate with equipment provided by VoIP infrastructure providers, thus enabling them to provide their customers with better multi-media exchange services.

Compliant with standard SIPv2.0 RFC 3261



Green IP Office

The Fax to Email/Email to Fax service provided by the Internet Telephony PBX system allows users to transfer and receive faxes directly to or from your email inbox as file attachments. It is an easy and confidential way of receiving, storing and forwarding important fax documents, thus creating a paperless green office.

Features

➤ **System Highlights**

- IPX-1100 / IPX-1102
 - 50 concurrent calls and up to 100 registers
 - 30 conference attendees
 - 400-hour recording
 - 2 built-in FXO interfaces (only for IPX-1102)
- IPX-2200
 - 80 concurrent calls and up to 200 registers
 - 60 conference attendees
 - 15000-hour recording (internal storage)
- Unlimited SIP/IMS trunks
- HD voice codec G.722 for perfect voice quality
- Voicemail to Email for not missing any important message
- Paging and intercom function strengthens the work efficiency
- Built-in SIP proxy server following RFC 3261
- Multiple language of GUI for international business
- Web-based control panel for easy configuration and management of the system
- Hardware echo cancellation module for great and smooth communication
- Strong security features protect your system from hacking
- Records voice and voicemail to external USB disk
- Quick setup wizard

➤ **Codec and Protocol**

- SIP 2.0 (RFC3261), IAX2 and Lync server compliant
- Audio Codec: G.711-Ulaw, G.711-Alaw, G.722, G.726, G.729, GSM, SPEEX, Opus, AMR, AMR-WB
- Video Codec: H.261, H.263, H.263+, H.264 and VP8
- DTMF: RFC 4733, SIP info, in-band and auto

➤ **Network and Security Features**

- DHCP server, DDNS client (PLANET DDNS & Easy DDNS)
- SNMP v1/v2, IEEE802.1Q VLAN
- IPv4/IPv6, TR069
- Manual configuration of static route table
- Troubleshooting (Ping and Traceroute)
- VPN server and VPN client

- Mitigates SIP Register DoS attacks
- Prevents Abort Invite DoS attacks
- Prevents SSH Login DoS attacks
- Firewall and enhances HTTPS connection
- Geo-IP (Security policy based on IP address geographical locations)
- Data backup and recovery

➤ **PBX Features**

- SIP Register with UDP/TCP/TLS/SRTP
- One Touch Recording
- Mobility Extension
- Black List
- BLF (Busy Lamp Field)
- CDR (Call Detailed Record)
- Conference Room
- DID (Direct Inward Dialing Number)
- SRTP (Secure Real time Transport Protocol)
- DND (Do Not Disturb)
- IVR (Interactive Voice Responses)
- Follow Me, Call Spy and PIN Set
- Distinctive Ringtone
- Multi-language System Prompt
- Phone Book, Speed Dial
- Ring Group, SIP Trunk
- Skype for SIP, Smart DID, System Log
- T.38 fax (pass-through), voicemail and voicemail to e-mail

➤ **Call Features**

- Call Back, Call Forward, Call Group
- Call Hold, Call Paging and Intercom
- Call Park, Call Pickup, Call Queue
- Call Record, Call Route, Blind Transfer
- Attend Transfer, Call Waiting
- Caller ID, Dial by Name
- Customized IVR, On-hold Music, Transfer
- 30 Conference attendees

1.1.1 Package Contents

Thank you for purchasing PLANET Internet Telephony PBX system. Open the box of the Internet Telephony PBX system and carefully unpack it. The box should contain the following items:

Model	Package Description
IPX-1100 IPX-1102	● Quick Installation Guide x 1 ● Power Adapter x 1 (12V DC) ● RJ45 x 1
IPX-2200	● Quick Installation Guide x 1 ● Power Adapter x 1 (12V DC) ● RJ45 x 1 ● Bracket x 2

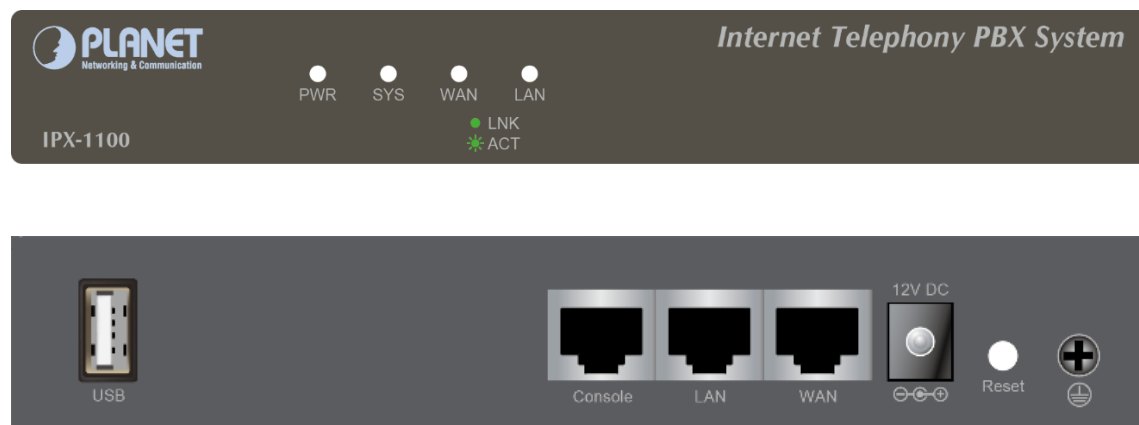


If any of the above items are damaged or missing, please contact your dealer immediately.

1.2 Mechanical Design

1.2.1 IPX-1100/IPX-1102/IPX-2200

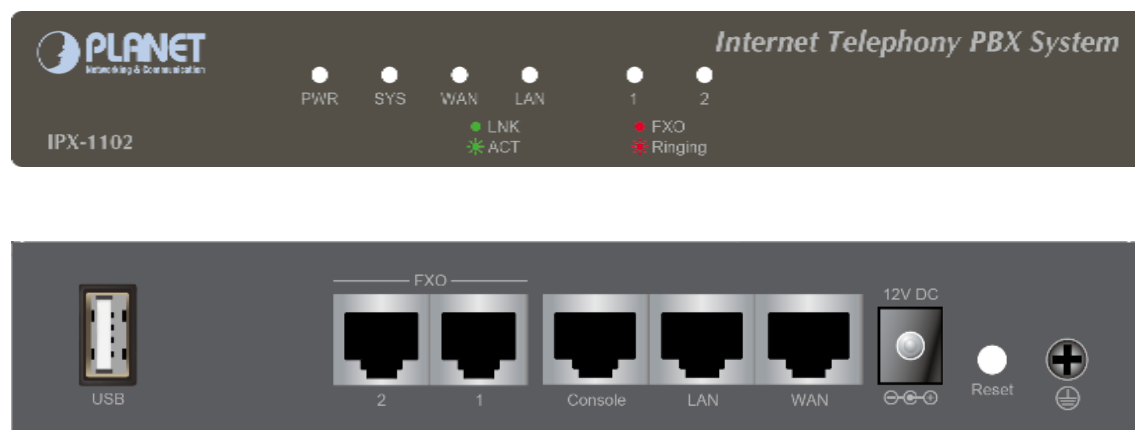
- IPX-1100 Front and Rear Panels



➤ LED Definition

Front Panel LED	Status	Description
PWR	Steady Green Off	PBX Power ON PBX Power OFF
SYS	Blinking Green On Off	System is working System doesn't boot System failure
WAN	Blinking Green On Off	Data transfer PBX network connection is established Waiting for network connection
LAN	Blinking Green On Off	Data transfer PBX network connection is established Waiting for network connection

- **IPX-1102 Front and Rear Panels**



➤ **LED Definition**

Front Panel LED	Status	Description
PWR	Steady Green Off	PBX Power ON PBX Power OFF
SYS	Blinking Green On Off	System is working System doesn't boot System failure
WAN	Blinking Green On Off	Data transfer PBX network connection is established Waiting for network connection
LAN	Blinking Green On Off	Data transfer PBX network connection is established Waiting for network connection
FXO 1/2	Steady Red Flashing Off	Ready/Standby Ringing Module not available

➤ **Physical interface descriptions**

1	Power Adapter	DC 12V, 1A
2	WAN/LAN	The WAN/LAN port facilitates auto-negotiating Fast Ethernet 10/100BASE-T networks. This port enables seamless connectivity of your IP PBX to an Internet access device, such as a router, cable modem, or ADSL modem, using a Cat5 twisted-pair Ethernet cable.
3	Reset Button	Yes
4	USB	For external store device to store voice and voicemail
5	Console Port	1 Port (Baud Rate: 115200)
6	FXO Interface 1/2	2 built-in FXO interfaces The FXO interface links to a PBX or CO line using an RJ11 analog line. The FXO port connects either to the extension port of a PBX or directly to a PSTN line provided by the carrier.

1.2.2 IPX-2200

- IPX-2200 Front and Rear Panels



➤ LED Definition

Front Panel LED	Status	Description
PWR	Steady Green Off	PBX Power ON PBX Power OFF
SYS	Blinking Green On Off	System is working System doesn't boot System failure
WAN	Blinking Green On Off	Data transfer PBX network connection is established Waiting for network connection
LAN	Blinking Green On Off	Data transfer PBX network connection is established Waiting for network connection
FXO	Steady Red Flashing Off	Ready/Standby Ringing Module not available
GSM	Steady Red Flashing Off	Ready/Standby (SIM card inserted) Ringing No SIM card inserted
FXS	Steady Green Flashing Off	Ready/Standby Ringing Module not available

➤ **Physical interface descriptions**

1	Power Switch	Switch the power on or off
2	Power Cord	AC 100~240V, 50/60Hz, 1.5A max
3	WAN/LAN	The WAN/LAN port facilitates auto-negotiating Fast Ethernet 10/100BASE-T networks. This port enables seamless connectivity of your IP PBX to an Internet access device, such as a router, cable modem, or ADSL modem, using a Cat5 twisted-pair Ethernet cable.
4	Reset Button	Yes
5	USB	For external store device to store voice and voicemail
6	Console Port	1 Port (Baud Rate: 115200)
7	Module Slot 1/Slot 2	2 external slots accommodating compliant FXO/FXS/GSM modules. - The FXO module links to a PBX or CO line using an RJ11 analog line. The FXO port connects either to the extension port of a PBX or directly to a PSTN line provided by the carrier. - The GSM module interfaces with the Global System for Mobile Communications (GSM) using a SIM card.

➤ **Slot 1~Slot 2 Definition**

Slot Module	Module Description	Slot 1	Slot 2
IPX-21FO	4-Port FXO Module	V	V
IPX-21SL	4-Port Life-Line Module (2 FXO + 2 FXS)	V	V
IPX-21GS	4-Port GSM Module	V	V

1.3 Plug-in Modules for IPX-2100/IPX-2200/IPX-2500

- **IPX-21FO Module**



The IPX-21FO module provides 4 FXO interfaces for connecting PSTN lines provided by the telecom. It can be installed on both slots of the IPX-2100, IPX-2200 and IPX-2500 and provides maximal 8 FXO interfaces.

- **IPX-21GS Module**



The IPX-21GS module provides 4 GSM channels; it can be installed on the IPX-2100, IPX-2200 and IPX-2500 for making and receiving phone calls from GSM network. It is designed with SIM900 for global market; SIM900 is a quad-band GSM engine that works on frequencies GSM 850MHz, EGSM 900MHz, DCS 1800MHz and PCS 1900MHz.

- **IPX-21FS Module (optional per project)**



The IPX-21FS module provides 4 FXS interfaces for connecting fax machines or analog phones. It can be installed on both slots of the IPX-2100, IPX-2200 and IPX-2500 and provides maximal 8 FXS interfaces.

- **IPX-21SL Module (optional per project)**



The IPX-21SL module provides 2 FXO and 2 FXS interfaces; it can be installed on both slots of the IPX-2100, IPX-2200 and IPX-2500. With the IPX-21SL module installed, it enables the IPPBX system with FXO to FXS lifeline feature. When there's power failure, you may still use the analog phone to make and receive phone calls.

- **IPX-21MA Module (optional per project)**



The IPX-21MA (WCDMA) module provides 4 GSM/3G voice channels; it can be installed on the IPX-2200 for making and receiving phone calls from the GSM/3G network. It is designed with the SIM5320 series module for global market, and the SIM5320 is a dual-band WCDMA and quad-band GSM engine that works on frequencies like UMTS 850MHz, UMTS 900MHz, UMTS 1900MHz, UMTS 2100MHz, GSM 850MHz, EGSM 900MHz, DCS 1800MHz and PCS 1900MHz.



The WCDMA modules for PLANET IP PBX series are only used for voice phone calls; they CANNOT be used for data transmission from 3G network.

1.4 Specifications

IPX-1100/IPX-1102

Product	IPX-1100	IPX-1102
	Internet Telephony PBX system (100 SIP User registrations)	Internet Telephony PBX system with 2-port FXO (100 SIP User registrations)
Hardware		
WAN	1 x 10/100BASE-T RJ45 port for WAN, connecting to broadband modem or a WAN router	
LAN	1 x 10/100BASE-T RJ45 port for LAN, connecting to a LAN switch	
FXO Interface	-	2 built-in FXO
USB	1 port for external storage device File system format: FAT16, FAT32, EXTFAT, NTFS, EXT3, EXT4	
Console Port	1 port (baud rate: 115200)	
Reset Key	Yes	
Protocols and Standard		
Standard	SIP 2.0 (RFC 3261), IAX2	
Protocols	RFC 768 UDP	
	RFC 793 TCP	
	RFC 5246 TLS	
	RFC 3711 SRTP	
	RFC 826 ARP	
	RFC 1034, 1035 DNS	
	RFC 1631 NAT	
	RFC 2068 HTTP	
	RFC 2131 DHCP	
	RFC 2516 PPPoE	
	RFC 3261, RFC 3311, RFC 3515	
	RFC 3265, RFC 3892, RFC 3361	
	RFC 3842, RFC 3389, RFC 3489	
	RFC 3428, RFC 2327, RFC 2833	
	RFC 2976, RFC 3263	
	IPv4, IPv6, VLAN, DHCP, PPPoE, DDNS, NTP, SNTP, TFTP, SSH, HTTPS, LDAP	
Audio Codecs	G.711-Ulaw, G.711-Alaw, G.722, G.726, G.729, GSM, SPEEX, Opus, AMR and AMR-WB	
Video Codec	H.261, H.263, H.263+, H.264 and VP8	

Fax over IP	T.38 Fax (pass-through)
	Note: T.38 support is dependent on fax machine, SIP provider and network, transport resilience
Voice Processing	DTMF detection and generation
	RFC 4733, SIP info, in-band and Auto
Internet Sharing	
Network Features	DDNS client (Planet DDNS and easy DDNS)
	DHCP server/SNMP v1/v2
	IEEE 802.1Q VLAN
	IP assignment (DHCP/Static)
	IPv4/IPv6
	Manual configuration of static route table
	Troubleshooting (ping and traceroute)
	VPN server and VPN client
Security Features	Mitigates SIP Register DoS attacks
	Prevents Abort Invite DoS attacks
	Prevents SSH Login DoS attacks
	Firewall and enhances HTTPS connection
Features	
PBX Features	SIP Register with UDP/TCP/TLS/SRTP
	Phone Auto-Provisioning
	One Touch Recording
	Mobility Extension
	Black List
	BLF (Busy Lamp Field)
	CDR (Call Detailed Record)
	Conference Room
	DID (Direct Inward Dialing Number)
	DISA (Direct Inward System Access)
	DNIS (Dialed Number Identification Service)
	SRTP (Secure Real time Transport Protocol)
	DND (Do Not Disturb)
	FOP (Flash Operation Panel) Status Monitoring
	IVR (Interactive Voice Responses)
	Follow Me, Call Spy and PIN Set
	Distinctive Ringtone
	Multi-language System Prompt
	Multiple Language of GUI
	Phone Book, Speed Dial

	LDAP Server for phonebook	
	Record Files Download	
	Ring Group, SIP Trunk	
	Skype for SIP, Smart DID, System Log	
	T.38 fax (pass-through), voicemail and voicemail to e-mail	
	Time-based Rule	
	PBX log, web access log and PBX debug log	
Call Features	Call Back, Call Forward, Call Group	
	Call Hold, Call Paging and Intercom	
	Call Park, Call Pickup, Call Queue	
	Call Record, Call Route, Blind Transfer	
	Attend Transfer, Call Waiting	
	Caller ID, Dial by Name	
	Customized IVR, On-hold Music, Transfer	
	30 Conference attendees	
One-on-One Video Call		
System Capacity		
System Capacity	50 simultaneous calls	
	Up to 100 IP phone registers/extensions	
	Recording and Voicemail: 400 hours	
Network and Configuration		
Access Mode	Static IP, DHCP	
LED Indications	PWR: 1, LNK/Off	PWR: 1, LNK/Off
	SYS: 1, LNK/Off	SYS: 1, LNK/Off
	WAN: 1, LNK/Off	WAN: 1, LNK/Off
	LAN: 1, LNK/Off	LAN: 1, LNK/Off
	-	Analog Interface 1/2: FXO (Red)
Dimensions (W x D x H)	167.6 x 115 x 28.8 mm	
Operating Environment	0~40 degrees C, 5~95% humidity	
Power Requirements	DC 12V, 1A	
EMC/EMI	CE, FCC Class B, RoHS	

IPX-2200

Product	IPX-2200 Internet Telephony PBX system (200 SIP Users registrations)
Hardware	
WAN	1 x 10/100BASE-T RJ45 for WAN, connecting to broadband modem or a WAN router
LAN	1 x 10/100BASE-T RJ45 for LAN, connecting to a LAN switch
USB	For external storage device File system format: FAT16, FAT32, EXTFAT, NTFS, EXT3, EXT4
Console Port	1 port (Baud rate: 115200)
Reset Key	Yes
2 Slots	Supports maximum 8 ports (FXO/GSM)
Protocols and Standard	
Standard	SIP 2.0 (RFC 3261), IAX2
Protocols	RFC 768 UDP RFC 793 TCP RFC 5246 TLS RFC 3711 SRTP RFC 826 ARP RFC 1034, 1035 DNS RFC 1631 NAT RFC 2068 HTTP RFC 2131 DHCP RFC 2516 PPPoE RFC 3261, RFC 3311, RFC 3515 RFC 3265, RFC 3892, RFC 3361 RFC 3842, RFC 3389, RFC 3489 RFC 3428, RFC 2327, RFC 2833 RFC 2976, RFC 3263 IPv4, IPv6, VLAN, DHCP, PPPoE, DDNS, NTP, SNTP, TFTP, SSH, HTTPS, LDAP
Audio Codecs	G.711-Ulaw, G.711-Alaw, G.722, G.726, G.729, GSM, SPEEX, Opus, AMR and AMR-WB
Video Codec	H.261, H.263, H.263+, H.264 and VP8
Fax over IP	T.38 Fax (pass-through) Note: T.38 support is dependent on fax machine, SIP provider and

	network, transport resilience
Voice Processing	DTMF detection and generation RFC 4733, SIP info, in-band and auto
Internet Sharing	
Network Features	DDNS client (Planet DDNS and easy DDNS) DHCP server/SNMP v1/v2 IEEE 802.1Q VLAN IP assignment (DHCP/Static) IPv4/IPv6 Manual configuration of static route table Troubleshooting (ping and traceroute) VPN server and VPN client
Security Features	Mitigates SIP Register DoS attacks Prevents Abort Invite DoS attacks Prevents SSH Login DoS attacks Firewall and enhances HTTPS connection
Features	
PBX Features	SIP Register with UDP/TCP/TLS/SRTP Phone Auto-Provision One Touch Recording Mobility Extension Black List BLF (Busy Lamp Field) CDR (Call Detailed Record) Conference Room DID (Direct Inward Dialing Number) DISA (Direct Inward System Access) DNIS (Dialed Number Identification Service) SRTP (Secure Realtime Transport Protocol) DND (Do Not Disturb) FOP (Flash Operation Panel) Status Monitoring IVR (Interactive Voice Responses) Follow Me, Call Spy and PIN Set Distinctive Ringtone Multi-language System Prompt Multiple Language of GUI Phone Book, Speed Dial

	LDAP Server for phonebook Record Files Download Ring Group, SIP Trunk Skype for SIP, Smart DID, System Log T.38 fax (pass-through), voicemail and voicemail to e-mail Time-based Rule PBX log, web access log and PBX debug log
Call Features	Call Back, Call Forward, Call Group Call Hold, Call Paging and Intercom Call Park, Call Pickup, Call Queue Call Record, Call Route, Blind Transfer Attend Transfer, Call Waiting Caller ID, Dial by Name Customized IVR, On-hold Music, Transfer 60 Conference attendees One-on-One Video Call
System Capacity	
System Capacity	80 simultaneous calls Up to 200 IP phone registers/extensions Recording and Voicemail: 15,000 hours
Network and Configuration	
Access Mode	Static IP, DHCP
LED Indications	SYS: 1, LNK/Off WAN: 1, LNK/Off LAN: 1, LNK/Off PWR: 1, LNK/Off SLOT: FXO/GSM (Red), FXS (Green)
Dimensions (W x D x H)	437.6 x 172 x 42.8 mm
Operating Environment	-10~45 degrees C, 10~80% humidity
Power Requirements	AC 100V-240V, 50/60Hz, 1.5A (max.)
EMC/EMI	CE, FCC Class B, RoHS

1.5 Key Features

- ✓ 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
- ✓ 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, supporting 10 VPN clients)
- ✓ VPN Client (PPTP/OpenVPN)
- ✓ IP Phone Provisioning (ALE, Cisco, Fanvil, Htek, Yealink)
- ✓ 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

2. Getting Started

2.1 Hardware Installation

Hardware installation of each model is documented in the “Quick Installation Guide”, and the guide was packed with each of the IP PBX 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.

2.2 Accessing the Web GUI

You may also access the PBX Web GUI by specifying its IP address in the browser address bar. It is recommended that users use the latest version of Google Chrome browser to access.

When there is DHCP server in the network, the WAN port obtains dynamic IP address by default. If the acquisition fails, the default WAN port IP address is 172.16.0.1. LAN port's default IP address is 192.168.0.1.

Clicking on the icon  provides access to the login page illustrated in the figure below. You can select the system language. Enter the username and password, and then click the "Login" button to access the system.

Default admin login credentials:

Username: admin

Password: sw + the last 6 characters of the MAC ID in lowercase

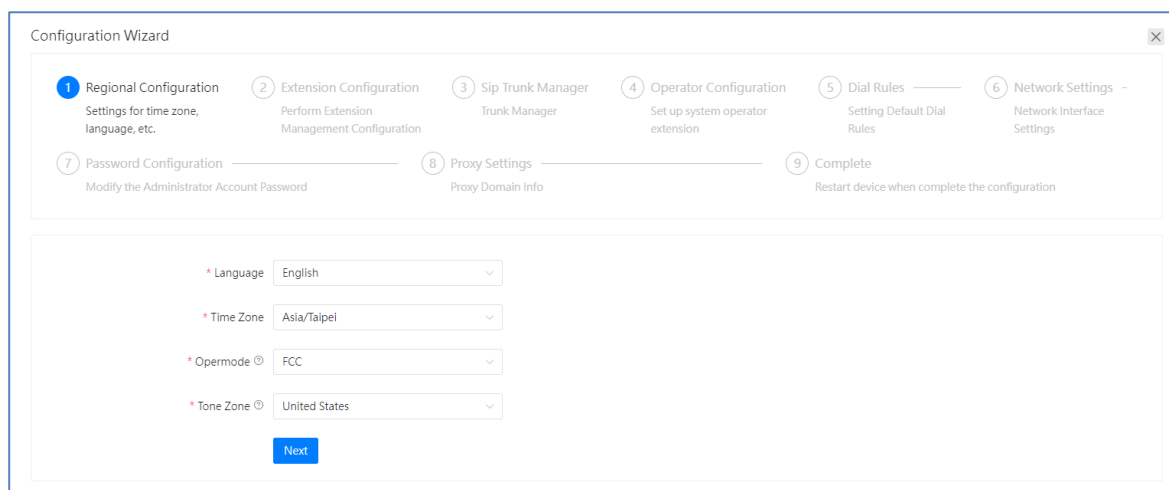


2.3 Configuration Wizard

Quick Setup Wizard is specially designed on v4.0.0 software for Planet's IP IPX series to help you quickly and easily set up your IP PBX system within minutes.

After logging to the system, click on the  Configuration Wizard button on the bottom left to start the Quick Setup Wizard journey.

● Step 1: Regional Configuration



Configuration Wizard

1 Regional Configuration Settings for time zone, language, etc.

2 Extension Configuration Perform Extension Management Configuration

3 Sip Trunk Manager Trunk Manager

4 Operator Configuration Set up system operator extension

5 Dial Rules Setting Default Dial Rules

6 Network Settings Network Interface Settings

7 Password Configuration Modify the Administrator Account Password

8 Proxy Settings Proxy Domain Info

9 Complete Restart device when complete the configuration

* Language English

* Time Zone Asia/Taipei

* Opermode FCC

* Tone Zone United States

Next

- **Language:** Set up the system's default language.
- **Time Zone:** Set up the system time zone.
- **Opermode:** Set up the system analog trunk's opermode.
- **Tone Zone:** Set up the system tone zone.

After the regional configuration is done, please click on the  button to the next step.

• Step 2: Extension Configuration

Set up the system's extension. Click on the **Add** button to bulk add the extension number. Please fill in the **Start Extension Number** and **Count**. If the **Password** is left blank, then the system will auto-generate random passwords for the extensions. Click on the **Submit** button to take effect on the extensions.

Add

* Start Extension Number ⓘ
100

* Count ⓘ
Please Input
-- +

Password ⓘ
Please Input

Cancel Submit

Configuration Wizard

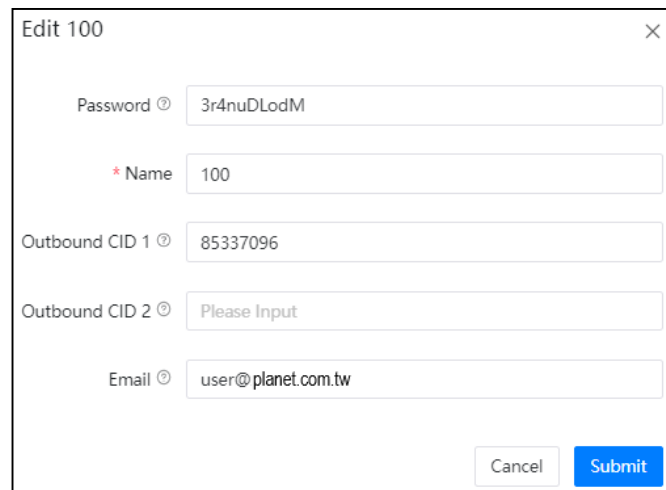
1 Regional Configuration
Settings for time zone, language, etc.
2 Extension Configuration
Perform Extension Management Configuration
3 Sip Trunk Manager
Trunk Manager
4 Operator Configuration
Set up system operator extension
5 Dial Rules
Setting Default Dial Rules
6 Network Settings
Network Interface Settings
7 Password Configuration
Modify the Administrator Account Password
8 Proxy Settings
Proxy Domain Info
9 Complete
Restart device when complete the configuration

Add Delete Selected
Previous Next

Extension Number	Name	Outbound CID 1 ⓘ	Outbound CID 2 ⓘ	Email	Operation
☐ 100	100				Edit Delete
☐ 101	101				Edit Delete
☐ 102	102				Edit Delete
☐ 103	103				Edit Delete
☐ 104	104				Edit Delete

Total 5 items
1
20 / page
Goto 1

Click on the  button to edit the extension parameter values, such as password, extension name, outbound CID, and email. Click on the  button to save.



The screenshot shows a dialog box titled "Edit 100" with a close button (X) in the top right corner. The dialog contains five input fields, each with a help icon (i) to its right:

- Password**: The input field contains the text "3r4nuDLodM".
- * Name**: The input field contains the text "100".
- Outbound CID 1**: The input field contains the text "85337096".
- Outbound CID 2**: The input field contains the text "Please Input".
- Email**: The input field contains the text "user@planet.com.tw".

At the bottom right of the dialog, there are two buttons: a "Cancel" button and a "Submit" button.

After the extension configuration is done, please click on the  button to move to the next step.

• Step 3: SIP Trunk Manager

Set up the system's SIP trunk settings. For detailed configuration, please refer to section **Telephony- >Outbound Control->Trunks**.

The screenshot shows the 'Configuration Wizard' window with the 'SIP Trunk Manager' step selected. The wizard progress bar shows steps 1 through 9. Below the progress bar, there is a table of SIP trunks. The table has columns: Name, Enable, Type, Status, Username, Server Address, Port, and Operation. A single row is visible with the name 'test', enabled status, Client Mode type, Rejected status, username 'xxx', server address '192.168.17.1', and port '5060'. There are buttons for 'Refresh', 'Add', 'Import', 'Export', and 'Delete Selected' above the table. At the bottom right, there are 'Previous' and 'Next' buttons.

Name	Enable	Type	Status	Username	Server Address	Port	Operation
test	Yes	Client Mode	Rejected	xxx	192.168.17.1	5060	 

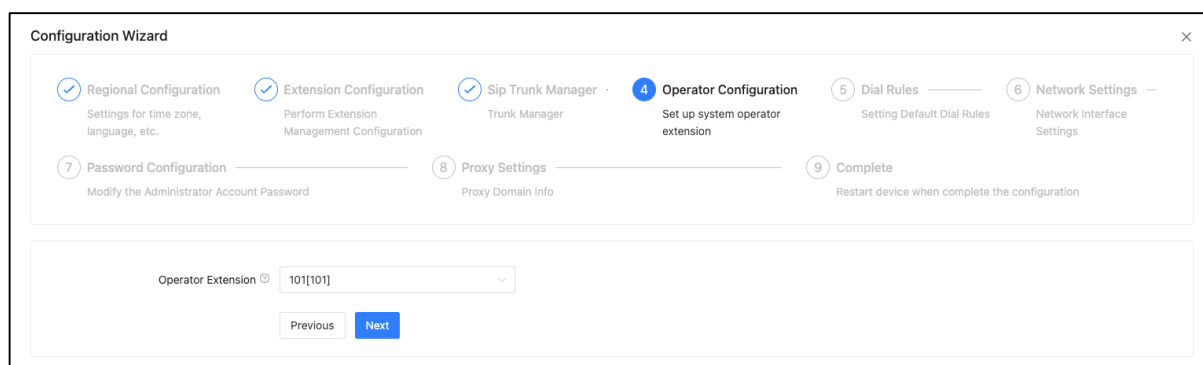
Click on the  button to edit the SIP trunk parameter values. Generally, Client Mode is the most commonly used to connect to the VoIP providers for low cost long distance and international phone calls, while the Server Mode is only used when users want to do SIP trunking between IPPBX's.

The screenshot shows the 'Add' configuration window for a SIP trunk. It has two tabs: 'Basic' and 'Other'. The 'Basic' tab is active. It contains several fields and controls: 'Enable' (checked), 'Type' (set to 'Client Mode'), 'Server Address' (Please Input), 'Out Proxy Server' (Please Input), 'Username' (Please Input), 'Password' (Please Input), 'Contact' (Please Input), 'Retry Interval' (60), 'Name' (Please Input), 'Authentication' (checked), 'Port' (5060), 'Out Proxy Port' (Please Input), 'AuthUser' (Please Input), 'Identify By' (set to 'Username'), 'Register Expiration' (3600), and 'Max Retry' (10). There are 'Cancel' and 'Submit' buttons at the bottom right.

You may also use the Import button to import the SIP trunk configuration file or export the selected SIP trunks file. After the SIP trunk set up is done, please click on the  button to move to the next step.

- **Step 4: Operator Configuration**

Set up the system's operator extension number. By default (when there is no incoming call destination number), all incoming calls will go directly to the operator extension number.



The screenshot shows the 'Configuration Wizard' window with a progress bar at the top. The steps are: 1. Regional Configuration (checked), 2. Extension Configuration (checked), 3. Sip Trunk Manager (checked), 4. Operator Configuration (active), 5. Dial Rules, 6. Network Settings, 7. Password Configuration, 8. Proxy Settings, and 9. Complete. Below the progress bar, the 'Operator Extension' is set to '101[101]' in a dropdown menu. At the bottom, there are 'Previous' and 'Next' buttons.

After the operator set up is done, please click on the [Next](#) button to move to the next step.

• Step 5: Dial Rules

The Dial Rules are configured to connect directly to the system's default outgoing dial rule. Simply choose the available trunks for the rule, indicating that outgoing calls will use the corresponding trunks. For a more in-depth configuration guide, please refer to section Telephony- >Outbound Control->Dial Rules.

The 'Edit' dialog box contains the following fields and options:

- Time Rule:** None (dropdown)
- Prepend:** Please Input (text field)
- Dial Prefix:** 9 (text field)
- Dial Pattern:** . (text field)
- PIN Sets:** None (dropdown)
- Outbound CID:** Outbound CID 1 (dropdown)
- Call Time limit(sec.):** Please Input (text field with minus and plus buttons)
- Via Trunk/Trunks:** (checkbox, currently unchecked)
- Call Method:** Linear (dropdown)
- Available Trunks:**
 - Select all (button)
 - Total 4 items
 - ☒ FXO-2
 - ☒ FXO-1
 - ☐ ToServer
 - ☐ IAXTrunk
- Selected Trunks:**
 - Clear (button)
 - 2 items selected
 - FXO-1
 - FXO-2
- Buttons:** Cancel, Submit

The Configuration Wizard progress bar shows the following steps:

1. Regional Configuration (Settings for time zone, language, etc.)
2. Extension Configuration (Perform Extension Management Configuration)
3. Sip Trunk Manager (Trunk Manager)
4. Operator Configuration (Set up system operator extension)
- 5. Dial Rules (Setting Default Dial Rules)** (Current step)
6. Network Settings (Network Interface Settings)
7. Password Configuration (Modify the Administrator Account Password)
8. Proxy Settings (Proxy Domain Info)
9. Complete (Restart device when complete the configuration)

Buttons: Add, Previous, Next

As the above picture shows, number starting with 9 will be sent from the FXO-1 and FXO-2 trunks.

After the Dial Rules set up is done, please click on the **Next** button to move to the next step.

- **Step 6: Network Settings**

Please fill in the required network parameter. And it can also be configured in the Network Settings.

Configuration Wizard

1 Regional Configuration

Settings for time zone, language, etc.

2 Extension Configuration

Perform Extension Management Configuration

3 SIP Trunk Manager

Trunk Manager

4 Operator Configuration

Set up system operator extension

5 Dial Rules

Setting Default Dial Rules

6 Network Settings

Network Interface Settings

7 Password Configuration

Modify the Administrator Account Password

8 Proxy Settings

Proxy Domain Info

9 Complete

Restart device when complete the configuration

Previous

Next

WAN

Network Mode 

Static IP

* IP Address

192.168.11.135

* Netmask

255.255.255.0

Gateway

192.168.11.1

Primary DNS

8.8.8.8

Alternative DNS

114.114.114.114

Enable Virtual IP 

☐

Submit

LAN

* IP Address

192.168.10.100

* Netmask

255.255.255.0

Enable Virtual IP 

☐

Submit

- **Step 7: Password Configuration**

The system default admin password is “admin”. You can change the admin password by following the step shown below.

The screenshot displays the 'Configuration Wizard' window. At the top, a progress bar shows the following steps: 1. Regional Configuration (checked), 2. Extension Configuration (checked), 3. Sip Trunk Manager (checked), 4. Operator Configuration (checked), 5. Dial Rules (checked), 6. Network Settings (checked), 7. Password Configuration (active), 8. Proxy Settings, and 9. Complete. Below the progress bar, the 'Password Configuration' section is active, showing three input fields: 'Password', 'New Password', and 'Confirm Password', each with a 'Please Input' placeholder and a password icon. At the bottom of the section are three buttons: 'Previous', 'Next' (highlighted in blue), and 'Skip'.

• Step 8: Proxy Settings

Please fill in the required proxy service user information to activate the service. Please refer to the Remote Settings for more detailed step-by-step guide.

Configuration Wizard

1 Regional Configuration
Settings for time zone, language, etc.

2 Extension Configuration
Perform Extension Management Configuration

3 SIP Trunk Manager
Trunk Manager

4 Operator Configuration
Set up system operator extension

5 Dial Rules
Setting Default Dial Rules

6 Network Settings
Network Interface Settings

7 Password Configuration
Modify the Administrator Account Password

8 Proxy Settings
Proxy Domain Info

9 Complete
Restart device when complete the configuration

Previous Next

Enjoy your first-year free Always-Online Plan. Contact us to renew your plan. Free Trial

Proxy Settings

* Company Name: zyc00

* Country: china

* City: chengdu

* Contact Name: xxx

* Email Address: xxx@163.com

* Contact Number: xxx

Additional information: Please Input

* Domain Server: Chengdu, China

* Domain: xxx .sip.zyc00.com

* Protocol: UDP

* Service Years: 1

Save Download

Step 1: Fill in the basic user information such as company name, company location, etc. Then, select the domain server and set your own domain name (please choose the nearest domain server from your location). After completion, click the **Submit** button to save.

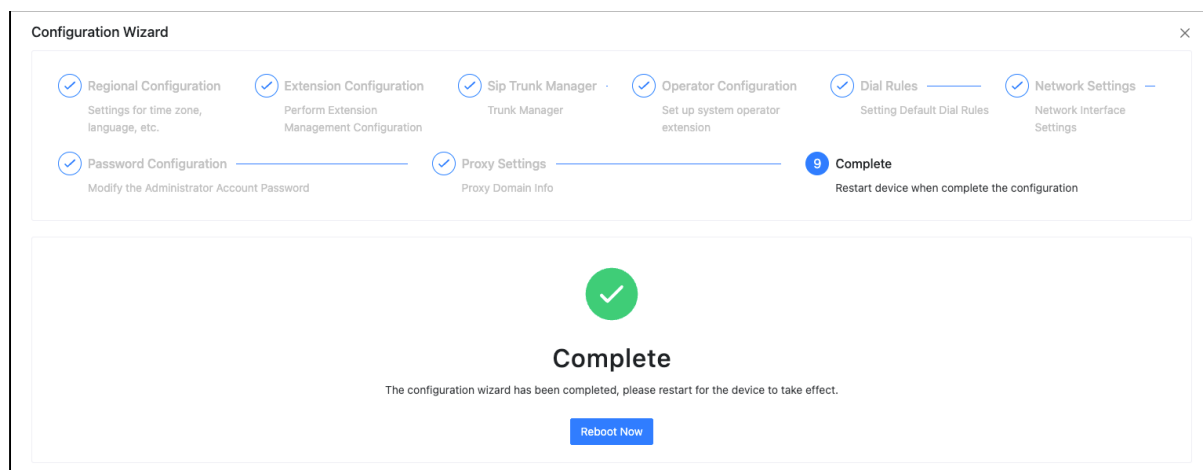
Step 2: Click on the **Download** button to download the user license file.

Step 3: Please send the downloaded file to the sales manager/distributor to obtain the key certificate file. Or click on the **Online Application** button to directly apply for a certificate online. Follow the provided instruction to complete the payment online to obtain the key certificate file.

Step 4: Click on the **Upload** button to upload the key certificate file so as to activate the proxy service.

- **Step 9: Complete**

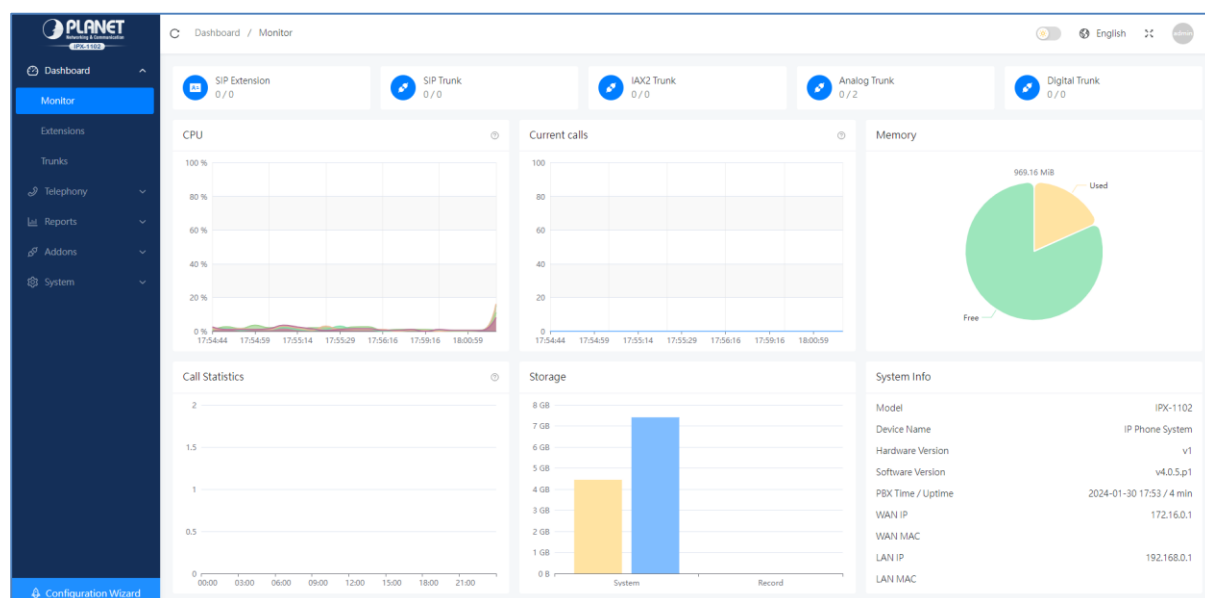
After all the configurations are done, you should see the Complete checkmark shown below. Please click on the Reboot button to reboot the system and take effect on all configuration changes.



3. Dashboard

3.1 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.
- **Analog Trunk:** The number of available FXO/GSM analog trunks and the total number of FXO/GSM analog trunks
- **Digital Trunk:** The number of available digital trunks and the total number of digital trunks.
- **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	
Device Name	IP Phone System
Hardware Version	v4
Software Version	v4.0.4
PBX Time / Uptime	2023-05-12 14:43 / 3 days, 22:49
WAN IP	
WAN MAC	
LAN IP	
LAN MAC	

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

3.2 Extensions

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

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

Dashboard / Extensions					
All [48] Offline [14] Online [34] Busy [0] Ringing [0] Refresh Number / Name					
100[100] 192.168.17.14[3ms]	101[101] 192.168.11.188[4ms]	102[102] 192.168.11.192[3ms]	103[103] 192.168.11.192[4ms]	104[104] 192.168.11.192[4ms]	105[105] 192.168.11.192[4ms]
106[106] 192.168.11.192[3ms]	107[107] 192.168.11.192[3ms]	108[108] 192.168.11.192[3ms]	109[109] 192.168.11.192[3ms]	110[110] 192.168.11.192[4ms]	Tam[111] 192.168.11.188[3ms]
Tam[111] 192.168.11.192[3ms]	112[112] 192.168.11.192[4ms]	113[113] 192.168.11.192[3ms]	114[114] 192.168.11.192[3ms]	115[115] 192.168.11.192[4ms]	116[116] 192.168.11.192[3ms]
117[117] 192.168.11.192[4ms]	118[118] 192.168.11.192[4ms]	119[119] 192.168.11.192[4ms]	120[120] 192.168.11.192[4ms]	121[121] 192.168.11.192[4ms]	122[122] 192.168.11.192[4ms]
Rosh[123] 192.168.11.192[4ms]	124[124] 192.168.11.192[4ms]	125[125] 192.168.11.192[4ms]	126[126] 192.168.11.192[4ms]	127[127] 192.168.11.192[3ms]	128[128] 192.168.11.192[4ms]
129[129] 192.168.11.192[3ms]	130[130] 192.168.11.192[4ms]	131[131] 192.168.11.192[4ms]	132[132] Unavailable	133[133] Unavailable	134[134] Unavailable
135[135] Unavailable	136[136] Unavailable	137[137] Unavailable	138[138] 113.91.55.43[46ms]	Unavailable	601[601] Unavailable

3.3 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 soundcard. You may click on the "Free Line" in the analog trunk list to free the current busy channel.

SIP				
Name	Trunk Type	IP	Delay(ms)	Status
ToServer	client	192.168.17.138	nan	Unregistered
IAX				
Name	Trunk Type	IP	Delay(ms)	Status
IAXTrunk	client	192.168.17.138	2	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

Analog						
No.	Channel	BLF	Trunk Type	Status	Channel Status	Operation
1	1	001	FXO	OK	Idle	Free Lines
2	2	002	FXO	OK	Idle	Free Lines

Analog

- **No.:** Order number of trunk
- **Channel:** Trunk channel number
- **BLF:** BLF label of the channel
- **Trunk Type:** type of channel: FXO/GSM
- **Status:** Trunk connection status
- **Channel Status:** Channel status: Idle/Busy
- **Operation:** Click on the "Free Lines" to force release the current channel.

Digital					
Channel	Signalling	Chan Status	Chan In Alarm	Chan Blocked	Chan In Service
 No Data					

Digital

- **Channel:** Channel number
- **Signaling:** Signaling type
- **Chan Status:** Channel status
- **Chan In Alarm:** Whether the channel is alarmed
- **Chan Blocked:** Whether the channel is blocked
- **Chan In Service:** Whether the channel is in service

4. Telephony

4.1 Extensions

Path: **Telephony -> Extensions**

Extensions and departments should have been created during the Quick Setup Wizard process. You may manage extensions and departments here on this screen. If you have skipped the Quick Setup Wizard, you may create them here on this screen as well.

4.1.1 Departments

Path: **Telephony -> Extensions -> Departments**

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

If you have created departments and extensions from Quick Setup Wizard, you should see all your departments and extensions here.

The screenshot displays the 'Add' dialog box for creating a new department. The background shows a table with columns: Name, Extension, Members, and Operation. The table contains one entry: 'Dep1' with extension '0400' and members '100[100]', '101[101]', and '102[102]'. The 'Add' dialog box is open, showing the following fields:

- Name:** Dep2
- Extension:** 0401
- Ring Strategy:** Ring All
- Ring Time:** 30
- Destination if no answer:** Hangup
- Members:** 101[101] (with a remove button 'x')
- Distinctive Ring:** Please Input

The dialog box has 'Cancel' and 'Submit' buttons at the bottom right.

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

Edit 0400

* Name

* Ring Strategy

* Ring Time

* Destination if no answer

Members

Distinctive Ring

Cancel Submit

- **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.

4.1.2 IP Extensions

Path: **Telephony -> Extensions -> IP Extensions**

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							
Name / Number							
☐	Name	Extension Number	Outbound CID 1	Outbound CID 2	Department Name	Dial Permission	QR Code
☐	914	914				DialPlan1	
☐	915	915				DialPlan1	
☐	916	916				DialPlan1	
☐	917	917				DialPlan1	
☐	918	918				DialPlan1	
☐	920	920				DialPlan1	
☐	952	952				DialPlan1	
☐		991				DialPlan1	
☐		992				DialPlan1	
☐		998				DialPlan1	
☐		999				DialPlan1	
Total 77 items							
< 1 2 3 4 > 20 / page Goto 4							

The extensions are created through the quick setup wizard. To check or modify the extension properties please click the button.

Edit 800

Profiles

Features

Advanced

Enable

Mobile Number

Dial Permission

Language

Outbound CID 1

Music On Hold

* Name

* Password

Email

Outbound CID 2

800

Zyc00123 Medium

Please Input

Please Input

Cancel

Submit

- **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 IP PBX 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.

Edit 100

×

Profiles

Features

Advanced

Voicemail ⓘ ☒

Remote Extension ⓘ ☐

Video Call ⓘ ☐

WebRTC ⓘ ☐

Call Spy ⓘ ☐

Whitelist ⓘ

None

* Pickup Group ⓘ

1 X

* Voicemail Password ⓘ

1234

Number Of Simultaneous Registrations ⓘ

1

Video Codecs ⓘ

H.264

Call Recording ⓘ

Disabled

* Register Expiration ⓘ

1800

— +

Web Login ⓘ ☐

Cancel

Submit

- **Voicemail:** If this option is enabled and 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 record, check contact list and send faxes, etc.
- **Voicemail Password:** Set the voicemail password. The extension user needs to enter the password when dialing *60 or *61 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 comma 「,」 to separate each group for multiple groups use.

Edit 800

Profiles

Features

Advanced

* Transport Protocol ⓘ

UDP

* DTMF Mode ⓘ

RFC4733(RFC2833)

SRTP ⓘ

* Qualify(sec.) ⓘ

300

NAT Support ⓘ

IAX2 Extension ⓘ

Permit IP ⓘ

Please Input

* Qualify Timeout(sec.) ⓘ

30

Send PAI ⓘ

Send RPID ⓘ

* RTP Timeout ⓘ

60

Inband Progress ⓘ

Optional Codes

Select all

Total 8 items

☒ Ulaw

☒ Alaw

☒ G.729

☐ GSM

☐ G.722

☐ G.726

☐ Speex

☐ G.723

Selected Codes

Clear

3 items selected

Alaw

Ulaw

G.729

Cancel

Submit

- **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 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 IP PBX 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 hang up 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:** Planet's IPX 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 IP PBX system in bulk.

Batch Add
×

Profiles

Features

Advanced

Enable ⓘ ☒

* Start Extension Number ⓘ

Start Outbound CID 1 ⓘ

Start Outbound CID 2 ⓘ

Password ⓘ

Language ⓘ

Call Out Trunk ⓘ

* Count ⓘ — +

CID Calculation 1 ⓘ

CID Calculation 2 ⓘ

Dial Permission ⓘ

Music On Hold

- 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.

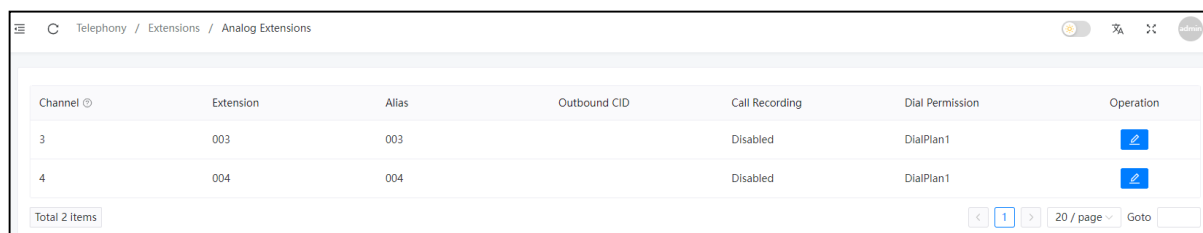
As for other options, you may configure accordingly as per your demands. The features/options configured will be applied to all newly-created extensions.

4.1.3 Analog Extensions

Path: **Telephony -> Extensions -> Analog Extensions**

Analog extensions are generated automatically by the IP PBX system if FXS interfaces are detected.

All you have to do is attach analog phones or fax machine to the FXS interface. The analog extensions can be used directly for phone calls; no more additional settings are required.



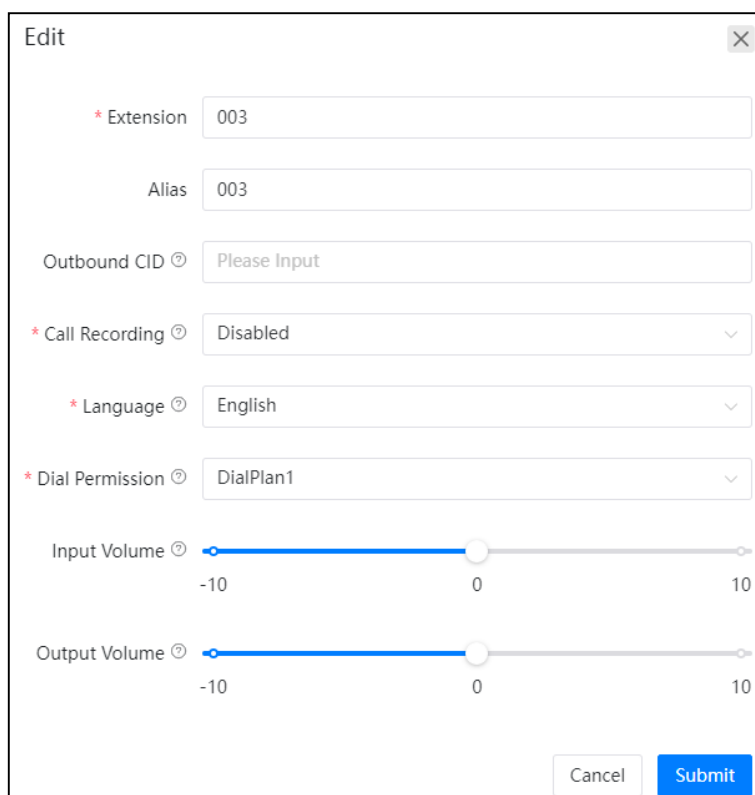
Channel ⓘ	Extension	Alias	Outbound CID	Call Recording	Dial Permission	Operation
3	003	003		Disabled	DialPlan1	
4	004	004		Disabled	DialPlan1	

Total 2 items

< 1 > 20 / page Goto

The **Channel** column and **Extension** column list the FXS interfaces and the corresponding extension numbers which are generated automatically by the IP PBX system.

You may click on the  button to change settings if necessary.



Edit

* Extension 003

Alias 003

Outbound CID ⓘ Please Input

* Call Recording ⓘ Disabled

* Language ⓘ English

* Dial Permission ⓘ DialPlan1

Input Volume ⓘ

Output Volume ⓘ

Cancel

Submit

- **Extension number:** This option can be defined as per your requirements.
- **Alias:** This option can be defined to identify this analog extension.
- **Outbound CID:** This option displays the number externally through digital trunk.
- **Call Recording:** This option could be enabled to record Inbound, Outbound or Both direction phone calls if necessary.
- **Language:** This option determines the language of the system prompts that the user will listen to/hear.
- **Dial Permission:** This option controls which dial rules the user can use to make phone calls.
- **Input Volume:** This option could be used to adjust the input gain of this analog extension.
- **Output Volume:** This option could be used to adjust the output gain of this analog extension.

4.2 Inbound Control

Path: **Telephony -> Inbound Control**

The Inbound Control section is where you define how Planet's IPX 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.

4.2.1 IVR

Path: **Telephony -> 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 shown below:

Add

* Name

Please Input

* Number ⓘ

0602

* Voice Prompts ⓘ

Please Select

Loop Count ⓘ

1

Dial Extension ⓘ

☒

Dial Permission ⓘ

Extension

Language ⓘ

Default

* Press Key Timeout(s)

3

— +

Events ⓘ

No Press

Hangup

Invalid Key

Hangup

+

Cancel

Submit

- In the **Name** field a name is required to identify this IVR menu.
- In the **Number** field a number has been created for this IVR menu so that the user is able to dial this number and test the IVR options.
- In **Voice Prompts** drop-down list, select a pre-recorded voice prompts 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 **Audio Library -> IVR Prompts** page.
- In **Loop Count** drop-down list, select the number of times to play back this IVR prompts before pressing a key by a caller.
- **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, allowing callers to dial internal extensions within this IVR menu. If you wish for callers to dial additional numbers, you may choose another dial permission here (Not Recommended).
- The **language** option determines the language of system voice prompts that callers will hear when landing on specific inbound destinations, such as voicemail, that play system voice prompts through this IVR menu.
- **Press Key Timeout(s)**: The maximum interval time, in seconds, between the pressing of the 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, 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.

4.2.2 Call Queue

Path: **Telephony -> 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 **Add** button, a popup window will show up shown below:

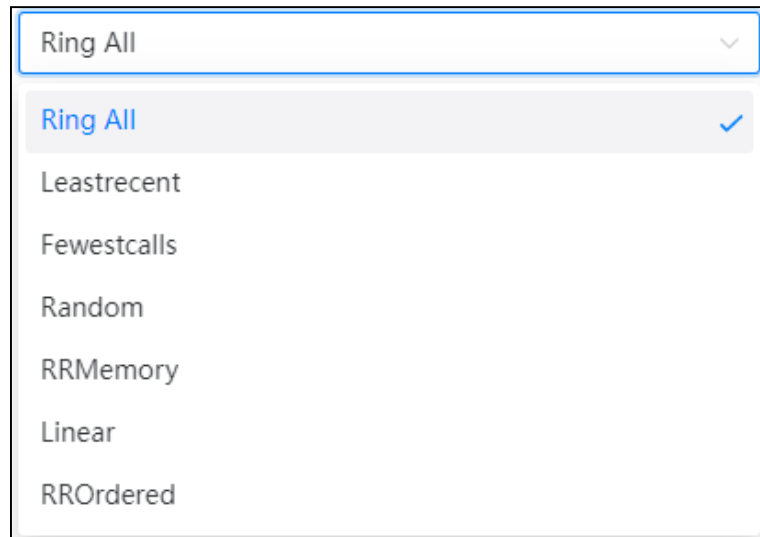
The screenshot shows a modal window titled "Add" with a close button (X) in the top right corner. It features three tabs: "General Settings" (active), "Advanced Settings", and "Announcements". The "General Settings" tab contains the following fields:

- * Name**: A text input field with the placeholder "Please Input".
- * Number**: A text input field with the value "0300" and a help icon (i).
- * Ring Strategy**: A dropdown menu with "Ring All" selected and a help icon (i).
- * Music On Hold**: A dropdown menu with "default" selected and a help icon (i).
- Static Agents**: A dropdown menu with "Please Select" selected and a help icon (i).
- Dynamic Agents**: A dropdown menu with "Please Select" selected and a help icon (i).
- * Destination if no answer**: A dropdown menu with "Hangup" selected and a help icon (i).

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

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](#) button 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.) ⓘ

15

— +

* Auto Pause ⓘ

No

▼

* Wrap Up Time(sec.) ⓘ

0

— +

Report Hold Time ⓘ

☐

* Max Callers ⓘ

0

— +

Add Queue Name Caller ID ⓘ

☐

Max Wait Time(sec.) ⓘ

Please Input

Join Empty ⓘ

☒

Leave When Empty ⓘ

☐

Cancel

Submit

- **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](#) button to setup customized announcements.

Add
×

General Settings
Advanced Settings
Announcements

Caller Position Announcements

* Announce Hold Time ? Once

Announce Position ? ☐

* Broadcast Frequency(sec.) ? 30 - +

Periodic Announcements

* Repeat Frequency(sec.) ? 0 - +

Announcements Prompts ? Please Select

Cancel Submit

- 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 a 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 prompts 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.

4.2.3 Time Conditions

Path: **Telephony -> Inbound Control -> Time Conditions**

Time conditions in Planet's IPX series 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 to 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.

The screenshot shows the configuration for a time condition named 'weekdays'. At the top, there is a text input field for the name, which contains 'weekdays'. Below this, there are fields for 'Weekdays' (a dropdown menu showing 'Mon'), 'From' (a time input field showing '09:00'), and 'To' (a time input field showing '18:00'). To the right of these fields is a blue '+' button. Below these fields is a table with columns for the days of the week: Sun, Mon, Tue, Wed, Thur, Fri, and Sat. The 'Mon' through 'Fri' columns contain two time ranges: '09:00 - 12:00' and '14:00 - 18:00', each with a small red square icon to its right. The 'Sun' and 'Sat' columns are empty. At the bottom right of the form are 'Cancel' and 'Submit' buttons.

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.

The screenshot shows a dialog box titled 'Edit holiday1'. It has a close button (X) in the top right corner. Inside the dialog, there is a text input field for the name, which contains 'holiday1'. Below this, there is a section labeled '* List of Holidays' with a list of two holiday periods: '2022-08-13 00:00:00 -> 2022-08-14 23:59:00' and '2022-08-20 00:00:00 -> 2022-08-21 23:59:59'. Each period has a small calendar icon to its right. To the right of the list are four buttons: a minus sign, a plus sign, an up arrow, and a down arrow. At the bottom right of the dialog are 'Cancel' and 'Submit' buttons.

Please ensure you add all upcoming holidays to the holiday list. Now you have all prerequisites to set up a time rule.

* Weekdays ⓘ	weekdays	▼
* Holidays ⓘ	holiday1	▼
— Business Hours Destination ⓘ —		
* Destination Type	IVR	▼
* Destination	welcome[0600]	▼
— Non-business Hours Destination ⓘ —		
* Destination Type	Extension	▼
* Destination	100[100]	▼
— Holiday destination ⓘ —		
* Destination Type	IVR	▼
* Destination	welcome[0600]	▼
		Cancel Submit

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.

4.2.4 Inbound Routes

Path: **Telephony -> 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 ? Please Select

* Inbound Destination ? Please Select

Status ? Disabled

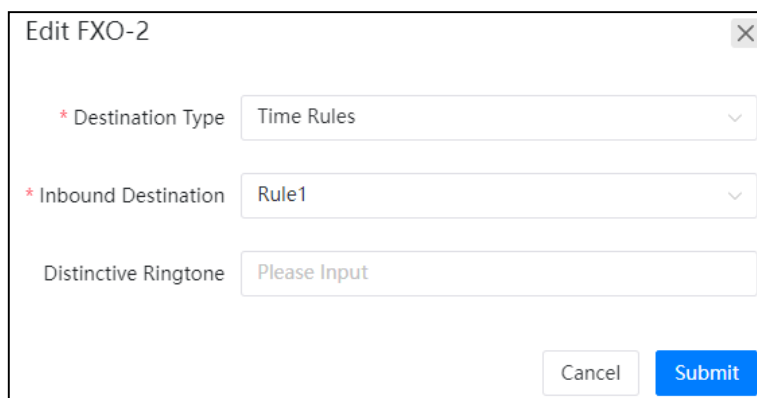
Submit

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.

Batch Edit		Trunk Name			Q
☐	Trunk Name	Destination Type	Inbound Destination	Distinctive Ringtone	Operation
☐	FXO-2	Time Rules	Rule1		
☐	FXO-1	IVR	welcome[0600]		
☐	11	Extension	100[100]		
Total 3 items		< 1 > 20 / page Goto			

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



Edit FXO-2

* Destination Type Time Rules

* Inbound Destination Rule1

Distinctive Ringtone Please Input

Cancel Submit

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.

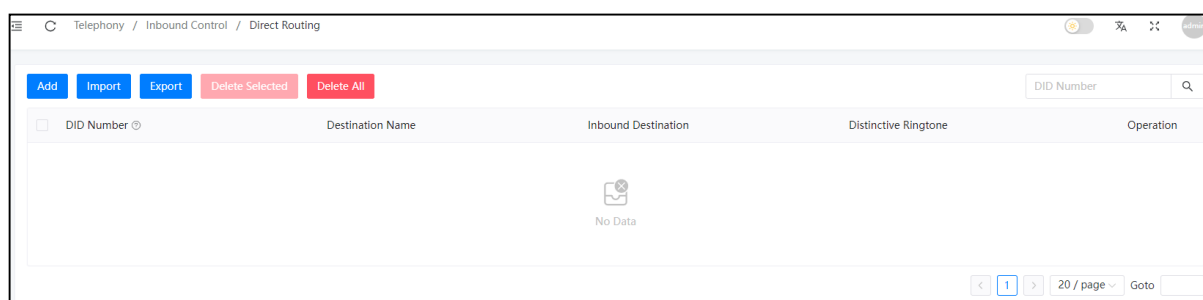
4.2.5 Direct Routing

Path: **Telephony -> Inbound Control -> Direct Routing**

You may set up Direct Routing based on the DID numbers of your VoIP/E1/T1/BRI trunk lines and the phone numbers of the external callers. Direct Routing has higher priority than time conditions (unless the inbound destination is a time rule) and other general inbound routes.

Direct 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 Direct 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.

The 'Add' popup window contains the following fields:

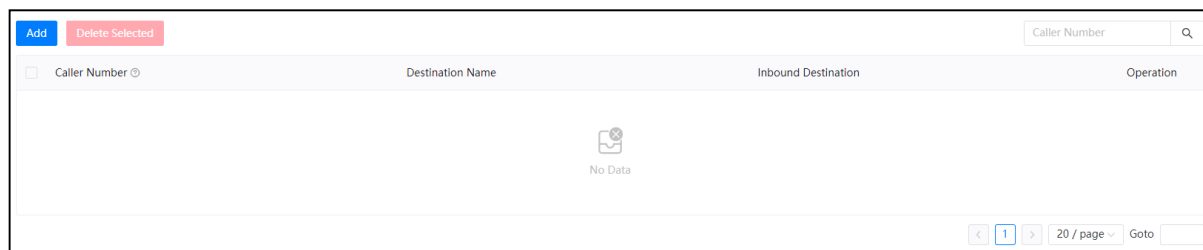
- * DID Number**: Text input field containing '94088322'.
- * Destination Name**: Dropdown menu with 'Extension' selected.
- * Inbound Destination**: Dropdown menu with '101[101]' selected.
- Distinctive Ringtone**: Text input field containing 'Please Input'.

At the bottom right of the popup are 'Cancel' and 'Submit' buttons.

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.

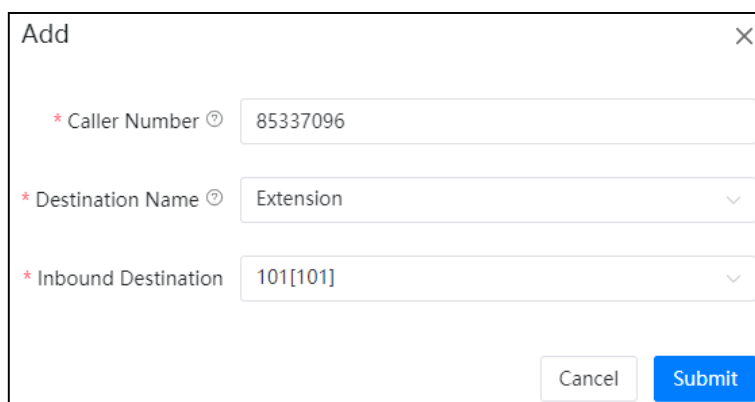
To add a Direct Routing rule base on the caller's number, please click "Add" button as shown below.



The screenshot shows a web interface for managing Direct Routing rules. At the top, there are two buttons: "Add" (blue) and "Delete Selected" (red). To the right is a search bar labeled "Caller Number" with a magnifying glass icon. Below these is a table with the following headers: "Caller Number", "Destination Name", "Inbound Destination", and "Operation". The table is currently empty, displaying a "No Data" message with a document icon. At the bottom right of the table, there is a pagination control showing "< 1 >" and "20 / page", along with a "Goto" input field.

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.

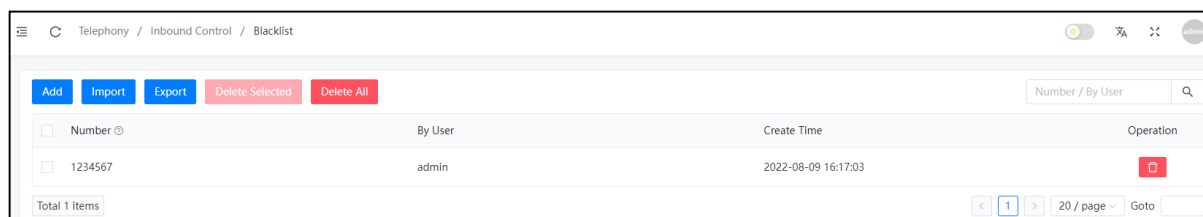


The screenshot shows a modal window titled "Add" with a close button (X) in the top right corner. It contains three required fields, each marked with a red asterisk and a help icon (i):
1. "Caller Number" with a text input field containing "85337096".
2. "Destination Name" with a dropdown menu showing "Extension".
3. "Inbound Destination" with a dropdown menu showing "101[101]".
At the bottom right of the modal, there are two buttons: "Cancel" (light gray) and "Submit" (blue).

4.2.6 Blacklist

Path: **Telephony -> Inbound Control -> Blacklist**

Blacklist feature allows you to create a list of numbers that are not allowed to call in to the IP PBX 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.



☐	Number	By User	Create Time	Operation
☐	1234567	admin	2022-08-09 16:17:03	

Total 1 items

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

4.3 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.

4.3.1 Trunks

A trunk on an IP PBX system is essential for extensions to be able to make outbound phone calls. On Planet's IPX IPPBX system, the trunks will be detected and generated automatically at the first time of the system initialization.

FXO/GSM Trunks

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

On the IP PBX front panel, red LED indicates the RJ11 interface is FXO. You should attach the telephone wire from your telecom socket to the FXO ports.

Physical Trunks				Batch Edit
☐	Name	Remark	Type	Operation
☐	FXO-2		Analog	
☐	FXO-1		Analog	
Total 2 items				   20 / page Goto

If needed you may edit the trunk settings by click on the  button, or you may select the same type of trunks and click on **Batch Edit** button to edit settings of the trunks together.

Edit FXO-1

Remark

Please Input

Output Volume

-10

0

10

Input Volume

-10

0

10

Answer Polarity Detection

Hangup Polarity Detection

Fax Detect

Quick Send Number

Caller ID Start

Default

* Call Recording

In & Out

* Prompts Language

English

* Busy Count

6

Busy Pattern

Please Input

Busy Detection

Fax DST

Please Select

Caller ID Signaling

Default

* Fax Wait Time(sec.)

5

-

+

Cancel

Submit

Select the parameters you want to configure before modifying them. Usually if the trunks are working fine please do not change these settings.

- **Remark:** Add remark description of the trunk.
- **Fax Wait Time (sec):** Setup duration for fax timeout.
- **Call recording:** To enable or disable call recording on the trunk/trunks. To enable recording you have options to record inbound calls only, outbound calls only or both inbound and outbound calls.
- **Output Volume:** Sets the volume of the outgoing calls from the FXO channels.
- **Input Volume:** Sets the volume of the incoming calls from the FXO channels.
- **Answer Polarity Detection:** When enabled, FXO (FXS signaled) ports watch for a polarity reversal to mark when an outgoing call is answered by the remote party.
- **Hangup Polarity Detection:** In certain countries, a polarity reversal is used to signal the disconnection of a phone line. If enabled, the calls will be considered "hang up" on a polarity reversal.
- **Fax Detect:** Enable or disable fax auto detection on this trunk.
- **Fax DST:** The extension number of the fax destination. If the extension number is set with an email address, the fax will be sent directly to the mailbox. If no email address is set, the fax will be sent directly to the fax machine corresponding to the extension number.
- **Caller ID Signaling:** Setup caller ID signaling for this trunk line instead of using global caller ID signaling.

- **Prompts Language:** You can choose a desired language of the system voice prompts to play to 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.
- **Busy Count:** Specify how many busy tones to wait for before hanging up, and it's configurable only if Busy Detection is enabled.
- **Busy Pattern:** If busy detection is enabled, it is also possible to specify the cadence of your busy signal.
- **Busy Detection:** Enable busy tone detection, it is also possible to specify how many busy tones to wait for before hanging up.
- **Quick Send Number:** When enabled, your calls will get through faster, as all numbers sent through this trunk will always be added with "#" at the end, it will cause the carrier to switch the calls immediately instead of waiting till digits timeout.
- **Caller ID Start:** Caller ID detection option for this trunk instead of using global settings. For more information please refer to Analog Settings.

SIP Trunks

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

Asterisk PBX 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 Planet's IPX IPPBX system for the user extensions to share and make outbound phone calls.

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

Add
✕

Basic

Other

Enable ⓘ ☒

* Type ⓘ Client Mode ▾

* Server Address ⓘ sip.zycoo.com

Out Proxy Server ⓘ Please Input

* Username ⓘ user

* Password ⓘ ⓘ

Contact ⓘ user

* Retry Interval ⓘ 60 - +

* Name siptrunk

Authentication ⓘ ☒

* Port 5060

Out Proxy Port Please Input

* AuthUser ⓘ user

* Identify By ⓘ Username ▾

* Register Expiration ⓘ 3600 - +

* Max Retry ⓘ 10 - +

Cancel
Submit

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, 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 IP PBXs.
- **Registration Expiration:** Expiration time of registration in seconds.
- **Max Retry:** Defines how many times the IP PBX system will attempt to register to the server before permanently giving up.

Add

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 C

Outbound CID

Dial Permission

* Video Codecs

Send RPID ☐

Qualify — +

Available codes

Select all

Total 10 items

☒ Ulaw
☒ Alaw
☒ G.729
☐ GSM

Selected codes

Clear

3 items selected

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 hang up 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:** Planet's IPX 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 IP PBX. The server mode IAX trunk should define username and password, the username and password should be applied on the client mode IAX trunk.

Below is an example of the client mode IAX trunk.

Add

Enable

* Name

Please Input

* Type

Client Mode

Authentication

* Server Address

Please Input

* Port

4569

Username

* Password

Please Input

Outbound CID

Please Input

* Preferred Outbound CID

Extension

Dial Permission

Default

Prompts Language

English

* Call Recording

Disabled

Available codes

Select all

Total 10 items

☒

 Ulaw

☒

 Alaw

☒

 G.729

☐

 GSM

☐

 G.722

☐

 G.726

☐

 Speex

☐

 G.723

Selected codes

Clear

3 items selected

Alaw
 Ulaw
 G.729

Cancel

Submit

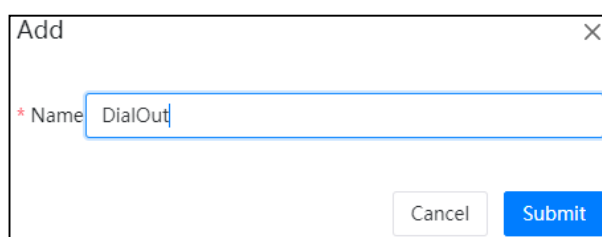
- **Trunk Name:** It should be the username of the IAX trunk account.
- **Authentication:** If the “Server Mode” trunk hasn’t enabled this option, then it doesn’t require a username and password for this account, you can disable this option and specify the Server Address for authentication.
- **Server 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:** Planet’s IPX 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 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.

4.3.2 Dial Rules

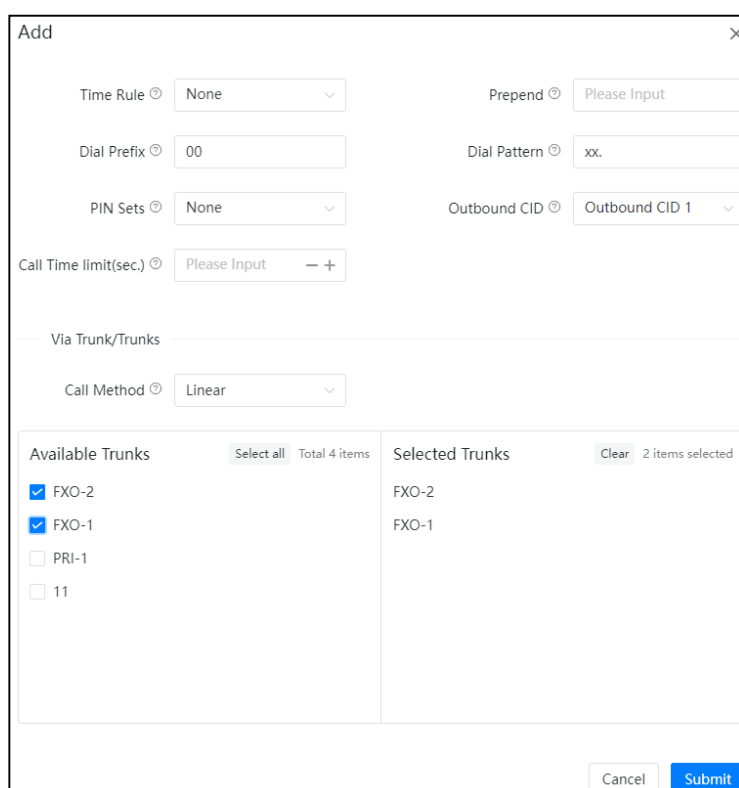
Path: **Telephony -> Outbound Control -> Dial Rules**

On the Planet's IPX IPPBX system you can set up 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  button to create a dial rule name; below is an example dial rule.



Click on the  button to create new dialing rules.

- 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 **Dial Prefix** 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.
- **Dial Prefix** 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 VoIP or E1/T1/BRI 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.



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.

4.3.3 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 number from 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

DialPlan1

Dial Rules

Available Rules

Unselect all

Total 1 items

☒ DialOut

Selected Rules

Clear

1 items selected

DialOut

Internal Permissions

Extension

☒

Paging & Intercom

☒

Department

☒

Call Parking

☒

Conference

☒

Call Pickup

☒

DISA

☒

Call Queue

☒

Feature Codes

☒

Call Spy

☐

IVR

☒

Seize CO Line

☐

Cancel

Submit

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 call 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 call directly.

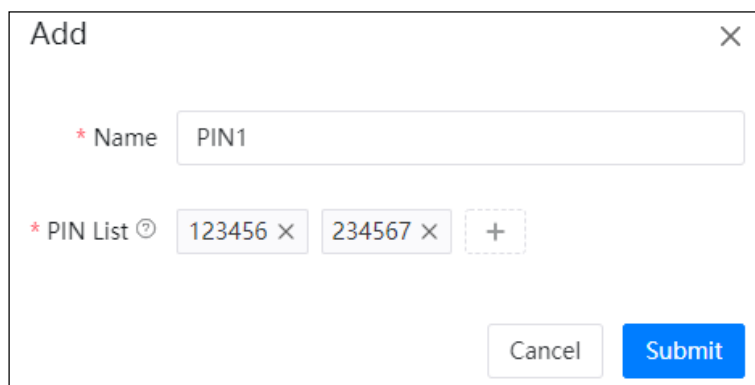
By default all extensions use the default dial permission “DialPlan1”, if you have created new dial permissions, please don’t forget to assign them to the extensions from **Telephony -> Extensions -> IP Extensions** and **Telephony -> Extensions -> Analog Extensions** (if there are analog extensions) page.

4.3.4 PIN Sets

Path: **Telephony -> 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 screenshot shows a web-based 'Add' dialog box. The title bar says 'Add' with a close 'X' button. Inside, there's a red asterisk followed by the label 'Name' and a text input field containing 'PIN1'. Below that is another red asterisk followed by the label 'PIN List' and a help icon. The PIN List section contains two input boxes with the values '123456' and '234567', each followed by a small 'X' delete button, and a dashed box with a '+' add button. At the bottom right of the dialog are two buttons: 'Cancel' and 'Submit'.

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.

4.4 Audio Library

4.4.1 Music On Hold

Path: **Telephony -> Audio Library -> Music On Hold**

Music On Hold (MOH), commonly known on an IP PBX system, allows audio files (such as WAV or MP3 files) to be uploaded to the IP PBX 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.

Add

* Directory Name

Please Input

* Playback Mode ⓘ

Please Select

Cancel

Submit

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)

Music On Hold Files Management ⓘ

New Directory

Directory Name	Playback Mode	Files	Operation
default	Shuffle	  countrywalks ×   metamorphosis ×   summer × 	
Music1	Shuffle		 
Total 2 Items		< 1 > 20 / page Goto	

4.4.2 IVR Prompts

Path: **Telephony -> Audio Library -> IVR Prompts**

To configure an IVR menu on Planet's IPX 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 Planet's IPX series IPPBX system.



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.

Recording
✕

* Filename ⓘ

* Extension ⓘ

Cancel
Submit

When done, click on Submit and the selected extension will ring. After the user picks up the phone, please follow the system voice prompts to complete the recording. When recording is done, the newly recorded audio will be listed on this page and ready to be used for setting up IVR.

4.4.3 Custom Prompts

Path: **Telephony -> Audio Library -> 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 IP PBX system to notify callers before forwarding their calls.

C

Telephony / Audio Library / Other Custom Prompts

Apply Changes

Other Custom Prompts

Upload

Files	Format	Play	Operation
1658211663	wav		

Total 1 Items

<

1

>

20 / page

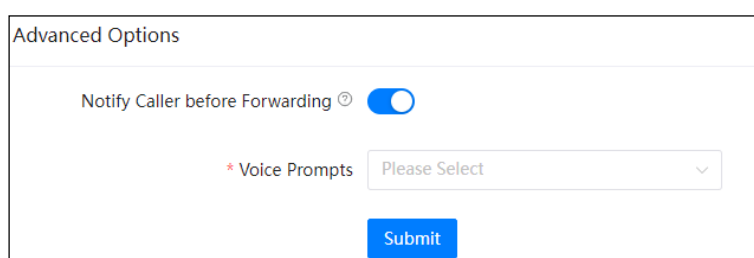
Goto

4.5 Advanced Features

4.5.1 Call Forward

Path: **Telephony -> 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.



Advanced Options

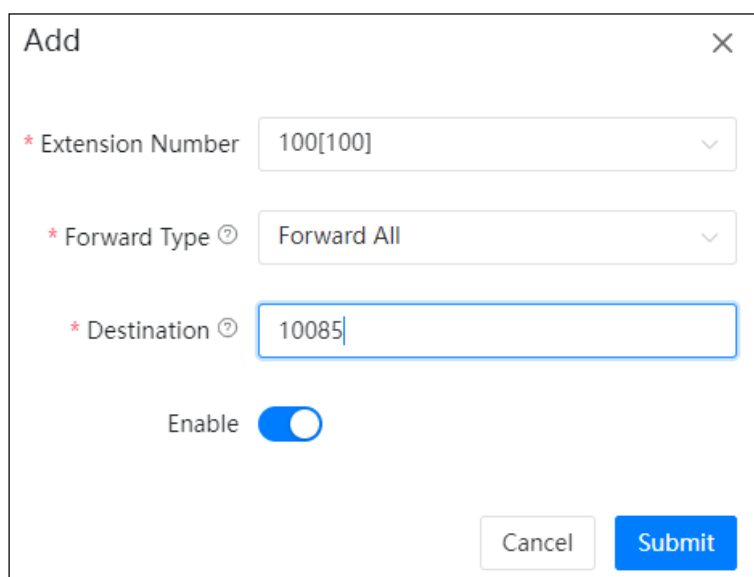
Notify Caller before Forwarding ☒

* Voice Prompts Please Select

Submit

- **Notify Caller before Forwarding** option allows you to choose a voice prompts to be played to the caller to notify caller that the call will be forwarded. The voice prompts is uploaded from **Telephony -> Audio Library -> 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.



Add

* Extension Number 100[100]

* Forward Type Forward All

* Destination 10085

Enable ☒

Cancel **Submit**

- 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 following list, you may disable or enable items based on requirements.

Add Activate Selected Deactivate Selected Delete Selected Delete All						
☐	Extension Number	Forward Type ⓘ	Timeout(sec.)	Destination	Enable	Operation
☐	101	Forward All	0	965302385	☒	✎ ✖
☐	100	Forward All	0	10085	☒	✎ ✖
Total 2 items						
< 1 > 20 / page Goto						

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

4.5.2 Follow Me

Path: **Telephony -> Advanced Features -> Follow Me**

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

- 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.

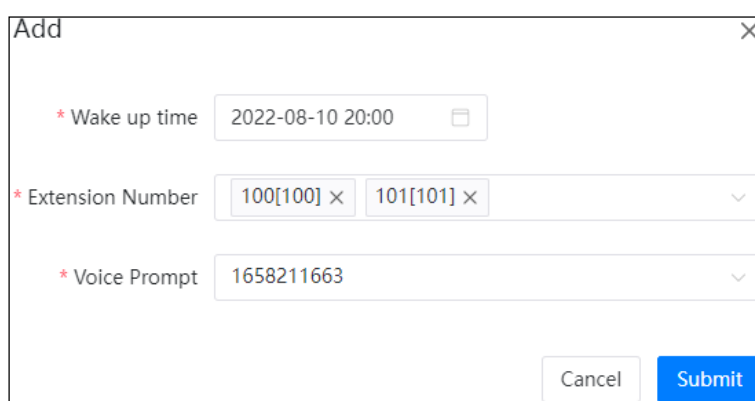
Take the above settings as an example, when extension 100 gets an incoming call, if it's not answered in 15 seconds, the call will be forwarded firstly to 101 and ring this extension for 10 seconds, if still not answered, it will try number 921432368 (9 is the dial prefix, not part of the number) for 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.

4.5.3 Wake Up Call

Path: **Telephony -> 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.



The screenshot shows a modal window titled "Add" with a close button (X) in the top right corner. It contains three required fields, each marked with a red asterisk:

- * Wake up time:** A date and time picker showing "2022-08-10 20:00" with a calendar icon on the right.
- * Extension Number:** A multi-select dropdown menu showing two selected items: "100[100] X" and "101[101] X".
- * Voice Prompt:** A dropdown menu showing the selected value "1658211663".

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

- 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 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.

4.5.4 Conference

Path: **Telephony -> 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.

Add						
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 ⓘ 0910

* Guest Password ⓘ Please Input

* Admin Password ⓘ Please Input

* Dial Permission ⓘ Please Select

* Hold Music ⓘ Please Select

Leader Wait ⓘ ☐

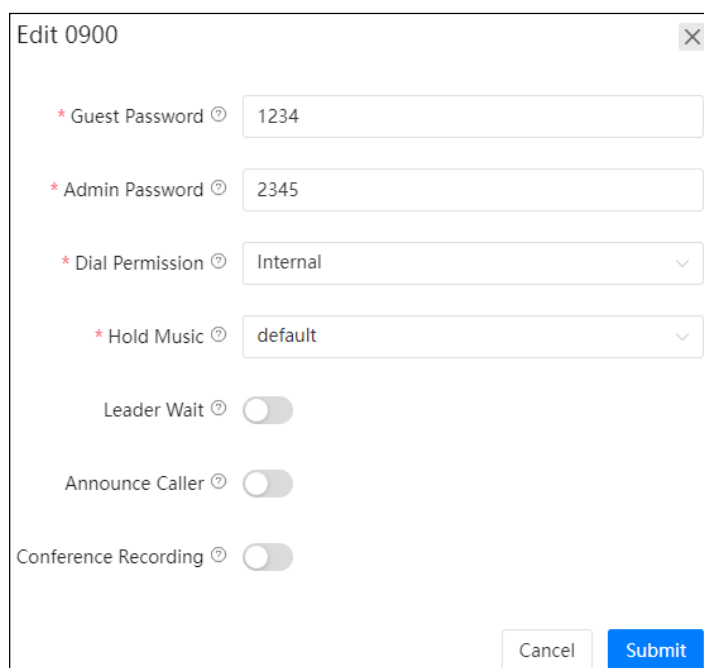
Announce Caller ⓘ ☐

Conference Recording ⓘ ☐

Cancel

Submit

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



- **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 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 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, 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.

4.5.5 DISA

Path: **Telephony -> Advanced Features -> DISA**

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

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

To add a DISA feature, follow the explanations below.

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

- Name:** A text input field containing "Disa1".
- Extension for this DISA:** A text input field containing "0700".
- PIN Code:** A dropdown menu currently showing "None".
- Response Timeout(sec.):** A numeric input field with "10" and minus/plus adjustment buttons.
- Digit Timeout(sec.):** A numeric input field with "5" and minus/plus adjustment buttons.
- Dial Permission:** A dropdown menu currently showing "DialPlan1".
- Buttons:** "Cancel" and "Submit" buttons at the bottom right.

- 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 IP PBX system.

4.5.6 Paging & Intercom

Path: **Telephony -> 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  button, a popup window will show up as shown below.

- In the **Group Number** field, a default group 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.
- 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 analog one, 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.

4.5.7 Smart DID

Path: **Telephony -> Advanced Features -> Smart DID**

With Smart DID feature, the IP PBX 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 DID** switch to turn on this feature.

Smart DID ?

Enable ☒

Time of Validation ?

One Day

Apply to Trunk/Trunks ?

PRI-1 ×

Submit

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 DID feature will be applied to.

4.5.8 Phonebook

Path: **Telephony -> Advanced Features -> Phonebook**

The screenshot shows the 'Phonebook' configuration page. At the top, there's a breadcrumb trail: 'Telephony / Advanced Features / Phonebook'. A green 'Apply Changes' button is in the top right. Below this is the 'LDAP Server Info' section with fields for Username (cn=user,dc=ippbx,dc=com), Password (password), and Directory Node (dc=ippbx,dc=com). There are also toggle switches for 'Activate' and 'Sync Extension Numbers' (which is turned on). A 'Contacts Sorting' dropdown is set to 'Phone Number'. Below the LDAP section is a toolbar with buttons: 'Add' (blue), 'Import' (blue), 'Export' (blue), 'Delete Selected' (red), 'Delete All' (red), and 'Sync with LDAP Server' (blue). To the right of the toolbar is a search bar labeled 'Contact Name / Phone Number'. Below the toolbar is a table with columns: 'Contact Name', 'Phone Number', 'E-mail', 'Company / Department', 'By User', 'Speed Dial Number', and 'Operation'. The table is currently empty, showing 'No Data' with a mail icon. At the bottom right of the table, there are pagination controls showing '1' of '20' pages and a 'Goto' field.

Phonebook feature for Planet's IPX series 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 **Add** button to add a new contact from the popup window.

The screenshot shows a 'Add' popup window with a close button (X) in the top right corner. It contains several input fields with labels and red asterisks indicating required fields: 'Contact Name' (filled with 'Tom'), 'Phone Number' (filled with '1234567'), 'E-mail' (filled with 'tom@gmail.com'), 'Company / Department' (filled with 'dep'), and 'Speed Dial Number' (filled with '11'). At the bottom right, there are two buttons: 'Cancel' (grey) and 'Submit' (blue).

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.

4.5.9 LDAP

Path: **Telephony -> Advanced Features -> Phonebook**

LDAP (Lightweight Directory Access Protocol) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an IP network. An LDAP server has been pre-configured on Planet's IPX IP PBX which is mainly used to centralize manage the phonebook.

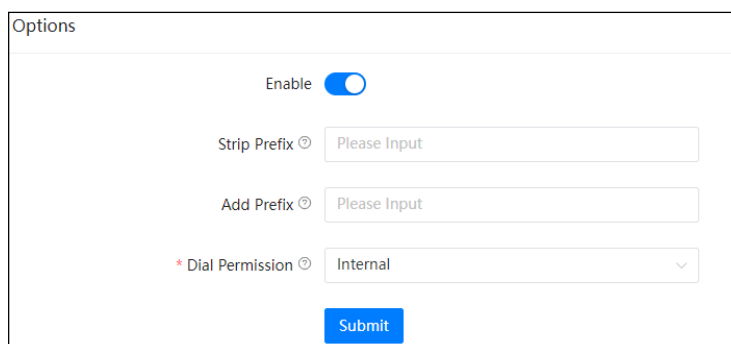
If you are using IP phones you'll need to manually configure LDAP configurations using the LDAP server credentials shown below. Also, you can select to synchronize internal extension numbers to the LDAP phonebook or not.

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

4.5.10 Callback

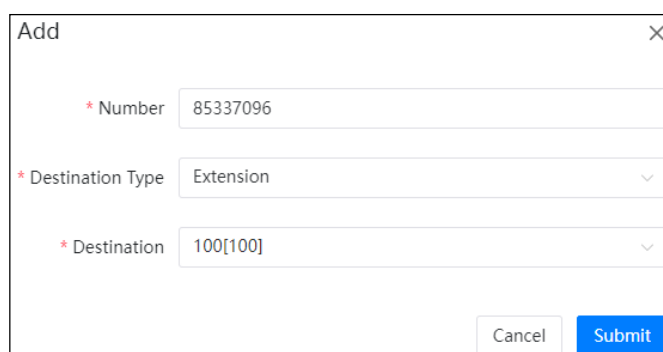
Path: **Telephony -> Advanced Features -> Callback**

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



The screenshot shows a web form titled "Options" for configuring the Callback feature. It includes an "Enable" toggle switch which is turned on. Below it are two text input fields: "Strip Prefix" and "Add Prefix", both containing the placeholder text "Please Input". There is also a dropdown menu for "Dial Permission" with "Internal" selected. A blue "Submit" button is at the bottom.

- **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.
- **Dial Permission:** Choose an appropriate dial plan to make sure the IPPBX system has the permissions for outbound calling.



The screenshot shows a modal window titled "Add" for adding a new callback entry. It contains three required fields: "Number" with the value "85337096", "Destination Type" with a dropdown menu showing "Extension", and "Destination" with a dropdown menu showing "100[100]". At the bottom right are "Cancel" and "Submit" buttons.

- **Number:** The number which will be used to call into the IP PBX system and handled by the Callback feature.
- **Destination:** An extension or another call destination which will be used to call the callback number.

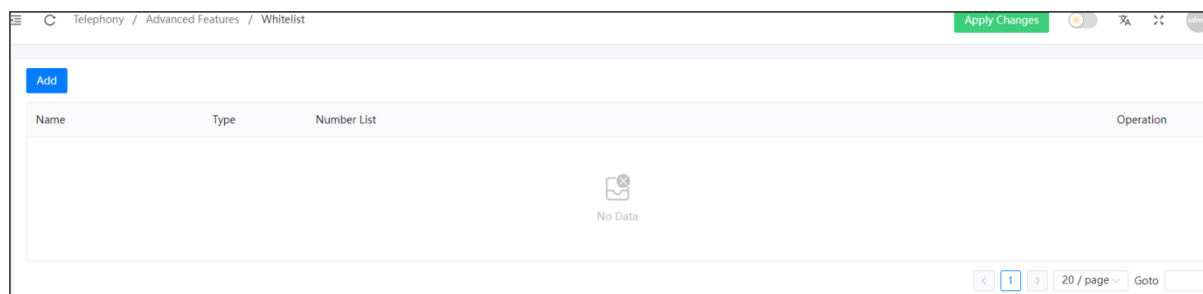
In the above example, if the caller 85337096 called the IP PBX system, IP PBX will disconnect this call and make a call back to this number using extension 100.

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.

4.5.11 Whitelist

Path: **Telephony -> 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'.



Add

* Name

list1

* Type

In

* Number List ⓘ

123456,2345678,3456789

Cancel

Submit

- **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.

4.6 Preferences

4.6.1 Global PBX Options

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

- **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.

Extension Ranges ?

Conference Extension Number Range	0900	-	0935
User Extension Number Range	100	-	899
Call Queue Extension Number Range	0300	-	0335
Department Number Range	0400	-	0435
Paging Group Extension Number Range	0500	-	0535
IVR Extension Number Range	0600	-	0635
DISA Number Range	0700	-	0735
Call Retrieve Number	41	-	49

Submit

Reset

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 needs to be modified from the **Feature Codes** screen.

4.6.2 VoIP Advanced

Path: **Telephony -> Preferences -> VoIP Advanced**

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

The screenshot shows the 'SIP Settings' configuration page. It includes the following fields and controls:

- * UDP Port**: Input field with value 5060 and increment/decrement buttons.
- * TCP Port**: Input field with value 5060 and increment/decrement buttons.
- * TLS Port**: Input field with value 5062 and increment/decrement buttons.
- ICE Enable**: A toggle switch currently turned off.
- STUN Server Address**: Input field with placeholder text 'Please Input'.
- * RTP Port Range**: Input field with value '10000 - 11000'.
- * User Agent**: Input field with value 'IPPBX'.
- * Endpoint Identifier Order**: Input field with value 'ip,username,auth_username,anonymous'.
- External Media Address**: Input field with placeholder text 'Please Input'.
- External Signaling Address**: Input field with placeholder text 'Please Input'.
- External UDP Signaling Port**: Input field with value 5060.
- External TCP Signaling Port**: Input field with value 5060.
- External TLS Signaling Port**: Input field with value 5062.
- Local Net(IP/Netmask Length) 1**: Input field with placeholder text 'Please Input'.
- Local Net(IP/Netmask Length) 2**: Input field with placeholder text 'Please Input'.
- Local Net(IP/Netmask Length) 3**: Input field with placeholder text 'Please Input'.
- Submit**: A blue button at the bottom right.

- **UDP Port:** SIP over UDP service port. By default, Planet 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.

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 IP PBX to the Internet will be risky. For security precautions please always use strong passwords.

IAX Settings ?

* UDP Port

4569

— +

Submit

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

CS3

TOS for RTP audio packets

ef

TOS for RTP video packets

AF41

COS Priority for Signaling packets

3

COS Priority for RTP audio packets

5

COS Priority for RTP video packets

4

4.6.3 Analog Settings

Global Analog Settings are used for configuring the IPPBX system to seamlessly work with the telephone lines from your telecommunications providers.

- **Caller ID Detection:** Allow\Disallow to detect caller ID.
- **Caller Name:** In some countries/regions caller name can be passed through the PSTN lines, by enabling this option the caller name will be received by the IPPBX system along with the caller ID.
- **Caller ID Signaling:** The signaling type applied on the PSTN lines to pass caller ID.
 - **Bell-US**—Also known as Bellcore FSK. Used in the Canada, China, Hong Kong and US.
 - **DTMF**—Dual Tone Multi-Frequency. Used in Denmark, Finland and Sweden.
 - **V23**—Mostly used in UK.
 - **V23-Japan**—Mostly used in Japan.
- **Caller ID Start:** Defines when the caller ID starts.
 - **Ring**—Caller ID starts when a ring is received.
 - **Polarity**—Caller ID starts when polarity reversal starts.
 - **Polarity (India)**—Can be used in India.
 - **Before Ring**—Caller ID starts before a ring received.
- **Caller ID Buffer Length:** The buffer length can be used to store caller ID info.
- **Ring Debounce:** Sets the minimum time in milliseconds to debounce extraneous ring events.
- **DTMF Hits Begin:** Sampling matching value of DTMF caller ID digits, you can choose 1 to 5 digits been matched then to consider it as part of the Caller ID.

- **DTMF Misses End:** Sample matching value of DTMF caller ID digits, you can choose 1 to 5 digits been mismatched then to consider it's not part of the caller ID.
- **Detect Caller ID After:** Sets the IPPBX to detect Caller ID after how many rings been detected.
- **Opermode:** Set the Opermode for FXO Ports.
- **Tone Zone:** Select the tone zone of your country.
- **Send Caller ID After:** Certain countries (UK) have ring tones with different ring tones (ring-ring), which means the caller ID needs to be set later on, and not just after the first ring, as per the default (1).
- **FXO Tune:** FXO Tune is a utility of tuning the various settings on the FXO ports for better adaptability with the PSTN lines, e.g. impedance.
- **Tone Duration:** used to adjust caller ID detection, non-professional users please do not modify.
- **FXO Ring Timeout:** This value can be tweaked to shorten how long it takes before the analog port (FXO) considers a non-ringing line to be hung up.
- **Relax DTMF:** If you are having trouble receiving DTMF key presses, enabling this option will make the DTMF interpreter much more permissive.
- **Denoise RX/TX:** The denoise parameter will help on noise reduction of the noisy analog lines, especially when gains have been increased on the lines.
- **Echo Cancel When Bridged:** It allows echo cancellation to be enabled or disabled for calls that are bridged between two TDM devices. As most of the time, the calls between two TDM endpoints will not have any echo, so this option is not required.
- **Echo Training:** The time length setting of echo training.

4.6.4 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.

4.7 Feature Codes

Path: **Telephony -> 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.

4.7.1 Voicemail Feature Code

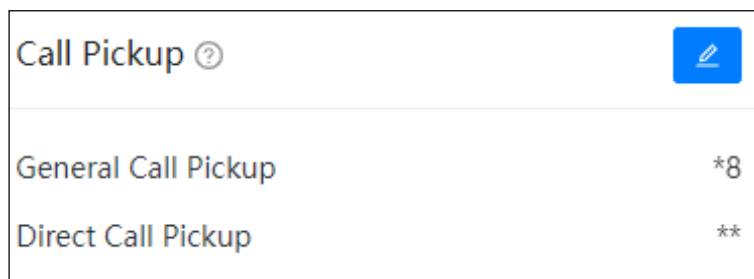
Voicemail ? 	
Dial Voicemail	*60
My Voicemail	*61

Dial *60 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 *61 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.

4.7.2 Call Pickup Feature Code

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



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.

4.7.3 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	*4
Call Retrieve Number	41-49

To park a call, extension user could dial *4 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.

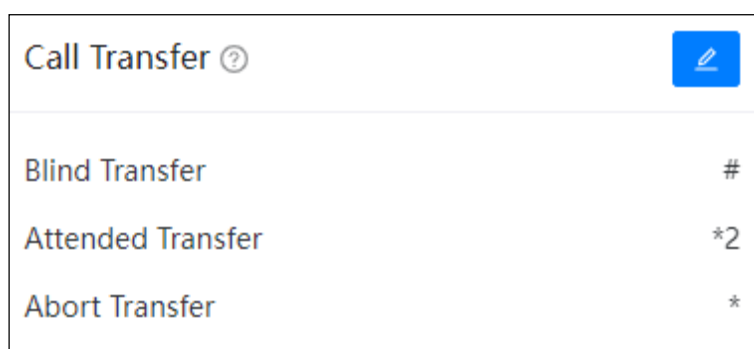
To retrieve the parked calls, user should dial the retrieve number given by the IPPBX system. And this could be done by any extension.

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 IP PBX system.

4.7.4 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).



In a live call, you can press # 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 hang up. 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 IP PBX 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 * when the third party is still ringing.

4.7.5 Blacklist Feature Code

Blacklist feature codes allow the extension users to add external phone numbers to IP PBX 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	*75
Whitelist a Number	*075

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 *75 (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 *075 (end with #) and follow the voice prompts to specify the number you wish to whitelist.

4.7.6 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	*90
Whisper	*91
Barge	*92

- **Normal Spy:** For example, extension 410 is talking to someone on the phone, you can dial *90410 (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 *91 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 *92 following by their extension number (end with #) to talk to both of the speakers.



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

4.7.7 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.

4.7.8 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 being 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.



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.

4.7.9 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.

4.7.10 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	*71
Deactivate All	*071
Activate Forward on Busy	*72
Deactivate Forward on Busy	*072
Activate Forward on No Answer	*73
Deactivate Forward on No Answer	*073

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

- **Forward All Activate:** Dial *71985337096, press 1 to confirm.
- **Deactivate Forward All:** Dial *071.
- **Activate Forward on Busy:** Dial *72985337096, press 1 to confirm.
- **Deactivate Forward on Busy:** Dial *072.
- **Activate Forward on No Answer:** Dial *73985337096, press 1 to confirm.
- **Deactivate Forward on No Answer:** Dial *073.

4.7.11 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 IP PBX system level. Any phone connected to the Planet's IPX series IPPBX system can use the DND feature code, no matter it's IP phone, analog phone or softphone.

DND ? 	
DND Activate	*74
DND Deactivate	*074

Simply dial *74 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 *074 to deactivate DND.

4.7.12 Office Closed Feature Code

Office Closed could be set on the IP phones from the phone level. Any phone connected to the Planet's IPX series 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.

4.7.13 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 *1 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.

5. Reports

5.1 Records

5.1.1 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 Date → End Date	Trunk	PinCode	Caller	Final Callee	Reset	Search
-----------------------	-------	---------	--------	--------------	-------	--------

- **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.

5.1.2 Conference Recordings

Path: **Reports -> Call Recordings -> 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	Search
------------	---	----------	----------------------	--------	----------------------	--------------	----------------------	-------	--------

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	Play Download
2022-09-01 04:14:24	887	0900	CONFERENCE(0900)	01:16	Internal	Answered	Play Download
Total 2 items						< 1 > 20 / page	Goto

5.1.3 One Touch Recordings

Path: **Reports -> Call Recordings -> 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 *1 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

Search

Start time	Caller	Callee	Final Callee	Duration	Trunk	PinCode	Type	Operation
2022-09-01 04:21:54	877	800	800	00:19			Internal	

Total 1 items

<

1

>

20 / page

Goto

5.2 Log

5.2.1 Call Log

Path: **Reports -> Logs -> Call Logs**

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 Date

→

End Date

☐

Trunk

PinCode

Caller

Callee

Final Callee

Reset

Search

Download

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

<

1

2

3

4

5

>

20 / page

Goto

1

- 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.

5.2.2 Fax Log

All fax records of the IP PBX 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 IP PBX system within the time period will be directly queried.

Start Date → End Date

Sender

Receiver

Reset

Search

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

6. Addons

6.1 API

6.1.1 AMI

Path: **Addons -> 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 ?

amiuser

Password ?

123456Abc

Allow IP/Subnet Mask ?

192.168.17.12/255.255.255.255

Submit

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

6.1.2 Push Event

Path: **Addons -> 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 ⓘ

http://192.168.21.12:8000/getEvent

Event

Cdr ×

▼

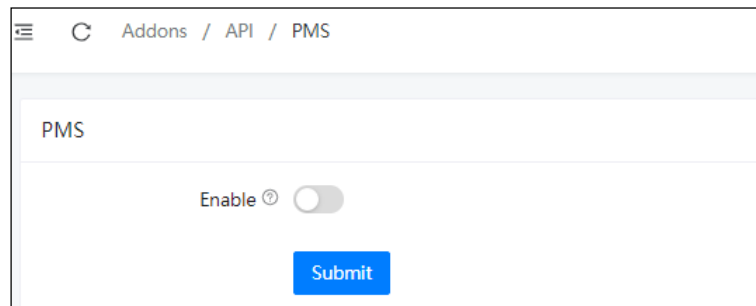
Submit

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

6.1.3 PMS

Path: **Addons -> API ->PMS**

The API of PMS system is based on TCP socket. When the PMS is enabled, the system will monitor port 8080. Third-party PMS system can send command or receive device's data through the TCP socket. For detailed configuration, please refer to the PMS Integration user guide.



Note: Enabling the PMS function will consume additional system performance. Please do not enable this function if you do not use related services.

- **Enable:** Enable/Disable the PMS service.

6.2 Control Panel

6.2.1 Group

Path: **Addons -> Control Panel->Group**

The extensions can be dispatched into different groups, and use the PBX Control Panel for paging, background music, tasks, etc.

Please click on the “Add” button to create a new group, fill out the group name and select the extensions that you would like to dispatch into this group. When the setting is finished, click on the “Submit” button to save the setting. The new group will be displayed on the PBX Control Panel.



The screenshot shows a web-based "Add" dialog box. It has a title bar with the text "Add" and a close button (X). Inside the dialog, there are two required fields, both marked with a red asterisk (*). The first field is labeled "Name" and contains the text "Group1". The second field is labeled "Extension" and is a multi-select dropdown menu. It currently displays five options: "100[100] x", "101[101] x", "102[102] x", "103[103] x", and "104[104] x". At the bottom right of the dialog are two buttons: "Cancel" and "Submit".

- **Name:** Name of the group
- **Extension:** The extension number included in the group.

6.2.2 Settings

Path: **Addons -> Control Panel->Settings**

The Control Panel is modules design, in which you can turn on and off specific modules on the Control Panel.

Panel Settings

Wake-up ☒

Address Book ☒

Blacklist ☒

Call Forward ☒

Conference ☒

Tasks ☒

Music ☒

DialPlan ☒

Display Mode

- **Wake up:** Enable/Disable the “Wake Up” module displayed on the Control Panel to manage wake-up calls.
- **Contact Person:** Enable/Disable the “Contact Person” module displayed on the Control Panel to manage contacts.
- **Blacklist:** Enable/Disable the “Blacklist” module displayed on the Control Panel to manage the blacklist.
- **Call Forward:** Enable/Disable the “Call Forward” module displayed on the Control Panel to manage the call forwarding.
- **Conference:** Enable/Disable the “Conference” module displayed on the Control Panel to manage all the conference rooms.
- **Tasks:** Enable/Disable the “Tasks” module displayed on the Control Panel to manage the paging/music tasks.
- **Music:** Enable/Disable the “Music” module displayed on the Control Panel to manage the music files.
- **Dial Plan:** Whether to enable the function of adding extension dial plan settings for the attendant console.
- **Display Mode:**
 - All: Enable all operation permissions to the Console Panel user.
 - Hotel: Block operations that violate customer privacy, such as call monitoring, etc.

6.3 Hot Standby

Path: **Addons -> Hot Standby**

The hot-standby function is using two same model of IPPBX servers 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 its status change from secondary to primary or the system restarts.

- **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, e.g., 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 supported. Please make sure DialPlan1 has the authority to dial this number.).

6.4 AutoConfig

6.4.1 Devices

Path: **Addons ->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

6.4.2 Files

Path: **Addons ->AutoConfig->Files**

This is a HTTP file server which is 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>.

Refresh Upload Delete All	
Name	Action
dialplan.xml	View File Delete
00a859eb44e9.cfg	View File Delete
68692E290375.json	View File Delete
021234586985.cfg	View File Delete
ptz	View File Delete
68692E2B0511.json	View File Delete
SEP3CCE73112233.cnf.xml	View File Delete
68692e024034.cfg	View File Delete
SEP3coe73112233.cnf.xml	View File Delete
< 1 > 10/page Total 9	

6.4.3 Custom Template

Path: **Addons** -> **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.

Devices		Files	Custom Template	
NewRefreshDelete				
☐	Name	Manufacturer	Phone Model	Action
No Data				
< 1 >		10/page	Total 0	

7. System

7.1 Reboot /Reset

7.1.1 Cron Reboot

Path: **System -> Reboot /Reset->Cron Reboot**

To periodically restart the driver or Asterisk service.

Cron Reboot

Asterisk ☐

DAHDI ☐

Interval(days) - +

Reboot Time ⌚

Submit

- **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.

7.1.2 Reboot

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

By clicking on the  button you may restart your Planet's IPX series IPPBX from the web UI.

Restarting the IP PBX system will terminate all active phone calls. Please make sure there're no phone calls going on before restarting the IP PBX system.

7.1.3 Reset

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

Method 1: Reset from web UI

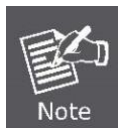
Resetting the IP PBX system

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 for restarting the system.

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: 172.16.0.1 / LAN Default IP: 192.168.0.1

After resetting it and when you access the web UI, you’ll first see the quick setup wizard. If you choose to use backup file to restore the system configurations, you may skip the quick setup wizard. If you wish to configure a fresh new phone system, you may follow the wizard to complete the configurations.



Resetting from Web UI will clear all system configurations unless you have enabled “I’d like to keep the network profiles” and “I’d like to keep the call logs and recordings” options.

By default, backups will be kept, so after resetting it from Web UI you may restore backup directly from the IP PBX system.

Method 2: Reset by pressing Reset button at system running stage.

When the IP PBX system is running, the SYS LED indicator winks once every 2 seconds. Now you may press and hold the Reset button on the back panel of the IP PBX for about 7 seconds, then the SYS LED will go off; the IPPBX system will reboot and start the reset process.

Reset IP PBX this way is the same as resetting it from the web UI. The only difference is that you cannot choose to keep the network profiles, call logs and recordings, and you will need to access the IP PBX system via the default IP.

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

Resetting the IPPBX system by Reset button at system booting stage will erase everything on the IP PBX system, including backups. Resetting this way will fully recover the IPPBX system to factory defaults.

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

To reset the IPPBX system at system booting stage, you need to first cut off the power supply. Press and hold the Reset button and then power it on. 4 to 5 seconds later, SYS LED will be on upon the release of the Reset button.

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

7.2 Region /Time

Path: **System -> Region / Time**

System time is very important for the IP PBX system, especially when the IP PBX 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 skip the quick setup wizard or you want to change the time zone, you can do it here.

Location

Country / Region ⓘ US

Submit

Time Settings

Current PBX Time 2022-08-10 02:47

Sync **NTP Time Settings** Manual Time Settings

Time Zone US/Central

* NTP Server time.nist.gov

Submit

Location and time may be configured separately. Both modifying location and time settings require rebooting the IP PBX system.

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

2022-08-10 15:46:59

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 the [Submit](#) button to save the manually set time to the IP PBX hardware.

7.3 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 IP PBX USB interface for saving the above-mentioned files.

7.3.1 USB Storage

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

The IPX-1100/IPX-1102 and IPX-2200 has 1 USB interface on the back panel. USB drives could be attached to the USB interface for data backup.

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 IP PBX 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** change to **Read And Write**.

The screenshot displays the 'USB Storage Status' and 'USB Storage Settings' configuration page. At the top, the 'USB Mount Status' is 'Read And Write', with an 'Unmount' button. A red warning message states 'Must Unmount USB before unplugging'. The 'USB Storage Settings' section includes an 'Enable' toggle (checked), a 'Frequency (days)' spinner set to 1, and an 'Upload Time' spinner set to 00:01. Below these are five toggle switches for 'Call Logs', 'Call Recordings' (checked), 'Voice Messages', and 'System Logs'. A 'Submit' button is at the bottom.

Setting	Value/Status
USB Mount Status	Read And Write
Unmount	Button
Enable	Checked
Frequency (days)	1
Upload Time	00:01
Call Logs	Unchecked
Call Recordings	Checked
Voice Messages	Unchecked
System Logs	Unchecked
Submit	Button

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

As the example shown above, the system will back up the call recording data only to the USB storage at 1AM 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.



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

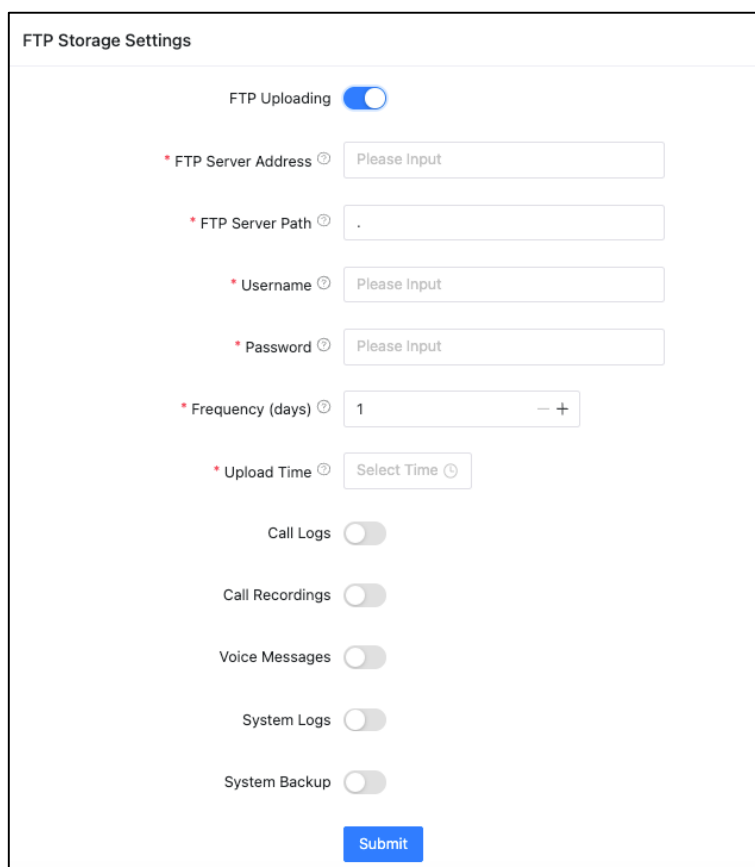
7.3.2 FTP Storage

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.



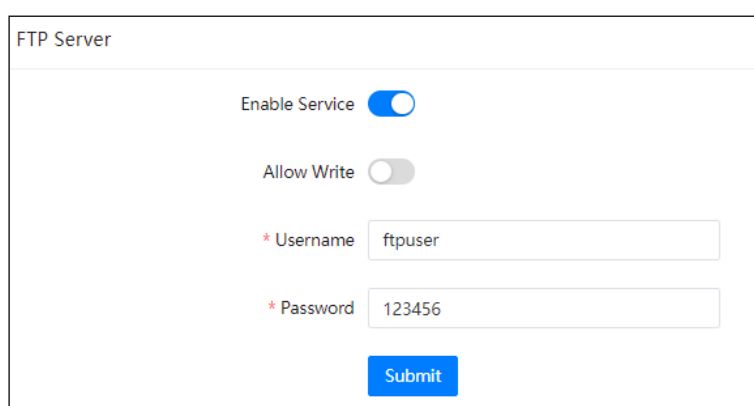
The screenshot shows the 'FTP Storage Settings' interface. At the top, there is a title 'FTP Storage Settings'. Below it, the 'FTP Uploading' toggle is turned on. There are five required fields, each marked with a red asterisk and a help icon: 'FTP Server Address' (placeholder: 'Please Input'), 'FTP Server Path' (placeholder: '.'), 'Username' (placeholder: 'Please Input'), 'Password' (placeholder: 'Please Input'), and 'Frequency (days)' (value: '1', with minus and plus buttons). Below these is the 'Upload Time' field with a 'Select Time' button. At the bottom, there are five toggle switches for 'Call Logs', 'Call Recordings', 'Voice Messages', 'System Logs', and 'System Backup', all of which are currently turned off. A blue 'Submit' button is located at the bottom right of the form.

- 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.

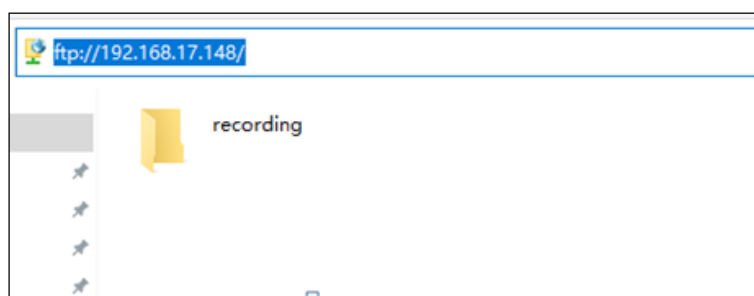
Once configurations done, click on **Submit** button to connect the IP PBX system with the FTP server. Once connected, you'll see the **FTP Connect Status** change to **Connected**.

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

To enable the FTP server service, you need to create an FTP user first. Afterward, you can use FTP client software on your desktop to connect to the IPPBX's FTP server and manage all the files.



The screenshot shows the 'FTP Server' configuration window. It has a title bar 'FTP Server'. Inside, there are two toggle switches: 'Enable Service' which is turned on (blue), and 'Allow Write' which is turned off (grey). Below these are two text input fields: '* Username' with the value 'ftpuser' and '* Password' with the value '123456'. At the bottom right is a blue 'Submit' button.



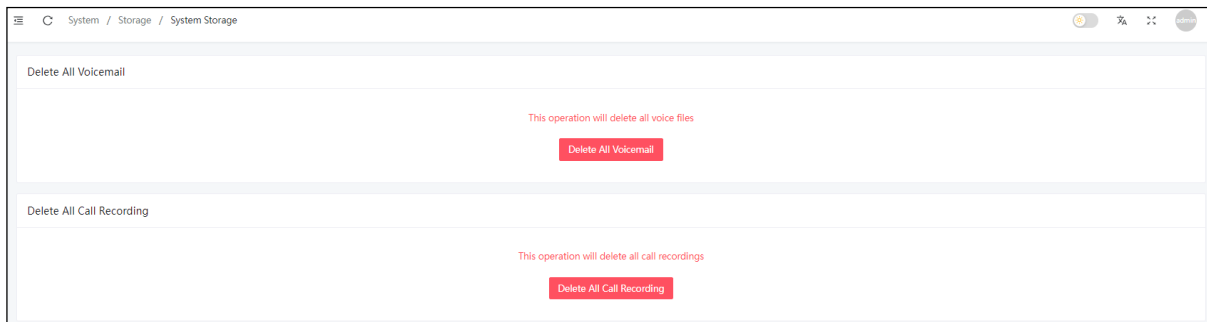
- **Enable Service:** Enable/Disable FTP server service.
- **Allow Write:** Whether to allow the client user to modify the data on the server after logging in.
- **Username:** FTP client login username.
- **Password:** FTP client login password.

7.3.3 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.



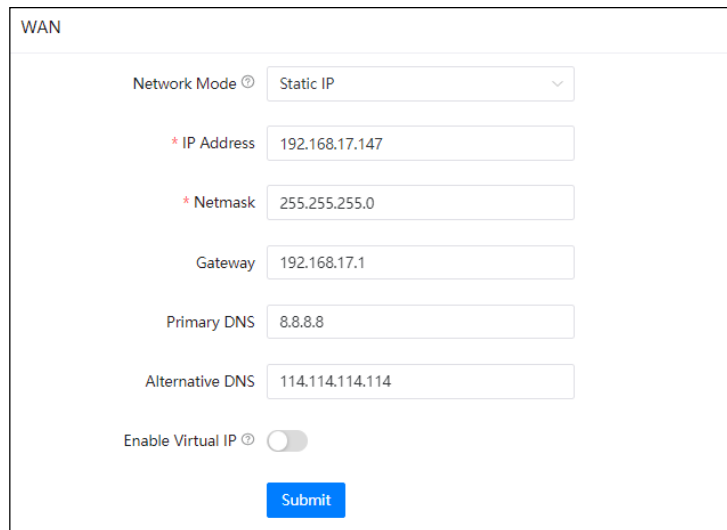
7.4 Network Settings

7.4.1 Network Profiles

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

Network profiles could be configured through the quick setup wizard at the initial setup of the IP PBX system.

When modification of the network profiles is required, it could be done here.

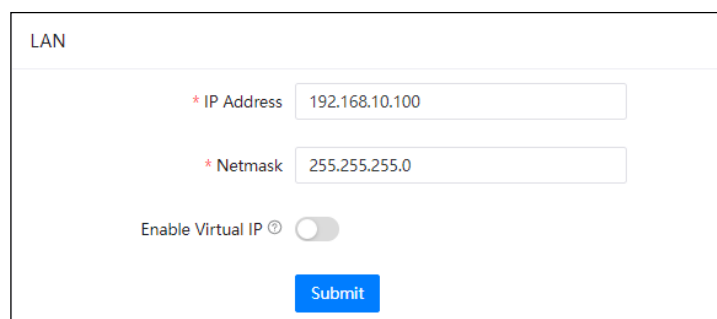


The screenshot shows the WAN configuration page. At the top, there's a tab labeled 'WAN'. Below it, the 'Network Mode' is set to 'Static IP' in a dropdown menu. There are several input fields: '* IP Address' with the value '192.168.17.147', '* Netmask' with '255.255.255.0', 'Gateway' with '192.168.17.1', 'Primary DNS' with '8.8.8.8', and 'Alternative DNS' with '114.114.114.114'. At the bottom, there's a toggle switch for 'Enable Virtual IP' which is currently turned off. A blue 'Submit' button is located at the bottom center.

The WAN network interface of Planet's IPX series 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 IP PBX through this IP address.

On WAN port, gateway and DNS could be configured so the IP PBX 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 IP PBX system to have Internet access.



The screenshot shows the LAN configuration page. At the top, there's a tab labeled 'LAN'. Below it, there are two input fields: '* IP Address' with the value '192.168.10.100' and '* Netmask' with '255.255.255.0'. At the bottom, there's a toggle switch for 'Enable Virtual IP' which is currently turned off. A blue 'Submit' button is located at the bottom center.

Default IP on LAN port is 192.168.0.1; you may change this IP but LAN IP should NOT be in the same network segment as WAN port.

7.4.2 VLAN

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

With a Layer 3 switch, you can configure VLAN on Planet's IPX IPPBX system to separate 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 ☐

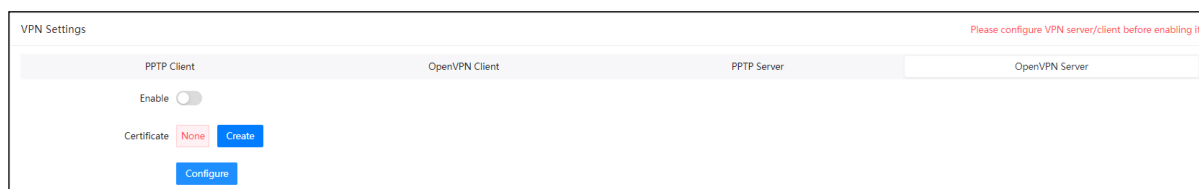
Submit

Ensure that the VLAN IPs for VLAN1 and VLAN2 on both WAN and LAN interfaces are in separate network segments.

7.4.3 VPN

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

VPN (Virtual Private Network) is mainly used for setting up long-distance and/or secure network connections. When used on the IP PBX system, all phone calls made and received are encrypted so it secures your remote offices/extensions' phone services. Built-in VPN Server on the Planet's IPX series IPPBX system is an easy way to set up a secure connection between other Planet's IPX series 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 use of random port numbers for establishing connections.



VPN Settings

Please configure VPN server/client before enabling it

PPTP Client OpenVPN Client PPTP Server OpenVPN Server

Enable ☐

Certificate None Create

Configure

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. It was written by James Yonan and is published under the GNU General Public License (GPL).

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. When used in a multiclient-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.

VPN Settings

Please configure VPN server/client before enabling it

PPTP Client

OpenVPN Client

PPTP Server

OpenVPN Server

Enable

Certificate

None

Create

Configure

Configure the VPN server before turning it on.

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

View OpenVPN Certificate

Country / Region

Province

City

Organization

Email

CA/KEY Expire

Close

Specify your customized information and click on [Submit](#) button to continue.

Click on [Configure](#) button to set up the OpenVPN server.

OpenVPN Server configuration

Stealth

* Port

1194

Protocol

UDP

Device Node

TUN

Cipher

default

Compress LZO

TLS Server

Remote Network IP

Please Input

Remote Network Netmask

Please Input

Route IP

Please Input

Route Netmask

Please Input

Client to Client

Cancel

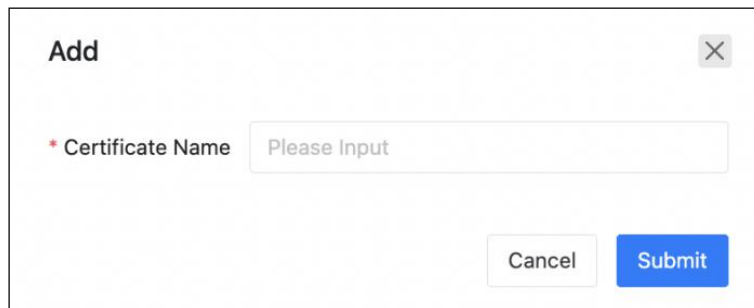
Submit

- **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.

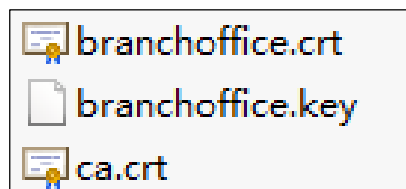
- **Device Node:** TUN or TAP; A TAP device is a virtual Ethernet adapter, while a TUN device is a virtual point-to-point IP link.
- **Cipher:** Cipher (or cypher) is an algorithm for performing encryption or decryption. □
- **Compress LZO:** LZO is an efficient data compression library which is suitable 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 uses the first available IP assigned by the VPN server.
- **Route:** The route entries adjust the local routing table, specifying which network to route over the VPN.
- **Client-to-Client:** Client-to-Client can enable intercommunication between clients.

Once configuration is 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 Planet's IPX series 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. You will obtain three files, which should be uploaded on a client to enable connection to this server.



Finally, turn on the switch to enable OpenVPN server.

OpenVPN Client

To configure OpenVPN client, please click on the  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

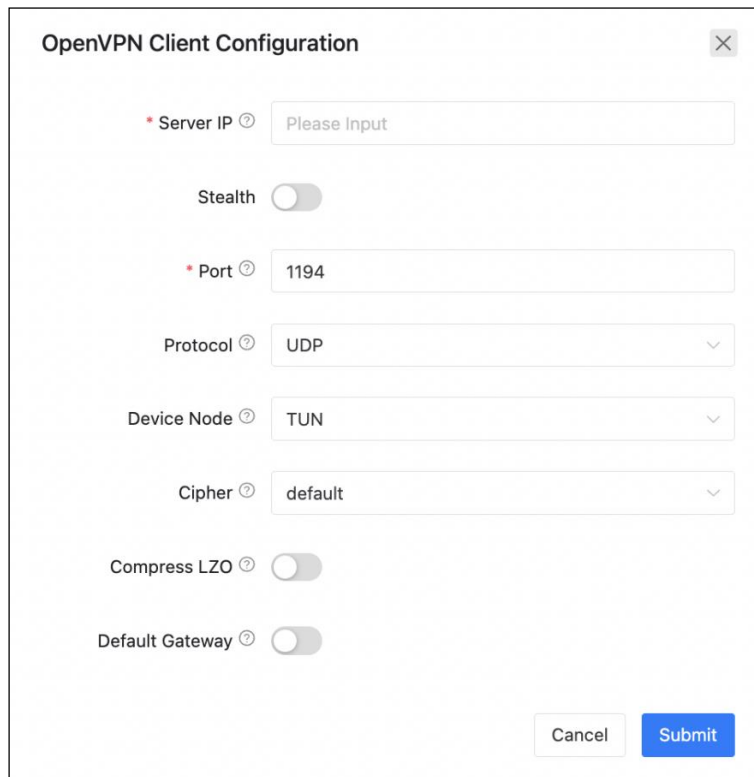
The certificate files downloaded from the OpenVPN server should be uploaded here.

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  button to configure the OpenVPN client to connect to the server.



The image shows a dialog box titled "OpenVPN Client Configuration" with a close button (X) in the top right corner. The dialog contains several configuration fields and toggle switches:

- Server IP**: A text input field with a red asterisk and a help icon. The placeholder text is "Please Input".
- Stealth**: A toggle switch currently turned off.
- Port**: A text input field with a red asterisk and a help icon. The value is "1194".
- Protocol**: A dropdown menu with a help icon, currently set to "UDP".
- Device Node**: A dropdown menu with a help icon, currently set to "TUN".
- Cipher**: A dropdown menu with a help icon, currently set to "default".
- Compress LZO**: A toggle switch currently turned off.
- Default Gateway**: A toggle switch currently turned off.

At the bottom right of the dialog are two buttons: "Cancel" and "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 identical to that configured on the OpenVPN server, typically set to the default value of 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.
- Whether to enable Compress LZO or not depends on whether you have enabled it on the server.
- If **Default Gateway** is enabled, it will use VPN connection as default gateway. Data which should be sent to the default gateway will now be sent through 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

Mode

Status

172.16.0.6

openvpn

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  button to show the configurations.



VPN Settings

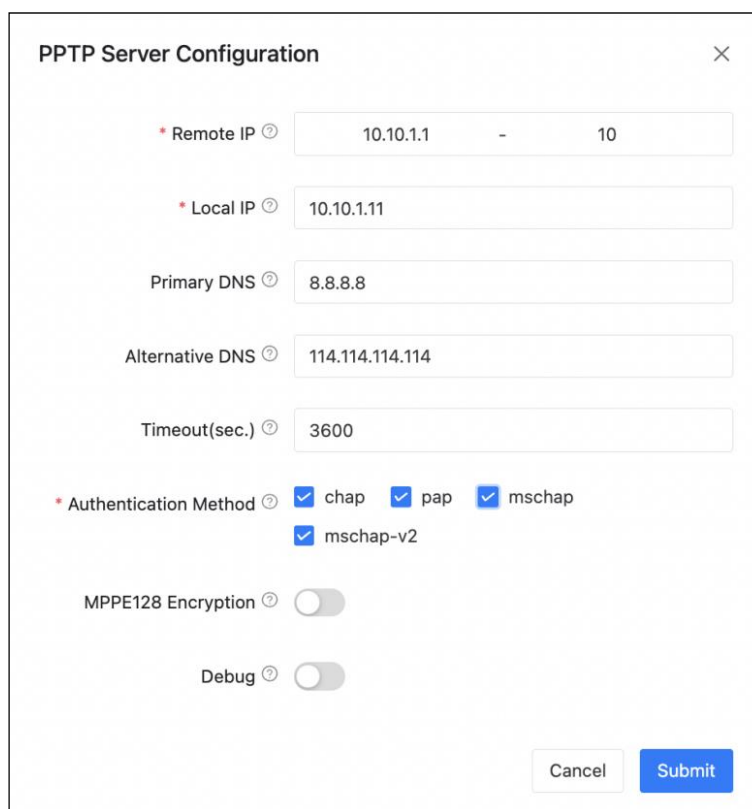
Please configure VPN server/client before enabling it

PPTP Client OpenVPN Client **PPTP Server** OpenVPN Server

Enable ☐

[Configure](#)

Configure the PPTP VPN server before enabling it.



PPTP Server Configuration

* 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 Planet's IPX-V series IPPBX can connect up to 20 PPTP VPN clients.

The screenshot displays a web-based interface for managing VPN users. On the left, a table titled 'List of VPN Users' has a header row with 'Username'. The main area is partially obscured by a central 'Add' dialog box. This dialog box contains fields for 'Username' (filled with 'pptpuser'), 'Password' (masked with asterisks), and an 'Available' toggle switch which is currently turned on. At the bottom of the dialog are 'Cancel' and 'Submit' buttons. To the right of the dialog, a table with an 'Operation' column is visible. At the bottom right of the interface, there is a pagination control showing '20 / page' and a 'Goto' button.

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.

List of VPN Users			Add
Username	Available	Operation	
pptpuser	Yes		
Total 1 items		< 1 > 20 / page Goto	

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

VPN Settings

Please configure VPN server/client before enabling it

PPTP Client

OpenVPN Client

PPTP Server

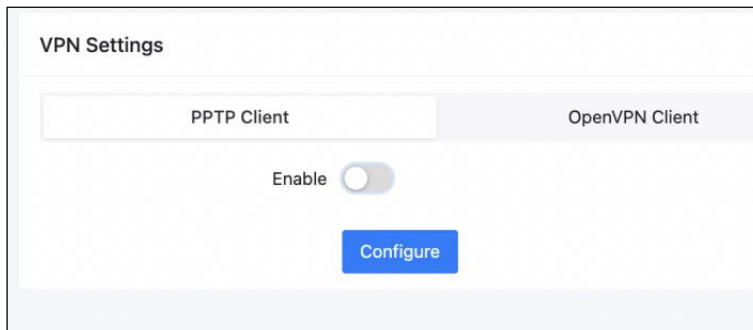
OpenVPN Server

Enable ☒

Configure

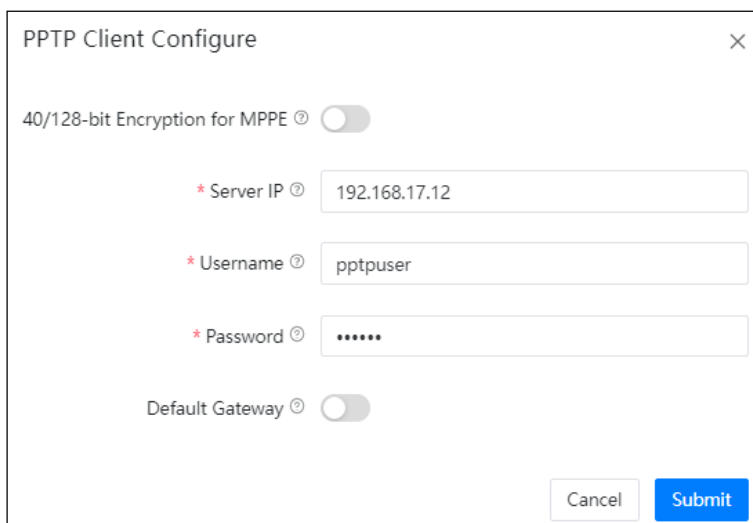
PPTP VPN Client

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



The 'VPN Settings' dialog box contains two tabs: 'PPTP Client' and 'OpenVPN Client'. The 'PPTP Client' tab is selected. Below the tabs, there is an 'Enable' toggle switch which is currently turned off. A blue 'Configure' button is positioned below the toggle switch.

Configure PPTP VPN client settings before enabling it.



The 'PPTP Client Configure' dialog box includes a close button (X) in the top right corner. It features a '40/128-bit Encryption for MPPE' toggle switch, which is currently off. Below this, there are three required fields: 'Server IP' (containing '192.168.17.12'), 'Username' (containing 'pptpuser'), and 'Password' (displayed as dots). At the bottom, there is a 'Default Gateway' toggle switch, which is also off. 'Cancel' and 'Submit' buttons are located at the bottom right.

- **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  button to continue, and now you may click on Enable switch to turn on PPTP VPN client.

VPN Settings

Please configure VPN server/client before enabling it

PPTP Client

OpenVPN Client

PPTP Server

OpenVPN Server

Enable

Configure

VPN Client Status

Address

Mode

Status

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

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.

7.4.4 Static Routing

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

Route Table			
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.

The screenshot shows the 'Add Static Route' dialog box overlaid on the static routing configuration page. The dialog box has three input fields: 'Destination', 'Netmask', and 'Gateway', each with a 'Please Input' placeholder. Below the fields are 'Cancel' and 'Submit' buttons. The background shows a table with columns for Destination, Gateway, Netmask, and Port, with rows for 0.0.0.0, 8.8.8.8, 192.168.10.0, and 192.168.18.0. An 'Add' button is visible in the bottom left of the background interface.

- **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.

7.4.5 DHCP Server

Path: **System -> Network Settings -> 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 Planet's IPX series IPPBXs WAN/LAN port. This saves administrators a significant amount of time compared to manually configuring these settings. Before activating DHCP services, please ensure there's no other DHCP server running in your LAN, otherwise there will be collision between servers.

Set the DHCP server network parameters and turn it on.

DHCP Services

Enable ☐

Port

LAN

* Start IP Address

192.168.10.150

* End IP Address

192.168.10.199

* Netmask

255.255.255.0

Gateway

192.168.10.1

DNS

192.168.10.1

TFTP

Please Input

* Address Lease Time(hour)

24

- +

Submit

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 a host or client to always get the same IP address, **IP Address Reservation** will help. Click on the  button.

Add

*

Name

Client1

*

MAC Address

2e:30:f3:12:33:df

*

IP Address

192.168.10.101

Cancel

Submit

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.

7.4.6 SNMP

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

SNMP Settings

Read Only

Enable ☒

* Community

* Network

* Subnet Length

Read Write

Enable ☒

* Community

* Network

* Subnet Length

Submit

- **Enable:** Enable/Disable SNMP
- **Community:** Community tag
- **Network:** The working network of SNMP

No need to add them to the IP whitelist.

7.5 Email Services

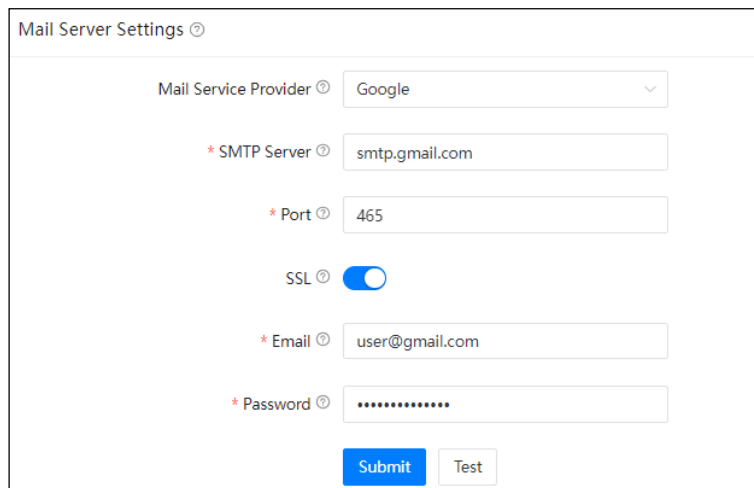
7.5.1 Mail Server Settings

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

Various kinds of Emails could be sent from the Planet's IPX series 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. At the initial system setup stage while you were going through the quick installation wizard, mail server could be configured. If you've not done it from the wizard, it still can be configured from here.

We have integrated pre-configured SMTP templates from popular email service providers, allowing users to swiftly deploy their mail server.

A screenshot of the 'Mail Server Settings' configuration page. The page has a title 'Mail Server Settings' with a help icon. It contains several fields: 'Mail Service Provider' is a dropdown menu with 'Google' selected; '* SMTP Server' is a text field with 'smtp.gmail.com'; '* Port' is a text field with '465'; 'SSL' is a toggle switch that is turned on; '* Email' is a text field with 'user@gmail.com'; and '* Password' is a text field with masked characters. At the bottom, there are two buttons: 'Submit' (blue) and 'Test' (grey).

- In the **Mail Service Provider** dropdown list, select your Email service provider. If it's not included here, please choose **Other**.
- After selecting the mail service provider, the SMTP Server field will be automatically populated. 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 IP PBX system will be sent out by this mail account.
- In **Password** field, input the password of the Email account you have specified.

Once done, click on **Submit** 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.



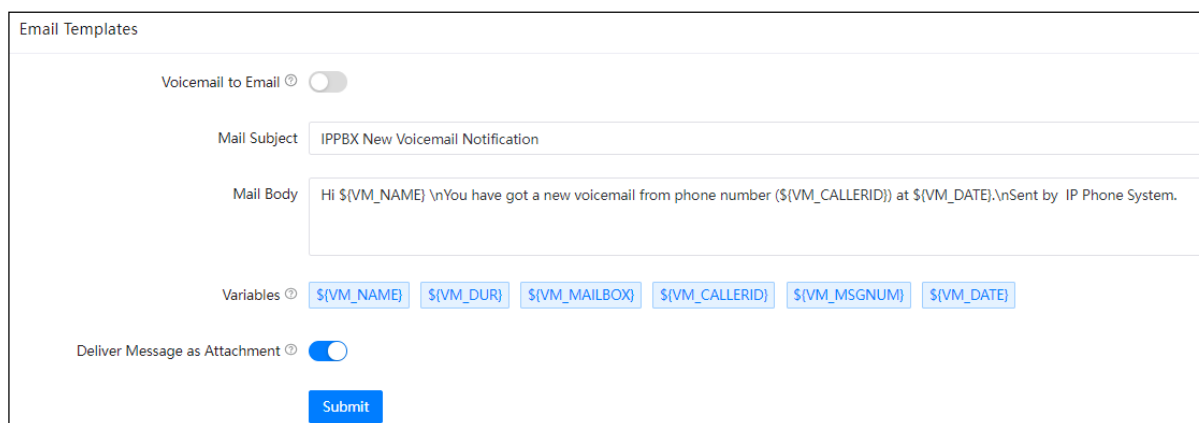
You may need to activate SMTP service from your Email web portal before you can successfully configure SMTP server on the IP PBX system.

7.5.2 Voicemail to Email Settings

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

Voicemail to Email is a highly beneficial feature for extension users. The IPPBX system can send newly received voicemail messages from their extensions to their email inbox. .

It could be an Email notification or administrator could set the IP PBX system to send Email with voice messages attached in the Email notifications.



The screenshot shows the 'Email Templates' configuration page. At the top, there is a toggle switch for 'Voicemail to Email' which is currently turned off. Below this, the 'Mail Subject' field is set to 'IPPBX New Voicemail Notification'. The 'Mail Body' field contains a template: 'Hi \${VM_NAME} \nYou have got a new voicemail from phone number (\${VM_CALLERID}) at \${VM_DATE}.\nSent by IP Phone System.' Below the mail body, there is a 'Variables' section with a list of available variables: \${VM_NAME}, \${VM_DUR}, \${VM_MAILBOX}, \${VM_CALLERID}, \${VM_MSGNUM}, and \${VM_DATE}. At the bottom, there is a toggle switch for 'Deliver Message as Attachment' which is currently turned on. A 'Submit' button is located at the bottom right of the form.

- 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 play back the voice messages when they got the notify Email.

When Voicemail to Email is enabled and the Mail Server is configured, extension users will receive email notifications upon receiving new voice messages on their extensions. Ensure that the extensions have their email addresses specified for this feature to work effectively.

7.6 Diagnostic

7.6.1 PING

Path: **Maintenance -> 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 output results from the system indicating the reachability of the destination.

Ping

IP Address / Domain *

8.8.8.8

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
```

7.6.2 Trace Route

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

Path: **Maintenance -> Diagnostic -> Traceroute**

In the IP Address/Domain Name field, specify the IP or domain name that you want to look up and click on

Submit button to begin tracing.

Trace Route

IP Address / Domain *

8.8.8.8

C

Submit

traceroute 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.

7.6.3 TCP Dump

Ethernet capture uses TCP DUMP 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 Planet's IPX IPPBX is attached. The captured packets can be downloaded from the IP PBX system and have been analyzed on your Windows PC to display the SIP traffic details. It can be used to debug a VoIP call problem.

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

To capture the network traffic, you'll need to select the network interface based on which the IP PBX system is operating. Then click on **Start** button to start capturing the network traffic.



The screenshot shows a web interface titled "TCP Dump". Below the title, there is a label "Interface *" followed by a dropdown menu currently displaying "all". To the right of the dropdown is a red button labeled "Stop" and a blue circular refresh icon.

Once the process begins, the Start button will change to Stop. At this moment, make a call to replicate the phone call problem or ensure that another issue has recurred. This way, the captured network traffic may contain 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 Planet support team for help.

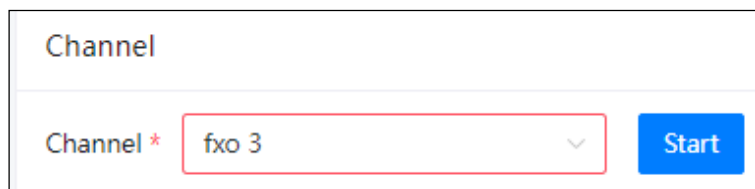
7.6.4 Channel Monitor

Path: **Maintenance -> Diagnostic -> Channel Monitor**

Channel Monitor, technically DAHDI Monitor, allows you to monitor signal levels on analog channel and record the output to a file. Recorded audio files are, by default, in raw signed linear PCM. You can play them through the speaker to listen to the phone call signaling on the analog channel. Or you can use a sounds editor to visually display the audio level at both the Rx (audio Received by Asterisk) and Tx (audio Transmitted by Asterisk).

Usually Channel Monitor can be used to capture the caller ID signaling of an FXO channel. If you are experiencing caller ID problem you can perform channel monitor on the FXO port and then analyze the captured packets. If needed, you can send this file to Planet support for help.

Before starting channel monitor, you need to select an FXO interface. Then click on **Start** button to capture signaling on the selected interface.



The screenshot shows a web interface for the Channel Monitor. It has a title 'Channel' in orange. Below it, there is a label 'Channel *' in grey. To the right of the label is a dropdown menu with a red border, containing the text 'fxo 3' and a small downward arrow. To the right of the dropdown menu is a blue button with the text 'Start' in white.

Once the process has started, the button will change to Stop. Now you should recur the problem by making a call in through the selected interface. When the extension started to ring the third time you may hang up and stop channel monitor by clicking on **Stop** button. As soon as the channel monitor stops, the captured signaling will be automatically downloaded.

If you have the knowledge of how to analyze the files, you may open them with some sound editors like Wavepad.

7.6.5 Asterisk CLI

The Asterisk CLI provides you with the access to execute the Asterisk CLI commands. To avoid incorrect operation that may affect the IPPBX system, it provides the pjsip and core command to check the status.

Path: *Maintenance -> Diagnostic ->Asterisk CLI*



7.7 Security Center

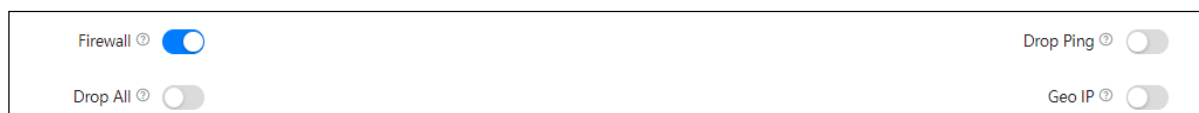
Planet's IPX IPPBX system has been preconfigured with a built-in firewall which prevents your IP phone system from unauthorized access, malicious users and some other attackers.

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

7.7.1 Firewall

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

Planet's IPX series 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 Planet's IPX 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 Planet's IPX IPPBX system to block all communication with the outside world. Only Web UI still works in local network while other services will all be terminated.
- **Geo IP** is a security policy which can be used to grant access to IP addresses from certain countries/regions but 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

Firewall ⓘ ☒	Drop Ping ⓘ ☐
Drop All ⓘ ☒	Geo IP ⓘ ☒

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 ⓘ	Lan
* Action ⓘ	Accept ▼
* Protocol ⓘ	TCP/UDP ▼
IP Address ⓘ	192.168.10.0
Netmask ⓘ	255.255.0.0
Port ⓘ	-
Mac Address ⓘ	Please Input

Cancel

Submit

- 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 IP PBX 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.

Common Rules							Add
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.



If you are going to add rules to block some IP addresses from accessing some kind of services on the IP PBX 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 defined, the firewall will consider as ALL); otherwise, misconfiguration of a deny rule might cause the IPPBX system a total lockdown, the only way would be using Console to unlock the IP PBX through command lines.

Auto Defense will help with the prevention of DDoS attacks.

Add

*

Name

AMI

*

Port

5038

- +

*

Protocol

TCP

▼

*

Packet

20

- +

*

Interval

60

- +

Cancel

Submit

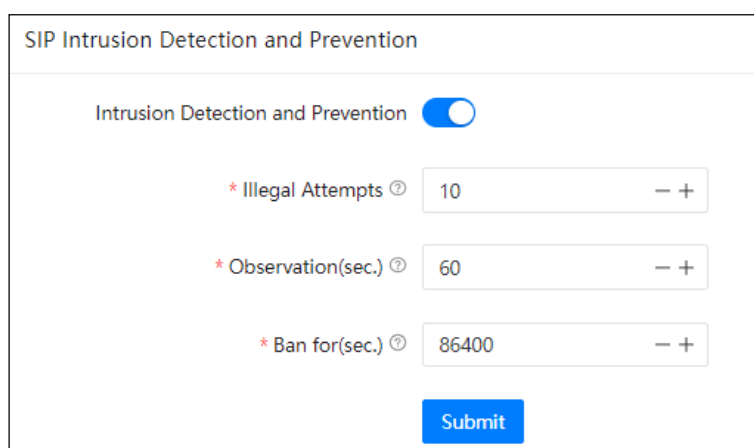
You may specify the service port number and the maximum packets to be accepted on this port number in a certain time interval. Except for the specified number of packets, more packets sent within the time interval will be dropped by the IPPBX system.

7.7.2 Intrusion Detection and Prevention

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

Planet's IPX series 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 IP PBX system safe.



The screenshot shows a web interface titled "SIP Intrusion Detection and Prevention". It features a toggle switch for "Intrusion Detection and Prevention" which is turned on. Below the toggle, there are three configuration fields, each with a red asterisk and a help icon: "Illegal Attempts" set to 10, "Observation(sec.)" set to 60, and "Ban for(sec.)" set to 86400. Each field has minus and plus buttons for adjustment. A blue "Submit" button is located at the bottom right of the configuration area.

Each of the intrusion detection and prevention rule is configured with a maximum **Illegal Attempts** and the **Observation** time duration. Once the **Illegal Attempts** reaches 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 in the **Auto Defense** section of the **Firewall** page.

7.7.3 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/attack has been detected. And the list will show the IP address of the banned hosts, as well as what kind of service intrusion is detected.

Type ⓘ	IP Address ⓘ	Operation
 No Data		

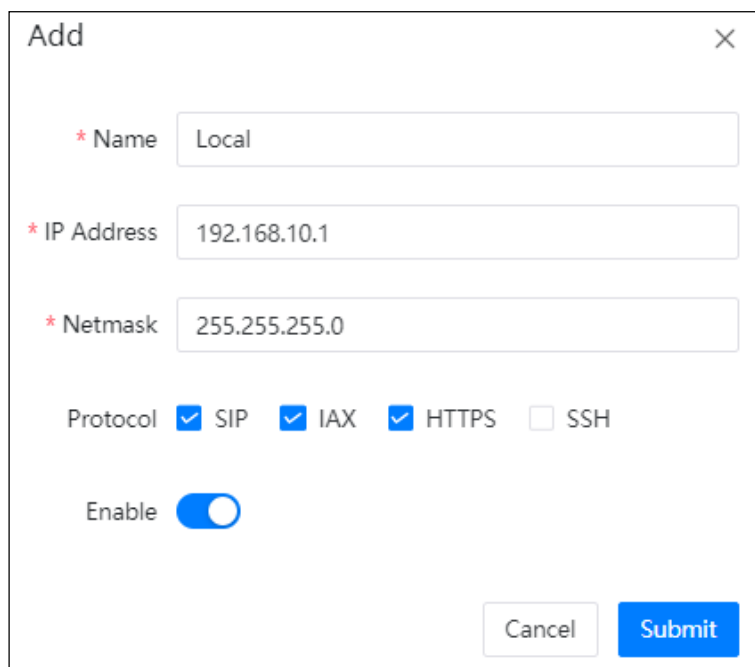
If an IP address appears incorrectly in the list of rejected IP, you can click on the  button to remove it from the IP blacklist.

7.7.4 IP Whitelist

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

IP Whitelist allows you to add IP addresses and network addresses to the IP PBX system as trusted entities.

The IP addresses in the whitelist will always be treated as trusted IPs and will not be regulated by the firewall rules.



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 IP PBX system.
- **SSH** allows the IP to access the IP PBX system command lines through SSH.

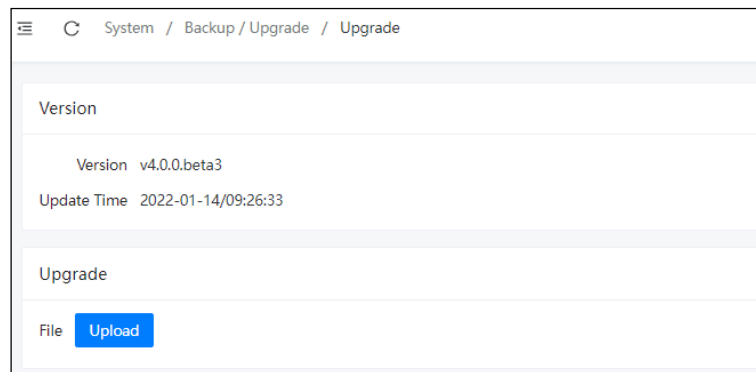


You'll only need to add trusted IP addresses to the IP Whitelist when you have configured Drop All or Geo IP security policies. And in the policies these IP addresses are not included as trusted IP addresses. Otherwise, you don't have to add them to the IP whitelist.

7.8 Backup/Upgrade

7.8.1 Upgrade

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



The screenshot shows a web interface for the 'Upgrade' section. At the top, there is a breadcrumb navigation path: 'System / Backup / Upgrade / Upgrade'. Below this, the page is divided into two main sections. The first section, titled 'Version', displays the current version as 'v4.0.0.beta3' and the 'Update Time' as '2022-01-14/09:26:33'. The second section, titled 'Upgrade', contains a 'File' label and a blue 'Upload' button.

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.

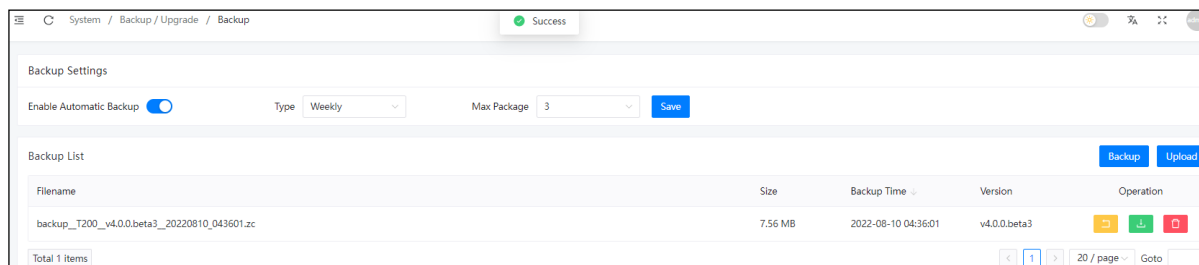
7.8.2 Backup

Taking a backup on Planet's IPX IPPBX system is similar to creating a recovery point on your Windows system. By restoring the backup you can recover the Planet's IPX IPPBX system configurations to the time when it is 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  button to download the backup to your operating system. Or click on  button to delete it from the IPPBX system.

When you want to restore the backup, you may click on the  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 do this.

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



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.

7.9 System Logs

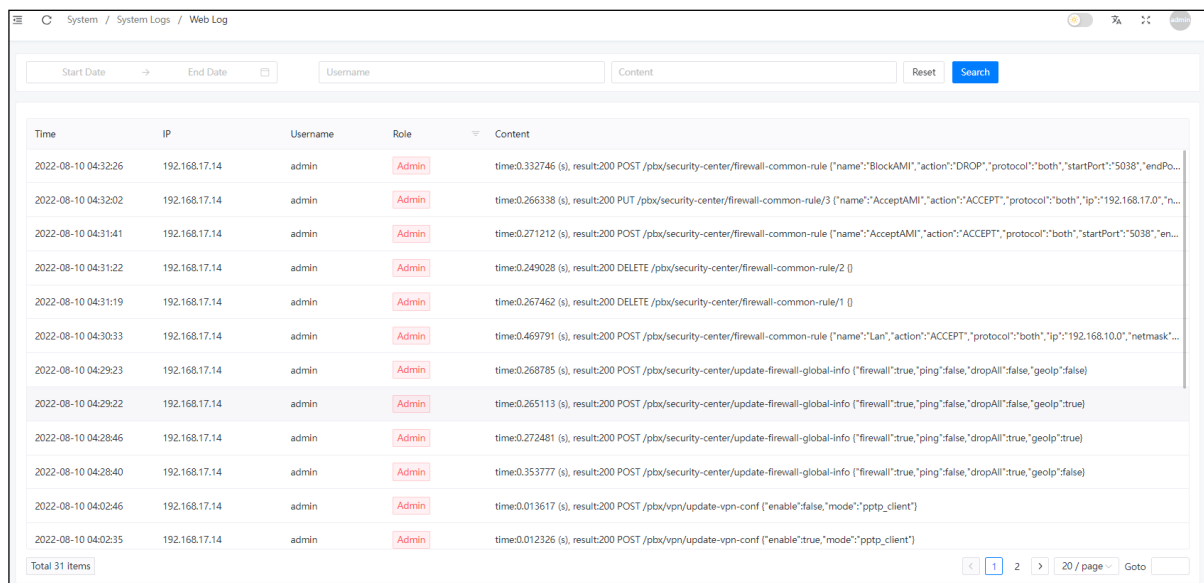
7.9.1 Web Log

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 and then finally click on [Search](#) button.

The searching results are shown below.



The screenshot displays the 'Web Log' page in a web application. At the top, there is a navigation bar with 'System / System Logs / Web Log'. Below this is a search filter area with fields for 'Start Date', 'End Date', 'Username', and 'Content', along with 'Reset' and 'Search' buttons. The main area contains a table with the following columns: Time, IP, Username, Role, and Content. The table lists 13 log entries, all from the IP 192.168.17.14 and user 'admin'. The 'Role' column shows 'Admin' in red text. The 'Content' column contains detailed log messages, such as firewall rule actions and VPN updates. At the bottom left, it says 'Total 31 items'. At the bottom right, there is a pagination control showing '1' of 2 pages, '20 / page', and a 'Goto' field.

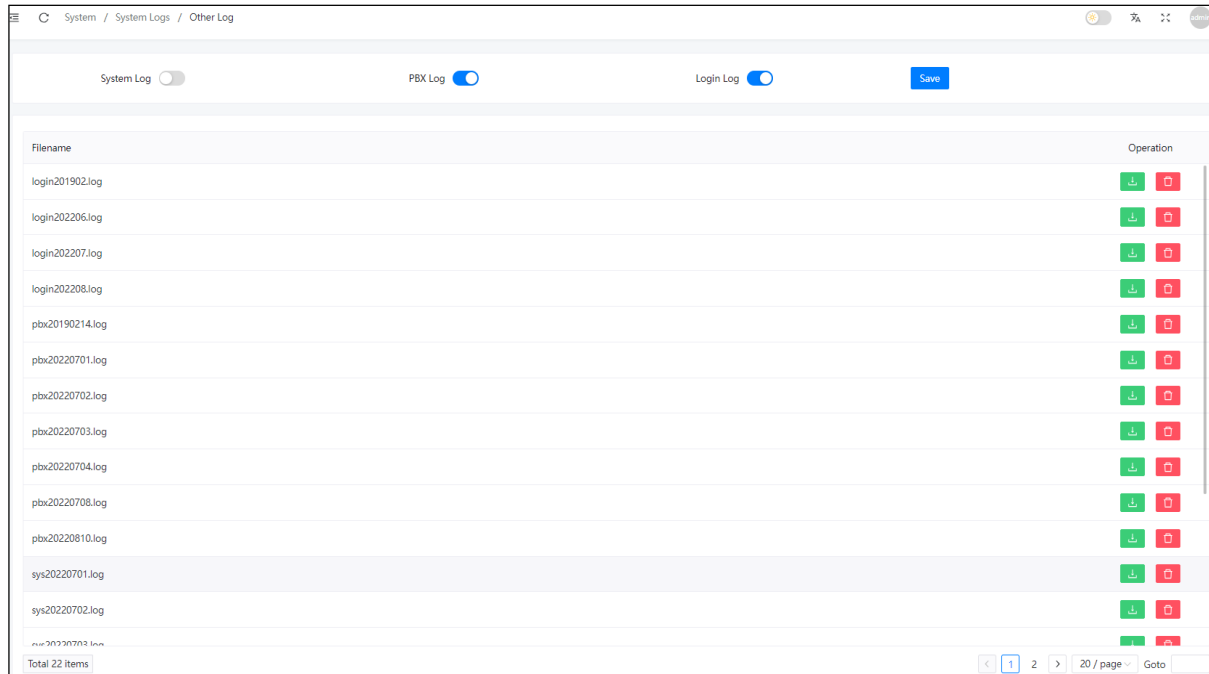
Time	IP	Username	Role	Content
2022-08-10 04:32:26	192.168.17.14	admin	Admin	time:0.332746 (s), result:200 POST /pbx/security-center/firewall-common-rule {"name":"BlockAMI","action":"DROP","protocol":"both","startPort":"5038","endPo...
2022-08-10 04:32:02	192.168.17.14	admin	Admin	time:0.266338 (s), result:200 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.

7.9.2 Other Log

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

Advanced logging can be employed for a higher level of troubleshooting on the IPPBX system.



The screenshot shows a web interface for 'Other Log'. At the top, there are three toggle switches: 'System Log' (disabled), 'PBX Log' (enabled), and 'Login Log' (enabled). A 'Save' button is located to the right of these toggles. Below the toggles is a table with two columns: 'Filename' and 'Operation'. The table lists 14 log files, each with a green download icon and a red delete icon. The files are: login201902.log, login202206.log, login202207.log, login202208.log, pbx20190214.log, pbx20220701.log, pbx20220702.log, pbx20220703.log, pbx20220704.log, pbx20220708.log, pbx20220810.log, sys20220701.log, sys20220702.log, and sys20220703.log. At the bottom left, it says 'Total 22 Items'. At the bottom right, there is a pagination control showing '1' of '2' pages, '20 / page', and a 'Goto' field.

Filename	Operation
login201902.log	 
login202206.log	 
login202207.log	 
login202208.log	 
pbx20190214.log	 
pbx20220701.log	 
pbx20220702.log	 
pbx20220703.log	 
pbx20220704.log	 
pbx20220708.log	 
pbx20220810.log	 
sys20220701.log	 
sys20220702.log	 
sys20220703.log	 

- **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 is asked for these kinds of logs for troubleshooting, otherwise please keep them disabled.

7.10 Settings

7.10.1 Account

The Account page is for managing different user roles and login accounts within the entire IP PBX system.

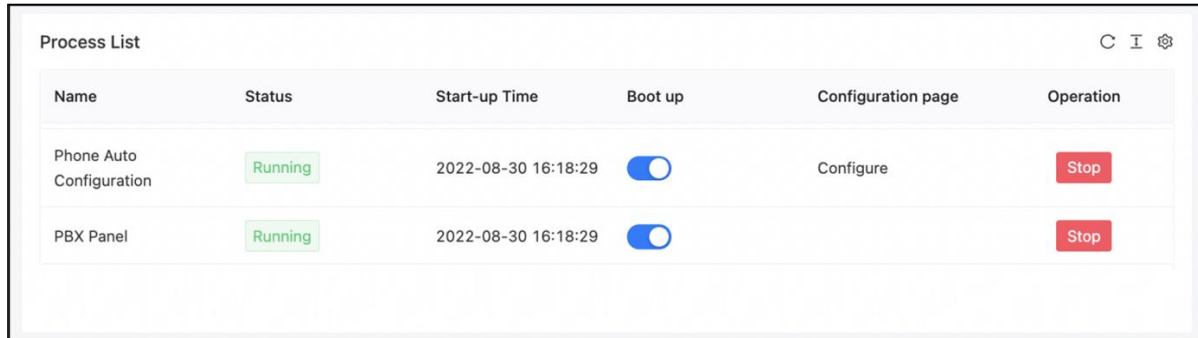
Please click on the “Add” button to create a new user account and select the corresponding user role for this account. When the user role is “Panel User”, an extension number is required to be bound to the user. In addition, the Administrator account can only change the password but cannot be deleted.

Add						
Username	↓ Password	Role	Extension	Operation		
admin	*****	Admin		Edit	Delete	
bill	*****	Billing Manager		Edit	Delete	
cgg	*****	Panel User	999	Edit	Delete	
user	*****	Panel User	877	Edit	Delete	
lookingsea	*****	Panel User	808	Edit	Delete	
ZY	*****	Panel User	855	Edit	Delete	
web	*****	Operator User		Edit	Delete	
test	*****	Panel User	873	Edit	Delete	
tqc	*****	Panel User	888	Edit	Delete	
Total 9 items				1 20 / page Goto 1		

- **Username and password:** Account username and password
- **Role:** User roles correspond to their respective e landing page or 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.

7.10.2 Plug-in

The Plug-in management page can control whether to enable or disable certain plug-in, such as the IP Phone auto provisioning, or the PBX panel. It is suggested to disable the plug-in that you are not using, because each plug-in requires extra system resources to run.



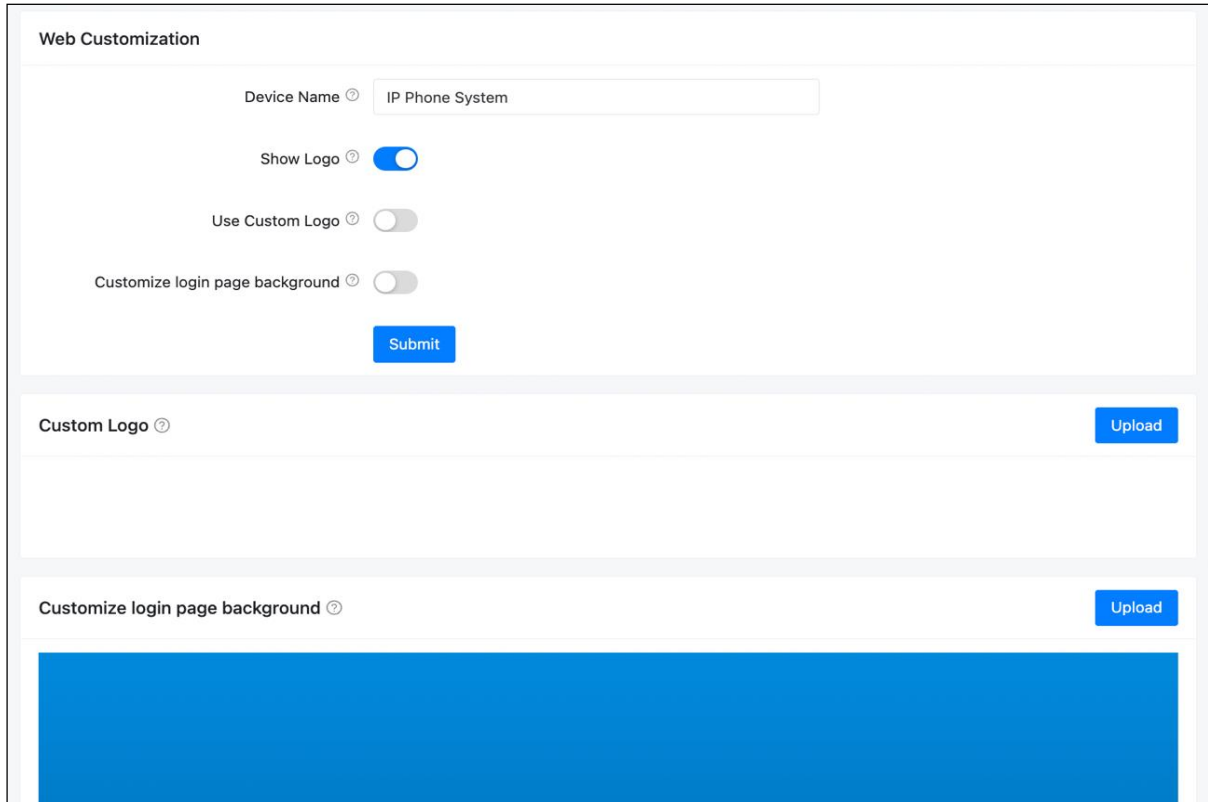
The screenshot displays a 'Process List' window with a table of active plug-ins. The table has six columns: Name, Status, Start-up Time, Boot up, Configuration page, and Operation. Two entries are listed: 'Phone Auto Configuration' and 'PBX Panel', both with a 'Running' status and a 'Stop' button in the Operation column. The 'Boot up' column contains toggle switches, both of which are currently turned on. The 'Configuration page' column shows a 'Configure' link for the Phone Auto Configuration entry.

Name	Status	Start-up Time	Boot up	Configuration page	Operation
Phone Auto Configuration	Running	2022-08-30 16:18:29	☒	Configure	Stop
PBX Panel	Running	2022-08-30 16:18:29	☒		Stop

Click on the “Configure” button on the IP Phone. Auto provisioning will redirect you to the auto configuration system page.

7.10.3 Web

Upload a custom logo, login page background image, and a device name for your IPPBX device.



The image shows a web interface titled "Web Customization". It contains three main sections:

- Device Name:** A text input field containing "IP Phone System".
- Show Logo:** A toggle switch that is currently turned on (blue).
- Use Custom Logo:** A toggle switch that is currently turned off (grey).
- Customize login page background:** A toggle switch that is currently turned off (grey).

Below these settings is a blue "Submit" button.

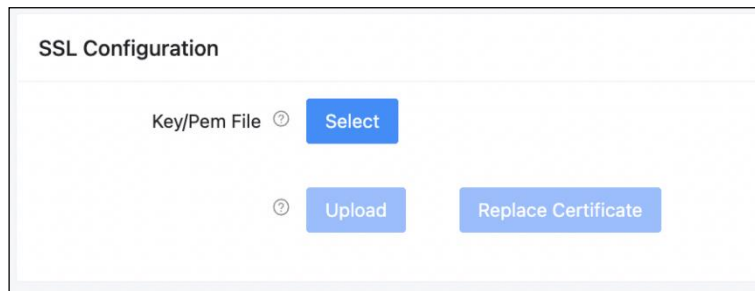
The second section is titled "Custom Logo" and features an "Upload" button. Below this is a large white rectangular area for the logo.

The third section is titled "Customize login page background" and features an "Upload" button. Below this is a large blue rectangular area for the background image.

- **Device's Name:** Customize device name to display on the Home page and the browser's title bar.
- **Show Logo:** Enable/Disable to display the default logo of the system.
- **Use Custom Logo:** Enable/Disable to display the custom logo.
- **Custom Login background:** Enable/Disable to display the uploaded custom background image on login page.

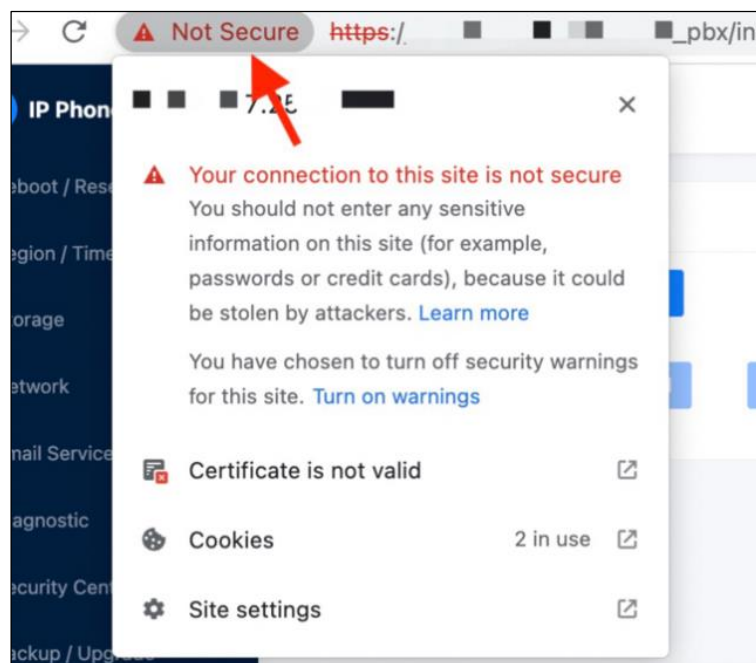
7.10.4 SSL

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. Lastly, click on the “Replace Certificate” button to use the new files to replace the old ones. Operation will fail if the certificate file is incorrect.



The image shows a web interface titled "SSL Configuration". It contains three buttons: "Select", "Upload", and "Replace Certificate". The "Select" button is positioned next to the label "Key/Pem File" with a question mark icon. The "Upload" and "Replace Certificate" buttons are positioned below the "Select" button, with a question mark icon to the left of the "Upload" button.

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



7.10.5 SSH

The IP PBX 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 - +

Submit

Change password

* Password 

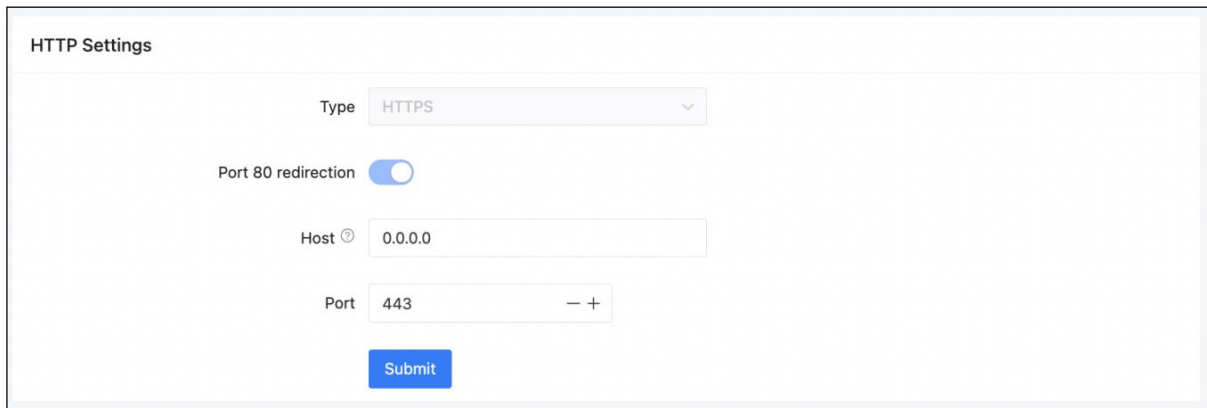
* New Password 

* Confirm Password 

Submit

7.10.6 HTTP

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



The screenshot shows a web interface titled "HTTP Settings". It contains the following elements:

- A "Type" dropdown menu set to "HTTPS".
- A "Port 80 redirection" toggle switch that is turned on (blue).
- A "Host" text input field with a help icon (ⓘ) and the value "0.0.0.0".
- A "Port" spinner control set to "443", with minus and plus buttons for adjustment.
- A blue "Submit" button at the bottom.

- **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 to access the web page.