Administrator Guide

Yeastar P-Series Appliance Edition

Version: 37.19.0.70
Date: 2025-06-09



+86-592-5503309 sales@yeastar.com www.yeastar.com

Contents

About This Guide..... 1
Getting Started..... 2
Log in to PBX Web Portal..... 2
Initial Setup Using the Installation Wizard..... 9
Change the Password of Super Administrator..... 13
Reset the Password of Super Administrator..... 14
Set up Company Information..... 16
View System Information..... 17
Change Web Interface Language..... 18
Log out of PBX web portal..... 18
Dashboard..... 19
Dashboard Overview..... 19
Extension..... 27
Extension Overview..... 27
Create Extensions..... 28
Create a SIP Extension..... 28
Create an FXS Extension..... 31
Bulk Create SIP Extensions..... 33
Set up Phones..... 38
Set up an Analog Phone..... 38
Set up a SIP Phone..... 38
Set up a Remote SIP Phone via Public IP Address and Port..... 39
Set up a Remote SIP Phone via Yeastar FQDN..... 42
Extension Outbound Caller ID..... 46
Allow Users to Select Outbound Caller ID (DOD) to Call..... 46
Extension Presence..... 49
Extension Presence Overview..... 49
Presence Settings..... 50
Manually Switch Extension Presence..... 54
Automatically Switch Extension Presence Based on Time..... 55

Monitor Extension Status by BLF Key....56
Forward Incoming Calls to Another Destination....59
Ring Office Phone and Mobile Phone Simultaneously....61
Extension Voicemail....62
Set up Extension Voicemail....62
Extension Function Keys....64
Set up Function Keys for Extensions Using a Template....64
Extension Features....67
Handle Incoming Calls Based on Caller ID....67
Set up Email Notifications for Missed Calls....69
Set up Email Notifications for User Password Change....70
Customize Music on Hold for an Extension....70
Allow Multiple Registrations for One Extension Number....71
Set Business Hours for an Extension....72
Stop Rejected Calls from Ringing Other Endpoints....74
Enable Video Preview of Intercom Calls for Extensions....75
Extension Advanced Settings....79
Advanced Settings of SIP Extension....79
Advanced Settings of FXS Extension....80
Extension Security....83
Extension Security Overview....83
Restrict Outbound Calls for an Extension....86
Restrict Extension Registration Based on User Agent....87
Restrict Extension Registration Based on IP Address....88
Block Outbound Calls Outside Business Hours....89
Limit Call Duration of an Outbound Call....89
Limit Outbound Call Frequency of an Extension....90
Set up Periodic Password Changes for an Extension....91
Manage Extensions....93
Edit Extensions....93
Reset an Extension's User Password....93
Export and Import SIP Extensions....94
Delete Extensions....95

Extension Visibility Permission..... 96
Set up Extension Visibility.....96
Manage Extension Visibility Rules.....97
Contacts..... 99
Overview..... 99
PBX-native Contacts..... 102
Add and Manage Company Contacts.....102
Export and Import Company Contacts..... 104
Third-party Contacts.....106
Microsoft SQL..... 106
LDAP Server..... 118
Phonebook..... 129
Add and Manage Company Phonebooks..... 129
Contacts Visibility.....131
Set up Contact Visibility.....131
Manage Contact Visibility Rules.....133
Identify Callers from Contacts..... 134
Allow Users to Query Contacts on IP Phones..... 136
Client Permission..... 139
Yeastar P-Series PBX System Client Permissions..... 139
LDAP Server..... 140
LDAP Server Overview..... 140
Set up Yeastar P-Series PBX System as an LDAP Server..... 142
Set up LDAP Client.....145
Auto Provision LDAP for IP Phones.....145
Manual Configuration Examples..... 148
Organization..... 155
Organization Overview..... 155
Enable or Disable Organization Management.....157
Set up Organizations.....158
Add Users to Organizations..... 161
Manage Users within Organizations.....163
Manage Organizations.....165

Export and Import Organizations....167
Extension Group....169
Extension Group Overview....169
Create an Extension Group....171
Manage Extension Groups....173
Assign a User Type to a Group Member....173
View or Change a Member's User Type in Multiple Groups....175
View or Change Permissions for Group Members....176
Auto Provisioning....179
Auto Provisioning Overview....179
Provision IP Phones....183
Auto Provision IP Phones in Local Network (PnP Method)....183
Auto Provision IP Phones in Local Network (DHCP Method)....186
Auto Provision IP Phones Remotely (RPS FQDN Method)....192
Auto Provision IP Phones Remotely (RPS Method)....196
Auto Provision IP Phones Remotely (Provision Link - FQDN Method)....201
Auto Provision IP Phones Remotely (Provision Link Method)....206
Provision Gateways....215
Auto Provision Yeastar TA FXS Gateways (PnP Method)....215
Auto Provision Yeastar TA FXS Gateways (DHCP Method)....218
Auto Provision Yeastar TA FXS Gateway (Provision Link Method)....225
Auto Provision Yeastar TA FXS Gateway (Provision Link FQDN Method)....230
Manage Provisioned Devices....234
Remotely Access a Provisioned IP Phone / Gateway....234
Reboot Provisioned IP Phones/Gateways....240
Reassign an Extension to a Provisioned IP Phone/Gateway....241
Release an Extension from a Provisioned IP Phone/Gateway....242
Remove IP Phones/Gateways from Provisioning List....243
Export and Import Auto Provisioning Phone Information....244
Auto Provisioning Options....245
IP Phone Auto Provisioning Options....245
Automatically Generate Random Passwords for Phones....247
Configure VLAN for a Provisioned Phone....248

Auto Provision Function Keys for Phones....250
Seize a Trunk to Call Out by BLF Key....258
Forward All Incoming Calls to Another Destination by BLF Key....260
Synchronize Phone Time with PBX....262
Modify a Provisioned Phone Settings....263
Modify a Provisioned Gateway Settings....264
Manage Auto Provisioning Templates....265
Apply a New Template to a Provisioned IP Phone/Gateway....265
View a Default Auto Provisioning Template....266
Update a Default Auto Provisioning Template....268
Create a Custom Auto Provisioning Template....269
Manage Custom Auto Provisioning Templates....272
Manage IP Phone Firmware....275
Update Phone Firmware via Auto Provisioning....275
Manage Device Firmware Files....275
Auto Provisioning - Supported Devices....277
Auto Provisioning - Variables in Templates....326
User Role....334
User Roles and Permissions....334
Create a User Role....335
Assign a Role to a User....336
Manage User Roles....337
User Role Permissions....338
Operator Panel....346
Manage Operator Panel....346
Trunk....348
Trunk Overview....348
SIP Trunk....351
SIP Trunk Overview....351
Create a SIP Trunk....352
Manage SIP Trunks....362
Export and Import SIP Trunks....362
SIP Trunk Settings....363

WebRTC Trunk....375
WebRTC Trunk Overview....375
Set up WebRTC Click-to-Call....376
Analog FXO Trunk....381
Analog FXO Trunk Overview....381
Set up an Analog FXO Trunk....382
Release an Analog FXO Trunk....383
Analog FXO Trunk Settings....384
GSM/3G/4G LTE Trunk....387
GSM/3G/4G LTE Trunk Overview....387
Set up a GSM/3G/4G LTE Trunk....389
GSM/3G/4G LTE Trunk Settings....390
ISDN E1/T1 Trunk....392
E1/T1/J1 Trunk Overview....392
Set up an E1/T1/J1 Trunk....393
E1/T1/J1 Trunk Settings....395
ISDN BRI Trunk....404
BRI Trunk Overview....404
Set up a BRI Trunk....405
BRI Trunk Settings....407
Call Control....411
Emergency Calling....411
Emergency Calling Overview....411
Set up Basic Emergency Calling....413
Set up Enhanced Emergency Calling....415
Set up a Route for PSAP Callbacks....417
Manage Emergency Numbers....417
Export and Import Emergency Numbers....418
Emergency Notification Contacts....419
Business Hours and Holidays....423
Overview of Business Hours and Holidays....423
Time Zones....425
Business Hours....428

Holidays....430
Time Condition....437
Time Condition Overview....437
Allow Users to Override Time Condition by Feature Code....441
Allow Users to Override Time Condition on Operator Panel....442
Override Time Condition for Inbound Calls....444
Monitor Time Condition Status....449
Automatic Reset of Time Condition....457
Enable or Disable Automatic Reset of Time Condition....460
Inbound Route....461
Inbound Route Overview....461
Set up an Inbound Route....463
Time Based Inbound Routes....466
Caller ID/DID Based Inbound Routes....477
Manage Inbound Routes....494
Export and Import Inbound Routes....495
DID Pattern and Caller ID Pattern....496
Outbound Route....497
Outbound Route Overview....497
Set up an Outbound Route....498
Restrict Outbound Calls by PIN Codes....500
Manage Outbound Routes....505
Export and Import Outbound Routes....506
Outbound Dial Pattern....507
Dial Pattern Examples....511
AutoCLIP Route....512
AutoCLIP Route Overview....512
Route Inbound Calls to Original Extensions via AutoCLIP Route....513
Delete AutoCLIP Records....516
DID Number....516
DID Number Overview....516
Configure DID Numbers on a Trunk....517
Export and Import Trunk DIDs/DDIs Numbers....519

Caller ID....521
Caller ID Overview....521
Reformat Inbound Caller ID based on a Trunk....522
Export and Import Inbound Caller ID Reformatting Rules....524
Customize Outbound Caller IDs for Outbound Calls....525
Export and Import Trunk Outbound Caller IDs....527
Distinctive Ringtone....528
Distinctive Ringtone Overview....528
Set Distinctive Ringtones for Internal Calls....529
Set Distinctive Ringtones for External Calls....531
Set Distinctive Ringtones for Queue Calls....533
Set Distinctive Ringtones for Ring Group Calls....535
Set Distinctive Ringtones for IVR Calls....538
Distinctive Caller ID Name....540
Distinctive Caller ID Name Overview....540
Enable or Disable Distinctive Caller ID Name....542
Call Features....544
Voicemail....544
Voicemail Overview....544
Group Voicemail....546
Send and Receive Voicemail Messages....556
Manage Voicemail Messages....560
Voicemail Security....567
Voicemail Greetings....569
Voicemail Notifications....576
Custom Voicemail Experience....580
Global Voicemail Settings....582
Voicemail Menu Options....583
Voicemail Capacity and Limitations....585
IVR....586
Interactive Voice Response (IVR) Overview....586
Set up an IVR....588
Set up IVR Prompts....590

Allow Callers to Dial Extensions via IVR....592
Allow Callers to Dial Numbers via IVR....593
Allow Callers to Dial by Name via IVR....594
Allow Callers to Dial Outbound Calls via IVR....598
Allow Callers to Change IVR Prompt Remotely....599
Forward Incoming Calls to an External Number via IVR....600
IVR Configuration Example....601
Advanced IVR Settings....605
Call Recording....624
Call Recording Overview....624
Set up Call Recording....626
Set up Recording Prompts....628
Allow Users to Switch Call Recording Status....629
Monitor Call Recording Status on an IP phone....631
Manage Call Recording Files....632
Auto Clean up Recording Files....635
Grant Manage Permission of Recording Files....636
Restrict Users from Viewing Recording Files....636
Ring Group....637
Ring Group Overview....637
Create a Ring Group....639
Manage Ring Groups....643
Call Queue....644
Call Queue Overview....644
Feature Code....645
Configure Feature Codes....645
Feature Code Reference....645
Conference....653
Conference Overview....653
Create a Conference Room....654
Join a Conference Call....655
Invite Users to a Conference Call....656
Manage Conference Rooms....656

Conference Voice Menu....657
Speed Dial....658
Speed Dial Overview....658
Set up Speed Dial Prefix....658
Add a Speed Dial Number....659
Manage Speed Dial Numbers....659
Export and Import Speed Dial Numbers....660
Call Transfer....661
Call Transfer Overview....661
Set up Call Transfer....662
Perform an Attended Transfer....663
Perform a Blind Transfer....663
Call Flip....664
Call Flip Overview....664
Enable or Disable 'Call Flip' Feature Code....666
Flip an Active Call by Dialing a Feature Code....667
Call Pickup....668
Call Pickup Overview....668
Pick up a Call for a Group Member....669
Pick up a Call for a Specific Extension....671
Call Parking....672
Call Parking Overview....672
Directed Call Parking....674
Call Parking....675
Set up Parking Number....675
Set up Parking Timeout Destination....676
Set up Music on Hold for Call Parking....677
Monitor a Parking Number on an IP Phone....677
Call Monitoring....679
Call Monitoring Overview....679
Allow Users to Monitor a Call by Dialing a Feature Code....682
Disallow Users to be Monitored by Others....683
Call Force Drop....684

Allow Users to Force Drop Extensions' Calls..... 684
Force Drop an Extension's Call.....685
Boss-Secretary.....686
Set up Boss-Secretary Feature for Extensions.....686
Monitor Call Status.....691
Hot Desking..... 697
Hot Desking Overview..... 697
Set up Hot Desing..... 699
Use Hot Desking.....707
Manage Hot Desking feature.....710
Busy Camp-on..... 711
Camp on to a Busy Extension..... 711
Cancel Busy Camp-on Requests..... 712
Fax..... 713
Fax Overview.....713
Send Faxes from an Analog Fax Machine.....715
Receive Faxes through a Dedicated Trunk..... 717
Receive Faxes and Calls through the Same Line.....719
Receive Faxes by Email..... 721
Set up Fax over IP (FoIP).....723
Paging/Intercom.....724
Overview of Paging and Intercom.....724
Paging/Intercom Group.....725
Scheduled Paging/Intercom Call.....735
PIN List.....737
Add a PIN List.....737
Call Disposition.....737
Add Disposition Codes.....737
Call Note..... 739
Allow Users to Add Notes to Calls.....739
Blocked/Allowed Numbers.....741
Block Calls To or From a Phone Number.....741
Export and Import Blocked Numbers.....744

Manage Blocked Numbers..... 745
Allow Calls To or From a Phone Number..... 746
Export and Import Allowed Numbers..... 748
Manage Allowed Numbers..... 749
Messaging..... 750
Omnichannel Messaging Overview..... 750
PBX System..... 752
System Preferences..... 752
Voice Prompt..... 756
Voice Prompt Overview..... 756
System Prompt..... 759
Music on Hold..... 760
Custom Prompt..... 766
Convert Audio Files..... 768
Audio Files Requirements..... 771
SIP Settings..... 772
Jitter Buffer..... 778
Jitter Buffer Overview..... 778
Configure Jitter Buffer..... 779
Network..... 780
Basic Network..... 780
Web Server..... 792
Service Ports..... 794
Yeastar FQDN..... 795
Public IP and Ports..... 810
Static Route..... 823
DHCP Server..... 829
Split DNS..... 830
Date and Time..... 838
Change System Time Manually..... 838
Synchronize System Time with an NTP Server..... 839
Email Server..... 840
Email Server Overview..... 840

Set up Yeastar SMTP Server as an Email Server....841
Set up Gmail as an Email Server....841
Set up Outlook as an Email Server....844
Customize Email Templates....853
Email Sent Logs....855
Storage....856
Storage Overview....856
Set up a USB Flash Drive....857
Set up a Hard Disk Drive....858
Set up an SD Card....860
Set up a Micro SD Card....861
Add a Windows Network Drive....863
Add a Mac Network Drive....869
Manage Storage Locations....874
Auto Cleanup Settings....876
File Sharing....881
Archive....892
Remote Archiving Overview....892
Archive Files to FTP Server....893
Archive Files to SFTP Server....898
Archive Files to Amazon S3....903
Archive Files to Google Cloud Storage....917
Event Notification....929
Event Notification Overview....929
Configure Event Notifications....933
Manage Notification Contacts....935
Manage Event Logs....936
Remote Management....938
Remote Management Overview....938
Connect Yeastar P-Series PBX System to Yeastar Central Management Using Authentication Code....939
Connect Yeastar P-Series PBX System to Yeastar Central Management Using Yeastar ID....941

Disconnect Yeastar P-Series PBX System with Yeastar Central Management..... 943
SNMP.....944
Yeastar P-Series PBX System SNMP Overview..... 944
Set up SNMP on Yeastar P-Series PBX System.....945
Monitor Yeastar P-Series PBX System through SNMP using Zabbix Server..... 947
Yeastar P-Series PBX System MIB.....956
Hot Standby..... 961
Hot Standby Overview.....961
Set up Hot Standby Pair..... 963
Primary Server Takes over the System from Secondary Server.....969
Secondary Server Takes over the System from Primary Server.....971
Enable and Schedule Maintenance Mode on Secondary Server.....972
Security..... 975
Security Overview.....975
Global Anti-hacking IP Blocklist Program..... 978
Download Yeastar Global Anti-hacking IP Blocklist.....978
Report PBX's IP Blocklist to Yeastar Global Anti-hacking IP Blocklist..... 979
Static Defense..... 980
Add a Static Defense Rule.....980
Manage Static Defense Rules..... 981
Export and Import Static Defense Rules.....982
Auto Defense..... 983
Add an Auto Defense Rule.....983
Manage Auto defense Rules..... 984
Export and Import Auto Defense Rules..... 984
Blocked IPs..... 986
Manage Blocked IP Addresses..... 986
Outbound Call Frequency Restriciton..... 986
Add an 'Outbound Call Frequency Restriction' Rule.....986
Manage 'Outbound Call Frequency Restriction' Rules..... 987
Export and Import 'Outbound Call Frequency Restriction' Rules.....988
Restrict Administrator Login..... 989
Restrict Access to Administrator Portal by IP Addresses..... 989

Console/SSH Access....991
Access the System via SSH....991
Certificates....994
Manage TLS certificates on the PBX....994
Manage HTTPS Certificates on the PBX....999
Supported DNS Providers....1003
Delete Certificates....1030
Allowed Country IPs....1031
Restrict Specific Countries or Regions from Accessing Yeastar P-Series PBX System....1031
Check Allowed Country/Region IP....1034
Allowed Country Codes....1035
Restrict International Calls to Specific Countries or Regions....1035
Block Outbound International Calls....1037
Two-Factor Authentication (2FA)....1039
Two-factor Authentication (2FA) Overview....1039
Configure Two-factor Authentication using Authenticator Application....1040
Configure Two-factor Authentication using Email....1043
Manage Two-factor Authentication of Super Administrator Account....1045
Enforce Two-factor Authentication for All Extension Users....1048
Maintenance....1050
Upgrade....1050
Check for Available Firmware Updates....1050
Schedule Automatic Firmware Upgrade....1051
Manually Upgrade PBX Firmware....1052
Backup and Restore....1054
Overview of Backup and Restore....1054
Create an On-Demand Backup....1056
Set up an Automatic Backup Schedule....1057
Restore Your System from a Backup....1059
Restore Another System from a Backup....1061
Reboot....1062
Reboot Yeastar P-Series PBX System on Web Interface....1062

Schedule Automatic Reboot....1063
Reset....1064
Reset the System on Web Interface....1064
Operation Logs....1065
Operation Logs Overview....1065
Manage Operation Logs....1066
Troubleshooting....1067
Capture Network Packet....1067
Use IP Ping Tool to Diagnose Network Issues....1068
Use Traceroute Tool to Diagnose Network Issues....1070
Troubleshoot and Monitor Analog Ports....1073
Enable Core Call Service Anomaly Detection....1074
System Logs....1075
System Logs Overview....1075
Configure Log Level....1076
Manage System Logs....1077
Forward System Logs to a Third-party Syslog Server....1078
CDR and Reports....1081
CDR....1081
Call Detail Record (CDR) Overview....1081
View and Manage CDR....1082
Scheduled CDR....1086
Call Report....1090
Call Reports Overview....1090
Call Reports....1092
Scheduled Reports....1110
Call Accounting....1116
Call Accounting Overview....1116
Call Rate....1117
Add a Call Rate Rule....1117
Manage Call Rate Rules....1119
Export and Import Call Rate Rules....1121
Call Accounting Report....1122

Extension Call Accounting Report....1122
Extension Call Accounting Details Report....1124
Integration....1127
Speech to Text (STT)....1127
Speech to Text (STT) Overview....1127
Integrate with Speech to Text (STT) API....1128
Disconnect Speech to Text (STT) API Integration....1135
Database Grant....1137
Database Grant Overview....1137
Get CDR Data from Database of Yeastar P-Series PBX System....1137
cdr Table in the PBX Database....1141
References....1144
Import and Export Parameters Overview....1144
Extension Parameters....1145
Organization Parameters....1167
Contacts Parameters....1167
Holidays Parameters....1169
Speed Dial Number Parameters....1171
Emergency Number Parameters....1171
Auto Provisioning Phone Information Parameters....1172
Auto Provisioning Phone Information Parameters - Permitted Value....1175
Trunk Parameters....1179
Trunk DIDs/DDIs Parameters....1190
Trunk Outbound Caller ID Parameters....1191
Inbound Caller ID Reformatting Rule Parameters....1193
DID Number to Specific Extension Parameters....1193
Inbound Route Parameters....1194
Outbound Route Parameters....1200
Static Defense Rule Parameters....1203
Auto Defense Rule Parameters....1205
Outbound Call Frequency Restriction Rule Parameters....1207
Rate Parameters....1208
Allowed Numbers Parameters....1209

Blocked Numbers Parameters..... 1210

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 Web Portal

Yeastar P-Series PBX System provides two different web portals for users with different roles to quickly access, set up, and manage the system. This topic describes the difference between them, and introduces how to log in to the PBX web portal.

Web portals overview

Table 1.

Web portal	Description
Administrator portal	Dedicated web portal for super administrator. Super administrator has the highest privileges. Once logged in, the super administrator can access and manage all the PBX system features, including creating extension accounts for users and granting privileges to the created user accounts. **Login address**: `PBX IP address/admin`. For more information, see Log in to administrator portal.
Management portal	The web portal for users with administrative privileges. Users who have a specific role assigned by the super administrator can log in through this portal. Once logged in, users can only access and manage the specific PBX system features that are granted to their roles. **Login address**: `PBX IP address`. For more information, see Log in to management portal.

Log in to administrator 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. The following table shows the compatible browsers.

Table 2.

Web Browser	Version
Google Chrome (recommended)	Chrome 87 or later
Microsoft Edge	Edge 87 or later
Opera	Opera 72 or later

  - 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 web portal, contact your network administrator to check if your PC can communicate with the IP address 192.168.5.150.

Procedure

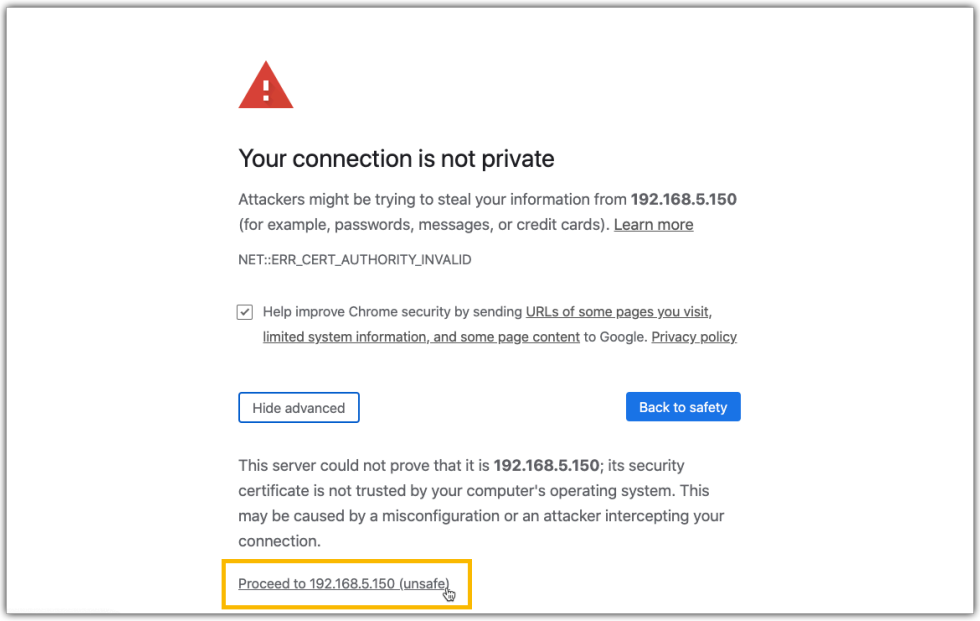
1. Open the web browser, enter the PBX IP address in the address bar, followed by a forward slash and the word "admin", i.e. **PBX IP address/admin**, and press **Enter**.

   For example, the default IP address is 192.168.5.150, then you should enter `192.168.5.150/admin`.

> **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.

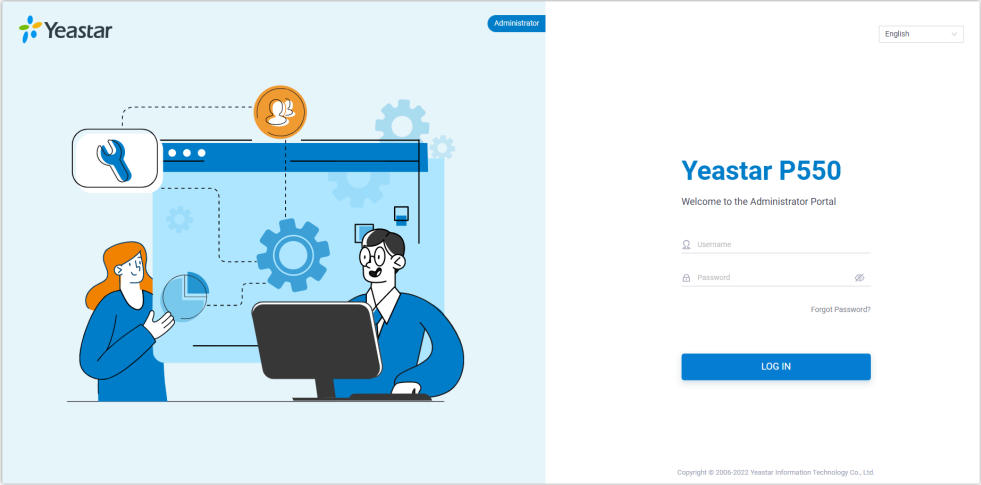
2. If a warning appears to remind you that the page is not secure, ignore the warning on the web page, expand the **Advanced** tab, and proceed to the PBX web.



3. Enter the credentials of the super administrator account, then click **LOG IN**.

> **Note:**
> Supports simultaneous login on up to 5 terminals.

- **Username**: The **username** or **email address** of super administrator account that you have configured in the Installation Wizard.
- **Password**: The password of the super administrator account.



4. If you have set up two-factor authentication, you need to enter an authentication code.



   a. Enter the authentication code provided by an authenticator application or email.
   b. **Optional:** Select the checkbox of **Trusted Device**.

      > **Note:**
      > For the device from which you log in most frequently, you can select the option to add it as a trusted device. In this way, you don't have to re-enter an authentication code with this device for the next 180 days.

   c. Click **LOG IN**.

Log in to management portal

Prerequisite

- An operation and maintenance terminal (a PC) is available. The PC must meet the following requirements:
  - Have a web browser installed. The following table shows the compatible browsers.

    Table 3.

Web Browser	Version
Google Chrome (recommended)	Chrome 87 or later
Microsoft Edge	Edge 87 or later
Opera	Opera 72 or later

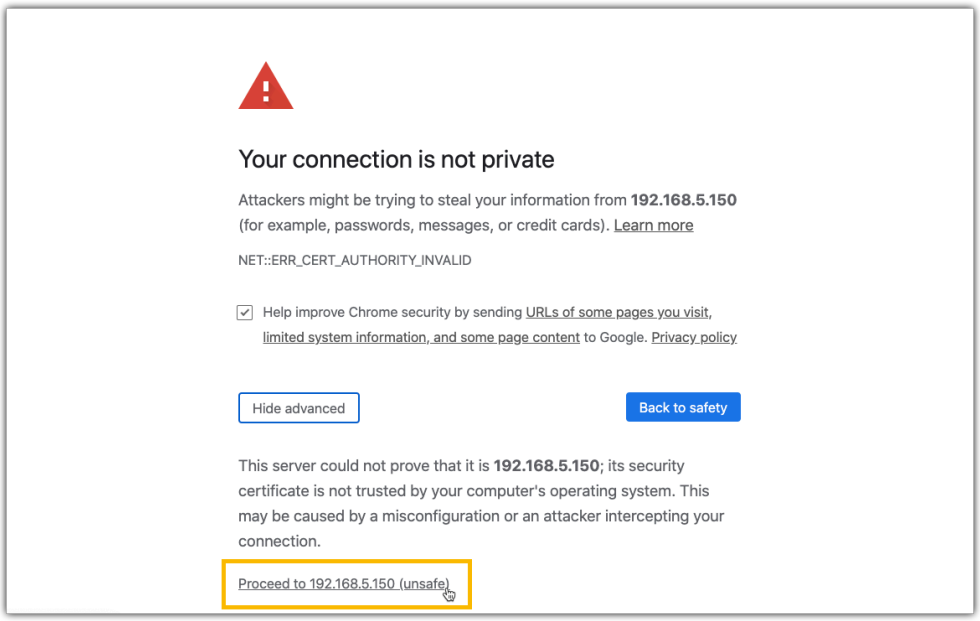
  - Support the resolution of 1366 x 768 or higher.
- You have set the IP address of your PC.

  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.

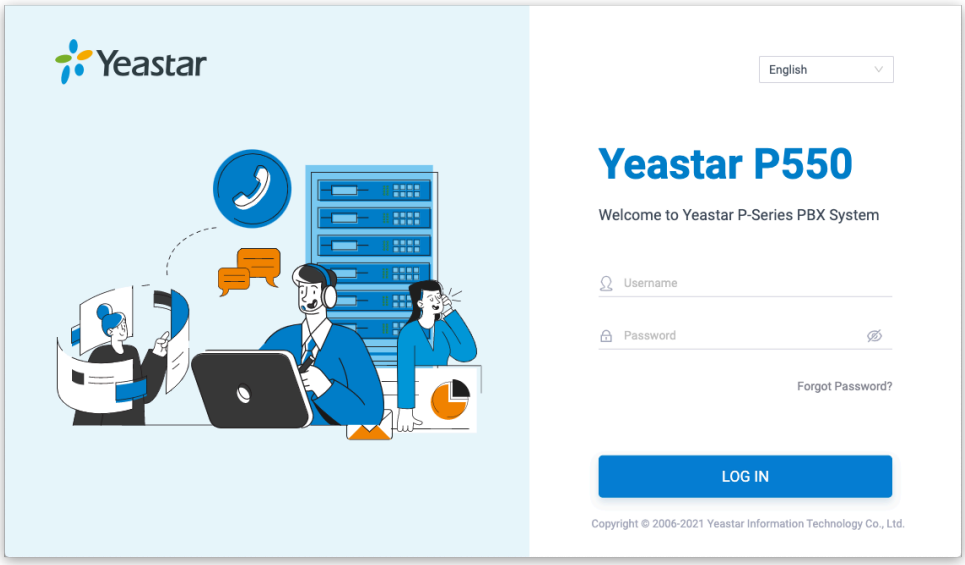
> **Note:**
> - The default IP address of Yeastar P-Series PBX System is 192.168.5.150, and the default gateway address is 192.168.5.1.
> - If you fail to access the PBX web portal, contact your network administrator to check if your PC can communicate with the IP address 192.168.5.150.

Procedure

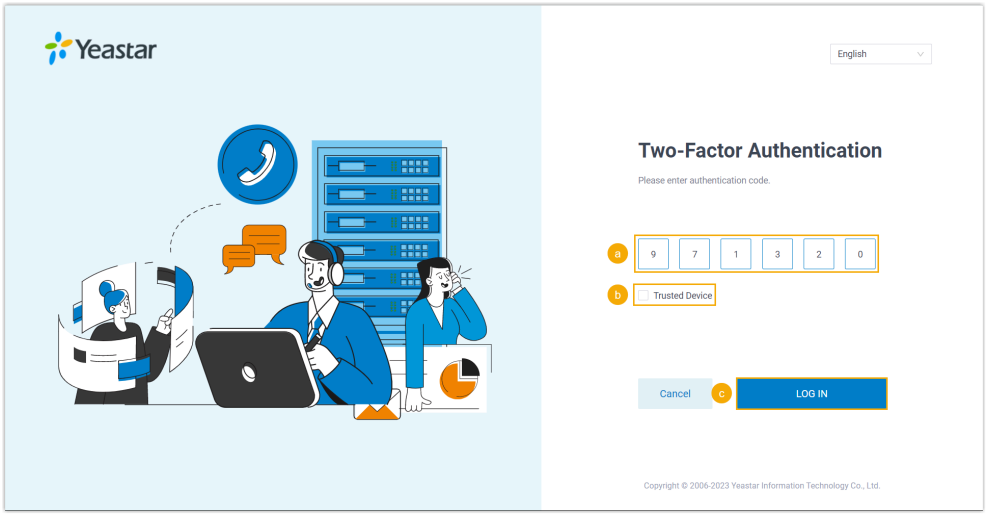
1. Open the web browser, enter the IP address of the PBX in the address bar, and press **Enter**.
2. If a warning appears to remind you that the page is not secure, ignore the warning on the web page, expand the **Advanced** tab, and proceed to the PBX web.



3. Enter the credential of the user account, then click **LOG IN**.
    - **Username**: The **email address** or **extension number** of the user account.
    - **Password**: The password of the user account.



4. If you have set up two-factor authentication, you need to enter an authentication code.

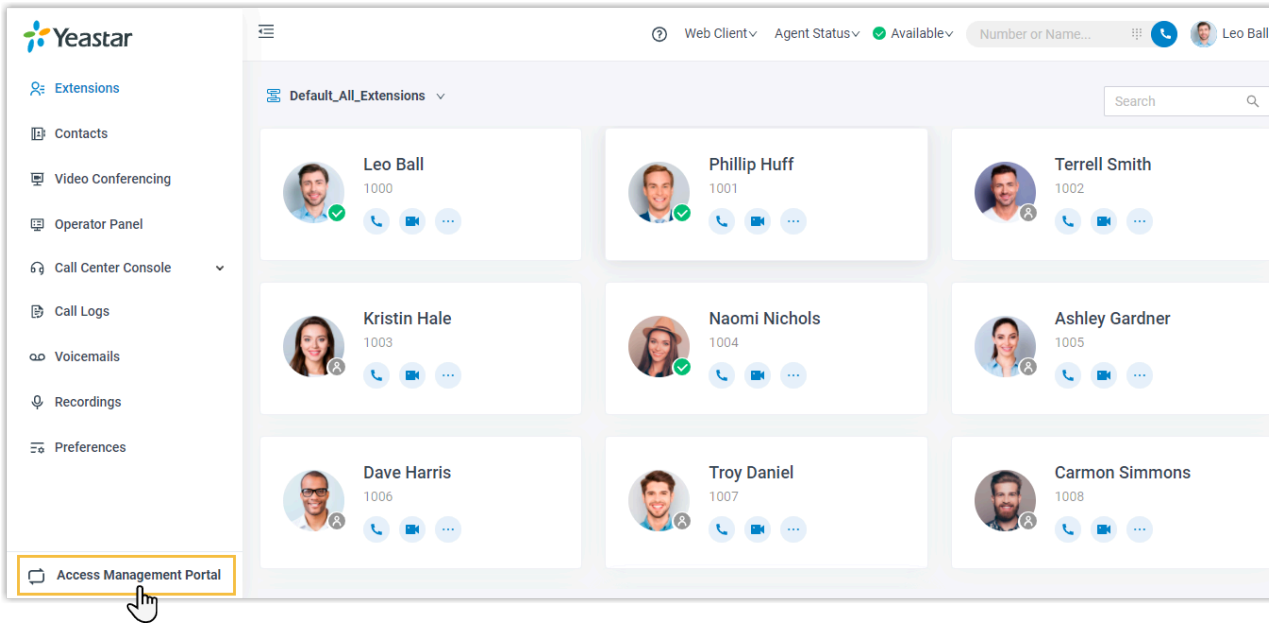


a. Enter the authentication code provided by an authenticator application or email.
b. **Optional:** Select the checkbox of **Trusted Device**.

> **Note:**
> For the device from which you log in most frequently, you can select the option to add it as a trusted device. In this way, you don't have to re-enter an authentication code with this device for the next 180 days.

c. Click **LOG IN**.

5. In the bottom left corner, click **Access Management Portal**.



Initial Setup Using the Installation Wizard

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

Prerequisites

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

For more information about how to access the PBX web interface, see Log in to PBX Web Portal.

> **Warning:**
> The Installation Wizard only appears when you first configure the system with factory settings.

Procedure

- Step 1. Configure the system network
- Step 2. Set up super administrator account
- Step 3. Configure the system time

- Step 4. Localize and customize the system
- Step 5. Check and confirm the configurations

Step 1. 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:**
     > When this mode is selected, if your Internet Telephony Service Provider (ITSP) offers dedicated networking for VoIP communication, and certain IP addresses or domains need to communicate through a dedicated interface, you must configure a static route. Otherwise, all traffic will be routed through the default network interface.

   - **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.

Step 2. 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 web portal.
- **Password**: Specify the password that is used to log in to PBX web 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, reset web login password, and log in to the administrator portal.
- **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**.

Step 3. 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**.

Step 4. 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.

Step 5. 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 web 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 administrator 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 your 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 administrator 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 administrator 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

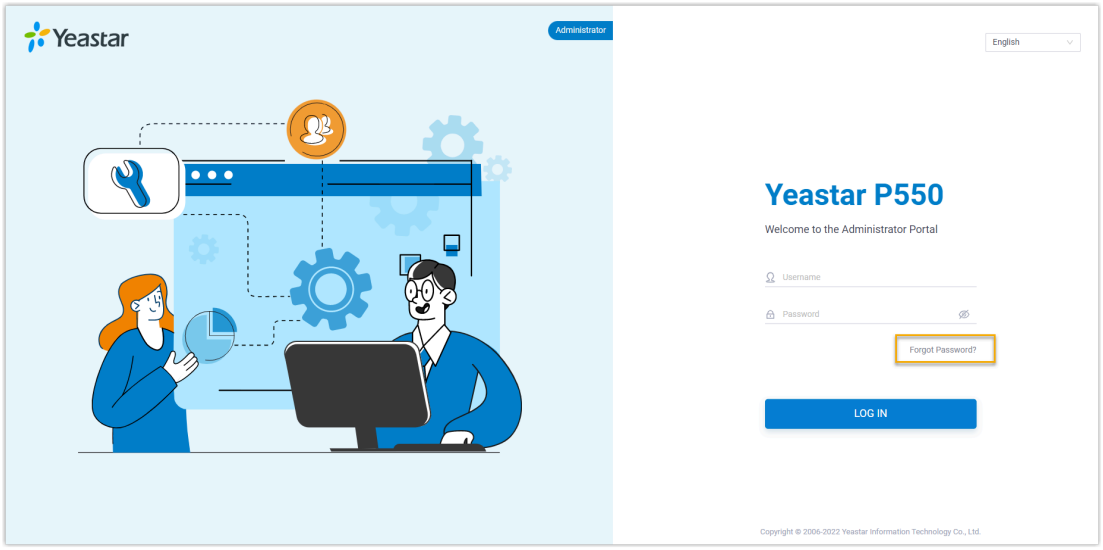
- You need to provide both username and email address, or you cannot reset your password.

  Important:
  If you forget the username of super administrator, you need to reset the system to reconfigure a new username.

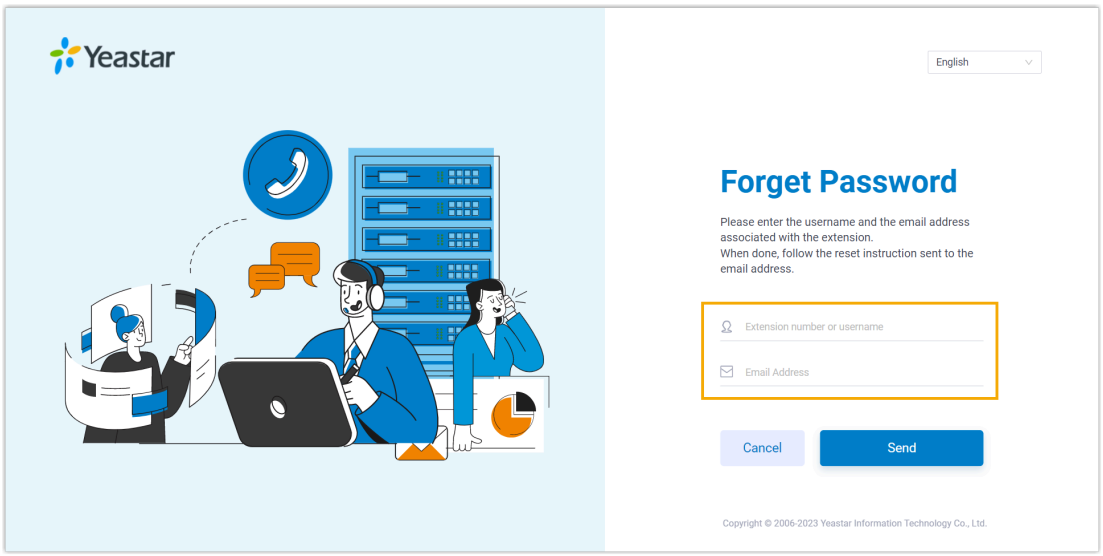
- For P-Series Basic Plan, you can only reset your password in the local network of the PBX system.

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:
   - **Extension number or 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

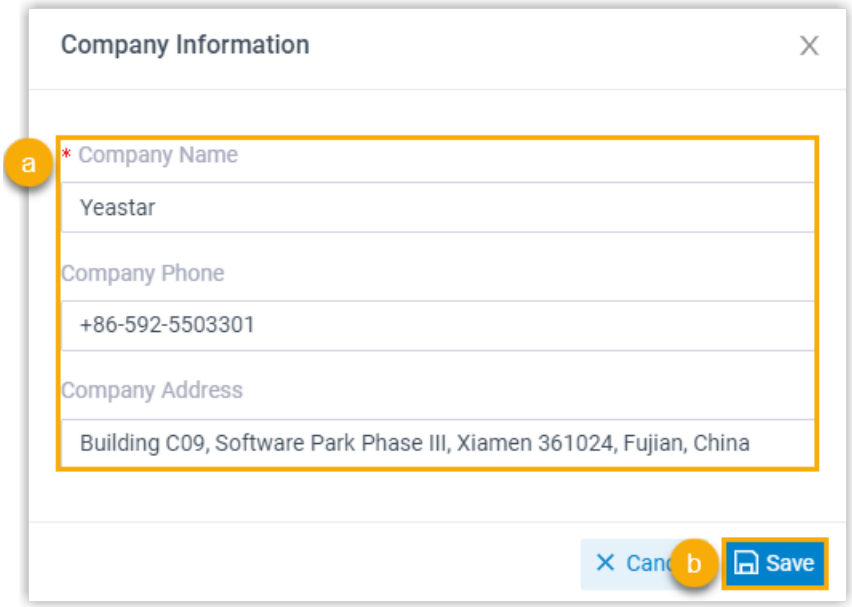
The password of super administrator is changed. You need to log in to PBX administrator portal by the new password next time.

Set up Company Information

Company information contains basic information about your company, including company name, company phone number, and company address. This topic describes how to set up company information.

Procedure

1. Log in to PBX web portal.
2. At the top-right corner of the web page, click and select **Company Information**.
3. In the pop-up window, do as follows:



   a. Configure the name, the phone number, and the address of your company as needed.

> **Note:**
> If you enable **Organization Management** feature on the system, the **Company Name** is required and will be used as the root organization name. For more information, see Enable or Disable Organization Management.

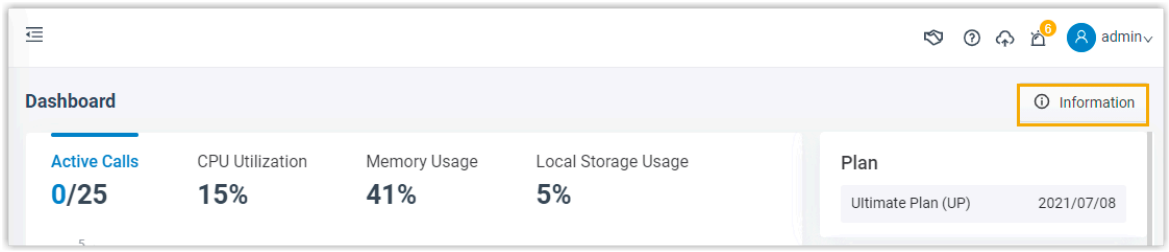
b. Click **Save**.

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 web 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 web portal.
2. At the top-right conner 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 web 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 web portal.

Procedure

1. At the top-right conner of the web page, click  .
2. Select **Log out**.

Related information

Change Automatic Logout Time

Dashboard

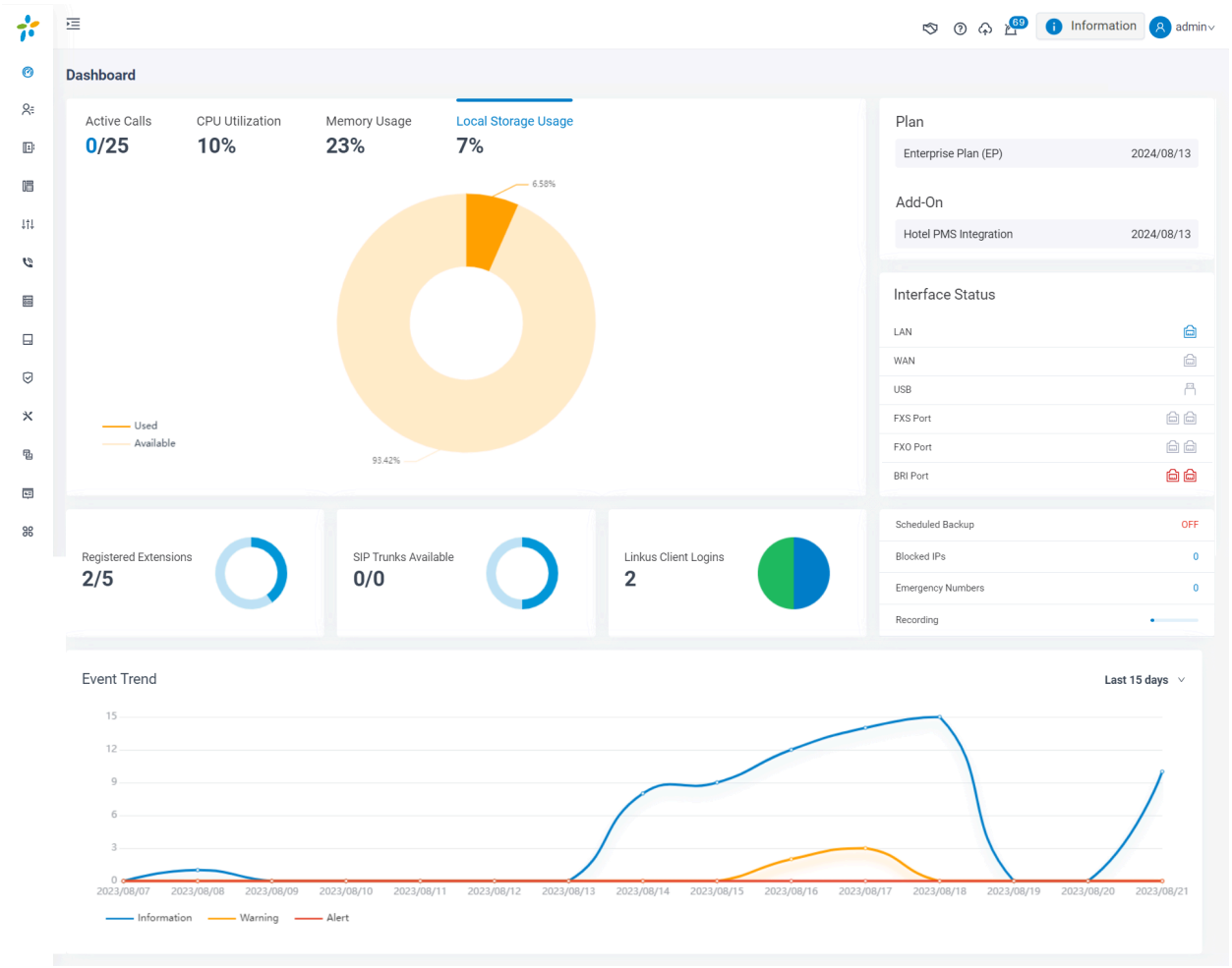
Dashboard Overview

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 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 widgets are as follows:

- System performance
- System information
- Plan
- Add-On
- Interface Status
- System status
- Event trend



1. System performance
2. System information
3. Plan
4. Add-On
5. Interface status
6. System status
7. Event trend

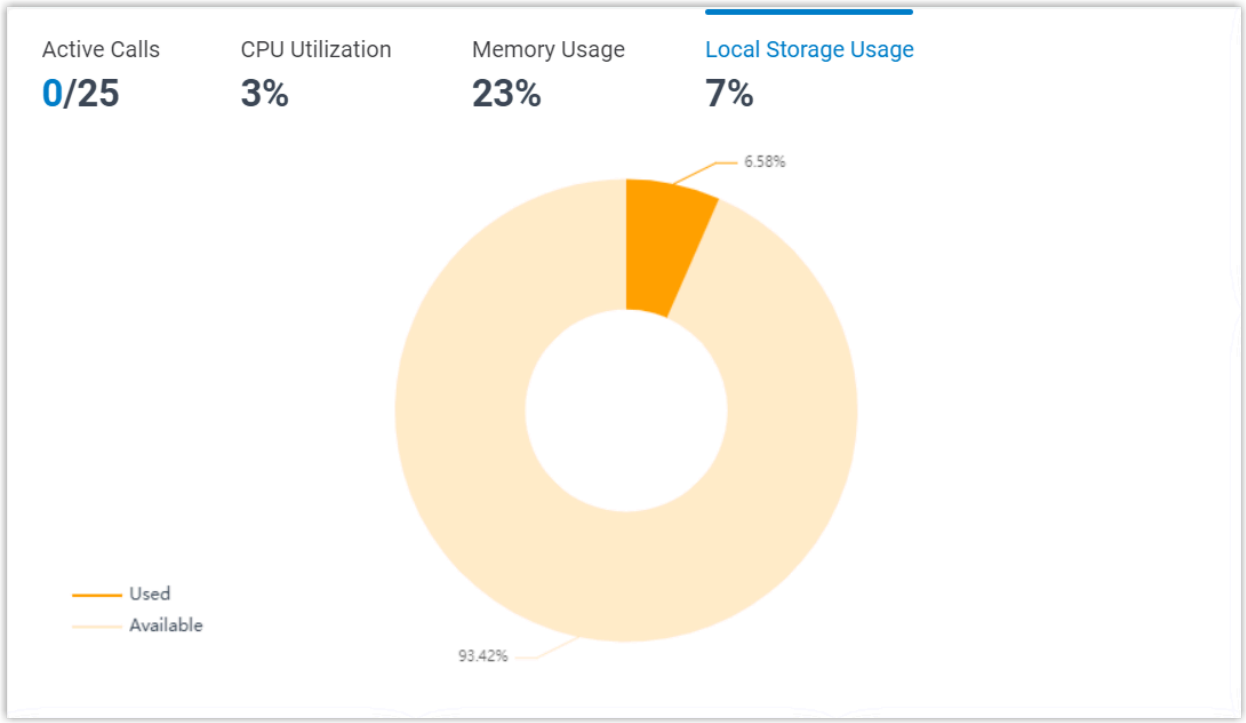
1. System performance
2. System information
3. Plan
4. Add-On
5. Interface status
6. System status
7. Event trend

1. System performance
2. System information
3. Plan
4. System status
5. System status
6. Event trend

System performance

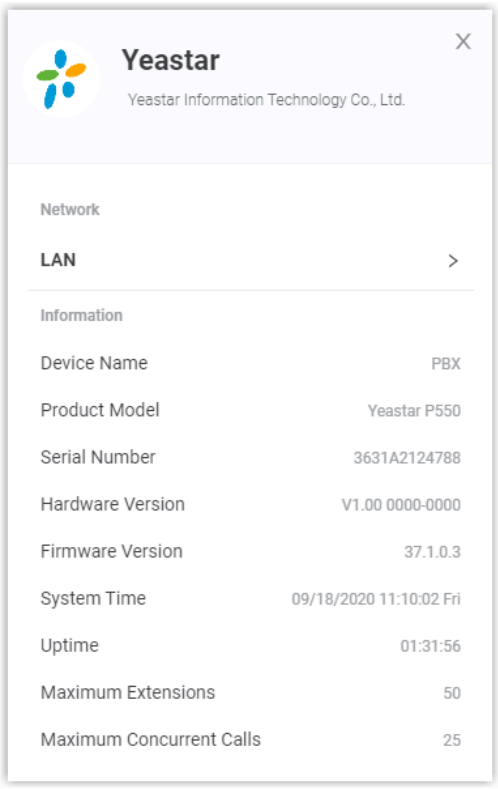
System performance displays the following information:

- **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**: The PBX's local storage usage.



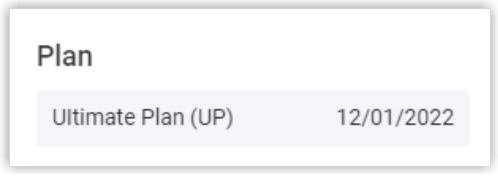
System information

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



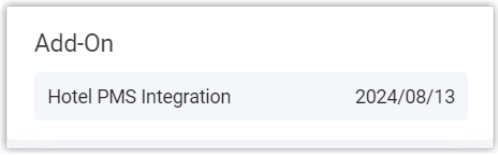
Plan

Plan displays the plan that you subscribe to or try and its expiration date.



Add-On

Add-On displays the additional service that you subscribe to or try and its expiration date.



Interface status

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

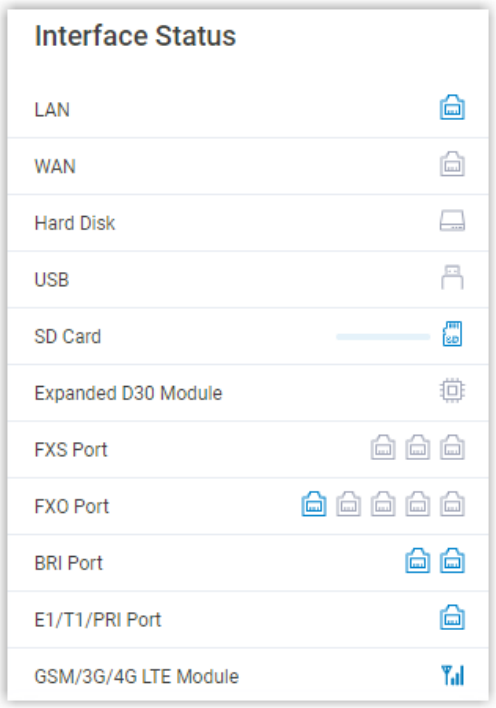


Table 4.

Interface	Description
LAN	• : Connected. • : Disconnected.
WAN	• : Connected. • : Disconnected.
Hard Disk	• : Connected. • : Not inserted. • : Connected, but the hard disk is "Read Only" or encounters format error. • : Connected, but the hard disk is formatting. **Note:** Hard Disk is ONLY supported on P560 and P570.
USB	• : Connected. • : Not inserted.

Table 4. (continued)

Interface	Description
	•  : Connected, but the USB flash drive is "Read Only" or encounters format error. •  : Connected, but the USB flash drive is formatting. **Note:** USB is ONLY supported on P550, P560, and P570.
SD Card	•  : Connected. •  : Not inserted. •  : Connected, but the SD card is "Read Only" or encounters format error. •  : Connected, but the SD card is formatting. **Note:** SD card is ONLY supported on P560 and P570.
Micro SD Card	•  : Connected. •  : Not inserted. •  : Connected, but the Micro SD card is "Read Only" or encounters format error. •  : Connected, but the Micro SD card is formatting. **Note:** Micro SD card is ONLY supported on P520, but it will display as **SD Card** on the web interface.
Expanded D30 Module	•  : Connected. •  : Not connected. •  : Connected, but the D30 module is abnormal. **Note:** D30 module is ONLY supported on P560 and P570.
FXS port	•  : An extension number is assigned to the FXS port.

Table 4. (continued)

Interface	Description
	•  : No extension number is assigned to the FXS port.
FXO port	•  : A PSTN line is connected to the FXO port. •  : No PSTN line is connected to the FXO port. •  : Abnormal. •  : Busy.
BRI port	•  : Available. •  : Unavailable. •  : Abnormal.
E1/T1/PRI port	•  : Available. •  : Unavailable. •  : Abnormal. **Note:** E1/T1/PRI port is ONLY supported on P560 and P570.
GSM/3G/4G LTE module	•  : Abnormal. •  : 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.

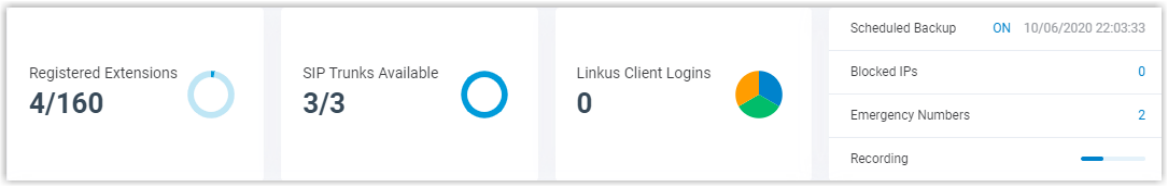
System status

System status displays the following information:

- **Registered Extensions**: The number of registered extensions and created extensions.

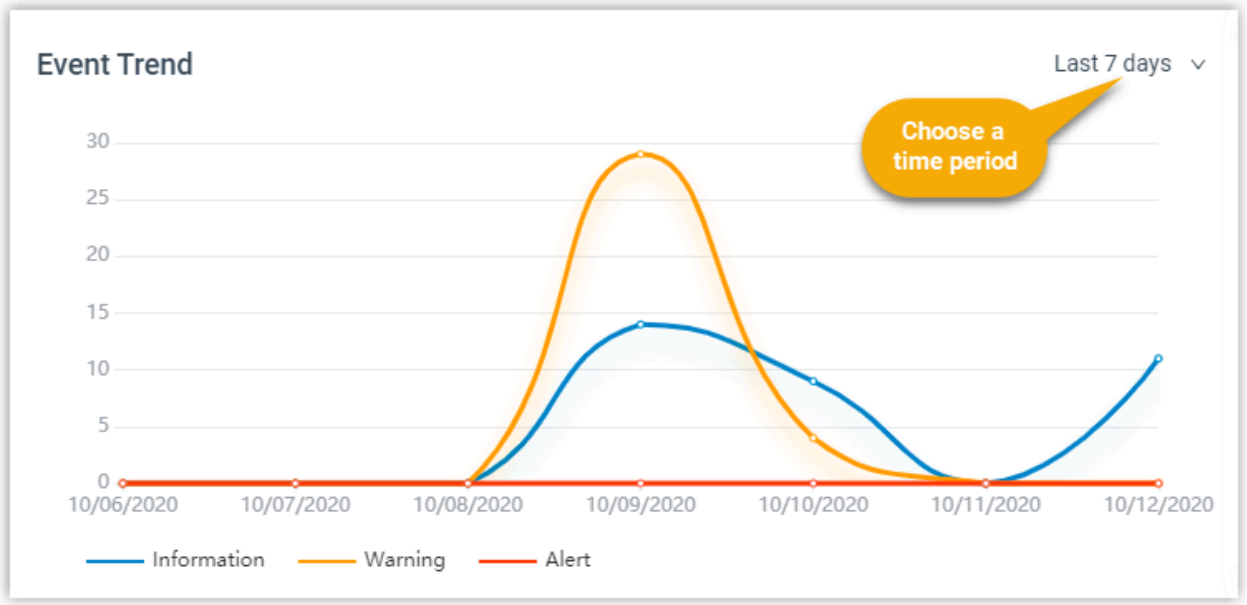
- **SIP Trunks Available**: The number of available trunks and created trunks.
- **Linkus Client Logins**: The number of Linkus clients where users has logged.
- **Scheduled Backup**: Whether scheduled backup feature is enabled or not. If enabled, the system displays the last time when a backup file 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 the following topics:

- Create a SIP Extension
- Set up a SIP Phone
- Set up a Remote SIP Phone via Public IP Address and Port
- Set up a Remote SIP Phone via Yeastar FQDN

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 web 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 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.

- **Organization**: Select one or more organizations to which the extension belongs.

> **Note:**
> This option is available only when you enable the **Organization Management** feature.

- **Job Title**: Enter a job title for the user, which will be displayed on Linkus clients.

4. In the **Language** section, configure language preferences for the extension.
   - **Notification Email Language**: Select language used in system-generated email notifications sent to the extension.

> **Note:**
> - If you select **Follow System**, the email language will follow the settings in **System > Email > Email Templates > Notification Email Language**.
> - This setting only applies to system default emails. It does not affect customized email templates.

   - **System Prompt Language**: Select the language of the system prompts heard by the extension user during a call.

> **Note:**

> The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**).

- **Voicemail Language**: Select the language of voicemail prompts heard by callers when they access the extension's voicemail.

> **Note:**
> - The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**).
> - If the extension's voicemail has set up a custom greeting, the custom greeting will be played to callers instead. In this case, the language setting will be ignored.

5. 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 5.
   > - Concurrent Registration setting only limits the registration number of non-Linkus SIP endpoints. The registration number of Linkus clients is not counted.

6. **Optional:** In the **Permission Configuration** section, assign the extension to extension groups or remove it from assigned groups, and manage user types and permissions within the assigned groups as needed.
7. **Optional:** Click other tabs to configure other settings according to your needs.

8. 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 via Public IP Address and Port and Set up a Remote SIP Phone via Yeastar FQDN.

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 web 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 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.

- **Organization**: Select one or more organizations to which the extension belongs.

  > **Note:**
  > This option is available only when you enable the **Organization Management** feature.

- **Job Title**: Enter a job title for the user, which will be displayed on Linkus clients.

4. In the **Language** section, configure language preferences for the extension.
   - **Notification Email Language**: Select language used in system-generated email notifications sent to the extension.

     > **Note:**
     > - If you select **Follow System**, the email language will follow the settings in **System > Email > Email Templates > Notification Email Language**.
     > - This setting only applies to system default emails. It does not affect customized email templates.

   - **System Prompt Language**: Select the language of the system prompts heard by the extension user during a call.

> **Note:**
> The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**).

- **Voicemail Language**: Select the language of voicemail prompts heard by callers when they access the extension's voicemail.

> **Note:**
> - The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**).
> - If the extension's voicemail has set up a custom greeting, the custom greeting will be played to callers instead. In this case, the language setting will be ignored.

5. 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.
6. **Optional:** In the **Permission Configuration** section, assign the extension to extension groups or remove it from assigned groups, and manage user types and permissions within the assigned groups as needed.
7. **Optional:** Click other tabs to configure other settings according to your needs.
8. 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 web 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.

- **Organization**: Select one or more organizations to which the extensions belong.

> **Note:**
> This option is available only when you enable the **Organization Management** feature.

- **Job Title**: Enter a job title for the extensions, which will be displayed on Linkus clients.

c. In the **Language** section, configure language preferences for the extension.

- **Notification Email Language**: Select language used in system-generated email notifications sent to the extension.

> **Note:**
> - If you select **Follow System**, the email language will follow the settings in **System > Email > Email Templates > Notification Email Language**.
> - This setting only applies to system default emails. It does not affect customized email templates.

- **System Prompt Language**: Select the language of the system prompts heard by the extension user during a call.

> **Note:**
> The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**).

- **Voicemail Language**: Select the language of voicemail prompts heard by callers when they access the extension's voicemail.

> **Note:**
> - The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**).

> ◦ If the extension's voicemail has set up a custom greeting, the custom greeting will be played to callers instead. In this case, the language setting will be ignored.

d. 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 5.
> ◦ 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 via Public IP Address and Port and Set up a Remote SIP Phone via Yeastar FQDN.

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 web 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.

Related information

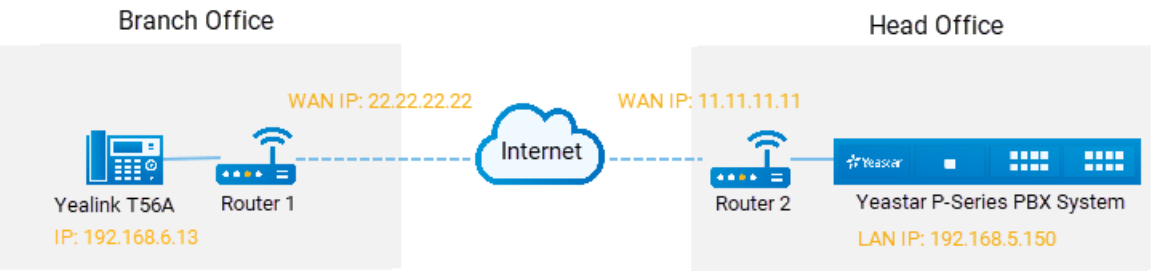
Set up a Remote SIP Phone via Public IP Address and Port
Set up a Remote SIP Phone via Yeastar FQDN

Set up a Remote SIP Phone via Public IP Address and Port

This topic provides a configuration example to help you understand how to register a remote SIP extension on a SIP phone using public IP address and port of the PBX.

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 5.

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 web 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**.

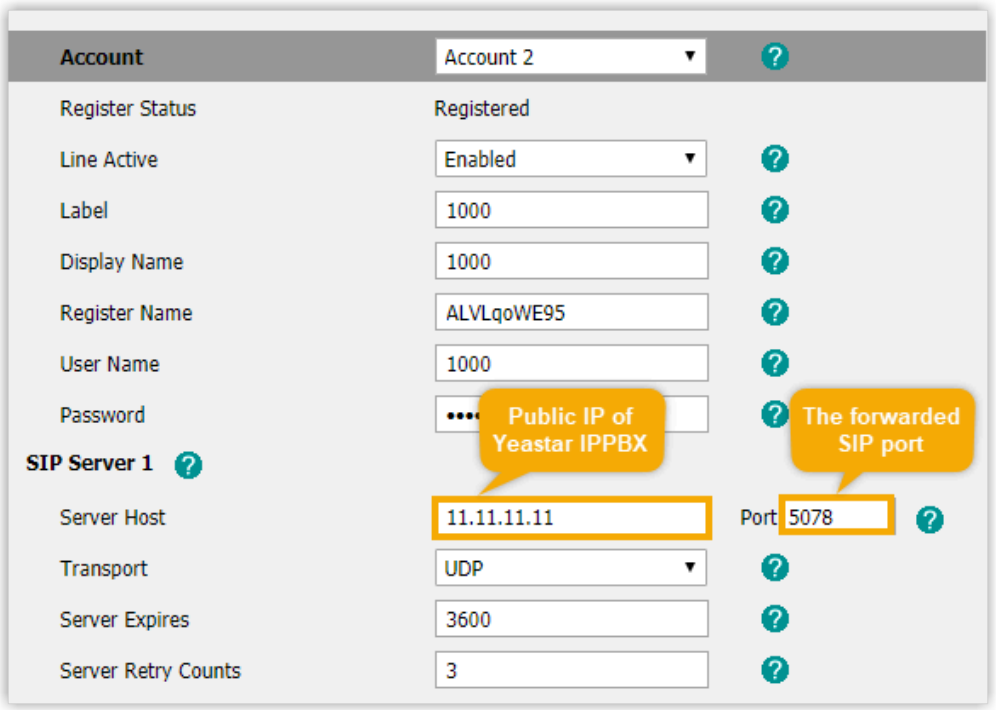
Step3. Set up an extension for remote access

1. On the PBX web 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.



Result

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

Related information

[Set up a Remote SIP Phone via Yeastar FQDN]

Set up a Remote SIP Phone via 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 SIP access, therefore it is more secure and convenient to set up a remote SIP phone using Yeastar FQDN. This topic takes Yealink T53W IP phone as an example to describe how to register a remote SIP phone via Yeastar FQDN.

Prerequisites

- You have subscribed **Enterprise Plan** or **Ultimate Plan**.
- Make sure the following required FQDN settings are ready.
  - The Yeastar FQDN domain name is available.
  - The extension account to be registered can perform remote SIP registration via FQDN.

For detailed configurations, see Configure Network for Remote SIP Access by a Yeastar FQDN.

Procedure

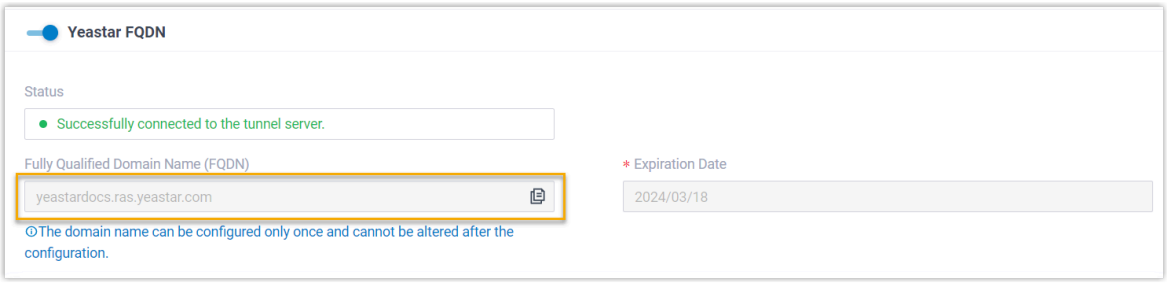
- Step 1. Gather information for extension registration
- Step 2. Register the extension on an IP phone
- Step 3. Confirm the extension's registration status

Step 1. Gather information for extension registration

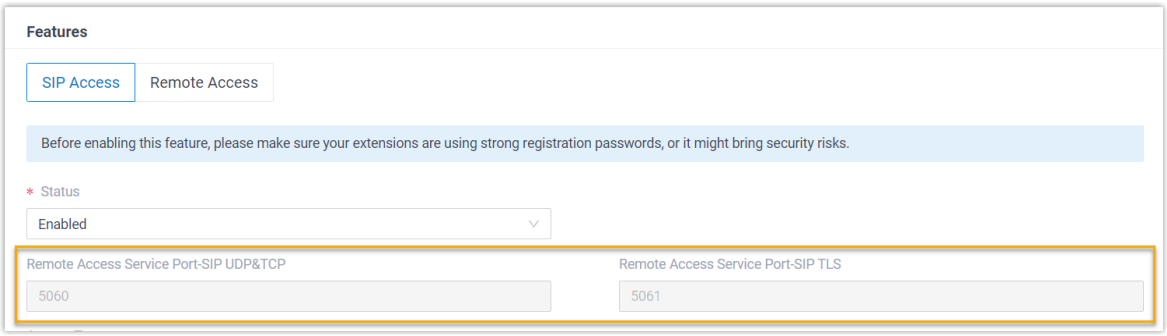
Log in to PBX web portal, and gather the required credentials.

- The FQDN of PBX (Path: **System > Network > Yeastar FQDN**)

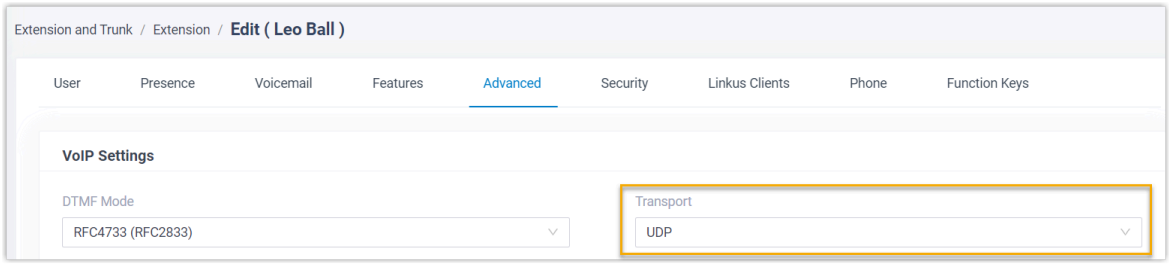
  In this example, the PBX FQDN is `yeastardocs.ras.yeastar.com`.



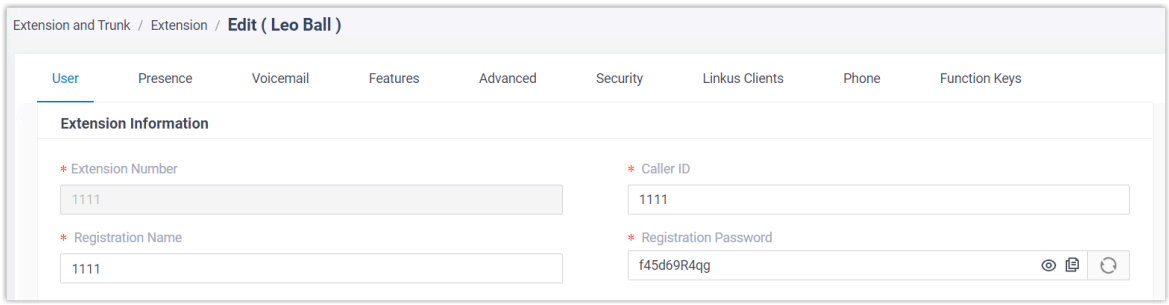
- Remote SIP registration port (Path: **System > Network > Yeastar FQDN > Features > SIP Access**)



- Transport protocol (Path: **Extension and Trunk > Extension > Advanced > Transport**)

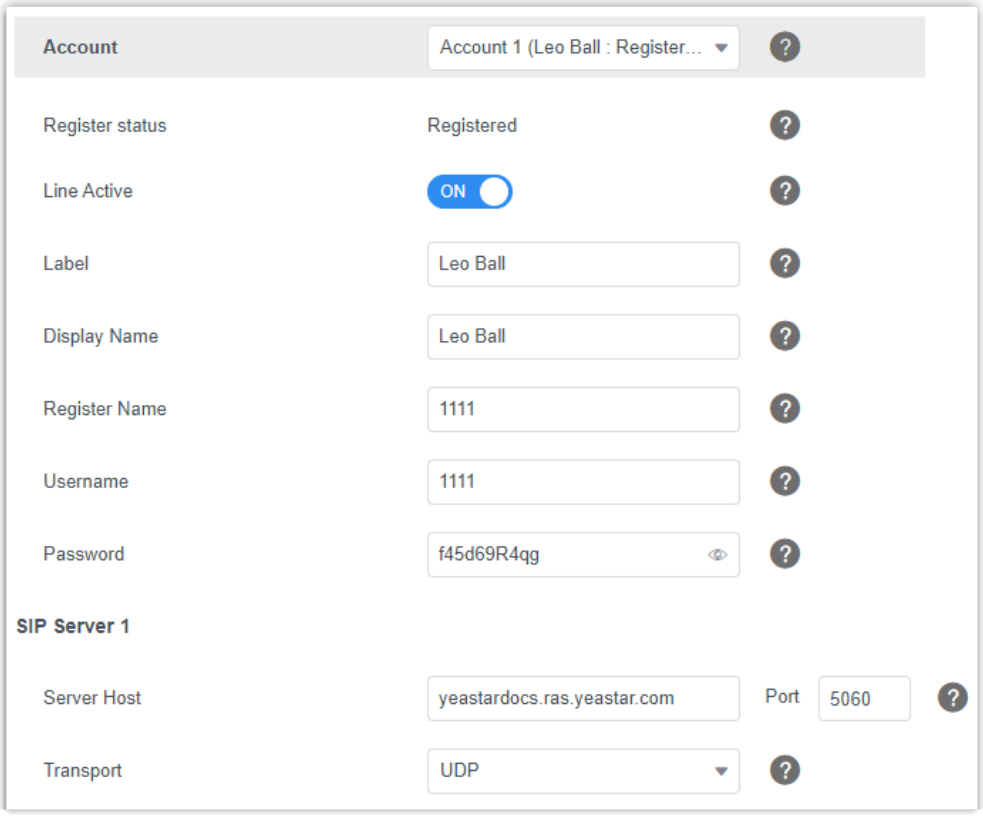


- Extension information (Path: **Extension and Trunk > Extension > User**)
  - Extension number
  - Registration name
  - Registration password



Step 2. Register the extension on an IP phone

1. Log in to phone web interface, go to **Account > Register**.
2. From the **Account** drop-down list, select an available account.
3. Set **Line Active** to **ON**.
4. Fill in the required information to register the SIP extension.



- **Label**: Specify the name to be displayed on the LCD screen of IP phone.
- **Display Name**: Specify the display name of the account when sending a call.
- **Register Name**: Enter the registration name of the extension.
- **Username**: Enter the extension number of the extension.
- **Password**: Enter the registration password of the extension.
- **Server Host**: Enter the FQDN of the PBX.
- **Port**: Enter the remote SIP registration port.
- **Transport**: Select the same transport as that of the extension.

5. Click **Confirm**.

Step 3. Confirm the extension's registration status

You can 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 web 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.

Extension Outbound Caller ID

Allow Users to Select Outbound Caller ID (DOD) to Call

By default, the value that you have configured in the From header field for a trunk will be used as outbound caller ID when extension users make outbound calls through the trunk. You can customize outbound caller IDs for extension users based on trunk and allow them to select DOD when making outbound calls.

Requirements and restrictions

Requirements

- The PBX version is 37.16.0.25 or later.
- Customizing outbound caller ID should be supported by the trunk provider.

Restrictions

- Customizing outbound caller ID is only supported on SIP trunk, BRI trunk, and E1/T1/J1 trunk.

Step 1. Set outbound caller IDs for extensions based on a trunk

Set up outbound caller IDs for extensions based on a trunk, so that an associated DOD can be sent out when a user calls out.

1. Log in to PBX web 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**
- **Default DOD Label**

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**
   - **Default DOD Label**
6. Click **Save** and **Apply**.

Step 2. Associate the trunk and extensions with an outbound route

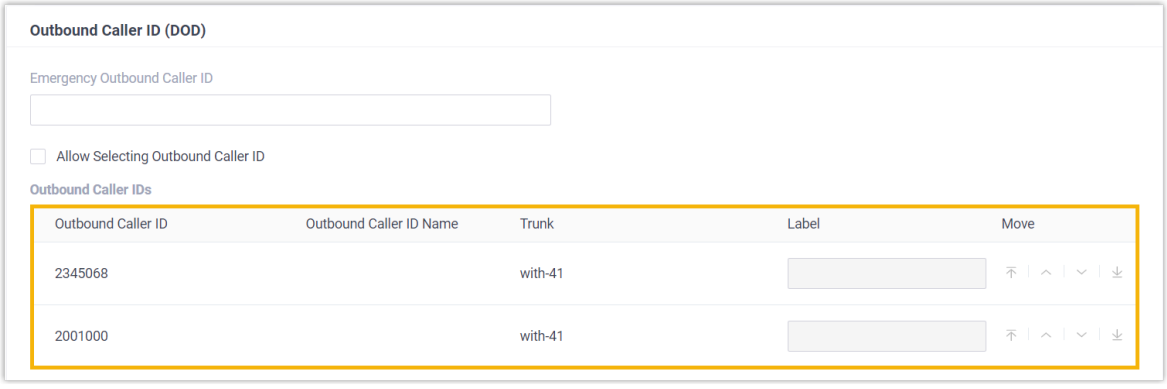
Set up an outbound route to allow extension users to dial out through the trunk that has been configured outbound caller IDs.

1. Go to **Call Control > Outbound Route**, edit the desired outbound route.
2. In the **Trunk** section, select the trunk that has outbound caller IDs configured for extensions.
3. In the **Extension / Extension Group** section, select the extensions that have been associated with the outbound caller IDs.
4. Click **Save** and **Apply**.

Step 3. Grant extensions the permission to select DOD when dialing out

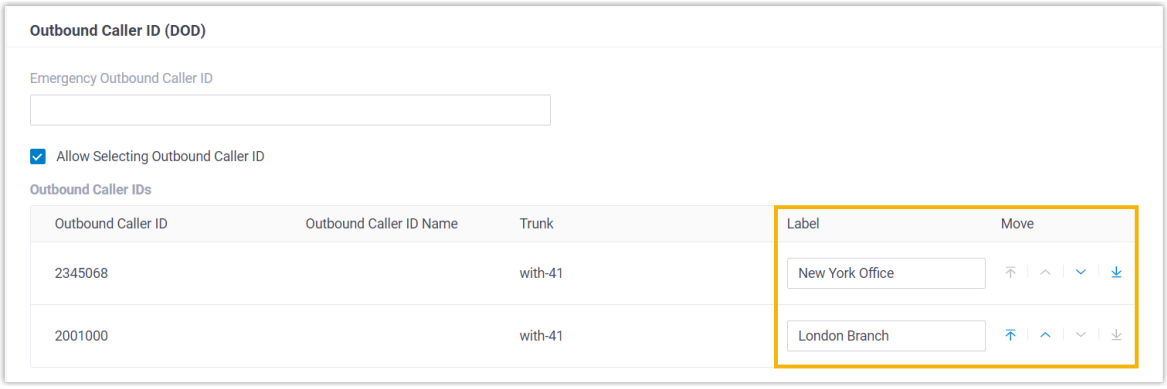
1. Go to **Extension and Trunk > Extension**, edit the desired extension.
2. Scroll down to the **Outbound Caller ID (DOD)** section.

   The outbound caller IDs that have been associated with the extension are displayed on the **Outbound Caller IDs** list.



3. Select the checkbox of **Allow Selecting Outbound Caller ID**.
4. Customize how the DOD will be displayed on the extension's Linkus UC Clients as needed.

> **Note:**
> The extension user can also customize the DOD display on his or her Linkus Desktop / Web Client (Path: **Preferences > User > Outbound Caller ID (DOD)**).



- **Label**: Use the default DOD label or customize a short description to label the DOD number.

  For example, if the label `New York Office` is set for DOD **2345068**, the DOD will appear as 2345068 (New York Office) on the extension user's Linkus UC Clients.
- **Move**: Click ⤒ ^ v ⤓ to adjust the order in which the DODs are displayed on the extension user's Linkus UC Clients.

5. Click **Save** and **Apply**.

Result

When making outbound calls from Linkus UC Clients, the extension user can select a DOD to dial out.

> **Note:**
> To achieve this, extension user must upgrade his or her Linkus UC Clients to the specified version:
>
> - **Linkus Mobile Client**: 5.6.6 or later

- **Linkus Desktop Client**: 1.6.0 or later

For more information, see Select Outbound Caller ID (DOD) to Call (Linkus Mobile Client), Select Outbound Caller ID (DOD) to Call (Linkus Desktop Client), and Select Outbound Caller ID (DOD) to Call (Linkus Web Client).

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 default statuses:

- **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.

You can keep the default extension presence configuration, or customize it as needed. For customization instructions, see Customize Extension Presence.

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 Extension 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 web 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

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.

Setting	Description
Types of incoming calls	• **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	Select a forwarding condition and configure a destination. • **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 registered.
- **Linkus Mobile Client**

- **Linkus Desktop Client (Softphone Only)**
- **Linkus Web Client (Web Client Mode Only)**
- **Linkus Pad Client (SDK)**

> **Note:**
> - This option is ONLY available when Linkus SDK is enabled (Path: **Integrations > Linkus SDK**).
> - To enable users receiving incoming calls through Linkus Pad Client, you need to integrate the Linkus SDK for Android or Linkus SDK for iOS.

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

> **Note:**
> The ring strategy setting does not take effect if the extension is a member of a queue or a ring group. In such cases, when the extension receives incoming calls, all endpoints with the extension registered would ring simultaneously.

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**.

Setting	Description
Ring Timeout	Enter a value or select a value from the drop-down list. **Note:** The valid range is from 5 to 300.

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.

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.

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

Accept calls from Ring Group

By default, the user can receive ring group calls under any presence. You can set whether to receive ring group calls under the specific presence for the user.

Setting	Description
Accept calls from Ring Group	Enable or disable receiving ring group calls under this presence.

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.

Setting	Description
Login	Log in to a queue.

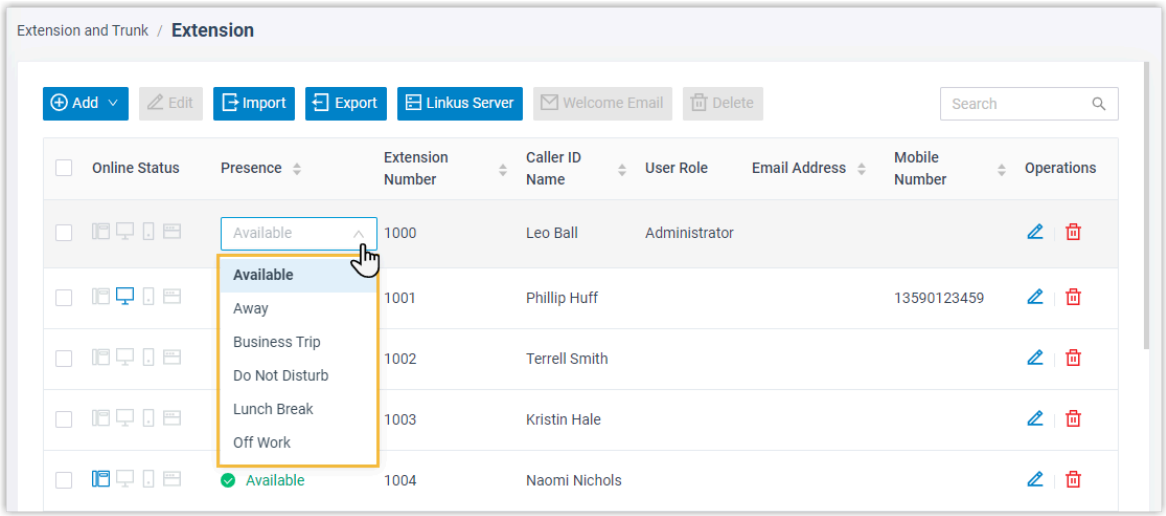
Setting	Description
	Note: The option is available ONLY in **Available** status.
Logout	Log out of a queue.
Pause	Pause receiving queue calls. **Note:** If you have set pause reasons for queue agents, you can select a specific pause reason in the **Pause Reason** drop-down list.
Do Nothing	Retain current status.

Manually Switch Extension Presence

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

Procedure

1. Log in to PBX web 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 Extension Presence Based on Time

Automatically Switch Extension Presence Based on Time

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 for the default time zone on the PBX system (Path: **Call Control > Business Hours and Holidays**), and you want the presence of extensions to be automatically switched according to the following time schedule:

> **Note:**
> This example uses the time settings in the default time zone. You can also customize business hours for an extension individually, based on which the extension will automatically switch its presence. For more information, see Set Business Hours for an Extension.

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 web 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 based on time.

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

> **Note:**
> If someone overrides time condition for the system, the presence status will be switched accordingly.
>
> For example, time condition is overridden to **Business Hours**, the presence status will be force switched to **Available**.

Related information

Overview of Business Hours and Holidays
Manually Switch Extension Presence

Monitor Extension Status by BLF Key

This topic describes how to configure a BLF key for auto-provisioned IP phone on PBX web portal, so as to monitor the call status and DND (Do Not Disturb) presence status of a specific extension.

Prerequisites

The phone is connected to Yeastar P-Series PBX System via Auto Provisioning, and has been assigned an extension.

For more information, see the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)
- Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
- Auto Provision IP Phones Remotely (Provision Link Method)

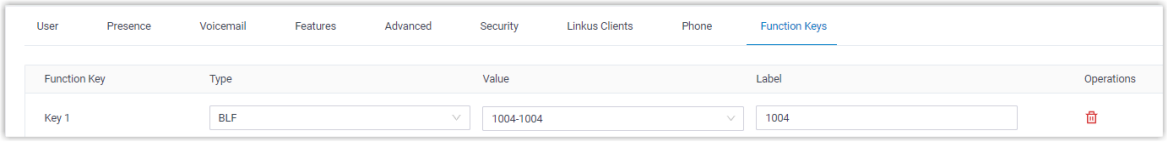
Procedure

- Step 1. Set up a function key for extension monitoring
- Step 2. Apply the configuration to the IP phone

Step 1. Set up a function key for extension monitoring

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the extension that is assigned to the phone.
2. Click the **Function Keys** tab.
3. Configure a function key to monitor the status of an extension.

   The following figure shows a configuration example of monitoring extension 1004.

   - **Type**: Select **BLF**.
   - **Value**: In the drop-down list, select an extension to monitor. In this example, select `1004`.
   - **Label**: Optional. Enter a value, which will be displayed on the phone screen.
4. Click **Save**.

Step 2. Apply the configuration to the IP phone

1. Go to **Auto Provisioning > Phones**, click beside the desired phone.

The system prompts you whether to reprovision the phone.

2. In the pop-up window, click **OK**.

Result

- The LED of the BLF key shows the real-time status of extension 1004:
  - **Solid Green**: The extension is being monitored, and the status is idle.
  - **Solid Red**: The extension is sending a call or is in a call; or the extension presence is DND (Do Not Disturb).

    > **Note:**
    > For Fanvil IP phones that support differentiated DND status indication, the DND status is indicated by a **Solid Yellow** LED light. For more information regarding the supported phone models and firmware versions, contact your Fanvil IP phone provider.

  - **Flashing Red**: The extension is ringing.
  - **LED off**: The extension is not registered, or the extension has been deleted from the PBX system.

- You can press the BLF key on the phone to achieve the followings:
  - Place a call to the monitored extension.
  - Pick up the monitored extension's incoming calls.

    > **Note:**
    > To achieve this, make sure that the Extension Pickup feature code is enabled (Path: **Call Features > Feature Code > Call Pickup > Extension Pickup**).

Related information

Pick up a Call for a Group Member
Pick up a Call for a Specific Extension
Linkus Web Client Guide - Configure Function Keys
Linkus Desktop Client Guide - Configure Function Keys
IP Phone Configuration Guide - Monitor Extension Status by BLF Key on Fanvil IP Phone

Forward Incoming Calls to Another Destination

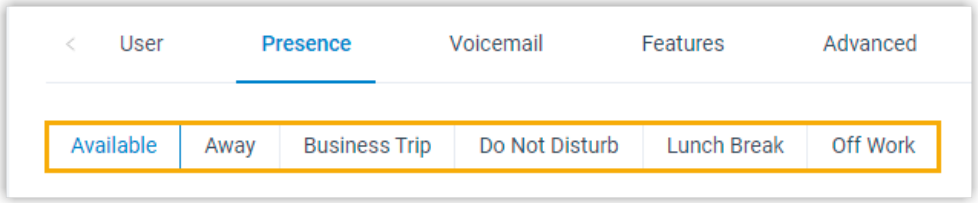
Yeastar P-Series PBX System supports status-based call forwarding, which allows users to forward incoming calls to different destinations based on their presence status. This topic describes how to preconfigure call forwarding rules for extension users on PBX, and how to enable and configure feature code so that extension users can make immediate changes to call forwarding destinations by dialing a feature code when needed.

Set up call forwarding (destination preset)

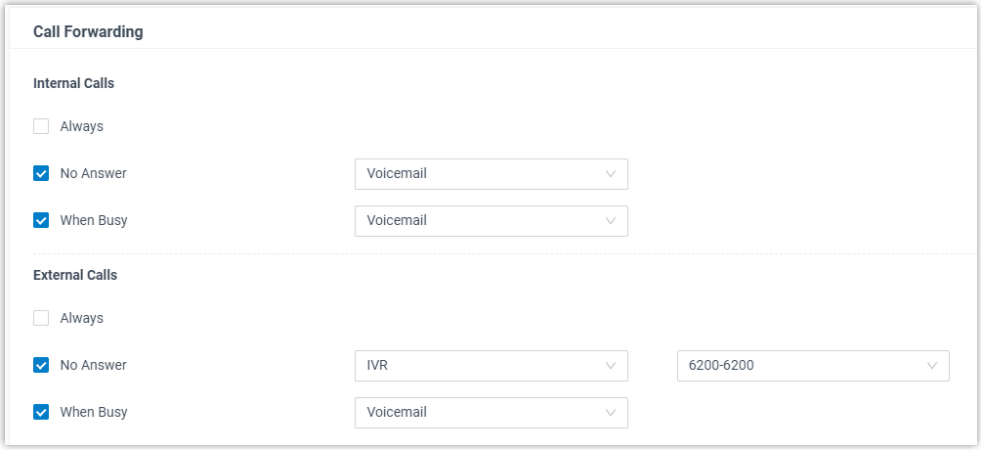
For each presence status of an extension, you can define a different destination to which the incoming calls will be forwarded. Every time the presence status changes, the incoming calls will be forwarded to the corresponding destination.

Procedure

1. Log in to PBX web 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** and **External Calls** section, select a forwarding action and specify a destination.



5. 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.

Enable feature code for call forwarding (destination immediate change)

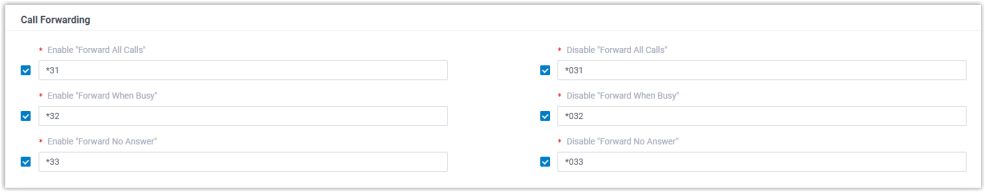
Extension users can change the preset call forwarding destinations on Linkus Web Client. For users with no access to Linkus Web Client, you can enable feature codes for call forwarding, so that these users can dial a feature code on their phones to change the call forwarding destinations.

Restrictions

- Be it internal calls or external calls, all the incoming calls received under the same forwarding type (**Always**, **No Answer**, and **When Busy**) will be routed to the same destination.
- Extension users can only change the call forwarding destination of their current presence status.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. In the **Call Forwarding** section, enable and configure the feature codes for call forwarding as needed.



- **Enable ''Forward All Calls''/''Forward When Busy''/''Forward No Answer''**: Select the checkbox, then configure a feature code.

  Extension users can dial the feature code to forward calls to voicemail or a specific number. For more information, see Call Forwarding Feature Code.
- **Disable ''Forward All Calls''/''Forward When Busy''/''Forward No Answer''**: Select the checkbox, then configure a feature code.

Extension users can dial the feature code to disable automatic call forwarding.

3. Click **Save** and **Apply**.

Result

When an extension user dials the feature code, incoming calls received under the current presence status will be routed to the specified destination.

> **Note:**
> Forwarding type **No Answer** and **When Busy** are not supported under **Do Not Disturb** presence status, which means that even if extension users dial the corresponding feature code, the configuration will not work.

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 web 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
- Email notifications
- Disallow voicemail messages
- Play options of voicemails
- Voicemail greetings
- Voicemail language

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, click  beside the desired extension.
2. Click **Voicemail** tab, turn on the option **Enable Voicemail**.
3. In the **Voicemail PIN Authentication** drop-down list, decide whether a PIN is required when the user accesses voicemail.
   - **Enabled**: This user needs to enter a PIN to access his or her voicemail messages.

     You can set the PIN number in the **Voicemail Access PIN** field.
   - **Disabled**: This user can access his or her voicemail messages directly.
4. In the **New Voicemail Notification** drop-down list, decide whether to send email notifications when the user receives a new voicemail.
   - To disable email notifications, select **Do Not Send Email Notifications**.
   - To enable email notifications, select one of the following options:
     - **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 notification emails only.
5. If you enabled email notifications, configure the following settings as needed:

Setting	Description
After Notification	Decide how to deal with voicemails after notification emails are sent out. • **Mark as Read**: Mark the voicemail message in mailbox as read. • **Delete Voicemail**: Delete the voicemail messages from mailbox. • **Do Nothing**: Keep the voicemail message in mailbox as unread.
Send to	Specify the email address for receiving notification emails. • **User Email**: Send notification emails to the user's email address. • **Custom Email**: Send notification emails to a custom email address. Enter the desired email address in the **Custom Email Address** field.

6. **Optional:** To restrict callers from leaving voicemail messages for the extension, select the checkbox of **Disallow Voicemail Messages**.

   The system will play voicemail greeting to the caller, and then hang up the call directly.
7. **Optional:** Set whether to play the following messages when playing a voicemail.
   - **Play Date and Time**: Enable this option to play date and time when the message is received.
     - **Time Display Format**: If **Play Date and Time** is enabled, you can specify the time format (12-hour or 24-hour) for announcing the message arrival time.
   - **Play Caller ID**: Enable this option to play caller ID information.
   - **Play Message Duration**: Enable this option to play duration of the message.
8. **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.
9. Click **Save** and **Apply**.

Related information

Forward Voicemail Messages to Email
Check Voicemail Messages

Extension Function Keys

Set up Function Keys for Extensions Using a Template

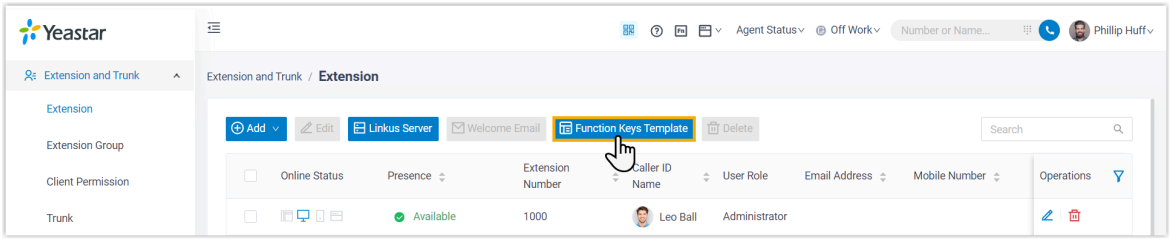
Yeastar P-Series PBX System allows you to create function keys templates and apply them to multiple extensions at once, significantly reducing the time spent in configuring individual extensions. This topic describes how to set up a function keys template and apply the template to extensions.

Requirements

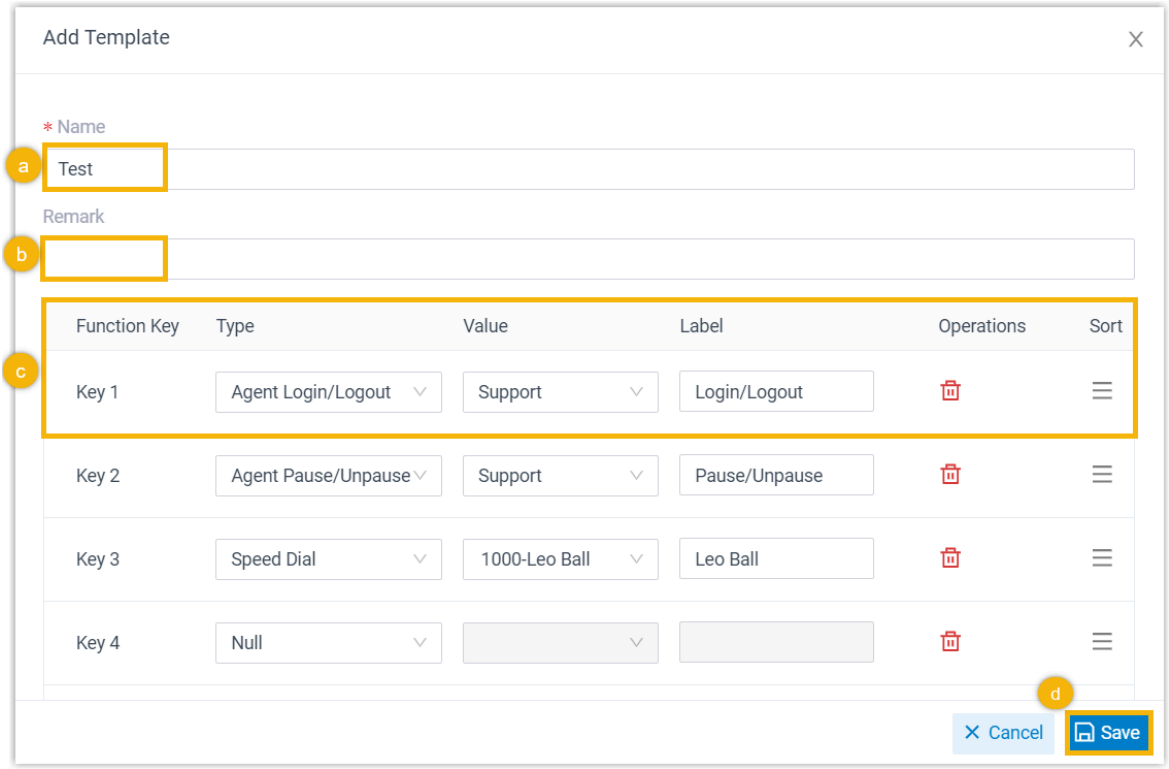
The firmware version of PBX server is 37.16.0.70 or later.

Step 1. Add a function keys template

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click **Function Keys Template**.



3. Click **Add** to add a function key template, then configure the following settings.



a. In the **Name** field, enter a name to help you identify the template.

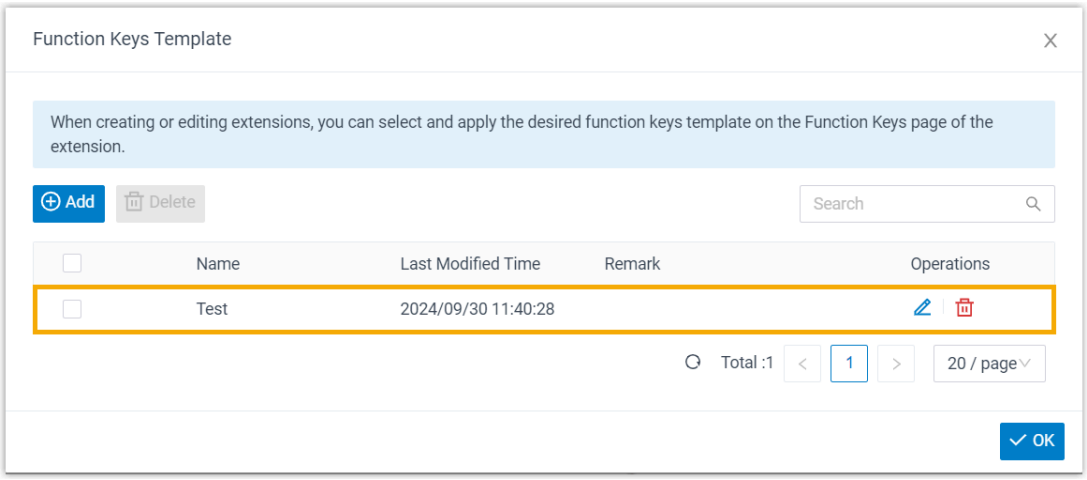
b. **Optional:** In the **Remark** field, enter a short description about the template.

c. In the function keys list, configure function keys according to your needs.

- **Type**: Select a key type.
- **Value**: Configure a desired value based on the key type.
- **Label**: Optional. Enter a value to help extension users identify the function key.

d. Click **Save**.

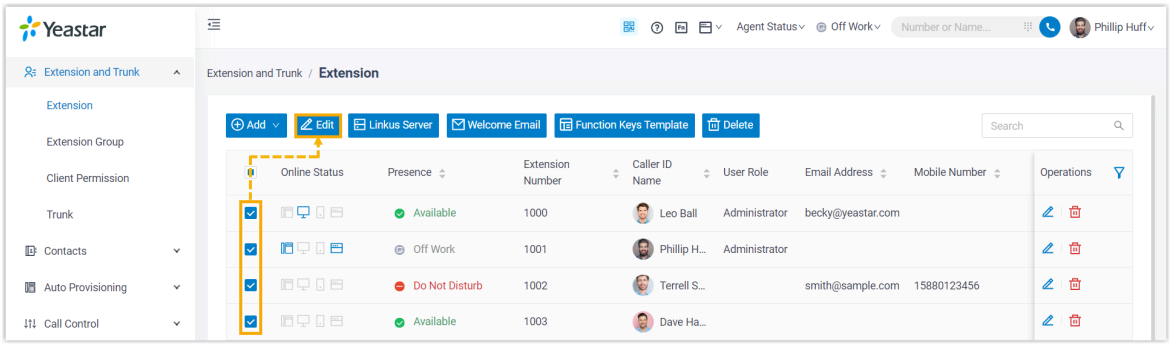
The function key template is created and displayed on the list.



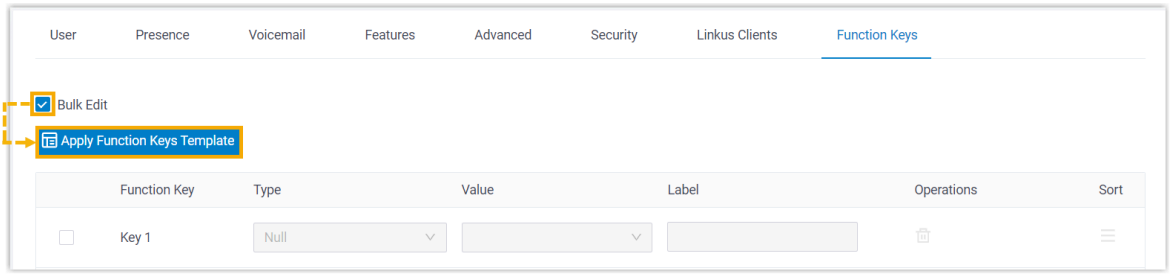
4. Click **OK**.

Step 2. Apply the function keys template to extensions

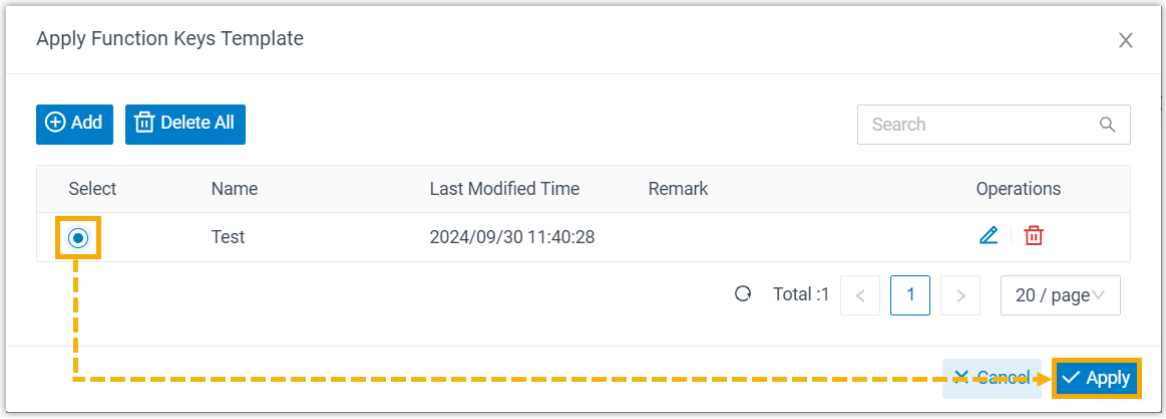
1. On the extension list, select the checkboxes of the desired extensions, then click **Edit**.



2. Under **Function Keys** tab, select the checkbox of **Bulk Edit**, then click **Apply Function Keys Template**.



3. In the pop-up window, select the function keys template, then click **Apply**.



4. Click **Save**.

Result

The function keys are applied to the selected extensions' **Linkus Desktop Client** and **Linkus Web Client**.

Note:

- If the extensions have been registered with IP phones via Auto Provisioning, you need to reprovision the phones so as to apply the changes on IP phones.

  For more information, see Auto Provision Function Keys for Phones.
- If the selected function keys template is changed or deleted, the previously applied function keys of the extensions will not be affected.

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 web 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.

> **Note:**
> If the extension user is a ring group member, and Record Missed Calls feature is enabled for the ring group, they system will also send notification emails when the user has missed calls from the ring group.

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 web 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.

Customize Music on Hold for an Extension

This topic describes how to customize music on hold for a specific extension on Yeastar P-Series PBX System, including the music played when an extension user holds a call and when a call is forwarded to another destination.

By default, extensions' music on hold follows the system's global prompt settings (set on **PBX Settings > Voice Prompt > Prompt Preferences > Music on Hold / Music on Hold for Call Forwarding**). You can refer to this topic to customize the prompts for individual extensions to provide a more personalized experience.

Requirements

The firmware version of PBX server is 37.15.0.22 or later.

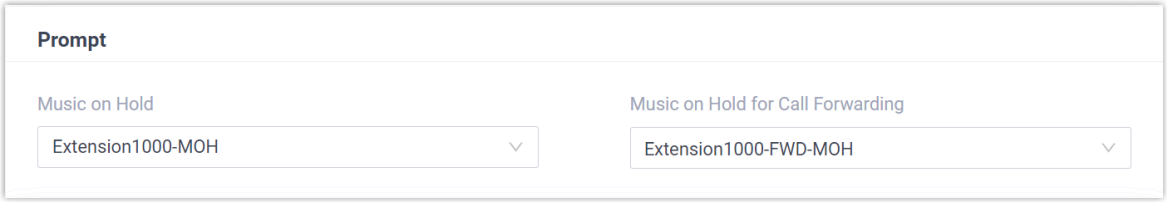
Prerequisites

You have prepared and uploaded music for the following scenarios:

- **Music on Hold**: The music played to the other party when the extension user holds a call.
- **Music on Hold for Call Forwarding**: The music played to the caller when the call is forwarded to another destination.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click beside the desired extension, then go to **Features > Prompt**.
3. In the drop-down list of the music on hold settings, select the desired music that you have uploaded.



4. Click **Save** and **Apply**.

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

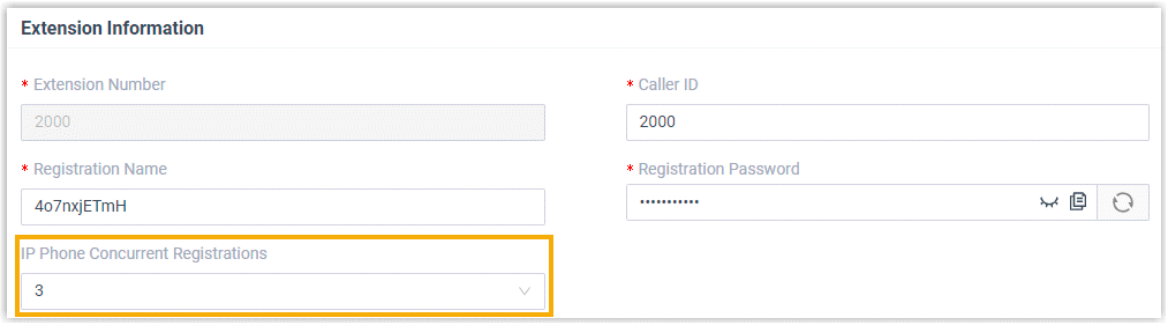
For employees who work flexibly anywhere, they can register their extensions on multiple SIP endpoints, such as an IP phone in their office, a softphone on computer, or a SIP client on mobile phone. In this way, an incoming call can ring all endpoints at the same time, and users can handle calls at anywhere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

Procedure

1. Log in to PBX web 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 5.
- Concurrent Registration setting only limits the registration number of non-Linkus SIP endpoints. The registration number of Linkus clients is not counted.



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 Business Hours for an Extension

This topic describes how to configure time zone and business hours for an extension, ensuring employees in different time zones can efficiently manage calls based on their local time.

Requirements

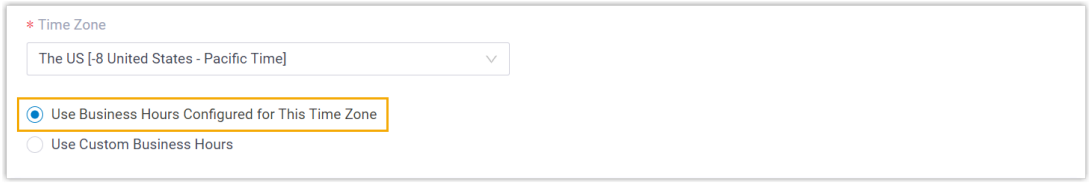
The firmware of Yeastar P-Series PBX System is 37.18.0.59 or later.

Prerequisites

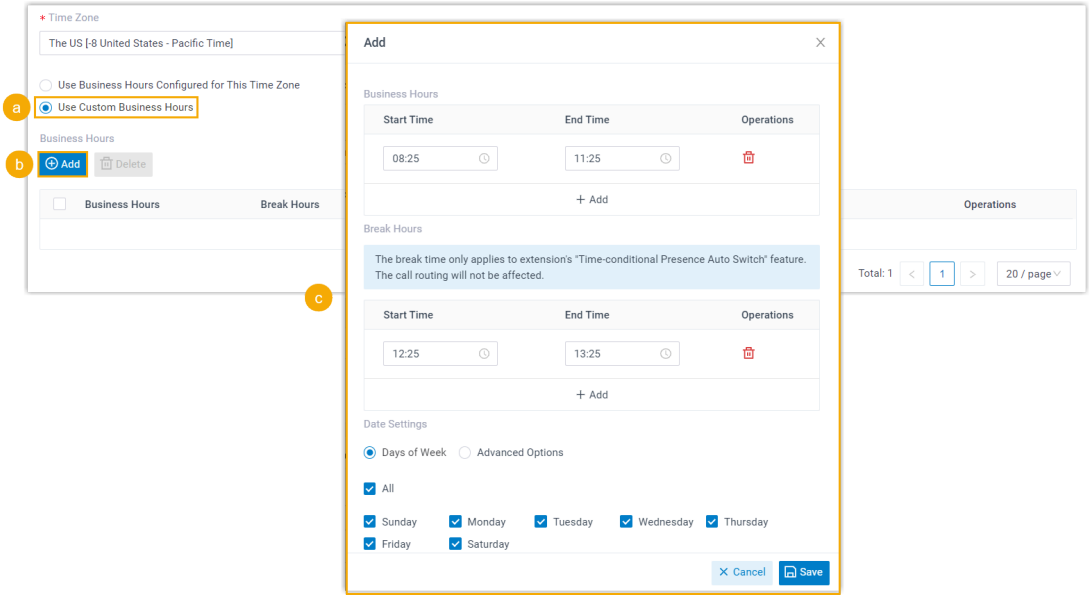
You have configured time zones and business hours for the system (Path: **Call Control > Business Hours and Holidays**).

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click beside the desired extension.
3. In the **Features** tab, scroll down to the **Business Hours** section.
4. In the **Time Zone** drop-down list, select a desired time zone for the extension.
5. Configure business hours for the extension according to your need.
   - To directly use the business hours defined in the selected time zone, select **Use Business Hours Configured for This Time Zone**.



   - To use custom business hours, do as follows:



a. Select **Use Custom Business Hours**.
b. In the **Business hours** section, click **Add**.
c. In the pop-up window, complete the time settings, then click **Save**.
   - **Business Hours**: Add and specify the time when the extension user is available to receive and make calls.
   - **Break Hours**: Add and specify rest breaks during the working days.
   - **Date Settings**: Select working days for the extension.

Option	Description
Days of Week	Use days of the week as date conditions for the extension's business hours.
Advanced Options	Flexibly configure business hours with a combination of week, month, and date.

6. Click **Save** and **Apply**.

Results

- The time displayed for the extension (such as emails, voicemails, etc.) will follow the time of the selected time zone.
- The business hours set for the extension apply when the extension automatically switches presence based on business hours and holidays.

> **Note:**
> The holiday follows the corresponding time settings in the selected time zone.

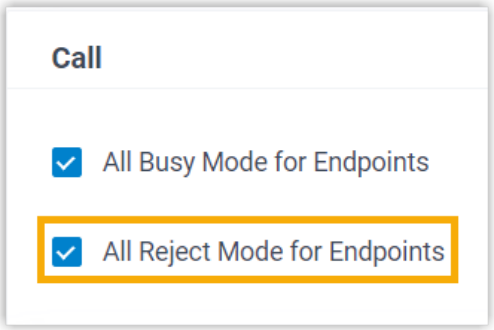
- If you customize business hours for extensions, the extension users can modify the business hours by their own on Linkus Web Client and Desktop Client (Path: **Preferences > Features > Business Hours**).

Stop Rejected Calls from Ringing Other Endpoints

If a user's extension has been registered on multiple endpoints, when the user rejects an incoming call on one of the endpoints, the call keeps ringing all the other endpoints. In this case, you can set up the extension to stop rejected calls from ringing other endpoints.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
2. Click the **Features** tab.
3. In the **Call** section, select the checkbox of **All Reject Mode for Endpoints**.



4. Click **Save**.

Result

When the extension user rejects an incoming call on an endpoint, the other endpoints will stop ringing. The call will be routed to the extension's **When Busy** destination (Path: **Extension and Trunk > Extension > Presence > Call Forwarding**).

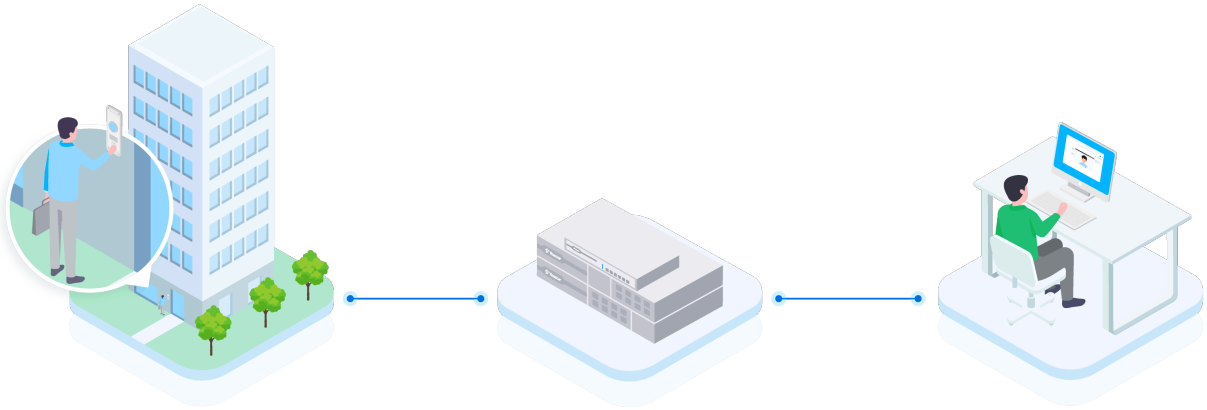
Enable Video Preview of Intercom Calls for Extensions

If you integrate video intercom system with Yeastar P-Series PBX System, you can enable video preview of intercom calls for the extension registered on the door station. In this way, when receiving an incoming call from the door station, users who have their extensions registered as the indoor station can preview the visitor's video on their Linkus UC clients while ringing, and control the opening of the door.

Scenario

A video intercom system contains a door station and an indoor station. If you integrate video intercom system with Yeastar P-Series PBX System, you can make the door station a regular PBX extension for making calls by registering an extension on it, and Linkus UC clients can work as the indoor station.

When visitors press the door station to ring the bell, the door station sends the doorbell (namely a call) to the indoor station. Users can preview the video on Linkus client while ringing, and decide whether to open the door for visitors.



Methods of previewing videos

Yeastar P-Series PBX System supports the following two methods of previewing videos:

- **Video Preview**: This method requires action from callee. When receiving an incoming call from door station (with video preview enabled on the extension), the callee can click the preview button on the Linkus client to preview the video while ringing.
- **Auto Preview**: This method does NOT require action from callee. When receiving an incoming call from door station (with auto preview enabled on the extension), the callee's Linkus client will automatically show the video while ringing.

Requirements and restrictions

Before you begin, read through the requirements and restrictions for the feature:

Requirements

- **PBX Version**: 37.10.0.30 or later
- **PBX Plan**: Ultimate Plan

Restrictions

- **Supported Door Station**: Fanvil

Note:

> Fanvil door stations have been tested and proven to interoperate with Yeastar P-Series PBX System. For other door stations, please contact Yeastar.

- **Supported Indoor Station**: Linkus UC Clients

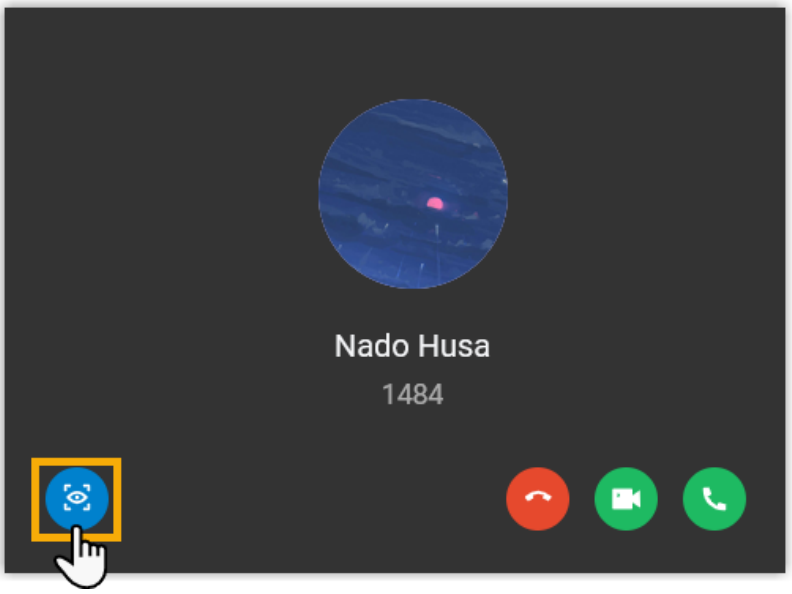
  Take note that the supported video preview methods vary depending on Linkus clients. For more information, see the following table:

	Video Preview	Auto Preview
Linkus Mobile Client (iOS)	×	×
Linkus Mobile Client (Android)	√	√
Linkus Desktop Client (Windows)	√	× (Coming Soon)
Linkus Desktop Client (Mac)	√	× (Coming Soon)
Linkus Web Client	√	√

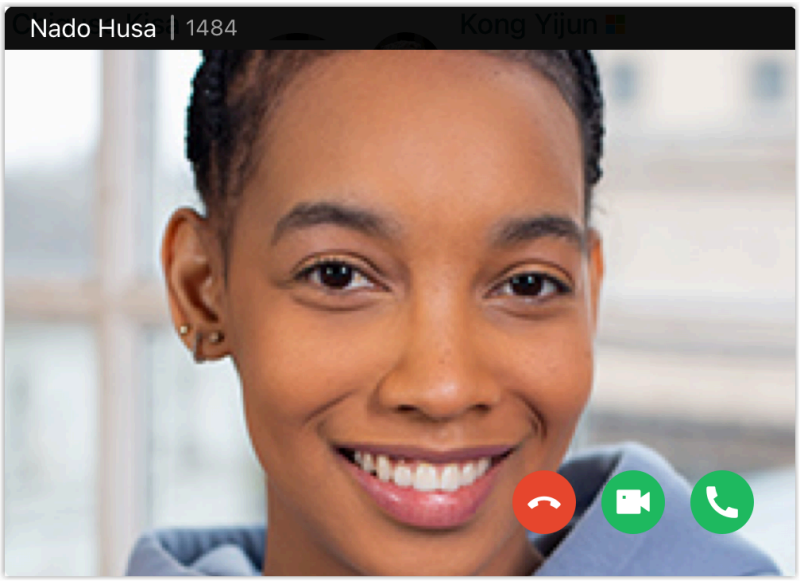
> **Note:**
> - If **Linkus Web Client** is set up to work with 'Yeastar Linkus for Google', the version of the Chrome extension must be **4.2.1** or later.
> - The version of **Linkus Android Client** must be **5.3.12** or later.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the extension for door station.
2. Click **Features** tab.
3. In the **Door Phone Application** section, set up the video preview feature:
   - **Video Preview**: If enabled, when receiving an incoming call from door station with the extension registered, the callee can click  on his or her Linkus client to preview the video while ringing.



- **Auto Preview**: If enabled, when receiving an incoming call from door station with the extension registered, the callee's Linkus client will automatically show the video while ringing.



4. Click **Save** and **Apply**.

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 6.

Setting	Description
DTMF Mode	Set the mode for sending DTMF tones. • **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	Set the transport protocol. • **UDP** • **TCP** • **TLS** **Note:** If you change the transport protocol, you must re-register the extension.
Qualify	Enable this option to send SIP OPTION packet to SIP device to check if the device is up.
T.38 Support	Enable or disable T.38 fax for the extension. **Note:** Enabling T.38 will add performance cost. We recommend that you disable T.38.
NAT	Enable this option when the PBX uses a public IP address. The feature is enabled by default.

Table 6. (continued)

Setting	Description
	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.
SRTP	Enable SRTP for voice encryption.

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 7.

Setting	Description
DTMF Mode	Set the mode for sending DTMF tones. • **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	Set the transport protocol. • **UDP** • **TCP** • **TLS** **Note:**

Table 7. (continued)

Setting	Description
	If you change the transport protocol, you must re-register the extension.
Qualify	Enable this option to send SIP OPTION packet to SIP device to check if the device is up.
T.38 Support	Enable or disable T.38 fax for the extension. **Note:** Enabling T.38 will add performance cost. We recommend that you disable T.38.
NAT	Enable this option when the PBX uses a public IP address. The feature is enabled by default. **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.
SRTP	Enable SRTP for voice encryption.

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 8.

Setting	Description
Hotline	Turn on the option to enable hotline feature.
Hotline Number	Enter the hotline number. **Note:** Only numbers, space, and `()` `.` `-` `+` `*` `#` are allowed.
Delay Dial (s)	Enter the waiting time (in seconds) before automatically dialing out the hotline number. **Note:** Only numbers are allowed.

Flash Detection

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

Table 9.

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 10.

Setting	Description
RX Volume	Set the volume from the analog phone to the PBX's FXS port. The default value is 40%. To change the value, select a value from the drop-down list. **Valid values**: 5%, 10%, 20%, 40%, 60%, 80%, 100%, 150%, Custom **Note:** If you choose **Custom**, you must go to **RX Gain (db)** field to enter an integer between -30 and 12.
TX Volume	Set the volume from the PBX's FXS port to the analog phone. The default value is 40%. To change the value, select a value from the drop-down list. **Valid values**: 5%, 10%, 20%, 40%, 60%, 80%, 100%, 150%, Custom **Note:** If you choose **Custom**, you must go to **TX Gain (db)** field to enter an integer between -30 and 12.

Options

Table 11.

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.

> **Note:**
> These restrictions don't apply to emergency calls. If you want to set up emergency calling, see Emergency Calling Overview.

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 Dialaing Protection**. For more information, see Block Outbound International Calls.

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.

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 Route Permission

Specify the outbound routes that an extension is allowed to use.

> **Note:**
> If this extension belongs to an organization or an extension group that has permission to use a specific outbound route, then you can't change the extension's permission to the outbound route here.

Login Security

Yeastar P-Series PBX System provides the following security options to protect extension user's account.

Two-Factor Authentication

Yeastar P-Series PBX System supports Two-factor Authentication (2FA) for extension users to protect their accounts by requiring an additional authentication code for login.

- To make 2FA mandatory for all extensions, see Enforce Two-factor Authentication for All Extension Users.

> **Note:**
> You cannot enable 2FA for a specific extension. But if a user has configured 2FA but failed to login via 2FA (e.g. unable to receive authentication code via email), you can disable 2FA for the specific extension individually (Path: **Extension and Trunk > Extension > Security > Login Security > Two-Factor Authentication**), so that the user can directly log in with the username and password.

- For more information about how users can configure 2FA, see Enable 2FA on Linkus Web Client and Enable 2FA on Linkus Desktop Client.

User must change password periodically

As a super administrator, you can set whether to force extension users to change password periodically, thus enhancing extension account security.

For more information, see Set up Periodic Password Changes for an Extension.

Restrict Outbound Calls for an Extension

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 web 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

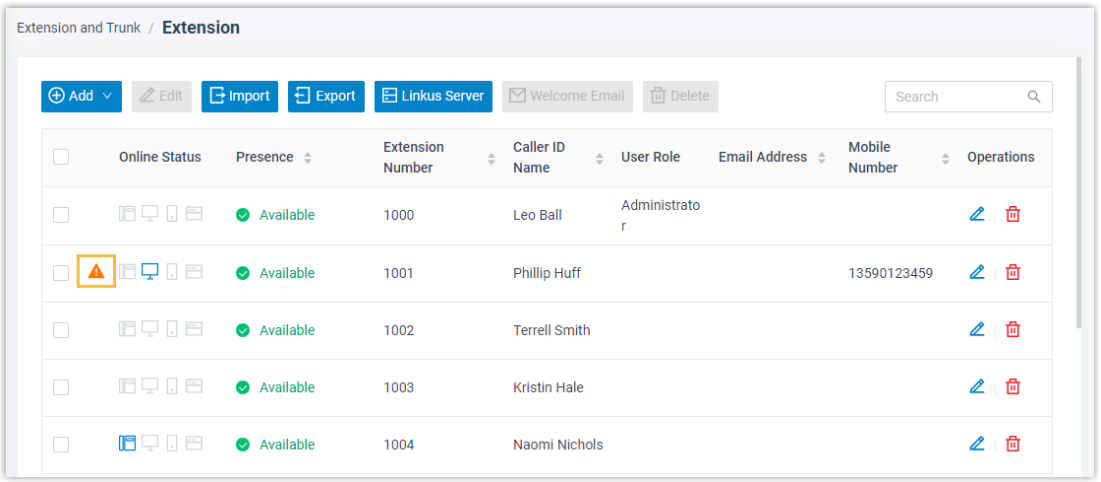
- Users cannot make outbound calls even if the extensions are selected in outbound routes.

> **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.



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 web 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

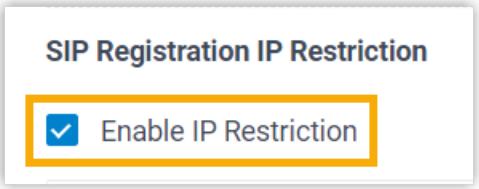
This topic describes how to allow devices with a specific IP address or in a specific IP section to register extensions on Yeastar P-Series PBX System.

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 web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
2. Click **Security** tab.
3. In the **SIP Registration IP Restriction** 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 the business hours of a specific time zone.

Prerequisites

- You have set business hours for a specific time zone.
- You have assigned the desired time zone to the extension (Path: **Extension and Trunk > Extension > Features > Business Hours**).

Procedure

1. Log in to PBX web 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 defined in the time zone of the extension.

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 web 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 web 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.

4. Click **Save** and **Apply**.

Result

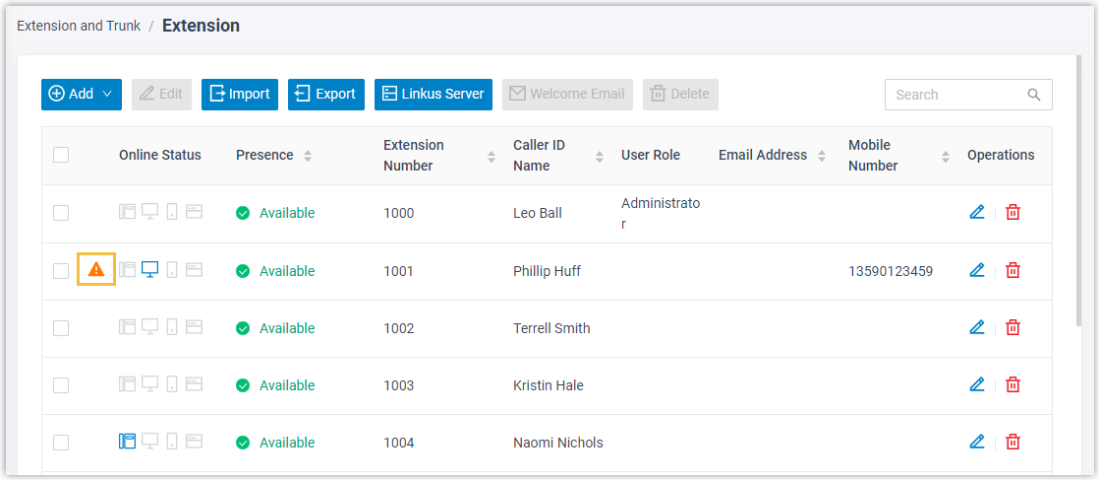
If an extension has exceeded the outbound call frequency restriction, the following things would happen.

- 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.



- The system sends a notification to inform the notification contacts of an Outbound Call Frequency Exceeded event.

Set up Periodic Password Changes for an Extension

Passwords that are kept unchanged for a prolonged period might lead information exploit. Super administrator can set whether to force extension users to change their passwords periodically, thus ensuring account security.

Requirements

The version of PBX server is 37.18.0.102 or later.

Procedure

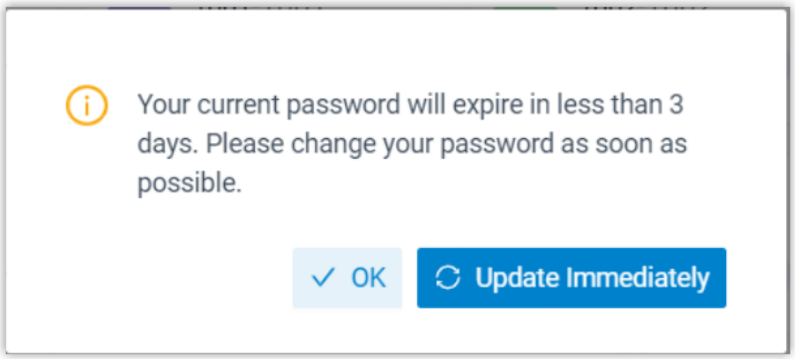
1. Log in to PBX administrator portal with super administrator account, go to **Extension and Trunk > Extension**.
2. Click to edit the desired extension.
3. Under **Security** tab, scroll down to **Login Security**, then configure the following settings.
   a. Select the checkbox of **User must change password periodically**.
   b. In the **Password Change Frequency (Day)** filed, set the password validity period in days.

   The valid value is 1-365, with a default value 30 indicating that the extension user have to change the password every 30 days.
4. Click **Save**.

Result

Extension users will receive reminders via different methods **3 days** and **1 day** before the passwords expire. After expiration, they are unable to log in.

- If extension users have set an email address to receive PBX notifications, the system will send a email **Password expiration reminder** to notify the users.
- When extension users log in to Linkus UC Clients, a pop-up window will prompt them that the password is about to expire and needs to be updated.



Note:
To achieve this extra login security, extension users must upgrade their Linkus UC Clients to the specified version:

- Linkus Desktop Client: Version 1.11.7 or later

- Linkus Mobile Client:
  - Linkus iOS client: 5.13.6 or later
  - Linkus Android client: 5.13.8 or later

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 web 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 web 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 web 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 web 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 web 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 web 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.

Related information

Import and Export -FAQ

Delete Extensions

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

Delete an extension

1. Log in to PBX web 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 web 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**.

Extension Visibility Permission

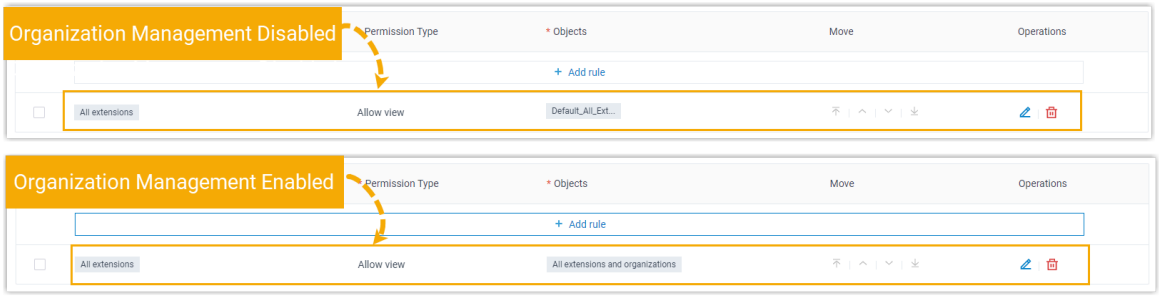
Set up Extension Visibility

By default, all the users can view all departments or the default extension group on Linkus clients, depending on whether you have enabled the organization management feature. To restrict users from viewing specific extensions, departments, or extension groups, you can set up extension visibility as the instructions provided in this topic.

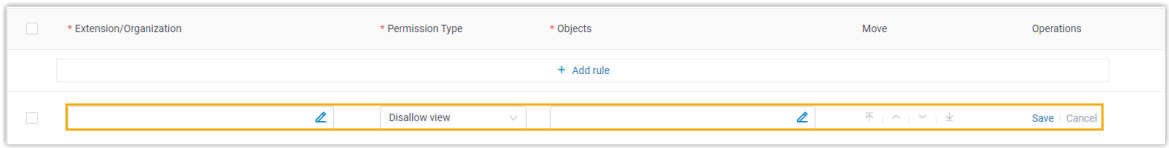
Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Extension Visibility**.

   The default extension visibility rule is displayed.



2. Click **Add rule** to create an extension visibility rule.
3. Set up the rule.



   a. Select desired members and option from the drop-down lists.

Item	Description
Extension/Extension Group/Organization	Click  to select the desired members for which you want to grant or restrict the viewing permission. • **All extensions** • **Specific extensions and extension groups/departments**
Permission Type	Select an option from the drop-down list to define the permission.

Item	Description
	• **Allow view**: Allow to view the extensions, extension groups, or departments, which are selected in the **Objects**. • **Disallow view**: Disallow to view the extensions, extension groups, or departments, which are selected in the **Objects**.
Objects	Click to select the desired extensions, extension groups, or departments, which are allowed or disallowed to be viewed. • **All extensions and extension groups/departments** • **Groups that the extension belongs to/Departments that the extension belongs to** • **Selected extensions and groups/departments** • **Specific extensions and extension groups/departments** **Note:** By default, when you select a department, its associated sub-departments are selected. Be careful when selecting departments.

b. Click **Save**.

4. **Optional:** To adjust the rules order, click , , , or .

> **Note:**
> The priority of extension visibility rules is from the top down. When encountering permission conflicts, the permission is subject to the visibility rule with the higher priority.

Result

On Linkus clients, users can view the extensions, extension groups, or departments that are visible to them.

> **Note:**
> Users can NOT make calls to the extensions that they can not view.

Manage Extension Visibility Rules

This topic describes how to edit and delete extension visibility rules.

Edit an extension visibility rule

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Extension Visibility**.
2. Click  beside a desired extension visibility rule.
3. Edit the rule as needed.
4. Click **Save**.

Delete extension visibility rules

> **Note:**
> Be careful when deleting extension visibility rules. If you delete all the extension visibility rules, all the internal calls would fail, as users can NOT make calls to the extensions invisible to them.

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Extension Visibility**.
2. To delete an extension visibility rule, do as follows:
    a. Click  beside a desired rule.
    b. In the pop-up window, click **OK**.
3. To bulk delete extension visibility rules, do as follows:
    a. Select the checkboxes of desired rules, click **Delete**.
    b. In the pop-up window, click **OK**.

Contacts

Contacts Overview

Yeastar Contacts feature allows users to store external contacts outside of your company on PBX, access and call these contacts on endpoints (IP phone and Linkus UC Clients) where their extensions have been registered.

Contacts

Yeastar P-Series PBX System supports two types of contacts:

Personal Contacts

Personal Contacts is exclusive to each extension user, allowing extension users to create and store a number of personal contacts (such as direct customers) on their own Linkus UC Clients.

> **Note:**
> Each user's Personal Contacts is only visible to himself or herself.

For more information, see Add Personal Contacts from Linkus Mobile Client / Desktop Client / Web Client.

Company Contacts

Company Contacts is shared among authorized users, allowing you and the authorized extension users to create and store a number of company-shared contacts (such as company's customers, resellers, or partners) on PBX web portal and Linkus UC Clients.

You can manually add company contacts (add contacts one by one using manual entry or bulk add contacts using a CSV file) or automatically synchronize contacts from third-party system integration (e.g. Database, CRM, Helpdesk, etc.), while the authorized users can add company contacts from their own Linkus UC Clients.

For more information, see the following topics:

- Manually add company contacts from PBX web portal (Add Contacts Using Manual Entry / Import Contacts with CSV)

- Automatically synchronize company contacts from third-party system integration (Microsoft SQL / LDAP Server)
- Add company contacts from Linkus Mobile Client / Desktop Client / Web Client

Phonebook

Phonebook is a value-added service for Company Contacts, allowing for grouping company contacts into organized phonebooks and implement robust control over access to each phonebook.

Types of phonebooks

Yeastar P-Series PBX System supports two types of phonebooks:

- **PBX-native company phonebook**: The phonebooks that store company contacts added from PBX web portal and Linkus UC Clients.

  You can manually create phonebooks to group company contacts. For more information, see Add Phonebooks.
- **Third-party company phonebook**: The phonebooks that store company contacts synchronized from the third-party system integration.

  If you schedule the synchronization of contacts from the integrated system, all the synced contacts will be grouped into a phonebook with a unique identifier, and the phonebook can't be modified or deleted unless you disconnect the integration.

Visibility of phonebooks

By default, phonebook is invisible to extension users, so they are unable to reach out to the external contacts from their IP phones or Linkus UC Clients.

You can assign the view permission of phonebooks to allow specific extension users to connect with external contacts via calls, or assign the management permission to allows for the co-management of phoneboooks.

For more information, see Set up Contact Visibility.

Restrictions

Before you start using the Contacts feature, check against the following tables to fully understand the restrictions.

Number of contacts

The table below shows the maximum number of contacts supported on Yeastar P-Series PBX System.

Type	P520	P550	P560	P570
Personal contacts (per extension)	3,000	3,000	3,000	3,000
Company contacts (total)	20,000	50,000	200,000	500,000
Company phonebooks	50	100	200	500

Available features

Yeastar P-Series PBX System supports multiple types of plans - **Basic Plan**, **Standard Plan**, **Enterprise Plan**, and **Ultimate Plan**. Some features are available across all plans, while others are exclusive to specific plans.

The table below shows the features included in each plan.

Key Feature	Basic Plan / Standard Plan	Enterprise Plan / Ultimate Plan
Group company contacts into phonebooks	×	√
Sync contacts from external sources (CRM, helpdesk, database, etc.)	×	√
Sync contacts across Linkus UC Clients	√	√
Sync contacts on IP phones	√	√
Identify incoming calls	√	√
Route inbound calls by matching phonebooks	×	√

Available operations

Super administrator and the extension users with **Administrator** role assigned or phonebook permission assigned can view and manage company contacts from PBX web portal, Linkus UC Clients, and IP phones.

The table below shows the operations available in each endpoint.

Operation	PBX Web Portal	Linkus UC Clients			IP Phone
		Web Client	Mobile Client	*Desktop Client	
View company contacts	√	√	√	√	√
Add company contacts	√	√	√	√	×
Edit company contacts	√	√	√	√	×
Delete company contacts	√	√	√	√	×
Import company contacts	√	×	×	×	×
Export company contacts	√	×	×	×	×

PBX-native Contacts

Add and Manage Company Contacts

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

Background information

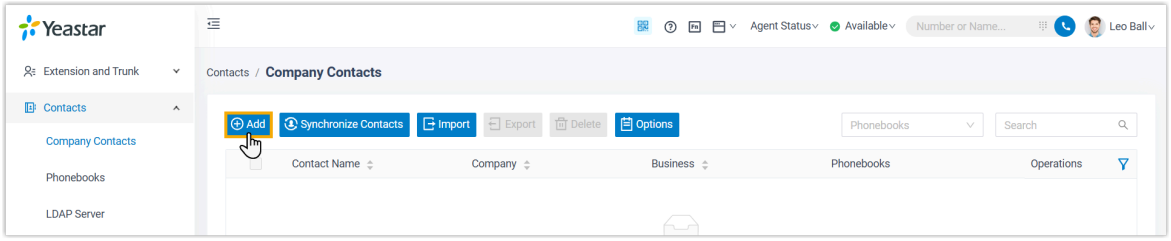
By default, only super administrator and extension users with **Administrator** role assigned can add and manage company contacts. Any other extension users can neither manage nor view any company contacts.

This topic introduces how administrators can add and manage company contacts from PBX web portal. For ordinary extension users, you can grant the view or management permission of company contacts to desired extension users, so as to allow them to access and manage company contacts from their own Linkus UC Clients and IP phones.

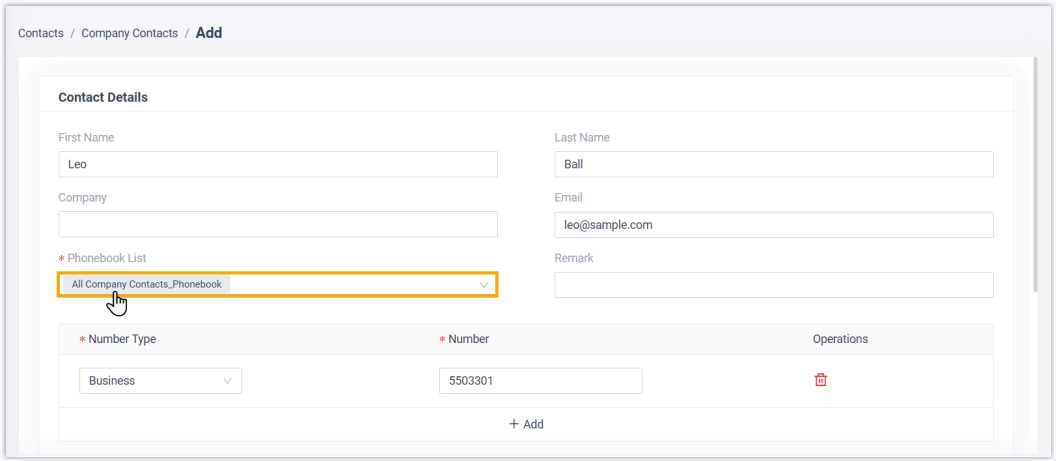
For more information, see Grant Company Contacts Permission, View and Manage Company Contacts from Linkus Mobile Client / Desktop Client / Web Client, and View Company Contacts from IP Phones.

Add a company contact

1. Log in to PBX web portal, go to **Contacts > Company Contacts**.
2. Click **Add**.



3. Enter contact information.

> **Note:**
> If your PBX has been subscribed to **Enterprise Plan** or **Ultimate Plan**, the contact will be automatically added to the default **All Company Contacts_Phonebook**. You can group the contact into other organized phonebook(s) by selecting existing phonebook(s) from the drop-down list of **Phonebook List**.
>
> 
>

4. Click **Save**.

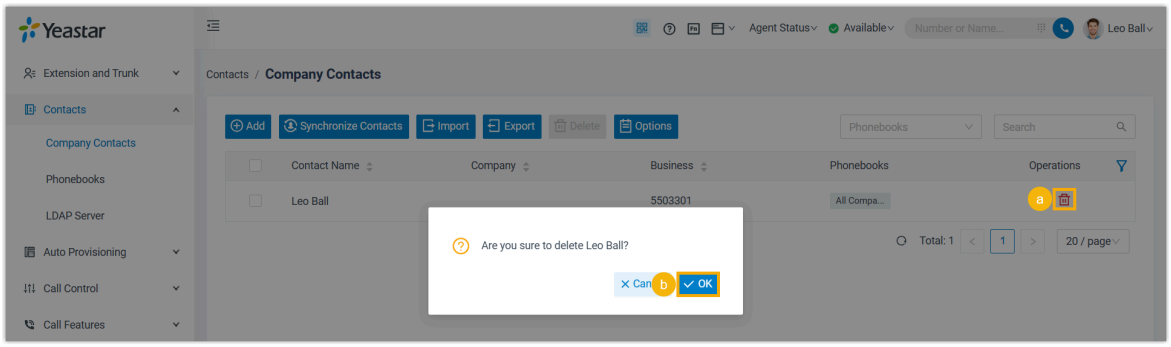
   The contact is stored as a company contact and shared among the authorized users from their Linkus UC Clients and IP phones.

Edit a company contact

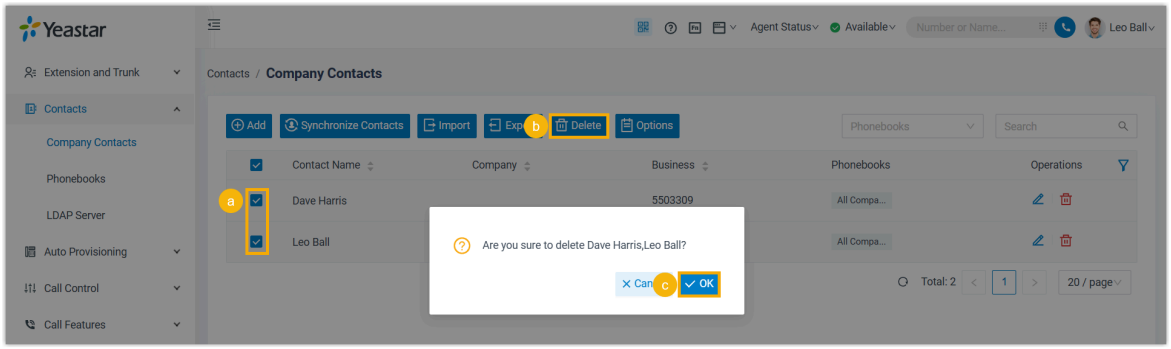
1. Log in to PBX web portal, go to **Contacts > Company Contacts**.
2. Click beside the desired contact.
3. Edit contact information as needed.
4. Click **Save**.

Delete company contacts

1. Log in to PBX web portal, go to **Contacts > Company Contacts**.
2. To delete a company contact, click beside the desired contact, then click **OK**.



3. To bulk delete company contacts, select the checkboxes of the desired contacts, then click **Delete** and **OK**.



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 web 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 web 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
Import and Export -FAQ

Third-party Contacts

Microsoft SQL

Microsoft SQL Integration Guide

Yeastar P-Series PBX System supports the integration with Microsoft SQL, which allows for automatically triggering contact lookup in your Microsoft SQL database when an inbound call reaches your PBX and displaying caller's name if a match is found. In addition, contact synchronization with phonebook(s) enables convenient outbound calling from Linkus UC Clients and intelligent inbound call routing based on phonebook(s) matches.

Requirements

Item	Requirement
Yeastar PBX	• **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP) • **Firmware**: Version 37.16.0.70 or later
Microsoft SQL	No requirement. All versions of Microsoft SQL Server can integrate with Yeastar P-Series PBX System.

Integration flow

The integration between Yeastar P-Series PBX System and Microsoft SQL enables a variety of features, including caller ID name display, contact synchronization, and intelligent inbound call routing based on phonebook matches.

Depending on the features that you want to implement, you will need to perform different operations for the integration, as shown below:

Scenario: Caller ID name display

1. Integrate Yeastar P-Series PBX System with Microsoft SQL

Scenario: Caller ID name display and contact synchronization

1. Integrate Yeastar P-Series PBX System with Microsoft SQL
2. Set up Contact Synchronization from Microsoft SQL

Scenario: Caller ID name display, contact synchronization, and inbound call routing based on phonebook match

1. Integrate Yeastar P-Series PBX System with Microsoft SQL
2. Set up Contact Synchronization from Microsoft SQL
3. Set up inbound routes based on phonebook matches

Integrate Yeastar P-Series PBX System with Microsoft SQL

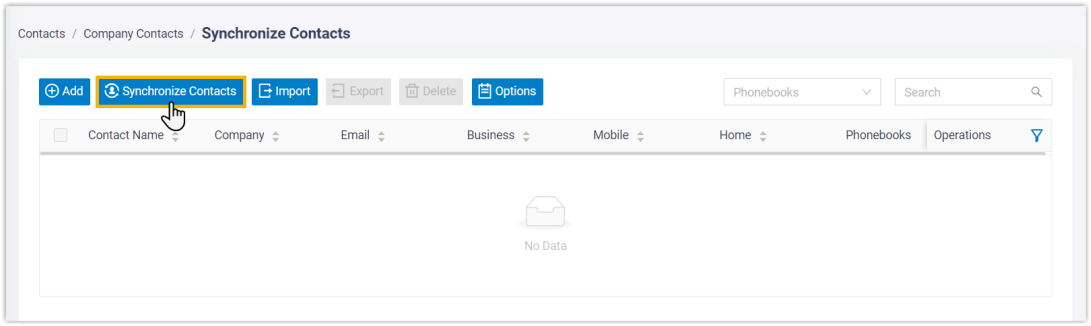
With the integration between Yeastar P-Series PBX System and Microsoft SQL, inbound calls to PBX will automatically trigger contact lookup in your Microsoft SQL database and display the caller's name if a match is found.

Requirements

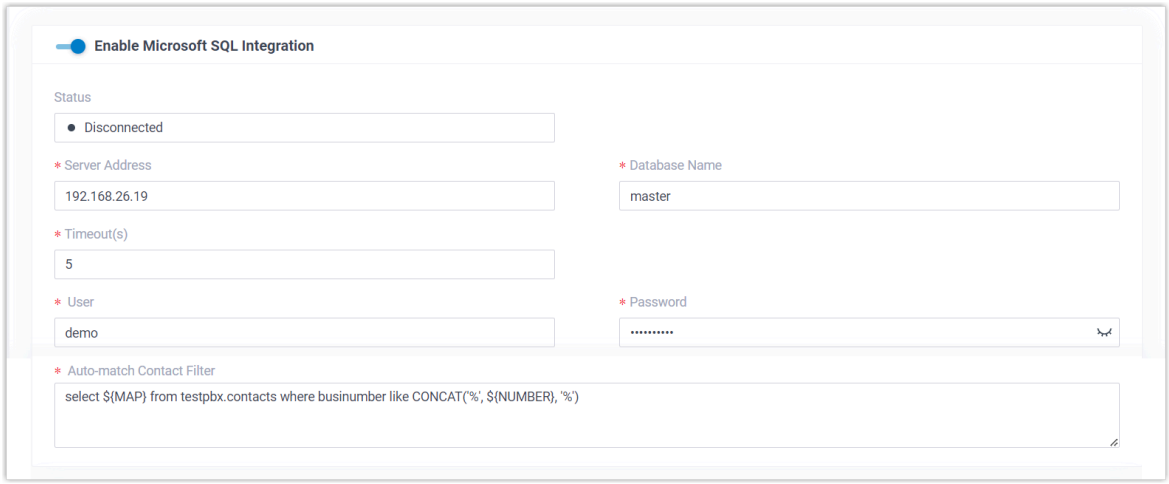
Item	Requirement
Yeastar PBX	• **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP) • **Firmware**: Version 37.16.0.70 or later
Microsoft SQL	No requirement. All versions of Microsoft SQL Server can integrate with Yeastar P-Series PBX System.

Step 1. Enable Microsoft SQL integration

1. Access the Microsoft SQL configuration page.
   a. Log in to PBX web portal, go to **Contacts > Company Contacts**.
   b. At the top of the page, click **Synchronize Contacts**.



2. Turn on the option **Enable Microsoft SQL Integration**, then complete the following settings.

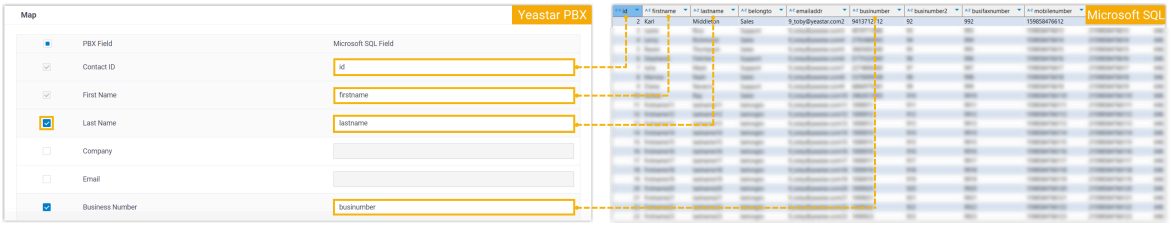


Item	Description
Server Address	Enter the address of Microsoft SQL server based on your situation. • If Microsoft SQL server runs on the default port `1433`, enter the server's IP address or domain name. For example, enter `192.168.26.19`. • If Microsoft SQL server runs on a non-default port, enter the server's IP address/domain name and port. For example, enter `192.168.26.19:2233`.
Database Name	Enter the name of the database.
Timeout(s)	Set the timeout for the connection to Microsoft SQL server.
User	Enter the username to connect to the database.
Password	Enter the password to connect to the database.
Auto-match Contact Filter	Enter a SELECT statement for contact caller ID matching, in the format **select ${MAP} from** *{schema_name}.{table_name}* **where** `{condition_to filter_number}`. **Example**: select ${MAP} from testpbx.contacts where businumber like CONCAT('%', ${NUMBER}, '%') • **select ${MAP}**: Specify the name of the column in the database that you want to display as the caller ID name. **Note:** *${MAP}* will be replaced by the field values corresponding to the PBX field (First Name, Last Name, or both) enabled in the **Map** section.

Item	Description
	• **from testpbx.contacts**: The table from which you want to select data, which must include two-part names (schema name and table name) in the format `{schema_name}.{table_name}`. • **where businumber like CONCAT('%', ${NUMBER}, '%')**: Retrieve the records where businumber contains the value of ${NUMBER} anywhere within it.

Step 2. Map contact fields between Yeastar P-Series PBX System and Microsoft SQL

1. Scroll down to the **Map** section.
2. Map the fields that are required for displaying caller's name.

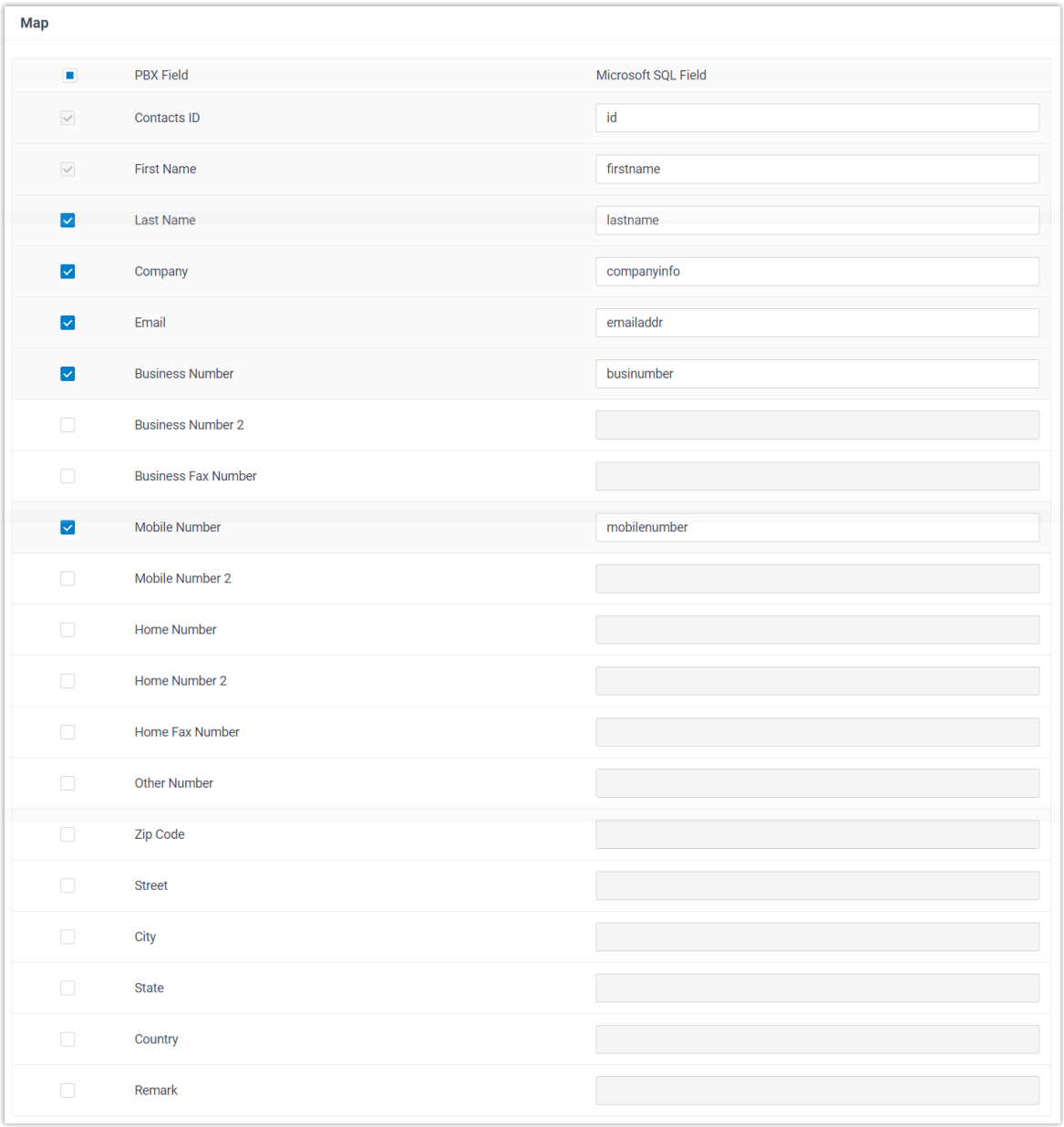


   a. For **Contacts ID**, **First Name**, and **Business Number**, enter the corresponding column name in Microsoft SQL contacts table.

   > **Note:**
   > In this example, **Business Number** is mapped because it is used as a number filter. You MUST map the number field based on your situation.

   When an inbound call matches a contact in your database, the contact's first name will be displayed.

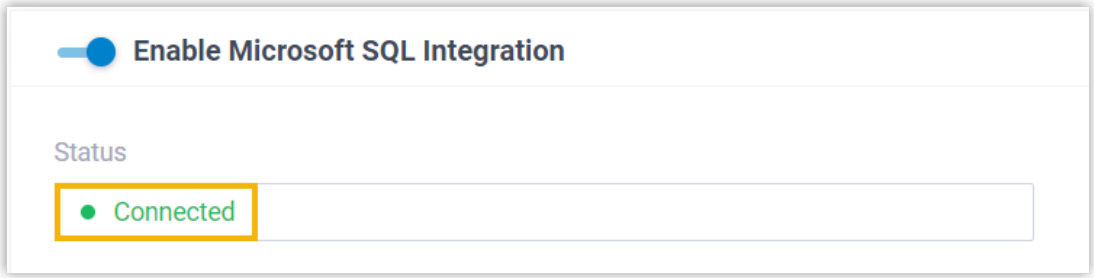
   b. **Optional:** To display contact's last name as well, select the checkbox of **Last Name**, then enter the corresponding column name in Microsoft SQL field.
3. If you want to synchronize Microsoft SQL contacts to PBX, enable and map the desired fields.



4. Click **Save**.

Result

- Yeastar P-Series PBX System is connected to your Microsoft SQL server.



- When an inbound call matches a contact in your database, the caller's name will be displayed.

What to do next

If you want to allow extension users to conveniently call Microsoft SQL contacts from Linkus UC Clients, you need to set up contact synchronization from Microsoft SQL server.

For more information, see Set up Contact Synchronization from Microsoft SQL.

Set up Contact Synchronization from Microsoft SQL

By synchronizing Microsoft SQL contacts to Yeastar P-Series PBX System, extension users can conveniently call these contacts from Linkus UC Clients. In addition, the system can automatically route inbound calls from Microsoft SQL contacts to the specified destinations based on phonebook matches.

Restrictions

Refer to the table below for the maximum number of company contacts and phonebooks supported by your system.

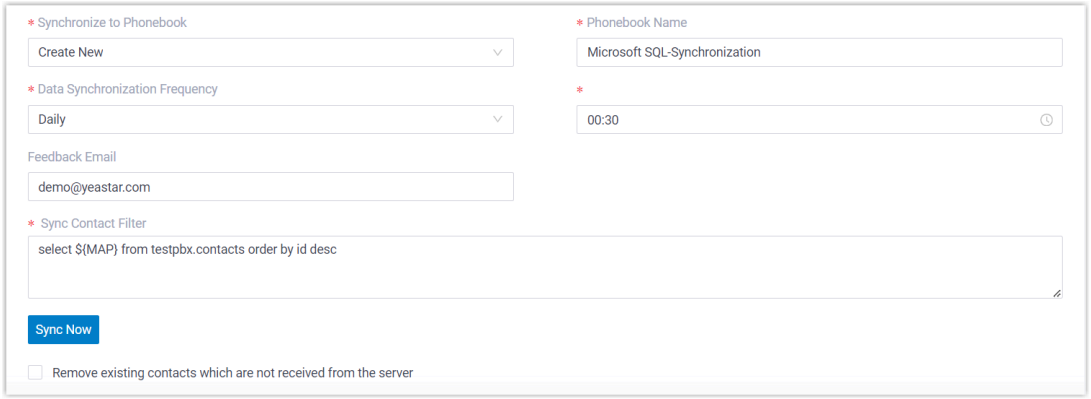
Type	P520	P550	P560	P570
Personal contacts (per extension)	3,000	3,000	3,000	3,000
Company contacts (total)	20,000	50,000	200,000	500,000
Company phonebooks	50	100	200	500

Prerequisites

You have mapped the desired contact fields between Yeastar P-Series PBX System and Microsoft SQL.

Procedure

1. On Microsoft SQL configuration page, scroll down to the **Contacts Synchronization** section.
2. Enable and set up contact synchronization from Microsoft SQL server.
   a. Turn on the option **Contacts Synchronization**.
   b. Complete the following settings.



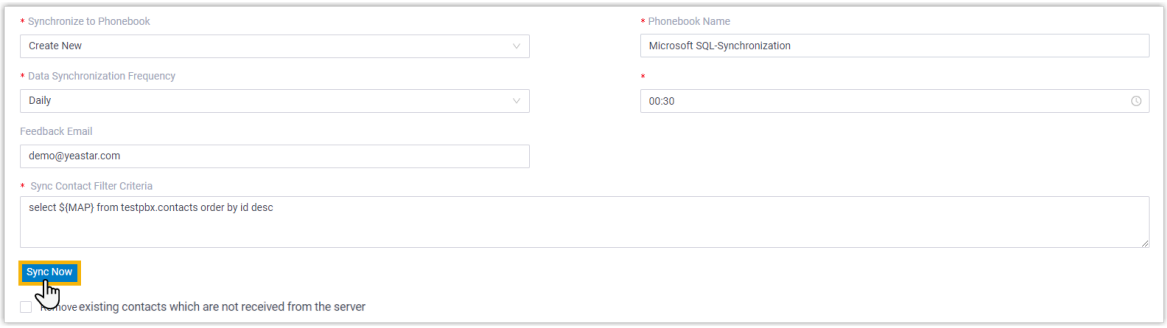
Item	Description
Synchronize to Phonebook	Select where to store the contacts that will be synchronized from your database. • **Create New**: Create a new phonebook from scratch to store the synced contacts. If you choose the option, enter the phonebook name in the **Phonebook Name** field. • **Read Specific Property Value and Create New**: Create a new phonebook based on the property value of a specific column in your contact table to store the synced contacts. If you choose the option, enter a column name of the contact table in the **Property Name** field. **Note:** This is helpful when you want to route inbound calls from Microsoft SQL contacts to the specified destinations in PBX based on phonebook matches. For example, there is a column named as **belongto**, which designates the team responsible for servicing the contacts - **Sales** and **Support**. By entering `belongto` in the

Item	Description
	field, the system will create two phonebooks - **Sales** and **Support** after you save the setting, and route inbound calls to the responsible team based on the phonebook matches after you configure proper inbound routes. • ***{existing_phonebook}***: Select an existing empty phonebook to store the synced contacts. **Note:** The existing empty phonebooks are synchronized from **Contacts > Phonebooks**.
Data Synchronization Frequency	Select the frequency to synchronize contacts, then configure time in the follow-up field. **Note:** Synchronizing a large number of contacts will affect system performance, we recommend that you schedule contact synchronization during off-peak hours.
Feedback Email	Optional. Enter an email address to get notified of the contact synchronization result. **Note:** A maximum of 5 email addresses are supported; Use a semicolon ; to separate multiple addresses.
Sync Contact Filter	Enter a SELECT statement for contact synchronization from Microsoft SQL, in the format **select ${MAP} from** ***{schema_name}.{table_name}***. **Note:** TOP clause is not supported. **Example**: select ${MAP} from testpbx.contacts order by id desc • **select ${MAP}**: Specify the name of the column in the database that you want to synchronize to PBX.

Item	Description
	Note: *${MAP}* will be replaced by the field values corresponding to the PBX field enabled in the **Map** section. • **from testpbx.contacts**: The table from which you want to select data, which must include two-part names (schema name and table name) in the format *{schema_name}.{table_name}*. • **order by id desc**: Sort the result in descending order.
Remove existing contacts which are not received from the server	If enabled, contacts that were successfully synchronized last time but do not exist in the current synchronization will be deleted by default.

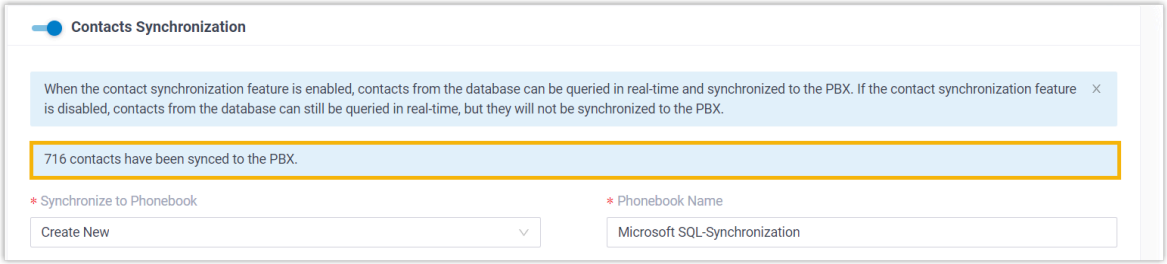
c. Click **Save**.

3. Click **Sync Now** to synchronize contacts to PBX immediately.

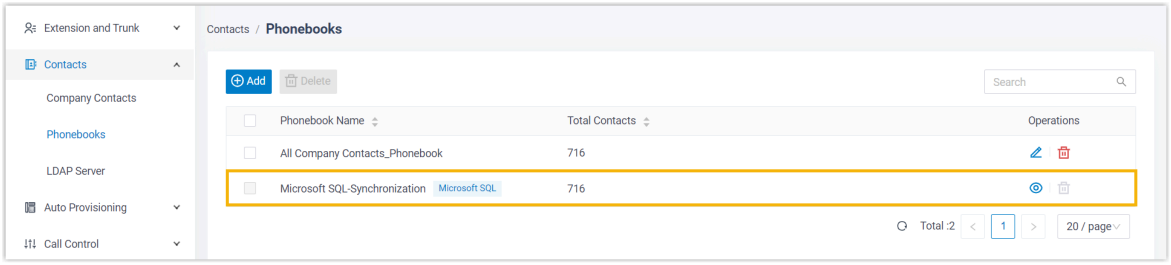


Result

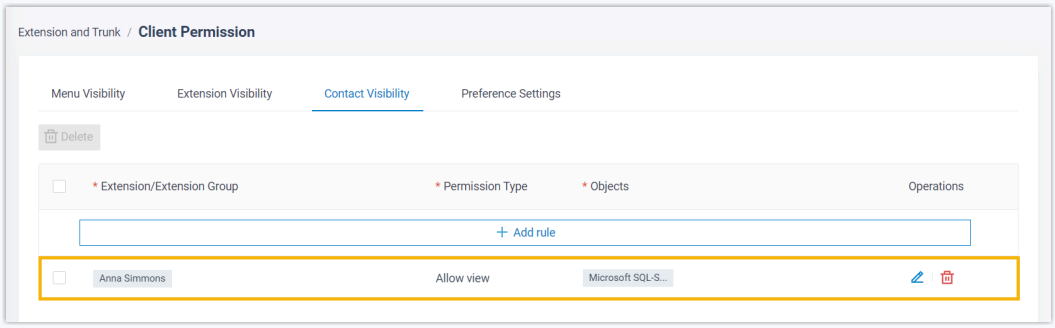
- A notification banner is appeared, displaying the number of contacts that have been successfully synchronized to PBX.



- You can check the synchronized contacts and their associated phonebook(s) in **Contacts > Company Contacts / Phonebooks**, which are tagged as Microsoft SQL.



- Authorized extension users can view and call the contacts directly from Linkus UC Clients.

> **Note:**
> To achieve this, you need to grant the viewing permission of the associated phonebook to extension users (Path: **Extension and Trunk > Client Permission > Contact Visibility**) and extension users need to upgrade Linkus UC Clients to the specified version, as shown below:
>
> - Linkus iOS Client: Version 5.7.3 or later
> - Linkus Android Client: Version 5.7.4 or later
> - Linkus Windows Desktop: Version 1.7.3 or later
> - Linkus Mac Desktop: Version 1.7.3 or later
>
> 
>

What to do next

If you want to route inbound calls to specified destinations based on phonebook matches, you need to configure inbound routes to route calls by matching contacts in different phonebooks.

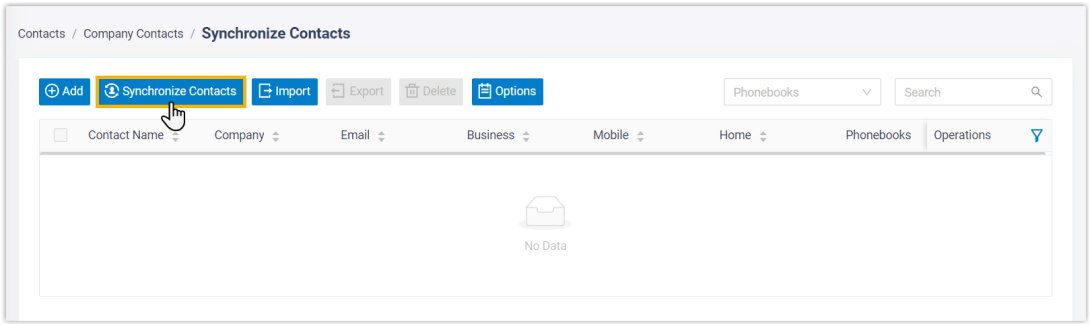
For more information, see Route Inbound Calls by Matched Phonebook Contacts.

Disable Microsoft SQL Integration

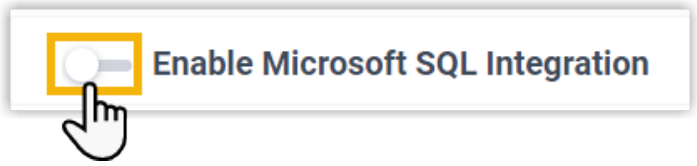
You can disable Microsoft SQL integration on Yeastar P-Series PBX System at any time when you want to pause the database integration.

Procedure

1. Access the Microsoft SQL configuration page.
   a. Log in to PBX web portal, go to **Contacts > Company Contacts**.
   b. At the top of the page, click **Synchronize Contacts**.



2. Turn off the option **Enable Microsoft SQL Integration**.



3. Click **Save**.

Result

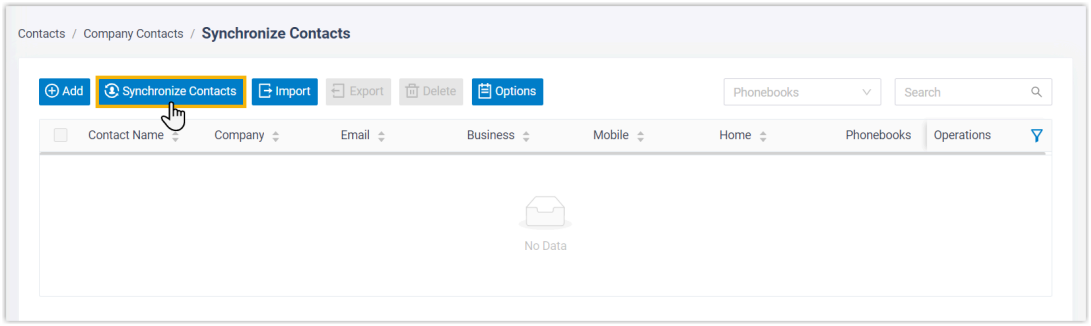
- The **Status** field displays **Disabled**.
- The Microsoft SQL configurations are retained, and can be used directly the next time the integration is enabled again.

Disconnect Microsoft SQL Integration

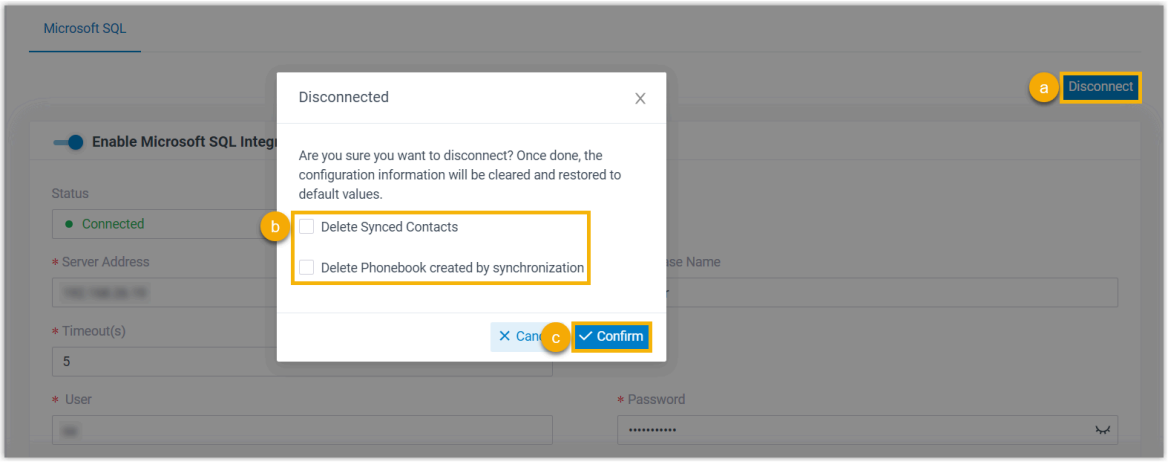
If you want to integrate with another database, you need to disconnect the current Microsoft SQL integration first.

Procedure

1. Access the Microsoft SQL configuration page.
    a. Log in to PBX web portal, go to **Contacts > Company Contacts**.
    b. At the top of the page, click **Synchronize Contacts**.



2. Disconnect Microsoft SQL integration.



    a. At the top-right corner, click **Disconnect**.
    b. **Optional:** To delete the synced contacts or created phonebook, select the check-box of **Delete Synced Contacts** and **Delete Phonebook created by synchronization**.
    c. Click **Confirm**.

Result

The Microsoft SQL integration is disconnected.

LDAP Server

LDAP Server Integration Guide

Yeastar P-Series PBX System supports the integration with third-party LDAP server (e.g-. MetaDirectory), which allows for automatically triggering contact lookup in your LDAP server when an inbound call reaches your PBX and displaying caller's name if a match is found. In addition, contact synchronization with phonebook(s) enables convenient outbound calling from Linkus UC Clients and intelligent inbound call routing based on phonebook(s) matches.

Requirements

Item	Requirement
Yeastar PBX	• **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP) • **Firmware**: Version 37.18.0.102 or later
Third-party LDAP Server	No requirement.

Integration flow

The integration between Yeastar P-Series PBX System and LDAP server enables a variety of features, including caller ID name display, contact synchronization, and intelligent inbound call routing based on phonebook matches.

Depending on the features that you want to implement, you will need to perform different operations for the integration, as shown below:

Scenario: Caller ID name display

1. Integrate Yeastar P-Series PBX System with LDAP Server

Scenario: Caller ID name display and contact synchronization

1. Integrate Yeastar P-Series PBX System with LDAP Server
2. Set up Contact Synchronization from LDAP Server

Scenario: Caller ID name display, contact synchronization, and inbound call routing based on phonebook match

1. Integrate Yeastar P-Series PBX System with LDAP Server
2. Set up Contact Synchronization from LDAP Server

3. Set up inbound routes based on phonebook matches

Integrate Yeastar P-Series PBX System with LDAP Server

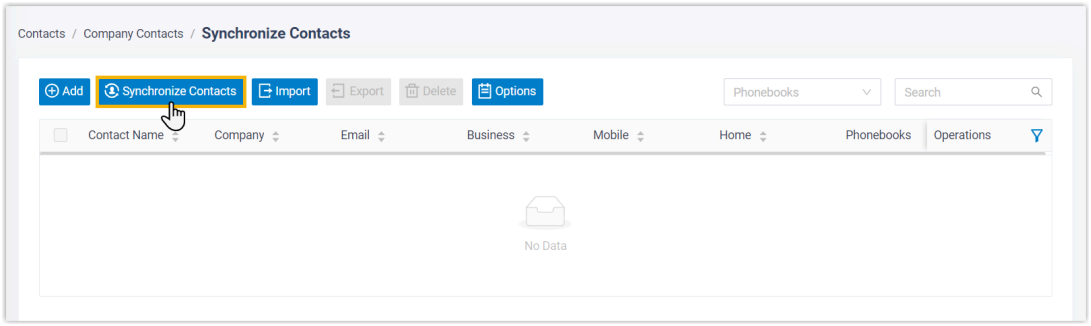
With the integration between Yeastar P-Series PBX System and LDAP server, inbound calls to PBX will automatically trigger contact lookup in your LDAP server and display the caller's name if a match is found.

Requirements

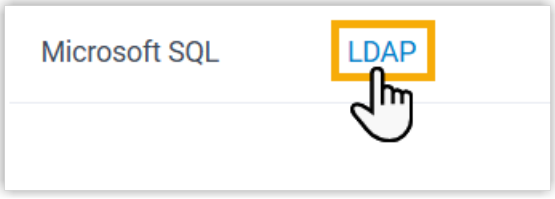
Item	Requirement
Yeastar PBX	• **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP) • **Firmware**: Version 37.18.0.102 or later
Third-party LDAP Server	No requirement.

Step 1. Enable LDAP integration

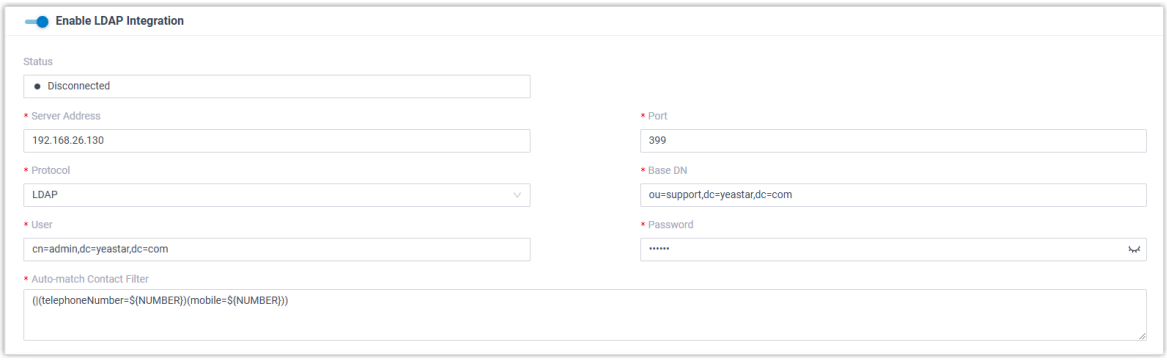
1. Access the LDAP configuration page.
   a. Log in to PBX web portal, go to **Contacts > Company Contacts**.
   b. At the top of the page, click **Synchronize Contacts**.



   c. Click **LDAP** tab.



2. Turn on the option **Enable LDAP Integration**, then complete the following settings.

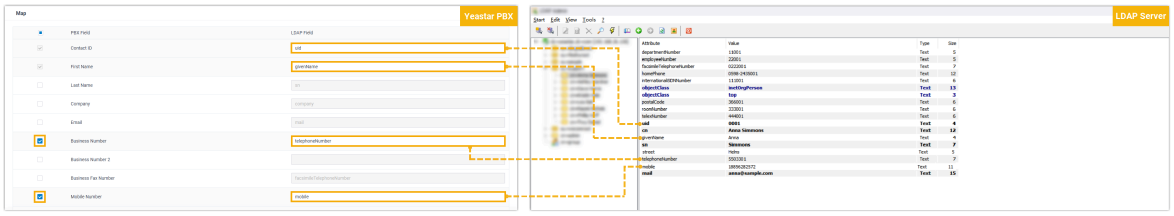


Item	Description
Server Address	Enter the address of LDAP server.
Port	Enter the port on which LDAP server is running.
Protocol	Select an LDAP protocol. • **LDAP**: Transmit data in plain text. • **LDAPS**: Use SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt and authenticate the data transmitted between the LDAP server and the LDAP client.
Base DN	Specify the Distinguished Name (DN) as the base for contact searches in caller ID matching and contacts synchronization. The Base DN must include the Domain Component (DC) attribute to define the root node of an LDAP tree, formatted as `dc=`*`{domain_prefix}`*`,dc=`*`domain_suffix`*. One or more Relative Distinguished Name (RDN) can be configured to narrow the scope of search. • **Example 1**: dc=yeastar,dc=com In this example, PBX will search contacts from yeastar.com (root entry of the LDAP tree). • **Example 2**: ou=support,dc=yeastar,dc=com In this example, PBX will search contacts from support (the Organizational Unit) within yeastar.com (root entry of the LDAP tree).
User	Enter the username to connect to the LDAP server. **Note:** This account must have permission to read the attribute types and object classes contained in the server schema.

Item	Description
Password	Enter the password associated with the username.
Auto-match Contact Filter	Enter a filter statement for contact caller ID matching. This filter statement must contain the `${NUMBER}` variable to represent the caller's number, and at least one number attribute for number lookup. **Example**: (\|(telephoneNumber=${NUMBER})(mobile=${NUMBER})) In this example, the PBX will search for entries in **telephoneNumber** or **mobile** attribute and compare them with `${NUMBER}`(caller's number) when receiving an inbound call. If a match is found, the PBX retrieves the corresponding contact entry and displays the caller's name.

Step 2. Map contact fields between Yeastar P-Series PBX System and LDAP server

1. Scroll down to the **Map** section.
2. Map the fields that are required for displaying caller's name.

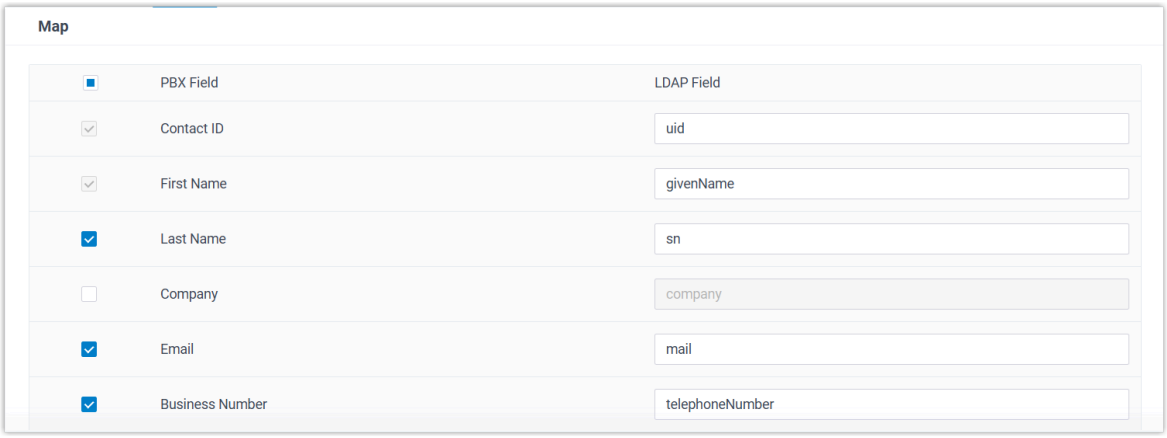


   a. For **Contact ID**, **First Name**, **Business Number**, and **Mobile Number**, enter the corresponding LDAP attribute name.

   > **Note:**
   > In this example, **Business Number** and **Mobile Number** are mapped because they are used as number filters. You MUST map the number field based on your situation.

   When an inbound call matches a contact in your LDAP server, the contact's first name will be displayed.

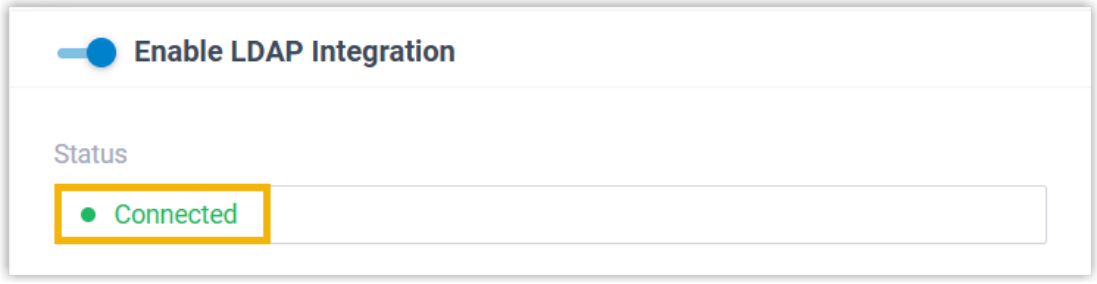
   b. **Optional:** To display contact's last name as well, select the checkbox of **Last Name**, then enter the corresponding LDAP attribute name.
3. If you want to synchronize LDAP contacts to PBX, enable and map the desired fields.



4. Click **Save**.

Result

- Yeastar P-Series PBX System is connected to your LDAP server.



- When an inbound call matches a contact in your LDAP server, the caller's name will be displayed.

What to do next

If you want to allow extension users to conveniently call LDAP contacts from Linkus UC Clients, you need to set up contact synchronization from LDAP server.

For more information, see Set up Contact Synchronization from LDAP Server.

Set up Contact Synchronization from LDAP Server

By synchronizing LDAP contacts to Yeastar P-Series PBX System, extension users can conveniently call these contacts from Linkus UC Clients. In addition, the system can automatically route inbound calls from LDAP contacts to the specified destinations based on phonebook matches.

Restrictions

Refer to the table below for the maximum number of company contacts and phonebooks supported by your system.

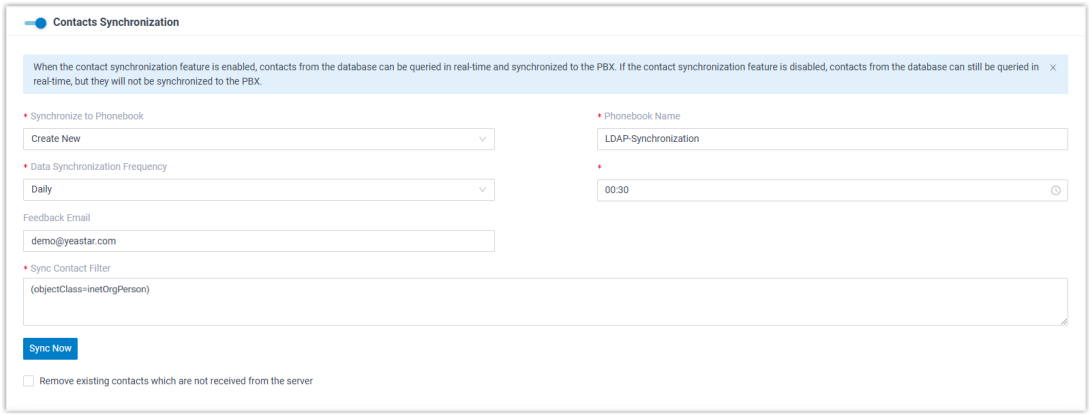
Type	P520	P550	P560	P570
Personal contacts (per extension)	3,000	3,000	3,000	3,000
Company contacts (total)	20,000	50,000	200,000	500,000
Company phonebooks	50	100	200	500

Prerequisites

You have mapped the desired contact fields between Yeastar P-Series PBX System and LDAP server.

Procedure

1. On LDAP configuration page, scroll down to the **Contacts Synchronization** section.
2. Enable and set up contact synchronization from LDAP server.
    a. Turn on the option **Contacts Synchronization**.
    b. Complete the following settings.



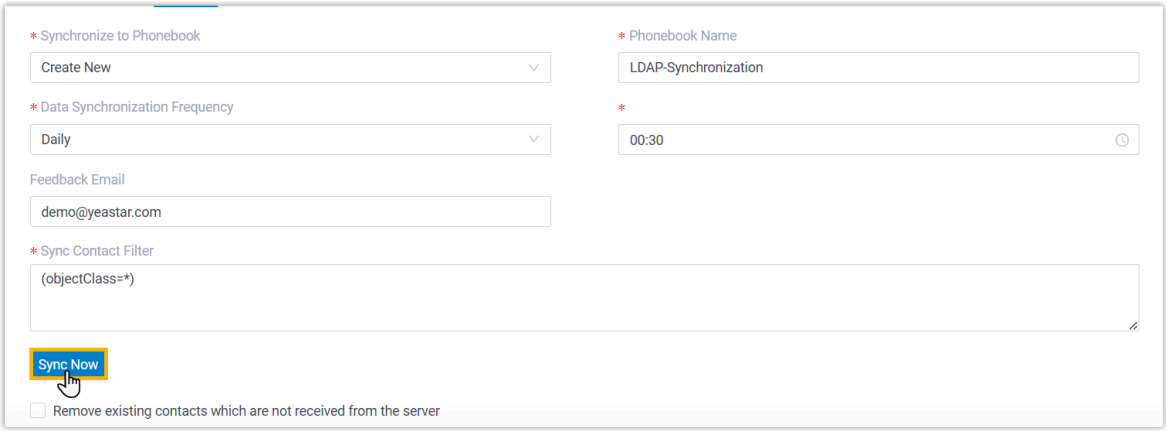
Item	Description
Synchronize to Phonebook	Select where to store the contacts that will be synchronized from LDAP server. • **Create New**: Create a new phonebook from scratch to store the synced contacts. If you choose the option, enter the phonebook name in the **Phonebook Name** field.

Item	Description
	• **Read Specific Property Value and Create New**: Create a new phonebook based on a specific LDAP attribute to store the synced contacts. If you choose the option, enter an LDAP attribute name in the **Property Name** field. **Note:** This is helpful when you want to route inbound calls from LDAP contacts to the specified destinations in PBX based on phonebook matches. For example, there is an LDAP attribute **department**, which designates the team responsible for serving the contacts - **Sales** and **Support**. By entering `department` in the field, the system will create two phonebooks - **Sales** and **Support** after you save the setting, and route inbound calls to the responsible team based on the phonebook matches after you configure proper inbound routes. • ***{existing_phonebook}***: Select an existing empty phonebook to store the synced contacts. **Note:** The existing empty phonebooks are synchronized from **Contacts > Phonebooks**.
Data Synchronization Frequency	Select the frequency to synchronize contacts, then configure time in the follow-up field. **Note:** Synchronizing a large number of contacts will affect system performance, we recommend that you schedule contact synchronization during off-peak hours.
Feedback Email	Optional. Enter an email address to get notified of the contact synchronization result. **Note:**

Item	Description
	A maximum of 5 email addresses are supported; Use a semicolon ; to separate multiple addresses.
Sync Contact Filter	Enter a filter statement for contact synchronization from LDAP server. **Note:** The filter condition is restricted to the Base DN, which means that PBX will start searching from the Base DN, and only synchronize entries that match the sync contact filter. **Example**: (objectClass=inetOrgPerson) In this example, all the LDAP contacts will be synchronized to PBX.
Remove existing contacts which are not received from the server	If enabled, contacts that were successfully synchronized last time but do not exist in the current synchronization will be deleted.

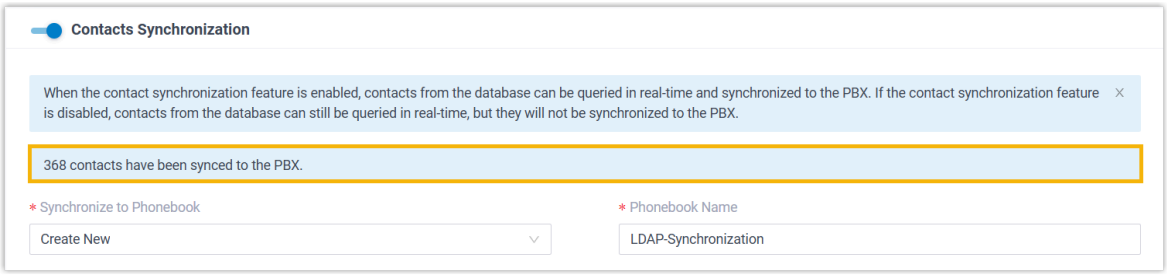
c. Click **Save**.

3. Click **Sync Now** to synchronize contacts to PBX immediately.

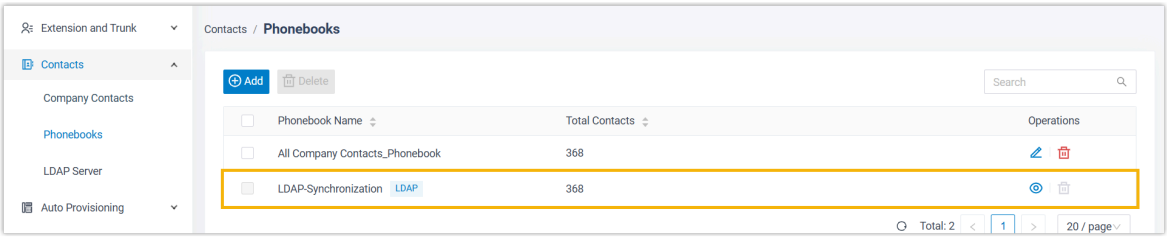


Result

- A notification banner is appeared, displaying the number of contacts that have been successfully synchronized to PBX.



- You can check the synchronized contacts and the associated phonebook(s) in **Contacts > Company Contacts / Phonebooks**, which are tagged as LDAP.

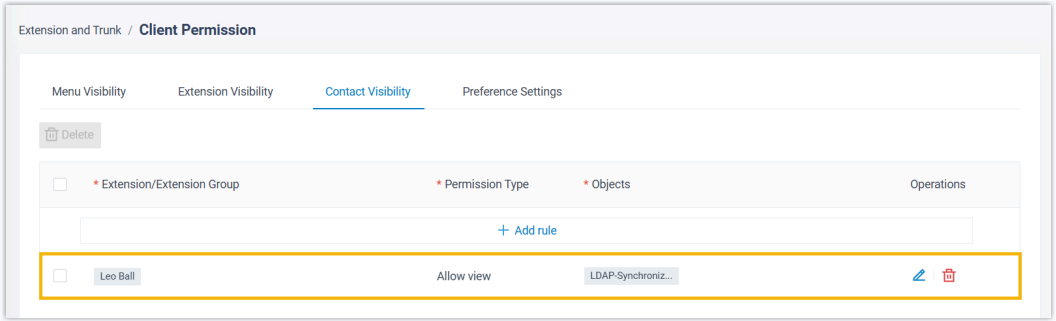


- Authorized extension users can view and call the contacts directly from Linkus UC Clients.

Note:

To achieve this, you need to grant the viewing permission of the associated phonebook to extension users (Path: **Extension and Trunk > Client Permission > Contact Visibility**) and extension users need to upgrade Linkus UC Clients to the specified version, as shown below:

- Linkus iOS Client: Version 5.13.6 or later
- Linkus Android Client: Version 5.13.8 or later



What to do next

If you want to route inbound calls to specified destinations based on phonebook matches, you need to configure inbound routes to route calls by matching contacts in different phonebooks.

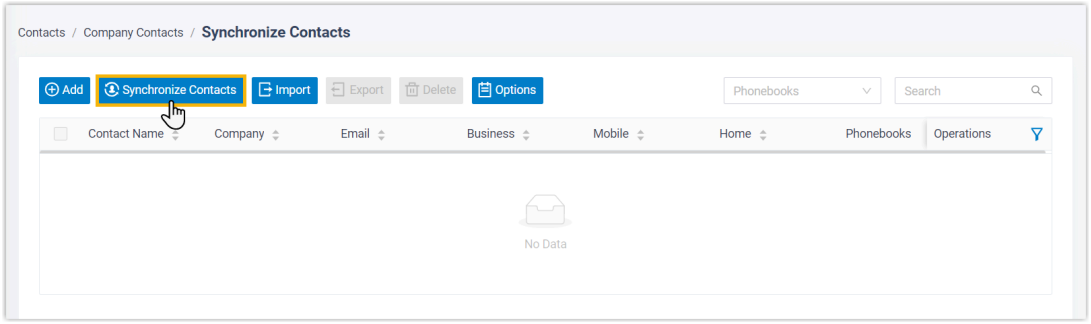
For more information, see Route Inbound Calls by Matched Phonebook Contacts.

Disable LDAP Integration

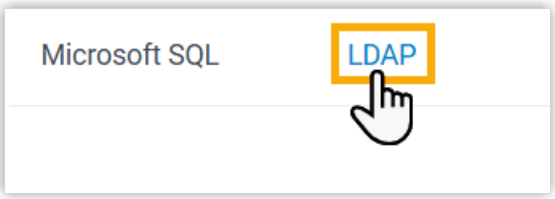
You can disable LDAP integration on Yeastar P-Series PBX System at any time when you want to pause the integration.

Procedure

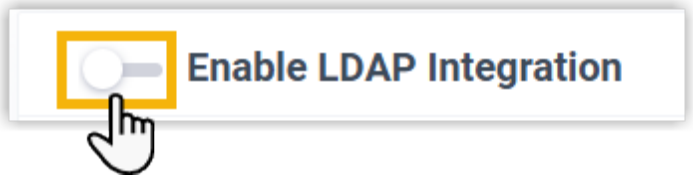
1. Access the LDAP configuration page.
   a. Log in to PBX web portal, go to **Contacts > Company Contacts**.
   b. At the top of the page, click **Synchronize Contacts**.



   c. Click **LDAP** tab.



2. Turn off the option **Enable LDAP Integration**.



3. Click **Save**.

Result

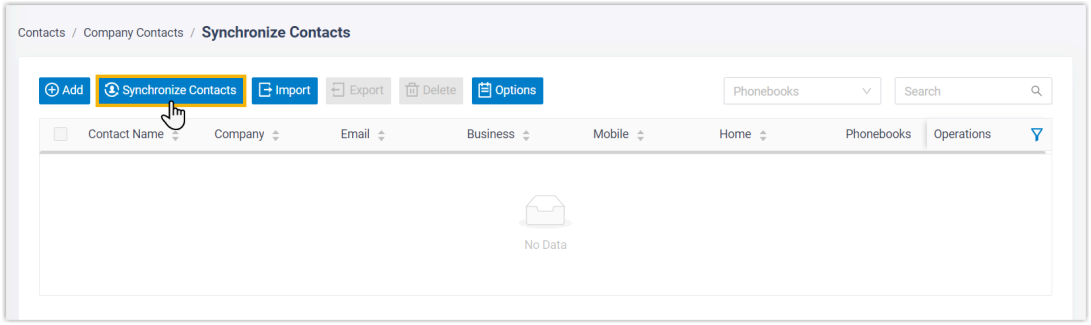
- The **Status** field displays **Disabled**.
- The LDAP configurations are retained, and can be used directly the next time the integration is enabled again.

Disconnect LDAP Integration

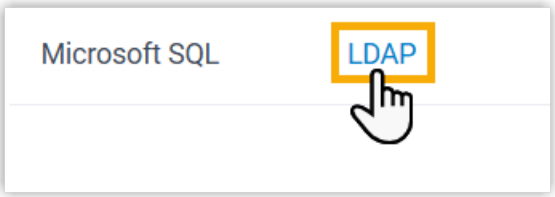
If you want to integrate with another database, you need to disconnect the current LDAP integration first.

Procedure

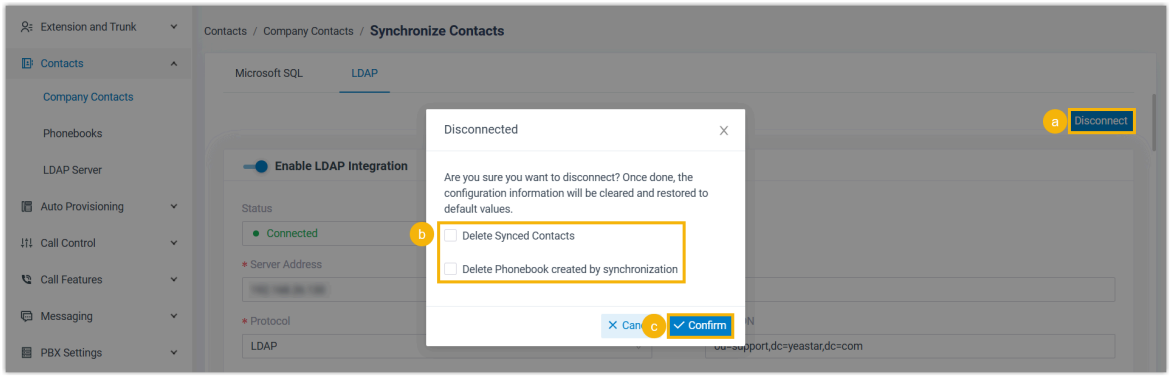
1. Access the LDAP configuration page.
    a. Log in to PBX web portal, go to **Contacts > Company Contacts**.
    b. At the top of the page, click **Synchronize Contacts**.



    c. Click **LDAP** tab.



2. Disconnect LDAP integration.



a. At the top-right corner, click **Disconnect**.
b. **Optional:** To delete the synced contacts or created phonebook, select the check-box of **Delete Synced Contacts** and **Delete Phonebook created by synchronization**.
c. Click **Confirm**.

Result

The LDAP integration is disconnected.

Phonebook

Add and Manage Company Phonebooks

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

Prerequisites

You have subscribed to **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 types of phonebooks:

- **PBX-native company phonebook**: The phonebooks that store company contacts added from PBX web portal and Linkus UC Clients.

  You can manually create phonebooks to group company contacts.

- **Third-party company phonebook**: The phonebooks that store company contacts synchronized from the third-party system integration.

  If you schedule the synchronization of contacts from the integrated system, all the synced contacts will be grouped into a phonebook with a unique identifier, and the phonebook can't be modified or deleted unless you disconnect the integration.

Add a company phonebook

1. Log in to PBX web 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.

   Define a All Contacts phonebook

   In the drop-down list of **Select Contacts**, select **All Company Contacts**.

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

   Group specific contacts into a phonebook

   a. In the drop-down list of **Select Contacts**, select **Specific Company Contacts**.
   b. Click **Add** to select the desired company contacts.
   c. Click **Confirm**.
5. Click **Save**.

Edit a company phonebook

1. Log in to PBX web 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 web 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

Contacts Overview
Set up Contact Visibility
Add and Manage Company Contacts
Identify Callers from Contacts
Allow Users to Query Contacts on IP Phones

Contacts Visibility

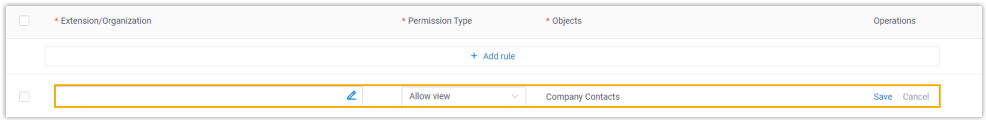
Set up Contact Visibility

By default, all the users can neither manage nor view company contacts. To allow specific users to manage or view company contacts, you can set up company contacts visibility as the instructions provided in this topic.

Set up contact visibility (Basic Plan)

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Contact Visibility**.
2. Click **Add rule** to create a contact visibility rule.
3. Set up the rule:



a. Select desired values from the drop-down lists.

- **Extension/Extension Group/Organization**: Click to select desired extensions, extension groups, or departments, for which you want to grant the viewing permission or management permission.
- **Permission Type**: Select an option from the drop-down list to define the permission.
  - **Allow view**: Allow to view company contacts.
  - **Allow manage**: Allow to view, add, edit, or delete company contacts.
- **Objects**: **Company Contacts** is displayed and can not be edited.

b. Click **Save**.

Result

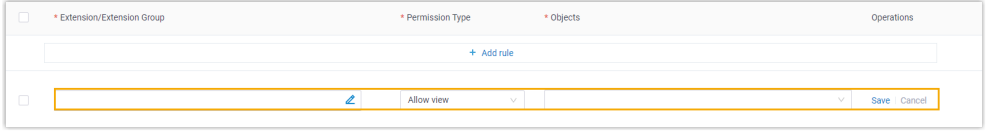
- On Linkus clients, the authorized users can view or manage company contacts.
- On auto-provisioned Yealink IP phones, the authorized users can view company contacts.

  For more information, see Allow Users to Query Contacts on IP Phones.

Set up contact visibility (EP/UP)

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Contact Visibility**.
2. Click **Add rule** to create a contact visibility rule.
3. Set up the rule:



a. Select desired values from the drop-down lists.

- **Extension/Extension Group/Organization**: Click to select desired extensions, extension groups, or departments, for which you want to grant the viewing permission or management permission.
- **Permission Type**: Select an option from the drop-down list to define the permission.
  - **Allow view**: Allow to view the phonebooks that are selected in **Objects**.
  - **Allow manage**: Allow to view, add, edit, or delete the phonebooks that are selected in **Objects**.
- **Objects**: Click to select desired phonebooks that are allowed to be viewed or managed.

b. Click **Save**.

Result

- On Linkus clients, the authorized users can view or manage company contacts.
- On auto-provisioned Yealink IP phones, the authorized users can view company contacts.

  For more information, see Allow Users to Query Contacts on IP Phones.

Manage Contact Visibility Rules

This topic describes how to edit and delete contact visibility rules.

Edit a contact visibility rule

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Contact Visibility**.
2. Click beside a desired contact visibility rule.
3. Edit the rule as needed.
4. Click **Save**.

Delete contact visibility rules

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Contact Visibility**.
2. To delete a contact visibility rule, do as follows:
   a. Click  beside a desired rule.
   b. In the pop-up window, click **OK**.
3. To bulk delete contact visibility rules, do as follows:
   a. Select the checkboxes of desired rules, click **Delete**.
   b. In the pop-up window, click **OK**.

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 Set up Contact Visibility.

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 web 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.
      - **Match the last *{number}* digits**: Display contact name based on the digits of incoming Caller ID.
        - If the digit length of an incoming Caller ID is shorter than or equal to the specified value, contact name will be displayed only when the incoming Caller ID exactly matches existing number.
        - If the digit length of an incoming Caller ID is longer than the specified value, contact name will be displayed when the last few digits of the incoming Caller ID matches that of existing number.

      > **Note:**
      > The default value is 7. To change the value, enter a number between 4 and 31.

   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.
- **Match the last 9 digits** is configured:
  - If the incoming Caller ID is 12345678, the contact name "Dora" will be displayed.

- If the incoming Caller ID is 15212345678, 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 Set up Contact Visibility.

> **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 been associated with phones, see the following topics to register the extensions to phones.
        - Auto Provision IP Phones in Local Network (PnP Method)
        - Auto Provision IP Phones in Local Network (DHCP Method)
        - Auto Provision IP Phones Remotely (RPS FQDN Method)
        - Auto Provision IP Phones Remotely (RPS Method)
        - Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
        - Auto Provision IP Phones Remotely (Provision Link Method)
    - 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.

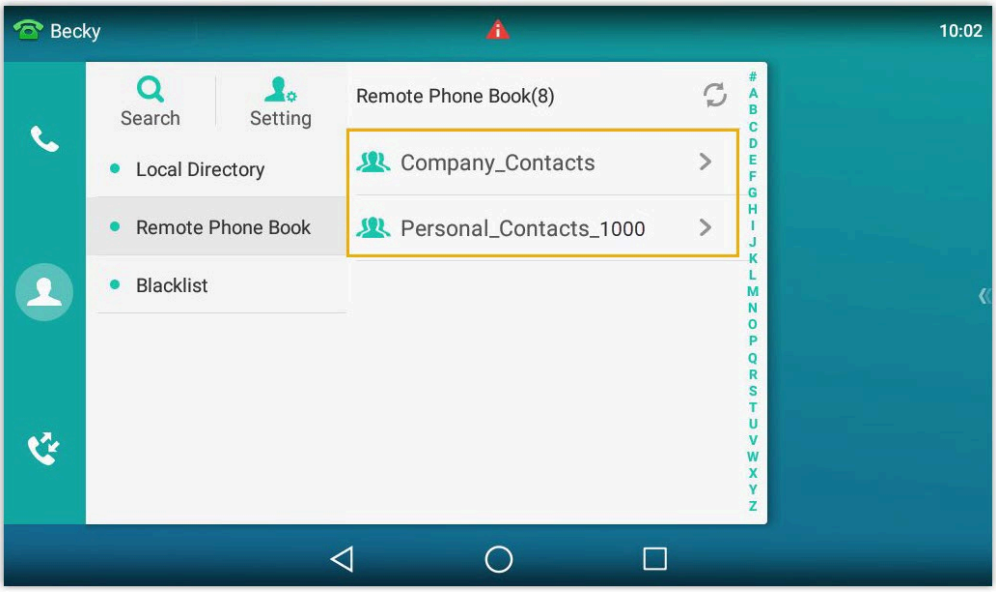
  Note:
  For Enterprise/Ultimate Plan, company contacts on IP phones can NOT be grouped into phonebooks.

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

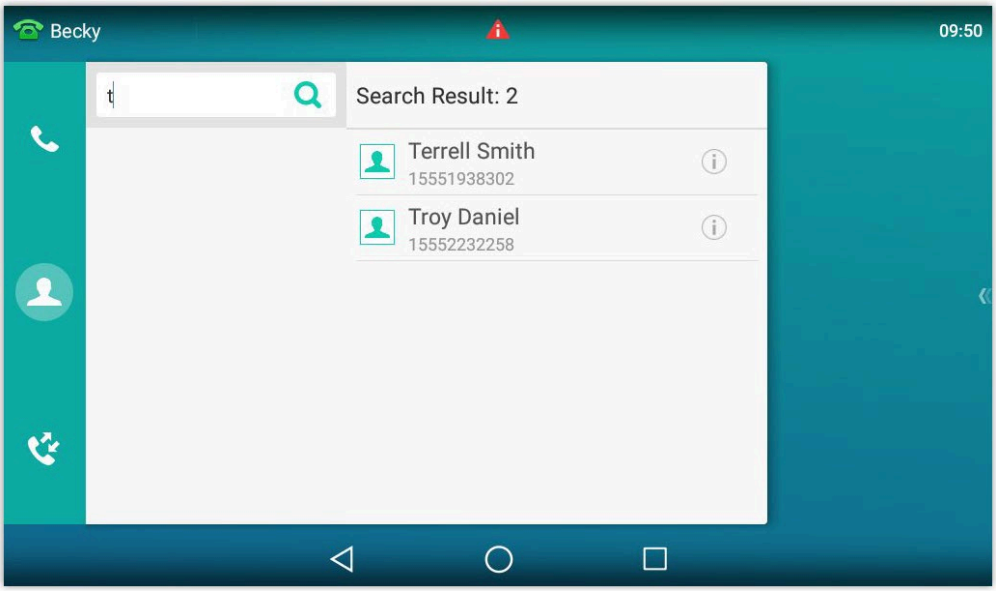
Example: Query contacts on Yealink T56A IP phone

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.

Client Permission

Yeastar P-Series PBX System Client Permissions

Client permissions enable you to control user access to specific information, features, and settings. Yeastar P-Series PBX System supports customizing permission rules to control Linkus client menu and operation permissions, Extension visibility permission, and Contacts visibility permission.

Linkus clients menu and operation permissions

By default, users can access all the menus and configure all the settings within Linkus clients. You can set up permission rules to restrict users' access and operation permission:

- **Menu Visibility Permission**: Restrict users from specific menus within Linkus clients.
- **Operation Permission**: Restrict users from specific settings within Linkus clients.

For more information, see Set up User Permissions of Linkus Clients .

Extension visibility permission

By default, all the users can view all departments or the default extension group on Linkus clients. You can set up visibility rules to restrict users from viewing specific extensions, extension groups,or departments.

For more information, see Set up Extension Visibility.

Contact visibility permission

By default, all the users can neither manage nor view company contacts. You can set up visibility rules to allow specific users to manage or view company contacts.

> **Note:**
> Personal contacts are ONLY visible to the users themselves.

For more information, see Set up Contact Visibility.

LDAP Server

LDAP Server Overview

Yeastar P-Series PBX System can be set as an LDAP Server, which provides centralized phonebook management. With this feature, you can store the contact information on the PBX, and quickly launch calls without wasting time finding a contact's number and subsequently entering it on your phone, thus greatly improving work efficiency.

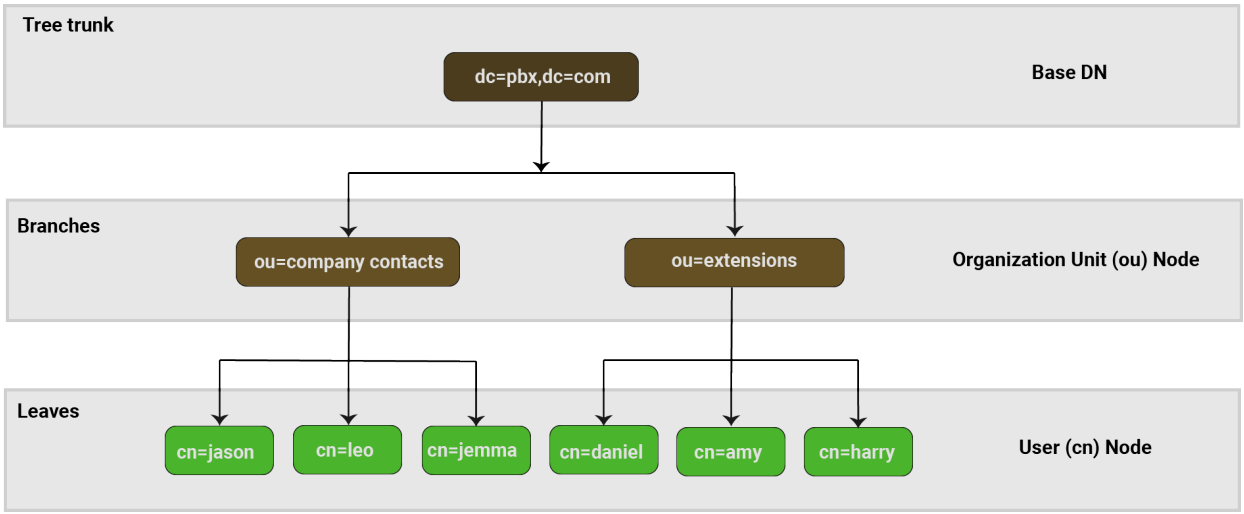
LDAP introduction

LDAP stands for Lightweight Directory Access Protocol, which is an application protocol for accessing and maintaining information services for the distributed directory over an IP network.

The LDAP directory server is based on the client/server mode. The LDAP Server contains directory data. An LDAP Client connects to the LDAP Server, and sends a request to obtain directory data from the LDAP Server, thus implementing global directory data management.

LDAP directory structure

The LDAP Server is a type of network database based on entries, which is a collection of information about an entity. In LDAP, directory entries are arranged in a hierarchical tree-like structure. The following figure shows an example of Yeastar P-Series PBX System LDAP directory tree.



LDAP terminologies

An LDAP entry is a collection of information about an entity. Each entry consists of three primary components: a distinguished name, a collection of attributes, and a collection of object classes.

Distinguished Name (DN)

A globally-unique entry's distinguished name, which uniquely identifies the entry and its position in the directory information tree hierarchy.

A DN usually consists of three components.

- dc: Domain Component, usually refers to a component of the domain name.
- ou: Organization Unit, usually refers to a name of a group object.
- cn: Common Name, usually refers to a user name.

The DN of an LDAP entry is much like the path to a file on a filesystem. For example, `cn=amy,ou=extensions,dc=pbx,dc=com` is like a file path of `com/pbx/extensions/amy`.

The **Base DN** is the root of the LDAP directory tree, which is the starting point of LDAP search. For example, `dc=pbx,dc=com`.

Attributes

Each entry can have multiple attributes. Each attribute has an attribute type and a set of values that comprise the actual data.

The syntax of values depends on the attribute type. The following table gives examples of attributes when `ou=company contacs`.

Attribute	Information details	Example
cn	Contact ID	Leo
displayName	Display Name	Leo Ball
givenName	First Name	Leo
sn	Last Name	Ball
mail	Email Address	leoball@example.com
company	Company	Yeastar
comment	Remark	partner
telephoneNumber	Business Number	+86-592-5503301

Attribute	Information details	Example
telephoneNumber2	Business Number 2	+86-592-5503308
facsimileTelephoneNumber	Fax Business Number	+86-592-5503301
mobile	Mobile Number	12345678902
mobile2	Mobile Number 2	12345678900
homePhone	Home Number	12345678902
homePhone2	Home Number 2	12345678903
facsimileHomePhone	Home Fax	12345678904
otherTelephone	Other Number	15880123456
postalCode	Zip Code	361024
street	Street	Software Park Phase III
l	City	Xiamen
st	State	Fujian
co	Country	China

Object Classes

Object Class defines collections of attribute types which may be used in entries containing that class, and which of those attribute types will be required rather than optional. Every entry has a structural object class, which indicates what kind of object an entry represents (e.g., whether it is information about a person, a group, a device, a service, etc.), and may also have zero or more auxiliary object classes that suggest additional characteristics for that entry.

For example, if the objectclass is `person`, then the required attributes are `givenName` and `sn`, the optional attributes are `description`, `seeAlso`, etc.

Related information

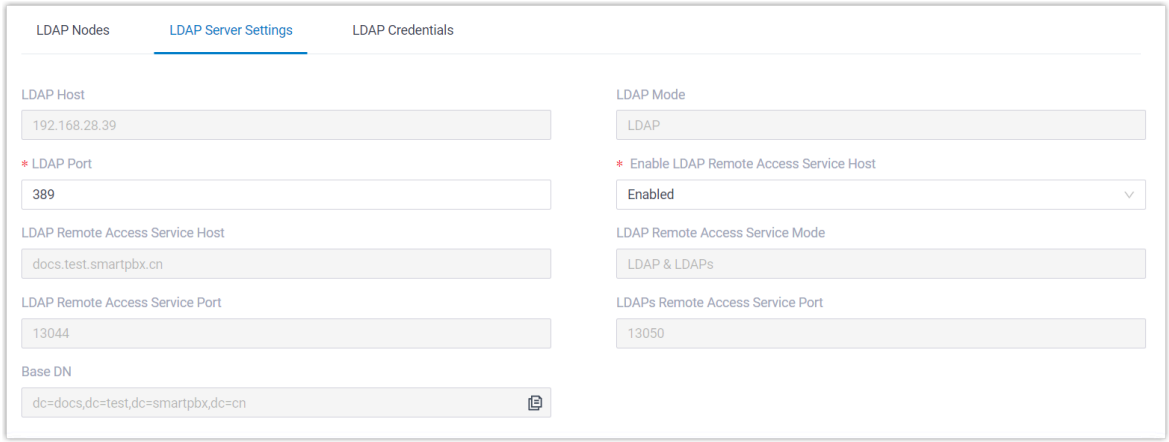
Set up Yeastar P-Series PBX System as an LDAP Server

Set up Yeastar P-Series PBX System as an LDAP Server

This topic describes how to set up Yeastar P-Series PBX System as an LDAP Server. In this way, you can store the contacts information on PBX and query from IP phones directly.

Procedure

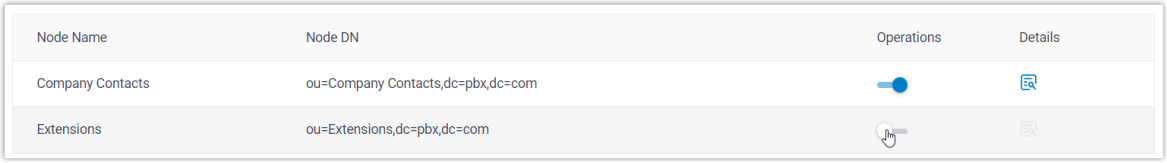
1. Log in to PBX web portal, go to **Contacts > LDAP Server**.
2. On the top of the page, turn on **LDAP Server**.
3. Click the **LDAP Server Settings** tab to check the LDAP Server settings or change the settings according to your needs.



Setting	Description
LDAP Host	The LDAP Server address of Yeastar P-Series PBX System. LDAP Client connects to the LDAP Server via the address.
LDAP Mode	The connection protocol used between the LDAP Server and the LDAP Clients.
LDAP Port	The LDAP port of the LDAP Server.
Enable LDAP Remote Access Service Host	Set whether to enable the LDAP Remote Access Service. If enabled, LDAP Clients will be able to connect to the LDAP Server via Remote Access Service. **Note:** To enable this feature, make sure you have enabled the Yeastar FQDN for remote LDAP access. For more information, see Configure Network for Remote LDAP Access by a Yeastar FQDN.
LDAP Remote Access Service Host	The remote access address of the Yeastar P-Series PBX System LDAP Server. **Note:**

Setting	Description
	This setting is only available after you enable the LDAP Remote Access Service.
LDAP Remote Access Service Mode	The connection protocol used between the LDAP Server and the LDAP Clients. **Note:** This setting is only available after you enable the LDAP Remote Access Service.
LDAP Remote Access Service Port	The LDAP remote access port of the LDAP Server. **Note:** This setting is only available after you enable the LDAP Remote Access Service.
LDAPs Remote Access Service Port	The LDAPs remote access port of the LDAP Server. **Note:** This setting is only available after you enable the LDAP Remote Access Service.
Base DN	Set up the base entry of the directory. For example, `dc=pbx,dc=com`. **Note:** If the LDAP remote access is enabled, the Base DN is based on the domain name of Yeastar P-Series PBX System.

4. Click **Save** to apply the change.
5. Click the **LDAP Nodes** tab, enable or disable the nodes according to your needs.



If a node is disabled, you can not query the information under this node.

Result

The Yeastar P-Series PBX System is now working as an LDAP Server. You can store contact information in the PBX directly. Users can connect an IP phone to PBX via LDAP, and query the contact information from IP phone directly.

Set up LDAP Client

Auto Provision LDAP for IP Phones

You can configure the LDAP for IP phone via Auto Provisioning, which is more convenient and easy to operate.

Supported IP phones

This topic can be applied to the IP phones listed in Auto Provisioning - Supported Devices.

Prerequisites

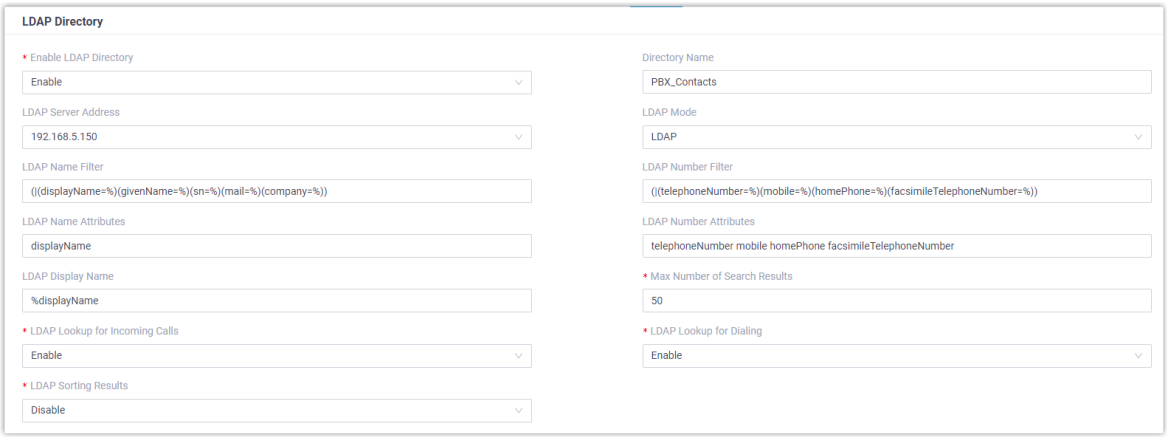
- Make sure the PBX version is 37.6.0.24 or later.
- You have set up the PBX as an LDAP server.
- The phone is connected to Yeastar P-Series PBX System via Auto Provisioning, and has been assigned with an extension.

  For more information, see the following topics:

  - Auto Provision IP Phones in Local Network (PnP Method)
  - Auto Provision IP Phones in Local Network (DHCP Method)
  - Auto Provision IP Phones Remotely (RPS FQDN Method)
  - Auto Provision IP Phones Remotely (RPS Method)

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**, click  to edit the phone.
2. Under **Phone** tab, scroll down to the **LDAP Directory** section, set up the LDAP feature according to your needs.



Setting	Description	Example
Enable LDAP Directory	Enable or disable the LDAP directory feature.	Enable
Directory Name	Specify a name for the LDAP directory.	PBX_Contacts
LDAP Server Address	Enter the LDAP Server address of Yeastar P-Series PBX System.	192.168.5.150
LDAP Mode	Select the connection mode between the LDAP Server and the IP phone. **Note:** You can only select **LDAP** when using a local host.	LDAP
LDAP Name Filter	Specify the name attributes for LDAP contact name lookup. **Note:** • The `*` symbol in the filter stands for any character. • The `%` symbol in the filter stands for the entering string used as the prefix of the filter condition.	(|(displayName=%)(givenName=%) (sn=%)(mail=%)(company=%))
LDAP Number Filter	Specify the number attributes for LDAP searching. **Note:** • The `*` symbol in the filter stands for any character.	(|(telephoneNumber=%)(mobile=%) (homePhone=%)(facsimileTelephoneNumber=%))

Setting	Description	Example
	• The % symbol in the filter stands for the entering string used as the prefix of the filter condition.	
LDAP Name Attributes	Specify the name attributes of each record to be returned by the LDAP Server. The user can configure multiple name attributes separated by space.	displayName
LDAP Number Attributes	Specify the number attributes of each record to be returned by the LDAP Server. The user can configure multiple number attributes.	telephoneNumber mobile homePhone
LDAP Display Name	Specify the display name of the contact record displayed on the LCD screen. **Note:** This parameter must start with % symbol.	%displayName
Max Number of Search Results	Specify the maximum number of search results to be returned by the LDAP Server.	50
LDAP Lookup for Incoming Call	Enable or disable IP phone to perform an LDAP search when receiving an incoming call.	Enabled
LDAP Lookup for Callout	Enable or disable IP phone to perform an LDAP search when placing a call.	Enabled
LDAP Sorting Results	Enable or disable IP phone to sort out search results in alphabetical and numerical order.	Enabled

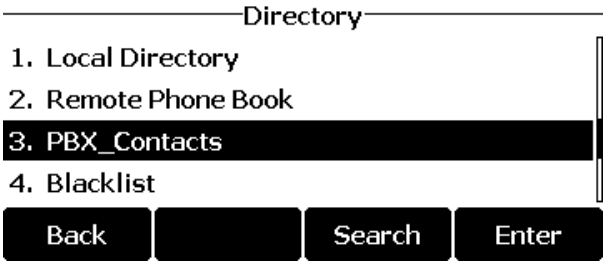
3. Click **Save**.

   The page returns to **Auto Provisioning > Phones**.

4. Click beside the phone to reprovision the settings.
5. In the pop-up dialog box, click **OK**.

Result

You can now query the contact information from IP phone on **Menu > Directory**.



Related information

Auto Provision Function Keys for Phones

Manual Configuration Examples

LDAP Configurations on Yealink Phones

This topic takes the Yealink SIP-T53W IP phone with a firmware version of 93.85.0.5 to describe how to configure LDAP on Yealink IP phones.

Configuration example

The example configurations are set according to default settings of Yeastar P-Series PBX System LDAP Server. You can use the following settings as a starting point and adjust the filter and display attributes according to your needs.

Prerequisites

You have set up the PBX as an LDAP server.

Procedure

1. Log in to the Yealink phone web interface, go to **Directory > LDAP**.
2. Turn on the **LDAP Enable** feature switch, and enter the desired values in the corresponding fields.

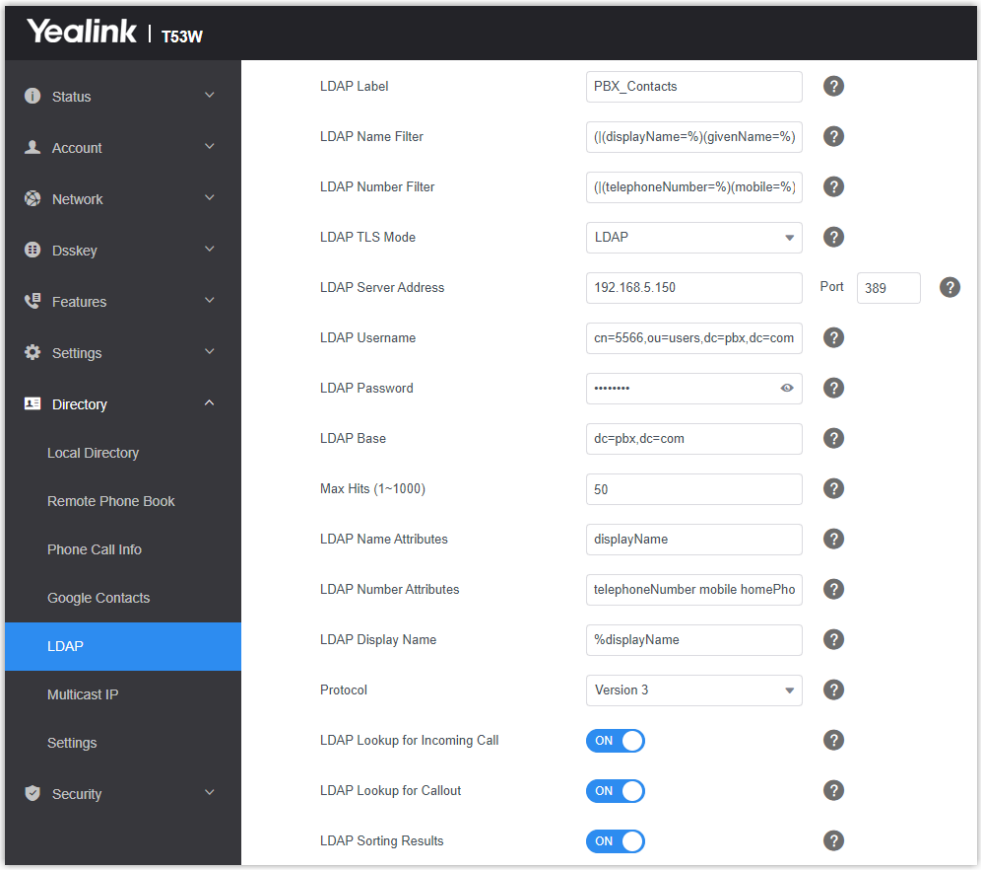


Table 12.

Setting	Description	Example
LDAP Label	Specify the name of LDAP phonebook.	PBX_Contacts
LDAP Name Filter	Specify the name attributes for LDAP contact name lookup. **Note:** • The * symbol in the filter stands for any character. • The % symbol in the filter stands for the entering string used as the prefix of the filter condition.	(|(displayName=%)(givenName=%) (sn=%)(mail=%)(company=%))

Setting	Description	Example
LDAP Number Filter	Specify the number attributes for LDAP searching. **Note:** • The `*` symbol in the filter stands for any character. • The `%` symbol in the filter stands for the entering string used as the prefix of the filter condition.	(|(telephoneNumber=%)(mobile=%)(homePhone=%)(facsimileTelephoneNumber=%)))
LDAP TLS Mode	Specify the connection mode between the LDAP Server and the IP Phone.	LDAP
LDAP Server Address	Enter the LDAP Server address of Yeastar P-Series PBX System.	192.168.5.150
Port	Enter the LDAP Server port.	389
LDAP Username	Enter the username to log in to the LDAP Server. **Note:** Obtain the username from PBX on **Contacts > LDAP Server > LDAP Credentials > LDAP Account Username**.	cn=5566,ou=users,dc=pbx,dc=com
LDAP Password	Enter the password to log in to the LDAP Server. **Note:** The password is the registration password of the user extension.	Regpwd123
LDAP Base	Enter the **Base DN** obtained from PBX, which is used as the LDAP search base.	dc=pbx,dc=com

Setting	Description	Example
Max Hits (1~1000)	Specify the maximum number of search results to be returned by the LDAP Server.	50
LDAP Name Attributes	Specify the name attributes of each record to be returned by the LDAP Server. The user can configure multiple name attributes separated by space.	displayName
LDAP Number Attributes	Specify the number attributes of each record to be returned by the LDAP Server. The user can configure multiple number attributes.	telephoneNumber mobile homePhone
LDAP Display Name	Specify the display name of the contact record displayed on the LCD screen. **Note:** This parameter must start with % symbol.	%displayName
Protocol	The LDAP protocol version. Yeastar P-Series PBX System uses Version 3.	Version 3
LDAP Lookup for Incoming Call	Enable or disable IP phone to perform an LDAP search when receiving an incoming call.	Enabled
LDAP Lookup for Callout	Enable or disable IP phone to perform an LDAP search when placing a call.	Enabled
LDAP Sorting Results	Enable or disable IP phone to sort out search results in alphabetical and numerical order.	Enabled

3. Click **Confirm** to apply the changes.

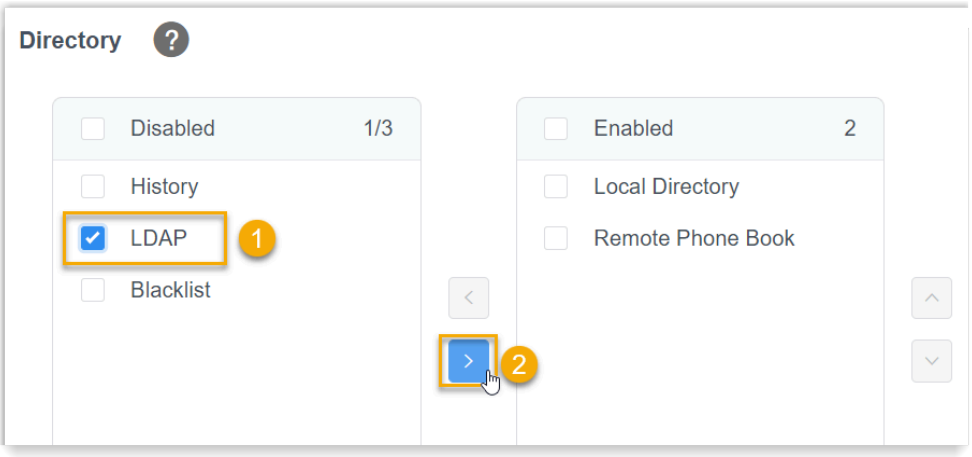
Result

Now you can directly check the contact information stored in the PBX from the IP phone.

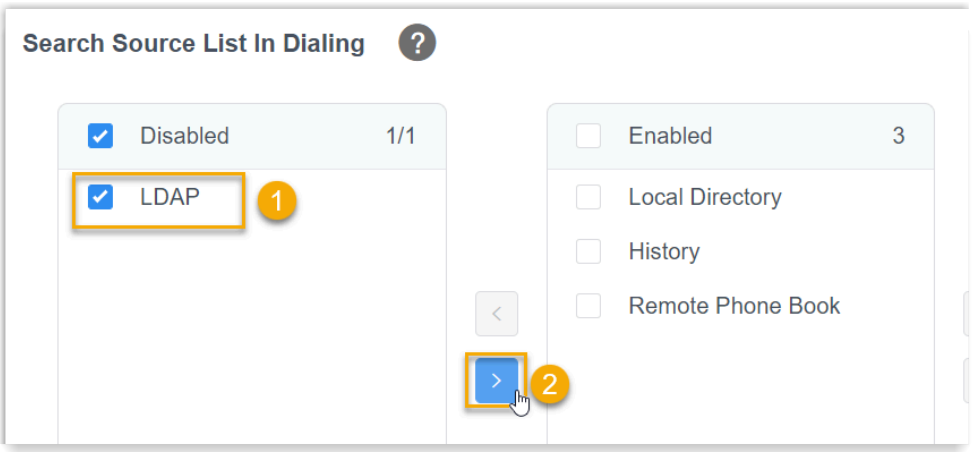
Search contacts via Directory

Enable LDAP directory on Yealink phone

1. Log in to the Yealink phone web interface, go to **Directory > Settings**.
2. In the **Directory** section, add **LDAP** from the **Disabled** box to the **Enabled** box.



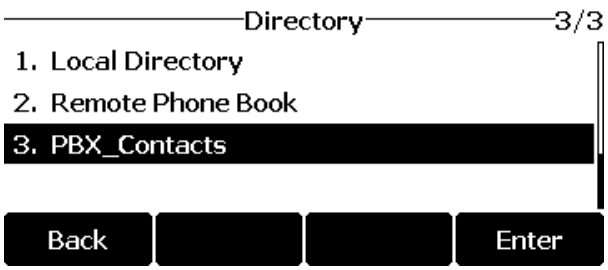
3. **Optional:** In the **Search Source List In Dialing** section, add **LDAP** from the **Disabled** box to the **Enabled** box.



4. Click **Confirm**.

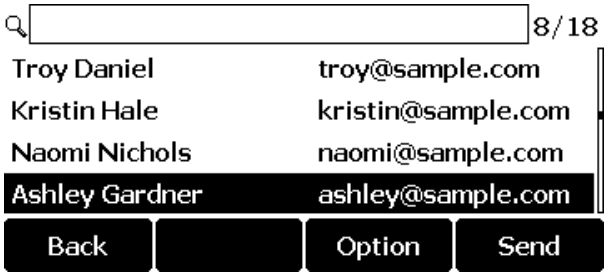
Search LDAP Contacts

1. On the IP phone, press **Directory** and enter the LDAP phonebook.



2. Search the contact name or number using the keypad.

   The contacts whose name or phone number matching the characters entered will appear on the phone screen.

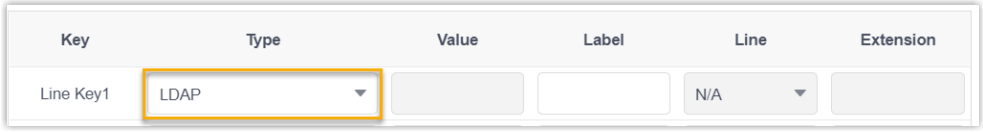


3. Press the navigation key to select the desired contact.
4. Press **Send** to call the contact.

Search contacts via LDAP key

Set an LDAP Key on Yealink Phone

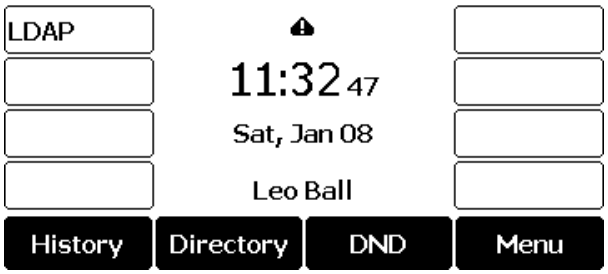
1. Log in to the Yealink phone web interface, go to **DssKey > Line Key** to configure a line key.
2. In the drop-down list of **Type**, select **LDAP**.



3. Click **Confirm**.

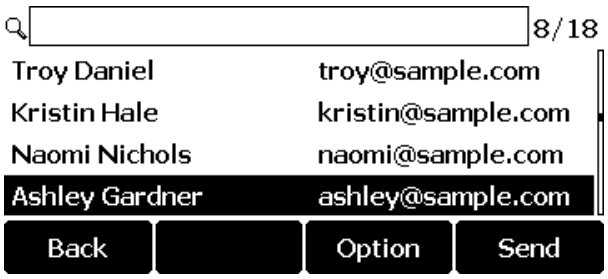
Search LDAP Contacts

1. Press the LDAP key to access the LDAP phonebook.



2. Search the contact name or number using the keypad.

   The contacts whose name or phone number matching the characters entered will appear on the phone screen.



3. Press the navigation key to select the desired contact.
4. Press **Send** to call the contact.

Organization

Organization Overview

Organizational structure is the group of rules, roles, relationships, and responsibilities that outline how your company's activities are directed to meet its goals. Yeastar P-Series PBX System provides Organization feature to help you organize employees by department based on their specific skills and corresponding function in the company, and enjoy easier administration with department-level control.

Organization vs Extension Group

Yeastar provides **Organization** feature and **Extension Group** feature to help you categorize and manage extensions.

The following contents compare the advantages and differences between the two features.

Organization

Organization feature is used to define a hierarchy within a company, ideal for large companies with many departments and for those companies that attach more importance to separation of duties.

Organization feature helps you achieve the followings:

- Multi-layer departments, displayed in hierarchical tree structure.
- Flexible adjustments for departments, adapting to a changing business environment.
- Clear-cut reporting structure, clarifying the reporting relationships across the company and every individual's role and responsibilities.

Extension Group

Extension Group feature is used to categorize extensions with common function or purpose into the same group, ideal for companies that attach more importance to call management.

Extension Group feature helps you achieve the followings:

- Same-layer groups, displayed in strict alphabetical order.

- Group permission presets, realizing granular control over users' call permission.
  - Preset permission on a per group basis: Preset different permissions for groups with different calling needs.
  - Preset permission on a per user role basis: Split users into Manager/User/Custom roles and implement role-based permission assignment.

For more information about extension group, see Extension Group Overview.

We provide the following figures to visualize the difference between Organization and Extension Group in display:



Organization application

After you enable Organization feature and set up departments, the followings can be achieved:

- On Linkus clients, extension users can search for and find colleagues by departments.

> **Note:**
> Make sure Linkus clients meet the following version requirements:
> - Linkus iOS version: 4.8.5 or later.
> - Linkus Android version: 4.8.6 or later.

◦ Linkus Web Client: 37.7.0.16 or later.

- On PBX web portal, you can implement department-based control over users' permission:
  - Control the visibility to specific extensions or company contacts.
  - Control the access to all the call features and Call Center Console.

> **Note:**
> The access to Operator Panel is under the control of Extension Group, be the Organization feature enabled or not.

Related information

Enable or Disable Organization Management

Enable or Disable Organization Management

You can enable or disable organization management feature based on your plan for company structure.

Enable organization management

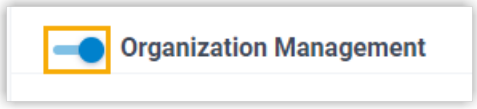
To group extension users into departments, you need to enable the **Organization Management** feature.

Prerequisites

The version of Yeastar P-Series PBX System is 37.7.0.16 or later.

Procedure

1. Log in to PBX web portal, go to **PBX Settings > Preferences**.
2. Turn on the option **Organization Management**.



3. In the **Company Name** field, enter your company name. The name will be used as the root organization.

> **Note:**

> If you have set up company information, the pre-defined company name is automatically synchronized here.

4. Click **Save** and **Apply**.

Result

The **Organization Management** feature is enabled.

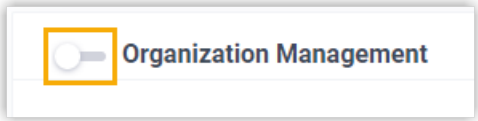
What to do next

Create departments.

Disable organization management

Procedure

1. Log in to PBX web portal, go to **PBX Settings > Preferences**.
2. Turn off the option **Organization Management**.



3. Click **Save** and **Apply**.

Result

The **Organization Management** feature is disabled, which bring changes to the way that extensions are displayed and permissions that extensions have.

- On PBX web portal, the organizational tree and organizational configuration page are hidden; On Linkus clients, extension users are arranged in extension groups.
- Extension users have no access to the features that are granted to organizations.

Set up Organizations

Organizational structure helps your company stay organized, improve communication and collaboration productively. This topic describes how to set up organizations.

Limitation

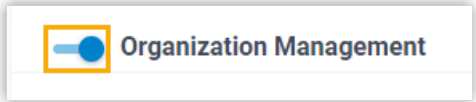
Type	P520	P550	P560	P570
Layers of Departments	15	15	15	15
Number of Departments	20	50	200	500

Prerequisites

The version of Yeastar P-Series PBX System is 37.7.0.16 or later.

Step 1. Enable Organization Management

1. Log in to PBX web portal, go to **PBX Settings > Preferences**.
2. Turn on the option **Organization Management**.



3. In the **Company Name** field, enter your company name. The name will be used as the root organization.

> **Note:**
> If you have set up company information, the pre-defined company name is automatically synchronized here.

4. Click **Save** and **Apply**.

Step 2. Create departments

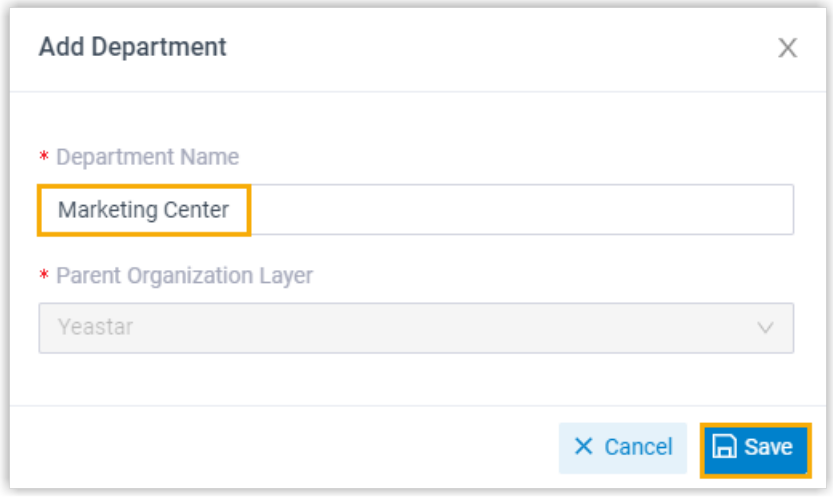
1. Go to **Extension and Trunk > Extension > Organization**.

   The root organization (namely the company name) is displayed.



2. Click + beside the root organization.

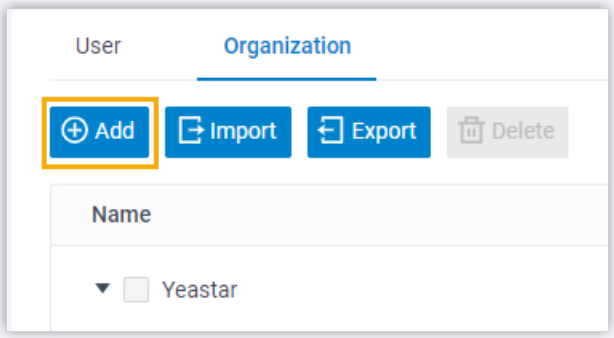
3. In the pop-up window, configure the following information, then click **Save**.



- **Department Name**: Enter a department name.
- **Parent Organization Layer**: The root organization is automatically filled in.

Result

- The department is created. You can create more departments as the instructions provided above. In this way, the parent organization is auto filled instead of manually selected.

> **Tip:**
> To select parent organization at you will when creating departments, you can click **Add** to create departments.
>
> 
>

- On Linkus clients, users can see all the departments. To restrict users from viewing specific departments, see Set up Extension Visibility.

What to do next

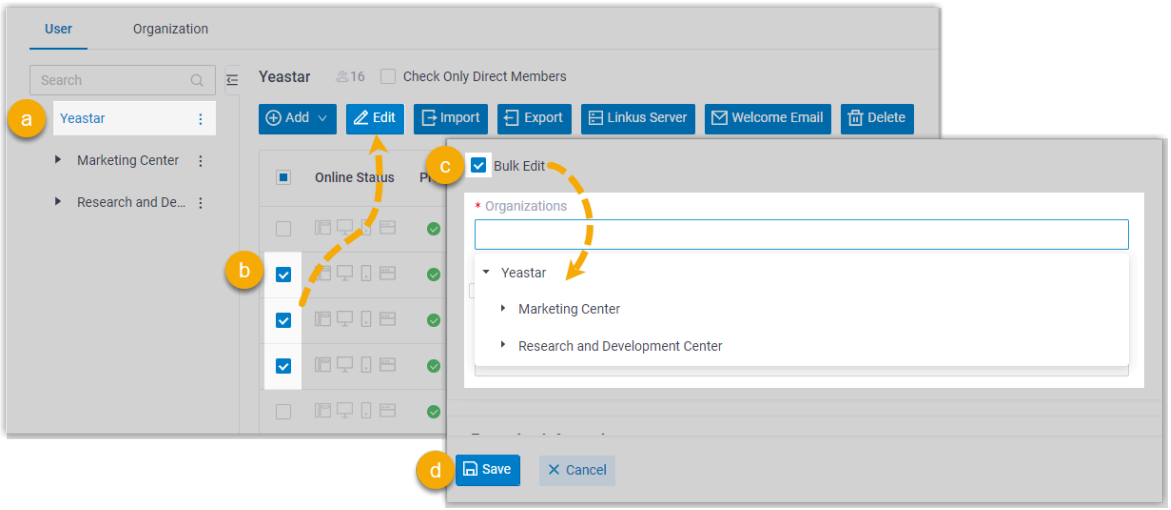
Add Users to Organizations.

Add Users to Organizations

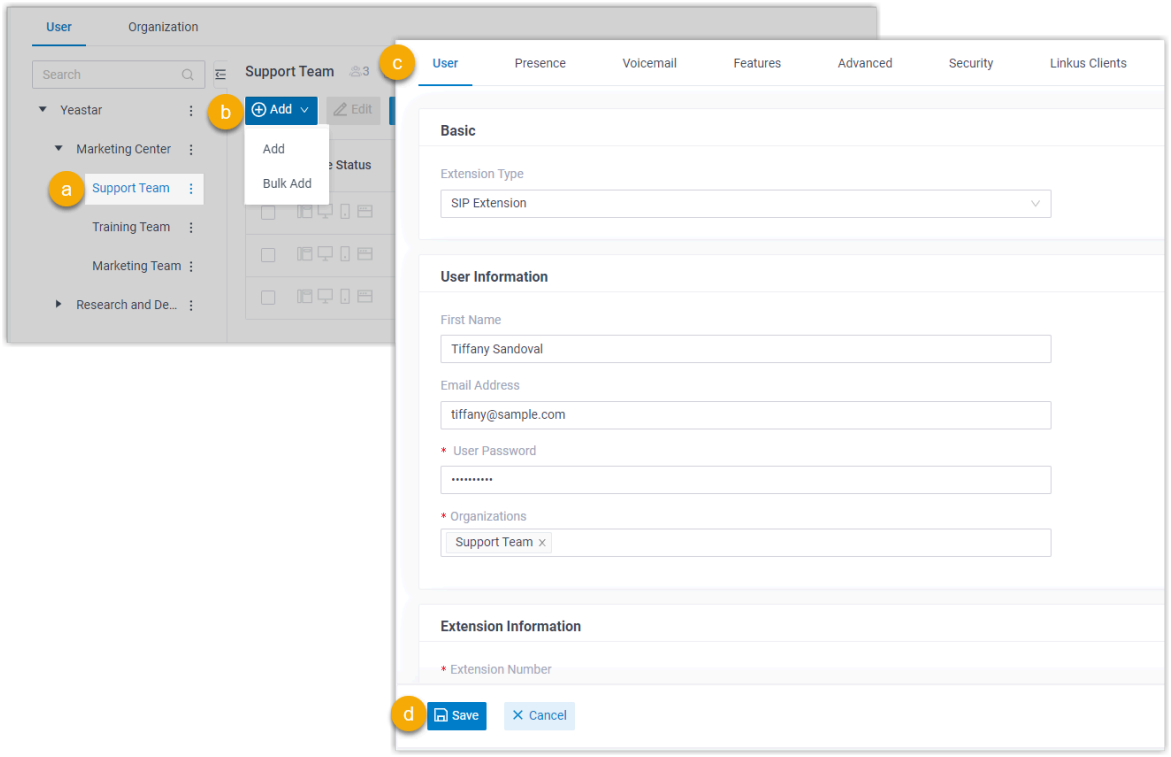
After setting up organizations, you need to group users into departments. This topic describes how to add users to departments.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension > User**.
2. To add existing users to an organization, do as follows:



   a. On the left organizational tree, click root organization.
   b. On user list, select the checkboxes of desired extensions, then click **Edit**.
   c. In the **User Information** section, select the checkbox of **Bulk Edit** for organizations, then select desired departments.
   d. Click **Save** and **Apply**.
3. To add new users to an organization, do as follows:



a. On the left organizational tree, click a department.
b. Click **Add**, then select **Add** to add an extension.
c. Configure the extension as needed.

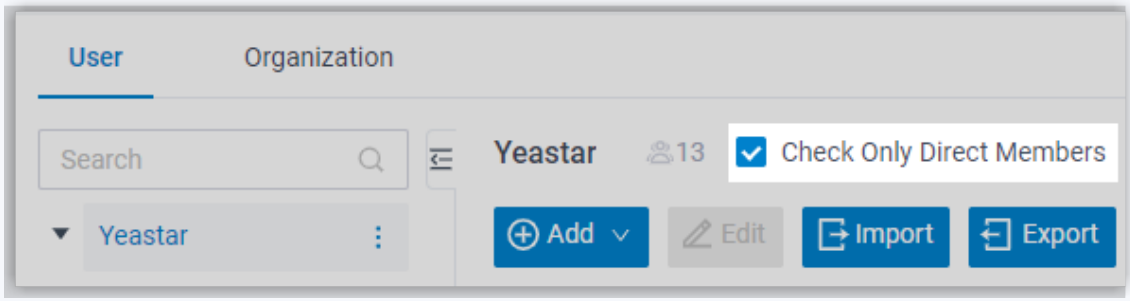
> **Note:**
> **Organization** is auto filled with the one that you have selected.

d. Click **Save** and **Apply**.

Result

Users are added to the specified departments. You can click a department to check all the associated members.

> **Note:**
> By default, when you click on a department, all the users within the department are displayed, be they belong to the parent department or the sub-departments. To hide the users of sub-departments, select the checkbox of **Check Only Direct Members**.



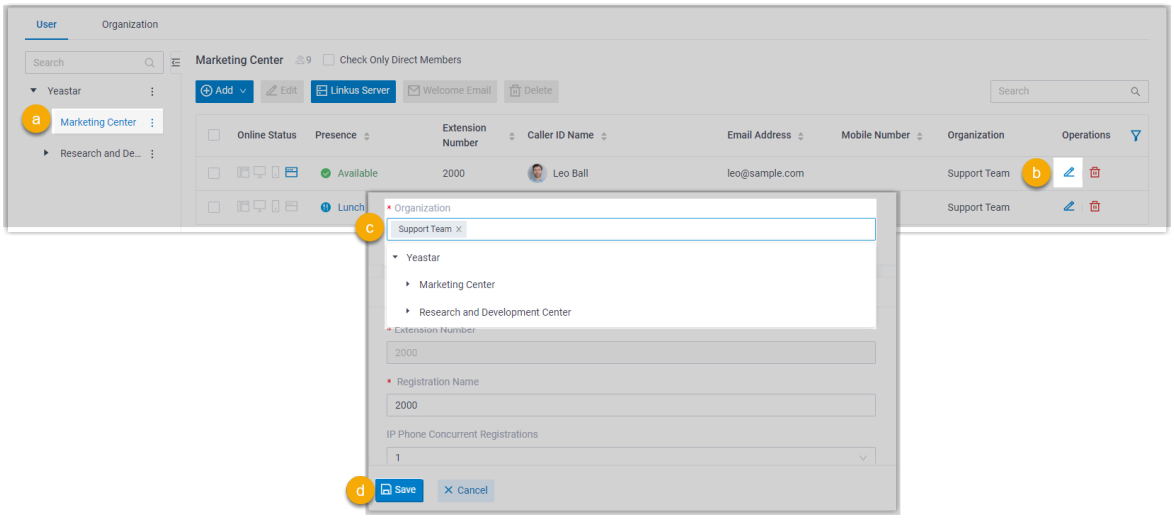
Manage Users within Organizations

This topic describes how to change users' departments or remove users from departments when there are job changes of employees.

Change users' departments

You can change users' departments when some of them transfer jobs at your company.

1. Log in to PBX web portal, go to **Extension and Trunk > Extension > User**.
2. To change a user's department, do as follows:



   a. On the left organizational tree, click a desired department.

      All the extensions within the department are displayed.

   b. Click beside a desired extension.

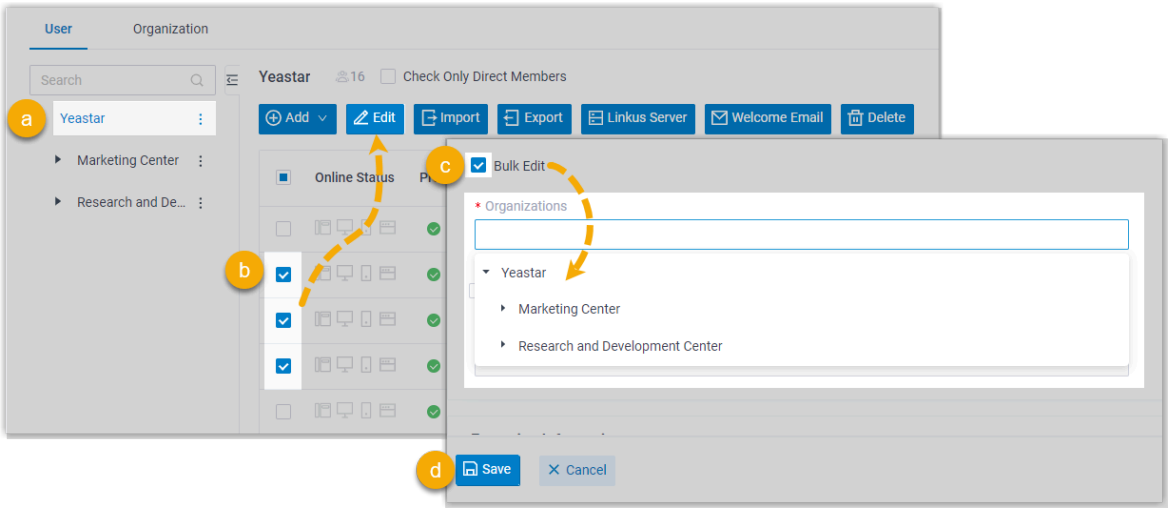
   c. In the **Organization** field , change department as needed.

> **Note:**
> An extension must be associated with at least one department.

d. Click **Save** and **Apply**.

3. To change multiple users' departments, do as follows:

> **Note:**
> This is suitable for changing multiple users to the same department. To change multiple users to different departments, you need to proceed one by one as step2 instructs.



a. On the left organizational tree, click the root organization.

   All the extensions within the organization are displayed.

b. Select the checkboxes of desired extensions, then click **Edit**.

   The departments to which the extensions belong are cleared.

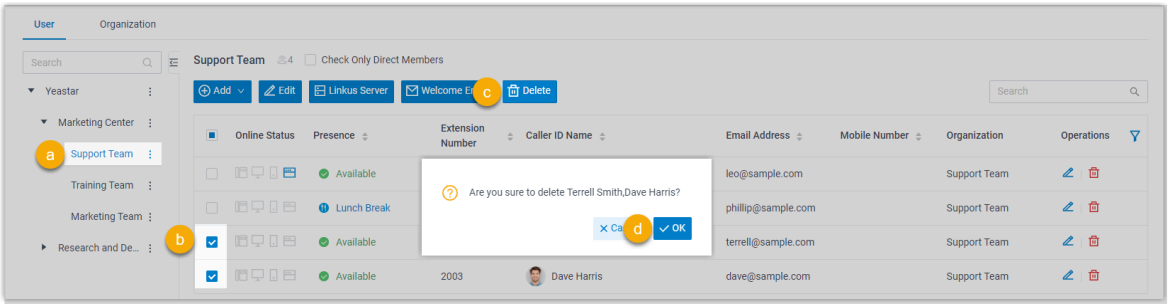
c. Select the checkbox of **Bulk Edit** for organization, then reselect departments.

d. Click **Save** and **Apply**.

Remove users from departments

You can remove users from departments when some of them leave their jobs.

1. Log in to PBX web portal, go to **Extension and Trunk > Extension > User**.
2. To remove users from the same department, do as follows:



a. On the left organizational tree, click a desired department.

   All the extensions within the department are displayed.

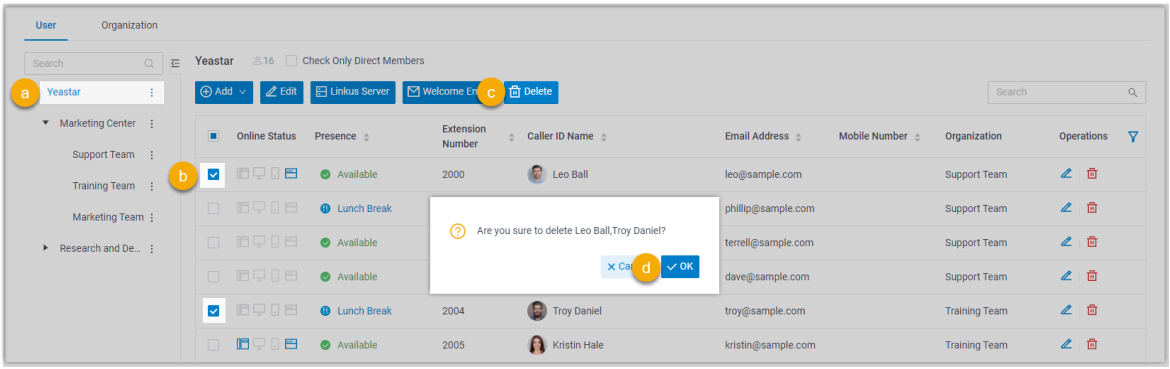
b. Select the checkboxes of desired extensions, then click **Delete**.

c. In the pop-up window, click **OK**.

d. Click **Apply**.

   The selected extensions are deleted from the system.

3. To remove users from different departments, do as follows:



a. On the left organizational tree, click the root organization.

   All the extensions within the organization are displayed.

b. Select the checkboxes of desired extensions, then click **Delete**.

c. In the pop-up window, click **OK**.

d. Click **Apply**.

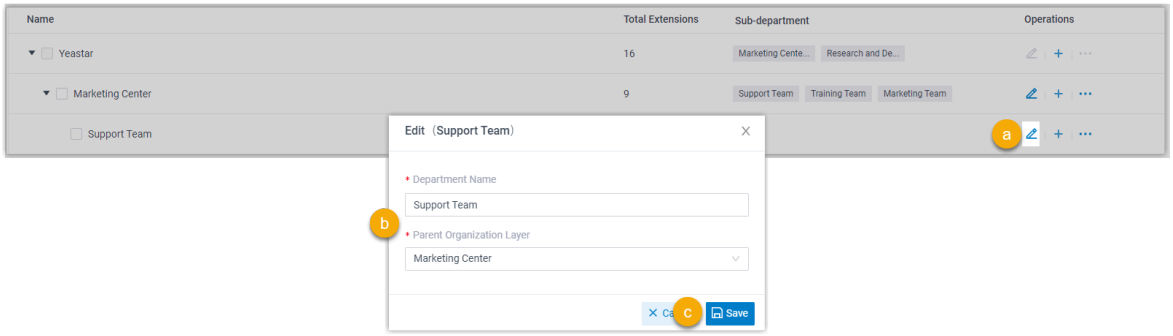
   The selected extensions are deleted from the system.

Manage Organizations

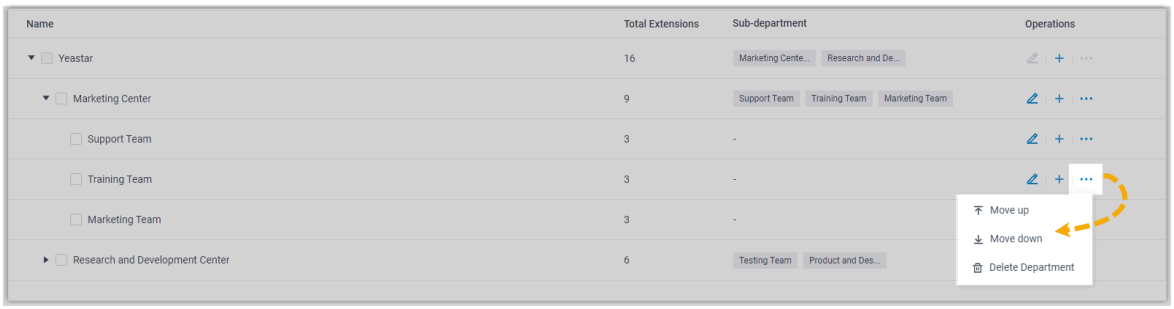
To remain competitive or adapt to changes in the company, you may change organizational structure. This topic describes how to manage the organizations on PBX web portal.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension > Organization**.
2. To rename department or change parent organization, do as follows:



   a. Click ✎ beside the desired department.
   b. In the pop-up window, rename department or change parent organization layer.
   c. Click **Save**.
3. To adjust the order of departments, click •••, then select **Move Up** or **Move Down** to adjust the order.

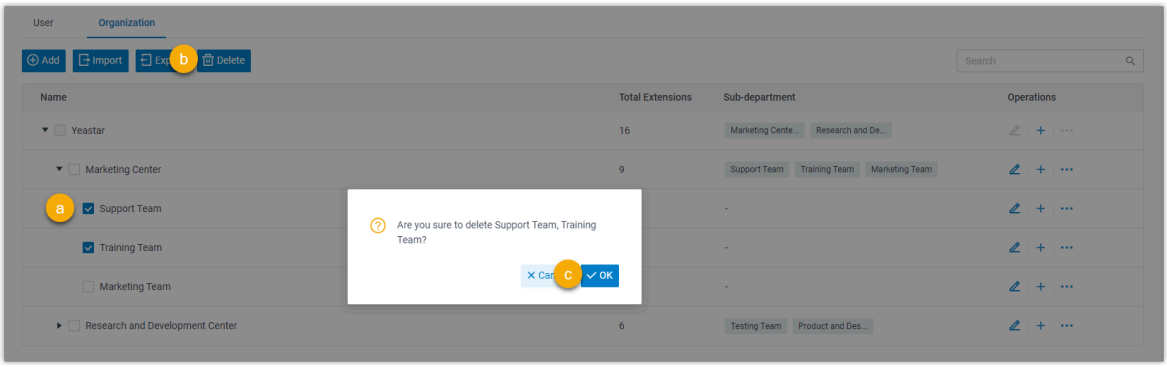


   On PBX web portal and Linkus clients, departments are displayed in the new order.
4. To delete departments, do as follows:

> **Note:**
> - If there are sub-departments under the departments that you want to delete, you need to delete the sub-departments first.
> - After you delete departments, the extensions within the departments will not be deleted, but they have no access to the features that are granted to the departments, and they will be grouped into root organization if they only belong to the departments deleted.

   a. Select the checkboxes of desired departments, then click **Delete**.

b. In the pop-up window, click **OK**.



Export and Import Organizations

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

Export all organizations

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

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

   A CSV file is saved to your computer. To check and edit parameters in the CSV file, see Organization Parameters.

Import organizations

We recommend that you export organization 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 Organization Parameters.

Procedure

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

   The organization data in the CSV file will be displayed in the **Organization** list.

Related information

Import and Export -FAQ

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 colleague within a group, and makes it possible for authorized users to 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 and usage on Operator Panel and Extension Page. 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.
- **User**: Assign the user type to ordinary members. Any time you add members to a group, they are assigned with 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	√	×

Module	Permission	Manager	User
	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	×	×
	Show Company Contacts Matching Results **Note:** Once enabled, the contacts matching results will be displayed on Operator Panel call panel, regardless of users' visibility permission for company contacts.	×	×
Extension Page	Call distribution management (Redirect, Transfer)	√	×
	Pick up or hang up other extension's calls	√	×
	Call monitoring operations (Listen, Whisper, Barge-in)	√	×
	Call parking operations (Park, Retrieve)	√	×
	Show Company Contacts Matching Results **Note:** Once enabled, the contacts matching results will be displayed on Extension Page, regardless of users'	×	×

Module	Permission	Manager	User
	visibility permission for company contacts.		

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.

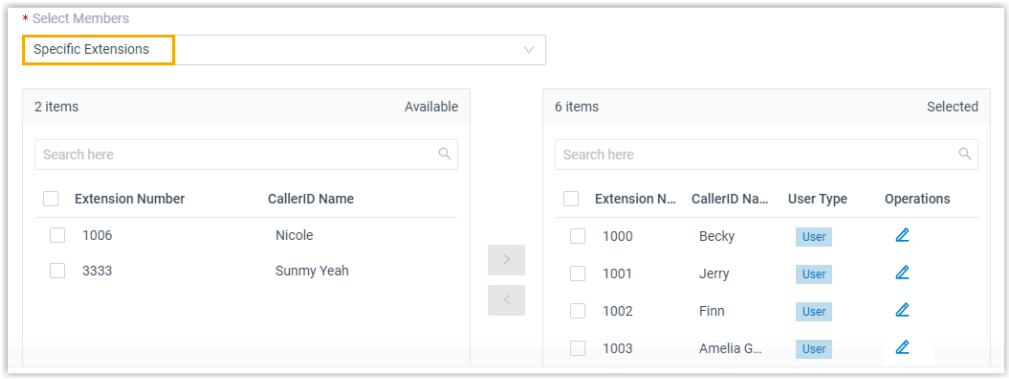
Create an Extension Group

This topic describes how to create an extension group.

Procedure

1. Log in to PBX web 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.



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. Click **Save**.

Result

- The extension group is displayed on **Extension Group** list.
- No one can view the group on Linkus clients. To allow specific users to view the group, see Set up Extension Visibility.

Manage Extension Groups

This topic describes how to edit or delete extension groups.

Edit an extension group

1. Log in to PBX web 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 web 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 web 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 web 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

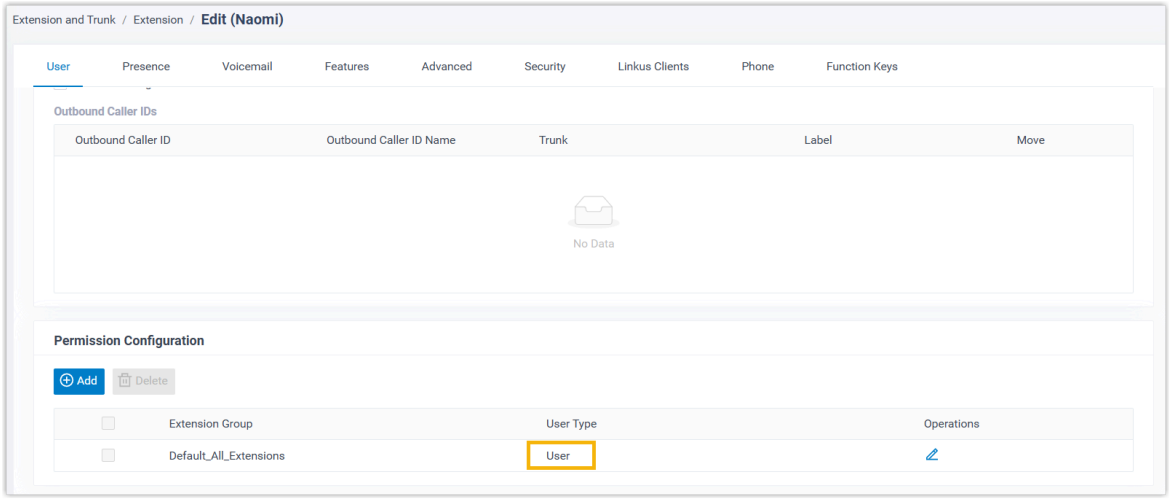
The member's user type and permissions in the group are updated.

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 web portal, go to **Extension and Trunk > Extension**, click beside desired extension.
2. In the **User** tab, scroll down to the **Permission Configuration** 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.



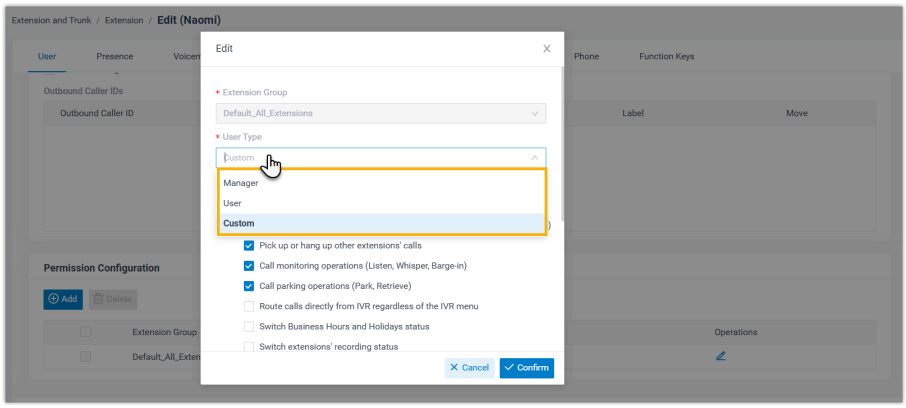
Change a member's user type in multiple groups

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 web portal, go to **Extension and Trunk > Extension**, click beside desired extension.

2. In the **User** tab, scroll down to the **Permission Configuration** 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**.
3. Repeat **Step4** to assign user types for the extension in more groups.
4. 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 web portal, go to **Extension and Trunk > Extension Group**, edit the desired extension group.
2. Click **Group Permissions** tab.

   You can view the permissions that are granted to **Manager** and **User** in the group.
3. To change permissions, do as follows:
   a. Select or unselect the checkboxes of corresponding permissions for **Manager** and **User**.
      - **Allow Using Operator Panel**: Allow members to perform the specified operations to control calls on Operator Panel.
      - **Allow Call Operations in the Extension page**: Allow members to perform the specified operations to control calls from the Extension page of Linkus Desktop Client or Linkus Web Client.

        > **Note:**
        > To achieve this, you need to upgrade PBX to version 37.16.0.25 or later and extension users need to upgrade Linkus Desktop Client to version 1.6.0 or later.

   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

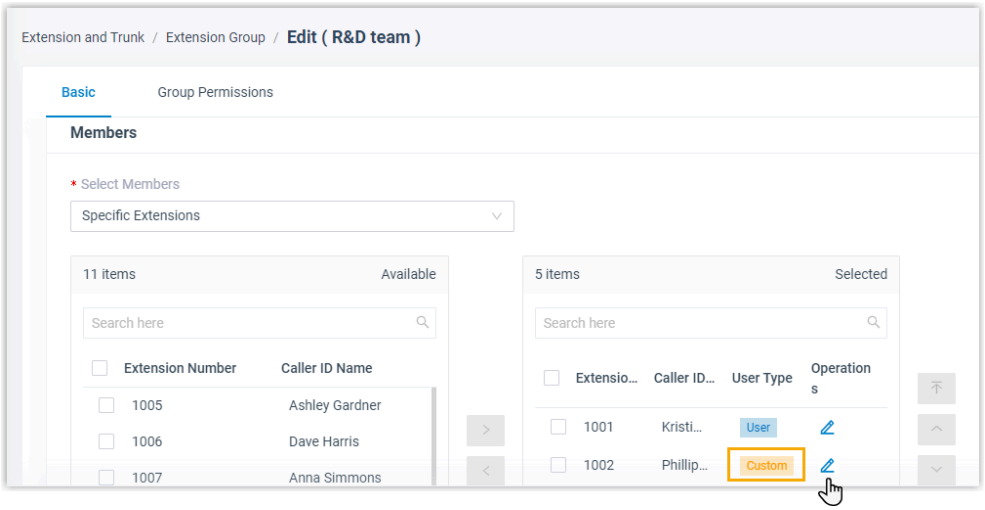
If you want to change members' user types to **Manager** or **User** in the group, see Assign a default user type to a group member.

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 web 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

Auto Provisioning is a time-saving feature that helps you to manage and deploy IP phones and gateways centrally on Yeastar P-Series PBX System. The process of configuring and managing IP phones and gateways is simplified, 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.

Auto Provisioning methods

Yeastar P-Series PBX System supports four Auto Provisioning methods, you can select a method to provision your IP phones and gateways according to your network environment.

PnP (Plug and Play)

PnP method supports auto provisioning IP phones and gateways that are located in the same LAN subnet as the PBX.

For more information, see Auto Provision IP Phones in Local Network (PnP Method) and Auto Provision Yeastar TA FXS Gateways (PnP Method).

DHCP Option 66

DHCP method supports auto provisioning IP phones and gateways that are located in the same local network as the PBX (same LAN subnet or different LAN subnet).

For more information, see Auto Provision IP Phones in Local Network (DHCP Method) and Auto Provision Yeastar TA FXS Gateways (DHCP Method).

RPS

RPS method supports auto provisioning remote IP phones via public IP address or Yeastar FQDN.

Note:

> Yeastar TA FXS gateways do not support RPS Auto Provisioning method.

For more information, see Auto Provision IP Phones Remotely (RPS Method) and Auto Provision IP Phones Remotely (RPS FQDN Method).

Provision Link

Provision Link method supports auto provisioning remote IP phones/gateways that don't support RPS Auto Provisioning method via public IP address or Yeastar FQDN.

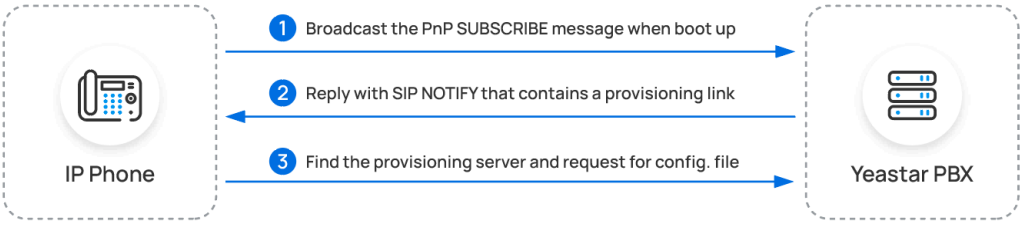
> **Note:**
> Cisco IP phones do not support Provision Link Auto Provisioning method.

For more information, see Auto Provision IP Phones Remotely (Provision Link Method), Auto Provision IP Phones Remotely (Provision Link - FQDN Method), Auto Provision Yeastar TA FXS Gateway (Provision Link Method), and Auto Provision Yeastar TA FXS Gateway (Provision Link FQDN Method).

How Auto Provisioning works

This section introduces how the Auto Provisioning methods work with IP phones and the PBX, which can help you understand the operating principle and locate the Auto Provisioning problem rapidly.

PnP Provisioning



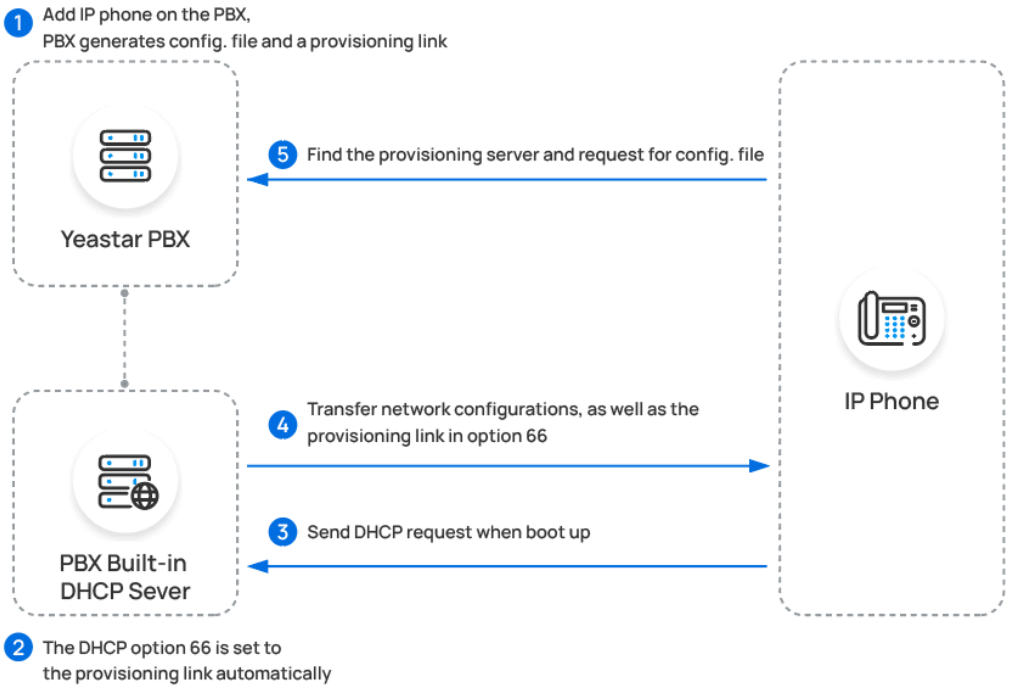
DHCP Provisioning

You can directly use the PBX as a DHCP server, or use a third-party DHCP server that supports DHCP option 66.

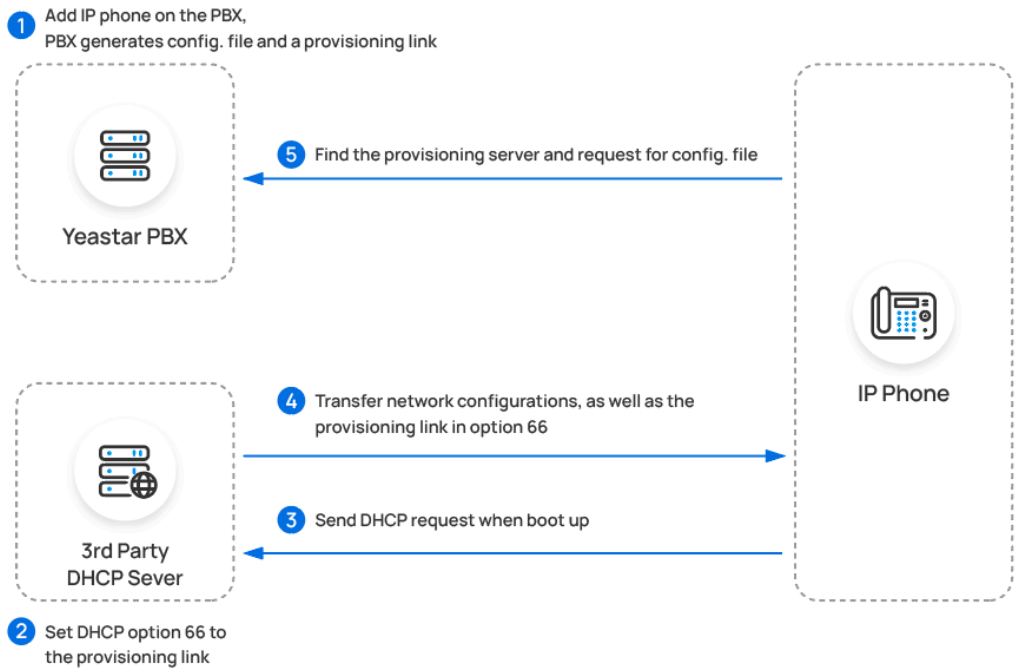
> **Note:**

The DHCP server in the PBX supports only one DHCP address pool.

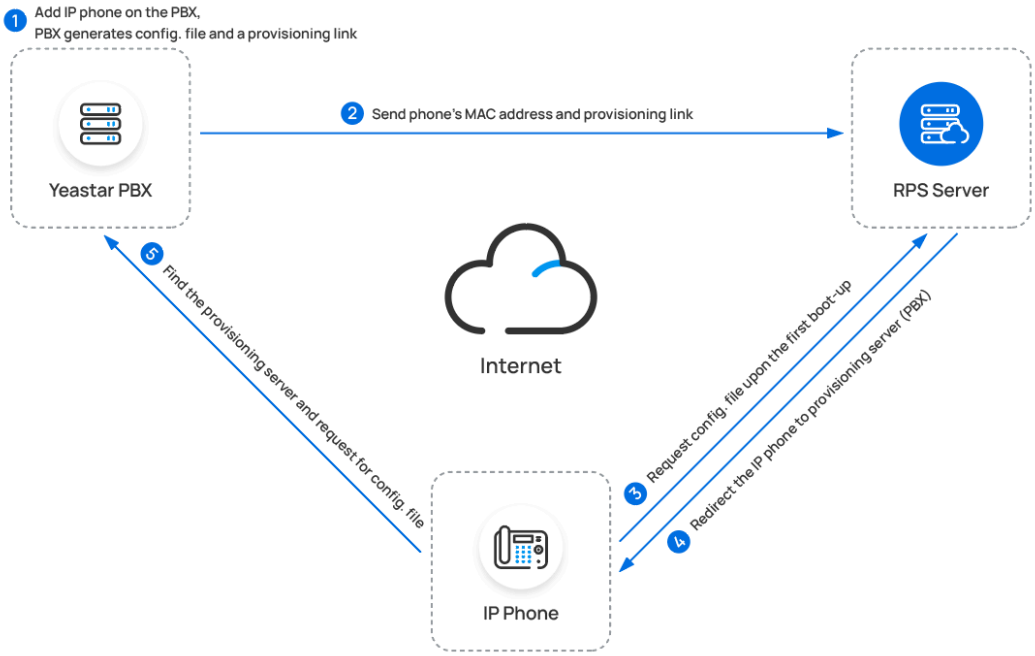
Using the PBX as a DHCP server



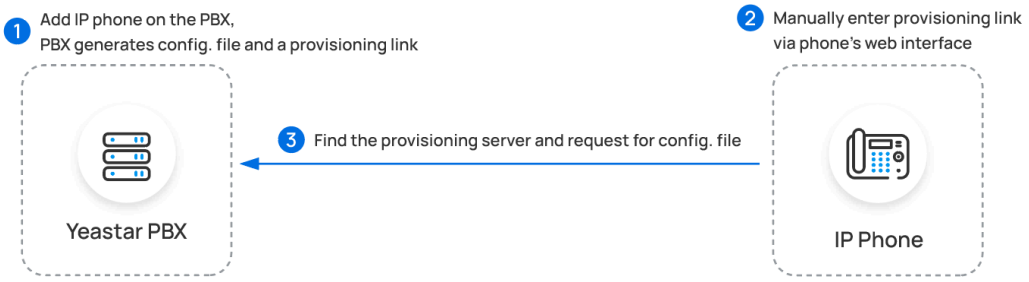
Using a third-party DHCP server



RPS Provisioning



Provision Link



Related information

IP Phone Configuration Guides

Provision IP Phones

Auto Provision IP Phones in Local Network (PnP Method)

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

> **Note:**
> This topic describes how to provision an IP phone and assign a user's extension to the phone. If you want to set up a hot desking phone via auto provisioning, see Set up a Hot Desking Phone.

Supported IP phones

This topic can be applied to all the IP phones listed in Auto Provisioning - Supported Devices.

Prerequisites

- The IP Phone and PBX must be in the same LAN subnet.
  - **Example: Same LAN subnet**

    IP: 192.168.5.150, Mask: 255.255.255.0

    IP: 192.168.5.170, Mask: 255.255.255.0
  - **Example: Different LAN subnet**

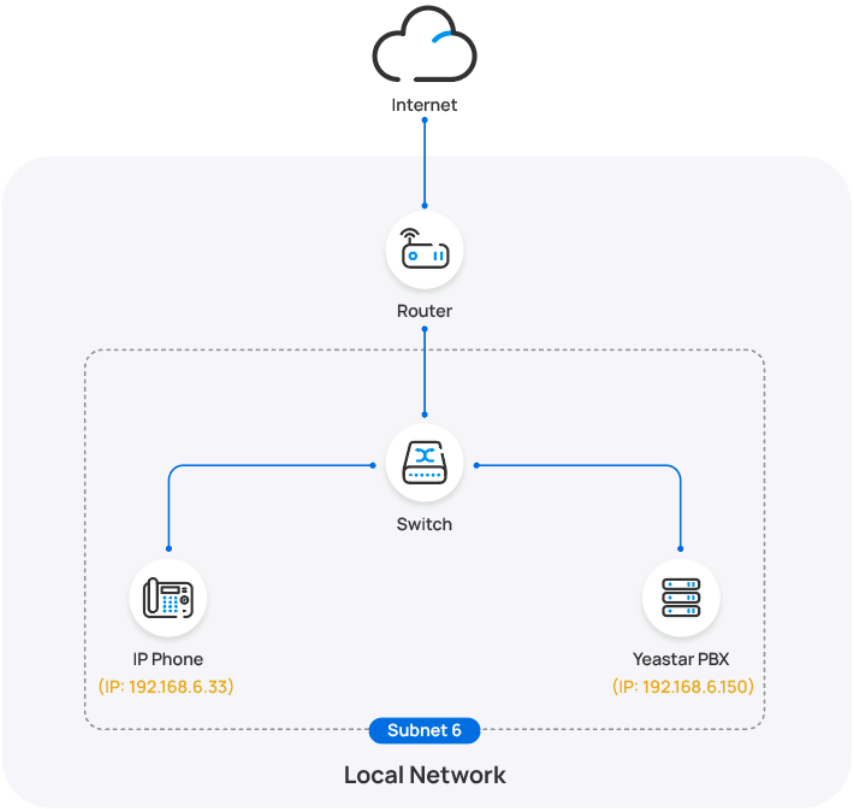
    IP: 192.168.5.150, Mask: 255.255.255.0

IP: 192.168.66.170, Mask: 255.255.255.0

- IP Phone MUST support PnP provisioning method.
- Make sure that you have downloaded the template for the desired phone model (Path: **Auto Provisioning > Resource Repository > Default Templates**).

Scenario

An IP phone (IP: 192.168.6.33) and the PBX (IP: 192.168.6.150) are deployed in the same LAN subnet 6.



Procedure

1. Power on the PBX first, then power on the IP phones.
2. RESET the IP phone if it is previously used.
3. Log in to PBX web portal, go to **Auto Provisioning > Phones**.

   The phone list displays all the discovered IP phones 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.

4. Click beside the desired phone.
5. In the **Options** section, configure the following settings:
   - **Template**: Select a desired template from the drop-down list.

     > **Note:**
     > The template provides configurations except extension assignment. You can select the default template corresponding to the phone model, or customize your own template.
     >
     > For more information, see Create a Custom Auto Provisioning Template.

   - **Provisioning Method**: Select **PnP (In the Office)**.

     A provisioning server URL is generated automatically and displayed on the web page.
6. In the **Assign Extension** section, assign an extension for the phone.

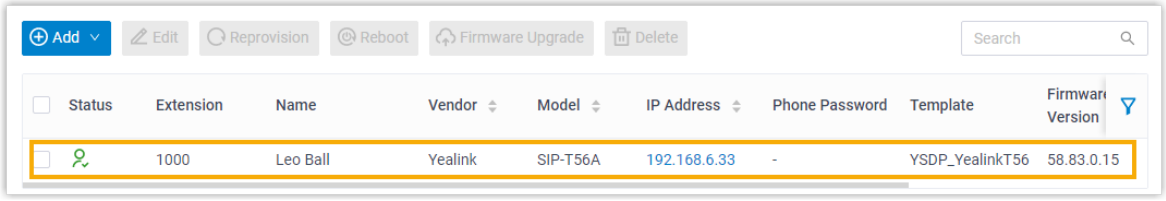
   > **Tip:**
   > If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other IP phone or gateway.
   > - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
   > - To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

7. Click **Save**.

Result

- The configurations will be automatically applied to the phone.
- The extension registration status of provisioned phones is displayed on **Auto Provisioning > Phones**.

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



Related information

Auto Provision IP Phones in Local Network (DHCP Method)
Auto Provision IP Phones Remotely (RPS FQDN Method)
Auto Provision IP Phones Remotely (RPS Method)
Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
Auto Provision IP Phones Remotely (Provision Link Method)
Modify a Provisioned Phone Settings
Auto Provision Function Keys for Phones

Auto Provision IP Phones in Local Network (DHCP Method)

For the IP phones that are located in different LAN subnet with the PBX or don't support PnP provisioning, you can provision the IP phones by DHCP method.

Note:
This topic describes how to provision an IP phone and assign a user's extension to the phone. If you want to set up a hot desking phone via auto provisioning, see Set up a Hot Desking Phone.

Supported IP phones

This topic can be applied to all the IP phones listed in Auto Provisioning - Supported Devices.

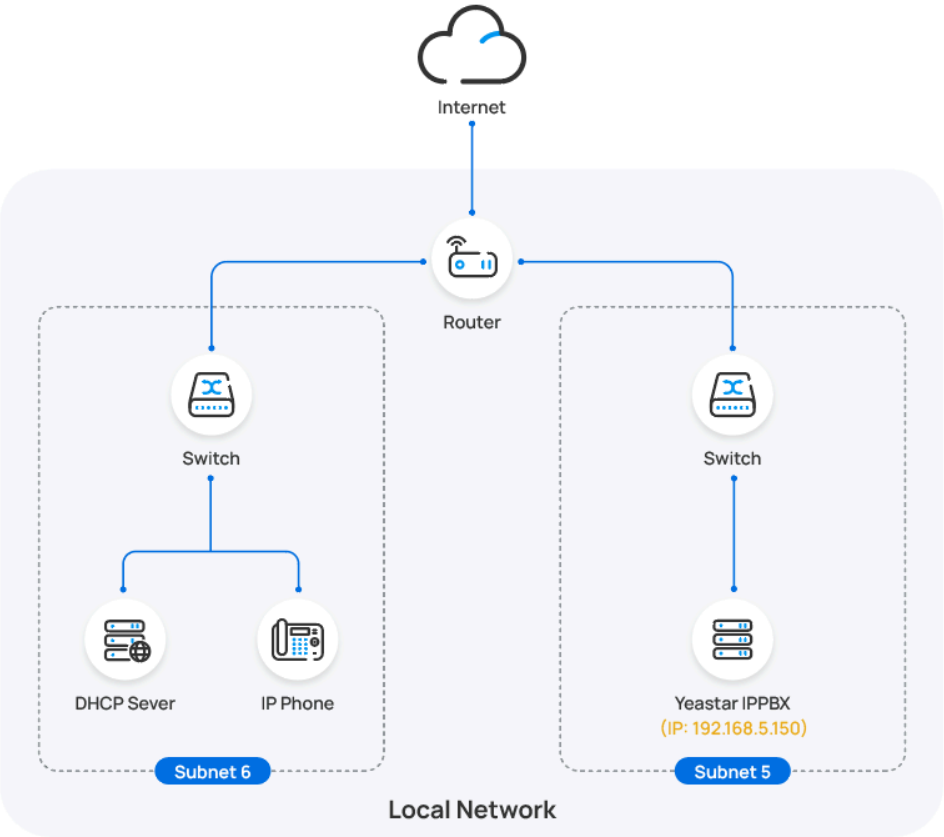
Prerequisites

- Make sure that there is only one DHCP server in the network where the IP phone is located, otherwise the IP phone may fail to obtain an IP address.
- Make sure that there is network connectivity between the subnet segments of the IP phone and the PBX server.

- DHCP provisioning is supported on the phone.
- Make sure that you have downloaded the template for the desired phone model (Path: **Auto Provisioning > Resource Repository > Default Templates**).
- Gather information of IP phone, including Vendor, Model, and MAC address.

Scenario

An IP phone and a DHCP server are deployed in subnet 6, while the PBX (IP: 192.168.5.150) is deployed in subnet 5.



Procedure

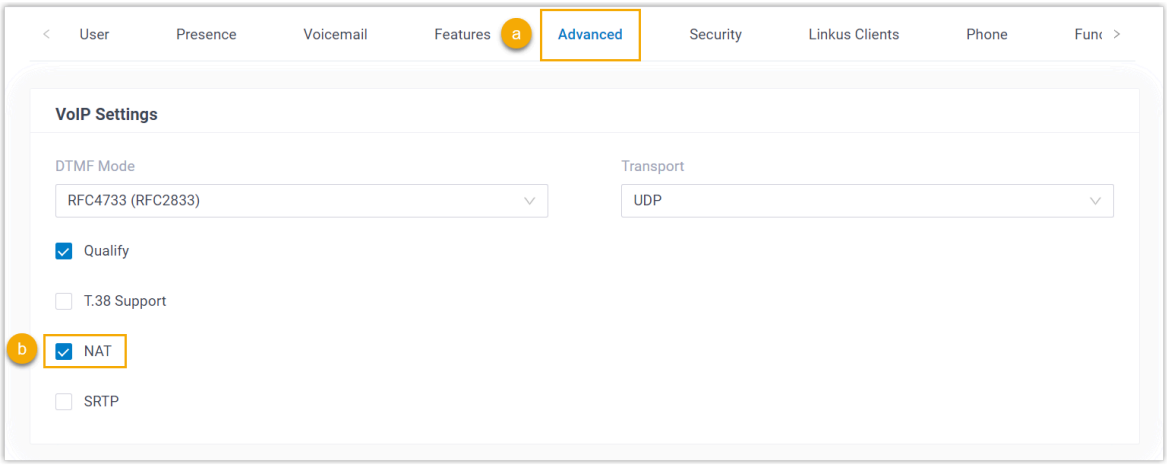
Step1. Set a remote extension

Step2. Generate configuration file for an IP phone on the PBX

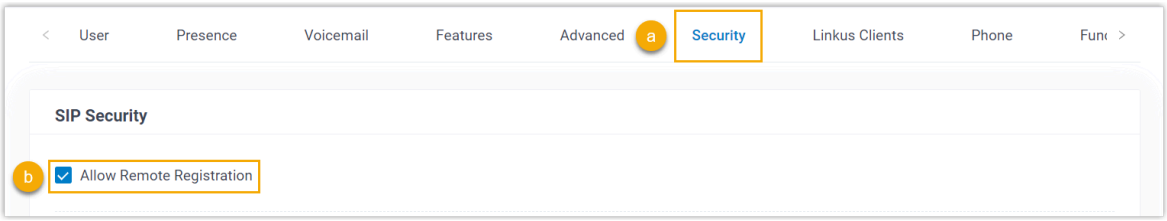
Step3. Set up a DHCP option 66

Step1. Set a remote extension

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the extension to be assigned.
2. Click **Advanced** tab, select the checkbox of **NAT** in the **VoIP Settings** section.



3. Click **Security** tab, select the checkbox of **Allow Remote Registration** in the **SIP Security** section.



4. Click **Save** and **Apply**.

The extension can be registered in different LAN subnet or in a remote network.

Step2. Generate configuration file for an IP phone on the PBX

1. RESET the phone if it is previously used.
2. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
3. Click **Add** to add a phone to the PBX.
4. 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 the phone.
5. In the **Options** section, configure the following settings.

- **Template**: Select a desired template from the drop-down list.

  > **Note:**
  > The template provides configurations except extension assignment. You can select the default template corresponding to the phone model, or customize your own template.
  >
  > For more information, see Create a Custom Auto Provisioning Template.

- **Provisioning Method**: Select **DHCP (In the Office)**.

  A provisioning server URL is generated automatically and displayed on the web page.

  > **Note:**
  > Take note of the generated provisioning link, you will use it later on the DHCP server.

6. In the **Assign Extension** section, assign an extension to the phone.

   > **Tip:**
   > If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other IP phone or gateway.
   > - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
   > - To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

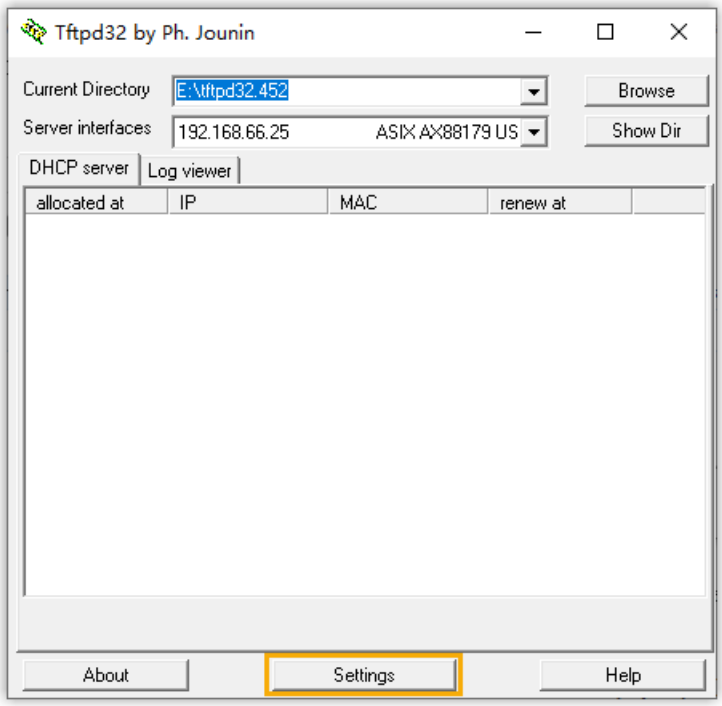
7. Click **Save**.

   A configuration file for the phone is generated in the PBX.

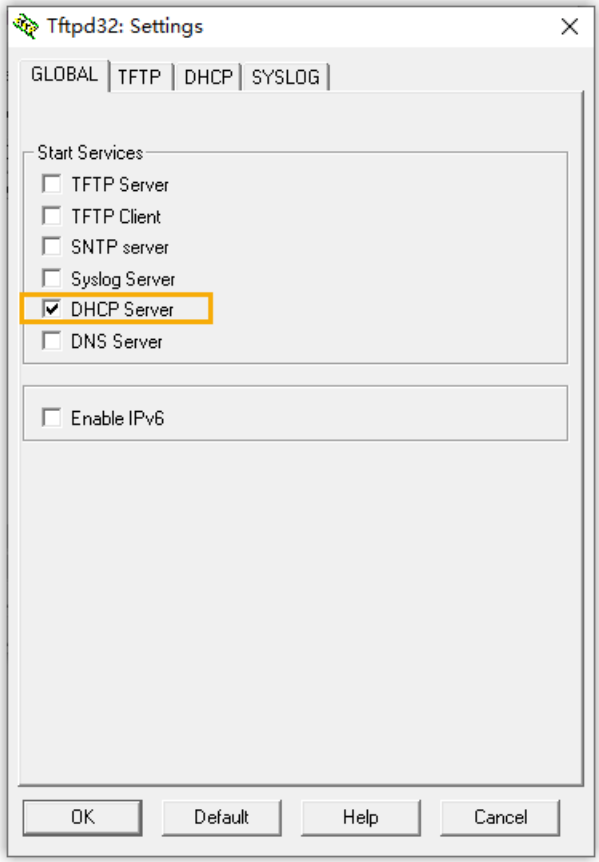
Step3. Set up a DHCP option 66

For most firewalls or routers, the built-in DHCP server does not have the capability to add or change the scope option. Tftpd32 software supports this function, which can be an alternative choice to accomplish this task. The following instructions are based on the Tftpd32 DHCP server.

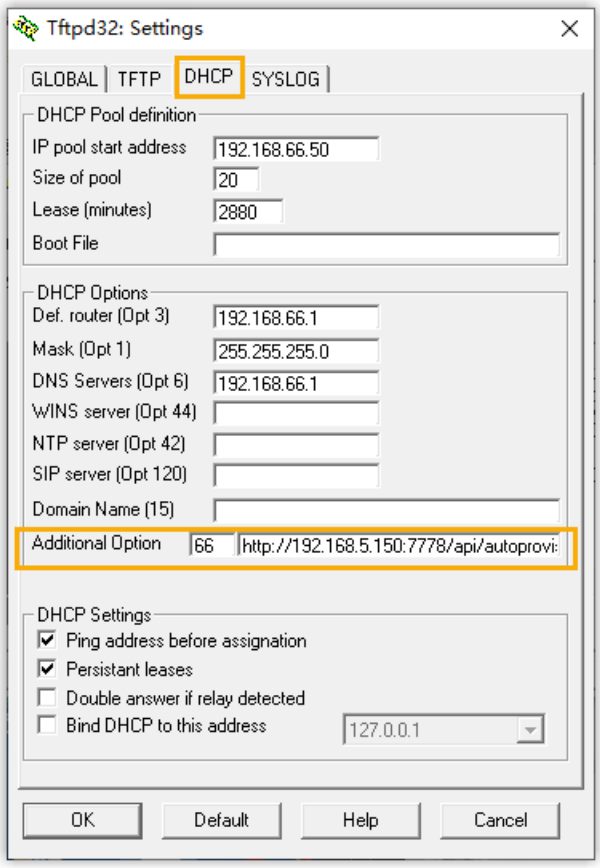
1. Run the Tftpd32 software, click **Settings** at the bottom of the window.



2. In the pop-up window, click **GLOBAL** tab, select the checkbox of **DHCP Server**.



3. Click **DHCP** tab, configure the DHCP server parameters.



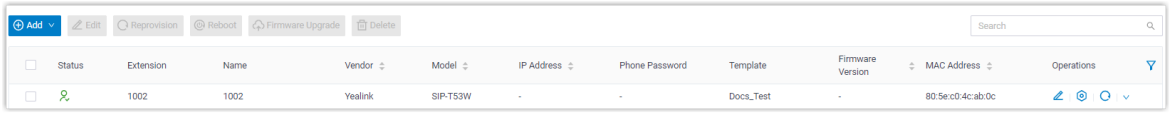
- **IP pool start address**: The starting IP addresses to be allocated.
- **Size of pool**: Total number of available IP addresses.
- **Lease time**: IP address lease time.
- **Def. Router (Opt 3)**: The gateway IP address. In this example, enter `192.168.66.1`.
- **Mask (Opt 1)**: Subnet mask that corresponds to the available IP address segment.
- **DNS Server (Opt 6)**: DNS server address for the DHCP server. In this example, enter `192.168.66.1`.
- **Additional Option**: Enter option to `66` and paste the PBX provisioning link besides the option.

4. Click **OK**.

   The PC starts to work as a DHCP server.

Result

- Connect an IP phone to the same LAN subnet as the DHCP server (PC), the IP phone gets an IP address and download the configuration file from the PBX to achieve Auto Provisioning
- The extension registration status of provisioned phones is displayed on **Auto Provisioning > Phones**.
  - : The assigned extension is registered on the phone.
  - : The assigned extension is unregistered on the phone.



Auto Provision IP Phones Remotely (RPS FQDN Method)

When IP phones are located in remote network, Yeastar P-Series PBX System supports to auto provision the IP phones using RPS (Redirection and Provisioning Service) method through the Yeastar-supplied Fully Qualified Domain Name (FQDN). This method frees you from complicated network settings and helps you quickly establish a secure tunnel for remote provisioning, greatly saving time and cost in mass deployment while resting assured with the remote access security.

> **Note:**
> This topic describes how to provision an IP phone and assign a user's extension to the phone. If you want to set up a hot desking phone via auto provisioning, see Set up a Hot Desking Phone.

Supported IP phones

This topic can be applied to the RPS supported IP phones that are deployed in a remote network.

Prerequisites

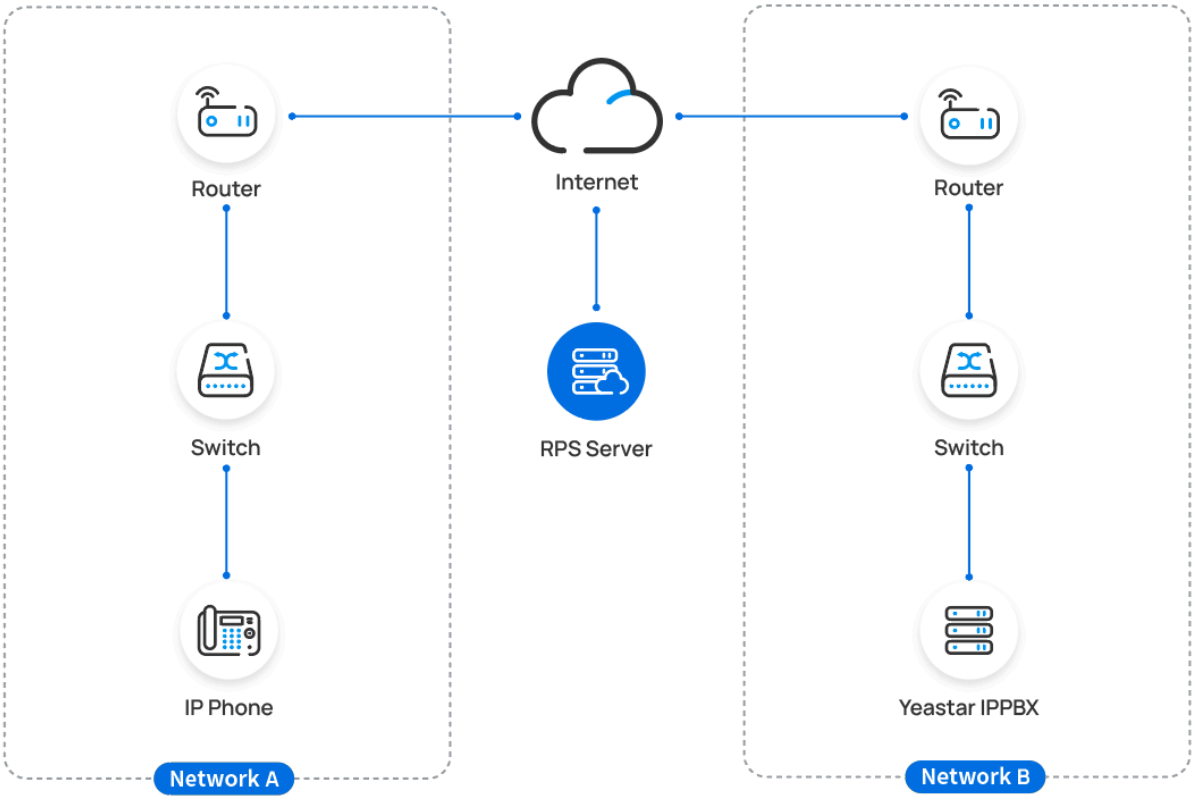
- You have subscribed Yeastar P-Series Enterprise Plan or Ultimate Plan.
- Make sure the following required FQDN settings are ready.
  - The Yeastar FQDN domain name is available.

  - The remote IP phones and the extension accounts to be assigned can perform remote SIP registration via FQDN. For detailed configurations, see Configure Network for Remote SIP Access by a Yeastar FQDN.
  - The remote IP phones are permitted to access the PBX system via FQDN to obtain configuration files.

    For detailed configurations, see Configure Network for Remote Web Access by a Yeastar FQDN.
- Make sure that you have downloaded the template for the desired phone model (Path: **Auto Provisioning > Resource Repository > Default Templates**).
- Gather information of IP phone, including Vendor, Model, and MAC address.

Scenario

Yeastar P-Series PBX System and IP phones are deployed in different networks. The PBX has enabled and configured the FQDN feature.



Procedure

Step 1. Generate configuration file for an IP phone on the PBX

Step 2. Reboot the IP phone to obtain the configuration file

Step 1. Generate configuration file for an IP phone on the PBX

1. RESET the phone if it is previously used.
2. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
3. Click **Add**, then select **Add** to add an IP phone.
4. 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 the phone.
5. In the **Options** section, configure the following settings:
   - **Template**: Select a desired template from the drop-down list.

     > **Note:**
     > The template provides configurations except extension assignment. You can select the default template corresponding to the phone model, or customize your own template.
     >
     > For more information, see Create a Custom Auto Provisioning Template.

   - **Provisioning Method**: Select **RPS FQDN (Remote)**.

     A provisioning server URL is generated automatically and displayed on the web page.

     > **Troubleshooting:**
     > Why don't see the RPS FQDN Auto Provisioning method option?

   - **Authentication for the First-time Auto Provisioning**: If enabled, users are requested to fill in authentication information on the IP phones before triggering the first-time provisioning.

     > **Note:**
     > We recommend that you keep this option selected for security purpose.

6. In the **Assign Extension** section, assign an extension to the phone.

> **Tip:**

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

- To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
- To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

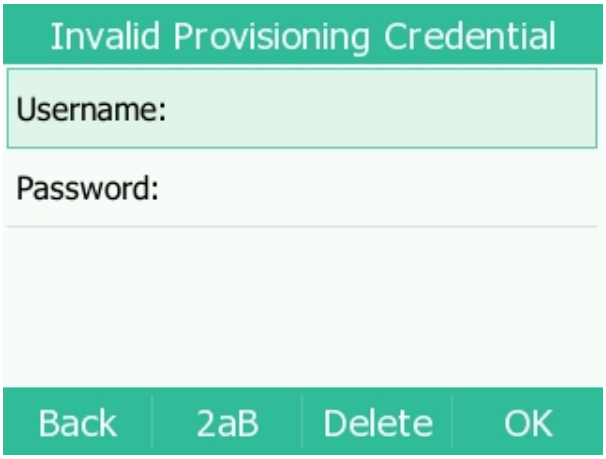
7. Click **Save**.

   A configuration file for the phone is generated in the PBX.

   The PBX will send an event notification of **RPS Request Success**, which means that the phone MAC is added automatically to the RPS server.

Step 2. Reboot the IP phone to obtain the configuration file

1. Reboot the IP phone.
2. If you have enabled **Authentication for the First-time Auto Provisioning** on the PBX, enter the authentication credential on the IP phone to finish phone provisioning.



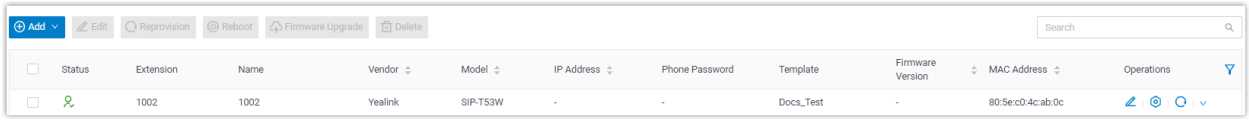
- **Username**: Enter the extension number that is assigned to the phone.
- **Password**: Enter the extension's Voicemail Access PIN.

Note:
Check the Voicemail Access PIN in the **Voicemail** tab on the extension configuration page.

Result

The extension registration status of provisioned phones is displayed on **Auto Provisioning > Phones**.

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



Auto Provision IP Phones Remotely (RPS Method)

When IP phones are located in remote network, Yeastar P-Series PBX System supports an RPS method. This method allows you to deploy and update IP phones remotely via public IP address/domain name and port, which can greatly save time and cost in mass deployment.

Note:
This topic describes how to provision an IP phone and assign a user's extension to the phone. If you want to set up a hot desking phone via auto provisioning, see Set up a Hot Desking Phone.

Supported IP phones

This topic can be applied to the RPS supported IP phones that are deployed in a remote network.

Prerequisites

- You have set up port forwarding on router and set up SIP NAT on the PBX to ensure remote registration.

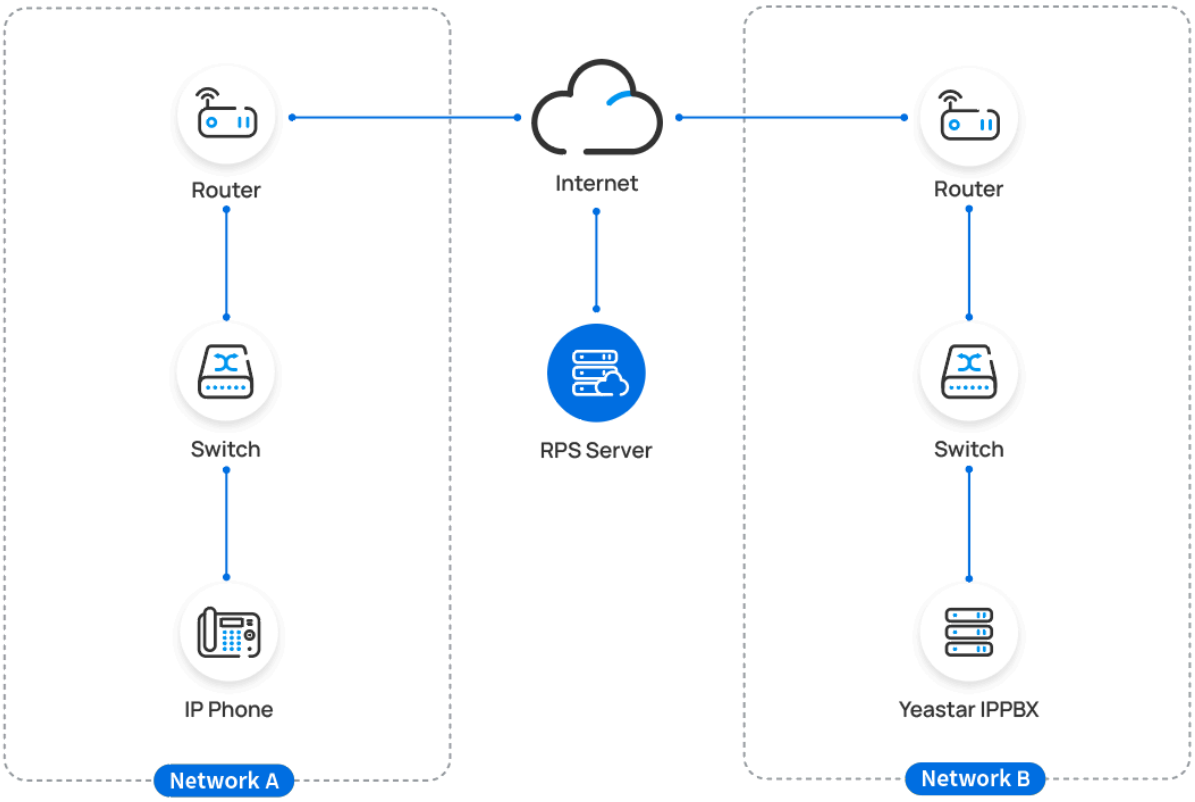
  Important:
  The following PBX ports must be forwarded.
  - RTP ports
  - SIP port
  - Web Server port

For more information, see Configure Network for Remote Access by a Public IP Address or Configure Network for Remote Access by a Domain Name.

- Make sure that you have downloaded the template for the desired phone model (Path: **Auto Provisioning > Resource Repository > Default Templates**).
- Gather information of IP phone, including Vendor, Model, and MAC address.

Scenario

Yeastar P-Series PBX System and IP phones are deployed in different networks. The PBX is behind a router and port forwarding is configured on the router.



Procedure

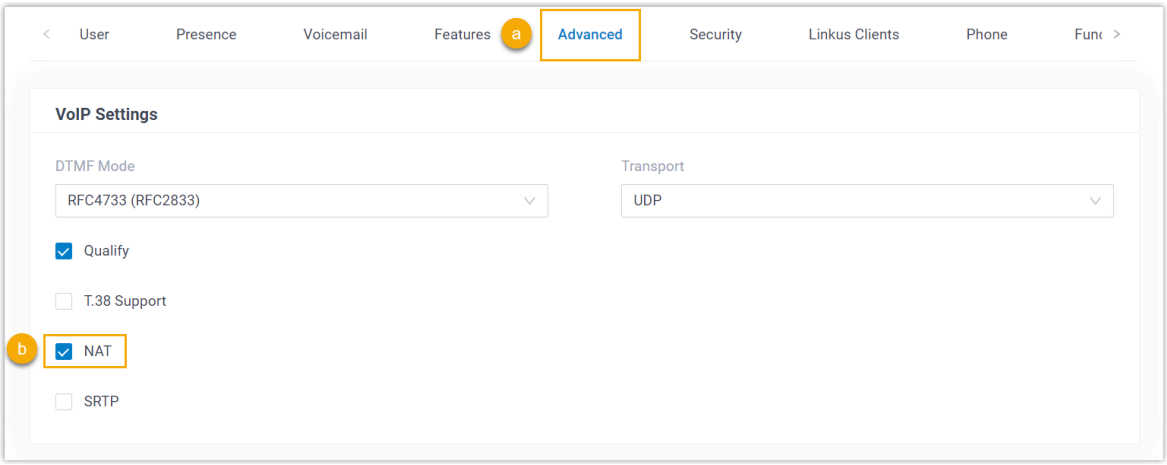
Step1. Set a remote extension

Step 2. Generate configuration file for an IP phone on the PBX

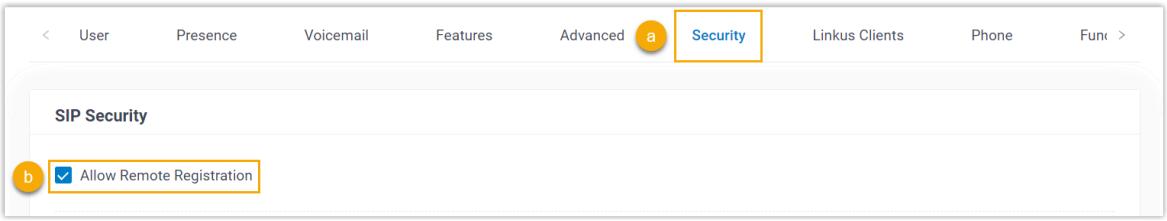
Step 3. Reboot the IP phone to obtain the configuration file

Step 1. Set a remote extension

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the extension to be assigned.
2. Click **Advanced** tab, select the checkbox of **NAT** in the **VoIP Settings** section.



3. Click **Security** tab, select the checkbox of **Allow Remote Registration** in the **SIP Security** section.



4. Click **Save** and **Apply**.

The extension can be registered in different LAN subnet or in a remote network.

Step 2. Generate configuration file for an IP phone on the PBX

1. RESET the phone if it is previously used.
2. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
3. Click **Add** to add an IP phone.
4. 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 the phone.
5. In the **Options** section, configure the following settings.

- **Template**: Select a desired template from the drop-down list.

  > **Note:**
  > The template provides configurations except extension assignment. You can select the default template corresponding to the phone model, or customize your own template.
  >
  > For more information, see Create a Custom Auto Provisioning Template.

- **Provisioning Method**: Select **RPS (Remote)**.

  A provisioning server URL is generated automatically and displayed on the web page.

  > **Troubleshooting:**
  > Why don't see the RPS Auto Provisioning method option?

- **Authentication for the First-time Auto Provisioning**: If enabled, users are requested to fill in authentication information on the IP phones before triggering the first-time provisioning.

  > **Note:**
  > We recommend that you keep this option selected for security purpose.

6. In the **Assign Extension** section, assign an extension to the phone.

   > **Tip:**
   > If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other IP phone or gateway.
   > - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
   > - To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

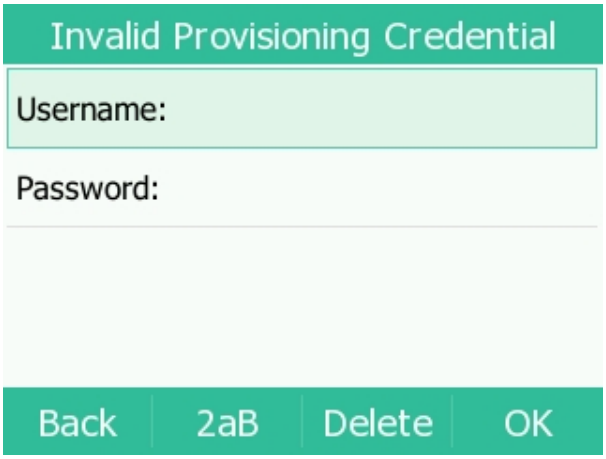
7. Click **Save**.

   A configuration file for the phone is generated in the PBX.

   The PBX will send an event notification of **RPS Request Success**, which means that the phone MAC is added automatically to the RPS server.

Step 3. Reboot the IP phone to obtain the configuration file

1. Reboot the IP phone.
2. If you have enabled **Authentication for the First-time Auto Provisioning** on the PBX, enter the authentication credential on the IP phone to finish phone provisioning.



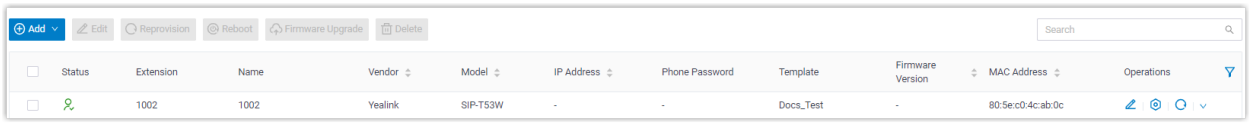
   - **Username**: Enter the extension number that is assigned to the phone.
   - **Password**: Enter the extension's Voicemail Access PIN.

> **Note:**
> Check the Voicemail Access PIN in the **Voicemail** tab on the extension configuration page.

Result

The extension registration status of provisioned phones is displayed on **Auto Provisioning > Phones**.

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



Related information

Auto Provision IP Phones Remotely (RPS FQDN Method)

Auto Provision IP Phones Remotely (Provision Link - FQDN Method)

For IP phones that are located in remote network but don't support RPS Auto Provisioning method, Yeastar P-Series PBX System supports to provision the IP phones using Provision Link - FQDN method through the Yeastar-supplied Fully Qualified Domain Name (FQDN).

Supported IP phones

This topic can be applied to the 'Provision Link' supported IP phones that are deployed in a remote network.

Prerequisites

- You have subscribed Yeastar P-Series Enterprise Plan or Ultimate Plan.
- Make sure the following required FQDN settings are ready.
  - The Yeastar FQDN domain name is available.
  - The remote IP phones and the extension accounts to be assigned can perform remote SIP registration via FQDN. For detailed configurations, see Configure Network for Remote SIP Access by a Yeastar FQDN.
  - The remote IP phones are permitted to access the PBX system via FQDN to obtain configuration files.

    For detailed configurations, see Configure Network for Remote Web Access by a Yeastar FQDN.
- Make sure that you have downloaded the template for the desired phone model (Path: **Auto Provisioning > Resource Repository > Default Templates**).
- Gather information of IP phone, including Vendor, Model, and MAC address.

Step 1. Generate configuration file for an IP phone on the PBX

1. RESET the phone if it is previously used.
2. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
3. Click **Add**, then select **Add** to add an IP phone.
4. 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 the phone.
5. In the **Options** section, configure the following settings:

- **Template**: Select a desired template from the drop-down list.

  > **Note:**
  > The template provides configurations except extension assignment. You can select the default template corresponding to the phone model, or customize your own template.
  >
  > For more information, see Create a Custom Auto Provisioning Template.

- **Provisioning Method**: Select **Provision Link - FQDN (Remote)**.
  A provisioning server URL is generated automatically and displayed on the web page.

  > **Note:**
  > Note down the generated provisioning link, as you will use it later.

6. In the **Assign Extension** section, assign an extension to the phone.

   > **Tip:**
   > If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other IP phone or gateway.
   > - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
   > - To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

7. Click **Save**.

   A configuration file for the phone is generated in the PBX.

Step 2. Make the configuration file accessible to the IP phone

Set up the provisioning link to where your IP phones can fetch the configuration files in one of the following ways:

- Configure a DHCP server and set up option 66
- Configure provisioning server address on the phone

Configure a DHCP server and set up option 66

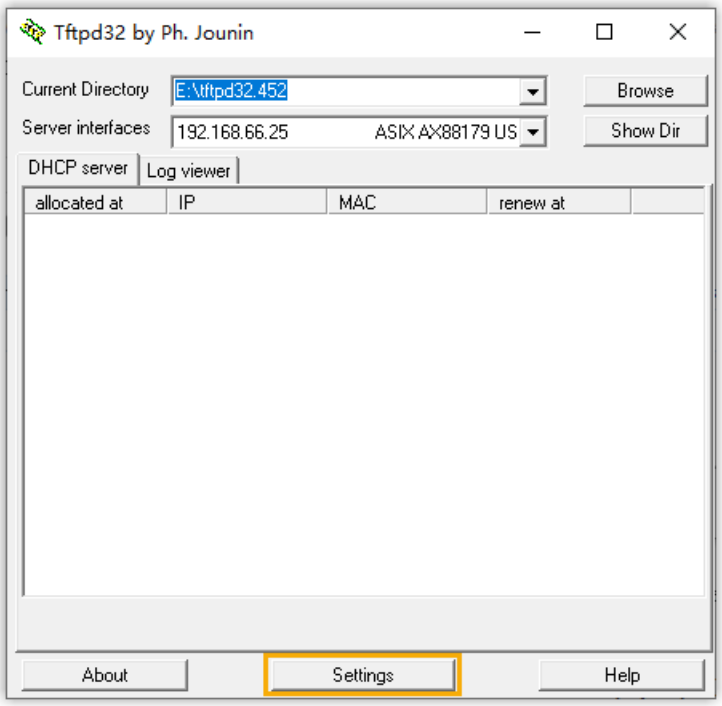
Configure a DHCP server and set up DHCP option 66 to the provisioning link. The IP phone will download configurations from PBX via the provisioning link, and apply the settings automatically.

You can use the PBX as a DHCP server, or use a third-party DHCP server that supports DHCP option 66.

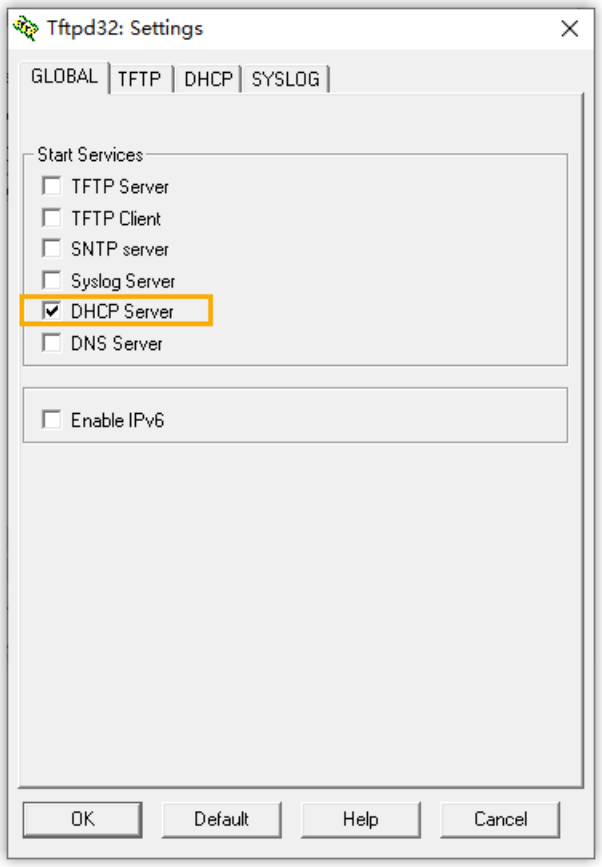
- If you use PBX as a DHCP server, the DHCP option 66 is set to the provisioning link automatically.
- If you use a third-party DHCP server, you need to set DHCP option 66.

  Here takes Tftpd32 DHCP server as an example.

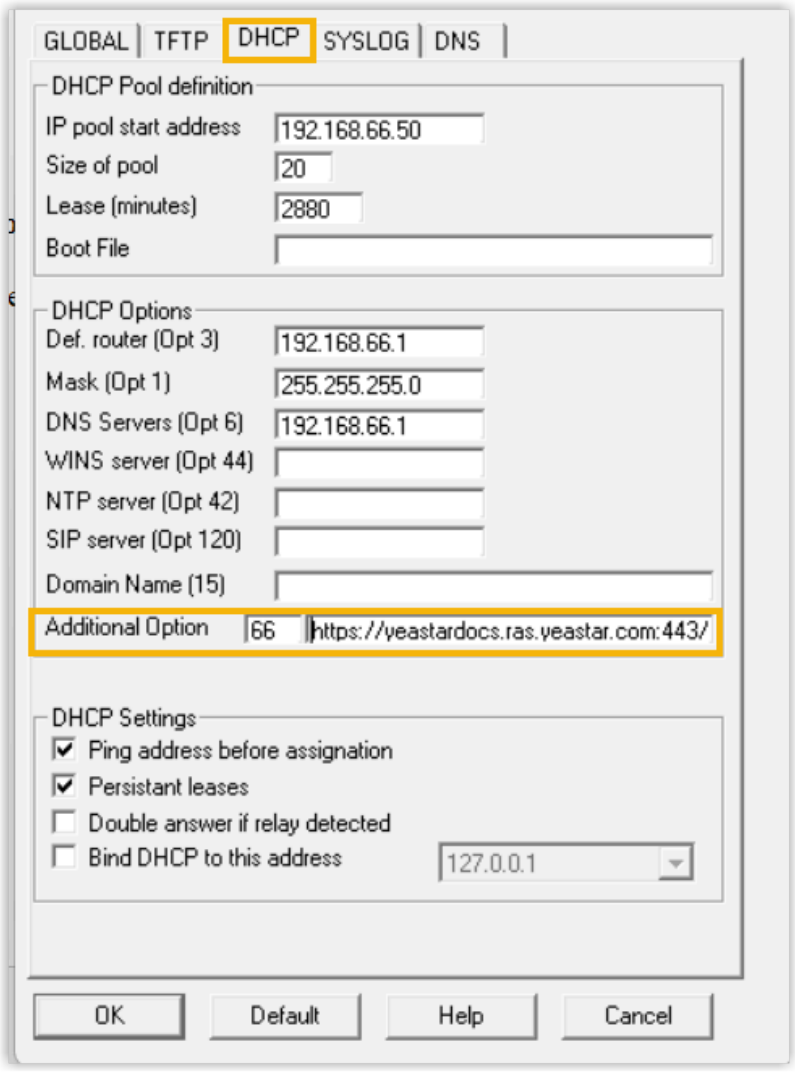
  1. Run the Tftpd32 software, click **Settings** at the bottom of the window.



  2. In the pop-up window, click **GLOBAL** tab, select the checkbox of **DHCP Server**.



3. Click **DHCP** tab, configure the DHCP server parameters.



- **IP pool start address**: The starting IP addresses to be allocated.
- **Size of pool**: Total number of available IP addresses.
- **Lease time**: IP address lease time.
- **Def. Router (Opt 3)**: The gateway IP address.
- **Mask (Opt 1)**: Subnet mask that corresponds to the available IP address segment.
- **DNS Server (Opt 6)**: DNS server address for the DHCP server.
- **Additional Option**: Enter option to 66 and paste the PBX provisioning link beside the option.

4. Click **OK**.

The IP phone downloads the configuration file from the PBX, and applies the configurations automatically.

Configure provisioning server address on the phone

Here takes the Yealink IP phone as an example.

1. On the IP phone, go to **Menu > Status**, check the IP address of the IP phone on the **IPv4** field.
2. Log in to the IP phone web page by the IP address, go to **Settings > Auto Provision**.
3. In the **Server URL** field, paste the PBX provisioning link.
4. Scroll down to the bottom, click **Auto Provision Now**.
5. In the pop-up dialog box, click **OK** to auto provision the IP phone.

   The IP phone downloads the configuration file from the PBX, and applies the configurations automatically.

Related information

Auto Provision IP Phones Remotely (Provision Link Method)

Auto Provision IP Phones Remotely (Provision Link Method)

For IP phones that are located in remote network but don't support RPS Auto Provisioning method, Yeastar P-Series PBX System supports to provision the IP phones using Provision Link method via public IP address/domain name and port.

Supported IP phones

This topic can be applied to the 'Provision Link' supported IP phones that are deployed in a remote network.

Prerequisites

- You have set up port forwarding on router and set up SIP NAT on the PBX to ensure remote registration.

> **Important:**
> The following PBX ports must be forwarded.
> - RTP ports

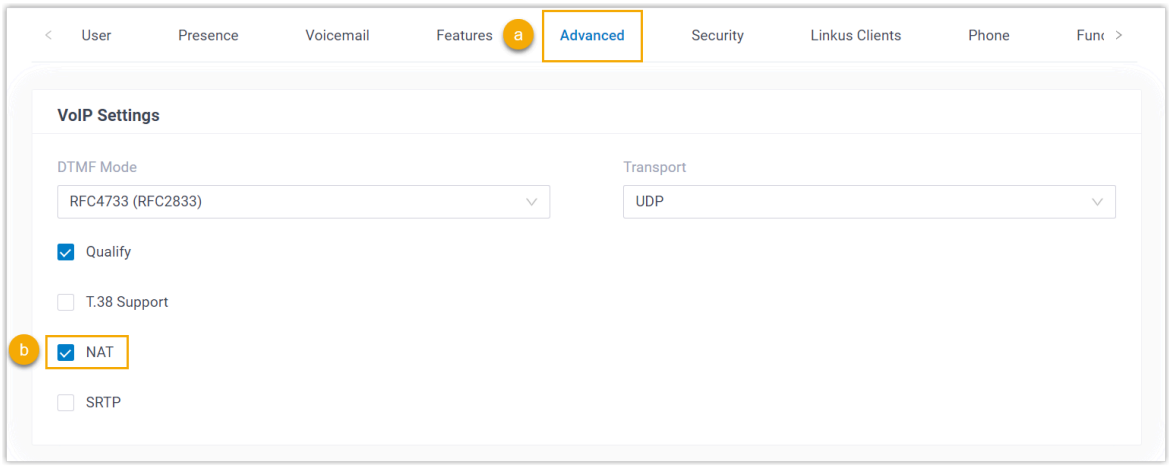
- SIP port
- Web Server port

For more information, see Configure Network for Remote Access by a Public IP Address or Configure Network for Remote Access by a Domain Name.

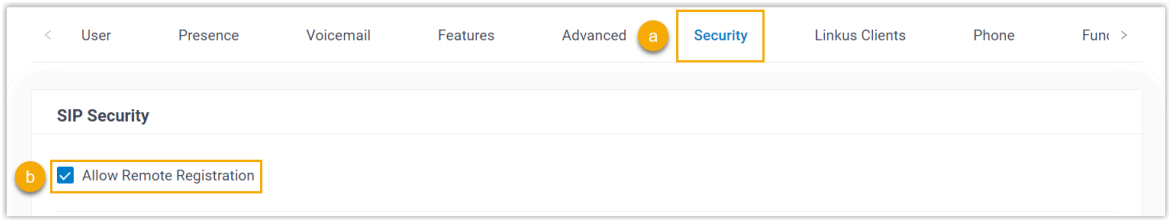
- Make sure that you have downloaded the template for the desired phone model (Path: **Auto Provisioning > Resource Repository > Default Templates**).
- Gather information of IP phone, including Vendor, Model, and MAC address.

Step 1. Set a remote extension

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the extension to be assigned.
2. Click **Advanced** tab, select the checkbox of **NAT** in the **VoIP Settings** section.



3. Click **Security** tab, select the checkbox of **Allow Remote Registration** in the **SIP Security** section.



4. Click **Save** and **Apply**.

The extension can be registered in different LAN subnet or in a remote network.

Step 2. Generate configuration file for an IP phone on the PBX

1. RESET the phone if it is previously used.
2. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
3. Click **Add** to add an IP phone.
4. 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 the phone.
5. In the **Options** section, configure the following settings.
   - **Template**: Select a desired template from the drop-down list.

     > **Note:**
     > The template provides configurations except extension assignment. You can select the default template corresponding to the phone model, or customize your own template.
     >
     > For more information, see Create a Custom Auto Provisioning Template.

   - **Provisioning Method**: Select **Provision Link (Remote)**.

     A provisioning server URL is generated automatically and displayed on the web page.

     > **Note:**
     > Note down the generated provisioning link, as you will use it later.

6. In the **Assign Extension** section, assign an extension to the phone.

   > **Tip:**
   > If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other IP phone or gateway.
   > - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
   > - To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

7. Click **Save**.

Step 3. Make the configuration file accessible to the IP phone

Set up the provisioning link to where your IP phones can fetch the configuration files in one of the following ways:

- Configure a DHCP server and set up option 66
- Configure provisioning server address on the phone

Configure a DHCP server and set up option 66

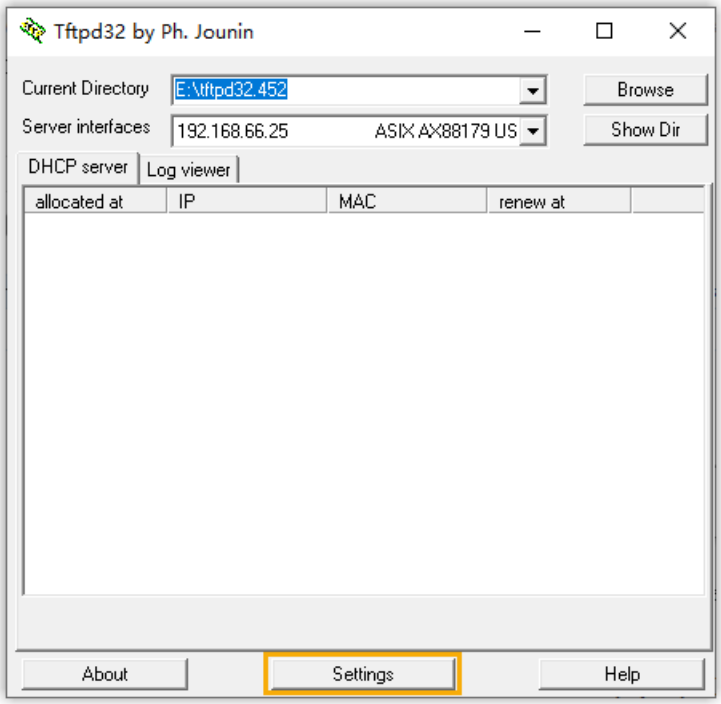
Configure a DHCP server and set up DHCP option 66 to the provisioning link. The IP phone will download configurations from PBX via the provisioning link, and apply the settings automatically.

You can use the PBX as a DHCP server, or use a third-party DHCP server that supports DHCP option 66.

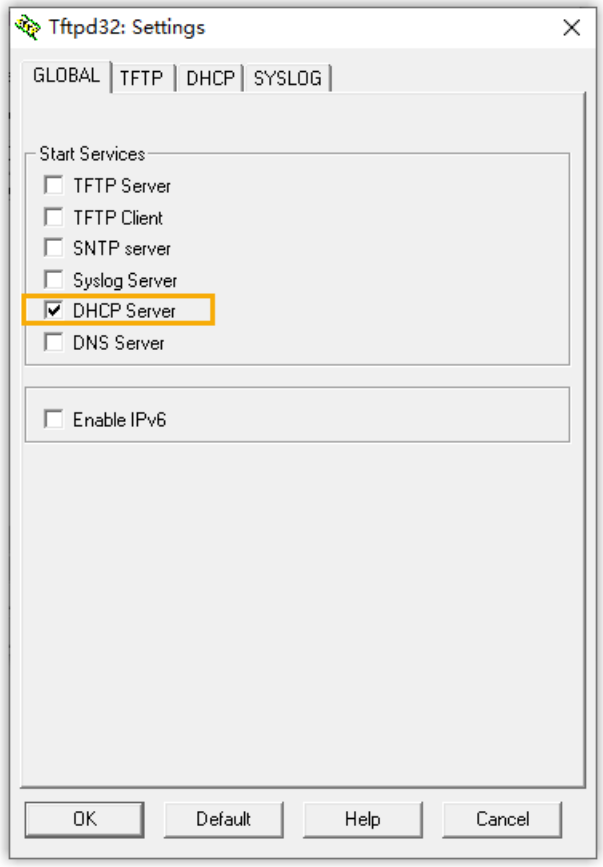
- If you use PBX as a DHCP server, the DHCP option 66 is set to the provisioning link automatically.
- If you use a third-party DHCP server, you need to set DHCP option 66.

  Here takes Tftpd32 DHCP server as an example.

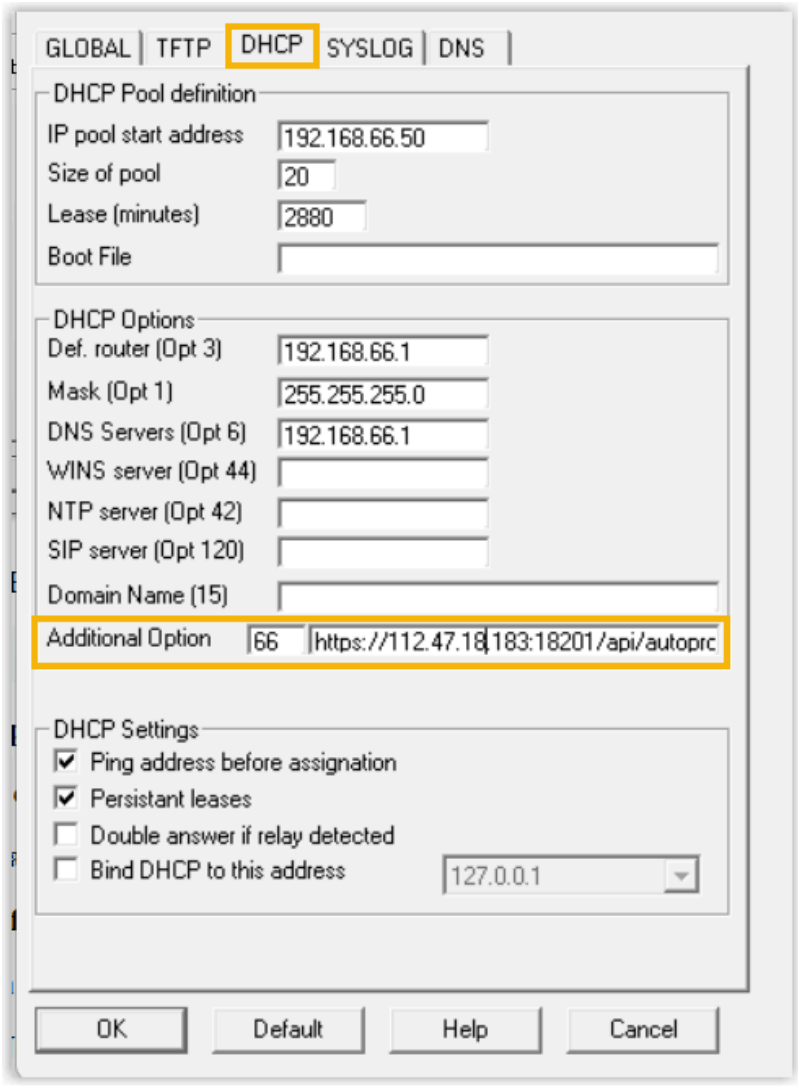
  1. Run the Tftpd32 software, click **Settings** at the bottom of the window.



2. In the pop-up window, click **GLOBAL** tab, select the checkbox of **DHCP Server**.



3. Click **DHCP** tab, configure the DHCP server parameters.



- **IP pool start address**: The starting IP addresses to be allocated.
- **Size of pool**: Total number of available IP addresses.
- **Lease time**: IP address lease time.
- **Def. Router (Opt 3)**: The gateway IP address.
- **Mask (Opt 1)**: Subnet mask that corresponds to the available IP address segment.
- **DNS Server (Opt 6)**: DNS server address for the DHCP server.
- **Additional Option**: Enter option to 66 and paste the PBX provisioning link beside the option.

4. Click **OK**.

The IP phone downloads the configuration file from the PBX, and applies the configurations automatically.

Configure provisioning server address on the phone

Here takes the Yealink IP phone as an example.

1. On the IP phone, go to **Menu > Status**, check the IP address of the IP phone on the **IPv4** field.
2. Log in to the IP phone web page by the IP address, go to **Settings > Auto Provision**.
3. In the **Server URL** field, paste the PBX provisioning link.
4. Scroll down to the bottom, click **Auto Provision Now**.
5. In the pop-up dialog box, click **OK** to auto provision the IP phone.

   The IP phone downloads the configuration file from the PBX, and applies the configurations automatically.

Related information

Auto Provision IP Phones Remotely (Provision Link - FQDN Method)

Manually Provision an IP Phone

If you fail to auto provision IP phones, you can manually add the provisioning link into the phone's web interface.

> **Note:**
> This topic describes how to provision an IP phone and assign a user's extension to the phone. If you want to set up a hot desking phone via auto provisioning, see Set up a Hot Desking Phone.

Supported IP phones

This topic can be applied to all the IP phones listed in Auto Provisioning - Supported Devices.

Prerequisites

- Make sure that you have downloaded the template for the desired phone model (Path: **Auto Provisioning > Resource Repository > Default Templates**).

- Gather information of IP phone, including Vendor, Model, and MAC address.
- RESET the phone if it is previously used.

Procedure

- Step 1. Add phone's MAC address on the PBX
- Step 2. Configure provisioning server address on the phone

Step 1. Add phone's MAC address on the PBX

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Click **Add** to add the IP phone to the PBX.
3. In the **IP Phone** section, configure phone information as follows:
   - **Vendor**: Select a phone vendor.
   - **Model**: Select a phone model.
   - **MAC Address**: Enter the MAC address of the IP phone
4. In the **Options** section, configure the auto provision settings.
   - **Template**: Select a desired template from the drop-down list.

     > **Note:**
     > The template provides configurations except extension assignment. You can select the default template corresponding to the phone model, or customize your own template.
     >
     > For more information, see Create a Custom Auto Provisioning Template.

   - **Provisioning Method**: Select the desired method according to your deployment environment.
   - **Provisioning Link**: A provisioning server URL is generated automatically and displayed on the web page.

     > **Note:**
     > Note down the generated provisioning link, as you will use it later.

5. In the **Assign Extension** section, assign an extension to the IP phone.

> **Tip:**

> If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other IP phone or gateway.
> - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
> - To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

6. Click **Save**.

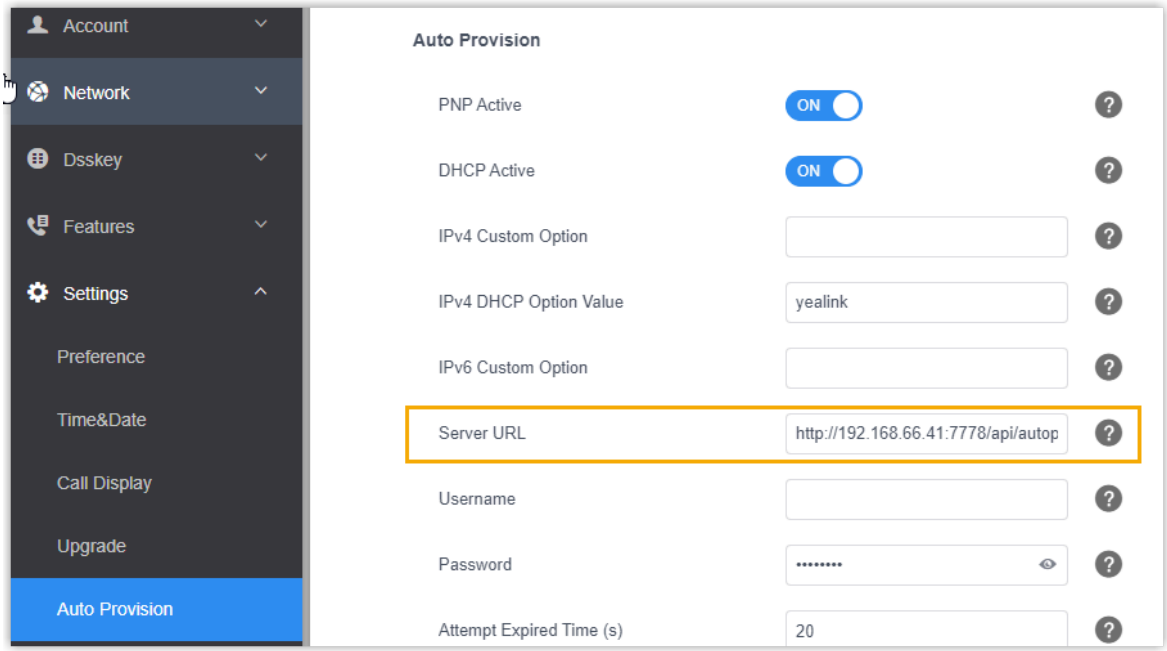
   A configuration file for the phone is generated in the PBX.

Step 2. Configure provisioning server address on the phone

Here takes the Yealink SIP-T53W IP phone as an example.

1. On the IP phone, go to **Menu > Status**, check the IP address of the IP phone on the **IPv4** field.
2. Log in to the IP phone web page by the IP address, go to **Settings > Auto Provision**.
3. In the **Server URL** field, paste the PBX provisioning link.

   For example, `http://192.168.66.41:7778/api/autoprovision/HF9FDqlQE9fx3WlR`.



4. Scroll down to the bottom, click **Auto Provision Now**.
5. In the pop-up dialog box, click **OK** to auto provision the IP phone.

Result

The IP phone downloads the configuration file from the PBX, and applies the configurations automatically.

Provision Gateways

Auto Provision Yeastar TA FXS Gateways (PnP Method)

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.

Supported gateway models

- TA100, TA200
- TA400, TA800
- TA1600, TA2400, TA3200

Prerequisites

Make sure that the TA gateway is in the same network segment as the PBX, or the PBX cannot detect the TA gateway.

> **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.

Procedure

1. Power on the PBX first, then power on the gateway.
2. RESET the TA gateway if it is previously used.
3. Log in to PBX web portal, go to **Auto Provisioning > Gateways**.

   The gateway list displays all the discovered gateways 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.

4. Click beside the desired gateway to configure it.
   a. In the **Options** section, configure the following settings.
      - **Template**: Select a desired template from the drop-down list.

        > **Note:**
        > The template provides configurations except extension assignment. You can select the default template corresponding to the gateway model, or customize your own template. For more information, see Create a Custom Auto Provisioning Template.

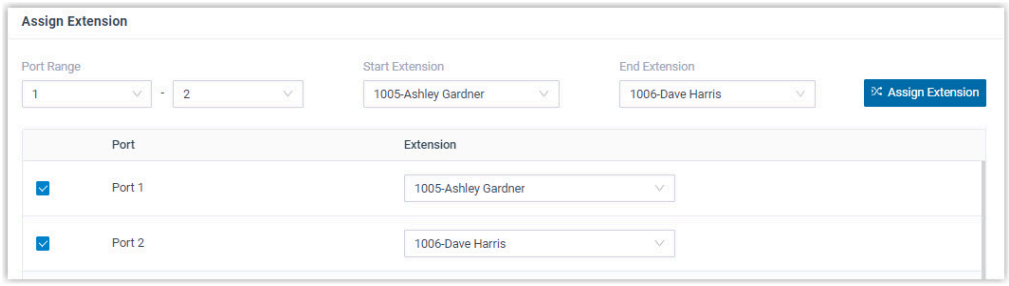
      - **Provisioning Method**: Select **PnP (In the Office)**.

        A provisioning server URL is generated automatically and displayed on the web page.

   b. 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.

      > **Tip:**
      > If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other IP phone or gateway.
      > - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
      > - To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.



c. In the **Preference** section, configure the settings as needed.

- **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.

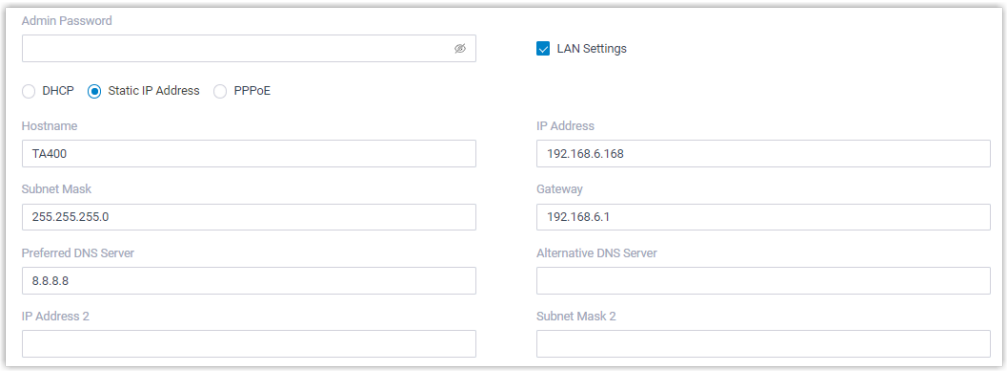
> **Note:**
> SIP VoIPServer IDX is not applicable for TA100 and TA200.

- **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.



d. In the **Codecs** section, select your preferred codec list for the gateway.

5. Click **Save**.

   The PBX prompts you whether to reboot the gateway.

6. 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 TA gateway.
- The extension registration status of provisioned phones is displayed on **Extension and Trunk > Extension**.
  - : The assigned extension is registered on the gateway.
  - : The assigned extension is unregistered on the gateway.

Related information

Modify a Provisioned Gateway Settings

Auto Provision Yeastar TA FXS Gateways (DHCP Method)

For the Yeastar TA FXS gateways that are located in different LAN subnet as the PBX, you can provision the gateways by DHCP method.

Supported gateway models

- TA100, TA200
- TA400, TA800
- TA1600, TA2400, TA3200

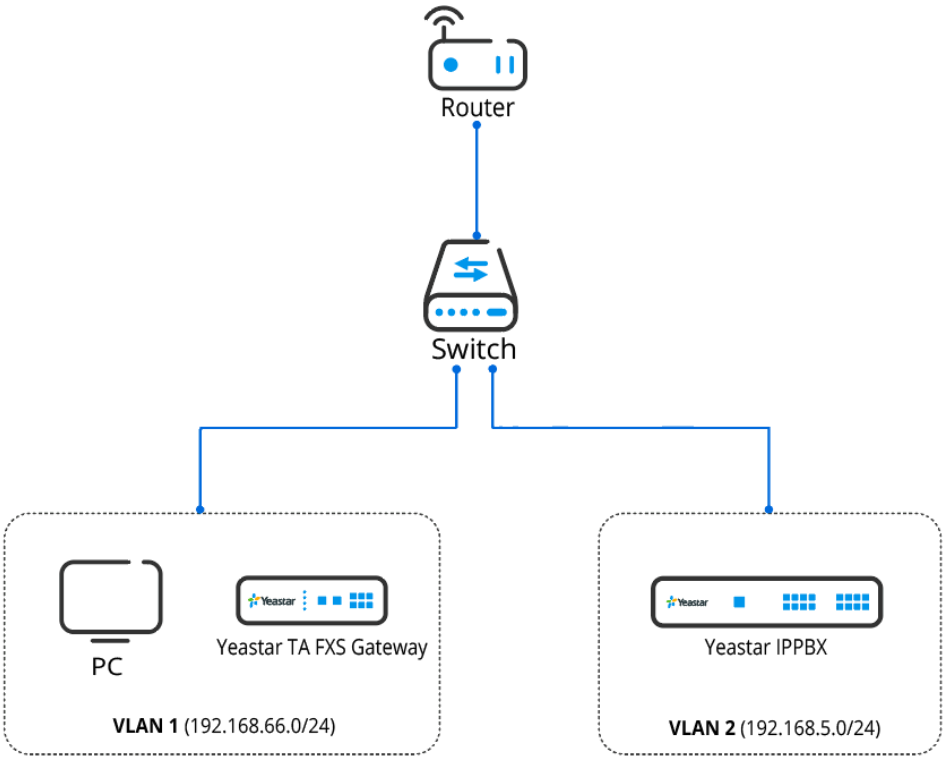
Prerequisites

- Make sure there is only one DHCP server, otherwise the gateway may fail to obtain an IP address.
- Gather information of Yeastar TA FXS gateway, including Model, and MAC address.

Scenario

A company subdivides a physical network into separate Virtual LANs (VLANs) as the following figure shows.

- **Gateway**: Located in VLAN 1 (192.168.66.0/24)
- **PBX**: Located in VLAN 2 (192.168.5.0/24)



Procedure

Step1. Set a remote extension

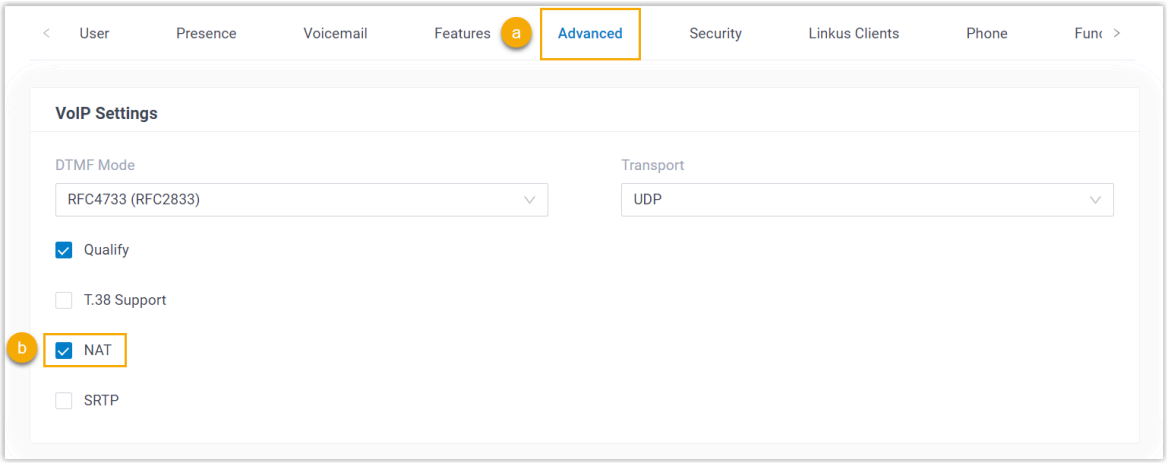
Step2. Add gateway's MAC address on the PBX

Step3. Set up a DHCP option 66

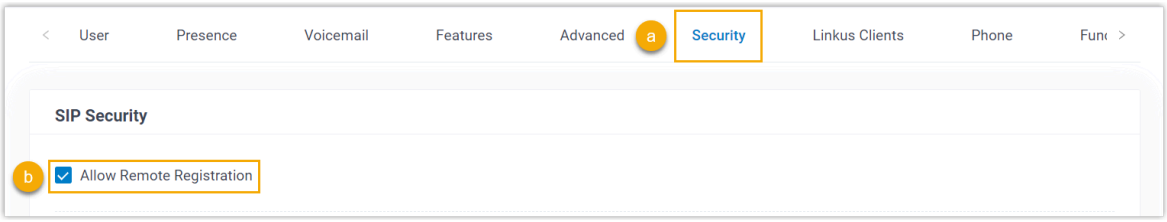
Step4. Enable DHCP provisioning on the gateway

Step1. Set a remote extension

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the extension to be assigned.
2. Click **Advanced** tab, select the checkbox of **NAT** in the **VoIP Settings** section.



3. Click **Security** tab, select the checkbox of **Allow Remote Registration** in the **SIP Security** section.



4. Click **Save** and **Apply**.

The extension can be registered in different LAN subnet or in a remote network.

Step2. Add gateway's MAC address on the PBX

1. RESET the TA gateway if it is previously used.
2. Log in to PBX web portal, go to **Auto Provisioning > Gateways**.
3. Click **Add** to add a gateway to the PBX.
4. In the **Gateway** section, configure gateway information as follows:
    - **Model**: Select a gateway model.
    - **MAC Address**: Enter MAC address of the gateway

5. In the **Options** section, configure the Auto Provisioning settings.
   - **Template**: Select a desired template from the drop-down list.

     > **Note:**
     > The template provides configurations except extension assignment. You can select the default template corresponding to the gateway model, or customize your own template. For more information, see Create a Custom Auto Provisioning Template.

   - **Provisioning Method**: Select **DHCP (In the Office)**.

     A provisioning server URL is generated automatically and displayed on the web page.

     > **Note:**
     > Take note of the generated provisioning link, you will use it later on the DHCP server.

6. In the **Assign Extension** section, 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.

      > **Tip:**
      > If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other IP phone or gateway.
      > - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
      > - To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

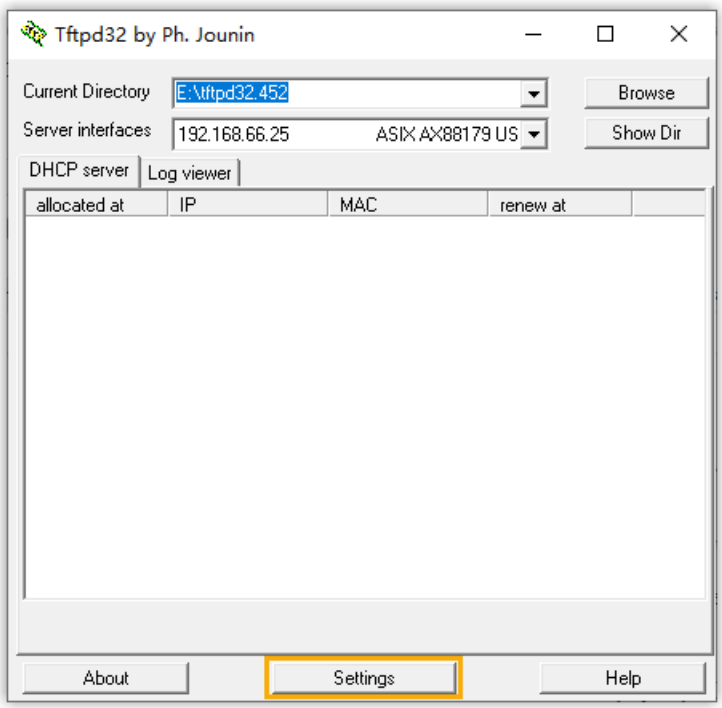
7. Click **Save**.

   A configuration file for the gateway is generated in the PBX.

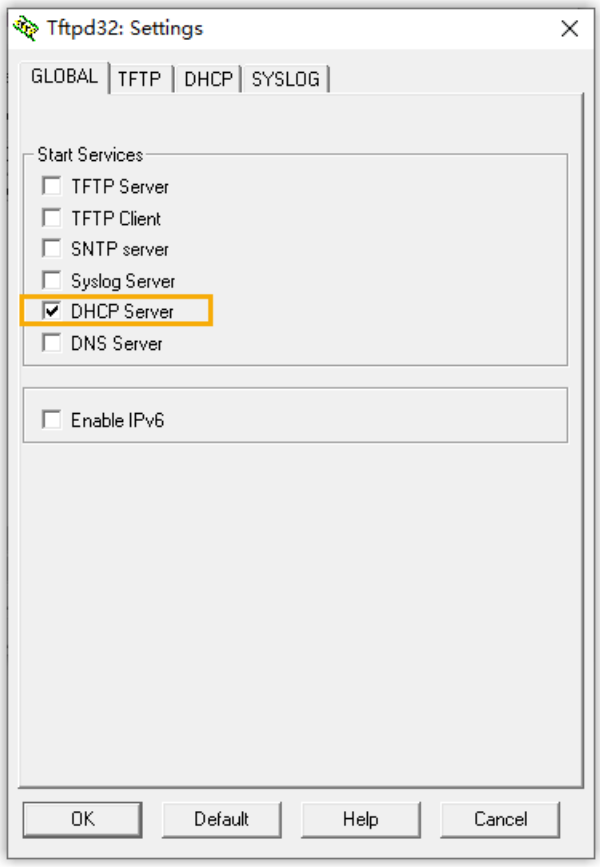
Step3. Set up a DHCP option 66

For most firewalls or routers, the built-in DHCP server does not have the capability to add or change the scope option. Tftpd32 software supports this function, which can be an alternative choice to accomplish this task. The following instructions are based on the Tftpd32 DHCP server.

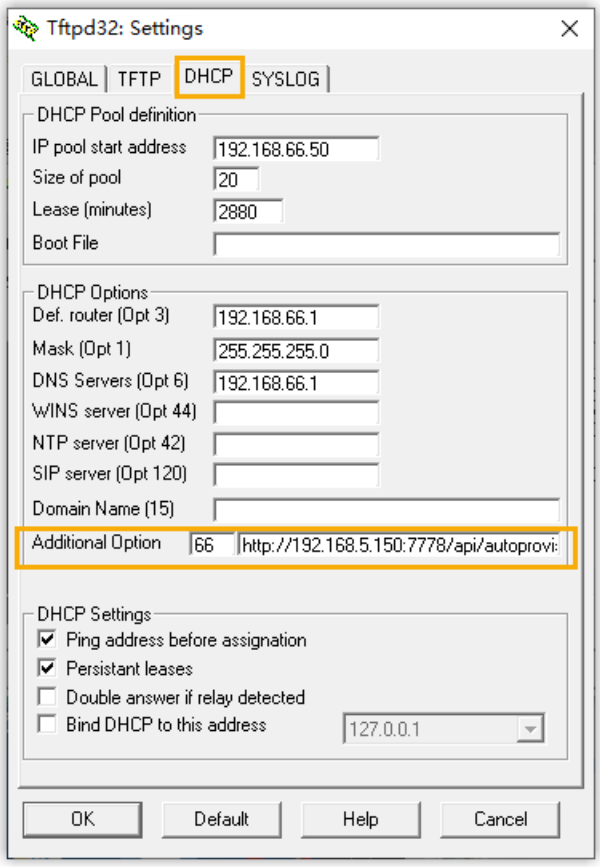
1. Run the Tftpd32 software, click **Settings** at the bottom of the window.



2. In the pop-up window, click **GLOBAL** tab, select the checkbox of **DHCP Server**.



3. Click **DHCP** tab, configure the DHCP server parameters.



- **IP pool start address**: The starting IP addresses to be allocated.
- **Size of pool**: Total number of available IP addresses.
- **Lease time**: IP address lease time.
- **Def. Router (Opt 3)**: The gateway IP address. In this example, enter `192.168.66.1`.
- **Mask (Opt 1)**: Subnet mask that corresponds to the available IP address segment.
- **DNS Server (Opt 6)**: DNS server address for the DHCP server. In this example, enter `192.168.66.1`.
- **Additional Option**: Enter option to `66` and paste the PBX provisioning link besides the option.

4. Click **OK**.

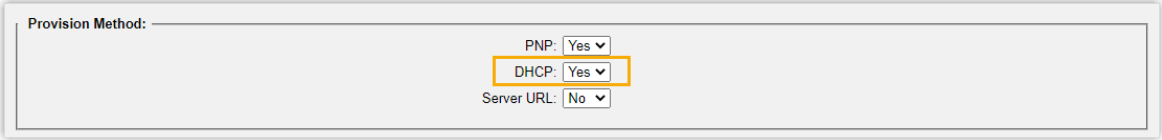
   The PC starts to work as a DHCP server.

Step4. Enable DHCP provisioning on the gateway

1. Reboot the gateway and get the IP address of the TA FXS gateway.

Connect an analog phone to any FXS port of the TA gateway, dial *** and follow the voice prompt to check the IP address.

2. Log in to the gateway web page by the IP address.
3. Go to **System > System Preferences > Auto Provision Settings**.
4. In the **Provision Method** section, enable the **DHCP** provisioning method.



5. Click **Save**, and then click **Apply Changes** appeared in the top-right corner.

Result

The extension registration status of provisioned analog phones is displayed on **Extension and Trunk > Extension**.

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

Auto Provision Yeastar TA FXS Gateway (Provision Link Method)

For Yeastar TA FXS gateways located in remote network, Yeastar P-Series PBX System supports remote provisioning using the Provision Link method through public IP address/domain name and port. By generating a provisioning link on the PBX and entering it on the gateway, remote provisioning can be completed effortlessly.

Supported gateway models

- TA100, TA200
- TA400, TA800
- TA1600, TA2400, TA3200

Prerequisites

- Set up PBX to make it ready for the remote provisioning.
  - Upgrade PBX firmware to version 37.18.0.18 or later.
  - Configure port forwarding on router and SIP NAT on PBX for remote access.

> **Important:**
> The following PBX ports must be forwarded.
> - RTP ports
> - SIP port
> - Web Server port

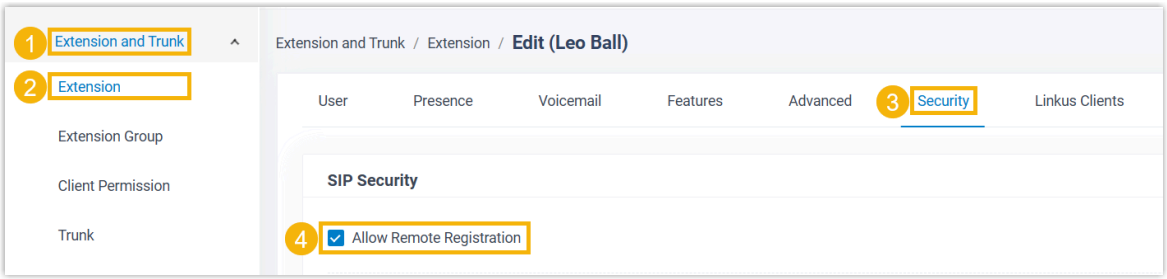
For more information, see Configure Network for Remote Access by a Domain Name and Configure Network for Remote Access by a Public IP Address.

- Configure transport protocol for Web server to HTTPS.

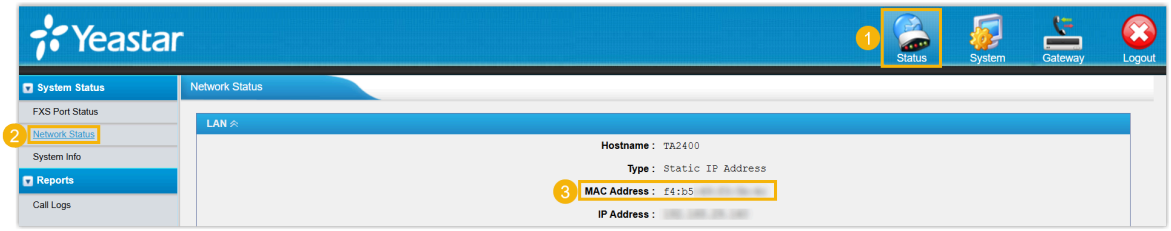
  For more information, see Change Web Server Protocol and Port.
- Download the latest template for Yeastar TA FXS gateway.

  For more information, see Update a Default Auto Provisioning Template.

- Set up extension(s) to make them ready for the remote registration.

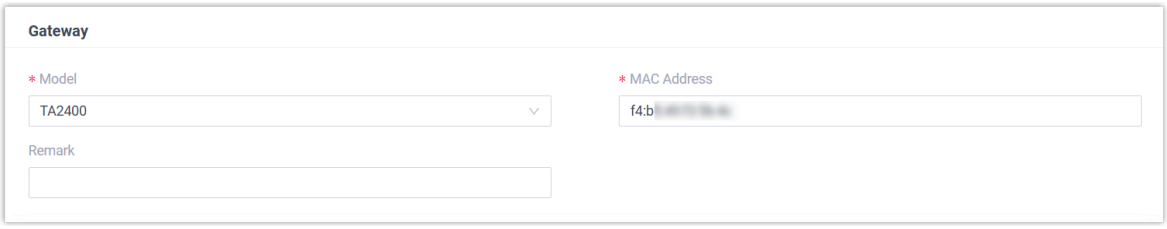


- Gather MAC address of TA FXS gateway.



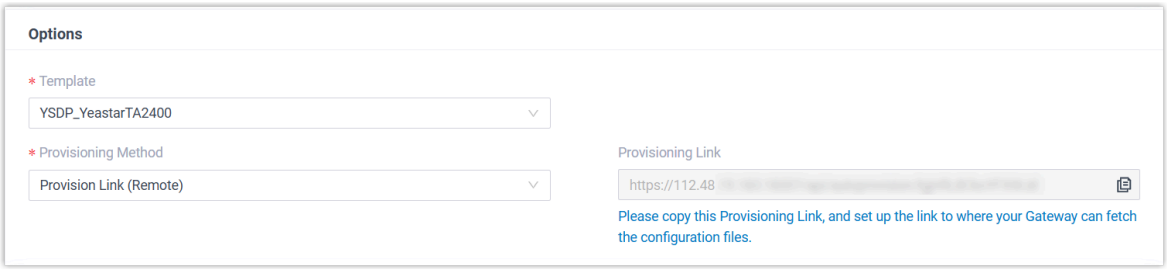
Step 1. Generate configuration file for a gateway on the PBX

1. Log in to PBX web portal, go to **Auto Provisioning > Gateways**.
2. Click **Add** to add a gateway.
3. In the **Gateway** section, configure gateway information as follows:



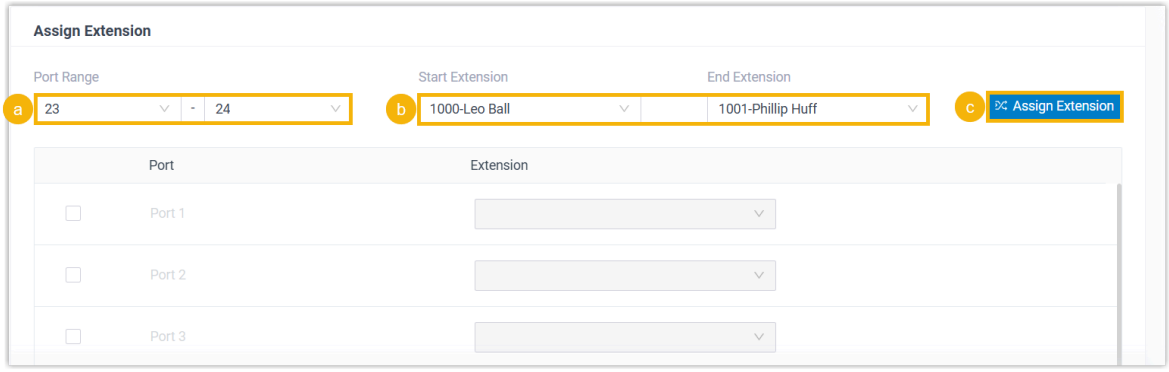
- **Model**: Select a gateway model.
- **MAC Address**: Enter MAC address of the gateway.
- **Remark**: Optional. Add a short description about the gateway.

4. In the **Options** section, configure the following settings to generate a configuration file for the gateway.



- **Template**: Select the corresponding template from the drop-down list.
- **Provisioning Method**: Select **Provision Link (Remote)**.
- **Provisioning Link**: Click to copy the provisioning link, as you will use it later.

5. In the **Assign Extension** section, assign extension(s) to the gateway port(s).

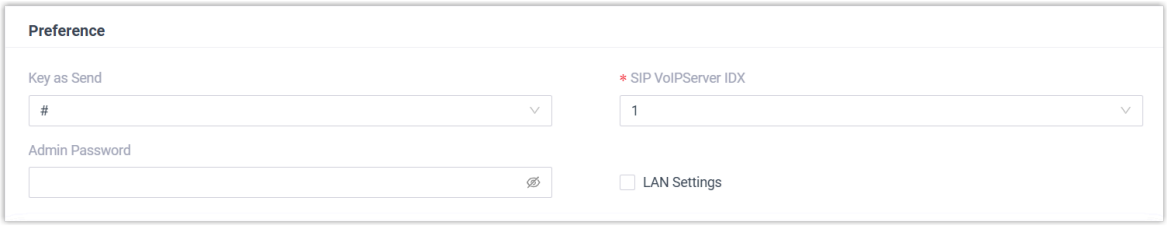


a. In the **Port Range** field, select the port range to assign extension(s).
b. In the **Start Extension** and **End Extension** field, select the extension range to assign the extensions to the specified ports.
c. Click **Assign Extension**.

The ports with assigned extensions are displayed below.

> **Tip:**
> If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other IP phone or gateway.
> - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
> - To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

6. **Optional:** In the **Preference** section, configure the settings as needed.

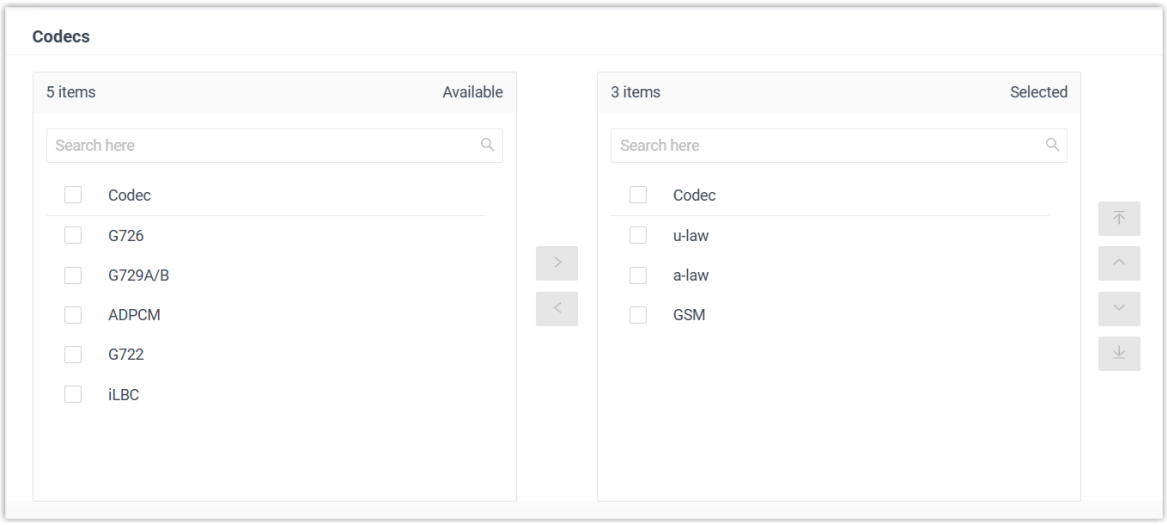


- **Key as Send**: Assign the pound key (“#”) or asterisk key (“*”) as the send key.
- **SIP VoIPServer IDX**: Select a VoIP server template ID to be provisioned.

> **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**: Keep it as default.

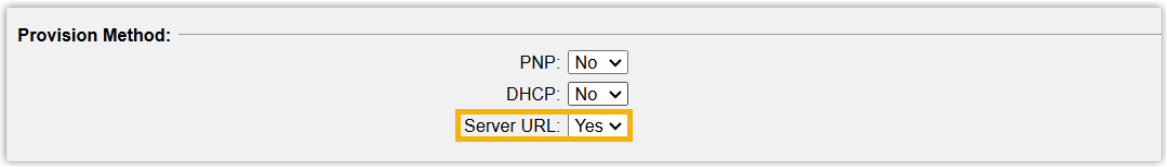
7. **Optional:** In the **Codecs** section, select your preferred codec list for the gateway.



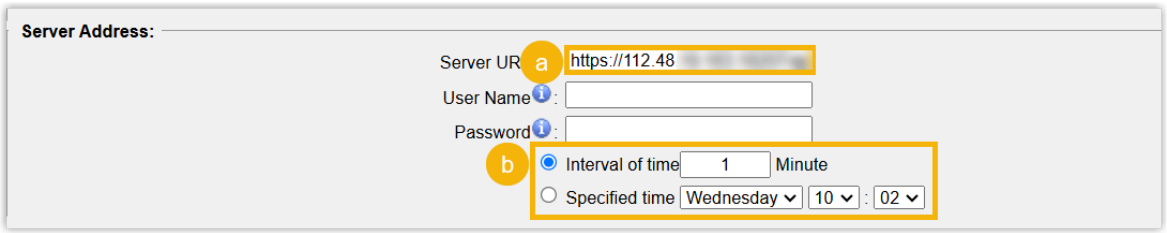
8. Click **Save**.

Step 2. Make the configuration file accessible to the gateway

1. Log in to the gateway web interface, go to **System > System Preferences > Auto Provision Settings**.
2. In the **Provision Method** section, set **Server URL** to **Yes**.



3. In the **Server Address** section, complete the following settings:



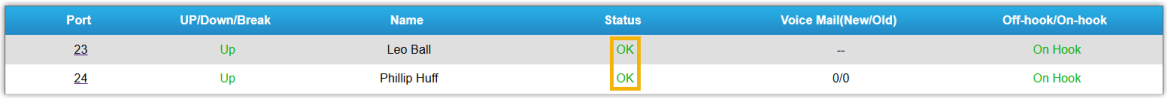
   a. In the **Server URL** field, paste the [provisioning link] that you have obtained from PBX.
   b. Set the time to perform auto provisioning.
4. Click **Save** and **Apply Changes**.

Result

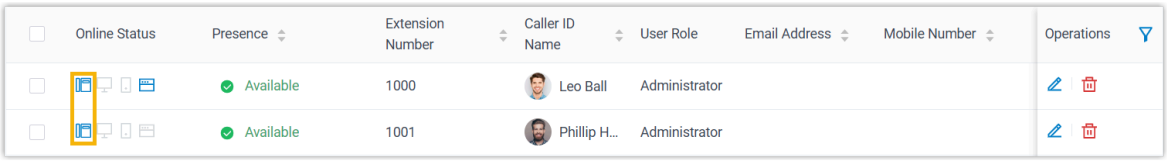
After the specified time, the configurations are applied to the gateway, and the specified extension(s) are registered on the corresponding port(s) of TA FXS gateway.

You can check extension registration status in the following ways:

- On gateway web interface, the port status is displayed as **OK** (Path: **Status > System Status > FXS Port Status**).



- On PBX web portal, the extension status is displayed as  (Path: **Extension and Trunk > Extension > Online Status**).



Auto Provision Yeastar TA FXS Gateway (Provision Link FQDN Method)

For Yeastar TA FXS gateways located in remote network, Yeastar P-Series PBX System supports remote provisioning using the Provision Link FQDN method through Yeastar-supplied Fully Qualified Domain Name (FQDN). By generating a provisioning link on the PBX and entering it on the gateway, remote provisioning can be completed effortlessly.

Supported gateway models

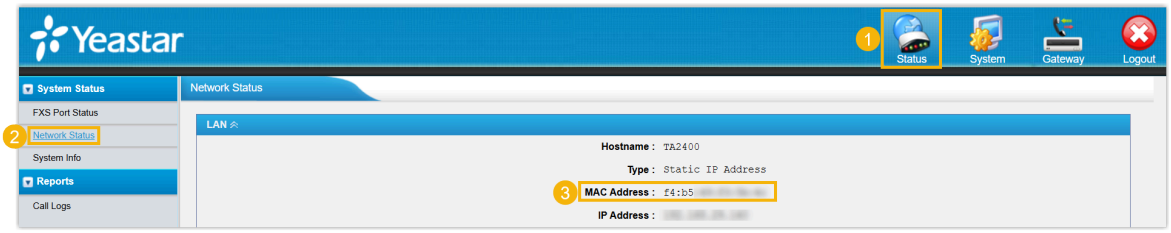
- TA100, TA200
- TA400, TA800
- TA1600, TA2400, TA3200

Prerequisites

- Set up PBX to make it ready for the remote provisioning.
  - Upgrade PBX firmware to version 37.18.0.18 or later.
  - Configure Yeastar FQDN on PBX, and enable Web access and SIP access for the extension(s) to be assigned to gateway.

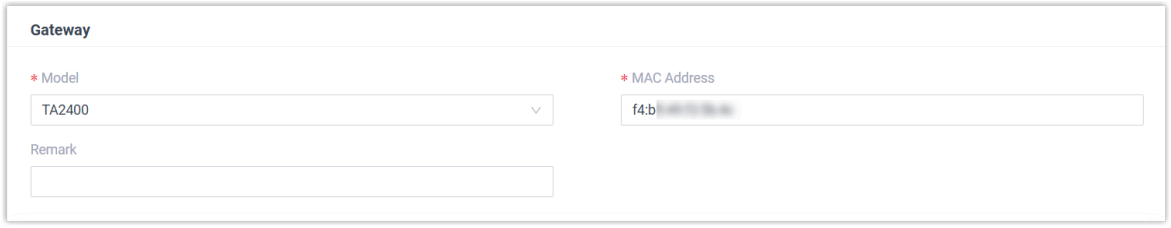
For more information, see Configure Network for Remote Web Access by a Yeastar FQDN and Configure Network for Remote SIP Access by a Yeastar FQDN.

- Gather MAC address of TA FXS gateway.

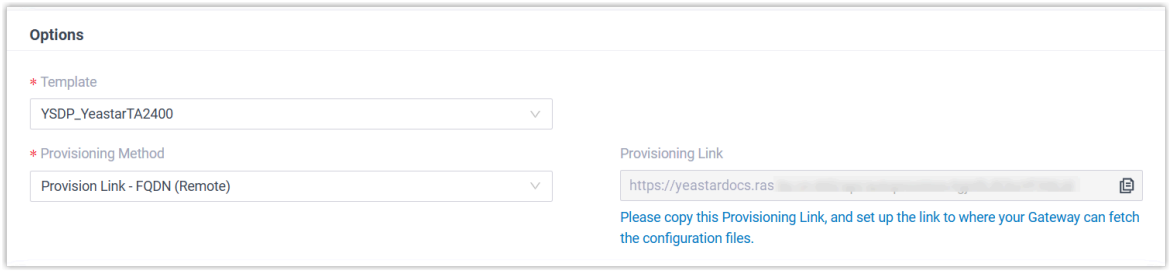


Step 1. Generate configuration file for a gateway on the PBX

1. Log in to PBX web portal, go to **Auto Provisioning > Gateways**.
2. Click **Add** to add a gateway.
3. In the **Gateway** section, configure gateway information as follows:



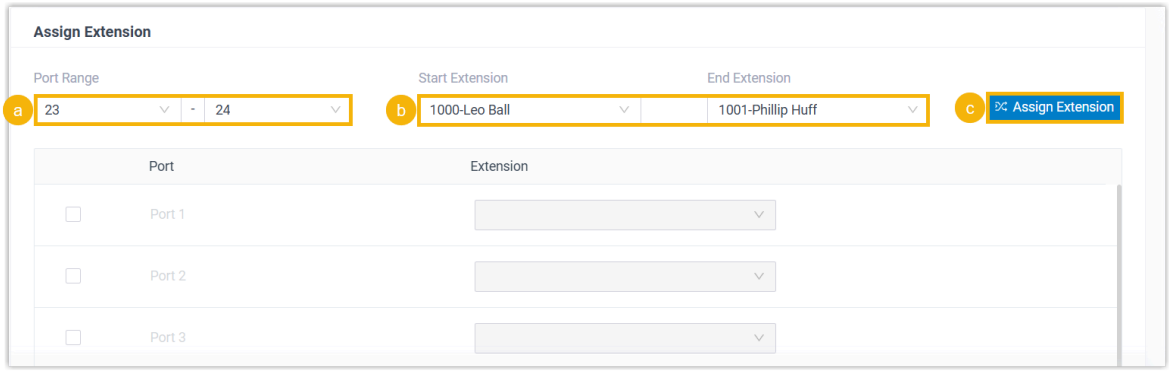
   - **Model**: Select a gateway model.
   - **MAC Address**: Enter MAC address of the gateway.
   - **Remark**: Optional. Add a short description about the gateway.
4. In the **Options** section, configure the following settings to generate a configuration file for the gateway.



   - **Template**: Select the corresponding template from the drop-down list.
   - **Provisioning Method**: Select **Provision Link - FQDN (Remote)**.

- **Provisioning Link**: Click to copy the provisioning link, as you will use it later.

5. In the **Assign Extension** section, assign extension(s) to the gateway port(s).

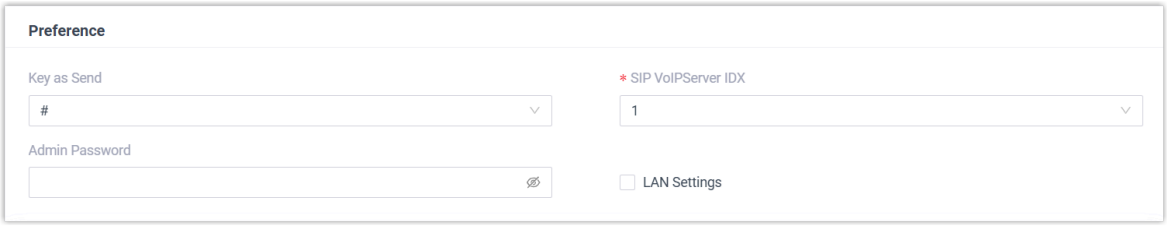


   a. In the **Port Range** field, select the port range to assign extension(s).
   b. In the **Start Extension** and **End Extension** field, select the extension range to assign the extensions to the specified ports.
   c. Click **Assign Extension**.

      The ports with assigned extensions are displayed below.

> **Tip:**
> If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other IP phone or gateway.
> - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
> - To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

6. **Optional:** In the **Preference** section, configure the settings as needed.

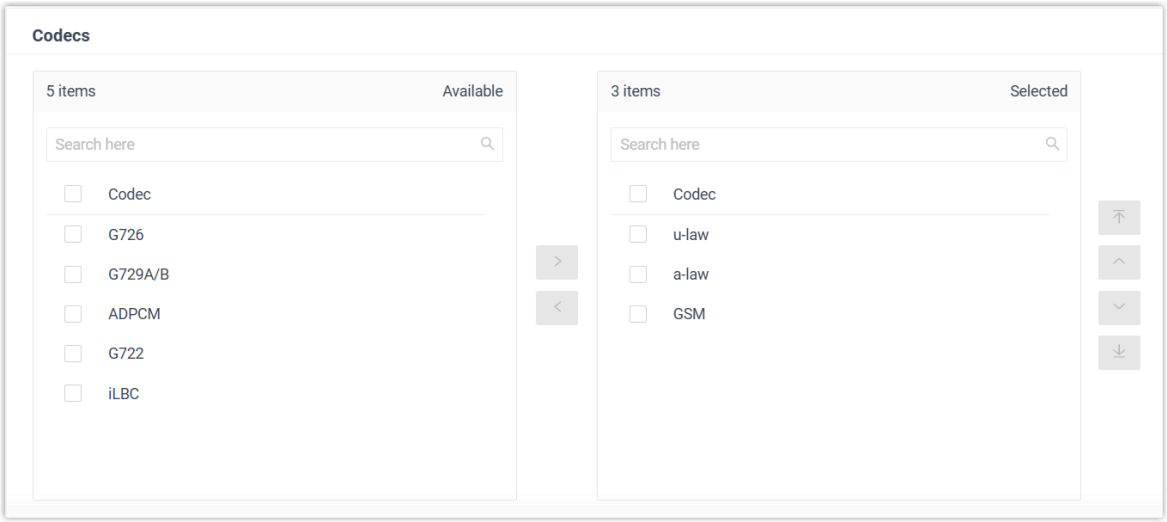


- **Key as Send**: Assign the pound key (“#”) or asterisk key (“*”) as the send key.
- **SIP VoIPServer IDX**: Select a VoIP server template ID to be provisioned.

> **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**: Keep it as default.

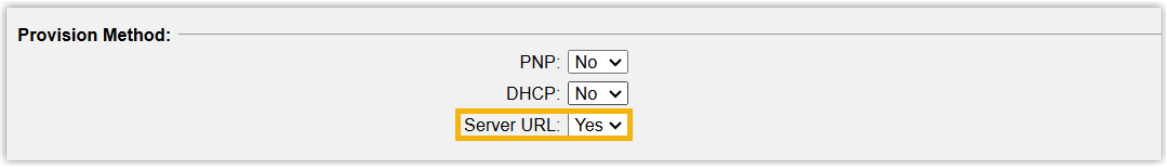
7. **Optional:** In the **Codecs** section, select your preferred codec list for the gateway.



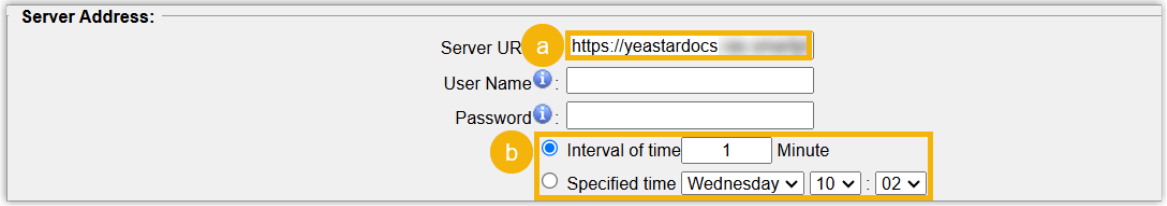
8. Click **Save**.

Step 2. Make the configuration file accessible to the gateway

1. Log in to the gateway web interface, go to **System > System Preferences > Auto Provision Settings**.
2. In the **Provision Method** section, set **Server URL** to **Yes**.



3. In the **Server Address** section, complete the following settings:



a. In the **Server URL** field, paste the provisioning link that you have obtained from PBX.
b. Set the time to perform auto provisioning.

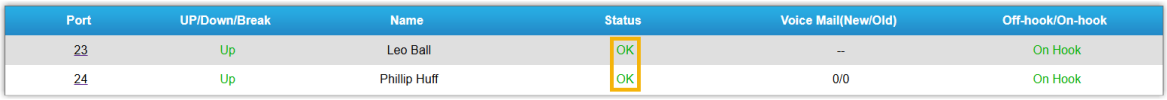
4. Click **Save** and **Apply Changes**.

Result

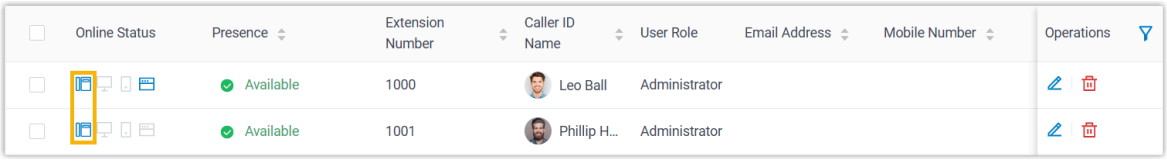
After the specified time, the configurations are applied to the gateway, and the specified extension(s) are registered on the corresponding port(s) of TA FXS gateway.

You can check extension registration status in the following ways:

- On gateway web interface, the port status is displayed as **OK** (Path: **Status > System Status > FXS Port Status**).



- On PBX web portal, the extension status is displayed as  (Path: **Extension and Trunk > Extension > Online Status**).



Manage Provisioned Devices

Remotely Access a Provisioned IP Phone / Gateway

Yeastar P-Series PBX System allows users to visit a provisioned IP phone or gateway when remotely accessing the PBX. This topic describes how to remotely connect to and access IP phone or gateway from the PBX.

Scenario

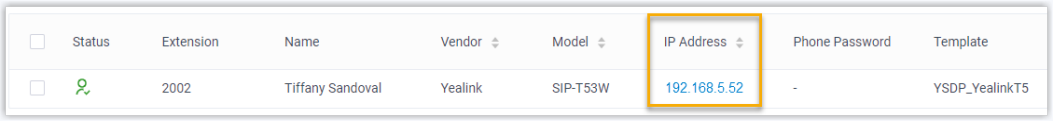
When tech supporters visit your PBX via either the FQDN domain name or a visit link randomly generated for PBX Remote Management to provide remote troubleshooting, they might also need to examine the configurations of the connected IP phones / gateways to address the problems.

For this sake, Yeastar P-Series PBX System supports to visit the IP phones / gateways when remotely accessing the PBX. Tech supporters can directly visit the web interface of an IP phone or a gateway from the PBX auto provisioning device list and conduct troubleshooting on the IP phone or gateway remotely.

Prerequisites

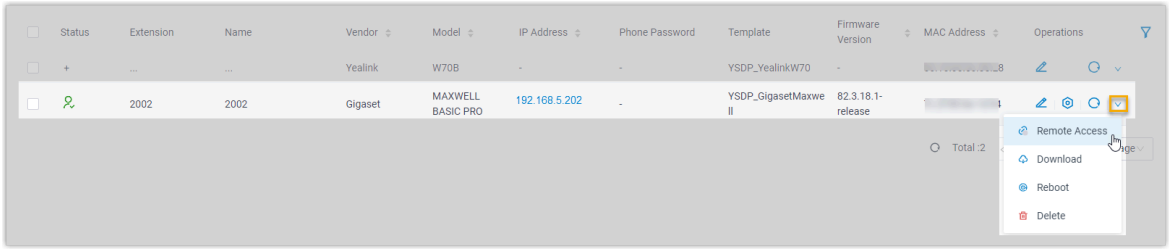
To implement the IP phone / gateway remote access, make sure the followings are ready:

- The PBX firmware version is 37.7.0.16 or later.
- Remote access to the PBX system via the FQDN domain name, or via the visit link randomly generated for PBX Remote Management.
- The PBX can visit the web interface of the IP phone / gateway in the local network.

> **Tip:**
> To make sure of this, check if the private IP address of the IP phone / gateway is recognized and displayed in the **Auto Provisioning** device list.
>
> 
>

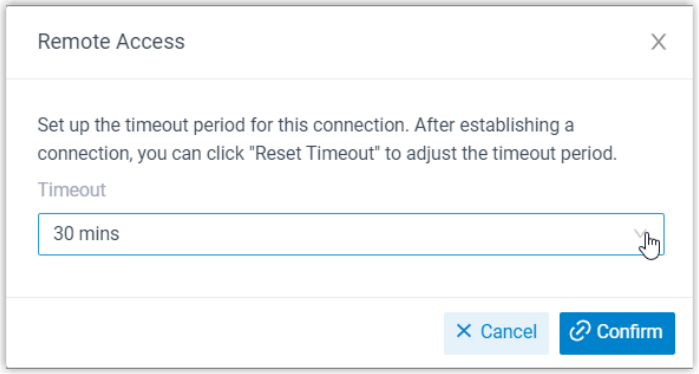
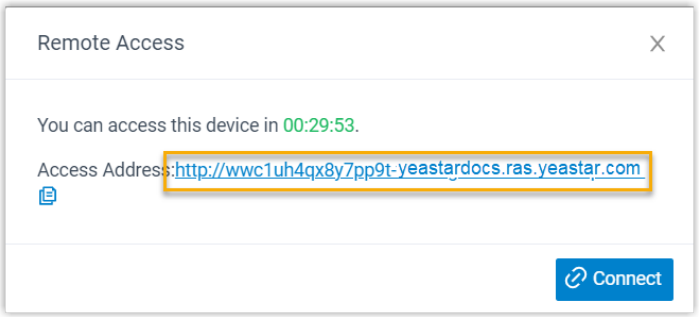
Remotely visit an IP phone on PBX

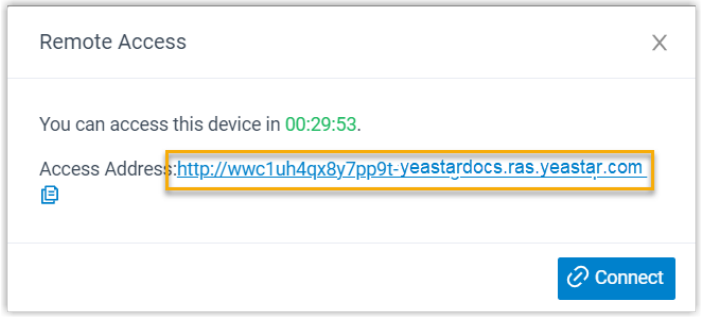
1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Hover the mouse over ⌄ beside the desired phone, and click **Remote Access**.



3. Connect to the IP phone as the following instructions guide according to the method users visit the PBX.

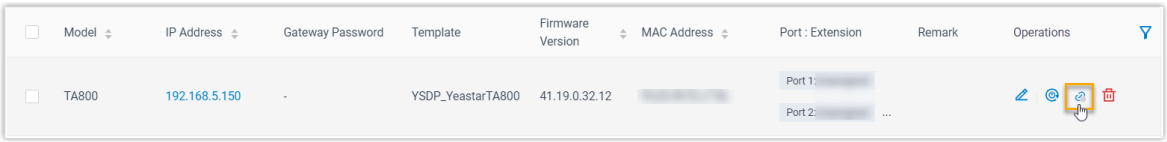
Table 13.

Method	Instruction
FQDN domain name	a. Set a connection timeout period. i. In the **Timeout** drop-down list of the pop-up window, set the timeout period.  ii. Click **Confirm**. The pop-up window displays a temporary remote access link and the connection time countdown; And the remote access icon turns to , indicating that the IP phone is connected.  b. Click **Connect** to visit the IP phone web interface.
Random PBX remote management link	The pop-up window directly displays a temporary link as well as the connection time countdown; And the remote access icon turns to , indicating that the IP phone is connected. **Note:** In this case, the time limit of IP phone remote access is synchronized with the remote management timeout of the PBX.

Method	Instruction
	 Click **Connect** to visit the IP phone web interface.

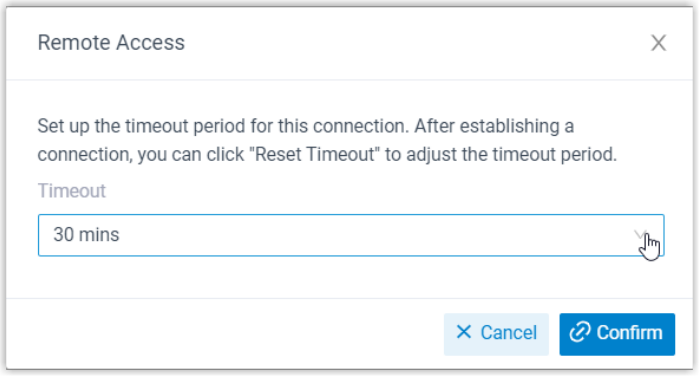
Remotely visit a gateway on PBX

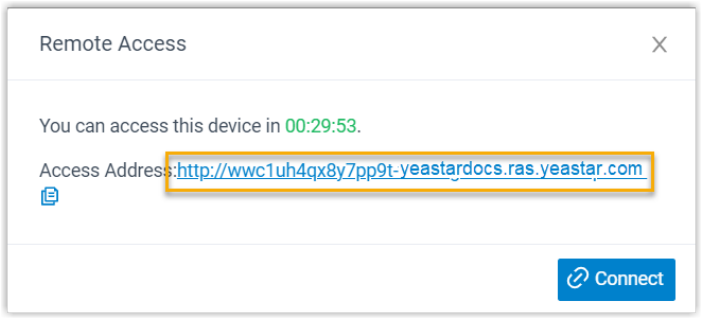
1. Log in to PBX web portal, go to **Auto Provisioning > Gateways**.
2. Click beside the desired gateway.

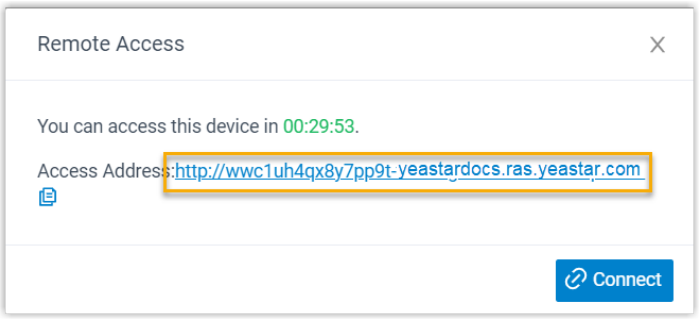


3. Connect to the gateway as the following instructions guide according to the method users visit the PBX.

Table 14.

Method	Instruction
FQDN domain name	a. Set a connection timeout period. i. In the **Timeout** drop-down list of the pop-up window, set the timeout period.  ii. Click **Confirm**.

<table>
<tr><th>Method</th><th>Instruction</th></tr>
<tr><td></td><td>The pop-up window displays a temporary remote access link and the connection time countdown; And the remote access icon turns to , indicating that the gateway is connected.
 

b. Click Connect to visit the gateway web interface.</td></tr>
<tr><td>Random PBX remote management link</td><td>The pop-up window directly displays a temporary link as well as the connection time countdown; And the remote access icon turns to , indicating that the gateway is connected.
Note:
In this case, the time limit of gateway remote access is synchronized with the remote management timeout of the PBX.
 

Click Connect to visit the gateway web interface.</td></tr>
</table>

FAQ

How to extend the IP phone / Gateway remote access time

After the connection is established, users can re-configure the timeout period to extend the connection time.

Note:

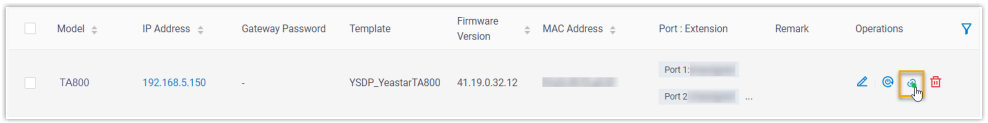
- Only when users access the PBX via the FQDN domain name can they reset the time limit of IP phone / gateway remote access on the PBX.
- If users access the PBX via a random visit link for PBX remote management, please contact the device provider to extend the remote access time.

1. On PBX web portal, go to **Remote Access** setting of the connected device.

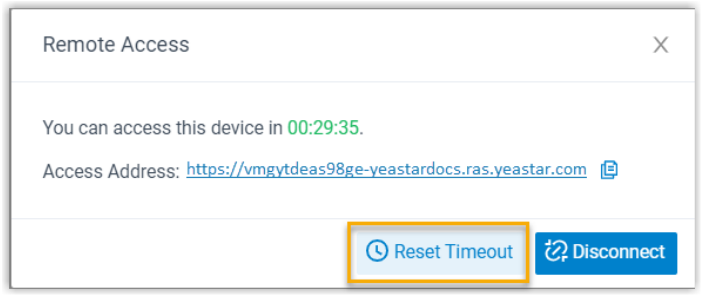
   IP Phone

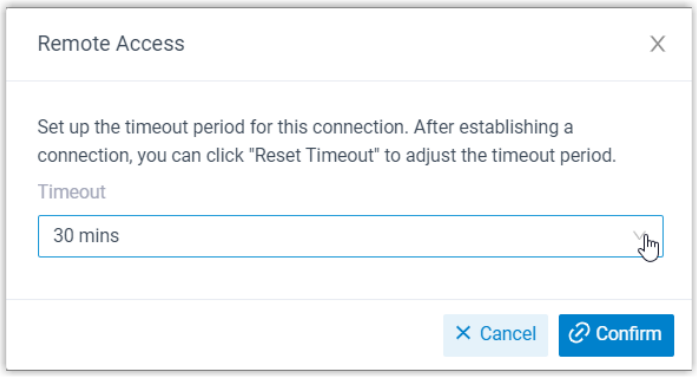
   Gateway

2. In the pop-up window, click **Reset Timeout**.

3. Reset the **Timeout** and click **Confirm**



The pop-up window displays the new countdown of connection time.

Reboot Provisioned IP Phones/Gateways

For some settings that need a device reboot to take effect, you can reboot the device remotely on PBX web portal if these devices have been auto provisioned on PBX.

Reboot provisioned IP phones

1. Log in to PBX web 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**.

Reboot provisioned gateways

1. Log in to PBX web 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**.

Reassign an Extension to a Provisioned IP Phone/Gateway

If a phone is previously provisioned but the phone owner or gateway port has been changed, you can reassign an extension to the provisioned phone or gateway.

Reassign an extension to a provisioned IP Phone

Procedure

1. Log in to PBX web 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 IP phone or gateway.
   > - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
   > - 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.

Reassign an extension to a provisioned gateway

Procedure

1. Log in to PBX web 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 IP phone or gateway.
>
> - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
> - To associate an extension with multiple IP phones, 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 IP Phone/Gateway

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

Release an extension from a provisioned phone

1. Release the extension from previous phone.
   a. Log in to PBX web 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.

Release an extension from a provisioned gateway

Procedure

1. Release the extension from previous port.
    a. Log in to PBX web 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.

Remove IP Phones/Gateways from Provisioning List

The provisioning list always displays all the devices that are discovered. For the out-of-use devices, you can remove them from the phone/gateway provisioning list manually.

Remove phones from provisioning list

Procedure

1. Log in to PBX web 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

The system erases all configuration files for the phone and releases the assigned extension.

Remove gateways from provisioning list

Procedure

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

2. 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**.
3. Click **OK**.

Result

The system erases all configuration files for the gateways and releases the assigned extension.

Export and Import Auto Provisioning Phone Information

The phones' information in the Auto Provisioning phone list can be exported and saved as a template. You can fill in the information of desired phones in the exported file, and import the file to PBX again, so as to add phones to the PBX in bulk conveniently. This topic describes how to export and import Auto Provisioning phone information.

Export Auto Provisioning phone information

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. At the top of the Auto Provisioning phone list, click **Export**.

   A CSV file is saved to your computer. To check and edit parameters in the CSV file, see Auto Provisioning Phone Information Parameters.

Import Auto Provisioning phone information

We recommend that you export Auto Provisioning phone information 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

Learn about the 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 Provisioning Phone Information Parameters.

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. At the top of the Auto Provisioning phone list, click **Import**.
3. In the pop-up window, click **Browse**, and select your CSV file.
4. Click **Import**.

   The phone information in the CSV file will be displayed in the Auto Provisioning phone list.

Related information

Import and Export -FAQ

Auto Provisioning Options

IP Phone Auto Provisioning Options

Yeastar P-Series PBX System provides a variety of Auto Provisioning options for IP phones that can meet general needs for end users. This topic introduces the settings that 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 Apply a New Template to a Provisioned IP Phone/Gateway.

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 the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)
- Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
- Auto Provision IP Phones Remotely (Provision Link Method)
- Reassign an Extension to a Provisioned IP Phone/Gateway

VLAN settings

Yeastar P-Series PBX System allows you to configure VLAN settings for a provisioned phone (either for the WAN port or PC port), or set the phone to acquire VLAN ID through DHCP option.

For more information, see Configure VLAN for a Provisioned Phone.

Function key

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.

Automatically Generate Random Passwords for Phones

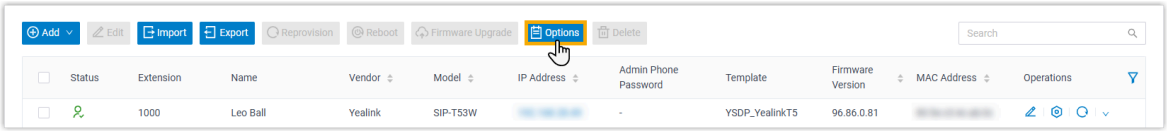
Yeastar P-Series PBX System supports to generate random and complex passwords for admin, user, and var accounts on auto provisioned phones, eliminating the need to manually change the default password for each phone. This topic describes how to enable this feature on PBX.

Requirements

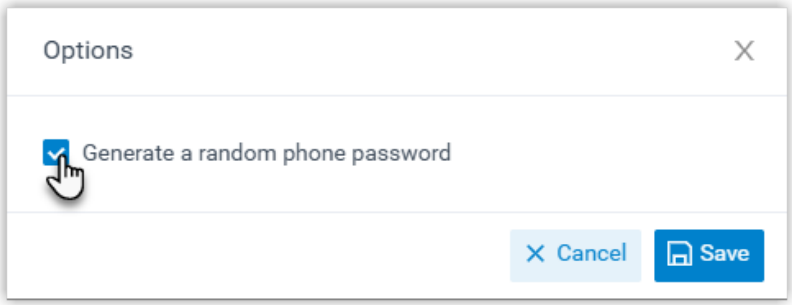
The PBX firmware version is 37.18.0.102 or later.

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. At the top of the list, click **Options**.



3. In the pop-up window, select the checkbox of **Generate a random phone password**, then click **Save**.

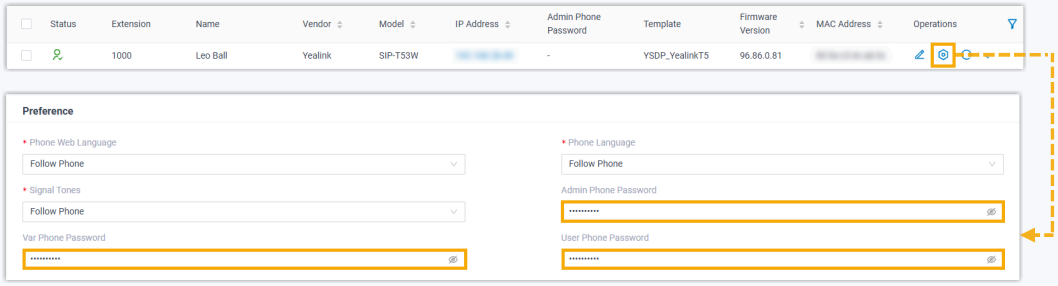


Result

When adding a phone, random phone password(s) are generated automatically.

Note:

- If you want to change the password, click , then edit the password in the corresponding fields.



- For DECT phones provisioned via PnP method, the default password will be used instead of a random one.

Configure VLAN for a Provisioned Phone

Yeastar P-Series PBX System allows you to configure the VLAN settings for a provisioned phone, which helps to enhance the quality of VoIP calls. This topic describes how to configure the VLAN settings for a phone via Auto Provisioning.

Requirements

The PBX firmware version is 37.18.0.18 or later.

Prerequisites

The phone is connected to Yeastar P-Series PBX System via Auto Provisioning, and has been assigned an extension.

For more information, see the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)
- Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
- Auto Provision IP Phones Remotely (Provision Link Method)

Procedure

- Step 1. Configure VLAN settings for the IP phone on PBX
- Step 2. Apply the configuration to IP phone

Step 1. Configure VLAN settings for the IP phone on PBX

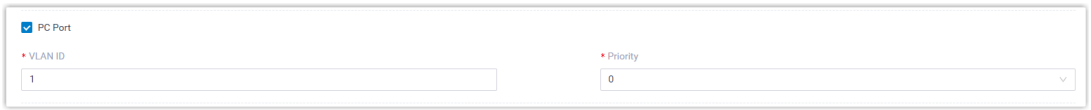
> **Note:**
> The VLAN settings vary according to different phone models.

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**, then click to edit the desired phone.
2. Scroll down to the **VLAN** section, then complete the following settings as needed.
   - To configure VLAN for WAN port of the phone, do as follows:



     a. Select the checkbox of **WAN Port**.
     b. In the **VLAN ID** field, enter a VLAN ID.
     c. In the **Priority** drop-down list, select a priority value for the VLAN.

     The priority value is between `0` (lowest) to `7` (highest).
   - To configure VLAN for PC port of the phone, do as follows:



     a. Select the checkbox of **PC port**.
     b. In the **VLAN ID** field, enter a VLAN ID.
     c. In the **Priority** drop-down list, select a priority value for the VLAN.

     The priority value is between `0` (lowest) to `7` (highest).
   - To acquire VLAN ID through DHCP option, do as follows:



     a. Select the checkbox of **DHCP VLAN**.
     b. In the **Option** field, enter the DHCP option(s) from which the phone will obtain the VLAN ID.

     > **Note:**
     > Use a comma to separate multiple DHCP options.

3. Click **Save**.

Step 2. Apply the configuration to IP phone

1. Go to **Auto Provisioning > Phones**, click beside the desired phone.

   The system prompts you whether to reprovision the phone.
2. In the pop-up window, click **OK**.

Result

The phones automatically apply the changes. Check the VLAN settings on the phone to see if the changes are applied.

Auto Provision Function Keys for Phones

Function keys allow extension users to monitor status of specific objects or quickly perform specific operations from Linkus or IP phone. This topic describes how to provision function keys for extension users' IP phones.

Supported key types

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

Key type	Function
N/A	No functionality.
Line	Configure line keys.
BLF	• Extension ◦ Monitor the call status of a specific extension. ◦ Monitor the DND (Do Not Disturb) presence of a specific extension. ◦ Place a call to the monitored extension. ◦ Pick up calls ringing on the monitored extension. • Trunk ◦ Monitor the status of a specific trunk. ◦ Place an outbound call through the monitored trunk. • Queue ◦ Monitor specific pause status of a queue agent. For more information, see Auto Provision a function key for an IP phone.
Speed Dial	Place a call to the most commonly dialed numbers or extensions.

Key type	Function
Check Voicemail	• Monitor the status of voicemail. • Check voicemail messages.
Check Group Voicemail	• Monitor the status of group voicemail in shared mode. • Check group voicemail messages.
Park & Retrieve	• 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 to the monitored extension to make an announcement.
DTMF	Send DTMF signals directly instead of manually entering the numbers each time.
Agent Login/Logout	• Monitor login status in a specific queue. • Log in to or log out of a specific queue.
Agent Pause/Unpause	• Monitor service status in a specific queue. • Pause or unpause receiving a call from a specific queue.
LDAP Directory	Quickly access the LDAP phonebook to query contact information. **Note:** This key type is only available for IP phone.
Boss-Secretary Feature	• For boss extensions: Monitor Secretary's Call Status. • For secretary extensions: Monitor Boss's Call Status.
Call Forward	Quickly enable or disable call forwarding. **Note:** The key type is only available for IP phone. For more information, see Forward All Incoming Calls to Another Destination by BLF Key.
Action URL	Quickly send an HTTP GET request to a specified URL for reporting specific events. **Note:** The key type is only available for IP phone.

Note:

If your desired function keys are not listed in the supported key types, you can create a custom Auto Provisioning template and apply the template to a provisioned IP phone.

Prerequisites

You have connected the IP phone to the PBX and associate it with an extension via auto provisioning. For more information about the configuration, see the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)
- Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
- Auto Provision IP Phones Remotely (Provision Link Method)

Auto Provision a function key for an IP phone

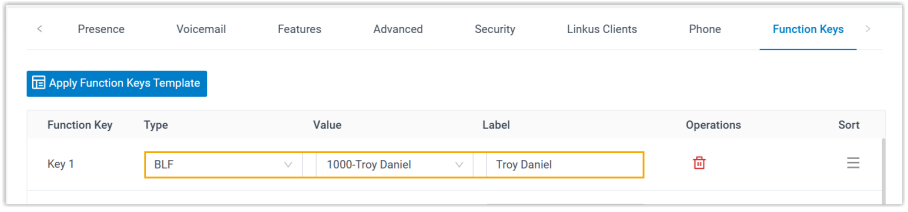
This section use the BLF function key as an example to show how to auto provision a specific function key to an IP phone.

1. Set up function key.
   a. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
   b. Click beside the desired phone.

      You are redirected to the setting page of the extension associated with the phone.
   c. Click the **Function keys** tab, then configure a BLF key according to your needs.
      - Monitor extension status by BLF key
      - Monitor trunk status by BLF key
      - Monitor agent status by BLF key

Monitor extension status by BLF key

Configure a BLF key to monitor a specific extension's status in real time, make calls to it, or pick up its incoming calls with a single press.



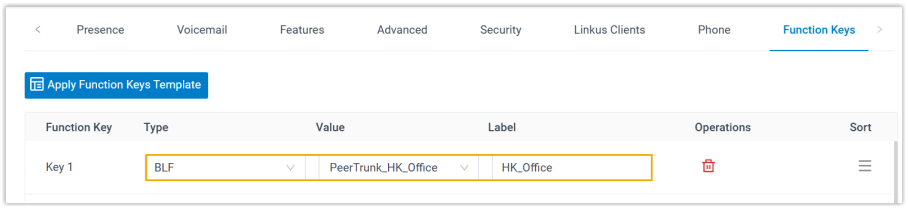
- **Type**: Select **BLF**.
- **Value**: In the drop-down list, select an extension to monitor.
- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

Monitor trunk status by BLF key

Configure a BLF key to monitor a specific trunk's status in real time, and seize the trunk to make outbound calls with a single press.

Note:

- Monitoring trunks by BLF key is NOT supported on E1/T1 trunk and BRI trunk.
- To seize a trunk to call out by BLF key, make sure the extension has the permission to use the monitored trunk for outbound calls.



- **Type**: Select **BLF**.
- **Value**: Enter the name of the trunk to be monitored.
- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

Monitor agent status by BLF key

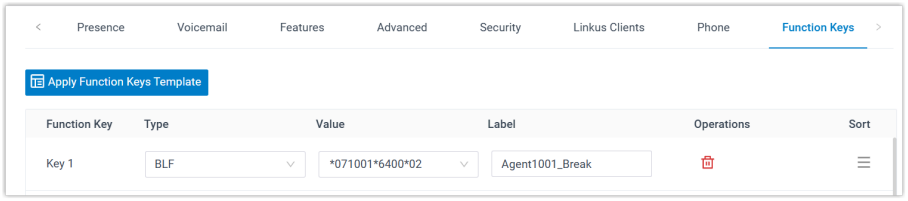
Configure a BLF key to monitor specific pause status of a queue agent.

Note:

Before you set up, you need to obtain the following feature codes:

- Pause feature code (Path: **Call Features > Feature Code > Queue > Pause/Unpause**)

> • Pause Reason feature code (Path: **Call Features > Feature Code > Pause Reason**)



- **Type**: Select **BLF** key.
- **Value**: Enter the feature codes.

  The format should be `Pause feature code` + `extension number` + `*` + `queue number` + `pause reason feature code`. For example, `*071001*6400*01`.
- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

d. Click **Save**.

2. Reprovision IP phones with the extensions registered.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone.
   c. In the pop-up window, click **OK**.

   The phone automatically applies the change, and the BLF key shows the real-time status of the monitored item.

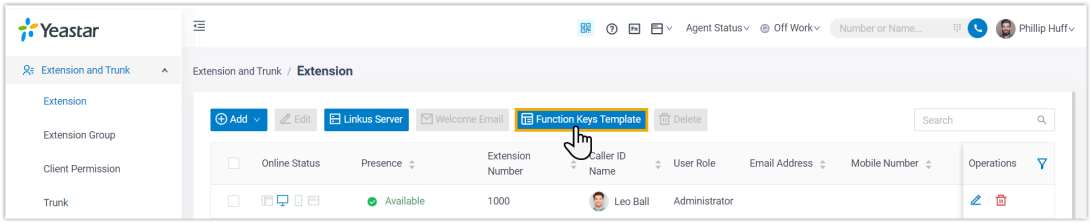
Scenario	BLF LED
Monitor extension status by BLF key	• **Solid Green**: The extension is being monitored, and the status is idle. • **Solid Red**: The extension is sending a call or is in a call; or the extension presence is DND (Do Not Disturb). **Note:** For Fanvil IP phones that support differentiated DND status indication, the DND status is indicated by a **Solid Yellow** LED light. • **Flashing Red**: The extension is ringing. • **LED off**: The extension is not registered, or the extension has been deleted from the PBX system. **Note:**

Scenario	BLF LED
	You can press the BLF key on the phone to achieve the followings: • Place a call to the monitored extension. • Pick up the monitored extension's incoming calls if the corresponding feature code is enabled on **Call Features > Feature Code > Call Pickup > Extension Pickup**.
Monitor trunk status by BLF key	• **Solid Green**: The trunk is being monitored, and the status is idle. • **Solid Red**: The trunk is busy. • **LED off**: The BLF key configuration failed. **Note:** You can press the BLF key to seize the trunk, then dial a number after a dial tone to call out.
Monitor agent status by BLF key	• **Solid Green**: The monitored agent is NOT in the specified pause status. • **Flashing Red**: The agent is in the specified pause status. • **LED off**: The BLF key configuration failed.

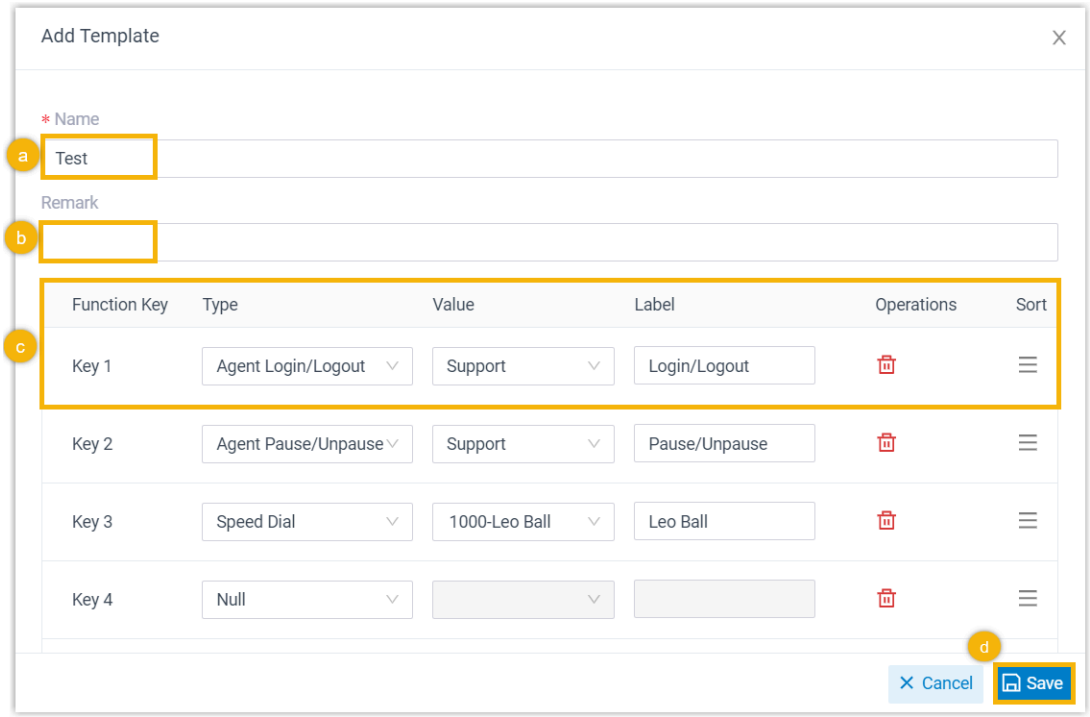
Auto Provision function keys for phones in bulk using a function key template

If you are managing many IP phones and want to simplify configuration while ensuring consistency across all phones, you can auto provision function keys in bulk using a function key template.

1. Add a function keys template.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
   b. Click **Function Keys Template**.



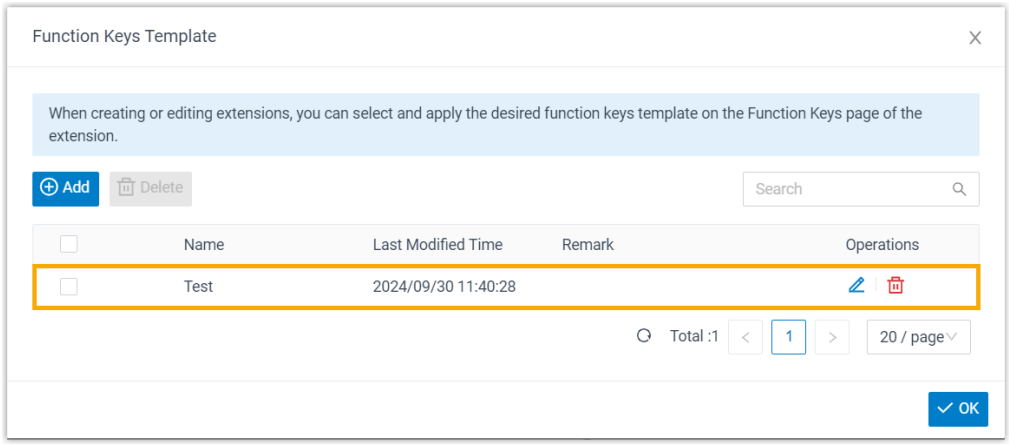
   c. Click **Add** to add a function key template, then configure the following settings.



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 excess function keys cannot take effect. However, if the user's IP phone is connected with an expansion module, the excess function keys are automatically applied to the expansion module.

i. In the **Name** field, enter a name to help you identify the template.
ii. **Optional:** In the **Remark** field, enter a short description about the template.
iii. In the function keys list, configure function keys according to your needs.
   - **Type**: Select a key type.
   - **Value**: Configure a desired value based on the key type.
   - **Label**: Optional. Enter a value to help extension users identify the function key.
iv. Click **Save**.

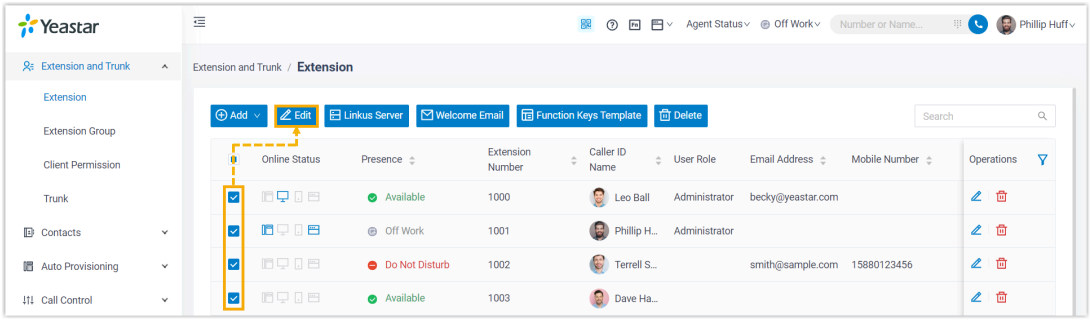
The function key template is created and displayed on the list.



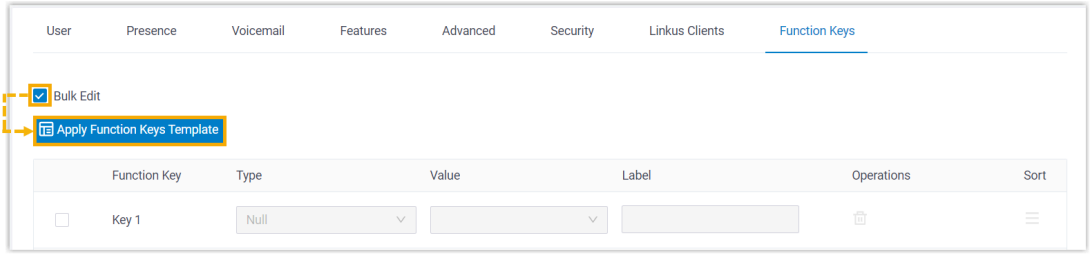
d. Click **OK**.

2. Apply the function keys template to extensions.

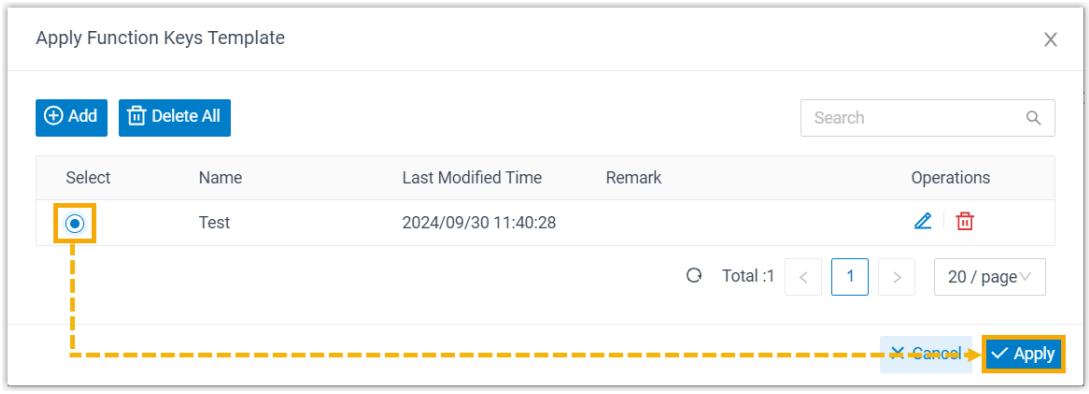
a. On the extension list, select the checkboxes of the desired extensions, then click **Edit**.



b. Under **Function Keys** tab, select the checkbox of **Bulk Edit**, then click **Apply Function Keys Template**.

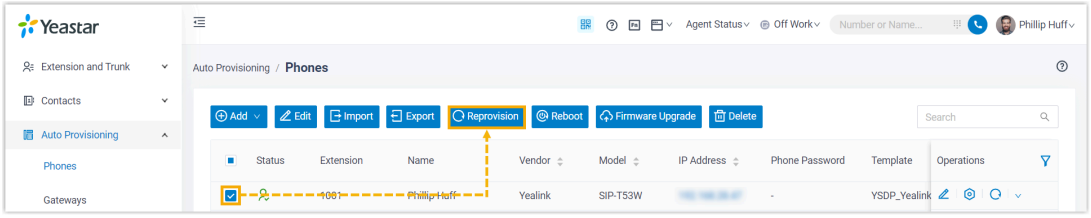


c. In the pop-up window, select the function keys template, then click **Apply**.



d. Click **Save**.

3. Reprovision IP phones with the extensions registered.
   a. Go to **Auto Provisioning > Phones**.
   b. Select the checkboxes of the desired phones, then click **Reprovision**.



   c. In the pop-up window, click **OK**.

      The phones automatically apply the changes. Check the function key status on the phones to see if the changes are applied.

Related information

[Auto Provision Yealink Expansion Module with Yeastar P-Series PBX System]

Seize a Trunk to Call Out by BLF Key

This topic describes how to configure a BLF key on your IP phone via Auto Provisioning to monitor the PBX trunk, and press the BLF key to quickly place an outbound call through the monitored trunk.

Restrictions

Monitoring trunks by BLF key is NOT supported on E1/T1 trunk and BRI trunk.

Prerequisites

- A phone is connected to Yeastar P-Series PBX System via Auto Provisioning, and has been assigned with an extension.

  For more information, see the following topics:

  - Auto Provision IP Phones in Local Network (PnP Method)
  - Auto Provision IP Phones in Local Network (DHCP Method)
  - Auto Provision IP Phones Remotely (RPS FQDN Method)
  - Auto Provision IP Phones Remotely (RPS Method)
  - Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
  - Auto Provision IP Phones Remotely (Provision Link Method)

- If you want to seize a trunk to call out by BLF key, make sure the extension assigned to the provisioned phone has the permission to use the monitored trunk for outbound calls.

Procedure

- Step 1. Set up a function key for trunk monitoring
- Step 2. Apply the configuration to IP phone

Step 1. Set up a function key for trunk monitoring

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the extension that is assigned to the phone.
2. Click the **Function Keys** tab.
3. Configure a function key to monitor the status of a trunk.

   The following figure shows a configuration example of monitoring the trunk `peer-trunk-66.41`.



   - **Type**: Select **BLF**.
   - **Value**: Enter the name of the trunk to be monitored. In this example, enter `peer-trunk-66.41`.
   - **Label**: Optional. Enter a value, which will be displayed on the phone screen.

4. Click **Save**.

Step 2. Apply the configuration to IP phone

1. Go to **Auto Provisioning > Phones**, click beside the desired phone.

   The system prompts you whether to reprovision the phone.
2. In the pop-up window, click **OK**.

Result

- The BLF key shows the real-time status of the monitored trunk:
  - **Green BLF LED**: The trunk is being monitored, and the status is idle.
  - **Red BLF LED**: The trunk is busy.
  - **BLF LED off**: The BLF key configuration failed.
- Press the BLF key to seize the trunk, you will get a dial tone, then dial the number that you want to call.

Forward All Incoming Calls to Another Destination by BLF Key

You can set up call forwarding for provisioned IP phones through Yeastar P-Series PBX System. This topic describes how to set a BLF key on the IP phone via Auto Provisioning, so that users can quickly enable forwarding for all incoming calls by the BLF key.

> **Note:**
> This feature is independent of the extension's call forwarding settings based on presence or feature code. Call forwarding by BLF key is only available for IP phone and will forward all incoming calls to the predefined destination.

Prerequisites

A phone is connected to Yeastar P-Series PBX System via Auto Provisioning, and has been assigned with an extension.

For more information, see the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

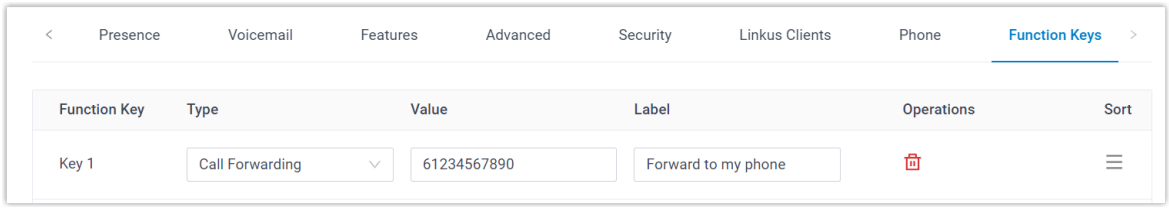
- Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
- Auto Provision IP Phones Remotely (Provision Link Method)

Procedure

- Step 1. Set up a function key for call forwarding
- Step 2. Apply the configuration to IP phone

Step 1. Set up a function key for call forwarding

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the extension that is assigned to the phone.
2. Click the **Function Keys** tab.
3. Configure a function key to set up call forwarding.



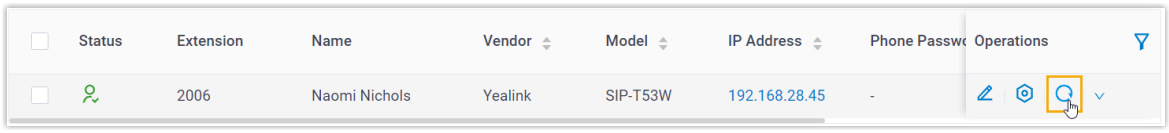
   - **Type**: Select **Call Forwarding**.
   - **Value**: Enter the number to which you want to forward all calls.

     Note:
     If the number is an external number, make sure that the extension associated with the phone has permission to use the outbound route, or the call forwarding would fail.

   - **Label**: Optional. Enter a value, which will be displayed on the phone screen.
4. Click **Save**.

Step 2. Apply the configuration to IP phone

1. On PBX web portal, go to **Auto Provisioning > Phones**, click beside the associated IP phone.



2. In the pop-up window, click **OK**.

Result

- The BLF key shows the current status of the call forwarding:
  - **Green BLF LED**: The call forwarding is enabled.
  - **BLF LED off**: The call forwarding is disabled.
- User can quickly enable the call forwarding by pressing the BLF key, and all incoming calls sent to the extension will be forwarded to the preset destination.

  In this example, all incoming calls sent to extension 2006 will be forwarded to an external number 61234567890.

Synchronize Phone Time with Yeastar P-Series PBX System via Auto Provisioning

You can synchronize the time of the provisioned phone with Yeastar P-Series PBX System via Auto Provisioning feature.

Prerequisites

The phone is connected to Yeastar P-Series PBX System via Auto Provisioning, and has been assigned an extension.

For more information, see the following topics:

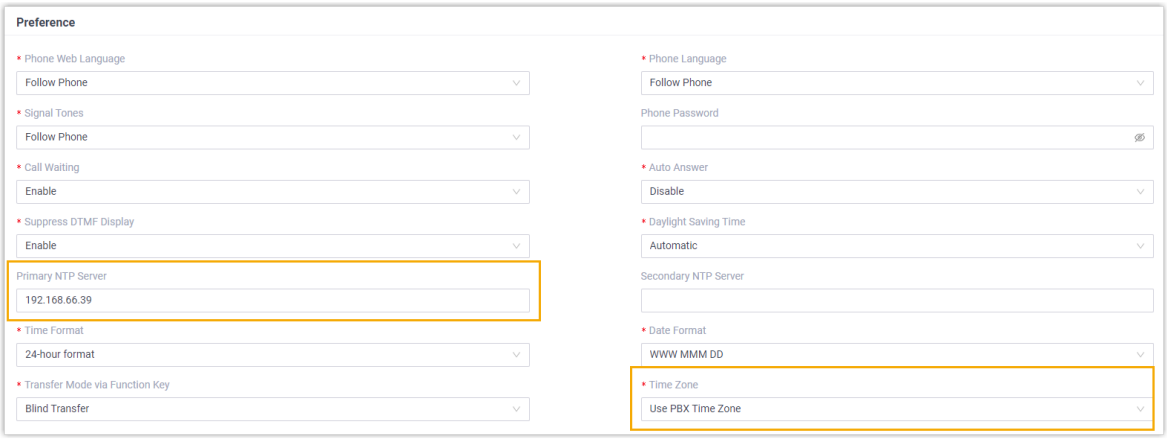
- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)
- Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
- Auto Provision IP Phones Remotely (Provision Link Method)

Procedure

- Step 1. Set up PBX as NTP Server
- Step 2. Apply the configuration to IP phone

Step 1. Set up PBX as NTP Server

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the extension that is assigned to the phone.
2. Click the **Phone** tab.
3. Scroll down to the **Preference** section, complete the following settings.



   - **Primary NTP Server**: Set the value as the IP address of your PBX.
   - **Time Zone**: Select **Use PBX Time Zone**.
4. Click **Save**.

Step 2. Apply the configuration to IP phone

1. Go to **Auto Provisioning > Phones**, click beside the desired phone.

   The system prompts you whether to reprovision the phone.
2. In the pop-up window, click **OK**.

Result

The phone time is now synchronized with the PBX.

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 web 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 web 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.

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.

Procedure

1. Log in to PBX web 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.

Manage Auto Provisioning Templates

Apply a New Template to a Provisioned IP Phone/Gateway

If you want to customize a device, you can create a custom template and apply the new template to the IP phone/gateway.

Apply a new template to a provisioned IP phone

Prerequisites

[Create a custom Auto Provisioning template](#).

Procedure

1. Log in to PBX web 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.

Apply a new template to a provisioned gateway

Prerequisites

Create a custom Auto Provisioning template.

Procedure

1. Log in to PBX web 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

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

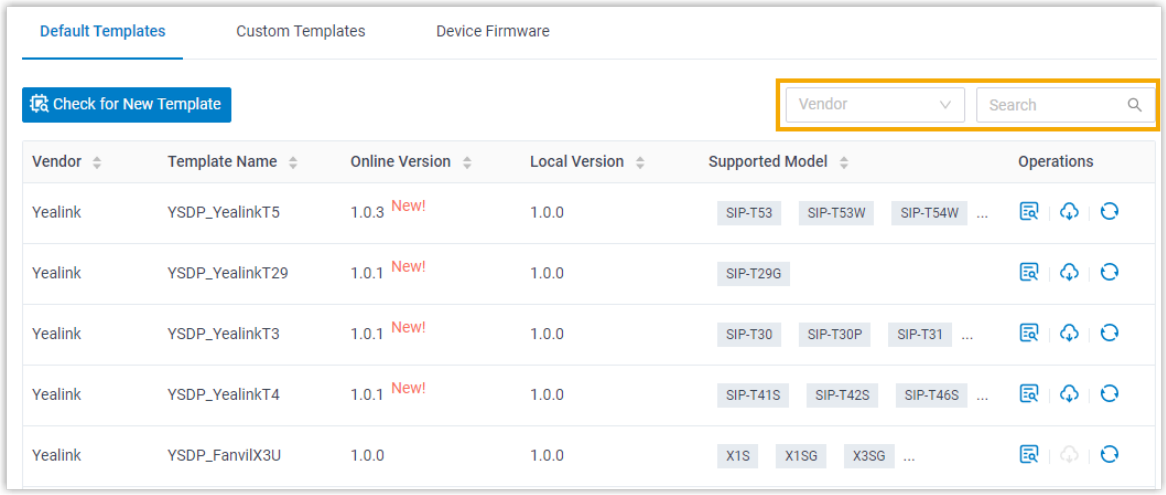
- **Absolute value**: Absolute is a fixed value that applies to all devices that use this template. For example, `features.dtmf.hide_delay = 1` means setting the parameter value to 1 (Enabled).

Procedure

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

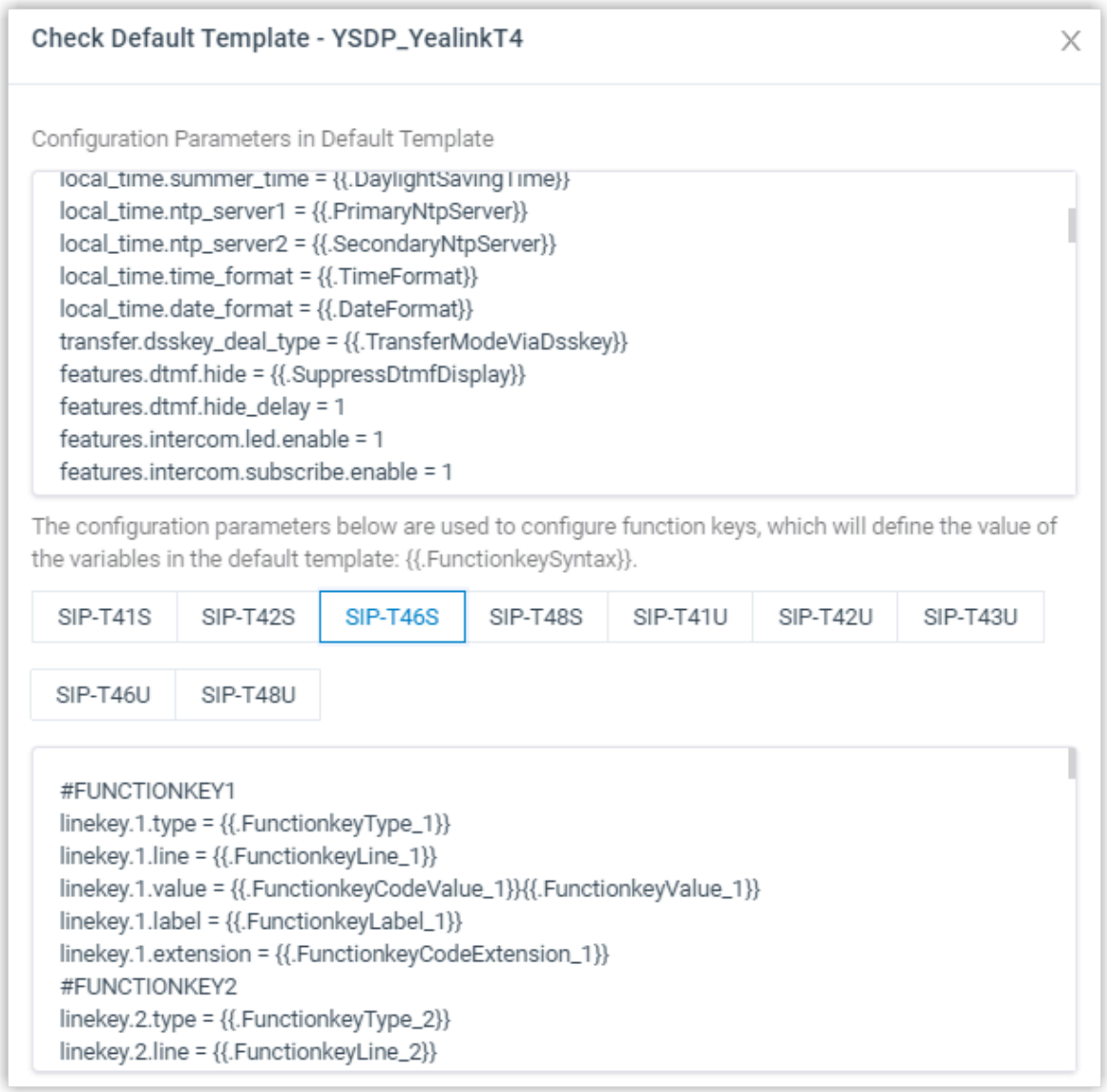
   You can search the template by vendor, provisioning template name, or device model.

   The search results are displayed automatically on the web page.



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.



Related information

[Create a Custom Auto Provisioning Template]
[Manage Custom Auto Provisioning Templates]

Update a Default Auto Provisioning Template

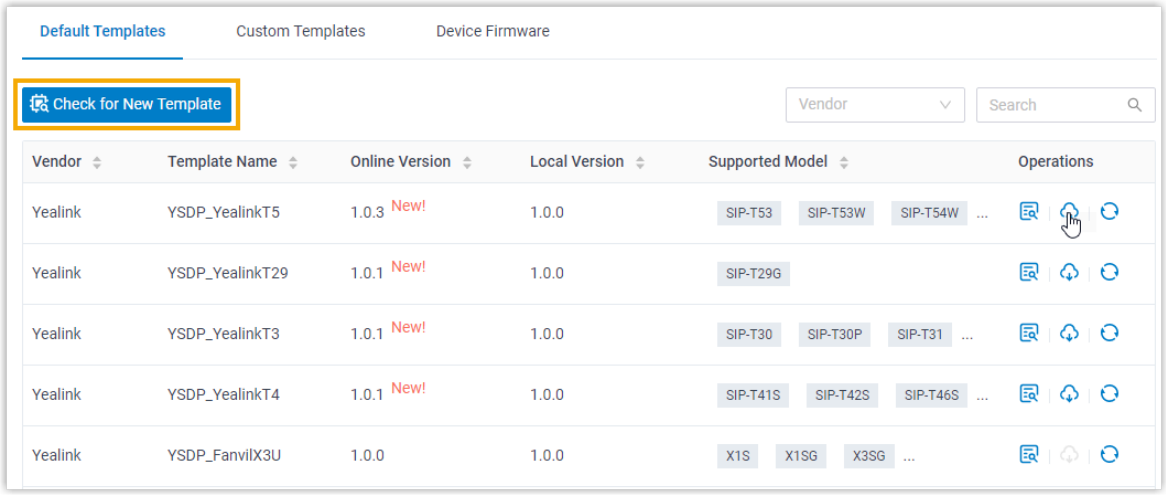
Yeastar P-Series PBX System regularly provides new template versions to release new features and fix bugs. You can check if a new template is available, and decide whether to update the default template. This topic describes how to update a default template.

Prerequisites

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

Procedure

1. Log in to PBX web 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.



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 web 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**, **Codecs** and **LDAP Directory** 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 **Distinctive Ringtone** section, modify the settings according to your needs.
6. In the **Codecs** section, select a desired codec according to your needs.
7. In the **LDAP Directory** section, modify the settings according to your needs.
8. In the **VLAN** section, configure the VLAN settings according to your needs.
9. 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 web 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**, **Codecs** and **LDAP Directory** 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 **Distinctive Ringtone** section, modify the settings according to your needs.
6. In the **Codecs** section, select a desired codec according to your needs.
7. In the **LDAP Directory** section, modify the settings according to your needs.
8. In the **VLAN** section, configure the VLAN settings according to your needs.
9. 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 web portal.

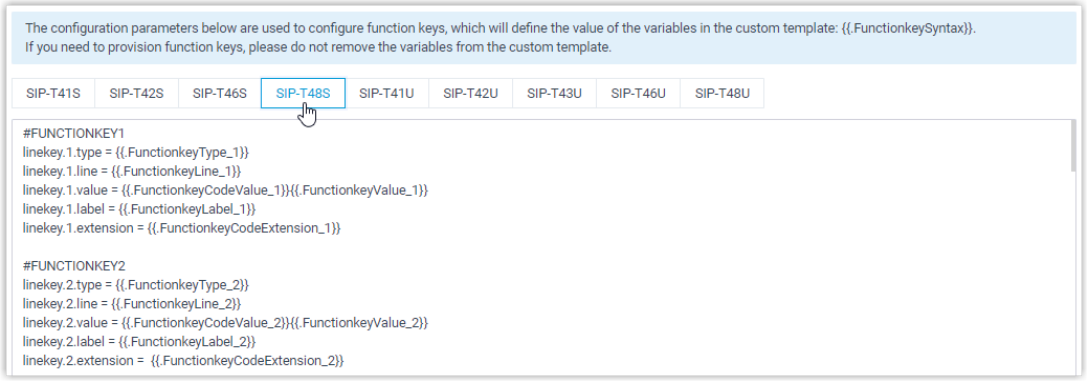
   a. In the **Customize Configuration Parameters In Text** section, add your configuration parameters in the first text box.

      > **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.



10. Click **Save**.

Related information

Edit a custom Auto Provisioning template
Update Auto Provisioning template(s) to all applicable devices

Manage Custom Auto Provisioning Templates

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

Edit a custom Auto Provisioning template

1. Log in to PBX web 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 web 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 web 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.

Download or upload custom Auto Provisioning templates

Yeastar P-Series PBX System support downloading and uploading of auto provisioning custom templates, which allows template reuse across multiple PBXs without the need to recreate templates manually.

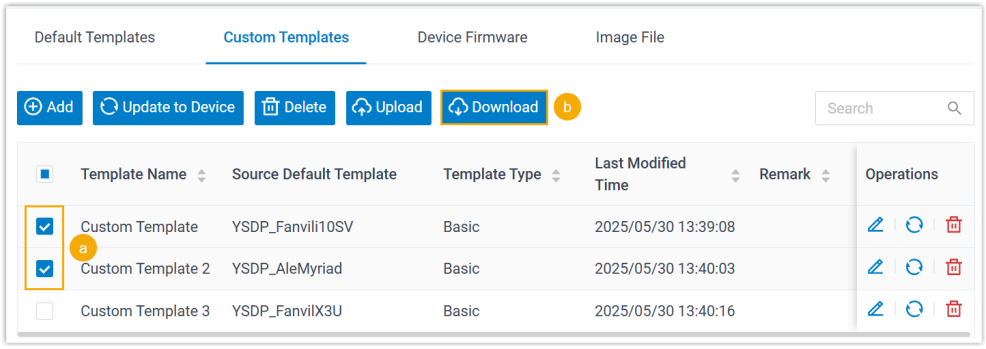
> **Important:**
> The downloaded template files are encrypted and cannot be opened directly; they can only be uploaded and parsed by the PBX.

Requirements

The firmware of Yeastar P-Series PBX System is 37.19.0.70 or later.

Procedure

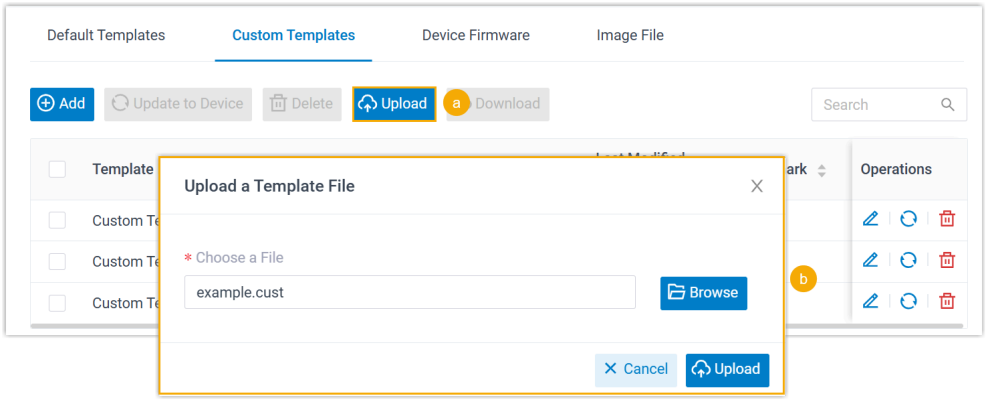
1. Log in to PBX web portal, go to **Auto Provisioning > Resource Repository > Custom Templates**.
2. To download custom auto provisioning templates, do as follows:



   a. Select one or more desired templates.
   b. At the top of the list, click **Download**.

      The template files are downloaded to your computer in `.cust` format.

3. To upload a custom auto provisioning template, do as follows:



   a. At the top of the list, click **Upload**.
   b. In the pop-up window, click **Browse** to select the downloaded `.cust` template file, then click **Upload**.

      The template is uploaded and displayed in the list.

Manage IP Phone Firmware

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 web 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 web 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.

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

Note:
You can upload up to **3** device firmware files to PBX server.

1. Log in to PBX web 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 web 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 web 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

Note:

- For more information about the auto provisioning configuration, see Auto Provision Yealink IP Phone with Yeastar P-Series PBX System.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Yealink IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
AX83H	180.86.0.5 or later	37.16.0.25 or later	• PnP • DHCP • RPS • Provision Link
AX86R	180.86.0.5 or later	37.18.0.59 or later	• PnP • DHCP • RPS • Provision Link
CP920	78.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
CP925	148.86.0.5 or later	37.5.0.9 or later	• PnP • DHCP • RPS • Provision Link
CP960	73.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
CP965	143.86.0.5 or later	37.5.0.9 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
SIP-CP935W	149.86.0.5 or later	37.5.0.9 or later	• PnP • DHCP • RPS • Provision Link
SIP-T19P_E2	53.84.0.125 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T20P	9.73.0.50 or later	37.18.0.102 or later	• PnP • DHCP • RPS • Provision Link
SIP-T21_E2	52.84.0.125 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T21P_E2	52.84.0.125 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T22P	7.73.0.50 or later	37.18.0.102 or later	• PnP • DHCP • RPS • Provision Link
SIP-T23G	44.84.0.125 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T23P	44.84.0.125 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T26P	6.73.0.50 or later	37.18.0.102 or later	• PnP • DHCP • RPS • Provision Link
SIP-T27G	69.85.0.5 or later	37.2.0.7 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
SIP-T28P	2.73.0.50 or later	37.18.0.102 or later	• PnP • DHCP • RPS • Provision Link
SIP-T29G	46.83.0.120 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T30	124.85.0.15 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T30P	124.85.0.15 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T31	124.85.0.15 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T31G	124.85.0.15 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T31P	124.85.0.15 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T31W	124.86.0.75 or later	37.11.0.56 or later	• PnP • DHCP • RPS • Provision Link
SIP-T32G	32.70.0.125 or later	37.18.0.102 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
SIP-T33G	124.85.0.15 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T33P	124.85.0.15 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T34W	124.86.0.75 or later	37.12.0.23 or later	• PnP • DHCP • RPS • Provision Link
SIP-T38G	38.70.0.185 or later	37.18.0.102 or later	• PnP • DHCP • RPS • Provision Link
SIP-T40G	76.84.0.125 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T40P	54.84.0.125 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T41P	36.83.0.120 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T41S	66.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T41U	108.85.0.39 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T42G	29.83.0.120 or later	37.2.0.7 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
SIP-T42S	66.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T42U	108.85.0.39 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T43U	108.85.0.39 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T44U	108.86.0.90 or later	37.10.0.32 or later	• PnP • DHCP • RPS • Provision Link
SIP-T44W	108.86.0.90 or later	37.10.0.32 or later	• PnP • DHCP • RPS • Provision Link
SIP-T46G	28.83.0.120 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T46S	66.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T46U	108.85.0.39 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T48G	35.83.0.120 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T48S	66.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
SIP-T48U	108.85.0.39 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T52S	70.84.0.70 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T53	96.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T53W	96.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T54S	70.84.0.70 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T54W	96.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T56A	58.83.0.15 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T57W	96.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T58	58.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
SIP-T58W	150.86.0.5 or later	37.2.0.7 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
SIP-T73W	185.87.0.15 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T73U	185.87.0.15 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T74W	185.87.0.15 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T74U	185.87.0.15 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T77U	185.87.0.15 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T85W	185.87.0.15 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T87W	185.87.0.15 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T88W	192.87.0.5 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T88V	192.87.0.5 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
T64LTE	132.86.0.25 or later	37.16.0.71 or later	• PnP • DHCP • RPS • Provision Link
T67LTE	132.86.0.35 or later	37.16.0.71 or later	• PnP • DHCP • RPS • Provision Link
VP59	91.85.0.5 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
W60B (W53P, W41P, W60P, CP930W-Base)	77.83.0.85 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
W70B (W79P, W76P, W73P)	146.85.0.20 or later	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
W75DM	175.85.0.5 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
W80B	W80DM-103.83.0.80	37.2.0.7 or later	• PnP • DHCP • RPS • Provision Link
W90DM	130.85.0.15 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link

Fanvil phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Fanvil IP Phone with Yeastar P-Series PBX System.

- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Fanvil IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
A10	2.12.4 or later	37.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
A10W	2.12.4 or later	37.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
A308i	2.6.10.1177 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
A32	2.6.0.408 or later	37.5.0.9 or later	• PnP • DHCP • RPS • Provision Link
A32i	2.6.0.408 or later	37.5.0.9 or later	• PnP • DHCP • RPS • Provision Link
A320	2.6.0.1402 or later	37.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
A320i	2.6.0.1402 or later	37.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
FH-S01	2.12.8 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
H1	2.12.1 or later	37.10.0.32 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
H2U	2.4.7 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
H2U-V2	2.4.7.6 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
H3	2.12.1.7334 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
H3W	2.4.4 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
H4	1.0.8 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
H4W	1.0.8 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
H5	2.12.1.7334 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
H5W	2.4.4 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
H6	1.0.8 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
H6W	1.0.8 or later	37.14.0.26 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
H603W	2.14.0.11 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
i10	1.2.7 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i10D	1.2.7 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i10S	2.4.4 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i10SD	2.4.4 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i10SV	2.4.4 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i10V	1.2.7 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i11S	1.2.7 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i11SV	2.4.4 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
i12	2.8.2.7009 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i16S	2.4.4 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i16SV	2.4.4 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i16V	2.8.2.7009 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i18S	2.8.2.7009 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i20S	2.8.2.7009 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i23S	2.8.2.7009 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i30	2.8.2.7009 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i31S	2.8.2.7009 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i32V	2.8.2.7009 or later	37.3.0.42 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
i33V	2.8.2.7009 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i33VF	2.8.2.7009 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i504	2.12.43.13 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i505	2.6.6.391 or later	37.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
i506W	2.12.43.13 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i507W	2.6.6.394 or later	37.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
i51	2.8.13 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i51W	2.8.13 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i52	2.8.13 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i52W	2.8.13 or later	37.3.0.42 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
i53	2.8.13 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i53W	2.8.13 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i55A	1.0.0.45 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
i56A	0.3.0.21 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
i57A	1.0.0.46 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
i61	2.4.0 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i62	2.4.0 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i63	2.4.0 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i64	2.4.0 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i68	2.8.40.22 or later	37.8.0.25 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
PA2	2.8.2.7009 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
PA2S	2.8.11 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
PA3	2.4.4 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
V50P	2.12.20.4 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V60P	2.12.20.3 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V60W	2.12.20.3 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V61G	2.12.18.8 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V61W	2.12.18.8 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V62	2.4.10 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
V62G	2.12.18.8 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V62W	2.12.18.8 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V62 Pro	2.12.18.2 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V63	2.12.16.19 or later	37.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
V64	2.4.10 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
V65	2.12.2.4 or later	37.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
V66	2.12.18.4 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V66 Pro	2.12.18.4 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V67	2.6.0 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
W610W	2.12.0 or later	37.11.0.22 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
W611W	pvt-2.8 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
W710D	1.16.2 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
W710H	1.0.14.5 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
X1S / X1SP	2.2.12 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X1SG	2.2.12 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X2/X2P	2.14.0.7386 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X2C/X2CP	2.14.0.7386 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X210	2.2.11 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X210-V2	2.12.1.3 or later	37.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
X210i	2.2.11 or later	37.2.0.80 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
X210i-V2	2.12.1.3 or later	37.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
X3SG	2.2.12 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X3S/X3SP/X3G	2.14.0.7386 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X3S Lite / X3SP Lite	2.4.5 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X3S Pro / X3SP Pro	2.4.5 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X3SW	2.4.5 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X3SG Lite	2.4.5 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X3SG Pro	2.4.5 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X3U	2.2.12 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X3U Pro	2.4.5 or later	37.2.0.80 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
X301	2.12.2 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X301G	2.12.2 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X301W	2.12.2 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X303	2.12.2 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X303G	2.12.2 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X303W	2.12.2 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X303-2 WIRE	1.0.3 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
X305	2.12.1.6 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X4/X4G	2.14.0.7386 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
X4U	2.2.11 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X4U-V2	2.12.1 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
X5U	2.2.11 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X5U-V2	2.12.1 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
X5S	2.2.1 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X6	2.2.1 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X6U	2.2.11 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X6U-V2	2.12.1 or later	37.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
X7	2.2.11 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X7A	2.2.0.229 or later	37.2.0.80 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
X7C	2.2.11 or later	37.2.0.80 or later	• PnP • DHCP • RPS • Provision Link
X7-V2	2.12.1.3 or later	37.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
X7C-V2	2.12.1.3 or later	37.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
Y501	2.12.4 or later	37.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
Y501W	2.12.4 or later	37.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
Y501-Y	2.12.4 or later	37.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
Y501W-Y	2.12.4 or later	37.11.0.22 or later	• PnP • DHCP • RPS • Provision Link

Grandstream phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Grandstream IP Phone with Yeastar P-Series PBX System.

- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Grandstream IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
GXP1610	1.0.7.13 or later	37.3.0.42 or later	• PnP • DHCP • Provision Link
GXP1620	1.0.7.13 or later	37.3.0.42 or later	• PnP • DHCP • Provision Link
GXP1625	1.0.7.13 or later	37.3.0.42 or later	• PnP • DHCP • Provision Link
GXP1628	1.0.7.13 or later	37.3.0.42 or later	• PnP • DHCP • Provision Link
GXP1630	1.0.7.13 or later	37.3.0.42 or later	• PnP • DHCP • Provision Link
GXP2130	1.0.11.16 or later	37.3.0.42 or later	• PnP • DHCP • Provision Link
GXP2135	1.0.11.16 or later	37.3.0.42 or later	• PnP • DHCP • Provision Link
GXP2140	1.0.11.16 or later	37.3.0.42 or later	• PnP • DHCP • Provision Link
GXP2160	1.0.11.16 or later	37.3.0.42 or later	• PnP • DHCP • Provision Link
GXP2170	1.0.11.16 or later	37.3.0.42 or later	• PnP • DHCP • Provision Link
GAC2500	1.0.3.45 or later	37.11.0.22 or later	• PnP • DHCP • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
GAC2570	1.0.1.36 or later	37.11.0.22 or later	• PnP • DHCP • Provision Link
GRP2601	1.0.3.63 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2601P	1.0.3.63 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2602	1.0.3.63 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2602P	1.0.3.63 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2602G	1.0.3.63 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2602W	1.0.3.63 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2603	1.0.3.63 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2603P	1.0.3.63 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2604	1.0.3.63 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2604P	1.0.3.63 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2612	1.0.7.25 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2612P	1.0.7.25 or later	37.7.0.51 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
GRP2612G	1.0.7.25 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2612W	1.0.7.25 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2613	1.0.7.25 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2614	1.0.7.25 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2615	1.0.7.25 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2616	1.0.7.25 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2624	1.0.7.25 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2634	1.0.7.25 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2670	1.0.7.25 or later	37.7.0.51 or later	• PnP • DHCP • Provision Link
GHP610	1.0.1.71 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
GHP610W	1.0.1.71 or later	37.17.0.17 or later	• PnP • DHCP • Provision Link
GHP611	1.0.1.71 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
GHP611W	1.0.1.71 or later	37.17.0.17 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • Provision Link
GHP620	1.0.1.71 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
GHP620W	1.0.1.71 or later	37.17.0.17 or later	• PnP • DHCP • Provision Link
GHP621	1.0.1.71 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
GHP621W	1.0.1.71 or later	37.17.0.17 or later	• PnP • DHCP • Provision Link
GHP630	1.0.1.71 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
GHP630W	1.0.1.71 or later	37.17.0.17 or later	• PnP • DHCP • Provision Link
GHP631	1.0.1.40 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
GHP631W	1.0.1.71 or later	37.17.0.17 or later	• PnP • DHCP • Provision Link
WP825	1.0.11.67 or later	37.17.0.17 or later	• PnP • DHCP • Provision Link

Htek phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Htek IP Phone with Yeastar P-Series PBX System.

- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Htek IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
UC803T	2.0.4.4.33 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC902	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC902S	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC903	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC912	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC912G	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC912E	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC921	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC921G	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
UC923	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC923U	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC924	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC924E	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC924U	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC924W	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC926	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC926E	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC926U	2.0.4.8.18 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UCV10	5.42.1.6.30b58 or later	37.12.0.23 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
UCV20	5.42.1.6.30b79 or later	37.12.0.23 or later	• PnP • DHCP • RPS • Provision Link
UCV50	5.42.1.6.30b62 or later	37.12.0.23 or later	• PnP • DHCP • RPS • Provision Link
UCV52	5.42.1.6.30b68 or later	37.12.0.23 or later	• PnP • DHCP • RPS • Provision Link
UCV53	5.42.1.6.32R76 or later	37.12.0.23 or later	• PnP • DHCP • RPS • Provision Link

Gigaset phones

Note:
For more information about the auto provisioning configuration, see Auto Provision Gigaset DECT System with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
N870 IP PRO	2.38.1 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
N870 VI PRO	2.38.1 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
N670 IP PRO	2.38.1 or later	37.3.0.42 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
N610 IP PRO	2.52.0 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
Maxwell Basic PRO	3.18.1 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
Maxwell 2 PRO	3.18.1 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
Maxwell 3 PRO	3.18.1 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
Maxwell 4 PRO	3.18.1 or later	37.3.0.42 or later	• PnP • DHCP • RPS • Provision Link
P820 IP PRO	10.1.198.16 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
P850W IP PRO	10.1.198.16 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
P710 IP PRO	10.1.198.16 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
P810 IP PRO	10.1.198.16 or later	37.19.0.70 or later	• PnP • DHCP • RPS • Provision Link

Snom phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Snom IP Phone with Yeastar P-Series PBX System.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Snom IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
D120	10.1.54.13 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D140	10.1.148.1 or later	37.12.0.33 or later	• PnP • DHCP • RPS • Provision Link
D150	10.1.148.1 or later	37.12.0.33 or later	• PnP • DHCP • RPS • Provision Link
D315	10.1.73.16 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D335	10.1.73.16 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D385	10.1.73.16 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D710	8.9.3.80 or later	37.19.0.22 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
D712	8.9.3.61 or later	37.19.0.22 or later	• PnP • DHCP • RPS • Provision Link
D713	10.1.73.16 or later	37.6.0.46 or later	• PnP • DHCP • RPS • Provision Link
D715	10.1.33.33 or later	37.19.0.22 or later	• PnP • DHCP • RPS • Provision Link
D717	10.1.73.16 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D720	8.9.3.80 or later	37.19.0.22 or later	• PnP • DHCP • RPS • Provision Link
D725	10.1.175.16 or later	37.19.0.22 or later	• PnP • DHCP • RPS • Provision Link
D735	10.1.73.16 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D785	10.1.73.16 or later	37.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D812	10.1.184.14 or later	37.12.0.30 or later	• PnP • DHCP • RPS • Provision Link
D815	10.1.184.14 or later	37.12.0.30 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
D862	10.1.137.15 or later	37.9.0.22 or later	• PnP • DHCP • RPS • Provision Link
D865	10.1.137.15 or later	37.9.0.22 or later	• PnP • DHCP • RPS • Provision Link
HD100	1.0.0.3-0 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
HD101	1.0.0.3-0 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
HD300 (HD30L)	1.0.0.7 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
HD350W	1.0.0.3-0 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
HD351W	1.0.0.3-0 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
HM201	1.0.0.3-0 or later	37.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
M100 KLE	1.0.5.7 or later	37.14.0.24 or later	• PnP • DHCP • RPS • Provision Link
M500	1.12.2 or later	37.14.0.24 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
M300	BSV530B2 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
M400	BSV610B5 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
M900	BSV530B7 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
SP800	10.1.169.15 or later	37.17.0.60 or later	• PnP • DHCP • RPS • Provision Link
PA1+	10.1.184.15 or later	37.17.0.60 or later	• PnP • DHCP • RPS • Provision Link

Flyingvoice phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Flyingvoice IP Phone with Yeastar P-Series PBX System.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Flyingvoice IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
FIP10	0.7.23.1 or later	37.8.0.25 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
FIP11C	0.7.23.1 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP12WP	0.7.23.1 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP13G	0.7.23.1 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP14G	0.7.23.1 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP15G	0.7.23.1 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP15G Plus	0.7.23.1 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP16	0.7.23.1 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP16 Plus	0.7.23.1 or later	37.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
P10	V0.7.56 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
P10P	V0.7.56 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P10G	V0.7.56 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P10W	V0.7.56 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P10LTE	V0.7.56 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P11	V0.7.56 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P11P	V0.7.56 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P11G	V0.7.56 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P11W	V0.7.56 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P11LTE	V0.7.56 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P20	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
P20P	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P20W	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P20G	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P21	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P21P	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P21W	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
flyphone	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P22P	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P22G	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P23G	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
P23GW	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P24G	V0.7.57 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
i86Box_Basic	V0.0.16.1 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
i86Box_Indoor	V0.0.16.1 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
i86Box_2Line	V0.0.16.1 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
i86Box_PCBA	V0.0.16.1 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
i86Box_NFC	V0.0.16.1 or later	37.9.0.20 or later	• PnP • DHCP • RPS • Provision Link

Alcatel-Lucent Enterprise phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Alcatel-Lucent Enterprise (ALE) IP Phone with Yeastar P-Series PBX System.

- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Alcatel-Lucent Enterprise (ALE) IP Phone with Yeastar P-Series PBX System.

Table 15.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
H2	2.10.00.0001083 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link
H2P	2.10.00.0001083 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link
H3P	2.12.43.010.2272 or later	37.5.0.9 or later	• PnP • DHCP • Provision Link
H3G	2.12.43.010.2272 or later	37.5.0.9 or later	• PnP • DHCP • Provision Link
H6	2.12.43.010.2272 or later	37.5.0.9 or later	• PnP • DHCP • Provision Link
M3	2.13.37.000.2202 or later	37.5.0.9 or later	• PnP • DHCP • Provision Link
M3s	2.15.10.000.3000 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
M5	2.13.37.000.2202 or later	37.5.0.9 or later	• PnP • DHCP • Provision Link
M5s	2.15.10.000.3000 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
M7	2.13.37.000.2202 or later	37.5.0.9 or later	• PnP • DHCP • Provision Link

Table 15. (continued)

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
M7s	2.15.10.000.3000 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
M7s-Pro	2.15.10.000.3000 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
M8	2.13.32.000.1535 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link

Tiptel phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Tiptel IP Phone with Yeastar P-Series PBX System.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Tiptel IP Phone with Yeastar P-Series PBX System.

Table 16.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
3310	2.42.6.5.55 or later	37.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
3320	2.42.6.5.55 or later	37.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
3330	2.42.6.5.55 or later	37.7.0.16 or later	• PnP • DHCP • RPS • Provision Link

Table 16. (continued)

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
3340	2.42.6.5.55 or later	37.7.0.16 or later	• PnP • DHCP • RPS • Provision Link

Dinstar phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Dinstar IP Phone with Yeastar P-Series PBX System.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Dinstar IP Phone with Yeastar P-Series PBX System.

Table 17.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
C60S	2.60.11.7.0 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link
C60L	2.60.11.7.0 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link
C60U	2.60.11.7.0 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link
C61S	2.61.6.7.0/2.61.11.7.0 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link
C62S	2.62.6.7.0/2.62.11.7.0 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link
C62G	2.62.6.7.0/2.62.11.7.0 or later	37.6.0.24 or later	• PnP • DHCP

Table 17. (continued)

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
C63S	2.63.11.7.0 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link
C63G	2.63.6.7.0/2.63.11.7.0 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link
C64G	2.64.6.7.0 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link
C66G	2.66.6.7.0 or later	37.6.0.24 or later	• PnP • DHCP • Provision Link

VTech phones

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
NG-S3211W	3.3.3.16-0 or later	37.13.0.29 or later	• PnP • DHCP • Provision Link
NG-S3311	3.3.3.16-0 or later	37.13.0.29 or later	• PnP • DHCP • Provision Link
NG-S3411W	3.3.3.16-0 or later	37.13.0.29 or later	• PnP • DHCP • Provision Link
S2211-SPK	3.3.3.16-0 or later	37.13.0.29 or later	• PnP • DHCP • Provision Link
S2210-X	3.3.3.16-0 or later	37.13.0.29 or later	• PnP • DHCP • Provision Link
S2411-X	3.3.3.16-0 or later	37.13.0.29 or later	• PnP • DHCP • Provision Link

Mitel phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Mitel IP Phone with Yeastar P-Series PBX System.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Mitel IP Phone with Yeastar P-Series PBX System.

Table 18.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
6863i	R5.1.0SP6 or later	37.9.0.103 or later	• DHCP • Provision Link
6865i	R5.1.0SP6 or later	37.9.0.103 or later	• DHCP • Provision Link
6867i	R5.1.0SP6 or later	37.9.0.103 or later	• DHCP • Provision Link
6869i	R5.1.0SP6 or later	37.9.0.103 or later	• DHCP • Provision Link
6873i	R5.1.0SP6 or later	37.9.0.103 or later	• DHCP • Provision Link
6905	6.3 SP3 or later	37.17.0.17 or later	• DHCP • Provision Link
6910	6.3 SP3 or later	37.17.0.17 or later	• DHCP • Provision Link
6915	6.3 SP3 or later	37.17.0.17 or later	• DHCP • Provision Link
6920	6.3.1 SP1 or later	37.9.0.103 or later	• DHCP • Provision Link
6930	6.3.1 SP1 or later	37.9.0.103 or later	• DHCP • Provision Link
6940	6.3.1 SP1 or later	37.9.0.103 or later	• DHCP • Provision Link
RFP 44	9.1 or later	37.18.0.18 or later	• DHCP

Table 18. (continued)

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
RFP 45	9.1 or later	37.18.0.18 or later	• DHCP • Provision Link
RFP 47	9.1 or later	37.18.0.18 or later	• DHCP • Provision Link
RFP 48	9.1 or later	37.18.0.18 or later	• DHCP • Provision Link

Cisco phones

Note:
For more information about the auto provisioning configuration, see Auto Provision Cisco IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
3905	9.4(1)SR3 or later	37.12.0.23 or later	• DHCP
7821	14.2(1)SR1 or later	37.12.0.23 or later	• DHCP
7861	SIP78xx.14-2-1-0201-40 or later	37.13.0.29 or later	• DHCP
7911	SIP11.9-2-1S or later	37.17.0.17 or later	• DHCP
7942	SIP42.9-4-2SR3-1S or later	37.12.0.23 or later	• DHCP
7975	SIP75.9-3-1SR4-1S or later	37.17.0.17 or later	• DHCP
8811	SIP88xx.12-1-1SR1-4 or later	37.13.0.29 or later	• DHCP
8845	14.2(1)SR1 or later	37.12.0.23 or later	• DHCP
SPA501G	7.4.7 or later	37.19.0.22 or later	• DHCP
SPA502G	7.4.7 or later	37.19.0.22 or later	• DHCP
SPA504G	7.4.7 or later	37.19.0.22 or later	• DHCP
SPA508G	7.4.7 or later	37.19.0.22 or later	• DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
SPA509G	7.4.7 or later	37.19.0.22 or later	• DHCP
SPA512G	7.4.7 or later	37.19.0.22 or later	• DHCP
SPA514G	7.4.7 or later	37.19.0.22 or later	• DHCP
SPA301	7.4.7 or later	37.19.0.22 or later	• DHCP
SPA303	7.4.7 or later	37.19.0.22 or later	• DHCP
SPA525G2	7.4.7 or later	37.19.0.22 or later	• DHCP

Avaya phones

Note:
For more information about the auto provisioning configuration, see Auto Provision Avaya IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
J129	4.1.1.0.7 or later	37.12.0.23 or later	• DHCP • Provision Link
J139	4.1.1.0.7 or later	37.12.0.23 or later	• DHCP • Provision Link
J159	4.1.1.0.7 or later	37.12.0.23 or later	• DHCP • Provision Link
J169	4.1.1.0.7 or later	37.12.0.23 or later	• DHCP • Provision Link
J179	4.1.1.0.7 or later	37.12.0.23 or later	• DHCP • Provision Link
J189	4.1.1.0.7 or later	37.12.0.23 or later	• DHCP • Provision Link
9608	7.1.15.2.1 or later	37.14.0.26 or later	• DHCP • Provision Link

Poly phones

Note:

For more information about the auto provisioning configuration, see Auto Provision Poly IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
Edge_E100	8.0.0.15602 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E220	8.0.0.15602 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E300	8.0.0.15602 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E320	8.0.0.15602 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E350	8.0.0.15602 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E400	8.0.0.15602 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E450	8.0.0.15602 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E500	8.0.0.15602 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E550	8.0.0.15602 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_101	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_201	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_301	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
VVX_310	5.9.8 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_311	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_401	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_410	5.9.8 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_411	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_501	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_601	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_150	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_250	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_350	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_450	6.4.3.5059 or later	37.15.0.22 or later	• DHCP • RPS • Provision Link

Wildix phones



Note:

For more information about the auto provisioning configuration, see Auto Provision Wildix IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
WP410R2	50.145.6.169 or later	37.15.0.22 or later	• DHCP • Provision Link
WP480R2	55.145.6.111 or later	37.15.0.22 or later	• DHCP • Provision Link
WP480R3	63.145.10.168 or later	37.15.0.22 or later	• DHCP • Provision Link
WP480R4	65.145.6.38 or later	37.15.0.22 or later	• DHCP • Provision Link
WP490R2	59.145.6.148 or later	37.15.0.22 or later	• DHCP • Provision Link
WP490R3	67.145.8.107 or later	37.15.0.22 or later	• DHCP • Provision Link

Xenios phones

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
ICD012	23.12.20 or later	37.14.0.24 or later	• DHCP • Provision Link

Huawei phones

Note:
For more information about the auto provisioning configuration, see Auto Provision Huawei IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
eSpace 7910	V200R003C30SPCf00 or later	37.16.0.25 or later	• DHCP • Provision Link
eSpace 7950	V200R003C00SPCs00 or later	37.16.0.25 or later	• DHCP • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
IP Phone 7920	V600R019C10SPC200 or later	37.16.0.25 or later	• DHCP • Provision Link
IP Phone 7960	V600R019C10SPC202 or later	37.16.0.25 or later	• DHCP • Provision Link
eSpace 8950	V200R003C00SPCg00B015 or later	37.16.0.25 or later	• DHCP • Provision Link
eSpace 8950HK	V200R003C30SPCh20 or later	37.17.0.17 or later	• DHCP • Provision Link

NEC phones

Note:

- By default, DT700 series models are not displayed in the drop-down list. In case of need, contact Yeastar Support.
- For more information about the auto provisioning configuration, see Auto Provision NEC IP Phone with Yeastar P-Series PBX System.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
DT700 ITL-2E-1P	03.01.64.00 or later	37.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-6DE-1P	03.01.64.00 or later	37.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-12D-1P	03.01.64.00 or later	37.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-24D-1P	03.01.64.00 or later	37.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-8LD-1P	03.01.64.00 or later	37.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-8LDE-1P	03.01.64.00 or later	37.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-12DG-3P	03.01.64.00 or later	37.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-12CG-3P	03.01.64.00 or later	37.17.0.53 or later	• DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
DT820 ITY-6D-1P	04.04.28.14 or later	37.17.0.53 or later	• DHCP • Provision Link
DT820 ITY-8LDX-1P	04.04.28.14 or later	37.17.0.53 or later	• DHCP • Provision Link
DT820 ITY-8LCGX-1P	04.04.28.14 or later	37.17.0.53 or later	• DHCP • Provision Link
DT820 ITY-6DG-1P	04.04.28.14 or later	37.17.0.53 or later	• DHCP • Provision Link
DT820 ITY-32LDG-1P	04.04.28.14 or later	37.17.0.53 or later	• DHCP • Provision Link
DT820 ITY-32LCG-1P	04.04.28.14 or later	37.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-6D-1P	05.03.04.99 or later	37.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-12D-1P	05.03.04.03 or later	37.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-8LCX-1P	05.03.04.99 or later	37.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-8TCGX-1P	05.03.04.99 or later	37.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-6DG-1P	05.03.04.99 or later	37.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-12DG-1P	05.03.04.99 or later	37.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-32LCG-1P	05.03.04.99 or later	37.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-32TCG-1P	05.03.04.99 or later	37.17.0.53 or later	• DHCP • Provision Link
DT900S ITK-6DGS-1P	05.03.04.99 or later	37.17.0.53 or later	• DHCP • Provision Link
DT900S ITK-32LCGS-1P	05.03.04.99 or later	37.17.0.53 or later	• DHCP • Provision Link
DT900S ITK-32TCGS-1P	05.03.04.99 or later	37.17.0.53 or later	• DHCP • Provision Link

Yeastar gateways

Note:
For more information about the auto provisioning configuration, see Auto Provision Yeastar TA FXS Gateways (PnP Method), Auto Provision Yeastar TA FXS Gateways (DHCP Method), Auto Provision Yeastar TA FXS Gateway (Provision Link Method), and Auto Provision Yeastar TA FXS Gateway (Provision Link FQDN Method).

Model	Gateway Requirement	PBX Requirement	Supported Auto Provisioning Method
TA100	44.19.86.30 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
TA200	44.19.86.30 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
TA400	41.19.0.32 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
TA800	41.19.0.32 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
TA1600	47.0.0.54 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
TA2400	47.0.0.54 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link
TA3200	47.0.0.54 or later	37.18.0.18 or later	• PnP • DHCP • Provision Link

Auto Provisioning - Variables in Templates

The provisioning 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 admin account to log in to the phone web interface.
{{.PhonePassword}}	The password for admin account to log in to the phone web interface.
{{.VarPassword}}	The password for var account to log in to the phone web interface.
{{.UserPassword}}	The password for user account to log in to the phone web interface.
{{.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.
{{.AutoProvisionServerProtocolUppercase}}	The uppercase representation of the transport protocol in the auto provisioning URL.
{{.AutoProvisionServerProtocolLowercase}}	The lowercase representation of the transport protocol in the auto provisioning URL.
{{.ProvisioningFile}}	The name of configuration file.
{{.FirmwareUrl}}	The URL of firmware.

Variable	Description
{{.FirmwareUrlWithoutProtocol}}	The URL of firmware without transport protocol.
{{.FirmwareFile}}	The name of firmware.
{{.FirmwareFullDownloadUrl}}	The full download URL 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.
{{.WallpaperImageServerUrl}}	The URL of the wallpaper image for the phone.
{{.WallpaperFileName}}	The file name of the wallpaper image for the phone.
{{.ScreenSaverImageServerUrl}}	The URL of the ScreenSaver image for the phone.
{{.ScreensaverFileName}}	The file name of the ScreenSaver image for the phone.
{{.BootLogoImageServerUrl}}	The URL of the boot logo image for the phone.
{{.BootLogoFileName}}	The file name of the boot logo image for the phone.
VLAN settings for phones	
{{.WanVlanEnable}}	Enable or disable VLAN for the WAN port of the phone.
{{.WanVlanId}}	The VLAN ID for the WAN port of the phone.
{{.WanVlanPriority}}	The VLAN priority for the WAN port of the phone.
{{.PcVlanEnable}}	Enable or disable VLAN for the PC port of the phone.
{{.PcVlanId}}	The VLAN ID for the PC port of the phone.
{{.PcVlanPriority}}	The VLAN priority for the PC port of the phone.
{{.DhcpVlanEnable}}	Enable or disable acquiring the VLAN ID through DHCP option.
{{.DhcpVlanOption}}	The DHCP option(s) from which the phone will obtain the VLAN ID. **Note:** Use a comma to separate multiple DHCP options.
Contact settings for Yealink / Flyingvoice / Wildix/ Dinstar 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.
{{.AccountSipServerTransportType}}	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.
{{.SRTP_x}}	Enable or disable extension SRTP feature.
{{.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.
{{.AccountSipServerTransportType_x}}	The type of transport protocol for extension registration.
{{.HandsetIPUI_X}}	The IPUI number 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)	
{{.TemplateNamex}}	The template name.
{{.TemplateServerAddrx}}	The URL of PBX server for extension registration.
{{.TemplateServerPortx}}	The port of PBX server for extension registration.

Variable	Description
{{.AcountSipServerTemplate}}	The type of transport protocol for extension registration.
{{.HandsetIPUI_X}}	The IPUI number 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.
{{.AccountCodecIlbc}}	Enable or disable iLBC audio codec.
{{.AccountCodecIlbc_Priority}}	The priority of the iLBC audio codec.
{{.AccountCodecIlbc_15_2_Kbps}}	Enable or disable iLBC_15_2 audio codec.
{{.AccountCodecIlbc_15_2_Kbps_Priority}}	The priority of the iLBC_15_2 audio codec.
{{.AccountCodecIlbc_13_33_Kbps}}	Enable or disable iLBC_13_33 audio codec.
{{.AccountCodecIlbc_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.
{{.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.

Variable	Description
{{.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.
{{.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.
LDAP Directory (x is the template ID, X=1, 2 or 3)	
{{.EnableLdap_X}}	Enable LDAP directory.
{{.LdapName_X}}	Specify the name of LDAP directory.
{{.LdapMode_X}}	Set up the LDAP mode.
{{.LdapHost_X}}	The address of LDAP Server.

Variable	Description
{{.LdapNameFilter_X}}	The LDAP name filter.
{{.LdapNumFilter_X}}	The LDAP number filter.
{{.LdapNameAttr_X}}	The name attribute returned by LDAP Server.
{{.LdapNumAttr_X}}	The number attribute returned by LDAP Server.
{{.LdapDisplayName_X}}	The name of the search results displayed on IP phones.
{{.LdapMaxHit_X}}	The maximum number of search results to be returned by LDAP Server.
{{.LdapIncomingLookup_X}}	Enable or disable IP phone to perform an LDAP search when receiving an incoming call.
{{.LdapDialLookup_X}}	Enable or disable IP phone to perform an LDAP search when placing a call.
{{.LdapSort_X}}	Enable or disable IP phone to sort out search results in alphabetical and numerical order.
{{.LdapPort_X}}	The port of LDAP Server.
{{.LdapBase_X}}	The base entry of the LDAP directory.
{{.LdapUser_X}}	The user accessing the LDAP Server.
{{.LdapPassword_X}}	The password for accessing to the LDAP Server.
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.

Variable	Description
Others	
{{.MacAddress}}	The MAC address of phone. **Note:** Here the value does not need a separator of :. For example, `09139876900e`.

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' web 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' web 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:

Role	Permission
Super administrator	Access and manage all the PBX features. **Note:** The username of super administrator is created when you first configure the system, and the username is unchangeable.
Administrator	Access and manage all the PBX features except the followings: • 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.

Role	Permission
Human Resource	View and manage all the extensions.
Accounting	Access and manage **Plan**.
Hotel Manager	Access and manage the following features: • **Hotel Settings** • **Room Management** • **Wake-up Service**

Related information

Create a User Role
Assign a Role to a User

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.

Restrictions

Note:
Only system super administrator can 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 web portal, go to **Extension and Trunk > Role**.
2. Click **Add** to create a new role.
3. In the **Role Name** field, enter a name to help you identify it.
4. Grant permissions to the user role.

   For permission details, see User Role Permissions.
5. 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 web 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.

Restrictions

> **Note:**
> Only system super administrator can assign a role to a user.

Prerequisites

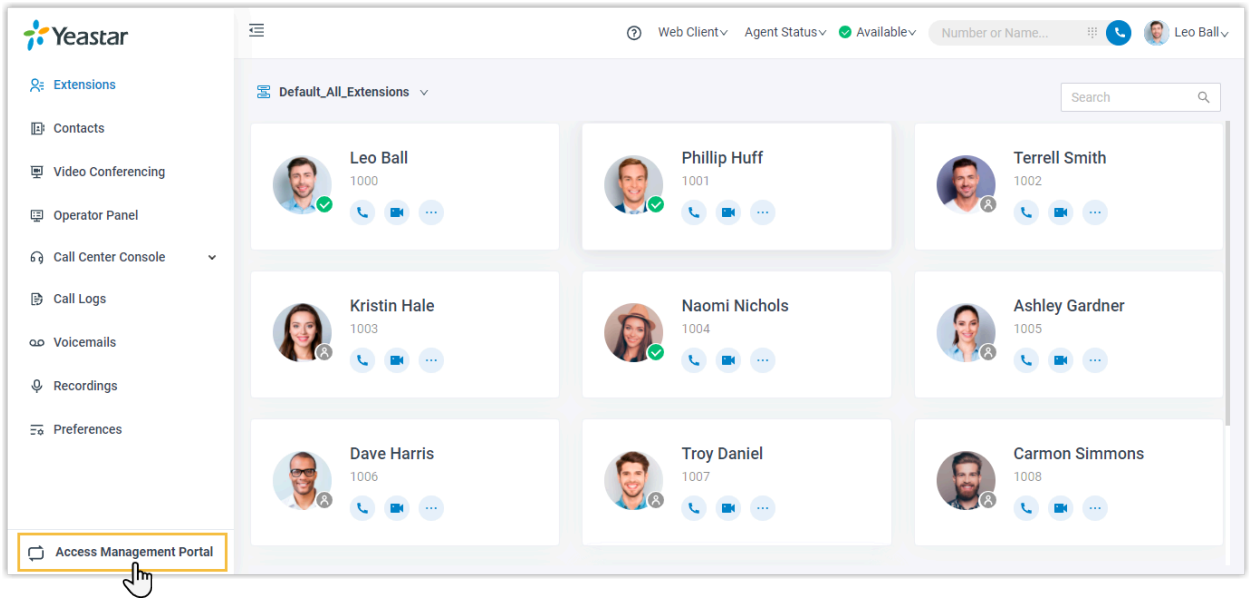
A user role is created.

Procedure

1. Log in to PBX web 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.

Restrictions

Note:
Only system super administrator can manage user roles.

Edit a role

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

1. Log in to PBX web 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 web 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
- Messaging
- PBX Settings
- Hotel Management
- 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.

Module	Permission	
Extension	**Manage Extensions**	• **All Departments**: View and manage all the departments.
		• **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. • **All other extensions of the same department**: Manage or send Linkus welcome emails to all the other extensions in the same department, excluding those in the associated sub-departments. • **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.
	Manage Extension Operation Permission	Specify whether users with the role assigned can view and manage Linkus Client related settings of extensions. • **Linkus Clients**: Set whether users can view the **Linkus Clients** feature tab. ◦ **Linkus Mobile Client**: Set whether users can view and manage settings for Linkus Mobile Client.

Module	Permission	
		◦ **Linkus Pad Client (SDK)**: Set whether users can view and manage Linkus SDK. **Note:** This option is available only when Linkus SDK (Path: **Integration > Linkus SDK**) is enabled. ◦ **Linkus Desktop Client**: Set whether users can view and manage settings for Linkus Desktop Client. ◦ **Linkus Web Client**: Set whether users can view and manage settings for Linkus Web Client.
Extension Group	Manage extension groups.	
Client Permission	Manage users' permissions to view or manage specific extensions/contacts.	
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.

- **LDAP Server**

Call Control

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

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

- **Allow to edit Emergency Outbound Caller ID in Management Portal > Extension**: Specify whether users with the role assigned can configure emergency outbound caller ID for extensions (Path: **Management Portal > Extension and Trunk > Extension > User > Outbound Caller ID (DOD) > Emergency Outbound Caller ID**), which changes the number displayed to the called party when the extension users make an emergency call.

> **Note:**
> To specify whether the extension users can edit the emergency outbound caller ID on their own Linkus clients, go to **Management Portal > Client Permissions > Preference Settings**.

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**
- **Call Disposition**
- **Blocked/Allowed Numbers**

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 and external chat logs.

Module	Permission
CDR	Specify users with the role assigned can view which extensions' CDR. • **All Extensions**: View all extensions' CDR.

Module	Permission	
	• **All the other extensions of the same Extension Groups**: View CDR of all the other extensions of the same group except the one that contains all the extensions. • **All other extensions of the same department**: View CDR of all the other extensions in the same department, excluding those in the associated sub-departments. • **Specific Extensions**: View CDR of specific extensions.	
	Specify how users with the role assigned can manage CDR. • **Download** • **Delete** • **Schedule Download**	
Recording Files	Specify users with the role assigned can view which extensions' recordings. • **All Extensions**: View all extensions' recordings. • **All the other extensions of the same Extension Groups**: View recordings of all the other extensions of the same group except the one that contains all the extensions. • **All other extensions of the same department**: View recordings of all the other extensions in the same department, excluding those in the associated sub-departments. • **Specific Extensions**: View recordings of specific extensions	
	Specify how users with the role assigned can manage recording files. • **Play** • **Download** • **Delete**	
Call Reports	**Call Report Operation Permission**	Specify how users with the role assigned can manage call reports. • **Download** • **Schedule Download** • **Rate**
	Call Report Data Permission	Specify users with the role assigned can view which call reports and the data scope. • **Queue Call Reports** • **Extension Call Reports** • **Other Call Reports**

Module	Permission
External Chat Logs	Specify whether users with the role assigned can access external chat logs.

Auto Provisioning

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

Messaging

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

- **Message Channel**
- **Message Queue**

PBX Settings

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

- **Preferences**
- **Voice Prompt**
- **SIP Settings**
- **Jitter Buffer**

Hotel Management

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

- **Hotel Settings**
- **Room Management**
- **Wake-up Service**

System

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

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

- **Remote Management**
- **SNMP**
- **Hot Standby**

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:

- **Collaboration**
- **CRM**
- **Helpdesk**
- **PMS**
- **Speech to Text**
- **AMI**
- **API**
- **Database Grant**
- **Linkus SDK**

Plan

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

Operator Panel

Manage Operator Panel

This topic describes instructions on setting up Operator Panel for extension user.

What is Operator Panel

Yeastar provides an embedded Operator Panel on Linkus Web Client and Desktop Client for call management. 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)	√	√	√

Permission	Extension Group Manager	Extension Group User	Custom role of Extension Group
Call parking operations (Park, Retrieve)	√	√	√
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 Trunk	No additional telephony module is required.
	SIP Peer Trunk	
	SIP Account Trunk	
WebRTC Trunk	WebRTC Trunk	No additional telephony module is required.
Analog Trunk	FXO	SO 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.

Status	Description
	Unreachable.
	Registration failed. • 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.

Status	Description
	Unavailable: PIN/PUK error.
	Unavailable: Cellular network registration failed. **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: • Malfunction in interface/module. Check the relevant interface/module. • No trunk plugged in. • Service provider doesn't activate the trunk.
	Failure. It may caused by the following problems on Data Link layer: • Incorrect protocol layer configuration. • Service provider doesn't activate the trunk.
	Available.

BRI Trunk status

Status	Description
	Failure. It may caused by the following problems on Physical layer: • Malfunction in interface/module. Check the relevant interface/module. • No trunk plugged in. • Service provider doesn't activate the trunk.

Status	Description
	Failure. It may caused by the following problems on Data Link layer: • 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 Account Trunk

Related information

WebRTC Trunk Overview

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 web 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 **DIDs/DDIs** tab to configure the DID numbers for the trunk.
   a. Click **Add**, then add DID number(s) according to your need.
      - To add a single DID number, do as follows:
        i. In the **Create Method** drop-down list, select **Single DID**.
        ii. 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.

          When the DID number is dialed, the name will be displayed on the called party's device.
      - To add a range of DID numbers, do as follows:
        i. In the **Create Method** drop-down list, select **DID Range**.
        ii. Configure the following settings:

- **DID Range**: Enter the start number and the end number of the DID range.
- **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

  When the DID number is dialed, the name will be displayed on the called party's device.

b. Click **Confirm**.

> **Note:**
> 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 web 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 *05JsOmsIS54SYh*.

- **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 **DIDs/DDIs** tab to configure the DID numbers for the trunk.
   a. Click **Add**, then add DID number(s) according to your need.
      - To add a single DID number, do as follows:
        i. In the **Create Method** drop-down list, select **Single DID**.
        ii. 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.

          When the DID number is dialed, the name will be displayed on the called party's device.
      - To add a range of DID numbers, do as follows:
        i. In the **Create Method** drop-down list, select **DID Range**.
        ii. Configure the following settings:
        - **DID Range**: Enter the start number and the end number of the DID range.
        - **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

          When the DID number is dialed, the name will be displayed on the called party's device.
   b. Click **Confirm**.

> **Note:**

> 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 web 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 **DIDs/DDIs** tab to configure the DID numbers for the trunk.
   a. Click **Add**, then add DID number(s) according to your need.
      - To add a single DID number, do as follows:
        i. In the **Create Method** drop-down list, select **Single DID**.
        ii. 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.

          When the DID number is dialed, the name will be displayed on the called party's device.
      - To add a range of DID numbers, do as follows:
        i. In the **Create Method** drop-down list, select **DID Range**.

ii. Configure the following settings:
- **DID Range**: Enter the start number and the end number of the DID range.
- **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

  When the DID number is dialed, the name will be displayed on the called party's device.

b. Click **Confirm**.

> **Note:**
> 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 web 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, configure the following settings:

> **Note:**
> You can leave the default SIP information or edit the information according to your needs.

Setting	Description
Trunk Type	Select **Account Trunk**.
Transport	Select a transport. The following options are supported: • **UDP** • **TCP** **Note:** By default, SIP TCP port is disabled. If you select this option, go to **PBX Settings > SIP Settings > General > Basic**, enable **SIP TCP Port**, then reboot the PBX to make it take effect. • **TLS**
Username	Enter a username for the SIP account.
Password	Enter a password for the SIP account.
Authentication Name	Retain the default authentication name or enter a custom one. **Note:** If the device to be connected does NOT support the **Authentication Name** field, select **Use User Name as Account Trunk's Authentication Name**.

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, External host domain name, or FQDN domain name of PBX

      Note:
      - If the account trunk uses public IP address or external host domain name, you need to configure the network and port forwarding first.

        For more information, see Configure Network for Remote Access by a Public IP Address or Configure Network for Remote Access by a Domain Name.
      - If the account trunk uses FQDN, make sure this account trunk can perform remote SIP registration via FQDN.

        For more information, see Configure Network for Remote SIP Access by a Yeastar FQDN.
    - 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 web 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 web 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 web 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 web 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.

Related information

Import and Export -FAQ

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.

Setting	Description
Select ITSP Template	Select the country of your ITSP. **Note:** If no SIP trunk template is provided for your ITSP, select **General**.
ITSP	Select your ITSP from the list of certified SIP trunk providers.

Detailed Configuration

Setting	Description
Trunk Type	Select a trunk type: • **Register Trunk** • **Peer Trunk** • **Account Trunk**
Register Trunk	
Transport	Select the transport that is provided by the ITSP. **Note:** If you select **TCP**, make sure SIP TCP Port is enabled (Path: **PBX Settings > SIP Settings > General > Basic > SIP TCP Port**.
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**.
Username	Enter the username to register to the ITSP.
Password	Enter the password that is associated with the username.
Authentication Name	Enter the authentication name to register to the ITSP.

Setting	Description
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. **Note:** If you select **TCP**, make sure SIP TCP Port is enabled (Path: **PBX Settings > SIP Settings > General > Basic > SIP TCP Port**.
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	
Transport	Select the transport for a third-party device to register with. **Note:** If you select **TCP**, make sure SIP TCP Port is enabled (Path: **PBX Settings > SIP Settings > General > Basic > SIP TCP Port**.
Username	Specify a username for the trunk. **Note:** The username is regarded as the trunk number.

Setting	Description
Password	Specify a password that is associated with the username.
Authentication Name	Specify an authentication name for a third-party device to register with.

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
- Opus

VoIP Setting

Setting	Description
DTMF Mode	Set the default mode for sending DTMF tones. • **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	Enable or disable T.38 fax for this trunk. Enabling T.38 will add the performance cost. We suggest that you disable T.38.
Inband Progress	This Inband Progress setting applies to the extensions which make calls through this trunk. **Note:** To configure global Inband Progress setting, you need to contact Yeastar support to configure a custom config file. • **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.

Setting	Description
Ignore 183 Message without SDP	This option determines the way PBX handles 183 messages without SDP. • **Check this option**: PBX will not forward 183 messages that don't contain SDP. • **Uncheck this option**: PBX will process all the 183 messages without SDP to those with SDP and forward them.
Forward the 180 (SDP) Message Following the Peer's Format	This option determines whether the PBX will forward a 180 message with SDP, depending on whether the 180 message received from the other party contains SDP. • **Check this option**: PBX will forward a 180 message if the 180 message received from the other party includes SDP. **Note:** This setting does not take effect when Inband Progress is enabled. • **Uncheck this option**: PBX will not forward a 180 message with SDP even if the 180 message received from the other party contains SDP.
Enable RTP Keep-alive	Whether to send an RTP Comfort Noise (CN) frame. This helps to keep the NAT and firewall holes open during a call, so as to ensure the transmission of RTP traffic. **Note:** • This option is only available for register trunk and peer trunk. • When this option is enabled, if the PBX does not send an RTP packet to the trunk within 1 second, an RTP Comfort Noise (CN) frame will be sent.

Call Restriction

Setting	Description
Call Restriction Type	Specify based on which type of calls to restrict the max concurrent call number of this trunk.

Setting	Description
	• **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 for Outbound Calls

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

Parameter	Description
Get Caller ID From	Decide from which header field will the trunk retrieve Caller ID. • **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	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. Adjust the setting after analysis of the SIP packets sent from the trunk provider. The following SIP headers are available to select: • **Follow System** The trunk will follow the global Get DID From setting. • **To** • **Invite** • **Diversion** • **Remote-Party-ID**

Parameter	Description
	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-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:

Parameter	Description
From User Part	Define the caller ID that will be used of a SIP From header. For more information, see Options of outbound parameters.
From Display Name Part	Define the caller ID name that will be used of a SIP From header. For more information, see Options of outbound parameters.
From Host Part	**Important:** • This parameter is only available for **Peer Trunks**. • Set the parameter according to the requirements of your SIP trunk provider, otherwise, it may cause call issues. Define the domain or IP address to be used in the **From** field of a SIP INVITE header. • **Default**: Use the domain or IP address configured in the **Domain** field when creating the Peer Trunk. • **Custom**: Use a custom domain or IP address. You can enter the custom value in the field next to the **Custom** drop-down list.
To Host Part	**Important:**

Parameter	Description
	• This parameter is only available for **Peer Trunks**. • Set the parameter according to the requirements of your SIP trunk provider, otherwise, it may cause call issues. Define the domain or IP address to be used in the **To** field of a SIP INVITE header. • **Default**: Use the domain or IP address configured in the **Domain** field when creating the Peer Trunk. • **Custom**: Use a custom domain or IP address. You can enter the custom value in the field next to the **Custom** drop-down list.
Diversion Remote-Party-ID P-Asserted-Identity P-Preferred-Identity	**Optional:** Define other parameters of a SIP INVITE header as needed. For more information, see Options of outbound parameters.
P-Asserted-Identity URI Format	**Note:** This parameter is available only when **P-Asserted-Identity** is not set to None. To assert and verify the identity of the caller, specify the format of P-Asserted-Identity: • SIP URI (sip:) • TEL URI (tel:)

Note:
For different types of SIP trunk, the optional items are different.

Table 19. Options of outbound parameters

Option	Description
[Default]	• For the **Diversion** outbound parameter, the system uses the original call destination number (DID number) as the parameter value when the call diversion occurs.

Table 19. Options of outbound parameters (continued)

Option	Description
	• For the **Remote-Party-ID**, **P-Asserted-Identity** and **P-Preferred-Identity** outbound parameter, the system selects a parameter by the following priority from top to bottom: ◦ Outbound Route Outbound Caller ID ◦ Extension's Outbound Caller ID in Trunk ◦ Trunk Outbound Caller ID ◦ Trunk Username ◦ Extension Caller ID ◦ The Originator Caller ID
[None]	Do not send the parameter with the SIP INVITE packet.
Extension Caller ID	The caller ID configured on the extension.
Trunk Outbound Caller ID	The global outbound caller ID for the trunk (**Trunk > Outbound Caller ID > General**).
Extension's Outbound Caller ID in Trunk	The extension's associated outbound caller ID with the trunk. • If the extension selects a DOD to call out, the selected DOD number will be taken. • If the extension uses the default DOD to call out, the DOD number associated with the extension will be taken. When multiple DOD numbers are associated, the one with the highest priority in the extension's DOD list will be taken (**Extension and Trunk > Extension > User > Outbound Caller ID (DOD) > Outbound Caller IDs**).
Outbound Route Outbound Caller ID	The outbound caller ID configured on the outbound route that is used for the outbound calls.
Originator Caller ID	The Caller ID of the call originator (the first caller in the case that the call is transferred). • 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].
Trunk Username	The username configured on the trunk.
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	Realm is a string displayed to users so they know which username and password to use. **Note:** If you don't know what to fill in, contact your service provider for further instructions.
100rel	Configure 100rel for this trunk. • **Required**: 100rel is required for this trunk. • **Supported**: 100rel is supported by this trunk. • **Disabled**: 100rel is disabled for this trunk.
Maxptime	Select the value of the maxptime used when the PBX sends the INVITE packet. **Note:** If you select **[Default]**, PBX will send a corresponding maxptime value according to the codec that is used for the outbound call.
Select which IP address to use in 'Contact'(SIP) and 'Connection'(SDP) fields	**Note:** This option is only available for register trunk and peer trunk. Select the option to decide which IP address will be used in 'Contact'(SIP) and 'Connection'(SDP) fields. • **Use Default Settings**: Use the IP address that the system provides by default. • **Use Custom IP Address**: Use the custom IP address specified in the **IP Address** field. **Note:** The custom IP address will be used in 'Contact'(SIP) and 'Connection'(SDP) fields instead of the public IP address configured in **Public IP and Ports** (Path: **System > Network**).

Setting	Description
Send Privacy ID	Whether to send the Privacy ID in SIP header or not. The default is unchecked.
User Phone	Whether to add the parameter `user=phone` as a request line in the header field of the SIP INVITE packet. **Note:** Enable this option only when the SIP provider requires.
Send X-OpenAPI-Call-ID	Set whether to include a `X-OpenAPI-Call-ID` field in the SIP INVITE packet to carry the Call ID for inbound calls and outbound calls routed through the trunk.
Support P-Early-Media	Set whether the P-Early-Media field is included in the INVITE packet.
Send 183 Message with P-Early-Media Header	Set whether the PBX will include the `P-Early-Media` header with the value of `sendrecv` in the 183 message for inbound calls routed through the trunk.

WebRTC Trunk

WebRTC Trunk Overview

Yeastar P-Series PBX System supports WebRTC trunk. Unlike traditional SIP trunks, WebRTC trunk uses WebRTC (Web Real-Time Communication) technology to implement real-time audio and video communication on web page. With a simple click on a call link provided by WebRTC trunk, your customers can make free calls directly from their browser to your company's phone system without the need for additional plug-ins or software. In addition, the audio call can be seamlessly switched to a video call for face-to-face communication, improving the customer service experience.

Requirements and restrictions

Requirements

- **Network**: PBX can be remotely accessed via a domain name.
  For more information about the domain configuration, see the following topics:
  - Configure Network for Remote Access by a Yeastar FQDN

    - Configure Network for Remote Access by a Yeastar Domain Name
    - Configure Network for Remote Access by a Domain Name
  - **Plan**: If you need video calls, **Ultimate Plan** is required.
  - **Firmware**: The version of Yeastar P-Series PBX System is 37.19.0.70 or later.

Restrictions

- You can create up to **5** WebRTC trunks.
- A WebRTC trunk supports up to **10** concurrent calls.

Supported web browsers

The following table shows the compatible web browsers.

Web browser	Version
Google Chrome	Chrome 87 or later
Microsoft Edge	Edge 87 or later
Opera	Opera 72 or later

Related information

Set up WebRTC Click-to-Call

Set up WebRTC Click-to-Call

To implement WebRTC click-to-call, you need to create a WebRTC trunk on PBX to obtain a WebRTC call link, then embed the call link into your web page. In this way, your website visitors can make calls to your company's phone system with a click.

Prerequisites

- Make sure that the PBX can be remotely accessed via a domain name.
  For more information about the domain configuration, see the following topics:
  - Configure Network for Remote Access by a Yeastar FQDN
  - Configure Network for Remote Access by a Yeastar Domain Name
  - Configure Network for Remote Access by a Domain Name
- If you need video calls, **Ultimate Plan** is required.
- Make sure the version of Yeastar P-Series PBX System is 37.19.0.70 or later.

Procedure

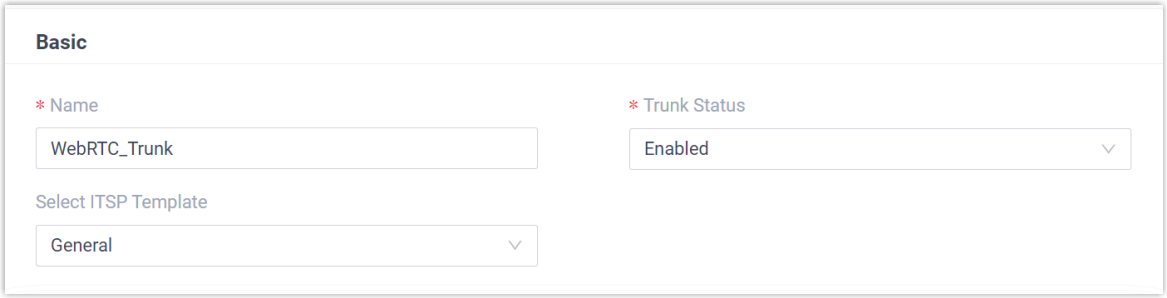
1. Create a WebRTC trunk
2. Set WebRTC inbound call destination
3. Test WebRTC Click-to-Call

Video Tutorial

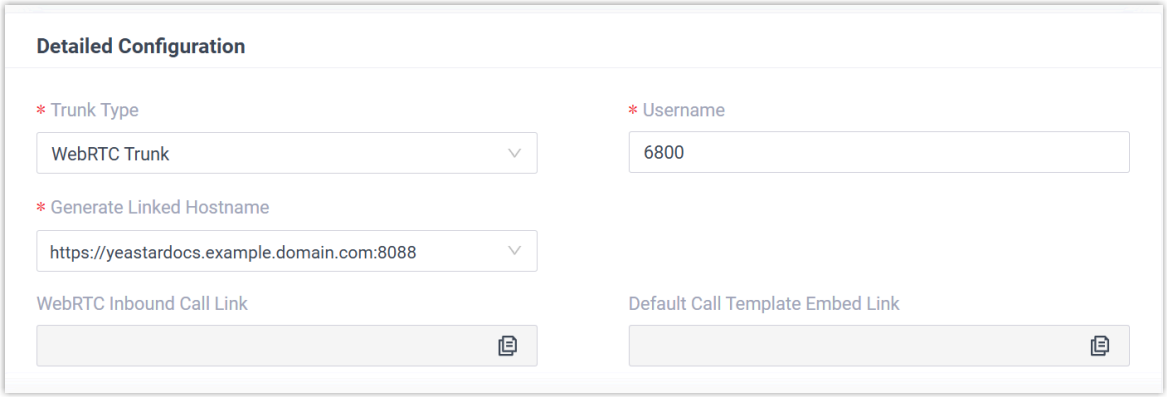
Create a WebRTC trunk

Create a WebRTC trunk to obtain a WebRTC call link.

1. Log in to PBX web portal, go to **Extension and Trunk > Trunk**, then click **Add**.
2. In the **Basic** section, complete 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, complete the following settings.



   - **Trunk Type**: Select **WebRTC Trunk**.
   - **Username**: Enter a username for the trunk.

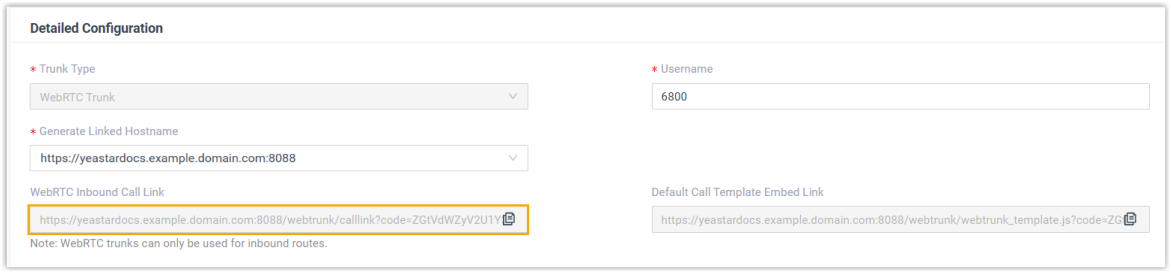
- **Generate Linked Hostname**: Select the hostname for generating the WebRTC Inbound Call Link and the Default Call Template Embed Link.

4. **Optional:** Click the **Advanced** tab to configure advanced WebRTC trunk settings.
   a. In the **Codec Settings** section, configure your preferred codecs.
   b. In the **Call Restriction** section, set the maximum number of concurrent calls for the trunk.

   > **Note:**
   > The default number is **5**, you can set up to **10** concurrent calls.

5. Click **Save** and **Apply**.

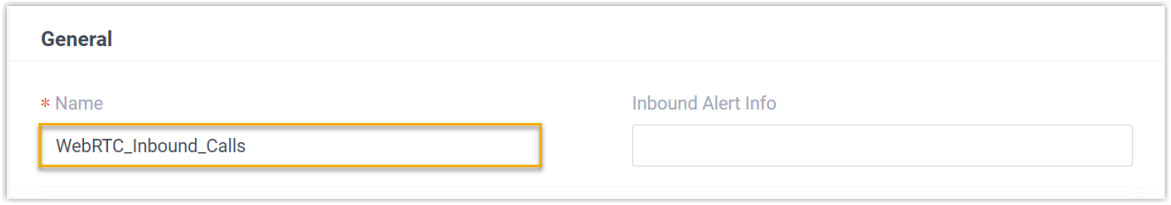
   A WebRTC trunk is displayed in the trunk list with the trunk status showing ; A WebRTC call link is generated and displayed in the **WebRTC Inbound Call Link** field of the trunk.



Set WebRTC inbound call destination

Set up an inbound route for the WebRTC trunk to route the WebRTC inbound calls to a desired destination.

1. Go to **Call Control > Inbound Route**, then click **Add** to add an inbound route.
2. In the **General** section, set a name for the inbound route.

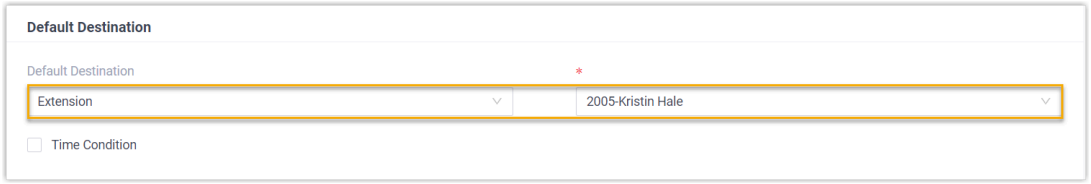


3. In the **Trunk** section, select the WebRTC trunk from **Available** box to **Selected** box.

> **Note:**

> You can NOT select both WebRTC trunk and other types of trunk for an inbound route at the same time.

4. In the **Default Destination** section, set destination(s) for the WebRTC inbound calls.
   - If you want the inbound calls to always be routed to a destination, set the desired destination in the **Default Destination** drop-down list.



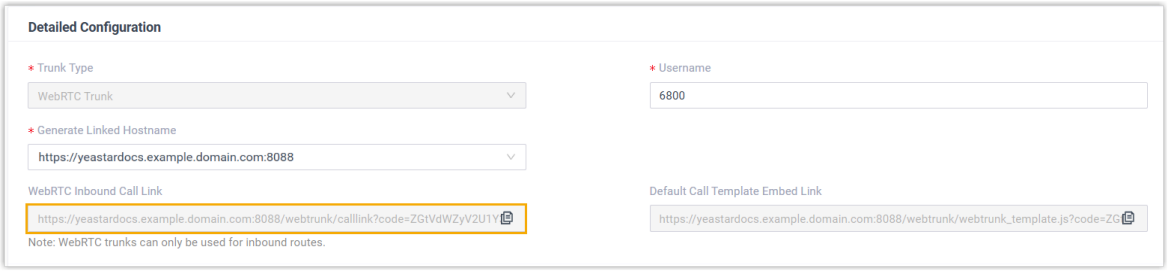
   - If you want the inbound calls to be routed to different destinations based on time, do as follows:
     a. Select the checkbox of **Time Condition**.
     b. In the **Time-based Routing Mode** drop-down list, select a time-based mode.
     c. Configure the corresponding destinations based on time.

     For more information of time-based inbound call routing, see the following topics:
     - Route Inbound Calls based on Business Hours
     - Route Inbound Calls based on Department Hours
     - Route Inbound Calls based on Employee Hours
5. Click **Save** and **Apply**.

Test WebRTC Click-to-Call

Test if the WebRTC inbound call can be routed to the given destination.

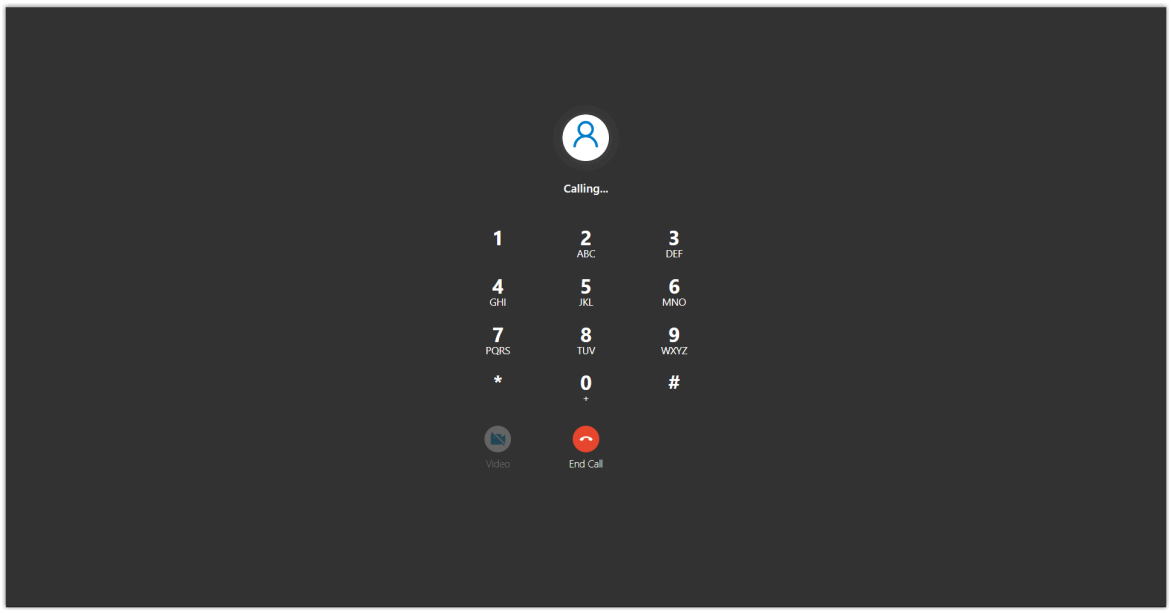
1. Go to **Extension and Trunk > Trunk**, click beside the WebRTC trunk.
2. In the **Detailed Configuration** section, copy the **WebRTC Inbound Call Link**.



3. Open a browser tab, paste the inbound call link in the address bar, then press **Enter**.

A dialpad is displayed on the web page, and a call is placed to the pre-set call destination.

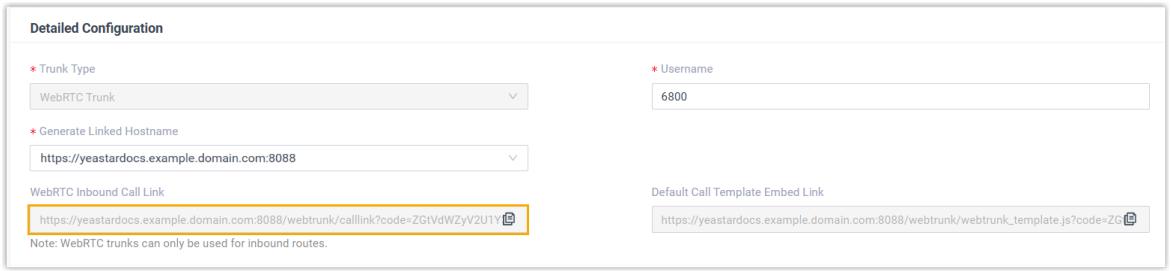
> **Tip:**
>
> During the call, you can switch to a video call by clicking at the bottom-left corner on the web page.



What to do next

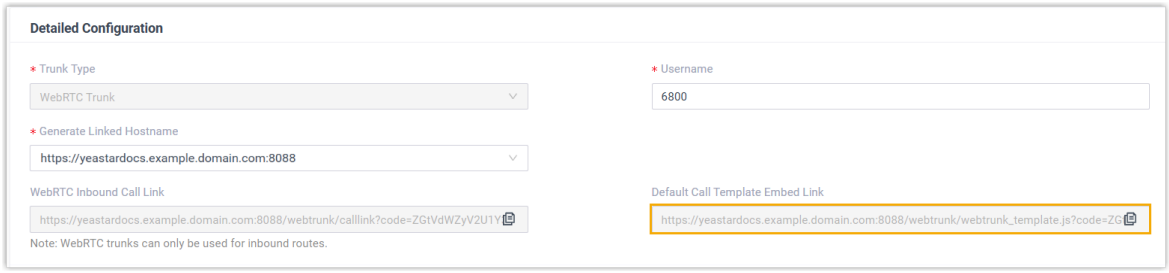
Embed the WebRTC inbound call link into your web page in either of the following ways:

- Customize a call button on your website, and set the button link to the WebRTC call link.

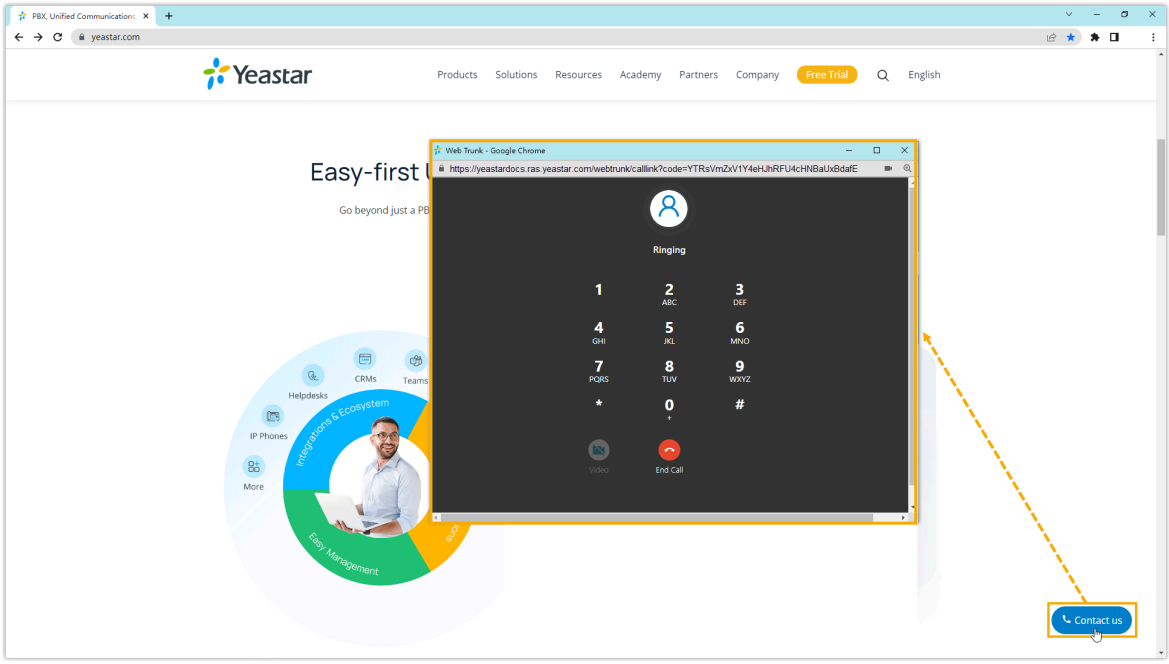


- Utilize the default call button template provided in the WebRTC trunk by referencing the embed link in your website using the following script:

```
<script src="{Default Call Template Embed Link}"></script>
```



The figure below shows the generated call button and the click-to-call effect:



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.

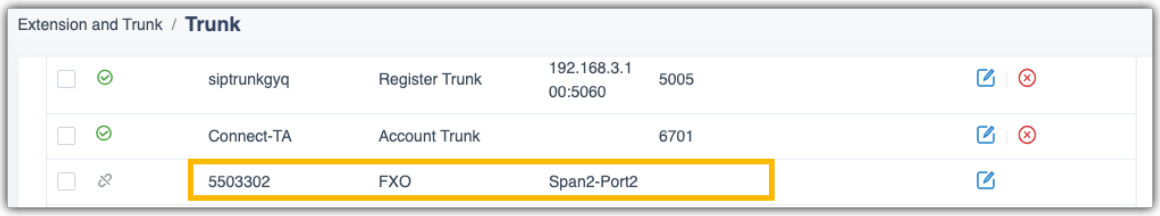
- If the module is successfully installed and detected by the PBX, the FXO port information will be displayed on the PBX web interface.
- If the module is not detected by the PBX, contact Yeastar support to check the problem.

Procedure

1. Find out the FXO port on the PBX.

   Log in to PBX web 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.

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 web 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.
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	Select the Hangup Detection method: • **Busy Tone**: The call will be disconnected if a busy tone is detected by the Yeastar P-Series PBX System.

Setting	Description
	• **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	Specify how many busy tones to wait for before disconnecting. The default value is 4. **Note:** PBX may fail to detect the busy tone if the value of **Busy Count** is too high.
Busy Pattern	Specify the cadence of busy signal. • **Format**: *{sound},{silence}*. For example, `500,500` means 500ms on, 500ms off. **Note:** 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.
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	Specify the method to detect if a call is answered. This setting affects the accuracy of call duration tracking. • **[None]**: PBX will start counting call duration after you use the FXO trunk to call out, whether the call is answered or not.

Setting	Description
	• **Polarity Reversal**: If this option is selected, PBX will start counting call duration after a polarity signal is detected. **Note:** Before you select this option, contact the PSTN provider to check if they supports polarity.

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. • **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. • **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. • Valid value: 1000-10000 • Default value: 5000

Setting	Description
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 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	• EGSM-900 MHz

Module Type	Module Model	Frequency Band
		• PGSM-900 MHz • DCS-1800 MHz • GSM850-850 MHz • PCS-1900 MHz
3G	UC15-A	• WCDMA: 850/1900 MHz • GSM: 850/900/1800/1900 MHz
3G	UC15-E	• WCDMA: 900/2100 MHz • GSM: 900/1800 MHz
3G	UC15-T	• WCDMA: 850/2100 MHz • GSM: 850/900/1800/1900 MHz
4G LTE	EC20-CEFAG	• 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	• 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	• FDD-LTE: B2/B4/B12 • WCDMA: B2/B4/B5
4G LTE	EC25-AU	• 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	• FDD-LTE: B1/B3/B5/B7/B8/B20 • TDD-LTE: B38/B40/B41 • WCDMA: B1/B5/B8 • GSM: B3/B8
4G LTE	EC25-J	• FDD-LTE: B1/B3/B8/B18/B19/B26 • TDD-LTE: B41 • WCDMA: B1/B6/B8/19
4G LTE	EC25-V	• 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.

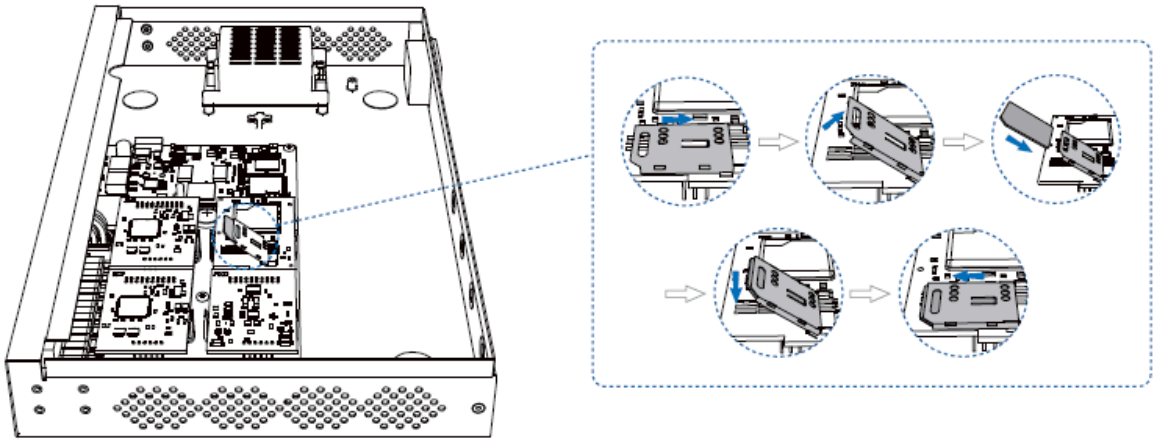
Prerequisites

Install at least one GSM module, 3G module, or 4G LTE module on the PBX.

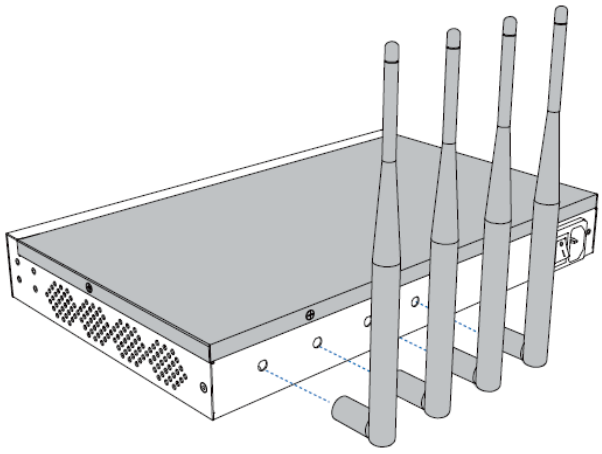
- If the module is successfully installed and detected by the PBX, the trunk will be displayed on the PBX web portal.
- If the module is not detected by the PBX, contact Yeastar support to check the problem.

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 web 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	Enter the SIM card PIN code if the card has one. **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.
RX Volume	Set the receiving volume of GSM/3G/4G LTE port or select **Custom** to define the RX Gain.

General	
Setting	**Description**
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	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 route, enter the destination number in this field.

Carrier Settings	
Setting	**Description**
Carrier	Select the carrier mode. **Note:** When the trunk is in unregistered status, you can try to manually select the correct carrier to fix the issue. • **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.

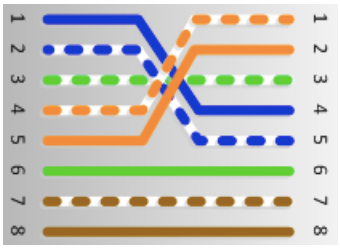
PRI Type	Description
E1	Contains 30 B-channel and one D-channel and is used in Europe, China, and most of the Asian countries.
T1	Contains 23 B-channel and one D-channel and is used in the USA, Canada, and Hong Kong.
J1	It is almost the same as T1 but used in Japan with some slight modifications, this 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 encompasses 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 Date 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 web 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. • 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. • When the **Interface Type** is E1, Framing options are: ◦ Enable CRC4 ◦ Disable CRC4 **Note:**

Setting	Description
Basic Settings	
	CRC4 is a method of checking for errors in data transmitted on E1 trunk lines. • When the **Interface Type** is T1 or J1, Framing options are: ◦ ESF ◦ D4
Line Code	Choose the line code for this trunk according to the direction provided by carrier. • When the **Interface Type** is E1, Line Code options are: ◦ HDB3 ◦ AMI • When the **Interface Type** is T1 or J1, Line Code options are: ◦ B8ZS ◦ AMI
Codec	Choose the codec for this trunk. • **a-law** • **u-law**
Echo Cancellation	This option enables or disables echo cancellation. **Note:** If an echo occurs during a call, you can enable echo cancellation.
D Channel	Set the channel used to carry control information and signaling information. • 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	Configure the switch type according to the direction provided by carrier. • If **Interface Type** is set to **E1**, Switch Type option are: ◦ **EuroISDN** ◦ **Q.SIG** • If **Interface Type** is set to **T1** or **J1**, Switch Type option are: ◦ **EuroISDN** ◦ **National 2** ◦ **National 1**

Setting	Description
Basic Settings	
	◦ **DMS100** ◦ **AT&T 4ess** ◦ **Lucent 5ess** ◦ **Q.SIG**
Signaling Role	Specify whether this interface will act as the user or the network. • **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	Define whether the system can dial this switch using overlap digits or not. If you need Direct Dial-in, then enable this option.
Advanced Settings	
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.
PRI Indication	Select the PRI Indication. • **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. **Note:** Inband notification is not available on all PRI/BRI subscription lines.
Reset Interval (s)	This sets the time in seconds between restart of unused B channels. The default is "Never". **Note:** Set the interval to "Never" if you do not wish the channel to restart.
Carrier Hangup Tone Detection	• 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.

Setting	Description
Basic Settings	
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'
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**.

Setting	Description
Basic Settings	
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. Framing options are: • Enable CRC4 • Disable CRC4 **Note:** CRC4 is a method of checking for errors in data transmitted on E1 trunk lines.
Line Code	Choose the line code for this trunk according to the direction provided by carrier. Line Code options are: • HDB3 • AMI
Echo Cancellation	This option enables or disables echo cancellation. **Note:** If an echo occurs during a call, you can enable echo cancellation.
Variant	Set the MFC/R2 variant. • **Argentina** • **Brazil** • **China** • **Czech** • **Colombia** • **Ecuador** • **Indonesia** • **ITU** • **Mexico** • **Philippines** • **Venezuela**
Category	Set the category of the calling party. • **National** • **National priority**

Setting	Description
Basic Settings	
	• **International** • **International Priority** • **Collect Call**
MAX DNIS	Maximum amount of DNIS to ask for. **Note:** If you wish to customize the size, enter the value in the text box directly.
MAX ANI	Maximum amount of ANI to ask for.
Advanced Settings	
Forced Release	Enable or disable forced release of channel. **Note:** If the call can not be hung up properly, check this option.
Immediate Accept	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.
Double Answer	Block collect calls with double answer. This will cause that every answer signal is changed by answer -> clear back -> answer. The default is unchecked.
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	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. Framing options are: • Enable CRC4 • Disable CRC4 **Note:** CRC4 is a method of checking for errors in data transmitted on E1 trunk lines.
Line Code	Choose the line code for this trunk according to the direction provided by your carrier. Line Code options are: • HDB3 • AMI
Codec	Choose the codec for this trunk.
Echo Cancellation	This option enables or disables echo cancellation. **Note:** If an echo occurs during a call, you can enable echo cancellation.
D Channel	Set the channel used to carry control information and signaling information. Enter a channel number from 1 to 31.
Variant	Set the SS7 variant. • **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.

Setting	Description
Basic Settings	
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.	Specify the Circuit Identification Code number of the first B channel of E1 line (SS7). **Note:** The suggested value is the multiples of 32 plus 1, for example: 1, 33, 65.
Calling Party Number Type	Specify the calling party number type. • **National** • **International** • **Subscriber** • **Unknown**
Called Party Number Type	Specify the called party number type. • **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	Specify the interface type according to the trunk specification. • E1 • T1 • J1
Signaling	Specify the Signaling type **E&M**.

Setting	Description
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. • When the **Interface Type** is E1, Framing options are: ◦ Enable CRC4 ◦ Disable CRC4 **Note:** CRC4 is a method of checking for errors in data transmitted on E1 trunk lines. • When the **Interface Type** is T1 or J1, Framing options are: ◦ ESF ◦ D4
Line Code	Choose the line code for this trunk according to the direction provided by your carrier. Line Code options are: • HDB3 • AMI
Codec	Choose the codec for this trunk.
Echo Cancellation	This option enables or disables echo cancellation. **Note:** If an echo occurs during a call, you can enable echo cancellation.

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 for Outbound Calls

ISDN BRI Trunk

BRI Trunk Overview

This topic describes what is BRI trunk and provides the information of BRI cable.

What is BRI trunk

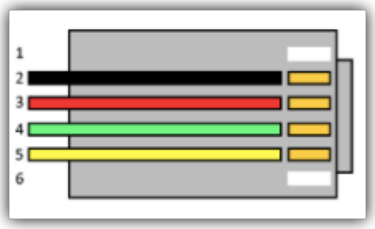
Basic Rate Interface (BRI) is an Integrated Services Digital Network (ISDN) access method, typically used for home and small offices.

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.

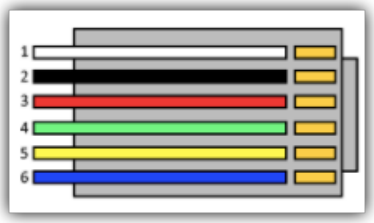
BRI cable

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 encompasses 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 Date 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 web 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. • **Peer to Peer** • **Peer to Multiple Peers**
Signaling Role	Specify whether this interface will act as the user or the network. • **User** • **Network** **Note:** • 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.
Switch Type	Configure the switch type according to the direction provided by your service provider. • **EuroISDN** • **National 2** • **National 1**

Setting	Description
	• **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 internal to **Never** if you don't like the channel to restart.
PRI Indication	Select the PRI Indication. • **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. **Note:** Inband notification is not available on all PRI/BRI subscription lines.

Setting	Description
Carrier Hangup Tone Detection	• Check this option: You will hear the hangup tone played by your carrier when the other party hangs up. **Note:** First check with your carrier whether they will send the prompt or not. • 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.
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'.

Setting	Description
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 for Outbound Calls

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 web 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. Under the **Outbound Rules** tab, 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. If the ITSP requires a prefix to place outbound calls, enter the provided prefix number in the **Prepend for Emergency Number** field.

   The prefix will be automatically added at the beginning of the dialed emergency number. For example, if you set the field to `1234`, when a user dials 911, the PBX system will add 1234 to the emergency number and call out 1234911.

> **Important:**
> Carefully configure the prefix according to the ITSP's requirements, or the emergency calls may fail.

e. **Optional:** Repeat **step a** - **step d** to add another trunk.

> **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 web 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. Under the **Outbound Rules** tab, 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. In the **Trunk's Emergency Outbound Caller ID** field, enter the Emergency Location Identification Number (ELIN) that you have purchased from the trunk provider.

d. If the ITSP requires a prefix to place outbound calls, enter the provided prefix number in the **Prepend for Emergency Number** field.

The prefix will be automatically added at the beginning of the dialed emergency number. For example, if you set the field to `1234`, when a user dials 911, the PBX system will add 1234 to the emergency number and call out 1234911.

> **Important:**
> Carefully configure the prefix according to the ITSP's requirements, or the emergency calls may fail.

e. **Optional:** Repeat **step a** - **step d** to add another trunk.

> **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 web 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 web 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 web 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 web 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 import 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 web 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 web 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.

Related information

Import and Export -FAQ

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 web 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 web 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 web 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 web 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 web 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 different types of time defined in the Yeastar P-Series PBX System. Read the concepts before you manage business hours and holidays.

Key Concepts

Time zones

Time zone is a standard time defined based on geographical regions, ensuring time synchronization across different areas and facilitating the coordination of business operations and communications.

Yeastar P-Series PBX System allows you to use a default time zone or set multiple time zones to meet the specific needs of your business operations.

- **Default Time Zone**

  The system automatically assigns a default time zone based on the date and time settings of the PBX (Path: **System > Date and Time > Time Zone**). This default time zone is applied to system-wide time settings unless additional time zones are configured.
- **Additional Time Zone**

  For businesses operating across different regions, you can add multiple time zones to accommodate regional offices or customers in different regions, and set up business hours and holidays based on each region's local time.

  For more information, see Set Multiple Time Zones.

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 Business Hours and Route Inbound Calls based on 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.

- **Custom Time Periods**

  Custom Time Periods is typically for individual employees who have their own work schedules.

  For more information, see Route Inbound Calls based on Employee 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, and set different prompts for different holidays. 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.

Application

After you configured Business Hours and Holidays feature, the time settings will be applied to various system features for user management and call handling. For detailed information

on the specific applications and how these time conditions are utilized, see Time Condition Overview.

Related information

Set Business Hours
Monitor Time Condition Status
Create a Holiday
Override Time Condition for Inbound Calls
Automatic Reset of Time Condition

Time Zones

Set Multiple Time Zones

Yeastar P-Series PBX System supports multiple time zones, enabling businesses to operate efficiently across different regions by managing calls and settings based on the local time. This topic describes how to set multiple time zones.

Scenarios

For businesses that operates across multiple time zones, or for multi-national companies with employees distributed across different regions, a single time zone setting is insufficient to meet daily operation needs. To ensure smooth collaboration and efficient call management, businesses need the flexibility to configure work hours tailored to each region's local time.

For example, if a business has offices in the US, the UK, and China, administrator can set the US Pacific time zone as the default, add additional time zones for the UK and China, and then configure business hours and holidays for the time zones accordingly. This ensures that staff can work and handle calls aligning with regional working hours, and customers can receive calls or services at appropriate times, improving work efficiency and customer satisfaction.

Requirements and restrictions

Requirements

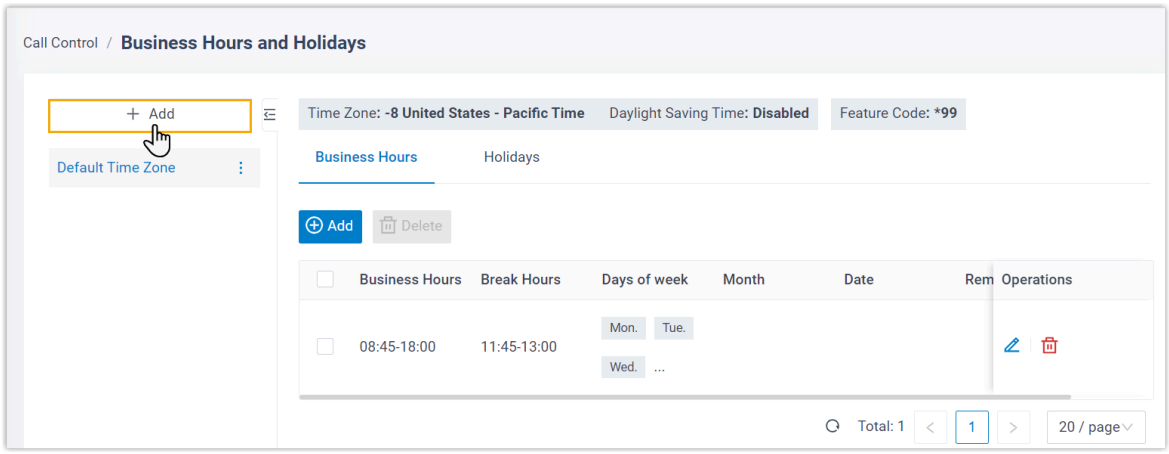
The firmware of Yeastar P-Series PBX System is 37.18.0.59 or later.

Restrictions

Yeastar P-Series PBX System supports up to **24** time zones (including the default time zone).

Procedure

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**.
2. On the side panel, click **Add**.



3. In the pop-up window, configure the time zone settings.

Setting	Description
Name	Set a name to help you identify the time zone.
Time Zone	Select the desired time zone.
Daylight Saving Time	Enable or disable Daylight Saving Time (DST) according to your needs.
Feature Code	This field is auto-populated with a system-generated feature code, which can be used to switch or subscribe to the Business Hours and Holidays status for the specific time zone. **Note:** The usage rules and user permissions follow the configurations on **Call Features > Feature Code > Switch Business Hours and Holidays Status**.
Assign to Extension	Optional. Assign the time zone to desired extensions in bulk. After assigned, the business hours and holidays configured in the time zone will be applied to the selected extensions. **Note:** You can change the time zone for extensions individually on **Extension and Trunk > Extension >** ✎ **> Features > Business Hours > Time Zone**.

4. Click **Save**.
5. Repeat step **2** - **4** to add more time zones as needed.
6. Reboot the PBX to take effect.

Results

The time zones are available in the system.

What to do next

Set Business Hours and Create a Holiday based on time zones.

Related information

Manage Time Zones

Manage Time Zones

This topic describes how to edit and delete the time zones that you've added on the PBX.

Edit a time zone

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**.
2. Click ⋮ beside the desired time zone, then click **Edit**.
3. In the pop-up window, change the time zone settings.
4. Click **Save** and **Apply**.
5. Reboot the PBX to take effect.

   The time zone settings are updated.

Delete a time zone

> **Note:**
> The default time zone can NOT be deleted.

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**.
2. Click ⋮ beside the desired time zone, then click **Delete**.
3. In the pop-up window, click **OK** and **Apply**.

   The time zone is deleted.

Business Hours

Set Business Hours

This topic describes how to set up Business Hours for a specific time zone.

Background information

Business Hours is the main working hours for your company, which may apply to most of the employees who have fixed work schedules.

For more information about different types of time in Yeastar P-Series PBX System, see Overview of Business Hours and Holidays.

Procedure

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, and click the desired time zone.
2. On the **Business Hours** page, click **Add**, then complete the following time settings.
    a. In the **Business Hours** section, click **Add**, then specify the hours when your business is open.
    b. In the **Break Hours** section, click **Add**, then specify rest breaks during the working days.
    c. In the **Date Settings** section, select your working days.
        - **Days of Week**: If enabled, you can only use the **Days of Week** as the date condition for your business hours.
        - **Advanced Options**: If enabled, you can configure business hours more flexibly with a mixed condition of Week, Month, and Date.
    d. **Optional:** In the **Other Options** section, enter a note in the text field to help you identify the time group.
3. Click **Save** and **Apply**.

Result

- A time group is created to define the global business hours in the specific time zone.
- You can create more time groups according to your company's business hours based on different time zones. All the time groups created on the **Business Hours** page are regarded as your company's global business hours in the specific time zone.

What to do next

- To handle inbound calls based on the Global Business Hours, see Route Inbound Calls based on Business Hours.
- To limit users to make outbound calls based on the Global Business Hours, see Set up an Outbound Route.

Related information

Set Multiple Time Zones
Monitor Time Condition Status
Override Time Condition for Inbound Calls
Route Inbound Calls based on Business Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on Employee Hours

Manage Business Hours

This topic describes how to edit and delete the time groups that you've defined as your global business hours for a specific time zone.

Edit a time group of Global Business Hours

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Business Hours** page, select a desired time group, click  .
3. Change the time settings.
4. Click **Save** and **Apply**.

   The global business hours in the time zone is updated.

Delete a time group of Global Business Hours

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Business Hours** page, select a desired time group, click **Delete**.
3. In the pop-up dialog box, click **OK** to confirm.

   The time group is deleted from the global business hours in the time zone.

Related information

Set Business Hours
Overview of Business Hours and Holidays

Holidays

Create a Holiday

This topic describes how to create holidays for a specific time zone by date, week, and month.

Create a holiday by date

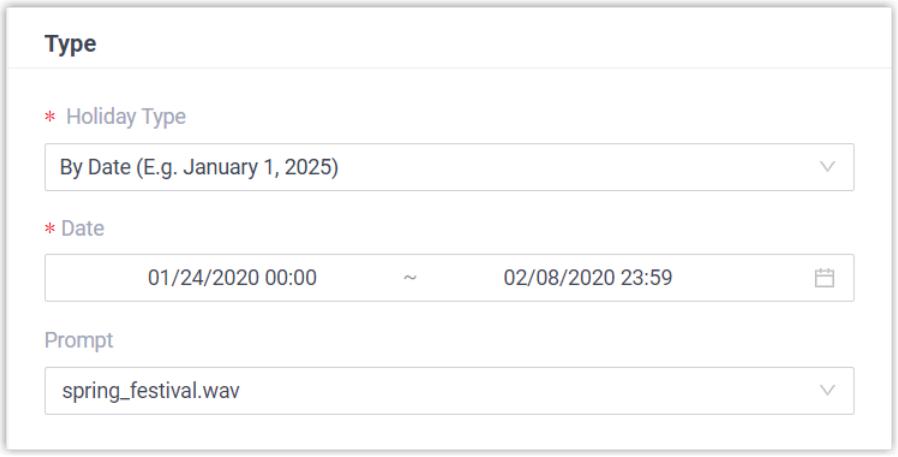
If the holiday date varies every year, you can create a holiday by date.

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 web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Add**, then complete the following holiday settings.
   a. In the **Basic** section, enter `2020 Chinese Spring Festival` in the text field.
   b. In the **Type** section, set the type, date, and prompt of the holiday.



- **Holiday Type**: Select **By Date**.
- **Date**: Select the holiday start date and end date.
- **Prompt**: Optional. Select an existing prompt or click **Upload** to upload a prompt.

> **Note:**
> - Prompts in the drop-down list are synchronized from **PBX Settings > Voice Prompt > Custom Prompt**.
> - To play the prompt to callers when they call to the PBX during holidays, you need to enable **Play Holiday Prompt During Holidays** (Path: **Call Control > Inbound Route > Default Destination > Play Holiday Prompt During Holidays**) for the time-based inbound route.

3. Click **Save** and **Apply**.

Create a holiday by month

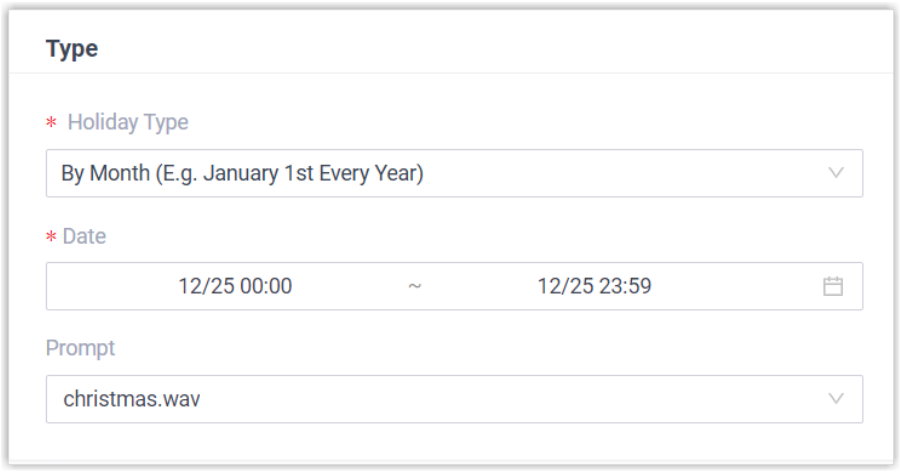
If the holiday always falls on the same date, you can set a holiday by month.

Example

The Christmas falls on Dec. 25 every year. You can set the holiday as follows.

Configuration Example

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Add**, then complete the following holiday settings.
   a. In the **Basic** section, enter `Christmas` in the text field.
   b. In the **Type** section, set the type, date, and prompt of the holiday.



- **Holiday Type**: Select **By Month**.
- **Date**: Select the holiday start date and end date.
- **Prompt**: Optional. Select an existing prompt or click **Upload** to upload a prompt.

> **Note:**
> - Prompts in the drop-down list are synchronized from **PBX Settings > Voice Prompt > Custom Prompt**.
> - To play the prompt to callers when they call to the PBX during holidays, you need to enable **Play Holiday Prompt During Holidays** (Path: **Call Control > Inbound Route > Default Destination > Play Holiday Prompt During Holidays**) for the time-based inbound route.

3. Click **Save** and **Apply**.

Create a holiday by week

If a holiday always falls on the specific week, you can set a holiday by week (which means the day of the specific week of the month).

> **Note:**

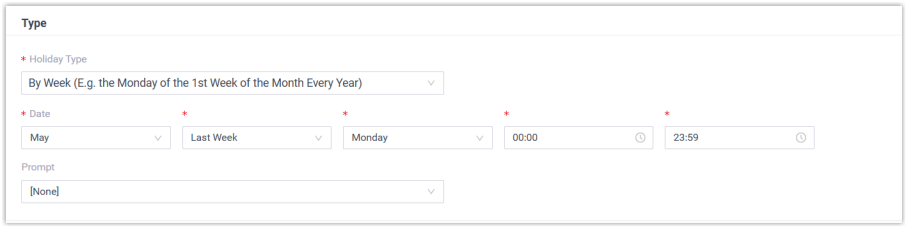
The system calculates the week as the period ending on and including Sunday, and the last week calculates from the last Monday.

Example

2024 Memorial Day falls on the Monday of the last week in May. You can set the holiday as follows.

Configuration Example

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Add**, then complete the following holiday settings.
   a. In the **Basic** section, enter `Memorial Day` in the text field.
   b. In the **Type** section, set the type, date, and prompt of the holiday.



   - **Holiday Type**: Select **By Week**.
   - **Date**: Select the month and the day of the specific week of the month.
   - **Prompt**: Optional. Select an existing prompt or click **Upload** to upload a prompt.

> **Note:**
> - Prompts in the drop-down list are synchronized from **PBX Settings > Voice Prompt > Custom Prompt**.
> - To play the prompt to callers when they call to the PBX during holidays, you need to enable **Play Holiday Prompt During Holidays** (Path: **Call Control > Inbound Route > Default Destination > Play Holiday Prompt**

During Holidays) for the time-based inbound route.

3. Click **Save** and **Apply**.

Create a holiday by weekday

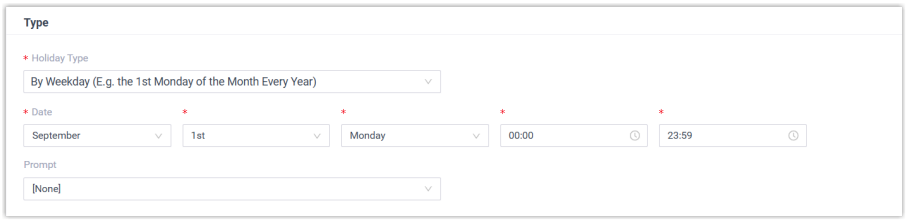
If a holiday always falls on the same weekday, you can set a holiday by weekday (which indicates the specific weekday of the month).

Example

Labor Day falls on the first Monday in September. You can set the holiday as follows.

Configuration Example

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Add**, then complete the following holiday settings.
   a. In the **Basic** section, enter `Labor Day` in the text field.
   b. In the **Type** section, set the type, date, and prompt of the holiday.



- **Holiday Type**: Select **By Weekday**.
- **Date**: Select the month and the weekday of the month.
- **Prompt**: Optional. Select an existing prompt or click **Upload** to upload a prompt.

Note:

- Prompts in the drop-down list are synchronized from **PBX Settings > Voice Prompt > Custom Prompt**.
- To play the prompt to callers when they call to the PBX during holidays, you need to enable **Play Holiday Prompt During Holidays**

(Path: **Call Control > Inbound Route > Default Destination > Play Holiday Prompt During Holidays**) for the time-based inbound route.

3. Click **Save** and **Apply**.

What to do next

- To handle inbound calls based on Holidays, see Set up an Inbound Route.
- To limit users to make outbound calls during holidays, see Set up an Outbound Route.

Related information

Overview of Business Hours and Holidays
Set Multiple Time Zones
Set Business Hours
Manage Holidays
Export and Import Holidays

Manage Holidays

This topic describes how to edit and delete a holiday for a specific time zone.

Edit a holiday

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, select a desired holiday, click .
3. Change the holiday settings.
4. Click **Save** and **Apply**.

   The holiday list is updated.

Delete a holiday

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, select a desired holiday, click **Delete**.
3. In the pop-up dialog box, click **OK** to confirm.

The holiday is deleted from the holiday list.

Related information

Create a Holiday
Overview of Business Hours and Holidays
Export and Import Holidays

Export and Import Holidays

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

Export holidays

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

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Export**.

   A CSV file is saved to your computer. To check and edit parameters in the CSV file, see Holidays Parameters.

Import holidays

We recommend that you export holidays 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 Holidays Parameters.

Procedure

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Import**.
3. In the pop-up window, click **Browse**, and select your CSV file.
4. Click **Import**.

   The holidays in the CSV file will be displayed in the **Holidays** list.

Related information

Overview of Business Hours and Holidays
Create a Holiday
Manage Holidays

Time Condition

Time Condition Overview

Time Condition is the communication feature in Yeastar P-Series PBX System that enables you to set up distinct time periods for call handling. Time Condition allows you to route calls to various destinations at a different time like business hours, outside business hours, and holidays.

Where can Time Condition be applied?

Time Condition can be applied to the following features:

Apply to extension presence switch

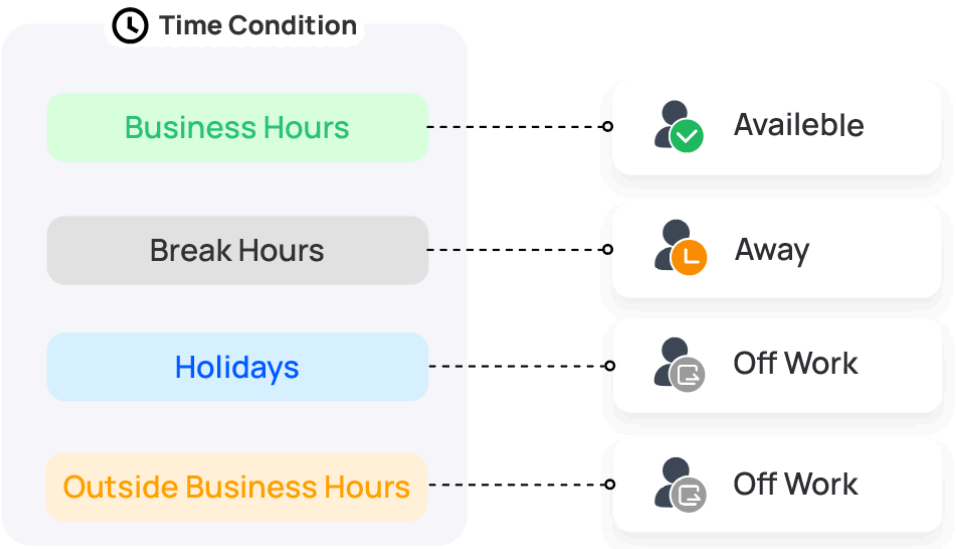
Extension presence status can be auto switched based on Time Condition. When time condition changes, extension presence status would be changed accordingly.

For example, when the PBX is in the time condition for Business Hours, the extension status is auto switched to **Available**.

Note:

- This feature should be configured on extension configuration page. For more information, see Automatically Switch Extension Presence Based on Time.

- In addition to the time group associated in the specific time zone, you can also customize business hours for an extension individually, which will be applied to the presence switch for the extension. For more information, see Set Business Hours for an Extension

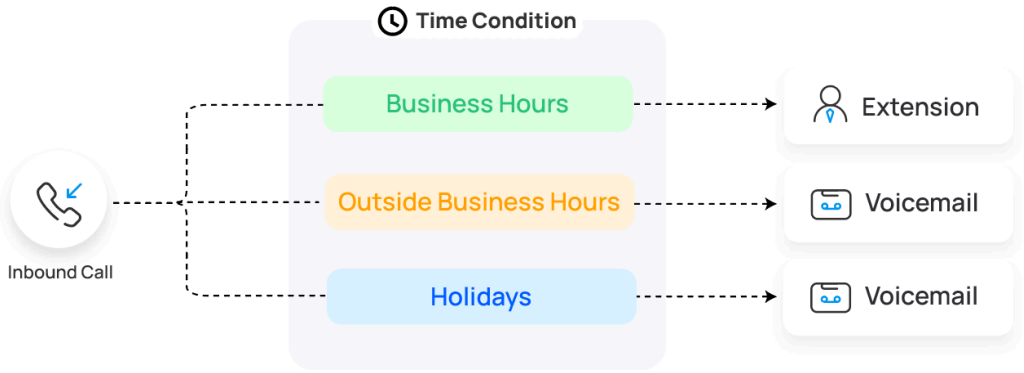


Apply to an Inbound Route

Time Condition can be used to control the destination of an inbound call based on date and time.

When a call reaches PBX, the system will check the date and time based on the specified time zone against the time group associated, and then route the call to corresponding destination.

For more information, see Set up an Inbound Route.

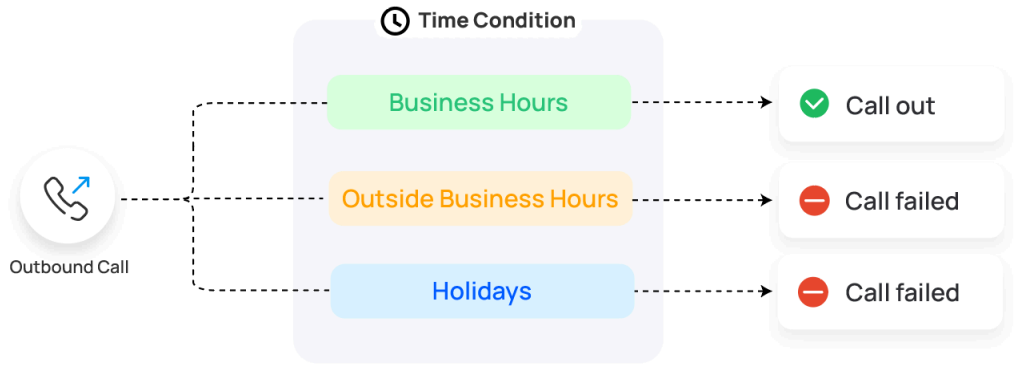


Apply to an Outbound Route

Time Condition can be used to limit the use of an Outbound Route based on date and time.

When a call is made, the system will check the date and time based on the specified time zone against the time group associated. Only when the time comes to the permitted time group can the outbound call be made.

For more information, see Set up an Outbound Route.

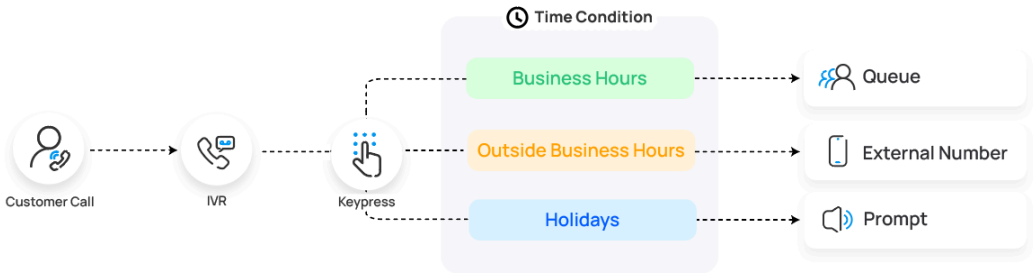


Apply to IVR

Time Condition can be used to control the destination of IVR key press event based on date and time.

When a caller calls an IVR and press a key, the system will check the date and time based on the specific time zone against the time group associated, and then route the call to corresponding destination.

For more information, see Set Key Events Based on Time Conditions.

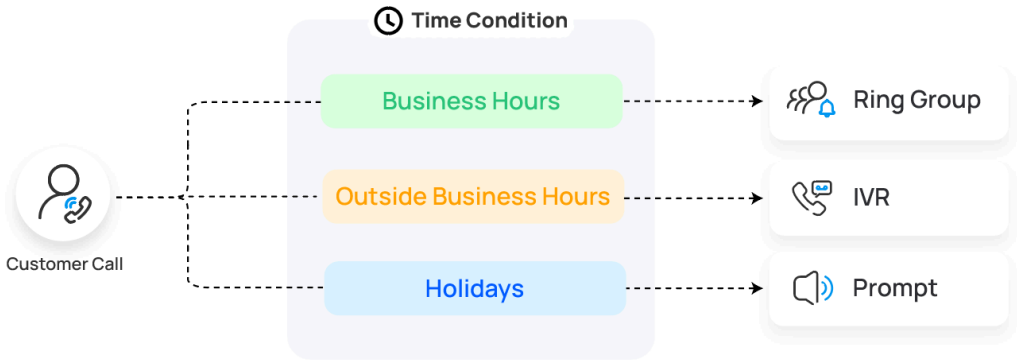


Apply to Ring Group

Time condition can be used to control the destination of calls sent to a ring group.

By default, the ring group receives incoming calls during all time periods. You can set the ring group to receive calls only during business hours, while routing calls to other destinations based on the specified time conditions.

For more information, see Create a Ring Group.

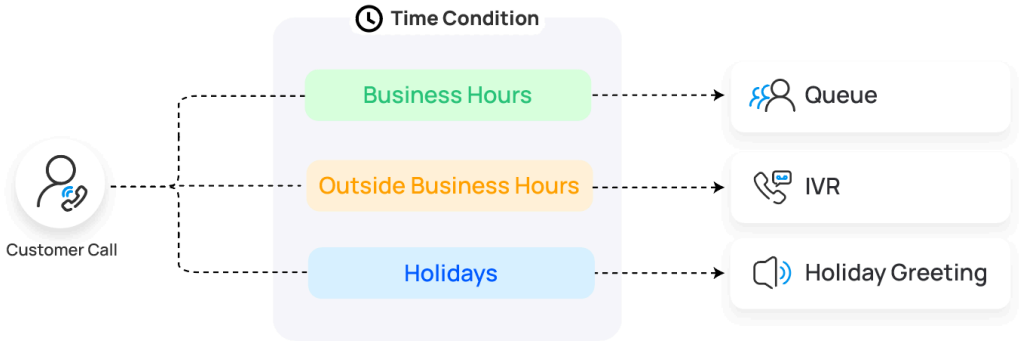


Apply to Call queue

Time condition can be used to control the destination of calls sent to a call queue.

By default, the call queue receives incoming calls during all time periods. You can set the call queue to receive calls only during business hours, while routing calls to other destinations based on the specified time conditions.

For more information Route Queue Call Based on Time Condition.



Time Condition override

For a time-based inbound route, the system routes inbound calls based on the system time. However, users may need to force open or close business occasionally. In this case, you can grant permissions to allow specific users to override time condition for inbound calls through the route. For more information, see Override Time Condition for Inbound Calls.

Note:

- If users do not manually clear time condition override, the system will automatically reset the time condition. For more information, see Automatic Reset of Time Condition.
- To keep the time condition after overriding, see Disable automatic reset of time condition.

Related information

Route Inbound Calls based on Business Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on Employee Hours
Set up an Outbound Route

Allow Users to Override Time Condition by Feature Code

By default, all the users can NOT override time condition. To allow users to override time condition by feature code, follow instructions in the topic to grant permissions to specific users.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. Scroll down the page, and configure the permission of time condition override in the **Switch Business Hours and Holidays Status** section.

   Table 20.

Setting	Feature Code	Permission
Switch Business Hours and Holidays Status (for Business Hours configured in the system's default time zone)	*99 **Note:** This feature code applies only to the system's default time zone. For additional time zones, you can check the corresponding feature code under the specific time zone settings (Path: **Call Control > Business Hours and Holidays**).	Select desired extensions.
Time Condition Switching Prefix (for Custom Business Hours and Custom Time Periods based on the system's default time zone)	Starting with prefix *8 **Note:** Feature codes starting with *8 would be generated for inbound routes that are based on Custom Business Hours or Custom Time Periods.	

3. Click **Save** and **Apply**.

Related information

Override Time Condition for Inbound Calls
Monitor Time Condition Status
Automatic Reset of Time Condition
Enable or Disable Automatic Reset of Time Condition

Allow Users to Override Time Condition on Operator Panel

By default, all the users can NOT override time condition. To allow users to override time condition on Operator Panel, follow instructions in the topic to grant permissions to specific users.

Restrictions

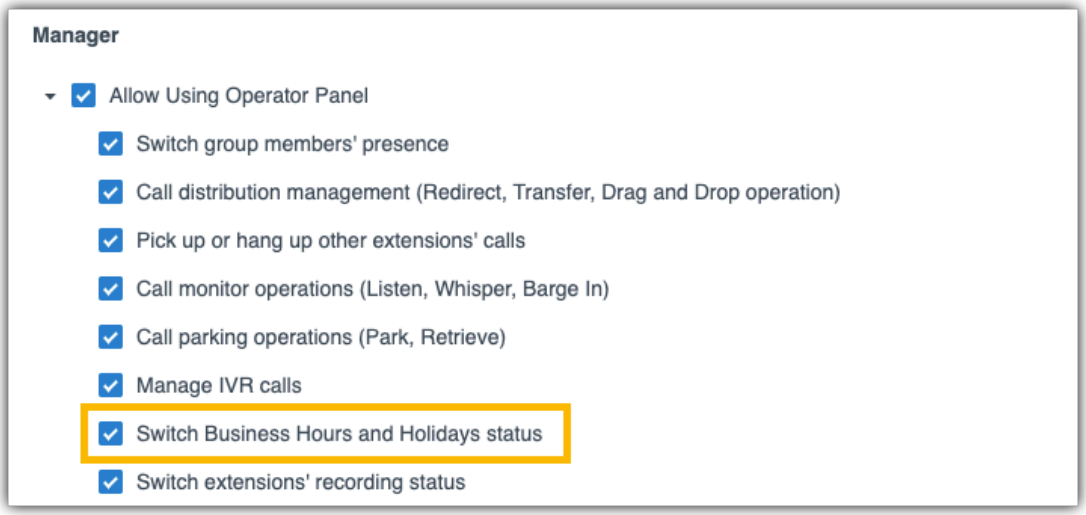
On Operator Panel, only time condition for Business Hours configured in the system's default time zone can be overridden.

Procedure

The permission of time condition override can only be assigned to extension group managers. Follow the instructions below to grant permission to extension group managers.

> **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.

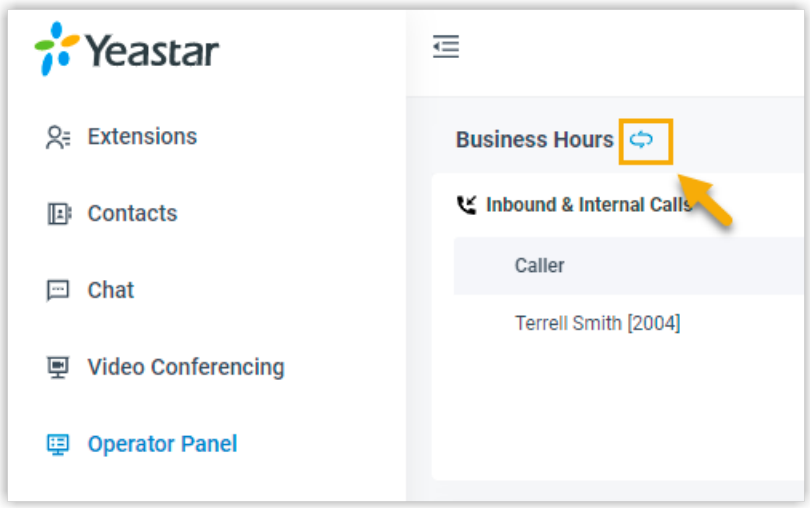
1. Log in to PBX web portal, go to **Extension and Trunk > Extension Group**.
2. Select an extension group, and click .
3. On the **Extension Group** page, click **Group Permissions** tab.
4. In the **Permission Configuration** section, select the checkbox of **Switch Business Hours and Holidays status**.



5. Click **Save** and **Apply**.

Result

On Operator Panel, the user whose user type is Manager can click to override time condition for Business Hours configured in the system's default time zone.



For more information, see Override Time Condition on Operator Panel.

Related information

Allow Users to Override Time Condition by Feature Code
Automatic Reset of Time Condition
Enable or Disable Automatic Reset of Time Condition

Override Time Condition for Inbound Calls

If you have configured a time-based inbound route, the system will automatically route calls to different destinations based on time. However, users may need to force open or close business occasionally. This topic describes how to achieve time condition override for inbound calls.

Background information

Users may need to override time condition in the following scenarios:

- **Temporary night shift**

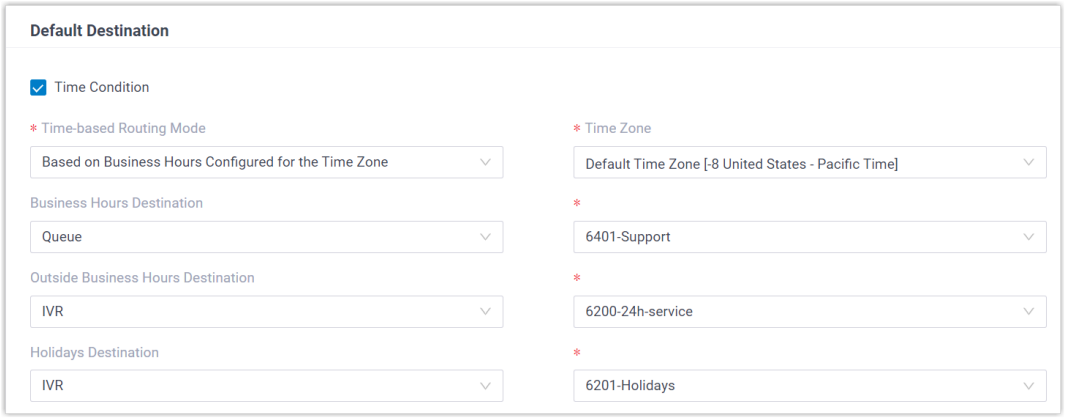
  After business hours, the employee who needs to work in the night can force open the business hours to provide communication services for customers.
- **Occasionally leaving**

  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.

Override time condition for inbound calls (Global Business Hours)

Background information

An inbound route based on business hours configured in the system's default time zone is set up as follows:



Procedure

Follow the instructions below to achieve time condition override for inbound calls through the route:

1. Grant permission to allow specific users to override time condition.
2. To override time condition, the authorized users should dial corresponding feature code (default ***99**).

   Inbound calls would be routed to different destinations based on the time when users dial feature code.

   Table 21.

Operate Time	Result
Dial *99 during **Business Hours**	Inbound calls will be routed to **Outside Business Hours** destination (IVR 6200).
Dial *99 during **Outside Business Hours**	Inbound calls will be routed to **Business Hours** destination (Queue 6400).
Dial *99 during **Holidays**	Inbound calls will be routed to **Business Hours** destination (Queue 6400).

3. To clear time condition override, the authorized users should dial feature code (default: *99) again.

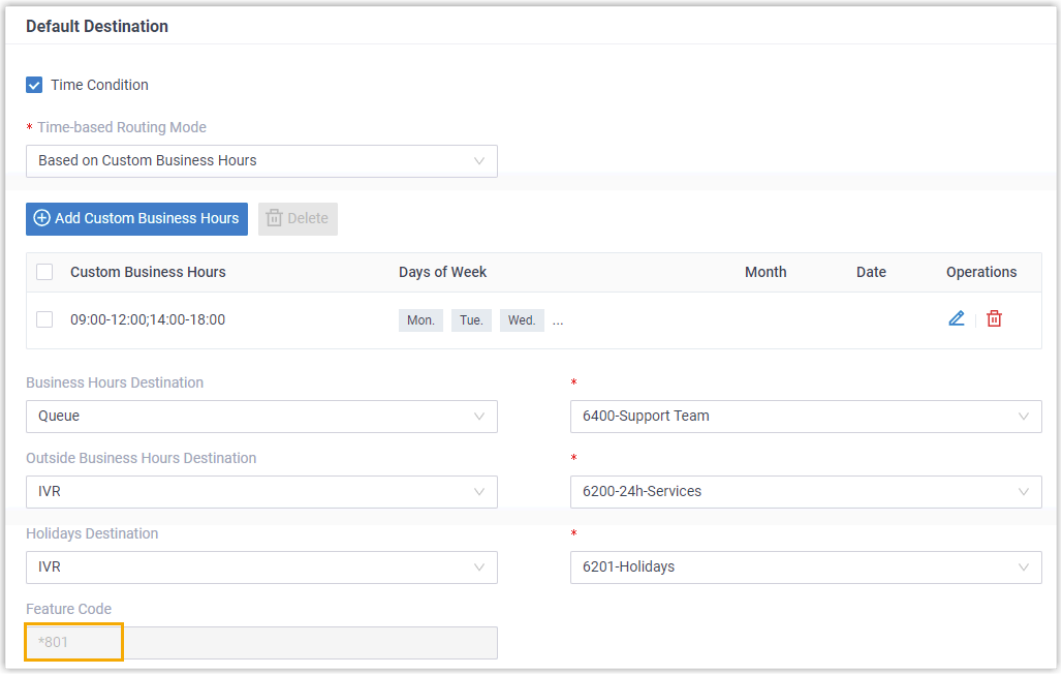
Note:

- If users do not manually clear time condition override, the system will automatically reset the time condition. For more information, see Automatic Reset of Time Condition.
- To keep the time condition after overriding, see Disable automatic reset of time condition.

Override time condition for inbound calls (Custom Business Hours)

Background information

An inbound route based on Custom Business Hours (follows the system's default time zone) is set up as follows:



Procedure

Follow the instructions below to achieve time condition override for inbound calls through the route:

1. Grant permission to allow specific users to override time condition.
2. To override time condition, the authorized users should dial feature code *801.

Inbound calls would be routed to different destinations based on the time when users dial feature code.

Table 22.

Operate Time	Result
Dial *801 during **Business Hours**	Inbound calls will be routed to **Outside Business Hours** destination (IVR 6200).
Dial *801 during **Outside Business Hours**	Inbound calls will be routed to **Business Hours** destination (Queue 6400).
Dial *801 during **Holidays**	Inbound calls will be routed to **Business Hours** destination (Queue 6400).

3. To clear time condition override, the authorized users should dial *801 again.

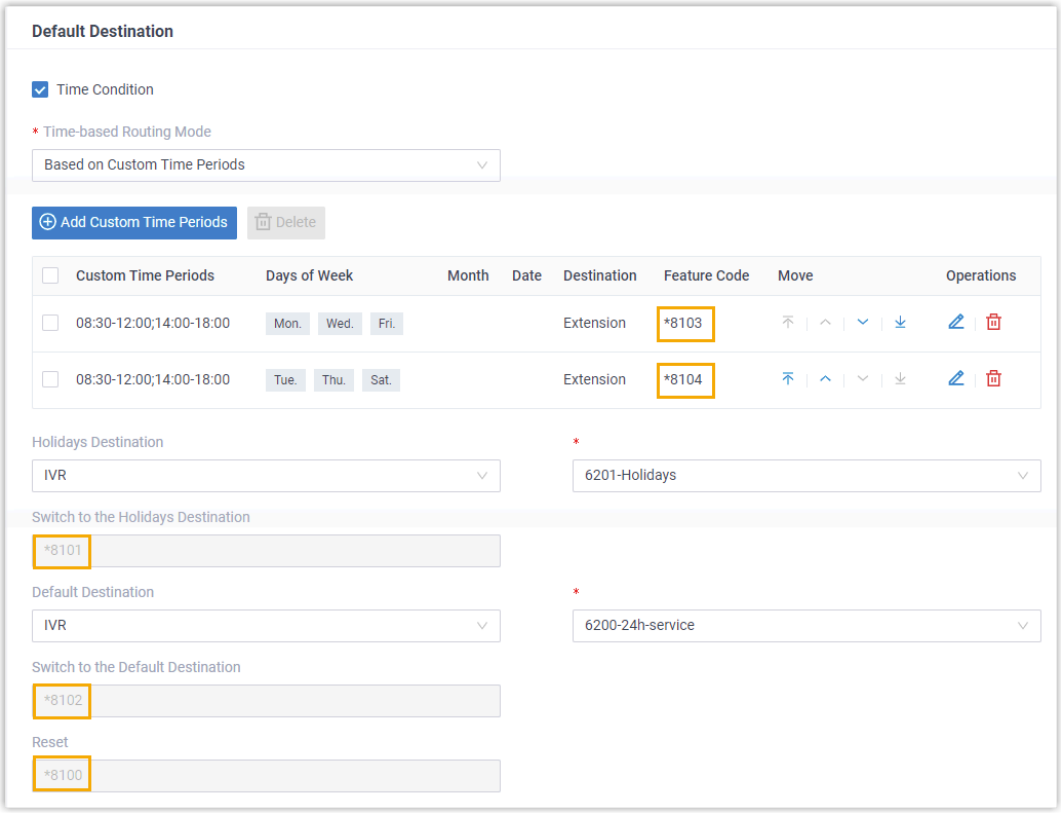
Note:

- If users do not manually clear time condition override, the system will automatically reset the time condition. For more information, see Automatic Reset of Time Condition.
- To keep the time condition after overriding, see Disable automatic reset of time condition.

Override time condition for inbound calls (Custom Time Periods)

Background information

An inbound route based on Custom Time Periods (follows the system's default time zone) is set up as follows:



Procedure

Follow the instructions below to achieve time condition override for inbound calls through the route:

1. Grant permission to allow specific users to override time condition.
2. To override time condition, the authorized users should dial a specific feature code.

   Inbound calls would be routed to corresponding destination based on the dialed feature code.

Table 23.

Time Group	Description	Destination	Feature Code
Time Period 1	Monday, Wednesday, Friday • 08:30 - 12:00 • 14:00 - 18:00	Extension (2000-Leo Ball)	*8103
Time Period 2	Tuesday, Thursday, Saturday	Extension	*8104

Time Group	Description	Destination	Feature Code
	• 08:30 - 12:00 • 14:00 - 18:00	(2004-Terrell Smith)	
Holidays		IVR (6201-Holidays)	*8101
Outside Business Hours		IVR (6200-24h-Services)	*8102

3. To clear time condition override, the authorized users should dial the **Reset** feature code *8100.

> **Note:**
> - If users do not manually clear time condition override, the system will automatically reset the time condition. For more information, see Automatic Reset of Time Condition.
> - To keep the time condition after overriding, see Disable automatic reset of time condition.

Related information

Allow Users to Override Time Condition by Feature Code
Allow Users to Override Time Condition on Operator Panel
Monitor Time Condition Status
Automatic Reset of Time Condition
Enable or Disable Automatic Reset of Time Condition

Monitor Time Condition Status

This topic describes how to set BLF keys on IP phones to monitor time condition status. In this way, users can know which time period the system is working and where inbound calls would be routed.

Background information

Users can monitor time condition status in the following ways:

Monitor time condition status on IP phone

For the users who want to monitor time condition status on their phones, you can set a BLF key for each user.

For more information, see the followings:

- Monitor time condition status for inbound calls (Global Business Hours)
- Monitor time condition status for inbound calls (Custom Business Hours)
- Monitor time condition status for inbound calls (Custom Time Periods)

Monitor time condition status on Operator Panel

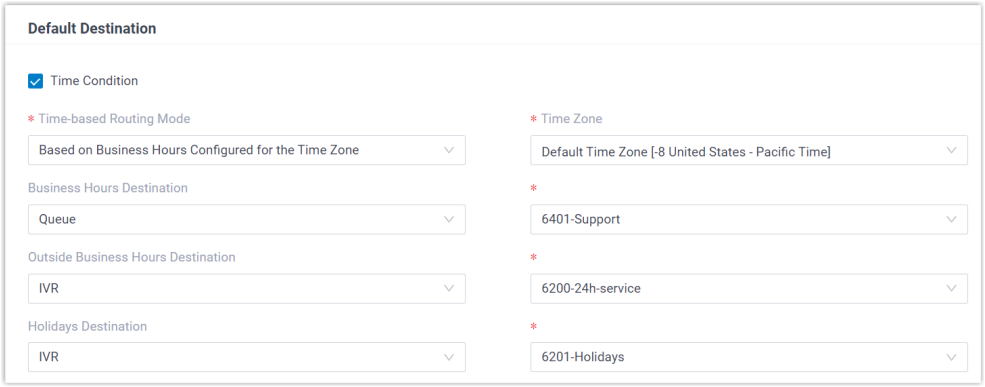
For the users who have permission to access Operator Panel, they can monitor time condition status on Operator Panel directly.

For more information, see Monitor Time Condition Status on Operator Panel.

Monitor time condition status for inbound calls (Global Business Hours)

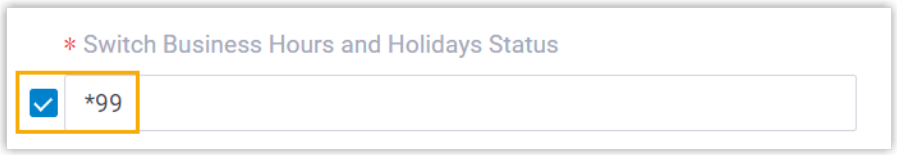
Background information

- An inbound route based on Business Hours configured in the system's default time zone is set up as follows:



- The feature code for **Switch Business Hours and Holidays Status** is *99.

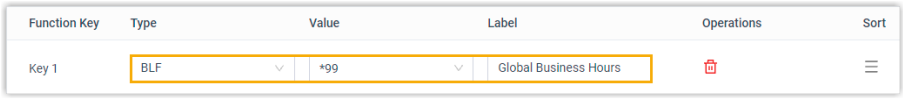
> **Note:**
> This feature code applies only to the system's default time zone. For additional time zones, you can check the corresponding feature code under the specific time zone settings (Path: **Call Control > Business Hours and Holidays**).



Procedure

1. Assign function keys for extension users to monitor time condition status.
    a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, click beside the desired extension.
    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 and Holidays Status**. In this example, enter `*99`.
    - **Label**: Optional. Enter a value, which will be displayed on the phone screen.

    d. Click **Save**.
2. If the extension has been provisioned and 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.
    c. In the pop-up window, click **OK** to reprovision the phone.
3. If the extension hasn't been associated with a phone, see the following topics to bind a phone with the extension.
    - Auto Provision IP Phones in Local Network (PnP Method)

- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

Result

The function key settings are automatically updated on the phone and different BLF LED indicates different status.

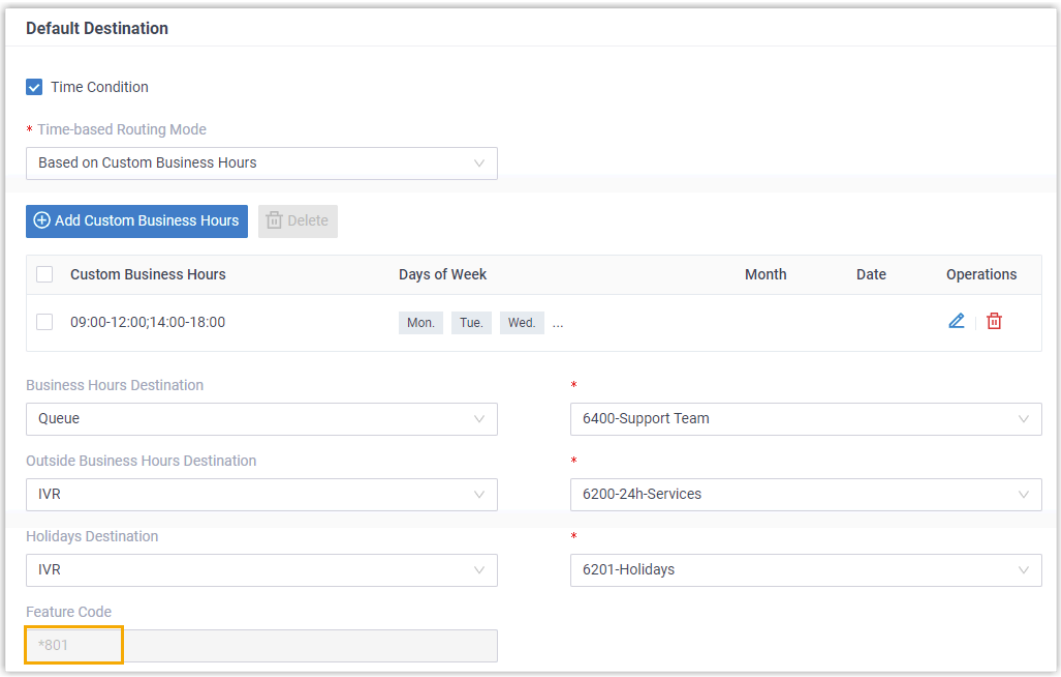
- **Red**: The system is in the status of **Business Hours**.
- **Green**: The system is in the status of **Outside Business Hours** or **Holidays**.
- **Off**: The BLF configurations are incorrect.

> **Note:**
> To change the BLF light color, go to **Call Features > Feature Code > Switch Business Hours and Holidays Status > BLF Light Color of Switching Global Business Hours Status**.

Monitor time condition status for inbound calls (Custom Business Hours)

Background information

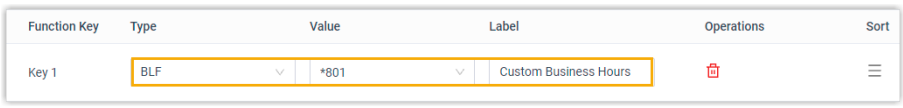
An inbound route based on Custom Business Hours (follows the system's default time zone) is set up as follows:



Procedure

1. Assign function keys for extension users to monitor time condition status.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, click ✎ beside the desired extension.
   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 feature code of the inbound route. In this example, enter `*801`.

- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

d. Click **Save**.

2. If the extension has been provisioned and associated with a phone, re-provision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to this extension.
   c. In the pop-up window, click **OK** to reprovision the phone.
3. If the extension hasn't been associated with a phone, see the following topics to bind a phone with the extension.
   - Auto Provision IP Phones in Local Network (PnP Method)
   - Auto Provision IP Phones in Local Network (DHCP Method)
   - Auto Provision IP Phones Remotely (RPS FQDN Method)
   - Auto Provision IP Phones Remotely (RPS Method)

Result

The function key settings are automatically updated on the phone and different BLF LED indicates different status.

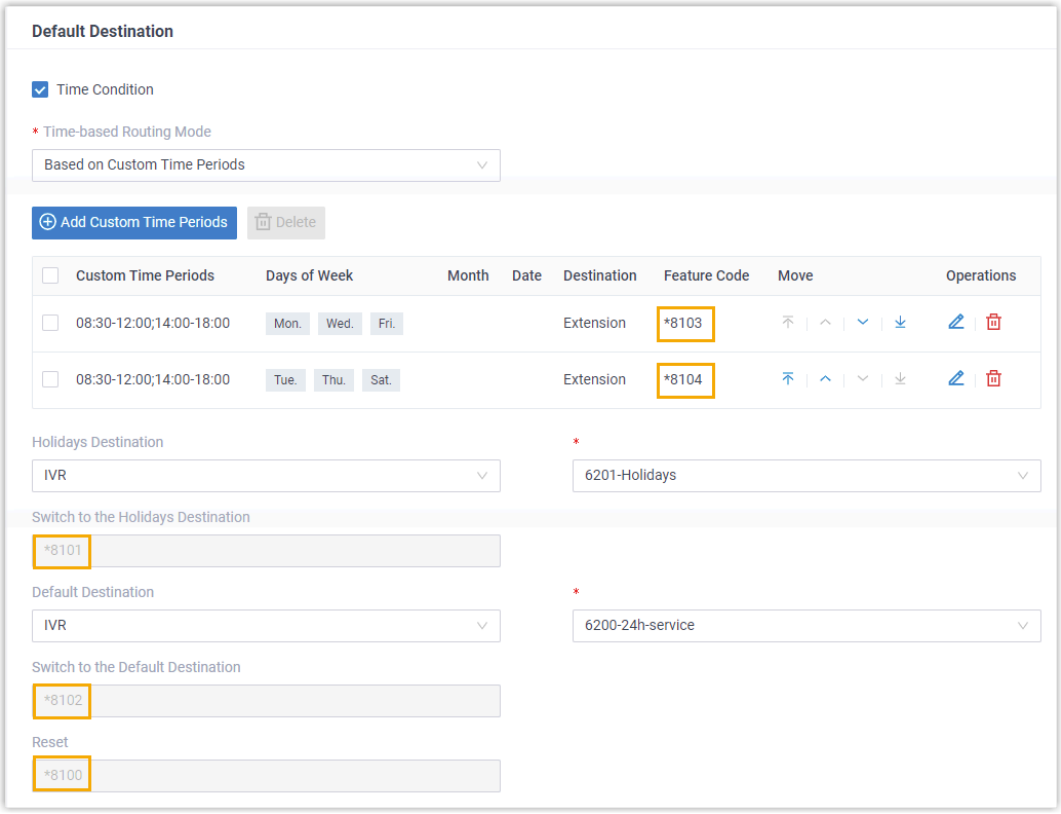
- **Red**: The system is in the status of **Business Hours**.
- **Green**: The system is in the status of **Outside Business Hours** or **Holidays**.
- **Off**: The BLF configurations are incorrect.

> **Note:**
> To change the BLF light color, go to **Call Features > Feature Code > Switch Business Hours and Holidays Status > BLF Light Color of Switching Global Business Hours Status**.

Monitor time condition status for inbound calls (Custom Time Periods)

Background information

An inbound route based on Custom Time Periods (follows the system's default time zone) is set up as follows:



Procedure

1. Assign function keys for extension users to monitor time condition status.
    a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, click beside the desired extension.
    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 codes as needed.
- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

d. Click **Save**.

2. If the extension has been provisioned and associated with a phone, re-provision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to this extension.
   c. In the pop-up window, click **OK** to reprovision the phone.
3. If the extension hasn't been associated with a phone, see the following topics to bind a phone with the extension.
   - Auto Provision IP Phones in Local Network (PnP Method)
   - Auto Provision IP Phones in Local Network (DHCP Method)
   - Auto Provision IP Phones Remotely (RPS FQDN Method)
   - Auto Provision IP Phones Remotely (RPS Method)

Result

The function key settings are automatically updated on the phone and different BLF LED indicates different status.

- **Red**: The system is in the status of **Business Hours**.
- **Green**: The system is in the status of **Outside Business Hours** or **Holidays**.
- **Off**: The BLF configurations are incorrect.

> **Note:**
> - If the BLF key is set for **Reset** feature code, the BLF LED should be off.

- To change the BLF light color, go to **Call Features > Feature Code > Switch Business Hours and Holidays Status > BLF Light Color of Switching Global Business Hours Status**.

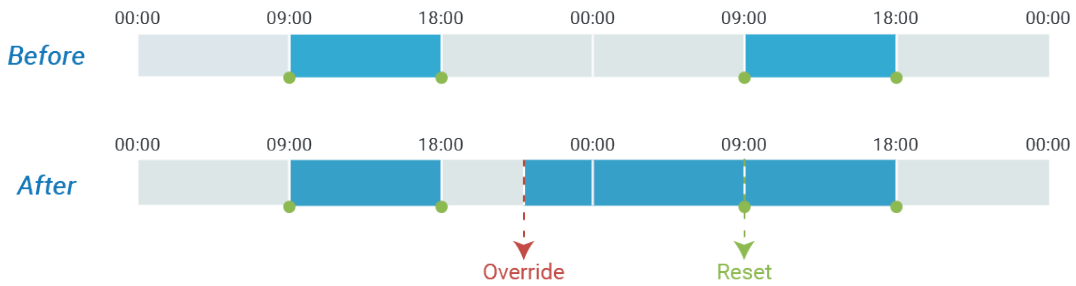
Automatic Reset of Time Condition

By default, if users have overridden time condition and don't clear the time condition override manually, PBX will automatically reset time condition in next period. The next period can be the starting point of business hours, outside business hours, or holidays. This topic gives examples to help you understand how the system automatically resets time condition.

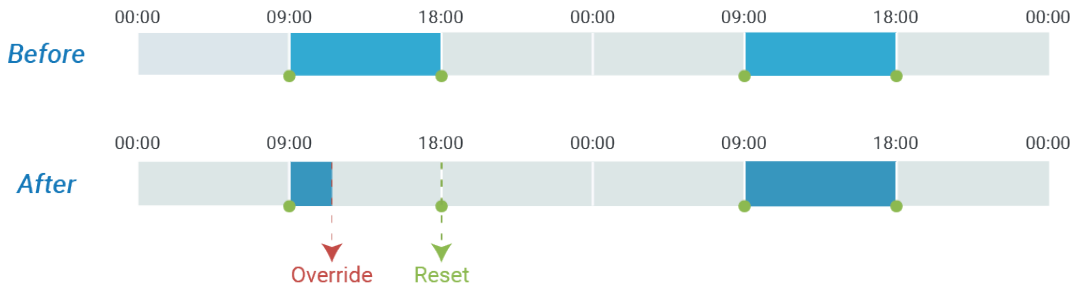
Examples for Global Business Hours/Custom Business Hours

	Business Hours
	Outside Business Hours
	Next hop of time condition: According to the time condition you configured, the system automatically switches the destination for incoming calls at the time point.
	Override time condition
	Automatically reset time condition

Example 1: Override to Business Hours



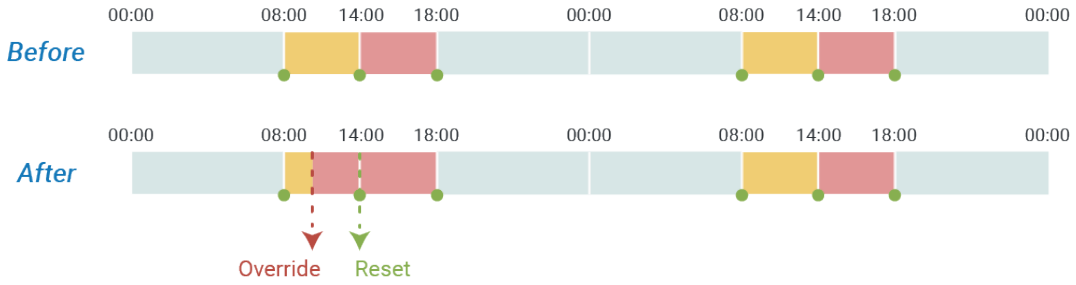
Example 2: Override to Outside Business Hours



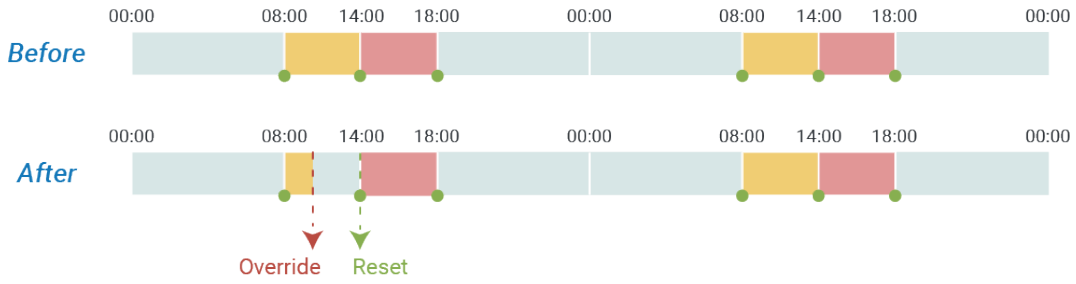
Examples for Custom Time Periods

	Time Period 1
	Time Period 2
	Outside Business Hours
	Next hop of time condition: According to the time condition you configured, the system automatically switches the destination for incoming calls at the time point.
	Override time condition
	Automatically reset time condition

Example 1: Override to Time Period 2



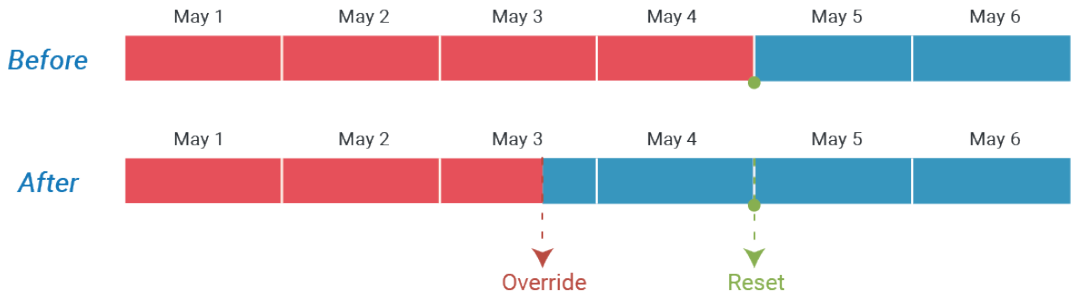
Example 2: Override to Outside Business Hours



Example for Holidays

	Business Hours
	Holidays
	Next hop of time condition (holiday or non-holiday): According to the time condition you configured, the system automatically switches the destination for incoming calls at the time point.
	Override time condition
	Automatically reset time condition

Example: Override to non-holiday



Related information

Enable or Disable Automatic Reset of Time Condition
Monitor Time Condition Status
Override Time Condition for Inbound Calls

Enable or Disable Automatic Reset of Time Condition

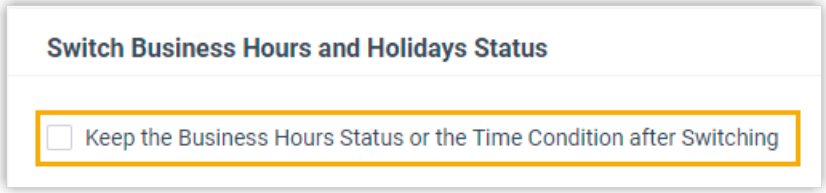
By default, if users have overridden time condition and don't clear the time condition override manually, PBX will automatically reset time condition in next period. You can decide whether to auto reset time condition or keep the time condition after overriding.

Enable automatic reset of time condition

To make the system go back to the normal schedule after users override time condition, follow the instructions below.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. Scroll down to **Switch Business Hours and Holidays Status** section.
3. Unselect the checkbox of **Keep the Business Hours Status or the Time Condition after Switching**.



4. Click **Save** and **Apply**.

Result

When it comes to the next starting point of business hours, outside business hours, or holidays, the system will reset time condition and go back to the normal schedule.

For more information, see Automatic Reset of Time Condition.

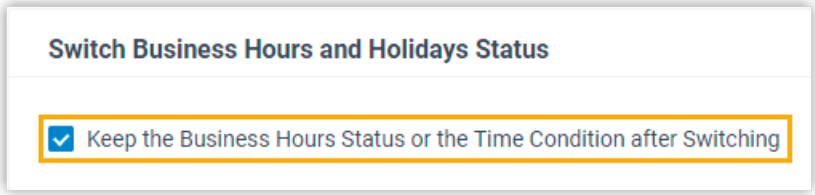
Disable automatic reset of time condition

To make the system keep the status after users override time condition, follow the instructions below.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. Scroll down to **Switch Business Hours and Holidays Status** section.

3. Select the checkbox of **Keep the Business Hours Status or the Time Condition after Switching**.



4. Click **Save** and **Apply**.

Result

After users override time condition, the system will stay in the state until someone manually clear the override.

> **Tip:**
> Tips for clearing the override:
>
> - For inbound route based on **Global Business Hours**, dial the feature code of **Switch Global Business Hours and Holidays Status**.
> - For inbound route based on **Custom Business Hours**, dial the feature code of corresponding inbound route.
> - For inbound route based on **Custom Time Periods**, dial the **Reset** feature code.

Related information

Override Time Condition for Inbound Calls
Monitor Time Condition Status

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 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 web 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. 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.
5. **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.

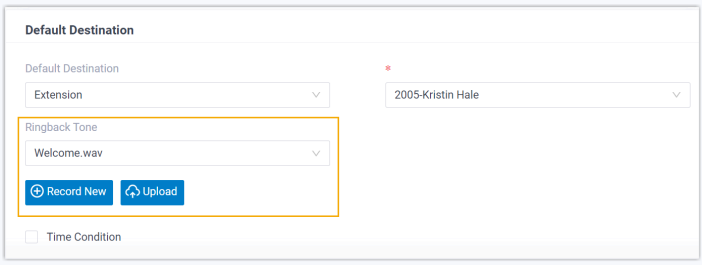
   For more information, see Route Inbound Calls based on DID Numbers.
6. **Optional:** If you want to route inbound calls based on Caller IDs, configure **Caller ID Pattern**.

   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.
7. Configure the inbound route destination.

   > **Note:**
   > When the destination is set to an extension, you can select or upload a music in the follow-up **Ringback Tone** field, which will be played to the caller before the extension user answers the call.



- 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.
  d. **Optional:** If you want to route inbound calls based on the business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**.

     Inbound calls during holiday will be distributed to other destinations according to your office hour setting.
  e. **Optional:** To play a prompt to callers before routing the inbound calls to the holiday destination, select the checkbox of **Play Holiday Prompt During Holidays**.

     > **Note:**
     > Make sure that you have set a prompt for the holiday (Path: **Call Control > Business Hours and Holidays > Holidays > Type > Prompt**). Otherwise, the inbound calls will be directly routed to the holiday destination without playing a prompt.

  For more information of inbound call routing based on time, see the following topics:

  - Route Inbound Calls based on 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**.

Time Based Inbound Routes

Route Inbound Calls based on Business Hours

This topic gives a configuration example to describe how to configure inbound route to control inbound calls based on Business Hours in a specific time zone, 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, and play a prompt "office_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.
- 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 play a prompt to customers when they make calls to the trunk during holidays, a prompt should be preconfigured.

  In this scenario, a prompt "office_holiday" is preconfigured.

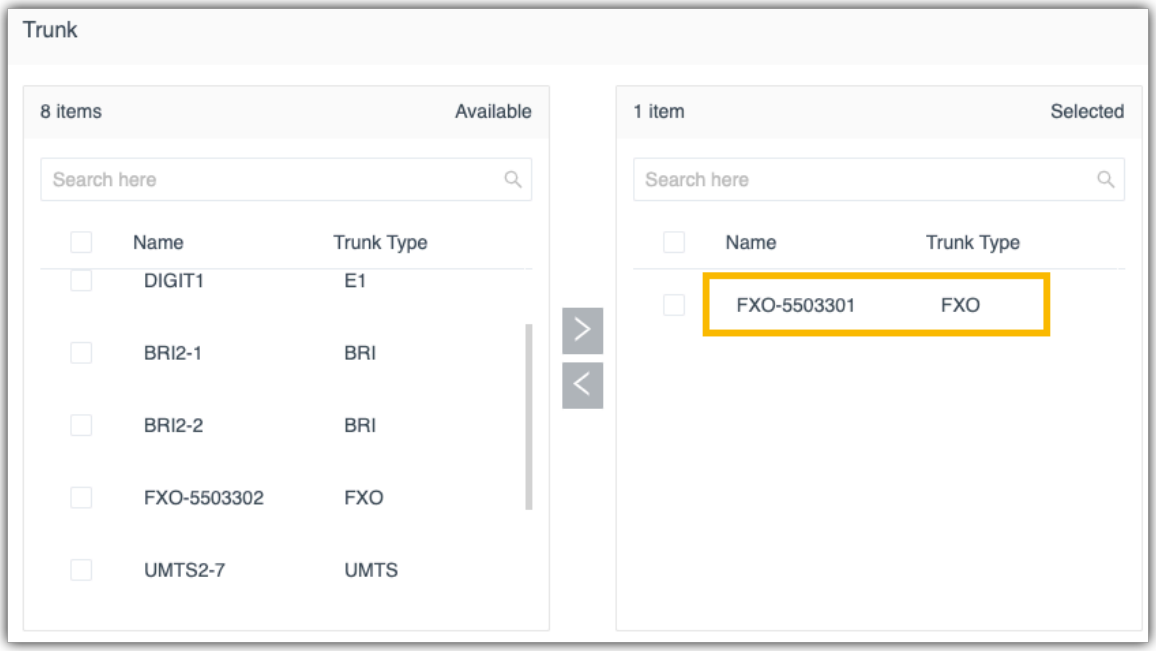
  For more information, see Create a Holiday.
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always directed to your desired destination.

  How to configure inbound route based on DID numbers, see Route Inbound Calls based on DID Numbers.

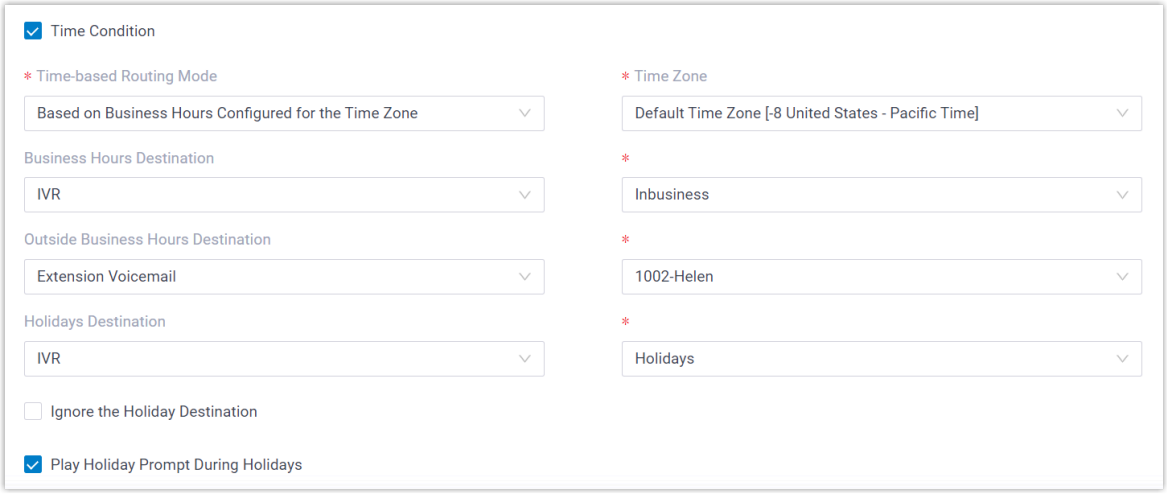
Procedure

1. Log in to PBX web 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:



   a. Select the checkbox of **Time Condition**.
   b. In the drop-down list of **Time-based Routing Mode**, select **Based on Business Hours Configured for the Time Zone**, then select the specific time zone.
   c. Configure the following destinations based on the time.
      - **Business Hours Destination**: Select the destination for inbound calls during the business hours configured for the selected time zone.

        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 configured for the selected time zone.

  In this scenario, select **IVR**, and select the IVR for holidays.

d. Select the checkbox of **Play Holiday Prompt During Holidays**.

   In this scenario, the system will play the prompt "office_holiday" before routing inbound calls to the holiday destination.

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 provides a configuration example on how to configure inbound routes for departments working in different time periods from the company's global business hours, based on the system's default time zone, and control the call destinations accordingly.

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, and play a prompt "office_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 about the configurations of queue and IVR, see Create a Queue and Set up an IVR.
- If you want to play a prompt to customers when they make calls to the trunk during holidays, a prompt should be preconfigured.

  In this scenario, a prompt "office_holiday" is preconfigured.

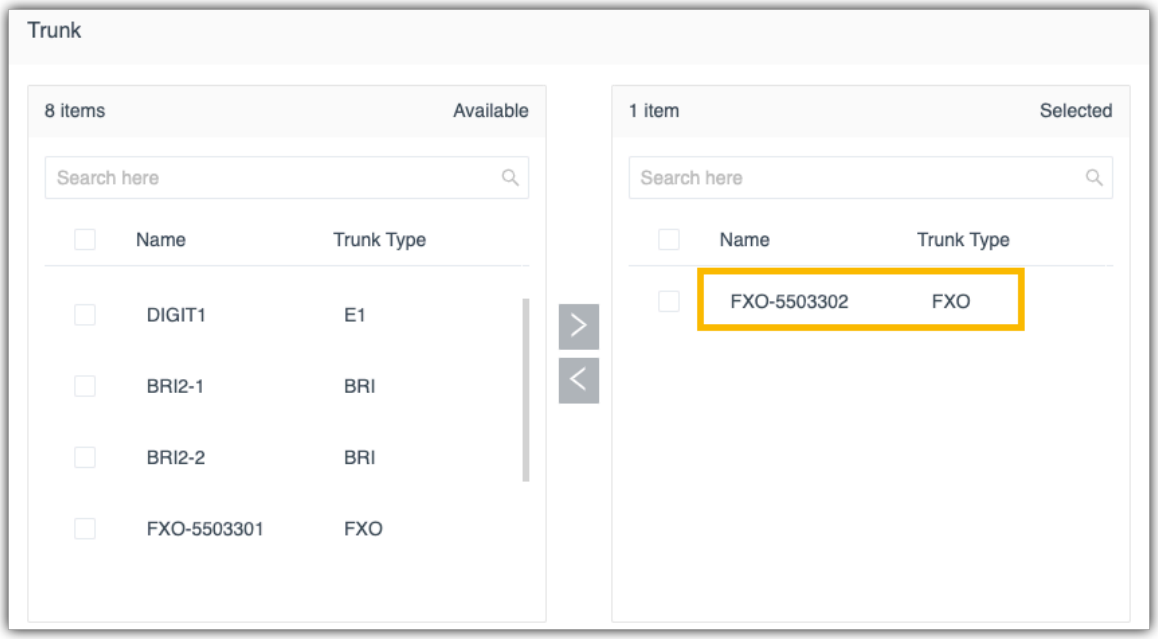
  For more information, see Create a Holiday.
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always directed to your desired destination.

  How to configure inbound route based on DID numbers, see Route Inbound Calls based on DID Numbers.

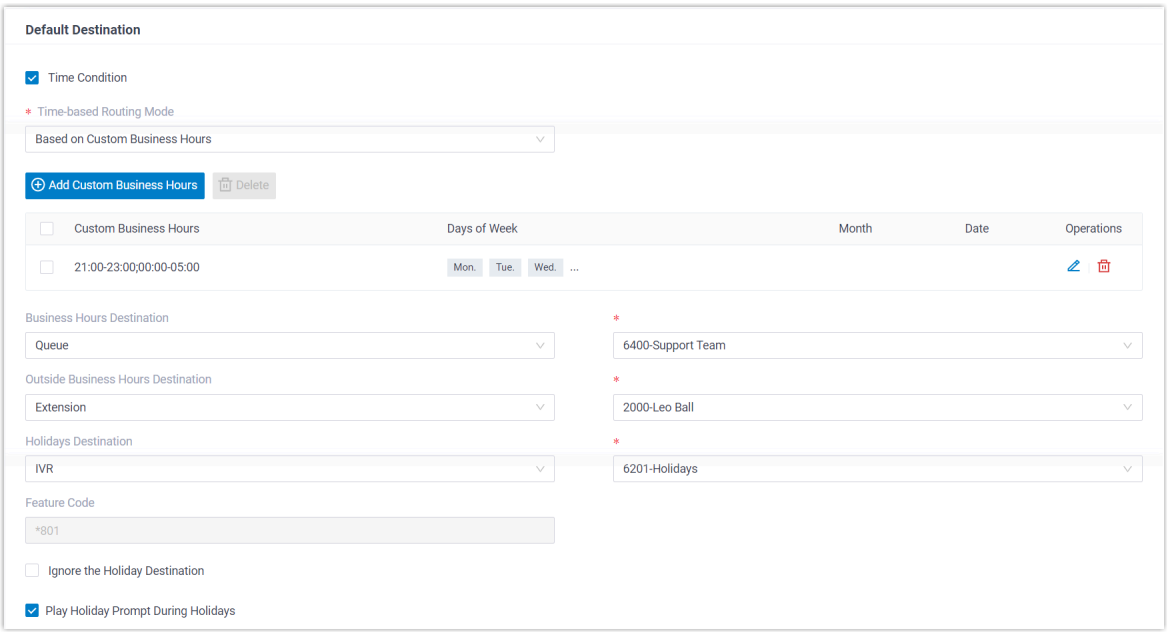
Procedure

1. Log in to PBX web 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 based on the system's default time zone.
      i. Click **Add Custom Business Hours**.

ii. In the **Custom Business Hours** section, click **Add** to add business hours.

In this scenario, add two business hours, 21:00 - 23:00 and 00:00 - 05:00.

iii. In the **Date Settings** section, select working days.

In this scenario, select **Days of Week** and select days from Monday to Friday.

iv. Click **Confirm**.

d. Configure the following destinations based on the time.

- **Business Hours Destination**: Select the destination for inbound calls during business hours set above.

  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**, and select an extension.
- **Holidays Destination**: Select the destination for inbound calls during holidays configured in the system's default time zone.

  In this scenario, select **IVR**, and select the IVR for holidays.

e. Select the checkbox of **Play Holiday Prompt During Holidays**.

In this scenario, the system will play the prompt "office_holiday" before routing inbound calls to the holiday destination.

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.
- Feature code ***801** is generated for the inbound route. The authorized user can dial *801 to override time condition of the inbound route. For more information, see Override Time Condition for Inbound Calls.

Related information

Route Inbound Calls based on 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 provides a configuration example on how to configure inbound route to control inbound calls for individual employees who have their own work schedules, based on the system's default time zone.

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.

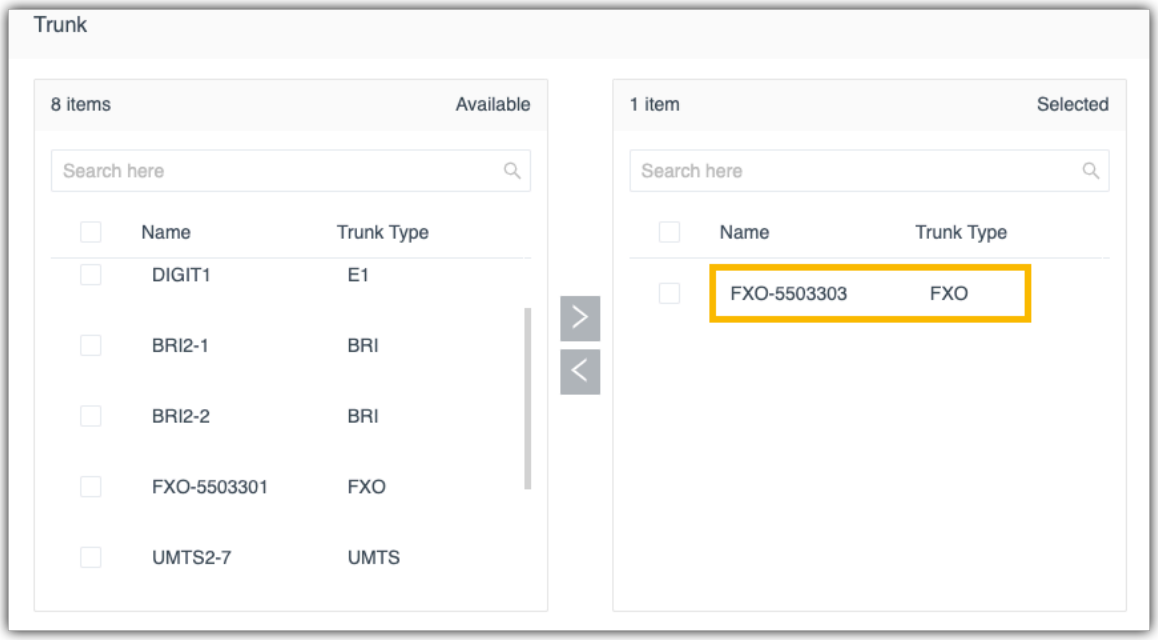
  For more information about IVR, see Set up an IVR.
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always directed to your desired destination.

  How to configure inbound route based on DID numbers, see Route Inbound Calls based on DID Numbers.

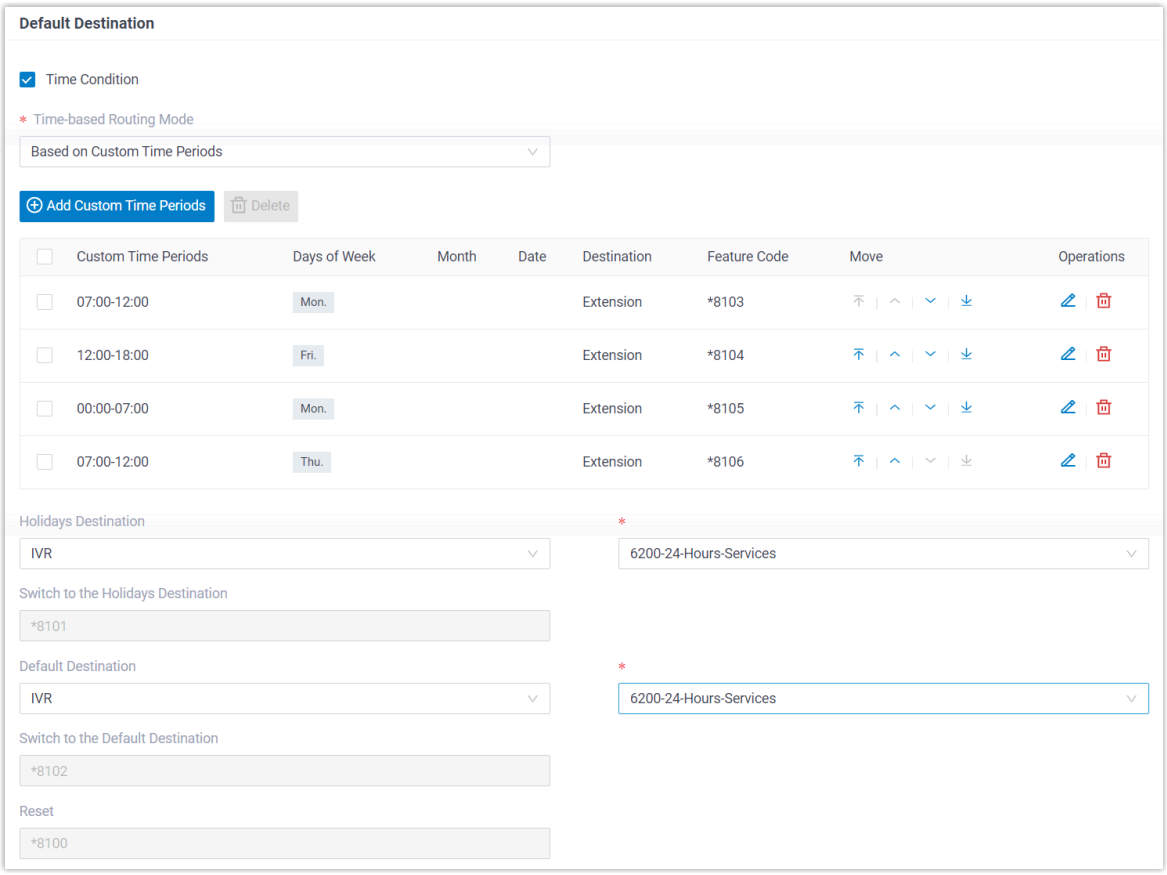
Procedure

1. Log in to PBX web 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 based on the system's default time zone.
    i. Click **Add Custom Time Periods**.
    ii. In the pop-up window, click **Add** to add time periods, set relevant destinations, and select days of week.
    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

Start Time	End Time	Days of Week	Destination
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 **Holidays 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.

5. Click **Save** and **Apply**.

Result

- When external users make calls to 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 **Holidays Destination**.
- Feature codes are generated as follows.

> **Tip:**
> The authorized users can dial a specific feature code to override time condition and route inbound calls to corresponding destinations. For more information, see Override Time Condition for Inbound Calls.

  - One feature code for each time period.
  - A **Switch to the Holidays Destination** feature code that allows for switching destination of inbound calls to **Holidays**.
  - A **Reset** feature code that allows for removing any overrides currently set.
  - A **Switch to the Default Destination** feature code that allows for switching destination of inbound calls to the default destination.

Related information

Route Inbound Calls based on 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

Caller ID/DID Based Inbound Routes

Route Inbound Calls based on DID Numbers

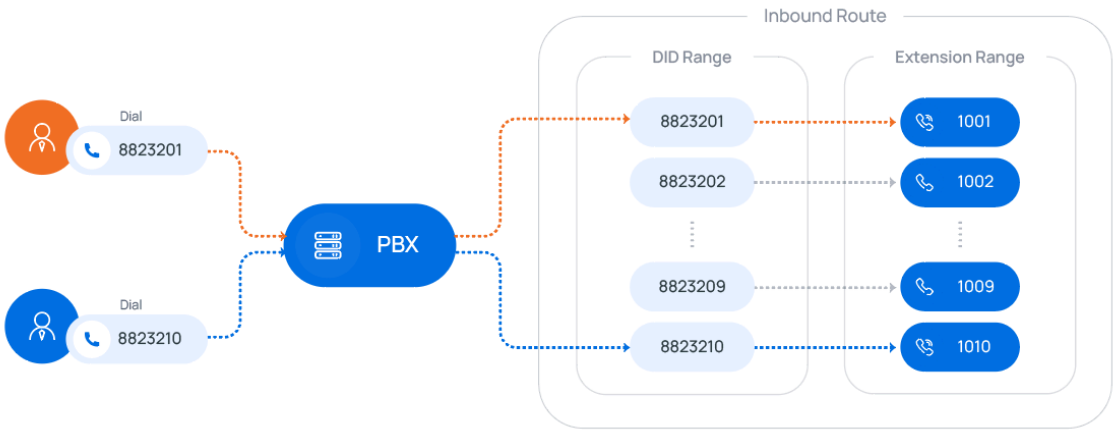
This topic gives configuration examples to describe how to route inbound calls based on the dialed numbers (also called DID numbers).

DID routing modes

Yeastar P-Series PBX System provides four DID matching modes to help you route inbound calls based on DID numbers.

- **Match DID Range to Extension Range**

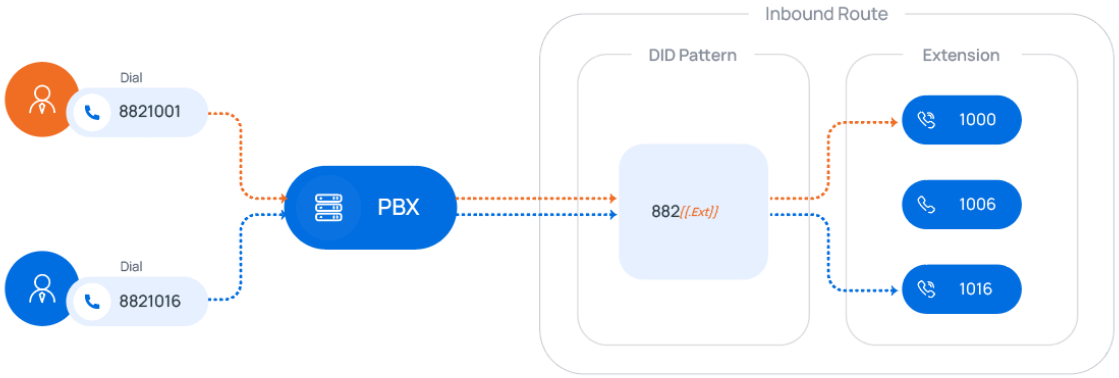
  Match DID Range and Extension Range in a one-to-one correspondence with sequential order.



  For more information, see the configuration example Route calls to extension users by matching DID range.

- **Match DID Pattern to Extensions**

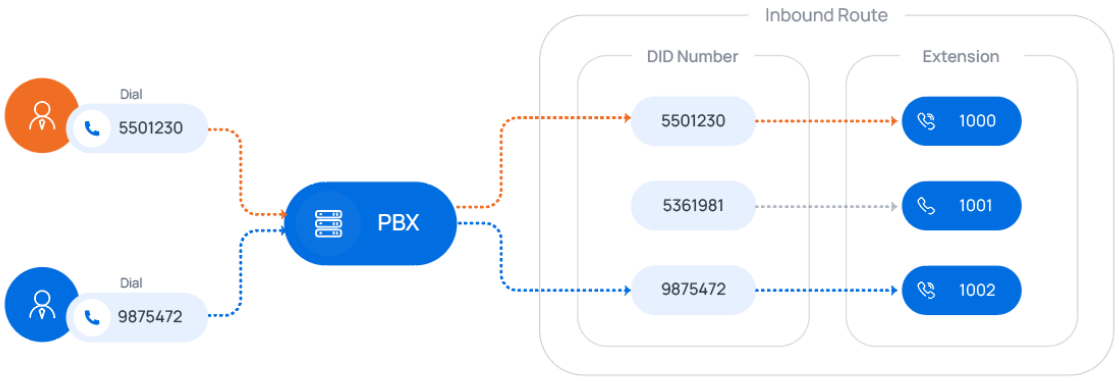
  Use the variable `{{.Ext}}` to match extension number in the DID pattern.



For more information, see the configuration example Route calls to extension users by matching DID patterns.

- **DID Number to Specific Extension**

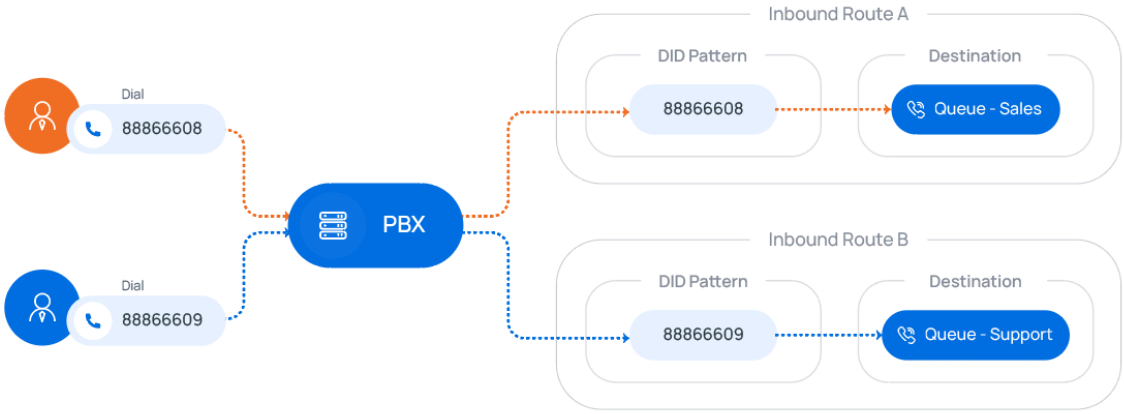
  The inbound calls that match the defined DID number(s) will be routed to the specified extension(s) in one-to-one correspondence.



For more information, see the configuration example Route calls to extension users by matching specific DID numbers.

- **DID Pattern**

  The inbound calls that match the defined DID number(s) or pattern(s) will be routed to a defined destination.



For more information, see the configuration example Route calls to different destinations by matching DID patterns.

Route calls to extension users by matching DID range

Scenario

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 24.

DID Number	Extension Number
8823201	1001
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.

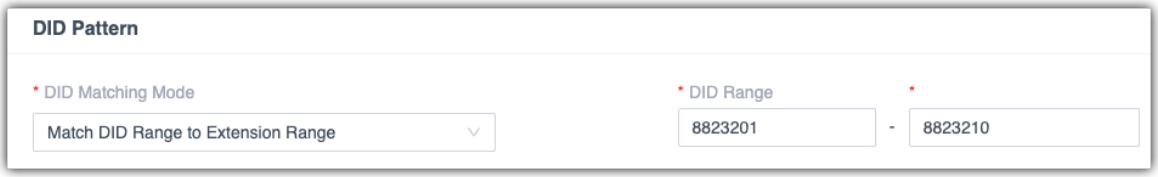
> **Note:**
> PSTN trunk and GSM trunk have no DID numbers, this solution is not suitable for these kinds of trunks.

Configuration example

According to this scenario, configure an inbound route based on the DID ranges as follows:

- **Name**: Enter a name to help you identify it.
- **Trunk**: Select the trunk that binds the DID numbers.
- **DID Pattern**:
  - **DID Matching Mode**: Select **Match DID Range to Extension Range**.
  - **DID Range**: Select or enter the start number and the end number of the DID range.

    In this scenario, enter *8823201* and *8823210*.



- **Caller ID Pattern**: Leave it blank, which means no limit on the inbound caller ID.
- **Default Destination**: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

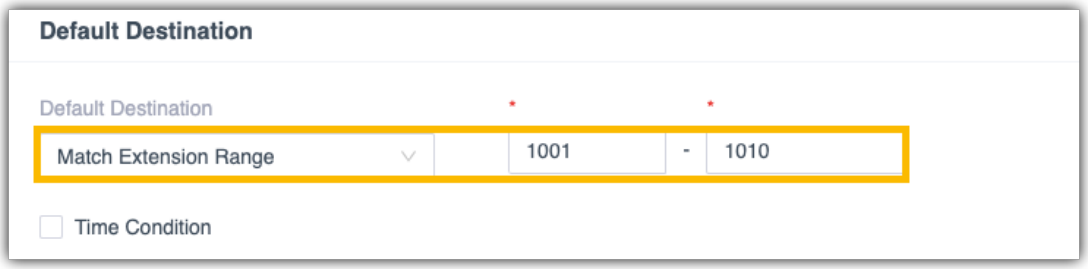
  In this scenario, route inbound calls to the default destination whenever the calls reach the system.

  - **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.



- **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 DID patterns

Scenario

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 25.

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

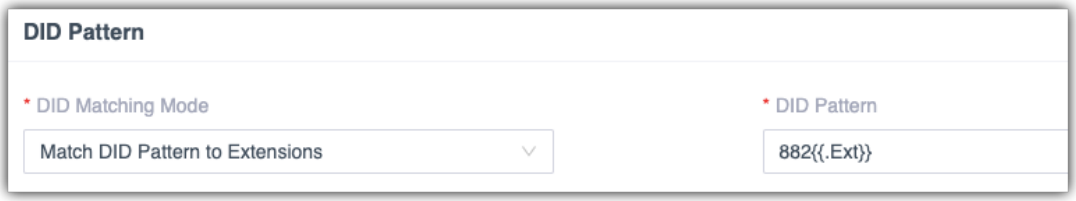
According to this scenario, configure an inbound route based on DID patterns as follows:

- **Name**: Enter a name to help you identify it.
- **Trunk**: Select the trunk that binds the DID numbers.

  In this scenario, select **siptrunk**.
- **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.

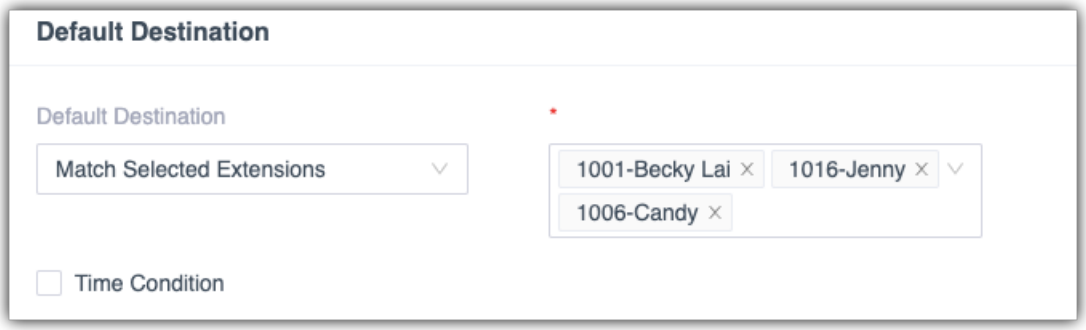


- **Caller ID Pattern**: Leave it blank, which means no limit of inbound caller ID.
- **Default Destination**: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  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.



- **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 extension users by matching specific DID numbers

Scenario

Company ABC purchases a SIP trunk, and gets 3 DID numbers as follows.

- 5501230, 5361981, 9875472

The company wants to redirect inbound calls to specific extensions based on the provided DID numbers as follows:

Table 26.

DID Number	Extension Number
5501230	1000
5361981	1001
9875472	1002

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.

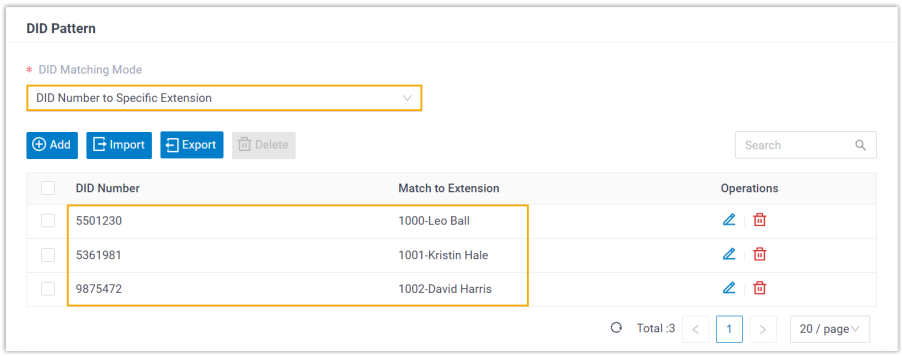
Configuration example

According to this scenario, configure an inbound route based on the specific DID numbers as follows:

- **Name**: Enter a name to help you identify it.
- **Trunk**: Select the trunk that binds the DID numbers.
- **DID Pattern**:
  - **DID Matching Mode**: Select **DID Number to Specific Extension**.
  - **DID Number**: Click **Add** and set up the DID number matching rules.

> **Tip:**
> You can also click **Export** to export the DID number matching rule to a CSV file first, use the file as a template to add DID number matching rules in bulk, then import the file into the inbound route. Refer to DID Number to Specific Extension Parameters to edit the parameters in the CSV file.

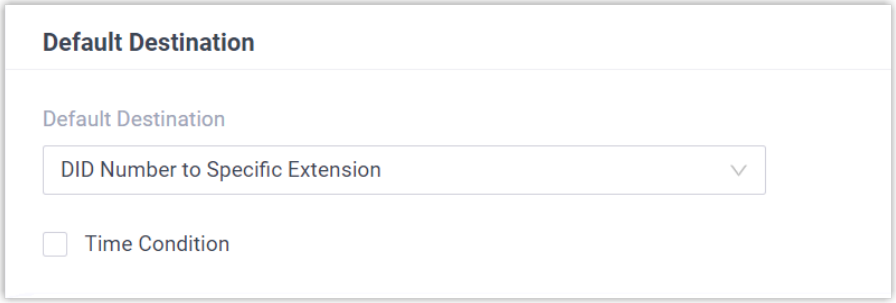
In this example, the configuration is as follows:



- **Caller ID Pattern**: Leave it blank, which means no limit on the inbound caller ID.
- **Default Destination**: Decide whether to route the inbound calls to different destinations based on time and configure the destinations.

  In this example, the configuration is as follows:

  - **Default Destination**: Select **DID Number to Specific Extension**.
  - **Time Condition**: Unselected.



- **Fax Detection**: Leave the settings as default.

Result

When an external user dials a number that equals to the DID number, the user can reach a specific extension user directly.

For example, if the external user dials 9875472, the call goes to the extension 1002 directly.

Route calls to different destinations 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.

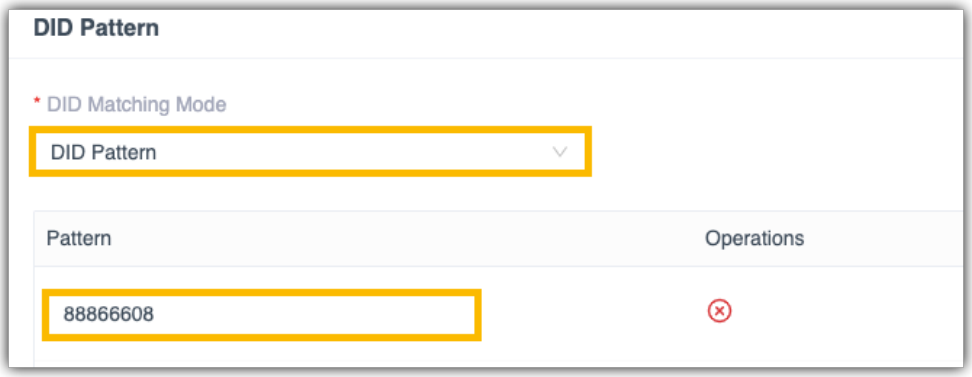
Configuration example

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.
- **Trunk**: Select the trunk that binds the DID numbers.
- **DID Pattern**:
  - **DID Matching Mode**: Select **DID Pattern**.
  - **DID Patterns**: Click **Add** and enter a DID pattern or a DID number.

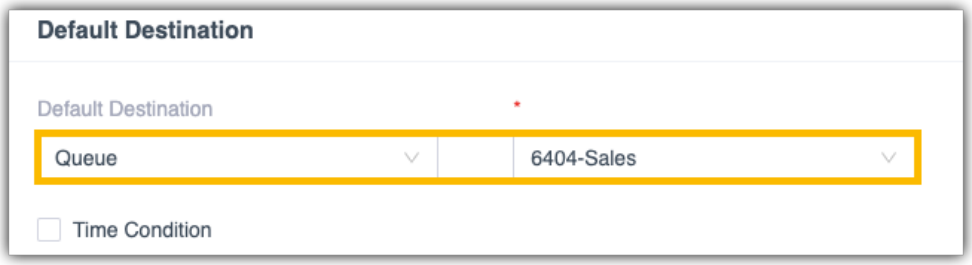
    In this scenario, enter *88866608*.



- **Caller ID Pattern**: Leave it blank, which means no limit of inbound caller ID.
- **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.

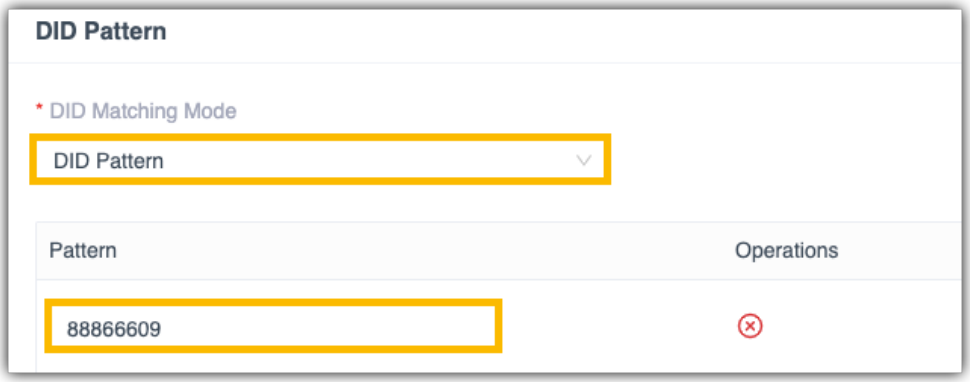


- **Fax Detection**: Leave the settings as default.

Inbound Route for support team

- **Name**: Enter a name to help you identify it.
- **Trunk**: Select the trunk that binds the DID numbers.
- **DID Pattern**:
  - **DID Matching Mode**: Select **DID Pattern**.
  - **DID Patterns**: Click **Add** and enter a DID pattern or a DID number.

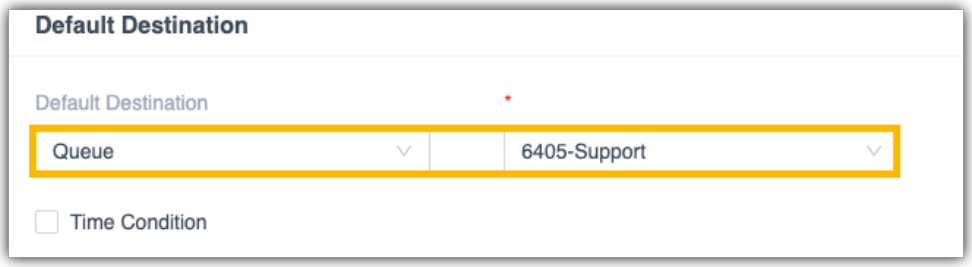
    In this scenario, enter *88866609*.



- **Caller ID Pattern**: Leave it blank, which means no limit of inbound caller ID.
- **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.



- **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 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	• 0591 • 0592 • 0593 • 0594 • 0595 • 0596 • 0597 • 0598 • 0599
Team-B	Guangdong	• 0662 • 0663 • 0668 • 0660

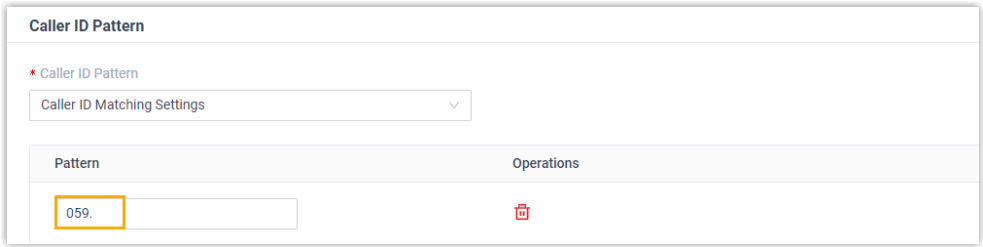
Configuration Example

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.

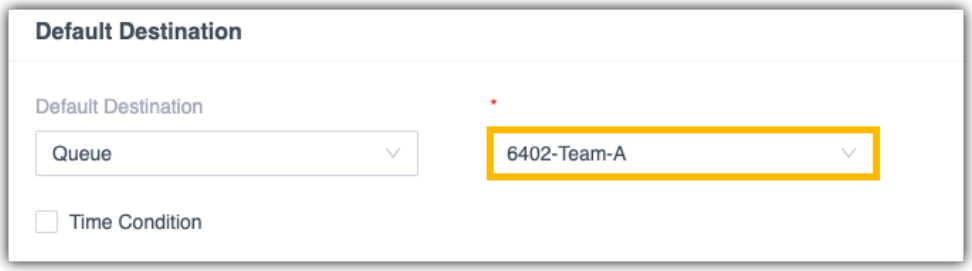
  In this scenario, enter `059.`, which matches all inbound caller IDs that start with digit 059. For more information of Caller ID pattern, see DID Pattern and Caller ID Pattern.



- **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.

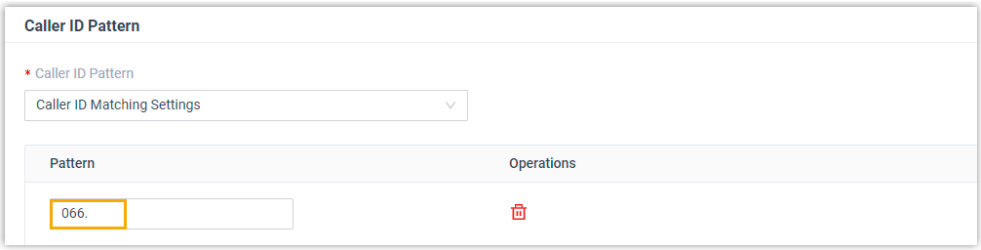


- **Fax Detection**: Leave the settings as default.

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.

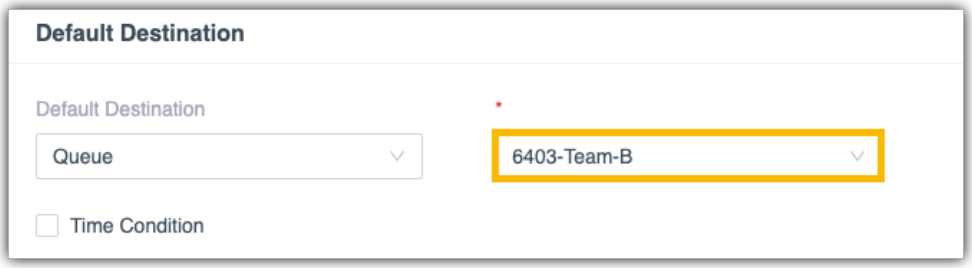


- **Trunk**: Select the trunk that users will call in.

  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.



- **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 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 Add and 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.

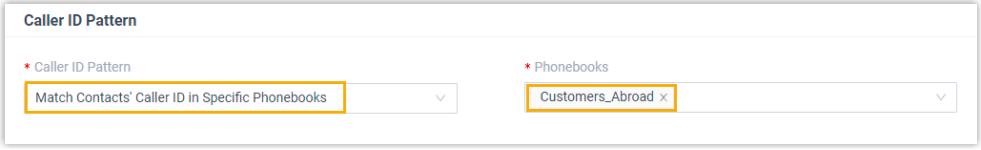
Team	Phonebook
Sales Team (Queue 6401)	Customers_Abroad
Support Team (Queue 6402)	Customers_China

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

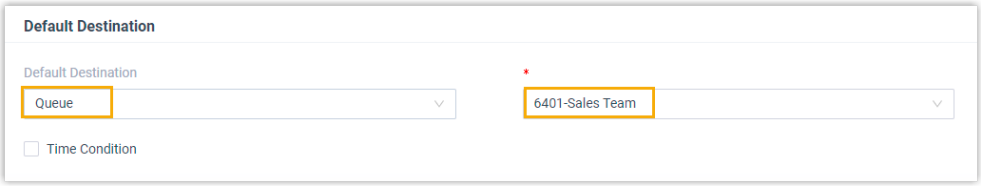
- **Name**: Enter a name to help you identify it.
- **DID Pattern**: Leave it blank, which means no limit of DID numbers.
- **Caller ID Pattern**: Select **Match Contacts' Caller ID in Specific Phonebooks** and select the phonebook **Customers_Abroad**.



- **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.

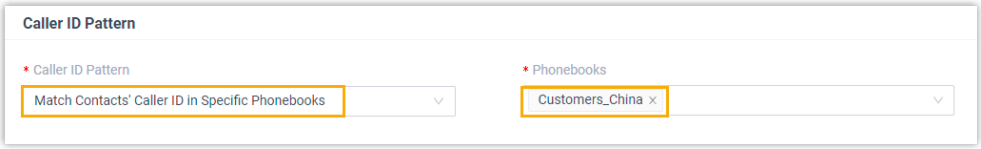
  - **Default Destination**: Select the destination to **Queue** and select the Sales Team.
  - **Time Condition**: Unselected.



- **Fax Detection**: Leave the settings as default.

Inbound Route for Support Team

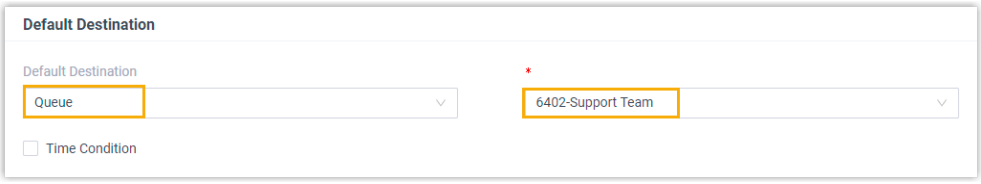
- **Name**: Enter a name to help you identify it.
- **DID Pattern**: Leave it blank, which means no limit of DID numbers.
- **Caller ID Pattern**: Select **Match Contacts' Caller ID in Specific Phonebooks** and select the phonebook **Customers_China**.



- **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.



- **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 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 web 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 web 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 web 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 web portal, go to **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 web portal, go to **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.

Related information

Import and Export -FAQ

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. **Note:** Range of numbers can be specified with a dash, example `[136-8]` matches the numbers 1, 3, 6, 7, or 8.
`.`	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.	• 05910 • 0591012345	• 0591 • 0592229929
+[13-5]XZN!	• +4022 • +1136282882	• +0136282882 • +1106282882
0591ZXXXX	• 059123456 • 059133456	• 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 web 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, extension groups, or organizations from **Available** box to **Selected** box.

> **Note:**

> - Organizations are displayed only when you enable the **Organization Management** feature.
> - By default, when you select an organization, its associated sub-organizations are selected. Be careful when selecting organizations.

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 Business Hours Configured for the Time Zone**: Set up whether to allow this route in the following time separately:
     - **Business Hours**: Business Hours specified for the specific time zone.
     - **Holidays**: Holidays specified for the specific time zone.
     - **Outside Business Hours**: The time periods that are not defined as Business Hours or Holidays in the specific time zone.
   - **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 based on the system's default time zone.
     - **Holidays**: Holidays specified for the system's default time zone in the system.
     - **Outside Business Hours**: The time periods that are not defined as Business Hours or Holidays for the system's default time zone.
   - **Based on Custom Time Periods**: Set up multiple time periods for this route based on the system's default time zone. You can also specify whether to allow this route in the Holidays configured for the default time zone.
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

To prevent the abuse of communication resources, you can restrict outbound calls by setting password for outbound routes to require callers to enter a PIN code before dialing out.

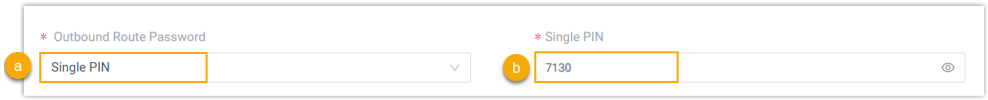
Only when a valid PIN code is entered can the call be sent out through the outbound route. This topic describes how to configure either a single PIN code or a list of PIN codes for an outbound route.

Restrict outbound calls by a single PIN code

To allow only specific employees or departments to make outbound calls via a specific outbound route, you can set a unique PIN code for the route. In this way, only users with the correct PIN code are able to use the outbound route.

Procedure

1. Log in to PBX web portal, go to **Call Control > Outbound Route**.
2. Click beside the desired outbound route.
3. Scroll down to the **Trunk** section, set up a password for the outbound route.



   a. In the **Outbound Route Password** drop-down list, select **Single PIN**.
   b. In the **Single PIN** field, set a PIN code.

> **Note:**
> - Only allows numeric value.
> - The length of the PIN code is limited from 3 to 15.

4. Click **Save** and **Apply**.

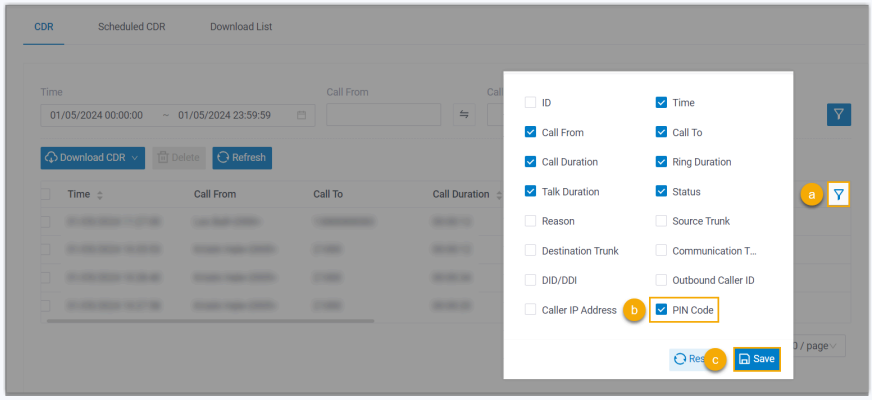
Result

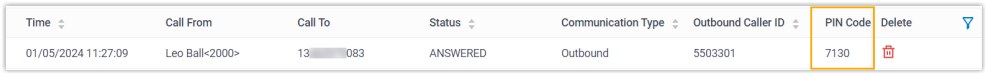
- Users need to enter the PIN code when making outbound calls via the outbound route.

> **Note:**
> If a user enters a wrong PIN code for three times, the call will be hung up automatically.

- In the CDR, you can see the PIN code used in the outbound calls made via the outbound route (Path: **Reports and Recordings > CDR**).

Note:
Make sure that you have set the CDR to display the **PIN Code** column.





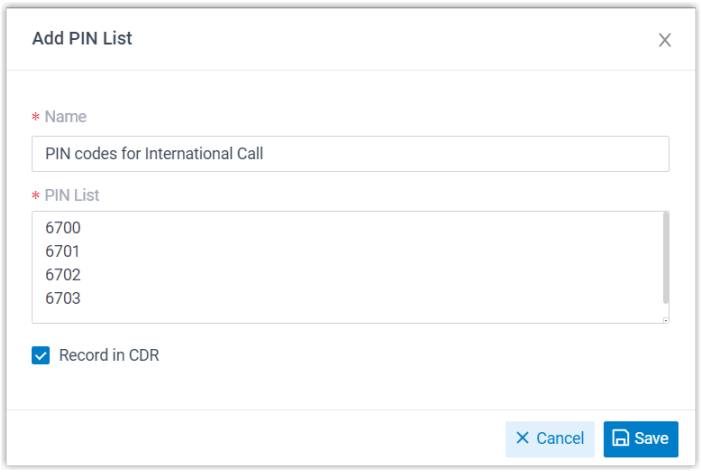
For more information about how extension users can use the PIN code for making outbound calls, see the usage example.

Restrict outbound calls by multiple PIN codes

In the scenario where a number of users share the same extension number across different endpoints to make outbound calls, it is difficult to track the calling activities of these users individually. In this case, you can set up a list of passwords for an outbound route and allocate them to users, so that users can make outbound calls via the outbound route, while you can track and distinguish their calls using the PIN codes.

Step 1. Add a PIN List

1. Log in to PBX web portal, go to **Call Features > PIN List**, click **Add**.
2. In the pop-up window, configure the following settings:

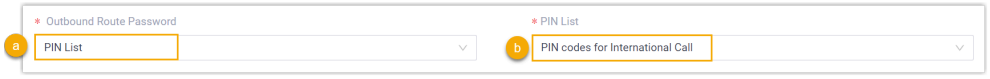


Setting	Description
Name	Enter a name to help you identify it.
PIN List	Enter PIN codes. **Note:** • Press the **Enter** key to separate multiple PIN codes. • Only allows numeric value. • The length of each PIN code is limited from 3 to 15.
Record in CDR	Enable this option. The system will record the PIN code in CDR when the PIN code has been used.

3. Click **Save**.

Step 2. Associate the PIN List with an outbound route

1. On PBX web portal, go to **Call Control > Outbound Route**.
2. Click beside the desired outbound route.
3. Scroll down to the **Trunk** section, set up passwords for the outbound route.



   a. In the **Outbound Route Password** drop-down list, select **PIN List**.

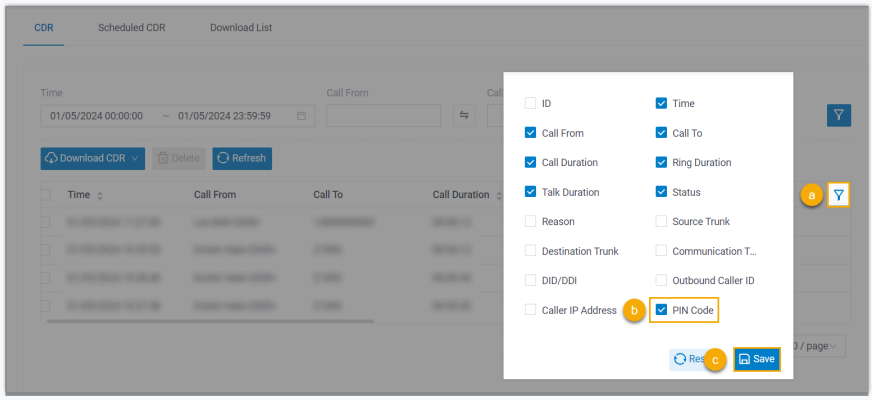
b. In the **PIN List** drop-down list, select an existing PIN list.

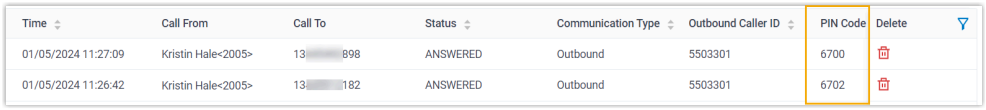
4. Click **Save** and **Apply**.

Result

- Users need to enter any PIN codes contained in the selected PIN list when making outbound calls via the outbound route.
- In the CDR, you can easily distinguish the users who made outbound calls via different PIN codes allocated to different users, even if they use the same extension to dial out (Path: **Reports and Recordings > CDR**).

Note:
Make sure that you have set the CDR to display the **PIN Code** column.





Time	Call From	Call To	Status	Communication Type	Outbound Caller ID	PIN Code	Delete
01/05/2024 11:27:09	Kristin Hale<2005>	13[redacted]898	ANSWERED	Outbound	5503301	6700	
01/05/2024 11:26:42	Kristin Hale<2005>	13[redacted]182	ANSWERED	Outbound	5503301	6702	

For more information about how extension users can use the PIN code for making outbound calls, see the usage example.

Usage example

We provide an example to help you understand the workflow of making outbound calls via a restricted outbound route using a PIN code.

1. An extension user 2000 dials an external number.

2. After hearing a voice prompt "Please enter your password followed by the pound key", the user enters a PIN code. When done, press # key.
    - If the PIN code is correct, the call will be successfully sent out through the outbound route.
    - If the PIN code is incorrect, the user will hear a voice prompt "password incorrect" and will be asked to enter a password again. If the user enters wrong password for three times, the call will be hung up automatically.

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 web portal, go to **Call Control > Outbound Route**.
2. Click the buttons ⤒ ^ v ⤓ 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 web 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 web 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 **OK** 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 web portal, go to **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 web portal, go to **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.

Related information

Import and Export -FAQ

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.

Pattern	Description
`N`	Match any digit from 2 - 9.
`[###]`	Match any digit in the bracket. **Example**: `[123]` matches the numbers 1, 2, or 3. **Note:** Range of numbers can be specified with a dash, example `[136-8]` matches the numbers 1, 3, 6, 7, or 8.
`.`	Match one or more numbers. **Example**: `9011.` matches any numbers starting with digits 9011 (excluding 9011 itself).
`!`	Wildcard *!* has different meanings for SIP extensions and FXS extensions. • 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.

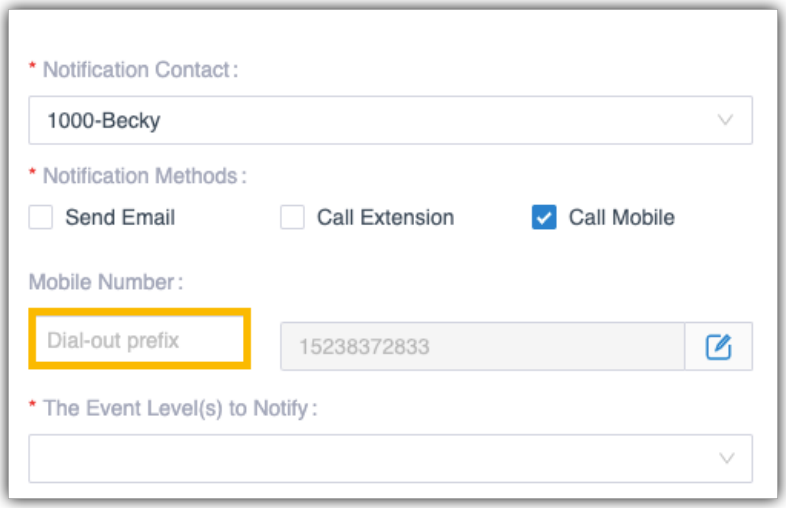
Prefix and Dial Pattern

A prefix is the digit that will be removed from the dialed number before sending to the carrier.

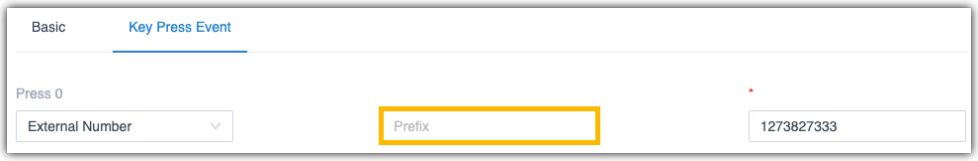
Scenarios

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

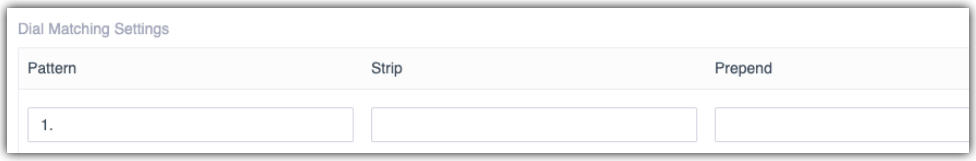
You need to configure prefix according to the dial pattern settings on your out-bound route. If the prefix is not configured correctly, the PBX cannot call to the external number successfully.

- **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.

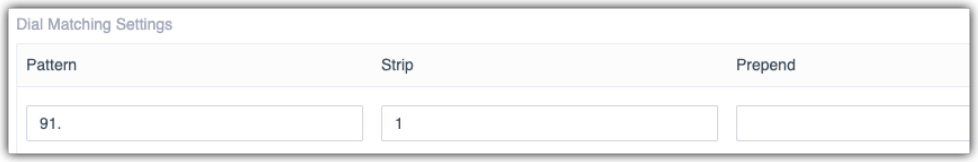


- **Add prefix before a number**

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.



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.

AutoCLIP Route

AutoCLIP Route Overview

Yeastar provides AutoCLIP (Auto Calling Line Identification Presentation) feature, which is an intelligent call matching feature. You can configure AutoCLIP to route customer inbound calls to original extensions, which will promote your customer satisfaction and help your business be more efficient, and professional.

Restriction

The AutoCLIP list supports up to 100,000 records.

Scenarios

Assume that sales representatives in your company often make outbound calls to customers for promotion. More or less, some customers may miss the calls. When customers call back, the calls are routed to the receptionist or business auto attendant. Neither receptionist/business auto attendant nor the customers know who placed the call.

With AutoCLIP feature, the PBX can redirect the calls to the original extension users who placed the calls when customers call back. Using this feature, you can avoid the embarrassing situation that customers cannot find the person when they call back to the PBX.

How does the PBX redirect calls to original extensions?

1. When extension users make outbound calls, the PBX automatically stores the records to AutoCLIP list, including extension number, called number, and the used trunk.
2. When customers call back to the PBX system, PBX will compare the phone numbers with the records in the AutoCLIP list.
    - If there're matched records in AutoCLIP list, the calls will be routed to corresponding extensions, bypassing any receptionists or business auto attendant.
    - If there're not matched records in AutoCLIP list, the calls will be routed to the destination specified in inbound routes.

Route Inbound Calls to Original Extensions via AutoCLIP Route

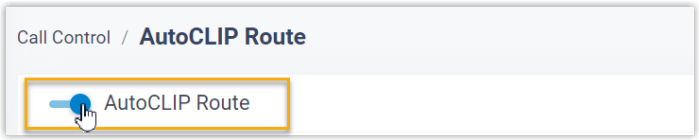
With AutoCLIP feature, Yeastar P-Series PBX System can route inbound calls from customers to original extension users who placed the calls. This intelligent call matching feature can greatly improve work efficiency and customer satisfaction. This topic describes how to set up the AutoCLIP route.

Prerequisites

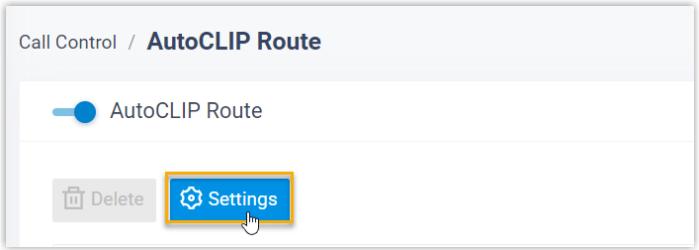
Make sure the desired trunk purchased from trunk provider has the Caller ID feature, or the PBX can not distinguish the Caller ID and implement AutoCLIP.

Procedure

1. Log in to PBX web portal, go to **Call Control > AutoCLIP Route**.
2. On the top of the page, enable the **AutoCLIP Route** feature.



3. Click **Settings** to set up rules for AutoCLIP route.



4. Configure the AutoCLIP settings according to your needs.

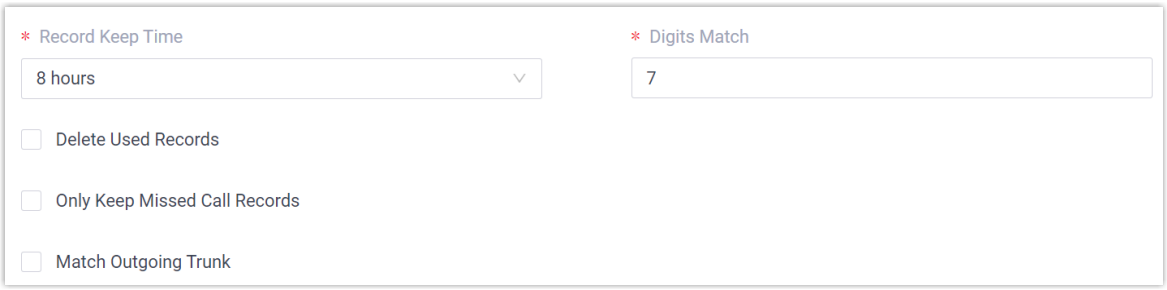
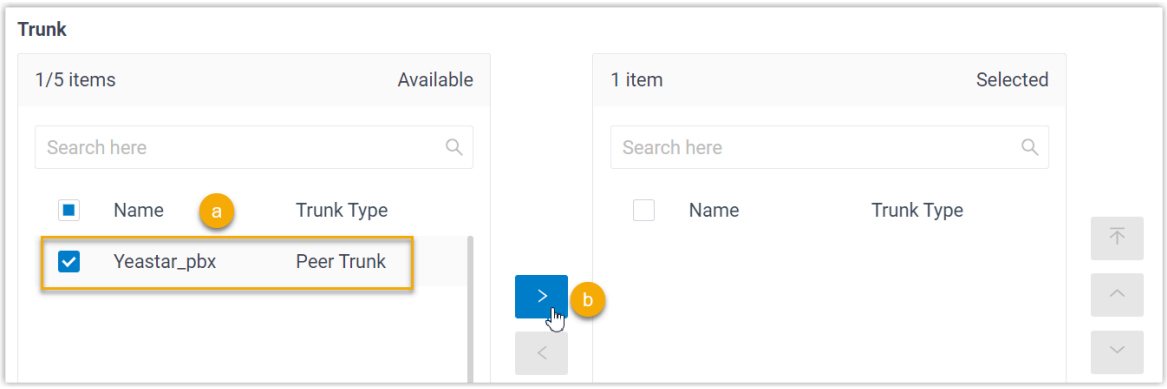


Table 31.

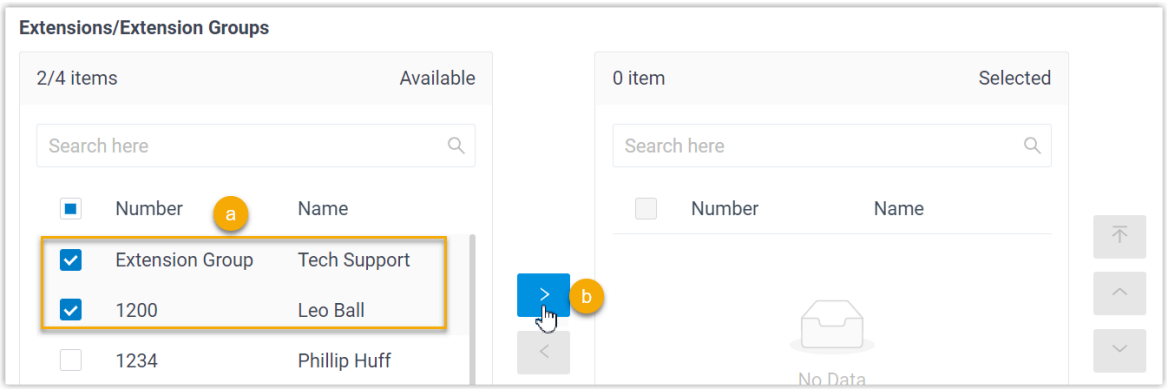
Setting	Description
Record Keep Time	Set how long records can be kept in AutoCLIP list. If keep time of a record exceeds the value, PBX will automatically delete the record. **Tip:** You can check the expiration time in the AutoCLIP record list directly.
Digits Match	Define how many digits from the last digit of the incoming Call ID will be used to match the AutoCLIP list. **Note:** If the number has fewer digits than the value defined here, it will be matched in full length.
Delete Used Records	If enabled, when an AutoCLIP record is matched, it will be deleted from the record list automatically after the original extension has answered the redirected customer call.
Only Keep Missed Call Records	If enabled, only when the outbound call is not answered will it be recorded in the AutoCLIP list. **Note:** All calls made through PSTN lines will be recorded in the AutoCLIP list, regardless of the setting.
Match Outgoing Trunk	If enabled, the PBX will route the call to the original extension only when the trunk number dialed by external users matches the trunk that was used to place the call earlier.

5. In the **Trunk** section, select which trunks will use AutoCLIP Route.



a. Select the desired trunk(s).
b. Add the desired trunk(s) from **Available** box to **Selected** box.

6. In the **Extensions/Extension Groups** section, select which extensions can use Auto-CLIP Route.



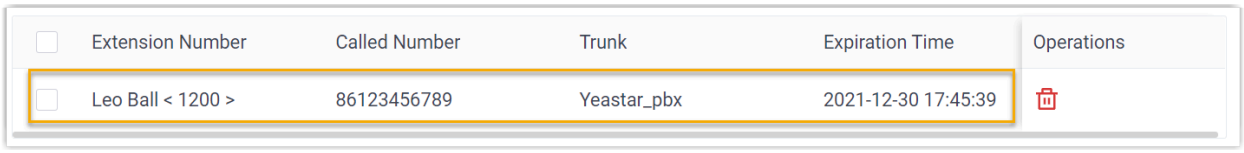
a. Select the desired extension(s)/extension group(s).
b. Add the extension(s)/extension group(s) from **Available** box to **Selected** box.

7. Click **Save**.

Result

When extension user uses the trunk with AutoCLIP feature to call external users out, PBX generates AutoCLIP records, including extension details, the numbers dialed and the used trunk. You can check the AutoCLIP record on **Call Control > AutoCLIP Route**.

Note:
If more than one extension user make outbound calls to the same external user, PBX will only match the last extension user that placed the call when the external user calls back.



Delete AutoCLIP Records

This topic describes how to delete AutoCLIP records.

Delete a record

1. Log in to PBX web portal, go to **Call Control > AutoCLIP Route**.
2. Click beside the record that you want to delete.
3. In the pop-up dialog box, click **OK**.

Bulk delete records

1. Log in to PBX web portal, go to **Call Control > AutoCLIP Route**.
2. Select the checkboxes of the desired records, and click **Delete**.
3. In the pop-up dialog box, click **OK**.

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:**
> Only P550, P560, and P570 support E1/T1/J1 trunk.

> **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 web portal, go to **Extension and Trunk > Trunk**, edit the desired trunk.
2. Click **DIDs/DDIs** tab.
3. Click **Add**, then add DID number(s) according to your need.
   - To add a single DID number, do as follows:
     a. In the **Create Method** drop-down list, select **Single DID**.
     b. 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.

       When the DID number is dialed, the name will be displayed on the called party's device.
   - To add a range of DID numbers, do as follows:
     a. In the **Create Method** drop-down list, select **DID Range**.
     b. Configure the following settings:
     - **DID Range**: Enter the start number and the end number of the DID range.

- **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

  When the DID number is dialed, the name will be displayed on the called party's device.

4. Click **Confirm**.
5. Click **Save** and **Apply**.

Delete DID numbers

1. Log in to PBX web portal, go to **Extension and Trunk > Trunk**, edit the desired trunk.
2. Click **DIDs/DDIs** tab.
3. On the **DIDs/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 DIDs/DDIs Numbers

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

Background information

The following types of trunks support DIDs/DDIs numbers:

- SIP
- BRI
- E1/T1/J1

Note:

- FXO trunk and GSM/3G/4G LTE trunk have no DID numbers.
- Only P550, P560, and P570 support E1/T1/J1 trunk.

Export all DIDs/DDIs numbers

You can export all DIDs/DDIs numbers to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX web 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 web 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.

Related information

Import and Export -FAQ

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 for Outbound Calls.

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 web 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**: 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**: 0592XXXXXXX
- **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 web 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 web 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.

Related information

Import and Export -FAQ

Customize Outbound Caller IDs for Outbound Calls

This topic describes different ways to customize outbound caller IDs for standard outbound calls, 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 web 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 web 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**
   - **Default DOD Label**
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**
   - **Default DOD Label**
6. Click **Save** and **Apply**.

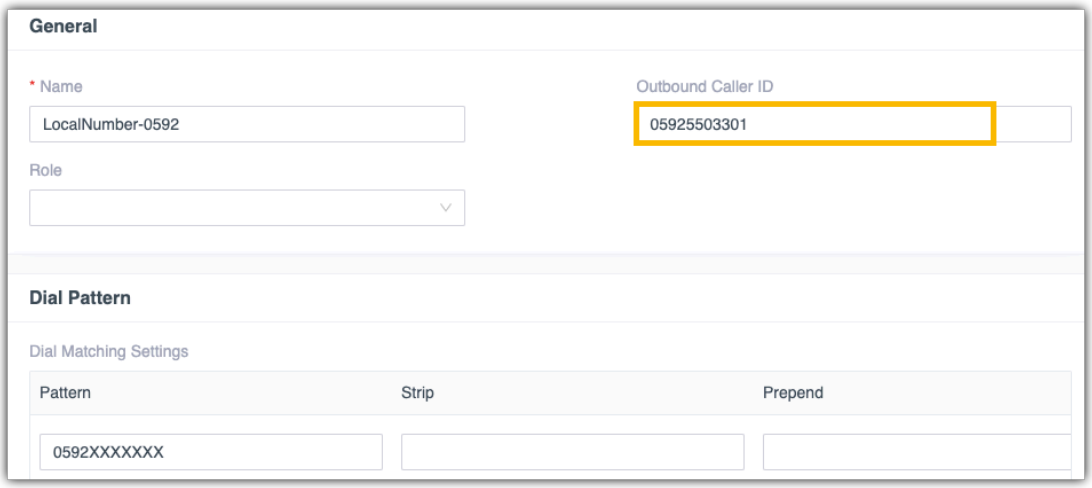
When extension users make outbound calls through the configured trunk, the associated outbound caller IDs will be displayed on the called party's device.

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 web 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.



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 web 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 web 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**.

Related information

Import and Export -FAQ

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 phones. 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 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.

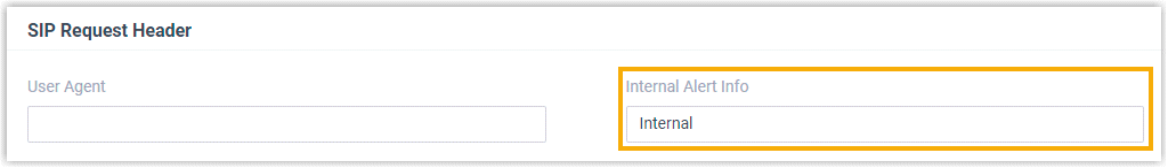
2. Set a specific ringtone for a phone.

Set alert info for internal calls on the PBX

1. Log in to PBX web 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`.



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 the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

Procedure

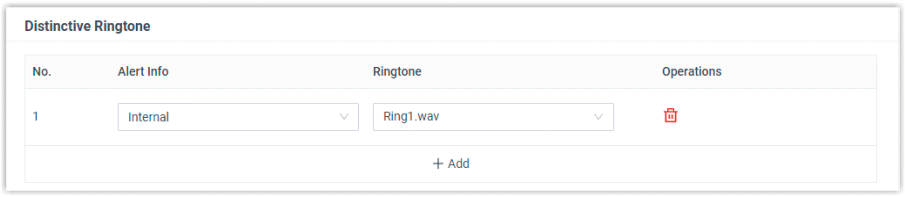
1. Set a specific internal ringtone for a user's phone.

a. Log in to PBX web 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.



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

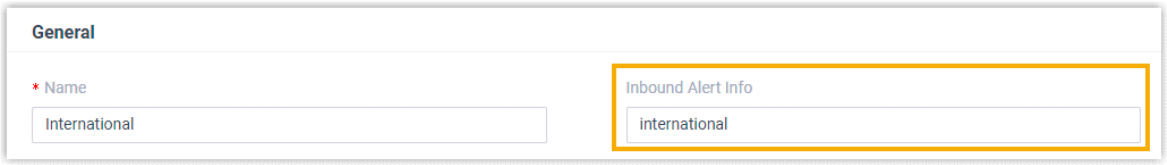
1. Set alert info for external calls on the PBX.
2. Set a specific ringtone for a phone.

Set alert info for external calls on the PBX

1. Log in to PBX web 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.

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 phones, 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 the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

Procedure

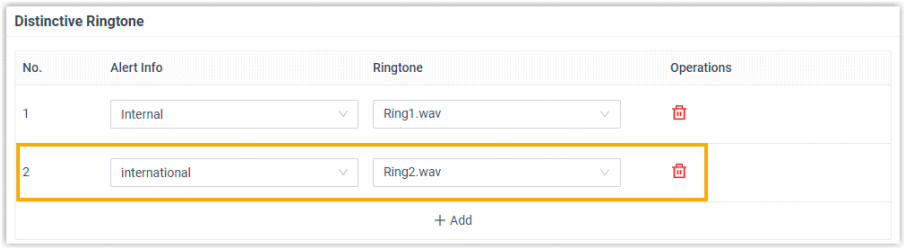
1. Set distinctive ringtones for a user.

a. Log in to PBX web 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.



f. Click **Save**.

2. Reprovision 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

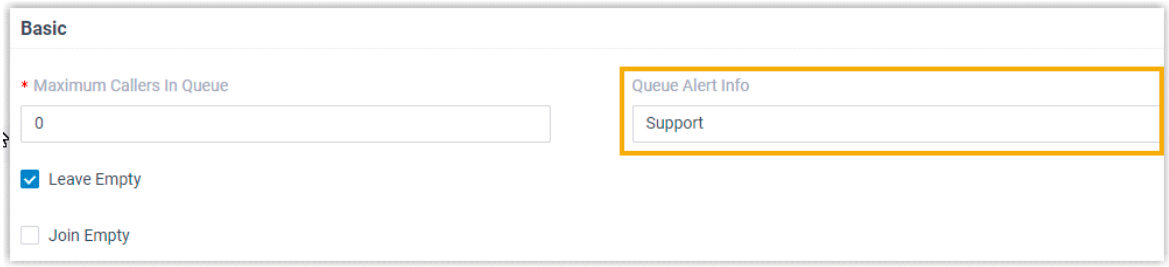
1. Set an alert info for queue calls on the PBX.
2. Set a specific ring tone for a phone.

Set an alert info for queue calls on the PBX

1. Log in to PBX web 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`.



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 the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

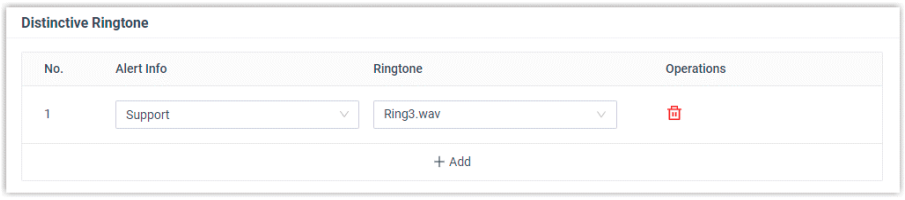
Procedure

1. Set a specific queue ring tone for an agent's phone.
    a. Log in to PBX web 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.

    f. Click **Save**.
2. Reprovision 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 ringtone *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

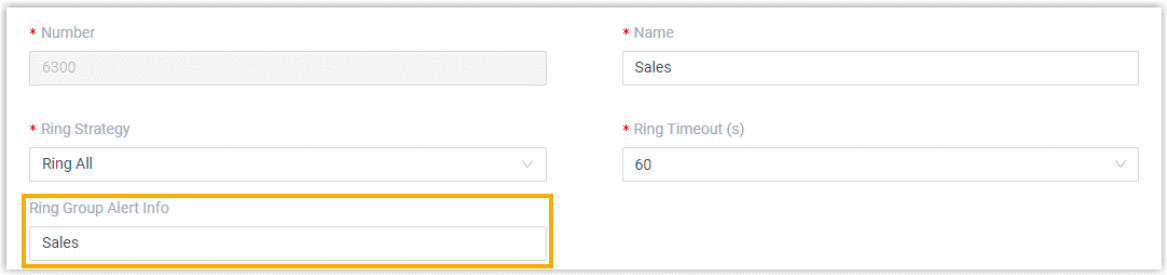
1. Set an alert info for ring group calls on the PBX.
2. Set a specific ringtone for a phone.

Set an alert info for ring group calls on the PBX

1. Log in to PBX web 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`.



Set a specific ringtone for a phone

For ring group members who want to play a specific ringtone for ring group calls on their phones, 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 the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)

- Auto Provision IP Phones Remotely (RPS Method)

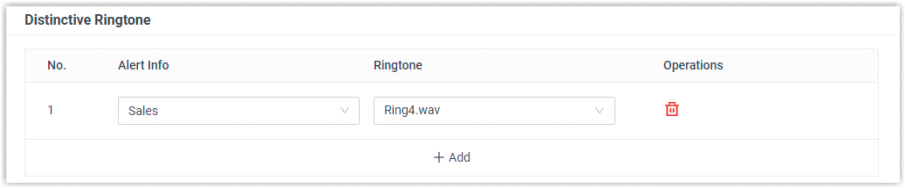
Procedure

1. Set a specific ringtone for a ring group member.
   a. Log in to PBX web 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.

   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

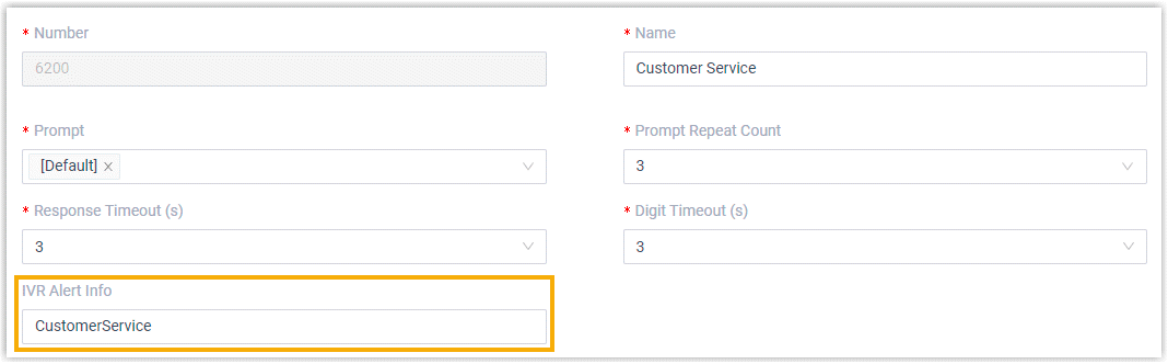
1. Set an alert info for IVR calls on the PBX.
2. Set a specific ringtone for a phone.

Set an alert info for IVR calls on the PBX

1. Log in to PBX web 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`.



Set a specific ringtone for a phone

For users who want to play a specific ringtone for IVR calls on their phones, 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 the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

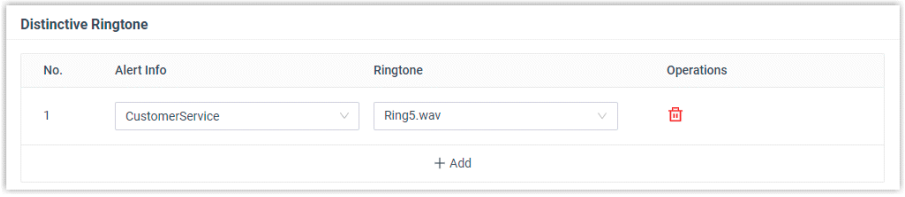
Procedure

1. Set a specific ringtone for a user.
   a. Log in to PBX web 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.

   f. Click **Save**.
2. Reprovision 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 32.

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
Sunmy	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 Sunmy dials 1256666 to reach the Support team and no Caller Name is sent from Sunmy, the caller ID name displayed is *Sunmy: 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*

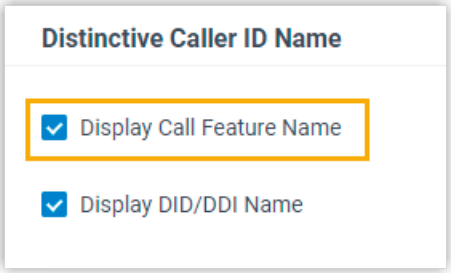
Enable or Disable Distinctive Caller ID Name

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.

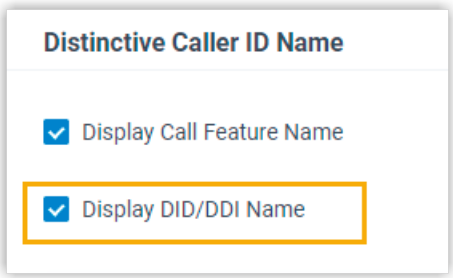
1. Log in to PBX web portal, go to **PBX Settings > > Preferences**.
2. In the **Distinctive Caller ID Name** section, configure the followings:
   - To display Queue names, Ring Group names, and IVR names, select the check-box of **Display Call Feature Name**.
   - To hide Queue names, Ring Group names, and IVR names, unselect the check-box of **Display Call Feature Name**.



3. Click **Save** and **Apply**.

Enable or disable the display of trunk DID/DDI name

1. Log in to PBX web 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**.



3. Click **Save** and **Apply**.

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 language**: Custom language for system prompts played in group voicemails or extension voicemails. Callers accessing the voicemail will hear prompts in the selected language.
- **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 web portal, go to **Call Features > Voicemail > Group Voicemail**.
2. Click **Add**.
3. Under **General** tab, complete the general settings:
   a. In the **Basic** section, configure the following settings.

Setting	Description
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

Setting	Description
	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.
Disallow Voicemail Messages	Optional. Enabling this option to restrict callers from leaving voicemail messages. The system will play voicemail greeting to the caller, and then hang up the call directly.
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.
Custom Prompt Language	Optional. Enable this option and set the language of voicemail prompts heard by callers when they access the group voicemail. **Note:** • The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**). • If the group voicemail has set up a custom greeting, the custom greeting will be played to callers instead. In this case, the language setting will be ignored.

b. 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.

c. In the **Group Voicemail Greeting** section, select a voicemail greeting.

You can also click **Greeting Management** to customize a greeting or mange your custom greetings.

4. Under **Voicemail Announcement** tab, set up call alerts for new voicemail messages in the group voicemail.

   > **Note:**
   > This feature is only supported on the group voicemail with the **Mode** set to **Shared by Members**.

5. 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 web portal, go to **Call Features > Voicemail > Group Voicemail**.
2. Click **Add**.
3. Under **General** tab, complete the general settings:
   a. In the **Basic** section, configure the following settings:

Setting	Description
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.

Setting	Description
	• **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.
Disallow Voicemail Messages	Optional. Enabling this option to restrict callers from leaving voicemail messages. The system will play voicemail greeting to the caller, and then hang up the call directly.
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.
Custom Prompt Language	Optional. Enable this option and set the language of voicemail prompts heard by callers when they access the group voicemail. **Note:** • The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**). • If the group voicemail has set up a custom greeting, the custom greeting will be played to callers instead. In this case, the language setting will be ignored.

b. 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.

c. In the **Group Voicemail Greeting** section, select a voicemail greeting.

You can also click **Greeting Management** to customize a greeting or mange your custom greetings.

4. Under **Voicemail Announcement** tab, set up call alerts for new voicemail messages in the group voicemail.

> **Note:**
> This feature is only supported on the group voicemail with the **Mode** set to **Shared by Members**.

5. 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

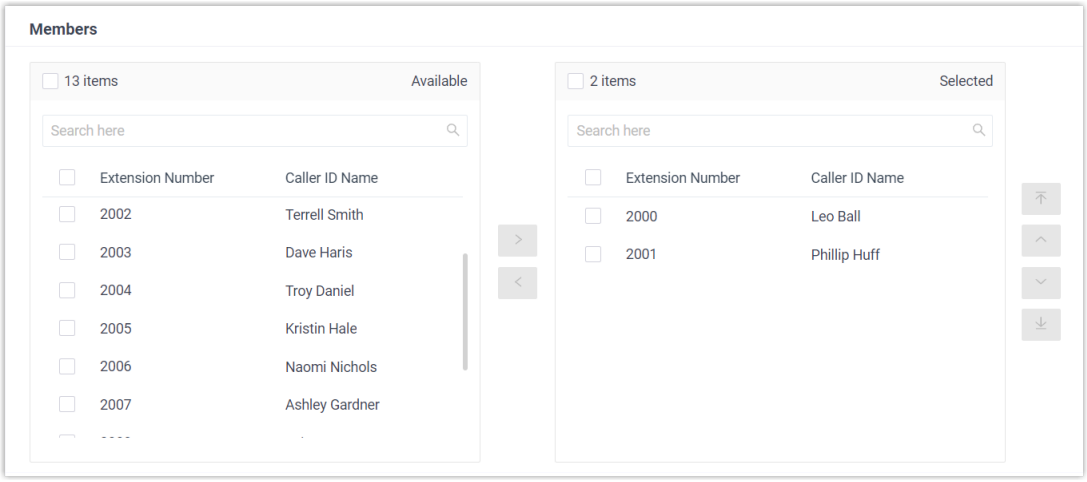
1. Log in to PBX web portal, go to **Call Features > Voicemail > Group Voicemail**.
2. Click **Add**.
3. Under **General** tab, complete the general settings:
   a. In the **Basic** section, configure the following settings:

Setting	Description
Type	Select **Custom**.

Setting	Description
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.
Group voicemail to Email	Optional. Enter the desired email addresses to receive group voicemails. **Note:** A maximum of 5 email addresses is supported; Use semicolons ; to separate multiple email addresses.
Voicemail PIN Authentication	Enable or disable voicemail PIN authentication.
Voicemail Access PIN	If enable voicemail PIN authentication, enter a desired access PIN number.
Disallow Voicemail Messages	Optional. Enabling this option to restrict callers from leaving voicemail messages. The system will play voicemail greeting to the caller, and then hang up the call directly.
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.
Custom Prompt Language	Optional. Enable this option and set the language of voicemail prompts heard by callers when they access the group voicemail. **Note:**

Setting	Description
	• The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**). • If the group voicemail has set up a custom greeting, the custom greeting will be played to callers instead. In this case, the language setting will be ignored.

b. In the **Members** section, select the desired extensions or extension groups from **Available** box to **Selected** box to receive group voicemails.



> **Note:**
> Group voicemails will be sent to the selected members and the specified email addresses if both are configured.

c. In the **Group Voicemail Greeting** section, select a voicemail greeting.

You can also click **Greeting Management** to customize a greeting or mange your custom greetings.

4. Under **Voicemail Announcement** tab, set up call alerts for new voicemail messages in the group voicemail.

> **Note:**
> This feature is only supported on the group voicemail with the **Mode** set to **Shared by Members**.

5. 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 Call Alerts for Group Voicemail

Yeastar P-Series PBX System allows you to configure call alerts for new group voicemail messages. When a new voicemail message is left, the system will call the specified phone numbers in a pre-defined priority order until all the voicemail messages are read or the specified call cycles are reached.

Scenario

A company has a team of on-call agents responsible for after-hours emergency. Instead of answering incoming calls, the company wants the calls to be routed to voicemail while the agents can be alerted as soon as possible. In this case, the company can configure an inbound route for such emergency calls, routing the calls to a dedicated group voicemail, and then set up call alerts to notify the agents whenever a new voicemail message is left.

Requirements and restrictions

Before you begin, read through the requirements and restrictions for the feature:

Requirements

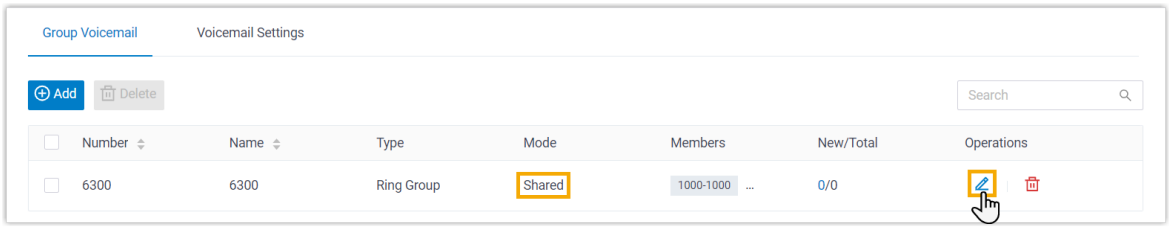
- **Version**: 37.13.0.25 or later
- **Plan**: Enterprise Plan or Ultimate Plan

Restrictions

- This feature is only available for the group voicemails that are **Shared by Members**.
- Allow calls to only **External Number** when there is a new voicemail message and only **5** external numbers are supported.

Procedure

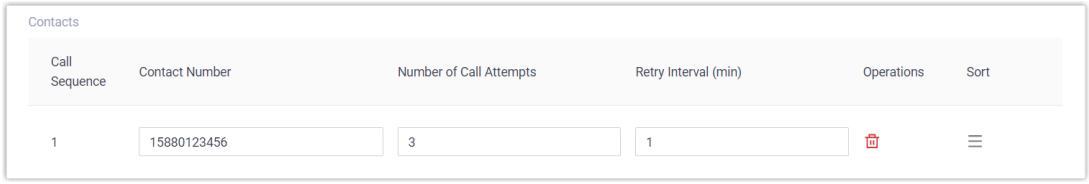
1. Log in to PBX web portal, go to **Call Features > Voicemail > Group Voicemail**, edit a group voicemail with the **Mode** displayed as **Shared**.



2. Click the **Voicemail Announcement** tab.
3. Turn on call notifications for new group voicemail messages, and set up the number and rule to call.
    a. Turn on the switch of **Voicemail Announcement**.
    b. In the **Max Number of Call Cycles** field, specify how many times you want to repeatedly call the contact list.

> **Note:**
> - The value you enter should not be greater than 30.
> - Notification calls will continue until the number of call cycle is reached or all voicemail messages have been read.

    c. In the **Contacts** section, click **Add** to configure the number to call and set up the rule.



- **Contact Number**: Enter an external number.

> **Note:**
> Notification calls to the number can be made via any matched outbound routes. Make sure that there are outbound routes that match the number, otherwise the notification call cannot be made.

- **Number of Call Attempts**: Specify the number of attempts to call the number if the callee doesn't answer the call or if the callee answers the call but does not listen to the new voicemail message.
- **Retry Interval (min)**: Specify the interval between the call attempts.

d. **Optional:** To add more contacts, repeat step c.

> **Note:**
> The system will call the external numbers from the top down. You can adjust the priority order using ☰.

4. Click **Save**.

Result

When the group voicemail receives a new message, the PBX will call the preset numbers in sequence. The callee can answer the call and follow the prompt to listen to the message or call the original caller back directly.

Related information

Extension Call Statistics Report
Extension Call Activity Report

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 web 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 web 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 web 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 web 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 web 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 web 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 someone 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 web 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 web 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 web 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

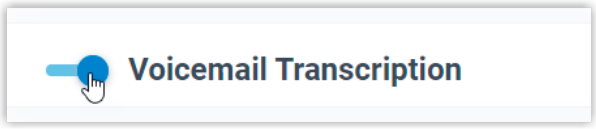
Prerequisites

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 web portal, go to **Call Features > Voicemail > Voicemail Settings**.
2. Scroll down to the bottom of the page, turn on **Voicemail Transcription**.



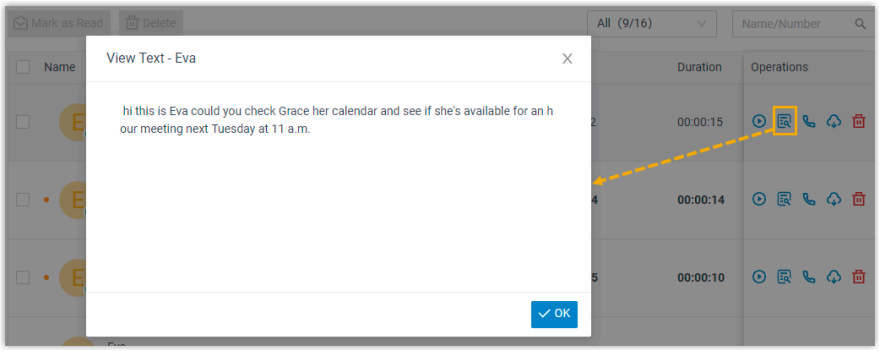
3. Click **Save**.

Result

The Voicemial Transcription feature is enabled, users can receive voicemails in the form of text on different platforms.

Linkus UC Clients

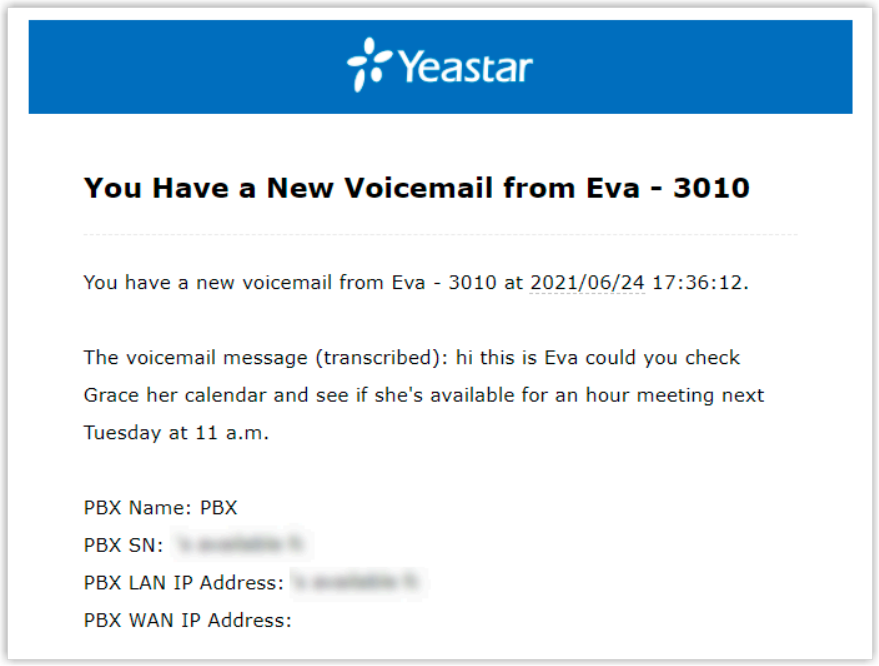
Users can check the transcribed text for each voicemail on Linkus Web Client, Desktop Client, and Mobile Client.



Email Client

If Voicemail to Email feature is enabled, the transcribed text will be displayed in the email content for received voicemails.

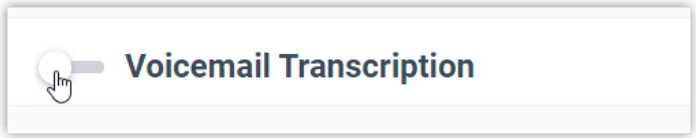
The figure below shows an example of voicemail notification email.



Disable Voicemail Transcription

Procedure

1. Log in to PBX web 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 envelop 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 web 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 web 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 web 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 web 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 web 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 web 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 web 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 web 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 web 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 web 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 web 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 web 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 web 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 web 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.
     b. Pick up the call to listen to the greeting on the phone.

Download a personal greeting

1. Log in to PBX web 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 web 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 web 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 web 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 web 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 web 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 web 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 web 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 web 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 been associated with a phone, see the following topics to bind a phone with the extension.
   - Auto Provision IP Phones in Local Network (PnP Method)
   - Auto Provision IP Phones in Local Network (DHCP Method)
   - Auto Provision IP Phones Remotely (RPS FQDN Method)
   - Auto Provision IP Phones Remotely (RPS Method)
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 web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
2. Click **Voicemail** tab.
3. In the **New Voicemail Notification** drop-down list, decide whether to send email notifications when the user receives a new voicemail.
    - To disable email notifications, select **Do Not Send Email Notifications**.
    - To enable email notifications, select one of the following options:
        - **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 notification emails only.
4. If you enabled email notifications, configure the following settings as needed:

Setting	Description
After Notification	Decide how to deal with voicemails after notification emails are sent out. • **Mark as Read**: Mark the voicemail message in mailbox as read. • **Delete Voicemail**: Delete the voicemail messages from mailbox. • **Do Nothing**: Keep the voicemail message in mailbox as unread.

Setting	Description
Send to	Specify the email address for receiving notification emails. • **User Email**: Send notification emails to the user's email address. • **Custom Email**: Send notification emails to a custom email address. Enter the desired email address in the **Custom Email Address** field.

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 web 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 web 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 web 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 web 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.

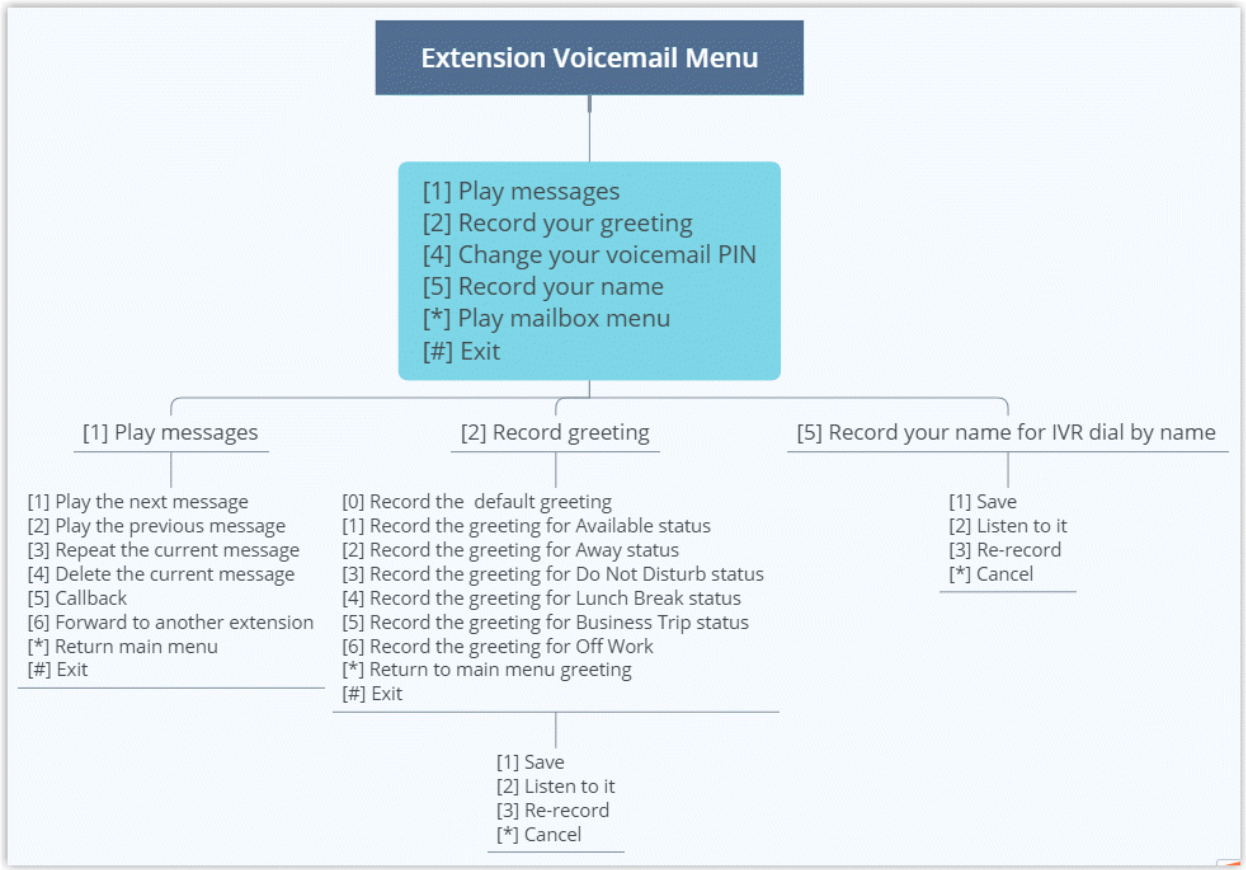
Voicemail Transcription

Decide to enable or disable Voicemail Transcription feature. For more information, see Enable or Disable Voicemail Transcription.

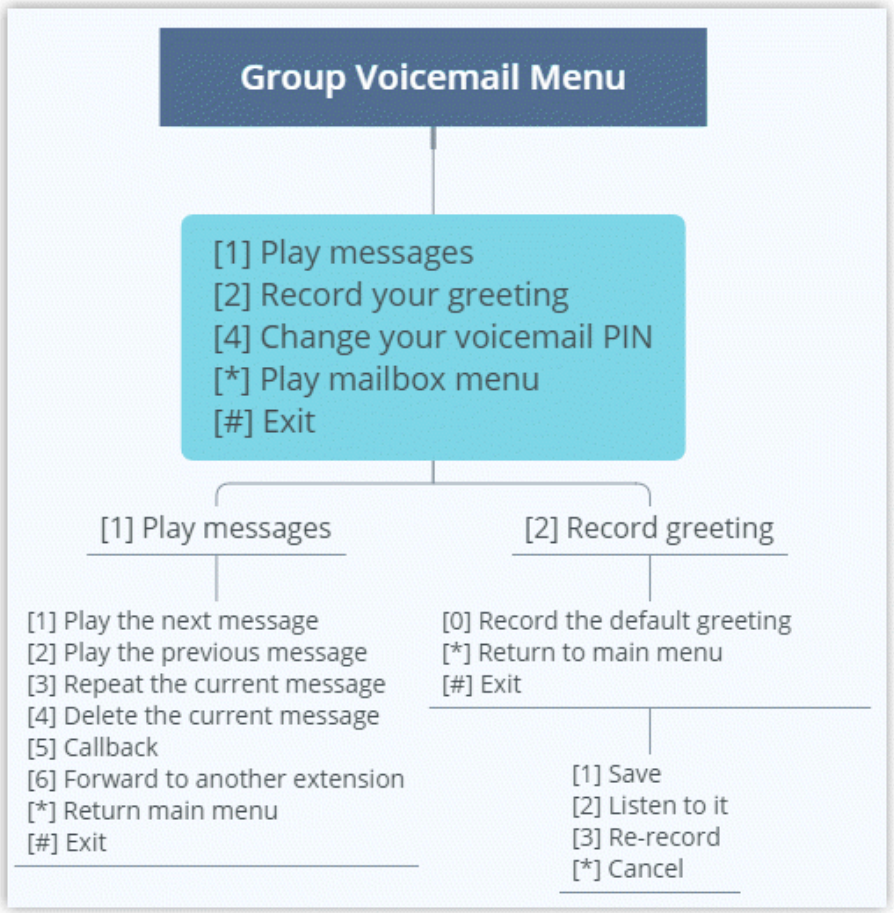
Voicemail Menu Options

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.
- Allow customers to dial ring group, queue, or conference numbers directly.

For employee

- Allow employees to make an outbound call via an IVR.
- Allow employees to check voicemail via an IVR.

- Allow employees to remotely change IVR prompt by dialing the feature code #9.

IVR keypress events

There are four types of keypress events:

- **Menu options**: The number keys, # key and * key for users to access a desired destination.
- **Invalid**: When an invalid key is pressed, route the call to a desired destination.
- **Timeout**: If no input is detected after the configured timeout, the PBX will forward the call based on the configuration.

Advanced settings

- **Time Condition**: Route inbound calls to different destinations based on time conditions.
- **Language**: Provide language options for callers and play system prompts in their preferred language.
- **Custom Key**: Route inbound calls to different destinations based on PIN code.

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.
- **Conference**: Route the call to a specified conference.
- **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.
- **Play Prompt and Return to IVR**: Play a custom prompt, and then back to the IVR.
- **Play IVR Prompt**: Play the IVR prompt, and then hang up the call.

> **Note:**
> - The option is only available for **Invalid Input Destination**.
> - When callers enter a DTMF digit that is not defined in the IVR, the system would repeat the IVR prompt. If the play counts of the IVR prompt reach the maximum number of times, the system would directly 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 web 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.
- **Allow Calling Numbers**: Whether to allow callers to dial ring group, queue, or conference numbers via IVR.
- **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.
- **Dial #9 to Modify IVR Prompt**: Whether to allow users to dial the feature code #9 to record and apply a new IVR prompt.

> **Note:**
> If the IVR prompt is replaced successfully, the previous voice prompt will be removed from the IVR prompt setting, and the new voice prompt will be retained.

3. Click the **Key Press Event** tab, set up an IVR menu.
   - To set key events to route calls to different destinations based on time, see Set Key Events Based on Time Conditions.
   - To set key events to route calls to different destinations based on PIN code, see Set up IVR Custom Key.
   - To set key events to always route calls to the designated destination, do as follows:
     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.

Related information

Allow Callers to Dial Extensions via IVR
Allow Callers to Dial Numbers via IVR
Allow Callers to Dial by Name via IVR
Allow Callers to Dial Outbound Calls via IVR
Allow Callers to Change IVR Prompt Remotely
Forward Incoming Calls to an External Number via IVR
Set up a Multi-language IVR
Set Key Events Based on Time Conditions
Set up IVR Custom Key

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 8 MB. Divide the audio file into multiple audio clips to solve this issue.

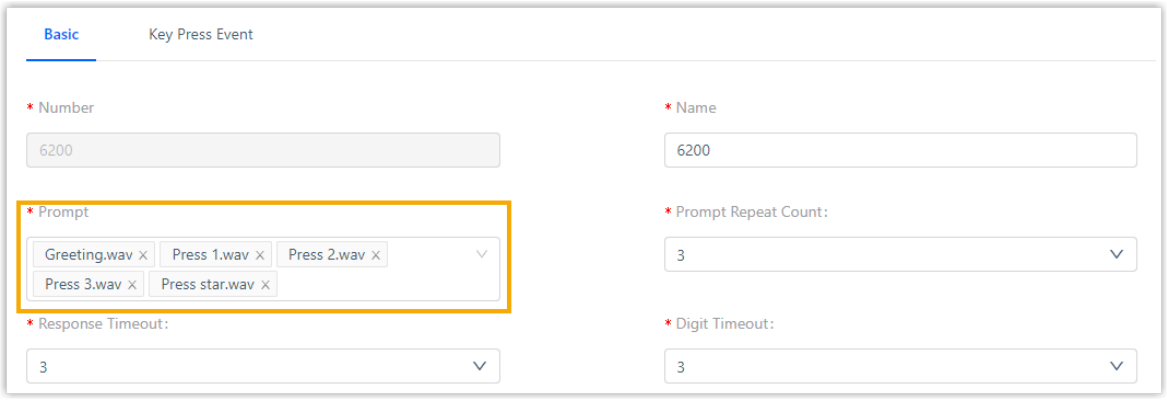
Update the IVR prompts

1. Log in to PBX web 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.



4. In the **Prompt Repeat Count** drop-down list, select prompt repeat times.
5. Click **Save** and **Apply**.

Related information

Allow Callers to Change IVR Prompt Remotely

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 dialing extension directly via an IVR, update your IVR prompt that would instruct callers to dial an extension number.

Procedure

1. Log in to PBX web 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.
    - **Allowed 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 Numbers via IVR

When callers enter an IVR, if they know the number of a ring group, queue or conference room, they can dial the number directly to reach the destination. This topic describes how to allow callers to dial ring group, queue, or conference room numbers via an IVR.

Requirements

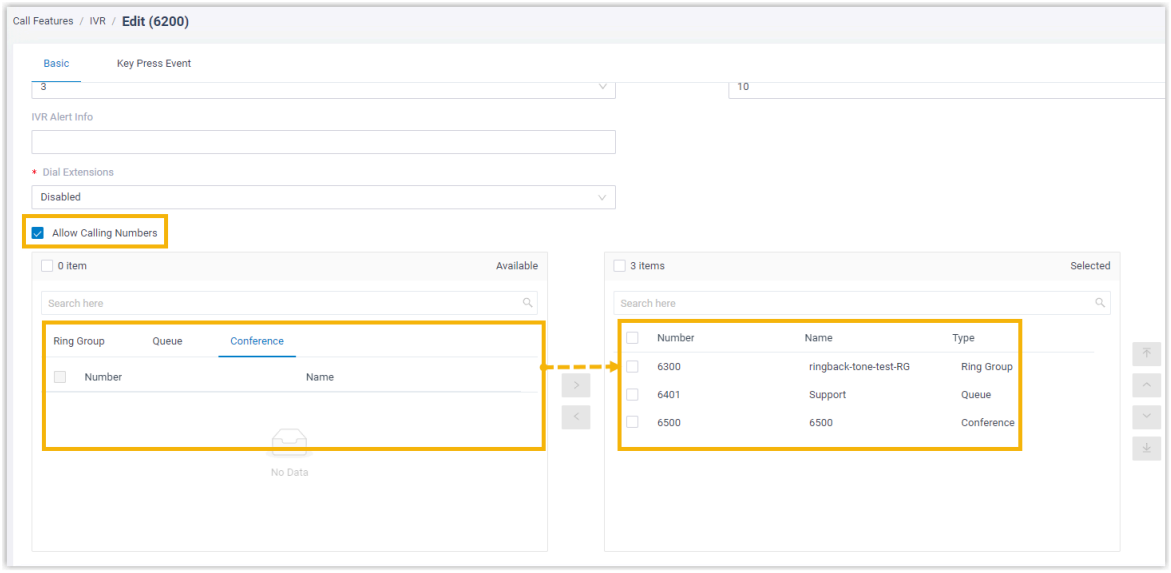
The firmware version of PBX server is 37.16.0.70 or later.

Prerequisites

- An IVR has already been set up, and ring group(s), queue(s) or conference(s) have been configured as you need.
- Upload or record an IVR prompt that would instruct customers to dial ring group, queue, or conference room numbers in an IVR.

Procedure

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. Select the checkbox of **Allow Calling Numbers**, then select the desired ring group, queue, or conference from the **Available** box to the **Selected** box.



3. Click **Save** and **Apply**.

Result

When callers enter an IVR, they can enter the number of ring group, queue or conference to reach the destination.

Allow Callers to Dial by Name via IVR

For the customers who don't remember an employee's extension number, you can allow them to reach the employee by entering the first three letters of the employee's first name or last name in an IVR. It is easier for customers to get to the right person.

Restrictions

The **Dial by Name** feature supports to search the extension users whose caller ID names are composed of English letters or Mandarin phonetic symbols.

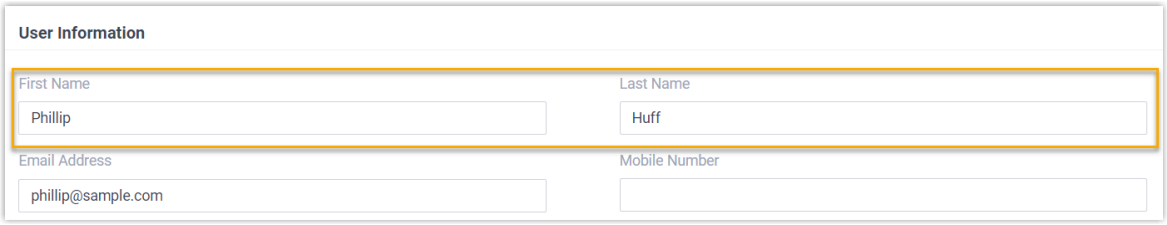
Procedure

1. Specify an extension's caller ID name
2. Set display format for extensions' caller ID name
3. Customize IVR prompt
4. Configure an IVR

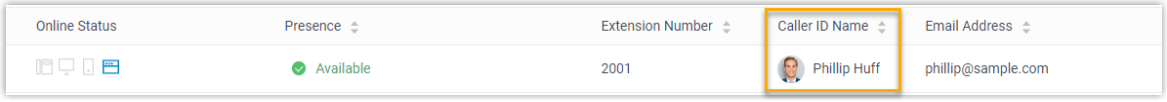
Specify an extension's caller ID name

When using **Dial by Name**, the IVR performs a search on an extension's caller ID name, which is composed of the first name and last name of the extension user. Therefore, make sure you have configured the caller ID name for extensions.

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
2. In the **User Information** section, specify the **First Name** and **Last Name** for the extension.



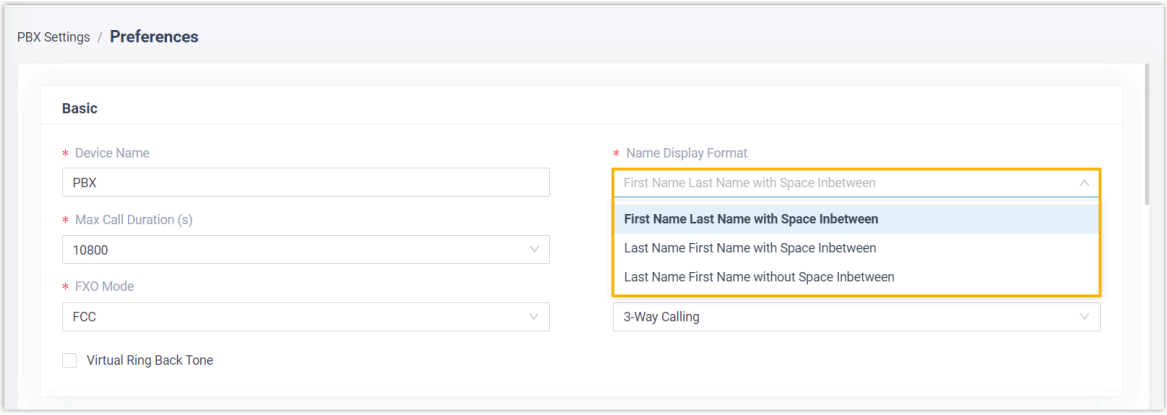
3. Click **Save** and **Apply**.



Set display format for extensions' caller ID name

When searching for extensions by name, the IVR starts from the beginning of extensions' caller ID name. By setting display format for extensions' caller ID name, you can determine how callers can reach employee - either by **First Name** or **Last Name**.

1. Log in to PBX web portal, go to **PBX Settings > Preferences**.
2. In the **Name Display Format** drop-down list, select a display format.



- To allow callers to reach extension users by first name, select **First Name Last Name with Space Inbetween**.
- To allow callers to reach extension users by last name, select **Last Name First Name with Space Inbetween** or **Last Name First Name without Space In-between**.

3. Click **Save** and **Apply**.

Customize IVR prompt

You need to prepare a custom IVR prompt, instructing the callers to press a specific key in an IVR to enter the **Dial by Name** feature.

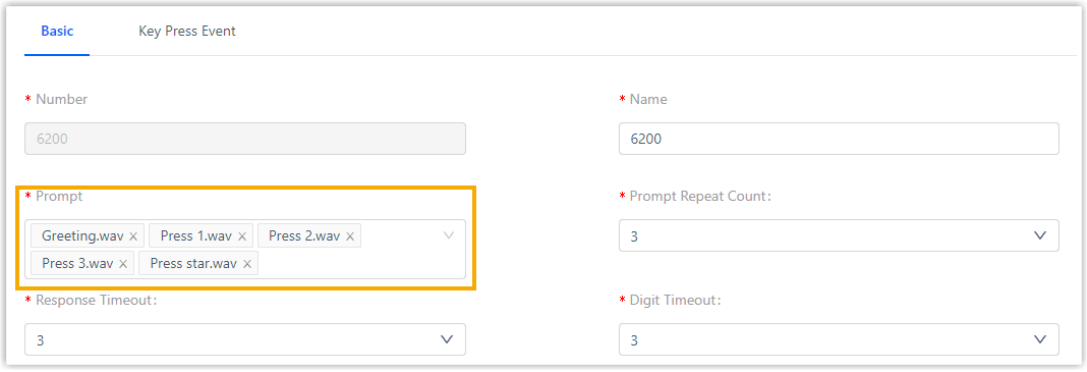
1. Log in to PBX web portal, go to **PBX Settings > Voice Prompt > Custom Prompt**.
2. Upload a custom prompt or record a custom prompt.

> **Note:**
> The uploaded file should meet the audio file requirements.

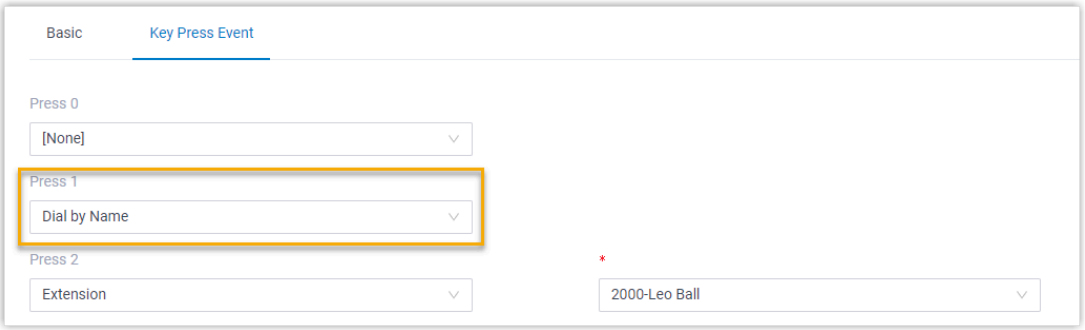
Configure an IVR

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. Update the IVR prompt.
   a. Go to the **Basic** tab.
   b. 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.



3. Set up the IVR keypress destination.
   a. Go to the **Key Press Event** tab.
   b. In the drop-down list of a key press, select **Dial by Name**.



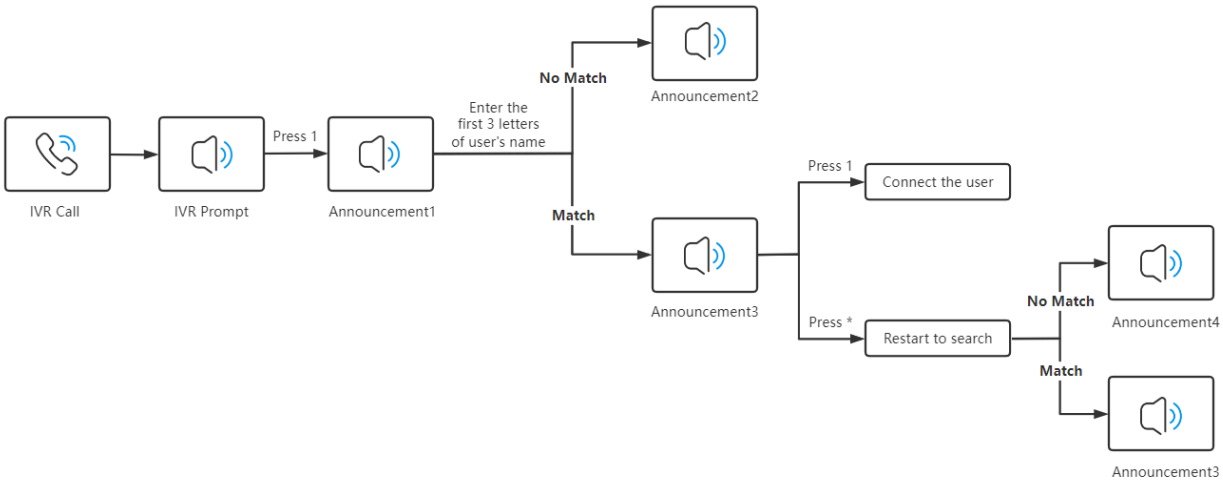
4. Click **Save** and **Apply**.

Result

Customers can call to the IVR, and quickly search the desired extension user by entering the first 3 letters of his/her name.

Example

We provide an example to help you understand the workflow of dial-by-name. In this example, the display format for extensions' caller ID name is set to **First Name Last Name with Space Inbetween** and the destination of key "1" is set to **Dial by Name**.



1. A caller calls into an IVR and hears the IVR prompt.
2. The caller presses "1" to enter the **Dial by Name** feature.
3. After hearing the announcement1, the caller enters the first 3 letters of an extension user's first name.

   For example, to search an extension user with the name "Phillips Huff", the caller needs to dial 7-4-4 (indicating `P H I`) on the phone's keypad.

4. The IVR will look for the best match and play the corresponding announcement.
   - If there is no matched user, the IVR plays announcement2.
   - If there is a matched user, the IVR plays announcement3, providing the extension user's name and extension number, as well as the following operation instructions:
     - **1**: If this is the person you are looking for, press 1 now.

       The IVR will send the call to the extension user.
     - *: Otherwise please press star now.

       The IVR will start a new search, and provide another matched user's information to the caller. If there is no more matched user, IVR will play announcement4.

Default announcement of Dial by Name

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 1 now, otherwise please press star now.	Play when there are matching directory entries after the caller enters three letters.
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 headquarters and branch, and only set an IVR on headquarters PBX. You can allow the customers to dial the headquarters' 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 web 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**.

Allow Callers to Change IVR Prompt Remotely

In case of emergency (e.g. the office needs to close early due to bad weather), you may need to change IVR prompt. Instead of logging in to PBX with a computer to change IVR prompt, you can just make a call to the IVR, then dial a specific feature code to record and apply a new IVR prompt.

Restrictions

- The number of custom prompts does NOT reach the maximum limit. Otherwise, users can NOT record new voice prompt for the IVR.
- A maximum of 2-minute recording time is allowed.

Procedure

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. In the **Basic** tab, select the checkbox of **Dial #9 to Modify IVR Prompt**.
3. In the **IVR Prompt Modify Password** field, enter a password for authentication.

   Callers need to enter the password to authenticate, so as to change the IVR prompt.
4. Click **Save** and **Apply**.

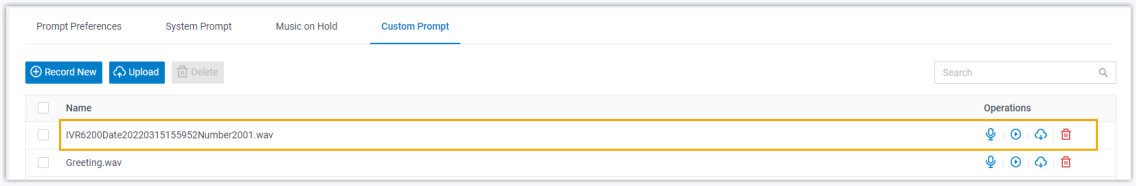
Result

Users can call to an IVR, dial #9 and enter the password, then follow the voice prompt to record a new IVR prompt on their phones.

If IVR prompt is replaced successfully, the previous voice prompt will be removed from the IVR setting, and the new voice prompt will be retained.

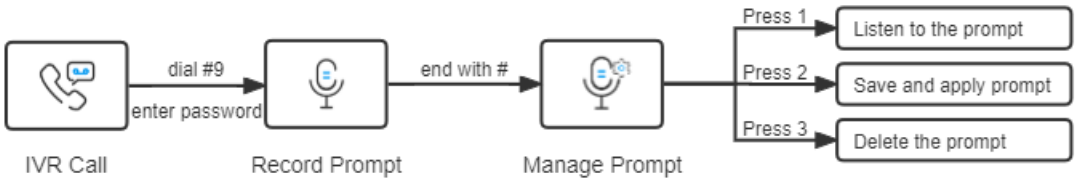
Note:

The new voice prompt is save on **PBX Settings > Voice Prompt > Custom Prompt**, with a prompt name in the format of **IVR*{ivr_number}*Date*{date}*Number*{extension_number}***.



Example

We provide an example to help you understand the workflow of remotely changing IVR prompt.



1. In an IVR call, a caller dials #9, then enter the password to authenticate.
2. After hearing the beep tone, the caller starts recording the prompt. When done, press # key.
3. The caller can press a specific key to manage the prompt:
    - **1**: Listen to the prompt.
    - **2**: Save and apply the prompt to the IVR.
    - **3**: Delete the prompt.

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 web 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

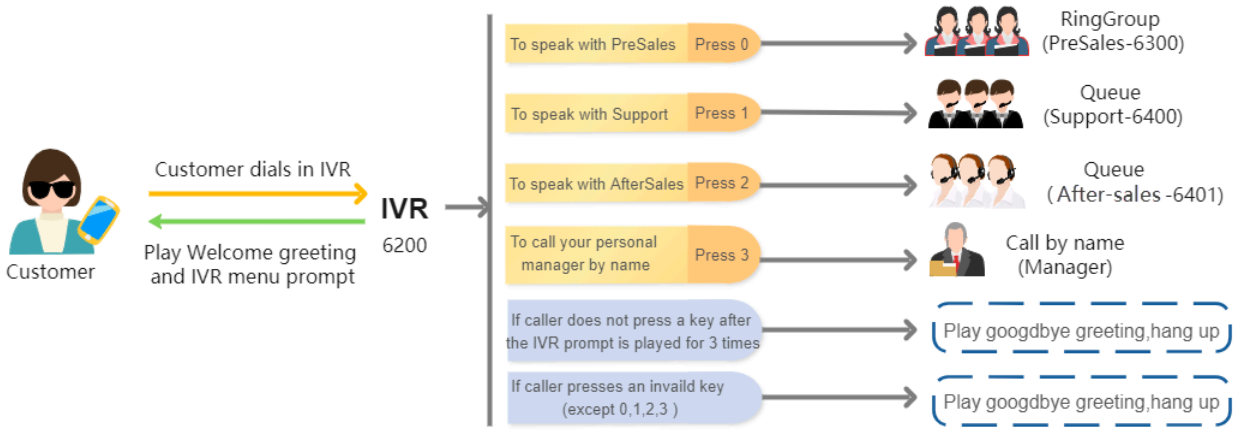
Background information

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.

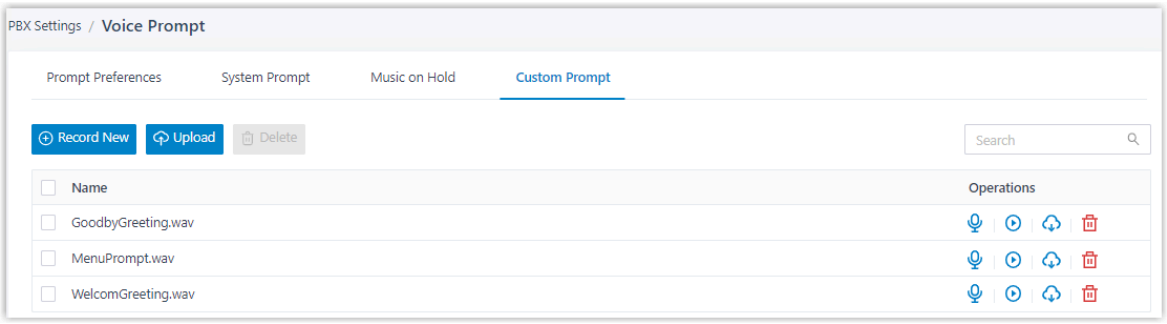
Step1. Design an IVR

When the customers dial in IVR (6200), they can access different service based on their business.



Step2. Upload IVR Prompts

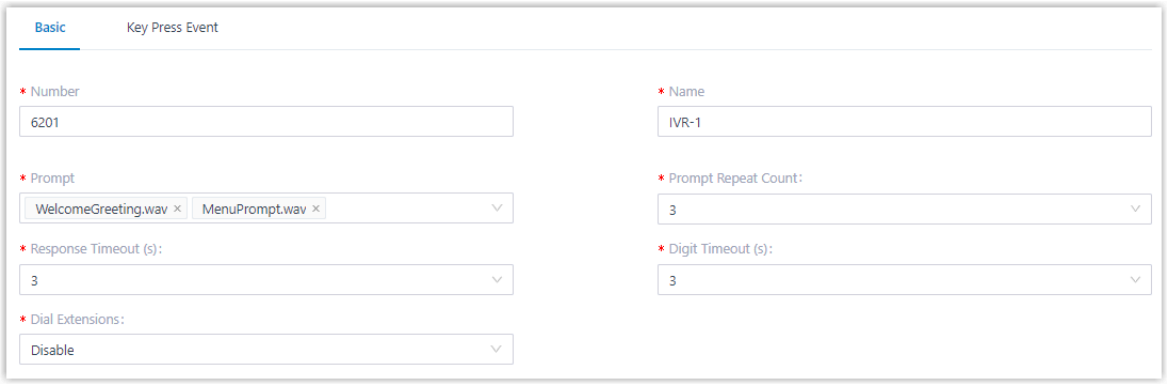
1. Go to **PBX Settings > Voice Prompt > Custom Prompts**, click **Upload**.
2. Select the audio files to upload.



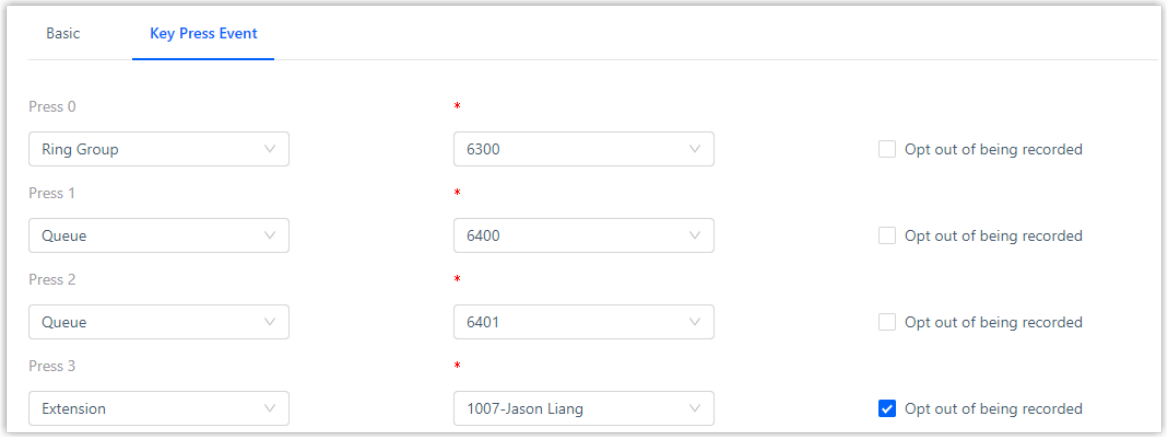
3. Click **Save** and **Apply**.

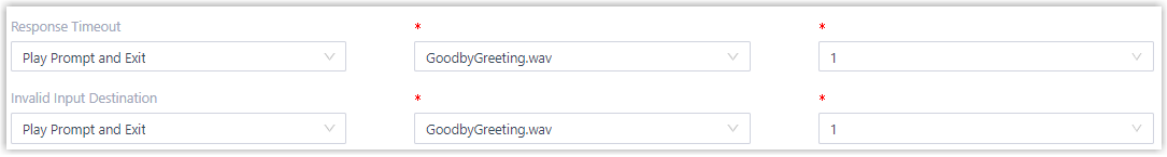
Step3. Set up an IVR

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.





4. Click **Save** and **Apply**.

Multi-level IVR Configuration

Background information

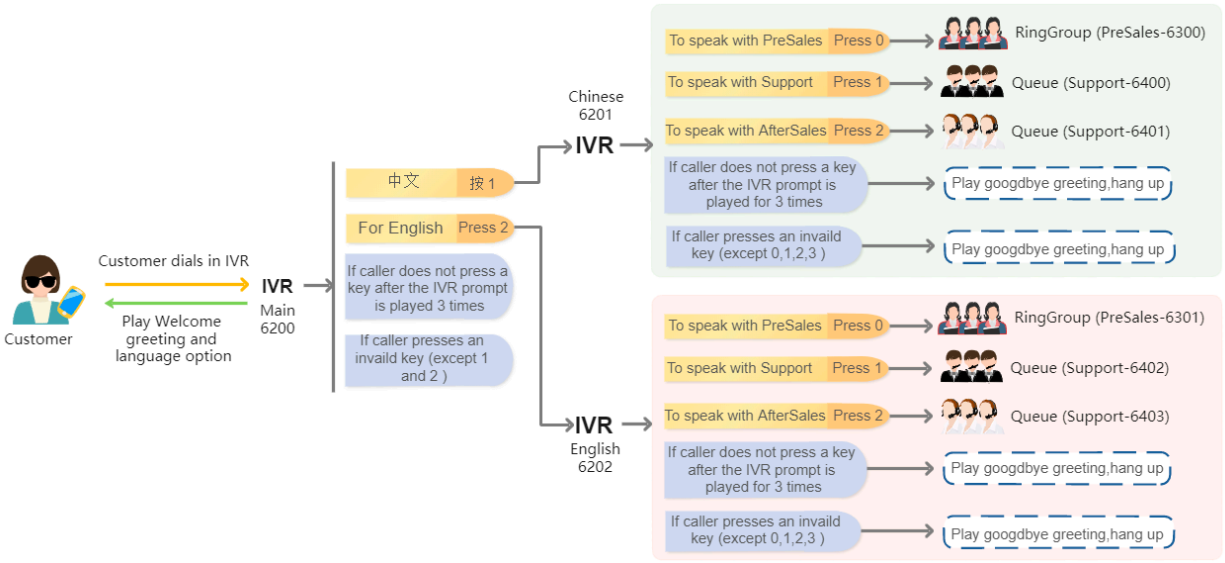
As business expands, the company needs to offer callers a bilingual auto-attendant feature based on their language selection. When the customer dials in to IVR, they can select a specific language to be used when playing prompts.

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

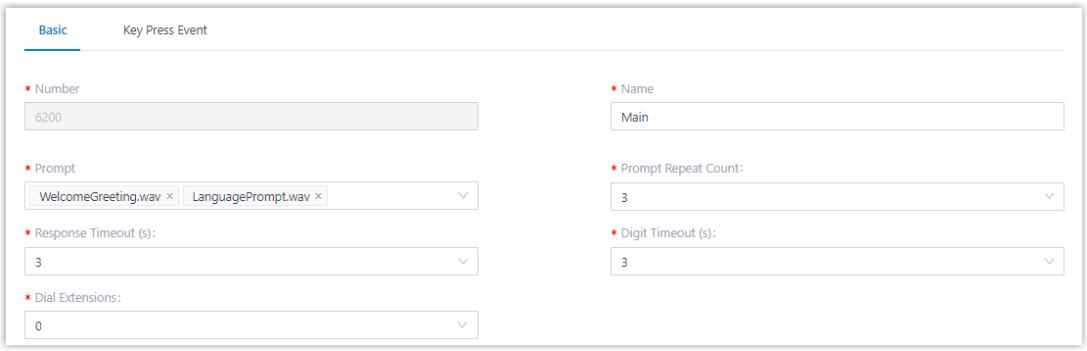
When the customers dial in to IVR-Main (6200), they can select a specific language to use.

- 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).



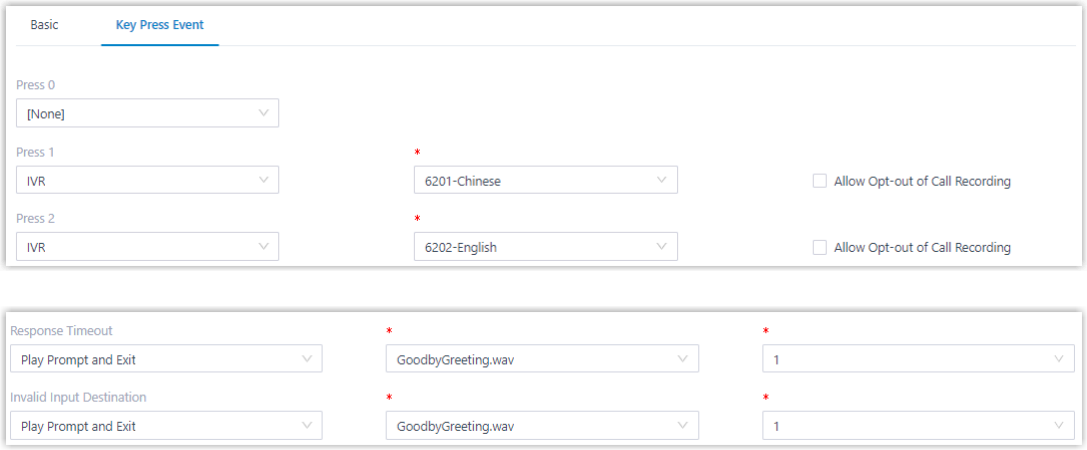
Step2. Set up IVRs

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.



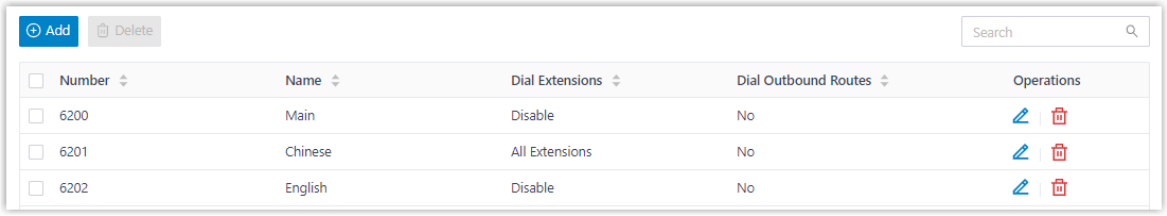
b. In the **Key Press Event** tab, set up an IVR menu.

- 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.



Advanced IVR Settings

Set Key Events Based on Time Conditions

Yeastar P-Series PBX System supports setting IVR key press events based on time conditions, enabling the routing of incoming calls to different destinations based on the time they

are received. You can apply a single time condition for all key press events or customize time conditions for each key press event.

Requirements

Yeastar P-Series PBX System is 37.18.0.59 or later.

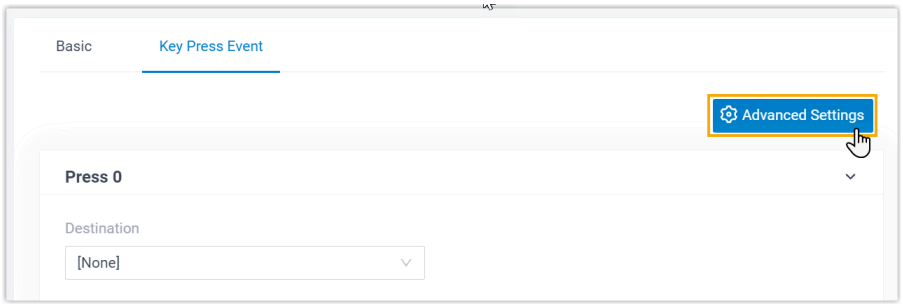
Apply the same time condition for all key press events

1. Log in to PBX web portal, go to **Call Features > IVR**.
2. Click  beside the desired IVR.
3. In the **Key Press Event** tab, configure key press events to route calls according to your needs.

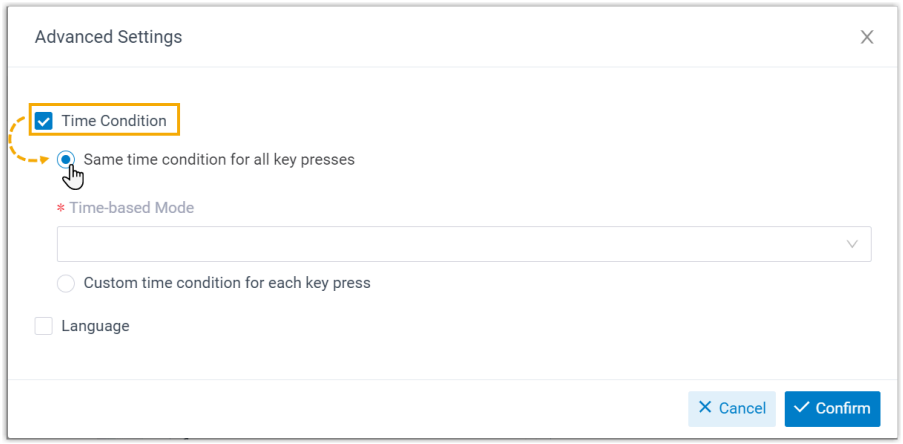
Scenario	Description
Route calls based on business hours configured in specific time zone	All key press events route calls to specified destinations based on the business hours, non-working hours, and holidays configured in a specific time zone (Defined on **Call Control > Business Hours and Holidays**). For detailed instructions, see Route calls based on business hours in specific time zone.
Route calls based on custom business hours	Create a custom business hours based on the system's default time zone, and all key press events route calls to specified destinations based on the custom business hours, non-working hours, and holidays. For detailed instructions, see Route calls based on custom business hours.
Route calls based on custom time periods	Create a custom time period based on the system's default time zone for each key press event, and route calls based on the custom time period accordingly. For detailed instructions, see Route calls based on custom time periods.

Route calls based on business hours in specific time zone

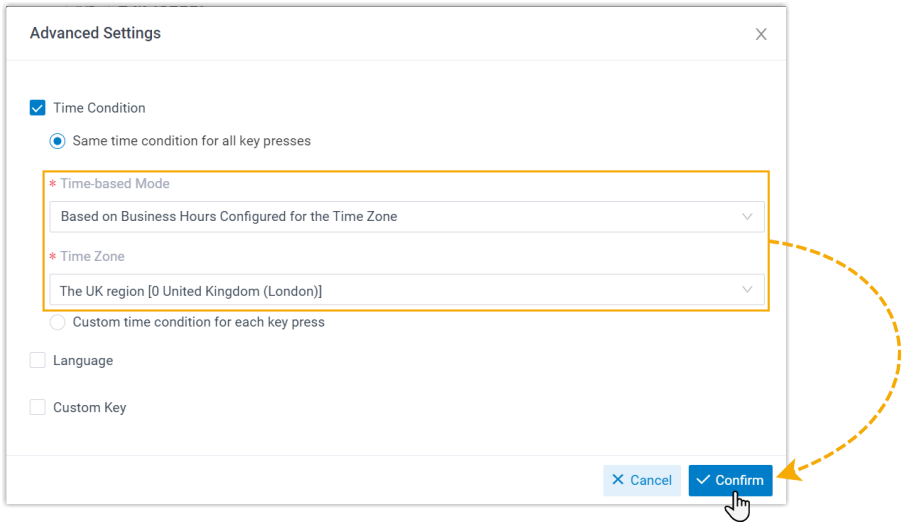
a. On the top-right corner, click **Advanced Settings**.



b. In the pop-up window, select the checkbox of **Time Condition**, and select **Same time condition for all key presses**.

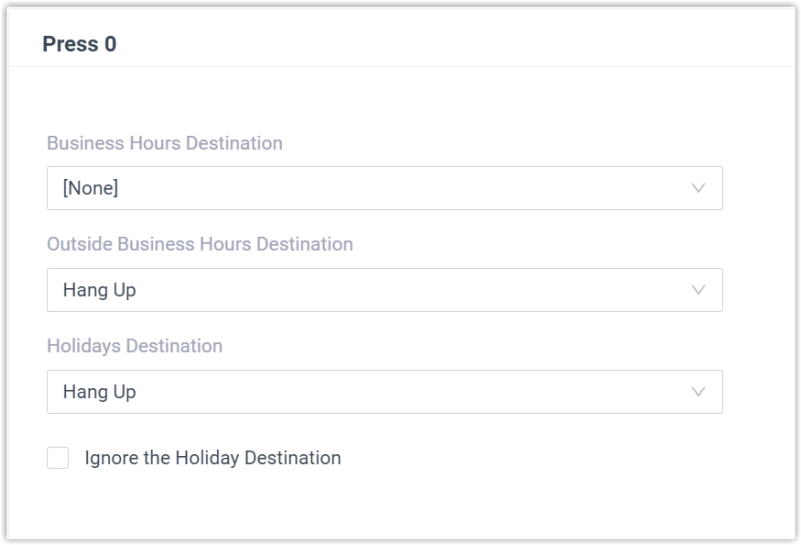


c. In the **Time-based Mode** drop-down list, select **Based on Business Hours Configured for the Time Zone**, select the desired time zone, and click **Confirm**.



The global business hours is applied to all key press events in the IVR.

d. Specify call routing destinations for a key press event based on the global business hours.



- **Business Hours Destination**
- **Outside Business Hours Destination**
- **Holidays Destination**

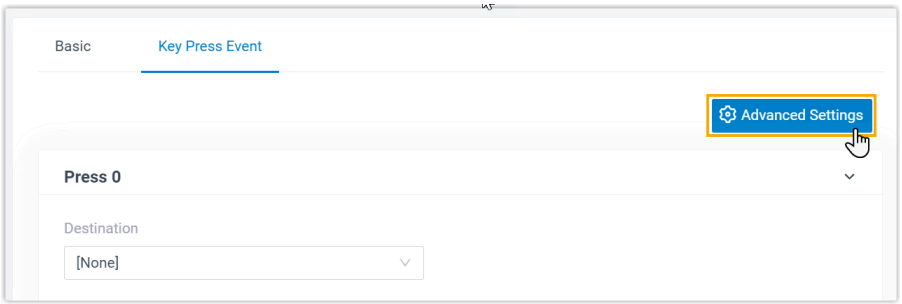
> **Note:**
> If you want to route calls based on global business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**.

e. Repeat step **d** for all the desired keys.

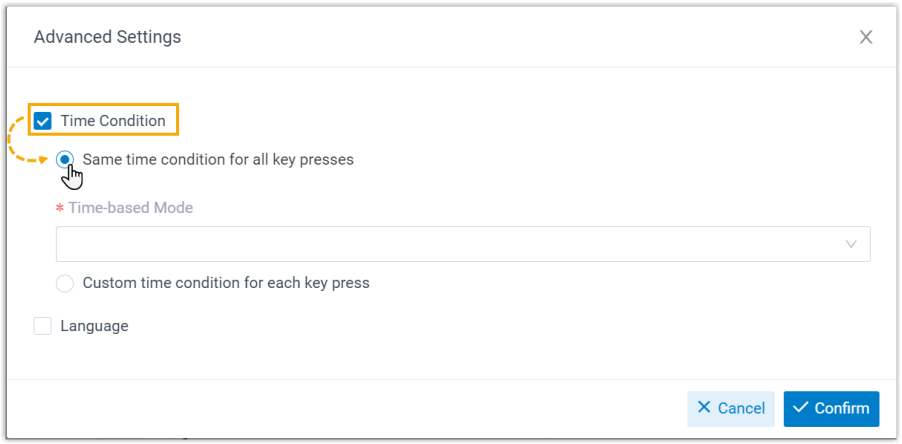
f. Click **Save** and **Apply**.

Route calls based on custom business hours

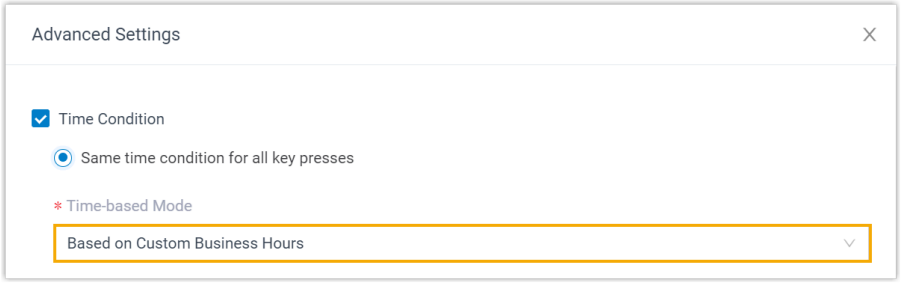
a. On the top-right corner, click **Advanced Settings**.



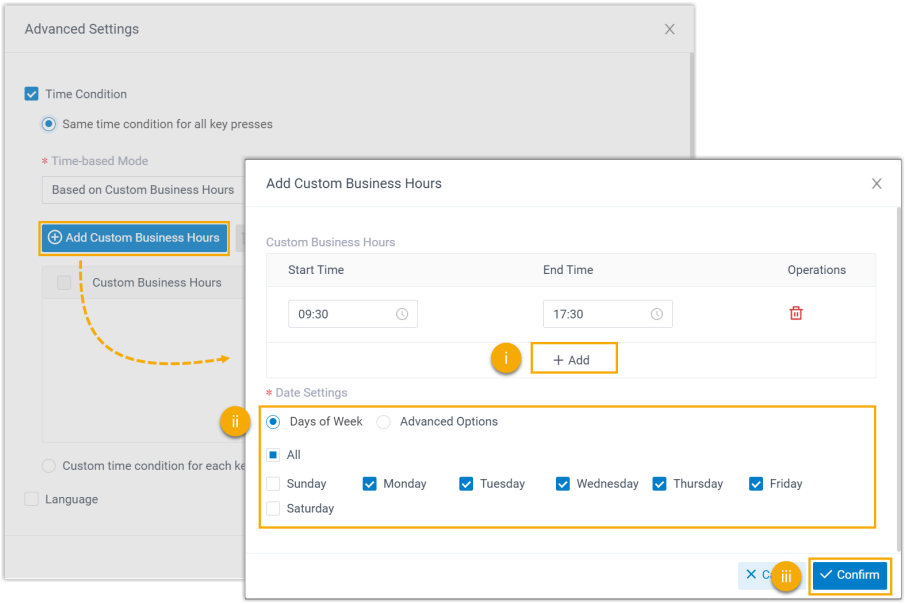
b. In the pop-up window, select the checkbox of **Time Condition**, and select **Same time condition for all key presses**.



c. In the **Time-based Mode** drop-down list, select **Based on Custom Business Hours**.



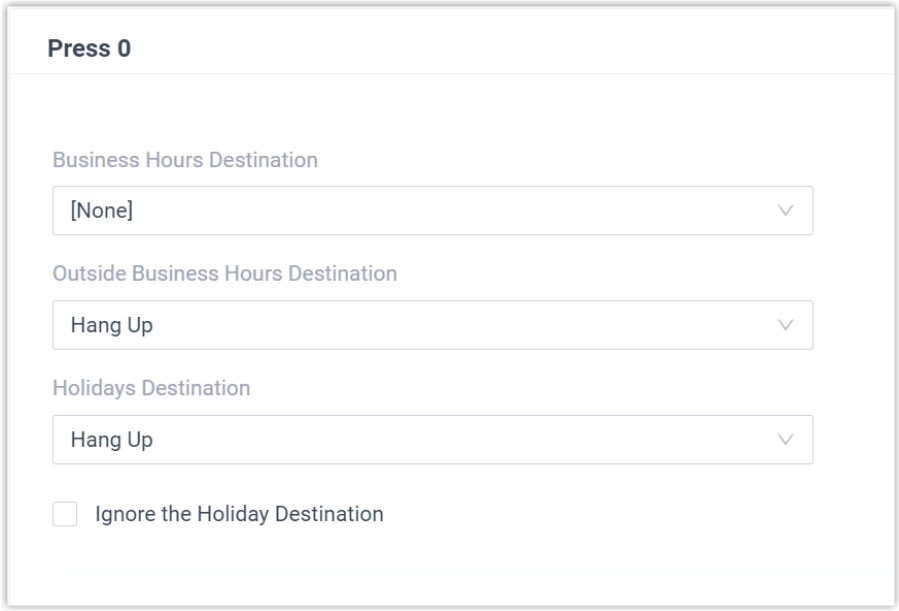
d. Click **Add Custom Business Hours** to create custom business hours based on the system's default time zone.



i. Click **Add** and specify the start time and end time.

ii. In the **Date Settings** section, specify the workdays.
iii. Click **Confirm**.

e. Click **Confirm** to apply this custom business hours to all key press events in the IVR.
f. Specify call routing destinations for a key press event based on the custom business hours.



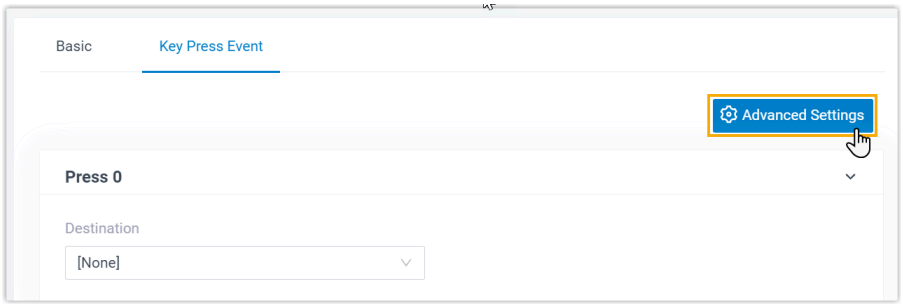
- **Business Hours Destination**
- **Outside Business Hours Destination**
- **Holidays Destination**

> **Note:**
> If you want to route incoming calls based on custom business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**.

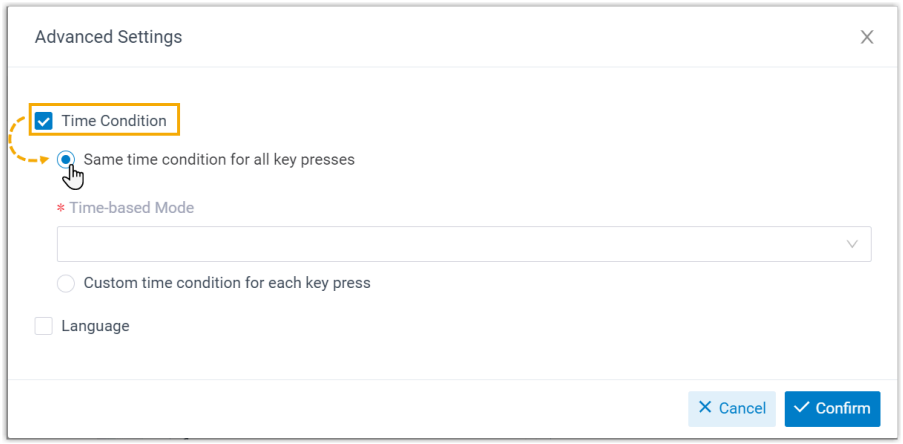
g. Repeat step **f** for all the desired keys.
h. Click **Save** and **Apply**.

Route calls based on custom time periods

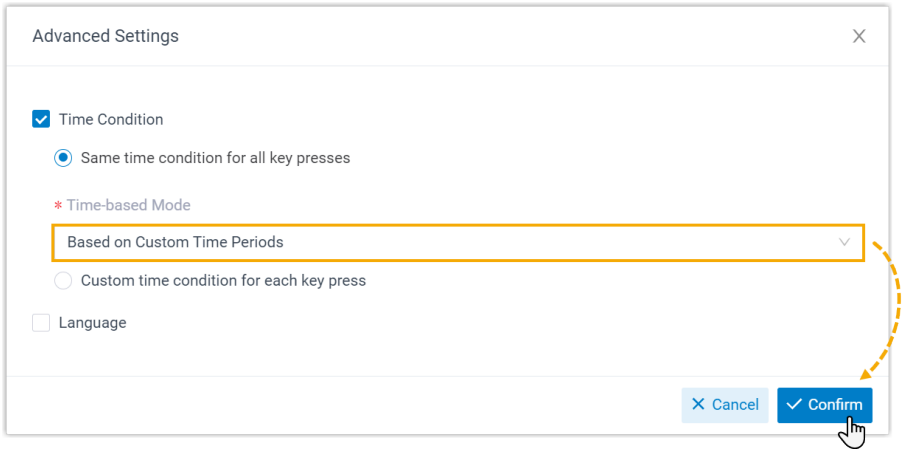
a. On the top-right corner, click **Advanced Settings**.



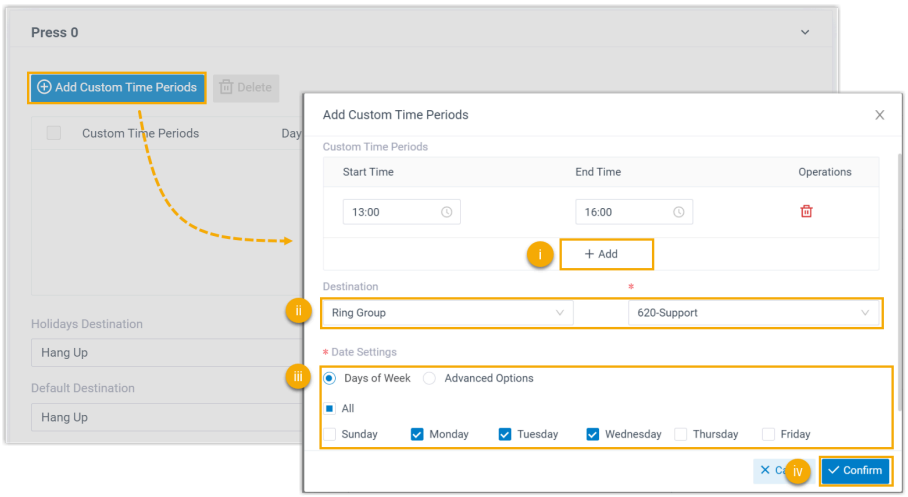
b. In the pop-up window, select the checkbox of **Time Condition**, and select **Same time condition for all key presses**.



c. In the **Time-based Mode** drop-down list, select **Based on Custom Time Periods**.



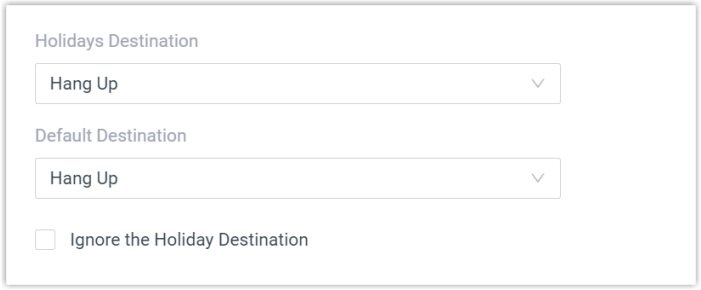
d. Under a key press event, click **Add Custom Time Periods** to create a custom time period based on the system's default time zone for the key.



i. Click **Add** and specify the start time and end time.
ii. In the **Destination** drop-down list, specify the destination for calls within the custom time periods.
iii. In the **Date Settings** section, specify the workdays.
iv. Click **Confirm**.

> **Note:**
> The specified custom time periods ONLY take effect for this key press event.

e. Specify the following call routing destinations for the key press event.



- **Holidays Destination**: Specify the call routing destination for calls during holidays.

> **Note:**

> If you want to route incoming calls based on custom time periods during holidays, select the checkbox of **Ignore the Holiday Destination**.

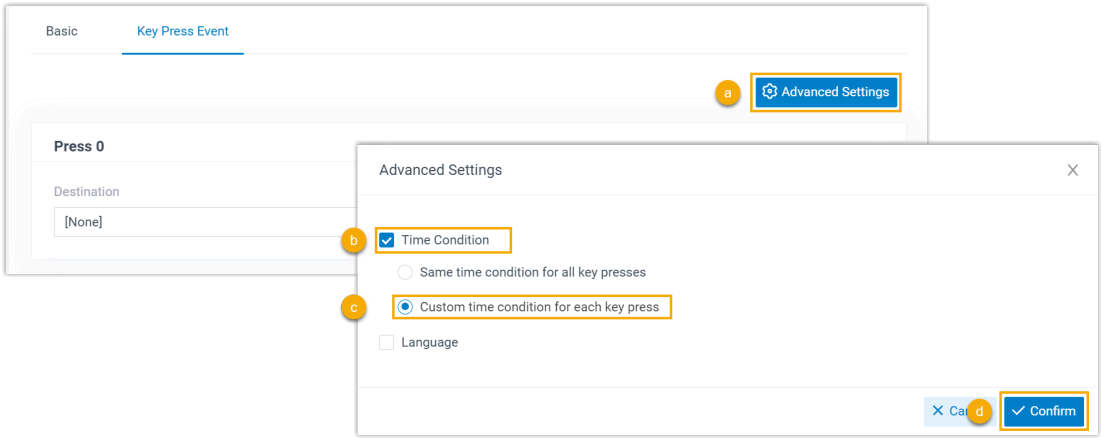
- **Default Destination**: Specify the call routing destination for calls outside the custom time periods.

f. Repeat step **d** - **e** for all the desired keys.

g. Click **Save** and **Apply**.

Apply different time conditions for each key press event

1. Log in to PBX web portal, go to **Call Features > IVR**.
2. Click beside the desired IVR.
3. In the **Key Press Event** tab, enable time-condition settings for this IVR.



a. On the top-right corner, click **Advanced Settings**

b. In the pop-up window, select **Time Condition**.

c. Select **Custom time condition for each key press**.

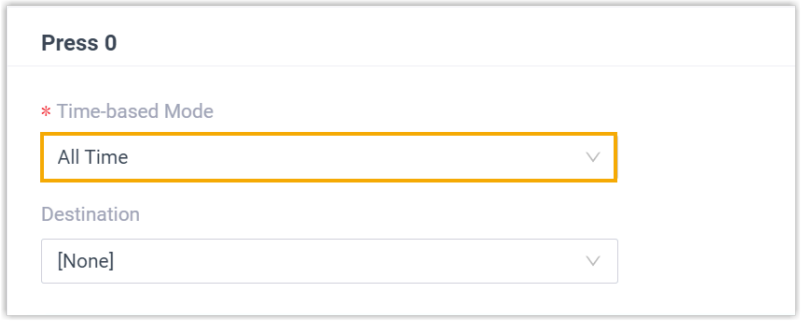
d. Click **Confirm**.

4. In the **Time-based Mode** drop-down list of a key, select the time condition and configure the call routing destinations.

Option	Description
All Time	Always route calls to the specified destination. For detailed instructions, see Route calls at all times.
Based on Business Hours Configured for the Time Zone	Route calls to specified destinations based on the business hours, non-working hours, and holidays of a specific time

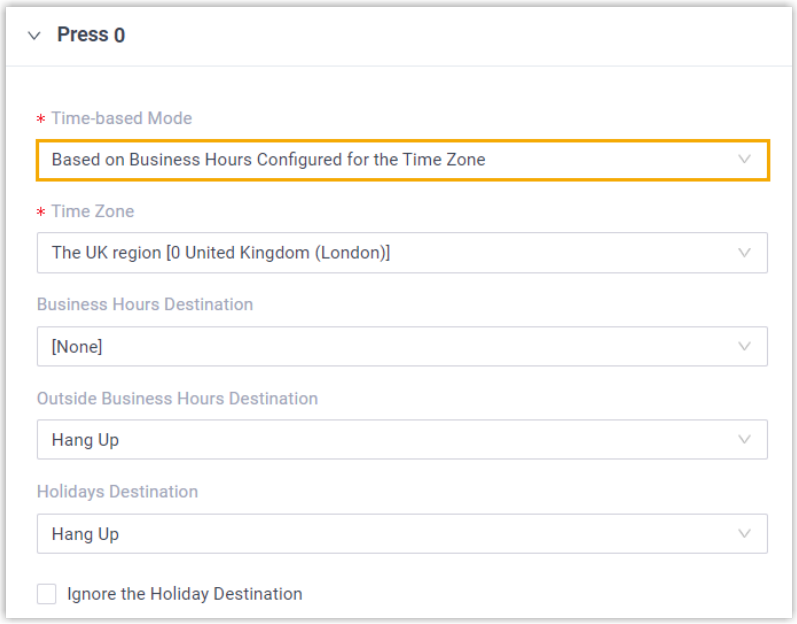
Option	Description
	zone (Defined in **Call Control > Business Hours and Holidays**). For detailed instructions, see Route calls based on global business hours.
Based on Custom Business Hours	Create a custom business hours based on the system's default time zone, and route calls to specified destinations based on the custom business hours, non-working hours, and holidays. For detailed instructions, see Route calls based on custom business hours.
Based on Custom Time Periods	Create a custom time period based on the system's default time zone and route calls based on the custom time period. For detailed instructions, see Route calls based on custom time periods.

Route calls at all times



a. In the **Time-based Mode** drop-down list, select **All Time**.
b. In the **Destination** drop-down list, specify the destination.

Route calls based on global business hours

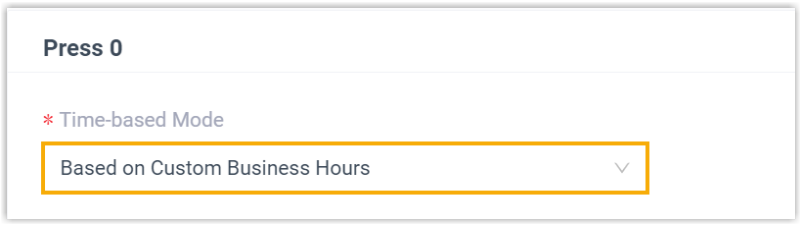


a. In the **Time-based Mode** drop-down list, select **Based on Business Hours Configured for the Time Zone**, then select the desired time zone.
b. Specify call routing destinations for the key press event based on the global business hours.
    - **Business Hours Destination**
    - **Outside Business Hours Destination**
    - **Holidays Destination**

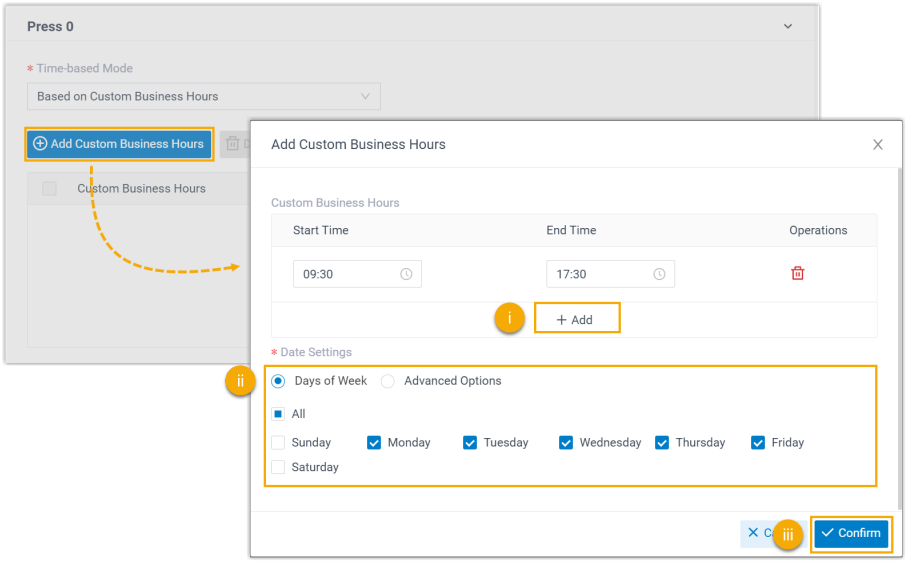
> **Note:**
> If you want to route incoming calls based on global business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**.

Route calls based on custom business hours

a. In the **Time-based Mode** drop-down list, select **Based on Custom Business Hours**.

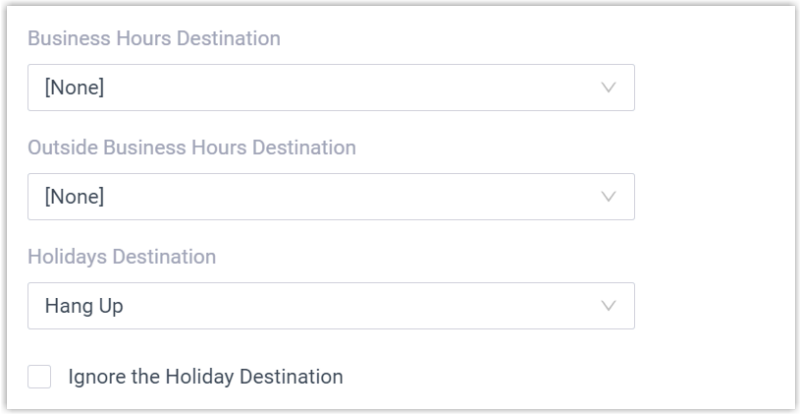


b. Click **Add Custom Business Hours** to create custom business hours based on the system's default time zone.



i. Click **Add** and specify the start time and end time.
ii. In the **Date Settings** section, specify the workdays.
iii. Click **Confirm**.

c. Specify call routing destinations for a key press event based on the custom business hours.



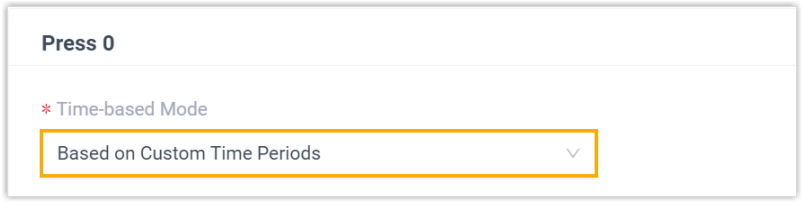
- **Business Hours Destination**

- **Outside Business Hours Destination**
- **Holidays Destination**

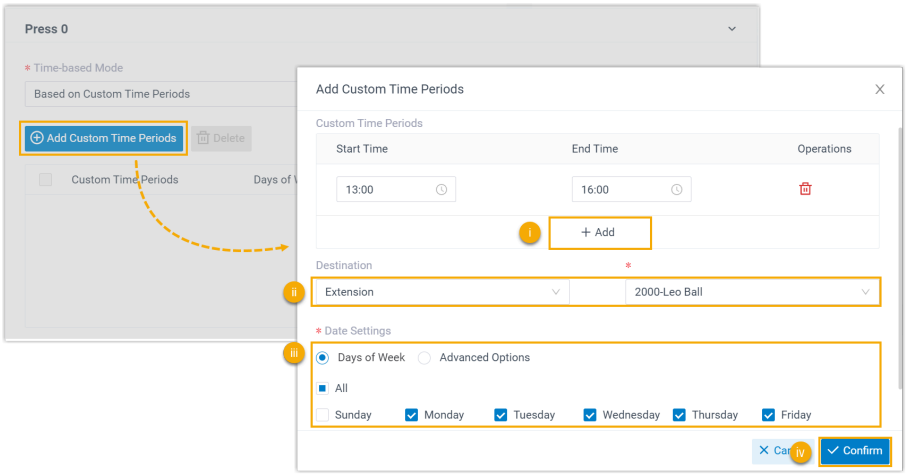
> **Note:**
> If you want to route incoming calls based on custom business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**.

Route calls based on custom time periods

a. In the **Time-based Mode** drop-down list, select **Based on Custom Time Periods**.

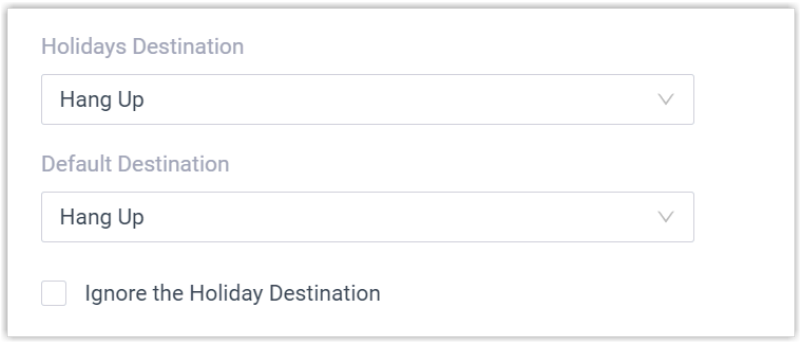


b. Click **Add Custom Time Periods** to create a custom time period based on the system's default time zone.



i. Click **Add** and specify the start time and end time.
ii. In the **Destination** drop-down list, specify the destination for calls within the custom time periods.
iii. In the **Date Settings** section, specify the workdays.
iv. Click **Confirm**.

c. Specify the following call routing destinations for the key event.



- **Holidays Destination**: Specify the call routing destination for calls during holidays.

> **Note:**
> If you want to route incoming calls based on custom time periods during holidays, select the checkbox of **Ignore the Holiday Destination**.

- **Default Destination**: Specify the call routing destination for calls outside custom time periods.

5. Repeat step **4** for all the desired keys.
6. Click **Save** and **Apply**.

Set up a Multi-language IVR

A multi-language IVR allows callers to select their language preferences and provides them with system prompts in their preferred language. You can set the IVR to route the callers to designated destinations based on different language selections, enabling better handling of customer calls and improved customer satisfaction.

Requirements

Yeastar P-Series PBX System is 37.14.0.24 or later.

Step 1. Design a multi-language IVR

Design a multi-language IVR and outlines the following information:

- Language options the IVR supports
- Key for each language option
- Call routing destination for each language option

> **Note:**
> Make sure that you have created the respective destinations on PBX.

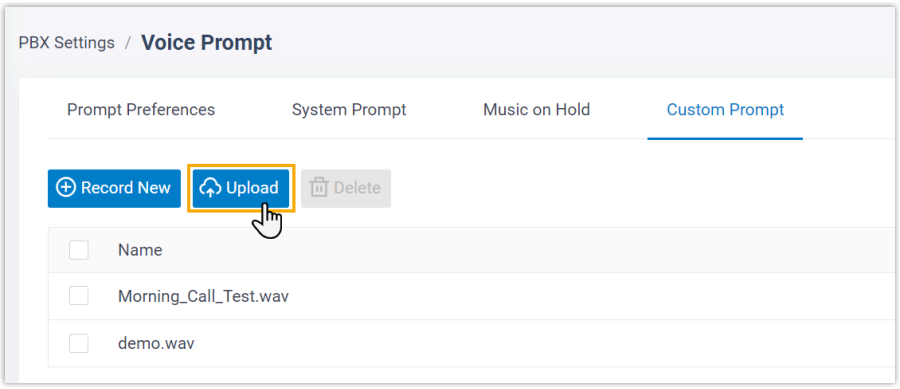
For example, design an IVR with 2 language options (English and Mandarin) supported.

Language Option	Key	Destination
English	key 1	IVR: English (6202)
Mandarin	key 2	Queue: Mandarin-agents (6400)

Step 2. Upload the IVR prompt

1. Prepare a voice prompt for the IVR to announce the available language options and their respective key actions.

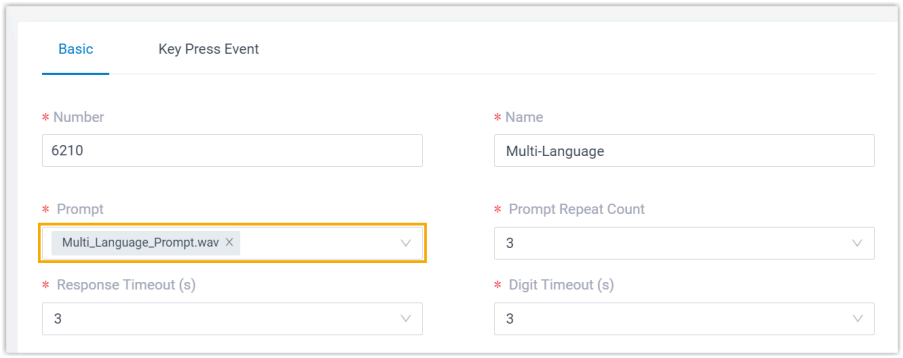
   For example, "Welcome. For English, please press 1. For Mandarin, please press 2".
2. Upload the voice prompt to the PBX system.
   a. Log in to PBX web portal, go to **PBX Settings > Voice Prompt > Custom Prompts**.
   b. Click **Upload**, and select the audio file to upload.



   c. Click **Save** and **Apply**.

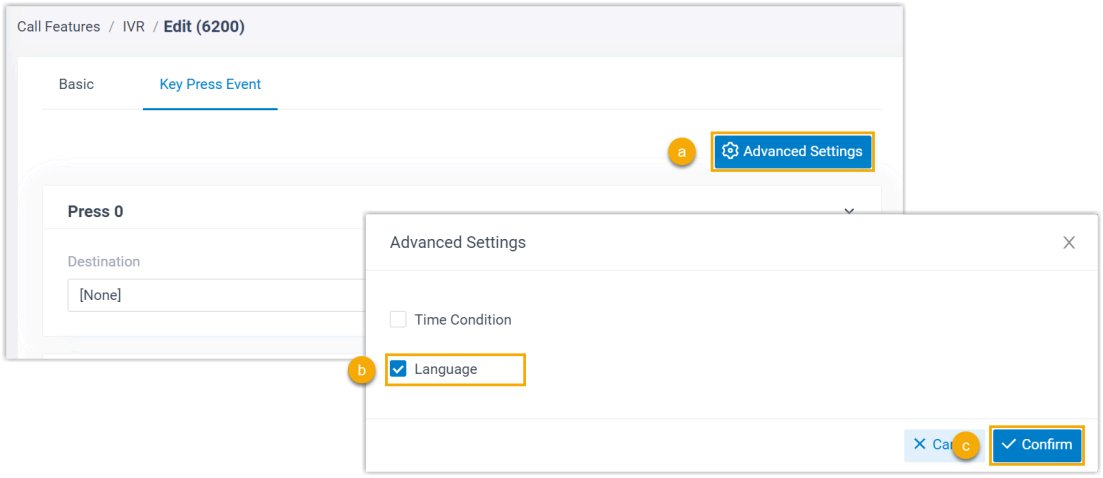
Step 3. Set up the multi-language IVR

1. On PBX web portal, go to **Call Features > IVR**, click **Add**.
2. In the **Basic** tab, configure the basic settings for the IVR.



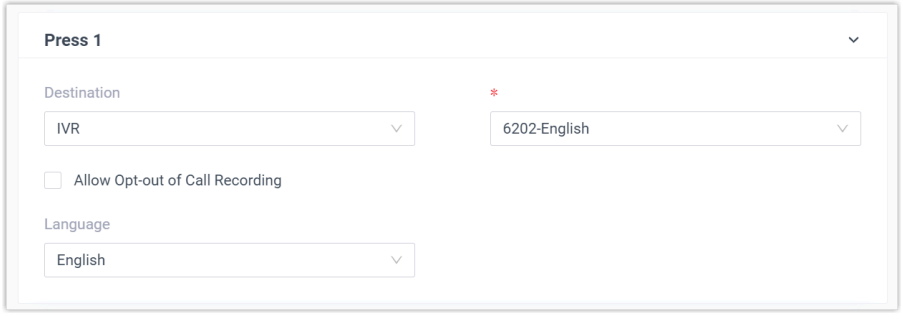
a. In the **Prompt** drop-down list, select the uploaded voice prompt.
b. Configure other settings as needed.

3. In the **Key Press Event** tab, enable multi-language setting for the IVR.



a. On the top-right corner, click **Advanced Settings**.
b. In the pop-up window, select the checkbox of **Language**.
c. Click **Confirm**.

4. Configure the corresponding key events based on your IVR design.



- **Destination**: Specify the call routing destination.

When callers press the key, the call will be routed to the specified destination.

- **Optional:** Select the checkbox of **Allow Opt-out of Call Recording**.

  If enabled, when the call is routed to the key press destination, the call would not be recorded even if **Call Recording** is enabled.
- **Language**: Select the system prompt language.

  > **Note:**
  > The displayed language options are synchronized from System Prompts (Path: **PBX Settings > Voice Prompt > System Prompt**).

  When callers press the key, all the subsequent system prompts will be played in the specified language.

5. Click **Save** and **Apply**.

Result

When calling into the IVR, callers hear the voice prompt for language preference selection. After they press the corresponding key, all subsequent system prompts (except the custom ones) will be played in the selected language, and the call will be routed to the respective key press destination.

Set up IVR Custom Key

Yeastar P-Series PBX System allows you to add custom keys for IVR to authenticate callers with PIN codes (either a single PIN or a list of PINs) before routing them to specific destinations. This is particularly useful to differentiate inbound calls and ensure that only verified callers can access premium services or dedicated support lines. This topic describes how to set up IVR custom keys.

Requirements

The firmware version of PBX server is 37.16.0.70 or later.

Prerequisites

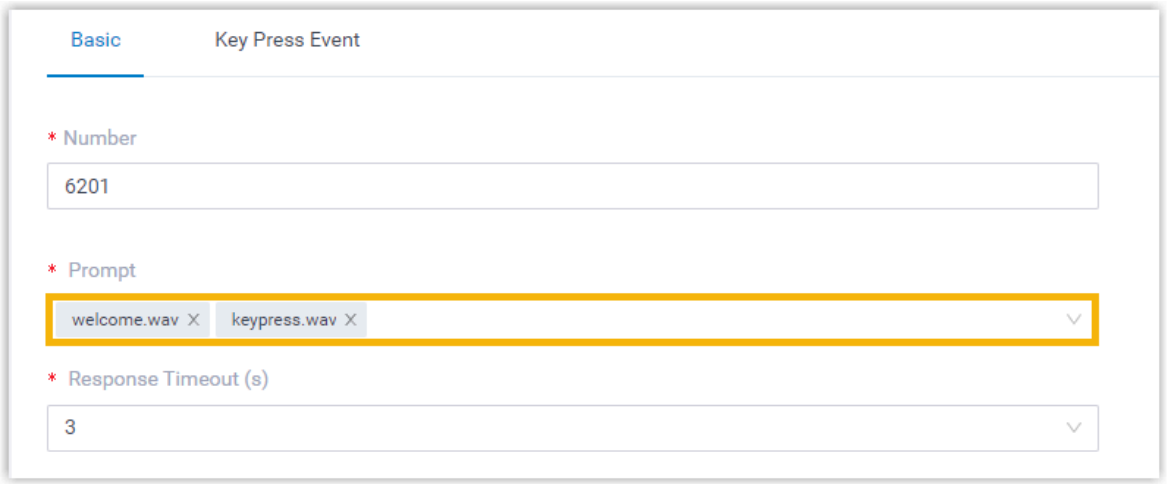
- Upload or record an IVR prompt that would instruct callers to press PIN codes to reach the corresponding destination.
- **Optional:** Add a PIN List that would authenticate callers before routing them to specific destinations.

> **Note:**
> If you prefer a single PIN for custom keys, you don't need to add a PIN list.

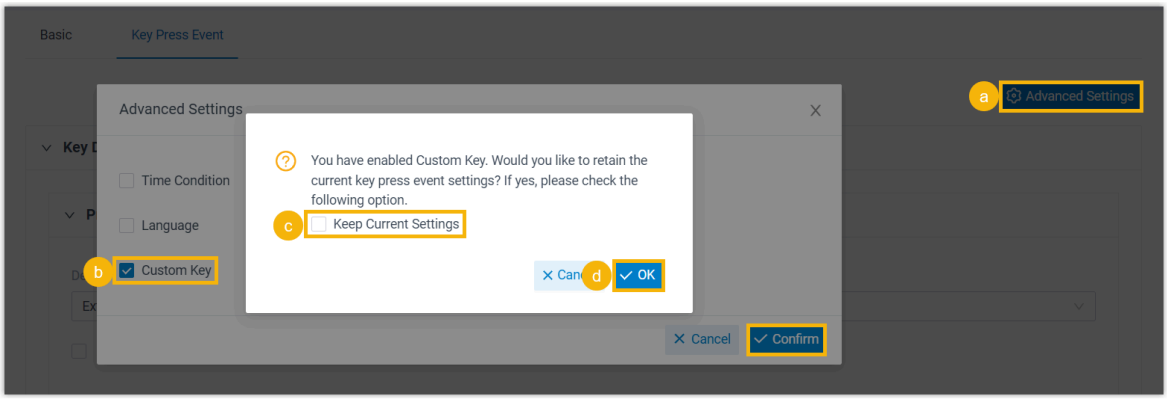
Procedure

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. Under **Basic** tab, select prompt(s) from the **Prompt** drop-down list to instruct callers to press custom key.

> **Note:**
> You can select up to 5 audio files, and the system plays the audio files in order.



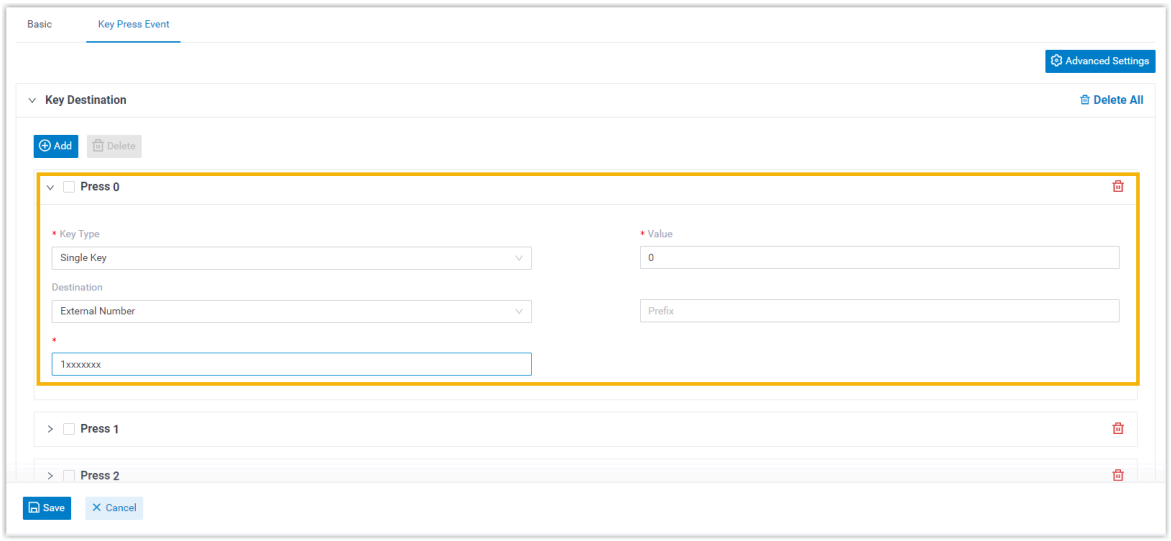
3. Under **Key Press Event** tab, enable custom keys.



   a. At the top-right corner, click **Advanced Settings**.

b. In the pop-up window, select the checkbox of **Custom Key**, then click **Confirm**.
c. **Optional:** Select the checkbox of **Keep Current Settings** to retain the current key press event settings.
d. Click **OK**.

4. Set up custom keys.



a. In the **Key Type** drop-down list, select a key type.
   - If you select **Single Key**, enter a PIN code in the **Value** field.

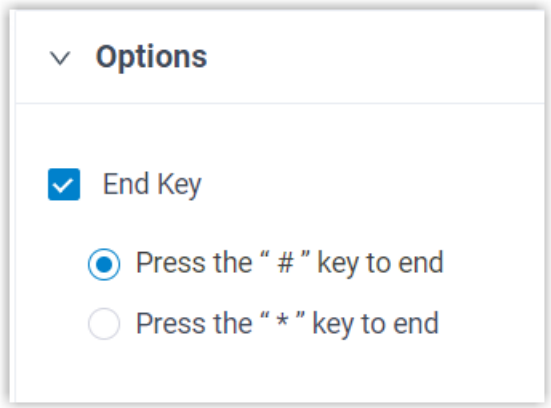
     > **Note:**
     > The length of PIN code should not be greater than 21.

   - If you select **PIN List**, select a PIN list from the **PIN List** drop-down list.

b. In the **Destination** drop-down list, specify a destination for the custom key.

5. **Optional:** Scroll down to the **Options** section, enable end key to allow callers to complete their input and be directed to the corresponding destination.

> **Note:**
> If **End Key** is enabled, `*` or `#` should not be included in your custom key.



a. Select the checkbox of **End Key**.
b. Select **Press the "#" key to end** or **Press the "*" key to end**.

6. Click **Save** and **Apply**.

Result

Callers who know the PIN code can press the key when enter an IVR and will be routed to the designated destination.

> **Note:**
> If you set key events based on time conditions, the PBX will match the key firstly when callers enter the IVR. If the key is right, calls will be routed to destinations according to time conditions; while it is wrong, calls will be routed to Response Timeout or Invalid Input Destination.

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 and switch call recording status on IP phones and Linkus Clients.
- **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.

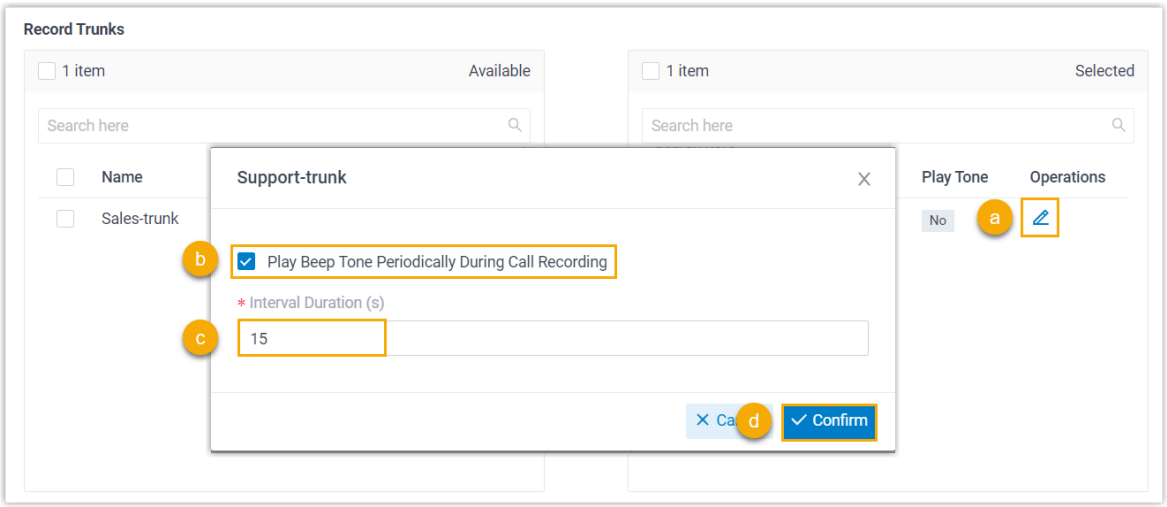
1. Log in to PBX web portal, go to **Call Features > Recording**.
2. **Optional:** Select the checkbox of **Enable Recording of Internal Calls** to automatically record the internal calls.
3. In the **Record Extensions** section, select the desired extensions from the **Available** box to the **Selected** box.
4. Click **Save** and **Apply**.

Set up call recording for trunks

The system automatically records the external calls on the selected trunks.

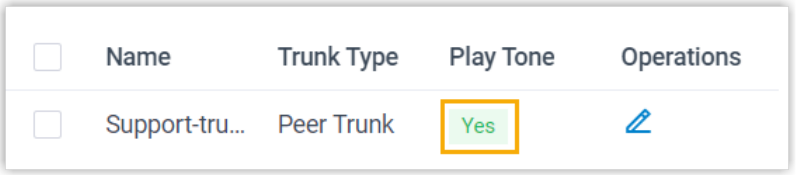
1. Log in to PBX web portal, go to **Call Features > Recording**.
2. In the **Record Trunks** section, select the desired trunks from the **Available** box to the **Selected** box.
3. **Optional:** To periodically play beep tones to inform both parties when the call on the selected trunk is being recorded, do as follows.

> **Note:**
> This setting will not take effect on the calls where multiple participants are involved, such as conference calls and multi-party calls.



a. In the **Selected** box, click beside a selected trunk.
b. In the pop-up window, select the checkbox of **Play Beep Tone Periodically During Call Recording**.
c. In the **Interval Duration (s)** field, specify the interval for playing the beep tone.
d. Click **Confirm**.

   The **Play Tone** of the selected trunk displays **Yes**, indicating that periodic playback of beep tone is enabled for the trunk.



4. 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 web 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 web 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 web 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 web 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 web 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**.

Allow Users to Switch Call Recording Status

By default, if you set up call recording for extensions, trunks, conferences, or queues, the specified calls would be recorded as soon as they are established, and all the users can NOT switch call recording status. To avoid sensitive information being recorded or to allow users to start recording their calls when necessary, you can grant permissions to specific users, so that they can start, pause, or resume recording during a call.

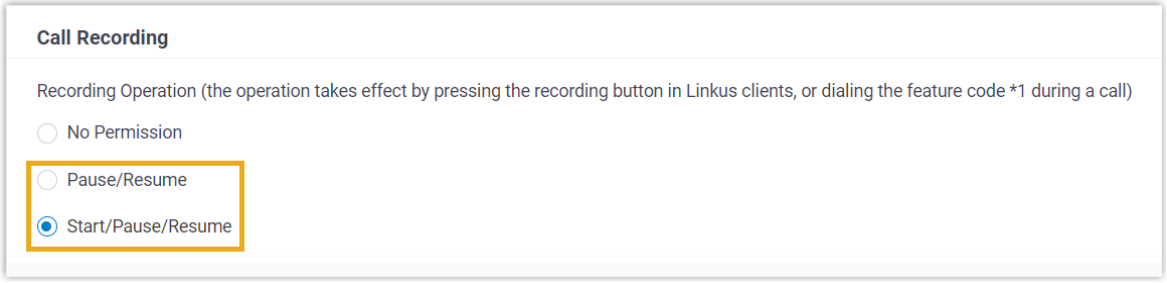
Restrictions

> **Note:**
> Extension users can NOT switch the recording status during a conference call, even if you have granted them permission.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit a desired extension.
2. Click **Features** tab.

3. In the **Call Recording** section, grant the operation permission of call recording to the extension user.



   - **Pause/Resume**: Allow the user to pause or resume recording during a call that is specified to be recorded.

     > **Tip:**
     > To specify the calls to be recorded, see Set up Call Recording.

   - **Start/Pause/Resume**: Allow the user to start, pause, or resume recording during any calls (except conference calls), be the calls specified to be recorded or not.

4. Click **Save** and **Apply**.

Result

- The user can switch call recording status in the following ways:
  - Press the recording button on Linkus Clients
  - Dial a feature code

  > **Note:**
  > The default feature code for switching call recording status is `*1`.
  > You can change, enable, or disable the code on PBX web portal (Path: **Call Features > Feature Code > Recording > Switch Extension's Recording Status**).

- By default, the user can view the call recording file that is generated when a call ends. To restrict the user from viewing recording files, see Restrict Users from Viewing Recording Files.

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 web 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 been associated with a phone, see the following topics to bind a phone with the extension.
    - Auto Provision IP Phones in Local Network (PnP Method)
    - Auto Provision IP Phones in Local Network (DHCP Method)
    - Auto Provision IP Phones Remotely (RPS FQDN Method)
    - Auto Provision IP Phones Remotely (RPS Method)
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**: 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 web 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.

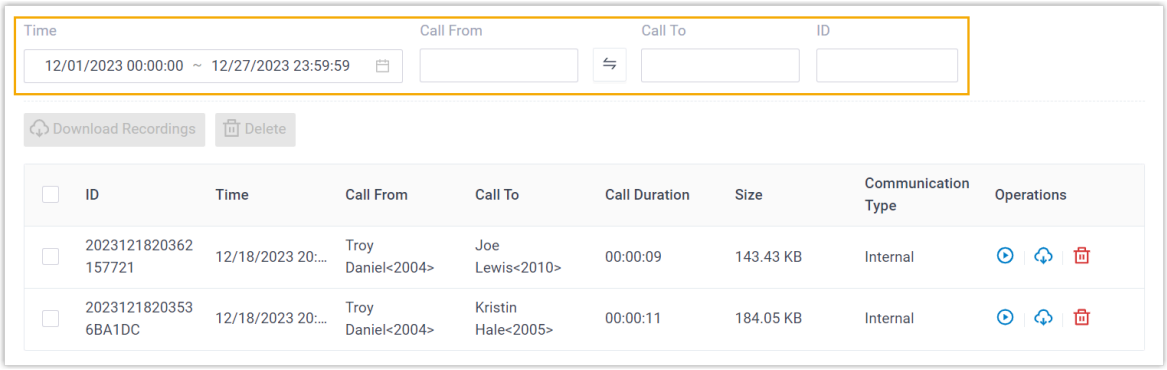
> **Tip:**
>
> To swap the callee for the caller, click ⇋.

- **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 web portal, go to **Reports and Recordings > Recording Files**.
2. **Optional:** Set the criteria to filter the desired recordings.



3. 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**.

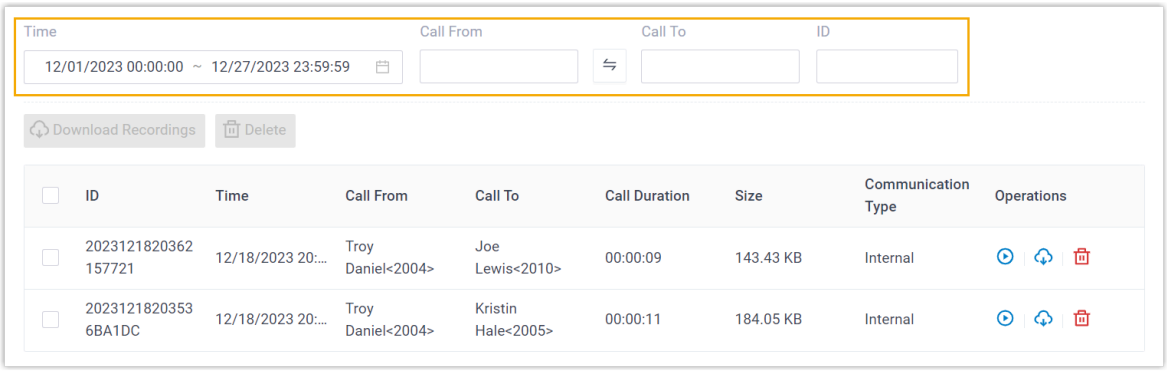
        The system places a call to the extension.
     b. Pick up the call to listen to the call recording on the phone.

Download recording files

You can download recording files to your local computer or to an external server (such as FTP server, SFTP server, Amazon S3, or Google Cloud Storage).

This section introduces how to download recording files to your local computer. For external server, see Yeastar P-Series PBX System Remote Archiving Overview.

1. Log in to PBX web portal, go to **Reports and Recordings > Recording Files**.
2. **Optional:** Set the criteria to filter the desired recordings.

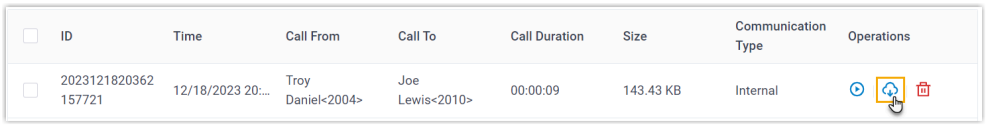


3. Download recording file(s) as needed.

> **Note:**
> You can download a maximum of 600 MB recording files or a maximum of 100 recording files at a time. The recordings that exceed the limit will not be downloaded.

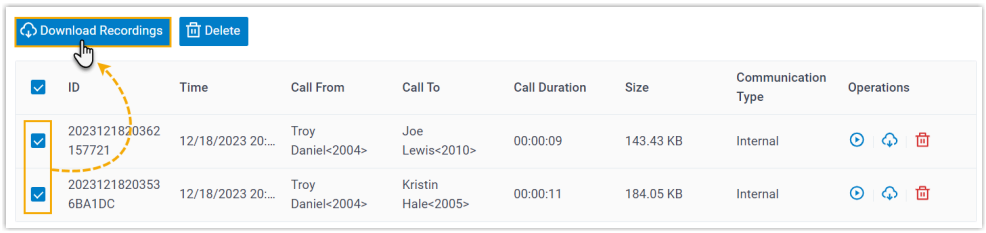
Download a recording file

Click beside the recording file.



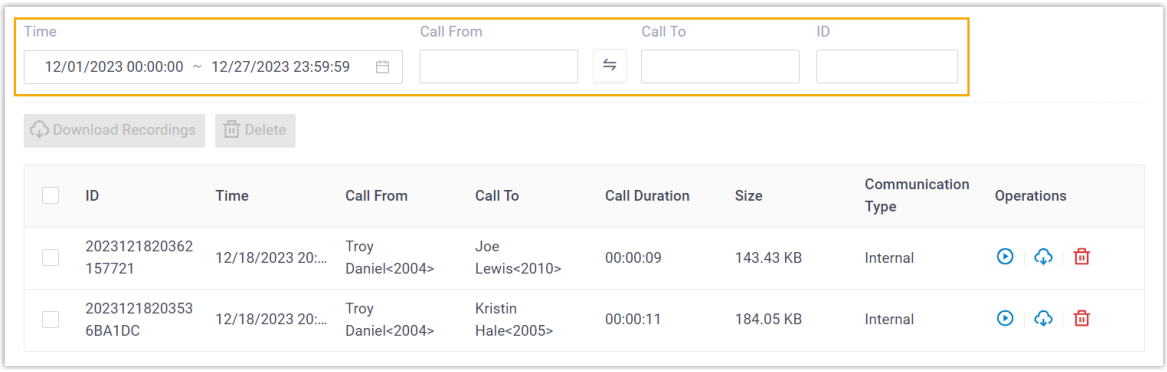
Download multiple recording files

Select the checkboxes of the recording files that you want to download, then click **Download Recordings**.



Delete recording files

1. Log in to PBX web portal, go to **Reports and Recordings > Recording Files**.
2. **Optional:** Set the criteria to filter the desired recordings.



3. 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. When the storage device reaches 80% of its maximum storage capacity or reaches the maximum preservation days, the PBX automatically deletes the oldest recording files. You can customize the maximum usage of device and preservation days. This topic describes how to set up auto cleanup of recording files.

Procedure

1. Log in to PBX web portal, go to **System > Storage > Auto Cleanup > Recording Auto Cleanup**.
2. In the **Max Usage of Device (%)** field, enter a value to specify the maximum storage percentage of the device that is allowed to store recording files.
3. In the **Recordings Preservation Days** field, 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 Cleanup 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 back up 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 web 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

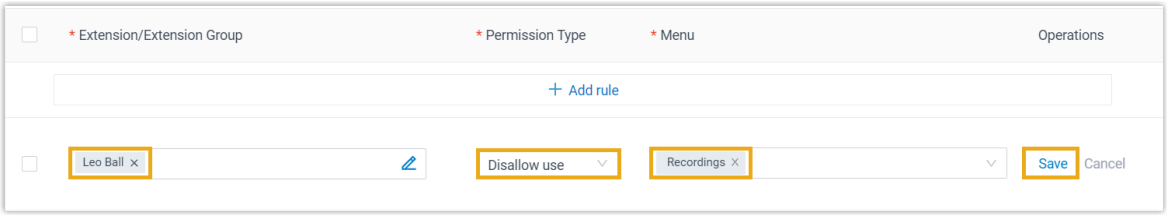
By default, all the users have access to viewing their own recording files. For security reasons, you can restrict specific users from view recording files.

Requirements

Server / Client	Version Requirement
PBX Server	Version 37.12.0.23 or later
Linkus Mobile Client	• **Linkus iOS Client**: Version 5.2.9 or later • **Linkus Android Client**: Version 4.13.16 or later
Linkus Desktop Client	• **Windows Desktop**: Version 1.2.14 or later • **Mac Desktop**: Version 1.2.10 or later

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Menu Visibility**.
2. Click **Add rule** to create a menu visibility rule.
3. Set up the rule, then click **Save**.



   - **Extension/Extension Group/Organization**: Click to select desired extensions, extension groups, or departments, for which you want to restrict the viewing permission of recordings.
   - **Permission Type**: Select **Disallow use**.
   - **Menu**: Select **Recordings**.

Result

The extension user can not view recording files on his or her Linkus UC Clients.

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, failover destination, and missed call alerts.

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 four 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.
- **Ring sequentially**: When receiving an incoming call, the system rings the first available member in the list. 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.
- **Memory hunt**: When receiving an incoming call, the system rings the first available member in the list. If no answer within the ring time, the system rings the first and second available member. If still no answer within the ring time, the system rings the first, second, and third available member, and the like, until all available members in the list rang. If no one answers the call, the system routes the call to the failover destination.
- **Custom**: When receiving an incoming call, the system rings members according to their individually set delay times and stops ringing after their individual ring timeouts. If no one answers the call, the system routes the call to the failover destination.

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**

Missed call alerts

When there are missed calls from ring group, the system can record the missed calls and notify members via email.

To record missed calls from ring group, see Record Missed Calls.

To set up email alerts for missed calls from ring group, see Set up Email Notifications for Missed Calls.

Create a Ring Group

This topic describes how to create a ring group.

Procedure

1. Log in to PBX web 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.
     - **Memory Hunt**: Ring the first available extension in the list. If no answer within the ring time, progressively add the next available extension to ring, until all the available extensions in the list rang.
     - **Custom**: Ring extensions according to their individual ring delays and stop ringing after their individual ring timeouts.

       > **Note:**
       > You can set ring delays and timeouts for each group member in the **Members** section.
   - **Ring Timeout (s)**: Set a number of seconds that the system waits before ringing next member or routing the call to **Failover Destination**.

> **Note:**
> This option is available only when **Ring Strategy** is set to **Ring All**, **Ring Sequentially**, or **Memory Hunt**.

- **Join Announcement**: Optional. Set the announcement to be played to callers, which will be played only once.
  - **Play full Join Announcement to the caller before ringing extensions**: Set whether to play full join announcement to callers before ringing members.
- **Ringback Tone**: Optional. Specify a prompt that will be played to callers before members answer the call.

  You can select an existing prompt from the drop-down list, or click **Record New** / **Upload** to record or upload a new prompt.

  > **Note:**
  > - The Ringback Tone is played after the Join Announcement.
  > - The existing prompts are synchronized from **PBX Settings > Voice Prompt > Music on Hold / Custom Prompt**. If you record or upload a new prompt here, it will also be synchronized to the location.

- **Music on Hold**: Optional. Specify the music that will be played to callers when the call is put on hold.

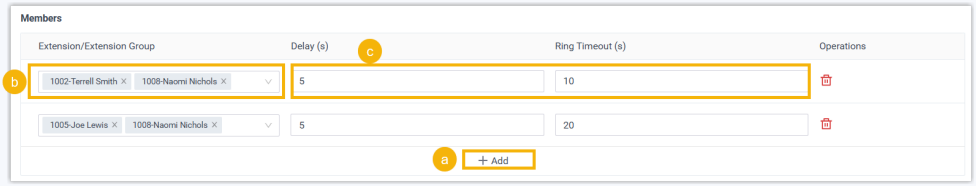
  You can select an existing MoH playlist from the drop-down list, or click **Create New** to add a new one.

  > **Note:**
  > The existing playlists are synchronized from **PBX Settings > Voice Prompt > Music on Hold**. If you create a new playlist here, it will also be synchronized to the location.

- **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.

- **Members**: Select the desired extensions from the **Available** box to the **Selected** box.

> **Note:**
> If you set **Ring Strategy** to **Custom**, you can set ring delay and timeout for different extensions, as shown below.
>
> 
>
>
> a. Click **Add**.
> b. Select extensions or extension groups from the drop-down list.
>
> > **Note:**
> > Each extension or extension group can be selected in at most 5 different member rules.
>
> c. Configure ring delay and timeout for group members.
> - **Delay (s)**: Set the time delay in seconds (0 - 600, where 0 indicates ring immediately). The member will start ringing after the configured delay time.
>
> > **Note:**
> > If you select an extension group, all extensions within the group will ring simultaneously after the ring delay.
>
> - **Ring Timeout (s)**: Set the ring timeout in seconds (1 - 600). The member will stop ringing after the configured ring timeout. If all members time out, the call will be routed to the Failover destination.
>
> > **Note:**
> > If you select an extension group, all extensions within the group will stop ringing simultaneously when the timeout is reached.

- **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.
- **Record Missed Calls**: Decide whether to record missed calls from ring group.

> **Note:**
>
> - This option is available only when both **Ring Strategy** and **Failover Destination** are set to the followings:
>   - **Ring Strategy** is set to **Ring All**, **Memory Hunt**, or **Custom**.
>   - **Failover Destination** is set to **Extension**, **Queue**, or **Ring Group**.
> - You can also set up email alert on missed calls from ring group for members. To achieve this, enable this option, then turn on email notifications on missed calls for members. For more information, see Set up Email Notifications for Missed Calls.

- **Time Condition**: Decide whether to route the calls received in non-business hours to different destination based on the time in a specific time zone.

Setting	Description
Time Zone	Select a desired time zone. The business hours and holidays settings of the selected time zone (Path: **Call Control > Business Hours and Holidays**) will be applied to the ring group. **Note:**

Setting	Description
	The ring group always receive calls in the business hours.
Outside Business Hours Destination	Select the destination for calls received during the time periods that are not defined as business hours or holidays in the selected time zone.
Holidays Destination	Select the destination for calls received during holidays defined in the selected time zone.
Ignore the Holiday Destination	If you want to route incoming calls based on the business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**. Incoming calls during holiday will be distributed to other destinations according to your office hour setting.
Play Holiday Prompt During Holidays	To play a prompt to callers before routing the inbound calls to the holiday destination, select the checkbox of **Play Holiday Prompt During Holidays**. **Note:** Make sure that you have set a prompt for the holiday (Path: **Call Control > Business Hours and Holidays > Holidays > Type > Prompt**). Otherwise, the inbound calls will be directly routed to the holiday destination without playing a prompt.

3. Click **Save** and **Apply**.

What to do next

Set up an inbound route, and specify the destination to the ring group.

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 web 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 web 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.

What is 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.

Configuration guide

For more detailed information and configurations of call queue and Yeastar Call Center, see Call Center Administrator Guide.

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 about feature code, see Feature Code Reference.

Procedure

1. Log in to PBX web 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
Switch Extension's Recording Status	*1	• An extension user with **Pause/Resume** recording operation permission dials *1 to pause or resume recording during a call that is specified to be recorded. • An extension user with **Start/Pause/Resume** recording operation permission dials *1 to start,

Name	Default Code	Usage
		pause, or resume recording during any calls (except conference calls), be the calls specified to be recorded or not.

Call Flip

Name	Default Code	Usage
Call Flip	*01	Dial *01 to flip an active call from current device to another device.

Voicemail

Name	Default code	Usage
Check Voicemail/Subscribe Voicemail Status	*2	• 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	• 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.
Transfer Bounce Back (Applicable to Both Blind/Semi-attended Transfer)	/	If enabled, when an extension user performs a blind transfer/semi-attended transfer and the transfer recipient doesn't answer, the call will be transferred back to the extension user.

Call Forwarding

Name	Default code	Usage
Enable "Forward All Calls"	*31	• Dial *31 to forward all calls to one's own voicemail.

Name	Default code	Usage
		• Dial *311000 to forward all calls to extension 1000.
Disable "Forward All Calls"	*031	• Dial *031 to disable the automatic call forwarding of all calls.
Enable "Forward When Busy"	*32	• Dial *32 to forward calls to one's own voicemail when busy. • Dial *321000 to forward calls to extension 1000 when busy.
Disable "Forward When Busy"	*032	• Dial *032 to disable the automatic call forwarding when busy.
Enable "Forward No Answer"	*33	• Dial *33 to forward the no-answered calls to one's own voicemail. • Dial *331000 to forward the no-answered calls to extension 1000.
Disable "Forward No Answer"	*033	• Dial *033 to disable the automatic call forwarding of no-answered calls.

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.
Directed Call Parking	*05	Dial *056000 during a call to park a call to parking number 6000.

Call Monitoring

Name	Default code	Usage
Listen	*51	An authorized user dials *511001 to listen to the call of extension 1001 in real time. The authorized user can NOT talk with both parties.

Name	Default code	Usage
Whisper	*52	An authorized user dials *521001 to listen to the call of extension 1001 in real time. The authorized user can talk with extension 1001 without being heard by the other party.
Barge-in	*53	An authorized user dials *531001 to listen to the call of extension 1001 in real time. The authorized user can talk with both parties.

Force Drop

Name	Default code	Usage
Call Force Drop	*54	• An authorized user dials *541001 to force drop the current call of extension 1001. • An authorized user dials *54 while monitoring the call of extension 1001 to force drop the call.

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	Dial *076400 to pause or unpause calls from queue 6400.

Hot Desking

Name	Default code	Usage
Guest In	*84	A user can dial *84 on a hot desking phone to register his or her extension to the phone.
Guest Out	*084	A user can dial *084 on a hot desking phone to de-register his or her extension from the phone.

Busy Camp-on

Name	Default code	Usage
Enable Busy Camp-on	*79	A user dials *791000 to camp on extension 1000 in case he or she gets a busy signal when dialing extension 1000. The PBX will automatically call the user back when extension 1000 becomes available.
Disable Busy Camp-on	*079	A user dials *079 to cancel all Busy Camp-on requests that he or she has initiated.

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**.
Off Work	*96	Dial *96 to switch one's own presence status to **Off Work**.

Query my extension number

Name	Default code	Usage
Query my extension number	*97	If enabled, extension user can dial *97 to query the extension number registered on the current endpoint. The system will play the prompt "Your extension number is *{extension_number}*." twice, then hang up the call.

Name	Default code	Usage
Line Status Detection Call	/	If enabled, the PBX system will initiate a line detection call to the extension after hanging up the number querying call, which detects whether the line functions normally or not. • If the line has no problem, the system will play the prompt "The line you are using is functioning normally.", and then hang up the call. • If the line has a problem, no line detection call will be sent to the extension.

Switch Business Hours and Holidays Status

Name	Default code	Usage
Keep the Business Hours Status or the Time Condition after switching	/	If enabled, keep the status after users switched the PBX's Business Hours status or dialed a feature code to switch the time condition of an inbound route.
Switch Business Hours and Holidays Status	*99	Dial *99 to override time condition for the Business Hours and Holidays configured in system's default time zone. **Note:** This feature code applies only to the system's default time zone. For additional time zones, you can check the corresponding feature code under the specific time zone settings (Path: **Call Control > Business Hours and Holidays**).
Time Condition Switching Prefix	*8	Dial a feature code starting with *8 to switch the time condition of inbound routes that are based on Custom Business Hours or Custom Time Periods.
BLF Light Color of Switching Global Business Hours Status	/	Set the BLF light color to indicate whether being at the destination or not when in Business Hours or Outside Business Hours (or custom time conditions).

Hotel Management

Name	Default code	Usage
Room Status	*63	Dial *63 and room status feature code on hotel room phone to update the room status. **Note:** The room status feature code is automatically generated when adding room status in **Hotel Management > Room Management > Customize Room Status > Feature Code**.

PMS Integration

Name	Default code	Usage
Housekeeping Status	*61	Dial *611 on hotel room phone to update the room status to "Dirty/Vacant". **Note:** • The housekeeping status code is available only when the PBX is integrated with a PMS system using FIAS protocol. • The housekeeping status code must be used in conjunction with maid status code, in the format of `{housekeeping_status_code}{maid_status_code}`. The maid status codes specified by FIAS protocol are listed below: ◦ `1`: Dirty/Vacant ◦ `2`: Dirty/Occupied ◦ `3`: Clean/Vacant ◦ `4`: Clean/Occupied ◦ `5`: Inspected/Vacant ◦ `6`: Inspected/Occupied
Minibar	*62	Depending on the **Minibar Billing Type** (Path: **Integrations > PMS**) set on the PBX, hotel staffs can dial specific feature codes on hotel room phone to post minibar charges.

Name	Default code	Usage
		Note: The minibar feature code is available only when the PBX is integrated with a PMS system using FIAS protocol. • If **Minibar Billing Type** is set to **Based on Item and Quantity**, hotel staffs can dial *{minibar_feature_code}*{item_code}*{quantity}* on room phone to post the item consumed and its quantity to the guest's bill in PMS. For example, if a guest bought 2 cans of Coke (item code 4000), hotel staffs can dial `*62*4000*2`. • If **Minibar Billing Type** is set to **Based on Total Amount**, hotel staffs can dial *{minibar_feature_code}{total_amount}* on room phone to post the total minibar charge to the guest's bill in PMS. For example, if a guest bought 2 cans of Coke (unit price $3), hotel staffs can dial `*626`.

Boss-Secretary Feature

Name	Default code	Usage
Enable Boss-Secretary Feature	*59	**Note:** This feature code is only available for extensions set as the boss extension. Dial *59 to enable the Boss-Secretary feature.
Disable Boss-Secretary Feature	*059	**Note:** This feature code is only available for extensions set as the boss extension. Dial *059 to disable the Boss-Secretary feature.

Pause Reason

Yeastar P-Series PBX System provides queue agents with the following default pause reasons and the corresponding feature codes. You can modify the default settings, or add new ones.

> **Note:**
>
> - Yeastar P-Series PBX System supports up to 20 feature codes for pause reasons.
> - The feature codes are synchronized with the settings on **Call Features > Queue > Pause Reason**.

After you set the feature codes, agents can dial feature codes with a format of `Pause feature code` + `queue number` + `pause reason feature code` to pause with a specific reason.

Pause reason	Default code	Usage
Lunch	*01	An agent can dial *076400*01 to pause receiving calls from queue 6400 for lunch.
Break	*02	An agent can dial *076400*02 to pause receiving calls from queue 6400 for a break.
Wrap up	*03	An agent can dial *076400*03 to pause receiving calls from queue 6400 for after-call processing.

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 web 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.
    - **Custom Prompt Language**: Optional. Enable this option and set the language of system prompts heard by participants when they join the conference call.

      > **Note:**
      > The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**).

    - **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 web 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 web 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 web 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 web portal, go to **Call Features > Speed Dial**.
2. Click **Prefix**.
3. In the **Speed Dial Prefix** field, enter a prefix according to your needs.

> **Note:**
> - Only numbers and special characters `*` `#` are allowed.
> - The maximum character length is 7.

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 web 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 web 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 web portal, go to **Call Features > Speed Dial**.
2. To delete a speed dial number, do as follows:
   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 as follows:
   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 web 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 web 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.

Related information

Import and Export -FAQ

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.
- **Transfer Bounce Back (Applicable to Both Blind/Semi-attended Transfer)**: If enabled, when an extension user performs a blind transfer/semi-attended transfer and the transfer recipient doesn't answer, the system sends the call back to the extension user.

Set up Call Transfer

This topic describes how to set up call transfer.

Set up attended transfer

1. Log in to PBX web 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 web 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. In the **Transfer Bounce Back (Applicable to Both Blind/Semi-attended Transfer)** option, set whether to transfer the call back to the transferor when the transfer recipient doesn't answer the call.
6. 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.

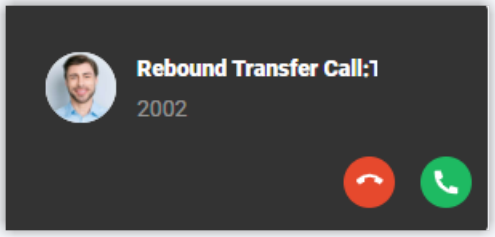
Procedure

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.

> **Note:**
> By default, if the transfer recipient doesn't answer the call, the call will be routed to the call forwarding destination of the transfer recipient. If you have enabled **Transfer Bounce Back (Applicable to Both Blind/Semi-attended Transfer)**, the call will be transferred back to you with Caller ID displayed as **Rebound Transfer Call: *{caller_id_name}***.
>
> 
>

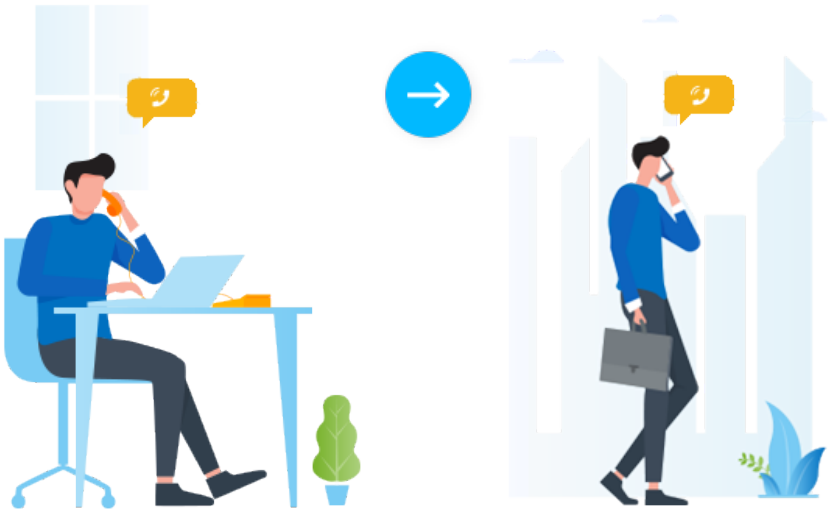
Call Flip

Call Flip Overview

Call Flip feature allows users to flip their ongoing calls from current device to another (with their extensions registered), without any interruption to the conversation.

Scenario

Assume that a sales representative is in a call with a customer on the desk phone, but has to get out of the office. In this case, the sales representative can flip the call to his mobile phone, keeping talking without customer knowing the switchover.



Methods of Call Flip

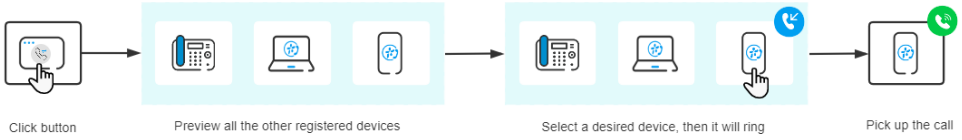
Extension users can flip an active call in the following ways:

- Flip an active call by clicking 'Call Flip' button
- Flip an active call by dialing 'Call Flip' feature code

Flip an active call by clicking 'Call Flip' button

With a simple click of the **Call Flip** button, users can preview all the other devices where their extensions are registered, and select a device to flip the call.

We provide a flowchart to help you understand the workflow:



This method is supported on the following endpoints:

- **Linkus Mobile Client**

  For more information, see Flip an Active Call between Devices.
- **Linkus Desktop Client**

  For more information, see Flip an Active Call between Devices.
- **Linkus Web Client**

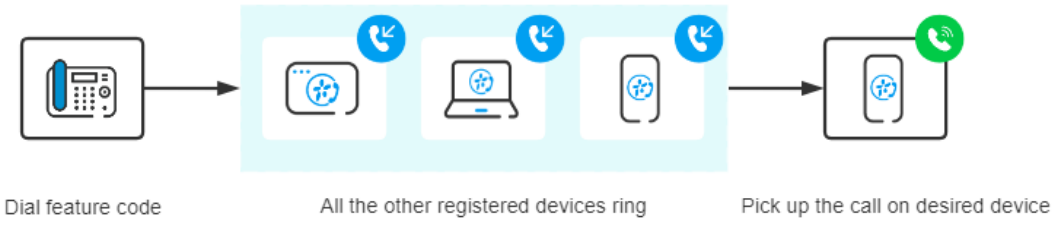
  For more information, see Flip an Active Call between Devices.

> **Note:**
> If Linkus Web Client is associated with 'Yeastar Linkus for Google', see Flip an Active Call between Devices.

Flip an active call by dialing 'Call Flip' feature code

By dialing the **Call Flip** feature code, all the other devices where users' extensions are registered will simultaneously ring. Users pick up the call on a desired device, then the call would be flipped.

We provide a flowchart to help you understand the workflow:



With the **Call Flip** feature code enabled on Yeastar P-Series PBX System, this method is supported on all endpoints.

For more information about how to enable the **Call Flip** feature code, see Enable 'Call Flip' feature code.

For more information about how to flip an active call by dialing the feature code, see Flip an Active Call by Dialing a Feature Code.

Enable or Disable 'Call Flip' Feature Code

This topic describes how to enable or disable 'Call Flip' feature code.

Enable 'Call Flip' feature code

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. In the **Call Flip** section, select the checkbox, then configure the feature code.



3. Click **Save** and **Apply**.

   During a call, extension users can dial the feature code to flip the active call to another device where their extensions are registered. For more information, see Flip an Active Call by Dialing a Feature Code.

Disable 'Call Flip' feature code

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. In the **Call Flip** section, unselect the checkbox.



3. Click **Save** and **Apply**.

   Extension users can NOT flip an active call by dialing the feature code.

Flip an Active Call by Dialing a Feature Code

This topic describes how to flip an active call from current device to another (with the same extension registered) by dialing a feature code.

Requirements

- **PBX Server**: 37.8.0.25 or later
- **Extension**: Extension has been registered on more than one device.

Procedure

1. During an active call, dial the **Call Flip** feature code (default: `*01`).

   All the other devices where the extension is registered simultaneously ring.
2. Answer the call on a desired device.

Result

The call is flipped to the device, and the rest of the devices stop ringing.

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 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.

Note:

- If the extension group has multiple ringing calls at the same time, the first ringing call will be picked up.

- The extension group does NOT include the group that contains all the PBX extensions.

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 web 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 web 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 web 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 o 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 been associated with a phone, see the following topics to bind a phone with the extension.
   - Auto Provision IP Phones in Local Network (PnP Method)
   - Auto Provision IP Phones in Local Network (DHCP Method)
   - Auto Provision IP Phones Remotely (RPS FQDN Method)
   - Auto Provision IP Phones Remotely (RPS Method)
   - Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
   - Auto Provision IP Phones Remotely (Provision Link Method)
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 extension group members receive a call, the user can press the Feature key directly to answer the call.

- When the call is picked up, the IP phones of other extension group members display a missed 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 web 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 web 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**: Select the desired extension.
- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

d. Click **Save**.

2. If the extension hasn't been associated with a phone, see the following topics to bind a phone with the extension.
   - Auto Provision IP Phones in Local Network (PnP Method)
   - Auto Provision IP Phones in Local Network (DHCP Method)
   - Auto Provision IP Phones Remotely (RPS FQDN Method)
   - Auto Provision IP Phones Remotely (RPS Method)
   - Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
   - Auto Provision IP Phones Remotely (Provision Link Method)
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 all, the BLF key fast flashes red. The user can press the BLF key directly to answer the call.
- When the call is picked up, the IP phone where the monitored extension is registered displays a missed 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 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

> **Tip:**
> You can change, enable, or disable the code on PBX web 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.

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.

> **Tip:**
> The default feature code for directed call park is `*05`. You can change, enable, or disable the code on PBX web 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.

> **Tip:**
> The default feature code for call park is `*5`. You can change, enable, or disable the code on PBX web portal: **Call Features > Feature Code > Call Parking > Call Parking**.

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 web 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**.

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 web 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 Music on Hold for Call Parking

This topic describes how to customize music on hold for call parking on Yeastar P-Series PBX System.

By default, the system plays a default music on hold (set on **PBX Settings > Voice Prompt > Prompt Preferences > Music on Hold**) to the parked party when a call is parked. You can refer to this topic to customize the music for call parking.

Requirements

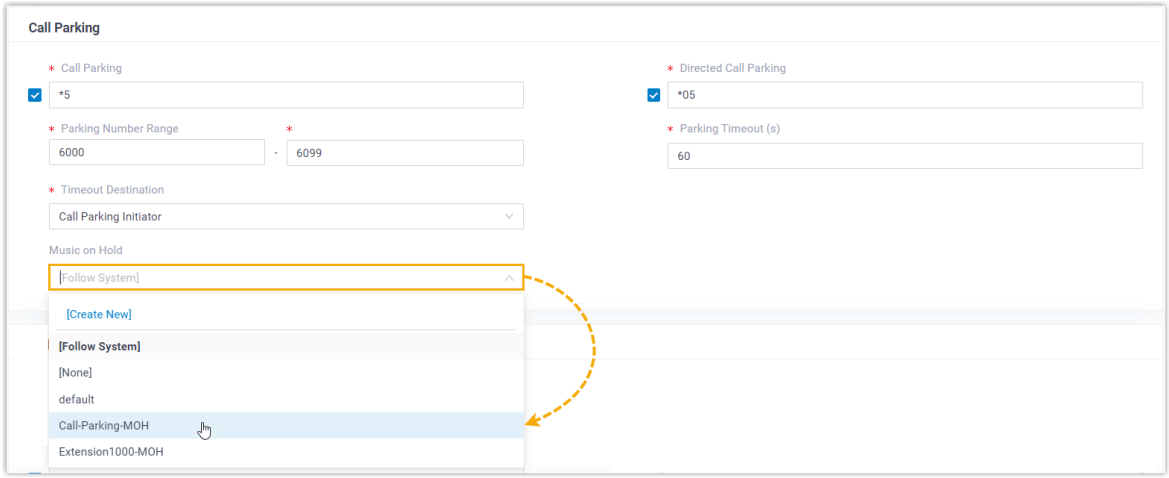
The firmware version of PBX server is 37.15.0.22 or later.

Prerequisites

You have prepared and uploaded a custom Music on Hold (MoH) playlist.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code > Call Parking**.
2. In the **Music on Hold** drop-down list, select the MoH playlist that you have uploaded.



3. Click **Save** and **Apply**.

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 web 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 o 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 been associated with a phone, see the following topics to register the extension to a phone.
   - Auto Provision IP Phones in Local Network (PnP Method)

- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

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.

Call Monitoring

Call Monitoring Overview

Call monitoring feature allows you to listen in on employee calls without interference or joining in the conversation as a third party. It helps you check on the quality of teams' sales calls, learn more about customer reactions and insights, and gain a better view for coaching and training the team.

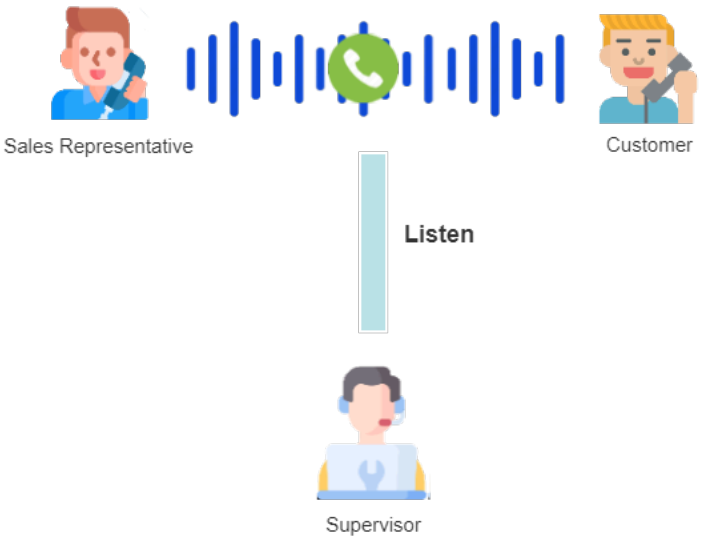
Modes of call monitoring

Yeastar P-Series PBX System supports the following monitoring modes:

Listen mode

Listen mode allows the authorized user to listen in on a call in real time, but can NOT talk with either party.

This mode is often used for supervisor to track the daily actions of sales representatives and evaluate their performance on the sales process.



Whisper mode

Whisper mode allows the authorized user to listen in on a call in real time, and directly talk with the monitored extension without being heard by the other party.

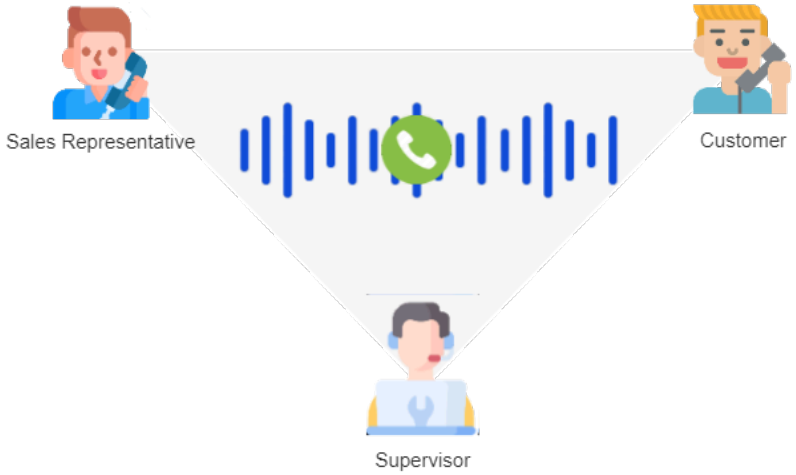
This mode is often used for supervisor to coach remote sales representatives and train them as they work on a sales call.



Barge-in mode

Barge-in mode allows the authorized user to listen in on a call in real time, and talk with both parties.

This mode is often used for supervisor to help sales representatives handle a difficult objection and move deals forward.



Methods of call monitoring

An authorized user can listen in on a call in the following ways:

- Operator Panel
- Queue Panel
- Dial **Feature Code + Extension Number**

Operator Panel

For users who have access to Operator Panel, you can assign the permission of call monitoring operations to them. In this way, the authorized users can listen in on an active call using any one of the three monitoring modes when they are working on Operator Panel.

To assign the permission of call monitoring operations on Operator Panel, see View or Change Permissions for Group Members.

To listen in on a call on Operator Panel, see Monitor a Call.

Queue Panel

For queue managers who have access to Queue Panel, you can assign the permission of call monitoring operations to them. In this way, the queue man-

agers can listen in on an active call using any one of the three monitoring modes when they are working on Queue Panel.

To assign the permission of call monitoring operations on Queue Panel, see Grant Queue Panel Permissions.

To listen in on a call on Queue Panel, see Monitor a Call.

Dial 'Feature Code + Extension Number'

For users who only have phones on hand, you can configure feature codes for each call monitoring mode, then assign permission to specific users. In this way, the authorized users can listen in on an active call using the specified monitoring mode by dialing **Feature Code + Extension Number** on their phones.

To configure the feature code and assign the permission of call monitoring operations, see Allow Users to Monitor a Call by Dialing a Feature Code.

Allow Users to Monitor a Call by Dialing a Feature Code

If users only have phones on hand, you can configure feature codes for each monitoring mode, then assign permission to users. In this way, the authorized users can listen in on a call by dialing a feature code on their phones.

Background information

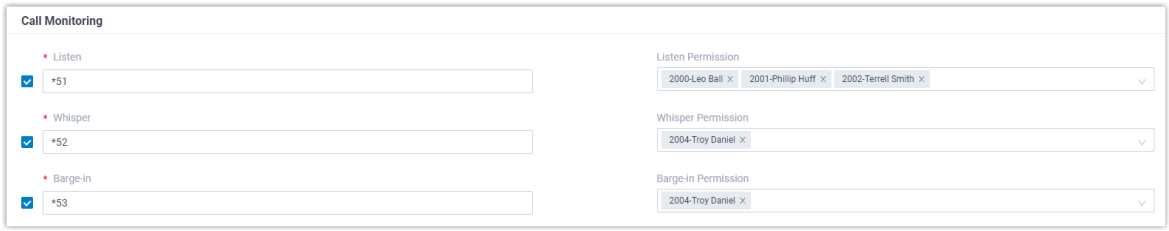
By default, all the extension users can NOT monitor others' calls by dialing a feature code, but their calls can be monitored instead.

To allow specific extension users to monitor others' calls by dialing a feature code, follow the procedure shown below.

To prevent specific extension users from being monitored, see Disallow Users to be Monitored by Others.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. In the **Call Monitoring** section, configure the feature code and assign permission to users.



a. Select the checkbox of a desired call monitoring mode, then configure the feature code.
   - **Listen**: Listen in on a call in real time, but can NOT talk with either party.

     The default feature code is *51.
   - **Whisper**: Listen in on a call in real time, and directly talk with the monitored extension without being heard by the other party.

     The default feature code is *52.
   - **Barge-in**: Listen in on a call in real time, and talk with both parties.

     The default feature code is *53.

b. In the **Listen/Whisper/Barge-in Permission** drop-down list, select the allowed extensions for each call monitoring mode respectively.

3. Click **Save** and **Apply**.

Result

The authorized user can dial **Feature Code + Extension Number** to monitor the calls of the extensions that are allowed to be monitored.

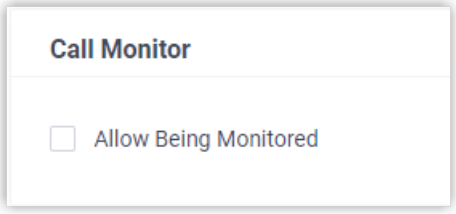
> **Important:**
>
> - Monitoring **Conference Calls** via feature code is NOT supported.
> - Monitoring calls of extensions that are invisible on Linkus clients is NOT supported.
> - During an internal call where one party allows being monitored while the other party disallows, the call can NOT be monitored even by the authorized user.

Disallow Users to be Monitored by Others

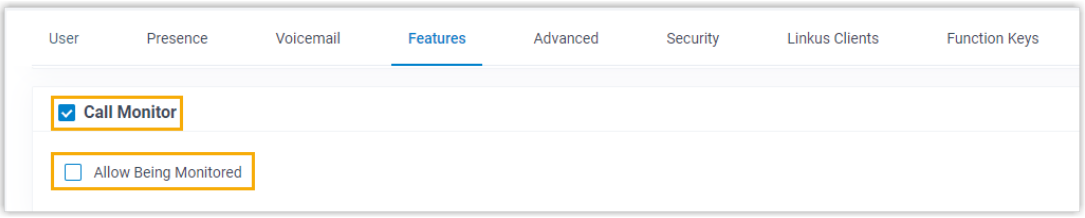
By default, all the extension users are allowed to be monitored. To keep specific users' calls private, you can disable the monitoring feature for users.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. To prevent an extension from being monitored, do as follows:
   a. Click beside the desired extension.
   b. Click **Features** tab.
   c. In the **Call Monitor** section, unselect the checkbox of **Allow Being Monitored**.



   d. Click **Save** and **Apply**.
3. To prevent multiple extensions from being monitored, do as follows:
   a. Select the checkboxes of the desired extensions, then click **Edit**.
   b. Click **Features** tab.
   c. Select the checkbox of **Call Monitor**, then unselect the checkbox of **Allow Being Monitored**.



   d. Click **Save** and **Apply**.

Result

The users' calls can NOT be monitored by anyone.

Call Force Drop

Allow Users to Force Drop Extensions' Calls

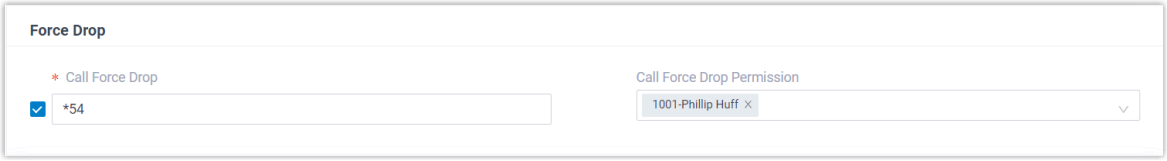
Call Force Drop feature allows the authorized users to force disconnect an extension's current call by dialing a feature code.

Requirements

The version of PBX is 37.16.0.25 or later.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. Scroll down to the **Force Drop** section, then complete the following settings.



   - **Call Force Drop**: Retain the default feature code `*54` or change it as needed.
   - **Call Force Drop Permission**: Select the extensions that are allowed to force drop extensions' calls by dialing the feature code.
3. Click **Save** and **Apply**.

Result

The authorized users can dial *{feature_code}* + *{extension_number}* to force drop an extension's current call, or dial *{feature_code}* to force drop the monitored extension's current call.

For more information, see Force Drop an Extension's Call.

Force Drop an Extension's Call

This topic describes how an authorized user can force drop an extension's current call by dialing a feature code.

Prerequisites

The user to force drop calls has been assigned the **Call Force Drop** permission.

Procedure

- The authorized user dials *{feature_code}* + *{extension_number}* to force drop an extension's current call.

  For example, dial `*541000` to force drop the current call of extension 1000.

- The authorized user dials *{feature_code}* to force drop the monitored extension's current call.

  For example, while monitoring the current call of extension 1000, dial `*54` to force drop the call.

Result

- The authorized user who forces drop the call hears a prompt "Call force drop succeeded", then the call hangs up.
- The extension user whose call is forcibly disconnected hears a prompt "This call was forcibly dropped", then the call hangs up.
- The other party on the call is hung up directly.

Boss-Secretary

Set up Boss-Secretary Feature for Extensions

Yeastar Boss-Secretary feature allows the secretary to filter incoming calls for the boss. You can enable this feature on an extension to designate it a boss extension, then assign secretary extension(s) to it and set forwarding rule. After the setup, any incoming calls to the boss extension that meet the forwarding rule will be automatically forwarded to the secretary extension. The secretary can answer the call and decide whether to transfer it to the boss.

Video Tutorial

Prerequisites

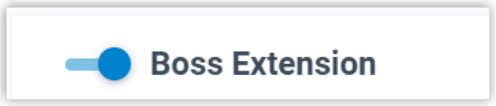
- If you want to assign multiple secretary extensions to one boss extension, you need to group all the secretary extensions into one ring group.

  For more information, see Create a Ring Group.

- If you want the boss extension to ring simultaneously when calls are forwarded to the secretary, you need to place both the boss extension and the secretary extension(s) into one ring group.

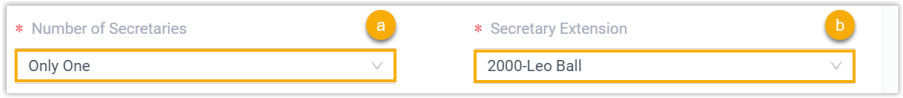
Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click beside the extension that you want to set as the 'Boss Extension'.
3. Click the **Features** tab.
4. In the **Boss Extension** section, turn on the switch to set the extension as the boss extension.

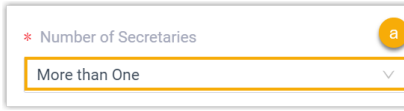
   The preselected **Enable Boss-Secretary Feature** option indicates the feature is enabled for this extension.
5. Specify secretary extension(s) for this boss extension.

   One Secretary

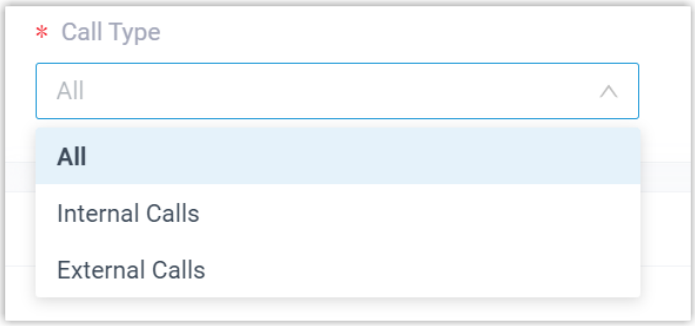
   

   a. In the **Number of Secretaries** drop-down list, select **Only One**.
   b. In the **Secretary Extension** drop-down list, select the desired extension.

   Multiple Secretaries

   a. In the **Number of Secretar**
   b. In the **Secretary Group** dro
6. In the **Call Type** drop-down list, decide which incoming calls to the boss extension need forwarding to the secretary extension(s).

   - **All**: Forward all the incoming calls firstly to the secretary extension(s).
   - **Internal Calls**: Forward only the internal incoming calls firstly to the secretary extension(s).
   - **External Calls**: Forward only the external incoming calls firstly to the secretary extension(s).

> **Note:**
> If you set up Call Handling Based on Caller ID for the boss extension, the incoming calls that meet the call handling rule will be handled accordingly, instead of following the forwarding rule you set here.

7. Click **Save** and **Apply**.

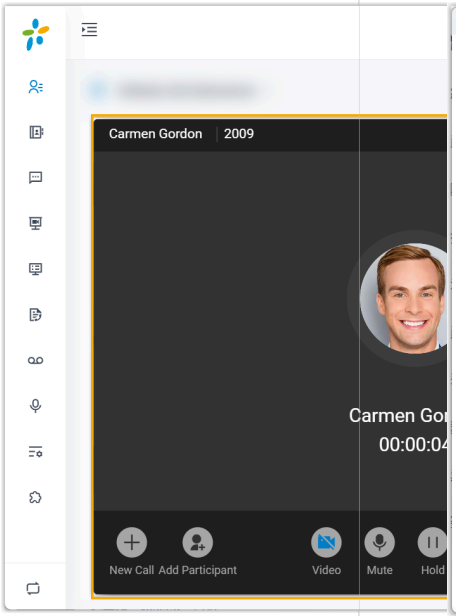
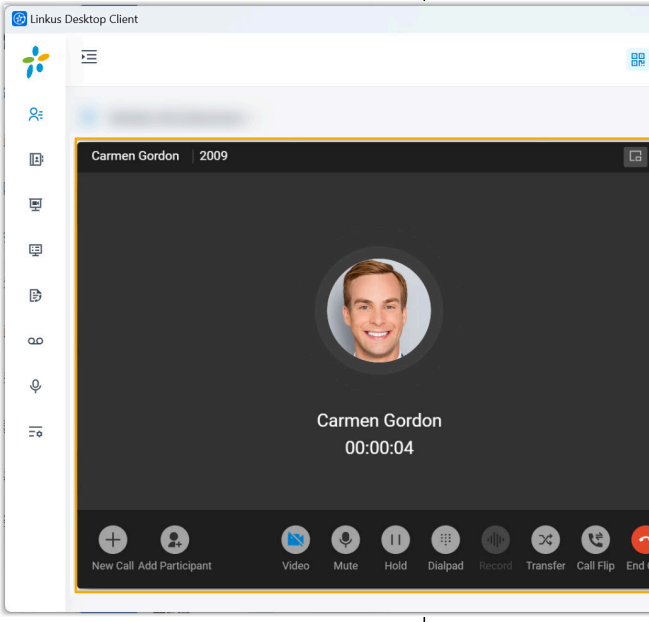
Result

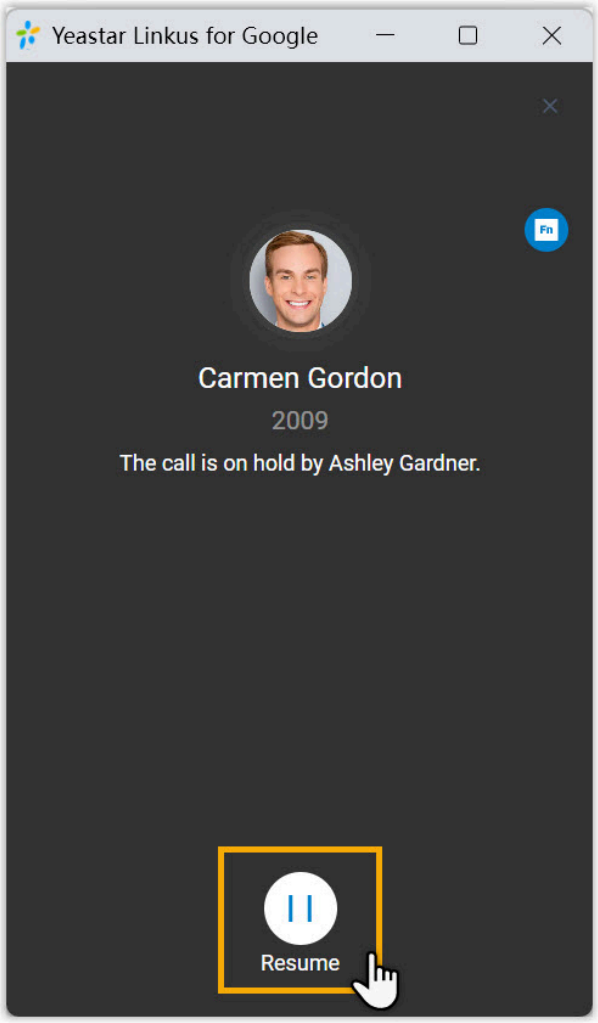
The extension is set up with the Boss-Secretary feature and designated as the boss extension.

The following features are achieved:

- Incoming calls of the selected call type to the boss extension will be automatically forwarded to the secretary extension(s). The secretary can answer the call and determine if it needs to be transferred to the boss.
- A call can be transferred between the boss and secretaries by putting it on hold and resuming it.
  When one party holds a call, the other party can resume and answer the call on the following endpoints:

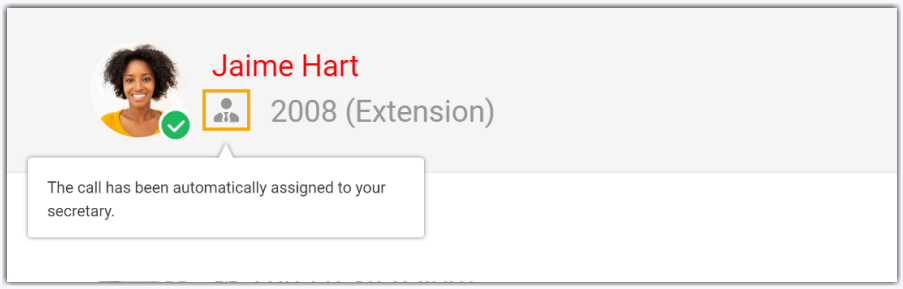
Endpoint	Description
Linkus Web Client & Linkus Desktop Client	Click **Resume** in the pop-up window to answer the call. **Note:** ◦ To use this feature, ensure the **Linkus Desktop Client** meets the following version requirements: ▪ **Windows Desktop**: 1.1.2 or later. ▪ **Mac Desktop**: 1.1.2 or later. ◦ **Linkus Mobile Client** does NOT support resuming calls transferred from boss/secretary.

Endpoint	Description
	Figure 1. **Linkus Web Client**  Figure 2. **Linkus Desktop Client** 
Yeastar Linkus for Google	Click **Resume** in 'Yeastar Linkus for Google' to answer the call.

Endpoint	Description
	
IP phone	Press the BLF key on the IP phone to answer the call. **Important:** To resume the transferred calls via IP phones, you need to set up IP phones for the boss or secretary. ◦ To allow the boss to resume calls transferred from the secretary via an IP phone, see Monitor secretary's call status on an IP phone. ◦ To allow the secretary to resume calls transferred from the boss via an IP phone, see Monitor boss's call status on an IP phone.

Note:

- Boss can disable this feature or change the call type that needs forwarding on their Linkus Web Client or Linkus Desktop Client (path: **Preferences > Features > Boss Extension**), and the updated settings will be synchronized to PBX automatically.
- On the **Call Logs** page of the boss's Linkus clients, missed calls with icon indicate that the calls were automatically forwarded to the secretary extension, distinguishing them from the actual missed calls of the boss extension.



Monitor Call Status

Monitor Secretary's Call Status

With the Boss-Secretary feature enabled, you can set up function keys and configure the IP phone for the boss, allowing the boss to check if the secretary is currently handling his or her call by monitoring the secretary's call status through Linkus clients and IP phone.

Monitor secretary's call status on Linkus clients

By setting up function key(s) for the boss's extension, the boss can monitor secretary's call status through **Linkus Desktop Client**, **Linkus Web Client**, and **Yeastar Linkus for Google**.

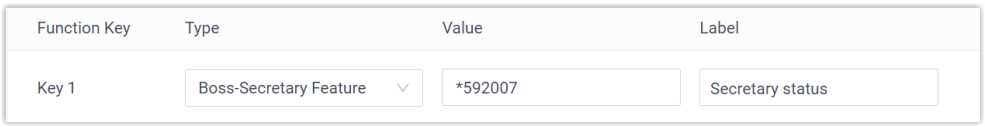
Prerequisites

- You have Set up Boss-Secretary Feature for Extensions.
- Obtain the **Enable Boss-Secretary Feature** feature code.

Note:
The default feature code is `*59`. You can view or update the feature code on **Call Features > Feature Code > Boss-Secretary Feature > Enable Boss-Secretary Feature**.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, select the boss extension and click .
2. Click the **Function Keys** tab.
3. Configure the following settings to subscribe to the secretary's call status.



   - **Type**: Select **Boss-Secretary Feature**.
   - **Value**: Enter the **Enable Boss-Secretary Feature Code** and **Secretary Extension Number**.

     For example, the **Enable Boss-Secretary Feature Code** is `*59`, and the **Secretary Extension Number** is `2007`, then enter `*592007`.
   - **Label**: Optional. Enter a display name for this function key.
4. Click **Save**.

Result

The boss can monitor the secretary's call status by the icons in the **Function Keys** list of Linkus clients.

Icons & Descriptions

- : The secretary is NOT handling any calls for the boss.
- : The secretary is answering calls for the boss.
- : The secretary is putting a call on hold, waiting for the boss to answer.

Linkus clients

Figure 3. **Linkus Web Client & Linkus Desktop Client**

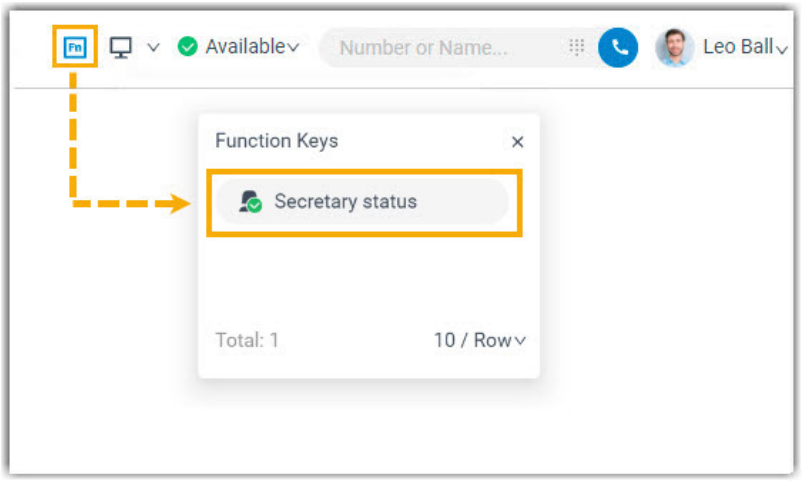
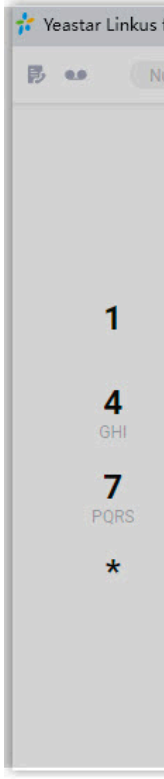


Figure 4. **Yeas**



Monitor secretary's call status on an IP phone

By setting up the boss's IP phone, the boss can monitor the secretary's call status by the BLF LED, and resume calls transferred from the secretary using the BLF key.

Prerequisites

- You have set up function keys for boss to monitor secretary's call status.
- Ensure that the IP phone is connected to Yeastar P-Series PBX System via auto provisioning, and has been assigned to the boss extension.

> **Note:**
> For more information about auto provisioning, see the following topics:
> - Auto Provision IP Phones in Local Network (PnP Method)
> - Auto Provision IP Phones in Local Network (DHCP Method)
> - Auto Provision IP Phones Remotely (RPS FQDN Method)
> - Auto Provision IP Phones Remotely (RPS Method)

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Click beside the boss's phone.
3. In the pop-up window, click **OK**.

Result

The boss can monitor the secretary's call status through the BLF LED on his or her IP phone:

- **Solid Green**: The secretary is NOT handling any calls for the boss.
- **Solid Red**: The secretary is answering calls for the boss.
- **Flashing Red**: The secretary is putting a call on hold, waiting for the boss to answer. And the boss can press the BLF key to resume and answer the call.

> **Note:**
> If the boss is using a **Fanvil phone**, you need to set the **BLF Hold** LED to either **Slowblink** or **Fastblink**. Otherwise, the BLF LED will not flash when the secretary places a call on hold.

Monitor Boss's Call Status

With the Boss-Secretary feature enabled, you can set up function keys and configure the IP phone for the secretary, allowing the secretary to check if the boss is holding calls for him or her to resume by monitoring the boss's call status on Linkus clients and IP phone.

Monitor boss's call status on Linkus clients

By setting up function key(s) for the secretary's extension, the secretary can monitor the boss's call status through **Linkus Desktop Client**, **Linku Web Client**, and **Yeastar Linkus for Google**.

Prerequisites

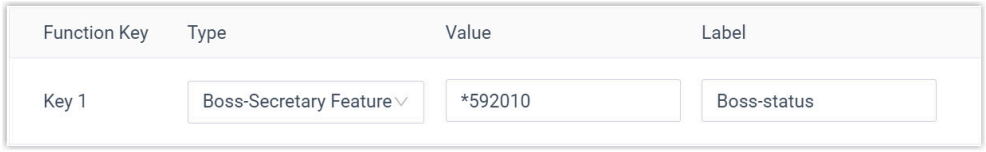
- You have Set up Boss-Secretary Feature for Extensions.
- Obtain the **Enable Boss-Secretary Feature** feature code.

> **Note:**

> The default feature code is `*59`. You can view or update the feature code on **Call Features > Feature Code > Boss-Secretary Feature > Enable Boss-Secretary Feature**.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, select the secretary extension and click .
2. Click the **Function Keys** tab.
3. Configure the following settings to subscribe to the boss's call status.



   - **Type**: Select **Boss-Secretary Feature**.
   - **Value**: Enter the **Enable Boss-Secretary Feature Code** and **Boss Extension Number**.

     For example, the **Enable Boss-Secretary Feature Code** is `*59`, and the **Boss Extension Number** is `2010`, then enter `*592010`.
   - **Label**: Optional. Enter a display name for this function key.
4. Click **Save**.

Result

The secretary can check if the boss is currently holding a call by the icons in the **Function Keys** list of Linkus clients.

Icons & Descriptions

- : The boss is NOT holding any calls for the secretary to resume.
- : The boss is putting a call on hold, waiting for the secretary to resume.

Linkus clients

Figure 5. **Linkus Web Client & Linkus Desktop Client**

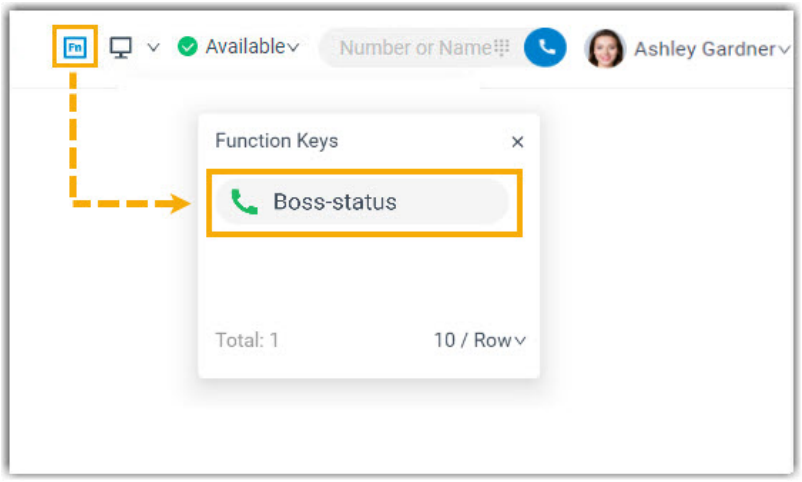
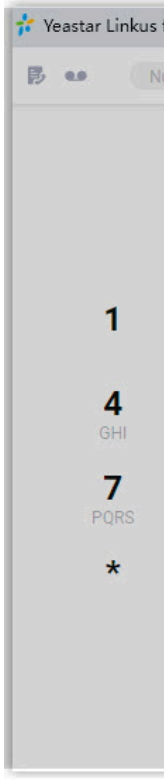


Figure 6. **Yeas**



Monitor boss's call status on an IP phone

By setting up the secretary's IP phone, the secretary can monitor the boss's call status by the BLF LED, and resume calls transferred from the boss using the BLF key.

Prerequisites

- You have set up function keys for secretary to monitor boss's call status.
- Ensure that the IP phone is connected to Yeastar P-Series PBX System via auto provisioning, and has been assigned to the secretary extension.

> **Note:**
> For more information about auto provisioning, see the following topics:
> - Auto Provision IP Phones in Local Network (PnP Method)
> - Auto Provision IP Phones in Local Network (DHCP Method)
> - Auto Provision IP Phones Remotely (RPS FQDN Method)
> - Auto Provision IP Phones Remotely (RPS Method)

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Click beside the secretary' phone.
3. In the pop-up window, click **OK**.

Result

The secretary can check if the boss is currently holding a call through the BLF LED on his or her IP phone:

- **Solid Green**: The boss is NOT holding any calls for the secretary to resume.
- **Flashing Red**: The boss is putting a call on hold, waiting for the secretary to resume. And the secretary can press the BLF key to resume the call.

> **Note:**
> If the secretary is using a **Fanvil phone**, you need to set the **BLF Hold** LED to either **Slowblink** or **Fastblink**. Otherwise, the BLF LED will not flash when the boss places a call on hold.

Hot Desking

Hot Desking Overview

Hot desking feature allows extension users to log in to a shared desk phone temporarily using their extension number and voicemail PIN, so that users can make and receive calls on the shared phone with their own extension numbers.

Scenario

The Hot Desking feature is ideal for shared offices, field teams, and call centers where employees have flexible schedules or work in shifts.

For example, call centers typically work in shifts to provide a 24-hour service, so employees may need to share a desk phone at different times. With hot desking feature, the employee can log in to a shared phone and answer incoming calls with his or her own extension during working hours. When the employee log out of the shared phone after work, the system automatically logs the user out of the queue, avoiding delays in responding to incoming

calls. This not only optimizes the use of telephone hardware resources but also improves the economic benefits of the call center.

Requirements and restrictions

Requirements

- **PBX Server**: The firmware of Yeastar P-Series PBX System is 37.10.0.30 or later.
- **IP Phone**: The model and firmware of the IP phone meets the requirements listed in Auto Provisioning - Supported Devices.

Restrictions

Hot desking is only applicable to SIP extensions.

Process of setting up hot desking

To implement hot desking, you need to complete the following configurations:

Set up a hot desking phone

You need to set up a hot desking phone via auto provisioning according to your network environment.

For more information, see Set up a Hot Desking Phone.

Enable hot desking for extension users

You need to enable hot desking feature for specific extension users. Only the extension users with hot desking feature enabled can log in to a hot desking phone.

For more information, see Enable Hot Desking for an Extension User.

Methods of using hot desking

After you set up a hot desking phone, authorized users can log in to and log out of the hot desking phone in the following ways:

- Dial a Guest In / Guest Out feature code
- Press a Guest In / Guest Out key

Dial a Guest In / Guest Out feature code

By dialing a feature code on a hot desking phone, users can log in and use the phone with their own extension number, and log out after finish using the phone.

The default hot desking feature code is listed below:

- **Guest In**: *84
- **Guest Out**: *084

> **Tip:**
> You can change, enable, or disable the hot desking feature code on PBX web portal: **Call Features > Feature Code > Hot Desking**.

For more information, see dial a feature code to log in and dial a feature code to log out.

Press a Guest In / Guest Out key

The PBX system automatically assigns a **Guest In** and **Guest Out** key to a hot desking phone for login or logout. Users can press the BLF key on the phone to log in and use the phone with their own extension number, or log out after finish using the phone.

For more information, see press a BLF key to log in and press a BLF key to log out.

Set up Hot Desing

Set up a Hot Desking Phone

This topic describes how to set up a phone for hot desking via auto provisioning.

> **Important:**
> If the desired phone has been assigned to an extension, you need to delete the phone from auto provisioning phone list and RESET the phone first.

Supported devices

Hot desking is applicable on the IP phones listed in Auto Provisioning - Supported Devices.

Supported methods

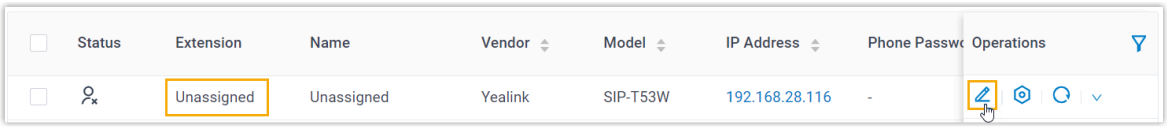
According to your network environment, you can set up a hot desking phone on PBX web portal via the following methods:

- Set up a hot desking phone in local network (PnP method)
- Set up a hot desking phone in local network (DHCP method)
- Set up a hot desking phone in remote network (RPS FQDN / RPS method)

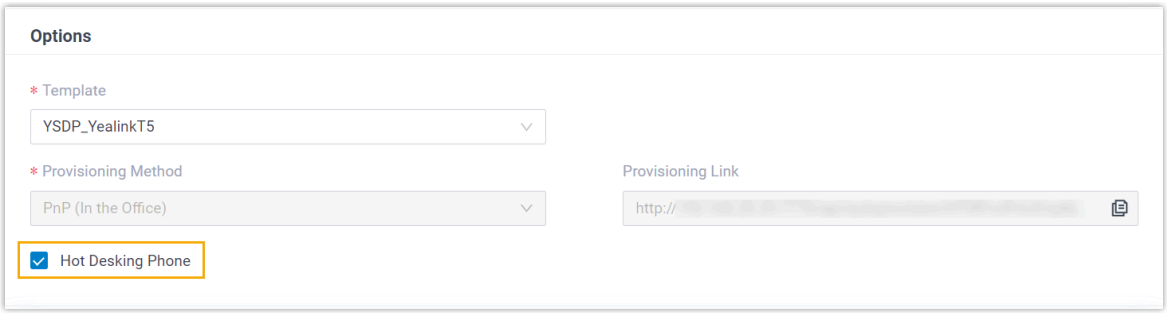
Set up a hot desking phone in local network (PnP method)

If the IP phone is in the same LAN subnet as the PBX, the PBX will detect the IP phone via PnP, and display the phone in the auto provisioning phone list. You can directly set an IP phone to a hot desking phone.

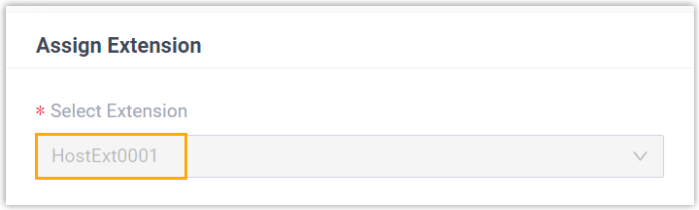
1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Click beside an unassigned IP phone.



3. In the **Options** section, select the checkbox of **Hot Desking Phone**.



The phone is automatically assigned to a virtual extension named HostExt*{virtual_num}*.



4. Click **Save**.

Set up a hot desking phone in local network (DHCP method)

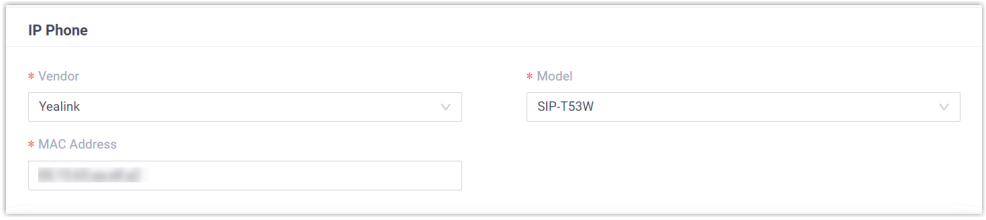
If the IP phone is in the same LAN subnet as the PBX server but doesn't support PnP provisioning method, or the IP phone is in different LAN subnet with the PBX server, you can set up the phone to a hot desking phone via DHCP provisioning method.

Prerequisites

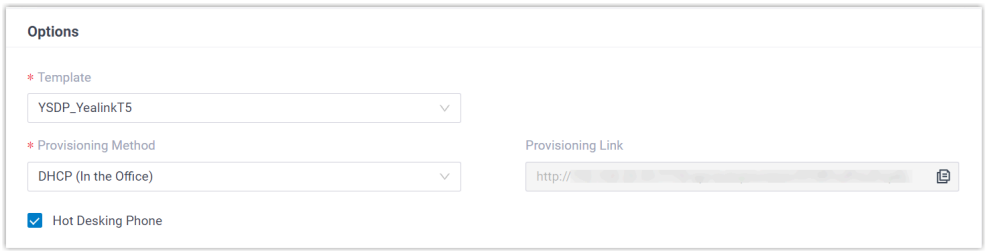
- Make sure the IP phone supports DHCP provisioning method.
- Gather information of IP phone, including Vendor, Model, and MAC address.

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Click **+Add > Add**.
3. In the **IP Phone** section, enter the phone's information:



   - **Vendor**: Select a phone vendor.
   - **Model**: Select a phone model.
   - **MAC Address**: Enter MAC address of the phone.
4. In the **Options** section, configure the following settings.

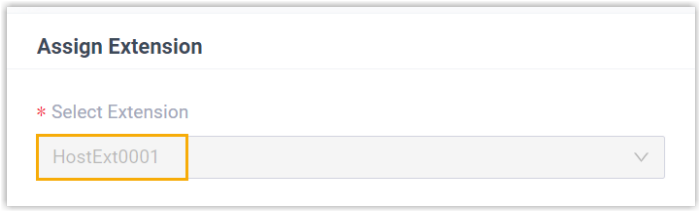


   - **Template**: Select a desired template for the phone from the drop-down list.
   - **Provisioning Method**: Select **DHCP (In the Office)**.

     A provisioning server URL is generated accordingly and displayed on the **Provisioning Link** field.

- **Hot Desking Phone**: Enable the option to set the phone as a hot desking phone.

  The phone is automatically assigned to a virtual extension named HostExt*{virtual_num}*.



5. Click **Save**.
6. Configure the DHCP server.

> **Note:**
> Make sure there is only one DHCP server running on the network where the IP phone is located, otherwise the IP phone may fail to obtain an IP address.

Scenario	Instructions
The IP phone is in the same LAN as the PBX server, but doesn't support PnP provisioning	You can configure the DHCP server in either of the following ways: • Set up PBX as a DHCP server **Note:** The PBX built-in DHCP server will automatically obtain the provisioning link. • Set up option 66 on a third-party DHCP server with the provisioning link.
The IP phone is in different LAN with the PBX server	Set up DHCP option 66 on a third-party DHCP server with the provisioning link.

7. Reboot the IP phone manually.

Set up a hot desking phone in remote network (RPS FQDN / RPS method)

If the IP phone is deployed in a remote network, you can set up the phone to a hot desking phone via RPS FQDN or RPS method.

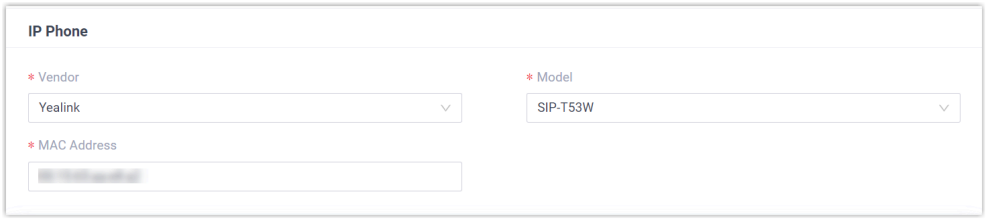
Prerequisites

Make sure that the following prerequisites are met according to your desired provisioning method.

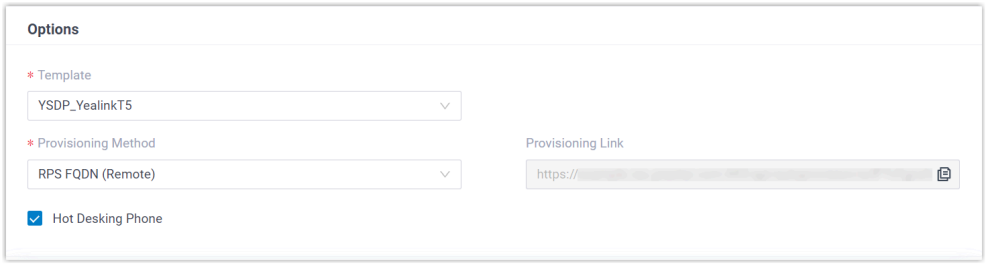
Method	Prerequisites
RPS FQDN	• You have subscribed **Enterprise Plan** or **Ultimate Plan**. • You have configured Yeastar FQDN for remote SIP access and remote web access. • Gather information of IP phone, including Vendor, Model, and MAC address.
RPS	• You have set up port forwarding on router (including RTP ports, SIP port, and Web Server port), and set up SIP NAT on the PBX to ensure remote registration. • Gather information of IP phone, including Vendor, Model, and MAC address.

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Click **+Add > Add**.
3. In the **IP Phone** section, enter the phone's information:



   - **Vendor**: Select a phone vendor.
   - **Model**: Select a phone model.
   - **MAC Address**: Enter MAC address of the phone.
4. In the **Options** section, configure the following settings:

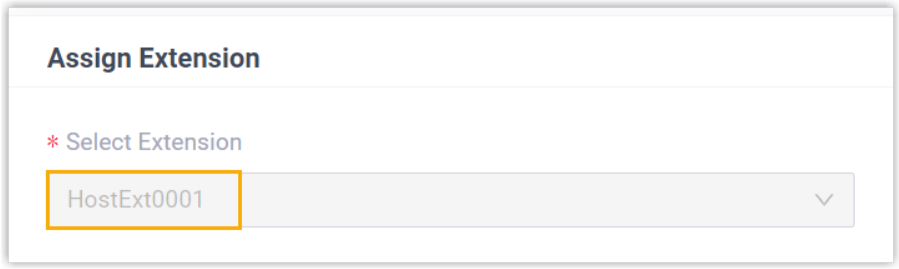


   - **Template**: Select a desired template for the phone from the drop-down list.

- **Provisioning Method**: Select a desired provisioning method.

  A provisioning server URL is generated accordingly and displayed on the **Provisioning Link** field.
- **Hot Desking Phone**: Enable the option to set the phone as a hot desking phone.

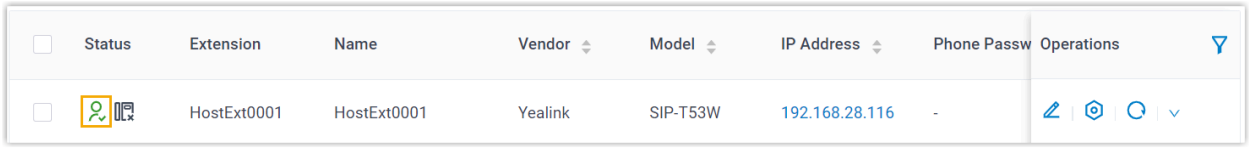
  The phone is automatically assigned to a virtual extension named HostExt*{virtual_num}*.



5. Click **Save**.
6. Reboot the IP phone manually.

Result

The phone is connected to the PBX and set as a hot desking phone with the virtual extension registered. You can check the registration status from the phone list; The PBX system automatically assigns a **Guest In** key to the phone.



Note:
Users can only use the phone with virtual extension registered to make emergency calls. To use the phone for regular calling, users must either dial the **Guest In** feature code or press the **Guest In** BLF key to log in the phone.

What to do next

- Enable Hot Desking for an Extension User
- (Optional) Retain Configurations for Hot Desking Phones

Related information

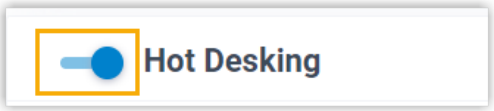
IP Phone Configuration Guide

Enable Hot Desking for an Extension User

This topic describes how to enable hot desking for an extension user, so that the user can log in and use a hot desking phone with his or her own extension number.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click beside the desired extension, then click the **Features** tab.
3. Scroll down to the **Hot Desking** section, then turn on the switch.



4. Configure the following settings according to your needs.

Setting	Description
Log Out of Queue	Decide whether to automatically log out the dynamic agent from a queue. If enabled, the system will automatically log the extension user out of the queue when the user logs out of a hot desking phone.
Automatic Guest Out	Decide whether to automatically log out the extension user from a hot desking phone: • **Never**: Disable automatic logout. • **After**: Specify a time period to log the user out of a hot desking phone since the extension user logs in. • **At Daily**: Specify a fixed time to log the user out of a hot desking phone every day.

5. Click **Save** and **Apply**.

Related information

Log in to a Hot Desking Phone
Log out of a Hot Desking Phone
Manage Hot Desking feature

Retain Configurations for Hot Desking Phones

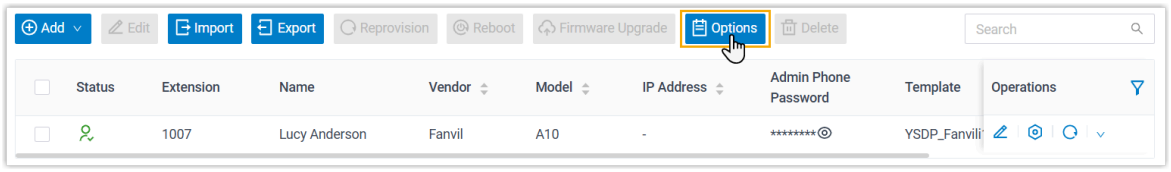
This topic describes how to configure retention of specific phone configurations on hot desking phones after guests log out.

Requirements

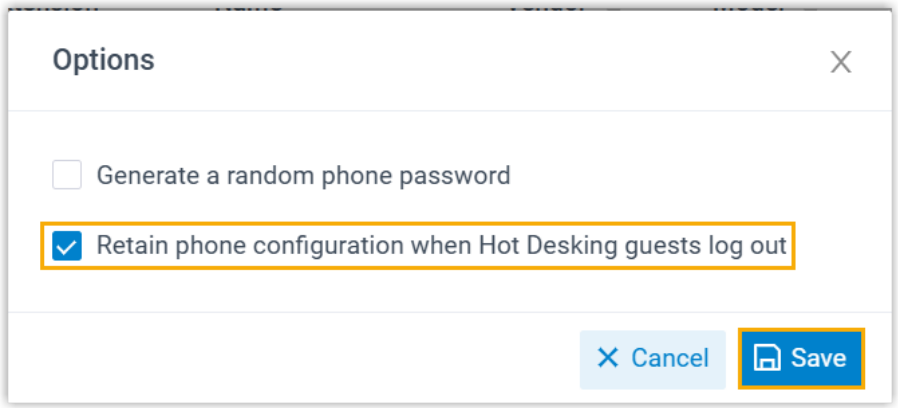
The firmware of Yeastar P-Series PBX System is 37.19.0.70 or later.

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. At the top of the list, click **Options**.



3. In the pop-up window, select the checkbox of **Retain phone configuration when Hot Desking guests log out**, then click **Save**.

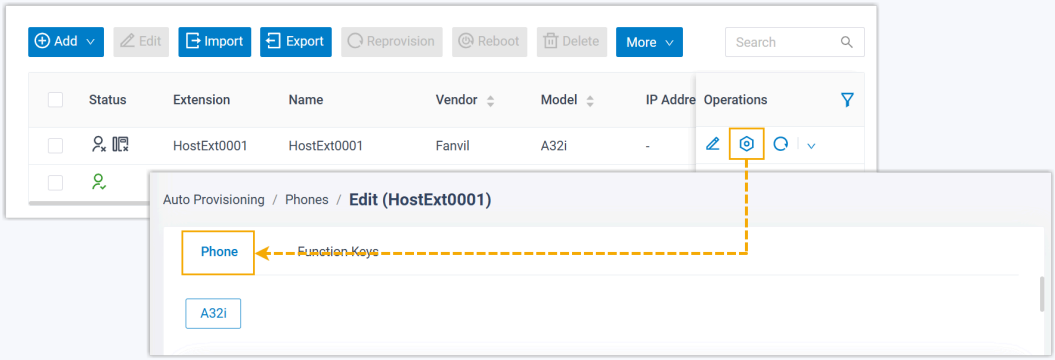


Result

When an extension user logs out of a Hot Desking phone, the general phone configurations will be retained.

Note:

- Only the general configurations will be retained (such as language, signal tones, distinctive ringtone, codecs, etc.), which are configured in the **Auto Provisioning > Phones >** **> Phone**.



- The extension registration-related configurations, LDAP directory settings, and function key settings will be cleared.

Use Hot Desking

Log in to a Hot Desking Phone

This topic describes how extension users can log in to a hot desking phone.

Prerequisites

- You have set up a hot desking phone.
- You have enabled hot desking feature for desired extension users.
- If the users have their own phones, and may occasionally log in to a hot desking phone, you need to set concurrent registrations.

Procedure

Extension users can log in to a hot desking phone via either of the following methods:

Method	Instruction
Dial a feature code to log in	1. On a hot desking phone, dial the **Guest In** feature code. **Note:**

Method	Instruction
	The default **Guest In** feature code is `*84`. You can customize the feature code on **Call Features > Feature Code > Hot Desking > Guest In**. 2. Follow the voice prompt, enter the extension number followed by the `#` key (e.g. 2000#). 3. Follow the voice prompt, enter the voicemail PIN followed by the `#` key (e.g. 8471#).
Press a BLF key to log in	After you set up a hot desking phone, the system automatically assigns a **Guest In** key to the phone, extension users can press the key to log in to the phone. 1. On a hot desking phone, press the **Guest In** key. 2. Follow the voice prompt, enter the extension number followed by the `#` key (e.g. 2000#). 3. Follow the voice prompt, enter the voicemail PIN followed by the `#` key (e.g. 8471#). **Troubleshooting:** If a user failed to log in to the hot desking phone by pressing the **Guest In** key, you can check if the **Guest In** feature code has been changed (Path: **Call Features > Feature Code > Hot Desking > Guest In**).

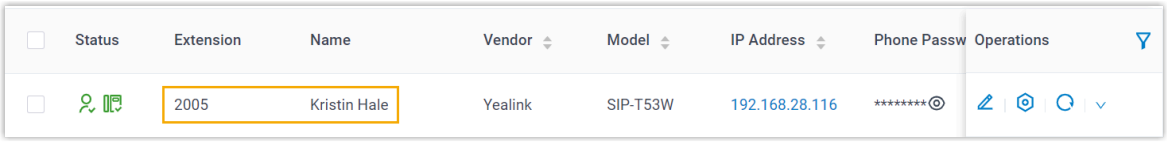
Result

- The user's extension configurations, including extension information and function key settings, are loaded onto the phone; The system automatically assigns a **Guest Out** key to the phone.
- The extension user can use the phone with his or her extension and implement the followings:
  - Make calls from the phone.
  - Receive calls on the phone.
  - Use the function keys of the extension.
  - Query contacts that are stored in the PBX on the IP phone via LDAP.

Note:

> This requires you to configure the LDAP directory settings for the phone on **Auto Provisioning > Phones >** **> LDAP Directory**. For more information about the settings, see Auto Provision LDAP for IP Phones.

- You can monitor the hot desking phone status, and know who is working on the hot desking phone on **Auto Provisioning > Phones**.



Related information

Log out of a Hot Desking Phone

Log out of a Hot Desking Phone

This topic describes how extension users can log out of a hot desking phone.

Procedure

Extension users can log out of a hot desking phone using either of the following methods:

Method	Instruction
Dial a feature code to log out	On a hot desking phone, dial the **Guest Out** feature code. **Note:** The default **Guest Out** feature code is *084. If you want to customize the feature code, go to **Call Features > Feature Code > Hot Desking > Guest Out**.
Press a BLF key to log out	The system automatically assigns a **Guest Out** key to a hot desking phone when a user logged in. The user can press the key on the phone to quickly log out. **Troubleshooting:** If a user failed to log out by pressing the **Guest Out** key, you need to check if the **Guest Out** feature code has been changed (Path: **Call Features > Feature Code > Hot Desking > Guest Out**).

Result

The user's extension is logged out of the phone; the phone is reverted to the default settings and can only be used to make emergency calls.

Important:
The call logs are kept on the hot desking phone, the user needs to manually clear the data if necessary.

Note:

- If you have set up the system to retain configurations for hot desking phones, the general phone configurations (such as language, signal tones, distinctive ringtone, codecs, etc.) will be retained, which are configured in the **Auto Provisioning > Phones >** **> Phone**; while the extension registration-related configurations, LDAP directory settings, and function key settings will be cleared.
- If a user forgot to log out, after another user logs in to the hot desking phone, the previous user would be logged out automatically, or you can forcibly log the user out of the phone on PBX web portal.

Related information

Log in to a Hot Desking Phone

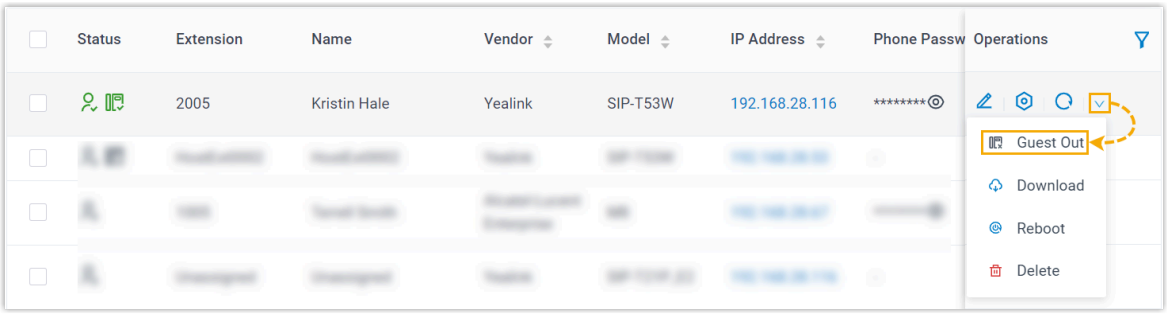
Manage Hot Desking feature

This topic describes how to manage the hot desking feature on PBX web portal, including forcibly log out a user, and disable hot desking for an extension user.

Forcibly log a user out of a hot desking phone

In case an extension user forgot to log out of a hot desking phone, you can forcibly log his or her extension out on PBX web portal, so as to prevent information disclosure or misuse of the extension.

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Hover your mouse over beside the desired phone, and click **Guest Out**.

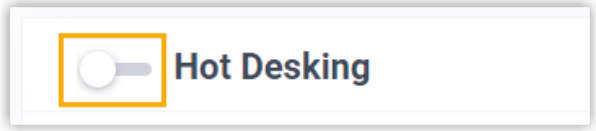


3. In the pop-up window, click **Confirm**.

   The user is logged out of the hot desking phone.

Disable Hot Desking for an extension user

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click beside the desired extension, then click the **Features** tab.
3. Scroll down to the **Hot Desking** section, then turn off the switch.



4. Click **Save** and **Apply**.

   The extension user will not be able to log in to a hot desking phone.

Busy Camp-on

Camp on to a Busy Extension

Busy Camp-on feature allows a caller to place a call reservation when he or she makes a call to an extension and receives a busy signal. The PBX will automatically call the caller back as soon as the called extension becomes available.

Restrictions

- The Busy Camp-on feature is only applicable for the calls between extensions.

- The timeout for a Busy Camp-on request is **3600** seconds. This means that the PBX will not call the caller back if the called party is still unavailable 1 hour after the request is initiated.
- A maximum of **10** Busy Camp-on requests is available for each extension. If exceeds, the PBX will cancel the earliest requests.

Procedure

Assume that extension 1000 makes a call to extension 2000, but extension 2000 is in a call.

In this case, extension 1000 can hang up the call and camp on to extension 2000 by dialing a feature code. The PBX will call extension 1000 back and connect it to extension 2000 as soon as extension 2000 becomes available.

1. Extension 1000 dials *792000 to camp on to extension 2000.

   > **Tip:**
   > The default feature code for enabling Busy Camp-on is `*79`. You can change, enable, or disable the code on PBX web portal: **Call Features > Feature Code > Busy Camp-on > Enable Busy Camp-on**.

   A prompt "The Busy Camp-on has been enabled" is played and the call is hung up automatically.
2. As soon as extension 2000 becomes available, the PBX will call extension 1000.

   Extension 1000 receives an incoming call pop-up with caller ID displayed as **Busy Camp-on** ***{name_of_called_extension}{number_of_called_extension}*** and will hear a prompt "This call is connected via Busy Camp-on feature" after answering the call.
3. The PBX calls extension 2000.

   After extension 2000 answers the call, extension 2000 and extension 1000 are connected.

Cancel Busy Camp-on Requests

If extension users are not available to accept the automatic callback, they can cancel Busy Camp-on requests as shown in the topic.

> **Note:**

We recommend that extension users think twice before proceeding, as this will cancel all the Busy Camp-on requests that they have initiated.

Procedure

Extension user dials *079 on the phone to cancel all the Busy Camp-on requests that he or she has initiated.

Tip:
The default feature code for disabling Busy Camp-on is `*079`. You can change, enable, or disable the code on PBX web portal: **Call Features > Feature Code > Busy Camp-on > Disable Busy Camp-on**.

Result

- A prompt "The Busy Camp-on has been disabled" is played and the call is hung up automatically.
- All Busy Camp-on requests from the extension user are cancelled.

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:

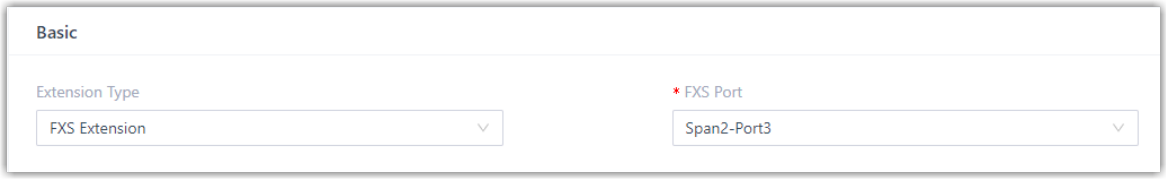
1. Install S2 module or S0 module on the PBX.
2. Connect fax machine to FXS port of the PBX.

   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 web 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**.

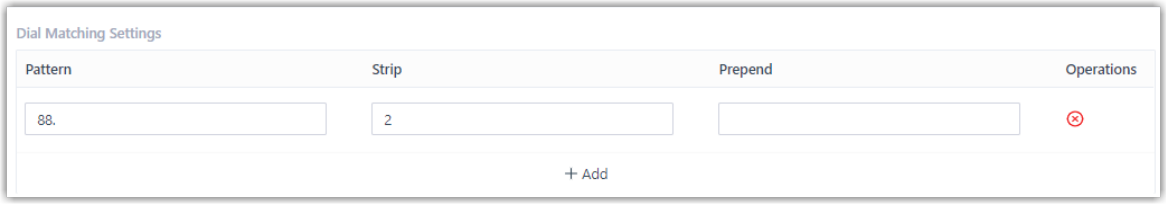
   

4. Leave other settings as default or change the settings according to your needs.
5. Click **Save** and **Apply**.

Step2. Set up an outbound route for sending faxes

1. Log in to PBX web 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.

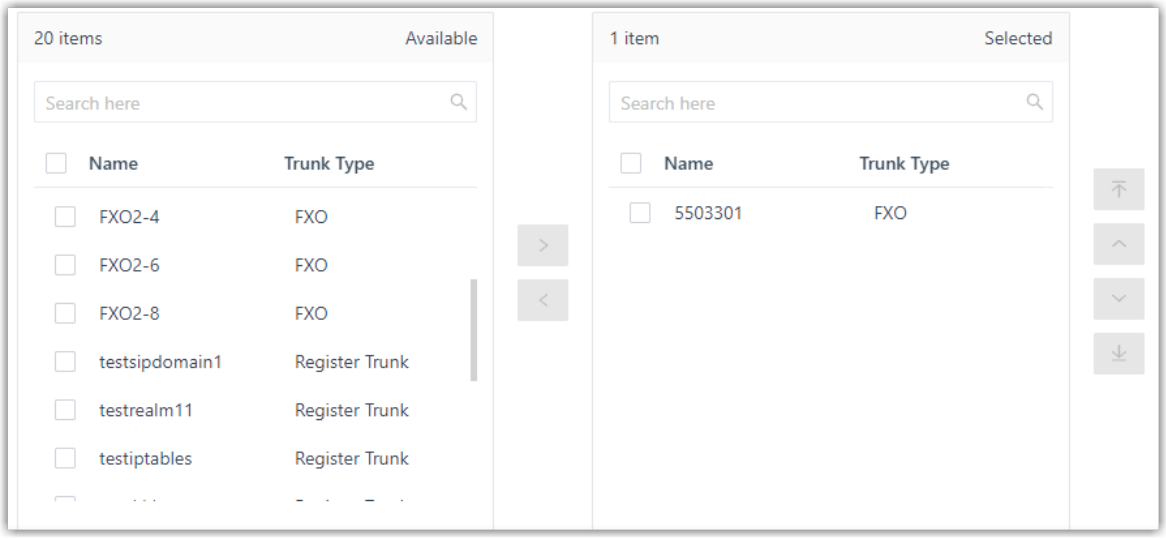
   As the following figure shows, set *88.* for **Pattern**, and *2* for **Strip**.

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.

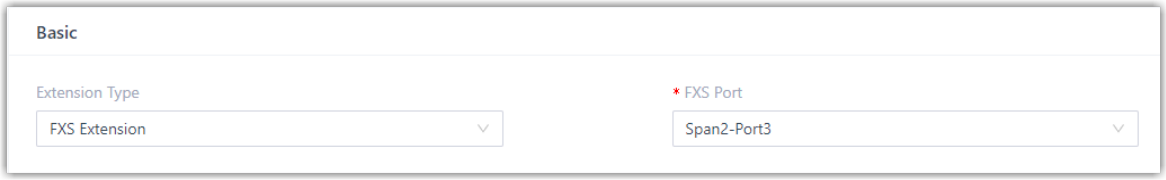
   In this topic, we connect fax machine to FXS port located in Span2-Port3.

Step1. Assign an extension to the fax machine

1. Log in to PBX web 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**.

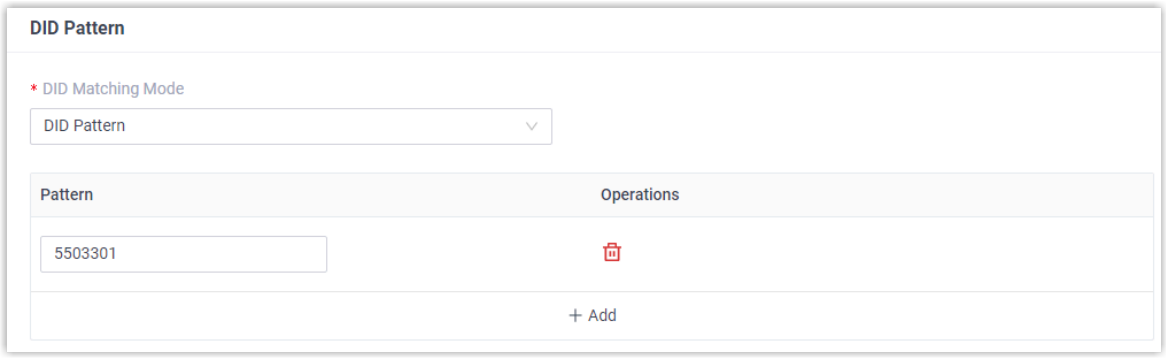


4. Click **Save** and **Apply**.

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.

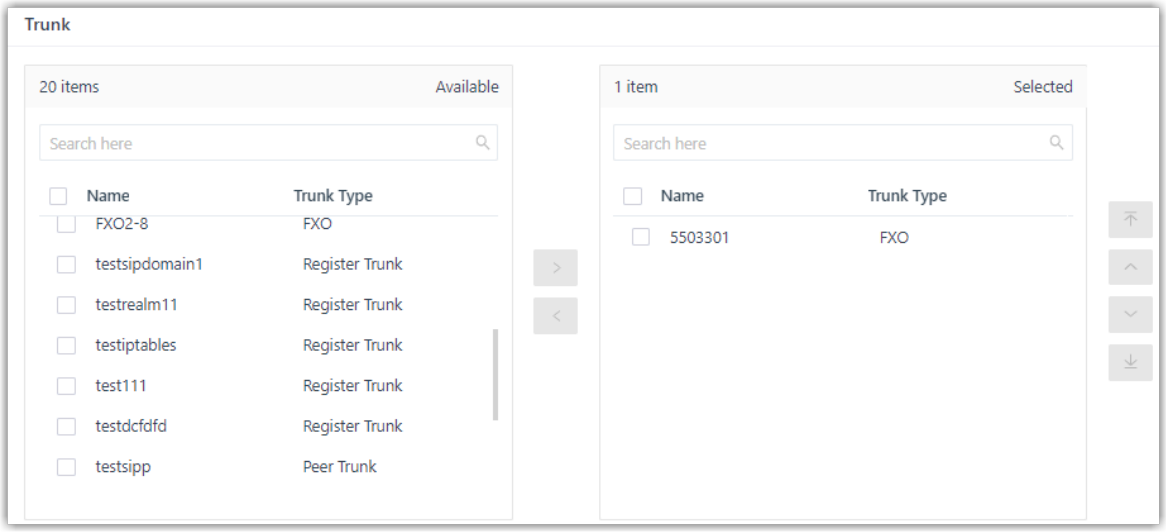
   As the following figure shows, set the trunk number as DID pattern.



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.

   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:

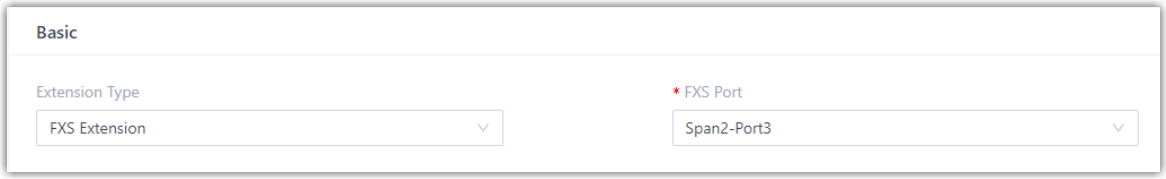
1. Install S2 module or SO module on the PBX.
2. Connect fax machine to FXS port of the PBX.

   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 web 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**.

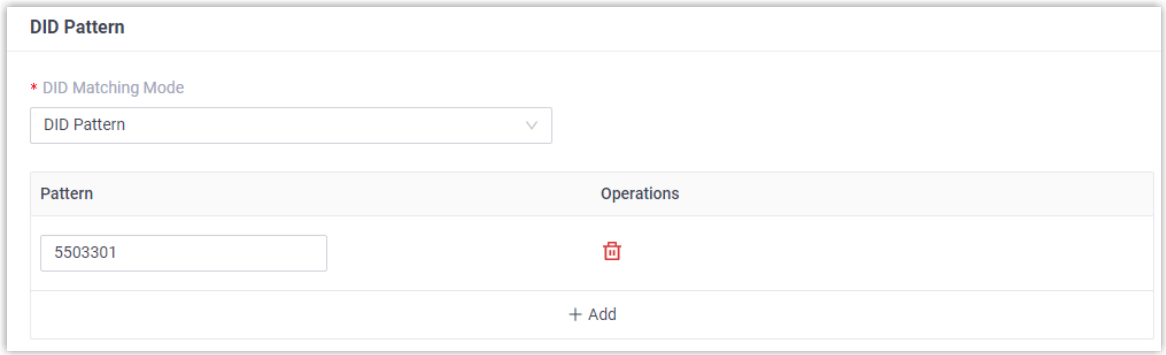
   

5. Click **Save** and **Apply**.

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.

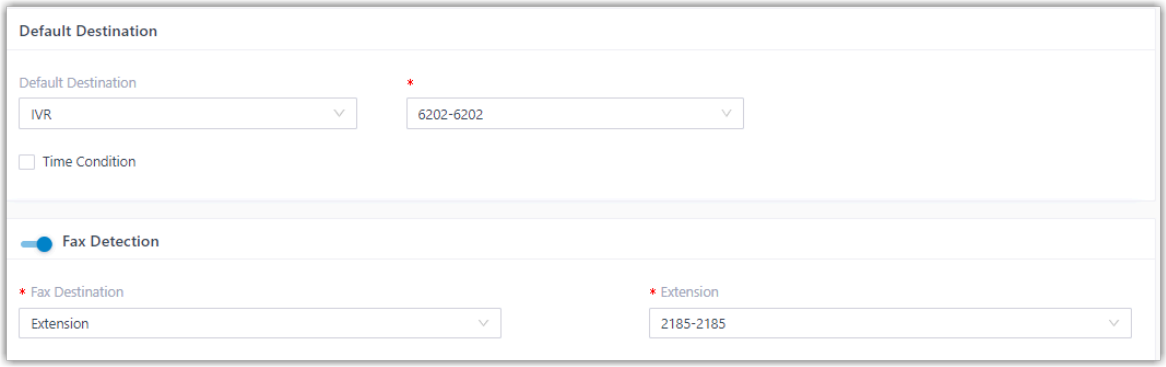
4. Select the trunk that supports to receive faxes.

   > **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.

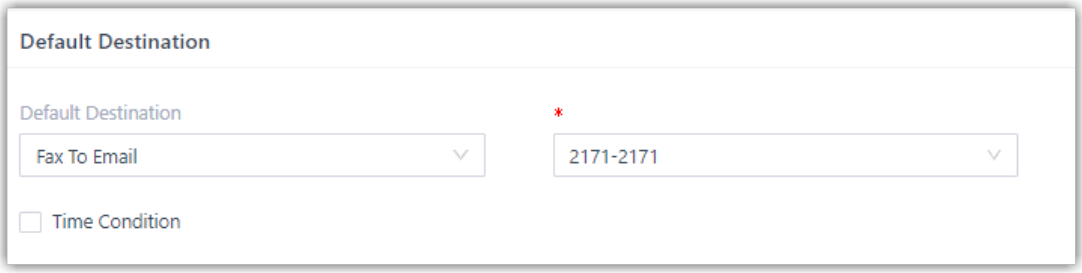
Prerequisites

- 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.

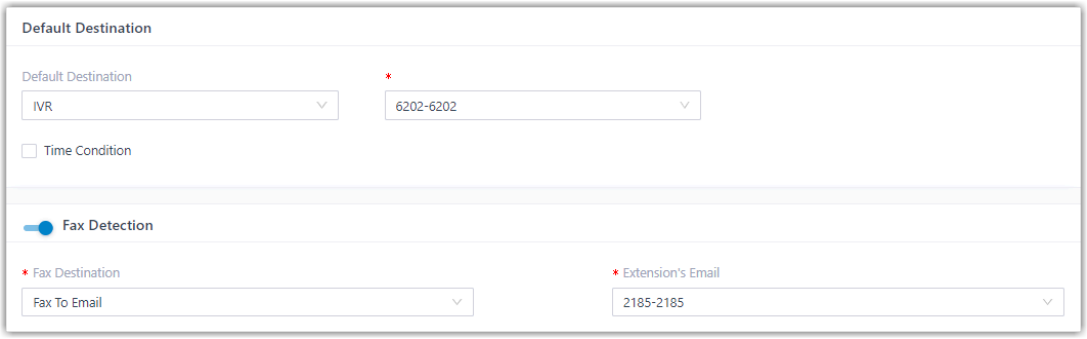
- **Optional**: Customize the fax email template.

Procedure

1. Log in to PBX web 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.



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.



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 web 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 web 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 web 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

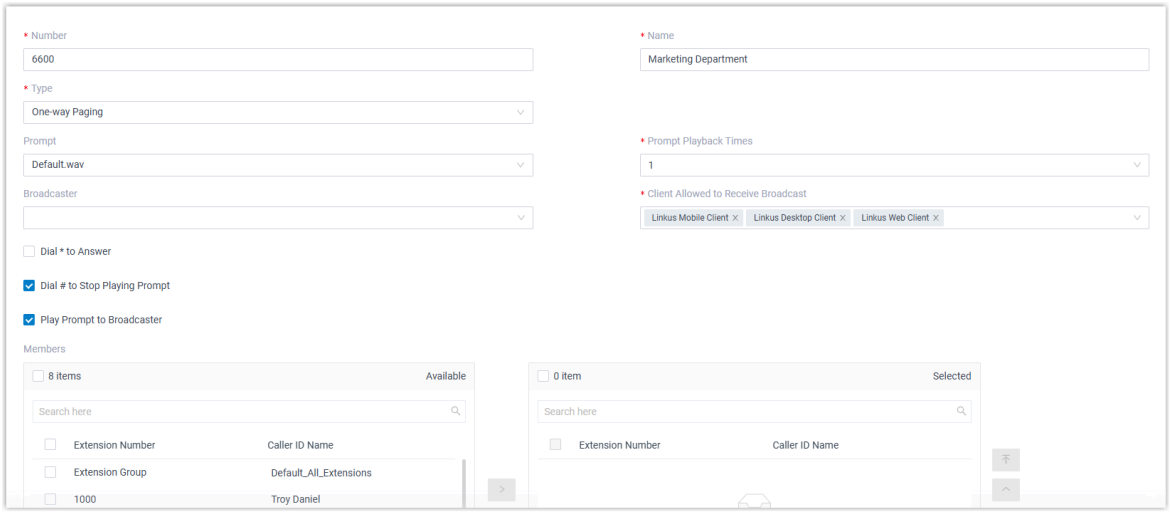
One-way Paging feature allows a broadcaster to make an announcement to users. The called parties' phones will not ring, but instead directly answering into speakerphone mode. This topic describes how to set up a one-way paging group.

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 Department. 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 web portal, go to **Call Features > Paging/Intercom**, click **Add**.
2. Configure a one-way paging group.



Item	Description
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, select **Default.wav**. **Note:** To customize a prompt, see Record a Custom Prompt or Upload a Custom Prompt.
Prompt Playback Times	Specify how many times the prompt will be played and repeated. **Note:** Enter a value between 1 and 100, or select **Unlimited** to play the prompt in a loop.
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.
Client Allowed to Receive Broadcast	Select the desired clients for receiving broadcasts.

Item	Description
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.
Dial # to Stop Playing Prompt	Optional. If a prompt is selected, enabling this option allows the broadcaster to dial # during playback to stop the prompt.
Play Prompt to Broadcaster	Optional. To restrict the broadcaster from hearing the prompt, disable this option. In this example, disable this option. **Note:** This option is available only when a custom prompt is selected and is enabled by default.
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

When dialing the number of the paging group, the selected members will receive broadcast through the client(s) you have specified.

- For Linkus clients (Mobile/Desktop/Web) and analog phones, they will ring first, and users need to manually answer the call to listen to the broadcasts.

  Note:
  If necessary, you can set up user's Linkus clients to automatically answer paging calls. For more information, see Set up Auto Answer for Linkus UC Clients.

- For IP phones, they will automatically answer into speakerphone mode and play the broadcasts.

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.

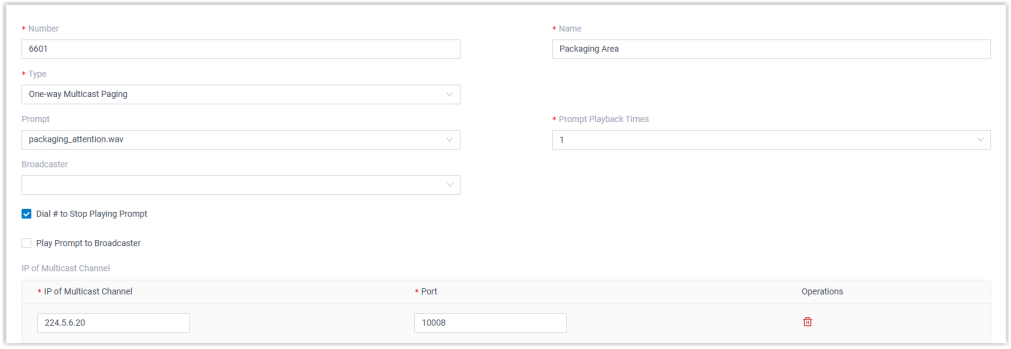
Requirements

The phone that will receive One-way Multicast Paging must support Multicast Paging feature, and 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 web portal, go to **Call Features > Paging/Intercom**, click **Add**.
        ii. Configure a one-way multicast paging group.



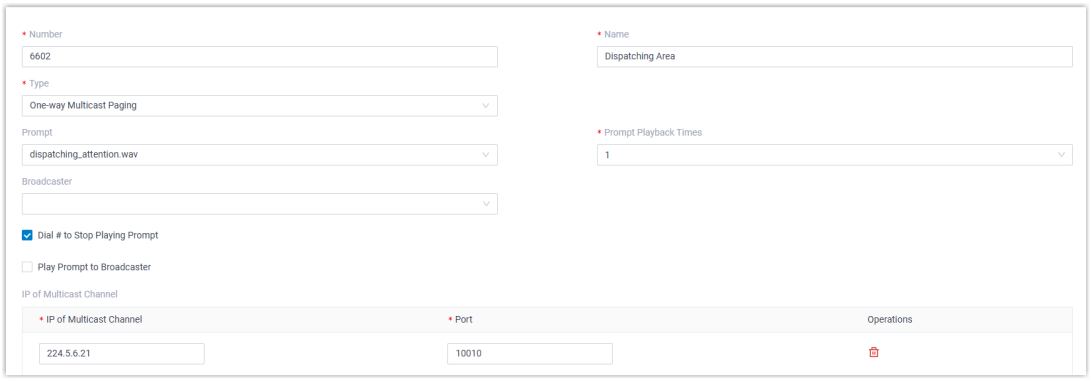
Item	Description
Number	Enter a number for the paging group. In this example, enter *6601*.

Item	Description
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, select **packaging_attention.wav**. **Note:** To customize a prompt, see Record a Custom Prompt or Upload a Custom Prompt.
Prompt Playback Times	Specify how many times the prompt will be played and repeated. **Note:** Enter a value between 1 and 100, or select **Unlimited** to play the prompt in a loop.
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 Stop Playing Prompt	Optional. If a prompt is selected, enabling this option allows the broadcaster to dial # during playback to stop the prompt.
Play Prompt to Broadcaster	Optional. To restrict the broadcaster from hearing the prompt, disable this option. In this example, disable this option. **Note:** This option is available only when a custom prompt is selected and is enabled by default.
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*.

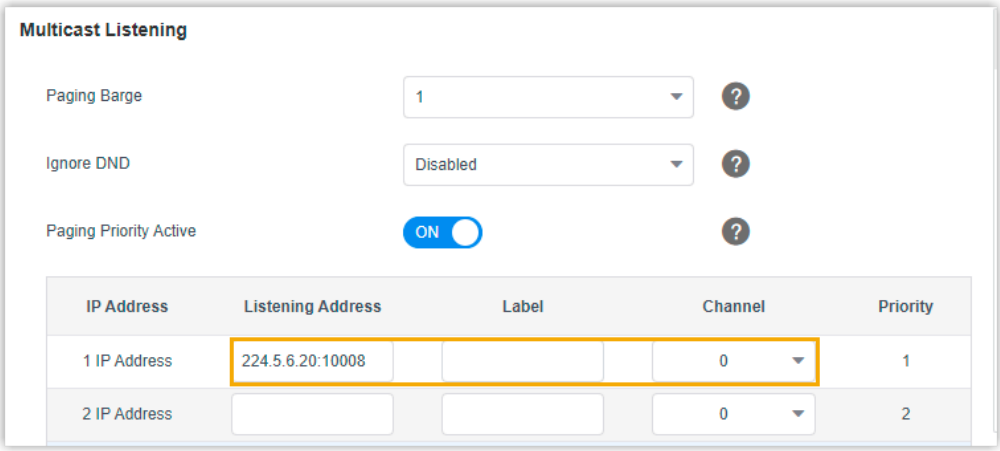


2. Set up multicast listening for the two phones in Packaging Area and Dispatching Area.

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*.

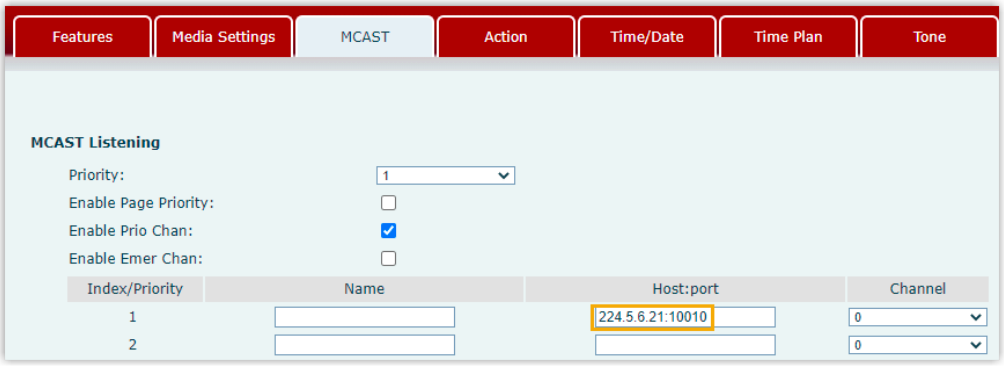


iii. Click **Confirm**.

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*.



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**.

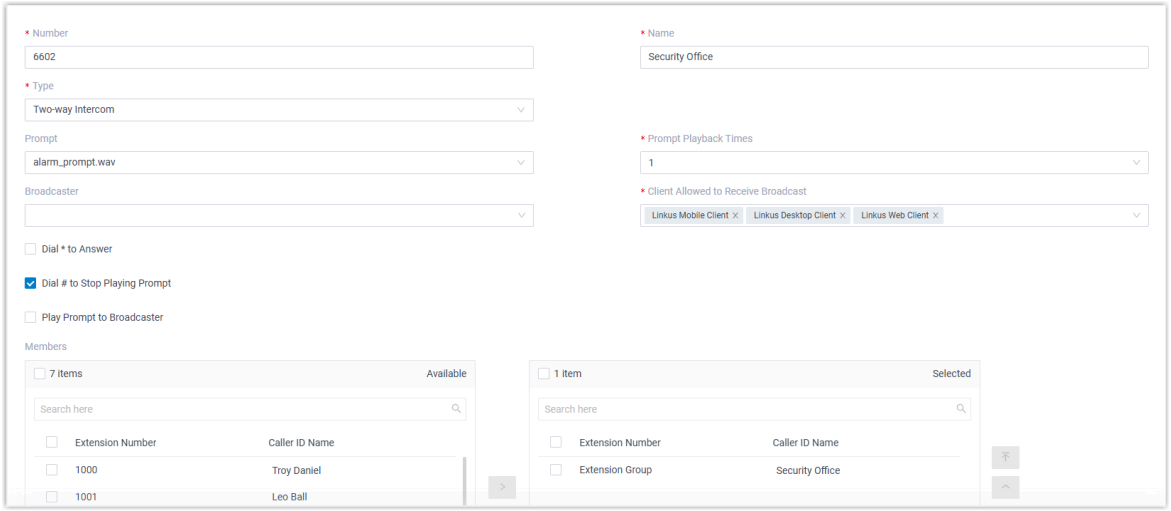
Place an intercom call to multiple users

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 web portal, go to **Call Features > Paging/Intercom**, click **Add**.
2. Configure a two-way intercom group.



Item	Description
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**.

Item	Description
Prompt	Optional. To play a prompt before making an announcement, you can select a custom prompt. In this example, select **alarm_prompt.wav**. **Note:** To customize a prompt, see Record a Custom Prompt or Upload a Custom Prompt.
Prompt Playback Times	Specify how many times the prompt will be played and repeated. **Note:** Enter a value between 1 and 100, or select **Unlimited** to play the prompt in a loop.
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.
Client Allowed to Receive Broadcast	Select the desired clients for receiving intercom calls. **Note:** Intercom calls initiated by the feature code will NOT be restricted by this configuration and will call all the clients and extension endpoints of members simultaneously.
Dial * to Answer	Optional. To allow users to dial `*` to talk to the broadcaster privately, enable this option. When a user dials `*`, the call is ended from other users' side, and the user can have a private talk with the broadcaster.
Dial # to Stop Playing Prompt	Optional. If a prompt is selected, enabling this option allows the broadcaster to dial # during playback to stop the prompt.
Play Prompt to Broadcaster	Optional. To restrict the broadcaster from hearing the prompt, disable this option. In this example, disable this option. **Note:** This option is available only when a custom prompt is selected and is enabled by default.
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

When dialing the number of the intercom group, the selected members will receive the call through the client(s) you have specified.

- For Linkus clients (Mobile/Desktop/Web) and analog phones, they will ring first, and users need to manually answer the call to listen to the broadcasts.

  > **Note:**
  > If necessary, you can set up user's Linkus clients to automatically answer paging calls. For more information, see Set up Auto Answer for Linkus UC Clients.

- For IP phones, they will 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 web 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 web 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 web 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:

Item	Description
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.

Item	Description
	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 web 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 web 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 web 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.

Call Disposition

Add Disposition Codes

Call Disposition feature allows you to define disposition code for call outcomes with custom labels and brief descriptions, which can be used to categorize and track business calls effectively. This topic describes how to add one or more disposition codes.

Requirements

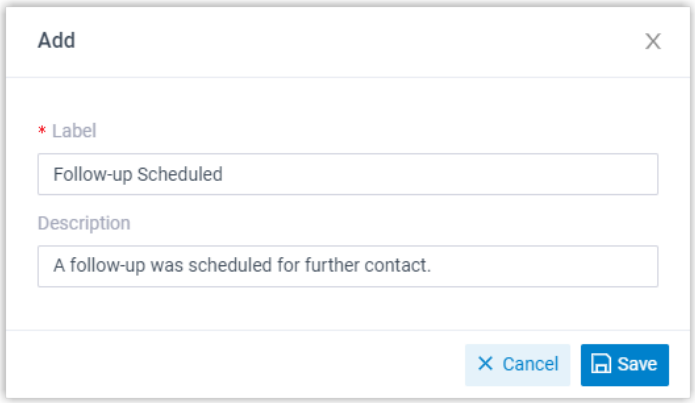
The firmware of Yeastar P-Series PBX System is 37.18.0.59.

Limitations

Supports to add up to 20 call disposition codes.

Procedure

1. Log in to PBX web portal, go to **Call Features > Call Disposition**.
2. Click **Add**.
3. In the pop-up window, complete the following settings.



   - **Label**: Enter a name to quickly identify the outcome of a call.
   - **Description**: Optional. Enter a detailed explanation for the label.
4. Click **Save**.
5. Repeat step **2** - **4** to add more disposition codes as needed.

Result

After adding disposition codes, extension users can conveniently select these pre-defined codes when using call notes to mark and categorize their calls.

> **Note:**
> To achieve this, you need to allow users to use the call note feature. For more information, see Allow Users to Add Notes to Calls.

Call Note

Allow Users to Add Notes to Calls

Call Note feature allows users to add tags and remarks to calls, capturing essential information or decisions made during the conversations. The call notes help users to keep track of calls, making it easier to reference information later or share it with others. This topic describes how to configure the call scenarios where users are allowed to add call notes.

Requirements

- **Firmware**: Version 37.18.0.102 or later
- **Subscription**: Enterprise Plan or Ultimate Plan

Procedure

1. Log in to PBX web portal, go to **PBX Settings > Preferences**.
2. Turn on the switch of **Call Note**.
3. Specify the call scenarios where users can add notes to calls.

Settings	Description
Calls from Queue	If enabled, queue agents can access the call note feature to add tags and remarks during queue calls or in the wrap-up time, and review or edit the call notes later in the corresponding call logs.
Calls from Ring Group	If enabled, ring group members can access the call note feature to add tags and remarks during ring group calls, and review or edit the call notes later in the corresponding call logs.
Calls to Voicemail	If enabled, extension users can access the call note feature to add tags and remarks to the calls that were sent to their extension's voicemails in the corresponding call log. **Note:** For calls sent to group voicemails, only administrators can add and edit call notes for the corresponding calls in the call detail records (CDR).
Calls to Extensions	If enabled, extension users can access the call note feature to add tags and remarks during the calls they receive, and

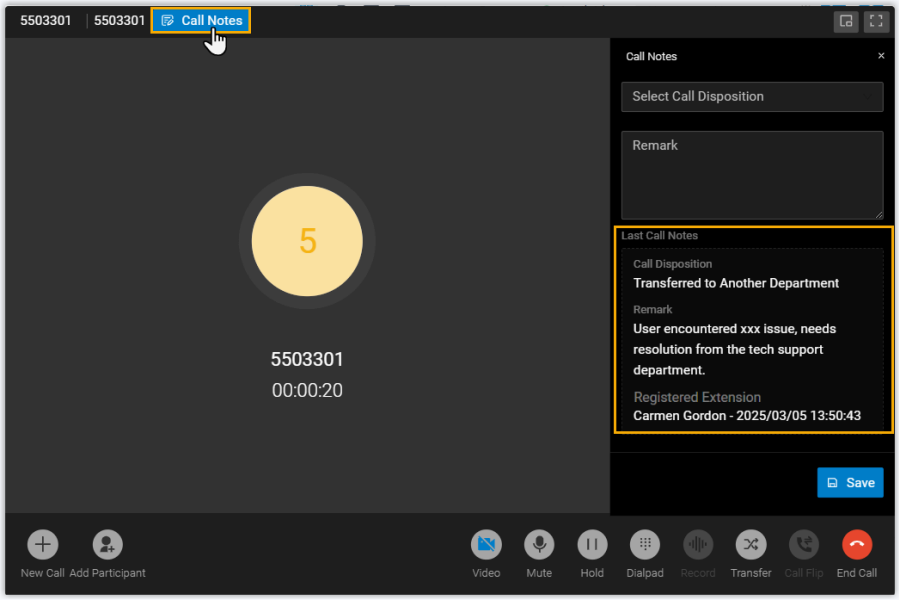
Settings	Description
	review or edit the call notes later in the corresponding call logs.
Outbound Calls	If enabled, extension users can access the call note feature to add tags and remarks during outbound calls they initiate, and review or edit the call notes later in the corresponding call logs.

4. Click **Save**.

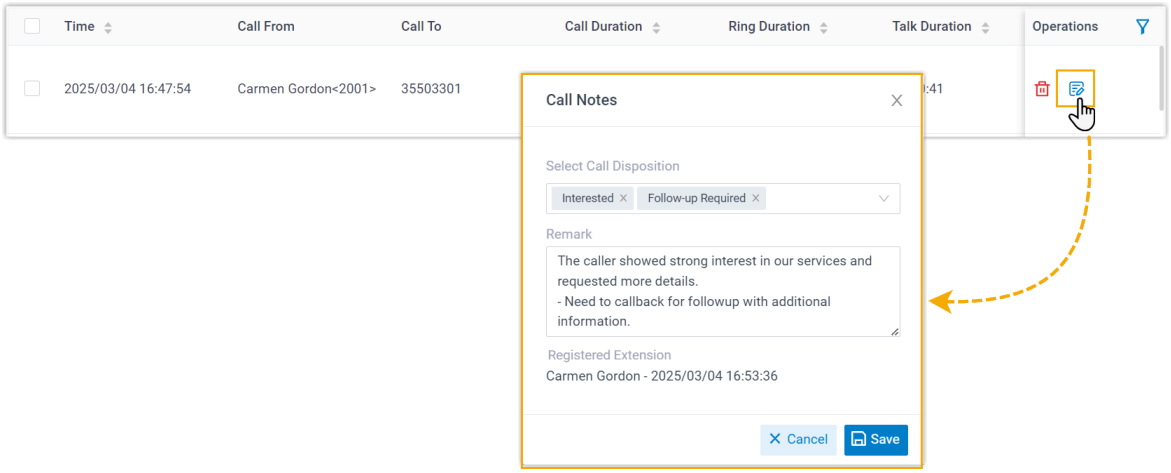
Result

- The call note feature is enabled. During an active call on Linkus Clients, users can conveniently select pre-defined disposition codes as call tags, and add remarks for the call to note down essential information.

> **Note:**
> - To ensure that users can select pre-defined codes in call notes, you MUST configure the disposition codes in advance. For more information, see Add Disposition Codes.
> - If a call is transferred to another user with access to the call note feature, he or she will be able to view the previous call notes after answering the call.



- You can review the call notes for calls in CDR, and edit the notes if necessary.



Blocked/Allowed Numbers

Block Calls To or From a Phone Number

Yeastar P-Series PBX System supports to block incoming and/or outgoing calls by phone number. To stop nuisance calls, you can add phone numbers to the system blocklist. Numbers in the blocklist will be blocked to dial in, dial out, or both.

Restriction

- Blocked numbers do NOT work for the extensions within the PBX. When an extension number matches a blocked number, the extension can still be used for outgoing and incoming calls.
- The maximum number of **Blocked Numbers Lists** and **Numbers per Blocked Numbers List** varies depending on your PBX model.

Model	Blocked Numbers Lists	Numbers per Blocked Numbers List
P520	256	100
P550	256	100
P560	256	100
P570	512	200

Background information

Yeastar P-Series PBX System allows you to handle calls by phone number in the following ways:

Call Handling Based on Caller ID

This feature makes it possible for routing or blocking incoming calls from internal or external users by phone number. You can customize different call handling rules for each extension.

For more information, see Handle Incoming Calls Based on Caller ID.

Blocked Numbers

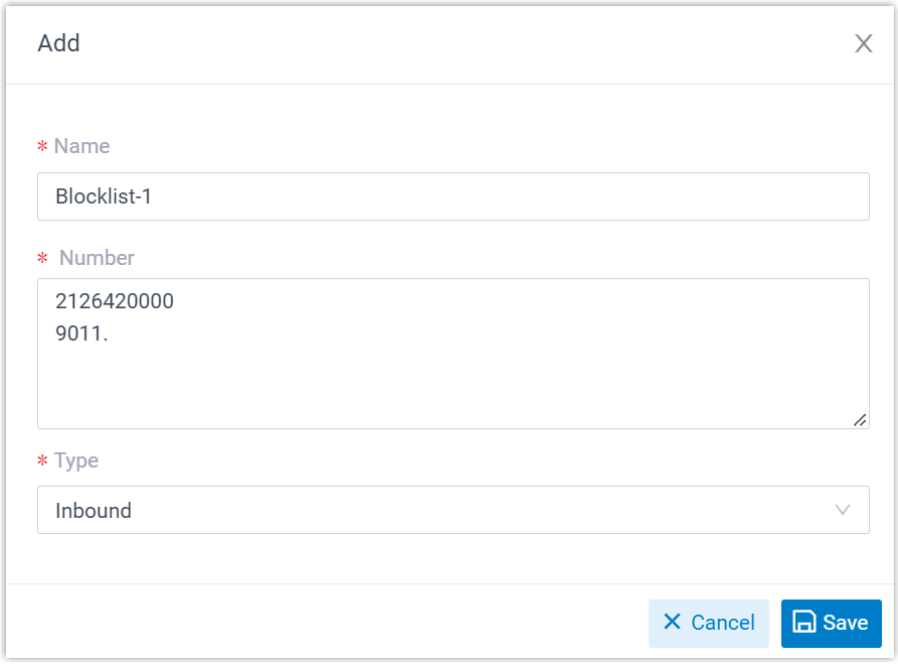
This feature makes it possible for blocking inbound and/or outbound calls to external users by phone number. If you list a phone number in the system blocklist, all the PBX extensions can NOT reach or be reached by the phone number.

For more information, see the following instructions.

> **Note:**
> System blocklist has higher priority than individual blocklist.

Procedure

1. Log in to PBX web portal, go to **Call Features > Blocked/Allowed Numbers > Blocked Numbers**.
2. Click **Add** to set up a blocked number list.
3. In the pop-up window, configure as follows:



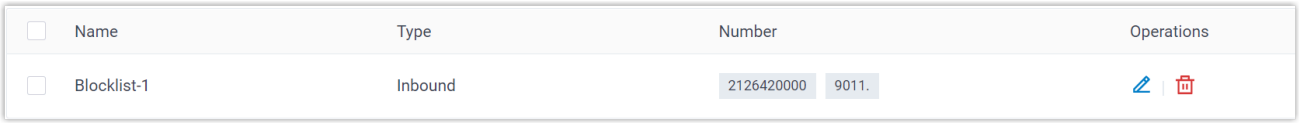
- **Name**: Enter a name to help you identify the number(s) to be blocked.
- **Number**: Enter a specific number or a number pattern per line.
  - To block a specific number, enter a specific number. For example, enter `2126420000`.
  - To block a range of numbers, enter a wildcard pattern. For example. enter `9011.` to block numbers starting with 9011.

    For more information about wildcard pattern, see DID Pattern and Caller ID Pattern.
- **Type**: Select a type from the drop-down list.
  - **Inbound**: Block the number(s) from calling into the PBX.
  - **Outbound**: Block PBX extensions from calling the number(s).
  - **Both**: Block the number(s) from calling into the PBX and block the PBX extensions from calling the number(s).

4. Click **Save** and **Apply**.

Result

The blocked numbers list is displayed on the web page as the following figure shows. The added numbers will be blocked based on the type you selected.



Export and Import Blocked Numbers

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

Export all blocked numbers

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

1. Log in to PBX web portal, go to **Call Features > Blocked/Allowed Numbers > Blocked Numbers**.
2. Click **Export**.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see Blocked Numbers Parameters.

Import blocked numbers

We recommend that you export blocked 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 Blocked Numbers Parameters.

Procedure

1. Log in to PBX web portal, go to **Call Features > Blocked/Allowed Numbers > Blocked Numbers**.
2. Click **Import**.
3. In the pop-up window, click **Browse** to select the UTF-8.csv file you prepared.

4. Click **Import**.

Result

The blocked numbers in the CSV file are displayed in the **Blocked Numbers** list.

Related information

Import and Export -FAQ

Manage Blocked Numbers

This topic describes how to edit and delete blocked numbers lists.

Edit blocked numbers lists

1. Log in to PBX web portal, go to **Call Features > Blocked/Allowed Numbers > Blocked Numbers**.
2. Click beside a desired list.
3. In the pop-up window, edit the name, the blocked number(s), or blocked type as needed.
4. Click **Save** and **Apply**.

Delete blocked numbers lists

1. Log in to PBX web portal, go to **Call Features > Blocked/Allowed Numbers > Blocked Numbers**.
2. To delete a blocked numbers list, do as follows:
   a. Select the checkbox of a desired list, then click .
   b. In the pop-up window, click **OK**.
3. To bulk delete blocked numbers lists, do as follows:
   a. Select the checkboxes of desired lists, then click **Delete**.
   b. In the pop-up window, click **OK**.

The blocked numbers lists are deleted successfully. All the numbers in the deleted lists are no longer blocked, they can call into the PBX and be called by PBX extension users.

Allow Calls To or From a Phone Number

If trusted phone numbers happen to be listed in system blocklist, you can add the trusted phone numbers to system allowlist. Numbers in the allowlist are allowed to dial in, dial out, or both.

> **Note:**
> The **Allowed Number** has higher priority than the **Blocked Number**; Adding numbers in **Allowed Number** doesn't mean that PBX only allow these numbers to dial in or be dialed out.

Limitations

The maximum number of **Allowed Numbers Lists** and **Numbers per Allowed Numbers List** varies depending on your PBX model.

Model	Allowed Numbers Lists	Numbers per Allowed Numbers List
P520	256	100
P550	256	100
P560	256	100
P570	512	200

Background information

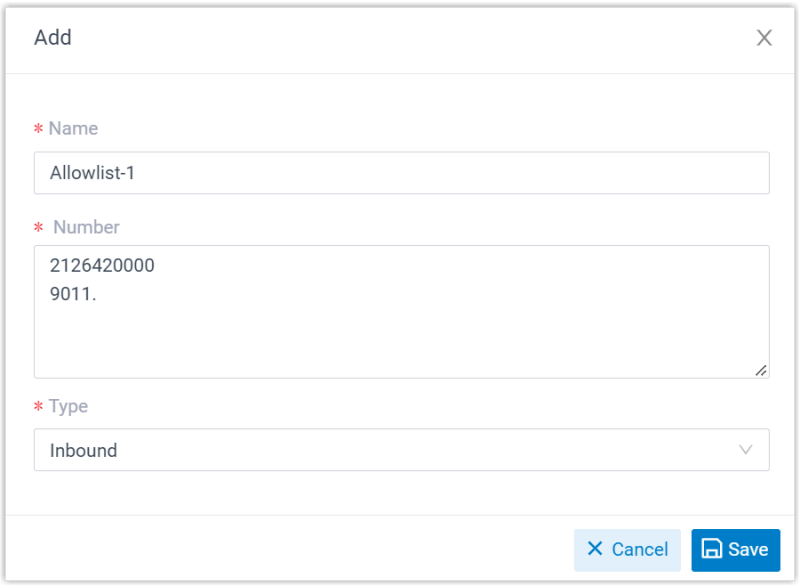
If your customers' phone numbers happen to be listed in system blocklist or individual blocklist, you can add trusted phone numbers to the allowlist.

To add trusted phone numbers to individual allowlist, see Handle Incoming Calls Based on Caller ID.

To add trusted phone numbers to system allowlist, see the following instructions.

Procedure

1. Log in to PBX web portal, go to **Call Features > Blocked/Allowed Numbers > Allowed Numbers** .
2. Click **Add** to set up an allowed number list.
3. In the pop-up window, configure as follows:



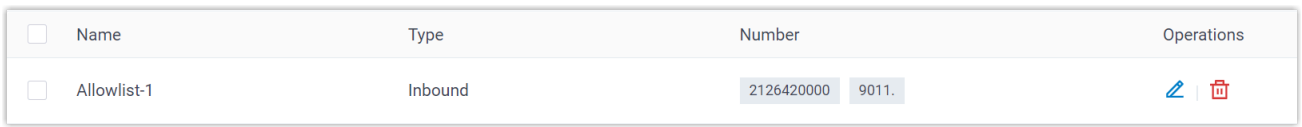
- **Name**: Enter a name to help you identify the number(s) to be allowed.
- **Number**: Enter a specific number or a number pattern per line.
  - To allow a specific number, enter a specific number. For example, enter `2126420000`.
  - To allow a range of numbers, enter a wildcard pattern. For example. enter `9011.` to allow numbers starting with 9011.

    For more information about wildcard pattern, see DID Pattern and Caller ID Pattern.
- **Type**: Select a type from the drop-down list.
  - **Inbound**: Allow the number(s) to call into the PBX.
  - **Outbound**: Allow PBX extensions to call the number(s).
  - **Both**: Allow the number(s) to call into the PBX and allow PBX extensions to call the number(s).

4. Click **Save** and **Apply**.

Result

The allowed numbers list is displayed on the web page as the following figure shows. The added numbers can communicate with the PBX extensions based on the type you selected.



Export and Import Allowed Numbers

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

Export all allowed numbers

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

1. Log in to PBX web portal, go to **Call Features > Blocked/Allowed Numbers > Allowed Numbers** .
2. Click **Export**.

A CSV file is saved to your computer. To check and edit parameters in the CSV file, see Allowed Numbers Parameters.

Import allowed numbers

We recommend that you export allowed 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 Allowed Numbers Parameters.

Procedure

1. Log in to PBX web portal, go to **Call Features > Blocked/Allowed Numbers > Allowed Numbers** .
2. Click **Import**.
3. In the pop-up window, click **Browse** to select the UTF-8.csv file you prepared.
4. Click **Import**.

Result

The allowed numbers in the CSV file are displayed in the **Allowed Numbers** list.

Related information

Import and Export -FAQ

Manage Allowed Numbers

This topic describes how to edit and delete allowed numbers lists.

Edit allowed numbers lists

1. Log in to PBX web portal, go to **Call Features > Blocked/Allowed Numbers > Allowed Numbers** .
2. Click beside a desired list.
3. In the pop-up window, edit the name, the allowed number(s), or type as needed.
4. Click **Save** and **Apply**.

Delete allowed numbers lists

1. Log in to PBX web portal, go to **Call Features > Blocked/Allowed Numbers > Allowed Numbers** .
2. To delete an allowed numbers list, do as follows:
   a. Select the checkbox of a desired list, then click .
   b. In the pop-up window, click **OK**.
3. To bulk delete allowed numbers lists, do as follows:
   a. Select the checkboxes of desired lists, then click **Delete**.
   b. In the pop-up window, click **OK**.

The allowed numbers lists are deleted successfully. If the numbers in the deleted lists match the numbers or the number patterns from Blocked Numbers, they would be blocked based on the blocking type.

Messaging

Yeastar P-Series PBX System Omnichannel Messaging Overview

Yeastar P-Series PBX System offers omnichannel messaging feature, which allows a business to integrate different messaging channels with the business phone system. In this way, customers are able to reach the business through SMS and social media they prefer, while business agents can centrally receive and respond to customers' queries sent from different messaging channels on their Linkus UC Clients.

Requirements

- **Firmware**: Version 37.12.0.23 or later
- **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP)

Feature highlights

All-in-one Message Inbox

Agents are able to receive and respond to customers' queries from different messaging channels directly on their Linkus UC Clients, greatly saving their time by eliminating the need of switching between apps or services to check for messages. The messages are stored on the PBX server, providing a central record of all the messaging sessions.

Customer Contact using Business Number

Agents can contact customers using a business number, while keeping their own personal mobile number private. If necessary, the messaging session can be easily elevated to a call to reach the customer, so that the agent can resolve issues faster via voice call.

Seamless Collaboration across Agents

Agents can hand off customers' issue to another agent by transferring the conversation, the new agent can quickly review the whole chat history and take over the conversation without hassle.

Automatic Chat Assignment

Route your business messages from different messaging channels to agents, who can share the workload across teams to reduce customer service response time. The system automatically assigns chats to the first agent that picks up the session from the queue.

Configuration guide

For more detailed information and configurations of Omnichannel Messaging, see Omnichannel Messaging Administrator Guide.

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

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. • **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**. **Note:** For outbound calls, the **Max Call Duration (s)** setting of the caller's extension takes precedence.
Tone Region	Select your country or the nearest neighboring country to enable the default dial tone, busy tone, and ring tone.
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.
Flash-Hook Event	Set which event will be triggered by pressing the hook flash. • **3-Way Calling** • **Call Transfer**
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.

Organization Management

Setting	Description
Organization Management	If enabled, you can arrange extension users into organizations.
Company Name	Set your company name, which will be used as the root organization name.

Internal Chat

Setting	Description
Internal Chat	The option is enabled by default. If disabled, extension users will NOT be able to access and use the internal chat feature (Instant Messaging, IM) on their Linkus UC clients. **Note:** The Linkus UC clients that can apply this setting are as listed below: • **Linkus Mobile Client** ◦ Linkus iOS Client: Version 5.2.9 or later ◦ Linkus Android Client: Version 4.13.16 or later • **Linkus Desktop Client** ◦ macOS Desktop: Version 1.2.10 or later ◦ Windows Desktop: Version 1.2.14 or later • **Linkus Web Client**

Distinctive Caller ID Name

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.

Masked Number

Specify the scenario(s) where external number will be masked. Once enabled, the number displayed in the call window and call logs will be masked.

Note:

- The masking rule applies when receiving and making calls using IP phones, softphones, or Linkus UC Clients. However, when using analog phones, the external numbers will not be masked.
- If the external number is shorter than 6 digits, it will not be masked.
- Callback to a masked number is not allowed.

Setting	Description
Calls initiated via "Open API"	If enabled, destination number will be masked when a third-party application initiates external calls through the API interface.
Calls initiated via "Speed Dial"	If enabled, destination number will be masked when extension users make external calls through Speed Dial.
Calls initiated via "Click to Call"	If enabled, when extension users initiate calls via click-to-call using 'Yeastar Linkus for Google' Chrome extension, destination number will be masked. **Note:** The version of the Chrome extension must be 4.11.1 or later.
Incoming Calls	If enabled, external numbers will be masked when extension users receiving inbound calls.

Call Notes

Specify the call scenarios where call notes can be used to add tags and remarks to calls.

Settings	Description
Calls from Queue	If enabled, queue agents can access the call note feature to add tags and remarks during queue calls or in the wrap-up time, and review or edit the call notes later in the corresponding call logs.
Calls from Ring Group	If enabled, ring group members can access the call note feature to add tags and remarks during ring group calls, and review or edit the call notes later in the corresponding call logs.
Calls to Voicemail	If enabled, extension users can access the call note feature to add tags and remarks to the calls that were sent to their extension's voicemails in the corresponding call log. **Note:**

Settings	Description
	For calls sent to group voicemails, only administrators can add and edit call notes for the corresponding calls in the call detail records (CDR).
Calls to Extensions	If enabled, extension users can access the call note feature to add tags and remarks during the calls they receive, and review or edit the call notes later in the corresponding call logs.
Outbound Calls	If enabled, extension users can access the call note feature to add tags and remarks during outbound calls they initiate, and review or edit the call notes later in the corresponding call logs.

Presence

Customize presence status to indicate extension users' availability. The presence setting will be synchronized across Linkus UC Clients with the following versions:

- **Linkus iOS Client**: Version 5.15.8 or later
- **Linkus Android Client**: Version 5.15.4 or later
- **Linkus Windows Desktop**: Version 1.13.3 or later
- **Links Mac Desktop**: Version 1.13.3 or later

Note:
It's recommended to keep the default configuration for **Do Not Disturb** status. In this status, all incoming calls are always routed to the designated destination, and extension users will not receive calls from queues, ring groups, or paging groups.

DTMF

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.

Extension Type	Default Range
User Extension	1000 - 5999
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
WebRTC Trunk Number	6800 - 6899

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 customize your own music on hold.

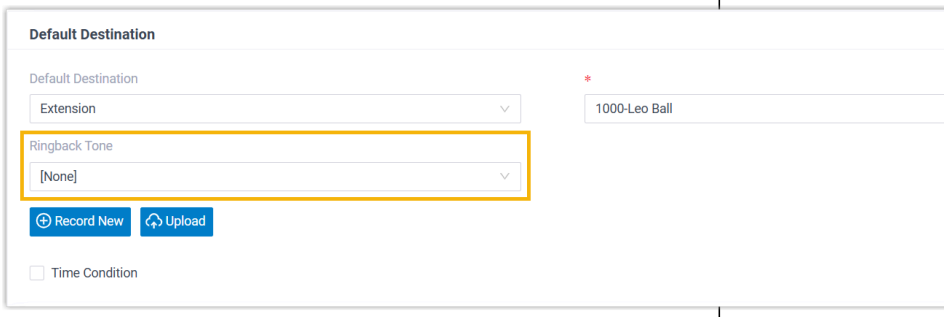
  For more information, see Set up a Custom MoH Playlist.

Voice prompt preference settings

Navigation path: **PBX Settings > Voice Prompt > Prompt Preferences**.

Setting	Description
Music on Hold	The playlist to be played when a call is on hold. **Note:** The available playlists are synchronized with playlists in **Music on Hold**.
Music on Hold for Call Forwarding	The music to be played when the caller is put on hold during call forwarding. • **Music on Hold**: Play **Music on Hold** to the caller. • **Ringing Tone**: Play ringing tone to the caller.
Invalid Phone Number Prompt	The prompt to be played when a callee number is invalid. **Note:** The available prompts are synchronized with **Custom Prompt**.
Busy Line Prompt	The prompt to be played when a trunk is in use.

Setting	Description
	Note: The available prompts are synchronized with **Custom Prompt**.
Call Failure Prompt	The prompt to be played when a call is failed to be sent out. **Note:** The available prompts are synchronized with **Custom Prompt**.
Event Notification Prompt	The prompt to be played when PBX places a call to notify callee that a specific event occurs. **Note:** The available prompts are synchronized with **Custom Prompt**.
Play Call Forwarding Prompt	Whether to inform the user that the current call will be forwarded.
Play Call Waiting Prompt	The prompt to be played when the caller is waiting to be connected to an extension user that is on a call. **Note:** This setting works only for SIP trunks, not for analog trunks. • If the caller is an **extension user**, the system will play call waiting prompt "Sorry! Please hold on, the number you dialed is busy now.", then play ringing tone. • If the caller is an **external user**, the system will play call waiting prompt "Sorry! Please hold on, the number you dialed is busy now.", then play ringing tone or ringback tone (depending on whether you have configured ringback tone for the inbound route via which the caller is routed: **Call Control > Inbound Route > Default Destination > Ringback Tone**).

Setting	Description
	

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 web 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 web 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

Music on Hold (MoH) is intended to reassure callers that they are connected to their calls. Yeastar P-Series PBX System has a default local audio playlist with built-in MoH files. This topic describes how to set up and use a custom MoH playlist.

Background information

Yeastar P-Series PBX System supports two types of MoH playlists:

- Local audio MoH playlist
- Streaming music MoH playlist

Playlist Type	Description
Local audio MoH playlist	This type of playlist contains a list of audio files that are uploaded to the system, and play back when a caller is placed on hold. For more information, see Set up a local audio MoH playlist.
Streaming music MoH playlist	This type of playlist contains a URL that is used to connect to a live audio feed from a particular source. For more information, see Set up a streaming music MoH playlist.

Set up a local audio MoH playlist

Requirements

The audio files to be uploaded must meet the following requirements:

Item	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 8 MB

Limitations

Item	Limitations
Max. local audio MoH playlists	16
Max. audio files in a playlist	8

Step1. Add a local audio MoH playlist

1. Log in to PBX web 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 Type**: Select **Local Audio**.
      - **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. Click **Browse** to choose the desired audio file, then click **Upload**.
   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 put on hold, the system will play audio files in the playlist to the waiting party.

Set up a streaming music MoH playlist

Limitation

Max. streaming music MoH playlists: 5

Step1. Add a streaming music MoH playlist

1. Log in to PBX web 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 Type**: Select **Streaming Music**.
      - **Playlist Name**: Enter a name to help you identify it.
      - **Streaming Music URL**: Enter the URL of an existing music stream.
   c. Click **Save**.
3. 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 put on hold, the system will play the streaming music from the URL to the waiting party.

> **Note:**
> If PBX can not access the URL or if there is no available audio in the URL, the system will not play any sound to the waiting party.

Manage MoH Playlists

This topic describes how to edit or delete MoH playlists.

Edit a MoH playlist

1. Log in to PBX web portal, go to **PBX Settings > Voice Prompt > Music on Hold**.
2. Select the desired playlist, click  .
3. Edit the playlist according to your needs.
   - **Playlist Name**: Change the playlist name.
   - **Play Order**: Decide whether to play the playlist alphabetically or randomly.

     > **Note:**
     > This option is only available for **Local Audio MoH Playlists**.

   - **Streaming Music URL**: Change the URL of the streaming music.

     > **Note:**
     > This option is only available for **Streaming Music MoH Playlists**.
4. Click **Save** and **Apply**.

Delete MoH playlists

1. Log in to PBX web portal, go to **PBX Settings > Voice Prompt > Music on Hold**.
2. Select the desired playlist, click  .
3. In the pop-up dialog box, click **OK**.
4. Click **Apply**.

If the deleted playlist is used for **Music on Hold** or **Music on Hold for Call Forwarding**, the system will not play any sound to the party who is put on hold during a call or call forwarding.

Manage MoH Audio Files

This topic describes how to manage audio files of a local audio MoH playlist.

Procedure

1. Log in to PBX web portal, go to **PBX Settings > Voice Prompt > Music on Hold**.
2. In the **Operations** column, click MoH beside the desired local audio MoH playlist.
3. In the pop-up window, manage MoH audio files according to your needs, then click **OK**.
   - 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 .
4. Click **OK** and **Apply**.

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 web 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

Type	P520	P550	P560	P570
Max number of Custom Prompts	32	64	128	128

Procedure

1. Log in to PBX web 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

Type	P520	P550	P560	P570
Max number of Custom Prompts	32	64	128	128

Procedure

1. Log in to PBX web 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 web 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.

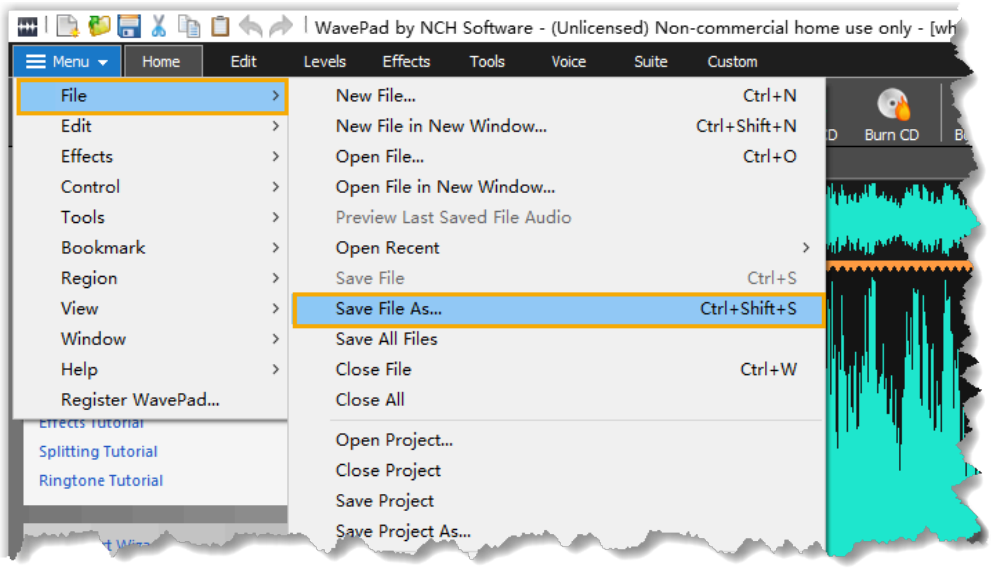
In this topic, we take the followings as examples to show you how to convert file format.

- Convert Audio Files via WavePad
- Convert Audio Files Online

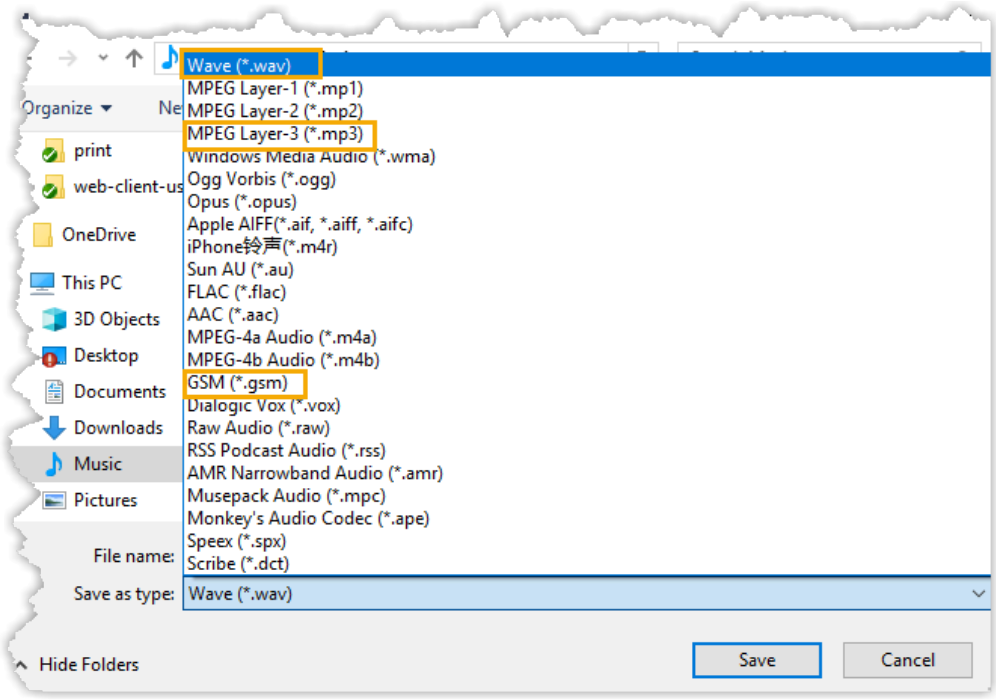
Convert audio files via WavePad

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**.



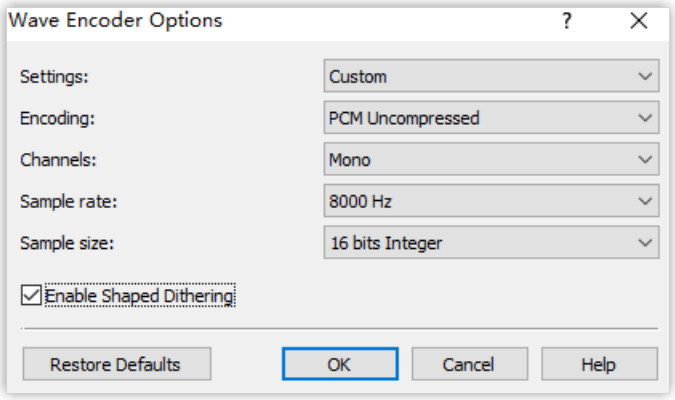
3. In the **Save as type** drop-down list, select `Wave(*.wav)`, `MPEG Layer-3(*.mp3)`, or `GSM(*.gsm)`, click **Save**.



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

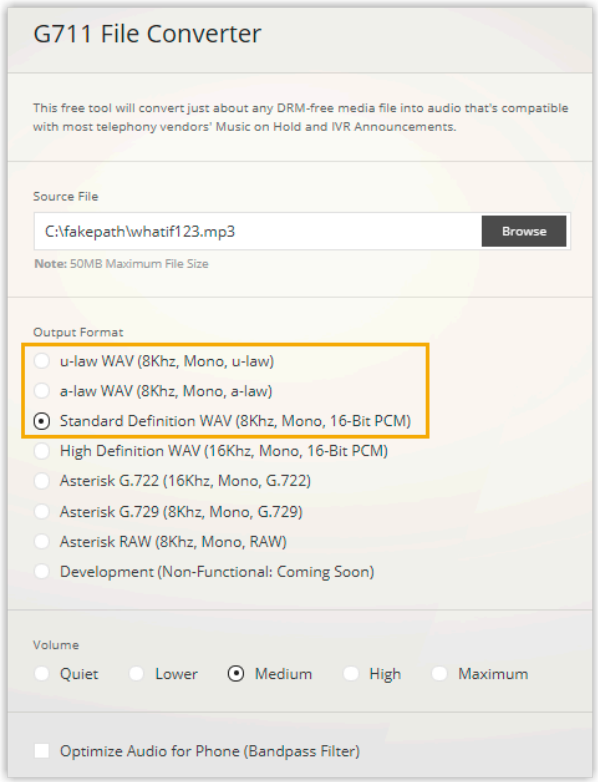


Convert audio files online

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
- Local audio MoH playlists

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.

Option	Requirement
File Size	Up to 8 MB.
File Format	`.wav`, `.mp3`, or `.gsm`. • PCM, 8Khz, 16bit, 128kbps • A-law (g.711), 8Khz, 8bit, 64kbps • u-law (g.711), 8Khz, 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 33.

Setting	Description
Basic Settings	
SIP UDP Port	UDP Port used for SIP registration. The default value is 5060. **Note:** If you change the port, the extensions that use UDP protocol must re-register to the new port.
SIP TCP Port	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. **Note:** If you change the port, the extensions that use TCP protocol must re-register to the new port.
RTP Port Range	RTP port for transmitting data. The default range is 10000-12000. **Note:** • The From-port value should be greater than 10000.

Table 33. (continued)

Setting	Description
	• The From-port and the To-port should have a difference value between 100 and 10000.
Outbound SIP Port Range	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. To change the port, select the checkbox of **Outbound SIP Port Range** and set the port.
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)	Default registration duration (in seconds). **Note:** The actual duration needs to subtract 10 seconds from the value you fill in.
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 34.

Setting	Description
iLBC Mode	The iLBC codec supports the following modes: • **20 ms** • **30 ms** To get better voice quality, you need to set the iLBC mode according to your SIP endpoints.
Codec Selection	Select the codec. **Available values**: u-law, a-law, GSM, H264, VP8, H263, H263P, iLBC, G722, G726, SPEEX, ADPCM, G729A, MPEG4, Opus. **Note:** • 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.
Allow Opus Transcoding	If this option is enabled, when one party in a call uses **Opus** codec and the other party does not support it, the PBX will automatically perform codec transcoding to match the other party's codec, ensuring successful call establishment even when both parties use different codecs, and improving call quality. **Note:** Enable this option will consume more system resources, such as system memory.

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	

Setting	Description
TLS Certificate	Upload a server certificate when PBX acts as a server.
TLS Verify Client	Verify client certificate when PBX acts as a server. **Note:** If enabled, you need to upload a client certificate to the PBX and TLS client.
When PBX acting as a Client	
TLS Connection Method	Specify a protocol for outbound client connections. • TLS V1.0 • TLS V1.2 **Note:** It's recommended to use the more secure TLS V1.2.
TLS Verify Server	Verify server certificate when PBX acts as a client. **Note:** If enabled, you need to upload a server certificate to the PBX.

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. • **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.
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-INVITE 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. • From • Contact • Remote-Party-ID • P-Asserted-Identity

Setting	Description
	• P-Preferred-Identity
Get DID From	Decide the system will retrieve DID from which header field. • To • Invite • Diversion • Remote-Party-ID • P-Asserted-Identity • P-Preferred-Identity • P-Called-Party-ID **Note:** If **Remote-Party-ID** is selected but the SIP trunk doesn't support this, the system will retrieve DID from **Invite** header.
SIP Request Header	
User Agent	Set the user agent that will be included when sending SIP packages out.
Internal Alert Info	Set an "alert info text" to add to Alert-info header in INVITE request for internal calls. When receiving an internal call, the phone will inspect "Alert-Info" header to determine which ring tone it should use for ringing.
Other Options	
Allow Guest	If enabled, PBX will accept unknown calls.
Support Message Request	Whether to support SIP Message Request or not.
Inband Progress	Whether to enable inband progress or not. The Inband Progress setting applies to all the extensions. **Note:** To configure global Inband Progress setting, you need to contact Yeastar support to configure a custom configuration file. • **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.

Setting	Description
Enable uaCSTA Connection	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. **Note:** Your IP phone should support uaCSTA standard to use this function.
Extension Forwarding with Diversion SIP Header	If this option is enabled, when an extension's call forwarding destination is another extension, a Diversion header will be included in the INVITE request to inform the destination of the source extension from which the call was forwarded.
P Asserted Identity	If this option is enabled, a `P Asserted Identity` field will be carried in the SIP header for calls that are transferred or forwarded to convey the identity of the call initiator. **Note:** This setting is only available for internal calls. For external calls, see SIP Headers settings for trunk.

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 web 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.

Internet protocols

Yeastar P-Series PBX System supports the following Internet protocols:

- **IPv4 only**: The PBX can be configured with IPv4 address, and can communicate with the devices that support IPv4 protocol.
- **IPv4 / IPv6 dual stack**: The PBX can be configured with both IPv4 address and IPv6 address, and can communicate with a wide range of devices that support IPv4 protocol or IPv6 protocol.

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.
- IPv6 over PPPoE is NOT supported.

Configure a Static IPv4 Address

This topic describes how to configure a static IPv4 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 and WAN port of Yeastar P-Series PBX System to connect different networks, so that LAN/WAN uplinks can carry different services through separate ports, optimizing the utilization of network bandwidth. The IP information is as below:

LAN	WAN
• IP address: 192.168.6.124 • Subnet mask: 255.255.255.0 • Gateway address: 192.168.6.1 • DNS server: 192.168.1.1	• IP address: 10.0.0.50 • Subnet mask: 255.255.255.0 • Gateway address: 10.0.0.1 • DNS server: 8.8.8.8

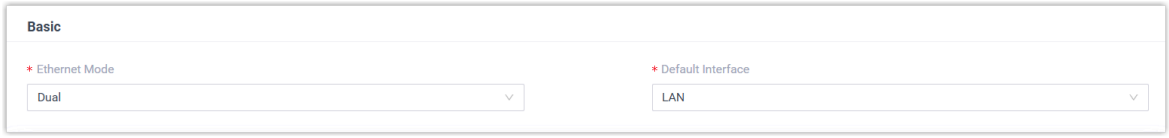
Prerequisites

- 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.

Tip:
To access the PBX, you need to change your PC to the same network segment of the PBX.

Procedure

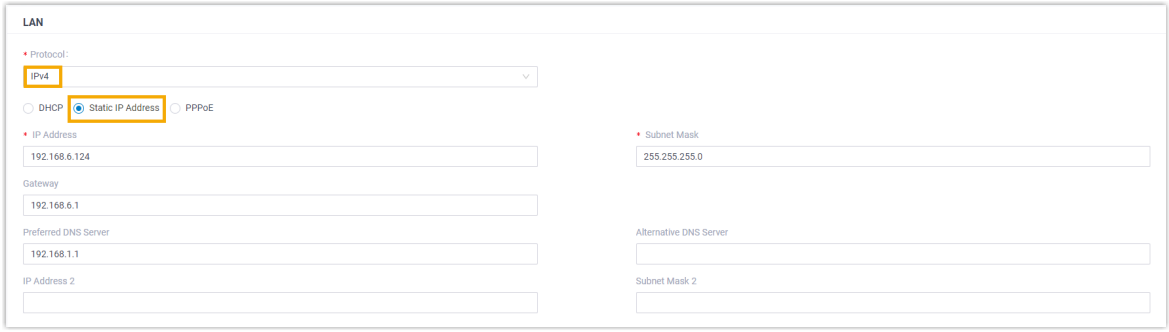
1. Log in to PBX web portal, go to **System > Network > Basic Settings**.
2. In the **Basic** section, configure the following settings:



   - **Ethernet Mode**: Select the Ethernet mode. In this scenario, select **Dual**.
     - **Single**: Only the LAN port 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**: Select a default interface if select **Dual** mode. In this scenario, select **LAN**.
3. In the **LAN** section, select **IPv4** Internet protocol and select **Static IP Address**, then enter the network information for LAN port.



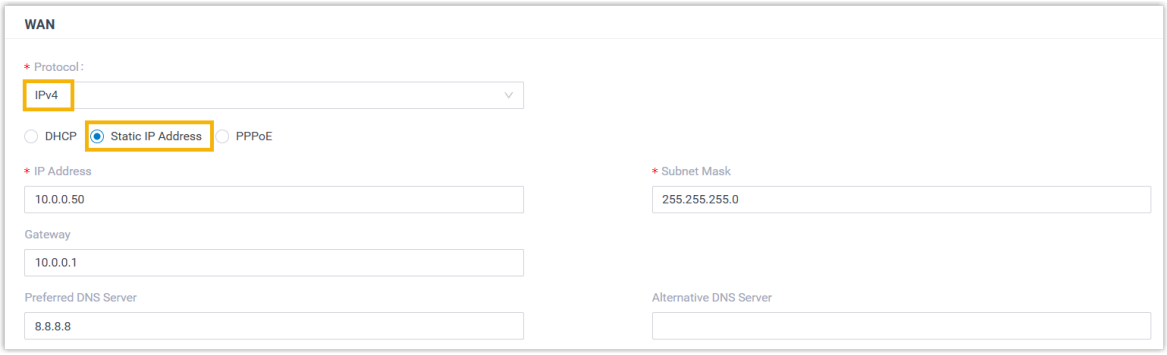
   - **IP Address**: Enter the IP address that is assigned to the PBX.
   - **Subnet Mask**: Enter the subnet mask.
   - **Gateway**: Enter the gateway address.
   - **Preferred DNS Server**: Enter the IP address of preferred DNS server.
   - **Alternative DNS Server**: Optional. Enter the IP address of 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.

4. In the **WAN** section, select **IPv4** Internet protocol and select **Static IP Address**, then enter the network information for WAN port.



- **IP Address**: Enter the IP address that is assigned to the WAN interface.
- **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.

5. Click **Save** and reboot the PBX to take effect.

Result

After the PBX reboots, the LAN interface is changed to 192.168.6.124, and the WAN interface is changed to 10.0.0.50.

Different services will be sent through different ports. For example, LAN interface can be used to send and receive internal network traffic, while the WAN interface can be used to connect SIP providers.

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 IPv4 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 IPv4 Address.

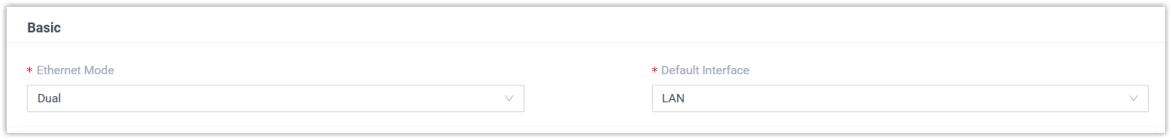
The following instructions assume that you need to use LAN port and WAN port of Yeastar P-Series PBX System to connect different networks, and need to obtain an IP address from the DHCP server.

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 web portal, go to **System > Network > Basic Settings**.
2. In the **Basic** section, configure the following settings:

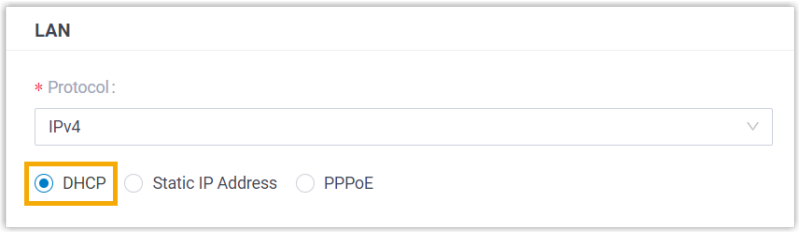


- **Ethernet Mode**: Select the Ethernet mode. In this scenario, select **Dual**.
  - **Single**: Only the LAN port will be used for up-link connection.
  - **Dual**: Both LAN and WAN can be used for up-link connection.

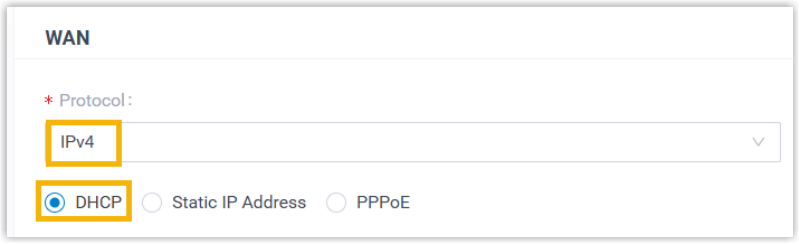
    Note:
    The traffic will be routed to the default interface; you may need to add a static route to override the default route entries, routing the traffic from a specific IP address to the specified destination.
  - **Bridge**: LAN port will be used for up-link connection. WAN port can be used as a bridge to connect other device.

- **Default Interface**: Select a default interface if select **Dual** mode. In this scenario, select **LAN**.

3. In the **LAN** section, select **IPv4** Internet protocol, then select **DHCP**.



4. In the **WAN** section, select **IPv4** Internet protocol, then select **DHCP**.



5. Click **Save** and reboot the PBX to take effect.

Result

The PBX will obtain new IP addresses from the DHCP server in your local network.

You need to log in to the web interface of your router to see assigned IP addresses.

Configure a PPPoE Connection

This topic describes how to configure a PPPoE connection on Yeastar P-Series PBX System to obtain an IPv4 address when the PBX is in Dual network mode.

> **Note:**
> IPv6 over PPPoE is NOT supported.

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:

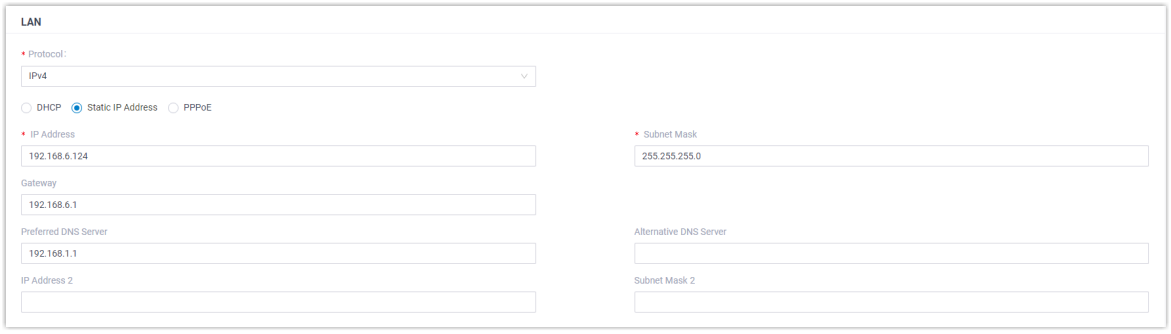
LAN	WAN
Static IP • IP address: 192.168.6.124 • Gateway address: 192.168.6.1 • Subnet mask: 255.255.255.0 • DNS: 192.168.1.1	**PPPoE** • Username: 059219383822 • Password: 19283772

Procedure

1. Log in to PBX web 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 an Internet protocol and select **Static IP Address**, then 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.

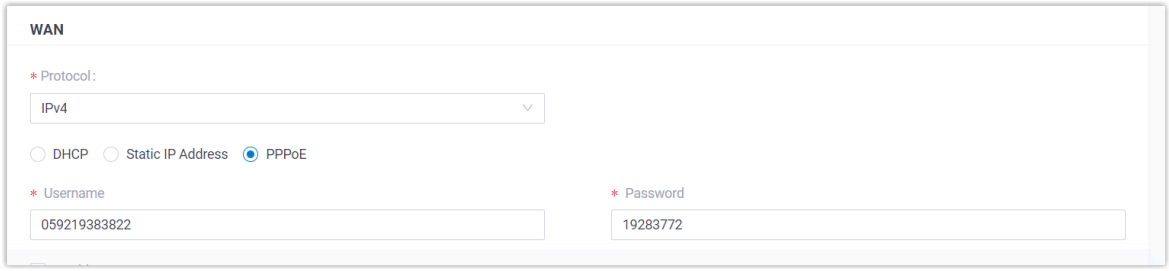
- **Preferred DNS Server**: Enter the IP address of preferred DNS server.
- **Alternative DNS Server**: Optional. Enter the IP address of alternative DNS server.
- **IP Address 2**: Optional. Enter a second IP address for the PBX.

> **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.

4. In the **WAN** section, select **IPv4** and select **PPPoE**, then enter the **Username** and **Password**.

> **Note:**
> IPv6 over PPPoE is NOT supported.



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 web 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 web portal, go to **System > Network > Basic Settings**.
2. Configure the Ethernet port that needs to set up a VLAN.

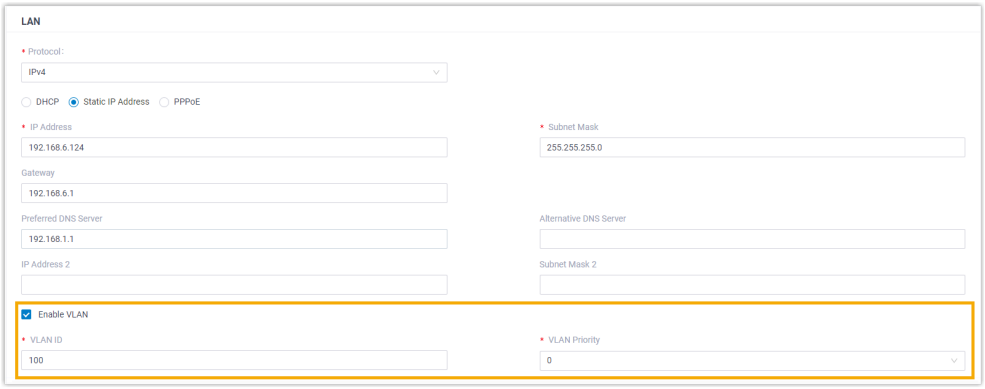
   In the scenario, configure LAN port.

   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.



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 subinterafce

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.

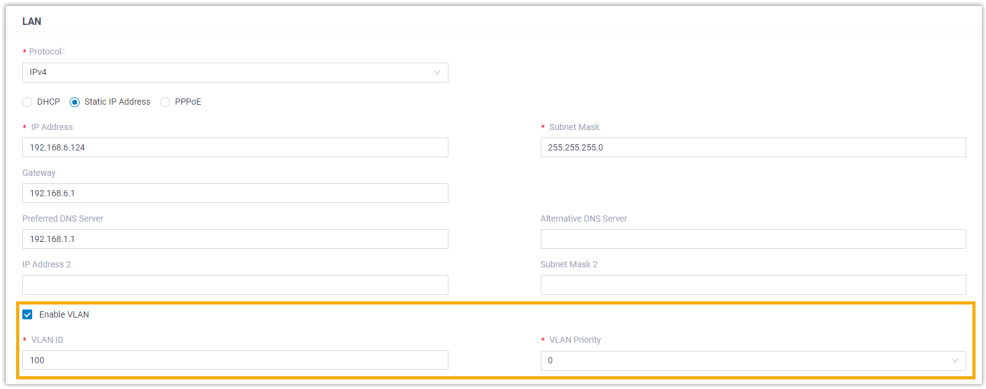
Procedure

1. Log in the PBX web 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*.

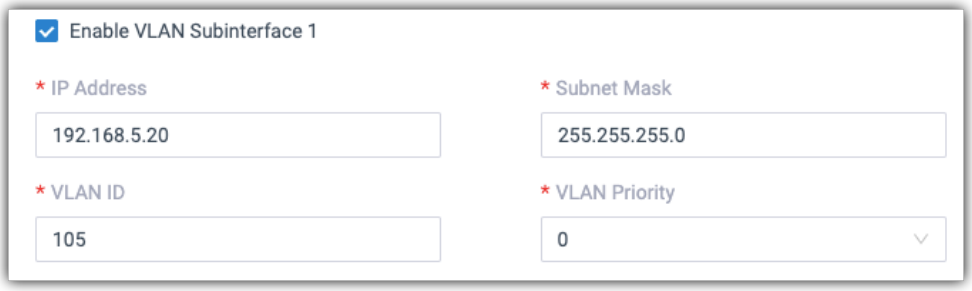
> **Note:**
> The devices that need to communicate with the PBX should have the same VLAN ID.

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.



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*.

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 web 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 web 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.

   > **Important:**
   > If you are using Linkus Web Client, select **HTTPS**.

   b. If **HTTPS** is selected, configure the following settings:
      - **HTTPS Port**: Enter an HTTPS port.
      - **HTTPS Certificate**: Select the default certificate or upload your own certificate.
      - **Supported TLS Version**: Select the supported TLS version for handshake negotiation between PBX server and the connected client.

- **TLS 1.2**: PBX server only supports TLS 1.2 for client-server communication.
- **TLS 1.0, TLS 1.1, and TLS 1.2**: PBX server supports TLS 1.0/1.1/1.2 for client-server communication. The version that will be used depends on the highest supported TLS version on the connected client.

- **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 web 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 web 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
LDAP Port	Port for LDAP Client to access the PBX LDAP Server via LDAP protocol.	389
FTP	Port for file sharing.	21

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 web 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

Yeastar FQDN Overview

A Yeastar-supplied Fully Qualified Domain Name (FQDN) helps you to quickly establish a secure remote connection in only one click. It frees you from the risky port forwarding, complicated network setup, and onerous Linkus server configurations. With the private and secure connection, you don't have to worry about exposing your intranet to the public, or NAT issues to happen and affect your remote calling experience.

What is FQDN?

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 provides the following advantages:

- **Dynamic DNS solution**: Provide a dynamic DNS service for network environments that has no static IP addresses to ensure proper access to the system.
- **Hassle-free network deployment**: Simplify network configurations for remote access as the complicated Network Address Translation (NAT) configurations and port forwarding are eliminated.
- **High call quality**: Avoid NAT issues that affect call quality, thus guarantee remote calling experience.
- **Secure communication**: Eliminate the risk of exposing service ports; secure remote connections with SSL certificates.

Applications

Yeastar FQDN supports remote access to the following features:

Table 35.

Feature	Description	Default Status	Usage Permission Setting
SIP Access	Support remote SIP registration via FQDN, including the registration of remote SIP extension and SIP account trunk. **Important:** The remote SIP access feature does NOT support the remote registration of SIP peer trunk.	Disabled.	• **Account**: Restrict or allow specific accounts to get access to the service via FQDN. **Note:** By default, all accounts are NOT allowed to use the remote SIP access feature. • **IP Address**: Only permit specific IP addresses to get access to the service via FQDN.
Web Access	Support remote access to the PBX web portal or Linkus Web Client via FQDN.	Enabled by default, and cannot be disabled.	• **Account**: Restrict or allow specific accounts to get access to the service via FQDN. **Note:** By default, the super administrator account is restricted from using the remote web access feature. • **IP Address**: Only permit specific IP addresses to get access to the service via FQDN.
Linkus Access	Support remote access to Linkus Clients via FQDN.	Enabled by default, and cannot be disabled.	• **IP Address**: Only permit specific IP addresses to get access to the service via FQDN.
LDAP Access	Support remote LDAP access via FQDN.	Disabled.	• **IP Address**: Only permit specific IP addresses to get access to the service via FQDN.
API Access	Support remote API access via FQDN.	Disabled.	• **IP Address**: Only permit specific IP addresses to get access to the service via FQDN.

For more detailed configurations, see the following topics:

- Configure Network for Remote SIP Access by a Yeastar FQDN
- Configure Network for Remote Web Access by a Yeastar FQDN
- Configure Network for Remote Linkus Access by a Yeastar FQDN
- Configure Network for Remote LDAP Access by a Yeastar FQDN
- Configure Network for Remote API Access by a Yeastar FQDN

Configure Network for Remote SIP Access by a Yeastar FQDN

With a Yeastar FQDN, you can quickly establish a secure tunnel for remote registration of IP phones, alike SIP endpoints, and account trunks, without the need of configuring public IP and port forwarding for the PBX. This topic describes how to configure network for remote SIP access via FQDN.

Prerequisites

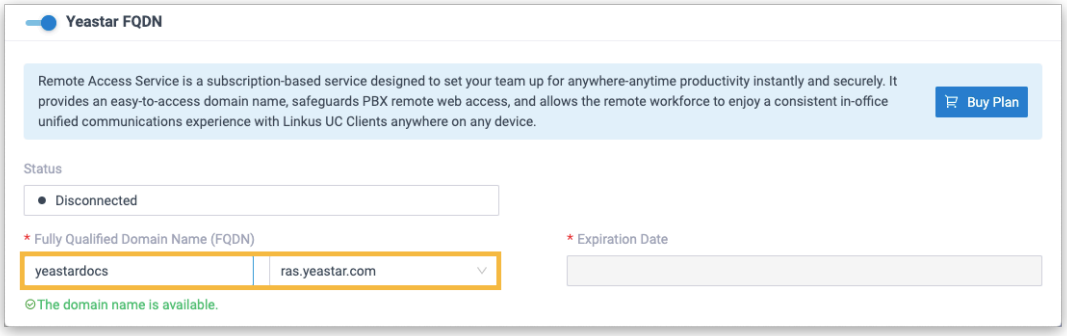
You have subscribed **Enterprise Plan** or **Ultimate Plan**.

Procedure

1. Log in to PBX web portal, go to **System > Network > Yeastar FQDN**.
2. Turn on **Yeastar FQDN**.
3. In the **Fully Qualified Domain Name (FQDN)** field, set up the FQDN domain name.
    a. Select a domain name from the drop-down list.
    b. Enter a host name in the first field.

    > **Note:**
    > Think twice before you enter the hostname. The FQDN cannot be changed after you save the configurations.

    For example, select domain name **ras.yeastar.com** and enter hostname `yeastardocs`, you will get an FQDN **yeastardocs.ras.yeastar.com**.



4. Enable remote SIP access feature and grant usage permissions.

> **Note:**
> By default, all accounts are NOT allowed to use the remote SIP access feature. You need to grant the usage permission to desired accounts.

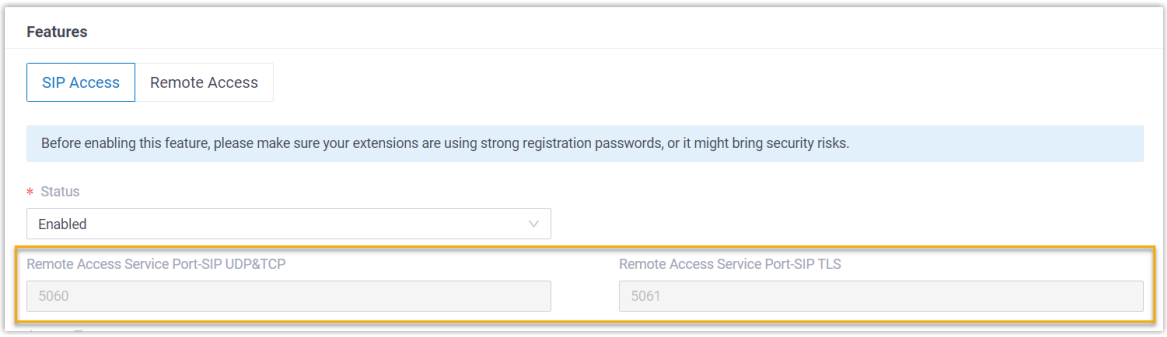
   a. In the **Features** section, go to the **SIP Access** tab.
   b. In the **Status** drop-down list, select **Enabled**.
   c. In the **Access Type** drop-down list, select the account access restriction type.
      - **Allowed Account**: Only the selected accounts can get access to the service.
      - **Restricted Account**: All accounts except for the selected accounts can get access to the service.
   d. Select the desired accounts from the **Available** box to the **Selected** box.
   e. **Optional:** Select the checkbox of **Enable IP Restriction**, and add at least one permitted IP address and subnet mask.

      If you configure this option, only the permitted IP address(es) can use the remote access feature.

5. Click **Save** and **Apply**.

Result

- The Remote Access Service automatically assigns ports for remote SIP access, you can check the port in **Remote Access Service Port**.



- You can implement the followings:
  - Set up a Remote SIP Phone via Yeastar FQDN.
  - Perform remote registration of SIP Account trunk via Yeastar FQDN.

> **Important:**
> The remote registration of SIP peer trunk via Yeastar FQDN is NOT supported.

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 **Standard Plan**, **Enterprise Plan** or **Ultimate Plan** in 60 days.

Related information

Auto Provision IP Phones Remotely (RPS FQDN Method)

Configure Network for Remote Web Access by a Yeastar FQDN

Yeastar FQDN provides secure remote access to PBX web portal or Linkus Web Client, without the need of configuring public IP and port forwarding. This topic describes how to configure network for remote web access via FQDN.

Prerequisites

You have subscribed any of the following plans:

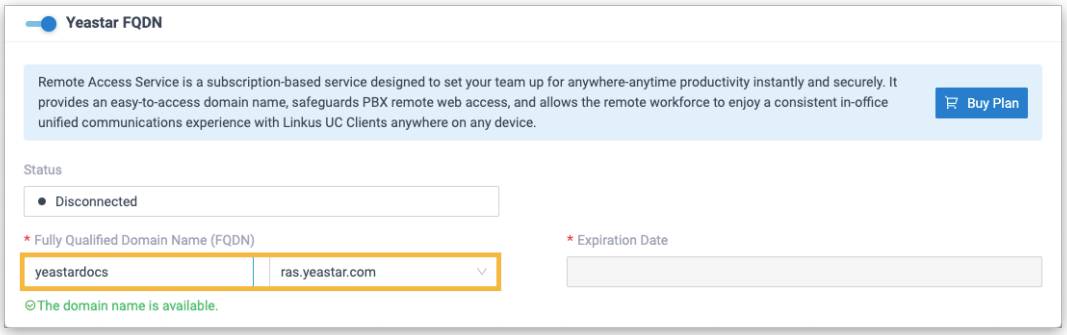
- **Standard Plan**
- **Enterprise Plan**
- **Ultimate Plan**

Procedure

1. Log in to PBX web portal, go to **System > Network > Yeastar FQDN**.
2. Turn on **Yeastar FQDN**.
3. In the **Fully Qualified Domain Name (FQDN)** field, set up the FQDN domain name.
   a. Select a domain name from the drop-down list.
   b. Enter a host name in the first field.

   > **Note:**
   > Think twice before you enter the hostname. The FQDN cannot be changed after you save the configurations.

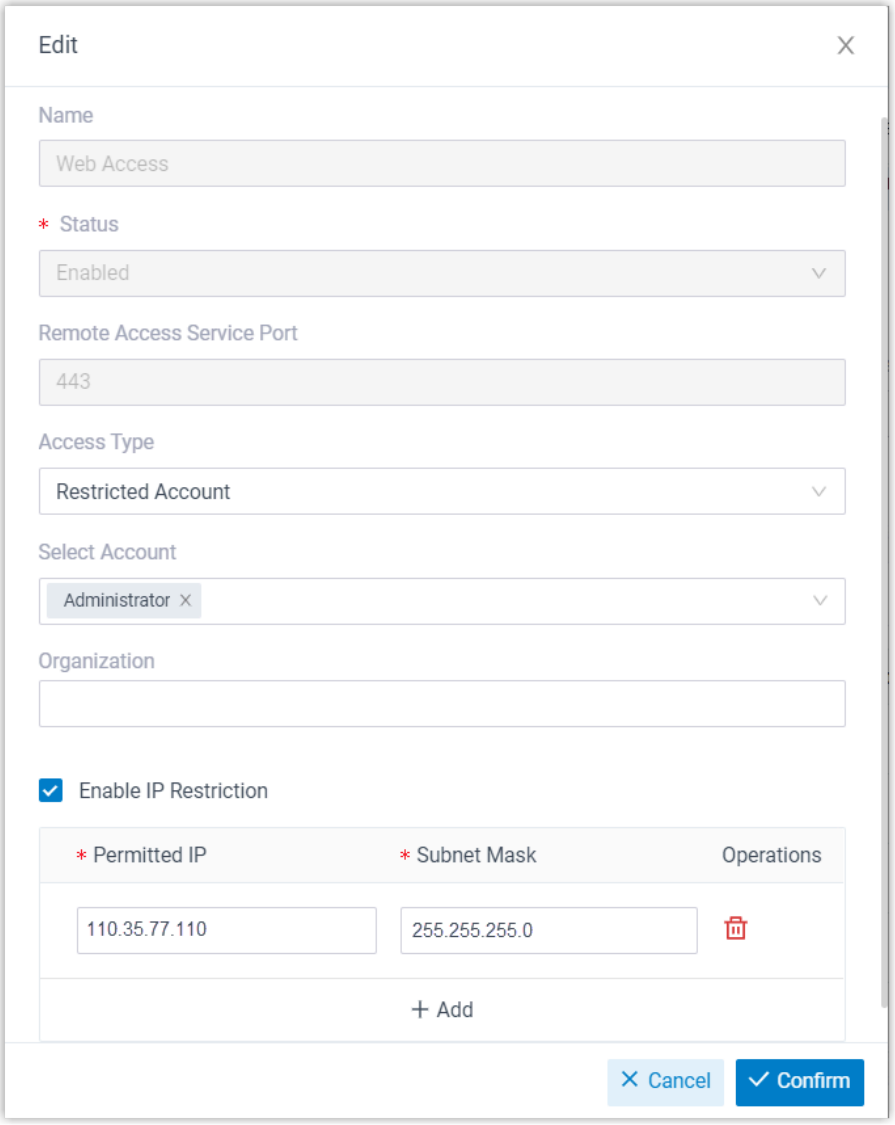
   For example, select domain name **ras.yeastar.com** and enter hostname `yeastardocs`, you will get an FQDN **yeastardocs.ras.yeastar.com**.

4. **Optional:** Configure remote web access usage permission.

   > **Note:**
   > By default, the super administrator account is restricted from using the remote web access feature.

   a. In the **Features** section, go to the **Remote Access** tab.
   b. Click ✎ beside the **Web Access**.
   c. In the pop-up window, complete the following settings according to your need.



- **Name**: Display the remote access feature name, and cannot be edited.
- **Status**: Enabled by default, and cannot be disabled.
- **Remote Access Service Port**: Display the remote web access port 443. The port is assigned by Remote Access Service automatically.
- **Access Type**: Define the account access restriction type.
    - **Allowed Account**: Only the selected accounts can get access to the service.
    - **Restricted Account**: All accounts except for the selected accounts can get access to the service.
- **Select Account**: Select the desired accounts that can or can not use the remote access feature.

- **Organization**: Select the desired organization(s) that can or can not use the remote access feature.

  > **Note:**
  > - This setting is available only when the **Organization Management** feature is enabled.
  > - By default, when you select an organization, its associated sub-organizations are selected. Be careful when selecting organizations.

- **Enable IP Restriction**: Select the checkbox of the option, and add at least one permitted IP address and subnet mask.

  If you configure this option, only the permitted IP address(es) can use the remote access feature.

d. Click **Confirm**.

5. Click **Save**.

Result

Network for remote web access is automatically configured, the authorized accounts can remotely access PBX web portal or Linkus Web Client 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 **Standard Plan**, **Enterprise Plan** or **Ultimate Plan** in 60 days.

Configure Network for Remote Linkus Access by a Yeastar FQDN

With a Yeastar FQDN, users can log in to the Linkus UC Clients anywhere anytime. This topic describes how to configure network for remote Linkus access via FQDN.

Prerequisites

You have subscribed any of the following plans:

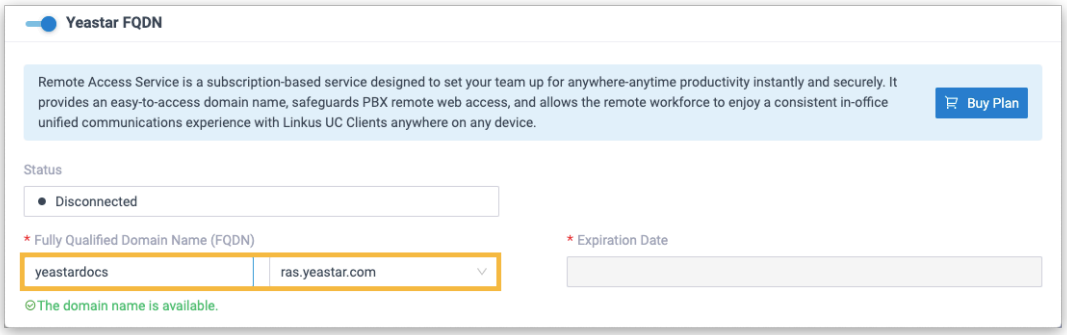
- **Standard Plan**
- **Enterprise Plan**
- **Ultimate Plan**

Procedure

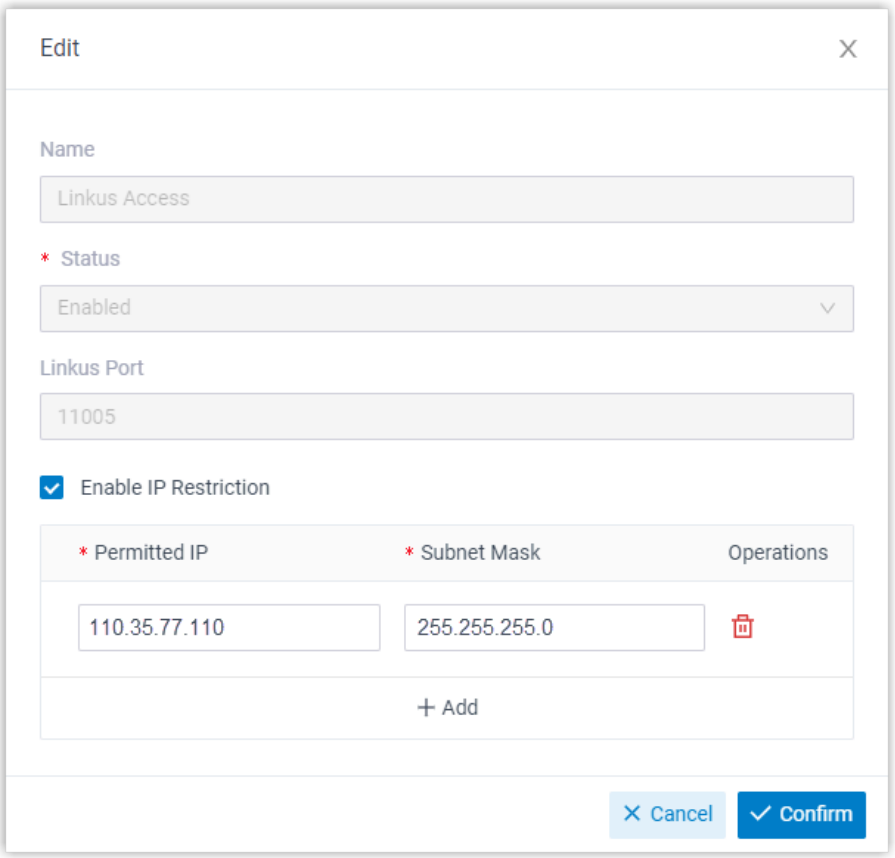
1. Log in to PBX web portal, go to **System > Network > Yeastar FQDN**.
2. Turn on **Yeastar FQDN**.
3. In the **Fully Qualified Domain Name (FQDN)** field, set up the FQDN domain name.
   a. Select a domain name from the drop-down list.
   b. Enter a host name in the first field.

   > **Note:**
   > Think twice before you enter the hostname. The FQDN cannot be changed after you save the configurations.

   For example, select domain name **ras.yeastar.com** and enter hostname `yeastardocs`, you will get an FQDN **yeastardocs.ras.yeastar.com**.



4. **Optional:** Configure remote Linkus access usage permission.
   a. In the **Features** section, go to the **Remote Access** tab.
   b. Click beside the **Linkus Access**.
   c. In the pop-up window, complete the following settings according to your need.



- **Name**: Display the remote access feature name, and cannot be edited.
- **Status**: Enabled by default, and cannot be disabled.
- **Linkus Port**: Display the remote Linkus access port 11005. The port is assigned by Remote Access Service automatically.
- **Enable IP Restriction**: Select the checkbox of the option, and add at least one permitted IP address and subnet mask.

  If you configure this option, only the permitted IP address(es) can use the remote access feature.

d. Click **Confirm**.

5. Click **Save**.

Result

Linkus Server is automatically set up for remote access, users can remotely log in to Linkus UC Clients via the FQDN.

Troubleshooting:

If a user can not access Linkus Web Client via the FQDN, check if you have allowed the user to use the remote web access service via 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 **Standard Plan**, **Enterprise Plan** or **Ultimate Plan** in 60 days.

Configure Network for Remote LDAP Access by a Yeastar FQDN

With a Yeastar FQDN, you can remotely access the LDAP server on PBX via secure LDAP connection without the need of configuring public IP and port forwarding for the PBX. This topic describes how to configure network for remote LDAP access via FQDN.

Prerequisites

You have subscribed any of the following plans:

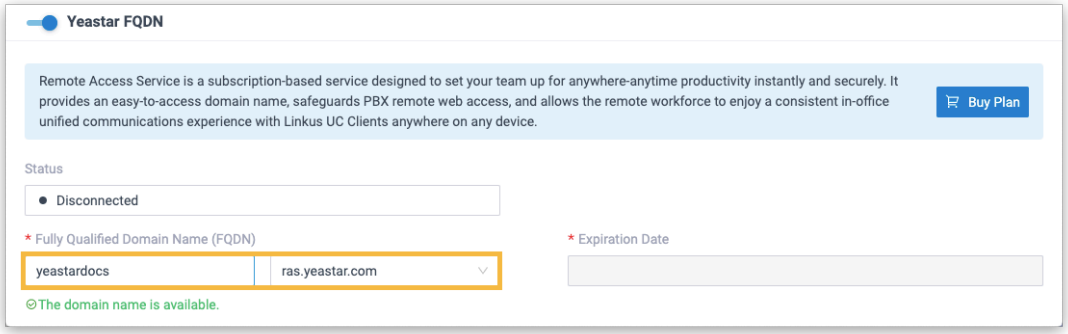
- **Standard Plan**
- **Enterprise Plan**
- **Ultimate Plan**

Procedure

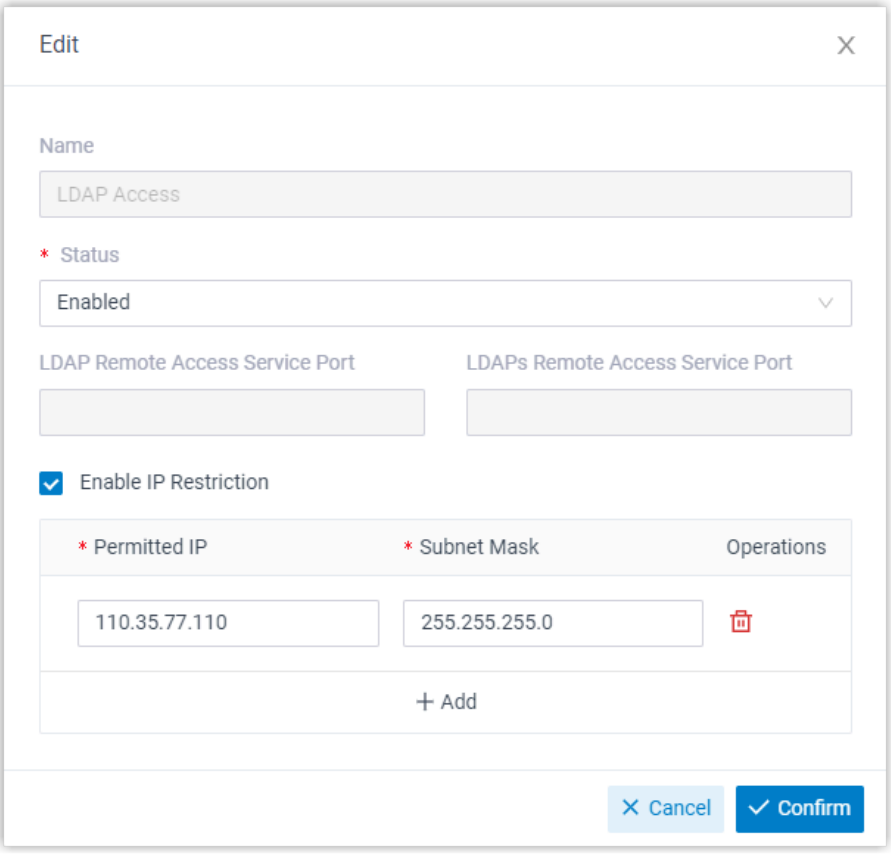
1. Log in to PBX web portal, go to **System > Network > Yeastar FQDN**.
2. Turn on **Yeastar FQDN**.
3. In the **Fully Qualified Domain Name (FQDN)** field, set up the FQDN domain name.
   a. Select a domain name from the drop-down list.
   b. Enter a host name in the first field.

   Note:
   Think twice before you enter the hostname. The FQDN cannot be changed after you save the configurations.

   For example, select domain name **ras.yeastar.com** and enter hostname `yeastardocs`, you will get an FQDN **yeastardocs.ras.yeastar.com**.



4. Enable remote LDAP access feature and configure usage permission.
   a. In the **Features** section, go to the **Remote Access** tab.
   b. Click ✎ beside the **LDAP Access**.
   c. In the pop-up window, complete the following settings according to your need.



- **Name**: Display the remote access feature name, and cannot be edited.
- **Status**: Select **Enabled**.
- **Remote Access Service Port**: The remote access ports will be assigned by Remote Access Service automatically.

- **Enable IP Restriction**: Optional. Select the checkbox of the option, and add at least one permitted IP address and subnet mask.

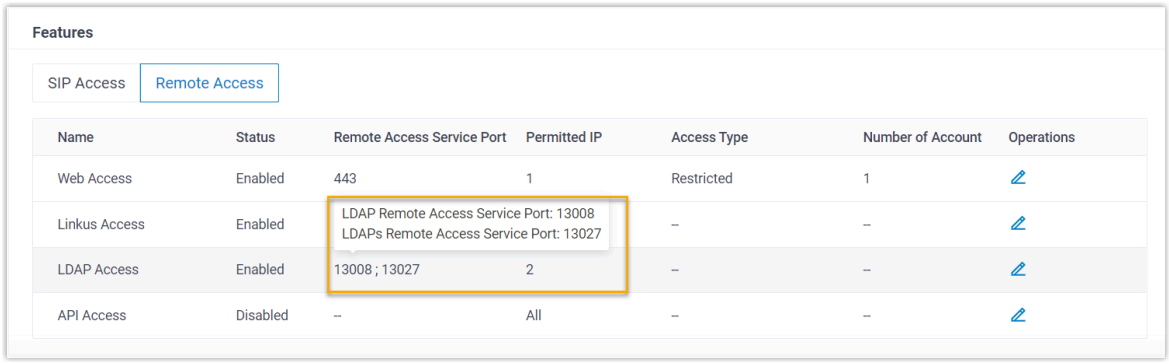
  If you configure this option, only the permitted IP address(es) can use the remote access feature.

d. Click **Confirm**.

5. Click **Save**.

Result

- The Remote Access Service automatically assigns ports for remote LDAP access.



- You can set up the PBX as an LDAP server via the FQDN, allowing an IP phone to remotely and securely query contacts' information within the PBX's directory. For more information of the remote LDAP settings, see Set up Yeastar P-Series PBX System as an LDAP Server.

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 **Standard Plan**, **Enterprise Plan** or **Ultimate Plan** in 60 days.

Configure Network for Remote API Access by a Yeastar FQDN

With a Yeastar FQDN, you can remotely access Yeastar P-Series APIs via a secure tunnel, without the need of configuring public IP and port forwarding for the PBX. This topic describes how to configure network for remote API access via FQDN.

Prerequisites

You have subscribed any of the following plans:

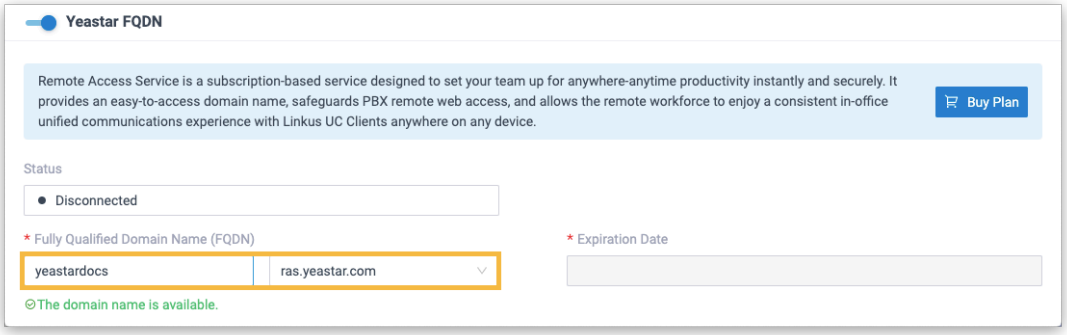
- **Standard Plan**
- **Enterprise Plan**
- **Ultimate Plan**

Procedure

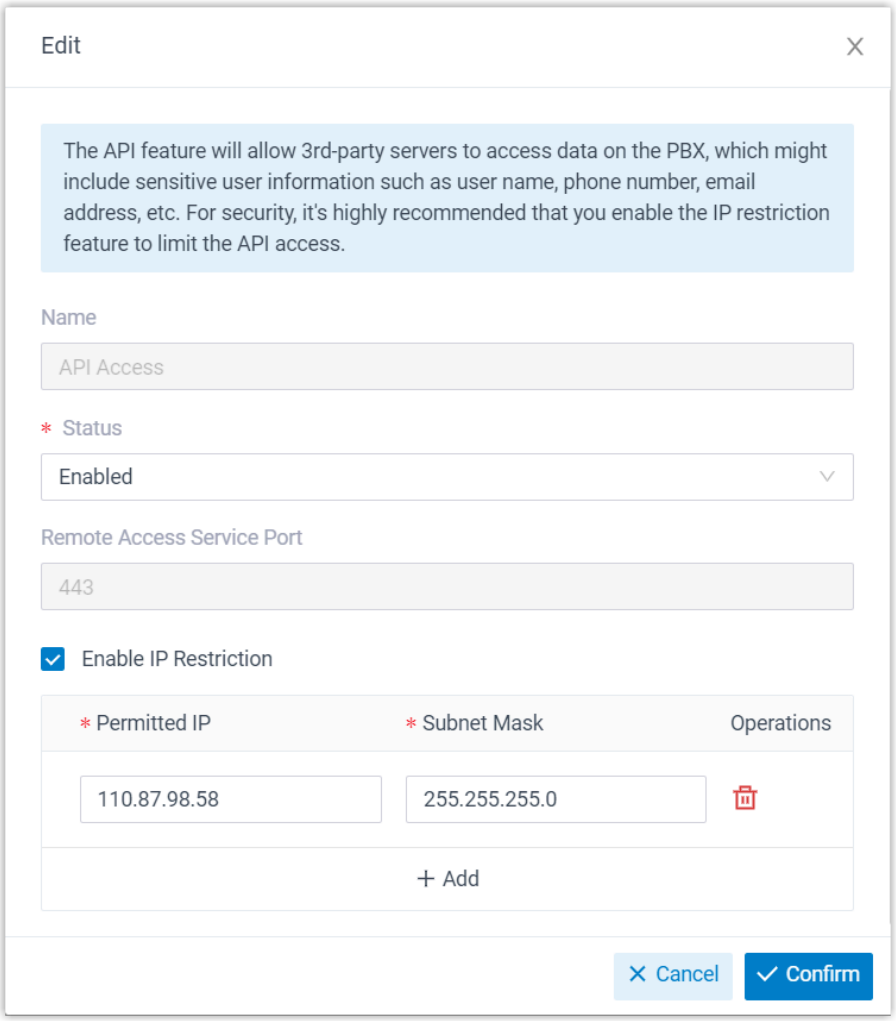
1. Log in to PBX web portal, go to **System > Network > Yeastar FQDN**.
2. Turn on **Yeastar FQDN**.
3. In the **Fully Qualified Domain Name (FQDN)** field, set up the FQDN domain name.
   a. Select a domain name from the drop-down list.
   b. Enter a host name in the first field.

   > **Note:**
   > Think twice before you enter the hostname. The FQDN cannot be changed after you save the configurations.

   For example, select domain name **ras.yeastar.com** and enter hostname `yeastardocs`, you will get an FQDN **yeastardocs.ras.yeastar.com**.

4. Enable remote API access feature and configure usage permission.
   a. In the **Features** section, go to the **Remote Access** tab.
   b. Click beside the **API Access**.
   c. In the pop-up window, complete the following settings according to your need.



- **Name**: Display the remote access feature name, and cannot be edited.
- **Status**: Select **Enabled**.
- **Remote Access Service Port**: Display the remote API access port 443. The port is assigned by Remote Access Service automatically.
- **Enable IP Restriction**: Optional. Select the checkbox of the option, and add at least one permitted IP address and subnet mask.

  If you configure this option, only the permitted IP address(es) can use the remote access feature.

d. Click **Confirm**.

5. Click **Save**.

Result

You can now remotely access P-Series APIs 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 **Standard Plan**, **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 three 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
- Yeastar Domain Name

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 Public IP Address.

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 Domain Name.

Yeastar Domain Name

If you want to implement direct remote communication between the PBX server and the clients via a domain name but prefer a simplified domain setup, Yeastar offers a domain service that makes the process hassle-free. You only need to configure a Yeastar domain name, without having to configure DNS resolution and request certificates, the PBX can automatically complete the rest of the process and renew the domain certificates.

For more information about the configurations, see Configure Network for Remote Access by a Yeastar Domain Name.

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.

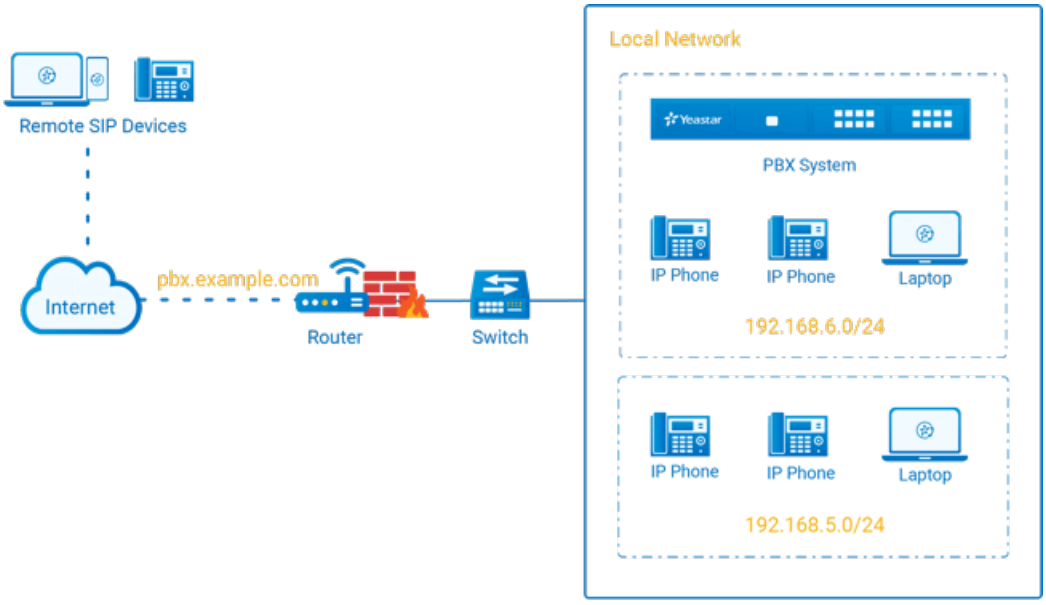
Configure Network for Remote Access by a Domain Name

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.

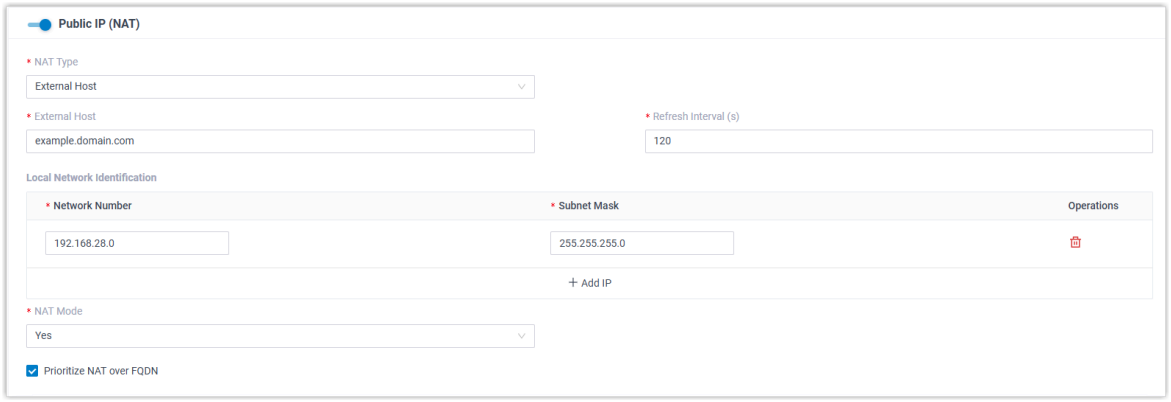
  In this scenario, forward the following ports:

Service	Internal Port	External Port
SIP registration	UDP 5060 (default)	UDP 8092
RTP	UDP 10000-12000 (default)	UDP 10000-12000
Web server	TCP 8088 (default)	TCP 9099
Linkus server	TCP&UDP 8111 (default)	TCP&UDP 6090

Procedure

Based on the scenario, configure the Public IP and Ports on PBX as follows.

1. Log in to PBX web 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.

  > **Note:**
  > If a security notice pop-up appears, you can set up allowed country/region IP access protection to better secure remote access.

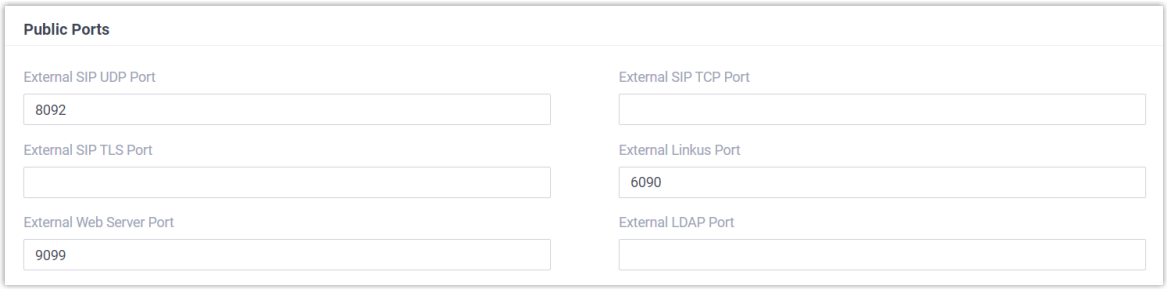
- **NAT Type**: Select **External Host**.
- **External Host**: Enter *example.domain.com*.
- **Refresh Interval (s)**: Leave the default setting or change the interval (in seconds) for PBX to request the external host for public IP.
- **Local Network Identification**: Add all your local network. This 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 the local network `192.168.28.0/255.255.255.0`.
- **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.
- **Prioritize NAT over FQDN**: Optional. Specify whether NAT should take precedence over FQDN when both network settings are enabled.

  If this option is enabled, the system will use the NAT address instead of the FQDN when generating remote access URLs, such as Linkus login link, Live Chat embed code, etc.

3. In the **Public Ports** section, enter the external ports that you have forwarded on your router.

> **Note:**
> At least one of the following fields must be filled: **External SIP UDP Port**, **External SIP TCP Port**, or **External SIP TLS Port**.



- **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*.
- **External LDAP Port**: Leave it blank because LDAP protocol is not used in this scenario.

4. Click **Save**.

Result

- Users can remotely access the PBX web 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.

What to do next

To ensure secure communication and protect data integrity, either apply for an HTTPS certificate for the domain through the PBX directly or upload the certificate you have prepared.

Related information

Configure Network for Remote Web Access by a Yeastar FQDN
Configure Network for Remote Access by a Public IP Address
Set up a Remote SIP Phone via Public IP Address and Port

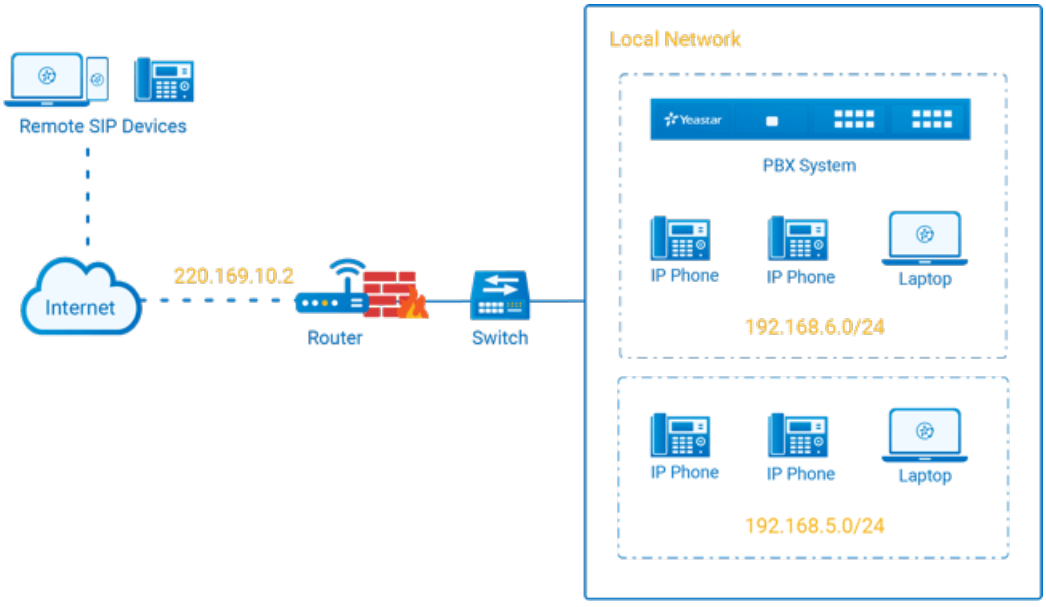
Configure Network for Remote Access by a Public IP Address

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.

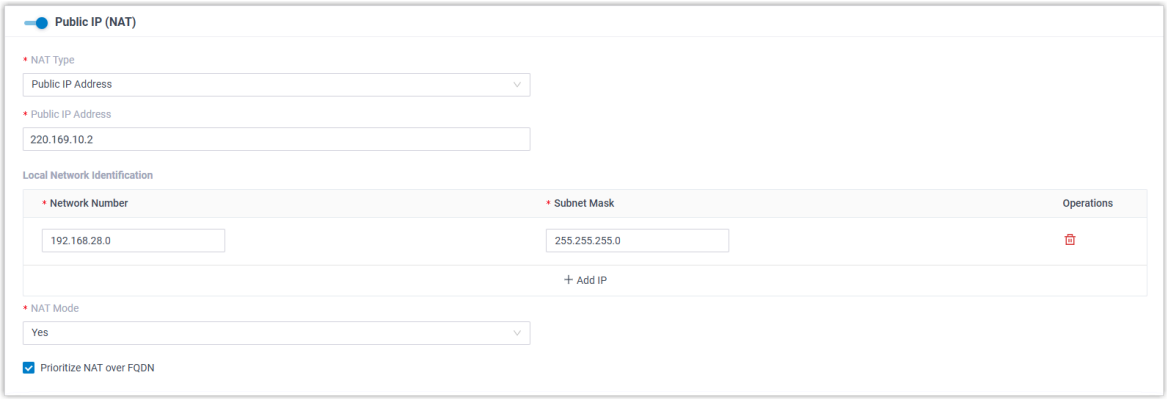
  In this scenario, forward the following ports:

Service	Internal Port	External Port
SIP registration	UDP 5060 (default)	UDP 8092
RTP	UDP 10000-12000 (default)	UDP 10000-12000
Web server	TCP 8088 (default)	TCP 9099
Linkus server	TCP&UDP 8111 (default)	TCP&UDP 6090

Procedure

Based on the scenario, configure the Public IP and Ports on PBX as follows.

1. Log in to PBX web 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.

     > **Note:**
     > If a security notice pop-up appears, you can set up allowed country/region IP access protection to better secure remote access.

   - **NAT Type**: Select **Public IP Address** .
   - **Public IP Address**: Enter *220.169.10.2*.

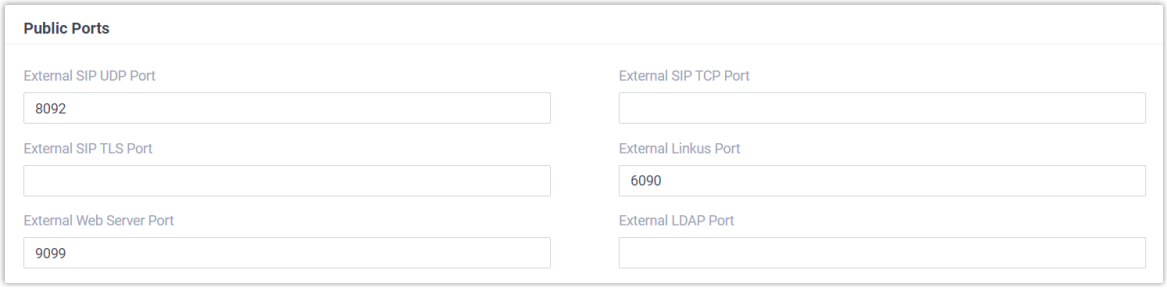
- **Local Network Identification**: Add all your local network. This setting will allow all your local devices to communicate with the PBX by the local IP address instead of passing through the router.

  In this scenario, add the local network `192.168.28.0/255.255.255.0`.
- **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.
- **Prioritize NAT over FQDN**: Optional. Specify whether NAT should take precedence over FQDN when both network settings are enabled.

  If this option is enabled, the system will use the NAT address instead of the FQDN when generating remote access URLs, such as Linkus login link, Live Chat embed code, etc.

3. In the **Public Ports** section, enter the external ports that you have forwarded on your router.

> **Note:**
> At least one of the following fields must be filled: **External SIP UDP Port**, **External SIP TCP Port**, or **External SIP TLS Port**.



- **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*.

- **External LDAP Port**: Leave it blank because LDAP protocol is not used in this scenario.

4. Click **Save**.

Result

- Users can remotely access the PBX web 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 Web Access by a Yeastar FQDN
Set up a Remote SIP Phone via Public IP Address and Port

Configure Network for Remote Access by a Yeastar 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 to describe how to easily implement remote connection by setting up a Yeastar-provided domain name.

Prerequisites

- The firmware version of Yeastar P-Series PBX System is 37.18.0.102 or later.
- You have subscribed to **Enterprise Plan** or **Ultimate Plan**.
- If SIP ALG option is provided in your router, disable it.
- You have configured the following settings on the router:
  - Configure a NAT rule to map the PBX server 's private IP address to a public IP address (static or dynamic) supplied by the Internet Service Provider (ISP).

- Set up port forwarding rules to forwarded the following ports to allow remote access of Linkus clients and other SIP devices.

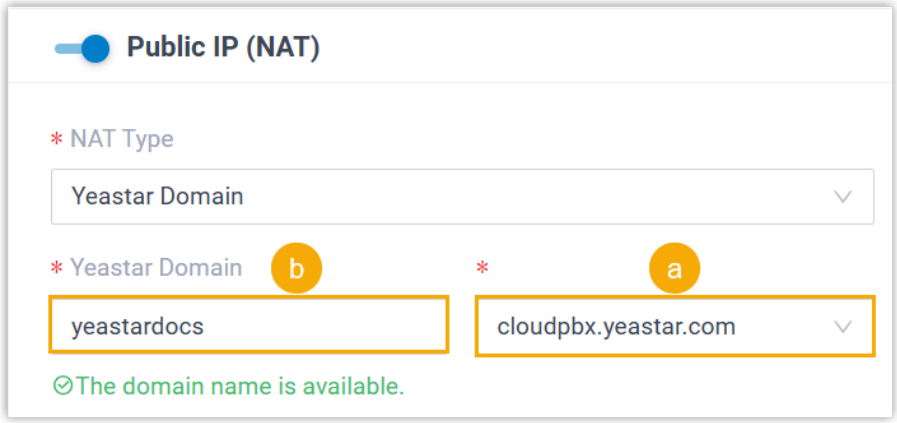
> **Note:**
> To check the relevant internal ports of your PBX, see Manage Service Ports of the PBX.

In this scenario, forward the following ports:

Service	Internal Port	External Port
SIP registration	UDP 5060 (default)	UDP 8092
RTP	UDP 10000-12000 (default)	UDP 10000-12000
Web server	TCP 8088 (default)	TCP 9099
Linkus server	TCP&UDP 8111 (default)	TCP&UDP 6090

Procedure

1. Log in to PBX web portal, go to **System > Network > Public IP and Ports**.
2. Turn on **Public IP (NAT)**.
3. In the **NAT Type** drop-down list, select **Yeastar Domain**.
4. In the **Yeastar Domain** section, set up the Yeastar domain name.



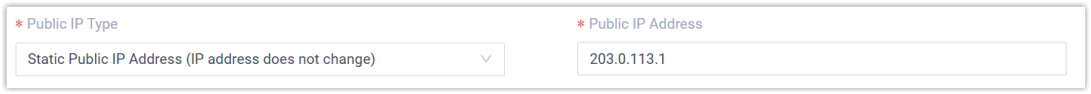
a. Select a domain suffix from the drop-down list.
b. Specify the subdomain in the first field.

> **Note:**

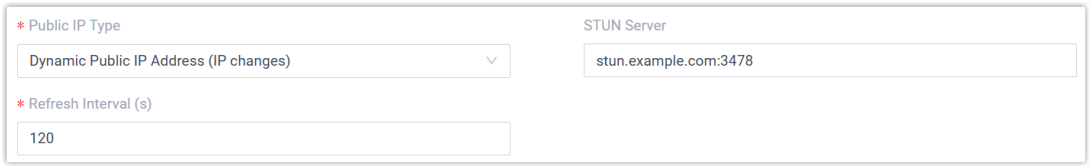
> Think twice before you enter the subdomain, as the Yeastar domain name cannot be changed after you save the configurations.

In this example, you will get a domain name `yeastardocs.cloudpbx.yeastar-.com`.

5. In the **Public IP Type** drop-down list, select the type of public IP address you use, and complete the related settings.
   - To use a static public IP address, do as follows:



     a. Select **Static Public IP Address (IP address does not change)**.
     b. In the **Public IP Address** field, enter your public IP address.
   - To use a dynamic public IP address, do as follows:



     a. Select **Dynamic Public IP Address (IP changes)**.
     b. **Optional:** In the **STUN Server** field, enter the address of your STUN server.

> **Note:**
> If left empty, Yeastar's STUN server will be used by default.

     c. In the **Refresh Interval (s)** field, specify the time interval for the PBX to request the STUN server for public IP.

        The default value is 120, and the available value should be an integer between 30 and 3600.
6. **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.

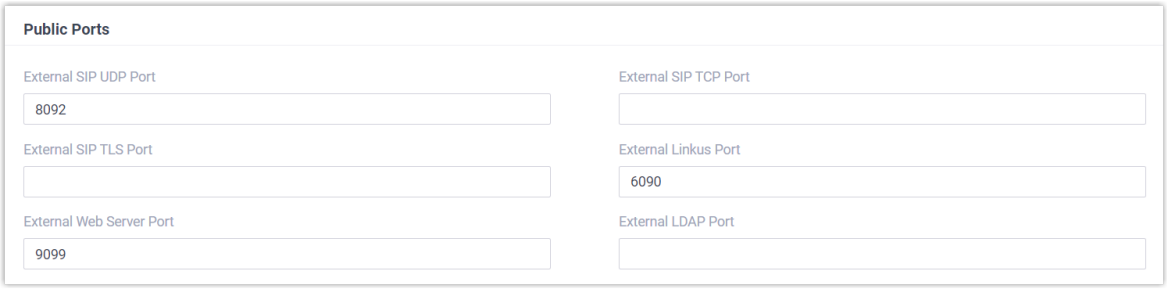
   In this scenario, add the local network `192.168.28.0/255.255.255.0`.
7. **NAT Mode**: Select a SIP NAT mode. In this scenario, select **Yes**.
   - **Yes**: Use NAT and ignore the address information in the SIP/SDP headers and reply to the sender's IP address and port.
   - **No**: Use NAT mode only according to RFC3581.

- **Never**: Never attempt NAT mode or RFC3581 support.
- **Route**: Use NAT but do not include Rport in headers.

8. **Prioritize NAT over FQDN**: Optional. Specify whether NAT should take precedence over FQDN when both network settings are enabled.

   If this option is enabled, the system will use the NAT address instead of the FQDN when generating remote access URLs, such as Linkus login link, Live Chat embed code, etc.
9. In the **Public Ports** section, enter the external ports that you have forwarded on your router.

   > **Note:**
   > At least one of the following fields must be filled: **External SIP UDP Port**, **External SIP TCP Port**, or **External SIP TLS Port**.

   - **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*.
   - **External LDAP Port**: Leave it blank because LDAP protocol is not used in this scenario.
10. Click **Save**.

Result

- Once the configuration is completed, the PBX will automatically apply for a certificate for the Yeastar domain name. The certificate can be check on **Security > Security Settings > Certificates**, and will be automatically renewed before it expires.

- The followings remote access features can be implemented:
  - Users can remotely access the PBX web portal and log in to Linkus clients via the Yeastar domain name.
  - Remote devices based on SIP protocol can register to the PBX via the domain name.
  - The login links and QR codes for Linkus remote access are generated 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.

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

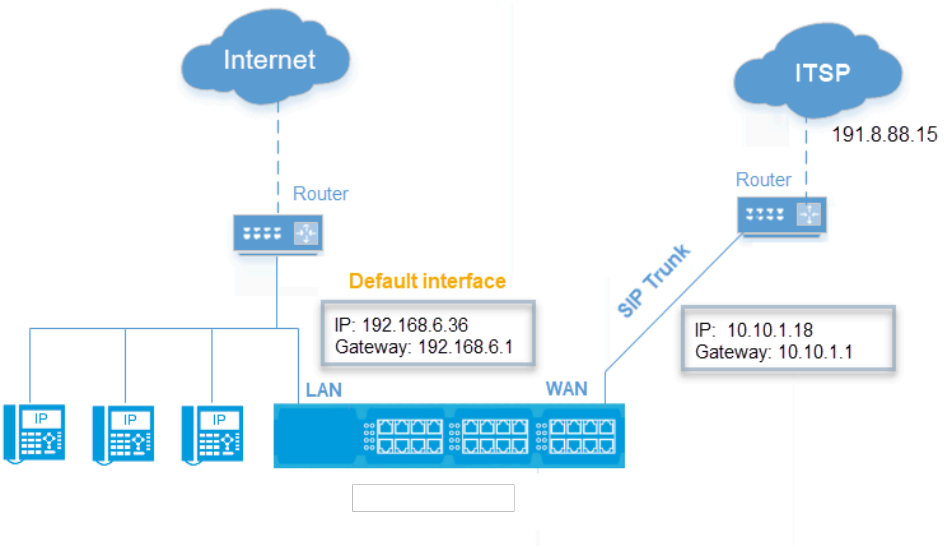
Adding custom static route is typically used in the "Dedicated SIP trunking" scenario.

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

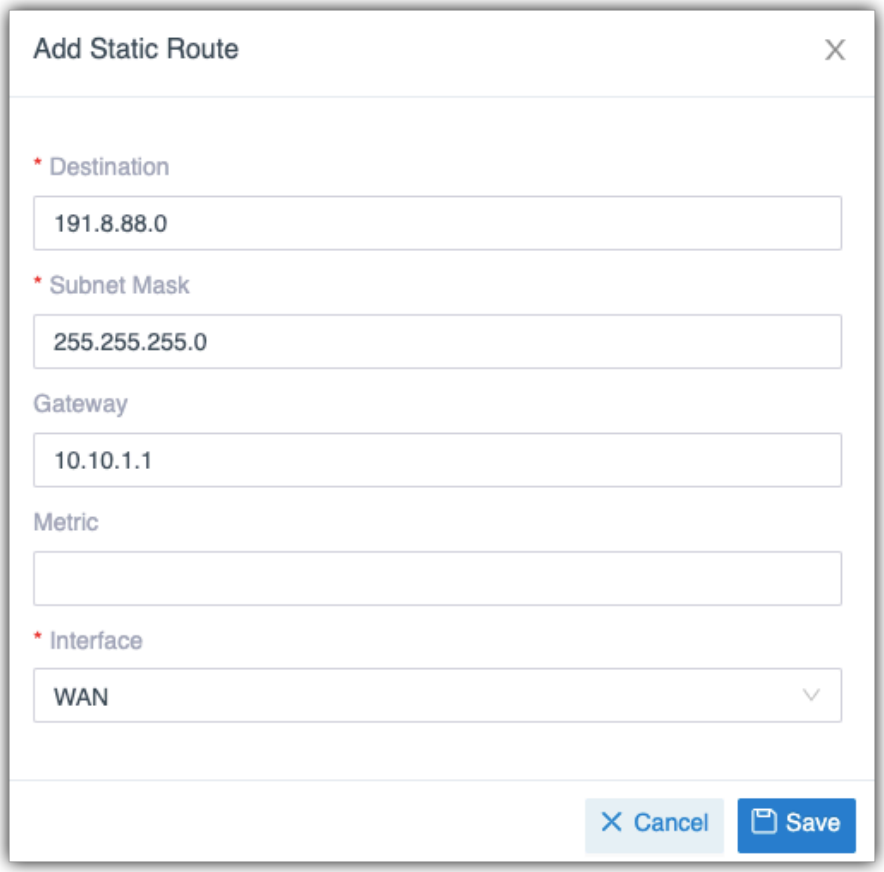
Setting	Value
Ethernet Mode	Dual
Default Interface	LAN
LAN	
IP Address	192.168.6.36
Subnet Mask	255.255.255.0
Gateway	192.168.6.1
Preferred DNS Server	192.168.1.1
WAN	
IP Address	10.10.1.18
Subnet Mask	255.255.255.0
Gateway	10.10.1.1
Preferred DNS Server	10.10.1.1

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 web portal, go to **System > Network > Static Routes**, click **Add**.

2. On the pop-up window, configure the route entry:



- **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**.

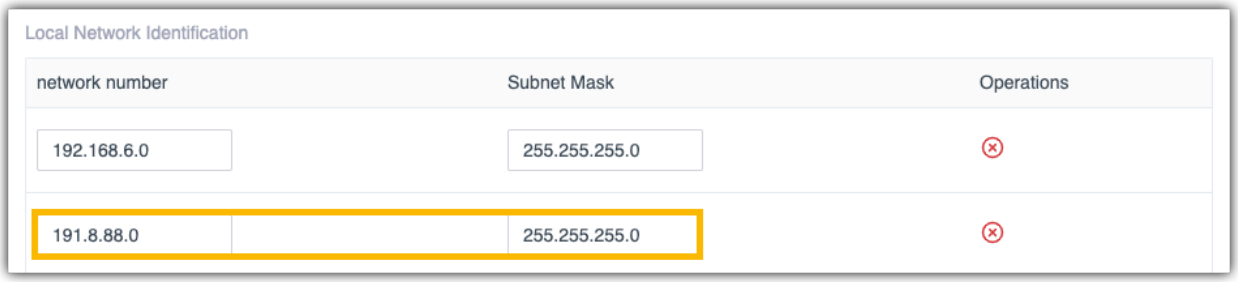
Result

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.



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 web 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 web 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

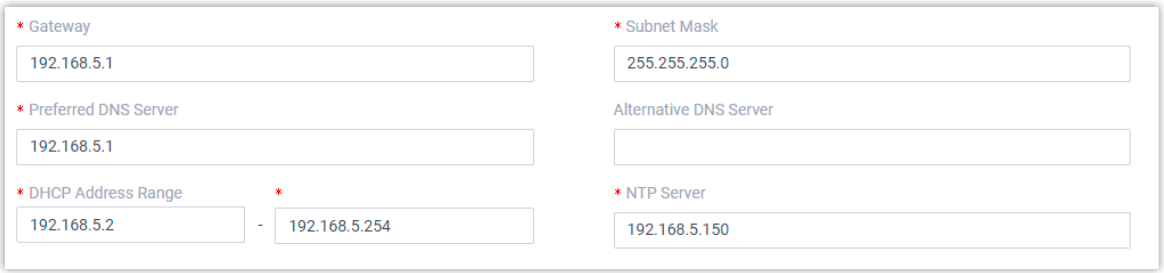
Yeastar P-Series PBX System provides a built-in DHCP server. When there is no DHCP server in the local network, you can set up the PBX as a DHCP server to assign IP addresses, gateway, DNS and other network parameters to devices in the same local network.

Prerequisites

Make sure there is only one DHCP server running in the local network.

Procedure

1. Log in to PBX web 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**: 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.

  > **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.

Split DNS

Set up Split DNS

Split DNS allows extension users to seamlessly access and use their Linkus clients via the same domain name, whether they are inside the office or working remotely, which improves access speed and reliability. This topic describes how to set up split DNS in a typical company network.

Introduction

Split DNS allows the same domain name to be resolved to different IP addressed based on the user's network location:

- For external users, the domain resolves to the public IP address of the PBX system (e.g. `203.0.113.10`).

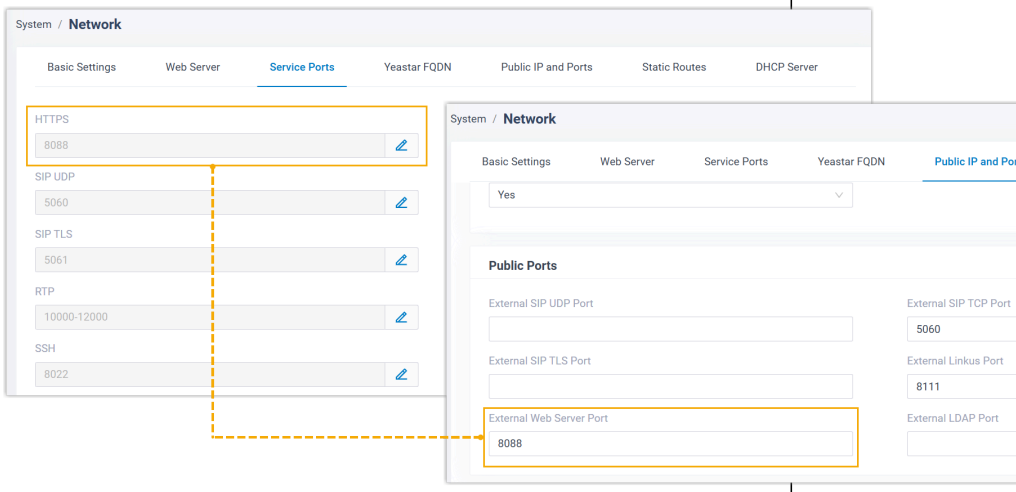
  This resolution is typically handled by public DNS servers, which rely on DNS records (such as A records) configured when the domain name is registered or managed with your domain registrar.
- For internal users, the domain resolves to the private IP address of the PBX system (e.g. `192.168.28.39`).

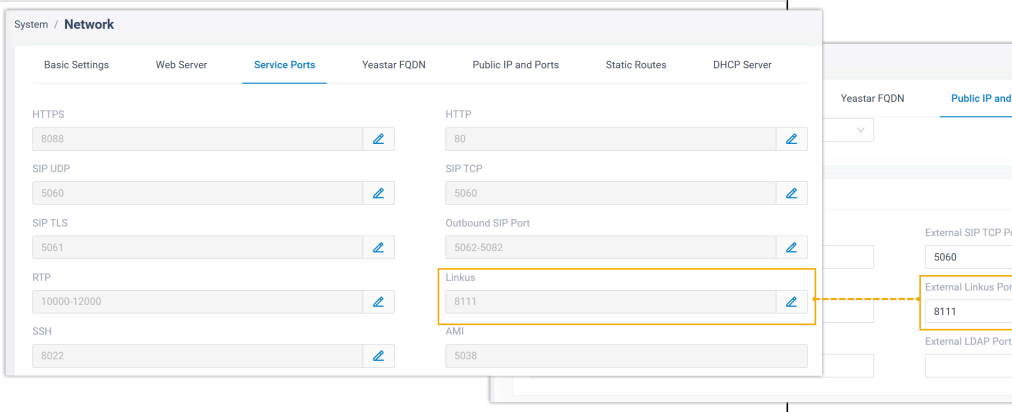
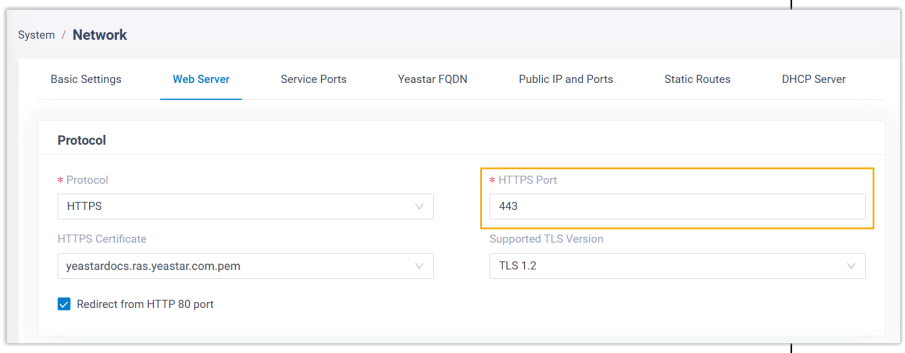
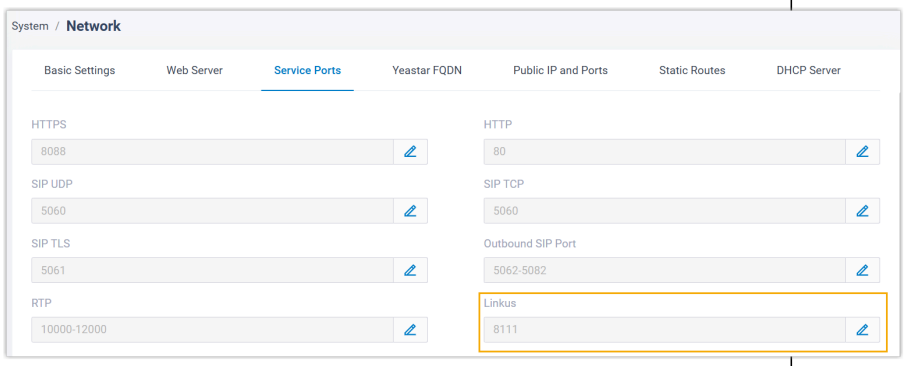
  This depends on your company's network configuration. It is recommended to implement this functionality on a firewall or router, if supported by the vendor. Alternatively, you can configure an internal DNS server to manage internal domain resolution. This

guide uses Microsoft DNS server as an example to demonstrate how to configure internal DNS resolution.

Prerequisites

To implement split DNS, make sure the followings are in place:

Item	Description
Domain	• You have a valid domain name (custom or Yeastar-provided) which will be used for both internal and external access. • The PBX has been configured for remote access via the domain name. For more information about the configurations, see the following topics: ◦ Configure Network for Remote Web Access by a Yeastar FQDN ◦ Configure Network for Remote Access by a Domain Name ◦ Configure Network for Remote Access by a Yeastar Domain Name
Port	Configure the ports for PBX server based on the domain type. • **For domains requiring NAT traversal (e.g. External Host & Yeastar Domain)** ◦ The external web server port should be mapped to the same port as the HTTPS port.  ◦ Ensure the external Linkus port is the same as the internal Linkus port.

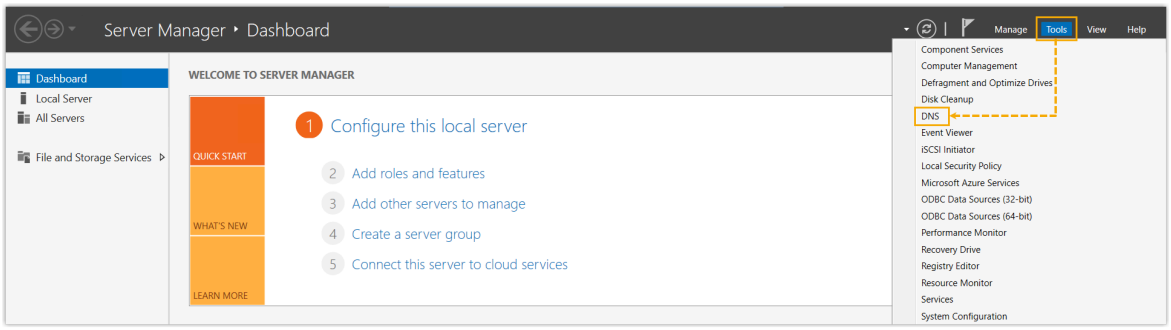
Item	Description
	 • **For Yeastar FQDN** ◦ The HTTPS port should be set to **443** for optimal performance (Path: **System > Network > Web Server > Protocol > HTTPS Port**).  ◦ Ensure the internal Linkus port is fixed at **8111** (Path: **System > Network > Service Ports > Linkus**). 
Internal DNS Server	A Microsoft DNS Server has been deployed within the company's internal network to handle internal domain resolution.

Procedures

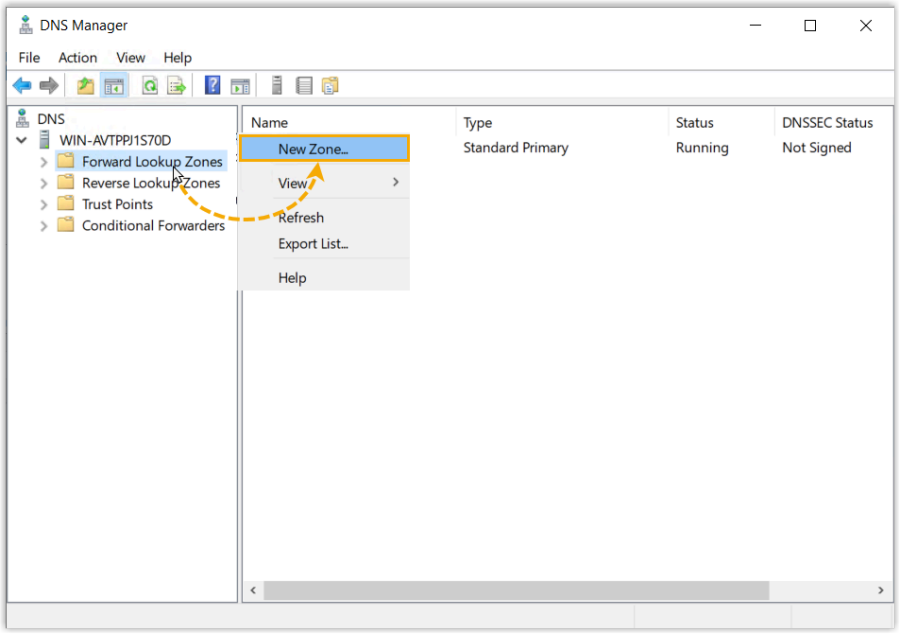
1. Create an internal DNS record
2. Verify internal DNS resolution
3. Enforce internal DNS usage for user devices

Create an internal DNS record

1. At the top-right of the Server Manager window on Windows Server, go to **Tools > DNS** to open the DNS manager.

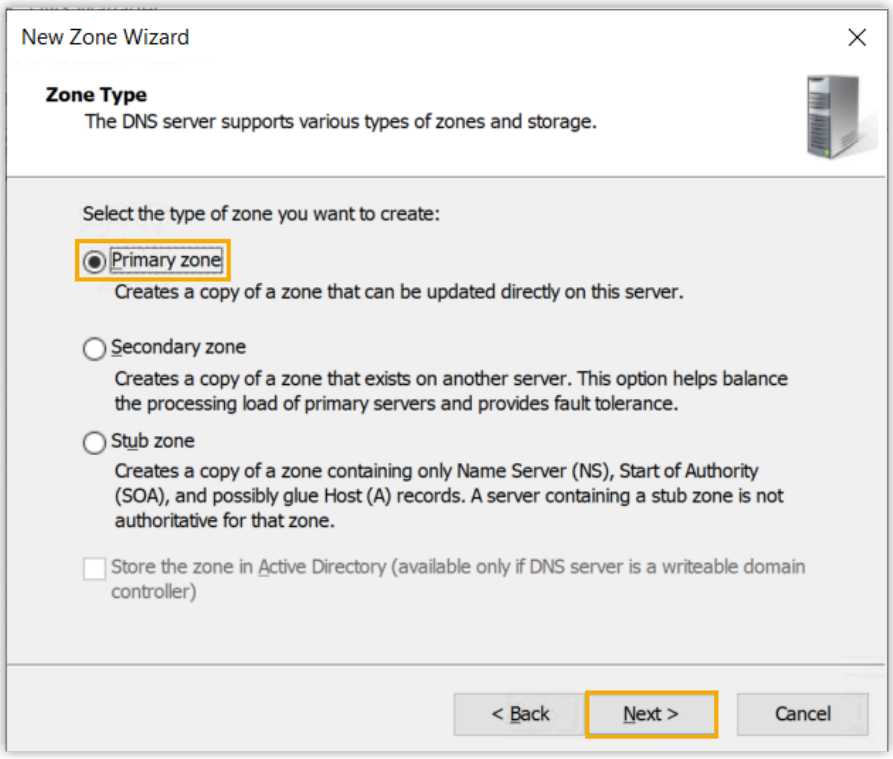


2. Add a Forward Lookup Zone.
   a. Right click **Forward Lookup Zones**, then select **New Zone...**.

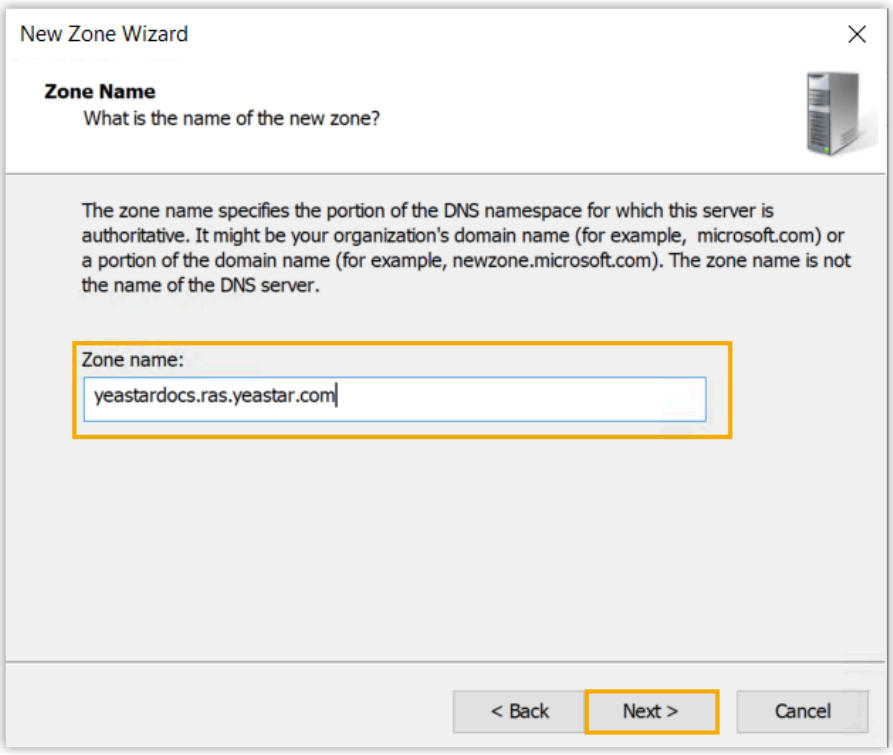


   The New Zone Wizard will open.
   b. On the wizard, click **Next** to continue.

c. In the **Zone Type** page, leave the default option **Primary zone** selected, then click **Next**.



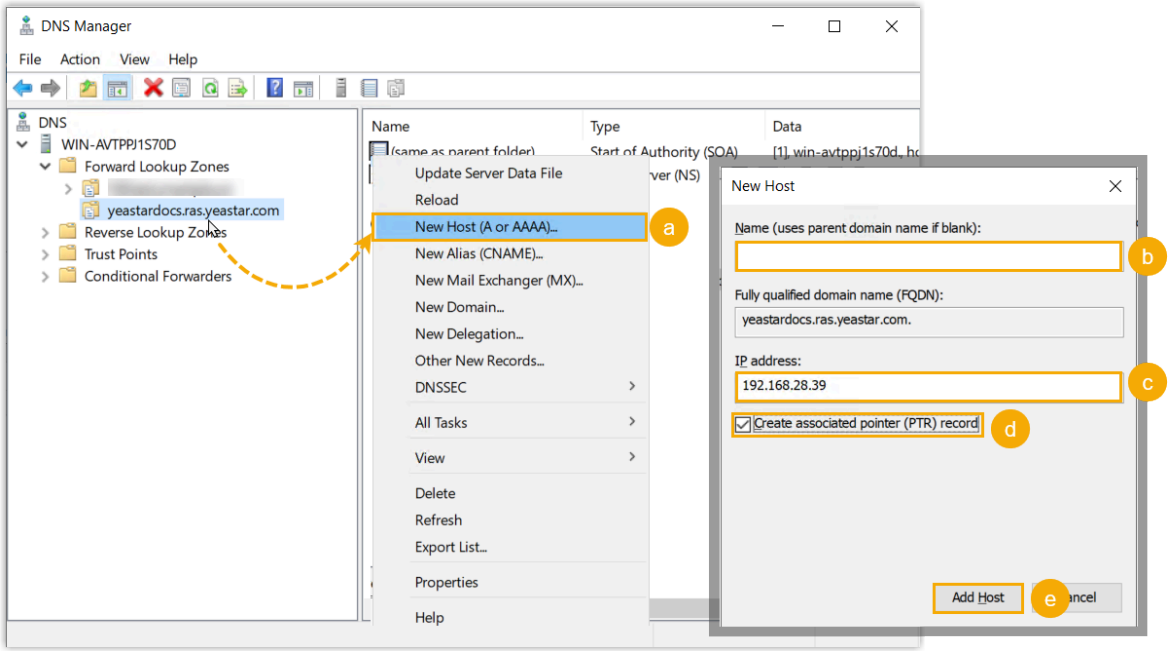
d. In the **Zone Name** page, enter the domain name of the PBX, then click **Next**.



e. On the remaining pages, keep the default settings and click **Next** until you reach the final step.

f. Click **Finish** to complete the setup.

3. Add a new host.

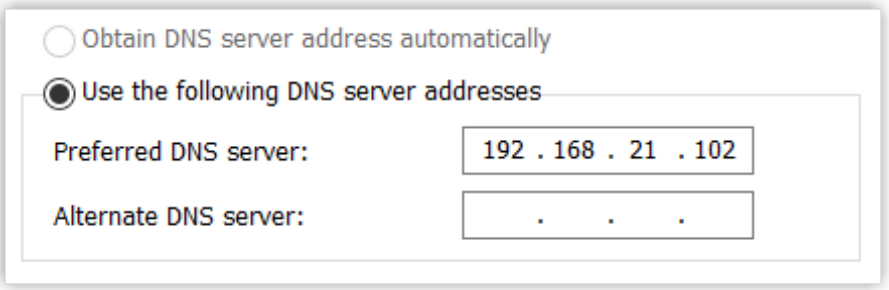


a. Right click on the domain name you added, then select **New Host (A or AAAA)...**.
b. Leave the **Name** field empty, which means the parent domain will be used.
c. In the **IP address** field, enter the private IP address of the PBX system.
d. **Optional:** To enable reverse DNS lookup, select the checkbox of **Create associated PTR record**.
e. Click **Add Host**.

A dialog box pops up to indicate that the host record is successfully created, click **OK** to close.

Verify internal DNS resolution

1. Configure your computer to use the internal DNS server.
   a. On your computer, press **Win+R** to open the **Run** dialog box.
   b. Type `ncpa.cpl`, then press **Enter**.
   c. In the **Network Connections** window, right click your active network connection, then go to **Properties**.
   d. Double click the **Internal Protocol Version 4 (TCP/IPv4)**.
   e. Select **Use the following DNS server addresses**, then enter the IP address of the internal DNS server (E.g. `192.168.21.102`).



   f. Click **OK** to save the settings, then click **OK** again to close the window.
2. Test internal DNS resolution on your computer.

> **Tip:**
> For external DNS resolution, you can verify using an online DNS checker to see if the domain name is correctly resolved to the PBX's public IP address.

   a. On your computer, press **Win+R** to open the **Run** dialog box.
   b. Type `cmd`, then press **Enter**.

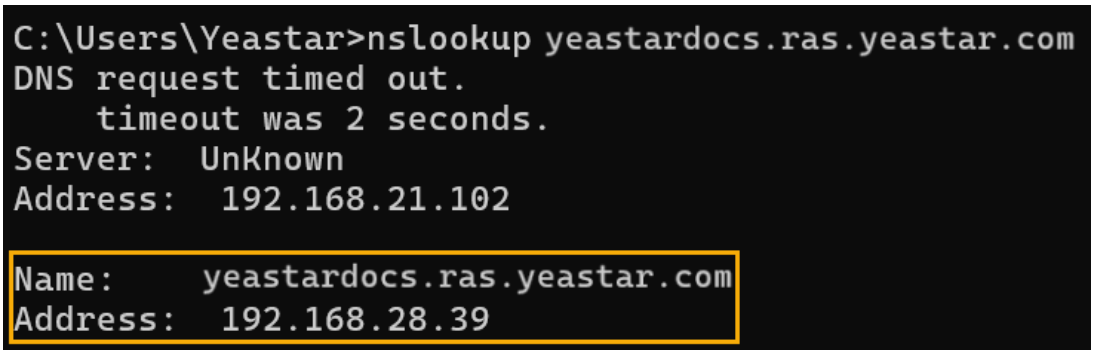
c. In the **Command Prompt** window, enter the following command and press **Enter**.

```
nslookup {your PBX's domain name}
```

For example,

```
nslookup yeastardocs.ras.yeastar.com
```

The output returns the private IP address of the PBX, indicating that the internal DNS resolution is configured successfully.



Enforce internal DNS usage for user devices

To ensure Split DNS works properly, user devices must use the internal DNS server when connected to the company network.

1. Configure DHCP server to assign internal DNS.

   Set the DHCP scope options to assign the IP address of the internal DNS server as the primary DNS for all devices connected to the corporate network.
2. **Optional:** Block external DNS requests on firewall.

   On the company's firewall, block outbound DNS requests (UDP/TCP port 53) to public DNS servers to prevent clients from bypassing the internal DNS.
3. Connect user devices to the company network.

Client Type	Connection Method
Linkus Web / Desktop Client	• Connect user's computer to the company's Wi-Fi to automatically obtain the internal DNS server via DHCP. **Note:** This method is recommended to avoid manual switching DNS settings when moving between different networks.

Client Type	Connection Method
	• If user's computer uses a static IP configuration, manually specify the internal DNS server address in the network settings.
Linkus Mobile Client	Connect to company's Wi-Fi to obtain internal DNS via DHCP.

Result

Extension users can access their Linkus clients using the same domain name from both internal and external networks, eliminating the need to manually switch between different addresses and ensuring a consistent login experience.

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 web 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 web 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 Yeastar 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 web 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.

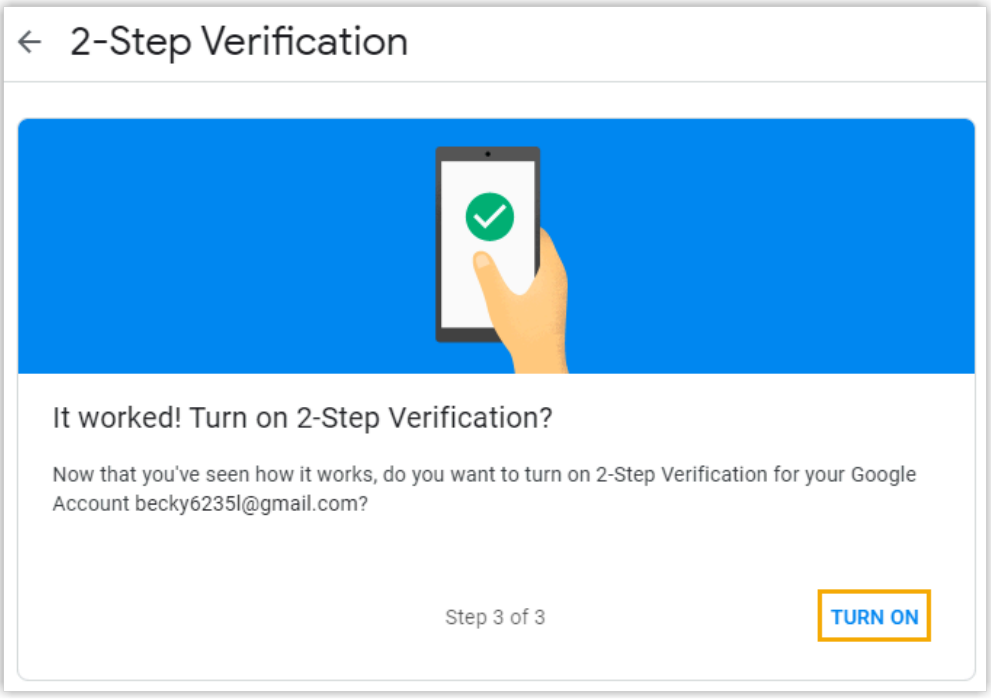
Prerequisites

Make sure Yeastar P-Series PBX System can access Google Server.

Step1. Create an app password on Google Account

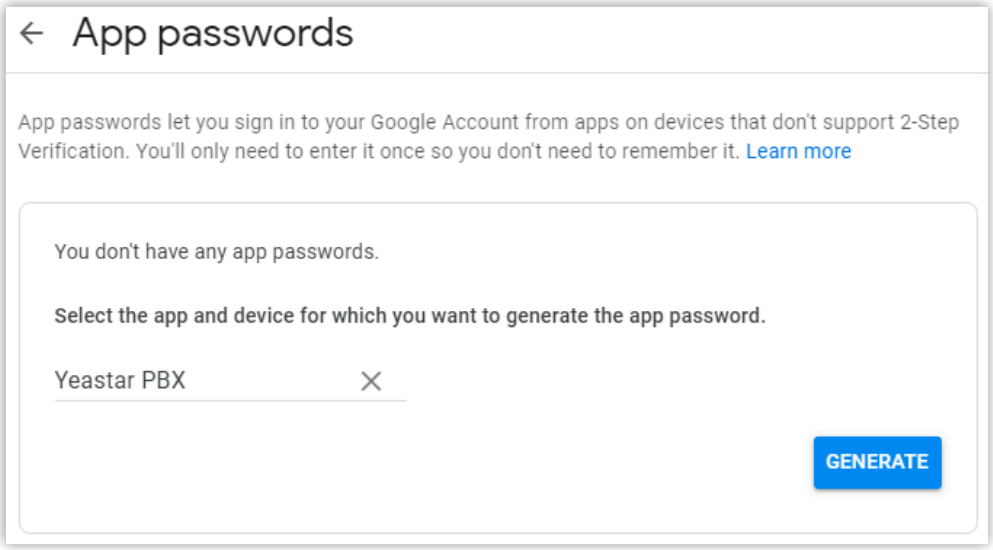
To ensure that the PBX can access Gmail server, you need to turn on 2-Step verification and create an app password as follows.

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.

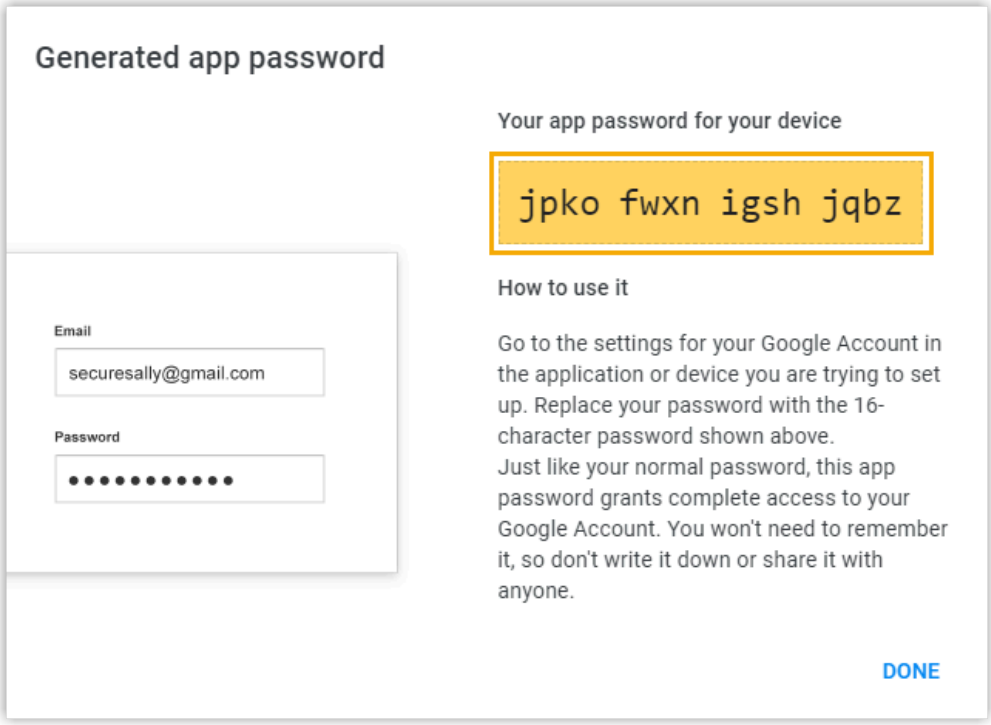


4. Right above the page, click ← to back to the security page.
5. Create an app password.
    a. In the **Signing in to Google** section, click **App passwords** and enter your Gmail password to verify your account.
    b. In the **Select app** drop-down list, select **Other (Custom name)**.

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 web portal, go to **System > Email > Email Server**.
2. In the **Type of Email Server** drop-down list, select **Custom Email Server**.
3. In the **Select Email Server Provider** drop-down list, select **General**.
4. 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.
5. 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**.
6. 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 Microsoft Outlook as the email server for Yeastar P-Series PBX System using modern authentication. This allows the PBX to send and receive emails through your Microsoft account.

Requirements

Platform	Requirement
PBX server	• **Firmware**: Version 37.18.0.102 or later • **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP) • The PBX can be remotely accessed. For more information about the configuration, see the following topics: ◦ Configure Network for Remote Access by a Yeastar FQDN ◦ Configure Network for Remote Access by a Yeastar Domain Name ◦ Configure Network for Remote Access by a Domain Name ◦ Configure Network for Remote Access by a Public IP Address
Microsoft 365	• A Microsoft account that meets the following requirements: **Note:** The account will be used as the designated email sender for the SMTP server. ◦ Assigned with the **Global Administrator** role. ◦ Assigned with **Microsoft 365 Business Standard** license. • The modern authentication is enabled in Microsoft 365 admin center.

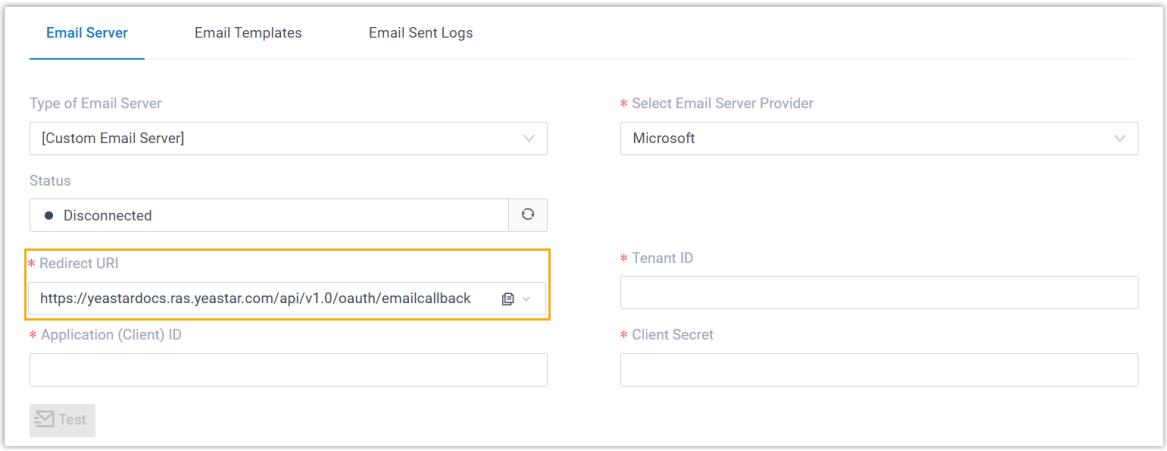
Procedure

- Step 1. Obtain redirect URI from PBX
- Step 2. Register an application on Microsoft Entra ID
- Step 3. Configure SMTP settings on PBX

Step 1. Obtain redirect URI from PBX

Obtain the redirect URI from Yeastar P-Series PBX System, which will be required when registering a Microsoft Entra application later.

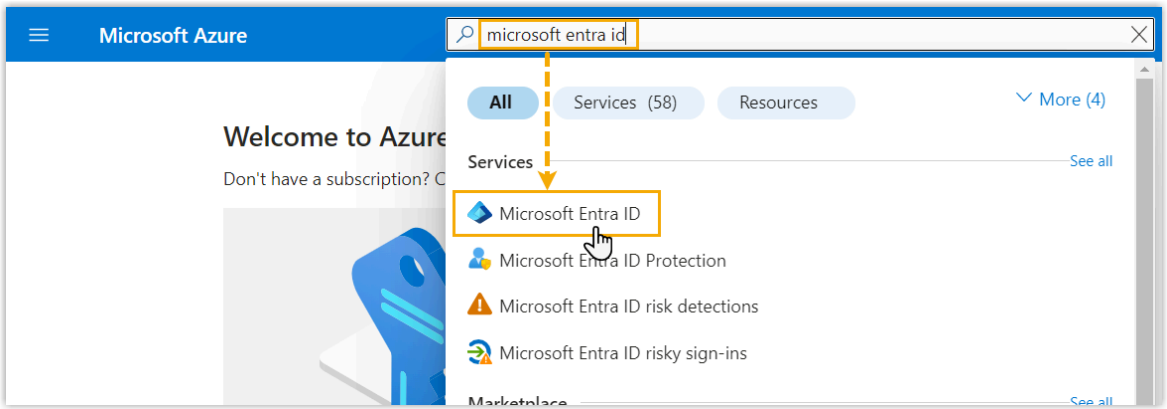
1. Log in to PBX web portal, go to **System > Email > Email Server**.
2. In the **Type of Email Server** drop-down list, select **Custom Email Server**.
3. In the **Select Email Server Provider** drop-down list, select **Microsoft**.
4. In the **Redirect URI** field, select and copy the desired redirect URI.



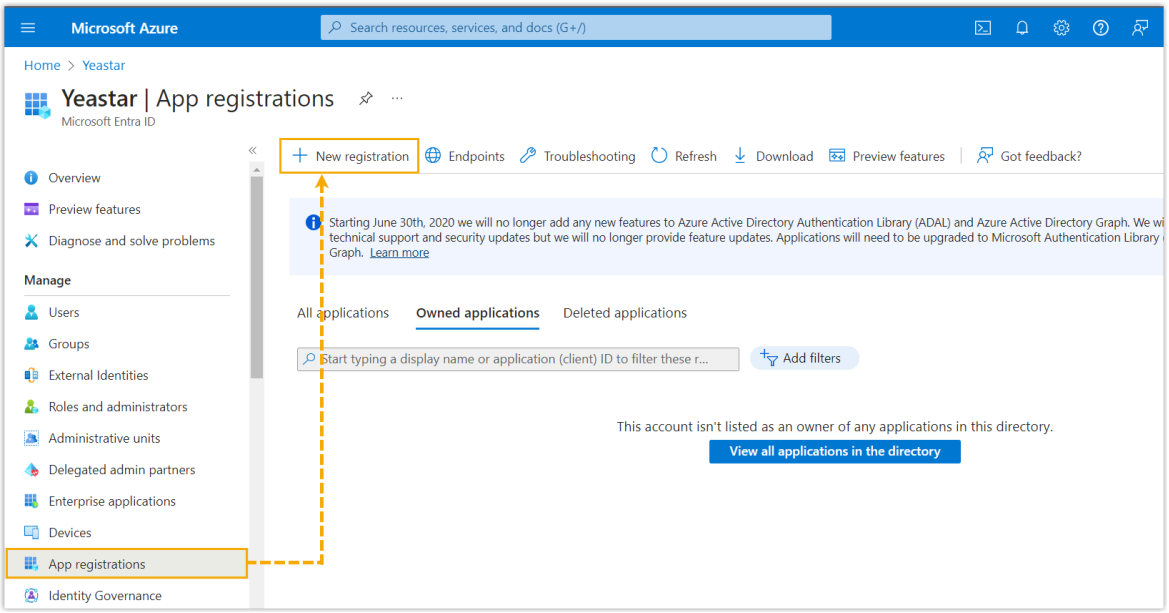
Step 2. Register an application on Microsoft Entra ID

Register an application on Microsoft Entra ID with the redirected URI provided by Yeastar PBX, then obtain the application authentication information for SMTP settings on PBX.

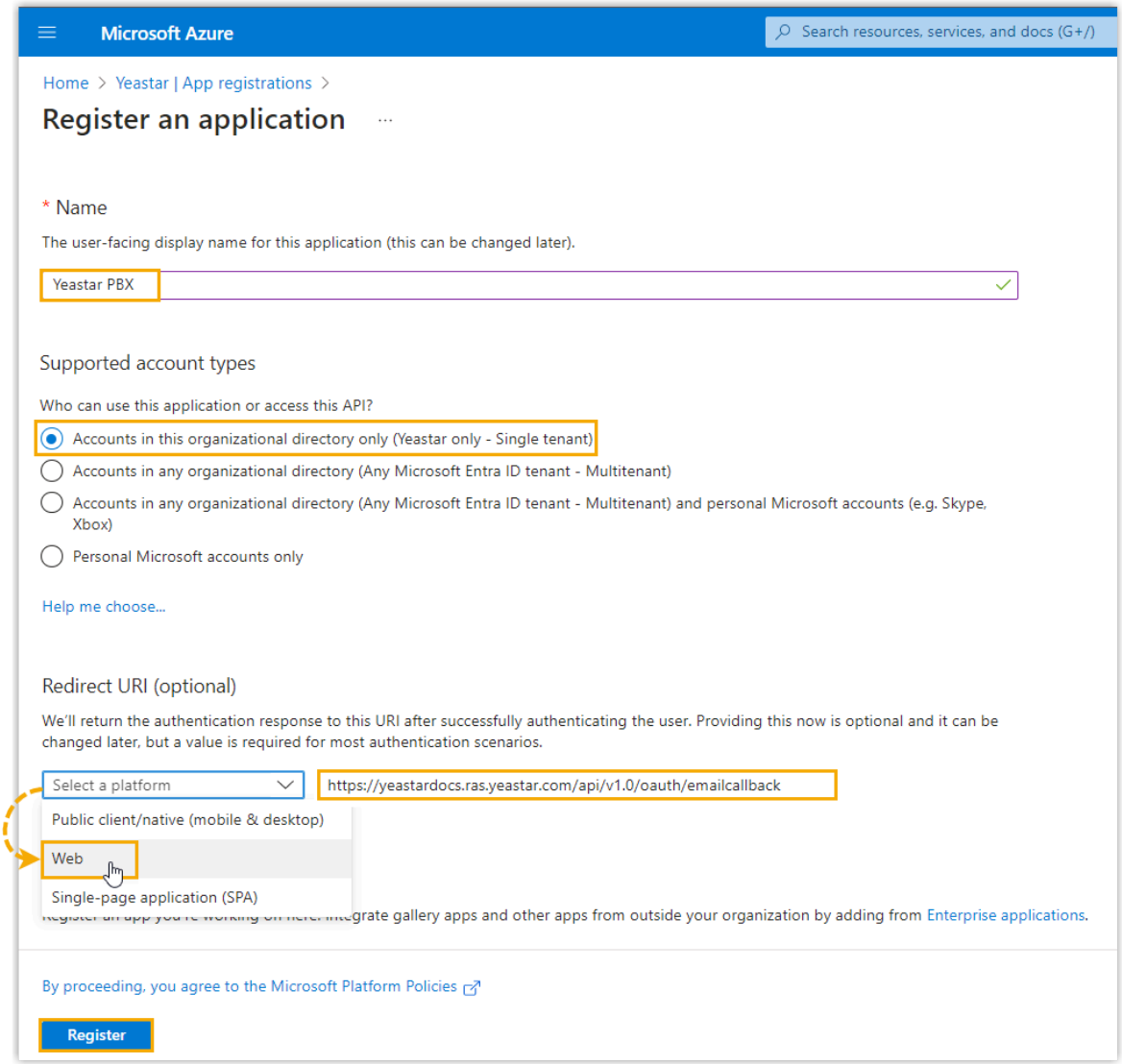
1. Log in to Microsoft Azure Portal with the Microsoft Administrator account.
2. In the search bar, search and select **Microsoft Entra ID** service to enter your organization's directory.



3. On the left navigation bar of organization's directory, go to **App registrations**, then click **New registration**.



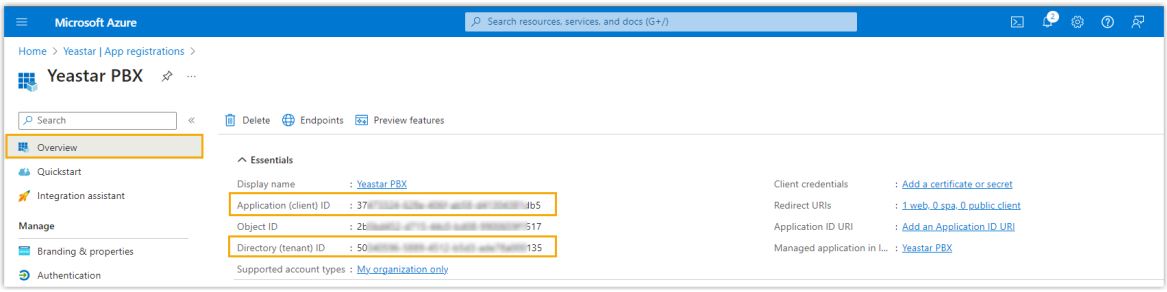
4. In the **Register an application** page, configure the registration information for the application, and click **Register**.



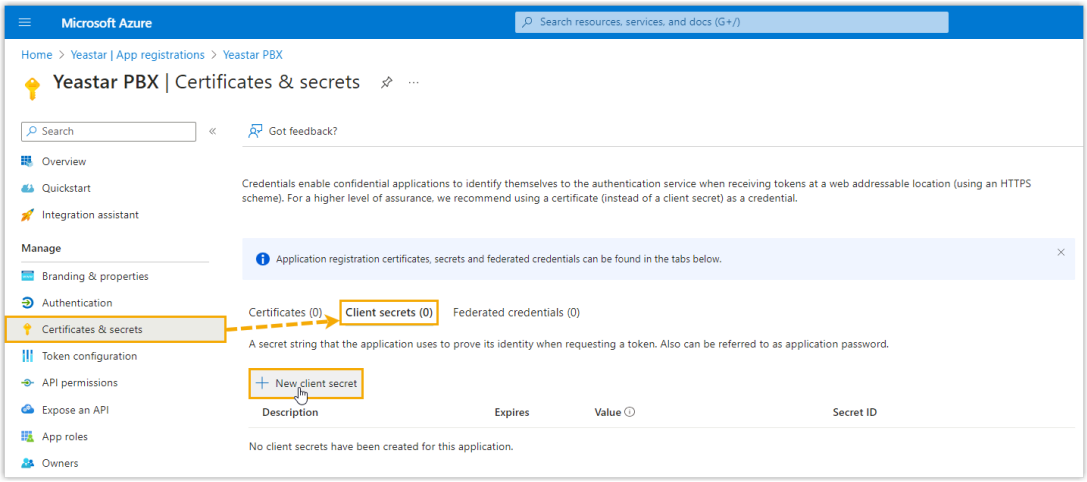
- **Name**: Specify a name to help you identify the application.
- **Supported account types**: Select **Accounts in this organizational directory only**.
- **Redirect URI**: In the **Select a platform** drop-down list, select **Web**, then paste the Redirect URI obtained from the PBX.

An application is registered successfully, you are redirected to the **Overview** page of the application.

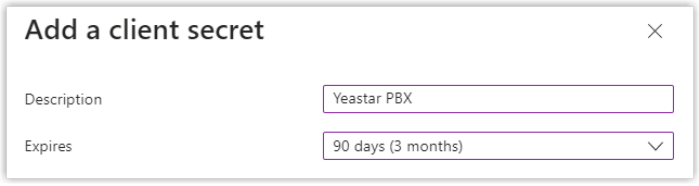
5. Note down the **Application (client) ID** and **Directory (tenant) ID** of the application, as you will need to fill them into the PBX later.



6. Generate a client secret for the application.
    a. On the left navigation bar of the application, go to **Certificates & secrets > Client secrets**, then click **New client secret**.

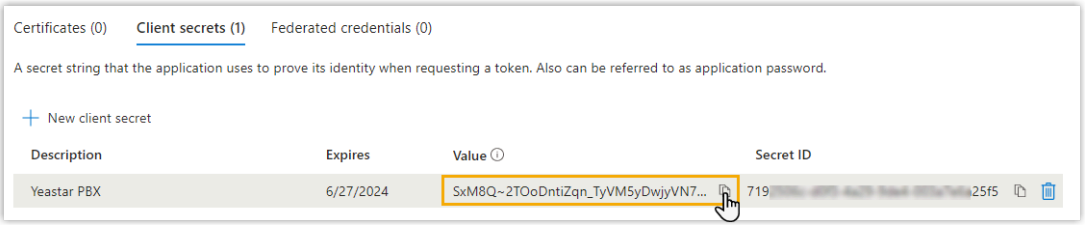


    b. In the **Add a client secret** page, add a description and set an expiration date for the client secret, then click **Add**.



    A client secret is created and displayed in the **Client secrets** list.
    c. Note down the client secret's **Value** as you will need to fill it into the PBX later.

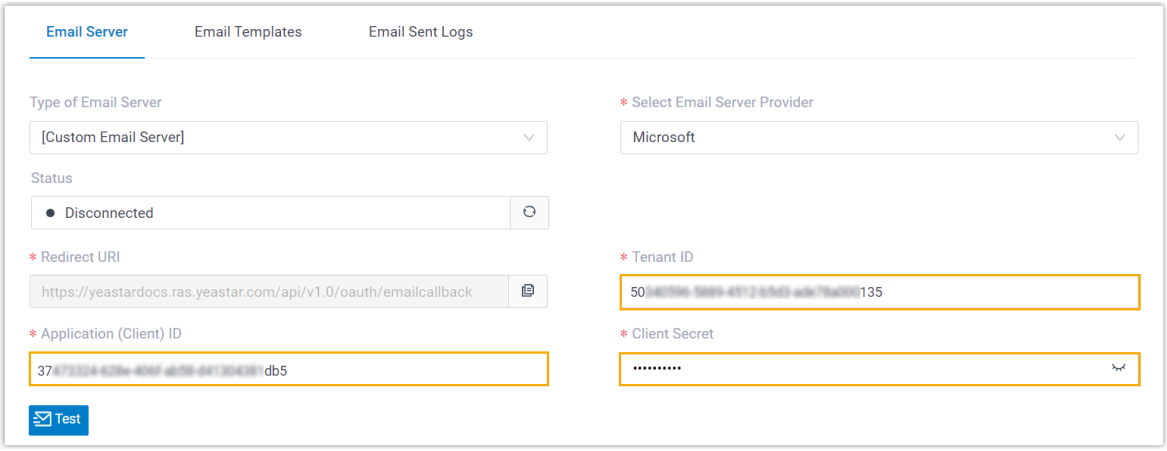
> **Important:**
> Record the client secret's value before leaving the page, as the key is only shown once. Otherwise, you will have to create a new client secret.



Step 3. Configure SMTP settings on PBX

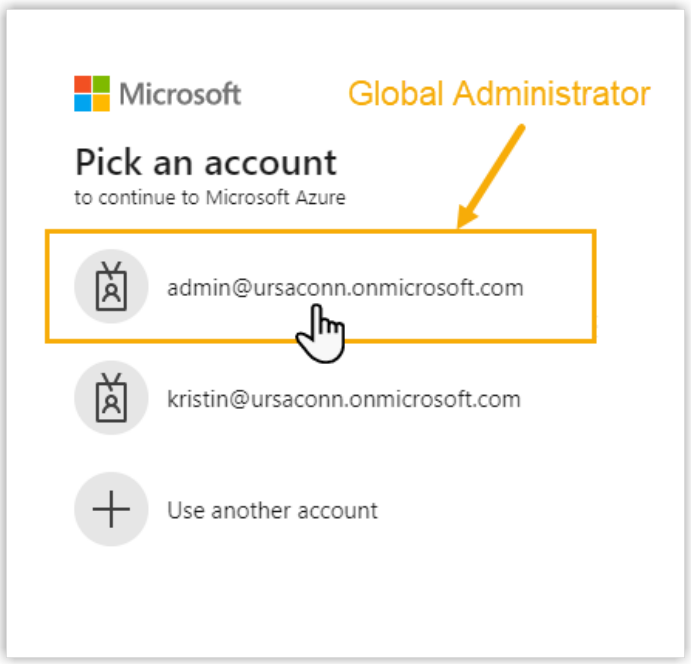
Configure the SMTP settings of the PBX with the authentication information obtained from the Microsoft Entra application, so as to set Microsoft Outlook as the PBX's email server.

1. Log in to PBX web portal, go to **System > Email > Email Server**.
2. In the **Type of Email Server** drop-down list, select **Custom Email Server**.
3. In the **Select Email Server Provider** drop-down list, select **Microsoft**.
4. Enter the following authentication information.

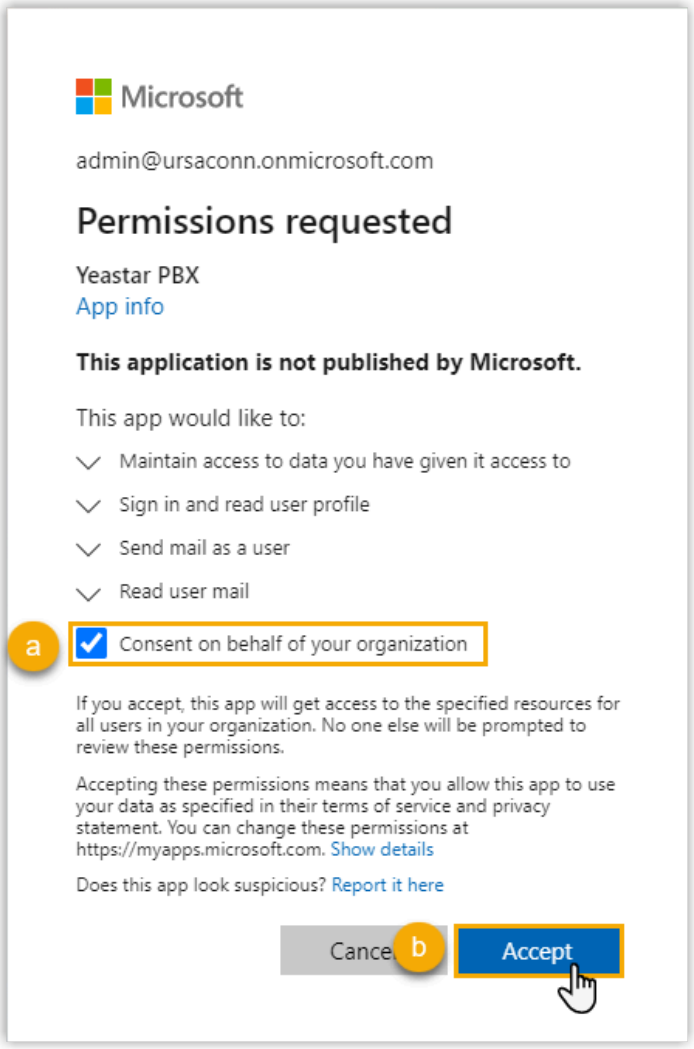


   - **Tenant ID**: Paste the Tenant ID of the Microsoft Entra application.
   - **Application (Client) ID**: Paste the Application ID of the Microsoft Entra application.
   - **Client Secret**: Paste the client secret of the Microsoft Entra application.
5. Click **Save**.

   You are redirect to the Microsoft Sign-in page.
6. Sign in with the Microsoft account that has **Global Administrator** privilege.



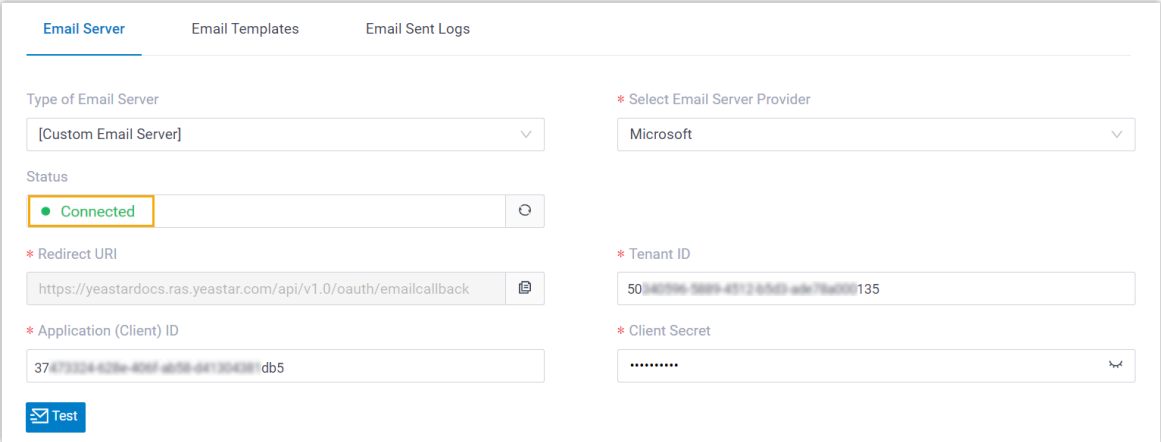
7. In the pop-up window, do as follows to confirm:



a. Select the checkbox of **Consent on behalf of your organization**.

b. Click **Accept**.

On the PBX configuration page, the **Status** field displays **Connected**, indicating that the Microsoft authentication is successful; The Microsoft Outlook is set up as the email server.



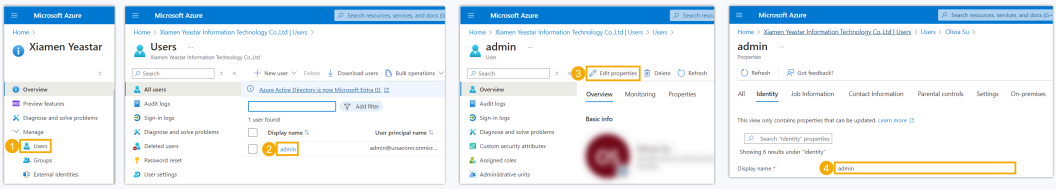
8. Test if the mail server can successfully send emails.
    a. Click **Test**.
    b. In the pop-up window, enter a recipient's email address in the **Email Address** field, then click **Test**.

Result

A test email is sent successfully using the Microsoft account; The page displays "Success" and the recipient's mailbox would receive the email where the sender name and email address are the Microsoft account's display name and user principal name respectively. For example, `admin<admin@ursaconn.onmicrosoft.com>`.

Note:

- If you want to change the sender name of the emails sent by the SMTP server, change the display name of the Microsoft account, as shown below:



- If the test email is failed to be sent, the page displays "Failed to send" and prompts you an error message.

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, system upgrade completed, 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 web 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

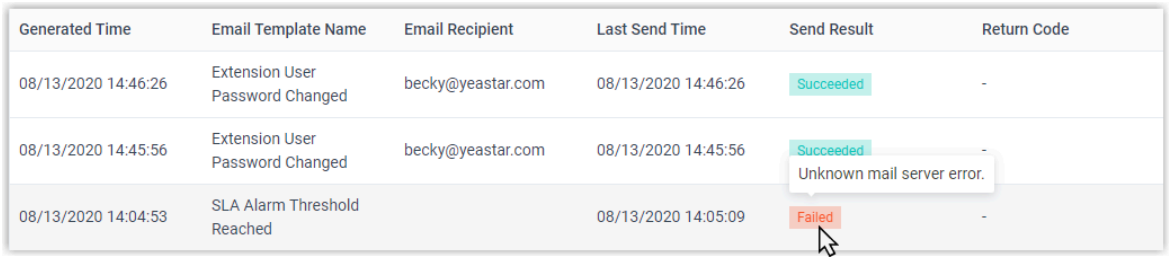
By default, when logs reach 50,000, the newest logs will replace the oldest logs. You can change the value, or restrict how long logs can be saved.

For more information, see Auto Cleanup Settings.

Query email sent logs

1. Log in to PBX web 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.



Storage

Storage Overview

Yeastar P-Series PBX System provides local storage and supports external storage and network drive storage.

Storage limitation

Storage	P520	P550	P560	P570
LOCAL (Local Flash)	1	1	1	1
USB 2.0 (USB Portable SSD, Up to 2 TB) (USB Flash Drive, Up to 256 GB)	0	1	1	1
Hard Disk (Up to 2 TB)	0	0	1	1
SD Card (Up to 64 GB)	0	0	1	1
Micro SD Card (Up to 64 GB)	1	0	0	0
Network drive	1	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).

- External Chat Files
- Backup files

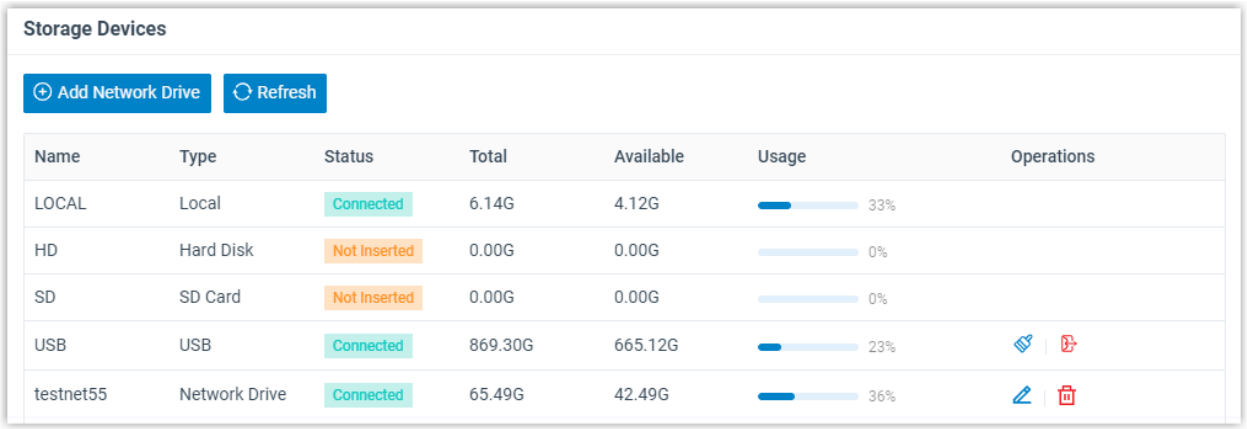
For more information, see Manage Storage Locations.

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, and SD card.
- Click to remove USB, hard disk, and SD card .



Set up a USB Flash Drive

This topic describes how to set up a USB flash drive on Yeastar P-Series PBX System.

> **Note:**
> USB flash drive is ONLY supported on P550, P560, and P570.

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 web 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.

> **Note:**
> Hard disk drive is ONLY supported on P560 and P570.

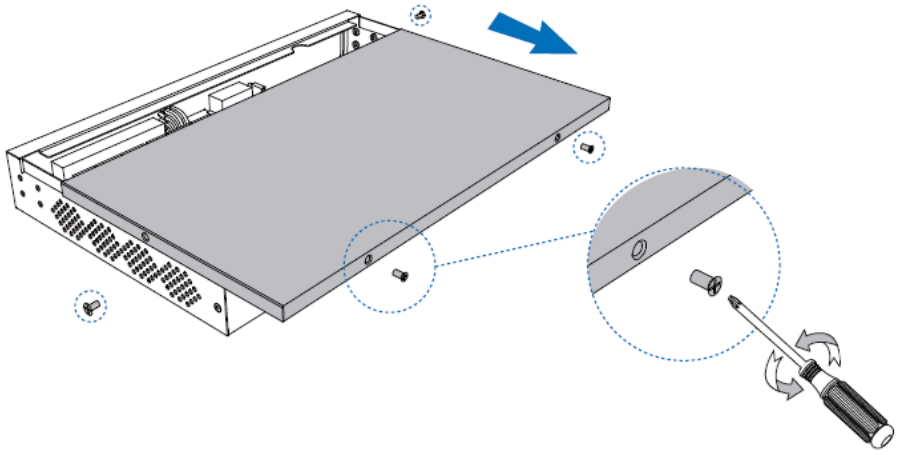
Prerequisites

- 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.

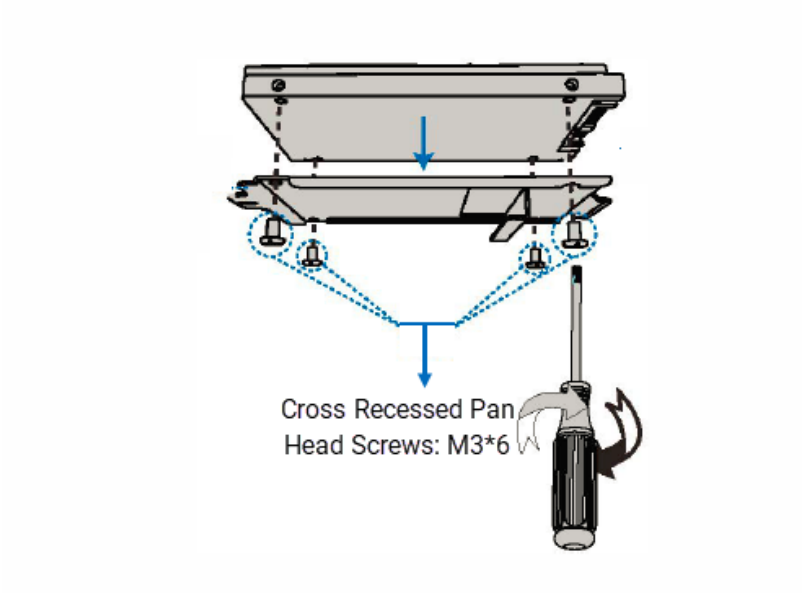
Procedure

1. Install hard disk drive on Yeastar P-Series PBX System.

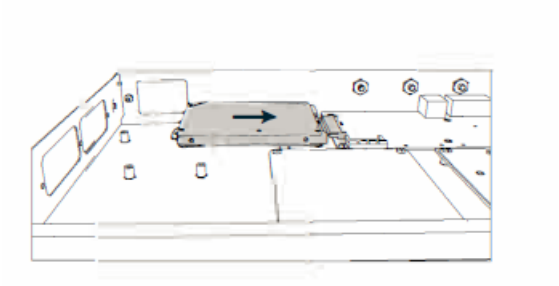
a. Loosen the screws at the bottom of the device and remove the upper cover.



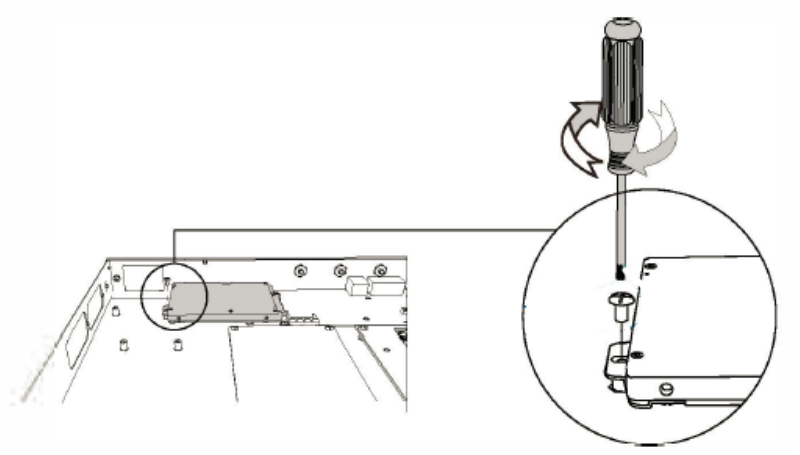
b. Lock the hard disk drive on the bracket.



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 web 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.

> **Note:**

SD card is ONLY supported on P560 and P570.

Prerequisites

- Prepare an SD card, which meets the following requirements:
  - Maximum capacity: Up to 64 GB
  - Minimum performance: SDHC/SDXC Class10 UHS-I U3
  - Minimum write speed: 60 MB/s
  - Recommended brands: Sandisk Extreme Pro Series, Sandisk Extreme Series, or Kingston
- 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.
   a. Log in to PBX web 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. All the data in the SD card will be cleared after 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.

Set up a Micro SD Card

This topic describes how to set up a Micro SD card on Yeastar P-Series PBX System.

> **Note:**
> Micro SD card is ONLY supported on P520.

Prerequisites

- Prepare a Micro SD card, which meets the following requirements:
  - Maximum capacity: Up to 64 GB
  - Minimum performance: SDHC/SDXC Class10 UHS-I U3
  - Minimum write speed: 60 MB/s
  - Recommended brands: Sandisk Extreme Pro Series, Sandisk Extreme Series, or Kingston
- Back up data on the Micro SD card in advance.

Procedure

1. Insert the Micro SD card to the PBX's Micro SD card slot.
2. Format the Micro SD card.
   a. Log in to PBX web portal, go to **System > Storage > Storage Devices**, find the Micro SD card.

      > **Note:**
      > In the **Type** field, the Micro SD card you inserted will display as **SD Card**.

   b. In the **Operations** column, click .
   c. In the pop-up dialog box, click **OK**.

      The Micro SD card is formatting. All the data in the Micro SD card will be cleared after formatting.
3. In the **Storage Devices** section, check status of the Micro SD card.
   - **Connected**: The Micro SD card is connected.
   - **Not Inserted**: No Micro SD card is inserted.
   - **Error**: Format error.
   - **Read Only**: Can NOT write data to the Micro SD card.

What to do next

Decide what data will be stored on the Micro 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:

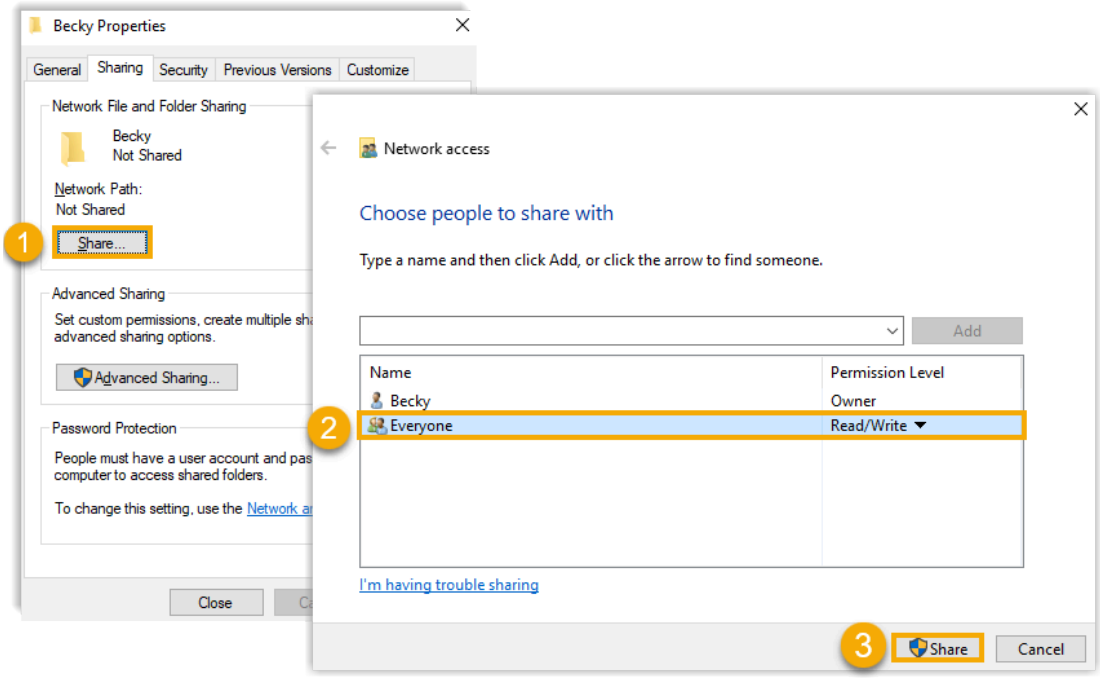
- **Yeastar P520**: Max. 1 network drive
- **Yeastar P550**: Max. 1 network drive
- **Yeastar P560**: Max. 2 network drive
- **Yeastar P570**: Max. 2 network drive

Prerequisites

Make sure that the computer is always in service, or Yeastar P-Series PBX System cannot add files to the shared folder.

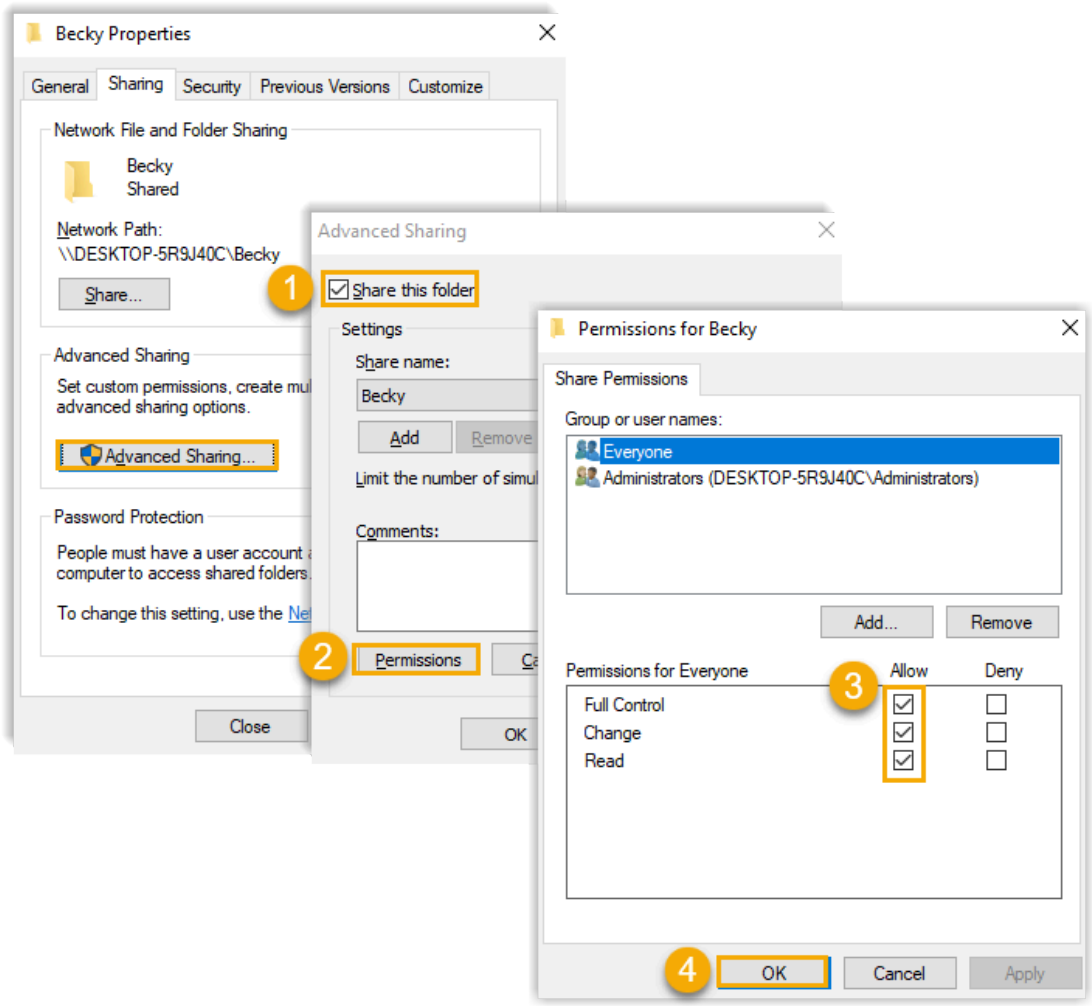
Step1. Create a shared folder in Windows 10

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**.

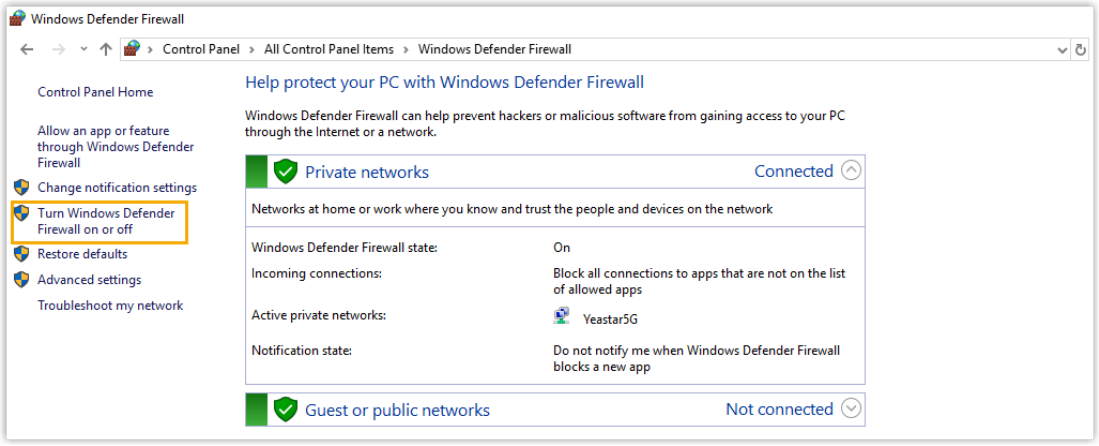
4. Click **Advanced Sharing...**, configure advanced Share properties.



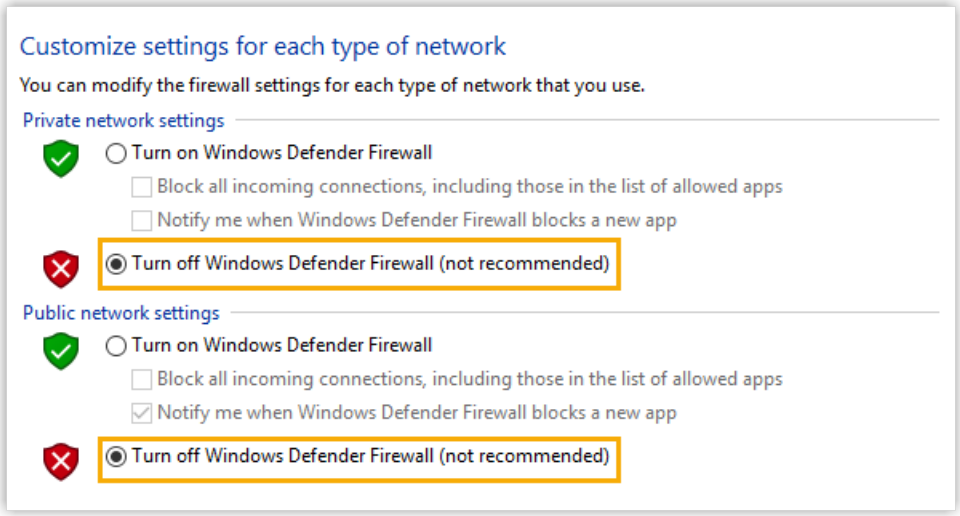
a. Select the checkbox of **Share this folder**.
b. Click **Permissions**.
c. In the pop-up window, allow all the permissions.
d. Click **OK**.

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 web 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}*. For example, shared_folder/recording.

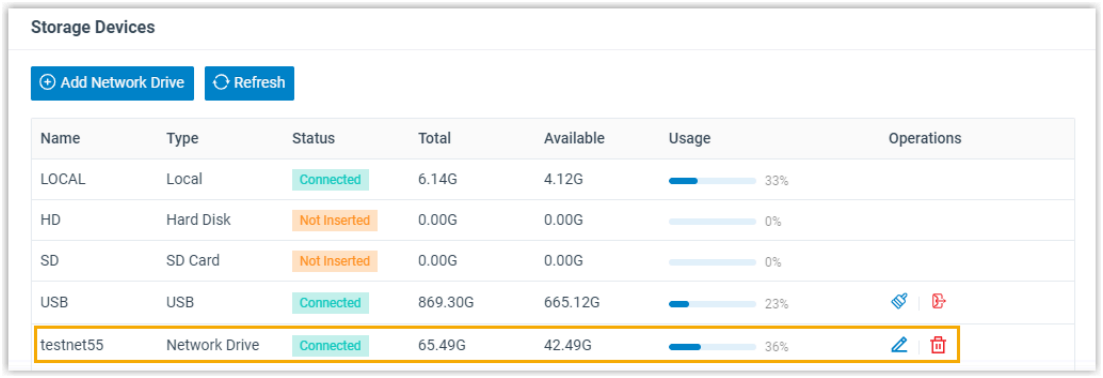
- **Access Username**: Enter the username to access the shared folder.
- **Access Password**: Enter the password to access the shared folder.
- **Work Group**: Optional. If you have set work group on your network drive, enter the name of the work group. If not, leave this field blank.
- **Samba Version**: 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**

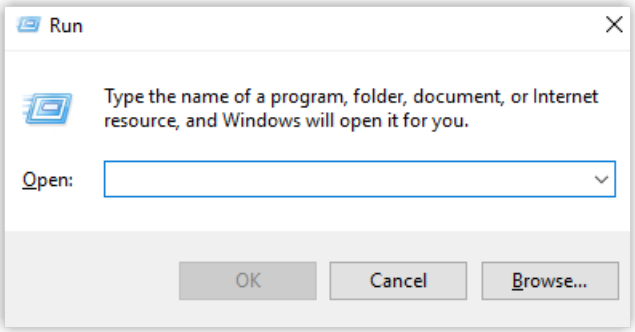


What to do next

Decide what data will be stored on the network drive. For more information, see Manage Storage Locations.

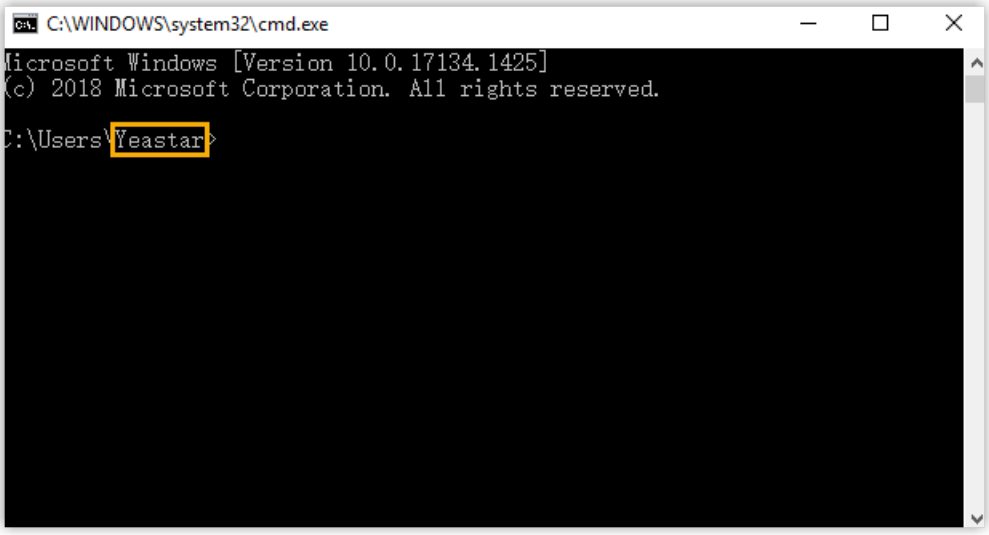
Network Drive FAQ

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**.

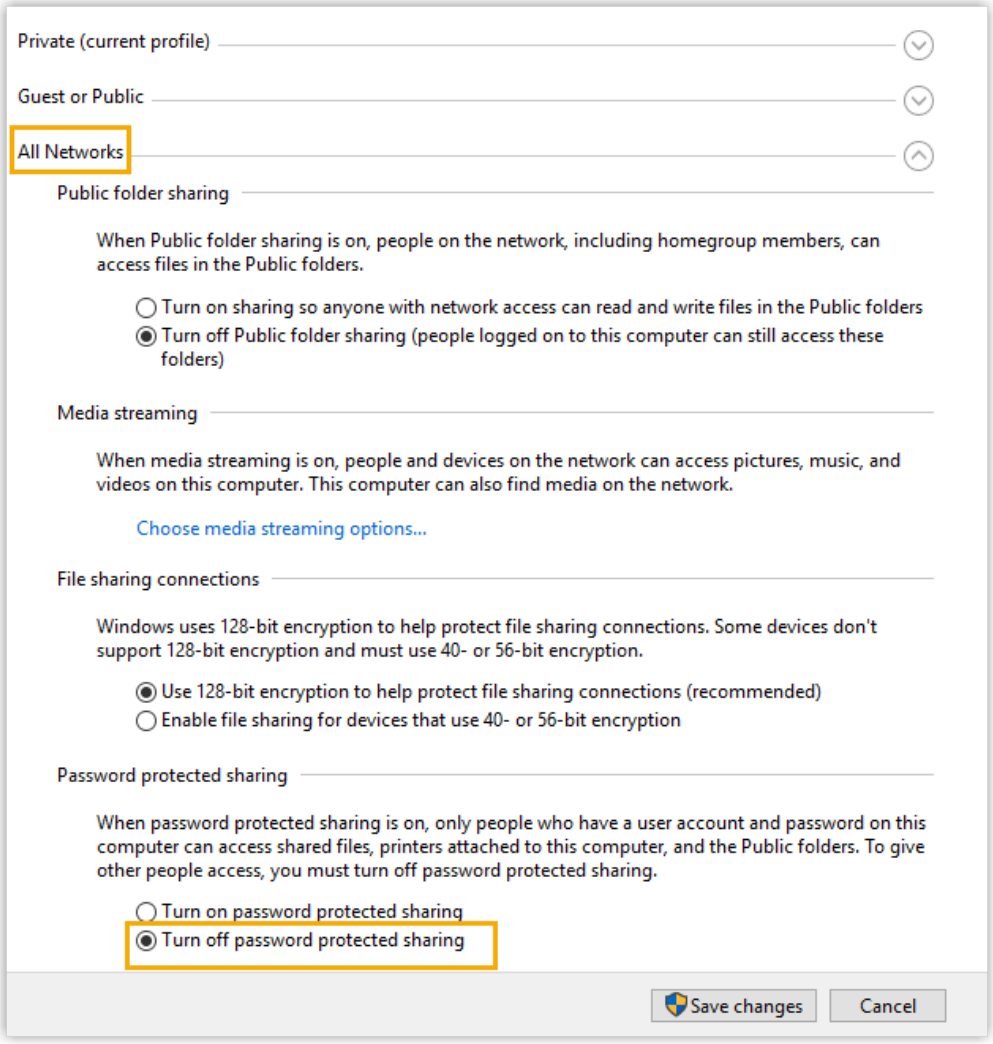
    The user name is displayed on the Command Prompt.



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:

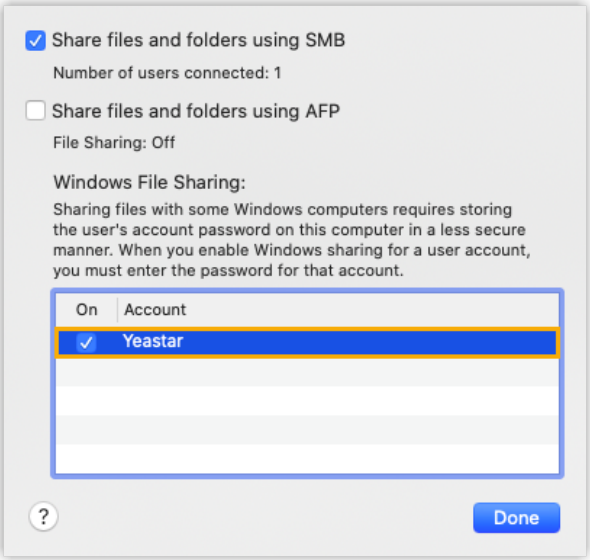
- **Yeastar P520**: Max. 1 network drive
- **Yeastar P550**: Max. 1 network drive
- **Yeastar P560**: Max. 2 network drive
- **Yeastar P570**: Max. 2 network drive

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

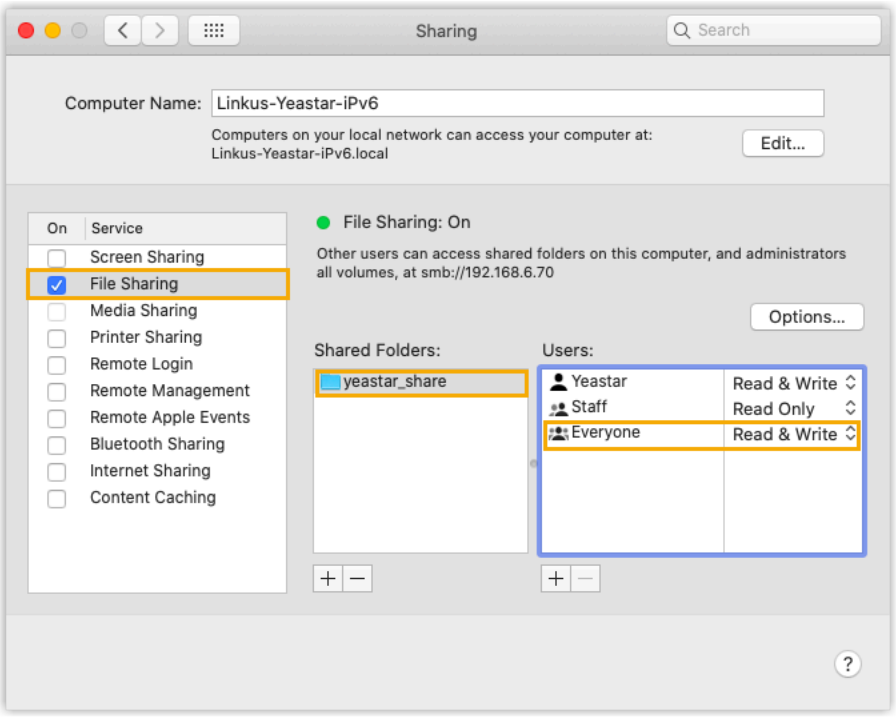
1. On your Mac, create a folder and specify a name to help you identify it.
2. Go to **Apple menu** **> System Preferences > Sharing** to set up file sharing.
   a. On the left navigation bar, select the checkbox of **File Sharing**.
   b. Click **Options** to configure sharing credentials.



      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**.

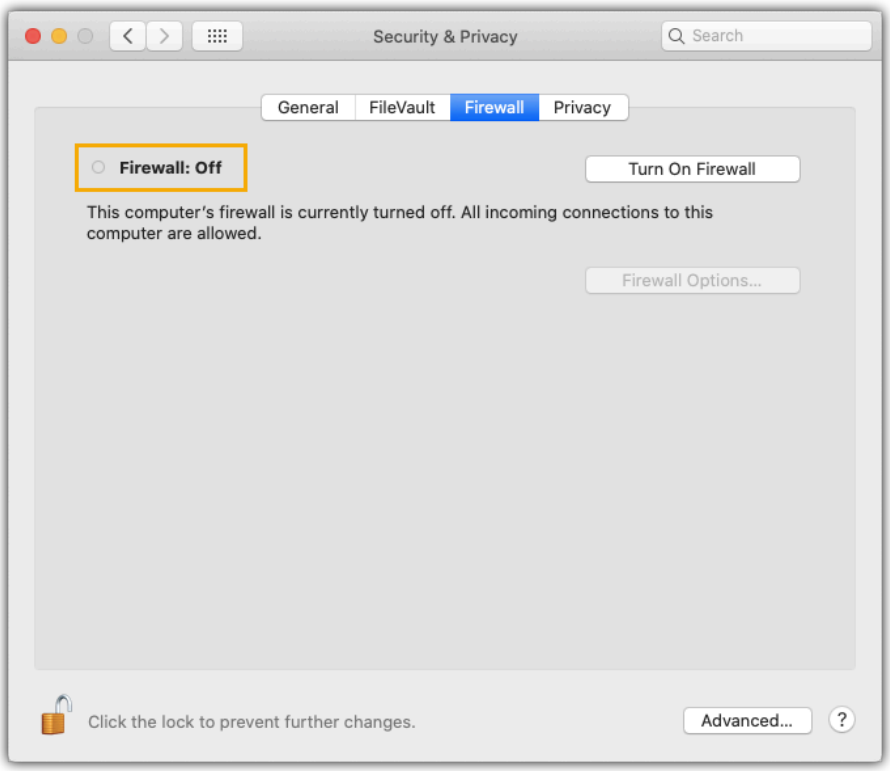
e. Click to close the window.



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 web 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.

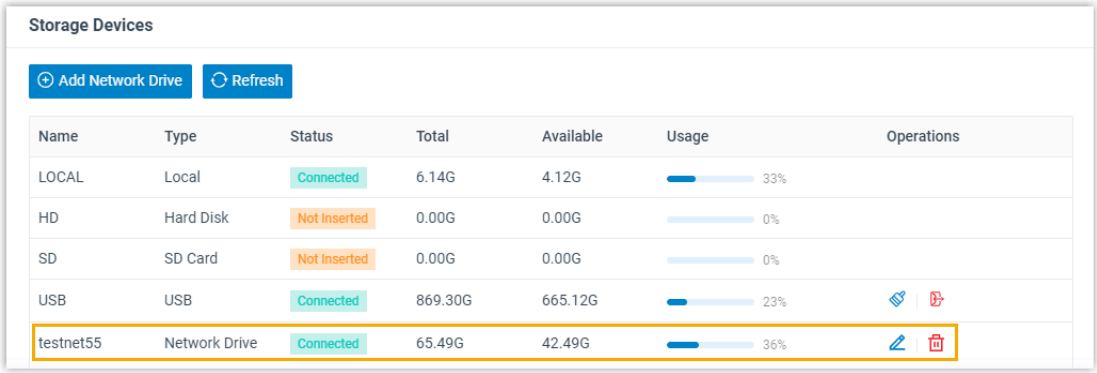
    - **Access Username**: Enter the username to access the shared folder.
    - **Access Password**: Enter the password to access the shared folder.
    - **Work Group**: Optional. If you have set work group on your network drive, enter the name of the work group. If not, leave this field blank.
    - **Samba 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**

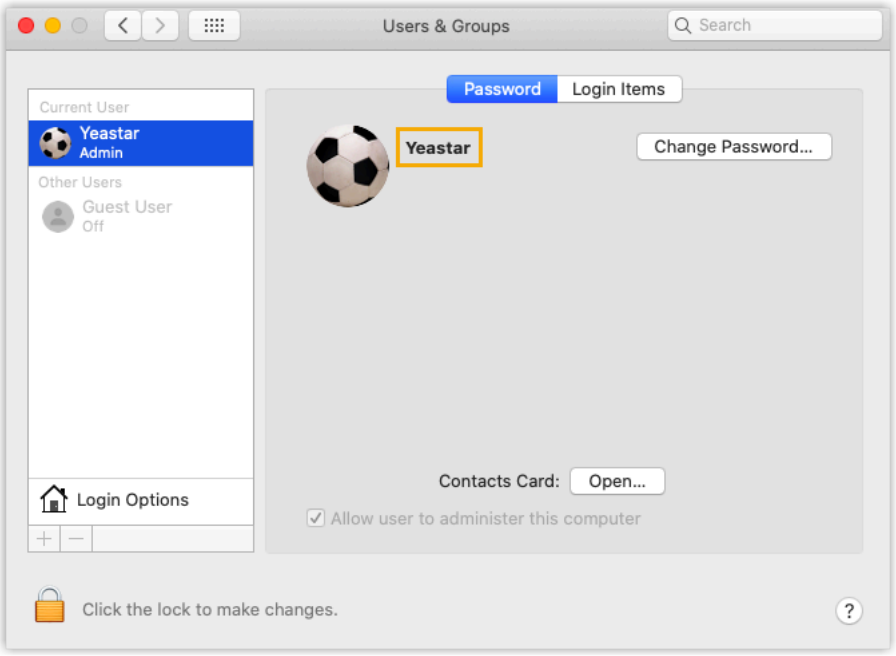


What to do next

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:

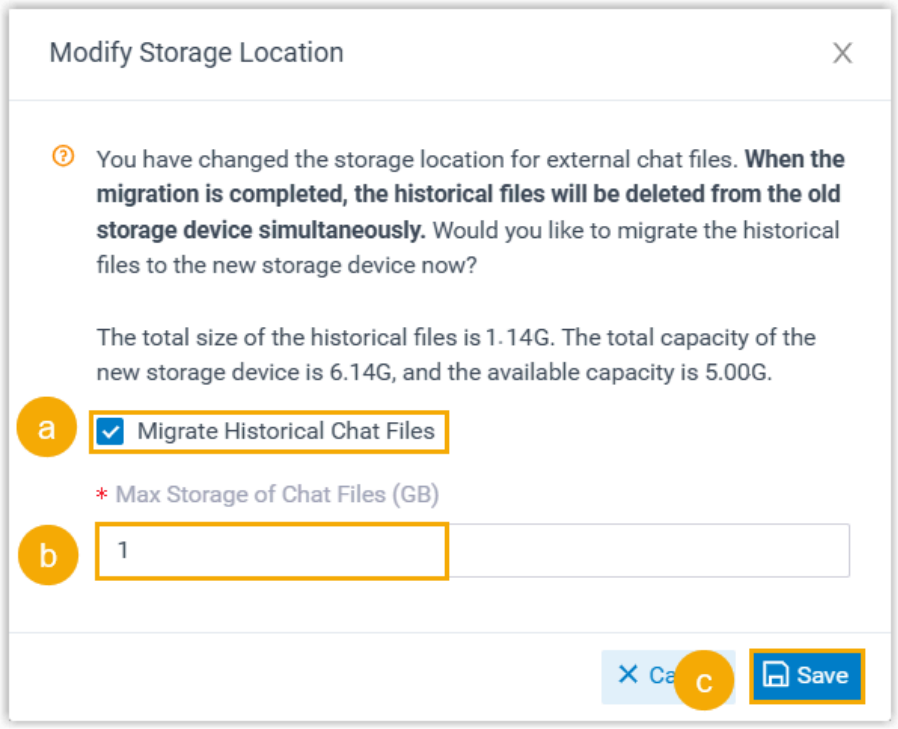
  - Set up a USB Flash Drive
  - Set up a Hard Disk Drive
  - Set up an SD Card
  - Set up a Micro SD Card
  - Add a Windows Network Drive
  - Add a Mac Network Drive

Procedure

1. Log in to PBX web 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.
- **External Chat Files**: Can be stored either on local flash or external device.

3. Click **Save**.
4. If you change the storage location for the external chat files, complete the further settings in the pop-up window.



a. If you want to migrate historical chat files to the new storage location, select the checkbox of **Migrate Historical Chat Files**.

> **Important:**
> Regardless of whether historical files are migrated or not, the files will be deleted from the original storage device after changing the storage location.

b. In the **Max Storage of Chat Files (GB)** field, set the maximum number of storage that external chat files could be retained.

> **Note:**

> The maximum storage for chat files set here will be synchronized to auto cleanup settings.

c. 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

Setting	Description
Max Number of CDR	Set the maximum number of CDR that should be retained. 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. When it reaches the maximum number, the oldest CDR will be deleted. **Default value**: 200,000 **Maximum value**: 1,000,000
CDR Preservation Days	Set the maximum number of days that CDR should be retained. 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. When it reaches the maximum preservation days, the oldest CDR will be deleted. **Default value**: 0, which means no limit.

Voicemail Auto Cleanup

Setting	Description
Max Number of Voicemail	Set the maximum number of voicemails that should be retained. 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. When it reaches the maximum number, the oldest voicemails will be deleted. **Default value**: 100 **Maximum value**: 500
Voicemail Preservation Days	Set the maximum number of days that voicemails should be retained. 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. When it reaches the maximum preservation days, the oldest voicemails will be deleted. **Default value**: 0, which means no limit.

Recording Auto Cleanup

Setting	Description
Max Usage of Device (%)	Set the maximum storage percentage that the device is allowed to store recording files. 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. When it reaches the maximum storage percentage, the oldest recording files will be deleted. **Default value**: 80% **Maximum value**: 99% **Note:** You can directly enter a value in this field to set the maximum storage percentage.
Recordings Preservation Days	Set the maximum number of days that recording files should be retained.

Setting	Description
	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. When it reaches the maximum preservation days, the oldest recording files will be deleted. **Default value**: 0, which means no limit.

External Chat Data Auto Cleanup

Data Type	Setting	Description
Chat Logs	Max Number of External Chat Logs	Set the maximum number of external chat logs to store. 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. When it reaches the maximum number, the oldest external chat logs will be deleted. **Default value**: 50,000 **Maximum value**: 100,000
	External Chat Data Preservation Days	Set the maximum number of days that external chat logs should be retained. 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. When it reaches the maximum preservation days, the oldest external chat logs will be deleted. **Default value**: 0, which means no limit.
Chat Files	Max Storage of Chat Files (GB)	Set the maximum number of storage that external chat files (including documents and images) should be retained. 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. When it reaches the maximum number, the oldest external chat files will be deleted. **Default value**: 1

Data Type	Setting	Description
	External Chat Files Preservation Days	Set the maximum number of days that external chat files (including documents and images) should be retained. 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. When it reaches the maximum preservation days, the oldest external chat files will be deleted. **Default value**: 7 **Note:** Entering 0 means no limit.

System Backup Files Auto Cleanup

Setting	Description
Max Number of Files	Set the maximum number of backup files that should be retained. 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. When it reaches the maximum number, the oldest backup files will be deleted. **Default value**: 5 **Maximum value**: 8

Event Logs Auto Cleanup

Setting	Description
Max Number of Logs	Set the maximum number of event logs that should be retained. When it reaches the maximum number, the oldest event logs will be deleted. **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.

Setting	Description
	Default value: 50,000 **Maximum value**: 1,000,000
Logs Preservation Days	Set the maximum number of days that event logs should be retained. When it reaches the maximum preservation days, the oldest event logs will be deleted. **Default value**: 0, which means no limit.

Email Sent Logs Auto Cleanup

Setting	Description
Max Number of Logs	Set the maximum number of email sent logs that should be retained. When it reaches the maximum number, the oldest email sent logs will be deleted. **Default value**: 50,000 **Maximum value**: 1,000,000
Logs Preservation Days	Set the maximum number of days that email sent logs should be retained. When it reaches the maximum preservation days, the oldest email sent logs will be deleted. **Default value**: 0, which means no limit.

Operation Logs Auto Cleanup

Setting	Description
Max Number of Logs	Set the maximum number of operation logs that should be retained. When it reaches the maximum number, the oldest operation logs will be deleted. **Default value**: 50,000 **Maximum value**: 1,000,000
Logs Preservation Days	Set the maximum number of days that operation logs should be retained. When it reaches the maximum preservation days, the oldest operation logs will be deleted. **Default value**: 0, which means no limit.

System Logs Auto Cleanup

Setting	Description
Max Storage of Logs (MB)	Set the maximum file size for a system log package. When it reaches the maximum file size, the oldest logs in the package will be deleted. **Default value**: 10
Logs Preservation Days	Set the maximum number of days that a system log should be retained. **Default value**: 7 **Maximum value**: 15

File Sharing

Set Up FTP File Sharing

After setting up FTP File Sharing, Yeastar P-Series PBX System can work as an FTP server, you can access the files that are stored in the PBX external storage and local storage via FTP from a local computer.

> **Note:**
> The default FTP port is 21. For security purpose, you can change the FTP port on **System > Network > Service ports**.

Procedure

Step1. Enable FTP on the PBX

Step2. Access the PBX files via FTP

Step1. Enable FTP on the PBX

1. Log in to PBX web portal, go to **System > Storage > File Sharing**.
2. In the **FTP** section, enable **FTP** and click **OK** in the pop-up window.
3. Select the checkbox of **Access Files via FTP**.

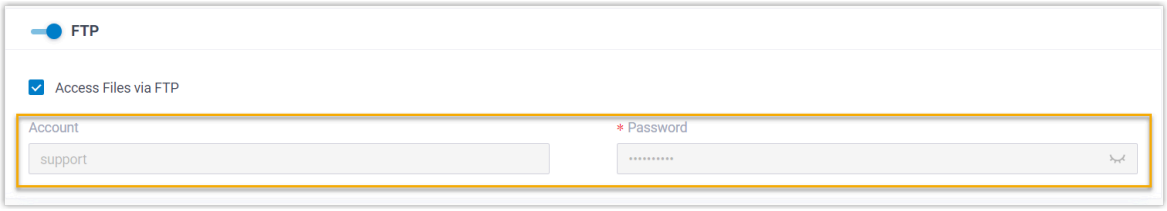
> **Note:**

> Ensure this option is selected otherwise you can not access the files stored in PBX external storage.

4. Click **Save**.

   The PBX can now be used as an FTP server.

5. Check the **Account**, and click the to check and note down the **Password**.

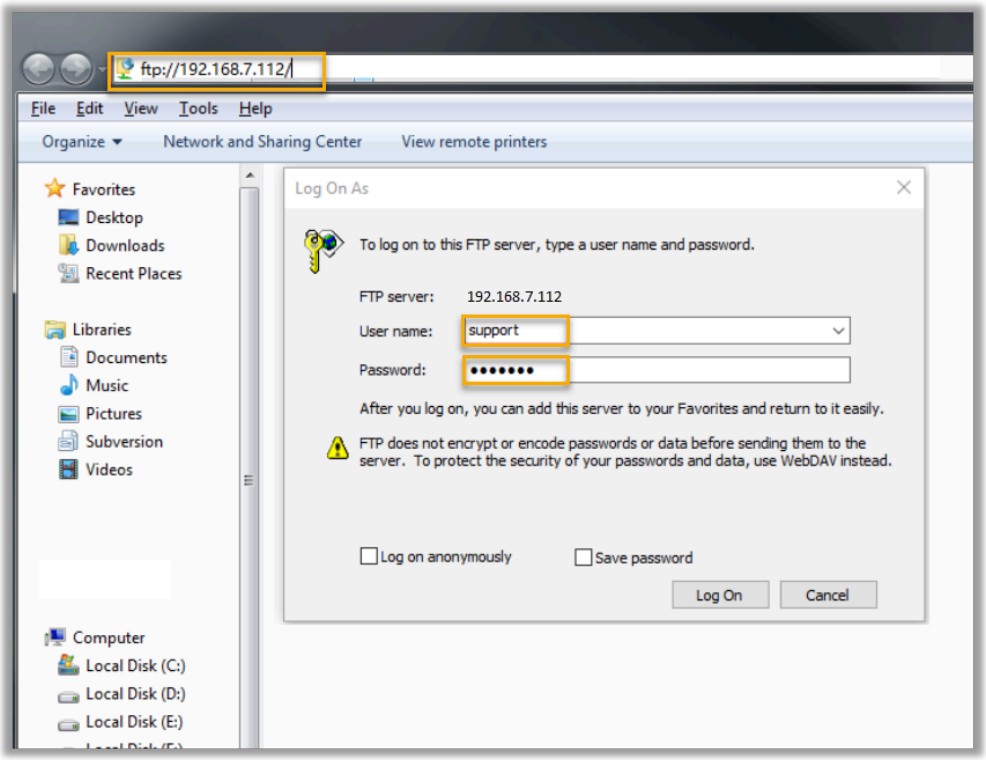


> **Note:**
> The FTP password is the same as the SSH password. If the SSH password is reset, the FTP password will be updated to the latest SSH password automatically.

Step2. Access the PBX files via FTP

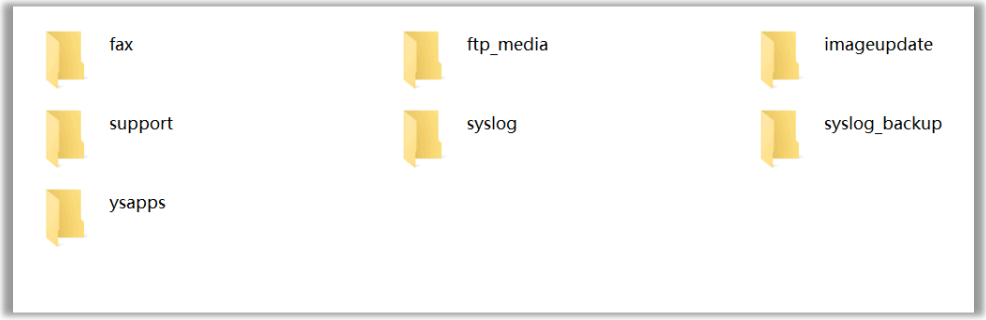
1. On a Windows PC, press **Win + E** to open a Windows Explorer window.
2. In the address bar, enter the FTP address of the PBX `ftp://{IP address of the PBX}`, then press **Enter**.

   For example, the IP address of the PBX is 192.168.7.112, then you should enter `ftp://192.168.7.112`.
3. In the pop-up window, enter the credentials to access the PBX files.



a. Enter the user name and password.
   - **User name**: Enter `support`.
   - **Password**: Enter the FTP password.

b. Click **Log On**.
   You will see the following folders that contain the files from PBX local storage and external storage.



4. **Optional**: Enter the folder `ftp_media` to check the files stored in PBX external storage.
   The subfolders in this folder vary depending on the PBX external storage devices:
   - **mmc** folder for the files stored in SD card.
   - **usb** folder for the files stored in USB drive.

- **harddisk** folder for the files stored in hard disk.

> **Note:**
> If no subfolder appears, check if the external storage device is connected to the PBX properly.

Result

Now you can check, edit, upload, and download the files that are stored in the PBX external storage and local storage according to your need via FTP.

Set Up File Sharing

Yeastar P-Series PBX System supports a file sharing feature, which allows you to access and share files that are stored in external storage devices of PBX from a local computer.

Prerequisite

- You have set up external storage devices on PBX.
- You have stored desired data on external storage devices. For more information, see Manage Storage Locations.

Procedure

Step1. Enable File Sharing feature on the PBX

Step2. Access the shared files on PC

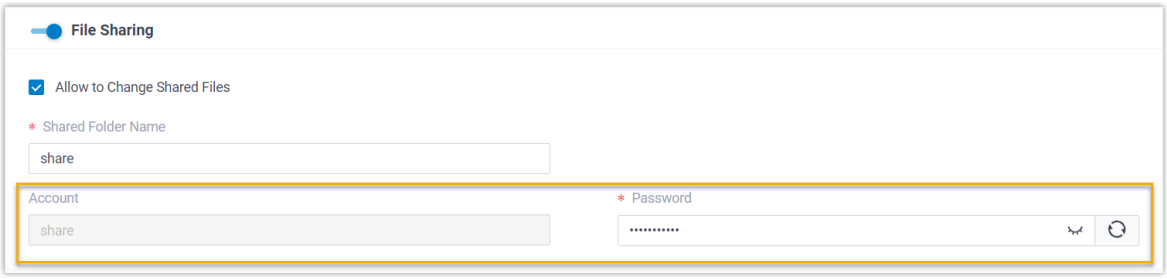
Step1. Enable File Sharing feature on the PBX

1. Log in to PBX web portal, go to **System > Storage > File Sharing**.
2. In the **File Sharing** section, enable **File Sharing** and click **OK** in the pop-up window.
3. Select the checkbox of **Allow to Change Shared Files**.

> **Note:**
> Ensure this option is selected otherwise you can not edit, upload or download the files in the shared file holder.

4. In the **Shared Folder Name** field, specify a folder name to help you identify it.
5. Click **Save**.

6. Check and note down the **Account** and **Password**.



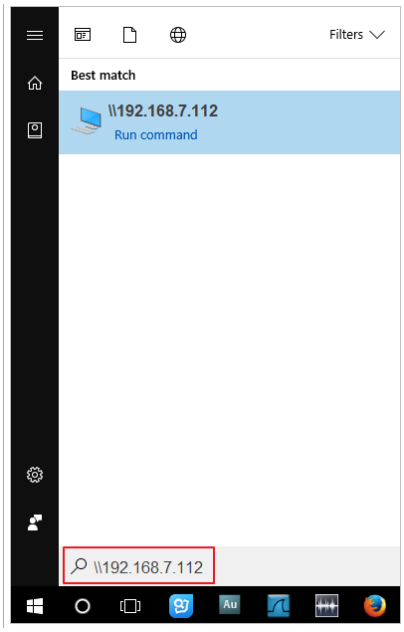
- **Account**: `share`.

> **Note:**
> The **Account** name can not be changed.

- **Password**: Auto-generated random password.
  - Click to check the password.
  - Click to generate a new random password.

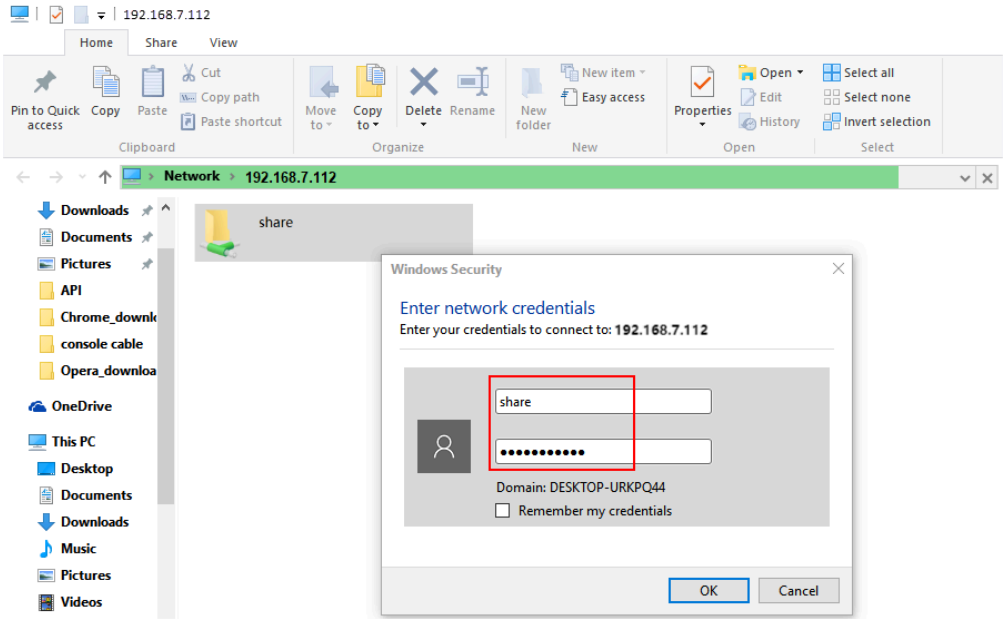
Step2. Access the shared files on PC

1. In the **Windows search** field, enter `\\{IP address of the PBX}`, then press **Enter**. For example, the IP address of the PBX is 192.168.7.112, then you should enter `\\192.168.7.112`.



2. Double-click the shared folder.

   A pop-up window requires login credentials.
3. In the pop-up window, enter the credentials.



   a. Enter the user name and password.
      - **User name**: Enter `share`.
      - **Password**: Enter the password.

   b. Click **OK**.

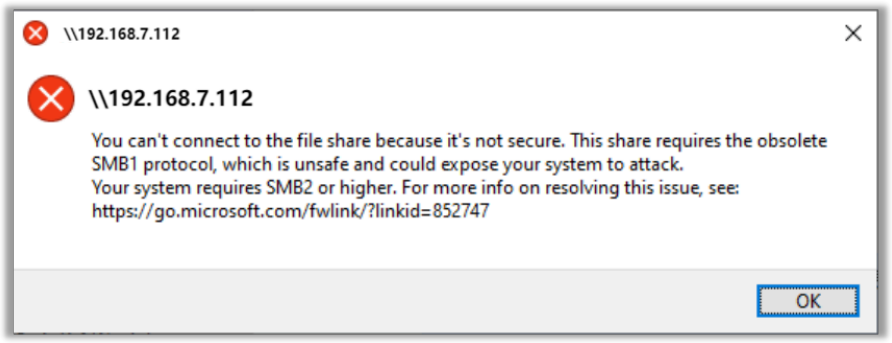
      You can now access the shared folder. In this folder, there are subfolders that contain the shared files from PBX external storage. The subfolders vary depending on the PBX external storage device:
      - **mmc** folder for the shared files in SD card.
      - **usb** folder for the shared files in USB drive.
      - **harddisk** folder for the shared files in hard disk.

> **Note:**
> If no subfolders appears, check if the external storage device is connected to the PBX properly.

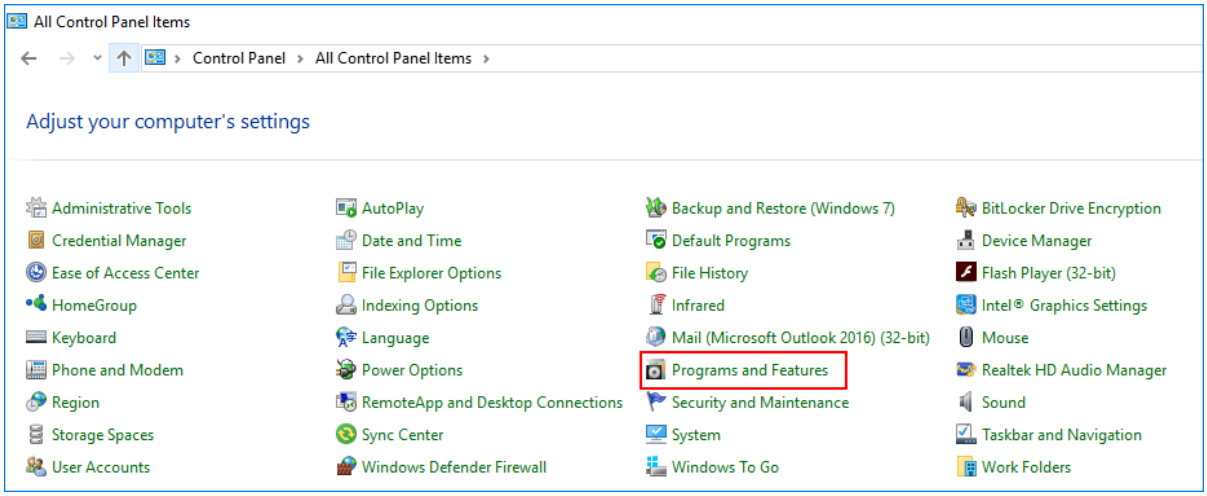
File Sharing FAQ

Windows 10 users cannot access the shared folder of the PBX

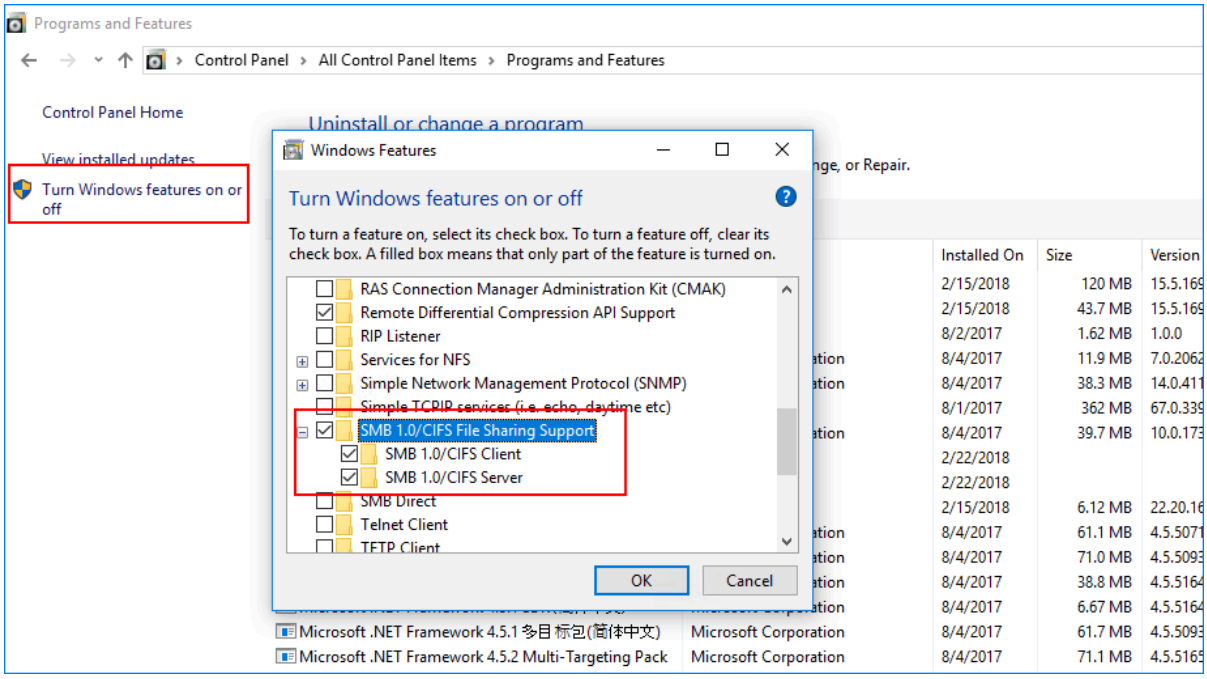
If you fail to access the shared folder and see the pop-up window shown as below, do as follows.



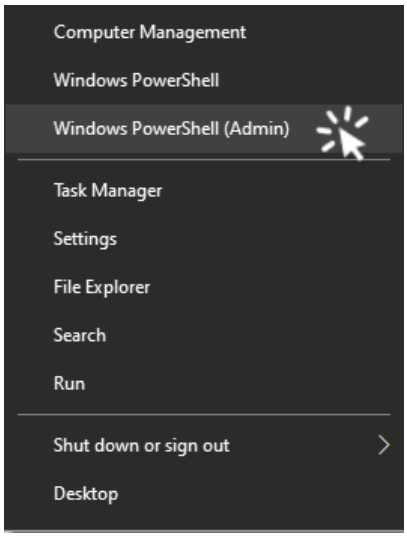
1. Go to **Control Panel > Programs and Features**.



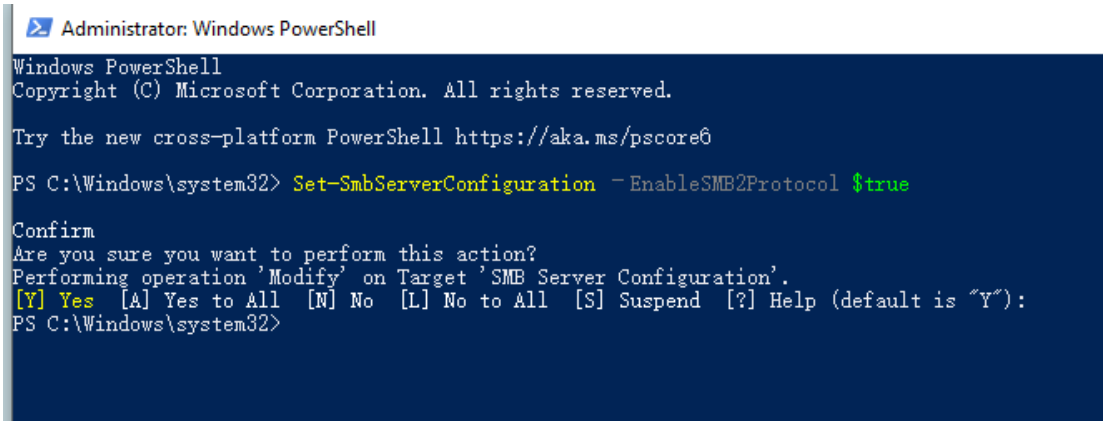
2. On the left column of the window, click **Turn Windows features on or off**.
3. In the pop-up window, check the option of **SMB 1.0/CIFS File Sharing Support**.



4. Press **Win** + **X**, and select **Windows Powershell(Admin)**.



5. In the pop-up window, enter `Set-SmbServerConfiguration –EnableSM-B2Protocol $true`, and press **Enter**.



6. Press **Enter** again to execute the command.
7. Reboot your computer and retry.

Set up PBX as a TFTP Server

By setting up the TFTP feature, Yeastar P-Series PBX System can work as a TFTP server, you can upload or download desired files to/from a specific PBX file folder (/ysdisk/tftp-boot) via TFTP.

Procedure

1. Log in to PBX web portal, go to **System > Storage > File Sharing**.
2. Scroll down to the **TFTP** section, enable **TFTP** and click **OK** in the pop-up window.
3. Click **Save**.

Result

The PBX can now be used as a TFTP server, you can upload or download desired files to/from the specific PBX file folder.

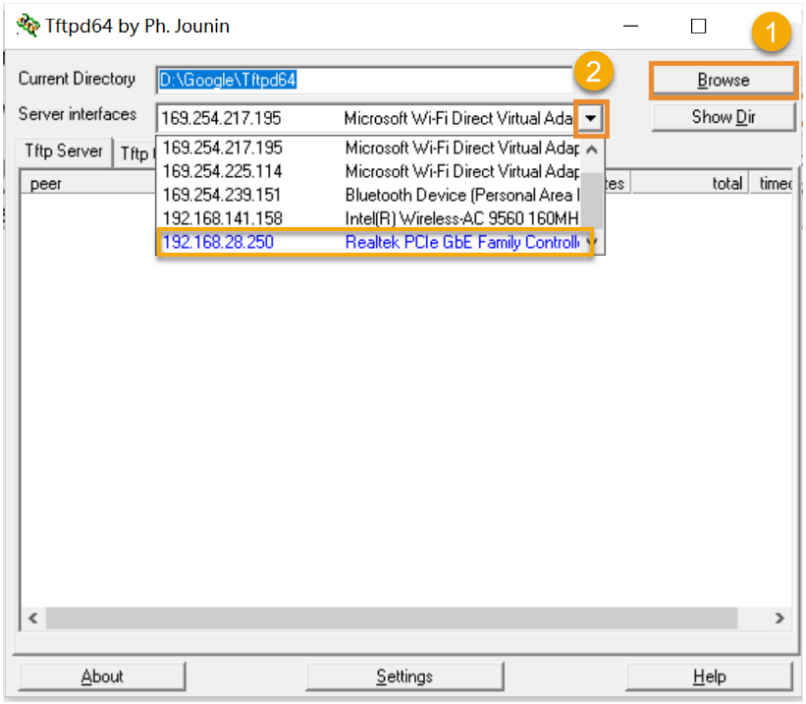
TFTP File Sharing examples

This section gives examples to show how to upload and download files in the specific PBX file holder using Tftpd64.

Configure a TFTP Client

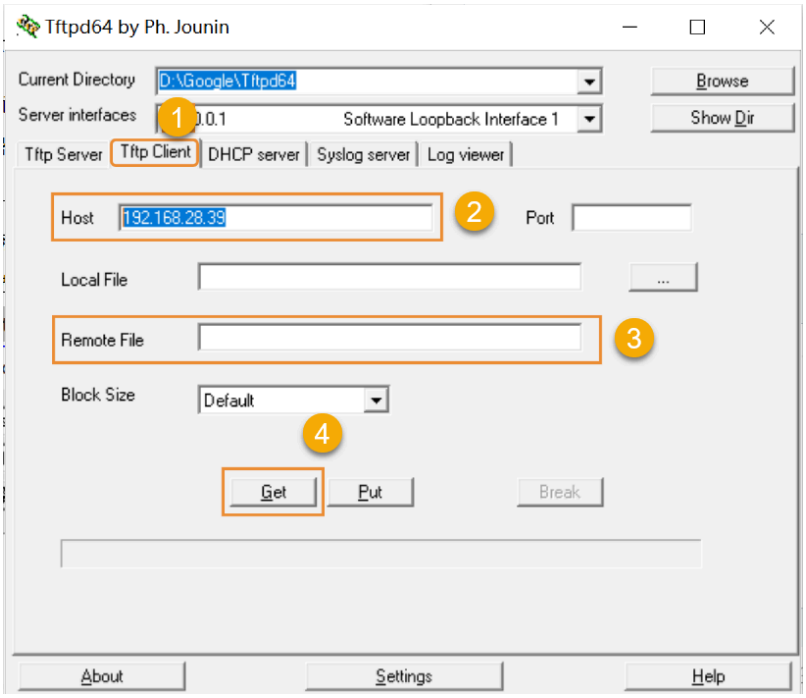
1. Download a Tftpd64 and run the software.
2. On the top of the window, click **Browse** to select the storage path for the shared files.

3. In the **Server interface** drop-down list, select the IP address of your computer.



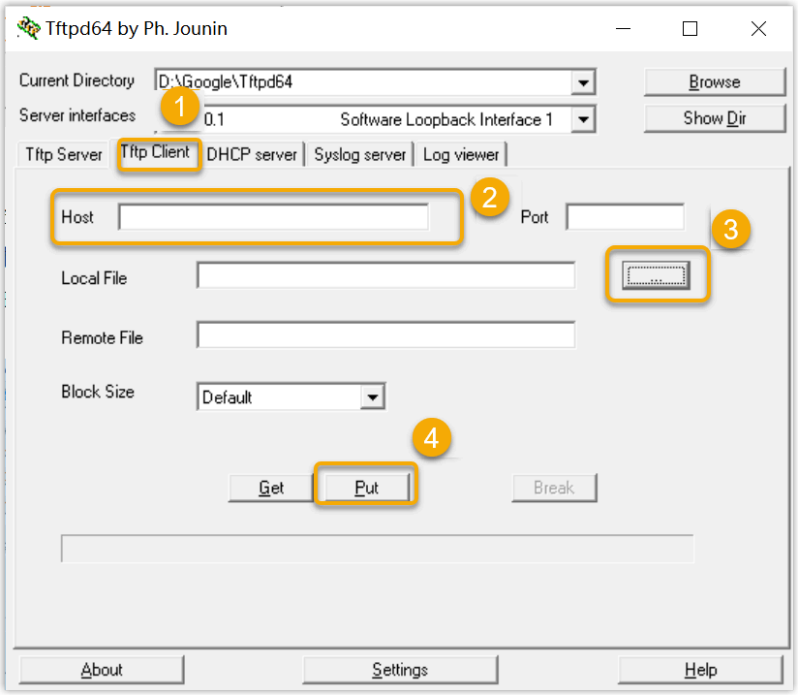
Download a file from PBX

1. In the Tftpd64, go to **Tftp Client** tab.
2. In the **Host** field, enter the IP address of the PBX.
3. In the **Remote File** field, enter the name of the desired file.
4. Click **Get** to download the file.



Upload a file to PBX

1. In the Tftpd64, go to **Tftp Client**.
2. In the **Host** field, enter the IP address of the PBX.
3. Click the ··· beside the **Local File** field to select the desired file.
4. Click **Put** to upload the file to the PBX.



Archive

Yeastar P-Series PBX System Remote Archiving Overview

Yeastar P-Series PBX System allows you to download and archive the system's call recordings and backup files to external servers via FTP, SFTP, Amazon S3, and Google Cloud Storage services, enabling less space occupying and minimized data loss risk on PBX, as well as easier file management on external server.

Requirements and restrictions

Requirements

- **PBX Firmware**: Version 37.18.0.59 or later
- **PBX Plan**: Enterprise Plan

Restrictions

- **Archive server**: 10
- **Archive task**: 200

Archive Files to FTP Server

Yeastar P-Series PBX System supports archiving the system's call recordings and backup files to FTP server, either on a regular interval or at any time you want. This topic describes how to add FTP server as an archive server and schedule tasks to archive the desired files.

Requirements and restrictions

Requirements

- **PBX Firmware**: Version 37.18.0.59 or later
- **PBX Plan**: Enterprise Plan

Restrictions

- **Archive server**: 10
- **Archive task**: 200

Prerequisites

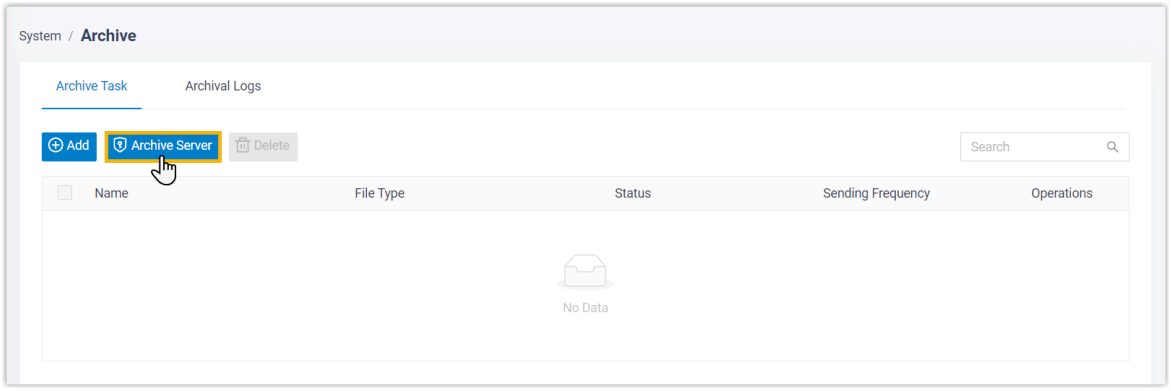
Before you begin, you need to prepare the following resources and collect the required information:

- Prepare an FTP server, and note down its **Domain/IP Address**, **Port**, and **File Transfer Protocol**.
- Prepare an FTP account with both read and write permissions, and note down its **Username** and **Password**.

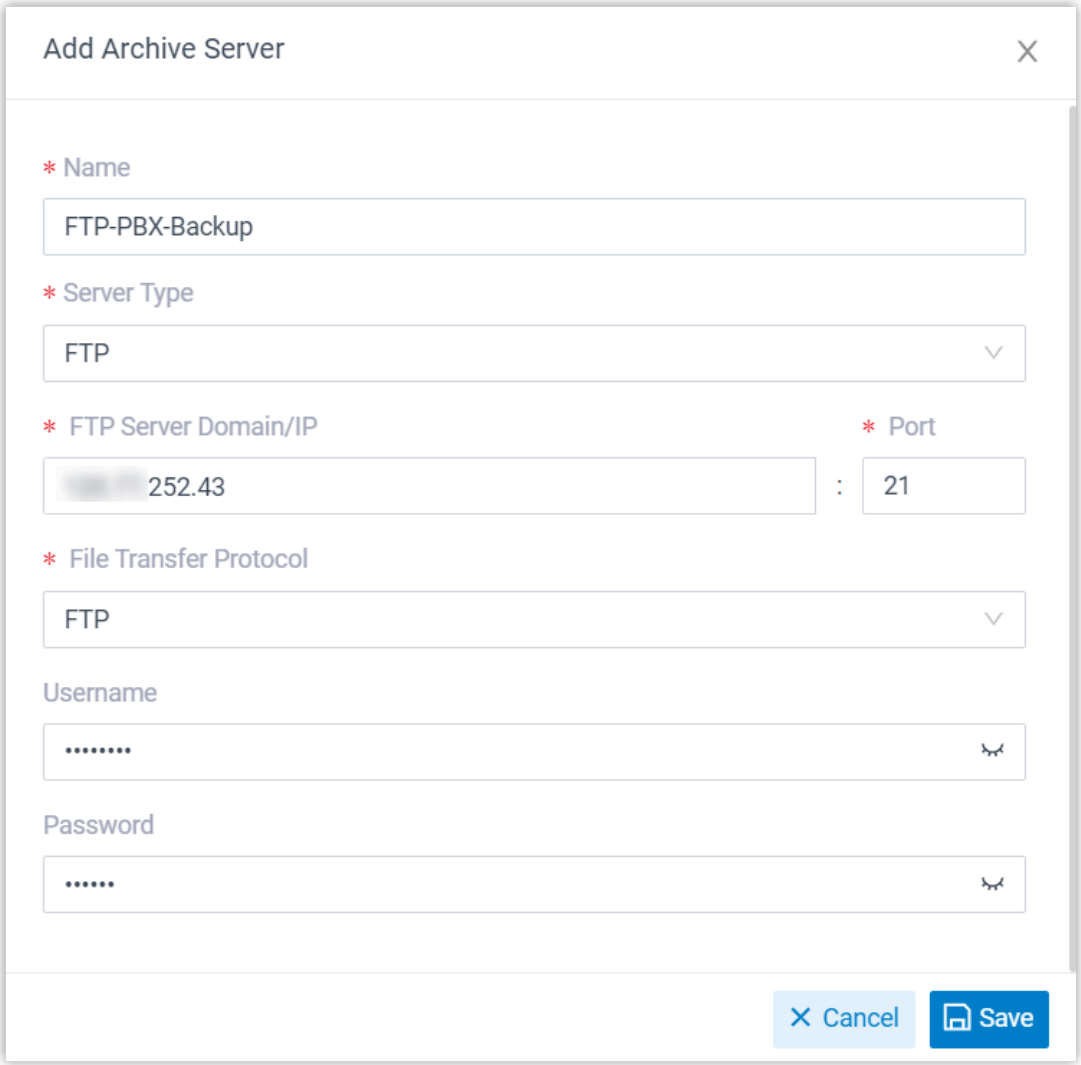
> **Note:**
> If you want old files to be automatically deleted from your FTP server, make sure the FTP account also has file deletion permission.

Step 1. Add FTP server as archive server

1. Log in to PBX web portal, go to **System > Archive**.
2. Under the **Archive Task** tab, click **Archive Server**.



3. Set up FTP server as the archive server.
    a. Click **Add**.
    b. In the pop-up window, complete the following settings.



Setting	Description
Name	Enter a name to help you identify the server.
Server Type	Select **FTP**.
FTP Server Domain/IP	Enter the address of your FTP server.
Port	Enter the port on which your FTP server is running. The default port is 21.
File Transfer Protocol	Select the transfer protocol supported by the FTP server. • **FTP**: Standard File Transfer Protocol. • **FTPES**: FTP over Explicit TLS/SSL. **Note:** ◦ The TLS feature on the FTP server must be enabled, and the encryption policy must be well-configured for security reason. ◦ The supported TLS protocol version is **TLS V1.2**.
Username	Enter the username for the FTP account.
Password	Enter the password associated with the username.

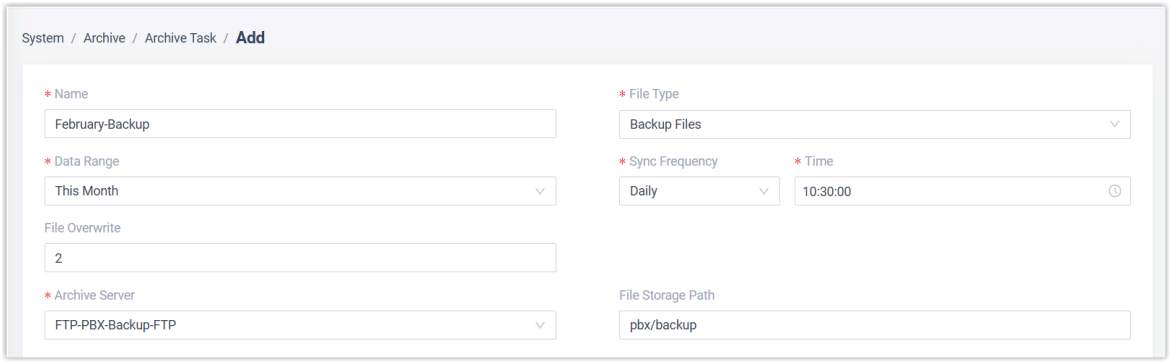
c. Click **Save**.

The FTP server is added as an archive server and displayed on the archive server list.

4. Click ✕ to close the window.

Step 2. Create a task to archive files to FTP server

1. Under **Archive Task** tab, click **Add**.
2. Create a one-time or recurring archive task.



Setting	Description
Name	Enter a name to help you identify the task.
File Type	Select **Recording Files** or **Backup Files** as needed.
Data Range	Specify a time range of the files to be archived. **Note:** You can archive files for up to 31 days at a time.
Sync Frequency	Set how often to archive files to FTP server. **Note:** As large amounts of data will consume PBX's CPU resources, we recommend that you schedule archive tasks during off-peak hours. • **Once**: If you choose the option, the system will archive files immediately after you save the task. • **Daily**: If you choose the option, select a time from the drop-down list. The system will archive files 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 will archive files 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 will archive files on this day and time of the month.
File Overwrite	Optional. Set the maximum number of files to be retained in the FTP server for the archive task. **Note:** • This option is available only when you schedule to archive backup files on a recurring basis.

Setting	Description
	• When it reaches the limit, the system will retain the latest backup files and delete the earlier ones.
Archive Server	Select the FTP server that you have added.
Select Folder/Path	Optional. Set the path to the folder in which you want to store archived files. For example, `pbx/backup/`. **Note:** If you leave this field blank, the files will be stored under the root directory.

3. Click **Save**.

Result

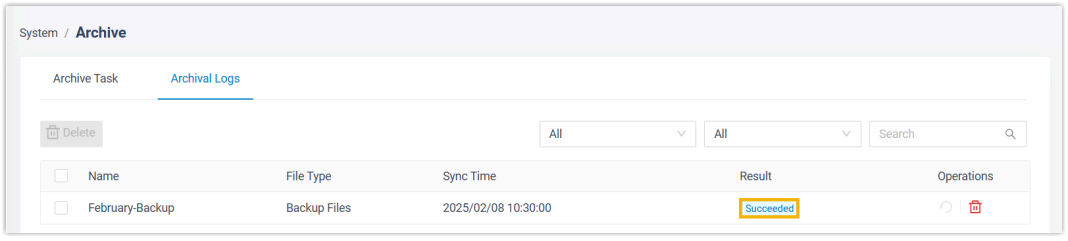
The specified files will be archived to the designated folder in your FTP server immediately or at the scheduled time.

Note:
The system executes only one task at a time to avoid affecting system performance. If there are multiple tasks, they will be queued up one after another.

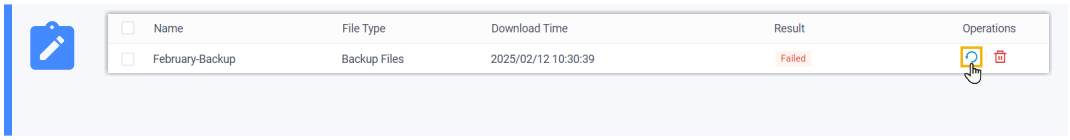
You can check the archive result in the following ways.

Check the archive result on PBX

On PBX web portal, go to **System > Archive > Archival Logs**. If the **Result** column of the task shows **Succeeded**, it indicates that the specified files have been successfully archived to the FTP server.

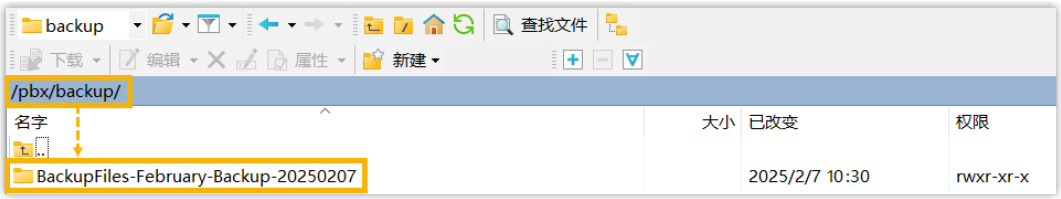


Note:
If the task is failed, the **Failed to Archive File(s)** event will be triggered; You can click to retry the task.



Check the archive result on FTP server

Go to the designated folder in FTP server. If the specified files appear in the list, it indicates that the archive is successful.



Archive Files to SFTP Server

Yeastar P-Series PBX System supports archiving the system's call recordings and backup files to SFTP server, either on a regular interval or at any time you want. This topic describes how to add SFTP server as an archive server and schedule tasks to archive the desired files.

Requirements and restrictions

Requirements

- **PBX Firmware**: Version 37.18.0.59 or later
- **PBX Plan**: Enterprise Plan

Restrictions

- **Archive server**: 10
- **Archive task**: 200

Prerequisites

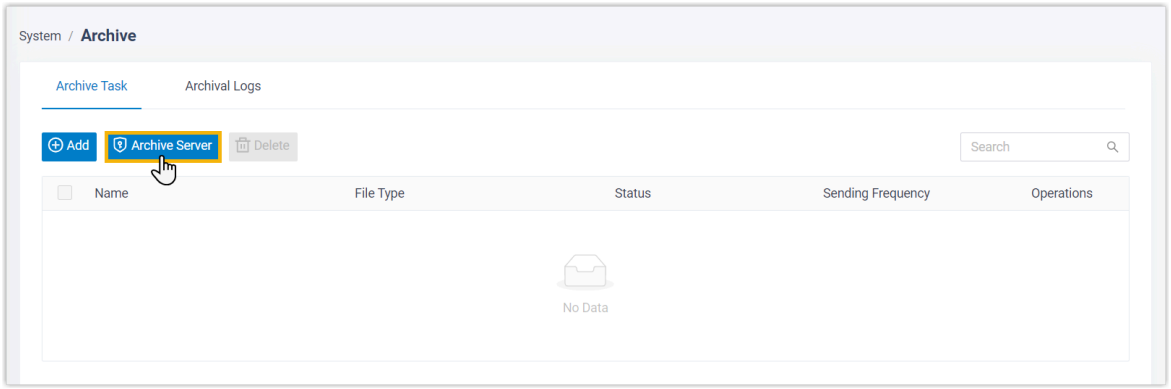
Before you begin, you need to prepare the following resources and collect the required information:

- Prepare an SFTP server and note down its **Domain/IP Address** and **Port**.
- Prepare an SFTP account with both read and write permissions, and note down its **Username** and **Password/Private Key**.

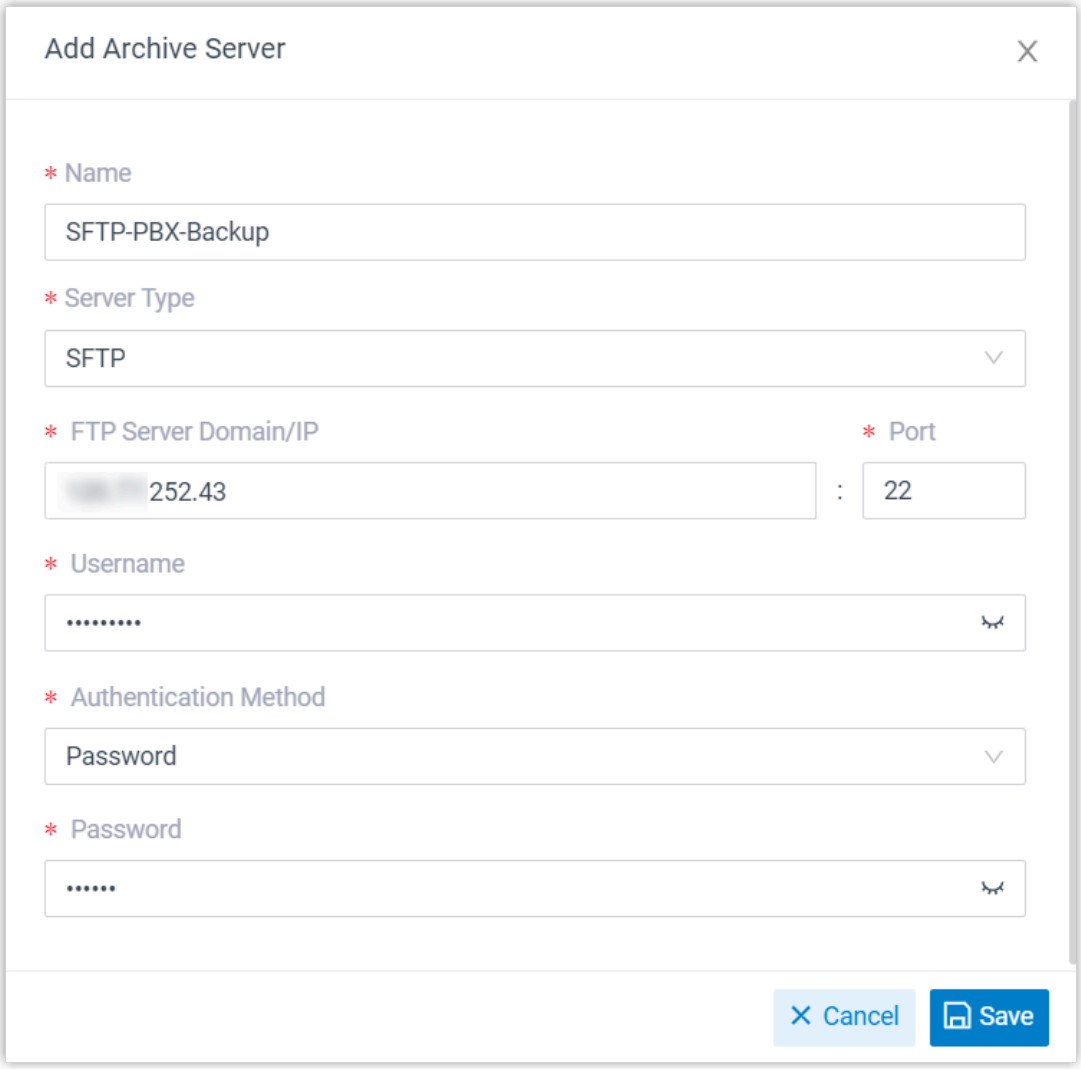
> **Note:**
> If you want old files to be automatically deleted from your SFTP server, make sure the SFTP account also has file deletion permission.

Step 1. Add SFTP server as archive server

1. Log in to PBX web portal, go to **System > Archive**.
2. Under the **Archive Task** tab, click **Archive Server**.



3. Set up SFTP server as the archive server.
    a. Click **Add**.
    b. In the pop-up window, complete the following settings.



Setting	Description
Name	Enter a name to help you identify the server.
Server Type	Select **SFTP**.
FTP Server Domain/IP	Enter the address of your SFTP server.
Port	Enter the port on which your SFTP server is running. The default port is 22.
Username	Enter the username for the SFTP account.
Authentication Method	Select an authentication method, then enter the credential.

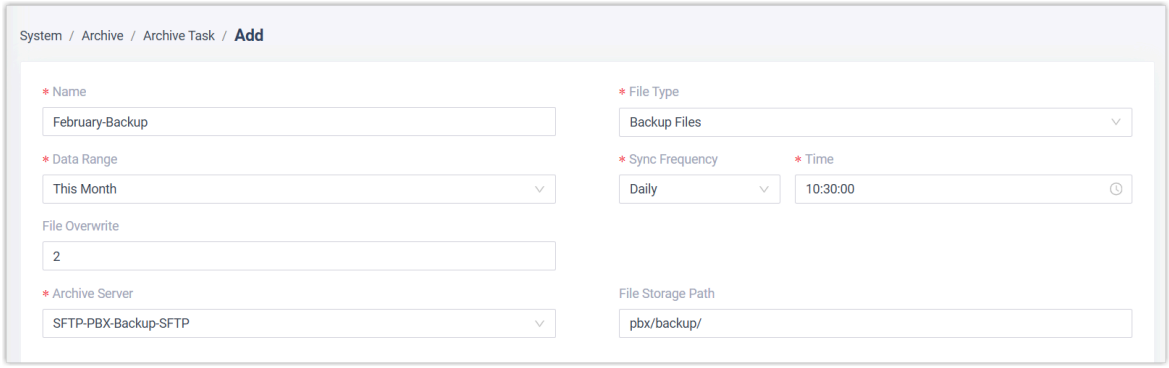
c. Click **Save**.

SFTP server is added as an archive server and displayed on the archive server list.

4. Click ✕ to close the window.

Step 2. Create a task to archive files to SFTP server

1. Under **Archive Task** tab, click **Add**.
2. Create a one-time or recurring archive task.



Setting	Description
Name	Enter a name to help you identify the task.
File Type	Select **Recording Files** or **Backup Files** as needed.
Data Range	Specify a time range of the files to be archived. **Note:** You can archive files for up to 31 days at a time.
Sync Frequency	Set how often to archive files to SFTP server. **Note:** As large amounts of data will consume PBX's CPU resources, we recommend that you schedule archive tasks during off-peak hours. • **Once**: If you choose the option, the system will archive files immediately after you save the task. • **Daily**: If you choose the option, select a time from the drop-down list. The system will archive files 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 will archive files at this time of the week.

Setting	Description
	• **Monthly**: If you choose the option, choose a day and select a time from the drop-down list. The system will archive files on this day and time of the month.
File Overwrite	Optional. Set the maximum number of files to be retained in the SFTP server for the archive task. **Note:** • This option is available only when you schedule to archive backup files on a recurring basis. • When it reaches the limit, the system will retain the latest backup files and delete the earlier ones.
Archive Server	Select the SFTP server that you have added.
Select Folder/Path	Optional. Set the path to the folder in which you want to store archived files. For example, `pbx/backup/`. **Note:** If you leave this field blank, the files will be stored under the root directory.

3. Click **Save**.

Result

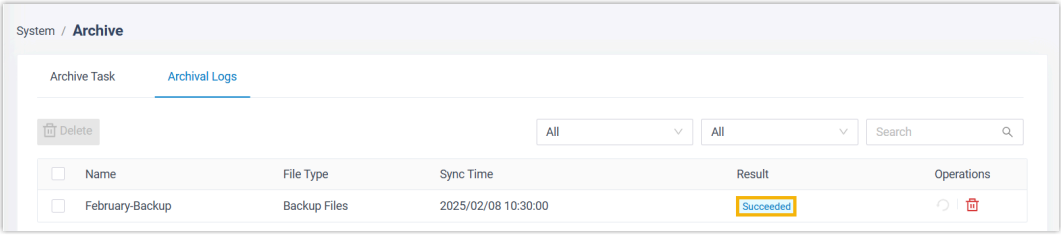
The specified files will be archived to the designated folder in your SFTP server immediately or at the scheduled time.

Note:
The system executes only one task at a time to avoid affecting system performance. If there are multiple tasks, they will be queued up one after another.

You can check the archive result in the following ways.

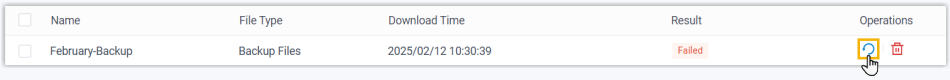
Check the archive result on PBX

On PBX web portal, go to **System > Archive > Archival Logs**. If the **Result** column of the task shows **Succeeded**, it indicates that the specified files have been successfully archived to SFTP server.



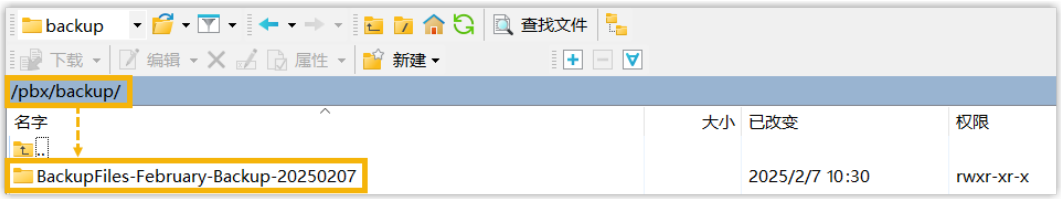
Note:

If the task is failed, the **Failed to Archive File(s)** event will be triggered; You can click to retry the task.



Check the archive result on SFTP server

Go to the designated folder in SFTP server. If the specified files appear in the list, it indicates that the archive is successful.



Archive Files to Amazon S3

Yeastar P-Series PBX System supports archiving the system's call recordings and backup files to Amazon S3, either on a regular interval or at any time you want. This topic describes how to add Amazon S3 bucket as an archive server and schedule tasks to archive the desired files.

Requirements and restrictions

Requirements

- **PBX Firmware**: Version 37.18.0.59 or later
- **PBX Plan**: Enterprise Plan

Restrictions

- **Archive server**: 10
- **Archive task**: 200

Introduction

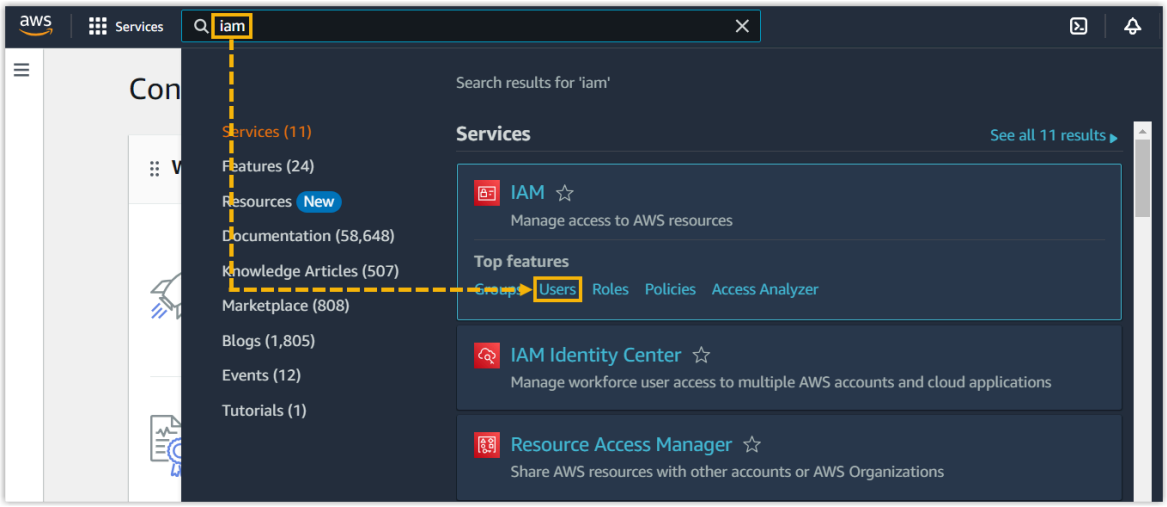
To archive PBX's call recordings and backup files to a specific bucket in Amazon S3, you need to complete the followings:

1. Prepare an eligible account and bucket on AWS.
   - An **IAM User** account that meets the requirements listed below:
     - Full access to Amazon S3 resources to archive PBX files
     - An access key pair (including an access key ID and a secret access key) to authenticate file archiving requests from PBX
   - An **S3 bucket** to store archived PBX files
2. Set up archive server and task on PBX.
   - Add the Amazon S3 bucket as an archive server
   - Create tasks to archive PBX files to Amazon S3

When it is time to execute the archive task, PBX will use the access key pair of the IAM user to send file archiving requests to Amazon S3. If the requests are considered authentic, the specified files will be archived to the designated bucket in Amazon S3.

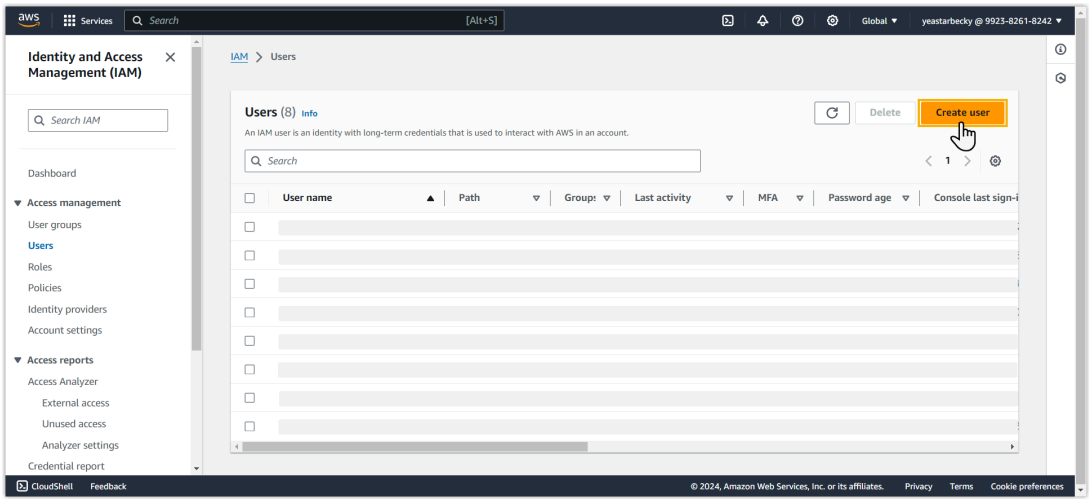
Step 1. Create an IAM user with full access to Amazon S3 bucket on AWS

1. Log in to AWS Management Console.
2. At the top of the console, search for IAM service and select **Users**.

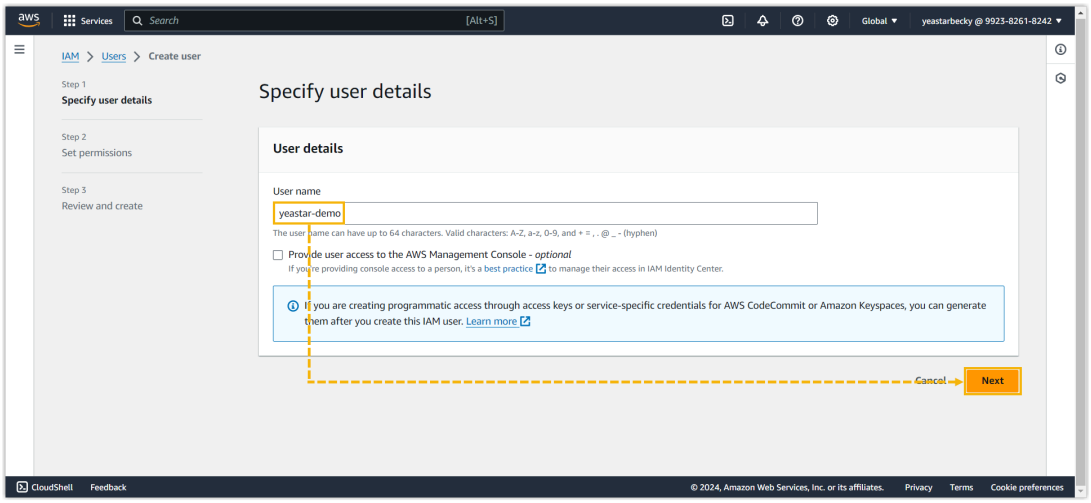


You are redirected to the IAM users page.

3. Create an IAM user and grant the user full access to Amazon S3 bucket.
   a. At the top-right corner, click **Create user**.

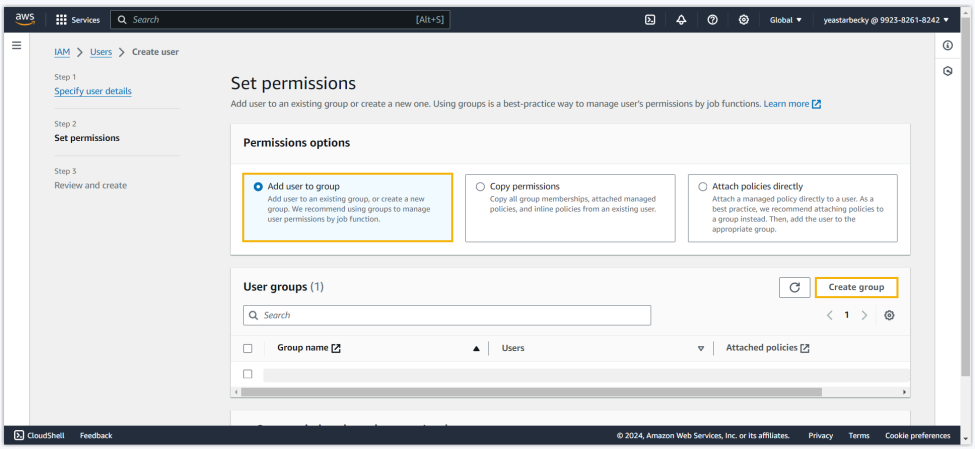


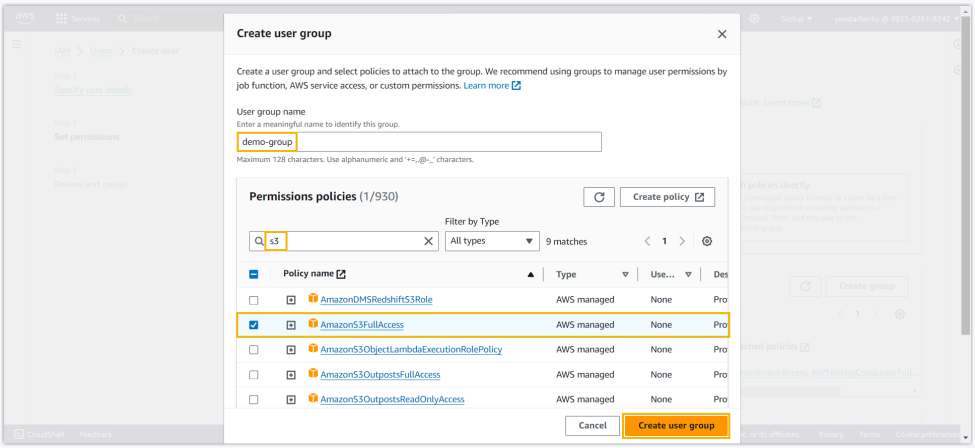
   b. On the **Specify user details** page, enter a name in the **User name** field to help you identify the IAM user, then click **Next**.

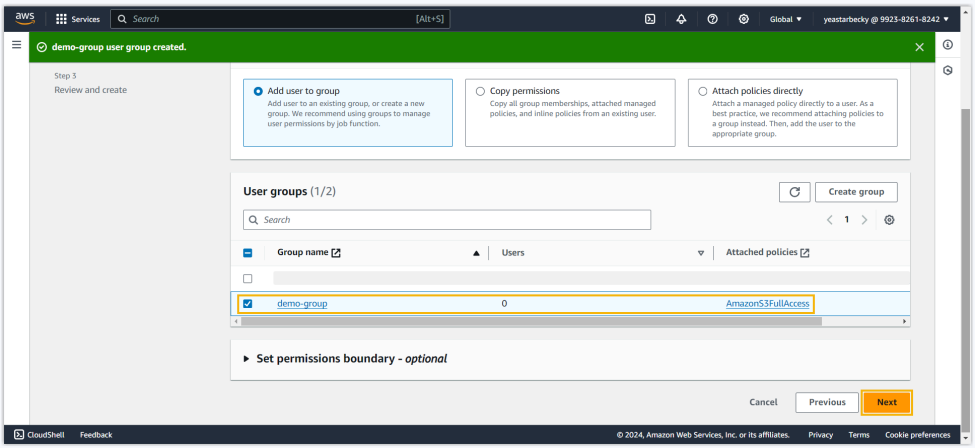


   c. On the **Set permissions** page, grant the user full access to Amazon S3 buckets, then click **Next**.

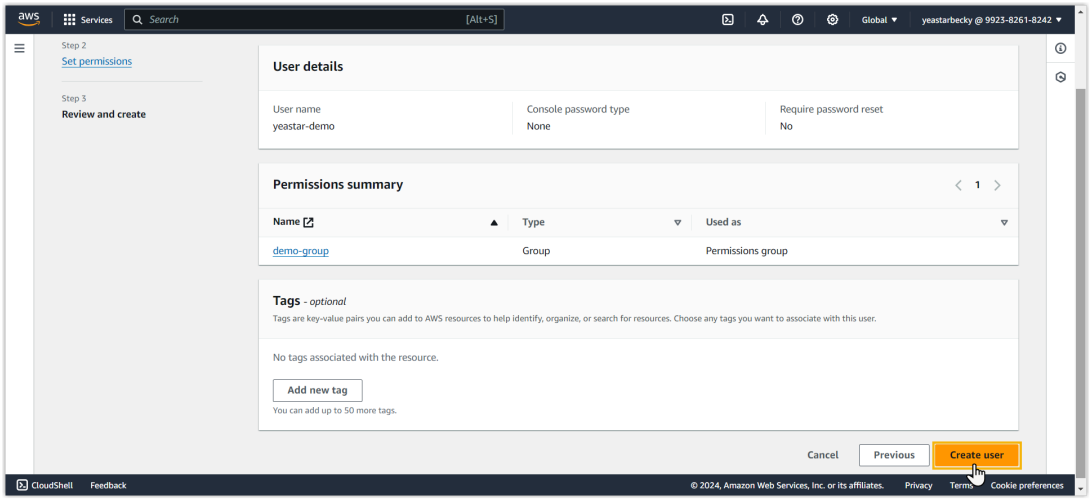
> **Note:**
> You can grant permission to the user by adding the user to an existing group, creating a new group, or attaching permission policy directly to the user.
>
> In this example, we create a new group with full Amazon S3 access permission and add the user to the group, as the following figure shows.





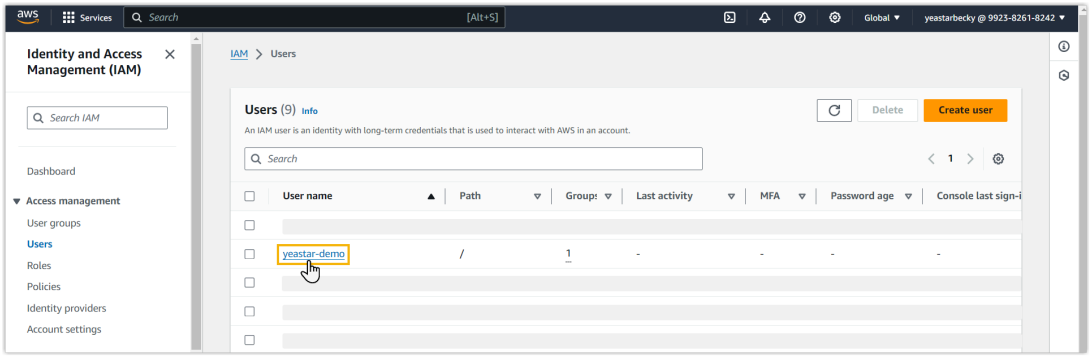


d. On the **Review and create** page, click **Create user**.

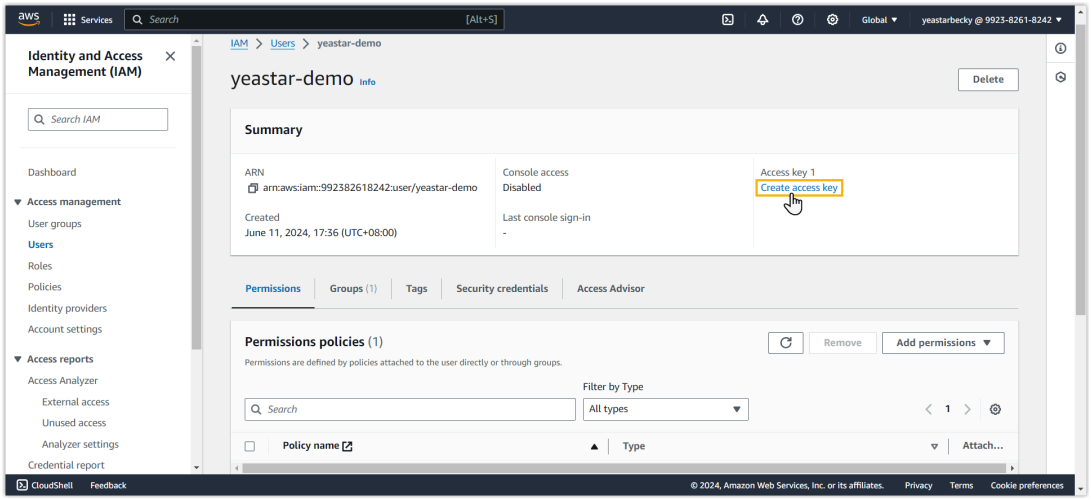


The IAM user with full access to Amazon S3 bucket is created and displayed on the users list.

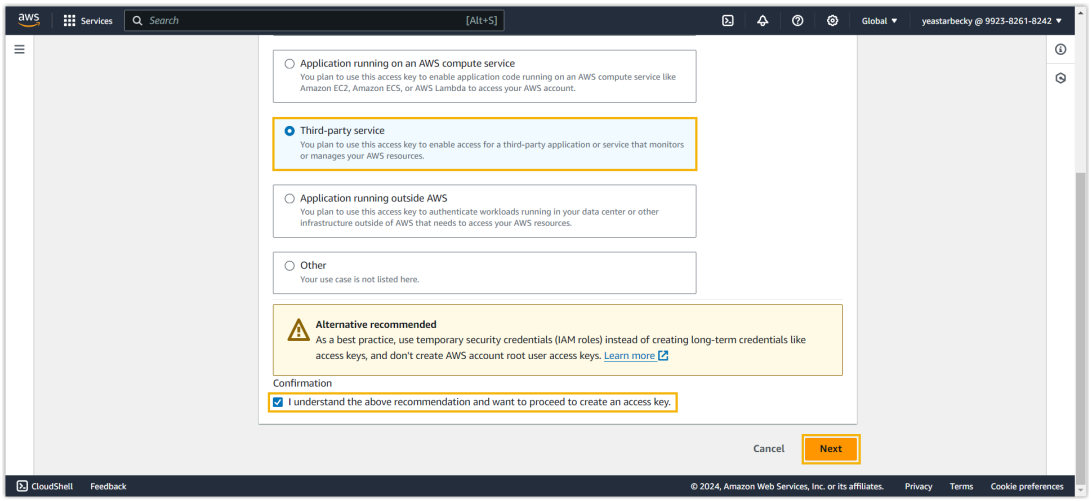
4. Create an access key for the IAM user.
   a. On the users list, click on the newly created IAM user to enter the details page.



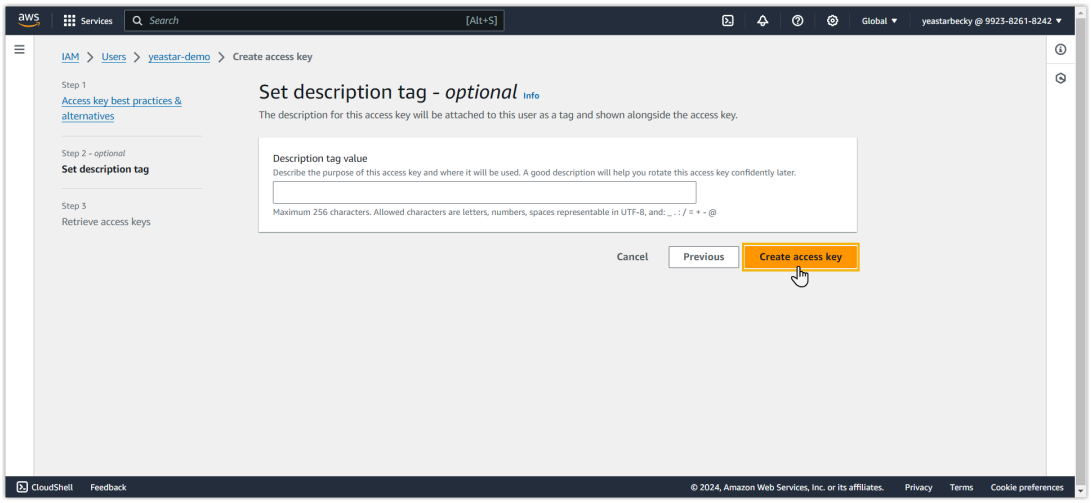
   b. In the **Summary** section, click **Create access key**.



c. On the **Access key best practices & alternatives** page, select **Third-party service**, confirm your operation, then click **Next**.

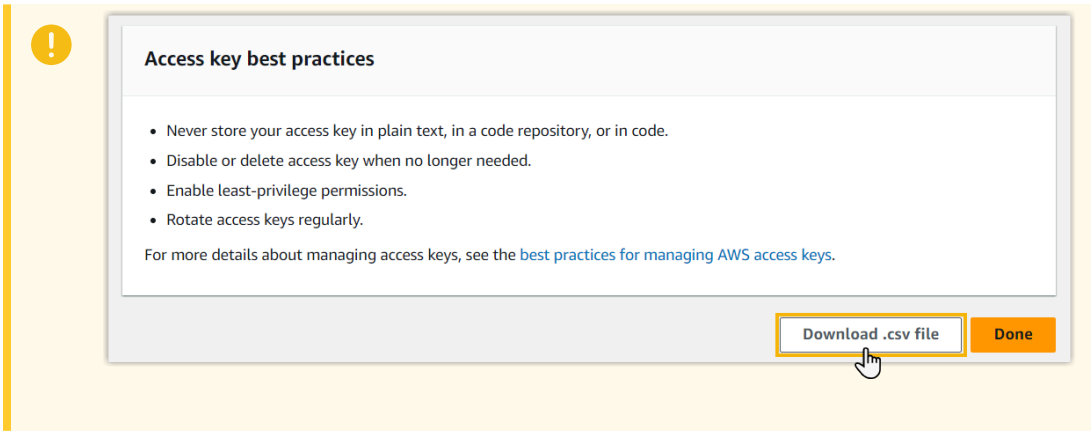


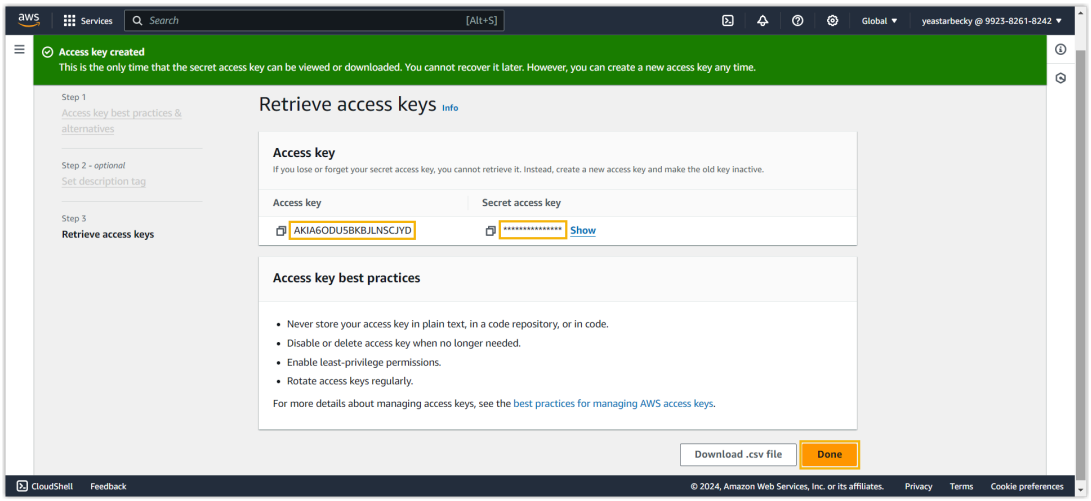
d. On the **Set description tag - optional** page, enter a description for the access key as needed, then click **Create access key**.



e. In the **Retrieve access keys** page, copy and note down the values of **Access key** and **Secret access key**, then click **Done**.

> **Important:**
> For **Secret access key**, the value is shown only ONCE, so make sure that you save the credential in a secure location before clicking **Done** to close the window. We recommend that you click **Download .csv file** to save the credential file to your computer.

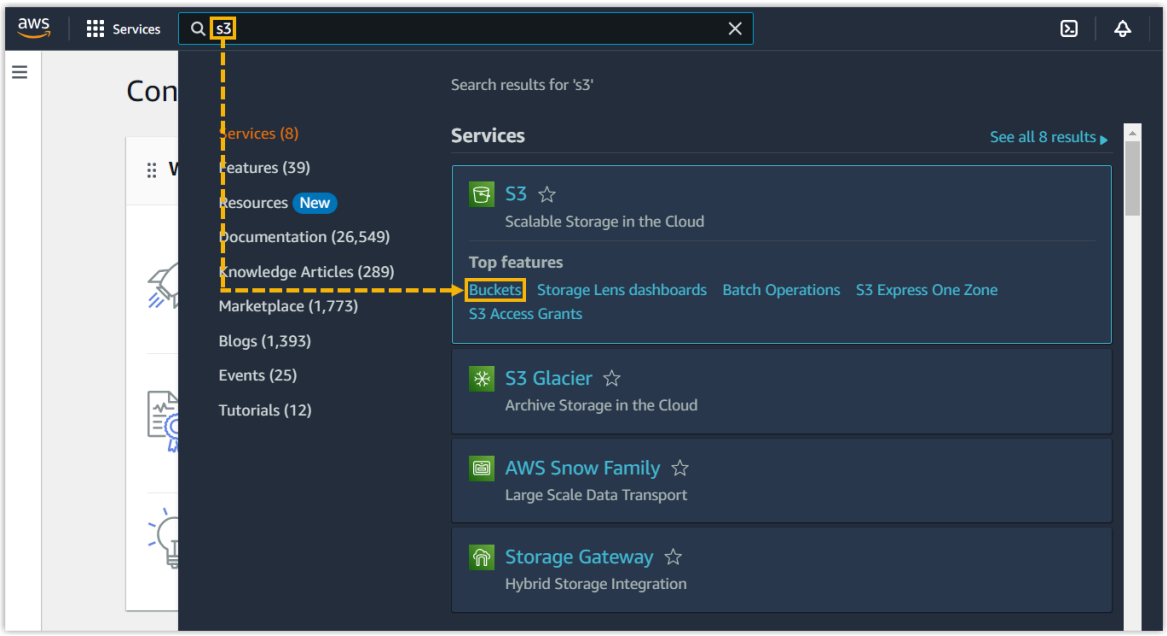




The access key is created and displayed on the access key list.

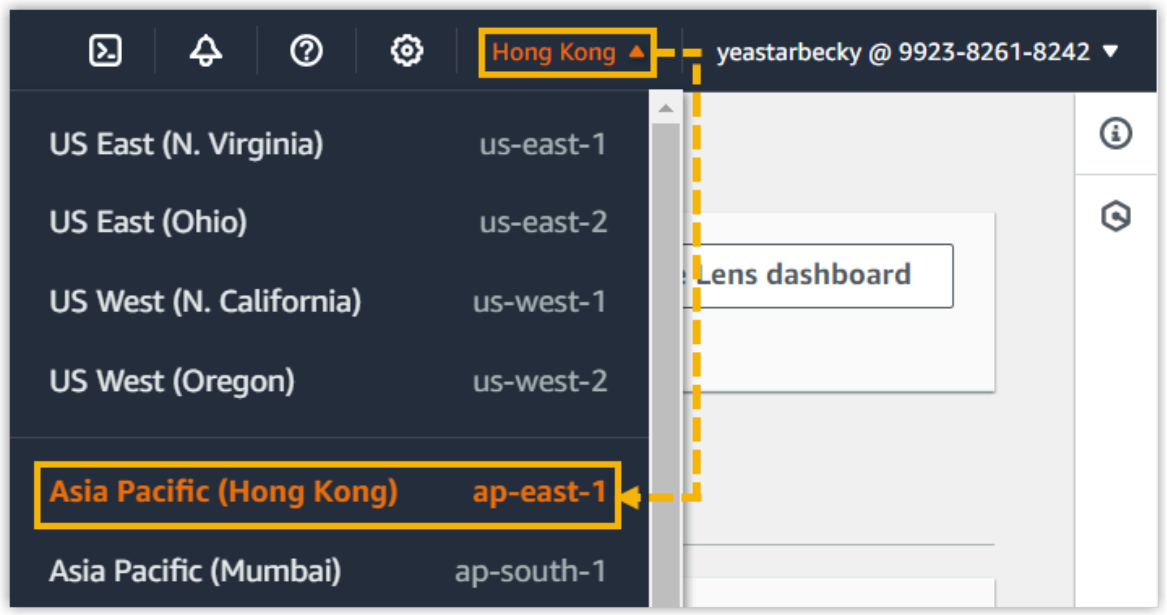
Step 2. Create an Amazon S3 bucket on AWS

1. On AWS Management Console, search for S3 service in the top-left search bar, then select **Buckets**.

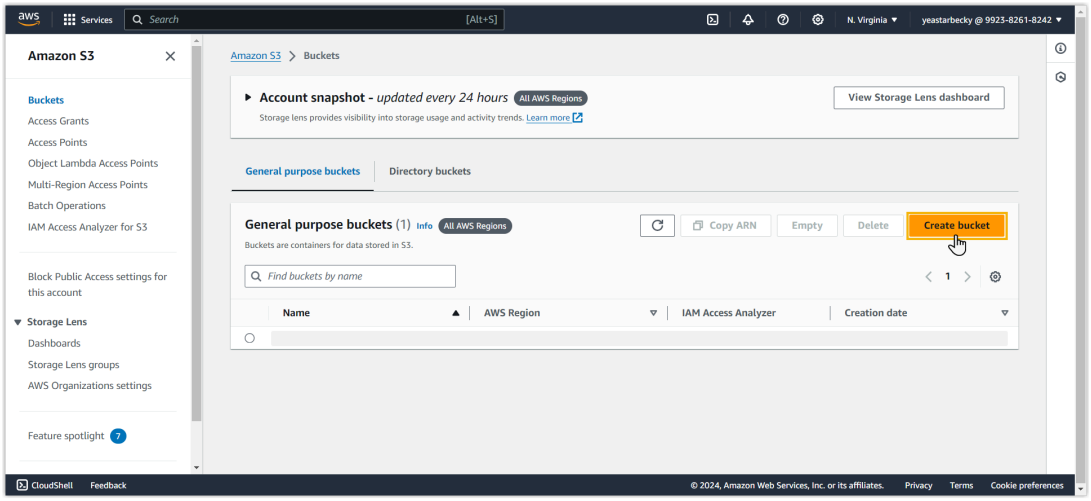


2. At the top-right corner, select the region in which you want to create an S3 bucket.

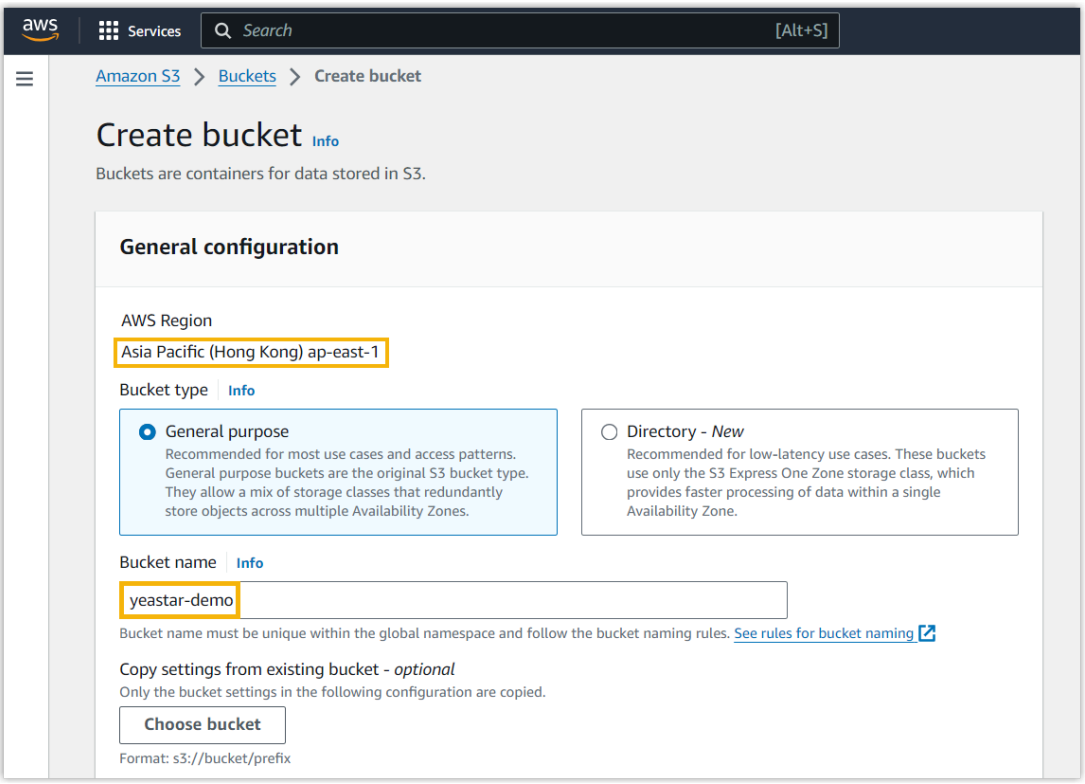
> **Note:**
> To minimize latency and costs and address regulatory requirements, choose a region that is closest to your PBX server.



3. Create an S3 bucket.
    a. On the right of the page, click **Create bucket**.



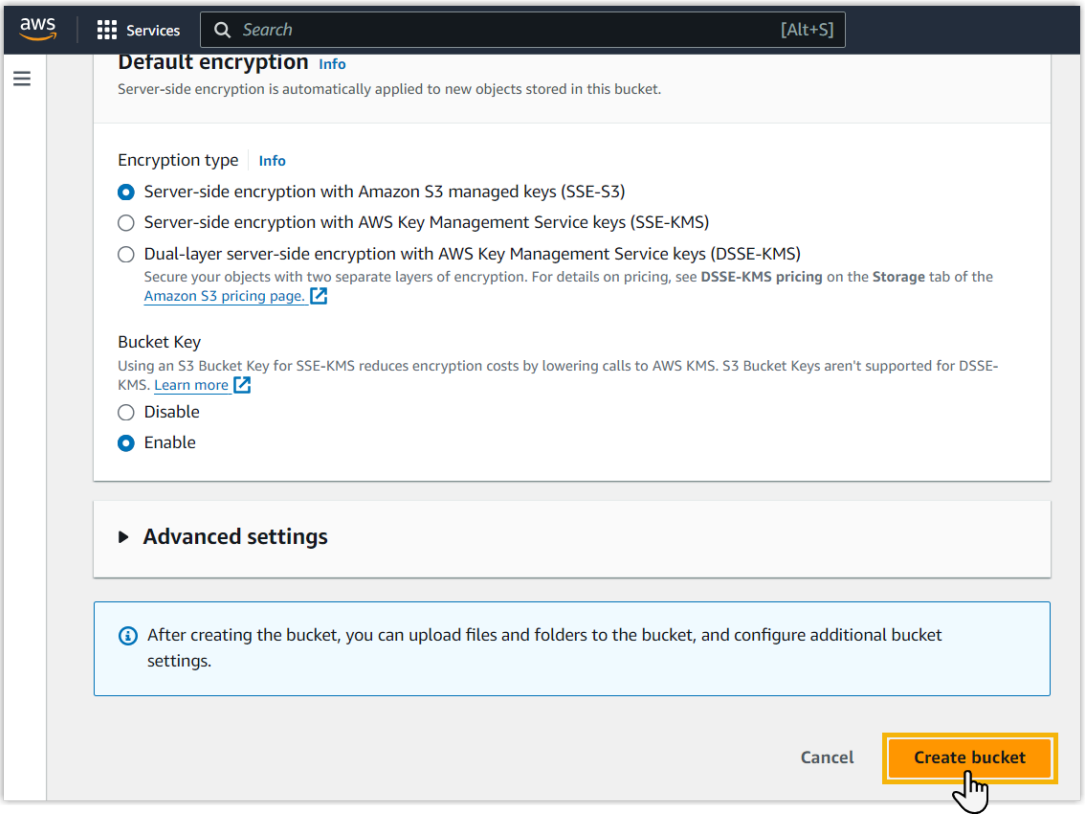
b. Check the region where the bucket will be created and specify a name for the bucket.



- **AWS Region**: Automatically show the region that you have selected.
- **Bucket name**: Enter a name to help you identify the bucket.

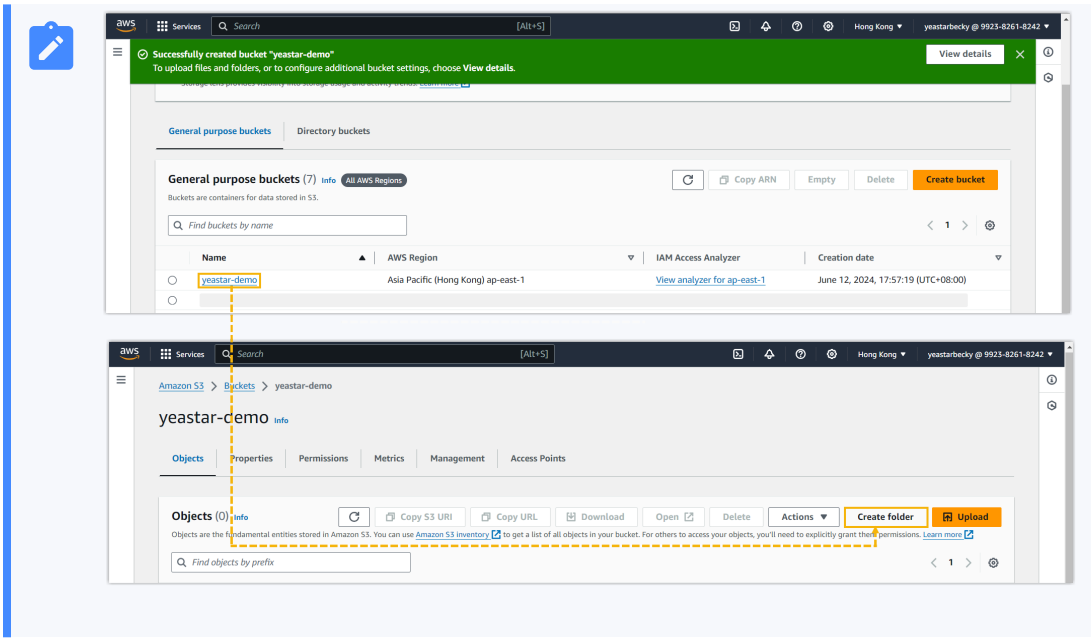
c. Configure other settings according to your needs.

d. At the bottom of the page, click **Create bucket**.



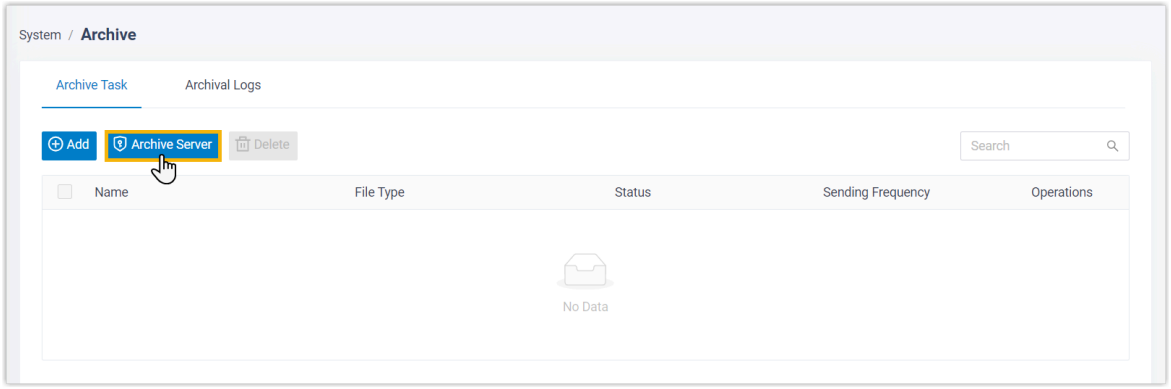
The S3 bucket is created and displayed on the buckets list.

Note:
If you want to group the archived PBX files in Amazon S3, you can create folders in the bucket. In this way, you can specify PBX files to be archived to the designated folder in the follow-up settings.

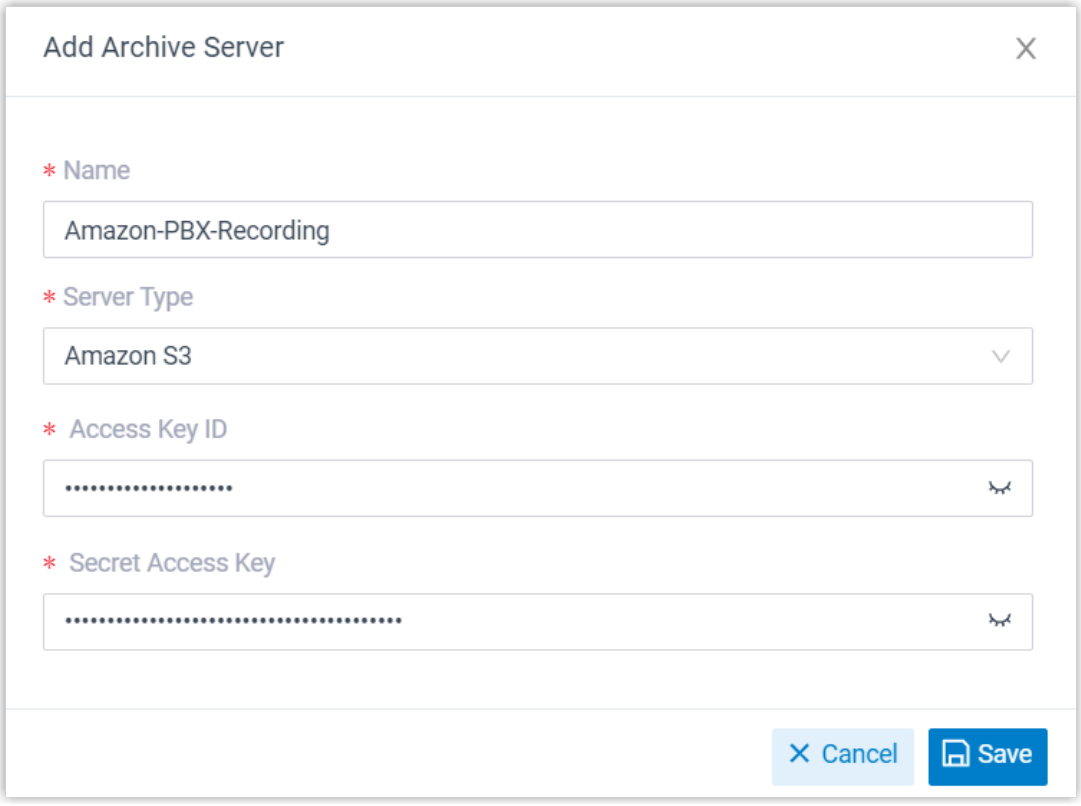


Step 3. Add Amazon S3 bucket as archive server on PBX

1. Log in to PBX web portal, go to **System > Archive**.
2. Under the **Archive Task** tab, click **Archive Server**.



3. Set up Amazon S3 bucket as an archive server.
    a. Click **Add**.
    b. In the pop-up window, complete the following settings.



Setting	Description
Name	Enter a name to help you identify the server.
Server Type	Select **Amazon S3**.
Access Key ID	Enter the access key that you have obtained from AWS.
Secret Access Key	Enter the secret access key that you have obtained from AWS.

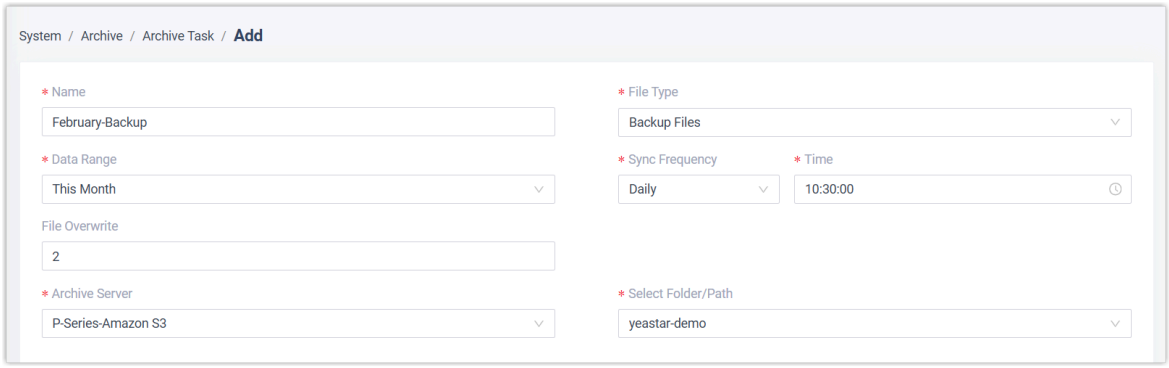
c. Click **Save**.

The Amazon S3 bucket is added as an archive server and displayed on the archive server list.

4. Click ✕ to close the window.

Step 4. Create a task to archive files to Amazon S3 on PBX

1. Under **Archive Task** tab, click **Add**.
2. Create a one-time or recurring archive task.



Setting	Description
Name	Enter a name to help you identify the task.
File Type	Select **Recording Files** or **Backup Files** as needed.
Data Range	Specify a time range of the files to be archived. **Note:** You can archive files for up to 31 days at a time.
Sync Frequency	Set how often to archive files to Amazon S3. **Note:** As large amounts of data will consume PBX's CPU resources, we recommend that you schedule archive tasks during off-peak hours. • **Once**: If you choose the option, the system will archive files immediately after you save the task. • **Daily**: If you choose the option, select a time from the drop-down list. The system will archive files 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 will archive files 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 will archive files on this day and time of the month.
File Overwrite	Optional. Set the maximum number of files to be retained in the Amazon S3 bucket for the archive task. **Note:** • This option is available only when you schedule to archive backup files on a recurring basis.

Setting	Description
	• When it reaches the limit, the system will retain the latest backup files and delete the earlier ones.
Archive Server	Select the Amazon S3 bucket that you have added.
Select Folder/Path	Select the bucket or the folder in which you want to store archived files.

3. Click **Save**.

Result

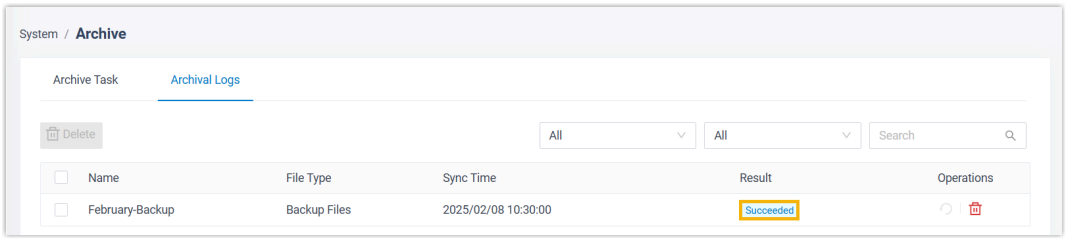
The specified files will be archived to the designated bucket or folder in Amazon S3 immediately or at the scheduled time.

Note:
The system executes only one task at a time to avoid affecting system performance. If there are multiple tasks, they will be queued up one after another.

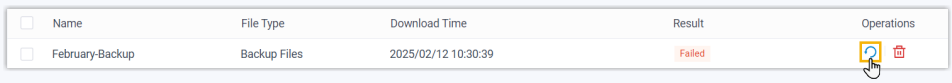
You can check the archive result in the following ways.

Check the archive result on PBX

On PBX web portal, go to **System > Archive > Archival Logs**. If the **Result** column of the task shows **Succeeded**, it indicates that the specified files have been successfully archived to Amazon S3.

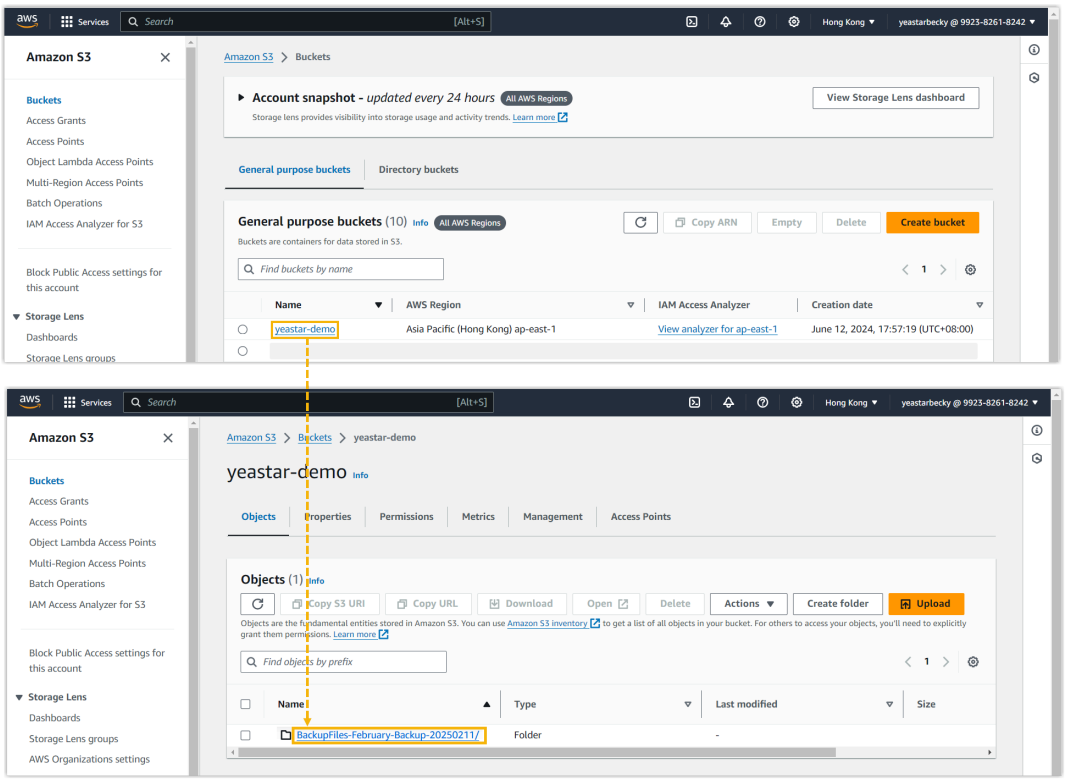


Note:
If the task is failed, the **Failed to Archive File(s)** event will be triggered; You can click to retry the task.



Check the archive result on AWS

On AWS Management Console, go to the created S3 bucket. If the specified files appear in the list, it indicates that the archive is successful.



Archive Files to Google Cloud Storage

Yeastar P-Series PBX System supports archiving the system's call recordings and backup files to Google Cloud Storage, either on a regular interval or at any time you want. This topic describes how to add Google Cloud Storage bucket as an archive server and schedule tasks to archive the desired files.

Requirements and restrictions

Requirements

- **PBX Firmware**: Version 37.18.0.59 or later
- **PBX Plan**: Enterprise Plan

Restrictions

- **Archive server**: 10
- **Archive task**: 200

Introduction

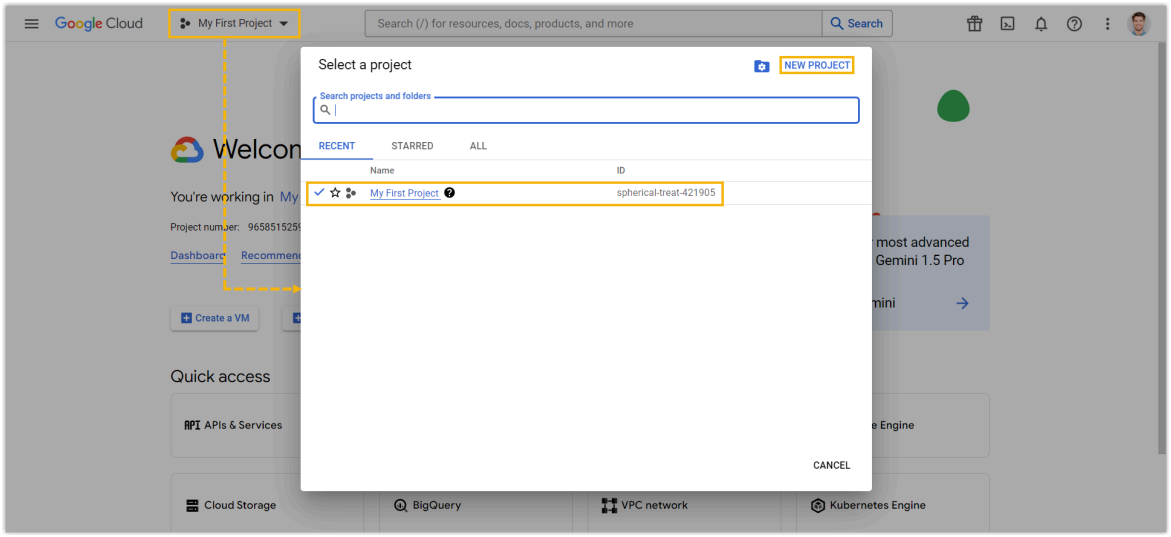
To archive PBX's call recordings and backup files to a specific bucket in Google Cloud Storage, you need to complete the followings:

1. Prepare an eligible account and bucket on Google Cloud.
   - A **service account** that meets the requirements listed below:
     - Full access to Google Cloud Storage resources to archive PBX files
     - An access key to authenticate file archiving requests from PBX
   - A **bucket** to store archived PBX files
2. Set up archive server and task on PBX.
   - Add the Google Cloud Storage bucket as an archive server
   - Create tasks to archive PBX files to Google Cloud Storage

When it is time to execute the archive task, PBX will use the access key of the service account to send file archiving requests to Google Cloud Storage. If the requests are considered authentic, the specified files will be archived to the designated bucket in Google Cloud Storage.

Step 1. Create a service account on Google Cloud

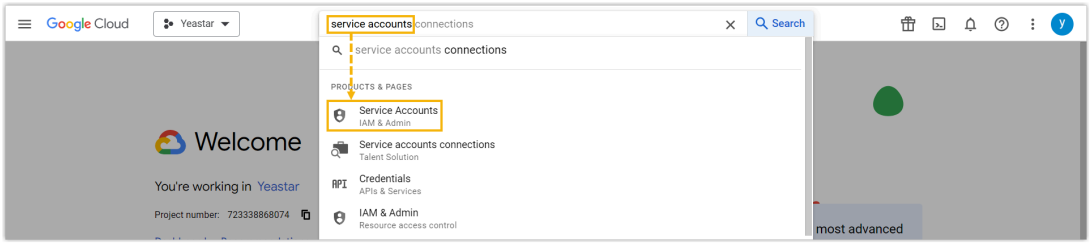
1. Log in to Google Cloud Console.
2. On the project selector page, select or create a Google Cloud project.



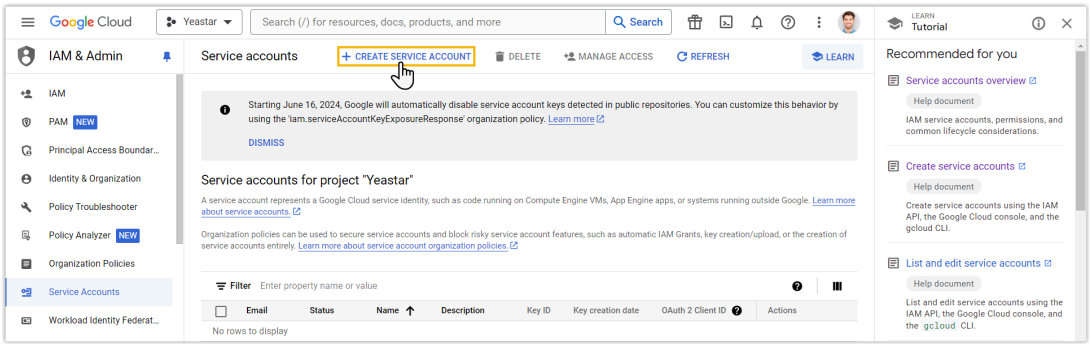
In this example, we create a new project "Yeastar".

3. Create a service account.

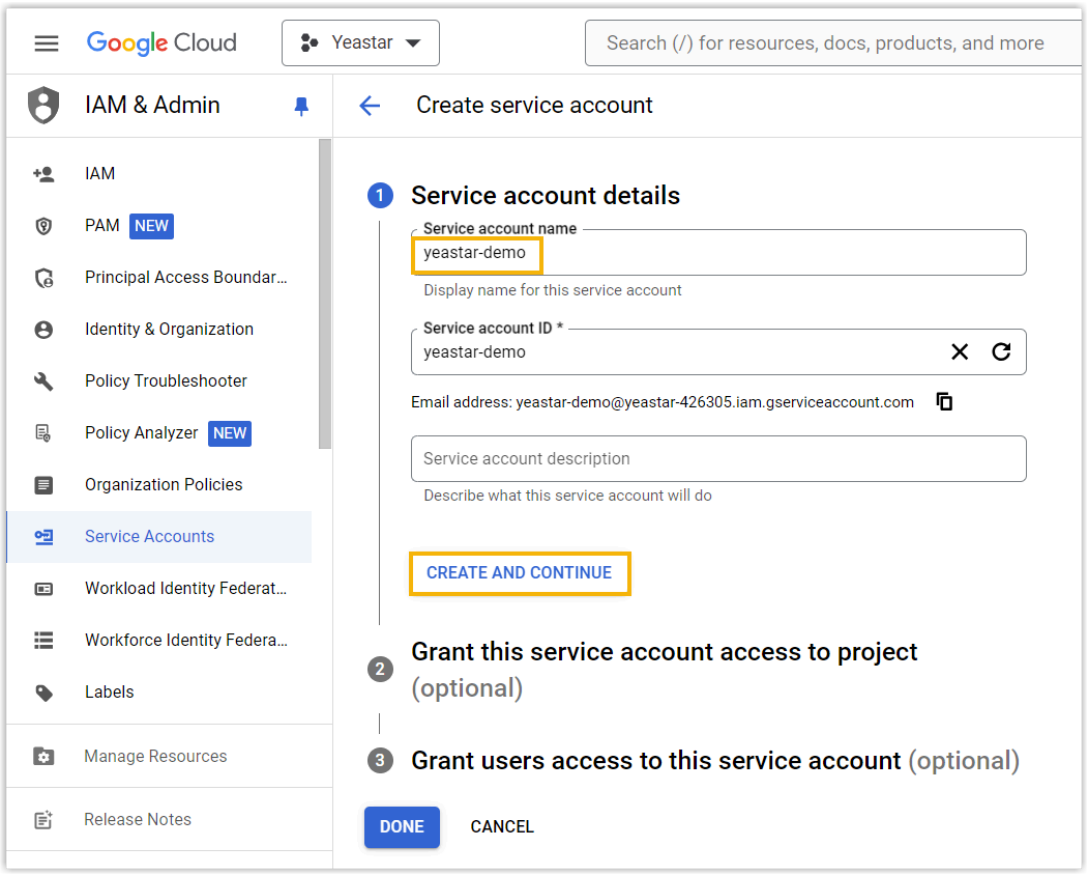
   a. In the top search bar, search for and select **Service Accounts**.



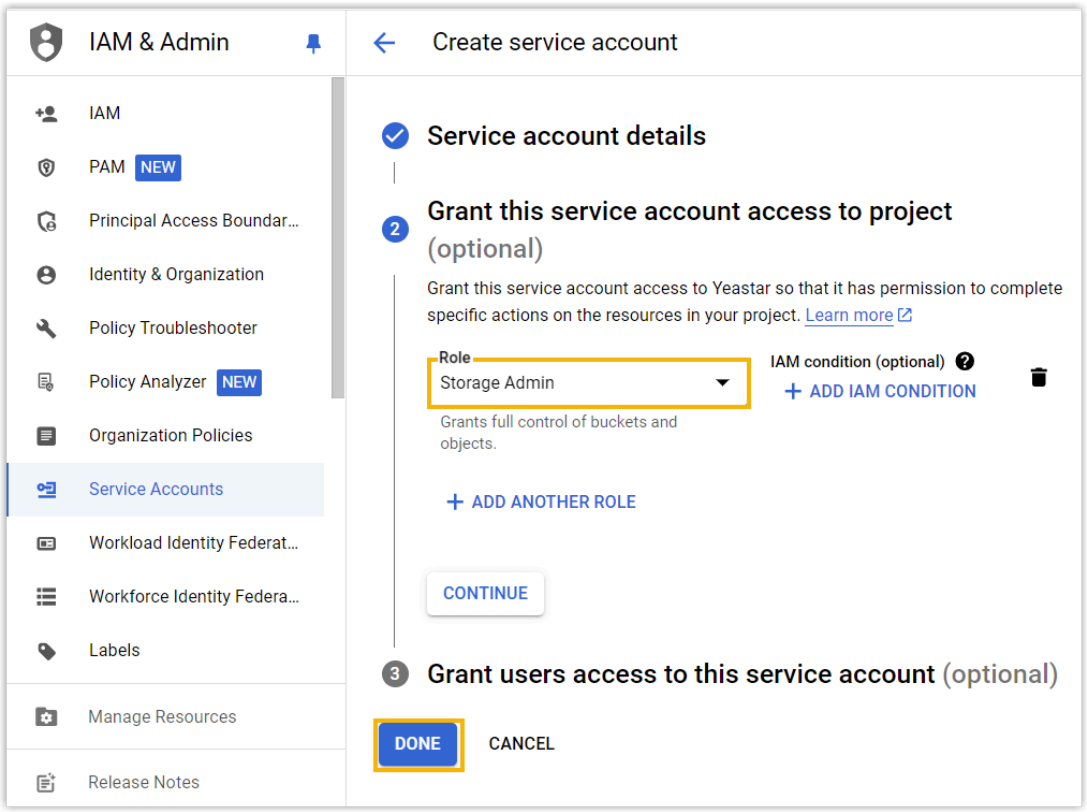
   b. In the top pane, click **CREATE SERVICE ACCOUNT**.



   c. In the **Service account details** section, enter a name in the **Service account name** field to help you identify the account, then click **CREATE AND CONTINUE**.



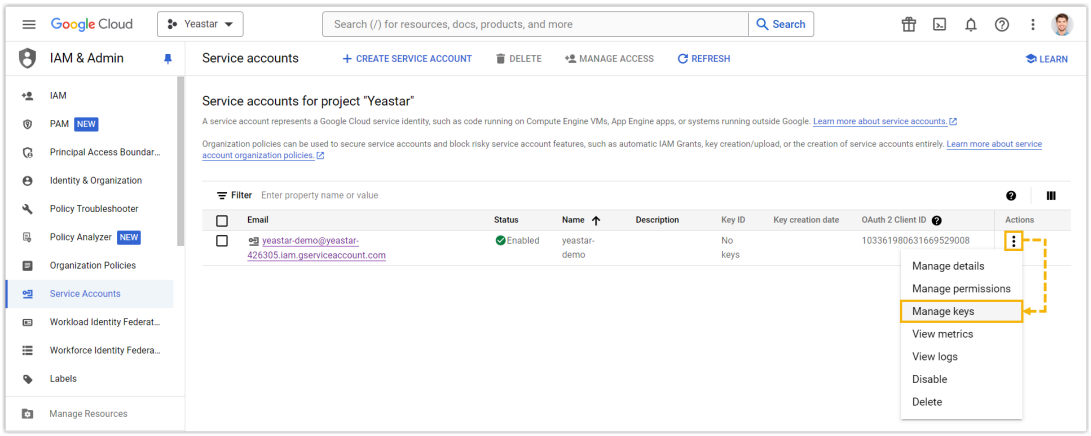
d. In the **Grant this service account access to project (optional)** section, search and select **Storage Admin** from the **Role** drop-down list, then click **DONE**.



The service account is created and displayed on the service accounts list.

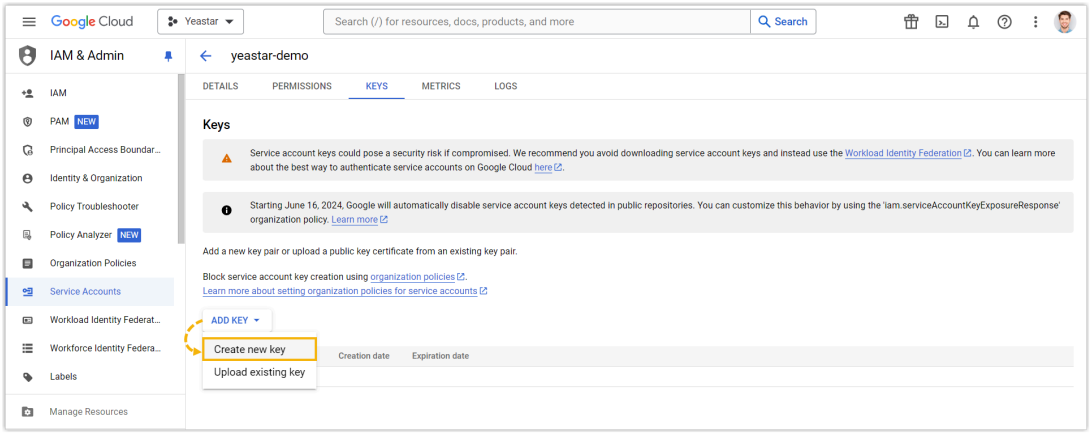
4. Create an access key for the service account.

   a. On the service accounts list, click ⋮ beside the service account that you have created, then select **Manage keys**.

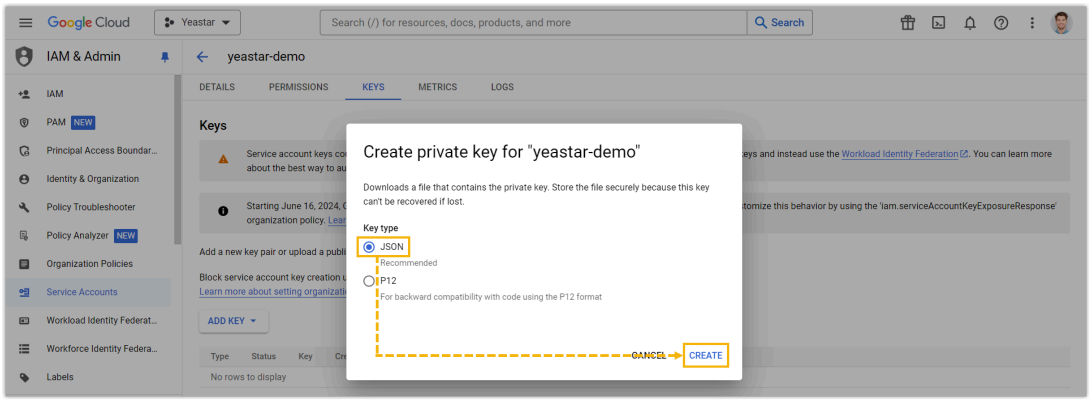


   You are redirected to the key configuration page.

   b. Click **ADD KEY**, then select **Create new key** from the drop-down list.



c. Set **Key type** to **JSON**, then click **CREATE**.



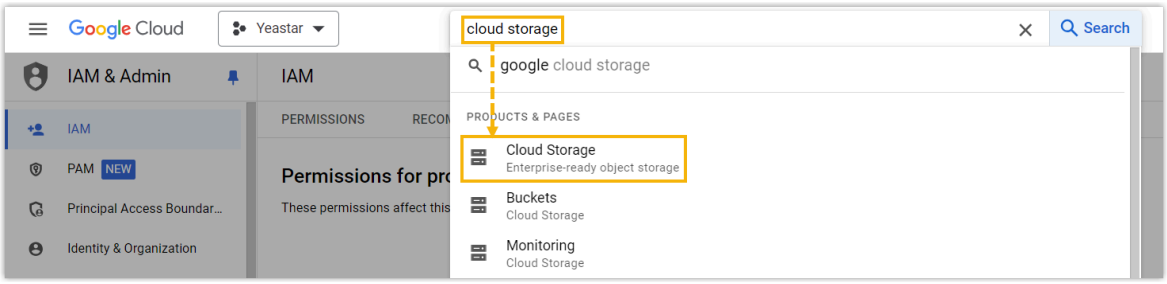
The access key is created and automatically downloaded to your computer as a JSON file.

> **Note:**
> Save the JSON file in a secure location, as you will need the file when setting up Google Cloud Storage bucket as archive server on PBX.

d. Click **CLOSE** to close the pop-up window.

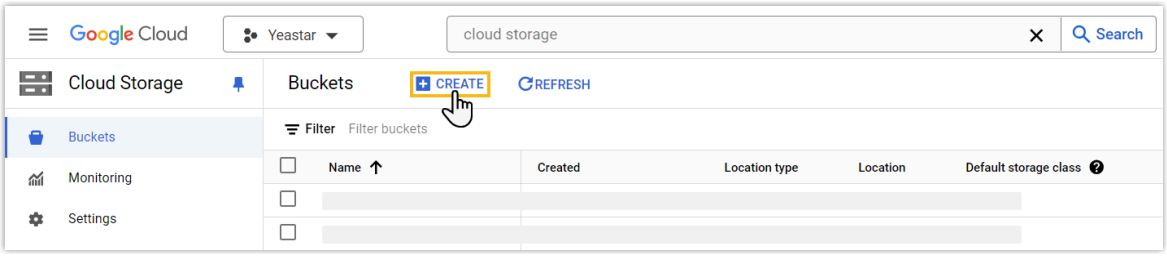
Step 2. Create a bucket on Google Cloud Storage

1. In the top search bar, search for and select **Cloud Storage**.

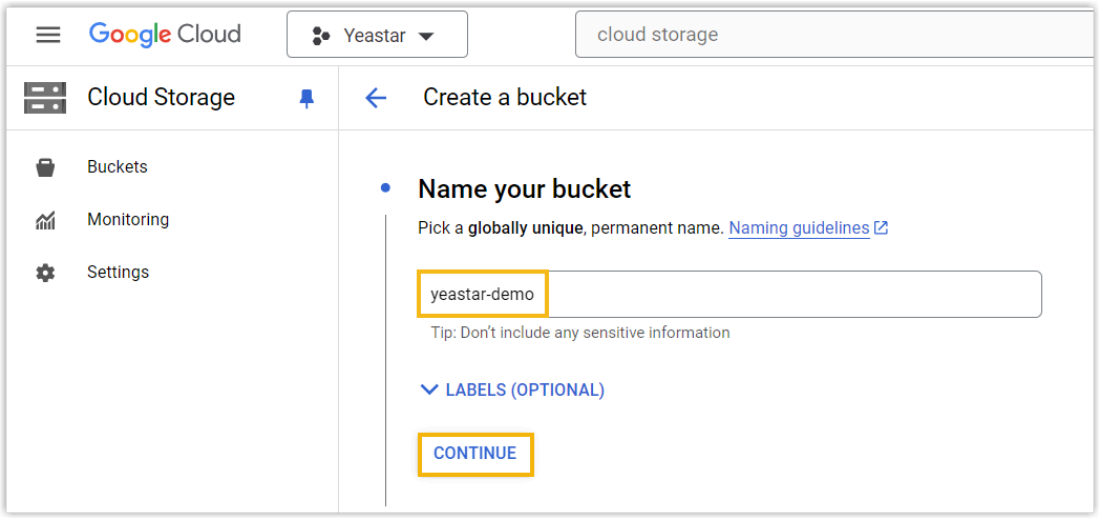


You are redirected to buckets configuration page.

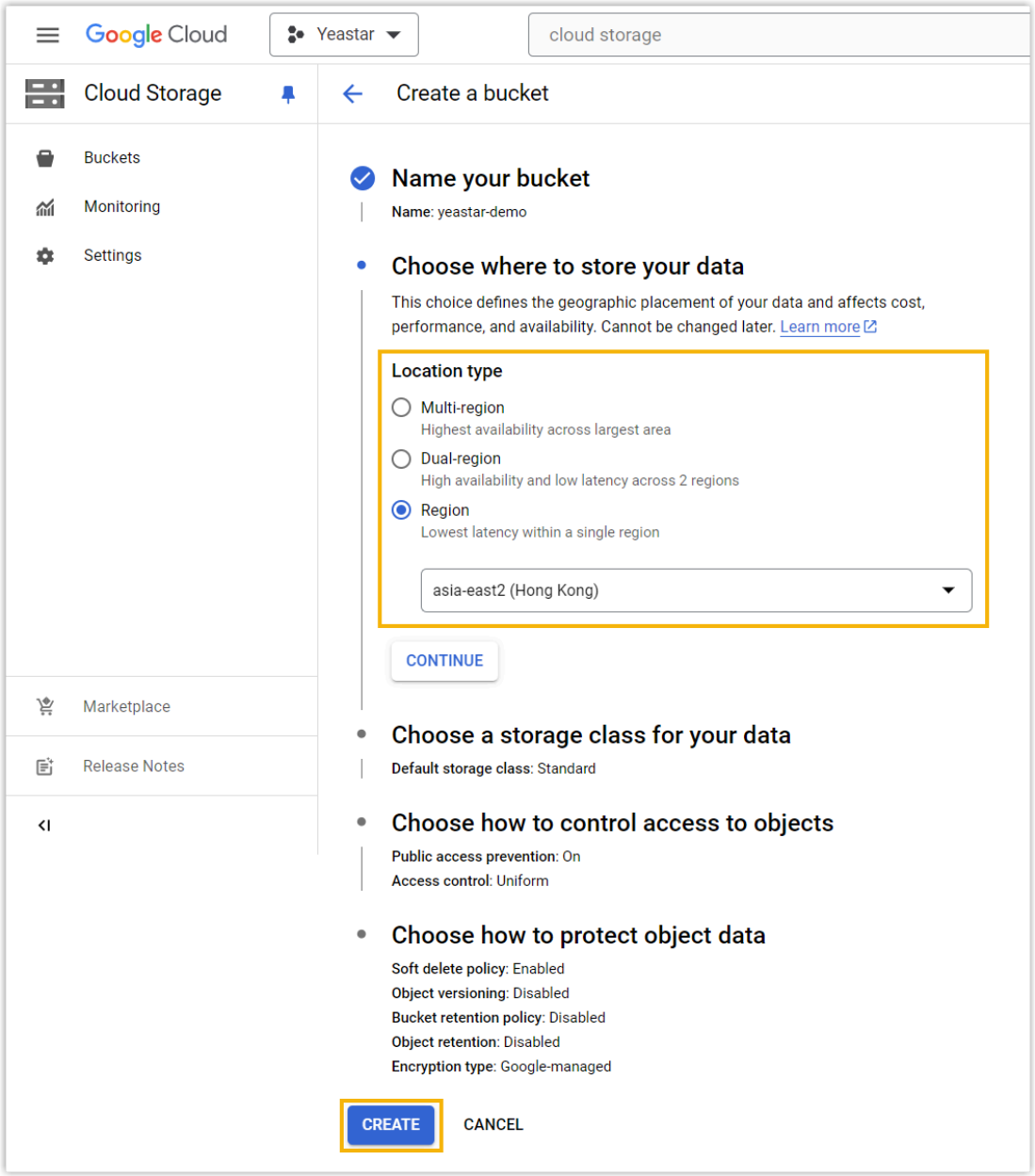
2. In the top pane, click **CREATE**.



3. In the **Name your bucket** field, enter a name to help you identify the bucket, then click **CONTINUE**.

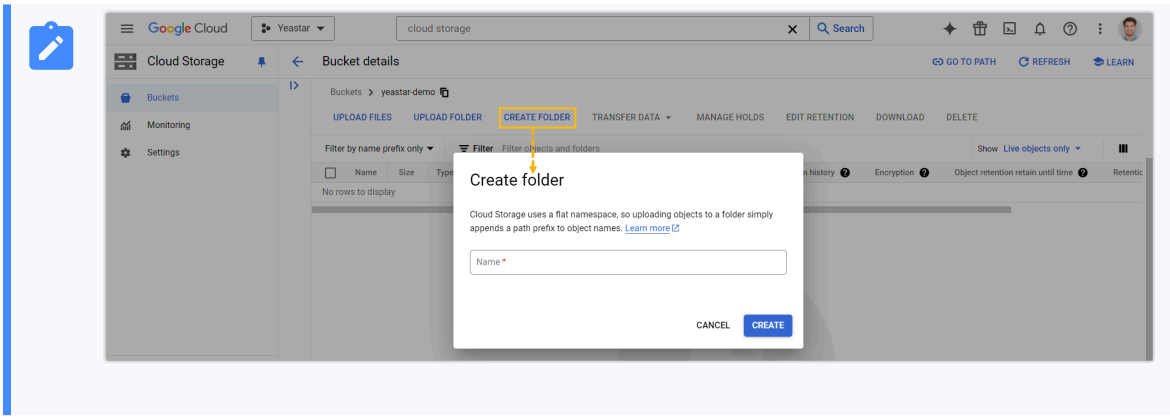


4. In the **Choose where to store your data** section, select the region in which you want to create a bucket, then click **CREATE**.



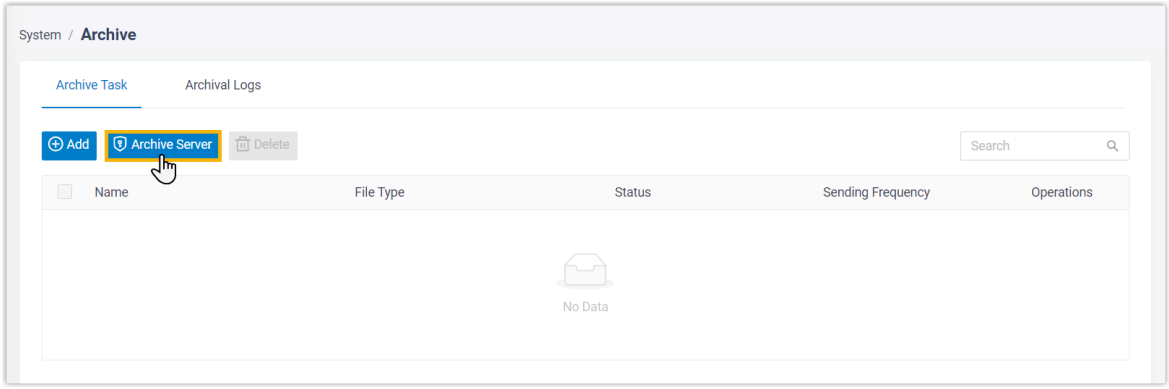
The bucket is created.

Note:
If you want to group the archived PBX files in Google Cloud Storage, you can create folders in the bucket. In this way, you can specify PBX files to be archived to the designated folder in the follow-up settings.

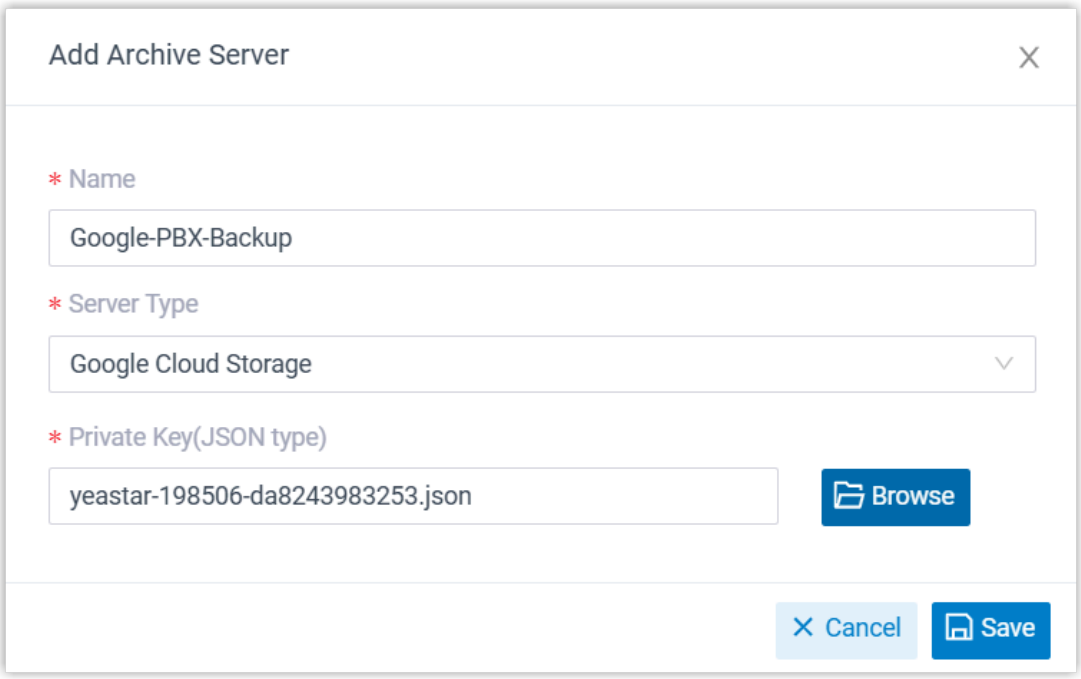


Step 3. Add Google Cloud Storage bucket as archive server on PBX

1. Log in to PBX web portal, go to **System > Archive**.
2. Under the **Archive Task** tab, click **Archive Server**.



3. Set up Google Cloud Storage bucket as an archive server.
    a. Click **Add**.
    b. In the pop-up window, complete the following settings.



Setting	Description
Name	Enter a name to help you identify the server.
Server Type	Select **Google Cloud Storage**.
Private Key(JSON type)	Click **Browse** to browse and upload the JSON file that you have downloaded in Google Cloud.

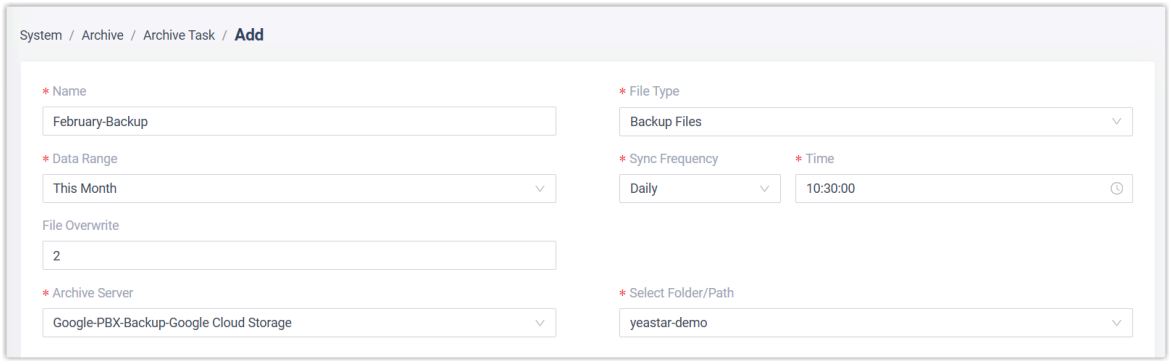
c. Click **Save**.

The Google Cloud Storage bucket is added as an archive server and displayed on the archive server list.

4. Click ✕ to close the window.

Step 4. Create a task to archive files to Google Cloud Storage on PBX

1. Under **Archive Task** tab, click **Add**.
2. Create a one-time or recurring archive task.



Setting	Description
Name	Enter a name to help you identify the task.
File Type	Select **Recording Files** or **Backup Files** as needed.
Data Range	Specify a time range of the files to be archived. **Note:** You can archive files for up to 31 days at a time.
Sync Frequency	Set how often to archive files to Google Cloud Storage. **Note:** As large amounts of data will consume PBX's CPU resources, we recommend that you schedule archive tasks during off-peak hours. • **Once**: If you choose the option, the system will archive files immediately after you save the task. • **Daily**: If you choose the option, select a time from the drop-down list. The system will archive files 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 will archive files 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 will archive files on this day and time of the month.
File Overwrite	Optional. Set the maximum number of files to be retained in Google Cloud Storage for the archive task. **Note:** • This option is available only when you schedule to archive backup files on a recurring basis.

Setting	Description
	• When it reaches the limit, the system will retain the latest backup files and delete the earlier ones.
Archive Server	Select the Google Cloud Storage bucket that you have added.
Select Folder/Path	Select the bucket or the folder in which you want to store archived files.

3. Click **Save**.

Result

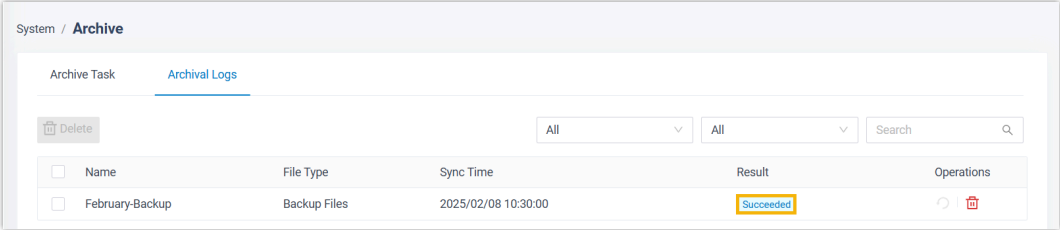
The specified files will be archived to the designated bucket or folder in your Google Cloud Storage immediately or at the scheduled time.

Note:
The system executes only one task at a time to avoid affecting system performance. If there are multiple tasks, they will be queued up one after another.

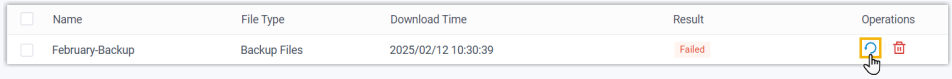
You can check the archive result in the following ways.

Check the archive result on PBX

On PBX web portal, go to **System > Archive > Archival Logs**. If the **Result** column shows **Succeeded**, it indicates that the specified files have been successfully archived to Google Cloud Storage.

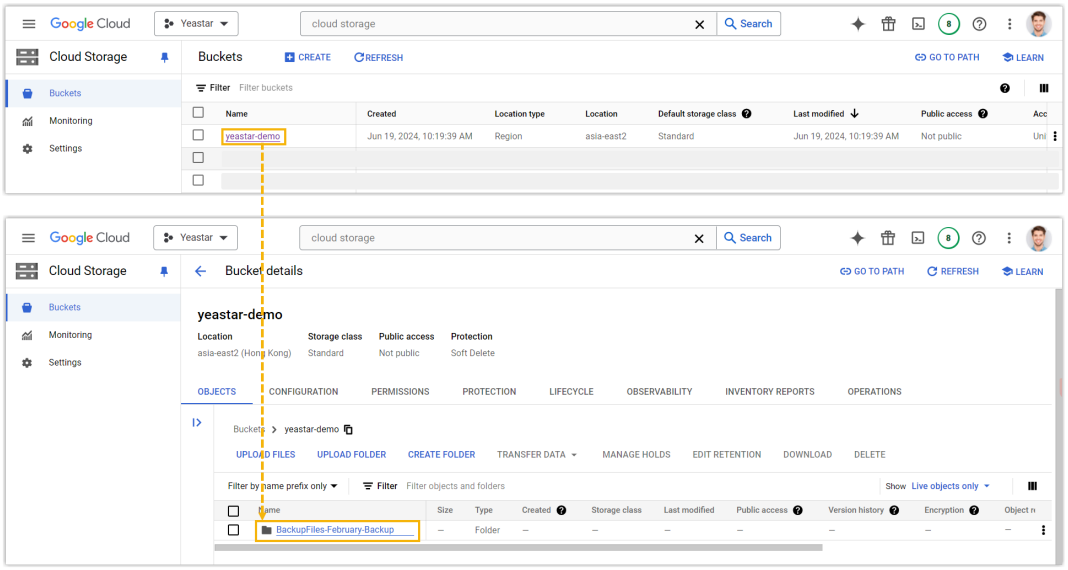


Note:
If the task is failed, the **Failed to Archive File(s)** event will be triggered; You can click to retry the task.



Check the archive result on Google Cloud Storage

On Google Cloud Console, go to the created bucket. If the specified files appear in the list, it indicates that the archive is successful.



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 36. Operations

Event	Description
Administrator Login Success	The administrator successfully logged in to the PBX management portal.
Web User Login Success	A user successfully logged in to the PBX web portal or the Linkus Web Client.
Web User Login Failed	A user failed to log in to PBX web 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.
Extension User Password Changed	An extension user's user password was changed.
RPS Request Success	The RPS request of the IP Phone(s) succeeded.
RPS Request Failed	The RPS request of the IP Phone(s) failed.

Table 37. 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 38. 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.
System Reboot	Either of the following situations triggered the event: • The PBX rebooted after configuration.

Table 38. System (continued)

Event	Description
	• The PBX automatically rebooted after system crash.
System Restore	The PBX was restored.
New System Firmware Detected	The PBX automatically detected a new firmware version.
System Upgrade Completed	The PBX was upgraded.
PBX Hot Standby Failover	A PBX failover has occurred, and the PBX system is taken over by the other server.
Primary Server Data Restoration Completed	The Primary Server is fixed and the data synchronization is completed now.
Both PBX Servers Failed to Function	Both the Primary Server and the Scondary Server of your PBX system were down.
Data Synchronization Error Due to Server Missing	The data synchronization could not function properly as the opposite PBX server is not detected.
Yeastar SMTP Server Error	Yeastar SMTP server failed to send emails.
Abnormal License Activation	Failed to connect to extranet License Activation Server.
Data Synchronization Error Due to Storage Missing	The data synchronization could not function properly as the storage device of the opposite PBX server is not detected.
Abnormal Core Call Services	A deadlock issue has been detected in the core call process.
Core Call Services Recovery Completed	The core call process has recovered successfully.

Table 39. Security

Event	Description
Web User Locked Out	PBX blocked the source IP when either of the following situations was met: • Web Login failure for more than 5 times in 24 hours. • More than 5 accounts were locked in 24 hours.
Linkus User Blocked Out	PBX blocked the source IP when either of the following situations was met: • 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	PBX blocked the source IP when either of the following situations was met:

Table 39. Security (continued)

Event	Description
	• 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.
API Authentication Blocked Out	PBX blocked the source IP due to too many failed API authentication attempts.
Linkus SDK Authentication Blocked Out	PBX blocked the source IP due to too many failed Linkus SDK authentication attempts.

Table 40. 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.
Video Conferencing Usage Limit Reached	Reach annual usage limit of video conferencing.
Failed to Archive File(s)	The task to archive recording files or backup files to an external server has failed.

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 web 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.

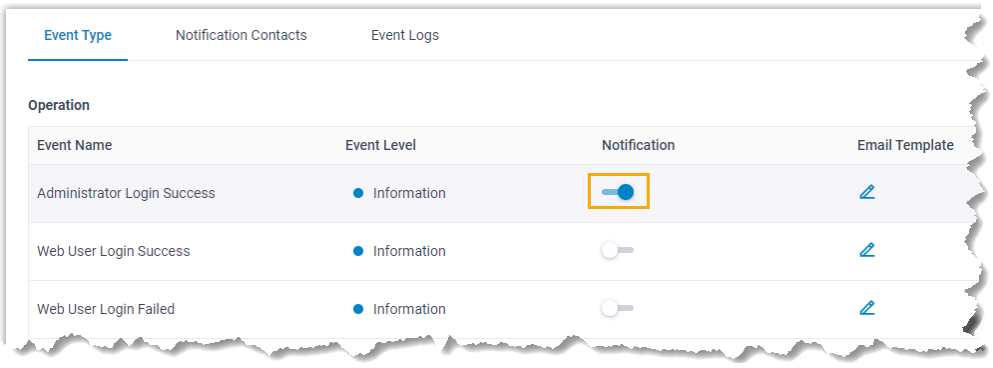
For more information, see Auto Cleanup Settings.

Configure Event Notifications

This topic describes how to configure event notifications.

Procedure

1. Log in to PBX web portal, go to **System > Event Notification > Event Type**.
2. In the **Notification** column, enable notifications for desired event.



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 web 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 web 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 web 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 web 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**.

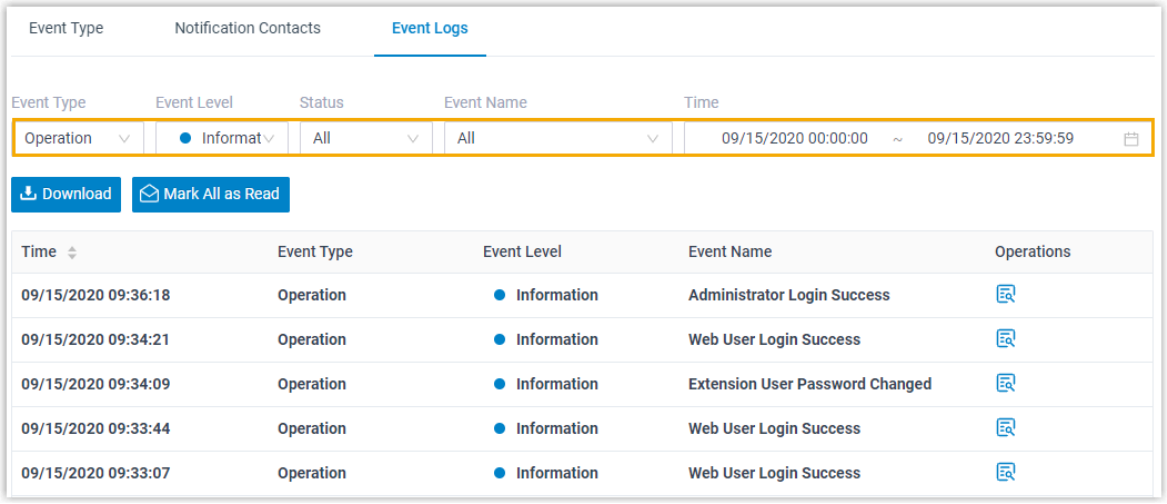
   The contacts are removed from the list, and will not receive notifications when events occur.

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 web portal, go to **System > Event Notification > Event Logs**.
2. Set the search criteria to search events.



- **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.

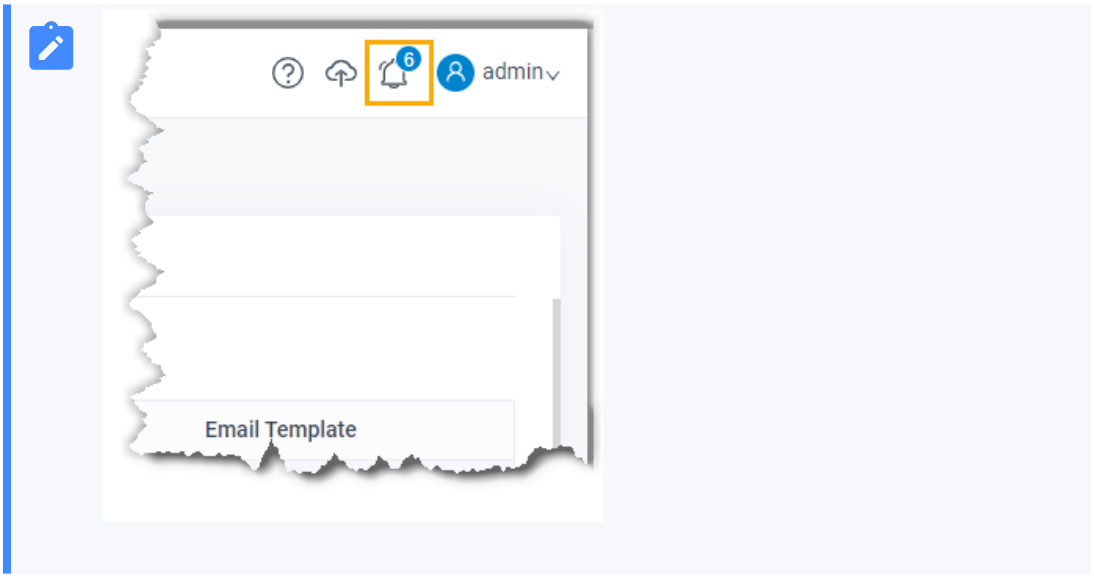
The matched events are displayed on the page.

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.



Remote Management

Remote Management Overview

If you need remote technical support or troubleshooting, you can contact device provider to connect your PBX to Yeastar Central Management, which is a Yeastar-hosted platform for all the device providers to remotely access and manage devices. In this way, you can secure remote connection to your PBX, while reducing IT and maintenance costs.

Activation methods

User Scenario	Instruction
In-house IT staff is responsible for routine maintenance of PBX system	Connect Yeastar P-Series PBX System to Yeastar Central Management Using Authentication Code
Device provider is responsible for routine maintenance of PBX system	Connect Yeastar P-Series PBX System to Yeastar Central Management Using Yeastar ID

Connection status

Status	Description
Connecting	The PBX is connecting to Yeastar Central Management.
Connected	The PBX is connected to Yeastar Central Management.

Status	Description
Disconnect	The PBX is NOT connected to Yeastar Central Management.
Error	The PBX is connected to Yeastar Central Management, but specific errors occur.
Expired	Device provider's subscription for Remote Management Service was expired.

Connect Yeastar P-Series PBX System to Yeastar Central Management Using Authentication Code

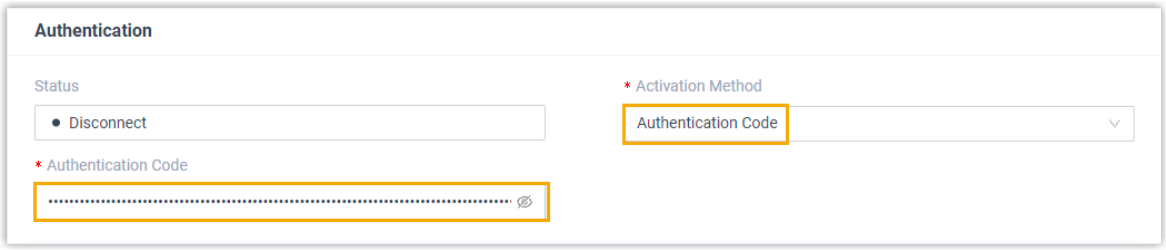
If you have in-house IT staff for routine maintenance of your PBX system, but the IT staff has difficulty handling specific system errors, you can connect PBX to Yeastar Central Management using an authentication code. In this way, device provider can help you troubleshoot issues.

Prerequisites

Make sure the version of your PBX system is 37.5.0.86 or later.

Procedure

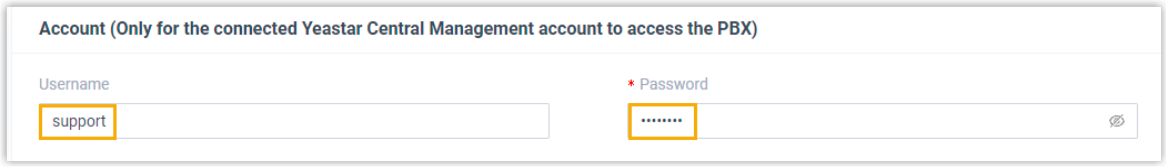
1. Contact device provider to obtain an authentication code.
2. Log in to PBX web portal, go to **System > Remote Management**.
3. In the **Authentication** section, complete the following settings:



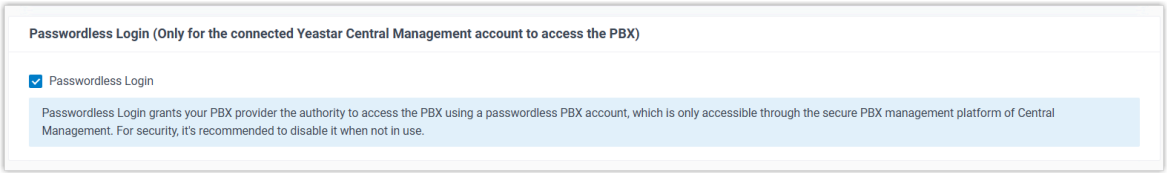
   - **Activation Method**: Select **Authentication Code**.
   - **Authentication Code**: Enter the authentication code that is provided by device provider.
4. If you don't want to expose your super administrator credential or extension credential, set a username and a password in the **Account** section.
   Device provider can use the username and password to remotely log in to your PBX web portal.

Note:

- The **Username** can NOT duplicate with the name of super administrator or the email address of an extension.
- Permissions of the account are the same as that of extensions with **Administrator** role assigned.



5. If you want to authorize device provider to log in to your PBX without entering username and password from Yeastar Central Management, select the checkbox of **Passwordless Login**.



Device provider can log in to PBX management portal with a dedicated **Passwordless** account by clicking on the encrypted web access link from Yeastar Central Management.

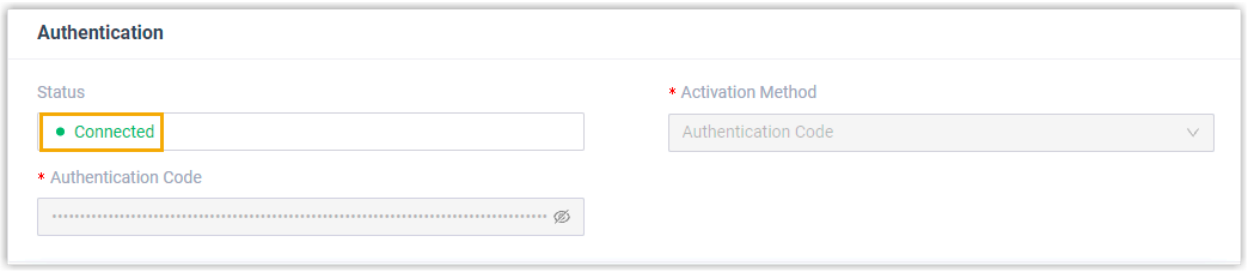
Note:

- If the **Passwordless Login** feature is not available on your PBX, upgrade PBX to version 37.17.0.16 or later.
- Permissions of the **Passwordless** account are the same as that of PBX super administrator.
- The PBX system automatically logs out the account according to Auto Logout Time if no operation is performed on the web page.

6. Click **Save**.

Result

The status is displayed as **Connected**, which indicates that your PBX system is connected to Yeastar Central Management.



Related information

[Connect Yeastar P-Series PBX System to Yeastar Central Management Using Yeastar ID]
[Disconnect Yeastar P-Series PBX System with Yeastar Central Management]

Connect Yeastar P-Series PBX System to Yeastar Central Management Using Yeastar ID

Assume that device provider is responsible for managing and maintaining your PBX system, when you encounter problems, you can connect your PBX to Yeastar Central Management using Yeastar ID. In this way, it only takes few clicks for device provider to remotely access your system and troubleshoot issues.

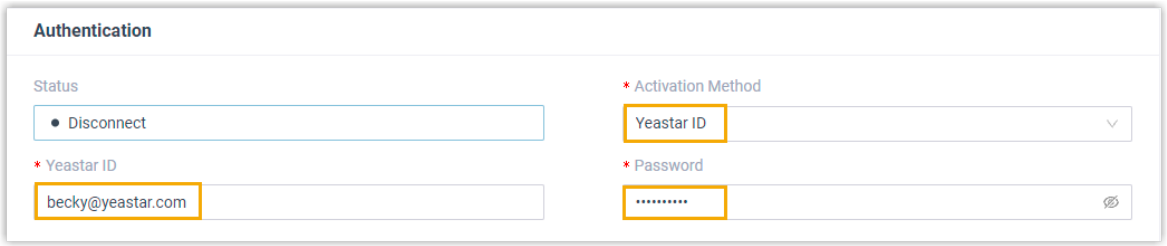
Prerequisites

Make sure the version of your PBX system is 37.5.0.86 or later.

Procedure

Contact device provider to connect your PBX system to Yeastar Central Management as follows:

1. Log in to PBX web portal, go to **System > Remote Management**.
2. In the **Authentication** section, complete the following settings:

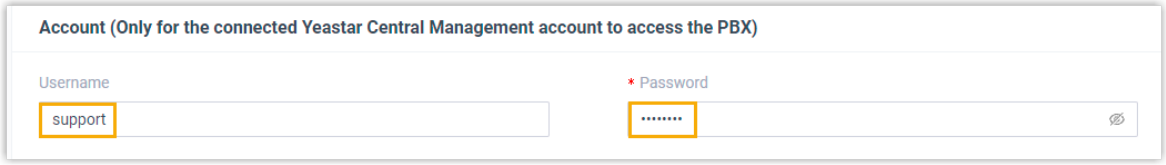


- **Activation Method**: Select **Yeastar ID**.
- **Yeastar ID**: Enter device provider's Yeastar ID.

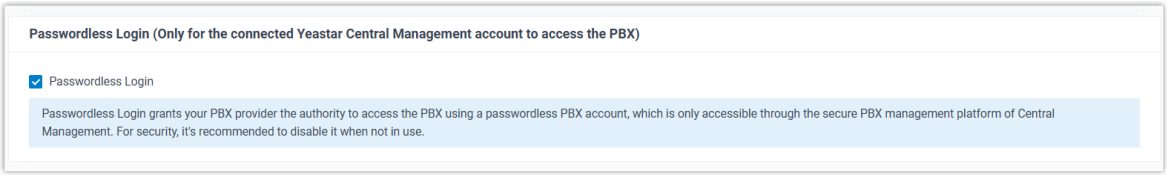
- **Password**: Enter device provider's password.

3. If you don't want to expose your super administrator credential or extension credential, set a username and a password in the **Account** section.
   Device provider can use the username and password to remotely log in to your PBX web portal.

> **Note:**
> - The **Username** can NOT duplicate with the name of super administrator or the email address of an extension.
> - Permissions of the account are the same as that of extensions with **Administrator** role assigned.



4. If you want to authorize device provider to log in to your PBX without entering username and password from Yeastar Central Management, select the checkbox of **Passwordless Login**.



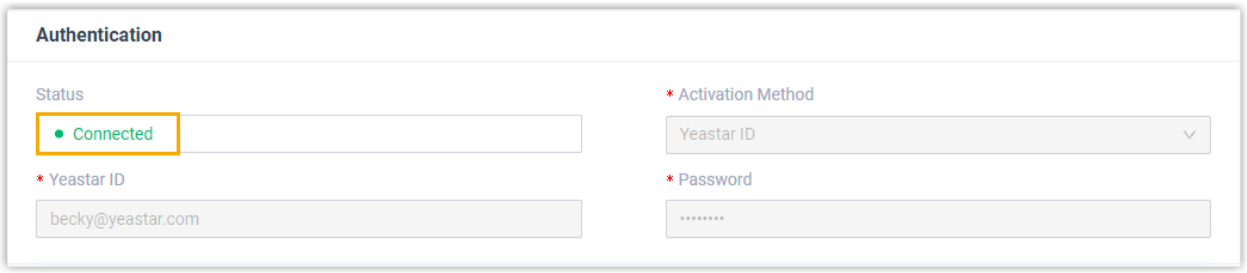
   Device provider can log in to PBX management portal with a dedicated **Passwordless** account by clicking on the encrypted web access link from Yeastar Central Management.

> **Note:**
> - If the **Passwordless Login** feature is not available on your PBX, upgrade PBX to version 37.17.0.16 or later.
> - Permissions of the **Passwordless** account are the same as that of PBX super administrator.
> - The PBX system automatically logs out the account according to Auto Logout Time if no operation is performed on the web page.

5. Click **Save**.

Result

The status is displayed as **Connected**, which indicates that your PBX system is connected to Yeastar Central Management.



Related information

Connect Yeastar P-Series PBX System to Yeastar Central Management Using Authentication Code

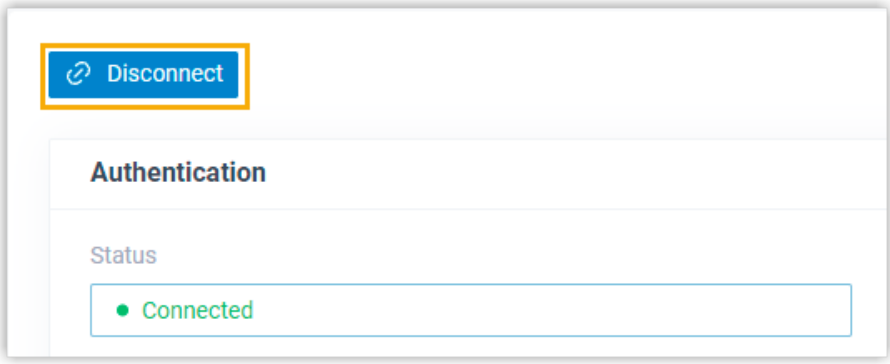
Disconnect Yeastar P-Series PBX System with Yeastar Central Management

Disconnect Yeastar P-Series PBX System with Yeastar Central Management

After device provider troubleshoots your PBX system issues, you can disconnect your PBX system with Yeastar Central Management.

Procedure

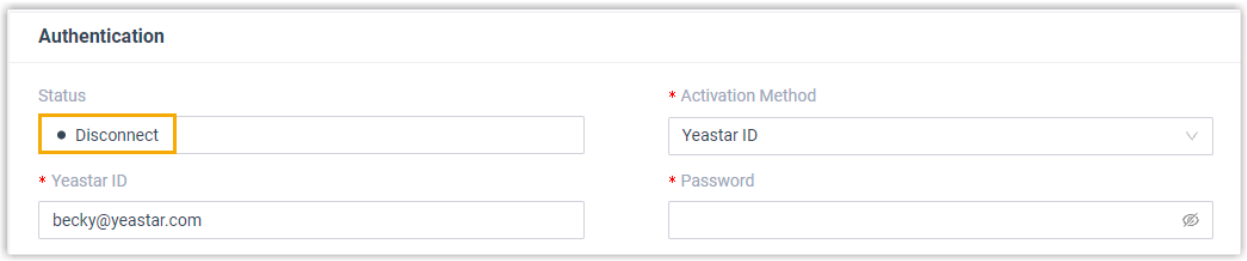
1. Log in to PBX web portal, go to **System > Remote Management**.
2. Click **Disconnect**.



3. In the pop-up dialog box, click **OK**.

Result

The status is displayed as **Disconnect**, which indicates that your PBX system is disconnected with Yeastar Central Management.



SNMP

Yeastar P-Series PBX System SNMP Overview

Simple Network Management Protocol (SNMP) is a standardized protocol for monitoring and managing network devices. By connecting Yeastar P-Series PBX System to a Network Management System (NMS) through SNMP, network administrator can query PBX information and monitor PBX on NMS.

Requirements

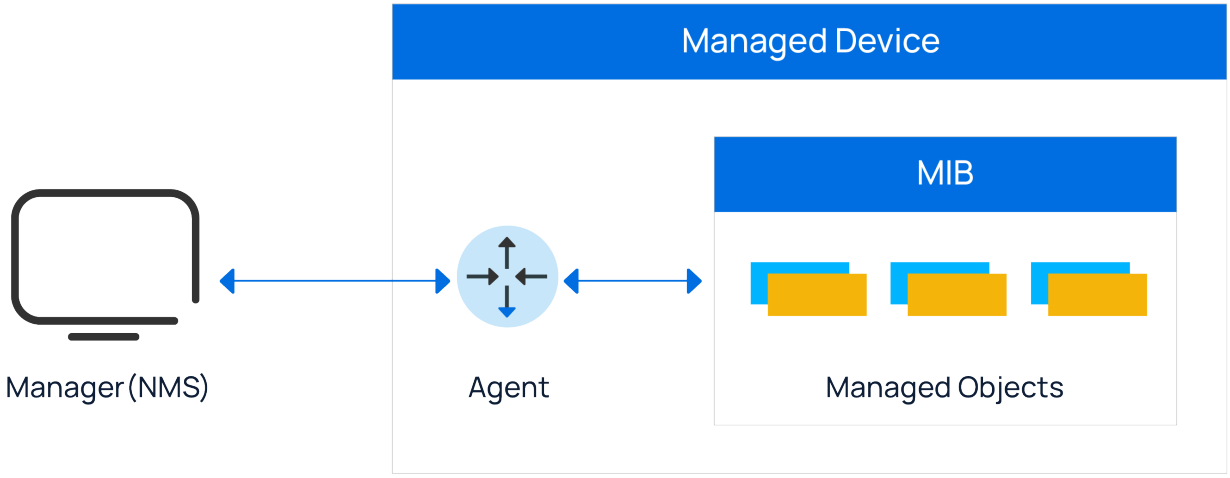
The version of Yeastar P-Series PBX System is 37.17.0.60 or later.

SNMP components

An SNMP system consists of 4 key components:

- **Manager**: A centralized system used to monitor the SNMP network, also known as Network Management System (NMS).
- **Managed devices**: An SNMP-enabled network entity that is managed by the SNMP manager. These are usually routers, switches, servers, etc.
- **Agent**: A network-management software module that runs on each managed device. It maintains data on the managed device, responds to requests from the NMS, and returns data to the NMS.
- **MIB (Management Information Base)**: An information base that contains definitions and information about the properties of a managed device. The manageable features of the device is called managed objects (or just objects or variables).

We provide a typology to help you understand the connection and interaction of each SNMP component.



As the typology shows, each managed device contains an SNMP agent process, an MIB, and multiple managed objects. Upon receiving requests from NMS, the agent queries or modifies variables in the MIB, and returns operation result to the NMS; In addition, when the managed device triggers a trap event regarding the MIB, it will send trap messages to NMS.

Supported SNMP version

Yeastar P-Series PBX System supports **SNMPv3**, which has all the functions of SNMPv1 and SNMPv2c. In addition, SNMPv3 provides secure access to devices by authenticating and encrypting data packets over the network.

Supported SNMP operation

Yeastar P-Series PBX System supports two operations:

- **SNMP Get**: Allow network administrator to collect data from the managed device.

  The NMS sends a Get request to the SNMP agent, the SNMP agent queries variables from the MIB and returns the data to the NMS.
- **SNMP Trap**: The managed device sends unsolicited trap messages to notify NMS that an urgent and significant event has occurred on the managed device.

Set up SNMP on Yeastar P-Series PBX System

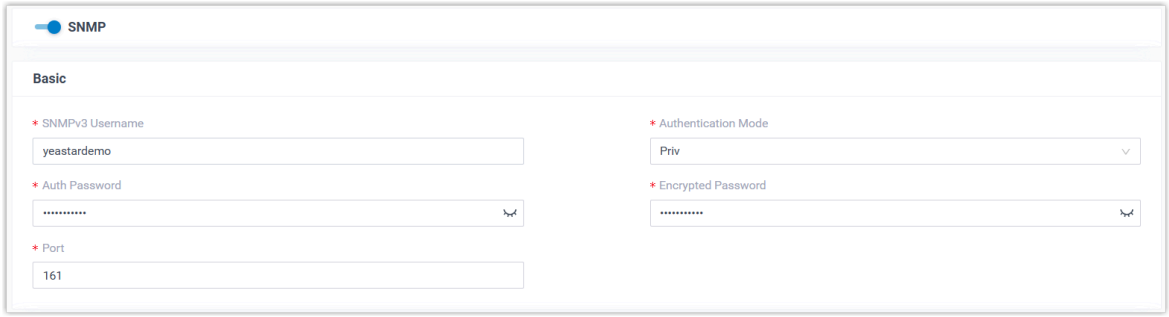
This topic describes how to enable SNMP and configure the related settings on Yeastar P-Series PBX System.

Requirements

The version of Yeastar P-Series PBX System is 37.17.0.60 or later.

Procedure

1. Log in to PBX web portal, go to **System > SNMP**.
2. In the **Basic** section, set up SNMP related settings that are required when adding the monitored device to the NMS.

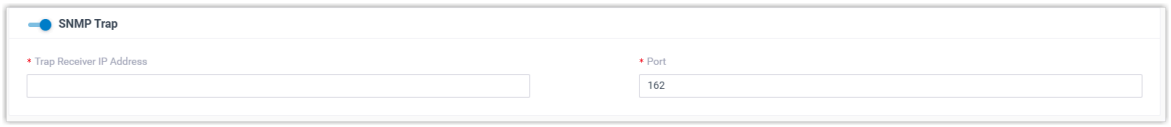


   a. Turn on **SNMP**.
   b. Complete the following settings.

Setting	Description
SNMPv3 Username	Enter a user name for authentication on NMS.
Authentication Mode	Select an authentication method. • **NoAuth**: Provide access control based on the user name. • **Auth**: Provide access control based on the HMAC-MD5 authentication. • **Priv**: Provide access control based on the HMAC-MD5 authentication and data encryption by CBC-DES.
Auth Password	Retain the default authentication password, or enter a desired password. **Note:** This option is available only when **Authentication Mode** is set to **Auth** or **Priv**.
Encrypted Password	Retain the default encryption password, or enter a desired password. **Note:**

Setting	Description
	This option is available only when **Authentication Mode** is set to **Priv**.
Port	Retain the default SNMP port `161`, or enter a desired port number.

3. **Optional:** To enable the PBX to send SNMP trap messages to NMS when a pre-defined event occurs and triggers the trap, set up SNMP trap.



   a. Turn on **SNMP Trap**.
   b. Enter the IP address of the SNMP trap receiver and the port to which the SNMP traps will be sent.
4. Click **Save**.

Result

The SNMP feature on Yeastar P-Series PBX System is set up.

What to do next

Connect Yeastar P-Series PBX System with Network Management System (NMS) via SNMP.

Note:

- Enter the **IP Address** of your PBX on NMS, instead of the Yeastar FQDN (Fully Qualified Domain Name).
- We provide an example on how to connect Yeastar P-Series PBX System with **Zabbix Server**.

  For more information, see Monitor Yeastar P-Series PBX System through SNMP using Zabbix Server.

Monitor Yeastar P-Series PBX System through SNMP using Zabbix Server

This topic takes Zabbix Server as an example to show you how to monitor Yeastar P-Series PBX System through SNMP.

Prerequisites

- The version of Yeastar P-Series PBX System is 37.18.0.18 or later.
- You have set up SNMP on Yeastar P-Series PBX System.

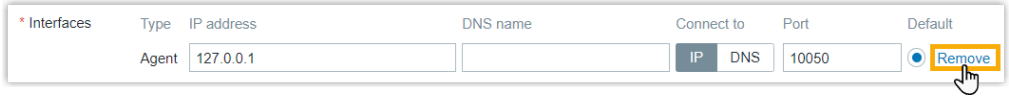
Procedure

- Step 1. Add a host to Zabbix Server
- Step 2. Add monitoring items to the host
- Step 3. Add triggers and actions

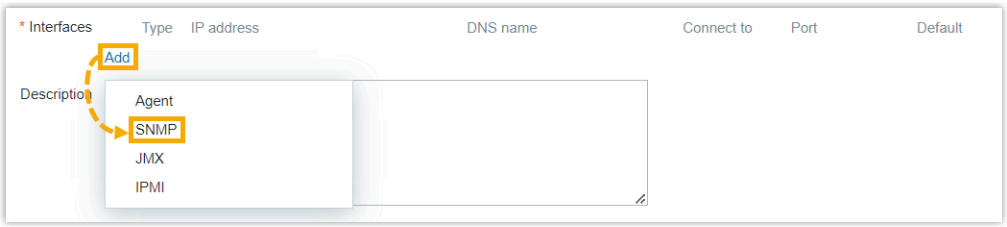
Step 1. Add a host to Zabbix Server

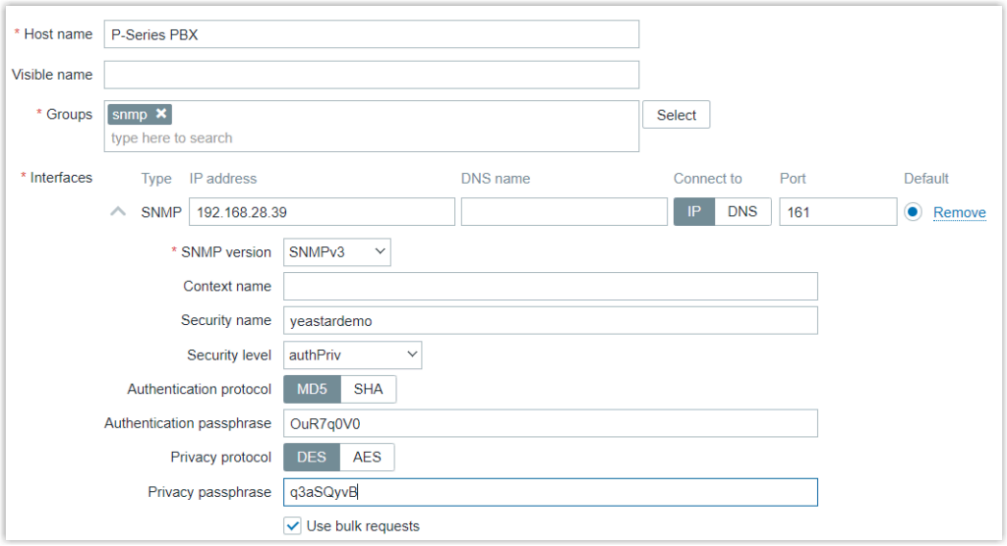
A host in Zabbix is a network entity (physical or virtual) that you want to monitor. In this example, we will add a host for Yeastar P-Series PBX System on Zabbix Server.

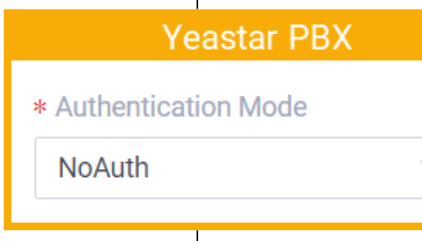
1. On the left navigation bar, go to **Configuration > Hosts**.
2. At the top-right corner, click **Create host**.
3. Under the **Host** tab, complete the following settings.
    a. In the **Host name** field, enter a name to help you identify the host. In this example, enter `P-Series PBX`.
    b. In the **Groups** field, enter the name of an existing group or click **Select** to select a group.
    c. In the **Interfaces** section, remove the default agent, then add a host.
        i. Click **Remove** to remove the default agent.

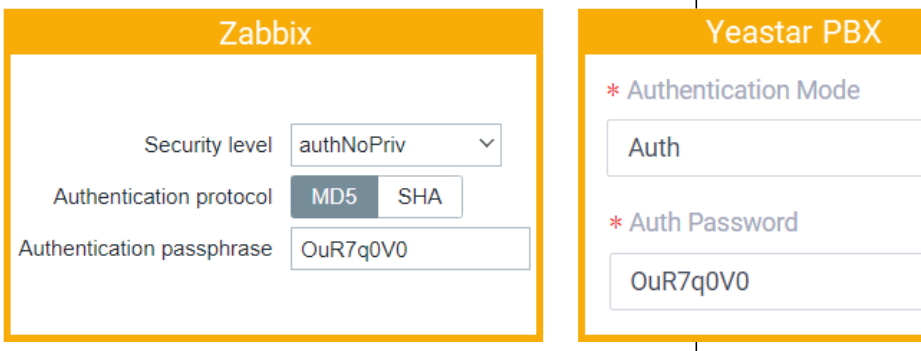
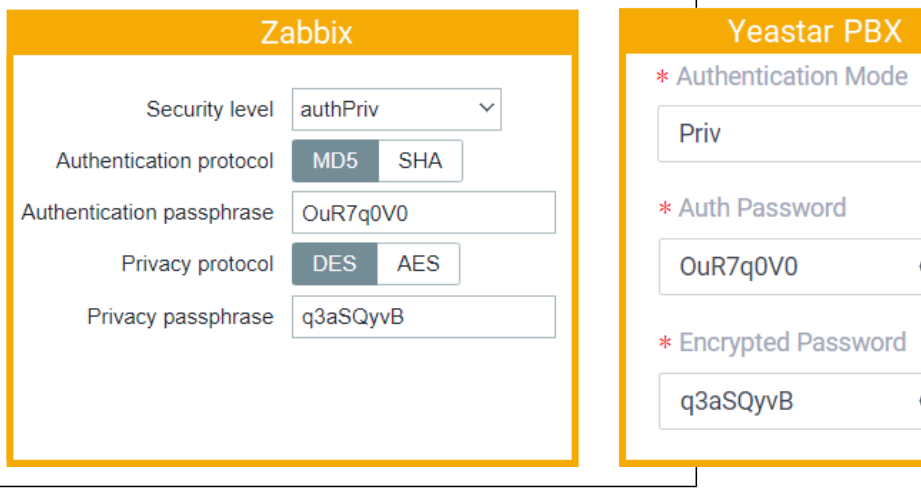


        ii. Click **Add**, select **SNMP**, then complete the following settings:



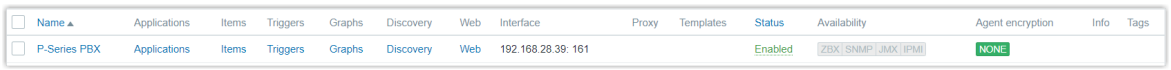


Setting	Description
IP address	Enter the IP address of PBX. In this example, enter `192.168.28.39`.
Port	Enter the SNMP port that is configured on PBX. In this example, retain `161`.
SNMP Version	Select **SNMPv3**.
Security name	Enter the SNMPv3 username that is configured on PBX. In this example, enter `yeastardemo`.
Security level	Select the authentication mode that is specified on PBX. • **noAuthNoPriv**: This option corresponds to **NoAuth** on PBX.  

Setting	Description
	• **authNoPriv**: This option corresponds to **Auth** on PBX. If you choose this option, you need to set **Authentication protocol** to **MD5**, and enter the authentication passphrase.  • **authPriv**: This option corresponds to **Priv** on PBX. If you choose this option, you need to set **Authentication protocol** to **MD5** and **Privacy protocol** to **DES**, and enter the authentication passphrase and privacy passphrase. 

4. Click **Add**.

   The host is added successfully. You can check it on the **Hosts** list.



Step 2. Add monitoring items to the host

A monitoring item defines a single metric or what kind of data to collect from a host. In this example, we will add monitoring items to collect data from the PBX host.

You can add monitoring items in the following ways:

- Import monitoring items
- Manually add monitoring items

Import monitoring items

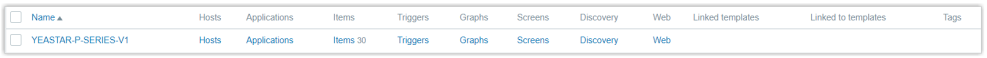
We provide a Yeastar PBX MIB file in both `.mib` and `.xml` formats, facilitating you to quickly import monitoring items into your Network Management System (NMS).

Download the file in the appropriate format, and follow the instructions below to import.

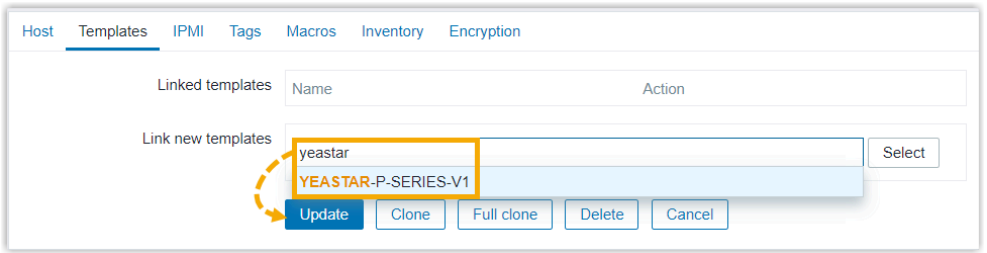
- Yeastar PBX MIB file in `.mib` format
- Yeastar PBX MIB file in `.xml` format

1. On the left navigation bar, go to **Configuration > Templates**.
2. At the top-right corner, click **Import**, select the MIB file, then click **Import**.

   You can check the imported template in the **Templates** list.



3. On the left navigation bar, go to **Configuration > Hosts**, search and find the PBX host, then go to the host detail page.
4. Click the **Templates** tab, search and select the imported template in the **Link new templates** field, then click **Update**.



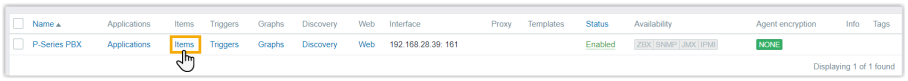
   On the **Hosts** list, you will find the template and the items are linked with PBX host successfully.



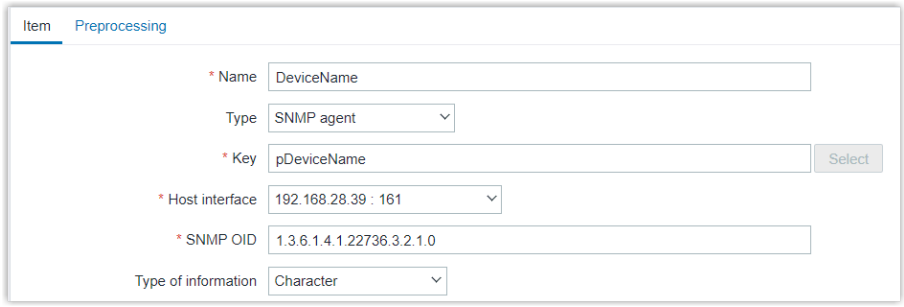
Manually add monitoring items

We provide a list of MIB objects as a reference for manually adding items on NMS. Check against the Yeastar P-Series PBX System MIB to add desired items.

1. Go to the creation page of monitoring items.
   a. On **Configuration > Hosts**, search and find the PBX host.
   b. Click **Items** beside the host.

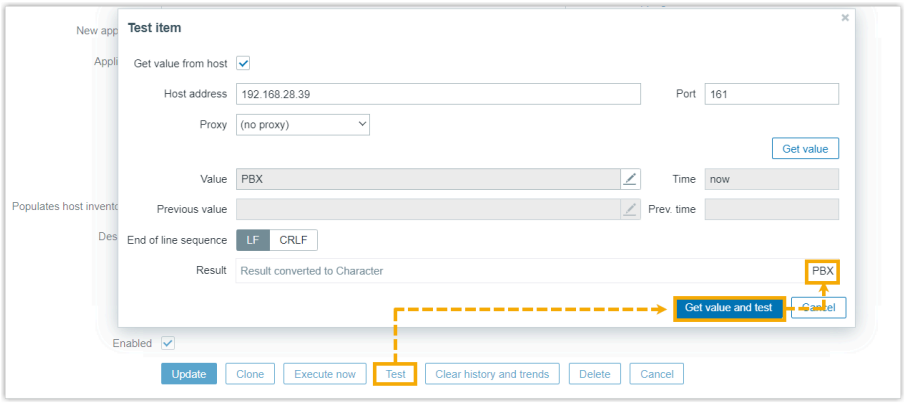


2. Add SNMP agent items to monitor and retrieve data from PBX.
   a. At the top-right corner, click **Create item**.
   b. Under **Item** tab, configure the following settings.



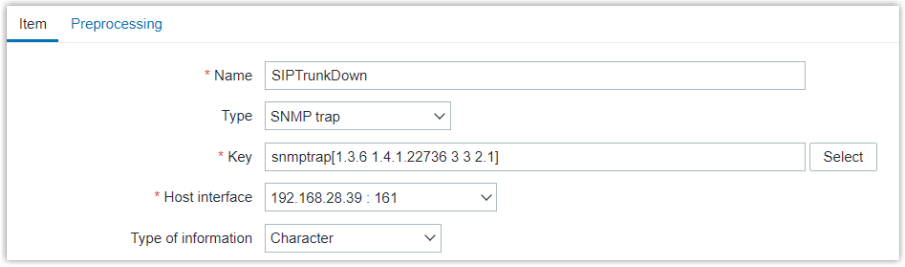
   - **Name**: Enter a name to help you identify the item. In this example, enter `DeviceName`.
   - **Type**: Select **SNMP agent**.
   - **Key**: Enter the name of the MIB object. In this example, enter `pDeviceName`.
   - **SNMP OID**: Enter the OID of the MIB object. In this example, enter `1.3.6.1.4.1.22736.3.2.1.0`.
   - **Type of information**: Select the information type. In this example, select **Character**.

   c. **Optional:** Click **Test > Get value and test** to test if the configuration works, then close the window.



d. Click **Add**.

3. Add SNMP trap items to monitor and receive trap messages from PBX.
   a. At the top-right corner, click **Create item**.
   b. Under **Item** tab, configure following settings.



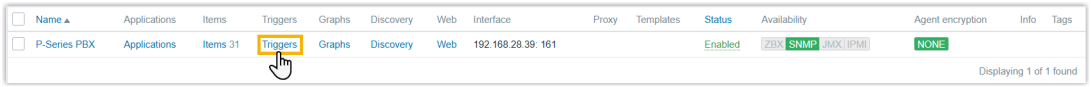
- **Name**: Enter a name to help you identify the item. In this example, enter `SIPTrunkDown`.
- **Type**: Select **SNMP trap**.
- **Key**: Enter a key, in the format of `snmptrap[{snmp_oid}]`. In this example, enter `snmptrap[1.3.6.1.4.1.22736.3.3.2-.1]`.
- **Type of information**: Select the information type. In this example, select **Character**.

   c. Click **Add**.

Step 3. Add triggers and actions

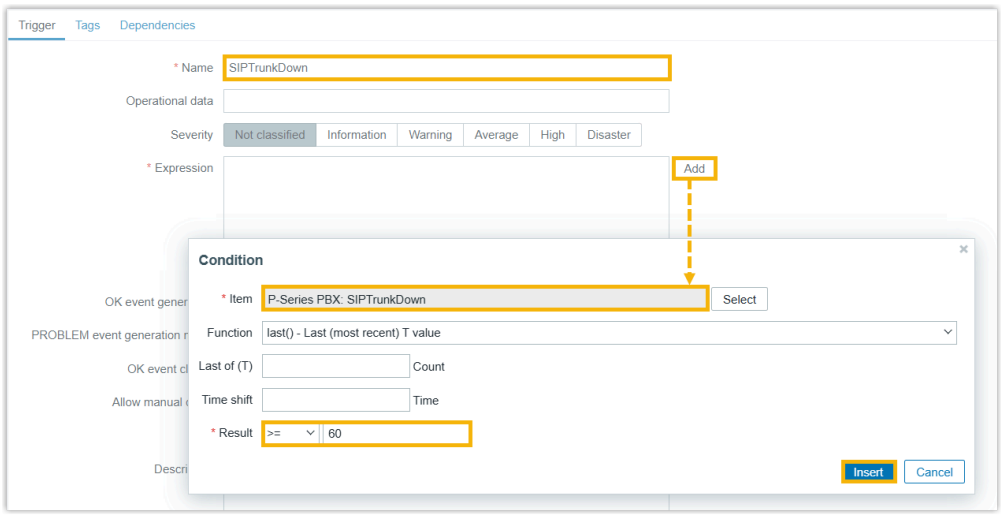
Add triggers and actions to receive timely alerts upon some condition change on PBX.

1. Add triggers to automatically evaluate whether the monitoring item reaches a threshold.
   a. Click **Triggers** beside the host.



b. At the top-right corner, click **Create trigger**.

c. Under **Trigger** tab, configure the trigger.

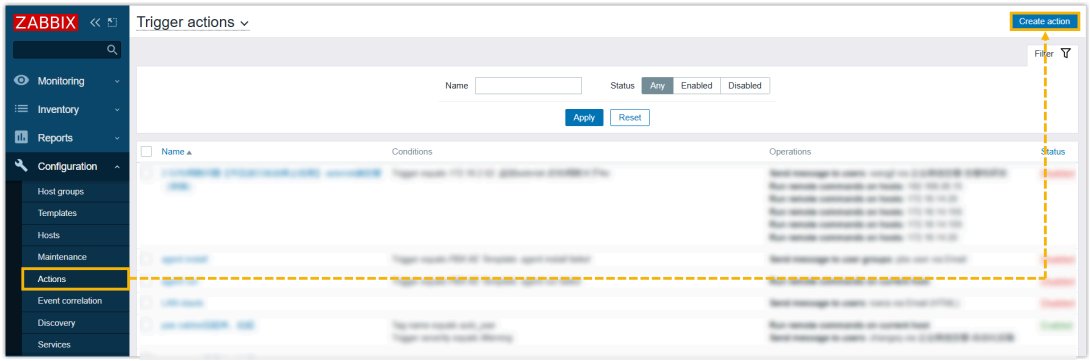


- **Name**: Enter a name to help you identify the trigger. In this example, enter `SIPTrunkDown`.
- **Expression**: Click **Add** to define the problem expression.

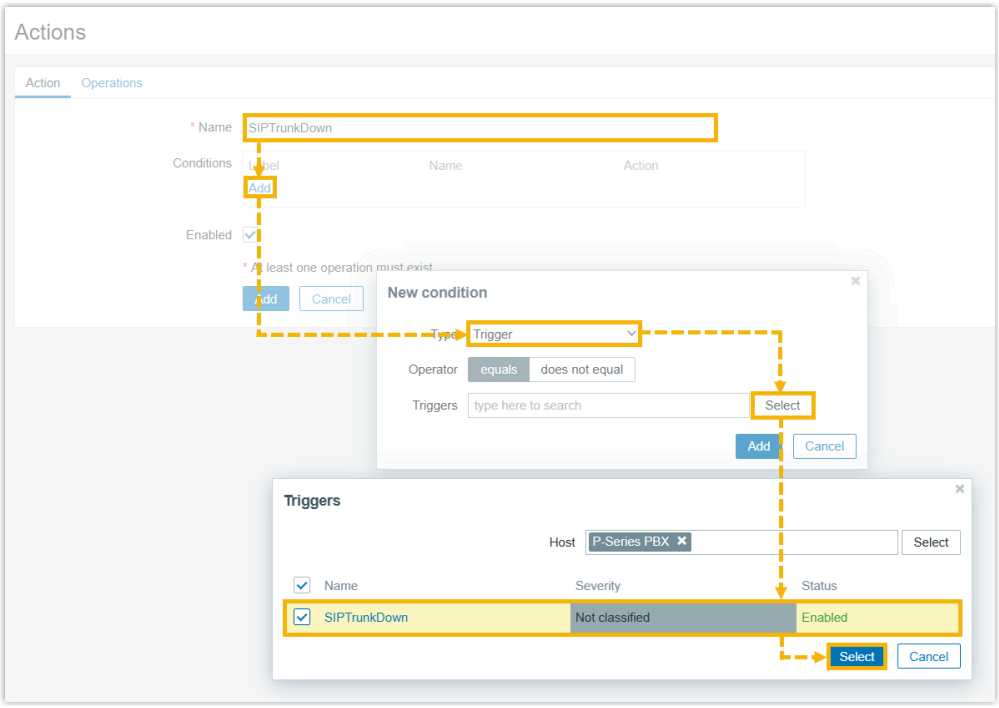
d. Click **Add**.

2. Add actions to send notifications when the monitoring item reaches a threshold.

a. On the left navigation bar, click **Actions**, then click **Create action**.

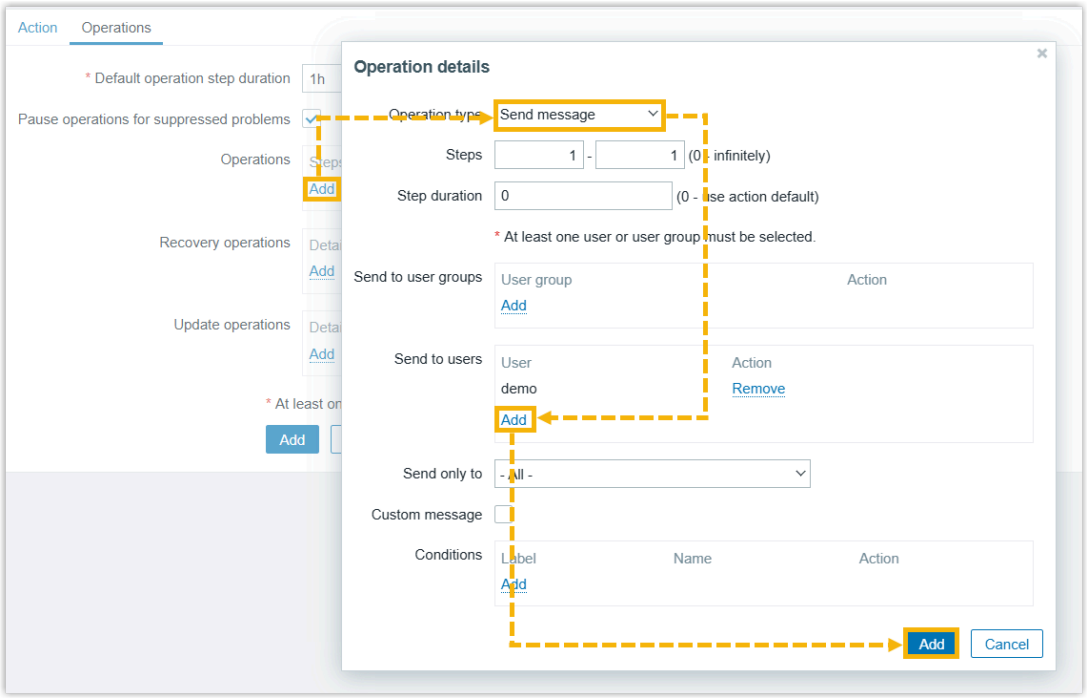


b. Under **Action** tab, set the conditions upon which operations will be carried out.



- **Name**: Enter a name to help you identify the action.
- **Condition**: Click **Add** to add a new condition for a trigger.

c. Under **Operations** tab, click **Add** to set the operations to carry out.



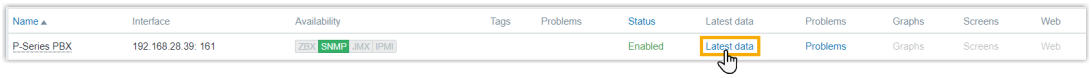
d. Click **Add**.

e. Click **Add**.

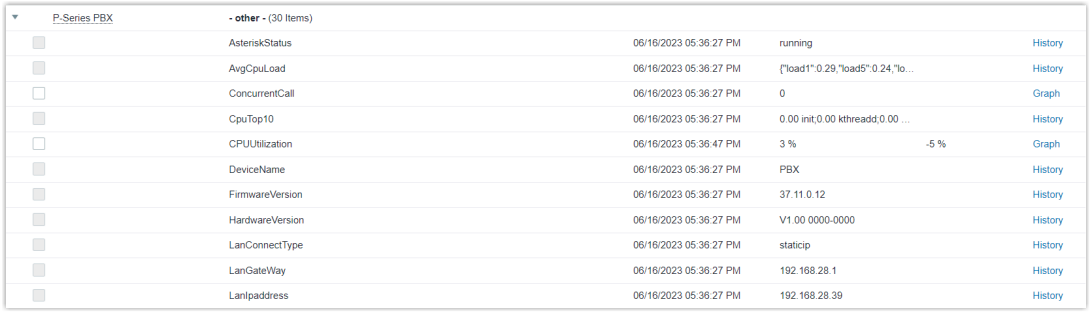
Result

- When a threshold is reached, notifications will be sent to the specified user.
- You can view the latest data collected by items on Zabbix.

1. On the left navigation bar, go to **Monitoring > Hosts**, search and find the PBX host.
2. Click **Latest data** beside the host.



You can view the latest data of the PBX.



Yeastar P-Series PBX System MIB

This topic lists the Yeastar P-Series PBX System MIB objects.

> **Tip:**
> To quickly add Yeastar P-Series PBX System MIB objects to Network Management System (NMS), you can download the Yeastar PBX MIB file, and import the file to NMS.

System

Name	OID	Type	Description
pProductModel	1.3.6.1.4.1.22736.3.1.1.0	String	The product model of PBX.
pHardwareVersion	1.3.6.1.4.1.22736.3.1.2.0	String	The hardware version of PBX.

Name	OID	Type	Description
pFirmwareVersion	1.3.6.1.4.1.22736.3.1.3.0	String	The firmware version of PBX.
pSerialNumber	1.3.6.1.4.1.22736.3.1.4.0	String	The serial number of PBX.
pUptime	1.3.6.1.4.1.22736.3.1.5.0	String	The uptime of PBX.
pLocalStorageUsage	1.3.6.1.4.1.22736.3.1.6.0	String	The local storage usage of PBX.
pMemoryUsage	1.3.6.1.4.1.22736.3.1.7.0	String	The memory usage of PBX.
pCPUUtilization	1.3.6.1.4.1.22736.3.1.8.0	String	The CPU utilization of PBX.
pConcurrentCall	1.3.6.1.4.1.22736.3.1.9.0	Integer	The number of occupied concurrent calls.
pAvgCpuLoad	1.3.6.1.4.1.22736.3.1.10.0	String	The load average of CPU.
pAsteriskStatus	1.3.6.1.4.1.22736.3.1.11.0	String	The asterisk status.
pCpuTop10	1.3.6.1.4.1.22736.3.1.12.0	String	The top 10 CPU consumption processes.
pMemTop10	1.3.6.1.4.1.22736.3.1.13.0	String	The top 10 memory consumption processes.

Network

Name	OID	Type	Description
pDeviceName	1.3.6.1.4.1.22736.3.2.1.0	String	The device name of PBX.
pLanStatus	1.3.6.1.4.1.22736.3.2.2.0	String	The LAN status.
pLanMac	1.3.6.1.4.1.22736.3.2.3.0	String	The MAC address of LAN.
pLanConnectType	1.3.6.1.4.1.22736.3.2.4.0	String	The network connection type of LAN.
pLanIpaddress	1.3.6.1.4.1.22736.3.2.5.0	String	The IP address of LAN.

Name	OID	Type	Description
pLanSubnetMask	1.3.6.1.4.1.22736.3.2.6.0	String	The subnet mask of LAN.
pLanGateWay	1.3.6.1.4.1.22736.3.2.7.0	String	The gateway of LAN.
pLanPrimaryDns	1.3.6.1.4.1.22736.3.2.8.0	String	The primary DNS of LAN.
pLanSecondaryDns	1.3.6.1.4.1.22736.3.2.9.0	String	The secondary DNS of LAN.
pWanStatus	1.3.6.1.4.1.22736.3.2.10.0	String	The WAN Status.
pWanMac	1.3.6.1.4.1.22736.3.2.11.0	String	The MAC address of WAN.
pWanConnectType	1.3.6.1.4.1.22736.3.2.12.0	String	The network connection type of WAN.
pWanIpaddress	1.3.6.1.4.1.22736.3.2.13.0	String	The IP address of WAN.
pWanSubnetMask	1.3.6.1.4.1.22736.3.2.14.0	String	The subnet mask of WAN.
pWanGateWay	1.3.6.1.4.1.22736.3.2.15.0	String	The gateway of WAN.
pWanPrimaryDns	1.3.6.1.4.1.22736.3.2.16.0	String	The primary DNS of WAN.
pWanSecondaryDns	1.3.6.1.4.1.22736.3.2.17.0	String	The secondary DNS of WAN.

Data

Name	OID	Type	Description
Extension			
pExtObjects	1.3.6.1.4.1.22736.3.4.1	Integer	The extension objects.
pExtTable	1.3.6.1.4.1.22736.3.4.2	/	The table of extension information.
pExtEntry	1.3.6.1.4.1.22736.3.4.2.1	/	The information of extension.
pExtIndex	1.3.6.1.4.1.22736.3.4.2.1.1	Integer	The index of extension.

Name	OID	Type	Description
pExtNum	1.3.6.1.4.1.22736.3.4.2.1.2	String	The extension number.
pExtName	1.3.6.1.4.1.22736.3.4.2.1.3	String	The name of extension.
pExtStatus	1.3.6.1.4.1.22736.3.4.2.1.4	String	The status of extension.
Trunk			
pTrunkObjects	1.3.6.1.4.1.22736.3.4 3	Integer	The trunk objects.
pTrunkTable	1.3.6.1.4.1.22736 3.4.4	/	The table of trunk information.
pTrunkEntry	1.3.6.1.4.1.22736.3.4.4.1	/	The information of trunk.
pTrunkIndex	1.3.6.1.4.1.22736.3.4.4.1.1	Integer	The index of trunk.
pTrunkName	1.3.6.1.4.1.22736.3.4.4.1.2	String	The name of trunk.
pTrunkType	1.3.6.1.4.1.22736.3.4.4.1.3	String	The type of trunk.
pTrunkStatus	1.3.6.1.4.1.22736.3.4.4.1.4	String	The status of trunk.

Traps

Name	OID	Type	Description
pTraps	1.3.6.1.4.1.22736.3.3	String	All traps from PBX.
Extension			
pExtAbnormalTraps	1.3.6.1.4.1.22736.3.3.1	String	The trap of abnormal extensions.
pIPphoneDown	1.3.6.1.4.1.22736.3.3.1.1	String	The IP phone or softphone is disconnected.
pIPphoneUp	1.3.6.1.4.1.22736.3.3.1.2	String	The IP phone or softphone is reconnected.
pExtDown	1.3.6.1.4.1.22736.3.3.1.3	String	The extension loses registration with all the endpoints (Linkus UC Clients, IP phones, and softphones).
pExtUp	1.3.6.1.4.1.22736.3.3.1.4	String	The extension is re-registered on at least one endpoint after losing registration on all the endpoints.

Name	OID	Type	Description
Trunk			
pTrunkAbnormalTraps	1.3.6.1.4.1.22736.3.3.2	String	The trap of abnormal trunks.
pSIPTrunkDown	1.3.6.1.4.1.22736.3.3.2.1	String	The SIP trunk is disconnected.
pSIPTrunkUp	1.3.6.1.4.1.22736.3.3.2.2	String	The SIP trunk is reconnected.
pTrunkDown	1.3.6.1.4.1.22736.3.3.2.3	String	The trunk is disconnected.
pTrunkUp	1.3.6.1.4.1.22736.3.3.2.4	String	The trunk is reconnected.
Call			
pCallAbnormalTraps	1.3.6.1.4.1.22736.3.3.3	String	The trap of call anomalies.
pPBXMaxCCTraps	1.3.6.1.4.1.22736.3.3.3.1	String	The maximum Concurrent Calls (CC) of PBX is reached.
pPBXMaxCCTrapsRecovery	1.3.6.1.4.1.22736.3.3.3.2	String	The Concurrent Calls (CC) of PBX becomes available again after reaching the maximum capacity.
pTrunkMaxCCTraps	1.3.6.1.4.1.22736.3.3.3.3	String	The maximum Concurrent Calls (CC) allowed in the SIP trunk, FXO trunk, 3G/4G LTE trunk, or T1/J1 trunk is reached.
pTrunkMaxCCTrapsRecovery	1.3.6.1.4.1.22736.3.3.3.4	String	The maximum number of Concurrent Calls (CC) allowed in the SIP trunk, FXO trunk, 3G/4G LTE trunk, or T1/J1 trunkbecomes available again after reaching the maximum capacity.
pCallFailedTraps	1.3.6.1.4.1.22736.3.3.3.5	String	The traps of failed calls.
pAsteriskTraps	1.3.6.1.4.1.22736.3.3.3.6	String	The trap of abnormal Asterisk.
pAsteriskTrapsRecovery	1.3.6.1.4.1.22736.3.3.3.7	String	The Asterisk returns to normal status.

Hot Standby

Hot Standby Overview

The high reliability and high availability performance of server plays a vital role in an application system. Once the key system is down, it may lead to significant losses in data and a variety of issues. Yeastar provides a Hot Standby solution, which can provide high system availability and prevent you from the unnecessary business loss caused by unexpected server failure.

Requirements and restrictions

Requirements

Two identical Yeastar P-Series PBX Systems are required to set up a Hot Standby pair, and the servers in the Hot Standby pair must meet the following requirements.

Item	Requirement
Product Model	The two PBXs are the same model.
Hardware Installation	The two PBXs have identical hardware installation (The same expansion board and telephony module are installed in the same position and slot).
Plan	Hot Standby can be used without additionally subscribing to a plan. **Note:** Make sure that you subscribe to the desired plan for the PBX that will act as the Primary Server in the Hot Standby pair. When the Secondary Server takes over the system, the features included in the plan will automatically be available on the Secondary Server.
Firmware	The firmware version of the two PBXs are the same (37.6.0.24 or later).
Network	The two PBXs use the same Internet Protocol, both assigned with static IP addresses, and are located in the same LAN subnet.

Restrictions

- Yeastar P-Series PBX System supports to set up Hot Standby pair that are located in the same LAN subnet.
- Hot Standby only works for LAN port.

> **Note:**
> If the Ethernet mode of the PBX is **Dual**, set the default interface to LAN port (Path: **System > Network > Basic Settings**).

- When setting up a Hot Standby pair, DO NOT connect the FXS module with a splitter, as it may cause a short circuit and damage the PBX during failover.

Operation Mechanism

The following content describes the operation mechanism of the Hot Standby feature.

Set up Hot Standby pair

The solution consists of two PBXs (a Primary Server and a Secondary Server) with the same hardware and firmware. The Primary Server works in "active" state while the Secondary Server works in "standby" state and cannot be configured.

The two PBXs share a virtual IP address, which always points to the active PBX. In this way, PBX administrator can access and operate the PBX system via the virtual IP address directly.

For more information about the configuration, see Set up Hot Standby Pair.

Failover

Under normal operating, the Secondary Server sends heartbeat keep-alive packets to the Primary Server periodically, and synchronizes the data and configuration from the Primary Server in real-time so that the two devices contain identical information.

Once the Primary Server goes down, the Secondary Server will take over the PBX system automatically if it doesn't receive any response from the Primary Server in a certain time. In this way, the system will continue to run.

Also, the system will send Hot Standby related event notifications to the notification contacts concerned, informing them to repair the Primary Server as soon as possible.

Take over the PBX system manually

After you have repaired the Primary Server, you need to manually set up the Primary Server to synchronize data and take over the PBX system from Secondary Server.

For more information about the configuration, see Primary Server Takes over the System from Secondary Server.

Set up Hot Standby Pair

This topic describes how to set up Hot Standby on the Primary Server and Secondary Server. When the Primary Server fails, the Secondary Server becomes active and takes over the entire phone system, thus minimizing downtime and data loss.

Requirements and restrictions

Requirements

Two identical Yeastar P-Series PBX Systems are required to set up a Hot Standby pair, and the servers in the Hot Standby pair must meet the following requirements.

Item	Requirement
Product Model	The two PBXs are the same model.
Hardware Installation	The two PBXs have identical hardware installation (The same expansion board and telephony module are installed in the same position and slot).
Plan	Hot Standby can be used without additionally subscribing to a plan. **Note:** Make sure that you subscribe to the desired plan for the PBX that will act as the Primary Server in the Hot Standby pair. When the Secondary Server takes over the system, the features included in the plan will automatically be available on the Secondary Server.
Firmware	The firmware version of the two PBXs are the same (37.6.0.24 or later).
Network	The two PBXs use the same Internet Protocol, both assigned with static IP addresses, and are located in the same LAN subnet.

Restrictions

- Yeastar P-Series PBX System supports to set up Hot Standby pair that are located in the same LAN subnet.
- Hot Standby only works for LAN port.

> **Note:**
> If the Ethernet mode of the PBX is **Dual**, set the default interface to LAN port (Path: **System > Network > Basic Settings**).

- When setting up a Hot Standby pair, DO NOT connect the FXS module with a splitter, as it may cause a short circuit and damage the PBX during failover.

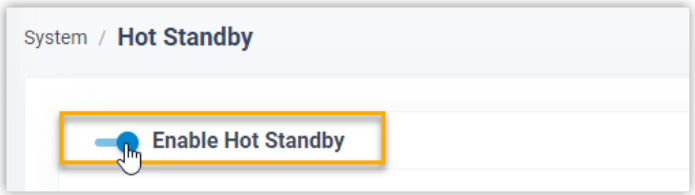
Scenarios

A company has set up a failover pair in the local network environment for high availability performance, the IP addresses are listed below:

- Primary Server: 192.168.5.151
- Secondary Server: 192.168.5.152
- Virtual IP address: 192.168.5.150

Procedure

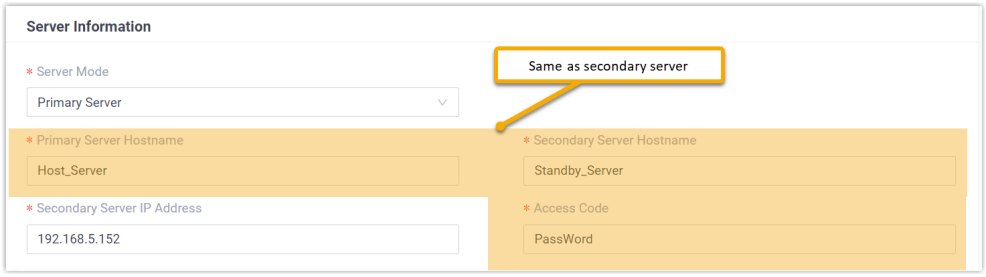
1. Log in to PBX web portal, go to **System > Hot Standby**.
2. On the top of the page, turn on the **Enable Hot Standby** switch.



3. In the **Server Information** section, enter the information of the Primary Server and Secondary Server respectively.

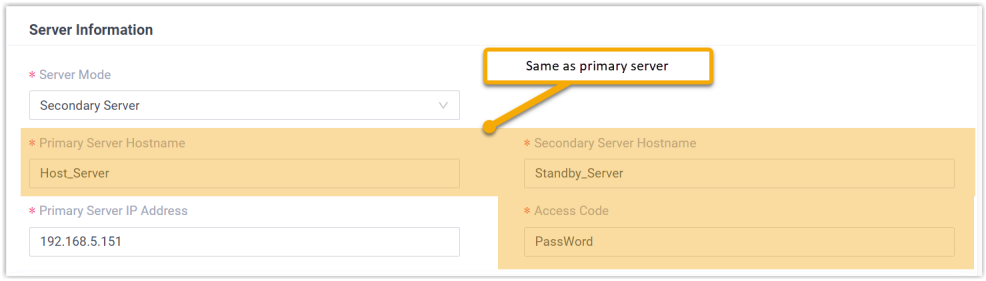
Set up Primary Server

In the **Hot Standby** configuration page of the Primary Server, complete the following settings.



Set up Secondary Server

In the **Hot Standby** configuration page of the Secondary Server, complete the following settings.



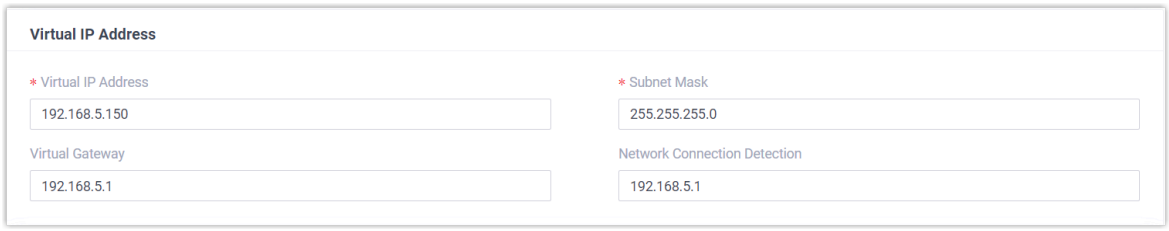
Settings

The detailed description of the settings are listed in the following table.

Setting	Description
Server Mode	In the drop-down list, select a server mode.
Primary Server Hostname	Enter a name to help you identify the Primary Server. In this example, enter `Host_Server`. **Note:** The **Primary Server Hostname** set in the Primary Server and Secondary Server should be the same to avoid confusion in the event notification.
Secondary Server Hostname	Enter a name to help you identify the Secondary Server. In this example, enter `Standby_Server`. **Note:** The **Secondary Server Hostname** set in the Primary Server and Secondary

Setting	Description
	Server should be the same to avoid confusion in the event notification.
Primary Server IP Address	Enter the IP address of the Primary Server. In this example, enter `192.168.5.151`.
Secondary Server IP Address	Enter the IP address of the Secondary Server. In this example, enter `192.168.5.152`.
Access Code	Set an access code. **Note:** The two PBXs must have the same access code to authenticate connection.

4. In the **Virtual IP Address** section, set up the network connection for the Hot Standby pair.

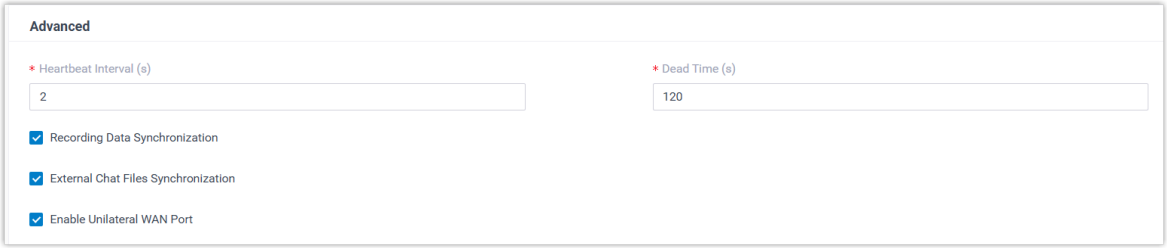


Note:
When you enter a virtual IP address, the corresponding information of **Subnet Mask**, **Virtual Gateway** and **Network Connection Detection** is automatically filled in.

Setting	Description
Virtual IP Address	Virtual IP address is an IP address that has not been assigned to other devices and will be the shared IP address for the two PBXs. The virtual IP always points to the active PBX server. **Note:** • Set the same virtual IP address on the Primary Server and Secondary Server. • After Hot Standby is enabled, you can access and operate the PBX system via the virtual IP. For example, use the virtual

Setting	Description
	IP address as server IP address when registering extensions in the local network.
Subnet Mask	A valid subnet mask can ensure the interactions between the PBX server and the virtual IP network.
Virtual Gateway	A valid gateway can ensure the interactions between the PBX server and the virtual IP network.
Network Connection Detection	If all nodes failed to be detected by the Secondary Server, it means that Internet outage(s) has occurred; both the Primary Server and the Secondary Server of your PBX system have abnormal internet connection. In this case, the PBX failover would not work.

5. In the **Advanced** section, complete the following settings.



Setting	Description
Heartbeat Interval (s)	Define the frequency to send heartbeat keep-alive packets. The default value is 2 seconds, which means that the Secondary Server sends packet every 2 seconds to detect whether the Primary Server is alive or not.
Dead Time (s)	Define the maximum time interval before the Primary Server responds to the Secondary Server. The default value is 120 seconds. If the Secondary Server receives no response after timeout, it will take over the PBX system automatically. **Note:** Set the **Dead Time** longer than the server rebooting time (about 2 minutes), or the Secondary Server will take over when the Primary Server is rebooting.
Recording Data Synchronization	If enabled, the Secondary Server will synchronize the call recording files in real-time.

Setting	Description
External Chat Files Synchronization	If enabled, the secondary server will synchronize the external chat files in real time.
Enable Unilateral WAN Port	If enabled, only one WAN port of the Primary Server and Secondary Server will be enabled. When PBX Hot Standby failover occurs, the WAN IP address will remain unchanged and will be switched to the active PBX server.

6. Click **Save**.

   The system prompts that you need to reboot the server to make Hot Standby take effect.

Result

Important:
If the system detects that the two PBXs do not meet with the requirement of Hot Standby, the Hot Standby setting will fail. In this case, you need to manually reboot the Secondary Server again, otherwise the physical modules on the Secondary Server will be abnormal and cannot be used.

Primary Server

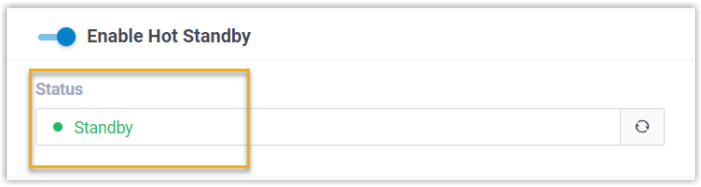
- After the PBX is rebooted, the **Status** displays **Running**.



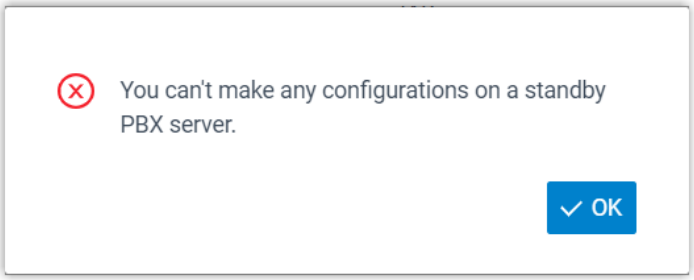
- When you configure the Primary Server, the configuration will be synchronized to the Secondary Server.

Secondary Server

- After the PBX is rebooted, the **Status** of the Secondary Server displays **Standby**.



- When you try to make configuration on the Secondary Server, the system prompts "You can't make any configurations on a standby server".



What to do next

Test if Hot Standby works.

1. On Primary Server, create an extension, save and apply the changes.
2. On Secondary Server, check if the Hot Standby configurations are correct.

   You can see the same extension is added automatically in the Secondary Server.

Primary Server Takes over the System from Secondary Server

The Secondary Server automatically takes over if the Primary Server goes down. You need to take over the PBX system on Primary Server after repairing. This topic describes how to take over the PBX system from the Secondary Server.

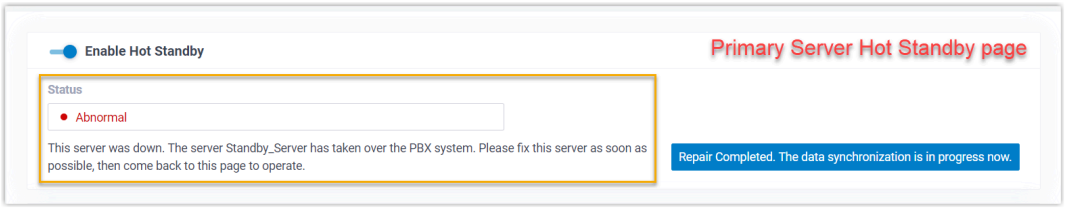
Background information

When the Primary Server fails, the Secondary Server will automatically take over the PBX system, and send a event notification of **PBX Hot Standby Failover** to the contacts concerned.

In this case, the Hot Standby status of Primary Server and Secondary Server is shown as below.

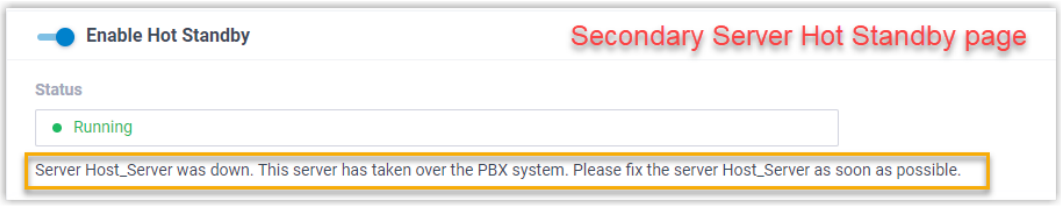
Primary Server

The Hot Standby status displays **Abnormal**, and the page prompts that the Secondary Server has taken over the PBX system, you need to repair the Primary Server as soon as possible.



Secondary Server

The hot standby status changes from **Standby** to **Running**, and the page prompts that the Secondary Server has taken over the PBX system, you need to fix the Primary Server as soon as possible.



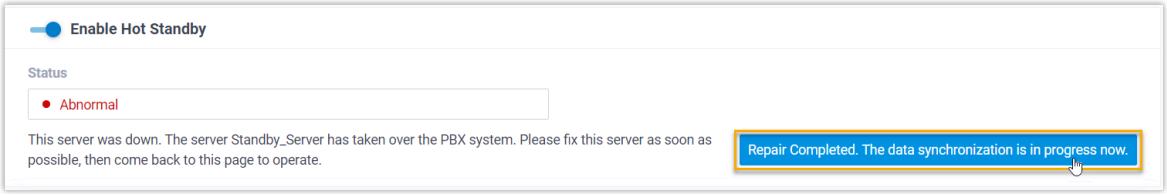
After you have repaired the Primary Server, you need to manually set up the Primary Server to take over the system from Secondary Server.

Prerequisites

- Make sure the firmwares of the Hot Standby pair are the same.
- Make sure there is no call in progress on the Secondary Server, or the call will be dropped.

Procedure

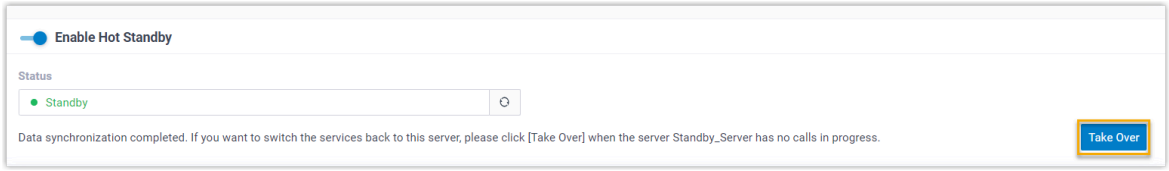
1. Log in to the PBX web portal of the Primary Server, go to **System > Hot Standby**.
2. Click **Repair Completed. The data synchronization is in progress now**.



The Hot Standby status of Primary Server becomes **Standby**, and the server starts to synchronize data from the Secondary Server.

After data synchronization is completed, the PBX system will send an event notification of **Primary Server Data Restoration Completed** to the contacts concerned.

3. Click **Take Over**.



4. In the pop-up window, click **OK**.

Result

- The **Status** of the Primary Server changes to **Running**, indicating that the Primary Server has taken over the PBX system.
- The Secondary Server returns to standby state.

Secondary Server Takes over the System from Primary Server

If the Primary Server becomes abnormal and hot standby failover is not triggered, you can manually switch the system to the Secondary Server while it is in Standby mode.

Requirements

The firmware version of Secondary Server is 83.17.0.60 or later.

Prerequisites

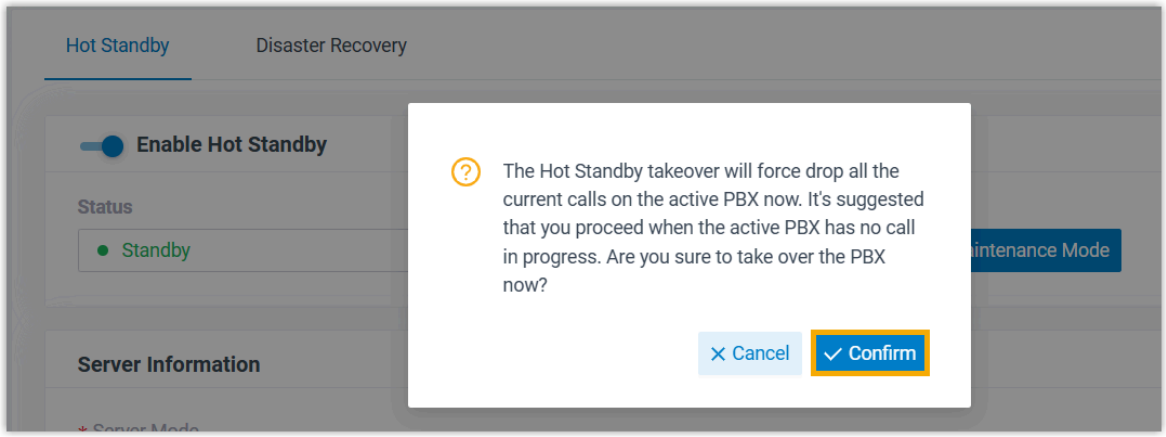
Make sure there is no call in progress on the Primary Server, or the call will be dropped.

Procedure

1. Log in to the web portal of Secondary Server, go to **System > High Availability > Hot Standby**.
2. Click **Take Over**.



3. In the pop-up window, click **Confirm**.



Result

- The webpage displays "This server has taken over the system.", and the **Status** of the Secondary Server changes to **Running**.
- The system will send a event notification of **Secondary Server Takeover (For Only 30 Days)** to the contacts concerned.

Enable and Schedule Maintenance Mode on Secondary Server

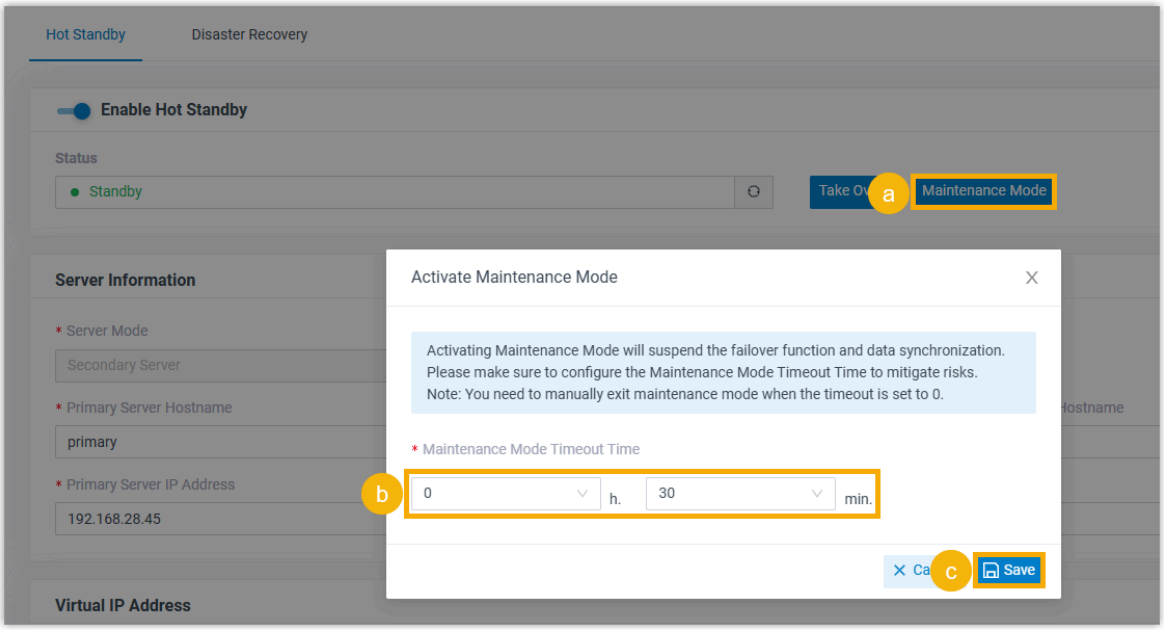
When Primary Server is under maintenance (e.g. firmware upgrade or system reboot), it may fail to respond to heartbeat packets from Secondary Server, which would trigger an unexpected takeover. To avoid this, you can enable and schedule Maintenance Mode on the Secondary Server to temporarily suspend health monitoring and prevent takeover during the maintenance window.

Requirements

The firmware version of Secondary Server is 37.19.0.70 or later.

Procedure

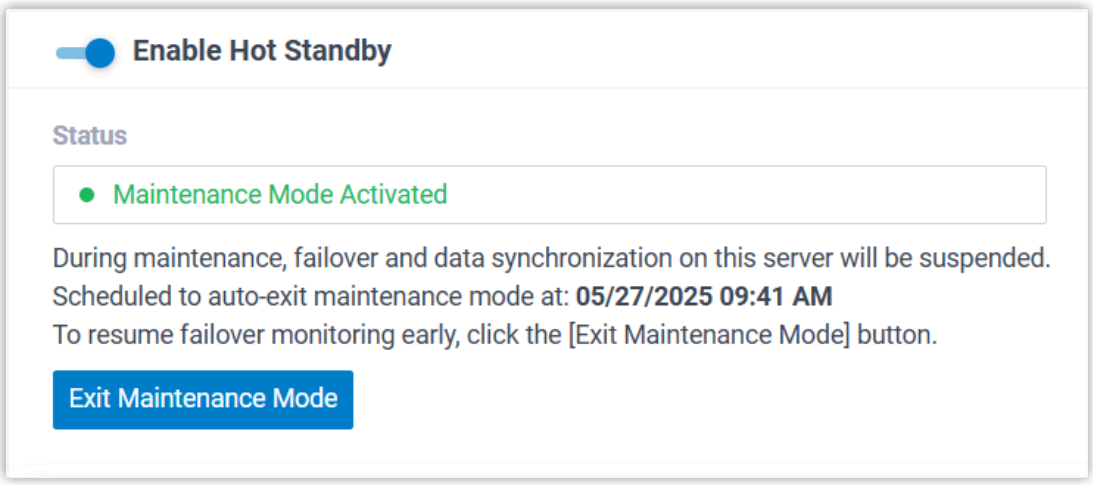
1. Log in to the web portal of Secondary Server, go to **System > High Availability > Hot Standby**.
2. Enable and schedule maintenance mode.



a. Click **Maintenance Mode**.
b. In the **Maintenance Mode Timeout Time** drop-down list, set the timeout.
c. Click **Save**.

Result

- The status displays **Maintenance Mode Activated**. During the maintenance window, failover and data synchronization are suspended.



- When the maintenance timeout is reached, the Secondary Server will automatically exit Maintenance Mode and resume failover monitoring as well as data synchronization.

> **Note:**
>
> - If the timeout is set to 0, you must click **Exit Maintenance Mode** to manually exit when the Primary Server is ready.
> - If a specific timeout is set, you can also exit manually in advance.

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 can control and filter traffic sent to the PBX based on IP address, domain, or MAC address.

Yeastar P-Series PBX System has default static defense rules to accept connections from devices on local network, auto provisioned devices, and Yeastar servers. You can also set up new rules to accept, drop, or reject access to the PBX. The IP addresses that are 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 can control and filter traffic sent to the PBX based on the frequency of packets sent, effectively preventing massive connection attempts or brute force attacks.

Yeastar P-Series PBX System has default auto defense rules to protect SSH connection, SIP registration, and Web access. You can also set up new rules according to your needs. 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**.

For more information, see Add an Auto Defense Rule and Manage Blocked IP Addresses.

Blocked IPs

The blocked IP addresses would be listed in the **Blocked IPs**. If a trusted IP address was blocked, you can go to **Blocked IPs** to delete the IP address.

For more information, see Manage Blocked IP Addresses.

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).

Download Global Anti-hacking IP Blocklist

If the option is enabled, Yeastar Global Anti-hacking IP Blocklist will be downloaded to the PBX. Any connections from the IP addresses in the blocklist will be dropped.

Report PBX's IP Blocklist

If the option is enabled, the IP addresses that are permanently blocked by the PBX will be reported to Yeastar Global Anti-hacking IP Blocklist.

Two-Factor Authentication

Yeastar P-Series PBX System supports to set two-factor authentication for super administrator account to ensure login security.

For more information, see Two-factor Authentication (2FA) Overview.

Enable IP Restriction for Administrator Login

Yeastar P-Series PBX System supports to add IP restrictions to specify the IP addresses from which super administrator are allowed to access administrator portal.

For more information, see Restrict Access to Administrator Portal by IP Addresses.

Console/SSH Access

Yeastar P-Series PBX System supports SSH access. Technical supporter engineers can establish a temporary SSH connection on the PBX to check logs and debug the PBX.

For more information, see Access the System via SSH.

Certificates

Yeastar P-Series PBX System supports TLS protocol and HTTPS protocol to secure SIP messaging. Before using TLS protocol and HTTPS protocol, you need to upload the relevant certificates to the PBX, or directly apply for a certificate on the PBX.

For more information, see the following topics:

- Manage TLS certificates on the PBX
- Manage HTTPS Certificates on the PBX

Allowed Country IPs

You can set up **Allowed Country IPs** to only allow specific countries or regions to access your phone system, thus preventing the situations that hackers 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.

For more information, see Restrict Specific Countries or Regions from Accessing Yeastar P-Series PBX System.

Allowed Country Codes

You can set up **Allowed Country Codes** to restrict users from making international calls to specific countries or regions, thus effectively preventing toll fraud.

For more information, see Restrict International Calls to Specific Countries or Regions.

Global Anti-hacking IP Blocklist Program

Download Yeastar Global Anti-hacking IP Blocklist

Yeastar Global Anti-hacking IP Blocklist is a central database of IP addresses that have been blocked by Yeastar PBX systems worldwide or that are suspected of malicious activity or attack. After downloading Yeastar Global Anti-hacking IP Blocklist, any connections to your PBX from the IP addresses in the blocklist will be dropped, reducing the risk of cyber attacks.

Procedure

1. Log in to PBX web portal, go to **Security > Security Settings**.
2. Click **Security Options** tab.
3. In the **Join Global Anti-hacking IP Blocklist Program** section, select the checkbox of **Download Global Anti-hacking IP Blocklist**.
4. Click **Save**.

Result

The IP blocklist is downloaded to the PBX; Any connections from the IP addresses in the blocklist will be dropped.

> **Note:**
> The IP blocklist will be automatically updated every 7 days to obtain the latest blocked IPs from Yeastar.

Report PBX's IP Blocklist to Yeastar Global Anti-hacking IP Blocklist

Yeastar Global Anti-hacking IP Blocklist is a central database of IP addresses that have been blocked by Yeastar PBX systems worldwide or that are suspected of malicious activity or attack. If you would like to contribute to the IP blocklist, you can share with Yeastar by reporting your system's IP blocklist. Yeastar security team will evaluate and analyze the reported addresses to ensure that only the malicious ones are added to the global blocklist.

Procedure

1. Log in to PBX web portal, go to **Security > Security Settings**.
2. Click **Security Options** tab.
3. In the **Join Global Anti-hacking IP Blocklist Program** section, select the checkbox of **Report PBX's IP Blocklist**.
4. Click **Save**.

Result

Permanent IP Blocklist of the PBX will be reported to Yeastar Global Anti-hacking IP Blocklist daily.

Note:

- Permanent IP Blocklist indicates the IP addresses on **Security > Security Rules > Blocked IPs**, which meet both of the following requirements:
  - **Block Type**: Block IP
  - **Expiration Date**: 12/30/2099 23:59:59
- To avoid legitimate VoIP servers or carriers being blocked, Yeastar security team will evaluate and analyze the IP addresses reported, then add the malicious ones to the global blocklist. The newly added IP addresses will be shared with all the users participating in the Yeastar Global Anti-hacking IP Blocklist Program.

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 web 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 web 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 web 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 web 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 web 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.

Related information

Import and Export -FAQ

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 web 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 web 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 web 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 web 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 web 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.

Related information

Import and Export -FAQ

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 web 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 web 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 Restriciton

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 web 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 web 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 web 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 web 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 web 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.

Related information

Import and Export -FAQ

Restrict Administrator Login

Restrict Access to Administrator Portal by IP Addresses

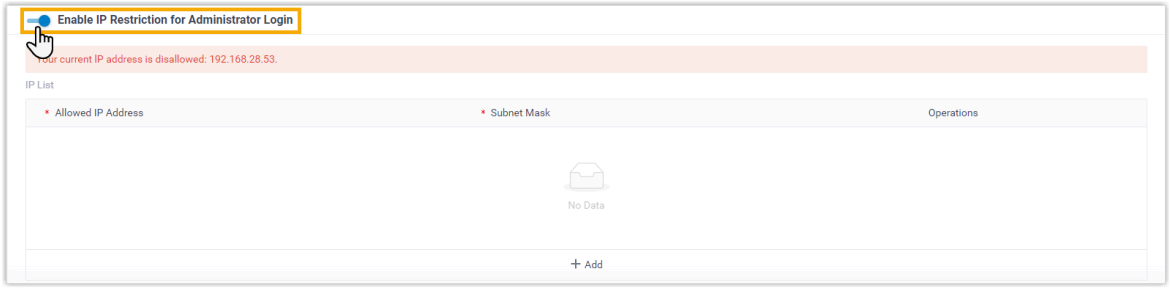
As a super administrator, you can add IP restrictions to specify the IP addresses from which super administrator are allowed to access administrator portal.

Requirements

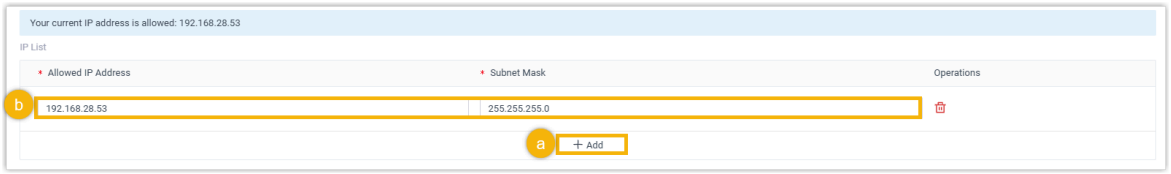
The firmware version of PBX server is 37.16.0.70 or later.

Procedure

1. Log in to PBX administrator portal, go to **Security > Security Settings > Security Options**.
2. Turn on the option **Enable IP Restriction for Administrator Login**.



   You are prompted that your current IP address is not allowed to log in to administrator portal.
3. Add one or more IPs.



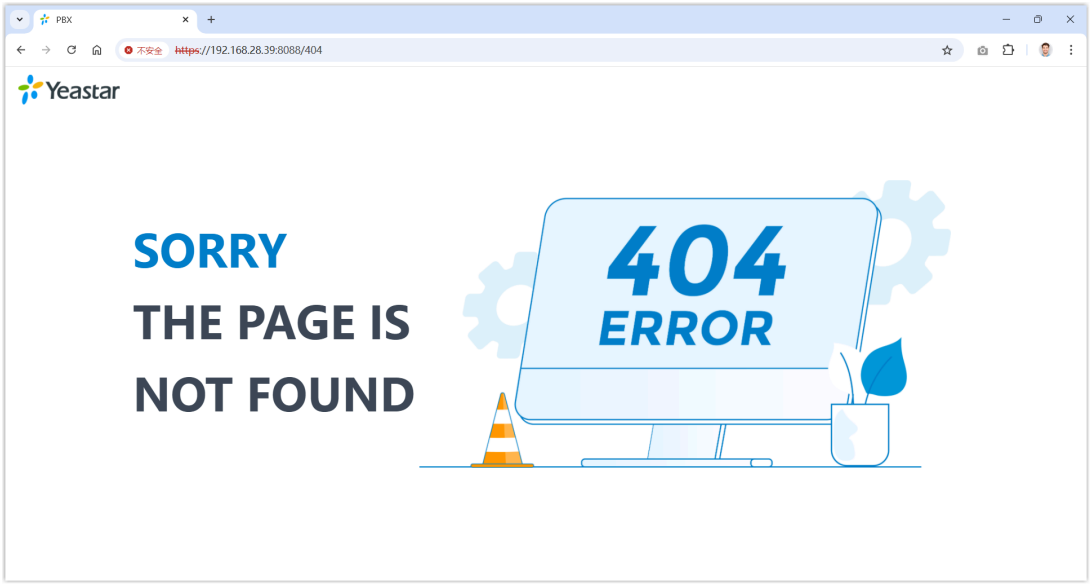
a. Click **Add**.
b. Enter the allowed IP address and the subnet mask.

> **Note:**
> The maximum number of allowed IP rule is 10.

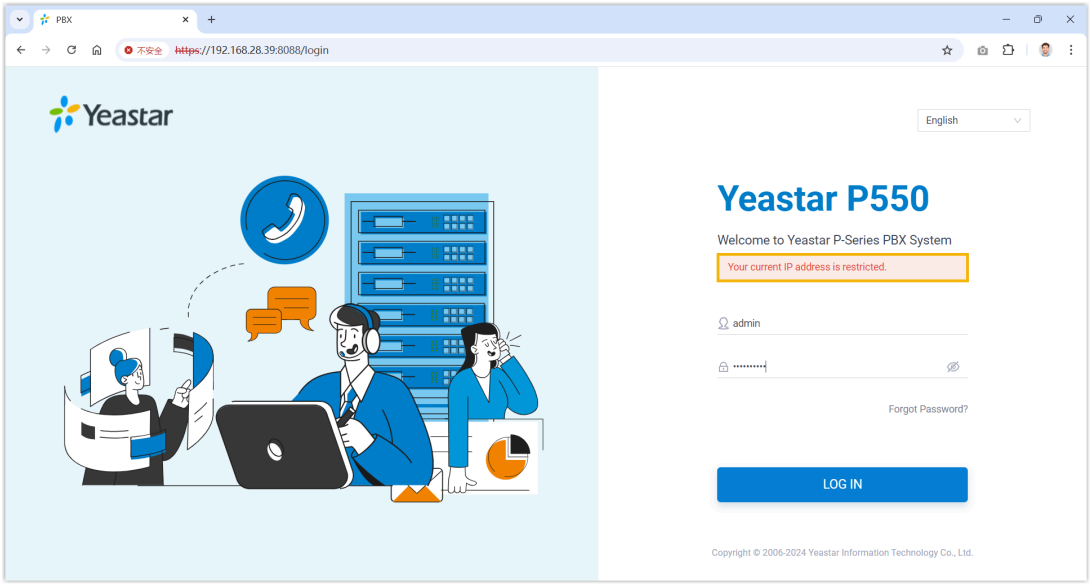
4. Click **Save**.

Result

- Only the allowed IP addresses can access PBX administrator portal, and the settings will take effect next time users log in. Users attempting to log in as super administrator from disallowed IP addresses will receive different prompts depending on the address they visit:
  - If a user logs in as super administrator using `PBX IP address/admin/login`, he or she will be prompted that the page is not found.

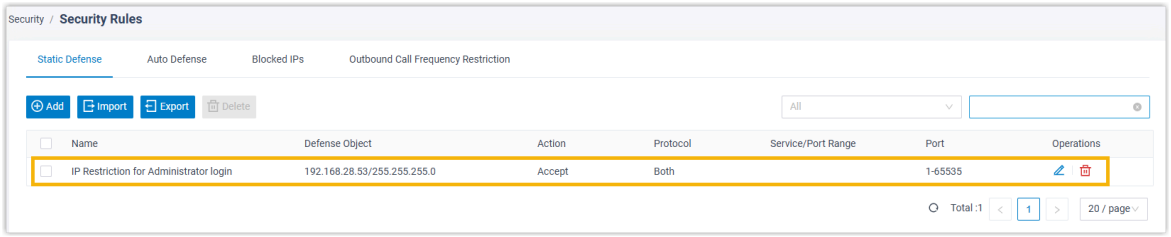


  - If a user logs in as super administrator using `PBX IP address/login`, he or she will be prompted that "Your current IP address is restricted".



- The IP address(es) are added to the system's static defense rules. You can check it on **Security > Security Rules > Static Defense**.

> **Note:**
> Changes made to the static defense will not be synchronized to the allowed IP list here.



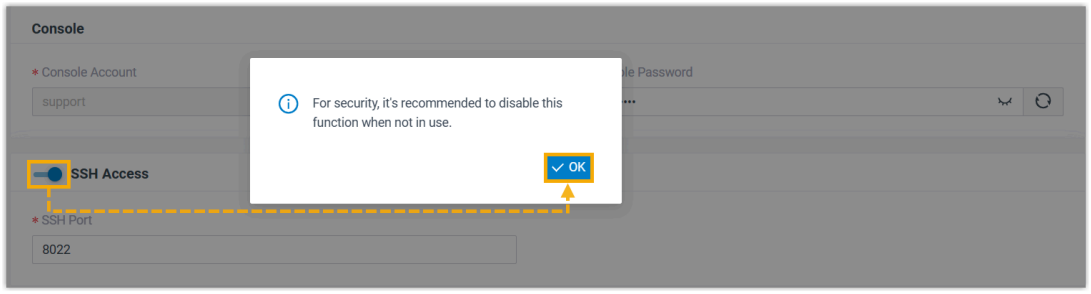
Console/SSH Access

Access the System via SSH

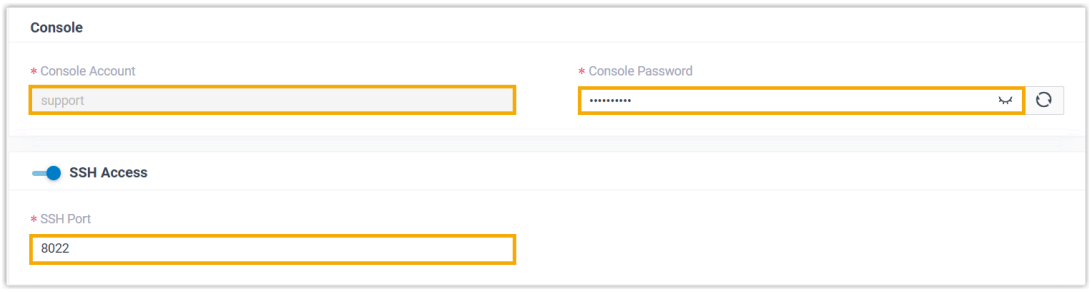
This topic takes Putty as an example to introduce how to access Yeastar P-Series PBX System via SSH.

Procedure

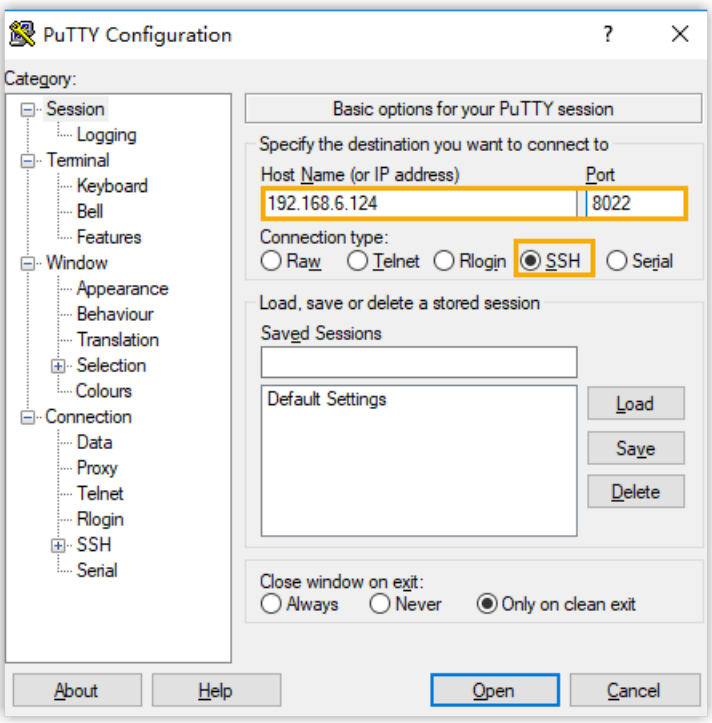
1. Enable SSH access on the PBX.
    a. Log in to PBX web portal, go to **Security > Security Settings > Console/SSH Access**.
    b. Turn on the switch of **SSH Access**, then click **OK**.



    c. Check and note down the SSH credentials.



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 scrollback 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. In the password field, enter the password.

Result

If the following figure shows, you can successfully access and debug the PBX.



Certificates

Manage TLS certificates on the PBX

Yeastar P-Series PBX System supports TLS protocol to secure SIP messaging. Before using TLS protocol, you may need to upload or apply for a TLS certificate on the PBX.

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. For more information, see Upload a TLS client certificate.
- 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 or apply for a server certificate. For more information, see Upload a TLS server certificate or Apply for a TLS server certificate.

Upload a TLS server certificate

Prerequisites

You have prepared a server certificate in `.pem` format.

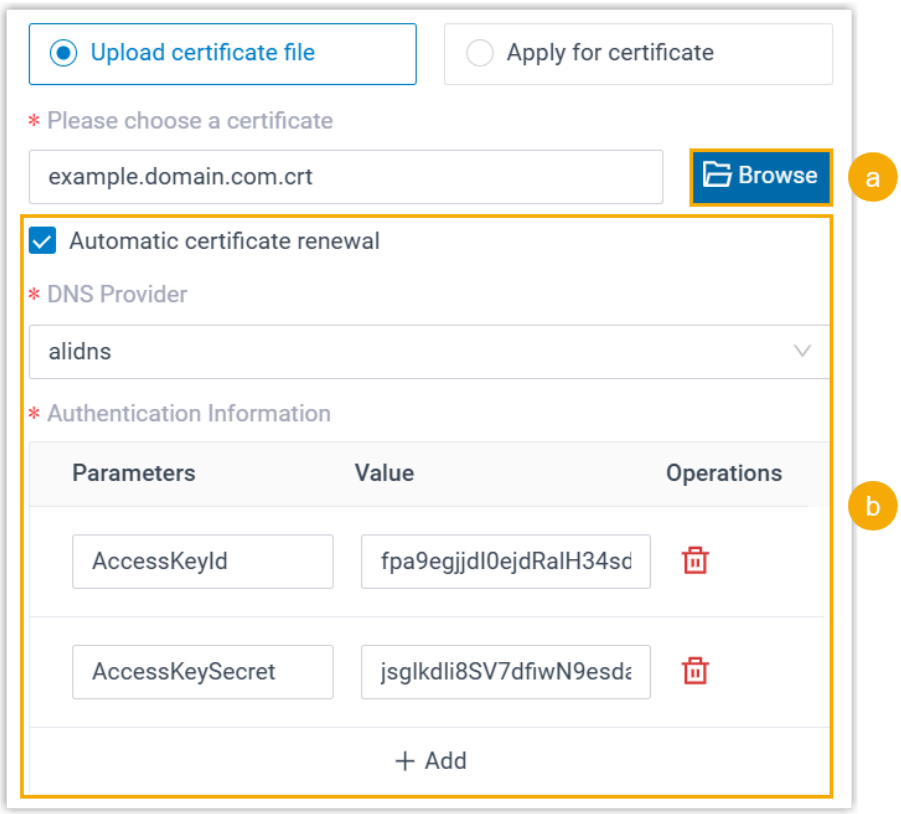
Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Certificates**, click **Add**.

   A window pops up, which requires you to select certificate type and upload a certificate.

   > **Note:**
   > You can ONLY upload or apply for 3 PBX certificates in total.

2. In the **Certificate Type** drop-down list, choose **PBX Certificate**.
3. Select **Upload certificate file**, and complete the following settings.



a. In the **Please choose a certificate** section, click **Browse** to select the desired certificate.
b. If you want the PBX to automatically renew the certificate, select the checkbox of **Automatic certificate renewal**, and provide the DNS provider information.

> **Note:**
> Only Let's Encrypt certificates can be automatically renewed. If the certificate is a non-Let's Encrypt certificate, the PBX will directly apply for a new Let's Encrypt certificate.

- **DNS Provider**: Search and select your desired DNS provider from the drop-down list.
- **Authentication Information**: Add one or more required authentication parameters, and enter the corresponding value.

> **Note:**
> For the specific authentication information of the DNS providers, see Supported DNS Providers.

4. Click **Save**.

Result

- The certificate is uploaded successfully, and is displayed on **Certificates** list.
- If you enable automatic certificate renewal, the system will automatically renew the certificate through the configured DNS provider 7 days before it expires.

Apply for a TLS server certificate

You can directly apply for a TLS server certificate on the PBX.

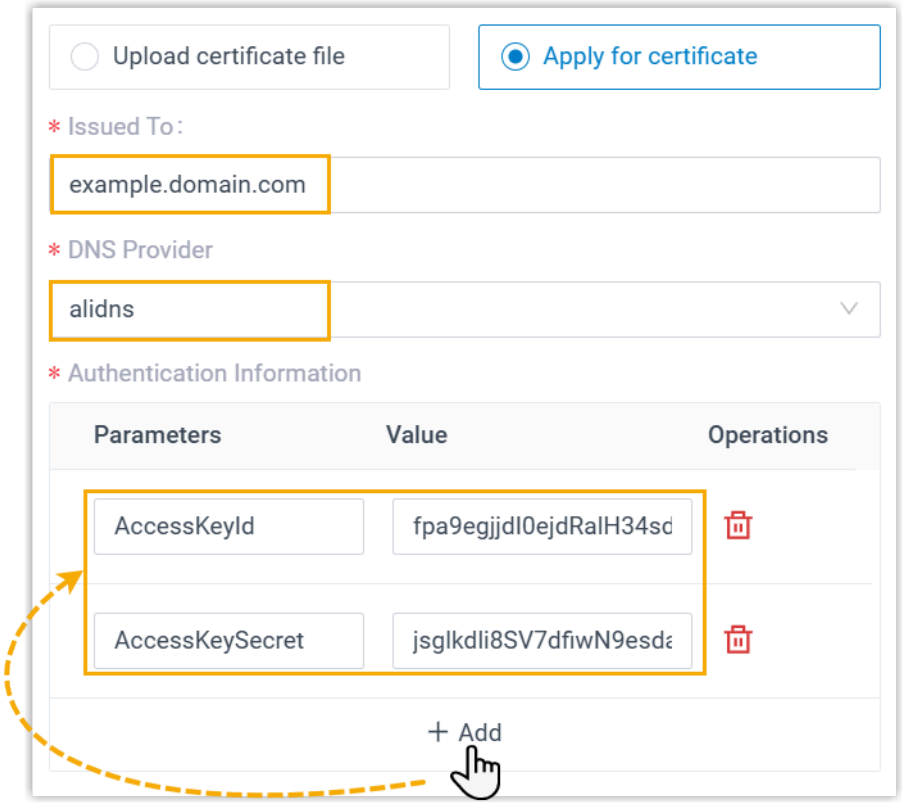
Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Certificates**, click **Add**.

   A window pops up, which requires you to select certificate type and upload a certificate.

   > **Note:**
   > You can ONLY upload or apply for 3 PBX certificates in total.

2. In the **Certificate Type** drop-down list, choose **PBX Certificate**.
3. Select **Apply for certificate**, and complete the following settings.



- **Issued To:**: Enter the domain name for which you want to apply for the certificate.
- **DNS Provider**: Search and select your desired DNS provider from the drop-down list.
- **Authentication Information**: Add one or more required authentication parameters, and enter the corresponding value.

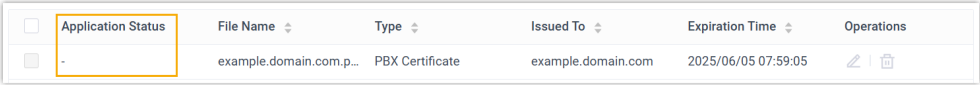
> **Note:**
> For the specific authentication information of the DNS providers, see Supported DNS Providers.

4. Click **Save**.

Result

- PBX will request a domain certificate from Let's Encrypt through the configured DNS provider. The obtained certificate files are named after the domain name.

- If the certificate is applied successfully, the **Application status** displays "-".



Upload a TLS client certificate

Prerequisites

You have prepared a client certificate in `.cer` or `.crt` format.

Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Certificates**, click **Add**.

   A window pops up, which requires you to select certificate type and upload a certificate.

   > **Note:**
   > You can ONLY upload 20 trusted 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.

Manage HTTPS Certificates on 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 or apply for 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.

Upload an HTTPS certificate

Prerequisites

You have prepared a server certificate in `.pem` format.

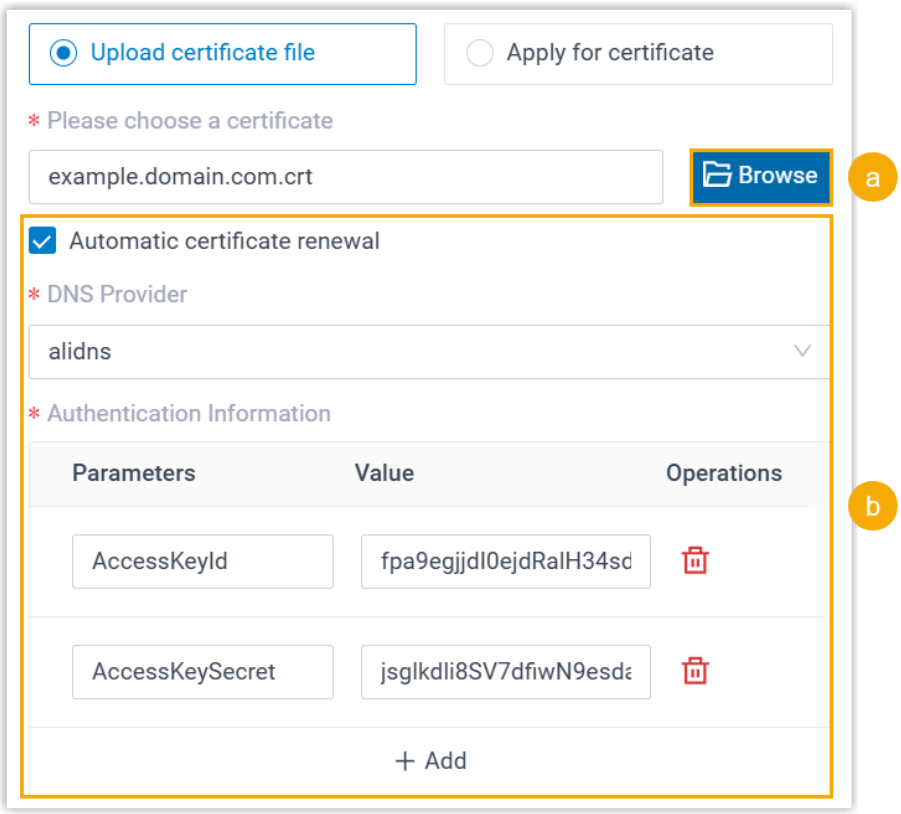
Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Certificates**, click **Add**.

   A window pops up, which requires you to select certificate type and upload a certificate.

   > **Note:**
   > You can ONLY upload or apply for 3 PBX certificates in total.

2. In the **Certificate Type** drop-down list, choose **PBX Certificate**.
3. Select **Upload certificate file**, and complete the following settings.



   a. In the **Please choose a certificate** section, click **Browse** to select the desired certificate.

b. If you want the PBX to automatically renew the certificate, select the checkbox of **Automatic certificate renewal**, and provide the DNS provider information.

> **Note:**
> Only Let's Encrypt certificates can be automatically renewed. If the certificate is a non-Let's Encrypt certificate, the PBX will directly apply for a new Let's Encrypt certificate.

- **DNS Provider**: Search and select your desired DNS provider from the drop-down list.
- **Authentication Information**: Add one or more required authentication parameters, and enter the corresponding value.

> **Note:**
> For the specific authentication information of the DNS providers, see Supported DNS Providers.

4. Click **Save**.

Result

- The certificate is uploaded successfully, and is displayed on **Certificates** list.
- If you enable automatic certificate renewal, the system will automatically renew the certificate through the configured DNS provider 7 days before it expires.

Apply for an HTTPS certificate

You can directly apply for a HTTPS certificate on the PBX.

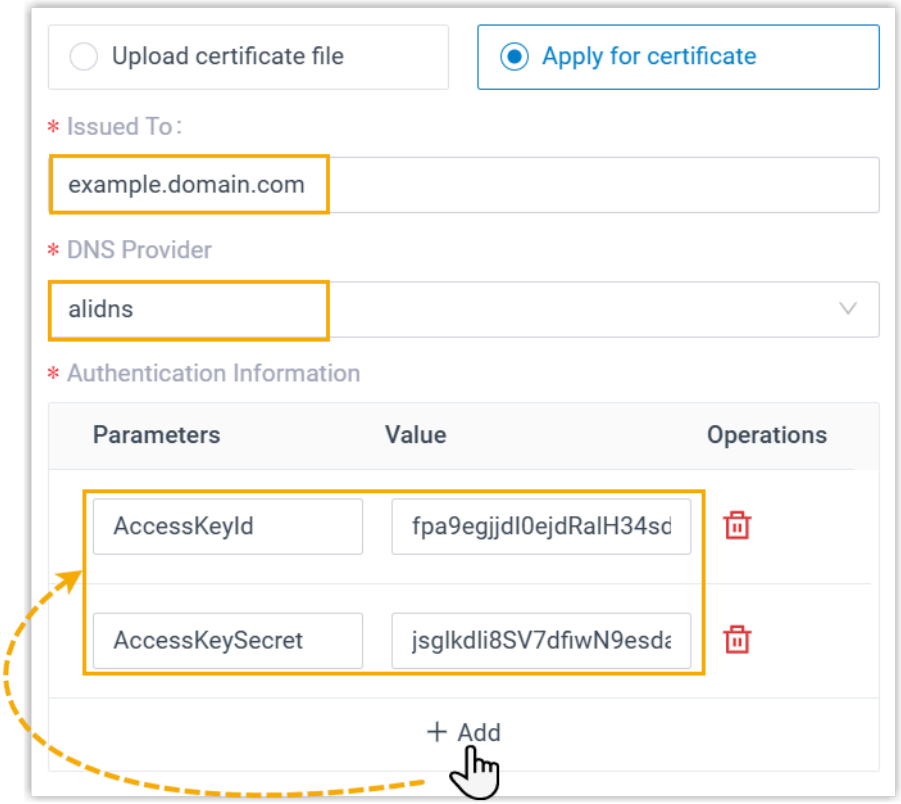
Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Certificates**, click **Add**.

   A window pops up, which requires you to select certificate type and upload a certificate.

> **Note:**
> You can ONLY upload or apply for 3 PBX certificates in total.

2. In the **Certificate Type** drop-down list, choose **PBX Certificate**.
3. Select **Apply for certificate**, and complete the following settings.



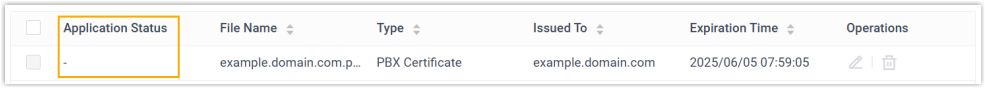
- **Issued To:**: Enter the domain name for which you want to apply for the certificate.
- **DNS Provider**: Search and select your desired DNS provider from the drop-down list.
- **Authentication Information**: Add one or more required authentication parameters, and enter the corresponding value.

> **Note:**
> For the specific authentication information of the DNS providers, see Supported DNS Providers.

4. Click **Save**.

Result

- PBX will request a domain certificate from Let's Encrypt through the configured DNS provider. The obtained certificate files are named after the domain name.
- If the certificate is applied successfully, the **Application status** displays "-".



Supported DNS Providers

This topic lists the DNS providers supported by PBX for automatic certificate request and renewal, and provides the description for their required authentication information parameters.

Note:

- You can use the flag name to search for the corresponding DNS provider.
- For parameters with default values, if a parameter is not specified, the system will automatically use its default value.

Provider Name	Flag Name	Supported Parameter
Akamai EdgeDNS	edgedns	• `Host`: API endpoint hostname, managed by the Akamai EdgeGrid client. • `ClientToken`: EdgeGrid client token, generated in the Akamai Control Center. • `ClientSecret`: EdgeGrid client secret, generated in the Akamai Control Center. • `AccessToken`: Access token, managed by the Akamai EdgeGrid client. • `PropagationTimeout`: Time between DNS propagation check in seconds. The default value is 15. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Alibaba Cloud DNS	alidns	• `AccessKeyId`: AccessKey ID. • `AccessKeySecret`: AccessKey secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
all-inkl	allinkl	• `Login`: KAS login username for authentication. • `Password`: KAS password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 60. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Amazon Route 53	route53	• `AccessKeyId`: AWS IAM Access Key ID. • `SecretAccessKey`: AWS IAM Secret Access Key. • `Region`: AWS region name (e.g., `us-east-1`). • `HostedZoneId`: Override the target hosted zone ID. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 120. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 10.
ArvanCloud	arvancloud	• `APIKey`: API key for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
Aurora DNS	auroradns	• `APIKey`: API key for authentication. • `Secret`: API secret paired with the API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Autodns	autodns	• `Username`: Autodns account username. • `Password`: Password for the Autodns account. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.

Provider Name	Flag Name	Supported Parameter
Azure DNS	azuredns	• `ResourceGroup`: Name of the resource group containing the DNS zone. • `TenantID`: Azure Active Directory tenant ID. • `ClientID`: Application (client) ID. • `ClientSecret`: Client secret for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Bindman	bindman	• `ManagerAddress`: Full URL of Bindman-DNS Manager server including scheme, hostname, and port (if required). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Bluecat	bluecat	• `ServerURL`: Full URL of BlueCat BAM server including scheme, hostname, and port. • `UserName`: API username. • `Password`: API password. • `DNSView`: Name of the external DNS view where records will be modified. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Bunny	bunny	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Checkdomain	checkdomain	• `Token`: API token for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Civo	civo	• `Token`: API token for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 30. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
Cloud.ru	cloudru	• `ServiceInstanceID`: Unique ID of the DNS service instance (parentId). • `KeyID`: API key ID (login credential). • `Secret`: API secret key for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
CloudDNS	clouddns	• `ClientID`: API Client ID. • `Email`: Account email. • `Password`: Account password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
Cloudflare	cloudflare	• `DnsApiToken`: API token with DNS:Edit permissions; can also be provided via `CF_DNS_API_TOKEN` environment variable. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
ClouDNS	cloudns	• `AuthID`: Main account ID (numeric) for API authentication. • `AuthPassword`: The password for the API user. • `SubAuthID`: Sub-account ID. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
ConoHa v2	conoha	• `Region`: Target region code (Default: `tyo1`). • `TenantID`: Project (tenant) ID. • `Username`: API username with DNS management permissions. • `Password`: API password for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Constellix	constellix	• `APIKey`: User API key. • `SecretKey`: Secret key paired with the API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Core-Networks	corenetworks	• `Login`: API account username with DNS management privileges. • `Password`: Corresponding account password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
CPanel/WHM	cpanel	• `Mode`: API type (`cpanel` = per-account, `whm` = server-wide). The default is `cpanel`. • `Username`: cPanel account username (for `cpanel` mode) or WHM root username (for `whm` mode). • `Token`: API authentication token. • `BaseURL`: Server API endpoint. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Derak Cloud	derak	• `APIKey`: Account authentication key. • `WebsiteID`: Explicitly specify target zone ID (override auto-detection) • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
deSEC.io	desec	• `Token`: Domain-specific API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Digital Ocean	digitalocean	• `BaseURL`: API endpoint URL. • `AuthToken`: Authentication token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 10.
DirectAdmin	directadmin	• `BaseURL`: The URL of the API. • `Username`: API username. • `Password`: API password. • `ZoneName`: The domain name (DNS zone) where the TXT record will be added. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 10.
DNS Made Easy	dnsmadeeasy	• `APIKey`: The API key. • `APISecret`: The API secret. • `Sandbox`: Activate the sandbox (boolean, the default value is `false`). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
dnsHome.de	dnshomede	• `Credentials`: Comma-separated list of `domain:password` credential pairs. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5.
DNSimple	dnsimple	• `AccessToken`: Your DNSimple API access token used for authentication. • `BaseURL`: The base URL for the DNSimple API. E.g. `https://api.dnsimple.com`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Domain Offensive (do.de)	dode	• `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5.
Domeneshop	domeneshop	• `APIToken`: API token. • `APISecret`: API secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 20.
DreamHost	dreamhost	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 3600. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 60.
Duck DNS	duckdns	• `Token`: Your DuckDNS account token used for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5.

Provider Name	Flag Name	Supported Parameter
Dyn	dyn	• `CustomerName`: Your Dyn customer account name. • `UserName`: Your Dyn Managed DNS username. • `Password`: The password associated with your Dyn Managed DNS username. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Dynu	dynu	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
EasyDNS	easydns	• `Endpoint`: (Optional) The base URL of the EasyDNS API server. • `Token`: API token. • `Key`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Efficient IP	efficientip	• `Username`: API username. • `Password`: Password associated with the API username. • `Hostname`: The Fully Qualified Domain Name (FQDN) of the DNS record to be managed. E.g. `foo.example.com`. • `DNSName`: The name of the DNS zone where the record resides. E.g. `dns.smart`. • `ViewName`: The DNS view name associated with the zone. E.g. `external`. • `InsecureSkipVerify`: Whether to skip SSL certificate verification when connecting to the EfficientIP API (Boolean, the default value is `false`, which means certificate verification is enabled to ensure secure connections). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Epik	epik	• `Signature`: Epik API signature. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Gandi	gandi	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 2400. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 60. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Gandi Live DNS (v5)	gandiv5	• `PersonalAccessToken`: Personal access token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 20. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Glesys	glesys	• `APIUser`: API username. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 20. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Go Daddy	godaddy	• `ApiKey`: API key. • `ApiSecret`: API secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
Google Cloud	gcloud	• `ServiceAccount`: Your Google Cloud service account. • `Project`: The Google Cloud project ID. If not specified, it will be automatically detected using the metadata server.

Provider Name	Flag Name	Supported Parameter
		• `ZoneID`: The managed zone name. Providing this skips automatic zone detection. • `AllowPrivateZone`: Allows the use of private DNS zones. This is supported only with a private ACME server (Boolean, the default value is `false`). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Google Domains	googledomains	• `AccessToken`: Access token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Hetzner	hetzner	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Hosting.de	hostingde	• `APIKey`: API key. • `ZoneName`: The DNS zone name in ACE (ASCII Compatible Encoding) format. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Hosttech	hosttech	• `APIKey`: API login key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 120. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
http.net	httpnet	• `APIKey`: API key. • `ZoneName`: The DNS zone name in ACE (ASCII Compatible Encoding) format.

Provider Name	Flag Name	Supported Parameter
		• `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Huawei Cloud	huaweicloud	• `AccessKeyId`: Huawei Cloud API access key ID. • `SecretAccessKey`: The secret key associated with your access key ID. • `Region`: Huawei Cloud region where your DNS service is located. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Hurricane Electric DNS	hurricane	• `Credentials`: List of TXT record names and corresponding tokens required to complete the DNS-01 challenge. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
IBM Cloud (SoftLayer)	ibmcloud	• `Username`: Username. • `APIKey`: API key for accessing the Classic Infrastructure services. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
IIJ DNS Platform Service	iijdpf	• `Token`: API token. • `ServiceCode`: The service code for IIJ Managed DNS Service. • `Endpoint`: The API endpoint URL. Defaults to `https://api.dns-platform.jp/dpf/v1`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Infoblox	infoblox	• `Host`: The base URI of the Infoblox grid manager API. • `Port`: Port number used to connect to the Infoblox grid manager. The default value is 443. • `Username`: Username for account authentication. • `Password`: Password for the account. • `DNSView`: The DNS view where the TXT records are managed. The default value is `External`. • `WapiVersion`: Version of the Infoblox WAPI (Web API) in use. The default value is `2.11`. • `SSLVerify`: Whether to verify the TLS certificate or not (Boolean, the default value is `true`). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Infomaniak	infomaniak	• `APIEndpoint`: Your infomaniak API endpoint URL. The default value is `https://api.infomaniak.com`. • `AccessToken`: Access token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Internet Initiative Japan	iij	• `AccessKey`: API access key. • `SecretKey`: API secret key. • `DoServiceCode`: The service code for IIJ Managed DNS. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Internet.bs	internetbs	• `APIKey`: API key. • `Password`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
INWX	inwx	• `Username`: Your account username. • `Password`: The password for your account. • `SharedSecret`: The shared secret key used for two-factor authentication (2FA). • `Sandbox`: Activate the sandbox (Boolean, the default value is `false`). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Ionos	ionos	• `APIKey`: API key in the format `prefix.secret`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
IPv64	ipv64	• `APIKey`: Account API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
iwantmyname	iwantmyname	• `Username`: API username. • `Password`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Joker	joker	• `APIKey`: API key, used only in DMAPI mode. • `Username`: Your Joker account username. • `Password`: Your Joker account password. • `APIMode`: API mode, either `DMAPI` or `SVC`. Default is `DMAPI`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Liara	liara	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Lima-City	limacity	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Linode (v4)	linode	• `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Liquid Web	liquidweb	• `BaseURL`: Liquid Web API endpoint URL. • `Username`: Liquid Web API username. • `Password`: Liquid Web API password. • `Zone`: DNS zone name. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Loopia	loopia	• `BaseURL`: API endpoint URL. E.g. `https://api.loopia.se/RPCSERV` (default) or `https://api.loopia.rs/RPCSERV`. • `APIUser`: API username. • `APIPassword`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 2400. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
LuaDNS	luadns	• `APIUsername`: Your username, which is your email address. • `APIToken`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Mail-in-a-Box	mailinabox	• `Email`: Email address. • `Password`: Password. • `BaseURL`: Base URL of the API (e.g. `https://box.example.com`). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
ManageEngine CloudDNS	manageengine	• `ClientID`: Client ID. • `ClientSecret`: Client secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Metaname	metaname	• `AccountReference`: The four-digit identifier for your Metaname account. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
mijn.host	mijnhost	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.

Provider Name	Flag Name	Supported Parameter
Mittwald	mittwald	• `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
MyDNS.jp	mydnsjp	• `MasterID`: Master ID. • `Password`: Password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
MythicBeasts	mythicbeasts	• `UserName`: Username. • `Password`: Password. • `APIEndpoint`: The API endpoint (must support v2). • `AuthAPIEndpoint`: The endpoint for Mythic Beasts' Authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Name.com	namedotcom	• `Username`: Username. • `ApiToken`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 20. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Namecheap	namecheap	• `BaseURL`: Your Namecheap API base URL. • `APIUser`: API user. • `APIKey`: API key. • `ClientIP`: The IP address authorized to access the API. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Namesilo	namesilo	• `ApiKey`: API key.

Provider Name	Flag Name	Supported Parameter
		• `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
NearlyFreeSpeech.NET	nearlyfreespeech	• `APIKey`: API key used for authenticating API requests. • `Login`: Username associated with your NearlyFreeSpeech.NET account. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Netcup	netcup	• `Key`: API key. • `Password`: API password. • `Customer`: Your Netcup customer number. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Netlify	netlify	• `Token`: Token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Nicmanager	nicmanager	• `Login`: Your login name for username-based authentication. • `Username`: Alternate field for username-based login (used interchangeably with `Login`). • `Email`: Email address used for email-based login. • `Password`: The account password. • `OTPSecret`: TOTP (Time-based One-Time Password) secret for two-factor authentication. • `Mode`: DNS mode, either `anycast` (default) or `zone`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 900.
NIFCloud	nifcloud	• `BaseURL`: The base URL for the NIFCloud API. • `AccessKey`: Access key. • `SecretKey`: Secret access key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Njalla	njalla	• `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Nodion	nodion	• `APIToken`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
NS1	ns1	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Open Telekom Cloud	otc	• `IdentityEndpoint`: The endpoint URL for identity authentication. • `DomainName`: The domain name associated with your account. • `ProjectName`: The name of the project under your account. • `UserName`: Username. • `Password`: Password.

Provider Name	Flag Name	Supported Parameter
		• `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Oracle Cloud	oraclecloud	• `CompartmentID`: The OCID of your Oracle Cloud compartment. • `Tenancy`: The OCID of your tenancy. • `User`: The OCID of your user account. • `Region`: The Oracle Cloud region to use. • `Fingerprint`: The fingerprint of your API public key. • `PrivateKey`: Path to your API private key file. • `PrivateKeyPassphrase`: The passphrase for the private key, if set. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
OVH	ovh	• `APIEndpoint`: Endpoint URL, typically `ovh-eu` or `ovh-ca`. • `ApplicationKey`: Application key used for Application Key authentication. • `ApplicationSecret`: Application secret used for Application Key authentication. • `ConsumerKey`: Consumer key used for Application Key authentication. • `OAuth2ClientID`: Client ID used for OAuth2 authentication. • `OAuth2ClientSecret`: Client secret used for OAuth2 authentication. • `AccessToken`: Access token for OAuth2 authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
plesk.com	plesk	• `BaseURL`: Base URL of the Plesk server. • `Username`: API username. • `Password`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Porkbun	porkbun	• `APIKey`: API key. • `SecretAPIKey`: Secret API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
PowerDNS	powerdns	• `ApiUrl`: API URL. • `ApiKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Rackspace	rackspace	• `APIUser`: API user. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Rain Yun	rainyun	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
RcodeZero	rcodezero	• `APIToken`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.

Provider Name	Flag Name	Supported Parameter
reg.ru	regru	• `Username`: API username. • `Password`: API password • `TLSCert`: Authentication certificate. • `TLSKey`: Authentication private key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Regfish	regfish	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
RFC2136	rfc2136	• `Nameserver`: Network address in the format `host` or `host:port`. • `TSIG`: Path to the key file generated by `tsig-keygen`. • `TSIGAlgorithm`: TSIG algorithm. Refer to here for supported values. To disable TSIG authentication, leave `RFC2136_TSIG_KEY` or `RFC2136_TSIG_SECRET` unset. • `TSIGKey`: Name of the secret key as defined in DNS server configuration. To disable TSIG authentication, leave `RFC2136_TSIG_KEY` unset. • `TSIGSecret`: Secret key value. To disable TSIG authentication, leave `RFC2136_TSIG_SECRET` unset. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
RimuHosting	rimuhosting	• `APIKey`: User API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Sakura Cloud	sakuracloud	• `Token`: Access token. • `Secret`: Access token secret.

Provider Name	Flag Name	Supported Parameter
		• `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Scaleway	scaleway	• `ProjectID`: Project ID. • `AccessKey`: Access key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Selectel	selectel	• `BaseURL`: API endpoint URL. • `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Selectel v2	selectelv2	• `BaseURL`: API endpoint URL. • `Username`: Openstack username. • `Password`: Password for the OpenStack username. • `Account`: Selectel account ID (integer). • `ProjectID`: Cloud project ID (UUID). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
SelfHost.(de|eu)	selfhostde	• `Username`: Username. • `Password`: Password. • `RecordsMapping`: Mapping of record IDs to domains. E.g. `"example.com":["123","456"],"example.org":["789"],"foo.example.com":["147"]`.
Servercow	servercow	• `Username`: API username. • `Password`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Shellrent	shellrent	• `Username`: Username. • `Token`: Token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Simply.com	simply	• `AccountName`: Account name. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Sonic	sonic	• `UserID`: User ID. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Stackpath	stackpath	• `ClientID`: Client ID. • `ClientSecret`: Client Secret. • `StackID`: Stack ID. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Technitium	technitium	• `BaseURL`: Server base URL. • `APIToken`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Tencent Cloud DNS	tencentcloud	• `SecretId`: Access key ID. • `SecretKey`: Access Key secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 0. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 0.
Timeweb Cloud	timewebcloud	• `AuthToken`: Authentication token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
TransIP	transip	• `AccountName`: Account name. • `PrivateKey`: Path to the private key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 10.
UKFast SafeDNS	safedns	• `AuthToken`: Authentication token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Ultradns	ultradns	• `Username`: API username. • `Password`: API password. • `Endpoint`: API endpoint URL, defaults to `https://api.ultradns.com/`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Variomedia	variomedia	• `APIToken`: API token.

Provider Name	Flag Name	Supported Parameter
		• `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
VegaDNS	vegadns	• `BaseURL`: API endpoint URL. • `APIKey`: API key. • `APISecret`: API secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 10.
Vercel	vercel	• `AuthToken`: Authentication token. • `TeamID`: Team ID (E.g. `team_xxxx`) • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Versio.[nl|eu|uk]	versio	• `BaseURL`: The endpoint URL of the API Server,optional, defaults to `https://www.versio.nl/api/v1/`. • `Username`: Basic authentication username. • `Password`: Basic authentication password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
VinylDNS	vinyldns	• `AccessKey`: The VinylDNS API key. • `SecretKey`: The VinylDNS API Secret key. • `Host`: The VinylDNS API URL. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 30.
VK Cloud	vkcloud	• `ProjectID`: String ID of project in VK Cloud. • `Username`: Email of VK Cloud account. • `Password`: Password for VK Cloud account.

Provider Name	Flag Name	Supported Parameter
		• `DNSEndpoint`: URL of DNS API. Defaults to `https://mcs.mail.ru/public-dns` but can be changed for private clouds. • `IdentityEndpoint`: URL of OpenStack Auth API, Defaults to `https://infra.mail.ru:35357/v3/` but can be changed for usage with private clouds. • `DomainName`: Openstack users domain name. Defaults to `users` but can be changed for private clouds. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Volcano Engine	volcengine	• `AccessKeyId`: Access key ID (AK). • `SecretAccessKey`: Secret access key (SK). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
Vscale	vscale	• `BaseURL`: API endpoint URL. • `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Vultr	vultr	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Webnames	webnames	• `APIKey`: Domain API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Websupport	websupport	• `APIKey`: API key.

Provider Name	Flag Name	Supported Parameter
		• `Secret`: API secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
WEDOS	wedos	• `Username`: Username is the same as the admin account. • `Password`: Password must be generated and the IP address allowed in the admin interface. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
West.cn	westcn	• `Username`: Username. • `Password`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Yandex 360	yandex360	• `OAuthToken`: The OAuth Token. • `OrgID`: The organization ID. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 21600.
Yandex Cloud	yandexcloud	• `IamToken`: The base64-encoded JSON containing IAM token info of a service account with `dns.admin` permissions. • `FolderID`: The string ID of the folder (i.e. project) in Yandex Cloud. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.

Provider Name	Flag Name	Supported Parameter
Yandex PDD	yandex	• `PddToken`: Basic authentication username. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 21600.
Zone.ee	zoneee	• `Endpoint`: API endpoint URL. • `Username`: API user. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Zonomi	zonomi	• `APIKey`: User API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.

Delete Certificates

This topic describes how to delete one or more certificates on Yeastar P-Series PBX System.

Procedure

1. Log in to PBX web 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

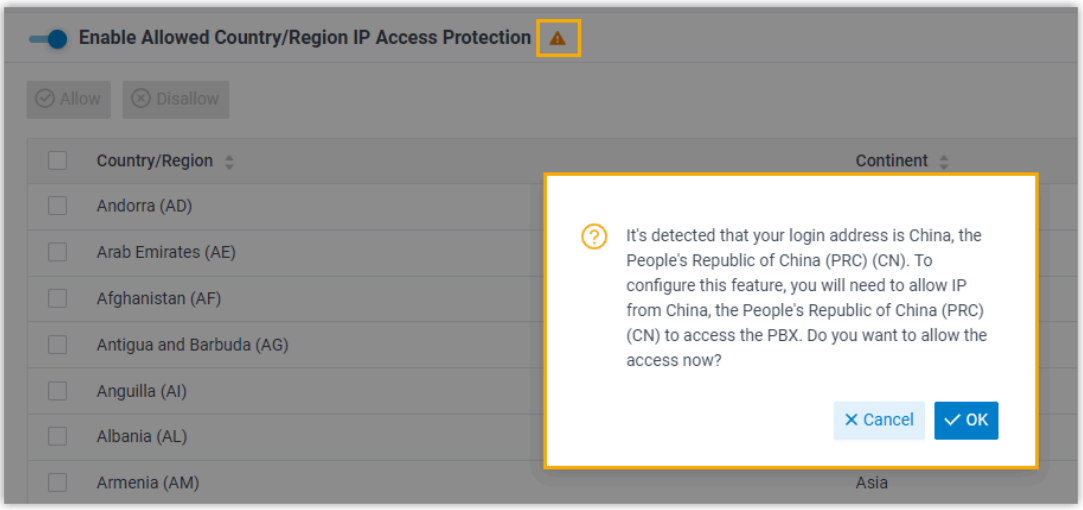
Restrict Specific Countries or Regions from Accessing Yeastar P-Series PBX System

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.

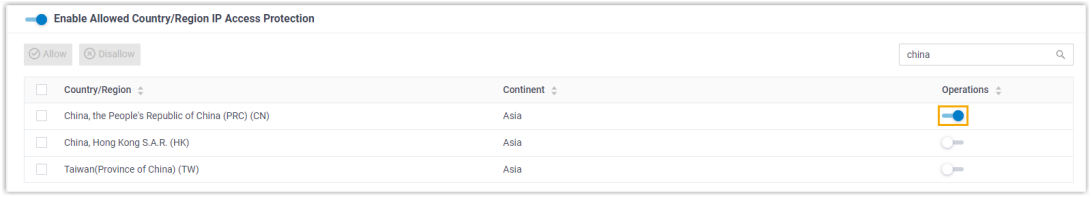
Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Allowed Country IPs**.
2. Turn on the option **Enable Allowed Country/Region IP Access Protection**.

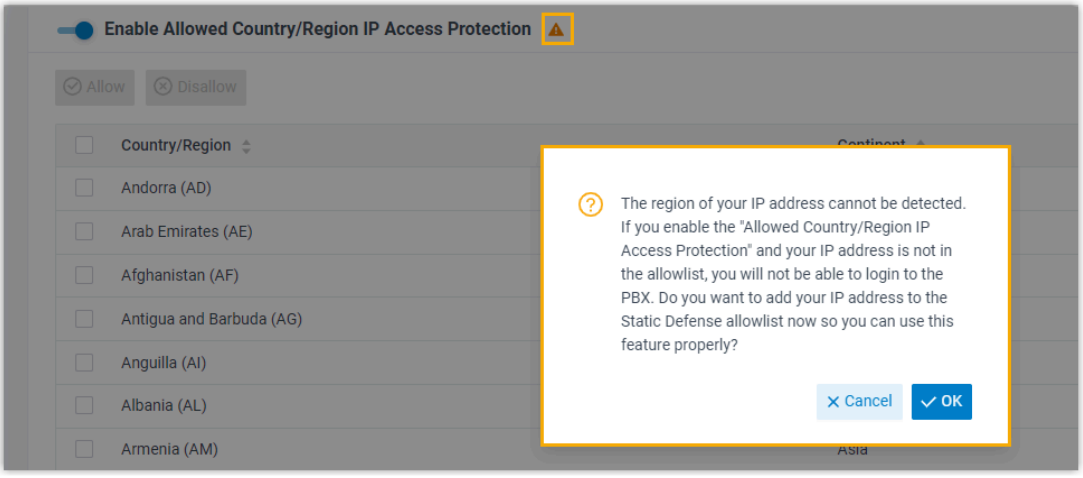
   The system tries to identify whether the connection from your current IP address is accepted in the Static Defense allowlist of your PBX.
3. If current IP address is not accepted in the Static Defense allowlist of your PBX, the system would try to identify the country/region from which your current IP address is originated. You need to allow connections from your current country/region. Otherwise, you can NOT enable and use the IP access protection feature.
   - If the system successfully detects your country/region, a warning icon and a pop-up window will be displayed, prompting you to allow access for your current country/region.



You should click **OK** to allow IPs from your current country/region to access the PBX. In doing so, the warning icon is disappeared, and operation status of your country/region is changed to .

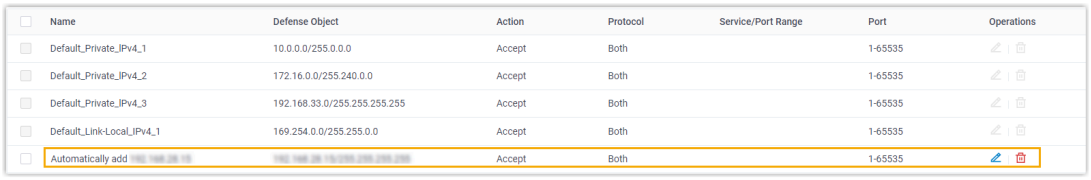


- If the system fails to detect your country/region, a warning icon and a pop-up window will be displayed, prompting you to allow access for your current IP address.

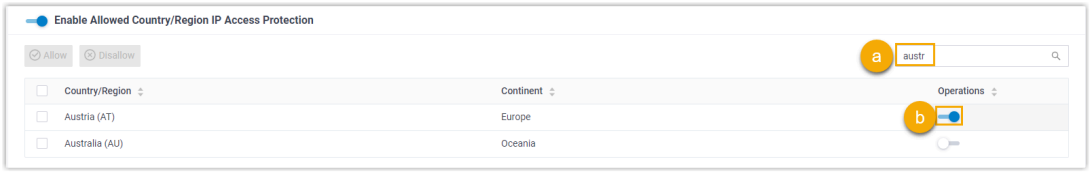


You should click **OK** to add your IP address to the Static Defense allowlist. In doing so, the warning icon is disappeared, and connections from your IP address are accepted.

> **Tip:**
> You can check the added IP address on **Security > Security Rules > Static Defense**.



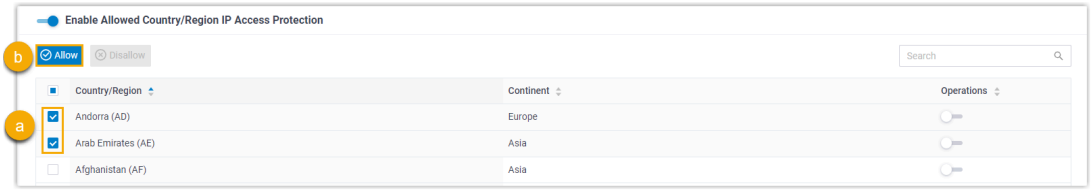
4. To allow desired countries/regions to access the PBX, do as follows:
   - To allow a country/region to access the PBX, do as follows:



     a. In the search box, enter a desired country or region.

     b. In the **Operations** column, set the status to .

   - To allow multiple countries/regions to access the PBX, do as follows:



     a. Select the checkboxes of desired countries or regions.

     b. Click **Allow**.

     The status will be changed to .

5. Click **Apply**.

Result

Only the devices with IP addresses originating from the allowed countries or regions can access the PBX.

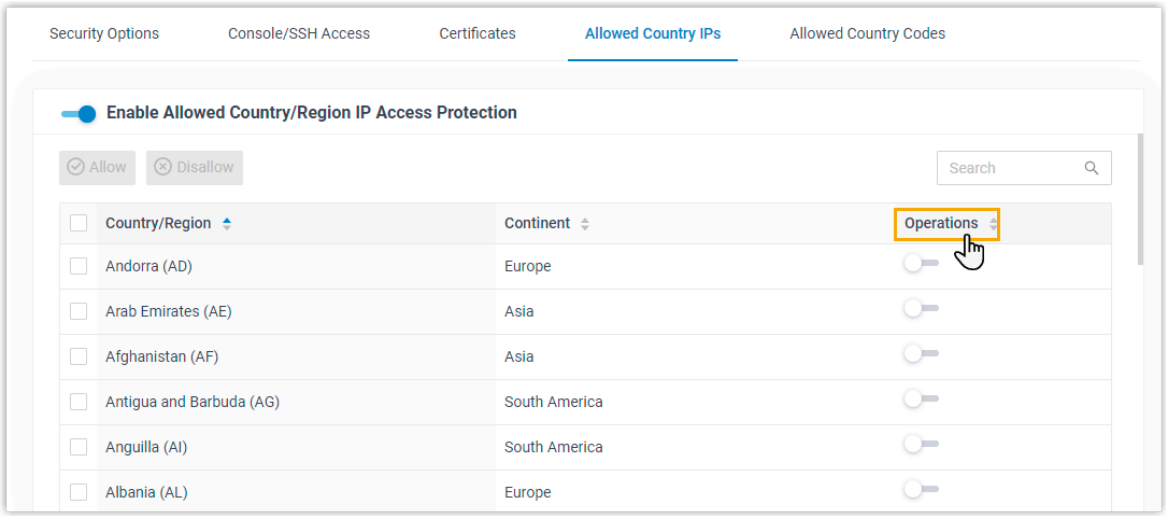
Tip:
For the disallowed countries or regions, if you want to allow a specific IP address to access the PBX, you can add a static defense rule to accept connections from the desired IP address. For more information, see Add a Static Defense Rule.

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.

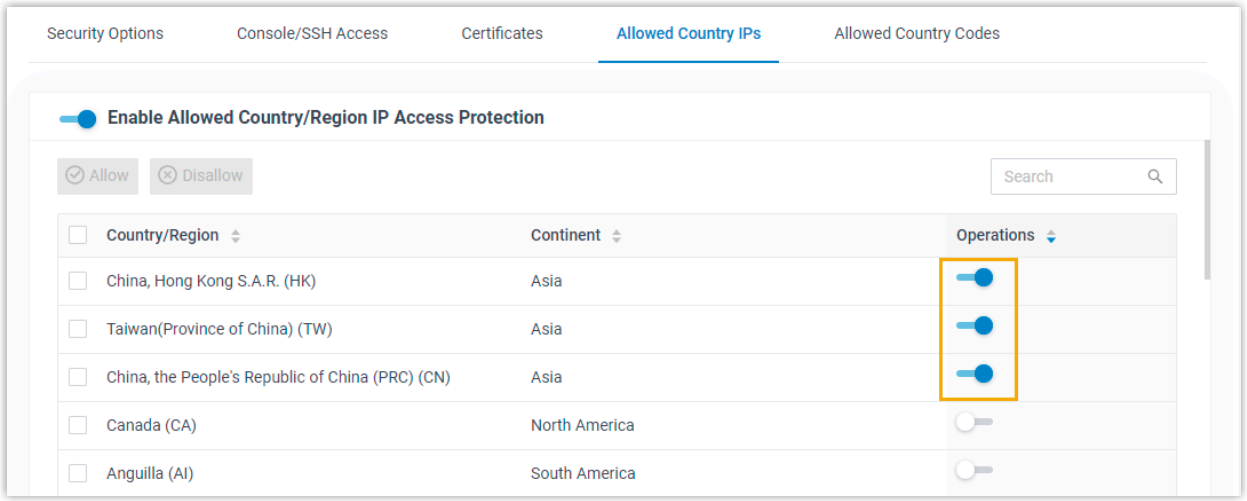
Procedure

1. Log in to PBX web 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

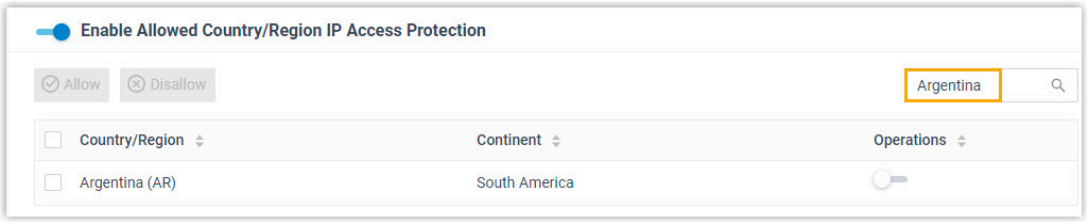
Step1. Allow international calls to Argentina only

1. Log in to PBX web 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*.

    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 region, 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.

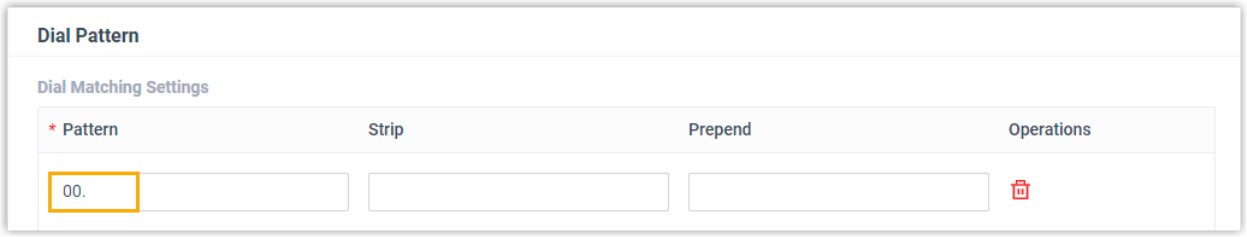
1. Go to **Extension and Trunk > Extension**.

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:



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 web 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.

Two-Factor Authentication (2FA)

Two-factor Authentication (2FA) Overview

Yeastar P-Series PBX System supports to configure two-factor authentication (2FA) for super administrator account. With 2FA enabled, both the account password and an additional authentication code are required for login, which adds an extra layer of security to the PBX. This topic provides an overview of the supported two-factor authentication methods.

> **Note:**
> Extension users can also configure two-factor authentication for their own accounts on Linkus **Web Client** or **Desktop Client**, and the configuration will be applied to all their Linkus clients.
>
> For more information, see Two-factor Authentication (2FA) on Linkus Web Client and Two-factor Authentication (2FA) on Linkus Desktop Client.

Requirements

Yeastar P-Series PBX System is 37.10.0.30 or later.

Two-factor authentication by authenticator application

This method requires you to install an authenticator application on your mobile phone. The supported applications are listed below:

- Google Authenticator
- FreeOTP
- Twilio Authy
- Microsoft Authenticator

After installing an authenticator application, you need to add your account to the application, via which you can obtain authentication codes for two-factor authentication. When you log in to the super administrator account, both account password and the authentication code generated by the authenticator application are required.

For more information about the configuration, see Configure Two-factor Authentication using Authenticator Application.

Two-factor authentication by Email

This method allows you to receive authentication codes for two-factor authentication via the email associated with the super administrator account. When you log in to the super administrator account, both account password and the authentication code sent to your email are required.

For more information about the configuration, see Configure Two-factor Authentication using Email.

Configure Two-factor Authentication using Authenticator Application

This topic describes how to configure two-factor authentication for super administrator account using an authenticator application on your mobile phone.

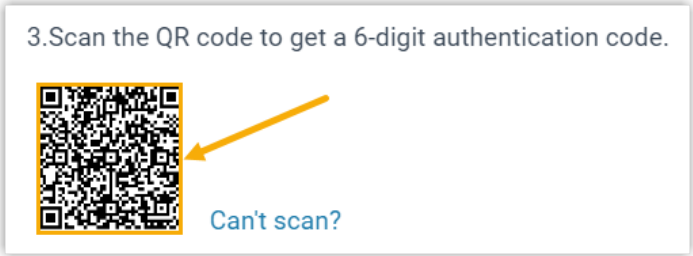
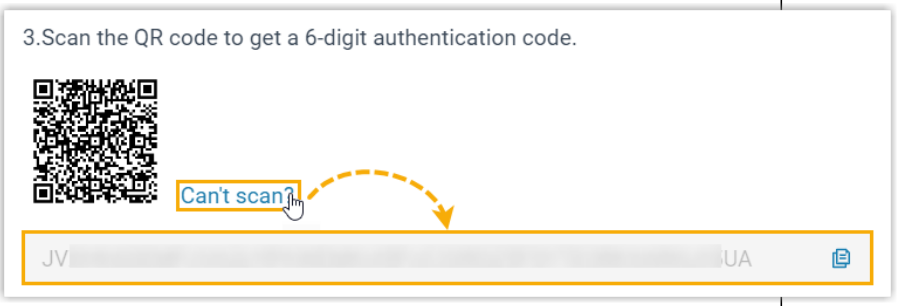
Prerequisites

You have installed one of the following supported authenticator applications on your mobile phone.

- Google Authenticator
- FreeOTP
- Twilio Authy
- Microsoft Authenticator

Procedure

1. Log in to PBX web portal, click your account at the top-right corner, then go to **Change Password & Security > Security Settings**.
2. Select the checkbox of **Two-Factor Authentication**.
3. In the pop-up **Password** window, enter your account password and click **Confirm** to verify your operation.
4. Select **Authenticated by Authenticator**.
5. Add your account to the authenticator application via either of the following methods.

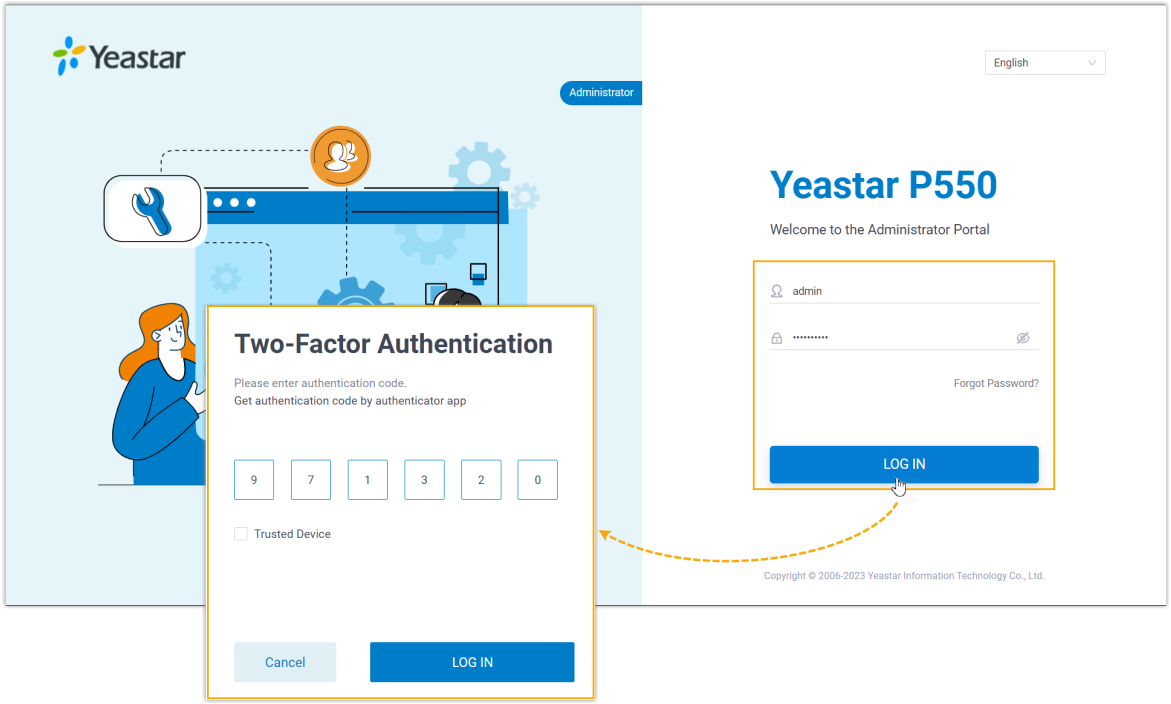
Method	Instruction
Scan QR Code to quickly add the account	You can quickly add your account to the authenticator application by scanning the QR code provided by PBX. a. On your mobile phone, open the authenticator application, and select to scan QR code. b. Scan the QR code shown on PBX web portal.  Your account is added to the application automatically, a 6-digit authentication code is shown.
Manually add the account	In case you can not scan QR code, you can manually add your account and enter the secret key provided by PBX. a. On PBX web portal, click **Can't scan** beside the QR code. PBX will generate a secret key, note it down for later use.  b. On your mobile phone, open the authenticator application, and select to manually add an account. c. Enter the relevant information, and paste the secret key. **Note:** If you need to complete more configurations for the secret key, you should set **SHA1** as the algorithm for **TOTP** protocol, and set to generate **6-digit** code with an interval of **30** seconds. Your account is added to the application, a 6-digit authentication code is shown.

6. On PBX web portal, enter the 6-digit authentication code in the **Authentication Code** field.
7. Click **Save**.

Result

- The webpage prompts a message "Edited successfully.", which means that you have successfully set up two-factor authentication.
- Next time you log in to PBX web portal, you need to enter an authentication code additionally.

> **Note:**
> For the device from which you log in most frequently, you can select the checkbox of **Trusted Device** to add it as a trusted device. In this way, you don't have to re-enter an authentication code with this device for the next 180 days.



> **Troubleshooting:**
> **What if my extension users fail to log in with two-factor authentication?**

You can disable two-factor authentication for their extension accounts, so that they can directly log in with their username and password.

Related information

Manage Two-factor Authentication of Super Administrator Account

Configure Two-factor Authentication using Email

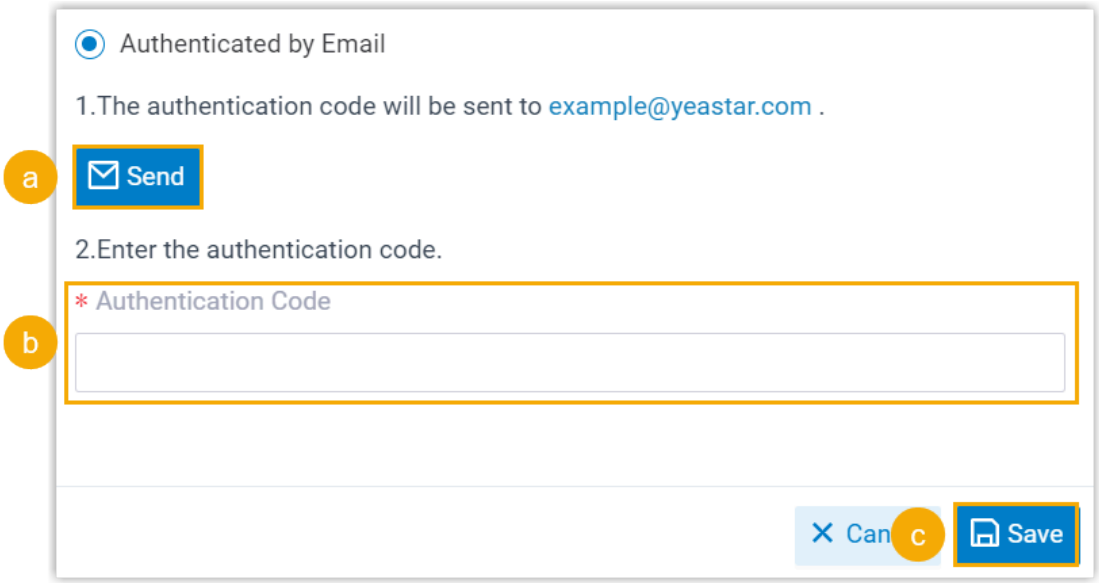
This topic describes how to configure two-factor authentication for super administrator account using email.

Prerequisites

System email server is set up.

Procedure

1. Log in to PBX web portal, click your account at the top-right corner, then go to **Change Password & Security > Security Settings**.
2. Select the checkbox of **Two-Factor Authentication**.
3. In the pop-up **Password** window, enter your account password and click **Confirm** to verify your operation.
4. Select **Authenticated by Email**, and complete the following settings:



a. Click **Send**.
   An email containing a 6-digit authentication code is sent to the email address that is associated with the super administrator account.

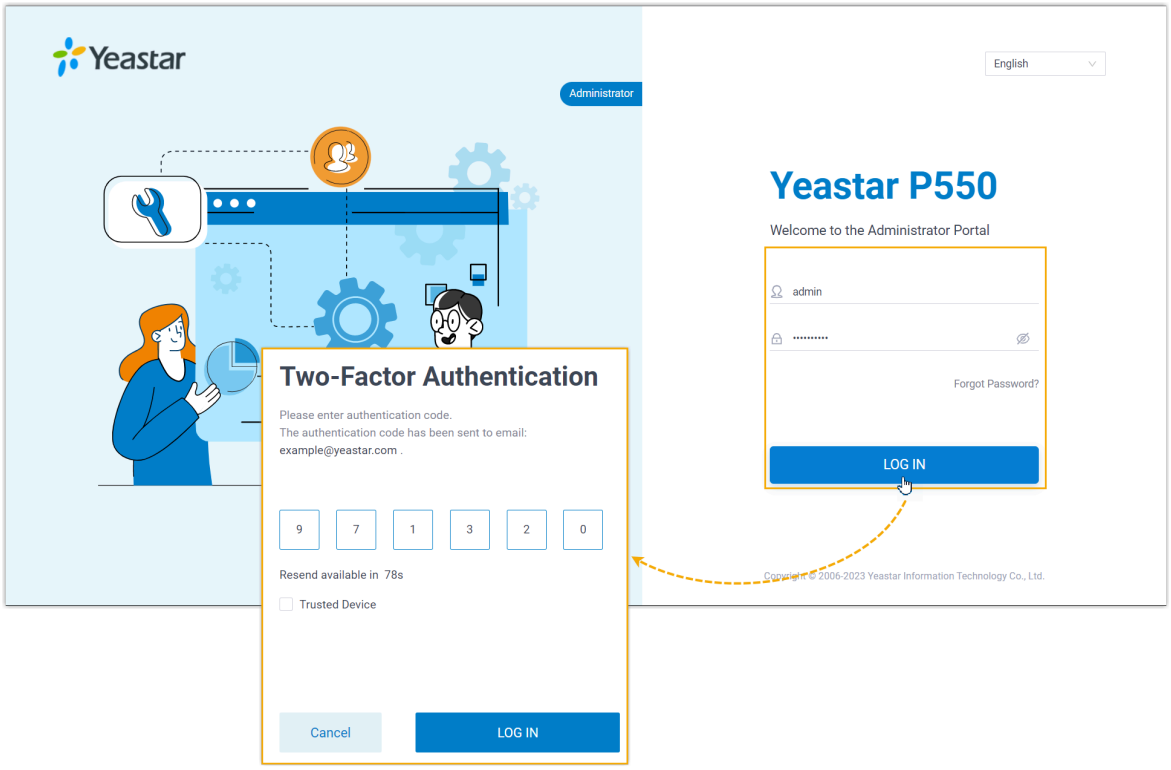
   > **Note:**
   > The code expires 5 minutes after the email is sent.

b. In the **Authentication Code** field, enter the authentication code.
c. Click **Save**.

Result

- The webpage prompts a message "Edited successfully.", which means that you have successfully set up two-factor authentication.
- Next time you log in to PBX web portal, you need to enter an authentication code additionally.

> **Note:**
> For the device from which you log in most frequently, you can select the checkbox of **Trusted Device** to add it as a trusted device. In this way, you don't have to re-enter an authentication code with this device for the next 180 days.



Troubleshooting:
What if my extension users fail to log in with two-factor authentication?

You can disable two-factor authentication for their extension accounts, so that they can directly log in with their username and password.

Related information

Manage Two-factor Authentication of Super Administrator Account

Manage Two-factor Authentication of Super Administrator Account

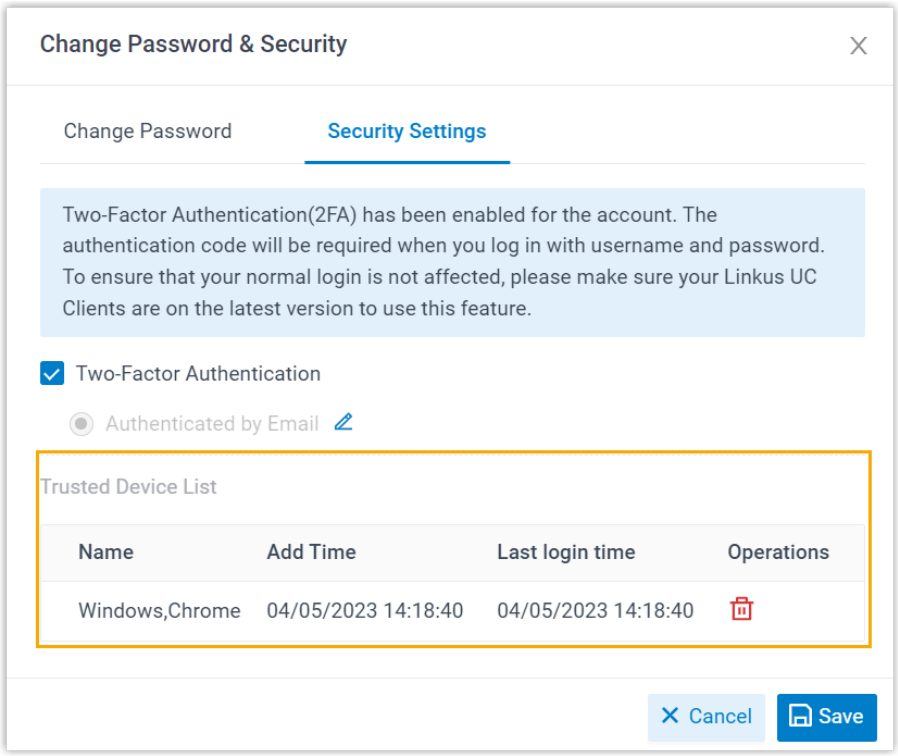
This topic describes how to manage the two-factor authentication feature for super administrator account, including removing trusted devices, changing authentication method, and disabling the two-factor authentication feature.

Remove a trusted device

As a super administrator, in case you lost access to a trusted device, you can remove it from the list if necessary.

1. Log in to PBX administrator portal with super administrator account, click your account at the top-right corner, then go to **Change Password & Security > Security Settings**.

   The trusted devices are displayed in the **Trusted Device List** section.



2. Click beside the device that you want to remove.
3. In the pop-up window, click **OK**.

Change two-factor authentication method

You can change the two-factor authentication method for your super administrator account as needed.

1. Log in to PBX administrator portal with super administrator account, click your account at the top-right corner, then go to **Change Password & Security > Security Settings**.

2. Click beside the current authentication method.
3. Select the desired method, then complete the follow-up settings accordingly.

Disable two-factor authentication

Disable two-factor authentication for your account

You can disable two-factor authentication for your super administrator account at any time.

1. Log in to PBX administrator portal with super administrator account, click your account at the top-right corner, then go to **Change Password & Security > Security Settings**.
2. Unselect the checkbox of **Two-Factor Authentication**.
3. In the pop-up **Password** window, enter your account password and click **Confirm** to verify your operation.
4. In the **Security Settings** tab, click **Save**.

   The webpage prompts a message "Edited successfully.", which means that you have successfully disabled two-factor authentication.

Disable two-factor authentication for your extension user

If your extension user lost access to their two-factor authentication (e.g. they lost their authenticator device or could not receive authentication code via email), you can disable the two-factor authentication for their extension accounts, so that they can directly log in with username and password.

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click beside the extension, then click the **Security** tab.
3. Scroll down to the **Login Security** section, then unselect the checkbox of **Two-Factor Authentication**.
4. In the pop-up **Password** window, enter your account password and click **Confirm** to verify your operation.
5. Click **Save**.

   The two-factor authentication of the extension account is disabled.

Related information

Configure Two-factor Authentication using Authenticator Application
Configure Two-factor Authentication using Email

Enforce Two-factor Authentication for All Extension Users

Enforce Two-factor Authentication for All Extension Users

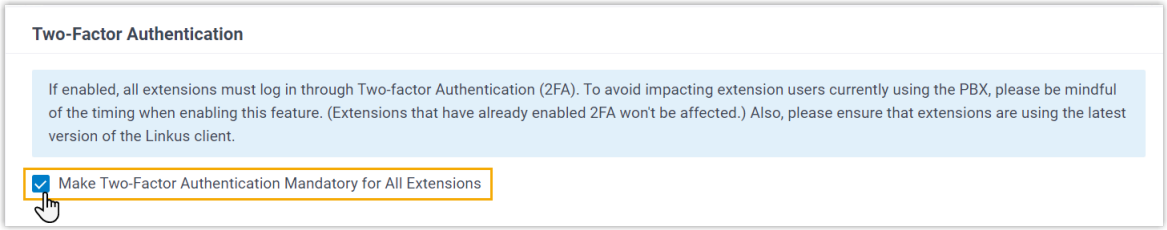
To enhance security for users' accounts, you can make Two-Factor Authentication (2FA) mandatory for all extension users. In this way, users will be required to go through two-factor authentication when logging in using their extension username and password, thus preventing unauthorized access.

Requirements

- Yeastar P-Series PBX System is 37.14.0.24 or later.
- Linkus Desktop Client is 1.4.9 or later.

Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Security Options**.
2. In the **Two-Factor Authentication** section, select the checkbox of **Make Two-Factor Authentication Mandatory for All Extensions**.



3. Click **Save**.

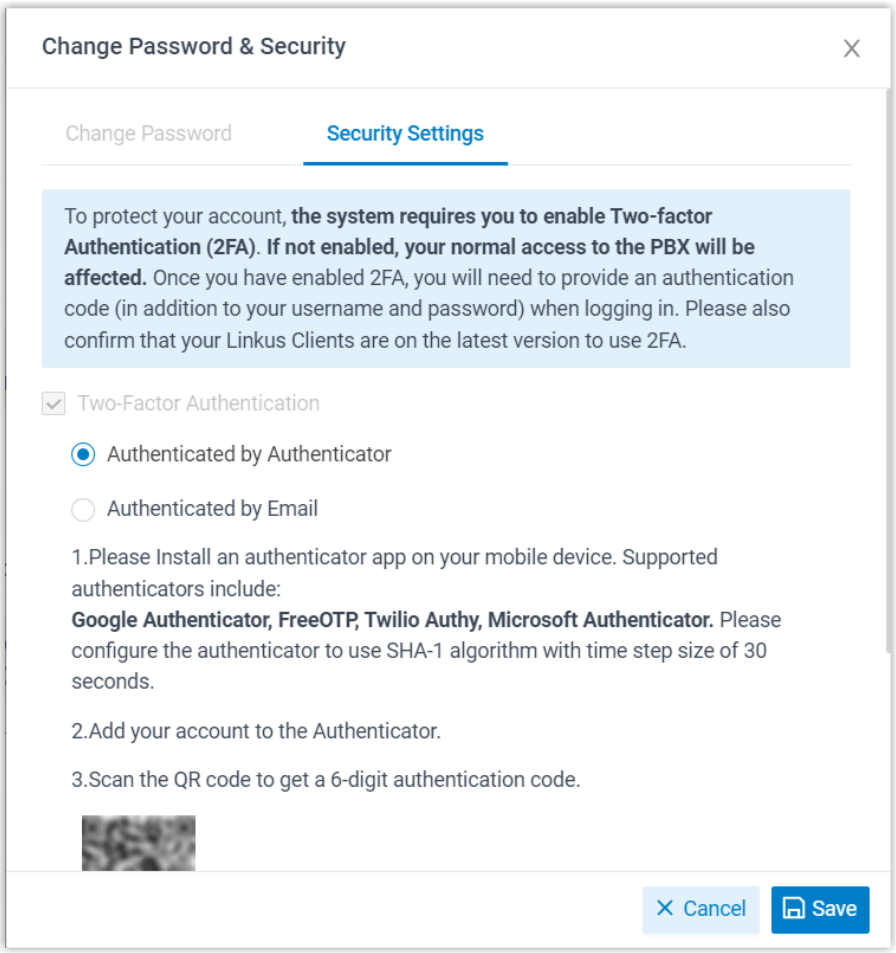
Result

The result varies depending on whether the two-factor authentication (2FA) feature is enabled on user's Linkus clients:

- **2FA is already enabled on users' Linkus clients**

  These users will not experience any interruption in using Linkus.
- **2FA is disabled on users' Linkus clients**

Users who attempt to log in or are already logged in Linkus Web Client or Desktop Client using their extension username and password, the two-factor authentication setup window will pop up, requiring the users to complete the 2FA setup for their accounts. Otherwise, their accounts will be automatically logged out.



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.

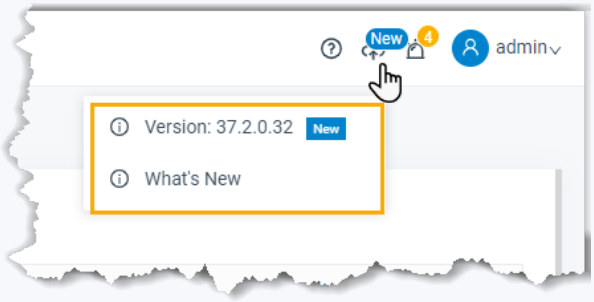
Procedure

1. Log in to PBX web portal, go to **Maintenance > Upgrade**.
2. In the **Automatic Upgrade** section, select **Check for updates and notify me**.
3. In the **Automatic 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 web 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 web 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 web 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

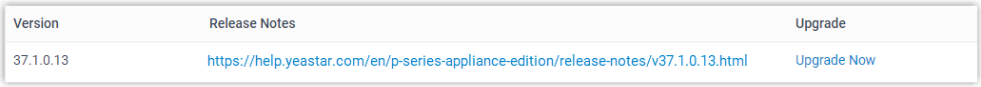
Prerequisites

We recommend that you create a backup file for PBX configurations before you start upgrading the PBX.

Procedure

1. Log in to PBX web 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:



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 web 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.

- **Chat Data for External Chat**

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.

- **Micro SD card**
- **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
  - Set up a Micro 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 web 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.

  - **Chat Data for External Chat**

3. Click **Save**.

Result

The created backup file is displayed in **Backup and Restore** list and is stored in the selected location.

> **Tip:**
> You can archive the backup file to external servers via FTP, SFTP, Amazon S3, and Google Cloud Storage services for less space occupying and minimized data loss risk on PBX, as well as easier file management on external server. For more information, see Yeastar P-Series PBX System Remote Archiving Overview.

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
- Set up a Micro 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 web 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 back-up.
      - **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.

   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**

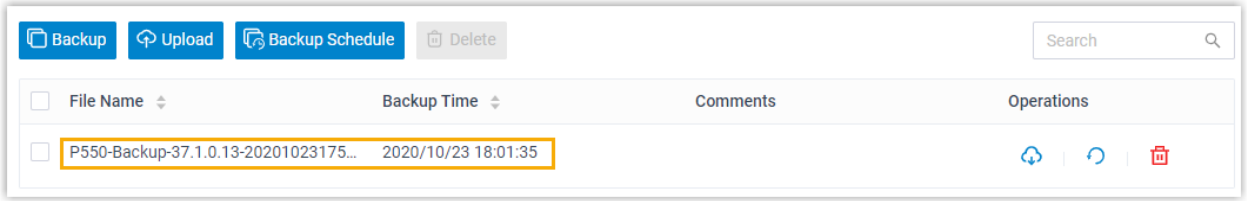
> **Note:**
> The option is available for Basic Plan.

- **Chat Data for External Chat**

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.



> **Tip:**
> You can archive the backup file to external servers via FTP, SFTP, Amazon S3, and Google Cloud Storage services for less space occupying and minimized data loss risk on PBX, as well as easier file management on external server. For more information, see Yeastar P-Series PBX System Remote Archiving Overview.

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

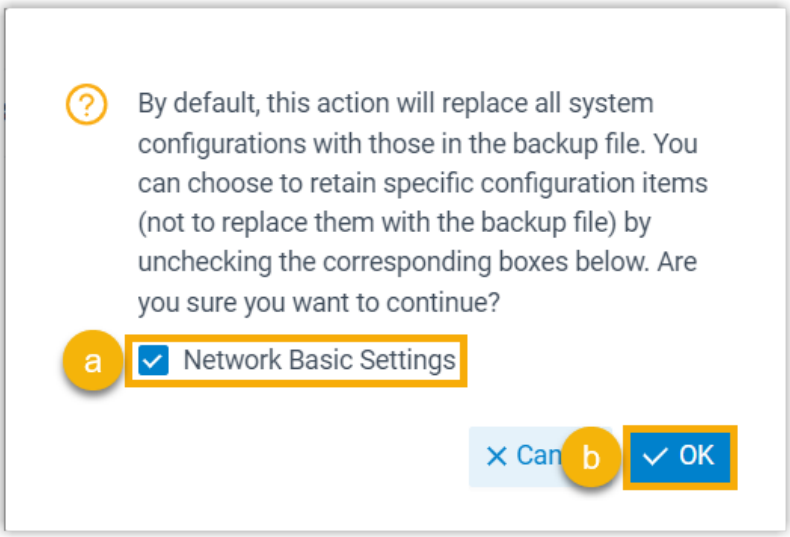
- Make sure that you have backed up system configurations and required files, such as custom prompts and CDR.
- Read and understand restrictions for data restoration.
  - You can restore a backup file that is created from an older version of PBX.

    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 web portal, go to **Maintenance > Backup and Restore**.
2. Select a backup file to which you want to restore, click .
3. In the pop-up window, do as follows:



   a. If you want to retain existing network basic settings (the settings on **System > Network > Basic Settings**), unselect the checkbox of **Network Basic Settings**.
   b. 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

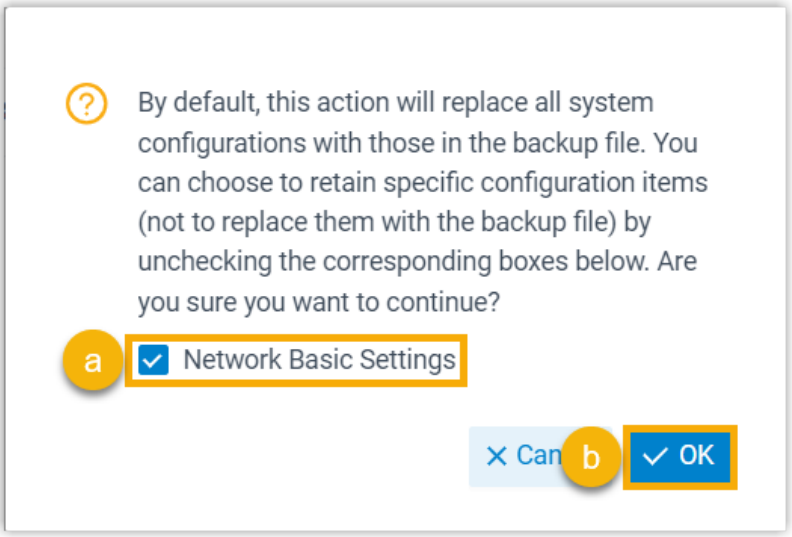
1. Upload a backup file.
   a. Log in to PBX web portal, go to **Maintenance > Backup and Restore**.
   b. Click **Upload**.
   c. In the pop-up window, select a backup file and add a note according to your needs.
      i. Click **Browse** to select a backup file.

      > **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 window, do as follows:



i. If you want to retain existing network basic settings (the settings on **System > Network > Basic Settings**), unselect the checkbox of **Network Basic Settings**.

ii. 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 web 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 web 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.
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 web 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 hod, 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 41.

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 web 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 web 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 web 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 web 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 web 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 byt
e 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 byt
e 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 web 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.

Enable Core Call Service Anomaly Detection

Anomaly in core call service will cause registration dropouts and call failures. Yeastar P-Series PBX System can minimize the impact by automatically detecting the health of core call service and initiating a recovery process when any abnormalities are detected.

Requirements

The firmware version of Yeastar P-Series PBX System is 37.15.0.22 or later.

Procedure

1. Log in to PBX web portal, go to **Maintenance > Troubleshooting > Advanced**.
2. Turn on the option **Core Call Service Anomaly Detection**, then configure the following settings:
   - **Detection Interval (s)**: Enter the interval between each detection to determine how frequently the system will check for core call service anomaly.

     > **Note:**
     > The value you enter should not be smaller than 10.

   - **Anomaly Confirmation Delay (s)**: Enter the waiting time before confirming a core call service anomaly after it is detected.

     > **Note:**
     > The value you enter should not be smaller than 30.

3. **Optional:** To allow the system to automatically initiate a recovery process after confirming a core call service anomaly, select the checkbox of **Automatic Recovery from Abnormality**.

   > **Note:**
   > During the recovery, all ongoing calls will be disconnected.

4. Click **Save** and **Apply**.

Result

The system will periodically check for the health of core call service.

- If core call service is found abnormal, the **Abnormal Core Call Services** event will be triggered to notify the relevant contacts.
- If automatic recovery is enabled, the system will automatically initiate a recovery process when any abnormalities are detected. Once the core call service is successfully recovered, the **Core Call Services Recovery Completed** event will be triggered to notify the relevant contacts.

> **Note:**
> If the core call service is not recovered, you can download system logs and contact Yeastar for support.

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 web 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.

- **Enable OpenAPI Event Notification Message Debug**

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.

Related information

Configure Log Level
Manage System Logs

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 web 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.

- **Enable OpenAPI Event Notification Message Debug**

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 web 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 web 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**.

Forward System Logs to a Third-party Syslog Server

By default, PBX system automatically and periodically deletes the oldest system logs. To ensure comprehensive logging for routine troubleshooting and incident handling, you can configure the PBX to forward system logs to a third-party syslog server (either local or remote) via Syslog protocol over UDP, TCP, or TLS, thus guarantee centralized logging and long-term storage.

Requirements

Yeastar P-Series PBX System is 37.18.0.10 or later.

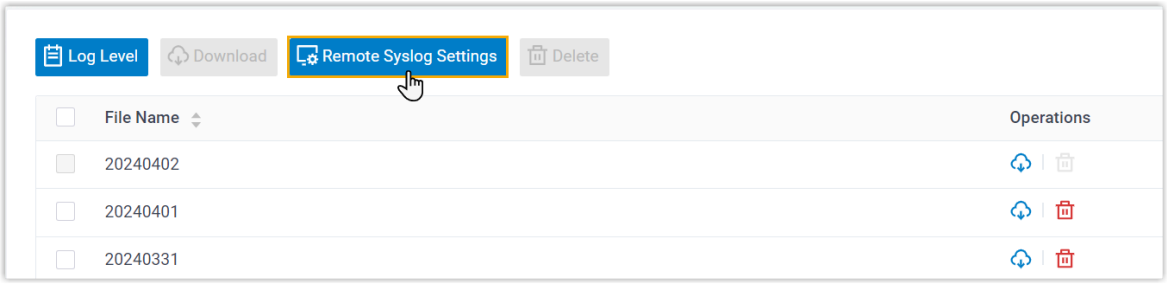
Prerequisites

You have set up a syslog server, and obtain the following information of the server:

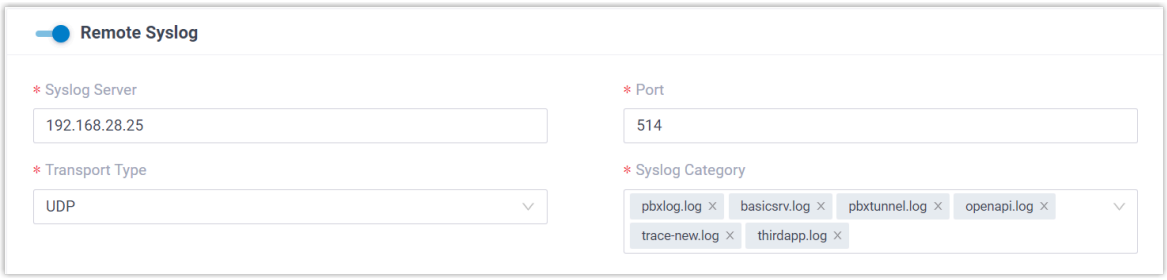
- IP address or hostname
- Supported transport protocol and the corresponding port

Procedure

1. Log in to PBX web portal, go to **Maintenance > System Logs**.
2. In the top menu, click **Remote Syslog Settings**.



3. Turn on the switch of **Remote Syslog**, and complete the following settings.



- **Syslog Server**: Enter the IP address or hostname of the syslog server.
- **Port**: Enter the port number to connect to the syslog server.
- **Transport Type**: In the drop-down list, select the transport type that the syslog server supports.

> **Note:**
> To forward system logs over TLS, you must enable TLS encryption, and upload the required certificate and key on the syslog server.

- **Syslog Category**: In the drop-down list, select the log categories to forwarded to the syslog server.

> **Note:**
> The information contained in the system logs depends on the log level settings (Path: **Maintenance > System Logs > Log Level**).

The following table lists the supported system log categories and the information they include.

Category	Description
pbxlog.log	Logs that provide detailed information about extension registration and PBX calls (call establishment, dialling rule matching, and call duration, etc.). These logs can be used to analyze call quality and investigate call issues.
basicsrv.log	Logical logs of using PBX features, such as Operator Panel, Queue Panel, Hot Standby, and other non-call related features. These logs can be used to track system operating behavior, detect abnormal situations, and conduct performance analysis.
pbxtunnel.log	Logs about the Yeastar PBX FQDN tunnel, including connection establishment and heartbeat detection.

Category	Description
	These logs can be used to monitor tunnel connection status, and troubleshoot connection issues.
openapi.log	Logs about API calls in the system, including interface requests, parameter transmission, and response results. These logs can be used to track API calls, troubleshoot interface issues, and analyze interface performance.
trace-new.log	Logs of system process status, including startup, shutdown, and abnormal exit of guardian processes, as well as inter-process communication and collaboration. These logs can be used for debugging and tracing purposes.
thridapp.log	Logs of third-party integrations, including the process and results of the integration with third-party systems or services. For example, CRM-related logs record the data interaction between the CRM system and PBX system. These logs can be used to monitor data synchronization and exchange, troubleshoot integration issues, etc.
apigateway.log	Logs of API Gateway that records the internal process of API Gateway, which involves rate limiting and circuit breaking when the PBX system receives large amounts of API requests. These logs can be used to monitor traffic management and actions of circuit breaking.

4. Click **Save**.

Result

PBX system starts to forward the selected system logs to the syslog server in real time.

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:

Item	Description
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.
Call Notes	The call notes added for each call.
Source Trunk	The call was received via which trunk.
Destination Trunk	The call was sent out via which trunk.
Communication Type	Communication Type. • **Internal** • **Outbound**

Item	Description
	• **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.
Recording File	The call recording file.

CDR auto cleanup

By default, when the number of call logs reaches 200,000, the system will automatically delete 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.

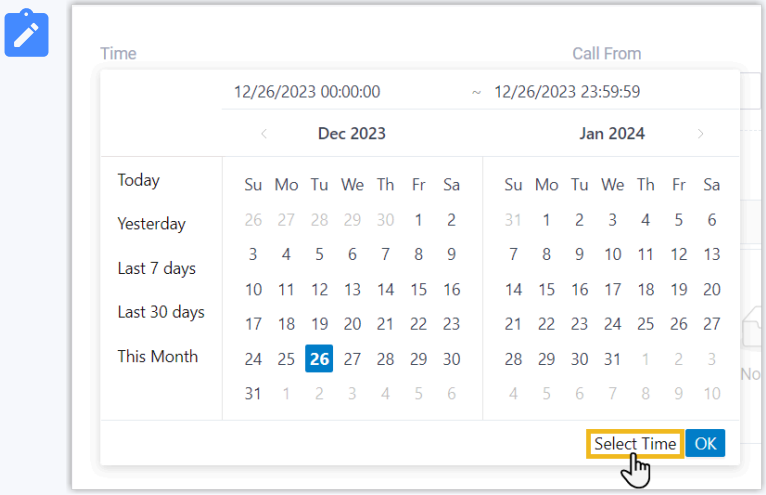
View and Manage CDR

This topic describes how to view, download, and delete CDR.

View CDR

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. **Optional:** Set the basic filter criteria.

Filter	Description
Time	Set the start date and the end date. **Note:** To specify a time period of a day, click **Select Time** to set the start time and the end time.

Filter	Description
	
Call From	Enter the caller's number or name.
Call To	Enter the callee's number or name. **Tip:** To swap the callee for the caller, click ⇆.
Status	Select a call status. • **All** • **ANSWERED** • **NO ANSWER** • **BUSY** • **FAILED** • **VOICEMAIL**

3. **Optional:** Set the advanced filter criteria.

   a. Click .

   b. On the **Filter** page, set the advanced criteria.

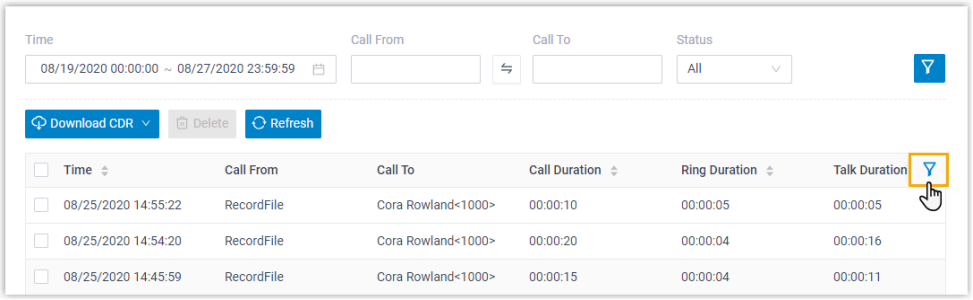
Option	Description
Queue	Select a queue. The system only queries the queue's calls.
Extension Group	Select an extension group. The system only queries the group members' calls.
Call Disposition	Select call disposition code(s).

Option	Description
Remark	Enter the remark added for the call.
Ring Duration	Enter how long the callee's phone rang before the call was answered. **Note:** Only numbers, -, =,<, <=, >, and >= are allowed.
Talk Duration	Enter 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 communication type. • **All** • **Internal** • **Outbound** • **Inbound**
ID	Enter the unique ID for a call.
Trunk	Select a trunk. The system only queries calls that are sent or received via the trunk.
Enable Number Fuzzy Search	Set whether to search for the fuzzy equivalent for the phone number.
DID	Select a DID number. The system only queries the calls that match this DID number.
PIN Code	Enter an existing 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.

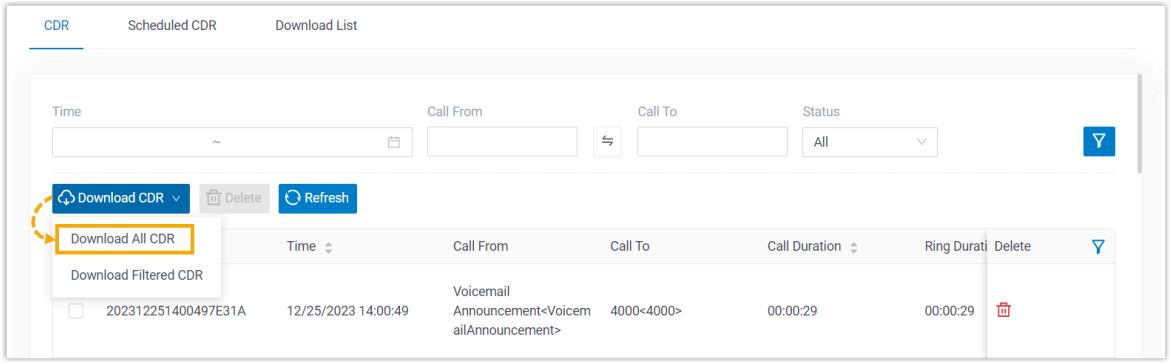
Note:

You can click to decide which item will be displayed.

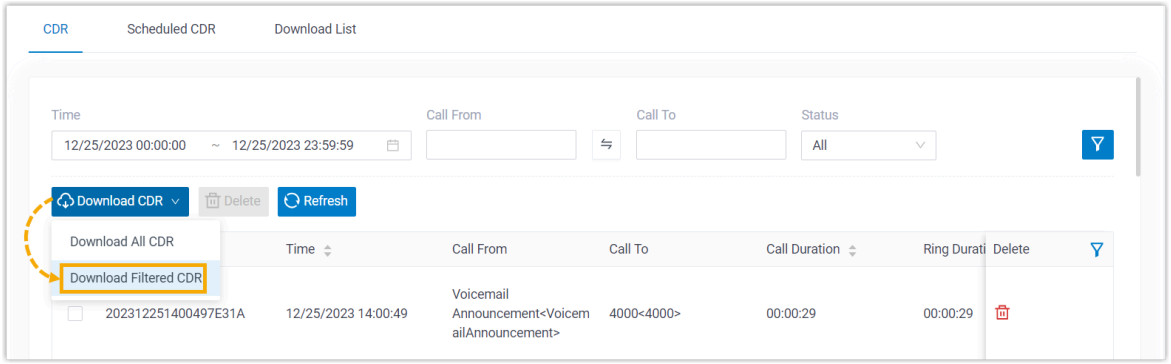


Download CDR

1. Log in to PBX web 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**.



CDR are exported to a CSV file.

Delete CDR

1. Log in to PBX web 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.

Scheduled CDR

Schedule CDR to Email

Yeastar P-Series PBX System allows you to schedule CDR to be sent to specific recipients' mailboxes at the specified time. The recipients can access the CDR via a link attached in the email and download it as a CSV, XLS, or PDF file.

Restrictions

- Only super administrator and the authorized users can schedule CDR to email.
- The maximum number of CDR that can be downloaded at one time varies depending on the file format of the downloaded CDR.
  - **CSV**: 10,000
  - **XLS**: 10,000
  - **PDF**: 5,000

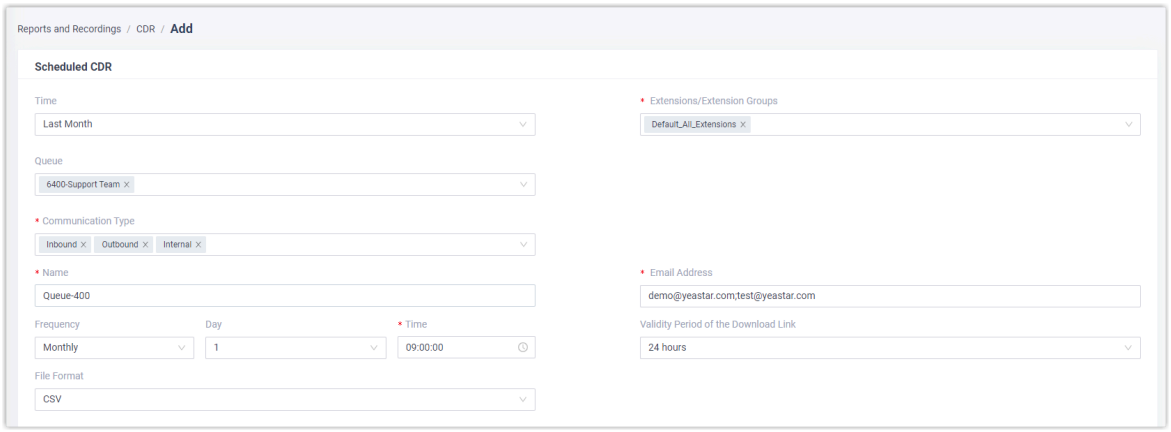
Prerequisites

Make sure email server works.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. Under the **Scheduled CDR** tab, click **Add**.

3. Schedule a task to send CDR via email.



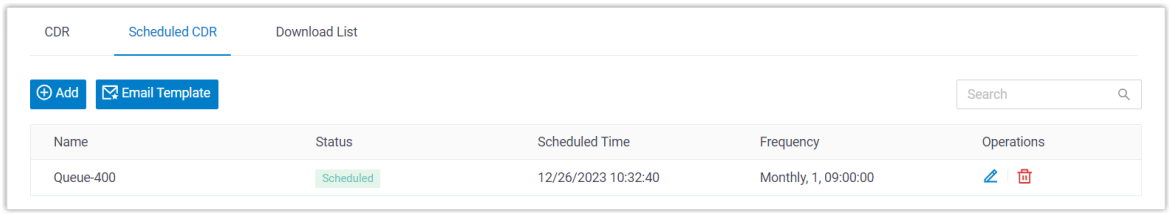
Setting	Description
Time	Select a time range to filter CDR.
Extensions/Extension Groups	Select extension(s) or extension group(s) to filter CDR.
Organization	Select department(s) to filter CDR.
Queue	Select call queue(s) to filter CDR.
Communication Type	Select communication type(s) to filter CDR.
DID	Select DID number(s) to filter CDR.
Name	Enter a name to help you identify the task.
Email Address	Enter recipients' email addresses. **Note:** You can set up to 10 email addresses; Separate multiple email addresses by semicolon `;`.
Frequency	Set how often to send CDR. • **Once**: If selected, the system will send the CDR immediately after you save the task. • **Daily**: If selected, choose a specific time from the drop-down list. The system will send the CDR at the selected time each day. • **Weekly**: If selected, choose a specific day of the week and select a specific time from the drop-down list. The system will send the CDR at the selected day and time each week. • **Monthly**: If selected, choose a specific day of the month and select a specific time from the drop-down list.

Setting	Description
	The system will send the CDR on the selected day and time each month.
Validity Period of the Download Link	Set the validity period of the download link for the scheduled CDR. After the link expires, the recipients can NOT access and download the CDR via the link.
File Format	Set in which file format the CDR can be downloaded. • **CSV** • **XLS** • **PDF**

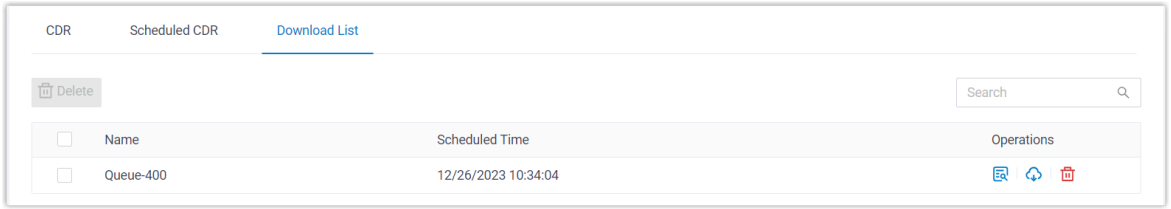
4. Click **Save**.

Result

- The task is scheduled and displayed in the list.



- When it comes to the scheduled time, the specified CDR will be automatically sent to the specified recipients' mailboxes; You can also check the CDR in the **Download List** tab, either by clicking to preview the CDR online, or by clicking to download the CDR for offline viewing.



Related information

Manage Scheduled CDR Tasks
Customize Email Template for Scheduled CDR

Manage Scheduled CDR Tasks

This topic describes how to edit and delete scheduled CDR tasks.

Edit a scheduled CDR task

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. Under the **Scheduled CDR** tab, click beside the desired task.
3. Edit the task according to your needs.
4. Click **Save**.

Delete a scheduled CDR task

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. Under the **Scheduled CDR** tab, do as follows:
   a. Click beside the desired task.
   b. In the pop-up window, click **OK**.

Download Scheduled CDR on PBX Web Portal

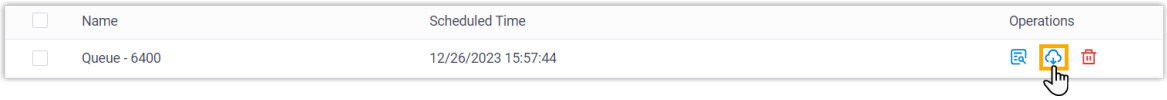
After the system sends scheduled CDR to recipients' mailboxes, the recipients can preview and download the CDR via an attached link, while you can also view and download the CDR on PBX web portal. This topic describes how to download scheduled CDR on PBX web portal.

Prerequisites

A scheduled CDR task has been performed successfully.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. Under **Download List** tab, click beside the desired scheduled CDR task.



Result

The CDR is downloaded to your computer in the pre-defined file format.

Customize Email Template for Scheduled CDR

This topic describes how to customize the email template for scheduled CDR.

Background information

By default, Yeastar P-Series PBX System sends scheduled CDR in the pre-defined language and in a default email template.

The language is what you have set in system email template, and the default email template contains the following information:

- A download link for CDR.
- Soft reminder of the download link.
  - The validity period of the download link.
  - If the PBX hasn't configured Yeastar FQDN or a public IP address, the download 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 web portal, go to **Reports and Recordings > CDR**.
2. Under the **Scheduled CDR** tab, 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 send scheduled CDR using the customized email template.

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.

Category	Reports	Requirement
Basic Reports	• Extension Call Statistics • Extension Call Activity • PBX Call Activity • DID/Outbound Caller ID Activity • IVR Report	No additional requirement.
Advanced Reports	• Unreturned Missed Call Report • Queue AVG Waiting & Talking Time • Queue Performance • Queue Performance Activity • Queue Callback Summary • Queue Callback Activity • Satisfaction Survey • Satisfaction Survey Details • Agent Login Activity • Agent Pause Activity • Agent Missed Call Activity • Agent Performance • Agent Call Summary • Ring Group Statistics • Extension Call Accounting • Extension Call Accounting Details	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 PBX web 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 PBX web portal, 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 web 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

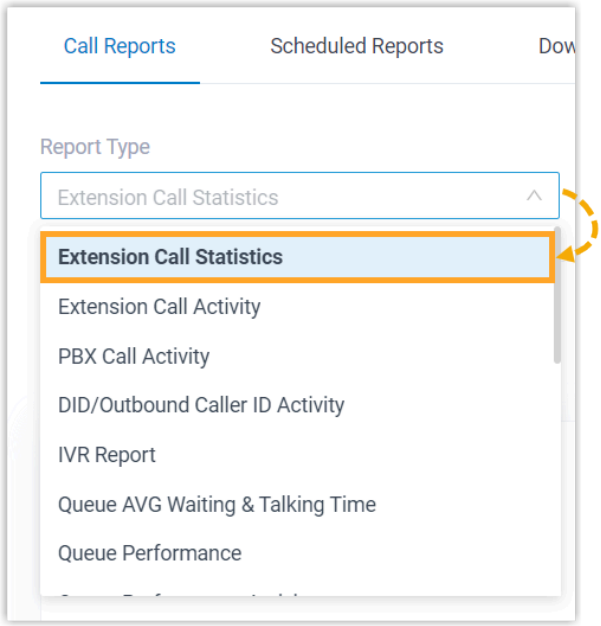
Relevant call statistics are displayed on the page.

Extension Call Statistics Report

Extension Call Statistics report provides a quick overview of the number of calls that have been made and received by extension(s), and can be broken down to specific extensions, groups of extensions, or organizations of extensions. This topic introduces how to access the report and explains the key metrics in detail.

Access Extension Call Statistics report

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Extension Call Statistics**.

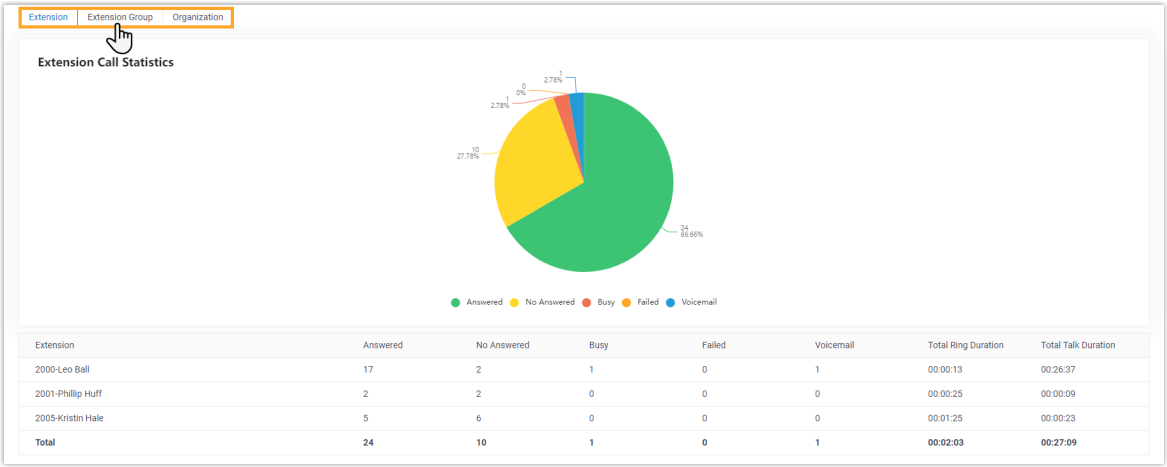


3. Filter data by system time, extension(s), extension group(s), organization(s), or communication type.

> **Note:**
> **Organization** filter is displayed only when you enable **Organization Management** feature (Path: **PBX Settings > Preferences**).



A report that meets the filter criteria is displayed on the page, as shown below.



Note:

- You can click the tab at the top-left corner to switch between the break-down reports.
- If you filter data by organization(s), the report data will include the selected organization and its subordinate departments.

Report details

We take the above report as an example to introduce the key metrics for **Extension Call Statistics** report.

Metric	Description
Answered	The total number of calls that the extension(s) answered.
No Answered	The total number of calls that were routed to the designated destination when the extension(s) didn't answer the calls.
Busy	The total number of calls that were routed to the designated destination when the extension(s) was busy.
Failed	The total number of calls that were failed to be made by the extension(s).
Voicemail	The total number of voicemails that the extension(s) received.
Total Ring Duration	The total time between calls started and calls answered. **Note:** This metric is displayed only when you set **Communication Type** filter to **All**, **Inbound**, **Outbound**, or **Internal**.
Total Talk Duration	The total time between calls answered and calls ended.
Total (displayed in row)	The sum of all the values in each column. **Note:** • This metric is only available for extension and extension group. • If you select multiple extension groups and one of the extensions belongs to two or more extension groups, the call statistics for the extension will be calculated more than once.
	The total number of calls for each communication type.

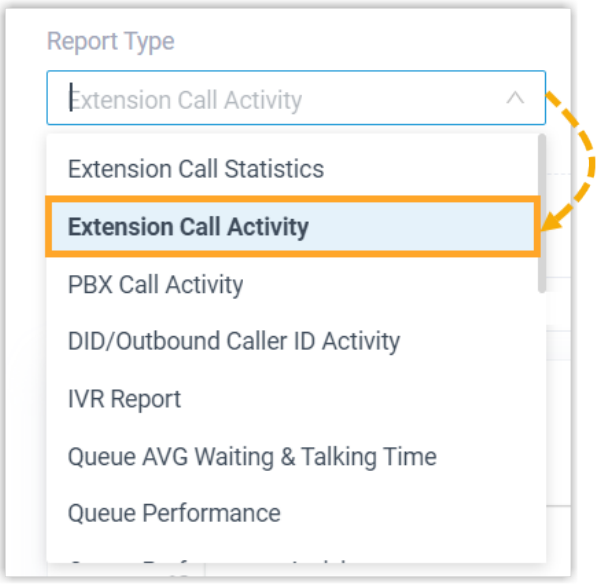
Metric	Description
Total (displayed in column)	**Note:** This metric is displayed only when you set **Communication Type** filter to **Inbound/Outbound**.

Extension Call Activity Report

Extension Call Activity report provides granular insights into the hourly, daily, and monthly breakdown of the number of calls that have been made or received by extension(s), and can be broken down to specific extensions, groups of extensions, or organizations of extensions. This topic introduces how to access the report and explains the key metrics in detail.

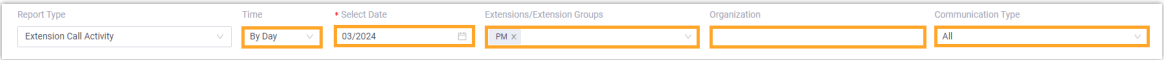
Access Extension Call Activity report

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Extension Call Activity**.

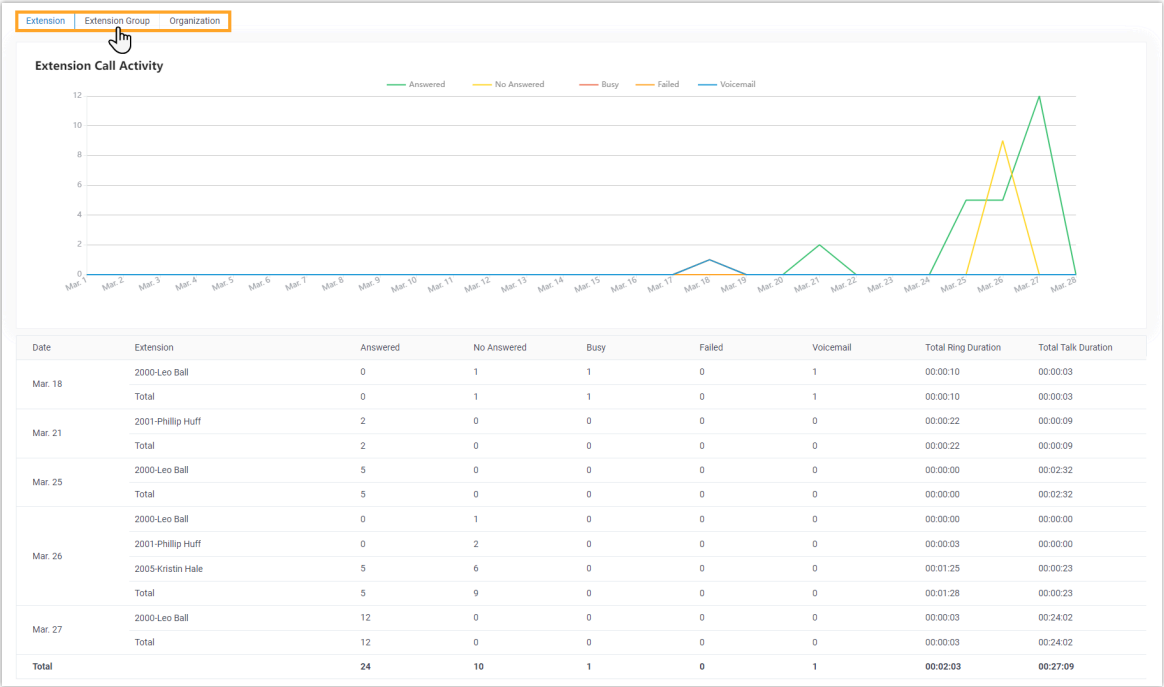


3. Filter data by system date and time, extension(s), extension group(s), organization(s), or communication type.

> **Note:**
> **Organization** filter is displayed only when you enable **Organization Management** feature (Path: **PBX Settings > Preferences**).



A report that meets the filter criteria is displayed on the page, as shown below.



Date	Extension	Answered	No Answered	Busy	Failed	Voicemail	Total Ring Duration	Total Talk Duration
Mar. 18	2000-Leo Ball	0	1	1	0	1	00:00:10	00:00:03
	Total	0	1	1	0	1	00:00:10	00:00:03
Mar. 21	2001-Phillip Huff	2	0	0	0	0	00:00:22	00:00:09
	Total	2	0	0	0	0	00:00:22	00:00:09
Mar. 25	2000-Leo Ball	5	0	0	0	0	00:00:00	00:02:32
	Total	5	0	0	0	0	00:00:00	00:02:32
Mar. 26	2000-Leo Ball	0	1	0	0	0	00:00:00	00:00:00
	2001-Phillip Huff	0	2	0	0	0	00:00:03	00:00:00
	2005-Kristin Hale	5	6	0	0	0	00:01:25	00:00:23
	Total	5	9	0	0	0	00:01:28	00:00:23
Mar. 27	2000-Leo Ball	12	0	0	0	0	00:00:03	00:24:02
	Total	12	0	0	0	0	00:00:03	00:24:02
Total		**24**	**10**	**1**	**0**	**1**	**00:02:03**	**00:27:09**

Note:

- You can click the tab at the top-left corner to switch between the break-down reports.
- If you filter data by organization(s), the report data will include the selected organization and its subordinate departments.

Report details

We take the above report as an example to introduce the key metrics for **Extension Call Activity** report.

Metric	Description
Answered	The total number of calls that the extension(s) answered.
No Answered	The total number of calls that were routed to the designated destination when the extension(s) didn't answer the calls.
Busy	The total number of calls that were routed to the designated destination when the extension(s) was busy.

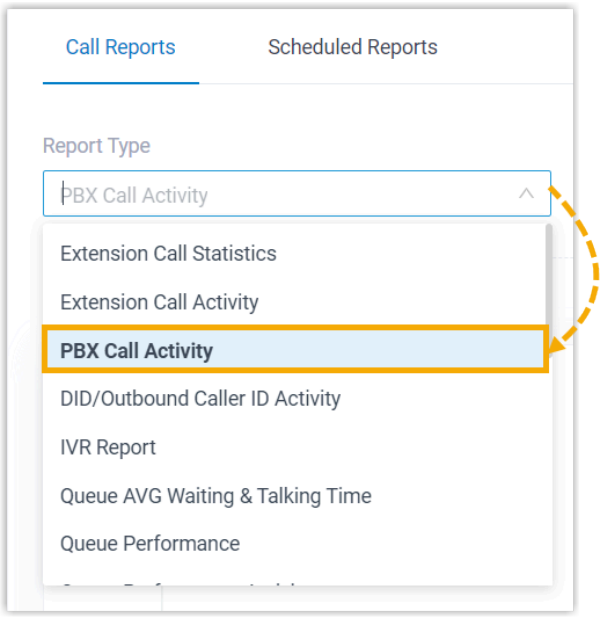
Metric	Description
Failed	The total number of calls that were failed to be made by the extension(s).
Voicemail	The total number of voicemails that the extension(s) received.
Total Ring Duration	The total time between calls started and calls answered.
Total Talk Duration	The total time between calls answered and calls ended.
Total (displayed in row)	The sum of all the values in each column. **Note:** • This metric is only available for extension and extension group. • If you select multiple extension groups and one of the extensions belongs to two or more extension groups, the call statistics for the extension will be calculated more than once.

PBX Call Activity Report

PBX Call Activity report provides granular insights into the hourly, daily, and monthly break-down of internal calls and external calls. This topic introduces how to access the report and explains the key metrics in detail.

Access PBX Call Activity report

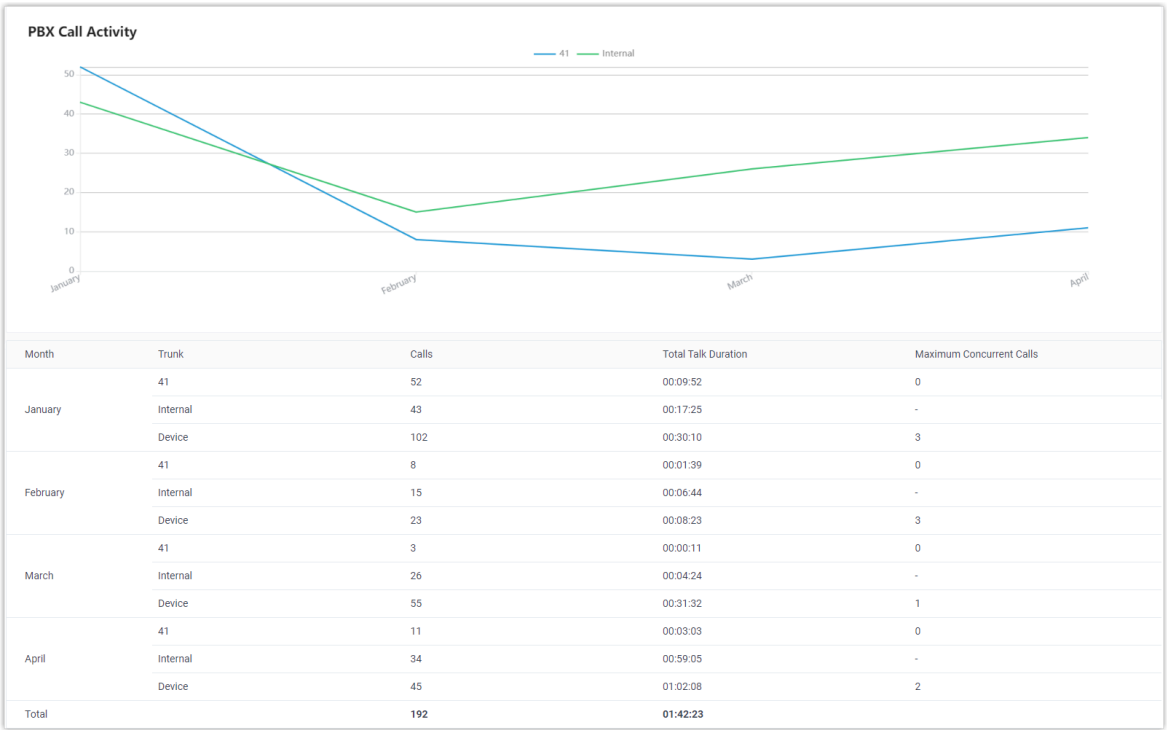
1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **PBX Call Activity**.



3. Filter data by system time, trunks, call type, or communication type.



A report that meets the filter criteria is displayed on the page, as shown below.



Month	Trunk	Calls	Total Talk Duration	Maximum Concurrent Calls
	41	52	00:09:52	0
January	Internal	43	00:17:25	-
	Device	102	00:30:10	3
	41	8	00:01:39	0
February	Internal	15	00:06:44	-
	Device	23	00:08:23	3
	41	3	00:00:11	0
March	Internal	26	00:04:24	-
	Device	55	00:31:32	1
	41	11	00:03:03	0
April	Internal	34	00:59:05	-
	Device	45	01:02:08	2
Total		**192**	**01:42:23**	

Report details

We take the above report as an example to introduce the key metrics for **PBX Call Activity** report.

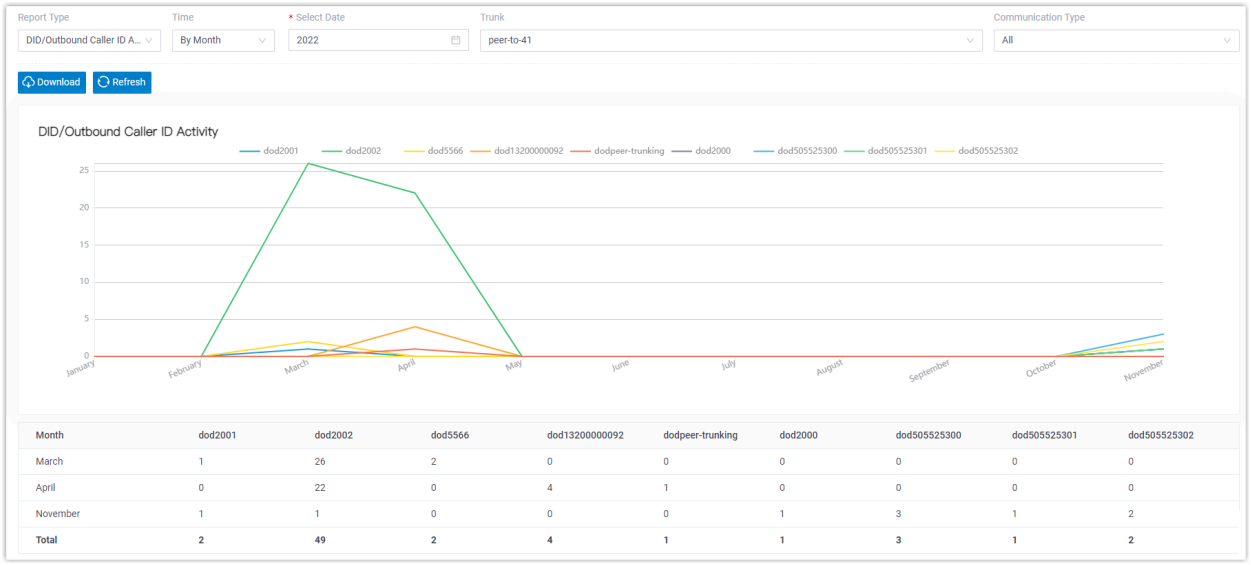
Metric	Description
Trunk	Trunk name. • *{trunk_name}*: Calls that are made or received via trunks. • **Internal**: Calls that are made between extensions. • **Device**: Calls of the entire system (including internal calls, inbound and outbound calls on all the trunks). **Note:** This value is displayed only when **Communication Type** filter is set to **All**.
Calls	The total number of calls that were made or received.
Total Talk Duration	The total time between calls answered and calls ended.
Maximum Concurrent Calls	The maximum number of concurrent calls within the time frame. **Note:** • Calls between extensions and the calls received from WebRTC trunks do NOT support the calculation of maximum concurrent calls. • For **Trunk** displayed as **Device**, it calculates the maximum concurrent calls for the entire phone system.
Total (displayed in row)	Total number of calls and total talk duration. **Note:** This shows the sum of the data for internal calls and the selected trunks, excluding the data for the entire phone system (namely the data for **Trunk** displayed as **Device**).

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 monthly DID/Outbound Caller ID statistics of the trunk **peer-to-41** on 2022.



Month	dod2001	dod2002	dod5566	dod13200000092	dodpeer-trunking	dod2000	dod505525300	dod505525301	dod505525302
March	1	26	2	0	0	0	0	0	0
April	0	22	0	4	1	0	0	0	0
November	1	1	0	0	0	1	3	1	2
Total	**2**	**49**	**2**	**4**	**1**	**1**	**3**	**1**	**2**

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.

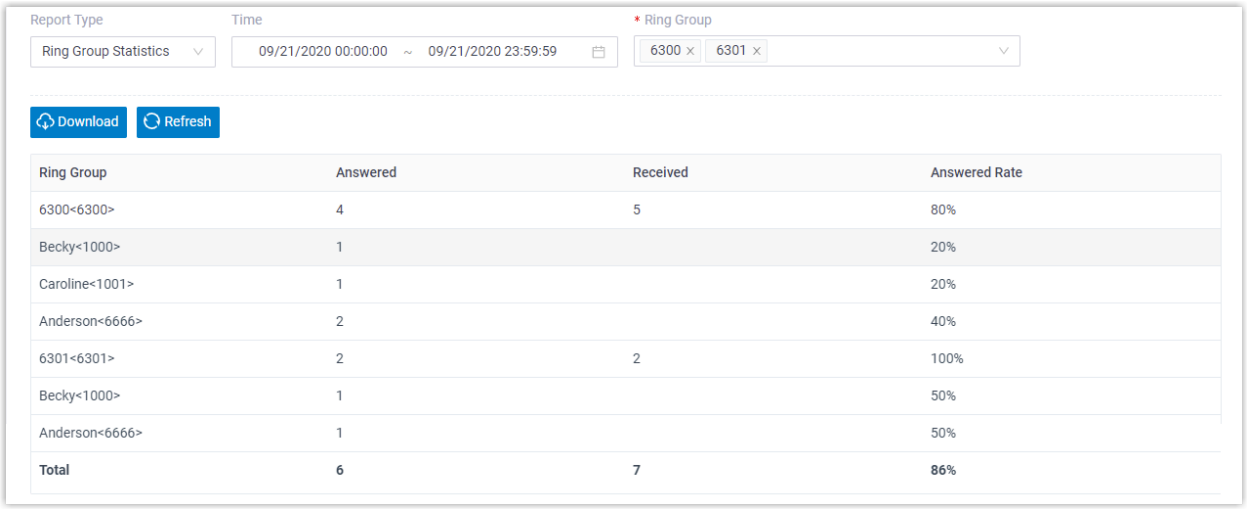
Report details

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.
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** on 09/21/2020.



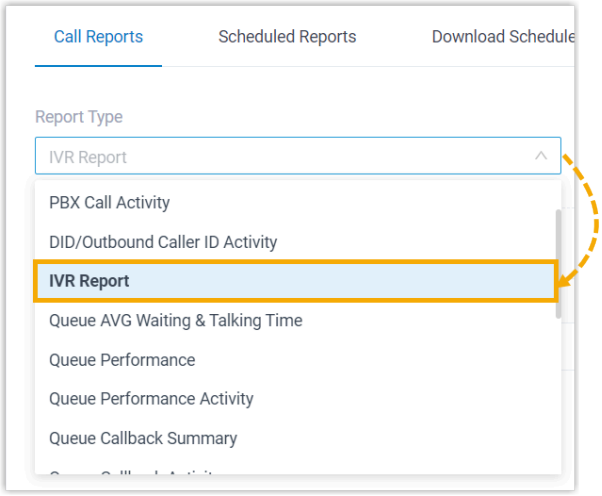
Ring Group	Answered	Received	Answered Rate
6300<6300>	4	5	80%
Becky<1000>	1		20%
Caroline<1001>	1		20%
Anderson<6666>	2		40%
6301<6301>	2	2	100%
Becky<1000>	1		50%
Anderson<6666>	1		50%
Total	**6**	**7**	**86%**

IVR Report

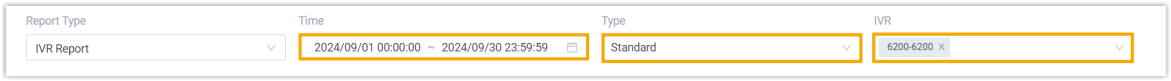
IVR report provides a quick overview of the keypress events for IVR as well as granular insights into the associated IVR calls. This topic introduces how to access the report and explains the key metrics in detail.

Access IVR Report

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **IVR Report**.



3. Filter data by system time, key type, and IVR(s).



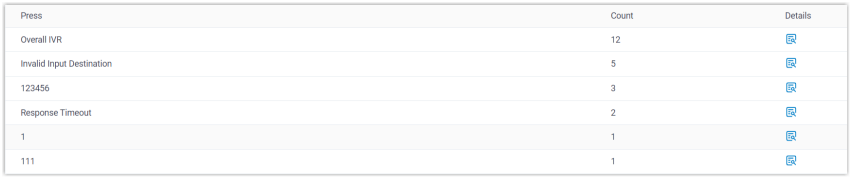
A report that meets the filter criteria is displayed on the page, as shown below.

Figure 7. IVR with standard keys



IVR	Press0	Press1	Press2	Press3	Press4	Press5	Press6	Press7	Press8	Press9	Press#	Press*	Response Timeout	Invalid Input Destination	Details
6200-6200	0	1	0	0	0	0	0	0	0	0	0	0	2	5	

Figure 7. IVR with custom keys



Press	Count	Details
Overall IVR	12	
Invalid Input Destination	5	
123456	3	
Response Timeout	2	
1	1	
111	1	

Report details

We take the above reports as examples to introduce the key metrics for **IVR** report.

IVR with standard keys

- **Metrics for IVR (with standard keys)**

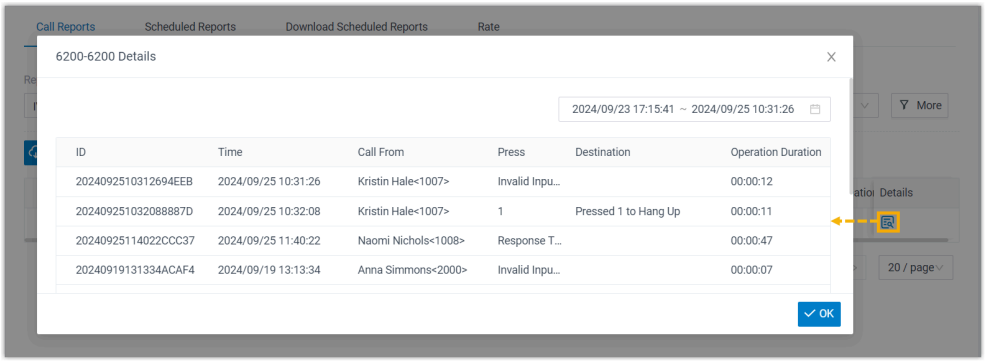


IVR	Press0	Press1	Press2	Press3	Press4	Press5	Press6	Press7	Press8	Press9	Press#	Press*	Response Timeout	Invalid Input Destination	Details
6200-6200	0	1	0	0	0	0	0	0	0	0	0	0	2	5	

Metric	Description
Press*key_pressed*	The number of times that the key was pressed.
Response Timeout	The number of times that IVR calls were routed to the timeout destination. **Note:** IVR calls will be routed to response timeout destination if no key was pressed after reaching the maximum **Prompt Repeat Count**.
Invalid Input Destination	The number of times that IVR calls were routed to the invalid input destination. **Note:** IVR calls will be routed to invalid input destination if callers repeatedly entered a DTMF digit that

Metric	Description
	is not defined for the IVR after reaching the maximum **Prompt Repeat Count**.

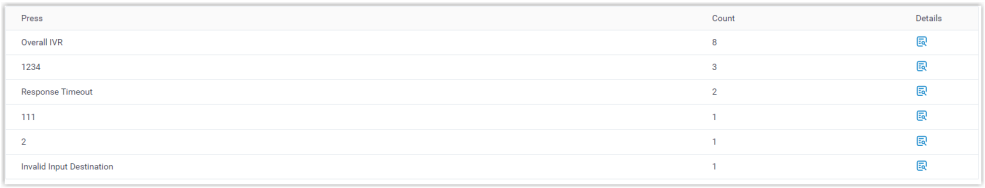
- **Metrics for IVR call (with standard keys)**



Metric	Description
ID	A unique ID for the call.
Time	When the call was received.
Call From	The number and the name of the caller.
Press	The keypress event.
Destination	The destination of the call.
Operation Duration	The time between the caller called into the IVR and exited the IVR.

IVR with custom keys

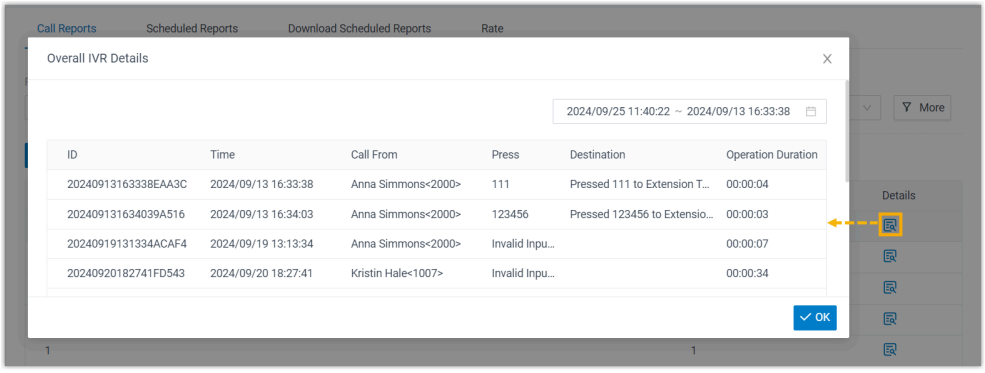
- **Metrics for IVR (with custom keys)**



Metric	Description
Overall IVR	The number of times that all key press events in the IVR were triggered.
{key_pressed}	The number of times that the key was pressed.

Metric	Description
Response Timeout	The number of times that IVR calls were routed to the timeout destination. **Note:** IVR calls will be routed to response timeout destination if no key was pressed after reaching the maximum **Prompt Repeat Count**.
Invalid Input Destination	The number of times that IVR calls were routed to the invalid input destination. **Note:** IVR calls will be routed to invalid input destination if callers repeatedly entered a DTMF digit that is not defined for the IVR after reaching the maximum **Prompt Repeat Count**.

- **Metrics for IVR call (with custom keys)**



Metric	Description
ID	A unique ID for the call.
Time	When the call was received.
Call From	The number and the name of the caller.
Press	The keypress event.
Destination	The destination of the call.
Operation Duration	The time between the caller called into the IVR and exited the IVR.

Unreturned Missed Call Report

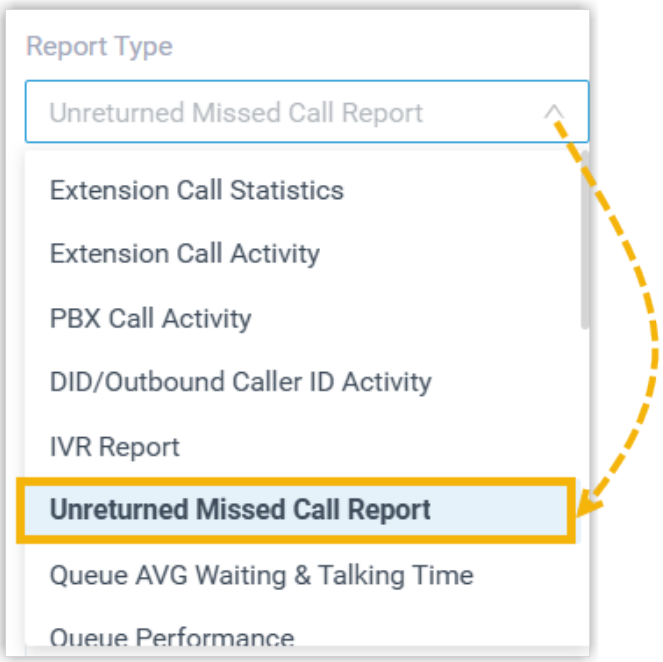
Unreturned Missed Call report provides a comprehensive overview of all the missed inbound calls, including callback status and details, which helps track missed call activities and follow-up actions. This topic introduces how to access and download the report and explains the key metrics in detail.

Prerequisites

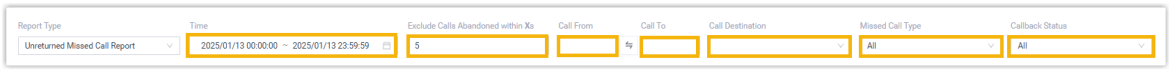
You have subscribed to **Enterprise Plan** or **Ultimate Plan**.

Access Unreturned Missed Call Report

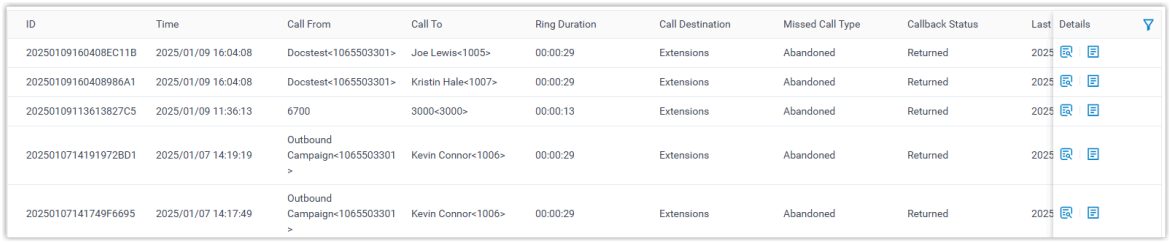
1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Unreturned Missed Call Report**.



3. Filter data by the following criteria.



A report that meets the filter criteria is displayed on the page, as shown below.

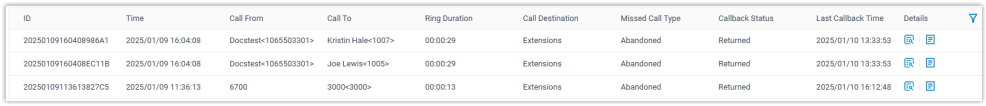


ID	Time	Call From	Call To	Ring Duration	Call Destination	Missed Call Type	Callback Status	Last	Details
20250109160408EC11B	2025/01/09 16:04:08	Docstest<1065503301>	Joe Lewis<1005>	00:00:29	Extensions	Abandoned	Returned	2025	
20250109160408986A1	2025/01/09 16:04:08	Docstest<1065503301>	Kristin Hale<1007>	00:00:29	Extensions	Abandoned	Returned	2025	
20250109113613827C5	2025/01/09 11:36:13	6700	3000<3000>	00:00:13	Extensions	Abandoned	Returned	2025	
20250107141191972BD1	2025/01/07 14:19:19	Outbound Campaign<1065503301>	Kevin Connor<1006>	00:00:29	Extensions	Abandoned	Returned	2025	
20250107141749F6695	2025/01/07 14:17:49	Outbound Campaign<1065503301>	Kevin Connor<1006>	00:00:29	Extensions	Abandoned	Returned	2025	

To understand each metric, refer to the following tables.

- Metrics for unreturned missed call
- Metrics for unreturned missed call details (segment details)
- Metrics for unreturned missed call details (callback details)

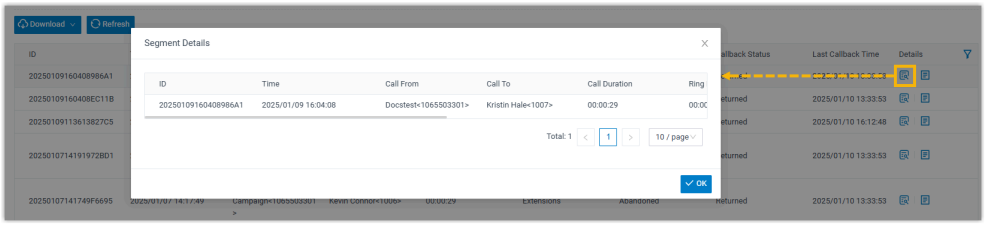
Metrics for unreturned missed call



ID	Time	Call From	Call To	Ring Duration	Call Destination	Missed Call Type	Callback Status	Last Callback Time	Details
20250109160408986A1	2025/01/09 16:04:08	Docstest<1065503301>	Kristin Hale<1007>	00:00:29	Extensions	Abandoned	Returned	2025/01/10 13:33:53	
20250109160408EC11B	2025/01/09 16:04:08	Docstest<1065503301>	Joe Lewis<1005>	00:00:29	Extensions	Abandoned	Returned	2025/01/10 13:33:53	
20250109113613827C5	2025/01/09 11:36:13	6700	3000<3000>	00:00:13	Extensions	Abandoned	Returned	2025/01/10 16:12:48	

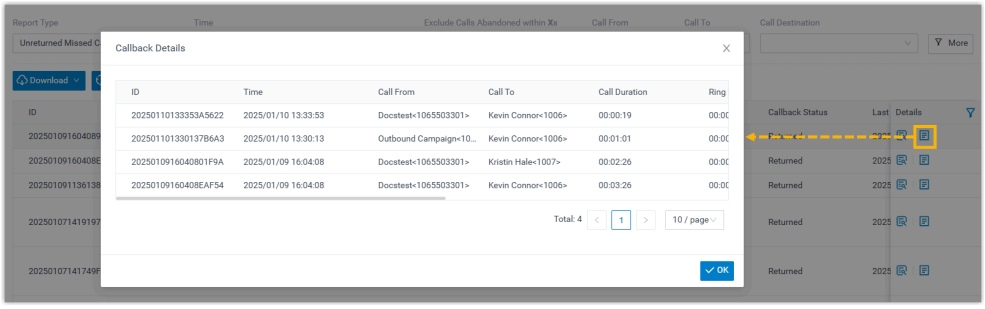
Metric	Description
ID	A unique ID for the call.
Time	The time when the call was received.
Call From	The number or the name of the caller.
Call To	The number or the name of the callee.
Ring Duration	The time between the call started and the call answered.
Call Destination	The type of the destination to which the inbound call was routed. • Extension • Ring Group • Queue
Missed Call Type	The type of the missed call. • No Answered • Abandoned • Busy
Callback Status	Whether the missed call was returned or not. • Returned • Unreturned
Last Callback Time	The last time that the callback was made.

Metrics for unreturned missed call details (segment details)



Metric	Description
ID	A unique ID for the call.
Time	The time when the call was 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 was answered and the call ended.
Status	Whether the call was answered or not.
Reason	The reason why the call was missed.
Communication Type	The type of the call.

Metrics for unreturned missed call details (callback details)

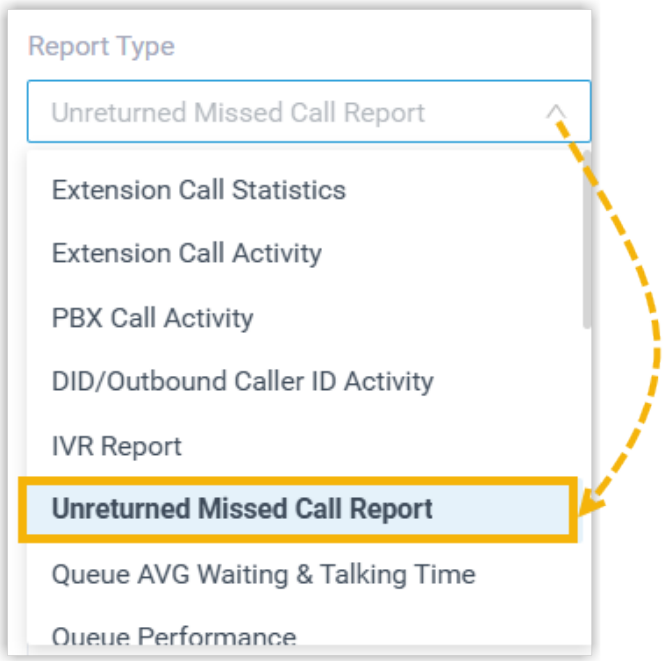


Metric	Description
ID	A unique ID for the call.
Time	The time when the call was received.
Call From	The number or the name of the caller.
Call To	The number or the name of the callee.

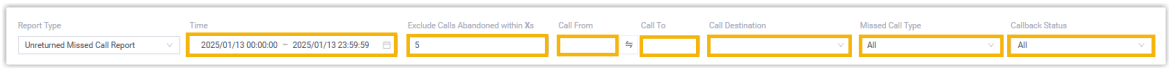
Metric	Description
Call Duration	The time between the call started and the call ended.
Ring Duration	The time that the callee's phone rang before the call was answered or disconnected.
Talk Duration	The time between the call was answered and the call ended.
Status	Whether the call was successful or not.
Reason	The reason why the call ended.
Communication Type	The type of the call.

Download Unreturned Missed Call Report

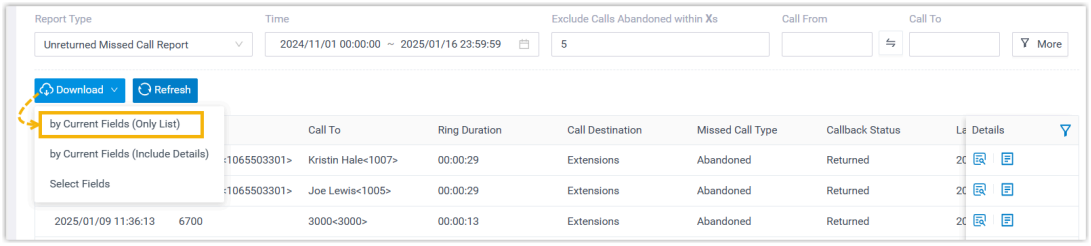
1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Unreturned Missed Call Report**.



3. Filter data by the following criteria.



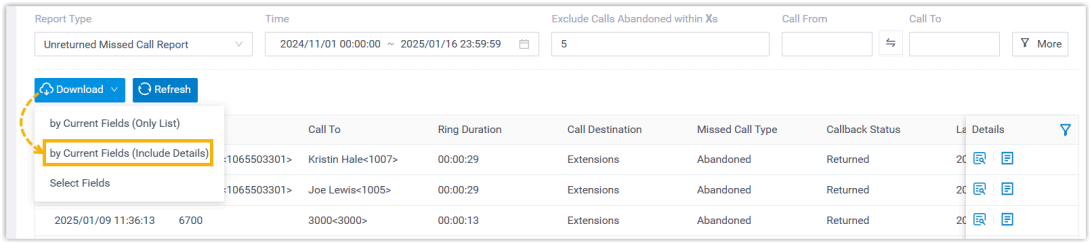
4. Download the report according to your needs.
    - To download the current displayed list of the report excluding details, do as follows:



a. At the top of the list, click **Download**.

b. In the drop-down list, select **by Current Fields (Only List)**.

- To download the current displayed list of the report including details, do as follows:

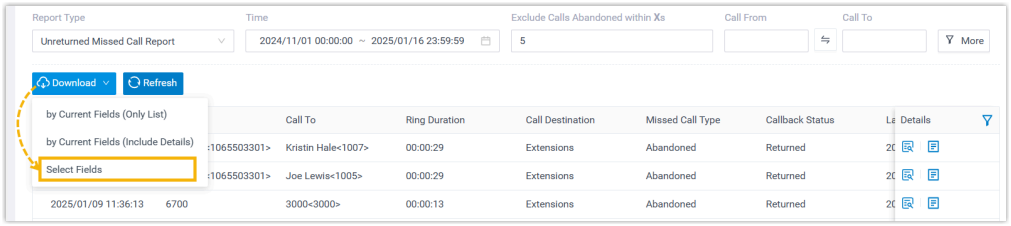


a. At the top of the list, click **Download**.

b. In the drop-down list, select **by Current Fields (Include Details)**.

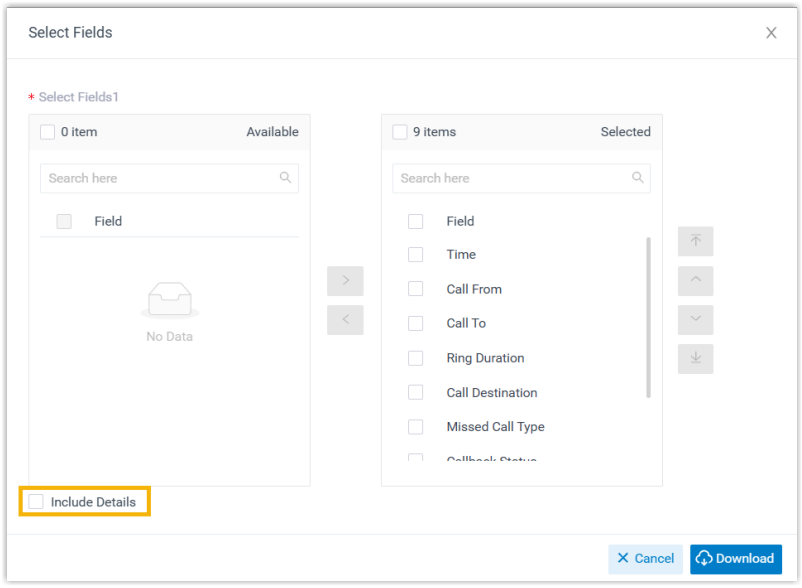
- To download reports with customized display fields, do as follows:

a. At the top of the list, click **Download**, then select **Select Fields** from the drop-down list.



b. In the pop-up window, select the desired fields which you want to display in the report, and decide whether to include details as needed.

> **Note:**
> By default, all fields will be displayed in the report.



c. Click **Download**.

The unreturned missed call report is exported to a CSV file.

Scheduled Reports

Schedule Call Reports

This topic describes how to schedule a call report to be sent to specific recipients' mailboxes 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.

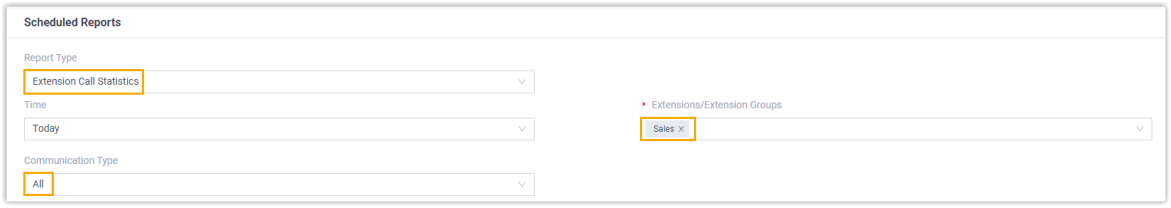
Prerequisites

- Make sure email server works.
- Customize Email Template for Scheduled Reports.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.

2. Under **Scheduled Reports** tab, click **Add Report**.
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 from **Inbound**, **Outbound**, **Internal**, **Inbound/Outbound**, or **All**. You can use the parameter to filter call statistics in the following reports:
  - **Extension Call Statistics**
  - **Extension Call Activity**
  - **PBX Call Activity**
  - **DID/Outbound Caller ID Activity**
- **Exclude Calls Abandoned within Xs**: 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**
  - **Queue Performance Activity**
  - **Agent Performance**
  - **Unreturned Missed Call Report**
- **Organization**: Select one or more departments. Calls of the department and its sub-departments will be included in the report.

  Note:
  This option is available only when you enable the **Organization Management** feature.
  You can use the parameter to filter call statistics in the following reports:
  - **Extension Call Statistics**
  - **Extension Call Activity**
  - **Extension Call Accounting**

- **Extension Call Accounting Details**

- **Type**: Select a type from **Standard** or **Custom**. You can use the parameter to filter call statistics in **IVR Report**.

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 recipients' email addresses, separated by semicolon `;`.

     Note:
     You can set up to 10 email addresses.

     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.
   - **Validity Period of the Download Link**: Set the validity period of the download link for the scheduled report.

     After the link expires, you can NOT download the report via the link.
   - **File Format**: Set in which format the report can be downloaded.
     - **CSV**
     - **XLS**
     - **PDF**
   - **Send Attachment**: Optional. If enabled, a file attachment will be included in the email sent to the specific email address.

     Note:

> This option is only available when the scheduled file format is set to **CSV** or **XLS**.

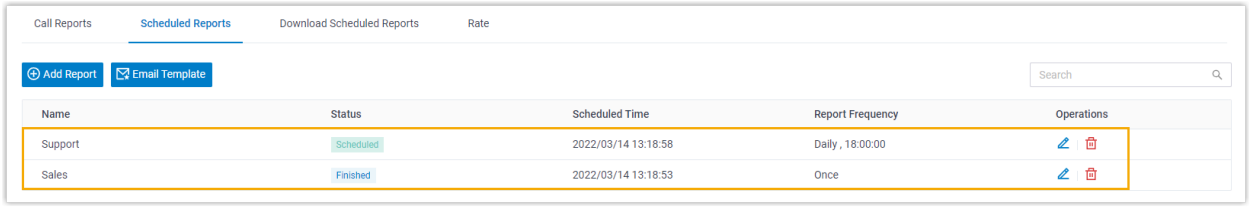
- **Select Fields**: Optional. If you want to customize the display fields in your scheduled report, adjust the desired fields in the **Selected** box.

> **Note:**
> This option is only available in the following reports:
> - **Unreturned Missed Call Report**
> - **Queue Performance**
> - **Queue Performance Activity**
> - **Agent Performance**
> - **Agent Call Summary**

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 recipients' email addresses.
- **Scheduled**: The call report is scheduled and valid. The system will send the report to the recipients' email addresses 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.

Manage Scheduled Reports

This topic describes how to edit and delete scheduled reports.

Edit scheduled reports

1. Log in to PBX web 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 web 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 web portal. This topic describes how to download scheduled reports on PBX web portal.

Prerequisites

A scheduled report was sent out.

Procedure

1. Log in to PBX web 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 web 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.

Call Accounting

Call Accounting Overview

The Call Accounting feature collects and records telecom usage, as well as estimating the expenses incurred based on the destination number and call duration, allowing you to get an eagle-eye overview of the telephone activity and cost of all employees.

Requirement

Enterprise Plan or **Ultimate Plan** is subscribed.

Scenario

In customer service businesses, many employees need to call potential customers via National Direct Dialing (NDD) or International Direct Dialing (IDD). Leaving such outbound calls unattended makes the way for telecommunication misuse, and eventually causes financial losses. These companies need a management tool to track telephone activity of employees, so as to keep telecom usage and expenses in control.

Highlights

Collect and record call statistics

Monitor, record, and track individual and department calls. Based on the historical and real-time call logs, you can measure and analyze employees' performance and identify telephone misuse and abuse.

Flexible call rate settings

Apply different call rate rules to local calls, long distance calls, and international calls. In this way, you can monitor the billing statistics for each type of call, and estimate call charges before telecommunications provider sends the bill.

Insightful call accounting reports

Get dedicated call accounting reports based on individuals or departments. Detailed information about the total number of calls, total call duration, average call duration, and total billing gives you deeper insights into the calling patterns and activity of employees.

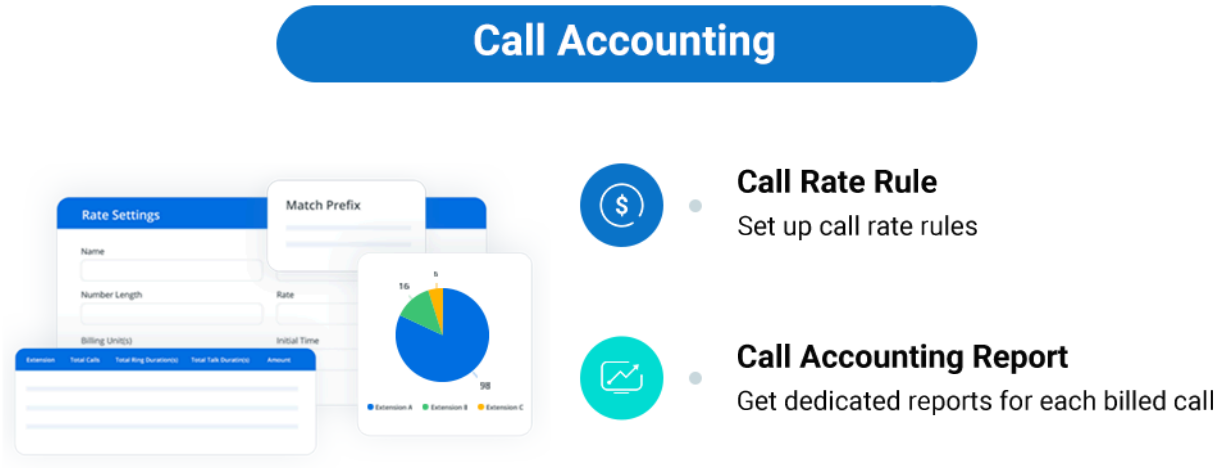
Improve telecom budget planning

Tracking and analyzing telecom usage by individuals or departments help you manage and control telecommunication expenses, making the budgeting more accurate and efficient.

A quick glance at Call Accounting

We provide a thumbnail for you to glance at the WebGUI and get to know the workflow of call accounting.

> **Tip:**
> You can click on the text on the right of the thumbnail to quickly redirect to the corresponding topic.



1. Add a Call Rate Rule
2. Extension Call Accounting Report

Call Rate

Add a Call Rate Rule

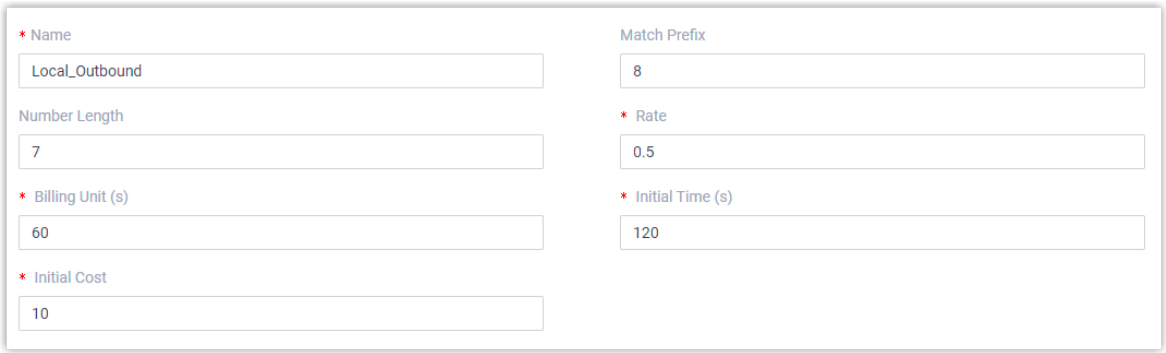
To monitor telecommunication costs for groups and individuals and prevent from potential fraudulent use of resources, you can add a call rate rule for outbound calls, such as local, long-distance, or international calls.

Restrictions

- Rate setting is only available for **Enterprise Plan** and **Ultimate Plan**.
- A maximum number of 30,000 call rate rules is supported on Yeastar P-Series PBX System.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. Under **Rate** tab, click **Add**.
3. Set up a call rate rule:



- **Name**: Enter a name to help you identify the call rate rule. For example, enter `Local_Outbound`.
- **Match Prefix**: Optional. Define the dialing prefix to match the call rate rule.

> **Note:**
> Only outbound calls matching the dialing prefix will apply this rate.

- **Number Length**: Optional. Define the length of the dialed number to match the call rate rule.

> **Note:**
> Only the dialed number whose length is shorter than or equal to the value will match this rule.

- **Rate**: Enter a call rate. After the initial time, each billing unit will be charged with this rate.
- **Billing Unit (s)**: Define the time increment (in seconds) that will be used to calculate the fee for a call after the initial time. The default value is 60 seconds.

For example, set **Rate** to 0.5 and **Billing Unit** to 60 seconds. In this way, the fee for a call will increase by 0.5 every 60 seconds.

- **Initial Time (s)**: Define the initial period of time (in seconds) during which the call will be charged with the initial cost.
- **Initial Cost**: Define the fixed cost incurred over the preset initial time.

  For example, set **Initial Time** to 120 seconds and **Initial Cost** to 2. In this case, it costs 2 for the call within 2 minutes. After 2 minutes, the call will be charged with the preset rate.

4. Click **Save** and **Apply**.

Result

- The call rate rule is created. Any outbound calls matching the rule will be charged with the call rate as the following formula from now on.

  ```
  Amount = Initial Cost + [(Talk Duration - Initial Time) / Billing Unit] * Rate
  ```

  > **Note:**
  > If the value to be multiplied by rate has decimals, it will be rounded upwards to the nearest integer.

- If you create more than one call rate rules in the list, the system will match outbound calls with these rules from the top down. You can click ⤒ ^ ⌄ ⤓ to adjust the priority.

What to do next

You can check the call accounting fee for extensions, extension groups, or departments in call reports.

For more information, see Extension Call Accounting Report and Extension Call Accounting Details Report.

Manage Call Rate Rules

This topic describes how to edit and delete call rate rules.

Prerequisites

Management of call rate rules is only available for **Enterprise Plan** and **Ultimate Plan**.

Adjust priority of call rate rules

When users make outbound calls, the system will match the outbound calls with call rate rules in the list from the top down, and use the first matched rule to charge the outbound calls. You can adjust the priority of call rate rules according to your needs.

1. Log in to PBX web portal, go to **Reports and Recording Files > Call Reports**.
2. Under **Rate** tab, click ⤒ ^ v ⤓ to adjust the priority of call rate rules.
3. Click **Apply**.

Edit a call rate rule

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. Under **Rate** tab, click ✎ beside a call rate rule.
3. Edit the call rate rule.

> **Important:**
> Modifying the rate would affect the newly generated call billing statistics.

4. Click **Save** and **Apply**.

Delete call rate rules

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. Click **Rate** tab.
3. To delete a call rate rule, do as follows:
   a. On the right of a desired call rate rule, click 🗑.
   b. In the pop-up window, click **OK**.
4. To bulk delete call rate rules, do as follows:
   a. Select the checkboxes of desired call rate rules, then click **Delete**.
   b. In the pop-up window, click **OK**.

Export and Import Call Rate Rules

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

Prerequisites

Management of call rate rules is only available for **Enterprise Plan** and **Ultimate Plan**.

Export all the call rate rules

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. Under **Rate** tab, click **Export**.

   A CSV file is saved to your computer. To check and edit parameters in the CSV file, see Rate Parameters.

Import call rate rules

We recommend that you export call rate 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 imported parameters meet requirements. For more information, see Rate Parameters.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. Under **Rate** tab, click **Import**.
3. In the pop-up window, click **Browse**, and select your CSV file.
4. Click **Import**.
   The call rate rules in the CSV file will be displayed in reverse order in the **Rate** list.

> **Note:**
> The system matches outbound calls with call rate rules from top down. In case of need, you can click ⤒ ^ v ⤓ to adjust the priority of call rate rules.

Related information

Import and Export -FAQ

Call Accounting Report

Extension Call Accounting Report

Extension Call Accounting report provides a quick overview of the bills for outbound calls made by extensions via specific trunks, and can be broken down to specific extensions, groups of extensions, or organizations of extensions. This topic introduces how to access the report and explains the key metrics in detail.

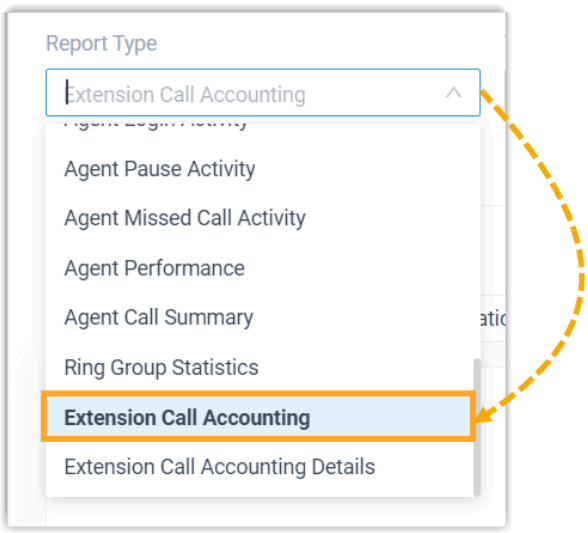
Prerequisites

- You have subscribed **Enterprise Plan** or **Ultimate Plan**.
- You have set up at least one call rate rule, otherwise the system wouldn't know how to charge outbound calls.

  For more information, see Add a Call Rate Rule.

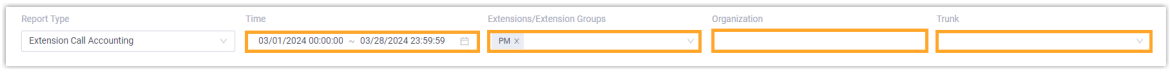
Access Extension Call Accounting report

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Extension Call Accounting**.

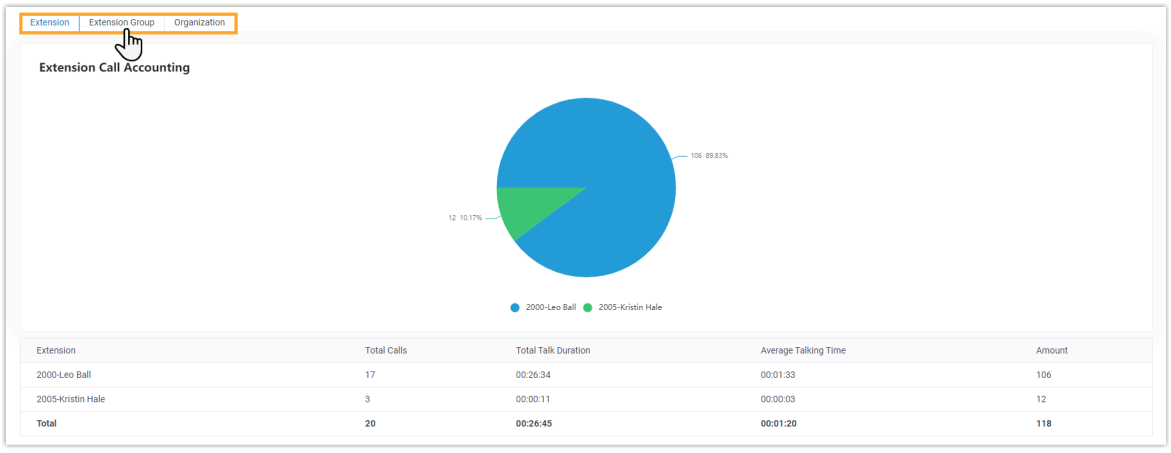


3. Filter data by system time, extension(s), extension group(s), organization(s), or trunk.

> **Note:**
> **Organization** filter is displayed only when you enable **Organization Management** feature (Path: **PBX Settings > Preferences**).



A report that meets the filter criteria is displayed on the page, as shown below.



> **Note:**
> - You can click the tab at the top-left corner to switch between the breakdown reports.

- If you filter data by extension group(s), the report will NOT include the call statistics from unknown source (the record where **Extension** column is displayed as **Other**).
- If you filter data by organization(s), the report data will include the selected organization and its subordinate departments, but will NOT include the call statistics from unknown source (the record where **Extension** column is displayed as **Other**).

Report details

We take the above report as an example to introduce the key metrics for **Extension Call Accounting** report.

Metric	Description
Total Calls	The total number of outbound calls made where a call rate rule is applied.
Total Talk Duration	The total time between calls answered and calls ended.
Average Talking Time	The average time between calls answered and calls ended.
Amount	The call cost.
Total (displayed in row)	The sum of all the values in each column. **Note:** • This metric is only available for extension and extension group. • If you select multiple extension groups and one of the extensions belongs to two or more extension groups, the call statistics for the extension will be calculated more than once.

Related information

Extension Call Accounting Details Report

Extension Call Accounting Details Report

Extension Call Accounting Details report provides granular insights into the bills for each outbound call made by extensions via specific trunks. This topic introduces how to access the report and explains the key metrics in detail.

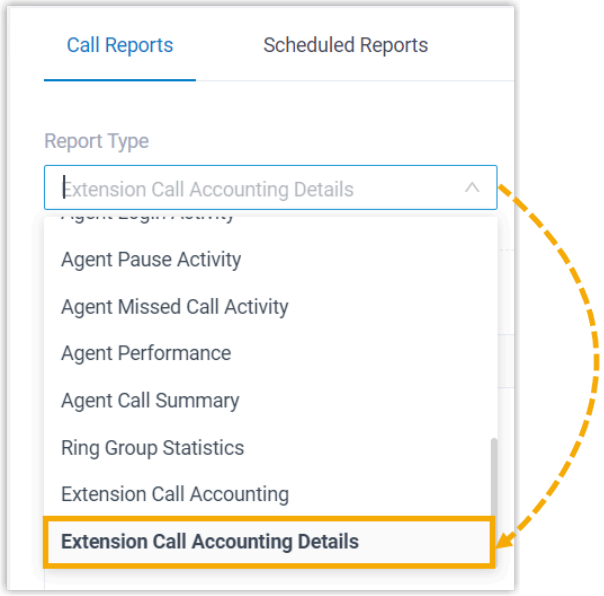
Prerequisites

- You have subscribed **Enterprise Plan** or **Ultimate Plan**.
- You have set up at least one call rate rule, otherwise the system wouldn't know how to charge outbound calls.

  For more information, see Add a Call Rate Rule.

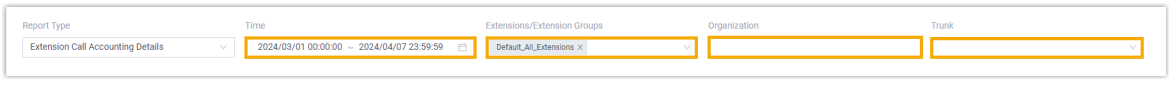
Access Extension Call Accounting Details report

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Extension Call Accounting Details**.

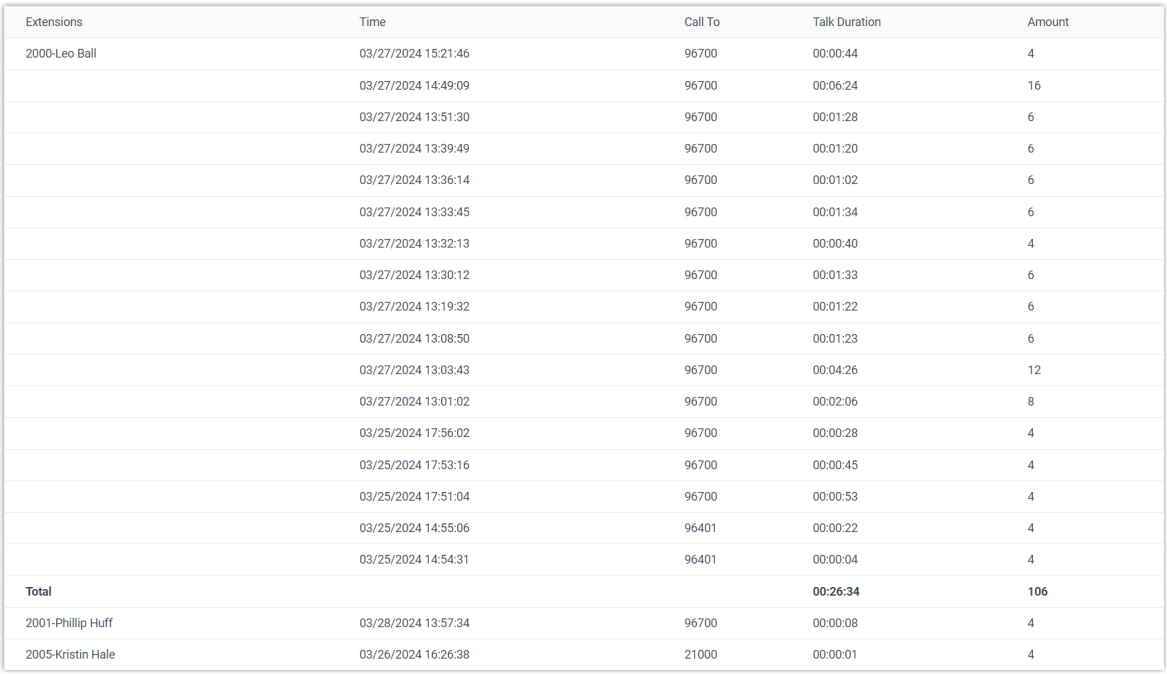


3. Filter data by system time, extension(s), extension group(s), organization(s), or trunk.

> **Note:**
> **Organization** filter is displayed only when you enable **Organization Management** feature (Path: **PBX Settings > Preferences**).



A report that meets the filter criteria is displayed on the page, as shown below.



Extensions	Time	Call To	Talk Duration	Amount
2000-Leo Ball	03/27/2024 15:21:46	96700	00:00:44	4
	03/27/2024 14:49:09	96700	00:06:24	16
	03/27/2024 13:51:30	96700	00:01:28	6
	03/27/2024 13:39:49	96700	00:01:20	6
	03/27/2024 13:36:14	96700	00:01:02	6
	03/27/2024 13:33:45	96700	00:01:34	6
	03/27/2024 13:32:13	96700	00:00:40	4
	03/27/2024 13:30:12	96700	00:01:33	6
	03/27/2024 13:19:32	96700	00:01:22	6
	03/27/2024 13:08:50	96700	00:01:23	6
	03/27/2024 13:03:43	96700	00:04:26	12
	03/27/2024 13:01:02	96700	00:02:06	8
	03/25/2024 17:56:02	96700	00:00:28	4
	03/25/2024 17:53:16	96700	00:00:45	4
	03/25/2024 17:51:04	96700	00:00:53	4
	03/25/2024 14:55:06	96401	00:00:22	4
	03/25/2024 14:54:31	96401	00:00:04	4
Total			**00:26:34**	**106**
2001-Phillip Huff	03/28/2024 13:57:34	96700	00:00:08	4
2005-Kristin Hale	03/26/2024 16:26:38	21000	00:00:01	4

Report details

We take the above report as an example to introduce the key metrics for **Extension Call Accounting Details** report.

Metric	Description
Time	When the outbound call was made.
Call To	The callee number.
Talk Duration	The time between call answered and call ended.
Amount	The call cost.
Total	Total talk duration and amount for extensions that make two or more outbound calls.
Total for All	Total talk duration and amount for the selected extensions. **Note:** This metric is displayed only when you set **Trunk** filter to a specific trunk.

Related information

[Extension Call Accounting Report]

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:

> **Note:**
> The **Speech to Text** feature on Yeastar P-Series PBX System is free. However, you will need to pay for the Speech-to-Text service of the third-party platforms.

- **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 UC Clients

Users can check the transcribed text for each voicemail on Linkus Web Client, Linkus Desktop Client, and Linkus Mobile Client.

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 describes 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.

Service cost

Google Cloud Speech-to-Text service provides a free amount of 60 minutes per month, you will be charged if the minutes of audio processed per month exceeds the free amount. For more information about the pricing, see Google Cloud Speech-to-Text Pricing.

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 web 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

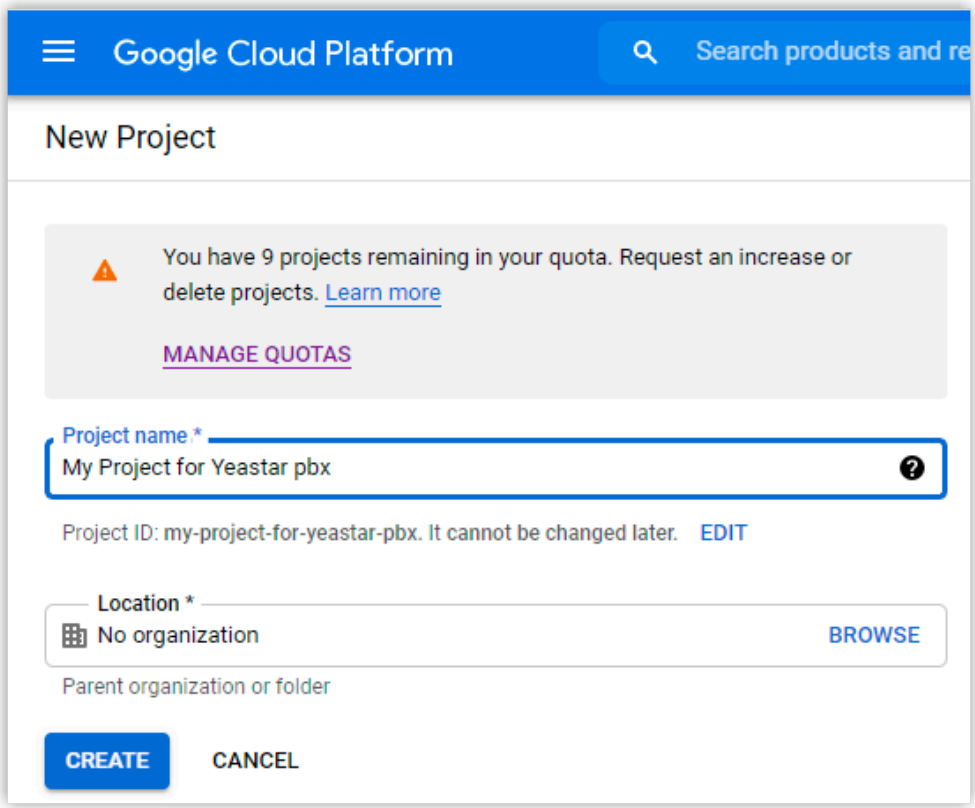
1. Log in to Google Cloud Platform.
2. In the top bar, click **My First Project** to open the project list.



3. On the **Select a project** page, click **NEW PROJECT** in the top-right corner.



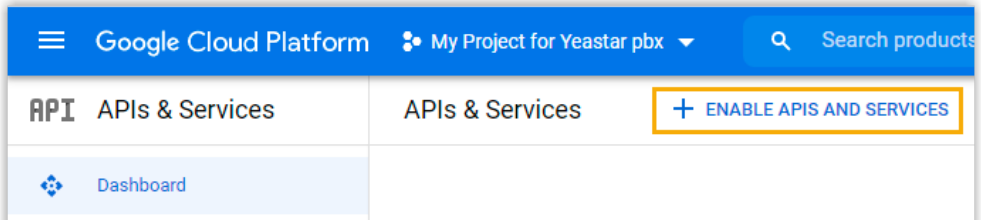
4. On the **New Project** page, set a project name, and click **CREATE**.



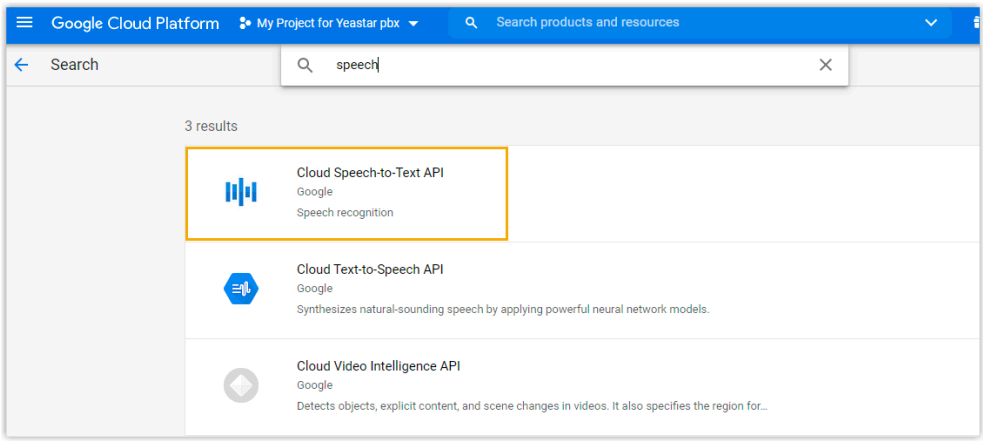
A new project is created, you can select the new project in the project list.

Step2. Enable Speech-to-Text API service on Google Cloud Platform

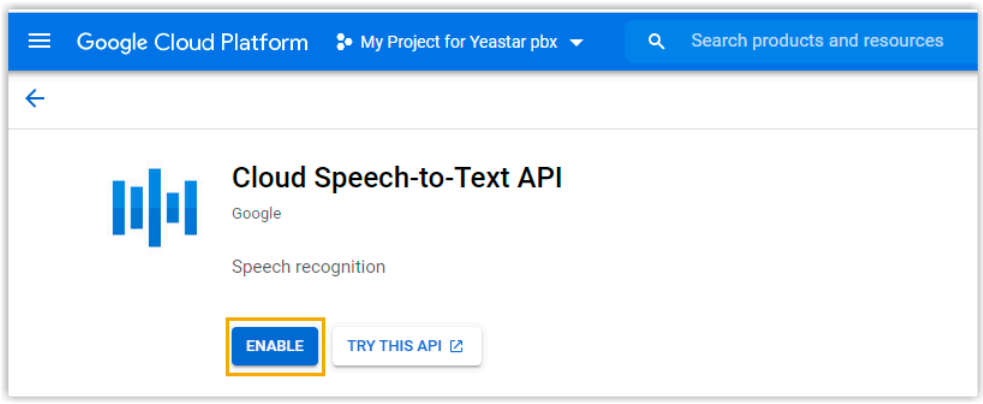
1. In the top-left conner, click ☰ to open the navigation menu, and go to **API & Services > Dashboard**.
2. Click **ENABLE APIS AND SERVICES**.



3. In the API Library, enter `speech` in the search box and press **`Enter`**, then select **Cloud Speech-to-Text API**.



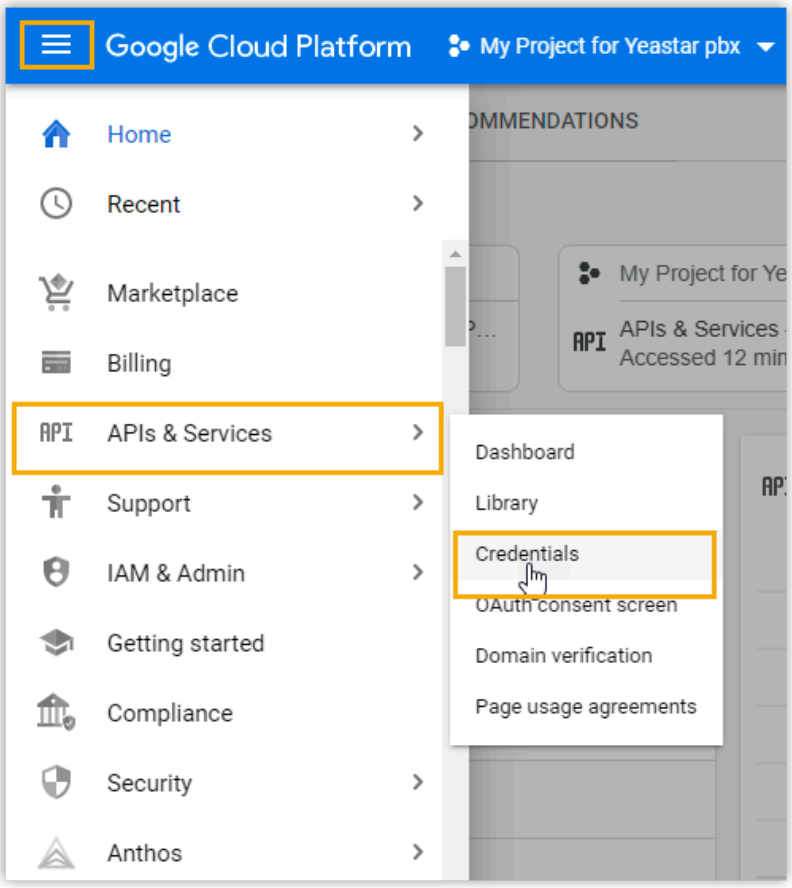
4. Click **ENABLE** button for the **Cloud Speech-to-Text API**.



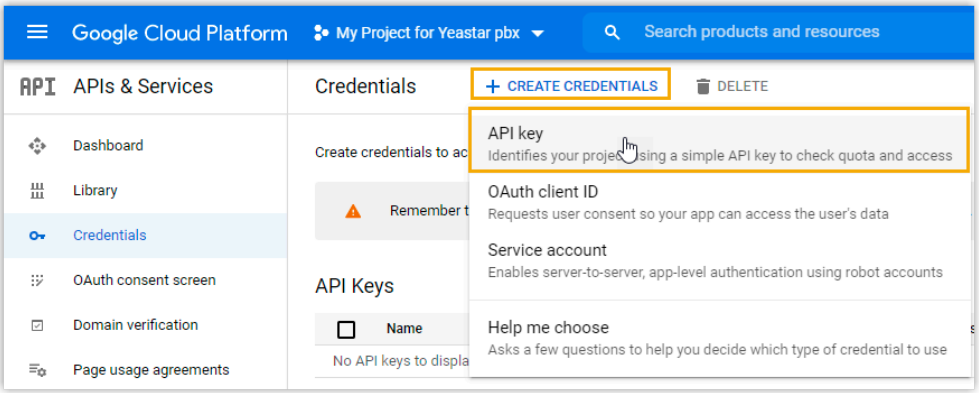
The Speech-to-Text service is enabled.

Step3. Create API credentials on Google Cloud Platform

1. In the left navigation panel, go to **API & Services > Credentials**.

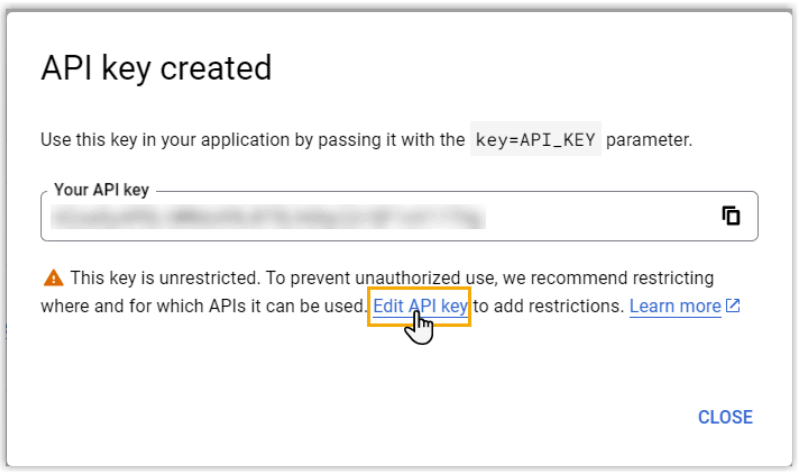


2. Click **CREATE CREDENTIALS** and select **API key**.



3. In the pop-up window, click **Edit API key** to edit and set restrictions for the key.

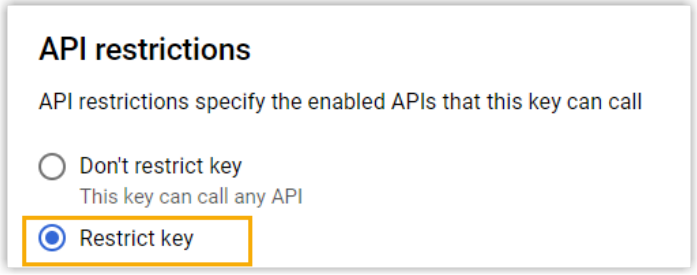
> **Important:**
> For security purpose, you need to restrict your API key, ensuring only authorized requests are made with your API key.



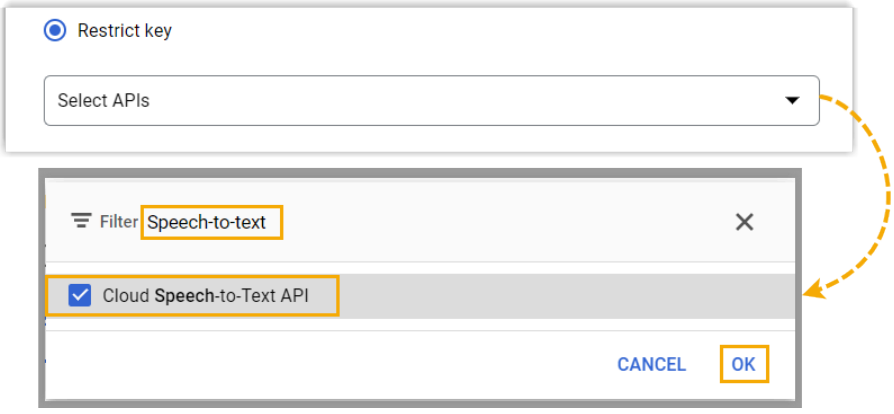
4. In the **Edit API key** page, complete the following configurations.
   a. In the **Name** field, set a name to help you identify the API key.



   b. In the **API restrictions** section, select **Restrict key**.



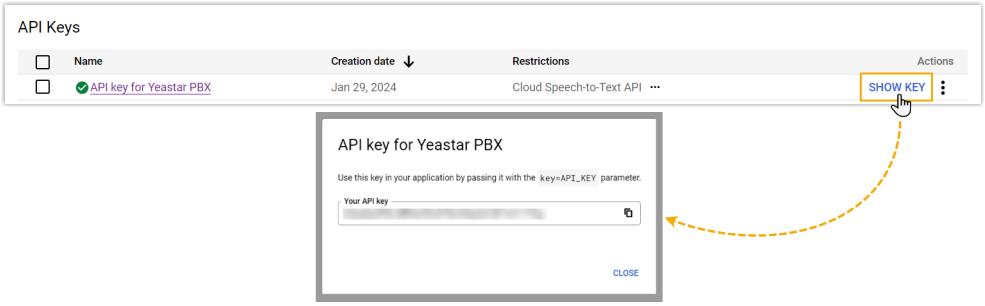
   c. In the **Select APIs** drop-down list, search and select the **Cloud Speech-to-Text API**, then click **OK**.



d. At the bottom of the page, click **SAVE** to apply your configuration.

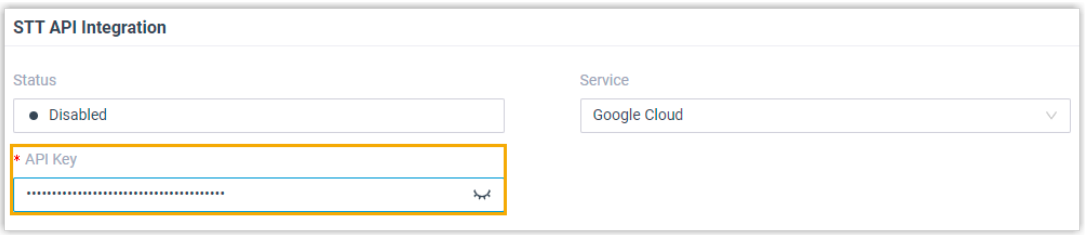
The API key is now only allowed to call the Cloud Speech-to-Text API.

5. In the **Credentials** page, click **SHOW KEY** beside the restricted API key, then in the pop-up window to copy the key.



Enable Speech to Text (STT) integration on Yeastar P-Series PBX System

1. Log in to PBX web 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.



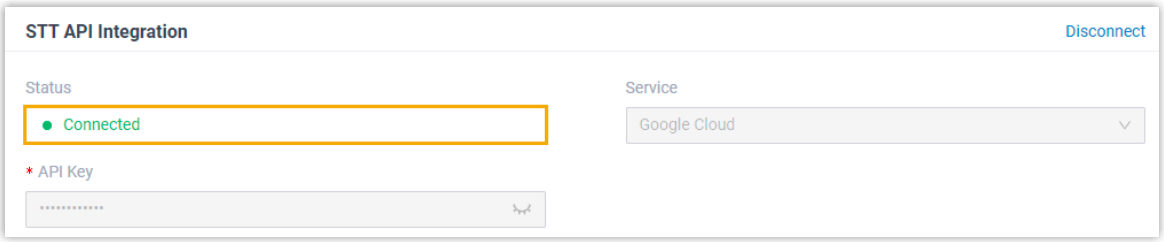
3. In **Settings** section, select the transcription language.

   The audio messages will be transcribed to text in the selected language.

> **Note:**
> If the language of voicemail is different from 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**.



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

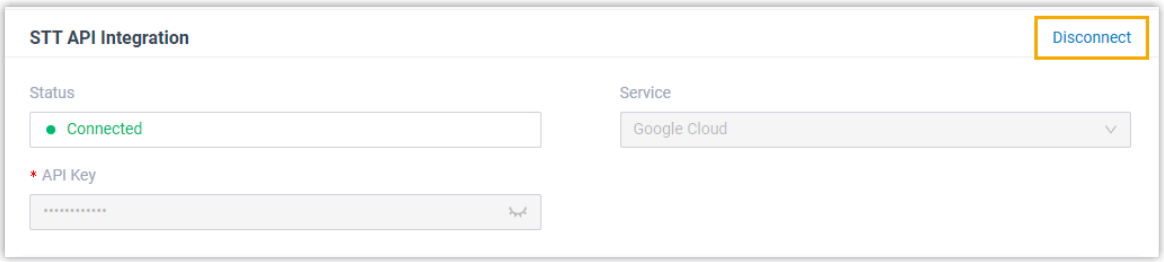
Speech to Text (STT) Overview
Disconnect Speech to Text (STT) API Integration

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 web 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 box, 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 web portal, go to **Integrations > 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 addresses.

> To prevent the permitted IP from being blocked by the system, 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

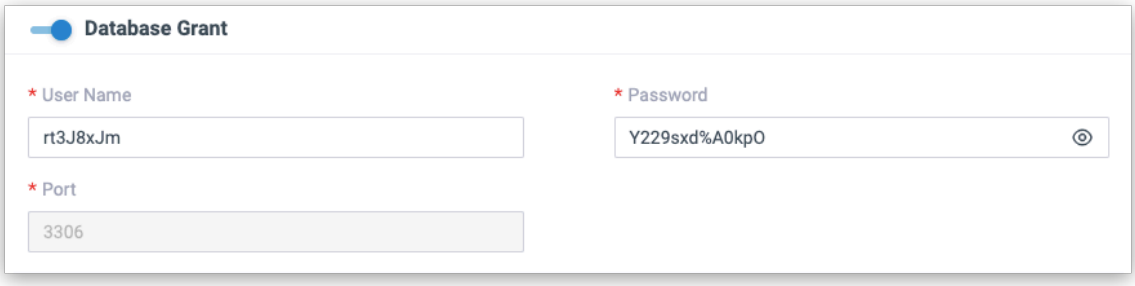
Yeastar P-Series PBX System allows you to access the system database and get CDR data. This topic describes how to get CDR data from the PBX database via Navicat software.

Procedure

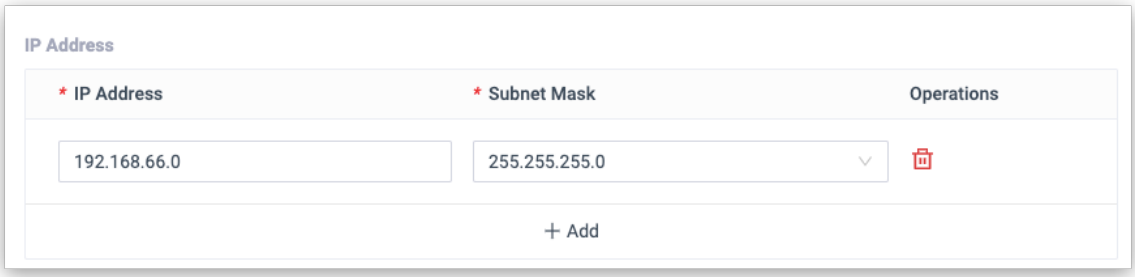
1. Grant access to the PBX database
2. Access the PBX database via Navicat software

Grant access to the PBX database

1. Log in to PBX web 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.



   - **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.



   a. Click **Add**.
   b. Enter the permitted IP address and subnet mask.

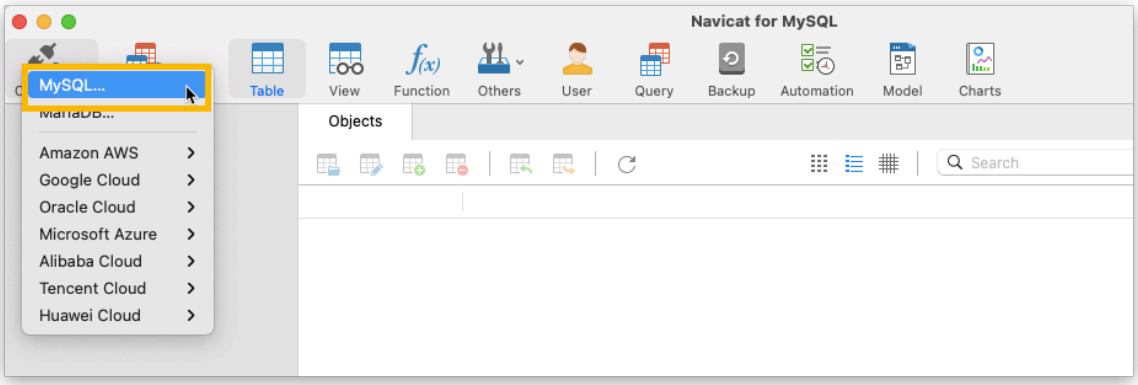
      In this example, enter IP address `192.168.66.0` and subnet mask `255.255.255.0` to allow all IP addresses in the segment 192.168.66.X to access the database.

> **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`.

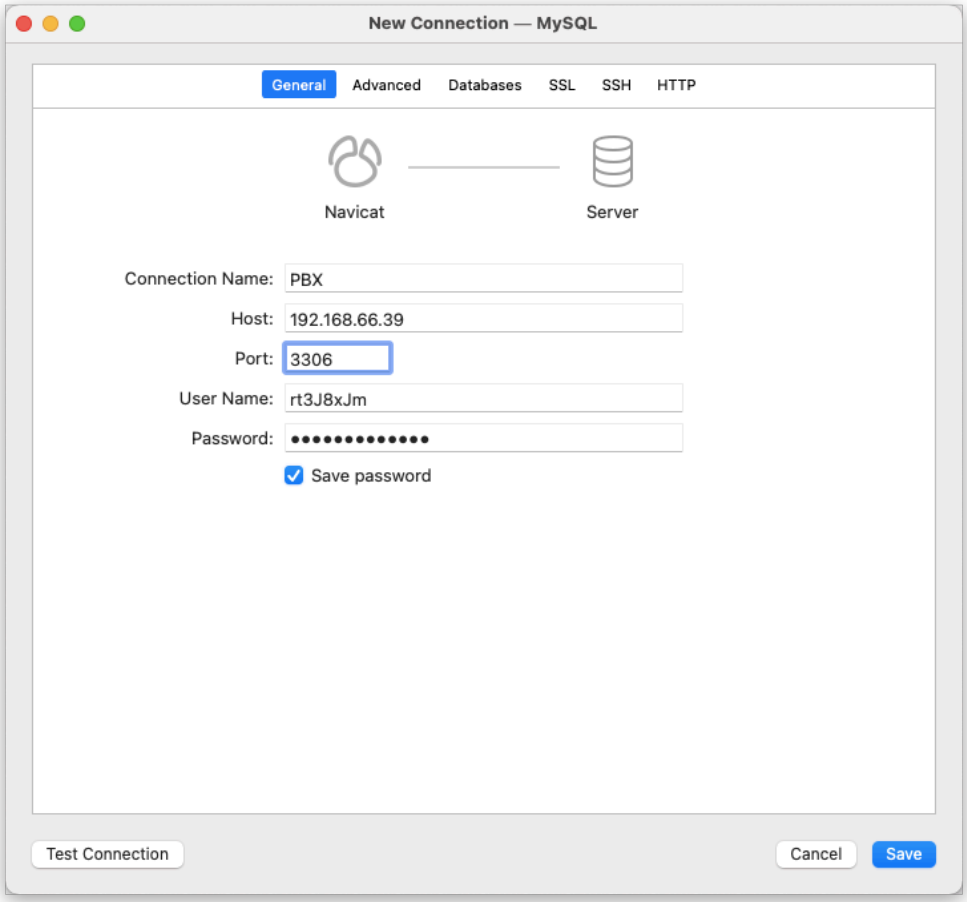
4. Click **Save** and **Apply**.

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**.



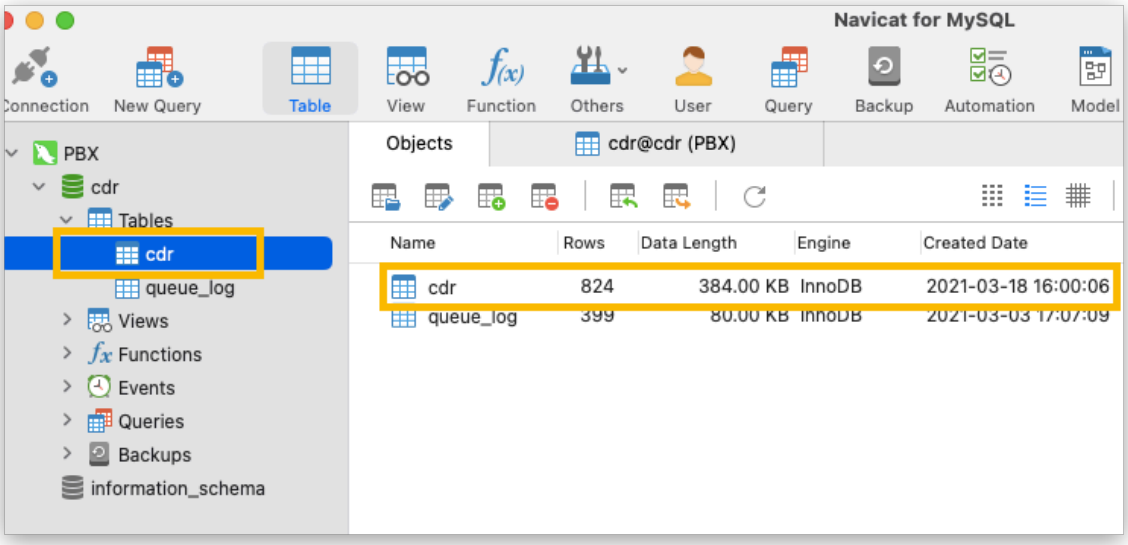
3. In the pop-up window, enter the following information:



- **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	Ringing duration of the call
talkduration	Talk duration of the call (calculates after the call is answered)
disposition	Call status: • NO ANSWER • FAILED • BUSY • ANSWERED • VOICEMAIL • CONGESTION
amaflags	System internal flag
calltype	Communication Type • Internal • Inbound • Outbound • Callback
accountcode	Pin code
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
reasonpartyc	System internal flag
reasonpartyd	System internal flag
reasonpartye	System internal flag

Field	Descriptions
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

References

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
- Organization Parameters
- Contacts Parameters
- Holidays Parameters
- Speed Dial Number Parameters
- Emergency Number Parameters
- Auto Provisioning Phone Information Parameters
- Trunk Parameters
- Trunk DIDs/DDIs Parameters
- Trunk Outbound Caller ID Parameters
- Inbound Caller ID Reformatting Rule Parameters
- Inbound Route Parameters
- DID Number to Specific Extension Parameters
- Outbound Route Parameters
- Static Defense Rule Parameters

- Auto Defense Rule Parameters
- Outbound Call Frequency Restriction Rule Parameters
- Rate Parameters
- Allowed Numbers Parameters
- Blocked Numbers 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 lease one is required	The maximum character length is 63. **Note:** **First Name** will be filled with a value of *Extension Number* if you leave these fields empty.	Extension number
Last name	The last name of extension user.			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 web portal.	Required	Must contain numbers, uppercase, and lowercase letters. The minimum character length is 10 and the maximum is 63. **Note:**	Generate Randomly

Parameter	Description	Importance	Restriction	Default Value
			User Password will be generated randomly if you leave this field empty.	
System Prompt Language	The language of the system prompts heard by the extension during a call.	Optional	Permitted value: `follow_system` or one of the prompt language existed in PBX System Prompt (e.g. `German`). **Note:** **System Prompt Language** will be filled with default value *`follow_system`* if the language you enter does not exist in PBX, or if you leave this field empty.	follow_system
Email Language	The language of email notifications for the extension.	Optional	Permitted value: `follow_system` or one of the email language that existed in PBX (e.g. `German`). **Note:** **Email Language** will be filled with default value *`follow_system`* if the language you enter does not exist in PBX, or if you leave this field empty.	follow_system
Organization	The organization to which the extension user belongs.	Optional	Permitted value: The organization names that existed in PBX. **Note:** • **Organization** will be filled with default value if you leave this field empty. • When entering the organization name, it must be the full path of parent organization, connected by	Root organization, namely the Company Name.

Parameter	Description	Importance	Restriction	Default Value
			`/`. For multiple organizations, please use `&` to separate. Examples are given below: • If belong to root organization "Yeastar", enter `Yeastar`. • If belong to first-layer organization "Marketing Center", enter `Yeastar/Marketing Center`. • If belong to second-layer organization "Support Team", enter `Yeastar/Marketing Center/Support Team`. • If belong to multiple organizations, enter `Yeastar/Marketing Center&Yeastar/Product Management Center`.	
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
Extension Number	The extension's number.	Required	Extension Number cannot be duplicated, and only numbers are allowed. The maximum character length is 8.	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`	Extension Number

Parameter	Description	Importance	Restriction	Default Value
			`Number` if you leave this field empty.	
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: • `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. • `4`: Allow four phones to register with the extension. • `5`: Allow five phones to register with the extension. **Note:** **IP Phone Concurrent Registrations** will be filled with default value `1` if you leave this field empty.	1
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

Parameter	Description	Importance	Restriction	Default Value
Enable Voicemail	Whether to enable or disable voicemail feature.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Enable Voicemail** will be filled with default value *1* 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: • *0*: Disable • *1*: Enable **Note:** **Voicemail PIN Authentication** will be filled with default value *1* 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
Voicemail Language	The language of the system prompts heard by caller when they access the extension's voicemail box.	Optional	Permitted value: `follow_system` or one of the prompt language existed in PBX System Prompt (e.g. `German`). **Note:** **Voicemail Language** will be filled with default value *follow_system* if the language you enter does not exist in PBX, or if you leave this field empty.	follow_system

Parameter	Description	Importance	Restriction	Default Value
New Voicemail Notification	The notification type for new voicemail.	Required if **Enable Voicemail** = *1*	Permitted value: • *no*: No Email Notifications • *with_attach*: Send Email Notifications with Attachment • *without_attach*: Send Email Notifications without Attachment **Note:** **New Voicemail Notification** will be filled with default value *no* if you leave this field or Email Address empty.	no
Send to	Specify the email address for receiving notification emails about new voicemails.	Required if **Enable Voicemail** = *1* & **New Voicemail Notification** = *with_attach* or *without_attach*	Permitted value: • *user Email*: Send notification emails to the user's email address. • *custom Email*: Send notification emails to a custom email address.	user Email
Voicemail Email Address	Enter a custom email address for receiving notification emails about new voicemails.	Required if **Enable Voicemail** = *1* & **New Voicemail Notification** = *with_attach* or *without_attach* & **Send to** = *custom Email*	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.	N/A

Parameter	Description	Importance	Restriction	Default Value
After Notification	The way to handle voicemail message in mailbox after receiving the message notification via email.	Required if **Enable Voicemail** = `1` & **New Voicemail Notification** = `with_attach`	Permitted value: • `no`: Do Nothing • `mark_read`: Mark as read • `delete`: Delete Voicemail **Note:** **After Notification** will be filled with default value `no` if you leave these fields empty.	no
		Required if **Enable Voicemail** = `1` & **New Voicemail Notification** = `without_attach`	Permitted value: • `no`: Do Nothing • `mark_read`: Mark as read **Note:** **After Notification** will be filled with default value `no` if you leave these fields empty.	no
Play Date and Time	Whether to announce arrival time of the message before playing the voicemail message.	Required if **Enable Voicemail** = `1`	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Play Date and Time** will be filled with default value `0` if you leave this field empty.	0
Time Display Format	The time format for announcing the message arrival time.	Required if **Play Date and Time** = `1`	Permitted value: • `Follow System` • `12-hour format` • `24-hour format` **Note:**	Follow System

Parameter	Description	Importance	Restriction	Default Value
			Time Display Format will be filled with default value if you leave this field empty.	
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: • *0*: Disable • *1*: Enable **Note:** **Play Caller ID** will be filled with default value *0* if you leave this field empty.	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: • *0*: Disable • *1*: Enable **Note:** **Play Message Duration** will be filled with default value *0* if you leave this field empty.	0
Send email notification when the User Password is changed	Whether to send email notification when the User Password is changed.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Send email notification when the User Password is changed** will be filled with default value *1* if you leave this field empty.	1
Send email notifications on missed calls	Whether to send email notifications on missed calls.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:**	0

Parameter	Description	Importance	Restriction	Default Value
			Send email notifications on missed calls will be filled with default value `0` if you leave this field empty.	
Recording operation	Whether to allow users to switch their own recording status during a call.	Required	Permitted value: • `0`: No permission • `1`: Pause/Resume • `2`: Start/Pause/Resume **Note:** **Recording operation** will be filled with default value `0` if you leave this field empty.	0
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: • `0`: Disable • `1`: Enable **Note:** **All Busy Mode for Endpoints** will be filled with default value `0` if you leave this field empty.	0
All Reject Mode for Endpoints	Whether to stop the incoming call from ringing other endpoints and forward to the Busy destination when it was rejected on an endpoint.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **All Reject Mode for Endpoints** will be filled with default value `0` if you leave this field empty.	0
Allow Being Monitored	Whether to allow the user's calls to be monitored.	Required	Permitted value: • `0`: Disable • `1`: Enable	1

Parameter	Description	Importance	Restriction	Default Value
			Note: **Allow Being Monitored** will be filled with default value `1` if you leave this field empty.	
Video Preview	Whether to allow other extension users to click a specific button to preview the extension's video when receiving a call from the extension.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Video Preview** will be filled with default value `0` if you leave this field empty.	0
Auto Preview	Whether to allow other extension users to automatically preview the extension's video when receiving a call from the extension.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Auto Preview** will be filled with default value `0` if you leave this field empty.	0
Hot Desking	Whether to allow the extension to log in to a hot desking phone.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Hot Desking** will be filled with default value `0` if you leave this field empty.	0
Log out of Queue	Whether to automatically log out the dynamic agent from the queue when the user log out of	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:**	0

Parameter	Description	Importance	Restriction	Default Value
	a hot desking phone.		**Log out of Queue** will be filled with default value *0* if you leave this field empty.	
Automatic Guest Out	Whether to automatically log out the extension from a hot desking phone.	Optional	Permitted value: • 0: Never • 1: After • 2: At Daily **Note:** **Automatic Guest Out** will be filled with default value 0 if you leave this field empty.	0
After hr.	The hour of the specified time period for automatically logging out the extension from a hot desking phone.	Required if **Automatic Guest Out** = *1*	Permitted value: 00 - 23 **Note:** **After hr.** will be filled with default value 08 if you leave this field empty.	08
After min.	The minute of the specified time period for automatically logging out the extension from a hot desking phone.	Required if **Automatic Guest Out** = *1*	Permitted value: 00 - 59 **Note:** **After min.** will be filled with default value 00 if you leave this field empty.	00
At Daily	The time for automatically logging out the extension from a hot desking phone on a daily basis.	Required if **Automatic Guest Out** = *2*	Time Format: HH:MM (e.g. 13:30) **Note:** The End Time must be later than the Start Time.	N/A
DTMF Mode	The mode for sending DTMF tones.	Required	Permitted value: *rfc4733*, *info*, *inband* or *auto*. **Note:**	rfc4733

Parameter	Description	Importance	Restriction	Default Value
			DTMF Mode will be filled with default value *rfc4733* if you leave this field empty.	
Transport	The protocol for transport.	Required	Permitted value: *udp*, *tcp*, or *tls*. **Note:** **Transport** will be filled with default value *udp* if you leave these fields empty.	udp
Qualify	Whether to send the SIP OPTIONS packet periodically to the SIP device to check if the device is online.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Qualify** will be filled with default value *1* if you leave this field empty.	1
T.38 Support	Whether to support T.38 fax for this extension.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **T.38 Support** will be filled with default value `0` if you leave this field empty.	0
NAT	Whether to enable NAT for this extension.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **NAT** will be filled with default value *1* if you leave this field empty.	1

Parameter	Description	Importance	Restriction	Default Value
SRTP	Whether to encrypt RTP packets.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **SRTP** will be filled with default value `0` if you leave this field empty.	0
Allow Remote Registration	Whether to allow user to register a remote SIP extension to PBX.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Allow Remote Registration** will be filled with default value `0` if you leave this field empty.	0
Disable Outbound Calls	Whether to restrict the user from making outbound calls.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Disable Outbound Calls** will be filled with default value `0` 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: • `0`: Disable • `1`: Enable **Note:** **Disable Outbound Calls outside Business Hours** will be filled with default	0

Parameter	Description	Importance	Restriction	Default Value
			value `0` if you leave this field empty.	
Disallow International Calls	Whether to restrict the user from making international calls.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Disable International Calls** will be filled with default value `1` if you leave this field empty.	1
Outbound Route Permission	Specify the outbound routes that this extension is allowed to use.	Optional	Permitted value: one or more outbound route names existed in PBX. **Note:** • 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.	N/A
Max Outbound Call Duration (s)	The maximum call duration in seconds for making outbound calls from this extension.	Required	Only numbers are allowed. Specially, `-1` means follow system and `0` means unlimited. The maximum character length is 7. **Note:** **Max Outbound Call Duration (s)** will be filled	-1

Parameter	Description	Importance	Restriction	Default Value
			with default value `-1` if you leave these fields empty.	
Outbound Call Frequency Restriction	The restriction rule(s) that used to limit the extension outbound call frequency within specified time period.	Optional	Permitted value: One or more Outbound Call Frequency Restriction names existed in PBX. **Note:** • Use & to separate multiple names, e.g. name1&name2. • 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.	Default_Ext_Outbound Call Frequency
Linkus Mobile Client	Whether to allow the extension user to log in to Linkus Mobile Client.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Linkus Mobile Client** will be filled with default value `1` if you leave this field empty.	1
Call Waiting (for Mobile Client)	Whether to receive another call while the extension user is on the phone.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Call Waiting (for Mobile Client)** will be filled with default value `1` if you leave this field empty.	1

Parameter	Description	Importance	Restriction	Default Value
Auto Answer (for Mobile Client)	Whether to automatically answer non-paging/intercom calls.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Auto Answer (for Mobile Client)** will be filled with default value *0* if you leave this field empty.	0
Auto Answer Delay Time(s) (for Mobile Client)	The delay time in seconds before automatically answering non-paging/intercom calls.	Required if **Auto Answer (for Mobile Client)** = *1*	Only numbers are allowed. The maximum allowed input is 60. **Note:** **Auto Answer Delay Time(s) (for Mobile Client)** will be filled with default value *0* if you leave this field empty.	0
Play Auto Answer Tone (for Mobile Client)	Whether to play a tone to alert the extension user when non-paging/intercom calls are auto answered.	Optional	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Play Auto Answer Tone (for Mobile Client)** will be filled with default value *1* if you leave this field empty.	1
Auto Answer Paging/Intercom Call (for Mobile Client)	Whether to automatically answer paging/intercom calls.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Auto Answer Paging/Intercom Call (for Mobile Client)** will be filled	0

Parameter	Description	Importance	Restriction	Default Value
			with default value `0` if you leave this field empty.	
Paging/Intercom Barge (for Mobile Client)	Whether to automatically answer the paging/intercom call when the extension user is already on the phone.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Paging/Intercom Barge (for Mobile Client)** will be filled with default value `0` if you leave this field empty.	0
Play Auto Answer Tone for Paging/Intercom Call (for Mobile Client)	Whether to play a tone to alert the extension user when paging/intercom calls are auto answered.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Play Auto Answer Tone for Paging/Intercom Call (for Mobile Client)** will be filled with default value `1` if you leave this field empty.	1
Linkus Desktop Client	Whether to allow the extension user to log in to Linkus Desktop Client.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Linkus Desktop Client** will be filled with default value `1` if you leave this field empty.	1
Call Waiting (for Desktop Client)	Whether to receive another call while the extension user is on the phone.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:**	1

Parameter	Description	Importance	Restriction	Default Value
			Call Waiting (for Desktop Client) will be filled with default value *1* if you leave this field empty.	
Auto Answer (for Desktop Client)	Whether to automatically answer non-paging/intercom calls.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Auto Answer (for Desktop Client)** will be filled with default value *0* if you leave this field empty.	0
Auto Answer Delay Time(s) (for Desktop Client)	The delay time in seconds before automatically answering non-paging/intercom calls.	Required if **Auto Answer (for Desktop Client)** = *1*	Only numbers are allowed. The maximum allowed input is 60. **Note:** **Auto Answer Delay Time(s) (for Desktop Client)** will be filled with default value *0* if you leave this field empty.	0
Play Auto Answer Tone (for Desktop Client)	Whether to play a tone to alert the extension user when non-paging/intercom calls are auto answered.	Optional	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Play Auto Answer Tone (for Desktop Client)** will be filled with default value *1* if you leave this field empty.	1
Auto Answer Paging/Intercom Call (for Desktop Client)	Whether to automatically answer paging/intercom calls.	Required	Permitted value: • *0*: Disable • *1*: Enable	0

Parameter	Description	Importance	Restriction	Default Value
			Note: **Auto Answer Paging/Intercom Call (for Desktop Client)** will be filled with default value `0` if you leave this field empty.	
Paging/Intercom Barge (for Desktop Client)	Whether to automatically answer the paging/intercom call when the extension user is already on the phone.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Paging/Intercom Barge (for Desktop Client)** will be filled with default value `0` if you leave this field empty.	0
Play Auto Answer Tone for Paging/Intercom Call (for Desktop Client)	Whether to play a tone to alert the extension user when paging/intercom calls are auto answered.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Play Auto Answer Tone for Paging/Intercom Call (for Desktop Client)** will be filled with default value `1` if you leave this field empty.	1
Linkus Web Client	Whether to allow the extension user to log in to Linkus Web Client.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Linkus Web Client** will be filled with default value `1` if you leave this field empty.	1

Parameter	Description	Importance	Restriction	Default Value
Call Waiting (for Web Client)	Whether to receive another call while the extension user is on the phone.	Optional	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Call Waiting (for Web Client)** will be filled with default value *1* if you leave this field empty.	1
Auto Answer (for Web Client)	Whether to automatically answer non-paging/intercom calls.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Auto Answer (for Web Client)** will be filled with default value *0* if you leave this field empty.	0
Auto Answer Delay Time(s) (for Web Client)	The delay time in seconds before automatically answering non-paging/intercom calls.	Required if **Auto Answer (for Web Client)** = *1*	Only numbers are allowed. The maximum allowed input is 60. **Note:** **Auto Answer Delay Time(s) (for Web Client)** will be filled with default value *0* if you leave this field empty.	0
Play Auto Answer Tone (for Web Client)	Whether to play a tone to alert the extension user when non-paging/intercom calls are auto answered.	Optional	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Play Auto Answer Tone (for Web Client)** will be	1

Parameter	Description	Importance	Restriction	Default Value
			filled with default value `1` if you leave this field empty.	
Auto Answer Paging/Intercom Call (for Web Client)	Whether to automatically answer paging/intercom calls.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Auto Answer Paging/Intercom Call (for Web Client)** will be filled with default value `0` if you leave this field empty.	0
Paging/Intercom Barge (for Web Client)	Whether to automatically answer the paging/intercom call when the extension user is already on the phone.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Paging/Intercom Barge (for Web Client)** will be filled with default value `0` if you leave this field empty.	0
Play Auto Answer Tone for Paging/Intercom Call (for Web Client)	Whether to play a tone to alert the extension user when paging/intercom calls are auto answered.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Play Auto Answer Tone for Paging/Intercom Call (for Web Client)** will be filled with default value `1` if you leave this field empty.	1
Linkus Pad Client (SDK)	Whether to allow the extension user to log in to Linkus Pad Client (SDK).	Required	Permitted value: • `0`: Disable • `1`: Enable	1

Parameter	Description	Importance	Restriction	Default Value
			Note: • This parameter only takes effect when Linkus SDK is enabled (Path: **Integrations > Linkus SDK**). • **Linkus Pad Client (SDK)** will be filled with default value `1` if you leave this field empty.	
Linkus Mobile Client Codec	Add necessary audio codecs for this user's Linkus Mobile Client.	Optional	Permitted value: • `ulaw` • `alaw` • `ilbc` • `g722` • `g729` • `opus` **Note:** Use commas to separate multiple codecs.	N/A
Linkus Mobile Client - ICE	Whether to enable ICE (Interactive Connectivity Establishment) for this user's Linkus Mobile Client.	Optional	Permitted value: • `0`: Disable • `1`: Enable	N/A

Related information

Export and Import SIP Extensions

Import and Export -FAQ

Organization Parameters

Descriptions for parameters in exported and imported Organization CSV file.

Parameter	Importance	Restriction	Default Value
Organization Name	Required	The maximum character length is 127.	N/A
Parent Organization	Required	Permitted value: The full path of parent organization. For multiple organizations, please use `&` to separate. Examples are shown as below: • If belong to root organization "Yeastar", enter `Yeastar`. • If belong to first-layer organization "Marketing Center", enter `Yeastar/Marketing Center`. • If belong to second-layer organization "Support Team", enter `Yeastar/Marketing Center/Support Team`. • If belong to multiple organizations, enter `Yeastar/Marketing Center&Yeastar/Product Management Center`.	N/A

Related information

Export and Import Organizations
Import and Export -FAQ

Contacts Parameters

Descriptions for parameters in exported and imported Company Contacts CSV file and Personal Contacts CSV file.

Parameter	Importance	Restriction
First Name	At lease 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.

Parameter	Importance	Restriction
		The maximum character length is 255.
Business Number	At lease 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. 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	**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. **Note:** • The feature is available for Enterprise/Ultimate Plan.

Parameter	Importance	Restriction
		• **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.

Related information

Export and Import Company Contacts
Linkus Web Client Guide - Export personal contacts
Linkus Web Client Guide - Import personal contacts
Import and Export -FAQ

Holidays Parameters

Descriptions for parameters in exported and imported Holidays CSV file.

Parameter	Importance	Restriction	Default Value
Name	Required	The maximum character length is 127. The holiday name can not be duplicated.	N/A
Holiday Type	Required	Permitted value: • `By Date` • `By Month` • `By Week` **Note:** **Holiday Type** will be filled with default value `By Date` if you leave this field empty.	By Date
Start Date (By Date)	Required if **Holiday Type** = `By Date`	Format: DD/MM/YYYY HH:MM E.g. 25/10/2020 13:30	N/A
End Date (By Date)		**Note:** The End Date must be later than the Start Date.	N/A

<table>
<tr><th>Parameter</th><th>Importance</th><th>Restriction</th><th>Default Value</th></tr>
<tr><td>Start Date (By Month)</td><td rowspan="2">Required if Holiday Type = By Month</td><td>Format: DD/MM HH:MM
E.g. 31/10 13:30

Note:
The End Date must be later than the Start Date.</td><td>N/A</td></tr>
<tr><td>End Date (By Month)</td><td>N/A</td></tr>
<tr><td>Month (By Week)</td><td rowspan="5">Required if Holiday Type = By Week</td><td>Permitted value:

• January
• February
• March
• April
• May
• June
• July
• August
• September
• October
• November
• December</td><td>N/A</td></tr>
<tr><td>Week (By Week)</td><td>Permitted value:

• First Week
• Second Week
• Third Week
• Fourth Week
• Last Week</td><td>N/A</td></tr>
<tr><td>Day (By Week)</td><td>Permitted value:

• Sunday
• Monday
• Tuesday
• Wednesday
• Thursday
• Friday
• Saturday</td><td>N/A</td></tr>
<tr><td>Start Time (By Week)</td><td>Format: HH:MM
E.g. 13:30</td><td>N/A</td></tr>
<tr><td>End Time (By Week)</td><td>Note:</td><td>N/A</td></tr>
</table>

Parameter	Importance	Restriction	Default Value
		The End Time must be later than the Start Time.	

Related information

Export and Import Holidays

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

Import and Export -FAQ

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.	N/A

Parameter	Importance	Restriction	Default Value
		Emergency number cannot be duplicated.	
Emergency Outbound Caller ID Priority	Required	Permitted value: • *emergency_first*: Trunk's Emergency Outbound Caller ID • *ext_first*: Extension's Emergency Outbound Caller ID **Note:** **Emergency Outbound Caller ID Priority** will be filled with default value *emergency_first* if you leave this field empty.	emergency_first
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
Prepend for Emergency Number	Optional	The maximum character length is 10. Numbers, letters, and characters `( ) . - + * #` are allowed.	N/A

Related information

Export and Import Emergency Numbers
Import and Export -FAQ

Auto Provisioning Phone Information Parameters

Descriptions for parameters in exported and imported Auto Provisioning Phone Information CSV file.

Parameter	Description	Importance	Restriction	Default Value
Vendor	Phone vendor.	Required	Refer to the permitted value for the supported phone vendor.	N/A

Parameter	Description	Importance	Restriction	Default Value
Model	Phone model.	Required	Refer to the permitted value for the supported phone model of various phone vendors.	N/A
MAC Address	MAC address of the phone.	Required	Only numbers `0` - `9`, letters `A` - `Z` or `a` - `z`, hyphens `-` and colons `:` are allowed. The maximum character length is 17, where you can enter a combination of letters or numbers with a total of 12 characters. Examples are given below: • FA-B5-49-1A-2B-3C • FA:B5:49:1A:2B:3C • FAB5491A2B3C	N/A
Template	The configuration template used to provision the phone.	Required	The name of default or custom template. **Tip:** To obtain the value for this parameter, go to **Auto Provisioning > Resource Repository > Default Templates / Custom Templates**, then copy the name in the **Template Name** column.	N/A
Provisioning Method	The method that is used to provision the phone.	Required	Refer to the permitted value for the supported provisioning method of different phone models.	N/A
Hot Desking Phone	Whether to set the phone as a hot desking phone.	Optional	Permitted value: • `0`: Disable. • `1`: Enable. **Note:** • **Hot Desking Phone** will be filled with default value	0

Parameter	Description	Importance	Restriction	Default Value
			`0` if you leave this field empty. • Do NOT set this parameter to `1` for DECT phones, or it will cause error when importing.	
Authentication First-time	Whether to require users to enter authentication information on the phone before triggering the first-time provisioning.	Optional	**Note:** • This parameter only takes effect on the phones that support **RPS** or **RPS FQDN** provisioning method. • If **Hot Desking Phone** is set to `1`, this parameter MUST be `0`, or it will cause error when importing. Permitted value: • `0`: Disable. • `1`: Enable. **Note:** **Authentication First-time** will be filled with a default value if you leave this field empty.	If **Hot Desking Phone** = `0`, the default value will be `1`. Otherwise, the default value will be `0`.
Assign Extension	The extension to be assigned to the phone.	Required if **Hot Desking Phone** = `0`.	**Note:** Do NOT set this parameter if **Hot Desking Phone** = `1`, or it will cause error when importing.	N/A

Parameter	Description	Importance	Restriction	Default Value
			Only numbers are allowed. For IP phones, the maximum character length is 7. For DECT phones, the maximum character length is 1024, and the format should be *Handset Number*:*Extension Number*. **Note:** Use & to separate multiple handsets. For example, 1:1002&2:1005&3:1006.	

Related information

Export and Import Auto Provisioning Phone Information
Import and Export -FAQ

Auto Provisioning Phone Information Parameters - Permitted Value

This topic provides the permitted values of the import and export Auto Provisioning phone information parameters, including Vendor, Model, and Provisioning Method.

Vendor	Model	Provisioning Method
Yealink	• AX83H, AX86R • CP920, CP925 • SIP-CP935W, SIP-CP960, SIP-CP965 • SIP-T19P_E2, SIP-T20P, SIP-T21_E2,SIP-T21P_E2, SIP-T22P • SIP-T23G, SIP-T23P, SIP-T26P, SIP-T27G, SIP-T28P, SIP-T29G, SIP-T32G, SIP-T38G • SIP-T30, SIP-T30P, SIP-T31, SIP-T31G, SIP-T31P, SIP-T31W, SIP-T33G, SIP-T33P, SIP-T34W • SIP-T40G, SIP-T40P, SIP-T41P, SIP-T41S, SIP-T41U, SIP-T42G, SIP-T42S, SIP-T42U, SIP-T43U, SIP-T44U, SIP-T44W, SIP-T46G, SIP-T46S, SIP-T46U, SIP-T48G, SIP-T48S, SIP-T48U • SIP-T52S, SIP-T53, SIP-T53W, SIP-T54S, SIP-T54W, SIP-T56A, SIP-T57W, SIP-T58, SIP-T58W, SIP-T73W,	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn

Vendor	Model	Provisioning Method
	SIP-T73U, SIP-T74W, SIP-T74U, SIP-T77U, SIP-T85W, SIP-T87W, SIP-T88W, SIP-T88V • SIP-W60B, W70B, SIP-W75DM, SIP-W80DM, SIP-W90DM • VP59 • T64LTE, T67LTE	
Fanvil	• A10, A10W, A308i, A32, A32i, A320, A320i • FH-S01 • H1, H2U, H2U-V2, H3, H3W, H4, H4W, H5, H5W, H6, H6W, H603W • i10, i10D, i10S, i10SD, i10SV, i10V, i11S, i11SV, i12, i16S, i16SV, i16V, i18S • i20S, i23S • i30, i31S, i32V, i33V, i33VF • i504, i505, i506W, i507W, i51, i51W, i52, i52W, i53, i53W, i55A, i56A, i57A • i61, i62, i63, i64, i68 • PA2, PA2S, PA3 • V50P, V60P, V60W, V61G, V61W, V62, V62 Pro, V62G, V62W, V63, V64, V65, V66, V66 Pro, V67 • W610W, W611W, W710D, W710H • X1S/X1SP, X1SG, X2, X2C, X210, X210-V2, X210i, X210i-V2 • X3SG, X3S, X3S(P) Lite, X3S(P) Pro, X3SW, X3SG Lite, X3SG Pro, X3U, X3U Pro, X301, X301G, X301W, X303, X303G, X303W, X305, X303-2 WIRE • X4, X4U, X4U-V2, X5U, X5U-V2, X5S • X6, X6U, X6U-V2 • X7, X7A, X7C, X7-V2, X7C-V2 • Y501, Y501W, Y501-Y, Y501W-Y	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Grandstream	• GAC2500, GAC2570 • GRP2601, GRP2601P, GRP2602, GRP2602P, GRP2602G, GRP2602W, GRP2603, GRP2603P, GRP2604, GRP2604P • GRP2612, GRP2612P, GRP2612G, GRP2612W, GRP2613, GRP2614, GRP2615, GRP2616 • GRP2624, GRP2634, GRP2670 • GXP1610, GXP1620, GXP1625, GXP1628, GXP1630 • GXP2130, GXP2135, GXP2140, GXP2160, GXP2170 • GHP610, GHP610W, GHP611, GHP611W, GHP620, GHP620W, GHP621, GHP621W, GHP630, GHP630W, GHP631, GHP631W • WP825	• pnp • dhcp • provision_link • provision_link_fqdn

Vendor	Model	Provisioning Method
Htek	• UC803T • UC902, UC902S, UC903 • UC912, UC912G, UC912E • UC921, UC921G, UC923, UC923U, UC924, UC924E, UC924U, UC924W, UC926, UC926E, UC926U • UCV10, UCV20, UCV50, UCV52, UCV53	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Gigaset	• Gigaset N610 IP PRO, Gigaset N670 IP PRO • Gigaset N870 IP PRO, Gigaset N870 VI PRO • GigasetP82x, GigasetP85x, GigasetP710, GigasetP810 • Maxwell Basic PRO • Maxwell 2 PRO, Maxwell 3 PRO, Maxwell 4 PRO	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Snom	• HD100, HD101, HD300, HD350W, HD351W, HM201 • M100KLE, M500 • snomD120, snomD140, snomD150 • snomD315, snomD335, snomD385 • snom710, snom712, snomD713, snom715, snomD717, snom720, snom725, snomD735, snomD785 • snomD812, snomD815, snomD862, snomD865 • snomM300, snomM400, snomM900 • snomSP800 • snomPA1P	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Flyingvoice	• FIP10, FIP11C, FIP12WP, FIP13G, FIP14G, FIP15G, FIP15GPlus, FIP16, FIP16Plus • P10, P10P, P10G, P10W, P10LTE, P11, P11P, P11G, P11W, P11LTE • P20, P20P, P20W, P20G, P21, P21P, P21W, P22P, P22G, P23G, P23GW, P24G • flyphone • i86Box_Basic, i86Box_Indoor, i86Box_2Line, i86Box_PCBA, i86Box_NFC	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Alcatel-Lucent Enterprise	• H2, H2P, H3P, H3G, H6 • M3, M3s, M5, M5s, M7, M7s, M7s-Pro, M8	• pnp • dhcp • provision_link • provision_link_fqdn

Vendor	Model	Provisioning Method
Tiptel	• 3310, 3320, 3330, 3340	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Dinstar	• C60S, C60L, C60U, C61S, C62S, C62G, C63S, C63G, C64G, C66G	• pnp • dhcp • provision_link • provision_link_fqdn
Vtech	• CTM-S2211-SPK, CTM-S2210-X, CTM-S2411-X • NG-S3211W, NG-S3311, NG-S3411W	• pnp • dhcp • provision_link • provision_link_fqdn
Mitel	• 6863i, 6865i, 6867i, 6869i, 6873i • 6920, 6930, 6940, 6905, 6910, 6915 • RFP 44, RFP 45, RFP 47, RFP 48	• dhcp • provision_link • provision_link_fqdn
Cisco	• Cisco3905 • Cisco7821 • Cisco7861 • Cisco7911 • Cisco7942 • Cisco7975 • Cisco8811 • Cisco8845 • SPA501G, SPA502G, SPA504G, SPA508G, SPA509G, SPA512G, SPA514G, SPA301, SPA303, SPA525G2	• dhcp
Avaya	• J129, J139, J159, J169, J179, J189 • 9608	• dhcp • provision_link • provision_link_fqdn

Vendor	Model	Provisioning Method
Poly	• Edge_E100, Edge_E220,Edge_E300, Edge_E320, Edge_E350, Edge_E400, Edge_E450, Edge_E500, Edge_E550 • VVX_101, VVX_201, VVX_301, VVX_310, VVX_311, VVX_401, VVX_410, VVX_411, VVX_501, VVX_601, VVX_150, VVX_250, VVX_350, VVX_450	• dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Wildix	• WP410R2, WP480R2, WP480R3, WP480R4, WP490R2, WP490R3	• dhcp • provision_link • provision_link_fqdn
Xenios	• ICD012	• dhcp • provision_link • provision_link_fqdn
Huawei	• eSpace 7910, eSpace 7950, eSpace 8950, eSpace 8950HK • IP Phone 7920, IP Phone 7960	• dhcp • provision_link • provision_link_fqdn
NEC	• DT700 ITL-2E-1P, DT700 ITL-6DE-1P, DT700 ITL-12D-1P, DT700 ITL-24D-1P, DT700 ITL-8LD-1P, DT700 ITL-8LDE-1P, DT700 ITL-12DG-3P, DT700 ITL-12CG-3P • DT820 ITY-6D-1P, DT820 ITY-8LDX-1P, DT820 ITY-8LCGX-1P, DT820 ITY-6DG-1P, DT820 ITY-32LDG-1P, DT820 ITY-32LCG-1P • DT900 ITK-6D-1P, DT900 ITK-12D-1P, DT900 ITK-8LCX-1P, DT900 ITK-8TCGX-1P, DT900 ITK-6DG-1P, DT900 ITK-12DG-1P, DT900 ITK-32LCG-1P, DT900 ITK-32TCG-1P, DT900S ITK-6DGS-1P, DT900S ITK-32LCGS-1P, DT900S ITK-32TCGS-1P	• dhcp • provision_link • provision_link_fqdn

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	
Name	The trunk name.	Required	The maximum character length is Space and special characters are Trunk's name cannot be duplicate
Trunk Status	Whether to enable or disable the trunk.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Trunk Status** will be fille empty.
Trunk Type	Trunk type.	Required	Permitted value: • `peer` • `register` **Note:** • Importing Account • **Trunk Type**will be leave this field emp
Transport	The transport protocol that is provided by the ITSP.	Required	Permitted value: `udp`, `tcp`, `tls`, o **Note:** **Transport** will be filled wi fields empty.
Hostname/IP	The IP address or the domain of the ITSP.	Required	The maximum character length is
Port	The trunk port.	Required	Only numbers between 0 and 655
Domain	The domain in SIP URI of a specific header like From, To header. **Note:**	Required	The maximum character length is

Parameter	Description	Importance	
	If the domain is not provided by ITSP, enter the same value as **Hostname/IP**.		
Username	The username to register to the ITSP.	Required if **Trunk Type** = `register`	The maximum character length is
Password	The password that is associated with the username.	Required if **Trunk Type** = `register`	The maximum character length is
Authentication Name	The authentication name to register to the ITSP.	Optional	The maximum character length is
Enable Outbound Proxy	Whether to enable or disable outbound proxy.	Required if **Trunk Type** = `register`	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Enable Outbound Proxy** leave this field empty.
Outbound Proxy Server	The address of outbound proxy server.	Required if **Enable Outbound Proxy** = `1`	The maximum character length is
Port of Outbound Proxy Server	The port of outbound proxy server.	Required if **Enable Outbound Proxy** = `1`	Only numbers between 1 and 655
Codec Setting	The audio codec for trunk.	Required	Permitted value: `ulaw`, `alaw`, `g729` `g726`, `speex`, `adpcm`, `vp8`, or `mpeg` For multiple Codec, please enter e.g. first_value1&second_value2. **Note:** If the value you enter is no skipped.
DTMF Mode	The default mode for sending DTMF tones.	Required	Permitted value: `rfc4733`, `info`, **Note:** **DTMF Mode** will be filled field empty.

Parameter	Description	Importance	
DTMF FMTP	The value of the DTMF fmtp attribute when the DTMF mode is *rfc4733*.	Optional	Permitted value: *0-16*, *0-15*. **Note:** This field will be filled with empty.
Qualify	Whether to send SIP OPTION packet to check if the SIP device is up.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Qualify** will be filled with
Enable SRTP	Whether to enable or disable SRTP (encrypted RTP) for the trunk.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Enable SRTP** will be filled empty.
T.38 Support	Whether to enable or disable T.38 fax.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **T.38 Support** will be fille empty.
Inband Progress	Whether to enable or disable inband progress.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Inband Progress** will be field empty.

Parameter	Description	Importance	
Ignore 183 Message without SDP	Whether to ignore 183 messages without SDP.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Ignore 183 Message wit** if you leave this field empt
Forward the 180 (SDP) Message Following the Peer's Format	Whether the PBX will send a 180 message with SDP, depending on whether the 180 message received from the other party contains SDP.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Forward the 180 (SDP)** will be filled with default va
Enable RTP Keep-alive	Whether to enable or disable RTP keep-alive.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Enable RTP Keep-alive** leave this field empty.
Maximum Concurrent Calls	Specify the maximum number of concurrent calls allowed in the trunk.	Required	Only numbers are allowed. Specially, 0 means unlimited. The maximum character length is **Note:** **Maximum Concurrent C** leave this field empty.
Call Restriction Type	Specify based on which type of calls to define the maximum number of concurrent calls for this trunk.	Required	Permitted value: `outbound` or `all` **Note:** **Call Restriction Type** wi you leave this field empty.

Parameter	Description	Importance	
Default Outbound Caller ID	The caller ID that is displayed on the callee's device.	Optional	Numbers, letters, and characters The maximum character length is **Note:** The outbound caller ID sh
Default Outbound Caller ID Name	The caller ID name that is displayed on the callee's device.	Optional	The maximum character length is
Get Caller ID From	Decide from which header field will the trunk retrieve Caller ID.	Required	Permitted value: • *follow_system*: [Follow S • *from*: From • *contact*: Contact • *rpid*: Remote-Party-ID • *pai*: P-Asserted-Identity • *ppi*: P-Preferred-Identity **Note:** **Get Caller ID From** will b you leave this field empty.
Get DID From	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. Adjust the setting after analysis of the SIP packets sent from the trunk provider.	Required	Permitted value: • *follow_system*: [Follow S • *to*: To • *invite*: Invite • *diversion*: Diversion • *rpid*: Remote-Party-ID • *pai*: P-Asserted-Identity • *ppi*: P-Preferred-Identity • *pcpid*: P-Called-Party-ID **Note:** **Get DID From** will be fille leave this field empty.
From User Part	A From header contains caller ID and caller ID name. **From User Part** indicates caller ID.	Required	Permitted value: • *default*: [Default] • *ext_cid*: Extension Caller • *trunk_user*: Trunk Userna **Note:**

Parameter	Description	Importance	
			Only available whe • `trunk_def_outbcid`: Trun • `ext_outbcid`: Extension's • `outrounter_outbcid`: Ou • `originator_cid`: Originat • A customized value. **Note:** Fill in a desired val is 31. Only number are allowed. **Note:** **From User Part** will be fil this field empty.
From Display Name Part	A From header contains caller ID and caller ID name. **From Display Name Part** indicates caller ID name.	Required	Permitted value: • `default`: [Default] • `ext_cid_name`: Extension • `trunk_def_outbcid_name` • `ext_outbcid_name`: Exten • `originator_cid_name`: O • A customized value. **Note:** Fill in a desired val is 63. **Note:** **From Display Name Par** you leave this field empty.
Diversion	Define the parameters included in the Diversion SIP header.	Optional	Permitted value: • `default`: [Default] • `ext_cid`: Extension Caller • `trunk_user`: Trunk Userna **Note:** Only available whe

Parameter	Description	Importance	
			• *trunk_def_outbcid*: Trun • *ext_outbcid*: Extension's • *outrounter_outbcid*: Ou • *originator_cid*: Originat • A customized value. **Note:** Fill in a desired val is 31. Only number allowed. **Note:** Leave **Diversion** field em parameter with SIP INVIT
Remote-Party-ID	Define the parameters included in the Remote-Party-ID SIP header.	Optional	Permitted value: • *default*: [Default] • *ext_cid*: Extension Caller • *trunk_user*: Trunk Userna **Note:** Only available whe • *trunk_def_outbcid*: Trun • *ext_outbcid*: Extension's • *outrounter_outbcid*: Ou • *originator_cid*: Originat • A customized value. **Note:** Fill in a desired val is 31. Only number allowed. **Note:** Leave **Remote-Party-ID** this parameter with SIP IN
P-Asserted-Identity	Define the parameters included in the P-Asserted-Identity SIP header.	Optional	Permitted value: • *default*: [Default] • *ext_cid*: Extension Caller

Parameter	Description	Importance	
			• `trunk_user`: Trunk Userna **Note:** Only available whe • `trunk_def_outbcid`: Trun • `ext_outbcid`: Extension's • `outrounter_outbcid`: Ou • `originator_cid`: Originat • A customized value. **Note:** Fill in a desired valu is 31. Only number allowed. **Note:** Leave **P-Asserted-Identi** this parameter with SIP IN
P-Preferred-Identity	Define the parameters included in the P-Preferred-Identity SIP header.	Optional	Permitted value: • `default`: [Default] • `ext_cid`: Extension Caller • `trunk_user`: Trunk Userna **Note:** Only available whe • `trunk_def_outbcid`: Trun • `ext_outbcid`: Extension's • `outrounter_outbcid`: Ou • `originator_cid`: Originat • A customized value. **Note:** Fill in a desired valu is 31. Only number allowed. **Note:**

Parameter	Description	Importance	
			Leave **P-Preferred-Iden** this parameter with SIP IN
From Host Part	Define the domain or IP address to be used in the **From** field of a SIP INVITE header.	Required	**Note:** This parameter is only req Permitted value: • *default*: [Default] • A customized value. **Note:** Fill in a desired val is 255.
To Host Part	Define the domain or IP address to be used in the **To** field of a SIP INVITE header.	Required	**Note:** This parameter is only req Permitted value: • *default*: [Default] • A customized value. **Note:** Fill in a desired val is 255.
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
Realm	Realm is a string displayed to users so they know which username and password to use.	Optional	The maximum character length is
Send Privacy ID	Whether to send the Privacy ID in SIP header or not.	Required	Permitted value: • *0*: Disable • *1*: Enable
User Phone	Whether to add the parameter `user=phone` as a request line in	Required	Permitted value: • *0*: Disable • *1*: Enable

Parameter	Description	Importance	
	the header field of the SIP INVITE packet.		
Send X-OpenAPI-Call-ID	Set whether to include a `X-OpenAPI-Call-ID` field in the SIP INVITE packet to carry the Call ID for inbound calls and outbound calls routed through the trunk.	Required	Permitted value: • `0`: Disable • `1`: Enable
100rel	Configure 100rel for this trunk.	Required	Permitted value: • `Required`: 100rel is require • `Supported`: 100rel is supp • `Disabled`: 100rel is disable
Maxptime	Select the value of the Maxptime used when the PBX sends the INVITE packet.	Required	Permitted value: • `default`: PBX will send a the codec that is used for t • A customized value. **Note:** Fill in a desired valu of 10 ranging from **Note:** **Maxptime** will be filled wi field empty.
Support P-Early-Media	Set whether the P-Early-Media field is included in the INVITE packet.	Required	Permitted value: • `0`: Disable • `1`: Enable
Select which IP address to use in 'Contact'(SIP) and 'Connection'(SDP) fields	Decide which IP address will be used in 'Contact'(SIP) and 'Connection'(SDP) fields.	Required	Permitted value: • `default_settings`: Use tl default. • `custom_ip`: Use the custo **Note:** • Only available whe

Parameter	Description	Importance	
			• **Select which IP a** **'Connection'(SDP** `default_settings`
IP Address	The custom IP address that will be used in 'Contact'(SIP) and 'Connection'(SDP) fields.	Required if **Select which IP address to use in 'Contact'(SIP) and 'Connection'(SDP) fields** = `custom_ip`	IP address in IPv4 or IPv6 format

Related reference

Trunk DIDs/DDIs Parameters

Related information

Export and Import SIP Trunks

Import and Export -FAQ

Trunk DIDs/DDIs Parameters

Descriptions for parameters in exported and imported Trunk DIDs/DDIs CSV file.

Note:
The following types of trunks support DIDs/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 `[ ] * # ( ) . - + !` are allowed. The maximum character length is 31.	N/A
DID/DDI Name	The name of DID/DDI that is used to identify	Optional	The maximum character length is 127.	N/A

Parameter	Description	Importance	Restriction	Default Value
	which path of the trunk is passing the call.			

Related information

Export and Import Trunk DIDs/DDIs Numbers
Import and Export -FAQ

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: • `single`: Shared Outbound Caller ID • `range`: Outbound Caller ID Range **Note:** **Create Method** will be filled with default value `single` if you leave this field empty.	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: • Only numbers and character + (before numbers) are allowed. Fill in the start caller ID and the end caller ID with separator -, e.g. 5503301-5503310. • 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	N/A

Parameter	Description	Importance	Restriction	Default Value
			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
Default DOD Label	The default label for the outbound caller ID that is displayed when extension users selecting a DOD to dial out.	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	Permitted value: one or more extension numbers and extension group names existed in PBX. • 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

Import and Export -FAQ

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
Import and Export -FAQ

DID Number to Specific Extension Parameters

Descriptions for parameters in exported and imported 'DID Number to Specific Extension' CSV file.

Parameter	Description	Importance	Restriction	Default Value
DID Number	The specific DID number that is used to match the callee number. Only when the callee number is equal to the DID number will the inbound call go through the inbound route.	Required if **DID Matching Mode** = `pattern_to_ext_list`	The maximum character length is 31. Only numbers, letters, and characters `( ) . - + * #` are allowed.	N/A

Parameter	Description	Importance	Restriction	Default Value
Extension Matched	The destination of the specific DID number. The DID number and the extension is in one-to-one correspondence.	Required if **DID Matching Mode** = `pattern_to_ext_list`	Permitted value: Extension numbers	N/A

Related information

Import and Export -FAQ

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 distinctive ring tones for incoming calls.	Optional	Only numbers and letters are allowed. The maximum character length is 31.	N/A
DID Matching Mode	The DID matching mode.	Optional	Permitted value: • *patterns*: DID Patterns • *pattern_to_ext*: DID Pattern to Extensions • *range_to_ext*: DID Range to Extension Range • pattern_to_ext_list: DID Number to Specific Extension **Note:**	patterns

Parameter	Description	Importance	Restriction	Default Value
			DID Matching Mode will be filled with default value `patterns` if you leave these fields empty.	
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`	• If **DID Matching Mode** = `patterns`, you can enter one or more patterns. Numbers, letters, and characters `[ ] * # ( ) . - + !` are allowed. The maximum character length is 31 (for each DID). Please use `&` as a separator for multiple patterns, e.g. pattern1&pattern2. • If **DID Matching Mode** = `pattern_to_ext`, only numbers, letters `X Z N`, characters `[ ] * # - +`, and placeholder `{{.Ext}}` are allowed. The maximum character length is 31. The **Default Destination** must be `pattern_to_ext`, then fill multiple extension numbers with separator `&` in Number. • If **DID Matching Mode** = `range_to_ext`, 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. The **Default Destination** must be `range_to_ext`, then fill the start number and the	N/A

Parameter	Description	Importance	Restriction	Default Value
			end number with separator `-` in Number, e.g. 1001-1005.	
Caller ID Matching Mode	The Caller ID matching mode.	Required	**For Basic Plan**: Permitted value: • `patterns`: Caller ID Matching Settings **Note:** **Caller ID Matching Mode** will be filled with default value `patterns` if you leave these fields empty. **For Enterprise/Ultimate Plan**: Permitted value: • `patterns`: Caller ID Matching Settings • `phonebook`: Match Contacts' Caller ID in Specific Phonebooks **Note:** **Caller ID Matching Mode** will be filled with default value `patterns` if you leave this fields empty.	patterns
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	**For Basic Plan**: The maximum character length is 31 (for each pattern). Numbers, letters, characters `[ ] * # ( ) . - + !` are allowed. For multiple patterns, enter patterns and use `&` as a separator, e.g. pattern1&pattern2. **For Enterprise/Ultimate Plan**:	N/A

Parameter	Description	Importance	Restriction	Default Value
			• If **Caller ID Matching Mode** = *patterns*, the maximum character length is 31 (for each pattern). Numbers, letters, characters *[ ] * # ( ) . - + !* are allowed. For multiple patterns, enter patterns and use *&* as a separator, e.g. pattern1&pattern2. • If **Caller ID Matching Mode** = *phonebook*, the permitted value is one or more phonebook names existed in PBX. For multiple phonebook names, enter names and use *&* as a separator, e.g. name1&name2. If the phonebook you enter does not exist in PBX, it will be skipped.	
Trunks	The trunks that incoming calls will be routed by this inbound route. The PBX will route inbound calls through this route when external users call the selected trunk number.	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 trunks you enter are not existing in PBX, Trunks will be skipped.	N/A
Default Destination	The default destination to receive inbound calls.	Required	Permitted value: • *end_call*: Hang up • *extension*: Extension • *range_to_ext*: Match extension Range (DID Matching Mode = range_to_ext)	end_call

Parameter	Description	Importance	Restriction	Default Value
			• *pattern_to_ext*: Match selected Extension (DID Matching Mode = pattern_to_ext) • pattern_to_ext_list: DID number match specific extension (DID Matching Mode = pattern_to_ext_list) • *ext_vm*: Extension Voicemail • *group_vm*: Group Extension • *ivr*: IVR • *ring_group*: Ring Group • *queue*: Queue • *conference*: Conference • *fax_to_email*: Fax to Email **Note:** **Default Destination** will be filled with default value *end_call* if you leave these fields empty.	
Number of Default Destination	The destination number to receive inbound calls.	Required if **Default Destination** ≠ *end_call* or *pattern_to_ext_list*	Permitted value: • If **Default Destination** = *Extension*, *Extension Email*, *Group Voicemail*, *IVR*, *Ring Group*, *Queue*, *Conference*, or *Fax to Email*, please fill in a number. • If **Default Destination** = *Match extension Range*, please fill in a range of extension, e.g. 1000-1010. The maximum number length is 7 (for each number). • If **Default Destination** = *Match selected Extension*, please fill in numbers or names and use *&* as a separator, e.g. extension_number1&extensi	N/A

Parameter	Description	Importance	Restriction	Default Value
			on_number2&extension_group_name3. **Note:** If the numbers or names you enter are not existing in PBX, Number of Default Destination will be skipped.	
Enable Fax Detection	Whether to enable or disable FAX detection.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Enable Fax Detection** will be filled with default value `0` if you leave this field empty.	0
Fax Destination	The destination to receive fax.	Required if **Enable Fax Detection** = `1`	Permitted value: • `end_call`: Hang Up • `extension`: Extension • `fax_to_email`: Fax to Email **Note:** **Fax Destination** will be filled with default value `extension` if you leave this field empty.	extension
Number of Fax Destination	The destination number to receive fax.	Required if **Fax Destination** ≠ `end_call`	Permitted value: extension numbers existed in PBX. • If **Fax Destination** = `Extension`, fax will be sent to extension number. • If **Fax Destination** = `Fax to Email`, fax will be sent to extension's email address.	N/A

Related reference

DID Number to Specific Extension Parameters

Related information

Export and Import Inbound Routes

Import and Export -FAQ

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	Space and special characters are not allowed. Outbound route's name cannot be duplicated. The maximum character length is 63.	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. The maximum character length is 31.	patterns
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, 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.	X.
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

Parameter	Description	Importance	Restriction	Default Value
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
Rrmemory Hunt	Whether to remember which trunk was used last time, and then use the next available trunk to call out.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Rrmemory Hunt** will be filled with default value `0` if you leave this field empty.	0
Extensions	The extensions that are allowed to make outbound calls through this route.	Optional	Permitted value: one or more extension numbers, extension group names, or organization names existed in PBX. **Format**: • When entering the organization name, you must enter the complete path with parent organization(s) connected by character `/`, and with the prefix `Organization_`, i.e. `Organization_{Parent Organization}/{Organization Name}`. For example,	extension

Parameter	Description	Importance	Restriction	Default Value
			`Organization_Yeastar/Marketing Center/Training Team`. • For multiple extensions, extension groups, or organizations, please enter the numbers or names and use *&* as a separator, e.g. extension_number1&extension_number2&extension_group_name3&Organization_Parent Organization/Organization Name4. **Note:** If the extensions, groups, or organizations you entered are not existing in PBX, it will be skipped.	
Outbound Route Password	Whether to require users to enter the same PIN to make outbound calls through this route.	Required	Permitted value: *disable*, *single_pin*, or *pin_list*. **Note:** **Outbound Route Password** will be filled with default value *disable* if you leave these fields empty.	disable
PIN	The PIN is required to make outbound calls through this route.	Required if **Outbound Route Password** is *single_pin*	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 list are required to make	Required if **Outbound Route**	Permitted value: The name of a PIN list existed in PBX.	N/A

Parameter	Description	Importance	Restriction	Default Value
	outbound calls through this route.	**Password** is *pin_list*	**Note:** If the PIN list name you entered is not existing in PBX, it will be skipped.	

Related information

Export and Import Outbound Routes
Import and Export -FAQ

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: • *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. **Note:**	accept

Parameter	Description	Importance	Restriction	Default Value
			Action will be filled with default value *accept* 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 *ip* if you leave this field empty.	ip
Source IP Address	The source IP address.	Required if **Object Type** = *ip*	Must be IPv4 address format XXX.XXX.XXX.XXX.XXX: 0 - 255	N/A
Subnet Mask	The subnet mask.	Required if **Object Type** = *ip*	Must be IPv4 address format XXX.XXX.XXX.XXX.XXX: 0 - 255	N/A
Domain	The domain name.	Required if **Object Type** = *domain*	The maximum character length is 255.	N/A
MAC Address	The MAC address.	Required if **Object 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 *service* if you leave this field empty.	service
Service	The service to which the rule is applied.	Required if **Service/Port Range** = *service*	Permitted value: • *sip* • *web* • *linkus* • *ssh* • *ami* • *database_grant* • *ldap* • *ftp* • *tftp*	N/A

Parameter	Description	Importance	Restriction	Default Value
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*	**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 *both* if you leave this field empty.	both

Related information

Export and Import Static Defense Rules
Import and Export -FAQ

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	service

Parameter	Description	Importance	Restriction	Default Value
			service if you leave this field empty.	
Service	The service to which the rule is applied.	Required if **Service/Port Range** = *service*	Permitted value: • *https* • *http* • *ssh* • *sip_udp* • *sip_tcp* • *sip_tls* • *outbound_sip* • *rtp* • *linkus* • *ami* • *database_grant* • *ldap* • *ftp* • *tftp*	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. **Note:** **Start Port** and **End Port** will be filled with default port range if you leave these fields empty.	1
End Port	The end port.	Required if **Service/port Range** = *port_range*		65535
Protocol	The protocol to which the rule is applied.	Required	Permitted value: • *both* • *udp* • *tcp* **Note:** **Protocol** will be filled with default value *both* if you leave this field empty.	both
Number of Packets	The number of packets permitted within	Required	Only numbers between 1 and 255 are allowed.	N/A

Parameter	Description	Importance	Restriction	Default Value
	a specific time interval.			
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
Import and Export -FAQ

Outbound Call Frequency Restriction Rule Parameters

Descriptions for parameters in exported and imported 'Outbound Call Frequency Restriction' CSV file.

Table 42.

Parameter	Description	Importance	Restriction	Default Value
Name	The name of Outbound Call Frequency Restriction rule.	Required	The maximum character length is 127. **Note:** The name of an Outbound Call Frequency Restriction cannot be duplicated.	N/A
Restrictions	How many outbound calls users can make within a specific time period.	Required	**Format**: *{number_of_calls_limit}*/*{time_limit}*/*{time_unit}* **Example**: `200/10/second` **Note:** Use *&* to separate multiple restrictions, e.g. `200/10/second&3000/1/minute`.	N/A

Table 42. (continued)

Parameter	Description	Importance	Restriction	Default Value
			Variables: *{number_of_calls_limit}*: • Only numbers are allowed. • The maximum character length is 5. *{time_limit}*: • Only numbers are allowed. • The maximum character length is 5. *{time_unit}*: Permitted value: *second* or *minute*.	

Related information

Export and Import 'Outbound Call Frequency Restriction' Rules
Import and Export -FAQ

Rate Parameters

Descriptions for parameters in exported and imported Rate CSV file.

Parameter	Importance	Restriction	Default Value
Name	Required	The maximum character length is 127.	N/A
Match Prefix	Optional	The maximum character length is 31. Numbers, letters, and characters *[]*#().-+!* are allowed.	N/A
Number Length	Optional	The maximum character length is 2. Only numbers are allowed.	N/A
Rate	Required	The maximum character length is 7. Only numbers and characters . are allowed.	0
Billable Unit(s)	Required	The maximum character length is 3. Only numbers are allowed.	60
Initial Time(s)	Required	The maximum character length is 3.	0

Parameter	Importance	Restriction	Default Value
		Only numbers are allowed.	
Initial Cost	Required	The maximum character length is 7. Only numbers and characters `.` are allowed.	0

Related information

Export and Import Call Rate Rules
Import and Export -FAQ

Allowed Numbers Parameters

Descriptions for parameters in exported and imported Allowed Numbers CSV files.

Table 43.

Parameter	Importance	Restriction	Default Value
Name	Required	The maximum character length is 127.	N/A
Type	Required	Permitted value: • *inbound*: Allow the number(s) to call into the PBX. • *outbound*: Allow PBX extensions to call the number(s). • *both*: Allow the number(s) to call into the PBX and allow PBX extensions to call the number(s). **Note:** **Type** will be filled with default value *inbound* if you leave this field empty.	inbound
Number	Required	Numbers, letters, and characters `[ ] * # ( ) . - + !` are allowed. For multiple numbers or number patterns, use *&* as a separator, eg. number1&number2.	N/A

Related information

Import and Export -FAQ

Blocked Numbers Parameters

Descriptions for parameters in exported and imported Blocked Numbers CSV files.

Table 44.

Parameter	Importance	Restriction	Default Value
Name	Required	The maximum character length is 127.	N/A
Type	Required	Permitted value: • *inbound*: Block the number(s) from calling into the PBX. • *outbound*: Block the PBX extensions from calling the number(s). • *both*: Block the number(s) from calling into the PBX and block the PBX extensions from calling the number(s). **Note:** **Type** will be filled with default value *inbound* if you leave this field empty.	inbound
Number	Required	Numbers, letters, and characters `[ ] * # ( ) . - + !` are allowed. For multiple numbers or number patterns, use *&* as a separator, eg. number1&number2.	N/A

Related information

Import and Export -FAQ