






Administrator Guide

Yeastar P-Series Appliance Edition

Version: 37.4.0.17

Date: 2021-07-26

-  Support: +86-592-5503301
-  Support: support@yeastar.com
-  <https://www.yeastar.com>

Contents

- About This Guide..... 1
- Getting Started..... 2
 - Log in to PBX Management Portal..... 2
 - Initial Setup Using the Installation Wizard..... 4
 - Change the Password of Super Administrator..... 7
 - Reset the Password of Super Administrator.....8
 - View System Information..... 9
 - Change Web Interface Language.....10
 - Log out of PBX management portal.....10
- Dashboard.....12
 - Dashboard Overview..... 12
- Extension..... 20
 - Extension Overview..... 20
 - Create Extensions.....21
 - Create a SIP Extension.....21
 - Create an FXS Extension.....22
 - Bulk Create SIP Extensions.....23
- Set up Phones..... 26
 - Set up an Analog Phone..... 26
 - Set up a SIP Phone..... 27
 - Set up a Remote SIP Phone..... 27
- Extension Presence.....30
 - Extension Presence Overview.....30
 - Presence Settings..... 31
 - Manually Switch an Extension's Presence..... 34
 - Automatically Switch Presence Based on Business Hours and Holidays..... 35
 - Forward Internal and External Calls to Different Destinations..... 36
 - Ring Office Phone and Mobile Phone Simultaneously..... 37
- Extension Voicemail.....38
 - Set up Extension Voicemail..... 38

Extension Features.....	40
Handle Incoming Calls Based on Caller ID.....	40
Set up Email Notifications for Missed Calls.....	41
Set up Email Notifications for User Password Change.....	41
Allow Multiple Registrations for One Extension Number.....	42
Set up Third-party Integration for Call Popup.....	43
Extension Advanced Settings.....	45
Advanced Settings of SIP Extension.....	45
Advanced Settings of FXS Extension.....	46
Extension Security.....	49
Extension Security Overview.....	49
Restrict Outbound Calls for an Extension.....	51
Restrict Extension Registration Based on User Agent.....	52
Restrict Extension Registration Based on IP Address.....	53
Block Outbound Calls Outside Business Hours.....	53
Limit Call Duration of an Outbound Call.....	54
Limit Outbound Call Frequency of an Extension.....	54
Manage Extensions.....	56
Edit Extensions.....	56
Reset an Extension's User Password.....	56
Export and Import SIP Extensions.....	57
Delete Extensions.....	57
Contacts.....	59
Contacts Overview.....	59
Manage Company Contacts.....	60
Manage Company Phonebooks.....	62
Export and Import Company Contacts.....	64
Grant Company Contacts Permissions.....	65
Identify Callers from Contacts.....	67
Allow Users to Query Contacts on IP Phones.....	69
Extension Group.....	72
Extension Group Overview.....	72
Create an Extension Group.....	73

Manage Extension Groups.....	75
Assign a User Type to a Group Member.....	76
View or Change a Member's User Type in Multiple Groups.....	77
View or Change Permissions for Group Members.....	78
Auto Provisioning.....	81
Auto Provisioning Overview.....	81
Manage Phones.....	82
Auto Provision IP Phones.....	82
Pre-provision IP Phones.....	84
Modify a Provisioned Phone Settings.....	85
Auto Provision Function Keys for Phones.....	86
Reassign an Extension to a Provisioned Phone.....	88
Release an Extension from a Provisioned Phone.....	89
Update Phone Firmware via Auto Provisioning.....	89
Apply a New Template to a Provisioned Phone.....	90
Reboot Provisioned Phones.....	90
Remove Phones from Provisioning List.....	91
Manage Gateways.....	91
Auto Provision Yeastar TA FXS Gateways.....	91
Pre-provision Yeastar TA FXS Gateways.....	94
Modify a Provisioned Gateway Settings.....	96
Reassign an Extension to a Provisioned Gateway.....	97
Release an Extension from a Provisioned Gateway.....	97
Apply a New Template to a Provisioned Gateway.....	98
Reboot Provisioned Gateways.....	98
Remove Gateways from Provisioning List.....	99
Manage Auto Provisioning Tempalte.....	99
View a Default Auto Provisioning Template.....	99
Update a Default Auto Provisioning Template.....	101
Create a Custom Auto Provisioning Template.....	102
Manage Custom Auto Provisioning Template.....	104
Manage Device Firmware.....	105
Manage Device Firmware Files.....	105

Auto Provisioning - Supported Devices.....	106
Auto Provisioning - Variables in Templates.....	112
User Role.....	118
User Roles and Permissions.....	118
Create a User Role.....	119
Assign a Role to a User.....	120
Manage User Roles.....	120
User Role Permissions.....	121
Linkus Server.....	126
Linkus Overview.....	126
Set up Linkus Server with Remote Access Service.....	128
Manually Set up Linkus Server.....	130
Configure Linkus Login Mode.....	134
Enable Linkus Clients for Users.....	135
Configure Linkus Welcome Email.....	136
Send Linkus Welcome Emails.....	136
Enable or Disable Push Notifications for Linkus Mobile Client.....	137
Operator Panel.....	139
Manage Operator Panel.....	139
Trunk.....	141
Trunk Overview.....	141
SIP Trunk.....	144
SIP Trunk Overview.....	144
Create a SIP Trunk.....	145
Manage SIP Trunks.....	151
Export and Import SIP Trunks.....	152
SIP Trunk Settings.....	153
Analog FXO Trunk.....	161
Analog FXO Trunk Overview.....	161
Set up an Analog FXO Trunk.....	162
Release an Analog FXO Trunk.....	163
Analog FXO Trunk Settings.....	163
GSM/3G/4G LTE Trunk.....	167

GSM/3G/4G LTE Trunk Overview.....	167
Set up a GSM/3G/4G LTE Trunk.....	168
GSM/3G/4G LTE Trunk Settings.....	170
ISDN E1/T1 Trunk.....	171
E1/T1/J1 Trunk Overview.....	171
Set up an E1/T1/J1 Trunk.....	172
E1/T1/J1 Trunk Settings.....	174
ISDN BRI Trunk.....	184
BRI Trunk Overview.....	184
Set up a BRI Trunk.....	185
BRI Trunk Settings.....	186
Call Control.....	191
Emergency Calling.....	191
Emergency Calling Overview.....	191
Set up Basic Emergency Calling.....	193
Set up Enhanced Emergency Calling.....	194
Set up a Route for PSAP Callbacks.....	195
Manage Emergency Numbers.....	196
Export and Import Emergency Numbers.....	196
Emergency Notification Contacts.....	197
Business Hours and Holidays.....	200
Overview of Business Hours and Holidays.....	200
Global Business Hours.....	202
Holidays.....	210
Inbound Route.....	214
Inbound Route Overview.....	214
Set up an Inbound Route.....	215
Inbound Route Examples.....	217
Manage Inbound Routes.....	238
Export and Import Inbound Routes.....	238
DID Pattern and Caller ID Pattern.....	239
Outbound Route.....	241
Outbound Route Overview.....	241

Set up an Outbound Route.....	241
Restrict Outbound Calls by PIN Codes.....	244
Manage Outbound Routes.....	244
Export and Import Outbound Routes.....	245
Outbound Dial Pattern.....	246
Dial Pattern Examples.....	250
DID Number.....	251
DID Number Overview.....	251
Configure DID Numbers on a Trunk.....	252
Export and Import Trunk DIDs/DDIs Numbers.....	253
Caller ID.....	254
Caller ID Overview.....	254
Reformat Inbound Caller ID based on a Trunk.....	256
Export and Import Inbound Caller ID Reformatting Rules.....	257
Customize Outbound Caller IDs.....	258
Export and Import Trunk Outbound Caller IDs.....	260
Distinctive Ringtone.....	261
Distinctive Ringtone Overview.....	261
Set Distinctive Ringtones for Internal Calls.....	262
Set Distinctive Ringtones for External Calls.....	264
Set Distinctive Ringtones for Queue Calls.....	265
Set Distinctive Ringtones for Ring Group Calls.....	267
Set Distinctive Ringtones for IVR Calls.....	269
Distinctive Caller ID Name.....	270
Distinctive Caller ID Name Overview.....	270
Enable or Disable Distinctive Caller ID Name.....	272
Call Center.....	274
Call Center Overview.....	274
Call Center Setup.....	275
Set up Queue Managers.....	275
Customize Queue Notification.....	275
Grant Queue Panel Permissions.....	276
Set up Service Level Agreement (SLA).....	277

Call Center Report.....	278
Call Center Reports Overview.....	278
Queue Performance reports.....	278
Agent Performance Report.....	282
Call Features.....	287
Voicemail.....	287
Voicemail Overview.....	287
Group Voicemail.....	289
Send and Receive Voicemail Messages.....	293
Manage Voicemail Messages.....	296
Voicemail Security.....	302
Voicemail Greetings.....	304
Voicemail Notifications.....	310
Custom Voicemail Experience.....	313
Global Voicemail Settings.....	316
Voicemail Menu Options.....	317
Voicemail Capacity and Limitations.....	318
IVR.....	319
Interactive Voice Response (IVR) Overview.....	319
Set up an IVR.....	320
Set up IVR Prompts.....	321
Allow Callers to Dial Extensions via IVR.....	323
Allow Callers to Dial by Name via IVR.....	324
Allow Callers to Dial Outbound Calls via IVR.....	325
Forward Incoming Calls to an External Number via IVR.....	325
IVR Configuration Example.....	326
Call Recording.....	330
Call Recording Overview.....	330
Set up Call Recording.....	331
Set up Recording Prompts.....	332
Pause or Resume Call Recording.....	333
Monitor Call Recording Status on an IP phone.....	334
Manage Call Recording Files.....	335

Auto Clean up Recording Files.....	337
Grant Manage Permission of Recording Files.....	337
Restrict Users from Viewing Recording Files.....	338
Ring Group.....	339
Ring Group Overview.....	339
Create a Ring Group.....	340
Manage Ring Groups.....	340
Call Queue.....	341
Call Queue Overview.....	341
Create a Queue.....	342
Manage Call Queues.....	344
Manage Agent Status by Dialing a Feature Code.....	345
Monitor and Switch Agent Status on an IP Phone.....	346
Queue Preferences.....	348
Feature Code.....	351
Configure Feature Codes.....	351
Feature Code Reference.....	351
Conference.....	354
Conference Overview.....	354
Create a Conference Room.....	354
Join a Conference Call.....	355
Invite Users to a Conference Call.....	356
Manage Conference Rooms.....	356
Conference Voice Menu.....	357
Speed Dial.....	357
Speed Dial Overview.....	357
Set up Speed Dial Prefix.....	358
Add a Speed Dial Number.....	358
Manage Speed Dial Numbers.....	359
Export and Import Speed Dial Numbers.....	359
Call Transfer.....	360
Call Transfer Overview.....	360
Set up Call Transfer.....	361

Perform an Attended Transfer.....	362
Perform a Blind Transfer.....	362
Call Pickup.....	363
Call Pickup Overview.....	363
Pick up a Call for a Group Member.....	363
Pick up a Call for a Specific Extension.....	364
Call Parking.....	366
Call Parking Overview.....	366
Directed Call Parking.....	367
Call Parking.....	368
Set up Parking Timeout Destination.....	368
Set up Parking Number.....	369
Monitor a Parking Number on an IP Phone.....	369
Fax.....	371
Fax Overview.....	371
Send Faxes from an Analog Fax Machine.....	373
Receive Faxes through a Dedicated Trunk.....	374
Receive Faxes and Calls through the Same Line.....	376
Receive Faxes by Email.....	378
Set up Fax over IP (FoIP).....	379
Paging/Intercom.....	380
Overview of Paging and Intercom.....	380
Paging/Intercom Group.....	381
Scheduled Paging/Intercom Call.....	389
PIN List.....	390
Add a PIN List.....	390
PBX System.....	392
System Preferences.....	392
Voice Prompt.....	394
Voice Prompt Overview.....	394
System Prompt.....	396
Music on Hold.....	397
Custom Prompt.....	400

Convert Audio Files.....	402
Audio Files Requirements.....	405
SIP Settings.....	406
Jitter Buffer.....	412
Jitter Buffer Overview.....	412
Configure Jitter Buffer.....	412
Network.....	413
Basic Network.....	413
Web Server.....	423
Service Ports.....	425
Yeastar FQDN.....	426
Public IP and Ports.....	427
Static Route.....	435
DHCP Server.....	441
Date and Time.....	442
Change System Time Manually.....	442
Synchronize System Time with an NTP Server.....	442
Email Server.....	443
Email Server Overview.....	443
Set up Yeastar SMTP Server as an Email Server.....	444
Set up Gmail as an Email Server.....	445
Set up Outlook as an Email Server.....	448
Customize Email Templates.....	450
Email Sent Logs.....	450
Storage.....	451
Storage Overview.....	451
Set up a USB Flash Drive.....	453
Set up a Hard Disk Drive.....	454
Set up an SD Card.....	456
Add a Windows Network Drive.....	457
Add a Mac Network Drive.....	463
Manage Storage Locations.....	468
Auto Cleanup Settings.....	468

Event Notification.....	473
Event Notification Overview.....	473
Configure Event Notifications.....	477
Manage Notification Contacts.....	478
Manage Event Logs.....	479
Security.....	481
Security Overview.....	481
Static Defense.....	483
Add a Static Defense Rule.....	483
Manage Static Defense Rules.....	484
Export and Import Static Defense Rules.....	484
Auto Defense.....	485
Add an Auto Defense Rule.....	485
Manage Auto defense Rules.....	486
Export and Import Auto Defense Rules.....	487
Blocked IPs.....	488
Manage Blocked IP Addresses.....	488
Outbound Call Frequency Restriction.....	488
Add an 'Outbound Call Frequency Restriction' Rule.....	488
Manage 'Outbound Call Frequency Restriction' Rules.....	489
Export and Import 'Outbound Call Frequency Restriction' Rules.....	489
Console/SSH Access.....	490
Access the System via SSH.....	490
Certificates.....	493
Upload TLS certificates to the PBX.....	493
Upload HTTPS Certificates to the PBX.....	494
Delete Certificates.....	495
Allowed Country IPs.....	495
Restrict Specific Countries or Regions from Accessing Yeastar P-Series PBX System.....	495
Check Allowed Country/Region IP.....	496
Allowed Country Codes.....	497
Restrict International Calls to Specific Countries or Regions.....	497

Block Outbound International Calls.....	499
Maintenance.....	501
Upgrade.....	501
Check for Available Firmware Updates.....	501
Schedule Automatic Firmware Upgrade.....	502
Manually Upgrade PBX Firmware.....	503
Backup and Restore.....	504
Overview of Backup and Restore.....	504
Create an On-Demand Backup.....	505
Set up an Automatic Backup Schedule.....	507
Restore Your System from a Backup.....	508
Restore Another System from a Backup.....	509
Reboot.....	510
Reboot Yeastar P-Series PBX System on Web Interface.....	510
Schedule Automatic Reboot.....	511
Reset.....	511
Reset the System on Web Interface.....	511
Operation Logs.....	512
Operation Logs Overview.....	512
Manage Operation Logs.....	514
Troubleshooting.....	514
Capture Network Packet.....	514
Use IP Ping Tool to Diagnose Network Issues.....	515
Use Traceroute Tool to Diagnose Network Issues.....	516
Troubleshoot and Monitor Analog Ports.....	519
System Logs.....	520
System Logs Overview.....	520
Configure Log Level.....	521
Manage System Logs.....	522
CDR and Reports.....	523
CDR.....	523
Call Detail Record (CDR) Overview.....	523
Manage CDR.....	524

Call Report.....	526
Call Reports Overview.....	526
Call Reports.....	527
Scheduled Reports.....	534
Customize Email Template for Scheduled Reports.....	537
Integration.....	539
Speech to Text (STT).....	539
Speech to Text (STT) Overview.....	539
Integrate with Speech to Text (STT) API.....	540
Disconnect Speech to Text (STT) API Integration.....	546
Asterisk Manager Interface (AMI) Overview.....	546
Database Grant.....	547
Database Grant Overview.....	547
Get CDR Data from Database of Yeastar P-Series PBX System.....	548
cdr Table in the PBX Database.....	551
Refereneces.....	554
Import and Export Parameters Overview.....	554
Extension Parameters.....	554
Contacts Parameters.....	566
Speed Dial Number Parameters.....	567
Emergency Number Parameters.....	568
Trunk Parameters.....	569
Trunk DID/DDI Parameters.....	577
Trunk Outbound Caller ID Parameters.....	578
'Inbound Caller ID Reformatting Rule' Parameters.....	580
Inbound Route Parameters.....	580
Outbound Route Parameters.....	586
Static Defense Rule Parameters.....	589
Auto Defense Rule Parameters.....	591
'Outbound Call Frequency Restriction Rule' Parameters.....	593

About This Guide

In this guide, we describe every detail on the functionality and configuration of the Yeastar P-Series PBX System.

Audience

This guide is for administrators who need to prepare for, configure, and operate the PBX system. We begin by assuming that you are familiar with networking and other IT disciplines.

Getting Started

Log in to PBX Management Portal

Yeastar P-Series PBX System provides a web management portal that allows you to quickly set up and manage the system. This topic describes how to log in to PBX management portal.

Prerequisites

- You have connected the network cable.

Select either of the following two methods to connect network cable.

- Use a network cable to connect the LAN port of the PBX to the network adapter port of the PC.
- Use a network cable to connect the LAN port of the PBX to a switch or a router, and also connect your PC to the switch or router.
- An operation and maintenance terminal (a PC) is available. The PC must meet the following requirements:
 - Have a web browser installed and Chrome web browser is recommended.
 - Support the resolution of 1366 x 768 or higher.
- You have set the IP address of your PC.

The IP address of the PC must be on the same network segment as that of the PBX and cannot conflict with IP addresses of other devices.



Note:

- The default IP address of Yeastar P-Series PBX System is 192.168.5.150, and the default gateway address is 192.168.5.1.
- If you fail to access the PBX management portal, contact your network administrator to check if your PC can communicate with the IP address 192.168.5.150.

Procedure

1. Open the web browser, enter the IP address of the PBX (default: 192.168.5.150) in the address bar, and press Enter.

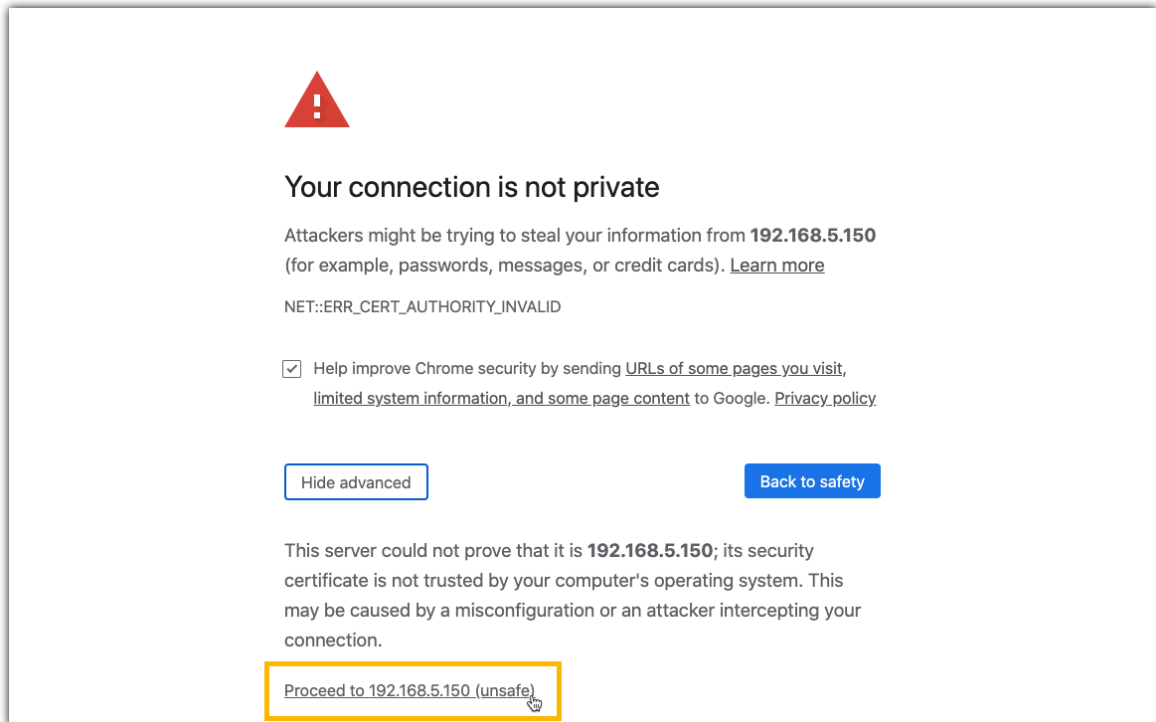


Note:

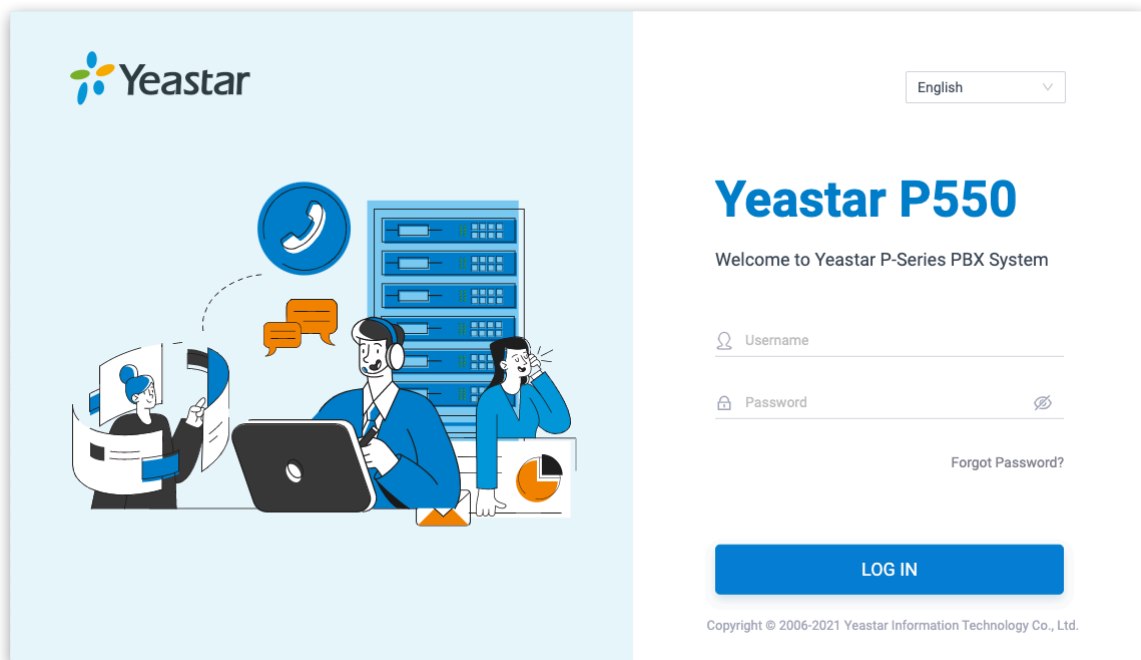
If it is your first time to access the system, you will be redirected to the Installation Wizard.

For more information of Installation Wizard, see [Initial Setup Using the Installation Wizard](#).

2. If a warning appears to remind you that the page is not secure, ignore the warning on the web page, expand the Advanced tab, and proceed to the PBX web.



3. Enter the administrator username and password, click LOG IN.
 - Username: The username of administrator account that you have configured in the Installation Wizard.
 - Password: The password of the administrator account.



Initial Setup Using the Installation Wizard

When you access the PBX management portal for the first time, you need to finish initial configurations for the system using the Installation Wizard.

Prerequisites

You have accessed the PBX management portal and entered the Installation Wizard.

For more information about how to access the PBX web interface, see [Log in to PBX Management Portal](#).



Warning:

The Installation Wizard only appears when you first configure the system with factory settings.

Procedure

- [Step1. Configure the system network.](#)
- [Step2. Set up super administrator account](#)
- [Step3. Configure the system time](#)
- [Step4. Localize and customize the system](#)
- [Step5. Check and confirm the configurations](#)

Step1. Configure the system network

Set the Ethernet mode and related configuration of corresponding Ethernet interface.

1. In the Basic section, select the Ethernet mode and default interface.
 - Ethernet Mode: Select an Ethernet mode.
 - Single: Only LAN interface is used for connection, WAN interface is disabled.
 - Bridge: LAN interface is used for connection, WAN interface is used as bridge for other devices' connection.
 - Dual: Both LAN interface and WAN interface are used for connection.



Note:

Dual Ethernet mode is typically for the scenario that the Internet Telephony Service Provider (ITSP) offers a dedicated networking for VoIP communication.

- Default Interface: Optional. Select a default interface if the system is in dual Ethernet mode.
2. In the LAN section, enter the network information for the LAN interface of the PBX.
 3. Optional: In the WAN section, enter the network information for the WAN interface of the PBX.

4. Click Next.

A pop-up window appears and displays the information of network detection.

For more information of network settings, see [Basic Network Overview](#).

Step2. Set up super administrator account

1. In the Basic section, enter the information of the super administrator account.



Note:

- Do NOT forget the username and password of the super administrator account, or you need to reset your system to reconfigure the account and log in to the PBX.
- The super administrator has access to all features on the system, and the super administrator can assign administrator role to users. For more information, see [User Roles and Permissions](#).

- Username: Specify the username that is used to log in to PBX management portal.
- Password: Specify the password that is used to log in to PBX management portal.
- Repeat the password: Repeat the password to confirm.
- Email Address: Enter the email address of the super administrator.

The email address can be used to receive system notifications and reset web login password.

- Mobile Number: Enter the mobile number that can be used to receive system notifications.
- Prefix: Optional. Enter the prefix according to the dial pattern of the outbound route, so that the system can successfully send calls to the mobile number.

For more information of the prefix setting, see [Prefix and Dial Pattern](#).

2. In the Event Notifications section, configure event notifications for the super administrator.

- Send Event Notification to PBX Administrator: Decide whether to enable notifications for the super administrator or not.
- Contact Name: Enter the name of the super administrator.



Note:

This name helps you identify the super administrator from the Notification Contacts list.


- Notification Level: System notifications are divided into different levels according to importance. You can select notification levels to filter and receive the relevant notifications.
- Notification Method: Select method(s) to receive notifications.

For more information of event notifications, see [Event Notification Overview](#).

3. Click Next.

Step3. Configure the system time

1. In the Date and Time section, configure the time zone and daylight saving time, and set up the date and time manually or synchronize with an NTP server.


 Note:

To synchronize system time with an NTP server, make sure that the PBX can access the Internet.

2. In the Display Format section, select the display format for date and time.
3. Click Next.


Step4. Localize and customize the system

1. In the System Prompt Language section, select the radio button beside a system prompt to set it as the default system prompt.

 Note:

Click [Download Online Prompts](#) to download more prompts.

2. In the Other Settings section, adjust the following settings for your local installation.
 - Notification Email Language: Select which language of email contents to be received.
 - Device Name: Specify a name for the PBX system.
 - Name Display Format: Select the display format for Extension User's Name and Contact Name.
 - Tone Region: Select your country/region or the nearest neighboring country/region to enable the default dial tone, busy tone, ring tone for your region.
 - Enable Allowed Country/Region Code Dialing Protection: To restrict users from making international calls, enable this option. When enabled, users can not make international calls to any countries or regions.

 Note:


To allow users to make international calls to specific countries or regions, you need to grant permission to desired users, and set the allowed countries or regions. For more information, see [Restrict International Calls to Specific Countries or Regions](#).

- International Dialing Code: Enter the prefix of international call according to your country.

When a user tries to call a number starting with the prefix, the PBX's outbound route will identify this call as an international call.

3. Click Next to see the summary.

Step5. Check and confirm the configurations

1. Check the all the configured settings on the Summary page.
2. To edit the configurations of a specific step, click  beside the step title.
3. To edit the configurations of the previous step, click Re-configure.
4. If all the configurations are confirmed, click Reboot to take effect.

Result

All the configurations take effect after the system reboots.

You need to access the new IP address of the PBX and log in to PBX management portal by the super administrator username and password.

Note:

The IP address of your PC must be on the same network segment as that of the PBX, or you cannot access the PBX.

Change the Password of Super Administrator

If you know the current password of super administrator, you can log in to the PBX management portal and follow the steps to change the super administrator's password.


Background information

The username and password of super administrator are configured in [Installation Wizard](#).

Important:

- The username of super administrator cannot be changed unless you reset the system.
- If you forget the password of super administrator, you can reset the password. For more information, see [Reset the Password of Super Administrator](#)

Procedure

1. Log in to PBX management portal.
2. At the top-right corner of the web page, click  and select Change Password.
3. On the pop-up window, enter the old password and new password.
4. Click Save.

Result

The password is reset, you will be logged out of the web page automatically. To log in to PBX management portal, enter the new password.

Reset the Password of Super Administrator

As a super administrator, you can reset your web login password if you forget the password.

Prerequisites

- You need to provide both username and email address, or you cannot reset your password.

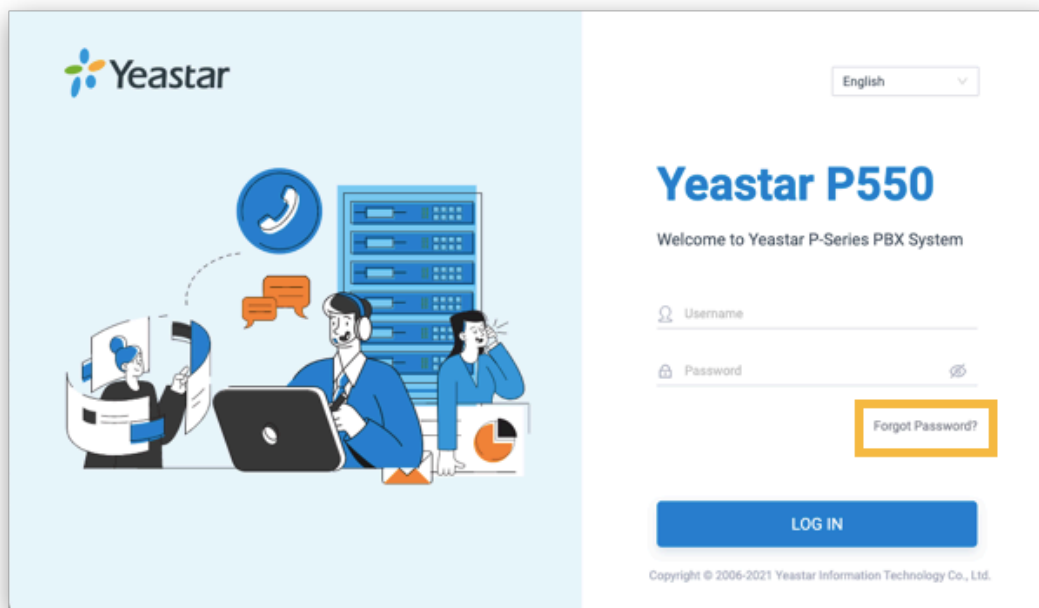
! Important:

If you forget the username of super administrator, you need to reset the system to re-configure a new username.

- For P-Series Basic Plan, you can only reset your password in the local network of the PBX system.

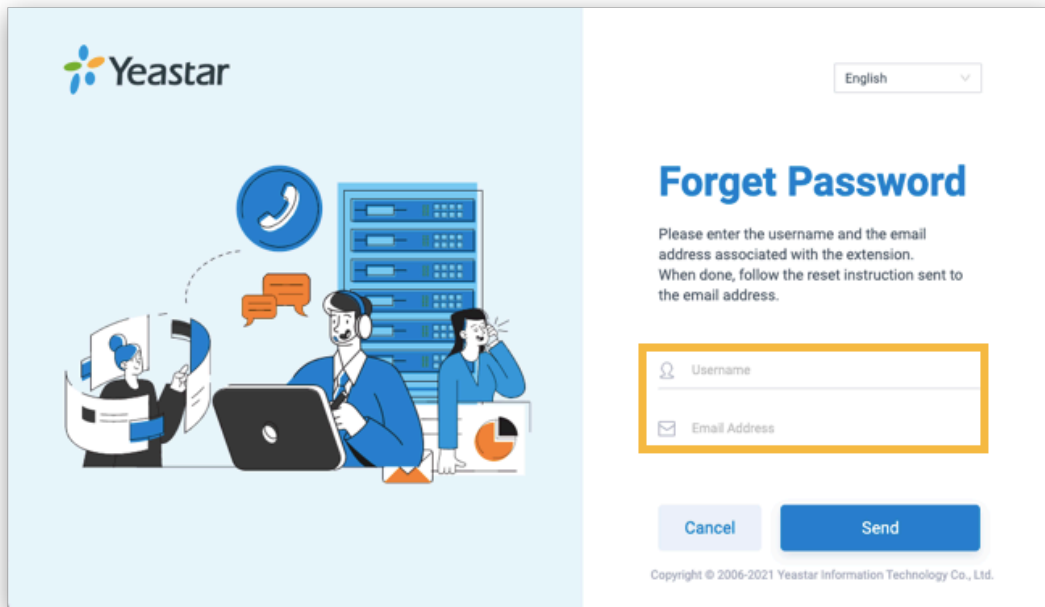
Procedure

1. Access the PBX web login page, click Forgot Password? to enter the Forget Password page.



2. On the Forget Password page, enter the following information:


- Username: The username of super administrator.
- Email Address: The email address that is associated with the super administrator.



3. Click Send.

A password reset email is sent to super administrator's email address.

4. Check the password reset email, and click the link provided in the email to enter the Reset Password page.

 Note:

This link is valid for 30 minutes and can only be used once.

5. On the Reset Password page, enter your new password twice, and click Save.

Result

The password of super administrator is changed. You need to log in to PBX management portal by the new password next time.

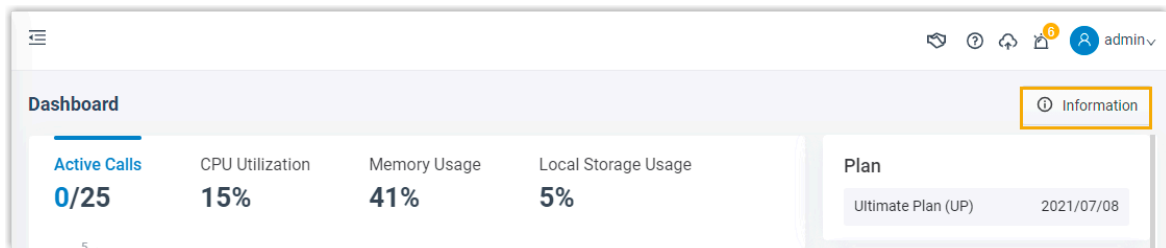
View System Information

This topic describes how to view a summary of information about your system hardware, firmware and network.

Procedure

1. Log in to PBX management portal, go to Dashboard.

2. At the top-right corner of Dashboard, click Information.




The following information is displayed:

- Network
- Device Name
- Product Model
- Serial Number
- Hardware Version
- Firmware Version
- System Time
- Uptime
- Maximum Extensions
- Maximum Concurrent Calls

Change Web Interface Language

The default web interface language of Yeastar P-Series PBX System is English, the interface can be easily switched to the language of your choice.

Procedure


1. Log in to PBX management portal.
2. At the top-right corner of the web page, click .
3. Select Language and select your desired language.

The web interface is switched to the selected language immediately.

Log out of PBX management portal

When you're ready to quit the Yeastar P-Series PBX System, simply close the web page or follow the steps below to log out of the PBX management portal.

Procedure

1. At the top-right corner of the web page, click .

2. Select Log out.

Related information

[Change Automatic Logout Time](#)

Dashboard

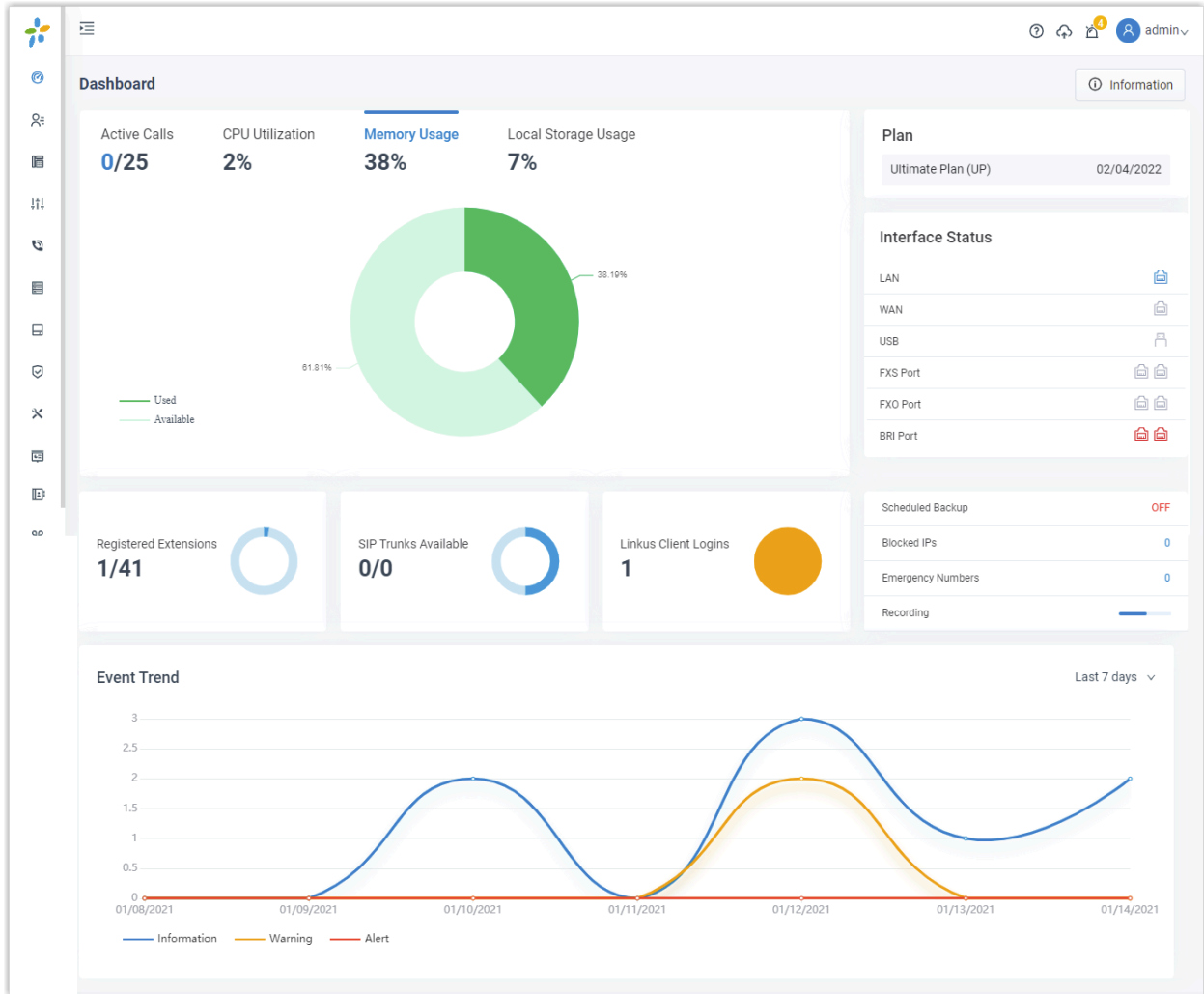
Dashboard Overview

Yeastar P-Series PBX System Dashboard gives you a historical and real-time view of what is happening on the PBX. This topic describes all the widgets on the Dashboard.

Yeastar P-Series PBX System Dashboard provides 6 widgets to help you monitor system performance in real time, and allows you to quickly access specific PBX features by simple click on headings.

The supported 6 widgets are as follows:

- System performance
- System information
- Plan
- System interface
- System status
- Event trend



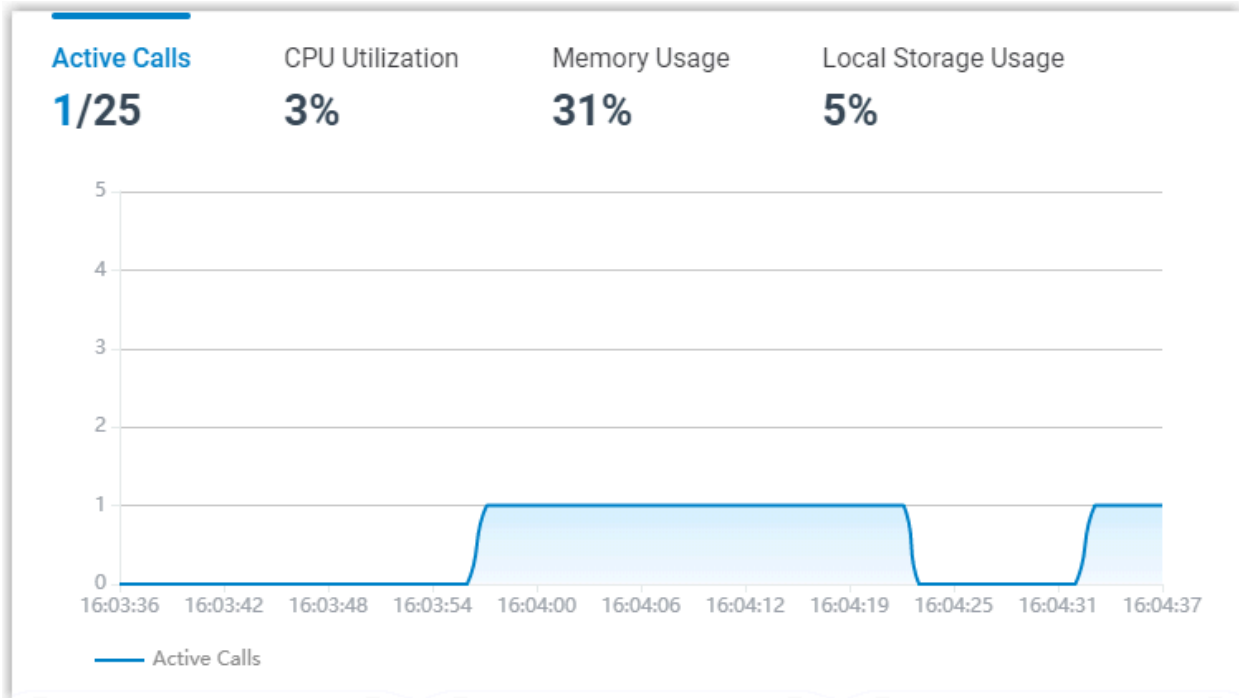
1. [System performance](#)
2. [System information](#)
3. [Plan](#)
4. [System interface](#)
5. [System status](#)
6. [Event trend](#)

1. [System performance](#)
2. [System information](#)
3. [Plan](#)
4. [System interface](#)
5. [System status](#)
6. [Event trend](#)

System performance

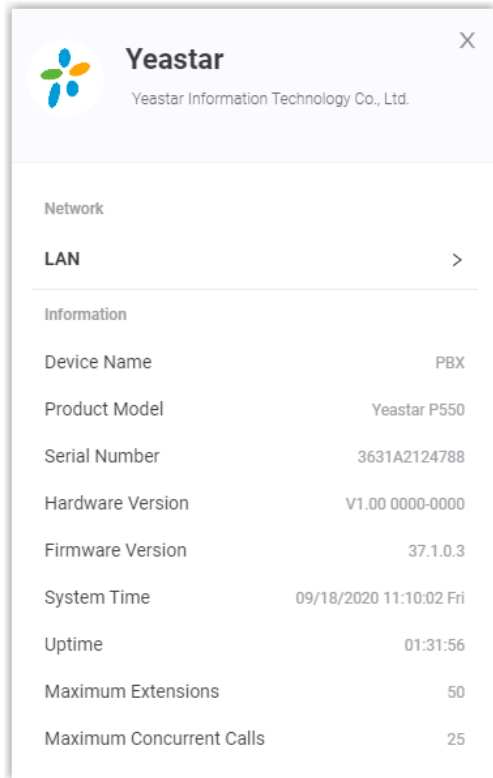
System performance displays the following information:

- Active Calls: The real-time and the supported concurrent calls.
- CPU Utilization: The PBX's CPU usage.
- Memory Usage: The PBX's memory usage.
- Local Storage Usage: Usage of the PBX's local storage.



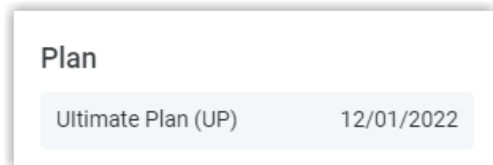
System information

Click Information at the top-right corner. System information displays the PBX's network information and basic information.



Plan

Plan displays your subscribed plan and expiration date.



If PBX loses connection to Yeastar License Activation Server, the following status may be displayed:

- Connecting: The system is trying to connect to the License Activation Server.
- Abnormal: The system failed to connect to the License Activation Server.

System interface

System interface displays connection status of interfaces on Yeastar P-Series PBX System.

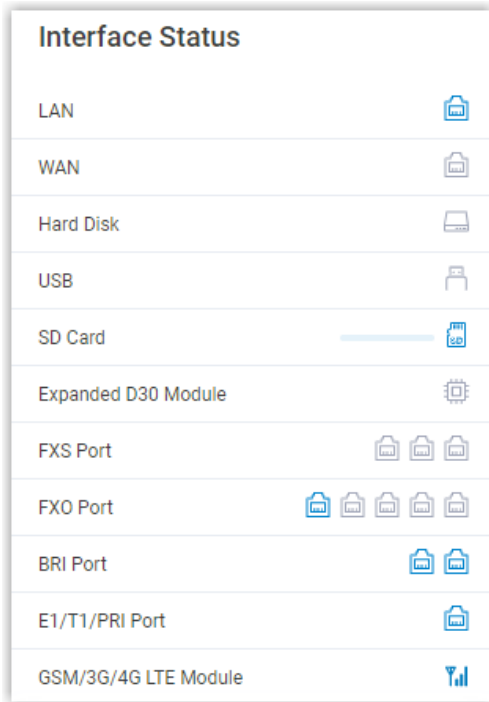


Table 1.













Interface	Description
LAN	<ul style="list-style-type: none"> : Connected. : Disconnected.
WAN	<ul style="list-style-type: none"> : Connected. : Disconnected.
Hard Disk	<ul style="list-style-type: none"> : Connected. : Not inserted. : Connected, but the hard disk is "Read Only" or encounters format error. : Connected, but the hard disk is formatting. <div data-bbox="592 1570 1386 1665" style="border: 1px solid #00aaff; padding: 5px; margin-top: 10px;"> <p> Note: Hard Disk is ONLY supported on P560 and P570.</p> </div>
USB	<ul style="list-style-type: none"> : Connected. : Not inserted. : Connected, but the USB flash drive is "Read Only" or encounters format error.

Table 1. (continued)






























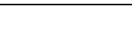
Interface	Description
	<ul style="list-style-type: none"> : Connected, but the USB flash drive is formatting.
SD Card	<ul style="list-style-type: none"> : Connected. : Not inserted. : Connected, but the SD card is "Read Only" or encounters format error. : Connected, but the SD card is formatting. <div data-bbox="516 674 1385 762" style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: SD card is ONLY supported on P560 and P570.</p> </div>
Expanded D30 Module	<ul style="list-style-type: none"> : Connected. : Not connected. : Connected, but the D30 module is abnormal. <div data-bbox="597 976 1385 1064" style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: D30 module is ONLY supported on P560 and P570.</p> </div>
FXS port	<ul style="list-style-type: none"> : An extension number is assigned to the FXS port. : No extension number is assigned to the FXS port.
FXO port	<ul style="list-style-type: none"> : A PSTN line is connected to the FXO port. : No PSTN line is connected to the FXO port. : Abnormal. : Busy.
BRI port	<ul style="list-style-type: none"> : Available. : Unavailable. : Abnormal.
E1/T1/PRI port	<ul style="list-style-type: none"> : Available. : Unavailable. : Abnormal.
GSM/3G/4G LTE module	<ul style="list-style-type: none"> : Abnormal.

Table 1. (continued)

Interface	Description
	<ul style="list-style-type: none"> • : No SIM card is inserted. • : The module is powered off. • : No signal. • : PIN/PUK error. • : Network registration failure. • : Different signal strength when the trunk is busy. • : Different signal strength when the trunk is idle.

System status

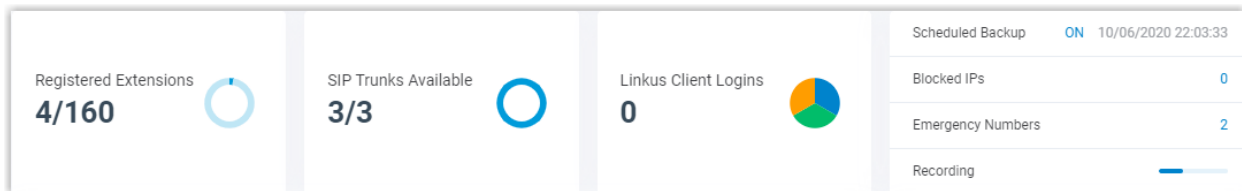
System status displays the following information:

- Registered Extensions: The number of registered extensions and created extensions.
- SIP Trunks Available: The number of available trunks and created trunks.
- Linkus Client Logins: The number of Linkus clients where users has logged.
- Scheduled Backup: Whether scheduled backup feature is enabled or not. If enabled, the system displays the last time when a backup file was created.
- Blocked IPs: Display the following information:
 - The number of IP address and account that were blocked by the PBX.
 - The last time when an IP address or an account was blocked by the PBX.
- Emergency Numbers: The number of created emergency numbers.
- Recording: How much storage space for recording has been used.



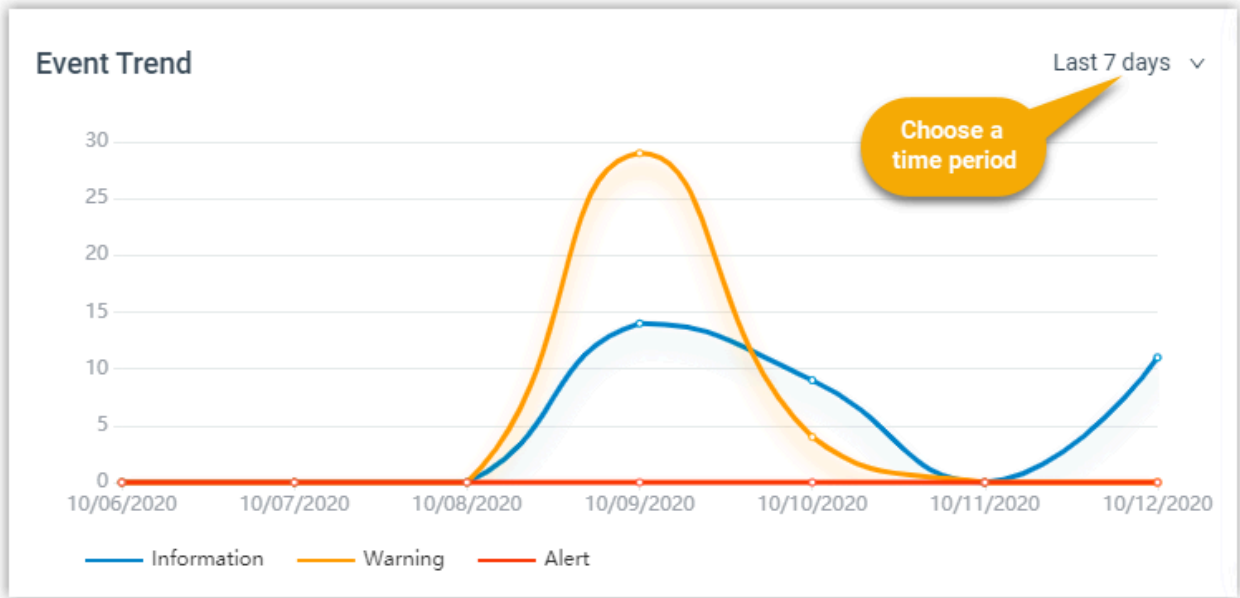
Note:

If it displays "Undefined Storage Location", it means that you haven't specified a storage location for recording files.



Event trend

Event trend provides historical and real-time view of system events. You can track frequency of events that were triggered during the last 7 days, 15 days, or 30 days.



Extension

Extension Overview

An extension is a short internal number. Extensions allow users to make and receive calls. You can assign extensions to every employee in your organization.

Extension types

Yeastar P-Series PBX System supports two extension types:

SIP extension

A SIP extension is based on SIP protocol.

To use a SIP extension to make or receive calls, you need to register the extension on an IP phone or a softphone.

For more information, see [Create a SIP Extension](#) and [Set up a SIP Phone](#).

FXS extension

An FXS extension is associated with an analog phone or a fax machine.

To use an FXS extension to make or receive calls, you need to connect an analog phone or a fax machine to PBX's FXS port, and assign an extension number to the analog phone or fax machine.


For more information, see [Create an FXS Extension](#) and [Set up an Analog Phone](#).

Online status

Online status allows you to view status of phone endpoints and Linkus clients.




• Phone endpoints

-  indicates that the SIP extension is registered and ready for use.

Hover your mouse over  to view the IP addresses of SIP phones where the extension is registered.

-  indicates that the FXS extension is assigned to an FXS port.

• Linkus clients

-  indicates that Linkus Desktop Client is ready for use.
-  indicates that Linkus Mobile Client is ready for use.
-  indicates that Linkus Web Client is ready for use.


Create Extensions

Create a SIP Extension

This topic describes how to create a SIP extension and configure relevant settings.


Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, click Add and select Add.
2. In the Basic section, select SIP Extension from the drop-down list of Extension Type.
3. In the User Information section, configure user information as follows:
 - First Name: Enter the user's first name.
 - Last Name: Enter the user's last name.
 - Email Address: Enter the user's email address. The user can reset login password of PBX web management portal and Linkus clients login password, receive voicemail messages, or PBX notifications via the email address.

 Note:


An email address is exclusive to a user.

- Mobile Number: Enter the user's mobile number. The user can receive calls or PBX notifications on this mobile number.
- User Password: Enter a user password. The user can use the password to log in to Linkus clients.

 Note:

The password is randomly generated by default. To change user password, a minimum of 10 characters with number, upper case, and lower case are required.


- User Role: Assign a role to the user to determine whether the user can manage specific PBX features.
The default value is None, which means that the user can not manage specific PBX features.

 Note:

The system has default user roles with [pre-configured permissions](#). You can also [Create a User Role](#).

4. In the Extension Information section, configure extension information as follows:
 - Extension Number: Enter an extension number.
 - Caller ID: Enter a caller ID number. The caller ID will be displayed on the callee's device.
 - Registration Name: Enter a name that is used to register the SIP extension. The default registration name is randomly generated.


- **Registration Password:** Enter a password that is used to register the SIP extension. The default registration password is randomly generated.

 **Note:**

For security reasons, we recommend that you set a strong password.

- **IP Phone Concurrent Registrations:** Select a value from the drop-down list.

This option defines how many SIP endpoints are allowed to register with the extension.

 **Note:**

- The maximum number of concurrent registration is 3.
- Concurrent Registration setting only limits the registration number of non-Linkus SIP endpoints. The registration number of Linkus clients is not counted.

5. Optional: Click other tabs to configure other settings according to your needs.
6. Click Save and Apply.

Result

The SIP extension is created.

What to do next

- To set up a SIP phone in your local network, see [Set up a SIP Phone](#).
- To set up a SIP phone remotely, see [Set up a Remote SIP Phone](#).

Create an FXS Extension

This topic describes how to create an FXS extension and configure relevant settings.


Prerequisites

You have installed an S2 module or S0 module on the PBX.

Procedure


1. Log in to PBX management portal, go to Extension and Trunk > Extension, click Add and select Add.
2. In the Basic section, configure basic settings of the extension as follows:
 - a. In the Extension Type drop-down list, select FXS Extension.
 - b. In the FXS Port drop-down list, select an FXS port.
3. In the User Information section, configure user information as follows:
 - **First Name:** Enter the user's first name.
 - **Last Name:** Enter the user's last name.

- **Email Address:** Enter the user's email address. The user can reset login password of PBX web management portal and Linkus clients login password, receive voicemail messages, or PBX notifications via the email address.

 **Note:**


An email address is exclusive to a user.

- **Mobile Number:** Enter the user's mobile number. The user can receive calls or PBX notifications on this mobile number.
- **User Password:** Enter a user password. The user can use the password to log in to Linkus clients.

 **Note:**

The password is randomly generated by default. To change user password, a minimum of 10 characters with number, upper case, and lower case are required.

- **User Role:** Assign a role to the user to determine whether the user can manage specific PBX features.
The default value is None, which means that the user can not manage specific PBX features.

 **Note:**

The system has default user roles with [pre-configured permissions](#). You can also [Create a User Role](#).

4. In the Extension Information section, configure extension information as follows:
 - **Extension Number:** Enter an extension number.
 - **Caller ID:** Enter a caller ID number. The caller ID will be displayed on the callee's device.
5. Optional: Click other tabs to configure other settings according to your needs.
6. Click Save and Apply.

Result

The FXS extension is created.

What to do next

[Connect an analog phone to the FXS port.](#)


Bulk Create SIP Extensions

This topic describes how to bulk create SIP extensions.

Procedure


1. Log in to PBX management portal, go to Extension and Trunk > Extension, click Add and select Bulk Add.
2. Configure basic settings for the extensions as follows.
 - a. In the Basic section, select SIP Extension from the drop-down list of Extension Type.
 - b. In the User Information section, configure user information as follows:

- Start Extension Number: Enter the start extension number.
The system will bulk create extensions starting with the extension number.
- Create Number: Enter the number of extensions that will be created.

 Note:


Only an integer ranging from 1 to 999 is allowed.

- User Password: Choose a password type.

 Important:

Set a password that contains a minimum of 10 characters with number, upper case, and lower case.


- Generate Randomly: Password will be randomly generated for each extension.
- Prefix + Extension Number: If you choose the type, enter a prefix in the Password Prefix field.
- Extension Number + Suffix: If you choose the type, enter a suffix in the Password Suffix field.
- Fixed Password: If you choose the type, enter a fixed password in the Fixed Password field.
- User Role: Assign a role to the extensions to determine whether these users can manage specific PBX features.
The default value is None, which means that these users can not manage specific PBX features.

 Note:


The system has default user roles with [pre-configured permissions](#). You can also [Create a User Role](#).

- c. In the Extension Information section, configure extension registration information as follows.
 - Registration Name: Choose how to configure registration name.
 - Generate Randomly: Registration name will be randomly generated for each extension.
 - Prefix + Extension Number: If you choose the type, enter a prefix in the Name Prefix field.


- Extension Number + Suffix: If you choose the type, enter a suffix in the Name Suffix field.
- Fixed Name: If you choose the type, enter a fixed name in the Fixed Name field.
- Extension Number: If you choose the type, extension number will be the registration name of each extension.
- Registration Password: Choose a password type.

 Note:

For security reasons, we recommend that you set a strong password.

If you set weak passwords for these extensions,  will be displayed in front of these extensions on Extension page.

- Generate Randomly: Password will be randomly generated for each extension.
- Prefix + Extension Number: If you choose the type, enter a prefix in the Password Prefix field.
- Extension Number + Suffix: If you choose the type, enter a suffix in the Password Suffix field.
- Fixed Password: If you choose the type, enter a fixed password in the Fixed Password field.
- IP Phone Concurrent Registrations: Select a value from the drop-down list. This option defines how many SIP phones are allowed to register with each extension.

 Note:

- The maximum number of concurrent registration is 3.
- Concurrent Registration setting only limits the registration number of non-Linkus SIP endpoints. The registration number of Linkus clients is not counted.

3. Optional: Click other tabs to configure other settings for the extensions.

- Presence: Configure presence settings.
- Voicemail: Turn on Enable Voicemail, choose a password type from the drop-down list of Voicemail PIN Authentication.

 Tip:

Configure [voicemail notifications and play options](#) according to your needs.

- Generate Randomly: A PIN code will be randomly generated for each extension.
- Prefix + Extension Number: If you choose the type, enter a prefix in the PIN Prefix field.
- Extension Number + Suffix: If you choose the type, enter a suffix in the PIN Suffix field.

- Fixed Password: If you choose the type, enter a PIN code in the Fixed PIN Code field.
- Extension Number: If you choose the type, extension number will be set to PIN code for each extension.
- Disabled: No PIN code is required when accessing voicemails.
- Features: Configure email notifications, time-conditional presence auto switch, call handling rules, call recording, etc.
- Advanced: Configure advanced settings.
- Security: Configure SIP security settings and call restriction settings.
- Linkus Clients: Enable Linkus clients for the extensions.
- Function Keys: Provision function keys.

When the extensions are bound with phones through auto provisioning, the function keys associated with the extensions will be applied to phones.

4. Click Save and Apply.

Result

The extensions are created. The system prompts you the number of created extensions, and the associated extension numbers.

What to do next

- To set up a SIP phone in your local network, see [Set up a SIP Phone](#).
- To set up a SIP phone remotely, see [Set up a Remote SIP Phone](#).

Set up Phones

Set up an Analog Phone

This topic describes how to set up an analog phone.

Prerequisites

- You have [created an FXS extension](#).
- You have prepared an analog phone and a RJ11 cable.

Procedure

1. Connect one end of the RJ11 cable to the analog phone; connect the other end to the FXS port to which you have assigned an FXS extension.
2. Check indicator of the FXS port that is connected to the analog phone.

Result

If the indicator displays solid green, it means that the analog phone is ready for use. Users can use the analog phone to make and receive calls.


Set up a SIP Phone

This topic describes how to register a SIP extension on a SIP phone in the local network.

Prerequisites

- You have [created a SIP extension](#).
- The SIP phone is in the same local network as Yeastar P-Series PBX System.

Procedure

1. Gather information of extension registration.
For most SIP phones, the following credentials are needed in order to register with Yeastar P-Series PBX System.
 - The PBX's IP address
 - SIP registration port (Path: System > Network > Service Ports)
 - Transport protocol (Path: Extension and Trunk > Extension > Advanced > Transport)
 - Extension information (Path: Extension and Trunk > Extension > User):
 - Extension number
 - Registration name
 - Registration password
 - Caller ID name
2. Register the extension on a phone.
Log in to the phone's web interface, fill in and save the required items to register the SIP extension.
3. Confirm the extension's registration status in one of the following ways:
 - On the phone's web interface, check if the extension is registered.
 - Log in to PBX management portal, go to Extension and Trunk > Extension, check if the endpoint icon displays  in the Online Status column.

Result

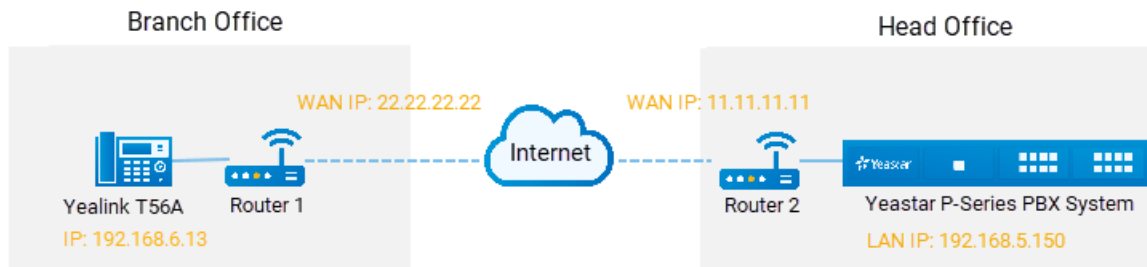
The SIP phone is ready for use. Users can use the SIP phone to make and receive calls.

Set up a Remote SIP Phone

This topic provides a configuration example to help you understand how to register a remote SIP extension on a SIP phone.

Background information

Yealink T56A and Yeastar P-Series PBX System are in different locations and networks. The administrator wants to register Yealink T56A on Yeastar P-Series PBX System, so that users in branch office can use Yealink T56A to make and receive calls.



Procedure

- [Step1. Forward the required ports on your router](#)
- [Step2. Configure SIP NAT settings on your PBX](#)
- [Step3. Set up an extension for remote access](#)
- [Step4. Register the extension on the phone](#)

Step1. Forward the required ports on your router

Forward the following ports on Router 2 that is connected to Yeastar P-Series PBX System, so that all the packets received on the router WAN port (11.11.11.11) can be forwarded to the PBX (192.168.5.150).

Table 2.

Service port	Local port	External port
SIP Registration Port	UDP 5060	UDP 5078
RTP Ports Range	UDP 10000-12000	UDP 10000-12000

Step2. Configure SIP NAT settings on your PBX

Configure SIP NAT settings to ensure that SIP data can be transmitted correctly between the PBX and the public Internet.

Procedure

1. Log in to PBX management portal, go to System > Network, click Public IP and Ports tab.
2. Turn on the option Public IP (NAT), and configure NAT settings.
 - a. In the NAT Type drop-down list, select Public IP Address.

- b. In the Public IP address field, enter the PBX's WAN IP. In this example, enter 11.11.11.11.
- c. In the Local Network Identification section, enter the local network segment and subnet mask.
 - i. Click +Add IP.
 - ii. In the Network Number field, enter the LAN IP. In this example, enter 192.168.5.0.
 - iii. In the Subnet Mask field, enter the subnet mask. In this example, enter 255.255.255.0.
- d. In the NAT Mode drop-down list, select Yes.

The PBX uses NAT, ignores the address information in the SIP headers or SDP headers, and replies to the sender's IP address and port.

3. Enter external ports that you have forwarded on the router 2.
 - External SIP UDP Port: In this example, enter 5078.
4. Click Save and Apply.

Step3. Set up an extension for remote access

1. On the PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Security tab, select the checkbox of Allow Remote Registration.
3. Click Save and Apply.

Step4. Register the extension on the phone

Log in to the phone web interface to register the desired extension on Yealink T56A.

Note:

Use the public IP address of the PBX and the forwarded SIP port to register the remote extension.

Account	Account 2	?
Register Status	Registered	
Line Active	Enabled	?
Label	1000	?
Display Name	1000	?
Register Name	ALVLqoWE95	?
User Name	1000	?
Password	?
SIP Server 1	?	
Server Host	11.11.11.11	Port 5078 ?
Transport	UDP	?
Server Expires	3600	?
Server Retry Counts	3	?

Public IP of Yeastar IPPBX

The forwarded SIP port

Result

Users in branch office can use Yealink T56A to make and receive calls.

Extension Presence

Extension Presence Overview

This topic describes what is extension presence and how presence benefits a user's work.

What is presence

Presence indicates a user's current status. By default, anyone in your organization using Yeastar P-Series PBX System can see if other users are available.

Yeastar P-Series PBX System supports the following status:

- Available: The user is online and ready for communication.
- Away: The user is away from desk.
- Business Trip: The user is on a business trip.
- Do Not Disturb: The user doesn't want to be disturbed, and he or she won't receive any calls.
- Lunch Break: The user is currently on lunch break.
- Off Work: The user is currently off work.

How presence benefits a user's work

Presence is associated with the following settings. You can configure the following settings for each presence. When a user's presence changes, the following settings will change accordingly.

- Presence information: Details about current presence.
- Call forwarding: Route internal and external calls to different destinations based on extension presence.
- Ring strategy: Adjust endpoints' ring strategy based on extension presence.
- Ring timeout: Adjust endpoints' ring timeout based on extension presence except Do Not Disturb status.
- Ring the Mobile Number Simultaneously: Whether to simultaneously ring mobile phone when a call reaches the extension number.
- Accept push notifications: Whether to receive Linkus push notifications on Linkus Mobile Client, such as missed calls, voicemails, etc.
- Agent Status Auto Switch: Adjust agent status automatically if the user is in a queue.
- Voicemail greetings: Adjust voicemail greetings based on extension presence.

For more information, see [Presence Settings](#) and [Change Voicemail Greetings](#).

Presence switch

There are two ways to switch extension presence:

- Switch presence manually: Extension users can switch their own presence on Linkus clients or by dialing a feature code; an administrator can also switch extension presence for specific users on PBX management portal.

For more information, see [Switch Presence on Linkus Client](#) and [Manually Switch an Extension's Presence](#).

- Switch presence automatically: Presence is switched based on [Business Hours and Holidays](#).

For more information, see [Auto Switch Presence Status based on Business Hours and Holidays](#).

Presence Settings

This topic describes presence settings.

Background information

Yeastar P-Series PBX System supports to configure presence settings under each presence for all the users. When a user's presence changes, presence settings will change accordingly.

Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension in the Presence tab.

- [Presence Information](#)
- [Call Forwarding](#)
- [Ring Strategy](#)
- [Ring Timeout](#)
- [Options](#)

Presence Information

Table 3.

Setting	Description
Presence Information	Add a note to the current presence. The note will be displayed on Linkus clients.

Call Forwarding

Call forwarding rules help forward incoming calls to a specific destination when the user is unavailable. You can set different destinations for incoming calls based on extension presence.

Table 4.

Setting	Description
Types of incoming calls	<ul style="list-style-type: none"> • Internal Calls: Set a call forwarding rule for incoming calls from colleagues. • External Calls: Set a call forwarding rule for incoming calls from external users.
Forwarding condition	<p>Select a forwarding condition and configure a destination.</p> <ul style="list-style-type: none"> • Always: Forward all incoming calls to the designated destination. • No Answer: Only forward unanswered calls to the designated destination. • When Busy: Only forward the calls that come in while the user is talking on the phone to the designated destination.

Ring Strategy

Ring strategy allows you to decide in which order incoming calls are distributed to the endpoints where the user's extension is registered.

- Extension Endpoint: The IP phone, analog phone, or softphone to which the user's extension has logged in.
- Linkus Mobile Client

- Linkus Desktop Client (Softphone Only)
- Linkus Web Client (Web Client Mode Only)


Table 5.

Setting	Description
Ring First	Set which endpoint will ring first.
Ring Secondly	Set which endpoint will ring secondly.

Ring Timeout

To prevent callers from waiting for a long time, you can configure ring timeout. If the call is not answered during the time period, it will be routed to the destination of No Answer.

Table 6.

Setting	Description
Ring Timeout	Enter a value or select a value from the drop-down list. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  Note: The valid range is from 5 to 300. </div>

Options

Ring the Mobile Number Simultaneously

To simultaneously ring both extension and the associated mobile number when anyone calls in the extension number, you can configure a simultaneous ring strategy.


 **Note:**
The feature is unavailable in Do Not Disturb status.

Table 7.

Setting	Description
Ring the Mobile Number Simultaneously	Check the option to enable this feature, and configure the user's mobile number.
Prefix	Enter the prefix of outbound route so that PBX can successfully send calls out.

Accept Push Notifications

By default, the user can receive push notifications on Linkus Mobile Client anywhere and anytime, such as missed calls, new voicemail messages and so on. If Linkus server is set up only in local network, in case the user can not connect to calls when he or she is out of the office, you can disable push notifications for the user.


Table 8.

Setting	Description
Accept Push Notification	Enable or disable push notifications on Linkus Mobile Client.

Agent Status Auto Switch

If the user is a dynamic agent who needs to frequently log in to or out of a queue, you can associate queue status with extension presence. The user's status in a queue will automatically change along with his or her extension presence.

Table 9.

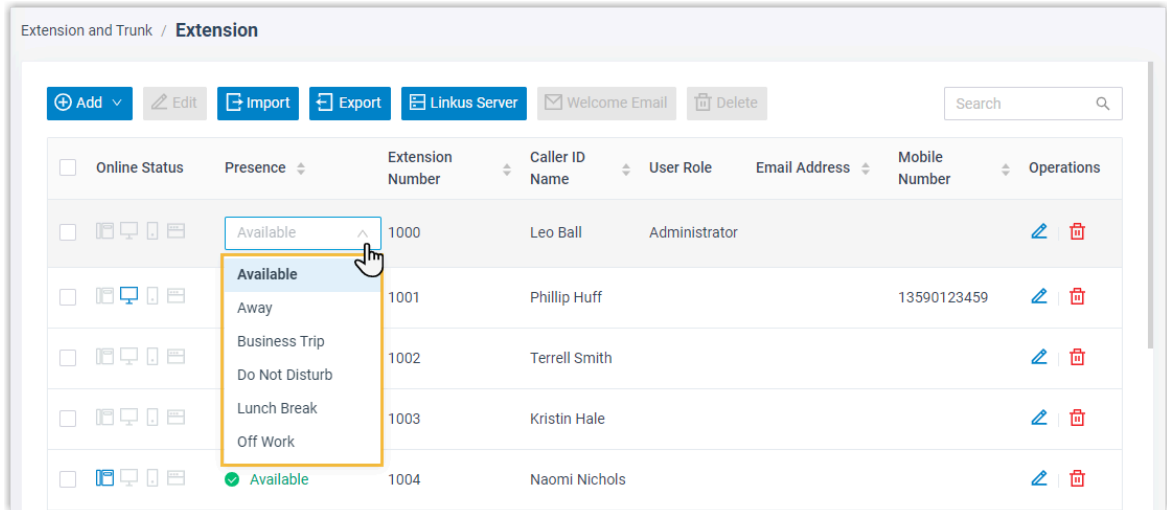
Setting	Description
Login	Log in to a queue. <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;">  Note: The option is available ONLY in Available status. </div>
Logout	Log out of a queue.
Pause	Pause receiving queue calls.
Do Nothing	Retain current status.

Manually Switch an Extension's Presence

This topic describes how to switch an extension's presence manually.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. On Extension list, find the desired extension.
3. In the Presence column, select a status from the drop-down list.



4. On the current page, click a blank space.
5. Click Apply.

Result

New presence is synchronized on Linkus clients; [presence settings](#) related with the status take effect.

Related information

[Automatically Switch Presence Based on Business Hours and Holidays](#)

Automatically Switch Presence Based on Business Hours and Holidays

This topic gives a configuration example to describe how to configure presence auto switch based on Business Hours and Holidays for specific extension users.

Background information

Assume that you have set Business Hours and Holidays on the PBX system, and you want the presence of extensions to be automatically switched according to the following time schedule:

Business Hours and Holidays	Time-based Presence
Business Hours: 09:00-12:00 and 14:00-18:00 from Monday to Friday.	Available
Break Hours: 12:00-14:00 from Monday to Friday.	Lunch Break
Holidays: December 25 to January 5.	Off Work
Outside Business Hours: The time periods that are not defined as Business Hours, Break Hours, or Holidays.	Off Work

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the extensions that need to switch presence status automatically based on the time schedule.
2. Click the Features tab, and go to Time-conditional Presence Auto Switch section.
3. Configure the following presence based on the time:
 - Business Hours: Select a status to be displayed during office hours.
In this scenario, select Available.
 - Break Hours: Select a status to be displayed during break time.
In this scenario, select Lunch Break.
 - Holidays: Select a status to be displayed during holiday.
In this scenario, select Off Work.
 - Outside Business Hours: Select a status to be displayed during non-office hours.
In this scenario, select Off Work.
4. Click Save.

Note:

The priority of presence switching at different times is: Holidays > Break Hours > Business Hours > Outside Business Hours.

Result

Presence status will be switched automatically according to the Business Hours and Holiday status.

For example, after 18:00, the presence displayed on Linkus client will be switched to Off Work.

Note:

If someone force switches Business Hours Status, the presence will be switched according to the current Business Hours status.

For example, Business Hours status is switched from Outside Business Hours to Business Hours, the presence will be switched from Off Work to Available.

Related information

- [Overview of Business Hours and Holidays](#)
- [Manually Switch an Extension's Presence](#)

Forward Internal and External Calls to Different Destinations

This topic describes how to forward internal and external calls to different destinations.

Scenario

A boss is in a meeting, and he or she only wants to receive calls from secretary. In this case, you can route external calls to a destination like voicemail, and internal calls to the secretary's extension.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Presence tab.
3. In the status bar, select a status to which the call forwarding rule will be applied.
4. In the Internal Calls section, select a forwarding action and specify a destination.

In this example, select the checkbox of *Always*, set the destination to Extension, and select the secretary's extension.

5. In the External Calls section, select a forwarding action and specify a destination.

In this example, select the checkbox of *Always*, set the destination to Voicemail.

6. Click Save and Apply.

Result

When a call reaches the extension number, the system will check the user's presence, identify whether it originates from an internal caller or external caller, and then route the call to the specified destination.

Ring Office Phone and Mobile Phone Simultaneously

This topic describes how to achieve simultaneous ring on office phone and mobile phone.

Scenario


A user may miss important calls when he or she is away from desk or on a business trip. In this case, you can enable simultaneous ring for the user. When a call reaches the user's extension number, both mobile phone and office phone with the extension number logged in will simultaneously ring.

Prerequisites

- You have set a mobile number for the extension.
- At least one outbound route is ready for use.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.

2. Click Presence tab.
3. In the status bar, select a status to which the strategy of simultaneous ring will be applied.
4. In the Options section, configure the following settings.
 - a. Select the checkbox of Ring the Mobile Number Simultaneously.
 - b. Click  to configure mobile number.
 - c. Optional: In the Prefix field, enter the [prefix of outbound route](#) so that PBX can successfully send calls to your phone.
 - If the Strip of outbound route is not set, you don't have to set the Prefix.
 - If the Strip of outbound route is set, you need to set the Prefix according to the Patterns of outbound route.
5. Click Save and Apply.

Result

If a call reaches the user's extension number when he or she is in the specified presence, both office phones and mobile phone will ring simultaneously.

Extension Voicemail

Set up Extension Voicemail

This topic introduces voicemail feature and describes how to set up voicemail for an extension.

Background information

Yeastar P-Series PBX System supports voicemail feature, which helps users receive audio messages when they are unavailable to answer calls. When you create an extension, the voicemail feature is enabled by default, and a 4-digit PIN code is randomly generated for accessing voicemail.

You can retain default settings, or change the following settings according to your needs.

- [Enable or disable voicemail feature](#)
- [Voicemail PIN Authentication](#)
- [Notification methods and play options of voicemails](#)
- [Voicemail greetings](#)

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Voicemail tab, turn on the option Enable Voicemail.

3. Optional: Configure voicemail PIN settings.

- Voicemail PIN Authentication: Set whether a PIN code is required when the user accesses voicemail.
 - Enabled
 - Disabled
- Voicemail Access PIN: Retain the default PIN code or change it according to your needs.



Note:

The PIN code must be number, and the length must be 3-15 digits.

4. Optional: Configure notification settings for new voicemails.

- New Voicemail Notification: Set whether to notify the user or not when receiving a new voicemail, and how to notify.
 - Do not Send Email Notifications: Disable email notification.
 - Send Email Notifications with Attachment: Send a notification email with the new voicemail message attached as a .wav file.
 - Send Email Notifications without Attachment: Send a notification email as soon as receiving a new voicemail message in mailbox.
- After Notification: Set how to deal with voicemails after sending emails to inform the user.
 - Make as Read: Keep the voicemail messages in mailbox as read to prevent users from repeatedly receiving reminders on their phones.
 - Delete Voicemail: Delete the voicemail message to avoid mailbox being filled up.



Note:

We recommend that you select this option only when the extension user has received a notification email with voicemail message attachment.

- Do Nothing: Keep the voicemail messages in mailbox as unread.

5. Optional: Set whether to play the following messages when playing a voicemail.

- Play Date and Time
- Play Caller ID
- Play Message Duration

6. Optional: To customize voicemail greetings that will be played to callers when they reach the user's voice mailbox, see [Record or Upload Voicemail Greetings](#).

7. Click Save and Apply.

Related information

[Forward Voicemail Messages to Email](#)

[Check Voicemail Messages](#)

Extension Features

Handle Incoming Calls Based on Caller ID

This topic describes how to create a call handling rule for a specific user to handle incoming calls (calls from colleagues and external contacts) based on incoming Caller ID.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Features tab.
3. In the Call Handling Based on Caller ID section, set up one or more rules according to your needs.
 - a. Click Add.
 - b. In the Caller ID field, enter a specific number or a number pattern.
 - To apply the rule to a specific number, enter a specific number.

For example, enter 10086 to handle incoming calls with Caller ID 10086 based on the rule.
 - To apply the rule to a number pattern, enter a wildcard pattern.

For example, enter 9011. to handle incoming calls with any Caller ID starting with 9011 based on the rule.


For more information, see [Caller ID Pattern](#).
 - c. In the Action drop-down list, set how to deal with incoming calls with the Caller ID.
 - Hang Up
 - Extension
 - Voicemail
 - IVR
 - Play Greeting then Hang up
 - Accept Call



Note:

By default, all incoming calls are allowed to reach the extension. If there is a call-handling rule to prevent spam calls (eg.728373XX) from reaching the extension, but the extension user wants to accept calls from a specific number (eg.72837300), you can create another rule to accept calls from 72837300.

- d. Click Save.
- e. Optional: To add more rules, repeat step a-d.
- f. Optional: In the Move column, adjust the rules' order. The rules take effect from the top down.

 Note:

For example, set the rule "Accept calls from 72837300" to a higher priority than the rule "Reject calls from numbers starting with 728373". In this way, when receiving calls from 72837300, the system will send calls to the extension user. For other incoming calls from number starting with 728373, the system will hang up directly.

4. Click Save and Apply.

Result

When incoming calls reach the extension, the system will handle the calls based on Caller IDs.

Set up Email Notifications for Missed Calls

To remind an extension user of missed calls, you can set up email notifications of missed calls for the extension user.

Prerequisites

- [System email server](#) is set up.
- An email address is associated with a desired extension.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Features tab.
3. In the Notifications section, select the checkbox of Send email notifications on missed calls.
4. Click Save and Apply.

Result

If the extension user has missed calls, system will send notification emails to the user's mailbox.

Set up Email Notifications for User Password Change

To remind an extension user of user password change, you can set up email notifications of user password change for the extension user.

Prerequisites

- [System email server](#) is set up.
- An email address is associated with a desired extension.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Features tab.
3. In the Notifications section, select the checkbox of Send email notification when the User Password is changed.
4. Click Save and Apply.

Result

If the extension user's user password has been changed, system will send notification emails to the user's mailbox.

Allow Multiple Registrations for One Extension Number

Registering one extension number to multiple SIP endpoints allows the employees to handle calls on any devices. This topic describes how to set the maximum concurrent registrations for an extension.

Background information

For employees who work flexibly anywhere, they can register their extensions on multiple SIP endpoints, such as an IP phone in their office, a softphone on computer, or a SIP client on mobile phone. In this way, an incoming call can ring all endpoints at the same time, and users can handle calls at anywhere on any devices.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. In the Extension Information section, set the maximum endpoints allowed to register the extension in the IP Phone Concurrent Registrations field.
In this example, set the concurrent registrations to 3.

Note:

- The maximum number of concurrent registration is 3.
- Concurrent Registration setting only limits the registration number of non-Linkus SIP endpoints. The registration number of Linkus clients is not counted.

Extension Information

<p>* Extension Number</p> <input style="width: 90%;" type="text" value="2000"/>	<p>* Caller ID</p> <input style="width: 90%;" type="text" value="2000"/>
<p>* Registration Name</p> <input style="width: 90%;" type="text" value="4o7nxjETmH"/>	<p>* Registration Password</p> <input style="width: 90%;" type="password" value="....."/>
<p>IP Phone Concurrent Registrations</p> <input style="width: 90%;" type="text" value="3"/>	

3. Click Save and Apply.

Result

In addition to being registered on Linkus clients, the extension can also be registered on 3 other SIP endpoints.

When the extension receives a call, all the endpoints will ring. The extension user can handle the calls on any endpoint.

Note:

By default, when the extension is busy in a call and a new call reaches, all the endpoints (Linkus and other SIP endpoints) can still ring.

To prevent other endpoints from receiving a new incoming call when an endpoint is busy, go to Extension and Trunk > Extension > Features > Call to enable All Busy Mode for Endpoints for the extension.

Set up Third-party Integration for Call Popup

Yeastar Popup URL allows a lightweight integration with a third-party application (such as CRM system, ERP system, etc.) to achieve call popup. When an extension receives a call, the PBX calls the URL of the third-party application and retrieves relevant customer data to display on the pop-up web page.

Restrictions and requirements

Restrictions

The feature only works when Linkus Web Client is logged in.

Requirements

- PBX server: Version 37.4.0.17 or later.
- Third-party application:
 - Web-based.
 - Support to provide a URL that can identify callers via Caller ID and Caller ID Name.

Procedure

Follow the instructions below to set up popup URL for extensions in bulk. You can also customize it for a specific extension.

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. Select the checkboxes of the desired extensions, click Edit.
3. Under the Features tab, select the checkbox of Bulk Edit and turn on the option Popup URL.

4. Set up the third-party integration via Popup URL.

Table 10.

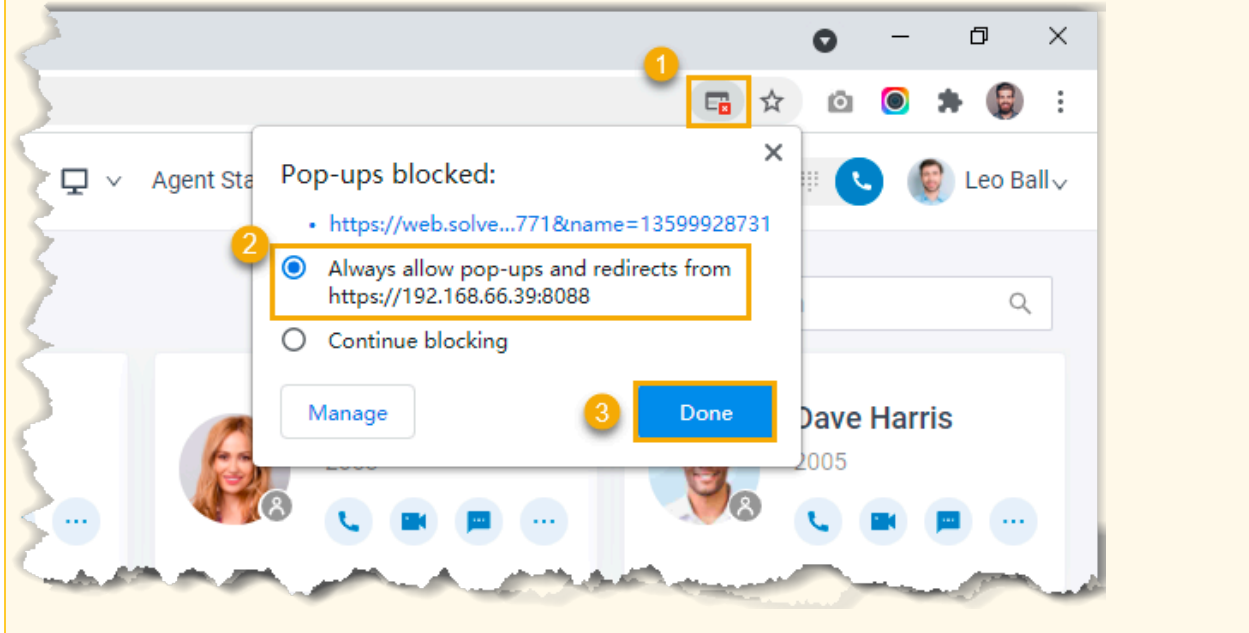
Settings	Descriptions
Popup URL	<p>Enter the third-party URL, followed by the variables that you want to pass.</p> <p>Supported variables:</p> <ul style="list-style-type: none"> • {{.CallerNumber}}: Incoming Caller ID. • {{.CallerDisplayName}}: Incoming Caller ID Name. <p>Take Solve360 CRM as an example: <code>https://web/solve.360-.com/{{.CallerNumber}}&{{.CallerDisplayName}}</code></p>
Communication Type	<p>Select which types of calls will trigger the call popup.</p> <ul style="list-style-type: none"> • Inbound: Inbound calls from external users. • Internal: Internal calls from colleagues.
Trigger Event	<p>Set when the call popup will be automatically triggered.</p> <ul style="list-style-type: none"> • Ringing: An incoming call reaches. • Answered: An incoming call is answered. • Call End: An incoming call is ended.

5. Click Save.

Result

When an incoming call reaches the extensions on Linkus Web Client, a pop-up screen automatically appears in the web browser and displays relevant customer data.

! Important:
For the first-time use, users need to allow pop-ups and redirection from Linkus Web Client, or the pop-up screen can NOT be opened automatically.



Extension Advanced Settings

Advanced Settings of SIP Extension




This topic describes the advanced settings of a SIP extension.

Note:
The SIP configurations require professional knowledge of SIP protocol. Incorrect configurations may cause calling issues on the SIP extension.

Table 11.


Setting	Description
DTMF Mode	Set the mode for sending DTMF tones. <ul style="list-style-type: none"> • RFC4733 (RFC2833): DTMF will be carried in the RTP stream in different RTP packets.

Table 11. (continued)

Setting	Description
	<ul style="list-style-type: none"> • Info: DTMF will be carried in the SIP info messages. • Inband: DTMF will be carried in the audio signal. • Auto: If the device supports RFC4733 (RFC2833), PBX will choose RFC4733 (RFC2833), otherwise the PBX will choose Inband.
Transport	<p>Set the transport protocol.</p> <ul style="list-style-type: none"> • UDP • TCP • TLS <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: If you change the transport protocol, you must re-register the extension.</p> </div>
Qualify	<p>Enable this option to send SIP OPTION packet to SIP device to check if the device is up.</p>
T.38 Support	<p>Enable or disable T.38 fax for the extension.</p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: Enabling T.38 will add performance cost. We recommend that you disable T.38.</p> </div>
NAT	<p>Enable this option when the PBX uses a public IP address. The feature is enabled by default.</p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: If you manually set up Linkus server, make sure the desired extension's NAT is enabled, or the extension user can not access Linkus when he or she is out of local network.</p> </div>
SRTP	<p>Enable SRTP for voice encryption.</p>

Advanced Settings of FXS Extension

This topic describes the advanced settings of an FXS extension.




 Note:

The FXS configurations require professional knowledge. Incorrect configurations may cause calling issues on the FXS extension.

VoIP settings

If you enable Linkus clients for an FXS extension, you may need to configure the following settings:



Table 12.

Setting	Description
DTMF Mode	<p>Set the mode for sending DTMF tones.</p> <ul style="list-style-type: none"> • RFC4733 (RFC2833): DTMF will be carried in the RTP stream in different RTP packets. • Info: DTMF will be carried in the SIP info messages. • Inband: DTMF will be carried in the audio signal. • Auto: If the device supports RFC4733 (RFC2833), PBX will choose RFC4733 (RFC2833), otherwise the PBX will choose Inband.
Transport	<p>Set the transport protocol.</p> <ul style="list-style-type: none"> • UDP • TCP • TLS <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: If you change the transport protocol, you must re-register the extension.</p> </div>
Qualify	<p>Enable this option to send SIP OPTION packet to SIP device to check if the device is up.</p>
T.38 Support	<p>Enable or disable T.38 fax for the extension.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Enabling T.38 will add performance cost. We recommend that you disable T.38.</p> </div>
NAT	<p>Enable this option when the PBX uses a public IP address. The feature is enabled by default.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: If you manually set up Linkus server, make sure the desired extension's NAT is enabled, or the extension user can not access Linkus when he or she is out of local network.</p> </div>
SRTP	<p>Enable SRTP for voice encryption.</p>

Hotline

Hotline feature allows a phone to automatically dial a pre-configured number when the user goes off hook and a specific time interval passes.

Table 13.

Setting	Description
Hotline	Turn on the option to enable hotline feature.
Hotline Number	Enter the hotline number. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> Note: Only numbers, space, and () . - + * # are allowed.</p> </div>
Delay Dial (s)	Enter the waiting time (in seconds) before automatically dialing out the hotline number. <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> Note: Only numbers are allowed.</p> </div>

Flash Detection

Set an amount of time to help the PBX identify if a hook flash is a valid event.

Table 14.

Setting	Description
Min Flash Detection (ms)	Set the minimum amount of time. The default value is 300. To change the value, select a value from the drop-down list. Valid values: 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000
Max Flash Detection (ms)	Set the maximum amount of time. The default value is 1000. To change the value, select a value from the drop-down list. Valid values: 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000



Volume Settings

Set the transmitted and received volume of PBX.

Table 15.

Setting	Description
RX Volume	Set the volume from the analog phone to the PBX's FXS port. The default value is 40%.

Table 15. (continued)

Setting	Description
	<p>To change the value, select a value from the drop-down list.</p> <p>Valid values: 5%, 10%, 20%, 40%, 60%, 80%, 100%, 150%, Custom</p> <div style="border: 1px solid black; padding: 5px;"> <p> Note: If you choose Custom, you must go to RX Gain (db) field to enter an integer between -30 and 12.</p> </div>
TX Volume	<p>Set the volume from the PBX's FXS port to the analog phone. The default value is 40%.</p> <p>To change the value, select a value from the drop-down list.</p> <p>Valid values: 5%, 10%, 20%, 40%, 60%, 80%, 100%, 150%, Custom</p> <div style="border: 1px solid black; padding: 5px;"> <p> Note: If you choose Custom, you must go to TX Gain (db) field to enter an integer between -30 and 12.</p> </div>

Options

Table 16.

Setting	Description
Call Waiting	When receiving an incoming call during an active call, the user can hear a weak beeping sound that informs the user of the new incoming call. The user can press FLASH key on the analog phone to toggle between incoming call and the current call.
DTMF Passthrough	If this option is enabled, PBX will not process the DTMF tones, and pass DTMF tones transparently to the other end.
Echo Cancellation	If this option is enabled, PBX removes extra noise and improves sound quality during a call.

Extension Security

Extension Security Overview


This topic describes security options to prevent Yeastar P-Series PBX System from unauthorized SIP registrations and abused outbound calls.

SIP security options

Yeastar P-Series PBX System provides the following options to prevent unauthorized SIP registrations.

Allow Remote Registration

Anytime you use a remote extension to access PBX, you expose your PBX to the public internet, which increases the risk of VoIP hacking and attack. The option is disabled by default.

 Note:

We recommend that you keep the option disabled unless you need a remote extension.

SIP User Agent Identification

By default, PBX allows phones to register extensions without user agent limit. To enhance extension security, you can restrict which user agent is allowed to register an extension.

When a phone is trying to register the extension, the phone will send SIP packets containing user agent. If the prefix of the user agent does not match the specified value, the registration will fail.

SIP Registration IP Restriction

By default, PBX allows SIP registrations without the limit of IP address.

To enhance extension security, you can specify which IP address or IP section is allowed to register an extension.

Call restrictions options

Yeastar P-Series PBX System provides the following options to prevent abused outbound calls.

Disable Outbound Calls


Restrict users from making outbound calls.

Disable Outbound Calls outside Business Hours

Restrict users from making outbound calls during off-duty time and holidays.

Disallow International Calls

Restrict users from making international calls.

 Note:

The option works only when you have enabled Enable Allowed Country/Region Code Dialing Protection. For more information, see [Block Outbound International Calls](#).

Max Outbound Call Duration (s)

When the user is in an outbound call and the call duration reaches the limit, the system would end the call.

Outbound Call Frequency Restriction

When an extension makes outbound calls and the number of calls exceeds the outbound call frequency restriction within specified time period, the system would restrict the extension from making outbound calls. For more information, see [Limit Outbound Call Frequency of an Extension](#).

Restrict Outbound Calls for an Extension

This topic describes why and how to restrict outbound calls for an extension.

Background information


Toll fraud is a global problem in telecommunication industry. It happens when hackers access your PBX system and make expensive phone calls from existing accounts. To prevent toll fraud, you can restrict outbound calls for an extension.

Procedure



1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit a desired extension.
2. Click Security tab.
3. In the Call Restrictions section, select the checkbox of Disable Outbound Calls.
4. Click Save and Apply.

Result

- Users cannot make outbound calls even if the extensions are selected in outbound routes.

 Note:
Emergency Calls like 911 is not restricted.

- On Extension list,  is displayed in front of the extension.

 Note:
To cancel the restriction of outbound calls, click  to edit the extension, go to Security tab and unselect the checkbox of Disable Outbound Calls in the Call Restrictions section.

<input type="checkbox"/>	Online Status	Presence	Extension Number	Caller ID Name	User Role	Email Address	Mobile Number	Operations
<input type="checkbox"/>			1000	Leo Ball	Administrator			
<input type="checkbox"/>			1001	Phillip Huff			13590123459	
<input type="checkbox"/>			1002	Terrell Smith				
<input type="checkbox"/>			1003	Kristin Hale				
<input type="checkbox"/>			1004	Naomi Nichols				

Restrict Extension Registration Based on User Agent

This topic describes how to restrict extension registration based on user agent.

Background information

SIP is a peer-to-peer protocol. The peers in a session are called User Agents (UAs). A user agent can play one of the following roles:

- User Agent Client (UAC): A client application that initiates a SIP request, such as INVITE, ACK, OPTIONS, BYE, CANCEL, and REGISTER.
- User Agent Server (UAS): A server application that receives the SIP request from a UAC, and returns a response to the request back to the UAC.

When a SIP endpoint tries to register an extension to Yeastar P-Series PBX System, the SIP endpoint working as UAC sends packets containing user agent string to the PBX. By default, Yeastar P-Series PBX System allows registrations from any UAC without authenticating user agent. For security reasons, you can restrict extension registration based on user agent.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Security tab.
3. In the SIP Security section, select the checkbox of Enable User Agent Registration Authorization.
4. Set the user agent.
 - a. Click Add User Agent.
 - b. In the User Agent field, enter a value.
5. Click Save and Apply.

Result

When a phone is trying to register an extension, the phone will send SIP packets containing a user agent, such as phone manufacturer, phone model, etc. If the prefix of the user agent does not match the specified value, the registration will fail.

Restrict Extension Registration Based on IP Address

This topic describes how to allow devices with a specific IP address or in a specific IP section to register extensions on Yeastar P-Series PBX System.

Background information

By default, Yeastar P-Series PBX System allows SIP registrations without the limit of IP address. In case hackers remotely register extensions and make expensive phone calls, you can restrict that only devices with a specific IP address or in a specific IP section can register extensions on Yeastar P-Series PBX System.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Security tab.
3. In the SIP Security section, select the checkbox of Enable IP Restriction.
4. Set which IP address or IP section is allowed to register the extension.
 - a. Click Add IP.
 - b. In the Permitted IP and Subnet Mask fields, set the allowed IP address or IP section.
5. Click Save and Apply.

Result

Only device with the IP address or in the IP section can register the extension.

Block Outbound Calls Outside Business Hours

This topic describes how to restrict an extension from making outbound calls outside business hours.

Prerequisites

You have set [global business hours](#).

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Security tab.
3. In the Call Restrictions section, select the checkbox of Disable Outbound Calls outside Business Hours.
4. Click Save and Apply.

Result

The user can NOT make outbound calls during off-duty time and holidays.

Limit Call Duration of an Outbound Call

This topic describes how to limit call duration of an outbound call.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Security tab.
3. In the Call Restrictions section, select a value from the drop-down list of Max Outbound Call Duration (s), or enter a value according to your needs.
4. Click Save and Apply.

Result

When the user is in an outbound call and call duration reaches the Max Outbound Call Duration (s), the system would end the call.

Limit Outbound Call Frequency of an Extension

To secure enterprise communications and reduce the economic loss if the PBX system has been hacked, we recommended that you set up rules to restrict the extension outbound call frequency.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Security tab.
3. Scroll down to the Call Restrictions section, in the Outbound Call Frequency Restriction drop-down list, select the desired rule (s).

Note:

The PBX has a default rule Default_Ext_Outbound Call Frequency, which limits extension users to make maximum 5 outbound calls in 1 second. You can add new rules according to your need. For more information, see [Add an 'Outbound Call Frequency Restriction' Rule](#).

- Click Save and Apply.

Result

If an extension has exceeded the outbound call frequency restriction, the following things would happen.


- Users cannot make outbound calls even if the extensions are selected in outbound routes.

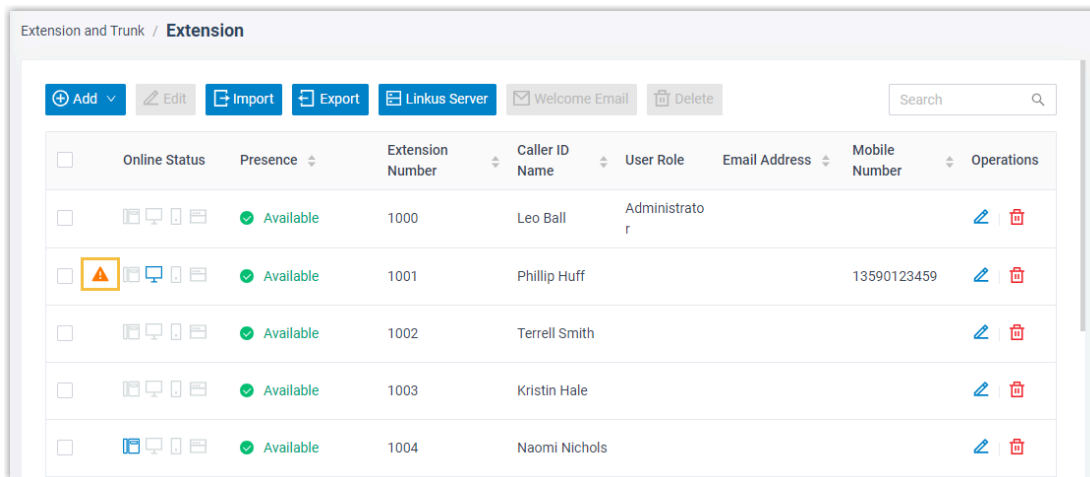
Note:

Emergency Calls like 911 is not restricted.

- On Extension list,  is displayed in front of the extension.

Note:

To cancel the restriction of outbound calls, click  to edit the extension, go to Security tab and unselect the checkbox of Disable Outbound Calls in the Call Restrictions section.



<input type="checkbox"/>	Online Status	Presence	Extension Number	Caller ID Name	User Role	Email Address	Mobile Number	Operations
<input type="checkbox"/>			1000	Leo Ball	Administrator			
<input type="checkbox"/>			1001	Phillip Huff			13590123459	
<input type="checkbox"/>			1002	Terrell Smith				
<input type="checkbox"/>			1003	Kristin Hale				
<input type="checkbox"/>			1004	Naomi Nichols				


- The system sends a notification to inform the notification contacts of an [Outbound Call Frequency Exceeded](#) event.

Manage Extensions

Edit Extensions

This topic describes how to edit an extension, or edit extensions in bulk.

Edit an extension

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. On Extension list, select the desired extension, click .
3. Change extension settings according to your needs.
4. Click Save and Apply.


Bulk edit extensions

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. On Extension list, select the checkboxes of the desired extensions, click Edit.
3. Select the checkbox of the desired feature, change extension settings according to your needs.
4. Click Save and Apply.

Reset an Extension's User Password

An extension's user password is used to log in to PBX management portal and Linkus clients. As an administrator, you can reset an extension's user password if the user forgets password.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. Search and select the desired extension, click .
3. In the User Information section, delete the value in the User Password field, and enter a new password.
4. Click Save.

Result

The extension's user password is changed. You need to inform the user of the new password.

Export and Import SIP Extensions

The SIP extensions configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired extension information in the exported file, and import the file to PBX again. This topic describes how to export and import SIP extensions.

Note:

Only system super administrator can import SIP extensions.

Export all extensions

You can export all the SIP extensions to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. Click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see [Extension Parameters](#).

Import SIP extensions

We recommend that you export extension data to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 50 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information, see [Extension Parameters](#).

Procedure


1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. Click Import.
3. In the pop-up window, click Browse, select your CSV file.
4. Click Import.

The extension data in the CSV file will be displayed in the Extension list.

Delete Extensions

This topic describes how to delete an extension or delete extensions in bulk.

Delete an extension

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. On Extension list, select the desired extension, click .
3. In the pop-up dialog box, click OK.
4. Click Apply.

Bulk delete extensions

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. On Extension list, select the checkboxes of the desired extensions, click Delete.
3. In the pop-up dialog box, click OK.
4. Click Apply.

Contacts

Contacts Overview


Yeastar Contacts feature allows users to store external contacts outside of your organization on PBX, access and call those contacts on endpoints (IP phone and Linkus clients) where their extensions have registered. This topic describes terminologies, requirements, key features, and limits of Yeastar Contacts feature.

Terminologies

Before using Yeastar Contacts feature, familiarize yourself with the following terminologies:

Personal Contacts

Personal Contacts is exclusive to each extension user, which allows users to store a number of personal contacts, such as direct customers.

 Note:

Each user's Personal Contacts is only visible to himself or herself.

Company Contacts

Company Contacts is shared among authorized users, which allows authorized users to store a number of company shared contacts, such as company's customers, resellers, and partners.

Phonebooks

Phonebooks is a value-added service for Company Contacts, which allows authorized users to group company contacts into phonebooks, and implement robust control over access to each phonebook.

Key features

Table 17.

Contacts Feature	Basic Plan	Enterprise Plan / Ultimate Plan
Group company contacts into phonebooks	×	√
Sync contacts from integrated CRMs	×	√
Sync contacts on Linkus clients	√	√

Table 17. (continued)

Contacts Feature	Basic Plan	Enterprise Plan / Ultimate Plan
Sync contacts on IP phones	√	√
Identify incoming calls	√	√
Route inbound calls by matched contacts	×	√

Limits

Table 18.

Type	P550	P560	P570
Company contacts (total)	50,000	200,000	500,000
Company phonebooks	100	200	500
Personal contacts (per extension)	100	200	300

Related information

- [Manage Company Contacts](#)
- [Manage Company Phonebooks](#)
- [Export and Import Company Contacts](#)
- [Grant Company Contacts Permissions](#)
- [Identify Callers from Contacts](#)
- [Allow Users to Query Contacts on IP Phones](#)

Manage Company Contacts

This topic describes how to add, edit, or delete company contacts on PBX management portal.

Operation permissions

The authorized users can view and manage company contacts on Linkus clients, or view company contacts on an IP phone.

To grant users Company Contacts permissions, see [Grant Company Contacts Permissions](#).

To manage contacts on Linkus clients or an IP phone, see the following topics:

- [Linkus Web Client - User Guide](#)

- [Use Contacts on an IP Phone](#)

The following table shows what operations can be done on different endpoints.



 Note:
*: For Enterprise/Ultimate Plan, there would be compatibility issues on Linkus Desktop Client. We recommend that you use Web Client and Mobile Client to manage contacts.

Table 19.

Permission	Linkus Clients			IP Phone
	Web Client	Mobile Client	*Desk-top Client	
View company contacts	√	√	√	√
Add company contacts	√	√	√	×
Edit company contacts	√	√	√	×
Delete company contacts	√	√	√	×
Import company contacts	×	×	×	×
Export company contacts	×	×	×	×

Add a company contact

1. Log in to PBX management portal.
2. Go to Contacts > Company Contacts, click Add.
3. Enter contact information.
4. Optional: In the Phonebook List drop-down list, select one more phonebooks where you want the contact to be grouped.


 Note:

- Phonebook feature is available for Enterprise Plan and Ultimate Plan.
- A newly created contact will be added to the default phonebook 'All Company Contacts_Phonebook', if any.

5. Click Save.


The contact is stored in Company Contacts and synchronized to users' endpoints (IP phones and Linkus clients).

Edit a company contact

1. Log in to PBX management portal.
2. Go to Contacts > Company Contacts, click  beside the desired contact.
3. Edit contact information.
4. Click Save.

Changes of the contact are synchronized to users' endpoints (IP phones and Linkus clients).

Delete company contacts

1. Log in to PBX management portal, go to Contacts > Company Contacts.
2. To delete a company contact, select the desired contact, click  and OK.
3. To delete company contacts in bulk, select the checkboxes of the desired contacts, click Delete and OK.

The contacts are removed from Company Contacts and users' endpoints (IP phones and Linkus clients).

Related information

[Grant Company Contacts Permissions](#)

Manage Company Phonebooks

This topic describes how to add, edit, and delete company phonebooks.

Prerequisites


You have subscribed Enterprise Plan or Ultimate Plan.

Background information

Yeastar Phonebooks feature allows you to create phonebooks to group company contacts in an organized way and implement robust control over users' access to each phonebook.

Yeastar P-Series PBX System supports two kinds of company phonebook:

- PBX native company phonebook: A phonebook that stores company contacts that are created on PBX management portal and Linkus Clients.

- CRM-synchronized company phonebook: A phonebook that stores company contacts that are synced from the integrated CRM. The phonebook will be marked with an identifier 'CRM' ().



Note:

Phonebooks synchronized from CRM can NOT be edited or deleted.

Group company contacts into phonebooks

1. Log in to PBX management portal.
2. Go to Contacts > Phonebooks, click Add.
3. In the Phonebook Name field, enter a name to help you identify it.
4. In the Members section, select desired company contacts.
 - To define a All Contacts phonebook:
 - a. Select All Company Contacts from the drop-down list of Select Contacts.




Note:

Any time you add a company contact, the contact will be automatically added to the phonebook.


- To group contacts into a phonebook:
 - a. Select Specific Company Contacts from the drop-down list of Select Contacts.
 - b. Click Add to select the desired company contacts.
 - c. Click Confirm.
5. Click Save.

Edit company phonebooks

1. Log in to PBX management portal.
2. Go to Contacts > Phonebooks, click  beside the desired phonebook.
3. Edit phonebook name, add or delete company contacts from the phonebook according to your needs.
4. Click Save.

Changes of the phonebook are synchronized to users' Linkus clients.

Delete company phonebooks

1. Log in to PBX management portal, go to Contacts > Phonebooks.
2. To delete a phonebook, select the desired phonebook, click  and OK.
3. To delete phonebooks in bulk, select the checkboxes of the desired phonebooks, click Delete and OK.

The phonebooks are removed from PBX server and users' Linkus clients.

**Note:**

Company contacts in the phonebook are still kept in the system.

Related information

[Grant Company Contacts Permissions](#)

[Contacts Overview](#)

[Manage Company Contacts](#)

[Identify Callers from Contacts](#)

[Allow Users to Query Contacts on IP Phones](#)

Export and Import Company Contacts

The company contacts configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired contacts in the exported file, and import the file to PBX again. This topic describes how to export and import company contacts.

Export company contacts

You can export all company contacts to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Contacts > Company Contacts.
2. Click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see [Company Contacts Parameters](#).

Import company contacts

We recommend that you export company contacts data to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 300 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information , see [Company Contacts Parameters](#).

Procedure

1. Log in to PBX management portal, go to Contacts > Company Contacts.
2. Click Import.

3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The company contacts in the CSV file will be displayed in the Contacts list.

Related information

[Linkus Web Client Guide - Export personal contacts](#)

[Linkus Web Client Guide - Import personal contacts](#)

Grant Company Contacts Permissions

By default, all the users have no access to company contacts. This topic describes how to allow users to view and manage company contacts.

Background information

As Phonebooks feature is not supported on Basic Plan, the description for company contacts permission varies. Refer to the following table for details.

Table 20.

PBX Plan	Permission
Basic Plan	<ul style="list-style-type: none"> • View Company Contacts • Manage Company Contacts (Add, Edit, Delete Company Contact)
Enterprise/Ultimate Plan	<ul style="list-style-type: none"> • View Phonebooks • Manage Phonebooks (Add, Edit, Delete)

Procedure

A Sales Department responsible for business in Europe is assigned a phonebook Customer-s_EU. The Sales Manager can view and manage contacts in the phonebook, while Sales can only view contacts.

Based on the above scenario, follow the instructions below to grant permissions to the Sales Manager and Sales.

Note:

If you want to grant permissions to a specific user, you can assign a custom user type to the member, and customize permissions. For more information, see [Assign a custom user type to a group member](#).

1. Log in to PBX management portal, go to Extension and Trunk > Extension Group, click  beside desired group.

2. Click Group Permissions tab, configure the permissions in the Permission Configuration section.

- For Sales Manager
 - a. Select the checkboxes of View Phonebooks and Manage Phonebooks (Add, Edit, Delete)
 - b. Select the phonebook Customers_EU.

Manager

- ▼ Allow Using Operator Panel
 - Switch group members' presence
- Call distribution management (Redirect, Transfer, Drag and Drop operation)
- Pick up or hang up other extensions' calls
- Call monitoring operations (Listen, Whisper, Barge-in)
- Call parking operations (Park, Retrieve)
- Route calls directly from IVR regardless of the IVR menu
- Switch Business Hours and Holidays status
- Switch extension's recording status
- View Phonebooks
 - * Phonebook
 - Customers_EU x ▼
- Manage Phonebooks (Add, Edit, Delete)
 - * Phonebook
 - Customers_EU x ▼

- For Sales
 - a. Select the checkbox of View Phonebooks.
 - b. Select the phonebook Customers_EU.

User

- Allow Using Operator Panel
 - Switch group member's presence
 - Call distribution management (Redirect, Transfer, Drag and Drop operation)
 - Pick up or hang up other extension's calls
 - Call monitoring operations (Listen, Whisper, Barge-in)
 - Call Parking
 - Route calls directly from IVR regardless of the IVR menu
 - View Phonebooks
 - * Phonebook
 - Customers_EU x
 - Manage Phonebooks (Add, Edit, Delete)

3. Click Save.

Result

The permissions are granted to all the managers and users in the group in a batch.

What to do next

If you want to change members' user types to Manager or User in the group, see [Assign a default user type to a group member](#).

Identify Callers from Contacts

This topic describes how to configure Caller ID match to help users identify callers whose information is stored in Yeastar Contacts.

Background information

Caller ID match is supported on all kinds of endpoints, including Linkus clients, desk phones, or softphones. Yeastar P-Series PBX System allows users to identify callers from Company Contacts and Personal Contacts.

Identify callers from Company Contacts

Support for authorized extension users who have permissions to view or manage company contacts.

For more information about how to grant permissions to users, see [Grant Company Contacts Permissions](#).

Identify callers from Personal Contacts

Support for each extension user.

Priority of Caller ID match

If an incoming number is stored in Company Contacts, Personal Contacts, mobile phone directory, and IP phone directory at the same time, the priority of Caller ID match from high to low is as follows:

- Mobile Phone Directory/IP Phone Directory
- Personal Contacts
- Company Contacts

Configure Caller ID match

1. Log in to PBX management portal, go to Contacts > Company Contacts.
2. Configure Caller ID match.
 - a. On the Company Contacts page, click Options.
 - b. Choose how to match incoming Caller ID.
 - Do Not Match: Display original incoming Caller ID.
 - Exact Match: Display contact name when an incoming Caller ID exactly matches existing number.
 - Fuzzy matching the last {number} digits: Display contact name when the last few digits of an incoming Caller ID matches that of existing number.
 - c. Click Save.

Caller ID match example

A contact Dora whose phone number is 12345678 is stored in Company Contacts; the system receives an incoming call from Dora.

- Do Not Match is selected:
 - When Dora calls in, the contact name "Dora" will not be displayed.
- Exact Match is selected:
 - If the incoming Caller ID is 12345678, the contact name "Dora" will be displayed.
 - If the incoming Caller ID is +012345678, the contact name "Dora" will NOT be displayed.
- Fuzzy matching the last 8 digits is configured:
 - If the incoming Caller ID is +012345678, the contact name "Dora" will be displayed.
 - If the incoming Caller ID is 62345678, the contact name "Dora" will NOT be displayed.

Related information

[Route Inbound Calls by Matched Phonebook Contacts](#)

Allow Users to Query Contacts on IP Phones

To allow users to query contacts on IP phones, you need to auto provision IP phones. This topic describes how to allow users to query contacts on IP phones.

Requirements

PBX Server

Version 37.2.0.80 or later.

IP Phone

Use Yealink phones of the required model and version. For more information, see [Yealink phones](#).

Note:

- Yealink conference phones and DECT bases are NOT supported.
- A maximum of 1000 company contacts and 300 personal contacts can be displayed on an Yealink phone.

Procedure

1. Grant permission for users to access company contacts.

For more information, see [Grant Company Contacts Permissions](#).

Note:

By default, all the users have access to their own personal contacts, but no access to shared company contacts.

2. Synchronize contacts data to users' IP phones via Auto Provisioning.
 - If users' extensions haven't be associated with phones, see [Auto Provision IP Phones](#) to bind phones with the extensions.
 - If users' extensions have been associated with phones, reprovision the phones to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Select the checkboxes of the desired phones, click Reprovision.

Result

Contacts data are synchronized to IP phones' remote phonebooks. Users can query and place calls to contacts from the remote phonebook.

Note:

Two remote phonebooks from the PBX server are displayed on the IP phone:

- **Company_Contacts:** Saves all the company shared contacts that you can view.

Note:

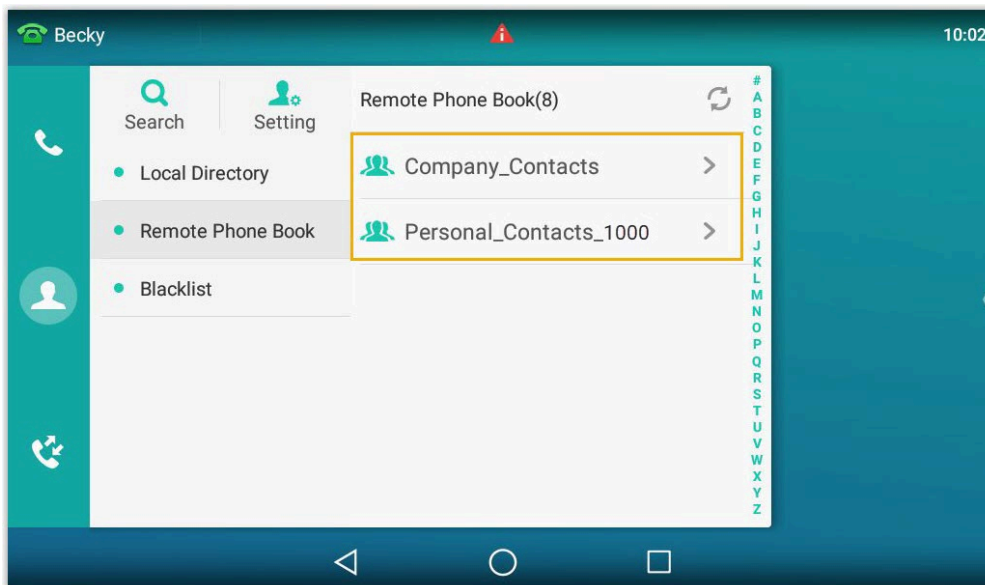
For Enterprise/Ultimate Plan, company contacts on IP phones can NOT be grouped into phonebooks.

- **Personal_Contacts_{extension_number}:** Saves all your personal contacts.

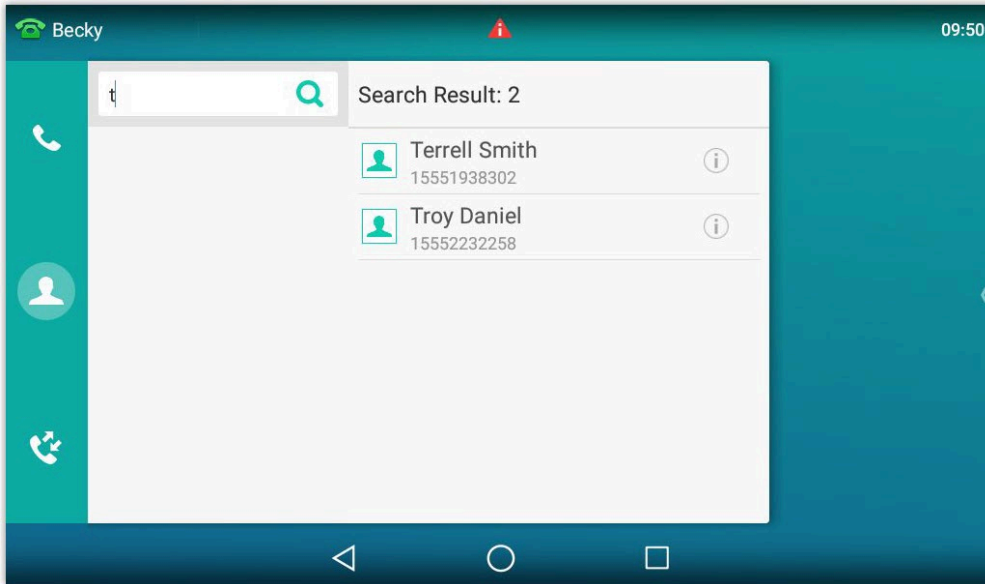
Example: Query contacts on Yealink T56A IP phone

1. Tap  > Remote Phonebook.

The directories that the user is allowed to view are displayed on the page.



2. Tap Search.
3. In the search box, enter contact name or number. The system will query contact from Contacts.



4. Select a contact, tap the contact number to quickly dial out.

Extension Group

Extension Group Overview

Yeastar P-Series PBX System supports to add specific extensions to a group, assign user types to these extensions, and grant permissions to extension users with different user types.

What is Extension Group

Extension group is a group that contains a number of extensions with a common function or purpose. Extension group is displayed on Linkus clients, which allows users to easily find a contact within a group, and makes it possible for authorized users to view or manage company contacts, or control calls of members within a specific group on Linkus Web Client.

User types in an extension group

A user type is a permission set, which allows you to control users' access to specific areas and features on Linkus Web Client. Yeastar P-Series PBX System provides 3 user types. You can grant permissions to each user type and assign user types to group members.


Default user types

- Manager: Assign the user type to a leader, so that he or she can manage members' calls or access organization's company contacts.
- User: Assign the user type to ordinary members. Any time you add members to a group, they are assigned the user type by default.

The following table displays default permissions for Manager and User, you can change the permissions according to your needs. For more information, see [View or change permissions for managers and users](#).

Module	Permission	Manager	User
Operator Panel	Switch group members' presence	√	√
	Call distribution management (Redirect, Transfer, Drag and Drop operation)	√	√
	Pick up or hang up other extensions' calls	√	√
	Call monitoring operations (Listen, Whisper, Barge-in)	√	√

Module	Permission	Manager	User
	Call parking operations (Park, Retrieve)	√	√
	Route calls directly from IVR regardless of the IVR menu	√	√
	Switch Business Hours and Holidays status	√	×
	Switch extension's recording status	√	×
Phonebooks	View Phonebooks	×	×
	Manage Phonebooks (Add, Edit, Delete)	×	×

 Note:

As Phonebooks feature is not supported on Basic Plan, the permission for company contacts is View Company Contacts and Manage Company Contacts (Add, Edit, Delete Company Contact).

Custom user type

Custom: If you want to grant permissions to a specific member, you can assign the user type to a desired member, and customize permissions.

For more information, see [View or change permissions for a member with custom user type](#).

Default extension group

Yeastar P-Series PBX System has a built-in group Default_All_Extensions that contains all the extensions on the PBX. Any time you create an extension, the extension will be automatically added to the extension group. You can delete the group, or create one or more groups according to your needs.


For more information, see [Create an Extension Group](#).

Create an Extension Group

This topic describes how to create an extension group.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension Group, click Add.
2. Configure basic settings for the extension group.
 - a. In the Name field, enter a group name to help you identify it.
 - b. In the Select Members drop-down list, set which extensions will be added to the group.
 - All Extensions: If you choose the option, all the extensions will be moved to the Selected box.

 **Note:**
ONLY one group that contains all the extensions is allowed.

- Specific extensions: If you choose the option, select the desired extensions from Available box to Selected box.

* Select Members

Specific Extensions





2 items Available

Search here


<input type="checkbox"/>	Extension Number	CallerID Name
<input type="checkbox"/>	1006	Nicole
<input type="checkbox"/>	3333	Sunny Yeah


6 items Selected


Search here

<input type="checkbox"/>	Extension N...	CallerID Na...	User Type	Operations
<input type="checkbox"/>	1000	Becky	User	
<input type="checkbox"/>	1001	Jerry	User	
<input type="checkbox"/>	1002	Finn	User	
<input type="checkbox"/>	1003	Amelia G...	User	

- c. Assign user types for group members.

 **Note:**
 Users of different user types have different permissions. For more information, see [User types in an extension group](#).

- i. In the Selected box, click  beside the desired member.
- ii. In the pop-up window, configure the User Type and permissions.
 - If you select Manager or User, the member has all the permissions that are granted to the user type.

 **Note:**
 The permissions of Manager and User are pre-defined. To change the permissions, see [View or change permissions for managers and users](#).

- If you select Custom, select the checkboxes of the desired permissions.
- iii. Click Save.

3. To define which users within your organization can view the group on Linkus clients, configure the group's visibility.
 - a. Click Group Permissions tab.
 - b. In the Group Information Visibility drop-down list, select a type.
 - Visible to all Extensions: All extension users can view the group.
 - Visible to Extensions in this Group: Only group members can view the group.
 - Visible to Specific Extensions: Only specific extension users can view the group.

If you choose the option, select the desired extensions from the drop-down list of Specific extensions, or enter the desired value.
4. Click Save.


Result

The extension group is displayed on Extension Group list; the authorized users can view the group on Linkus clients.


Manage Extension Groups

This topic describes how to edit or delete extension groups.

Edit an extension group

1. Log in to PBX management portal, go to Extension and Trunk > Extension Group, click  beside the desired group.
2. Change group settings according to your needs.
3. Click Save and Apply.

Delete extension groups

1. Log in to PBX management portal, go to Extension and Trunk > Extension Group.
2. To delete an extension group, do as follows:
 - a. Click  beside the desired group.
 - b. In the pop-up dialog box, click OK.
 - c. Click Apply.
3. To delete extension groups in bulk, do as follows:
 - a. Select the checkboxes of the desired groups, click Delete.
 - b. In the pop-up dialog box, click OK.
 - c. Click Apply.

The groups are removed from Extension Group list and are not displayed on Linkus clients.

Assign a User Type to a Group Member

Members of different user types have different permissions. You can control members' access to specific features by assigning different user types in an extension group. This topic describes how to assign a user type to a group member.

Assign a default user type to a group member


Yeastar P-Series PBX System provides two default user types: Manager and User, each of them has preset permissions. By assigning the two user types to members, you can bulk grant permissions to multiple members who share common responsibilities.

Prerequisites

Familiarize yourself with permissions of Manager and User in the desired group and change permissions according to your needs.

For more information, see [View or change permissions for managers and users](#).

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension Group, edit the desired extension group.
2. Assign Manager or User to a group member.
 - a. In the Members section, click  beside the desired member.
 - b. In the User Type drop-down list, select Manager or User according to your needs.
 - c. Click Confirm.


Result

The member's user type and permissions in the group are updated.

Assign a custom user type to a group member

If you want a member to have different permissions from members with default user types, you can assign a custom user type to a desired member, and customize permissions.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension Group, edit the desired extension group.
2. Assign Custom to a group member, and grant permissions to the member according to your needs.
 - a. In the Members section, click  beside the desired member.
 - b. In the User Type drop-down list, select Custom.
 - c. Select the checkboxes of the desired permissions.

- d. Click Confirm.
3. Click Save and Apply.


Result

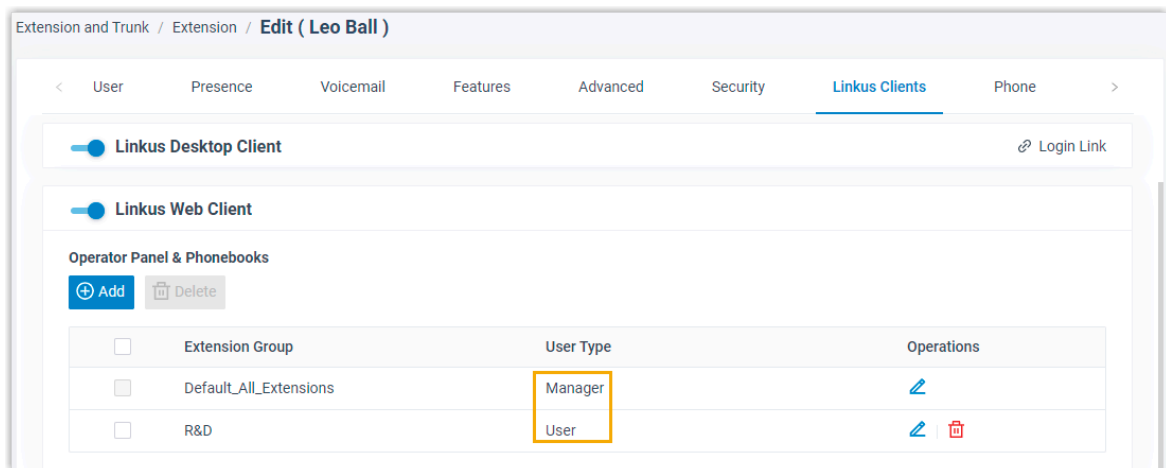
The member's user type and permissions in the group are updated.

View or Change a Member's User Type in Multiple Groups

If an extension user plays different roles in different extension groups, you can quickly view or change multiple user types of the extension user without having to go to each group to view or assign the user types. This topic describes how to view or change a member's user type in multiple groups.

View a member's user type in multiple groups



1. Log in to PBX management portal, go to Extension and Trunk > Extension, click  beside desired extension.
2. Click Linkus Clients tab.
3. In the Operator Panel & Phonebooks section, you can see all the groups to which the extension user belongs. Check the user's user type in each group in User Type column.

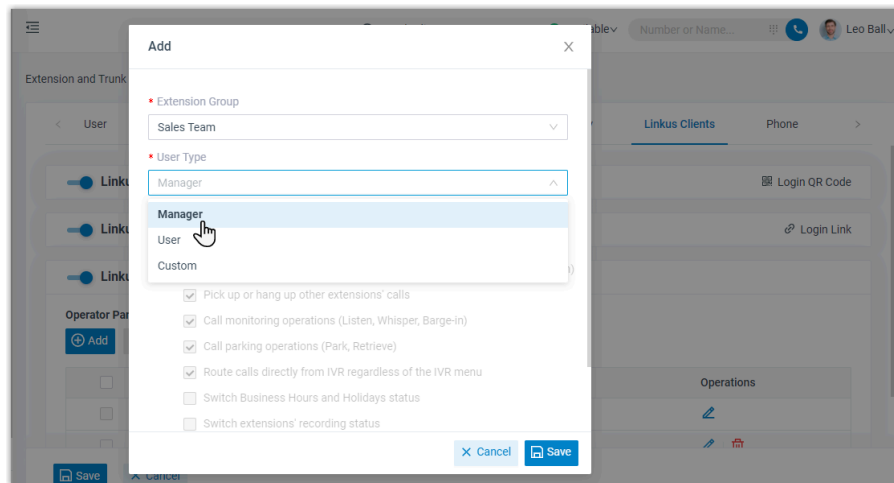


Change a member's user type in multiple groups

The permissions of Manager and User vary from one group to another. Make sure you change permissions for the right group.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, click  beside desired extension.
2. Click Linkus Clients tab.
3. In the Operator Panel & Phonebooks section, change the extension user's user type in a group.
 - a. Click  beside the desired extension group.
 - b. In the User Type drop-down list, select a user type.
 - If you select Manager or User, the user has all the permissions that are granted to the user type.
 - If you select Custom, select the checkboxes of the desired permissions.



- c. Click Confirm.
4. Repeat Step4 to assign user types for the extension in more groups.
5. Click Save.

Result

The user's user types and permissions in different groups are updated accordingly.

Related information

[Assign a User Type to a Group Member](#)

View or Change Permissions for Group Members

This topic describes how to view or change permissions for group members.

View or change permissions for managers and users

If members are assigned Manager or User in a group, all the members with the same user type have the same permissions. You can view the permissions of managers and users within a specific group, and change permissions according to your needs.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension Group, edit the desired extension group.
2. Click Group Permissions tab.
3. To view permissions, scroll down to Permission Configuration section.

You can view the permissions that are granted to Manager and User in the group.

4. To change permissions, do as follows:
 - a. In the Permission Configuration section, select or unselect the checkboxes of corresponding permissions for Manager and User.
 - b. Click Save and Apply.

Result

The permissions of all the managers and users in the group are updated in a batch.


What to do next

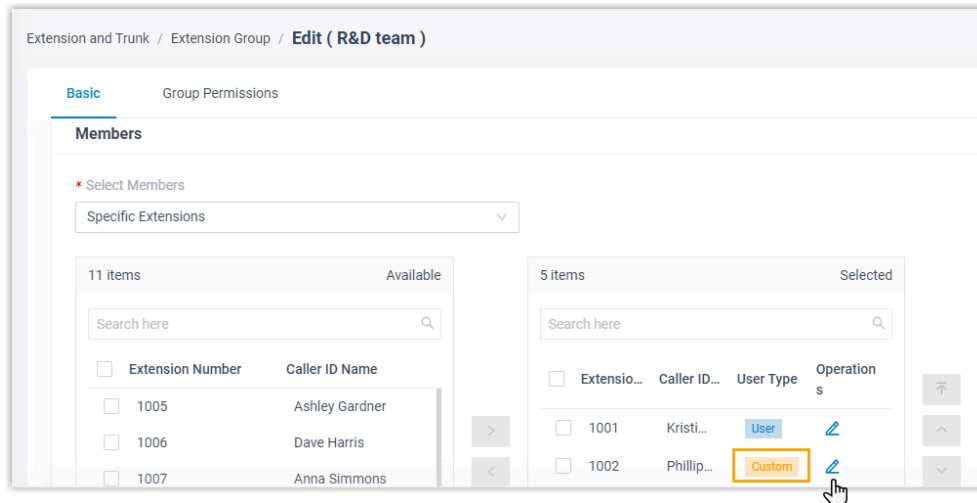
If you want to change members' user types to Manager or User in the group, see [Assign a default user type to a group member](#).

View or change permissions for a member with custom user type

For members with Custom user type assigned, permissions may vary from one member to another. You can view or change permissions for a specific member according to your needs.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension Group, edit the desired extension group.
2. In the Members section, click  beside the desired member whose user type is Custom.



- a. In the pop-up window, select or unselect the checkboxes of the desired permissions for the user.
 - b. Click Confirm.
3. Click Save and Apply.

Result

The member's permissions are updated.

Auto Provisioning

Auto Provisioning Overview

This topic describes what is Auto Provisioning, provisioning supported devices, provisioning method, and which settings can be configured via Auto Provisioning.

What is Auto Provisioning

Auto Provisioning is a time-saving feature that helps you to manage and deploy devices centrally on Yeastar P-Series PBX System. The process of configuring devices, and managing firmware update is simplified to one-click provisioning, which makes deployment and management of devices fast and convenient.

Auto Provisioning supported devices

Yeastar P-Series PBX System supports various models for Auto Provisioning.

Find the [Auto Provisioning - Supported Devices](#) before you start deploying devices.

Provisioning method

Yeastar P-Series PBX System supports auto provisioning devices via Plug and Play (PnP) method.

PnP provides a proprietary method to auto provision devices from PBX server that are located in the local network.

Steps to provision devices via PnP method

1. Power on the PBX first then power on the devices (phones or gateways).
2. RESET the devices if they have been used previously.
3. Connect the devices to the same local network as PBX, and power on the devices.



Note:

The devices must be in the same network segment as the PBX (for example, the devices and PBX are all in the network segment 192.168.6.X), or the Auto Provisioning could not take effect.

4. Prepare a provisioning template.
5. Apply the provisioning template and assign extensions to these devices.

Which settings can be configured via Auto Provisioning

- General settings (preferences & codecs)

General settings provide the most common needs for extension users, such as phone language, date and time, etc. These settings can be auto provisioned by a template, so that the settings can be applied to multiple devices globally.

For more information, see [Auto Provision IP Phones](#).

- Extension registration

An extension will be registered on the device after auto provisioning. If you change extension registration settings (such as registration password, registration name, SIP UDP/TCP port), you need to reprovision your devices.



Note:

Limit of extension registration

- For IP phone: Only one extension can be assigned to a phone via Auto Provisioning.
- For DECT phone: Each handset registers with an extension via Auto Provisioning.

For more information, see [Auto Provision IP Phones](#) and [Reassign an Extension to a Provisioned Phone](#).

- Function Keys

Various function keys are available for you to customize for each extension user, such as BLF, speed dial, etc. The function keys are associated with extensions, and can be applied when auto provisioning phones.

For more information about the function keys, see [Auto Provision Function Keys for Phones](#).

- Device Firmware

Yeastar P-Series PBX System allows you to update the device firmware in bulk by auto provisioning. For more information about firmware update, see [Update Phone Firmware via Auto Provisioning](#).

- Additional settings

In addition to the above settings, if you need to configure additional settings for the devices, you can also customize a template with additional parameters, and provision devices globally to apply the additional settings.

For more information, see [Create a Custom Auto Provisioning Template](#).

Manage Phones

Auto Provision IP Phones

This topic describes how to auto provision phones that are located in the same local network as Yeastar P-Series PBX System.

Prerequisites

- RESET the phones if they are previously used.
- Make sure that the phones are in the same network segment as the PBX.
- Prepare an auto provisioning template.

Procedure


1. Log in to PBX management portal, go to Auto Provisioning > Phones.

The phone list displays all the discovered devices with their related information including model, MAC address, IP address, etc.

Note:

- Only the [supported devices](#) can be discovered and displayed on the phone provisioning list.
- Restart the phones if they are not discovered and displayed on the phone provisioning list.

2. Select the desired phones to provision.

- To provision an individual phone, click  beside the desired phone.
- To provision multiple phones, select the checkboxes of the desired phones, and click Edit.

Note:

The selected phones must be of the same model.

3. In the Options section, select a desired template from the Template drop-down list.
4. In the Assign Extension section, assign an extension for each phone or handset.

Tip:

If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other phone (s).

- To release the previous phone, see [Release an Extension from a Provisioned Phone](#).
- To associate an extension with multiple IP phones, see [Allow Multiple Registrations for One Extension Number](#).



5. Click Save.


Result

The configurations will be automatically applied to the phones.

What to do next

Go to Auto Provisioning > Phones, check extension registration status of provisioned phones.

- : The assigned extension is registered on the phone.
- : The assigned extension is unregistered on the phone.

<input type="checkbox"/>	Status	Extension	Name	Vendor	Model	IP Address	Phone Password	Template	Firmware Version
<input type="checkbox"/>		1000	Leo Ball	Yealink	SIP-T56A	192.168.6.33	-	YSDP_YealinkT56	58.83.0.15

Related information

[Modify a Provisioned Phone Settings](#)

[Auto Provision Function Keys for Phones](#)

Pre-provision IP Phones

This topic describes how to pre-provision IP phones.

Background information

Pre-provisioning is particularly useful for out-of-the-box scenarios in deployments of large number of phones.

Pre-provisioning allows you to provide general configurations for phones in advance. Instead of powering on and connecting each new phone to the same LAN as PBX, you can just add the new phones (Vendor, Model, and MAC address) to provisioning list on PBX, assign extensions to each phone and configure corresponding settings.

When users get their phones, power on and connect them to the same LAN as PBX system, the phones will be provisioned automatically.

Prerequisites

- Gather information of all phones, including Vendor, Model, and MAC address.
- Prepare an auto provisioning template.

Procedure

1. Log in to PBX management portal, go to Auto Provisioning > Phones.
2. Click Add and select Bulk Add.
3. In the IP Phone section, configure phone information as follows:
 - Vendor: Select a phone vendor.
 - Model: Select a phone model.
 - MAC Address: Enter MAC address of each phone. Each on a separate line.
4. In the Options section, select a desired template from the drop-down list of Template.
5. In the Assign Extension section, assign an extension to each phone.

i Tip:

You can select an extension range from the Start Extension and End Extension, and click Assign Extension to assign an extension to each phone.

6. Click Save.



Result


The PBX generates a configuration file for each phone.

What to do next

1. Connect the phones to the same local network as the PBX, and power on the phones. The phones automatically get configuration files from the PBX and apply the configurations.

📄 Note:

- If the phones are previously used, a factory reset is required.
 - The phones must be in the same network segment as the PBX (for example, the phones and PBX are all in the network segment 192.168.6.X), or the Auto Provisioning could not take effect.
2. Go to Auto Provisioning > Phones, check extension registration status of provisioned phones.
 - : The assigned extension is registered on the phone.
 - : The assigned extension is unregistered on the phone.

<input type="checkbox"/>	Status	Extension	Name	Vendor	Model	IP Address	Phone Password	Template	Firmware Version
<input type="checkbox"/>		1000	Leo Ball	Yealink	SIP-T56A	192.168.6.33	-	YSDP_YealinkT56	58.83.0.15

Modify a Provisioned Phone Settings

Centralized provisioning enables you to configure phones with the same settings, you can also customize settings for a specific phone after provisioning. This topic describes how to modify general settings for an IP phone and a DECT phone.


Modify settings of a provisioned IP phone

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Modify the phone that is associated with the extension.

- a. Click the Phone tab.
- b. Modify phone settings in the Preference and Codecs sections.
- c. Click Save.


**Note:**

If you want to change other settings, click the phone IP address displayed on the provisioning list to access the phone web interface, and change the configurations as your need.

3. Reprovision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click  beside the phone assigned to the extension user.

The phone automatically applies the changes.

Modify settings of a provisioned DECT phone

1. Log in to PBX management portal, go to Auto Provisioning > Phones, edit a desired DECT phone.
2. Modify phone settings in the Preference and Codecs sections, and click Save.
3. On the phone provisioning list, click  beside the desired DECT phone to reprovision the phone.

The phone automatically applies the changes.

Auto Provision Function Keys for Phones

Each extension user can set his or her own function keys. When an extension and a phone are bound through auto provisioning, the function keys associated with the extension will be applied to the phone. This topic describes how to provision function keys for extension users.

Supported key types


The following table lists the function keys that you can assign for an extension user:

Key type	Function
Line	Monitor the registered extension.
BLF	<ul style="list-style-type: none"> • Monitor the status of a specific extension or a specific number. • Place a call to the monitored extension or number. • Pick up another user's incoming calls.
Speed Dial	Speed dial a number.
Check Voicemail	<ul style="list-style-type: none"> • Monitor the status of voicemail.

Key type	Function
	<ul style="list-style-type: none"> • Check voicemail messages.
Check Group Voice-mail	<ul style="list-style-type: none"> • Monitor the status of group voicemail in shared mode. • Access group voicemail box and check group voicemail messages.
Park & Retrieve	<ul style="list-style-type: none"> • Monitor the status of a specific parking number. • Park a call on a specific parking number. • Retrieve a parked call from a specific parking number.
Intercom	Place an intercom call.
DTMF	Send DTMF signal.
Agent Login/Logout	<ul style="list-style-type: none"> • Log in to a specific queue. • Log out of a specific queue.
Agent Pause/Un-pause	<ul style="list-style-type: none"> • Pause receiving a call from a specific queue. • Unpause receiving a call from a specific queue.

Procedure

1. Assign function keys for extension users.

- a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
 - If you want to assign function keys for a specific extension user, click  beside the desired extension.
 - If you want to assign function keys for multiple extensions, select the checkboxes of the desired extensions, and click Edit.
- b. Click the Function Keys tab.
- c. Configure function keys.


Note:

The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

- Type: Select a key type.
- Value: Configure a desired value based on the key type, such as parking number, queue, or extension.
- Label: Optional. Enter a value, which will be displayed on the phone screen.

d. Click Save.

2. If the extensions haven't been associated with phones, see [Auto Provision IP Phones](#) to bind phones with the extensions.

3. If the extensions have been associated with phones, reprovision the phones to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. To reprovision a phone, click  beside the phone assigned to this extension user.
 - c. To reprovision multiple phones, select the checkboxes of the desired phones, click Reprovision.

Result

The phone automatically applies the changes. Check the function key status on the phone to see if the changes are applied.

Reassign an Extension to a Provisioned Phone

If you want to assign a provisioned phone to another user, you can reassign an extension to the provisioned phone. This topic describes how to reassign an extension to a provisioned phone.

Procedure

1. Log in to PBX management portal, go to Auto Provisioning > Phones, edit the desired phone.
2. In the Assign Extension section, select a desired extension.

Tip:

If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other phone (s).

- To release the previous phone, see [Release an Extension from a Provisioned Phone](#).
- To associate an extension with multiple IP phones, see [Allow Multiple Registrations for One Extension Number](#).

3. Click Save.

Result

The extension is automatically registered on the phone, and configurations in the selected template are applied to the phone.

Note:

If the selected extension has ever been configured via Auto Provisioning with the same template, the configurations in the previous phone will be inherited in the new phone.

Release an Extension from a Provisioned Phone


When an employee resigns or doesn't need the phone that is currently bound with the employee's extension, you can release the employee's extension from the phone. This topic describes how to release an extension from a provisioned phone.

Procedure

1. Release the extension from previous phone.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit a desired extension.
 - b. Click the Phone tab.
 - c. Click Release From Phone and Yes.
 - d. Click Save.

The extension is released from the phone.

2. Reprovision the phone to de-register the extension.

Go to Auto Provisioning > Phones, click  beside the phone from which you want to release extension.


Update Phone Firmware via Auto Provisioning

This topic describes how to update phone firmware via auto provisioning.

Prerequisites

Upload the desired phone firmware to PBX. For more information, see [Add a device firmware](#).

Update firmware to all applicable phones

1. Log in to PBX management portal, go to Auto Provisioning > Resource Repository > Device Firmware.
2. Click  beside the desired firmware.
3. Click Yes to upgrade the phones.

Update firmware to specific phones

1. Log in to PBX management portal, go to Auto Provisioning > Phones.
2. Select the checkboxes of the desired phones.
3. Click Firmware Upgrade.
4. Select the firmware that you want to upgrade, click Upgrade Now.

Result

The phones automatically reboot and update their firmwares to the new version.

Apply a New Template to a Provisioned Phone

If an extension user needs to customize his or her phone, you can create a custom template and apply the new template to his or her phone. This topic describes how to apply a new template to a provisioned phone.

Prerequisites

[Create a custom auto provisioning template.](#)

Procedure

1. Log in to PBX management portal, go to Auto Provisioning > Phones, edit the desired phones.
2. In the Options section, select a desired template from the Template drop-down list.
3. Click Save.

Result

The configurations in the new template will be applied automatically to the phone.


Related information

[Update Auto Provisioning template\(s\) to all applicable devices](#)

Reboot Provisioned Phones

For some settings that need a phone reboot to take effect, you can reboot the phone remotely on PBX management portal. This topic describes how to reboot provisioned phones.

Procedure

1. Log in to PBX management portal, go to Auto Provisioning > Phones.
2. Reboot phones according to your needs:
 - To reboot a phone, hover your mouse over  beside the desired phone, and click Reboot.
 - To reboot phones in bulk, select the checkboxes of desired phones, and click Reboot.


The system prompts you whether to reboot the phones.

3. Click OK.

Remove Phones from Provisioning List

The provisioning list always displays all the phones that are discovered. For the out-of-use phones, you can remove them from the phone provisioning list manually. This topic describes how to remove out-of-use phones from provisioning list.

Procedure

1. Log in to PBX management portal, go to Auto Provisioning > Phones.
2. Remove phones according to your needs:
 - To remove a phone, hover your mouse over  beside the desired phone, and click Delete.
 - To remove phones in bulk, select the checkboxes of the desired phones, and click Delete.
3. Click OK.

Result

For the provisioned phones, the system erases all configuration files for the phone and releases the assigned extension.

Manage Gateways

Auto Provision Yeastar TA FXS Gateways

This topic describes how to auto provision Yeastar TA FXS gateways that are located in the same local network as Yeastar P-Series PBX System.

Prerequisites

- RESET the gateways if they are previously used.
- Make sure that the gateways are in the same network segment as the PBX, or Auto Provisioning configurations will not take effect.



Note:


A factory Yeastar TA FXS gateway is in DHCP network mode. You can connect an analog phone to any FXS port, dial *** and follow the voice prompt to check the IP address.

- Prepare an auto provisioning template.

Procedure


1. Log in to PBX management portal, go to Auto Provisioning > Gateways.

The gateway list displays all the discovered devices with their related information including model, MAC address, IP address, etc.

 **Note:**

Restart the gateways if they are not discovered and displayed on the gateway provisioning list.

2. Configure the gateway.

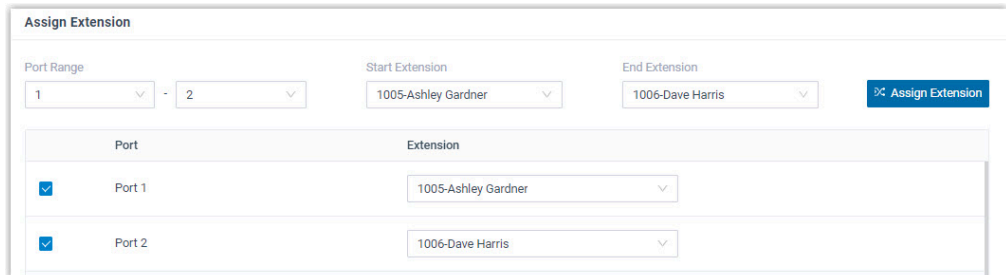
- a. Click  beside the desired gateway.
- b. In the Options section, select a desired template from the Template drop-down list.
- c. Assign an extension for each port on gateway.
 - i. In the Port Range field, select the port range to assign extensions.
 - ii. In the Start Extension and End Extension field, select the extension range to assign to the specified ports.
 - iii. Click Assign Extension.

The ports with assigned extensions are displayed below. You can reassign an extension for a specific port.

 **Tip:**


If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other device (s).

- To release the previous devices, see [Release an Extension from a Provisioned Gateway](#) or [Release an Extension from a Provisioned Phone](#).
- To associate an extension with multiple devices, see [Allow Multiple Registrations for One Extension Number](#).



Port	Extension
<input checked="" type="checkbox"/> Port 1	1005-Ashley Gardner
<input checked="" type="checkbox"/> Port 2	1006-Dave Harris


- d. In the Preference section, configure the settings as your need.
 - Key as Send: Assign the pound key (“#”) or asterisk key (“*”) as the send key.
 - SIP VoIPServer IDX: Select a VoIP server template ID to be provisioned.

 **Note:**

SIP VoIPServer IDX is not applicable for TA100 and TA200.

- Admin Password: Set the password for logging in to the gateway web interface.

- LAN Settings: Select the checkbox and configure a static IP address for gateway to ensure that the gateway can always be accessed by the PBX system.
 - IP Address: Enter the IP address that is assigned to the gateway.
 - Subnet Mask: Enter the subnet mask.
 - Gateway: Enter the gateway address.
 - Preferred DNS Server: Enter the IP address of preferred DNS server.
 - Alternative DNS Server: Optional. Enter the IP address of alternative DNS server.
 - IP Address 2: Optional. Enter a second IP address for the gateway.

 **Note:**

According to your network environment, you may need to set another IP address to allow users in different IP segment to access the gateway.

- Subnet Mask 2: Optional. Enter another subnet mask for the second IP address.

The following figure shows you an example of Static IP configuration.

The screenshot shows the 'LAN Settings' configuration page. At the top, there is an 'Admin Password' field. Below it, the 'LAN Settings' checkbox is checked. There are three radio buttons: 'DHCP' (unchecked), 'Static IP Address' (checked), and 'PPPoE' (unchecked). The configuration fields are as follows:

Field	Value
Hostname	TA400
Subnet Mask	255.255.255.0
Preferred DNS Server	8.8.8.8
IP Address 2	
IP Address	192.168.6.168
Gateway	192.168.6.1
Alternative DNS Server	
Subnet Mask 2	

- e. In the Codecs section, select your preferred codec list for the gateway.
- f. Click Save.

The PBX prompts you whether to reboot the gateway.

- g. Click OK to reboot the gateway to apply the configurations.



Result

The configurations will be automatically applied to the gateways after reboot:

- The specified extensions will be registered on the corresponding ports of gateway.
- The gateway's IP is changed to a static IP address (192.168.6.168).

What to do next

Go to Extension and Trunk > Extension, check extension registration status in the Online Status column.

- : The assigned extension is registered on the gateway.
- : The assigned extension is unregistered on the gateway.

Related information

[Modify a Provisioned Gateway Settings](#)

Pre-provision Yeastar TA FXS Gateways

This topic describes how to pre-provision gateways.

Background information

Pre-provisioning is particularly useful for out-of-the-box scenarios.

Pre-provisioning allows you to provide general configurations for a gateway in advance. Instead of powering on and connecting a new gateway to the same LAN as PBX, you can just add the new gateway (Vendor, Model, and MAC address) to provisioning list on PBX, assign extensions to each port and configure corresponding settings.

When you power on and connect the gateway to the same LAN as PBX system, the gateways will be provisioned automatically.

Prerequisites

- Gather information of gateway, including Model and MAC address.
- Prepare an auto provisioning template.

Procedure

1. Log in to PBX management portal, go to Auto Provisioning > Gateways, click Add.
2. In the Gateways section, configure gateway information as follows:
 - Model: Select a gateway model.
 - MAC Address: Enter MAC address of gateway.
 - Remark: Optional. Enter a short description about the gateway.
3. In the Options section, select a desired template from the drop-down list of Template.
4. Assign an extension for each port on gateway.
 - a. In the Port Range field, select the port range to assign extensions.
 - b. In the Start Extension and End Extension field, select the extension range to assign to the specified ports.
 - c. Click Assign Extension.

The ports with assigned extensions are displayed below. You can reassign an extension for a specific port.

Port	Extension
<input checked="" type="checkbox"/> Port 1	1005-Ashley Gardner
<input checked="" type="checkbox"/> Port 2	1006-Dave Harris

- In the Preference section, configure the settings as your need.
 - Key as Send: Assign the pound key (“#”) or asterisk key (“*”) as the send key.
 - SIP VoIPServer IDX: Select a VoIP server template ID to be provisioned.

Note:
SIP VoIPServer IDX is not applicable for TA100 and TA200.

- Admin Password: Set the password for logging in to the gateway web interface.
- LAN Settings: Select the checkbox and configure static IP address for gateway.
 - IP Address: Enter the IP address that is assigned to the gateway.
 - Subnet Mask: Enter the subnet mask.
 - Gateway: Enter the gateway address.
 - Preferred DNS Server: Enter the IP address of preferred DNS server.
 - Alternative DNS Server: Optional. Enter the IP address of alternative DNS server.
 - IP Address 2: Optional. Enter a second IP address for the gateway.

Note:
According to your network environment, you may need to set another IP address to allow users in different IP segment to access the gateway.

- Subnet Mask 2: Optional. Enter another subnet mask for the second IP address.

The following figure shows you an example of Static IP configuration.

- In the Codecs section, select your preferred codec list for gateway.
- Click Save.

Result



The PBX generates a configuration file for gateway.

What to do next

1. Connect your gateway to the same local network as the PBX, and power on your gateway.

The gateway automatically gets the configuration file from the PBX and applies the configurations.

Note:

- If the gateways are previously used, a factory reset is required.
 - The gateways must be in the same network segment as the PBX (for example, the gateways and PBX are all in the network segment 192.168.6.X), or the Auto Provisioning can not take effect.
2. Go to Extension and Trunk > Extension, check extension registration status on Online Status field.
 - : The assigned extension is registered on the gateway.
 - : The assigned extension is unregistered on the gateway.

Modify a Provisioned Gateway Settings

Centralized provisioning enables you to configure gateways with the same settings, you can also customize settings for a specific gateway after provisioning. This topic describes how to modify general settings for a gateway.

Procedures

1. Log in to PBX management portal, Auto Provisioning > Gateways, edit a desired gateway.
2. Modify gateway settings in the Preference and Codecs sections, and click Save.

Note:

If you want to change other settings, click the gateway IP address displayed on the provisioning list to access the gateway web interface, and change the configurations as your need.

The PBX prompts you whether to reboot the gateway.

3. Click OK to reboot the gateway to apply the configurations.

The gateway will automatically apply the changes after reboot.

Reassign an Extension to a Provisioned Gateway

This topic describes how to reassign an extension to a provisioned gateway.

Procedure

1. Log in to PBX management portal, go to Auto Provisioning > Gateways, edit the desired gateway.
2. In the Assign Extension section, select a desired extension for a desired port.

Tip:

If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other device (s).

- To release the previous devices, see [Release an Extension from a Provisioned Gateway](#) or [Release an Extension from a Provisioned Phone](#).
- To associate an extension with multiple devices, see [Allow Multiple Registrations for One Extension Number](#).

3. Click Save.

The PBX generates a configuration file for gateway, and prompts you whether to reboot the gateway.

4. Click OK to reboot the gateway to apply the configurations.

Result

The extension is automatically registered on the gateway port after reboot.

Release an Extension from a Provisioned Gateway

This topic describes how to release an extension from a provisioned gateway port.

Procedure

1. Release the extension from previous port.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit a desired extension.
 - b. Click the Phone tab.
 - c. Click Release From Phone and Yes.
 - d. Click Save.

The extension is released from the gateway.

2. Reboot the gateway to apply the configurations.

Result

The extension is automatically unregistered on the gateway port after reboot.

Apply a New Template to a Provisioned Gateway

If you want to customize a gateway, you can create a custom template and apply the new template to the gateway. This topic describes how to apply a new template to a provisioned gateway.

Prerequisites

[Create a custom auto provisioning template.](#)

Procedure

1. Log in to PBX management portal, go to Auto Provisioning > Gateways, edit a desired gateway.
2. In the Options section, select a desired template from the Template drop-down list.
3. Click Save.

The PBX prompts you whether to reboot the gateway.

4. Click OK to reboot the gateway to apply the configurations.

Result

The configurations in the new template will be applied automatically to the gateway.


Related information

[Update Auto Provisioning template\(s\) to all applicable devices](#)

Reboot Provisioned Gateways

Every time you change settings for a gateway, you need to reboot the gateway to make configurations take effect. This topic describes how to reboot provisioned gateways remotely on PBX management portal.

Procedure

1. Log in to PBX management portal, go to Auto Provisioning > Gateways.
2. Reboot gateways according to your needs:
 - To reboot a gateway, click  beside the desired gateway.
 - To reboot gateways in bulk, select the checkboxes of desired gateways, click Reboot.


The system prompts you whether to reboot the gateways.

3. Click OK.

Remove Gateways from Provisioning List

The provisioning list always displays all the gateways that are discovered. For the out-of-use gateways, you can remove them from the gateways provisioning list manually. This topic describes how to remove out-of-use gateways from provisioning list.

Procedure

1. Remove gateway from provisioning list.
 - a. Log in to PBX management portal, go to Auto Provisioning > Gateways.
 - b. Remove gateways according to your needs:
 - To remove a gateway, click  beside the desired gateways.
 - To remove gateways in bulk, select the checkboxes of the desired gateways, and click Delete.
 - c. Click OK.
2. If the gateways you remove have been provisioned, reboot the provisioned gateways.

Result

For the provisioned gateways, the system erases all configuration files for the gateways and releases the assigned extension.

Manage Auto Provisioning Template

View a Default Auto Provisioning Template

The default template of different models contains different parameters, you can view what configurations are included in the default template. This topic describes how to search and view a default template.

Background information

Yeastar P-Series PBX System provides various default templates for each supported device. Devices of different models may share the same template. For example, the template `YSD-P_YealinkT5xS` of Yealink applies to Yealink T52S and T54S.

The value of default template

The default template contains general settings that are pre-defined based on device model. There are two types of parameter value in the template: variables and absolute value.

- Variables: Variables are attributes to which various values can be assigned. A variable starts with `{{`, and ends with `}}`. For example, `{{.PhoneWebLanguage}}` means a variable of Phone Web Language set-

ting. The phone web language varies on each phone according to specific phone configuration.


- **Absolute value:** Absolute is a fixed value that applies to all devices that use this template. For example, `features.dtmf.hide_delay = 1` means setting the parameter value to 1 (Enabled).

Procedure

1. Log in to PBX management portal, go to Auto Provisioning > Resource Repository.
2. Select a device vendor or enter a keyword.

You can search the template by vendor, provisioning template name, or device model. The search results are displayed automatically on the web page.

Vendor	Template Name	Online Version	Local Version	Supported Model	Operations
Yealink	YSDP_YealinkT5	1.0.3 New!	1.0.0	SIP-T53 SIP-T53W SIP-T54W ...	[Icon] [Icon] [Icon]
Yealink	YSDP_YealinkT29	1.0.1 New!	1.0.0	SIP-T29G	[Icon] [Icon] [Icon]
Yealink	YSDP_YealinkT3	1.0.1 New!	1.0.0	SIP-T30 SIP-T30P SIP-T31 ...	[Icon] [Icon] [Icon]
Yealink	YSDP_YealinkT4	1.0.1 New!	1.0.0	SIP-T41S SIP-T42S SIP-T46S ...	[Icon] [Icon] [Icon]
Yealink	YSDP_FanvilX3U	1.0.0	1.0.0	X1S X1SG X3SG ...	[Icon] [Icon] [Icon]

3. Click  beside the desired template to view the default configurations. The following figure shows a default template of Yealink T56A. The default template consists of two parts:

- **Configuration parameters in Default Template:** The pre-defined configuration parameters in this template are displayed in the first text box.
- **Function keys of device model:** The pre-defined function keys supported by the device model are displayed in the second text box.

You can click the device model tab to view the supported keys.

Check Default Template - YSDP_YealinkT4 X

Configuration Parameters in Default Template

```

local_time.summer_time = {{.DaylightSavingTime}}
local_time.ntp_server1 = {{.PrimaryNtpServer}}
local_time.ntp_server2 = {{.SecondaryNtpServer}}
local_time.time_format = {{.TimeFormat}}
local_time.date_format = {{.DateFormat}}
transfer.dsskey_deal_type = {{.TransferModeViaDsskey}}
features.dtmf.hide = {{.SuppressDtmfDisplay}}
features.dtmf.hide_delay = 1
features.intercom.led.enable = 1
features.intercom.subscribe.enable = 1

```

The configuration parameters below are used to configure function keys, which will define the value of the variables in the default template: {{.FunctionkeySyntax}}.

SIP-T41S	SIP-T42S	SIP-T46S	SIP-T48S	SIP-T41U	SIP-T42U	SIP-T43U
SIP-T46U		SIP-T48U				

```

#FUNCTIONKEY1
linekey.1.type = {{.FunctionkeyType_1}}
linekey.1.line = {{.FunctionkeyLine_1}}
linekey.1.value = {{.FunctionkeyCodeValue_1}}{{.FunctionkeyValue_1}}
linekey.1.label = {{.FunctionkeyLabel_1}}
linekey.1.extension = {{.FunctionkeyCodeExtension_1}}
#FUNCTIONKEY2
linekey.2.type = {{.FunctionkeyType_2}}
linekey.2.line = {{.FunctionkeyLine_2}}

```

Related information

- [Create a Custom Auto Provisioning Template](#)
- [Manage Custom Auto Provisioning Template](#)


Update a Default Auto Provisioning Template

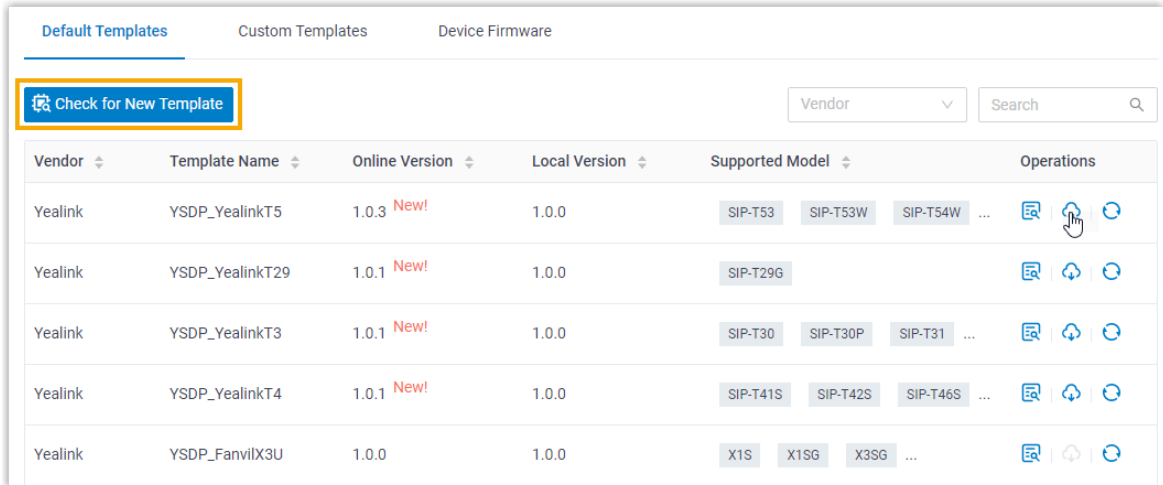
Yeastar P-Series PBX System regularly provides new template versions to release new features and fix bugs. You can check if a new template is available, and decide whether to update the default template. This topic describes how to update a default template.
















Prerequisites


Make sure that your PBX can connect to Internet, or new templates will not be detected

Procedure

1. Log in to PBX management portal, go to Auto Provisioning > Resource Repository.
2. Click Check for New Template to obtain the new template.
3. If a new template is detected, click  to download the new template.




Vendor	Template Name	Online Version	Local Version	Supported Model	Operations
Yealink	YSDP_YealinkT5	1.0.3 New!	1.0.0	SIP-T53 SIP-T53W SIP-T54W ...	  
Yealink	YSDP_YealinkT29	1.0.1 New!	1.0.0	SIP-T29G	  
Yealink	YSDP_YealinkT3	1.0.1 New!	1.0.0	SIP-T30 SIP-T30P SIP-T31 ...	  
Yealink	YSDP_YealinkT4	1.0.1 New!	1.0.0	SIP-T41S SIP-T42S SIP-T46S ...	  
Yealink	YSDP_FanvilX3U	1.0.0	1.0.0	X1S X1SG X3SG ...	  

4. Click  beside the desired template to view the default configurations.

For more information, see [View a Default Auto Provisioning Template](#).

What to do next

To apply the new template to the devices that have been auto provisioned by the same template with previous version, click .

Create a Custom Auto Provisioning Template

If you want to customize the general settings defined in a default provisioning template, or you want to add custom parameters, you can create a custom Auto Provisioning template. This topic describes how to create a custom Auto Provisioning template.

Background information

Custom template allows you to customize device settings. You can easily modify and apply the custom template to a group of devices, or an individual device.

Yeastar P-Series PBX System provides two types of custom template:

- Basic Custom Template: Allow you to customize the parameters provided in the default template.
- Advanced Custom Template: Allow you to customize parameters provided in the default template, and add additional parameters for the desired phones.

**Note:**

Contact your vendor to make sure that the added parameters are supported.

Create a Auto Provisioning basic template

If you want to customize the settings that are defined in a default provisioning template, you can create a basic Auto Provisioning template.

1. Log in to PBX management portal, go to Auto Provisioning > Resource Repository > Custom Templates.
2. Click Add.
3. In the Basic section, set basic information.
 - Template Name: Enter a name to help you identify it.
 - Source Default Template: Select a default provisioning template to customize.
 - Template Type: Select Basic.

The general settings that the source default template provides will be displayed in the Preference, Distinctive Ringtone, and Codecs sections.

- Remark: Optional. Enter a short description about this template.
4. In the Preference section, modify the preference settings that are provided by the source default template.
 5. In the Codecs section, select a desired codec according to your needs.
 6. Click Save.

Create an advanced Auto Provisioning template

If the settings that you want to configure for your devices are not defined in the default provisioning template, you can create an advanced Auto Provisioning template.

1. Log in to PBX management portal, go to Auto Provisioning > Resource Repository > Custom Templates.
2. Click Add.
3. In the Basic section, set the basic information.
 - Template Name: Enter a name to help you identify it.
 - Source Default Template: Select a default template to customize.
 - Template Type: Select Advanced.

The general settings that the source default template provides will be displayed in the Preference, Distinctive Ringtone, and Codecs sections; A text box containing all configuration parameters will be displayed in the Customize Configuration Parameters In Text section.

- Remark: Optional. Enter a short description about this template.
4. In the Preference section, modify the preference settings that are provided by the source default template.
 5. In the Codecs section, select a desired codec according to your needs.
 6. Add additional parameters that are not provided by the source default template.

Note:

The general settings defined in source default template are assigned with variables. The variable that starts with `{{` and ends with `}}` is associated with the configuration that can be configured on Preference, Codecs, and [Function Keys](#) sections. Please don't change the variable if you want to modify the settings from PBX management portal.

- a. In the Customize Configuration Parameters In Text section, add your configuration parameters in the first text box.

Note:

Contact your vendor to make sure that the parameters are supported for the device model.

- b. In the second text box, select which function keys to be applied according to the phone model.

You can also add your function key parameters in the second text box.

The configuration parameters below are used to configure function keys, which will define the value of the variables in the custom template: `{{FunctionkeySyntax}}`. If you need to provision function keys, please do not remove the variables from the custom template.

SIP-T41S SIP-T42S SIP-T46S **SIP-T48S** SIP-T41U SIP-T42U SIP-T43U SIP-T46U SIP-T48U

```
#FUNCTIONKEY1
linekey.1.type = {{FunctionkeyType_1}}
linekey.1.line = {{FunctionkeyLine_1}}
linekey.1.value = {{FunctionkeyCodeValue_1}}{{FunctionkeyValue_1}}
linekey.1.label = {{FunctionkeyLabel_1}}
linekey.1.extension = {{FunctionkeyCodeExtension_1}}

#FUNCTIONKEY2
linekey.2.type = {{FunctionkeyType_2}}
linekey.2.line = {{FunctionkeyLine_2}}
linekey.2.value = {{FunctionkeyCodeValue_2}}{{FunctionkeyValue_2}}
linekey.2.label = {{FunctionkeyLabel_2}}
linekey.2.extension = {{FunctionkeyCodeExtension_2}}
```

7. Click Save.

Related information


[Edit a custom Auto Provisioning template](#)

[Update Auto Provisioning template\(s\) to all applicable devices](#)

Manage Custom Auto Provisioning Template

This topic describes how to edit or delete custom Auto Provisioning templates.

Edit a custom Auto Provisioning template


1. Log in to PBX management portal, go to Auto Provisioning > Resource Repository > Custom Templates.
2. Click  beside a desired custom template.
3. Modify the device settings.

4. Click Save.

The system prompts you whether to update the new configurations to devices that use this template.


- Yes: The system generates new configuration files and immediately triggers provisioning for all devices that use this template.
- No: The system saves the changes to this template, and generates new configuration files for all devices that use this template. You can trigger provisioning manually for specific devices later.

Delete custom Auto Provisioning templates

1. Log in to PBX management portal, go to Auto Provisioning > Resource Repository > Custom Templates.
2. Delete custom templates according to your needs.
 - To delete a custom template, click  beside the desired template.
 - To delete custom templates in bulk, select the checkboxes of desired templates, click Delete.
3. In the pop-up dialog box, click Yes.

If the template is in use, you need to release it from the devices that use the template first.

Update Auto Provisioning template(s) to all applicable devices

1. Log in to PBX management portal, go to Auto Provisioning > Resource Repository > Custom Templates.
2. Update the configurations to the devices:
 - To update the configuration of a specific template, click  beside the desired template.
 - To update the configuration of multiple templates, select the checkboxes of desired templates, click Update to Device.
3. Click Yes to trigger phone provisioning.

Manage Device Firmware

Manage Device Firmware Files

This topic describes how to manage device firmwares, including add, edit, and delete device firmware files.


Add a device firmware file

You can upload up to three device firmware files to PBX server.


1. Log in to PBX management portal, go to Auto Provisioning > Resource Repository > Device Firmware, click Add.
2. In the Device section, select a firmware vendor and device model.
3. In the Firmware section, upload the firmware.
 - Firmware Version: Enter a name (firmware version) to help you identify it.
 - Upload Firmware File: Click Browse and select the corresponding firmware.
 - Remark: Optional. Enter a short description about the firmware.
4. Click Save.

The uploaded firmware is displayed on the Device Firmware list. When you update phone firmware, the uploaded firmware can be detected and displayed for you to choose.

Edit a device firmware file

1. Log in to PBX management portal, go to Auto Provisioning > Resource Repository > Device Firmware.
2. Click  beside the desired firmware.
3. In the Firmware section, edit the firmware information or update the firmware file.
 - Firmware Version: Enter a name (firmware version) to help you identify it.
 - Upload: Click Browse and select the corresponding firmware.
 - Remark: Optional. Edit the note.
4. Click Save.

Delete device firmware files

1. Log in to PBX management portal, go to Auto Provisioning > Resource Repository > Device Firmware.
2. Delete device firmware files.
 - To delete a device firmware, click  beside the desired firmware.
 - To delete device firmwares in bulk, select the checkboxes of the desired firmware, and click Delete.
3. Click OK.

Auto Provisioning - Supported Devices

This topic lists the devices that are currently supported for Auto Provisioning by Yeastar P-Series PBX System.

Yealink phones

Model	Phone Requirement	PBX Requirement
SIP-T19P_E2	53.84.0.125 or later	37.2.0.7 or later

Model	Phone Requirement	PBX Requirement
SIP-T21P_E2	52.84.0.125 or later	37.2.0.7 or later
SIP-T21_E2	52.84.0.125 or later	37.2.0.7 or later
SIP-T23P	44.84.0.125 or later	37.2.0.7 or later
SIP-T23G	44.84.0.125 or later	37.2.0.7 or later
SIP-T27G	69.85.0.5 or later	37.2.0.7 or later
SIP-T29G	46.83.0.120 or later	37.2.0.7 or later
SIP-T30	124.85.0.15 or later	37.2.0.7 or later
SIP-T30P	124.85.0.15 or later	37.2.0.7 or later
SIP-T31	124.85.0.15 or later	37.2.0.7 or later
SIP-T31P	124.85.0.15 or later	37.2.0.7 or later
SIP-T31G	124.85.0.15 or later	37.2.0.7 or later
SIP-T33P	124.85.0.15 or later	37.2.0.7 or later
SIP-T33G	124.85.0.15 or later	37.2.0.7 or later
SIP-T40P	54.84.0.125 or later	37.2.0.7 or later
SIP-T40G	76.84.0.125 or later	37.2.0.7 or later
SIP-T41P	36.83.0.120 or later	37.2.0.7 or later
SIP-T42G	29.83.0.120 or later	37.2.0.7 or later
SIP-T46G	28.83.0.120 or later	37.2.0.7 or later
SIP-T48G	35.83.0.120 or later	37.2.0.7 or later
SIP-T41S	66.85.0.5 or later	37.2.0.7 or later
SIP-T42S	66.85.0.5 or later	37.2.0.7 or later
SIP-T46S	66.85.0.5 or later	37.2.0.7 or later
SIP-T48S	66.85.0.5 or later	37.2.0.7 or later
SIP-T41U	108.85.0.39 or later	37.2.0.7 or later
SIP-T42U	108.85.0.39 or later	37.2.0.7 or later
SIP-T43U	108.85.0.39 or later	37.2.0.7 or later
SIP-T46U	108.85.0.39 or later	37.2.0.7 or later
SIP-T48U	108.85.0.39 or later	37.2.0.7 or later

Model	Phone Requirement	PBX Requirement
SIP-T52S	70.84.0.70 or later	37.2.0.7 or later
SIP-T54S	70.84.0.70 or later	37.2.0.7 or later
SIP-T53	96.85.0.5 or later	37.2.0.7 or later
SIP-T53W	96.85.0.5 or later	37.2.0.7 or later
SIP-T54W	96.85.0.5 or later	37.2.0.7 or later
SIP-T57W	96.85.0.5 or later	37.2.0.7 or later
SIP-T56A	58.83.0.15 or later	37.2.0.7 or later
SIP-T58	58.85.0.5 or later	37.2.0.7 or later
SIP-T58W	150.86.0.5 or later	37.2.0.7 or later
VP59	91.85.0.5 or later	37.2.0.7 or later
W80B	W80DM-103.83.0.80	37.2.0.7 or later
W60B	77.83.0.85 or later	37.2.0.7 or later
W70B	146.85.0.20 or later	37.2.0.7 or later
W90DM	130.85.0.15 or later	37.2.0.80 or later
CP960	73.85.0.5 or later	37.2.0.7 or later
CP920	78.85.0.5 or later	37.2.0.7 or later

Fanvil phones

Model	Phone Requirement	PBX Requirement
X1S / X1SP	2.2.12 or later	37.2.0.80 or later
X1SG	2.2.12 or later	37.2.0.80 or later
X3SG	2.2.12 or later	37.2.0.80 or later
X3U	2.2.12 or later	37.2.0.80 or later
X4U	2.2.11 or later	37.2.0.80 or later
X5U	2.2.11 or later	37.2.0.80 or later
X5S	2.2.1 or later	37.2.0.80 or later
X6	2.2.1 or later	37.2.0.80 or later
X6U	2.2.11 or later	37.2.0.80 or later
X7	2.2.11 or later	37.2.0.80 or later

Model	Phone Requirement	PBX Requirement
X7C	2.2.11 or later	37.2.0.80 or later
X7A	2.2.0.229 or later	37.2.0.80 or later
X210	2.2.11 or later	37.2.0.80 or later
X210i	2.2.11 or later	37.2.0.80 or later
X3S Lite / X3SP Lite	2.4.5 or later	37.2.0.80 or later
X3S Pro / X3SP Pro	2.4.5 or later	37.2.0.80 or later
X3SW	2.4.5 or later	37.2.0.80 or later
X3SG Lite	2.4.5 or later	37.2.0.80 or later
X3SG Pro	2.4.5 or later	37.2.0.80 or later
X3U Pro	2.4.5 or later	37.2.0.80 or later
H3	2.12.1.7334 or later	37.3.0.42 or later
H5	2.12.1.7334 or later	37.3.0.42 or later
H2U	2.4.7 or later	37.3.0.42 or later
H3W	2.4.4 or later	37.3.0.42 or later
H5W	2.4.4 or later	37.3.0.42 or later
i56A	0.3.0.21 or later	37.3.0.42 or later
i51	2.8.13 or later	37.3.0.42 or later
i52	2.8.13 or later	37.3.0.42 or later
i53	2.8.13 or later	37.3.0.42 or later
i51W	2.8.13 or later	37.3.0.42 or later
i52W	2.8.13 or later	37.3.0.42 or later
i53W	2.8.13 or later	37.3.0.42 or later

Grandstream phones

Model	Phone Requirement	PBX Requirement
GXP1610	1.0.7.13 or later	37.3.0.42 or later
GXP1620	1.0.7.13 or later	37.3.0.42 or later
GXP1625	1.0.7.13 or later	37.3.0.42 or later
GXP1628	1.0.7.13 or later	37.3.0.42 or later

Model	Phone Requirement	PBX Requirement
GXP1630	1.0.7.13 or later	37.3.0.42 or later
GXP2130	1.0.11.16 or later	37.3.0.42 or later
GXP2135	1.0.11.16 or later	37.3.0.42 or later
GXP2140	1.0.11.16 or later	37.3.0.42 or later
GXP2160	1.0.11.16 or later	37.3.0.42 or later
GXP2170	1.0.11.16 or later	37.3.0.42 or later

Htek phones

Model	Phone Requirement	PBX Requirement
UC902	2.0.4.8.18 or later	37.4.0.17 or later
UC902S	2.0.4.8.18 or later	37.4.0.17 or later
UC903	2.0.4.8.18 or later	37.4.0.17 or later
UC912	2.0.4.8.18 or later	37.4.0.17 or later
UC912G	2.0.4.8.18 or later	37.4.0.17 or later
UC912E	2.0.4.8.18 or later	37.4.0.17 or later
UC921	2.0.4.8.18 or later	37.4.0.17 or later
UC921G	2.0.4.8.18 or later	37.4.0.17 or later
UC923	2.0.4.8.18 or later	37.4.0.17 or later
UC923U	2.0.4.8.18 or later	37.4.0.17 or later
UC924	2.0.4.8.18 or later	37.4.0.17 or later
UC924E	2.0.4.8.18 or later	37.4.0.17 or later
UC924U	2.0.4.8.18 or later	37.4.0.17 or later
UC924W	2.0.4.8.18 or later	37.4.0.17 or later
UC926	2.0.4.8.18 or later	37.4.0.17 or later
UC926E	2.0.4.8.18 or later	37.4.0.17 or later
UC926U	2.0.4.8.18 or later	37.4.0.17 or later

Gigaset phones

Model	Phone Requirement	PBX Requirement
N870 IP PRO	2.38.1 or later	37.3.0.42 or later
N870 VI PRO	2.38.1 or later	37.3.0.42 or later
N670 IP PRO	2.38.1 or later	37.3.0.42 or later
N610 IP PRO (Coming soon)	N/A	37.3.0.42 or later
Maxwell Basic PRO	3.18.1 or later	37.3.0.42 or later
Maxwell 2 PRO	3.18.1 or later	37.3.0.42 or later
Maxwell 3 PRO	3.18.1 or later	37.3.0.42 or later
Maxwell 4 PRO	3.18.1 or later	37.3.0.42 or later

Snom phones

Model	Phone Requirement	PBX Requirement
D120	10.1.54.13 or later	37.4.0.17 or later
D315	10.1.73.16 or later	37.4.0.17 or later
D335	10.1.73.16 or later	37.4.0.17 or later
D385	10.1.73.16 or later	37.4.0.17 or later
D717	10.1.73.16 or later	37.4.0.17 or later
D735	10.1.73.16 or later	37.4.0.17 or later
D785	10.1.73.16 or later	37.4.0.17 or later

FlyingVoice phones

Model	Phone Requirement	PBX Requirement
FIP10	0.6.16 or later	37.3.0.42 or later
FIP11C	0.6.16 or later	37.3.0.42 or later
FIP12WP	0.6.16 or later	37.3.0.42 or later
FIP13G	0.6.16 or later	37.3.0.42 or later
FIP14G	0.6.16 or later	37.3.0.42 or later
FIP15G	0.6.16 or later	37.3.0.42 or later

Model	Phone Requirement	PBX Requirement
FIP15G Plus	0.6.16 or later	37.3.0.42 or later
FIP16	0.6.16 or later	37.3.0.42 or later
FIP16 Plus	0.6.16 or later	37.3.0.42 or later


Yeastar gateways

Model	Gateway Firmware	PBX Requirement
TA100	44.19.86.30 or later	37.2.0.80 or later
TA200	44.19.86.30 or later	37.2.0.80 or later
TA400	41.19.0.32 or later	37.2.0.80 or later
TA800	41.19.0.32 or later	37.2.0.80 or later
TA1600	47.0.0.54 or later	37.2.0.80 or later
TA2400	47.0.0.54 or later	37.2.0.80 or later
TA3200	47.0.0.54 or later	37.2.0.80 or later

Auto Provisioning - Variables in Templates

The provision templates make use of a set of variables that are replaced by the actual value when a device is provisioned. This topic shows you the variables used in the provisioning templates.


Variable	Description
Preference settings	
{{.PhoneWebLanguage}}	The language configured on phone web interface.
{{.PhoneLanguage}}	The language configured on phone interface.
{{.Tones}}	The default ringtone of the phone.
{{.CallWaiting}}	Enable or disable call waiting feature.
{{.PhoneUser}}	The user name for logging in to the phone web interface.
{{.PhonePassword}}	The password for logging in to the phone web interface.

Variable	Description
{{.TimeZone}}	The time zone.
{{.TimeZoneName}}	The time zone name.
{{.DaylightSavingTime}}	The daylight saving time.
{{.PrimaryNtpServer}}	The primary NTP server address.
{{.SecondaryNtpServer}}	The second NTP server address.
{{.TimeFormat}}	The time format.
{{.DateFormat}}	The date format.
{{.DateSeparatorFormat}}	The date separator format.
{{.TransferModeViaDsskey}}	The transfer mode for function key.
{{.SuppressDtmfDisplay}}	Enable or disable the IP phone to suppress the display of DTMF digits.
{{.AutoProvisionServerUrl}}	The URL of provision server.
{{.AutoProvisionServerUrlWithoutProtocol}}	The URL of provision server without transport protocol.
{{.ProvisioningFile}}	The name of configuration file.
{{.FirmwareUrl}}	The URL of firmware.
{{.FirmwareUrlWithoutProtocol}}	The URL of firmware without transport protocol.
{{.FirmwareFile}}	The name of firmware.
{{.FirmwareVersion}}	The version of firmware.
{{.EnableUacsta}}	Enable or disable uaCSTA.
{{.AlertInfoText_X}}	The alert info text to trigger the IP phone to play a specific ring tone.
{{.AlertInfoRingtone_X}}	The specific ring tone corresponding to Alert info.
Contact settings for Yealink phones	
 Note: Contact settings are not available for VP59, W80B, W60B, W90DM, CP960, and CP920 phones.	
{{.CompanyPbUrl}}	The URL of company contact file.
{{.CompanyPbName}}	The name of company contact.

Variable	Description
{{.PersonalPbUrl}}	The URL of personal contact file.
{{.PersonalPbName}}	The name of personal contact.
Account settings for IP phones	
{{.EnbAccount}}	Enable or disable extension registration.
{{.AccountLabel}}	The extension label.
{{.AccountDisplayName}}	The display name of extension.
{{.AccountRegistrationName}}	The registration name of extension.
{{.AccountRegistrationExtNumber}}	The registration number of extension.
{{.AccountRegistrationPassword}}	The registration password of extension.
{{.AccountSipServerAddr}}	The URL of PBX server for extension registration.
{{.AccountSipServerPort}}	The port of PBX server for extension registration.
{{.AccountSipServerTransport-Type}}	The type of transport protocol for extension registration.
{{.AutoAnswer}}	Enable or disable auto answer feature.
{{.CheckVoicemail}}	The voicemail feature code.
Account settings for DECT phones(x is the handset ID)	
{{.EnbAccount_x}}	Enable or disable extension registration.
{{.AccountLabel_x}}	The extension label.
{{.AccountDisplayName_x}}	The display name of extension.
{{.AccountRegistrationName_x}}	The registration name of extension.
{{.AccountRegistrationExtNumber_x}}	The registration number of extension.
{{.AccountRegistrationPassword_x}}	The registration password of extension.
{{.AccountSipServerAddr_x}}	The URL of provisioning server for extension registration.
{{.AccountSipServerPort_x}}	The port of provisioning server for extension registration.

Variable	Description
{{.AccountSipServerTransport-Type_x}}	The type of transport protocol for extension registration.
{{.CheckVoicemail_x}}	The voicemail feature code.
SIP server template for Yealink W80B(x is the template ID, X=1, 2 or 3)	
{{.TemplateName_x}}	The template name.
{{.TemplateServerAddr_x}}	The URL of PBX server for extension registration.
{{.TemplateServerPort_x}}	The port of PBX server for extension registration.
{{.AccountSipServerTemplate}}	The type of transport protocol for extension registration.
Audio codec(x is the codec priority, X=1, 2, 3 or 4)	
{{.AccountAudioCodec_X}}	The priority of the audio codec.
{{.AudioCodecsPriorities}}	The priority of the audio codec.
{{.AccountCodecPcmu}}	Enable or disable PCMU audio codec.
{{.AccountCodecPcmu_Priority}}	The priority of the PCMU audio codec.
{{.AccountCodecPcma}}	Enable or disable PCMA audio codec.
{{.AccountCodecPcma_Priority}}	The priority of the PCMA audio codec.
{{.AccountCodecllbc}}	Enable or disable iLBC audio codec.
{{.AccountCodecllbc_Priority}}	The priority of the iLBC audio codec.
{{.AccountCodecllbc_15_2_Kbps}}	Enable or disable iLBC_15_2 audio codec.
{{.AccountCodecllbc_15_2_Kbps_Priority}}	The priority of the iLBC_15_2 audio codec.
{{.AccountCodecllbc_13_33_Kbps}}	Enable or disable iLBC_13_33 audio codec.
{{.AccountCodecllbc_13_33_Kbps_Priority}}	The priority of the iLBC_13_33 audio codec.
{{.AccountCodecG722}}	Enable or disable G722 audio codec.
{{.AccountCodecG722_Priority}}	The priority of the G722 audio codec.
{{.AccountCodecG729}}	Enable or disable G729 audio codec.
{{.AccountCodecG729_Priority}}	The priority of the G729 audio codec.
{{.AccountCodecG726_32}}	Enable or disable G726_32 audio codec.

Variable	Description
{{.AccountCodecG726_32_Priority}}	The priority of the G726_32 audio codec.
{{.AccountCodecSpeex}}	Enable or disable Speex audio codec.
{{.AccountCodecSpeex_Priority}}	The priority of the Speex audio codec.
{{.AccountAdpcmCodec}}	Enable or disable Adpcm audio codec.
{{.AccountCodecAdpcm_Priority}}	The priority of the Adpcm audio codec.
::{{.AccountCodecMpeg4}}	Enable or disable Mpeg4 audio codec.
{{.AccountCodecMpeg4_Priority}}	The priority of the Mpeg4 audio codec.
{{.AccountCodecGsm}}	Enable or disable GSM audio codec.
{{.AccountCodecGsm_Priority}}	The priority of the GSM audio codec.
{{.AccountCodecOpus}}	Enable or disable Opus audio codec.
{{.AccountCodecOpus_Priority}}	The priority of the Opus audio codec.
Video codec(x is the codec priority, X=1, 2, 3 or 4)	
{{.AccountVideoCodec_X}}	The priority of the video codec.
{{.AccountCodecH264}}	Enable or disable H264 codec.
{{.AccountCodecH264_Priority}}	The priority of the H264 codec.
{{.AccountCodecH264_Hp}}	Enable or disable H264_Hp codec.
{{.AccountCodecH264_Hp_Priority}}	The priority of the H264_Hp codec.
{{.AccountCodecH263}}	Enable or disable H263 codec.
{{.AccountCodecH263_Priority}}	The priority of the H263 codec.
{{.AccountCodecH263_P}}	Enable or disable H263_P codec.
{{.AccountCodecH263_P_Priority}}	The priority of the H263_P codec.
{{.AccountCodecVp8}}	Enable or disable Vp8 codec.
{{.AccountCodecVp8_Priority}}	The priority of the Vp8 codec.
Function key (x is the function key ID)	
{{.FunctionkeyType_x}}	The type of function key.
{{.FunctionkeyType2_x}}	The type of function key (for Dynamic VPK).
{{.FunctionkeySubtype_x}}	The subtype of function key.
{{.FunctionkeyLine_x}}	The extension to which function key applies.

Variable	Description
{{.FunctionkeyCodeValue_x}}	The feature code of function key.
{{.FunctionkeyValue_x}}	The object of function key.
{{.FunctionkeyExtension_x}}	The number where the call can be picked up by function key.
{{.FunctionkeyCodeExtension_x}}	The pickup code applied for function key.
{{.FunctionkeyLabel_x}}	The label of function key that is displayed on phone screen.
Gateway	
{{.KeyAsSend}}	Enable or disable Key as Send feature.
{{.SipVoipServerIdx}}	The VoIP server template ID.
{{.AdminPassword}}	The admin password.
{{.EnbLanSettings}}	Enable or disable LAN settings.
{{.Hostname}}	The host name.
{{.LanIpAddress}}	The primary IP address of LAN port.
{{.LanSubnetMask}}	The subnet mask of LAN port.
{{.LanGateway}}	The gateway of LAN Port.
{{.LanPrimaryDns}}	The primary DNS of LAN port.
{{.LanSecondaryDns}}	The secondary DNS of LAN Port.
{{.LanIpAddress2}}	The secondary IP address of LAN port.
{{.LanSubnetMask2}}	The secondary subnet mask of LAN port.
{{.PppoeUsername}}	The user name of PPPoE.
{{.PppoePassword}}	The password of PPPoE.
Others	
{{.MacAddress}}	The MAC address of phone. <div data-bbox="737 1598 1386 1724" style="border: 1px solid #00aaff; padding: 5px; margin-top: 10px;">  Note: Here the value does not need a separator of :. For example, 09139876900e. </div>

User Role

User Roles and Permissions

Yeastar P-Series PBX System allows super administrator to have a role-based control over the PBX features that are accessible and manageable on users' management portals. This topic describes what is a user role, and introduces the pre-defined user roles and their permissions.

What is a user role

A user role includes a set of permissions, which allows super administrator to control what PBX features users can manage on users' management portals.

Super administrator can assign user roles to employees based on their job duties, each user role has different permissions. For example, you can assign Operator to an employee who is responsible for security of PBX server and network; assign Human Resource to an employee who is responsible for dealing with employee profiles.

Pre-defined user roles

Yeastar P-Series PBX System has pre-defined user roles that cover the most common permission configurations. The pre-defined user roles and their permissions are as follows:

Table 21.


Role	Permission
Super administrator	Access and manage all the PBX features. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> Note: The username of super administrator is created when you first configure the system, and the username is unchangeable.</div>
Administrator	Access and manage all the PBX features except the followings: <ul style="list-style-type: none">• View Dashboard• Manage Role
Supervisor	No access to PBX features.
Operator	Access and manage all the features under Security and Maintenance modules. For more information, see Security and Maintenance .
Employee	No access to PBX features.

Table 21. (continued)

Role	Permission
Human Resource	View and manage all the extensions.
Accounting	Access and manage Plan.

Create a User Role

If the pre-defined roles can not meet your need, you can create a user role and grant permissions to the role. This topic describes how to create a user role.

Create a new role

Based on an employee's job duty, you can create a user role and grant corresponding permissions.

1. Log in to PBX management portal, go to Extension and Trunk > Role, click Add.
2. In the Role Name field, enter a name to help you identify it.
3. Grant permissions to the user role.

For permission details, see [User Role Permissions](#).


4. Click Save.

Create a role by copying an existing role

You can create a role based on an existing user role, the new role automatically inherits permissions from the existing role. After copying permissions, you can add or remove permissions as needed.

1. Log in to PBX management portal, go to Extension and Trunk > Role.
2. Create a role.
 - a. Click Copy Role.
 - b. In the Choose a role to copy drop-down list, select a role.
 - c. In the Role Name field, enter a name to help you identify the role.
 - d. Click Save.

The new role inherits permissions from the existing role.

3. Update permissions for the newly created role.
 - a. On Role list, click  beside the role that you have created.
 - b. Select or unselect the checkboxes of the desired permissions.

For permission details, see [User Role Permissions](#).

- c. Click Save.

What to do next

[Assign a Role to a User.](#)


Assign a Role to a User

This topic describes how to assign a role to a user.

Prerequisites

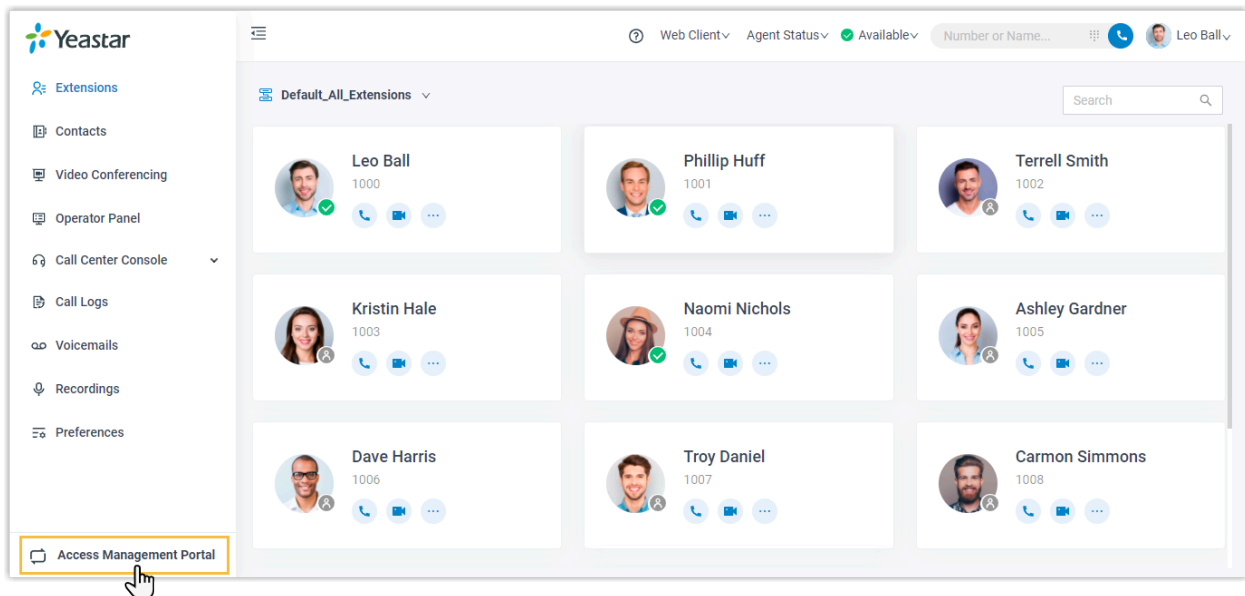
[A user role is created.](#)

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. On Extension list, select an extension, click .
3. On the User page, select a role from the drop-down list of User Role.
4. Click Save and Apply.

Result

If specific permissions are granted to the role, after the user logs in to Linkus Web Client, the user can go to management portal, and access specific system features.




Manage User Roles

This topic describes how to edit or delete roles.


Edit a role

After creating a role, you can edit role permissions according to your needs.

1. Log in to PBX management portal, go to Extension and Trunk > Role.
2. On Role list, select a role, click .
3. Edit the role name or change role permissions according to your needs.
For permission details, see [User Role Permissions](#).
4. Click Save.

Delete roles

If you don't need roles, you can delete them. After roles are deleted, users with the roles assigned will have no role definition.

1. Log in to PBX management portal, go to Extension and Trunk > Role.
2. Delete one or more roles according to your needs.
 - To delete a role, select a role, click  and OK.
 - To delete roles in bulk, select the checkboxes of the desired roles, click Delete and OK.

User Role Permissions

This topic describes all the available permissions that can be granted to a role.

Available permissions on Yeastar P-Series PBX System are as follows:

- [Extension and Trunk](#)
- [Contacts](#)
- [Call Control](#)
- [Call Features](#)
- [Reports and Recordings](#)
- [Auto Provisioning](#)
- [PBX Settings](#)
- [System](#)
- [Security](#)
- [Maintenance](#)
- [Integration](#)
- [Plan](#)

Extension and Trunk

Specify the extensions that users with the role assigned can manage, and whether users can manage extension group or trunks.

Table 22.

Module	Permission
Extension	<ul style="list-style-type: none"> • All Extensions: View and manage all the extensions. For example, grant the permission to a human resource. If there are changes of employees, the human resource can update extensions timely. • All the other extensions of the same Extension Groups: Manage or send Linkus welcome emails to all the other extensions in the same extension group except the one that contains all the extensions. For example, grant the permission to a supervisor. The supervisor can view and manage his or her subordinates' extensions. • Specific Extensions: Manage or send Linkus welcome emails to specific extensions. For example, grant the permission to a leader. The leader can view and manage different departments' extensions. • Extension itself only: Manage or send Linkus welcome emails to his or her own extension.
Extension Group	Manage extension groups.
Trunks	Manage trunks.

Contacts

Specify whether users with the role assigned can manage the following features:

- Company Contacts
- PhoneBooks



Note:

The feature is only available for Enterprise/Ultimate Plan.

Call Control

Specify whether users with the role assigned can manage the following features:

- Inbound Route
- Outbound Route
- Business Hours and Holidays
- Emergency Number

Call Features

Specify whether users with the role assigned can manage the following features:

- Voicemail
- Feature Code
- IVR
- Ring Group
- Queue
- Conference
- Speed Dial
- Paging/Intercom
- Recording
- PIN List

Reports and Recordings

Specify users with the role assigned can view or manage which extensions' CDR and recordings, and whether users can access call reports.

Table 23.

Module	Permission
CDR and Recording Files	Specify users with the role assigned can view which extensions' CDR and recordings. <ul style="list-style-type: none"> • All Extensions: View all extensions' CDR and recordings. • All the other extensions of the same Extension Groups: View CDR and recordings of all the other extensions of the same group except the one that contains all the extensions. • Specific Extensions: View CDR and recordings of specific extensions or extension.
	Specify how users with the role assigned can manage CDR. <ul style="list-style-type: none"> • Download • Delete
	Specify how users with the role assigned can manage recording files. <ul style="list-style-type: none"> • Play • Download • Delete

Table 23. (continued)

Module	Permission
Call Reports	Specify whether users with the role assigned can access call reports.

Auto Provisioning

Specify whether users with the role assigned can manage Auto Provisioning.

PBX Settings

Specify whether users with the role assigned can manage the following features:

- Preferences
- Voice Prompt
- SIP Settings
- Jitter Buffer

System

Specify whether users with the role assigned can manage the following features:

- Network
- Date and Time
- Email
- Storage
- Event Notification

Security

Specify whether users with the role assigned can manage the following features:

- Security Rules
- Security Settings

Maintenance

Specify whether users with the role assigned can manage the following features:

- Upgrade
- Backup and Restore
- Reboot
- Reset
- Operation Logs
- Troubleshooting
- System Logs

Integration

Specify whether users with the role assigned can manage the following features:

- CRM
- Speech to Text
- AMI
- Database Grant

Plan

Specify whether users with the role assigned can buy or enable free trial of Yeastar-provided plan.

Linkus Server

Linkus Overview


Yeastar Linkus is designed to keep you connected with colleagues and business anywhere and anytime. This topic describes Linkus server, Linkus client, Linkus client login methods, and Linkus events.

Linkus server

To get started with Linkus, you need to set up Linkus server and enable Linkus clients for users. Yeastar P-Series PBX System allows you to set up Linkus server in two ways:

- Auto configuration by Remote Access Service

Remote Access Service (RAS) is a subscription-based service designed for remote working. After RAS is subscribed, you can bind a Yeastar FQDN to the PBX, and the following functions will be provided:


 Note:
RAS provides remote access, not remote control.

- Secure connection
- Remote access of PBX web
- Network Address Translation (NAT) for Linkus service auto configured
- Linkus server for remote access auto configured

For more information about Linkus auto configuration by RAS , see [Set up Linkus Server with Remote Access Service](#).

- Manual configuration

Manual configuration of Linkus remote server requires professional network knowledge.

 Note:

- Weak network protection will cause SIP attacks.
- Incorrect configurations may cause a one-way audio issue.

For more information about manual configuration, see [Manually Set up Linkus Server](#).

Linkus client

Yeastar P-Series PBX System supports the following Linkus clients:

- Linkus Mobile Client
- Linkus Desktop Client

- Linkus Web Client

For more information about Linkus Mobile Client and Linkus Desktop Client, see [Linkus Help Center](#).

For more information about Linkus Web Client, see [Linkus Web Client User Guide](#).

Linkus client login methods

Yeastar P-Series PBX System allows users to quickly log in to Linkus clients via a specific link or QR code, or manually log in by entering the provided credentials.

- Quick login
 - Login link: Provide users with login links so that they can quickly log in to Linkus clients.
 - Login QR code: Provide users with login QR codes so that they can quickly log in to Linkus Mobile Client.

You can copy and share login credential of a specific client with a user, or bulk send Linkus welcome emails to multiple users, which contain login credentials of all the Linkus clients.


For more information, see [Configure Linkus Welcome Email](#) and [Send Linkus Welcome Emails](#).

- Manual login

Depending on different kinds of Linkus server that you have set up, you need to provide different information for users to log in to Linkus clients.

Table 24.

Linkus Server	Mobile & Desktop Login Credentials	Web Client Login Credentials
Linkus Server (RAS)	<ul style="list-style-type: none"> ◦ The PBX's serial number or the FQDN that is bound with the PBX ◦ Username <p>Username can be extension number or email address, which depends on how you Configure Linkus Login Mode.</p> <ul style="list-style-type: none"> ◦ User password 	
Linkus Server (Manual configuration)	<ul style="list-style-type: none"> ◦ PBX's local IP address and local Linkus port ◦ PBX's public IP address or domain name and external Linkus port ◦ Username 	No supported.

Linkus Server	Mobile & Desktop Login Credentials	Web Client Login Credentials
	<div data-bbox="646 300 959 569" style="border: 1px solid #0070C0; background-color: #E6F2FF; padding: 5px;">  Note: Username can be extension number or email address, which depends on how you Configure Linkus Login Mode. </div> <ul style="list-style-type: none"> ◦ User password 	

Linkus events

Yeastar P-Series PBX System provides event notification feature, which records events in logs and notifies relevant contacts via specific notification methods when events occur.

Yeastar P-Series PBX System provides the following Linkus events:

- Web User Login Success
- Web User Login Failed
- Linkus Client Login Failed
- Extension User Password Changed
- Web User Locked Out
- Linkus User Blocked Out

For more information, see [Event Notification Overview](#) and [Configure Event Notifications](#).


Set up Linkus Server with Remote Access Service

After you subscribe Yeastar P-Series Enterprise Plan or Ultimate Plan to get Remote Access Service, users can remotely access Linkus Mobile Client and Desktop Client. To allow remote access to Linkus Web Client, you need to further configure a Yeastar-supplied Fully Qualified Domain Name (FQDN) on the system.

Background information

Remote Access Service (RAS) is included in both Yeastar P-Series Enterprise Plan and Ultimate Plan. You can subscribe either of the two plans to get RAS. With RAS, you can enjoy the following features:

- Linkus server is automatically set up for remote access with the PBX Serial Number.

 Note:

Only remote access to Linkus Mobile Client and Desktop Client is supported. For remote access to Linkus Web Client, further network configurations are required.

Remote Access Service

Remote Access Service is a subscription-based turnkey remote working solution. It provides an easy-to-access domain name, safeguards PBX remote web access, and allows the remote workforce to enjoy a consistent in-office unified communications experience with Linkus UC Clients anywhere, on any device. [Buy Plan](#)

Status

● Connected

Serial Number

3631A2124788

Expiration Date

2023/12/01

- A Fully Qualified Domain Name (FQDN) can be quickly set up to complete the remote working solution with all Linkus clients (Mobile Client, Desktop Client, and Web Client).

Procedure

1. Log in to PBX management portal, go to System > Network > Yeastar FQDN.
2. Turn on Yeastar FQDN.
3. In the Fully Qualified Domain Name (FQDN) field, select a domain name then enter a hostname.

For example, select domain name ras.yeastar.com and enter hostname yeastardocs, you will get an FQDN yeastardocs.ras.yeastar.com

Note:
Think twice before you enter the hostname. The FQDN cannot be changed after you save the configurations.

Yeastar FQDN

Remote Access Service is a subscription-based service designed to set your team up for anywhere-anytime productivity instantly and securely. It provides an easy-to-access domain name, safeguards PBX remote web access, and allows the remote workforce to enjoy a consistent in-office unified communications experience with Linkus UC Clients anywhere on any device. [Buy Plan](#)

Status

● Disconnected

* Fully Qualified Domain Name (FQDN)

yeastardocs ras.yeastar.com

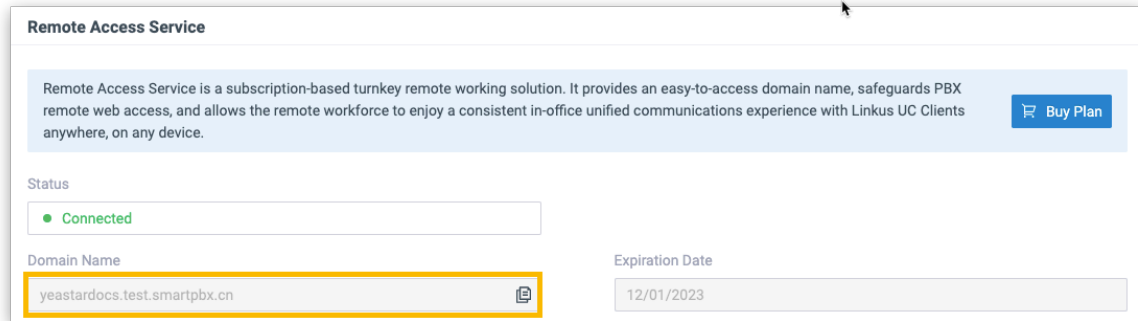
* Expiration Date

Ⓞ The domain name is available.

4. Click Save.

Result

- Linkus server is automatically set up for remote access with the FQDN. The following information is displayed on the Linkus Server page:



- Status: Connected, which means that Linkus server is set up successfully.
 - Domain Name: The domain name is used as a unique identifier for Linkus remote access.
 - Expiration Date: When the service will expire.
- Users can use Linkus (Mobile Client, Desktop Client, and Web Client) anywhere any-time.

Note:

For Linkus Mobile Client and Desktop Client, the App version should be updated:

- Linkus Android version: 3.6.9 or later
- Linkus iOS version: 3.6.8 or later
- Linkus Windows version: 2.4.8 or later
- Linkus MacOS version: 2.4.8 or later

What to do next

- [Configure Linkus Login Mode](#)
- [Enable Linkus clients for users](#)

Manually Set up Linkus Server

This topic describes how to manually set up Linkus server according to different network scenarios.

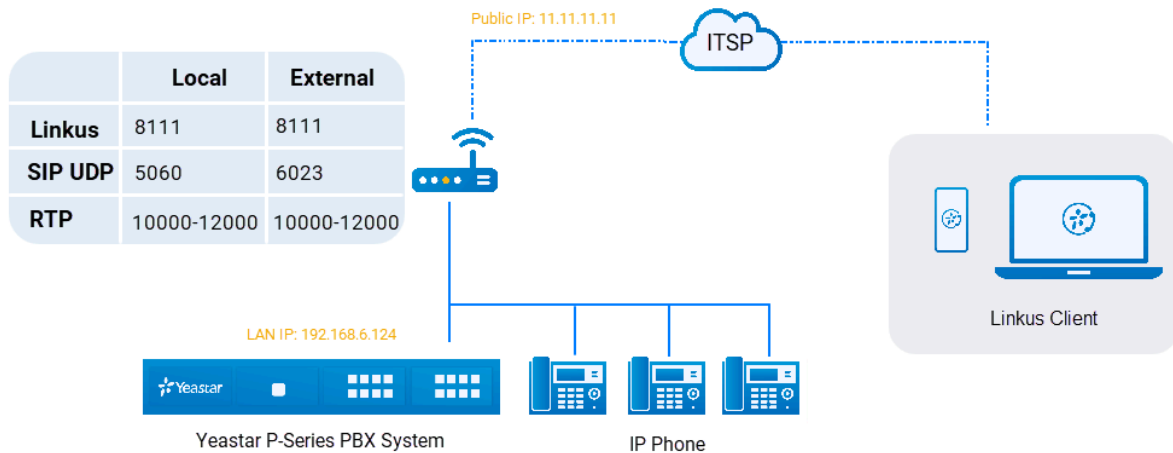
Restrictions

To allow users to remotely use Linkus Web Client, you need to subscribe Enterprise Plan or Ultimate Plan, and set up Linkus server with Remote Access Service (RAS).

For more information, see [Set up Linkus Server with Remote Access Service](#).

PBX is behind a router

If your PBX is behind a router and Linkus communicates with the PBX through the network interface that is configured with a private IP, you need to forward Linkus-related ports on your router and configure SIP NAT settings on your PBX.



Procedure

Based on the above network topology diagram, you can configure Linkus server as follows:

1. Log in to PBX management portal, go to System > Network > Service Ports to [check and manage local service ports](#) on your PBX system.
2. Forward Linkus-related ports on your router.

In this example, forward the following ports:

Service Port	Local Port	External Port
Linkus Service Port	TCP&UDP 8111	TCP&UDP 8111
SIP Registration Port	UDP 5060	UDP 6023
RTP Ports	UDP 10000-12000	UDP 10000-12000

3. Configure SIP NAT on your PBX for remote access.

The [SIP NAT settings](#) are configured to ensure that SIP data can be transmitted correctly between the PBX and the public Internet.

Public IP (NAT)

* NAT Type
Public IP Address

* Public IP Address
11.11.11.11

Local Network Identification

Network Number	Subnet Mask	Operations
192.168.6.0	255.255.255.0	

- a. On the PBX management portal, go to System > Network > Public IP and Ports.
 - b. Enable Public IP (NAT).
 - c. In the NAT Type drop-down list, select Public IP Address.
 - d. In the Public IP Address field, enter the public IP address. In this example, enter 11.11.11.11.
 - e. In the Local Network Identification section, click + Add IP to add all your local network. In this example, enter 192.168.6.0/255.255.255.0.
 - f. In the NAT Mode drop-down list, select Yes.
4. Enter external SIP port and Linkus service port, which helps the router to direct appropriate traffic from the Internet to the PBX.
 - External SIP UDP Port: In this example, enter 6023.
 - External Linkus Port: In this example, enter 8011.
 5. Click Save.

Result

Linkus server for both local access and remote access is set up.

What to do next

- [Configure Linkus Login Mode](#)
- [Enable Linkus clients for users](#)

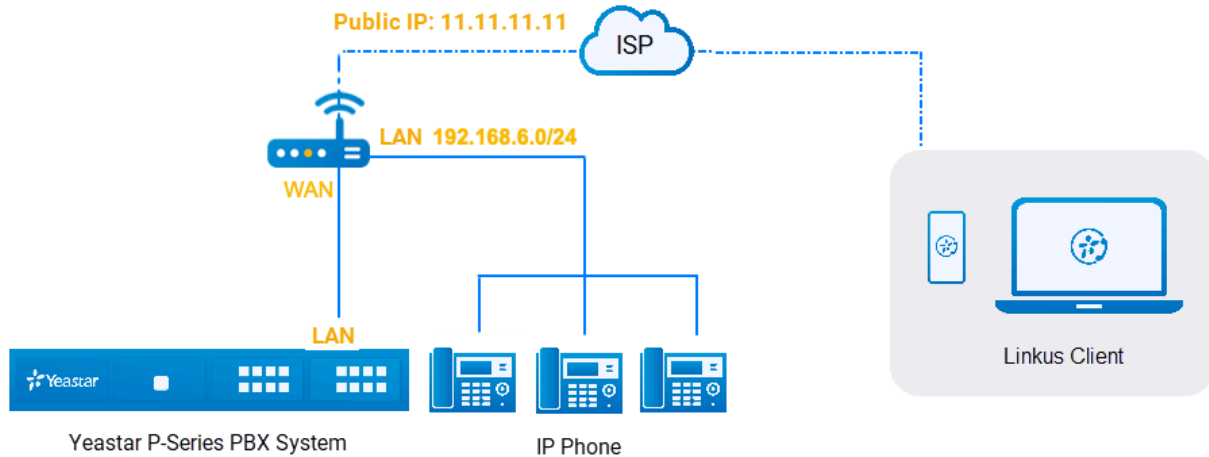
PBX is connected to the ISP router directly

If the PBX is connected to an Internet Service Provider (ISP) router, the Linkus server is ready to be accessed remotely.

Note:

- In this network scenario, you do NOT need to do port forwarding on your router and configure SIP NAT settings on your PBX.

- For this network scenario, you should change the SIP UDP port on the PBX to improve the system security.



What to do next

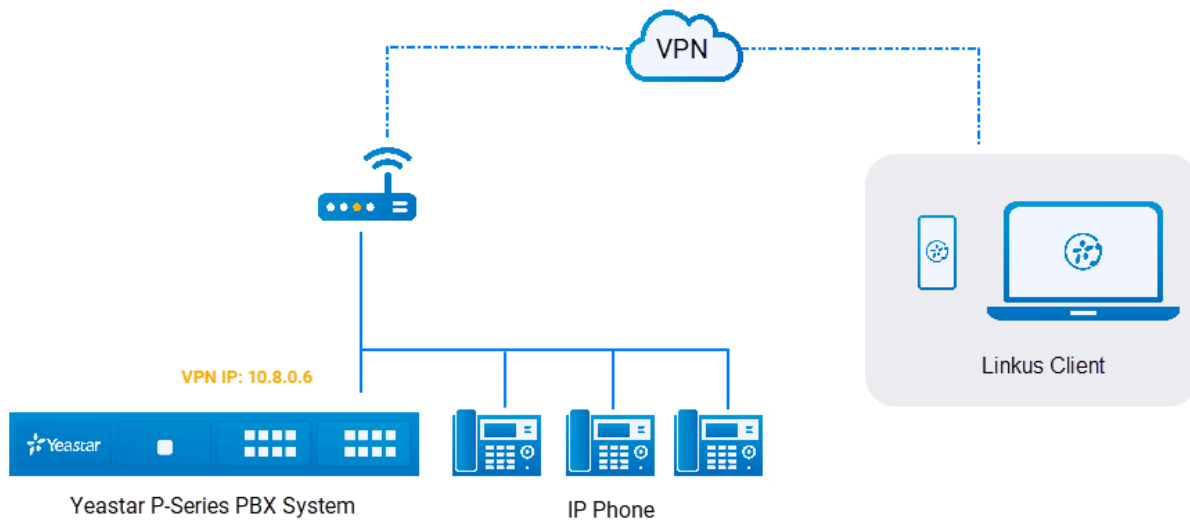
- [Configure Linkus Login Mode](#)
- [Enable Linkus clients for users](#)

PBX is connected to a VPN network

If your PBX is connected to a VPN network, the Linkus server is ready to be accessed by the VPN network.

Note:

In this network scenario, you do NOT need to do port forwarding on your router or configure SIP NAT settings on your PBX.



What to do next


- [Configure Linkus Login Mode](#)
- [Enable Linkus clients for users](#)

Configure Linkus Login Mode

Yeastar P-Series PBX System supports two login modes for Linkus clients. You can decide how users can manually log in to Linkus clients.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. Click Linkus Server tab.
3. In the Linkus Client Login Mode section, select the checkboxes of the desired login modes.
 - Extension Number: Use an extension number as the username.
 - Email Address: Use an email address as the username.

 Note:


The email address is associated with user's extension number.

4. Click Save.




Enable Linkus Clients for Users

After Linkus server is set up, you need to enable Linkus clients for users, so that users can log in to Linkus and use it. This topic describes how to enable Linkus clients for a user.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. Select a desired extension, click .
3. Click Linkus Clients tab.
4. Enable the following Linkus clients for the user.
 - Linkus Mobile Client
 - Linkus Desktop Client
 - Linkus Web Client

Result

- Linkus Mobile Client: The status shows , and a login QR code is displayed on the right.
- Linkus Desktop Client: The status shows , and a login link is displayed on the right.
- Linkus Web Client: The status shows .

What to do next

Send Linkus login credentials to users.

- To send login credentials in bulk, you can send Linkus welcome emails to users, which contain login credentials of all the Linkus clients.

For more information, see [Send Linkus Welcome Emails](#).

- To send login credential of a specific Linkus client to a user, do the followings:
 - Linkus Mobile Client: Provide user with the login QR code.

Note:

The QR code can be used ONLY once, and is valid for 24 hours.



- Linkus Desktop Client: Provide user with the login link.

Note:

The link can be used ONLY once, and is valid for 24 hours.



- Linkus Web Client: Provide user with the following information:

- [The FQDN that is bound with the PBX system](#)
- Username

The username can be extension number or email address, which depends on how you configure login mode. For more information, see [Configure Linkus Login Mode](#).

- User password

Configure Linkus Welcome Email

Before sending Linkus welcome emails to provide users with login credentials of all the Linkus clients, you may need to configure Linkus welcome email.

Background information

By default, Yeastar P-Series PBX System sends Linkus welcome emails in the language that you have set in [system email template](#). A welcome email contains the following information:

- Extension information: Include extension number and voicemail PIN.
- Login instructions and credentials: Include login instructions and credentials for all the Linkus clients.

Procedure

Yeastar P-Series PBX System provides a default email template, you can also customize your own template as follows.

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. Click Linkus Server tab.
3. Click Email Templates tab.
4. Customize email template.
 - a. In the Template drop-down list, select Custom.
 - b. Edit email subject and content according to your needs.
 - c. Click Save.

What to do next

[Send Linkus Welcome Emails](#)

Send Linkus Welcome Emails

To provide multiple users with Linkus login credentials, you can send Linkus welcome emails. This topic describes how to send Linkus welcome emails.

Prerequisites

- Make sure the [system email server](#) works.
- Make sure Linkus server has been set up.

For more information about the configurations, see [Set up Linkus Server with Remote Access Service](#) or [Manually Set up Linkus Server](#).

- You have configured email addresses for the desired extensions.
- You have enabled at least one Linkus client for the desired extensions.

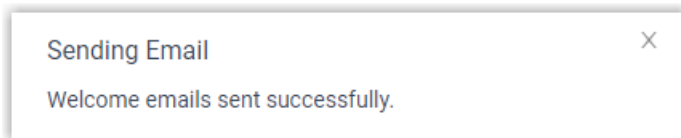
Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension.
2. On Extension list, select the checkboxes of the desired extensions, click Welcome Email.

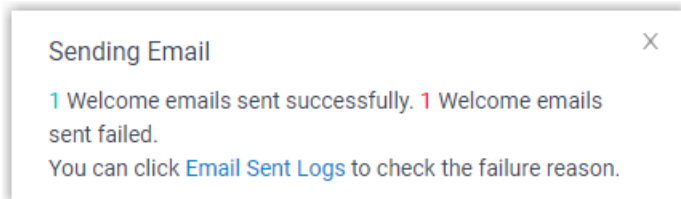
The system sends welcome emails to the extensions' email addresses.

Result

- If all the welcome emails are sent successfully, the web interface displays the following confirmation.



- If there are any emails failed to be sent, you will get an error prompt like the following figure. Click Email Sent Logs to check the error.



Enable or Disable Push Notifications for Linkus Mobile Client

This topic describes how to enable or disable push notifications for Linkus Mobile Client.

Background information

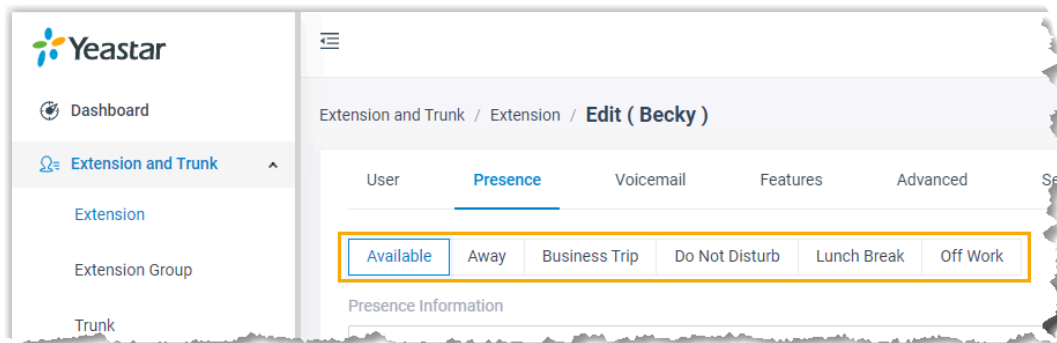
Push notification is an important tool for showing users alert messages and bringing them back to Linkus Mobile Client. By default, users can receive Linkus notifications anywhere and anytime, such as missed calls, new voicemail messages and so on.

Note:

If Linkus server is set up only in local network, in case users can not connect to calls when they are out of the office, you can disable push notifications for them.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Presence tab.
3. To configure push notifications for a specific presence, select one on the status bar.



4. In the Options section, select or unselect the checkbox of Accept Push Notifications.
5. To configure push notification for other presence status, repeat step3-4.
6. Click Save.

Operator Panel

Manage Operator Panel

This topic describes instructions on setting up Operator Panel for extension user.

What is Operator Panel

Operator Panel is a web-based utility integrated with the Yeastar Linkus Web Client. It is designed for employee who needs to manage and transfer a large number of calls, such as receptionist or agent manager.

For more information of managing calls on Operator Panel, see [Operator Panel User Guide](#).

User types and permissions

There are three user types available for you to assign to an extension group member: manager, user, and custom. What they can do on Operator Panel depends on the following permission.

The following table displays the permissions available to extension group members of different user types.

Note:

By default, an extension group manager has all permissions to manage calls on Operator Panel, while the extension group users have no permission to access and use the Operator Panel.

Permission	Extension Group Manager	Extension Group User	Custom role of Extension Group
Switch group members' presence	√	√	√
Call distribution management (Redirect, Transfer, Drag and Drop operation)	√	√	√
Pick up or hang up other extensions' calls	√	√	√
Call monitoring operations (Listen, Whisper, Barge-in)	√	√	√
Call parking operations (Park, Retrieve)	√	√	√

Permission	Extension Group Manager	Extension Group User	Custom role of Extension Group
Route calls directly from IVR regardless of the IVR menu	√	√	√
Switch Business Hours and Holidays status	√	×	√
Switch extensions' recording status	√	×	√

Related information

[Assign a User Type to a Group Member](#)

[View or Change Permissions for Group Members](#)

[View or Change a Member's User Type in Multiple Groups](#)


Trunk

Trunk Overview

A trunk is a telephone line that connects your PBX to the users in the external world. This topic gives an overview of various trunks supported on the Yeastar P-Series PBX System and describes status of different trunks.



Trunk types





The following table shows supported trunk types on Yeastar P-Series PBX System.

Category	Trunk Type	Requirement
SIP Trunk	SIP Register	No additional telephony module is required.
	SIP Peer	
	SIP Account	
Analog Trunk	FXO	S0 module or O2 module.
Cellular Trunk	GSM	GSM module.
	3G	3G module.
	4G LTE	4G LTE module.
ISDN E1/T1/J1	E1	EX30 expansion board.  Note: E1/T1/J1 trunk is only supported on Yeastar P560 and P570.
	T1	
	J1	
ISDN BRI	BRI	B2 module.





Trunk status

SIP Trunk status







Status	Description
	Disabled.
	Unreachable.
	Registration failed.




Status	Description
	<ul style="list-style-type: none"> • Authentication failed. • Transport type inconsistent. • Rejected.
	Registering.
	Registered.
	Unmonitored.
	Busy. Maximum channels reached.

FXO Trunk status




Status	Description
	Failure: Malfunction in FXO interface, please examine the relevant interface and module.
	Unavailable: No PSTN line plugged in FXO interface.
	Available.
	Busy.

GSM/3G/4G LTE Trunk status


Status	Description
	Failure: Malfunction in module, please examine the relevant module.
	Unavailable: The module is powered off.
	Unavailable: No SIM card inserted.
	Unavailable: No signal.
	Unavailable: PIN/PUK error.
	Unavailable: Cellular network registration failed.



Status	Description
	 Note: Try to manually select the correct carrier setting to fix this issue.
	Available, the icon shows the signal strength.
	Busy, the icon shows the signal strength.

E1/T1/J1 Trunk status

Status	Description
	Failure. It may be caused by the following problems on Physical layer: <ul style="list-style-type: none"> • Malfunction in interface/module. Check the relevant interface/module. • No trunk plugged in. • Service provider doesn't activate the trunk.
	Failure. It may be caused by the following problems on Data Link layer: <ul style="list-style-type: none"> • Incorrect protocol layer configuration. • Service provider doesn't activate the trunk.
	Available.

BRI Trunk status

Status	Description
	Failure. It may be caused by the following problems on Physical layer: <ul style="list-style-type: none"> • Malfunction in interface/module. Check the relevant interface/module. • No trunk plugged in. • Service provider doesn't activate the trunk.

Status	Description
	<p>Failure. It may be caused by the following problems on Data Link layer:</p> <ul style="list-style-type: none"> • Incorrect protocol layer configuration. • Service provider doesn't activate the trunk.
	Available.

SIP Trunk

SIP Trunk Overview

A SIP trunk is a virtual telephone line offered by an Internet Telephony Service Provider (ITSP). Through a SIP trunk, users can make and receive calls over the internet.

Terminology

SIP

Session Initiation Protocol (SIP) is a multimedia communication protocol developed by the Internet Engineering Task Force (IETF), an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.

ITSP

An Internet Telephony Service Provider (ITSP) is a provider of VoIP telephone service, also known as VoIP service provider.

SIP Trunk Types

Yeastar P-Series PBX System supports the following SIP trunk types:

SIP Register Trunk

Registration-based SIP trunk that uses username and password for registration with SIP providers.

SIP Peer Trunk

IP-based SIP trunk that uses IP address and port of PBX for authentication.


SIP Account Trunk

SIP Account Trunk is designed for connection between Yeastar P-Series PBX System and other devices. Yeastar P-Series PBX System will act as a VoIP account provider, the other device should register this account to connect to Yeastar P-Series PBX System.

SIP trunk creation methods

Create a SIP trunk by a template

Yeastar P-Series PBX System supports leading ITSP across the globe, you can use the pre-configured ITSP templates included in Yeastar P-Series PBX System to set up a SIP trunk quickly and easily. For more information, see [Create a SIP Trunk from a Template](#).

 Note:

Check tested and supported ITSP from [ITSP partner page](#).

Create a general SIP trunk

If your ITSP has not undergone an interoperability test by Yeastar, you can set up a general SIP trunk.

For more information, see the following topics:

- [Create a SIP Register Trunk](#)
- [Create a SIP Peer Trunk](#)

Create a SIP Trunk

Create a SIP Trunk from a Template

Yeastar has tested leading ITSP across the globe and provides configuration templates for the tested and certificated ITSP. If a template is provided for your ITSP on the PBX, you can quickly create a SIP Trunk by the template.

Prerequisites

- Check if your ITSP is tested and supported by Yeastar from [ITSP partner page](#).
- Your PBX can connect to the ITSP.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, click Add.
2. In the Basic section, configure the following settings:
 - Name: Enter a name to help you identify it.
 - Trunk Status: Select Enabled.
 - Select ITSP Template: Select your country.
 - ITSP: Select your ITSP.

The trunk details are displayed automatically in the Detailed Configuration section.

- If the trunk type is displayed as Register Trunk, configure the following settings:

- Username: Enter the username provided by the ITSP.
 - Password: Enter the password provided by the ITSP.
 - Authentication Name: Optional. Authentication name is used for SIP authentication. If the ITSP provides an authentication name, enter the name.
 - If the trunk type is displayed as Peer Trunk, leave the settings as default.
3. Optional: If you have purchased DID numbers from the ITSP, click DID/DDIs tab to configure the DID numbers for the trunk.
 - a. Click Add.
 - b. In the pop-up window, configure the following settings:
 - DID/DDI: Enter the provided DID number.
 - DID/DDI Name: Optional. Enter a name to distinguish inbound calls by DID numbers.


The name will be displayed on the called party's device when the DID number is dialed.
 - c. Click Save.
 - d. To add more DID numbers, repeat step a - c.

For more information of DID configurations, see [Configure DID Numbers on a Trunk](#).

4. Click Save and Apply.

Result

Go to Extension and Trunk > Trunk to check the trunk status on the trunk list page.

If the status shows , the trunk is registered successfully.

For more information of SIP trunk status, see [SIP Trunk status](#).

What to do next

- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see [Set up an Inbound Route](#).
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see [Set up an Outbound Route](#).

Create a SIP Register Trunk

This topic gives a configuration example to describe how to create a general SIP Register Trunk, which can be applied to all kinds of SIP Register Trunk.

Background information

Assume that you have bought a SIP account from the ITSP ABC, and the trunk information is displayed as below.

- Provider domain: abc.provider.com
- Protocol: SIP

- Registration Port: 5060
- Transport: UDP
- Username: 254258255
- Authentication name: 254258255
- Password: 05JsOmsIS54SYh

Prerequisites

- You have purchased a SIP account from an ITSP and a username and a password are offered.
- Your PBX can connect to the ITSP.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, click Add.
2. In the Basic section, configure the following settings:
 - Name: Enter a name to help you identify it.
 - Trunk Status: Select Enabled.
 - Select ITSP Template: Select General.
3. In the Detailed Configuration section, select the trunk type and enter the SIP information that is provided by the ITSP.
 - Trunk Type: Select Register Trunk.
 - Transport: Select the transport provided by the ITSP. In this example, select UDP.
 - Hostname/IP: Enter the domain name or IP address of the ITSP. In this example, enter abc.provider.com.
 - Port: Enter the provided registration port. In this example, enter 5060.
 - Domain: Enter the domain in SIP URI of a specific header like From, To header. In this example, enter abc.provider.com.

Note:


If the domain is not provided by ITSP, enter the same value as Hostname/IP.

- Username: Enter the provided user name. In this example, enter 254258255.
- Password: Enter the provided password. In this example, enter 05JsOms-IS54SYh.
- Authentication Name: Enter the provided authentication name. In this example, enter 254258255.

Note:

In most cases, authentication name is the same as the user name.

- Enable Outbound Proxy: Optional. If the trunk is configured to use an outbound proxy server, when users make outbound calls through this trunk, all the SIP packets will be sent to the outbound proxy server.

 Note:


Contact your ITSP to check if outbound proxy is supported, then configure outbound proxy settings under the ITSP's guidance.

4. Optional: If you have purchased DID numbers from the ITSP, click DID/DDIs tab to configure the DID numbers for the trunk.
 - a. Click Add.
 - b. In the pop-up window, configure the following settings:
 - DID/DDI: Enter the provided DID number.
 - DID/DDI Name: Optional. Enter a name to distinguish inbound calls by DID numbers.
The name will be displayed on the called party's device when the DID number is dialed.
 - c. Click Save.
 - d. To add more DID numbers, repeat step a - c.

For more information of DID configurations, see [Configure DID Numbers on a Trunk](#).
5. Optional: Click Advanced, Inbound Caller ID Reformatting, Outbound Caller ID, or SIP Headers tab to configure other settings.
6. Click Save and Apply.

Result

Go to Extension and Trunk > Trunk to check the trunk status on the trunk list page.

If the status shows , the trunk is registered successfully.

For more information of SIP trunk status, see [SIP Trunk status](#).

What to do next

- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see [Set up an Inbound Route](#).
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see [Set up an Outbound Route](#).

Create a SIP Peer Trunk

This topic gives a configuration example to describe how to create a general SIP Peer Trunk, which can be applied to all kinds of SIP Peer Trunk.

Background information

Assume that you have bought a SIP account from the ITSP ABC, and the trunk information is displayed as below.


- Provider domain: abc.provider.com
- Protocol: SIP
- Registration Port: 5060
- Transport: UDP

Prerequisites

- You have purchased a SIP account from an ITSP and no username and password is offered but only a domain name or IP address.
- Your PBX can connect to the ITSP.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, click Add.
2. In the Basic section, configure the following settings:
 - Name: Enter a name to help you identify it.
 - Trunk Status: Select Enabled.
 - Select ITSP Template: Select General.
3. In the Detailed Configuration section, select the trunk type and enter the SIP information that is provided by the ITSP.
 - Trunk Type: Select Peer Trunk.
 - Transport: Select the transport provided by the ITSP. In this scenario, select UDP.
 - Hostname/IP: Enter the domain name or IP address of the ITSP. In this scenario, enter abc.provider.com.
 - Port: Enter the provided registration port. In this scenario, enter 5060.
 - Domain: Enter the domain in SIP URI of a specific header like From, To header. In this example, enter abc.provider.com.

 Note:

If the domain is not provided by ITSP, enter the same value as Hostname/IP.

4. Optional: If you have purchased DID numbers from the ITSP, click DID/DDIs tab to configure the DID numbers for the trunk.
 - a. Click Add.
 - b. In the pop-up window, configure the following settings:
 - DID/DDI: Enter the provided DID number.
 - DID/DDI Name: Optional. Enter a name to distinguish inbound calls by DID numbers.


The name will be displayed on the called party's device when the DID number is dialed.
 - c. Click Save.
 - d. To add more DID numbers, repeat step a - c.

For more information of DID configurations, see [Configure DID Numbers on a Trunk](#).

5. Click Save and Apply.

Result

Go to Extension and Trunk > Trunk to check the trunk status on the trunk list page.

If the status shows , the trunk is registered successfully.

For more information of SIP trunk status, see [SIP Trunk status](#).

What to do next

- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see [Set up an Inbound Route](#).
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see [Set up an Outbound Route](#).

Create a SIP Account Trunk

A SIP Account is used for the other device to register with Yeastar P-Series PBX System. In this way, Yeastar P-Series PBX System and the other device are connected. This topic describes how to create a SIP Account Trunk on Yeastar P-Series PBX System.

Prerequisites

To connect a third-party device with Yeastar P-Series PBX System by a SIP Account Trunk, you need to make sure that there is no duplicate extension numbers on both sides.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, click Add.
2. In the Basic section, configure the following settings:
 - Name: Enter a name to help you identify it.
 - Trunk Status: Select Enabled.
 - Select ITSP Template: Select General.
3. In the Detailed Configuration section, select the trunk type and define the information of the SIP account.

Note:

You can leave the default SIP information or edit the information according to your needs.

- Trunk Type: Select Account Trunk.
- Transport: Select a transport. The following options are supported:
 - UDP
 - TCP
 - TLS
- Username: Enter a username for the SIP account.


- Password: Enter a password for the SIP account.
 - Authentication Name: Enter an authentication name for the SIP account.
4. Optional: Click Advanced, Inbound Caller ID Reformatting, Outbound Caller ID, or SIP Headers to configure other settings.
 5. Click Save and Apply.

What to do next

- Register the SIP Account Trunk on the third-party software or device. Depending on the network of the third-party software or device, you need to provide different information:
 - Same local network as Yeastar P-Series PBX System
 - SIP Account Trunk details
 - Local IP address of PBX
 - Local SIP port of PBX
 - Different network from Yeastar P-Series PBX System
 - SIP Account Trunk details
 - Public IP address or domain name of PBX
 - External SIP port of PBX
- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see [Set up an Inbound Route](#).
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see [Set up an Outbound Route](#).

Result

Go to Extension and Trunk > Trunk to check the trunk status on the trunk list page.


If the SIP Account Trunk is successfully registered on the third-party software or device, the trunk status will show , which also indicates that the two devices are connected.

For more information of SIP trunk status, see [SIP Trunk status](#).


Manage SIP Trunks

After you create SIP trunks, you can edit or delete the SIP trunks.

Edit a SIP trunk

1. Log in to PBX management portal, go to Extension and Trunk > Trunk.
2. On the Trunk list page, select a trunk and click .
3. Click the desired tab to edit the relevant settings.
4. Click Save and Apply.

Delete SIP trunks

1. Log in to PBX management portal, go to Extension and Trunk > Trunk.
2. To delete a SIP trunk, do the followings:
 - a. Click  beside the trunk.
 - b. Click Yes in the pop-up dialog box to confirm.
3. To delete multiple SIP trunks, do the followings:
 - a. Select checkboxes of the desired trunks.
 - b. Click Delete.
 - c. Click Yes in the pop-up dialog box to confirm.

Export and Import SIP Trunks

The SIP trunks configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired SIP trunks in the exported file, and import the file to PBX again. This topic describes how to export and import SIP trunks.

Background information

Only Peer Trunks and Register Trunks can be imported.

Export all SIP trunks

You can export all SIP trunks to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Extension and Trunk > Trunk.
2. Click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see [Trunk Parameters](#).

Import SIP trunks

We recommend that you export SIP trunks data to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 50 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information , see [Trunk Parameters](#).

Procedure


1. Log in to PBX management portal, go to Extension and Trunk > Trunk.
2. Click Import.
3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The trunks in the CSV file will be displayed in the Trunk list.





SIP Trunk Settings

This topic describes all the settings on a SIP trunk for reference.

Basic settings

Basic	
Setting	Description
Name	Give this trunk a name to help you identify it.
Trunk Status	Enable or disable the trunk.
Select ITSP Template	Select the country of your ITSP. <div style="border: 1px solid #add8e6; padding: 5px; background-color: #e6f2ff;">  Note: If no SIP trunk template is provided for your ITSP, select General. </div>
ITSP	Select your ITSP from the list of certified SIP trunk providers.

Detailed Configuration	
Setting	Description
Trunk Type	Select a trunk type: <ul style="list-style-type: none"> • Register Trunk • Peer Trunk • Account Trunk
Register Trunk	
Transport	Select the transport that is provided by the ITSP.
Hostname/IP	Enter the IP address or the domain of the ITSP.
Port	Enter the SIP port provided by the ITSP.
Domain	Enter the domain in SIP URI of a specific header like From, To header.

Detailed Configuration	
Setting	Description
	 Note: If the domain is not provided by ITSP, enter the same value as Hostname/IP.
Username	Enter the username to register to the ITSP.
Authentication Name	Enter the authentication name to register to the ITSP.
Password	Enter the password that is associated with the username.
Enable Outbound Proxy	If the trunk is configured to use an outbound proxy server, when users make outbound calls through this trunk, all the SIP packets will be sent to the outbound proxy server.
	 Note: Contact your ITSP to check if they support outbound proxy, then configure outbound proxy settings under their guidance.
Peer Trunk	
Transport	Select the transport that is provided by the ITSP.
Hostname/IP	Enter the IP address or the domain of the ITSP.
Port	Enter the SIP port provided by the ITSP.
Domain	Enter the domain in SIP URI of a specific header like From, To header.
	 Note: If the domain is not provided by ITSP, enter the same value as Hostname/IP.
Account Trunk	
Protocol	Select the protocol for a third-party device to register with.
Transport	Select the transport for a third-party device to register with.
Username	Specify a username for the trunk.
	 Note:

Detailed Configuration	
Setting	Description
	The username is regarded as the trunk number.
Authentication Name	Specify an authentication name for a third-party device to register with.
Password	Specify a password that is associated with the user-name.

Advanced settings

The advanced settings of VoIP trunk require professional knowledge of SIP protocol. Incorrect configurations may cause calling issues. It is wise to leave the default settings provided on the SIP trunk page. However, for a few fields, you need to change them to suit your situation.

The following settings are included on the Advanced page.

- [Codec Setting](#)
- [VoIP Setting](#)
- [Call Restriction](#)

Codec Setting


Each newly created SIP trunk has a default preferred codec list. However, the default codec list may not match the codecs supported by your ITSP. To maximize the quality of calls and the amount of bandwidth used for calls, you can configure your preferred codec list to match the settings that your ITSP supports.

Yeastar P-Series PBX System supports the following codecs:

- u-law
- a-law
- G729A
- GSM
- H264
- H261
- H263
- H263P
- iLBC
- G722
- G726
- SPEEX
- ADPCM
- MPEG4

- VP8

VoIP Setting

Setting	Description
DTMF Mode	<p>Set the default mode for sending DTMF tones.</p> <ul style="list-style-type: none"> • RFC4733 (RFC2833): DTMF will be carried in the RTP stream in different RTP packets rather than the audio signal. • Info: DTMF will be carried in the SIP info messages. • Inband: DTMF will be carried in the audio signal. • Auto: The PBX will detect if the device supports RFC4733(RFC2833) DTMF. If RFC4733(RFC2833) is supported, PBX will choose RFC4733(RFC2833), or the PBX will choose Inband.
Qualify	Enable this option to send SIP OPTION packet to SIP device to check if the device is up.
Enable SRTP	Enable or disable SRTP (encrypted RTP) for the trunk.
T.38 Support	<p>Enable or disable T.38 fax for this trunk. Enabling T.38 will add the performance cost.</p> <p>We suggest that you disable T.38.</p>
Inband Progress	<p>This Inband Progress setting applies to the extensions which make calls through this trunk.</p> <div style="border: 1px solid #00aaff; padding: 5px; margin: 10px 0;"> <p> Note: To configure global Inband Progress setting, you need to contact Yeastar support to configure a custom config file.</p> </div> <ul style="list-style-type: none"> • Check this option: PBX will send a 183 Session Progress to the extension when told to indicate ringing and will immediately start sending ringing as audio. • Uncheck this option: PBX will send a 180 Ringing to the extension when told to indicate ringing and will NOT send it as audio.

Call Restriction

Setting	Description
Call Restriction Type	<p>Specify based on which type of calls to restrict the max concurrent call number of this trunk.</p> <ul style="list-style-type: none"> • Outbound Call: Only outbound calls will be restricted. • All: Both outbound calls and inbound calls will be restricted.
Maximum Concurrent Calls	Specify the maximum number of concurrent calls allowed in this trunk. The default is Unlimited.

DIDs/DDIs

Direct Inward Dialling (DID), also called Direct Dial-in (DDI), is a service offered by telephone companies. For more information of DID concepts, see [DID Number Overview](#).

- DID numbers are usually configured on inbound routes to distinguish inbound calls.
For more information, see [Route Inbound Calls based on DID Numbers](#).
- For more instructions on configuring the DID numbers, see [Configure DID Numbers on a Trunk](#).

Inbound Caller ID Reformatting

When a user calls in the PBX, the trunk provider may send a caller ID that is inconvenient for you to redial directly.

In this case, you can reformat inbound caller ID based on a trunk. The caller ID will be reformatted before it is sent to the called party.

For more information, see [Reformat Inbound Caller ID based on a Trunk](#).

Outbound Caller ID

Outbound caller ID is the phone number or name that is displayed on the called party's device.

You can set up a global outbound caller ID for a trunk or assign caller IDs for extension users.

Note:

By default, each trunk has a default phone number that will be displayed on the called party's device. Outbound Caller ID configuration requires support from the trunk provider. Contact your trunk provider first before you configure Outbound Caller ID, or the settings won't take effect and outbound calls may fail.

If you set the caller ID number, when users make outbound calls through this trunk, the called party will see this caller ID number instead of the calling party's number.

For more information of outbound caller ID configurations, see [Customize Outbound Caller IDs](#)

SIP Headers


The SIP Headers settings require professional knowledge of SIP protocol. Incorrect configurations may cause calling issues. It is wise to leave the default settings provided on the SIP trunk page. However, for a few fields, you need to change them to suit your situation.

The following settings are included on the SIP Headers page.

- [Inbound Parameters](#)
- [Outbound Parameters](#)
- [Other Settings](#)

Inbound Parameters

Setting	Description
Get Caller ID From	<p>Decide from which header field will the trunk retrieve Caller ID.</p> <ul style="list-style-type: none"> • Follow System The trunk will follow the global Get Caller ID From setting. • From • Contact • Remote-Party-ID • P-Asserted Identify • P-Preferred-Identity
Get DID From	<p>Different devices or providers may contain DID numbers in different SIP headers. When an inbound call through a SIP trunk reaches the PBX, the PBX needs to retrieve a correct DID number, or the call will fail.</p> <p>Adjust the setting after analysis of the SIP packets sent from the trunk provider. The following SIP headers are available to select:</p> <ul style="list-style-type: none"> • Follow System The trunk will follow the global Get DID From setting. • To • Invite

Setting	Description
	<ul style="list-style-type: none"> • Diversion • Remote-Party-ID <div style="border: 1px solid #add8e6; padding: 5px; margin: 10px 0;"> <p> Note: If this option is selected, but the SIP provider doesn't support Remote Party ID, the PBX will retrieve DID from INVITE header.</p> </div> <ul style="list-style-type: none"> • P-Asserted Identify • P-Called-Party-ID • P-Preferred-Identity

Outbound Parameters

For outbound calls, you can define the parameters included in the following SIP INVITE headers:

- From


A From header contains caller ID and caller ID name, which are defined as the followings in Yeastar P-Series PBX System.

- From User Part: Indicates caller ID.
- From Display Name Part: Indicates caller ID name.

You can define which parameters will be used in these two parts of a SIP From header.

- Diversion
- Remote Party ID
- P-Asserted Identify
- P-Preferred-Identity


Each SIP header has multiple options to define the parameters. The following tables describe the options.



 **Note:**
For different types of SIP trunk, the optional items are different.

Setting	Description
[Default]	<p>The system selects a parameter by the following priority from top to bottom:</p> <ul style="list-style-type: none"> • Outbound Route Outbound Caller ID • Extension's Outbound Caller ID in Trunk • Trunk Outbound Caller ID • Trunk Username

Setting	Description
	<ul style="list-style-type: none"> • Extension Caller ID • The Originator Caller ID
[None]	Do not send the parameter with the SIP INVITE packet.
Outbound Route Outbound Caller ID	The outbound caller ID configured on the outbound route that is used for the outbound calls.
Extension's Outbound Caller ID in Trunk	The extension's associated outbound caller ID with the trunk.
Trunk Outbound Caller ID	The global outbound caller ID for the trunk (Trunk > Outbound Caller ID > General).
Trunk Username	The username configured on the trunk.
Extension Caller ID	The caller ID configured on the extension.
Originator Caller ID	<p>The Caller ID of the call originator (the first caller in the case that the call is transferred).</p> <ul style="list-style-type: none"> • If the call originator is an external number, the external number will be taken. • If the call originator is an extension, the priority order will be Extension Outbound Caller ID → [Default].
Custom	Define a custom value.

Other Settings

Setting	Description
User Agent	If the ITSP requires User Agent for authentication, enter the User Agent information that is provided by the ITSP.
Realm	<p>Realm is a string displayed to users so they know which username and password to use.</p> <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> Note: If you don't know what to fill in, contact your service provider for further instructions.</p> </div>
Send Privacy ID	Whether to send the Privacy ID in SIP header or not. The default is unchecked.

Setting	Description
User Phone	<p>Whether to add the parameter <code>user=phone</code> as a request line in the header field of the SIP INVITE packet.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Enable this option only when the SIP provider requires.</p> </div>
100rel	Whether to support 100rel or not.
Maxptime	<p>Select the value of the maxptime used when the PBX sends the INVITE packet.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: If you select [Default], PBX will send a corresponding maxptime value according to the codec that is used for the outbound call.</p> </div>
Support P-Early-Media	Set whether the P-Early-Media field is included in the INVITE packet.

Analog FXO Trunk

Analog FXO Trunk Overview

This topic describes what is analog FXO trunk and usages of analog FXO trunk.

What is analog FXO trunk

An analog FXO trunk is a telephone line that connects your PBX and the Public Switched Telephone Network (PSTN) or a traditional PBX.

- Connect FXO port of Yeastar P-Series PBX System and a PSTN provider
Extension users can make and receive calls with the external users through the trunk.
- Connect FXO port of Yeastar P-Series PBX System and FXS port of a traditional PBX
A company can integrate their legacy PBX with Yeastar P-Series PBX System to utilize the benefit of VoIP easily and achieve cost-effective communication.

Set up an Analog FXO Trunk

This topic describes how to set up an analog FXO trunk on Yeastar P-Series PBX System.

Prerequisites

Install at least one O2 module or SO module on the PBX.

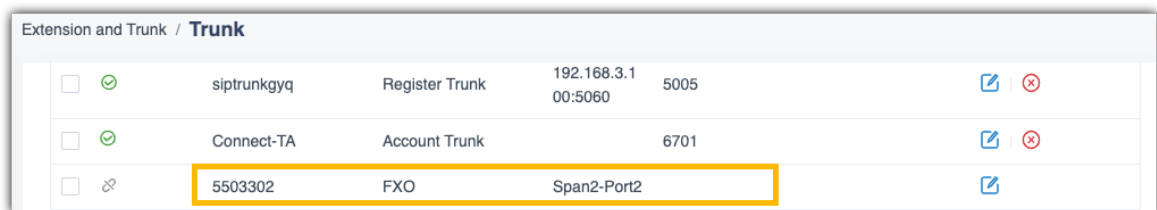
- If the module is successfully installed and detected by the PBX, the FXO port information will be displayed on the PBX web interface.
- If the module is not detected by the PBX, contact Yeastar support to check the problem.

Procedure

1. Find out the FXO port on the PBX.

Log in to PBX management portal, go to Extension and Trunk > Trunk, check the location of the FXO port.

As the following figure shows, an FXO port is located in Span2-Port2.



Extension and Trunk / Trunk						
<input type="checkbox"/>	✔	siptrunkgyq	Register Trunk	192.168.3.1 00:5060	5005	✎ ✖
<input type="checkbox"/>	✔	Connect-TA	Account Trunk		6701	✎ ✖
<input type="checkbox"/>	✘	5503302	FXO	Span2-Port2		✎

2. Use a RJ11 phone line to connect the FXO port of PBX and the PSTN provider's FXS port.

In this example, connect the phone line to port 2 on span 2.

3. Optional: Configure the FXO trunk settings.

Go to Extension and Trunk > Trunk, select the FXO trunk to edit the trunk settings.

Note:

The advanced settings require professional knowledge of analog telephony, carefully configure the advanced settings, or the trunk would not work.

For more information of FXO trunk settings, see [Analog FXO Trunk Settings](#).

Result

Go to Extension and Trunk > Trunk to check the trunk status on the trunk list page.

If the status shows , the trunk is connected successfully.

See [FXO Trunk status](#) to know more information of FXO trunk status.

What to do next

- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see [Set up an Inbound Route](#).
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see [Set up an Outbound Route](#).

Release an Analog FXO Trunk


If an FXO trunk keeps in Busy status after a call is hung up, you can mandatory release the trunk to make the trunk available to use.

Background information

The issue that the trunk cannot be released automatically after a call is hung up is usually caused by incorrect Hangup Detection settings.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit the problematic FXO trunk.
2. Click Advanced tab.
3. On the Advanced page, click Release Trunk.

The trunk will be released, and the trunk status shows .

What to do next

Adjust the [Hangup Detection settings](#) for the problematic FXO trunk.

Note:

The Hangup Detection settings require good knowledge of analog telephony, you may need to contact the trunk provider or Yeastar Support to configure the settings.

Analog FXO Trunk Settings

This topic describes all the settings on an FXO trunk for reference.

Basic settings

Setting	Description
Name	Give this trunk a name to help you identify it.
RX Volume	Set the receiving volume of the FXO port.

Setting	Description
TX Volume	Set the transmitting volume of the FXO port.

Advanced settings


The advanced settings require professional knowledge of analog telephony, carefully configure the advanced settings, or the trunk would not work. For different PSTN providers, you may need to adjust the advanced settings to suit your situation.


The following settings are included on the Advanced page.

- [Hangup Detection](#)
- [Answer Detection](#)
- [Caller ID Settings](#)
- [Other Settings](#)


Hangup Detection

Hangup Detection settings help the PBX to detect if a call is hung up. If you find outbound calls through the FXO trunk cannot be disconnected, adjust the Hangup Detection settings.

Setting	Description
Hangup Detection Method	<p>Select the Hangup Detection method:</p> <ul style="list-style-type: none"> • Busy Tone: The call will be disconnected if a busy tone is detected by the Yeastar P-Series PBX System. • Polarity Reversal: The call will be disconnected if a polarity reversal is detected by the Yeastar P-Series PBX System. • Loop Current Disconnect: When the remote side of FXO trunk disconnects the call and creates a loop current, Yeastar P-Series PBX System will detect the loop current and disconnect the call.
Busy Count	<p>Specify how many busy tones to wait for before disconnecting.</p> <p>The default value is 4.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: PBX may fail to detect the busy tone if the value of Busy Count is too high.</p> </div>
Busy Pattern	Specify the cadence of busy signal.

Setting	Description
	<ul style="list-style-type: none"> • Format: {sound},{silence}. <p>For example, 500,500 means 500ms on, 500ms off.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note:</p> <ul style="list-style-type: none"> • If you select [None], the system will accept any regular sound-silence pattern that repeats Busy Count times as a busy signal. • If you select a busy tone, the system will further check the length of the tone and silence, which will further reduce the chance of a false positive disconnection. </div>
Busy Interval (s)	The busy detection interval.
Frequency Detection	Enable or disable detection of busy signal frequency.
Busy Frequency	If the Frequency Detection is enabled, you need to specify the local frequency.

Answer Detection

Setting	Description
Answer Detection Method	<p>Specify the method to detect if a call is answered. This setting affects the accuracy of call duration tracking.</p> <ul style="list-style-type: none"> • [None]: PBX will start counting call duration after you use the FXO trunk to call out, whether the call is answered or not. • Polarity Reversal: If this option is selected, PBX will start counting call duration after a polarity signal is detected. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note:</p> <p>Before you select this option, contact the PSTN provider to check if they supports polarity.</p> </div>

Caller ID Settings

Caller ID Settings helps the system to detect Caller ID. If an incoming PSTN call does not display Caller ID, you need to confirm with your service provider if the line has enabled Caller ID feature. If this line does support Caller ID, configure these settings to solve this problem.

Setting	Description
Caller ID Detection	Enable or disable Caller ID detection.
Caller ID Detection Mode	Define the start of a Caller ID signal. <ul style="list-style-type: none"> • After Ringing: Detect Caller ID after first ringing. • After Polarity: Detect Caller ID after polarity reversal. • Before Ringing: Detect Caller ID before first ringing.
Caller ID Signaling	Specify the type of caller ID signaling to use according to the direction provided by your service provider. <ul style="list-style-type: none"> • Bell202 • V23-Japan • DTMF • ETSI-V23

Other Settings

Setting	Description
Ringing Detection Timeout (ms)	FXO (FXS signalled) devices must have a timeout to determine if there was a hangup before the line was answered. <ul style="list-style-type: none"> • Valid value: 1000-10000 • Default value: 5000
Echo Cancellation	Enable or disable echo cancellation.
DID Name	DID Name is used to identify which telephone number was dialed. When an inbound call reaches the trunk, the name will be displayed on the called party's device.
Inbound to Outbound Number	This setting is typically for Inbound Route to Outbound Route feature. If you wish the inbound call through this trunk to be redirected via an outbound

Setting	Description
	route, enter the destination number in this field.

Inbound Caller ID Reformatting

When a user calls in the PBX, the trunk provider may send a caller ID that is inconvenient for you to redial directly.

In this case, you can reformat inbound caller ID based on a trunk. The caller ID will be reformatted before it is sent to the called party.

For more information, see [Reformat Inbound Caller ID based on a Trunk](#).

GSM/3G/4G LTE Trunk

GSM/3G/4G LTE Trunk Overview

This topic describes what is GSM/3G/4G LTE trunk and frequency bands supported on Yeastar P-Series PBX System.

What is GSM/3G/4G LTE trunk

A GSM/3G/4G LTE trunk connects the Yeastar P-Series PBX System and the relevant cellular network provider directly, and capitalizes on the cheaper mobile-to-mobile call tariffs.

To use a GSM/3G/4G LTE trunk, you need to install a relevant module on the PBX and insert a SIM card that can work in the supported frequency bands.

GSM/3G/4G LTE Module frequency bands

Module Type	Module Model	Frequency Band
GSM	SIM800	<ul style="list-style-type: none"> • EGSM-900 MHz • PGSM-900 MHz • DCS-1800 MHz • GSM850-850 MHz • PCS-1900 MHz
3G	UC15-A	<ul style="list-style-type: none"> • WCDMA: 850/1900 MHz • GSM: 850/900/1800/1900 MHz
3G	UC15-E	<ul style="list-style-type: none"> • WCDMA: 900/2100 MHz • GSM: 900/1800 MHz
3G	UC15-T	<ul style="list-style-type: none"> • WCDMA: 850/2100 MHz • GSM: 850/900/1800/1900 MHz

Module Type	Module Model	Frequency Band
4G LTE	EC20-CEFAG	<ul style="list-style-type: none"> • FDD-LTE: B1/B3/B8/B5 • TDD-LTE: B38/B39/B40/B41 • WCDMA: B1/B8 • TD-SCDMA: B34/B39 • CDMA2000 1X: BC0 • CDMA2000 EVDO: BC0 • GSM: 900/1800 MHz
4G LTE	EC20-CEFD	<ul style="list-style-type: none"> • FDD-LTE: B1/B3/B8 • TDD-LTE: B38/B39/B40/B41 • WCDMA: B1/B8 • TD-SCDMA: B34/B39 • CDMA2000 1X: BC0 • CDMA2000 EVDO: BC0 • GSM: 900/1800 MHz
4G LTE	EC25-A	<ul style="list-style-type: none"> • FDD-LTE: B2/B4/B12 • WCDMA: B2/B4/B5
4G LTE	EC25-AU	<ul style="list-style-type: none"> • FDD-LTE: B1/B2/B3/B4/B5/B7/B8/B28 • TDD-LTE: B40 • WCDMA: B1/B2/B5/B8 • GSM: B2/B3/B5/B8
4G LTE	EC25-E	<ul style="list-style-type: none"> • FDD-LTE: B1/B3/B5/B7/B8/B20 • TDD-LTE: B38/B40/B41 • WCDMA: B1/B5/B8 • GSM: B3/B8
4G LTE	EC25-J	<ul style="list-style-type: none"> • FDD-LTE: B1/B3/B8/B18/B19/B26 • TDD-LTE: B41 • WCDMA: B1/B6/B8/19
4G LTE	EC25-V	<ul style="list-style-type: none"> • FDD-LTE: B4/B13

Set up a GSM/3G/4G LTE Trunk

This topic describes how to set up a GSM/3G/4G LTE trunk on Yeastar P-Series PBX System.

Prerequisites

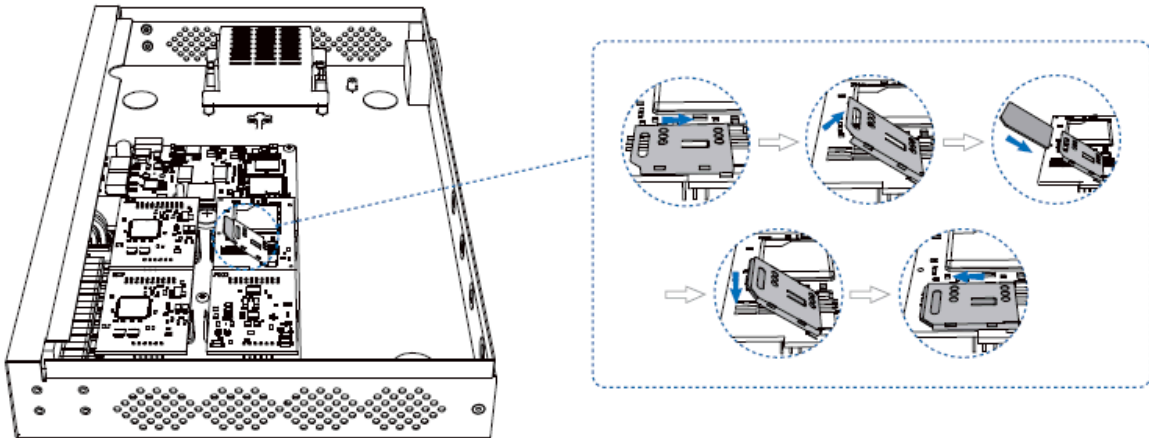
Install at least one GSM module, 3G module, or 4G LTE module on the PBX.

- If the module is successfully installed and detected by the PBX, the trunk will be displayed on the PBX management portal.

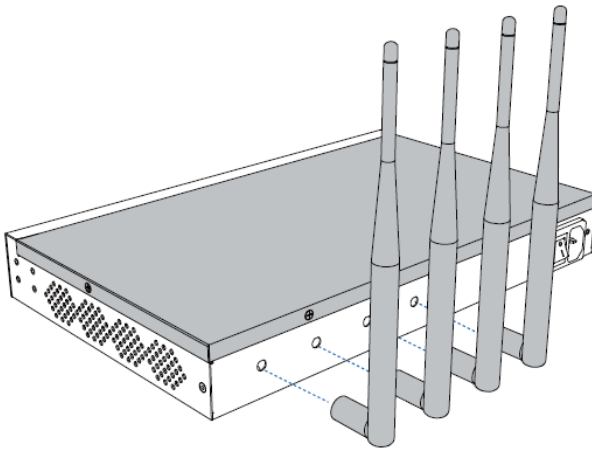
- If the module is not detected by the PBX, contact Yeastar support to check the problem.

Procedure

1. Install a SIM card on the GSM/3G/4G LTE module.



2. Rotate the antenna into the Antenna Socket.






3. Optional: Configure the GSM/3G/4G LTE trunk settings.

Log in to the PBX management portal, go to Extension and Trunk > Trunk, select the GSM/3G/4G LTE trunk to edit the trunk settings.

For more information of GSM/3G/4G LTE trunk settings, see [GSM/3G/4G LTE Trunk Settings](#).

Result

Go to Extension and Trunk > Trunk to check the trunk status on the trunk list page.

If the status shows , , or , the trunk is successfully set up, and the icon also indicates the signal strength of the trunk.

For more information of GSM/3G/4G LTE trunk status, see [GSM/3G/4G LTE Trunk Settings](#).


What to do next


- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see [Set up an Inbound Route](#).
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see [Set up an Outbound Route](#).

GSM/3G/4G LTE Trunk Settings

This topic describes all the settings on an GSM/3G/4G LTE trunk for reference.

Basic settings

General	
Setting	Description
Name	Give this trunk a name to help you identify it.
PIN Code	<p>Enter the SIM card PIN code if the card has one.</p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: If you fail to enter your correct PIN code for 3 times in succession, the SIM card will be permanently locked, which means you will need a new SIM card.</p> </div>
RX Volume	Set the receiving volume of GSM/3G/4G LTE port or select Custom to define the RX Gain.
TX Volume	Set the transmitting volume of GSM/3G/4G LTE port or select Custom to define the TX Gain.
Echo Cancellation	Enable or disable echo cancellation.
DID Name	DID Name is used to identify which telephone number was dialed. When an inbound call reaches the trunk, the name will be displayed on the called party's device.
Inbound to Outbound Number	<p>This setting is typically for Inbound Route to Outbound Route feature.</p> <p>If you wish the inbound call through this trunk to be redirected via an outbound route, enter the destination number in this field.</p>

Carrier Settings	
Setting	Description
Carrier	<p>Select the carrier mode.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin: 5px 0;"> <p> Note: When the trunk is in unregistered status, you can try to manually select the correct carrier to fix the issue.</p> </div> <ul style="list-style-type: none"> • Automatic: The system will detect the SIM card and select a carrier automatically. • Manual: Select a carrier from the available carrier that the system provided.

Inbound Caller ID Reformatting

When a user calls in the PBX, the trunk provider may send a caller ID that is inconvenient for you to redial directly.

In this case, you can reformat inbound caller ID based on a trunk. The caller ID will be reformatted before it is sent to the called party.

For more information, see [Reformat Inbound Caller ID based on a Trunk](#).

ISDN E1/T1 Trunk

E1/T1/J1 Trunk Overview

This topic describes what is E1/T1/J1 trunk and the differences among the three types of trunk. This topic also provides the information of E1/T1/J1 crossover cable.

What is E1/T1/J1 trunk

E1/T1/J1 is known as Primary Rate Interface (PRI), an Integrated Services Digital Network (ISDN) access method, which enables traditional phone lines to carry voice, data, and video traffic.

Note:

- E1/T1/J1 trunk is only supported on Yeastar P560 and P570.
- To extend E1/T1/J1 trunk, you need to install EX30 expansion board on the PBX. One EX30 expansion board provides an E1/T1/J1 port.

Differences between E1, T1, and J1

The PRI consists of B channels at 64 kbit/s each and D channel at 64 kbit/s each. The B channels are used for voice or user data, and the D channel is used for any combination of data, control/signalling, and X.25 packet networking.

According to the number of B-channels and D-channels, there are three types of PRI interface: E1, T1, and J1.

PRI Type	Description
E1	Contains 30 B-channel and 2 D-channel and is used in Europe, China, and most of the Asian countries.
T1	Contains 23 B-channel and one D-channel and is used in the USA, Canada, and Hong Kong.
J1	It is almost the same as T1 but used in Japan with some slight modifications, this is the Japanese standard for PRI.

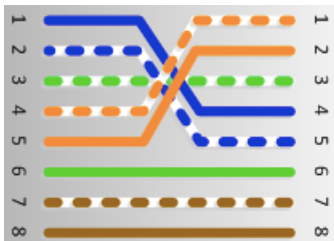
E1/T1/J1 crossover cable

You can get an E1/T1/J1 crossover cable from the carrier or make a crossover cable yourself.

Note:

E1/T1/J1 crossover cable is different from the Ethernet cable, but you can make a crossover cable by an Ethernet cable.

The pinouts of an E1/T1/J1 crossover cable is shown as the following figure.



Set up an E1/T1/J1 Trunk

This topic describes how to set up an E1/T1/J1 trunk on Yeastar P-Series PBX System.

Background information

ISDN uses circuit-switching to establish a physical permanent point-to-point connection from the source to the destination. ISDN has standards defined by the ITU that encompass the OSI bottom three layers of which are Physical, Data Link, and Network.

To set up an E1/T1/J1 trunk, you need to make sure both the Physical layer and the Data Link layer run properly.




Prerequisites

- E1/T1/J1 trunk is only supported on Yeastar P560 and P570.
- Install at least one EX30 expansion board on the PBX.
- Prepare an [E1/T1/J1 crossover cable](#).
- Gather signalling information of the E1/T1/J1 trunk from the ISDN carrier, such as the following information.
 - Carrier type
 - Signalling type
 - Line coding Mechanism
 - Framing Mode
 - D-Channel
 - B-Channel

Procedure

1. Connect one end of E1/T1/J1 cable to the E1/T1/J1 port on the PBX, and connect the other end of the cable to the ISDN provider's equipment.
2. Check if the trunk is successfully connected to the PBX on the Physical layer.

Log in to PBX management portal, go to Extension and Trunk > Trunk to check the E1/T1/J1 trunk status.

- If the trunk status shows  or , the physical layer of this trunk is correct.
 - If the trunk status shows , the physical layer of this trunk is incorrect, check the cable or contact Yeastar support to solve it.
3. Configure the E1/T1/J1 trunk settings to make the Data Link layer up.
 - a. Go to Extension and Trunk > Trunk, edit the desired E1/T1/J1 trunk.
 - b. On the Basic page, configure the required settings according to the parameters that are provided by the ISDN carrier.
 - c. Optional: Configure other settings of the E1/T1/J1 trunk according to the carrier's requirements.

For more information of the E1/T1/J1 trunk information, see [E1/T1/J1 Trunk Settings](#).

- d. Click Save.
- e. Reboot the system to take effect.

Result

Go to Extension and Trunk > Trunk to check the trunk status on the trunk list page.

If the status shows , the trunk is ready for use.

For more information of E1/T1/J1 trunk status, see [E1/T1/J1 Trunk status](#).

What to do next

- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see [Set up an Inbound Route](#).
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see [Set up an Outbound Route](#).

E1/T1/J1 Trunk Settings

This topic describes all the settings on an E1/T1/J1 trunk for reference.

E1/T1/J1 signaling type



Yeastar P560 and P570 support the following ISDN signaling type, you can configure the trunk according to the information provided by the ISDN carrier.


- [PRI](#)
- [MFC/R2](#)
- [SS7](#)
- [E&M](#)


PRI settings

The table below shows the Basic settings and Advanced settings for the E1/T1/J1 trunk (PRI signaling type).

Setting	Description
Basic Settings	
Name	Give this trunk a name to help you identify it.
Interface Type	Specify the interface type according to the trunk specification. <ul style="list-style-type: none"> • E1 • T1 • J1
Signaling	Specify the Signaling type PRI.
Framing	Select the frame format for this trunk according to the requirements of your country and carrier. The frame format of the PBX must be the same as that of the carrier. Otherwise, the link cannot be established. <ul style="list-style-type: none"> • When the Interface Type is E1, Framing options are:

Setting	Description
Basic Settings	
	<ul style="list-style-type: none"> ◦ Enable CRC4 ◦ Disable CRC4 <div style="border: 1px solid #add8e6; padding: 5px; margin: 10px 0;"> <p> Note: CRC4 is a method of checking for errors in data transmitted on E1 trunk lines.</p> </div> <ul style="list-style-type: none"> • When the Interface Type is T1 or J1, Framing options are: <ul style="list-style-type: none"> ◦ ESF ◦ D4
Line Code	<p>Choose the line code for this trunk according to the direction provided by carrier.</p> <ul style="list-style-type: none"> • When the Interface Type is E1, Line Code options are: <ul style="list-style-type: none"> ◦ HDB3 ◦ AMI • When the Interface Type is T1 or J1, Line Code options are: <ul style="list-style-type: none"> ◦ B8ZS ◦ AMI
Codec	<p>Choose the codec for this trunk.</p> <ul style="list-style-type: none"> • a-law • u-law
Echo Cancellation	<p>This option enables or disables echo cancellation.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin: 10px 0;"> <p> Note: If an echo occurs during a call, you can enable echo cancellation.</p> </div>
D Channel	<p>Set the channel used to carry control information and signaling information.</p> <ul style="list-style-type: none"> • If Interface Type is set to E1, enter a channel number from 1 to 31. • If Interface Type is set to T1 or J1, enter a channel number from 1 to 24.
Switch Type	<p>Configure the switch type according to the direction provided by carrier.</p>



Setting	Description
Basic Settings	
	<ul style="list-style-type: none"> • If Interface Type is set to E1, Switch Type option are: <ul style="list-style-type: none"> ◦ EuroISDN ◦ Q.SIG • If Interface Type is set to T1 or J1, Switch Type option are: <ul style="list-style-type: none"> ◦ EuroISDN ◦ National 2 ◦ National 1 ◦ DMS100 ◦ AT&T 4ess ◦ Lucent 5ess ◦ Q.SIG
Signaling Role	<p>Specify whether this interface will act as the user or the network.</p> <ul style="list-style-type: none"> • User: If the service provider acts as the network, the PBX needs to be set as the User. • Network: If the service provider acts as the user, the PBX needs to be set as the Network.
Overlap Dial	<p>Define whether the system can dial this switch using overlap digits or not. If you need Direct Dial-in, then enable this option.</p>
Advanced Settings	
Facility-based ISDN Supplementary Services	<p>Decide whether to enable transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility) or not.</p>
PRI Indication	<p>Select the PRI Indication.</p> <ul style="list-style-type: none"> • Out-of-Band: Use RELEASE, DISCONNECT or other messages with CAUSE to indicate call progress (e.g. cause: unassigned number or user busy). • Inband: Use in-band tones to play busy or congestion signal to the other side. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Inband notification is not available on all PRI/BRI subscription lines.</p> </div>
Reset Interval (s)	<p>This sets the time in seconds between restart of unused B channels. The default is "Never".</p>



Setting	Description
Basic Settings	
	 Note: Set the interval to "Never" if you do not wish the channel to restart.
Carrier Hangup Tone Detection	<ul style="list-style-type: none"> • If this option is enabled, you will hear the hangup tone played by your carrier when the other party hangs up. (Please first check with your carrier whether they will send the prompt or not.). • If disabled, you will hear the hangup tone played by the system when the other party hangs up.
Dialplan	
Calling Party Numbering Plan	Select the Calling Party Numbering Plan.
Calling Party Numbering Type	Select the Calling Party Numbering Type.
Called Party Numbering Plan	Select the Called Party Numbering Plan.
Called Party Numbering Type	Select the Called Party Numbering Type.
Presentation Indicator	The PI provides instructions on whether the provided calling line identity is allowed to be presented, or indicates that the number is not available.
Screen Indicator	The SI provides information on the source and the quality of the provided information.
ISDN Dialplan	Enable or disable the ISDN/telephony numbering plan (Recommendation E.164)
International Prefix	Dialplan: '(Calling Party Numbering Plan:ISDN +)Calling Party Numbering Type:International'
National Prefix	Dialplan: '(Calling Party Numbering Plan:ISDN +)Calling Party Numbering Type:National'
Local Prefix	Dialplan: '(Calling Party Numbering Plan:ISDN +)Calling Party Numbering Type:Subscriber'
Private Prefix	Dialplan: 'Calling Party Numbering Plan:private + Calling Party Numbering Type:Subscriber'

Setting	Description
Basic Settings	
Unknown Prefix	Dialplan: '(Calling Party Numbering Plan:ISDN +)Calling Party Numbering Type:Unknown'

MFC/R2 settings

The table below shows the Basic settings and Advanced settings for the E1/T1/J1 trunk (MFC/R2 signaling type).


Setting	Description
Basic Settings	
Name	Give this trunk a name to help you identify it.
Signaling	Specify the Signaling type MFC/R2.
Framing	<p>Select the frame format for this trunk according to the requirements of your country and carrier. The frame format of the PBX must be the same as that of the carrier. Otherwise, the link cannot be established.</p> <p>Framing options are:</p> <ul style="list-style-type: none"> • Enable CRC4 • Disable CRC4 <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: CRC4 is a method of checking for errors in data transmitted on E1 trunk lines.</p> </div>
Line Code	<p>Choose the line code for this trunk according to the direction provided by carrier.</p> <p>Line Code options are:</p> <ul style="list-style-type: none"> • HDB3 • AMI
Echo Cancellation	<p>This option enables or disables echo cancellation.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: If an echo occurs during a call, you can enable echo cancellation.</p> </div>
Variant	Set the MFC/R2 variant.



Setting	Description
Basic Settings	
	<ul style="list-style-type: none"> • Argentina • Brazil • China • Czech • Colombia • Ecuador • Indonesia • ITU • Mexico • Philippines • Venezuela
Category	<p>Set the category of the calling party.</p> <ul style="list-style-type: none"> • National • National priority • International • International Priority • Collect Call
MAX DNIS	<p>Maximum amount of DNIS to ask for.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: If you wish to customize the size, enter the value in the text box directly.</p> </div>
MAX ANI	Maximum amount of ANI to ask for.
Advanced Settings	
Forced Release	<p>Enable or disable forced release of channel.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: If the call can not be hung up properly, check this option.</p> </div>
Immediate Accept	<p>Most variants of MFC/R2 offer a way to go directly to the call accepted state, by passing the use of group B and II tones. This option enables or disables the use of that feature for incoming calls. The default is unchecked.</p>
Double Answer	<p>Block collect calls with double answer. This will cause that every answer signal is changed by answer -> clear back -> answer. The default is unchecked.</p>

Setting	Description
Basic Settings	
Charge Calls	Whether to report to the other end "accept call with charge" or not.
Allow Collect Calls	Specify whether to accept collect calls or not.
MF Back Timeout (ms)	MFC/R2 value in milliseconds for the MF timeout.
Metering Pulse Timeout (ms)	MFC/R2 value in milliseconds for the metering pulse timeout. Enter "-1" to use the value.
Incoming DTMF Mode	Specify the incoming DTMF mode.
Outgoing DTMF Mode	Specify the outgoing DTMF mode.

SS7 settings

The table below shows the Basic settings and Advanced settings for the E1/T1 trunk (SS7 signaling type).


Setting	Description
Basic Settings	
Name	Give this trunk a name to help you identify it.
Signaling	Specify the Signaling type SS7.
Framing	<p>Select the frame format for this trunk according to the requirements of your country and carrier. The frame format of the PBX must be the same as that of the carrier. Otherwise, the link cannot be established.</p> <p>Framing options are:</p> <ul style="list-style-type: none"> • Enable CRC4 • Disable CRC4 <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: CRC4 is a method of checking for errors in data transmitted on E1 trunk lines.</p> </div>
Line Code	<p>Choose the line code for this trunk according to the direction provided by your carrier.</p> <p>Line Code options are:</p>


Setting	Description
Basic Settings	
	<ul style="list-style-type: none"> • HDB3 • AMI
Codec	Choose the codec for this trunk.
Echo Cancellation	<p>This option enables or disables echo cancellation.</p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: If an echo occurs during a call, you can enable echo cancellation.</p> </div>
D Channel	Set the channel used to carry control information and signaling information. Enter a channel number from 1 to 31.
Variant	<p>Set the SS7 variant.</p> <ul style="list-style-type: none"> • ANSI: 24 bits • China: 24 bits • ITU: 14 bits
Linkset	Display SS7 linkset numbers.
Network indicator	Specify the network indicator according to the network environment.
SLC	Specify the Signal Linking Code.
OPC	Specify the Originating Point Code. This is generally assigned by your carrier.
DPC	Specify the Destination Point Code. This is generally assigned by your carrier.
Advanced Settings	
Start CIC No.	<p>Specify the Circuit Identification Code number of the first B channel of E1 line (SS7).</p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: The suggested value is the multiples of 32 plus 1, for example: 1, 33, 65.</p> </div>
Calling Party Number Type	<p>Specify the calling party number type.</p> <ul style="list-style-type: none"> • National • International • Subscriber

Setting	Description
Basic Settings	
	<ul style="list-style-type: none"> • Unknown
Called Party Number Type	<p>Specify the called party number type.</p> <ul style="list-style-type: none"> • National • International • Subscriber • Unknown

E&M settings

The table below shows the Basic settings and Advanced settings for the E1/T1/J1 trunk (E&M signaling type).

Setting	Description
Name	Give this trunk a name to help you identify it.
Interface Type	<p>Specify the interface type according to the trunk specification.</p> <ul style="list-style-type: none"> • E1 • T1 • J1
Signaling	Specify the Signaling type E&M.
Framing	<p>Select the frame format for this trunk according to the requirements of your country and carrier. The frame format of the PBX must be the same as that of the carrier. Otherwise, the link cannot be established.</p> <ul style="list-style-type: none"> • When the Interface Type is E1, Framing options are: <ul style="list-style-type: none"> ◦ Enable CRC4 ◦ Disable CRC4 <div style="border: 1px solid #add8e6; padding: 5px; margin: 10px 0;"> <p> Note: CRC4 is a method of checking for errors in data transmitted on E1 trunk lines.</p> </div> • When the Interface Type is T1 or J1, Framing options are: <ul style="list-style-type: none"> ◦ ESF ◦ D4

Setting	Description
Line Code	Choose the line code for this trunk according to the direction provided by your carrier. Line Code options are: <ul style="list-style-type: none"> • HDB3 • AMI
Codec	Choose the codec for this trunk.
Echo Cancellation	This option enables or disables echo cancellation. <div style="border: 1px solid #00a0e3; padding: 5px;">  Note: If an echo occurs during a call, you can enable echo cancellation. </div>

DIDs/DDIs

Direct Inward Dialling (DID), also called Direct Dial-in (DDI), is a service offered by telephone companies. For more information of DID concepts, see [DID Number Overview](#).

- DID numbers are usually configured on inbound routes to distinguish inbound calls.
For more information, see [Route Inbound Calls based on DID Numbers](#).
- For more instructions on configuring the DID numbers, see [Configure DID Numbers on a Trunk](#).

Inbound Caller ID Reformatting

When a user calls in the PBX, the trunk provider may send a caller ID that is inconvenient for you to redial directly.


In this case, you can reformat inbound caller ID based on a trunk. The caller ID will be reformatted before it is sent to the called party.

For more information, see [Reformat Inbound Caller ID based on a Trunk](#).

Outbound Caller ID

Outbound caller ID is the phone number or name that is displayed on the called party's device.

You can set up a global outbound caller ID for a trunk or assign caller IDs for extension users.

 **Note:**
By default, each trunk has a default phone number that will be displayed on the called party's device. Outbound Caller ID configuration requires support from the trunk provider. Con-

tact your trunk provider first before you configure Outbound Caller ID, or the settings won't take effect and outbound calls may fail.

If you set the caller ID number, when users make outbound calls through this trunk, the called party will see this caller ID number instead of the calling party's number.

For more information of outbound caller ID configurations, see [Customize Outbound Caller IDs](#)

ISDN BRI Trunk

BRI Trunk Overview

This topic describes what is BRI trunk and provides the information of BRI cable.

What is BRI trunk

Basic Rate Interface (BRI) is an Integrated Services Digital Network (ISDN) access method, typically used for home and small offices.

The BRI configuration provides 2 bearer channels (B channels) at 64 kbit/s each and 1 data channel (D channel) at 16 kbit/s. The B channels are used for voice or user data, and the D channel is used for any combination of data, control/signalling, and X.25 packet networking.

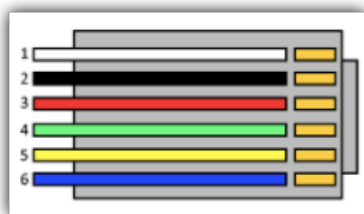
BRI cable

Yeastar P-Series PBX System supports for connecting an RJ11 4 pin cable or an RJ12 6 pin cable to a BRI port.

RJ11 4 pin connector



RJ12 6 pin connector



Set up a BRI Trunk

This topic describes how to set up a BRI trunk on Yeastar P-Series PBX System.

Prerequisites

- Install at least one B2 module on the PBX.
- Prepare a [BRI cable](#).
- Gather signalling information of the BRI trunk from the ISDN carrier, such as the following information.
 - Signalling
 - Switch Type
 - Signalling Role

Background information




ISDN uses circuit-switching to establish a physical permanent point-to-point connection from the source to the destination. ISDN has standards defined by the ITU that encompass the OSI bottom three layers of which are Physical, Data Link, and Network.

To set up a BRI trunk, you need to make sure both the Physical layer and the Data Link layer run properly.

Procedure

1. Connect one end of BRI cable to the BRI port on the PBX, and connect the other end of the cable to the ISDN provider's equipment.
2. Check if the trunk is successfully connected to the PBX on the Physical layer.

Log in to PBX management portal, go to Extension and Trunk > Trunk to check the BRI trunk status.

- If the trunk status shows  or , the physical layer of this trunk is correct.
 - If the trunk status shows , the physical layer of this trunk is incorrect, check the cable or contact Yeastar support to solve it.
3. Configure the BRI trunk settings to make the Data Link layer up.
 - a. Go to Extension and Trunk > Trunk, edit the desired BRI trunk.
 - b. On the Basic page, configure the required settings according to the parameters that are provided by the ISDN carrier.
 - c. Optional: Configure other settings of the BRI trunk according to the carrier's requirements.

For more information of the BRI trunk information, see [BRI Trunk Settings](#).

- d. Click Save.
- e. Reboot the system to take effect.

Result

Go to Extension and Trunk > Trunk to check the trunk status on the trunk list page.

If the status shows , the trunk is ready for use.

For more information of BRI trunk status, see [BRI Trunk status](#).

What to do next


- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see [Set up an Inbound Route](#).
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see [Set up an Outbound Route](#).

BRI Trunk Settings

This topic describes all the settings on a BRI trunk for reference.

Basic settings

The following settings are required for a BRI trunk, which affect the connection status of the trunk.

Setting	Description
Name	Give this trunk a name to help you identify it.
Signaling	Specify the signaling type according to the direction provided by your service provider. <ul style="list-style-type: none"> • Peer to Peer • Peer to Multiple Peers
Signaling Role	Specify whether this interface will act as the user or the network. <ul style="list-style-type: none"> • User • Network <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note:</p> <ul style="list-style-type: none"> • If the service provider acts as the network, the PBX needs to be set as the user. • If the service provider acts as the user, the PBX needs to be set as the network. </div>

Setting	Description
Switch Type	<p>Configure the switch type according to the direction provided by your service provider.</p> <ul style="list-style-type: none"> • EuroISDN • National 2 • National 1 • DMS100 • AT&T 4ess • Lucent 5ess • Q.SIG

Advanced settings



Advanced settings affect inbound calls and outbound calls through the BRI trunk. Incorrect configuration may cause call failure.

The following settings are included on the Advanced page.

- [Advanced](#)
- [Dialplan](#)

Advanced

Setting	Description
Echo Cancellation	Enable or disable echo cancellation.
Facility-based ISDN Supplementary Services	Decide whether to enable transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility) or not.
Codec	Select the codec for this trunk.
Overlap Dial	Define whether the system can dial this switch using overlap digits or not. If you need Direct Dial-in, then enable this option.
Reset Interval	This sets the time in seconds between restart of unused B channels. Set the interval to Never if you don't like the channel to restart.
PRI Indication	<p>Select the PRI Indication.</p> <ul style="list-style-type: none"> • Out-of-Band: Use RELEASE, DISCONNECT or other messages with CAUSE to indicate call

Setting	Description
	<p>progress (e.g. cause: unassigned number or user busy).</p> <ul style="list-style-type: none"> • Inband: Use in-band tones to play busy or congestion signal to the other side. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Inband notification is not available on all PRI/BRI subscription lines.</p> </div>
Carrier Hangup Tone Detection	<ul style="list-style-type: none"> • Check this option: You will hear the hangup tone played by your carrier when the other party hangs up. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: First check with your carrier whether they will send the prompt or not.</p> </div> <ul style="list-style-type: none"> • Uncheck this option: You will hear the hangup tone played by the system when the other party hangs up.
Hide Outbound Caller ID	Whether to hide caller ID or not when calling out through this trunk.
Ignore Remote Hold Indications	If you wish to ignore remote hold indications and use PBX's Music on Hold, enable this option.

Dialplan

Setting	Description
Calling Party Numbering Plan	Select the Calling Party Numbering Plan.
Calling Party Numbering Type	Select the Calling Party Numbering Type.
Called Party Numbering Plan	Select the Called Party Numbering Plan.
Called Party Numbering Type	Select the Called Party Numbering Type.
Presentation Indicator	The PI provides instructions on whether the provided calling line identity is allowed to be presented, or indicates that the number is not available.

Setting	Description
Screen Indicator	The SI provides information on the source and the quality of the provided information.
ISDN Dialplan	ISDN/telephony numbering plan (Recommendation E.164)
International Prefix	Dialplan: '(Calling Party Numbering Plan:ISDN +)Calling Party Numbering Type:International'.
National Prefix	Dialplan: '(Calling Party Numbering Plan:ISDN +)Calling Party Numbering Type:National'.
Local Prefix	Dialplan: '(Calling Party Numbering Plan:ISDN +)Calling Party Numbering Type:Subscriber'.
Private Prefix	Dialplan: 'Calling Party Numbering Plan:private + Calling Party Numbering Type:Subscriber'.
Unknown Prefix	Dialplan: '(Calling Party Numbering Plan:ISDN +)Calling Party Numbering Type:Unknown'.

DIDs/DDIs

Direct Inward Dialling (DID), also called Direct Dial-in (DDI), is a service offered by telephone companies. For more information of DID concepts, see [DID Number Overview](#).

- DID numbers are usually configured on inbound routes to distinguish inbound calls.
For more information, see [Route Inbound Calls based on DID Numbers](#).
- For more instructions on configuring the DID numbers, see [Configure DID Numbers on a Trunk](#).

Inbound Caller ID Reformatting

When a user calls in the PBX, the trunk provider may send a caller ID that is inconvenient for you to redial directly.


In this case, you can reformat inbound caller ID based on a trunk. The caller ID will be reformatted before it is sent to the called party.

For more information, see [Reformat Inbound Caller ID based on a Trunk](#).

Outbound Caller ID

Outbound caller ID is the phone number or name that is displayed on the called party's device.

You can set up a global outbound caller ID for a trunk or assign caller IDs for extension users.

 Note:

By default, each trunk has a default phone number that will be displayed on the called party's device. Outbound Caller ID configuration requires support from the trunk provider. Contact your trunk provider first before you configure Outbound Caller ID, or the settings won't take effect and outbound calls may fail.

If you set the caller ID number, when users make outbound calls through this trunk, the called party will see this caller ID number instead of the calling party's number.

For more information of outbound caller ID configurations, see [Customize Outbound Caller IDs](#)

Call Control

Emergency Calling

Emergency Calling Overview

This topic describes concepts that you need to know before managing emergency calling, including requirements and restrictions, basic emergency calling, and enhanced emergency calling.

Requirements

To make an emergency call, you should make sure the following requirements are met:

- IP phones or soft phones must be registered to Yeastar P-Series PBX System.
- At least one trunk should be configured for an emergency number.

Basic emergency calling

The basic emergency service only connects a caller to the local Public Safety Answering Point (PSAP), but no location is provided. Emergency callers must be ready to provide their location information for the PSAP. PSAP then arranges appropriate emergency response after communicating with the callers.

For more information, see [Set up Basic Emergency Calling](#).

Enhanced emergency calling

Enhanced emergency service is only available for specific countries and regions, such as E911 in North America, E112 in continental Europe, E999 in England, etc.

For an enhanced emergency call, PSAP can immediately pinpoint the caller's location based on the calling number.

Important:

For wireless IP phones and softphones (such as Linkus), the emergency caller's location can only be determined by the Emergency Outbound Caller ID configured on the PBX.

For more information, see [Set up Enhanced Emergency Calling](#).

Terminology

The following list defines the key terminology for enhanced emergency calling.

PSAP

A Public Safety Answering Point (PSAP) is responsible for receiving emergency calls and arranging appropriate emergency response, such as dispatching a police, fire, or ambulance team.

ERL

An Emergency Response Location (ERL) is a specific geographic location to which an emergency response team may be dispatched. To provide the PSAP with the emergency caller's precise location, you may need to set multiple ERLs.

ELIN

An Emergency Location Identification Number (ELIN) is the phone number (Caller ID), which is associated with an ERL. When an emergency call is made, the ELIN is displayed on the PSAP side so that they can match the caller ID with the ERL.

Note:

ELIN is also helpful for PSAP to call the emergency caller back in case the call is disconnected.

Examples of ERL/ELIN mapping:

- One ERL for each building

All the users in the same building are associated with the same ELIN.

ELIN	ERL
6085225672	No. 63-2 Wanghai Road, 2nd Software Park, Xiamen
6085225673	No. 63-3 Wanghai Road, 2nd Software Park, Xiamen

- One ERL for each building floor

All the users on the same floor of a building are associated with the same ELIN.

ELIN	ERL
6085225682	5/F, No. 63-2 Wanghai Road, 2nd Software Park, Xiamen
6085225683	4/F, No. 63-2 Wanghai Road, 2nd Software Park, Xiamen

- One ERL for each room

Each user of a room has a unique ELIN.


ELIN	ERL
6085225692	Room3005, No.1 Guanri Road, Software Park Siming District Xiamen
6085225693	Room3006, No.1 Guanri Road, Software Park Siming District Xiamen

Set up Basic Emergency Calling


To ensure that users can make emergency calls for help when an accident occurs, you need to set up emergency calling in Yeastar P-Series PBX System. This topic describes how to set up [basic emergency calling](#) in Yeastar P-Series PBX System.

Procedure

1. Log in to PBX management portal, go to Call Control > Emergency Number, click Add.
2. In the Name field, specify a name to help you identify it.
3. In the Emergency Number field, enter the emergency number.
4. Leave the Emergency Outbound Caller ID Priority field as the default setting.


 Note:

- Emergency Outbound Caller ID Priority setting is typically for [enhanced emergency calling](#), this setting will not affect basic emergency calling.
 - For basic emergency calling, you don't need to set Emergency Outbound Caller ID for extensions and trunks.
5. In the Trunk's Emergency Outbound Caller ID field, configure trunks for emergency calls.

 Note:


Emergency calls have the highest priority. If the selected trunk is occupied, PBX will terminate the ongoing call, and place the emergency call.

- a. Click Add.
- b. In the drop-down list of Trunk, select a trunk.
- c. Leave the Trunk's Emergency Outbound Caller ID field blank.

 Note:

Do not set emergency outbound caller ID for basic emergency calling, or the emergency calls may fail.

- d. Optional: Click Add to add another trunk and repeat step a - step c.

 Note:

If the first trunk cannot work properly, the PBX will use the second trunk to make calls.

6. Click Save and Apply.

What to do next

After setting up an emergency calling, you may need to consider the following configurations:

- [Set up a Route for PSAP Callbacks](#)
- [Add an Emergency Notification Contact](#)

Set up Enhanced Emergency Calling

To ensure that users can make emergency calls for help when an accident occurs, you need to set up emergency calling in Yeastar P-Series PBX System. This topic describes how to set up [enhanced emergency calling](#) in Yeastar P-Series PBX System.


Prerequisites

Purchase enhanced emergency service from an Internet Telephony Service Provider (ITSP).

ITSP will provide DID numbers that are associated with your locations. DID number is also called Emergency Location Identification Number (ELIN).


Procedure

1. Log in to PBX management portal, go to Call Control > Emergency Number, click Add.
2. In the Name field, specify a name to help you identify it.
3. In the Emergency Number field, enter the emergency number.
4. In the Emergency Outbound Caller ID Priority field, select which outbound caller ID will be sent to the Public Safety Answering Point (PSAP) in priority when an emergency call is made.
 - Trunk's Emergency Outbound Caller ID: Select this option if you want to set a common ELIN for all extension users. PSAP receives the trunk's emergency outbound caller ID no matter who makes the emergency call, which indicates PSAP receives a common location information.
 - Extension's Emergency Outbound Caller ID: Select this option if you want to [assign ELINs for individual users](#).
 - Extension users with specific ELINs are associated with their respective locations.
 - Extension users without specific ELINs share a common ELIN (the trunk's emergency outbound caller ID) and are associated with a common location.
5. In the Trunk's Emergency Outbound Caller ID field, configure trunks for emergency calls.
 - a. In the drop-down list of Trunk, select a trunk.

 Note:

Emergency calls have the highest priority. If the selected trunk is occupied, PBX will terminate the ongoing call, and place the emergency call.

- b. In the Trunk's Emergency Outbound Caller ID, enter the Emergency Location Identification Number (ELIN) that you have purchased from the trunk provider.
- c. Optional: Click Add to add another trunk and repeat step a - step c.

 Note:

If the first trunk cannot work properly, the PBX will use the second trunk to make calls.

6. Click Save and Apply.

Assign ELINs for individual users

To provide the PSAP with the emergency caller's precise location, you may need to purchase multiple ELINs and assign these ELINs to extension users.

1. Log in to PBX management portal, go to Extension and Trunk > Extension, click to edit the desired extension.
2. On the extension User page, scroll down the page, enter the ELIN in the Emergency Outbound Caller ID field.
3. Click Save and Apply.

After the user dials an emergency number, the PSAP will locate the specific geographic location of the user by the extension user's ELIN.

What to do next

After setting up an emergency calling, you may need to consider the following configurations:

- [Set up a Route for PSAP Callbacks](#)
- [Add an Emergency Notification Contact](#)

Set up a Route for PSAP Callbacks

In case that the emergency caller is not available to answer the returned call from PSAP, you can set up an inbound route to forward the call to an on-site security personnel.

Procedure

1. Log in to PBX management portal, go to Call Control > Inbound Route.
2. Click Add to add an inbound route for PSAP callbacks.
3. In the Name field, specify a name to help you identify it.

4. In the Caller ID Pattern section, add all the emergency numbers that you have set on the PBX.
 - a. Click Add.
 - b. In the Pattern field, enter the emergency number.
 - c. Optional: To add another emergency number, repeat step a - b.
5. In the Trunk section, select the trunks that are used for emergency calls to the Selected box.
6. In the Default Destination field, select Extension, and select the user who is responsible for answering the returned calls from PSAP.
7. Leave other fields as the default settings.
8. Click Save and Apply.

Result

When a PSAP operator calls back, the call will be forwarded to the extension user that is configured on the inbound route.

Related information


[Set up Basic Emergency Calling](#)

[Set up Enhanced Emergency Calling](#)


Manage Emergency Numbers

After you add emergency numbers, you can edit or delete them.

Edit an emergency number

1. Log in to PBX management portal, go to Call Control > Emergency Number, click  beside the emergency number that you want to edit.
2. Edit information of emergency number.
3. Click Save and Apply.

Delete an emergency number

1. Log in to PBX management portal, go to Call Control > Emergency Number, click  beside the emergency number that you want to delete.
2. In the pop-up dialog box, click OK to confirm.
3. Click Apply.

Export and Import Emergency Numbers

The emergency numbers configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired emergency numbers in the exported file, and im-

port the file to PBX again. This topic describes how to export and import emergency numbers.

Export emergency numbers

You can export all emergency numbers to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Call Control > Emergency Number.
2. Click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see [Emergency Number Parameters](#).

Import emergency numbers

We recommend that you export emergency numbers to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 50 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information, see [Emergency Number Parameters](#).

Procedure

1. Log in to PBX management portal, go to Call Control > Emergency Number.
2. Click Import.
3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The emergency numbers in the CSV file will be displayed in the Emergency Number list.

Emergency Notification Contacts

Add an Emergency Notification Contact

When a user makes an emergency call, Yeastar P-Series PBX System sends a notification to remind the emergency contacts that who dialed which emergency number.

Procedure

1. Log in to PBX management portal, go to Call Control > Emergency Number > Notification Contacts.
2. Click Add.
3. In the Notification Contact field, select a contact type to receive emergency notifications.

- **Specific Extension:** Send emergency notification to a specific extension (for example, receptionist).

If you select this contact type, select a desired extension from the Specific Extension drop-down list.

- **The Extension Group Manager of the Extension who dialed the emergency number:** Send emergency notification to the extension group manager of the extension who dialed the emergency number.
- **Specific Group Manager:** Send emergency notification to the manager of a specific extension group.


If you select this contact type, select the desired extension group from the Specific Group Manager drop-down list.

- **Custom:** Send emergency notification to an external contact.

If you select this contact type, enter a contact name in the Contact Name field.

4. In the Notification Method field, select a notification method.
 - **Send Email:** The PBX will send notifications to the Email address of the contact.


For more information about emergency Email template, see [Configure Emergency Notification Email](#).

 Note:

- To ensure that PBX can successfully send notifications to the Email address, make sure that the [Email Server](#) is configured correctly.
- If the notification contact is an extension user, make sure that an effective Email address is associated with the user's extension.

- **Call Mobile:** The PBX will call the mobile number of the contact, and play an announcement.

For more information about the announcement, see [Configure Emergency Notification Prompt](#).

 Note:

To ensure that PBX can successfully call the mobile number, make sure that the [Prefix](#) is configured correctly according to the outbound route rule.

- **Call Extension:** The PBX will call the extension number of the contact, and play an announcement.


For more information about the announcement, see [Configure Emergency Notification Prompt](#).

5. Click Save.


Manage Emergency Notification Contacts

After you add emergency notification contacts, you can edit or delete them.

Edit an emergency notification contact

1. Log in to PBX management portal, go to Call Control > Emergency Number > Notification Contact, click  beside the emergency notification contact that you want to edit.
2. Edit emergency notification contact or notification method.
3. Click Save.

Delete an emergency notification contact

1. Log in to PBX management portal, go to Call Control > Emergency Number > Notification Contact.
2. To delete an emergency notification contact, do as follows:
 - a. Click  beside the desired contact.
 - b. In the pop-up dialog box, click OK.
3. To delete emergency notification contacts in bulk, do as follows:
 - a. Select the checkboxes of the desired contacts, click Delete.
 - b. In the pop-up dialog box, click OK.

Configure Emergency Notification Email

Yeastar P-Series PBX System provides a default email template for emergency notification, you can also customize your own template.

Background information

By default, Yeastar P-Series PBX System sends emergency notification emails in the language that you have set in [system email template](#). An emergency notification Email contains the following information:

- Caller information: Include extension name and number.
- Emergency information: Include emergency name and number, and emergency call time.
- PBX information: Include PBX name, SN, LAN IP address, and WAN IP address.

Procedure

1. Log in to PBX management portal, go to Call Control > Emergency Number > Notification Contact.
2. Click Email Template.
3. Customize email template.
 - a. In the Template drop-down list, select Custom.

- b. Edit email subject and content according to your needs.
- c. Click Save.

Configure Emergency Notification Prompt


Yeastar P-Series PBX System provides a default voice prompt for emergency call notification, you can also customize your own prompt.

Background information

The default emergency announcement reminds the contacts that who dialed which emergency number.

Procedure

1. Log in to PBX management portal, go to Call Control > Emergency Number > Notification Contact.
2. Click Notification Prompt.
3. In the pop-up window, change the notification prompt.
 - a. In the Prompt drop-down list, select a desired prompt or upload a custom prompt.

 Note:

The upload prompt file should meet the [audio file requirements](#).

- b. In the Prompt Repeat Count field, set how many times to play the prompt.
- c. Click Save.

Business Hours and Holidays

Overview of Business Hours and Holidays

This topic describes concepts that you need to know before managing business hours and holidays.

Time definition

The following list describes different types of time defined in the Yeastar P-Series PBX System.

Business Hours

Business Hours is the working hours during which you conduct business. A rest break that allows an employee to rest for a short period of time during working days is also considered as Business Hours.

Yeastar P-Series PBX System allows you to set a global business hours and also supports custom business hours for designated users.

- Global Business Hours

Global Business Hours is the main business hours for your company. Global Business Hours may apply to most of the employees who have fixed work schedules.

For more information, see [Set Global Business Hours](#).

- Custom Business Hours

Custom Business Hours is typically for departments with different hours from your main business hours. You need to create custom schedules that accommodate each department's unique hours and call handling needs.

For more information, see [Route Inbound Calls based on Department Hours](#).

Holidays

Holiday defines the days your business is closed due to a holiday. Holidays can be divided into two types:

- Fixed-date Holidays
- Moveable-date Holidays

You can add holidays by date, month, or week according to the holiday type. For more information, see [Create a Holiday](#).

Outside Business Hours

Outside Business Hours is the time periods that are not defined as Business Hours or Holidays.

What is the Business Hours and Holidays used for?

Business Hours and Holidays can be applied to an Inbound Route, an Outbound Route, or Presence Switch.

Apply to an Inbound Route and Outbound Route

Business Hours and Holidays is typically applied in an Inbound Route to control destination of incoming calls based on date and time, and can be also applied in an Outbound Route to limit the use of the Outbound Route based on date and time.

Apply to Extension Presence Switch

Business Hours and Holidays can be applied to automatically switch the extension presence status, regardless of the current presence status.

Global Business Hours

Set Global Business Hours

This topic gives a configuration example to introduce how to set up global business hours for your company.

Background information

Global Business Hours is the main business hours for your company. Global Business Hours may apply to most of the company employees who have fixed work schedules.

This topic assumes that your business hours is as follows:

- Working days: Monday to Friday
- Working hours: 09:00-12:00 and 14:00-18:00
- Lunch break: 12:00-14:00

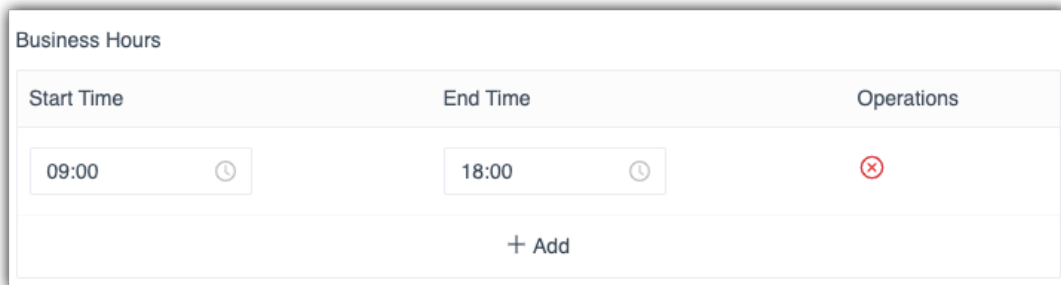
Procedure


1. Log in to PBX management portal, go to Call Control > Business Hours and Holidays.
2. On the Business Hours page, click Add.
3. In the pop-up window, configure your business hours:
 - a. In the Business Hours section, click Add, and specify the hours when your business is open.

Tip:

You can enter the time directly in the text field to quickly set the time.

In this scenario, set the Start Time to 9:00 and set the End Time to 18:00.



Start Time	End Time	Operations
09:00	18:00	
+ Add		

- b. In the Break Hours section, click Add, and specify reset breaks during the working days.

In this scenario, set the Start Time to 12:00 and set the End Time to 14:00.

Break Hours

Start Time	End Time	Operations
12:00 🕒	14:00 🕒	✖
+ Add		

- c. In the Days of week section, select your working days.
 In this scenario, select Monday to Friday.

*** Days of week**

Monday ✕
Tuesday ✕
Wednesday ✕
Thursday ✕
Friday ✕
▼

- d. Click Save and Apply.

Result

- A time group is created for Global Business Hours. In this scenario, the configured time group is defined as below:
 - Business Hours:
 - Monday to Friday, 09:00-18:00
 - Outside Business Hours:
 - Monday to Friday, 18:00 - 23:59, 00:00 - 08:59
 - Saturday and Sunday, 00:00 - 23:59
- You can create more time groups according to your company's business hours. All the time groups created on the Business Hours page are regarded as your company's global business hours.

Business Hours
Holiday

+ Add
Delete

	Business Hours	Break Hours	Days of week	Operations
<input type="checkbox"/>	09:00-12:00		Saturday	✎ ✖
<input type="checkbox"/>	09:00-18:05	12:00-14:00	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday	✎ ✖

Global Business Hours

Total: 2
< 1 >
10 / page ▼


What to do next

- To create call schedules based on the Global Business Hours, see [Route Inbound Calls based on Global Business Hours](#).
- To limit users to make outbound calls based on the Global Business Hours, see [Set up an Outbound Route](#).

Manage Global Business Hours

This topic describes how to edit and delete the time groups that you've defined as your Global Business Hours.

Edit a time group of Global Business Hours

1. Log in to PBX management portal, go to Call Control > Business Hours and Holidays.
2. On the Business Hours page, select a desired time group, click .
3. In the pop-up window, change the time settings.
4. Click Save and Apply.

The Global Business Hours is updated.

Delete a time group of Global Business Hours

1. Log in to PBX management portal, go to Call Control > Business Hours and Holidays.
2. On the Business Hours page, select a desired time group, click Delete.
3. In the pop-up dialog box, click Yes to confirm.

The time group is deleted from the Global Business Hours.

Allow Users to Switch Business Hours Status

If you have configured a time-based inbound route, the system will automatically route calls to different destinations based on the time. However, users may need to force open or close business occasionally. This topic describes how to allow users to switch Business Hours status.

Background information

Scenarios


Users may need to override time condition in the following scenarios:

- Temporary night shift

After business hours, the employee who needs to work in the night can force open the business hours to provide communication services for customers.

- Occasionally leaving

Your company may close the business earlier than usual on a special day. For example, your company will close the business one hour in advance on the Christmas day and you can force close business before you leave.

 Note:

If [presence auto switch based on Business Hours](#) and Holidays is enabled for extension users, their presence status will be switched when Business Hours Status is switched.

Methods

Yeastar P-Series PBX System provides two methods to switch Business Hours status. The permission configurations are different for different methods:

- [Allow users to switch Business Hours status by feature code](#)
- [Allow users to switch Business Hours status on Operator Panel](#)

Allow users to switch Business Hours status by feature code

Procedure


1. Log in to PBX management portal, go to Call Features > Feature Code.
2. Check the feature code of Switch Business Hours Status.

The default feature code is *99. You can use the default one or change it according to your needs.

3. In the Permission field, select the extension users.
4. Click Save and Apply.

Result

The allowed users can dial feature code (default *99) on their phones to switch the current Business Hours status to another one.

 Note:

The Business Hours status will automatically return to a normal status based on the system time.

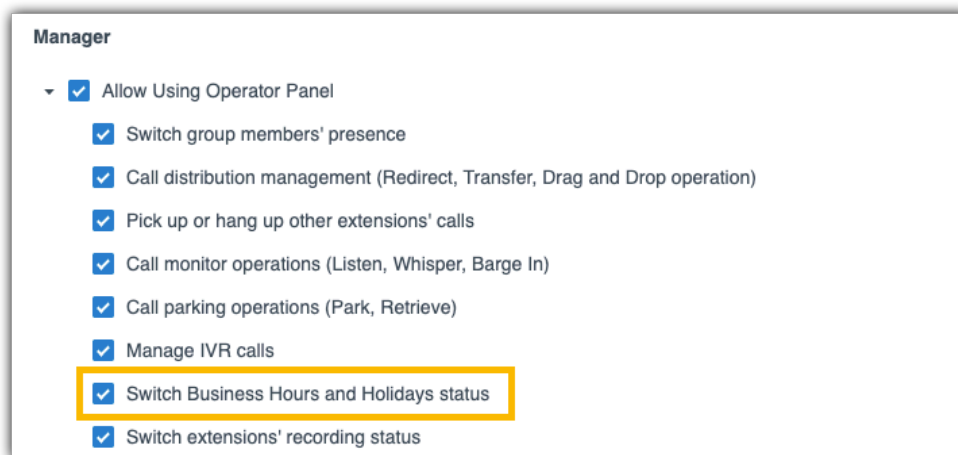
- If the status is Business Hours, dial *99 to force switch the status to Outside Business Hours.
- If the status is Outside Business Hours, dial *99 to force switch the status to Business Hours.
- If the status is Holiday, dial *99 to force switch the status to Business Hours, dial *99 again to switch the status back to Holiday.

Allow users to switch Business Hours status on Operator Panel

You can assign the permission of switching Business Hours status to an extension group manager or a specific user with custom permissions.

Allow an extension group manager to switch Business Hours status

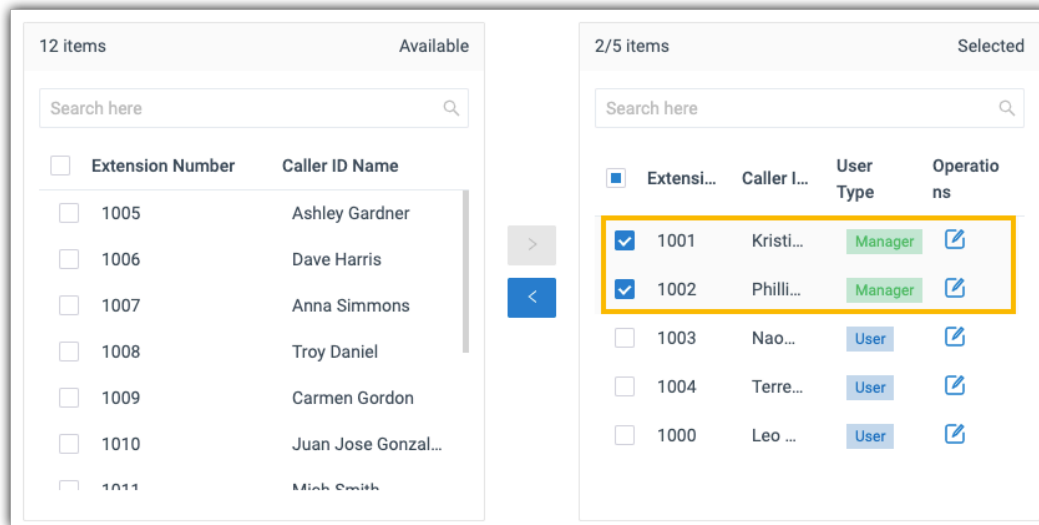
1. Log in to PBX management portal, go to Extension and Trunk > Extension Group.
2. Select an extension group, and click [✎](#).
3. On the Extension Group page, click Group Permissions tab.
4. In the Permission Configuration section, select the checkbox of Switch Business Hours and Holidays status.



5. Click Save and Apply.

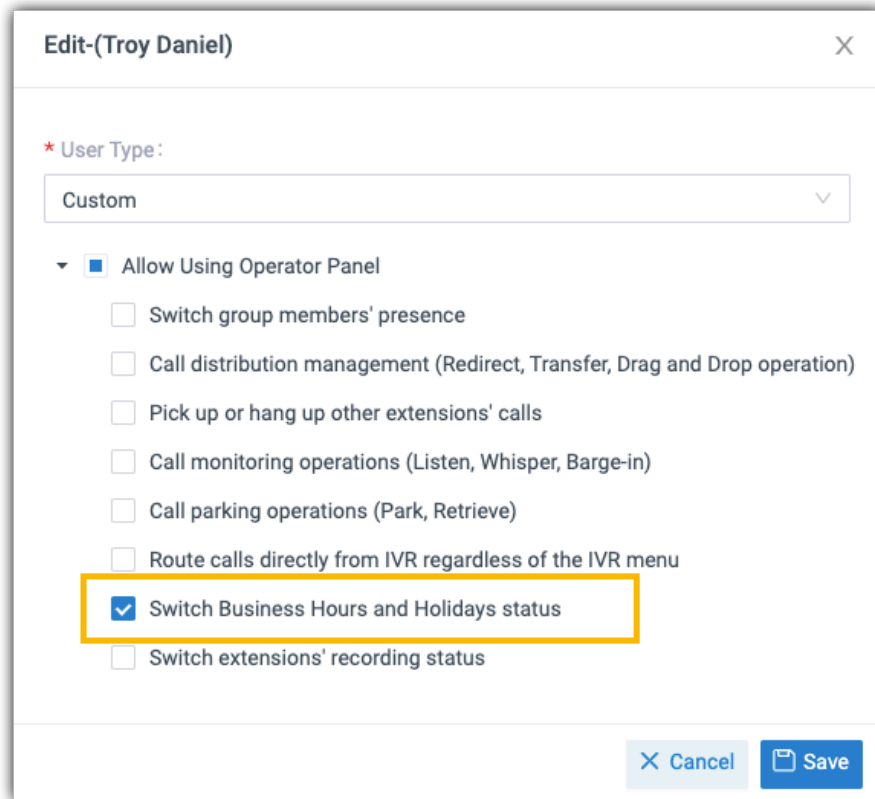
The user whose user type is Manager can switch Business Hours status on Operator Panel.

For more information of the operations, see [Operator Panel User Guide](#).

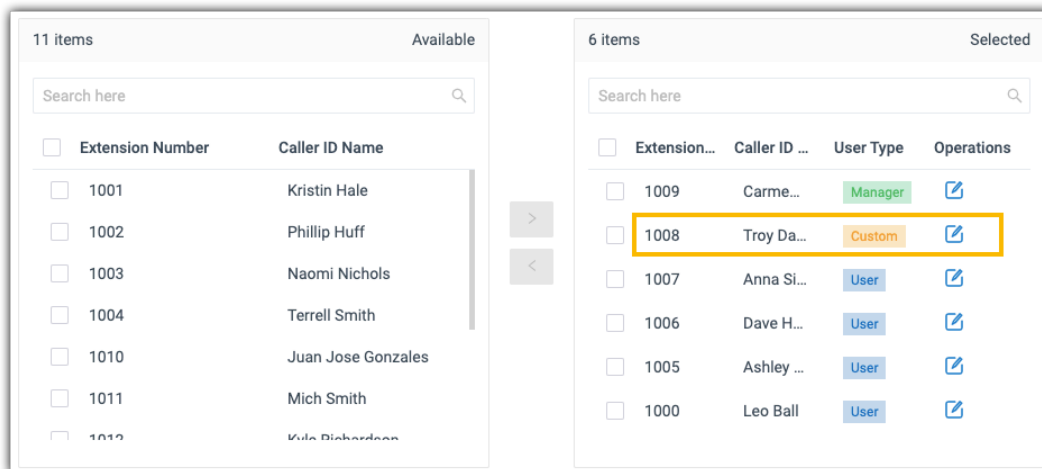


Allow a specific user to switch Business Hours status

1. Log in to PBX management portal, go to Extension and Trunk > Extension Group.
2. Select an extension group, and click
3. In the Members section, edit an extension in the Selected box.
 - a. Select User Type to Custom.
 - b. Select the checkbox of Switch Business Hours and Holidays status.
 - c. Click Save.



The permitted the user can switch Business Hours status on Operator Panel. For more information of the operations, see [Operator Panel User Guide](#).



What to do next

To monitor the Business Hours status, see [Monitor Business Hours Status](#).

Monitor Business Hours Status

You can monitor Business Hours status to ensure that the system is working based on the desired time periods. This topic describes how to monitor Business Hours status by a BLF key on an IP phone.

Background information

For the users who want to monitor Business Hours Status on their phones, you can set a BLF key for each user by [auto provisioning](#).

Note:


Users can also set function keys on their own IP phones. For more information, contact the phone manufacturer.

The users who have [permission to access the Operator Panel](#) can monitor Business Hours Status on the web page directly. For more information, see [Operator Panel User Guide](#).

Prerequisites

Only the permitted extension user can monitor and switch Business Hours status by a BLF key. For more information, see [Allow users to switch Business Hours status by feature code](#).


Procedure

1. Assign function keys for extension users to monitor agent status.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
 - If you want to assign function keys for a specific extension user, click  beside the desired extension.
 - If you want to assign function keys for multiple extensions, select the checkboxes of the desired extensions, and click Edit.
 - b. Click the Function Keys tab.
 - c. Configure function keys.

Note:

The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

- Type: Select BLF.
 - Value: Enter the feature code of Switch Business Hours (*99).
 - Label: Optional. Enter a value, which will be displayed on the phone screen.
- d. Click Save.

2. If the extension hasn't be associated with a phone, see [Auto Provision IP Phones](#) to bind a phone with the extension.
3. If the extension has been associated with a phone, reprovision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click  beside the phone assigned to this extension.

Result

Different status of BLF LED indicates different status.

- Red: The system is in the status of Outside Business Hours or Holiday.
- Green: The system is in the status of Business Hours.
- Off: The BLF configurations are incorrect.

Holidays

Create a Holiday

This topic describes how to create holidays by date, week, and month.

Create a holiday by date

If the holiday date varies every year, you can create a holiday by date.

Example

Chinese Spring Festival varies every year, and 2020 Chinese Spring Festival falls on Jan. 24 to Feb. 8. You can set the holiday as follows.

Configuration Example

1. Log in to PBX management portal, go to Call Control > Business Hours and Holidays > Holidays.
2. On the Holidays page, click Add.
3. In the pop-up window, configure the holiday by date.

The screenshot shows a dialog box titled "Edit Holiday". It has a close button (X) in the top right corner. The dialog contains three required fields, each marked with a red asterisk:

- Name:** A text input field containing "2020 Chinese Spring Festival".
- Holiday Type:** A dropdown menu with "By Date" selected and a downward arrow.
- Date:** A date range input field showing "01/24/2020" followed by a tilde (~) and "02/08/2020", with a calendar icon on the right.

At the bottom right of the dialog, there are two buttons: "Cancel" (with an X icon) and "Save" (with a floppy disk icon).

- Name: Enter the holiday name 2020 Chinese Spring Festival.
- Holiday Type: Select By Date.
- Date: Select the holiday start date and end date.

4. Click Save and Apply.

Create a holiday by month

If the holiday always falls on the same date, you can set a holiday by month.

Example

The Christmas falls on Dec. 25 every year. You can set the holiday as follows.

Configuration Example

1. Log in to PBX management portal, go to Call Control > Business Hours and Holidays > Holidays.
2. On the Holidays page, click Add.
3. In the pop-up window, configure the holiday by month.

The screenshot shows a dialog box titled "Edit Holiday" with a close button (X) in the top right corner. The dialog contains three required fields, each marked with a red asterisk:

- Name:** A text input field containing the text "Christmas".
- Holiday Type:** A dropdown menu with "By Month" selected and a downward arrow on the right.
- Date:** A date range input field showing "12/25" followed by a tilde (~) and another "12/25", with a calendar icon on the right.

At the bottom right of the dialog, there are two buttons: a light blue "Cancel" button with an 'X' icon and a dark blue "Save" button with a floppy disk icon.

- **Name:** Enter the holiday name `Christmas`.
- **Type:** Select `By Month`.
- **Date:** Select the holiday start date and end date.

4. Click `Save` and `Apply`.

Create a holiday by week

If a holiday always falls on the same week, you can set a holiday by week.

Example

Thanksgiving Day falls on the fourth Thursday of November. You can set the holiday as follows.

Configuration Example

1. Log in to PBX management portal, go to `Call Control > Business Hours and Holidays > Holidays`.
2. On the `Holiday` page, click `Add`.
3. In the pop-up window, configure the holiday by week.

The screenshot shows a dialog box titled "Edit Holiday" with a close button (X) in the top right corner. The dialog contains the following fields:

- * Name:** A text input field containing "Thanksgiving Day".
- * Holiday Type:** A dropdown menu with "By Week" selected.
- * Date:** Three dropdown menus: "November", "Fourth Week", and "Tuesday".

At the bottom right of the dialog, there are two buttons: "Cancel" (with an X icon) and "Save" (with a floppy disk icon).

- **Name:** Enter the holiday name Thanksgiving Day.
 - **Holiday Type:** Select By Week.
 - **Date:** Select the month and the day of a specific week.
4. Click Save and Apply.


What to do next

- To set up holiday schedules for inbound calls, see [Set up an Inbound Route](#).
- To limit users to make outbound calls during holidays, see [Set up an Outbound Route](#).

Manage Holidays

This topic describes how to edit and delete a holiday.

Edit a holiday

1. Log in to PBX management portal, go to Call Control > Business Hours and Holidays > Holidays.
2. On the Holidays page, select a desired holiday, click .
3. In the pop-up window, change the holiday settings.
4. Click Save and Apply.

The holiday list is updated.

Delete a holiday

1. Log in to PBX management portal, go to Call Control > Business Hours and Holidays > Holidays.
2. On the Holidays page, select a desired holiday, click Delete.
3. In the pop-up dialog box, click Yes to confirm.

The holiday is deleted from the holiday list.

Inbound Route

Inbound Route Overview

An inbound route allows external callers to reach your system and routes the inbound calls to a specific destination based on the pre-configured rules and criteria.

Types of inbound call routing

Yeastar P-Series PBX System has the following types of inbound call routing based on different criteria, such as time, DID numbers, and Caller IDs.

Note:

- If you don't specify any criteria on an inbound route, there will be no restriction on the inbound route. The system will route all inbound calls to the inbound route destination.
- You can set up multiple criteria on an inbound route. For example, route inbound calls based on time and DID number, or route inbound calls based on DID number and Caller ID number.

Time-based call routing

Time-based call routing connects callers to a destination based on the time that they call. The inbound calls are handled differently according to your company's time schedules.

For more information, see the following topics:

- [Route Inbound Calls based on Global Business Hours](#)
- [Route Inbound Calls based on Department Hours](#)
- [Route Inbound Calls based on Employee Hours](#)

DID-based call routing

DID-based call routing connects callers to a destination based on the phone numbers (also known as DID) that the callers dial. Only when the dialed DID numbers match the DID rules on the inbound route will the calls be routed to the destination.

For more information, see [Route Inbound Calls based on DID Numbers](#).

Caller-ID-based call routing

Caller-ID-based call routing allows you to accept or reject calls based on the caller's phone number. Inbound calls that match the Caller ID pattern on PBX will be routed to the pre-configured destination. For those unmatched, calls can not be established.

For more information, see [Route Inbound Calls based on Caller ID](#) and [Route Inbound Calls by Matched Phonebook Contacts](#).

Inbound route destinations

Yeastar P-Series PBX System provides various inbound destinations to meet your business needs.

The following options are available to help you decide the inbound route destinations:

- Extension
- Extension Voicemail
- Group Voicemail
- Match Selected Extensions
- DID Range to Extension Range
- DID Pattern to Selected Extensions
- IVR
- Ring Group
- Queue
- Conference
- External Number
- Outbound Route
- Fax to Email
- Hang up
- Play Greeting then Hang up

Set up an Inbound Route

To receive inbound calls from external users, you need to set up at least one inbound route.

Background information

Yeastar P-Series PBX System has a default inbound route that will route all the inbound calls to an IVR. You can delete the default inbound route, and add a new one to configure settings according to your needs.

Prerequisites

Ensure that you have set up at least one trunk for external users to call in.


Procedure

1. Log in to PBX management portal, go to Call Control > Inbound Route, click Add.
2. In the Name field, enter a name to help you identify it.
3. Optional: Set an "alert info text" to add to Alert-info header in INVITE request for inbound calls.

When receiving an inbound call, the phone will inspect "Alert-Info" header to determine which ring tone it should use for ringing.

4. Optional: If you want to route inbound calls based on DID numbers, configure DID Pattern.

The PBX will route inbound calls only when the callers dial the matched DID numbers.


 Note:

Leave this field blank to match calls with any or no DID information.

For more information, see [Route Inbound Calls based on DID Numbers](#).

5. Optional: If you want to route inbound calls based on Caller IDs, configure Caller ID Pattern.

The PBX will route inbound calls only when the Caller IDs match the Caller ID pattern.

 Note:

Leave this field blank to match calls with any or no Caller ID info.

For more information, see [Route Inbound Calls based on Caller ID](#).

6. In the Trunk section, select the desired trunks from Available box to Selected box.

The PBX will route inbound calls through this inbound route when external users call the selected trunk number.

7. Configure the inbound route destination.
 - If you want to route inbound calls to one destination whenever the calls reach the system, perform the following operations:
 - a. Keep the Time Condition unselected.
 - b. Configure the Default Destination.
 - If you want to route inbound calls to different destinations based on the time, perform the following operations:
 - a. Select the checkbox of Time Condition.

- b. Select an option from the drop-down list of Time-based Routing Mode.
- c. Configure the destinations based on the time.


If an inbound call reaches the PBX during the time period, PBX will route the call to the selected destination.

For more information of inbound call routing based on time, see the following topics:

- [Route Inbound Calls based on Global Business Hours](#)
- [Route Inbound Calls based on Department Hours](#)
- [Route Inbound Calls based on Employee Hours](#)


8. Optional: To receive faxes through this inbound route, enable Fax Detection and configure the fax destination.

- Extension: The faxes will be sent to the selected extension.
 - For an FXS extension, you need to connect a fax machine to the relevant FXS port to receive faxes.
 - For a SIP extension, you need to register the extension on a SIP compatible fax machine.

 Note:

If the selected extension is deleted, the fax destination will automatically jump to Hang up, and faxes cannot be received through this inbound route.

- Fax to Email: The faxes will be converted to email attachments and be sent to an extension's email address.

 Note:

Make sure the system email is configured correctly, or Fax to Email will fail to work.

For more information of fax setting, see [Fax Overview](#).

9. Click Save and Apply.

Inbound Route Examples

Route Inbound Calls based on Global Business Hours

This topic gives a configuration example to describe how to configure inbound route to control inbound calls based on Global Business Hours, which can be applied to most of the employees.

Background information

Assume that your company's business hours are as follows:

- Working days: Monday to Friday
- Business hours: 09:00-12:00 and 14:00-18:00

When customers call in the trunk FXO-5503301, you want to route the calls based on the time as follows:

- During business hours, route inbound calls to an IVR for business.
- During a holiday, route inbound calls to another IVR for holiday.
- For other time periods, route inbound calls to a voicemail.

Prerequisites

- The trunk for inbound calling has been set up and is ready for use.
- [Global Business Hours is configured](#) according to your company's business hours.
- The desired destination of the inbound route has been configured on the system.

In this scenario, an IVR for business hours, an IVR for holiday should be preconfigured.

For more information of IVR, see [Set up an IVR](#).

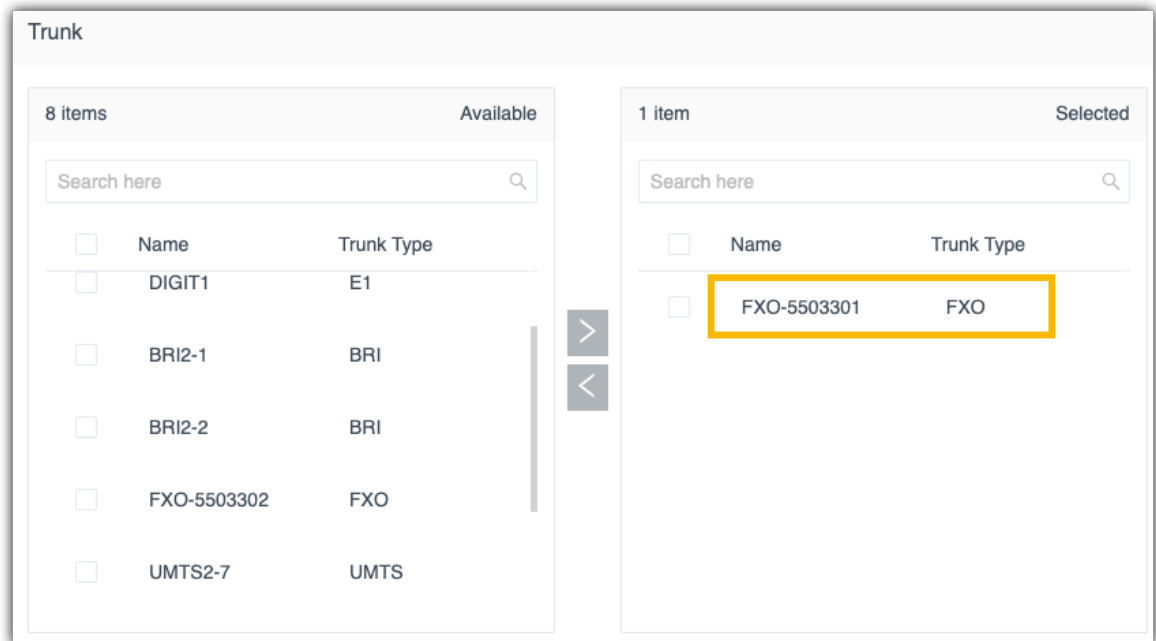
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always be directed to your desired destination.

How to configure inbound route based on DID numbers, see [Route Inbound Calls based on DID Numbers](#).

Procedure

1. Log in to PBX management portal, go to Call Control > Inbound Route, click Add.
2. In the Name field, enter a name to help you identify it.
3. In the Trunk section, select the desired trunks from Available box to Selected box.

In this scenario, select the trunk FXO-5503301.



4. In the Default Destination section, complete the following operations:
- Select the checkbox of Time Condition.
 - In the drop-down list of Time-based Routing Mode, select Based on Global Business Hours.
 - Configure the following destinations based on the time.
 - Business Hours Destination: Select the destination for inbound calls during [global business hours](#).
In this scenario, select IVR, and select the IVR for business hours.
 - Outside Business Hours Destination: Outside Business Hours is the time periods that are not defined as Business Hours or Holidays.
In this scenario, select Extension Voicemail then select an extension number.
 - Holidays Destination: Select the destination for inbound calls during [holidays](#).
In this scenario, select IVR, and select the IVR for holidays.

Default Destination

Time Condition

* Time-based Routing Mode

Based on Global Business Hours

Business Hours Destination *

IVR InBusiness

Outside Business Hours Destination *

Extension Voicemail 1002-Helen

Holidays Destination *

IVR Holidays

5. Click Save and Apply.

Result

When customers make calls to the phone number of the selected trunk (FXO-5503301), the calls will be routed to different destinations based on the time.

Related information

- [Route Inbound Calls based on Department Hours](#)
- [Route Inbound Calls based on Employee Hours](#)
- [Route Inbound Calls based on DID Numbers](#)
- [Route Inbound Calls based on Caller ID](#)
- [Route Inbound Calls by Matched Phonebook Contacts](#)

Route Inbound Calls based on Department Hours

This topic gives a configuration example to describe how to configure inbound route to control inbound calls for the departments that maintain different hours from the company's global business hours.

Scenarios

The employees in the branch office's support department have different business hours from the head office. The department hours is listed as below:

- Working days: Monday to Friday
- Business hours: 21:00 - 23:00 and 00:00 - 05:00

When customers call in the trunk FXO-5503302, you want to route the calls based on the time as follows:

- During business hours, route inbound calls to the support team's queue.
- During a holiday, route inbound calls to another IVR for holiday.
- For other time periods, route inbound calls to a voicemail.

Prerequisites

- The trunk for inbound calling has been set up and is ready for use.
- The desired destination of the inbound route should be configured on the system.

In this scenario, a queue and an IVR for holiday should be preconfigured.

For more information of the configurations of queue and IVR, see [Create a Queue](#) and [Set up an IVR](#).

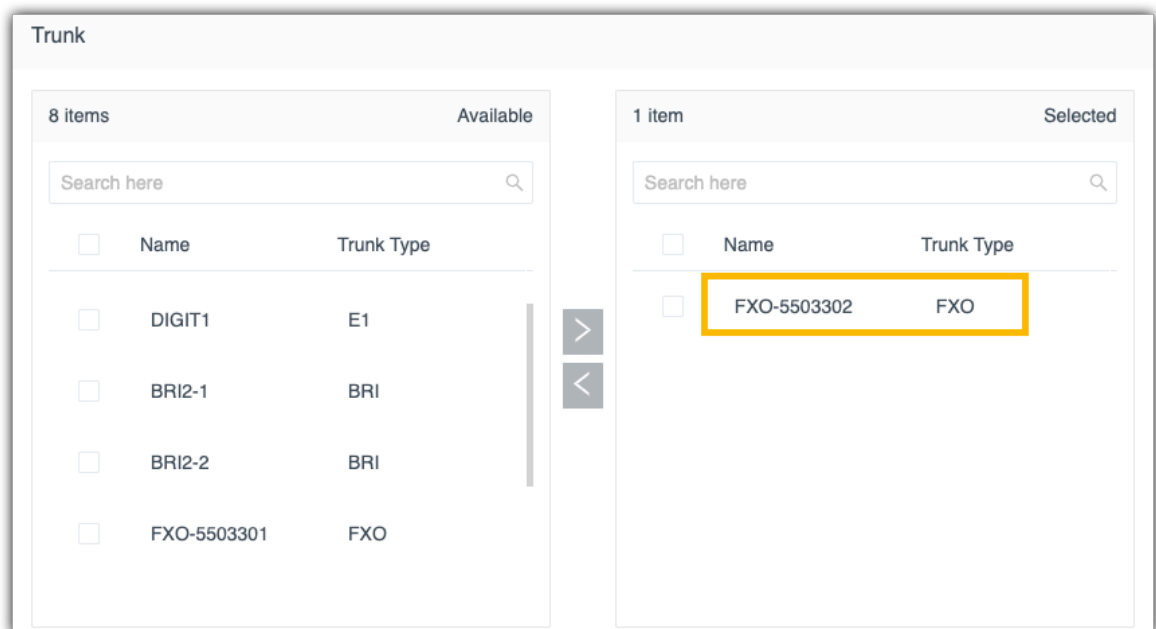
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always be directed to your desired destination.

How to configure inbound route based on DID numbers, see [Route Inbound Calls based on DID Numbers](#).

Procedure

1. Log in to PBX management portal, go to Call Control > Inbound Route, click Add.
2. In the Name field, enter a name to help you identify it.
3. In the Trunk section, select the desired trunks from Available box to Selected box.

In this scenario, select the trunk FXO-5503302.



4. In the Default Destination section, complete the following operations:

- a. Select the checkbox of Time Condition.
- b. In the drop-down list of Time-based Routing Mode, select Based on Custom Business Hours.
- c. Configure custom business hours.
 - i. Click Add Custom Business Hours.
 - ii. In the pop-up window, click Add to add time periods and select days of week.

In this scenario, add two time periods, 21:00 - 23:00 and 00:00 - 05:00; select days from Monday to Friday.

- iii. Click Confirm.
- d. Configure the following destinations based on the time.
 - Business Hours Destination: Select the destination for inbound calls during [global business hours](#).
In this scenario, select Queue, and select the Queue "Support Team".
 - Outside Business Hours Destination: Outside Business Hours is the time periods that are not defined as Business Hours or Holidays.
In this scenario, select Extension Voicemail then select an extension number.
 - Holidays Destination: Select the destination for inbound calls during [holidays](#).
In this scenario, select IVR, and select the IVR for holidays.

Default Destination

Time Condition

* Time-based Routing Mode

Based on Custom Business Hours

+ Add Custom Business Hours Delete

<input type="checkbox"/> Custom Business Hours	Days of Week	Operations
<input type="checkbox"/> 21:00-23:00;00:00-05:00	Monday.Tuesday.Wednesday.Thursday.Friday	✎ ✖

Business Hours Destination *

Queue

6400-Support Team

Outside Business Hours Destination *

Extension Voicemail

1000-Leo Ball

Holidays Destination *

IVR

6201-Holidays

5. Click Save and Apply.

Result

When customers make calls to the phone number of the selected trunk (FXO-5503302), the calls will be routed to different destinations based on time.

Related information

- [Route Inbound Calls based on Global Business Hours](#)
- [Route Inbound Calls based on Employee Hours](#)
- [Route Inbound Calls based on DID Numbers](#)
- [Route Inbound Calls based on Caller ID](#)
- [Route Inbound Calls by Matched Phonebook Contacts](#)

Route Inbound Calls based on Employee Hours

This topic gives a configuration example to describe how to configure inbound route to control inbound calls for individual employees who have their own work schedules.

Scenarios

Duty doctors in a hospital are responsible for supporting emergency patient needs or arranging appointments for patients over phone calls.

- Each duty doctor has a different time schedule and will provide services based on the time schedule.
- During the time periods that no doctors are on duty or when it comes to a holiday, the incoming calls from patients will be routed to an IVR.

The following shows time schedule for the duty doctors.

Doctor Name	Time Schedule
Dr. Tommy Tse	Monday 07:00 -12:00 Friday 12:00 - 18:00
Dr. Eric Chan	Monday 00:00 - 07:00 Thursday 07:00 - 12:00

Prerequisites

- The trunk for inbound calling has been set up and is ready for use.
- The desired destination of the inbound route should be configured on the system.

In this scenario, an IVR should be configured to ensure that patients can reach their desired services.

For more information of IVR, see [Set up an IVR](#).

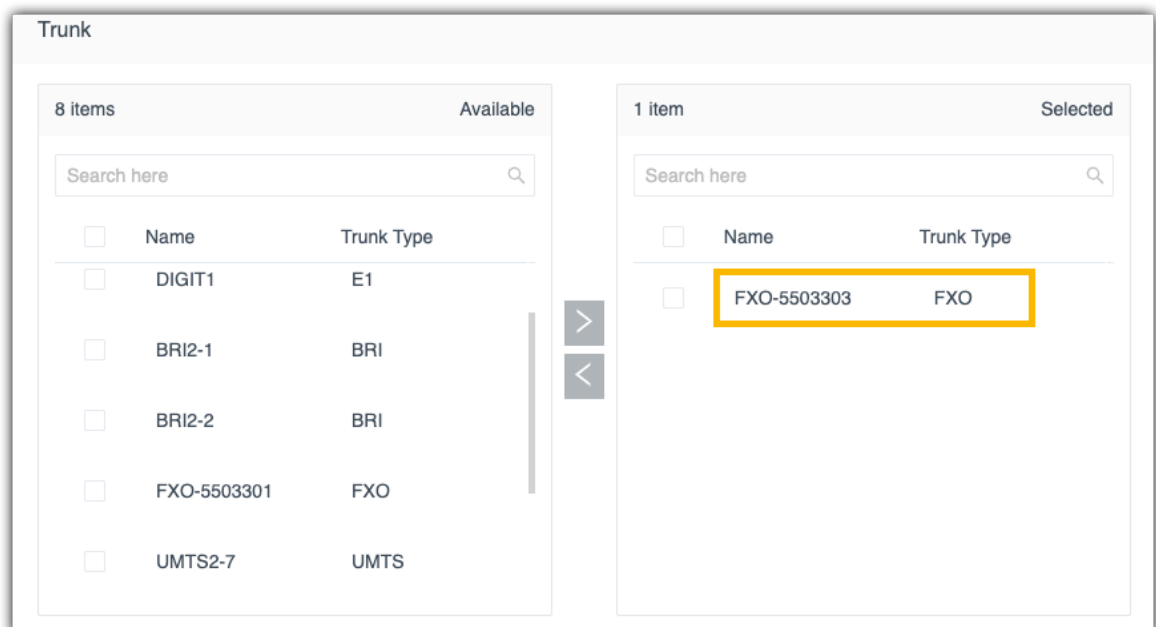
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always be directed to your desired destination.

How to configure inbound route based on DID numbers, see [Route Inbound Calls based on DID Numbers](#).

Procedure

1. Log in to PBX management portal, go to Call Control > Inbound Route, click Add.
2. In the Name field, enter a name to help you identify it.
3. In the Trunk section, select the desired trunks from Available box to Selected box.

In this scenario, select the trunk FXO-5503303.



4. In the Default Destination section, complete the following operations:
 - a. Select the checkbox of Time Condition.
 - b. In the drop-down list of Time-based Routing Mode, select Based on Custom Time Periods.
 - c. Add time schedule for the duty doctors.
 - i. Click Add Custom Time Periods.
 - ii. In the pop-up window, click Add to add time periods, select days of week and set the relevant destination.
 - iii. Click Confirm.
 - iv. Repeat step i - iii to add another time schedule.

In this scenario, add four time schedules as below.

Start Time	End Time	Days of Week	Destination
07:00	12:00	Monday	Tommy's extension
12:00	18:00	Friday	Tommy's extension
00:00	07:00	Monday	Eric's extension
07:00	12:00	Thursday	Eric's extension

d. Configure the Holiday Destination.

In this scenario, select IVR, and select an IVR to guide patients.

e. Configure the Default Destination.

In this scenario, select IVR, and select an IVR to guide patients.

Time Condition

* Time-based Routing Mode

Based on Custom Time Periods ▼

+ Add Custom Time Periods Delete

<input type="checkbox"/>	Custom Time Periods	Days of Week	Destination	Move
<input type="checkbox"/>	07:00-12:00	Monday	Extension	↑ ^ v ↓
<input type="checkbox"/>	12:00-18:00	Friday	Extension	↑ ^ v ↓
<input type="checkbox"/>	00:00-07:00	Monday	Extension	↑ ^ v ↓
<input type="checkbox"/>	07:00-12:00	Thursday	Extension	↑ ^ v ↓

Holidays Destination *

IVR ▼ 24-Hours-Services ▼

Default Destination *

IVR ▼ 24-Hours-Services ▼

5. Click Save and Apply.

Result

When external users make calls to the phone number of the selected trunk (FXO-5503303), the calls will be routed to different destinations based on time:

- During the custom time periods, inbound calls go to the specified destination.
- During the rest of time that is not defined, inbound calls go to the Default Destination.
- When it comes to holiday, inbound calls go to the Holiday Destination.

Related information

- [Route Inbound Calls based on Global Business Hours](#)
- [Route Inbound Calls based on Department Hours](#)
- [Route Inbound Calls based on DID Numbers](#)
- [Route Inbound Calls based on Caller ID](#)
- [Route Inbound Calls by Matched Phonebook Contacts](#)

Route Inbound Calls based on DID Numbers

This topic gives configuration examples to describe how to route inbound calls based on the dialed numbers (also called DID numbers).

DID routing modes

Yeastar P-Series PBX System provides three DID matching modes to help you route inbound calls based on DID numbers.

- Match DID Range to Extension Range

Match DID Range and Extension Range in one-to-one correspondence.

See configuration example [Route calls to extension users by matching DID range](#).

- Match DID Pattern to Extensions

Use the variable `{{.Ext}}` to match extension number in the DID pattern.

See configuration example [Route calls to extension users by matching specific DIDs](#).

- DID Pattern

The calls match the defined DID(s) will be routed to a defined destination.

See configuration example [Route calls to a specific destination by matching DID patterns](#).

Route calls to extension users by matching DID range

Background information

Company ABC purchases a SIP trunk, and gets 10 DID numbers that are in order: 8823201-8823210.

The company wants to redirect inbound calls to specific extensions based on the provided DID numbers as follows:

Table 25.

DID Number	Extension Number
8823201	1001

Table 25. (continued)

DID Number	Extension Number
8823202	1002
8823203	1003
8823204	1004
8823205	1005
8823206	1006
8823207	1007
8823208	1008
8823209	1009
8823210	1010

Prerequisites

- You have purchased DID numbers from the trunk provider.
- The trunk for inbound calling has been set up and is ready for use.



Note:

PSTN trunk and GSM trunk have no DID numbers, this solution is not suitable for these kinds of trunks.

Configuration example

According to this scenario, configure an inbound route based on DIDs as follows:

- Name: Enter a name to help you identify it.
- DID Pattern:
 - DID Matching Mode: Select Match DID Range to Extension Range.
 - DID Range: Enter the start number and the end number of the DID range.

In this scenario, enter 8823201 and 8823210.

DID Pattern

• DID Matching Mode:


• DID Range: -

- Caller ID Pattern: Leave it blank, which means no limit on the inbound caller ID.
- Trunk: Select the trunk that binds the DID numbers.

- **Default Destination:** Decide whether to route inbound calls to different destinations based on time and configure the destinations.

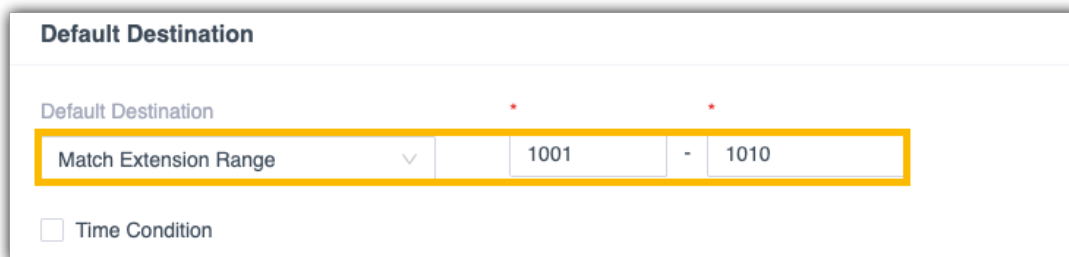
In this scenario, route inbound calls to the default destination whenever the calls reach the system.

- **Default Destination:** Select Match Extension Range, and enter the extension range 1001 - 1010.

 **Note:**

The DID range and extension range should have the same size (for example, DID range 991000-991003 and the extension range 1000-1003 have the same size).

- **Time Condition:** Unselected.



Default Destination

Default Destination

Match Extension Range ▼ 1001 - 1010

Time Condition

- **Fax Detection:** Leave the settings as default.

Result

When an external user dials a number that is in the DID range, the user can reach a corresponding extension user directly.

For example, if an external user dials 8823201, the call goes to the extension 1001 directly.


Route calls to extension users by matching specific DIDs

Scenarios

Company ABC purchases a SIP trunk, and gets 3 DID numbers as follows.

- 8821001, 8821006, 8821016

The company wants to redirect inbound calls to specific extensions based on the provided DID numbers as follows:

 **Note:**

The provided DIDs have the following characteristics:

- Not consecutive

- Each DID number consists of a string of fixed digits and a specific extension number.

Table 26.

DID Number	Extension Number
8821001	1001
8821006	1006
8821016	1016

Prerequisites

- You have purchased DID numbers from the trunk provider.
- The trunk for inbound calling has been set up and is ready for use.



Note:

PSTN trunk and GSM trunk have no DID numbers, this solution is not suitable for these kinds of trunks.

Configuration example

According to this scenario, configure an inbound route based on DIDs as follows:

- Name: Enter a name to help you identify it.
- DID Pattern:
 - DID Matching Mode: Select Match DID Pattern to Extensions.
 - DID Pattern: Enter the DID pattern according to the provided DIDs.

In this scenario, enter `882{{.Ext}}`.



Note:

- `{{.Ext}}` is a variable that will match the destination extension.
- The wildcard `.` and `!` are not allowed.
- Only one DID pattern is allowed.

DID Pattern

* DID Matching Mode * DID Pattern

Match DID Pattern to Extensions 882{{.Ext}}

- Caller ID Pattern: Leave it blank, which means no limit of inbound caller ID.
- Trunk: Select the trunk that binds the DID numbers.

In this scenario, select siptrunk.

- **Default Destination:** Decide whether to route inbound calls to different destinations based on time and configure the destinations.

In this scenario, route inbound calls to the default destination whenever the calls reach the system.

- **Default Destination:** Select Match Selected Extensions, and select extensions. In this scenario, select extension 1001, 1006, and 1016.
- **Time Condition:** Unselected.

Default Destination

Default Destination

Match Selected Extensions

1001-Becky Lai × 1016-Jenny ×

1006-Candy ×

Time Condition

- **Fax Detection:** Leave the settings as default.

Result

When an external user dials a number that matches the DID pattern, the user can reach a specific extension user directly.

For example, if the external user dials 8821001, the call goes to the extension 1001 directly.

Route calls to a specific destination by matching DID patterns

Scenario

Company ABC purchases a SIP trunk, and gets 2 DID numbers as follows.

- 88866608
- 88866609

The company wants to assign the two DID numbers to support team and sales team.

- When external users call 88866609, the calls go directly to support team.
- When external users call 88866608, the calls go directly to sales team.

Prerequisites

- You have purchased DID numbers from the trunk provider.
- The trunk for inbound calling has been set up and is ready for use.

**Note:**

PSTN trunk and GSM trunk have no DID numbers, this solution is not suitable for these kinds of trunks.

Configuration example

Set up two inbound routes to route calls to different destinations based on DID numbers.

Inbound Route for sales team

- Name: Enter a name to help you identify it.
- DID Pattern:
 - DID Matching Mode: Select DID Pattern.
 - DID Patterns: Click Add and enter a DID pattern or a DID number.

In this scenario, enter 88866608.

Pattern	Operations
88866608	

- Caller ID Pattern: Leave it blank, which means no limit of inbound caller ID.
- Trunk: Select the trunk that binds the DID numbers.
- Default Destination: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

In this example, route inbound calls to the default destination whenever the calls reach the system.

- Default Destination: Select the destination to the queue of sales team.
- Time Condition: Unselected.

Default Destination: Queue | 6404-Sales

Time Condition

- Fax Detection: Leave the settings as default.

Inbound Route for support team

- Name: Enter a name to help you identify it.
- DID Pattern:
 - DID Matching Mode: Select DID Pattern.
 - DID Patterns: Click Add and enter a DID pattern or a DID number.

In this scenario, enter 88866609.

DID Pattern

* DID Matching Mode

DID Pattern

Pattern	Operations
88866609	⊗

- Caller ID Pattern: Leave it blank, which means no limit of inbound caller ID.
- Trunk: Select the trunk that binds the DID numbers.
- Default Destination: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

In this example, route inbound calls to the default destination whenever the calls reach the system.

- Default Destination: Select the destination to the queue of support team.
- Time Condition: Unselected.

Default Destination

Default Destination

Queue | 6405-Support

Time Condition

- Fax Detection: Leave the settings as default.

Result

External users will reach different teams according to the DID numbers they dial.

Related information

- [Route Inbound Calls based on Global Business Hours](#)
- [Route Inbound Calls based on Department Hours](#)
- [Route Inbound Calls based on Employee Hours](#)
- [Route Inbound Calls based on Caller ID](#)
- [Route Inbound Calls by Matched Phonebook Contacts](#)

Route Inbound Calls based on Caller ID

Caller ID routing connects external callers with the appropriate party quickly. This topic gives a configuration example to describe how to route calls by [a caller-ID-based inbound route](#).

Scenarios

Company ABC is a Chinese company that provides consulting services around multiple cities.

For better customer experience, the company has a countrywide toll-free number 400-661-8815 and has multiple teams to provide professional services for customers from different regions.

For example, the following two teams will handle inbound calls based on different caller IDs.

Table 27.

Team	Responsible Region	Area Code
Team-A	Fujian	<ul style="list-style-type: none"> • 0591 • 0592 • 0593 • 0594 • 0595 • 0596 • 0597 • 0598 • 0599
Team-B	Guangdong	<ul style="list-style-type: none"> • 0662 • 0663 • 0668 • 0660

Configuration Example

Set up two inbound routes to route calls to different destinations based on caller IDs.

Inbound Route for Team-A

- Name: Enter a name to help you identify it.
- DID Pattern: Leave it blank, which means no limit of DID numbers.
- Caller ID Pattern: Select Caller ID Matching Settings, click Add and enter a Caller ID pattern or a full Caller ID.

In this scenario, enter 059., which matches all inbound caller IDs that start with digit 059. For more information of Caller ID pattern, see [DID Pattern and Caller ID Pattern](#).

- Trunk: Select the trunk that users will call in.
- Default Destination: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

In this example, route inbound calls to the default destination whenever the calls reach the system.

- Default Destination: Select the destination to the queue of Team-A.
- Time Condition: Unselected.

- Fax Detection: Leave the settings as default.

Inbound Route for Team-B

- Name: Enter a name to help you identify it.
- DID Pattern: Leave it blank, which means no limit of DID numbers.
- Caller ID Pattern: Select Caller ID Matching Settings, click Add and enter a Caller ID pattern or a full Caller ID.

In this scenario, enter 066., which matches all inbound Caller IDs that start with digit 066. For more information of Caller ID pattern, see [DID Pattern and Caller ID Pattern](#).

Caller ID Pattern

* Caller ID Pattern

Caller ID Matching Settings

Pattern	Operations
066.	

- **Trunk:** Select the trunk that users will call in.

In this example, select siptrunk, whose phone number is 400-661-8815.

- **Default Destination:** Decide whether to route inbound calls to different destinations based on time and configure the destinations.

In this example, route inbound calls to the default destination whenever the calls reach the system.

- **Default Destination:** Select the destination to the queue of Team-B.
- **Time Condition:** Unselected.

Default Destination

Default Destination

Queue

6403-Team-B

Time Condition

- **Fax Detection:** Leave the settings as default.

Result

- When users from Fujian dial the number 400-661-8815, agents in Team-A will handle the calls.
- When users from Guangdong dial the number 400-661-8815, agents in Team-B will handle the calls.

Related information

- [Route Inbound Calls based on Global Business Hours](#)
- [Route Inbound Calls based on Department Hours](#)
- [Route Inbound Calls based on Employee Hours](#)
- [Route Inbound Calls based on DID Numbers](#)
- [Route Inbound Calls by Matched Phonebook Contacts](#)

Route Inbound Calls by Matched Phonebook Contacts

After grouping company contacts into phonebooks, you can set up inbound routes to distribute inbound calls from contacts to different destinations based on phonebooks.

Prerequisites

- You have subscribed Enterprise Plan or Ultimate Plan.
- You have added phonebooks and enabled Caller ID Match feature.

For more information, see [Manage Company Phonebooks](#) and [Identify Callers from Contacts](#).

Scenario

Company ABC has a Sales Team and a Support Team, both teams have their own customer groups. System administrator has added the customer information into two phonebooks.

Table 28.

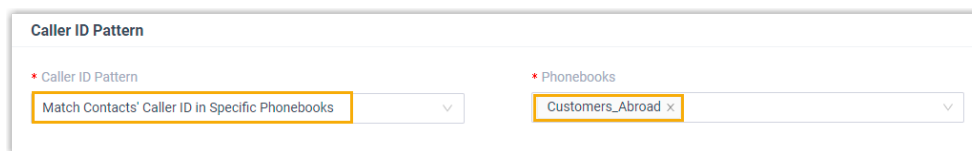
Team	Phonebook
Sales Team (Queue 6401)	Customers_Abroad
Support Team (Queue 6402)	Customers_China

Configuration Example

To distribute inbound calls from customers to corresponding team, you can set up two inbound routes to route calls by matching contacts in different phonebooks.

Inbound Route for Sales Team

- **Name:** Enter a name to help you identify it.
- **DID Pattern:** Leave it blank, which means no limit of DID numbers.
- **Caller ID Pattern:** Select Match Contacts' Caller ID in Specific Phonebooks and select the phonebook Customers_Abroad.



The screenshot shows a configuration window titled "Caller ID Pattern". It contains two dropdown menus. The first dropdown, labeled "Caller ID Pattern", is set to "Match Contacts' Caller ID in Specific Phonebooks". The second dropdown, labeled "Phonebooks", is set to "Customers_Abroad".

- **Trunk:** Select the trunk that contacts will call in.
- **Default Destination:** Decide whether to route inbound calls to different destinations based on time and configure the destinations.

In this example, route inbound calls to the default destination whenever the calls reach the system.

- **Default Destination:** Select the destination to Queue and select the Sales Team.
- **Time Condition:** Unselected.

Default Destination

Default Destination: Queue

Phonebooks: 6401-Sales Team

Time Condition

- Fax Detection: Leave the settings as default.

Inbound Route for Support Team

- Name: Enter a name to help you identify it.
- DID Pattern: Leave it blank, which means no limit of DID numbers.
- Caller ID Pattern: Select Match Contacts' Caller ID in Specific Phonebooks and select the phonebook Customers_China.

Caller ID Pattern

Caller ID Pattern: Match Contacts' Caller ID in Specific Phonebooks

Phonebooks: Customers_China

- Trunk: Select the trunk that contacts will call in.
- Default Destination: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

In this example, route inbound calls to the default destination whenever the calls reach the system.

- Default Destination: Select the destination to Queue and select Support Team.
- Time Condition: Unselected.

Default Destination

Default Destination: Queue

Phonebooks: 6402-Support Team

Time Condition

- Fax Detection: Leave the settings as default.

Result

- When customers from Phonebook 'Customers_Abroad' call to PBX, Sales Team will handle the calls.
- When customers from Phonebook 'Customers_China' call to PBX, Support Team will handle the calls.

Related information

- [Route Inbound Calls based on Caller ID](#)
- [Route Inbound Calls based on DID Numbers](#)





- [Route Inbound Calls based on Employee Hours](#)
- [Route Inbound Calls based on Department Hours](#)
- [Route Inbound Calls based on Global Business Hours](#)

Manage Inbound Routes


After you create inbound routes, you can adjust the priority of the inbound routes. You can also edit or delete the inbound routes.

Adjust priority of inbound routes


A trunk can be selected to multiple inbound routes. When users call to a trunk that is selected in multiple inbound routes, the system will route inbound calls through the route with higher priority. You can adjust the priority of inbound routes according to your needs.

1. Log in to PBX management portal, go to Call Control > Inbound Route.
2. In the Inbound Route list, click     to adjust the priority of your inbound routes.

Edit an inbound route

1. Log in to PBX management portal, go to Call Control > Inbound Route.
2. Click  beside the inbound route that you want to edit.
3. Edit the inbound route.
4. Click Save and Apply.

Delete an inbound route

1. Log in to PBX management portal, go to Call Control > Inbound Route.
2. Click  beside the inbound route that you want to delete.
3. On the pop-up window, click Yes to confirm.
4. Click Apply.

Export and Import Inbound Routes

The inbound routes configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired inbound routes in the exported file, and import the file to PBX again. This topic describes how to export and import inbound routes.

Export inbound routes

You can export all inbound routes to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Extension and Trunk > Call Control > Inbound Route.
2. Click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see [Inbound Route Parameters](#).

Import inbound routes

We recommend that you export inbound route data to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 50 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information , see [Inbound Route Parameters](#).

Procedures

1. Log in to PBX management portal, go to Extension and Trunk > Call Control > Inbound Route.
2. Click Import.
3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The inbound routes in the CSV file will be displayed in the Inbound Route list.

DID Pattern and Caller ID Pattern


This topic describes special characters that can be defined in a DID pattern or a Caller ID pattern, and provides examples to help you understand and configure the pattern.

Pattern

A Pattern field appears when you are configuring DID numbers or Caller IDs. The Pattern field allows you to enter a full number or special characters that will match specific numbers.

The following table shows descriptions of the allowed characters in the Pattern field.

Table 29.

Pattern	Description
x	Match any digit from 0 -9.
z	Match any digit from 1- 9.
N	Match any digit from 2 - 9.
[###]	Match any digit in the bracket. Example: [123] matches the numbers 1, 2, or 3. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Range of numbers can be specified with a dash, example [136-8] matches the numbers 1, 3, 6, 7, or 8.</p> </div>
.	Match one or more numbers. Example: 9011. matches any numbers starting with digits 9011 (excluding 9011 itself).
!	Match none or more than one characters. Example: 9011! matches any numbers starting with 9011 (including 9011 itself).

Pattern examples

The following table gives several patterns and list examples of matched numbers and mismatched numbers.

Table 30.

Pattern	Matched Number	Mismatched Number
0591.	<ul style="list-style-type: none"> • 05910 • 0591012345 	<ul style="list-style-type: none"> • 0591 • 0592229929
+ [13-5]XZN!	<ul style="list-style-type: none"> • +4021 • +1136282882 	<ul style="list-style-type: none"> • +0136282882 • +1106282882
0591ZXXXX	<ul style="list-style-type: none"> • 059123456 • 059133456 	<ul style="list-style-type: none"> • 05912345 • 059103456

Outbound Route

Outbound Route Overview

An outbound route tells the Yeastar P-Series PBX System how to handle outbound calls based on pre-configured rules and criteria. When a user makes an outbound call, the system analyses the user's extension number and the dialed number, then routes the call through a matched outbound route.

Outbound Route matching criteria

Yeastar P-Series PBX System provides the following criteria for you to configure outbound routes.

Dial Pattern

A dial pattern matches the dialed number and reformats the dialed number before sending the number out to the carrier.

For more information of dial patterns, see [Outbound Dial Pattern](#).

Outbound Route Password

Users need to enter the PIN number before they can make calls through the outbound route.

Time Condition

A Time Condition defines when the outbound route is available.

Outbound Route priority

When a user makes an outbound call, the system compares the dialed number with the dial patterns in each outbound route (from highest to lowest priority) until a match is found.

- If the first outbound route is matched, the system will place the call through the outbound route.
- If the first outbound route is not matched, the system will check the second outbound route, and so on.

For more information, see [Adjust priority of outbound routes](#).

Set up an Outbound Route

To allow users to make outbound calls through trunks, you need to set up at least one outbound route on the Yeastar P-Series PBX System.

Background information

Yeastar P-Series PBX System has a default outbound route with dial pattern `x.` that allows users to dial any outgoing numbers. You can delete the default outbound route, then add a new one to configure settings according to your needs.

Prerequisites

Ensure that you have set up at least one trunk for outbound calls.

Procedure

1. Log in to PBX management portal, go to Call Control > Outbound Route, click Add.
2. In the General section, complete the following configurations:
 - Name: Enter a name to help you identify it.
 - Outbound Caller ID: Optional. By default, each trunk is associated with a main caller ID. When users make outbound calls through a trunk, the main caller ID is displayed on the called party's device. If this option is configured, the system will override the main caller ID with the Outbound Caller ID.





For more information of caller ID, see [Caller ID Overview](#).

Note:

Only configure this setting when the trunk provider supports Caller ID override, or the following errors may happen:

- Outbound calls failed to be established.
- Caller ID doesn't be overridden.

3. In the Dial Pattern section, configure dial rules for the outbound route.
 - a. Click Add.
 - b. Configure the dial pattern to match dialed numbers and reformat dialed numbers.
 - Pattern: Enter a pattern to match dialed numbers. Only when the dialed number is matched will the call go through this outbound route.
 - Strip: Optional. To strip digits from the beginning of the dialed numbers, enter a value in this field to define how many digits will be removed.
 - Prepend: Optional. To add digits at the beginning of the dialed number, enter the digits that you want to prepend in this field.
 - c. To add more dial patterns, repeat step a-b.
4. In the Trunk section, configure the followings:
 - a. Select one or more trunks from the Available box to Selected box.
 - b. Optional: If multiple trunks are selected, configure the trunk sequence.
 - Default trunk sequence

Click the buttons     beside the Selected box to specify the default trunk sequence. By default, the system always selects an idle trunk from top to bottom, and uses the trunk to call out.
 - Rrmemory Hunt

If the option Rrmemory Hunt is selected, the system will remember which trunk was used last time, and use the next idle trunk to call out.

- c. To enhance the outbound route security, configure the Outbound Route Password.
 - Disable: No password is required to call out through this outbound route.
 - Single PIN: Set a single PIN. All the users need to enter the same PIN to make outbound calls through this outbound route.
 - PIN List: Select a PIN list. Users are required to dial a password included in this list before an outbound call go through.



Note:

Generally, each user has a specific PIN code assigned by the administrator. For more information, see [Add a PIN List](#).

5. Select which users are allowed to make calls through this outbound route.

In the Extension/Extension Group section, select extensions or extension groups from Available box to Selected box.

6. Optional: In the Time Condition section, select an option from Available Time drop-down list to specify when this outbound route is available to use.
 - Always: This outbound route is available at any time for allowed extension users.
 - Based on Global Business Hours: Set up whether to allow this route in the following time separately:
 - Business Hours: [Global Business Hours](#) specified in the system.
 - Holidays: [Holidays](#) specified in the system.
 - Outside Business Hours: The time periods that are not defined as Business Hours or Holidays.
 - Based on Custom Business Hours: Set up custom business hours and configure whether to allow this route in the following time:
 - Business Hours: The custom business hours.
 - Holidays: [Holidays](#) specified in the system.
 - Outside Business Hours: The time periods that are not defined as Business Hours or Holidays.
 - Based on Custom Time Periods: Set up multiple time periods for this route. You can also specify whether to allow this route in the [Holidays](#).

7. Click Save and Apply.

What to do next

After you finish the outbound route configurations, you need to check and adjust the priority of your outbound routes, so that the system can match and route the call out through the proper outbound route.

For more information, see [Adjust priority of outbound routes](#).


Restrict Outbound Calls by PIN Codes

Many companies restrict the outbound calls by using PIN codes. You can set multiple PIN codes, and assign these PIN codes to different users. Users are required to dial a specified PIN code to make an outbound call via the restricted outbound route. In this way, you can easily track the calls made by different users.

Prerequisites

You need to add a PIN list or several PIN lists. For more information, see [Add a PIN List](#).

Procedure

1. Log in to PBX management portal, go to Call Control > Outbound Route.
2. Click  beside the desired outbound route.
3. On the outbound route configuration page, go to Trunk section, and in the Outbound Route Password drop-down list, select PIN List.
4. In the PIN List drop-down list, select the desired PIN list.
5. Click Save and Apply.

Result

- To make an outbound call via the restricted outbound route, users need to enter a correct PIN code included in the selected PIN list.
- When users enter wrong PIN codes for three times, the call will be hung up automatically.
- If the Record in CDR option of PIN list is enabled, the Call Detailed Record (CDR) will display the PIN code of each call.

Manage Outbound Routes

After you create outbound routes, you can adjust the priority of the outbound routes. You can also edit or delete the outbound routes.

Adjust priority of outbound routes

When a user places a call, if the dialed number matches multiple dial patterns, the outbound route with the highest priority will be used. You can adjust the priority of outbound routes to route calls through proper outbound routes.

Note:





The route priority is important, especially if there is some overlap. For example, the number 5503305 matches both dial patterns of `zxxxxxx` and `x.`, the PBX will send the call through the outbound route with the highest priority.

Example:

When users dial 05503301, both of the two outbound routes match 05503301:

- Outbound Route-Long-distance call: The dial pattern is 0xxxxxxx and uses trunk 1.
- Outbound Route-Local call: The dial pattern is x. and uses trunk 2.

To call 5503301 through trunk 1, you need to prioritize the outbound route of "Long-distance call"; or PBX will match the outbound route of "Local call" and route the call out using trunk 2.


1. Log in to PBX management portal, go to Call Control > Outbound Route.
2. Click the buttons     to adjust the priority of your outbound routes.




Note:

PBX will match outbound route from top to bottom.

Edit an outbound route

1. Log in to PBX management portal, go to Call Control > Outbound Route.
2. Click  beside the inbound route that you want to edit.
3. On the outbound route configuration page, edit the outbound route.
4. Click Save and Apply.

Delete an outbound route

1. Log in to PBX management portal, go to Call Control > Outbound Route.
2. Click  beside the outbound route that you want to delete.
3. On the pop-up dialog box, click Yes to confirm.
4. Click Apply.

Export and Import Outbound Routes

The outbound routes configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired outbound routes in the exported file, and import the file to PBX again. This topic describes how to export and import outbound routes.

Export outbound routes

You can export all outbound routes to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Extension and Trunk > Call Control > Outbound Route.

2. Click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see [Outbound Route Parameters](#).

Import outbound routes

We recommend that you export outbound route data to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 50 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information , see [Outbound Route Parameters](#).

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Call Control > Outbound Route.
2. Click Import.
3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The outbound routes in the CSV file will be displayed in the Outbound Route list.

Outbound Dial Pattern

This topic describes dial pattern settings of Outbound Route.

Dial Pattern components


A dial pattern comprises Pattern, Strip, and Prepend.

Pattern

Required.

Defines which dialed numbers will be matched.

The Pattern field allows a full number or special characters that will match specific numbers. The following table shows descriptions of the allowed characters in the Pattern field.

Pattern	Description
x	Match any digit from 0 -9.
z	Match any digit from 1- 9.
N	Match any digit from 2 - 9.
[###]	<p>Match any digit in the bracket.</p> <p>Example: [123] matches the numbers 1, 2, or 3.</p> <div style="border: 1px solid #00a0c0; padding: 5px; margin-top: 10px;"> <p> Note: Range of numbers can be specified with a dash, example [136-8] matches the numbers 1, 3, 6, 7, or 8.</p> </div>
.	<p>Match one or more numbers.</p> <p>Example: 9011. matches any numbers starting with digits 9011 (excluding 9011 itself).</p>
!	<p>Wildcard ! has different meanings for SIP extensions and FXS extensions.</p> <ul style="list-style-type: none"> • If the call is made by a SIP extension, ! matches one or more characters. Example: 9011! matches any numbers starting with 9011 (including 9011 itself). • If the call is made by an FXS extension, ! limits the digit and number that users dial. Example: 9011! only matches the dial number 9011.

Strip


Optional.

Defines how many digits will be stripped from the beginning of a dialed number when the dialed number successfully matches a Pattern.

Example:

If you set Pattern as 9. and set Strip as 1.

If a user wants to call number 1588902923, the user should dial 91588902923. The PBX will strip digit 9 from the dialed number, and call the number 1588902923.

 **Note:**

- The system strips leading digits before sending the number to the carrier.
- If both Strip and Prepend are configured, the system first strips leading digits from the dialed number then prepends digits to the dialed number.

Prepend


Optional.

Defines which digits will be added at the beginning of a dialed number when the dialed number successfully matches a Pattern.

Example:

202 is the area code for Washington, D.C. For users who often make calls to the city, you can set Prepend as 202.

In this case, if a user wants to call number 2025553097, the user should dial 5553097.

 Note:

- The system prepends the digits before sending the number to the carrier.
- If both Strip and Prepend are configured, the system first strips leading digits from the dialed number then prepends digits to the dialed number.

Prefix and Dial Pattern

A prefix is the digit that will be removed from the dialed number before sending to the carrier.

Scenarios

Prefix setting appears when you are configuring the following settings:

- Mobile phone number for notification contacts.

- External number for IVR keypress.

How to configure Prefix

You need to configure prefix according to the dial pattern settings on your outbound route. If the prefix is not configured correctly, the PBX cannot call to the external number successfully.

- Leave Prefix setting blank

If the Strip of outbound route is not set, you don't have to add a prefix before the phone number.

As the following figure shows, only the destination number that starts with digit 1 can be called out through this outbound route.

For example, to call number 125451, you should dial the number 125451 directly.

Pattern	Strip	Prepend
1.		

- Add prefix before a number

If Strip is set on an outbound route, you need to set the prefix according to the Pattern.

As the following figure shows, to make calls through the outbound route, you need to add prefix 9 before the number, and the destination number should start with digit 1.

For example, to call number 125451, you should add prefix 9 before the number 125451.

Pattern	Strip	Prepend
91.	1	

Dial Pattern Examples

This topic provides sample dial patterns to help you understand dial patterns of outbound route.

Local calls

In Xiamen, China, local numbers are all 7-digit numbers and the numbers do not start with 0, such as 5503305.

For the local calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
ZXXXXXX	Leave it blank.	Leave it blank.

Long distance calls

In Xiamen, China, users need to dial 4-digit area code and 7-digit local number to make a long distance call, such as 0595-7588123.

- Area code format: 0ZXX, the first digit is 0, and the second digit cannot be 0.
- Local number format: 7-digit number that does not start with 0.

For long distance calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
0ZXXZXXXXXX	Leave it blank.	Leave it blank.

Mobile calls

All mobile phone numbers in China are 11-digit numbers and start with digit 1, such as 15880260666.

For mobile calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
1XXXXXXXXXX	Leave it blank.	Leave it blank.

International calls

All international numbers start with digits 00.

For international calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
00.	Leave it blank.	Leave it blank.

DID Number

DID Number Overview

This topic describes what is DID number and DID usages on Yeastar P-Series PBX System.

What is a DID number?

Direct Inward Dialling (DID), also called Direct Dial-in (DDI), is a service offered by telephone companies. A telephone company usually assigns a range of numbers to a trunk. There is an extra charge for the DID numbers, you need to contact the trunk provider to purchase DID numbers. The following types of trunks support DID numbers:

- SIP
- BRI
- E1/T1/J1

Note:

FXO trunk and GSM/UMTS/LTE trunk have no DID numbers.

DID usages

Yeastar P-Series PBX System allows you to configure DID numbers on an inbound route or a trunk to achieve different functions.

DID configuration on an inbound route

- A company can use DID numbers to identify incoming calls of different purposes, such as incoming calls for customer service, sales, etc.

- DID numbers can also be assigned to individual employees. In this way, callers can dial directly into extension users on the Yeastar P-Series PBX System.

For more information, see [Route Inbound Calls based on DID Numbers](#).

DID configuration on a trunk

- For SIP Register Trunk

For a SIP Register Trunk, if ITSP provides DID numbers that are different from SIP authentication name, you need to add the provided DID numbers on the trunk, or inbound calls through this trunk would fail.

- Identify inbound calls

To identify which DID number is dialed, you can bind each DID number with a DID name.

For more information, see [Configure DID Numbers on a Trunk](#).

Configure DID Numbers on a Trunk

This topic describes when and how to configure DID numbers on a trunk.

Background information

DID numbers are usually configured on inbound routes to distinguish inbound calls. For more information, see [Route Inbound Calls based on DID Numbers](#).

In the following scenarios, you need to configure DID numbers on a trunk:

- For SIP Register Trunk

For a SIP Register Trunk, if ITSP provides DID numbers that are different from SIP authentication name, you need to add the provided DID numbers on the trunk, or inbound calls through this trunk would fail.

- Identify inbound calls

To identify which DID number is dialed, you can bind each DID number with a DID name.

Prerequisites

Purchase DID numbers from the trunk provider.

Note:


DID number is only supported on SIP trunk, BRI trunk, and E1/T1/J1 trunk.

Add a DID number

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit the desired trunk.
2. Click DID/DDIs tab.
3. In the pop-up window, click Add and configure the DID.
 - DID/DDI: Enter the provided DID number.
 - DID/DDI Name: Bind a name with the DID number.

When the DID number is dialed, the name will be displayed on the called party's device.
4. Click Save and Apply.

Delete DID numbers

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit the desired trunk.
2. Click DID/DDIs tab.
3. On the DID/DDIs page, click  to delete a DID number.
4. To bulk delete DID numbers, select the checkboxes of DID numbers, click Delete.
5. Click Save.

Export and Import Trunk DID/DDI Numbers

Trunk DID/DDI numbers configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired DID/DDI numbers in the exported file, and import the file to PBX again. This topic describes how to export and import DID/DDI numbers.

Background information

The following types of trunks support DID/DDI numbers:

- SIP
- BRI
- E1/T1/J1

Note:

FXO trunk and GSM/3G/4G LTE trunk have no DID numbers.

Export all DID/DDI numbers

You can export all DID/DDI numbers to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit a desired trunk.
2. In the DIDs/DDIs tab, click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see [Trunk DIDs/DDIs Parameters](#).

Import DIDs/DDIs numbers

We recommend that you export DIDs/DDIs numbers to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 5 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information , see [Trunk DIDs/DDIs Parameters](#).

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit a desired trunk.
2. In the DIDs/DDIs tab, click Import.
3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The DIDs/DDIs numbers in the CSV file will be displayed in the DIDs/DDIs list.

Caller ID

Caller ID Overview

This topic describes what is caller ID, differences between all the types of caller ID defined in Yeastar P-Series PBX System.

What is Caller ID?

Caller ID is a telephone service that transmits a caller's telephone number and name to the called party's device when a call is established.

Caller ID types

Yeastar P-Series PBX System supports the following types of Caller ID:

Outbound caller ID

Outbound caller ID is the phone number that will be displayed on the called party's phone when an extension user makes an outbound call. Each trunk has a main number, the number appears when an outbound call is received by a recipient.

To customize the outbound caller ID, you need to purchase the service from the trunk provider, and set the custom outbound caller ID on the PBX. In Yeastar P-Series PBX System, you can configure outbound caller ID based on the following features:

- Emergency Numbers
- Outbound Route
- Trunk
- Extension

For more information, see [Customize Outbound Caller IDs](#).

Inbound caller ID

Inbound caller ID is an external user's phone number that will be displayed on an extension user's phone when the external user calls in Yeastar P-Series PBX System.

Inbound Caller IDs can be reformatted before they are sent to the destination users. For more information, see [Reformat Inbound Caller ID based on a Trunk](#).

Priority of outbound caller ID

When an extension user makes an outbound call, the system first identifies if the call is an emergency call, then sends an outbound caller ID by the following priority (from the highest to the lowest).

1. Extensions' emergency outbound caller ID
2. Trunk's emergency outbound caller ID
3. Outbound Route caller ID
4. Trunk's outbound caller IDs that are associated with extension users
5. Trunk's general outbound caller ID
6. Trunk's default phone number that is provided by the carrier
7. Extension's caller ID

Reformat Inbound Caller ID based on a Trunk

This topic describes how to reformat inbound caller ID and gives configuration examples to help you understand the reformatting rule.

Background information

If an inbound caller ID is in the format that is inconvenient for users to redial directly, you can reformat the inbound caller ID.

Reformatting inbound caller ID is supported on all types of trunk. Based on different trunk providers, you may need to set up different rules to reformat inbound caller IDs.

Add a rule to reformat inbound Caller ID

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit the desired trunk.
2. Click Inbound Caller ID Reformatting tab.
3. On the Inbound Caller ID Reformatting page, click Add.
4. In the pop-up window, configure the reformatting rule and click Confirm.
 - Patterns: Specify which Caller IDs will be reformatted. The inbound caller ID that matches this pattern will be reformatted.
 - Strip: Specify how many digits will be stripped from the beginning of the inbound caller ID.
 - Prepend: Specify the digits that will be prepended to the inbound caller ID.



Note:

If both Strip and Prepend are configured, the system will first strip the leading digits then add the prepend digits to the inbound caller ID.

5. Click Save and Apply.

Example 1

Company A wants to add a digit 0 to the 11-digit inbound caller ID number that begins with digit 1 for quick redial purpose.

For example, company A wants to display 012345678910 instead of 12345678910.

In this case, you can configure the reformatting rule as below:

* Patterns

1XXXXXXXXXX

Strip

Prepend

0

- Patterns: 1XXXXXXXXXX
- Strip: Leave it blank.
- Prepend: 0

Example 2

Company B wants all local numbers to be displayed without area code (0592).

For example, company B wants to display number 5503301 instead of 05925503301.

In this case, you can configure the reformatting rule as below:

* Patterns

0592XXXXXXXX

Strip

4

Prepend

- Patterns: 0592XXXXXXXX
- Strip: 4
- Prepend: Leave it blank.

Export and Import Inbound Caller ID Reformatting Rules

The inbound caller ID reformatting rules configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired inbound caller ID reformatting rules in the exported file, and import the file to PBX again. This topic describes how to export and import inbound caller ID reformatting rules.

Export all inbound caller ID reformatting rules

You can export all inbound caller ID reformatting rules to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit a desired trunk.
2. In the Inbound Caller ID Reformatting tab, click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see ['Inbound Caller ID Reformatting Rule' Parameters](#).

Import inbound caller ID reformatting rules

We recommend that you export inbound caller ID reformatting rules to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 5 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information, see ['Inbound Caller ID Reformatting Rule' Parameters](#).

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit a desired trunk.
2. In the Inbound Caller ID Reformatting tab, click Import.
3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The inbound caller ID reformatting rules in the CSV file will be displayed in the Inbound Caller ID Reformatting list.

Customize Outbound Caller IDs

This topic describes different ways to customize outbound caller IDs, which help customers recognize who's calling.

Background information

Before you start to customize outbound caller IDs, you may need to know the following concepts:

- [Caller ID types](#)
- [Priority of outbound caller ID](#)

Prerequisites

Customizing outbound caller ID should be supported by the trunk provider.

Customize outbound caller ID for a trunk

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit the desired trunk.
2. Click Outbound Caller ID tab.
3. In the General section, configure a general Outbound Caller ID and Outbound Caller ID Name for the trunk.
4. Click Save and Apply.

The general outbound caller ID and caller ID name will be displayed on the called party's device when users make outbound calls through this trunk.

Customize outbound caller IDs for extensions

You can set up an outbound caller ID for a specific extension based on a trunk, so that an associated caller ID is sent out when the user calls out.

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit the desired trunk.
2. Click Outbound Caller ID tab.
3. In the Outbound Caller ID List section, click Add, and configure outbound caller IDs for extensions by different methods.
4. To associate one outbound caller ID with multiple extensions, select Shared Outbound Caller ID and configure the following settings:
 - Outbound Caller ID
 - Outbound Caller ID Name
 - Associated Extensions
5. To bind consecutive outbound caller IDs to consecutive extensions with one-to-one correspondence, select Outbound Caller ID Range and configure the following settings:
 - Outbound Caller ID Range
 - Extension Range
 - Outbound Caller ID Name
6. Click Save and Apply.

When extension users make outbound calls through the configured trunk, the associated outbound caller IDs will be displayed on the called party's device.

Customize outbound caller IDs based on dialed numbers

When calling to multiple areas, you may need to display pre-defined local number for the area code you are dialling. In this case, you can configure outbound caller IDs based on the dialed numbers.

The following instruction describes how to display a custom outbound caller ID 05925503301 when users call to local numbers that have area code 0592.

1. Log in to PBX management portal, go to Call Control > Outbound Route, edit the outbound route that is for local calls with area code 0592.
2. In the General section, enter the custom caller ID in the Outbound Caller ID field.

The screenshot shows the configuration interface for an outbound route. The 'General' section includes a 'Name' field with the value 'LocalNumber-0592' and an 'Outbound Caller ID' field with the value '05925503301'. Below this is a 'Dial Pattern' section with 'Dial Matching Settings' which contains a table with the following data:

Pattern	Strip	Prepend
0592XXXXXXXX		

3. Click Save and Apply.

Export and Import Trunk Outbound Caller IDs

Trunk outbound caller IDs configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired outbound caller ID list numbers in the exported file, and import the file to PBX again. This topic describes how to export and import outbound caller ID list.

Export all outbound caller ID list

You can export all outbound caller ID list to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit a desired trunk.
2. Click the Outbound Caller ID tab.
3. In the Outbound Caller ID List section, click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see [Trunk Outbound Caller ID Parameters](#).

Import outbound caller ID list

We recommend that you export outbound caller ID list to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 5 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information , see [Trunk Outbound Caller ID Parameters](#).

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit a desired trunk.
2. In the Outbound Caller ID List section, click Import.
3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The outbound caller id in the CSV file will be displayed in the Outbound Caller ID List.

Distinctive Ringtone


Distinctive Ringtone Overview

This topic describes what is Distinctive ringtone, applications, and how does Distinctive ringtone work.

What is Distinctive ringtone

Distinctive ringtone is an effective feature for businesses. Distinctive ringtone allows employees to distinguish incoming calls without looking at the Caller Name or Caller ID on the phone display.

For example, company may have different ring groups or queues for the sales team, the customer service team, and the support team. This could all be fed from IVR where the caller presses 1, 2, or 3 that equates to each team. For smaller businesses that have the same employee answering most of the calls, separating each business by its own distinctive ringtone can make the employee quickly identify who is calling or if the call is for him/her.

 Important:

Distinctive ringtone is not support on all SIP phone. Make sure that your phones support playing distinctive ringtone by "alert info text".

Applications

With the Distinctive ringtone feature, you can assign different call ringtones for the following types of calls:

- [Set Distinctive Ringtones for Internal Calls](#)
- [Set Distinctive Ringtones for External Calls](#)
- [Set Distinctive Ringtones for Queue Calls](#)
- [Set Distinctive Ringtones for Ring Group Calls](#)
- [Set Distinctive Ringtones for IVR Calls](#)

How does Distinctive ringtone work

Distinctive ringtone feature allows certain incoming calls to trigger IP phones to play specific d ringtones. The achievement of distinctive ringtone relies on an "alert info text".

1. Yeastar P-Series PBX System adds an "alert info text" in Alert-Info header for incoming calls, and then sends the incoming call (an INVITE request with the Alert-Info header) to the IP phone.
2. The IP phone inspects the INVITE request for an "Alert-Info" header, strips out the "alert info text", and then plays corresponding ringtone associated with the "alert info text".

Set Distinctive Ringtones for Internal Calls

When an extension user hears the ringtone of an internal incoming call, the user may notice the intention of the call.

Procedure

1. [Set alert info for internal calls on the PBX.](#)
2. [Set a specific ringtone for a phone.](#)

Set alert info for internal calls on the PBX

1. Log in to PBX management portal, go to PBX Settings > SIP Settings > Advanced.
2. In the SIP Request Header section, enter an alert info in the Internal Alert Info field.

The alert info is used to trigger IP phones to play a specific ringtone when receiving an internal call.

In this example, set alert info to `Internal`.

SIP Request Header

User Agent

Internal Alert Info

Internal

Set a specific ringtone for a phone

For users who want to play a specific ringtone for internal calls on their phones, you can set a specific ringtone for their phones by [auto provisioning](#).

Note:

Users can also log in to phone web interface to set distinctive ringtone manually on their own IP phones. For more information, contact the phone manufacturer.

Prerequisites

Each user who wants distinctive ringtone has bound a phone with their extensions.

For more information, see [Auto Provision IP Phones](#).

Procedure

1. Set a specific internal ringtone for a user's phone.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the user's extension.
 - b. Click Phone tab to edit the phone associated with the extension.
 - c. In the Distinctive Ringtone section, click Add.
 - d. In the Alert Info field, select the alert info that is pre-defined for internal calls.

In this example, select `Internal`.

- e. In the Ringtone field, select a ringtone for the internal calls.

In this example, select `Ring1.wav`.


Note:

The available ringtones vary by phone models.

No.	Alert Info	Ringtone	Operations
1	Internal	Ring1.wav	

+ Add

- f. Click Save.
2. Reprovision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.

- b. Click  beside the phone assigned to the user's extension.

Result

The user's phone plays ringtone Ring1.wav when receiving internal calls.

Set Distinctive Ringtones for External Calls

You can set distinctive ringtones on different inbound routes. When an extension user hears the ringtone of an external incoming call, the user may notice the intention of the call.

Procedure

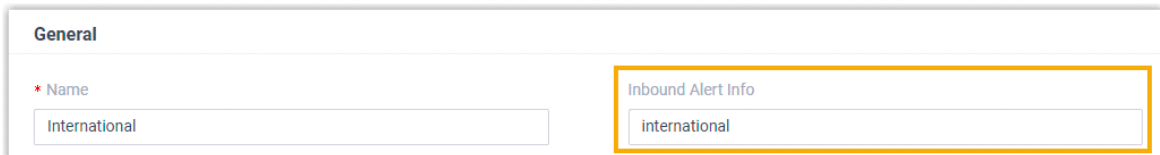
1. [Set alert info for external calls on the PBX.](#)
2. [Set a specific ringtone for a phone.](#)

Set alert info for external calls on the PBX

1. Log in to PBX management portal, go to Call Control > Inbound Route, edit a desired inbound route.
2. In the General section, enter an alert info in the Inbound Alert Info field.

The alert info is used to trigger IP phones to play a specific ringtone when receiving external calls from the inbound route.

In this example, set alert info to `international` to identify international calls.



The screenshot shows a configuration form with two input fields. The first field is labeled '* Name' and contains the text 'International'. The second field is labeled 'Inbound Alert Info' and contains the text 'international'. The second field is highlighted with a yellow border.

3. Click Save and Apply.

Set a specific ringtone for a phone

For users who want to play a specific ringtone for external calls on their phone, you can set a specific tone for their extensions by [auto provisioning](#).

Note:

Users can also log in to phone web interface to set distinctive ringtone manually on their own IP phones. For more information, contact the phone manufacturer.

Prerequisites

The user's extension should have been associated with a phone.

For more information, see [Auto Provision IP Phones](#).


Procedure



1. Set distinctive ringtones for a user.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the user's extension.
 - b. Click the Phone tab.
 - c. In the Distinctive Ringtone section, click Add.
 - d. In the Alert Info field, select the alert info that is pre-defined for external calls.

In this example, select `international`.


- e. In the Ringtone field, select a specific ringtone for international calls.

In this example, select `Ring2.wav`.

 **Note:**
The available ringtones vary by phone models.

Distinctive Ringtone			
No.	Alert Info	Ringtone	Operations
1	Internal	Ring1.wav	
2	international	Ring2.wav	

+ Add

- f. Click Save.
2. Reversion the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click  beside the phone assigned to user's extension.

Result

The user's phone plays ringtone `Ring2.wav` when receiving external calls from the specific inbound route.

Set Distinctive Ringtones for Queue Calls

You can set a unique ring tone per call queue so that the agents can easily identify who is calling. This is especially useful for the agents who are in multiple call queues to help them identify calls.

Procedure

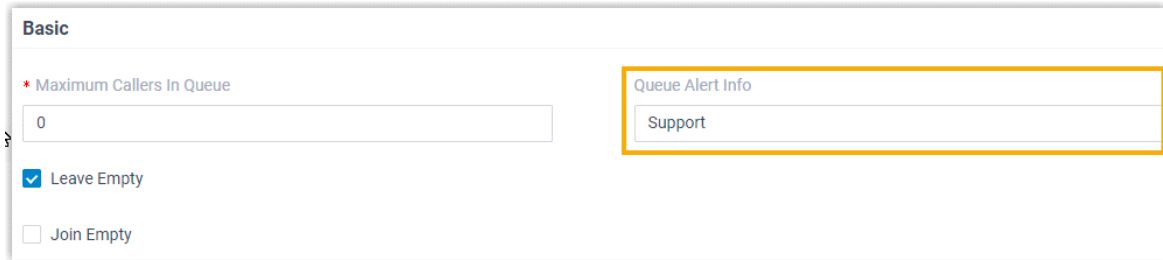
1. [Set an alert info for queue calls on the PBX.](#)
2. [Set a specific ring tone for a phone.](#)

Set an alert info for queue calls on the PBX

1. Log in to PBX management portal, go to Call Features > Queue, edit a desired queue.
2. Click the Preferences tab.
3. In the Basic section, enter an alert info in the Queue Alert Info field.

The alert info is used to trigger IP phones to play a specific ring tone when receiving a call through this queue.

In this example, set the alert info to `Support`.



The screenshot shows a configuration window titled "Basic". It contains several fields and checkboxes:

- Maximum Callers In Queue:** A text input field containing the number "0".
- Queue Alert Info:** A text input field containing the word "Support", which is highlighted with a yellow border.
- Leave Empty:** A checked checkbox.
- Join Empty:** An unchecked checkbox.

Set a specific ring tone for a phone

For the agents who want to play unique ring tones for different queue calls on their phones, you can set distinctive ring tones for their phones by [auto provisioning](#).

Note:

Users can also log in to phone web interface to set distinctive ring tone manually on their own IP phones. For more information, contact the phone manufacturer.

Prerequisites

The agent's extension should have been associated with a phone.

For more information, see [Auto Provision IP Phones](#).

Procedure

1. Set a specific queue ring tone for an agent's phone.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the agent's extension.
 - b. Click the Phone tab.
 - c. In the Distinctive Ringtone section, click Add.
 - d. In the Alert Info field, select the alert info that is pre-defined for queue calls.

In this example, select `Support`.

- e. In the Ringtone field, select a specific ring tone for the queue calls.

In this example, select `Ring3.wav`.

Note:

The available ring tones vary by phone models.

No.	Alert Info	Ringtone	Operations
1	Support	Ring3.wav	
+ Add			

- f. Click Save.
2. Re provision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click beside the phone assigned to agent's extension.

Result

The agent's phone plays ring tone Ring3.wav when receiving calls from the Support queue.

Set Distinctive Ringtones for Ring Group Calls

You can set a unique ringtone per ring group so that the members can easily identify who is calling. This is especially useful for the members who are in multiple ring groups to help them identify calls.

Procedure

1. [Set an alert info for ring group calls on the PBX.](#)
2. [Set a specific ringtone for a phone.](#)

Set an alert info for ring group calls on the PBX

1. Log in to PBX management portal, go to Call Features > Ring Group, edit a desired ring group.
2. In the Ring Group Alert Info section, enter an alert info.

The alert info is used to trigger IP phones to play a specific ringtone when receiving a call through this ring group.

In this example, set alert info to Sales.

* Number 6300	* Name Sales
* Ring Strategy Ring All	* Ring Timeout (s) 60
Ring Group Alert Info Sales	

Set a specific ringtone for a phone

For ring group members who want to play a specific ringtone for ring group calls on their phone, you can set a specific tone for their extensions by [auto provisioning](#).

Note:

Users can also log in to phone web interface to set distinctive ringtone manually on their own IP phones. For more information, contact the phone manufacturer.

Prerequisites

The ring group member's extension should have been associated with a phone.

For more information, see [Auto Provision IP Phones](#).

Procedure

1. Set a specific ringtone for a ring group member.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit ring group member's extension.
 - b. Click the Phone tab.
 - c. In the Distinctive Ringtone section, click Add.
 - d. In the Alert Info field, select the alert info that is pre-defined for ring group calls.


In this example, we select `Sales`.


- e. In the Ringtone field, select a specific ringtone for the ring group calls.

In this example, we select `Ring4.wav`.

Note:

The available ringtones vary by phone models.

Distinctive Ringtone			
No.	Alert Info	Ringtone	Operations
1	Sales	Ring4.wav	
+ Add			

- f. Click Save.
2. Reprovision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click  beside the phone assigned to ring group member's extension.

Result

The ring group member's phone plays ringtone Ring4.wav when receiving calls from the Sales ring group.

Set Distinctive Ringtones for IVR Calls

You can set a unique ringtone per IVR so that the extension users can easily identify who is calling.

Procedure

1. [Set an alert info for IVR calls on the PBX.](#)
2. [Set a specific ringtone for a phone.](#)

Set an alert info for IVR calls on the PBX

1. Log in to PBX management portal, go to Call Features > IVR.
2. In the IVR Alert Info field, enter an alert info.

The alert info is used to trigger IP phones to play a specific ringtone when receiving a call through this IVR.

In this example, set alert info to `CustomerService`.

The screenshot shows a configuration form for IVR settings. The fields are as follows:

- * Number:** 6200
- * Name:** Customer Service
- * Prompt:** [Default] x
- * Prompt Repeat Count:** 3
- * Response Timeout (s):** 3
- * Digit Timeout (s):** 3
- IVR Alert Info:** CustomerService (highlighted with a yellow border)

Set a specific ringtone for a phone

For users who want to play a specific ringtone for IVR calls on their phone, you can set a specific tone for their extensions by [auto provisioning](#).

Note:

Users can also log in to phone web interface to set distinctive ringtone manually on their own IP phones. For more information, contact the phone manufacturer.

Prerequisites

The user's extension should have been associated with a phone.

For more information, see [Auto Provision IP Phones](#).


Procedure


1. Set a specific ringtone for a user.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the user's extension.
 - b. Click the Phone tab.
 - c. In the Distinctive Ringtone section, click Add.
 - d. In the Alert Info field, select the alert info that is pre-defined for IVR calls.


In this example, select `CustomerService`.

- e. In the Ringtone field, select a specific ringtone for the IVR calls.

In this example, select `Ring5.wav`.

 **Note:**
The available ringtones vary by phone models.

Distinctive Ringtone			
No.	Alert Info	Ringtone	Operations
1	CustomerService	Ring5.wav	
+ Add			

- f. Click Save.
2. Re provision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click  beside the phone assigned to user's extension.

Result

The user's phone plays ringtone `Ring5.wav` when receiving calls from `CustomerService` IVR.

Distinctive Caller ID Name


Distinctive Caller ID Name Overview

This topic describes what is Distinctive Caller ID Name, and an example of Distinctive Caller ID Name.

What is Distinctive Caller ID Name


Distinctive Caller ID Name allows employees to know where the incoming call is routed, and who is calling. Distinctive Caller ID Name is a string that will be displayed on employees' phones, which may include the followings (from the highest to the lowest):

1. Contact name that is stored in Company Contacts directory or Personal Contacts directory.

 Note:


If the extension user does not have permission to view Company Contacts, the contact name stored in Company Contact will not be displayed on the extension user's phone.

2. Call feature name (the name of IVR, Ring Group, or Queue)

 Note:

If an incoming call reaches an extension through multiple call features, the name of the last call feature will be displayed. For example, if a call reaches an IVR and then goes to a queue, the queue name will be displayed on agents' phones.

3. Trunk DID/DDI name
4. Caller Name (CNAM): CNAM is sent from the caller that displays the caller name or the caller's company name.

 Note:

CNAM is configured by the caller's side.

An example of Distinctive Caller ID Name

Your company has a support team that is responsible for providing technical services for customers from China and America.. The following settings are configured on your PBX to achieve your goal:

Queue

A queue named "Support" for support team.

SIP trunk

A SIP trunk with two DID numbers that are bound with their respective names.

Table 31.

DID Number	DID Name
1258888	China
1256666	America

Assume that you have the following two contacts stored in your Company Contact directory.

Name	Phone Number
Sunny	5502222
Becky	5503333

When customers dial different DID numbers and reach the Support queue, the caller ID names displayed differently on agents' phones. The display priority of Distinctive Caller ID Name is as below:

{contact_name}: {queue_name}: {trunk_did_name}: {caller_name}



Note:

If none of the above names are provided, the names will not be displayed.

Example:

- Customer Becky dials 1258888 to reach the Support team and no Caller Name is sent from Becky, the caller ID name displayed is Becky: Support: China.
- Customer Sunny dials 1256666 to reach the Support team and no Caller Name is sent from Sunny, the caller ID name displayed is Sunny: Support: America.
- Customer C dials 1258888 to reach the Support team and a Caller Name "Yeastar" is sent from customer C, the caller ID name displayed is Support: China: Yeastar

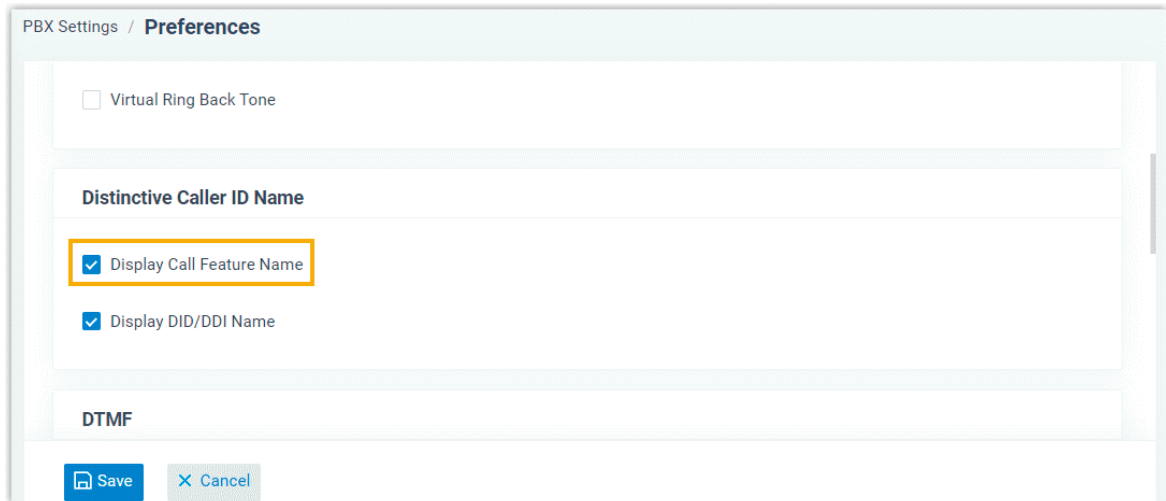
Enable or Disable Distinctive Caller ID Name

You can decide whether to display a call feature name (Queue name, IVR name, or Ring Group name) or a name associated with a trunk DID/DDI number when an incoming call reaches.

Enable or disable the display of call feature name

The call feature name refers to the name of an IVR, a Ring Group, or a Queue.

1. Log in to PBX management portal, go to PBX Settings > > Preferences.
2. In the Distinctive Caller ID Name section, configure the followings:
 - To display Queue names, Ring Group names, and IVR names, select the check-box of Display Call Feature Name.
 - To hide Queue names, Ring Group names, and IVR names, unselect the check-box of Display Call Feature Name.



PBX Settings / **Preferences**

Virtual Ring Back Tone

Distinctive Caller ID Name

Display Call Feature Name

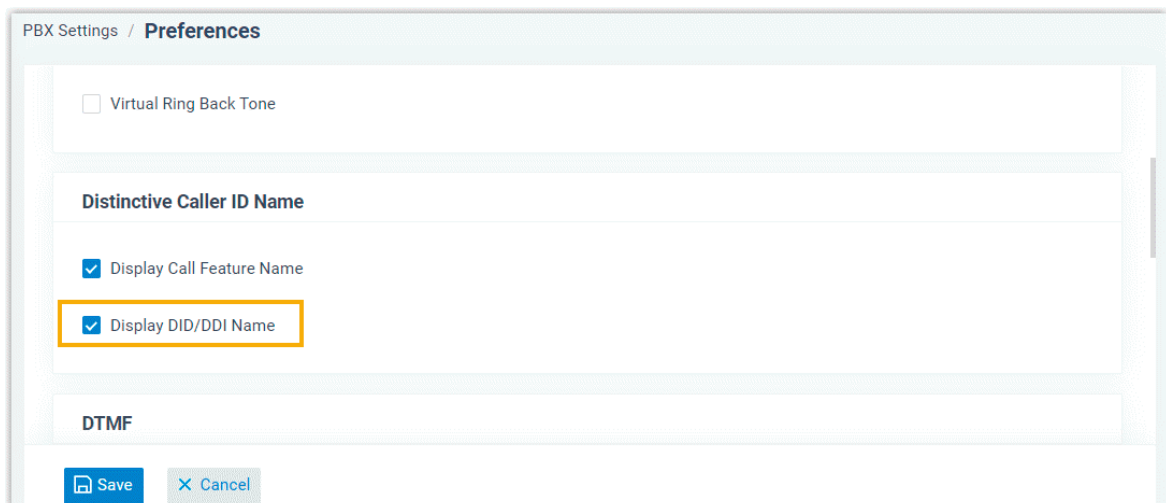
Display DID/DDI Name

DTMF

3. Click Save and Apply.

Enable or disable the display of trunk DID/DDI name

1. Log in to PBX management portal, go to PBX Settings > Preferences.
2. In the Distinctive Caller ID Name section, configure the followings:
 - To display trunk DID/DDI name, select the checkbox of Display DID/DDI Name.
 - To hide trunk DID/DDI name, unselect the checkbox of Display DID/DDI Name.



PBX Settings / **Preferences**

Virtual Ring Back Tone

Distinctive Caller ID Name

Display Call Feature Name

Display DID/DDI Name

DTMF

3. Click Save and Apply.

Call Center

Call Center Overview

This topic describes what is Yeastar Call Center service, highlight, and the steps to set up a Call Center.

Prerequisites

Yeastar Call Center is a service that is only available on Yeastar Enterprise Plan and Ultimate Plan.

What is Yeastar Call Center service

Yeastar P-Series PBX System introduces an inbound call center solution to improve agent efficiency, responsiveness, and ultimate customer satisfaction for SMEs running service centers.

Yeastar Call Center provides a powerful console for manager and agents to handle [queue](#) calls. Call Center Console is a web-based utility integrated with Linkus Web Client, including a customizable Wallboard for proactive tracking of 16 key performance metrics, and a switchboard-type Queue Panel for real-time monitoring & control of queue activities.

For more information of monitoring queue performance and managing queue calls on Call Center Console, see [Yeastar Call Center Console User Guide](#).

Highlight

- Real-time metrics on Wallboard: Display a range of call center metrics and KPIs that allow queue managers to monitor and optimize performance, and spot emerging trends in a central location.
- Switchboard-type Queue Panel: Show the call metrics and agents' performance in real time, and offer a comprehensive view on activity of call that allows manager and agents to handle queue calls.
- SLA for performance measurement: Consistent delivering service that meets or exceeds the expectations set out in the SLA.
- Insightful Call Center reports: Real-time and historical reports that help system administrator to track queue performance indicators, and assess agent performance.

Steps to set up Call Center

1. [Create a queue](#).
2. Set up Call Center.
 - a. Manage queue managers: Set one or more extension users as queue managers.
The queue managers can receive queue notifications by email.

- b. Customize queue notification: Send email notifications to queue manager when a queue call is missed or abandoned, or the service level agreement reaches the alarm threshold.
 - c. Grant queue panel permissions: Grant the permissions respectively for queue manager and agents.
 - d. Set up Service Level Agreement (SLA): Define a certain level of service for a queue.
3. Manage Call Center report: View and schedule Call Center reports.

Call Center Setup

Set up Queue Managers

With call center service activated, you can set any extension as queue manager. A queue manager does not need to be a queue agent. This topic describes how to set queue managers.

Procedure

1. Log in to PBX management portal, go to Call Features > Queue, edit the desired queue.
2. Click Members tab.
3. In the Queue Managers section, manage the queue managers:
 - To add queue managers: Select the desired extensions from the Available box to the Selected box.
 - To delete queue managers: Select the desired extensions from the Selected box to the Available box.
4. Click Save and Apply.

Customize Queue Notification

With call center service activated, the system sends email notifications to queue managers when a queue call is missed or abandoned, or when the service level agreement reaches the alarm threshold. This topic describes how to customize these notifications.

Prerequisites

- Make sure there is a valid email address assigned to queue manager's extension.
- Make sure [system email](#) works.

Procedure

1. Log in to PBX management portal, go to Call Features > Queue, edit the desired queue.
2. Click Members tab.

3. Select the checkbox of notification option according your needs.
 - Notify Manager when a queue call is missed: Send an email to manager when a queue call is missed.
 - Notify Manager when a queue call is abandoned: Send an email to manager when a queue call is abandoned.
 - Notify Manager when the SLA is lower than its alarm threshold: Send an email to manager when the SLA alarm threshold is reached.
4. Click Save and Apply.

Grant Queue Panel Permissions

With call center service activated, you can decide what the queue managers and agents can do on Queue Panel, and grant the Queue Panel permissions for queue manager and agents respectively. This topic describes how to grant permissions for queue manager and agents.

Queue Panel permissions

Permission	Manager	Agents
Switch agents' Status	√	×
Call monitoring operations (Listen, Whisper, Barge In)	√	×
Switch agent's recording status	√	×
Call distribution management (Redirect, Transfer, Drag and Drop operation)	√	√
Allow for picking up or hanging up agents' calls	√	√
Call parking operation	√	√

Grant permissions for queue managers

1. Log in to PBX management portal, go to Call Features > Queue, edit the desired queue.
2. Click Queue Panel Permissions tab.
3. In the Manager section, select the checkboxes of permissions according to your needs.
4. Click Save and Apply.

Grant permissions for agents

1. Log in to PBX management portal, go to Call Features > Queue, edit the desired queue.
2. Click Queue Panel Permissions tab.

3. In the Agents section, select the checkboxes of permissions according to your needs.
4. Click Save and Apply.

Set up Service Level Agreement (SLA)

With call center service activated, you can set up service level agreement for a queue. This topic describes what is service level agreement and how to set up service level agreement.

What is Service Level Agreement (SLA)

Service Level Agreement is a call center performance statistic. It is the goal for how quickly the agent should answer a portion of the customers, and makes sure everyone is working to the same objectives.

SLA is expressed as the percentage of conversations answered within a predefined amount of time. Let us suppose that the goal is to answer 80% of calls within 20 seconds. If the measurement is less than 80%, the manager knows they are outside their target Service Level.

The calculated formula shows as below:

$$\text{SLA} = \frac{\text{total calls} - (\text{calls answered after SLA time} + \text{calls abandoned after SLA time})}{\text{total calls}} \times 100\%$$

How to set up Service Level Agreement

You can set a target service level and SLA threshold for each queue, and evaluate the service level periodically.

1. Log in to PBX management portal, go to Call Features > Queue, edit the desired queue.
2. Click Preferences tab.
3. In the Service Level Agreement section, edit the SLA according to your needs.
 - SLA Time(s): Enter the maximum amount of time (in seconds) that an agent needs to answer an incoming call.
If a caller waits for a duration of time shorter than the SLA Time, the SLA is met.
 - Evaluation Interval(min): Enter the time interval to compare the queue's SLA performance against the alarm threshold so that the system can send a notification email timely.
 - Alarm Threshold(%): Enter the service level threshold for the queue.
4. Click Save and Apply.

Call Center Report

Call Center Reports Overview

Yeastar P-Series PBX System provides a set of predefined reports concerning detailed information about call center performance. This topic describes what you can do with call center report, and the report types.

What you can do with call center reports

The system automatically generates reports in the format of graphs or charts, and helps you to simplify analysis and extract invaluable data with ease. These reports can be historical and real-time. You can view and schedule reports on demand to evaluate past activities and plan future actions.

Reports types

We divide reports into two categories: queue performance and agent performance.

- Queue performance reports: The queue performance reports give you insight into the work efficiency of one or more queues over a period of time, and help you evaluate the performance of each queue.
 - Queue Performance
 - Queue AVG Waiting & Talking Time
 - Satisfaction Survey
- Agent performance reports: The agent performance reports give you insight into the performance of one or more agents, and help you evaluate if every agent meets the expectations of your call center over a period of time.
 - Agent Login Activity
 - Agent Pause Activity
 - Agent Missed Call Activity
 - Agent Call Summary

Queue Performance reports

'Queue Performance' Report

Queue Performance provides information about how calls are handled by queues. This topic describes the report details, and shows you a report example.

Report details

The following table lists the related parameters for Queue Performance report.

Parameter	Description
Total Calls	The total number of calls that queue received.
Answered	The total number of calls that queue answered.
Missed	The total number of calls that queue missed.
Abandoned	The total number of calls that callers abandoned before connecting to an agent.
Max Waiting Time	The longest time a caller waited in the queue before an agent answered the call.
Average Waiting Time	The average amount of time that it takes for an incoming call to be distributed to an agent.
Answered Rate	The percentage of answered calls in relation to the total received calls.
Missed Rate	The percentage of missed calls in relation to the total received calls.
Abandon Rate	The percentage of abandoned calls in relation to the total received calls.
SLA	The Service Level Agreement (SLA) for the queue. SLA is the percentage of conversations answered within a predefined amount of time.

Report example

The following report shows the performance of the Service department in the past 30 days. Calls abandoned within 10 seconds are not included in the report.

Queue	Total Calls	Answered	Missed	Abandoned	Average Waiting Time	Max Wait Time	Answered Rate	Missed Rate	Abandon Rate	SLA
Service	20	13	4	3	00:00:17	00:01:42	65%	20%	15%	55%
Total	20	13	4	3						

'Queue AVG Waiting & Talking Time' Report

Queue AVG Waiting & Talking Time report provides information about the average amount of time that callers are waiting in a queue, and the average amount of time that an agent spends in handling calls. The report helps you to identify the peak times of queue calls, and allocate your agent accordingly. This topic describes the report details, and shows you a report example.

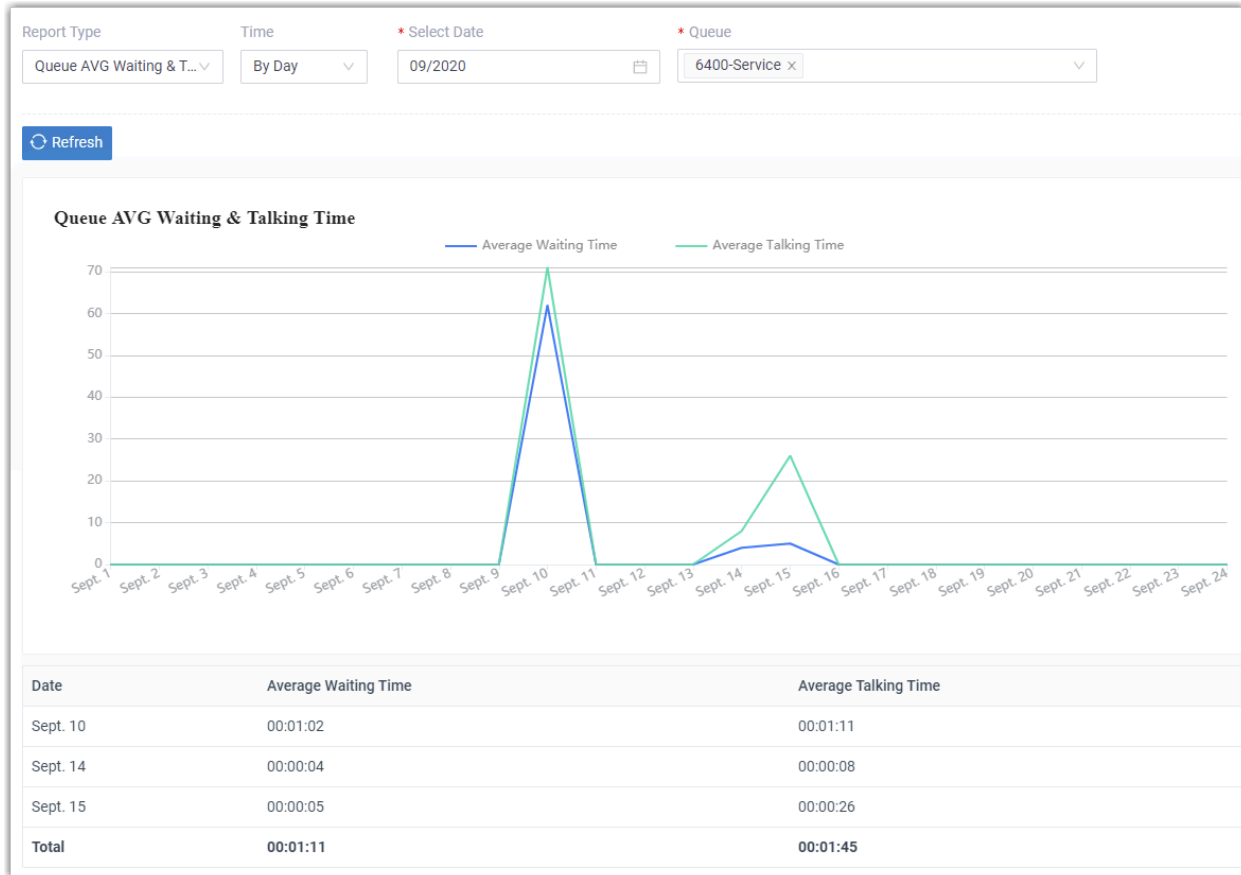
Report details

The Queue AVG Waiting & Talking Time includes a graph and a table that shows the following information for each queue:

Parameter	Description
Average Waiting Time	The average amount of time that it takes for an incoming call to be distributed to an agent.
Average Talking Time	The average amount of time that a caller talks to an agent.

Report example

The following report shows the daily average waiting & talking time of Service department during 09/2020.



'Satisfaction Survey' Report

Satisfaction Survey report provides statistic about the key pressed collected from callers. The report helps you measure customer satisfaction and improve service. This topic describes the report details, and shows you a report example.

Report details

After the agent hangs up a call, the system plays a pre-defined prompt to ask callers to rate their satisfaction scale. For example, "Please rate your satisfaction with our service, press 1 for satisfied, press 2 for dissatisfied. Thank you.". The Satisfaction Survey report displays how many times that a key is pressed by callers.

Report example

The following report shows the satisfaction survey of Service department and its agents in the last 7 days.

Queue	KEY:1	KEY:2	KEY:4
6400-Service	4	2	1
3333-Sunny Yeah	1	1	0
3334-John Snow	3	1	1

Agent Performance Report

'Agent Login Activity' Report

Agent Login Activity report provides information about the login and logout activities of each agent. The report helps you count the working hours of the agents working in shifts. This topic describes the report details, and shows you a report example.

Report details

The Agent Login Activity includes a table that shows the following information for each agent:

Parameter	Description
Logged in	The date and time that an agent logged in to a queue.
Logged out	The date and time that an agent logged out of a queue.
Total Login Time	The elapsed time between the login time and the logout time.

Report example

The following report shows the login activities of all agents in Service department in the past 7 days.

Report Type	Time	Queue	Agent
Agent Login Activity	09/14/2020 00:00:00 ~ 09/21/2020 23:59:59	6400-Service	
Refresh			
Agent	Logged In	Logged Out	Total Login Time
1000-Becky	09/21/2020 10:54:20	09/21/2020 10:58:36	00:04:16
	09/21/2020 11:01:39	09/21/2020 11:02:22	00:00:43
Total			00:04:59
3333-Sunny Yeah	09/21/2020 10:54:24	09/21/2020 10:58:49	00:04:25
Total			00:04:25
3334-John Snow	09/21/2020 10:54:27	09/21/2020 11:01:29	00:07:02
	09/21/2020 11:02:11	09/21/2020 11:02:56	00:00:45
Total			00:07:47
3335-Jim	09/21/2020 10:54:29	09/21/2020 11:01:32	00:07:03
	09/21/2020 11:02:13	09/21/2020 11:02:58	00:00:45
Total			00:07:48

'Agent Pause Activity' Report

Agent Pause Activity report provides information about the pause and unpause activities of each agent. The report helps you count the pause time of each agents. This topic describes the report details, and shows you a report example.

Report details

The Agent Pause Activity shows the following information for each agent:

Parameter	Description
Pause	The date and time that an agent changed status to pause.
Unpause	The date and time that an agent changed status to unpause.
Total Pause Time	The elapsed time between the paused time and the unpaused time.

Report example

The following report shows the pause activities of all agents in Service department in the past 7 days.

Agent	Pause	Unpause	Total Pause Time
3333-Sunny Yeah	09/14/2020 15:16:03	09/14/2020 15:16:31	00:00:28
Total			00:00:28
3334-John Snow	09/21/2020 10:55:06	09/21/2020 10:58:28	00:03:22
Total			00:03:22
1000-Becky	09/21/2020 10:55:04	09/21/2020 10:58:33	00:03:29
Total			00:03:29
3335-Jim	09/21/2020 10:55:09	09/21/2020 10:58:40	00:03:31
Total			00:03:31

'Agent Missed Call Activity' Report

Agent Missed Call Activity report provides the missed call information for each agent. The report helps you assess an agent's efficiency. This topic describes the report details, and shows you a report example.

Report details

Parameter	Description
Time	The date and time that an agent missed a call.
Waiting Time	The amount of time that the caller waited for the assigned agent to answer the call.
Call From	The caller's caller ID.
Agent Status	The final status of missed calls, indicating whether the missed calls were answered by other agents.
Polling Attempts	The number of polling attempts to call an agent.

Report example

The following report shows the missed call activities of all agents in Service department in the past 30 days. Calls abandoned within 10 seconds are not included in the report.

Report Type	Time	Queue	Agent	Short Abandoned Calls	
Agent Missed Cal... ▾	08/26/2020 00:00:00 ~ 09/24/2020 23:59:59 🗑️	6400-Service ▾	▾	10	
Refresh					
Agent	Time	Waiting Time	Call From	Agent Status	Polling Attempts
3333-Summy Yeah	09/10/2020 17:16:31	00:02:28	3337	NO ANSWER	5
	09/10/2020 17:31:44	00:00:30	4444	NO ANSWER	1
Total		00:02:58			6
3334-John Snow	09/10/2020 17:45:07	00:00:10	3337	NO ANSWER	1
Total		00:00:10			1

'Agent Call Summary' Report

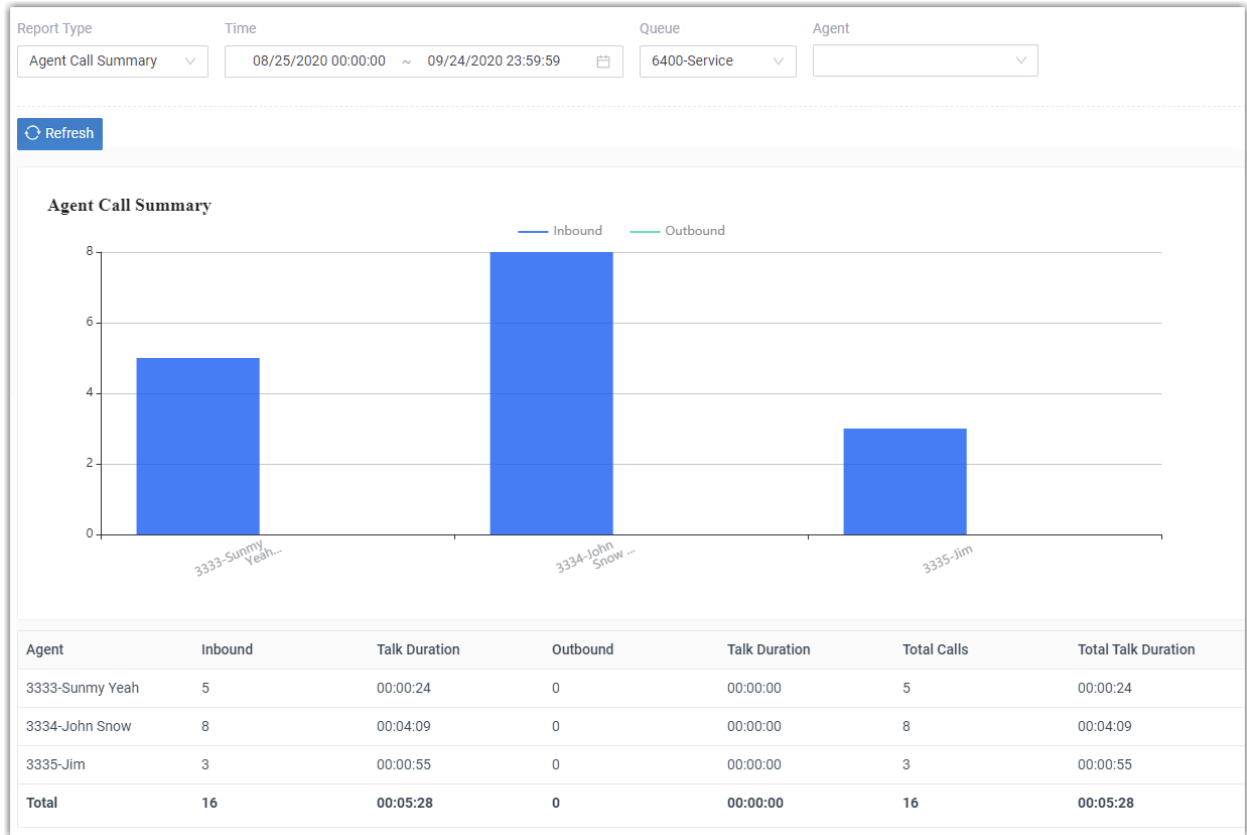
Agent Call Summary report provides information about the number of incoming and outgoing calls that were received and placed by each agent. This topic describes the report details, and shows you a report example.

Report details

Parameter	Description
Inbound	The number of incoming calls received by an agent.
Outbound	The number of outgoing calls placed by an agent.
Talk Duration	The amount of time an agent spent in incoming calls or outgoing calls.
Total calls	The total number of incoming calls and outgoing calls handled by an agent.
Total Talk Duration	The total amount of time an agent spent in incoming calls and outgoing calls.

Report example

The following report shows the call summary of all agents in Service department in the last 30 days.



Call Features

Voicemail

Voicemail Overview

Yeastar P-Series PBX System integrates a free voicemail system. This topic describes the voicemail types, voicemail usages, voicemail personalization, and the adjustable voicemail capacity and limitations.

Voicemail types

Yeastar P-Series PBX System provides two types of voicemail:

- Extension Voicemail: Voicemail for individual extension.
- Group Voicemail: Group Voicemail is a feature for a team to share the workload of reading and responding to voicemail messages.

Group Voicemail is useful if your company is organized into departments. For example, after setting up a group voicemail for Support team, a customer can deliver voicemail messages to the Support team, then any team members can access the group voicemail box to check the customer's voicemail.

Voicemail usages

A flexible call route system for forwarding calls to voicemail:

- Extension: Allow the caller to leave a message when the extension user is unavailable to take a call.
For more information, see [Forward extension users' calls to voicemail](#).
- Ring Group/Queue: Failover to group voicemail if no agents are available or timeout is reached.
For more information, see [Set failover destination to voicemail for a ring group or queue](#).
- IVR: Give the customers an option to leave a voicemail message. When the customers cannot get the information from IVR, they can leave a message.
For more information, see [Allow users to leave voicemail messages by IVR](#).
- Any inbound calls: Provide a dedicated line to collect user feedback if immediate phone support is not required.
For more information, see [Forward inbound calls to voicemail](#).

Voicemail personalization

Various options are available for personalizing voicemail:

- Voicemail greeting: Custom greeting is available for global or a specific extension. The extension users can also customize their greetings based on presence.
For more information, see [Voicemail Greeting Overview](#).
- Voicemail notification: Various ways to get notified of new voicemail messages, including on IP phones, emails, or Linkus clients.
For more information, see [Voicemail Notification Overview](#).
- Envelope playback: Play optional envelope information before listening to voicemail message, including date and time, caller ID, and message duration.
For more information, see [Configure Message Envelope](#).
- Caller experience: User-friendly experience in leaving a message, such as allow the caller to review message, send a message without ringing extensions, break out of voicemail to operator, etc.
For more information, see:
 - [Allow Callers to Press a Key to Leave Messages](#)
 - [Allow Callers to Dial Extension from Voicemail](#)
 - [Allow Callers to Break out from Voicemail](#)
 - [Allow Callers to Review Voicemail Messages](#)

Voicemail capacity and limitations

The default and adjustable capacity and limitations for each voicemail box are as follows:

- Message length: 1 to 15 minutes.
The default minimum duration of a message is 2 seconds; the default maximum duration of a message is 10 minutes.
To change the message length, see [Limit Voicemail Message Length](#).
- Mailbox capacity: 1 to 500.
The default max number of voicemail is 100.
To change mailbox capacity, see [Auto Cleanup Voicemail Messages](#).
- Storage time: Unlimited.
The default is 0, which means no limit.
To change the storage time, see [Auto Cleanup Voicemail Messages](#).

Group Voicemail

Set up Group Voicemail for a Queue

You can set up a Group Voicemail for a queue. All agents of the queue will get notified when a group voicemail message is received.

Procedure

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail.
2. Click Add.
3. In the Basic section, configure the following settings.
 - Type: Select Queue.
 - Queue: Select a queue.
 - Number: The Group Voicemail number is the queue number, and is not editable.
 - Name: The Group Voicemail name is the queue name, and is not editable.
 - Mode: Select the mode to handle received voicemail messages.
 - Shared by Members: The voicemail messages are saved in the group mailbox, and are shared by all members. Any members can manage the group voicemail messages.
 - Broadcast to Members: The voicemail messages are not stored in the group mailbox. Instead, the system broadcasts (copies and forwards) the voicemail messages to the individual mailboxes of all the members.
 - Voicemail PIN Authentication: Enable or disable voicemail PIN authentication.
 - Voicemail Access PIN: If enable voicemail PIN authentication, enter a desired access PIN number.
 - Play Date and Time: Optional. Play the date and time that the message was received before a voicemail message is played.
 - Play Caller ID: Optional. Play the caller ID information before a voicemail message is played.
 - Play Message Duration: Optional. Play the duration of the message before a voicemail message is played.
4. In the Members section, all the agents of the queue are selected, and the members are not editable.



Note:

If the queue agents are changed, the members of the group's voice mailboxes also change.

5. In the Group Voicemail Greeting section, select a voicemail greeting.

You can also click Greeting Management to customize a greeting or manage your custom greetings.

6. Click Save and Apply.

Related information

- [Enable or Disable Voicemail Access PIN](#)
- [Change Voicemail Access PIN](#)
- [Configure Message Envelope](#)
- [Change Voicemail Greetings](#)
- [Record or Upload Voicemail Greetings](#)
- [Manage Group Voicemail Greetings](#)

Set up Group Voicemail for a Ring Group

You can set up a Group Voicemail for a ring group. All members of the ring group will get notified when a group voicemail message is received.

Procedure

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail.
2. Click Add.
3. In the Basic section, configure the following settings:
 - Type: Select Ring Group.
 - Ring Group: Select a ring group.
 - Number: The group voicemail number is the ring group number, and is not editable.
 - Name: The group voicemail name is the ring group name, and is not editable.
 - Mode: Select the mode to handle received voicemail messages.
 - Shared by Members: The voicemail messages are saved in the group mailbox, and are shared by all members. Any members can manage the group voicemail messages.
 - Broadcast to Members: The voicemail messages are not stored in the group mailbox. Instead, the system broadcasts (copies and forwards) the voicemail messages to the individual mailboxes of all the members.
 - Voicemail PIN Authentication: Enable or disable voicemail PIN authentication.
 - Voicemail Access PIN: If enable voicemail PIN authentication, enter a desired access PIN number.
 - Play Date and Time: Optional. Play the date and time that the message was received before a voicemail message is played.
 - Play Caller ID: Optional. Play the caller ID information before a voicemail message is played.
 - Play Message Duration: Optional. Play the duration of the message before a voicemail message is played.
4. In the Members section, all the members of the ring group are selected, and the members are not editable.

Note:

If the ring group members are changed, the members of the group's voice mailboxes also change.

5. In the Group Voicemail Greeting section, select a voicemail greeting.

You can also click Greeting Management to customize a greeting or manage your custom greetings.

6. Click Save and Apply.

Related information

[Enable or Disable Voicemail Access PIN](#)

[Change Voicemail Access PIN](#)

[Configure Message Envelope](#)

[Change Voicemail Greetings](#)

[Record or Upload Voicemail Greetings](#)

[Manage Group Voicemail Greetings](#)

Set up Group Voicemail for a Custom Group

For a team whose members come from different departments, you can set up a Group Voicemail for the team members. All team members will get notified when a group voicemail message is received.

Procedure

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail.
2. Click Add.
3. In the Basic section, configure the following settings:
 - Type: Select Custom.
 - Number: Specify a virtual number for callers to access the group voicemail.
 - Name: Enter a group voicemail name to help you identify it.
 - Mode: Select the mode to handle received voicemail messages.
 - Shared by Members: The voicemail messages are saved in the group mailbox, and are shared by all members. Any members can manage the group voicemail messages.
 - Broadcast to Members: The voicemail messages are not stored in the group mailbox. Instead, the system broadcasts (copies and forwards) the voicemail messages to the individual mailboxes of all the members.
 - Voicemail PIN Authentication: Enable or disable voicemail PIN authentication.
 - Voicemail Access PIN: If enable voicemail PIN authentication, enter a desired access PIN number.
 - Play Date and Time: Optional. Play the date and time that the message was received before a voicemail message is played.
 - Play Caller ID: Optional. Play the caller ID information before a voicemail message is played.
 - Play Message Duration: Optional. Play the duration of the message before a voicemail message is played.
4. In the Members section, select the custom group members.
5. In the Group Voicemail Greeting section, select a voicemail greeting.

You can also click Greeting Management to customize a greeting or manage your custom greetings.

6. Click Save and Apply.


Related information

- [Enable or Disable Voicemail Access PIN](#)
- [Change Voicemail Access PIN](#)
- [Configure Message Envelope](#)
- [Change Voicemail Greetings](#)
- [Record or Upload Voicemail Greetings](#)
- [Manage Group Voicemail Greetings](#)


Manage Group Voicemails

This topic describes how to edit a group voicemail, and delete group voicemails.

Edit a group voicemail

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail.
2. Click  beside the group voicemail that you want to edit.
3. Change the settings according to your needs.
 - [Enable or Disable Voicemail Access PIN](#)
 - [Change Voicemail Access PIN](#)
 - [Configure Message Envelope](#)
 - [Change Voicemail Greetings](#)
 - [Record or Upload Voicemail Greetings](#)
 - [Manage Group Voicemail Greetings](#)
4. Click Save and Apply.

Delete group voicemails

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail.
2. To delete a group voicemail:
 - a. Click  beside the group voicemail that you want to delete.
 - b. Click Apply.
3. To delete group voicemails in bulk:
 - a. Select the checkboxes of the group voicemails that you want to delete, click Delete.
 - b. Click OK and Apply.

Send and Receive Voicemail Messages

Forward Calls to Voicemail

Never miss a lead by allowing your customers to leave voicemail messages. This topic describes how to forward various kinds of calls to voicemail.

Background information

A growing business cannot afford to miss incoming calls. A missed call may make your customers impatient. Forwarding calls to voicemail automatically helps you to stay connected with customers and enhance the service.

In the following scenarios, you can consider a destination as voicemail, which helps the system to forward calls to voicemail:

- [Forward extension users' calls to voicemail](#): The extension user is unavailable to answer a call.
- [Set failover destination to voicemail for a ring group or queue](#): No members or agents are available to take a call or the call reaches the timeout.
- [Allow users to leave voicemail messages by IVR](#): Give the customers an option to leave a voicemail message. When the customers cannot get the information from IVR, they can leave a message.
- [Forward inbound calls to voicemail](#): Immediate phone support is not required.

Forward extension users' calls to voicemail

You can set call forwarding rules for each presence status as users' need, the system will forward extension users' calls to voicemail according to the presence status.

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Presence tab, select a presence status to configure.
3. In the Call Forwarding section, configure call forwarding rules for internal calls (incoming calls from colleagues) and external calls (inbound calls from customers).
 - a. Select the checkbox of a forwarding condition.
 - b. Select a corresponding destination for the forwarding condition to one of the following options:
 - Voicemail: Forward calls to the extension's voicemail box.
 - Group Voicemail: Forward calls to a selected group mailbox.
4. Click Save and Apply.

Set failover destination to voicemail for a ring group or queue

1. Log in to PBX management portal, set failover destination to voicemail.

- To set failover destination for a ring group, go to Call Features > Ring Group, edit the desired ring group.
 - To set failover destination for a queue, go to Call Features > Queue, edit the desired queue.
2. In the Failover Destination drop-down list, select a corresponding destination to one of the following options:
 - Extension Voicemail: Forward calls to the extension's voicemail box.
 - Group Voicemail: Forward calls to a selected group mailbox.
 3. Click Save and Apply.

Allow users to leave voicemail messages by IVR

Prerequisites

Update your IVR prompt that would instruct callers to press a key to access voicemail.

Procedure

1. Log in to PBX management portal, go to Call Features > IVR, edit the desired IVR.
2. Click Key Press Event tab, select a corresponding destination to one of the following options:
 - Extension Voicemail: Forward calls to the extension's voicemail box.
 - Group Voicemail: Forward calls to a selected group mailbox.
3. Click Save and Apply.

Forward inbound calls to voicemail

On non-working days, you can forward inbound calls to voicemail.

1. Log in to PBX management portal, go to Call Control > Inbound Route, edit the desired inbound route.
2. In the Default Destination section, select a corresponding destination to one of the following options:
 - Extension Voicemail: Forward calls to the extension's voicemail box.
 - Group Voicemail: Forward calls to a selected group mailbox.
3. Click Save and Apply.

Leave a Voicemail Message without Calling the User

This topic describes how to send a voicemail message without ringing extensions.

Background information

Although you can send a message by email or text, sometimes there is no replacement for the emotion, inflection, and sincerity of your voice. When you do not want to disturb some-

one or when you do not have time for a phone conversation, you can send a voicemail message without calling extension.

It is useful in a team work. When your partners are busy in a meeting or after work, but you have some information that need to share with them, you can send a voicemail message without calling them. It allows your partner to reflect prior to responding.

Prerequisites

This feature is only for internal extension users.

Procedure

1. To leave a voicemail message to a specific extension user, dial feature code (*12) followed by extension number (for example, *121001).
2. To leave a voicemail message to a queue, a ring group, or a custom group, dial feature code (*12) followed by group voicemail number (for example, *126100).
3. Follow the voice prompt to leave your message.
4. When done, hang up or press #.

Tip:

The default feature code for sending voicemail messages is *12. You can change, enable, or disable the code on PBX management portal: Call Features > Feature Code > Voicemail > Leave a Voicemail for Extension/Group Voicemail.

Forward Voicemail Messages to Email

Email is one of the most popular communication tools for business. Forwarding voicemail messages to email is an efficient business feature that allows employees to receive voicemail audio files as email attachments. This topic describes what you can do with voicemail to email and how to forward voicemail message to email for specific extension users.

Background information

Scenario

For employees who travel frequently and require an efficient way to keep up with voicemail and provide a quick response for the customers, it is an efficient way to get alert timely, listen to voicemails anywhere, and handle business over email.

Benefit

Each time the employees receive a voicemail message, they can receive an email with the new voicemail message attached as a .wav file, including caller ID, time of the call, and callback number.

- **Easy to identify:** In emails, the employees can quickly identify the person who left the message, and listen to voicemail message as they need.
- **Easy to listen:** The employees can check and listen to their voicemail messages via computer, smart phone or mobile device at convenience, instead of calling to voicemail box and navigating through the maze of voice prompts. They can also fast-forward or rewind to reach and repeat the important portion.
- **Easy to share:** The employees can forward emails to share voice messages with teammates to improve collaboration efficiency.
- **Easy to manage:** Managing the communications is easier since all the voicemail messages are in the email box. It is faster to sort, prioritize, scan, delete, and save voicemail message.

Prerequisites

- Make sure there is a valid email address assigned to each extension.
- Make sure the PBX [system email](#) works, or the PBX cannot forward the received voicemail to an extension user's email.

Procedure

1. Log in to PBX management portal, go to Extension and trunk > Extension, edit the desired extension.
2. Click Voicemail tab.
3. In the New Voicemail Notification drop-down list, select Send Email Notifications with Attachment.
4. In the After Notification drop-down list, set how to handle the voicemail message after the system has successfully notified the extension user by email.
5. Click Save and Apply.

Manage Voicemail Messages

Check Voicemail Messages

This topic describes how to check voicemail messages.

Background information

Methods

Extension users can get an [instant voicemail notification](#) when receiving a new voicemail message. There are multiple ways to check voicemail messages anytime and anywhere.

- On an IP phone

- On Linkus client
- Via Email
- Via IVR

Feature code

The default feature code for checking voicemail messages is *2. You can change, enable, or disable the code on PBX management portal: Call Features > Feature Code > Voicemail > Check Voicemail/Subscribe Voicemail Status.

Check voicemail messages on an IP phone

Check voicemail messages on a user's own phone

1. Dial feature code *2.
2. Follow the voice prompt to enter your PIN number followed by #.
3. Navigate through the [voicemail menu](#) to check your voicemail message.

Check voicemail messages from another phone

1. Dial feature code *2 followed by the extension number whose voicemail will be checked. (for example, to check voicemail of extension 1001, dial *21001).
2. Follow the voice prompt to enter your PIN number followed by #.
3. Navigate through the [voicemail menu](#) to check your voicemail message.

Check group voicemail messages from an IP phone

If the Mode of group voicemail is set to Shared by Members, the users can check the messages in group mailbox. If any users check the new messages, the status of messages will be set as read.

1. Dial feature code *2 followed by the group voicemail number (for example, *26100).
2. Navigate through the [voicemail menu](#) to check your voicemail message.

Check voicemail messages on Linkus client

If you have enabled Linkus Clients for extension users, the extension users can check voicemail messages on their Linkus clients.

Check voicemail messages via Email

If you have set up the feature of [forwarding voicemail messages to email](#) for extensions, the extension users can check their voicemail messages in their email boxes.

Check voicemail messages via IVR

If you have allowed extension users to [dial in an IVR to check voicemail messages](#), the extension users can also check voicemail messages when they are out of office.

1. Dial in an IVR, follow the voice prompt.
2. Dial feature code *2 followed by extension number or group voicemail number, and then enter the PIN number.
3. Navigate through the [voicemail menu](#) to check voicemail messages.

Enable or Disable Voicemail Transcription

Yeastar P-Series PBX System supports a Voicemail Transcription feature. Using this feature can transcribe voice messages to texts, users can view the message content directly, which brings great convenient and efficiency.

Enable Voicemail Transcription

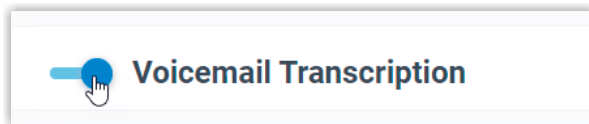
Prerequisites

Voicemail Transcription feature requires the use of a third-party transcription service to convert the voice message to text. Before you start to use Voicemail Transcription, make sure that the PBX is integrated with a third-party Speech-to-Text (STT) service.

For now, Yeastar P-Series PBX System allows you to integrate with Google Cloud STT API service. For more information, see [Integrate Yeastar P-Series PBX System with Google Cloud Speech-to-Text Service](#).

Procedure

1. Log in to PBX management portal, go to Call Features > Voicemail > Voicemail Settings.
2. Scroll down to the bottom of the page, turn on Voicemail Transcription.



3. Click Save.

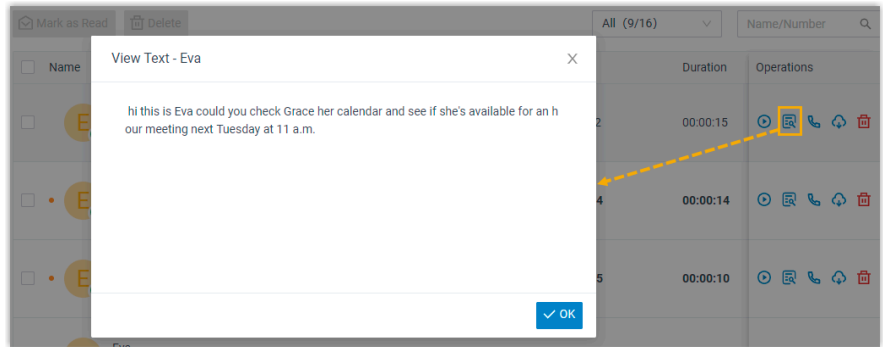
Result

The Voicemail Transcription feature is enabled, users can receive voicemails in the form of text on different platforms.

Linkus Web Client

Users can check the transcribed text for each voicemail on Linkus Web Client.

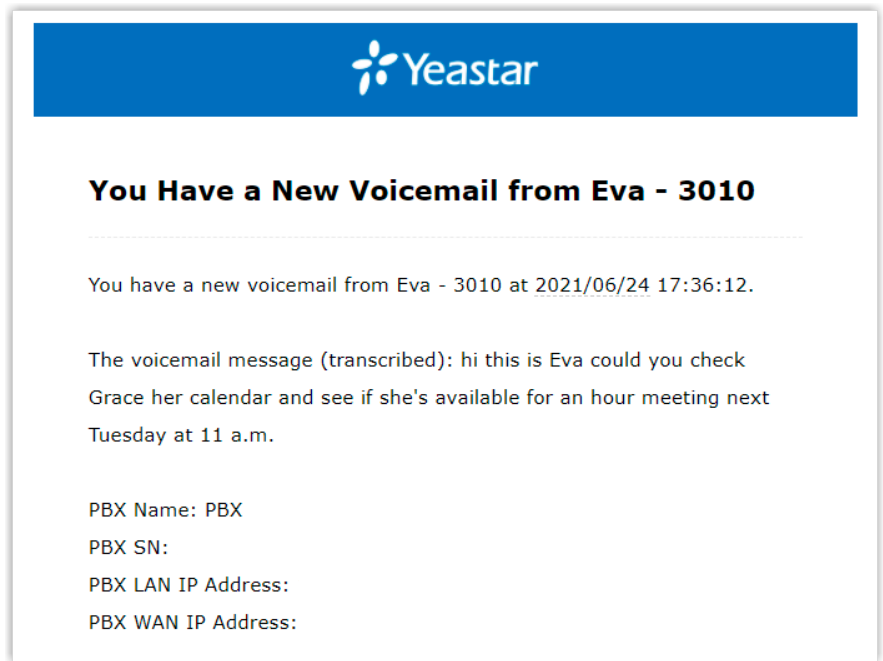
Note:
 Voicemail Transcription is NOT supported on Linkus Mobile Client but will be supported in the future.



Email Client

If [Voicemail to Email](#) feature is enabled, the transcribed text will be displayed in the email content for received voicemails.

The figure below shows an example of voicemail notification email.

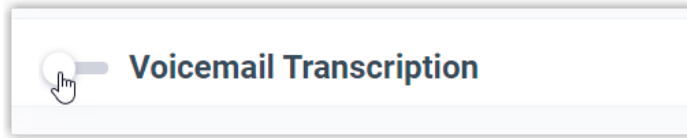


Disable Voicemail Transcription

Procedure

1. Log in to PBX management portal, go to Call Features > Voicemail > Voicemail Settings.

2. Scroll down to the bottom of the page, turn off Voicemail Transcription.



3. Click Save.

Result

The Voicemail Transcription feature is unavailable.

Configure Message Envelope

This topic describes how to enable or disable message envelope.

Background information

Message envelope is given before a voicemail message is played. Message envelope includes the following information:

- Date and Time that the message was received.
- Caller ID information.
- Duration of the message.

You can enable or disable envelope information separately according to user needs.

Configure message envelope for extension voicemail

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Voicemail tab.
3. Decide whether to enable the following information for the message envelope:
 - Play Date and Time: Play the date and time that the message was received.
 - Play Caller ID: Play the caller ID information.
 - Play Message Duration: Play the duration of message.
4. Click Save and Apply.

Configure message envelope for group voicemail

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail, edit the desired group voicemail.
2. In the Basic section, decide whether to enable the following information for the message envelope:
 - Play Date and Time: Play the date and time that the group voicemail message was received.

- Play Caller ID: Play the caller ID information.
 - Play Message Duration: Play the duration of group voicemail message.
3. Click Save and Apply.

Limit Voicemail Message Length

Limiting voicemail message length is a good way to reduce invalid or lengthy voicemails. This topic describes how to specify the message length (max and min) for a caller to leave a voicemail message.

Procedure

1. Log in to PBX management portal, go to Call Features > Voicemail > Voicemail Settings > Message Options.
2. In the Max Message Time(s) drop-down list, select a number of seconds.
Messages exceeding the maximum duration will be automatically cut off.
3. In the Min Message Time(s) drop-down list, select a number of seconds.
Messages less than the minimal duration will be automatically discarded.
4. Click Save and Apply.

Tip:

You may need to inform the callers in the greeting to keep their messages brief or under the maximum duration.

Set up a Storage Location for Voicemail Messages

The voicemail messages are stored in Yeastar P-Series PBX System by default, you can specify other storage locations for voicemail messages.

Prerequisites

Set up a [storage device](#).

Procedure

1. Log in to PBX management portal, go to System > Storage > Storage Locations.
2. In the Voicemail drop-down list, select a storage device.
3. Click Save and Apply.

Result


The voicemail messages are stored in the specified storage device.

Auto Cleanup Voicemail Messages

Clean up old messages to free up space for new voicemail messages. You can determine how many and how long that the system retains voicemail messages in a mailbox. The system automatically deletes the old voicemail messages when the threshold is reached. This topic describes how to set up auto cleanup of voicemail messages for each extension.

Procedure

1. Log in to PBX management portal, go to System > Storage > Auto Cleanup > Voicemail Auto Cleanup.
2. In the Max Number of Voicemail field, enter the maximum number of voicemail messages that should be retained for each mailbox.
3. In the Voicemail Preservation Days field, enter the maximum number of days that voicemail messages should be retained.

 Note:
The value 0 indicates no limit.

4. Click Save.

Result

If [Auto Clean up Reminder](#) is enabled, and the retained voicemail messages reach 90% of the threshold, the system sends you a notification email.


Voicemail Security

Change Voicemail Access PIN

This topic describes how to change voicemail access PIN for extension voicemail and group voicemail.

Background information

By default, the extension users need to enter the voicemail access PIN for authentication when checking their voicemail messages. The default voicemail access PIN is randomly generated.

 Note:
The PIN can be numerics only, and a minimum of 3 digits is required.

Change voicemail access PIN for extension voicemail

There are two ways to change voicemail access PIN:

- [On web interface](#)
- [Via voicemail mailbox](#)

Change extension voicemail access PIN on web interface

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Voicemail tab.
3. In the Voicemail Access PIN field, enter a PIN number.
4. Click Save and Apply.

Change extension voicemail access PIN via voicemail mailbox

1. Dial *2 to enter mailbox, enter the access PIN.
2. Press 4 to change the voicemail access PIN.
3. Follow the voice prompt, and enter the new PIN followed by # key.

The call ends automatically after saving the new PIN.

Change voicemail access PIN for group voicemail

There are two ways to change voicemail access PIN:

- [On web interface](#)
- [Via voicemail mailbox](#)

Change group voicemail access PIN on web interface

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail, edit the desired group voicemail.
2. In the Voicemail Access PIN field, enter a PIN number.
3. Click Save and Apply.

Change group voicemail access PIN via voicemail mailbox

1. Dial *2 followed by the group voicemail number to enter mailbox, enter the access PIN.
2. Press 4 to change the voicemail access PIN.
3. Follow the voice prompt, and enter the new PIN followed by # key.

The call ends automatically after saving the new PIN.

Enable or Disable Voicemail Access PIN

A voicemail access PIN is helpful to prevent unauthorized access. This topic describes how to enable or disable voicemail access PIN.

**Note:**

For security reasons, we recommend that you enable voicemail access PIN.

Enable or disable voicemail access PIN for extension voicemail

1. Log in to PBX management portal, go to Extension and Trunk > Extensions, edit the desired extension.
2. Click Voicemail tab.
3. To enable voicemail access PIN, select Enabled from the Voicemail PIN Authentication drop-down list.
4. To disable voicemail access PIN, select Disabled from the Voicemail PIN Authentication drop-down list.
5. Click Save and Apply.

Enable or disable voicemail access PIN for group voicemail

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail, edit the desired group voicemail.
2. To enable voicemail access PIN, select Enabled from the Voicemail PIN Authentication drop-down list.
3. To disable voicemail access PIN, select Disabled from the Voicemail PIN Authentication drop-down list.
4. Click Save and Apply.

Voicemail Greetings

Voicemail Greeting Overview

Voicemail greeting is a short message that is played before a caller records a message. Via the greeting, you can inform the callers your information, like when you will be available, other methods to contact you, or other options that the caller can use to receive assistance.

Greeting types

There are two types of voicemail greetings that you can set up for extension voicemail and group voicemail:

- **System Global Greeting:** A greeting that is applied to extension voicemail or group voicemail by default.
- **Custom Greeting:** A greeting that is personalized.

Personal greeting based on presence

For extension voicemail, extension users can choose how to play greetings in different presence:

- Default greeting: Play a greeting for any presence that doesn't have a personal greeting.
- Presence greetings: Play a personal greeting for each presence (available, away, do not disturb, lunch break, business trip, and off work).

For example, an extension user has different greetings for Lunch Break status and Away status.

- Lunch Break: "I'm currently on a lunch and unable to take your call".
- Away: "I'm currently away from my desk".

Record or Upload Voicemail Greetings

This topic describes how to record or upload voicemail greetings for extension voicemail or group voicemail.

Background information

The personalized greetings can delight the callers, and let them know why you're unavailable and how they can contact you.

Up to ten individual greetings are customizable for each voicemail. It is easy to customize greetings in two ways:

- Upload an audio file: Prepare an audio file.

Note:

The uploaded file should meet the [audio file requirements](#).

- Record a voicemail greeting from a phone: Place a call from system, the extension users can answer the call and record their voice as voicemail greetings.

Record or upload voicemail greetings for extension voicemail

The extension users may want to make their voicemails more personalized and professional depending on presence, you can set personalized voicemail greetings for each user.

Upload an extension voicemail greeting

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Voicemail tab.
3. In the Voicemail Greeting section, click Greeting Management.
4. In the pop-up window, click Upload.
5. Select an audio file to upload.

You can view and manage the greeting in Greeting Management.

Record an extension voicemail greeting from a phone

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Voicemail tab.
3. In Voicemail Greeting section, click Greeting Management.
4. In the pop-up window, click Record New Greeting tab.
5. In the Audio File Name field, enter a name to help you identify it.
6. In the Extension drop-down list, select an extension to record a greeting.
7. Click Save.

The system places a call to the selected extension.

8. Answer the call, and record greeting on the phone.

Press # key or hang up after recording greeting, you can view and manage the greeting in Greeting Management tab.

Record or upload voicemail greetings for a group voicemail

Upload a group voicemail greeting

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail, edit the desired group voicemail.
2. In the Group Voicemail Greeting section, click Greeting Management.
3. In the pop-up window, click Upload.
4. Select an audio file to upload.

You can view and manage the greeting in Greeting Management.

Record a group voicemail greeting from phone

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail, edit the desired group voicemail.
2. In Group Voicemail Greeting section, click Greeting Management.
3. In the pop-up window, click Record New Greeting tab.
4. In the Audio File Name field, enter a name to help you identify it.
5. In the Extension drop-down list, select an extension to record a greeting.
6. Click Save.

The system places a call to the selected extension.

7. Answer the call, and record greeting on the phone.



Press # key or hang up after recording greeting, you can view and manage the greeting in Greeting Management tab.

Manage Personal Voicemail Greetings


This topic describes how you can manage an extension user's personal greeting, including playing, downloading, and deleting greetings.

Play a personal greeting


To check the uploaded greetings or recorded greetings, you can play the greeting on a phone or on web.

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Voicemail tab.
3. In the Voicemail Greeting section, click Greeting Management.
4. Select a greeting that you want to play, click .
5. In the pop-up window, choose how to play the greeting:
 - Play on Web: Click  to play the greeting on the web directly.
 - Play to Extension: Play the greeting on a phone.
 - a. Select an extension, and click Play.
 - The system places a call to the extension.
 - Pick up the call to listen to the greeting on the phone.

Download a personal greeting

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Voicemail tab.
3. In the Voicemail Greeting section, click Greeting Management.
4. Select a greeting that you want to download, click .

Delete personal greetings



1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Voicemail tab.
3. In the Voicemail Greeting section, click Greeting Management.
4. To delete a greeting, do the following:
 - a. Click  beside the greeting.
 - b. Click OK and Apply.
5. To delete greetings in bulk, do the following:
 - a. Select the checkboxes of the greetings, click Delete.
 - b. Click OK and Apply.

Manage Group Voicemail Greetings

This topic describes how you can manage group voicemail greetings, including playing, downloading, and deleting greetings.


Play a group voicemail greeting

To check the uploaded greetings or recorded group voicemail greetings, you can play the greeting on a phone or on web.


1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail, edit the desired group voicemail.
2. In the Group Voicemail Greeting section, click Greeting Management.
3. Select a greeting that you want to play, click .
4. In the pop-up window, choose how to play the greeting:
 - Play on Web: Click  to play the greeting on the web directly.
 - Play to Extension: Play the greeting on a phone.
 - a. Select an extension, and click Play.

The system places a call to the extension.
 - b. Pick up the call to listen to the greeting on the phone.

Download group voicemail greeting

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail, edit the desired group voicemail.
2. In the Group Voicemail Greeting section, click Greeting Management.
3. Select a greeting that you want to download, click .

Delete group voicemail greetings

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail, edit the desired group voicemail.
2. In the Group Voicemail Greeting section, click Greeting Management.
3. To delete a greeting, do the following:
 - a. Click  beside the greeting.
 - b. Click OK and Apply.
4. To delete greetings in bulk, do the following:
 - a. Select the checkboxes of the greetings, click Delete.
 - b. Click OK and Apply.

Change Voicemail Greetings

Both the global and personalized voicemail greeting are changeable. This topic describes how to change voicemail greetings for extension voicemail and group voicemail.

Change global voicemail greetings for all voicemails

Prerequisites

[Upload a custom greeting](#) or [record a custom greeting](#).

Procedure

1. Log in to PBX management portal, go to Call Features > Voicemail > Voicemail Settings > Greeting Options.
2. In the Global Voicemail Greeting drop-down list, select an audio prompt.
3. Click Save and Apply.

Result

The global voicemail greeting will be applied to all the extension voicemails and group voicemails that do not have a custom greeting.

Change voicemail greetings for a specific extension

Prerequisites

[Record or upload voicemail greeting](#) for the specific extension.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Voicemail tab.
3. In the Voicemail Greeting section, select a greeting:
 - Default Greeting: Select a greeting from Default Greeting drop-down list.

Default greeting is played for the presence with Presence Greetings set to None.

 - Presence Greetings (Available, Away, Do Not Disturb, Lunch Break, Business Trip, and Off Work): Select a greeting from the corresponding presence drop-down list.

The presence greeting is played based on extension presence.



Tip:

You can also select Record New to add a new greeting and apply.

4. Click Save and Apply.

Change voicemail greetings for a group voicemail

Prerequisites

[Record or upload voicemail greeting](#) for the group voicemail.

Procedure

1. Log in to PBX management portal, go to Call Features > Voicemail > Group Voicemail, edit the desired group voicemail.
2. In the Group Voicemail Greeting section, select a greeting.



Tip:

You can also select Record New to add a new greeting and apply.

3. Click Save and Apply.

Voicemail Notifications

Voicemail Notification Overview

Extension users can get an instant notification when receiving a new voicemail message. This topic describes various ways to get notified of new voicemail messages.

Notification on IP phones

There are two methods that you can use to monitor voicemail status on an IP phone.

Monitor voicemail status by function keys

You can use a function key to monitor changes of voicemail status, including monitor your voicemails, other users' voicemails, or group voicemails. It is useful when sharing a single voicemail in a team. The team members can monitor and access the voicemail in time. Once someone reads or deletes the message, no one else should have to deal with it.

For more information, see [Monitor Voicemail Status on an IP Phone](#).

Monitor voicemail status by MWI

Message Waiting Indicator (MWI) is a commonly supported phone feature that alerts you when receiving a new voicemail message. MWI typically involves a flashing light and optional audio alert. This can differ from device to device.

Notification by email

You can set up email notification for extension users. When receiving a voicemail message, users can get alert timely, read the message at a glance to see the caller and when the message is left, and listen to voicemails. This improves work efficiency.

- For employees who do not use the phone frequently, they don't need to pay attention to keep checking voicemail on the phone at all time.
- For employees who travel frequently, they can process voice messages in real time and respond to customers promptly.

For more information, see [Set up Email Notifications for Voicemail](#).

Monitor Voicemail Status on an IP Phone

This topic describes how to monitor voicemail status on an IP phone by function keys.


Background information

For extension users who want to monitor voicemail status on their phones, you can set a function key for each extension user by [auto provisioning](#).

Note:

Users can also set function keys manually on their own IP phones. For more information, contact the phone manufacturer.

Procedure

1. Assign function keys for extension users to monitor voicemail status.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
 - If you want to assign function keys for a specific extension user, click  beside the desired extension.
 - If you want to assign function keys for multiple extensions, select the checkboxes of the desired extensions, and click Edit.
 - b. Click the Function Keys tab.
 - c. Configure function keys.


Note:

The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

- Type: Select the voicemail type that you want to monitor.
 - To monitor extension voicemail, select Check Voicemail.
 - To monitor group voicemail in shared mode, select Check Group Voicemail.

Note:

Monitor voicemail by function key is not applicable for group voicemail in broadcast mode, because the voicemail messages are not stored in the group mailbox.

- Value: Select an extension voicemail or group voicemail that you want to monitor.
 - Label: Optional. Enter a value, which will be displayed on the phone screen.
- d. Click Save.
2. If the extension hasn't be associated with a phone, see [Auto Provision IP Phones](#) to bind a phone with the extension.
 3. If the extension has been associated with a phone, reprovision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click  beside the phone assigned to this extension.

Result

The function key shows the real-time status of voicemail.

- Green: The monitored extension has no unread voicemail messages.
- Red: The monitored extension has unread voicemail messages.

To check the voicemail message, press the function key to access the voicemail box and operate following by the prompt instructions.

Note:

The key LED status may vary by phone models.

Set up Email Notifications for Voicemail

This topic describes how to set up email notifications for new voicemail messages.

Limitation

This feature is only for extensions' personal voicemails. New voicemail messages to Group Voicemail doesn't support email notifications.

Note:

The group voicemail in [broadcast mode](#) will forward messages to extensions' personal voicemails, the extension users can also receive email notifications.

Prerequisites

- Make sure there is a valid email address assigned to each extension user.
- Make sure the PBX [system email](#) works, or the PBX cannot send voicemail messages to an extension user's email.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Voicemail tab.
3. In the New Voicemail Notification drop-down list, select a voicemail notification method or disable email notification.
 - Do not Send Email Notifications: Disable email notification.
 - Send Email Notifications without Attachment: Send a notification email as soon as receiving a new voicemail message in mailbox.
 - Send Email Notifications with Attachment: Send a notification email with the new voicemail message attached as a .wav file.

Note:

If you use the default Voicemail to Email email template, the notification email contains the followings. To customize the email template, see [Customize Email Templates](#).

- Who left the message
 - The caller ID
 - When the message was left
 - The transcribed voicemail text (Need to [enable Voicemail Transcription](#) first)
 - The PBX device information
4. In the After Notification drop-down list, select a desired option from the drop-down list.
 - Do Nothing: Keep the voicemail messages in mailbox as unread.
 - Make as Read: Keep the voicemail messages in mailbox as read to prevent users from repeatedly receiving reminders on their phones.
 - Delete Voicemail: Delete the voicemail message to avoid mailbox being filled up.

Note:

We recommend that you select this option only when the extension user has received a notification email with voicemail message attachment.

5. Click Save and Apply.

Custom Voicemail Experience

Allow Callers to Press a Key to Leave Messages

This topic describes how to allow callers to press a key to leave messages.

Background information

By default, when the caller accesses a user's voicemail, PBX starts to record message automatically. It may make callers embarrassed when they are not ready to leave a message or they don't need to leave a message. Even if the caller hangs up directly, the voice mailbox still generates a lot of invalid information.

Procedure

1. Log in to PBX management portal, go to Call Features > Voicemail > Voicemail Greetings.
2. In the Caller Options section, select the checkbox of Ask callers to press 5 for leaving a message.
3. Click Save.

Result

The caller can choose whether to leave a message after listening to the greeting, and press 5 to leave a message after he or she is ready.

What to do next

If a custom greeting is used for voicemail, [update the greeting](#) that would instruct callers to press 5 for leaving a message.

Allow Callers to Dial Extension from Voicemail

This topic describes how to allow callers to dial extension from voicemail.

Background information

For the employees working in multiple places, they can record a greeting to prompt the caller to dial another extension to reach them. Instead of hanging up and calling again, you can allow the caller to dial extensions directly from voicemail.

It is also useful when the boss is unavailable to answer a call, instead of leaving a message in emergency, the caller can dial the secretary's extension, .

Procedure

1. Log in to PBX management portal, go to Call Features > Voicemail.
2. In the Caller Options section, select the checkbox of Allow callers to dial extension.
3. Select the extensions that can be dialed from the Available box to the Selected box.
4. Click Save and Apply.

Result

The caller can press * key to dial an extension.

What to do next

If a custom greeting is used for voicemail, [update the greeting](#) that would instruct callers to press * key for dialing an extension.

Allow Callers to Break out from Voicemail

This topic describes how to allow callers to break out from voicemail, and access the operator.

Background information

For technical support, doctor office or sales manager, they do need someone available in case of any emergencies after hours. When callers access the voicemail, it would be nice to allow the callers to press 0 to get to the operator directly in emergency. Otherwise, they have to hang up and redial.

Procedure

You can specify an IVR or an extension for answering such emergency calls.

1. Log in to PBX management portal, go to Call Features > Voicemail.
2. In the Caller Options section, select the checkbox of Allow callers to press 0 to break out from voicemail.
3. In the Destination drop-down list, select a destination.
 - IVR: Forward the call to an [IVR](#).
 - Extension: Forward the call to the specific extension.
4. Click Save and Apply.

What to do next

If a custom greeting is used for voicemail, [update the greeting](#) that would instruct callers to press 0 to break out from voicemail.

Allow Callers to Review Voicemail Messages

Callers can review their voicemail messages after recording. This is important for callers to confirm whether the message is appropriate. This topic describes how to allow callers to review voicemail messages.

Procedure

1. Log in to PBX management portal, go to Call Features > Voicemail.
2. In the Caller Options section, select the checkbox of Allow callers to review message.
3. Click Save and Apply.

Global Voicemail Settings

The topic describes the global voicemail message settings, including caller options, message options, and greeting options.

Caller options

Setting	Description
Allow callers to press 0 to break out from voicemail	Allow callers to press 0 to exit the voicemail, and reach a specific IVR or an extension.
Allow callers to dial extension	Allow callers to dial other extensions.
Allow callers to press 5 for leaving a message	Allow callers to press 5 to leave a voicemail message after greeting, instead of auto starting recording immediately.
Allow callers to review message	Allow callers to review his/her voicemail message after recording.

Message options

Settings	Description
Max Message Time(s)	Set the maximum duration of one voicemail message. The default maximum voicemail duration that callers can leave is 600 seconds (10 minutes).
Min Message Time(s)	Set the minimum duration of one voicemail message. The default minimum voicemail duration that callers must leave is 2 seconds.

Greeting Options

Settings	Description
Max Greeting Time(s)	Set the maximum greeting duration that is played to caller. The default maximum greeting duration is 60 seconds (1 minute).
Global Voicemail Greeting	Select the greeting that is applied to all extensions.

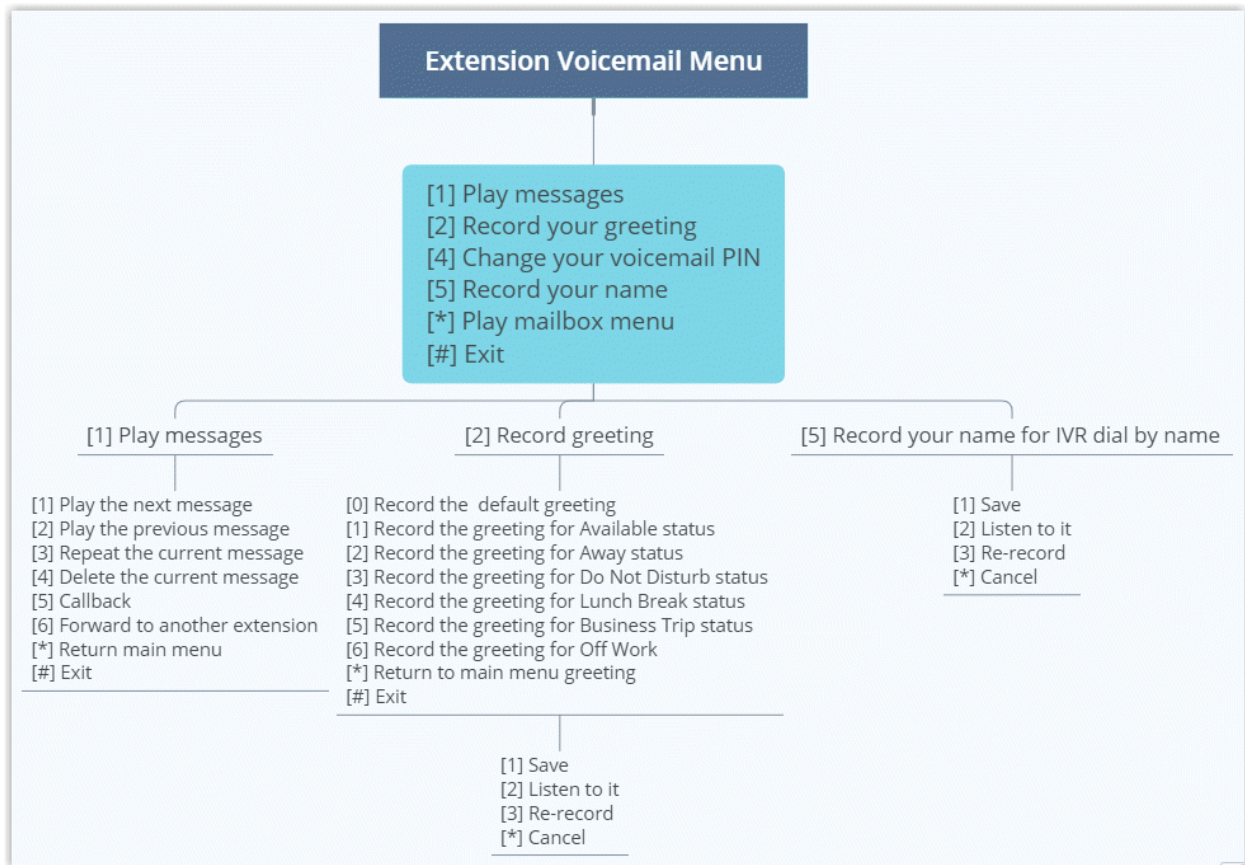
Voicemail Transcription

Decide to enable or disable Voicemail Transcription feature. For more information, see [Enable or Disable Voicemail Transcription](#).

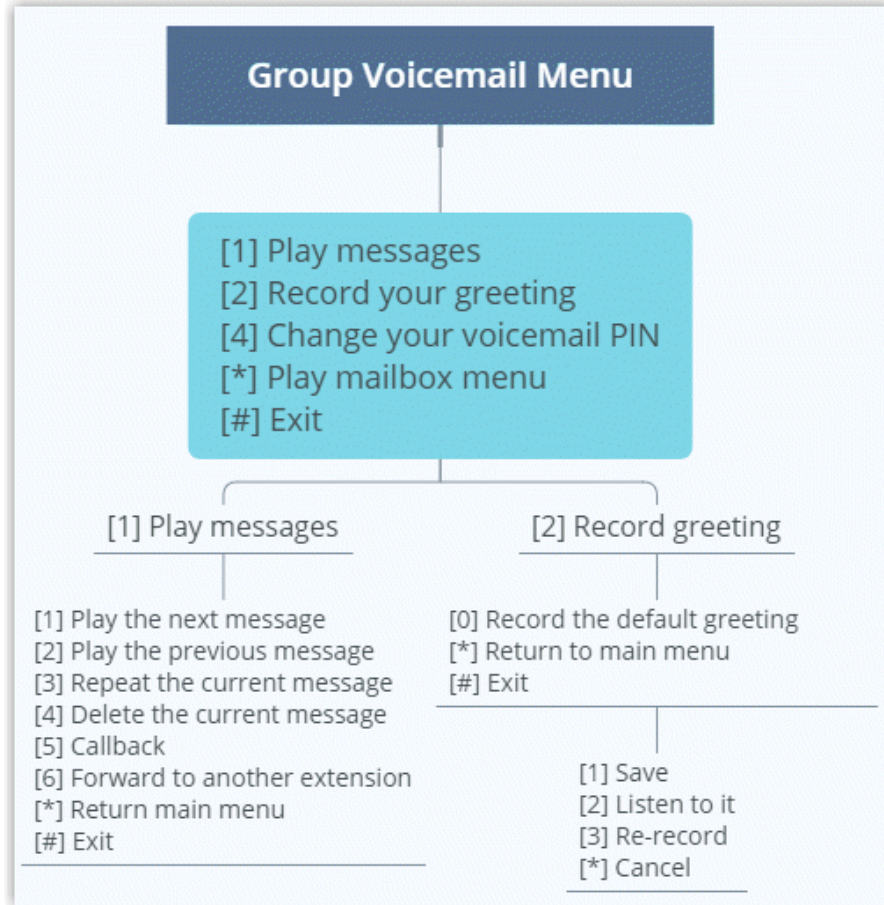
Voicemail Menu Options

This topic shows the quick reference of voicemail menu.

Extension voicemail menu



Group voicemail menu



Voicemail Capacity and Limitations

This topic describes the voicemail capacity and limitation for a voicemail.

Default capacity and limitations for each mailbox

Voicemail box capacity has a limit of 100 messages with maximum 10 minutes for each message. Once they hit that limit, the system auto deletes the old voicemail messages.

There is no limit of the time to keep the voicemail on PBX.

Adjust the capacity and limitations for each mailbox

- To adjust the capacity of voicemail box, see [Auto Cleanup Voicemail Messages](#).
- To adjust the limitation of maximum message time, see [Limit Voicemail Message Length](#).

IVR

Interactive Voice Response (IVR) Overview

Yeastar P-Series PBX System integrates a free IVR system. This topic describes what is IVR, what you can do with IVR, and what is multi-level IVR.

What is IVR?

Interactive Voice Response (IVR) is an automated telephony technology that interacts with callers, gathers information, and routes calls to the appropriate destinations. IVR can act as a virtual receptionist to handle large volumes of calls. It means that you don't need a dedicated person to redirect calls to appropriate departments. With IVR, customers can get quick response or access appropriate service on their own.

What you can do with IVR?

Yeastar IVR uses customizable voice prompts to provide callers with instructions and directions for accessing information via phone, such as "press 1 for sales, and press 2 to leave a message.". IVR connects callers to individuals, departments, call queues, etc, based on the customers' selections from voice menus.

Multi-level IVR is an alternative that allows you to assign a new IVR to an IVR option, and provides more powerful options to route incoming calls. Multi-level IVR gives you the flexibility to classify the menu of an interaction, such as divides a sales department into regions, and routes calls more precisely.

You can customize your IVR to provide a seamless experience.

For customer

- Play personal greeting to make the customer feel welcome.
- Allow customer to leave a voicemail.
- Allow customer to call employees directly by dialing extension or by name.

For employee

- Allow employees to make an outbound call via an IVR.
- Allow employees to check voicemail via an IVR.

IVR keypress events

There are three types of keypress events:

- Menu options: The number keys, # key and * key for users to access a desired destination.

- **Timeout:** If no input is detected after the configured timeout, the PBX will forward the call based on the configuration.
- **Invalid:** When an invalid key is pressed, route the call to a desired destination.

Keypress destination

The following options are available for you to assign to the keypress events:

- **Hang up:** End the current call.
- **Extension:** Route the call to the specified extension.
- **Extension Voicemail:** Allow callers to leave a message for the specified extension.
- **Group Voicemail:** Allow callers to leave a message for a queue, a ring group, or a custom group.
- **IVR:** Allow callers to enter another IVR menu.
- **Ring Group:** Route the call to a specified ring group.
- **Queue:** Route the call to a specified queue.
- **Dial by Name:** Allow callers to place a call by extension user's name.
For more information, see [Allow Callers to Dial by Name via IVR](#).
- **External Number:** Route the call to an external number.
- **Play Prompt and Exit:** Play a custom prompt, and then hang up the call.

Set up an IVR

Yeastar P-Series PBX System provides easy-to-create menus that allow you to set up an IVR and keep up with changing requirements. This topic describes how to set up an IVR.

Prerequisites

Before you set up an IVR, [record a custom prompt](#) or [upload a custom prompt](#) to provide callers with the IVR menu.

Procedure

1. Log in to PBX management portal, go to Call Features > IVR, click Add.
2. In the Basic tab, set the basic settings of IVR.

- **Number:** Specify a virtual number for callers to access the IVR.

The default [IVR number range](#) is from 6200 to 6299.

- **Name:** Enter an IVR name to help you identify it.
- **Prompt:** Set the IVR prompt that plays greeting and explains the IVR menu options to callers.

The default prompt is "Dial the extension number or press 0 for operator".

You can select up to 5 audio files, and the system plays the audio files in order.

- **Prompt Repeat Count:** Set how many times to play the prompt when the caller remains inactive during the Response Timeout(s).

- Response Timeout(s): Set how long (in seconds) to wait for the caller to operate.
- Digit Timeout(s): Set how long (in seconds) to wait for the caller to enter the next digit.
- IVR Alert Info: Optional. Set an "alert info text" to add to Alert-info header in INVITE request for IVR calls.

When receiving an IVR call, the phone will inspect "Alert-Info" header to determine which ring tone it should use for ringing.

- Dial Extensions: Whether to allow callers to dial specific extension numbers via IVR.
 - Disable: Disable to dial extensions via IVR.
 - All Extensions: Allow the callers to dial all the extension numbers.
 - Allowed Extensions: Select the extensions that the callers can dial.
 - Restricted Extensions: Select the extensions that the callers can NOT dial.
 - Dial Outbound Routes: Whether to allow callers to make outbound calls via IVR.
 - Dial to Check Voicemail: Whether to allow users to check voicemail via IVR.
3. Click the Key Press Event tab, set up an IVR menu.
 - a. In the Key Press drop-down list, select a key event for each key: 0-9, *, and #.
 - b. In the Response Timeout drop-down list, select a call routing destination if the caller remains inactive within the Prompt Repeat Count.
 - c. In the Invalid Input Destination drop-down list, select a call routing destination if the caller enters a digit that is not defined in the IVR.
 - d. Optional: Select the checkbox of Allow Opt-out of Call Recording.

When the call is routed to the key press destination, the call would not be recorded even [Call Recording](#) is enabled.
 4. Click Save and Apply.

What to do next

[Set up an inbound route](#), and specify the destination to the IVR.

Set up IVR Prompts

A custom greeting and prompt allow you to provide a more personalized experience for your customers. This topic describes how to set up IVR prompts according to your IVR menu.

IVR prompt types

Generally, an IVR prompt consists of several pieces of information:

- Welcome greeting: Welcome greeting is the first message that callers hear when they call in an IVR.

For example, "Thank you for calling Yeastar".
- Menu prompt: Present callers with a series of options.

For example, "If you got something urgent, please press 1 to contact our support. To leave a voicemail, please press 2".

- Goodbye greeting: Play the greeting before ending a call.

Prepare audio files for IVR prompt

The PBX system has a default IVR prompt. You can customize IVR prompt using a single audio file or multiple audio clips.

Customize IVR prompt by a single audio file

You can record greeting, IVR menu, or any messages in a single audio file. It is easy to manage and reduce the number of prompts.

Customize IVR prompt by multiple audio clips

Yeastar IVR also allows you to specify up to 5 different audio files as IVR prompt. The system plays the audio files in order when a customer calls in IVR.

It is better to divide your IVR prompt into multiple audio clips in the following scenarios:

- Modify the IVR prompt frequently.

Every time you modify the IVR menu, you need to update IVR prompt. Divide your IVR prompt into multiple audio clips according to the content, such as clip 1 for Welcome greeting, clip 2 for menu prompt, and so on. Next time, when you need to change the IVR prompt, just replace the specific clip.

- A single audio file exceeds the limit.

The uploaded file should meet the [audio file requirements](#). You can not upload an audio file larger than 8MB. Divide the audio file into multiple audio clips to solve this issue.

Update the IVR prompts

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > Custom Prompt, [upload a custom prompt](#) or [record a custom prompt](#).

Note:

The uploaded file should meet the [audio file requirements](#).

2. Go to Call Features > IVR, edit the desired IVR.
3. In the Prompt drop-down list, select your custom prompts.

You can select up to 5 audio files, and the system plays the audio files in order.

The screenshot shows the 'Key Press Event' configuration interface. The 'Number' field is set to 6200. The 'Name' field is also set to 6200. The 'Prompt' field is highlighted with a yellow box and contains a list of audio prompts: Greeting.wav, Press 1.wav, Press 2.wav, Press 3.wav, and Press star.wav. The 'Prompt Repeat Count' is set to 3. The 'Response Timeout' is set to 3. The 'Digit Timeout' is set to 3.

4. In the Prompt Repeat Count drop-down list, select prompt repeat times.
5. Click Save and Apply.

Allow Callers to Dial Extensions via IVR

This topic describes how to allow callers to dial extensions directly via an IVR.

Background information

For new customers, IVR can help them reach the desired employee or department. But for old customers, it is inconvenient for them to listen to audio prompts and make selections to reach the right employee or department, even they know the extension number.

For the callers who know the extension number, it is better to allow them to dial an extension number directly.

Prerequisites

Before you set up dial extension directly via an IVR, update your IVR prompt that would instruct callers to dial an extension number.

Procedure

1. Log in to PBX management portal, go to Call Features > IVR, edit the desired IVR.
2. In the Prompt drop-down list, select the updated IVR prompt.
3. In the Dial Extensions drop-down list, select which extension as available or available for callers to dial.
 - All Extensions: The callers can dial all the extensions.
 - Allow Extensions: The callers can dial the selected extensions.
 - Restricted Extensions: The callers can dial any extensions except the restricted extensions.
4. Click Save and Apply.

Allow Callers to Dial by Name via IVR

This topic describes how to allow customers to reach an employee just by typing his/her name in an IVR.

Background information

For the customers who don't remember the employee's extension number, you can allow them to call an employee by entering the first three letters of the first name or last name. For example, press 2-4-5 (B-I-L) to call "Bill Johnson".

It is easier for customers to get to the right person.

Add an option for Dial by Name

Prerequisites

Before you set up dial by name, perform the following tasks:

- Specify the first name or last name for employee's extension.
- [Updated your IVR prompt](#) that would instruct callers to dial by first name or last name.

Procedure

1. Log in to PBX management portal, go to Call Features > IVR, edit the desired IVR.
2. In the Prompt drop-down list, select the updated IVR prompt.
3. Click Key Press Event tab.
4. In the drop-down list of a key press, select Dial by Name.
5. Click Save and Apply.

Default announcement

Yeastar provides the default announcements when the caller selects the Dial by Name option. An announcement is played in the following scenarios:

Announcement	scenario
Welcome to the directory. Please enter the first three letters of your party's first name,using your touch tone keypad, use the 7 key for Q, and the 9 key for Z.	Play when the caller presses a key to dial by name.
No directory entries match your search.	Play when there is no matching directory entries after the caller enters three letters.
[Name] extension [Number] If this is the person you are looking for, press	Play when there are matching directory entries after the caller enters three letters.

Announcement	scenario
1 now, otherwise please press star now.	
There are no more compatible entries in the directory.	Play when there are no more compatible entries in the directory after the caller presses * key to search.

Allow Callers to Dial Outbound Calls via IVR

This topic describes how to allow callers to dial outbound calls in an IVR.

Background information

Dialing outbound calls via an IVR is useful when you interconnect two PBXs between headquarter and branch, and only set an IVR on headquarters PBX. You can allow the customers to dial the headquarter's extension number to contact the employees or departments in branch directly.

Prerequisites

- Set up the appropriate [outbound route](#) and [inbound route](#) on the two interconnected PBXs.
- [Upload or record IVR prompt](#) that would instruct customers to dial an outbound call.

Procedure

1. Log in to PBX management portal, go to Call Features > IVR, edit the desired IVR.
2. In the Prompt drop-down list, select the updated IVR prompt.
3. Select the checkbox of Dial Outbound Routes.
4. Select the desired outbound route from the Available box to the Selected box.
5. Click Save and Apply.

Forward Incoming Calls to an External Number via IVR

This topic describes how to allow callers to reach a specific external number in an IVR.

Background information

Forward Incoming Calls to an External Number with IVR is typical and important for 24x7 services, such as Doctor Answering Services and IT Support Services.

For Doctor Answering Services

When a patient calls in an hospital IVR, the patient can press a key to reach the external Doctor Answering Service to schedule an appointment or ask health questions and medical questions.

For IT Support Services

When your customers call in your office IVR after hours, you can give them an option to connect to an emergency support line. This emergency support line can be a Maintenance Engineer's mobile phone number.

Prerequisites

Before you allow callers to reach a specific external number in an IVR, [update your IVR prompt](#) that would instruct callers to press a key to reach the external number.

Procedure

1. Log in to PBX management portal, go to Call Features > IVR, edit the desired IVR.
2. In the Prompt drop-down list, select the updated IVR prompt.
3. Click Key Press Event tab.
4. Select a key to set key press event to External Number.
5. Optional: In the Prefix field, enter the [prefix of outbound route](#) so that PBX can successfully route incoming calls to external number.
 - If the Strip of outbound route is not set, you don't have to set the Prefix.
 - If the Strip of outbound route is set, you need to set the Prefix according to the Patterns of outbound route.
6. Enter the external number, such as a Doctor Answering Service number or a mobile phone number.
7. Click Save and Apply.

IVR Configuration Example

This topic shows the examples of single IVR configuration and multi-level IVR configuration.

A Single IVR Configuration

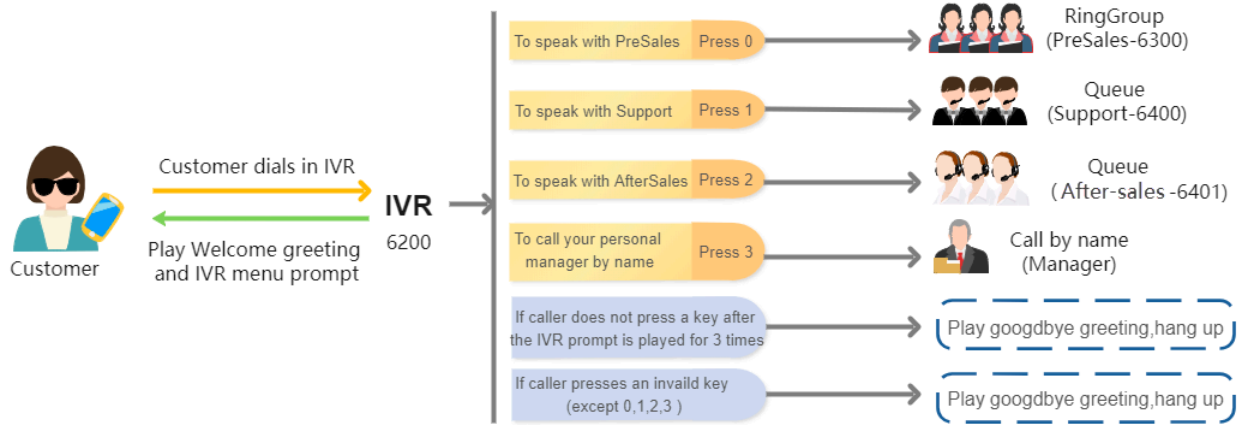
Background information

A company needs an IVR to redirect calls to Pre-sales, Support, After-sales, and personal manager.

We assume that all ring groups, call queues, audio prompts, and inbound routes used in this example are previously configured.

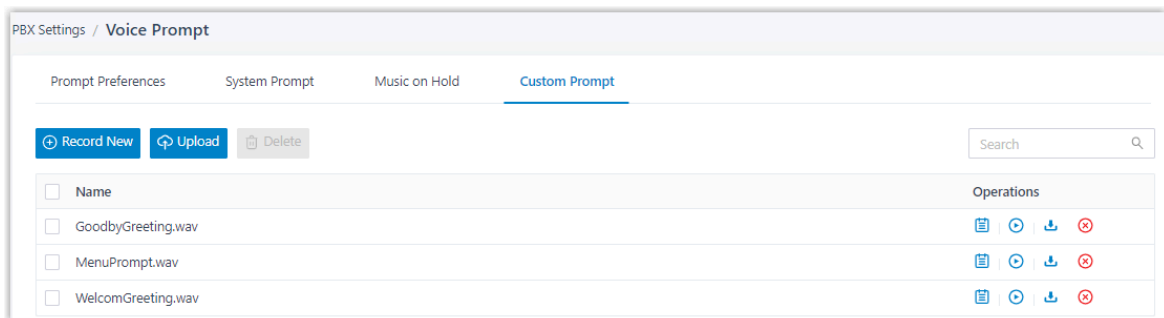
Step1. Design an IVR

When the customers dial in IVR (6200), they can access different service based on their business.



Step2. Upload IVR Prompts

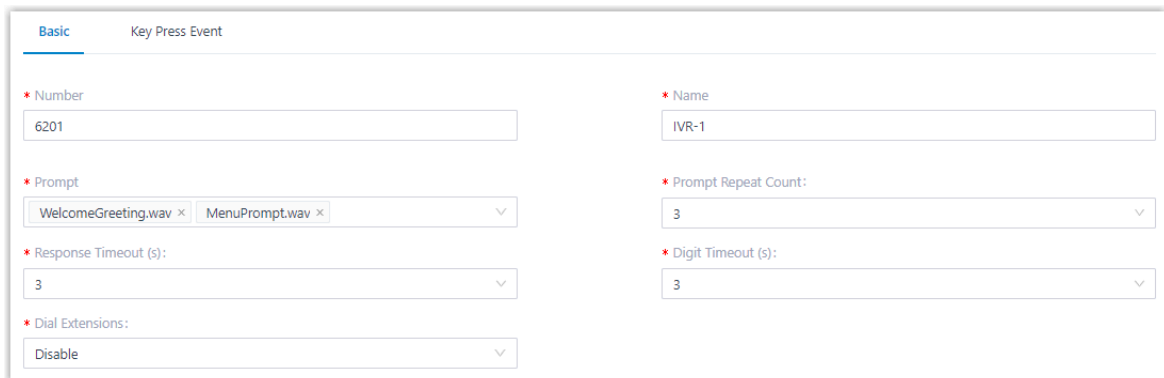
1. Go to PBX Settings > Voice Prompt > Custom Prompts, click Upload.
2. Select the audio files to upload.



3. Click Save and Apply.

Step3. Set up an IVR

1. Go to Call Features > IVR, click Add.
2. In the Basic tab, set the basic settings of IVR.



3. In the Key Press Event tab, set up an IVR menu.

Basic **Key Press Event**

Press 0 *
 Ring Group 6300 Opt out of being recorded

Press 1 *
 Queue 6400 Opt out of being recorded

Press 2 *
 Queue 6401 Opt out of being recorded

Press 3 *
 Extension 1007-Jason Liang Opt out of being recorded

Response Timeout * *
 Play Prompt and Exit GoodbyGreeting.wav 1

Invalid Input Destination * *
 Play Prompt and Exit GoodbyGreeting.wav 1

4. Click Save and Apply.

Multi-level IVR Configuration

Background information

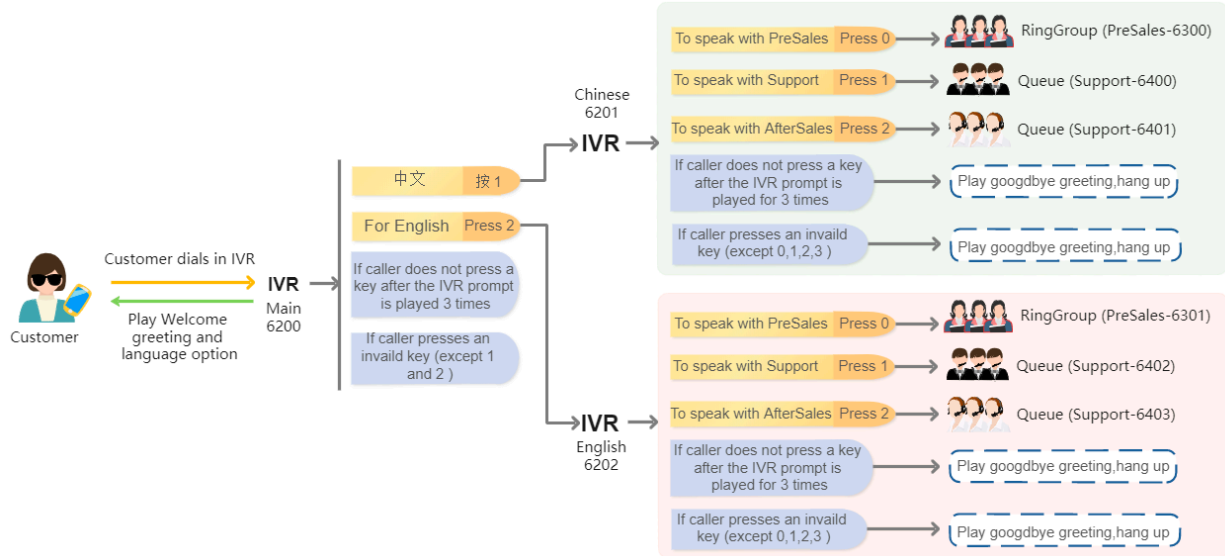
As business expands, the company needs to offer callers a bilingual auto-attendant feature based on their language selection. When the customer dials in to IVR, they can select a specific language to be used when playing prompts.

To achieve this, company needs to upgrade its IVR system allowing support of multi-language. We assume that all ring groups, call queues, extensions, audio prompts, and inbound routes used in this example are previously configured.

Step1. Design IVRs

When the customers dial in to IVR-Main (6200), they can select a specific language to use.

- If customers select Chinese, the call will be redirected to IVR-Chinese (6201).
- If customers select English, the call will be redirected to IVR-English (6202).



Step2. Set up IVRs

1. Set up the different IVRs with the same configuration for different language as shown in [a single IVR configuration](#).
 - IVR-1 (6201)
 - IVR-2 (6202)
2. Set up main IVR-Main (6200).
 - a. In the Basic tab, set the basic settings of IVR.

The screenshot shows the configuration for a Key Press Event in the 'Basic' tab. The fields are as follows:

- Number:** 6200
- Name:** Main
- Prompt:** WelcomeGreeting.wav, LanguagePrompt.wav
- Prompt Repeat Count:** 3
- Response Timeout (s):** 3
- Digit Timeout (s):** 3
- Dial Extensions:** 0

- b. In the Key Press Event tab, set up an IVR menu.
 - Specify IVR-Chinese (6201) for key 1.
 - Specify IVR-English (6202) for key 2.

3. Click Save and Apply.

The following figure displays the different IVRs created.

Number	Name	Dial Extensions	Dial Outbound Routes	Operations
6200	Main	Disable	No	Edit Delete
6201	Chinese	All Extensions	No	Edit Delete
6202	English	Disable	No	Edit Delete


Call Recording

Call Recording Overview

Call recording is valuable to keep important conversations, help train employees, evaluate their performance, and provide them with feedback. This topic describes how does call recording work, recording types, recording prompt, and recording management.

How does call recording work


The system records the conversation automatically when a call is established. During call recording, the user can pause and resume recording to avoid the sensitive information being recorded. After the call ends, the system converts the conversation into audio files (.wav) with a digital signature.

 **Note:**
The digital signature ensures a recording is not altered in any way.

Recording types

You can set up call recording for extensions, trunks, conferences, and queues respectively.

- **Extensions:** Record all the calls of the specified extensions, including the internal calls and external calls.

 **Note:**


Paging/Intercom call and voicemail on the specified extension would not be recorded.

- **Trunks:** Record all the calls on the specified trunks, including inbound calls and outbound calls.

For example, for employees who use a dedicated trunk to deal with customer issues, the system only records all the calls on this trunk.

- **Conferences:** Record the conversation of all members who join the specified conference rooms.
- **Queues:** Record the calls based on the specified queues.

For example, an agent logs in to two queues (Service and Support), and call recording is enabled for Service. The system can record all the calls from Service, but not record the calls from Support.

 **Note:**

The system automatically records a queue call or a conference call only when you activate recording for a queue or conference. For example, extension 1000 is an agent of a queue, you activate recording for extension 1000, but not activate recording for the queue. When extension 1000 answers a queue call, the call is not recorded.

Recording prompts

By default, the system does not play any prompts when a call is being recorded.

To ensure that recordings are lawful and callers have given their consent, you can customize recording prompt for internal calls, inbound calls, and outbound calls respectively. The system plays the recording prompt before call recording begins.

Recording management

- **For users:** The users can monitor call recording status on IP phones, pause and resume recording during a call.
- **For administrator:** The administrator can set up a storage location for recording files, manage the recording files, and grant permission to other users.

Set up Call Recording

This topic describes how to set up call recording for extensions, trunks, conferences, and queues.

Prerequisites

Only when the storage location for recording files is configured will the recording function take effect. For more information, see [manage storage locations](#).

Set up call recording for extensions

The system records the internal calls and external calls on the selected extensions.

1. Log in to PBX management portal, go to Call Features > Recording.
2. Optional: Select the checkbox of Enable Recording of Internal Calls to automatically record the internal calls.
3. In the Record Extensions section, select the desired extensions from the Available box to the Selected box.
4. Click Save and Apply.

Set up call recording for trunks

The system automatically records the external calls on the selected trunks.

1. Log in to PBX management portal, go to Call Features > Recording.
2. In the Record Trunks section, select the desired trunks from the Available box to the Selected box.
3. Click Save and Apply.

Set up call recording for conferences

The system automatically records the calls on the selected conferences.

1. Log in to PBX management portal, go to Call Features > Recording.
2. In the Record Conferences section, select the desired conferences from the Available box to the Selected box.
3. Click Save and Apply.

Set up call recording for queues

The system automatically records the calls on the selected queues.


1. Log in to PBX management portal, go to Call Features > Recording.
2. In the Record Queues section, select the desired queues from the Available box to the Selected box.
3. Click Save and Apply.

Set up Recording Prompts

This topic describes how to set up recording prompts for internal calls, inbound calls, and outbound calls respectively.

Set up recording prompt for internal calls

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > Custom Prompt, upload a custom prompt or record a custom prompt for internal calls.


 Note:

The uploaded file should meet the [audio file requirements](#).

2. Go to Call Features > Recording.
3. In the Internal Call Being Recorded Prompt drop-down list, select a prompt for internal calls.
4. Click Save and Apply.

Set up recording prompt for inbound calls

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > Custom Prompt, upload a custom prompt or record a custom prompt for inbound calls.


 Note:

The uploaded file should meet the [audio file requirements](#).

2. Go to Call Features > Recording.
3. In the Inbound Call Being Recorded Prompt drop-down list, select a prompt for inbound calls.
4. Click Save and Apply.

Set up recording prompt for outbound calls

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > Custom Prompt, upload a custom prompt or record a custom prompt for outbound calls.

 Note:

The uploaded file should meet the [audio file requirements](#).

2. Go to Call Features > Recording.
3. In the Outbound Call Being Recorded Prompt drop-down list, select a prompt for outbound calls.
4. Click Save and Apply.

Pause or Resume Call Recording

To avoid sensitive personal information such as credit card details being recorded, you can pause the recording by a feature code. This topic describes how to pause or resume recording.

Background information

The default feature code for pausing or resuming recording is *1. You can change, enable, or disable the code on PBX management portal: Call Features > Feature Code > Recording > Pause/Resume Recording.

Allow extension user to pause or resume call recording

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit a desired extension.
2. Click Features tab.
3. In the Call Recording section, select the checkbox of Allow the extension to stop or restart call recording during a call.
4. Click Save and Apply.

Result

During a call, do the following to pause or resume call recording:

- To pause call recording: Press the feature code (*1) to pause the call recording. When you play the recording files, the paused part is absent.
- To resume call recording: Press the feature code (*1) again to resume the call recording.

Monitor Call Recording Status on an IP phone

This topic describes how to set up a BLF key on an IP phone to monitor the call recording status.


Background information

For the users who want to know whether the call recording state is switched successfully or not, you can set a BLF key for each user by [auto provisioning](#).


Note:

Users can also set function keys on their own IP phones. For more information, contact the phone manufacturer.


Procedure

1. Assign function keys for extension users to monitor agent status.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
 - If you want to assign function keys for a specific extension user, click  beside the desired extension.

- If you want to assign function keys for multiple extensions, select the checkboxes of the desired extensions, and click Edit.
- b. Click the Function Keys tab.
 - c. Configure function keys.

 Note:


The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

- Type: Select BLF.
 - Value: Enter the code (*1) followed by extension number (for example *11000).
 - Label: Optional. Enter a value, which will be displayed on the phone screen.
- d. Click Save.
2. If the extension hasn't be associated with a phone, see [Auto Provision IP Phones](#) to bind a phone with the extension.
 3. If the extension has been associated with a phone, reprovision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click  beside the phone assigned to this extension.

Result

The BLF key shows the real-time status of call recording.

- Red: An active call of the monitored extension is being recorded.
- Green: An active call of the monitored extension is not in a call or the call recording is paused.
- Off: The BLF key does not subscribe the recording status of this extension. Check if your configurations are correct.

 Note:

The key LED status may vary by phone models.

Manage Call Recording Files

This topic describes how to manage call recording files, including searching, playing, downloading, or deleting the recording files.

Search recording files

You can search the recording files by time, caller number, callee number, or call ID.


1. Log in to PBX management portal, go to Reports and Recordings > Recording Files.
2. Set the search criteria.

- Time: Set the start date and the end date.

To specify a time period, click select time to set the start time and the end time.

- Call From: Set the caller's number or name.
- Call To: Set the callee's number or name.


 Tip:


To swap the callee for the caller, click .

- ID: Enter the unique identifier for the recording file.

The search results are displayed in the list.

Play recording files


1. Log in to PBX management portal, go to Reports and Recordings > Recording Files.
2. Click  beside the recording to which you want to listen.

- Play on Web: Click  to play the call recording on the web directly.
- Play to Extension: Play the call recording on the phone.
 - a. Select an extension, and click Play.


The system places a call to the extension.

- b. Pick up the call to listen to the call recording on the phone.


Download recording files

 Note:

You can download a maximum of 600MB recording files or a maximum of 100 recording files at a time. The recordings that exceed the limit will not be downloaded.

1. Log in to PBX management portal, go to Reports and Recordings > Recording Files.
2. To download a recording file, click  beside a recording log.
3. To download multiple recording files, do the following:
 - a. Select the checkboxes of recording files that you want to download.
 - b. Click Download Recording(s).

Delete recording files

1. Log in to PBX management portal, go to Reports and Recordings > Recording Files.
2. Delete a recording file, or delete recording files in bulk.
 - Delete a recording: Select the recording file that you want to delete, click  and OK.

- Delete recordings in bulk: Select the checkboxes of the recording files that you want to delete, click Delete and OK.

Auto Clean up Recording Files

Clean up old recording files to free up space. This topic describes how to set up auto cleanup of recording files.

Background information

By default, when the storage device reaches 80% of its [maximum storage capacity](#), the PBX automatically deletes the oldest recording files.

Procedure

1. Log in to PBX management portal, go to System > Storage > Auto Cleanup > Recording Auto Cleanup.
2. In the Max Usage of Device (%) drop-down list, select the maximum storage percentage of the device that is allowed to store recording files.
3. In the Recordings Preservation Days, enter the maximum number of days that the recording files should be retained.

The value 0 indicates no limit.

4. Click Save and Apply.

Note:

If [Auto Clean up Reminder](#) is enabled, and the retained recording files reach 90% of threshold, the system sends you a notification email. If the old recording files have continuing retention value, you can backup recording files or expand the retain limit in time.

Grant Manage Permission of Recording Files

By default, only the super administrator has permission to manage the call recording files. This topic describes how to grant manage permission to extension users.

Background information

As a super administrator, you can grant manage permission to a role, and assign the role to extension users. When the user logs in to the web client, he/she can manage recording files.

Procedure

1. Set up a user role.
 - a. Log in to PBX management portal, go to Extension and Trunk > Role, edit a role.
 - b. In the Reports and Recordings section, specify the manageable extensions and accessible permissions of recordings files for the role.

- **Manage Extensions:** Specify the manageable extension range.
 - **Recording Files Operation Permission:** Specify the accessible permission, including Play, Download, and Delete.
- c. click Save.
2. Assign a role to a user.
 - a. Go to Extension, edit the extension to which you want to grant recording permission.
 - b. In the User Information section, select the role from the User Role drop-down list.
 - c. Click Save and Apply.

Restrict Users from Viewing Recording Files

By default, all the users have access to viewing their own recording files. For security reasons, you can restrict specific users from view recording files.

Requirements and restrictions

Requirements

The version of PBX server must be 37.4.0.17 or later.

Restrictions

The feature works for Linkus Web Client and Linkus Mobile Client:

- Linkus Web Client: Version 37.4.0.17 or later.
- Linkus iOS Client: Version 4.3.8 or later.
- Linkus Android Client: Version 4.3.11 or later.

Procedure

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit a desired extension.
2. Click Features tab.
3. In the Call Recording section, unselect the checkbox of Allow the extension to view recordings.
4. Click Save.

Result

The extension user can not view recording files on Linkus Web Client and Linkus Mobile Client.

Ring Group

Ring Group Overview

Ring group is a feature to share the distribution of incoming calls among employees. This topic describes what is ring group, ring strategy, and failover destination.

What is ring group

Ring group allows you to merge multiple extension numbers into a virtual number. The customers can dial the virtual number, and the calls ring through all the members to make sure that no call goes unanswered. It is often used to efficiently distribute calls to specific departments such as Sales, Support, and Accounting.

Ring strategy

Ring group can ring members in two ways:

- Ring all simultaneously: When receiving an incoming call, the system rings all the available members at the same time and stops ringing when any member in the group picks up the call. If no one answers the call within the ring time, the system routes the call to the failover destination.

You can set this option for teams such as Support or Customer Service, where all members are equally responsible for answering incoming calls.

- Ring sequentially: When receiving an incoming call, the system rings the first available member in the list firstly. If no answer within the ring time, the system rings the next available member until the last one. If no one answers the call, the system routes the call to the failover destination.

You can set this option for receptionist who holds the primary responsibility for answering the phone while other individuals acting as backups.

Failover destination

When a call comes in to the ring group, and no one is available to answer the call, you can end the call or route the call to the following destinations:

- Hang Up
- Extension
- Extension Voicemail
- Group Voicemail
- IVR
- Ring Group
- Queue
- External Number
- Play Prompt and Exit

Create a Ring Group

This topic describes how to create a ring group.

Procedure

1. Log in to PBX management portal, go to Call Features > Ring Group, click Add.
2. Configure the ring group.
 - Number: Enter a virtual number for callers to access the group.

The default ring group [number range](#) is from 6300 to 6399.
 - Name: Enter a group name to help you identify it.
 - Ring Strategy: Select a ring method to distribute calls to members.
 - Ring All: Ring all available extensions simultaneously.
 - Ring Sequentially: Ring all available extensions sequentially.
 - Ring Group Alert Info: Optional. Set an "alert info text" to add to Alert-info header in INVITE request for ring group calls.

When receiving a ring group call, the phone will inspect "Alert-Info" header to determine which ring tone it should use for ringing.
 - Ring Timeout (s): Set a number of seconds that the system waits before ringing next member or routing the call to Failover Destination.
 - Members: Select the desired extensions from the Available box to the Selected box.
 - Failover Destination: Select a destination to route the call when no member answers the call within ring time.
 - Hang up: End the current call.
 - Extension: Route the call to the specified extension.
 - Extension Voicemail: Route the call to voicemail box of the specified extension.
 - Group Voicemail: Route the call to voicemail box of a queue, a ring group, or a custom group.
 - IVR: Route the call to the specified IVR.
 - Ring Group: Route the call to another ring group.
 - Queue: Route the call to the specified queue.
 - External Number: Route the call to an external number.
 - Play Prompt and Exit: Play a custom prompt, and then hang up the call.
3. Click Save and Apply.

What to do next


[Set up an inbound route](#), and specify the destination to the queue.

Manage Ring Groups


This topic describes how to edit a ring group, and delete ring groups.

Edit a ring group

You can edit the group settings, including adding or removing a member, or change the ring strategy.

1. Log in to PBX management portal, go to Call Features > Ring Group.
2. Click  beside the ring group that you want to edit.
3. Change the ring group settings according to your needs.
4. Click Save and Apply.

Delete ring groups

1. Log in to PBX management portal, go to Call Features > Ring Group.
2. To delete a ring group, click  beside the ring group that you want to delete.
3. To delete ring groups in bulk, select the checkboxes of the ring groups that you want to delete, click Delete.
4. Click OK and Apply.

Call Queue

Call Queue Overview

Call queue is a method of handling large calls and provides callers with engaging holding experiences. This topic describes what is call queue, queue compositions, queue preference, and call center service.

What is call queue

A queue is like a virtual waiting room, in which callers wait in line to talk with the available agent. When the customer calls in PBX and reaches the queue, he/she can hear the hold music and announcement while the queue distributing the call to the available agents.

Queue components

A queue call consists of the following parts:

- Callers: Customers who place calls to the queue.
- Agents: Members who answer the queue calls (extensions or users that log in as agents)
 - Static agent: The agent is always a member of the queue and cannot log out.
 - Dynamic agent: The agent can log in to or log out of a queue at any time.
- Announcement: Announcements played to callers and agents, including agent ID announcement, position announcement, and periodic announcement.
- Music on Hold: Music or advertisements played to callers while waiting in the queue.

- Ring Strategy: A strategy for how to distribute calls to agents.
- Failover destination: A destination to which calls will be routed in the following scenarios.
 - The number of callers that wait in a queue reaches the Maximum Callers In Queue.
 - The time that callers wait reaches the Maximum Waiting Time.
 - No agents in queue and the caller is pulled out of a queue.

Call Center service

Call Center service is an additional service that drives faster call resolution and real-time call center monitoring, reporting, and management. It provides a powerful call center console, including a customizable Wallboard for proactive tracking of 16 key performance metrics, and a switchboard-type Queue Panel for real-time monitoring & control of queue activities, insightful call center reports, SLA and more.

For more information on call center service, see [Call Center Console User Guide](#).



Note:

For call center service, contact Yeastar support.

Queue preference

Queue preference settings are available, including queue capacity, service level agreement, announcement, and satisfaction survey.

- Queue capacity
 - Define the maximum number of calls to wait in the queue.
 - Whether to pull the caller out of queue when no agents available in the queue.
 - Whether to allow the caller to join when no agents in the queue.
- Service Level Agreement (SLA)

With call center service activated, you can use SLA to define a certain level of service in a call center scenario, such as answering 80% of calls within 20 seconds.

- Announcement
 - Caller announcement, including the agent ID announcement and position announcement.
 - Periodic announcement

- Satisfaction survey

In a call center scenario, you can make a satisfaction survey to collect customer feedback.

Create a Queue

You can create and design queues to allow callers to talk with agents according to your business. This topic describes how to create a queue.

Prerequisites

- Customize a [voice prompt](#) as agent announcement.
- Configure the [Music on Hold](#) for the queue.


Procedure

1. Log in to PBX management portal, go to Call Features > Queue, click Add.
2. In the Basic page, configure the basic settings for the queue and agent settings.
 - a. In the Basic section, configure the following settings:
 - Number: Enter a virtual number for callers to access the queue.
The default queue [number range](#) is from 6400 to 6499.
 - Name: Enter a queue name to help you identify it.
 - Ring Strategy: Select a ring method to distribute calls to agents.
 - Ring All: Ring all available agents simultaneously until someone answers.
 - Least Recent: Ring the available agent that was least recently called.
 - Fewest Calls: Ring the available agent with the fewest completed calls.
 - Random: Ring the agents randomly.
 - Rrmemory: Round robin with memory.
The system remembers the last agent it tried and rings the next agent.
 - Linear: Rings agents in the order specified in the agents list.
 - Music On Hold: Select a prompt to play to callers waiting for an available agent.
 - Maximum Waiting Time(s): Set a number of seconds that the caller can wait for an available agent.
 - Failover Destination: Select a destination to route the call when the call is not answered by any agent.
 - Hang up: End the current call.
 - Extension: Route the call to the specified extension.
 - Extension Voicemail: Route the call to voicemail box of the specified extension.
 - Group Voicemail: Route the call to voicemail box of a queue, a ring group, or a custom group.
 - IVR: Route the call to the specified IVR.
 - Ring Group: Route the call to another ring group.
 - Queue: Route the call to the specified queue.
 - External Number: Route the call to an external number.
 - Play Prompt and Exit: Play a custom prompt, and then hang up the call.
 - b. In the Agent Options section, configure the following settings.
 - Agent Timeout(s): Set a number of seconds that the system rings an agent's phone.

- **Retry Interval(s):** Set a number of seconds to wait before trying all the agents again.
- **Wrap-up Time(s):** Set a number of seconds for agents to complete post-call processing after finishing a call.


The next call will come after this period following the ring strategy.

- **Agent Announcement:** Select a prompt to play to agent prior to bridging in the caller.
 - **Ring In Use:** Set whether to distribute additional queue calls to the agents who are already in calls.
3. Click the **Members** tab, set agents for the queue.
 - **Dynamic Agents:** Select the dynamic agents that can log in to or log out of a queue at any time.

 **Note:**

The queue distributes calls to the dynamic agents only when they log in to the queue and unpause the queue calls.

- **Static Agents:** Select the static agents that are always stay in the queue.

 **Note:**

Static agents do not need to “log in” to the queue, and cannot “log out” of the queue.

4. Click **Preferences** tab to customize the queue according to your needs.

For more information of the preference settings, see [Queue Preferences](#).

5. Click **Save and Apply**.

What to do next


[Set up an inbound route](#), and specify a destination to the queue.

Manage Call Queues


You can not change the queue number after setting up a queue. This topic describes how to edit a queue, and delete queues.

Edit a queue

You can manage the agents, change the ring strategy, or other queue settings.

1. Log in to PBX management portal, go to **Call Features > Queue**.
2. Click  beside the queue that you want to edit.
3. Change the queue settings according to your needs.
4. Click **Save and Apply**.

Delete queues

1. Log in to PBX management portal, go to Call Features > Queue.
2. To delete a queue, do the followings:
 - a. Click  beside the queue that you want to delete.
 - b. Click OK and Apply.
3. To delete queues in bulk, do the followings:
 - a. Select the checkboxes of the queues that you want to delete, click Delete.
 - b. Click OK and Apply.

Manage Agent Status by Dialing a Feature Code

This topic describes how to manage agent status by dialing a feature code.

Background information

The PBX defines feature codes that allow the agents to switch their status. You can change, enable, or disable the feature code on PBX management portal: Call Features > Feature Code > Queue.

The default feature codes for switching agent:

- Log in/Log out: *7
- Pause/Unpause: *07

Log in to a queue

Only dynamic agents can log in to a queue; static agents are always in the queue.

For example, a dynamic agent dials *76400 to log in to queue 6400.

Log out of a queue

Only dynamic agents can log out of a queue; static agents are always in the queue.

For example, a dynamic agent 1000 dials *76400 to log out of queue 6400.

Pause receiving queue calls

Both static agents and dynamic agents can pause the queue calls when they are away from desk. The system will not distribute queue calls to the agents in "Paused" status.

For example, an agent 1000 dials *076400 to pause calls from queue 6400.

Unpause receiving queue calls

Both static agents and dynamic agents can unpause queue calls when they are ready to take calls.

For example, an agent 1000 dials *076400 to unpause calls from queue 6400.

Related information

[Monitor and Switch Agent Status on an IP Phone](#)

Monitor and Switch Agent Status on an IP Phone

This topic describes how to set up function keys on agents' phones to monitor and switch agent status.

Background information

There are two ways to monitor and switch agent status:

- **Function key:** For agents who want to monitor their own status in a specific queue on their phones, you can set a function key for each agent by [auto provisioning](#).

Note:

Agents can also set function keys on their own IP phones. For more information, contact the phone manufacturer.

- **Queue Panel:** If you have activated Call Center service, agents can monitor and switch their status on queue panel. For more information, see [Call Center Console User Guide](#).

Procedure

Assume that an agent Sunny wants to monitor and switch her status in the "Support" queue on IP phone.

You can set two function keys for the agent Sunny as follows:

1. Assign function keys for the agent.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the agent's extension.
 - b. Click the Function Keys tab.

Note:

Function Key feature is only supported on SIP extensions.

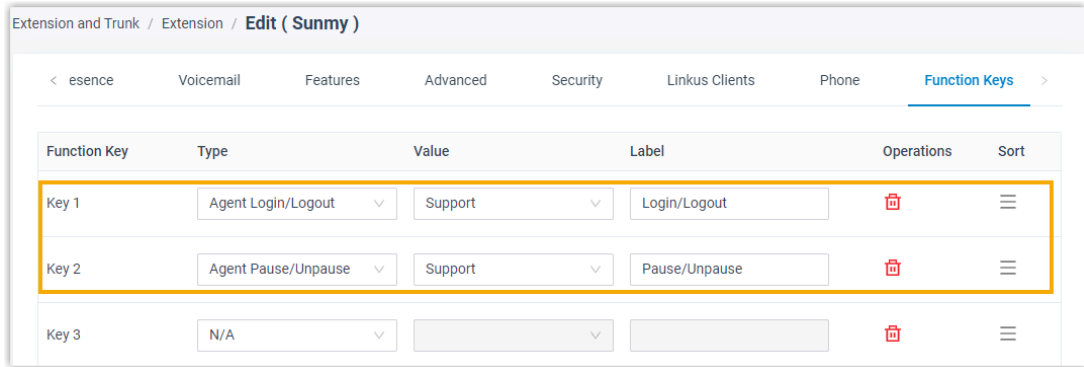
- c. Configure function keys.


Note:

The number of programmable keys varies by phone models. If the number of function keys you assign to an agent exceeds the number of programmable keys, the redundant function keys cannot take effect.

- **Type:** Select a key type.
 - Select Agent Login/Logout for logging in to or logging out of a queue.


- Select Agent Pause/Unpause for pausing or unpausing receiving queue calls.
 - Value: Select the "Support" queue that the agent sits in.
 - Label: Optional. Enter a value, which will be displayed on the phone screen.
- d. Click Save.



2. If the agent hasn't be associated with a phone, see [Auto Provision IP Phones](#) to bind a phone with the agent.
3. If the agent has been associated with a phone, reprovision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click  beside the phone assigned to the agent.

Result

The LED status of function keys shows the agent's status in real time.

 **Note:**
The key LED status may vary by phone models.

Function key	LED status	Description
Log in/Log out	Green	The monitored agent has logged in to the queue and unpaused queue calls. The agent can press the Log in/Log out function key to log out of the queue.
	Red	The monitored agent has logged out of the queue. The agent can press the Log in/Log out function key to log in to the queue.
	Off	The function key does not subscribe the agent's status. Check if your configurations are correct or if the agent's extension is registered.

Function key	LED status	Description
Pause/un-pause	Green	The monitored agent has logged in to the queue and un-paused queue calls. The agent can press the Pause/Unpause function key to pause receiving queue calls.
	Flashing Red	The monitored agent has paused receiving queue calls. The agent can press the Pause/Unpause function key to resume receiving queue calls.
	Off	The function key does not subscribe the agent's status. Check if your configurations are correct or if the agent's extension is registered.


Queue Preferences

This topic describes the queue preference settings, including distinctive ring tone, queue capacity, service level agreement, announcement, and satisfaction survey.

Distinctive ring tone

Setting	Description
Queue Alert Info	Set an "alert info text" to add to Alert-info header in INVITE request for queue calls. When receiving a queue call, the phone will inspect "Alert-Info" header to determine which ring tone it should use for ringing.

Queue capacity

Setting	Description
Maximum Callers in Queue	The maximum number of callers that can wait in the queue. The default value is 0 (unlimited). <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: When the number of callers waiting in queue reaches the Maximum Callers In Queue, the system routes the additional calls to Failover Destination.</p> </div>

Setting	Description
Leave Empty	Pull the caller out of a queue when no agent is in the queue, and forward the call to the Failover Destination.
Join Empty	Allow callers to join a queue when there is no agent in the queue.

Service level agreement

Setting	Description
SLA Time(s)	The maximum amount of time (in seconds) that an agent needs to answer an incoming call. The default SLA time is 60 seconds.
Evaluation Interval(min)	The time interval to compare the queue's SLA performance against the alarm threshold so the system can send a notification email accordingly.
Alarm Threshold(%)	The service level threshold for the queue. The default alarm threshold is 80%.

Announcement

Setting	Description
Announcement	
Join Announcement	The announcement played to callers before they join the queue.
Agent ID Announcement	The announcement played to callers to prompt the agent ID. <ul style="list-style-type: none"> • Default: The system plays the prompt "{extension_number} will be connected. Please wait". • Custom prompt: If you choose your custom prompt, the system will play {extension_number} + your custom prompt.
Call Position Announcement	
Announce Position	Announce position of caller in the queue.
Announce Hold Time	Announce the hold time to the caller periodically based on Frequency.

Setting	Description
Frequency(s)	The time interval to announce queue position and estimated hold time to the caller.
Queue Announcements	
Prompt	The announcement played to callers periodically.
Frequency(s)	The time interval to play the announcements.

Satisfaction survey

Setting	Description
Satisfaction Survey Prompt	<p>The prompt played to caller to ask the caller to rate their satisfaction scale after the agent hangs up.</p> <p>The default prompt is "Please rate your satisfaction with our service, press 1 for satisfied, press 2 for dissatisfied. Thank you.". "Thanks for your calling, goodbye." is prompted after the caller presses a key.</p>

Key Press Event

Setting	Description
Key	<p>The caller can press the key to enter the specific destination when waiting in queue.</p> <p>Generally, set a Periodic Announcements to guide the callers to press the key.</p>
Key Destination	<p>The destination to route the call when the caller presses a key.</p> <ul style="list-style-type: none"> • Hang up: End the current call. • Extension: Route the call to the specified extension. • Extension Voicemail: Route the call to voicemail box of the specified extension. • Group Voicemail: Route the call to group voicemail box of a queue, a ring group, or a custom group. • IVR: Route the call to the specified IVR. • Ring Group: Route the call to another ring group.

Setting	Description
	<ul style="list-style-type: none"> • Queue: Route the call to the specified ring group. • External Number: Route the call to an external number. • Play Prompt and Exit: Play a custom prompt, and then hang up the call.

Feature Code

Configure Feature Codes

Feature codes are a set of digits that the extension user can dial to activate a specific feature. This topic describes how to configure feature codes.

Background information

Yeastar P-Series PBX System provides various feature codes for users to activate or deactivate a specific feature. You can change, enable, or disable the code, and change the digit timeout for entering the feature code.

For more information on feature code, see [Feature Code Reference](#).

Procedure

1. Log in to PBX management portal, go to Call Features > Feature Code.
2. In the Feature Code Digit Timeout (ms) field, enter a number of seconds for inputting next digit.

The digit timeout is the time between consecutive key presses on the phone's keypad.

3. Decide whether to enable or disable a feature code.
 - Enable a feature code: Select the checkbox of the specific feature code.
 - Disable a feature code: Unselect the checkbox of the specific feature code.
4. Optional: Change the code according to your needs.
5. Click Save and Apply.

Feature Code Reference

This topic describes the list of default feature codes.

Recording

Name	Default Code	Usage
Pause/Resume Recording	*1	Press *1 during a call to pause recording; Press *1 again to resume recording.

Voicemail

Name	Default code	Usage
Check Voice-mail/Subscribe Voicemail Status	*2	<ul style="list-style-type: none"> To check the voicemail of extension 1000, dial *21000. To check the group voicemail of queue 6400, dial *26400.
Leave a Voicemail for Extension/Group Voicemail	*12	<ul style="list-style-type: none"> To leave a voicemail message for extension 1000, dial *121000. To leave a voicemail message for queue 6400, dial *126400.

Call Transfer

Name	Default code	Usage
Attended Transfer	*3	Press *31000 to attended transfer a call to extension 1000.
Blind Transfer	*03	Press *031000 to blind transfer a call to extension 1000.

Call Pickup

Name	Default code	Usage
Group Call Pickup	*4	Dial *4 to pick up the ringing call for a group member.
Extension Pickup	*04	Dial *041000 to pick up the ringing call for extension 1000.

Call Parking

Name	Default code	Usage
Call Parking	*5	Dial *5 during a call to park a call.

Name	Default code	Usage
Directed Call Parking	*05	Dial *056000 during a call to park a call to parking number 6000.

Intercom

Name	Default code	Usage
Intercom	*6	Dial *61001 to place an intercom call to extension 1001.

Queue

Name	Default code	Usage
Log in/Log out	*7	A dynamic agent dials *76400 to log in to or log out of queue 6400.
Pause/Unpause	*07	A dynamic agent dials *076400 to pause or unpause calls from queue 6400.

Speed Dial

Name	Default code	Usage
Speed Dial Prefix	*89	Specify a number to speed dial code 1, dial *891 to dial the specified number.

Presence Status

Name	Default code	Usage
Available	*91	Dial *91 to switch one's own presence status to Available.
Away	*92	Dial *92 to switch one's own presence status to Away.
Do Not Disturb	*93	Dial *93 to switch one's own presence status to Do Not Disturb.
Lunch Break	*94	Dial *94 to switch one's own presence status to Lunch Break.
Business Trip	*95	Dial *95 to switch one's own presence status to Business Trip.

Name	Default code	Usage
Off Work	*96	Dial *96 to switch one's own presence status to Off Work.

Switch Business Hours Status

Name	Default code	Usage
Switch Business Hours Status	*99	Dial *99 to switch the system in or outside business hours.

Conference

Conference Overview

Conference calls increase employee efficiency and productivity, and provide a more cost-effective way to hold meetings. This topic describes what is conference call, and conference member.

What is conference call

Yeastar P-Series PBX System supports dial-in conference that allows multiple participants, including internal users and external users, to start a conference call, and talk to each other anywhere and anytime.

Conference member

- Moderator: The conference moderator is a participant who can lock the conference call and manage the participants in a conference call.
- Participant: The conference member who can talk with each other and adjust the volume.

Create a Conference Room

To make a conference call, you should create a conference room on Yeastar P-Series PBX System first. This topic describes how to create a conference room.

Procedure

1. Log in to PBX management portal, go to Call Features > Conference, click Add.
2. Set up the conference room.
 - Number: Enter a room number for callers to dial into the conference call.

- Name: Enter a room name to help you identify it.
- Participant Password: Optional. The participants need to enter the password to join conference call.
- Moderator Password: Optional. The participants can enter the password to join conference call as moderators.
- Voice Prompt: Select a prompt to announce to the participants when someone joins or exits from the conference call.
 - Default: Prompt a tone when participant joins or exits from conference call.
 - Extension: Prompt the extension number of the participant when the participant joins or exits from conference call.
- Wait for Moderator: Whether to forbid the participants to talk with each other till the moderator joins the conference call.
- Allow Extension Participants to Invite: Whether to allow the extension participants to invite users to join the conference.
- Moderator(s): Select the moderators.

The moderators can join the conference calls without any password.

3. Click Save and Apply.

What to do next

If the external participants want to join conference, you need to set an [inbound route](#) and specify the Destination to Conference.

Join a Conference Call

Both the PBX extension users and the external users can join the conference. This topic describes how to join a conference call.

Join as a conference participant

1. Dial the conference room number.
2. If participant password is required, enter the participant password.

If you are the first participant in the conference call, the system plays a [hold music](#) to you.

Join as a conference moderator

For moderators

If you are a moderator specified by administrator, you can dial the conference room number to join the conference call.

If you are the first participant in the conference call, the system plays a [hold music](#) to you.

For participants who want to join conference as moderators

If you are not a moderator, and the moderator password is set for the conference room, you can also join conference call as a moderator

1. Dial the conference room number.
2. Enter the moderator password.

If you are the first participant in the conference call, the system plays a [hold music](#) to you.

Invite Users to a Conference Call

By default, only the conference moderators can invite users to the conference. This topic describes how to allow participants to invite users and how to invite users to a conference call.

Allow participants to invite users

1. Log in to PBX management portal, go to Call Features > Conference, edit the desired conference.
2. Select the checkbox of Allow Extension Participants to Invite.
3. Click Save and Apply.

Invite users to a conference call

1. During a conference call, press the # key.

You are forced out of the conference call temporarily.

2. Dial the number that you want to invite.

After the invited user joins or rejects the conference call, you will return to the conference call.


Manage Conference Rooms

This topic describes how to edit conference room settings and delete conference rooms.

Edit a conference room


Note:

You can not change the conference room number after setting up a conference room.

1. Log in to PBX management portal, go to Call Features > Conference.
2. Click  beside the conference room that you want to edit.
3. Change the conference room settings according to your needs.
4. Click Save and Apply.

Delete conference rooms

You can delete a conference room, or delete conference rooms in bulk.

1. Log in to PBX management portal, go to Call Features > Conference.
2. To delete a conference room, do the following:
 - a. Click  beside the conference room that you want to delete.
 - b. Click OK and Apply.
3. Delete conference rooms in bulk, do the following:
 - a. Select the checkboxes of the conference rooms that you want to delete, click Delete.
 - b. Click OK and Apply.

Conference Voice Menu

This topic describes the conference voice menu.

During the conference call, the participants can manage the conference by pressing * key on their phones to access voice menu for conference room.

The following table shows the conference voice menu.

Key	Description	Moderator	Participant
1	Mute or unmute yourself.	√	√
2	Lock or unlock the conference.	√	×
3	Eject the last user.	√	×
4	Decrease the conference volume.	√	√
6	Increase the conference volume.	√	√
7	Decrease your volume.	√	√
8	Exit the voice menu.	√	√
9	Increase your volume.	√	√

Speed Dial

Speed Dial Overview

Speed dial is often the easiest way to quickly connect with people and extensions that you dial frequently. This topic describes what is speed dial, and how to use speed dial.

What is speed dial

Speed dial is a feature that allows you to assign a speed dial code to a number that the users frequently dial. When dialing long strings of overseas numbers, the users do not have to remember or enter long telephone numbers on their phones.

How to use speed dial

You can create speed dial with a Prefix in front of the Speed Dial Number to avoid interference with your extensions.

- Speed Dial Number: The shorter number you assign to the phone number.
- Prefix: The code to access the speed dial feature. The default prefix is *89.

The users can dial {prefix}+{speed_dial_number} to call an assigned phone number. For example, assign 1 to phone number 5503302, dial *891 to place a call to 5503302.

Set up Speed Dial Prefix

You need to dial the speed dial code with a prefix. The prefix is used to access the speed dial feature, and avoid interference with the extensions. This topic describes how to set up speed dial prefix.

Procedure

1. Log in to PBX management portal, go to Call Features > Speed Dial.
2. Click Prefix.
3. In the Speed Dial Prefix field, enter a prefix according to your needs..
The default speed dial prefix is *89.
4. Click Save and Apply.

Tip:

To disable the speed dial prefix, go to Call Features > Feature code > Speed Dial > Speed Dial Prefix.

Add a Speed Dial Number

This topic describes how to add a speed dial number.

Background information

- Assume that you have an outbound route that allows you to dial an external number 15990234988, and you want to dial speed number 111 to reach an external number 15990234988 through the route.

- The [speed dial prefix](#) is enabled and set to *89.

Procedure

1. Log in to PBX management portal, go to Call Features > Speed Dial, click Add.
2. In the Speed Dial Number field, enter 111.
3. In the Phone Number field, enter 15990234988.
4. Click Save and Apply.


Result

Dial *89111 on your phone to call the external number 15990234988.

Manage Speed Dial Numbers


This topic describes how to edit a speed dial number, or delete speed dial numbers.

Edit a speed dial number

1. Log in to PBX management portal, go to Call Features > Speed Dial.
2. Click  beside the speed dial entry that you want to edit.
3. Change the Speed Dial Number or Phone Number according to your needs.
4. Click Save and Apply.

Delete speed dial numbers

You can delete a speed dial entry, or delete speed dial entries in bulk.

1. Log in to PBX management portal, go to Call Features > Speed Dial.
2. To delete a speed dial number, do the following:
 - a. Click  beside the speed dial entry that you want to delete.
 - b. Click OK and Apply.
3. To delete speed dial numbers in bulk, do the following:
 - a. Select the checkboxes of the speed dial entries that you want to delete, click Delete.
 - b. Click OK and Apply.

Export and Import Speed Dial Numbers

The speed dial numbers configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired speed dial numbers in the exported file, and import the file to PBX again. This topic describes how to export and import speed dial numbers.

Export speed dial numbers

You can export all speed dial numbers to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Call Features > Speed Dial.
2. Click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see [Speed Dial Number Parameters](#).

Import speed dial numbers

We recommend that you export speed dial numbers to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 50 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information, see [Speed Dial Number Parameters](#).

Procedure

1. Log in to PBX management portal, go to Call Features > Speed Dial.
2. Click Import.
3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The speed dial numbers in the CSV file will be displayed in the Speed Dial list.

Call Transfer

Call Transfer Overview

Call transfer is an in-call feature that allows the users to transfer current calls from their phones to another phone number or extension. This topic describes the call transfer types, and call transfer options.

Call transfer types

There are two scenarios to transfer a call:

- **Attended Transfer:** An attended transfer, also called consult transfer or warm transfer, allows the transferor to consult with the transfer recipient before transferring a call, such as the assistant can confirm with the executive whether he is free to answer the call before transferring the call.
- **Blind Transfer:** A blind transfer, also called cold transfer, allows the transferor to transfer a call to transfer recipient immediately without consultative communication, such as transfer a call to ring group.

Call transfer options

The following options are available for you to set up call transfer:

- **Feature code:** Extension users can use the call transfer code to transfer a call.
The default call transfer code:
 - Attended Transfer: *3
 - Blind Transfer: *03
- **Digit Timeout(s):** The timeout for transferor to enter the transfer recipient's number after dialing the feature code. The time interval between each digit should be within the digit timeout.
- **Attended Transfer Timeout(s):** The ring timeout for transfer recipient to take the transferring call.

If the transfer recipient does not answer the transferring call within the timeout, the system sends the call back to transferor.

Set up Call Transfer

This topic describes how to set up call transfer.

Set up attended transfer

1. Log in to PBX management portal, go to Call Features > Feature code > Call Transfer.
2. Select the checkbox of Attended Transfer to enable the attended transfer feature.
If unselected, the extension users can not perform attended transfer by dialing the feature code.
3. Enter a code number according to your needs.
4. In the Digit Timeout(s) drop-down list, select a timeout for entering transfer recipient's number after you hear a dial tone.
5. In the Attended Transfer Timeout(s) field, enter a number of seconds for transfer recipient to take the transferring call.
6. Click Save and Apply.

Set up blind transfer

1. Log in to PBX management portal, go to Call Features > Feature code > Call Transfer.

2. Select the checkbox of Blind Transfer to enable the blind transfer feature.

If unselected, the extension users can not perform blind transfer by dialing the feature code.

3. Enter a code number according to your needs.
4. In the Digit Timeout(s) drop-down list, select a timeout for entering transfer recipient's number after you hear a dial tone.
5. Click Save and Apply.

Perform an Attended Transfer

If you want to make sure someone is ready to take a transferred call or you need to explain something to the transfer recipient, you can perform an attended transfer. This topic describes how to perform an attended transfer.

Procedure

1. During a call, press the feature code of attended transfer (default *3).

The original call is placed on hold, and the system prompts "transfer" and the dial tone.

2. Dial the phone number of the contact where you want the call to be transferred.
3. Wait for the call to be answered.

When the call is answered, talk to the transfer recipient.

4. Hang up the call directly to complete the call transfer.

The original caller and the transfer recipient are connected.

Perform a Blind Transfer

If you do not need any interaction with the user who receives the call, you can perform a blind transfer. This topic describes how to perform a blind transfer.

Procedure

1. During a call, press the feature code of blind transfer (default *03).

The original call is placed on hold, and the system prompts "transfer" and the dial tone.

2. Dial the phone number of the contact where you want the call to be transferred.

The call ends automatically, and the transfer recipient's phone rings.

A new call between original caller and transfer recipient is established after transfer recipient answers.

Call Pickup

Call Pickup Overview

Call Pickup is a feature that allows employees to pick up colleagues' calls remotely, without having to walk to the his/her telephone. This topic describes the two pickup types including extension call pickup, group call pickup, and pickup code.

Extension call pickup

Extension call pickup, also known as directed call pickup, allows employees to pick up a call for a specific extension.

For example, the executive's phone is ringing, and the assistant knows the executive is in a meeting and is unavailable to answer the call, the assistant can pick up the executive's call from his/her phone.

Group call pickup

Group call pickup allows the [extension group](#) members to share their incoming calls. For a group of employees working on the same subject, when a member receives an incoming call and is unavailable to take the call, other members can pick up the call from their phones.

Pickup feature code

Extension users can use the pickup code to pick up a call.

The default pickup code:

- Group Call Pickup: *4
- Extension Pickup: *04

Tip:


You can change, enable, or disable the code on PBX management portal: Call Features > Feature Code > Call Pickup.

Pick up a Call for a Group Member

This topic describes how to set up a Feature key on an IP phone to pick up a call for an extension group member.

Background information


For the users who want to pick up a call for an extension group member, you can set a Feature key for each user by [auto provisioning](#). Users can also set function keys on their own IP phones. For more information, contact the phone manufacturer.


 Note:

The default feature code for picking up a group member's call is *4. You can change, enable, or disable the code on PBX management portal: Call Features > Feature Code > Call Pickup > Group Call Pickup.


Set up a Feature key

The following takes Yealink phone as an example to set a Speed Dial key for group pickup.

1. Assign function keys for extension users to monitor extension status.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
 - If you want to assign function keys for a specific extension user, click  beside the desired extension.
 - If you want to assign function keys for multiple extensions, select the checkboxes of the desired extensions, and click Edit.
 - b. Click the Function Keys tab.
 - c. Configure function keys.

 Note:

The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

- Type: Select Speed Dial.
 - Value: Enter the code (*4).
 - Label: Optional. Enter a value, which will be displayed on the phone screen.
- d. Click Save.
2. If the extension hasn't be associated with a phone, see [Auto Provision IP Phones](#) to bind a phone with the extension.
 3. If the extension has been associated with a phone, reprovision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click  beside the phone assigned to this extension.

Result

When an extension group member receives a call, the user can press the Feature key directly to answer the call.

Pick up a Call for a Specific Extension

This topic describes how to set up a BLF key on an IP phone to pick up a call for a specific extension.

Background information


For the users who want to monitor call status changes of a specific extension, and pick up the call on their phones, you can set a BLF key for each user by [auto provisioning](#). Users can also set function keys on their own IP phones. For more information, contact the phone manufacturer.

Note:

The default feature code for picking up an extension call is *04. You can change, enable, or disable the code on PBX management portal: Call Features > Feature Code > Call Pickup > Extension Pickup.


Set up a BLF key

The following takes Yealink phone as an example to set a BLF key for call pickup.

1. Assign function keys for extension users to monitor agent status.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
 - If you want to assign function keys for a specific extension user, click  beside the desired extension.
 - If you want to assign function keys for multiple extensions, select the checkboxes of the desired extensions, and click Edit.
 - b. Click the Function Keys tab.
 - c. Configure function keys.

Note:

The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

- Type: Select BLF.
 - Value: Enter the code (*04) followed by extension number (for example *041001).
 - Label: Optional. Enter a value, which will be displayed on the phone screen.
- d. Click Save.
2. If the extension hasn't be associated with a phone, see [Auto Provision IP Phones](#) to bind a phone with the extension.
 3. If the extension has been associated with a phone, reprovision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click  beside the phone assigned to this extension.

Result

When the monitored extension receives an incoming call, the BLF key fast flashes red. The user can press the BLF key directly to answer the call.

Call Parking

Call Parking Overview

Call parking is a method of holding a call on a phone, anyone can retrieve the call on another phone. This topic describes what is call parking, parking number, parking types, parking recall, and parking code.

What is call parking

Traditionally, you can only retrieve the call on the same phone when you hold a call. Call parking allows you to hold a call on a parking number, and allows you to dial the parking number on any phone to retrieve the call.

Parking number

Parking number, also known as slot or orbit, is a 4-digit virtual extension number that the system assigns to the parked call. One parked call occupies one parking number.

The maximum number of simultaneous parking number is 100.

Parking types

Yeastar P-Series PBX System supports two parking types.

- Call parking: Park a call randomly on the first available parking number.
- Directed call parking: Park a call on the specified parking number.

Parking timeout destination

The parked call remains on the parking number for a specified period of time (default 60 seconds). If no one retrieves the parked call within the timeout period, the system routes the call to a designated destination (default initiator).

Parking feature code

Extension users can use the parking code to park a call.

The default parking code:

- Call Parking: *5
- Directed Call Parking: *05

i Tip:

You can change, enable, or disable the code on PBX management portal: Call Features > Feature Code > Call Parking.

Directed Call Parking

This topic describes how to park a call on a specific parking number, and retrieve the parked call.

Background information

For sales or support, it probably doesn't matter exactly who picks up the call. You can allocate different parking numbers to different departments. For example, 6099 for sales, 6098 for support, and so on. The receptionist can park the call directly on the parking number based on business. Anyone in the department can retrieve the call by the parking number.

📄 Note:

The default range of parking number is from 6000 to 6099. The randomly call parking occupies parking number from 6000. To avoid that the allocated parking number is occupied by randomly call parking, we recommend that you allocate the parking number backwards from 6099.

Prerequisites

Make sure that the parking number is vacant. If the specified parking number is occupied, the system parks the call to the next available parking number.

i Tip:

[Set up a function key for users to monitor the status of parking number.](#)

- For receptionist, he/she can press the function key to park the call to the parking number.
- For users in different departments, a parked call is visible on the function key, so that they can press the function key to retrieve the parked call easily.

Procedure

Parking number 6099 is assigned to salesmen. The receptionist receives a call, and the customer wants to consult business information.

1. The receptionist dials *056099 to park the call to parking number 6099.
2. The receptionist tells the sales there is a parked call for business.

If function keys are configured on the sales' IP phones, they will be notified.

3. The sales who is available can dial 6099 or press the function key to retrieve the call.

i Tip:

The default feature code for directed call park is *05. You can change, enable, or disable the code on PBX management portal: Call Features > Feature Code > Call Parking > Directed Call Parking.

Call Parking

This topic describes how to park a call randomly on the available parking number, and retrieve the parked call.

Background information

During a conversation, the employee may need to go to another office for retrieving an important file or for security, he/she can park the call, and to continue the conversation after arriving at the other office.

Procedure

1. Dial the feature code (*5) to park a call.
The system prompts you the parking number (6000) where the call is parked.
2. Go to another office, dial the parking number (6000) to retrieve the parked call.

i Tip:

The default feature code for call park is *5. You can change, enable, or disable the code on PBX management portal: Call Features > Feature Code > Call Parking > Call Parking.

Set up Parking Timeout Destination

By default, if a parked call is not retrieved after 60 seconds, the call will be transferred back to the originator. You can set up the parking timeout and timeout destination. This topic describes how to set up parking timeout and timeout destination for an unretrieved call.


Procedure

1. Log in to PBX management portal, go to Call Features > Feature Code > Call Parking.
2. In the Parking Timeout (s) field, enter the number of seconds for the parked call.
3. In the Timeout Destination drop-down list, select a destination to receive the unretrieved call.

A parked call will be routed to the designated destination when the call parking times out.

- Call Parking Initiator: Route the call to the user who parks this call.
- Extension: Route the call to the designated extension number.
- Extension Voicemail: Route the call to the designated extension's voicemail.

- Group Voicemail: Route the call to the voicemail box of a queue, a ring group, or a custom group.
- External Number: Route the call to the designated external number.

 Note:

Set the [Prefix](#) according to your outbound route so that PBX can successfully route incoming calls to external number.

- If the Strip of outbound route is not set, you don't have to set the Prefix.
- If the Strip of outbound route is set, you need to set the Prefix according to the Patterns of outbound route.

4. Click Save and Apply.

Set up Parking Number

The default range of parking number is from 6000 to 6099. This topic describes how to define the range of parking numbers for parked call.

Procedure

1. Log in to PBX management portal, go to Call Features > Feature code > Call Parking.
2. In the Parking Number Range field, enter a number range for parked call.
3. Click Save and Apply.

 Tip:


You can also change the parking number range at PBX Settings > Preferences > Extension Preference > Parking Extension.

Monitor a Parking Number on an IP Phone

This topic describes how to set up a function key on a user's phone to monitor a parking number.

Background information

For users who use directed call parking and want to monitor a specific parking number, you can set a function key for each user by [auto provisioning](#).


 Note:


Users can also set function keys on their own IP phones. For more information, contact the phone manufacturer.

 Tip:


Agents can also press the function keys to park or retrieve a call.

Procedure

1. Assign function keys for extension users to monitor parking number.
 - a. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
 - If you want to assign function keys for a specific extension user, click  beside the desired extension.
 - If you want to assign function keys for multiple extensions, select the checkboxes of the desired extensions, and click Edit.
 - b. Click the Function Keys tab.
 - c. Configure function keys.

 Note:


The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

- Type: Select Park & Retrieve.
 - Value: Select a parking number.
 - Label: Optional. Enter a value, which will be displayed on the phone screen.
- d. Click Save.
2. If the extension hasn't be associated with a phone, see [Auto Provision IP Phones](#) to bind a phone with the extension.
 3. If the extension has been associated with a phone, reprovision the phone to take effect.
 - a. Go to Auto Provisioning > Phones.
 - b. Click  beside the phone assigned to this extension.

Result

The function key shows the real-time status of the parking number.

- Green: The parking number is idle.
The user can press the function key to park an active call to the idle parking number.
- Red: The parking number is occupied.
The user can press the function key to retrieve a parked call from the monitored parking number.

 Note:

The key LED status may vary by phone models.

Fax

Fax Overview

Yeastar P-Series PBX System allows you to connect your fax machine to PBX system. Then you can send or receive faxes on a fax machine, and receive faxes by email. This topic describes how fax works with Yeastar P-Series PBX System, and introduces fax to email, fax detection, and Fax over VoIP settings.

How does fax work with PBX

The fax machines traditionally use the T.30 protocol to transmit analog data over Public Switched Telephone Network (PSTN). However, the analog data cannot be sent over an Voice over Internet Protocol (VoIP) network. Thus the T.38 protocol is created to provide reliable real-time faxing over IP (FoIP).

Yeastar P-Series PBX System supports both T.30 and T.38 protocols. With Yeastar P-Series PBX System, you can send or receive fax over PSTN or VoIP network in real time.

Faxing over PSTN (T.30)

T.30 protocol defines the procedures for transmitting data between two fax machines over the Public Switched Telephone Network (PSTN).

With S2 module or SO module installed on the PBX, you can connect the analog fax machine directly to the FXS port, and then send and receive fax on your fax machine.

Faxing over IP (T.38)

T.38 is a protocol that enables fax over the Internet and is supported on Yeastar P-Series PBX System. T.38 utilizes Voice over IP (VoIP) to send a fax. This process is known as virtual fax or FoIP (Fax over IP).

The diagram below explains how T.38 Fax works:

1. A fax machine sends a fax through a T.38 compatible gateway, which acts as an emitting server.
2. The emitting server partitions data from the fax into an image that can be encoded and sent over the Internet in real time, then sends the T.38 data stream to another T.38 compatible server, such as a PBX, which acts as a receiving server.
3. The receiving server converts the T.38 data stream to analog signal, and sends to the terminal fax machine.



Fax to email

Faxes traditionally are sent directly to a fax machine; the recipient receives a printed copy. Yeastar P-Series PBX System provides fax to email feature that allows you to receive faxes as PDF by email.

The benefits of fax to email:

- Keep your faxes private without paper trail.
- Access faxes in real-time from anywhere.
- No need to pay for expensive hardware, printer paper, ongoing maintenance or a dedicated fax line.

Fax detection

Fax detection is used to detect automatically whether an incoming call is voice or fax. It is useful when you have fax call and voice call on the same line.

- If the PBX detects a fax signal, the PBX immediately routes the call to the designated fax destination.
- If the PBX does not detect a fax signal, the PBX handles the call as a regular voice call.

Fax over IP (FoIP) settings

The following settings are available when you want to improve the Fax transmission over VoIP network.

- T.38 Support: Enable or disable T.38 protocol for extension and trunk according to your needs.
- T.38 Max BitRate: The maximum bit rate of the fax transmission.
The default value is 14400.
- No T.38 Attributes in re-INVITE SDP: Whether to contain T.38 attributes in SDP re-invite packet.
- Error Correction Mode: Error Correction Mode (ECM) is an optional transmission mode. ECM automatically detects and corrects errors in the fax transmission process that are sometimes caused by telephone line noise.

Send Faxes from an Analog Fax Machine

To send faxes from Yeastar P-Series PBX System, you need to set up an FXS extension for the fax machine and set up an outbound route for outgoing faxes. This topic describes the configurations for outgoing faxes on the PBX.

Prerequisites

Before you send faxes from an analog fax machine, perform the following tasks:

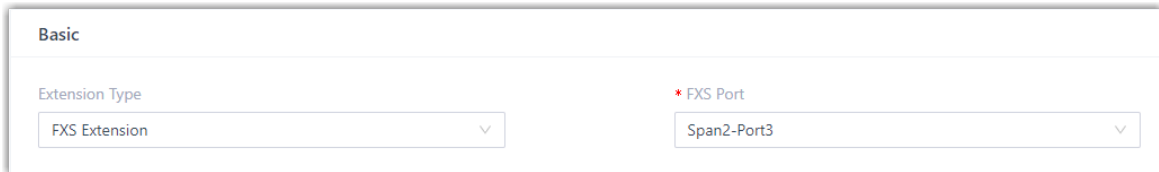
1. [Install S2 module or SO module on the PBX.](#)
2. Connect fax machine to FXS port of the PBX.

In this topic, we connect fax machine to FXS port located in Span2-Port3.

Step1. Assign an extension to the analog fax machine

1. Log in to PBX management portal, go to Extension and Trunk > Extension, click Add.
2. In the Basic section, select FXS Extension from the Extension Type drop-down list.
3. In the FXS Port drop-down list, select the FXS port to which the fax machine is connected.

As the following figure shows, select fax port Span2-Port3.



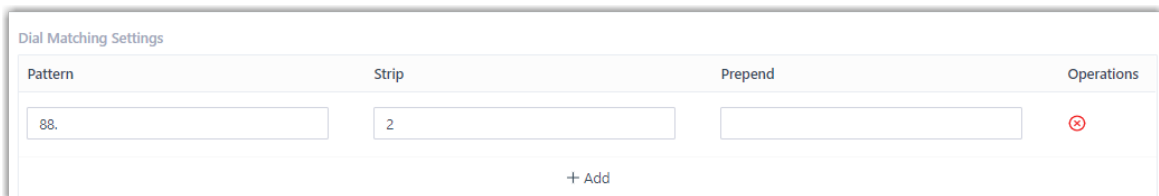
The screenshot shows the 'Basic' configuration section. It contains two dropdown menus. The first is labeled 'Extension Type' and is set to 'FXS Extension'. The second is labeled '* FXS Port' and is set to 'Span2-Port3'.

4. Leave other settings as default or change the settings according to your needs.
5. Click Save and Apply.

Step2. Set up an outbound route for sending faxes

1. Log in to PBX management portal, go to Call Control > Outbound Route, click Add.
2. In the Name field, enter an outbound route name to help you identify it.
3. Set the [Dial Patterns](#) for the outbound route.


As the following figure shows, set 88. for Pattern, and 2 for Strip.



The screenshot shows the 'Dial Matching Settings' table. It has four columns: Pattern, Strip, Prepend, and Operations. The Pattern column contains '88.', the Strip column contains '2', and the Prepend column is empty. There is a red 'X' icon in the Operations column. Below the table is a '+ Add' button.

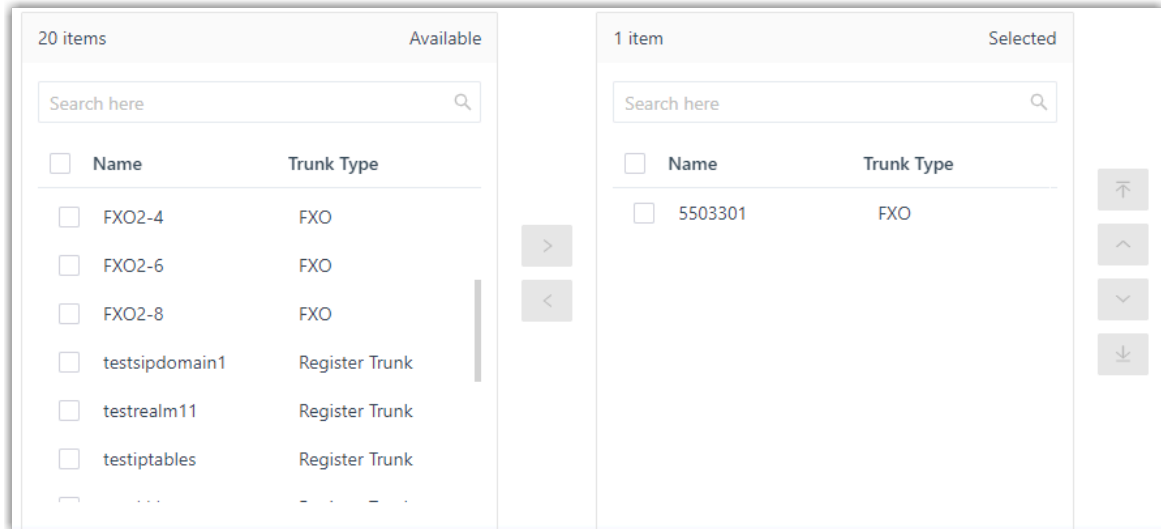
Pattern	Strip	Prepend	Operations
88.	2		⊗

4. Select a trunk that supports to send faxes.

 Note:

If you choose a SIP trunk to send faxes, you need to [enable T.38 Support for this trunk](#).

As the following figure shows, select a trunk to send faxes.



5. Select the extension that you have assigned to fax machine.
6. Click Save and Apply.

Result

In the example shown above, you can dial 885503304 to send faxes to 5503304. After you hear a fax tone, you can start to send fax.

Receive Faxes through a Dedicated Trunk

Having a dedicated trunk for faxing is the best way to prevent interruptions and other problems that arise from using a shared trunk. This topic describes how to receive faxes on an analog fax machine through a dedicated trunk .

Prerequisites

Before you receive faxes by an analog fax machine, perform the following tasks:

1. [Install S2 module or SO module on the PBX](#).
2. Connect fax machine to FXS port of the PBX.

In this topic, we connect fax machine to FXS port located in Span2-Port3.

Step1. Assign an extension to the fax machine

1. Log in to PBX management portal, go to Extension and Trunk > Extension, click Add.
2. In the Basic section, select FXS Extension from the Extension Type drop-down list.

- In the FXS Port drop-down list, select the FXS port to which the fax machine is connected.

As the following figure shows, select fax port Span2-Port3.

The screenshot shows a configuration window titled 'Basic'. It contains two dropdown menus. The first is labeled 'Extension Type' and has 'FXS Extension' selected. The second is labeled '* FXS Port' and has 'Span2-Port3' selected.

- Click Save and Apply.

Step2. Set up an inbound route for receiving faxes

- Go to Call Control > Inbound Route, click Add.
- In the Name field, enter an inbound route name to help you identify it.
- Set the DID Pattern through which this route pass the incoming call.

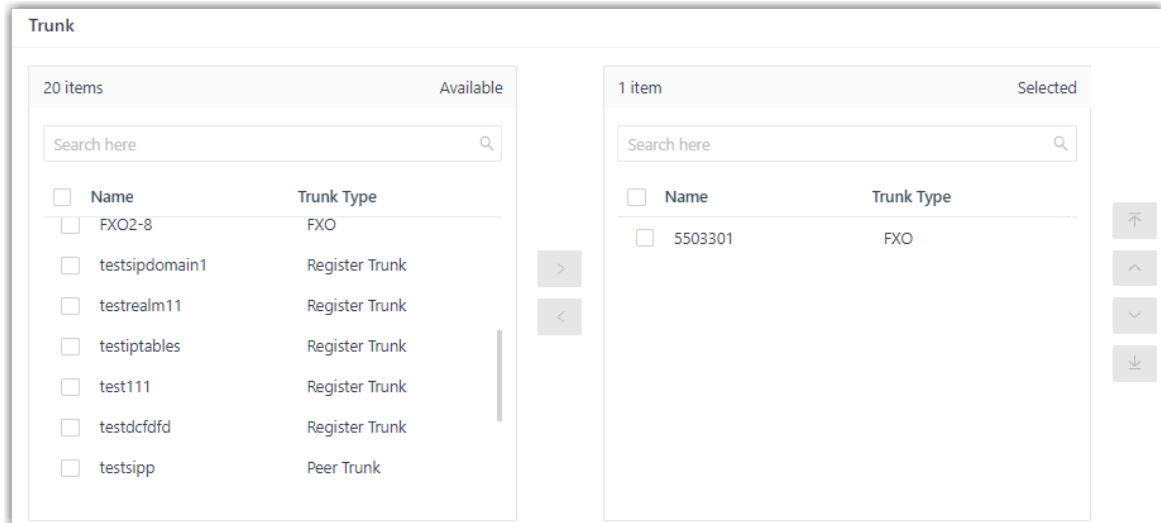
As the following figure shows, set the trunk number as DID pattern.

The screenshot shows a configuration window titled 'DID Pattern'. It has a dropdown menu for '* DID Matching Mode' set to 'DID Pattern'. Below is a table with two columns: 'Pattern' and 'Operations'. The 'Pattern' column contains the value '5503301'. The 'Operations' column contains a red trash can icon. At the bottom of the table is a '+ Add' button.

- Select the trunk that supports to receive faxes.

Note:
If you choose a SIP trunk to receive faxes, you need to [enable T.38 Support for this trunk](#).

As the following figure shows, select a trunk to receive faxes.



5. In the Default Destination drop-down list, select Extension.
6. Select the extension that you have assigned to the fax machine.
7. Click Save and Apply.

Result

In the example shown above, when a customer sends faxes to trunk 5503301, you can receive the faxes on your analog fax machine.

Receive Faxes and Calls through the Same Line

If your company only has a single telephone line, you can have fax and voice call on the same line. This topic describes how to receive faxes on an analog fax machine through a shared line.

Background information

Generally, we use an IVR to receive fax and voice on the same line. When the call is answered, the PBX detects fax signal throughout the duration of the call.

Prerequisites

Before you receive faxes from an analog fax machine, perform the following tasks:

1. [Install S2 module or SO module on the PBX.](#)
2. Connect fax machine to FXS port of the PBX.

In this topic, we connect fax machine to FXS port located in Span2-Port3.

Step1. Assign an extension to the analog fax machine

1. Log in to PBX management portal, go to Extension and Trunk > Extension.

2. Click Add.
3. In the Basic section, select FXS Extension from the Extension Type drop-down list.
4. In the FXS Port drop-down list, select the FXS port to which the fax machine is connected.

As the following figure shows, select fax port Span2-Port3.

The screenshot shows a configuration window titled "Basic". It contains two dropdown menus. The first dropdown, labeled "Extension Type", has "FXS Extension" selected. The second dropdown, labeled "* FXS Port", has "Span2-Port3" selected.

5. Click Save and Apply.

Step2. Set up an inbound route for receiving faxes

1. Go to Call Control > Inbound Route, click Add.
2. In the Name field, enter an inbound route name to help you identify it.
3. Set the [DID Pattern](#) through which this route pass the incoming call.

As the following image shows, set the trunk number as DID pattern.

The screenshot shows a configuration window titled "DID Pattern". It contains a dropdown menu for "* DID Matching Mode" with "DID Pattern" selected. Below this is a table with two columns: "Pattern" and "Operations". The table has one row with the value "5503301" in the "Pattern" column and a trash icon in the "Operations" column. At the bottom of the table is a "+ Add" button.

4. Select the trunk that supports to receive faxes.

Note:

If you choose a SIP trunk to receive faxes, you need to [enable T.38 Support for this trunk](#).

5. In the Default Destination drop-down list, select IVR.
6. Set the destination for receiving the faxes.
 - a. Turn on Fax Detection.
 - b. In the Fax Destination drop-down list, select Extension.
 - c. Select the extension that you have assigned for fax machine.

As the following figure shows, set the assigned extension 2185 to the fax machine.

7. Click Save and Apply.

Result

When the customer places a call to your company, the call is automatically answered by IVR. The customer can follow the voice menu to access the desired department, send fax after negotiation or send the fax directly.

1. The customer sends a fax to your company (5503301).
The originating fax machine sends a fax signal to system to indicate that this is a fax call.
2. The PBX detects the fax signal, automatically forwards the call to the extension (2185) you have assigned to your fax machine.
3. Receive fax on your fax machine.

Receive Faxes by Email

Yeastar P-Series PBX System provides fax to email feature that allows you to receive faxes as PDF by email. This topic describes how to receive faxes by email.

Prerequisites

- Make sure the PBX [system email](#) works, or the PBX cannot forward the received faxes to an extension user's email.
- Make sure there is a valid email address assigned to extension.
- Optional: Customize the fax [email template](#).

Procedure

1. Log in to PBX management portal, go to Call Control > Inbound Route, edit the inbound route for incoming faxes.
2. If you receive faxes through a dedicated line, go to Default Destination section.
 - a. In the Default Destination drop-down list, select Fax To Email.
 - b. Select an extension user to receive faxes by email.

Default Destination

Default Destination *

Fax To Email 2171-2171

Time Condition

3. If you receive faxes through a shared line, go to Fax Detection section.
 - a. In the Fax Destination drop-down list, select Fax To Email.
 - b. In the Extension's Email drop-down list, select an extension user to receive faxes by email.

Default Destination

Default Destination *

IVR 6202-6202

Time Condition

Fax Detection

* Fax Destination * Extension's Email

Fax To Email 2185-2185

4. Click Save and Apply.

Result

When receiving a fax, PBX converts the received fax and simply forwards it to the email address as an PDF attachment.

Set up Fax over IP (FoIP)

Fax over IP (FoIP) is the process of using T.38 protocol to send a fax from a fax machine to another fax machine over the Internet. This topic describes how to enable T.38 for extension and trunk respectively, and how to change T.38 settings to improve the Fax transmission over VoIP network.

Enable T.38 protocol for SIP extension

If you want to register a SIP extension on a SIP compatible fax machine, you need to enable T.38 Support for this extension.

1. Log in to PBX management portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Go to Advanced > VoIP Settings.
3. Select the checkbox of T.38 Support.
4. Click Save and Apply.

Enable T.38 protocol for SIP trunk

If you want to use a SIP trunk to send or receive faxes, you need to enable T.38 Support for this trunk.

1. Log in to PBX management portal, go to Extension and Trunk > Trunk, edit the desired trunk.
2. Go to Advanced > VoIP Settings.
3. Select the checkbox of T.38 Support.
4. Click Save and Apply.

Change T.38 settings

If the Fax over IP doesn't work, you can change the T.38 settings.

1. Log in to PBX management portal, go to PBX Settings > SIP Settings > T.38.
2. Change the T.38 settings.
 - T.38 Max BitRate: Set the maximum bit rate of the fax transmission.
 - No T.38 Attributes in re-INVITE SDP: If enabled, SDP re-invite packet does not contain T.38 attributes.
 - Error Correction Mode: If enabled, after receiving the packet for a complete fax page, PBX notifies the transmitting fax machine of the frames with errors. The transmitting fax machine then retransmits the specified frames.
This process is repeated until all frames are received without errors.
3. Click Save and Apply.

Paging/Intercom

Overview of Paging and Intercom

This topic describes what is Paging and Intercom, scheduled paging call and intercom call.

What is Paging and Intercom

Yeastar P-Series PBX System Paging and Intercom feature helps users broadcast announcements over one or more speakers, without the called party picking up the handset.

Paging

Paging feature is used to make a one-way announcement to users via a phone speaker.

There are two kinds of Paging:

- One-way Paging: One-way announcement to users with extensions registered.

When a broadcaster makes a paging call, the group members' phones automatically answer into speakerphone mode. Group members can not talk with the broadcaster during the call.

For more information, see [Set up a One-way Paging Group](#).

- **One-way Multicast Paging:** One-way announcement to users who have their phones listen on the same multicast IP and port as the PBX.

When trying to make an announcement to group members, the broadcaster's phone sends out an RTP stream to the multicast IP and port. Upon receiving the forwarded RTP packets from local network switch and router, the listening phones play RTP stream out of speakers.

For more information, see [Set up a One-way Multicast Paging Group](#).

Intercom

Intercom feature is used to establish two-way communication with users via a phone speaker.

When a broadcaster makes an intercom call, the group members' phones automatically answer into speakerphone mode. The broadcaster and all the group members can talk with each other during the call.

For more information, see [Set up a Two-way Intercom Group](#).

Scheduled paging call and intercom call

Besides real-time paging calls or intercom calls, you can set a time schedule to automatically start your broadcast. The Scheduled Paging/Intercom feature is perfect for schools, airports, or other facilities that require routine notifications set in advance.

For more information, see [Schedule a Paging Call or an Intercom Call](#).

Paging/Intercom Group

Set up a One-way Paging Group

One-way Paging feature allows a broadcaster to make an announcement to users. The called parties' phones will not ring, but instead directly answering into speakerphone mode. This topic describes how to set up a one-way paging group.

Scenario

A company has different departments on different floors in a building. Each department is deployed with a phone for communication. The boss has an urgent case that needs to confirm with marketers. In this case, you can set up a One-way paging group for Marketing De-

partment. The boss can make a paging call to the department and ask marketers concerned to go to the office.

Procedure

1. Log in to PBX management portal, go to Call Features > Paging/Intercom, click Add.
2. Configure a one-way paging group.

The screenshot shows the configuration interface for a one-way paging group. The form is divided into several sections:

- Number:** A text input field containing "6600".
- Name:** A text input field containing "Marketing Department".
- Type:** A dropdown menu set to "One-way Paging".
- Prompt:** A dropdown menu set to "[None]".
- Broadcaster:** A dropdown menu that is currently blank.
- Dial * to Answer:** A checkbox that is unchecked.
- Members:** Two tables for selecting members.
 - Available (12 items):** A table with columns "Extension Number" and "Caller ID Name". It lists "Default_All_Extensions" and several individual extensions (2000-2006) with their respective names.
 - Selected (1 item):** A table with columns "Extension Number" and "Caller ID Name". It lists "Marketing Department" under the "Extension Group" column.

- **Number:** Enter a number for the paging group. In this example, enter 6600.
- **Name:** Enter a name for the paging group. In this example, enter Marketing Department.
- **Type:** Select One-way Paging.
- **Prompt:** Optional. To play a prompt before making an announcement, you can select a custom prompt. In this example, leave it as None.

Note:

To customize a prompt, see [Record a Custom Prompt](#) or [Upload a Custom Prompt](#).

- **Broadcaster:** Optional. To restrict users from making an announcement to the paging group, select allowed extensions or extension groups from the drop-down list. In this example, leave it blank.
- **Dial * to Answer:** Optional. To allow users to dial * to talk to the broadcaster privately, enable this option. In this example, keep the option disabled.

Note:

When a user dials *, announcement will terminate, and the user can have a private talk with the broadcaster.

- Members: Select desired members from Available box to Selected box. In this example, select Marketing Department.
3. Click Save and Apply.

What to do next

The boss dials 6600 from any endpoint with extension registered. The marketers' phones automatically answer into speakerphone mode.

Note:

If called parties' extensions are registered on the following endpoints, these endpoints will ring first, instead of automatically answering into speakerphone mode.

- Analog phone
- Softphone, including Linkus Web Client, Linkus Mobile Client, and softphones of other brands.

Related information

[Schedule a Paging Call or an Intercom Call](#)

Set up a One-way Multicast Paging Group

One-way Multicast Paging feature allows a broadcaster to make an announcement to the users who are listening to a specific multicast group on a specific channel. The called parties' phones will not ring, but instead directly answering into speakerphone mode. This topic describes how to set up a one-way multicast paging group.

Scenario

For a warehouse, the work flow in product line is closely connected and tends to be complex. For example, one zone is responsible for packaging goods, another zone is for dispatching goods. To facilitate supervisors in coordinating daily warehouse activities, you can set up paging groups for each zone.

Requirements

The phone that will receive One-way Multicast Paging must meet the following requirements:

- A Yealink or Fanvil IP phone that supports multicast feature.
- The IP phone is on the same local subnet as the PBX.

Procedure

Based on the above scenario, you need to create two paging groups on the PBX and set up multicast listening on two phones.

1. On Yeastar P-Series PBX System, create two paging groups.
 - a. Create a paging group 6601 for Packaging Area.
 - i. Log in to PBX management portal, go to Call Features > Paging/Intercom, click Add.
 - ii. Configure a one-way multicast paging group.

* Number		* Name	
<input type="text" value="6601"/>		<input type="text" value="Packaging Area"/>	
* Type		Prompt	
<input type="text" value="One-way Multicast Paging"/>		<input type="text" value="[None]"/>	
Broadcaster			
<input type="text"/>			
IP of Multicast Channel			
* IP of Multicast Channel	* Port	Operations	
<input type="text" value="224.5.6.20"/>	<input type="text" value="10008"/>		

- Number: Enter a number for the paging group. In this example, enter 6601.
- Name: Enter a name for the paging group. In this example, enter Packaging Area.
- Type: Select One-way Multicast Paging.
- Prompt: Optional. To play a prompt before making an announcement, you can select a custom prompt. In this example, leave it as None.

Note:
 To customize a prompt, see [Record a Custom Prompt](#) and [Upload a Custom Prompt](#).

- Broadcaster: Optional. To restrict users from making an announcement to the paging group, select allowed extensions or extension groups from the drop-down list. In this example, leave it blank.
- IP of Multicast Channel: Enter a multicast IP address and port.
 - IP of Multicast Channel: Enter a multicast IP address. In this example, enter 224.5.6.20.
 - Port: Enter a multicast port. In this example, enter 10008.

Note:

- The range of multicast IP address is 224.0.0.0 - 239.255.255.255.
- You can add at most 30 IP addresses.

- iii. Click Save and Apply.
 - b. Repeat step a to create another paging group 6602 for Dispatching Area.

Note:

Set a multicast IP address and port that are different from Packaging Area. For example, set IP of Multicast Channel to 224.5.6.21 and set Port to 10010.

* Number	6602	* Name	Dispatching Area
* Type	One-way Multicast Paging	Prompt	[None]
Broadcaster			
IP of Multicast Channel			
* IP of Multicast Channel	* Port	Operations	
224.5.6.21	10010		

2. Set up multicast listening for the two phones in Packaging Area and Dispatching Area.
 - a. Set up multicast listening for the phone in Packaging Area. In this example, we take Yealink T56A as an example.
 - i. Log in to the phone web interface, go to Directory > Multicast IP.
 - ii. In the Listening Address field, enter the same multicast IP address and port as the PBX. In this example, enter 224.5.6.20:10008.

Multicast Listening

Paging Barge: 1

Ignore DND: Disabled

Paging Priority Active: ON

IP Address	Listening Address	Label	Channel	Priority
1 IP Address	224.5.6.20:10008		0	1
2 IP Address			0	2

- iii. Click Confirm.
 - b. Set up multicast listening for the phone in Dispatching Area. In this example, we take Fanvil X210 as an example.
 - i. Log in to the phone web interface, go to Phone Settings > MCAST.
 - ii. In the Host:Port field, enter the same multicast IP address and port as the PBX. In this example, enter 224.5.6.21:10010.

Features	Media Settings	MCAST	Action	Time/Date	Time Plan	Tone
MCAST Listening						
Priority:			1			
Enable Page Priority:			<input type="checkbox"/>			
Enable Prio Chan:			<input checked="" type="checkbox"/>			
Enable Emer Chan:			<input type="checkbox"/>			
Index/Priority	Name	Host:port	Channel			
1	<input type="text"/>	224.5.6.21:10010	0			
2	<input type="text"/>	<input type="text"/>	0			

iii. Click Apply.

What to do next

- Supervisor dials 6601 to reach employees in Packaging Area. Yealink T56A automatically answers into speakerphone mode.
- Supervisor dials 6602 to reach employees in Dispatching Area. Fanvil X210 automatically answers into speakerphone mode.

Related information

[Schedule a Paging Call or an Intercom Call](#)

Set up a Two-way Intercom Group

Two-way Intercom feature allows you to establish two-way communication with an individual user or a group of users. The called parties can respond without picking up the handset. This topic describes how to set up a two-way intercom group.

Background information

In office complexes, hospitals, or schools, there are either static guards or patrol guards to ensure safety within the workplace. The Two-way Intercom feature helps improve communication efficiency. For example, a security guard can ask for help when security incidents happen, a supervisor can flexibly dispatch employees in daily activities.

Yeastar P-Series PBX System supports to place an intercom call to one or more users:

Place an intercom call to a specific user

Dial Intercom feature code (default: *6) followed by a desired extension number.

For example, dial *61002 to place an intercom call to 1002.

 Tip:

To change intercom feature code, go to Call Features > Feature Code > Intercom.

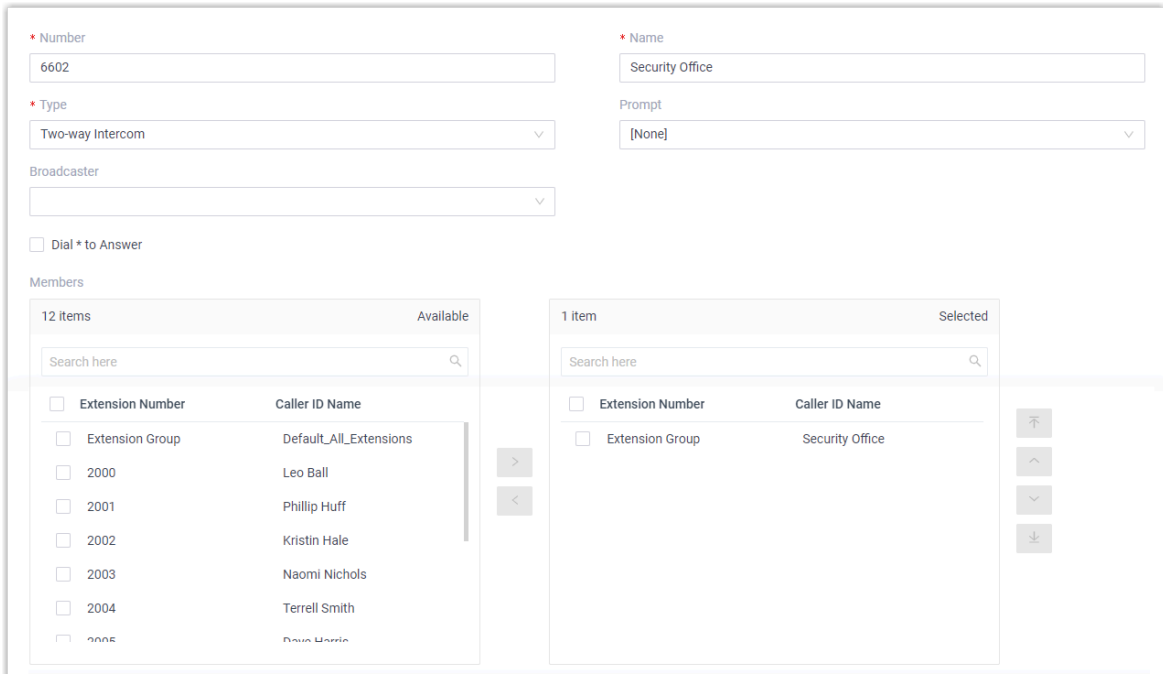
Place an intercom call to multiple users

Set up a two-way intercom group on the PBX and place a call to group numbers.

For more information, see the following instructions.

Procedure

1. Log in to PBX management portal, go to Call Features > Paging/Intercom, click Add.
2. Configure a two-way intercom group.



The screenshot displays the configuration interface for a two-way intercom group. The form is divided into several sections:

- Number:** A text input field containing "6602".
- Name:** A text input field containing "Security Office".
- Type:** A dropdown menu set to "Two-way Intercom".
- Prompt:** A dropdown menu set to "[None]".
- Broadcaster:** A dropdown menu that is currently blank.
- Dial * to Answer:** An unchecked checkbox.
- Members:** A section with two columns: "Available" (12 items) and "Selected" (1 item).
 - The "Available" column contains a search bar and a list of items with checkboxes:

Extension Number	Caller ID Name
<input type="checkbox"/>	Extension Group
<input type="checkbox"/>	2000
<input type="checkbox"/>	2001
<input type="checkbox"/>	2002
<input type="checkbox"/>	2003
<input type="checkbox"/>	2004
<input type="checkbox"/>	2005
<input type="checkbox"/>	2006
<input type="checkbox"/>	2007
<input type="checkbox"/>	2008
<input type="checkbox"/>	2009
<input type="checkbox"/>	2010
<input type="checkbox"/>	2011
<input type="checkbox"/>	2012
 - The "Selected" column contains a search bar and a list of items with checkboxes:

Extension Number	Caller ID Name
<input type="checkbox"/>	Extension Group
<input type="checkbox"/>	Security Office


- **Number:** Enter a number for the intercom group. In this example, enter 6602.
- **Name:** Enter a name for the intercom group. In this example, enter Security Office.
- **Type:** Select Two-way Intercom.
- **Prompt:** Optional. To play a prompt before making an announcement, you can select a custom prompt. In this example, leave it as None.

Note:

To customize a prompt, see [Record a Custom Prompt](#) or [Upload a Custom Prompt](#).

- **Broadcaster:** Optional. To restrict users from placing an intercom call to the intercom group, select allowed extensions or extension groups from the drop-down list. In this example, leave it blank.

- Dial * to Answer: Optional. To allow users to dial * to talk to the broadcaster privately, enable this option.

 Note:

When a user dials *, the call is ended from other users' side, and the user can have a private talk with the broadcaster.

- Members: Select desired members from Available box to Selected box. In this example, select the group Security Office.
3. Click Save and Apply.

What to do next

Dial 6602 to reach all the security guards. The security guards' phones automatically answer into speakerphone mode.


Related information

[Schedule a Paging Call or an Intercom Call](#)


Manage Paging Groups and Intercom Groups


This topic describes how to edit or delete paging groups and intercom groups.

Edit a paging/intercom group

1. Log in to PBX management portal, go to Call Features > Paging/Intercom.
2. On Paging/Intercom List page, click  beside desired group.
3. Edit group settings.
4. Click Save and Apply.

Delete a paging/intercom group

1. Log in to PBX management portal, go to Call Features > Paging/Intercom.
2. On Paging/Intercom List page, click  beside desired group.
3. Click OK and Apply.

 Note:

If you have scheduled a paging call or an intercom call for the group, the scheduled call will also be deleted.

Scheduled Paging/Intercom Call

Schedule a Paging Call or an Intercom Call

A scheduled paging call or intercom call allows Yeastar P-Series PBX System or an extension user to make an announcement at a specific date and time. For facilities that require routine notifications set in advance, you can schedule a paging call or an intercom call.


Prerequisites

You have set up a paging group or an intercom group.

- [Set up a One-way Paging Group](#)
- [Set up a One-way Multicast Paging Group](#)
- [Set up a Two-way Intercom Group](#)


Procedure

1. Log in to PBX management portal, go to Call Features > Paging/Intercom, click Scheduled Paging/Intercom tab.
2. Schedule a paging call or an intercom call.
 - a. Click Add.
 - b. Configure the following settings:
 - Paging: Select a pre-configured paging group from the drop-down list.
 - Caller: Select a broadcaster.
 - {extension_user}: The extension user will make the announcement. On the specified date and time, the PBX will place a call to the user. When the user answers the call, group members' phones directly answer into speakerphone mode.

 Note:


If the user rejects the call, the announcement will be cancelled.

- None: The PBX will make the announcement. On the specified date and time, the PBX will place a call to group members and play a specific custom prompt. After the prompt ends, the PBX hangs up. The option can be applied to school bells, church bells, etc.

 Note:

The option is available only when a custom prompt is assigned to the selected paging group or intercom group.

- Start Date: Set the start date of the scheduled paging call or intercom call.
- Time: Set the start time of the scheduled paging call or intercom call.

 Note:

You can set up to 8 timings, which means that the paging call or intercom call can be placed at different time on the same day.

- Days of Week: Select the days of week.


The scheduled paging call or intercom call will be weekly placed on the specified days of week.

- c. Click Save and Apply.


Manage Scheduled Paging Calls and Intercom Calls

This topic describes how to edit or delete scheduled paging calls and intercom calls.

Edit a scheduled paging/intercom call

1. Log in to PBX management portal, go to Call Features > Paging/Intercom.
2. On Scheduled Paging/Intercom page, click  beside desired group.
3. Edit relevant settings.
4. Click Save and Apply.

Delete a scheduled paging/intercom call

1. Log in to PBX management portal, go to Call Features > Paging/Intercom.
2. On Scheduled Paging/Intercom page, click  beside desired group.
3. Click OK and Apply.

The announcement will not be made on the specified date and time.


PIN List

Add a PIN List

A PIN list allows you to define groups and then assign a list of passwords to each group. The PIN list can be used to restrict outbound routes to enhance communication security. Users need to enter a correct PIN code when making outbound calls through a restricted outbound route.

Procedure

1. Log in to PBX management portal, go to Call Features > PIN List, click Add.
2. In the pop-up window, configure the following settings:
 - Name: Specify a name to help you identify it.
 - PIN List: Enter the PIN codes. Press the Enter key to separate multiple PIN codes.

 Note:

- The PIN code only allows numeric value.
 - The length of each PIN code is limited from 3 to 15.
- Record in CDR: Whether to record the PIN code in CDR when the PIN code has been used.

3. Click Save.

What to do next

1. Assign the PIN codes included in the PIN list to different users.
2. Select a PIN list in an outbound route to restrict outbound calls. For more information, see [Restrict Outbound Calls by PIN Codes](#).

PBX System

System Preferences

This topic describes the preference settings that will be applied globally to Yeastar P-Series PBX System.

Go to PBX Settings > Preferences to configure preferences settings.

Basic preferences

Table 32.


Setting	Description
Device Name	Set a name for the PBX. The name will be used as the sender name when PBX sends emails out.
Name Display Format	Set display format for extension user's name and contact's name. <ul style="list-style-type: none">• First Name Last Name with Space Inbetween• Last Name First Name with Space Inbetween• Last Name First Name without Space Inbetween
Max Call Duration (s)	Set the global maximum call duration for an active call. When the call duration reaches the limit, the call will be ended. The default value is 10800. <div data-bbox="511 1266 1388 1396" style="border: 1px solid #add8e6; padding: 5px;"><p> Note: For outbound calls, the Max Call Duration (s) setting of the caller's extension takes precedence.</p></div>
FXO Mode	Select a mode to set the On Hook Speed, Ringer Impedance, Ringer Threshold, Current Limiting, TIP/RING voltage, adjustment, Minimum Operational Loop Current, and AC Impedance as pre-defined for your country's analog line characteristics.
Tone Region	Select your country or the nearest neighboring country to enable the default dial tone, busy tone, and ring tone.
Flash-Hook Event	Set which event will be triggered by pressing the hook flash. <ul style="list-style-type: none">• 3-Way Calling• Call Transfer

Table 32. (continued)

Setting	Description
Virtual Ring Back Tone	If enabled, when the caller calls out via cellular trunk, the caller will hear the virtual ring back tone generated by the system before the callee answers the call.

Distinctive Caller ID Name

Table 33.

Setting	Description
Display Call Feature Name	If enabled, the Caller ID will display the originated name when users receive a call from a ring group, queue, and IVR.
Display DID/DDI Name	If enabled, the Caller ID will display the DID name of the source trunk.

DTMF preferences

Table 34.

Setting	Description
DTMF Passthrough	If enabled, PBX will pass DTMF tones directly to the other end without processing the DTMF tones.
DTMF Duration (ms)	Set the duration (in millisecond) of DTMF audio signal sent by the PBX. The default value is 120.
DTMF Gap (ms)	Set the interval (in millisecond) between two DTMF audio signals sent by the PBX. The default value is 120.

Extension preferences

Below are default extension ranges. You can change the extension range according to your needs.

Note:

PBX treats the followings as extensions. Extension users can dial extension numbers to reach them directly.

Table 35.

Extension Type	Default Range
User Extension	1000 - 5999

Table 35. (continued)

Extension Type	Default Range
Parking Extension	6000 - 6099
Group Voicemail Extension	6100 - 6199
IVR Extension	6200 - 6299
Ring Group Extension	6300 - 6399
Queue Extension	6400 - 6499
Conference Extension	6500 - 6599
Paging Extension	6600 - 6699
Account Trunk	6700 - 6799

Voice Prompt

Voice Prompt Overview

This topic describes the definition, types, and preference settings of voice prompt on Yeastar P-Series PBX System.

What is a voice prompt

A voice prompt is a recorded audio message that is played to callers. The voice prompt can be a request that requires callers to input data through DTMF, or an intermediary that provides instructions and directions to help callers obtain information.

Voice prompt types

Yeastar P-Series PBX System supports 3 types of voice prompt:

- **System Prompt:** System prompt is Yeastar-provided prompt to provide instructions for callers. For example, if a password is required for a meeting, users will be prompted to enter password before they successfully join the meeting.

You can use pre-defined system prompt, or change system prompt by downloading online prompts or uploading custom system prompts.

For more information, see [Change System Prompt](#) and [Customize System Prompt](#).

- **Custom Prompt:** Custom prompt can be company-specific prompt, which is used in specific call scenario. For example, when a call is forwarded to another destination, the caller will be prompted that the call is forwarded.

You can record new prompt on your phone, or upload pre-recorded prompt to the PBX.

For more information, see [Record a Custom Prompt](#) and [Upload a Custom Prompt](#).

- Music on Hold: Music on Hold (MoH) is the business practice of playing recorded music to fill the silence that would be heard by callers who have been placed on hold.

You can use pre-defined music on hold, or create a playlist and upload audio files to the PBX.

For more information, see [Set up a Custom MoH Playlist](#).

Voice prompt preference settings

Navigation path: PBX Settings > Voice Prompt > Prompt Preferences.

Table 36.






Setting	Description
Music on Hold	<p>The playlist to be played when a call is on hold.</p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: The available playlists are synchronized with playlists in Music on Hold.</p> </div>
Music on Hold for Call Forwarding	<p>The music to be played when the caller is put on hold during call forwarding.</p> <ul style="list-style-type: none"> • Music on Hold: Play Music on Hold to the caller. • Ringing Tone: Play ringing tone to the caller.
Invalid Phone Number Prompt	<p>The prompt to be played when a callee number is invalid.</p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: The available prompts are synchronized with Custom Prompt.</p> </div>
Busy Line Prompt	<p>The prompt to be played when a trunk is in use.</p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: The available prompts are synchronized with Custom Prompt.</p> </div>
Call Failure Prompt	<p>The prompt to be played when a call is failed to be sent out.</p> <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: The available prompts are synchronized with Custom Prompt.</p> </div>

Table 36. (continued)

Setting	Description
Event Notification Prompt	<p>The prompt to be played when PBX places a call to notify callee that a specific event occurs.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: The available prompts are synchronized with Custom Prompt.</p> </div>
Play Call Forwarding Prompt	Whether to inform the user that the current call will be forwarded.

System Prompt

Change System Prompt



This topic describes how to download an online prompt and change it to the default system prompt.

Prerequisites

Make sure that Yeastar P-Series PBX System can access the Internet.

Procedure

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > System Prompt.
2. Download the desired system prompt.
 - a. Click Download Online Prompts.

All the supported system prompts are displayed on Download Online Prompts page.
 - b. Select a prompt, click .
 - c. Click  to close the window.

The downloaded prompt is displayed on System Prompt list.
3. In the Default column, set the desired system prompt to default.
4. Click Save and Apply.

Result

The prompt is applied to the system.

Customize System Prompt

This topic describes how to customize system prompt and change it to the default prompt.

Background information

Yeastar P-Series PBX System provides [multiple online prompts](#) for your choice. If you want to use custom system prompt, you need to contact Yeastar Support to record your own prompt, and upload it to your PBX.

Prerequisites

- Contact Yeastar Support to record your own prompt.
- The prompt file must meet the following requirements:
 - File Type: `.tar`
 - File Name: Special characters are NOT allowed.
 - File Size: Up to 100 MB

Procedure

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > System Prompt.
2. Upload the custom system prompt.
 - a. Click Upload System Prompts.
 - b. In the pop-up window, select a `.tar` file from your local PC, click Open.

The uploaded prompt file is displayed on System Prompt list.
3. In the Default column, set the desired system prompt to default.
4. Click Save and Apply.

Result

The prompt is applied to the system.

Music on Hold

Set up a Custom MoH Playlist

Yeastar P-Series PBX System has a default playlist with built-in MoH files. This topic describes how to set up and use a custom MoH playlist.

Prerequisites

The audio files to be uploaded must meet the following requirements:

- File format: `.wav`, `.mp3`, or `.gsm`

- PCM, 8K, 16bit, 128kbps
- A-law(g.711), 8k, 8bit, 64kbps
- u-law(g.711), 8k, 8bit, 64kbps



Tip:


If file format does not meet the requirement, you can [convert audio files via WavePad](#) or [G711 File Converter online](#).

- File size: Up to 8MB



Limitations

- Max. MoH playlists: 16
- Max. audio files in a playlist: 8

Step1. Add a custom MoH playlist

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > Music on Hold.
2. Create a new playlist.
 - a. Click Create New Playlist.
 - b. In the pop-up window, configure the playlist.
 - Playlist Name: Enter a name to help you identify it.
 - Play Order: Decide whether to play the playlist alphabetically or randomly.
 - c. Click Save.
3. Add one or more audio files to the playlist.
 - a. Select the created playlist, click .
 - b. In the pop-up window, click Upload.
 - c. Choose the desired audio file, click Open.
 - d. Optional: To add more audio files, repeat step b-c.

The uploaded audio files are displayed on the MoH Files list.

4. Optional: Check sound quality and completeness of the audio files.
 - a. On MoH Files page, select the desired audio file, click .
 - b. In the pop-up window, set where to play the audio file.
 - In the Play on Web section, click  to play the audio file.
 - In the Extension drop-down list, select an extension and click Play.

PBX will call and play the audio file to the extension.
 - c. Click OK.
5. Click Apply.

Step2. Change the system MoH playlist

1. Click Prompt Preferences tab.

2. In the Music on Hold drop-down list, select the desired playlist.
3. Click Save and Apply.



Result

When a call is on held, the system will play audio files in the playlist to the waiting party.

Manage MoH Playlist and Audio Files




This topic describes how to edit or delete a MoH playlist, and manage MoH audio files.


Manage a MoH playlist

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > Music on Hold.
2. Manage a MoH playlist.
 - To edit a MoH playlist, do as follows:
 - a. Select the desired playlist, click .
 - b. Edit the playlist according to your needs.
 - Playlist Name: Change the playlist name.
 - Play Order: Decide whether to play the playlist alphabetically or randomly.
 - c. Click Save and Apply.
 - To delete a MoH playlist, do as follows:
 - a. Select the desired playlist, click .
 - b. In the pop-up dialog box, click OK.
 - c. Click Apply.

If the deleted playlist is used for [Music on Hold](#) or [Music on Hold for Call Forwarding](#), the system will not play audio file to the party who is put on hold during a call or call forwarding.

Manage MoH audio files

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > Music on Hold.
2. Manage MoH audio files.
 - a. In the Operations column, click  beside the desired MoH playlist.
 - b. In the pop-up window, manage MoH audio files according to your needs.
 - To upload an audio file, click Upload and select the desired file.
 - To listen to an audio file, click , decide whether to play the audio file to an extension or on web.
 - To download an audio file, click .

- To delete an audio file, click .
- c. Click OK.

Configure Call Forwarding Prompt

This topic describes how to configure call forwarding prompt.

Background information

Call forwarding prompt is used to prompt a caller that the call is forwarded to another destination. By default, when PBX is forwarding an incoming call to another number, the PBX will play the call forwarding prompt "please hold when I try to locate the person you are calling", and then play the MoH music. If you do not want the caller to find out that the call is being forwarded, you can disable Play Call Forwarding Prompt.

Procedure

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > Prompt Preferences.
2. Unselect the checkbox of Play Call Forwarding Prompt.
3. Optional: To change MoH music, select Music on Hold or Ringing Tone from the drop-down list of Music on Hold for Call Forwarding.



Note:

The Music on Hold is the playlist that you have defined in Music on Hold (PBX Settings > Voice Prompt > Prompt Preferences > Music on Hold).

4. Click Save and Apply.

Custom Prompt

Record a Custom Prompt

This topic describes how to record a custom prompt on a phone.

Prerequisites

At least one extension is ready for use.

Limitation

Up to 32 custom prompts are supported on the PBX.

Procedure

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > Custom Prompt.
2. Record a custom prompt.

- a. Click Record New.

A window pops up.

- b. In the Name field, enter a name to help you identify the prompt.
- c. In the Extension drop-down list, select an extension to record the prompt.
- d. Click Record.

The system places a call to the selected extension. After you answer the call, you will hear a prompt for the recording.



- e. Record your prompt on the phone.

When done, hang up or press the # key.

Result

Refresh the web page and click Custom Prompt tab.

The recorded prompt is displayed on the Custom Prompt page.

- To listen to the prompt, click .
- To change the voice content, click  to record again.

Upload a Custom Prompt

This topic describes how to upload a custom prompt.

Prerequisites

Prepare an audio file that meets the following requirements:

- File format: `.wav`, `.mp3`, or `.gsm`
 - PCM, 8K, 16bit, 128kbps
 - A-law(g.711), 8k, 8bit, 64kbps
 - u-law(g.711), 8k, 8bit, 64kbps

Tip:

If the audio file does not meet the requirements, you can [convert the audio file via WavePad or G711 File Converter online](#).

- File size: Up to 8MB.

Limitation

Up to 32 custom prompts are supported on the PBX.

Procedure

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > Custom Prompt.
2. Click Upload.
3. In the pop-up window, select an audio file from your local PC and click Open.





Result

The uploaded file is displayed on Custom Prompt page.

Manage Custom Prompts

This topic describes how to manage custom prompts, such as re-record, play, download, and delete a prompt.

Procedure

1. Log in to PBX management portal, go to PBX Settings > Voice Prompt > Custom Prompt.
2. In the Operations column, manage custom prompts according to your needs.
 - To re-record a prompt, click , select an extension to record.
 - To listen to a prompt, click , decide whether to play the audio file to an extension or on web.
 - To download a prompt, click .
 - To delete a prompt, click , click OK and Apply.

Convert Audio Files

This topic describes how to convert audio files via WavePad or G711 File Converter online.

Background information

Audio files to be uploaded as MoH files or custom prompts must [meet the requirements](#). If your audio file does not meet the requirement, you can use audio editor to convert file format.

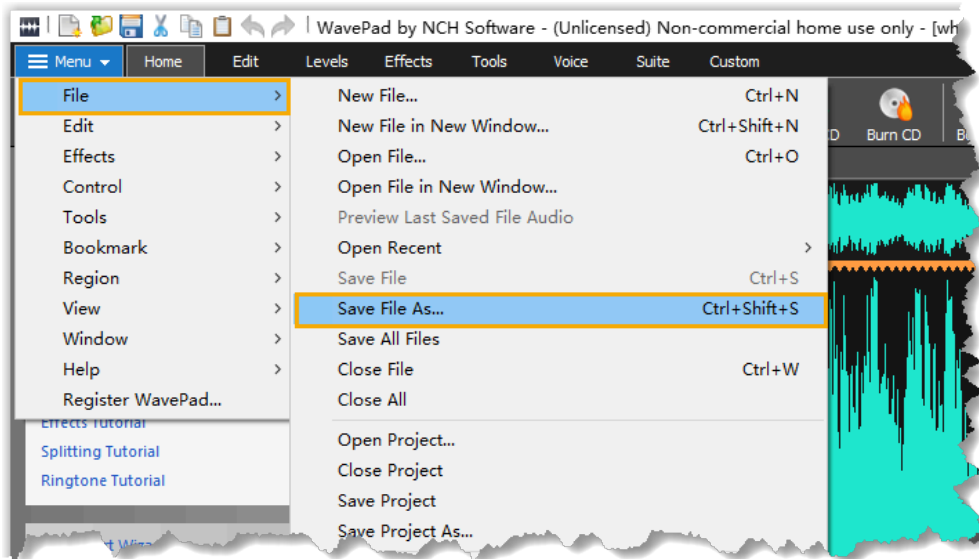
In this topic, we take the followings as examples to show you how to convert file format.

- [Convert Audio Files via WavePad](#)
- [Convert Audio Files Online](#)

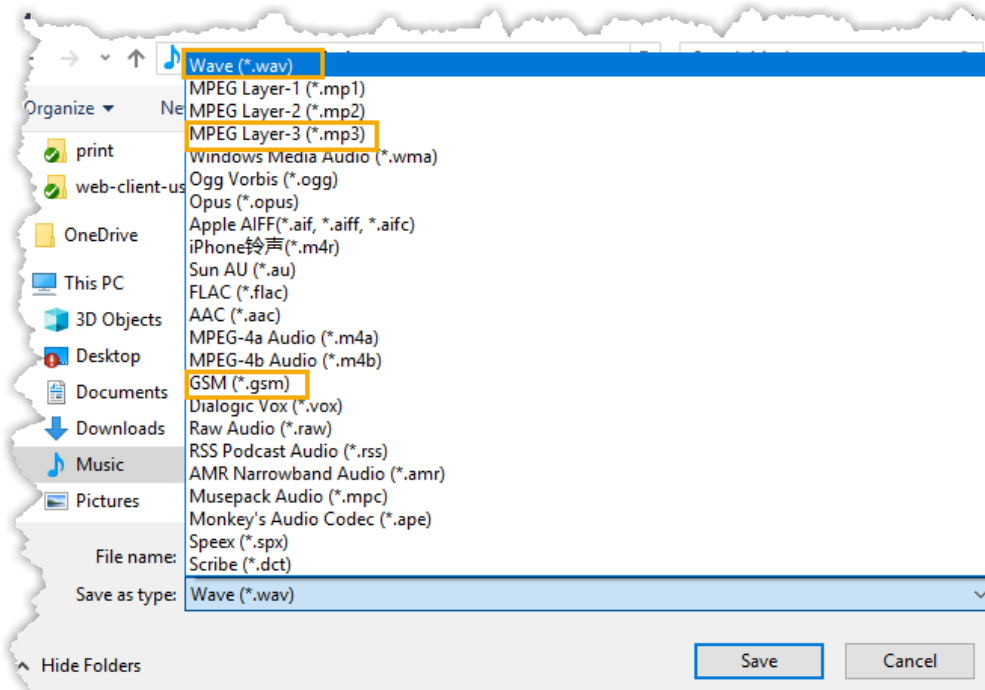
Convert audio files via WavePad

To use WavePad to convert audio files to new formats, download [WavePad](#) to your local PC, and proceed as follows.


1. Launch WavePad, open your audio file.
2. Click File > Save File As.



3. In the Save as type drop-down list, select Wave (*.wav), MPEG Layer-3 (*.mp3), or GSM (*.gsm), click Save.

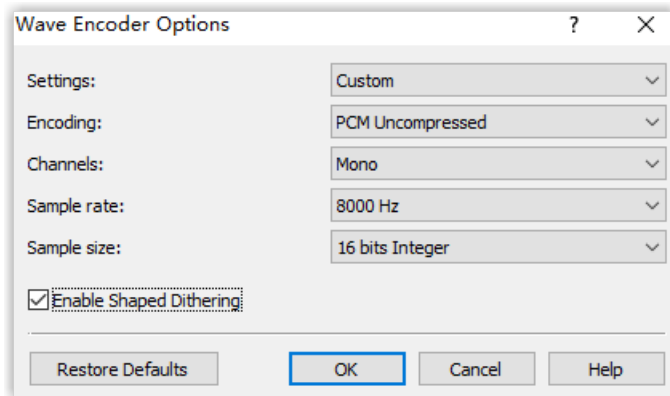


4. If you save the audio file as `Wave (*.wav)` or `MPEG Layer-3 (*.mp3)`, you need to configure the encoder options and click OK.

 **Note:**

Select any one of the encoders, and configure relevant options as below.


- PCM Uncompressed, Mono, 8000 Hz, 16 bits Integer
- CCITT A-law, Mono, 8000 Hz, 8 bits Integer
- CCITT u-law, Mono, 8000 Hz, 8 bits Integer



Convert audio files online

If you don't want to download an app, you can quickly convert your audio files via G711 File Converter online.

1. Go to g711.org.
2. Click Browse to upload your audio file.
3. Set the Output Format.

 **Note:**

Select any one of u-law WAV (8Khz, Mono, u-law), a-law WAV (8Khz, Mono, a-law), and Standard Definition WAV (8Khz, Mono, 16-Bit PCM).

4. Click Submit to start converting the file.

Audio Files Requirements

This topic describes the requirements for audio files to be uploaded to Yeastar P-Series PBX System.

Applications of audio files

You may need to upload a custom audio file in the following scenarios:

- Voicemail greetings
- Custom prompt
- Music on hold

Audio file requirements

Audio files to be uploaded to the PBX must meet the following requirements:

Option	Requirement
File Name	Should NOT contain special characters.
File Size	Up to 8 MB.

Option	Requirement
File Format	<p data-bbox="505 268 764 296">.wav, .mp3, Or .gsm.</p> <ul data-bbox="565 342 987 447" style="list-style-type: none"> • PCM, 8K, 16bit, 128kbps • A-law (g.711), 8k, 8bit, 64kbps • u-law (g.711), 8k, 8bit, 64kbps

SIP Settings

This topic describes the SIP settings on the Yeastar P-Series PBX System for reference.

The SIP configurations require professional knowledge of SIP protocol, incorrect configuration may cause calling issues on the SIP extensions and SIP trunks.

Go to PBX Settings > SIP Settings to configure SIP settings.

SIP general settings

Table 37.





Setting	Description
Basic Settings	
SIP UDP Port	<p data-bbox="540 1087 1362 1115">UDP Port used for SIP registration. The default value is 5060.</p> <div data-bbox="540 1157 1390 1283" style="border: 1px solid #ccc; padding: 5px;"> <p data-bbox="540 1167 662 1194"> Note:</p> <p data-bbox="540 1209 1354 1276">If you change the port, the extensions that use UDP protocol must re-register to the new port.</p> </div>
SIP TCP Port	<p data-bbox="540 1308 1362 1409">TCP Port used for SIP registration. The default value is 5060. To change the port, select the checkbox of SIP TCP Port and set the port.</p> <div data-bbox="540 1451 1390 1577" style="border: 1px solid #ccc; padding: 5px;"> <p data-bbox="540 1461 662 1488"> Note:</p> <p data-bbox="540 1503 1354 1570">If you change the port, the extensions that use TCP protocol must re-register to the new port.</p> </div>
RTP Port Range	<p data-bbox="540 1598 1227 1656">RTP port for transmitting data. The default range is 10000-12000.</p> <div data-bbox="540 1698 1390 1824" style="border: 1px solid #ccc; padding: 5px;"> <p data-bbox="540 1709 662 1736"> Note:</p> <ul data-bbox="602 1793 1308 1820" style="list-style-type: none"> • The From-port value should be greater than 10000. </div>


Table 37. (continued)

Setting	Description
	<ul style="list-style-type: none"> The From-port and the To-port should have a difference value between 100 and 10000.
Outbound SIP Port Range	<p>To prevent from being blocked by carrier due to overloaded calls and subscriptions, you can specify an outbound SIP port range. PBX will select a port from the range to register to the carrier. The default range is 5062-5082.</p> <p>To change the port, select the checkbox of Outbound SIP Port Range and set the port.</p>
SIP Endpoint Registration Timer	
Max Registration Time (s)	Maximum duration (in seconds) of incoming registrations and subscriptions.
Min Registration Time (s)	Minimum duration (in seconds) of incoming registrations and subscriptions.
Qualify Frequency (s)	How often to send SIP OPTIONS packet to SIP device to check if the device is up.
Outbound SIP Registration Timer	
Registration Attempts	The number of registration attempts before giving up (0 indicates no limit).
Default Registration Time(s)	<p>Default registration duration (in seconds).</p> <p> Note: The actual duration needs to subtract 10 seconds from the value you fill in.</p>
SIP Endpoint Subscription Timer	
Max Subscription Time(s)	Maximum duration (in seconds) of incoming subscriptions.
Min Subscription Time(s)	Minimum duration (in seconds) of incoming subscriptions.


SIP codec


A codec is a compression or decompression algorithm used in the transmission of voice packets over a network or the Internet.

Table 38.

Setting	Description
iLBC Mode	<p>The iLBC codec supports the following modes:</p> <ul style="list-style-type: none"> • 20 ms • 30 ms <p>To get better voice quality, you need to set the iLBC mode according to your SIP endpoints.</p>
Codec Selection	<p>Select the codec. Available values: u-law, a-law, GSM, H264, VP8, H263, H263P, i-LBC, G722, G726, SPEEX, ADPCM, G729A, MPEG4.</p> <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> Note:</p> <ul style="list-style-type: none"> • To ensure that users can have audio calls on Linkus Web Client, you must enable at least any one of u-law, a-law, or G722. • To ensure that users can have video calls on Linkus Web Client after you subscribe Yeastar P-Series Ultimate Plan, you must enable either VP8 or H264. We recommend that you enable VP8 or set VP8 to a higher priority. </div>

TLS settings

Setting	Description
TLS	Enable or disable TLS.
SIP TLS Port	TLS port used for SIP registration. The default value is 5061.
When PBX acting as a Sever	
TLS Certificate	Upload a server certificate when PBX acts as a server.
TLS Verify Client	Verify client certificate when PBX acts as a server.
	<div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> Note: If enabled, you need to upload a client certificate to the PBX and TLS client.</p> </div>
When PBX acting as a Client	
TLS Connection Method	Specify a protocol for outbound client connections.

Setting	Description
	<ul style="list-style-type: none"> • TLS V1.0 • TLS V1.2
TLS Verify Server	Verify server certificate when PBX acts as a client. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Note: If enabled, you need to upload a server certificate to the PBX. </div>

Session Timer

A periodic refreshing of a SIP session that allows both user agent and proxy to determine if the SIP session is still active.

Setting	Description
Session Timer	Select a session timer mode. <ul style="list-style-type: none"> • No: Do not include “timer” value in any field. • Supported: Include “timer” value in Supported header. • Required: Include “timer” value in Required header. • Forced: Include “timer” value in both Supported and Required header.
Session-Expires (s)	The max refresh interval in seconds.
Min-SE (s)	The min refresh interval in seconds. The value should not be smaller than 90.

QoS

Quality of Service (QoS) is a major issue in VoIP implementations. The issue is how to guarantee that packet traffic for a voice or other media connection will not be delayed or dropped due to interference from other traffic of lower priority.

When the network capacity is insufficient, QoS can provide users with priority by setting the value.

Setting	Description
ToS (Type of Service)	
ToS SIP	Type of Service for SIP packets.
ToS Audio	Type of Service for RTP audio packets.
ToS Video	Type of Service for RTP video packets.

Setting	Description
CoS (Class of Service)	
Cos SIP	Class of Service for SIP packets.
Cos Audio	Class of Service for RTP audio packets.
Cos Video	Class of Service for RTP video packets.




T.38

Adjust T.38 settings if T.38 Fax doesn't work.

Setting	Description
T.38 Max BitRate	Adjust the max BitRate for T.38 fax.
No T.38 Attributes in re-IN-VITE SDP	If enabled, SDP re-invite packet will not contain T.38 attributes.
Error Correction Mode	Enable or disable Error Correction for the fax.

Advanced SIP settings

Setting	Description
Incoming Caller ID/DID Retrieval	
Get Caller ID From	Decide the system will retrieve Caller ID from which header field. <ul style="list-style-type: none"> • From • Contact • Remote-Party-ID • P-Asserted-Identity • P-Preferred-Identity
Get DID From	Decide the system will retrieve DID from which header field. <ul style="list-style-type: none"> • To • Invite • Diversion • Remote-Party-ID • P-Asserted-Identity • P-Preferred-Identity • P-Called-Party-ID

Setting	Description
	<p> Note: If Remote-Party-ID is selected but the SIP trunk doesn't support this, the system will retrieve DID from Invite header.</p>
SIP Request Header	
User Agent	Set the user agent that will be included when sending SIP packages out.
Internal Alert Info	<p>Set an "alert info text" to add to Alert-info header in INVITE request for internal calls.</p> <p>When receiving an internal call, the phone will inspect "Alert-Info" header to determine which ring tone it should use for ringing.</p>
Other Options	
Allow Guest	If enabled, PBX will accept unknown calls.
Support Message Request	Whether to support SIP Message Request or not.
Inband Progress	<p>Whether to enable inband progress or not. The Inband Progress setting applies to all the extensions.</p> <p> Note: To configure global Inband Progress setting, you need to contact Yeastar support to configure a custom configuration file.</p> <ul style="list-style-type: none"> • Check this option: PBX will send a 183 Session Progress to the extension when told to indicate ringing and immediately start sending ringing as audio. • Uncheck this option: PBX will send a 180 Ringing to the extension when told to indicate ringing, but will NOT send it as audio.
Enable uaCSTA Connection	<p>If this option is enabled, the PBX will allow user agent Computer Supported Telecommunications Application (uaCSTA) to remotely control the IP phone via Linkus Web Client CTI or Linkus Desktop Client CTI.</p> <p> Note: Your IP phone should support uaCSTA standard to use this function.</p>

Jitter Buffer

Jitter Buffer Overview

This topic describes what is and when to use jitter buffer, and introduces two jitter buffer types supported on Yeastar P-Series PBX System.

What is jitter buffer

Jitter is a variation between the time that voice packets are sent and received. For example, two packets may arrive at the same time, or out of order due to network congestion, which can cause the problem of audio quality. In this case, jitter buffer can be used to arrange packets according to their expected timing values.

Jitter buffer types

Yeastar P-Series PBX System supports two types of jitter buffer:

- Fixed jitter buffer: The fixed jitter buffer has a fixed size and the packets leaving the jitter buffer have a constant delay.
- Adaptive jitter buffer: Adapting to network's delay, the adaptive jitter buffer has a variable size and the packets leaving the jitter buffer have a variable delay.

When to use jitter buffer

If you have networking issues like packet loss or packets arriving out of order, you can enable jitter buffer to improve call quality.

Packets loss

If the packets are partially lost, the jitter buffer inserts the lost frame and passes them on in an evenly spaced continuous stream.

Packets arriving out of order

If the arriving packets are out of order, the jitter buffer inserts the packets into the buffer in the correct order, and passes them on in the expected order.

For more information of jitter buffer configuration, see [Configure Jitter Buffer](#).

Configure Jitter Buffer

This topic describes how to configure jitter buffer on Yeastar P-Series PBX System.

Background information

If you have networking issues like [packet loss](#) or [packets arriving out of order](#), you can enable jitter buffer to improve call quality.

Procedure

1. Log in to PBX management portal, go to PBX Settings > Jitter Buffer.
2. Enable Jitter Buffer.
3. To enable jitter buffer for trunks, select the desired trunks from Available box to Selected box.

The outbound audio through the selected trunk will be dejittered on the other side.

4. To enable jitter buffer for extensions, select the desired extensions from Available box to Selected box.

The received audio on the selected extensions will be dejittered.

Note:

Jitter buffer doesn't work in the following situations:

- In an internal call, the audio is received from an analog phone.
- In an external call, the other side sends audio through a non-SIP trunk, and jitter buffer is not enabled for the trunk.

5. In the Implementation drop-down list, select the implementation of jitter buffer.
 - Adaptive: Adapting to network's delay, the adaptive jitter buffer has a variable size and the packets leaving the jitter buffer have a variable delay. If you choose the option, specify the adjustment size and the max jitter buffer size as follows.
 - Adaptive Adjustment Size (ms): The size of each adaptive adjustment of jitter buffer. The default value is 50. If you retain the default value, the jitter buffer size will be adjusted dynamically based on current network condition. It will start from 0 ms and grow at a size of 50 ms each time.
 - Max Jitter Buffer Size (ms): The maximum value of adaptive jitter buffer. The default value is 200.
 - Fixed: The fixed jitter buffer has a fixed size and the packets leaving the jitter buffer have a constant delay.

If you choose the option, enter a value in the Jitter Buffer Size (ms) field. The default value is 200.
6. Click Save and Apply.

Network

Basic Network

Basic Network Overview

This topic describes the network modes in Yeastar P-Series PBX System.

Ethernet modes

Yeastar P-Series PBX System provides LAN interface and WAN interface. By default, the LAN interface is enabled, and the WAN interface is disabled. You can configure the following Ethernet modes for the system:

- Single: Only LAN port is used for connection, WAN port is disabled.
- Bridge: LAN port is used for connection. WAN port will be used as bridge for PC connection.
- Dual: Both LAN port and WAN port are used for connection.
If you use Dual mode, you need to specify a default network interface for the PBX.

Note:

The traffic will be routed to the default interface, you need to [add a static route](#) to override the default route entries, routing the traffic from a specific IP address to the specified destination.

IP address assignment

Yeastar P-Series PBX System supports three types of IP address assignment:

- Assign a static IP address

Contact your network administrator to assign an IP address to the PBX. Then you need to manually configure settings such as the IP address, subnet mask, default gateway, and DNS servers on the PBX.

- Obtain an IP address from a DHCP server

You can configure the PBX to automatically obtain an IP address when it starts up from a DHCP server running in your network.

Note:

The IP address assigned to the PBX may vary every time the PBX is started up.

- Obtain an IP address from a PPPoE client

You can connect the PBX to a PPPoE client, and set up a PPPoE connection on the PBX to get an IP address.

Note:

The IP address assigned to the PBX may vary every time the PPPoE is started up.

Configure a Static IP Address

This topic describes how to configure a static IP address for Yeastar P-Series PBX System.

Background information

The default IP address of Yeastar P-Series PBX System is 192.168.5.150. According to your network environment, you may need to change the IP address to the same network segment of your local network.

The following instructions assume that you need to use LAN port of Yeastar P-Series PBX System to send and receive network traffic. The IP information is as below:

- IP address: 192.168.6.124
- Subnet mask: 255.255.255.0
- Gateway address: 192.168.6.1
- DNS server: 192.168.1.1

Prerequisites

- PBX and PC are connected to the same local network.
- Your PC has ability to access the default network segment 192.168.5.X of the PBX.

i Tip:
To access the PBX, you need to change your PC to the same network segment of the PBX.

Procedure

1. Log in to PBX management portal, go to System > Network > Basic Settings.
2. In the Basic section, configure the following settings:

The screenshot shows a configuration window titled 'Basic'. It contains two dropdown menus. The first is labeled 'Ethernet Mode' and is currently set to 'Single'. The second is labeled 'Default Interface' and is currently set to 'LAN'.


- Ethernet Mode: Select the Ethernet mode. In this scenario, select Single.
 - Single: Only the LAN port is used for up-link connection.
 - Dual: Both LAN and WAN are used for up-link connection.

Note:
The traffic will be routed to the default interface; you may need to [add a static route](#) to override the default route entries, routing the traffic from a specific IP address to the specified destination.

- Bridge: LAN port is used for up-link connection. WAN port can be used as a bridge to connect other device.
- Default Interface: Optional. Select a default interface if you select Dual mode.

- In the LAN section, select Static IP Address, and enter the network information for LAN port.

- IP Address: Enter the IP address that is assigned to the PBX.
- Subnet Mask: Enter the subnet mask.
- Gateway: Enter the gateway address.
- Preferred DNS Server: Enter the IP address of preferred DNS server.
- Alternative DNS Server: Optional. Enter the IP address of alternative DNS server.
- IP Address 2: Optional. Enter a second IP address for the PBX.

 Note:

According to your network environment, you may need to set another IP address to allow users in different IP segment to access the PBX.

- Subnet Mask 2: Optional. Enter another subnet mask for the second IP address.
- Click Save and reboot the PBX to take effect.

Result

After the PBX reboots, the PBX's IP is changed to 192.168.6.124.

What to do next

To access the PBX, change your PC's IP to the same network segment of the PBX, for example, 192.168.6.110.

Obtain an IP Address from a DHCP Server

This topic describes how to configure Yeastar P-Series PBX System to automatically obtain an IP address from a DHCP server running in your network.

Background information

If you choose this method to configure IP address for the PBX, the IP address assigned to the PBX may vary every time the PBX starts up. We suggest that you configure a static IP address for the PBX. For more information, see [Configure a Static IP Address](#).

The following instructions assume that you connect an Ethernet cable to LAN port of Yeastar P-Series PBX System and need to obtain an IP address from the local DHCP server.

Prerequisites

- DHCP feature is enabled on your router.
- Only one DHCP server in the local network, or the PBX cannot get the IP address.

Procedure

1. Log in to PBX management portal, go to System > Network > Basic Settings.
2. In the Basic section, configure the following settings:

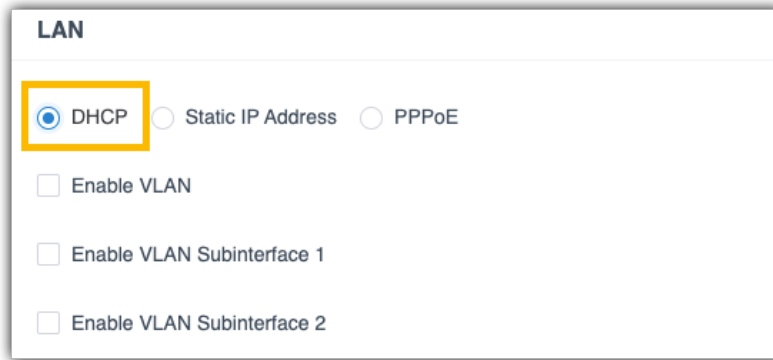
The screenshot shows a configuration window titled 'Basic'. It contains two dropdown menus. The first is labeled 'Ethernet Mode' and is set to 'Single'. The second is labeled 'Default Interface' and is set to 'LAN'.

- Ethernet Mode: Select the Ethernet mode. In this scenario, select Single.
 - Single: Only the LAN port will be used for up-link connection.
 - Dual: Both LAN and WAN can be used for up-link connection.

Note:

The traffic will be routed to the default interface; you may need to [add a static route](#) to override the default route entries, routing the traffic from a specific IP address to the specified destination.

- Bridge: LAN port will be used for up-link connection. WAN port can be used as a bridge to connect other device.
 - Default Interface: Select a default interface if you select Dual mode.
3. In the LAN section, select DHCP.



4. Click Save and reboot the PBX to take effect.

Result

The PBX's IP address will obtain a new IP address from the DHCP server in your local network.

You need to log in to the web interface of your router, and check which IP address is assigned to the PBX.

Configure a PPPoE Connection

This topic describes how to configure a PPPoE connection on Yeastar P-Series PBX System to obtain an IP address when the PBX is in Dual network mode.

Background information

A PPPoE client assigns a dynamic IP address to the PBX, the IP address of the PBX may vary every time the PBX starts up. In this case, you need to configure dual network, and configure a static IP address on the PBX to ensure that you can always access the PBX.

The following instructions assume that you need to connect LAN port to local network, connect WAN port to PPPoE. The network information is as the following:


LAN	WAN
Static IP <ul style="list-style-type: none"> • IP address: 192.168.6.124 • Gateway address: 192.168.6.1 • Subnet mask: 255.255.255.0 • DNS: 192.168.1.1 	PPPoE <ul style="list-style-type: none"> • Username: 059219383822 • Password: 19283772

Procedure

1. Log in to PBX management portal, go to System > Network > Basic Settings.

2. In the Basic section, configure the following settings:

- Ethernet Mode: Select the Ethernet mode. In this scenario, select Dual.
 - Single: Only the LAN port will be used for up-link connection.
 - Dual: Both LAN and WAN can be used for up-link connection.

 Note:

The traffic will be routed to the default interface; you may need to [add a static route](#) to override the default route entries, routing the traffic from a specific IP address to the specified destination.

- Bridge: LAN port will be used for up-link connection. WAN port can be used as a bridge to connect other device.
 - Default Interface: Select the port where PPPoE is connected. In the scenario, select WAN.
3. In the LAN section, select Static IP Address, and enter the network information for LAN port.

LAN

DHCP
 Static IP Address
 PPPoE


* IP Address: * Subnet Mask:

* Gateway:

* Preferred DNS Server: Alternative DNS Server:

IP Address 2: Subnet Mask 2:

- IP Address: Enter the IP address that is assigned to the PBX.
- Subnet Mask: Enter the subnet mask.
- Gateway: Enter the gateway address.
- Preferred DNS Server: Enter the IP address of preferred DNS server.
- Alternative DNS Server: Optional. Enter the IP address of alternative DNS server.
- IP Address 2: Optional. Enter a second IP address for the PBX.

 Note:

According to your network environment, you may need to set another IP address to allow users in different IP segment to access the PBX.

- Subnet Mask 2: Optional. Enter another subnet mask for the second IP address.
4. In the WAN section, select PPPoE and enter the Username and Password.

WAN

DHCP
 Static IP Address
 PPPoE

* Username: 059219383822

* Password: 19283772

5. Click Save and reboot the PBX to take effect.

Result

Both LAN and WAN are set up for the PBX.

- All network traffic will be sent and received by the WAN port (default network interface).
- You can access the PBX management portal by the LAN IP address to configure the PBX settings.

What to do next

If you want to route network traffic through LAN port, you need to add static routes on the PBX. For more information, see [Add a Static Route](#).

Configure a VLAN on Yeastar P-Series PBX System

This topic describes how to configure a VLAN on Yeastar P-Series PBX System.

Background information

VLAN allows you to segment out a physical network into virtual networks with different subnets. For example, one network is used by one department and another network is used by another department.

VLAN feature on the Yeastar P-Series PBX System is used to filter network traffic. Only the devices that have the same VLAN ID can communicate with the PBX. You can set up VLAN on LAN interface or WAN interface. To allow network traffic from multiple subnets, you can add VLAN sub interfaces on the PBX.

- [Configure a VLAN for LAN/WAN port](#)
- [Add a VLAN subinterface](#)

Configure a VLAN for a network interface

The following instructions assume that you need to set a VLAN for LAN port, and the network information of the LAN port is as the following. You want to restrict that only the devices with VLAN ID 100 can communicate with the PBX.

- IP address: 192.168.6.124
- Gateway address: 192.168.6.1
- Subnet mask: 255.255.255.0

Procedure

1. Log in the PBX management portal, go to System > Network > Basic Settings.
2. Configure the Ethernet port that needs to set up a VLAN.

In the scenario, configure LAN port.

- a. In the LAN section, select the checkbox of Enable VLAN.
- b. In the VLAN ID field, enter an ID for the PBX. In this example, enter 100.

Note:

The devices that need to communicate with the PBX should have the same VLAN ID.

- c. In the drop-down list of VLAN Priority, select the priority value that is associated with the VLAN ID.

The priority value is between 0 to 7. 7 has the highest priority.

The screenshot shows the LAN configuration interface. At the top, there are three radio buttons: DHCP, Static IP Address (selected), and PPPoE. Below this, there are several input fields: IP Address (192.168.6.124), Subnet Mask (255.255.255.0), Gateway (192.168.6.1), Preferred DNS Server (192.168.1.1), and Alternative DNS Server. There are also fields for IP Address 2 and Subnet Mask 2. At the bottom, there is a section for VLAN configuration. The 'Enable VLAN' checkbox is checked and highlighted with a yellow box. Below it, the 'VLAN ID' field contains '100' and the 'VLAN Priority' field contains '0'.

3. Click Save and reboot the PBX to take effect.

Result

Only the device that is in the same local network segment 192.168.6.X and has the same VLAN ID 100 can communicate with the PBX.

Add a VLAN subinterface

A VLAN subinterface is a virtual interface created by dividing one physical Ethernet interface (LAN or WAN) into multiple logical interfaces.

If the PBX has only one physical Ethernet interface, but needs to route traffic via two different subnets, you can configure VLAN for the main interface (LAN or WAN) and add a VLAN subinterface with a different subnet.

The following instructions assume that you need to add a VLAN subinterface for LAN interface.

- Main interface (LAN): For network traffic in subnet 192.168.6.0/24 with VLAN ID 100.
- Sub interface: For network traffic in subnet 192.168.5.0/24 with VLAN ID 105.

Procedure

1. Log in the PBX management portal, go to System > Network > Basic Settings.
2. Configure the Ethernet port that needs to set up a VLAN.
 - a. In the LAN section, select the checkbox of Enable VLAN.
 - b. In the VLAN ID field, enter an ID for the PBX. In this example, enter 100.

Note:

The devices that need to communicate with the PBX should have the same VLAN ID.

- c. In the drop-down list of VLAN Priority, select the priority value that is associated with the VLAN ID.

The priority value is between 0 to 7. 7 has the highest priority.

The screenshot shows the LAN configuration interface. At the top, there are radio buttons for DHCP, Static IP Address (selected), and PPPoE. Below are fields for IP Address (192.168.6.124), Subnet Mask (255.255.255.0), Gateway (192.168.6.1), Preferred DNS Server (192.168.1.1), and Alternative DNS Server. There are also empty fields for IP Address 2 and Subnet Mask 2. A yellow box highlights the 'Enable VLAN' checkbox (checked), the 'VLAN ID' field (100), and the 'VLAN Priority' field (0).

3. In the LAN section, select the checkbox of Enable VLAN Subinterface 1 and configure the following settings.
 - IP Address: Assign an IP address that is in the subnet 192.168.5.0/24, for example, 192.168.5.20
 - Subnet Mask: Enter the subnet mask. In this scenario, enter 255.255.255.0.

- VLAN ID: Assign a VLAN ID for the sub interface, for example, enter 105.
- VLAN Priority: Set a priority for the VLAN ID, for example, enter 0.

Enable VLAN Subinterface 1

* IP Address: 192.168.5.20

* Subnet Mask: 255.255.255.0

* VLAN ID: 105

* VLAN Priority: 0

4. Click Save and reboot the PBX to take effect.

Result

- The network traffic from subnet 192.168.6.0/24 and has VLAN ID 100 will be routed to the PBX VLAN interface.
- The network traffic from subnet 192.168.5.0/24 and has VLAN ID 105 will be routed to the VLAN sub interface.

Web Server

Change Web Server Protocol and Port

This topic describes how to change the web protocol and port of Yeastar P-Series PBX System.

Background information

By default, the PBX uses HTTPS 8088 port for web service, and allows redirecting from HTTP 80 port.

When you need to access the PBX management portal, you can type one of the following URLs:

- `https://{pbx_ip}:8088`
For example, `https://192.168.5.150:8088`
- `http://{pbx_ip}`
For example, `http:192.168.5.150`

Procedure

1. Log in to PBX management portal, go to System > Network > Web Server.

2. In the Protocol section, complete the following configurations:
 - a. In the drop-down list of Protocol, select a protocol.
 - b. If HTTPS is selected, configure the following settings:
 - HTTPS Port: Enter a HTTPS port.
 - HTTPS Certificate: Select the default certificate or upload your own certificate.
 - Redirect from HTTP 80 port: Decide whether to allow requests to HTTP port 80.

If the option is enabled, the requests to HTTP port 80 will be redirected to the respective HTTPS service.
 - c. If HTTP is selected, enter the HTTP port in the HTTP Port field.
3. Click Save and Apply.

Result

The next time, you need to access the PBX management portal by the configured protocol and port.

Change Automatic Logout Time

For security purposes, Yeastar P-Series PBX System automatically logs out a user session after 15 minutes if no operation is performed on the web page. You can change this session logout period.

Prerequisites

Automatic Logout feature is only for the super administrator. The system will not automatically log out an extension user from web client.

Procedure

1. Log in to PBX management portal, go to System > Network > Web Server.
2. In the Logout Time section, select a value from the drop-down list of Auto Logout Time (min).

 Tip:

You can also enter a custom value in the text field directly. The valid value is from 5 to 120 minutes.

3. Click Save.

Service Ports

Manage Service Ports of the PBX

This topic describes the services and the relevant service ports used on the Yeastar P-Series PBX System and how to manage the ports centrally.

Background information

The following table describes the PBX's services and the default ports.

Service	Description	Default Port
HTTPS	HTTPS port for web service.	8088
HTTP	HTTP port for web service.	80
SSH	SSH port is used to access the PBX underlying configurations to debug the system.	8022
SIP UDP	SIP registration port for UDP protocol.	5060
SIP TCP	SIP registration port for TCP protocol.	5060
SIP TLS	SIP registration port for TLS protocol.	5061
Outbound SIP Port	A random port in the port range will be used when sending packets to a SIP server.	5062-5082
RTP	RTP ports for transmitting voice audio stream.	10000-12000
Linkus	Port for logging in to Linkus clients.	8111
AMI	Port for third party to access the AMI of PBX.	5038
Database Grant	Port for third party to access the PBX database.	3306

Procedure

The settings of different services are in different web page, however, you can check or edit the ports centrally on the PBX.

1. Log in to PBX management portal, go to System > Network > Service Ports.

All the service ports are displayed on the web page.

2. To configure a port, click [🔗](#).

You will be redirected to the configuration page of the service.

- a. Enter a new value of the service port.
- b. Click Save and Apply.

Yeastar FQDN

Configure Network for Remote Access by a Yeastar FQDN

A Yeastar-supplied Fully Qualified Domain Name (FQDN) frees you from complicated network settings and helps you quickly establish a secure tunnel for remote access. You can create a Yeastar FQDN in the PBX to allow remote access within seconds.

Background information

A Fully Qualified Domain Name (FQDN) is the complete domain name for a specific device on the internet. An FQDN consists of two parts: the hostname and the domain name.

Yeastar-supplied FQDN function has the following advantages and limitations.

Advantages

- For the network environment that has no static public IP address, a Yeastar-supplied FQDN implements a dynamic DNS service for you.
- Simplify network configurations for remote access as the complicated Network Address Translation (NAT) configurations and port forwarding are eliminated.
- Secure remote connections with SSL certificates.

Limitations

Yeastar FQDN is only for Linkus remote access and web remote access.

Prerequisites

You have subscribed Yeastar P-Series Enterprise Plan or Ultimate Plan.

Procedure

1. Log in to PBX management portal, go to System > Network > Yeastar FQDN.
2. Turn on Yeastar FQDN.
3. In the Fully Qualified Domain Name (FQDN) field, select a domain name then enter a hostname.

For example, select domain name ras.yeastar.com and enter hostname yeastardocs, you will get an FQDN yeastardocs.ras.yeastar.com

Note:

Think twice before you enter the hostname. The FQDN cannot be changed after you save the configurations.

Yeastar FQDN

Remote Access Service is a subscription-based service designed to set your team up for anywhere-anytime productivity instantly and securely. It provides an easy-to-access domain name, safeguards PBX remote web access, and allows the remote workforce to enjoy a consistent in-office unified communications experience with Linkus UC Clients anywhere on any device. [Buy Plan](#)

Status

• Disconnected

* Fully Qualified Domain Name (FQDN)

yeastardocs ras.yeastar.com


* Expiration Date

🟢 The domain name is available.

4. Click Save.

Result

- Linkus server is automatically set up for remote access, users can use Linkus (Mobile Client, Desktop Client, and Web Client) anywhere anytime.

 **Note:**

For Linkus Mobile Client and Desktop Client, the App version should be updated:

- Linkus Android version: 3.6.9 or later
- Linkus iOS version: 3.6.8 or later
- Linkus Windows version: 2.4.8 or later
- Linkus MacOS version: 2.4.8 or later

- Network for remote web access is automatically configured, users can log in to the PBX management portal remotely via the FQDN.

What to do next

If your subscription trial period is up or the subscription is not renewed on time, your FQDN will be suspended. To ensure that your FQDN won't be taken by others, you need to subscribe or renew Yeastar P-Series Enterprise Plan or Ultimate Plan in 60 days.

Public IP and Ports

Public IP and Ports Overview

This topic describes when you need to configure the Public IP and Ports settings and introduces two functions of Public IP and Ports settings.

Applications

When your PBX is connected behind a router and needs to communicate with SIP devices on the external network, you need to set Public IP and Ports settings. Public IP and Port settings can be applied to different types of networks:

- [Public IP Address](#)
- [External Host](#)

Public IP Address

If your Internet Service Provider (ISP) provides a static public IP address, you can configure PBX network for remote access with the IP address.

For more information about the configurations, see [Configure Network for Remote Access by a Domain Name](#).

External Host

If static public IP address is not available in your network environment, you must have a registered domain name, and configure PBX network for remote access with the domain name.

For more information about the configurations, see [Configure Network for Remote Access by a Public IP Address](#).

Functions


Public IP and Ports settings have the following two functions to ensure that remote devices can access and communicate with the PBX via SIP protocol:

- [Solve SIP NAT issue](#)
- [Provide PBX with information of Linkus remote access](#)

Solve SIP NAT issue

If your PBX is connected behind a router, it can be said that the PBX is behind a Network Address Translation (NAT) router. To allow remote devices to access the PBX, you need to set up NAT rules and port forwarding on the router. In this way, the router will forward the right inbound packets from the internet to the PBX.

SIP-based communication does not reach devices in the Local Area Network (LAN) behind firewalls and NAT routers automatically. Public IP and Ports settings on the Yeastar P-Series PBX System provide a SIP NAT solution to ensure that SIP data can be transmitted correctly between the PBX and the public internet.

 Note:

Yeastar P-Series PBX System doesn't support NAT feature, you need to set up NAT rules and port forwarding on your router.

NAT process

When a request is sent to the public internet, that request will have a source address consistent with the local LAN address (for example, 192.168.6.124).

That local IP address will not be publicly routable because it is a private IP address. NAT replaces the local source IP address with a public IP address which is routable on the public internet.

SIP NAT

NAT only replaces a local IP address with a public IP address for IP header in a data packet, but not for SIP headers, which may cause one-way audio issue for SIP calls or SIP registration failure.

To solve the SIP issues, you need to configure Public IP and Ports on the PBX. PBX will replace local IP address with public IP address and replace local SIP port with external SIP port before sending the packets to the public internet.

Provide PBX with information of Linkus remote access

The Public IP and Ports configurations allow Linkus remote access by solving SIP NAT issue. In addition, Yeastar P-Series PBX System can generate QR codes and links for Linkus remote access based on the information provided on the Public IP and Ports page.

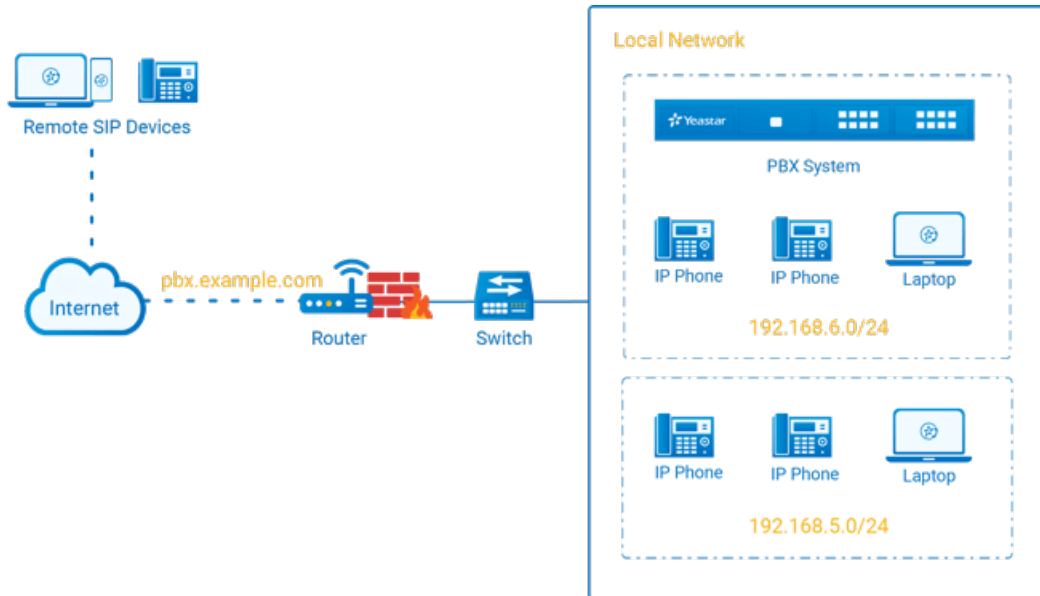
Configure Network for Remote Access by a Domain Name

To ensure that remote Linkus clients and other SIP devices can communicate with Yeastar P-Series PBX System normally, you need to configure Public IP and Ports on the PBX. This topic provides a configuration example based on the network scenario that no static public IP address is available and a domain name is set up for remote connection.

Background information

This topic assumes that your network environment is as follows:

- Domain name: pbx.example.com
- Local network:
 - 192.168.6.0/24
 - 192.168.5.0/24



Prerequisites

- You have purchased Dynamic DNS, and bound the domain name with your router.
- If SIP ALG option is provided in your router, disable it.
- You have configured NAT settings and forwarded the following ports to allow remote access of Linkus clients and other SIP devices. To check the relevant internal ports of your PBX, see [Manage Service Ports of the PBX](#).

In this scenario, forward the following ports:

Service	Internal Port	External Port
SIP registration	UDP 5060	UDP 8092
RTP	UDP 10000-12000	UDP 10000-12000
Linkus server	TCP&UDP 8111	TCP&UDP 6090
Linkus web client	TCP 8088	TCP 9099

Procedure

Based on the scenario, configure the Public IP and Ports on PBX as follows.

1. Log in to PBX management portal, go to System > Network > Public IP and Ports.
2. In Public IP (NAT) section, complete the following configurations:
 - Public IP (NAT): Turn on this option.
 - NAT Type: Select External Host.
 - External Host: Enter pbx.example.com.

- Refresh Interval (s): Leave the default setting or change the interval (in seconds) for PBX to request the external host for public IP.
- Local Network Identification: Add all your local network. This setting will allow all your local devices to communicate with the PBX by the local IP address instead of passing through the router.

In this scenario, add two local network: 192.168.5.0/255.255.255.0 and 192.168.6.0/255.255.255.0.

- NAT Mode: Select a SIP NAT mode. In this scenario, select Yes.
 - Yes: Use NAT and ignore the address information in the SIP/SDP headers and reply to the sender's IP address and port.
 - No: Use NAT mode only according to RFC3581.
 - Never: Never attempt NAT mode or RFC3581 support.
 - Route: Use NAT but do not include rport in headers.

Public IP (NAT)

* NAT Type
External Host

* External Host
pbx.example.com

* Refresh Interval (s)
120

Local Network Identification

Network Number	Subnet Mask	Operations
192.168.5.0	255.255.255.0	⊗
192.168.6.0	255.255.255.0	⊗

+ Add IP

* NAT Mode
Yes

3. In the Public Ports section, enter the external ports that you have forwarded on your router.

- External SIP UDP Port: Enter 8092.
- External SIP TCP Port: Leave it blank because SIP TCP protocol is not used in this scenario.
- External SIP TLS Port: Leave it blank because SIP TLS protocol is not used in this scenario.
- External Linkus Port: Enter 6090.
- External Web Server Port: Enter 9099.

Public Ports	
External SIP UDP Port <input type="text" value="8092"/>	External SIP TCP Port <input type="text"/>
External SIP TLS Port <input type="text"/>	External Linkus Port <input type="text" value="6090"/>
External Web Server Port <input type="text" value="9099"/>	

4. Click Save.

Result

- Users can remotely access the PBX management portal and log in to Linkus clients via the domain name.
- Remote devices based on SIP protocol can register to the PBX via the domain name.
- PBX will generate login links and QR codes for Linkus remote access based on the information provided on the Public IP and Ports page.



Note:

If you have [configured network for remote access by a Yeastar FQDN](#), the login links and QR codes are generated based on the FQDN.

Related information

- [Configure Network for Remote Access by a Yeastar FQDN](#)
- [Configure Network for Remote Access by a Public IP Address](#)
- [Set up a Remote SIP Phone](#)

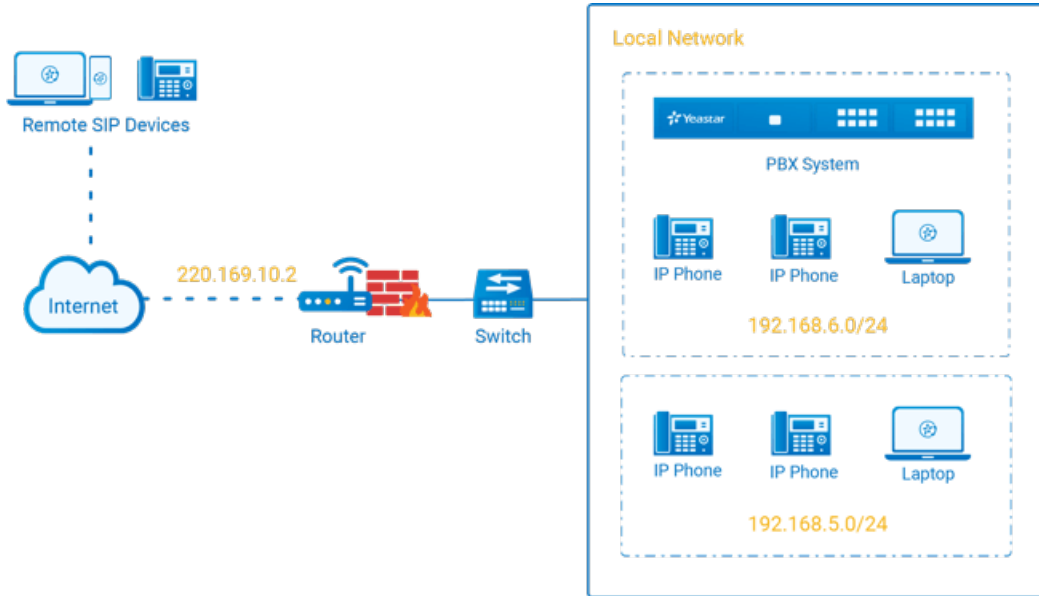
Configure Network for Remote Access by a Public IP Address

To ensure that remote Linkus clients and other SIP devices can communicate with Yeastar P-Series PBX System normally, you need to configure Public IP and Ports on the PBX. This topic provides a configuration example based on the network scenario that a static public IP address is supplied by the Internet Service Provider (ISP).

Background information

This topic assumes that your network environment is as follows:

- Public IP address: 220.169.10.2
- Local network:
 - 192.168.6.0/24
 - 192.168.5.0/24



Prerequisites

- If SIP ALG option is provided in your router, disable it.
- You have configured NAT settings and forwarded the following ports to allow remote access of Linkus clients and other SIP devices. To check the relevant internal ports of your PBX, see [Manage Service Ports of the PBX](#).

In this scenario, forward the following ports:

Service	Internal Port	External Port
SIP registration	UDP 5060	UDP 8092
RTP	UDP 10000-12000	UDP 10000-12000
Linkus server	TCP&UDP 8111	TCP&UDP 6090
Linkus web client	TCP 8088	TCP 9099

Procedure

Based on the scenario, configure the Public IP and Ports on PBX as follows.

1. Log in to PBX management portal, go to System > Network > Public IP and Ports.
2. In Public IP (NAT) section, complete the following configurations:
 - Public IP (NAT): Turn on this option.
 - NAT Type: Select Public IP Address .
 - Public IP Address: Enter 220.169.10.2.

- **Local Network Identification:** Add all your local network. This setting will allow all your local devices to communicate with the PBX by the local IP address instead of passing through the router.

In this scenario, add two local network: 192.168.5.0/255.255.255.0 and 192.168.6.0/255.255.255.0.

- **NAT Mode:** Select a SIP NAT mode. In this scenario, select Yes.
 - **Yes:** Use NAT and ignore the address information in the SIP/SDP headers and reply to the sender's IP address and port.
 - **No:** Use NAT mode only according to RFC3581.
 - **Never:** Never attempt NAT mode or RFC3581 support.
 - **Route:** Use NAT but do not include rport in headers.

Public IP (NAT)

* NAT Type
Public IP Address

* Public IP Address
220.169.10.2

Local Network Identification

Network Number	Subnet Mask	Operations
192.168.5.0	255.255.255.0	⊗
192.168.6.0	255.255.255.0	⊗
+ Add IP		

* NAT Mode
Yes

3. In the Public Ports section, enter the external ports that you have forwarded on your router.


- **External SIP UDP Port:** Enter 8092.
- **External SIP TCP Port:** Leave it blank because SIP TCP protocol is not used in this scenario.
- **External SIP TLS Port:** Leave it blank because SIP TLS protocol is not used in this scenario.
- **External Linkus Port:** Enter 6090.
- **External Web Server Port:** Enter 9099.

Public Ports	
External SIP UDP Port <input type="text" value="8092"/>	External SIP TCP Port <input type="text"/>
External SIP TLS Port <input type="text"/>	External Linkus Port <input type="text" value="6090"/>
External Web Server Port <input type="text" value="9099"/>	

4. Click Save.

Result

- Users can remotely access the PBX management portal and log in to Linkus clients via the public IP address.
- Remote devices based on SIP protocol can register to the PBX via the public IP address.
- PBX will generate login links and QR codes for Linkus remote access based on the information provided on the Public IP and Ports page.

 **Note:**
If you have [configured network for remote access by a Yeastar FQDN](#), the login links and QR codes are generated based on the FQDN.

Related information

[Configure Network for Remote Access by a Domain Name](#)

[Configure Network for Remote Access by a Yeastar FQDN](#)

[Set up a Remote SIP Phone](#)

Static Route

Static Route Overview

This topic provides an overview of static route table and all associated system routes.

Route table

Yeastar P-Series PBX System provides a route table that contains default system route entries and custom route entries.

Default system entries

After you configure the system network, the system automatically adds system routes to the route table for traffic management. You cannot delete the system routes.

For more information, see [System route entries](#).

Custom route entries

If the system is in Dual network mode, you need to add a static route to override the default system routes, routing the packets from specific IP address to the specified destination. For more information, see [Add a Static Route](#).

System route entries

System route entries are automatically added after you configure the PBX network. The following route entries are considered as system route entries:

- A default route entry. The packets that are destined to any unknown destinations will be routed to the default gateway.
- A route entry destined for the IP address range of LAN or WAN interface. The packets that are destined to the IP address range can be sent directly to the destination.

Example:

The following example describes the automatically added system routes.

Network settings

Both LAN interface and WAN interface are enabled, and LAN is the default interface. The detailed network information is as the followings.

	LAN (Default Interface)	WAN
IP address	192.168.6.124	10.10.1.18
Subnet mask	255.255.255.0	255.255.255.0
Gateway	192.168.6.1	10.10.1.1
Preferred DNS Server	192.168.1.1	10.10.1.1

System route entries

The following route entries are automatically added to the routing table of the PBX.

Destination	Subnet Mask	Gateway	Metric	Interface	Operations
default	0.0.0.0	192.168.6.1	0	LAN	
10.10.1.0	255.255.255.0	0.0.0.0	0	WAN	
192.168.6.0	255.255.255.0	0.0.0.0	0	LAN	

- The route entry with the Destination of `default` is the default route entry. By default, all the packets will be routed to the gateway `192.168.6.1` through LAN interface.
- The route entry with the Destination of `10.10.1.0/255.255.255.0` is the route entry that is automatically added for WAN interface.

The packets for the network `10.10.1.0/255.255.255.0` don't need to be routed. The network is locally connected, so packets can be sent directly to the destination.

- The route entry with the Destination of `192.168.6.0/255.255.255.0` is the route entry that is automatically added for LAN interface.

The packets for the network `192.168.6.0/255.255.255.0` don't need to be routed. The network is locally connected, so packets can be sent directly to the destination.

Add a Static Route

This topic gives a configuration example to show you how to add a static route on Yeastar P-Series PBX System.

Background information

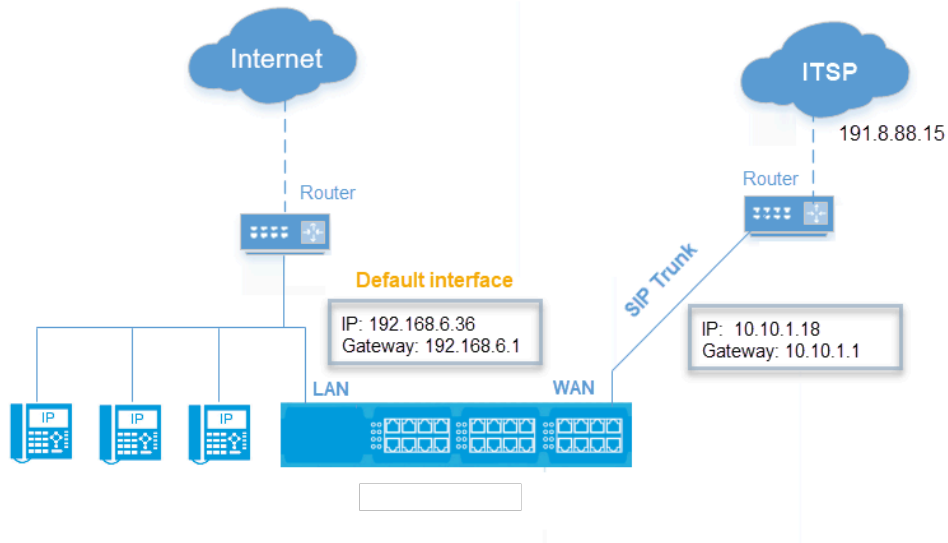
Adding custom static route is typically used in the "Dedicated SIP trunking" scenario.

This topic assumes that you have bought a dedicated SIP trunk from the Internet Telephony Service Provider (ITSP) . The ITSP provides a router for the dedicated SIP trunk. The router is used for the SIP trunk only, but cannot access the Internet.

Network topology

The following figure shows the network topology for the dedicated SIP trunking on the PBX.

- All network traffic goes through the default interface LAN.
- The network traffic of SIP trunking `191.8.88.15` will go through the WAN port.



PBX Network settings

Setting	Value
Ethernet Mode	Dual
Default Interface	LAN
LAN	
IP Address	192.168.6.36
Subnet Mask	255.255.255.0
Gateway	192.168.6.1
Preferred DNS Server	192.168.1.1
WAN	
IP Address	10.10.1.18
Subnet Mask	255.255.255.0
Gateway	10.10.1.1
Preferred DNS Server	10.10.1.1

Procedure

To route the network traffic of SIP trunking 191.8.88.15 through WAN port, you need to add a static route on the PBX. Follow the instructions below to add a static route for SIP trunking.

1. Log in to PBX management portal, go to System > Network > Static Routes, click Add.


2. On the pop-up window, configure the route entry:

The screenshot shows a dialog box titled "Add Static Route" with a close button (X) in the top right corner. The dialog contains the following fields and values:

- Destination:** 191.8.88.0
- Subnet Mask:** 255.255.255.0
- Gateway:** 10.10.1.1
- Metric:** (empty)
- Interface:** WAN (selected from a dropdown menu)

At the bottom right of the dialog, there are two buttons: "Cancel" (with an X icon) and "Save" (with a floppy disk icon).

- **Destination:** Enter the destination IP address or IP subnet for the PBX to reach using the static route.

 **Note:**

To ensure that both SIP registration packets and SIP media packets can be routed to the desired destination, set the IP range of the SIP trunking. In this scenario, enter 191.8.88.0.

- **Subnet Mask:** Enter the subnet mask for the destination address. In this scenario, enter 255.255.255.0.
- **Gateway:** Enter the gateway address. The PBX will reach the destination address through this gateway. In this scenario, enter 10.10.1.1.
- **Metric:** Optional.

Routing metric is used to determine whether one route should be chosen over another.

- **Interface:** Select the network interface.

The PBX will reach the destination address using the static route through the selected network interface. In the scenario, select WAN.

3. Click Save and Apply.

Result

After you set up a SIP trunk with the IP address 191.8.88.15 on the PBX, the SIP packets are sent and received by the WAN port, which ensure the communication between the PBX and the ITSP.

What to do next

To avoid SIP audio issues through the SIP trunk, you may need to add the network segment of the SIP trunk as a local network identification in PBX NAT settings.


In this scenario, add the IP segment 191.8.88.0/255.255.255.0 in the NAT settings as the following figure shows. For more information of NAT, see [Configure Network for Remote Access by a Domain Name](#).

Local Network Identification		
network number	Subnet Mask	Operations
192.168.6.0	255.255.255.0	⊗
191.8.88.0	255.255.255.0	⊗


Manage Static Routes

After you add static routes on the Yeastar P-Series PBX System, you can edit or delete them.

Edit a static route

1. Log in to PBX management portal, go to System > Network > Static Routes.
2. Click  beside the static route that you want to edit.
3. Edit the static route settings.
4. Click Save.

Delete a static route

1. Log in to PBX management portal, go to System > Network > Static Routes.
2. Click  beside the static route that you want to delete.
3. Click Yes to confirm the deletion.

DHCP Server

Set up PBX as a DHCP Server

Yeastar P-Series PBX System provides a built-in DHCP server. When there is no DHCP server in the local network, you can set up the PBX as a DHCP server to assign IP addresses, gateway, DNS and other network parameters to devices in the same local network .

Prerequisites

Make sure there is only one DHCP server running in the local network.

Procedure

1. Log in to PBX management portal, go to System > Network, click DHCP Server tab.
2. Turn on the DHCP Server on the top.
3. Complete the following network configurations.

* Gateway	192.168.5.1	* Subnet Mask	255.255.255.0
* Preferred DNS Server	192.168.5.1	Alternative DNS Server	
* DHCP Address Range	192.168.5.2 - 192.168.5.254	* NTP Server	192.168.5.150

- Gateway: Specify the IP address of the default gateway for the DHCP server.
- Subnet Mask: Specify the subnet mask used to subdivide your IP address.
- Preferred DNS Server: Specify a DNS server for the DHCP server.
- Alternative DNS Server: Optional. Specify a secondary DNS server for the DHCP server.
- DHCP Address Range: Specify the IP address range that will be allocated to DHCP clients.
- NTP Server: Enter the IP address of an NTP server.

i Tip:

The default value is the IP address of the PBX, which can synchronize the network time of the client devices with the PBX.

4. Click Save.

The Status field displays Running, indicating the DHCP server is running.

Result

The PBX can now be used as a DHCP server and assign IP addresses, gateway, and other network configurations to the devices located in the local network.

Date and Time

Change System Time Manually

In case you want to change system time when the PBX can not access the Internet, you can change system time manually. This topic describes how to manually change system time to your local time.

Background information

To ensure that the time of logs and CDRs generated on Yeastar P-Series PBX System is consistent with your local time, you need to adjust system time to your local time.

Procedure

1. Log in to PBX management portal, go to System > Date and Time.
2. In the Date and Time section, set your local date and time.
 - a. In the Time Zone drop-down list, select your current time zone.
 - b. Optional: Configure Daylight Saving Time according to your needs.
 - c. Choose Set Up Manually and set the date and time.
3. In the Display Format section, set the display format of date and time.
 - Date Display Format
 - Year/Month/Day
 - Month/Day/Year
 - Day/Month/Year
 - Time Display Format
 - 12-hour format
 - 24-hour format
4. Click Save and Apply.
5. Reboot the PBX to take effect.

Result

The current system time is updated; the time of logs and CDRs are also updated.

Synchronize System Time with an NTP Server

If the PBX can access the Internet, you can use an NTP server to synchronize system time. This topic describes how to synchronize system time with an NTP server.

Background information

To ensure that the time of logs and CDRs generated on Yeastar P-Series PBX System is consistent with your local time, you need to adjust system time to your local time.

Prerequisites

Make sure Yeastar P-Series PBX System can access the Internet.

Procedure

1. Log in to PBX management portal, go to System > Date and Time.
2. In the Date and Time section, configure the following settings:
 - a. In the Time Zone drop-down list, select your current time zone.
 - b. Optional: Configure Daylight Saving Time according to your needs.
 - c. Choose Synchronize with NTP Server.
 - d. Retain the default value of NTP Server or enter the URL of an NTP server.
3. In the Display Format section, set the display format of date and time.
 - Date Display Format
 - Year/Month/Day
 - Month/Day/Year
 - Day/Month/Year
 - Time Display Format
 - 12-hour format
 - 24-hour format
4. Click Save and Apply.
5. Reboot the PBX to take effect.

Result

The current system time is updated; the time of logs and CDRs are also updated.

Email Server

Email Server Overview

This topic describes SMTP server, email template, email daily sending limit, and email sent logs.

Email server

Emails to users or the administrator are required in the following situations:

- Send Linkus welcome email.
- Send fax to email.
- Send voicemail to email.

- Send event notifications.

You can use the built-in Yeastar SMTP server or custom SMTP server to send emails.

For the built-in SMTP server, see [Set up Yeastar SMTP Server as an Email Server](#).

For the custom SMTP server, see [Set up Gmail as an Email Server](#) and [Set up Outlook as an Email Server](#).

Email template

Yeastar P-Series PBX System has default email templates for different events, you can also customize email templates according to your needs.

For more information, see [Customize Email Templates](#).

Email daily sending limit

If you use custom email server to send emails, you need to know that email server may limit the number of emails that users can send per day to keep system healthy and account safe.

Yeastar P-Series PBX System obtains the quantity from the email server. If reaching the sending limit, users can NOT send emails via the email server.

Email sent logs

Yeastar P-Series PBX System provides email sent logs, which allows you to monitor mail delivery, and offers you error messages to help you troubleshoot delivery issues more quickly.

For more information, see [Email Sent Logs](#).

Set up Yeastar SMTP Server as an Email Server

This topic describes how to set up Yeastar SMTP server as the email server of Yeastar P-Series PBX System.

Prerequisites

Make sure Yeastar P-Series PBX System can access the Internet.

Procedure

1. Log in to PBX management portal, go to System > Email > Email Server.
2. In the Type of Email Server drop-down list, select Yeastar SMTP Server.
3. Test if the email server can successfully send emails.
 - a. Click Test.
 - b. In the pop-up window, enter a recipient's email address in the Email Address field.
 - c. Click Test.

Result

- If the test email is sent successfully, the page displays "Success" and the recipient's mailbox would receive the email.
- If the test email is failed to be sent, the page displays "Failed to send" and prompts you an error message. You can check the error in [Email Sent Logs](#).

Set up Gmail as an Email Server

This topic describes how to set up Gmail as an email server in Yeastar P-Series PBX System.

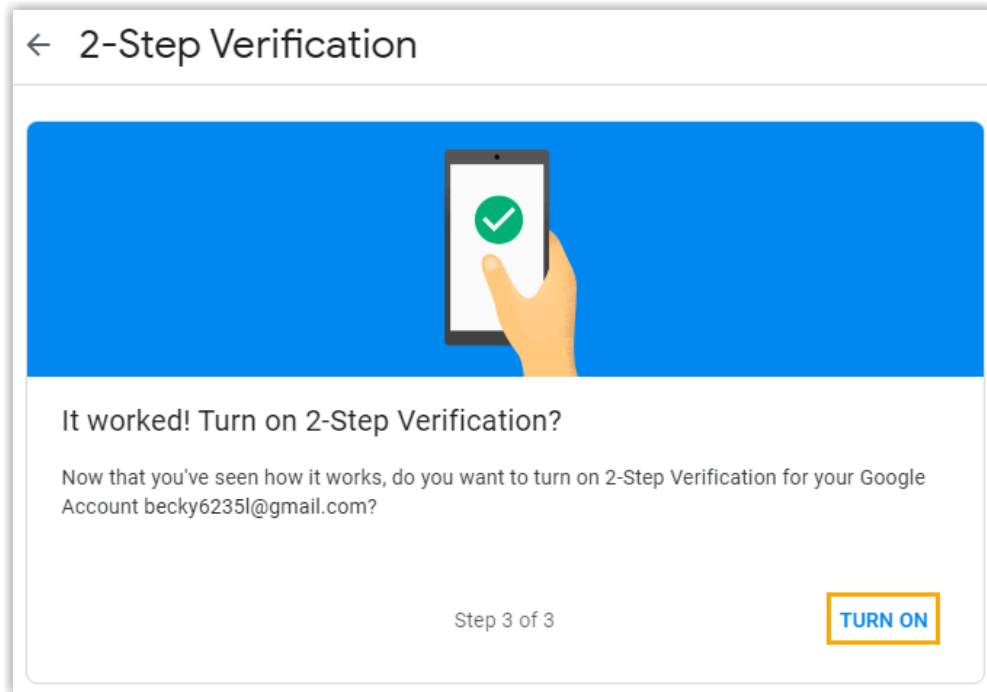
Prerequisites

Make sure Yeastar P-Series PBX System can access Google Server.

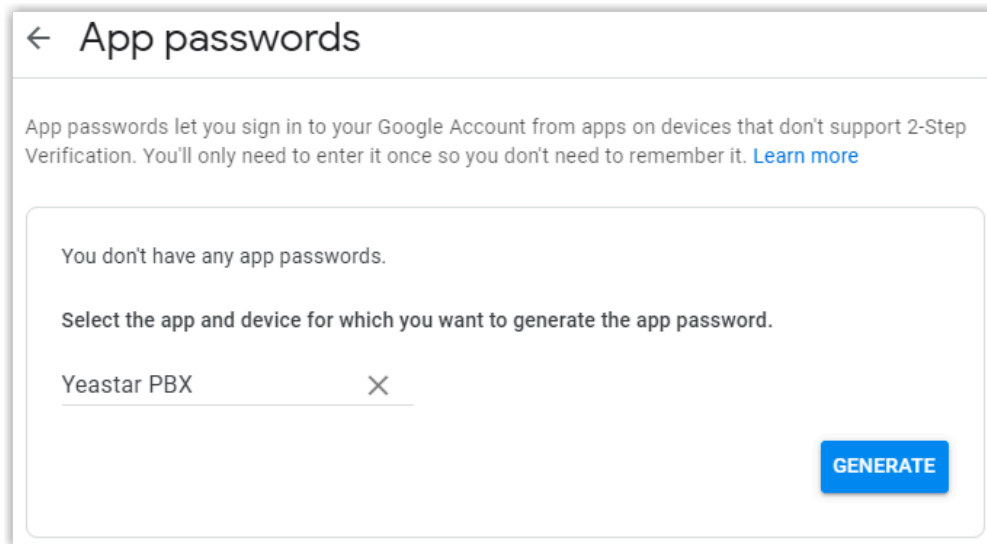
Step1. Create an app password on Google Account

To ensure that the PBX can access Gmail server, you need to turn on 2-Step verification and create an app password as follows.

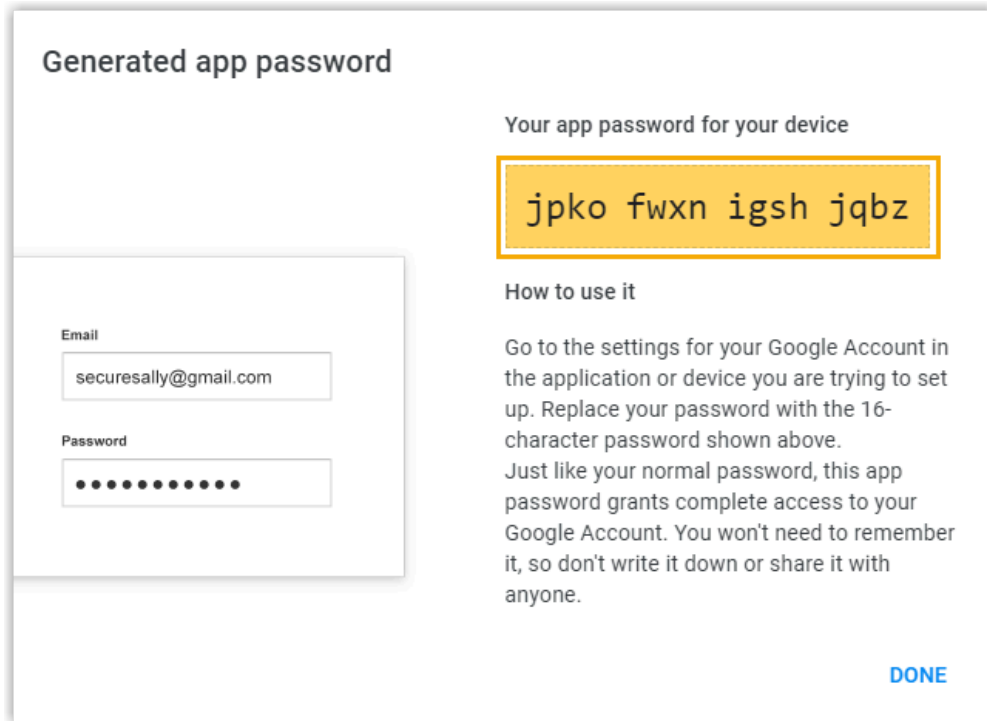
1. Sign in to [Google Account](#) by your Gmail account.
2. On the left navigation bar, click Security.
3. Turn on 2-Step Verification.
 - a. In the Signing in to Google section, click 2-Step Verification and enter your Gmail password to verify your account.
 - b. On the 2-Step Verification page, click GET STARTED and enter your Gmail password to verify your account.
 - c. Select a verification method, verify your account according to the prompt.
 - d. Click TURN ON to turn on 2-step verification.



4. Right above the page, click ← to back to the security page.
5. Create an app password.
 - a. In the Signing in to Google section, click App passwords and enter your Gmail password to verify your account.
 - b. In the Select app drop-down list, select Other (Custom name).
 - c. In the text field, enter a name to help you identify the app password. For example, enter Yeastar PBX.
 - d. Click GENERATE.



An app password is generated. Note down the password, which is used to verify your Gmail account when you configure Gmail as the mail server in the PBX.



Step2. Configure Gmail as mail server of Yeastar P-Series PBX System

To ensure that the PBX can access Gmail server via your Google account, you need to proceed as follows:

1. Log in to PBX management portal, go to System > Email > Email Server.
2. In the Type of Email Server drop-down list, select Custom Email Server.
3. Configure email server settings.
 - Sender Email Address: Enter your Gmail address, which will appear as the From address for outgoing emails sent by the PBX.
 - Email Address or Username: Enter your Gmail address.
 - Password: Enter the 16-digit app password, which is used to access Gmail server.
 - Outgoing Mail Server (SMTP): Retain the default value smtp.gmail.com.
 - Port: Retain the default value 587.
 - Enable TLS Encryption: Keep the option unselected.
4. Test if the mail server can successfully send emails.
 - a. Click Test.
 - b. In the pop-up window, enter a recipient's email address in the Email Address field.
 - c. Click Test.
5. Click Save.

Result

- If the test email is sent successfully, the page displays "Success" and the recipient's mailbox would receive the email.
- If the test email is failed to be sent, the page displays "Failed to send" and prompts you an error message. You can check the error in [Email Sent Logs](#).

Set up Outlook as an Email Server

This topic describes how to set up Outlook as an email server in Yeastar P-Series PBX System.

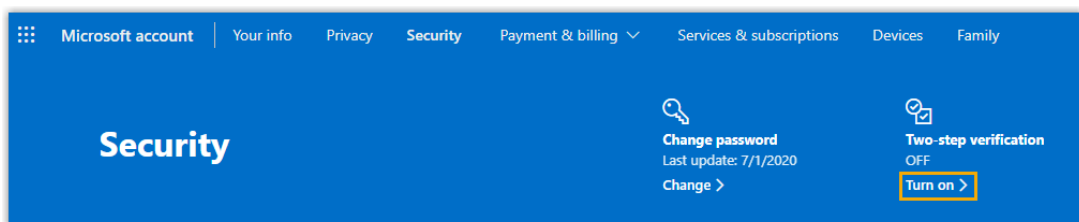
Prerequisites

Make sure the PBX can access the Internet.

Step1. Create an app password on Microsoft Account

To ensure that PBX can access Outlook server via your Microsoft account, you need to turn on 2-Step verification and create an app password as follows.

1. Sign in to [Microsoft Account](#).
2. At the top navigation bar, click Security tab and enter your Outlook password to verify your account.
3. Turn on 2-Step Verification.
 - a. In the Two-step verification section, click Turn on, and verify your account according to the prompt.



- b. In the Two-step verification section, click Set up two-step verification.
 - c. Read the tips and click Next.
 - d. In the Verify my identity with drop-down list, select a method and verify your account according to the prompt.
- Two-step verification is enabled.
4. Create an app password.
 - a. At the top navigation bar, click Security tab.
 - b. In the Two-step verification section, click Manage.
 - c. In the App passwords section, click Create a new app password.

Use this app password to sign in

Enter the app password below in the password field of the app or device that can't accept security codes. If you're not sure how to update your app or device with an app password, [follow these steps](#).

App password
pvqyxfoubbiwylg

For each app or device that can't accept security codes, you need to create a new app password to use instead.
[Create another app password](#)

Done

An app password is generated. Note down the password, which is used to verify your Outlook account when you configure Outlook as the mail server of the PBX.

Step2. Configure Outlook as email server of Yeastar P-Series PBX System

To ensure that the PBX can access and send mails from Outlook server via your Microsoft account, you should proceed as follows:

1. Log in to PBX management portal, go to System > Email > Email Server.
2. In the Type of Email Server drop-down list, select Custom Email Server.
3. Configure email server settings.
 - Sender Email Address: Enter your Outlook address, which will appear as the From address for outgoing emails sent by the PBX.
 - Email Address or Username: Enter your Outlook address.
 - Password: Enter the 16-digit app password, which is used to access Outlook server.
 - Outgoing Mail Server (SMTP): Retain the default value smtp-mail.outlook.com.
 - Port: Retain the default value 587.
 - Enable TLS Encryption: Keep the option unselected.
4. Test if the mail server can successfully send emails.
 - a. Click Test.
 - b. In the pop-up window, enter a recipient's email address in the Email Address field.
 - c. Click Test.
5. Click Save.

Result

- If the test email is sent successfully, the page displays "Success" and the recipient's mailbox would receive the email.
- If the test email is failed to be sent, the page displays "Failed to send" and prompts you an error message. You can check the error in [Email Sent Logs](#).

Customize Email Templates

This topic describes how to customize email notification language and email templates.

Background information


If you have enabled notification for a specific event, and have chosen to send emails to notify contacts, the system will send emails in the pre-configured email template to inform contacts when the event is triggered.

Yeastar P-Series PBX System provides the following types of email templates:

- Operations: Changes of password and login status.
- Telephony: SIP trunk registration and emergency calling.
- System: System performance, such as CPU overload, memory overload, new system firmware detected, etc.
- Security: Such as web login block, auto defense, etc.
- Event Reminder: Reminders related with the subscribed plan and services.
- Email: Email notifications related with extensions.

Procedure


1. Log in to PBX management portal, go to System > Email > Email Templates.
2. Set the language of notification emails.


 Note:

If you fail to find the desired language, you can update templates based on English.

- a. Click Notification Email Language.
- b. In the pop-up window, select a language from the drop-down list.
- c. Click Save.

The system will send emails in the selected language.

3. Edit a desired email template.
 - a. In the Email Templates list, click  beside the desired email template.
 - b. In the Template drop-down list, select Custom.
 - c. Edit email subject and content according to your needs.

 Note:

Images, videos, and audios are not supported.

4. Click Save and Apply.

Email Sent Logs

This topic introduces email sent logs and describes how to query logs.

Email sent logs overview

Email sent logs allow you to monitor mail delivery and provide you with error messages to help you troubleshoot delivery issues more quickly.

Storage of email sent logs

Email sent logs are saved in local storage, you can NOT change the storage location.

Auto cleanup of email sent logs

By default, when logs reach 50,000, the newest logs will replace the oldest logs. You can change the value, or restrict how long logs can be saved.

For more information, see [Auto Cleanup Settings](#).

Query email sent logs

1. Log in to PBX management portal, go to System > Email > Email Sent Logs.
2. Query logs by the following criteria according to your needs.
 - Send Result: Query all logs or query logs by send result.
 - Email Template Name: Query logs by email template.
 - Generated Time: Query logs by the generated date and time.
 - Email Recipient: Query logs by emails' recipients.

After logs are filtered, you can hover your mouse over Failed beside the failed log to check the error message.

Generated Time	Email Template Name	Email Recipient	Last Send Time	Send Result	Return Code
08/13/2020 14:46:26	Extension User Password Changed	becky@yeastar.com	08/13/2020 14:46:26	Succeeded	-
08/13/2020 14:45:56	Extension User Password Changed	becky@yeastar.com	08/13/2020 14:45:56	Succeeded	-
08/13/2020 14:04:53	SLA Alarm Threshold Reached		08/13/2020 14:05:09	Failed	-

Unknown mail server error.

Storage

Storage Overview

Yeastar P-Series PBX System provides local storage and supports external storage and network drive storage.

Storage limitation

Table 39.

Storage	P550	P560	P570
LOCAL (Local Flash)	1	1	1
USB 2.0	1	1	1
Hard Disk	0	1	1
SD Card (Up to 256 GB)	0	1	1
Network drive	1	2	2

The supported data for changing storage locations

Yeastar P-Series PBX System supports to change storage locations for the following data:

- Voicemail
- Logs, including event logs, email sent logs, operation logs, and system logs.
- Recordings



Note:

Recording files can NOT be stored on LOCAL (Local Flash).






- Backup files

For more information, see [Manage Storage Locations](#).

By default, data will be periodically cleared when it reaches the system limit. For more information, see [Auto Cleanup Settings](#).

Storage devices

The Storage Devices section shows the local storage, external storage, and network drive. You can click specific icons to manage storage devices.

- Click  to refresh the status.
- Click  to edit network drive settings.
- Click  to delete a network drive.
- Click  to format USB, hard disk, or SD card.
- Click  to remove USB, hard disk, or SD card.

Storage Devices						
Name	Type	Status	Total	Available	Usage	Operations
LOCAL	Local	Connected	6.14G	4.12G	33%	
HD	Hard Disk	Not Inserted	0.00G	0.00G	0%	
SD	SD Card	Not Inserted	0.00G	0.00G	0%	
USB	USB	Connected	869.30G	665.12G	23%	
testnet55	Network Drive	Connected	65.49G	42.49G	36%	

Set up a USB Flash Drive

This topic describes how to set up a USB flash drive on Yeastar P-Series PBX System.

Prerequisites

- Prepare a USB 2.0 flash drive.
- Back up data on the USB flash drive in advance.

Procedure

1. Insert the USB flash drive to the PBX's USB port.
2. Format the USB flash drive.

Note:

All the data in the USB flash drive will be cleared after formatting.

- a. Log in to PBX management portal, go to System > Storage > Storage Devices, find the USB flash drive.
 - b. In the Operations column, click .
 - c. In the pop-up dialog box, click OK.
- The USB flash drive is formatting.
3. In the Storage Devices section, check status of the USB flash drive.
 - Connected: The USB flash drive is connected.
 - Not Inserted: No USB flash drive is inserted.
 - Error: Format error.
 - Read Only: Can NOT write data to the USB flash drive.

What to do next

Decide what data will be stored on the USB flash drive. For more information, see [Manage Storage Locations](#).

Set up a Hard Disk Drive

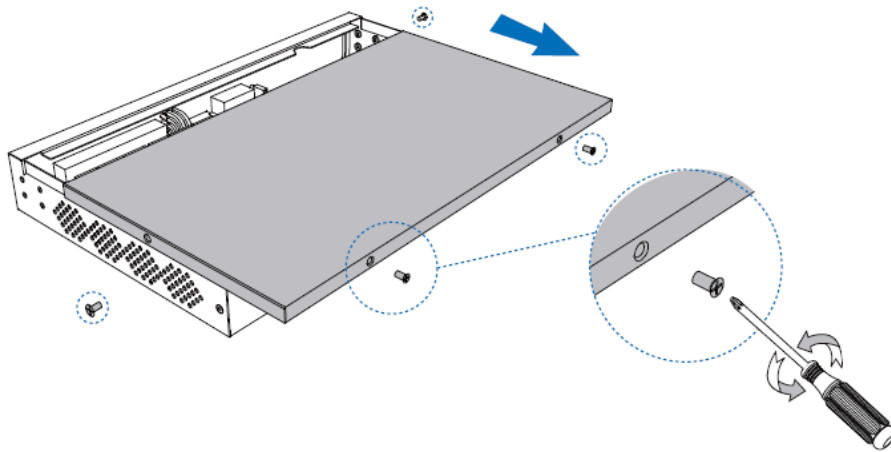
This topic describes how to set up a hard disk drive on Yeastar P-Series PBX System.

Prerequisites

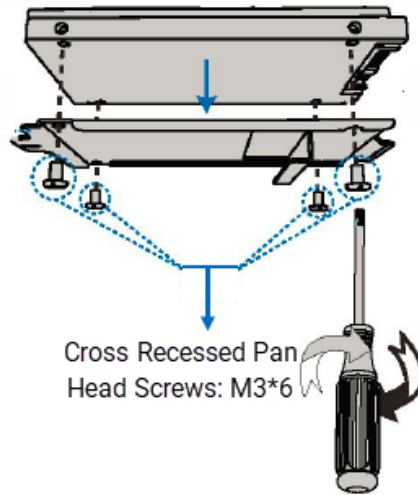
- Hard disk drive is only supported on P560 and P570.
- Make sure your PBX is power off.
- Prepare a 2.5" SATA hard disk drive.
- Back up data on the hard disk drive in advance.

Procedure

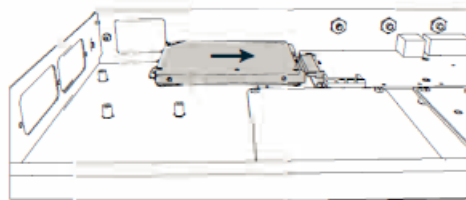
1. Install hard disk drive on Yeastar P-Series PBX System.
 - a. Loosen the screws at the bottom of the device and remove the upper cover.



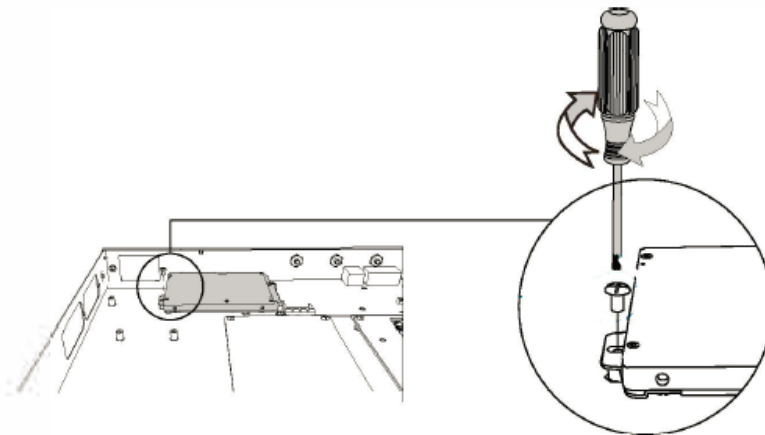
- b. Lock the hard disk drive on the bracket.




c. Push the hard disk drive to the right.




d. Lock the screws to fix the hard disk drive.



2. Format the hard disk drive.

 **Note:**
All the data in the hard disk drive will be cleared after formatting.

- a. Log in to PBX management portal, go to System > Storage > Storage Devices, find the hard disk drive.
- b. In the Operations column, click .
- c. In the pop-up dialog box, click OK.

The hard disk drive is formatting.

3. In the Storage Devices section, check status of the hard disk drive.
 - Connected: The hard disk drive is connected.
 - Not Inserted: No hard disk drive is inserted.
 - Error: Format error.
 - Read Only: Can NOT write data to the hard disk drive.

What to do next

Power on the PBX, and decide what data will be stored on the hard disk drive. For more information, see [Manage Storage Locations](#).

Set up an SD Card

This topic describes how to set up an SD card on Yeastar P-Series PBX System.

Prerequisites

- SD card is only supported on P560 and P570.
- Prepare an SD card, which meets the following requirements:
 - Maximum capacity: Up to 256 GB
 - Minimum performance: SDHC/SDXC Class10 UHS-I U3
 - Minimum write speed: 60 MB/s
 - Recommended brands: Sandisk Extreme Pro Series, Sandisk Extreme Series, TOSHIBA EXCERIA Series, or Samsung Pro Series.
- Back up data on the SD card in advance.


Procedure

1. Insert the SD card to the PBX's SD card slot.
2. Format the SD card.



Note:

All the data in the SD card will be cleared after formatting.

- a. Log in to PBX management portal, go to System > Storage > Storage Devices, find the SD card.
- b. In the Operations column, click .

c. In the pop-up dialog box, click OK.

The SD card is formatting.

3. In the Storage Devices section, check status of the SD card.

- Connected: The SD card is connected.
- Not Inserted: No SD card is inserted.
- Error: Format error.
- Read Only: Can NOT write data to the SD card.

What to do next

Decide what data will be stored on the SD card. For more information, see [Manage Storage Locations](#).

Add a Windows Network Drive

Network drive is used to extend storage space. You can save voicemails, recordings, and logs on a network drive. This topic describes how to add a shared folder on Windows 10 and mount the shared folder to Yeastar P-Series PBX System.

Restriction

There are restrictions for the number of network drives that can be added for each model:

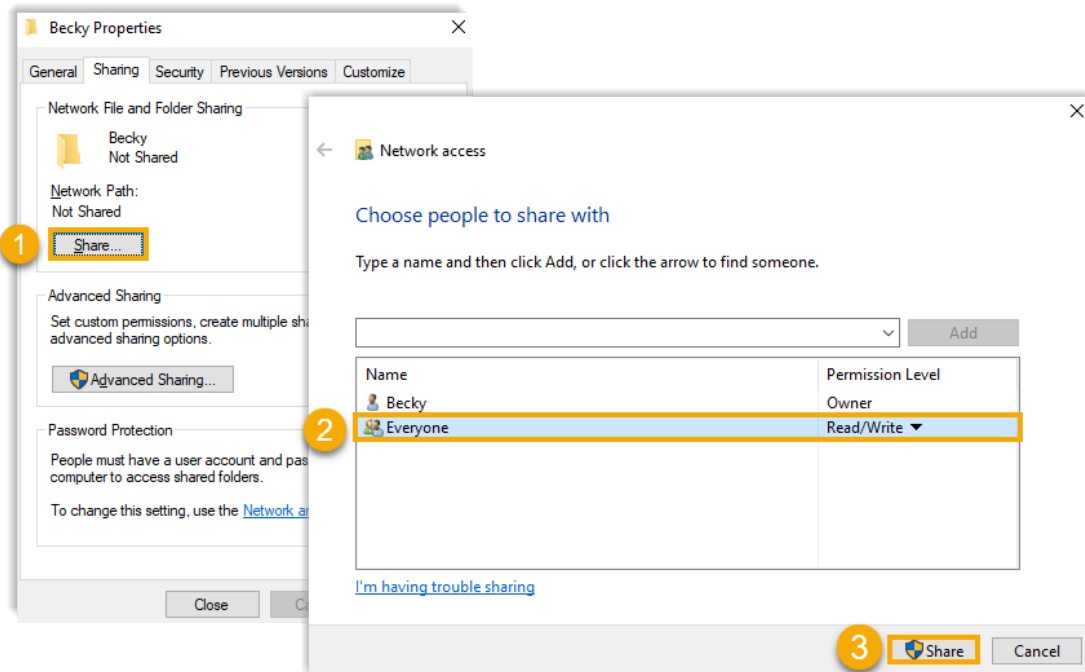
- Yeastar P550: Max. 1 network drive
- Yeastar P560: Max. 2 network drive
- Yeastar P570: Max. 2 network drive

Prerequisites

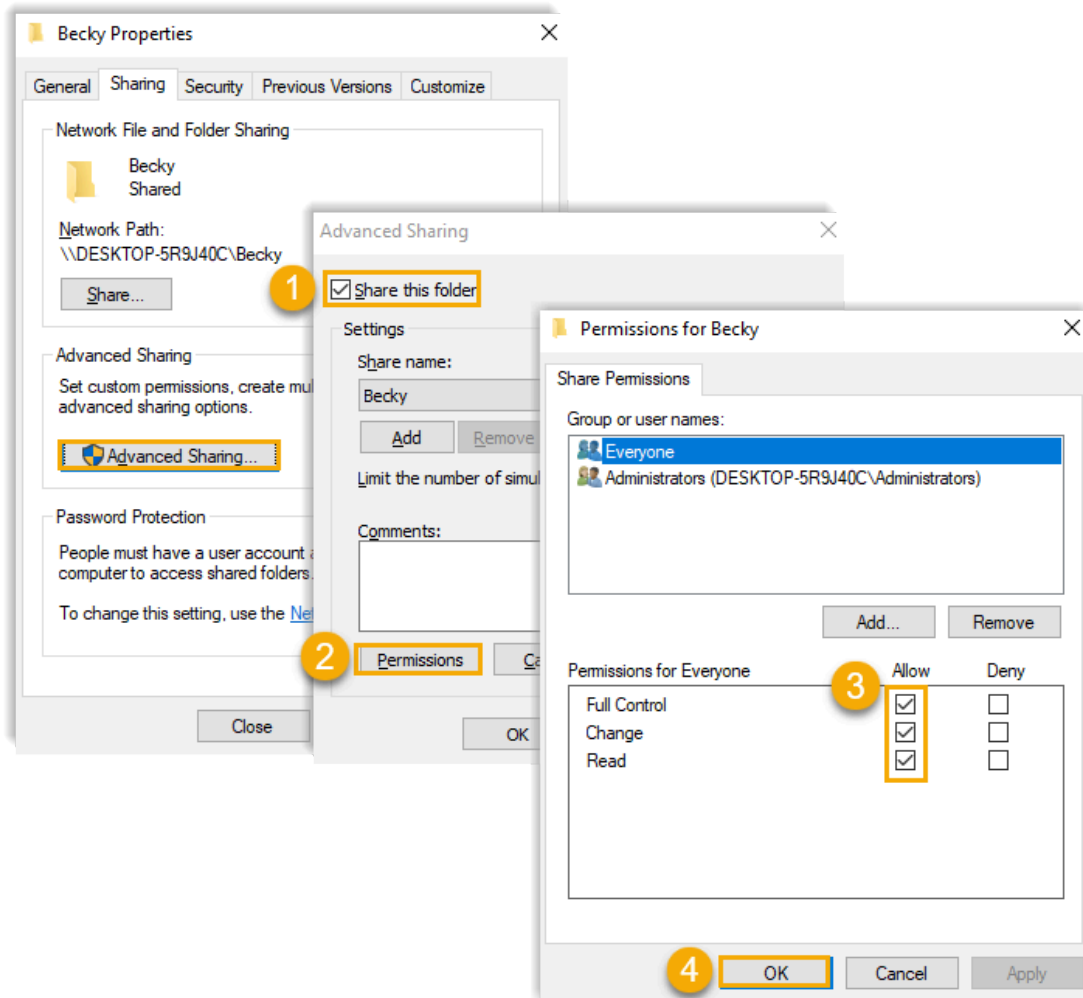
Make sure that the computer is always in service, or Yeastar P-Series PBX System cannot add files to the shared folder.

Step1. Create a shared folder in Windows 10

1. On your computer, create a folder and specify a name to help you identify it.
2. Right click the folder, select Properties > Sharing.
3. Click Share..., configure the Share properties.



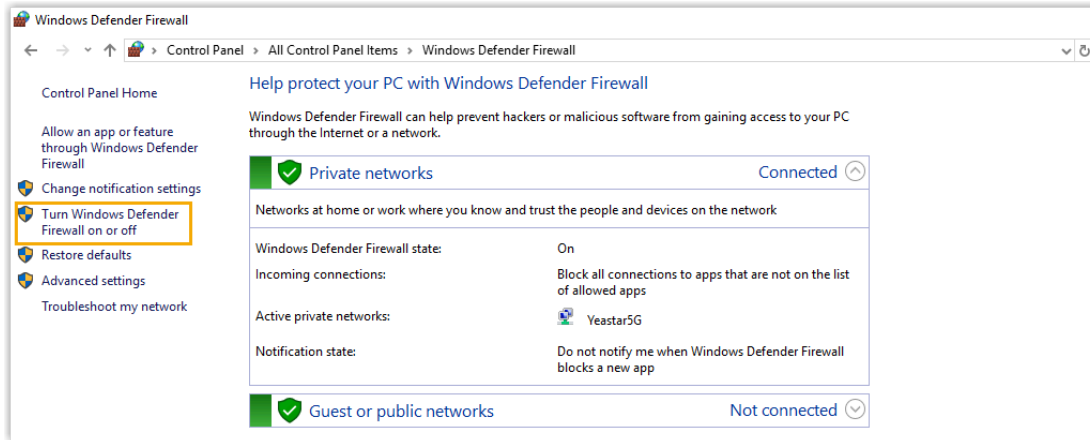
- a. Share the folder to Everyone.
 - b. In the Permission Level column, select Read/Write from the drop-down list.
 - c. Click Share.
 - d. In the pop-up dialog box, click Done.
4. Click Advanced Sharing..., configure advanced Share properties.



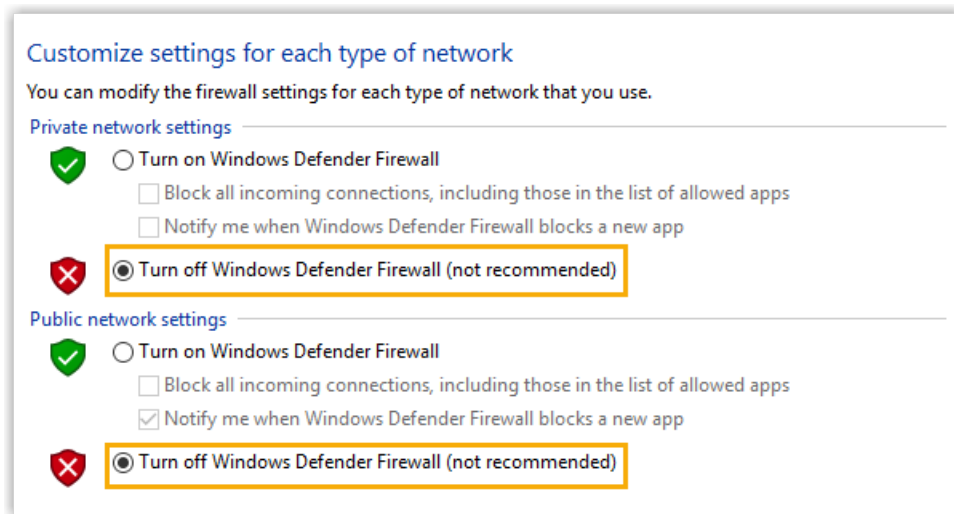
- a. Select the checkbox of Share this folder.
- b. Click Permissions.
- c. In the pop-up window, allow all the permissions.
- d. Click OK.

Step2. Turn off Windows Defender Firewall

1. On your computer, go to Control Panel > Windows Defender Firewall.
2. On the left navigation bar, click Turn Windows Defender Firewall on or off.




3. In both Private network settings and Public network settings sections, select Turn off Windows Defender Firewall (not recommended).



4. Click OK.

Step3. Mount the shared folder to PBX

1. Log in to PBX management portal, go to System > Storage > Storage Locations.
2. In the Storage Devices section, click Add Network Drive.
3. In the pop-up window, configure the following settings.
 - Name: Specify a name to help you identify the network drive.
 - Host/IP: Enter the IP address of the Windows PC.
 - Share Name: Enter the name of the shared folder that you have created on the Windows PC.





 **Note:**
To mount a subdirectory of the shared folder, enter {share_folder_name/subdirectory_name}.

- Access Username: Enter the [username](#) to access the shared folder.
 - Access Password: Enter the [password](#) to access the shared folder.
 - Work Group: Optional. If you have set work group on your network drive, enter the name of the work group. If not, leave this field blank.
 - Samba Version: Select the Samba version for the network drive. The default value is Auto.
4. Click Save.

Step4. Check connection status

In the Storage Devices section, check status of the network drive.


- Connected: The network drive is connected.
- Unmounted: No network drive is mounted.
- Read Only: Can NOT write data to the network drive.
- Error

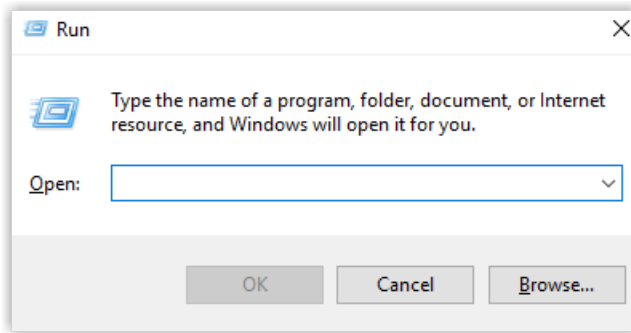
Storage Devices						
Name	Type	Status	Total	Available	Usage	Operations
LOCAL	Local	Connected	6.14G	4.12G	<div style="width: 33%;"></div> 33%	
HD	Hard Disk	Not Inserted	0.00G	0.00G	<div style="width: 0%;"></div> 0%	
SD	SD Card	Not Inserted	0.00G	0.00G	<div style="width: 0%;"></div> 0%	
USB	USB	Connected	869.30G	665.12G	<div style="width: 23%;"></div> 23%	 
testnet55	Network Drive	Connected	65.49G	42.49G	<div style="width: 36%;"></div> 36%	 

What to do next

Decide what data will be stored on the network drive. For more information, see [Manage Storage Locations](#).

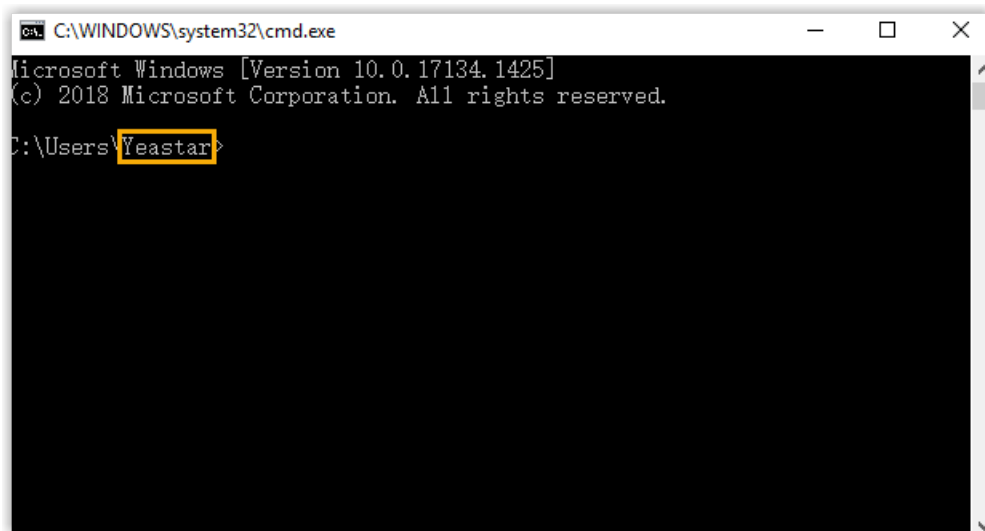
Network Drive FAQ

1. How to check the user name that is used to access the shared folder?
 - a. On the Windows PC where the shared folder is created, press  + R key to open the Run Window.



b. Enter `cmd` and click OK.

The user name is displayed on the Command Prompt.

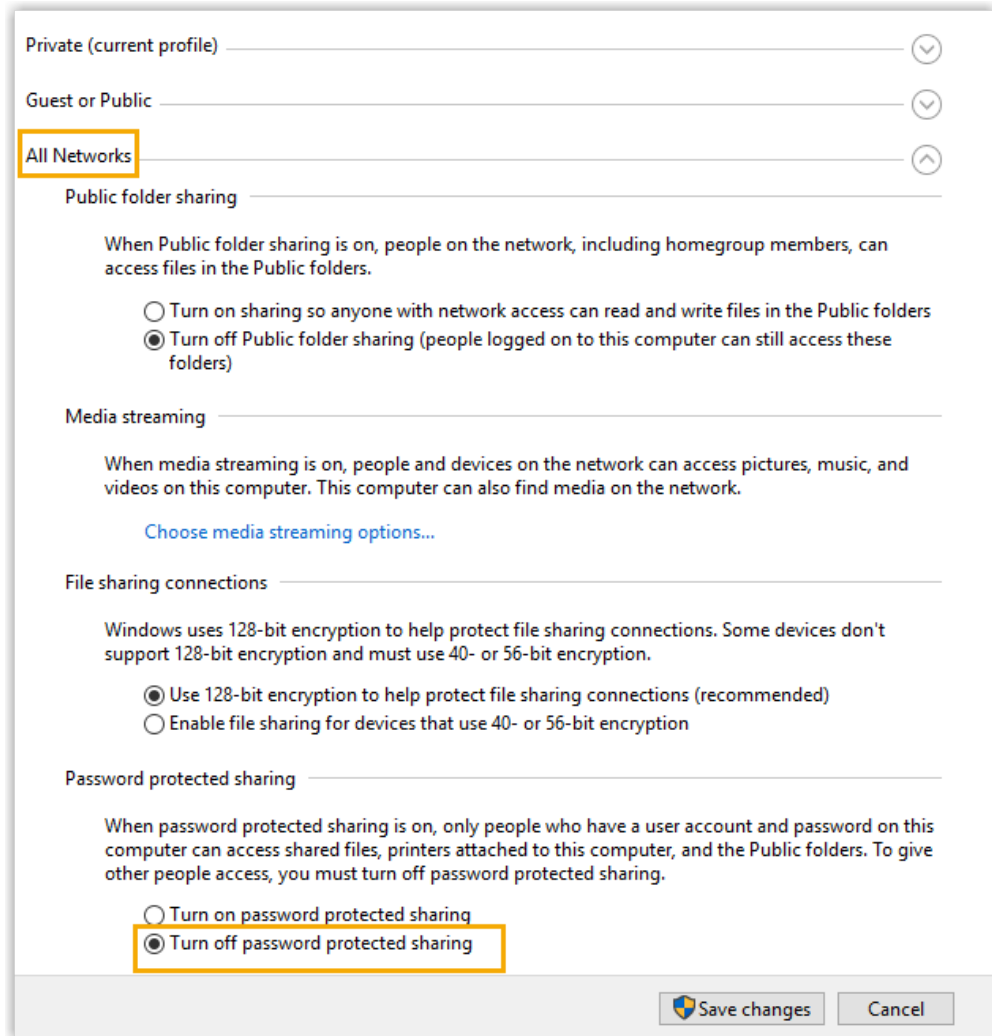


2. How to configure Network Drive if no password is set on the Windows PC?

- We recommend that you set a password on the Windows PC.

Enter the access password on PBX when you configure the Network Drive, then try to mount the network drive again.

- If you want to leave the blank password on the Windows PC, configure the following settings, and try to mount the network drive again.
 - a. On the Windows PC, go to Control Panel > Network and Internet > Network and Sharing Center > Change advanced sharing settings > All Networks > Password protected sharing, select Turn off password protected sharing.



- b. On the Network Drive configuration page, leave the Username and Password blank.

Add a Mac Network Drive

Network drive is used to extend storage space. You can save voicemails, recordings, and logs on a network drive. This topic describes how to add a shared folder on Mac and mount the shared folder to Yeastar P-Series PBX System.

Restriction


There are restrictions for the number of network drives that can be added for each model:

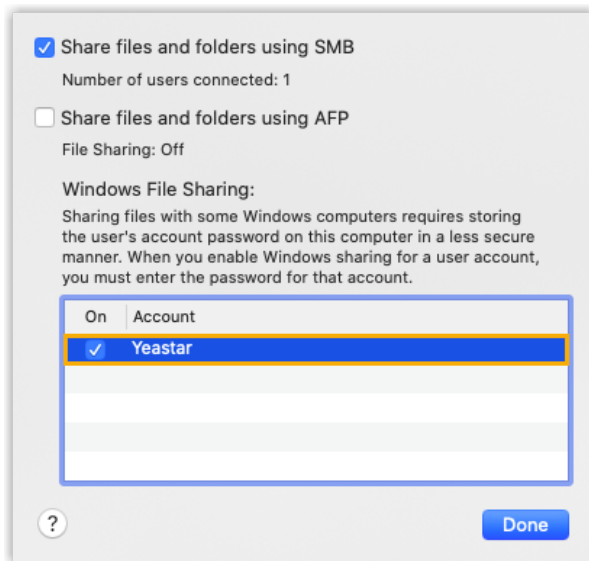
- Yeastar P550: Max. 1 network drive
- Yeastar P560: Max. 2 network drive
- Yeastar P570: Max. 2 network drive



Prerequisites

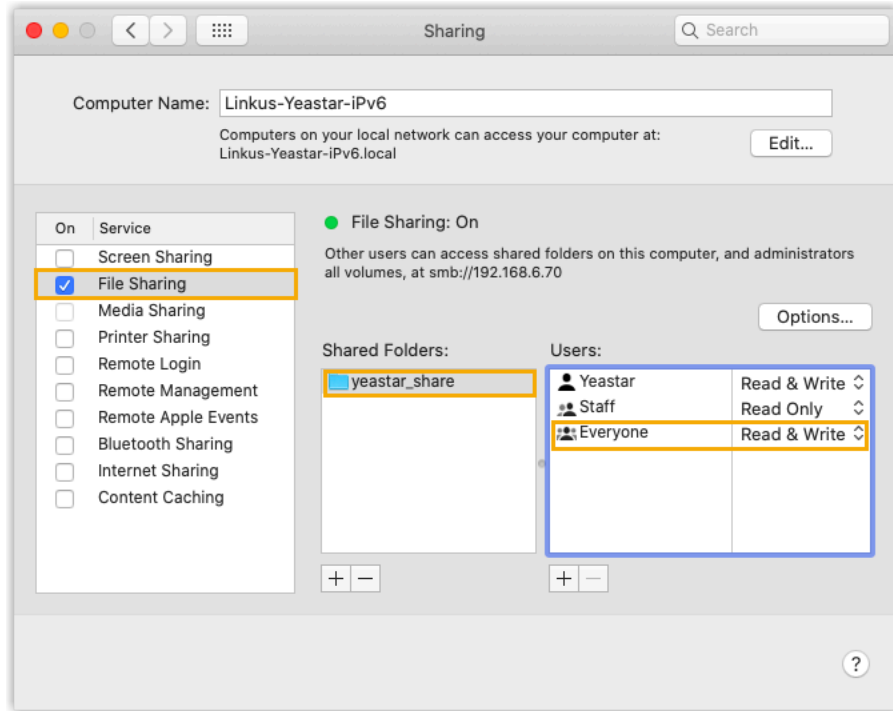
Make sure that the computer is always in service, or Yeastar P-Series PBX System cannot add files to the shared folder.

Step1. Create a shared folder on Mac

1. On your Mac, create a folder and specify a name to help you identify it.
2. Go to Apple menu  > System Preferences > Sharing to set up file sharing.
 - a. On the left navigation bar, select the checkbox of File Sharing.
 - b. Click Options to configure sharing credentials.




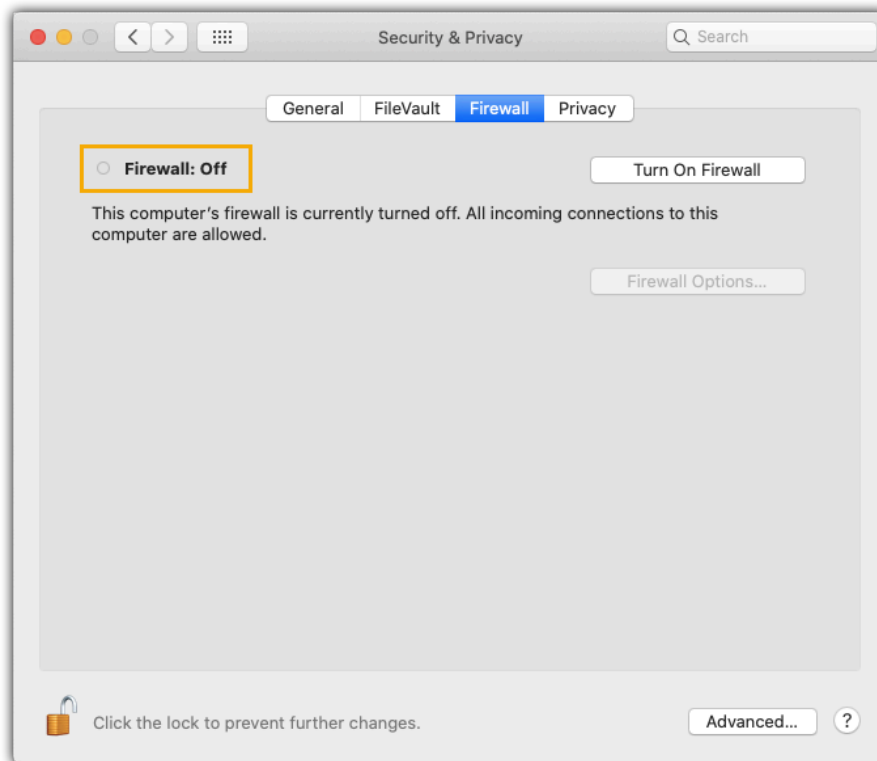
- i. Select the checkbox of Share files and folders using SMB.
 - ii. In the Windows File Sharing section, enable the admin account and enter login password.
 - iii. Click Done.
 - c. In the Shared Folders section, click  to add the folder that you want to share.
 - d. In the Users section, select Everyone and set permission level to Read & Write.
 - e. Click  to close the window.



Step2. Turn off Mac firewall

Firewall on Mac is disabled by default. Follow the instructions below to ensure that the firewall is disabled, or the shared folder on the Mac may not be accessed.

1. Go to Apple menu  > System Preferences > Security & Privacy, click Firewall tab.
2. Make sure that firewall is disabled as follows.



Step3. Mount the shared folder to PBX

1. Log in to PBX management portal, go to System > Storage > Storage Locations.
2. In the Storage Devices section, click Add Network Drive.
3. In the pop-up window, configure the following settings.
 - Name: Specify a name to help you identify the network drive.
 - Host/IP: Enter the IP address of the Mac.
 - Share Name: Enter the name of the shared folder that you have created on the Mac.

Note:





To mount a subdirectory of the shared folder, enter subdirectory name.

- Access Username: Enter the [username](#) to access the shared folder.
 - Access Password: Enter the password to access the shared folder.
 - Work Group: Optional. If you have set work group on your network drive, enter the name of the work group. If not, leave this field blank.
 - Samba Version: Select the Samba version for the network drive. The default value is Auto.
4. Click Save.

Step4. Check connection status

In the Storage Devices section, check status of the network drive.


- Connected: The network drive is connected.
- Unmounted: No network drive is mounted.
- Read Only: Can NOT write data to the network drive.
- Error

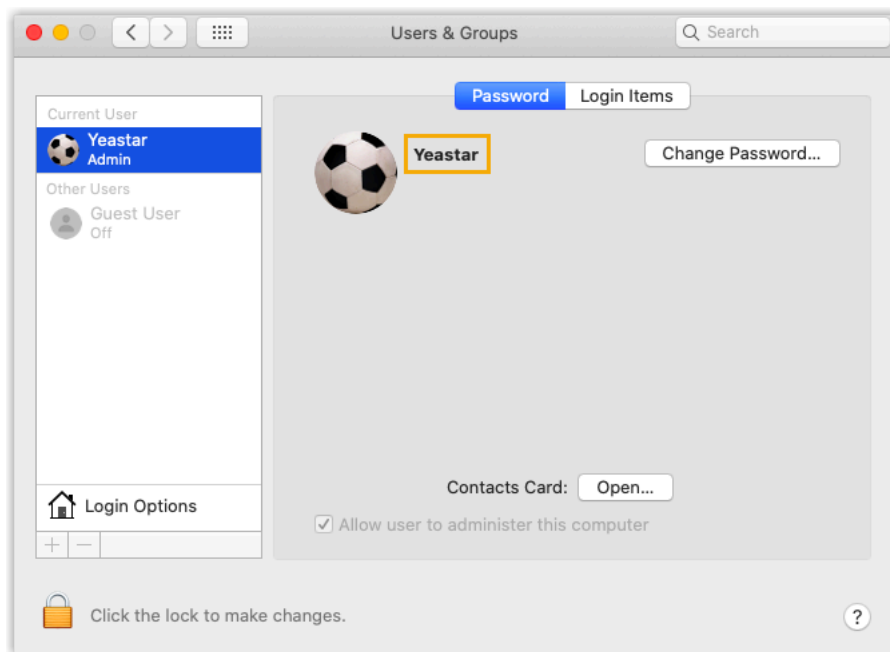
Storage Devices						
Name	Type	Status	Total	Available	Usage	Operations
LOCAL	Local	Connected	6.14G	4.12G	<div style="width: 33%;"></div> 33%	
HD	Hard Disk	Not Inserted	0.00G	0.00G	<div style="width: 0%;"></div> 0%	
SD	SD Card	Not Inserted	0.00G	0.00G	<div style="width: 0%;"></div> 0%	
USB	USB	Connected	869.30G	665.12G	<div style="width: 23%;"></div> 23%	 
testnet55	Network Drive	Connected	65.49G	42.49G	<div style="width: 36%;"></div> 36%	 

What to do next

Decide what data will be stored on the network drive. For more information, see [Manage Storage Locations](#).

Network Drive FAQ

1. How to check the user name that is used to access the shared folder?
 - a. Go to Apple menu  > System Preferences > Users & Groups, check the current user name.



Manage Storage Locations

This topic describes how to manage storage locations for voicemail, logs, and recordings.

Prerequisites

- To store data on local flash, make sure there is enough storage space.
- To store data on external storage device or network drive, make sure the external device or network drive is connected. For more information, see the following topics:
 - [Set up a USB Flash Drive](#)
 - Set up a Hard Disk Drive
 - [Set up an SD Card](#)
 - [Add a Windows Network Drive](#)
 - [Add a Mac Network Drive](#)

Procedure

1. Log in to PBX management portal, go to System > Storage > Storage Locations.
2. In the Storage Locations section, set storage location for the desired data.
 - Voicemail: Can be stored either on local flash or external device.
 - Recordings: Can be stored ONLY on external device.
 - Logs: Can be stored either on local flash or external device.
3. Click Save.

Result

New data will be stored on the specified location.

What to do next

Set the maximum number and preservation days that data can be stored. For more information, see [Auto Cleanup Settings](#).

Auto Cleanup Settings

Auto Cleanup feature automatically and periodically cleans up your CDR, voicemails, recording files, backup files, and logs (including event logs, email sent logs, operation logs, and system logs). This topic describes relevant configuration parameters of auto cleanup.

CDR Auto Cleanup

Table 40.

Setting	Description
Max Number of CDR	Set the maximum number of CDR that should be retained.

Table 40. (continued)

Setting	Description
	<p>When it reaches 90% of the maximum number, the Auto Cleanup Reminder event will be triggered, the system will notify contacts concerned via specific methods.</p> <p>When it reaches the maximum number, the oldest CDR will be deleted.</p> <p>Default value: 200,000</p> <p>Maximum value: 1,000,000</p>
CDR Preservation Days	<p>Set the maximum number of days that CDR should be retained.</p> <p>When it reaches 90% of the maximum preservation days, the Auto Cleanup Reminder event will be triggered, the system will notify contacts concerned via specific methods.</p> <p>When it reaches the maximum preservation days, the oldest CDR will be deleted.</p> <p>Default value: 0, which means no limit.</p>

VoiceMail Auto Cleanup

Table 41.

Setting	Description
Max Number of Voice-mail	<p>Set the maximum number of voicemails that should be retained.</p> <p>When it reaches 90% of the maximum number, the Auto Cleanup Reminder event will be triggered, the system will notify contacts concerned via specific methods.</p> <p>When it reaches the maximum number, the oldest voicemails will be deleted.</p> <p>Default value: 100</p> <p>Maximum value: 500</p>
VoiceMail Preservation Days	<p>Set the maximum number of days that voicemails should be retained.</p> <p>When it reaches 90% of the maximum preservation days, the Auto Cleanup Reminder event will be triggered, the system will notify contacts concerned via specific methods.</p>

Table 41. (continued)

Setting	Description
	<p>When it reaches the maximum preservation days, the oldest voicemails will be deleted.</p> <p>Default value: 0, which means no limit.</p>

Recording Auto Cleanup

Table 42.

Setting	Description
Max Usage of Device (%)	<p>Set the maximum storage percentage that the device is allowed to store recording files.</p> <p>When it reaches 90% of the maximum storage percentage, the Auto Cleanup Reminder event will be triggered, the system will notify contacts concerned via specific methods.</p> <p>When it reaches the maximum storage percentage, the oldest recording files will be deleted.</p> <p>Default value: 80%</p> <p>Maximum value: 90%</p>
Recordings Preservation Days	<p>Set the maximum number of days that recording files should be retained.</p> <p>When it reaches 90% of the maximum preservation days, the Auto Cleanup Reminder event will be triggered, the system will notify contacts concerned via specific methods.</p> <p>When it reaches the maximum preservation days, the oldest recording files will be deleted.</p> <p>Default value: 0, which means no limit.</p>

System Backup Files

Table 43.


Setting	Description
Max Number of Files	<p>Set the maximum number of backup files that should be retained.</p> <p>When it reaches 90% of the maximum number, the Auto Cleanup Reminder event will be triggered, the system will notify contacts concerned via specific methods.</p>

Table 43. (continued)

Setting	Description
	<p>When it reaches the maximum number, the oldest backup files will be deleted.</p> <p>Default value: 5</p> <p>Maximum value: 8</p>

Event Logs Auto Cleanup

Table 44.

Setting	Description
Max Number of Logs	<p>Set the maximum number of event logs that should be retained.</p> <p>When it reaches the maximum number, the oldest event logs will be deleted.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;"> <p> Note: Some event logs are not allowed to be automatically cleaned up. When those logs reach 5,000, the oldest event logs will be deleted.</p> </div> <p>Default value: 50,000</p> <p>Maximum value: 1,000,000</p>
Logs Preservation Days	<p>Set the maximum number of days that event logs should be retained.</p> <p>When it reaches the maximum preservation days, the oldest event logs will be deleted.</p> <p>Default value: 0, which means no limit.</p>

Email Sent Logs Auto Cleanup

Table 45.

Setting	Description
Max Number of Logs	<p>Set the maximum number of email sent logs that should be retained.</p> <p>When it reaches the maximum number, the oldest email sent logs will be deleted.</p> <p>Default value: 50,000</p>

Table 45. (continued)

Setting	Description
	Maximum value: 1,000,000
Logs Preservation Days	<p>Set the maximum number of days that email sent logs should be retained.</p> <p>When it reaches the maximum preservation days, the oldest email sent logs will be deleted.</p> <p>Default value: 0, which means no limit.</p>

Operation Logs Auto Cleanup

Table 46.

Setting	Description
Max Number of Logs	<p>Set the maximum number of operation logs that should be retained.</p> <p>When it reaches the maximum number, the oldest operation logs will be deleted.</p> <p>Default value: 50,000</p> <p>Maximum value: 1,000,000</p>
Logs Preservation Days	<p>Set the maximum number of days that operation logs should be retained.</p> <p>When it reaches the maximum preservation days, the oldest operation logs will be deleted.</p> <p>Default value: 0, which means no limit.</p>

System Logs Auto Cleanup

Table 47.

Setting	Description
Max Storage of Logs (MB)	<p>Set the maximum file size for a system log package.</p> <p>When it reaches the maximum file size, the oldest logs in the package will be deleted.</p> <p>Default value: 10</p> <p>Maximum value: 50</p>
Logs Preservation Days	<p>Set the maximum number of days that a system log should be retained.</p>

Table 47. (continued)

Setting	Description
	Default value: 7 Maximum value: 15

Event Notification

Event Notification Overview

Event Notification feature is designed to provide information about changes on Yeastar P-Series PBX System and helps you monitor operations on the PBX. When an event occurs, the system will record the event and notify contacts concerned via specific methods. This topic describes event types, event levels, notification methods, notification email templates, and auto cleanup of events.

Event types

Yeastar P-Series PBX System supports the following event types:

- [Operations](#)
- [Telephony](#)
- [System](#)
- [Security](#)
- [Reminder](#)

Table 48. Operations

Event	Description
Administrator Login Success	The administrator successfully logged in to the PBX web interface.
Web User Login Success	A user successfully logged in to the PBX web or the Linkus Web Client.
Web User Login Failed	A user failed to log in to PBX management portal or the Linkus Web Client.
Linkus Client Login Failed	An extension user failed to log in to Linkus Mobile Client or Linkus Desktop Client.
Administrator Password Changed	The administrator's password was changed.

Table 48. Operations (continued)

Event	Description
Extension User Password Changed	An extension user's user password was changed.

Table 49. Telephony

Event	Description
SIP Trunk Registration Failed	Failed to register or connect to a SIP trunk.
SIP Trunk Re-registered	Successfully re-registered or re-connected to a SIP trunk.
Emergency Call Dialed Out	An extension user placed an emergency call.

Table 50. System

Event	Description
CPU Overload	CPU ran over 90% in 10s.
Memory Overload	Memory ran over 90% in 10s.
Abnormal D30 Module	The D30 module was abnormal.
Storage Device Failure	Failed to write data to storage device.
Insufficient Storage	The storage ran out of 90%.
Lost Connectivity to Storage Device	Lost connection to storage device.
Auto Cleanup Reminder	Reach 90% of the allowed storage limit.
New System Firmware Detected	The PBX automatically detected a new firmware version.
System Upgrade Completed	The PBX was upgraded.
System Reboot	Either of the following situations triggered the event: <ul style="list-style-type: none"> • The PBX rebooted after configuration. • The PBX automatically rebooted after system crash.
System Restore	The PBX was restored.
Yeastar SMTP Server Error	Yeastar SMTP server failed to send emails.

Table 50. System (continued)

Event	Description
Abnormal License Activation	Failed to connect to extranet License Activation Server.

Table 51. Security

Event	Description
Web User Locked Out	<p>PBX blocked the source IP when either of the following situations was met:</p> <ul style="list-style-type: none"> • Web Login failure for more than 5 times in 24 hours. • More than 5 accounts were locked in 24 hours.
Linkus User Blocked Out	<p>PBX blocked the source IP when either of the following situations was met:</p> <ul style="list-style-type: none"> • Login failure (Linkus Mobile Client or Linkus Desktop Client) for more than 5 times in 24 hours. • More than 5 accounts were locked in 24 hours.
Extension Registration Blocked Out	<p>PBX blocked the source IP when either of the following situations was met:</p> <ul style="list-style-type: none"> • Registration failure for more than 20 times. • More than 3 accounts were locked.
Auto Defense IP Blocked Out	The monitored service or port reached the limit of Number of Packets during specific Time Interval.
Outbound Call Frequency Exceeded	An extension has exceeded the limit of Number of Calls during specified Time Period set in an Outbound Call Frequency Restriction rule.
Outbound Call to a Disallowed Country	An extension user made an outbound call to a disallowed country.

Table 52. Reminder

Event	Description
Plan Expiration Reminder	The current plan will expire soon.
Video Conferencing Usage Has Reached 90% of Time Limit	Reach 90% of the annual time limit of video conferencing.

Table 52. Reminder (continued)

Event	Description
Video Conferencing Usage Limit Reached	Reach annual usage limit of video conferencing.

Event levels

Event level is used to indicate how severe or important an event is. Choosing an appropriate level prevents recipients from receiving repetitive information.

Yeastar P-Series PBX System supports the following event levels:

- **Information:** Events that pass general information to recipients.
- **Warning:** Events that indicate specific components or applications are not in ideal states, and further action could result in errors.
- **Alert:** Events that indicate problems require timely attention.



Note:

- When an event occurs, the system gives you a pop-up reminder on the right of PBX management portal.
- For event whose default level is not Alert, the system will NOT give you a pop-up reminder even if you change the level from Information or Warning to Alert.

Notification contacts and methods

You can set notification contacts to internal users or external users, and notify users in the following ways when events occur:

- Send Email
- Call Extension
- Call Mobile

For more information, see [Manage Notification Contacts](#).

Notification email templates

If notification method is set to Send Email for a specific contact, the system will send notification emails in corresponding email template when an event occurs. Yeastar P-Series PBX System provides default email template for each event, you can also customize email templates according to your needs.

For more information, see [Customize Email Templates](#).

Auto cleanup of event logs

By default, when event logs reach 50,000, the system automatically deletes the oldest logs. You can change the value, or set the maximum days that logs can be retained.

For more information, see [Auto Cleanup Settings](#).

Configure Event Notifications

This topic describes how to configure event notifications.

Procedure

1. Log in to PBX management portal, go to System > Event Notification > Event Type.
2. In the Notification column, enable notifications for desired event.


Event Name	Event Level	Notification	Email Template
Administrator Login Success	● Information	<input checked="" type="checkbox"/>	✎
Web User Login Success	● Information	<input type="checkbox"/>	✎
Web User Login Failed	● Information	<input type="checkbox"/>	✎


3. Configure notification settings for a desired event.
 - Event Level: A proper level helps you identify seriousness of an event. Use default level or select a level from the drop-down list.
 - Email Template: To customize template of the email that will be sent to relevant contacts when the event occurs, click [✎](#).
 - Notification Contacts: Add notification contacts and select proper notification methods.

For more information, see [Manage Notification Contacts](#).

Result

When the event occurs, the followings can be achieved:

- The PBX sends notifications to relevant contacts via specific notification methods.
- On [Event Trend](#) section, the event is included in the statistics of corresponding event level.
- At the top right corner of the page,  automatically adds 1 in the color that indicates the event level.

 Note:

If default level for the event is Error, the system also gives you a pop-up reminder on the right of PBX management portal.

What to do next

At the top right corner, click  to check event details.

Manage Notification Contacts

This topic describes how to add, edit, or delete a notification contact.

Add a notification contact


1. Log in to PBX management portal, go to System > Event Notification > Notification Contacts, click Add.
2. In the pop-up window, configure contact settings.
 - Notification Contact: Select an internal user or set an external user. If you choose Custom, enter a name in the Contact Name field.
 - Notification Methods: Set how to notify the contact when events occur.
 - Call Extension: The PBX will call the extension number of the contact when an event occurs.
 - Send Email: The PBX will send notifications to the email address of the contact when an event occurs.
 - Call Mobile: The PBX will call the mobile number of the contact when an event occurs.

Note:


To ensure that PBX can successfully call the mobile number, make sure that the [Prefix](#) is configured correctly according to the outbound route rule.

- The Event Levels to Notify: Select the level of events that you want to notify the contact. The contact will only receive notifications when events at the level occur.
3. Click Save.

Edit a notification contact


1. Log in to PBX management portal, go to System > Event Notification > Notification Contacts.
2. Select a desired contact, click .

Note:

To edit the event notifications of super administrator, click the  at the top-right corner and select Administrator Settings.

3. Change the notification methods and notification level according to your needs.
4. Click Save.

Delete notification contacts

1. Log in to PBX management portal, go to System > Event Notification > Notification Contacts.
2. Delete one or more contacts according to your needs.
 - To delete a contact, click  beside the desired contact, click OK.
 - To delete contacts in bulk, select the checkboxes of the desired contacts, click Delete and OK.

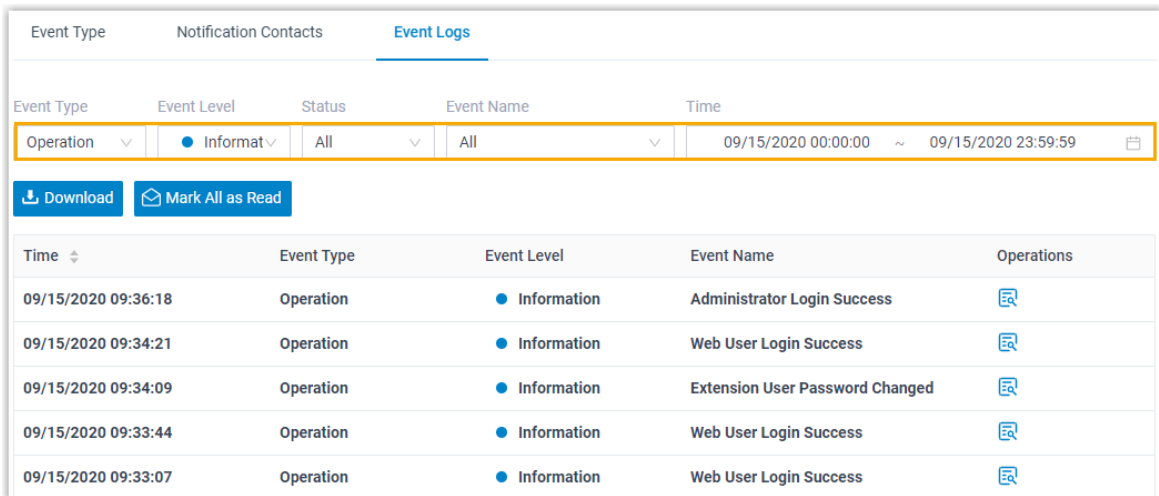
The contacts are removed from the list, and will not receive notifications when events occur.






Manage Event Logs

All the occurred events are saved in event logs so that you can trace the events. This topic describes how to view, download, and mark event logs as read.

Procedure

1. Log in to PBX management portal, go to System > Event Notification > Event Logs.
2. Set the search criteria to search events.



Time	Event Type	Event Level	Event Name	Operations
09/15/2020 09:36:18	Operation	Information	Administrator Login Success	
09/15/2020 09:34:21	Operation	Information	Web User Login Success	
09/15/2020 09:34:09	Operation	Information	Extension User Password Changed	
09/15/2020 09:33:44	Operation	Information	Web User Login Success	
09/15/2020 09:33:07	Operation	Information	Web User Login Success	

- **Event Type:** Search all the event logs or search logs by a specific event type.
- **Event Level:** Search all the event logs or search logs by a specific event level.
- **Status:** Search all the event logs or search logs by a specific acknowledgement status.

- Event Name: Search all the event logs or search a specific event.
- Time: Set the start date and end date of the events.


The matched events are displayed on the page.


3. Handle the searched events according to your needs.

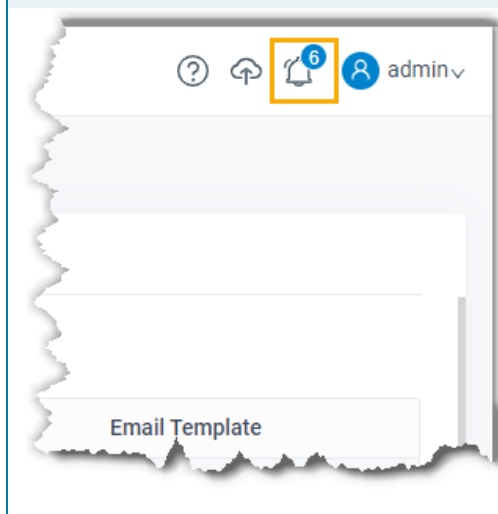
- To check log details, click  beside the desired event log.

The event log will be marked as read.

- To download all the searched logs, click Download.
- To mark all the searched logs as read, click Mark All as Read.

 Note:

At the top right corner, the number of unread events of the event level prompted on  will be cleared.



Security

Security Overview

Yeastar P-Series PBX System provides robust security options to ensure a secure and reliable phone service to your business operation, such as static defense rules, auto defense rules, IP blocking and so on.


Static defense

Static defense rules are used to control and filter traffic sent to the PBX by IP address, domain, or MAC address.

Yeastar P-Series PBX System has default static defense rules to ensure the communication among Yeastar server, Yeastar P-Series PBX System, and devices in your local network.

By default, the PBX always accepts connections from the following addresses:

- Local network
 - 10.0.0.0/255.0.0.0
 - 172.16.0.0/255.240.0.0
 - 192.168.0.0/255.255.0.0
 - 169.254.0.0/255.255.0.0

 Note:

These rules can NOT be edited or deleted.

- Domain related with Yeastar
 - update.yeastar.com
 - rmtunnel.yeastar.com
 - cttlunnel.yeastar.com
 - tunnel.yeastar.com
 - appcenter.yeastar.com
 - mail.pbxsmt.com
 - active.yeastar.com
- IP address of phones that have been auto provisioned

You can also set up new rules to accept, drop, or reject access to the PBX. The IP address that was denied access to the PBX would be blocked when trying to connect to the PBX. You can check the blocked IP address in Block IPs.

For more information, see [Add a Static Defense Rule](#) and [Manage Blocked IP Addresses](#).

Auto defense

Auto defense rules are used to prevent massive connection attempts or brute force attacks. When a source address sends packets over the limit within the specified time period, the PBX will block the source address. You can check the blocked IP address in [Block IPs](#).

Yeastar P-Series PBX System has default auto defense rules as below:

Table 53.

Rule Name	Defense Object				
	Type	Port	Protocol	Number of IP Packets	Time Interval (s)
SSH	Service	8022	TCP	10	60s
SIP UDP	Service	5060	UDP	40	2s
SIP TCP	Service	5060	TCP	40	2s
HTTP	Service	80	Both	120	60s
HTTPS	Service	8088	Both	120	60s

You can also set up new rules according to your needs.

For more information, see [Add an Auto Defense Rule](#).

Outbound Call Frequency Restriction

Outbound Call Frequency Restriction rule is used to limit the number of outbound calls over specified time period.


The PBX has a default rule to limit extension users to make maximum 5 outbound calls in 1 second.

You can also set up new rules according to your needs. For more information, see [Add an 'Outbound Call Frequency Restriction' Rule](#).

Security options

The PBX provides additional options so that you can flexibly adjust your security scheme:

- **Disable Auto Defense:** If the option is enabled, the auto defense feature will not work.
- **Disable Extension Registration Defense:** If the option is enabled, the SIP security settings will not work.
- **Drop All but Accepted IPs in Static Defense:** If the option is enabled, the PBX will drop all the packets and connections from other hosts except the accepted addresses defined in static defense rules.

 Note:

We recommend that you [create a backup on the PBX](#) before you enable the feature.

- Drop IP Ping Request: If the option is enabled, the PBX will disable Ping response (ICMP echo).

Static Defense

Add a Static Defense Rule

Static defense rules are used to control and filter traffic sent to Yeastar P-Series PBX System. This topic describes how to add a static defense rule.

Procedure

1. Log in to PBX management portal, go to Security > Security Rules > Static Defense, click Add.
2. In the Basic section, configure basic settings for the rule.
 - Name: Enter a name to help you identify the rule.
 - Description: Optional. Add a note to the rule.
 - Action: Select an action for the rule.
 - Accept: Accept connections from a specific address.
 - Drop: Restrict a specific address from accessing a specific service or port of the PBX, and do NOT send any error notifications back to the sender.
 - Reject: Restrict a specific address from accessing a specific service or port of the PBX, and send error notifications back to the sender.
3. In the Defense Object section, configure relevant settings of defense objects.
 - Object Type: Choose the type of the source traffic.
 - IP Address: If you choose the option, enter an IP address or an IP section in the Source IP Address / Subnet Mask field.
 - Domain: If you choose the option, enter a domain in the Domain Name field.
 - MAC Address: If you choose the option, enter a MAC address in the MAC Address field.
 - Service/Port Range: Set whether the rule is applied to a specific service or a port range.

Note:

The setting is available ONLY when you set Action to Drop or Reject.

- Service: Select a service from the drop-down list. The defense rule will be applied to the service and the service port.

Note:

The port follows the setting in Service Ports (System > Network).

- Port Range: Set a port range.
 - Protocol: Choose a protocol to which the rule is applied.
 - UDP
 - TCP
 - BOTH: Both UDP and TCP.
4. Click Save.


Result

- For address that is allowed to access the PBX, the system will always accept connections from the address.
- For address that is restricted from accessing a specific service or port of the PBX, the system will block it when the address tries to access the service or the port.


Manage Static Defense Rules

This topic describes how to edit or delete static defense rules.

Edit a static defense rule

1. Log in to PBX management portal, go to Security > Security Rules > Static Defense.
2. Select the desired rule, click .
3. Edit rule settings according to your needs.
4. Click Save.

Delete static defense rules

1. Log in to PBX management portal, go to Security > Security Rules > Static Defense.
2. Delete one or more rules according to your needs.
 - To delete a rule, click  beside the desired rule, click OK.
 - To delete rules in bulk, select the checkboxes of the desired rules, click Delete and OK.

Export and Import Static Defense Rules

The static defense rules configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired static defense rules in the exported file, and import the file to PBX again. This topic describes how to export and import static defense rules.

Export static defense rules

You can export all static defense rules to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Security > Security Rules > Static Defense.
2. Click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see [Static Defense Rule Parameters](#).

Import static defense rules

We recommend that you export static defense rules to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 50 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information , see [Static Defense Rule Parameters](#).

Procedure

1. Log in to PBX management portal, go to Security > Security Rules > Static Defense.
2. Click Import.
3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The static defense rules in the CSV file will be displayed in the Static Defense list.

Auto Defense

Add an Auto Defense Rule

Auto defense rules are used to prevent massive connection attempts or brute force attacks. This topic describes how to add an auto defense rule.

Procedure

1. Log in to PBX management portal, go to Security > Security Rules > Auto Defense, click Add.
2. In the Name field, enter a name to help you identify the rule.
3. In the Defense Object section, configure relevant settings of the defense object.

- **Service/Port Range:** Set whether the rule is applied to a specific service or a port range.
 - **Service:** Select a service from the drop-down list. The defense rule will be applied to the service and the service port.

**Note:**

The port follows the setting in Service Ports (System > Network).

- **Port Range:** Set a port range.
- **Protocol:** Choose a protocol to which the rule is applied.
 - UDP
 - TCP
 - **BOTH:** Both UDP and TCP.
- **Number of IP Packets:** The number of IP packets permitted within a specific time period.
- **Time Interval (s):** The time interval to receive IP Packets.

For example, Number of IP Packets is 90 and Time Interval (s) is 60; The PBX will block the IP that sends more than 90 IP packets in 60 seconds.

4. Click Save.

Result


When a source address sends packets over the limit within the specified time period, the followings can be achieved:

- The PBX blocks the IP address. You can check the details in [Blocked IPs](#).
- If you have enabled notification for Auto Defense IP Blocked Out event, the PBX will give you a pop-up reminder on the web interface, and notify you via a specific method.


Manage Auto defense Rules

This topic describes how to edit or delete auto defense rules.

Edit an auto defense rule

1. Log in to PBX management portal, go to Security > Security Rules > Auto Defense.
2. Select the desired rule, click .
3. Edit rule settings according to your needs.
4. Click Save.

Delete auto defense rules

1. Log in to PBX management portal, go to Security > Security Rules > Auto Defense.
2. Delete one or more rules according to your needs.
 - To delete a rule, click  beside the desired rule, click OK.

- To delete rules in bulk, select the checkboxes of the desired rules, click Delete and OK.

Export and Import Auto Defense Rules

The auto defense rules configured on Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired auto defense rules in the exported file, and import the file to PBX again. This topic describes how to export and import auto defense rules.

Export auto defense rules

You can export all auto defense rules to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Security > Security Rules > Auto Defense.
2. Click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see [Auto Defense Rule Parameters](#).

Import auto defense rules

We recommend that you export auto defense rules to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 50 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information , see [Auto Defense Rule Parameters](#).

Procedure

1. Log in to PBX management portal, go to Security > Security Rules > Auto Defense.
2. Click Import.
3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The auto defense rules in the CSV file will be displayed in the Auto Defense list.

Blocked IPs


Manage Blocked IP Addresses

This topic describes how to view or delete IP addresses that were blocked.

View blocked IP address

1. Log in to PBX management portal, go to Security > Security Rules > Blocked IPs.
2. Check details of the IP address that was blocked.
 - Defense Type: The defense type.
 - Block Type: Whether an account or an IP address was blocked.
 - Block Range: The account range or port range that was blocked.
 - Time of Attack: The time that the blocked account or IP address tried to attack the system.
 - Protocol: The protocol that the blocked account or IP address tried to attack.
 - Attacked Port: The port that the blocked account or IP address tried to attack.
 - Source IP Address: The IP address from which the attack was originated.
 - Expiration Date: The date and time on which the block would expire.

Delete blocked IP address

1. Log in to PBX management portal, go to Security > Security Rules > Blocked IPs.
2. Delete one or more IP addresses according to your needs.
 - To delete an IP address, click  beside the desired IP address, click OK.
 - To delete IP addresses in bulk, select the checkboxes of the desired IP addresses, click Delete and OK.

Outbound Call Frequency Restriction

Add an 'Outbound Call Frequency Restriction' Rule

For security purpose, we recommended that you use Outbound Call Frequency Restriction rule to restrict the outbound call frequency in Yeastar P-Series PBX System. The PBX has a default rule to limit extension users to make maximum 5 outbound calls in 1 second, you can also set up your own rules according to your need. With the restriction rules, the system can be protected against the threat of toll fraud.

Procedure

1. Log in to PBX management portal, go to Security > Security Rules > Outbound Call Frequency Restriction, click Add.
2. In the pop-up window, configure the following settings:
 - a. In the Name field, set a name to help you identify the rule.
 - b. Click Add and set up the restriction parameters:
 - Number of Calls: Set the limit number of outbound calls.
 - Time Period: Set a specific time period, and then select the time unit as Minute(s) or Second(s).
 - c. Click Save and Apply.


What to do next

Apply the Outbound Call Frequency Restriction rule to limit the extensions. For more information, see [Limit Outbound Call Frequency of an Extension](#).


Manage 'Outbound Call Frequency Restriction' Rules

This topic describes how to edit or delete Outbound Call Frequency Restriction rules.

Edit an 'Outbound Call Frequency Restriction' rule

1. Log in to PBX management portal, go to Security > Security Rules > Outbound Call Frequency Restriction.
2. Select the desired rule, click .
3. Edit rule settings according to your needs.
4. Click Save and Apply.

Delete 'Outbound Call Frequency Restriction' rules

1. Log in to PBX management portal, go to Security > Security Rules > Outbound Call Frequency Restriction.
2. Delete one or more rules according to your needs.
 - To delete a rule, click  beside the desired rule, click OK.
 - To delete rules in bulk, select the checkboxes of the desired rules, click Delete and OK.

Export and Import 'Outbound Call Frequency Restriction' Rules

The Outbound Call Frequency Restriction rules configured in Yeastar P-Series PBX System can be exported and saved as a template. You can fill in desired Outbound Call Frequency Restrictions in the exported file, and import the file to PBX again.

Export 'Outbound Call Frequency Restriction' rules

You can export all Outbound Call Frequency Restriction rules to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX management portal, go to Security > Security Rules > Outbound Call Frequency Restriction.
2. Click Export.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see ['Outbound Call Frequency Restriction Rule' Parameters](#).

Import 'Outbound Call Frequency Restriction' rules

We recommend that you export Outbound Call Frequency Restriction rules to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 50 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information, see ['Outbound Call Frequency Restriction Rule' Parameters](#).

Procedure

1. Log in to PBX management portal, go to Security > Security Rules > Outbound Call Frequency Restriction.
2. Click Import.
3. In the pop-up window, click Browse, and select your CSV file.
4. Click Import.

The Outbound Call Frequency Restriction rules in the CSV file will be displayed in the Outbound Call Frequency Restriction list.



Console/SSH Access

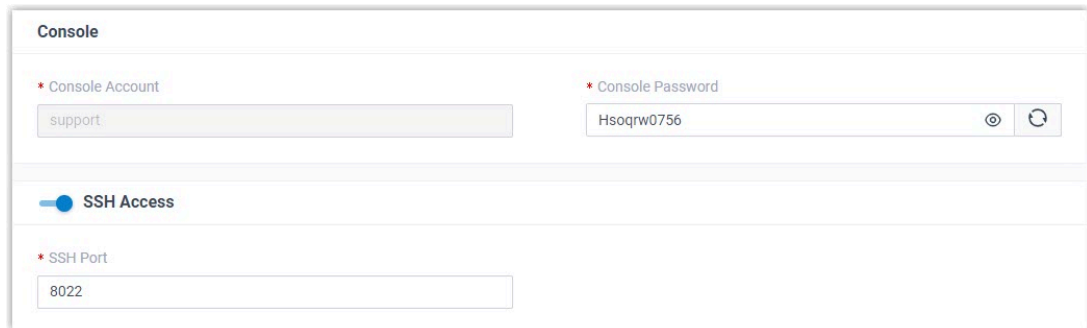
Access the System via SSH

This topic takes Putty as an example to introduce you how to access Yeastar P-Series PBX System via SSH.

Procedure

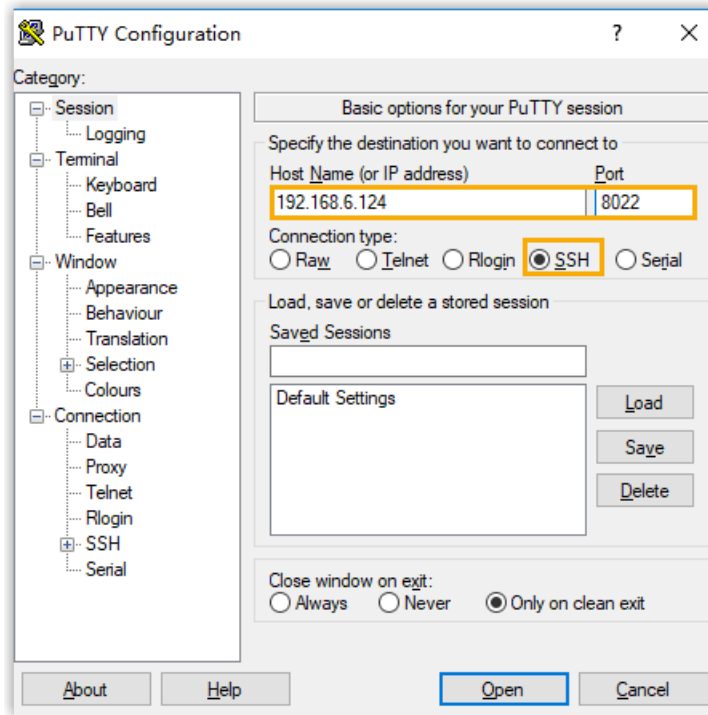
1. Enable SSH, check SSH port, console account, and console password on the PBX.
 - a. Log in to PBX management portal, go to Security > Security Settings > Console/SSH Access.
 - b. Enable SSH Access.
 - c. Check SSH port, console account, and console password.

 **Tip:**
Click  to view the password.



The screenshot shows the 'Console' settings page in the PBX management portal. It features three main sections: 'Console Account' with a text input field containing 'support'; 'Console Password' with a text input field containing 'Hsoqrw0756' and a toggle icon (an eye with a slash) and a refresh icon; and 'SSH Access' which is currently turned on, indicated by a blue slider. Below this, the 'SSH Port' is set to '8022' in a text input field.

2. Enter access information on Putty.
 - a. In the Connection type field, choose SSH.
 - b. In the Host Name (or IP address) field, enter your PBX's IP address.
 - c. In the Port field, enter SSH port that you have configured on the PBX.
 - d. Optional: On the left navigation bar, click Window > Lines of scrollback, set a scrollbar line number, so that you can get sufficient lines of log for debug analysis.
 - e. Click Open.



3. Verify your account and password.
 - a. In the login as field, enter support.
 - b. Copy console password from PBX.
 - c. In the password field, right click to paste the password.

Result

If the following figure shows, you can successfully access and debug the PBX.



Certificates

Upload TLS certificates to the PBX

Yeastar P-Series PBX System supports TLS protocol to secure SIP messaging. Before using TLS protocol, you may need to upload a TLS certificate.

Background information

With TLS protocol enabled on the PBX, a TLS certificate may be required in the following situations:

- When the PBX acts as a server, a server certificate is required.

If the PBX requires to verify TLS client (PBX Settings > SIP Settings > TLS > TLS Verify Client), you need to upload a client certificate to both PBX and TLS client, or the TLS connection would fail.

- When the PBX acts as a client, whether a client certificate is required depends on the server.

If the PBX requires to verify TLS server (PBX Settings > SIP Settings > TLS > TLS Verify Server), you need to upload a server certificate.

Upload a TLS server certificate

Prerequisites

You have prepared a server certificate in `.pem` format.

Procedure

1. Log in to PBX management portal, go to Security > Security Settings > Certificates, click Upload.

A window pops up, which requires you to select certificate type and upload a certificate.



Note:

You can ONLY upload 3 certificates.

2. In the Certificate Type drop-down list, choose PBX Certificate.
3. Click Browse to select the desired certificate.
4. Click Upload.

Result

The certificate is uploaded successfully, and is displayed on Certificates list.

Upload a TLS client certificate

Prerequisites

You have prepared a client certificate in `.cer` or `.crt` format.

Procedure

1. Log in to PBX management portal, go to Security > Security Settings > Certificates, click Upload.

A window pops up, which requires you to select certificate type and upload a certificate.



Note:

You can ONLY upload 20 certificates.

2. In the Certificate Type drop-down list, choose Trusted Certificate.
3. Click Browse to select the desired certificate.
4. Click Upload.

Result

The certificate is uploaded successfully, and is displayed on Certificates list.

Upload HTTPS Certificates to the PBX

Yeastar P-Series PBX System supports HTTPS protocol to secure SIP messaging when you access the PBX from web browser. Before using HTTPS protocol, you need to upload a PBX certificate.

Background information

When you access PBX from web browser, the PBX acts as a server and the web browser acts as a client. A certificate helps verify your PBX's IP address and secures your data transmission.

Prerequisites

You have prepared a server certificate in `.pem` format.

Procedure

1. Log in to PBX management portal, go to Security > Security Settings > Certificates, click Upload.

A window pops up, which requires you to select certificate type and upload a certificate.



Note:

You can ONLY upload 3 certificates.

2. In the Certificate Type drop-down list, choose PBX Certificate.
3. Click Browse to select the desired certificate.
4. Click Upload.


Result

The certificate is uploaded successfully, and is displayed on Certificates list.

Delete Certificates

This topic describes how to delete one or more certificates on Yeastar P-Series PBX System.

Procedure

1. Log in to PBX management portal, go to Security > Security Settings > Certificates.
2. Delete one or more certificates according to your needs.
 - To delete a certificate, click  beside the desired certificate, click OK.
 - To delete certificates in bulk, select the checkboxes of the desired certificates, click Delete and OK.

Result

The certificates are removed from the list.

What to do next


Reboot the system to take effect.


Allowed Country IPs

Restrict Specific Countries or Regions from Accessing Yeastar P-Series PBX System

By default, all the countries and regions are allowed to access Yeastar P-Series PBX System. Sometimes hackers may remotely access your phone system to make international and long-distance calls, monitor conversations, or do other operations that may cause security threats to your phone system. In this case, you can restrict specific countries or regions from accessing your phone system.

Procedure

1. Log in to PBX management portal, go to Security > Security Settings > Allowed Country IPs.
2. Turn on the option Enable Allowed Country/Region IP Access Protection.
3. Allow one or more countries or regions to access the PBX.
 - To allow a specific country or region to access the PBX, do as follows:
 - a. In the search box, enter a desired country or region.
 - b. In the Operations column, set the status to  .
 - To allow multiple countries or regions to access the PBX, do as follows:
 - a. Select the checkboxes of desired countries or regions, click Allow.

The status will be changed to  .

Result

Only the devices with IP addresses originating from the allowed countries or regions can access the PBX.


Tip:

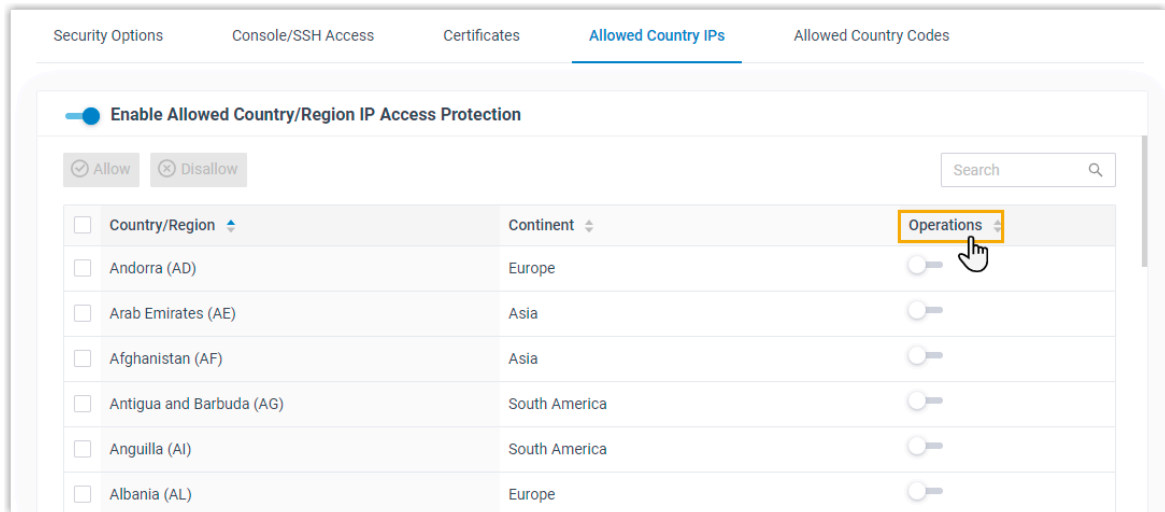
For the disallowed countries or regions, if you want to allow a specific IP address to access the PBX, you can add a static defense rule to accept connections from the desired IP address. For more information, see [Add a Static Defense Rule](#).

Check Allowed Country/Region IP

By default, all the countries and regions are displayed in ascending (A to Z) alphabetical order, whether they are allowed to access Yeastar P-Series PBX System or not. To check the allowed country/region IP, you need to sort all the countries and regions again.

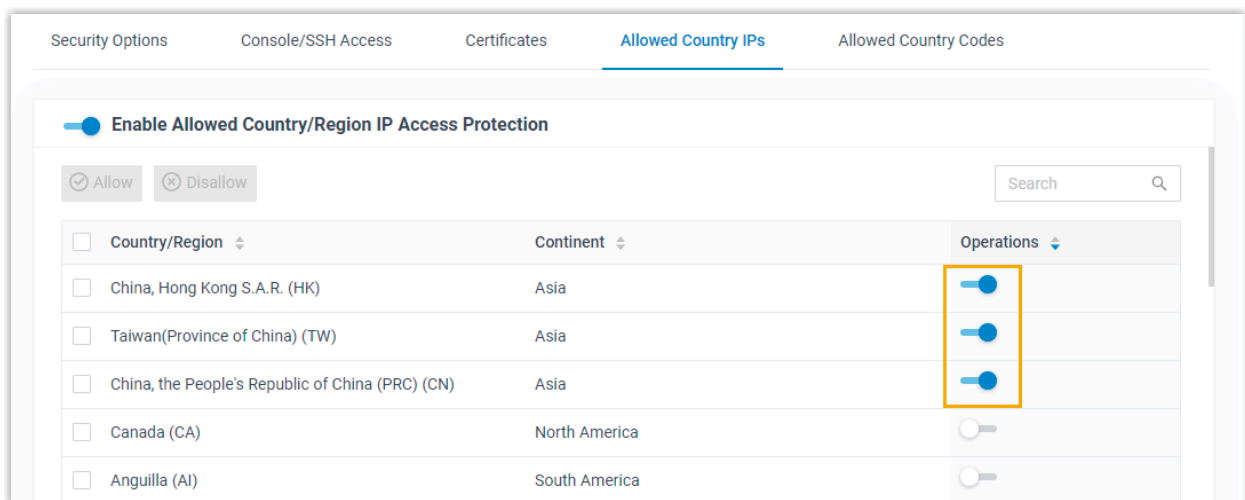
Procedure

1. Log in to PBX management portal, go to Security > Security Settings > Allowed Country IPs.
2. Click  beside Operations.



Result

All the countries and regions that are allowed to access the PBX are moved to the top.



Allowed Country Codes

Restrict International Calls to Specific Countries or Regions

If there is an outbound route on your PBX that allows outbound international calls, the authorized users can make international calls to all the countries and regions. To prevent toll fraud, you can restrict users from making international calls to specific countries or regions.

Scenario

A manufacturer has a factory in Mexico, and his or her target customers are in Argentina. The manufacturer wants to restrict employees from making international calls to countries and regions except Argentina (country code 54).

Procedure

Based on the above scenario, you need to follow the instructions below to realize restrictions on international dialing:


- [Step1. Allow international calls to Argentina only](#)
- [Step2. Allow employees to make international calls](#)

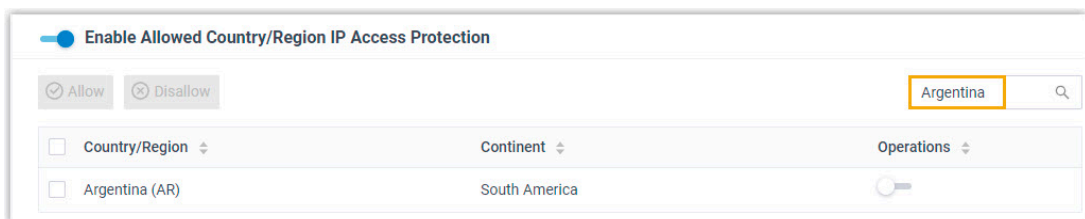
Step1. Allow international calls to Argentina only

1. Log in to PBX management portal, go to Security > Security Settings > Allowed Country Codes.
2. Enable international dialing protection, and set international dialing code.
 - a. Turn on the option Enable Allowed Country/Region Code Dialing Protection.
 - b. In the International Dialing Code field, enter the prefix of international call according to your country. In the scenario, enter 00.
When an employee tries to call a number starting with 00, the PBX's outbound route will identify this call as an international call.

Note:

Make sure there is at least one outbound route that matches with the international dialing code to route international calls out.

- c. Click  and Apply.
3. Set the countries or regions to which employees can make international calls.
 - a. In the search box, enter a desired country or region. In the scenario, enter Argentina.



Country/Region	Continent	Operations
Argentina (AR)	South America	<input type="checkbox"/>

- b. In the Operations column, set the status to .

Note:

Some countries or regions share the same code (e.g. the country code for Canada and America is 1). If you allow international dialing to a country or a re-

gion, employees can also make calls to the countries or regions that share the same code.

c. Click Apply.

Step2. Allow employees to make international calls

By default, after you enable country/region code dialing protection, all the users are not allowed to make international calls. To allow employees to make international calls, you need to grant permission to desired employees.

1. Go to Extension and Trunk > Extension.
2. Select the checkboxes of desired extensions, click Edit.
3. Click Security tab.
4. In the Call Restrictions section, select the checkbox of Bulk Edit and unselect the checkbox of Disallow International Calls.
5. Click Save and Apply.

Result

Authorized employees can make international calls to Argentina (country code 54).

The PBX has an outbound route configured as follows:

* Pattern	Strip	Prepend	Operations
00.			


When an authorized employee dials a number, PBX's outbound route will check if the dialing is valid:

- When an authorized employee dials 00541938384, the dialing is considered as valid.
- When an authorized employee dials 00621938384, the dialing is considered as invalid.
- When an authorized employee dials 541938384, it will not be considered as an international dialing, and the PBX will check if there is a matched outbound route to route the call out.

Block Outbound International Calls

To restrict users from making international calls, you can restrict dial pattern of outbound routes, or set up international dialing protection. This topic describes how to set up international dialing protection to block outbound international calls.

Procedure

1. Log in to PBX management portal, go to Security > Security Settings > Allowed Country Codes.
2. Turn on the option Enable Allowed Country/Region Code Dialing Protection.
3. In the International Dialing Code field, enter the prefix of international call according to your country.
4. Click  and Apply.

Result

All the extension users can NOT make international calls.

Maintenance

Upgrade

Check for Available Firmware Updates

This topic describes how to automatically or manually check for firmware updates.

Automatic check for firmware updates

Prerequisites


Make sure the PBX can access the Internet.

Procedure


1. Log in to PBX management portal, go to Maintenance > Upgrade.
2. In the Automatic Upgrade section, select Check for updates and notify me.
3. In the Automatically check for updates at drop-down list, set when the system should check for new version. This can be a daily or weekly check.
4. Click Save.


Result

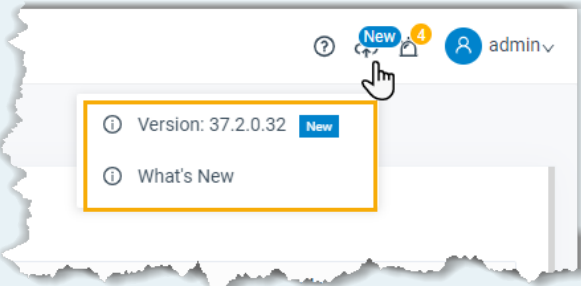
The system will regularly check for new firmware.

 Note:

If a new firmware is detected, the followings can be achieved:

- At the top-right corner of PBX management portal,  is displayed.

Click , click What's New to check release notes for the new version or click Version to go to upgrade page.



- The system will notify you via specific notification methods if you have enabled notification for New System Firmware Detected event.

Manual check for firmware updates

Prerequisites

Make sure the PBX can access the Internet.

Procedure

1. Log in to PBX management portal, go to Maintenance > Upgrade.
2. Click Check for the New Firmware.

Result

If a new firmware is detected, you will find a table as below. Click the link under Release Notes to check what's updated in the new version, and decide whether to upgrade the firmware now.

Version	Release Notes	Upgrade
37.1.0.13	https://help.yeastar.com/en/p-series-appliance-edition/release-notes/v37.1.0.13.html	Upgrade Now

Schedule Automatic Firmware Upgrade

This topic describes how to schedule auto detection and upgrade of new firmware.

Prerequisites

- Make sure Yeastar P-Series PBX System can access the Internet.
- We recommend that you [create a backup file](#) for PBX configurations.

Procedure

1. Log in to PBX management portal, go to Maintenance > Upgrade.
2. In the Automatic Upgrade section, select Check for updates and automatically install.
3. In the Automatically check for updates at drop-down list, set when the system should check for and upgrade new version. This can be a daily or weekly check and upgrade.

Note:

We recommend that you set a time that is beyond your office hours.

4. Click Save.

Result

The system will regularly compare local version with the latest version on Yeastar Firmware Server, and automatically upgrade the firmware.

Manually Upgrade PBX Firmware

This topic describes two methods to manually upgrade PBX firmware.

Manually upgrade PBX via Internet

Prerequisites

We recommend that you [create a backup file](#) for PBX configurations before you start upgrading the PBX.

Procedure

1. Log in to PBX management portal, go to Maintenance > Upgrade, click Check for the New Firmware to check if there's a new firmware.

If the system detects a new firmware, the following table is displayed:

Version	Release Notes	Upgrade
37.1.0.13	https://help.yeastar.com/en/p-series-appliance-edition/release-notes/v37.1.0.13.html	Upgrade Now

2. Click the Release Notes link to check the update details of the new version.
3. Upgrade system firmware.
 - a. Click Upgrade Now.

Important:

- Ensure the connection to Internet and power supply when the PBX is upgrading.
- Make sure there aren't ongoing calls, or the calls would be disconnected.

- b. In the pop-up dialog box, click OK.

Result

The PBX starts upgrading the firmware.

Important:

When the PBX is upgrading, do NOT turn off the power, or the system will get damaged.

Manually upgrade PBX via a local firmware file

Prerequisites

- Go to [Yeastar Firmware Download Center](#) to check and download the new firmware.
- We recommend that you [create a backup file](#) for PBX configurations before you start upgrading the PBX.

Procedure

1. Log in to PBX management portal, go to Maintenance > Upgrade > Manual Upgrade.
2. Click Browse to select a firmware file.



Note:

The firmware file format should be `.bin`, and the file name should not contain special characters.

3. Optional: To reset system configurations to factory defaults, check the option Reset Configuration to Factory Defaults.



Important:

If you check the option, all your PBX configurations will be erased.

4. Click Upgrade.

Result

The PBX starts uploading the file and upgrading the firmware automatically.



Important:

When the PBX is upgrading, do NOT turn off the power, or the system will get damaged.

Backup and Restore

Overview of Backup and Restore

Yeastar P-Series PBX System supports to back up configuration data, and restore data on the same PBX or another PBX.

How Backup and Restore feature benefits your work


Yeastar P-Series PBX System integrates backup and restore feature, which helps you achieve the followings:

- Create regular and scheduled backups.
- Easy data transfer from one PBX to another.
- Quick restoration and recovery in case of system failure.


Backup data

Yeastar P-Series PBX System supports to back up the following configuration data:

- System Configuration: All the configurations on the system.
- Custom Prompts
- CDR
- Company Contacts and Phonebooks Settings

 Note:
The option is available for Enterprise/Ultimate Plan.


- Company Contacts

 Note:
The option is available for Basic Plan.

Backup locations

Backup files can be stored in the following locations:

- Local drive: The PBX's local drive.
- External device: USB flash drive, hard disk drive, and SD card.

 Note:
Hard disk drive and SD card are ONLY supported on P560 and P570.

- Network drive

Backup file cleanup

By default, when the number of backup files reaches 5, the oldest files will be replaced by the newest files. You can retain the default value, or change the value according to your needs.

For more information, see [Auto Cleanup Settings](#).

Backup and restore logs

The PBX always makes records whoever backs up or restores the PBX configuration data, you can check the operation details on PBX web interface.

For more information, see [Manage Operation Logs](#).

Create an On-Demand Backup

This topic describes how to manually back up PBX configurations.

Prerequisites

Before backing up configuration data, you need to decide the followings:

- Where - Whether to save the backup file to local drive, external device, or network drive. If you want to save the file to external device or network drive, you need to set up an external device or add a network drive on the system first. For more information, see the following topics:
 - [Set up a USB Flash Drive](#)
 - Set up a Hard Disk Drive
 - [Set up an SD Card](#)
 - [Add a Windows Network Drive](#)
 - [Add a Mac Network Drive](#)
- What - Whether to back up custom prompts, CDR, or company contacts and phonebooks settings.

Procedure

1. Log in to PBX management portal, go to Maintenance > Backup and Restore, click Backup.
2. Configure backup settings.
 - File Name: Retain the default name or enter a name to help you identify it.
 - Comments: Add a note to the backup file.
 - Storage Location: Select a location to save the backup file.

Note:

To prevent backup failure in case of disconnection to external device or network drive, we recommend that you save the backup file on the local flash (LOCAL).

- The backup file will include: Select the items that will be backed up.
 - System Configuration: All the configurations on the system.
 - Custom Prompts
 - CDR
 - Company Contacts and Phonebooks Settings

Note:

The option is available for Enterprise/Ultimate Plan.

- Company Contacts

Note:

The option is available for Basic Plan.

3. Click Save.

Result

The created backup file is displayed in Backup and Restore list and is stored in the selected location.

Set up an Automatic Backup Schedule

Yeastar P-Series PBX System supports to automatically back up specific configuration data at the scheduled time. This topic describes how to set up an automatic backup schedule.


Prerequisites

Before backing up configuration data, you need to decide the followings:

- Where - Whether to save the backup file to local drive, external device, or network drive. If you want to save the file to external device or network drive, you need to set up an external device or add a network drive on the system first. For more information, see the following topics:
 - [Set up a USB Flash Drive](#)
 - Set up a Hard Disk Drive
 - [Set up an SD Card](#)
 - [Add a Windows Network Drive](#)
 - [Add a Mac Network Drive](#)
- What - Whether to back up custom prompts, CDR, or company contacts and phone-books settings.
- When - Make a daily, weekly, or monthly backup.

Procedure

1. Log in to PBX management portal, go to Maintenance > Backup and Restore, click Backup Schedule.
2. In the pop-up window, enable Backup Schedule.
3. Configure an automatic backup schedule.
 - a. Set the automatic backup period. This can be a daily, weekly, or monthly backup.
 - Frequency: Choose to make a daily, weekly, or monthly backup.
 - Daily: If you choose the option, select a time from the drop-down list. The system backs up the settings at this time of the day.
 - Weekly: If you choose the option, choose a day of week and select a time from the drop-down list. The system backs up the settings at this time of the week.
 - Monthly: If you choose the option, choose a day and select a time from the drop-down list. The system backs up the settings on this day and time of the month.

 Note:

If you set the day to 31, but the month only has 29 or 30 days, the system will not make a backup.

- b. In the Storage Location drop-down list, select where you want to save the backup file.

Note:

To prevent backup failure in case of disconnection to external device or network drive, we recommend that you save the backup file on the local flash (LOCAL).

c. In the The backup file will include section, choose the items that will be backed up.

- System Configuration: All the configurations on the system.
- Custom Prompts
- CDR
- Company Contacts and Phonebooks Settings

Note:

The option is available for Enterprise/Ultimate Plan.

- Company Contacts

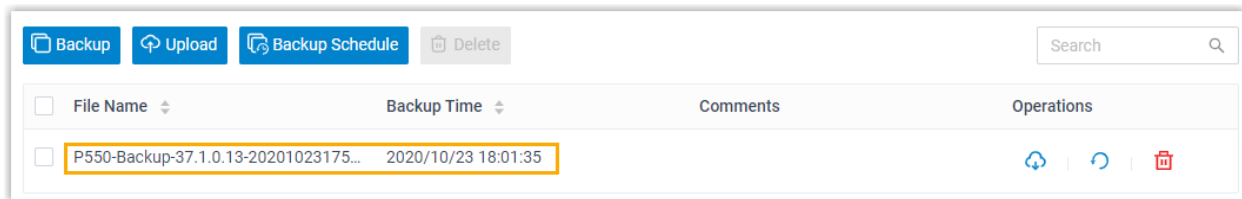
Note:

The option is available for Basic Plan.

4. Click Save.

Result

The system will back up the specified configuration data at the scheduled time. The automatic generated backup file will be displayed in the Backup and Restore list.



Restore Your System from a Backup


In case of data loss or system failure, you can restore the PBX from a backup. This topic describes how to restore data on the PBX.

Prerequisites

- Make sure that you have backed up system configurations and required files, such as custom prompts and CDR.
- Read and understand restrictions for data restoration.
 - You can restore a backup file that is created from an older version of PBX.
 - Example: Restoring a backup file (v37.1.0.10) to PBX (v37.1.0.13) would work.
 - You can NOT restore a backup file that is created from a newer version of PBX.

Example: Restoring a backup file (v37.1.0.13) to PBX (v37.1.0.10) would not work.

Procedure

1. Log in to PBX management portal, go to Maintenance > Backup and Restore.
2. Select a backup file to which you want to restore, click .
3. In the pop-up dialog box, click OK.
4. Reboot the PBX to take effect.

Result

The current configurations on your PBX are OVERWRITTEN with the backup data.

Related information

- [Create an On-Demand Backup](#)
- [Set up an Automatic Backup Schedule](#)

Restore Another System from a Backup

In case you have two PBXs of different models, and you want to replace one with the other, you can restore configuration data on the other PBX. This topic describes how to upload a backup file and restore configuration data on another PBX.

Prerequisites

- Make sure that you have backed up and downloaded the required configuration data.
- Read and understand restrictions for data restoration.
 - You can restore a backup from a PBX with lower model number onto a PBX with higher model number.

Example: Restoring a backup file (created on P550) to P560 would work.

- You can NOT restore a backup from a PBX with higher model number onto a PBX with lower model number.

Example: Restoring a backup file (created on P560) to P550 would not work.


Procedure

1. Upload a backup file.
 - a. Log in to PBX management portal, go to Maintenance > Backup and Restore.
 - b. Click Upload.
 - c. In the pop-up window, select a backup file and add a note according to your needs.
 - i. Click Browse to select a backup file.



Note:

The file format should be `.bak` and the file name should NOT contain special characters.

- ii. Optional: In the Comments field, add a note.
 - d. Click Upload.
2. Restore the backup file.
- a. In the Backup and Restore list, select the file that you want to restore, click .
 - b. In the pop-up dialog box, click OK.
 - c. Reboot the PBX to take effect.

Result

The current configurations on your PBX are **OVERWRITTEN** with the backup data.

Related information

[Create an On-Demand Backup](#)

[Set up an Automatic Backup Schedule](#)

Reboot

Reboot Yeastar P-Series PBX System on Web Interface

This topic describes how to reboot Yeastar P-Series PBX System on web interface.

Prerequisites

Make sure there aren't ongoing calls, or the calls would be disconnected.

Procedure

1. Log in to PBX management portal, go to Maintenance > Reboot.
2. In the Reboot Now section, click Reboot Now.
3. In the pop-up dialog box, click Yes to reboot the PBX.

Result

It takes about one minute to reboot the system.


If you have enabled notification for System Reboot event, the system will inform relevant contacts of the reboot via specific notification methods.

Schedule Automatic Reboot

To ensure the stability and robustness of Yeastar P-Series PBX System, you can schedule automatic reboot of the PBX at the scheduled time (non-office hours or weekends). This topic describes how to schedule a daily, weekly, or monthly reboot of Yeastar P-Series PBX System.

Procedure

1. Log in to PBX management portal, go to Maintenance > Reboot.
2. In the Reboot Schedule section, select the checkbox of Enable Auto Reboot.
3. Set when to perform an auto reboot.
 - Daily: If you choose the option, select a time from the drop-down list of Time.
The system will daily reboot itself at this time.
 - Weekly: If you choose the option, select a day of week from the drop-down list of Weekly, and select a time from the drop-down list of Time.
The system will weekly reboot itself at this time.
 - Monthly: If you choose the option, select a day from the drop-down list of Date, and select a time from the drop-down list of Time.
The system will monthly reboot itself on the day and time.

 Note:

If you set Date to 31, but the month only has 28, 29, or 30 days, the system will NOT reboot itself automatically.

4. Click Save.

Reset

Reset the System on Web Interface

This topic describes how to reset Yeastar P-Series PBX System on web interface.


Prerequisites

- Make sure there aren't ongoing calls, or the calls would be disconnected.
- We recommend that you [create a backup file](#) for PBX configurations.

Procedure

1. Log in to PBX management portal, go to Maintenance > Reset.
2. Set which configurations and data that you want to clear.
 - Reset All: Clear all the configurations and data on the PBX.

- **Reset Network Settings:** Reset the PBX's IP address to 192.168.5.150, and clear the configurations in Network > Basic Settings and Network > Public IP and Ports.
- **Reset CDR:** Clear all call logs.
- **Reset Backup Files:** Clear backup files.
- **Reset Prompts:** Clear custom prompts.

 **Note:**

Whether the option is enabled or not, system prompts, music on hold, and preference settings for all the prompts would be cleared.

- **Reset Company Contacts:** Clear company contacts, phonebooks, and Caller ID match settings.
 - **Reset Other System Configurations:** Reset all the logs and configurations except network, CDR, backup files, prompts, and contacts.
3. Click Factory Reset.
 4. In the pop-up dialog box, verify your operation and click Yes.

Result

It takes several minutes to reset the PBX. After resetting, you are redirected to the Installation Wizard page.

What to do next

Follow the [Installation Wizard](#) to set up the PBX.

Operation Logs

Operation Logs Overview

This topic describes what are operation logs, what operations are recorded, and introduces the storage and auto cleanup of operation logs.

What are operation logs

Operation logs record successful operations performed on Yeastar P-Series PBX System, and provide you with the followings to help you monitor and analyze the causes of systems errors or other types of problems.

- **Who:** Check who performed the operation. You can query all users' operations, or query operations by administrator or a specific extension.
- **When:** Check when the operation was performed. You can query operations by specific date and time.
- **What:** Check what operation was performed.

- Where: Check on which module the operation was performed. You can query operations by a specific module.

Storage of operation logs

Operation logs are saved in local storage, you can NOT change the storage location.

Auto cleanup of operation logs

By default, when operation logs reach 50,000, the system automatically deletes the oldest logs. You can change the value, or set the maximum days that logs can be retained. For more information, see [Auto Cleanup Settings](#).

Note:

A few logs related with system security and user privacy are RETAINED so that Yeastar Support can help you troubleshoot problems when toll fraud happens or PBX suffers from attack.

The operation logs that will NOT be automatically cleaned up are as follows:


Table 54.

Event Type	Event
Operation	Administrator Login Success
	Administrator Password Changed
	Web User Login Success
	Web User Login Failed
	Linkus Client Login Failed
	Extension User Password Changed
Telephony	Emergency Call Dialed Out
System	Yeastar SMTP Server Error
Security	Web User Locked Out
	Linkus User Blocked Out
	Extension Registration Blocked Out
	Auto Defense IP Blocked Out
	Outbound Call Frequency Exceeded
	Outbound Call to a Disallowed Country

Manage Operation Logs

This topic describes how to view and download operation logs on Yeastar P-Series PBX System.

View operation logs

1. Log in to PBX management portal, go to Maintenance > Operation Logs.
2. Set the filter criteria.
 - User: Query all users' operations, or query operations by administrator or a specific extension.
 - Module: Query operations on all modules, or query operations by a specific module.
 - IP Address: Query operations by the originated IP address.
 - Time: Query operations by specific date and time.
3. Optional: Click  beside the desired log to check operation details.

Download operation logs

1. Log in to PBX management portal, go to Maintenance > Operation Logs.
2. To download all the operation logs, click Download.
3. To download the filtered operation logs, set [the filter criteria](#), click Download.

Logs are exported to a CSV file.

Troubleshooting

Capture Network Packet

This topic describes how to capture packets on LAN port, WAN port, or loopback address of your local network interface card (NIC).

Background information


Ethernet Capture Tool may be required to capture packets in the following situations:

- Extension registration failure.
- No audio or one-way audio during a call.
- Occasional VoIP interconnection failure.

Procedure


1. Log in to PBX management portal, go to Maintenance > Troubleshooting > Ethernet Capture Tool.

2. In the Ethernet Interface drop-down list, set where you want to capture packets.
 - Any: Capture the packets on LAN port, WAN port, and loopback address (127.0.0.1) of your local network interface card (NIC).
 - LAN: Capture the packets on LAN port.
 - WAN: Capture the packets on WAN port.
3. Optional: In the IP Address field, enter an IP address. The system will only capture packets that travel to or from the IP address.

 Note:

If you don't set an IP address, the PBX will capture packets for all the IP addresses.

4. Optional: In the Port field, enter a port. The system will only capture packets that go through the port.

 Note:

If you don't set a port, the PBX will capture packets for all the ports.

5. Click Start.

The PBX starts to capture the Ethernet packet. During the time period, you should reproduce the problem of your VoIP trunks or extensions.
6. Click Stop to stop capturing.

The packets are intercepted and saved on PBX's local flash.
7. Click Download to download the captured packet.

What to do next

Decompress the `.tar` file and use [Wireshark](#) software to open the packet file.

Use IP Ping Tool to Diagnose Network Issues

This topic describes how to use IP Ping tool to test if Yeastar P-Series PBX System can reach a specific hostname or IP address, and introduces the test result.

Background information

Based on the Internet Control Message Protocol (ICMP), IP Ping is a network tool to determine if a destination server is accessible and estimate how long a packet takes to send and receive data from the server.

If you are suffering from the followings, you can use IP Ping to diagnose:

- Network issues.

For example, if you can not make calls, you can use IP Ping to check if the PBX can access external network.

- Poor VoIP call quality.

For example, if you are experiencing echo, buzzing, or latency during a call, you can use IP Ping to check jitter and latency, or if there are any packet loss.

Procedure

1. Log in to PBX management portal, go to Maintenance > Troubleshooting > IP Ping.
2. In the Target Host field, enter the target domain or IP address.
3. Click Start.
4. Click Stop as your need.

Read the output

Example1: A successful Ping

```
start...
PING 192.168.6.11 (192.168.6.11): 56 data bytes
64 bytes from 192.168.6.11: seq=0 ttl=64 time=8.853 ms
64 bytes from 192.168.6.11: seq=1 ttl=64 time=0.778 ms
64 bytes from 192.168.6.11: seq=2 ttl=64 time=1.394 ms

--- 192.168.6.11 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.778/3.675/8.853 ms
```

The above example shows the followings:

- The device sends 3 ping packets and receives response for all the 3 packets.
- The ping packets' size are 64 bytes.
- The TTL value is 64, which indicates that packets are always forwarded to the same region.
- The time indicates that how long it takes to receive an Echo Response message after an Echo Request message is sent. This parameter can be used as a reference to determine whether the network is congested.

Example2: A failed Ping

```
start...
PING 192.168.7.2 (192.168.7.2): 56 data bytes

--- 192.168.7.2 ping statistics ---
60 packets transmitted, 0 packets received, 100% packet loss
```

The above example indicates that there is an issue of either the connection or the target device.

Use Traceroute Tool to Diagnose Network Issues

This topic describes how to use Traceroute tool to trace routes to a specific hostname or IP address, and introduces test results.

Background information

Traceroute is a network tool that tracks the gateways that packets pass through from Yeastar P-Series PBX System to a destination server and helps you check network connectivity and locate network faults.

Procedure

1. Log in to PBX management portal, go to Maintenance > Troubleshooting > Traceroute.
2. In the Target Host field, enter the target domain or IP address.
3. Click Start.

The PBX starts to trace routes to the target domain or IP address.

4. Click Stop, or the traceroute will terminate automatically when completed.

Read the output

Example1: A good traceroute

```
start...
traceroute to www.baidu.com (36.152.44.95), 30 hops max, 46 byte
packets
 1 * * *
 2 * * *
 3 192.168.1.1 (192.168.1.1) 1.853 ms 11.642 ms 19.951 ms
 4 110.80.36.161 (110.80.36.161) 3.008 ms 2.966 ms 3.943 ms
 5 61.154.238.133 (61.154.238.133) 7.369 ms 27.982 ms 7.808
ms
 6 117.30.27.177 (117.30.27.177) 6.125 ms 117.30.24.213 (117.
30.24.213) 4.664 ms 4.376 ms
 7 202.97.36.117 (202.97.36.117) 26.446 ms 202.97.64.178 (202
.97.64.178) 22.534 ms 202.97.79.33 (202.97.79.33) 20.897 ms
 8 202.97.63.18 (202.97.63.18) 33.276 ms 202.97.76.238 (202.9
7.76.238) 36.685 ms 202.97.18.46 (202.97.18.46) 33.961 ms
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 221.183.14.14 (221.183.14.14) 40.599 ms 221.183.18.2 (221.
183.18.2) 54.233 ms
15 21.22.207.183.static.js.chinamobile.com (183.207.22.21) 43.
056 ms 53.602 ms 50.481 ms
16 122.23.207.183.static.js.chinamobile.com (183.207.23.122) 4
7.251 ms 126.23.207.183.static.js.chinamobile.com (183.207.23.1
26) 47.401 ms 110.23.207.183.static.js.chinamobile.com (183.20
7.23.110) 54.380 ms
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
```

```

22 * * *
23 202.97.23.149 (202.97.23.149) 14.133 ms * 202.97.23.157 (
202.97.23.157) 28.851 ms
24 61.154.238.69 (61.154.238.69) 7.096 ms 117.30.24.213 (117.
30.24.213) 4.682 ms 117.30.27.189 (117.30.27.189) 2.758 ms
25 113.96.4.170 (113.96.4.170) 14.663 ms 113.96.5.118 (113.96
.5.118) 17.857 ms 113.96.4.190 (113.96.4.190) 20.665 ms
26 * * *
27 * * *
28 * * *
29 110.80.36.161 (110.80.36.161) 4.278 ms 2.696 ms 3.900 ms
30 61.154.238.133 (61.154.238.133) 11.424 ms 4.690 ms 7.770
ms

```

The above example displays in the format of `HOP Domain Name (IP Address)`
`RTT1 RTT2 RTT3`.

- **Hop:** Whenever a packet is passed between a router, this is referred to as a “hop.” For example, in the output above, we can see that it takes 14 hops to reach `www.baidu.com` from the current location.
- **Domain Name [IP Address]:** The domain name, if available, often helps you see the location of a router. If this is unavailable, only the IP address of the router is displayed.
- **RTT1, RTT2, RTT3:** This is the round-trip time that it takes for a packet to get to a hop and back to your computer (in milliseconds). This is often referred to as latency, and is the same number you see when using ping. Traceroute sends three packets to each hop and displays each time, so you have some idea of how consistent (or inconsistent) the latency is. If you see a * in some columns, you didn’t receive a response - which could indicate packet loss.

Example2: A failed hop

```

start...
traceroute to www.baidu.com (14.215.177.38), 30 hops max, 46 byte
packets
1 * * *
2 * * *
3 192.168.1.1 (192.168.1.1) 1.702 ms 4.912 ms 1.873 ms
4 110.80.36.161 (110.80.36.161) 16.068 ms 2.642 ms 2.705 ms
5 61.154.238.129 (61.154.238.129) 5.405 ms 61.154.238.133 (6
1.154.238.133) 9.038 ms 61.154.238.129 (61.154.238.129) 4.084
ms
6 117.30.27.185 (117.30.27.185) 3.183 ms 117.30.24.213 (117.
30.24.213) 5.256 ms 29.543 ms
7 202.97.19.125 (202.97.19.125) 23.899 ms 202.97.23.153 (202
.97.23.153) 15.059 ms 202.97.21.69 (202.97.21.69) 12.542 ms
8 113.96.4.130 (113.96.4.130) 20.978 ms 113.96.4.54 (113.96.
4.54) 17.600 ms 113.96.4.102 (113.96.4.102) 18.980 ms

```

```

 9  113.96.4.209 (113.96.4.209)  18.324 ms  25.160 ms  106.96.13
5.219.broad.fs.gd.dynamic.163data.com.cn (219.135.96.106)  29.13
5 ms
10  14.29.117.242 (14.29.117.242)  22.918 ms  121.14.67.150 (121
.14.67.150)  15.187 ms  14.215.32.126 (14.215.32.126)  15.963 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *

```

In the above example, hop1 and hop2 do not respond to the request, but they forward traffic to hop3. The test fails at hop11, and continues to fail all the way to hop30 (the max hops).

Example3: A routing loop

```

start...
traceroute to 192.168.8.127 (192.168.8.127), 30 hops max, 46 byte
 packets
 1  192.168.8.127 (192.168.8.127)  1.725 ms  1.455 ms  1.343 ms
 2  192.168.8.127 (192.168.8.127)  1.702 ms  4.912 ms  1.873 ms
 3  192.168.8.128 (192.168.8.128)  1.068 ms  2.642 ms  2.705 ms
 4  192.168.8.127 (192.168.8.127)  3.183 ms  5.256 ms  9.543 ms
 5  192.168.8.128 (192.168.8.128)  2.978 ms  1.600 ms  1.980 ms

```

In the above example, a loop occurs between 192.168.8.127 and 192.168.8.128. Data will pass back and forth from one to the other until the session times out or the maximum hop limit is reached.

Troubleshoot and Monitor Analog Ports

If there is a problem on the FXO port, FXS port, or GSM/3G/4G channel, you can use the Port Monitor Tool to monitor the port, and download the packet to analyze it.

Procedure

1. Log in to PBX management portal, go to Maintenance > Troubleshooting > Port Monitor Tool.
2. Choose the Port that has a problem.
3. Click Start.

The PBX will start to monitor the port. During this time, you should duplicate the problem of the port.

4. Click Stop to stop monitoring.
5. Click Download to download the file.

What to do next

Decompress the `.tar` file and use Audition software to open the `.raw` file and analyze it.

System Logs

System Logs Overview

This topic describes what are system logs, which level's logs are recorded, and introduces the storage and auto cleanup of system logs.


What are system logs

System logs are log files that contain information about system activities, which helps you troubleshoot and debug the system. The daily-generated system logs are displayed on System Logs, you can view and download logs on PBX management portal.

Log levels

Yeastar P-Series PBX System provides multiple log levels, each of them records different information. The supported log levels are as follows:

- Information: Basic information.
- Notice: Notice information.
- Warning: Warning information.
- Error: Error information.
- DTMF: DTMF information.
- Time Log: Add time stamp of system logs.
- Debug: Debug information.
 - Enable SIP Debug
 - Enable RTP Debug
 - Enable BRI Debug
 - Enable SS7/PRI Debug

 Note:

The feature is ONLY supported on P560 and P570.

Storage of system logs

System logs are saved in local storage, you can NOT change the storage location.

Auto cleanup of system logs


By default, the system automatically deletes the oldest system logs every 7 days, or when logs reach 10MB. You can change the maximum file size or days that logs can be retained. For more information, see [Auto Cleanup Settings](#).

Configure Log Level

Yeastar P-Series PBX System allows you to configure log level to gather only information that you consider important. This topic describes how to configure log level.


Procedure

1. Log in to PBX management portal, go to Maintenance > System Logs.
2. Click Log Level.
3. In the pop-up window, decide which level's logs that you want to trace.
 - Information: Basic information.
 - Notice: Notice information
 - Warning: Warning information.
 - Error: Error information.
 - DTMF: DTMF information.
 - Time Log: Add time stamp of system logs.
 - Debug: Debug information.
 - Enable SIP Debug
 - Enable RTP Debug
 - Enable BRI Debug

 Note:

To enable the feature, you must select the checkbox of Information.

- Enable SS7/PRI Debug

 Note:

The feature is ONLY supported on P560 and P570.

4. Click Save and Apply.


Result

The system will generate logs of the specified levels every day.

Manage System Logs

This topic describes how to download or delete system logs on Yeastar P-Series PBX System.

Download system logs

1. Log in to PBX management portal, go to Maintenance > System Logs.
2. Download one or more system logs according to your needs.
 - To download a system log, click  beside the desired log.
 - To bulk download system logs, select the checkboxes of the desired logs, click Download.


The desired logs are downloaded and compressed into a `.tar` file.



Tip:

You can decompress the file and open logs by Notepad++ or other editor software.

Delete system logs

1. Log in to PBX management portal, go to Maintenance > System Logs.
2. To delete a system log, click  beside the desired log.
3. To bulk delete system logs, select the checkboxes of the desired logs, click Delete.

CDR and Reports

CDR

Call Detail Record (CDR) Overview

The Call Detail Record (CDR) feature provides information about calls over Yeastar P-Series PBX System. This topic describes parameters and auto cleanup of CDR.

CDR parameters

A CDR contains the following information:

- ID: A unique identifier for each call.
- Time: When the call was made or received.
- Call From: The number or the name of the caller.
- Call To: The number or the name of the callee.
- Call Duration: The time between the call started and the call ended.
- Ring Duration: The time between the call started and the call answered.
- Talk Duration: The time between the call answered and the call ended.
- Status: Call status.
 - ANSWERED
 - NO ANSWER
 - BUSY
 - FAILED
 - VOICEMAIL
- Reason: The reason why the call was ended.
- Source Trunk: The call was received via which trunk.
- Destination Trunk: The call was sent out via which trunk.
- Communication Type:
 - Internal
 - Outbound
 - Inbound
- DID/DDI: The phone number that the caller dialed.
- Outbound Caller ID: The phone number that was displayed on the callee's phone.
- Caller IP Address: The IP address of the caller's device.
- PIN Code: The PIN code entered when making a call via a restricted outbound route.

CDR auto cleanup

By default, when the number of call logs reaches 200,000, the system automatically deletes the oldest call logs (relevant recordings are retained.). You can change the maximum value, or you can also set the maximum preservation days.

For more information, see [Auto Cleanup Settings](#).

Manage CDR

This topic describes how to view, download, and delete call logs.

View CDR


1. Log in to PBX management portal, go to Reports and Recordings > CDR.
2. Optional: Set the basic filter criteria.

- Time: Set the start date and the end date.

To specify a time period, click select time to set the start time and the end time.

- Call From: Set the caller's number or name.
- Call To: Set the callee's number or name.

 Tip:


To swap the callee for the caller, click .

- Status: Select a call status.
3. Optional: Set the advanced filter criteria.

a. Click .


b. On the Filter page, set the advanced criteria.

- Extension Group: Select an extension group. The system only queries group members' calls.
- Ring Duration: Set how long the callee's phone rang before the call was answered.

 Note:


Only numbers, -, =, <, <=, >, and >= are allowed.


- Talk Duration: Set the time between the call was answered and the call was ended.


 Note:

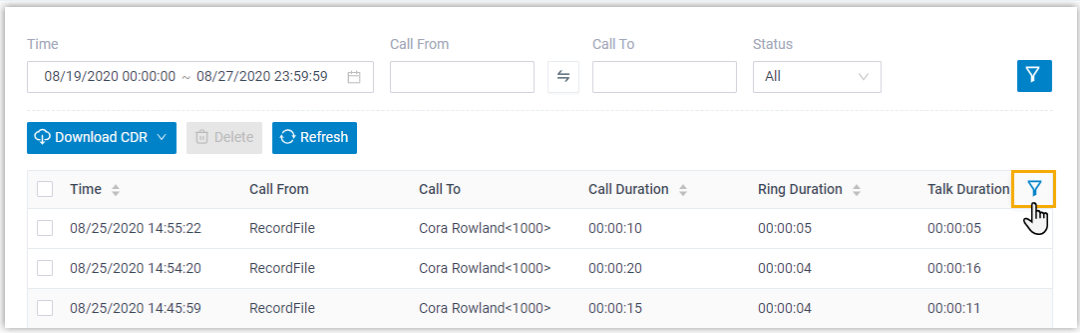
Only numbers, -, =, <, <=, >, and >= are allowed.

- Status: Select call status.
- All
 - ANSWERED
 - NO ANSWER
 - BUSY
 - FAILED

- VOICEMAIL
 - Communication Type: Select a type.
 - All
 - Internal
 - Outbound
 - Inbound
 - ID: Enter the unique identifier for a call.
 - Trunk: Select a trunk, which specifies the source or the destination trunk that the call went through.
 - Enable Number Fuzzy Search: Set whether to search for the fuzzy equivalent for the phone number.
 - PIN Code: Enter an existed PIN code, the system only queries the calls using this PIN code.
- c. Scroll up to click  to close the window.
The filtered call logs are displayed on the page.

 Note:

You can click  to decide which item will be displayed.



The screenshot shows a CDR interface with the following elements:

- Time range: 08/19/2020 00:00:00 ~ 08/27/2020 23:59:59
- Call From: [Empty field]
- Call To: [Empty field]
- Status: All
- Buttons: Download CDR (dropdown), Delete, Refresh
- Table with columns: Time, Call From, Call To, Call Duration, Ring Duration, Talk Duration
- A filter icon is highlighted in the Talk Duration column.

Time	Call From	Call To	Call Duration	Ring Duration	Talk Duration
<input type="checkbox"/> 08/25/2020 14:55:22	RecordFile	Cora Rowland<1000>	00:00:10	00:00:05	00:00:05
<input type="checkbox"/> 08/25/2020 14:54:20	RecordFile	Cora Rowland<1000>	00:00:20	00:00:04	00:00:16
<input type="checkbox"/> 08/25/2020 14:45:59	RecordFile	Cora Rowland<1000>	00:00:15	00:00:04	00:00:11

Download CDR

1. Log in to PBX management portal, go to Reports and Recordings > CDR.
2. To download all the call logs, select Download All CDR from the drop-down list of Download CDR.
3. To download the filtered call logs, [set the filter criteria](#) and select Download Filtered CDR from the drop-down list of Download CDR.

Call logs are exported to a CSV file.

Delete CDR

1. Log in to PBX management portal, go to Reports and Recordings > CDR.
2. Optional: [Filter call logs](#).
3. Select the checkboxes of the desired call logs, click Delete and OK.

! Important:
The relevant recording files will also be deleted.

Both call logs and recording files are deleted.

Call Report

Call Reports Overview

Yeastar P-Series PBX System provides intuitive visual call reports, which allow you to check call statistics of different objects, such as extensions, trunks, queues, ring groups, etc. This topic describes category of call reports, and methods of getting an instant or a scheduled call report.

Category of Call Reports

Yeastar Call Reports are categorized as Basic Reports and Advanced Reports. Which reports are accessible depends on the plan that your PBX supports.

Table 55.

Category	Description	Requirement
Basic Reports	Reports related with extensions, trunks, and DID/Outbound Caller ID activity. <ul style="list-style-type: none"> • Extension Call Statistics • Extension Call Activity • Trunk Activity • DID/Outbound Caller ID Activity 	No additional requirement.
Advanced Reports	Reports related with queues and ring groups. <ul style="list-style-type: none"> • Queue AVG Waiting & Talking Time • Queue Performance • Satisfaction Survey • Agent Login Activity • Agent Pause Activity • Agent Missed Call Activity • Agent Call Summary • Ring Group Statistics 	Require subscription to Yeastar P-Series Enterprise Plan or Ultimate Plan

Methods of getting a call report

Yeastar P-Series PBX System allows you to have an instant search and view of call reports on the PBX's management portal, or schedule call reports to be sent to your mailbox at the specified time and download the reports to your local device.

For more information about searching and viewing call reports on the PBX's web interface, see [View Call Reports](#).

For more information about scheduling call reports, see [Schedule Call Reports](#).

Call Reports

View Call Reports

This topic describes how to view call reports on Yeastar P-Series PBX System.

Procedure

1. Log in to PBX management portal, go to Reports and Recordings > Call Reports > Call Reports.
2. Set search criteria.
 - a. In the Report Type drop-down list, select the desired report.
 - b. Set a time period that the report covers.
 - c. Set one or more objects that you want to query.

Result

Relevant call statistics are displayed on the page.

Extension Call Statistics Report

Extension Call Statistics Report is a summary report displayed in pie chart, which makes it possible for you to query statistics of calls that have been made or received by a specific extension or extensions within a specific group, and view percentage and proportional data of call statistics.

Report details

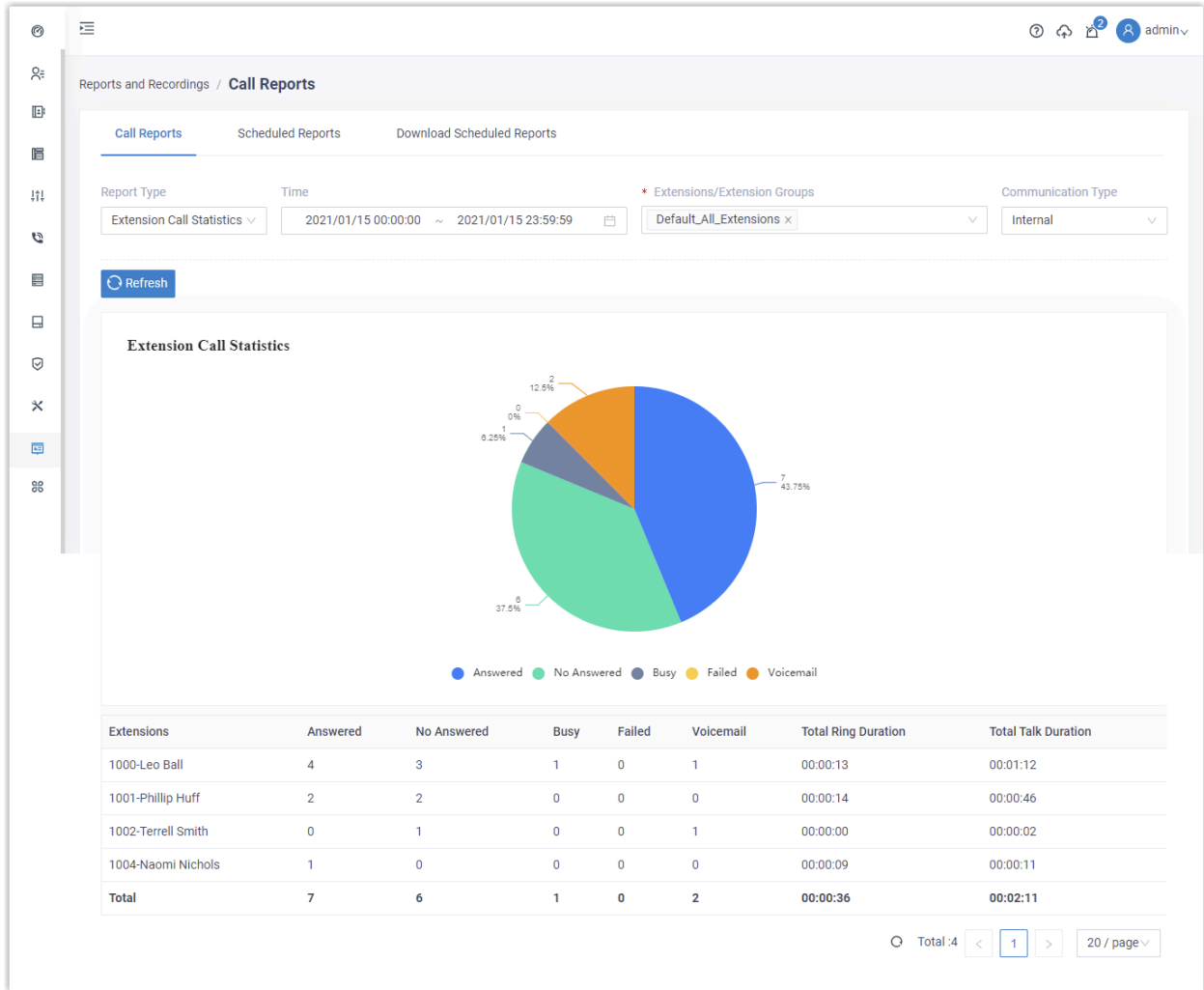
The following table lists the related parameters for Extension Call Statistics report.

Parameter	Description
Answered	The total number of calls that the extension answered.
No Answered	The total number of calls that were routed to the designated destination when the extension didn't answer the calls.

Parameter	Description
Busy	The total number of calls that were routed to the designated destination when the extension was busy.
Failed	The total number of calls that were failed to be made by the extension.
Voicemail	The total number of voicemails that the extension received.
Total Ring Duration	The total time between calls started and calls answered.
Total Talk Duration	The total time between calls answered and calls ended.

Report example

The following report shows internal call statistics of all the extensions in group Default_All-Extensions during 2021/01/15 00:00:00-2021/01/15 23:59:59.



Extension Call Activity Report

Extension Call Activity Report is a summary report displayed in line graph, which makes it possible for you to query statistics of calls that have been made or received by a specific extension or extensions within a specific group. The report allows you to track changes of call activity over a specific period of time, or compare changes over the same period of time.

Report details

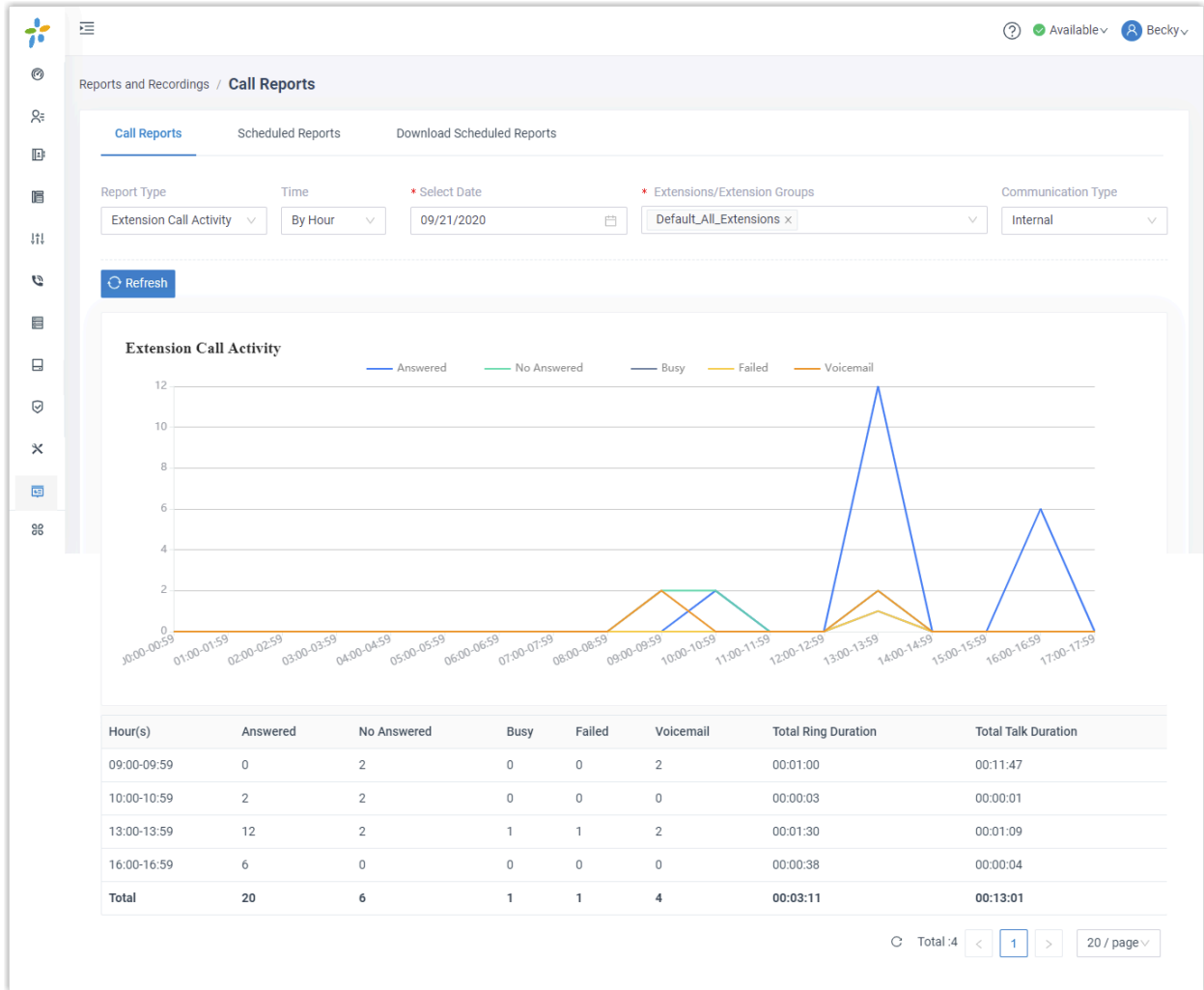
The following table lists the related parameters for Extension Call Activity report.

Parameter	Description
Answered	The total number of calls that the extensions answered.

Parameter	Description
No Answered	The total number of calls that were routed to the designated destination when the extensions didn't answer the calls.
Busy	The total number of calls that were routed to the designated destination when the extensions were busy.
Failed	The total number of calls that were failed to be made by the extensions.
Voicemail	The total number of voicemails that the extensions received.
Total Ring Duration	The time between the call started and the call answered.
Total Talk Duration	The time between the call answered and the call ended.

Report example

The following report shows daily inbound call statistics of all the extensions in group Default_All_Extensions on September, 2020.

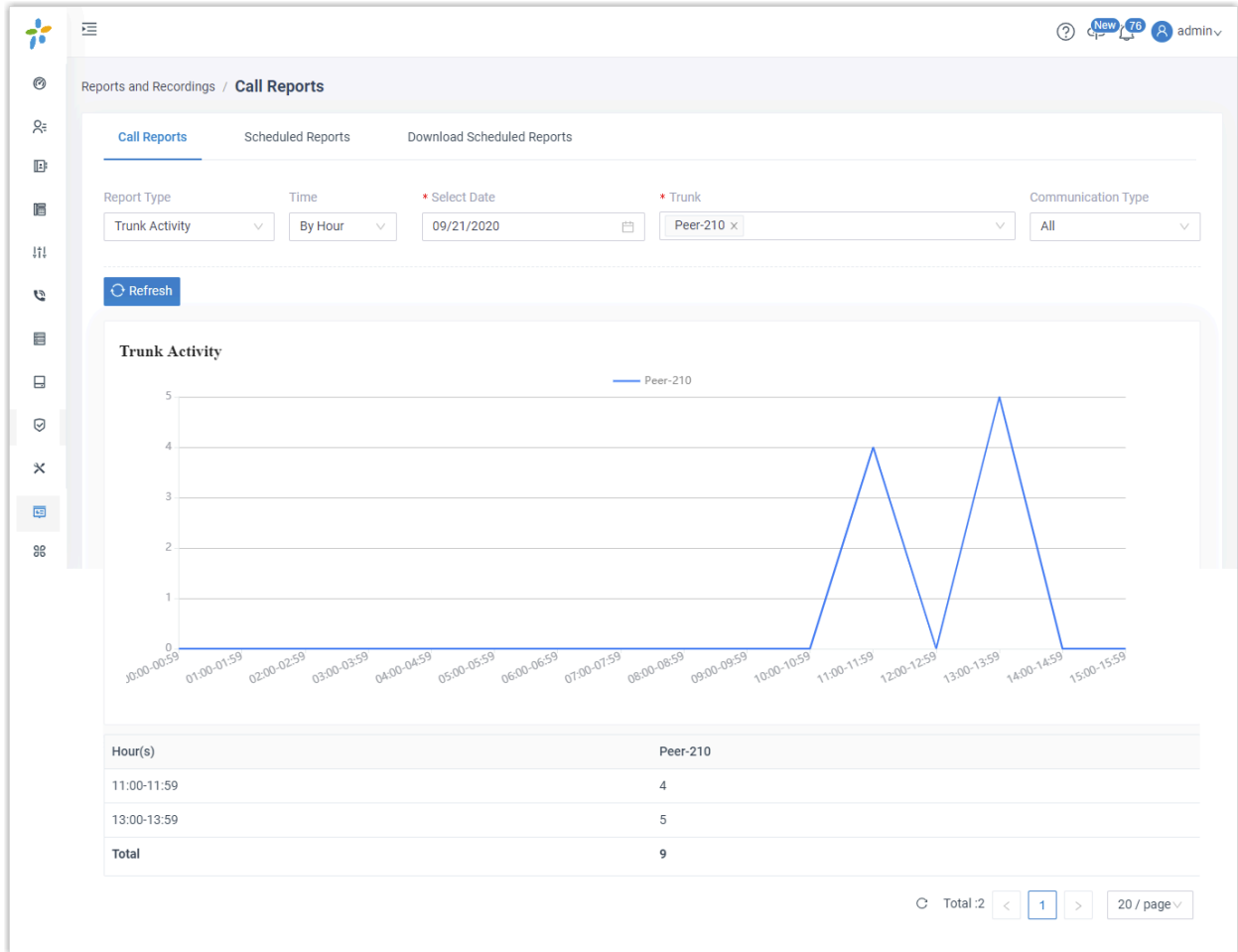


Trunk Activity Report

Trunk Activity Report is a summary report displayed in line graph, which makes it possible for you to query how many inbound and outbound calls have been received or made via a specific trunk. The report allows you to track changes of trunk activity by hour, by date, or by month.

Report example

The following report shows daily inbound & outbound call statistics of all the extensions in group Default_All_Extensions on September, 2020.

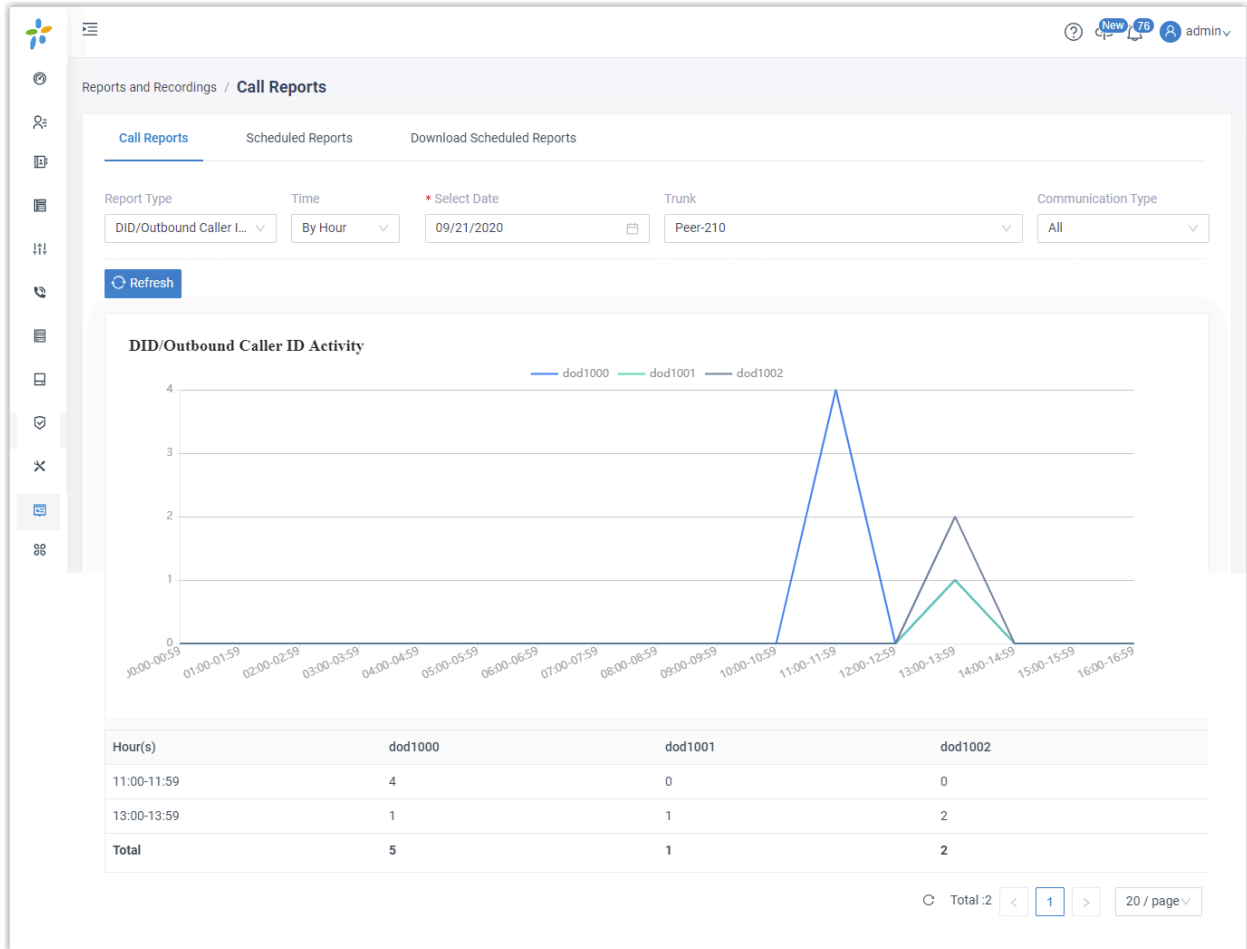


DID/Outbound Caller ID Activity Report

DID/Outbound Caller ID Activity Report is a summary report displayed in line graph, which allows you to track changes of DID/Outbound Caller ID activity by hour, by date, or by month.

Report example

The following report shows hourly call statistics of all the extensions in group Default_All_Extensions on September 21, 2020.



Ring Group Statistics Report

Ring Group Statistics Report is a summary report based on Yeastar Enterprise Plan or Ultimate Plan, which allows you to query the number of received and answered calls for a specific ring group, thus helping you evaluate performance of members within the ring group.

Prerequisites

Ring Group Statistics Report is only available for Yeastar P-Series Enterprise Plan and Ultimate Plan.

Report details

The following table lists the related parameters for Ring Group Statistics report.

Parameter	Description
Answered	The total number of calls that were answered.
Received	The total number of calls that were received.

Parameter	Description
Answered Rate	The answered rate for the ring group or for each group member.

Report example

The following report shows call statistics of ring group 6300 and 6301 during 09/21/2020 00:00:00-09/21/2020 23:59:59.

Ring Group	Answered	Received	Answered Rate
6300<6300>	4	5	80%
Becky<1000>	1		20%
Caroline<1001>	1		20%
Anderson<6666>	2		40%
6301<6301>	2	2	100%
Becky<1000>	1		50%
Anderson<6666>	1		50%
Total	6	7	86%

Scheduled Reports

Schedule Call Reports

This topic describes how to schedule a call report to be sent to a recipient's mailbox at the specified time.

Background information

A scheduled call report is a diagram containing call statistics for the selected objects within a specific time frame. It automatically runs at a pre-defined frequency and is emailed to a specific address as a link and can be downloaded in CSV, XLS, or PDF.

Prerequisites

- Make sure [email server](#) works.

- [Customize Email Template for Scheduled Reports.](#)

Procedure

1. Log in to PBX management portal, go to Reports and Recordings > Call Reports, click Scheduled Reports tab.
2. Click Add Reports.
3. In the Report Type drop-down list, choose the desired report, and select one or more objects that you want to query.

Note:

Descriptions for specific parameters:

- **Communication Type:** Select a communication type Inbound, Outbound, and Internal. You can use the parameter to filter call statistics in the following reports:
 - Extension Call Statistics
 - Extension Call Activity
 - Trunk Activity
 - DID/Outbound Caller ID Activity
- **Short Abandoned Calls:** Set a time. Calls abandoned within the specified time will not be included in report. You can use the parameter to filter call statistics in the following reports:
 - Queue Performance
 - Agent Missed Call Activity


4. Schedule the report.

- **Time:** Set a time frame that the desired report covers.
- **Report Name:** Enter a name to help you identify it.
- **Email Address:** Enter a recipient's email address.

The report will be sent to the email address at the specified time.

- **Report Frequency:** Set how often to send the report.
 - **Once:** If you choose the option, the system sends the report immediately after you save the setting.

- Daily: If you choose the option, select a time from the drop-down list. The system sends the report at this time of the day.
- Weekly: If you choose the option, choose a day of week and select a time from the drop-down list. The system sends the report at this time of the week.
- Monthly: If you choose the option, choose a day and select a time from the drop-down list. The system sends the report on this day and time of the month.

 **Note:**
If you set the day to 31, but the month only has 29 or 30 days, the system will not send the report.

- Format: Set in which format the report can be downloaded.
 - CSV
 - XLS
 - PDF
5. Click Save.

Result

On Scheduled Reports list, check status of the scheduled call report.

- Finished: The one-off call report was sent to the recipient's email address.
- Scheduled: The call report is scheduled and valid. The system will send the report to the recipient's email address at the specified time.
- Paused: The scheduled call report is on hold because the Call Center Service expired. To renew it, go to Yeastar P-Series Enterprise Plan or Ultimate Plan.

Reports and Recordings / **Call Reports**

Call Reports Scheduled Reports Download Scheduled Reports


[Add Report](#) [Email Template](#)

Name	Status	Scheduled Time	Report Frequency	Operations
Sales	Scheduled	2021/01/15 15:59:12	Weekly	Edit Delete
Support	Finished	2021/01/15 15:59:04	Once	Edit Delete


Manage Scheduled Reports

This topic describes how to edit and delete scheduled reports.

Edit scheduled reports

1. Log in to PBX management portal, go to Reports and Recordings > Call Reports, click Scheduled Reports.
2. Select the desired report, click .
3. Edit the scheduled report according to your needs.
4. Click Save.

Delete scheduled reports

1. Log in to PBX management portal, go to Reports and Recordings > Call Reports, click Scheduled Reports.
2. Select the desired report, click .
3. In the pop-up dialog box, click OK.


Download Scheduled Reports on Web Interface

After the system sends scheduled reports to recipients' mailboxes, the recipients can download reports via attached links and system administrator can view and download reports on PBX management portal. This topic describes how to download scheduled reports on the PBX management portal.

Prerequisites

A scheduled report was sent out.

Procedure

1. Log in to PBX management portal, go to Reports and Recordings > Call Reports, click Download Scheduled Reports tab.
2. Select the desired call report, click .
- The report contains a snapshot of data for the time frame you have selected.
3. At the top-right corner, click Download.

Result

The report is downloaded to your computer in the pre-defined format.

Customize Email Template for Scheduled Reports

This topic describes how to customize email template for scheduled reports.

Background information

By default, Yeastar P-Series PBX System sends scheduled call reports in the pre-defined language and email template.

The language is what you have set in [system email template](#), and the email template contains the following information:

- A download link for call report.
- Soft reminder of the download link.
 - The link is valid for 24 hours.
 - The link can only be accessed over the same local network as the PBX.
- System information, including PBX name, PBX serial number, PBX LAN IP address, and PBX WAN IP address.

Procedure

1. Log in to PBX management portal, go to Reports and Recordings > Call Reports > Scheduled Reports.
2. Click Email Template.
3. Configure template settings.
 - a. In the Template drop-down list, select Custom.
 - b. Edit email subject and content according to your needs.
 - c. Click Save.

Result

The PBX will use the email template to send scheduled reports.

Integration

Speech to Text (STT)

Speech to Text (STT) Overview

Speech to Text, also known as speech recognition, enables transcription of audio messages into texts. Yeastar P-Series PBX System allows you to use a third-party transcription service to implement the audio transcription.

Supported Service Platform

Yeastar P-Series PBX System supports the following third-party transcription service:

- Google Cloud Speech-to-Text API

For more information about the integrations, see [Integrate Yeastar P-Series PBX System with Google Cloud Speech-to-Text Service](#).

Applications

After STT integration is set up on the PBX, the speech recognition can be applied to [Voicemail Transcription](#). Users can receive voicemails in the form of text on different platform:

Linkus Web Client

Users can check the transcribed text for each voicemail on Linkus Web Client.

Note:

Voicemail Transcription is NOT supported on Linkus Mobile Client but will be supported in the future.

Email Client

If [Voicemail to Email](#) feature is enabled, the transcribed text will be displayed in the email content for received voicemails.

Related information

[Enable or Disable Voicemail Transcription](#)

Integrate with Speech to Text (STT) API

Integrate Yeastar P-Series PBX System with Google Cloud Speech-to-Text Service

Before using Voicemail Transcription feature, you need to integrate Yeastar P-Series PBX System with a third-party Speech-to-Text service. This topic introduces how to configure the integration of Google Cloud Speech-to-Text (STT) service with Yeastar P-Series PBX System.


Limitations

Audio length: 1 minute

The integration of Yeastar P-Series PBX System with Google Cloud Speech-to-Text service uses the Synchronous Recognition method for speech recognition, which can process up to 1 minute of speech audio data.

Prerequisites

- You need to create a Google Cloud billing account.
- Make sure the Yeastar P-Series PBX System can access Google services.
 1. Log in to PBX management portal, go to Maintenance > Troubleshooting > IP Ping.
 2. In the Target Host field, enter `www.google.com`.
 3. Click Start.
 4. Check the Result box to see if the packet transmission is normal.

 Note:

If the PBX can not access Google service, go to System > Network > Basic Settings to check and configure the PBX network.

5. Click Stop to stop pinging.

Procedure

1. [Get the API key from Google Cloud Platform](#)
2. [Enable Speech to Text \(STT\) integration on Yeastar P-Series PBX System](#)

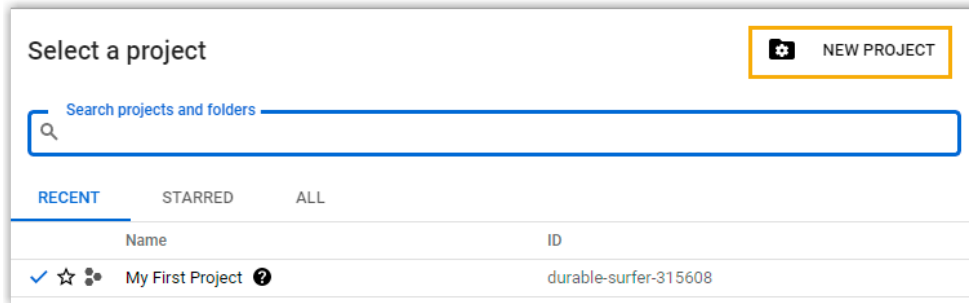
Get the API key from Google Cloud Platform

Step1. Create a project on Google Cloud Platform

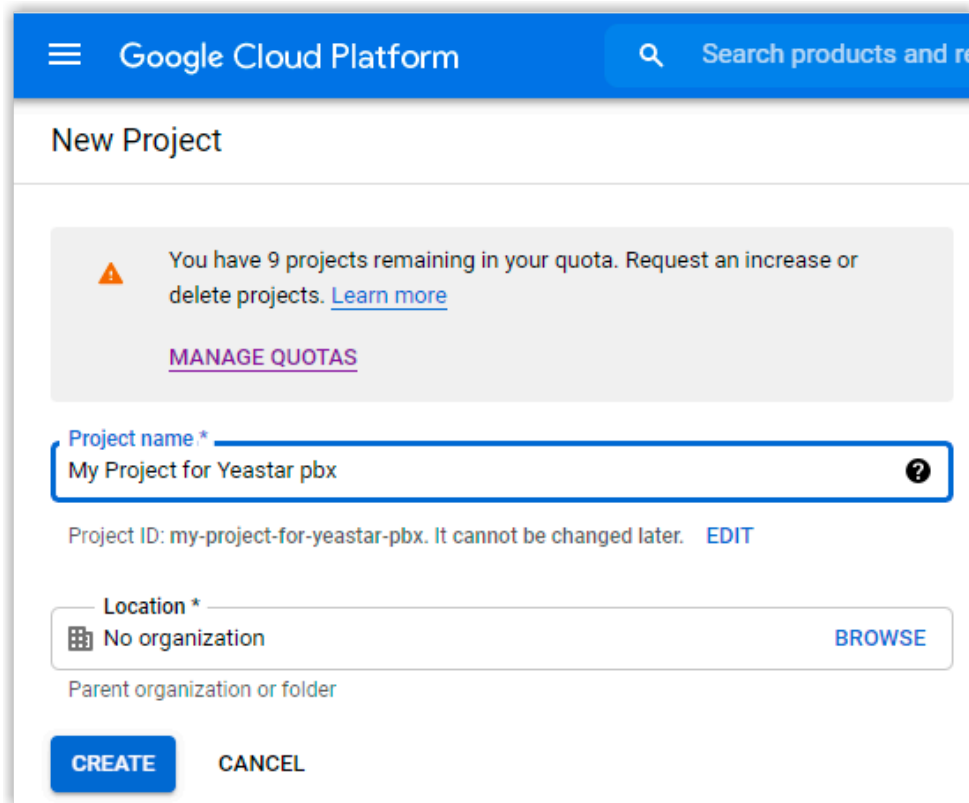
1. Log in to [Google Cloud Platform](#).
2. In the top bar, click My First Project to open the project list.



3. On the Select a project page, click NEW PROJECT in the top-right corner.




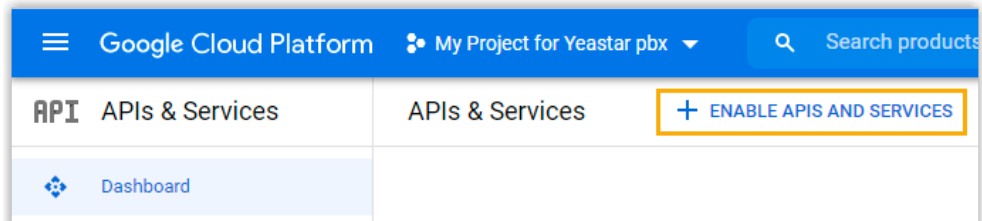
4. On the New Project page, set a project name, and click CREATE.



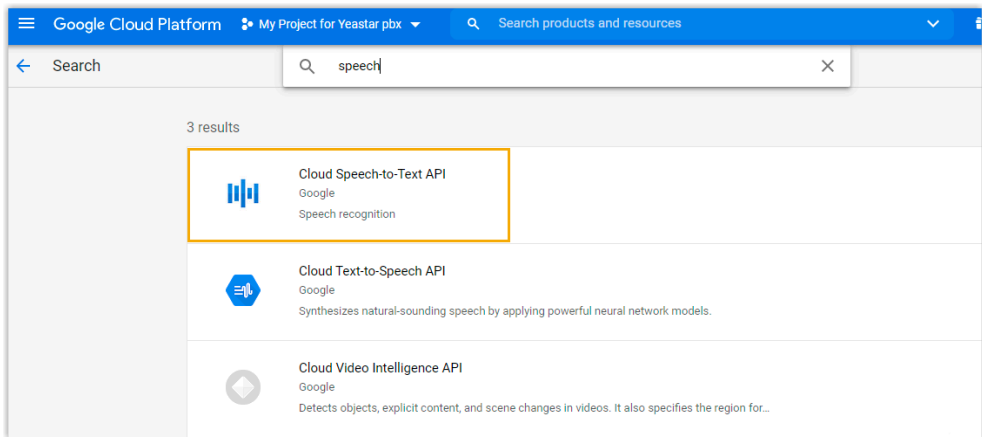
A new project is created, you can select the new project in the project list.

Step2. Enable Speech-to-Text API service on Google Cloud Platform

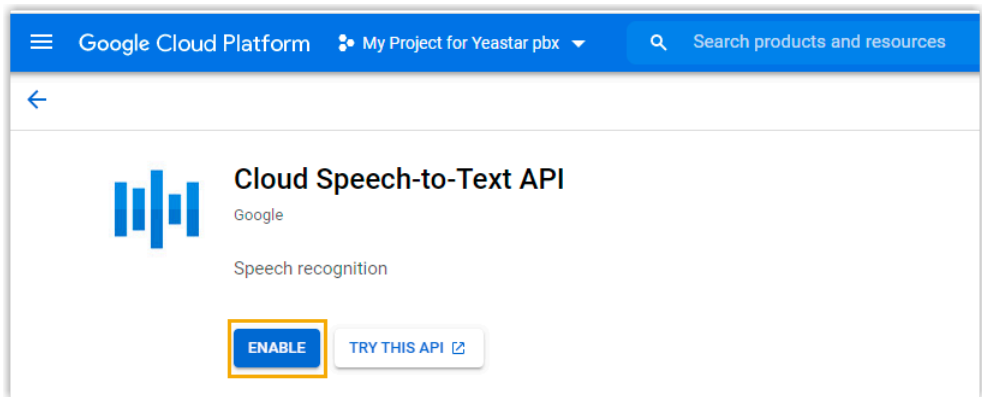
1. In the top-left conner, click  to open the navigation menu, and go to API & Services > Dashboard.
2. Click ENABLE APIS AND SERVICES.



3. In the API Library, enter `speech` in the search box and select Cloud Speech-to-Text API.



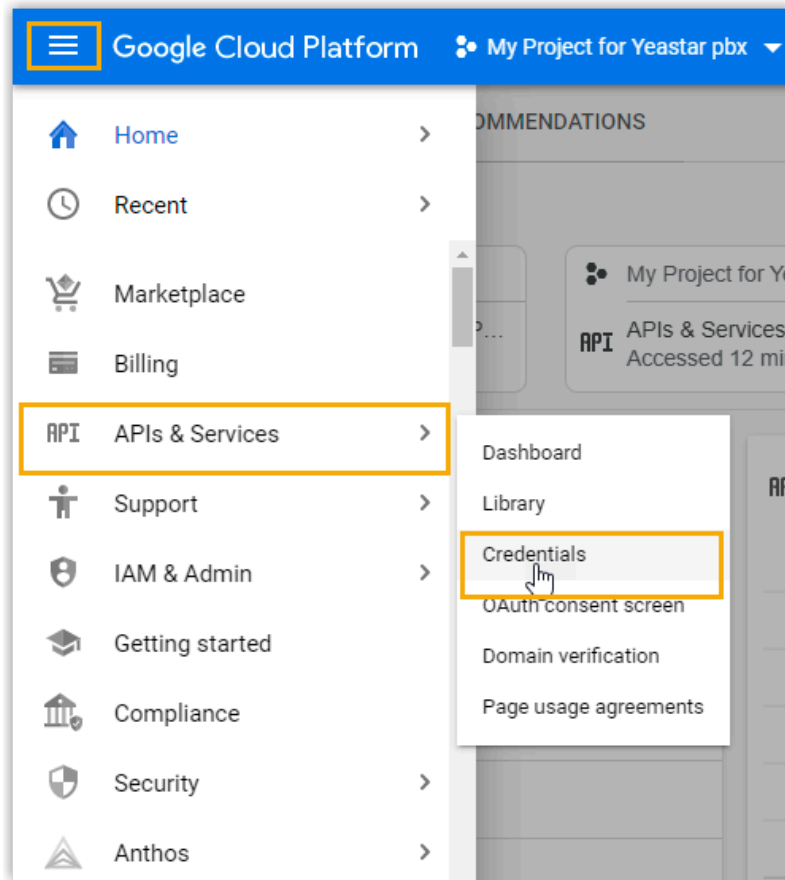
4. Click ENABLE button for the Cloud Speech-to-Text API.



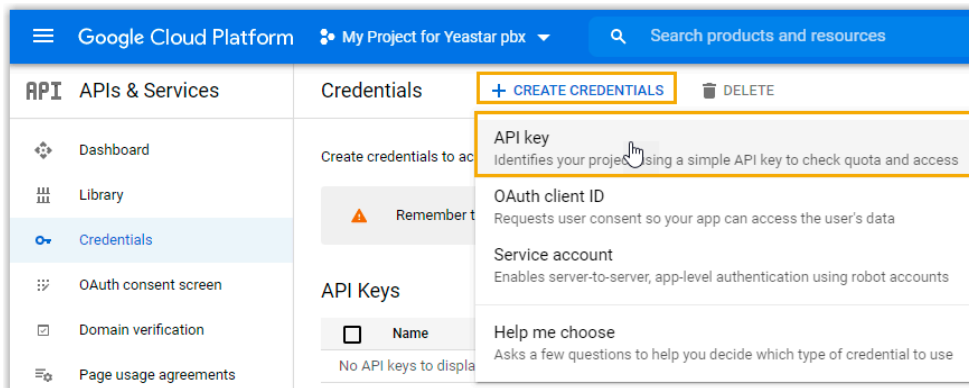
The Speech-to-Text service is enabled.

Step3. Create API credentials on Google Cloud Platform

1. In the left navigation panel, go to API & Services > Credentials.

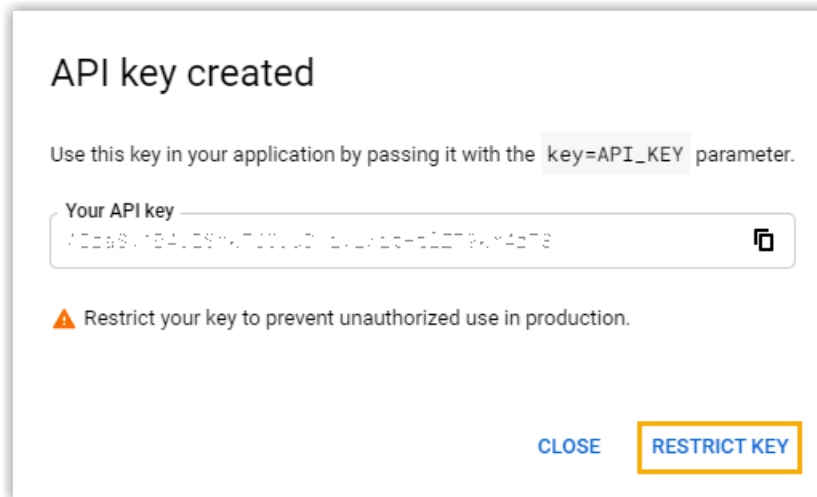


2. Click CREATE CREDENTIALS and select API key.

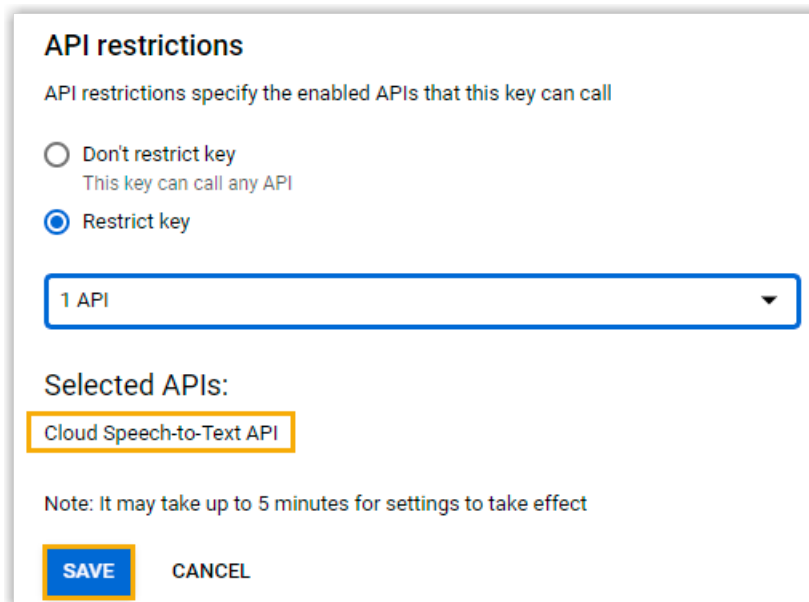


3. In the pop-up window, click RESTRICT KEY.


! Important:
For security purpose, you need to restrict your API key, ensuring only authorized requests are made with your API key.




4. On the Restrict and rename API key page, complete the following configurations.
 - a. In the Name field, specify the API key name.
 - b. In the Application restrictions section, select None.
 - c. In the API restrictions section, select Restrict key.
 - d. Enter `speech` in the search box below to search and select the Cloud Speech-to-Text API, then click OK.
 - e. Click Save to apply your configuration.



The API key is only allowed to call the Cloud Speech-to-Text API.

5. Go back to the Credentials page, in the API key section, click  to copy the restricted API key.

<input type="checkbox"/>	Name	Creation date ↓	Restrictions	Key
<input checked="" type="checkbox"/>	API key for Yeastar test	Jun 22, 2021	Cloud Speech-to-Text API	AIzaSyByav...957ju7ytVY 


Enable Speech to Text (STT) integration on Yeastar P-Series PBX System

1. Log in to PBX management portal, go to Integrations > Speech to Text.
2. In STT API Integration section, fill in the required API credentials.
 - Service: Select Google Cloud.
 - API Key: Paste the restricted API key copied in the former procedure.


STT API Integration

Status: ● Disabled

Service: Google Cloud

* API Key: 

3. In Settings section, select the transcription language.
The audio messages will be transcribed to text in the selected language.


 **Note:**
If the language of voicemail is different with the selected language, the transcribed text will be inaccurate.

4. Click Save.
If the integration succeeds, the Status in the STT API Integration section will display Connected.

STT API Integration [Disconnect](#)

Status: ● Connected

Service: Google Cloud

* API Key: 

What to do next

After the STT API integration succeeds, go to Call Features > Voicemail > Voicemail Settings to enable the Voicemail Transcription feature. For more information, see [Enable or Disable Voicemail Transcription](#).

Related information

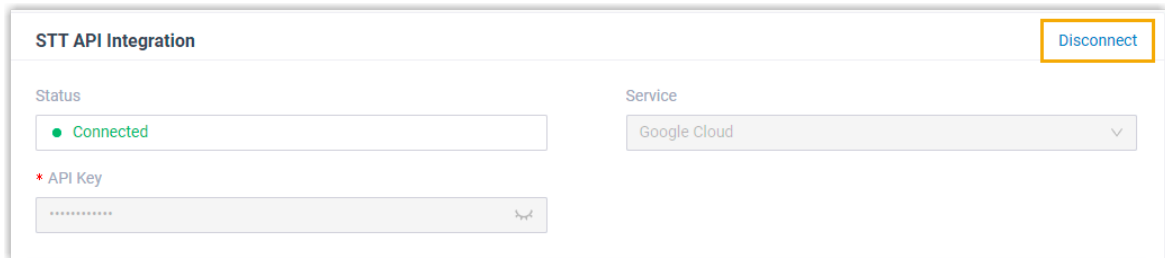
- [Speech to Text \(STT\) Overview](#)
- [Disconnect Speech to Text \(STT\) API Integration](#)

Disconnect Speech to Text (STT) API Integration

After the STT API integration is connected, you can directly disconnect the API service on PBX if you don't need the Speech to Text feature any more, or want to pause the API service.

Procedure

1. Log in to PBX management portal, go to Integrations > Speech to Text.
2. In the STT API Integration section, click Disconnect in the top-right corner.



3. In the pop-up dialog, click Confirm to disconnect the API service.

The API integration is disconnected, and the Status displays Disabled.

Result

The [Voicemail Transcription](#) feature is unavailable.

Asterisk Manager Interface (AMI) Overview

The Asterisk Manager Interface (AMI) is a system monitoring and management interface provided by Asterisk. Yeastar P-Series PBX System supports AMI that allows you to connect an AMI client to Yeastar P-Series PBX System.

What is Asterisk Manager Interface (AMI)

Asterisk Manager Interface (AMI) is a standard management interface into Asterisk server. It is a client/server model over TCP that allows a client program to connect to an Asterisk server and issue commands or read events over a TCP/IP stream. With the manager interface, you can control the PBX, originate calls, check mailbox status, monitor extensions and so on.

Connect to Yeastar P-Series PBX System via AMI

1. Enable AMI on PBX.
 - a. Log in to PBX management portal, go to Integration > AMI.
 - b. Enable AMI.
 - c. In the AMI section, configure the connection authentication.

- Username: Enter the username that can be used by third party to access the AMI of PBX.
 - Password: Enter the password that can be used by third party to access the AMI of PBX.
 - Port: The default port for AMI interface is 5038, and is not editable.
- d. In the Permitted IP section, set which clients are allowed to access the AMI of PBX.
- i. In the IP Address field, click Add.
 - ii. Enter the IP address or IP section that is allowed to access the AMI of PBX.

The input format should be XXX.XXX.XXX.XXX.

For example: IP address 216.207.245.47 with subnet mask 255.255.255.255 means that only the device with IP address 216.207.245.47 is allowed to access the PBX via AMI.



Note:

You can add up to 4 permitted IP address.

To prevent the permitted IP from being blocked by security rules, the added permitted IP address will be automatically added to the Static Defense list, you can also [delete them from the Static Defense list](#) as your need.

- e. Click Save and Apply.
2. Configure AMI client with the authentication information provided on PBX, and connect client to PBX.

Database Grant

Database Grant Overview

Yeastar P-Series PBX System is based on MySQL database. Database Grant is a feature that allows you to grant permissions for a third-party software to access the PBX database.

Applications

Database Grant is usually applied in the following scenarios:

- Billing System

By accessing the PBX database, you can get CDR and save it to the local database of billing software. Then you can charge calls by CDR.

- Call Center

Get CDR and save it to the local database of call center software.

Limitation

After accessing the PBX database, only cdr data is available to be checked and downloaded, other data cannot be accessed.

Get CDR Data from Database of Yeastar P-Series PBX System

Yeastar P-Series PBX System allows you to access the system database and get CDR data. This topic describes how to get CDR data from the PBX database via Navicat software.

Procedure

1. [Grant access to the PBX database](#)
2. [Access the PBX database via Navicat software](#)

Grant access to the PBX database

1. Log in to PBX management portal, go to Integration > Database Grant.
2. Turn on Database Grant option and configure the authentication information for the third-party software to access the PBX database.

The screenshot shows the 'Database Grant' configuration interface. It includes three input fields:

- * User Name:** A text input field containing the value 'rt3J8xJm'.
- * Password:** A password input field containing the value 'Y229sxd%A0kp0' with a toggle icon on the right.
- * Port:** A text input field containing the value '3306'.

- User Name: Use the randomly generated user name or change the name.
 - Password: Use the randomly generated password or change password.
 - Port: Default port is 3306 and is unchangeable.
3. In the Permitted IP section, configure which IP addresses are allowed to access the database.

The screenshot shows the 'IP Address' configuration table with the following structure:


* IP Address	* Subnet Mask	Operations
192.168.66.0	255.255.255.0	

 Below the table is a '+ Add' button.

- a. Click Add.

- b. Enter the permitted IP address and subnet mask.

In this example, enter IP address 192.168.66.0 and subnet mask 255.255.255.0 to allow all IP addresses in the segment 192.168.66.X to access the database.

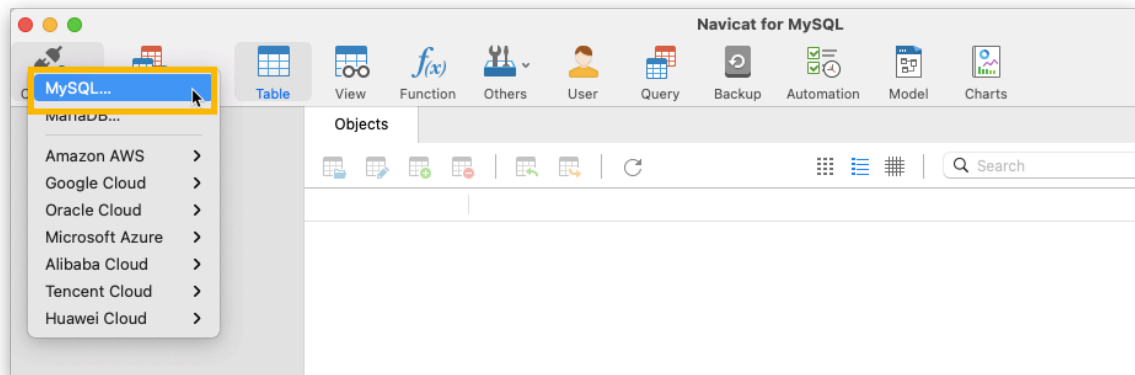
 Note:

Restricted from MySQL database, only the two subnet masks are allowed to be filled in: 255.255.255.255 and 255.255.255.0.

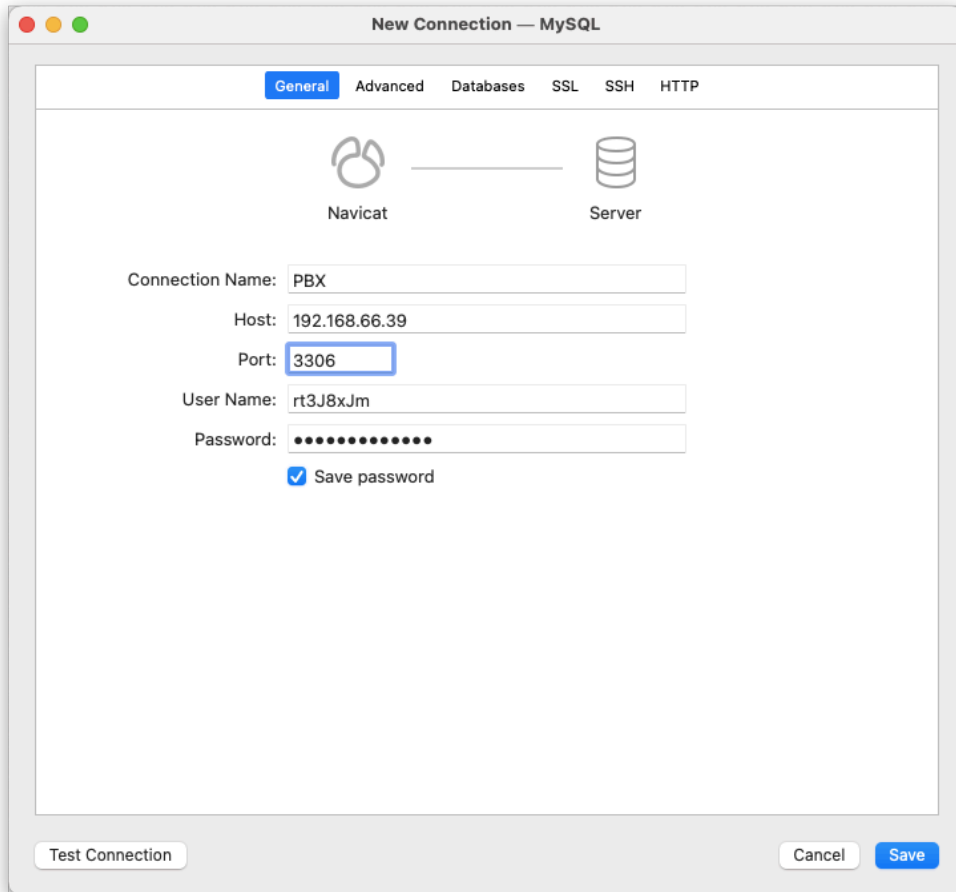
4. Click Save and Apply.

Access the PBX database via Navicat software

1. Launch [Navicat for MySQL](#) on the PC that has IP address being in the segment 192.168.66.X.
2. On the Navicat for MySQL, click Connection and select MySQL.

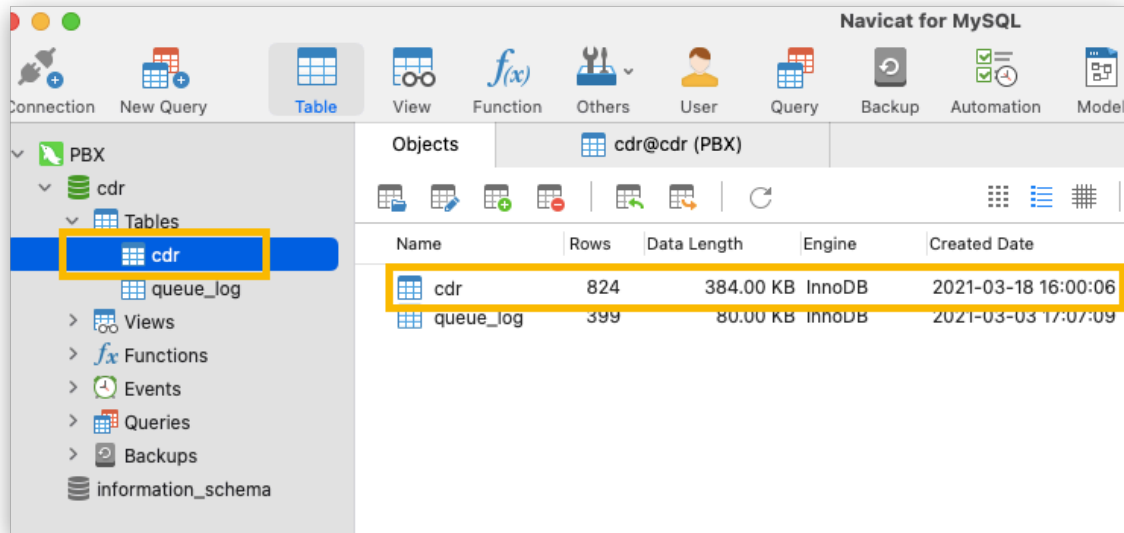


3. In the pop-up window, enter the following information:



- Connection Name: Enter a connection name to help you identify it.
 - Host: Enter the IP address of PBX.
 - Port: Enter 3306.
 - User Name: Enter the user name that is configured on the PBX. In this example, enter `rt3J8xJm`.
 - Password: Enter the password that is configured on the PBX. In this example, enter `Y229sxd%A0kpO`.
4. Click Save.
 5. To check CDR data, double click the new connection, and select cdr table.

For more information about the cdr table, see [cdr Table in the PBX Database](#).



cdr Table in the PBX Database

This topic describes details of cdr table stored in the database of Yeastar P-Series PBX System.

Field	Descriptions
id	System internal flag
datetime	Date and time
timestamp	System internal flag
uid	System internal flag
clid	System internal flag
src	Caller's number
srcname	Caller's name
srcaddr	System internal flag
dst	Callee's number
dstname	Callee's name
dcontext	System internal flag
channel	System internal flag
dstchannel	System internal flag
srctrunk	Source trunk

Field	Descriptions
dsttrunk	Destination trunk
lastapp	System internal flag
lastdata	System internal flag
duration	Total duration of the call (calculates from the beginning of the call)
ringduration	Ring duration of the call
talkduration	Talk duration of the call (calculates after the call is answered)
disposition	Call status: <ul style="list-style-type: none"> • NO ANSWER • FAILED • BUSY • ANSWERED • VOICEMAIL • CONGESTION
amaflags	System internal flag
calltype	Communication Type <ul style="list-style-type: none"> • Internal • Inbound • Outbound • Callback
accountcode	System internal flag
uniqueid	System internal flag
didnumber	DID number
dodnumber	DOD number
recordfile	Recording file name
recordpath	Recordings path (with file name)
srcchanurl	Caller's SIP URI
dstchanurl	Callee's SIP URI
reasonpartya	System internal flag
reasonpartyb	System internal flag

Field	Descriptions
reasonpartyc	System internal flag
reasonpartyd	System internal flag
reasonpartye	System internal flag
reasonpartyf	System internal flag
displayonweb	System internal flag
src_del_cdr	System internal flag
dst_del_cdr	System internal flag
src_del_recording	System internal flag
dst_del_recording	System internal flag
srcnameprefix	System internal flag
dstnameprefix	System internal flag
misscall_isread	System internal flag
in2outbound	System internal flag
concurrentcalls	System internal flag
videocall	System internal flag
rascall	System internal flag
tryvideocall	System internal flag

Refereneces

Import and Export Parameters Overview

Check the required parameters, optional parameters, and restrictions in the import and export files.


Background information

CSV (comma-separated values) files can expedite the bulk creation of various settings. A CSV file is a plain text file that stores tabular data from database-style tools, such as Excel.

Yeastar P-Series PBX System allows you to export data as a CSV file, specify data in the CSV file, and import the file to PBX to modify settings in bulk, such as creating extensions in bulk using CSV file.

Which features support importing and exporting data

Yeastar P-Series PBX System supports importing and exporting data of the following modules:




 Note:




The supported parameters are different depending on firmware version.





- [Extension Parameters](#)
- [Contacts Parameters](#)
- [Speed Dial Number Parameters](#)
- [Emergency Number Parameters](#)
- [Trunk Parameters](#)
- [Trunk DID/DDIs Parameters](#)
- [Trunk Outbound Caller ID Parameters](#)
- ['Inbound Caller ID Reformatting Rule' Parameters](#)
- [Inbound Route Parameters](#)
- [Outbound Route Parameters](#)
- [Static Defense Rule Parameters](#)
- [Auto Defense Rule Parameters](#)
- ['Outbound Call Frequency Restriction Rule' Parameters](#)




Extension Parameters





Descriptions for parameters in exported and imported Extension CSV file.





Parameter	Description	Importance	Restriction	Default Value
First Name	The first name of extension user.	At least one is required	The maximum character length is 63.	Extension number
Last name	The last name of extension user.		 Note: First Name will be filled with a value of Extension Number if you leave these fields empty.	N/A
Email Address	The email address of extension user.	Optional	Only numbers, letters, and characters @ _ - . are allowed. Must start with a number, letter, or character _ and follow the email address format XXX@XXX.XX. Extension's email address cannot be duplicated. The maximum character length is 255.	N/A
Mobile Number	The mobile number of extension user.	Optional	Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.	N/A
User Password	The password for extension user to log in to Linkus client and PBX management portal.	Required	Must contain numbers, uppercase, and lowercase letters. The minimum character length is 10 and the maximum is 63.  Note: User Password will be generated randomly if you leave this field empty.	Generate Randomly
User Role	The role for extension user with PBX management permission.	Required	Permitted value: 0 or one of the role names defined in the PBX. 0 means [None].  Note: User Role will be filled with default value 0 if you leave this field empty.	0




Parameter	Description	Importance	Restriction	Default Value
Extension Number	The extension's number.	Required	Extension Number cannot be duplicated, and only numbers are allowed. The maximum character length is 7.	N/A
Caller ID	The caller ID that is displayed on the callee's device.	Required	Numbers, letters, and special characters () . - + * # are allowed. The maximum character length is 31.  Note: Caller ID will be filled with default value Extension Number if you leave this field empty.	Extension Number
Registration Name	The registration name that is used to validate extension registration.	Required	The maximum character length is 63.  Note: Registration Name will be generated randomly if you leave this field empty.	Generate Randomly
Registration Password	The password for the user to register the SIP extension.	Required	The minimum character length is 8 and the maximum is 63.  Note: Registration Password will be generated randomly if you leave this field empty.	Generate Randomly
IP Phone Concurrent Registrations	How many SIP phones are allowed to register with the extension.	Required	Permitted value: <ul style="list-style-type: none"> • 1: Allow one phone to register with the extension. • 2: Allow two phones to register with the extension. • 3: Allow three phones to register with the extension. 	1





Parameter	Description	Importance	Restriction	Default Value
			 Note: IP Phone Concurrent Registrations will be filled with default value if you leave this field empty.	
Emergency Outbound Caller ID	The outbound Caller ID for the extension when it makes emergency calls.	Optional	Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.	N/A
Enable Voicemail	Whether to enable or disable voicemail feature.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable  Note: Enable Voicemail will be filled with default value if you leave this field empty.	1
Voicemail PIN Authentication	Whether to enable or disable voicemail PIN authentication.	Required if Enable Voicemail = 1	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable  Note: Voicemail PIN Authentication will be filled with default value if you leave this field empty.	1
Voicemail Access PIN	The PIN for authentication when accessing voicemail box.	Required if Enable Voicemail = 1 & Voicemail PIN Authentication = 1	Only numbers are allowed. The minimum character length is 3 and the maximum is 15.  Note: Voicemail Access PIN will be generated randomly if you leave this field empty.	Generate Randomly






Parameter	Description	Importance	Restriction	Default Value
New Voice-mail Notification	The notification type for new voicemail	Required if Enable Voicemail = 1	Permitted value: <ul style="list-style-type: none"> no: No Email Notifications with_attach: Send Email Notifications with Attachment without_attach: Send Email Notifications without Attachment <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  Note: New Voicemail Notification will be filled with default value if you leave this field or Email Address empty. </div>	no
After Notification	The way to handle voice-mail message in mailbox after receiving the message notification via email.	Required if Enable Voicemail = 1 & New Voice-mail Notification = with_attach	Permitted value: <ul style="list-style-type: none"> no: Do Nothing mark_read: Mark as read delete: Delete Voicemail <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  Note: After Notification will be filled with default value no if you leave these fields empty. </div>	no
		Required if Enable Voicemail = 1 & New Voice-mail Notification = without_attach	Permitted value: <ul style="list-style-type: none"> no: Do Nothing mark_read: Mark as read <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  Note: After Notification will be filled with default value no if you leave these fields empty. </div>	no
Play Date and Time	Whether to announce arrival time of the	Required if Enable	Permitted value: <ul style="list-style-type: none"> 0: Disable 	0




Parameter	Description	Importance	Restriction	Default Value
	message before playing the voicemail message.	Voicemail = 1	<ul style="list-style-type: none"> • 1: Enable <div style="border: 1px solid #00aaff; padding: 5px; margin-top: 10px;"> <p> Note: Play Date and Time will be filled with default value if you leave this field empty.</p> </div>	
Play Caller ID	Whether to announce caller ID of the party that left the message before playing the voicemail message.	Required if Enable Voicemail = 1	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable <div style="border: 1px solid #00aaff; padding: 5px; margin-top: 10px;"> <p> Note: Play Caller ID will be filled with default value if you leave this field empty.</p> </div>	0
Play Message Duration	The duration of the message (in minutes) will be announced before playing the voicemail message.	Required if Enable Voicemail = 1	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable <div style="border: 1px solid #00aaff; padding: 5px; margin-top: 10px;"> <p> Note: Play Message Duration will be filled with default value if you leave this field empty.</p> </div>	0
Send email notification when the User Password is changed	Whether to send email notification when the User Password is changed.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable <div style="border: 1px solid #00aaff; padding: 5px; margin-top: 10px;"> <p> Note: Send email notification when the User Password is changed will be filled with default value if you leave this field empty.</p> </div>	1
Send email notifications on	Whether to send email notifications on missed calls.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable 	0




Parameter	Description	Importance	Restriction	Default Value
missed calls			 Note: Send email notifications on missed calls will be filled with default value if you leave this field empty.	
Allow the extension to view recordings	Whether to allow users to view and manage their own recordings.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable  Note: Allow the extension to view recordings will be filled with default value if you leave this field empty.	1
Allow users to start and stop recording	Whether to allow users to start and stop recording.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable  Note: Allow users to start and stop recording will be filled with default value if you leave this field empty.	1
All Busy Mode for Endpoints	Whether to forward a new incoming call to the Busy destination when one of the endpoints with extension registered is busy in a call.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable  Note: All Busy Mode for Endpoints will be filled with default value if you leave this field empty.	0
Call Popup URL	Whether to automatically open a custom URL (web	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable 	0

Parameter	Description	Importance	Restriction	Default Value
	page) upon receiving an incoming call.		 Note: Call Popup URL will be filled with default value if you leave this field empty.	
Popup URL	The address of third-party URL, followed by the variables that you want to pass.	Required if Call Popup URL = 1	The maximum character length is 255.	http://example.com/somepage.php?number={{.Caller-Number}}&name={{.Caller-Display-Name}}
Communication type	The types of calls that will trigger the call popup.	Required if Call Popup URL = 1	Permitted value: Internal and Inbound. <ul style="list-style-type: none"> • For multiple types, enter values in order and use & as a separator, e.g. Internal & Inbound. • If the value you enter is not permitted, it will be skipped. 	Inbound
Trigger Event	When the call popup will be automatically triggered.	Required if Call Popup URL = 1	Permitted value: Ringing, Answered, and Call End.  Note: Trigger Event will be filled with default value Ringing if you leave the field empty.	Ringing
DTMF Mode	The mode for sending DTMF tones.	Required	Permitted value: rfc4733, info, inband or auto.  Note: DTMF Mode will be filled with default value rfc4733 if you leave this field empty.	rfc4733

Parameter	Description	Importance	Restriction	Default Value
Transport	The protocol for transport.	Required	Permitted value: udp, tcp, or tls. <div style="border: 1px solid #00a0e3; padding: 5px; background-color: #e6f2ff;">  Note: Transport will be filled with default value udp if you leave these fields empty. </div>	udp
Qualify	Whether to send the SIP OPTIONS packet periodically to the SIP device to check if the device is online.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable <div style="border: 1px solid #00a0e3; padding: 5px; background-color: #e6f2ff;">  Note: Qualify will be filled with default value if you leave this field empty. </div>	1
T.38 Support	Whether to support T.38 fax for this extension.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable <div style="border: 1px solid #00a0e3; padding: 5px; background-color: #e6f2ff;">  Note: T.38 Support will be filled with default value if you leave this field empty. </div>	0
NAT	Whether to enable NAT for this extension.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable <div style="border: 1px solid #00a0e3; padding: 5px; background-color: #e6f2ff;">  Note: NAT will be filled with default value if you leave this field empty. </div>	1
SRTP	Whether to encrypt RTP packets.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable 	0

Parameter	Description	Importance	Restriction	Default Value
			 Note: SRTP will be filled with default value if you leave this field empty.	
Allow Remote Registration	Whether to allow user to register a remote SIP extension to PBX.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable  Note: Allow Remote Registration will be filled with default value if you leave this field empty.	0
Disable Outbound Calls	Whether to restrict the user from making outbound calls.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable  Note: Disable Outbound Calls will be filled with default value if you leave this field empty.	0
Disable Outbound Calls outside Business Hours	Whether to restrict the user from making outbound calls outside business hours.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable  Note: Disable Outbound Calls outside Business Hours will be filled with default value if you leave this field empty.	0
Disallow International Calls	Whether to restrict the user from making international calls.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable  Note:	1

Parameter	Description	Importance	Restriction	Default Value
			<p>Disable International Calls will be filled with default value if you leave this field empty.</p>	
Outbound Route Permission	Specify the outbound routes that this extension is allowed to use.	Optional	<p>Permitted value: one or more outbound route names existed in PBX.</p> <div data-bbox="797 562 1230 1031" style="border: 1px solid #add8e6; padding: 5px;"> <p> Note:</p> <ul style="list-style-type: none"> • If the outbound route name you enter does not exist in PBX, it will be skipped. • For multiple outbound routes, please enter outbound route names and use & as a separator, e.g. name1&name2. </div>	N/A
Max Outbound Call Duration (s)	The maximum call duration in seconds for making outbound calls from this extension.	Required	<p>Only numbers are allowed. Specially, -1 means follow system and 0 means unlimited. The maximum character length is 7.</p> <div data-bbox="797 1293 1230 1497" style="border: 1px solid #add8e6; padding: 5px;"> <p> Note:</p> <p>Max Outbound Call Duration (s) will be filled with default value follow_system if you leave these fields empty.</p> </div>	-1
Outbound Call Frequency Restriction	The restriction rule(s) that used to limit the extension outbound call frequency within specified time period.	Optional	<p>Permitted value: One or more Outbound Call Frequency Restriction names existed in PBX.</p> <div data-bbox="797 1654 1230 1858" style="border: 1px solid #add8e6; padding: 5px;"> <p> Note:</p> <ul style="list-style-type: none"> • Use & to separate multiple names, e.g. name1&name2. </div>	Default_Ext_Outbound Call Frequency

Parameter	Description	Importance	Restriction	Default Value
			<ul style="list-style-type: none"> • If you leave this field empty, it will be filled with default value. • If the names you entered are not existing in PBX, it will be skipped. 	
Linkus Mobile Client	Whether to allow the extension user to log in to Linkus Mobile Client.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  Note: Linkus Mobile Client will be filled with default value if you leave this field empty. </div>	1
Linkus Desktop Client	Whether to allow the extension user to log in to Linkus Desktop Client.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  Note: Linkus Desktop Client will be filled with default value if you leave this field empty. </div>	1
Linkus Web Client	Whether to allow the extension user to log in to Linkus Web Client.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;">  Note: Linkus Web Client will be filled with default value if you leave this field empty. </div>	1


Related information

[Export and Import SIP Extensions](#)

Contacts Parameters

Descriptions for parameters in exported and imported Company Contacts CSV file and Personal Contacts CSV file.

Parameter	Importance	Restriction
First Name	At least one is required	The maximum character length is 127 (63 for first name and 63 for last name).
Last Name		
Company Name	Optional	The maximum character length is 127.
Email	Optional	Only numbers, letters, and characters @ _ - . are allowed. Must start with a number, letter, or character _ and follow the email address format XXX@XXX.XX. The maximum character length is 255.
Business Number	At least one is required	Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.
Business Number 2		Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.
Business Fax		Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.
Mobile		Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.
Mobile 2		Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.
Home		Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.
Home 2		Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.
Home Fax		Numbers, letters, and characters () . - + * # are allowed.

Parameter	Importance	Restriction
		The maximum character length is 31.
Other		Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.
ZIP Code	Optional	The maximum character length is 255.
Street	Optional	The maximum character length is 255.
City	Optional	The maximum character length is 255.
State	Optional	The maximum character length is 255.
Country	Optional	The maximum character length is 255.
Remark	Optional	The maximum character length is 1024.
Phonebook	Optional	<p>Permitted value: One or more phonebook names existed in PBX. For multiple phonebooks, enter the names and use & as a separator, e.g. phonebook_name1&phonebook_name2.</p> <div style="border: 1px solid #00a0e3; padding: 10px; margin-top: 10px;"> <p> Note:</p> <ul style="list-style-type: none"> The feature is available for Enterprise/Ultimate Plan. Phonebook will be filled with default value Default_All_Contacts if you leave these fields empty. System will create new phonebook(s) if you fill in a name that doesn't exist. </div>

Related information

[Export and Import Company Contacts](#)

[Linkus Web Client Guide - Export personal contacts](#)

[Linkus Web Client Guide - Import personal contacts](#)

Speed Dial Number Parameters

Descriptions for parameters in exported and imported Speed Dial Number CSV file.


Parameter	Importance	Restriction
Speed Dial Number	Required	The maximum character length is 4. Only numbers and characters * # are allowed. Speed dial number cannot be duplicated.
Phone Number	Required	The maximum character length is 31. Numbers, letters, and characters () . - + * # are allowed.

Related information

[Export and Import Speed Dial Numbers](#)

Emergency Number Parameters

Descriptions for parameters in exported and imported Emergency Number CSV file.

Parameter	Importance	Restriction	Default Value
Name	Required	The maximum character length is 63. Characters ; " , \ are not allowed. Emergency number's name cannot be duplicated.	N/A
Emergency Number	Required	The maximum character length is 31. Numbers, letters, and characters () . - + * # are allowed. Emergency number cannot be duplicated.	N/A
Emergency Outbound Caller ID Priority	Required	Permitted value: <ul style="list-style-type: none"> • emergency_first: Trunk's Emergency Outbound Caller • IDext_first: Extension's Emergency Outbound Caller ID <div style="border: 1px solid #00aaff; padding: 5px; margin-top: 10px;"> <p> Note: Emergency Outbound Caller ID Priority will be filled with default value if you leave this field empty.</p> </div>	emergency_first

Parameter	Importance	Restriction	Default Value
Trunk	Required	Permitted value: one of trunks' name existed in PBX.	N/A
Trunk's Emergency Outbound Caller ID	Optional	The maximum character length is 31. Numbers, letters, and characters () . - + * # are allowed.	N/A

Related information

[Export and Import Emergency Numbers](#)

Trunk Parameters




Descriptions for parameters in exported and imported Trunk CSV file.












Note:






Only SIP Peer Trunk and Register Trunks can be exported and imported.






Parameter	Description	Importance	Restriction
Name	The trunk name.	Required	The maximum character length is 31. Space and special characters are not allowed. Trunk's name cannot be duplicated.
Trunk Status	Whether to enable or disable the trunk.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable <div data-bbox="1234 1407 1624 1533" style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> Note: Trunk Status will be filled with 0 if empty.</p> </div>
Trunk Type	Trunk type.	Required	Permitted value: <ul style="list-style-type: none"> • peer • register <div data-bbox="1234 1743 1624 1869" style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p> Note: • Importing Account Trunk</p> </div>






Parameter	Description	Importance	
			<ul style="list-style-type: none"> • Trunk Typewill be filled field empty.
Transport	The transport protocol that is provided by the ITSP.	Required	Permitted value: udp, tcp, tls  Note: Transport will be filled with fields empty.
Hostname/IP	The IP address or the domain of the ITSP.	Required	The maximum character len
Port	The trunk port.	Required	Only numbers between 0 and
Domain	The domain in SIP URI of a specific header like From, To header.  Note: If the domain is not provided by ITSP, enter the same value as Hostname/IP.	Required	The maximum character len
Username	The username to register to the ITSP.	Required if Trunk Type = register	The maximum character len
Password	The password that is associated with the username.	Required if Trunk Type = register	The maximum character len
Authentication Name	The authentication name to register to the ITSP.	Optional	The maximum character len
Enable Outbound Proxy	Whether to enable or disable outbound proxy.	Required if Trunk Type = register	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable  Note: Enable Outbound Proxy will leave this field empty.
Outbound Proxy Server	The address of outbound proxy server.	Required if Enable Outbound Proxy = 1	The maximum character len





Parameter	Description	Importance	
Port of Outbound Proxy Server	The port of outbound proxy server.	Required if Enable Outbound Proxy = 1	Only numbers between 1 and 65535.
Codec Setting	The audio codec for trunk.	Required	<p>Permitted value: ulaw, alaw, g722, g726, speex, adpcm, vbr, vbr1, vbr2, vbr3, vbr4, vbr5, vbr6, vbr7, vbr8, vbr9, vbr10, vbr11, vbr12, vbr13, vbr14, vbr15, vbr16, vbr17, vbr18, vbr19, vbr20, vbr21, vbr22, vbr23, vbr24, vbr25, vbr26, vbr27, vbr28, vbr29, vbr30, vbr31, vbr32, vbr33, vbr34, vbr35, vbr36, vbr37, vbr38, vbr39, vbr40, vbr41, vbr42, vbr43, vbr44, vbr45, vbr46, vbr47, vbr48, vbr49, vbr50, vbr51, vbr52, vbr53, vbr54, vbr55, vbr56, vbr57, vbr58, vbr59, vbr60, vbr61, vbr62, vbr63, vbr64, vbr65, vbr66, vbr67, vbr68, vbr69, vbr70, vbr71, vbr72, vbr73, vbr74, vbr75, vbr76, vbr77, vbr78, vbr79, vbr80, vbr81, vbr82, vbr83, vbr84, vbr85, vbr86, vbr87, vbr88, vbr89, vbr90, vbr91, vbr92, vbr93, vbr94, vbr95, vbr96, vbr97, vbr98, vbr99, vbr100.</p> <p>For multiple Codec, please use & separator, e.g. first_value1&second_value2.</p> <p> Note: If the value you enter is not permitted, it will be skipped.</p>
DTMF Mode	The default mode for sending DTMF tones.	Required	<p>Permitted value: rfc4733, info, none.</p> <p> Note: DTMF Mode will be filled with rfc4733 if these fields empty.</p>
Qualify	Whether to send SIP OPTION packet to check if the SIP device is up.	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> • 0: Disable • 1: Enable <p> Note: Qualify will be filled with default value if empty.</p>
Enable SRTP	Whether to enable or disable SRTP (encrypted RTP) for the trunk.	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> • 0: Disable • 1: Enable <p> Note: Enable SRTP will be filled with default value if empty.</p>
T.38 Support	Whether to enable or disable T.38 fax.	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> • 0: Disable • 1: Enable <p> Note: T.38 Support will be filled with default value if empty.</p>



Parameter	Description	Importance	
			T.38 Support will be filled with empty.
Inband Progress	Whether to enable or disable inband progress.	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> • 0: Disable • 1: Enable <p> Note: Inband Progress will be filled with empty field empty.</p>
Maximum Concurrent Calls	Specify the maximum number of concurrent calls allowed in the trunk.	Required	<p>Only numbers are allowed. Specially, 0 means unlimited. The maximum character length is 10.</p> <p> Note: Maximum Concurrent Calls must leave this field empty.</p>
Call Restriction Type	Specify based on which type of calls to define to restrict the max concurrent call number for this trunk.	Required	<p>Permitted value: outbound only</p> <p> Note: Call Restriction Type will be filled with empty if this field empty.</p>
Default Outbound Caller ID	The caller ID that is displayed on the callee's device.	Optional	<p>Numbers, letters, and characters. The maximum character length is 20.</p> <p> Note: The outbound caller ID should be filled with empty.</p>
Default Outbound Caller ID Name	The caller ID name that is displayed on the callee's device.	Optional	The maximum character length is 20.
Get Caller ID From	Decide from which header field will the trunk retrieve Caller ID.	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> • follow_system: [Follow System] • from: From • contact: Contact • rpid: Remote-Party-ID • pai: P-Asserted-Identity • ppi: P-Preferred-Identity

Parameter	Description	Importance	F
			<p> Note: Get Caller ID From will be filled field empty.</p>
Get DID From	<p>Different devices or providers may contain DID numbers in different SIP headers. When an inbound call through a SIP trunk reaches the PBX, the PBX needs to retrieve a correct DID number, or the call will fail.</p> <p>Adjust the setting after analysis of the SIP packets sent from the trunk provider.</p>	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> • follow_system: [Follow] • to: To • invite: Invite • diversion: Diversion • rpid: Remote-Party-ID • pai: P-Asserted-Identity • ppi: P-Preferred-Identity • pcpid: P-Called-Party-ID <p> Note: Get DID From will be filled with empty.</p>
From User Part	<p>A From header contains caller ID and caller ID name.</p> <p>From User Part indicates caller ID.</p>	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> • default: [Default] • ext_cid: Extension Caller ID • trunk_user: Trunk User <p> Note: Only available when Trunk User is enabled.</p> <ul style="list-style-type: none"> • trunk_def_outbcid: Trunk Default Outbound Caller ID • ext_outbcid: Extension Outbound Caller ID • outrounter_outbcid: Outbound Caller ID • originator_cid: Originator Caller ID • A customized value. <p> Note: Fill in a desired value of length is 31. Only numbers, *, # are allowed.</p> <p> Note: From User Part will be filled field empty.</p>

Parameter	Description	Importance	Permitted value:
From Display Name Part	<p>A From header contains caller ID and caller ID name.</p> <p>From Display Name Part indicates caller ID name.</p>	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> • default: [Default] • ext_cid_name: Extension Call • trunk_def_outbcid_name: Trunk • ext_outbcid_name: Extension • originator_cid_name: Originator • A customized value. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note: Fill in a desired value of length is 63.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note: From Display Name Part will leave this field empty.</p> </div>
Diversion	Define the parameters included in the Diversion SIP header.	Optional	<p>Permitted value:</p> <ul style="list-style-type: none"> • default: [Default] • ext_cid: Extension Call • trunk_user: Trunk User <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note: Only available when Trunk</p> <ul style="list-style-type: none"> • trunk_def_outbcid: Trunk • ext_outbcid: Extension • outrounter_outbcid: Out • originator_cid: Originator • A customized value. </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note: Fill in a desired value of length is 31. Only numbers, *, # are allowed.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note: Leave Diversion field empty in SIP INVITE packet.</p> </div>

Parameter	Description	Importance	Permitted value:
Remote-Party-ID	Define the parameters included in the Remote-Party-ID SIP header.	Optional	<p>Permitted value:</p> <ul style="list-style-type: none"> • default: [Default] • ext_cid: Extension Call • trunk_user: Trunk User <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p> Note: Only available when Tr</p> <ul style="list-style-type: none"> • trunk_def_outbcid: Tru • ext_outbcid: Extension • outrounter_outbcid: Ou • originator_cid: Originat • A customized value. </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p> Note: Fill in a desired value c length is 31. Only num *, # are allowed.</p> </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p> Note: Leave Remote-Party-ID field this parameter with SIP INV</p> </div>
P-Asserted-Identity	Define the parameters included in the P-Asserted-Identity SIP header.	Optional	<p>Permitted value:</p> <ul style="list-style-type: none"> • default: [Default] • ext_cid: Extension Call • trunk_user: Trunk User <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <p> Note: Only available when Tr</p> <ul style="list-style-type: none"> • trunk_def_outbcid: Tru • ext_outbcid: Extension • outrounter_outbcid: Ou • originator_cid: Originat • A customized value. </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p> Note: Fill in a desired value c length is 31. Only num *, # are allowed.</p> </div>

Parameter	Description	Importance	F
			<p> Note: Leave P-Asserted-Identity field empty. If you want to use this parameter with SIP INVITE, set it to SIP INVITE.</p>
P-Preferred-Identity	Define the parameters included in the P-Preferred-Identity SIP header.	Optional	<p>Permitted value:</p> <ul style="list-style-type: none"> • default: [Default] • ext_cid: Extension Call ID • trunk_user: Trunk User <p> Note: Only available when Trunk User is set.</p> <ul style="list-style-type: none"> • trunk_def_outbcid: Trunk Default Outbound Call ID • ext_outbcid: Extension Outbound Call ID • outrounter_outbcid: Outbound Call ID • originator_cid: Originator Call ID • A customized value. <p> Note: Fill in a desired value of length 31. Only numbers, *, # are allowed.</p> <p> Note: Leave P-Preferred-Identity field empty. If you want to use this parameter with SIP INVITE, set it to SIP INVITE.</p>
User Agent	If the ITSP requires User Agent for authentication, enter the User Agent information that is provided by the ITSP.	Optional	The maximum character length is 31.
Realm	Realm is a string displayed to users so they know which username and password to use.	Optional	The maximum character length is 31.
Send Privacy ID	Whether to send the Privacy ID in SIP header or not.	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> • 0: Disable • 1: Enable
User Phone	Whether to add the parameter <code>user=phone</code> as a request line	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> • 0: Disable


Parameter	Description	Importance	
	in the header field of the SIP INVITE packet.		<ul style="list-style-type: none"> • 1: Enable
100rel	Whether to support 100rel or not.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable
Maxptime	Select the value of the Maxptime used when the PBX sends the INVITE packet.	Required	Permitted value: <ul style="list-style-type: none"> • default: PBX will send according to the codec th • A customized value. <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Fill in a desired value c ple of 10 ranging from</p> </div> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Maxptime will be filled with empty.</p> </div>
Support P-Early-Media	Set whether the P-Early-Media field is included in the INVITE packet.	Required	Permitted value: <ul style="list-style-type: none"> • 0: Disable • 1: Enable

Related information

[Export and Import SIP Trunks](#)

Trunk DID/DDIs Parameters

Descriptions for parameters in exported and imported Trunk DID/DDIs CSV file.

 Note:

The following types of trunks support DID/DDIs:

- SIP
- BRI
- E1/T1/J1


Parameter	Description	Importance	Restriction	Default Value
DID/DDI	A virtual number that is used to identify which path of the trunk is passing the call.	Required	Numbers, letters, and characters [] * # () . - + ! The maximum character length is 31.	N/A
DID/DDI Name	The name of DID/DDI that is used to identify which path of the trunk is passing the call.	Optional	The maximum character length is 127.	N/A

Related information

[Export and Import Trunk DID/DDI Numbers](#)

Trunk Outbound Caller ID Parameters

Descriptions for parameters in exported and imported Trunk Outbound Caller ID CSV file.

Parameter	Description	Importance	Restriction	Default Value
Create Method	The way to add outbound caller ID.	Required	Permitted value: <ul style="list-style-type: none"> • single: Shared Outbound Caller ID • range: Outbound Caller ID Range <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Create Method will be filled with default value if you leave this field empty.</p> </div>	single
Outbound Caller ID	The caller ID that is displayed on the callee's device for specific extensions.	Required	Numbers, letters, characters [] () . - + * #, and placeholder {{.Ext}} are allowed. The maximum character length is 31(for each caller ID). For outbound caller id range: <ul style="list-style-type: none"> • Only numbers and character + (before numbers) are allowed. Fill in the start caller id and the 	N/A

Parameter	Description	Importance	Restriction	Default Value
			<p>end caller id with separator -, e.g. 5503301-5503310.</p> <ul style="list-style-type: none"> The start number and the end number must have the same amount of digits and both contain character + or neither. The range of start number and end number cannot exceed 500. Then fill the extension range in Associated Extensions. The extension range and the outbound caller id range must have the same amount of numbers. 	
Outbound Caller ID Name	The caller ID that is displayed on the callee's device for specific extensions.	Optional	The maximum character length is 127.	N/A
Associated Extensions	The extensions that are associated with the Outbound Caller ID and Outbound Caller Name.	Required	<p>Permitted value: one or more extension numbers and extension group names existed in PBX.</p> <ul style="list-style-type: none"> For multiple extensions or groups, please enter the numbers or names and use & as a separator, e.g. extension_number1&extension_number2&extension_group_name3. If the extensions or groups you enter are not existing in PBX, it will be skipped. For extension range, please fill in the start extension number and the end extension number with separator -, e.g. 1001-1010. The maximum number length is 7(for each number). 	N/A

Related information

[Export and Import Trunk Outbound Caller IDs](#)

'Inbound Caller ID Reformatting Rule' Parameters

Descriptions for parameters in exported and imported 'Inbound Caller ID Reformatting Rule' CSV file.

Parameter	Description	Importance	Restriction	Default Value
Patterns	The inbound caller ID that matches this pattern will be reformatted.	Required	Numbers, letters, and characters [] * # () . - + ! are allowed. The maximum character length is 31.	N/A
Strip	Specify how many digits will be stripped from the beginning of the inbound caller ID.	Optional	Only numbers are allowed. The maximum character length is 2.	N/A
Prepend	Specify the digits that will be prepended to the inbound caller ID.	Optional	Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.	N/A


Related information


[Export and Import Inbound Caller ID Reformatting Rules](#)


Inbound Route Parameters



Descriptions for parameters in imported and exported Inbound Route CSV file.



Parameter	Description	Importance	Restriction	Default Value
Name	The name of inbound route.	Required	Space and special characters are not allowed. Inbound route's name cannot be duplicated. The maximum character length is 63.	N/A
Inbound Alert Info	The Alert Info field is used to configure dis-	Optional	Only numbers and letters are allowed.	N/A


Parameter	Description	Importance	Restriction	Default Value
	tinctive ring tones for incoming calls.		The maximum character length is 31.	
DID Matching Mode	The DID matching mode.	Optional	Permitted value: <ul style="list-style-type: none"> • <code>patterns</code>: DID Patterns • <code>pattern_to_ext</code>: DID Pattern to Extensions • <code>range_to_ext</code>: DID Range to Extension Range <div style="border: 1px solid #00a0e3; padding: 5px; margin-top: 10px;"> <p> Note: DID Matching Mode will be filled with default value patterns if you leave these fields empty.</p> </div>	patterns
DID Pattern	The DID pattern that is used to match callee number. Only when the callee number is matched will the inbound call go through this route.	Required if DID Matching Mode ≠ patterns	<ul style="list-style-type: none"> • If DID Matching Mode = <code>patterns</code>, you can enter one or more patterns. Numbers, letters X Z N, and characters [] * # () . - + ! are allowed. The maximum character length is 31 (for each DID). Please use & as a separator for multiple patterns, e.g. <code>pattern1&pattern2</code>. • If DID Matching Mode = <code>pattern_to_ext</code>, only numbers, letters X Z N, characters [] * # () - +, and placeholder <code>{{ .Ext }}</code> are allowed. The maximum character length is 31. The Default Destination must be <code>pattern_to_ext</code>, then fill multiple ex- 	N/A

Parameter	Description	Importance	Restriction	Default Value
			<p>tension numbers with separator & in Number.</p> <ul style="list-style-type: none"> If DID Matching Mode = <code>range_to_ext</code>, only numbers and character + (before numbers) are allowed. The maximum character length is 16 (for each DID). Please enter the start DID and the end DID with separator -, e.g. 5503301-5503305. <p>The Default Destination must be <code>range_to_ext</code>, then fill the start number and the end number with separator - in Number, e.g. 1001-1005.</p>	
<p>Caller ID Matching Mode</p>	<p>The Caller ID matching mode.</p>	<p>Required</p>	<p>For Basic Plan: Permitted value:</p> <ul style="list-style-type: none"> <code>patterns</code>: Caller ID Matching Settings <div data-bbox="917 1255 1250 1493" style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: Caller ID Matching Mode will be filled with default value <code>patterns</code> if you leave these fields empty.</p> </div> <p>For Enterprise/Ultimate Plan: Permitted value:</p> <ul style="list-style-type: none"> <code>patterns</code>: Caller ID Matching Settings <code>phonebook</code>: Match Contacts' Caller ID in Specific Phonebooks 	<p><code>patterns</code></p>

Parameter	Description	Importance	Restriction	Default Value
			<div style="border: 1px solid #add8e6; padding: 5px;">  Note: Caller ID Matching Mode will be filled with default value <code>patterns</code> if you leave this fields empty. </div>	
Caller ID Pattern	The pattern used to match caller ID. Only when the caller ID matches the pattern can user dials in through this route.	Optional	<p>For Basic Plan: The maximum character length is 31 (for each pattern). Numbers, letters, characters [] * # () . - + ! are allowed.</p> <p>For multiple patterns, enter patterns and use & as a separator, e.g. pattern1&pattern2.</p> <p>For Enterprise/Ultimate Plan:</p> <ul style="list-style-type: none"> • If Caller ID Matching Mode = <code>patterns</code>, the maximum character length is 31 (for each pattern). Numbers, letters, characters [] * # () . - + ! are allowed. • If Caller ID Matching Mode = <code>phonebook</code>, the permitted value is one or more phonebook names existed in PBX. <p>For multiple phonebook names, enter names and use & as a separator, e.g. name1&name2.</p> <p>If the phonebook you enter does not exist in PBX, it will be skipped.</p>	N/A
Trunks	The trunks that incoming calls	Required	Permitted value: one or more trunk names existed in PBX.	N/A

Parameter	Description	Importance	Restriction	Default Value
	will be routed by this inbound route. The PBX will route inbound calls through this route when external users call the selected trunk number.		<p>For multiple trunks, please enter trunk names and use & as a separator, e.g. name1&name2.</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: If the trunks you enter are not existing in PBX, Trunks will be skipped.</p> </div>	
Default Destination	The default destination to receive inbound calls.	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> • <code>end_call</code>: Hang Up • <code>extension</code>: Extension • <code>range_to_ext</code>: Match extension Range (DID Matching Mode = <code>range_to_ext</code>) • <code>pattern_to_ext</code>: Match selected Extension (DID Matching Mode = <code>pattern_to_ext</code>) • <code>ext_vm</code>: Extension Voicemail • <code>group_vm</code>: Group Extension • <code>ivr</code>: IVR • <code>ring_group</code>: Ring Group • <code>queue</code>: Queue • <code>conference</code>: Conference • <code>fax_to_email</code>: Fax to Email <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Default Destination will be filled with default value if you leave these fields empty.</p> </div>	end_call
Number of Default Destination	The destination number to receive inbound calls.	Required if Default Desti-	<p>Permitted value:</p> <ul style="list-style-type: none"> • If Default Destination = <code>Extension, Extension</code> 	N/A

Parameter	Description	Importance	Restriction	Default Value
		nation ≠ end_call	<p>Email, Group Voice-mail, IVR, Ring Group, Queue, Conference, Or Fax to Email, please fill in a number.</p> <ul style="list-style-type: none"> If Default Destination = Match extension Range, please fill in a range of extension, e.g. 1000-1010. <p>The maximum number length is 7 (for each number).</p> <ul style="list-style-type: none"> If Default Destination = Match selected Extension, please fill in numbers or names and use & as a separator, e.g. extension_number1&extension_number2&extension_group_name3. <div data-bbox="836 1150 1252 1352" style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: If the numbers or names you enter are not existing in PBX, Number of Default Destination will be skipped.</p> </div>	
Enable Fax Detection	Whether to enable or disable FAX detection.	Required	<p>Permitted value:</p> <ul style="list-style-type: none"> 0: Disable 1: Enable <div data-bbox="836 1562 1252 1730" style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Enable Fax Detection will be filled with default value if you leave this field empty.</p> </div>	0
Fax Destination	The destination to receive fax.	Required if Enable Fax De-	<p>Permitted value:</p> <ul style="list-style-type: none"> end_call: Hang Up extension: Extension 	extension

Parameter	Description	Importance	Restriction	Default Value
		Importance = 1	<ul style="list-style-type: none"> <code>fax_to_email</code>: Fax to Email <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Fax Destination will be filled with default value if you leave these fields empty.</p> </div>	
Number of Fax Destination	The destination number to receive fax.	Required if Fax Destination \neq <code>end_call</code>	<p>Permitted value: extension numbers existed in PBX.</p> <ul style="list-style-type: none"> If Fax Destination = <code>Extension</code>, fax will be sent to extension number. If Fax Destination = <code>Fax to Email</code>, fax will be sent to extension's email address. 	N/A



Related information




[Export and Import Inbound Routes](#)


Outbound Route Parameters

Descriptions for parameters in exported and imported Outbound Route CSV file.

Parameter	Description	Importance	Restriction	Default Value
Name	The name of outbound route.	Required	<p>Space and special characters are not allowed.</p> <p>Outbound route's name cannot be duplicated.</p> <p>The maximum character length is 63.</p>	N/A
Outbound Caller ID	The caller ID that is displayed on the callee's device.	Optional	Numbers, letters, and characters [] () . - + * # and placeholder {{.Ext}} are allowed.	patterns

Parameter	Description	Importance	Restriction	Default Value
			The maximum character length is 31.	
Pattern	The pattern used to match a callee number. Only when the callee number is matched will the outbound call go through this route.	Required	Numbers, letters X Z N, and characters [] * # () . - + ! are allowed. The maximum character length is 31.  Note: Pattern will be filled with default value X if you leave these fields empty.	N/A
Strip	The number of digits that will be stripped from the front of callee number before the call is placed.	Optional	Only numbers 1 - 16 are allowed.	N/A
Prepend	The digits that will be prepended to the callee number before the call is placed.	Optional	Numbers, letters, and characters () . - + * # are allowed. The maximum character length is 31.	N/A
Trunks	The trunks that can be used to dial out. The PBX will route outbound calls through this trunk when the dialed number matches the outbound route.	Required	Permitted value: one or more trunk names existed in PBX. For multiple trunks, please enter trunk names and use & as a separator, e.g. name1&name2.  Note: If the trunk you enter does not exist in PBX, it will be skipped.	N/A
Rmemory Hunt	Whether to remember which trunk was used last time, and then use the	Required	Permitted value: • 0: Disable • 1: Enable	0

Parameter	Description	Importance	Restriction	Default Value
	next available trunk to call out.		 Note: Rrmemory Hunt will be filled with default value if you leave this field empty.	
Extensions	The extensions that are allowed to make outbound calls through this route.	Optional	Permitted value: one or more extension numbers and extension group names existed in PBX. For multiple extensions or extension groups, please enter the numbers or names and use & as a separator, e.g. extension_number1&extension_number2&extension_group_name3.  Note: If the extensions or group names you enter are not existing in PBX, Extensions will be skipped.	extension
Outbound Route Password	Whether to require users to enter the same PIN to make outbound calls through this route.	Required	Permitted value: <code>disable</code> , <code>single_pin</code> , or <code>pin_list</code> .  Note: Outbound Route Password will be filled with default value if you leave these fields empty.	N/A
PIN	The PIN is required to make outbound calls through this route.	Required if Outbound Route Password is <code>single_pin</code>	Only numbers are allowed. The minimum character length is 3 and the maximum is 15.	N/A
PIN List	The PIN codes in the selected PIN	Required if Out-	Permitted value: The name of a PIN list existed in PBX.	N/A


Parameter	Description	Importance	Restriction	Default Value
	list is required to make outbound calls through this route.	bound Route Pass- word is <code>pin_list</code>	 Note: If the PIN list name you entered is not existing in PBX, it will be skipped.	




Related information



[Export and Import Outbound Routes](#)

Static Defense Rule Parameters

Descriptions for parameters in exported and imported 'Static Defense Rule' CSV file.

Parameter	Description	Importance	Restriction	Default Value
Name	The name of defense rule.	Required	The maximum character length is 127.  Note: The name of Static Defense Rule cannot be duplicated.	N/A
Description	The note to the rule.	Optional	The maximum character length is 2047.	N/A
Action	The action for the rule.	Required	Permitted value: <ul style="list-style-type: none"> • accept: Accept connections from a specific address. • drop: Restrict a specific address from accessing a specific service or port of the PBX, and do NOT send any error notifications back to the sender. • reject: Restrict a specific address from accessing a specific service or port of the PBX, and send error notifications back to the sender. 	accept

Parameter	Description	Importance	Restriction	Default Value
			 Note: Action will be filled with default value if you leave this field empty.	
Object Type	The type of the source traffic.	Required	Permitted value: ip, domain, or mac.  Note: Object Type will be filled with default value if you leave this field empty.	ip
Source IP Address	The source IP address.	Required if Type = ip	Must be IPv4 address format XXX.XXX.XXX.XXX.XXX: 0 - 255	N/A
Subnet Mask	The subnet mask.	Required if Type = ip	Must be IPv4 address format XXX.XXX.XXX.XXX.XXX: 0 - 255	N/A
Domain	The domain name.	Required if Type = domain	The maximum character length is 255.	N/A
MAC Address	The MAC address.	Required if Type = mac	Only numbers, letters A to F, a to f and character - : are allowed. The character length must be 12 or 17.	N/A
Service/Port Range	The type of defense objects.	Required if Action = drop or reject (leave it empty if Action = accept)	Permitted value: service or port_range.  Note: Service/Port Range will be filled with default value if you leave this field empty.	service
Service	The service to which the rule is applied.	Required if Service/Port Range = service	Permitted value: https, http, ssh, ftp, sip_udp, sip_tcp, sip_tls, outbound_sip, rtp, or linkus.	N/A
Start Port	The start port.	Required if Service/Port Range = port_range	Only numbers between 1 and 65535 are allowed. Start port must be less than or equal to end port.	1


Parameter	Description	Importance	Restriction	Default Value
End Port	The end port.	Required if Service/Port Range = port_range	 Note: Start Port and End Port will be filled with default port range if you leave these fields empty.	65535
Protocol	The protocol to which the rule is applied.	Required	Permitted value: both, udp, or tcp.  Note: Protocol will be filled with default value if you leave this field empty.	both



Related information

[Export and Import Static Defense Rules](#)

Auto Defense Rule Parameters

Descriptions for parameters in exported and imported 'Auto Defense Rule' CSV file.

Parameter	Description	Importance	Restriction	Default Value
Name	The name of defense rule.	Required	The maximum character length is 127. Auto defense's name cannot be duplicated.	N/A
Service/Port Range	The type of defense objects.	Required	Permitted value: service or port_range.  Note: Service/Port Range will be filled with default value if you leave this field empty.	service
Service	The service to which the rule is applied.	Required if Service/Port Range = service	Permitted value: <ul style="list-style-type: none"> • https • http • ssh • ftp 	N/A

Parameter	Description	Importance	Restriction	Default Value
			<ul style="list-style-type: none"> • sip_udp • sip_tcp • sip_tls • outbound_sip • rtp • linkus 	
Start Port	The start port.	Required if Service/Port Range = port_range	Only numbers between 1 and 65535 are allowed. Start Port must be less than or equal to End Port.	1
End Port	The end port.	Required if Service/port Range = port_range	<div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: Start Port and End Port will be filled with default port range if you leave these fields empty.</p> </div>	65535
Protocol	The protocol to which the rule is applied.	Required	Permitted value: <ul style="list-style-type: none"> • both • udp • tcp <div style="border: 1px solid #add8e6; padding: 5px; margin-top: 10px;"> <p> Note: Protocol will be filled with default value if you leave this field empty.</p> </div>	both
Number of Packets	The number of packets permitted within a specific time interval.	Required	Only numbers between 1 and 255 are allowed.	N/A
Time Interval(s)	The time interval (in seconds) to receive IP packets.	Required	Only numbers are allowed. The maximum character length is 5.	N/A



Related information

[Export and Import Auto Defense Rules](#)

'Outbound Call Frequency Restriction Rule' Parameters

Descriptions for parameters in exported and imported 'Outbound Call Frequency Restriction' CSV file.

Table 56.

Parameter	Description	Importance	Restriction	Default Value
Name	The name of Outbound Call Frequency Restriction rule.	Required	The maximum character length is 127. <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: The name of an Outbound Call Frequency Restriction cannot be duplicated.</p> </div>	N/A
Restrictions	How many outbound calls users can make within a specified time period.	Required	Format: <code>{number_of_calls_limit}/{time_limit}/{time_unit}</code> Example: <code>200/10/second</code> <div style="border: 1px solid #add8e6; padding: 5px;"> <p> Note: Use & to separate multiple restrictions, e.g. <code>200/10/second&3000/1/minute</code>.</p> </div> <p>Variables:</p> <p><code>{number_of_calls_limit}</code>:</p> <ul style="list-style-type: none"> • Only numbers are allowed. • The maximum character length is 5. <p><code>{time_limit}</code>:</p> <ul style="list-style-type: none"> • Only numbers are allowed. • The maximum character length is 5. <p><code>{time_unit}</code>:</p> <p>Permitted value: second or minute.</p>	N/A

Related information

[Export and Import 'Outbound Call Frequency Restriction' Rules](#)