Yeastar

Administrator Guide

Yeastar P-Series Software Edition

Version: 83.9.0.18
Date: 2023-04-25

☎ Support: +86-592-5503301
✉ Support: support@yeastar.com
🌐 https://www.yeastar.com

Yeastar Information Technology Co.Ltd.

Contents

About This Guide........ 1

Getting Started........ 2

- Log in to PBX Web Portal........ 2
- Initial Setup Using the Installation Wizard........ 7
- Change the Password of Super Administrator........ 11
- Reset the Password of Super Administrator........ 12
- Set up Company Information........ 14
- View System Information........ 15
- Change Web Interface Language........ 15
- Log out of PBX web portal........ 16

Dashboard........ 17

- Dashboard Overview........ 17

Extension........ 23

- Extension Overview........ 23
- Create Extensions........ 23
  - Create a SIP Extension........ 23
  - Bulk Create SIP Extensions........ 25
- Set up Phones........ 28
  - Set up a SIP Phone........ 28
  - Set up a Remote SIP Phone via Public IP Address and Port........ 29
  - Set up a Remote SIP Phone via Yeastar FQDN........ 31
- Extension Presence........ 35
  - Extension Presence Overview........ 35
  - Presence Settings........ 36
  - Manually Switch Extension Presence........ 39
  - Automatically Switch Extension Presence Based on Time........ 40
  - Monitor Extension Status by BLF Key........ 41
  - Forward Incoming Calls to Another Destination........ 43
  - Ring Office Phone and Mobile Phone Simultaneously........ 45
- Extension Voicemail........ 46

Set up Extension Voicemail.. 46

Extension Features..48

Handle Incoming Calls Based on Caller ID...48

Set up Email Notifications for Missed Calls..49

Set up Email Notifications for User Password Change... 50

Allow Multiple Registrations for One Extension Number..50

Set up Third-party Integration for Call Popup..51

Extension Advanced Settings..53

Advanced Settings of SIP Extension..53

Extension Security.. 55

Extension Security Overview..55

Restrict Outbound Calls for an Extension...56

Restrict Extension Registration Based on User Agent.. 57

Restrict Extension Registration Based on IP Address.. 58

Block Outbound Calls Outside Business Hours... 59

Limit Call Duration of an Outbound Call.. 59

Limit Outbound Call Frequency of an Extension.. 59

Manage Extensions..61

Edit Extensions...61

Reset an Extension's User Password..62

Export and Import SIP Extensions.. 62

Delete Extensions... 63

Extension Visibility Permission.. 63

Set up Extension Visibility...63

Manage Extension Visibility Rules..65

Contacts...66

Contacts Overview.. 66

Manage Company Contacts..67

Manage Company Phonebooks.. 69

Export and Import Company Contacts..70

Identify Callers from Contacts.. 71

Allow Users to Query Contacts on IP Phones..73

Contact Visibility Permission.. 76

Set up Contact Visibility..76

Manage Contact Visibility Rules..77

LDAP Server..78

LDAP Server Overview..78

Set up Yeastar P-Series Software Edition as an LDAP Server..80

Set up LDAP Client..83

Auto Provision LDAP for IP Phones..83

Manual Configuration Examples..86

Organization..93

Organization Overview..93

Enable or Disable Organization Management..95

Set up Organizations..96

Add Users to Organizations..98

Manage Users within Organizations..100

Manage Organizations..103

Export and Import Organizations..104

Extension Group..106

Extension Group Overview..106

Create an Extension Group..107

Manage Extension Groups..108

Assign a User Type to a Group Member..109

View or Change a Member's User Type in Multiple Groups..110

View or Change Permissions for Group Members..112

Auto Provisioning..114

Auto Provisioning Overview..114

Provision IP Phones..117

Auto Provision IP Phones in Local Network (PnP Method)..117

Auto Provision IP Phones in Local Network (DHCP Method)..120

Auto Provision IP Phones Remotely (RPS FQDN Method)..126

Auto Provision IP Phones Remotely (RPS Method)..129

Provision IP Phones on Multiple Servers..133

Manually Provision an IP Phone..135

Provision Gateways..137

Auto Provision Yeastar TA FXS Gateways (PnP Method).................................... 137
Auto Provision Yeastar TA FXS Gateways (DHCP Method)................................. 140
Manage Provisioned Devices.. 146
Remotely Access a Provisioned IP Phone / Gateway.. 146
Reboot Provisioned IP Phones/Gateways.. 151
Reassign an Extension to a Provisioned IP Phone/Gateway............................... 152
Release an Extension from a Provisioned IP Phone/Gateway............................. 153
Remove IP Phones/Gateways from Provisioning List.. 154
Auto Provisioning Options.. 155
IP Phone Auto Provisioning Options.. 155
Auto Provision Function Keys for Phones... 156
Synchronize Phone Time with PBX... 159
Modify a Provisioned Phone Settings... 160
Modify a Provisioned Gateway Settings.. 161
Manage Auto Provisioning Templates... 161
Apply a New Template to a Provisioned IP Phone/Gateway............................... 161
View a Default Auto Provisioning Template.. 162
Update a Default Auto Provisioning Template... 164
Create a Custom Auto Provisioning Template... 165
Manage Custom Auto Provisioning Templates.. 167
Manage IP Phone Firmware.. 168
Update Phone Firmware via Auto Provisioning... 168
Manage Device Firmware Files.. 169
Auto Provisioning - Supported Devices.. 170
Auto Provisioning - Variables in Templates... 194
Auto Provisioning Example.. 200
Auto Provision Yealink DECT Phones with Yeastar P-Series Software Edition......200
Auto Provision Yealink Expansion Module with Yeastar P-Series Software Edition... 203
User Role... 207
User Roles and Permissions.. 207
Create a User Role.. 208
Assign a Role to a User... 209

Manage User Roles....210

User Role Permissions....211

Linkus Server....216

Linkus Overview....216

Set up Linkus Server with Remote Access Service....218

Manually Set up Linkus Server....221

Configure Linkus Login Mode....225

Enable Linkus Clients for Users....226

Configure Linkus Welcome Email....227

Send Linkus Welcome Emails....227

Enable or Disable Push Notifications for Linkus Mobile Client....228

Operator Panel....230

Manage Operator Panel....230

Trunk....232

SIP Trunk....232

SIP Trunk Overview....232

Create a SIP Trunk....234

Manage SIP Trunks....240

Export and Import SIP Trunks....241

SIP Trunk Settings....242

Seize a Trunk to Call Out by BLF Key....251

Call Control....253

Emergency Calling....253

Emergency Calling Overview....253

Set up Basic Emergency Calling....255

Set up Enhanced Emergency Calling....256

Set up a Route for PSAP Callbacks....257

Manage Emergency Numbers....258

Export and Import Emergency Numbers....258

Emergency Notification Contacts....259

Business Hours and Holidays....262

Overview of Business Hours and Holidays....262

Global Business Hours....263

- Holidays....265
Time Condition....268
- Time Condition Overview....268
- Allow Users to Override Time Condition by Feature Code....270
- Allow Users to Override Time Condition on Operator Panel....271
- Override Time Condition for Inbound Calls....273
- Monitor Time Condition Status....277
- Automatic Reset of Time Condition....283
- Enable or Disable Automatic Reset of Time Condition....286
Inbound Route....288
- Inbound Route Overview....288
- Set up an Inbound Route....289
- Time Based Inbound Routes....291
- Caller ID/DID Based Inbound Routes....299
- Manage Inbound Routes....311
- Export and Import Inbound Routes....312
- DID Pattern and Caller ID Pattern....313
Outbound Route....314
- Outbound Route Overview....314
- Set up an Outbound Route....315
- Restrict Outbound Calls by PIN Codes....317
- Manage Outbound Routes....318
- Export and Import Outbound Routes....319
- Outbound Dial Pattern....320
- Dial Pattern Examples....323
AutoCLIP Route....324
- AutoCLIP Route Overview....324
- Route Inbound Calls to Original Extensions via AutoCLIP Route....325
- Delete AutoCLIP Records....327
DID Number....328
- DID Number Overview....328
- Configure DID Numbers on a Trunk....329
- Export and Import Trunk DIDs/DDIs Numbers....330

Caller ID......331

Caller ID Overview......331

Reformat Inbound Caller ID based on a Trunk......332

Export and Import Inbound Caller ID Reformatting Rules......334

Customize Outbound Caller IDs......335

Export and Import Trunk Outbound Caller IDs......336

Distinctive Ringtone......337

Distinctive Ringtone Overview......337

Set Distinctive Ringtones for Internal Calls......338

Set Distinctive Ringtones for External Calls......340

Set Distinctive Ringtones for Queue Calls......342

Set Distinctive Ringtones for Ring Group Calls......344

Set Distinctive Ringtones for IVR Calls......345

Distinctive Caller ID Name......347

Distinctive Caller ID Name Overview......347

Enable or Disable Distinctive Caller ID Name......349

Call Center......351

Call Center Overview......351

Call Center Setup......352

Set up Queue Managers......352

Customize Queue Notification......352

Grant Queue Panel Permissions......353

Set up Service Level Agreement (SLA)......354

Call Center Report......355

Call Center Reports Overview......355

Queue Performance reports......356

Agent Performance Report......363

Call Features......369

Voicemail......369

Voicemail Overview......369

Group Voicemail......371

Send and Receive Voicemail Messages......375

Manage Voicemail Messages......378

Voicemail Security..384

Voicemail Greetings..386

Voicemail Notifications..392

Custom Voicemail Experience..396

Global Voicemail Settings..398

Voicemail Menu Options..399

Voicemail Capacity and Limitations..401

IVR..402

Interactive Voice Response (IVR) Overview..402

Set up an IVR..403

Set up IVR Prompts..405

Allow Callers to Dial Extensions via IVR..407

Allow Callers to Dial by Name via IVR..407

Allow Callers to Dial Outbound Calls via IVR..411

Allow Callers to Change IVR Prompt Remotely..411

Forward Incoming Calls to an External Number via IVR..413

IVR Configuration Example..414

Call Recording..417

Call Recording Overview..417

Set up Call Recording..419

Set up Recording Prompts..420

Allow Users to Switch Call Recording Status..421

Monitor Call Recording Status on an IP phone..422

Manage Call Recording Files..423

Auto Clean up Recording Files..424

Grant Manage Permission of Recording Files..425

Restrict Users from Viewing Recording Files..426

Ring Group..426

Ring Group Overview..426

Create a Ring Group..427

Manage Ring Groups..429

Call Queue..429

Call Queue Overview..429

Create a Queue.......... 431

Set Pause Reasons for Queue Agents.......... 433

Manage Agent Status by Dialing a Feature Code.......... 436

Monitor and Switch Agent Status on an IP Phone.......... 437

Monitor Specific Pause Status of an Agent by Function Key.......... 439

Manage Call Queues.......... 441

Queue Preferences.......... 442

Feature Code.......... 446

Configure Feature Codes.......... 446

Feature Code Reference.......... 446

Conference.......... 451

Conference Overview.......... 451

Create a Conference Room.......... 451

Join a Conference Call.......... 452

Invite Users to a Conference Call.......... 453

Manage Conference Rooms.......... 453

Conference Voice Menu.......... 454

Speed Dial.......... 455

Speed Dial Overview.......... 455

Set up Speed Dial Prefix.......... 455

Add a Speed Dial Number.......... 456

Manage Speed Dial Numbers.......... 456

Export and Import Speed Dial Numbers.......... 457

Call Transfer.......... 458

Call Transfer Overview.......... 458

Set up Call Transfer.......... 458

Perform an Attended Transfer.......... 459

Perform a Blind Transfer.......... 459

Call Flip.......... 460

Call Flip Overview.......... 460

Enable or Disable 'Call Flip' Feature Code.......... 462

Flip an Active Call by Dialing a Feature Code.......... 462

Call Pickup.......... 463

Call Pickup Overview....463
Pick up a Call for a Group Member....464
Pick up a Call for a Specific Extension....465
Call Parking....467
Call Parking Overview....467
Directed Call Parking....468
Call Parking....469
Set up Parking Timeout Destination....469
Set up Parking Number....470
Monitor a Parking Number on an IP Phone....470
Call Monitoring....472
Call Monitoring Overview....472
Allow Users to Monitor a Call by Dialing a Feature Code....474
Disallow Users to be Monitored by Others....476
Fax....476
Fax Overview....476
Receive Faxes by Email....478
Set up Fax over IP (FoIP)....479
Paging/Intercom....480
Overview of Paging and Intercom....480
Paging/Intercom Group....481
Scheduled Paging/Intercom Call....489
PIN List....490
Add a PIN List....490
Blocked/Allowed Numbers....491
Block Calls To or From a Phone Number....491
Export and Import Blocked Numbers....494
Manage Blocked Numbers....495
Allow Calls To or From a Phone Number....495
Export and Import Allowed Numbers....497
Manage Allowed Numbers....498
PBX System....500
System Preferences....500

Voice Prompt....502
- Voice Prompt Overview....502
- System Prompt....504
- Music on Hold....506
- Custom Prompt....510
- Convert Audio Files....512
- Audio Files Requirements....515

SIP Settings....516

Jitter Buffer....522
- Jitter Buffer Overview....522
- Configure Jitter Buffer....523

Network....523
- Basic Network....523
- Web Server....530
- Service Ports....531
- Yeastar FQDN....532
- Public IP and Ports....545
- Static Route....552
- DHCP Server....558

Date and Time....559
- Change System Time Manually....559
- Synchronize System Time with an NTP Server....559

Email Server....560
- Email Server Overview....560
- Set up Yeastar SMTP Server as an Email Server....561
- Set up Gmail as an Email Server....562
- Set up Outlook as an Email Server....565
- Customize Email Templates....567
- Email Sent Logs....567

Storage....568
- Storage Overview....568
- Set up a Hard Disk Drive....570
- Add a Windows Network Drive....574

Add a Mac Network Drive.......580
Manage Storage Locations.......585
Auto Cleanup Settings.......585
File Sharing.......590
Event Notification.......600
Event Notification Overview.......600
Configure Event Notifications.......604
Manage Notification Contacts.......605
Manage Event Logs.......607
Remote Management.......608
Remote Management Overview.......608
Connect Yeastar P-Series Software Edition to Yeastar Central Management Using Authentication Code.......609
Connect Yeastar P-Series Software Edition to Yeastar Central Management Using Yeastar ID.......610
Disconnect Yeastar P-Series Software Edition with Yeastar Central Management.......612
Hot Standby.......612
Hot Standby Overview.......612
Set up Hot Standby Pair.......614
Primary Server Takes over the System from Secondary Server.......620
Security.......623
Security Overview.......623
Static Defense.......626
Add a Static Defense Rule.......626
Manage Static Defense Rules.......627
Export and Import Static Defense Rules.......627
Auto Defense.......628
Add an Auto Defense Rule.......628
Manage Auto defense Rules.......629
Export and Import Auto Defense Rules.......630
Blocked IPs.......631
Manage Blocked IP Addresses.......631
Outbound Call Frequency Restriciton.......631

Add an 'Outbound Call Frequency Restriction' Rule.....631
Manage 'Outbound Call Frequency Restriction' Rules.....632
Export and Import 'Outbound Call Frequency Restriction' Rules.....632
Console/SSH Access.....634
Access the System via SSH.....634
Certificates.....636
Upload TLS certificates to the PBX.....636
Upload HTTPS Certificates to the PBX.....637
Delete Certificates.....638
Allowed Country IPs.....639
Restrict Specific Countries or Regions from Accessing Yeastar P-Series Software Edition.....639
Check Allowed Country/Region IP.....641
Allowed Country Codes.....642
Restrict International Calls to Specific Countries or Regions.....642
Block Outbound International Calls.....644
Maintenance.....646
Upgrade.....646
Check for Available Firmware Updates.....646
Schedule Automatic Firmware Upgrade.....647
Manually Upgrade PBX Firmware.....648
Backup and Restore.....650
Overview of Backup and Restore.....650
Create an On-Demand Backup.....651
Set up an Automatic Backup Schedule.....652
Restore Your System from a Backup.....653
Reboot.....654
Reboot Yeastar P-Series Software Edition on Web Interface.....654
Shut Down Yeastar P-Series Software Edition.....654
Schedule Automatic Reboot.....655
Reset.....655
Reset the System on Web Interface.....655
Operation Logs.....656

Operation Logs Overview....656
Manage Operation Logs....658
Troubleshooting....658
Capture Network Packet....658
Use IP Ping Tool to Diagnose Network Issues....659
Use Traceroute Tool to Diagnose Network Issues....661
Activation....664
Overview of Yeastar P-Series Software Edition Activation....664
Activate Yeastar P-Series Software Edition....665
Update License of Yeastar P-Series Software Edition....666
System Logs....667
System Logs Overview....667
Configure Log Level....668
Manage System Logs....669
CDR and Reports....670
CDR....670
Call Detail Record (CDR) Overview....670
Manage CDR....671
Call Report....673
Call Reports Overview....673
Call Reports....674
Scheduled Reports....679
Call Accounting....684
Call Accounting Overview....684
Call Rate....685
Add a Call Rate Rule....685
Manage Call Rate Rules....687
Export and Import Call Rate Rules....688
Call Accounting Report....689
Extension Call Accounting Report....689
Extension Call Accounting Details Report....691
Integration....693
Speech to Text (STT)....693

Speech to Text (STT) Overview....693
Integrate with Speech to Text (STT) API....694
Disconnect Speech to Text (STT) API Integration....700
Asterisk Manager Interface (AMI) Overview....700
Database Grant....701
Database Grant Overview....701
Get CDR Data from Database of Yeastar P-Series Software Edition....702
cdr Table in the PBX Database....705
Refereneces....708
System Capacity Comparison....708
Import and Export Parameters Overview....710
Extension Parameters....711
Organization Parameters....723
Contacts Parameters....724
Speed Dial Number Parameters....726
Emergency Number Parameters....726
Trunk Parameters....727
Trunk DIDs/DDIs Parameters....736
Trunk Outbound Caller ID Parameters....737
Inbound Caller ID Reformatting Rule Parameters....738
Inbound Route Parameters....739
Outbound Route Parameters....744
Static Defense Rule Parameters....748
Auto Defense Rule Parameters....750
Outbound Call Frequency Restriction Rule Parameters....752
Rate Parameters....753
Allowed Numbers Parameters....754
Blocked Numbers Parameters....755

About This Guide

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

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 Software Edition 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

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 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.

- If the PBX is installed on a virtual machine or an on-premise server, make sure 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 Software Edition 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.

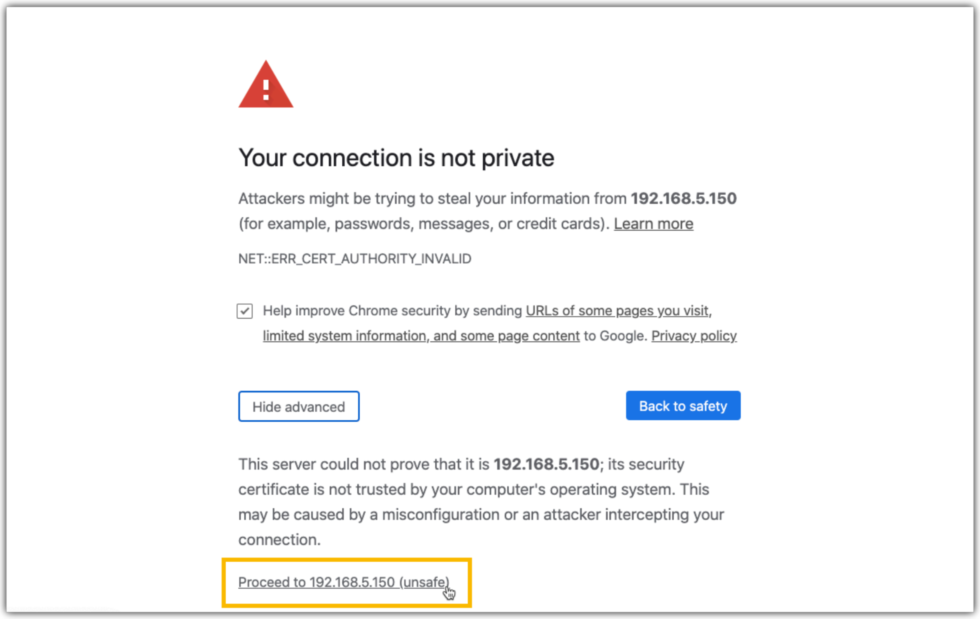
Procedure

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.



Your connection is not private

Attackers might be trying to steal your information from **192.168.5.150** (for example, passwords, messages, or credit cards). Learn more

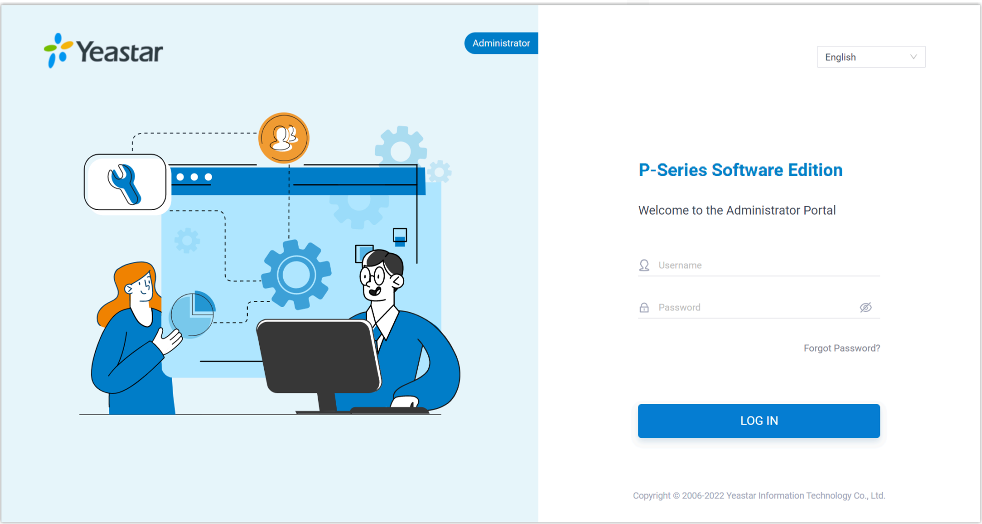
NET::ERR_CERT_AUTHORITY_INVALID

☑ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

This server could not prove that it is **192.168.5.150**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.5.150 (unsafe)

3. Enter the credentials of super administrator account, and click LOG IN.
    - 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.



P-Series Software Edition

Welcome to the Administrator Portal

Copyright © 2006-2022 Yeastar Information Technology Co., Ltd.

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

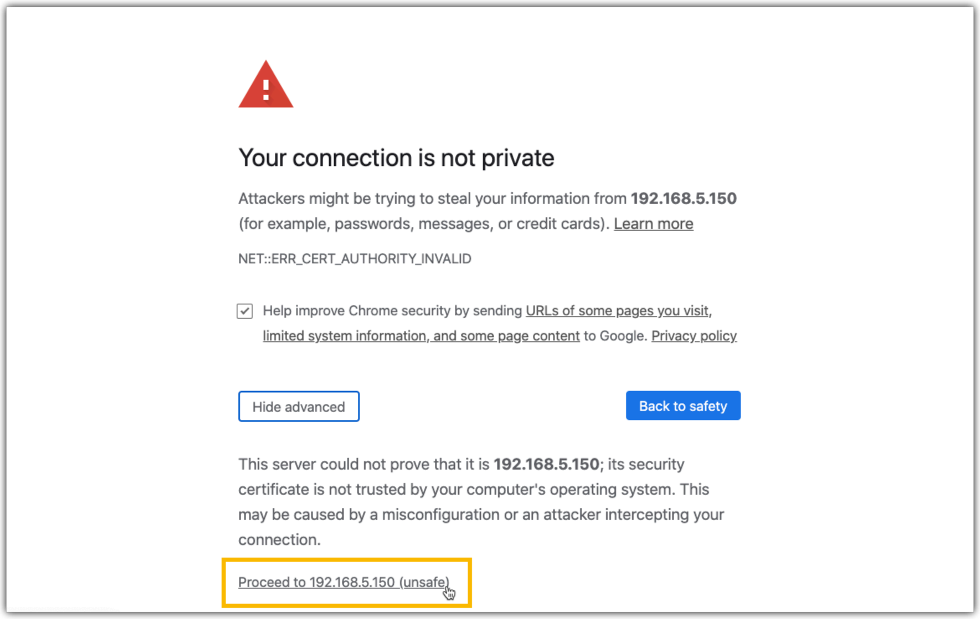
  - Support the resolution of 1366 x 768 or higher.
- If the PBX is installed on virtual machines or on-premise servers, make sure you have set the IP address of your PC.

  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 Software Edition 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 a 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.



Your connection is not private

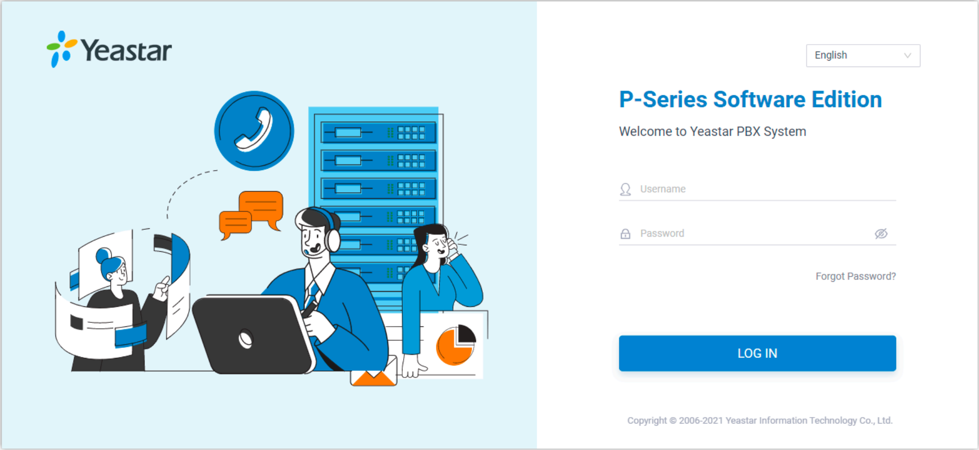
Attackers might be trying to steal your information from **192.168.5.150** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

☑ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

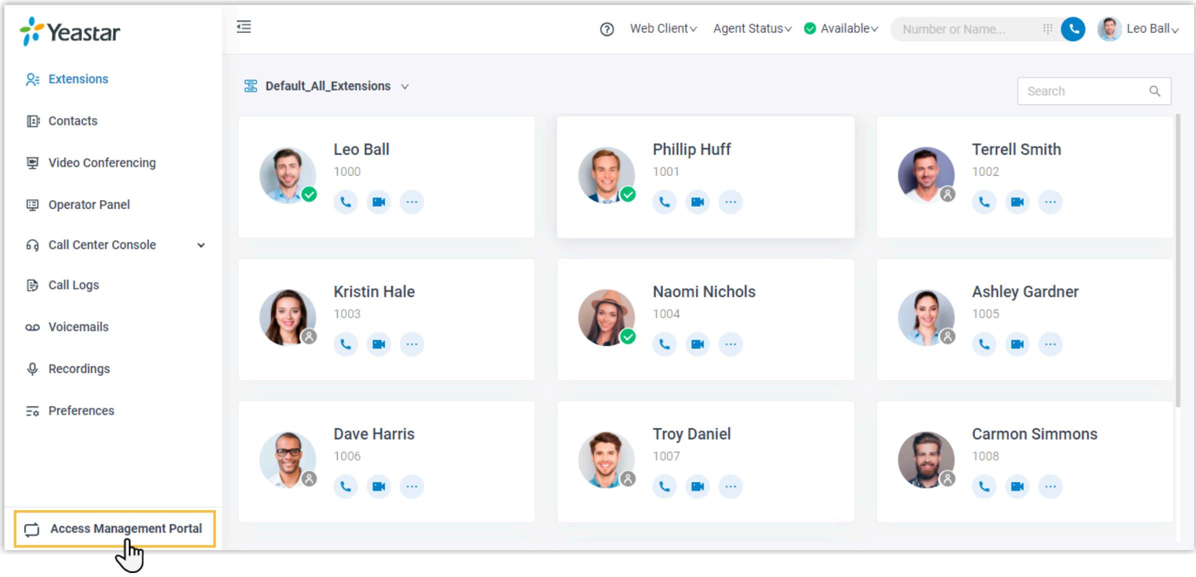
This server could not prove that it is **192.168.5.150**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

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



Yeastar
English
P-Series Software Edition
Welcome to Yeastar PBX System
Username
Password
Forgot Password?
LOG IN
Copyright © 2006-2021 Yeastar Information Technology Co., Ltd.

4. 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

- Step1. Configure the system network
- Step2. Activate Yeastar P-Series Software Edition

- Step3. Set up super administrator account
- Step4. Configure the system time
- Step5. Localize and customize the system
- Step6. Check and confirm the configurations

Step1. Configure the system network

> ! Important:
>
> For PBX system installed on a cloud-based server, retain the default settings, click Next.

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.
        - Dual: Both LAN interface and WAN interface are used for connection.

          > Note:
          >
          > Dual Ethernet mode is typically for the scenario that the Internet Telephony Service Provider (ITSP) offers a dedicated networking for VoIP communication.
    - Default Interface: Optional. Select a default interface if the system is in dual Ethernet mode.
2. In the LAN section, enter the network information for the LAN interface of the PBX.
3. Optional: In the WAN section, enter the network information for the WAN interface of the PBX.
4. Click Next.

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

    For more information of network settings, see Basic Network Overview.

Step2. Activate Yeastar P-Series Software Edition

To activate Yeastar P-Series Software Edition, you need to purchase a license from Yeastar and fill in the provided activation code on the system.

> Note:
>
> If the activation code is not ready, click Skip to skip this procedure. After the system is set up, you can go to Maintenance > Activation to fill in the activation code and activate the system.

Follow the instructions below to activate Yeastar P-Series Software Edition based on the network availability of the PBX.

- If PBX can access the Internet, see Activate the PBX online.
- If PBX can NOT access the Internet, see Activate the PBX offline.

Activate the PBX online

1. Contact your PBX provider to purchase a license and get an activation code.
2. Enter the activation code on the Installation Wizard to activate PBX.
    a. Select Online.
    b. In the Activation Code field, enter the activation code.
    c. Click Activate.

Activate the PBX offline

1. Select Offline.
2. Click Download Request File and send the request file to your PBX provider to get an activation code.
3. In the Activation Code field, enter the activation code.
4. Click Activate.

Step3. 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.

Step4. 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.

Step5. 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 Settingssection, 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.

Step6. 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:
> For PBX system installed on a virtual machine or an on-premise server, 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.

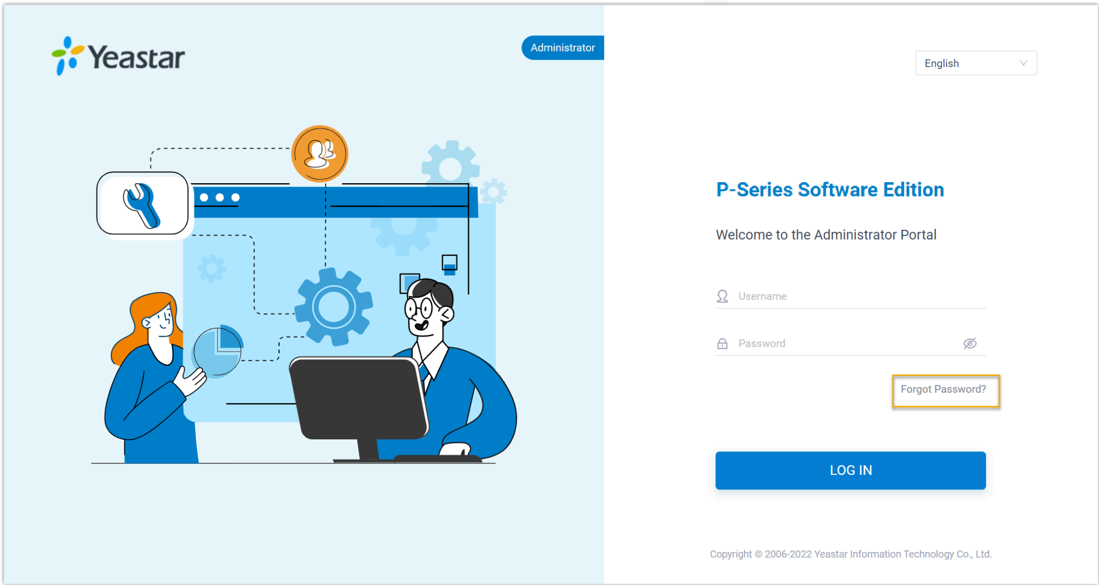
Prerequisites

- 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 re-configure a new username.

Procedure

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



Yeastar

Administrator

English

P-Series Software Edition

Welcome to the Administrator Portal

Username

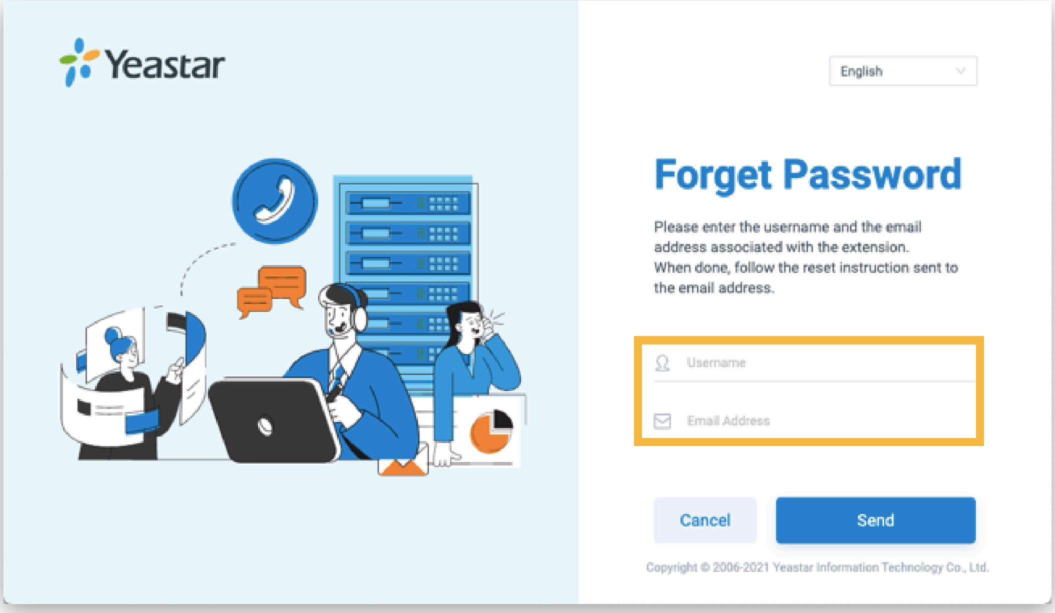
Password

Forgot Password?

LOG IN

Copyright © 2006-2022 Yeastar Information Technology Co., Ltd.

2. On the Forget Password page, enter the following information:
   - Username: The username of super administrator.
   - Email Address: The email address that is associated with the super administrator.



Yeastar

English

Forget Password

Please enter the username and the email address associated with the extension. When done, follow the reset instruction sent to the email address.

Username

Email Address

Cancel

Send

Copyright © 2006-2021 Yeastar Information Technology Co., Ltd.

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

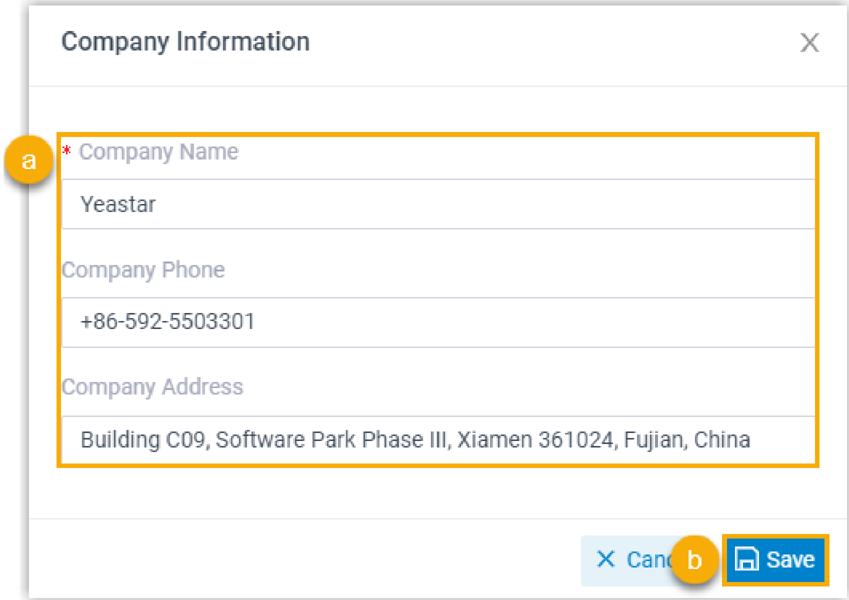
The password of super administrator is changed. You need to log in to PBX administrator portal by the new password next time.

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:



Company Information

* Company Name: Yeastar

Company Phone: +86-592-5503301

Company Address: Building C09, Software Park Phase III, Xiamen 361024, Fujian, China

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.

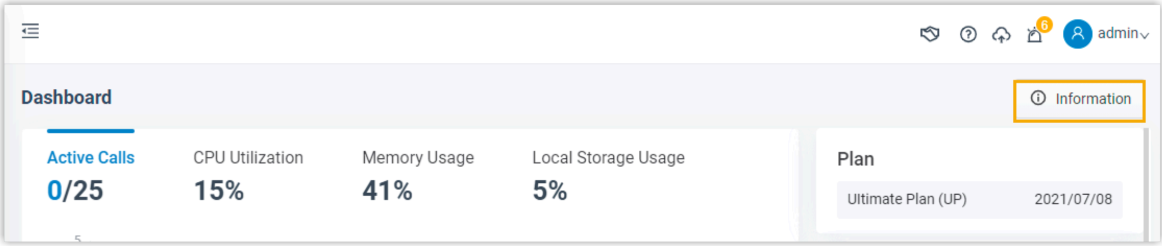
b. Click Save.

View System Information

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

Procedure

1. Log in to PBX web portal, go to Dashboard.
2. At the top-right corner of Dashboard, click Information.



Active Calls 0/25
CPU Utilization 15%
Memory Usage 41%
Local Storage Usage 5%

Plan
Ultimate Plan (UP) 2021/07/08

The following information is displayed:

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

Change Web Interface Language

The default web interface language of Yeastar P-Series Software Edition 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 Software Edition, 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

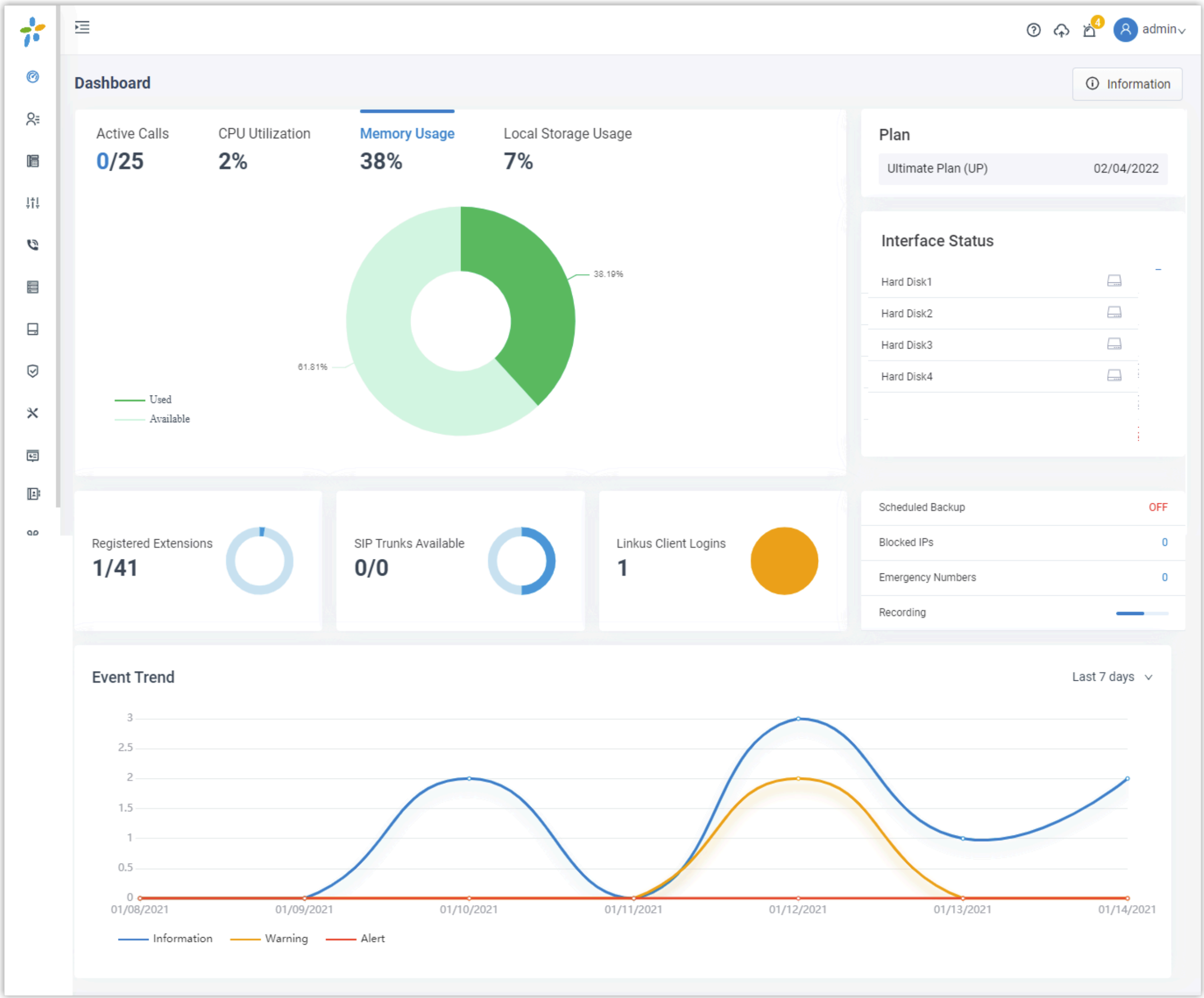
Yeastar P-Series Software Edition Dashboard gives you a historical and real-time view of what is happening on the PBX. This topic describes all the widgets on the Dashboard.

Yeastar P-Series Software Edition 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
- System interface
- System status
- Event trend

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



Active Calls 0/25

CPU Utilization 2%

Memory Usage 38%

Local Storage Usage 7%

Plan

Ultimate Plan (UP) 02/04/2022

Interface Status

Hard Disk1

Hard Disk2

Hard Disk3

Hard Disk4

Registered Extensions 1/41

SIP Trunks Available 0/0

Linkus Client Logins 1

Scheduled Backup OFF

Blocked IPs 0

Emergency Numbers 0

Recording

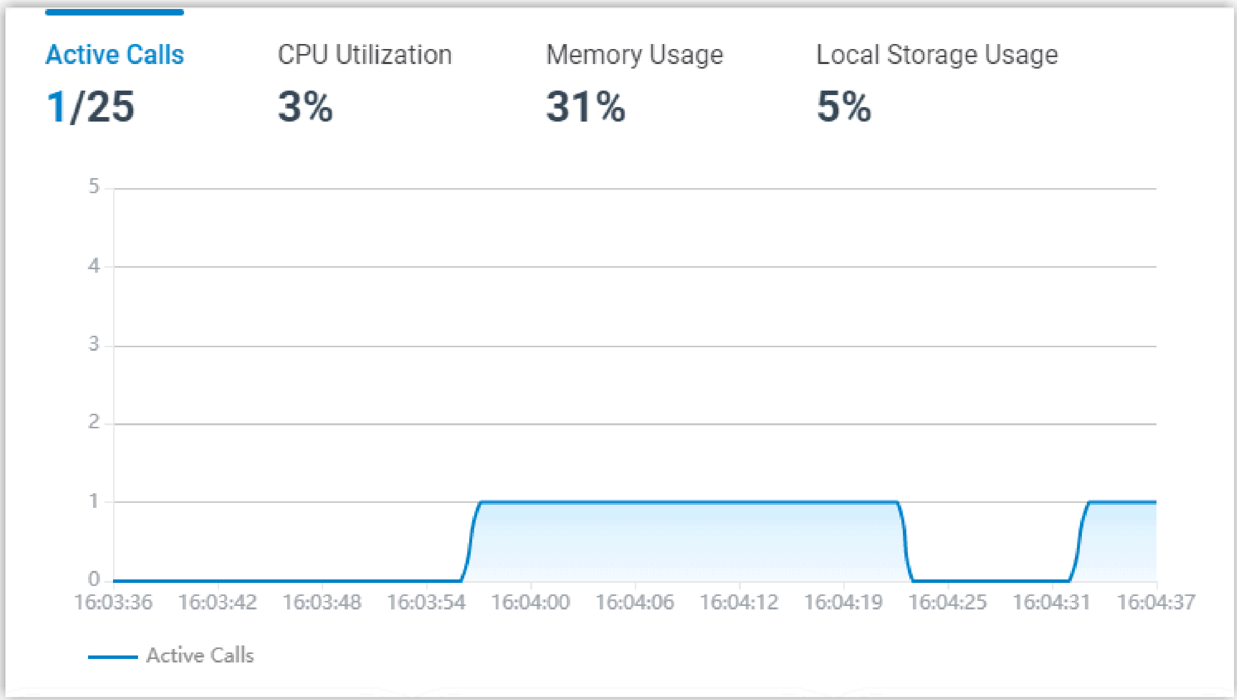
1. System performance
2. System information
3. Plan
4. System interface
5. System status
6. Event trend

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

System performance

System performance displays the following information:

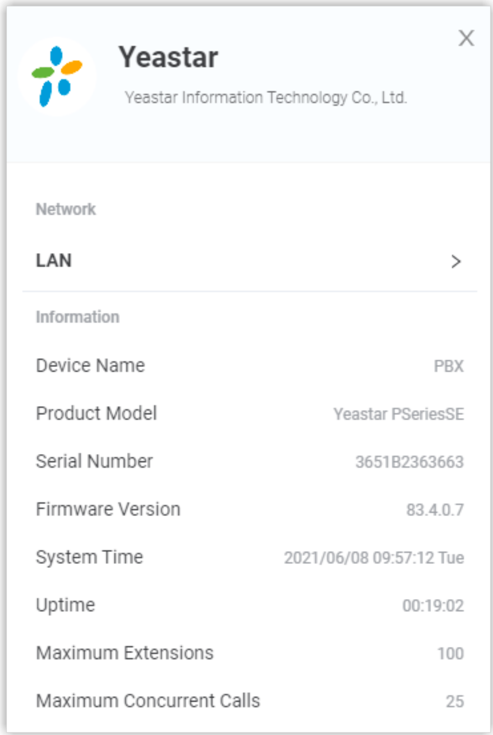
- Active Calls: The real-time and the supported concurrent calls.
- CPU Utilization: The PBX's CPU usage.
- Memory Usage: The PBX's memory usage.
- Local Storage Usage: Usage of the PBX's local storage.



Active Calls 1/25 | CPU Utilization 3% | Memory Usage 31% | Local Storage Usage 5%

System information

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



Yeastar

Yeastar Information Technology Co., Ltd.

Network

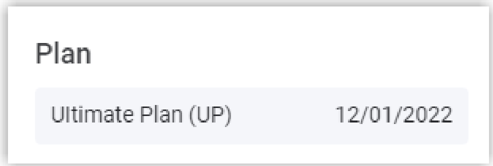
LAN

Information

Device Name	PBX
Product Model	Yeastar PSeriesSE
Serial Number	3651B2363663
Firmware Version	83.4.0.7
System Time	2021/06/08 09:57:12 Tue
Uptime	00:19:02
Maximum Extensions	100
Maximum Concurrent Calls	25

Plan

Plan displays your subscribed plan and expiration date.



Plan

Ultimate Plan (UP)	12/01/2022

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

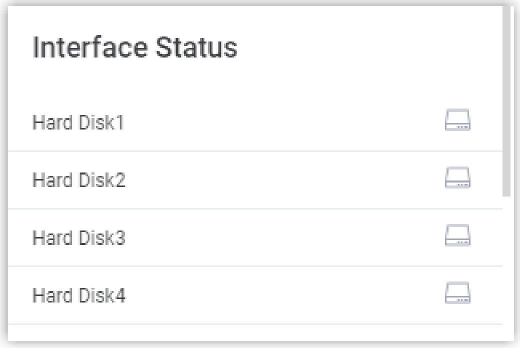
- Connecting: The system is trying to connect to the License Activation Server.
- Abnormal: The system failed to connect to the License Activation Server.

System interface

System interface displays connection status of hard disk of Yeastar P-Series Software Edition.

- 🖴: Connected.
- 🖴: Not inserted.
- 🖴: Connected, but the hard disk is "Read Only" or encounters format error.

- 🖴: Connected, but the hard disk is formatting.



Interface Status

Hard Disk1 🖴

Hard Disk2 🖴

Hard Disk3 🖴

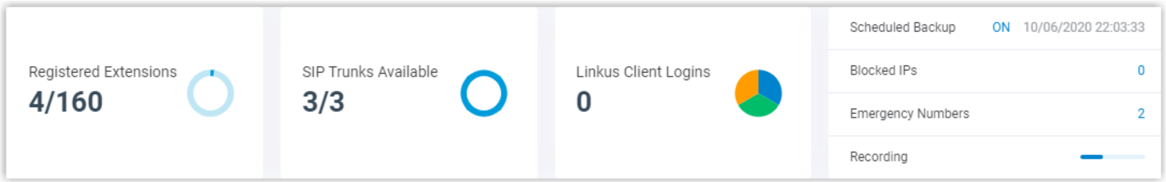
Hard Disk4 🖴

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.



Registered Extensions 4/160

SIP Trunks Available 3/3

Linkus Client Logins 0

Scheduled Backup ON 10/06/2020 22:03:33

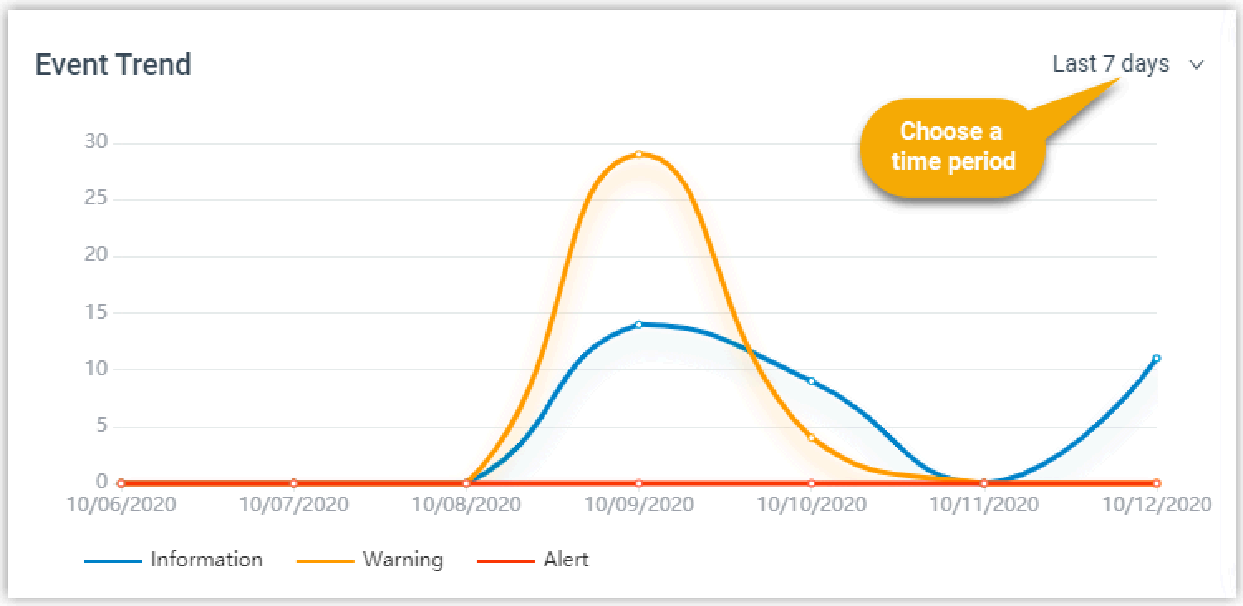
Blocked IPs 0

Emergency Numbers 2

Recording

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.


Event Trend
Last 7 days
Choose a time period
30
25
20
15
10
5
0
10/06/2020
10/07/2020
10/08/2020
10/09/2020
10/10/2020
10/11/2020
10/12/2020
Information
Warning
Alert

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 Software Edition supports SIP extension, which 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

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

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

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

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

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

4. Optional: Click other tabs to configure other settings according to your needs.
5. 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.

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 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.

b. In the Extension Information section, configure extension registration information as follows.

- Registration Name: Choose how to configure registration name.
  - Generate Randomly: Registration name will be randomly generated for each extension.
  - Prefix + Extension Number: If you choose the type, enter a prefix in the Name Prefix field.
  - Extension Number + Suffix: If you choose the type, enter a suffix in the Name Suffix field.
  - Fixed Name: If you choose the type, enter a fixed name in the Fixed Name field.
  - Extension Number: If you choose the type, extension number will be the registration name of each extension.
- Registration Password: Choose a password type.

> Note:

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

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

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

Note:

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

3. Optional: Click other tabs to configure other settings for the extensions.
   - Presence: Configure presence settings.
   - Voicemail: Turn on Enable Voicemail, choose a password type from the drop-down list of Voicemail PIN Authentication.

   Tip:

   Configure voicemail notifications and play options according to your needs.

     - ◦ Generate Randomly: A PIN code will be randomly generated for each extension.
     - ◦ Prefix + Extension Number: If you choose the type, enter a prefix in the PIN Prefix field.
     - ◦ Extension Number + Suffix: If you choose the type, enter a suffix in the PIN Suffix field.
     - ◦ Fixed Password: If you choose the type, enter a PIN code in the Fixed PIN Code field.
     - ◦ Extension Number: If you choose the type, extension number will be set to PIN code for each extension.
     - ◦ Disabled: No PIN code is required when accessing voicemails.
   - Features: Configure email notifications, time-conditional presence auto switch, call handling rules, call recording, etc.
   - Advanced: Configure advanced settings.
   - Security: Configure SIP security settings and call restriction settings.
   - Linkus Clients: Enable Linkus clients for the extensions.

    - Function Keys: Provision function keys.

      When the extensions are bound with phones through auto provisioning, the function keys associated with the extensions will be applied to phones.
4. Click Save and Apply.

Result

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

What to do next

- To set up a SIP phone in your local network, see Set up a SIP Phone.
- To set up a SIP phone remotely, see Set up a Remote SIP Phone via Public IP Address and Port and Set up a Remote SIP Phone via Yeastar FQDN.

Set up Phones

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 Software Edition.

Procedure

1. Gather information of extension registration.
   For most SIP phones, the following credentials are needed in order to register with Yeastar P-Series Software Edition.
    - 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

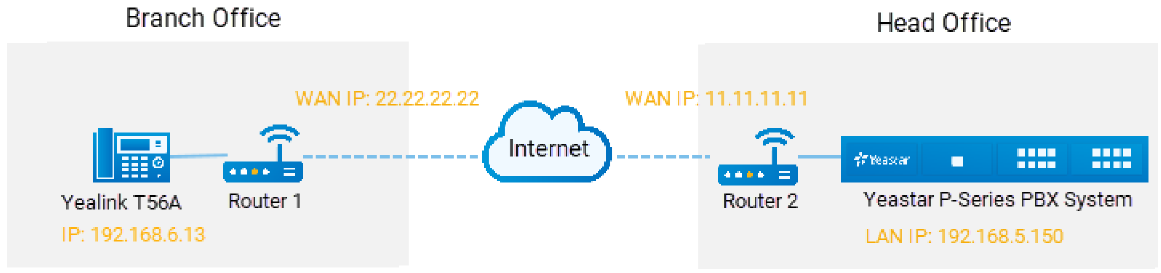
[Set up a Remote SIP Phone via Public IP Address and Port](#)
[Set up a Remote SIP Phone via Yeastar FQDN](#)

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 Software Edition are in different locations and networks. The administrator wants to register Yealink T56A on Yeastar P-Series Software Edition, 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 Software Edition, 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 4.

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

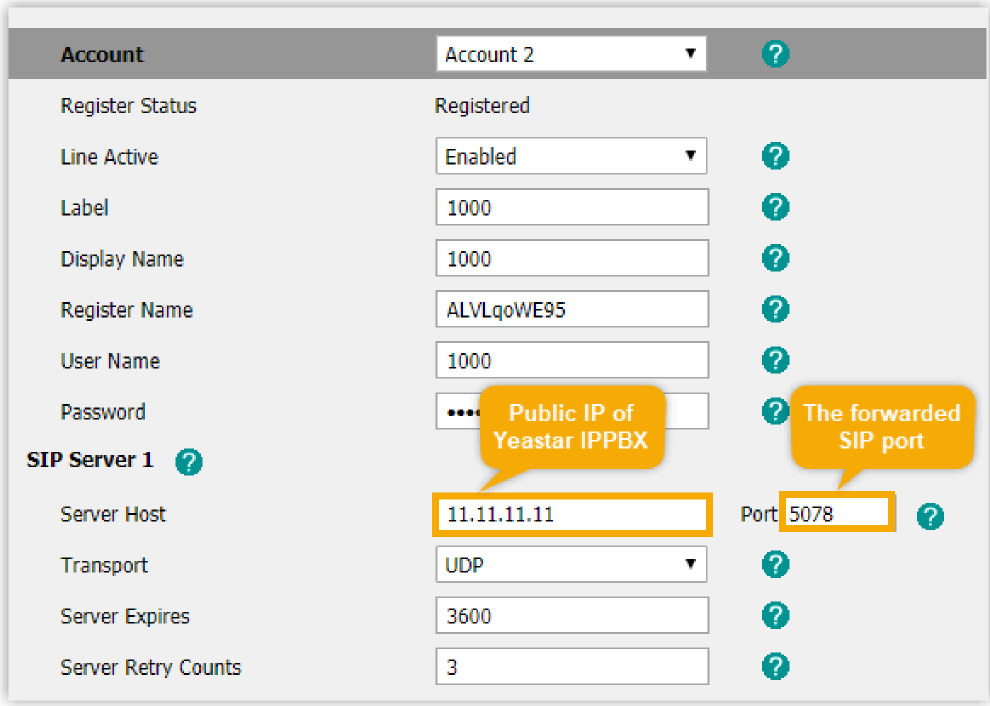
1. On the PBX web portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Security tab, select the checkbox of Allow Remote Registration.

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.



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

Public IP of Yeastar IPPBX

The forwarded SIP port

Result

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

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

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

Step1. Gather information for extension registration

Step2. Register the extension on an IP phone

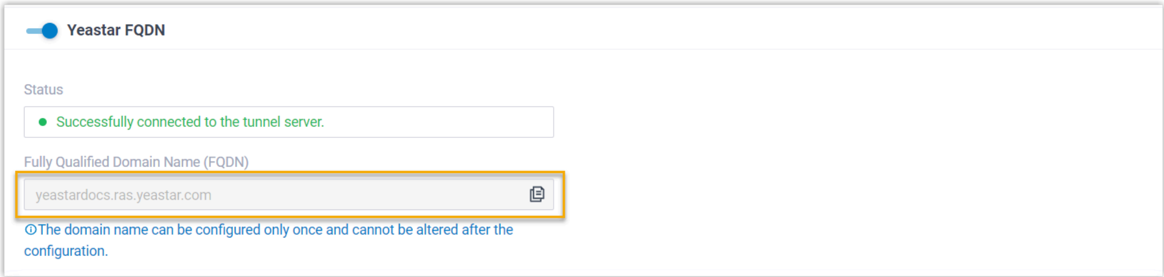
Step3. Confirm the extension's registration status

Step1. 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`.



Yeastar FQDN

Status

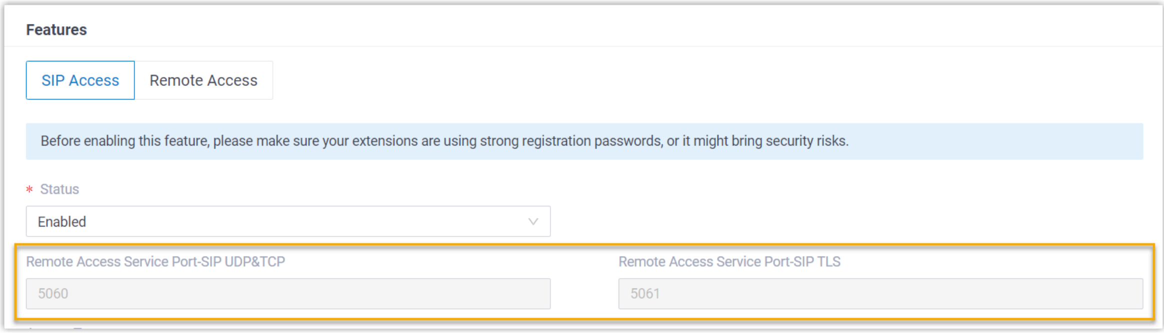
Successfully connected to the tunnel server.

Fully Qualified Domain Name (FQDN)

yeastardocs.ras.yeastar.com

ⓘThe domain name can be configured only once and cannot be altered after the configuration.

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



Features

Before enabling this feature, please make sure your extensions are using strong registration passwords, or it might bring security risks.

* Status

Enabled

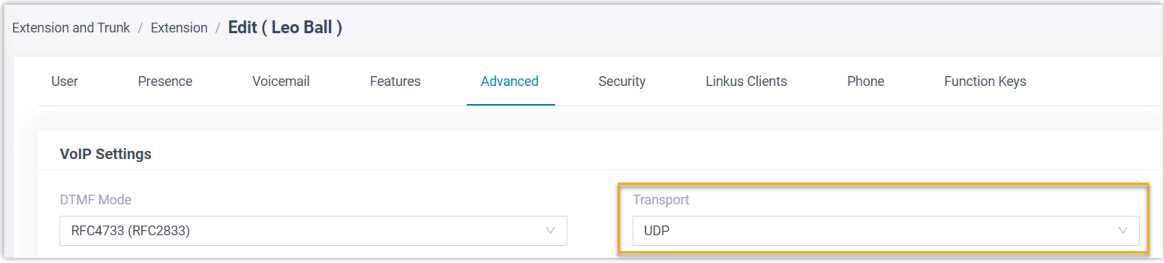
Remote Access Service Port-SIP UDP&TCP

5060

Remote Access Service Port-SIP TLS

5061

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

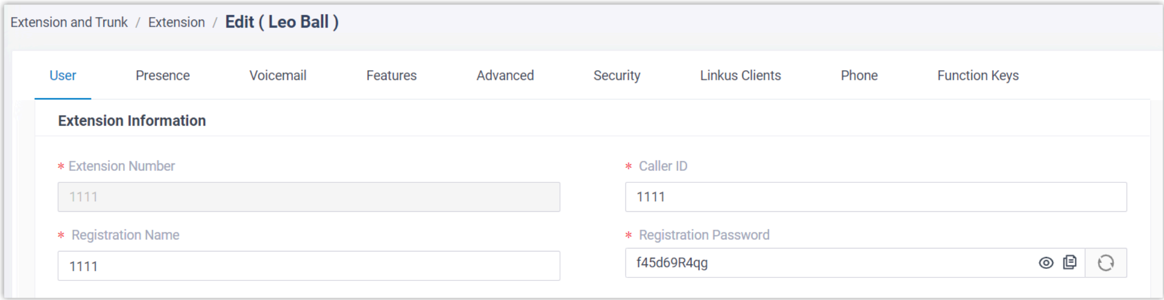


VoIP Settings

DTMF Mode: RFC4733 (RFC2833)

Transport: UDP

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



Extension Information

* Extension Number: 1111

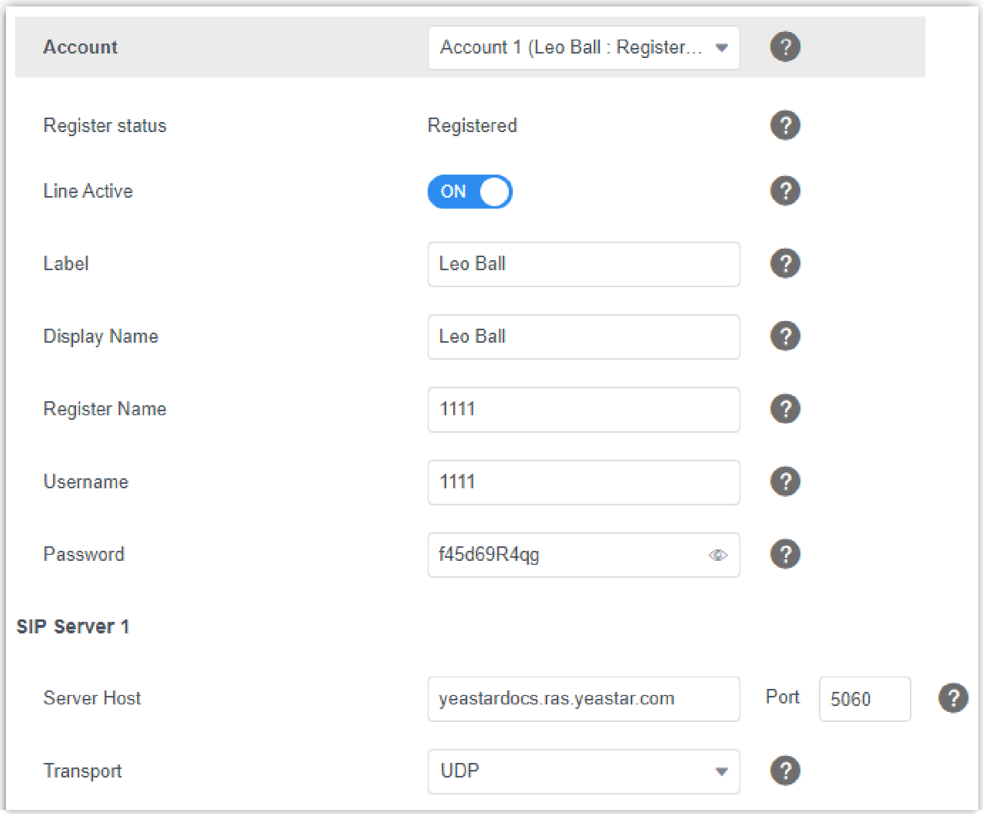
* Caller ID: 1111

* Registration Name: 1111

* Registration Password: f45d69R4qg

Step2. 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.



Account	Account 1 (Leo Ball : Register…		
Register status	Registered		
Line Active	ON		
Label	Leo Ball		
Display Name	Leo Ball		
Register Name	1111		
Username	1111		
Password	f45d69R4qg		
SIP Server 1			
Server Host	yeastardocs.ras.yeastar.com	Port	5060
Transport	UDP		

- 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.

Step3. 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 end-point 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 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 Software Edition can see if other users are available.

Yeastar P-Series Software Edition supports the following status:

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

How presence benefits a user's work

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

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

For more information, see Presence Settings and Change Voicemail Greetings.

Presence switch

There are two ways to switch extension presence:

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

  For more information, see Switch Presence on Linkus Client and Manually Switch 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 Software Edition 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

Table 5.

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

Call Forwarding

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

Table 6.

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 or softphone to which the user's extension has logged in.
- Linkus Mobile Client
- Linkus Desktop Client (Softphone Only)
- Linkus Web Client (Web Client Mode Only)

Table 7.

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

Ring Timeout

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

Table 8.

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.

Table 9.

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

Accept Push Notifications

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

Table 10.

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

Agent Status Auto Switch

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

Table 11.

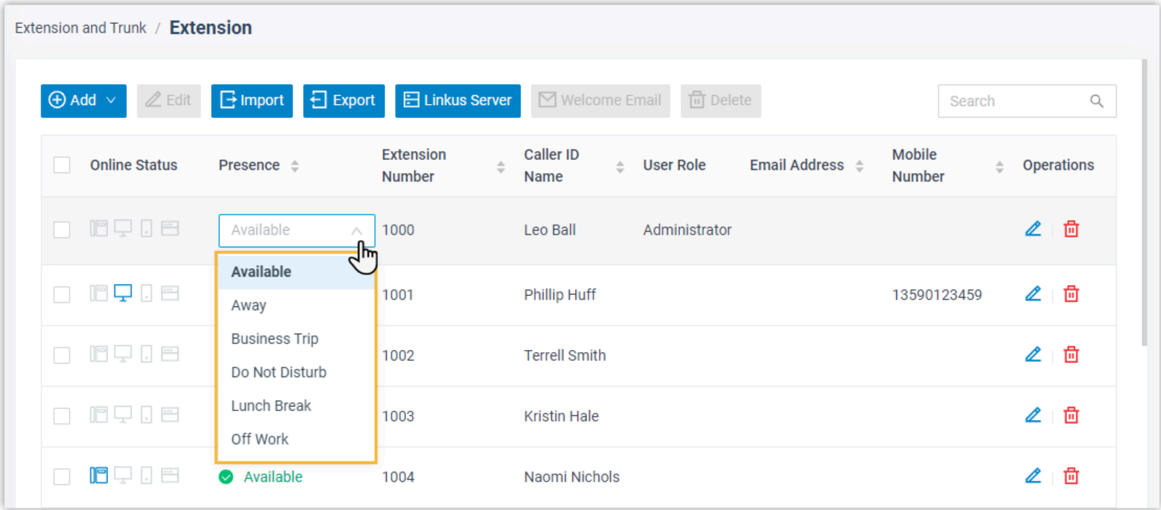
Setting	Description
Login	Log in to a queue. Note: The option is available ONLY in Available status.
Logout	Log out of a queue.
Pause	Pause receiving queue calls. Note: If you have set pause reasons for queue agents, you can select a specific pause reason in the Pause Reason drop-down list.
Do Nothing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



Online Status	Presence	Extension Number	Caller ID Name	User Role	Email Address	Mobile Number	Operations
	Available	1000	Leo Ball	Administrator			
		1001	Phillip Huff			13590123459	
		1002	Terrell Smith				
		1003	Kristin Hale				
	Available	1004	Naomi Nichols				

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 on the PBX system, and you want the presence of extensions to be automatically switched according to the following time schedule:

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

Procedure

1. Log in to PBX 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 on your IP phone via Auto Provisioning to monitor extension call status and DND (Do Not Disturb) presence.

Prerequisites

The phone is connected to Yeastar P-Series Software Edition 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)

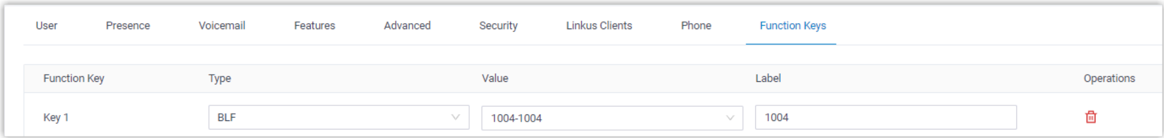
Procedure

- Step1. Set up a function key for extension monitoring
- Step2. Apply the configuration to the IP phone

Step1. 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 the extension 1004.

Function Key	Type	Value	Label	Operations
Key 1	BLF	1004-1004	1004	🗑

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

Step2. 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).
  - Flashing Red: The extension is ringing.
  - LED off: The BLF key configuration failed.

- 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.

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](#)

Forward Incoming Calls to Another Destination

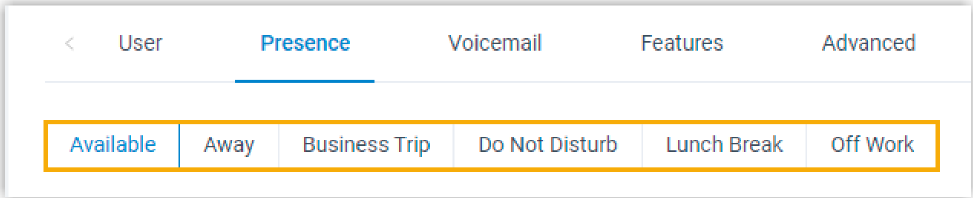
Yeastar P-Series Software Edition supports status-based call forwarding, which allows users to forward incoming calls to different destinations based on their presence status. This topic describes how to preconfigure call forwarding rules for extension users on PBX, and how to enable and configure feature 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)

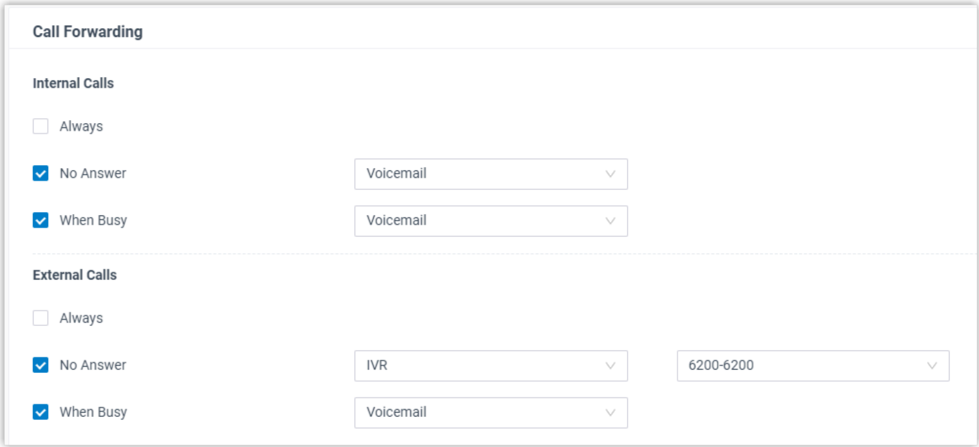
For each presence status of an extension, you can define a different destination to which the incoming calls will be forwarded. Every time the presence status changes, the incoming calls will be forwarded to the corresponding destination.

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.



Call Forwarding

Internal Calls

☐ Always

☑ No Answer Voicemail

☑ When Busy Voicemail

External Calls

☐ Always

☑ No Answer IVR 6200-6200

☑ When Busy Voicemail

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)

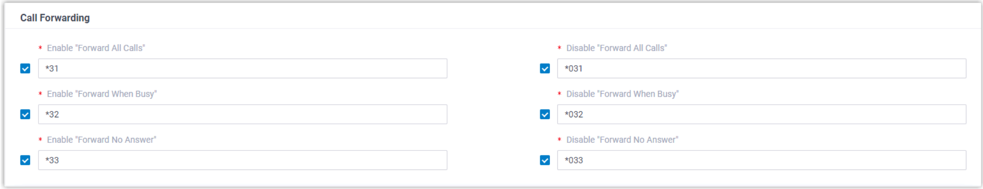
Extension users can change the preset call forwarding destinations on Linkus Web Client. For users with no access to Linkus Web Client, you can enable feature codes for call forwarding, so that these users can dial a feature code on their phones to change the call forwarding destinations.

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.



Call Forwarding

* Enable "Forward All Calls" ☑ *31
* Disable "Forward All Calls" ☑ *031
* Enable "Forward When Busy" ☑ *32
* Disable "Forward When Busy" ☑ *032
* Enable "Forward No Answer" ☑ *33
* Disable "Forward No Answer" ☑ *033

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

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

- Enable or disable voicemail feature
- Voicemail PIN Authentication
- Notification methods and play options of voicemails
- Voicemail greetings

Procedure

1. Log in to PBX web portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Voicemail tab, turn on the option Enable Voicemail.
3. Optional: Configure voicemail PIN settings.
    - Voicemail PIN Authentication: Set whether a PIN code is required when the user accesses voicemail.

        - Enabled
        - Disabled
    - Voicemail Access PIN: Retain the default PIN code or change it according to your needs.

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

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

          > Note:
          >
          > We recommend that you select this option only when the extension user has received a notification email with voicemail message attachment.
        - Do Nothing: Keep the voicemail messages in mailbox as unread.
5. Optional: Set whether to play the following messages when playing a voicemail.
    - Play Date and Time
    - Play Caller ID
    - Play Message Duration
6. Optional: To customize voicemail greetings that will be played to callers when they reach the user's voice mailbox, see Record or Upload Voicemail Greetings.
7. Click Save and Apply.

Related information

Forward Voicemail Messages to Email

Check Voicemail Messages

Extension Features

Handle Incoming Calls Based on Caller ID

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

Procedure

1. Log in to PBX 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.

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

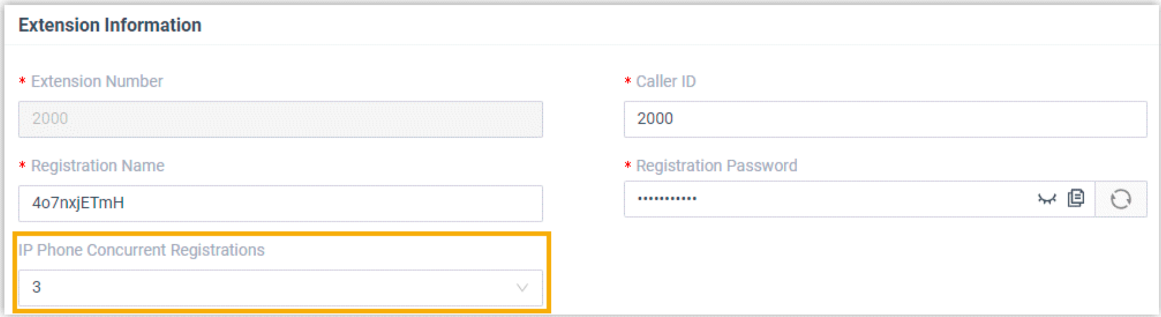
For employees who work flexibly anywhere, they can register their extensions on multiple SIP endpoints, such as an IP phone in their office, a softphone on computer, or a SIP client on mobile phone. In this way, an incoming call can ring all endpoints at the same time, and users can handle calls at anywhere 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 3.
- Concurrent Registration setting only limits the registration number of non-Linkus SIP endpoints. The registration number of Linkus clients is not counted.



Extension Information

* Extension Number: 2000	* Caller ID: 2000
* Registration Name: 4o7nxjETmH	* Registration Password: •••••••••••
IP Phone Concurrent Registrations: 3	

3. Click Save and Apply.

Result

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

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

Note:

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

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

Set up Third-party Integration for Call Popup

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

Restrictions and requirements

Restrictions

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

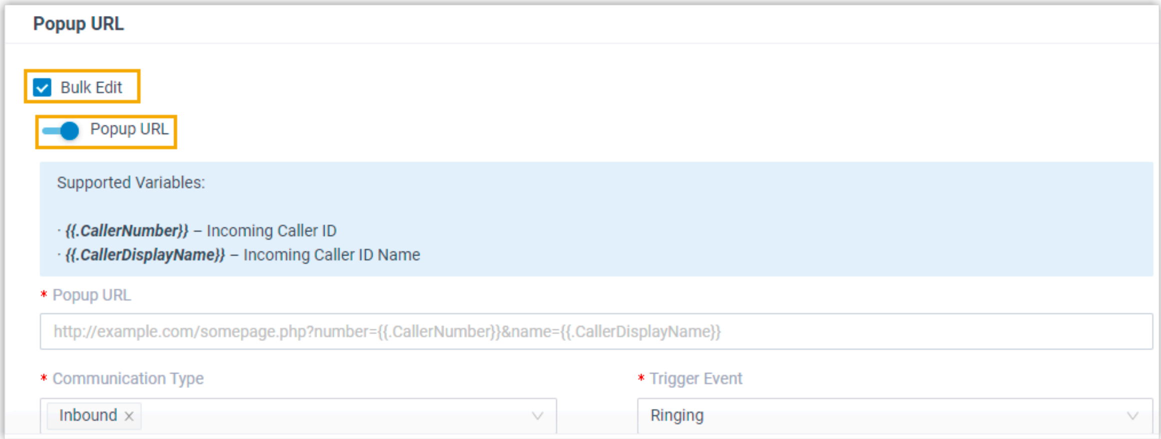
Requirements

- Third-party application:
  - Web-based.
  - Support to provide a URL that can identify callers via Caller ID and Caller ID Name.

Procedure

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

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



Popup URL

☑ Bulk Edit

● Popup URL

Supported Variables:

· {{.CallerNumber}} – Incoming Caller ID
· {{.CallerDisplayName}} – Incoming Caller ID Name

* Popup URL

http://example.com/somepage.php?number={{.CallerNumber}}&name={{.CallerDisplayName}}

* Communication Type: Inbound ×

* Trigger Event: Ringing

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

Table 12.

Settings	Descriptions
Popup URL	Enter the third-party URL, followed by the variables that you want to pass. Supported variables: • .{{.CallerNumber}}: Incoming Caller ID. • .{{.CallerDisplayName}}: Incoming Caller ID Name. Take Solve360 CRM as an example: https://web/solve.360.com/{{.CallerNumber}}&{{.CallerDisplayName}}
Communication Type	Select which types of calls will trigger the call popup. • Inbound: Inbound calls from external users. • Internal: Internal calls from colleagues.
Trigger Event	Set when the call popup will be automatically triggered. • Ringing: An incoming call reaches.

Settings	Descriptions
	• Answered: An incoming call is answered. • Call End: An incoming call is ended.

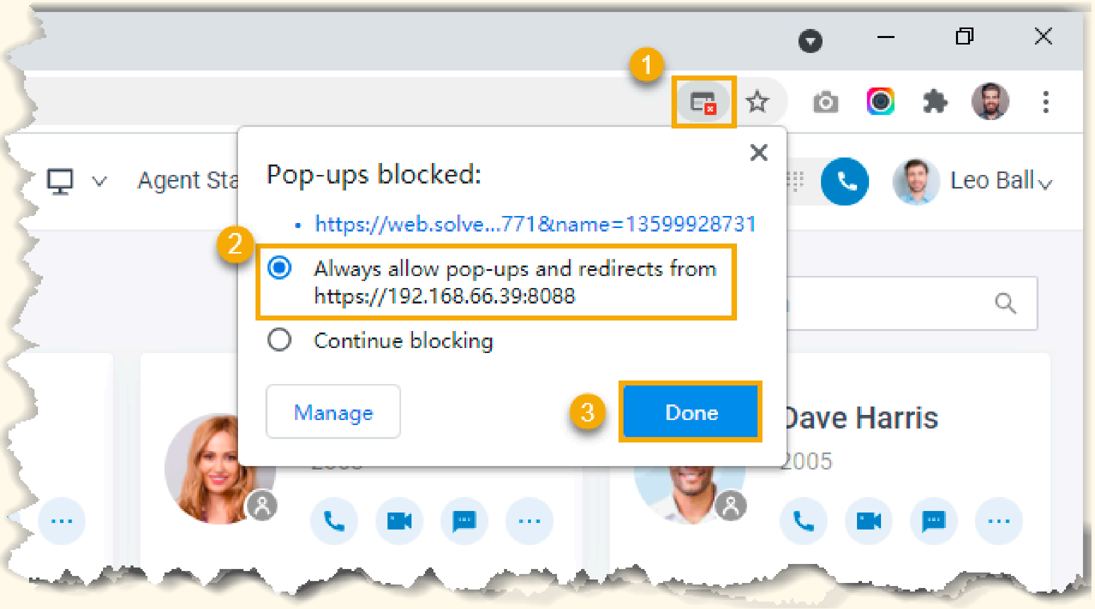
5. Click Save.

Result

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

Important:

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



Pop-ups blocked:

- https://web.solve...771&name=13599928731

● Always allow pop-ups and redirects from https://192.168.66.39:8088

○ Continue blocking

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 13.

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. 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.

Extension Security

Extension Security Overview

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

SIP security options

Yeastar P-Series Software Edition 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 Software Edition provides the following options to prevent abused outbound calls.

Disable Outbound Calls

Restrict users from making outbound calls.

Disable Outbound Calls outside Business Hours

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

Disallow International Calls

Restrict users from making international calls.

> Note:
> The option works only when you have enabled Enable Allowed Country/Region Code Dialaing Protection. For more information, see Block Outbound International Calls.

Max Outbound Call Duration (s)

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

Outbound Call Frequency Restriction

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

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.

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.

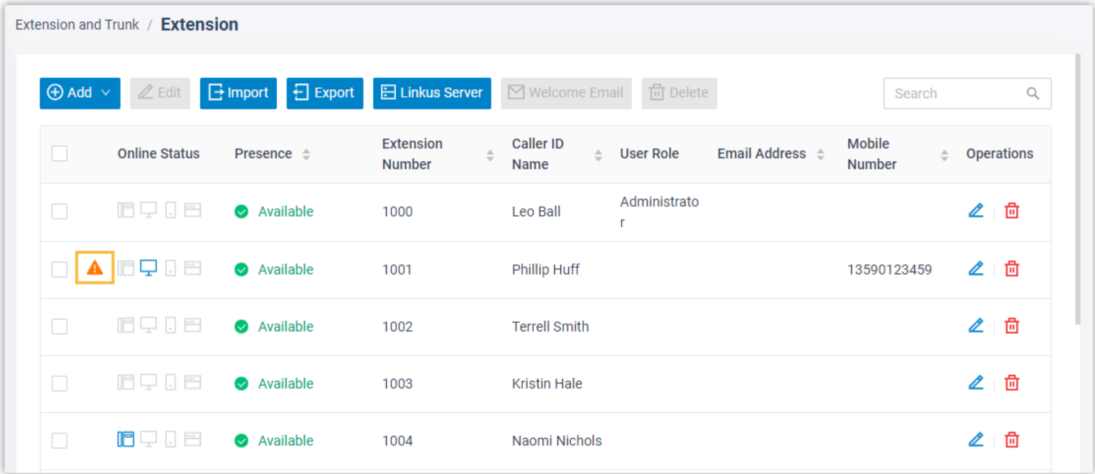
Result

- 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.



□	Online Status	Presence	Extension Number	Caller ID Name	User Role	Email Address	Mobile Number	Operations
□		● Available	1000	Leo Ball	Administrator			✎ 🗑
□	⚠	● Available	1001	Phillip Huff			13590123459	✎ 🗑
□		● Available	1002	Terrell Smith				✎ 🗑
□		● Available	1003	Kristin Hale				✎ 🗑
□		● Available	1004	Naomi Nichols				✎ 🗑

Restrict Extension Registration Based on User Agent

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

Background information

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

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

When a SIP endpoint tries to register an extension to Yeastar P-Series Software Edition, the SIP endpoint working as UAC sends packets containing user agent string to the PBX. By default, Yeastar P-Series Software Edition 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 Software Edition.

Background information

By default, Yeastar P-Series Software Edition 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 Software Edition.

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 IP Restriction.
4. Set which IP address or IP section is allowed to register the extension.
    a. Click Add IP.
    b. In the Permitted IP and Subnet Mask fields, set the allowed IP address or IP section.
5. Click Save and Apply.

Result

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

Block Outbound Calls Outside Business Hours

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

Prerequisites

You have set global business hours.

Procedure

1. Log in to PBX 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.

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

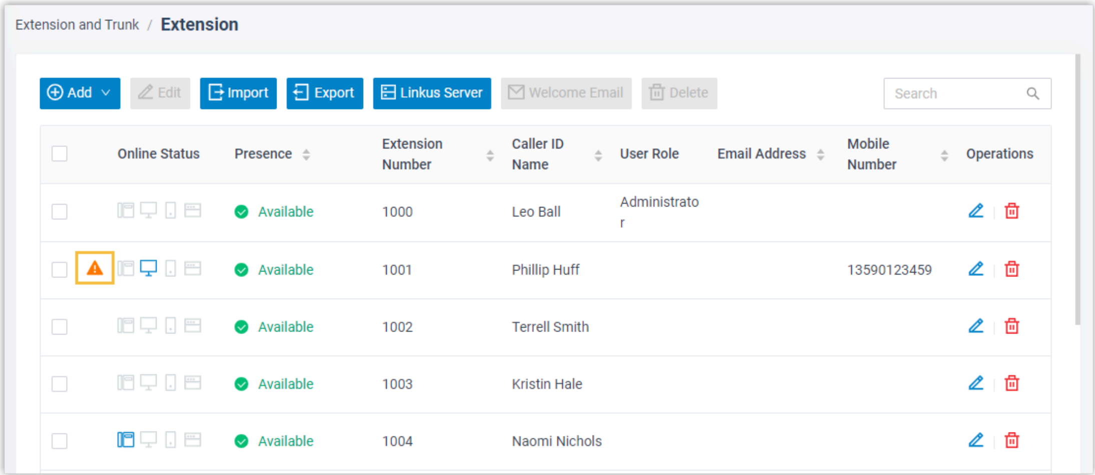
If an extension has exceeded the outbound call frequency restriction, the following things would happen.

- 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.



Extension and Trunk / **Extension**

□	Online Status	Presence	Extension Number	Caller ID Name	User Role	Email Address	Mobile Number	Operations
□		Available	1000	Leo Ball	Administrator			✎ 🗑
□	⚠	Available	1001	Phillip Huff			13590123459	✎ 🗑
□		Available	1002	Terrell Smith				✎ 🗑
□		Available	1003	Kristin Hale				✎ 🗑
□		Available	1004	Naomi Nichols				✎ 🗑

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

Manage Extensions

Edit Extensions

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

Edit an extension

1. Log in to PBX 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 Software Edition 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

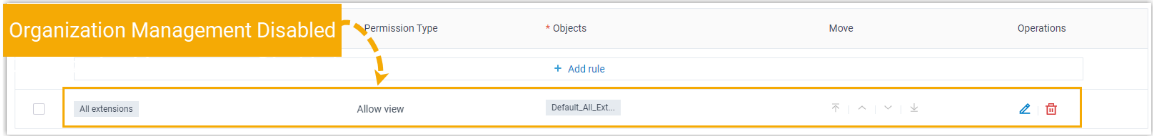
Set up Extension Visibility

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

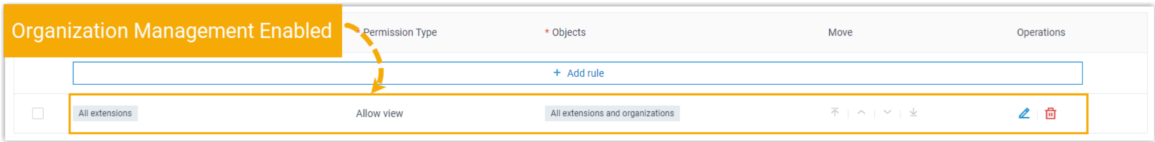
1. Log in to PBX web portal, go to Extension and Trunk > Client Permission > Extension Visibility Permission.

   The default extension visibility rule is displayed.



Organization Management Disabled

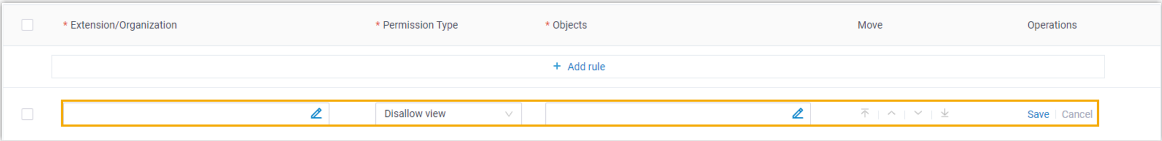
	Permission Type	* Objects	Move	Operations
	+ Add rule			
All extensions	Allow view	Default_All_Ext...	⤒ ︿ ﹀ ⤓	✎ 🗑



Organization Management Enabled

	Permission Type	* Objects	Move	Operations
	+ Add rule			
All extensions	Allow view	All extensions and organizations	⤒ ︿ ﹀ ⤓	✎ 🗑

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



* Extension/Organization	* Permission Type	* Objects	Move	Operations
+ Add rule				
✎	Disallow view	✎	⤒ ︿ ﹀ ⤓	Save | Cancel

   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 or restrict the viewing permission.
   - Permission Type: Select an option from the drop-down list to define the permission.
     - 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 desired extensions, extension groups, or departments, which are allowed or disallowed to be viewed.

   > 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 Mobile Client and Linkus Web Client, 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 Permission.
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 Permission.
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 those contacts on endpoints (IP phone and Linkus clients) where their extensions have registered. This topic describes terminologies, requirements, key features, and limits of Yeastar Contacts feature.

Terminologies

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

Personal Contacts

> Personal Contacts is exclusive to each extension user, which allows users to store a number of personal contacts, such as direct customers.
>
> Note:
>
> Each user's Personal Contacts is only visible to himself or herself.

Company Contacts

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

Phonebooks

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

Key features

Group company contacts into phonebooks

> Group company contacts into organized phonebooks and access them securely with robust permission control.

Sync contacts across Linkus clients

> Sync contacts across Linkus Web Client and Linkus Mobile Client and allow you to make changes on either client.

Sync contacts from integrated CRMs

> Sync contacts from Customer Relationship Management (CRM) systems that are integrated with Yeastar P-Series Software Edition.

Identify incoming calls

When receiving an incoming call from a personal contact or a company contact, callee's phone screen will display the contact name. By knowing who is calling, users can handle calls efficiently.

For more information, see Identify Callers from Contacts.

Maximum Number of Extensions (N)	N $<$ 1000	N ≥ 1000
Company contacts (total)	200,000	500,000
Company phonebooks	200	500
Personal contacts (per extension)	100	500

Related information

Manage Company Contacts
Manage Company Phonebooks
Export and Import Company Contacts
Identify Callers from Contacts
Set up Contact Visibility
Allow Users to Query Contacts on IP Phones

Manage Company Contacts

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

Operation permissions

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

To grant users Company Contacts permissions, see Set up Contact Visibility.

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

- Linkus Web Client - User Guide
- Use Contacts on an IP Phone

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

Table 14.

Permission	Linkus 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	×	×	×	×

Add a company contact

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

   Note:

   - A newly created contact will be added to the default phonebook 'All Company Contacts_Phonebook', if any.
5. Click Save.

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

Edit a company contact

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

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

Delete company contacts

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

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

Manage Company Phonebooks

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

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 Software Edition supports two kinds of company phonebook:

- PBX native company phonebook: A phonebook that stores company contacts that are created on PBX web portal and Linkus Clients.
- CRM-synchronized company phonebook: A phonebook that stores company contacts that are synced from the integrated CRM. The phonebook will be marked with an identifier 'CRM' (CRM).

> Note:
> Phonebooks synchronized from CRM can NOT be edited or deleted.

Group company contacts into phonebooks

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.
   - To define a All Contacts phonebook:
     a. Select All Company Contacts from the drop-down list of Select Contacts.

        > Note:

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

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

5. Click Save.

Edit company phonebooks

1. Log in to PBX 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](#)
[Manage Company Contacts](#)
[Identify Callers from Contacts](#)
[Allow Users to Query Contacts on IP Phones](#)

Export and Import Company Contacts

The company contacts configured on Yeastar P-Series Software Edition 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

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 Software Edition 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

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)
    - 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

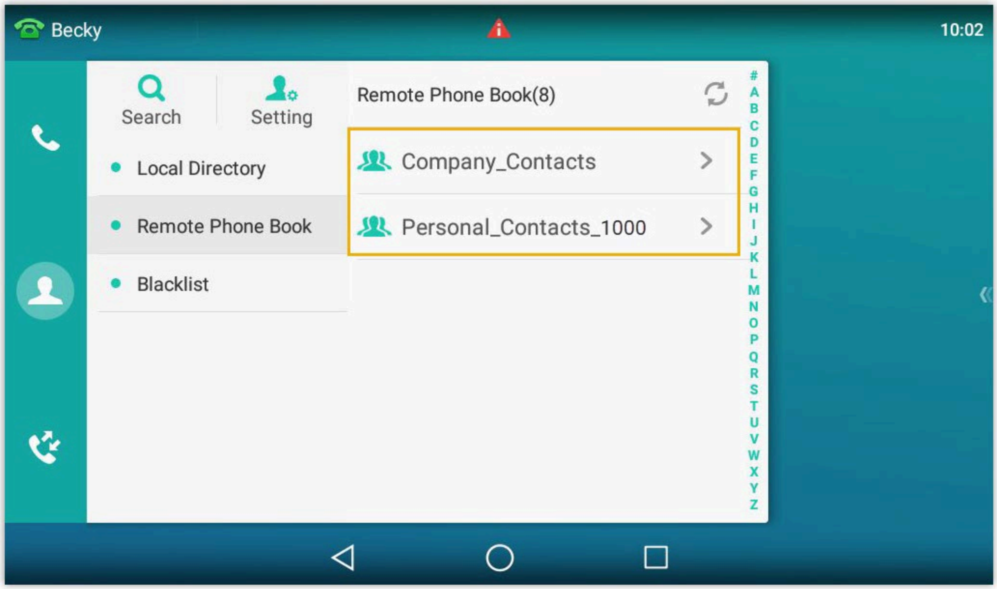
Contacts data are synchronized to IP phones' remote phonebooks. Users can query and place calls to contacts from the remote phonebook.

> 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:
>   >
>   > Company contacts on IP phones can NOT be grouped into phonebooks.
> - Personal_Contacts_{extension_number}: Saves all your personal contacts.

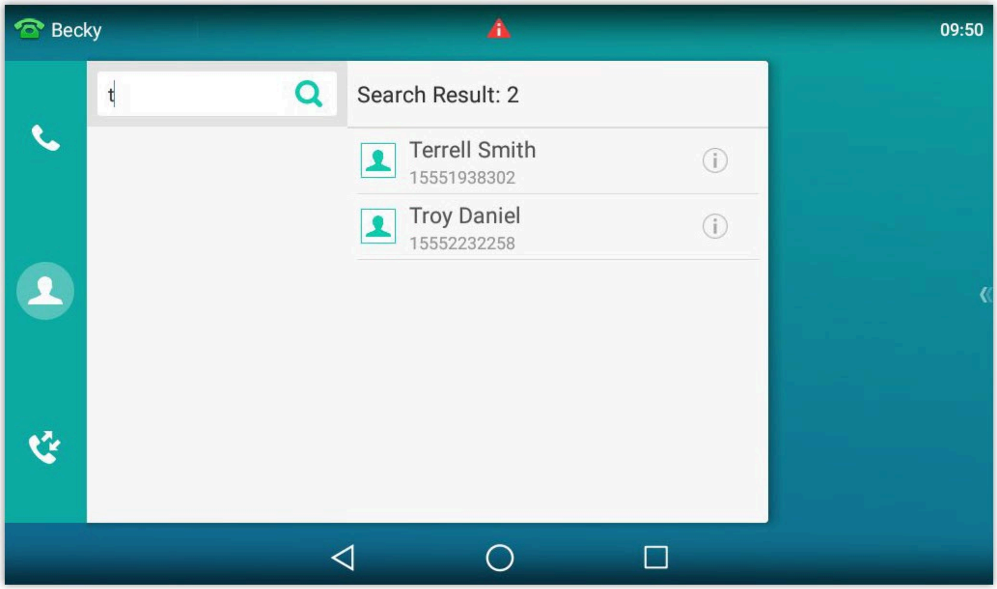
Example: Query contacts on Yealink T56A IP phone

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.

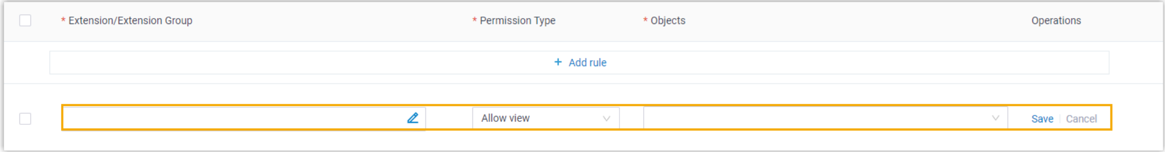
Contact Visibility Permission

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.

Procedure

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

LDAP Server

LDAP Server Overview

Yeastar P-Series Software Edition 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.

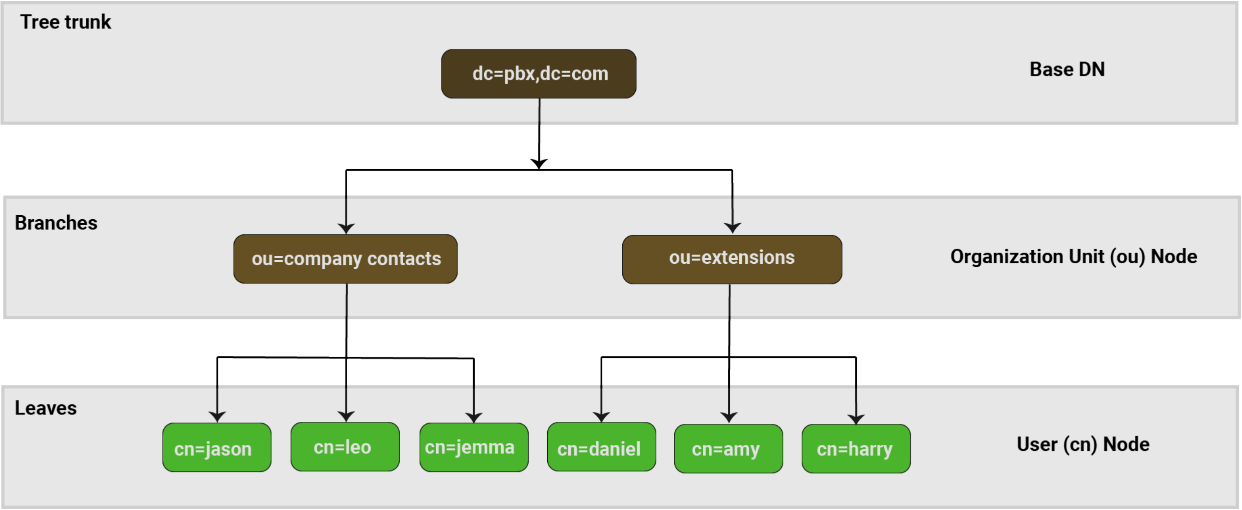
LDAP introduction

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 Software Edition 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`.

Table 15.

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
title	Job Title	Manager
department	Organization	Sales
telephoneNumber	Business number	+86-592-5503301
mobile	Mobile Number	12345678902
homePhone	Home Number	12345678902
facsimileTelephoneNumber	Fax Number	+86-592-5503301

Table 15. (continued)

Attribute	Information details	Example
postalCode	Zip Code	361024
l	City	Xiamen
st	Street	Software Park Phase III
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

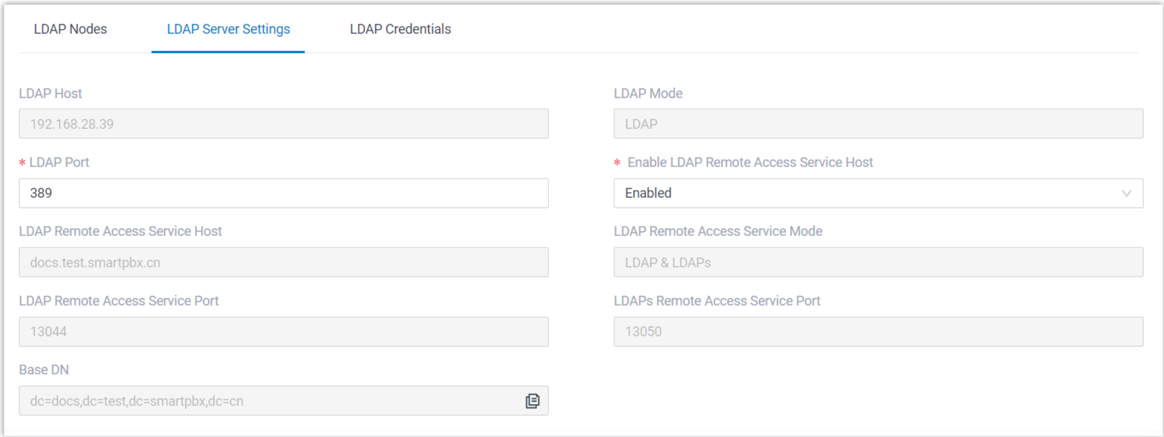
Set up Yeastar P-Series Software Edition as an LDAP Server

Set up Yeastar P-Series Software Edition as an LDAP Server

This topic describes how to set up Yeastar P-Series Software Edition 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.



LDAP Host: 192.168.28.39

LDAP Mode: LDAP

* LDAP Port: 389

* Enable LDAP Remote Access Service Host: Enabled

LDAP Remote Access Service Host: docs.test.smartpbx.cn

LDAP Remote Access Service Mode: LDAP & LDAPs

LDAP Remote Access Service Port: 13044

LDAPs Remote Access Service Port: 13050

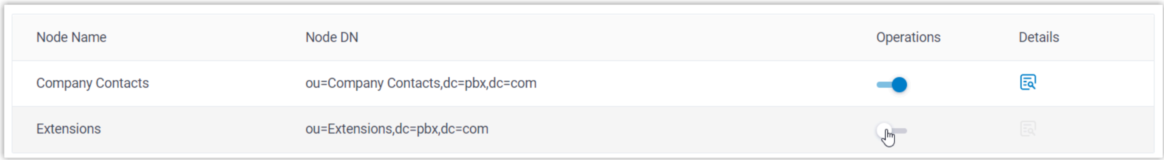
Base DN: dc=docs,dc=test,dc=smartpbx,dc=cn

Table 16.

Setting	Description
LDAP Host	The LDAP Server address of Yeastar P-Series Software Edition. 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 Software Edition LDAP Server. Note: 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.

Setting	Description
	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 Software Edition.

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



Node Name	Node DN	Operations	Details
Company Contacts	ou=Company Contacts,dc=pbx,dc=com	●	
Extensions	ou=Extensions,dc=pbx,dc=com	○	

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

Result

The Yeastar P-Series Software Edition 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

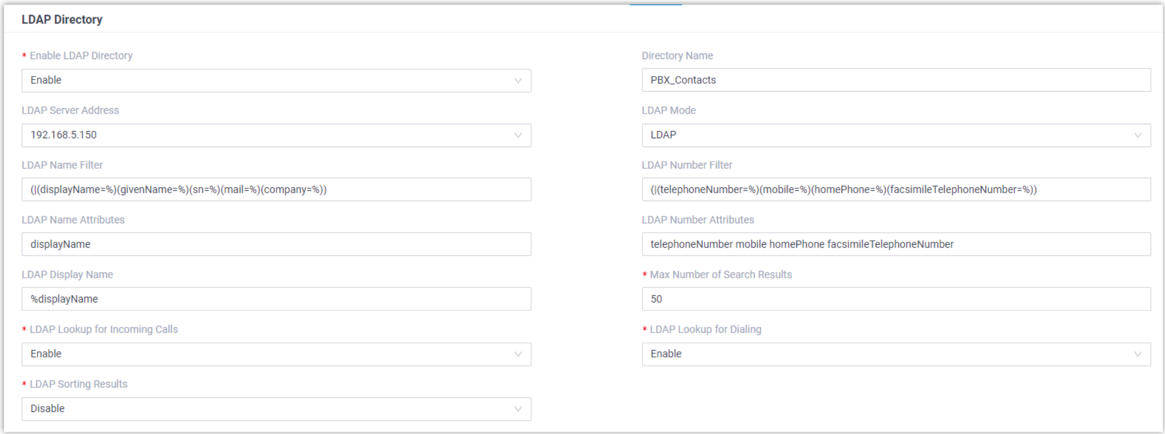
- Make sure the PBX version is 83.6.0.24 or later.
- The phone is connected to Yeastar P-Series Software Edition via Auto Provisioning, and has been assigned with an extension.

  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)
- You have granted the Company Contact viewing permission for extension users. For more information, see Set up Contact Visibility.

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.



LDAP Directory

* Enable LDAP Directory: Enable	Directory Name: PBX_Contacts
LDAP Server Address: 192.168.5.150	LDAP Mode: LDAP
LDAP Name Filter: (|(displayName=%)(givenName=%)(sn=%)(mail=%)(company=%))	LDAP Number Filter: (|(telephoneNumber=%)(mobile=%)(homePhone=%)(facsimileTelephoneNumber=%))
LDAP Name Attributes: displayName	LDAP Number Attributes: telephoneNumber mobile homePhone facsimileTelephoneNumber
LDAP Display Name: %displayName	* Max Number of Search Results: 50
* LDAP Lookup for Incoming Calls: Enable	* LDAP Lookup for Dialing: Enable
* LDAP Sorting Results: Disable	

Table 17.

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 Software Edition.	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. • The % symbol in the filter stands for the entering string used as the prefix of the filter condition.	(|(telephoneNumber=%)(mobile=%) (homePhone=%)(facsimileTelephoneNumber=%))
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

Setting	Description	Example
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

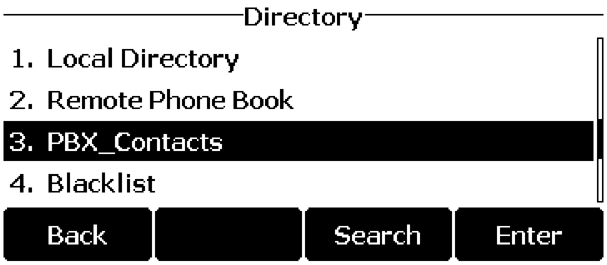
3. Click Save.

   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

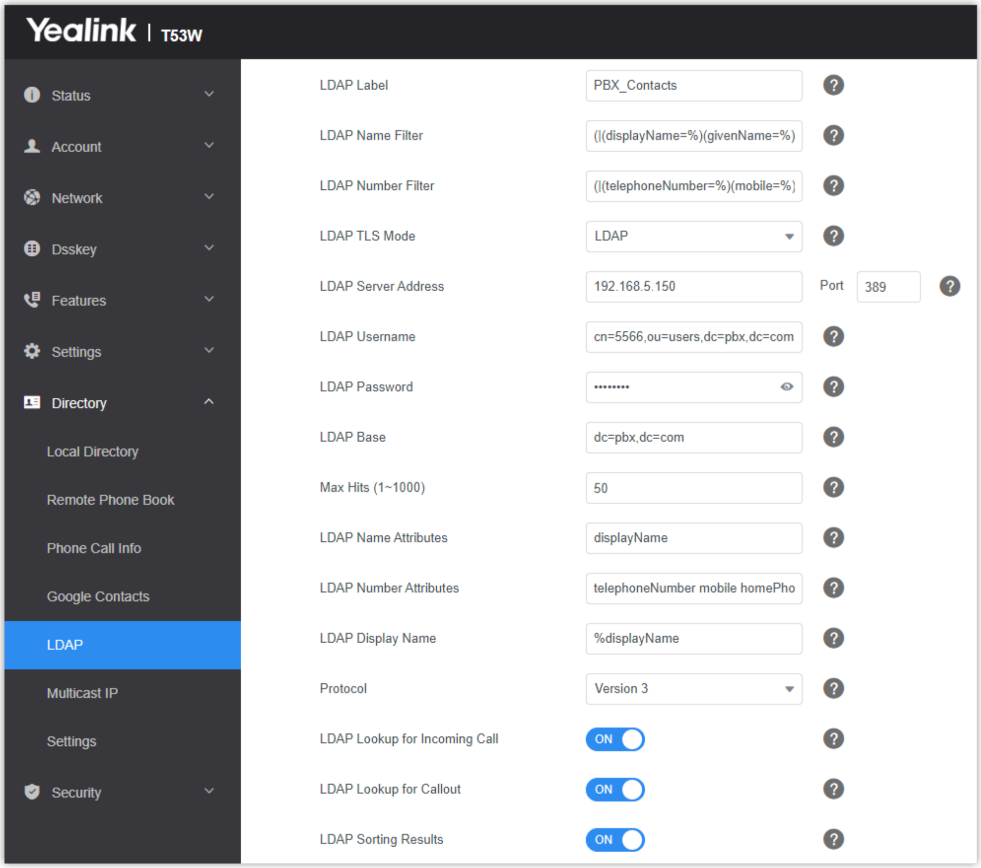
The example configurations are set according to default settings of Yeastar P-Series Software Edition LDAP Server. You can use the following settings as a starting point and adjust the filter and display attributes according to your needs.

Prerequisites

You have granted the Company Contact viewing permission for extension users. For more information, see Set up Contact Visibility.

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.



LDAP Label	PBX_Contacts
LDAP Name Filter	(|(displayName=%)(givenName=%)
LDAP Number Filter	(|(telephoneNumber=%)(mobile=%)
LDAP TLS Mode	LDAP
LDAP Server Address	192.168.5.150 Port 389
LDAP Username	cn=5566,ou=users,dc=pbx,dc=com
LDAP Password	••••••••
LDAP Base	dc=pbx,dc=com
Max Hits (1~1000)	50
LDAP Name Attributes	displayName
LDAP Number Attributes	telephoneNumber mobile homePho
LDAP Display Name	%displayName
Protocol	Version 3
LDAP Lookup for Incoming Call	ON
LDAP Lookup for Callout	ON
LDAP Sorting Results	ON

Table 18.

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 Software Edition.	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 Software Edition 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.

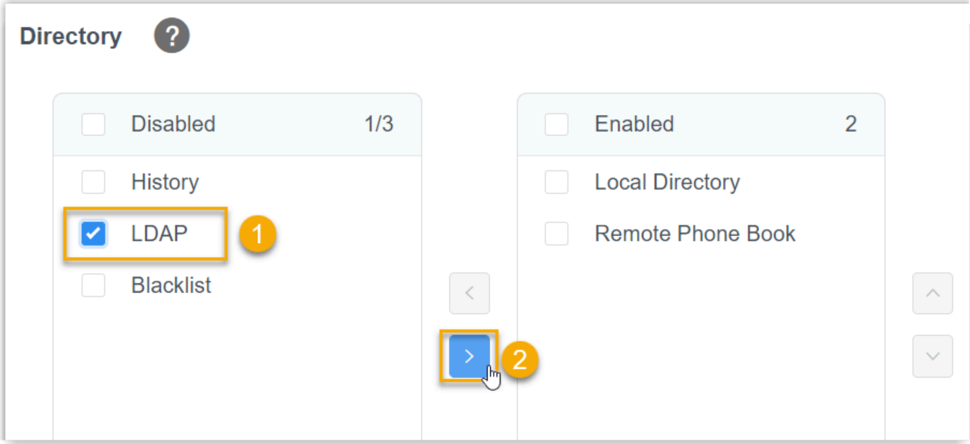
Result

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

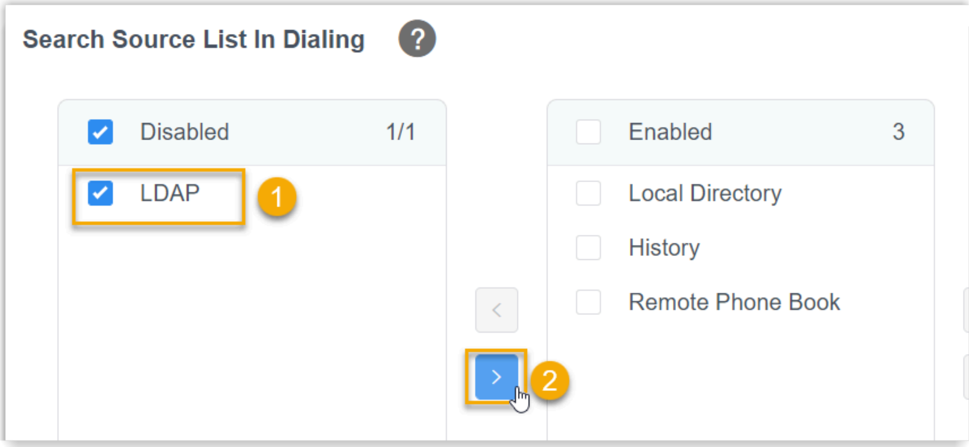
1. Log in to the Yealink phone web interface, go to Directory > Settings.
2. In the Directory section, add LDAP from the Disabled box to the Enabled box.



Directory ?

□ Disabled 1/3	□ Enabled 2
□ History	□ Local Directory
☑ LDAP	□ Remote Phone Book
□ Blacklist	

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



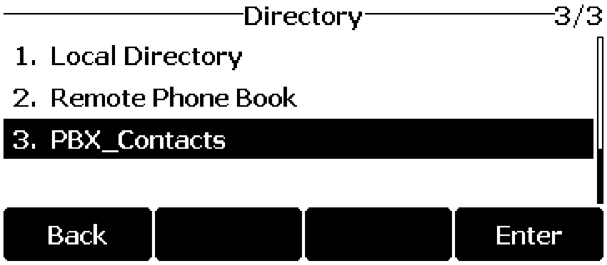
Search Source List In Dialing ?

☑ Disabled 1/1	□ Enabled 3
☑ LDAP	□ Local Directory
	□ History
	□ Remote Phone Book

4. Click Confirm.

Search LDAP Contacts

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

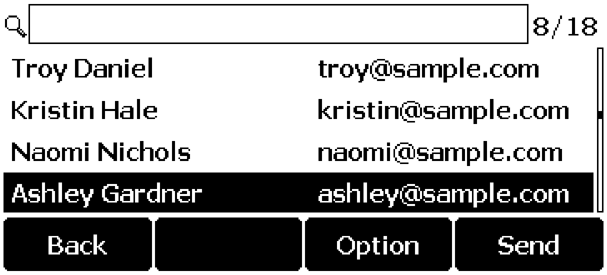


Directory 3/3

1. Local Directory
2. Remote Phone Book
3. PBX_Contacts

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.



8/18

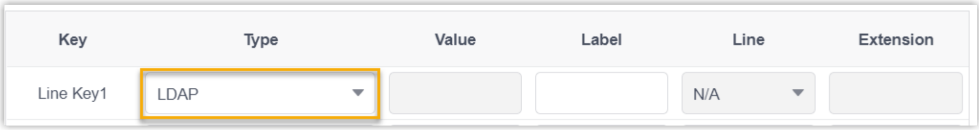
Troy Daniel	troy@sample.com
Kristin Hale	kristin@sample.com
Naomi Nichols	naomi@sample.com
Ashley Gardner	ashley@sample.com

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.

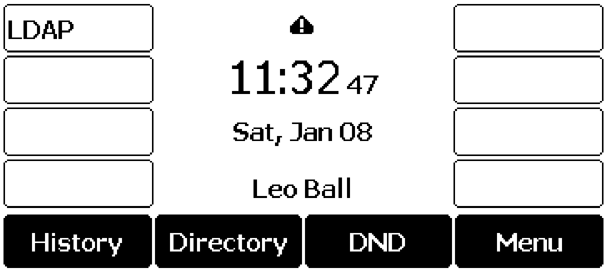


Key	Type	Value	Label	Line	Extension
Line Key1	LDAP			N/A	

3. Click Confirm.

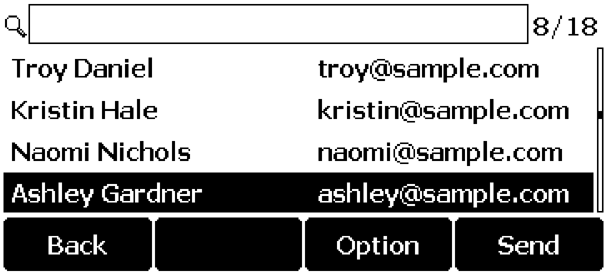
Search LDAP Contacts

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.



Troy Daniel	troy@sample.com
Kristin Hale	kristin@sample.com
Naomi Nichols	naomi@sample.com
Ashley Gardner	ashley@sample.com

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 Software Edition 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.

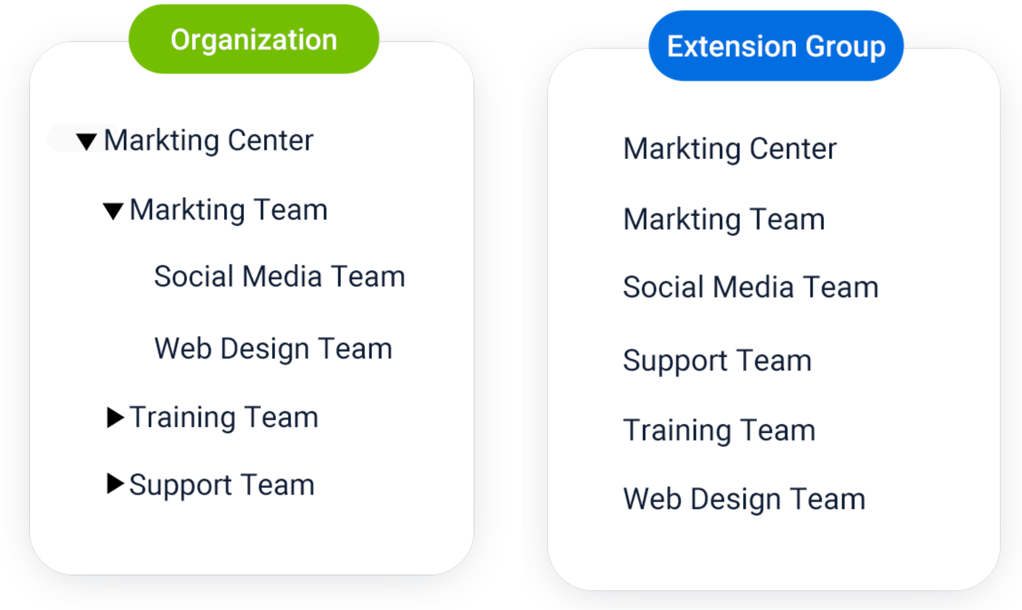
Extension Group feature helps you achieve the followings:

- 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: 83.7.0.16 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

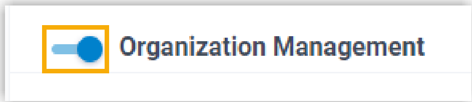
To group extension users into departments, you need to enable the Organization Management feature.

Prerequisites

The version of Yeastar P-Series Software Edition is 83.7.0.16 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

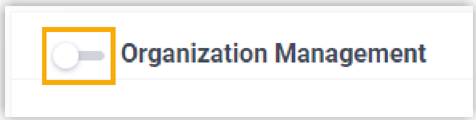
Create departments.

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

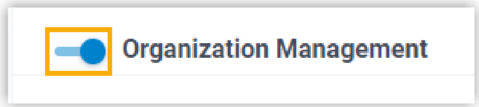
Maximum Number of Extensions (N)	N ≤500	N > 500
Layers of Departments	15	20
Number of Departments	100	1000

Prerequisites

The version of Yeastar P-Series Software Edition is 83.7.0.16 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.

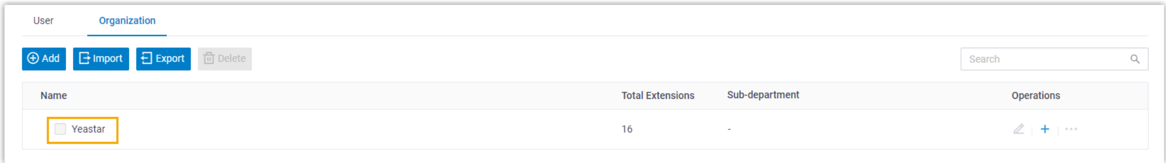
> Note:
> If you have set up company information, the pre-defined company name is automatically synchronized here.

4. Click Save and Apply.

Step 2. Create departments

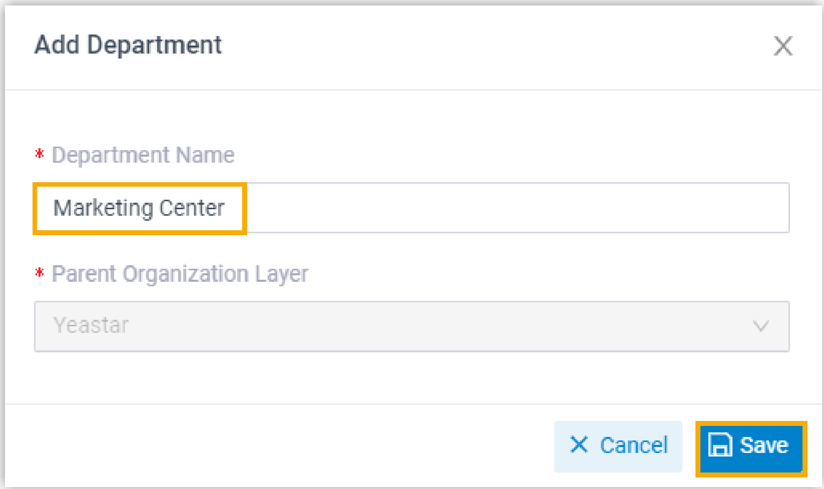
1. Go to Extension and Trunk > Extension > Organization.

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



Name	Total Extensions	Sub-department	Operations
Yeastar	16	-	

2. Click + beside the root organization.
3. In the pop-up window, configure the following information, then click Save.



* Department Name: Marketing Center

* Parent Organization Layer: Yeastar

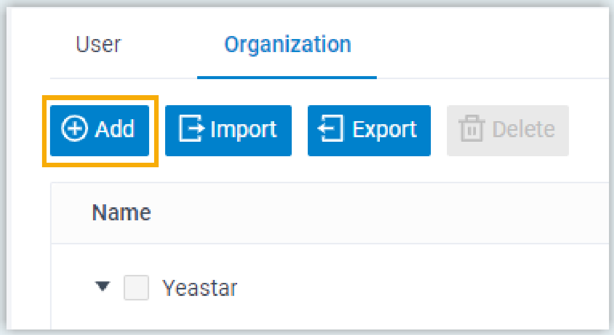
- Department Name: Enter a department name.
- Parent Organization Layer: The root organization is automatically filled in.

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

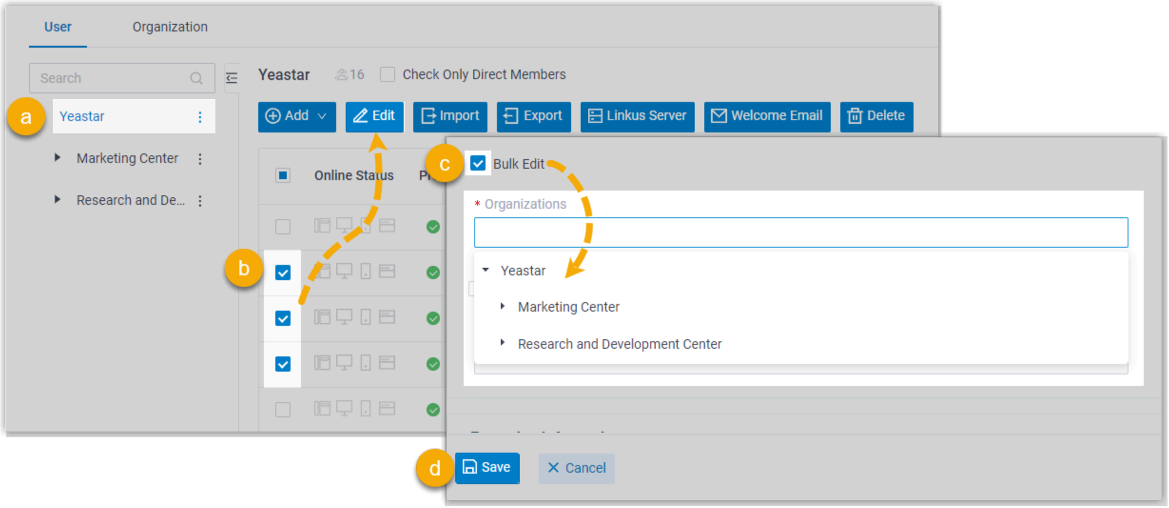
Add Users to Organizations.

Add Users to Organizations

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

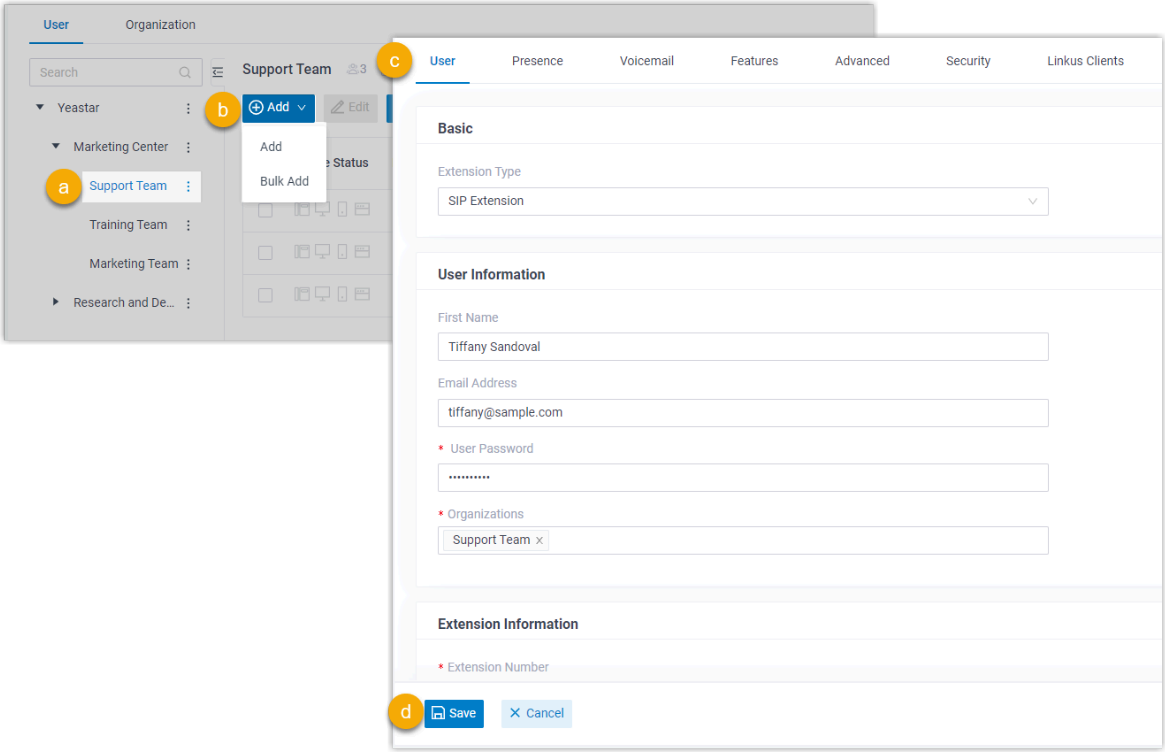
Procedure

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:



Basic

Extension Type: SIP Extension

User Information

First Name: Tiffany Sandoval

Email Address: tiffany@sample.com

* User Password: ••••••••••

* Organizations: Support Team ×

Extension Information

* Extension Number

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.

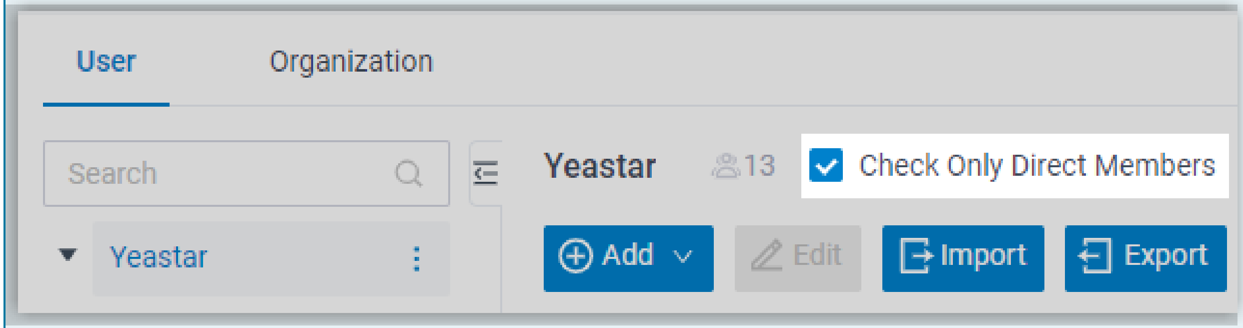
d. Click Save and Apply.

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.



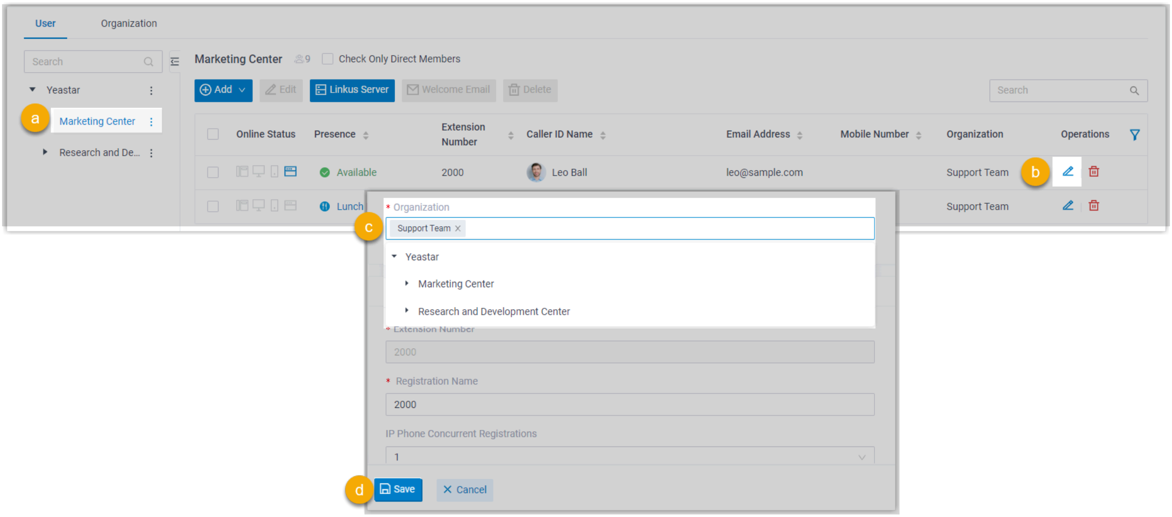
Manage Users within Organizations

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:



Online Status	Presence	Extension Number	Caller ID Name	Email Address	Mobile Number	Organization	Operations
	Available	2000	Leo Ball	leo@sample.com		Support Team	
	Lunch					Support Team	

Organization: Support Team

- Yeastar
  - Marketing Center
  - Research and Development Center

Extension Number: 2000

Registration Name: 2000

IP Phone Concurrent Registrations: 1

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

All the extensions within the department are displayed.

b. Click ✎ beside a desired extension.

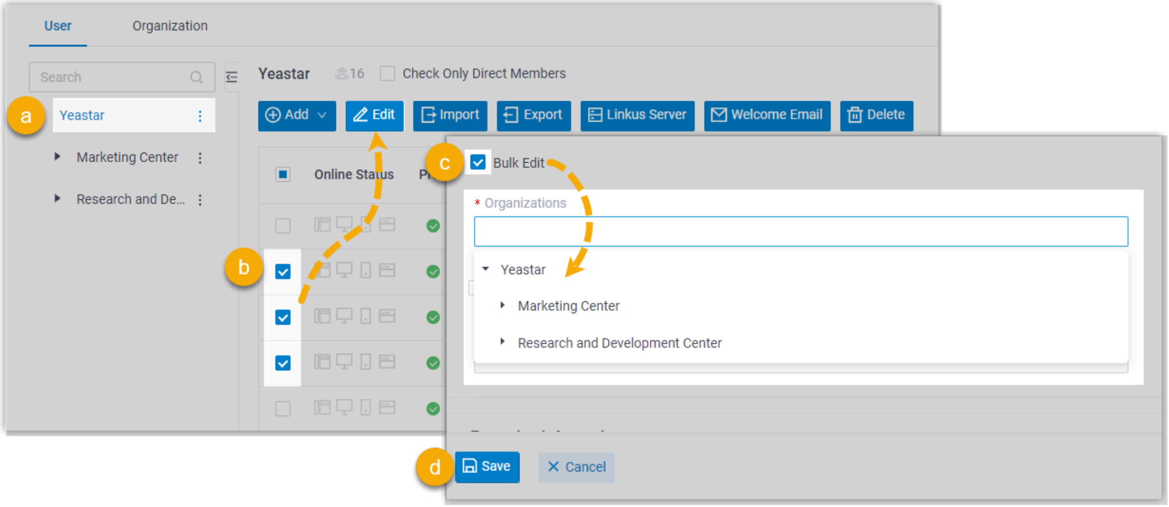
c. In the Organization field , change department as needed.

> 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.

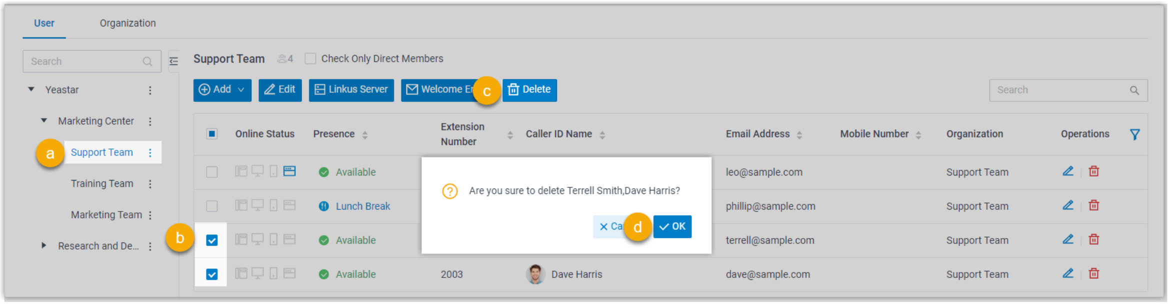
c. Select the checkbox of Bulk Edit for organization, then reselect departments.

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:



Are you sure to delete Terrell Smith,Dave Harris?

	Online Status	Presence	Extension Number	Caller ID Name	Email Address	Mobile Number	Organization	Operations
□		Available			leo@sample.com		Support Team	
□		Lunch Break			phillip@sample.com		Support Team	
☑		Available			terrell@sample.com		Support Team	
☑		Available	2003	Dave Harris	dave@sample.com		Support Team	

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

All the extensions within the department are displayed.

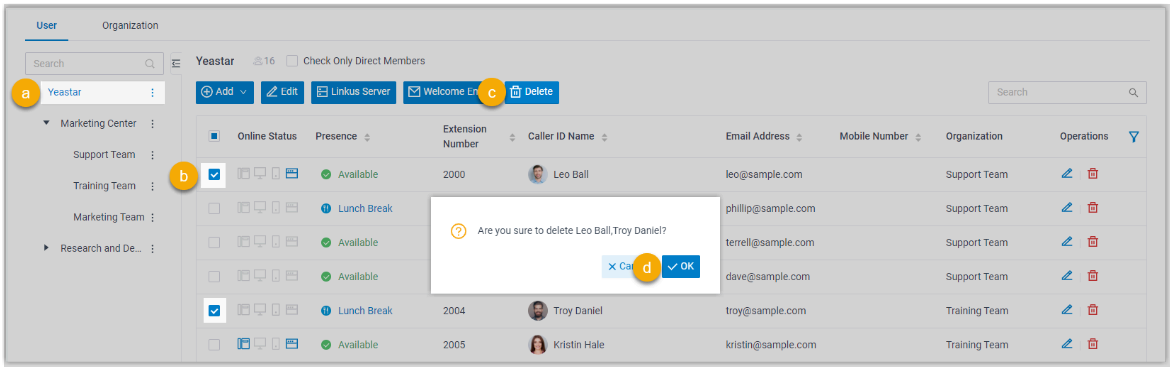
b. Select the checkboxes of desired extensions, then click Delete.

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:



Are you sure to delete Leo Ball,Troy Daniel?

	Online Status	Presence	Extension Number	Caller ID Name	Email Address	Mobile Number	Organization	Operations
☑		Available	2000	Leo Ball	leo@sample.com		Support Team	
□		Lunch Break			phillip@sample.com		Support Team	
□		Available			terrell@sample.com		Support Team	
□		Available			dave@sample.com		Support Team	
☑		Lunch Break	2004	Troy Daniel	troy@sample.com		Training Team	
□		Available	2005	Kristin Hale	kristin@sample.com		Training Team	

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.

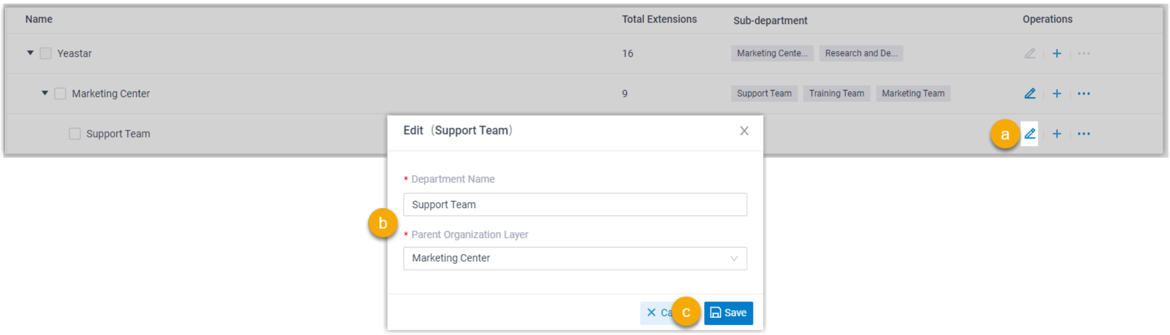
The selected extensions are deleted from the system.

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:



Name	Total Extensions	Sub-department	Operations
Yeastar	16	Marketing Cente... Research and De...	✎ + ···
Marketing Center	9	Support Team Training Team Marketing Team	✎ + ···
Support Team			✎ + ···

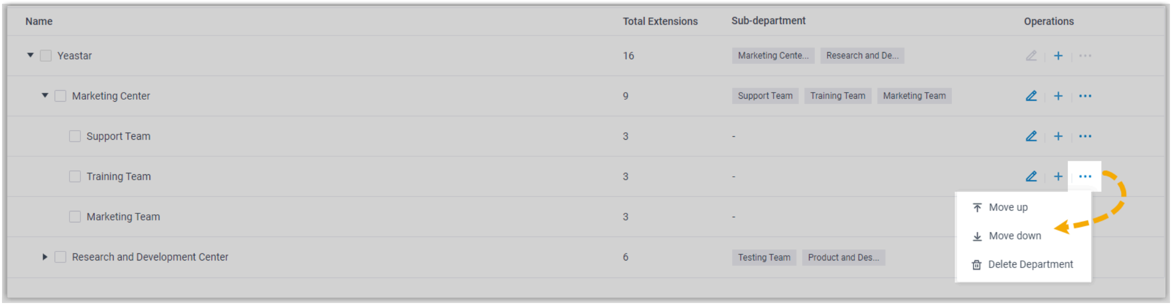
Edit（Support Team）

* Department Name: Support Team

* Parent Organization Layer: Marketing Center

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.



Name	Total Extensions	Sub-department	Operations
Yeastar	16	Marketing Cente... Research and De...	✎ + ···
Marketing Center	9	Support Team Training Team Marketing Team	✎ + ···
Support Team	3	-	✎ + ···
Training Team	3	-	✎ + ···
Marketing Team	3	-	
Research and Development Center	6	Testing Team Product and Des...	

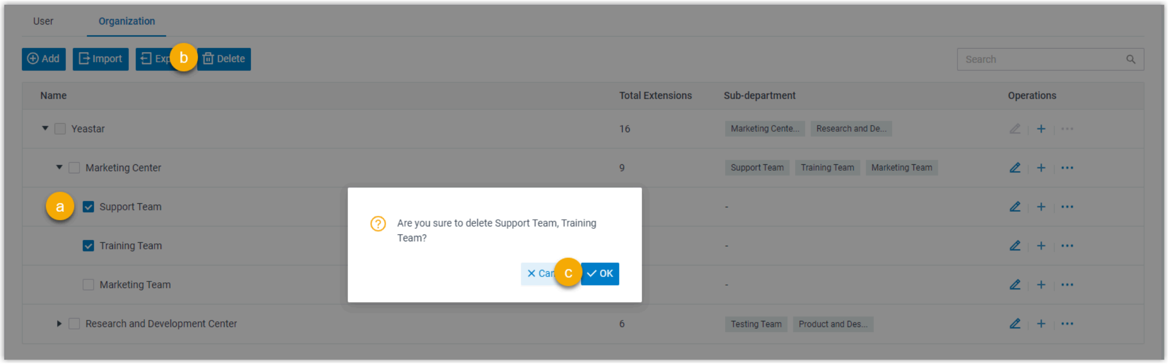
On PBX web portal and Linkus clients, departments are displayed in the new order.

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.



Name	Total Extensions	Sub-department	Operations
▼ □ Yeastar	16	Marketing Cente... Research and De...	
▼ □ Marketing Center	9	Support Team Training Team Marketing Team	
☑ Support Team		-	
☑ Training Team		-	
□ Marketing Team		-	
▶ □ Research and Development Center	6	Testing Team Product and Des...	

Are you sure to delete Support Team, Training Team?

Export and Import Organizations

The organizations configured on Yeastar P-Series Software Edition 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 Software Edition 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 of Operator Panel. Yeastar P-Series Software Edition 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	√	×
	Call monitoring operations (Listen, Whisper, Barge-in)	√	×

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

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 Software Edition 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

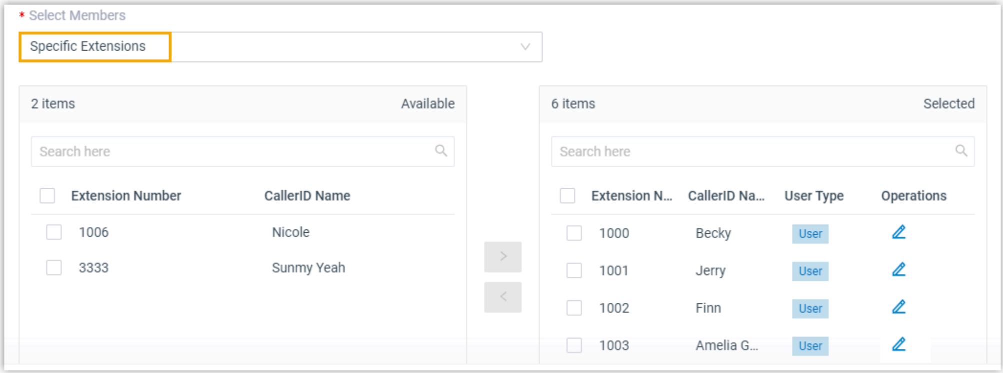
This topic describes how to create an extension group.

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.



* Select Members

Specific Extensions

2 items	Available
Extension Number	CallerID Name
1006	Nicole
3333	Sunmy Yeah

6 items			Selected
Extension N...	CallerID Na...	User Type	Operations
1000	Becky	User	✎
1001	Jerry	User	✎
1002	Finn	User	✎
1003	Amelia G...	User	✎

c. Assign user types for group members.

> Note:
> Users of different user types have different permissions. For more information, see User types in an extension group.

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

> Note:
> The permissions of Manager and User are pre-defined. To change the permissions, see View or change permissions for managers and users.

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

iii. Click Save.

3. 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 Software Edition 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

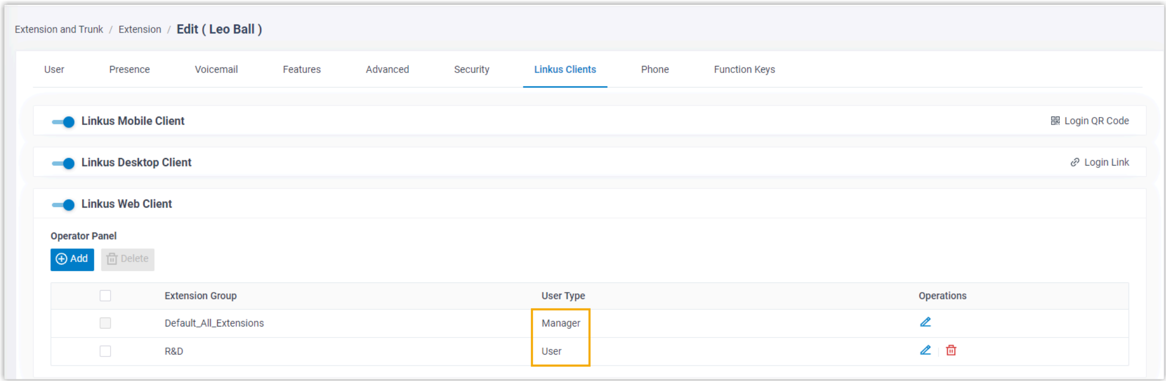
The member's user type and permissions in the group are updated.

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. Click Linkus Clients tab.
3. In the Operator Panelsection, 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.



Extension and Trunk / Extension / Edit (Leo Ball)

Linkus Mobile Client

Linkus Desktop Client

Linkus Web Client

Operator Panel

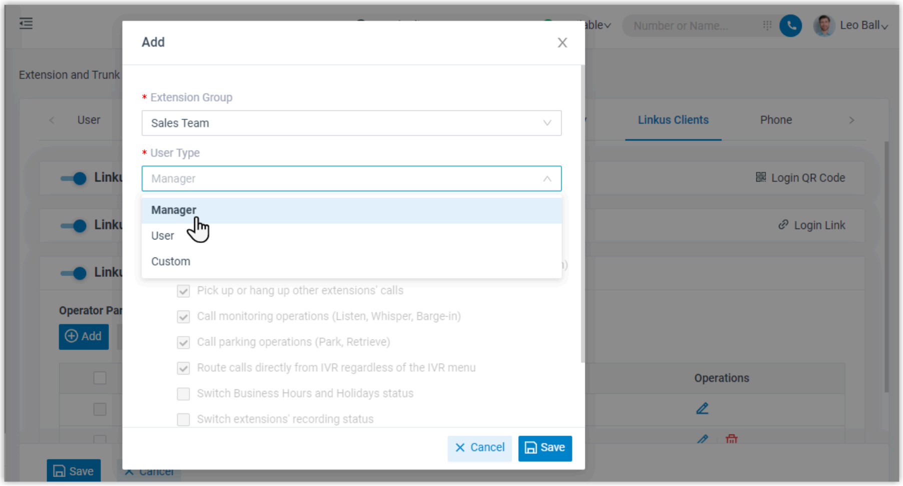
	Extension Group	User Type	Operations
□	Default_All_Extensions	Manager	✎
□	R&D	User	✎ 🗑

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. Click Linkus Clients tab.
3. In the Operator Panel 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.



Add

* Extension Group: Sales Team

* User Type: Manager

- Manager
- User
- Custom

☑ Pick up or hang up other extensions' calls
☑ Call monitoring operations (Listen, Whisper, Barge-in)
☑ Call parking operations (Park, Retrieve)
☑ Route calls directly from IVR regardless of the IVR menu
□ Switch Business Hours and Holidays status
□ Switch extensions' recording status

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

Result

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

Related information

[Assign a User Type to a Group Member]

View or Change Permissions for Group Members

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

View or change permissions for managers and users

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

Procedure

1. Log in to PBX 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.

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

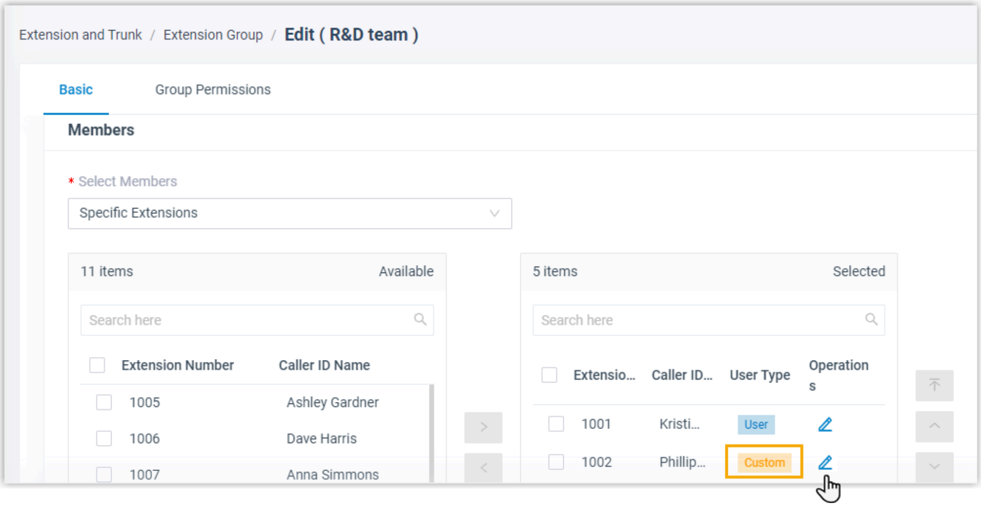
If you want to change members' user types to Manager or User in the group, see Assign a default user type to a group member.

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.



11 items — Available

	Extension Number	Caller ID Name
□	1005	Ashley Gardner
□	1006	Dave Harris
□	1007	Anna Simmons

5 items — Selected

	Extensio...	Caller ID...	User Type	Operations
□	1001	Kristi...	User	✎
□	1002	Phillip...	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 Software Edition. 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 Software Edition supports various models for Auto Provisioning.

Find the Auto Provisioning - Supported Devices before you start deploying devices.

Auto Provisioning methods

Yeastar P-Series Software Edition supports three 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).

> Note:
> Snom IP phones do not support DHCP Auto Provisioning method.

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:
> The Yeastar TA FXS gateway does 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).

Note:

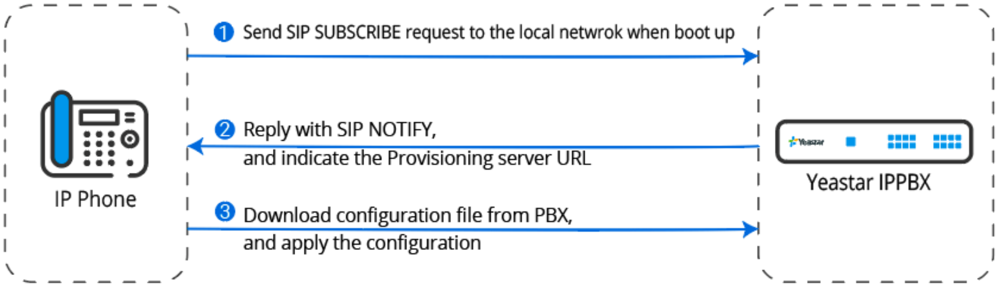
In practice, the actual implemented Auto Provisioning method of IP phone/gateways does not limit to your selected method. The followings shows the detailed information.

- When you select PnP Auto Provisioning method, the available methods are PnP and DHCP.
- When you select DHCP Auto Provisioning method, the available methods are PnP and DHCP.
- When you select RPS Auto Provisioning method, the available methods are PnP, DHCP, and RPS.

How Auto Provisioning works

This section introduces how the three 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



IP Phone
1 Send SIP SUBSCRIBE request to the local netwrok when boot up
2 Reply with SIP NOTIFY, and indicate the Provisioning server URL
3 Download configuration file from PBX, and apply the configuration
Yeastar IPPBX

1. When an IP phone boots up, it sends a multicast SIP SUBSCRIBE message to the local network.
2. The PBX detects the SUBSCRIBE message and replies a SIP NOTIFY to the IP phone, indicating the provisioning server URL.
3. The IP phone downloads configuration file from the PBX and applies the configurations automatically.

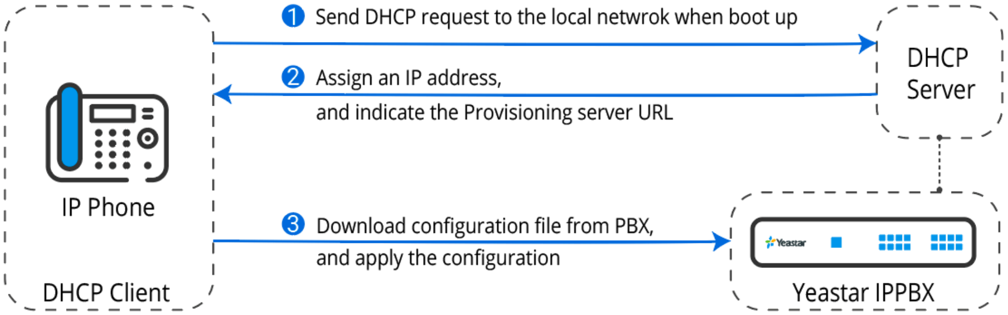
DHCP Provisioning

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

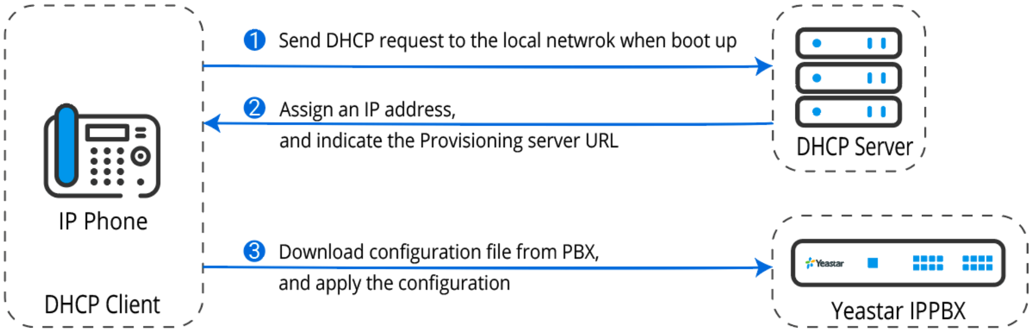
Note:

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

Using the PBX as a DHCP server

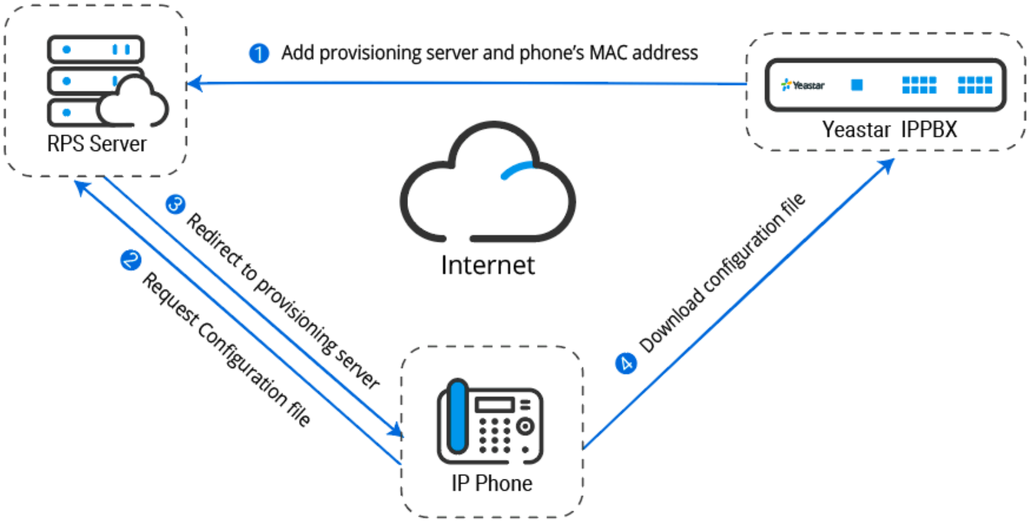

1 Send DHCP request to the local netwrok when boot up
2 Assign an IP address,
and indicate the Provisioning server URL
3 Download configuration file from PBX,
and apply the configuration
IP Phone
DHCP Client
DHCP Server
Yeastar
Yeastar IPPBX

Using a third-party DHCP server


1 Send DHCP request to the local netwrok when boot up
2 Assign an IP address,
and indicate the Provisioning server URL
3 Download configuration file from PBX,
and apply the configuration
IP Phone
DHCP Client
DHCP Server
Yeastar
Yeastar IPPBX

1. When an IP phone boots up, it sends DHCP requests to the local network.
2. The DHCP server assigns an IP address, and indicates the provisioning server URL in DHCP option 66.
3. The IP phone downloads the configuration file from the provisioning server (PBX), and applies the configuration.

RPS Provisioning


1 Add provisioning server and phone's MAC address
RPS Server
Yeastar IPPBX
Internet
3 Redirect to provisioning server
2 Request Configuration file
4 Download configuration file
IP Phone

1. After you add a phone's MAC address to the PBX, the phone's MAC address and provisioning server (PBX) are automatically added to the phone manufacture's RPS server.
2. When the IP phone boots up, it sends a request to the RPS server, asking for a configuration file.
3. The RPS server redirects the phone to visit the provisioning server (PBX).
4. The IP phone downloads its configuration file from the provisioning server (PBX), and applies the configuration.

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 Software Edition.

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

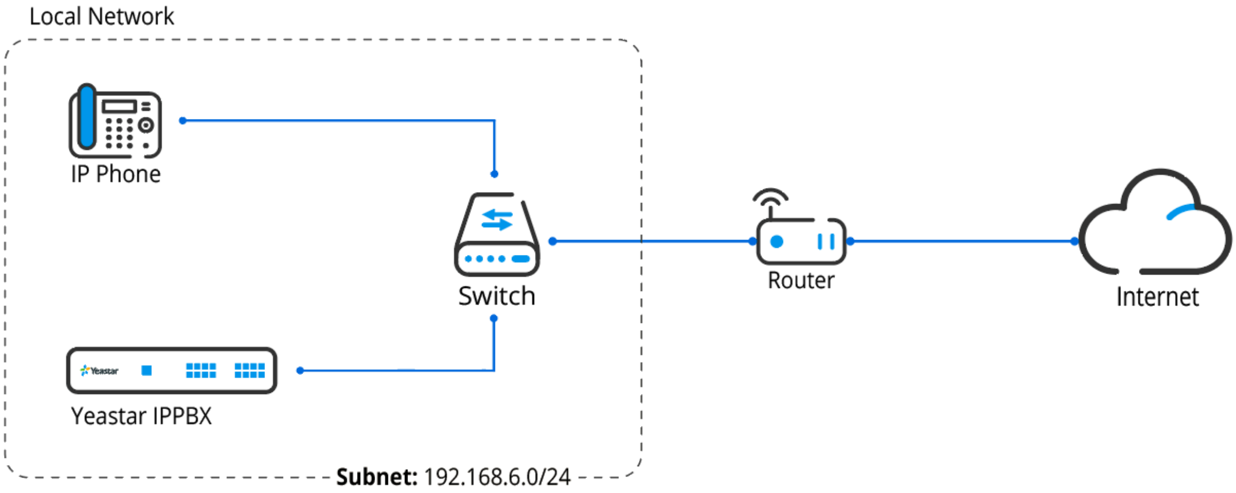
  IP: 192.168.5.150, Mask: 255.255.255.0

  IP: 192.168.66.170, Mask: 255.255.255.0

- IP Phone MUST support PnP provisioning method.

Scenario

An IP phone (IP address: 192.168.6.33) and a PBX (IP address: 192.168.6.150) are located in the same LAN subnet.



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.

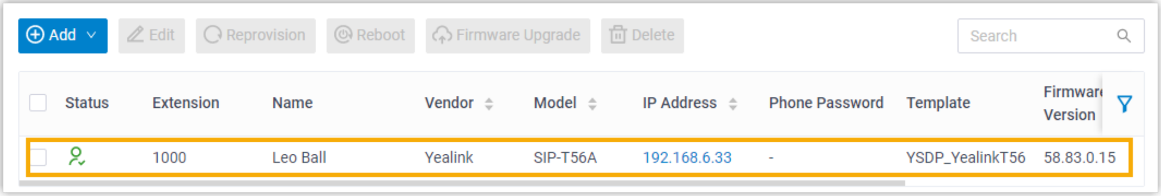
6. In the Assign Extension section, assign an extension for the phone.

> 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.



Status	Extension	Name	Vendor	Model	IP Address	Phone Password	Template	Firmware Version
👤✓	1000	Leo Ball	Yealink	SIP-T56A	192.168.6.33	-	YSDP_YealinkT56	58.83.0.15

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)
Manually Provision an IP Phone
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 doesn't support PnP provisioning, you can provision the IP phones by DHCP method.

Supported IP phones

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

Note:

Snom IP phones don't support DHCP Auto Provisioning method.

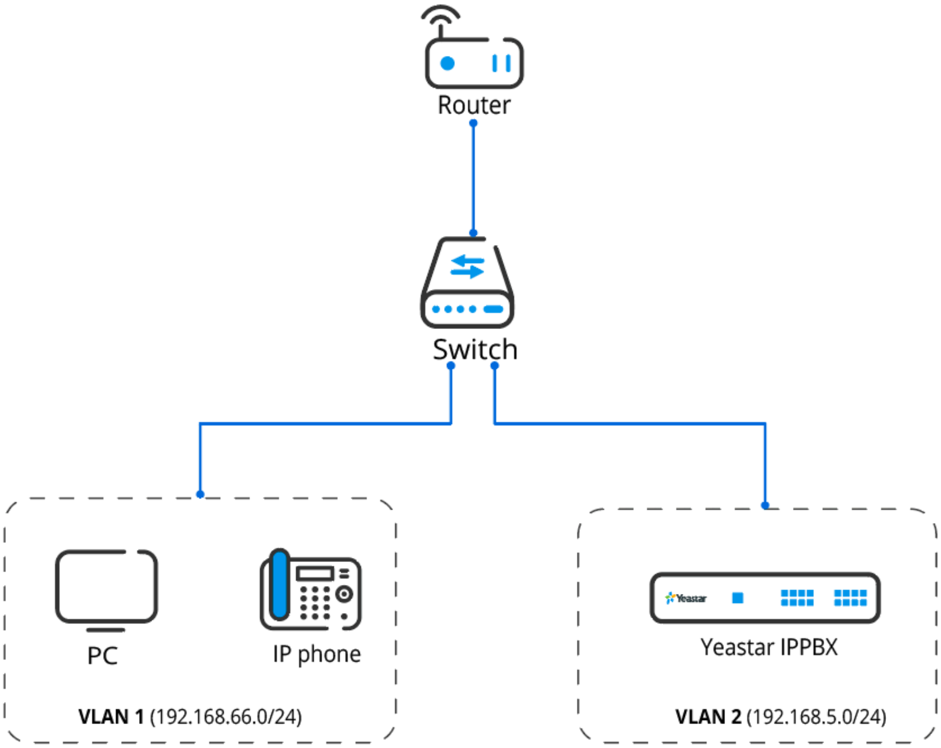
Prerequisites

- Make sure there is only one DHCP server, otherwise the IP phone may fail to obtain an IP address.
- DHCP provisioning is supported on the phone.
- Gather information of IP phone, including Vendor, Model, and MAC address.

Scenario

A company subdivides a physical network into separate Virtual LANs (VLANs) as the following figure shows.

- IP phone: Located in VLAN 1 (192.168.66.0/24)
- PBX: Located in VLAN 2 (192.168.5.0/24)



Procedure

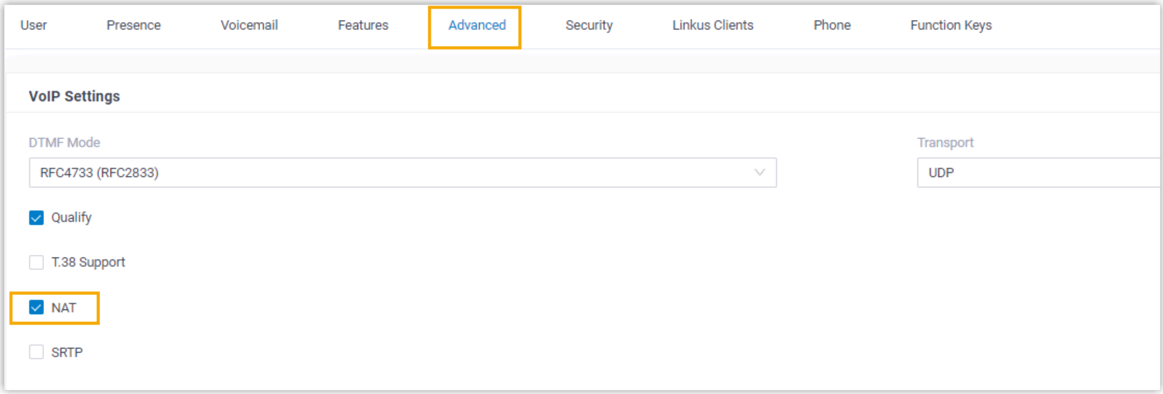
Step1. Set a remote extension

Step2. 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.



VoIP Settings

DTMF Mode: RFC4733 (RFC2833)

Transport: UDP

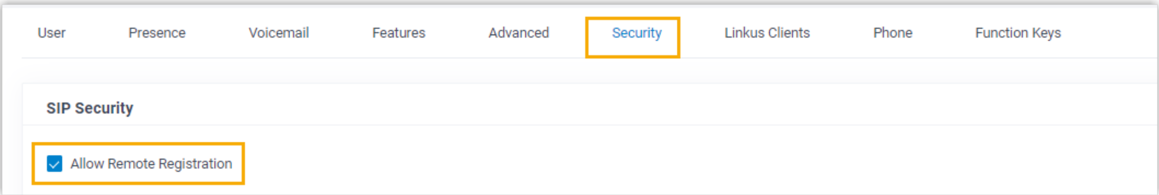
☑ Qualify

☐ T.38 Support

☑ NAT

☐ SRTP

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



SIP Security

☑ Allow Remote Registration

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.

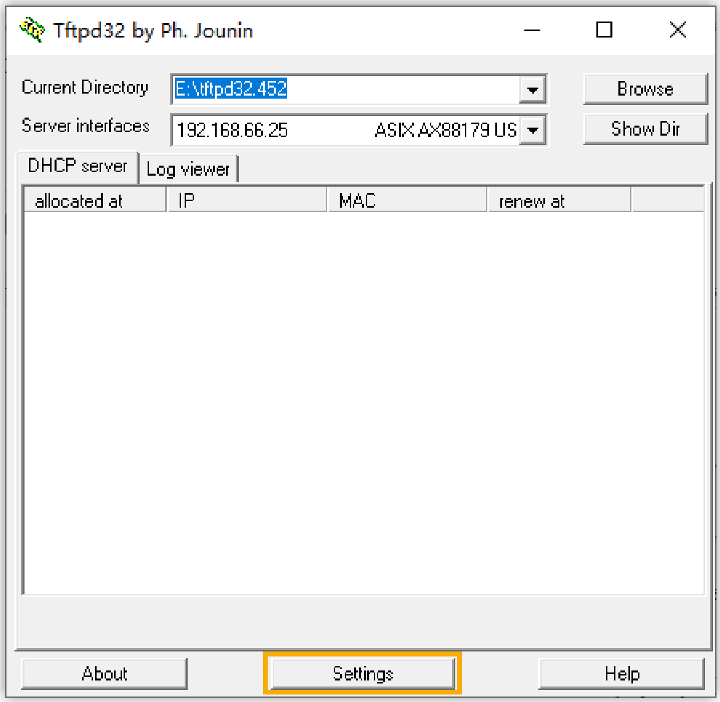
7. Click Save.

   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.

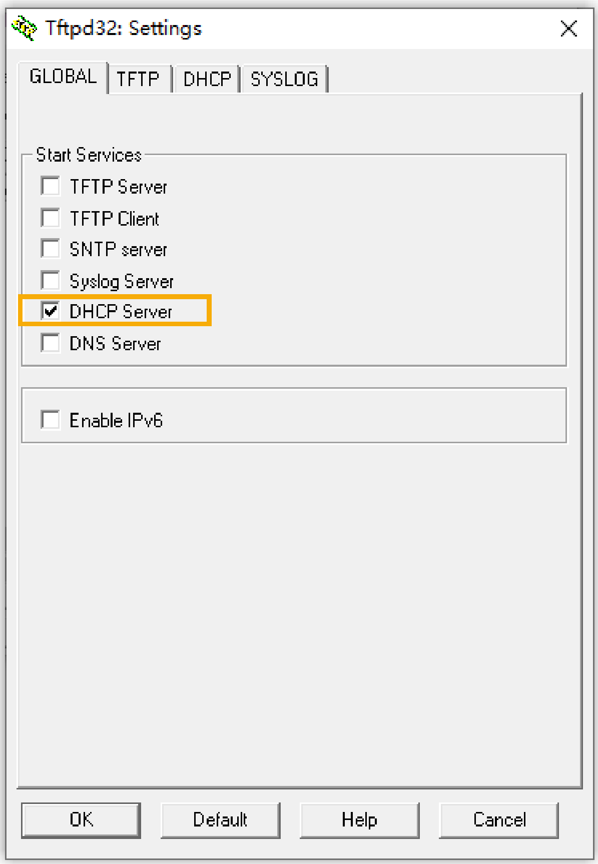


Tftpd32 by Ph. Jounin

Current Directory: E:\tftpd32.452

Server interfaces: 192.168.66.25 ASIX AX88179 US

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

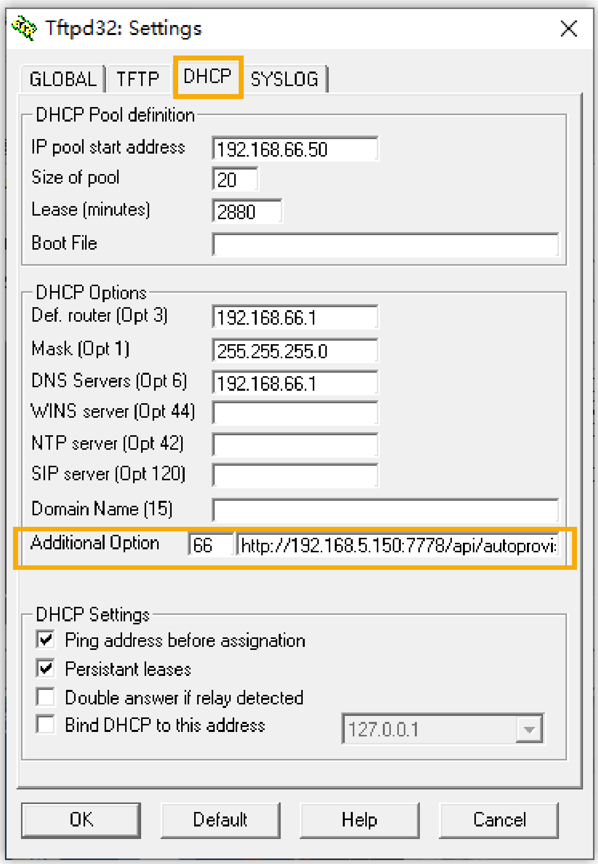


Start Services

- □ TFTP Server
- □ TFTP Client
- □ SNTP server
- □ Syslog Server
- ☑ DHCP Server
- □ DNS Server

□ Enable IPv6

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



DHCP Pool definition

IP pool start address: 192.168.66.50
Size of pool: 20
Lease (minutes): 2880
Boot File:

DHCP Options

Def. router (Opt 3): 192.168.66.1
Mask (Opt 1): 255.255.255.0
DNS Servers (Opt 6): 192.168.66.1
WINS server (Opt 44):
NTP server (Opt 42):
SIP server (Opt 120):
Domain Name (15):
Additional Option: 66 http://192.168.5.150:7778/api/autoprovi:

DHCP Settings

☑ Ping address before assignation
☑ Persistant leases
□ Double answer if relay detected
□ Bind DHCP to this address 127.0.0.1

- 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.

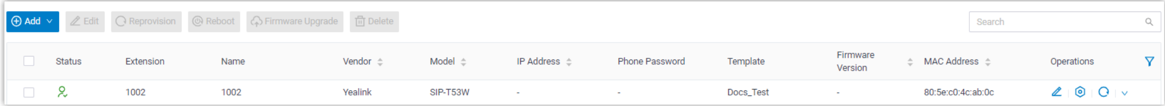
4. Click OK.

   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.



□	Status	Extension	Name	Vendor	Model	IP Address	Phone Password	Template	Firmware Version	MAC Address	Operations
□	✓	1002	1002	Yealink	SIP-T53W	-	-	Docs_Test	-	80:5e:c0:4c:ab:0c	

Auto Provision IP Phones Remotely (RPS FQDN Method)

When IP phones are located in remote network, Yeastar P-Series Software Edition 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.

Supported IP phones

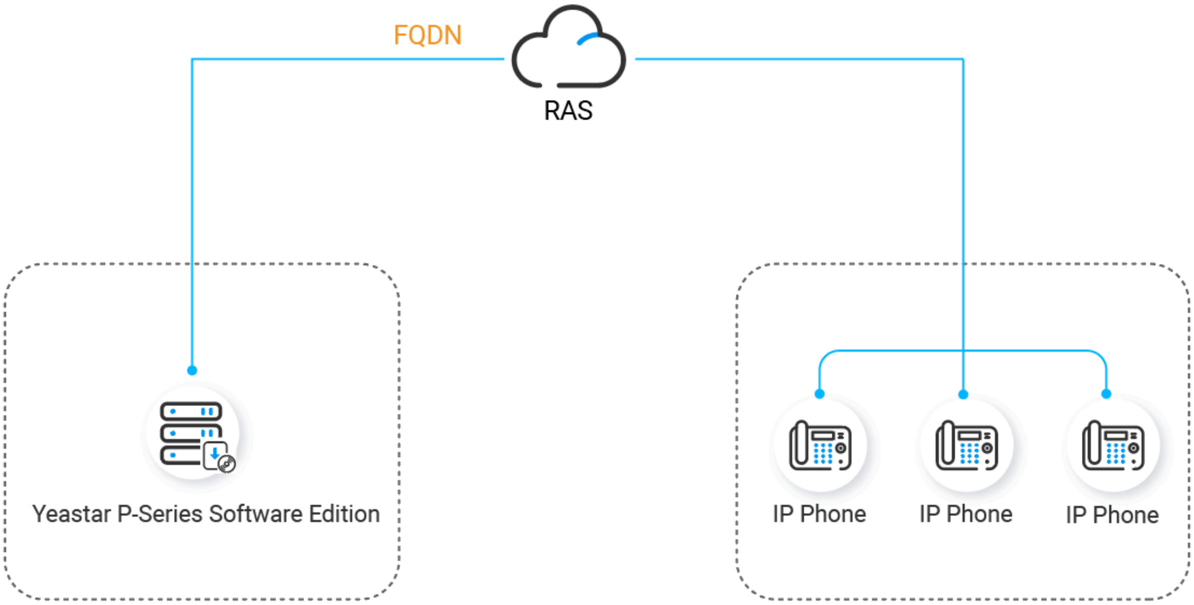
This topic can be applied to the RPS supported IP phones that are deployed in a remote network.

Prerequisites

- 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.
- Gather information of IP phone, including Vendor, Model, and MAC address.

Scenario

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



Procedure

Step1. Generate configuration file for an IP phone on the PBX

Step2. Reboot the IP phone to obtain the configuration file

Step1. 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.

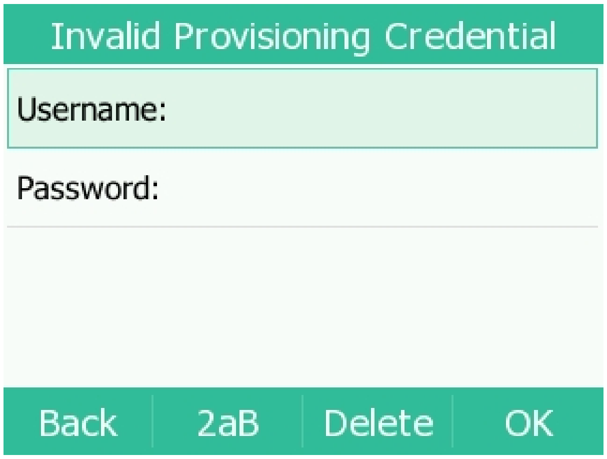
7. Click Save.

   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.

Step2. 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.



Invalid Provisioning Credential

Username:

Password:

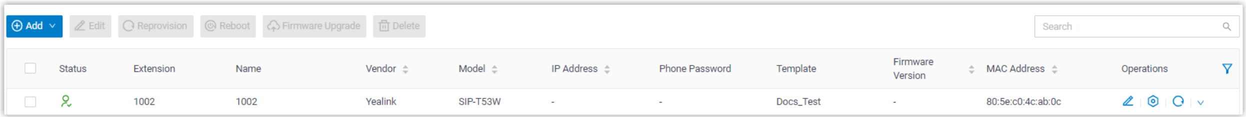
- Username: Enter the extension number that is assigned to the phone.
- Password: Enter the extension's Voicemail Access PIN.

> 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.



□	Status	Extension	Name	Vendor	Model	IP Address	Phone Password	Template	Firmware Version	MAC Address	Operations
□	👤✓	1002	1002	Yealink	SIP-T53W	-	-	Docs_Test	-	80:5e:c0:4c:ab:0c	

Auto Provision IP Phones Remotely (RPS Method)

When IP phones are located in remote network, Yeastar P-Series Software Edition 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.

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.

  > Note:
  > The port forwarding is not necessary if your Yeastar P-Series Software Edition is installed on a cloud server.

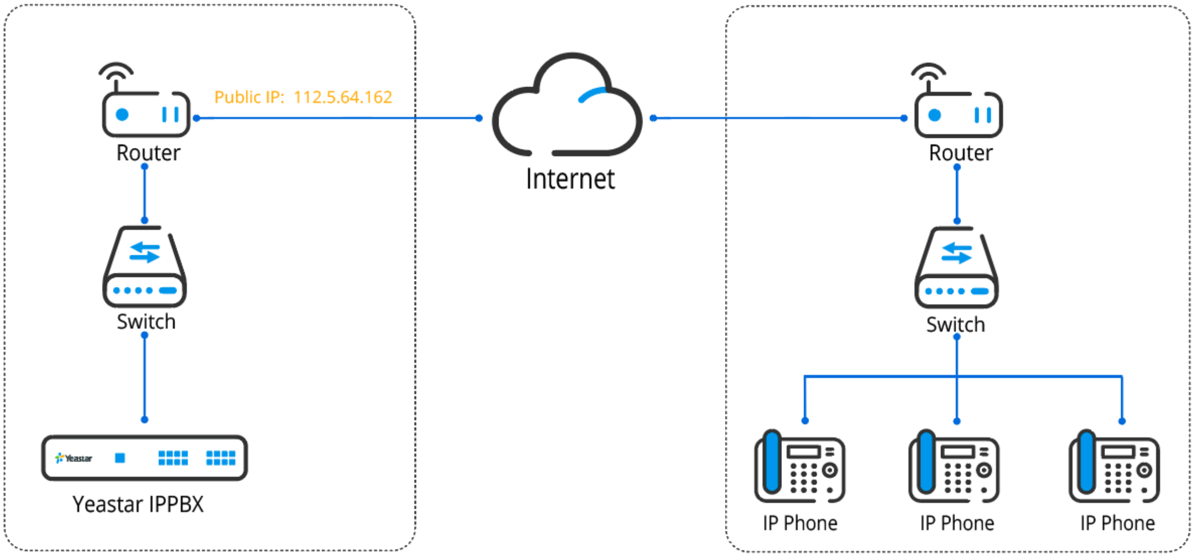
  > Important:
  > The following ports must be forwarded for RPS provisioning.
  > - RTP ports
  > - SIP port
  > - Web Server port

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

- Gather information of IP phone, including Vendor, Model, and MAC address.

Scenario

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



Procedure

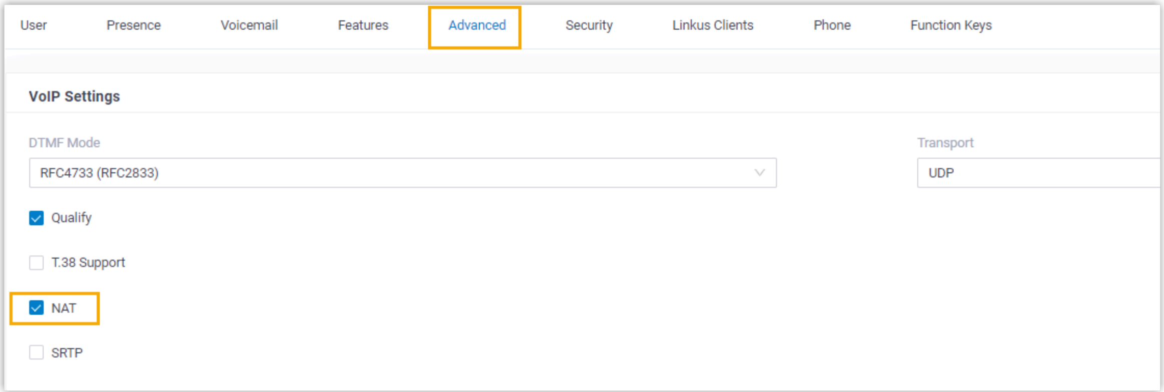
Step1. Set a remote extension

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

Step3. Reboot the IP phone to obtain the configuration file

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.



VoIP Settings

DTMF Mode: RFC4733 (RFC2833)

Transport: UDP

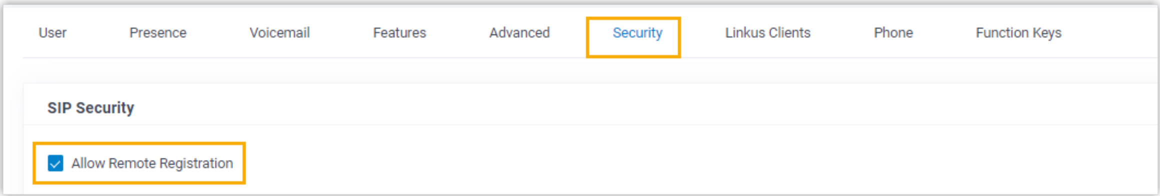
☑ Qualify

☐ T.38 Support

☑ NAT

☐ SRTP

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



SIP Security

☑ Allow Remote Registration

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 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.

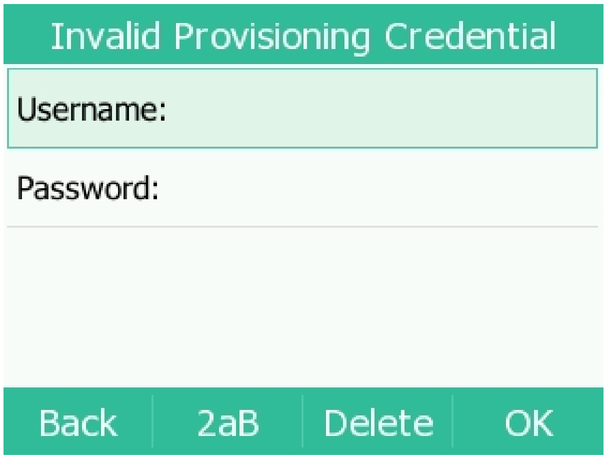
7. Click Save.

   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.

Step3. 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.


Invalid Provisioning Credential

Username:

Password:

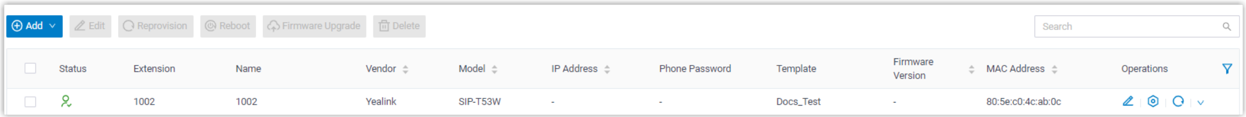
   - Username: Enter the extension number that is assigned to the phone.
   - Password: Enter the extension's Voicemail Access PIN.

> 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.



□	Status	Extension	Name	Vendor	Model	IP Address	Phone Password	Template	Firmware Version	MAC Address	Operations
□	✓	1002	1002	Yealink	SIP-T53W	-	-	Docs_Test	-	80:5e:c0:4c:ab:0c	

Related information

[Auto Provision IP Phones Remotely (RPS FQDN Method)]

Provision IP Phones on Multiple Servers

When you want to conduct IP phone diagnostics and manage the IP phones on the Yealink device management platform, and assign extension, supply configuration files and upgrade device firmware for the IP phones on Yeastar P-Series Software Edition, you can provision the IP phones on both servers.

Applications

This topic is applied to the remote deployment of Yealink IP phones.

Prerequisites

You have an account of the Yealink Device Management Platform.

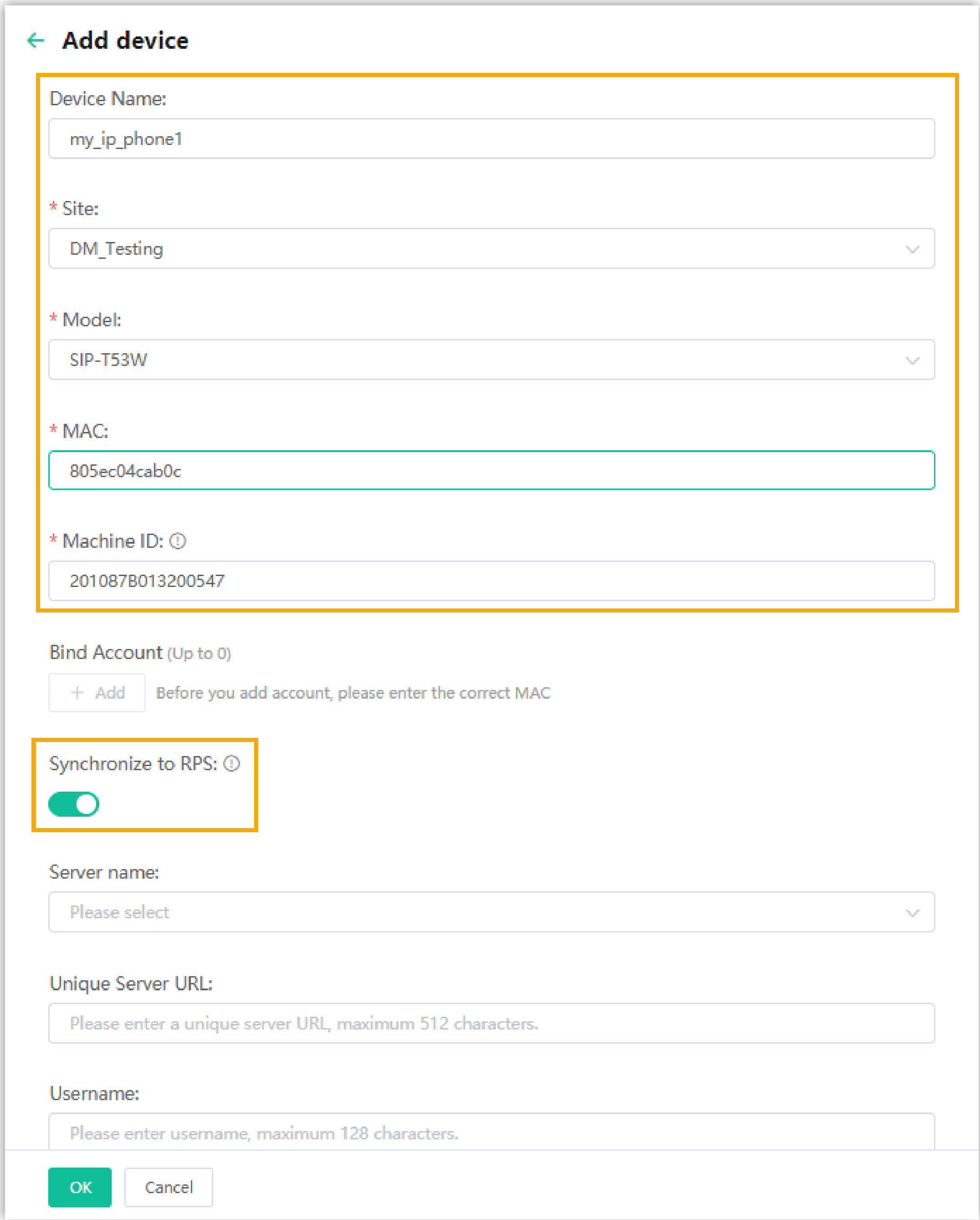
Procedure

- Step1. Add IP phones on Yealink Device Management Platform

  > Note:
  > If the IP phone is already added to the PBX, you need to remove it from PBX first.
- Step2. Add IP phones on the PBX
- Step3. Configure global Auto Provisioning URL on Yealink Device Management Platform

Add IP phones on Yealink device management platform

1. Log in to the Yealink Device Management Platform.
2. Go to Device Management > Phone Device, click Add device to add a phone.
    a. Complete the following configurations.



Add device

Device Name: my_ip_phone1

* Site: DM_Testing

* Model: SIP-T53W

* MAC: 805ec04cab0c

* Machine ID: 201087B013200547

Bind Account (Up to 0)

Before you add account, please enter the correct MAC

Synchronize to RPS: on

Server name: Please select

Unique Server URL: Please enter a unique server URL, maximum 512 characters.

Username: Please enter username, maximum 128 characters.

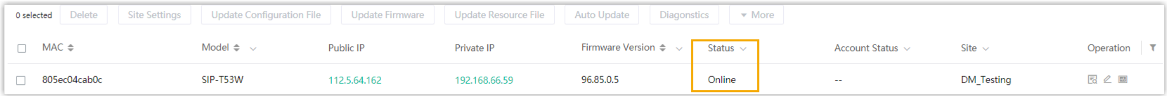
- Device Name: Specify a device name.
- Site: Select a site in the drop-down list.
- Model: Select the phone model in the drop-down list.

- MAC: Enter the MAC address of the IP phone.
- Machine ID: Enter the serial number of the IP phone.
- Synchronize to RPS: Enable this feature to synchronize the IP phone to RPS server.

b. Click OK.

3. Reboot the IP phone.

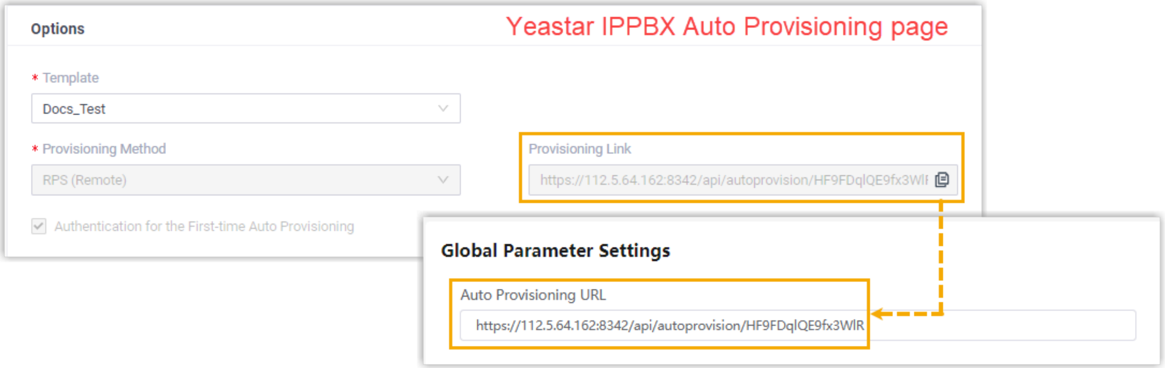
   The phone is connected to the Device Management Platform, and the status displays "Online" on the platform.



MAC	Model	Public IP	Private IP	Firmware Version	Status	Account Status	Site	Operation
805ec04cab0c	SIP-T53W	112.5.64.162	192.168.66.59	96.85.0.5	Online	--	DM_Testing	

Configure global Auto Provisioning URL on Yealink Device Management Platform

1. Log in to 'Yealink Device Management Platform.
2. Go to Device Configuration > Global Parameter Settings.
3. Paste the PBX provisioning link in the Auto Provisioning URL.



Options

* Template: Docs_Test

* Provisioning Method: RPS (Remote)

☑ Authentication for the First-time Auto Provisioning

Provisioning Link: https://112.5.64.162:8342/api/autoprovision/HF9FDqlQE9fx3WlI

Global Parameter Settings

Auto Provisioning URL: https://112.5.64.162:8342/api/autoprovision/HF9FDqlQE9fx3WlR

4. Click Save and update.
5. In the pop-up dialog box, click OK to update the settings.

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.

Supported IP phones

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

Prerequisites

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

Procedure

- Step1. Add phone's MAC address on the PBX
- Step2. Configure provisioning server address on the phone

Step1. 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.

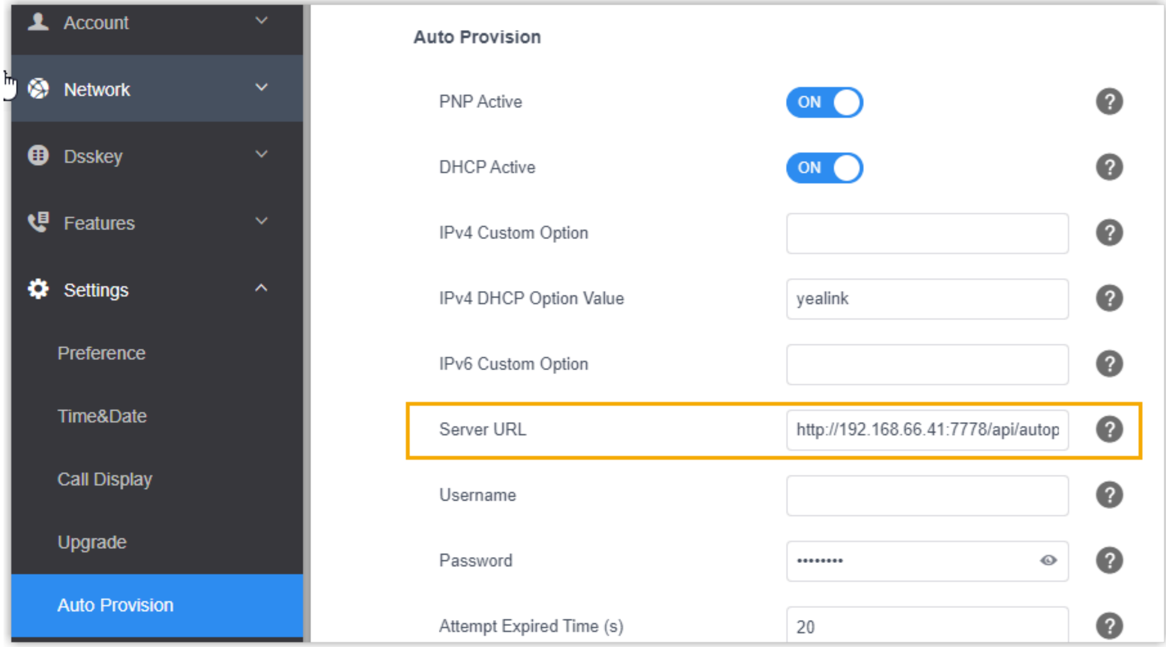
    A configuration file for the phone is generated in the PBX.

Step2. 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, followed by the configuration file for the phone.

   For example, `http://192.168.66.41:7778/api/autoprovision/HF9FDqlQE9fx3Wl-R/05ec04cab0c.cfg`.



Auto Provision

PNP Active	ON
DHCP Active	ON
IPv4 Custom Option	
IPv4 DHCP Option Value	yealink
IPv6 Custom Option	
Server URL	http://192.168.66.41:7778/api/autop
Username	
Password	••••••••
Attempt Expired Time (s)	20

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 Software Edition.

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.

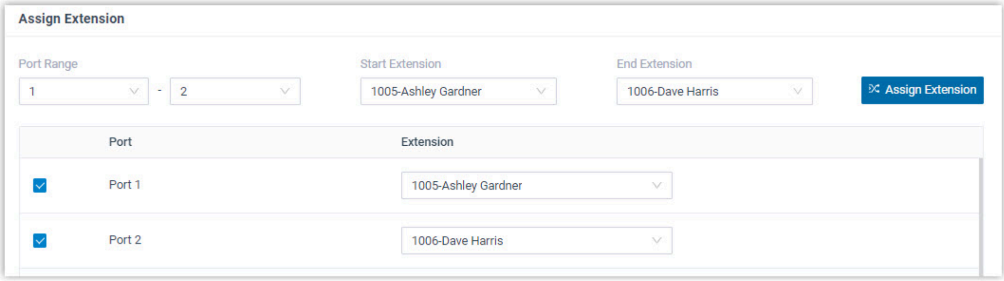
        > Note:
        >
        > The template provides configurations except extension assignment. You can select the default template corresponding to the gateway model, or customize your own template. For more information, see Create a Custom Auto Provisioning Template.
      - Provisioning Method: Select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



Assign Extension

Port Range: 1 - 2
Start Extension: 1005-Ashley Gardner
End Extension: 1006-Dave Harris

	Port	Extension
☑	Port 1	1005-Ashley Gardner
☑	Port 2	1006-Dave Harris

c. In the Preference section, configure the settings as your need.

- Key as Send: Assign the pound key (“#”) or asterisk key (“*”) as the send key.
- SIP VoIPServer IDX: Select a VoIP server template ID to be provisioned.

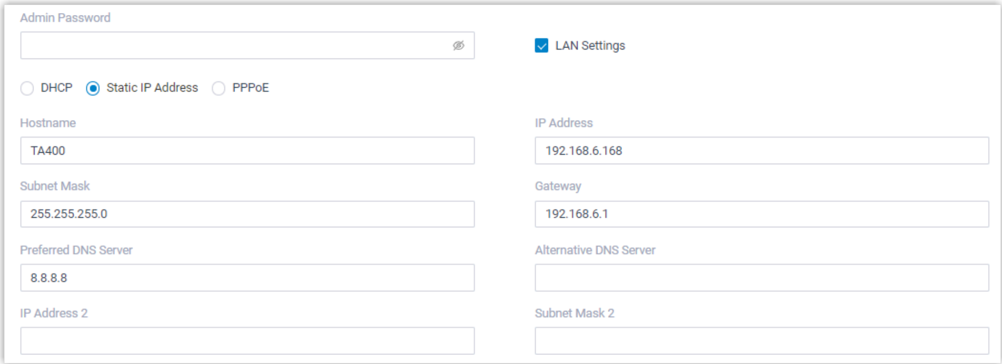
> Note:
>
> SIP VoIPServer IDX is not applicable for TA100 and TA200.

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

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

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

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



Admin Password	☑ LAN Settings
○ DHCP ● Static IP Address ○ PPPoE	
Hostname: TA400	IP Address: 192.168.6.168
Subnet Mask: 255.255.255.0	Gateway: 192.168.6.1
Preferred DNS Server: 8.8.8.8	Alternative DNS Server:
IP Address 2:	Subnet Mask 2:

   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

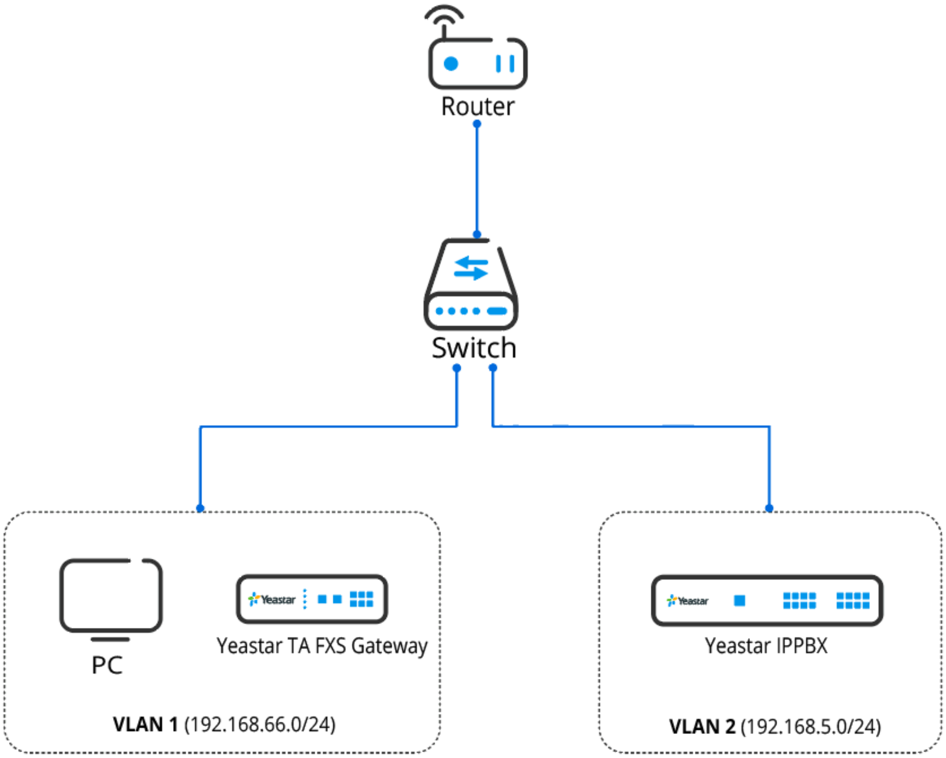
- Make sure there is only one DHCP server, otherwise the gateway may fail to obtain an IP address.

- 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

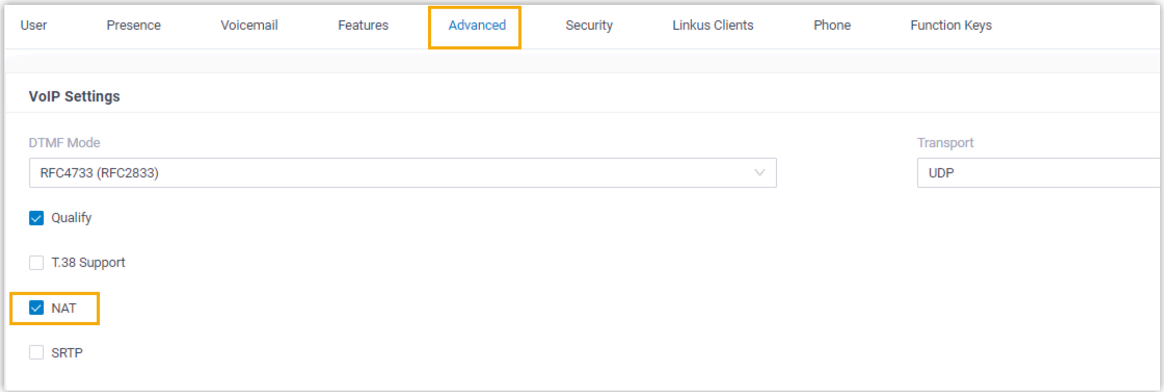
Step2. Add gateway's MAC address on the PBX

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.



VoIP Settings

DTMF Mode: RFC4733 (RFC2833)

Transport: UDP

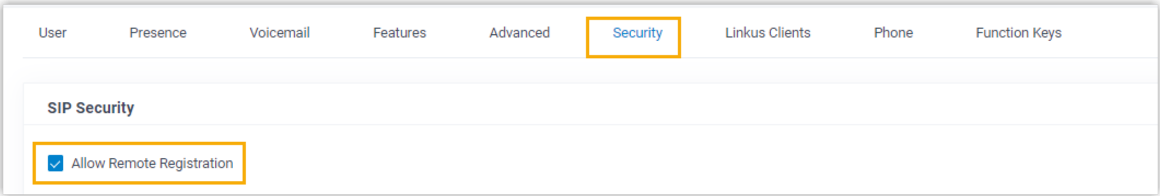
☑ Qualify

□ T.38 Support

☑ NAT

□ SRTP

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



SIP Security

☑ Allow Remote Registration

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.

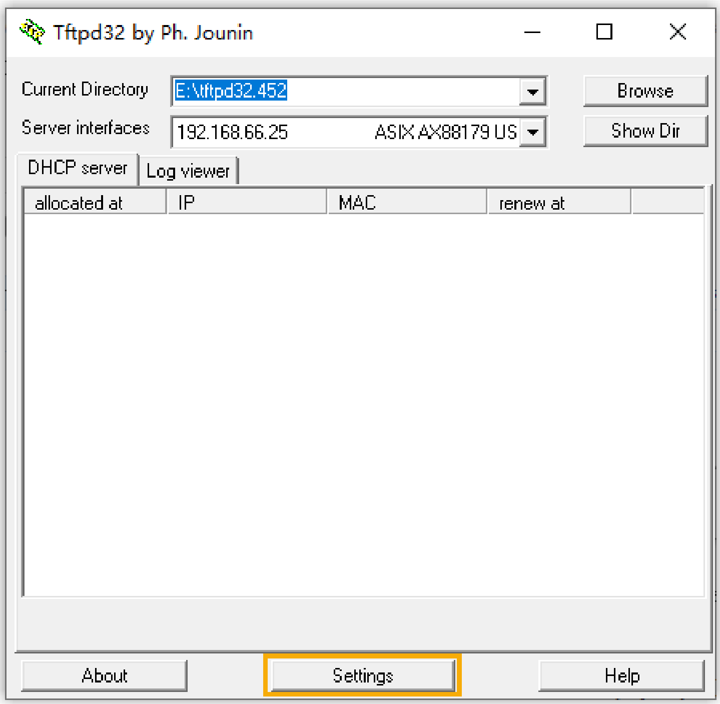
    > Tip:
    > If your desired extension is not listed in the drop-down list, you can check if the extension has been associated with other IP phone or gateway.
    > - To release the previous phone or gateway, see Release an Extension from a Provisioned IP Phone/Gateway.
    > - To associate an extension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

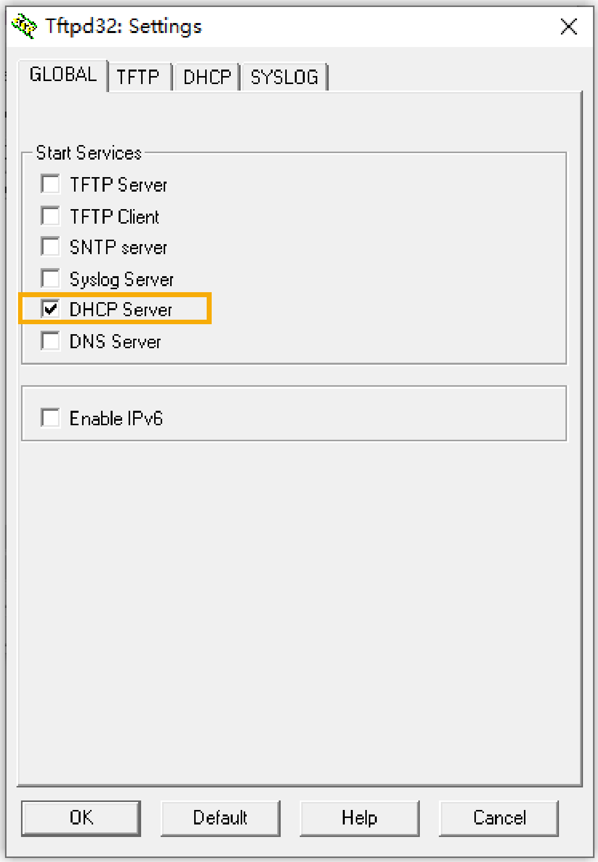

Tftpd32 by Ph. Jounin

Current Directory: E:\tftpd32.452

Server interfaces: 192.168.66.25 ASIX AX88179 US

allocated at	IP	MAC	renew at

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

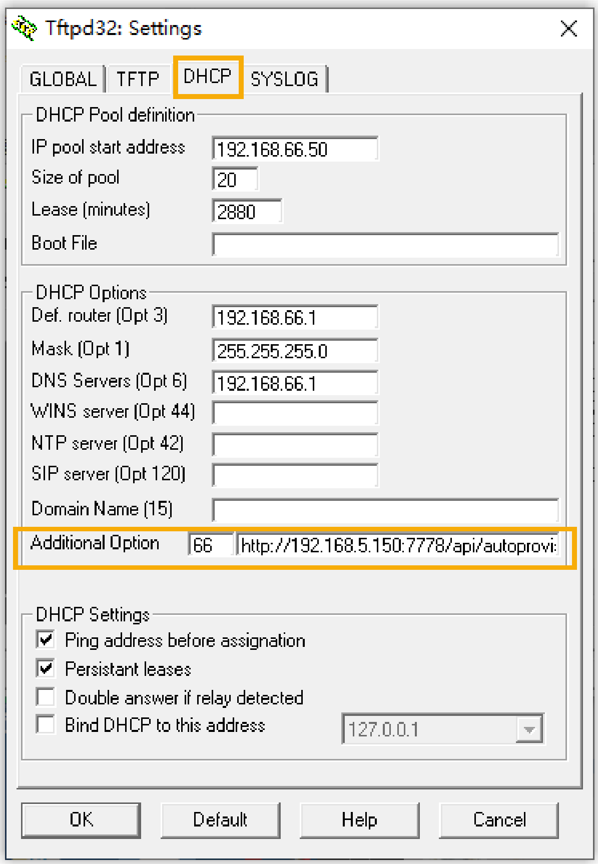

Tftpd32: Settings

Start Services

□ TFTP Server
□ TFTP Client
□ SNTP server
□ Syslog Server
☑ DHCP Server
□ DNS Server

□ Enable IPv6

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



DHCP Pool definition

IP pool start address: 192.168.66.50

Size of pool: 20

Lease (minutes): 2880

Boot File:

DHCP Options

Def. router (Opt 3): 192.168.66.1

Mask (Opt 1): 255.255.255.0

DNS Servers (Opt 6): 192.168.66.1

WINS server (Opt 44):

NTP server (Opt 42):

SIP server (Opt 120):

Domain Name (15):

Additional Option: 66 http://192.168.5.150:7778/api/autoprovi:

DHCP Settings

☑ Ping address before assignation

☑ Persistant leases

☐ Double answer if relay detected

☐ Bind DHCP to this address 127.0.0.1

- 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.

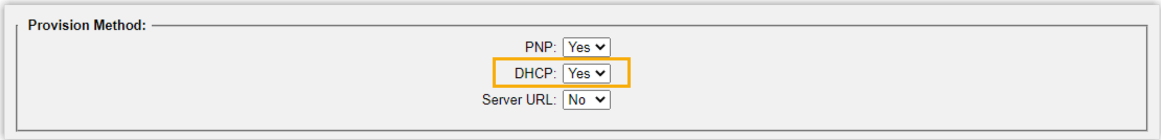
   The PC starts to work as a DHCP server.

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.



Provision Method:

PNP: Yes

DHCP: Yes

Server URL: No

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.

Manage Provisioned Devices

Remotely Access a Provisioned IP Phone / Gateway

Yeastar P-Series Software Edition 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 Software Edition 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.

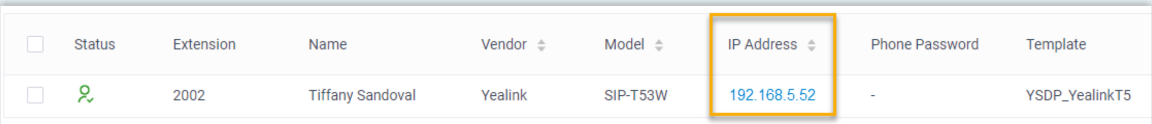
Prerequisites

To implement the IP phone / gateway remote access, make sure the followings are ready:

- The PBX is installed on an on-premise server or a virtual machine.
- The PBX firmware version is 83.7.0.16 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.

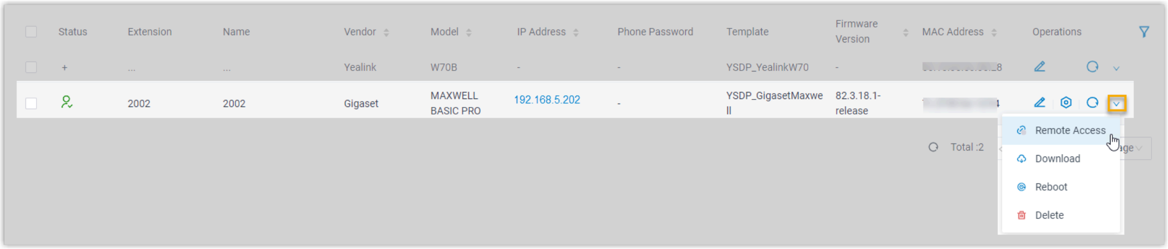
> **Tip:**
> To make sure of this, check if the private IP address of the IP phone / gateway is recognized and displayed in the Auto Provisioning device list.



□	Status	Extension	Name	Vendor	Model	IP Address	Phone Password	Template
□		2002	Tiffany Sandoval	Yealink	SIP-T53W	192.168.5.52	-	YSDP_YealinkT5

Remotely visit an IP phone on PBX

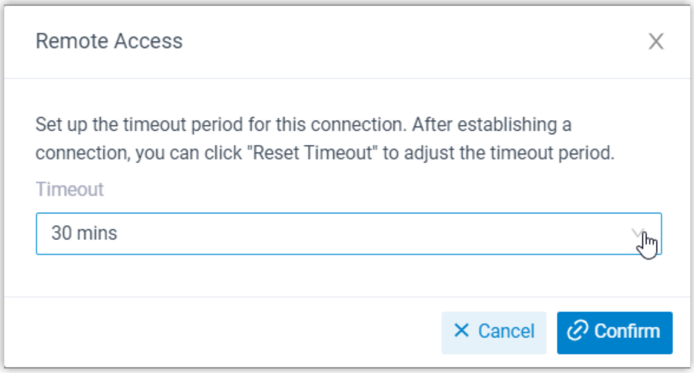
1. Log in to PBX web portal, go to Auto Provisioning > Phones.
2. Hover the mouse over ﹀ beside the desired phone, and click Remote Access.

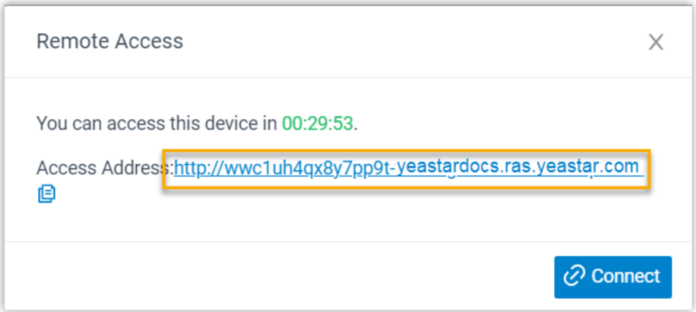
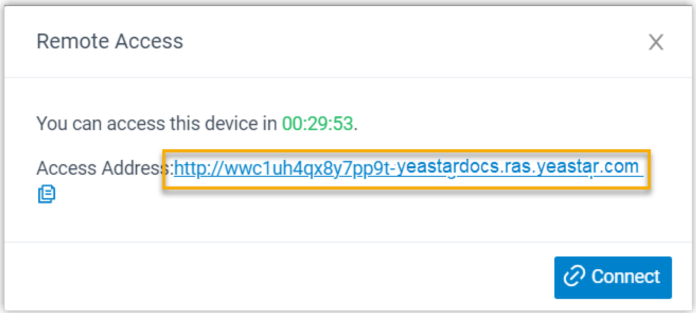


□	Status	Extension	Name	Vendor	Model	IP Address	Phone Password	Template	Firmware Version	MAC Address	Operations
□	+	...	...	Yealink	W70B	-	-	YSDP_YealinkW70	-	[redacted]	
□		2002	2002	Gigaset	MAXWELL BASIC PRO	192.168.5.202	-	YSDP_GigasetMaxwell	82.3.18.1-release	[redacted]	

3. Connect to the IP phone as the following instructions guide according to the method users visit the PBX.

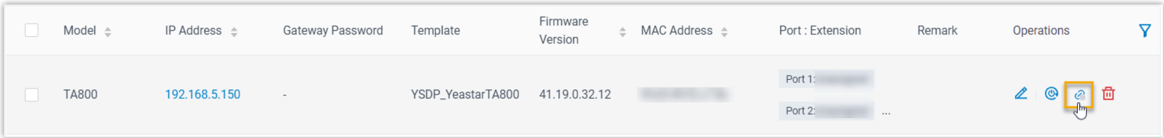
Table 19.

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.  Remote Access Set up the timeout period for this connection. After establishing a connection, you can click "Reset Timeout" to adjust the timeout period. Timeout: 30 mins ii. Click Confirm.

Method	Instruction
	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.  Remote Access You can access this device in 00:29:53. Access Address:http://wwc1uh4qx8y7pp9t-yeastardocs.ras.yeastar.com 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.  Remote Access You can access this device in 00:29:53. Access Address:http://wwc1uh4qx8y7pp9t-yeastardocs.ras.yeastar.com Click Connect to visit the IP phone web interface.

Remotely visit a gateway on PBX

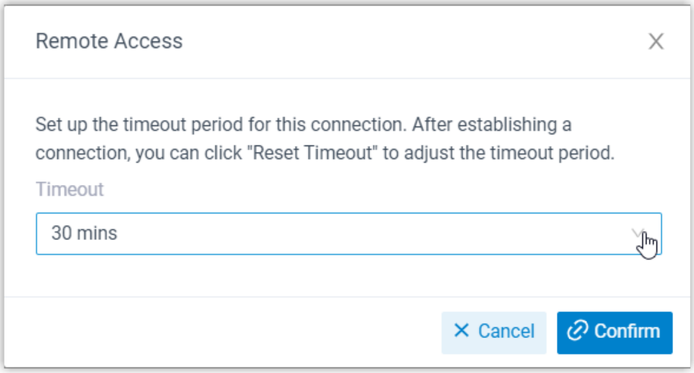
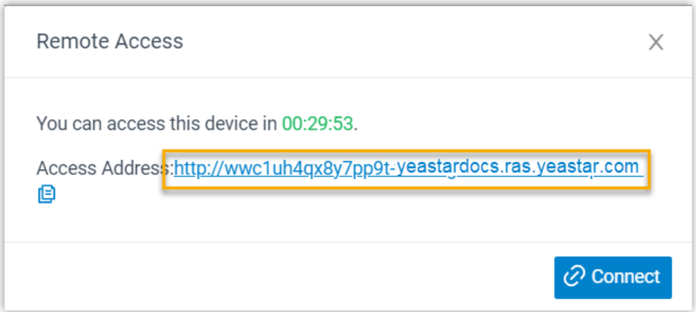
1. Log in to PBX web portal, go to Auto Provisioning > Gateways.
2. Click 🔗 beside the desired gateway.

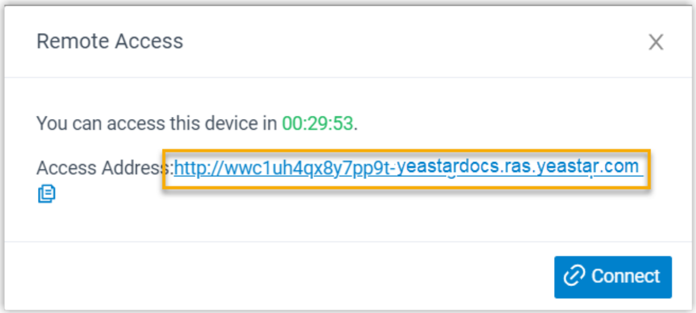


Model	IP Address	Gateway Password	Template	Firmware Version	MAC Address	Port : Extension	Remark	Operations
TA800	192.168.5.150	-	YSDP_YeastarTA800	41.19.0.32.12	[redacted]	Port 1: [redacted] Port 2: [redacted] ...		

3. Connect to the gateway as the following instructions guide according to the method users visit the PBX.

Table 20.

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.  Remote Access Set up the timeout period for this connection. After establishing a connection, you can click "Reset Timeout" to adjust the timeout period. Timeout: 30 mins 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 gateway is connected.  Remote Access You can access this device in 00:29:53. Access Address:http://wwc1uh4qx8y7pp9t-yeastardocs.ras.yeastar.com b. Click Connect to visit the gateway 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 gateway is connected.

Method	Instruction
	Note: In this case, the time limit of gateway remote access is synchronized with the remote management timeout of the PBX.  Remote Access You can access this device in 00:29:53. Access Address:http://wwc1uh4qx8y7pp9t-yeastardocs.ras.yeastar.com Click Connect to visit the gateway web interface.

FAQ

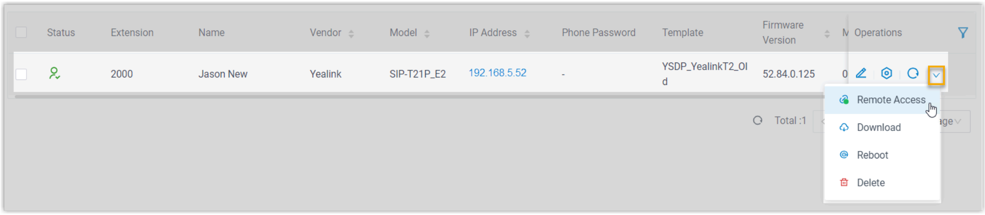
How to extend the IP phone / Gateway remote access time

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.

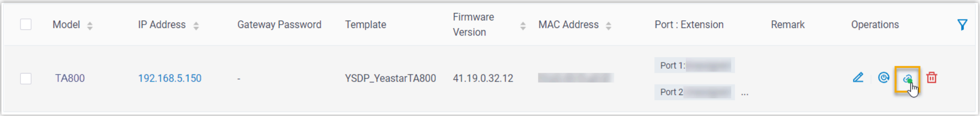
   IP Phone

Status	Extension	Name	Vendor	Model	IP Address	Phone Password	Template	Firmware Version	M	Operations
	2000	Jason New	Yealink	SIP-T21P_E2	192.168.5.52	-	YSDP_YealinkT2_Old	52.84.0.125	0	

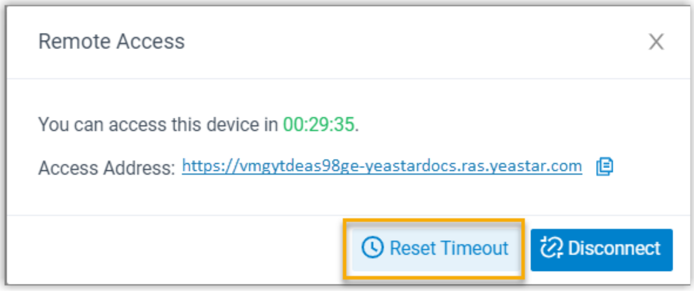
   Total :1

   Gateway



	Model	IP Address	Gateway Password	Template	Firmware Version	MAC Address	Port : Extension	Remark	Operations
□	TA800	192.168.5.150	-	YSDP_YeastarTA800	41.19.0.32.12	[redacted]	Port 1: [redacted] Port 2 [redacted] ...		

2. In the pop-up window, click Reset Timeout.

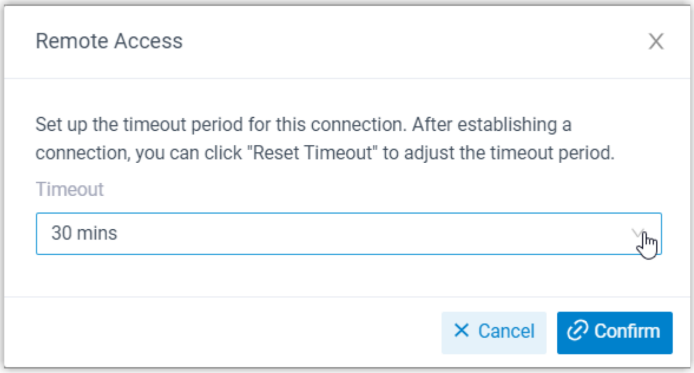


Remote Access

You can access this device in 00:29:35.

Access Address: https://vmgytdeas98ge-yeastardocs.ras.yeastar.com

3. Reset the Timeout and click Confirm



Remote Access

Set up the timeout period for this connection. After establishing a connection, you can click "Reset Timeout" to adjust the timeout period.

Timeout: 30 mins

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.

    > ℹ 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.

Auto Provisioning Options

IP Phone Auto Provisioning Options

Yeastar P-Series Software Edition 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)
- Reassign an Extension to a Provisioned IP Phone/Gateway

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 Software Edition 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.

Auto Provision Function Keys for Phones

Each extension user can set his or her own function keys, you can also set up for them. These function keys can be applied to auto-provisioned IP phones, Linkus Web Client, and Chrome extension 'Yeastar Linkus for Google'. 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 for IP phone. Note: The key type Line is only available for IP phones.
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. For more information about configuration, see Monitor Extension Status by BLF Key. • Trunk ◦ Monitor the status of a specific trunk. ◦ Place an outbound call through the monitored trunk.

Key type	Function
	For more information about configuration, see Seize a Trunk to Call Out by BLF Key. • Queue ◦ Monitor specific pause status of a queue agent. For more information about configuration, see Monitor Specific Pause Status of an Agent by Function Key.
Speed Dial	Place a call to the most commonly dialed numbers or extensions.
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 on IP phones. Note: The key type LDAP Directory is only available for IP phones.

Supported methods

You can provision function keys for user's IP phone either using an auto provisioning template or by setting them up directly on PBX web portal.

- To provision function keys using a template, see Create an custom Auto Provisioning template and Apply a new template to a provisioned IP phone.
- To provision function keys on PBX web portal, see the instructions below.

Procedure

1. Assign function keys for extension users.
   1. 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.
   2. Click the Function Keys tab.
   3. 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 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.

      - Type: Select a key type.
      - Value: Configure a desired value based on the key type, such as parking number, queue, or extension.
      - Label: Optional. Enter a value, which will be displayed on the phone screen.
   4. 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 extensions have been associated with phones, reprovision the phones to take effect.
   1. Go to Auto Provisioning > Phones.
   2. To reprovision a phone, click ⟳ beside the phone assigned to this extension user.
   3. To reprovision multiple phones, select the checkboxes of the desired phones, click Reprovision.

Result

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

Related information

Auto Provision Yealink Expansion Module with Yeastar P-Series Software Edition

Synchronize Phone Time with Yeastar P-Series Software Edition via Auto Provisioning

You can synchronize the time of the provisioned phone with Yeastar P-Series Software Edition via Auto Provisioning feature.

Prerequisites

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

For more information, see the following topics:

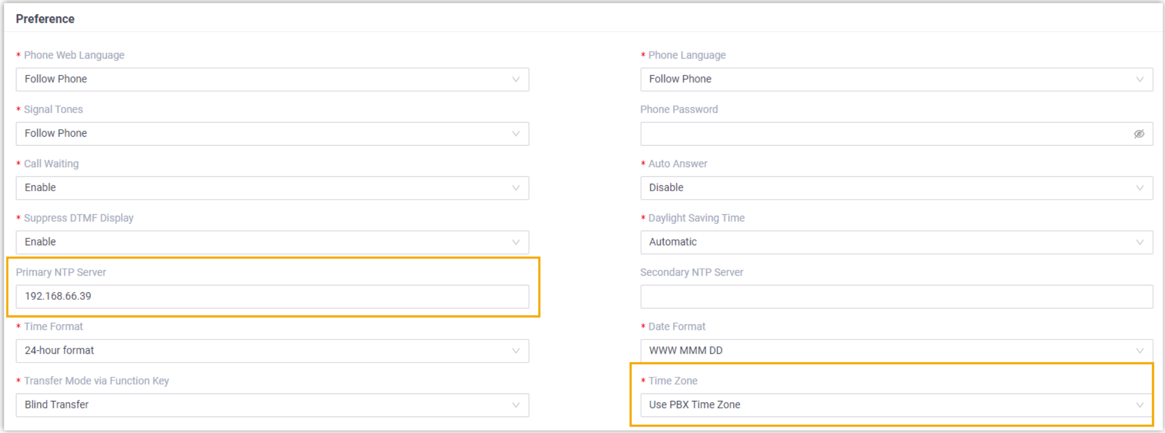
- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

Procedure

- Step1. Set up PBX as NTP Server
- Step2. Apply the configuration to IP phone

Step1. 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.



Preference

* Phone Web Language	Follow Phone	* Phone Language	Follow Phone
* Signal Tones	Follow Phone	Phone Password	
* Call Waiting	Enable	* Auto Answer	Disable
* Suppress DTMF Display	Enable	* Daylight Saving Time	Automatic
Primary NTP Server	192.168.66.39	Secondary NTP Server	
* Time Format	24-hour format	* Date Format	WWW MMM DD
* Transfer Mode via Function Key	Blind Transfer	* Time Zone	Use PBX Time Zone

   - Primary NTP Server: Set the value as the IP address of your PBX.
   - Time Zone: Select Use PBX Time Zone.
4. Click Save.

Step2. 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 Software Edition provides various default templates for each supported device. Devices of different models may share the same template. For example, the template `YSDP_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.

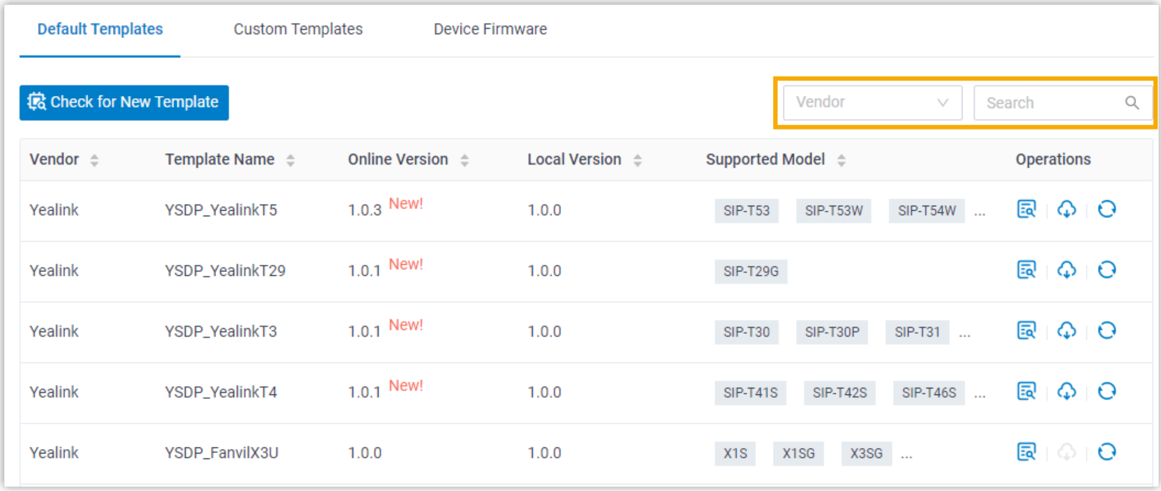
- Absolute value: Absolute is a fixed value that applies to all devices that use this template. For example, `features.dtmf.hide_delay = 1` means setting the parameter value to 1 (Enabled).

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.

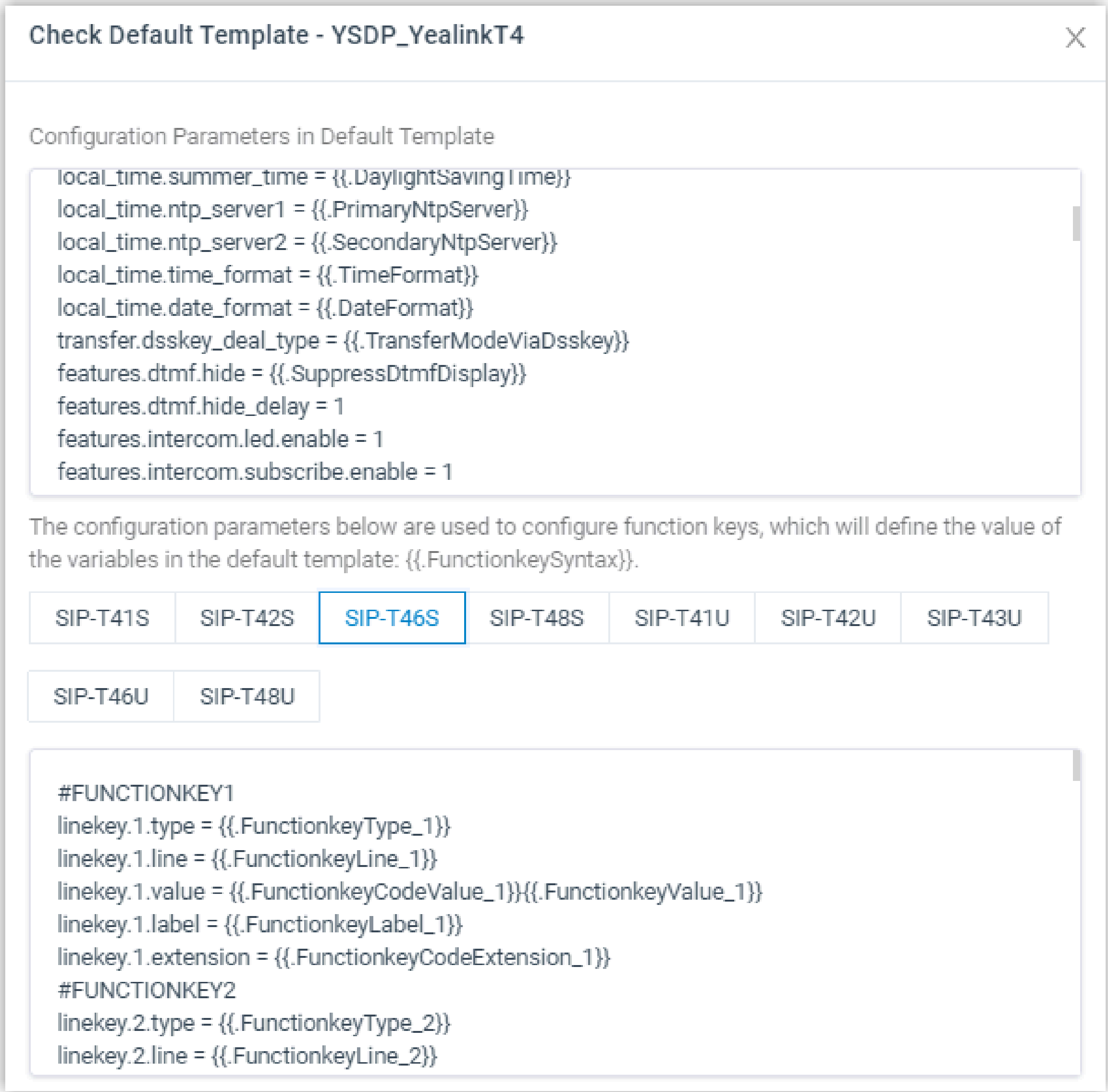
   The search results are displayed automatically on the web page.



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

3. Click 🔍 beside the desired template to view the default configurations.
   The following figure shows a default template of Yealink T56A. The default template consists of two parts:
   - Configuration parameters in Default Template: The pre-defined configuration parameters in this template are displayed in the first text box.
   - Function keys of device model: The pre-defined function keys supported by the device model are displayed in the second text box.

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


Check Default Template - YSDP_YealinkT4
Configuration Parameters in Default Template

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

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

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

Related information

- Create a Custom Auto Provisioning Template
- Manage Custom Auto Provisioning Templates

Update a Default Auto Provisioning Template

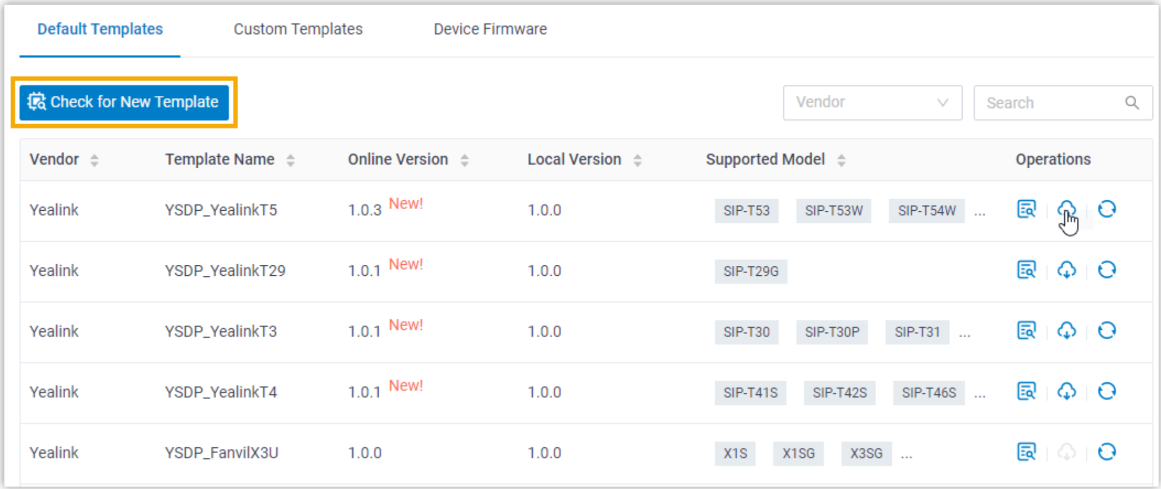
Yeastar P-Series Software Edition regularly provides new template versions to release new features and fix bugs. You can check if a new template is available, and decide whether to update the default template. This topic describes how to update a default template.

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.



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

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

   For more information, see View a Default Auto Provisioning Template.

What to do next

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

Create a Custom Auto Provisioning Template

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

Background information

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

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

Create an advanced Auto Provisioning template

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

1. Log in to PBX 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, and Codecs sections; A text box containing all configuration parameters will be displayed in the Customize Configuration Parameters In Text section.
    - Remark: Optional. Enter a short description about this template.
4. In the Preference section, modify the preference settings that are provided by the source default template.
5. In the Codecs section, select a desired codec according to your needs.
6. Add additional parameters that are not provided by the source default template.

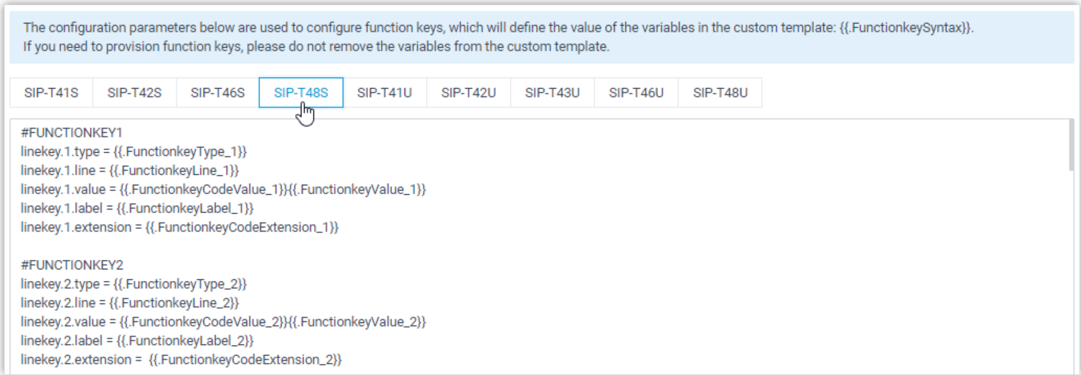
> Note:
>
> The general settings defined in source default template are assigned with variables. The variable that starts with `{{.` and ends with `}}` is associated with the configuration that can be configured on Preference, Codecs, and Function Keys sections. Please don't change the variable if you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



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

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

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

7. Click Save.

Related information

Edit a custom Auto Provisioning template

Update Auto Provisioning template(s) to all applicable devices

Manage Custom Auto Provisioning 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.

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

You can upload up to three 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 Software Edition.

Yealink phones

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
SIP-T19P_E2	53.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T21P_E2	52.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T21_E2	52.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T23P	44.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T23G	44.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS
SIP-T27G	69.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T29G	46.83.0.120 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T30	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T30P	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T31	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T31P	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T31G	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T33P	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T33G	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T40P	54.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T40G	76.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T41P	36.83.0.120 or later	83.4.0.17 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS
SIP-T42G	29.83.0.120 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T46G	28.83.0.120 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T48G	35.83.0.120 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T41S	66.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T42S	66.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T46S	66.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T48S	66.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T41U	108.85.0.39 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T42U	108.85.0.39 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T43U	108.85.0.39 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T46U	108.85.0.39 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T48U	108.85.0.39 or later	83.4.0.17 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS
SIP-T52S	70.84.0.70 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T54S	70.84.0.70 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T53	96.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T53W	96.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T54W	96.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T57W	96.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T56A	58.83.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T58	58.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
SIP-T58W	150.86.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
VP59	91.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
W80B	W80DM-103.83.0.80	83.4.0.17 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
W60B (W53P, W41P, W60P, CP930W-Base)	77.83.0.85 or later	83.4.0.17 or later	• PnP • DHCP • RPS
W70B (W79P, W76P, W73P)	146.85.0.20 or later	83.4.0.17 or later	• PnP • DHCP • RPS
W90DM	130.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS
CP960	73.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
CP965	143.86.0.5 or later	83.5.0.9 or later	• PnP • DHCP • RPS
CP920	78.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
CP925	148.86.0.5 or later	83.5.0.9 or later	• PnP • DHCP • RPS
SIP-CP935W	149.86.0.5 or later	83.5.0.9 or later	• PnP • DHCP • RPS

Fanvil phones

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
X1S / X1SP	2.2.12 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X1SG	2.2.12 or later	83.4.0.17 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
X3SG	2.2.12 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X3U	2.2.12 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X2/X2P	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X2C/X2CP	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X3S/X3SP/X3G	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X4/X4G	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X2/X2P	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X2C/X2CP	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X3S/X3SP/X3G	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X4/X4G	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X4U	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X4U-V2	2.12.1 or later	83.6.0.24 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
X5U	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X5U-V2	2.12.1 or later	83.6.0.24 or later	• PnP • DHCP • RPS
X5S	2.2.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X6	2.2.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X6U	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X6U-V2	2.12.1 or later	83.6.0.24 or later	• PnP • DHCP • RPS
X7	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X7C	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X7A	2.2.0.229 or later	83.4.0.17 or later	• PnP • DHCP • RPS
A32	2.6.0.408 or later	83.4.0.17 or later	• PnP • DHCP • RPS
A32i	2.6.0.408 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X210	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
X210i	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X7-V2	2.12.1.3 or later	83.7.0.16 or later	• PnP • DHCP • RPS
X7C-V2	2.12.1.3 or later	83.7.0.16 or later	• PnP • DHCP • RPS
X210-V2	2.12.1.3 or later	83.7.0.16 or later	• PnP • DHCP • RPS
X210i-V2	2.12.1.3 or later	83.7.0.16 or later	• PnP • DHCP • RPS
V65	2.12.2.4 or later	83.7.0.16 or later	• PnP • DHCP • RPS
X3S Lite / X3SP Lite	2.4.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X3S Pro / X3SP Pro	2.4.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X3SW	2.4.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X3SG Lite	2.4.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X3SG Pro	2.4.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS
X3U Pro	2.4.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
V62	2.4.10 or later	83.6.0.24 or later	• PnP • DHCP • RPS
V64	2.4.10 or later	83.6.0.24 or later	• PnP • DHCP • RPS
V67	2.6.0 or later	83.6.0.24 or later	• PnP • DHCP • RPS
FH-S01	2.12.8 or later	83.9.0.20 or later	• PnP • DHCP • RPS
H3	2.12.1.7334 or later	83.4.0.17 or later	• PnP • DHCP • RPS
H5	2.12.1.7334 or later	83.4.0.17 or later	• PnP • DHCP • RPS
H2U	2.4.7 or later	83.4.0.17 or later	• PnP • DHCP • RPS
H2U-V2	2.4.7.6 or later	83.4.0.17 or later	• PnP • DHCP • RPS
H3W	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS
H5W	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i56A	0.3.0.21 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i55A	1.0.0.45 or later	83.8.0.25 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
i57A	1.0.0.46 or later	83.8.0.25 or later	• PnP • DHCP • RPS
i51	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i52	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i53	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i51W	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i52W	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i53W	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i10	1.2.7 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i10V	1.2.7 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i10D	1.2.7 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i10S	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i10SV	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
i10SD	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i11S	1.2.7 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i11SV	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i12	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i16V	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i16S	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i16SV	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i18S	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i20S	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i23S	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i30	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i31S	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
i32V	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i33V	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i33VF	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i61	2.4.0 or later	83.6.0.24 or later	• PnP • DHCP • RPS
i62	2.4.0 or later	83.6.0.24 or later	• PnP • DHCP • RPS
i63	2.4.0 or later	83.6.0.24 or later	• PnP • DHCP • RPS
i64	2.4.0 or later	83.6.0.24 or later	• PnP • DHCP • RPS
PA2	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS
PA2S	2.8.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS
PA3	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS
i68	2.8.40.22 or later	83.8.0.25 or later	• PnP • DHCP • RPS
X301	0.0.16 or later	83.8.0.25 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
X303	0.0.16 or later	83.8.0.25 or later	• PnP • DHCP • RPS
X301G	0.0.16 or later	83.8.0.25 or later	• PnP • DHCP • RPS
X303G	0.0.16 or later	83.8.0.25 or later	• PnP • DHCP • RPS
X301W	0.0.16 or later	83.8.0.25 or later	• PnP • DHCP • RPS
X303W	0.0.16 or later	83.8.0.25 or later	• PnP • DHCP • RPS
W611W	pvt-2.8 or later	83.8.0.25 or later	• PnP • DHCP • RPS

Grandstream phones

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
GXP1610	1.0.7.13 or later	83.4.0.17 or later	• PnP • DHCP
GXP1620	1.0.7.13 or later	83.4.0.17 or later	• PnP • DHCP
GXP1625	1.0.7.13 or later	83.4.0.17 or later	• PnP • DHCP
GXP1628	1.0.7.13 or later	83.4.0.17 or later	• PnP • DHCP
GXP1630	1.0.7.13 or later	83.4.0.17 or later	• PnP • DHCP
GXP2130	1.0.11.16 or later	83.4.0.17 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP
GXP2135	1.0.11.16 or later	83.4.0.17 or later	• PnP • DHCP
GXP2140	1.0.11.16 or later	83.4.0.17 or later	• PnP • DHCP
GXP2160	1.0.11.16 or later	83.4.0.17 or later	• PnP • DHCP
GXP2170	1.0.11.16 or later	83.4.0.17 or later	• PnP • DHCP
GRP2601	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP
GRP2601P	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP
GRP2602	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP
GRP2602P	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP
GRP2602G	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP
GRP2602W	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP
GRP2603	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP
GRP2603P	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP
GRP2604	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP
GRP2604P	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP
GRP2612	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP
GRP2612P	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
GRP2612G	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP
GRP2612W	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP
GRP2613	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP
GRP2614	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP
GRP2615	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP
GRP2616	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP
GRP2624	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP
GRP2634	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP
GRP2670	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP

Htek phones

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
UC902	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC902S	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC903	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC912	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS
UC912G	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC912E	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC921	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC921G	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC923	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC923U	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC924	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC924E	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC924U	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC924W	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC926	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS
UC926E	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS
UC926U	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS

Gigaset phones

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
N870 IP PRO	2.38.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS
N870 VI PRO	2.38.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS
N670 IP PRO	2.38.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS
N610 IP PRO (Coming soon)	N/A	83.4.0.17 or later	• PnP • DHCP • RPS
Maxwell Basic PRO	3.18.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS
Maxwell 2 PRO	3.18.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS
Maxwell 3 PRO	3.18.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS
Maxwell 4 PRO	3.18.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS

Snom phones

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
D120	10.1.54.13 or later	83.4.0.17 or later	• PnP • RPS
D315	10.1.73.16 or later	83.4.0.17 or later	• PnP • RPS
D335	10.1.73.16 or later	83.4.0.17 or later	• PnP • RPS
D385	10.1.73.16 or later	83.4.0.17 or later	• PnP • RPS
D713	10.1.73.16 or later	83.6.0.46 or later	• PnP • RPS
D717	10.1.73.16 or later	83.4.0.17 or later	• PnP • RPS
D735	10.1.73.16 or later	83.4.0.17 or later	• PnP • RPS
D785	10.1.73.16 or later	83.4.0.17 or later	• PnP • RPS
D862	10.1.137.15 or later	83.9.0.22 or later	• PnP • RPS
D865	10.1.137.15 or later	83.9.0.22 or later	• PnP • RPS
M300	BSV530B2 or later	83.8.0.25 or later	• PnP • RPS
M400	BSV610B5 or later	83.8.0.25 or later	• PnP • RPS
M900	BSV530B7 or later	83.8.0.25 or later	• PnP • RPS

Flyingvoice phones

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
FIP10	0.7.23.1 or later	83.8.0.25 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS
FIP11C	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS
FIP12WP	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS
FIP13G	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS
FIP14G	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS
FIP15G	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS
FIP15G Plus	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS
FIP16	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS
FIP16 Plus	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS
P10	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P10P	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P10G	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P10W	V0.7.56 or later	83.9.0.20 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS
P10LTE	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P11	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P11P	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P11G	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P11W	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P11LTE	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P20	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P20P	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P20W	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P20G	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P21	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P21P	V0.7.57 or later	83.9.0.20 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS
P21W	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
flyphone	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P22P	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P22G	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P23G	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P23GW	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
P24G	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS
i86Box_Basic	V0.0.16.1 or later	83.9.0.20 or later	• PnP • DHCP • RPS
i86Box_Indoor	V0.0.16.1 or later	83.9.0.20 or later	• PnP • DHCP • RPS
i86Box_2Line	V0.0.16.1 or later	83.9.0.20 or later	• PnP • DHCP • RPS
i86Box_PCBA	V0.0.16.1 or later	83.9.0.20 or later	• PnP • DHCP • RPS
i86Box_NFC	V0.0.16.1 or later	83.9.0.20 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS

Alcatel-Lucent Enterprise phones

Table 21.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
H2	2.10.00.0001083 or later	83.6.0.24 or later	• PnP • DHCP
H2P	2.10.00.0001083 or later	83.6.0.24 or later	• PnP • DHCP
H3P	22.12.43.010.2272 or later	83.5.0.9 or later	• PnP • DHCP
H3G	22.12.43.010.2272 or later	83.5.0.9 or later	• PnP • DHCP
H6	2.12.43.010.2272 or later	83.5.0.9 or later	• PnP • DHCP
M3	22.13.37.000.2202 or later	83.5.0.9 or later	• PnP • DHCP
M5	2.13.37.000.2202 or later	83.5.0.9 or later	• PnP • DHCP
M7	2.13.37.000.2202 or later	83.5.0.9 or later	• PnP • DHCP
M8	2.13.32.000.1535 or later	83.6.0.24 or later	• PnP • DHCP

Tiptel phones

Table 22.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
3310	2.42.6.5.55 or later	83.7.0.16 or later	• PnP

Table 22. (continued)

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS
3320	2.42.6.5.55 or later	83.7.0.16 or later	• PnP • DHCP • RPS
3330	2.42.6.5.55 or later	83.7.0.16 or later	• PnP • DHCP • RPS
3340	2.42.6.5.55 or later	83.7.0.16 or later	• PnP • DHCP • RPS

Dinstar phones

Table 23.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
C60S	2.60.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP
C60L	2.60.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP
C60U	2.60.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP
C61S	2.61.6.7.0/2.61.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP
C62S	2.62.6.7.0/2.62.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP
C62G	2.62.6.7.0/2.62.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP
C63S	2.63.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP
C63G	2.63.6.7.0/2.63.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP

Table 23. (continued)

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
C64G	2.64.6.7.0 or later	83.6.0.24 or later	• PnP • DHCP
C66G	2.66.6.7.0 or later	83.6.0.24 or later	• PnP • DHCP

Mitel phones

Table 24.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
6863i	R5.1.0SP6 or later	83.9.0.103 or later	• DHCP
6865i	R5.1.0SP6 or later	83.9.0.103 or later	• DHCP
6867i	R5.1.0SP6 or later	83.9.0.103 or later	• DHCP
6869i	R5.1.0SP6 or later	83.9.0.103 or later	• DHCP
6873i	R5.1.0SP6 or later	83.9.0.103 or later	• DHCP
6920	6.3.1 SP1 or later	83.9.0.103 or later	• DHCP
6930	6.3.1 SP1 or later	83.9.0.103 or later	• DHCP
6940	6.3.1 SP1 or later	83.9.0.103 or later	• DHCP

Yeastar gateways

Model	Gateway Firmware	PBX Requirement	Supported Auto Provisioning Method
TA100	44.19.86.30 or later	83.4.0.17 or later	• PnP • DHCP
TA200	44.19.86.30 or later	83.4.0.17 or later	• PnP • DHCP
TA400	41.19.0.32 or later	83.4.0.17 or later	• PnP • DHCP
TA800	41.19.0.32 or later	83.4.0.17 or later	• PnP

Model	Gateway Firmware	PBX Requirement	Supported Auto Provisioning Method
			• DHCP
TA1600	47.0.0.54 or later	83.4.0.17 or later	• PnP • DHCP
TA2400	47.0.0.54 or later	83.4.0.17 or later	• PnP • DHCP
TA3200	47.0.0.54 or later	83.4.0.17 or later	• PnP • DHCP

Auto Provisioning - Variables in Templates

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

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

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

Variable	Description
{{.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.
{{.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.

Variable	Description
{{.TemplateServerPortx}}	The port of PBX server for extension registration.
{{.AcountSipServerTemplate}}	The type of transport protocol for extension registration.
Audio codec(x is the codec priority, X=1, 2, 3 or 4)	
{{.AccountAudioCodec_X}}	The priority of the audio codec.
{{.AudioCodecsPriorities}}	The priority of the audio codec.
{{.AccountCodecPcmu}}	Enable or disable PCMU audio codec.
{{.AccountCodecPcmu_Priority}}	The priority of the PCMU audio codec.
{{.AccountCodecPcma}}	Enable or disable PCMA audio codec.
{{.AccountCodecPcma_Priority}}	The priority of the PCMA audio codec.
{{.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.

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

Variable	Description
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.
{{.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.

Variable	Description
{{.LanSubnetMask}}	The subnet mask of LAN port.
{{.LanGateway}}	The gateway of LAN Port.
{{.LanPrimaryDns}}	The primary DNS of LAN port.
{{.LanSecondaryDns}}	The secondary DNS of LAN Port.
{{.LanIpAddress2}}	The secondary IP address of LAN port.
{{.LanSubnetMask2}}	The secondary subnet mask of LAN port.
{{.PppoeUsername}}	The user name of PPPoE.
{{.PppoePassword}}	The password of PPPoE.
Others	
{{.MacAddress}}	The MAC address of phone. Note: Here the value does not need a separator of `:`. For example, `09139876900e`.

Auto Provisioning Example

Auto Provision Yealink DECT Phones with Yeastar P-Series Software Edition

This topic describes how to provision Yealink DECT base and DECT handsets with Yeastar P-Series Software Edition in the local network.

Supported phone models

Check the supported devices and device firmwares in Auto Provisioning - Supported Devices.

This topic takes the following Yealink devices as an example:

Device Model	Firmware Version
Yealink DECT base	
Yealink W70B	146.85.0.20
Yealink DECT handset	

Device Model	Firmware Version
Yealink W73H	116.85.254.20

Prerequisites

Make sure that a DHCP Server is enabled in your local network to assign an IP address to the DECT base.

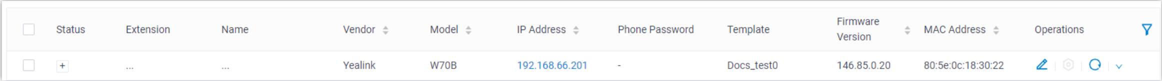
Procedure

- Step1. Provision the DECT base
- Step2. Register the DECT handset

Step1. Provision the DECT base

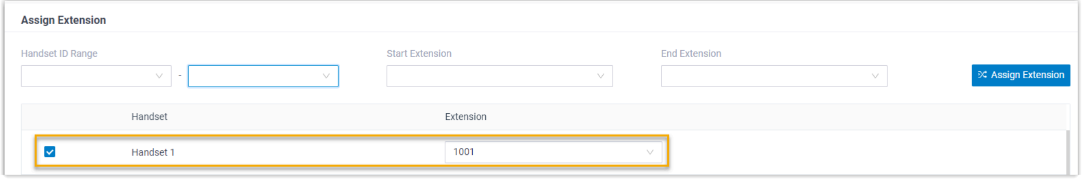
1. Power on PBX first, then power on the DECT base.
2. Log in to PBX web portal, go to Auto Provisioning > Phones.

   The DECT base is detected.



□	Status	Extension	Name	Vendor	Model	IP Address	Phone Password	Template	Firmware Version	MAC Address	Operations
□	+	...	...	Yealink	W70B	192.168.66.201	-	Docs_test0	146.85.0.20	80:5e:0c:18:30:22	

3. Click to edit the desired DECT base.
   a. In the Options section, select a desired template from the Template drop-down list.
   b. In the Assign Extension section, assign an extension for the DECT handset.



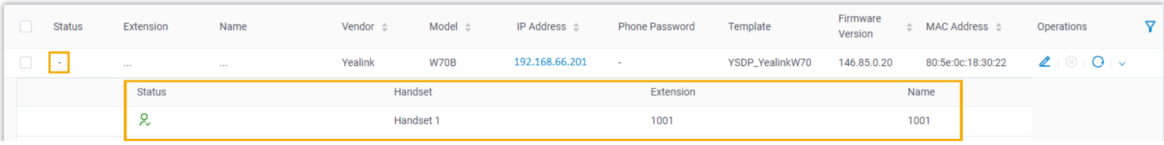
Assign Extension

Handset ID Range · Start Extension · End Extension · Assign Extension

	Handset	Extension
☑	Handset 1	1001

   c. Configure other settings according to your needs.
4. Click Save.

   The handset is listed under the DECT base.

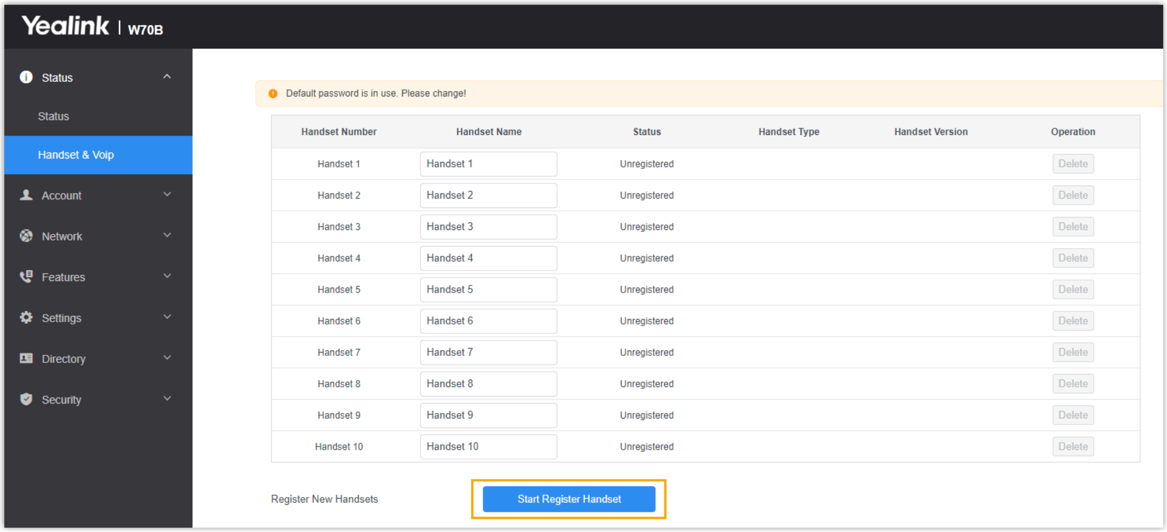


□	Status	Extension	Name	Vendor	Model	IP Address	Phone Password	Template	Firmware Version	MAC Address	Operations
□	-	...	...	Yealink	W70B	192.168.66.201	-	YSDP_YealinkW70	146.85.0.20	80:5e:0c:18:30:22	

Status	Handset	Extension	Name
✓	Handset 1	1001	1001

Step2. Register the DECT handset

1. Click on the IP address beside the DECT base to log in to the DECT base web interface.
2. Go to Status > Handset & Voip to register the handset.
3. In the Register New Handsets section, click Start Register Handset.



Default password is in use. Please change!

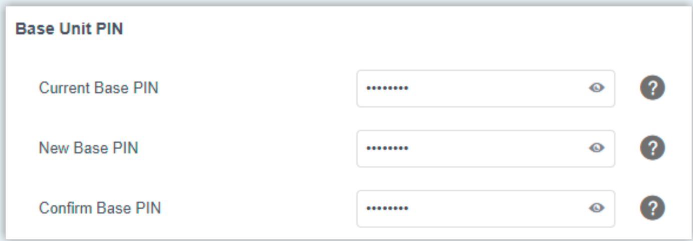
Handset Number	Handset Name	Status	Handset Type	Handset Version	Operation
Handset 1	Handset 1	Unregistered			Delete
Handset 2	Handset 2	Unregistered			Delete
Handset 3	Handset 3	Unregistered			Delete
Handset 4	Handset 4	Unregistered			Delete
Handset 5	Handset 5	Unregistered			Delete
Handset 6	Handset 6	Unregistered			Delete
Handset 7	Handset 7	Unregistered			Delete
Handset 8	Handset 8	Unregistered			Delete
Handset 9	Handset 9	Unregistered			Delete
Handset 10	Handset 10	Unregistered			Delete

Register New Handsets

4. Confirm registration on DECT handset.
   a. On the handset, press OK > Settings > Registration > Register Handset > OK.

      The handset starts to search for a DECT base, and displays the MAC address of the detected DECT base.
   b. Press OK.

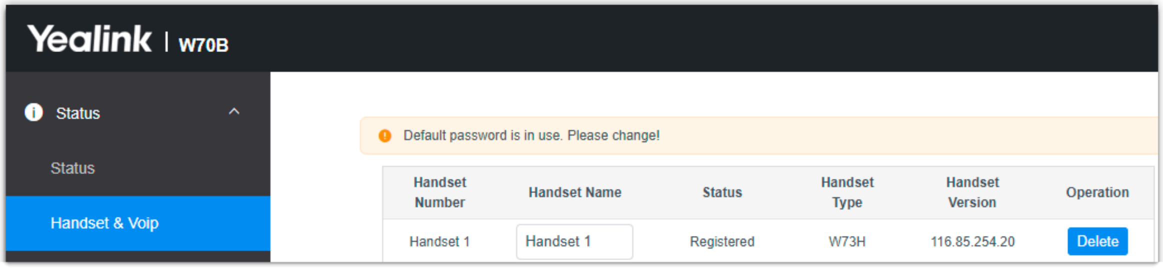
      You are requested to enter the PIN of the DECT base.
   c. Enter the PIN code, and press Done.

> Note:
>
> The default PIN is `0000`. You can change the PIN on the DECT base web interface (Path: Security > Base PIN).
>
> 
>
> **Base Unit PIN**
>
> | | |
> |---|---|
> | Current Base PIN | •••••••• |
> | New Base PIN | •••••••• |
> | Confirm Base PIN | •••••••• |

The handset prompts Handset Subscribed, indicating the handset is successfully registered.

Result

- You can manage the handset on the DECT base web interface.



Default password is in use. Please change!

Handset Number	Handset Name	Status	Handset Type	Handset Version	Operation
Handset 1	Handset 1	Registered	W73H	116.85.254.20	Delete

- You can use the handset as an extension to make and receive calls.

Auto Provision Yealink Expansion Module with Yeastar P-Series Software Edition

This topic takes Yealink T53W as an example to describe how to provision Yealink expansion module with Yeastar P-Series Software Edition, so as to add extra programmable keys.

Requirements

Refer to the table below to learn about the supported Yealink IP phone models for different expansion modules, as well as the required phone provisioning templates.

Expansion Module	Phone model	Phone provisioning template
EXP40	T46S, T48S	YSDP_YealinkT4 (`1.0.5` or later)
	T46G, T48G	YSDP_YealinkT4xG (`1.0.4` or later)
EXP43	T43U, T46U, T48U	YSDP_YealinkT4 (`1.0.5` or later)
EXP50	SIP-T53, SIP-T53W, SIP-T54W, SIP-T57W	YSDP_YealinkT5 (`1.0.5` or later)
	SIP-T56A	YSDP_YealinkT56 (`1.0.5` or later)
	SIP-T58, SIP-T58W	YSDP_YealinkT58 (`1.0.5` or later)

Prerequisites

- The Yealink expansion module is connected to a Yealink IP phone.
- The Yealink IP phone is connected to Yeastar P-Series Software Edition via Auto Provisioning, and has been assigned with an extension.
  For more information about auto provisioning an IP phone, 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)

Supported methods

- Provision function keys for Yealink expansion module via web interface
- Provision function keys for Yealink expansion module using auto provisioning template

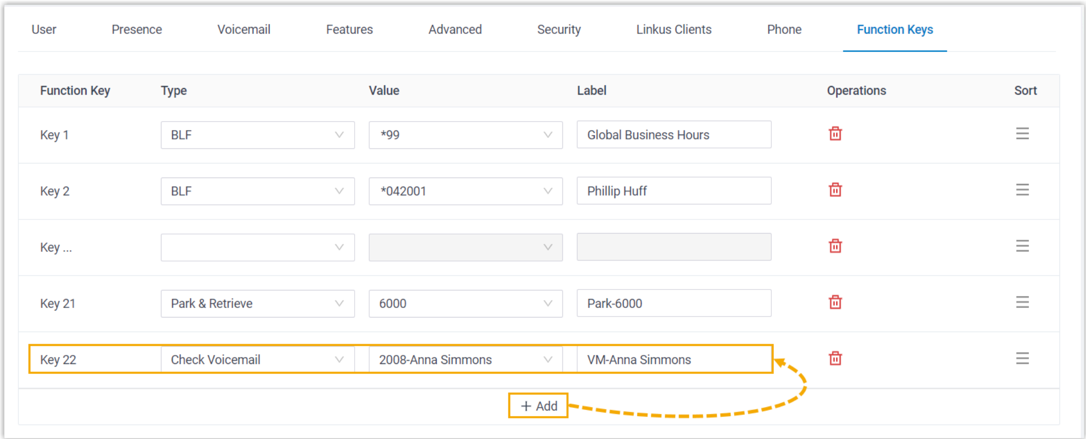
Provision function keys for Yealink expansion module via web interface

On PBX web portal, you can easily customize function keys by directly selecting key types from the menu and setting up specific operation for each function key.

> Note:
> Yeastar P-Series Software Edition supports to add up to 120 function keys on PBX web portal.

1. Add and configure function keys.
   a. Log in to PBX web portal, go to Extension and Trunk > Extension, edit the desired extension.
   b. Click Function Keys tab.
   c. Click Add to add and configure function keys for the expansion module.

   > Note:
   > Function key settings that exceed the supported programmable keys of the IP phone will be automatically applied to the connected expansion module. For example, Yealink T53W supports 21 programmable keys, then the function key settings starting from the 22nd key will take effect on the expansion module.



Function Key	Type	Value	Label	Operations	Sort
Key 1	BLF	*99	Global Business Hours	🗑	≡
Key 2	BLF	*042001	Phillip Huff	🗑	≡
Key ...				🗑	≡
Key 21	Park & Retrieve	6000	Park-6000	🗑	≡
Key 22	Check Voicemail	2008-Anna Simmons	VM-Anna Simmons	🗑	≡

- Type: Select a key type.

        - Value: Configure a desired value based on the key type.
        - Label: Optional. Enter a label, which will be displayed on the LCD screen.
    d. Click Save.
2. Reprovision the IP phone.
    a. On PBX web portal, go to Auto Provisioning > Phones.
    b. Click ⟳ beside the phone.
    c. In the pop-up window, click OK.

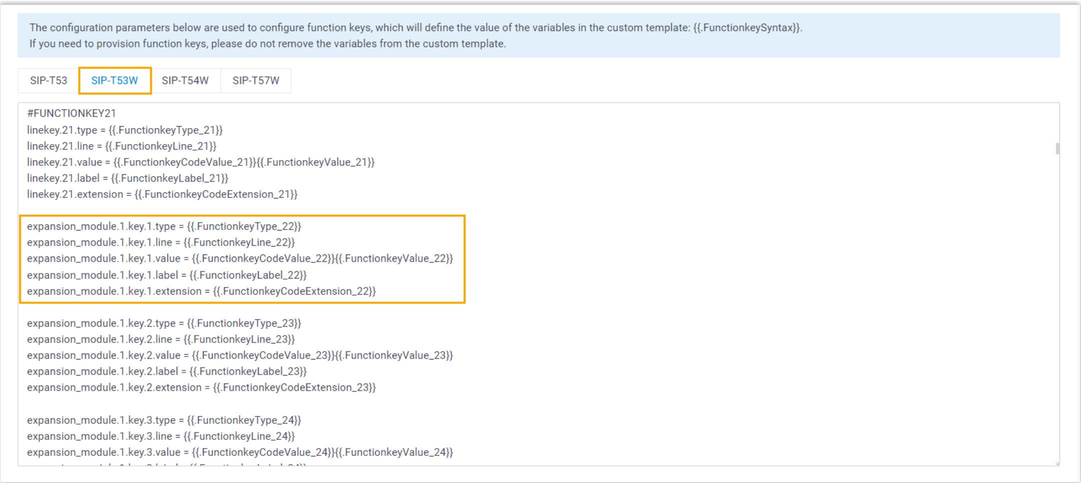
Provision function keys for Yealink expansion module using auto provisioning template

If you are familiar with the configuration parameters of IP phone, you can bulk configure function keys in a template file, via which the function key settings will be applied on the phone and expansion module automatically, thus saving time and effort.

> Important:
>
> As custom auto provisioning template is created based on the default phone provisioning template, make sure that you have updated the default template of the desired phone model to the required version on PBX (Path: Auto Provisioning > Resource Repository > Default Templates).

1. Create a custom auto provisioning template.
    a. Log in to PBX web portal, go to Auto Provisioning > Resource Repository > Custom Templates.
    b. Click Add.
    c. In the Basic section, set the basic information.
        - Template Name: Enter a name to help you identify the template.
        - Source Default Template: Search and select the default template of the phone model. In this example, select YSDP_YealinkT5.
        - Template Type: Select Advanced.
        - Remark: Optional. Add a note for the template.
    d. Optional: In the Preference, Distinctive Ringtone, Codecs, and LDAP Directory sections, configure the settings according to your needs.
    e. In the second text box of the Customize Configuration Parameters in Text section, select the specific phone model, then refer to specific IP phone's configuration parameter explanations to add function key settings for the expansion module.

    > Note:
    >
    > Function key settings that exceed the supported programmable keys of the IP phone will be automatically applied to the connected expansion module. For example, Yealink T53W supports 21 programmable keys, then the function key settings starting from the 22nd key will take effect on the expansion module.



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

```
#FUNCTIONKEY21
linekey.21.type = {{.FunctionkeyType_21}}
linekey.21.line = {{.FunctionkeyLine_21}}
linekey.21.value = {{.FunctionkeyCodeValue_21}}{{.FunctionkeyValue_21}}
linekey.21.label = {{.FunctionkeyLabel_21}}
linekey.21.extension = {{.FunctionkeyCodeExtension_21}}

expansion_module.1.key.1.type = {{.FunctionkeyType_22}}
expansion_module.1.key.1.line = {{.FunctionkeyLine_22}}
expansion_module.1.key.1.value = {{.FunctionkeyCodeValue_22}}{{.FunctionkeyValue_22}}
expansion_module.1.key.1.label = {{.FunctionkeyLabel_22}}
expansion_module.1.key.1.extension = {{.FunctionkeyCodeExtension_22}}

expansion_module.1.key.2.type = {{.FunctionkeyType_23}}
expansion_module.1.key.2.line = {{.FunctionkeyLine_23}}
expansion_module.1.key.2.value = {{.FunctionkeyCodeValue_23}}{{.FunctionkeyValue_23}}
expansion_module.1.key.2.label = {{.FunctionkeyLabel_23}}
expansion_module.1.key.2.extension = {{.FunctionkeyCodeExtension_23}}

expansion_module.1.key.3.type = {{.FunctionkeyType_24}}
expansion_module.1.key.3.line = {{.FunctionkeyLine_24}}
expansion_module.1.key.3.value = {{.FunctionkeyCodeValue_24}}{{.FunctionkeyValue_24}}
```

2. Apply the template to the phone.
    a. On PBX web portal, go to Auto Provisioning > Phones, edit the desired phone.
    b. In the Options section, select the template from the Template drop-down list.
    c. Click Save.
3. Reprovision the IP phone.
    a. On PBX web portal, go to Auto Provisioning > Phones.
    b. Click ↻ beside the phone.
    c. In the pop-up window, click OK.

User Role

User Roles and Permissions

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

Table 25.

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.

Table 25. (continued)

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

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

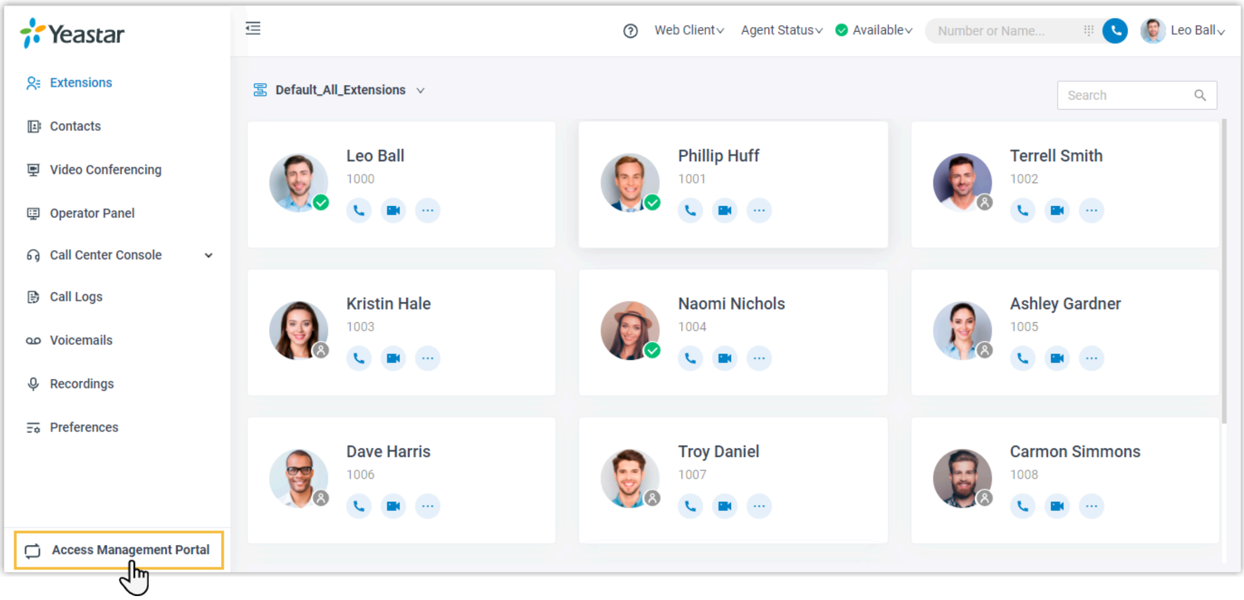
A user role is created.

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 Software Edition are as follows:

- Extension and Trunk
- Contacts
- Call Control
- Call Features
- Reports and Recordings
- Auto Provisioning
- PBX Settings
- System
- Security
- Maintenance
- Integration
- Plan

Extension and Trunk

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

Table 26.

Module	Permission
Extension	• 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.

Table 26. (continued)

Module	Permission
	• 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.
Extension Group	Manage extension groups.
Trunks	Manage trunks.

Contacts

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

- Company Contacts
- PhoneBooks
- 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

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
- 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.

Table 27.

Module	Permission
CDR and Recording Files	Specify users with the role assigned can view which extensions' CDR and recordings. • All Extensions: View all extensions' CDR and recordings. • All the other extensions of the same Extension Groups: View CDR and recordings of all the other extensions of the same group except the one that contains all the extensions. • All other extensions of the same department: View CDR and recordings of all the other extensions in the same department, excluding those in the associated sub-departments. • Specific Extensions: View CDR and recordings of specific extensions.
	Specify how users with the role assigned can manage CDR. • Download • Delete
	Specify how users with the role assigned can manage recording files. • Play • Download • Delete
Call Reports	Specify whether users with the role assigned can access call reports.

Auto Provisioning

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

PBX Settings

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

- Preferences
- Voice Prompt
- SIP Settings
- Jitter Buffer

System

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

- Network
- Date and Time
- Email
- Storage
- Event Notification
- Remote Management
- 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
- Activation
- System Logs

Integration

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

- CRM

- Speech to Text
- AMI
- Database Grant

Plan

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

Linkus Server

Linkus Overview

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

Linkus server

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

- Auto configuration by Remote Access Service

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

  > Note:
  >
  > RAS provides remote access, not remote control.

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

  For more information about Linkus auto configuration by RAS, see Set up Linkus Server with Remote Access Service.
- Manual configuration

  Manual configuration of Linkus remote server requires professional network knowledge.

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

  For more information about manual configuration, see Manually Set up Linkus Server.

Linkus client

Yeastar P-Series Software Edition supports the following Linkus clients:

- Linkus Mobile Client
- Linkus Desktop Client

- Linkus Web Client

For more information about Linkus Mobile Client and Linkus Desktop Client, see Linkus Help Center.

For more information about Linkus Web Client, see Linkus Web Client User Guide.

Linkus client login methods

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

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

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

  For more information, see Configure Linkus Welcome Email and Send Linkus Welcome Emails.
- Manual login

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

Table 28.

Linkus Server	Mobile & Desktop Login Credentials	Web Client Login Credentials
Linkus Server (RAS)	◦ The PBX's serial number or the FQDN that is bound with the PBX ◦ Username Username can be extension number or email address, which depends on how you Configure Linkus Login Mode. ◦ User password	
Linkus Server (Manual configuration)	◦ PBX's local IP address and local Linkus port ◦ PBX's public IP address or domain name and external Linkus port ◦ Username	No supported.

Linkus Server	Mobile & Desktop Login Credentials	Web Client Login Credentials
	Note: Username can be extension number or email address, which depends on how you Configure Linkus Login Mode. ◦ User password	

Linkus events

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

Yeastar P-Series Software Edition provides the following Linkus events:

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

For more information, see Event Notification Overview and Configure Event Notifications.

Set up Linkus Server with Remote Access Service

After you get Remote Access Service, users can remotely access Linkus Mobile Client and Desktop Client using the PBX Serial Number (SN). To allow remote access to Linkus Web Client, you need to further configure a Yeastar-supplied Fully Qualified Domain Name (FQDN) on the system.

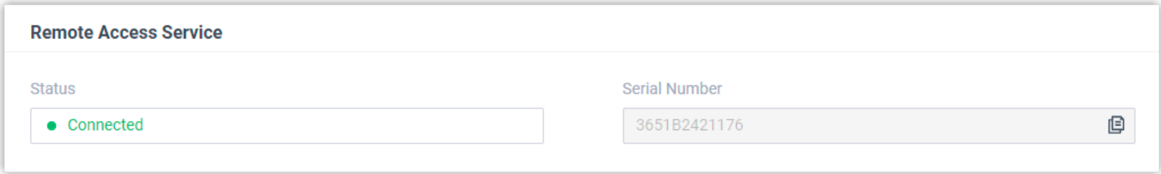
Background information

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

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

Note:

Only remote access to Linkus Mobile Client and Desktop Client is supported. For remote access to Linkus Web Client, you need to further configure the Yeastar FQDN.



Remote Access Service

Status: ● Connected

Serial Number: 3651B2421176

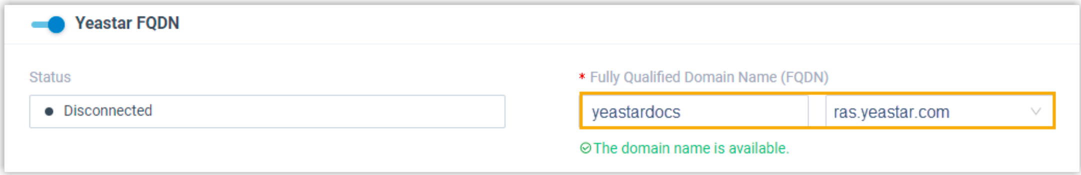
- A Fully Qualified Domain Name (FQDN) can be quickly set up to complete the remote working solution with all Linkus clients (Mobile Client, Desktop Client, and Web Client).

Procedure

1. Log in to PBX 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.



Yeastar FQDN

Status: ● Disconnected

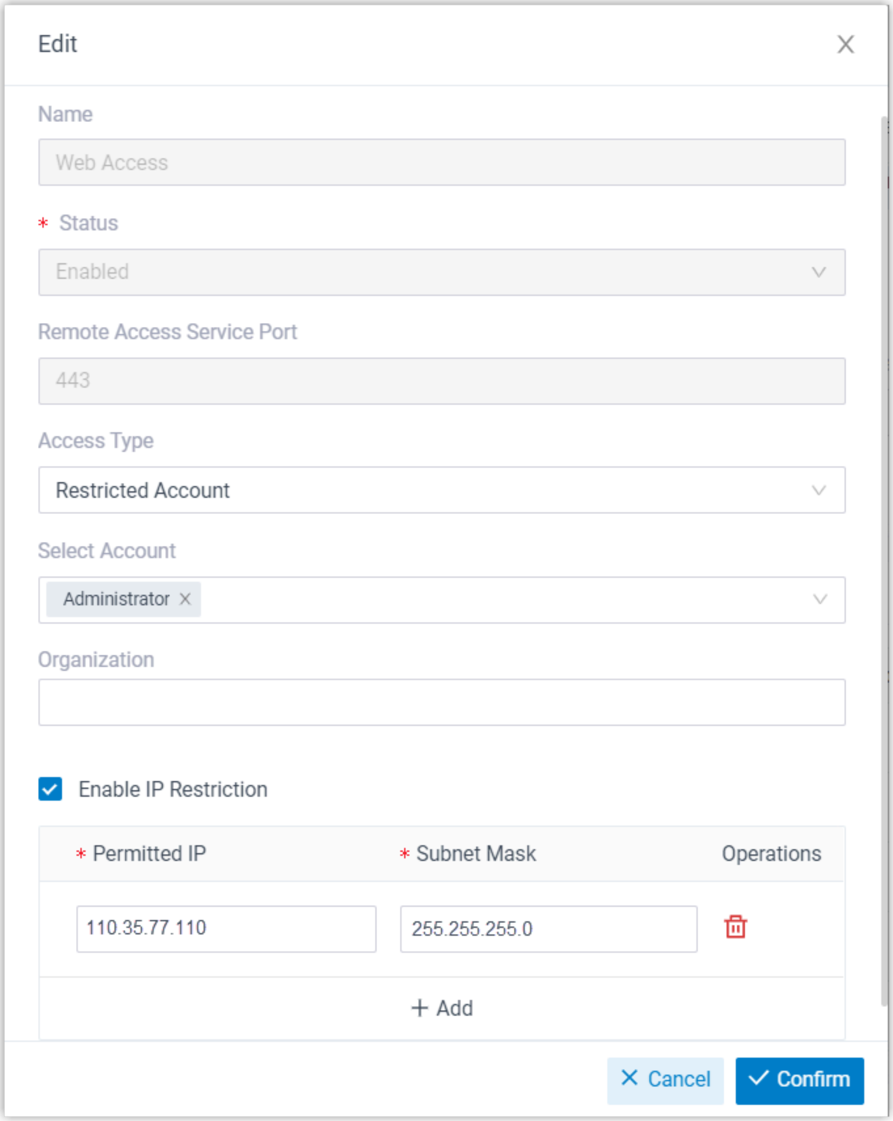
* Fully Qualified Domain Name (FQDN): yeastardocs | ras.yeastar.com

The domain name is available.

4. Optional: Configure the remote access permission of Linkus Web Client.

Note:
By default, all extension accounts are allowed to access Linkus Web Client via FQDN. You can change the remote access permission as needed.

   a. In the Features section, go to the Remote Access tab.
   b. Click ✎ beside the Web Access feature.
   c. In the pop-up window, set up the usage permissions:



Edit

Name

Web Access

* Status

Enabled

Remote Access Service Port

443

Access Type

Restricted Account

Select Account

Administrator

Organization

☑ Enable IP Restriction

* Permitted IP	* Subnet Mask	Operations
110.35.77.110	255.255.255.0	

- 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.

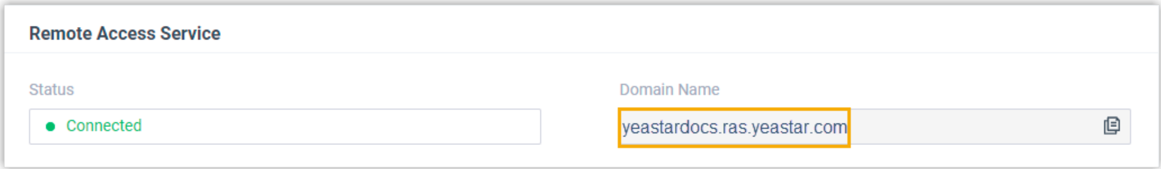
  If you configure this option, only the permitted IP address(es) can use the remote access feature.

d. Click Confirm.

5. Click Save.

Result

- Linkus server is automatically set up for remote access with the FQDN. The following information is displayed on the Linkus Server page:



Remote Access Service

Status: Connected

Domain Name: yeastardocs.ras.yeastar.com

  - Status: Connected, which means that Linkus server is set up successfully.
  - Domain Name: The domain name can be used for Linkus remote access.

- Users can use Linkus (Mobile Client, Desktop Client, and Web Client) via the FQDN remotely.

What to do next

- Configure Linkus Login Mode
- Enable Linkus clients for users

Manually Set up Linkus Server

This topic describes how to manually set up Linkus server according to different network scenarios.

Restrictions

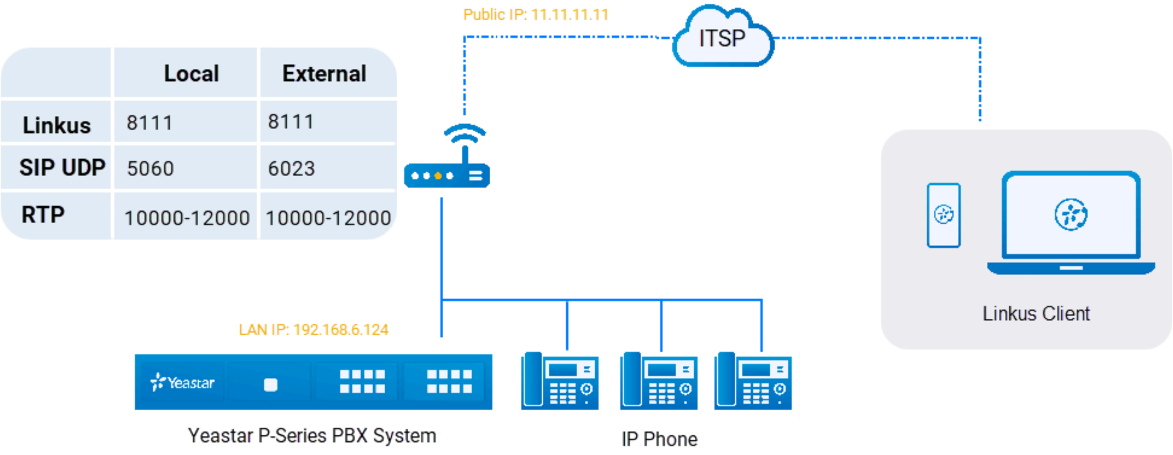
Important:

To allow users to remotely use Linkus Web Client, you need to set up Linkus server with Remote Access Service (RAS).

For more information, see Set up Linkus Server with Remote Access Service.

PBX is behind a router

If your PBX is behind a router and Linkus communicates with the PBX through the network interface that is configured with a private IP, you need to forward Linkus-related ports on your router and configure SIP NAT settings on your PBX.



	Local	External
Linkus	8111	8111
SIP UDP	5060	6023
RTP	10000-12000	10000-12000

Procedure

Based on the above network topology diagram, you can configure Linkus server as follows:

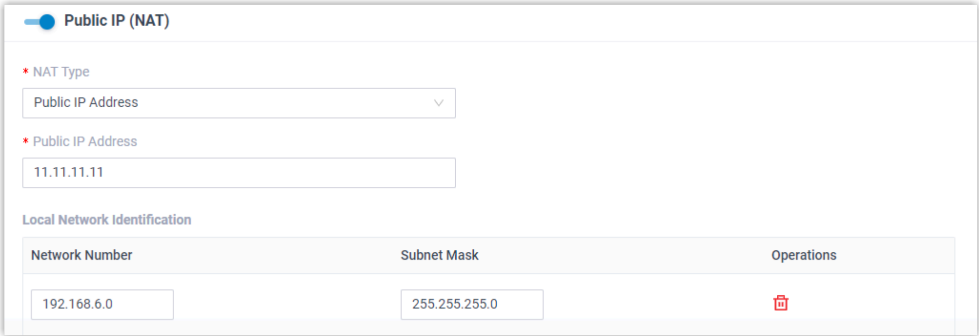
1. Log in to PBX web portal, go to System > Network > Service Ports to check and manage local service ports on your PBX system.
2. Forward Linkus-related ports on your router.

   In this example, forward the following ports:

Service Port	Local Port	External Port
Linkus Service Port	TCP&UDP 8111	TCP&UDP 8111
SIP Registration Port	UDP 5060	UDP 6023
RTP Ports	UDP 10000-12000	UDP 10000-12000

3. Configure SIP NAT on your PBX for remote access.

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


Public IP (NAT)

* NAT Type: Public IP Address

* Public IP Address: 11.11.11.11

Local Network Identification

Network Number	Subnet Mask	Operations
192.168.6.0	255.255.255.0	🗑

a. On the PBX web portal, go to System > Network > Public IP and Ports.
b. Enable Public IP (NAT).
c. In the NAT Type drop-down list, select Public IP Address.
d. In the Public IP Address field, enter the public IP address. In this example, enter 11.11.11.11.
e. In the Local Network Identification section, click + Add IP to add all your local network. In this example, enter 192.168.6.0/255.255.255.0.
f. In the NAT Mode drop-down list, select Yes.

4. Enter external SIP port and Linkus service port, which helps the router to direct appropriate traffic from the Internet to the PBX.
   - External SIP UDP Port: In this example, enter 6023.
   - External Linkus Port: In this example, enter 8111.
5. Click Save.

Result

Linkus server for both local access and remote access is set up.

What to do next

- Configure Linkus Login Mode
- Enable Linkus clients for users

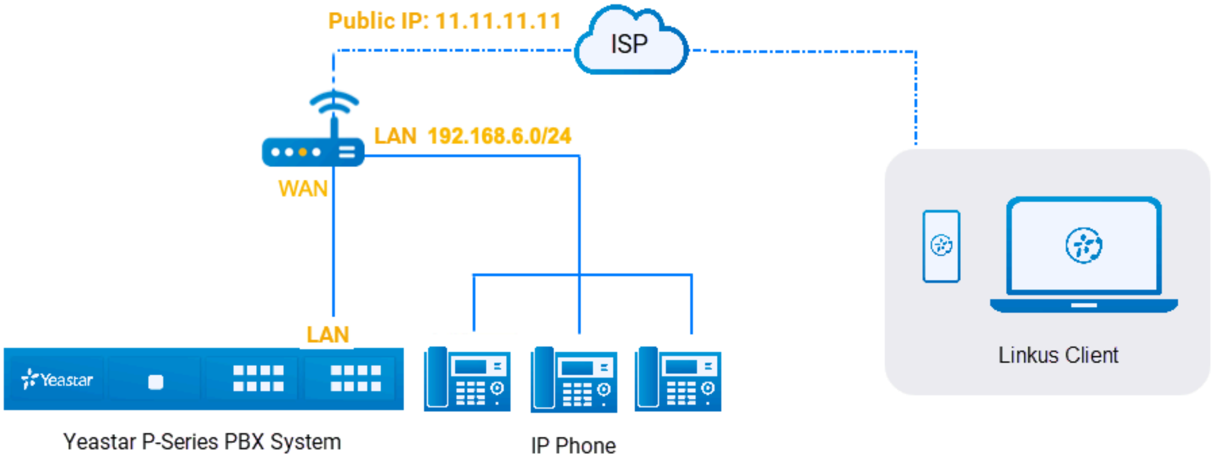
PBX is connected to the ISP router directly

If the PBX is connected to an Internet Service Provider (ISP) router, the Linkus server is ready to be accessed remotely.

Note:

- In this network scenario, you do NOT need to do port forwarding on your router and configure SIP NAT settings on your PBX.

- For this network scenario, you should change the SIP UDP port on the PBX to improve the system security.



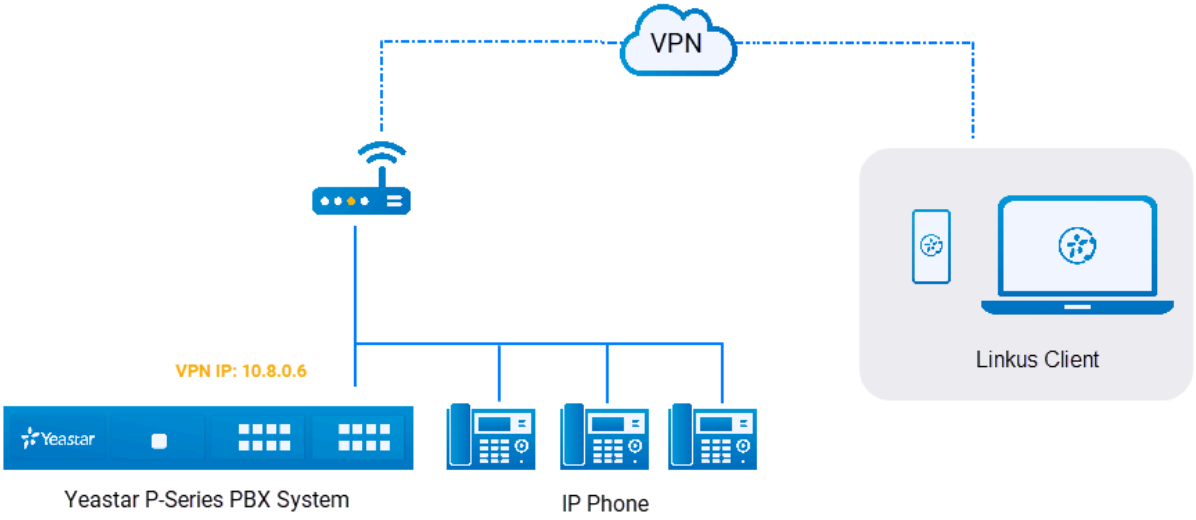
What to do next

- Configure Linkus Login Mode
- Enable Linkus clients for users

PBX is connected to a VPN network

If your PBX is connected to a VPN network, the Linkus server is ready to be accessed by the VPN network.

Note:
In this network scenario, you do NOT need to do port forwarding on your router or configure SIP NAT settings on your PBX.



What to do next

- Configure Linkus Login Mode
- Enable Linkus clients for users

Configure Linkus Login Mode

Yeastar P-Series Software Edition supports two login modes for Linkus clients. You can decide how users can manually log in to Linkus clients.

Procedure

1. Log in to PBX web portal, go to Extension and Trunk > Extension.
2. Click Linkus Server tab.
3. In the Linkus Client Login Mode section, select the checkboxes of the desired login modes.
    - Extension Number: Use an extension number as the username.
    - Email Address: Use an email address as the username.

    > Note:
    > The email address is associated with user's extension number.
4. Click Save.

Enable Linkus Clients for Users

After Linkus server is set up, you need to enable Linkus clients for users, so that users can log in to Linkus and use it. This topic describes how to enable Linkus clients for a user.

Procedure

1. Log in to PBX web portal, go to Extension and Trunk > Extension.
2. Select a desired extension, click ✎.
3. Click Linkus Clients tab.
4. Enable the following Linkus clients for the user.
    - Linkus Mobile Client
    - Linkus Desktop Client
    - Linkus Web Client

Result

- Linkus Mobile Client: The status shows ●, and a login QR code is displayed on the right.
- Linkus Desktop Client: The status shows ●, and a login link is displayed on the right.
- Linkus Web Client: The status shows ●.

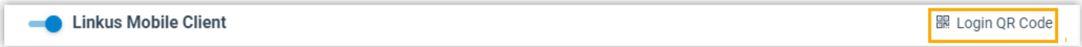
What to do next

Send Linkus login credentials to users.

- To send login credentials in bulk, you can send Linkus welcome emails to users, which contain login credentials of all the Linkus clients.

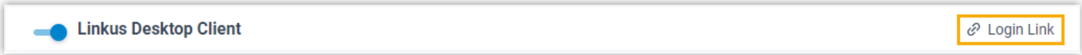
  For more information, see Send Linkus Welcome Emails.
- To send login credential of a specific Linkus client to a user, do the followings:
    - Linkus Mobile Client: Provide user with the login QR code.

      Note:
      The QR code can be used ONLY once, and is valid for 24 hours.

    - Linkus Desktop Client: Provide user with the login link.

      Note:
      The link can be used ONLY once, and is valid for 24 hours.

    - Linkus Web Client: Provide user with the following information:

- The FQDN that is bound with the PBX system
- Username

  The username can be extension number or email address, which depends on how you configure login mode. For more information, see Configure Linkus Login Mode.
- User password

Configure Linkus Welcome Email

Before sending Linkus welcome emails to provide users with login credentials of all the Linkus clients, you may need to configure Linkus welcome email.

Background information

By default, Yeastar P-Series Software Edition sends Linkus welcome emails in the language that you have set in system email template. A welcome email contains the following information:

- Extension information: Include extension number and voicemail PIN.
- Login instructions and credentials: Include login instructions and credentials for all the Linkus clients.

Procedure

Yeastar P-Series Software Edition provides a default email template, you can also customize your own template as follows.

1. Log in to PBX web portal, go to Extension and Trunk > Extension.
2. Click Linkus Server tab.
3. Click Email Templates tab.
4. Customize email template.
   a. In the Template drop-down list, select Custom.
   b. Edit email subject and content according to your needs.
   c. Click Save.

What to do next

Send Linkus Welcome Emails

Send Linkus Welcome Emails

To provide multiple users with Linkus login credentials, you can send Linkus welcome emails. This topic describes how to send Linkus welcome emails.

Prerequisites

- Make sure the system email server works.
- Make sure Linkus server has been set up.

  For more information about the configurations, see Set up Linkus Server with Remote Access Service or Manually Set up Linkus Server.
- You have configured email addresses for the desired extensions.
- You have enabled at least one Linkus client for the desired extensions.

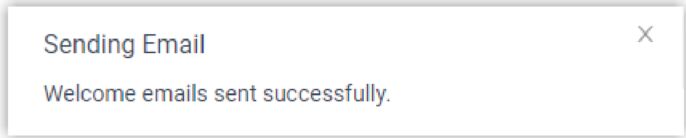
Procedure

1. Log in to PBX web portal, go to Extension and Trunk > Extension.
2. On Extension list, select the checkboxes of the desired extensions, click Welcome Email.

   The system sends welcome emails to the extensions' email addresses.

Result

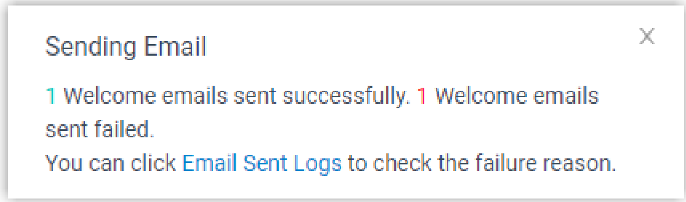
- If all the welcome emails are sent successfully, the web interface displays the following confirmation.



Sending Email

Welcome emails sent successfully.

- If there are any emails failed to be sent, you will get an error prompt like the following figure. Click Email Sent Logs to check the error.



Sending Email

1 Welcome emails sent successfully. 1 Welcome emails sent failed.

You can click Email Sent Logs to check the failure reason.

Enable or Disable Push Notifications for Linkus Mobile Client

This topic describes how to enable or disable push notifications for Linkus Mobile Client.

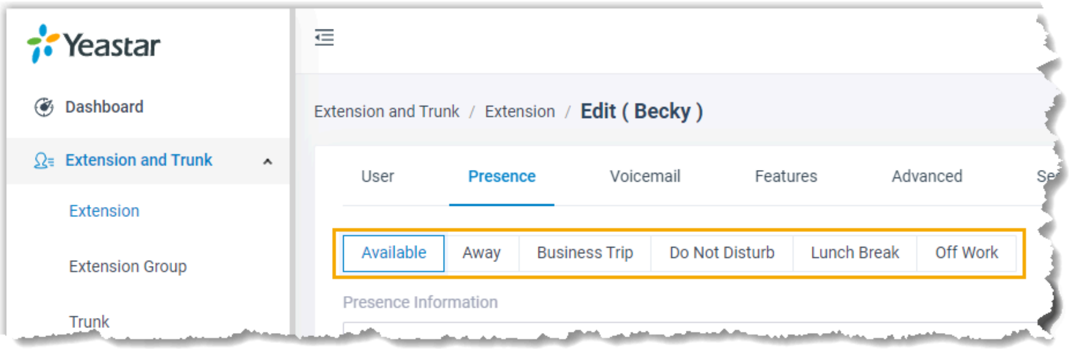
Background information

Push notification is an important tool for showing users alert messages and bringing them back to Linkus Mobile Client. By default, users can receive Linkus notifications anywhere and anytime, such as missed calls, new voicemail messages and so on.

> Tip:
>
> If Linkus server is set up in local network only, in case users receive an incoming call notification when they are out of the office but can not actually connect to the call, you can disable push notifications for them.

Procedure

1. Log in to PBX web portal, go to Extension and Trunk > Extension, edit the desired extension.
2. Click Presence tab.
3. To configure push notifications for a specific presence, select one on the status bar.



4. In the Options section, select or unselect the checkbox of Accept Push Notifications.
5. To configure push notification for other presence status, repeat step3-4.
6. Click Save.

Operator Panel

Manage Operator Panel

This topic describes instructions on setting up Operator Panel for extension user.

What is Operator Panel

Operator Panel is a web-based utility integrated with the Yeastar Linkus Web Client. It is designed for employee who needs to manage and transfer a large number of calls, such as receptionist or agent manager.

> Note:
> Operator Panel is only recommended for groups with no more than 1000 extensions, otherwise the user experience will be affected as web browser can not work properly with excessive data volume.

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)	√	√	√

Permission	Extension Group Manager	Extension Group User	Custom role of Extension Group
Pick up or hang up other extensions' calls	√	√	√
Call monitoring operations (Listen, Whisper, Barge-in)	√	√	√
Call parking operations (Park, Retrieve)	√	√	√
Route calls directly from IVR regardless of the IVR menu	√	√	√
Switch Business Hours and Holidays status	√	×	√
Switch 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

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 Software Edition 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 Software Edition and other devices. Yeastar P-Series Software Edition will act as a VoIP account provider, the other device should register this account to connect to Yeastar P-Series Software Edition.

SIP trunk creation methods

Create a SIP trunk by a template

Yeastar P-Series Software Edition supports leading ITSP across the globe, you can use the pre-configured ITSP templates included in Yeastar P-Series Software Edition 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

SIP Trunk status

Status	Description
🚫	Disabled.
⊗	Unreachable.
	Registration failed. • Authentication failed. • Transport type inconsistent. • Rejected.
🕓	Registering.
✓	Registered.
?	Unmonitored.
☎	Busy. Maximum channels reached.

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.
    b. In the pop-up window, configure the following settings:
        - DID/DDI: Enter the provided DID number.
        - DID/DDI Name: Optional. Enter a name to distinguish inbound calls by DID numbers.

            The name will be displayed on the called party's device when the DID number is dialed.
    c. Click Save.
    d. To add more DID numbers, repeat step a - c.

    For more information of DID configurations, see Configure DID Numbers on a Trunk.
4. Click Save and Apply.

Result

Go to Extension and Trunk > Trunk to check the trunk status on the trunk list page.

If the status shows ✓, the trunk is registered successfully.

For more information of SIP trunk status, see SIP Trunk status.

What to do next

- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see Set up an Inbound Route.
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see Set up an Outbound Route.

Create a SIP Register Trunk

This topic gives a configuration example to describe how to create a general SIP Register Trunk, which can be applied to all kinds of SIP Register Trunk.

Background information

Assume that you have bought a SIP account from the ITSP ABC, and the trunk information is displayed as below.

- Provider domain: abc.provider.com
- Protocol: SIP
- Registration Port: 5060
- Transport: UDP
- Username: 254258255
- Authentication name: 254258255
- Password: 05JsOmsIS54SYh

Prerequisites

- You have purchased a SIP account from an ITSP and a username and a password are offered.
- Your PBX can connect to the ITSP.

Procedure

1. Log in to PBX 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 05JsOms-IS54SYh.
    - Authentication Name: Enter the provided authentication name. In this example, enter 254258255.

    > Note:
    >
    > In most cases, authentication name is the same as the user name.

    - Enable Outbound Proxy: Optional. If the trunk is configured to use an outbound proxy server, when users make outbound calls through this trunk, all the SIP packets will be sent to the outbound proxy server.

    > Note:
    >
    > Contact your ITSP to check if outbound proxy is supported, then configure outbound proxy settings under the ITSP's guidance.

4. Optional: If you have purchased DID numbers from the ITSP, click DIDs/DDIs tab to configure the DID numbers for the trunk.
    a. Click Add.
    b. In the pop-up window, configure the following settings:
        - DID/DDI: Enter the DID number provided by the ITSP.
        - DID/DDI Name: Optional. Enter a name to distinguish inbound calls by DID numbers.

          The name will be displayed on the called party's device when the DID number is dialed.
    c. Click Save.
    d. To add more DID numbers, repeat step a - c.

    For more information of DID configurations, see Configure DID Numbers on a Trunk.
5. Optional: Click Advanced, Inbound Caller ID Reformatting, Outbound Caller ID, or SIP Headers tab to configure other settings.
6. Click Save and Apply.

Result

Go to Extension and Trunk > Trunk to check the trunk status on the trunk list page.

If the status shows ✓, the trunk is registered successfully.

For more information of SIP trunk status, see SIP Trunk status.

What to do next

- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see Set up an Inbound Route.
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see Set up an Outbound Route.

Create a SIP Peer Trunk

This topic gives a configuration example to describe how to create a general SIP Peer Trunk, which can be applied to all kinds of SIP Peer Trunk.

Background information

Assume that you have bought a SIP account from the ITSP ABC, and the trunk information is displayed as below.

- Provider domain: abc.provider.com
- Protocol: SIP
- Registration Port: 5060
- Transport: UDP

Prerequisites

- You have purchased a SIP account from an ITSP and no username and password is offered but only a domain name or IP address.
- Your PBX can connect to the ITSP.

Procedure

1. Log in to PBX 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.
   b. In the pop-up window, configure the following settings:
      - DID/DDI: Enter the provided DID number.
      - DID/DDI Name: Optional. Enter a name to distinguish inbound calls by DID numbers.

        The name will be displayed on the called party's device when the DID number is dialed.

   c. Click Save.
   d. To add more DID numbers, repeat step a - c.

   For more information of DID configurations, see Configure DID Numbers on a Trunk.
5. Click Save and Apply.

Result

Go to Extension and Trunk > Trunk to check the trunk status on the trunk list page.

If the status shows ✓, the trunk is registered successfully.

For more information of SIP trunk status, see SIP Trunk status.

What to do next

- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see Set up an Inbound Route.
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see Set up an Outbound Route.

Create a SIP Account Trunk

A SIP Account is used for the other device to register with Yeastar P-Series Software Edition. In this way, Yeastar P-Series Software Edition and the other device are connected. This topic describes how to create a SIP Account Trunk on Yeastar P-Series Software Edition.

Prerequisites

To connect a third-party device with Yeastar P-Series Software Edition 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, select the trunk type and define the information of the SIP account.

    > Note:
    > You can leave the default SIP information or edit the information according to your needs.

    - Trunk Type: Select Account Trunk.
    - Transport: Select a transport. The following options are supported:
        - UDP
        - TCP

            > 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: Enter an authentication name for the SIP account.
4. Optional: Click Advanced, Inbound Caller ID Reformatting, Outbound Caller ID, or SIP Headers to configure other settings.
5. Click Save and Apply.

What to do next

- Register the SIP Account Trunk on the third-party software or device. Depending on the network of the third-party software or device, you need to provide different information:
    - Same local network as Yeastar P-Series Software Edition
        - SIP Account Trunk details
        - Local IP address of PBX
        - Local SIP port of PBX

    - Different network from Yeastar P-Series Software Edition
        - 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 Software Edition 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.
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.

Detailed Configuration	
Setting	Description
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.
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.

Detailed Configuration	
Setting	Description
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.
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 Software Edition 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.

Setting	Description
	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.
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.

Call Restriction

Setting	Description
Call Restriction Type	Specify based on which type of calls to restrict the max concurrent call number of this trunk. • Outbound Call: Only outbound calls will be restricted. • All: Both outbound calls and inbound calls will be restricted.
Maximum Concurrent Calls	Specify the maximum number of concurrent calls allowed in this trunk. The default is Unlimited.

DIDs/DDIs

Direct Inward Dialling (DID), also called Direct Dial-in (DDI), is a service offered by telephone companies. For more information of DID concepts, see DID Number Overview.

- DID numbers are usually configured on inbound routes to distinguish inbound calls.

  For more information, see Route Inbound Calls based on DID Numbers.

- For more instructions on configuring the DID numbers, see Configure DID Numbers on a Trunk.

Inbound Caller ID Reformatting

When a user calls in the PBX, the trunk provider may send a caller ID that is inconvenient for you to redial directly.

In this case, you can reformat inbound caller ID based on a trunk. The caller ID will be reformatted before it is sent to the called party.

For more information, see Reformat Inbound Caller ID based on a Trunk.

Outbound Caller ID

Outbound caller ID is the phone number or name that is displayed on the called party's device.

You can set up a global outbound caller ID for a trunk or assign caller IDs for extension users.

> Note:
> By default, each trunk has a default phone number that will be displayed on the called party's device. Outbound Caller ID configuration requires support from the trunk provider. Contact your trunk provider first before you configure Outbound Caller ID, or the settings won't take effect and outbound calls may fail.

If you set the caller ID number, when users make outbound calls through this trunk, the called party will see this caller ID number instead of the calling party's number.

For more information of outbound caller ID configurations, see Customize Outbound Caller IDs

SIP Headers

The SIP Headers settings require professional knowledge of SIP protocol. Incorrect configurations may cause calling issues. It is wise to leave the default settings provided on the SIP trunk page. However, for a few fields, you need to change them to suit your situation.

The following settings are included on the SIP Headers page.

- Inbound Parameters
- Outbound Parameters
- Other Settings

Inbound Parameters

Setting	Description
Get Caller ID From	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 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:

- From

A From header contains caller ID and caller ID name, which are defined as the followings in Yeastar P-Series Software Edition.

  - From User Part: Indicates caller ID.
  - From Display Name Part: Indicates caller ID name.

  You can define which parameters will be used in these two parts of a SIP From header.
- Diversion
- Remote Party ID
- P-Asserted Identify
- P-Preferred-Identity

Each SIP header has multiple options to define the parameters. The following tables describe the options.

Note:
For different types of SIP trunk, the optional items are different.

Setting	Description
[Default]	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.
Outbound Route Outbound Caller ID	The outbound caller ID configured on the outbound route that is used for the outbound calls.
Extension's Outbound Caller ID in Trunk	The extension's associated outbound caller ID with the trunk.
Trunk Outbound Caller ID	The global outbound caller ID for the trunk (Trunk > Outbound Caller ID > General).
Trunk Username	The username configured on the trunk.
Extension Caller ID	The caller ID configured on the extension.
Originator Caller ID	The Caller ID of the call originator (the first caller in the case that the call is transferred).

Setting	Description
	• If the call originator is an external number, the external number will be taken. • If the call originator is an extension, the priority order will be Extension Outbound Caller ID → [Default].
Custom	Define a custom value.

Other Settings

Setting	Description
User Agent	If the ITSP requires User Agent for authentication, enter the User Agent information that is provided by the ITSP.
Realm	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.
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.
100rel	Whether to support 100rel or not.
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.
Support P-Early-Media	Set whether the P-Early-Media field is included in the INVITE packet.

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.

Prerequisites

- A phone is connected to Yeastar P-Series Software Edition 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)

- 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.

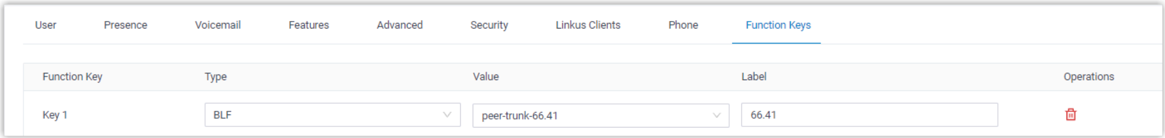
Procedure

- Step1. Set up a function key for trunk monitoring
- Step2. Apply the configuration to IP phone

Step1. 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`.

Function Key	Type	Value	Label	Operations
Key 1	BLF	peer-trunk-66.41	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.

Step2. 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.

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 Software Edition.
- 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 Software Edition. This topic describes how to set up basic emergency calling in Yeastar P-Series Software Edition.

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. In the Trunk's Emergency Outbound Caller ID field, configure trunks for emergency calls.

   > Note:
   >
   > Emergency calls have the highest priority. If the selected trunk is occupied, PBX will terminate the ongoing call, and place the emergency call.

   a. Click Add.
   b. In the drop-down list of Trunk, select a trunk.
   c. Leave the Trunk's Emergency Outbound Caller ID field blank.

      > Note:
      >
      > Do not set emergency outbound caller ID for basic emergency calling, or the emergency calls may fail.

   d. Optional: Click Add to add another trunk and repeat step a - step c.

      > Note:

If the first trunk cannot work properly, the PBX will use the second trunk to make calls.

6. Click Save and Apply.

What to do next

After setting up an emergency calling, you may need to consider the following configurations:

- Set up a Route for PSAP Callbacks
- Add an Emergency Notification Contact

Set up Enhanced Emergency Calling

To ensure that users can make emergency calls for help when an accident occurs, you need to set up emergency calling in Yeastar P-Series Software Edition. This topic describes how to set up enhanced emergency calling in Yeastar P-Series Software Edition.

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. In the Trunk's Emergency Outbound Caller ID field, configure trunks for emergency calls.
    a. In the drop-down list of Trunk, select a trunk.

> Note:
> Emergency calls have the highest priority. If the selected trunk is occupied, PBX will terminate the ongoing call, and place the emergency call.

b. In the Trunk's Emergency Outbound Caller ID, enter the Emergency Location Identification Number (ELIN) that you have purchased from the trunk provider.
c. Optional: Click Add to add another trunk and repeat step a - step c.

> Note:
> If the first trunk cannot work properly, the PBX will use the second trunk to make calls.

6. Click Save and Apply.

Assign ELINs for individual users

To provide the PSAP with the emergency caller's precise location, you may need to purchase multiple ELINs and assign these ELINs to extension users.

1. Log in to PBX 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 Software Edition 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 Software Edition 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 Software Edition provides a default email template for emergency notification, you can also customize your own template.

Background information

By default, Yeastar P-Series Software Edition 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 Software Edition 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 Software Edition. Read the concepts before you manage business hours and holidays.

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 Software Edition allows you to set a global business hours and also supports custom business hours for designated users.

- Global Business Hours

Global Business Hours is the main business hours for your company. Global Business Hours may apply to most of the employees who have fixed work schedules.

For more information, see Set Global Business Hours and Route Inbound Calls based on Global Business Hours.

- Custom Business Hours

  Custom Business Hours is typically for departments with different hours from your main business hours. You need to create custom schedules that accommodate each department's unique hours and call handling needs.

  For more information, see Route Inbound Calls based on Department Hours.

- 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. 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.

Related information

Set Global Business Hours
Monitor Time Condition Status
Create a Holiday
Override Time Condition for Inbound Calls
Automatic Reset of Time Condition

Global Business Hours

Set Global Business Hours

This topic describes how to set up Global Business Hours.

Background information

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 about different types of time in Yeastar P-Series Software Edition, see Overview of Business Hours and Holidays.

Procedure

1. Log in to PBX web portal, go to Call Control > Business Hours and Holidays > Business Hours, click Add.
2. In the Business Hours section, click Add, then specify the hours when your business is open.
3. In the Break Hours section, click Add, then specify rest breaks during the working days.
4. 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.
5. Optional: In the Other Options section, enter a note in the text field to help you identify the time group.
6. Click Save and Apply.

Result

- A time group is created for Global Business Hours.

- You can create more time groups according to your company's business hours. All the time groups created on the Business Hours page are regarded as your company's global business hours.

What to do next

- To handle inbound calls based on the Global Business Hours, see Route Inbound Calls based on Global Business Hours.
- To limit users to make outbound calls based on the Global Business Hours, see Set up an Outbound Route.

Related information

Monitor Time Condition Status
Override Time Condition for Inbound Calls
Route Inbound Calls based on Global Business Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on Employee Hours

Manage Global Business Hours

This topic describes how to edit and delete the time groups that you've defined as your Global Business Hours.

Edit a time group of Global Business Hours

1. Log in to PBX web portal, go to Call Control > Business Hours and Holidays.
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 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.
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.

Related information

Set Global Business Hours

Overview of Business Hours and Holidays

Holidays

Create a Holiday

This topic describes how to create holidays by date, week, and month.

Create a holiday by date

If the holiday date varies every year, you can create a holiday by date.

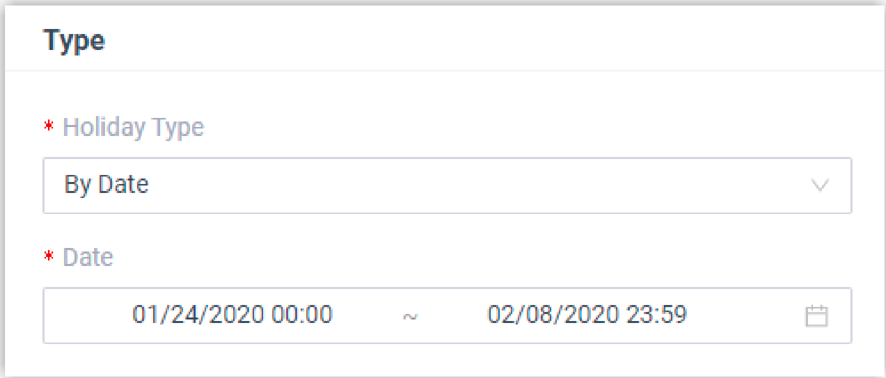
Example

Chinese Spring Festival varies every year, and 2020 Chinese Spring Festival falls on Jan. 24 to Feb. 8. You can set the holiday as follows.

Configuration Example

1. Log in to PBX web portal, go to Call Control > Business Hours and Holidays > Holidays.
2. On the Holidays page, click Add.

3. In the Basic section, enter `2020 Chinese Spring Festival` in the text field.
4. In the Type section, set the type and the date of holiday.



Type

* Holiday Type

By Date

* Date

01/24/2020 00:00 ~ 02/08/2020 23:59

   - Holiday Type: Select By Date.
   - Date: Select the holiday start date and end date.
5. Click Save and Apply.

Create a holiday by month

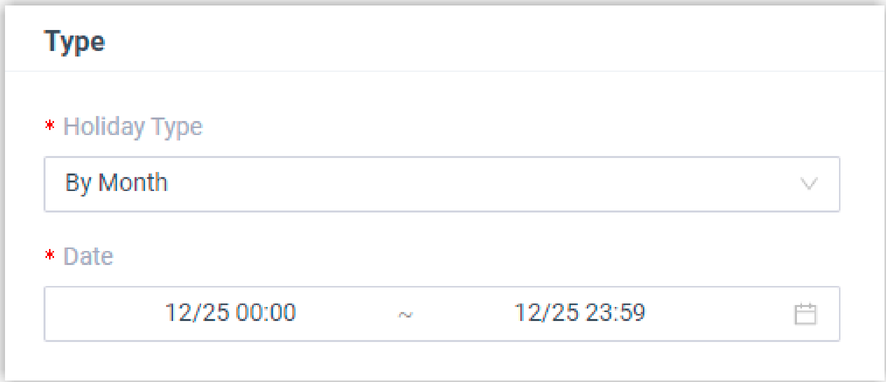
If the holiday always falls on the same date, you can set a holiday by month.

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 > Holidays.
2. On the Holidays page, click Add.
3. In the Basic section, enter `Christmas` in the text field.
4. In the Type section, set the type and the date of holiday.



Type

* Holiday Type

By Month

* Date

12/25 00:00 ~ 12/25 23:59

   - Holiday Type: Select By Month.
   - Date: Select the holiday start date and end date.

5. Click Save and Apply.

Create a holiday by week

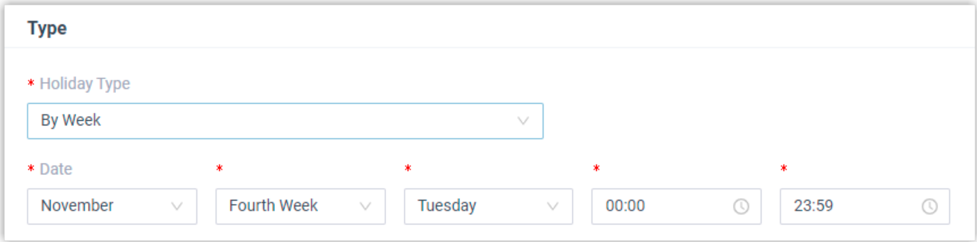
If a holiday always falls on the same week, you can set a holiday by week.

Example

Thanksgiving Day falls on the fourth Thursday of November. You can set the holiday as follows.

Configuration Example

1. Log in to PBX web portal, go to Call Control > Business Hours and Holidays > Holidays.
2. On the Holiday page, click Add.
3. In the Basic section, enter `Thanksgiving Day` in the text field.
4. In the Type section, set the type and the date of holiday.



Type

* Holiday Type: By Week

* Date: November | Fourth Week | Tuesday | 00:00 | 23:59

   - Holiday Type: Select By Week.
   - Date: Select the month and the day of a specific week.
5. 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
Manage Holidays

Manage Holidays

This topic describes how to edit and delete a holiday.

Edit a holiday

1. Log in to PBX web portal, go to Call Control > Business Hours and Holidays > Holidays.

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 > Holidays.
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]

Time Condition

Time Condition Overview

Time Condition is the communication feature in Yeastar P-Series Software Edition 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.

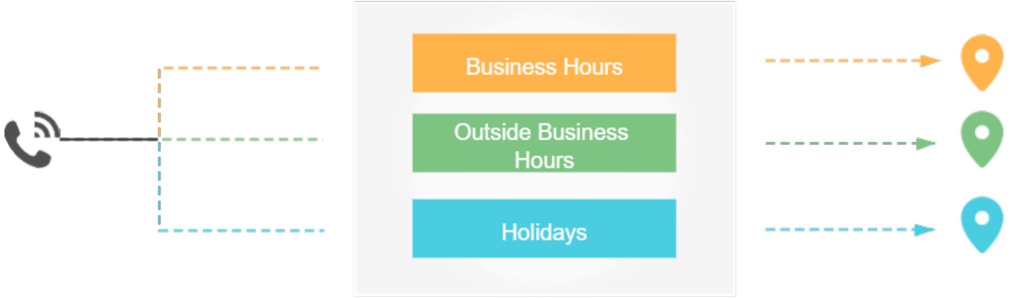
Where can Time Condition be applied?

Time Condition can be applied to an Inbound Route, an Outbound Route, and extension presence switch.

Apply to an Inbound Route

Time Condition can be used to control the destination of an inbound call based on date and time.

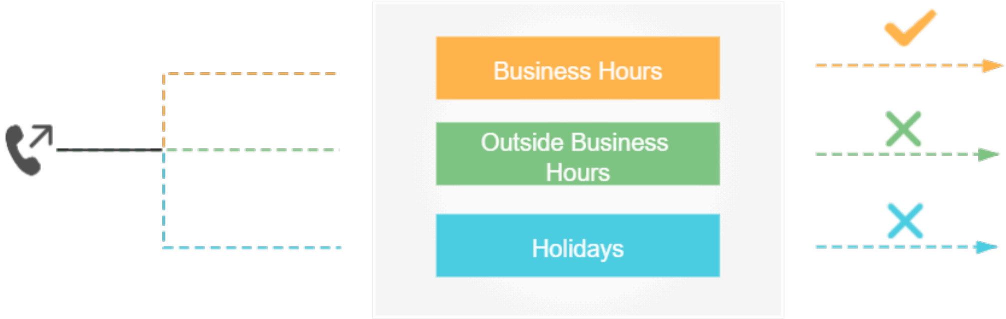
When a call reaches PBX, PBX will check the current system date and time against the time group associated, and then route the call to corresponding destination.



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 current system date and time against the time group associated. Only when the time comes to the permitted time group can the outbound call be made.

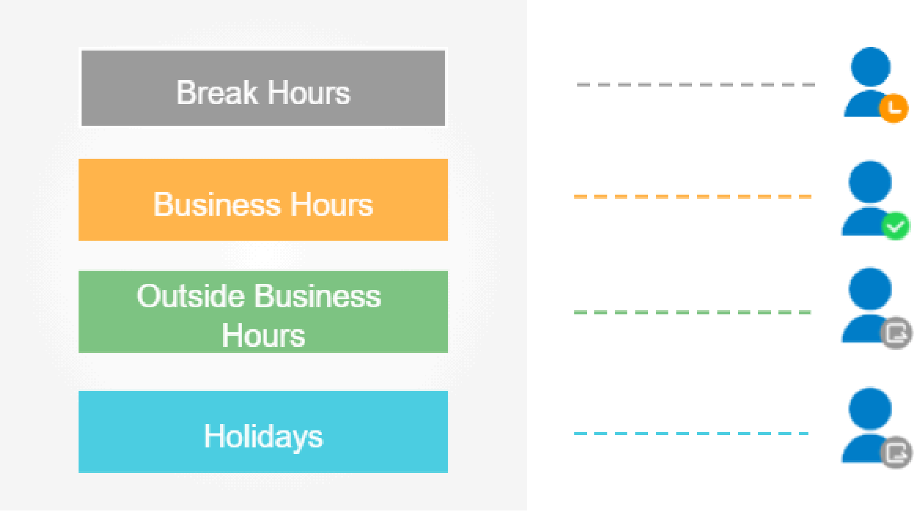


Apply to extension presence switch

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 enabled on extension configuration page. For more information, see Automatically Switch Extension Presence Based on Time.



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 Global 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 29.

Setting	Feature Code	Permission
Switch Global Business Hours and Holidays Status (for Global Business Hours)	*99	Select desired extensions.
Time Condition Switching Prefix (for Custom Business Hours and Custom Time Periods)	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 Global Business Hours can be overridden.

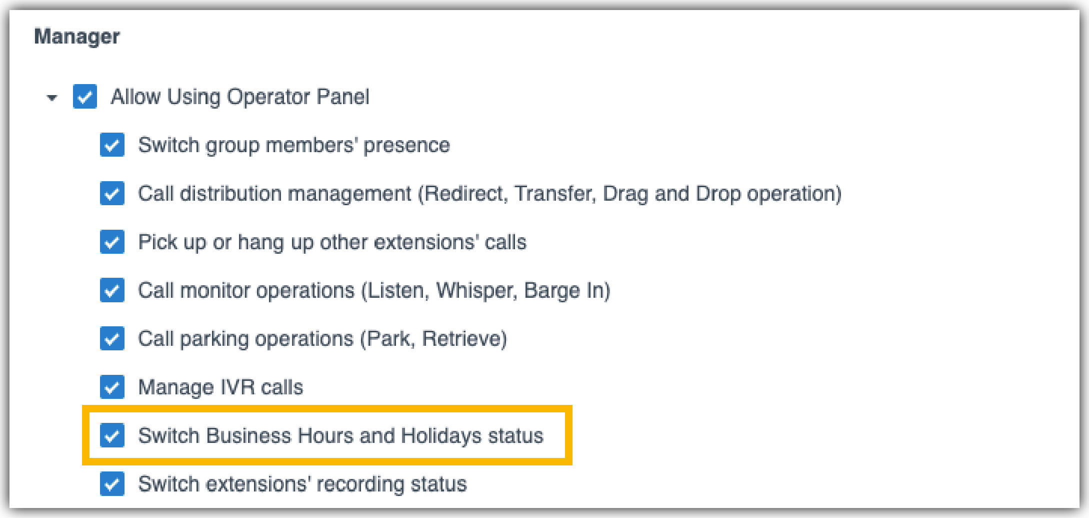
Procedure

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.



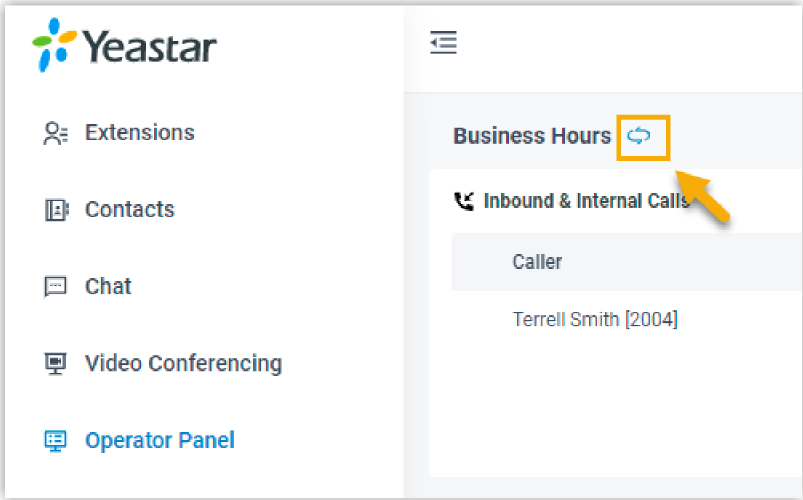
Manager

- ☑ Allow Using Operator Panel
  - ☑ Switch group members' presence
  - ☑ Call distribution management (Redirect, Transfer, Drag and Drop operation)
  - ☑ Pick up or hang up other extensions' calls
  - ☑ Call monitor operations (Listen, Whisper, Barge In)
  - ☑ Call parking operations (Park, Retrieve)
  - ☑ Manage IVR calls
  - ☑ Switch Business Hours and Holidays status
  - ☑ Switch extensions' recording status

5. Click Save and Apply.

Result

On Operator Panel, the user whose user type is Manager can click ⟲ to override time condition for Global Business Hours.



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

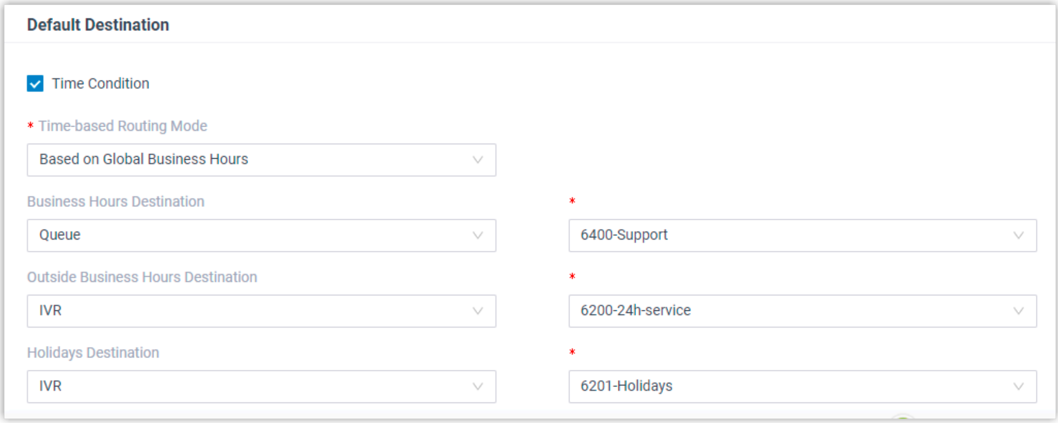
  After business hours, the employee who needs to work in the night can force open the business hours to provide communication services for customers.
- Occasionally leaving

  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 Global Business Hours is set up as follows:



Default Destination

☑ Time Condition

* Time-based Routing Mode: Based on Global Business Hours

Business Hours Destination: Queue | * 6400-Support

Outside Business Hours Destination: IVR | * 6200-24h-service

Holidays Destination: IVR | * 6201-Holidays

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 30.

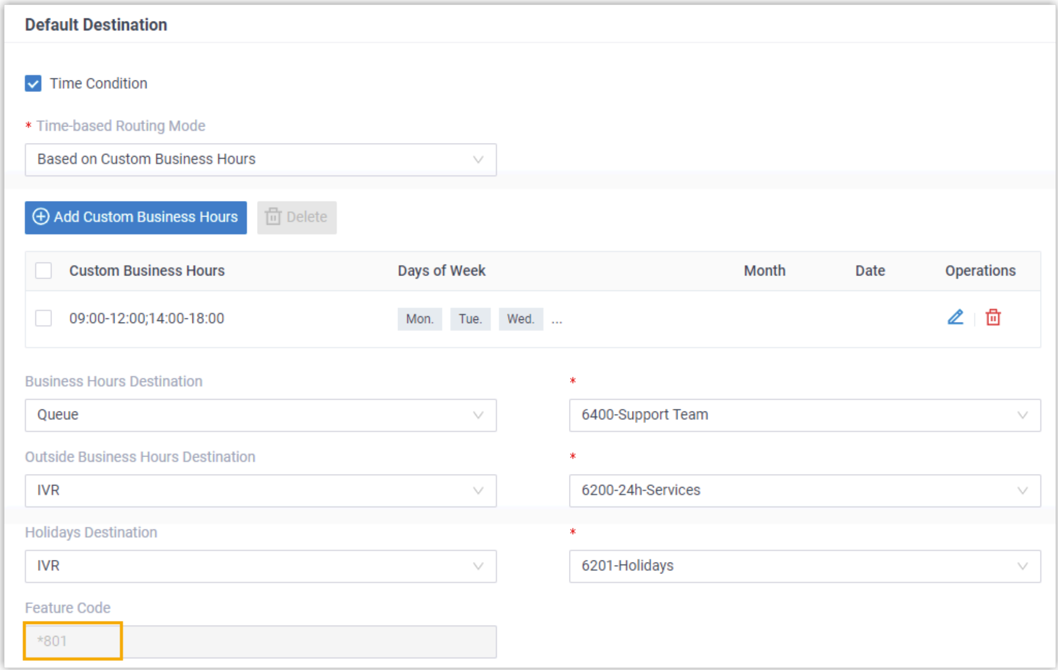
Operate Time	Result
Dial *99 during Business Hours	Inbound calls will be routed to Outside Business Hours destination (IVR 6200).
Dial *99 during Outside Business Hours	Inbound calls will be routed to Business Hours destination (Queue 6400).
Dial *99 during Holidays	Inbound calls will be routed to Business 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 is set up as follows:



Default Destination

☑ Time Condition

* Time-based Routing Mode: Based on Custom Business Hours

□	Custom Business Hours	Days of Week	Month	Date	Operations
□	09:00-12:00;14:00-18:00	Mon. Tue. Wed. ...			

Business Hours Destination: Queue — 6400-Support Team

Outside Business Hours Destination: IVR — 6200-24h-Services

Holidays Destination: IVR — 6201-Holidays

Feature Code: *801

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 31.

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).

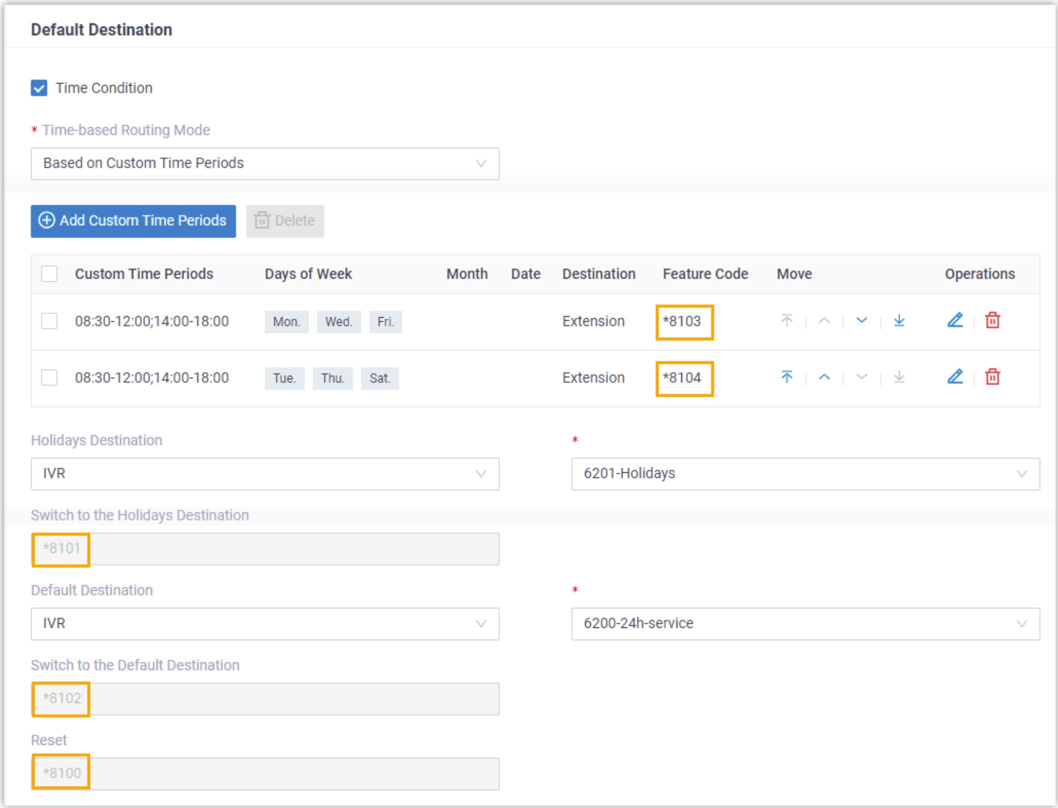
3. To clear time condition override, the authorized users should dial *801 again.

> 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 is set up as follows:



Default Destination

☑ Time Condition

* Time-based Routing Mode

Based on Custom Time Periods

Add Custom Time Periods | Delete

□	Custom Time Periods	Days of Week	Month	Date	Destination	Feature Code	Move	Operations
□	08:30-12:00;14:00-18:00	Mon. Wed. Fri.			Extension	*8103		
□	08:30-12:00;14:00-18:00	Tue. Thu. Sat.			Extension	*8104		

Holidays Destination

IVR | * 6201-Holidays

Switch to the Holidays Destination

*8101

Default Destination

IVR | * 6200-24h-service

Switch to the Default Destination

*8102

Reset

*8100

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 32.

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 • 08:30 - 12:00 • 14:00 - 18:00	Extension (2004-Terrell Smith)	*8104
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

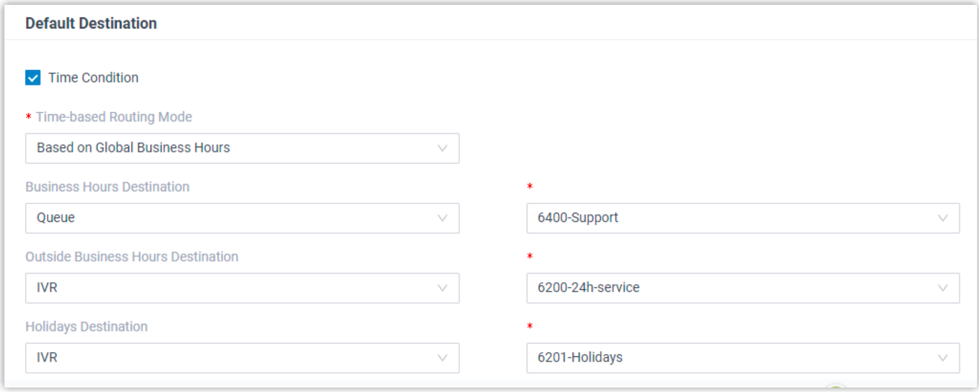
For the users who have permission to access Operator Panel, they can monitor time condition status on Operator Panel directly.

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 Global Business Hours is set up as follows:



Default Destination

☑ Time Condition

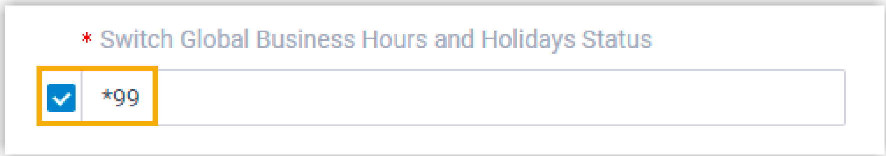
* Time-based Routing Mode: Based on Global Business Hours

Business Hours Destination: Queue — * 6400-Support

Outside Business Hours Destination: IVR — * 6200-24h-service

Holidays Destination: IVR — * 6201-Holidays

- The feature code for Switch Global Business Hours and Holidays Status is *99.



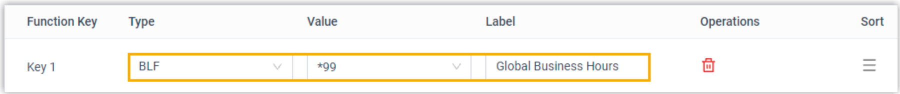
* Switch Global Business Hours and Holidays Status

☑ *99

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.



Function Key	Type	Value	Label	Operations	Sort
Key 1	BLF	*99	Global Business Hours	🗑	≡

- Type: Select BLF.
- Value: Enter the feature code of Switch Global 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

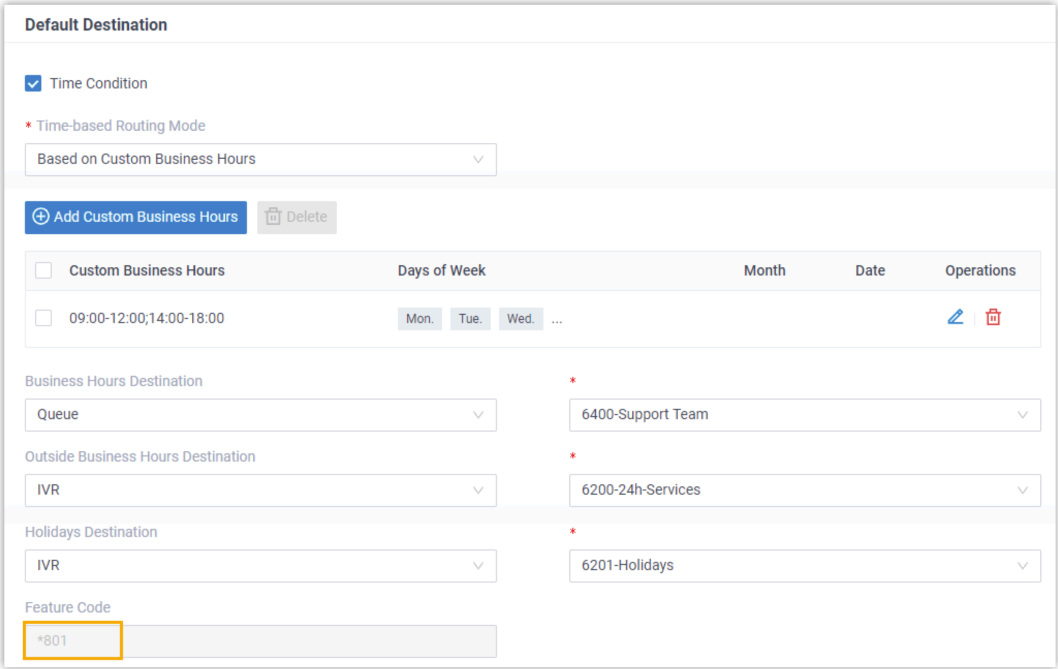
The function key settings are automatically updated on the phone and different BLF LED indicates different status.

- 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.

Monitor time condition status for inbound calls (Custom Business Hours)

Background information

An inbound route based on Custom Business Hours is set up as follows:



Default Destination

☑ Time Condition

* Time-based Routing Mode

Based on Custom Business Hours

☐	Custom Business Hours	Days of Week	Month	Date	Operations
☐	09:00-12:00;14:00-18:00	Mon. Tue. Wed. ...			✎ 🗑

Business Hours Destination: Queue | * 6400-Support Team

Outside Business Hours Destination: IVR | * 6200-24h-Services

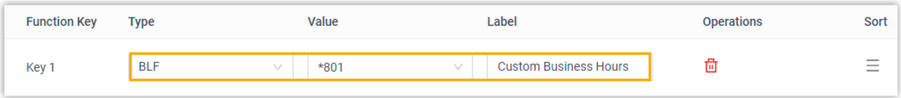
Holidays Destination: IVR | * 6201-Holidays

Feature Code: *801

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.



Function Key	Type	Value	Label	Operations	Sort
Key 1	BLF	*801	Custom Business Hours	🗑	☰

- 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

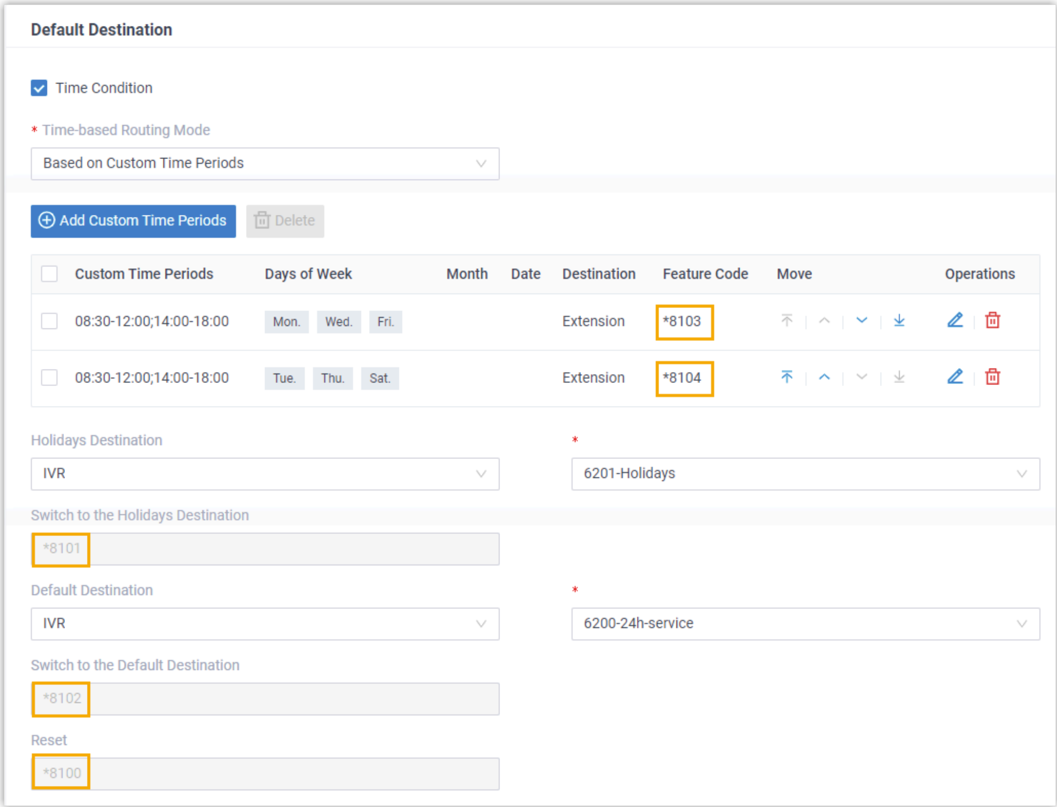
The function key settings are automatically updated on the phone and different BLF LED indicates different status.

- 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.

Monitor time condition status for inbound calls (Custom Time Periods)

Background information

An inbound route based on Custom Time Periods is set up as follows:



Default Destination

☑ Time Condition

* Time-based Routing Mode

Based on Custom Time Periods

□	Custom Time Periods	Days of Week	Month	Date	Destination	Feature Code	Move	Operations
□	08:30-12:00;14:00-18:00	Mon. Wed. Fri.			Extension	*8103		
□	08:30-12:00;14:00-18:00	Tue. Thu. Sat.			Extension	*8104		

Holidays Destination: IVR | * 6201-Holidays

Switch to the Holidays Destination: *8101

Default Destination: IVR | * 6200-24h-service

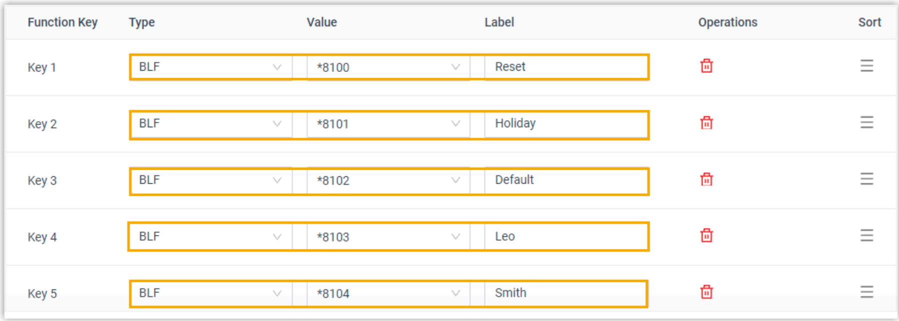
Switch to the Default Destination: *8102

Reset: *8100

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.



Function Key	Type	Value	Label	Operations	Sort
Key 1	BLF	*8100	Reset	🗑	☰
Key 2	BLF	*8101	Holiday	🗑	☰
Key 3	BLF	*8102	Default	🗑	☰
Key 4	BLF	*8103	Leo	🗑	☰
Key 5	BLF	*8104	Smith	🗑	☰

- 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: Current inbound calls would be routed to the destination.
- Green: Current inbound calls would NOT be routed to the destination.
- Off: The BLF configurations are incorrect.

> Note:
> If the BLF key is set for Reset feature code, the BLF LED should be off.

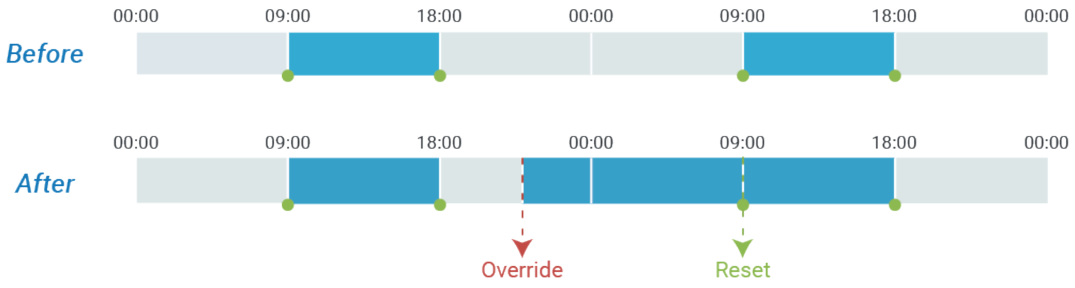
Automatic Reset of Time Condition

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.

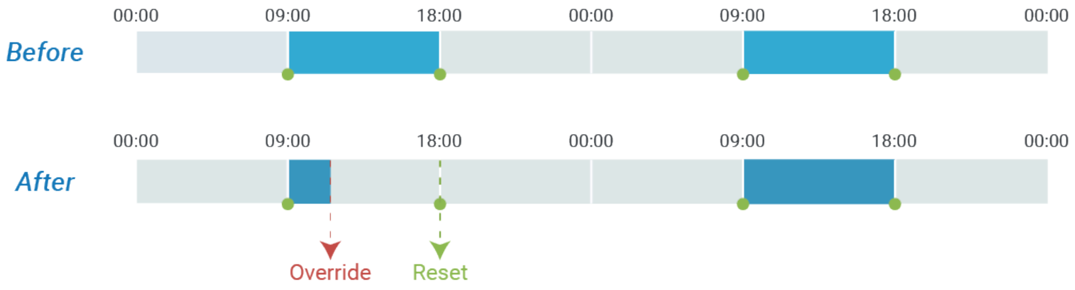
Examples for Global Business Hours/Custom Business Hours

🟦	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

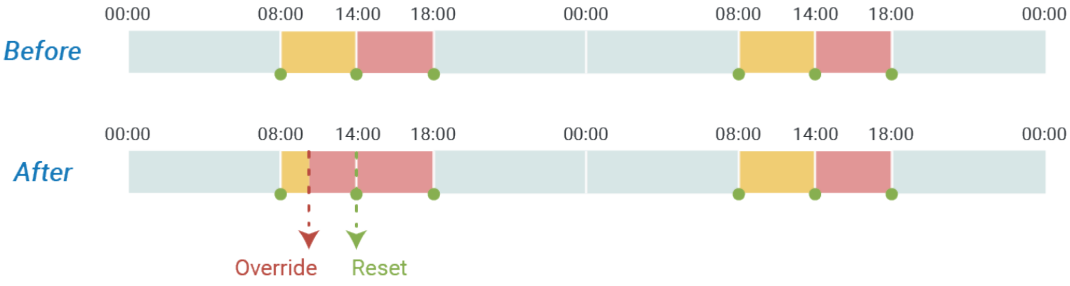


Examples for Custom Time Periods

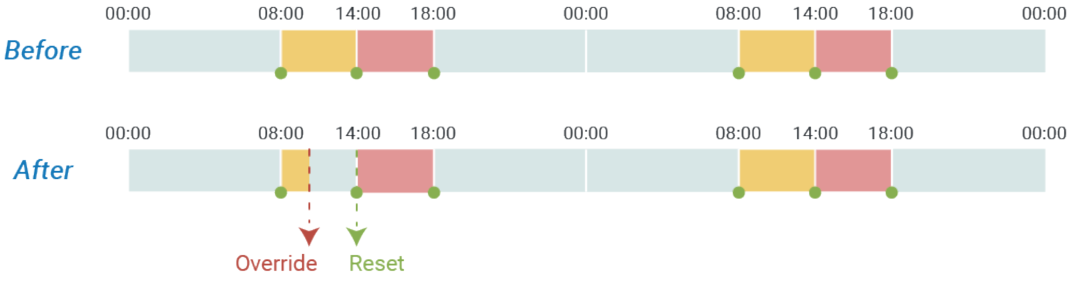
🟨	Time Period 1
🟥	Time Period 2
⬜	Outside Business Hours

●	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



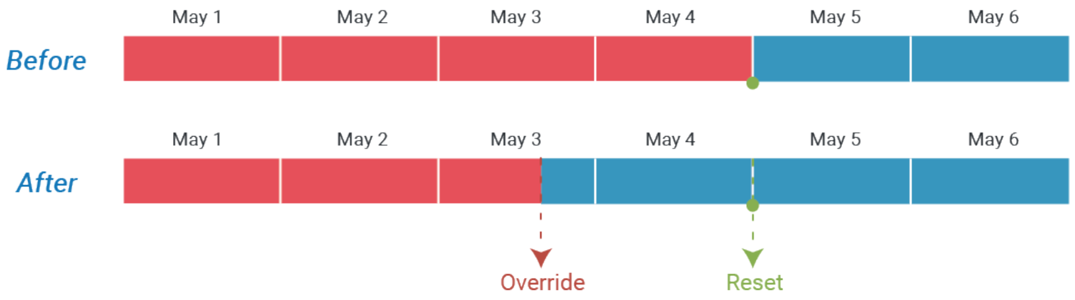
Example 2: Override to Outside Business Hours



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

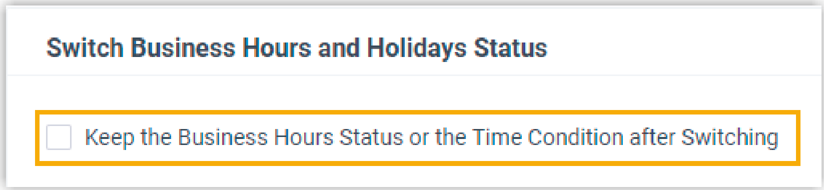
By default, if users have overridden time condition and don't clear the time condition override manually, PBX will automatically reset time condition in next period. You can decide whether to auto reset time condition or keep the time condition after overriding.

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.



Switch Business Hours and Holidays Status

☐ 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.

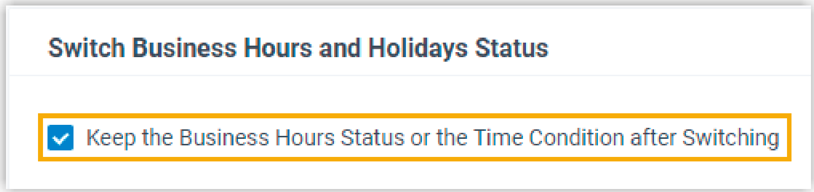
For more information, see Automatic Reset of Time Condition.

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.



Switch Business Hours and Holidays Status

☑ 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 Software Edition has the following types of inbound call routing based on different criteria, such as time, DID numbers, and Caller IDs.

Note:

- If you don't specify any criteria on an inbound route, there will be no restriction on the inbound route. The system will route all inbound calls to the inbound route destination.
- You can set up multiple criteria on an inbound route. For example, route inbound calls based on time and DID number, or route inbound calls based on DID number and Caller ID number.

Time-based call routing

Time-based call routing connects callers to a destination based on the time that they call. The inbound calls are handled differently according to your company's time schedules.

For more information, see the following topics:

- Route Inbound Calls based on Global Business Hours
- Route Inbound Calls based on Department Hours
- Route Inbound Calls based on Employee Hours

DID-based call routing

DID-based call routing connects callers to a destination based on the phone numbers (also known as DID) that the callers dial. Only when the dialed DID numbers match the DID rules on the inbound route will the calls be routed to the destination.

For more information, see Route Inbound Calls based on DID Numbers.

Caller-ID-based call routing

Caller-ID-based call routing allows you to accept or reject calls based on the caller's phone number. Inbound calls that match the Caller ID pattern on PBX will be routed to the pre-configured destination. For those unmatched, calls can not be established.

For more information, see Route Inbound Calls based on Caller ID and Route Inbound Calls by Matched Phonebook Contacts.

Inbound route destinations

Yeastar P-Series Software Edition 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 Software Edition 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. Optional: If you want to route inbound calls based on DID numbers, configure DID Pattern.

   The PBX will route inbound calls only when the callers dial the matched DID numbers.

   > Note:
   > Leave this field blank to match calls with any or no DID information.

   For more information, see Route Inbound Calls based on DID Numbers.
5. Optional: If you want to route inbound calls based on Caller IDs, configure Caller ID Pattern.

   The PBX will route inbound calls only when the Caller IDs match the Caller ID pattern.

   > Note:
   > Leave this field blank to match calls with any or no Caller ID info.

   For more information, see Route Inbound Calls based on Caller ID.
6. In the Trunk section, select the desired trunks from Available box to Selected box.

   The PBX will route inbound calls through this inbound route when external users call the selected trunk number.
7. Configure the inbound route destination.
   - If you want to route inbound calls to one destination whenever the calls reach the system, perform the following operations:
     a. Keep the Time Condition unselected.
     b. Configure the Default Destination.
   - If you want to route inbound calls to different destinations based on the time, perform the following operations:
     a. Select the checkbox of Time Condition.
     b. Select an option from the drop-down list of Time-based Routing Mode.
     c. Configure the destinations based on the time.

        If an inbound call reaches the PBX during the time period, PBX will route the call to the selected destination.

     For more information of inbound call routing based on time, see the following topics:

     - Route Inbound Calls based on Global Business Hours
     - Route Inbound Calls based on Department Hours
     - Route Inbound Calls based on Employee Hours
8. Optional: To receive faxes through this inbound route, enable Fax Detection and configure the fax destination.

- Extension: The faxes will be sent to the selected extension. 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 Global Business Hours

This topic gives a configuration example to describe how to configure inbound route to control inbound calls based on Global Business Hours, which can be applied to most of the employees.

Background information

Assume that your company's business hours are as follows:

- Working days: Monday to Friday
- Business hours: 09:00-12:00 and 14:00-18:00

When customers call in the trunk sip_routein_GBH, you want to route the calls based on the time as follows:

- During business hours, route inbound calls to an IVR for business.
- During a holiday, route inbound calls to another IVR for holiday.
- For other time periods, route inbound calls to a voicemail.

Prerequisites

- The trunk for inbound calling has been set up and is ready for use.
- Global Business Hours is configured according to your company's business hours.
- The desired destination of the inbound route has been configured on the system.

In this scenario, an IVR for business hours, an IVR for holiday should be preconfigured.

For more information of IVR, see Set up an IVR.

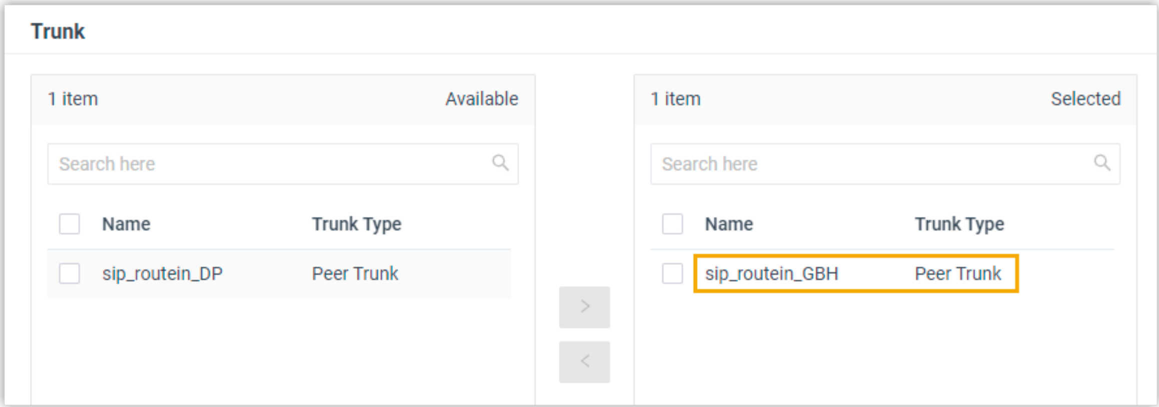
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always directed to your desired destination.

  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 sip_routein_GBH.

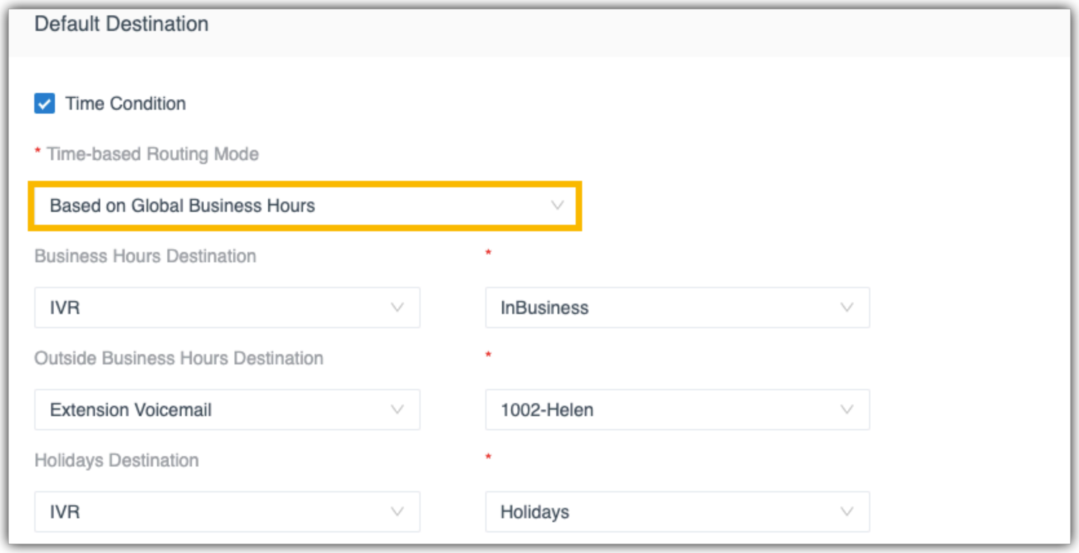


4. In the Default Destination section, complete the following operations:
   a. Select the checkbox of Time Condition.
   b. In the drop-down list of Time-based Routing Mode, select Based on Global Business Hours.
   c. Configure the following destinations based on the time.
      - Business Hours Destination: Select the destination for inbound calls during global business hours.

        In this scenario, select IVR, and select the IVR for business hours.
      - Outside Business Hours Destination: Outside Business Hours is the time periods that are not defined as Business Hours or Holidays.

        In this scenario, select Extension Voicemail then select an extension number.
      - Holidays Destination: Select the destination for inbound calls during holidays.

In this scenario, select IVR, and select the IVR for holidays.



Default Destination

☑ Time Condition

* Time-based Routing Mode

Based on Global Business Hours

Business Hours Destination *

IVR | InBusiness

Outside Business Hours Destination *

Extension Voicemail | 1002-Helen

Holidays Destination *

IVR | Holidays

5. Click Save and Apply.

Result

When customers make calls to the phone number of the selected trunk sip_routein_GBH, the calls will be routed to different destinations based on the time.

Related information

Route Inbound Calls based on Department Hours
Route Inbound Calls based on Employee Hours
Route Inbound Calls based on DID Numbers
Route Inbound Calls based on Caller ID
Route Inbound Calls by Matched Phonebook Contacts

Route Inbound Calls based on Department Hours

This topic gives a configuration example to describe how to configure inbound route to control inbound calls for the departments that maintain different hours from the company's global business hours.

Scenarios

The employees in the branch office's support department have different business hours from the head office. The department hours is listed as below:

- Working days: Monday to Friday
- Business hours: 21:00 - 23:00 and 00:00 - 05:00

When customers call in the trunk sip_routein_DP, you want to route the calls based on the time as follows:

- During business hours, route inbound calls to the support team's queue.
- During a holiday, route inbound calls to another IVR for holiday.
- For other time periods, route inbound calls to a voicemail.

Prerequisites

- The trunk for inbound calling has been set up and is ready for use.
- The desired destination of the inbound route should be configured on the system.

  In this scenario, a queue and an IVR for holiday should be preconfigured.

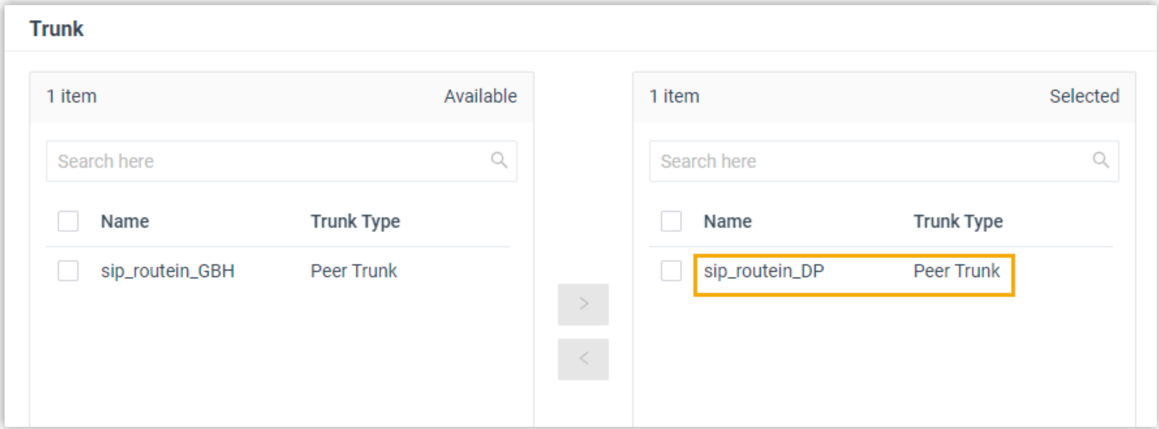
  For more information about the configurations of queue and IVR, see Create a Queue and Set up an IVR.
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always 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 sip_routein_DP.



Trunk

1 item Available

Search here

□	Name	Trunk Type
□	sip_routein_GBH	Peer Trunk

1 item Selected

Search here

□	Name	Trunk Type
□	sip_routein_DP	Peer Trunk

4. In the Default Destination section, complete the following operations:
   a. Select the checkbox of Time Condition.

b. In the drop-down list of Time-based Routing Mode, select Based on Custom Business Hours.

c. Configure custom business hours.

   i. Click Add Custom Business Hours.

   ii. In the 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.

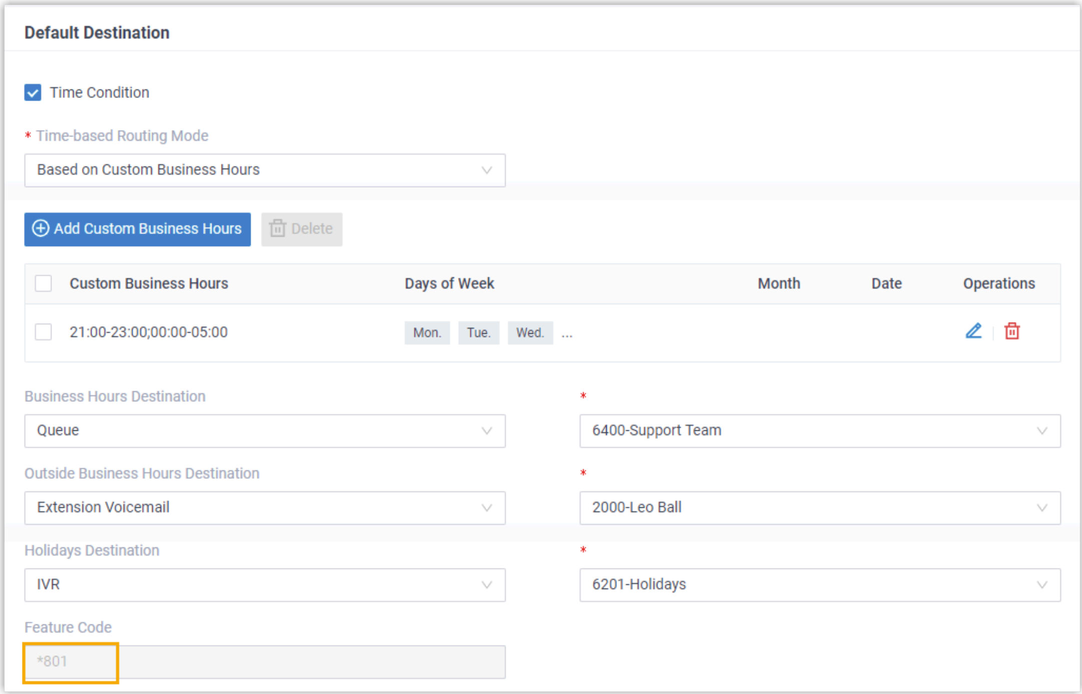
d. Configure the following destinations based on the time.

   - Business Hours Destination: Select the destination for inbound calls during business hours.

     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.

     In this scenario, select IVR, and select the IVR for holidays.



Default Destination

☑ Time Condition

* Time-based Routing Mode: Based on Custom Business Hours

□	Custom Business Hours	Days of Week	Month	Date	Operations
□	21:00-23:00;00:00-05:00	Mon. Tue. Wed. ...			

Business Hours Destination: Queue | * 6400-Support Team

Outside Business Hours Destination: Extension Voicemail | * 2000-Leo Ball

Holidays Destination: IVR | * 6201-Holidays

Feature Code: *801

5. Click Save and Apply.

Result

- When customers make calls to the phone number of the selected trunk sip_routein_-DP, 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 Global Business Hours
Route Inbound Calls based on Employee Hours
Route Inbound Calls based on DID Numbers
Route Inbound Calls based on Caller ID
Route Inbound Calls by Matched Phonebook Contacts

Route Inbound Calls based on Employee Hours

This topic gives a configuration example to describe how to configure inbound route to control inbound calls for individual employees who have their own work schedules.

Scenarios

Duty doctors in a hospital are responsible for supporting emergency patient needs or arranging appointments for patients over phone calls.

- Each duty doctor has a different time schedule and will provide services based on the time schedule.
- During the time periods that no doctors are on duty or when it comes to a holiday, the incoming calls from patients will be routed to an IVR.

The following shows time schedule for the duty doctors.

Doctor Name	Time Schedule
Dr. Tommy Tse	Monday 07:00 -12:00 Friday 12:00 - 18:00
Dr. Eric Chan	Monday 00:00 - 07:00 Thursday 07:00 - 12:00

Prerequisites

- The trunk for inbound calling has been set up and is ready for use.
- The desired destination of the inbound route should be configured on the system.

In this scenario, an IVR should be configured to ensure that patients can reach their desired services.

For more information about IVR, see Set up an IVR.

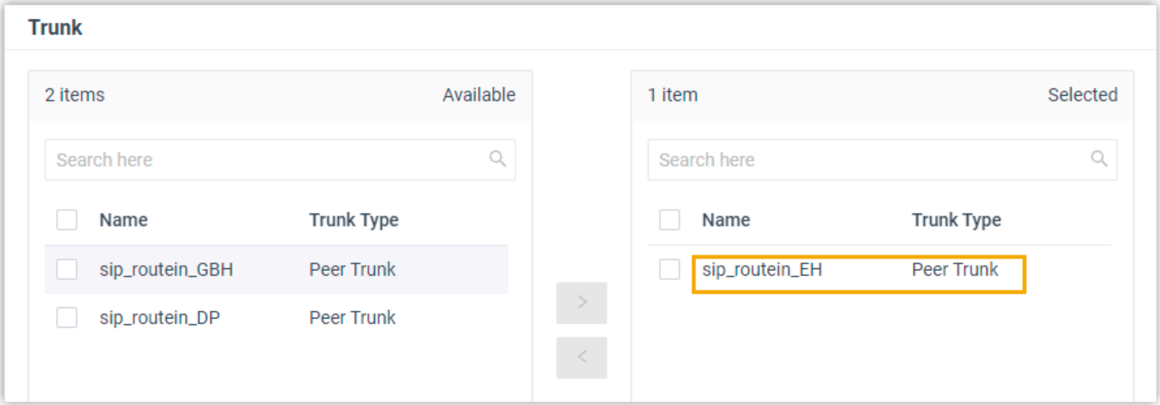
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always directed to your desired destination.

  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 sip_routein_EH.



Trunk

2 items Available

Search here

□	Name	Trunk Type
□	sip_routein_GBH	Peer Trunk
□	sip_routein_DP	Peer Trunk

1 item Selected

Search here

□	Name	Trunk Type
□	sip_routein_EH	Peer Trunk

4. In the Default Destination section, complete the following operations:
   a. Select the checkbox of Time Condition.
   b. In the drop-down list of Time-based Routing Mode, select Based on Custom Time Periods.
   c. Add time schedule for the duty doctors.
      i. Click Add Custom Time Periods.
      ii. In the pop-up window, click Add to add time periods, 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.

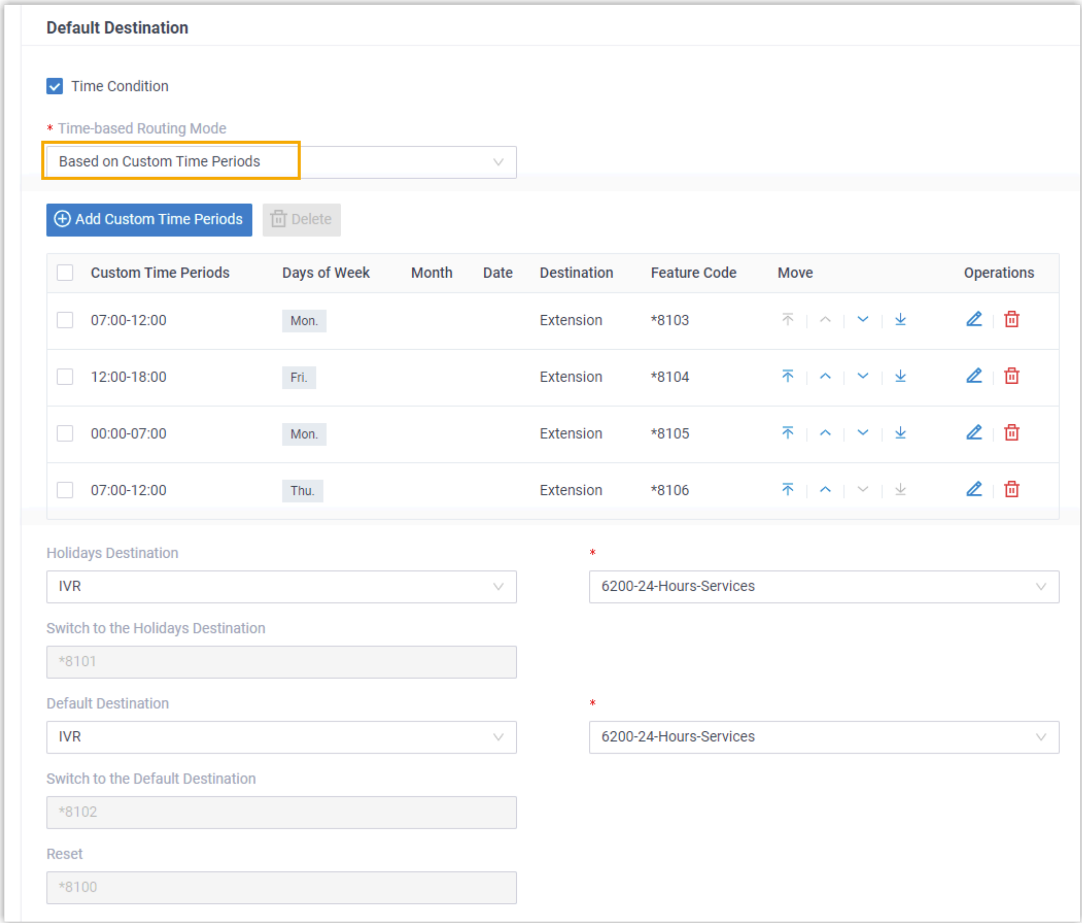
Start Time	End Time	Days of Week	Destination
07:00	12:00	Monday	Tommy's extension
12:00	18:00	Friday	Tommy's extension
00:00	07:00	Monday	Eric's extension
07:00	12:00	Thursday	Eric's extension

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.



Default Destination

☑ Time Condition

* Time-based Routing Mode: Based on Custom Time Periods

□	Custom Time Periods	Days of Week	Month	Date	Destination	Feature Code	Move	Operations
□	07:00-12:00	Mon.			Extension	*8103		
□	12:00-18:00	Fri.			Extension	*8104		
□	00:00-07:00	Mon.			Extension	*8105		
□	07:00-12:00	Thu.			Extension	*8106		

Holidays Destination: IVR | * 6200-24-Hours-Services

Switch to the Holidays Destination: *8101

Default Destination: IVR | * 6200-24-Hours-Services

Switch to the Default Destination: *8102

Reset: *8100

5. Click Save and Apply.

Result

- When external users make calls to the selected trunk sip_routein_EH, 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.

> ℹ 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 Global Business Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on DID Numbers
Route Inbound Calls based on Caller ID
Route Inbound Calls by Matched Phonebook Contacts

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 Software Edition provides three DID matching modes to help you route inbound calls based on DID numbers.

- Match DID Range to Extension Range

  Match DID Range and Extension Range in one-to-one correspondence.

See configuration example Route calls to extension users by matching DID range.

- Match DID Pattern to Extensions

  Use the variable `{{.Ext}}` to match extension number in the DID pattern.

  See configuration example Route calls to extension users by matching specific DIDs.
- DID Pattern

  The calls match the defined DID(s) will be routed to a defined destination.

  See configuration example Route calls to a specific destination by matching DID patterns.

Route calls to extension users by matching DID range

Background information

Company ABC purchases a SIP trunk, and gets 10 DID numbers that are in order: 8823201-8823210.

The company wants to redirect inbound calls to specific extensions based on the provided DID numbers as follows:

Table 33.

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

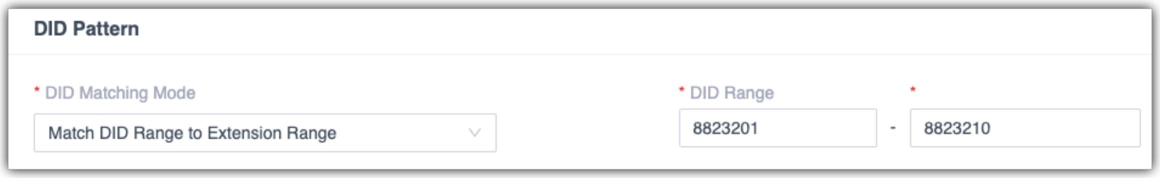
- You have purchased DID numbers from the trunk provider.
- The trunk for inbound calling has been set up and is ready for use.

Configuration example

According to this scenario, configure an inbound route based on DIDs as follows:

- Name: Enter a name to help you identify it.
- DID Pattern:
    - DID Matching Mode: Select Match DID Range to Extension Range.
    - DID Range: Enter the start number and the end number of the DID range.

      In this scenario, enter 8823201 and 8823210.



DID Pattern

* DID Matching Mode: Match DID Range to Extension Range

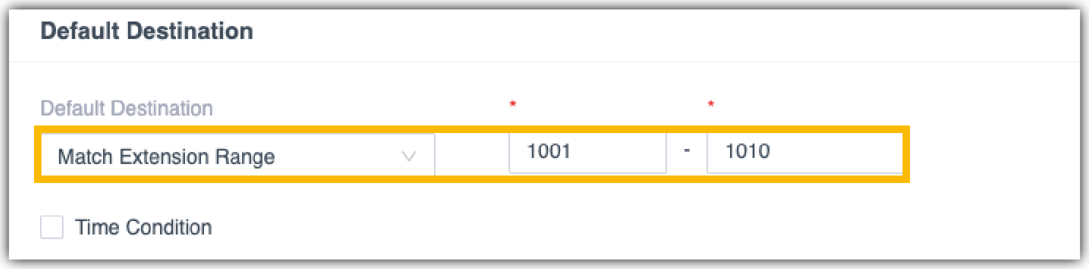
* DID Range: 8823201 - 8823210

- Caller ID Pattern: Leave it blank, which means no limit on the inbound caller ID.
- Trunk: Select the trunk that binds the DID numbers.
- Default Destination: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this scenario, route inbound calls to the default destination whenever the calls reach the system.

    - Default Destination: Select Match Extension Range, and enter the extension range 1001 - 1010.

      Note:
      The DID range and extension range should have the same size (for example, DID range 991000-991003 and the extension range 1000-1003 have the same size).
    - Time Condition: Unselected.



Default Destination

Default Destination: Match Extension Range * 1001 - * 1010

□ Time Condition

- Fax Detection: Leave the settings as default.

Result

When an external user dials a number that is in the DID range, the user can reach a corresponding extension user directly.

For example, if an external user dials 8823201, the call goes to the extension 1001 directly.

Route calls to extension users by matching specific DIDs

Scenarios

Company ABC purchases a SIP trunk, and gets 3 DID numbers as follows.

- 8821001, 8821006, 8821016

The company wants to redirect inbound calls to specific extensions based on the provided DID numbers as follows:

> Note:
> The provided DIDs have the following characteristics:
>
> - Not consecutive
> - Each DID number consists of a string of fixed digits and a specific extension number.

Table 34.

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.

Configuration example

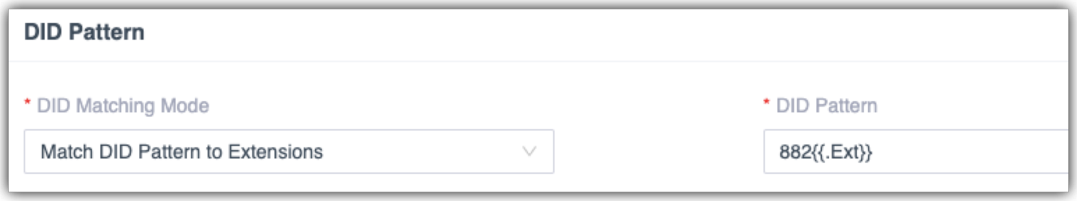
According to this scenario, configure an inbound route based on DIDs as follows:

- Name: Enter a name to help you identify it.
- DID Pattern:
  - DID Matching Mode: Select Match DID Pattern to Extensions.
  - DID Pattern: Enter the DID pattern according to the provided DIDs.

    In this scenario, enter 882{{.Ext}} .

    > Note:
    > - {{.Ext}} is a variable that will match the destination extension.
    > - The wildcard `.` and `!` are not allowed.

- Only one DID pattern is allowed.



DID Pattern

* DID Matching Mode: Match DID Pattern to Extensions

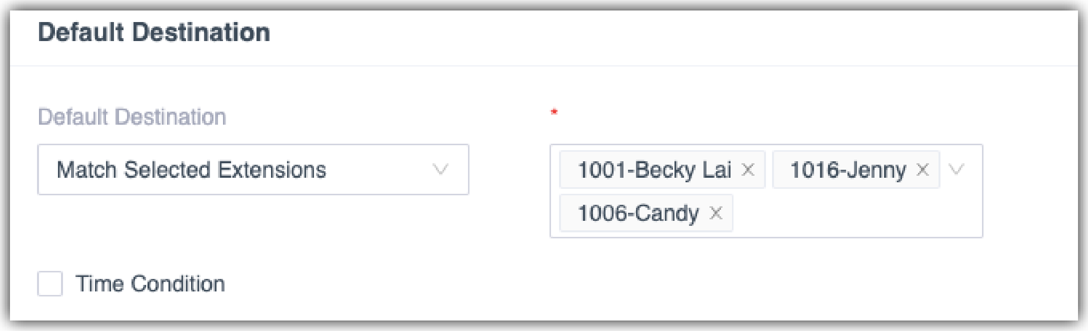
* DID Pattern: 882{{.Ext}}

- Caller ID Pattern: Leave it blank, which means no limit of inbound caller ID.
- Trunk: Select the trunk that binds the DID numbers.

  In this scenario, select siptrunk.
- Default Destination: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this scenario, route inbound calls to the default destination whenever the calls reach the system.
  - Default Destination: Select Match Selected Extensions, and select extensions.

    In this scenario, select extension 1001, 1006, and 1016.
  - Time Condition: Unselected.



Default Destination

Default Destination: Match Selected Extensions

*: 1001-Becky Lai × 1016-Jenny × 1006-Candy ×

□ Time Condition

- Fax Detection: Leave the settings as default.

Result

When an external user dials a number that matches the DID pattern, the user can reach a specific extension user directly.

For example, if the external user dials 8821001, the call goes to the extension 1001 directly.

Route calls to a specific destination by matching DID patterns

Scenario

Company ABC purchases a SIP trunk, and gets 2 DID numbers as follows.

- 88866608
- 88866609

The company wants to assign the two DID numbers to support team and sales team.

- When external users call 88866609, the calls go directly to support team.
- When external users call 88866608, the calls go directly to sales team.

Prerequisites

- You have purchased DID numbers from the trunk provider.
- The trunk for inbound calling has been set up and is ready for use.

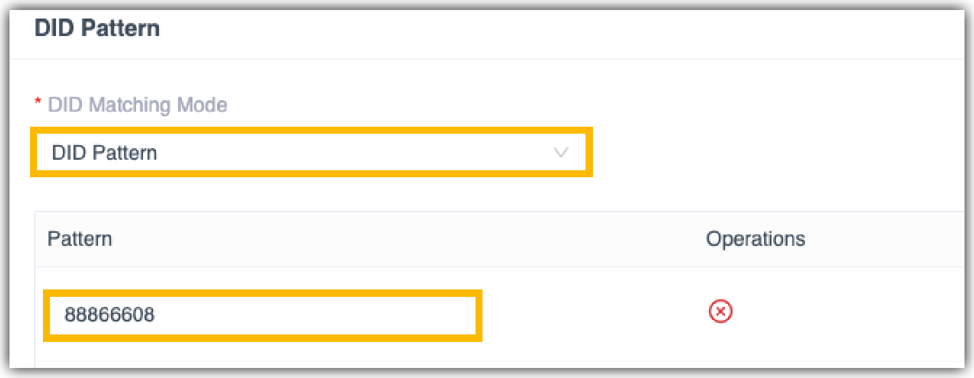
Configuration example

Set up two inbound routes to route calls to different destinations based on DID numbers.

Inbound Route for sales team

- Name: Enter a name to help you identify it.
- DID Pattern:
    - DID Matching Mode: Select DID Pattern.
    - DID Patterns: Click Add and enter a DID pattern or a DID number.

      In this scenario, enter 88866608.



DID Pattern

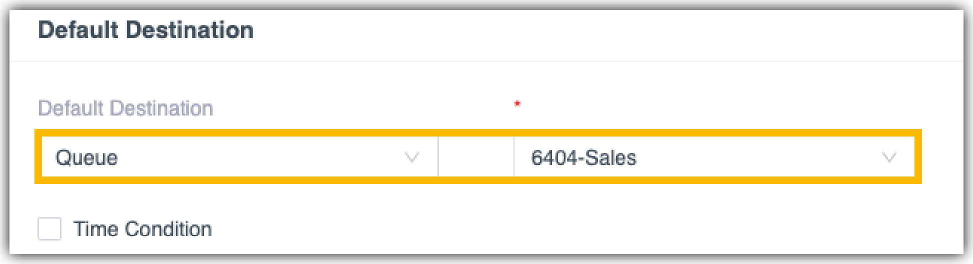
* DID Matching Mode: DID Pattern

Pattern	Operations
88866608	⊗

- Caller ID Pattern: Leave it blank, which means no limit of inbound caller ID.
- Trunk: Select the trunk that binds the DID numbers.
- Default Destination: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this example, route inbound calls to the default destination whenever the calls reach the system.

    - Default Destination: Select the destination to the queue of sales team.
    - Time Condition: Unselected.



Default Destination

Default Destination *

Queue 6404-Sales

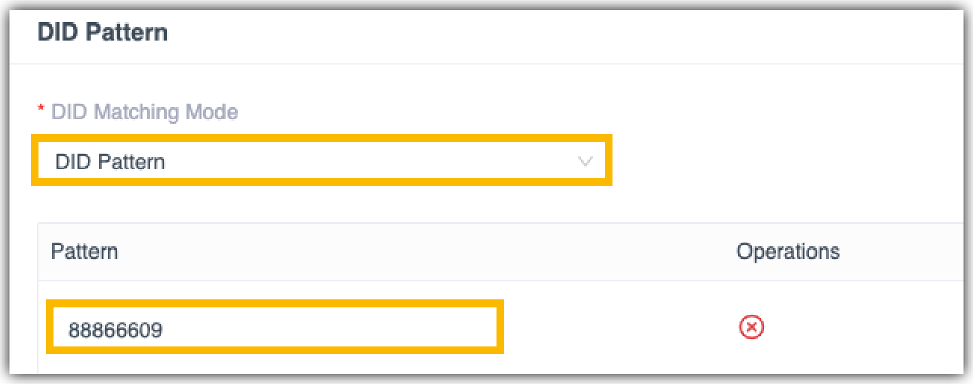
□ Time Condition

- Fax Detection: Leave the settings as default.

Inbound Route for support team

- Name: Enter a name to help you identify it.
- DID Pattern:
    - DID Matching Mode: Select DID Pattern.
    - DID Patterns: Click Add and enter a DID pattern or a DID number.

      In this scenario, enter 88866609.



DID Pattern

* DID Matching Mode

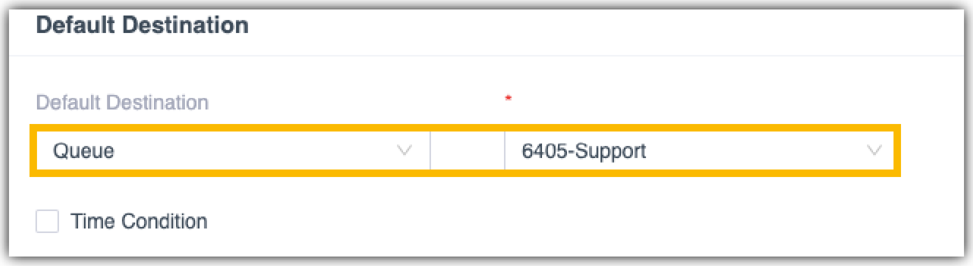
DID Pattern

Pattern	Operations
88866609	⊗

- Caller ID Pattern: Leave it blank, which means no limit of inbound caller ID.
- Trunk: Select the trunk that binds the DID numbers.
- Default Destination: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this example, route inbound calls to the default destination whenever the calls reach the system.

    - Default Destination: Select the destination to the queue of support team.
    - Time Condition: Unselected.



Default Destination

Default Destination *

Queue | 6405-Support

- Fax Detection: Leave the settings as default.

Result

External users will reach different teams according to the DID numbers they dial.

Related information

- Route Inbound Calls based on Global Business Hours
- Route Inbound Calls based on Department Hours
- Route Inbound Calls based on Employee Hours
- Route Inbound Calls based on Caller ID
- Route Inbound Calls by Matched Phonebook Contacts

Route Inbound Calls based on Caller ID

Caller ID routing connects external callers with the appropriate party quickly. This topic gives a configuration example to describe how to route calls by a caller-ID-based inbound route.

Scenarios

Company ABC is a Chinese company that provides consulting services around multiple cities.

For better customer experience, the company has a countrywide toll-free number 400-661-8815 and has multiple teams to provide professional services for customers from different regions.

For example, the following two teams will handle inbound calls based on different caller IDs.

Table 35.

Team	Responsible Region	Area Code
Team-A	Fujian	• 0591 • 0592 • 0593 • 0594 • 0595 • 0596

Table 35. (continued)

Team	Responsible Region	Area Code
		• 0597 • 0598 • 0599
Team-B	Guangdong	• 0662 • 0663 • 0668 • 0660

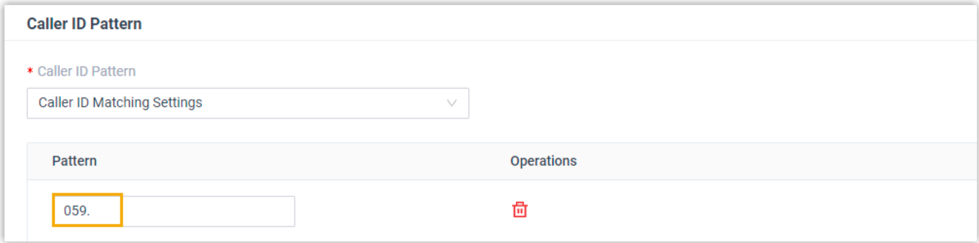
Configuration Example

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.

  Caller ID Pattern

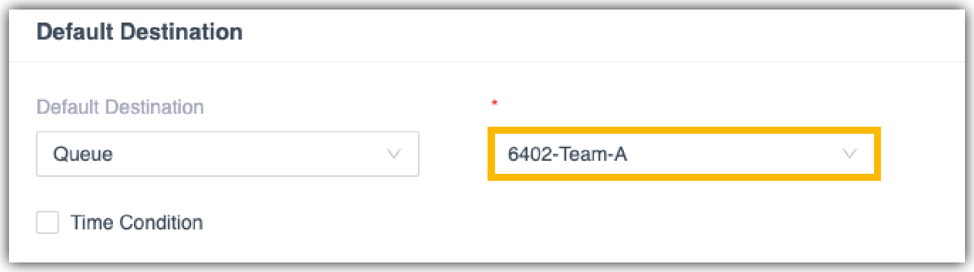
  * Caller ID Pattern: Caller ID Matching Settings

Pattern	Operations
059.	🗑

- 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.



Default Destination

Default Destination: Queue | 6402-Team-A

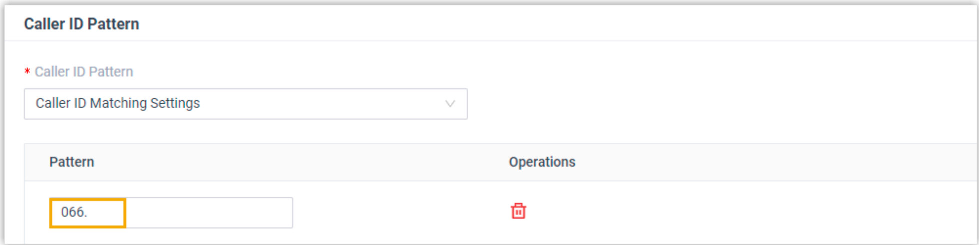
□ Time Condition

- Fax Detection: Leave the settings as default.

Inbound Route for Team-B

- Name: Enter a name to help you identify it.
- DID Pattern: Leave it blank, which means no limit of DID numbers.
- Caller ID Pattern: Select Caller ID Matching Settings, click Add and enter a Caller ID pattern or a full Caller ID.

  In this scenario, enter `066.`, which matches all inbound Caller IDs that start with digit 066. For more information of Caller ID pattern, see [DID Pattern and Caller ID Pattern](#).



Caller ID Pattern

* Caller ID Pattern: Caller ID Matching Settings

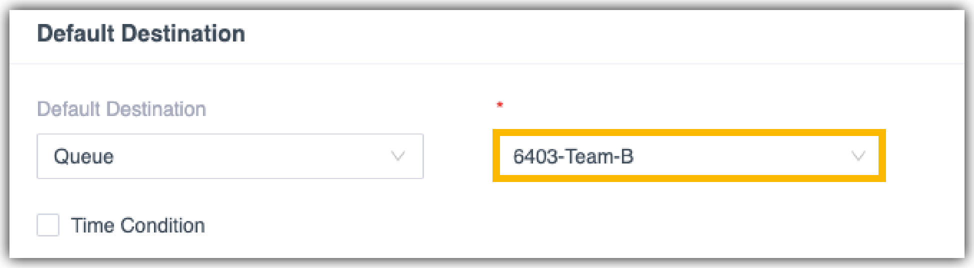
Pattern	Operations
066.	🗑

- Trunk: Select the trunk that users will call in.

  In this example, select siptrunk, whose phone number is 400-661-8815.
- Default Destination: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this example, route inbound calls to the default destination whenever the calls reach the system.

  - Default Destination: Select the destination to the queue of Team-B.
  - Time Condition: Unselected.



Default Destination

Default Destination: Queue | 6403-Team-B

□ Time Condition

- Fax Detection: Leave the settings as default.

Result

- When users from Fujian dial the number 400-661-8815, agents in Team-A will handle the calls.
- When users from Guangdong dial the number 400-661-8815, agents in Team-B will handle the calls.

Related information

Route Inbound Calls based on Global Business Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on Employee Hours
Route Inbound Calls based on DID Numbers
Route Inbound Calls by Matched Phonebook Contacts

Route Inbound Calls by Matched Phonebook Contacts

After grouping company contacts into phonebooks, you can set up inbound routes to distribute inbound calls from contacts to different destinations based on phonebooks.

Prerequisites

- You have added phonebooks and enabled Caller ID Match feature.

  For more information, see Manage Company Phonebooks and Identify Callers from Contacts.

Scenario

Company ABC has a Sales Team and a Support Team, both teams have their own customer groups. System administrator has added the customer information into two phonebooks.

Table 36.

Team	Phonebook
Sales Team (Queue 6401)	Customers_Abroad
Support Team (Queue 6402)	Customers_China

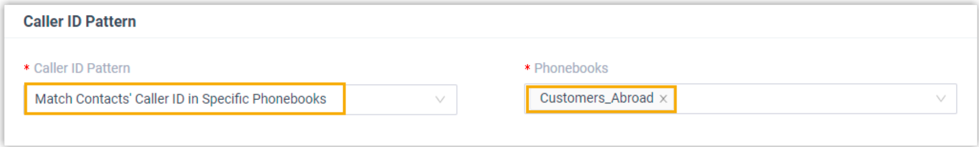
Configuration Example

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.



Caller ID Pattern

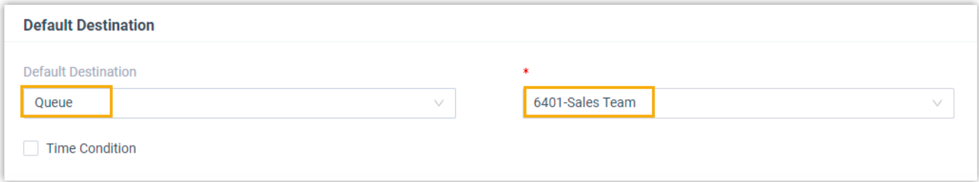
* Caller ID Pattern: Match Contacts' Caller ID in Specific Phonebooks

* Phonebooks: Customers_Abroad

- Trunk: Select the trunk that contacts will call in.
- Default Destination: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this example, route inbound calls to the default destination whenever the calls reach the system.

  - Default Destination: Select the destination to Queue and select the Sales Team.
  - Time Condition: Unselected.



Default Destination

Default Destination: Queue

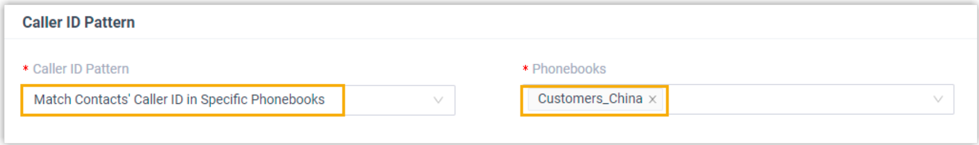
* 6401-Sales Team

□ Time Condition

- Fax Detection: Leave the settings as default.

Inbound Route for Support Team

- Name: Enter a name to help you identify it.
- DID Pattern: Leave it blank, which means no limit of DID numbers.
- Caller ID Pattern: Select Match Contacts' Caller ID in Specific Phonebooks and select the phonebook Customers_China.



Caller ID Pattern

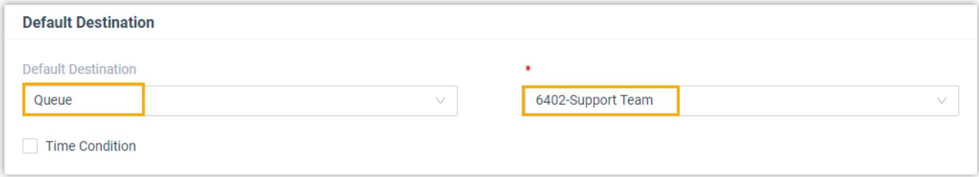
* Caller ID Pattern: Match Contacts' Caller ID in Specific Phonebooks

* Phonebooks: Customers_China

- Trunk: Select the trunk that contacts will call in.
- Default Destination: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this example, route inbound calls to the default destination whenever the calls reach the system.

  - Default Destination: Select the destination to Queue and select Support Team.
  - Time Condition: Unselected.



Default Destination

Default Destination

Queue | * 6402-Support Team

□ Time Condition

- Fax Detection: Leave the settings as default.

Result

- When customers from Phonebook 'Customers_Abroad' call to PBX, Sales Team will handle the calls.
- When customers from Phonebook 'Customers_China' call to PBX, Support Team will handle the calls.

Related information

Route Inbound Calls based on Caller ID
Route Inbound Calls based on DID Numbers
Route Inbound Calls based on Employee Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on Global Business Hours

Manage Inbound Routes

After you create inbound routes, you can adjust the priority of the inbound routes. You can also edit or delete the inbound routes.

Adjust priority of inbound routes

A trunk can be selected to multiple inbound routes. When users call to a trunk that is selected in multiple inbound routes, the system will route inbound calls through the route with higher priority. You can adjust the priority of inbound routes according to your needs.

1. Log in to PBX 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 Software Edition 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 Extension and Trunk > Call Control > Inbound Route.
2. Click Export.

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

Import inbound routes

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

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 50 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information , see Inbound Route Parameters.

Procedures

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

The inbound routes in the CSV file will be displayed in the Inbound Route list.

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 37.

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 38.

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 Software Edition 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 Software Edition 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 Software Edition.

Background information

Yeastar P-Series Software Edition 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 Global Business Hours: Set up whether to allow this route in the following time separately:
     - Business Hours: Global Business Hours specified in the system.
     - Holidays: Holidays specified in the system.
     - Outside Business Hours: The time periods that are not defined as Business Hours or Holidays.

    - Based on Custom Business Hours: Set up custom business hours and configure whether to allow this route in the following time:
        - Business Hours: The custom business hours.
        - Holidays: Holidays specified in the system.
        - Outside Business Hours: The time periods that are not defined as Business Hours or Holidays.
    - Based on Custom Time Periods: Set up multiple time periods for this route. You can also specify whether to allow this route in the Holidays.
7. Click Save and Apply.

What to do next

After you finish the outbound route configurations, you need to check and adjust the priority of your outbound routes, so that the system can match and route the call out through the proper outbound route.

For more information, see Adjust priority of outbound routes.

Restrict Outbound Calls by PIN Codes

Many companies restrict the outbound calls by using PIN codes. You can set multiple PIN codes, and assign these PIN codes to different users. Users are required to dial a specified PIN code to make an outbound call via the restricted outbound route. In this way, you can easily track the calls made by different users.

Prerequisites

You need to add a PIN list or several PIN lists. For more information, see Add a PIN List.

Procedure

1. Log in to PBX web portal, go to Call Control > Outbound Route.
2. Click ✎ beside the desired outbound route.
3. On the outbound route configuration page, go to Trunk section, and in the Outbound Route Password drop-down list, select PIN List.
4. In the PIN List drop-down list, select the desired PIN list.
5. Click Save and Apply.

Result

- To make an outbound call via the restricted outbound route, users need to enter a correct PIN code included in the selected PIN list.
- When users enter wrong PIN codes for three times, the call will be hung up automatically.
- If the Record in CDR option of PIN list is enabled, the Call Detailed Record (CDR) will display the PIN code of each call.

Manage Outbound Routes

After you create outbound routes, you can adjust the priority of the outbound routes. You can also edit or delete the outbound routes.

Adjust priority of outbound routes

When a user places a call, if the dialed number matches multiple dial patterns, the outbound route with the highest priority will be used. You can adjust the priority of outbound routes to route calls through proper outbound routes.

> Note:
>
> The route priority is important, especially if there is some overlap. For example, the number 5503305 matches both dial patterns of `ZXXXXXX` and `X.`, the PBX will send the call through the outbound route with the highest priority.

Example:

When users dial 05503301, both of the two outbound routes match 05503301:

- Outbound Route-Long-distance call: The dial pattern is `0XXXXXXX` and uses trunk 1.
- Outbound Route-Local call: The dial pattern is `X.` and uses trunk 2.

To call 5503301 through trunk 1, you need to prioritize the outbound route of "Long-distance call"; or PBX will match the outbound route of “Local call" and route the call out using trunk 2.

1. Log in to PBX web portal, go to Call Control > Outbound Route.
2. Click the buttons ⤒ ⌃ ⌄ ⤓ to adjust the priority of your outbound routes.

   > Note:
   >
   > PBX will match outbound route from top to bottom.

Edit an outbound route

1. Log in to PBX 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 Software Edition 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 Extension and Trunk > Call Control > Outbound Route.
2. Click Export.

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

Import outbound routes

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

Prerequisites

Requirements of an imported file:

- Format: UTF-8 .CSV
- Size: Less than 50 MB
- File name: Less than 127 characters
- Import parameters: Ensure that the import parameters meet requirements. For more information , see Outbound Route Parameters.

Procedure

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

   The outbound routes in the CSV file will be displayed in the Outbound Route list.

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.
`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 one or more characters. Example: 9011! matches any numbers starting with 9011 (including 9011 itself).

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.

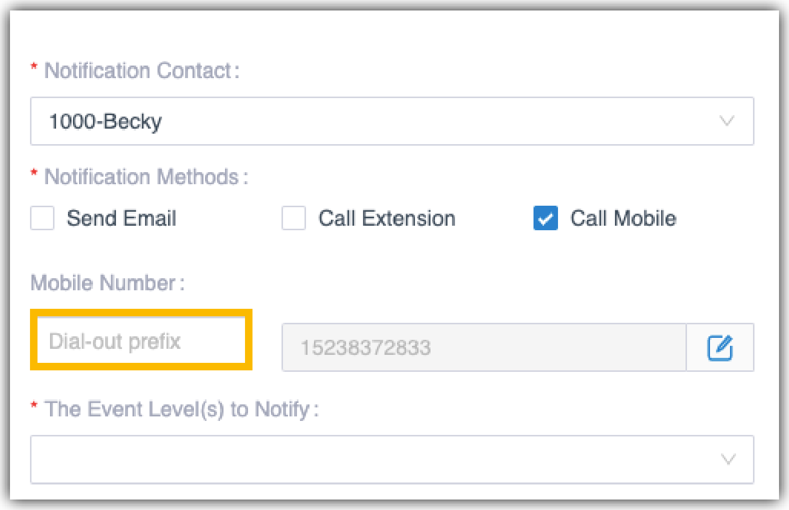
Prefix and Dial Pattern

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.



* Notification Contact:

1000-Becky

* Notification Methods:

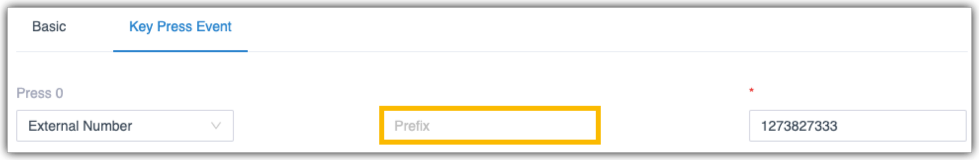
□ Send Email □ Call Extension ☑ Call Mobile

Mobile Number:

Dial-out prefix | 15238372833

* The Event Level(s) to Notify:

- External number for IVR keypress.



Press 0

External Number | Prefix | 1273827333

How to configure Prefix

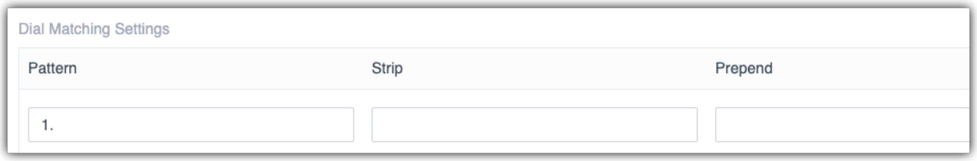
You need to configure prefix according to the dial pattern settings on your outbound route. If the prefix is not configured correctly, the PBX cannot call to the external number successfully.

- Leave Prefix setting blank

  If the Strip of outbound route is not set, you don't have to add a prefix before the phone number.

  As the following figure shows, only the destination number that starts with digit 1 can be called out through this outbound route.

  For example, to call number 125451, you should dial the number 125451 directly.



Dial Matching Settings

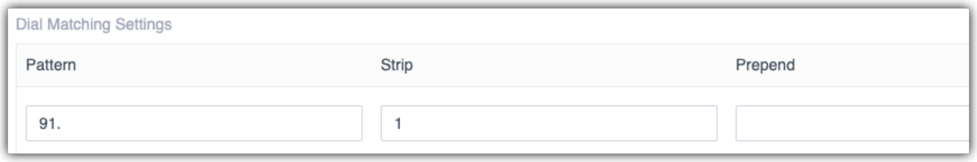
Pattern	Strip	Prepend
1.		

- Add prefix before a number

  If Strip is set on an outbound route, you need to set the prefix according to the Pattern.

As the following figure shows, to make calls through the outbound route, you need to add prefix 9 before the number, and the destination number should start with digit 1.

For example, to call number 125451, you should add prefix 9 before the number 125451.



Dial Matching Settings

Pattern	Strip	Prepend
91.	1	

Dial Pattern Examples

This topic provides sample dial patterns to help you understand dial patterns of outbound route.

Local calls

In Xiamen, China, local numbers are all 7-digit numbers and the numbers do not start with 0, such as 5503305.

For the local calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
`ZXXXXXX`	Leave it blank.	Leave it blank.

Long distance calls

In Xiamen, China, users need to dial 4-digit area code and 7-digit local number to make a long distance call, such as 0595-7588123.

- Area code format: 0ZXX, the first digit is 0, and the second digit cannot be 0.
- Local number format: 7-digit number that does not start with 0.

For long distance calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
`0ZXXZXXXXXX`	Leave it blank.	Leave it blank.

Mobile calls

All mobile phone numbers in China are 11-digit numbers and start with digit 1, such as 15880260666.

For mobile calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
1XXXXXXXXXX	Leave it blank.	Leave it blank.

International calls

All international numbers start with digits 00.

For international calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
00.	Leave it blank.	Leave it blank.

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

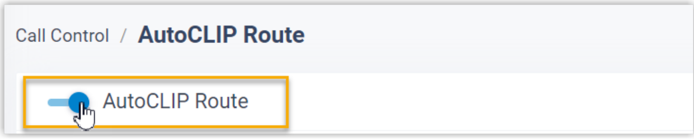
With AutoCLIP feature, Yeastar P-Series Software Edition can route inbound calls from customers to original extension users who placed the calls. This intelligent call matching feature can greatly improve work efficiency and customer satisfaction. This topic describes how to set up the AutoCLIP route.

Prerequisites

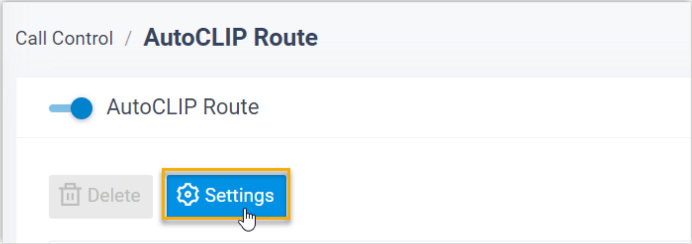
Make sure the desired trunk purchased from trunk provider has the Caller ID feature, or the PBX can not distinguish the Caller ID and implement AutoCLIP.

Procedure

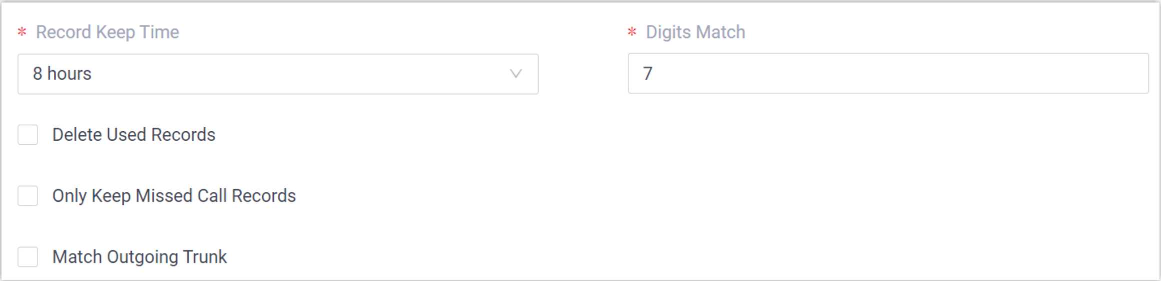
1. Log in to PBX web portal, go to Call Control > AutoCLIP Route.
2. On the top of the page, enable the AutoCLIP Route feature.



3. Click Settings to set up rules for AutoCLIP route.



4. Configure the AutoCLIP settings according to your needs.



* Record Keep Time	* Digits Match
8 hours	7

□ Delete Used Records

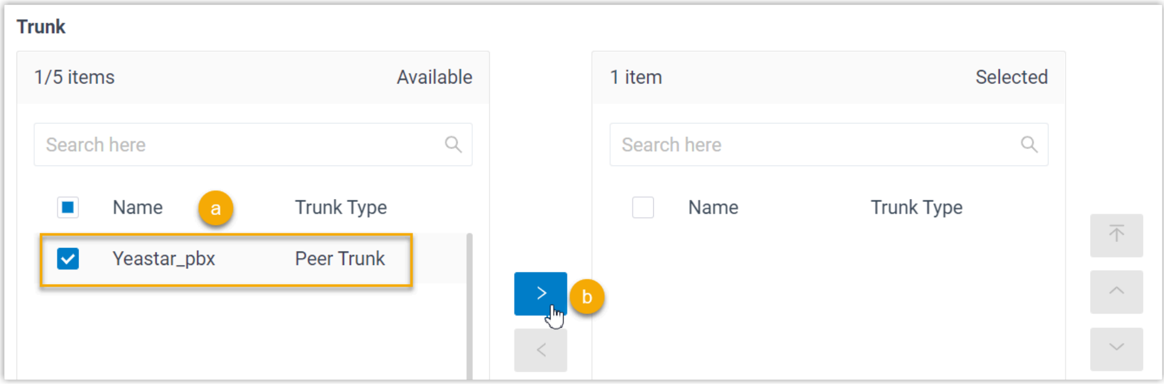
□ Only Keep Missed Call Records

□ Match Outgoing Trunk

Table 39.

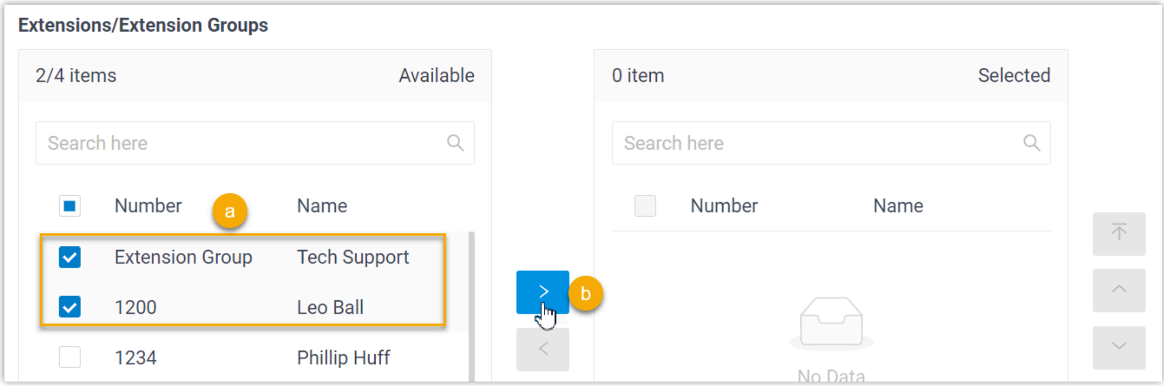
Setting	Description
Record Keep Time	Set how long records can be kept in AutoCLIP list. If keep time of a record exceeds the value, PBX will automatically delete the record. Tip: You can check the expiration time in the AutoCLIP record list directly.
Digits Match	Define how many digits from the last 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.
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.



Extensions/Extension Groups

2/4 items Available

Search here

■	Number	Name
☑	Extension Group	Tech Support
☑	1200	Leo Ball
□	1234	Phillip Huff

0 item Selected

Search here

□	Number	Name

No Data

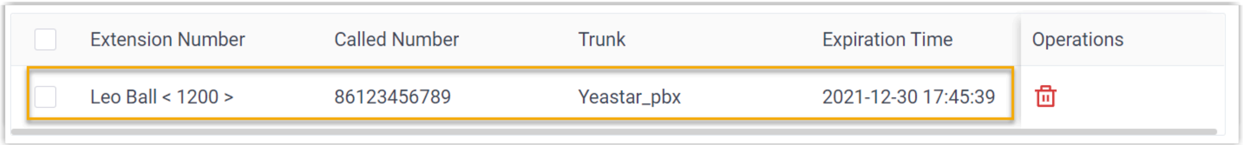
   a. Select the desired extension(s)/extension group(s).
   b. Add the extension(s)/extension group(s) from Available box to Selected box.

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.



□	Extension Number	Called Number	Trunk	Expiration Time	Operations
□	Leo Ball < 1200 >	86123456789	Yeastar_pbx	2021-12-30 17:45:39	🗑

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 Software Edition.

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.

DID usages

Yeastar P-Series Software Edition 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 Software Edition.

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.

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. In the pop-up window, click Add and configure the DID.
   - DID/DDI: Enter the provided DID number.
   - DID/DDI Name: Bind a name with the DID number.

     When the DID number is dialed, the name will be displayed on the called party's device.
4. Click Save and Apply.

Delete DID numbers

1. Log in to PBX 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 Software Edition 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.

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 Software Edition.

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 Software Edition 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 Software Edition, you can configure outbound caller ID based on the following features:

- Emergency Numbers
- Outbound Route
- Trunk
- Extension

For more information, see Customize Outbound Caller IDs.

Inbound caller ID

Inbound caller ID is an external user's phone number that will be displayed on an extension user's phone when the external user calls in Yeastar P-Series Software Edition.

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.

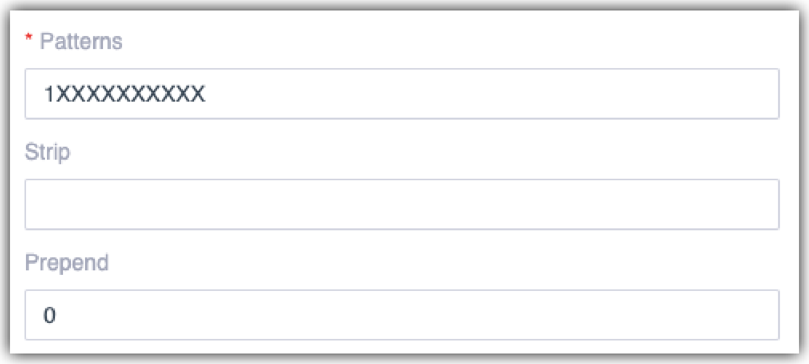
    > Note:
    >
    > If both Strip and Prepend are configured, the system will first strip the leading digits then add the prepend digits to the inbound caller ID.
5. Click Save and Apply.

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

Prepend

0

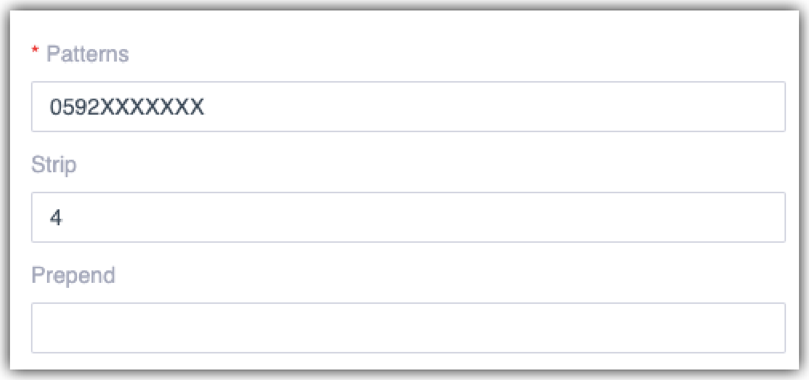
- Patterns: 1XXXXXXXXXX
- Strip: Leave it blank.
- Prepend: 0

Example 2

Company B wants all local numbers to be displayed without area code (0592).

For example, company B wants to display number 5503301 instead of 05925503301.

In this case, you can configure the reformatting rule as below:



* Patterns

0592XXXXXXX

Strip

4

Prepend

- 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 Software Edition 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

This topic describes different ways to customize outbound caller IDs, which help customers recognize who's calling.

Background information

Before you start to customize outbound caller IDs, you may need to know the following concepts:

- Caller ID types
- Priority of outbound caller ID

Prerequisites

Customizing outbound caller ID should be supported by the trunk provider.

Customize outbound caller ID for a trunk

1. Log in to PBX 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
5. To bind consecutive outbound caller IDs to consecutive extensions with one-to-one correspondence, select Outbound Caller ID Range and configure the following settings:
   - Outbound Caller ID Range
   - Extension Range

- Outbound Caller ID Name

6. Click Save and Apply.

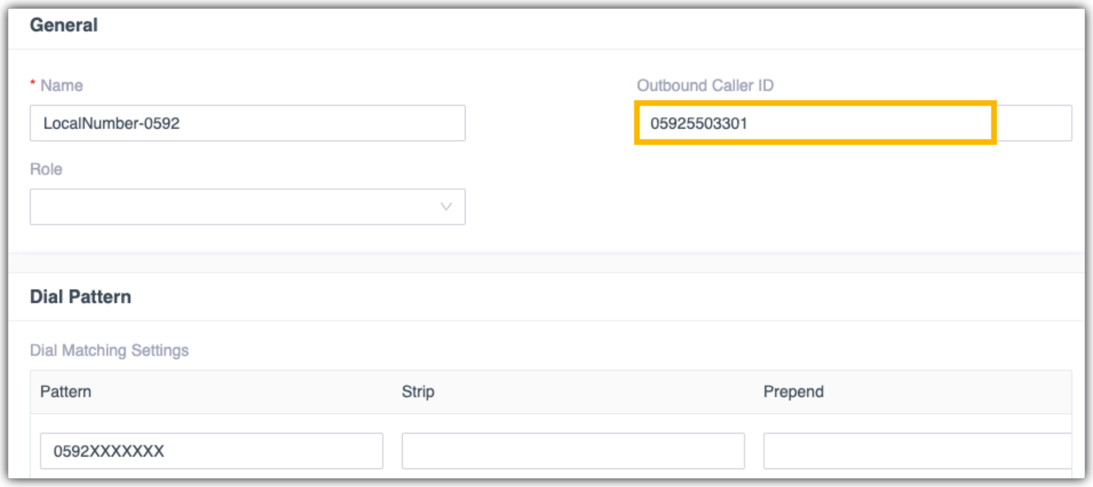
When extension users make outbound calls through the configured trunk, the associated outbound caller IDs will be displayed on the called party's device.

Customize outbound caller IDs based on dialed numbers

When calling to multiple areas, you may need to display pre-defined local number for the area code you are dialling. In this case, you can configure outbound caller IDs based on the dialed numbers.

The following instruction describes how to display a custom outbound caller ID 05925503301 when users call to local numbers that have area code 0592.

1. Log in to PBX 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.



General

* Name: LocalNumber-0592

Outbound Caller ID: 05925503301

Role:

Dial Pattern

Dial Matching Settings

Pattern	Strip	Prepend
0592XXXXXXX		

3. Click Save and Apply.

Export and Import Trunk Outbound Caller IDs

Trunk outbound caller IDs configured on Yeastar P-Series Software Edition 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 Software Edition 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.

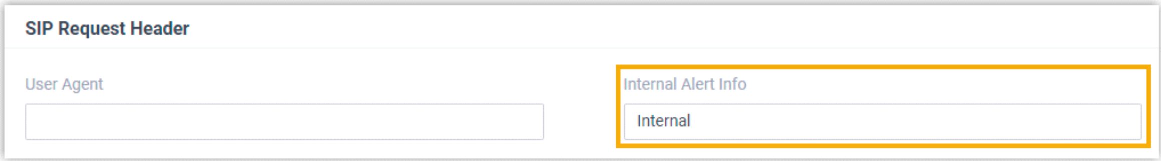
Set alert info for internal calls on the PBX

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`.



SIP Request Header

User Agent

Internal Alert Info

Internal

Set a specific ringtone for a phone

For users who want to play a specific ringtone for internal calls on their phones, you can set a specific ringtone for their phones by auto provisioning.

> Note:
>
> Users can also log in to phone web interface to set distinctive ringtone manually on their own IP phones. For more information, contact the phone manufacturer.

Prerequisites

Each user who wants distinctive ringtone has bound a phone with their extensions.

For more information, see 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

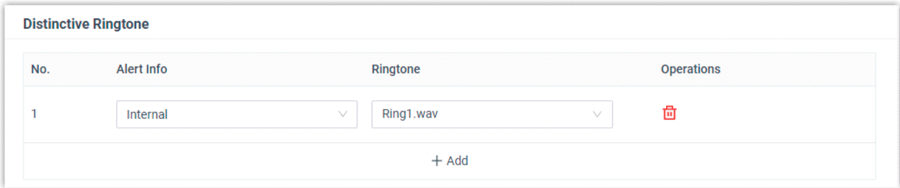
1. Set a specific internal ringtone for a user's phone.
   a. Log in to PBX web portal, go to Extension and Trunk > Extension, edit the user's extension.
   b. Click Phone tab to edit the phone associated with the extension.
   c. In the Distinctive Ringtone section, click Add.
   d. In the Alert Info 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.



Distinctive Ringtone

No.	Alert Info	Ringtone	Operations
1	Internal	Ring1.wav	🗑

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

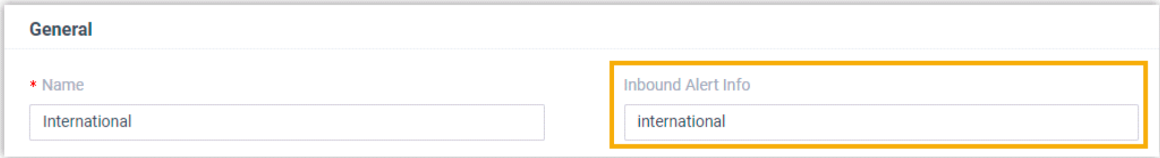
1. Set alert info for external calls on the PBX.
2. Set a specific ringtone for a phone.

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.



General

* Name	Inbound Alert Info
International	international

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)

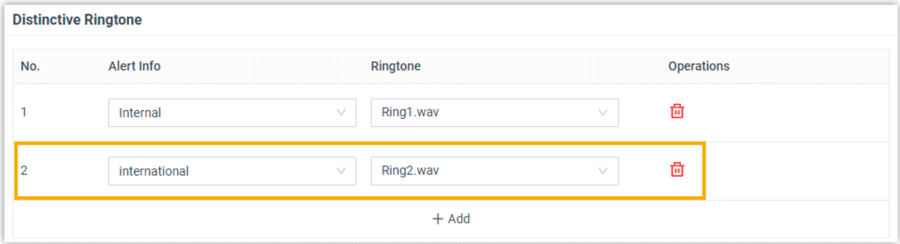
Procedure

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.



Distinctive Ringtone

No.	Alert Info	Ringtone	Operations
1	Internal	Ring1.wav	🗑
2	international	Ring2.wav	🗑

   f. Click Save.

2. Reprovision the phone to take effect.
    1. Go to Auto Provisioning > Phones.
    2. 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

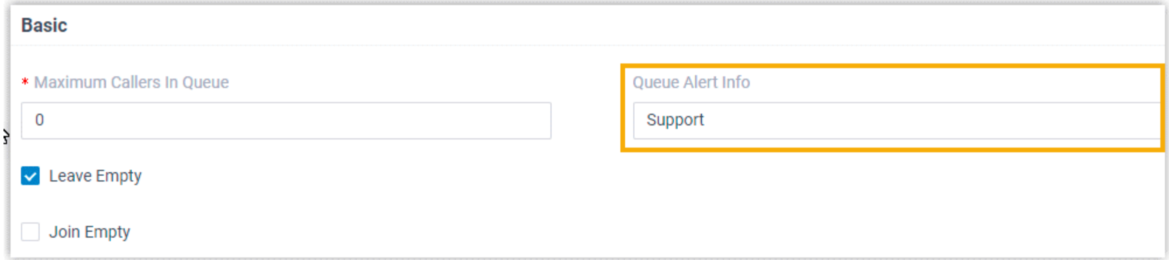
1. Set an alert info for queue calls on the PBX.
2. Set a specific ring tone for a phone.

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`.



Basic

* Maximum Callers In Queue: 0

Queue Alert Info: Support

☑ Leave Empty

□ Join Empty

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)

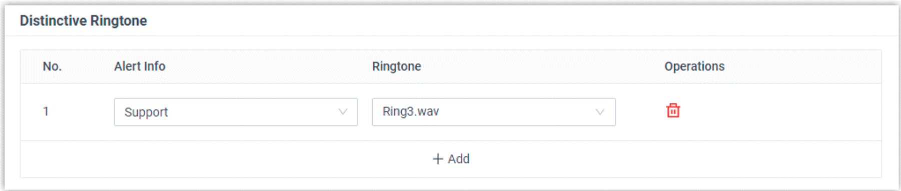
Procedure

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.



Distinctive Ringtone

No.	Alert Info	Ringtone	Operations
1	Support	Ring3.wav	🗑

    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

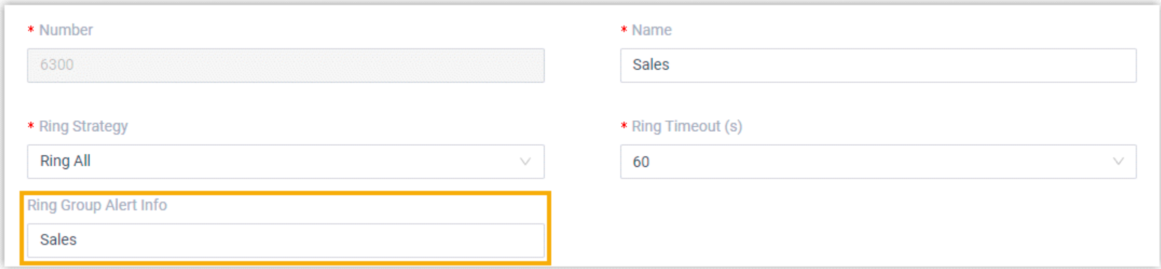
1. Set an alert info for ring group calls on the PBX.
2. Set a specific ringtone for a phone.

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`.



* Number	* Name
6300	Sales
* Ring Strategy	* Ring Timeout (s)
Ring All	60
Ring Group Alert Info	
Sales	

Set a specific ringtone for a phone

For ring group members who want to play a specific ringtone for ring group calls on their 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)

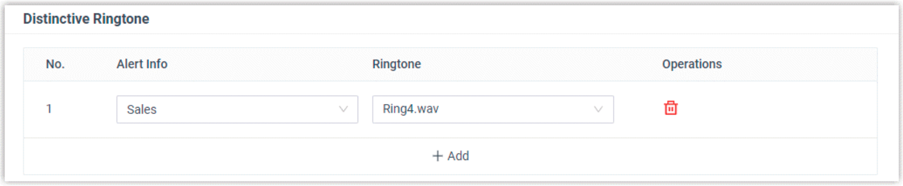
Procedure

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.



Distinctive Ringtone

No.	Alert Info	Ringtone	Operations
1	Sales	Ring4.wav	🗑

+ Add

   f. Click Save.
2. Reprovision the phone to take effect.
   a. Go to Auto Provisioning > Phones.
   b. Click ↻ beside the phone assigned to ring group member's extension.

Result

The ring group member's phone plays ringtone Ring4.wav when receiving calls from the Sales ring group.

Set Distinctive Ringtones for IVR Calls

You can set a unique ringtone per IVR so that the extension users can easily identify who is calling.

Procedure

1. Set an alert info for IVR calls on the PBX.

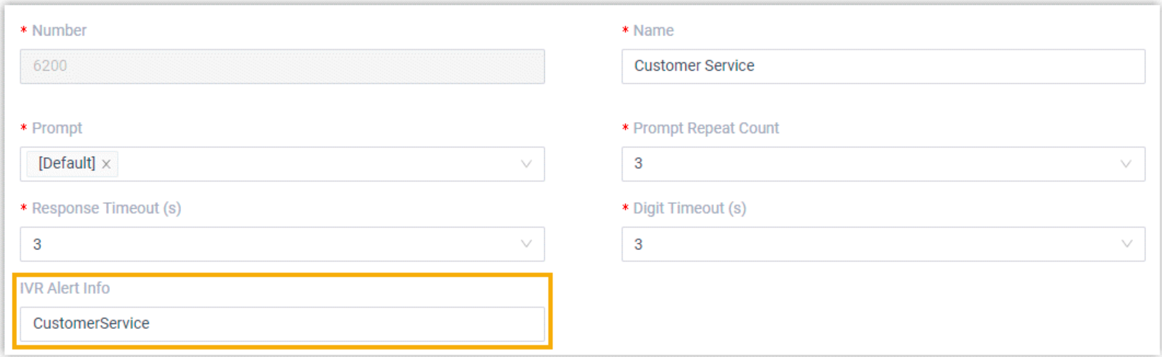
2. Set a specific ringtone for a phone.

Set an alert info for IVR calls on the PBX

1. Log in to PBX 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`.

   * Number: 6200
   * Name: Customer Service
   * Prompt: [Default] ×
   * Prompt Repeat Count: 3
   * Response Timeout (s): 3
   * Digit Timeout (s): 3
   IVR Alert Info: 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

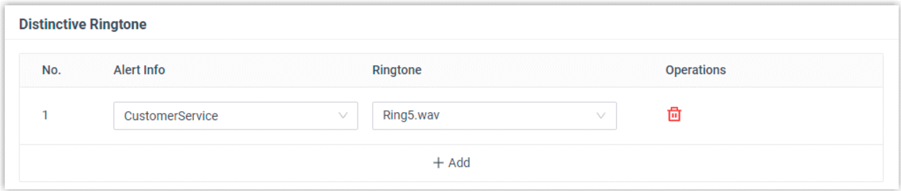
1. Set a specific ringtone for a user.

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.



Distinctive Ringtone

No.	Alert Info	Ringtone	Operations
1	CustomerService	Ring5.wav	🗑

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 40.

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

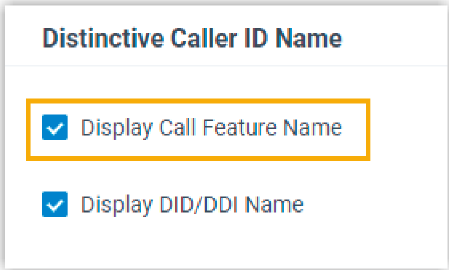
Enable or Disable Distinctive Caller ID Name

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 checkbox of Display Call Feature Name.
   - To hide Queue names, Ring Group names, and IVR names, unselect the checkbox of Display Call Feature Name.



Distinctive Caller ID Name

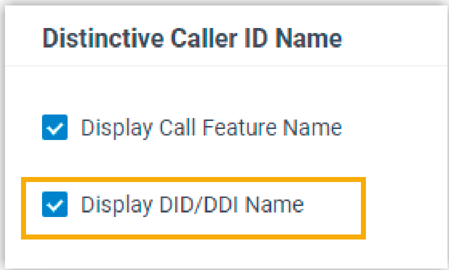
☑ Display Call Feature Name

☑ Display DID/DDI 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.



Distinctive Caller ID Name

☑ Display Call Feature Name

☑ Display DID/DDI Name

3. Click Save and Apply.

Call Center

Call Center Overview

This topic describes what is Yeastar Call Center service, highlight, and the steps to set up a Call Center.

What is Yeastar Call Center service

Yeastar P-Series Software Edition introduces an inbound call center solution to improve agent efficiency, responsiveness, and ultimate customer satisfaction for SMEs running service centers.

Yeastar Call Center provides a powerful console for manager and agents to handle queue calls. Call Center Console is a web-based utility integrated with Linkus Web Client, including a customizable Wallboard for proactive tracking of 16 key performance metrics, and a switchboard-type Queue Panel for real-time monitoring & control of queue activities.

> Note:
> Queue Panel is only recommended for queues with no more than 1000 extensions, otherwise the user experience will be affected as web browser can not work properly with excessive data volume.

For more information of monitoring queue performance and managing queue calls on Call Center Console, see Yeastar Call Center Console User Guide.

Highlight

- Real-time metrics on Wallboard: Display a range of call center metrics and KPIs that allow queue managers to monitor and optimize performance, and spot emerging trends in a central location.
- Switchboard-type Queue Panel: Show the call metrics and agents' performance in real time, and offer a comprehensive view on activity of call that allows manager and agents to handle queue calls.
- SLA for performance measurement: Consistent delivering service that meets or exceeds the expectations set out in the SLA.
- Insightful Call Center reports: Real-time and historical reports that help system administrator to track queue performance indicators, and assess agent performance.

Steps to set up Call Center

1. Create a queue.
2. Set up Call Center.
    a. Manage queue managers: Set one or more extension users as queue managers.

The queue managers can receive queue notifications by email.

b. Customize queue notification: Send email notifications to queue manager when a queue call is missed or abandoned, or the service level agreement reaches the alarm threshold.
c. Grant queue panel permissions: Grant the permissions respectively for queue manager and agents.
d. Set up Service Level Agreement (SLA): Define a certain level of service for a queue.

3. Manage Call Center report: View and schedule Call Center reports.

Call Center Setup

Set up Queue Managers

With call center service activated, you can set any extension as queue manager. A queue manager does not need to be a queue agent. This topic describes how to set queue managers.

Procedure

1. Log in to PBX web portal, go to Call Features > Queue, edit the desired queue.
2. Click Members tab.
3. In the Queue Managers section, manage the queue managers:
    - To add queue managers: Select the desired extensions from the Available box to the Selected box.
    - To delete queue managers: Select the desired extensions from the Selected box to the Available box.
4. Click Save and Apply.

Customize Queue Notification

With call center service activated, the system sends email notifications to queue managers when a queue call is missed or abandoned, when the service level agreement reaches the alarm threshold, when a callback request is made or a callback failed. This topic describes how to customize these notifications.

Prerequisites

- Make sure there is a valid email address assigned to queue manager's extension.
- Make sure system email works.

Procedure

1. Log in to PBX web portal, go to Call Features > Queue, edit the desired queue.
2. Click Members tab.
3. Select the checkbox of notification option according your needs.
    - Notify Manager when a queue call is missed: Send an email to manager when a queue call is missed.
    - Notify Manager when a queue call is abandoned: Send an email to manager when a queue call is abandoned.
    - Notify Manager when the SLA is lower than its alarm threshold: Send an email to manager when the SLA alarm threshold is reached.
    - Notify Manager when a callback request is made: Send an email to manager when a callback request is made.
    - Notify Manager when a callback failed: Send an email to manager when a callback is failed.
4. Click Save and Apply.

Grant Queue Panel Permissions

With call center service activated, you can decide what the queue managers and agents can do on Queue Panel, and grant the Queue Panel permissions for queue manager and agents respectively. This topic describes how to grant permissions for queue manager and agents.

Queue Panel permissions

Permission	Manager	Agents
Switch agents' Status	√	×
Call monitoring operations (Listen, Whisper, Barge In)	√	×
Switch agent's recording status	√	×
Call distribution management (Redirect, Transfer, Drag and Drop operation)	√	√
Allow for picking up or hanging up agents' calls	√	√
Call parking operation	√	√

Grant permissions for queue managers

1. Log in to PBX web portal, go to Call Features > Queue, edit the desired queue.
2. Click Queue Panel Permissions tab.

3. In the Manager section, select the checkboxes of permissions according to your needs.
4. Click Save and Apply.

Grant permissions for agents

1. Log in to PBX web portal, go to Call Features > Queue, edit the desired queue.
2. Click Queue Panel Permissions tab.
3. In the Agents section, select the checkboxes of permissions according to your needs.
4. Click Save and Apply.

Set up Service Level Agreement (SLA)

With call center service activated, you can set up service level agreement for a queue. This topic describes what is service level agreement and how to set up service level agreement.

What is Service Level Agreement (SLA)

Service Level Agreement is a call center performance statistic. It is the goal for how quickly the agent should answer a portion of the customers, and makes sure everyone is working to the same objective.

SLA is expressed as the percentage of conversations answered within a predefined amount of time. Let us suppose that the goal is to answer 80% of calls within 20 seconds. If the measurement is less than 80%, the manager knows they are outside their target Service Level.

The calculated formula shows as below:

$$\text{SLA} = \frac{\text{total calls - (calls answered after SLA time+ calls abandoned after SLA time)}}{\text{total calls}} \text{ X } 100\%$$

How to set up Service Level Agreement

You can set a target service level and SLA threshold for each queue, and evaluate the service level periodically.

1. Log in to PBX web portal, go to Call Features > Queue, edit the desired queue.
2. Click Preferences tab.
3. In the Service Level Agreement section, edit the SLA according to your needs.
    - SLA Time(s): Enter the maximum amount of time (in seconds) that an agent needs to answer an incoming call.

      If a caller waits for a duration of time shorter than the SLA Time, the SLA is met.
    - Evaluation Interval(min): Enter the time interval to compare the queue's SLA performance against the alarm threshold so that the system can send a notification email timely.

- Alarm Threshold(%): Enter the service level threshold for the queue.

4. Click Save and Apply.

Call Center Report

Call Center Reports Overview

Yeastar P-Series Software Edition provides a set of predefined reports concerning detailed information about call center performance. This topic describes what you can do with call center report, and the report types.

What you can do with call center reports

The system automatically generates reports in the format of graphs or charts, and helps you to simplify analysis and extract invaluable data with ease. These reports can be historical and real-time. You can view and schedule reports on demand to evaluate past activities and plan future actions.

Reports types

We divide reports into two categories: queue performance and agent performance.

- Queue performance reports: The queue performance reports give you insight into the work efficiency of one or more queues over a period of time, and help you evaluate the performance of each queue.
    - Queue AVG Waiting & Talking Time
    - Queue Performance
    - Queue Performance Activity
    - Queue Callback Summary
    - Queue Callback Activity
    - Satisfaction Survey
    - Satisfaction Survey Details
- Agent performance reports: The agent performance reports give you insight into the performance of one or more agents, and help you evaluate if every agent meets the expectations of your call center over a period of time.
    - Agent Login Activity
    - Agent Pause Activity
    - Agent Missed Call Activity
    - Agent Performance
    - Agent Call Summary

Queue Performance reports

'Queue AVG Waiting & Talking Time' Report

'Queue AVG Waiting & Talking Time' report provides information about the average amount of time that callers are waiting in a queue, and the average amount of time that an agent spends in handling calls. The report helps you to identify the peak times of queue calls, and allocate your agent accordingly. This topic describes the report details, and shows you a report example.

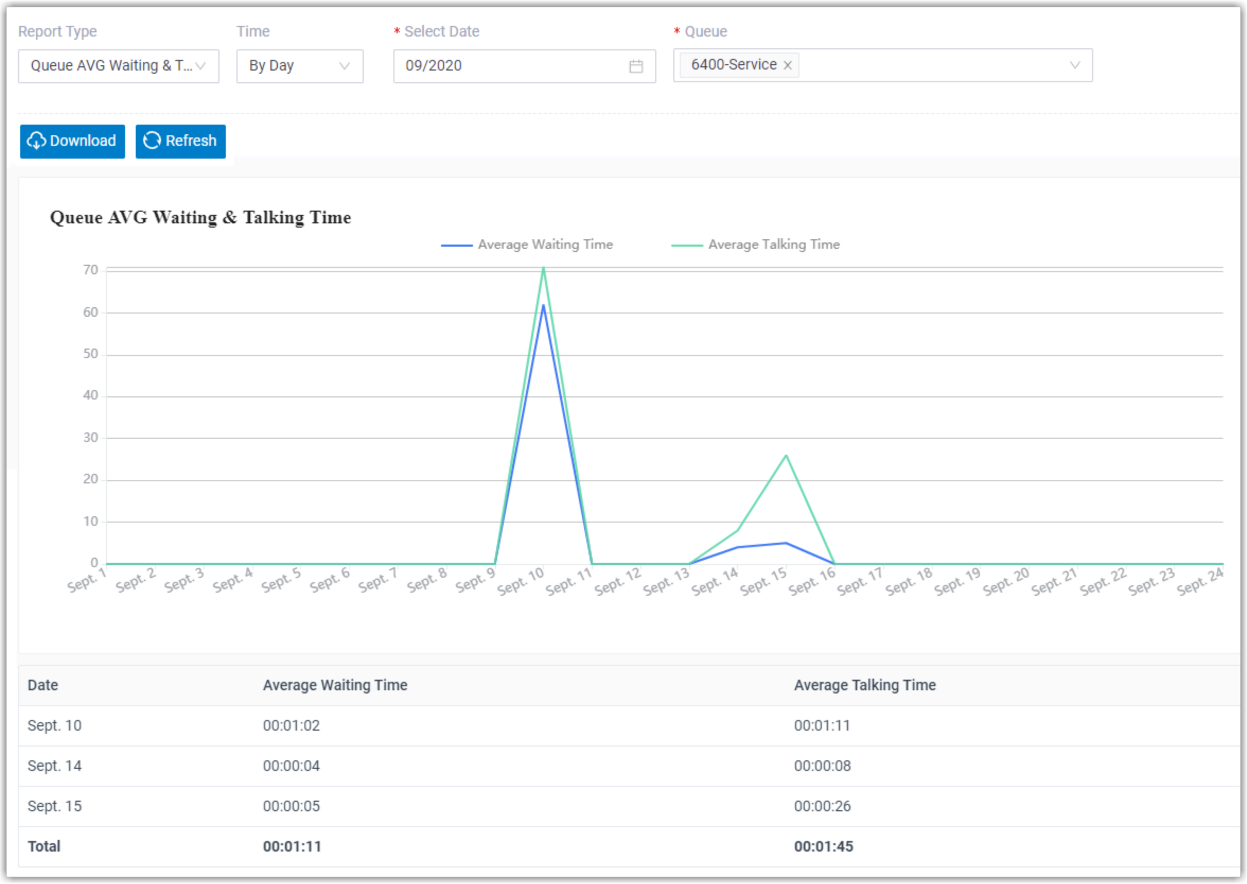
Report details

The Queue AVG Waiting & Talking Time includes a graph and a table that shows the following information for each queue:

Parameter	Description
Average Waiting Time	The average amount of time that it takes for an incoming call to be distributed to an agent.
Average Talking Time	The average amount of time that a caller talks to an agent.

Report example

The following report shows the daily average waiting & talking time of Service department during 09/2020.



Date	Average Waiting Time	Average Talking Time
Sept. 10	00:01:02	00:01:11
Sept. 14	00:00:04	00:00:08
Sept. 15	00:00:05	00:00:26
Total	**00:01:11**	**00:01:45**

'Queue Performance' Report

'Queue Performance' report provides information about how calls are handled by queues. This topic describes the report details, and shows you a report example.

Report details

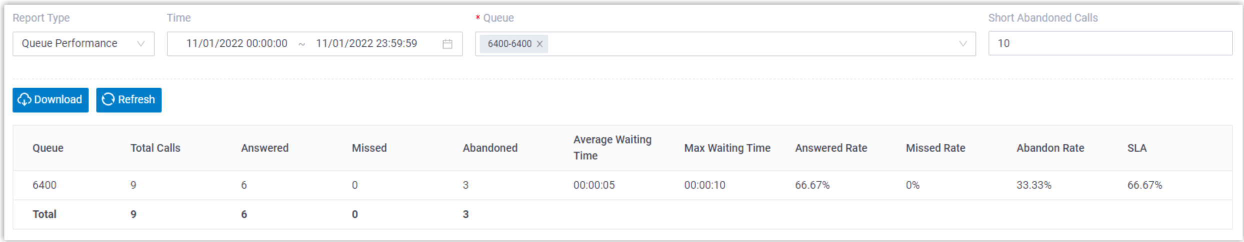
The following table lists the related parameters for Queue Performance report.

Parameter	Description
Total Calls	The total number of calls that queue received.
Answered	The total number of calls that queue answered.
Missed	The total number of calls that queue missed.
Abandoned	The total number of calls that callers abandoned before connecting to an agent.
Average Waiting Time	The average amount of time that it takes for an incoming call to be distributed to an agent.

Parameter	Description
Max Waiting Time	The longest time a caller waited in the queue before an agent answered the call.
Answered Rate	The percentage of answered calls in relation to the total received calls.
Missed Rate	The percentage of missed calls in relation to the total received calls.
Abandon Rate	The percentage of abandoned calls in relation to the total received calls.
SLA	The Service Level Agreement (SLA) for the queue. SLA is the percentage of conversations answered within a predefined amount of time.

Report example

The following report shows the performance of Queue 6400 on 11/01/2022. Calls abandoned within 10 seconds are not included in the report.



Report Type: Queue Performance

Time: 11/01/2022 00:00:00 ~ 11/01/2022 23:59:59

* Queue: 6400-6400 ×

Short Abandoned Calls: 10

Queue	Total Calls	Answered	Missed	Abandoned	Average Waiting Time	Max Waiting Time	Answered Rate	Missed Rate	Abandon Rate	SLA
6400	9	6	0	3	00:00:05	00:00:10	66.67%	0%	33.33%	66.67%
Total	**9**	**6**	**0**	**3**						

'Queue Performance Activity' Report

'Queue Performance Activity' report provides details about queue calls by hour, by day, and by month. This topic describes the report details, and shows you a report example.

Report details

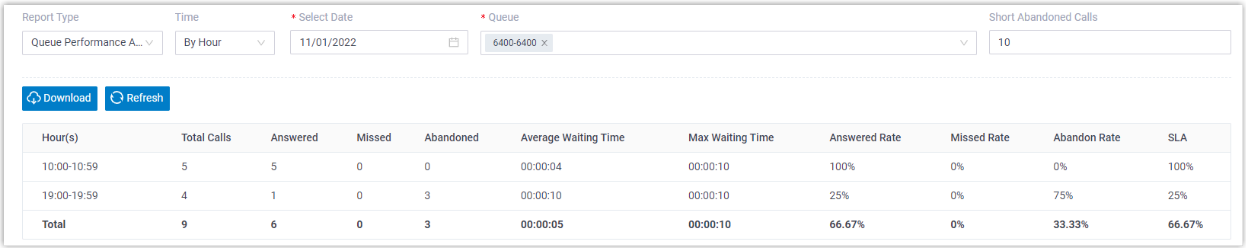
The following table lists the related parameters for Queue Performance Activity report.

Parameter	Description
Total Calls	The total number of calls that queue received.
Answered	The total number of calls that queue answered.
Missed	The total number of calls that queue missed.
Abandoned	The total number of calls that callers abandoned before connecting to an agent.

Parameter	Description
Average Waiting Time	The average amount of time that it takes for an incoming call to be distributed to an agent.
Max Waiting Time	The longest time a caller waited in the queue before an agent answered the call.
Answered Rate	The percentage of answered calls in relation to the total received calls.
Missed Rate	The percentage of missed calls in relation to the total received calls.
Abandon Rate	The percentage of abandoned calls in relation to the total received calls.
SLA	The Service Level Agreement (SLA) for the queue. SLA is the percentage of conversations answered within a predefined amount of time.

Report example

The following report shows the hourly performance of Queue 6400 on 11/01/2022. Calls abandoned within 10 seconds are not included in the report.



Report Type: Queue Performance A...

Time: By Hour

* Select Date: 11/01/2022

* Queue: 6400-6400

Short Abandoned Calls: 10

Hour(s)	Total Calls	Answered	Missed	Abandoned	Average Waiting Time	Max Waiting Time	Answered Rate	Missed Rate	Abandon Rate	SLA
10:00-10:59	5	5	0	0	00:00:04	00:00:10	100%	0%	0%	100%
19:00-19:59	4	1	0	3	00:00:10	00:00:10	25%	0%	75%	25%
Total	**9**	**6**	**0**	**3**	**00:00:05**	**00:00:10**	**66.67%**	**0%**	**33.33%**	**66.67%**

'Queue Callback Summary' Report

'Queue Callback Summary' report provides queue manager with an overview of queue callback statistics, including how many calls a queue received, how many callbacks callers request, how many callbacks were made, and how many callbacks failed.

Report details

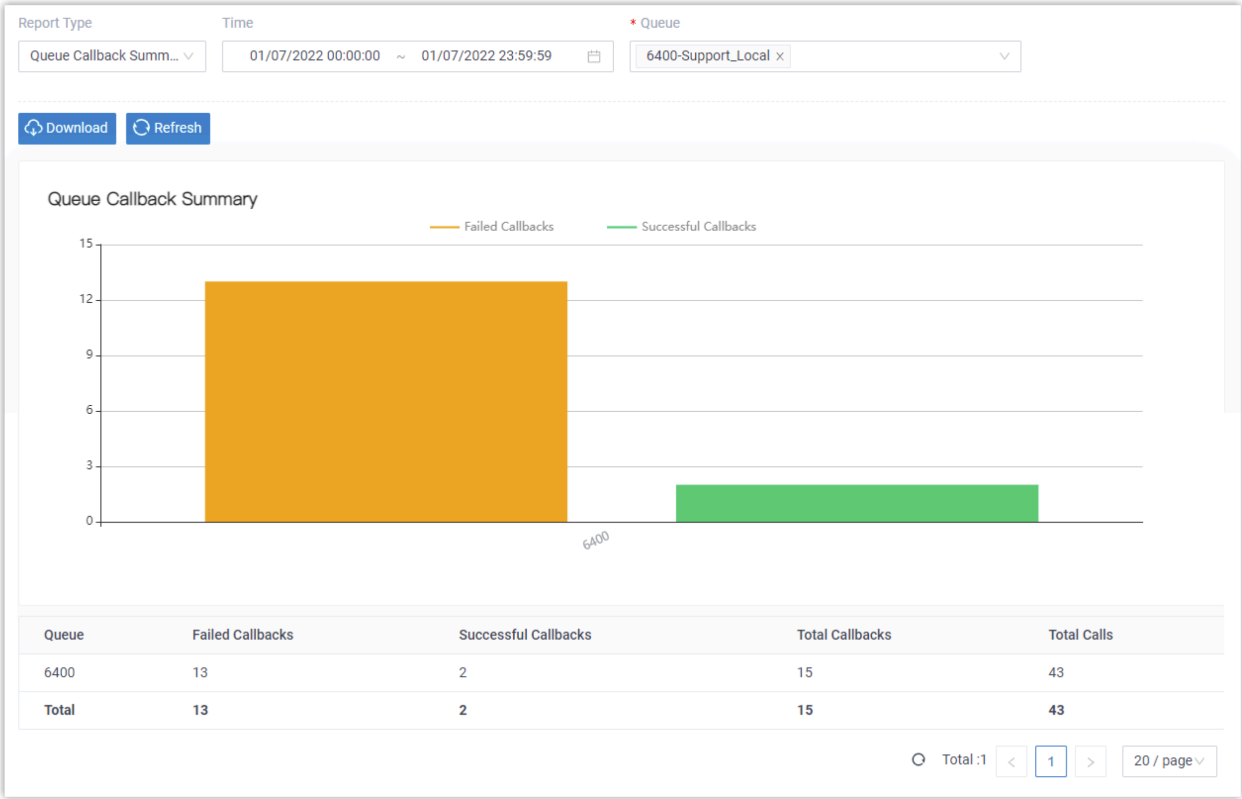
The following table lists the related parameters for 'Queue Callback Summary' report.

Parameter	Description
Failed Callbacks	The number of failed callbacks.
Successful Callbacks	The number of successful callbacks.

Parameter	Description
Total Callbacks	The total number of callbacks for which callers requested successfully.
Total Calls	The total number of calls that the queue received.

Report example

The following report shows callback summary statistics of the queue 6400-Support_Local on 01/07/2022.



Queue	Failed Callbacks	Successful Callbacks	Total Callbacks	Total Calls
6400	13	2	15	43
Total	**13**	**2**	**15**	**43**

'Queue Callback Activity' Report

'Queue Callback Activity' report provides detailed information about callbacks, which helps queue manager analyze queue performance and improve customer service.

Report details

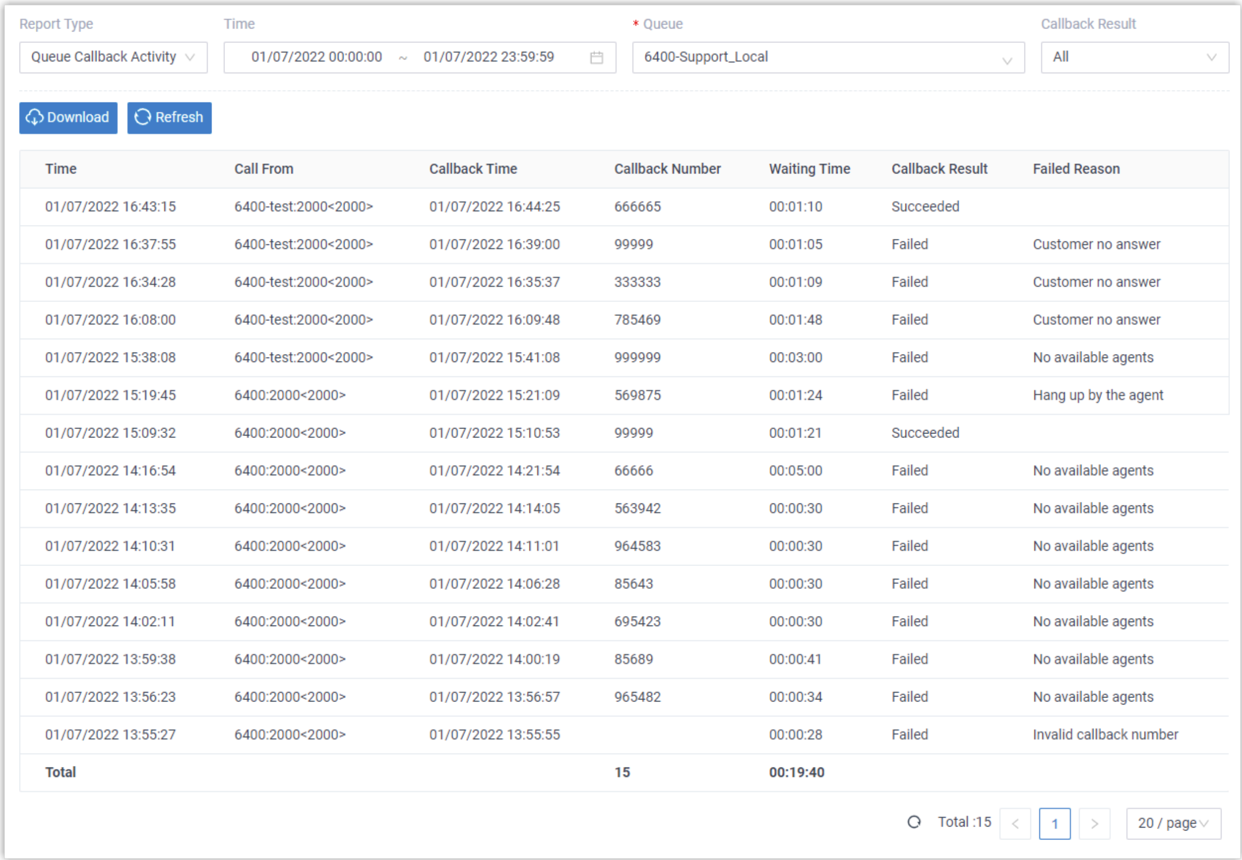
The following table lists the related parameters for 'Queue Callback Activity' report.

Parameter	Description
Time	The time that the caller called to the queue.

Parameter	Description
Call From	The caller's caller ID.
Callback Time	The time that the system performed the callback.
Callback Number	The callback number that the caller registered.
Waiting Time	The time between the call started and the callback answered.
Callback Result	Whether the callback is successful or not.
Failed Reason	The reason that failed to make the callback.

Report example

The following report shows callback activity statistics of the queue 6400-Support_Local on 01/07/222.



Report Type: Queue Callback Activity

Time: 01/07/2022 00:00:00 ~ 01/07/2022 23:59:59

* Queue: 6400-Support_Local

Callback Result: All

Time	Call From	Callback Time	Callback Number	Waiting Time	Callback Result	Failed Reason
01/07/2022 16:43:15	6400-test:2000<2000>	01/07/2022 16:44:25	666665	00:01:10	Succeeded	
01/07/2022 16:37:55	6400-test:2000<2000>	01/07/2022 16:39:00	99999	00:01:05	Failed	Customer no answer
01/07/2022 16:34:28	6400-test:2000<2000>	01/07/2022 16:35:37	333333	00:01:09	Failed	Customer no answer
01/07/2022 16:08:00	6400-test:2000<2000>	01/07/2022 16:09:48	785469	00:01:48	Failed	Customer no answer
01/07/2022 15:38:08	6400-test:2000<2000>	01/07/2022 15:41:08	999999	00:03:00	Failed	No available agents
01/07/2022 15:19:45	6400:2000<2000>	01/07/2022 15:21:09	569875	00:01:24	Failed	Hang up by the agent
01/07/2022 15:09:32	6400:2000<2000>	01/07/2022 15:10:53	99999	00:01:21	Succeeded	
01/07/2022 14:16:54	6400:2000<2000>	01/07/2022 14:21:54	66666	00:05:00	Failed	No available agents
01/07/2022 14:13:35	6400:2000<2000>	01/07/2022 14:14:05	563942	00:00:30	Failed	No available agents
01/07/2022 14:10:31	6400:2000<2000>	01/07/2022 14:11:01	964583	00:00:30	Failed	No available agents
01/07/2022 14:05:58	6400:2000<2000>	01/07/2022 14:06:28	85643	00:00:30	Failed	No available agents
01/07/2022 14:02:11	6400:2000<2000>	01/07/2022 14:02:41	695423	00:00:30	Failed	No available agents
01/07/2022 13:59:38	6400:2000<2000>	01/07/2022 14:00:19	85689	00:00:41	Failed	No available agents
01/07/2022 13:56:23	6400:2000<2000>	01/07/2022 13:56:57	965482	00:00:34	Failed	No available agents
01/07/2022 13:55:27	6400:2000<2000>	01/07/2022 13:55:55		00:00:28	Failed	Invalid callback number
Total			**15**	**00:19:40**		

'Satisfaction Survey' Report

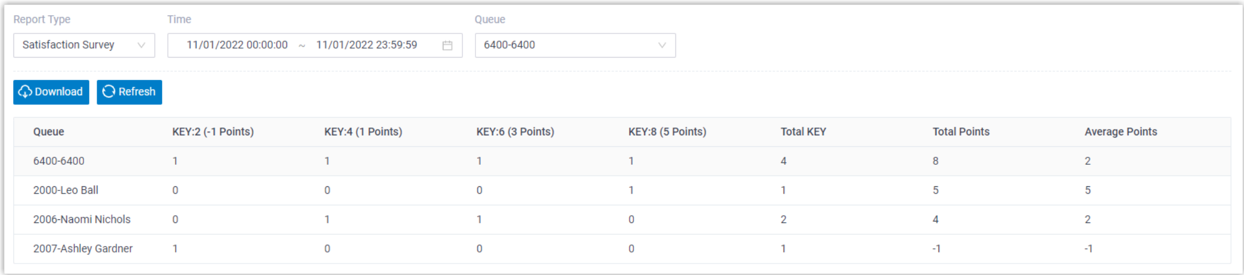
'Satisfaction Survey' report provides statistics about the key pressed collected from callers for a queue and its agents. This topic describes the report details, and shows you a report example.

Report details

Parameter	Description
KEY: {key_pressed}({numeric} Points)	The key pressed by caller and corresponding score for the key.
Total KEY	The total number of keys that were collected for the queue or an agent.
Total Points	The total satisfaction survey scores for the queue or an agent.
Average Points	The average satisfaction survey scores for the queue or an agent. Note: Average Points = Total Points / Total KEY, where the calculated average points will be truncated to two decimal places without rounding up.

Report example

The following report shows the satisfaction survey of Queue 6400 and its agents on 11/01/2022.



Report Type: Satisfaction Survey

Time: 11/01/2022 00:00:00 ~ 11/01/2022 23:59:59

Queue: 6400-6400

Queue	KEY:2 (-1 Points)	KEY:4 (1 Points)	KEY:6 (3 Points)	KEY:8 (5 Points)	Total KEY	Total Points	Average Points
6400-6400	1	1	1	1	4	8	2
2000-Leo Ball	0	0	0	1	1	5	5
2006-Naomi Nichols	0	1	1	0	2	4	2
2007-Ashley Gardner	1	0	0	0	1	-1	-1

'Satisfaction Survey Details' Report

'Satisfaction Survey Details' report provides customers' feedbacks on each call handled by an agent. This topic describes the report details, and shows you a report example.

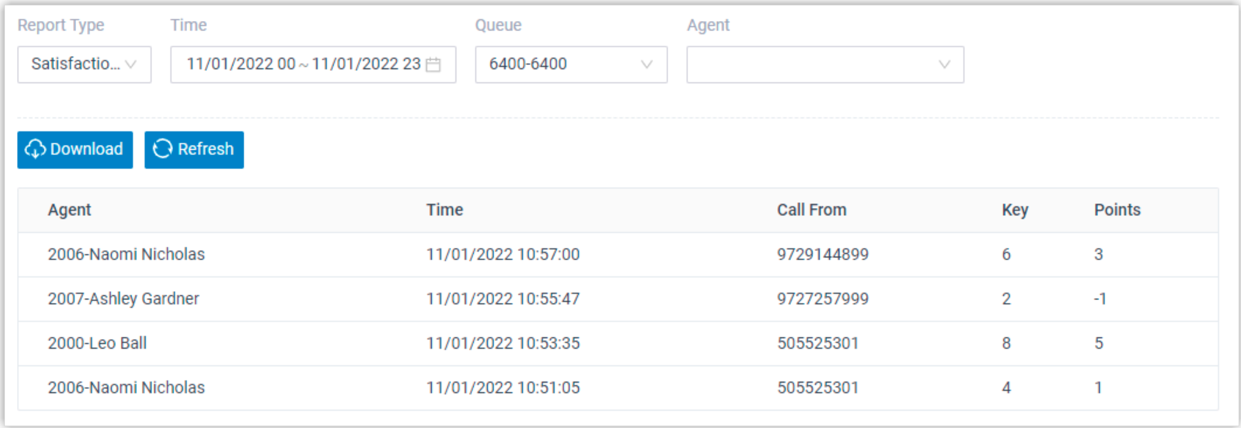
Report details

Parameter	Description
Time	The time that the caller called to the queue.
Call From	The caller's caller ID.
Key	The key that the caller pressed to rate the agent's service.

Parameter	Description
Points	The score for the key pressed.

Report example

The following report shows the satisfaction survey details of each agent in Queue 6400 on 11/01/2022.



Agent	Time	Call From	Key	Points
2006-Naomi Nicholas	11/01/2022 10:57:00	9729144899	6	3
2007-Ashley Gardner	11/01/2022 10:55:47	9727257999	2	-1
2000-Leo Ball	11/01/2022 10:53:35	505525301	8	5
2006-Naomi Nicholas	11/01/2022 10:51:05	505525301	4	1

Agent Performance Report

'Agent Login Activity' Report

'Agent Login Activity' report provides information about the login and logout activities of each agent. The report helps you count the working hours of the agents working in shifts. This topic describes the report details, and shows you a report example.

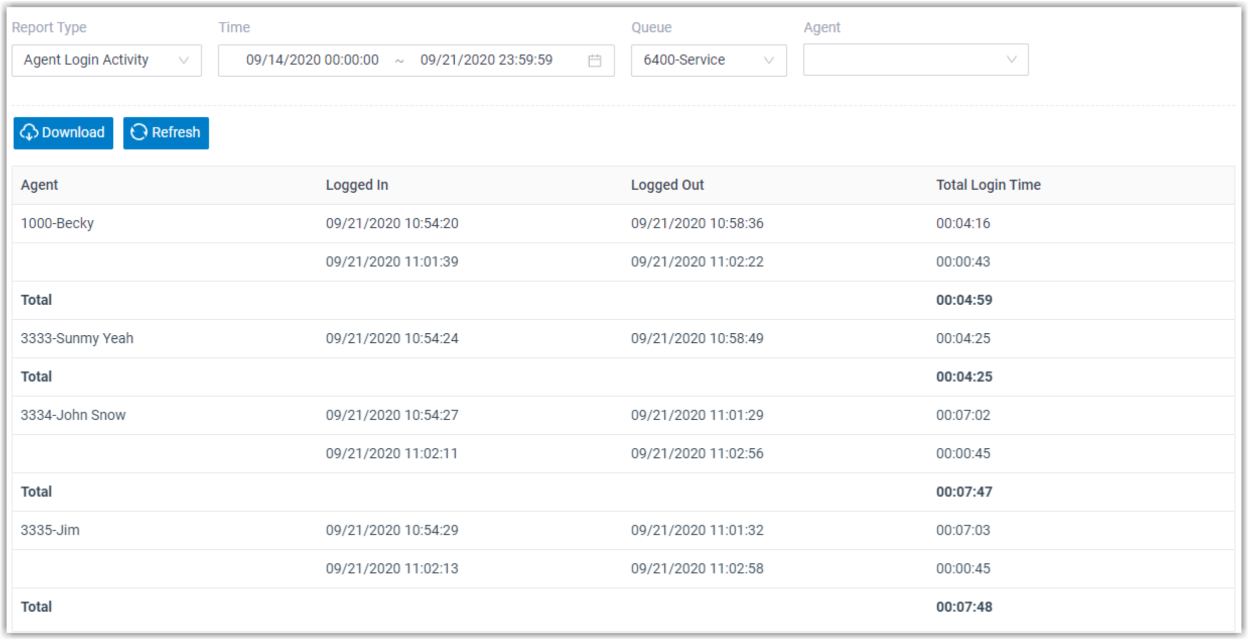
Report details

The 'Agent Login Activity' report includes a table that shows the following information for each agent:

Parameter	Description
Logged In	The date and time that an agent logged in to a queue.
Logged Out	The date and time that an agent logged out of a queue.
Total Login Time	The elapsed time between the login time and the logout time.

Report example

The following report shows the login activities of all agents in Service department in the past 7 days.



Report Type: Agent Login Activity
Time: 09/14/2020 00:00:00 ~ 09/21/2020 23:59:59
Queue: 6400-Service
Agent:

Agent	Logged In	Logged Out	Total Login Time
1000-Becky	09/21/2020 10:54:20	09/21/2020 10:58:36	00:04:16
	09/21/2020 11:01:39	09/21/2020 11:02:22	00:00:43
Total			**00:04:59**
3333-Sunmy Yeah	09/21/2020 10:54:24	09/21/2020 10:58:49	00:04:25
Total			**00:04:25**
3334-John Snow	09/21/2020 10:54:27	09/21/2020 11:01:29	00:07:02
	09/21/2020 11:02:11	09/21/2020 11:02:56	00:00:45
Total			**00:07:47**
3335-Jim	09/21/2020 10:54:29	09/21/2020 11:01:32	00:07:03
	09/21/2020 11:02:13	09/21/2020 11:02:58	00:00:45
Total			**00:07:48**

'Agent Pause Activity' Report

'Agent Pause Activity' report provides information about the pause and unpause activities of each agent. The report helps you count the pause time of each agent. This topic describes the report details, and shows you a report example.

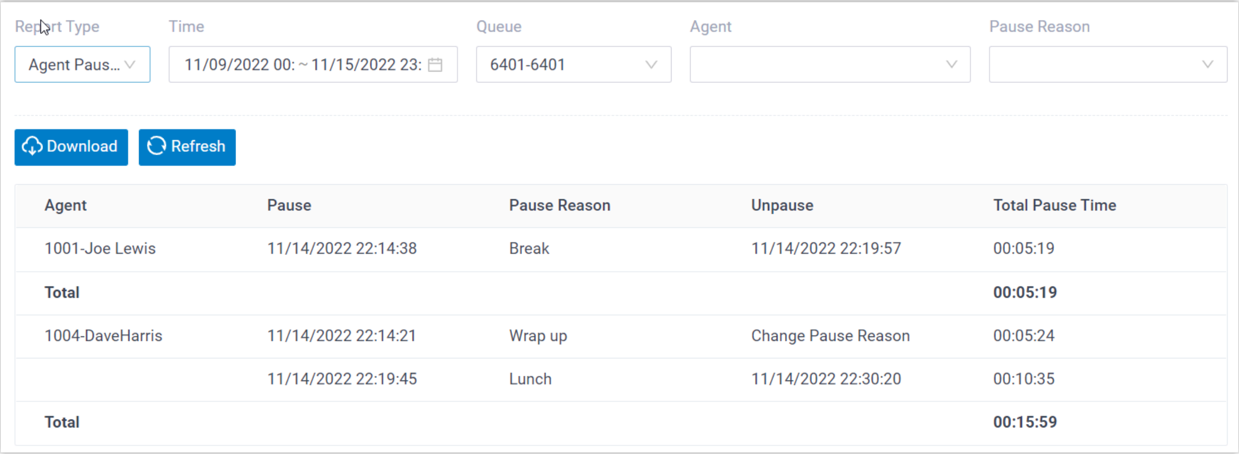
Report details

The 'Agent Pause Activity' report shows the following information for each agent:

Parameter	Description
Pause	The date and time that an agent changed status to pause.
Pause Reason	The reason why an agent changed status to pause.
Unpause	Indicate that the pause reason was changed; or display the date and time that an agent changed status to unpause.
Total Pause Time	The elapsed time between switching to the current pause status and changing to another status (unpause or other pause reason).

Report example

The following report shows the pause activities of all agents in queue 6401 in the past 7 days.



Agent	Pause	Pause Reason	Unpause	Total Pause Time
1001-Joe Lewis	11/14/2022 22:14:38	Break	11/14/2022 22:19:57	00:05:19
Total				**00:05:19**
1004-DaveHarris	11/14/2022 22:14:21	Wrap up	Change Pause Reason	00:05:24
	11/14/2022 22:19:45	Lunch	11/14/2022 22:30:20	00:10:35
Total				**00:15:59**

'Agent Missed Call Activity' Report

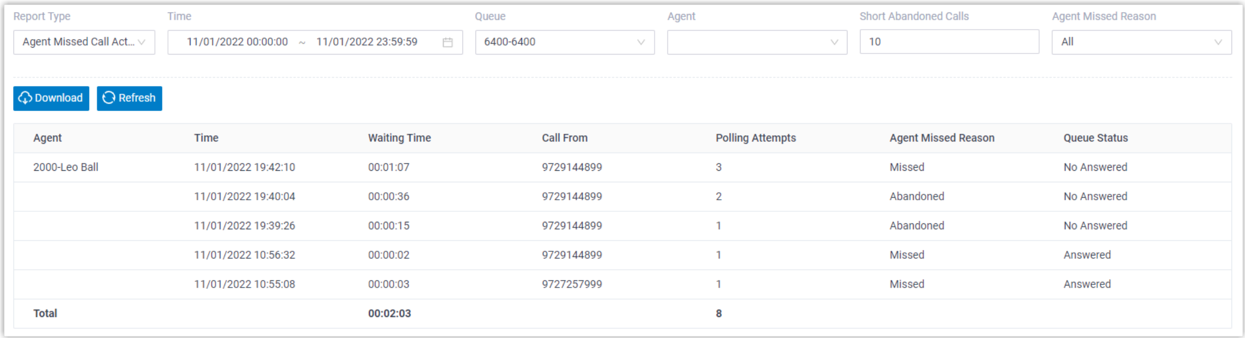
'Agent Missed Call Activity' report provides the missed call information for each agent. The report helps you assess an agent's efficiency. This topic describes the report details, and shows you a report example.

Report details

Parameter	Description
Time	The date and time that an agent missed a call.
Waiting Time	The amount of time that the caller waited for the assigned agent to answer the call.
Call From	The caller's caller ID.
Polling Attempts	The number of polling attempts to call an agent.
Agent Missed Reason	The reason why the call was not answered. • Abandoned: The caller hung up the call. • Missed: The call was not answered in the key destination, or was routed to the failover destination.
Queue Status	The final status of missed calls, indicating whether the missed calls were answered by other agents.

Report example

The following report shows the missed call activities of all agents in Queue 6400 on 11/01/2022. Calls abandoned within 10 seconds are not included in the report.



Report Type: Agent Missed Call Act...
Time: 11/01/2022 00:00:00 ~ 11/01/2022 23:59:59
Queue: 6400-6400
Agent:
Short Abandoned Calls: 10
Agent Missed Reason: All

Agent	Time	Waiting Time	Call From	Polling Attempts	Agent Missed Reason	Queue Status
2000-Leo Ball	11/01/2022 19:42:10	00:01:07	9729144899	3	Missed	No Answered
	11/01/2022 19:40:04	00:00:36	9729144899	2	Abandoned	No Answered
	11/01/2022 19:39:26	00:00:15	9729144899	1	Abandoned	No Answered
	11/01/2022 10:56:32	00:00:02	9729144899	1	Missed	Answered
	11/01/2022 10:55:08	00:00:03	9727257999	1	Missed	Answered
Total		**00:02:03**		**8**		

'Agent Performance' Report

'Agent Performance' report provides agent call details to help you measure agent performance. This topic describes the report details, and shows you a report example.

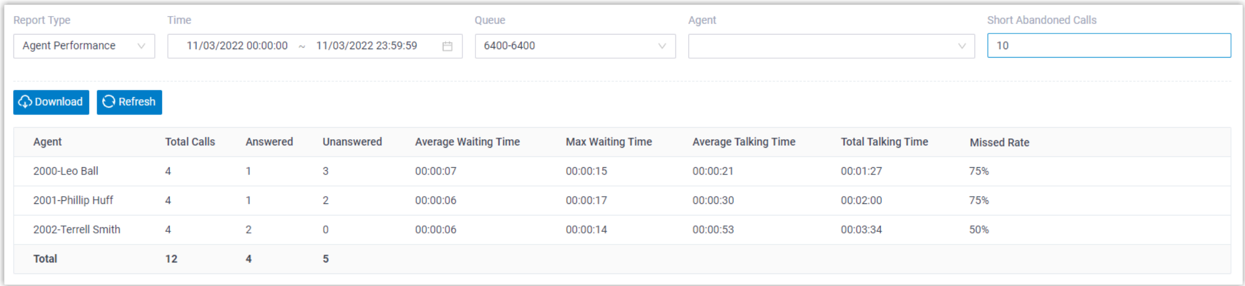
Report details

The following table lists the related parameters for Agent Performance report.

Parameter	Description
Total Calls	The total number of calls that agent received.
Answered	The total number of calls that agent answered.
Unanswered	The total number of calls that agent unanswered.
Average Waiting Time	The average amount of time that it takes for an incoming call to be distributed to the agent.
Max Waiting Time	The longest time a caller waited in the queue before the agent answered the call.
Average Talking Time	The average amount of time that the agent talks to callers.
Total Talking Time	The total amount of time that the agent talks to callers.
Missed Rate	The percentage of missed calls in relation to the total received calls.

Report example

The following report shows the call summary of all agents in Queue 6400 on 11/03/2022.



Report Type: Agent Performance

Time: 11/03/2022 00:00:00 ~ 11/03/2022 23:59:59

Queue: 6400-6400

Agent:

Short Abandoned Calls: 10

Agent	Total Calls	Answered	Unanswered	Average Waiting Time	Max Waiting Time	Average Talking Time	Total Talking Time	Missed Rate
2000-Leo Ball	4	1	3	00:00:07	00:00:15	00:00:21	00:01:27	75%
2001-Phillip Huff	4	1	2	00:00:06	00:00:17	00:00:30	00:02:00	75%
2002-Terrell Smith	4	2	0	00:00:06	00:00:14	00:00:53	00:03:34	50%
Total	**12**	**4**	**5**					

'Agent Call Summary' Report

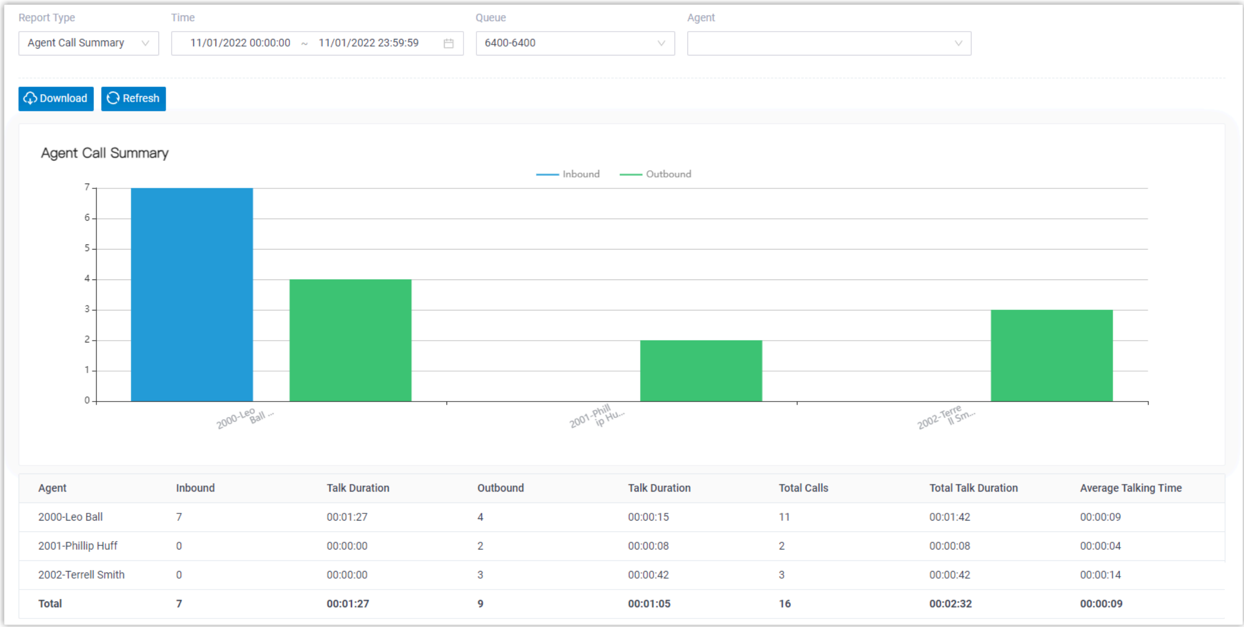
'Agent Call Summary' report provides information about the number of incoming and outgoing calls that were received and placed by each agent. This topic describes the report details, and shows you a report example.

Report details

Parameter	Description
Inbound	The number of incoming calls received by an agent.
Outbound	The number of outgoing calls placed by an agent.
Talk Duration	The amount of time an agent spent in incoming calls or outgoing calls.
Total calls	The total number of incoming calls and outgoing calls handled by an agent.
Total Talk Duration	The total amount of time an agent spent in incoming calls and outgoing calls.
Average Talking Time	The average amount of time an agent spent in incoming calls and outgoing calls.

Report example

The following report shows the call summary of all agents in Queue 6400 on 11/01/2022.



Report Type: Agent Call Summary

Time: 11/01/2022 00:00:00 ~ 11/01/2022 23:59:59

Queue: 6400-6400

Agent:

Agent	Inbound	Talk Duration	Outbound	Talk Duration	Total Calls	Total Talk Duration	Average Talking Time
2000-Leo Ball	7	00:01:27	4	00:00:15	11	00:01:42	00:00:09
2001-Phillip Huff	0	00:00:00	2	00:00:08	2	00:00:08	00:00:04
2002-Terrell Smith	0	00:00:00	3	00:00:42	3	00:00:42	00:00:14
Total	**7**	**00:01:27**	**9**	**00:01:05**	**16**	**00:02:32**	**00:00:09**

Call Features

Voicemail

Voicemail Overview

Yeastar P-Series Software Edition 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 Software Edition provides two types of voicemail:

- Extension Voicemail: Voicemail for individual extension.
- Group Voicemail: Group Voicemail is a feature for a team to share the workload of reading and responding to voicemail messages.

  Group Voicemail is useful if your company is organized into departments. For example, after setting up a group voicemail for Support team, a customer can deliver voicemail messages to the Support team, then any team members can access the group voicemail box to check the customer's voicemail.

Voicemail usages

A flexible call route system for forwarding calls to voicemail:

- Extension: Allow the caller to leave a message when the extension user is unavailable to take a call.

  For more information, see Forward extension users' calls to voicemail.
- Ring Group/Queue: Failover to group voicemail if no agents are available or timeout is reached.

  For more information, see Set failover destination to voicemail for a ring group or queue.
- IVR: Give the customers an option to leave a voicemail message. When the customers cannot get the information from IVR, they can leave a message.

  For more information, see Allow users to leave voicemail messages by IVR.
- Any inbound calls: Provide a dedicated line to collect user feedback if immediate phone support is not required.

  For more information, see Forward inbound calls to voicemail.

Voicemail personalization

Various options are available for personalizing voicemail:

- Voicemail greeting: Custom greeting is available for global or a specific extension. The extension users can also customize their greetings based on presence.

  For more information, see Voicemail Greeting Overview.

- Voicemail notification: Various ways to get notified of new voicemail messages, including on IP phones, emails, or Linkus clients.

  For more information, see Voicemail Notification Overview.

- Envelope playback: Play optional envelope information before listening to voicemail message, including date and time, caller ID, and message duration.

  For more information, see Configure Message Envelope.
- Caller experience: User-friendly experience in leaving a message, such as allow the caller to review message, send a message without ringing extensions, break out of voicemail to operator, etc.
  For more information, see:
  - Allow Callers to Press a Key to Leave Messages
  - Allow Callers to Dial Extension from Voicemail
  - Allow Callers to Break out from Voicemail
  - Allow Callers to Review Voicemail Messages

Voicemail capacity and limitations

The default and adjustable capacity and limitations for each voicemail box are as follows:

- Message length: 1 to 15 minutes.

  The default minimum duration of a message is 2 seconds; the default maximum duration of a message is 10 minutes.

  To change the message length, see Limit Voicemail Message Length.
- Mailbox capacity: 1 to 500.

  The default max number of voicemail is 100.

  To change mailbox capacity, see Auto Cleanup Voicemail Messages.
- Storage time: Unlimited.

  The default is 0, which means no limit.

  To change the storage time, see Auto Cleanup Voicemail Messages.

Group Voicemail

Set up Group Voicemail for a Queue

You can set up a Group Voicemail for a queue. All agents of the queue will get notified when a group voicemail message is received.

Procedure

1. Log in to PBX web portal, go to Call Features > Voicemail > Group Voicemail.
2. Click Add.
3. In the Basic section, configure the following settings.
    - Type: Select Queue.
    - Queue: Select a queue.
    - Number: The Group Voicemail number is the queue number, and is not editable.
    - Name: The Group Voicemail name is the queue name, and is not editable.
    - Mode: Select the mode to handle received voicemail messages.
        - Shared by Members: The voicemail messages are saved in the group mailbox, and are shared by all members. Any members can manage the group voicemail messages.
        - Broadcast to Members: The voicemail messages are not stored in the group mailbox. Instead, the system broadcasts (copies and forwards) the voicemail messages to the individual mailboxes of all the members.
    - Voicemail PIN Authentication: Enable or disable voicemail PIN authentication.
    - Voicemail Access PIN: If enable voicemail PIN authentication, enter a desired access PIN number.
    - Play Date and Time: Optional. Play the date and time that the message was received before a voicemail message is played.
    - Play Caller ID: Optional. Play the caller ID information before a voicemail message is played.
    - Play Message Duration: Optional. Play the duration of the message before a voicemail message is played.
4. In the Members section, all the agents of the queue are selected, and the members are not editable.

    > Note:
    >
    > If the queue agents are changed, the members of the group's voice mailboxes also change.
5. In the Group Voicemail Greeting section, select a voicemail greeting.

    You can also click Greeting Management to customize a greeting or mange your custom greetings.
6. Click Save and Apply.

Related information

- Enable or Disable Voicemail Access PIN
- Change Voicemail Access PIN
- Configure Message Envelope
- Change Voicemail Greetings
- Record or Upload Voicemail Greetings
- Manage Group Voicemail Greetings

Set up Group Voicemail for a Ring Group

You can set up a Group Voicemail for a ring group. All members of the ring group will get notified when a group voicemail message is received.

Procedure

1. Log in to PBX web portal, go to Call Features > Voicemail > Group Voicemail.
2. Click Add.
3. In the Basic section, configure the following settings:
    - Type: Select Ring Group.
    - Ring Group: Select a ring group.
    - Number: The group voicemail number is the ring group number, and is not editable.
    - Name: The group voicemail name is the ring group name, and is not editable.
    - Mode: Select the mode to handle received voicemail messages.
        - Shared by Members: The voicemail messages are saved in the group mailbox, and are shared by all members. Any members can manage the group voicemail messages.
        - Broadcast to Members: The voicemail messages are not stored in the group mailbox. Instead, the system broadcasts (copies and forwards) the voicemail messages to the individual mailboxes of all the members.
    - Voicemail PIN Authentication: Enable or disable voicemail PIN authentication.
    - Voicemail Access PIN: If enable voicemail PIN authentication, enter a desired access PIN number.
    - Play Date and Time: Optional. Play the date and time that the message was received before a voicemail message is played.
    - Play Caller ID: Optional. Play the caller ID information before a voicemail message is played.
    - Play Message Duration: Optional. Play the duration of the message before a voicemail message is played.
4. In the Members section, all the members of the ring group are selected, and the members are not editable.

> Note:
>
> If the ring group members are changed, the members of the group's voice mailboxes also change.

5. In the Group Voicemail Greeting section, select a voicemail greeting.

   You can also click Greeting Management to customize a greeting or mange your custom greetings.
6. Click Save and Apply.

Related information

- Enable or Disable Voicemail Access PIN
- Change Voicemail Access PIN
- Configure Message Envelope
- Change Voicemail Greetings
- Record or Upload Voicemail Greetings
- Manage Group Voicemail Greetings

Set up Group Voicemail for a Custom Group

For a team whose members come from different departments, you can set up a Group Voicemail for the team members. All team members will get notified when a group voicemail message is received.

Procedure

1. Log in to PBX web portal, go to Call Features > Voicemail > Group Voicemail.
2. Click Add.
3. In the Basic section, configure the following settings:
   - Type: Select Custom.
   - Number: Specify a virtual number for callers to access the group voicemail.
   - Name: Enter a group voicemail name to help you identify it.
   - Mode: Select the mode to handle received voicemail messages.
     - Shared by Members: The voicemail messages are saved in the group mailbox, and are shared by all members. Any members can manage the group voicemail messages.
     - Broadcast to Members: The voicemail messages are not stored in the group mailbox. Instead, the system broadcasts (copies and forwards) the voicemail messages to the individual mailboxes of all the members.
   - Voicemail PIN Authentication: Enable or disable voicemail PIN authentication.
   - Voicemail Access PIN: If enable voicemail PIN authentication, enter a desired access PIN number.
   - Play Date and Time: Optional. Play the date and time that the message was received before a voicemail message is played.
   - Play Caller ID: Optional. Play the caller ID information before a voicemail message is played.
   - Play Message Duration: Optional. Play the duration of the message before a voicemail message is played.
4. In the Members section, select the custom group members.
5. In the Group Voicemail Greeting section, select a voicemail greeting.

You can also click Greeting Management to customize a greeting or mange your custom greetings.

6. Click Save and Apply.

Related information

Enable or Disable Voicemail Access PIN
Change Voicemail Access PIN
Configure Message Envelope
Change Voicemail Greetings
Record or Upload Voicemail Greetings
Manage Group Voicemail Greetings

Manage Group Voicemails

This topic describes how to edit a group voicemail, and delete group voicemails.

Edit a group voicemail

1. Log in to PBX 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 Software Edition 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

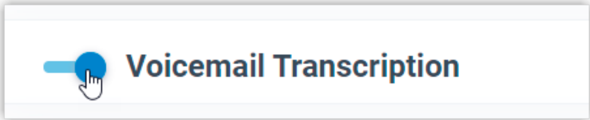
Prerequisites

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 Software Edition allows you to integrate with Google Cloud STT API service. For more information, see Integrate Yeastar P-Series Software Edition 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.



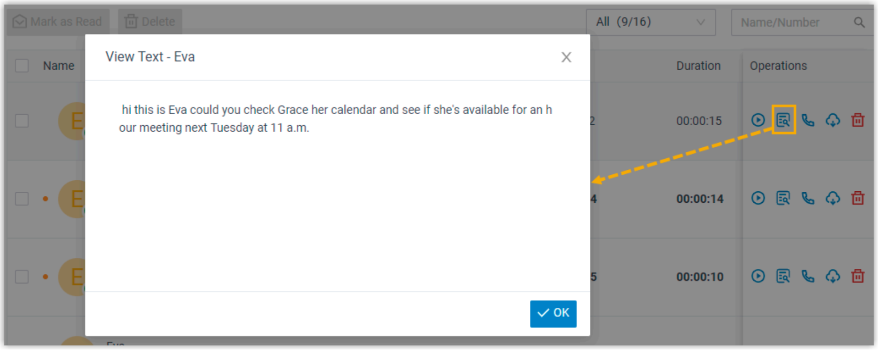
3. Click Save.

Result

The Voicemial Transcription feature is enabled, users can receive voicemails in the form of text on different platforms.

Linkus Web Client and Linkus Mobile Client

Users can check the transcribed text for each voicemail on Linkus Web Client and Linkus Mobile Client.



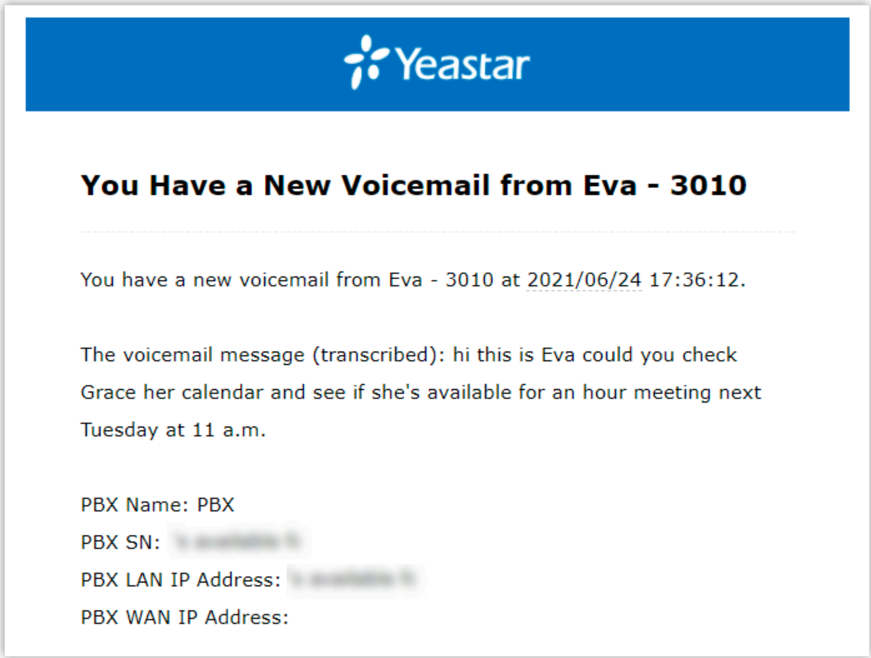
View Text - Eva

hi this is Eva could you check Grace her calendar and see if she's available for an h our meeting next Tuesday at 11 a.m.

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.



You Have a New Voicemail from Eva - 3010

You have a new voicemail from Eva - 3010 at 2021/06/24 17:36:12.

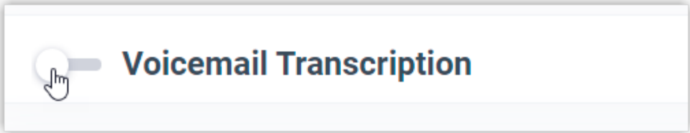
The voicemail message (transcribed): hi this is Eva could you check Grace her calendar and see if she's available for an hour meeting next Tuesday at 11 a.m.

PBX Name: PBX
PBX SN: [redacted]
PBX LAN IP Address: [redacted]
PBX WAN IP Address:

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 Software Edition 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, select a voicemail notification method or disable email notification.
    - Do not Send Email Notifications: Disable email notification.
    - Send Email Notifications without Attachment: Send a notification email as soon as receiving a new voicemail message in mailbox.
    - Send Email Notifications with Attachment: Send a notification email with the new voicemail message attached as a .wav file.

    > Note:
    >
    > If you use the default Voicemail to Email email template, the notification email contains the followings. To customize the email template, see Customize Email Templates.
    >
    > - Who left the message
    > - The caller ID
    > - When the message was left
    > - The transcribed voicemail text (Need to enable Voicemail Transcription first)
    > - The PBX device information

4. In the After Notification drop-down list, select a desired option from the drop-down list.
    - Do Nothing: Keep the voicemail messages in mailbox as unread.
    - Make as Read: Keep the voicemail messages in mailbox as read to prevent users from repeatedly receiving reminders on their phones.
    - Delete Voicemail: Delete the voicemail message to avoid mailbox being filled up.

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

5. Click Save and Apply.

Custom Voicemail Experience

Allow Callers to Press a Key to Leave Messages

This topic describes how to allow callers to press a key to leave messages.

Background information

By default, when the caller accesses a user's voicemail, PBX starts to record message automatically. It may make callers embarrassed when they are not ready to leave a message or they don't need to leave a message. Even if the caller hangs up directly, the voice mailbox still generates a lot of invalid information.

Procedure

1. Log in to PBX 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.

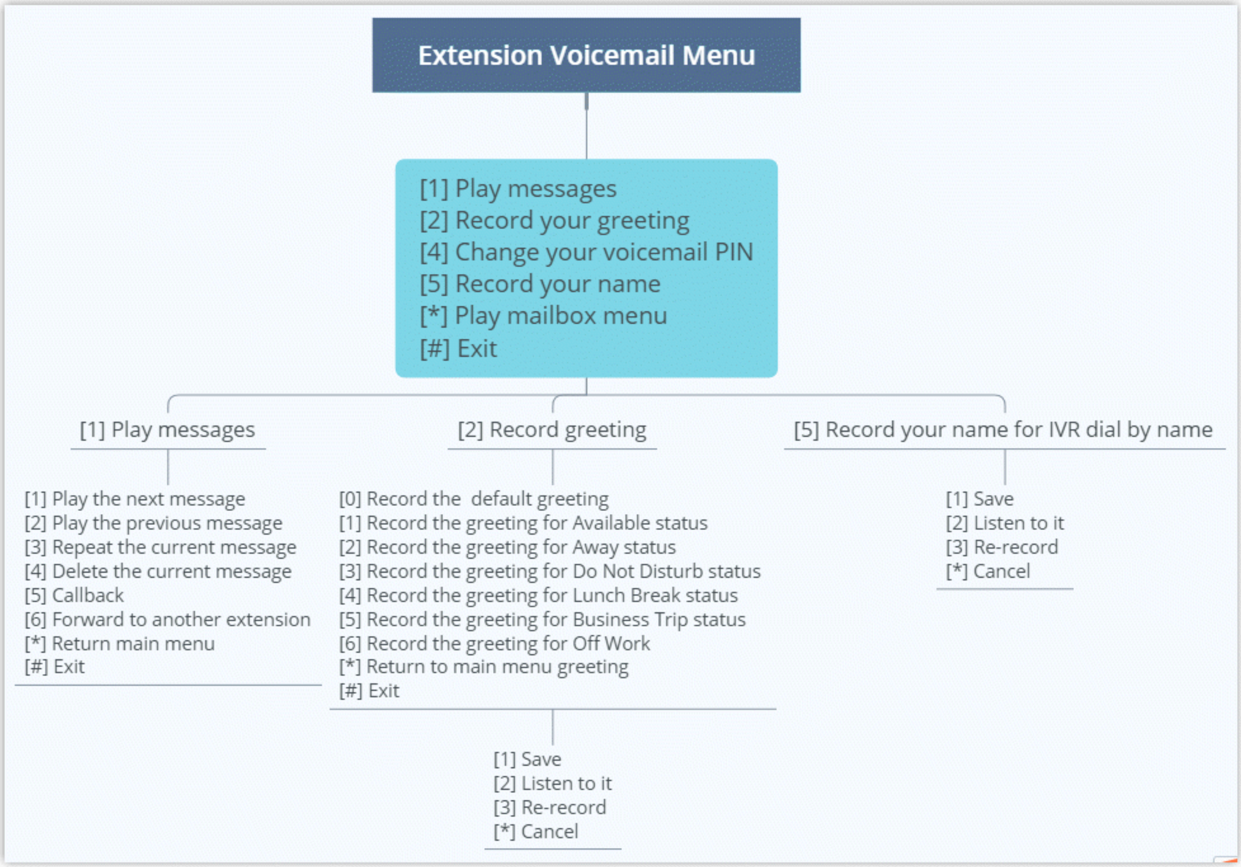
Voicemail Transcription

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



Extension Voicemail Menu

[1] Play messages
[2] Record your greeting
[4] Change your voicemail PIN
[5] Record your name
[*] Play mailbox menu
[#] Exit

[1] Play messages

[1] Play the next message
[2] Play the previous message
[3] Repeat the current message
[4] Delete the current message
[5] Callback
[6] Forward to another extension
[*] Return main menu
[#] Exit

[2] Record greeting

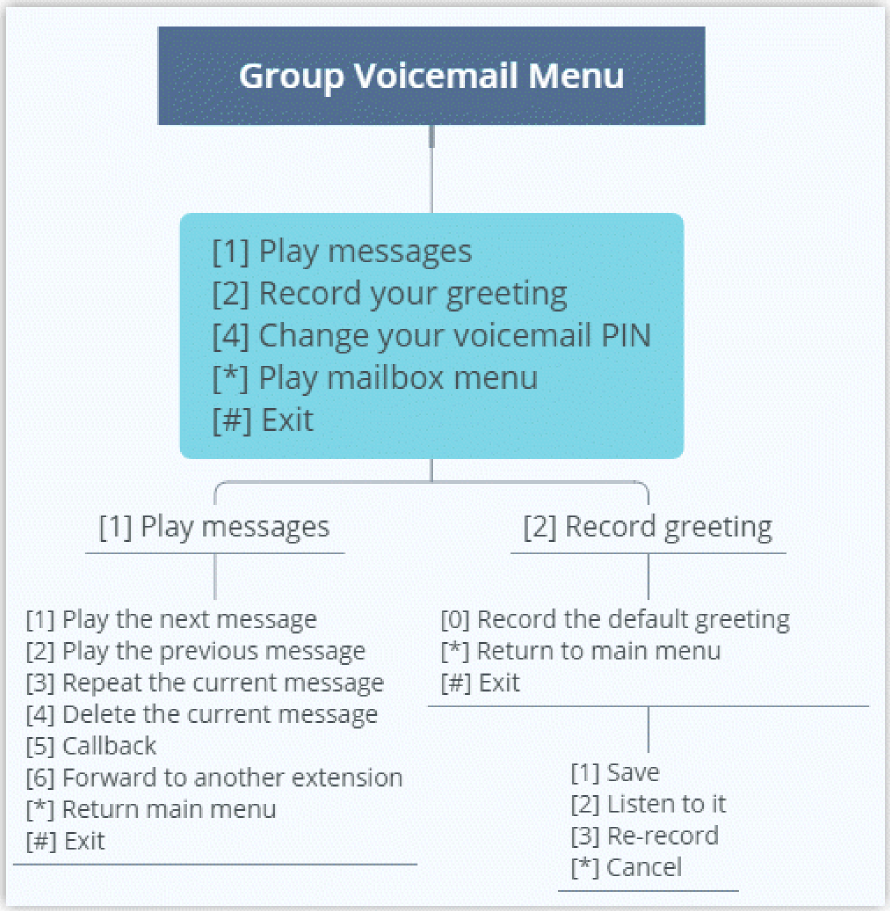
[0] Record the default greeting
[1] Record the greeting for Available status
[2] Record the greeting for Away status
[3] Record the greeting for Do Not Disturb status
[4] Record the greeting for Lunch Break status
[5] Record the greeting for Business Trip status
[6] Record the greeting for Off Work
[*] Return to main menu greeting
[#] Exit

[1] Save
[2] Listen to it
[3] Re-record
[*] Cancel

[5] Record your name for IVR dial by name

[1] Save
[2] Listen to it
[3] Re-record
[*] Cancel

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 Software Edition integrates a free IVR system. This topic describes what is IVR, what you can do with IVR, and what is multi-level IVR.

What is IVR?

Interactive Voice Response (IVR) is an automated telephony technology that interacts with callers, gathers information, and routes calls to the appropriate destinations. IVR can act as a virtual receptionist to handle large volumes of calls. It means that you don’t need a dedicated person to redirect calls to appropriate departments. With IVR, customers can get quick response or access appropriate service on their own.

What you can do with IVR?

Yeastar IVR uses customizable voice prompts to provide callers with instructions and directions for accessing information via phone, such as “press 1 for sales, and press 2 to leave a message.”. IVR connects callers to individuals, departments, call queues, etc, based on the customers' selections from voice menus.

Multi-level IVR is an alternative that allows you to assign a new IVR to an IVR option, and provides more powerful options to route incoming calls. Multi-level IVR gives you the flexibility to classify the menu of an interaction, such as divides a sales department into regions, and routes calls more precisely.

You can customize your IVR to provide a seamless experience.

For customer

- Play personal greeting to make the customer feel welcome.
- Allow customer to leave a voicemail.
- Allow customer to call employees directly by dialing extension or by name.

For employee

- Allow employees to make an outbound call via an IVR.
- Allow employees to check voicemail via an IVR.
- Allow employees to remotely change IVR prompt by dialing the feature code #9.

IVR keypress events

There are three types of keypress events:

- Menu options: The number keys, # key and * key for users to access a desired destination.
- Timeout: If no input is detected after the configured timeout, the PBX will forward the call based on the configuration.
- Invalid: When an invalid key is pressed, route the call to a desired destination.

Keypress destination

The following options are available for you to assign to the keypress events:

- Hang Up: End the current call.
- Extension: Route the call to the specified extension.
- Extension Voicemail: Allow callers to leave a message for the specified extension.
- Group Voicemail: Allow callers to leave a message for a queue, a ring group, or a custom group.
- IVR: Allow callers to enter another IVR menu.
- Ring Group: Route the call to a specified ring group.
- Queue: Route the call to a specified queue.
- 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 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 Software Edition 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.

     > Note:
     >
     > - If the total of PBX extensions is less than or equal to 6000, the default IVR number range is from 6200 to 6299.
     > - If the total of PBX extensions is greater than 6000, the default IVR number range is from 50200 to 50299.
   - Name: Enter an IVR name to help you identify it.
   - Prompt: Set the IVR prompt that plays greeting and explains the IVR menu options to callers.

     The default prompt is "Dial the extension number or press 0 for operator".

     You can select up to 5 audio files, and the system plays the audio files in order.
   - Prompt Repeat Count: Set how many times to play the prompt when the caller remains inactive during the Response Timeout(s).
   - Response Timeout(s): Set how long (in seconds) to wait for the caller to operate.
   - Digit Timeout(s): Set how long (in seconds) to wait for the caller to enter the next digit.
   - IVR Alert Info: Optional. Set an "alert info text" to add to Alert-info header in INVITE request for IVR calls.

     When receiving an IVR call, the phone will inspect "Alert-Info" header to determine which ring tone it should use for ringing.
   - Dial Extensions: Whether to allow callers to dial specific extension numbers via IVR.
     - Disable: Disable to dial extensions via IVR.
     - All Extensions: Allow the callers to dial all the extension numbers.
     - Allowed Extensions: Select the extensions that the callers can dial.
     - Restricted Extensions: Select the extensions that the callers can NOT dial.
   - Dial Outbound Routes: Whether to allow callers to make outbound calls via IVR.
   - Dial to Check Voicemail: Whether to allow users to check voicemail via IVR.
   - 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.
   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 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 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.

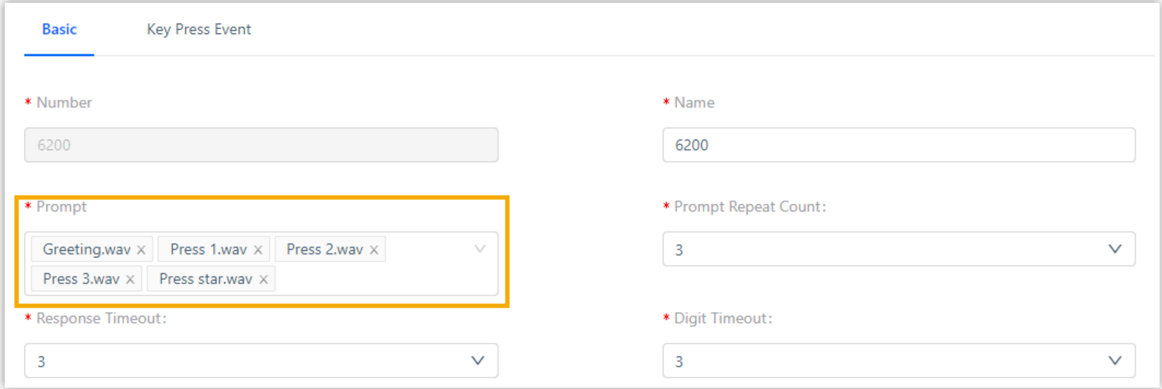
  The uploaded file should meet the audio file requirements. You can not upload an audio file larger than 8 MB. Divide the audio file into multiple audio clips to solve this issue.

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.



* Number: 6200

* Name: 6200

* Prompt: Greeting.wav × Press 1.wav × Press 2.wav × Press 3.wav × Press star.wav ×

* Prompt Repeat Count: 3

* Response Timeout: 3

* Digit Timeout: 3

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 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.

Procedures

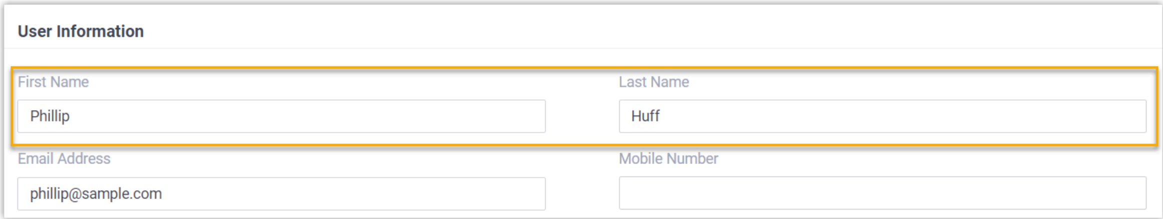
1. Specify an extension's caller ID name

2. Customize IVR prompt
3. 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.

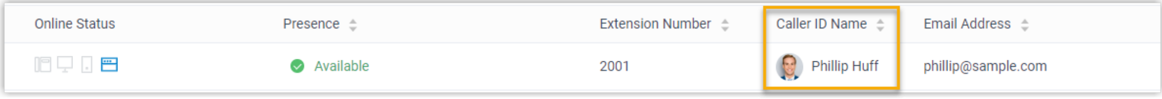
1. Log in to PBX web portal, go to Extension and Trunk > Extension, edit the desired extension.
2. In the User Information section, specify the First Name and Last Name for the extension.



User Information

First Name	Last Name
Phillip	Huff
Email Address	Mobile Number
phillip@sample.com	

3. Click Save and Apply.



Online Status	Presence	Extension Number	Caller ID Name	Email Address
	● Available	2001	Phillip Huff	phillip@sample.com

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.

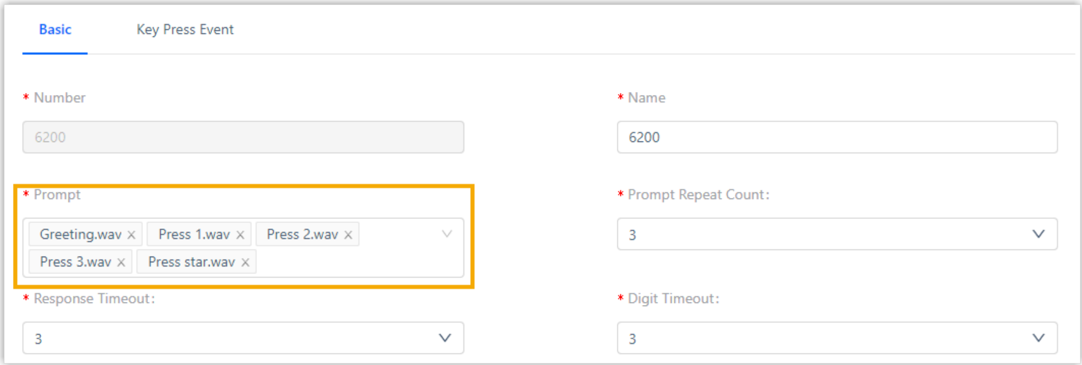
1. Log in to PBX web portal, go to PBX Settings > Voice Prompt > Custom Prompt.
2. Upload a custom prompt or record a custom prompt.

> 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.



* Number: 6200

* Name: 6200

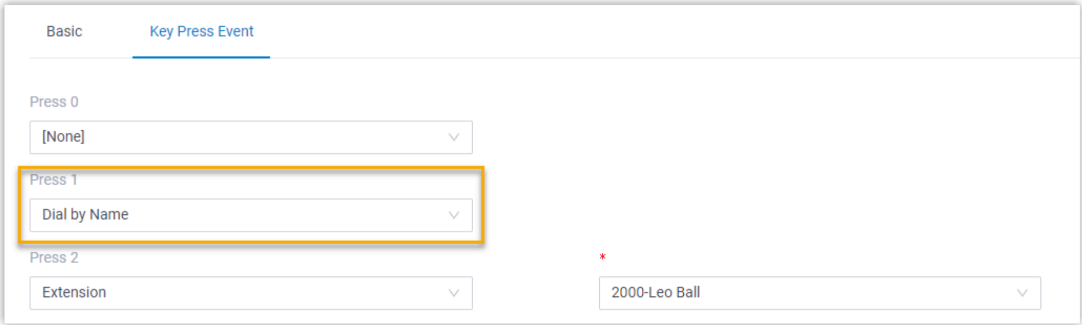
* Prompt: Greeting.wav, Press 1.wav, Press 2.wav, Press 3.wav, Press star.wav

* Prompt Repeat Count: 3

* Response Timeout: 3

* Digit Timeout: 3

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.



Press 0: [None]

Press 1: Dial by Name

Press 2: Extension; * 2000-Leo Ball

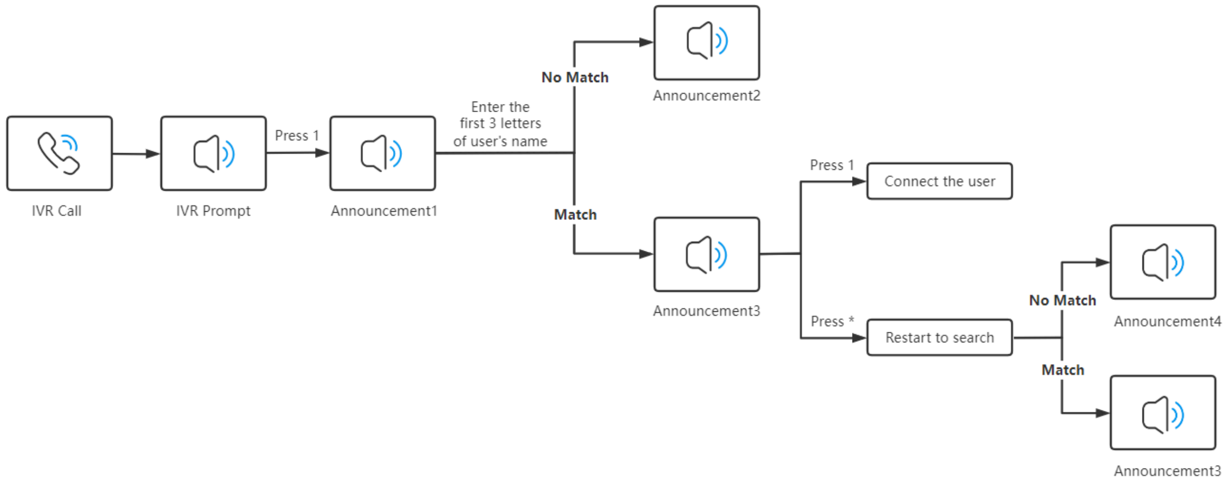
4. Click Save and Apply.

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 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 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.

Announcement	scenario
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.

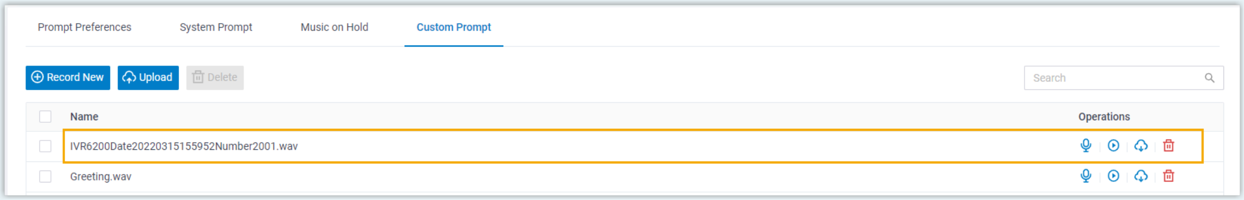
Result

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:

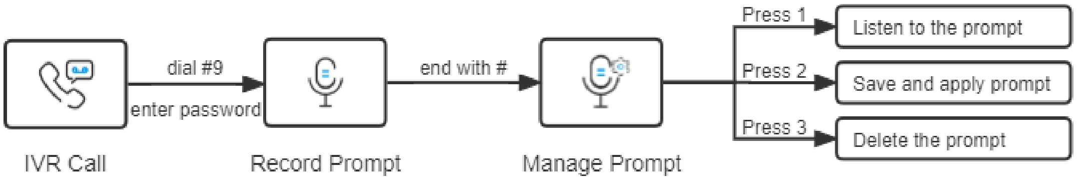
The new voice prompt is save on PBX Settings > Voice Prompt > Custom Prompt, with a prompt name in the format of IVR{ivr_number}Date{date}Number{extension_number}.



□	Name	Operations
□	IVR6200Date20220315155952Number2001.wav	
□	Greeting.wav	

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

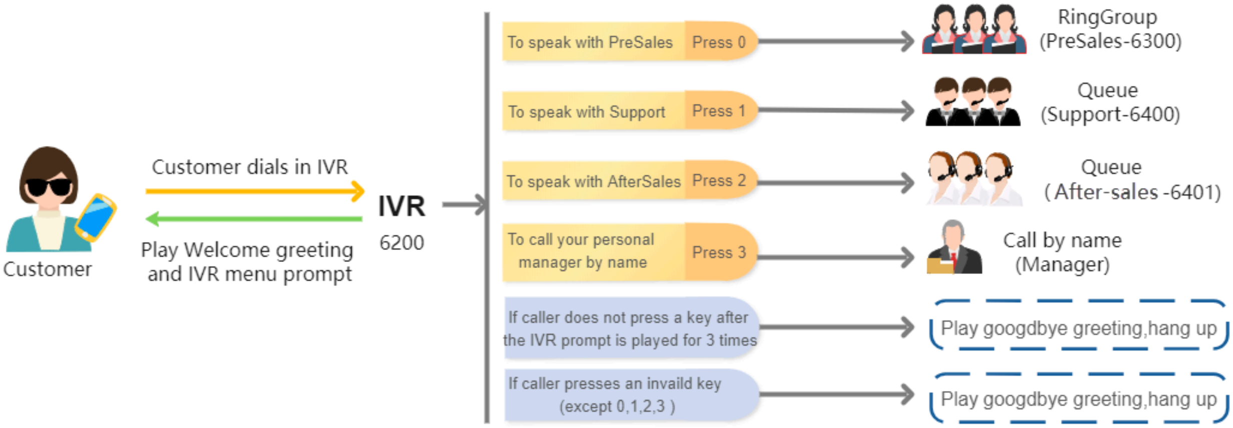
Background information

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.

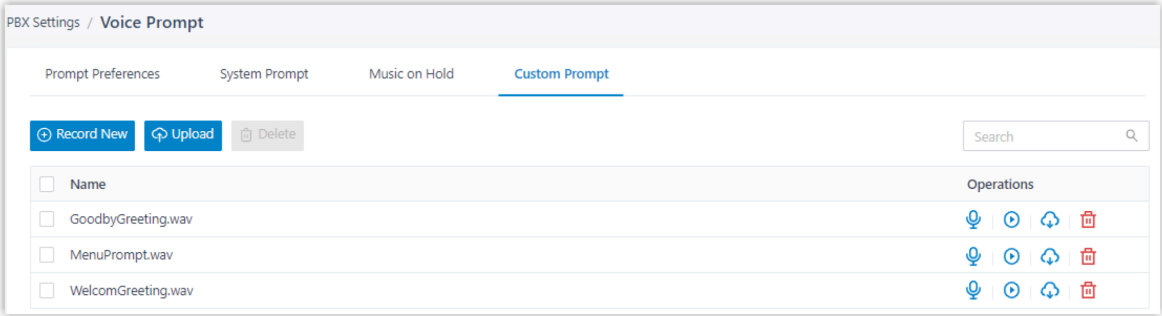
Step1. Design an IVR

When the customers dial in IVR (6200), they can access different service based on their business.


Customer
Customer dials in IVR
Play Welcome greeting and IVR menu prompt
IVR
6200
To speak with PreSales
Press 0
RingGroup (PreSales-6300)
To speak with Support
Press 1
Queue (Support-6400)
To speak with AfterSales
Press 2
Queue (After-sales -6401)
To call your personal manager by name
Press 3
Call by name (Manager)
If caller does not press a key after the IVR prompt is played for 3 times
Play googdbye greeting,hang up
If caller presses an invaild key (except 0,1,2,3)
Play googdbye greeting,hang up

Step2. Upload IVR Prompts

1. Go to PBX Settings > Voice Prompt > Custom Prompts, click Upload.
2. Select the audio files to upload.


PBX Settings / Voice Prompt

Prompt Preferences
System Prompt
Music on Hold
Custom Prompt

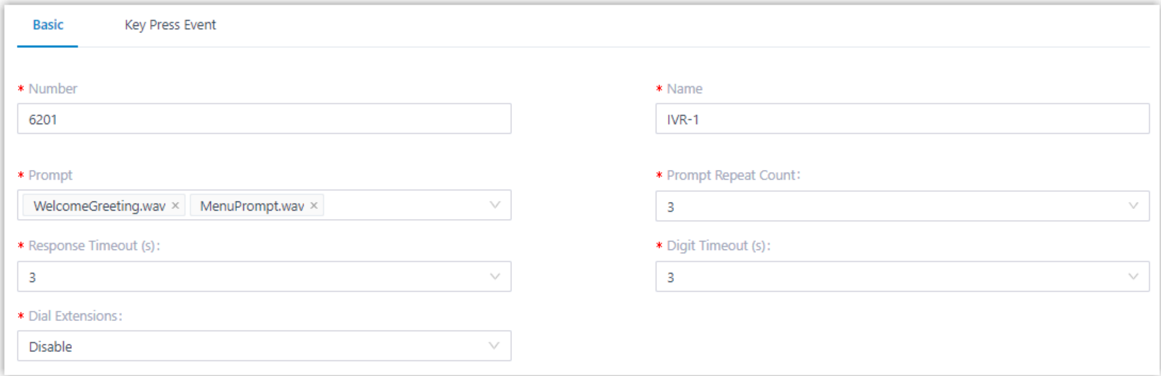
Record New
Upload
Delete
Search

	Name	Operations
□	GoodbyGreeting.wav	
□	MenuPrompt.wav	
□	WelcomGreeting.wav	

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.



* Number: 6201

* Name: IVR-1

* Prompt: WelcomeGreeting.wav × MenuPrompt.wav ×

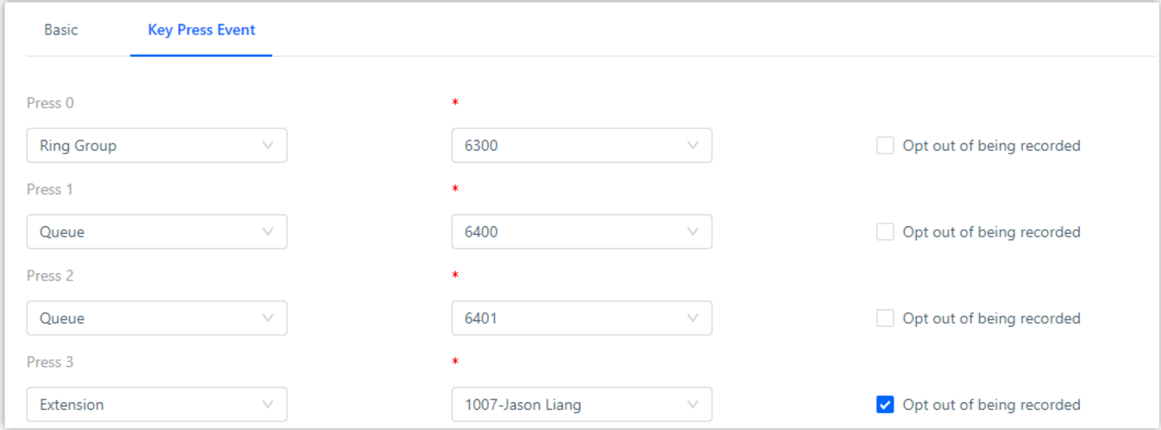
* Prompt Repeat Count: 3

* Response Timeout (s): 3

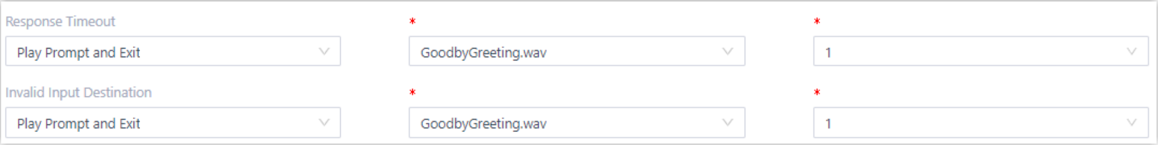
* Digit Timeout (s): 3

* Dial Extensions: Disable

3. In the Key Press Event tab, set up an IVR menu.



Press 0	*	
Ring Group	6300	☐ Opt out of being recorded
Press 1	*	
Queue	6400	☐ Opt out of being recorded
Press 2	*	
Queue	6401	☐ Opt out of being recorded
Press 3	*	
Extension	1007-Jason Liang	☑ Opt out of being recorded



Response Timeout	*	*
Play Prompt and Exit	GoodbyGreeting.wav	1
Invalid Input Destination	*	*
Play Prompt and Exit	GoodbyGreeting.wav	1

4. Click Save and Apply.

Multi-level IVR Configuration

Background information

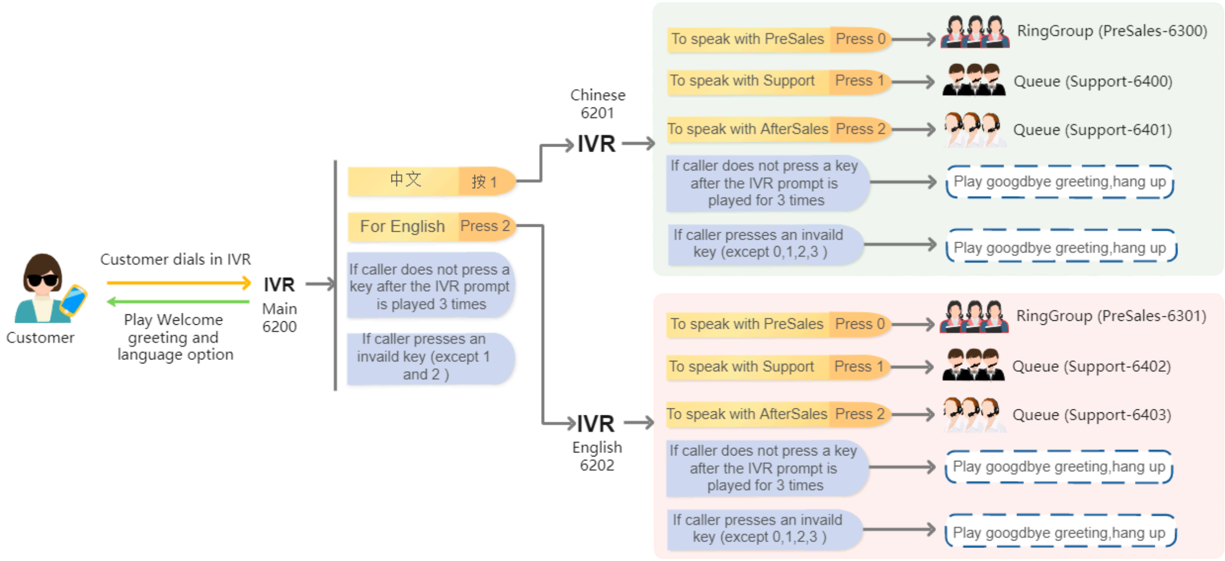
As business expands, the company needs to offer callers a bilingual auto-attendant feature based on their language selection. When the customer dials in to IVR, they can select a specific language to be used when playing prompts.

To achieve this, company needs to upgrade its IVR system allowing support of multi-language. We assume that all ring groups, call queues, extensions, audio prompts, and inbound routes used in this example are previously configured.

Step1. Design IVRs

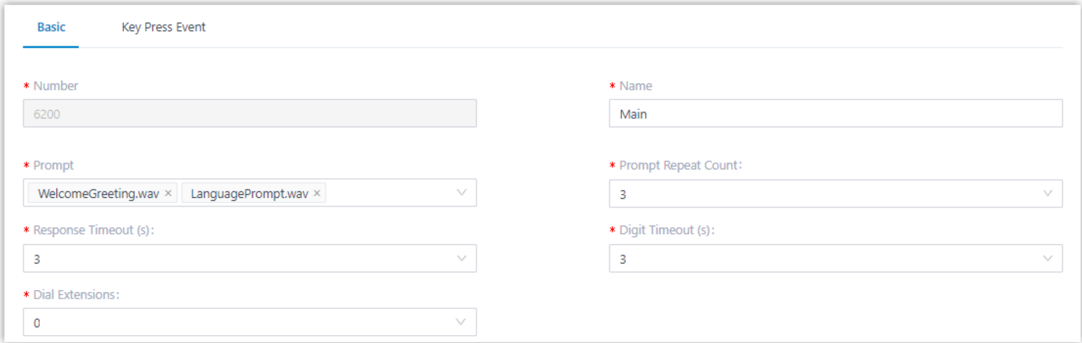
When the customers dial in to IVR-Main (6200), they can select a specific language to use.

- If customers select Chinese, the call will be redirected to IVR-Chinese (6201).
- If customers select English, the call will be redirected to IVR-English (6202).


Customer
Customer dials in IVR
Play Welcome greeting and language option
IVR
Main
6200
中文 按 1
For English Press 2
If caller does not press a key after the IVR prompt is played 3 times
If caller presses an invaild key (except 1 and 2)
Chinese
6201
IVR
To speak with PreSales Press 0
RingGroup (PreSales-6300)
To speak with Support Press 1
Queue (Support-6400)
To speak with AfterSales Press 2
Queue (Support-6401)
If caller does not press a key after the IVR prompt is played for 3 times
Play googdbye greeting,hang up
If caller presses an invaild key (except 0,1,2,3)
Play googdbye greeting,hang up
IVR
English
6202
To speak with PreSales Press 0
RingGroup (PreSales-6301)
To speak with Support Press 1
Queue (Support-6402)
To speak with AfterSales Press 2
Queue (Support-6403)
If caller does not press a key after the IVR prompt is played for 3 times
Play googdbye greeting,hang up
If caller presses an invaild key (except 0,1,2,3)
Play googdbye greeting,hang up

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.



Basic | Key Press Event

* Number: 6200

* Name: Main

* Prompt: WelcomeGreeting.wav × LanguagePrompt.wav ×

* Prompt Repeat Count: 3

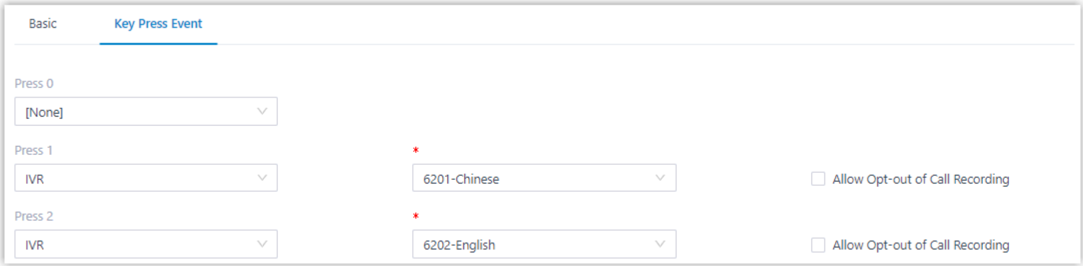
* Response Timeout (s): 3

* Digit Timeout (s): 3

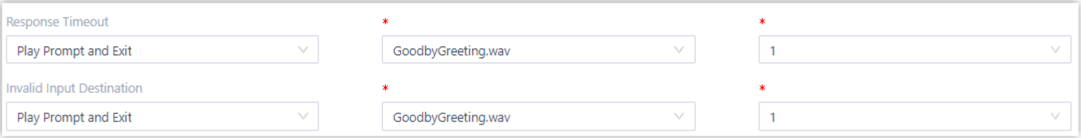
* Dial Extensions: 0

b. In the Key Press Event tab, set up an IVR menu.

- Specify IVR-Chinese (6201) for key 1.
- Specify IVR-English (6202) for key 2.



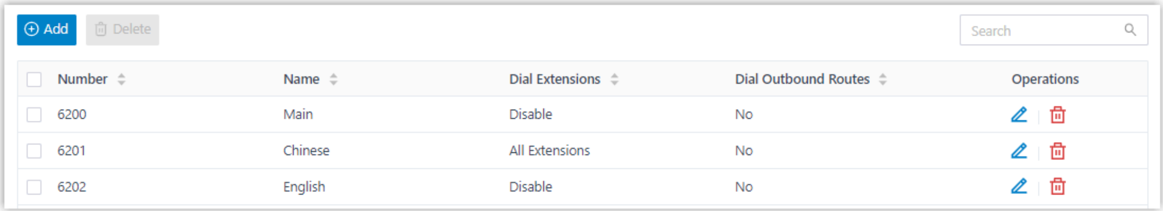
Press 0		
[None]		
Press 1	*	
IVR	6201-Chinese	□ Allow Opt-out of Call Recording
Press 2	*	
IVR	6202-English	□ Allow Opt-out of Call Recording



Response Timeout	*	*
Play Prompt and Exit	GoodbyGreeting.wav	1
Invalid Input Destination	*	*
Play Prompt and Exit	GoodbyGreeting.wav	1

3. Click Save and Apply.

The following figure displays the different IVRs created.



□	Number	Name	Dial Extensions	Dial Outbound Routes	Operations
□	6200	Main	Disable	No	
□	6201	Chinese	All Extensions	No	
□	6202	English	Disable	No	

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. 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

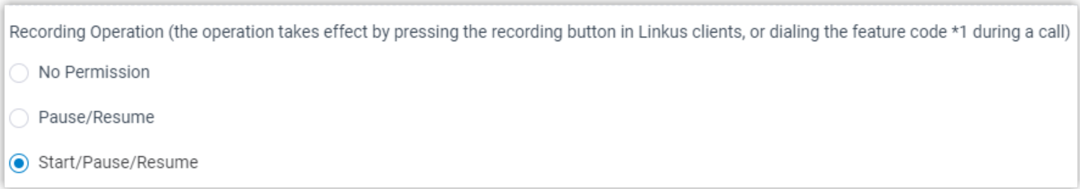
By default, if you set up call recording for extensions, trunks, conferences, or queues, the specified calls would be recorded as soon as they are established, and all the users can NOT switch call recording status. To avoid sensitive information being recorded or to allow users to start recording their 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 call recording permission to the extension user.
    a. In the Recording Operation section, grant recording operation permission to the extension user.

    Recording Operation (the operation takes effect by pressing the recording button in Linkus clients, or dialing the feature code *1 during a call)

    ○ No Permission

    ○ Pause/Resume

    ● Start/Pause/Resume

    - Pause/Resume: Allow users to pause or resume the recording during a call that is specified to be recorded.
    - Start/Pause/Resume: Allow users to start, pause, or resume the recording during any calls (except conference calls), be the calls specified to be recorded or not.

    > Tip:
    > To specify the calls to be recorded, see Set up Call Recording.

    b. Optional: To allow the extension user to view recordings, select the checkbox of Allow the extension to view recordings.
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).

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. Click ▶ beside the recording to which you want to listen.
    - Play on Web: Click ▶ to play the call recording on the web directly.
    - Play to Extension: Play the call recording on the phone.
        a. Select an extension, and click Play.

           The system places a call to the extension.

        b. Pick up the call to listen to the call recording on the phone.

Download recording files

> Note:
> You can download a maximum of 600 MB recording files or a maximum of 100 recording files at a time. The recordings that exceed the limit will not be downloaded.

1. Log in to PBX web portal, go to Reports and Recordings > Recording Files.
2. To download a recording file, click ⤓ beside a recording log.
3. To download multiple recording files, do the following:
    a. Select the checkboxes of recording files that you want to download.
    b. Click Download Recording(s).

Delete recording files

1. Log in to PBX web portal, go to Reports and Recordings > Recording Files.
2. Delete a recording file, or delete recording files in bulk.
    - Delete a recording: Select the recording file that you want to delete, click 🗑 and OK.
    - Delete recordings in bulk: Select the checkboxes of the recording files that you want to delete, click Delete and OK.

Auto Clean up Recording Files

Clean up old recording files to free up space. This topic describes how to set up auto cleanup of recording files.

Background information

By default, when the storage device reaches 80% of its maximum storage capacity, the PBX automatically deletes the oldest recording files.

Procedure

1. Log in to PBX web portal, go to System > Storage > Auto Cleanup > Recording Auto Cleanup.
2. In the Max Usage of Device (%) drop-down list, select the maximum storage percentage of the device that is allowed to store recording files.
3. In the Recordings Preservation Days, enter the maximum number of days that the recording files should be retained.

   The value `0` indicates no limit.
4. Click Save and Apply.

> Note:
>
> If Auto Clean up Reminder is enabled, and the retained recording files reach 90% of threshold, the system sends you a notification email. If the old recording files have continuing retention value, you can backup recording files or expand the retain limit in time.

Grant Manage Permission of Recording Files

By default, only the super administrator has permission to manage the call recording files. This topic describes how to grant manage permission to extension users.

Background information

As a super administrator, you can grant manage permission to a role, and assign the role to extension users. When the user logs in to the web client, he/she can manage recording files.

Procedure

1. Set up a user role.
   a. Log in to PBX 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.

Restrictions

The feature works for Linkus Web Client and Linkus Mobile Client:

- Linkus Web Client: Version 83.4.0.17 or later
- Linkus iOS Client: Version 4.3.8 or later.
- Linkus Android Client: Version 4.3.11 or later.

Procedure

1. Log in to PBX web portal, go to Extension and Trunk > Extension, edit a desired extension.
2. Click Features tab.
3. In the Call Recording section, unselect the checkbox of Allow the extension to view recordings.
4. Click Save.

Result

The extension user can not view recording files on Linkus Web Client and Linkus Mobile Client.

Ring Group

Ring Group Overview

Ring group is a feature to share the distribution of incoming calls among employees. This topic describes what is ring group, ring strategy, 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 three 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.

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.

      > Note:
      > - If the total of PBX extensions is less than or equal to 6000, the default ring group number range is from 6300 to 6399.
      > - If the total of PBX extensions is greater than 6000, the default ring group number range is from 50300 to 50399.
    - 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.
    - Ring Group Alert Info: Optional. Set an "alert info text" to add to Alert-info header in INVITE request for ring group calls.

      When receiving a ring group call, the phone will inspect "Alert-Info" header to determine which ring tone it should use for ringing.
    - Ring Timeout (s): Set a number of seconds that the system waits before ringing next member or routing the call to Failover Destination.
    - Members: Select the desired extensions from the Available box to the Selected box.
    - Failover Destination: Select a destination to route the call when no member answers the call within ring time.
        - Hang up: End the current call.
        - Extension: Route the call to the specified extension.
        - Extension Voicemail: Route the call to voicemail box of the specified extension.
        - Group Voicemail: Route the call to voicemail box of a queue, a ring group, or a custom group.
        - IVR: Route the call to the specified IVR.
        - Ring Group: Route the call to another ring group.
        - Queue: Route the call to the specified queue.
        - External Number: Route the call to an external number.
        - Play Prompt and Exit: Play a custom prompt, and then hang up the call.
    - 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 or Memory Hunt.
      >   - 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.

3. Click Save and Apply.

What to do next

Set up an inbound route, and specify the destination to the queue.

Manage Ring Groups

This topic describes how to edit a ring group, and delete ring groups.

Edit a ring group

You can edit the group settings, including adding or removing a member, or change the ring strategy.

1. Log in to PBX 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.

Queue components

A queue call consists of the following parts:

- Callers: Customers who place calls to the queue.
- Agents: Members who answer the queue calls (extensions or users who log in as agents).
    - Static agent: The agent is always a member of the queue and cannot log out.
    - Dynamic agent: The agent can log in to or log out of a queue at any time.
- Announcement: Announcements played to callers and agents, including agent ID announcement, position announcement, and periodic announcement.
- Music on Hold: Music or advertisements played to callers while waiting in the queue.
- Ring Strategy: A strategy for how to distribute calls to agents.
- Failover destination: A destination to which calls will be routed in the following scenarios.
    - The number of callers that wait in a queue reaches the Maximum Callers In Queue.
    - The time that callers wait reaches the Maximum Waiting Time.
    - No agents in queue and the caller is pulled out of a queue.

Call Center service

Call Center service is an additional service that drives faster call resolution and real-time call center monitoring, reporting, and management. It provides a powerful call center console, including a customizable Wallboard for proactive tracking of 16 key performance metrics, and a switchboard-type Queue Panel for real-time monitoring & control of queue activities, insightful call center reports, SLA and more.

For more information on call center service, see Call Center Console User Guide.

Note:

- For call center service, contact Yeastar support.
- Queue Panel is only recommended for queues with no more than 1000 extensions, otherwise the user experience will be affected as web browser can not work properly with excessive data volume.

Queue preference

Queue preference settings are available, including queue capacity, service level agreement, announcement, and satisfaction survey.

- Queue capacity
    - Define the maximum number of calls to wait in the queue.
    - Whether to pull the caller out of queue when no agents available in the queue.
    - Whether to allow the caller to join when no agents in the queue.

- Queue callback

  To save callers' time while keeping their positions in the queue, you can enable callback feature for the queue, and decide whether callers can press a digit or wait till timeout to request a callback.
- Service Level Agreement (SLA)

  With call center service activated, you can use SLA to define a certain level of service in a call center scenario, such as answering 80% of calls within 20 seconds.
- Announcement
  - Caller announcement, including the agent ID announcement and position announcement.
  - Periodic announcement
- Satisfaction survey

  In a call center scenario, you can make a satisfaction survey to collect customer feedback and evaluate agent performance.

Create a Queue

You can create and design queues to allow callers to talk with agents according to your business. This topic describes how to create a queue.

Prerequisites

- Customize a voice prompt as agent announcement.
- Configure the Music on Hold for the queue.

Procedure

1. Log in to PBX web portal, go to Call Features > Queue, click Add.
2. In the Basic page, configure the basic settings for the queue and agent settings.
   a. In the Basic section, configure the following settings:
      - Number: Enter a virtual number for callers to access the queue.

        > Note:
        > - If the total of PBX extensions is less than or equal to 6000, the default queue number range is from 6400 to 6499.
        > - If the total of PBX extensions is greater than 6000, the default queue number range is from 50400 to 50499.
      - Name: Enter a queue name to help you identify it.
      - Ring Strategy: Select a ring method to distribute calls to agents.
        - Ring All: Ring all available agents simultaneously until someone answers.
        - Least Recent: Ring the available agent that was least recently called.

        - Fewest Calls: Ring the available agent with the fewest completed calls.
        - Random: Ring the agents randomly.
        - Rrmemory: Round robin with memory.

          The system remembers the last agent it tried and rings the next agent.
        - Linear: Ring the available agent in specific order.
            - If there are only static agents in the queue, the system rings agents in the order specified in the agents list.
            - If there are only dynamic agents in the queue, the system rings agents in the order that agents have logged in.
            - If there are both static agents and dynamic agents in the queue, the system rings agents in the order that agents have logged in.
    - Music On Hold: Select a prompt to play to callers waiting for an available agent.
    - Maximum Waiting Time(s): Set a number of seconds that the caller can wait for an available agent.
    - Failover Destination: Select a destination to route the call when the call is not answered by any agent.
        - Hang up: End the current call.
        - Extension: Route the call to the specified extension.
        - Extension Voicemail: Route the call to voicemail box of the specified extension.
        - Group Voicemail: Route the call to voicemail box of a queue, a ring group, or a custom group.
        - IVR: Route the call to the specified IVR.
        - Ring Group: Route the call to another ring group.
        - Queue: Route the call to the specified queue.
        - External Number: Route the call to an external number.
        - Play Prompt and Exit: Play a custom prompt, and then hang up the call.

b. In the Agent Options section, configure the following settings.
    - Agent Timeout(s): Set a number of seconds that the system rings an agent's phone.
    - Retry Interval(s): Set a number of seconds to wait before ringing the next available agent when the last available agent has been ringed and timed out.
    - Wrap-up Time(s): Set a number of seconds for agents to complete post-call processing after finishing a call.

      The next call will come after this period following the ring strategy.
    - Agent Announcement: Select a prompt to play to agent prior to bridging in the caller.
    - Ring In Use: Set whether to distribute additional queue calls to the agents who are already in calls.

3. Click the Members tab, set agents for the queue.
    - Dynamic Agents: Select the dynamic agents that can log in to or log out of a queue at any time.

      > Note:
      > The queue distributes calls to the dynamic agents only when they log in to the queue and unpause the queue calls.
    - Static Agents: Select the static agents that always stay in the queue.

      > Note:
      > Static agents do not need to "log in" to the queue, and cannot "log out" of the queue.
4. Click Preferences tab to customize the queue according to your needs.

   For more information of the preference settings, see Queue Preferences.
5. Click Save and Apply.

What to do next

Set up an inbound route, and specify a destination to the queue.

Set Pause Reasons for Queue Agents

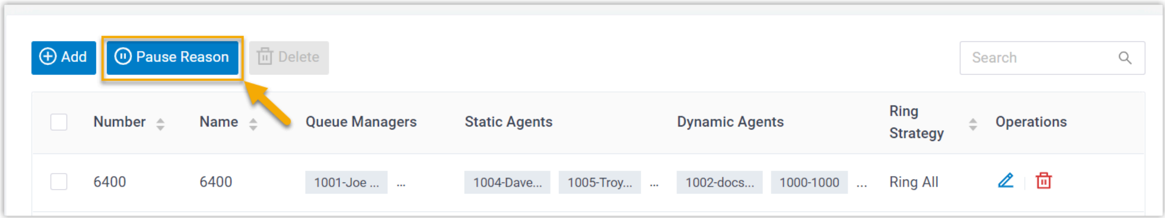
Yeastar P-Series Software Edition allows you to set specific reasons for pause status of queue agents. Agents can pause with reasons by feature code, or by dedicated button on their Linkus Clients. Queue managers can track the pause reasons and duration of agents in call reports.

Limitation

Yeastar P-Series Software Edition supports up to 20 pause reasons.

Procedure

1. Log in to PBX web portal, go to Call Features > Queue.
2. On the top of the queue list, click Pause Reason.

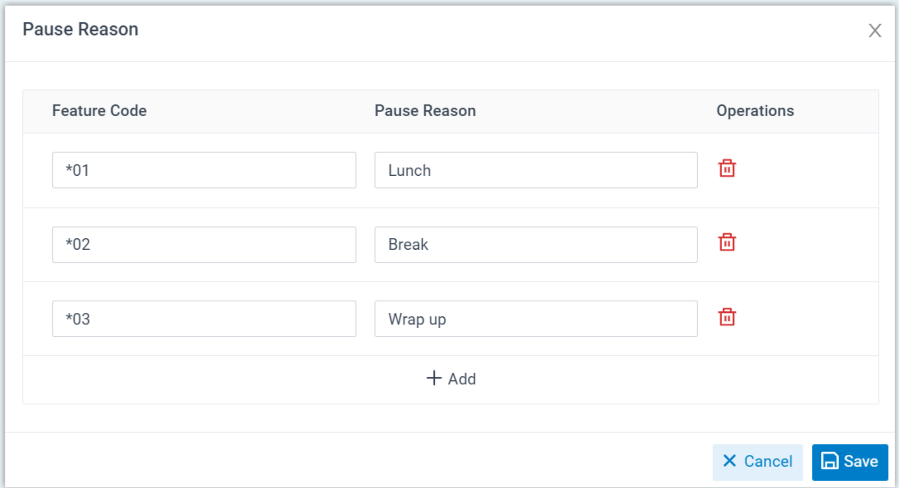


	Number	Name	Queue Managers	Static Agents	Dynamic Agents	Ring Strategy	Operations
□	6400	6400	1001-Joe	1004-Dave... 1005-Troy... ...	1002-docs... 1000-1000 ...	Ring All	

3. In the pop-up window, complete the following settings:

> Note:

Yeastar P-Series Software Edition provides the following default pause reasons and the corresponding feature codes. You can modify them or add new ones.



Pause Reason

Feature Code	Pause Reason	Operations
*01	Lunch	🗑
*02	Break	🗑
*03	Wrap up	🗑

a. Specify pause reasons and the corresponding feature codes.
    - Feature Code: Assign a feature code to the pause reason.
    - Pause Reason: Specify the reason why an agent pauses receiving calls.

b. Click Save.

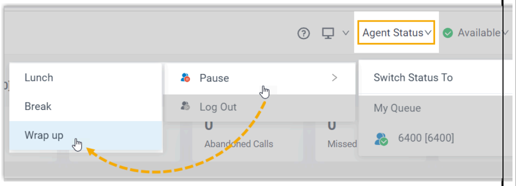
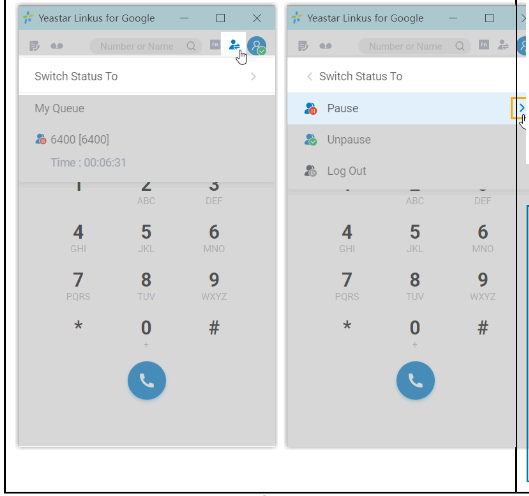
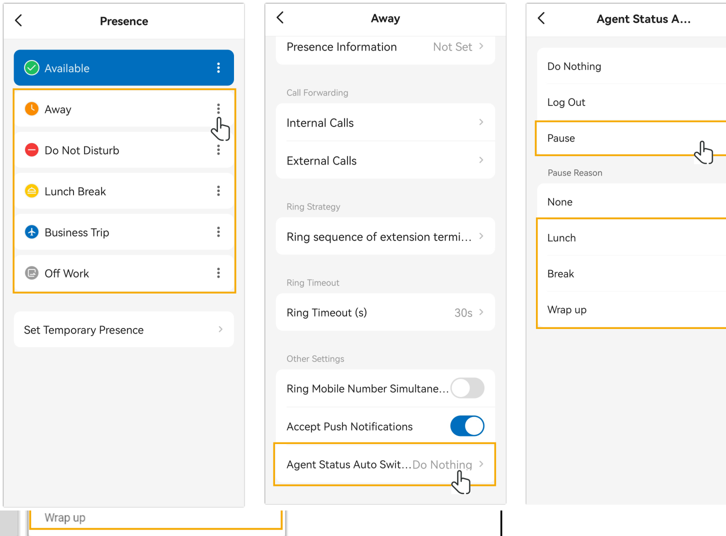
Result

- The pause reasons are available for all queues in the PBX.
- Queue agents can pause with reasons in the following ways:
    - By feature code

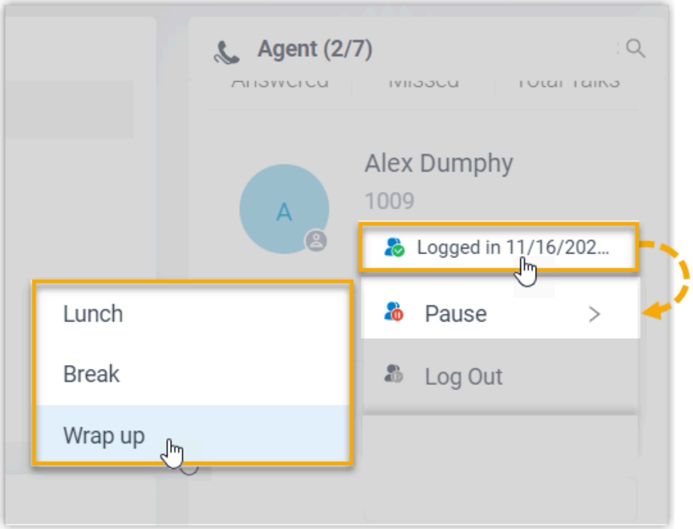
      Queue agents can dial Pause Feature Code + Queue Number + Pause Reason Feature Code to pause from a queue for corresponding reason.

      > Tip:
      > You can obtain the Pause feature code on Call Features > Feature Code > Queue > Pause/Unpause.

      For example, an agent dials "*076400*03" to pause from queue 6400 for Wrap up reason.
    - By dedicated button on Linkus Clients
      Queue agents can click Pause button and select a specific pause reason on their Linkus Clients, as shown in the following table.

Linkus Web Client	Linkus Mobile Client
On web page  On 'Yeastar Linkus for Google' Chrome extension 	 **Note:** To use the feature, the App version should be updated. ▪ Linkus Android Client: 4.10.6 or later ▪ Linkus iOS Client: 4.10.3 or later

- Queue managers can switch agents to pause on a specific reason from the queue panel.



Related information

['Agent Pause Activity' Report](#)

Monitor Specific Pause Status of an Agent by Function Key

Manage Agent Status by Dialing a Feature Code

This topic describes how to manage agent status by dialing a feature code.

Background information

The PBX defines feature codes that allow the agents to switch their status. You can change, enable, or disable the feature code on PBX web portal: Call Features > Feature Code > Queue.

The default feature codes for switching agent status:

- Log in/Log out: *7
- Pause/Unpause: *07

> Note:
>
> Yeastar P-Series Software Edition provides three default reasons for agent pause status. You can change the pause reasons and feature codes on Call Features > Feature Code > Pause Reason. After that, agents can pause with specific reason by dialing the feature codes.

Log in to a queue

Only dynamic agents can log in to a queue; static agents are always in the queue.

For example, a dynamic agent dials `*76400` to log in to queue 6400.

Log out of a queue

Only dynamic agents can log out of a queue; static agents are always in the queue.

For example, a dynamic agent 1000 dials `*76400` to log out of queue 6400.

Pause receiving queue calls

Both static agents and dynamic agents can pause queue calls when they are away from desk. The system will not distribute queue calls to the agents in "Paused" status.

Pause without reason

For example, an agent 1000 dials `*076400` to directly pause calls from queue 6400.

Pause with specific reason

For example, an agent 1000 dials `*076400*03` to pause calls from queue 6400 for after-call processing.

Unpause receiving queue calls

Both static agents and dynamic agents can unpause queue calls when they are ready to take calls.

For example, an agent 1000 dials `*076400` to unpause calls from queue 6400.

Related information

- Monitor and Switch Agent Status on an IP Phone
- Monitor Specific Pause Status of an Agent by Function Key

Monitor and Switch Agent Status on an IP Phone

This topic describes how to set up function keys on agents' phones to monitor and switch agent status.

Background information

There are two ways to monitor and switch agent status:

- Function key: For agents who want to monitor their own status in a specific queue on their phones, you can set a function key for each agent by auto provisioning.

  > Note:
  > Agents can also set function keys on their own IP phones. For more information, contact the phone manufacturer.

- Queue Panel: Agents can monitor and switch their status on Queue Panel. For more information, see Call Center Console User Guide.

Procedure

Assume that an agent Sunmy wants to monitor and switch her status in the "Support" queue on IP phone.

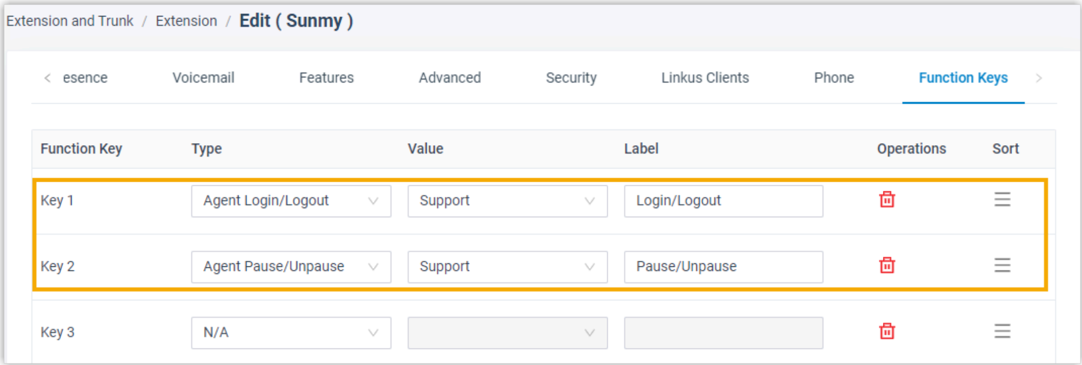
You can set two function keys for the agent Sunmy as follows:

1. Assign function keys for the agent.
    a. Log in to PBX web portal, go to Extension and Trunk > Extension, edit the agent's 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 agent exceeds the number of programmable keys, the redundant function keys cannot take effect.

- Type: Select a key type.
  - Select Agent Login/Logout for logging in to or logging out of a queue.
  - Select Agent Pause/Unpause for pausing or unpausing receiving queue calls.
- Value: Select the "Support" queue that the agent sits in.
- Label: Optional. Enter a value, which will be displayed on the phone screen.

d. Click Save.



Function Key	Type	Value	Label	Operations	Sort
Key 1	Agent Login/Logout	Support	Login/Logout	🗑	☰
Key 2	Agent Pause/Unpause	Support	Pause/Unpause	🗑	☰
Key 3	N/A			🗑	☰

2. If the agent hasn't been associated with a phone, see the following topics to bind a phone with the agent.
   - 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 agent has been associated with a phone, reprovision the phone to take effect.

   a. Go to Auto Provisioning > Phones.

   b. Click ↻ beside the phone assigned to the agent.

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

Result

The LED status of function keys shows the agent's status in real time.

Note:
The key LED status may vary by phone models.

Function key	LED status	Description
Log in/Log out	Green	The monitored agent has logged in to the queue and unpaused queue calls. The agent can press the Log in/Log out function key to log out of the queue.

Function key	LED status	Description
	Red	The monitored agent has logged out of the queue. The agent can press the Log in/Log out function key to log in to the queue.
	Off	The function key does not subscribe the agent's status. Check if your configurations are correct or if the agent's extension is registered.
Pause/unpause	Green	The monitored agent has logged in to the queue and unpaused queue calls. The agent can press the Pause/Unpause function key to pause receiving queue calls.
	Flashing Red	The monitored agent has paused receiving queue calls. The agent can press the Pause/Unpause function key to resume receiving queue calls.
	Off	The function key does not subscribe the agent's status. Check if your configurations are correct or if the agent's extension is registered.

Related information

Monitor Specific Pause Status of an Agent by Function Key

Monitor Specific Pause Status of an Agent by Function Key

This topic provides an example on how to monitor specific pause status of an agent by function key on Linkus Web Client, or on an IP phone.

Prerequisites

- 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)
- To monitor specific agent pause status on an IP phone, make sure that the IP phone is connected to Yeastar P-Series Software Edition via auto provisioning, and has been assigned with an extension.

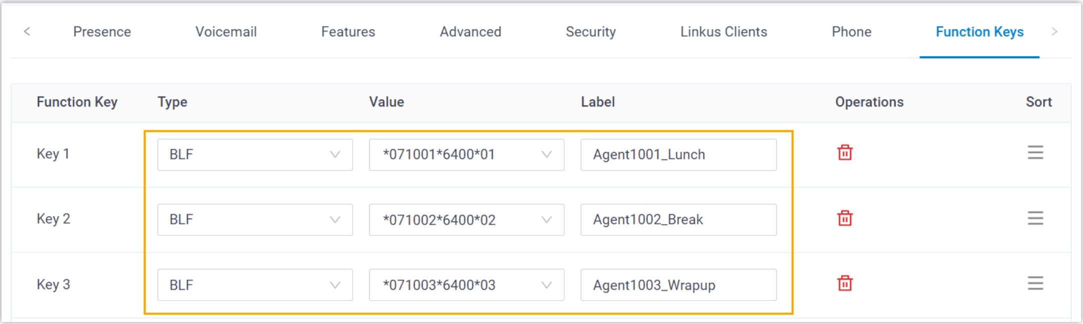
> Note:
>
> For more information about auto provisioning, see the following topics:
>
> - Auto Provision IP Phones in Local Network (PnP Method)

- ◦ 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

Assume that you want to monitor the three default pause status of agents 1001, 1002 and 1003 in queue 6400, do as follows to configure function keys for your extension.

1. Set up function keys for monitoring specific pause status.
    a. Log in to PBX web portal, go to Extension and Trunk > Extension, edit your extension.
    b. Click the Function Keys tab.
    c. Configure the following function keys.



Function Key	Type	Value	Label	Operations	Sort
Key 1	BLF	*071001*6400*01	Agent1001_Lunch	🗑	≡
Key 2	BLF	*071002*6400*02	Agent1002_Break	🗑	≡
Key 3	BLF	*071003*6400*03	Agent1003_Wrapup	🗑	≡

- 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 display label for the function key.

    d. Click Save.

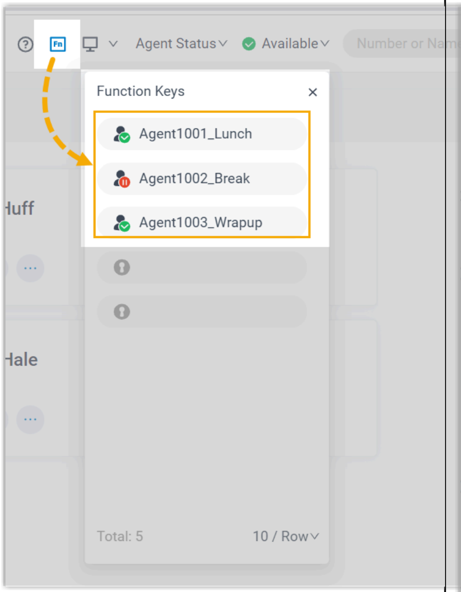
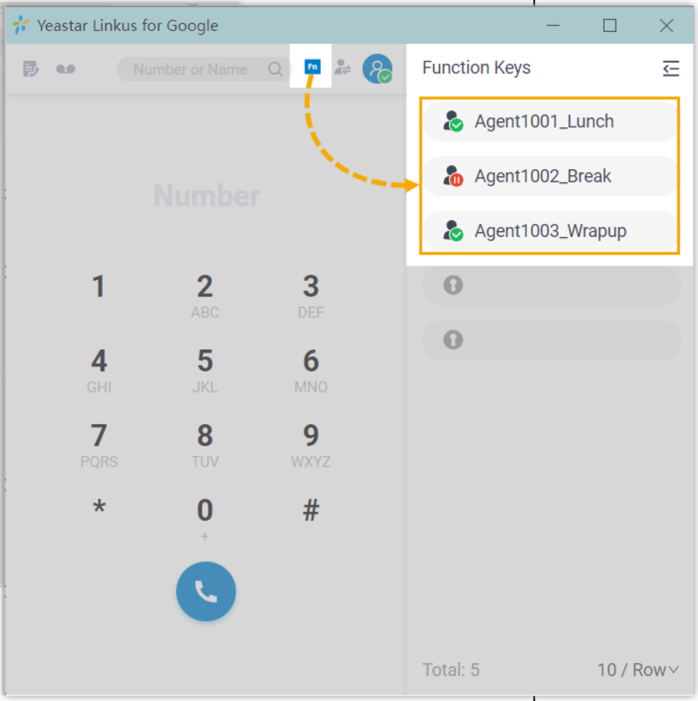
2. If you want to monitor specific agent pause status on IP phone, apply the function key configuration to the IP phone.
    a. Go to Auto Provisioning > Phones, click ↻ beside the desired phone.
    b. In the pop-up window, click OK.

Result

You can monitor specific pause status of the agents via the followings:

Function key on Linkus Web Client and Linkus Chrome extension

- ✓: The monitored agent is NOT in the specified pause status.
- ⏸: The monitored agent is in the specified pause status.
- ⊗: The function key configuration failed.

Linkus Web Client	'Yeastar Linkus for Google' Chrome extension
 Agent Status Available Number or Name Function Keys Agent1001_Lunch Agent1002_Break Agent1003_Wrapup Huff Hale Total: 5 10 / Row	 Yeastar Linkus for Google Number or Name Number 1 2 ABC 3 DEF 4 GHI 5 JKL 6 MNO 7 PQRS 8 TUV 9 WXYZ * 0 + # Function Keys Agent1001_Lunch Agent1002_Break Agent1003_Wrapup Total: 5 10 / Row

BLF LED on IP phone

- BLF LED Solid Green: The monitored agent is NOT in the specified pause status.
- BLF LED Flashing Red: The agent is in the specified pause status.
- BLF LED off: The BLF key configuration failed.

Manage Call Queues

You can not change the queue number after setting up a queue. This topic describes how to edit a queue, and delete queues.

Edit a queue

You can manage the agents, change the ring strategy, or other queue settings.

1. Log in to PBX web portal, go to Call Features > Queue.
2. Click ✎ beside the queue that you want to edit.
3. Change the queue settings according to your needs.
4. Click Save and Apply.

Delete queues

1. Log in to PBX web portal, go to Call Features > Queue.
2. To delete a queue, do the followings:
   a. Click 🗑 beside the queue that you want to delete.
   b. Click OK and Apply.
3. To delete queues in bulk, do the followings:
   a. Select the checkboxes of the queues that you want to delete, click Delete.
   b. Click OK and Apply.

Queue Preferences

This topic describes the queue preference settings, including distinctive ring tone, queue capacity, queue callback, service level agreement, announcement, and satisfaction survey.

Distinctive ring tone

Setting	Description
Queue Alert Info	Set an "alert info text" to add to Alert-info header in INVITE request for queue calls. When receiving a queue call, the phone will inspect "Alert-Info" header to determine which ring tone it should use for ringing.

Queue capacity

Setting	Description
Maximum Callers in Queue	The maximum number of callers that can wait in the queue. The default value is 0 (unlimited). Note: When the number of callers waiting in queue reaches the Maximum Callers In Queue, the system routes the additional calls to Failover Destination.
Leave Empty	Pull the caller out of a queue when no agent is in the queue, and forward the call to the Failover Destination.

Setting	Description
Join Empty	Allow callers to join a queue when there is no agent in the queue.

Callback

Setting	Description
Request Callback Method	Define how a caller can request a callback when the queue is busy.
Digit to press	Define what digit a caller can press to request a callback when the queue is busy. Note: The option is available only when Request Callback Method is set to Triggered by caller input.
Timeout (s)	Define the amount of time (in seconds) that a caller can wait in the queue. After the timeout, the system will play the callback option to the caller automatically. Note: The option is available only when Request Callback Method is set to Auto triggered after the timeout.
Callback Outbound Prefix	Define the prefix of outbound route, which will be used to call the callback number. Note: All agents in this queue must have permission to use this outbound route, or the callback would fail.

Service level agreement

Setting	Description
SLA Time(s)	The maximum amount of time (in seconds) that an agent needs to answer an incoming call. The default SLA time is 60 seconds.

Setting	Description
Evaluation Interval(min)	The time interval to compare the queue's SLA performance against the alarm threshold, so the system can send a notification email accordingly.
Alarm Threshold(%)	The service level threshold for the queue. The default alarm threshold is 80%.

Announcement

Setting	Description
Announcement	
Join Announcement	The announcement played to callers before they join the queue.
Agent ID Announcement	The announcement played to callers to prompt the agent ID. • Default: The system plays the prompt “{extension_number} will be connected. Please wait”. • Custom prompt: If you choose your custom prompt, the system will play {extension_number} + your custom prompt.
Play "Thank You for Your Patience" Prompt	Play the prompt "Thank You for Your Patience" to callers periodically while the caller is waiting in a queue.
Call Position Announcement	
Announce Position	Announce position of caller in the queue.
Announce Hold Time	Announce the hold time to the caller periodically based on Frequency.
Frequency(s)	The time interval to announce queue position and estimated hold time to the caller.
Queue Announcements	
Prompt	The announcement played to callers periodically.
Frequency(s)	The time interval to play the announcements.

Satisfaction survey

Setting	Description
Satisfaction Survey Prompt	The prompt played to caller to ask the caller to rate their satisfaction scale after the agent hangs up. The default prompt is "Please rate your satisfaction with our service, press 1 for satisfied, press 2 for dissatisfied. Thank you.". "Thanks for your calling, goodbye." is prompted after the caller presses a key.
Satisfaction Survey Points	The scores for the keys that the caller can press to rate an agent's service. Note: This allows you to collect customer feedback and gain valuable insight into agent performance. You can check satisfaction survey score in Satisfaction Survey report and Satisfaction Survey Details report. For more information, see 'Satisfaction Survey' Report and 'Satisfaction Survey Details' Report.

Key Press Event

Setting	Description
Key	The caller can press the key to enter the specific destination when waiting in queue. Generally, set a Periodic Announcements to guide the callers to press the key.
Key Destination	The destination to route the call when the caller presses a key. • Hang up: End the current call. • Extension: Route the call to the specified extension. • Extension Voicemail: Route the call to voicemail box of the specified extension. • Group Voicemail: Route the call to group voicemail box of a queue, a ring group, or a custom group. • IVR: Route the call to the specified IVR.

Setting	Description
	• 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.

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 Software Edition 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, 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.

Call Forwarding

Name	Default code	Usage
Enable "Forward All Calls"	*31	• Dial *31 to forward all calls to one's own voicemail. • 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.

Intercom

Name	Default code	Usage
Intercom	*6	Dial *61001 to place an intercom call to extension 1001.

Queue

Name	Default code	Usage
Log in/Log out	*7	A dynamic agent dials *76400 to log in to or log out of queue 6400.
Pause/Unpause	*07	A dynamic agent dials *076400 to pause or unpause calls from queue 6400.

Pause Reason

Yeastar P-Series Software Edition 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 Software Edition 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.

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.
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.

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.

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 Global Business Hours and Holidays Status	*99	Dial *99 to override time condition for Global 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.

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 Software Edition 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 Software Edition 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.
    - 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..

   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 the following:
    a. Click 🗑 beside the speed dial entry that you want to delete.
    b. Click OK and Apply.
3. To delete speed dial numbers in bulk, do the following:
    a. Select the checkboxes of the speed dial entries that you want to delete, click Delete.
    b. Click OK and Apply.

Export and Import Speed Dial Numbers

The speed dial numbers configured on Yeastar P-Series Software Edition 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.

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. Click Save and Apply.

Perform an Attended Transfer

If you want to make sure someone is ready to take a transferred call or you need to explain something to the transfer recipient, you can perform an attended transfer. This topic describes how to perform an attended transfer.

Procedure

1. During a call, press the feature code of attended transfer (default *3).

   The original call is placed on hold, and the system prompts "transfer" and the dial tone.
2. Dial the phone number of the contact where you want the call to be transferred.
3. Wait for the call to be answered.

   When the call is answered, talk to the transfer recipient.
4. Hang up the call directly to complete the call transfer.

   The original caller and the transfer recipient are connected.

Perform a Blind Transfer

If you do not need any interaction with the user who receives the call, you can perform a blind transfer. This topic describes how to perform a blind transfer.

Procedure

1. During a call, press the feature code of blind transfer (default *03).

   The original call is placed on hold, and the system prompts "transfer" and the dial tone.
2. Dial the phone number of the contact where you want the call to be transferred.

   The call ends automatically, and the transfer recipient's phone rings.

   A new call between original caller and transfer recipient is established after transfer recipient answers.

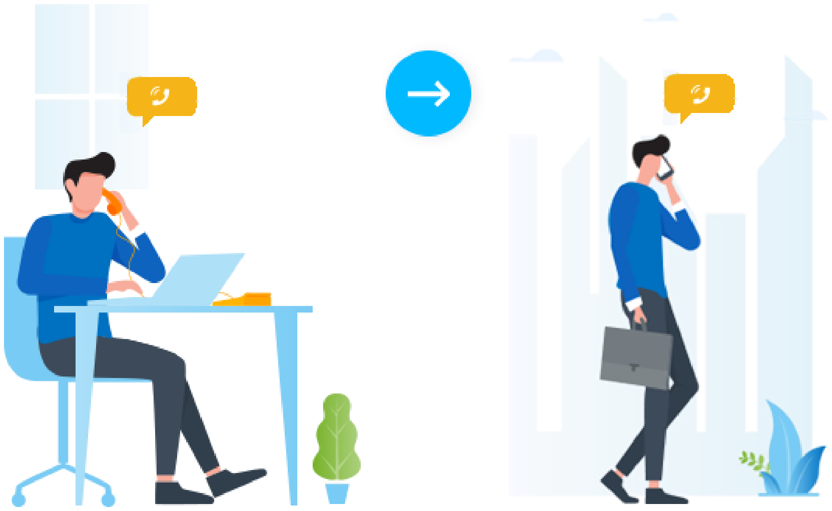
Call Flip

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:

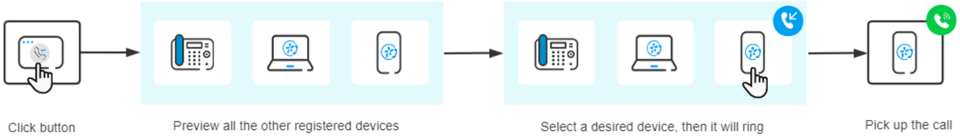
- Flip an active call by clicking 'Call Flip' button

- 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:


Click button
Preview all the other registered devices
Select a desired device, then it will ring
Pick up the call

This method is supported on the following endpoints:

- Linkus Mobile Client

  For more information, see How to flip an active call between devices?
- Linkus Web Client

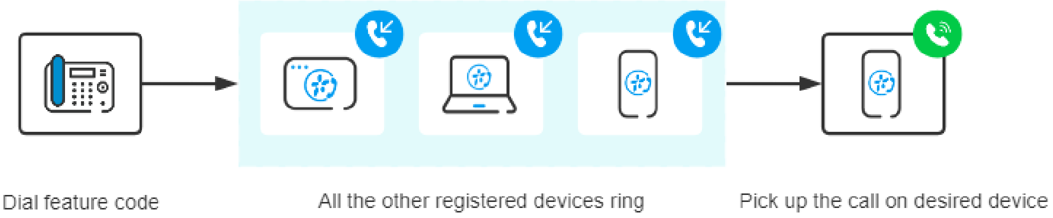
  For more information, see Flip an Active Call between Devices.

> 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:


Dial feature code
All the other registered devices ring
Pick up the call on desired device

With the Call Flip feature code enabled on Yeastar P-Series Software Edition, 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.

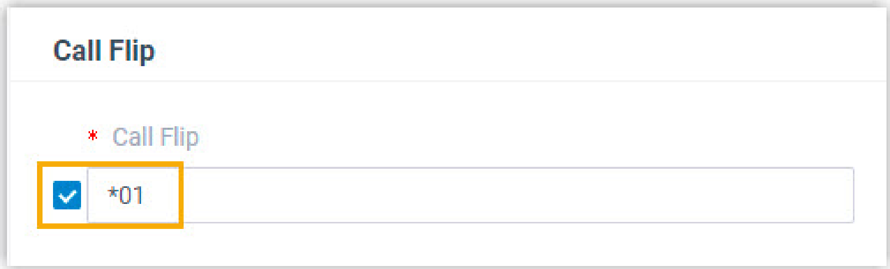
For more information about how to flip an active call by dialing the feature code, see Flip an Active Call by Dialing a Feature Code.

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.



Call Flip

* Call Flip

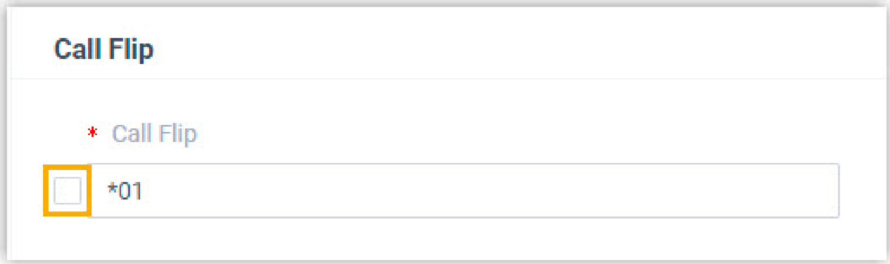
☑ *01

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.



Call Flip

* Call Flip

☐ *01

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: 83.8.0.25 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)
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: Enter the code (`*04`) followed by extension number (for example *041001).
        - Label: Optional. Enter a value, which will be displayed on the phone screen.

    d. Click Save.
2. If the extension hasn't 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

- 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 re-call, 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 Software Edition 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:

Assume that the 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 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 Parking Number

This topic describes how to define the range of parking numbers for parked call.

Background information

Default range of parking number varies according to the total of PBX extensions.

- If the total of PBX extensions is less than or equal to 6000, the default range of parking number is from 6000 to 6099.
- If the total of PBX extensions is greater than 6000, the default range of parking number is from 50010 to 50099.

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.

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.

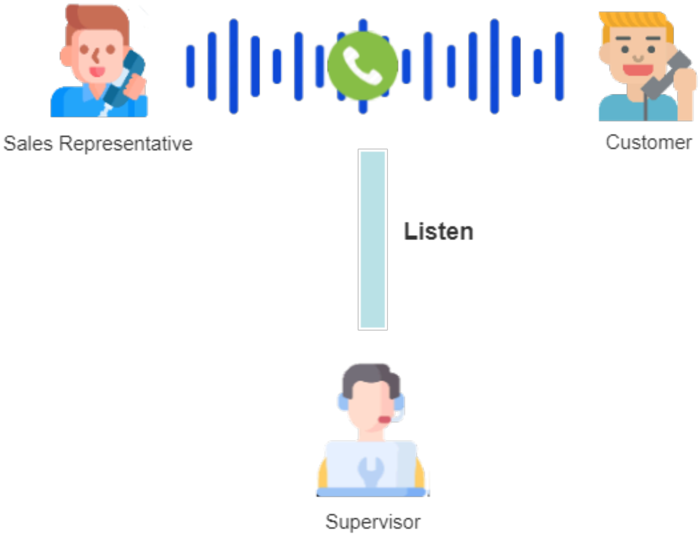
Modes of call monitoring

Yeastar P-Series Software Edition 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.

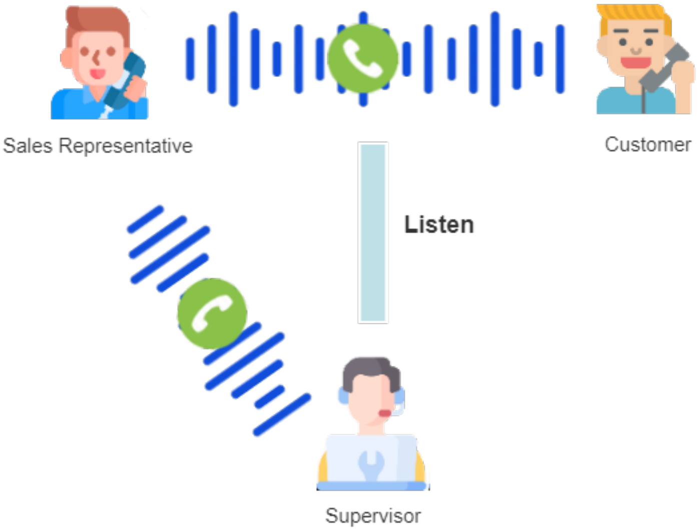
This mode is often used for supervisor to track the daily actions of sales representatives and evaluate their performance on the sales process.



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.

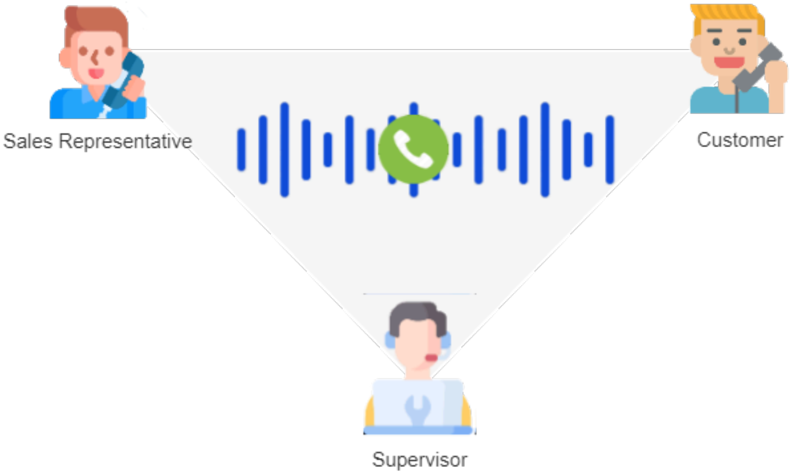
This mode is often used for supervisor to coach remote sales representatives and train them as they work on a sales call.



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 managers 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

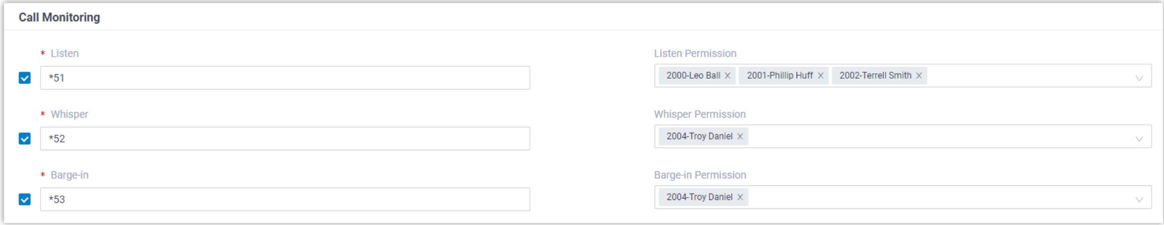
By default, all the extension users can NOT monitor others' calls by dialing a feature code, but their calls can be monitored instead.

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.



Call Monitoring

☑ * Listen: *51 — Listen Permission: 2000-Leo Ball, 2001-Phillip Huff, 2002-Terrell Smith

☑ * Whisper: *52 — Whisper Permission: 2004-Troy Daniel

☑ * Barge-in: *53 — Barge-in Permission: 2004-Troy Daniel

   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:

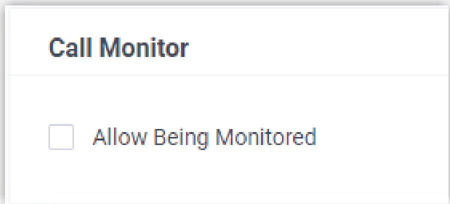
- Monitoring Conference Calls via feature code is NOT supported.
- Monitoring calls of extensions that are invisible on Linkus clients is NOT supported.
- During an internal call where one party allows being monitored while the other party disallows, the call can NOT be monitored even by the authorized 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

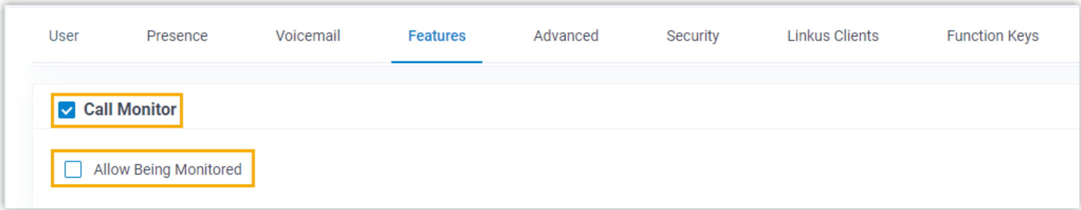
1. Log in to PBX web portal, go to Extension and Trunk > Extension.
2. To prevent an extension from being monitored, do as follows:
    a. Click ✎ beside the desired extension.
    b. Click Features tab.
    c. In the Call Monitor section, unselect the checkbox of Allow Being Monitored.



Call Monitor

☐ 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.



☑ Call Monitor

☐ Allow Being Monitored

    d. Click Save and Apply.

Result

The users' calls can NOT be monitored by anyone.

Fax

Fax Overview

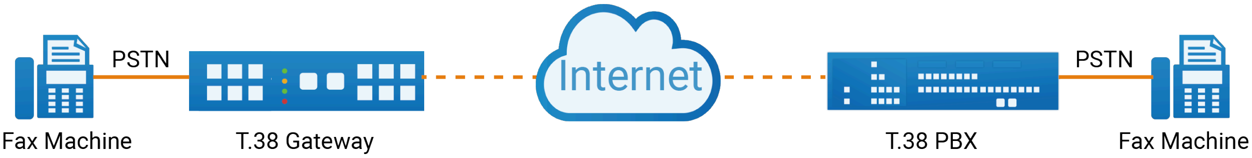
Yeastar P-Series Software Edition allows you to connect your fax machine to PBX system. Then you can send or receive faxes on a fax machine, and receive faxes by email. This topic describes how fax works with Yeastar P-Series Software Edition, and introduces fax to email, fax detection, and Fax over VoIP settings.

T.38 Fax

T.38 is a protocol that enables fax over the Internet and is supported on Yeastar P-Series Software Edition. 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 Software Edition 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.

Receive Faxes by Email

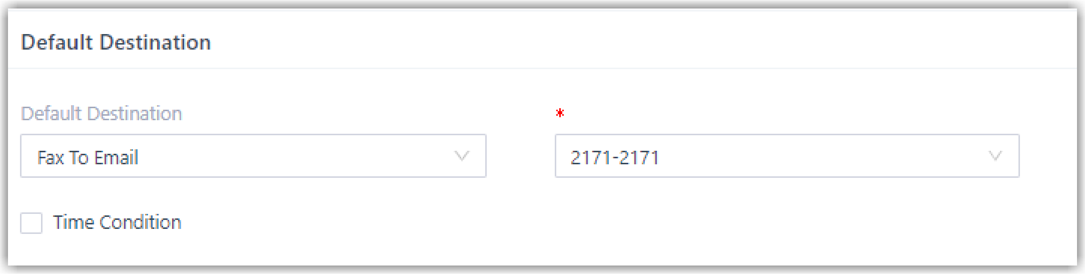
Yeastar P-Series Software Edition provides fax to email feature that allows you to receive faxes as PDF by email. This topic describes how to receive faxes by email.

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.



Default Destination

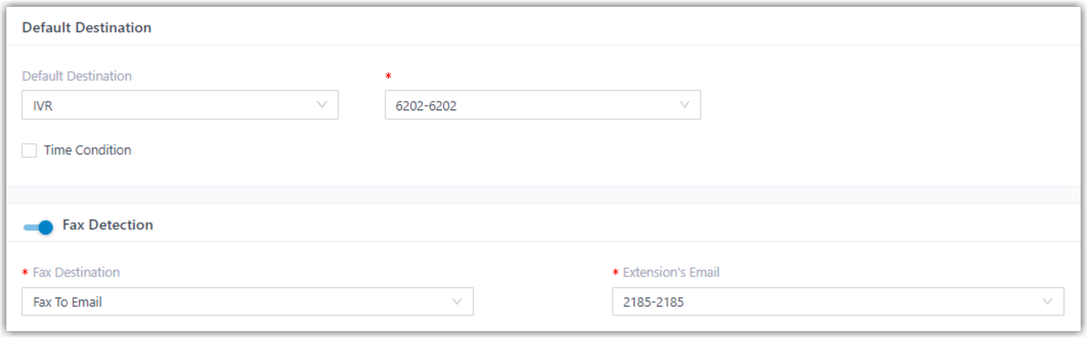
Default Destination: Fax To Email

*: 2171-2171

□ Time Condition

3. If you receive faxes through a shared line, go to Fax Detection section.
   a. In the Fax Destination drop-down list, select Fax To Email.

b. In the Extension's Email drop-down list, select an extension user to receive faxes by email.



Default Destination

Default Destination: IVR

* 6202-6202

□ Time Condition

Fax Detection

* Fax Destination: Fax To Email

* Extension's Email: 2185-2185

4. Click Save and Apply.

Result

When receiving a fax, PBX converts the received fax and simply forwards it to the email address as an PDF attachment.

Set up Fax over IP (FoIP)

Fax over IP (FoIP) is the process of using T.38 protocol to send a fax from a fax machine to another fax machine over the Internet. This topic describes how to enable T.38 for extension and trunk respectively, and how to change T.38 settings to improve the Fax transmission over VoIP network.

Enable T.38 protocol for SIP extension

If you want to register a SIP extension on a SIP compatible fax machine, you need to enable T.38 Support for this extension.

1. Log in to PBX 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 Software Edition 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

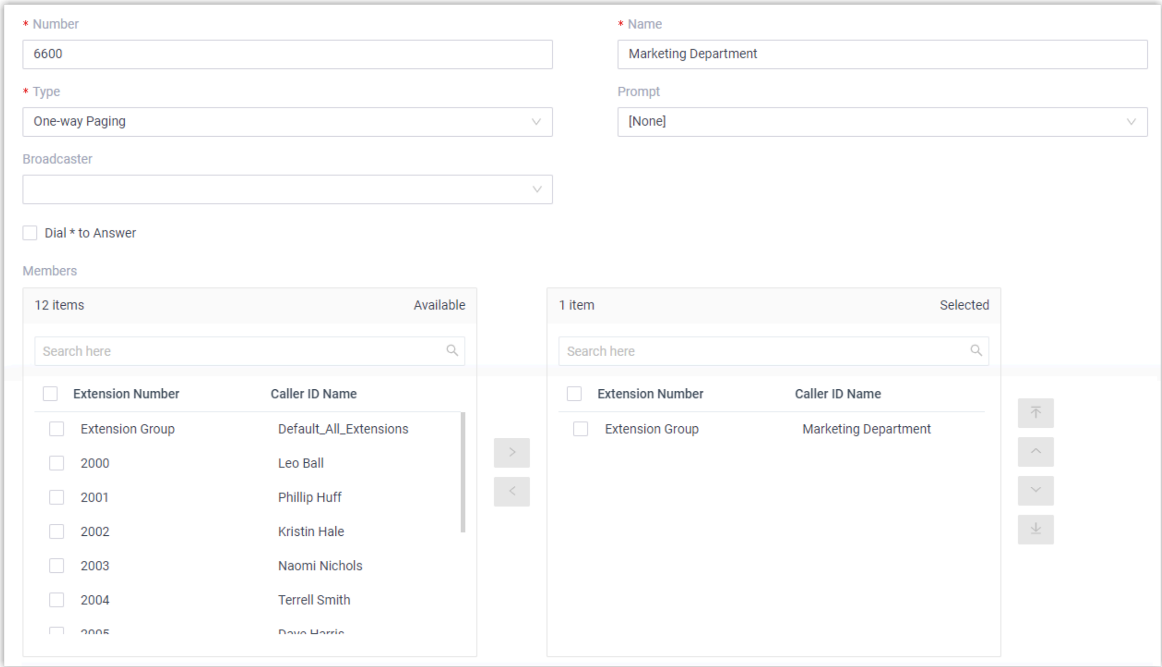
One-way Paging feature allows a broadcaster to make an announcement to users. The called parties' phones will not ring, but instead directly answering into speakerphone mode. This topic describes how to set up a one-way paging group.

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.



* Number: 6600

* Name: Marketing Department

* Type: One-way Paging

Prompt: [None]

Broadcaster:

□ Dial * to Answer

Members

12 items — Available

□	Extension Number	Caller ID Name
□	Extension Group	Default_All_Extensions
□	2000	Leo Ball
□	2001	Phillip Huff
□	2002	Kristin Hale
□	2003	Naomi Nichols
□	2004	Terrell Smith
□	2005	Dave Harris

1 item — Selected

□	Extension Number	Caller ID Name
□	Extension Group	Marketing Department

- Number: Enter a number for the paging group. In this example, enter 6600.
- Name: Enter a name for the paging group. In this example, enter Marketing Department.
- Type: Select One-way Paging.
- Prompt: Optional. To play a prompt before making an announcement, you can select a custom prompt. In this example, leave it as None.

> Note:
>
> To customize a prompt, see Record a Custom Prompt or Upload a Custom Prompt.

- Broadcaster: Optional. To restrict users from making an announcement to the paging group, select allowed extensions or extension groups from the drop-down list. In this example, leave it blank.
- Dial * to Answer: Optional. To allow users to dial `*` to talk to the broadcaster privately, enable this option. In this example, keep the option disabled.

> Note:
>
> When a user dials `*`, announcement will terminate, and the user can have a private talk with the broadcaster.

- Members: Select desired members from Available box to Selected box. In this example, select Marketing Department.

3. Click Save and Apply.

What to do next

The boss dials `6600` from any endpoint with extension registered. The marketers' phones automatically answer into speakerphone mode.

Note:

If called parties' extensions are registered on the following endpoints, these endpoints will ring first, instead of automatically answering into speakerphone mode.

- Softphone, including Linkus Web Client, Linkus Mobile Client, and softphones of other brands.

Related information

Schedule a Paging Call or an Intercom Call

Set up a One-way Multicast Paging Group

One-way Multicast Paging feature allows a broadcaster to make an announcement to the users who are listening to a specific multicast group on a specific channel. The called parties' phones will not ring, but instead directly answering into speakerphone mode. This topic describes how to set up a one-way multicast paging group.

Scenario

For a warehouse, the work flow in product line is closely connected and tends to be complex. For example, one zone is responsible for packaging goods, another zone is for dispatching goods. To facilitate supervisors in coordinating daily warehouse activities, you can set up paging groups for each zone.

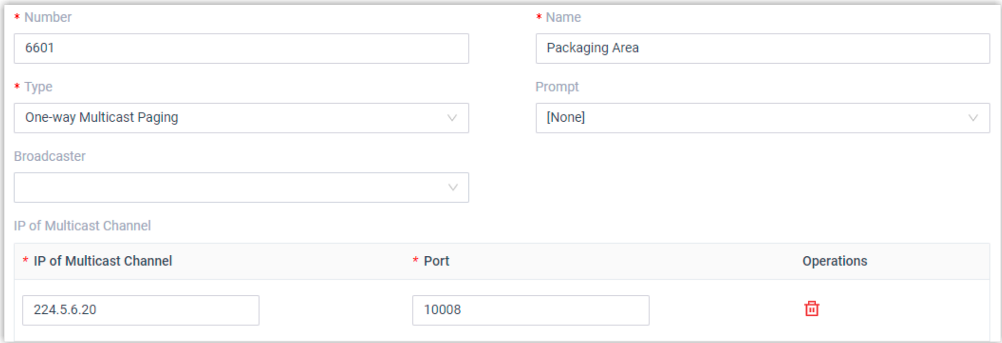
Requirements

The phone that will receive One-way Multicast Paging must 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 Software Edition, 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.



* Number: 6601

* Name: Packaging Area

* Type: One-way Multicast Paging

Prompt: [None]

Broadcaster:

IP of Multicast Channel

* IP of Multicast Channel	* Port	Operations
224.5.6.20	10008	🗑

- Number: Enter a number for the paging group. In this example, enter 6601.
- Name: Enter a name for the paging group. In this example, enter Packaging Area.
- Type: Select One-way Multicast Paging.
- Prompt: Optional. To play a prompt before making an announcement, you can select a custom prompt. In this example, leave it as None.

> Note:
>
> To customize a prompt, see Record a Custom Prompt and Upload a Custom Prompt.

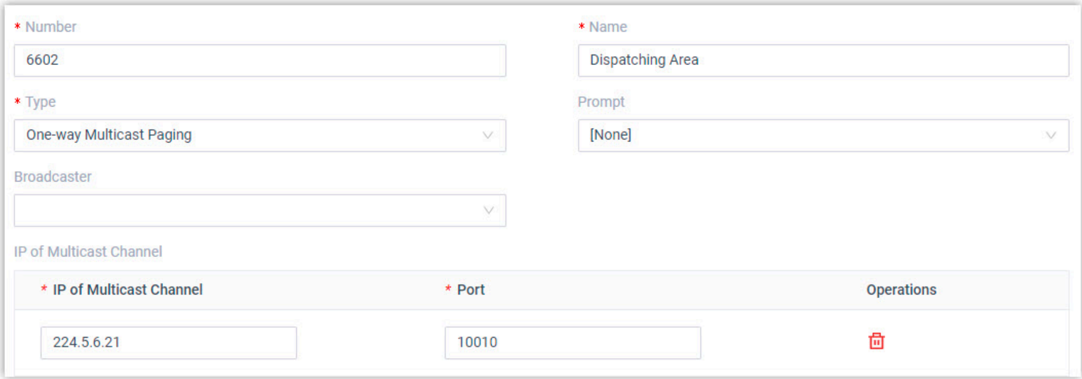
- Broadcaster: Optional. To restrict users from making an announcement to the paging group, select allowed extensions or extension groups from the drop-down list. In this example, leave it blank.
- IP of Multicast Channel: Enter a multicast IP address and port.
  - IP of Multicast Channel: Enter a multicast IP address. In this example, enter 224.5.6.20.
  - Port: Enter a multicast port. In this example, enter 10008.

> Note:
>
> - The range of multicast IP address is 224.0.0.0 - 239.255.255.255.
> - You can add at most 30 IP addresses.

iii. Click Save and Apply.

b. Repeat step a to create another paging group 6602 for Dispatching Area.

> Note:
>
> Set a multicast IP address and port that are different from Packaging Area. For example, set IP of Multicast Channel to 224.5.6.21 and set Port to 10010.



* Number: 6602

* Name: Dispatching Area

* Type: One-way Multicast Paging

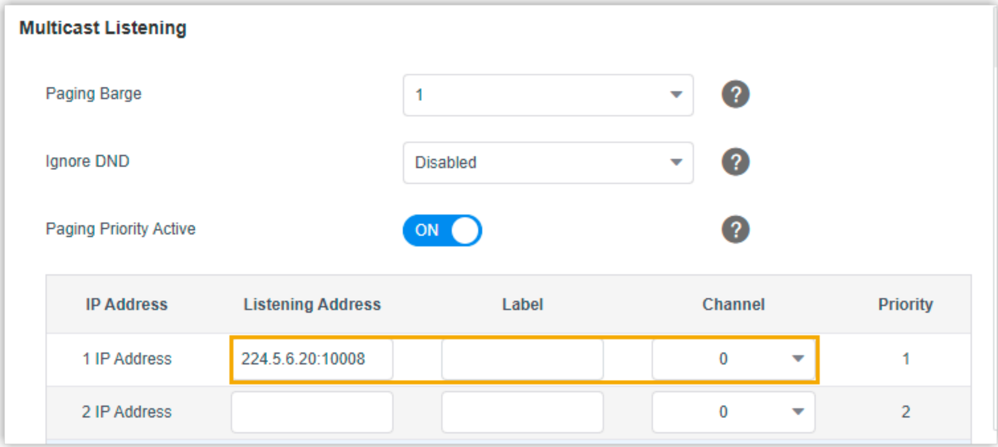
Prompt: [None]

Broadcaster:

IP of Multicast Channel

* IP of Multicast Channel	* Port	Operations
224.5.6.21	10010	🗑

2. Set up multicast listening for the two phones in Packaging Area and Dispatching Area.
    a. Set up multicast listening for the phone in Packaging Area. In this example, we take Yealink T56A as an example.
        i. Log in to the phone web interface, go to Directory > Multicast IP.
        ii. In the Listening Address field, enter the same multicast IP address and port as the PBX. In this example, enter 224.5.6.20:10008.



Multicast Listening

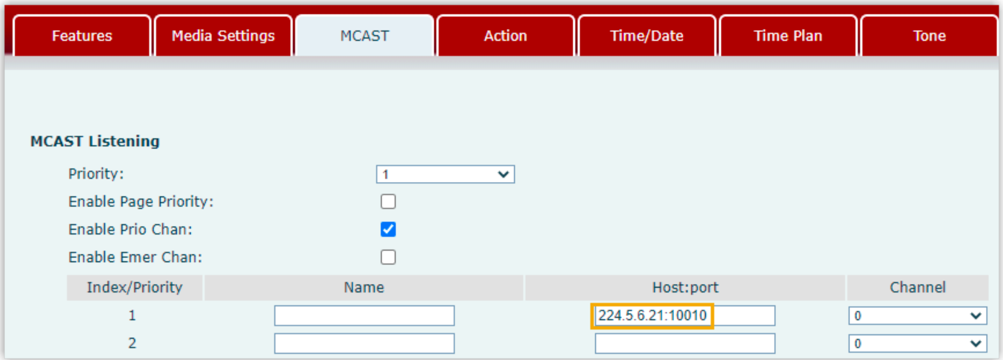
Paging Barge: 1

Ignore DND: Disabled

Paging Priority Active: ON

IP Address	Listening Address	Label	Channel	Priority
1 IP Address	224.5.6.20:10008		0	1
2 IP Address			0	2

        iii. Click Confirm.
    b. Set up multicast listening for the phone in Dispatching Area. In this example, we take Fanvil X210 as an example.
        i. Log in to the phone web interface, go to Phone Settings > MCAST.
        ii. In the Host:Port field, enter the same multicast IP address and port as the PBX. In this example, enter 224.5.6.21:10010.



MCAST Listening

Priority: 1

Enable Page Priority: ☐

Enable Prio Chan: ☑

Enable Emer Chan: ☐

Index/Priority	Name	Host:port	Channel
1		224.5.6.21:10010	0
2			0

iii. Click Apply.

What to do next

- Supervisor dials `6601` to reach employees in Packaging Area. Yealink T56A automatically answers into speakerphone mode.
- Supervisor dials `6602` to reach employees in Dispatching Area. Fanvil X210 automatically answers into speakerphone mode.

Related information

Schedule a Paging Call or an Intercom Call

Set up a Two-way Intercom Group

Two-way Intercom feature allows you to establish two-way communication with an individual user or a group of users. The called parties can respond without picking up the handset. This topic describes how to set up a two-way intercom group.

Background information

In office complexes, hospitals, or schools, there are either static guards or patrol guards to ensure safety within the workplace. The Two-way Intercom feature helps improve communication efficiency. For example, a security guard can ask for help when security incidents happen, a supervisor can flexibly dispatch employees in daily activities.

Yeastar P-Series Software Edition 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.

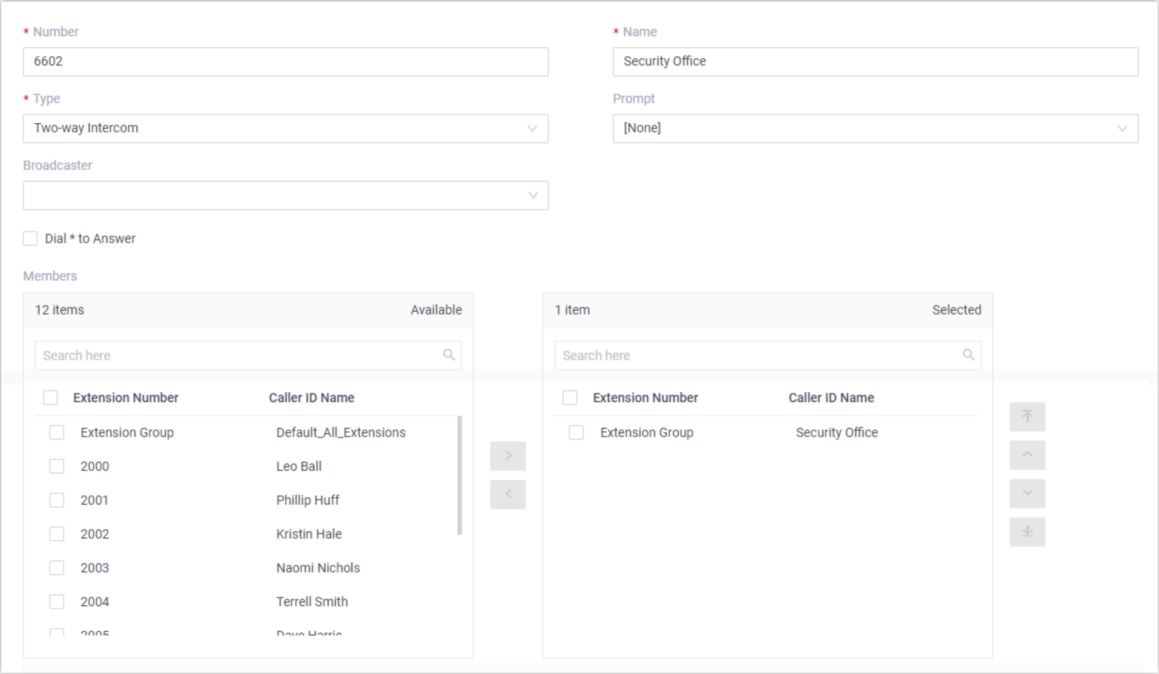
Place an intercom call to multiple users

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.



* Number: 6602

* Name: Security Office

* Type: Two-way Intercom

Prompt: [None]

Broadcaster:

□ Dial * to Answer

Members

12 items — Available

Search here

□	Extension Number	Caller ID Name
□	Extension Group	Default_All_Extensions
□	2000	Leo Ball
□	2001	Phillip Huff
□	2002	Kristin Hale
□	2003	Naomi Nichols
□	2004	Terrell Smith
□	2005	Dave Harris

1 item — Selected

Search here

□	Extension Number	Caller ID Name
□	Extension Group	Security Office

- Number: Enter a number for the intercom group. In this example, enter 6602.
- Name: Enter a name for the intercom group. In this example, enter Security Office.
- Type: Select Two-way Intercom.
- Prompt: Optional. To play a prompt before making an announcement, you can select a custom prompt. In this example, leave it as None.

  Note:
  To customize a prompt, see Record a Custom Prompt or Upload a Custom Prompt.
- Broadcaster: Optional. To restrict users from placing an intercom call to the intercom group, select allowed extensions or extension groups from the drop-down list. In this example, leave it blank.

- Dial * to Answer: Optional. To allow users to dial `*` to talk to the broadcaster privately, enable this option.

  > Note:
  >
  > When a user dials `*`, the call is ended from other users' side, and the user can have a private talk with the broadcaster.

- Members: Select desired members from Available box to Selected box. In this example, select the group Security Office.

3. Click Save and Apply.

What to do next

Dial `6602` to reach all the security guards. The security guards' phones automatically answer into speakerphone mode.

Related information

Schedule a Paging Call or an Intercom Call

Manage Paging Groups and Intercom Groups

This topic describes how to edit or delete paging groups and intercom groups.

Edit a paging/intercom group

1. Log in to PBX 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 Software Edition 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:
        - Paging: Select a pre-configured paging group from the drop-down list.
        - Caller: Select a broadcaster.
            - {extension_user}: The extension user will make the announcement.
              On the specified date and time, the PBX will place a call to the user. When the user answers the call, group members' phones directly answer into speakerphone mode.

              > Note:
              > If the user rejects the call, the announcement will be cancelled.
            - None: The PBX will make the announcement.
              On the specified date and time, the PBX will place a call to group members and play a specific custom prompt. After the prompt ends, the PBX hangs up. The option can be applied to school bells, church bells, etc.

              > Note:
              > The option is available only when a custom prompt is assigned to the selected paging group or intercom group.
        - Start Date: Set the start date of the scheduled paging call or intercom call.
        - Time: Set the start time of the scheduled paging call or intercom call.

> Note:
> You can set up to 8 timings, which means that the paging call or intercom call can be placed at different time on the same day.

- Days of Week: Select the days of week.

  The scheduled paging call or intercom call will be weekly placed on the specified days of week.

c. Click Save and Apply.

Manage Scheduled Paging Calls and Intercom Calls

This topic describes how to edit or delete scheduled paging calls and intercom calls.

Edit a scheduled paging/intercom call

1. Log in to PBX 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. For more information, see Restrict Outbound Calls by PIN Codes.

Blocked/Allowed Numbers

Block Calls To or From a Phone Number

Yeastar P-Series Software Edition 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 the number of your extensions.

Table 41.

Maximum Number of Extensions (N)	Blocked Numbers Lists	Numbers per Blocked Numbers List
N $<$ 1000	256	100
N ≥1000	512	200

Background information

Yeastar P-Series Software Edition 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

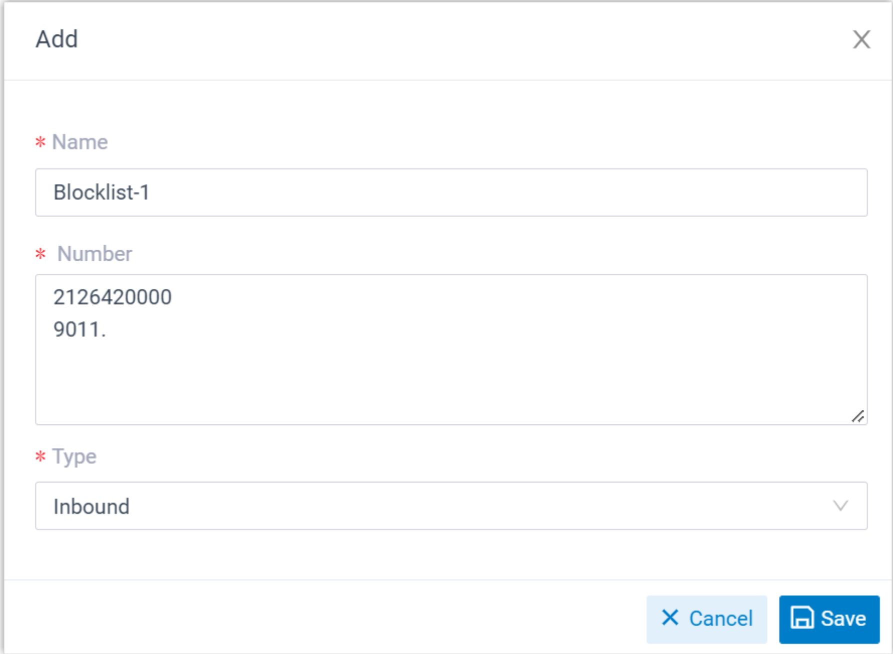
This feature makes it possible for blocking inbound and/or outbound calls to external users by phone number. If you list a phone number in the system blocklist, all the PBX extensions can NOT reach or be reached by the phone number.

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:



Add

* Name

Blocklist-1

* Number

2126420000
9011.

* Type

Inbound

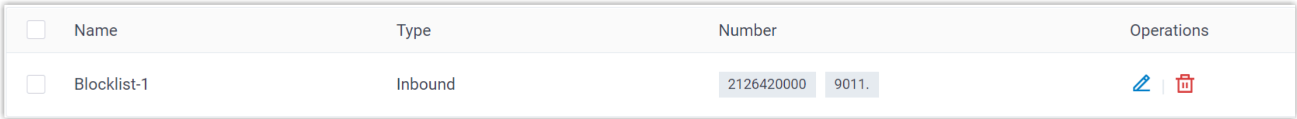
- Name: Enter a name to help you identify the number(s) to be blocked.
- Number: Enter a specific number or a number pattern per line.
    - To block a specific number, enter a specific number. For example, enter `2126420000`.
    - To block a range of numbers, enter a wildcard pattern. For example. 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.



□	Name	Type	Number	Operations
□	Blocklist-1	Inbound	2126420000 9011.	✎ | 🗑

Export and Import Blocked Numbers

The blocked numbers added on Yeastar P-Series Software Edition 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:
   1. Select the checkbox of a desired list, then click 🗑.
   2. In the pop-up window, click OK.
3. To bulk delete blocked numbers lists, do as follows:
   1. Select the checkboxes of desired lists, then click Delete.
   2. 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 the number of your extensions.

Table 42.

Maximum Number of Extensions (N)	Allowed Numbers Lists	Numbers per Allowed Numbers List
N $<$ 1000	256	100
N ≥1000	512	200

Background information

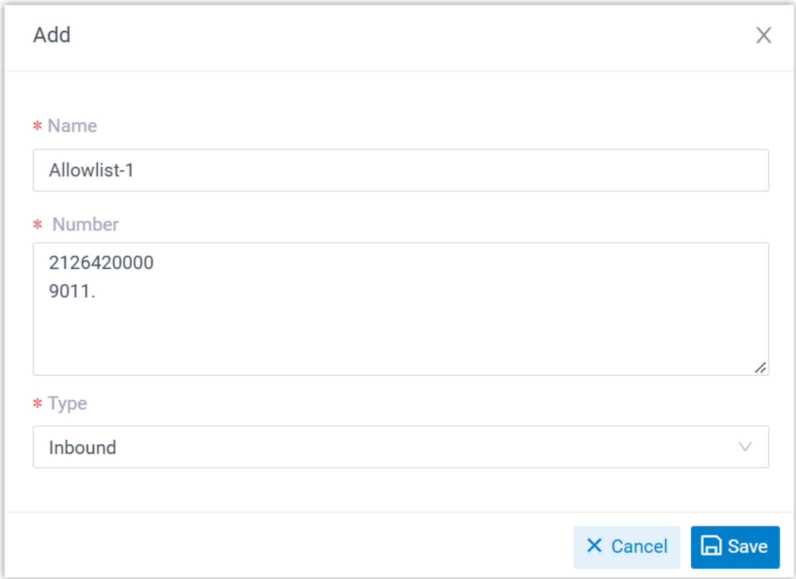
If your customers' phone numbers happen to be listed in system blocklist or individual blocklist, you can add trusted phone numbers to the allowlist.

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:



Add

* Name

Allowlist-1

* Number

2126420000
9011.

* Type

Inbound

- 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.

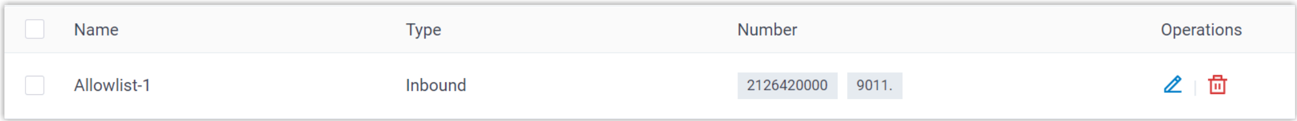
For more information about wildcard pattern, see DID Pattern and Caller ID Pattern.

- 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.



□	Name	Type	Number	Operations
□	Allowlist-1	Inbound	2126420000 9011.	✎ 🗑

Export and Import Allowed Numbers

The allowed numbers added on Yeastar P-Series Software Edition 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.

PBX System

System Preferences

This topic describes the preference settings that will be applied globally to Yeastar P-Series Software Edition.

Go to PBX Settings > Preferences to configure preferences settings.

Basic preferences

Table 43.

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.

Organization Management

Table 44.

Setting	Description
Organization Management	If enabled, you can arrange extension users into organizations.

Table 44. (continued)

Setting	Description
Company Name	Set your company name, which will be used as the root organization name.

Distinctive Caller ID Name

Table 45.

Setting	Description
Display Call Feature Name	If enabled, the Caller ID will display the originated name when users receive a call from a ring group, queue, and IVR.
Display DID/DDI Name	If enabled, the Caller ID will display the DID name of the source trunk.

DTMF preferences

Table 46.

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

Default extension ranges vary according to the total of PBX extensions. 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.

The total of PBX extensions ≤6000

Table 47.

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

The total of PBX extensions $>$ 6000

Table 48.

Extension Type	Default Range
User Extension	1000 - 9999
Parking Extension	50010-50099
Group Voicemail Extension	50100-50199
IVR Extension	50200-50299
Ring Group Extension	50300-50399
Queue Extension	50400-50499
Conference Extension	50500-50599
Paging Extension	50600-50699
Account Trunk	50700-50799

Voice Prompt

Voice Prompt Overview

This topic describes the definition, types, and preference settings of voice prompt on Yeastar P-Series Software Edition.

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 Software Edition 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.

Table 49.

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.

Table 49. (continued)

Setting	Description
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. 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.

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 Software Edition 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 Software Edition 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 Software Edition 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 Software Edition 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

Item	Requirements
	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	32
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 MoH.
   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

Up to 128 custom prompts are supported on the PBX.

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

    > ℹ Tip:
    >
    > If the audio file does not meet the requirements, you can convert the audio file via WavePad or G711 File Converter online.
- File size: Up to 8MB.

Limitation

Up to 128 custom prompts are supported on the PBX.

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.

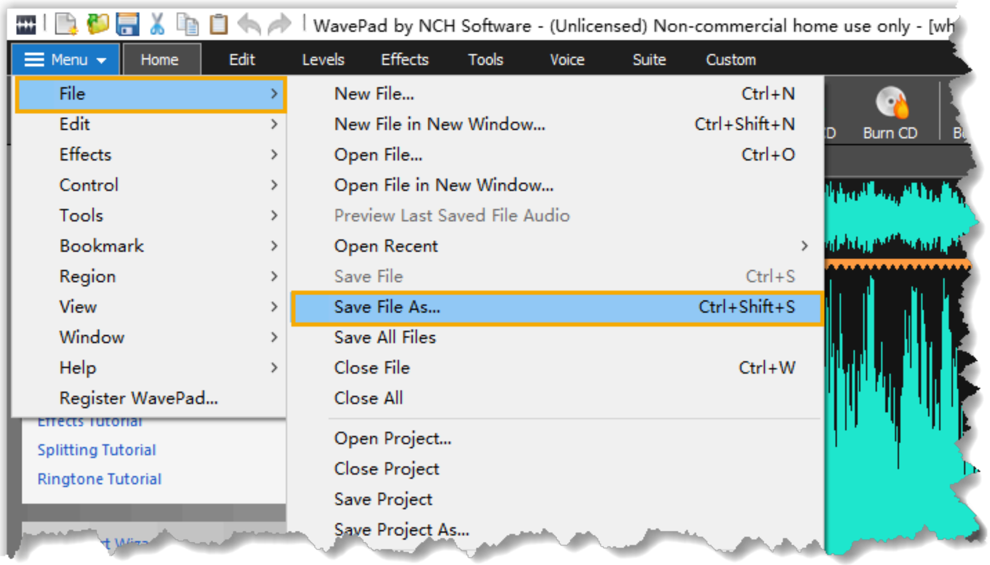
In this topic, we take the followings as examples to show you how to convert file format.

- Convert Audio Files via WavePad
- Convert Audio Files Online

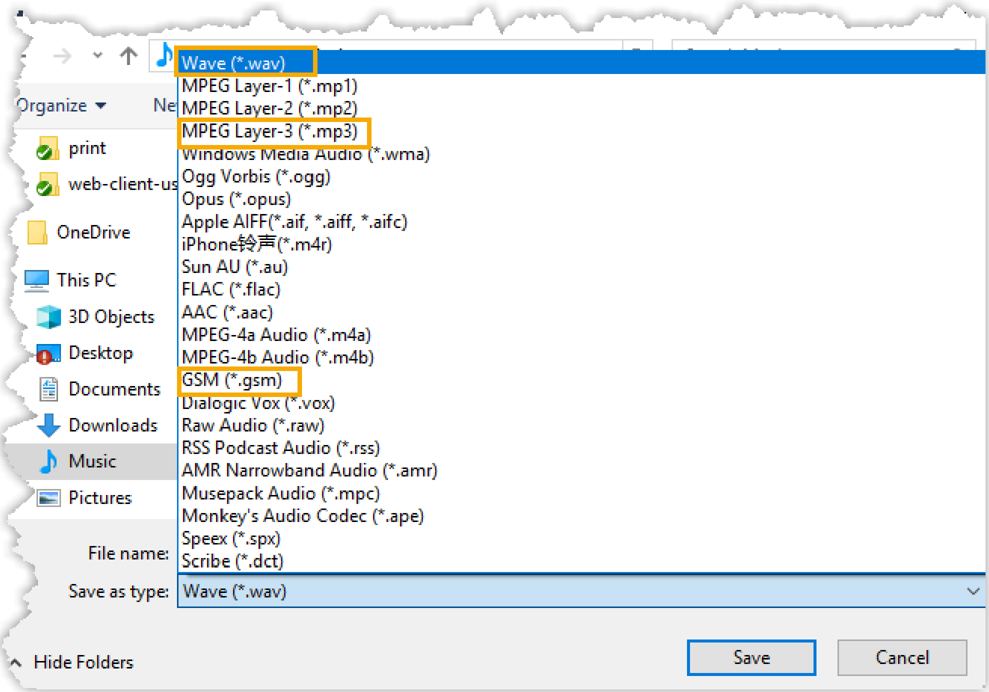
Convert audio files via WavePad

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.



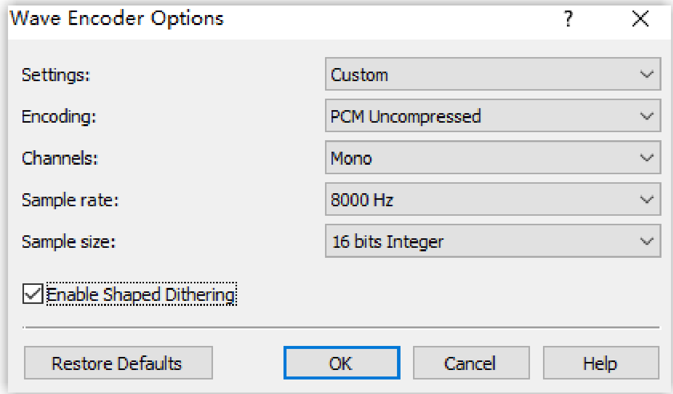
4. If you save the audio file as `Wave(*.wav)` or `MPEG Layer-3(*.mp3)`, you need to configure the encoder options and click OK.

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



Wave Encoder Options

Settings: Custom

Encoding: PCM Uncompressed

Channels: Mono

Sample rate: 8000 Hz

Sample size: 16 bits Integer

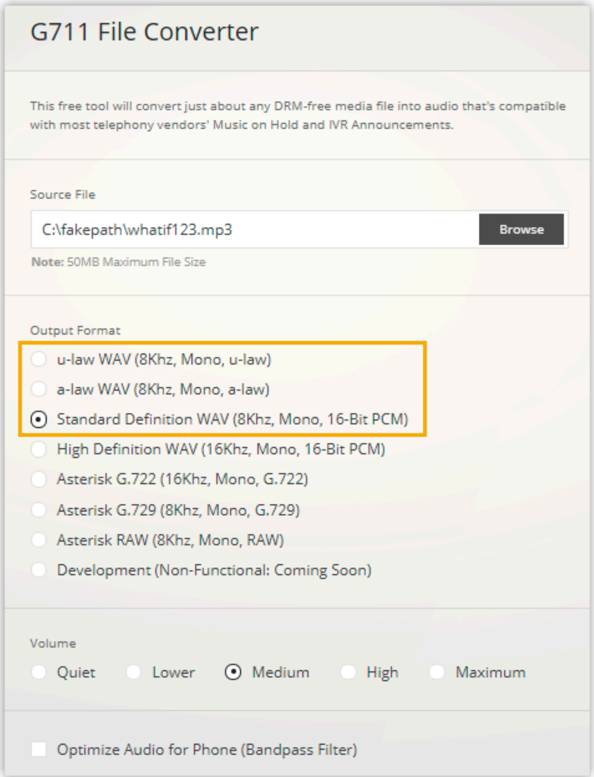
☑ Enable Shaped Dithering

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).



G711 File Converter

This free tool will convert just about any DRM-free media file into audio that's compatible with most telephony vendors' Music on Hold and IVR Announcements.

Source File

C:\fakepath\whatif123.mp3

Note: 50MB Maximum File Size

Output Format

○ u-law WAV (8Khz, Mono, u-law)
○ a-law WAV (8Khz, Mono, a-law)
● Standard Definition WAV (8Khz, Mono, 16-Bit PCM)
○ High Definition WAV (16Khz, Mono, 16-Bit PCM)
○ Asterisk G.722 (16Khz, Mono, G.722)
○ Asterisk G.729 (8Khz, Mono, G.729)
○ Asterisk RAW (8Khz, Mono, RAW)
○ Development (Non-Functional: Coming Soon)

Volume

○ Quiet ○ Lower ● Medium ○ High ○ Maximum

□ Optimize Audio for Phone (Bandpass Filter)

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 Software Edition.

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.
File Size	Up to 8 MB.

Option	Requirement
File Format	`.wav`, `.mp3`, or `.gsm`. • PCM, 8K, 16bit, 128kbps • A-law (g.711), 8k, 8bit, 64kbps • u-law (g.711), 8k, 8bit, 64kbps

SIP Settings

This topic describes the SIP settings on the Yeastar P-Series Software Edition 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 50.

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 50. (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 51.

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.

TLS settings

Setting	Description
TLS	Enable or disable TLS.
SIP TLS Port	TLS port used for SIP registration. The default value is 5061.
When PBX acting as a Sever	
TLS Certificate	Upload a server certificate when PBX acts as a server.
TLS Verify Client	Verify client certificate when PBX acts as a server. 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.

Setting	Description
	- 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)	

Setting	Description
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 • P-Preferred-Identity
Get DID From	Decide the system will retrieve DID from which header field. • To • Invite • Diversion • Remote-Party-ID

Setting	Description
	• 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.
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.

Setting	Description
	Note: Your IP phone should support uaCSTA standard to use this function.

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 Software Edition.

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 Software Edition 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 Software Edition.

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.
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 Software Edition.

Ethernet modes

Yeastar P-Series Software Edition 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:

> Note:
>
> For the PBX that is installed on a cloud server (e.g. Amazon AWS), only Single mode is supported.

- Single: Only LAN port is used for connection, WAN port is disabled.
- Dual: Both LAN port and WAN port are used for connection.
  If you use Dual mode, you need to specify a default network interface for the PBX.

  > Note:
  >
  > The traffic will be routed to the default interface, you need to add a static route to override the default route entries, routing the traffic from a specific IP address to the specified destination.

IP address assignment

Yeastar P-Series Software Edition supports three types of IP address assignment:

> Note:
>
> For the PBX that is installed on a cloud server (e.g. Amazon AWS), IP address can only be obtained from a DHCP server.

- Assign a static IP address

  Contact your network administrator to assign an IP address to the PBX. Then you need to manually configure settings such as the IP address, subnet mask, default gateway, and DNS servers on the PBX.
- Obtain an IP address from a DHCP server

  You can configure the PBX to automatically obtain an IP address when it starts up from a DHCP server running in your network.

  > Note:
  >
  > The IP address assigned to the PBX may vary every time the PBX is started up.
- Obtain an IP address from a PPPoE client

  You can connect the PBX to a PPPoE client, and set up a PPPoE connection on the PBX to get an IP address.

  > Note:
  >
  > The IP address assigned to the PBX may vary every time the PPPoE is started up.

Configure a Static IP Address

This topic describes how to configure a static IP address for Yeastar P-Series Software Edition.

Background information

The default IP address of Yeastar P-Series Software Edition is 192.168.5.150. According to your network environment, you may need to change the IP address to the same network segment of your local network.

The following instructions assume that you need to use LAN port of Yeastar P-Series Software Edition to send and receive network traffic. The IP information is as below:

- IP address: 192.168.6.124
- Subnet mask: 255.255.255.0
- Gateway address: 192.168.6.1
- DNS server: 192.168.1.1

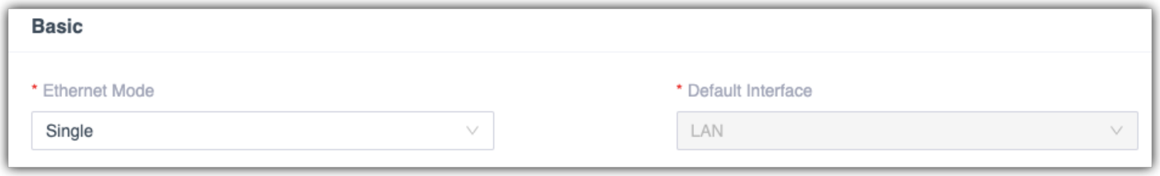
Prerequisites

- PBX and PC are connected to the same local network.
- Your PC has ability to access the default network segment 192.168.5.X of the PBX.

> 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:



Basic

* Ethernet Mode: Single

* Default Interface: LAN

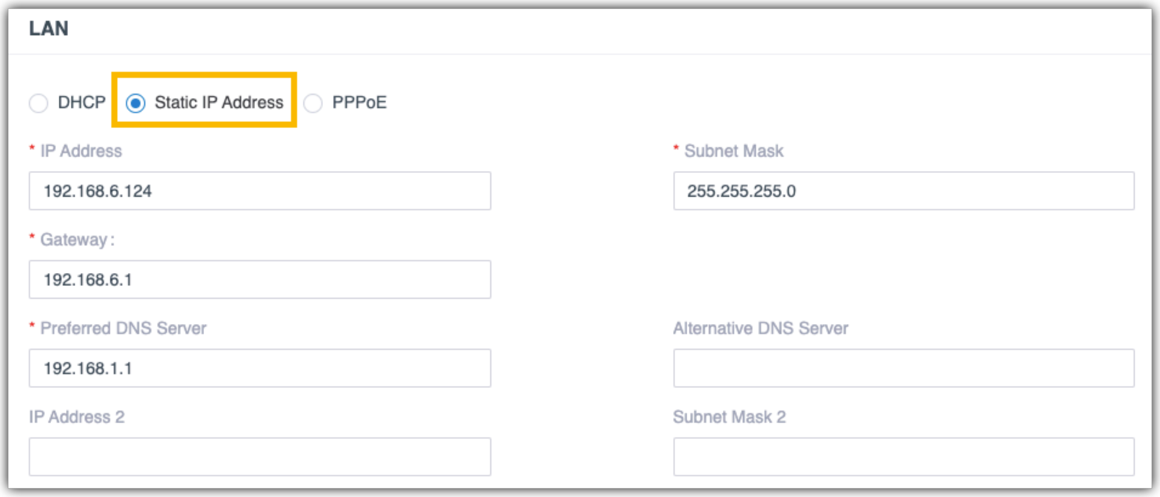
- Ethernet Mode: Select the Ethernet mode. In this scenario, select Single.
    - Single: Only the LAN port is used for up-link connection.
    - Dual: Both LAN and WAN are used for up-link connection.

> Note:

> The traffic will be routed to the default interface; you may need to add a static route to override the default route entries, routing the traffic from a specific IP address to the specified destination.

- Default Interface: Optional. Select a default interface if you select Dual mode.

3. In the LAN section, select Static IP Address, and enter the network information for LAN port.



LAN

○ DHCP ● Static IP Address ○ PPPoE

* IP Address: 192.168.6.124

* Subnet Mask: 255.255.255.0

* Gateway: 192.168.6.1

* Preferred DNS Server: 192.168.1.1

Alternative DNS Server:

IP Address 2:

Subnet Mask 2:

- IP Address: Enter the IP address that is assigned to the PBX.
- Subnet Mask: Enter the subnet mask.
- Gateway: Enter the gateway address.
- Preferred DNS Server: Enter the IP address of preferred DNS server.
- Alternative DNS Server: Optional. Enter the IP address of alternative DNS server.
- IP Address 2: Optional. Enter a second IP address for the PBX.

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

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

4. Click Save and reboot the PBX to take effect.

Result

After the PBX reboots, the PBX's IP is changed to 192.168.6.124.

What to do next

To access the PBX, change your PC's IP to the same network segment of the PBX, for example, 192.168.6.110.

Obtain an IP Address from a DHCP Server

This topic describes how to configure Yeastar P-Series Software Edition to automatically obtain an IP address from a DHCP server running in your network.

Background information

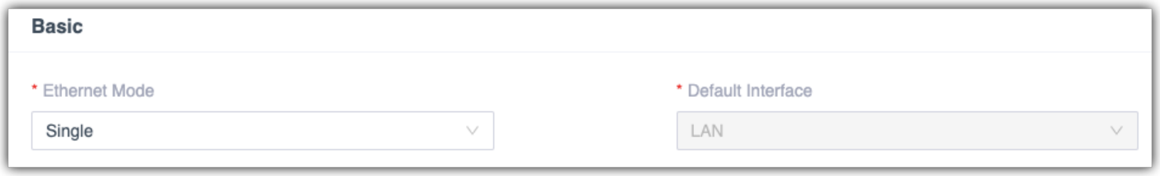
If you choose this method to configure IP address for the PBX, the IP address assigned to the PBX may vary every time the PBX starts up. We suggest that you configure a static IP address for the PBX. For more information, see Configure a Static IP Address.

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:



Basic

* Ethernet Mode: Single

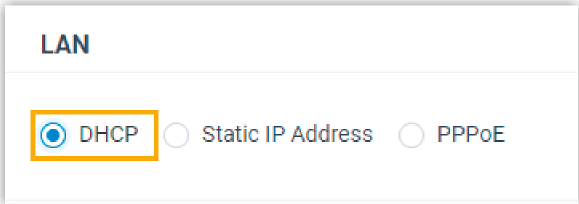
* Default Interface: LAN

- Ethernet Mode: Select the Ethernet mode. In this scenario, select Single.
  - Single: Only the LAN port will be used for up-link connection.
  - Dual: Both LAN and WAN can be used for up-link connection.

> Note:
> The traffic will be routed to the default interface; you may need to add a static route to override the default route entries, routing the traffic from a specific IP address to the specified destination.

- Default Interface: Select a default interface if you select Dual mode.

3. In the LAN section, select DHCP.



LAN

● DHCP ○ Static IP Address ○ PPPoE

4. Click Save and reboot the PBX to take effect.

Result

The PBX's IP address will obtain a new IP address from the DHCP server in your local network.

You need to log in to the web interface of your router, and check which IP address is assigned to the PBX.

Configure a PPPoE Connection

This topic describes how to configure a PPPoE connection on Yeastar P-Series Software Edition to obtain an IP address when the PBX is in Dual network mode.

Background information

A PPPoE client assigns a dynamic IP address to the PBX, the IP address of the PBX may vary every time the PBX starts up. In this case, you need to configure dual network, and configure a static IP address on the PBX to ensure that you can always access the PBX.

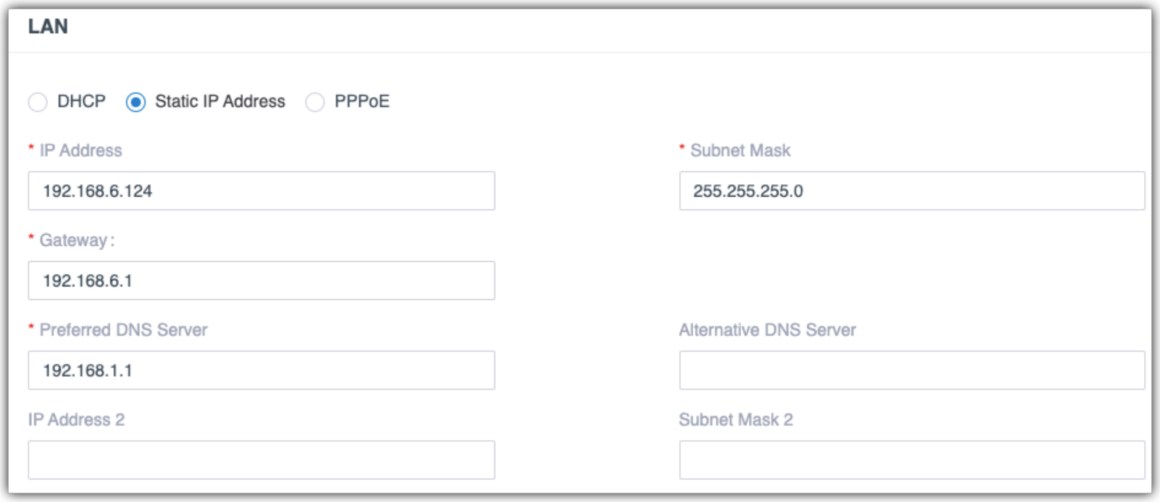
The following instructions assume that you need to connect LAN port to local network, connect WAN port to PPPoE. The network information is as the following:

LAN	WAN
Static IP • 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.
    - Default Interface: Select the port where PPPoE is connected. In the scenario, select WAN.
3. In the LAN section, select Static IP Address, and enter the network information for LAN port.



LAN

○ DHCP ● Static IP Address ○ PPPoE

* IP Address: 192.168.6.124

* Subnet Mask: 255.255.255.0

* Gateway: 192.168.6.1

* Preferred DNS Server: 192.168.1.1

Alternative DNS Server:

IP Address 2:

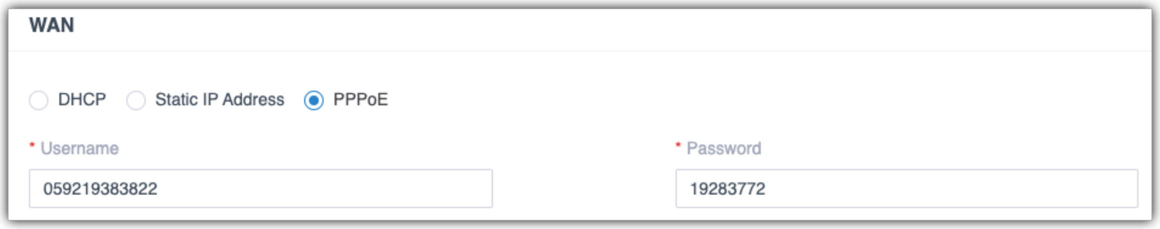
Subnet Mask 2:

- IP Address: Enter the IP address that is assigned to the PBX.
- Subnet Mask: Enter the subnet mask.
- Gateway: Enter the gateway address.
- Preferred DNS Server: Enter the IP address of preferred DNS server.
- Alternative DNS Server: Optional. Enter the IP address of alternative DNS server.
- IP Address 2: Optional. Enter a second IP address for the PBX.

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

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

4. In the WAN section, select PPPoE and enter the Username and Password.



WAN

○ DHCP ○ Static IP Address ● PPPoE

* Username: 059219383822

* Password: 19283772

5. Click Save and reboot the PBX to take effect.

Result

Both LAN and WAN are set up for the PBX.

- All network traffic will be sent and received by the WAN port (default network interface).
- You can access the PBX 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.

Web Server

Change Web Server Protocol and Port

This topic describes how to change the web protocol and port of Yeastar P-Series Software Edition.

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 a HTTPS port.
        - HTTPS Certificate: Select the default certificate or upload your own certificate.
        - Redirect from HTTP 80 port: Decide whether to allow requests to HTTP port 80.

          If the option is enabled, the requests to HTTP port 80 will be redirected to the respective HTTPS service.

    c. If HTTP is selected, enter the HTTP port in the HTTP Port field.
3. Click Save and Apply.

Result

The next time, you need to access the PBX web portal by the configured protocol and port.

Change Automatic Logout Time

For security purposes, Yeastar P-Series Software Edition 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 Software Edition 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

Service	Description	Default Port
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 52.

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 restrict-

Table 52. (continued)

Feature	Description	Default Status	Usage Permission Setting
			ed 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.

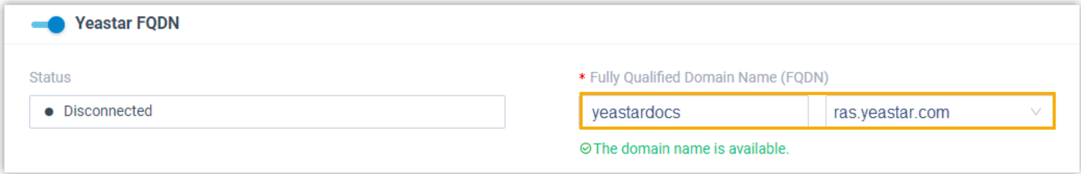
Procedure

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.



Yeastar FQDN

Status: ● Disconnected

* Fully Qualified Domain Name (FQDN): yeastardocs | ras.yeastar.com

The domain name is available.

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.

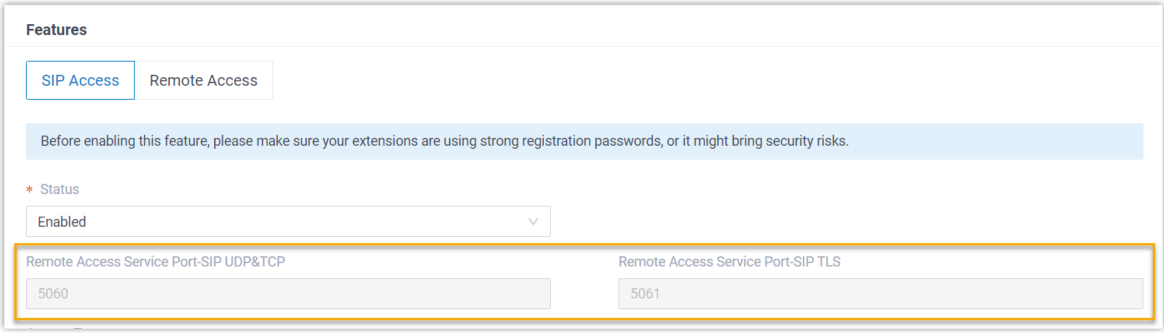
a. In the Features section, go to the SIP Access tab.
b. In the Status drop-down list, select Enabled.
c. In the Access Type drop-down list, select the account access restriction type.
   - Allowed Account: Only the selected accounts can get access to the service.
   - Restricted Account: All accounts 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.



Features

SIP Access | Remote Access

Before enabling this feature, please make sure your extensions are using strong registration passwords, or it might bring security risks.

* Status: Enabled

Remote Access Service Port-SIP UDP&TCP: 5060

Remote Access Service Port-SIP TLS: 5061

- 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.

Related information

Auto Provision IP Phones Remotely (RPS FQDN Method)

Configure Network for Remote Web Access by a Yeastar FQDN

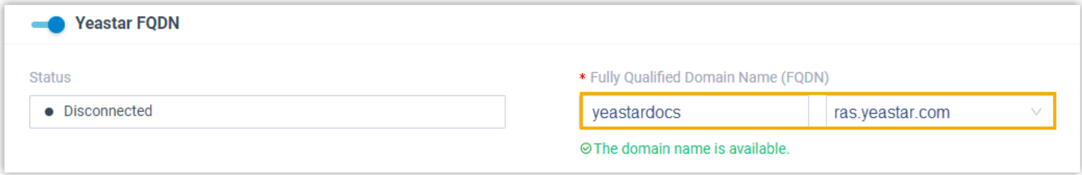
Yeastar FQDN provides secure remote access to PBX web portal or Linkus Web Client, without the need of configuring public IP and port forwarding. This topic describes how to configure network for remote web access via FQDN.

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.



Status

● Disconnected

* Fully Qualified Domain Name (FQDN)

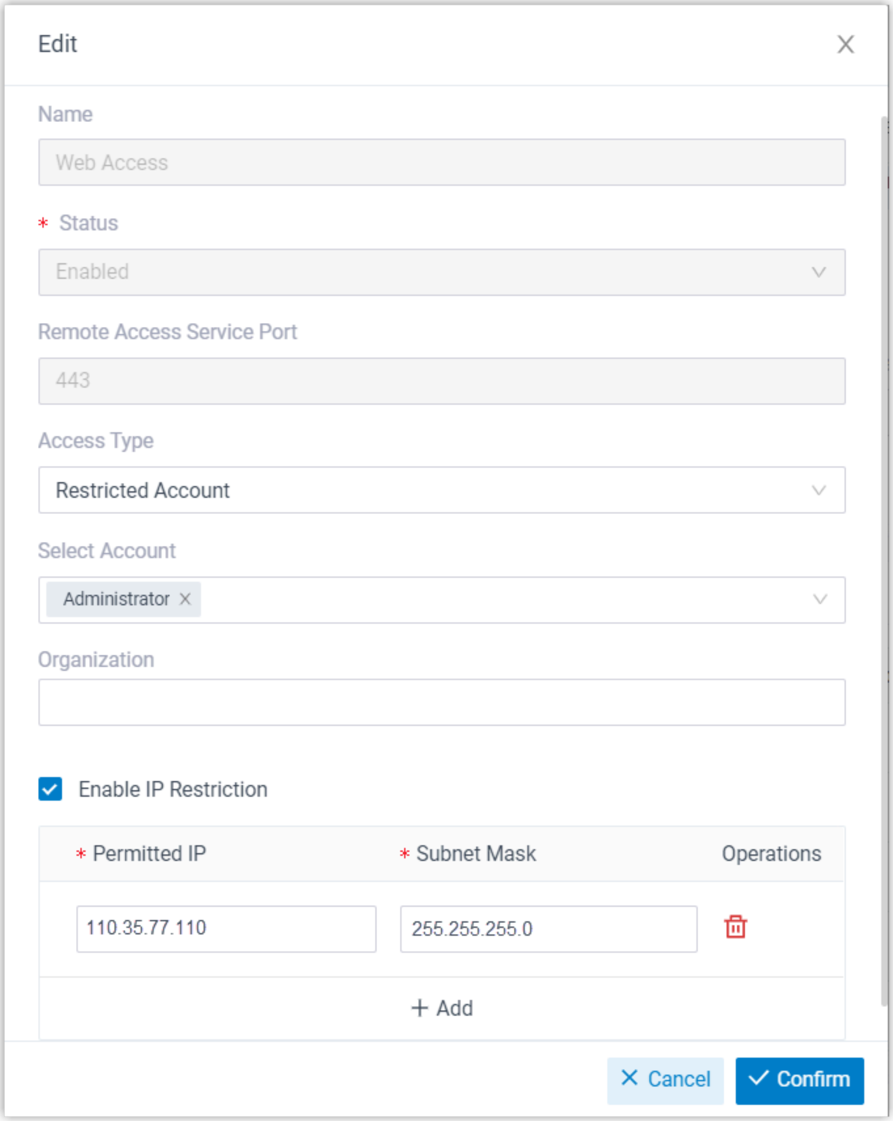
yeastardocs | ras.yeastar.com

The domain name is available.

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.



Edit

Name

Web Access

* Status

Enabled

Remote Access Service Port

443

Access Type

Restricted Account

Select Account

Administrator

Organization

☑ Enable IP Restriction

* Permitted IP	* Subnet Mask	Operations
110.35.77.110	255.255.255.0	🗑

- 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.

Configure Network for Remote Linkus Access by a Yeastar FQDN

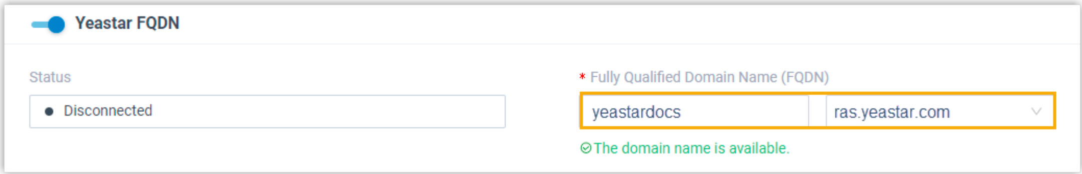
With a Yeastar FQDN, users can log in to the Linkus UC Clients anywhere anytime. This topic describes how to configure network for remote Linkus access via FQDN.

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.


Yeastar FQDN

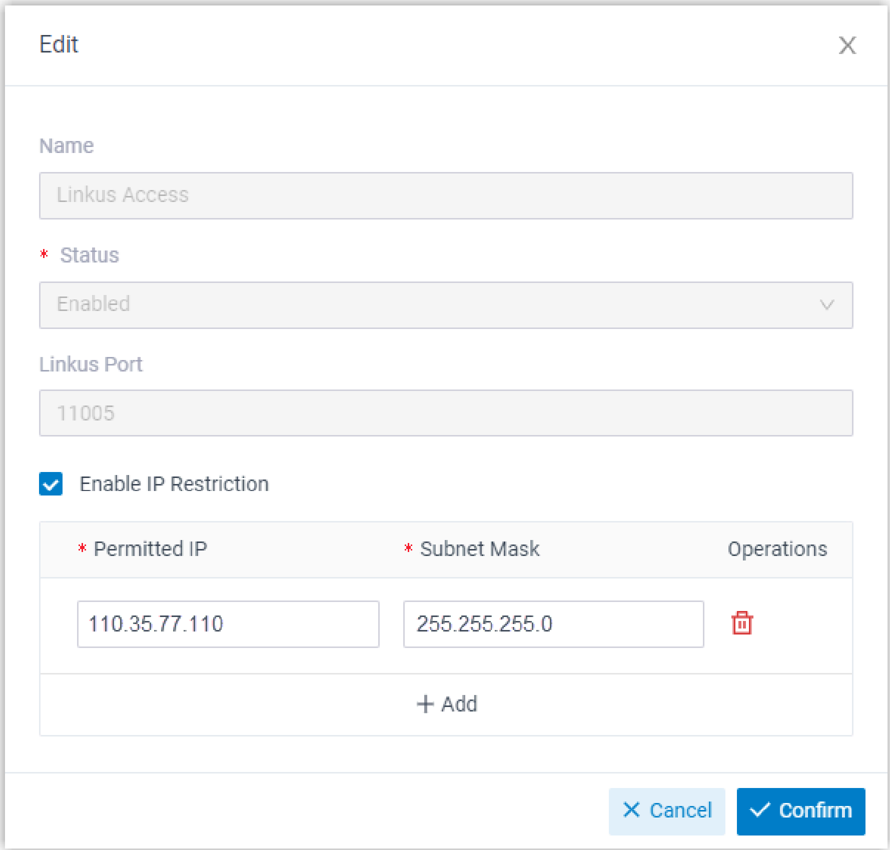
Status: ● Disconnected

* Fully Qualified Domain Name (FQDN): yeastardocs | ras.yeastar.com

The domain name is available.

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.



Edit

Name: Linkus Access

* Status: Enabled

Linkus Port: 11005

☑ Enable IP Restriction

* Permitted IP	* Subnet Mask	Operations
110.35.77.110	255.255.255.0	🗑

- 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.

Configure Network for Remote LDAP Access by a Yeastar FQDN

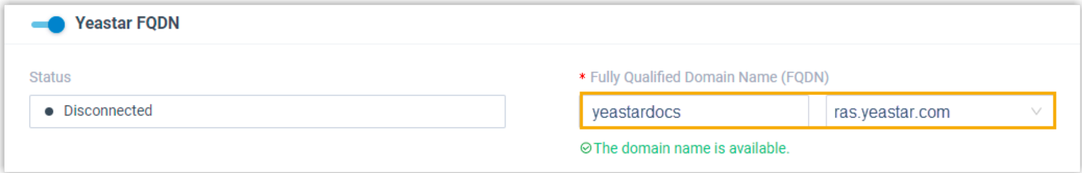
With a Yeastar FQDN, you can remotely access the LDAP server on PBX via secure LDAP connection without the need of configuring public IP and port forwarding for the PBX. This topic describes how to configure network for remote LDAP access via FQDN.

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.

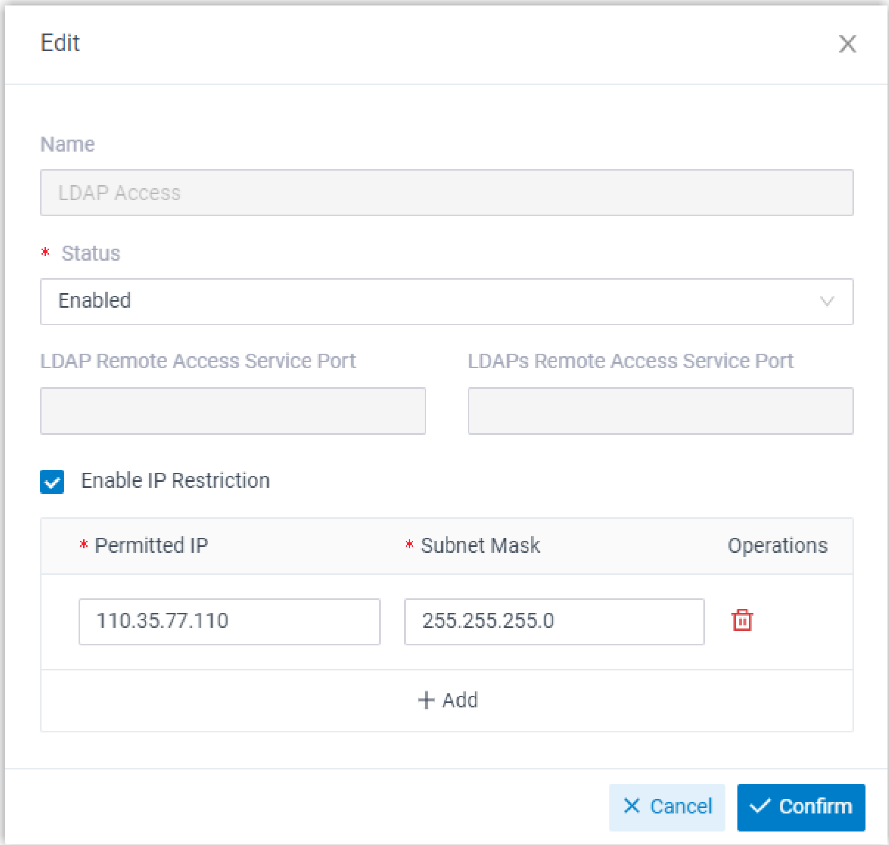
    Yeastar FQDN

    Status: Disconnected

    * Fully Qualified Domain Name (FQDN): yeastardocs | ras.yeastar.com

    The domain name is available.

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.



Edit

Name: LDAP Access

* Status: Enabled

LDAP Remote Access Service Port:

LDAPs Remote Access Service Port:

☑ Enable IP Restriction

* Permitted IP	* Subnet Mask	Operations
110.35.77.110	255.255.255.0	🗑

- 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.

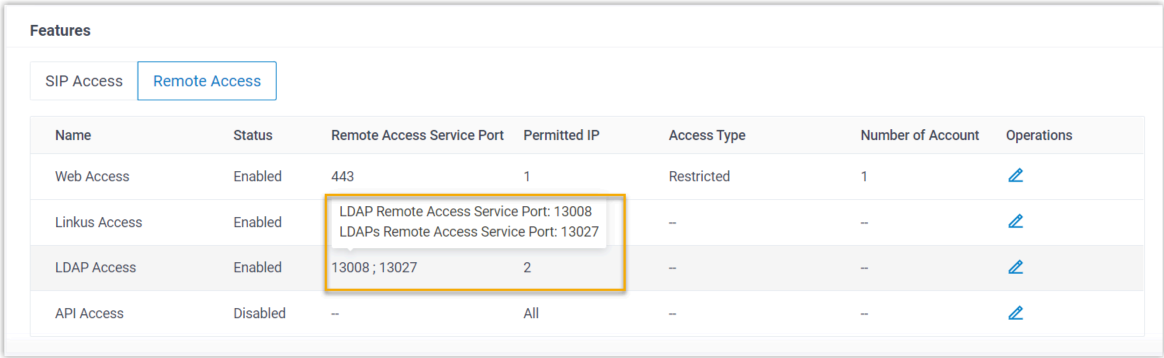
  If you configure this option, only the permitted IP address(es) can use the remote access feature.

d. Click Confirm.

5. Click Save.

Result

- The Remote Access Service automatically assigns ports for remote LDAP access.



Features

Name	Status	Remote Access Service Port	Permitted IP	Access Type	Number of Account	Operations
Web Access	Enabled	443	1	Restricted	1	✎
Linkus Access	Enabled	LDAP Remote Access Service Port: 13008 LDAPs Remote Access Service Port: 13027		--	--	✎
LDAP Access	Enabled	13008 ; 13027	2	--	--	✎
API Access	Disabled	--	All	--	--	✎

- 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 Software Edition as an LDAP Server.

Configure Network for Remote API Access by a Yeastar FQDN

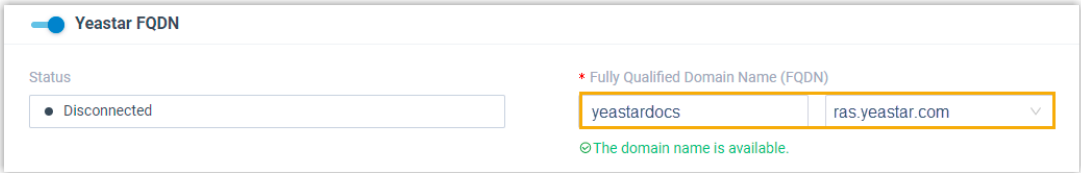
With a Yeastar FQDN, you can remotely access Yeastar P-Series APIs via a secure tunnel, without the need of configuring public IP and port forwarding for the PBX. This topic describes how to configure network for remote API access via FQDN.

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.



Yeastar FQDN

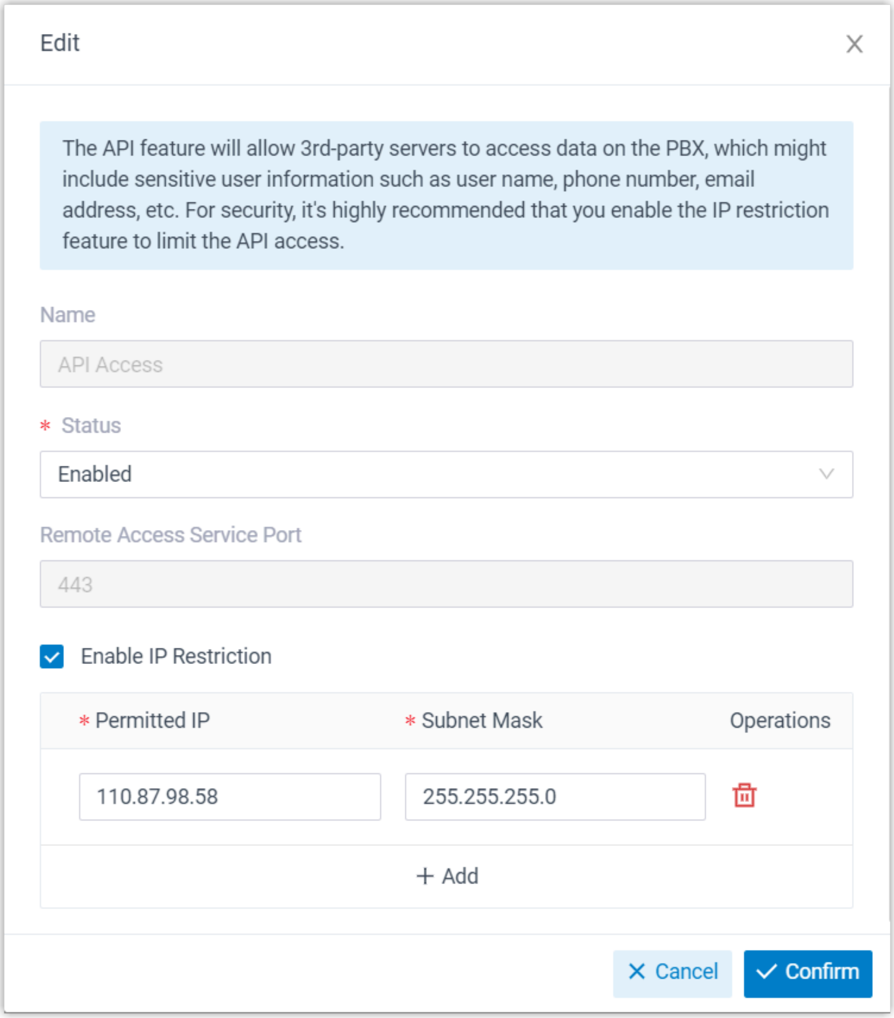
Status: ● Disconnected

* Fully Qualified Domain Name (FQDN): yeastardocs | ras.yeastar.com

The domain name is available.

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.



Edit

The API feature will allow 3rd-party servers to access data on the PBX, which might include sensitive user information such as user name, phone number, email address, etc. For security, it's highly recommended that you enable the IP restriction feature to limit the API access.

Name: API Access

* Status: Enabled

Remote Access Service Port: 443

☑ Enable IP Restriction

* Permitted IP	* Subnet Mask	Operations
110.87.98.58	255.255.255.0	🗑

- 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.

Public IP and Ports

Public IP and Ports Overview

This topic describes when you need to configure the Public IP and Ports settings and introduces two functions of Public IP and Ports settings.

Applications

When your PBX is connected behind a router and needs to communicate with SIP devices on the external network, you need to set Public IP and Ports settings. Public IP and Port settings can be applied to different types of networks:

- Public IP Address
- External Host

Public IP Address

If your Internet Service Provider (ISP) provides a static public IP address, you can configure PBX network for remote access with the IP address.

For more information about the configurations, see Configure Network for Remote Access by a Domain Name.

External Host

If static public IP address is not available in your network environment, you must have a registered domain name, and configure PBX network for remote access with the domain name.

For more information about the configurations, see Configure Network for Remote Access by a Public IP Address.

Functions

Public IP and Ports settings have the following two functions to ensure that remote devices can access and communicate with the PBX via SIP protocol:

- Solve SIP NAT issue
- Provide PBX with information of Linkus remote access

Solve SIP NAT issue

If your PBX is connected behind a router, it can be said that the PBX is behind a Network Address Translation (NAT) router. To allow remote devices to access the PBX, you need to set up NAT rules and port forwarding on the router. In this way, the router will forward the right inbound packets from the internet to the PBX.

SIP-based communication does not reach devices in the Local Area Network (LAN) behind firewalls and NAT routers automatically. Public IP and Ports settings on the Yeastar P-Series Software Edition 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 Software Edition 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 Software Edition 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

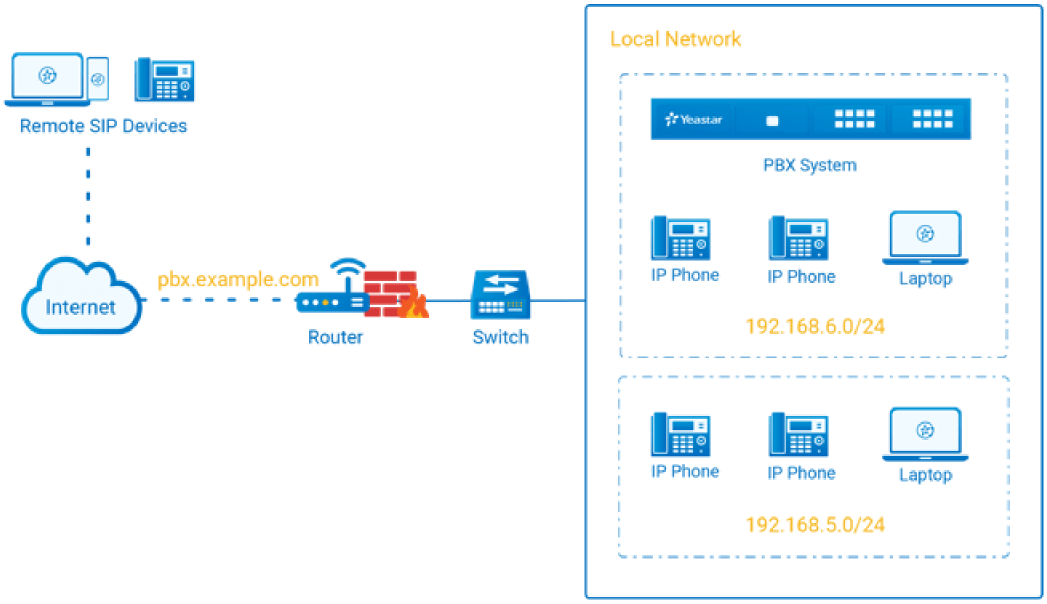
To ensure that remote Linkus clients and other SIP devices can communicate with Yeastar P-Series Software Edition normally, you need to configure Public IP and Ports on the PBX. This topic provides a configuration example based on the network scenario that no static public IP address is available and 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

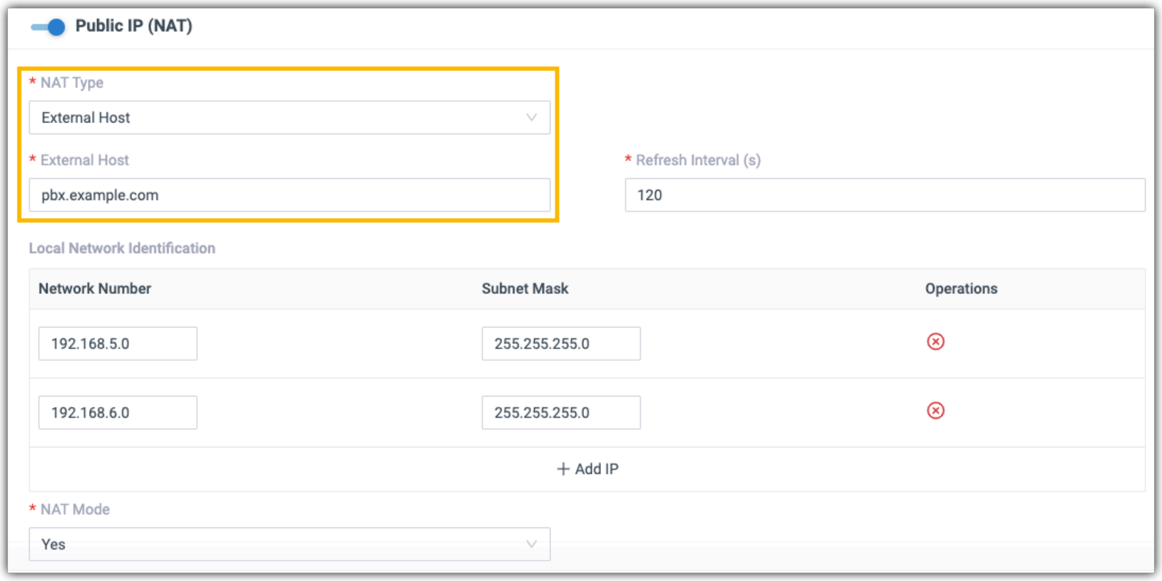
Procedure

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.

- NAT Type: Select External Host.
- External Host: Enter pbx.example.com.
- Refresh Interval (s): Leave the default setting or change the interval (in seconds) for PBX to request the external host for public IP.
- Local Network Identification: Add all your local network. This setting will allow all your local devices to communicate with the PBX by the local IP address instead of passing through the router.

  In this scenario, add two local network: 192.168.5.0/255.255.255.0 and 192.168.6.0/255.255.255.0.
- NAT Mode: Select a SIP NAT mode. In this scenario, select Yes.
    - Yes: Use NAT and ignore the address information in the SIP/SDP headers and reply to the sender's IP address and port.
    - No: Use NAT mode only according to RFC3581.
    - Never: Never attempt NAT mode or RFC3581 support.
    - Route: Use NAT but do not include rport in headers.



Public IP (NAT)

* NAT Type: External Host

* External Host: pbx.example.com

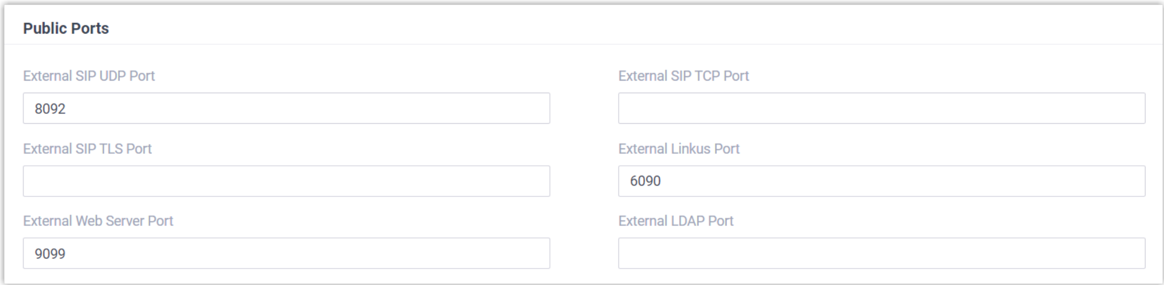
* Refresh Interval (s): 120

Local Network Identification

Network Number	Subnet Mask	Operations
192.168.5.0	255.255.255.0	⊗
192.168.6.0	255.255.255.0	⊗

* NAT Mode: Yes

3. In the Public Ports section, enter the external ports that you have forwarded on your router.
    - External SIP UDP Port: Enter 8092.
    - External SIP TCP Port: Leave it blank because SIP TCP protocol is not used in this scenario.
    - External SIP TLS Port: Leave it blank because SIP TLS protocol is not used in this scenario.
    - External Linkus Port: Enter 6090.
    - External Web Server Port: Enter 9099.
    - External LDAP Port: Leave it blank because LDAP protocol is not used in this scenario.



Public Ports

External SIP UDP Port: 8092

External SIP TCP Port:

External SIP TLS Port:

External Linkus Port: 6090

External Web Server Port: 9099

External LDAP Port:

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.

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

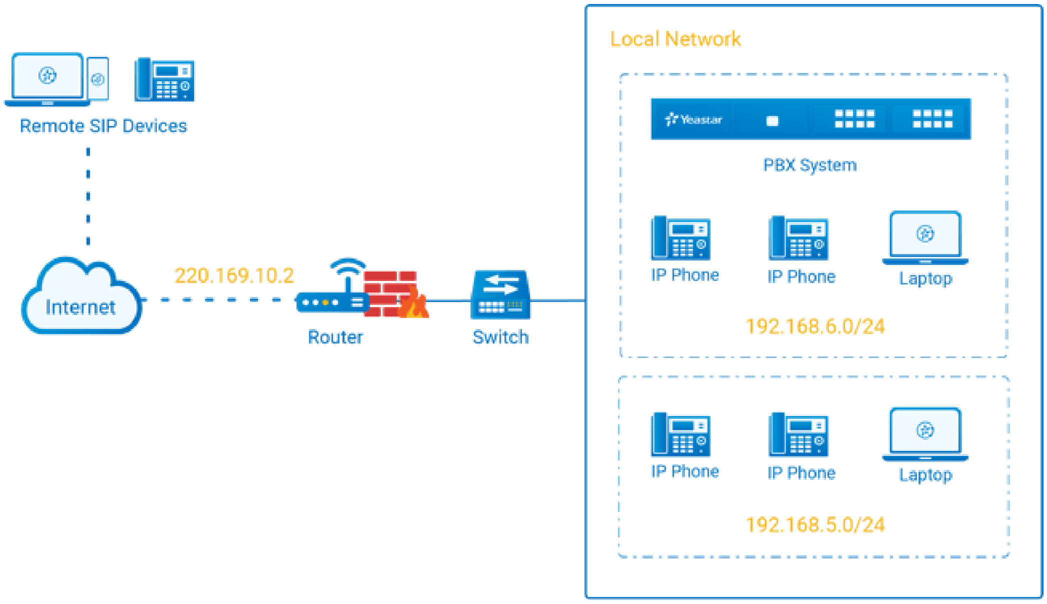
Configure Network for Remote Access by a Public IP Address

To ensure that remote Linkus clients and other SIP devices can communicate with Yeastar P-Series Software Edition 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

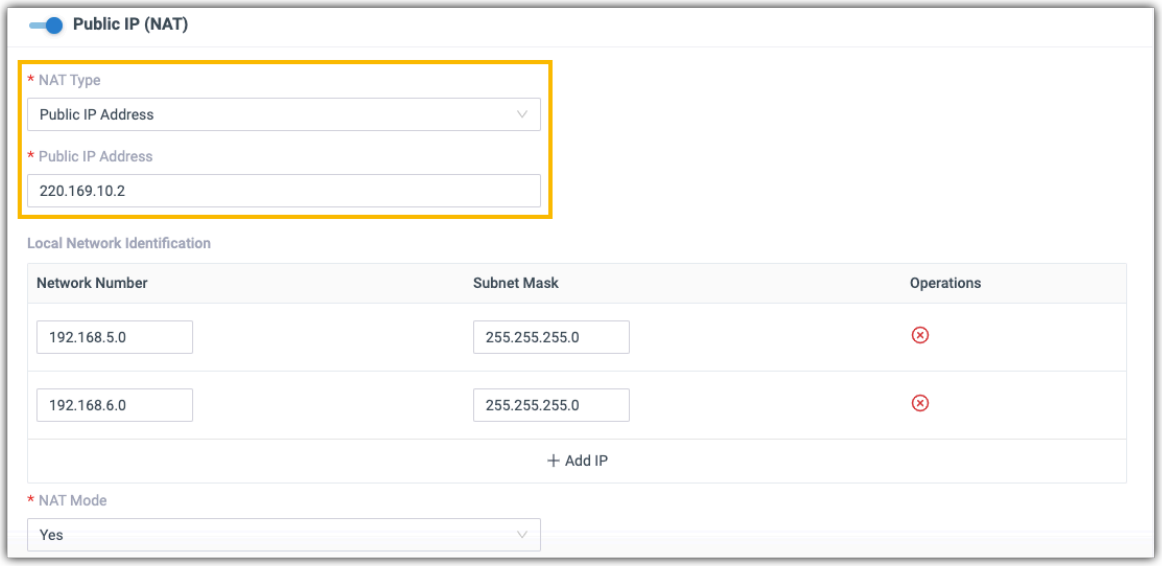
Procedure

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.
   - NAT Type: Select Public IP Address .
   - Public IP Address: Enter 220.169.10.2.

- Local Network Identification: Add all your local network. This setting will allow all your local devices to communicate with the PBX by the local IP address instead of passing through the router.

  In this scenario, add two local network: 192.168.5.0/255.255.255.0 and 192.168.6.0/255.255.255.0.
- NAT Mode: Select a SIP NAT mode. In this scenario, select Yes.
  - Yes: Use NAT and ignore the address information in the SIP/SDP headers and reply to the sender's IP address and port.
  - No: Use NAT mode only according to RFC3581.
  - Never: Never attempt NAT mode or RFC3581 support.
  - Route: Use NAT but do not include rport in headers.



Public IP (NAT)

* NAT Type

Public IP Address

* Public IP Address

220.169.10.2

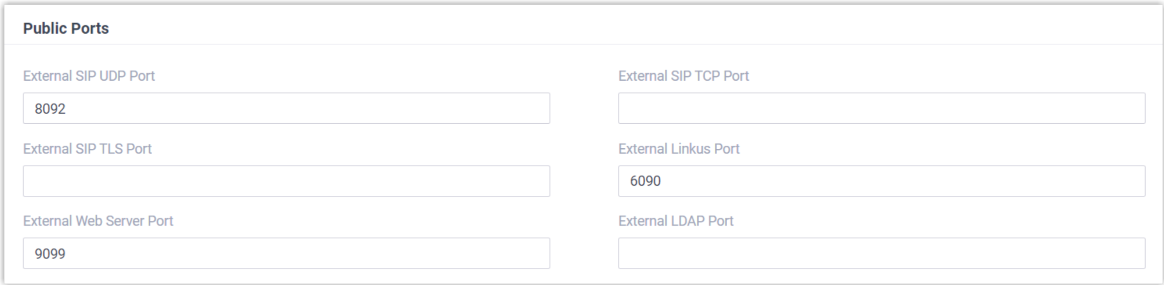
Local Network Identification

Network Number	Subnet Mask	Operations
192.168.5.0	255.255.255.0	⊗
192.168.6.0	255.255.255.0	⊗

* NAT Mode

Yes

3. In the Public Ports section, enter the external ports that you have forwarded on your router.
   - External SIP UDP Port: Enter 8092.
   - External SIP TCP Port: Leave it blank because SIP TCP protocol is not used in this scenario.
   - External SIP TLS Port: Leave it blank because SIP TLS protocol is not used in this scenario.
   - External Linkus Port: Enter 6090.
   - External Web Server Port: Enter 9099.
   - External LDAP Port: Leave it blank because LDAP protocol is not used in this scenario.



Public Ports

External SIP UDP Port: 8092	External SIP TCP Port:
External SIP TLS Port:	External Linkus Port: 6090
External Web Server Port: 9099	External LDAP Port:

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

Static Route

Static Route Overview

This topic provides an overview of static route table and all associated system routes.

Route table

Yeastar P-Series Software Edition 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.

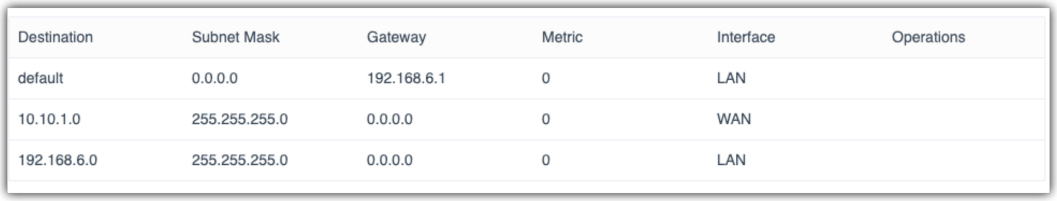
Network settings

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 Software Edition.

Background information

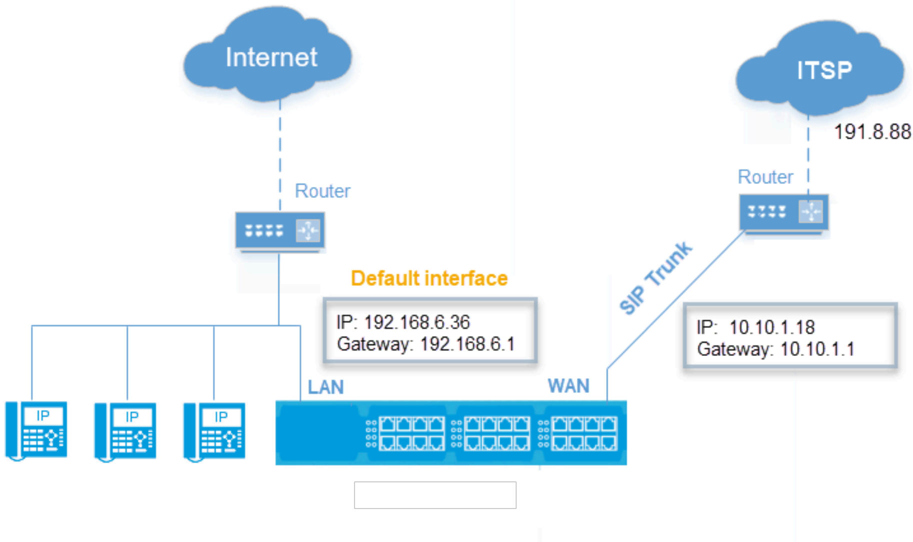
Adding custom static route is typically used in the "Dedicated SIP trunking" scenario.

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

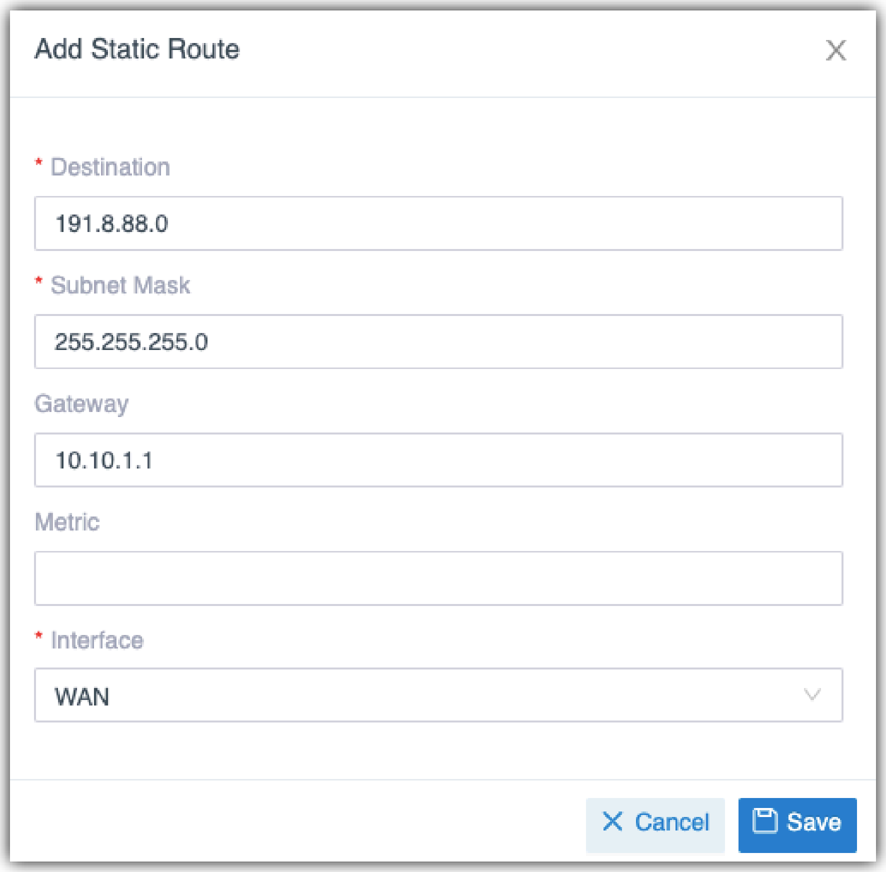
Setting	Value
Ethernet Mode	Dual
Default Interface	LAN
LAN	
IP Address	192.168.6.36
Subnet Mask	255.255.255.0
Gateway	192.168.6.1
Preferred DNS Server	192.168.1.1
WAN	
IP Address	10.10.1.18
Subnet Mask	255.255.255.0
Gateway	10.10.1.1
Preferred DNS Server	10.10.1.1

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:



Add Static Route

* Destination: 191.8.88.0

* Subnet Mask: 255.255.255.0

Gateway: 10.10.1.1

Metric:

* Interface: WAN

- Destination: Enter the destination IP address or IP subnet for the PBX to reach using the static route.

  Note:
  To ensure that both SIP registration packets and SIP media packets can be routed to the desired destination, set the IP range of the SIP trunking. In this scenario, enter 191.8.88.0.
- Subnet Mask: Enter the subnet mask for the destination address. In this scenario, enter 255.255.255.0.
- Gateway: Enter the gateway address. The PBX will reach the destination address through this gateway. In this scenario, enter 10.10.1.1.
- Metric: Optional.

  Routing metric is used to determine whether one route should be chosen over another.
- Interface: Select the network interface.

  The PBX will reach the destination address using the static route through the selected network interface. In the scenario, select WAN.

3. Click Save and Apply.

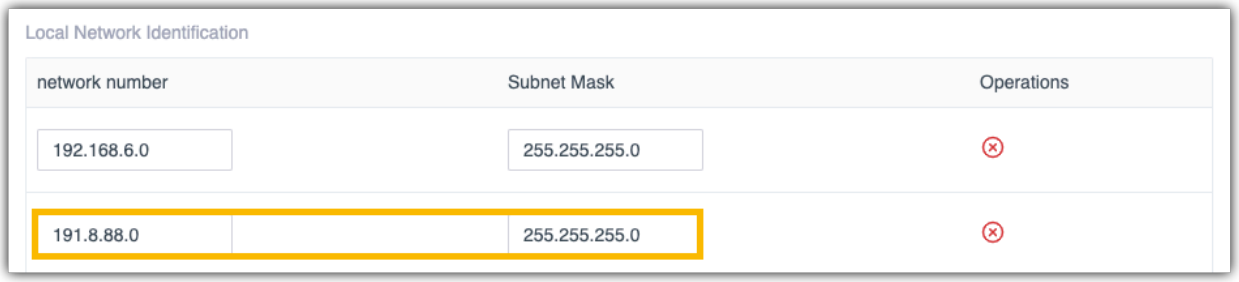
Result

After you set up a SIP trunk with the IP address 191.8.88.15 on the PBX, the SIP packets are sent and received by the WAN port, which ensure the communication between the PBX and the ITSP.

What to do next

To avoid SIP audio issues through the SIP trunk, you may need to add the network segment of the SIP trunk as a local network identification in PBX NAT settings.

In this scenario, add the IP segment 191.8.88.0/255.255.255.0 in the NAT settings as the following figure shows. For more information of NAT, see Configure Network for Remote Access by a Domain Name.



Local Network Identification

network number	Subnet Mask	Operations
192.168.6.0	255.255.255.0	⊗
191.8.88.0	255.255.255.0	⊗

Manage Static Routes

After you add static routes on the Yeastar P-Series Software Edition, 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

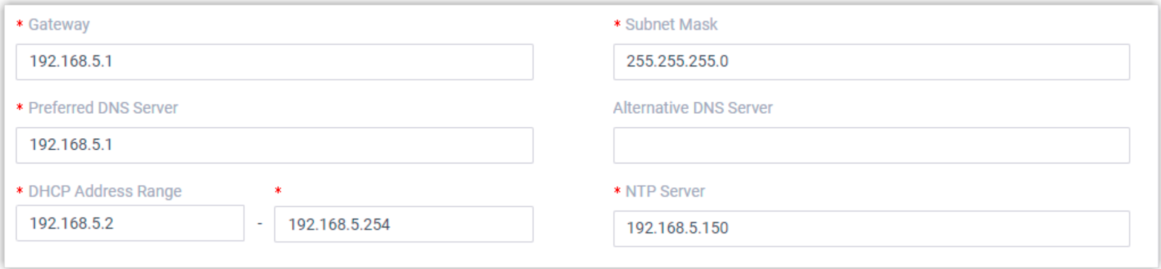
Yeastar P-Series Software Edition provides a built-in DHCP server. When there is no DHCP server in the local network, you can set up the PBX as a DHCP server to assign IP addresses, gateway, DNS and other network parameters to devices in the same local network .

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: 192.168.5.1

* Subnet Mask: 255.255.255.0

* Preferred DNS Server: 192.168.5.1

Alternative DNS Server:

* DHCP Address Range: 192.168.5.2 - * 192.168.5.254

* NTP Server: 192.168.5.150

   - Gateway: Specify the IP address of the default gateway for the DHCP server.
   - Subnet Mask: Specify the subnet mask used to subdivide your IP address.
   - Preferred DNS Server: Specify a DNS server for the DHCP server.
   - Alternative DNS Server: Optional. Specify a secondary DNS server for the DHCP server.
   - DHCP Address Range: Specify the IP address range that will be allocated to DHCP clients.
   - NTP Server: Enter the IP address of an NTP server.

   > Tip:
   > The default value is the IP address of the PBX, which can synchronize the network time of the client devices with the PBX.
4. Click Save.

   The Status field displays Running, indicating the DHCP server is running.

Result

The PBX can now be used as a DHCP server and assign IP addresses, gateway, and other network configurations to the devices located in the local network.

Date and Time

Change System Time Manually

In case you want to change system time when the PBX can not access the Internet, you can change system time manually. This topic describes how to manually change system time to your local time.

Background information

To ensure that the time of logs and CDRs generated on Yeastar P-Series Software Edition 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 Software Edition is consistent with your local time, you need to adjust system time to your local time.

Prerequisites

Make sure Yeastar P-Series Software Edition 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 Software Edition 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 Software Edition 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 Software Edition 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 Software Edition.

Prerequisites

Make sure Yeastar P-Series Software Edition 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 Software Edition.

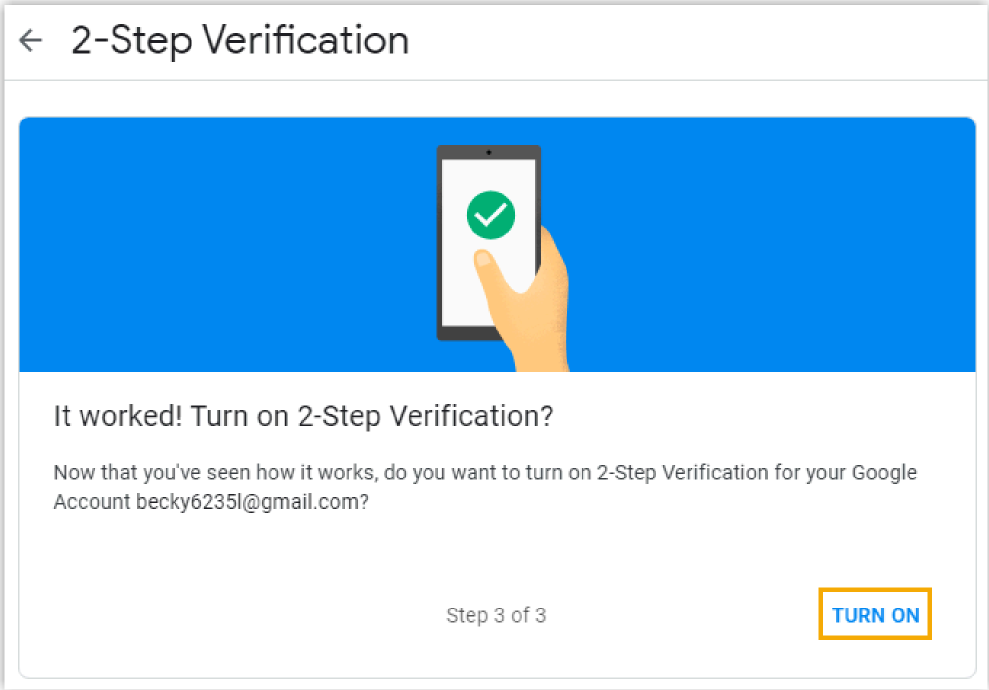
Prerequisites

Make sure Yeastar P-Series Software Edition 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.

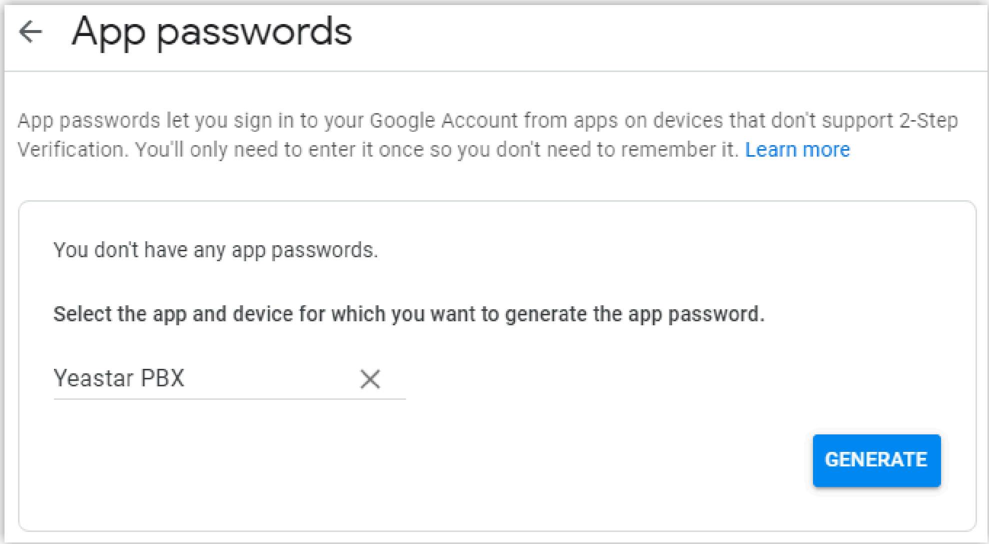


2-Step Verification

It worked! Turn on 2-Step Verification?

Now that you've seen how it works, do you want to turn on 2-Step Verification for your Google Account becky6235l@gmail.com?

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.



App passwords

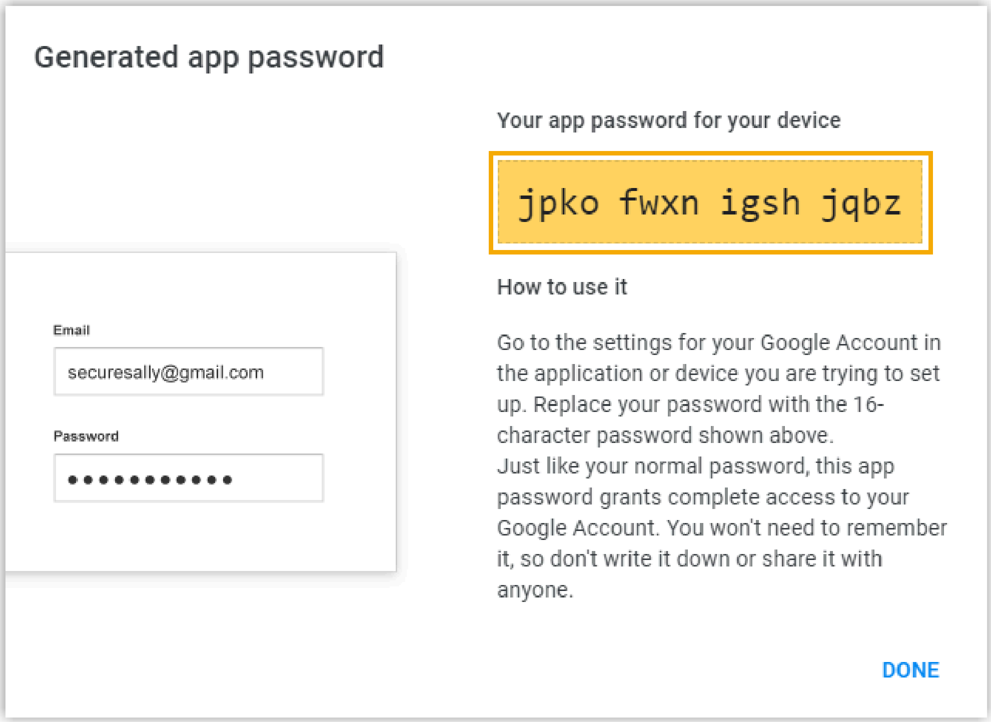
App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

You don't have any app passwords.

Select the app and device for which you want to generate the app password.

Yeastar PBX

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.



Generated app password

Your app password for your device

jpko fwxn igsh jqbz

How to use it

Go to the settings for your Google Account in the application or device you are trying to set up. Replace your password with the 16-character password shown above.

Just like your normal password, this app password grants complete access to your Google Account. You won't need to remember it, so don't write it down or share it with anyone.

Email: securesally@gmail.com

Password: ●●●●●●●●●●●

Step2. Configure Gmail as mail server of Yeastar P-Series Software Edition

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. Configure email server settings.
   - Sender Email Address: Enter your Gmail address, which will appear as the From address for outgoing emails sent by the PBX.
   - Email Address or Username: Enter your Gmail address.
   - Password: Enter the 16-digit app password, which is used to access Gmail server.
   - Outgoing Mail Server (SMTP): Retain the default value smtp.gmail.com.
   - Port: Retain the default value 587.
   - Enable TLS Encryption: Keep the option unselected.
4. Test if the mail server can successfully send emails.
   a. Click Test.
   b. In the pop-up window, enter a recipient's email address in the Email Address field.
   c. Click Test.
5. Click Save.

Result

- If the test email is sent successfully, the page displays "Success" and the recipient's mailbox would receive the email.
- If the test email is failed to be sent, the page displays "Failed to send" and prompts you an error message. You can check the error in Email Sent Logs.

Set up Outlook as an Email Server

This topic describes how to set up Outlook as an email server in Yeastar P-Series Software Edition.

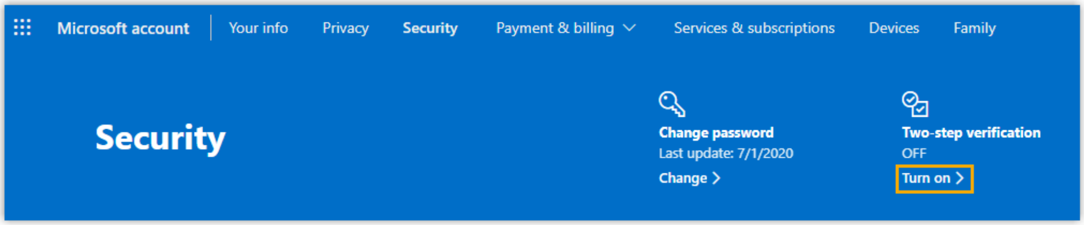
Prerequisites

Make sure the PBX can access the Internet.

Step1. Create an app password on Microsoft Account

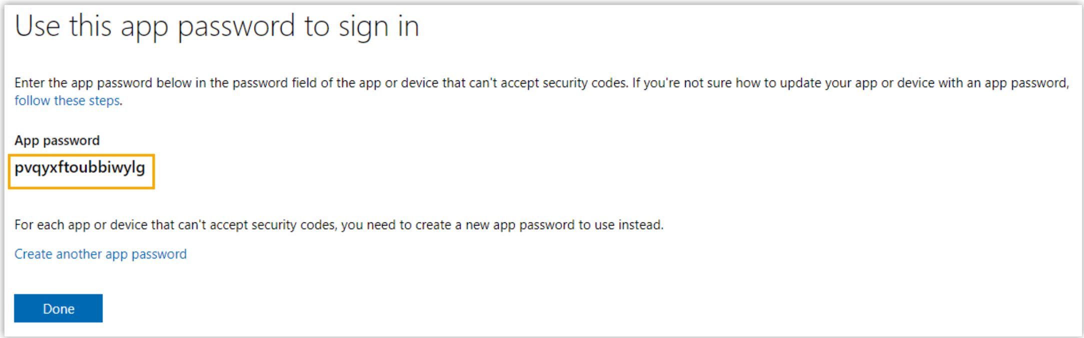
To ensure that PBX can access Outlook server via your Microsoft account, you need to turn on 2-Step verification and create an app password as follows.

1. Sign in to Microsoft Account.
2. At the top navigation bar, click Security tab and enter your Outlook password to verify your account.
3. Turn on 2-Step Verification.
   a. In the Two-step verification section, click Turn on, and verify your account according to the prompt.



   b. In the Two-step verification section, click Set up two-step verification.
   c. Read the tips and click Next.
   d. In the Verify my identity with drop-down list, select a method and verify your account according to the prompt.

      Two-step verification is enabled.
4. Create an app password.
   a. At the top navigation bar, click Security tab.
   b. In the Two-step verification section, click Manage.
   c. In the App passwords section, click Create a new app password.



Use this app password to sign in

Enter the app password below in the password field of the app or device that can't accept security codes. If you're not sure how to update your app or device with an app password, follow these steps.

App password

pvqyxftoubbiwylg

For each app or device that can't accept security codes, you need to create a new app password to use instead.

Create another app password

An app password is generated. Note down the password, which is used to verify your Outlook account when you configure Outlook as the mail server of the PBX.

Step2. Configure Outlook as email server of Yeastar P-Series Software Edition

To ensure that the PBX can access and send mails from Outlook server via your Microsoft account, you should proceed as follows:

1. Log in to PBX web portal, go to System > Email > Email Server.
2. In the Type of Email Server drop-down list, select Custom Email Server.
3. Configure email server settings.
    - Sender Email Address: Enter your Outlook address, which will appear as the From address for outgoing emails sent by the PBX.
    - Email Address or Username: Enter your Outlook address.
    - Password: Enter the 16-digit app password, which is used to access Outlook server.
    - Outgoing Mail Server (SMTP): Retain the default value smtp-mail.outlook.com.
    - Port: Retain the default value 587.
    - Enable TLS Encryption: Keep the option unselected.
4. Test if the mail server can successfully send emails.
    a. Click Test.
    b. In the pop-up window, enter a recipient's email address in the Email Address field.
    c. Click Test.
5. Click Save.

Result

- If the test email is sent successfully, the page displays "Success" and the recipient's mailbox would receive the email.
- If the test email is failed to be sent, the page displays "Failed to send" and prompts you an error message. You can check the error in Email Sent Logs.

Customize Email Templates

This topic describes how to customize email notification language and email templates.

Background information

If you have enabled notification for a specific event, and have chosen to send emails to notify contacts, the system will send emails in the pre-configured email template to inform contacts when the event is triggered.

Yeastar P-Series Software Edition 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

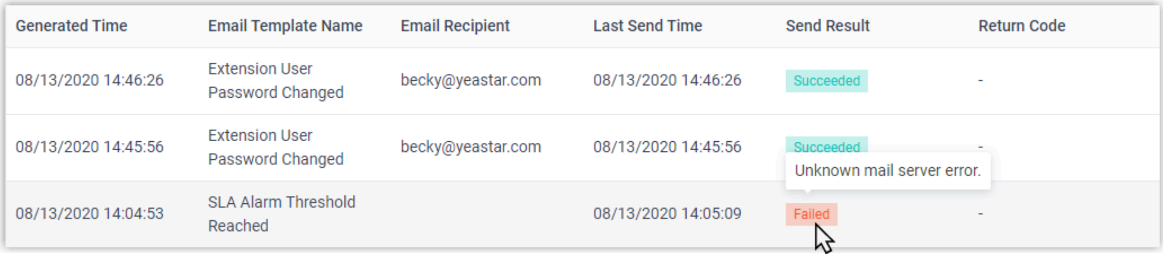
By default, when logs reach 50,000, the newest logs will replace the oldest logs. You can change the value, or restrict how long logs can be saved.

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.



Generated Time	Email Template Name	Email Recipient	Last Send Time	Send Result	Return Code
08/13/2020 14:46:26	Extension User Password Changed	becky@yeastar.com	08/13/2020 14:46:26	Succeeded	-
08/13/2020 14:45:56	Extension User Password Changed	becky@yeastar.com	08/13/2020 14:45:56	Succeeded	-
08/13/2020 14:04:53	SLA Alarm Threshold Reached		08/13/2020 14:05:09	Failed	-

Unknown mail server error.

Storage

Storage Overview

Yeastar P-Series Software Edition provides local storage and supports external storage and network drive storage.

Storage limitation

Storage limitation

- LOCAL (Local Flash): Max. 1
- Network drive: Max. 2
- Hard disk drive (SATA/SAS/VSD): Max. 4

The supported data for changing storage locations

Yeastar P-Series Software Edition supports to change storage locations for the following data:

- Voicemail
- Logs, including event logs, email sent logs, operation logs, and system logs.
- Recordings
- Backup files

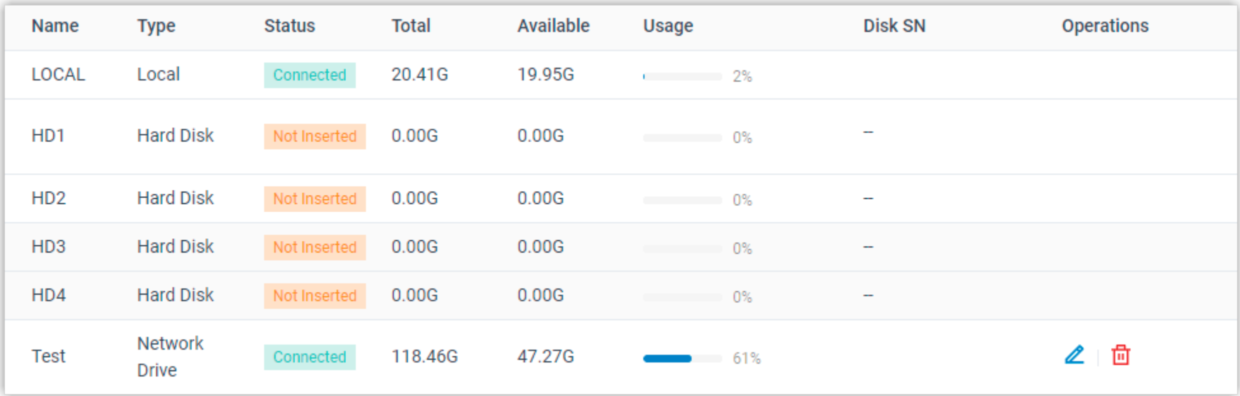
For more information, see Manage Storage Locations.

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 hard disk.
- Click ⇥ to remove hard disk.



Name	Type	Status	Total	Available	Usage	Disk SN	Operations
LOCAL	Local	Connected	20.41G	19.95G	2%		
HD1	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
HD2	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
HD3	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
HD4	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
Test	Network Drive	Connected	118.46G	47.27G	61%		✎ | 🗑

Set up a Hard Disk Drive

By default, all the voicemails, logs, and backup files are stored in the local disk (LOCAL). If you install Yeastar P-Series Software Edition on a physical machine, you can set up hard disk drives for storage. This topic describes how to set up a hard disk drive on Dell EMC PowerEdge R340 Server.

Restrictions

Before you get started, familiarize yourself with the following restrictions:

- Number of hard disk drive: Max. 4
- Type of hard disk drive: SATA/SAS/VSD

Prerequisites

- If you want to replace an installed hard disk drive with a new one, make sure the hard disk drive is not used for storage.

  > Note:
  >
  > Go to System > Storage > Storage Locations to check.
- Shut down the PBX system.

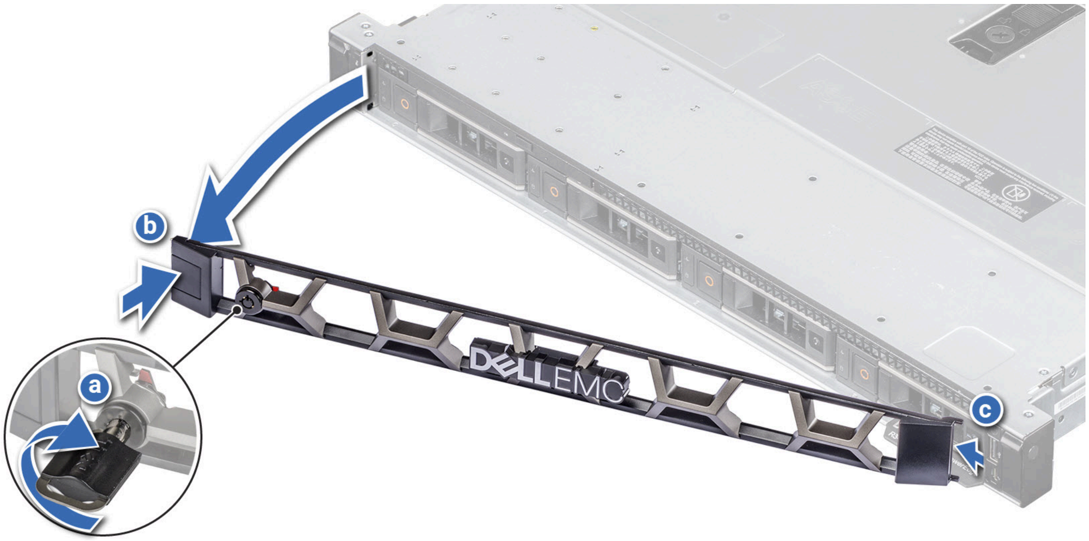
  For more information, see Shut Down Yeastar P-Series Software Edition.

Procedure

- Step1. Install a hard disk drive on Dell EMC PowerEdge R340 Server
- Step2. Set up the hard disk drive on Yeastar P-Series Software Edition

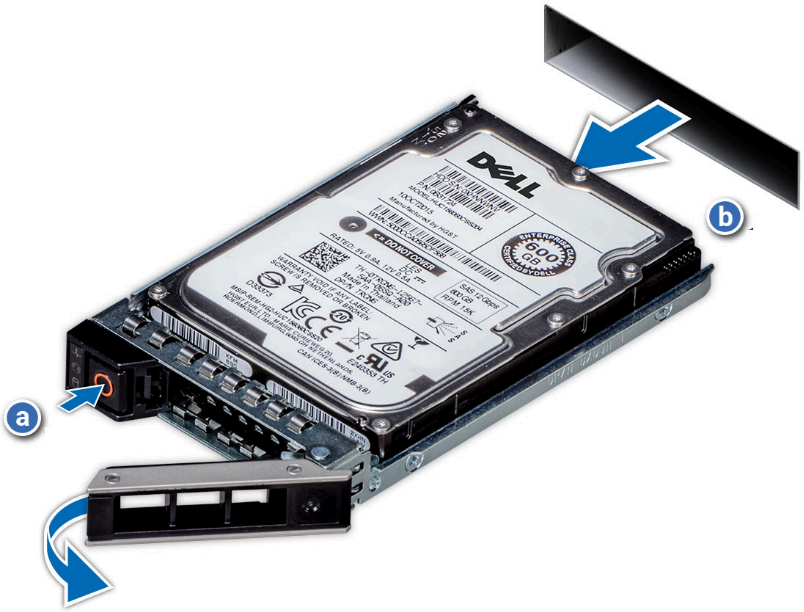
Step1. Install a hard disk drive on Dell EMC PowerEdge R340 Server

1. Power off Dell EMC PowerEdge R340 Server.
2. Remove the front bezel.



a. Unlock the bezel.
b. Press the release button, and remove the left end of the bezel.
c. Slide the tabs on the right end of the bezel out of the slots on the chassis and remove the bezel.

3. Remove drive carrier.

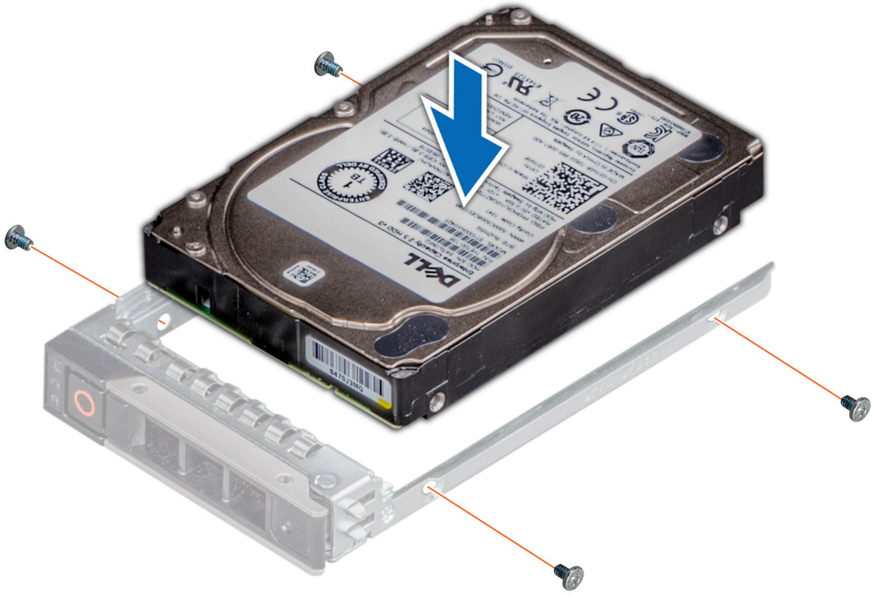


a. Press the release button to open the drive carrier release handle.
b. Holding the drive carrier release handle, slide the drive carrier out of the drive slot.

4. Install the drive into the drive carrier.

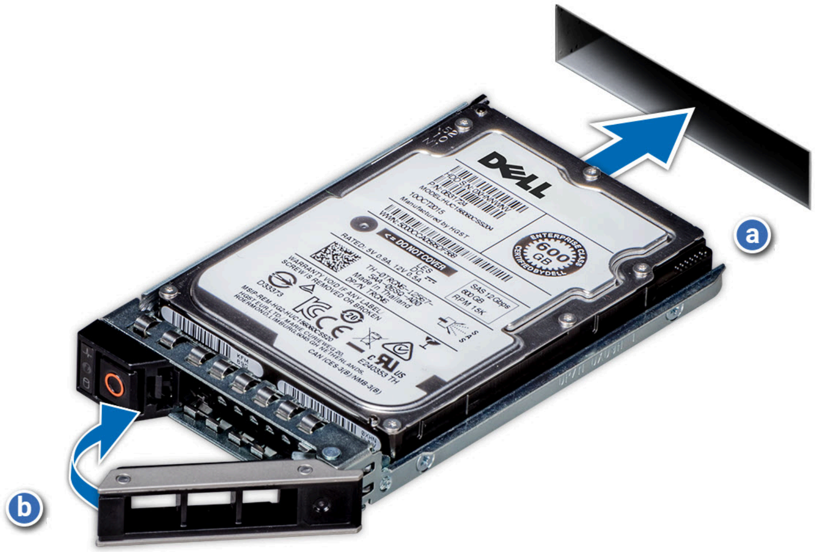
> Important:

The system names hard disk drives based on the installation order, whichever drive carrier the drive is installed. For example, the system names the firstly installed hard disk drive as HD1, the second one as HD2, and the alike. To avoid confusion, install the drive in strict order.



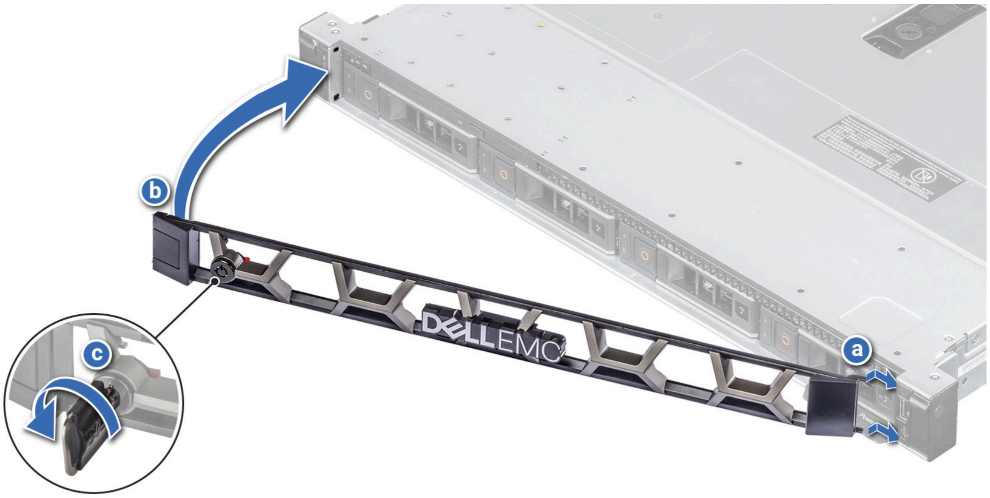
a. Insert the drive into the drive carrier with the drive connector facing towards the rear of the carrier.
b. Align the screw holes on the drive with the screws holes on the drive carrier.
c. Using a Phillips #1 screwdriver, replace the screws to secure the drive to the drive carrier.

5. Install drive carrier.



a. Slide the drive carrier into the drive slot.
b. Close the drive carrier release handle to lock the drive in place.

6. Install the front bezel.

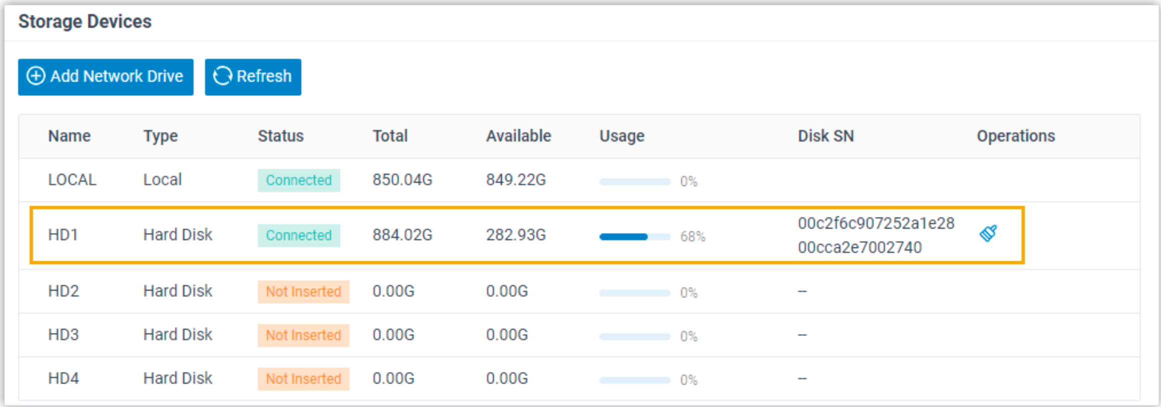


a. Align and insert the tabs on the bezel into the slots on the chassis.
b. Press the bezel until the release button clicks in place.
c. Lock the bezel.

7. Power on Dell EMC PowerEdge R340 Server.

Step2. Set up the hard disk drive on Yeastar P-Series Software Edition

1. Log in to PBX web portal, go to System > Storage.
2. In the Storage Devices section, check the installed hard disk drive.



Name	Type	Status	Total	Available	Usage	Disk SN	Operations
LOCAL	Local	Connected	850.04G	849.22G	0%		
HD1	Hard Disk	Connected	884.02G	282.93G	68%	00c2f6c907252a1e28 00cca2e7002740	🖌
HD2	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
HD3	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
HD4	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	

3. Format the hard disk drive.
    a. Click 🖌 beside the hard disk drive.
    b. In the pop-up dialog box, click Yes.

Result

The Status is displayed as Connected, which indicates that the hard disk drive is ready for storage.

What to do next

Decide what data will be stored on the hard disk drive. 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 Software Edition.

Restriction

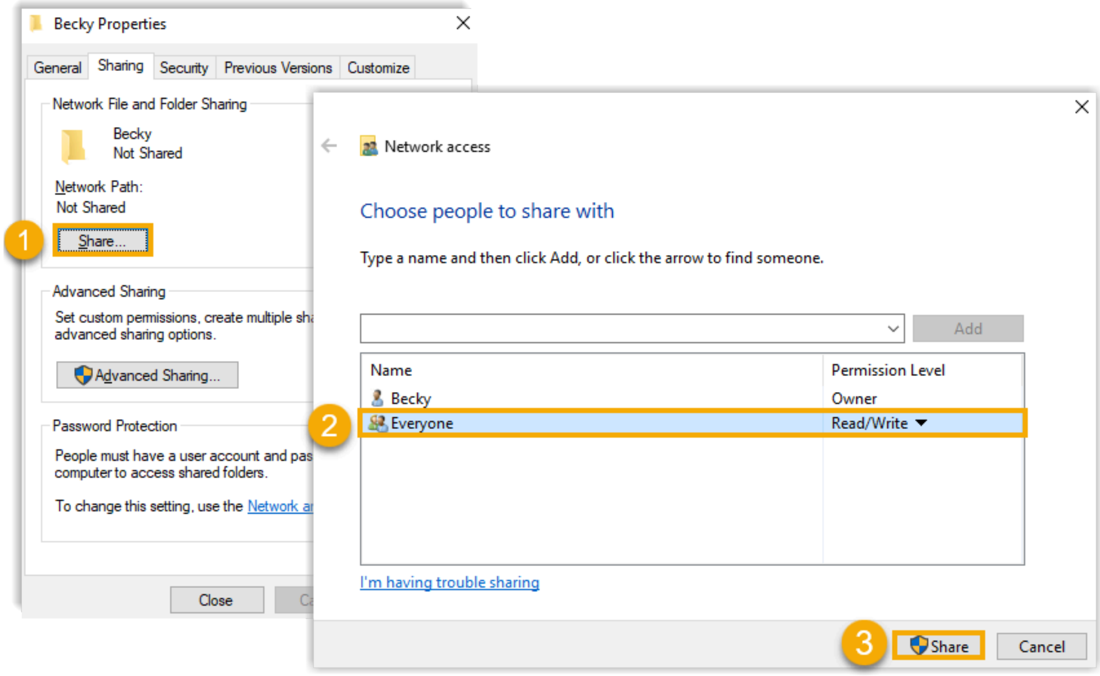
You can add up to 2 network drives.

Prerequisites

Make sure that the computer is always in service, or Yeastar P-Series Software Edition 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.



Set custom permissions, create multiple sh advanced sharing options.

People must have a user account and pas computer to access shared folders.

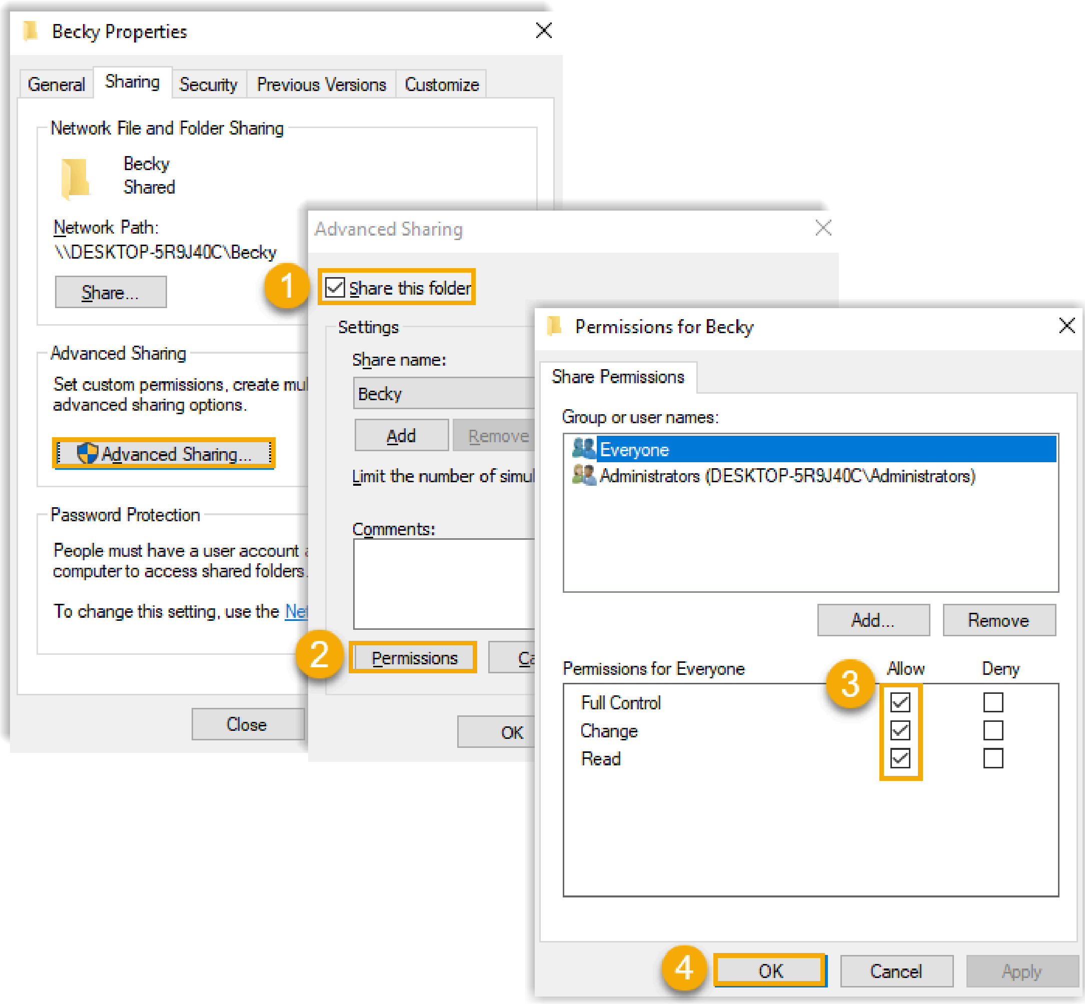
To change this setting, use the Network a

Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

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.

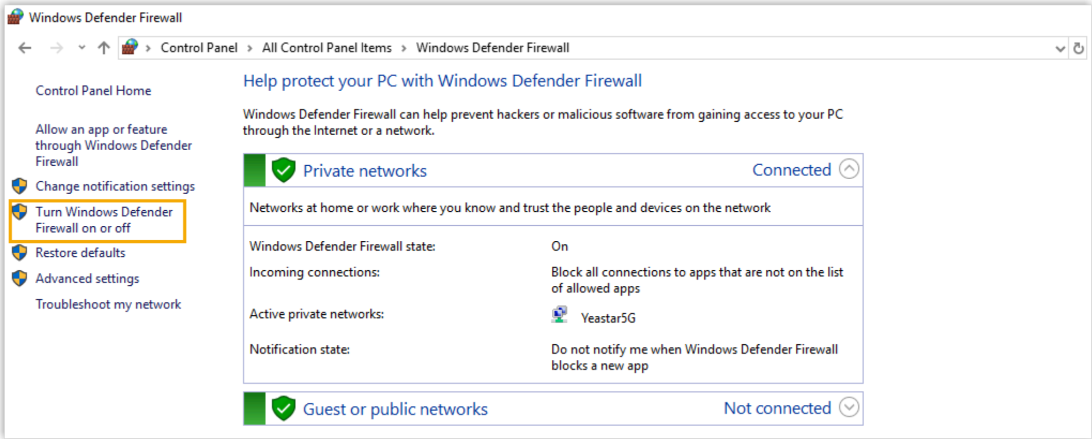
4. Click Advanced Sharing..., configure advanced Share properties.



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.


Windows Defender Firewall
Control Panel > All Control Panel Items > Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Defender Firewall state: On

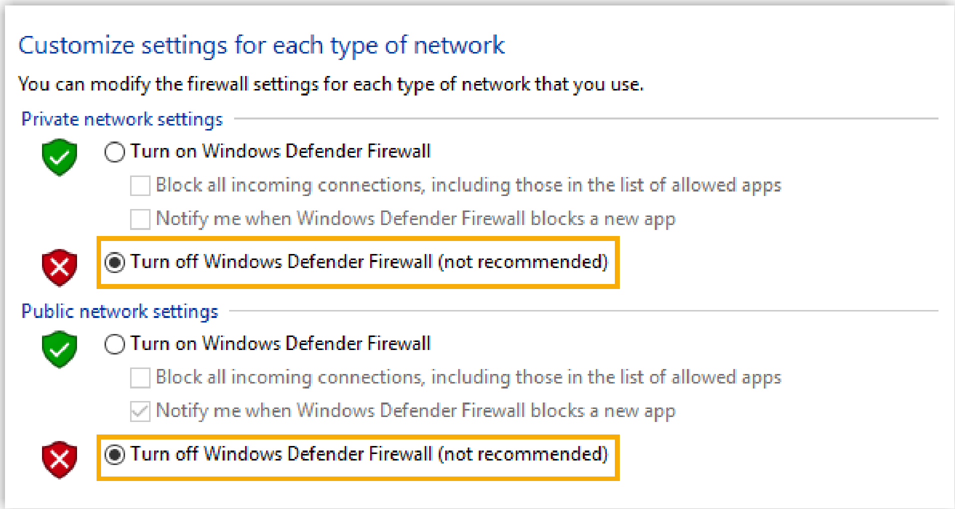
Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active private networks: Yeastar5G

Notification state: Do not notify me when Windows Defender Firewall blocks a new app

Guest or public networks — Not connected

3. In both Private network settings and Public network settings sections, select Turn off Windows Defender Firewall (not recommended).



Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

□ Notify me when Windows Defender Firewall blocks a new app

● Turn off Windows Defender Firewall (not recommended)

Public network settings

○ Turn on Windows Defender Firewall

□ Block all incoming connections, including those in the list of allowed apps

☑ Notify me when Windows Defender Firewall blocks a new app

● 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.

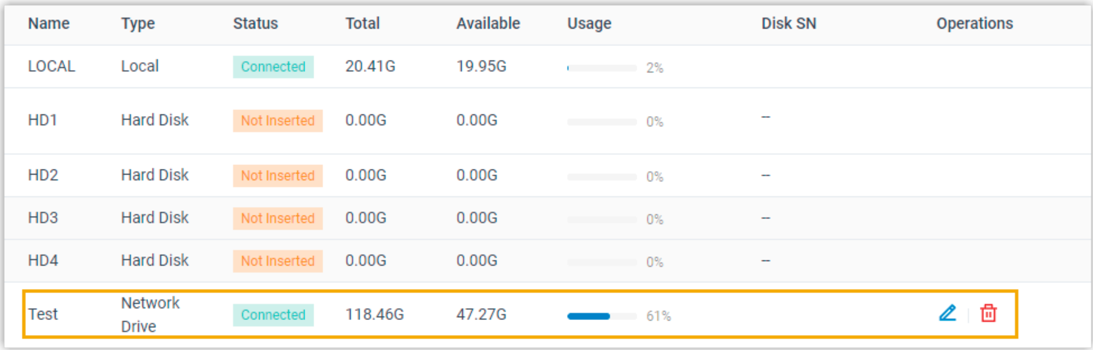
- Access Username: Enter the username to access the shared folder.
- Access Password: Enter the password to access the shared folder.
- Work Group: Optional. If you have set work group on your network drive, enter the name of the work group. If not, leave this field blank.
- Samba Version: Select the 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



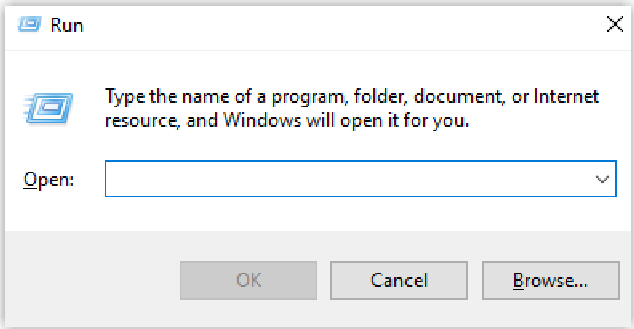
Name	Type	Status	Total	Available	Usage	Disk SN	Operations
LOCAL	Local	Connected	20.41G	19.95G	2%		
HD1	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
HD2	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
HD3	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
HD4	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
Test	Network Drive	Connected	118.46G	47.27G	61%		✎ 🗑

What to do next

Decide what data will be stored on the network drive. For more information, see Manage Storage Locations.

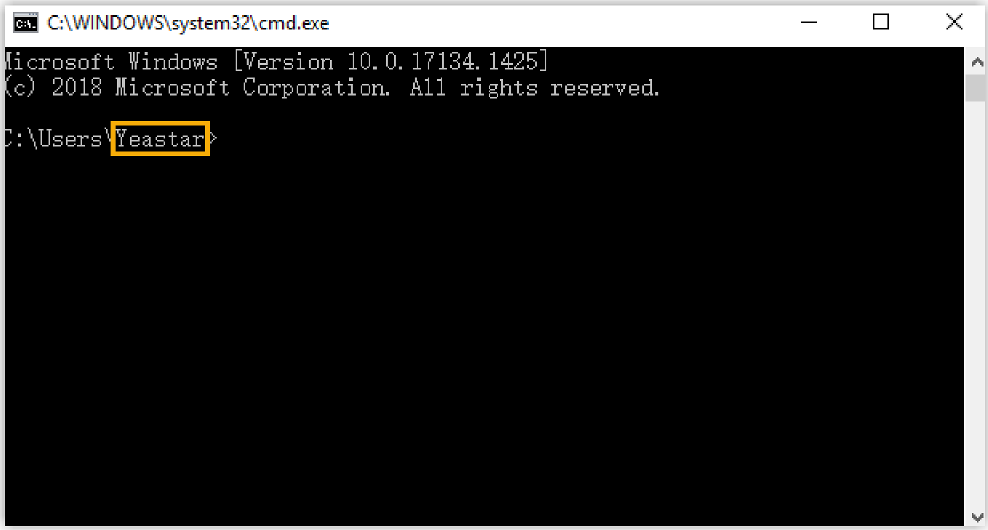
Network Drive FAQ

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.


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...

b. Enter `cmd` and click OK.

The user name is displayed on the Command Prompt.

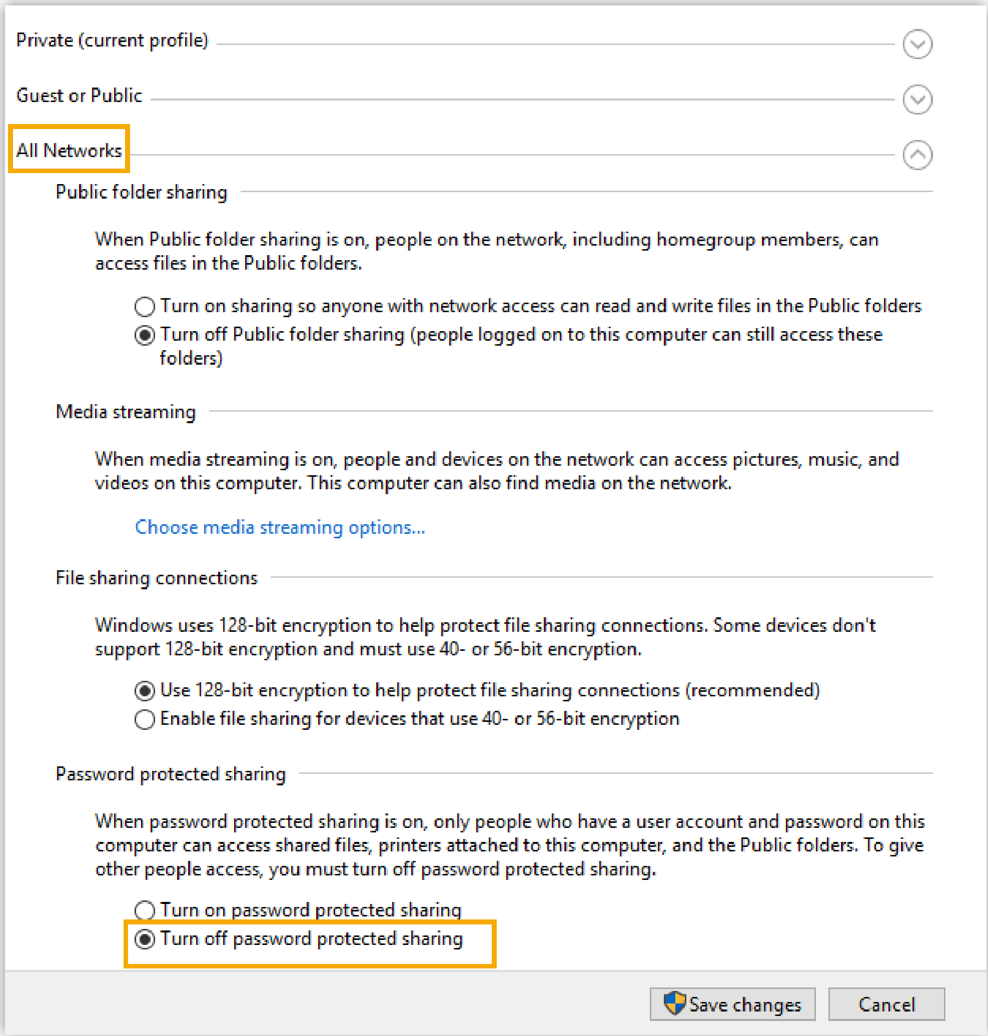


```
Microsoft Windows [Version 10.0.17134.1425]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Yeastar>
```

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.



Private (current profile)

Guest or Public

All Networks

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders.

○ Turn on sharing so anyone with network access can read and write files in the Public folders

● Turn off Public folder sharing (people logged on to this computer can still access these folders)

Media streaming

When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.

Choose media streaming options...

File sharing connections

Windows uses 128-bit encryption to help protect file sharing connections. Some devices don't support 128-bit encryption and must use 40- or 56-bit encryption.

● Use 128-bit encryption to help protect file sharing connections (recommended)

○ Enable file sharing for devices that use 40- or 56-bit encryption

Password protected sharing

When password protected sharing is on, only people who have a user account and password on this computer can access shared files, printers attached to this computer, and the Public folders. To give other people access, you must turn off password protected sharing.

○ Turn on password protected sharing

● 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 Software Edition.

Restriction

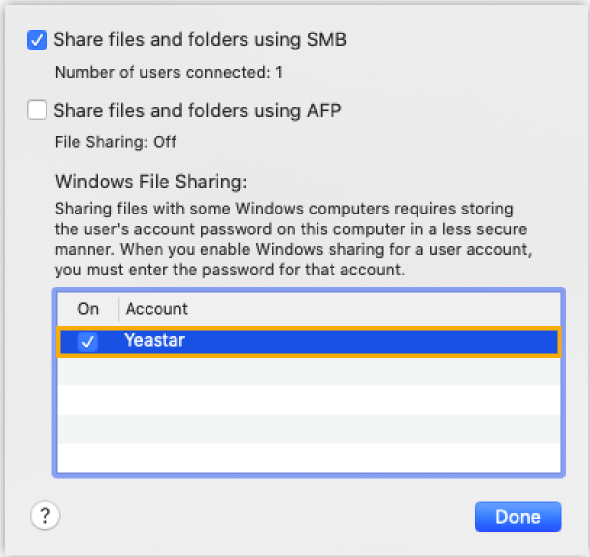
You can add up to 2 network drives.

Prerequisites

Make sure that the computer is always in service, or Yeastar P-Series Software Edition 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.



☑ Share files and folders using SMB

Number of users connected: 1

□ Share files and folders using AFP

File Sharing: Off

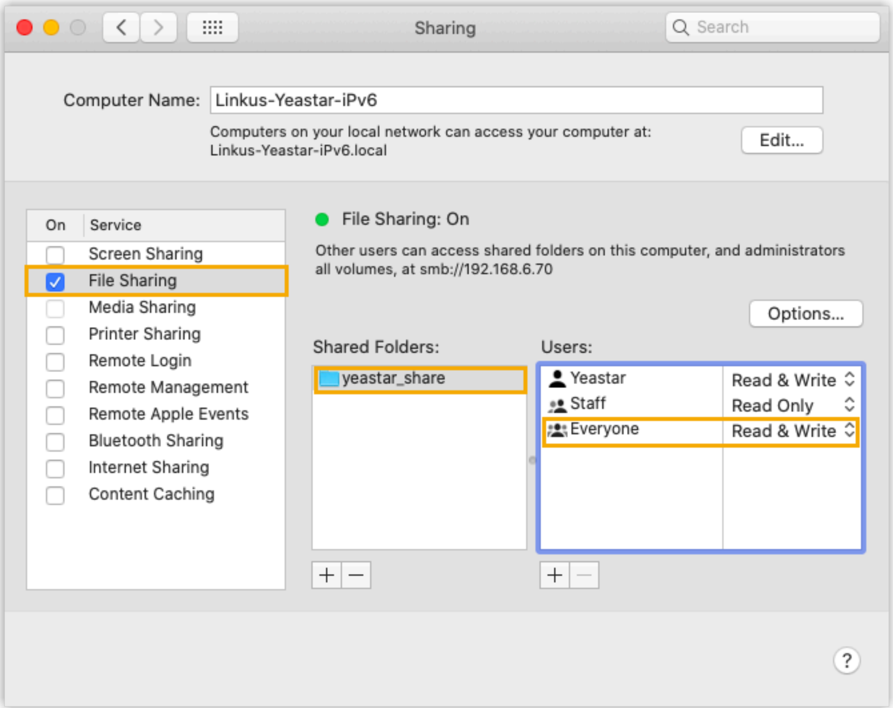
Windows File Sharing:

Sharing files with some Windows computers requires storing the user's account password on this computer in a less secure manner. When you enable Windows sharing for a user account, you must enter the password for that account.

On	Account
☑	Yeastar

      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.



Computer Name: Linkus-Yeastar-iPv6

Computers on your local network can access your computer at:
Linkus-Yeastar-iPv6.local

On	Service
□	Screen Sharing
☑	File Sharing
□	Media Sharing
□	Printer Sharing
□	Remote Login
□	Remote Management
□	Remote Apple Events
□	Bluetooth Sharing
□	Internet Sharing
□	Content Caching

● File Sharing: On

Other users can access shared folders on this computer, and administrators all volumes, at smb://192.168.6.70

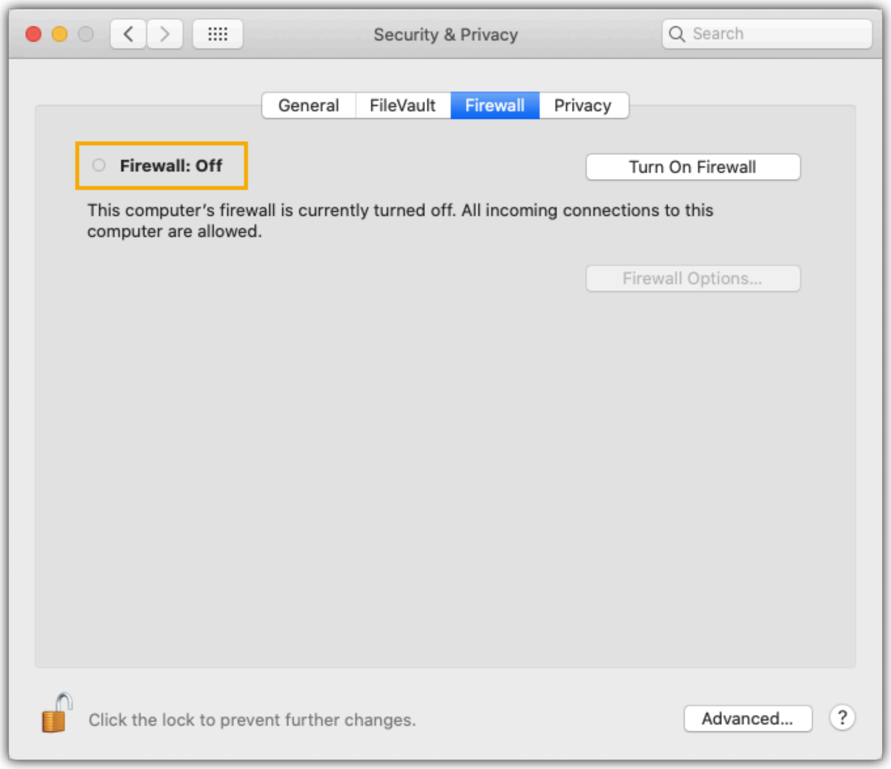
Shared Folders: yeastar_share

Users:	
Yeastar	Read & Write
Staff	Read Only
Everyone	Read & Write

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.



○ Firewall: Off

This computer's firewall is currently turned off. All incoming connections to this computer are allowed.

Click the lock to prevent further changes.

Step3. Mount the shared folder to PBX

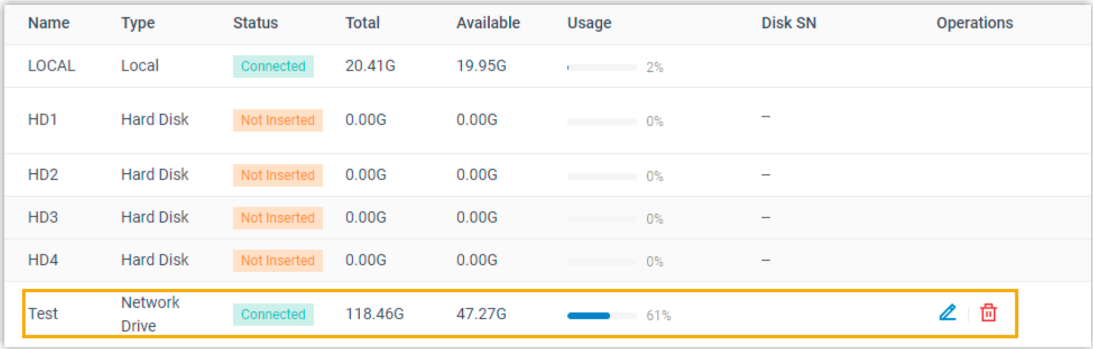
1. Log in to PBX web portal, go to System > Storage > Storage Locations.
2. In the Storage Devices section, click Add Network Drive.
3. In the pop-up window, configure the following settings.
   - Name: Specify a name to help you identify the network drive.
   - Host/IP: Enter the IP address of the Mac.
   - 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



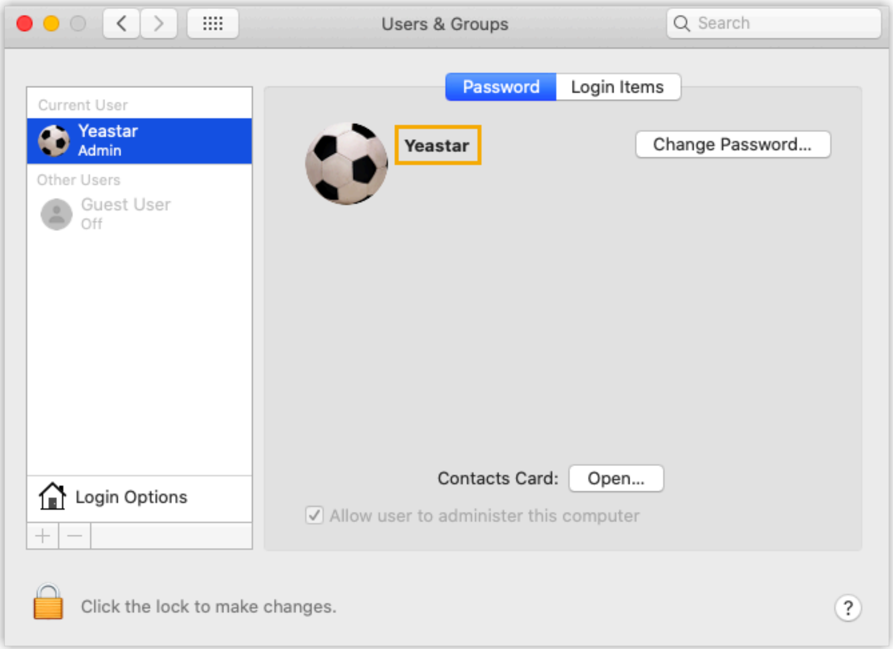
Name	Type	Status	Total	Available	Usage	Disk SN	Operations
LOCAL	Local	Connected	20.41G	19.95G	2%		
HD1	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
HD2	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
HD3	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
HD4	Hard Disk	Not Inserted	0.00G	0.00G	0%	–	
Test	Network Drive	Connected	118.46G	47.27G	61%		✎ 🗑

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.



☑ Allow user to administer this computer

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 Hard Disk Drive
    - 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.
3. Click Save.

Result

New data will be stored on the specified location.

What to do next

Set the maximum number and preservation days that data can be stored. For more information, see Auto Cleanup Settings.

Auto Cleanup Settings

Auto Cleanup feature automatically and periodically cleans up your CDR, voicemails, recording files, backup files, and logs (including event logs, email sent logs, operation logs, and system logs). This topic describes relevant configuration parameters of auto cleanup.

CDR Auto Cleanup

Table 53.

Setting	Description
Max Number of CDR	Set the maximum number of CDR that should be retained.

Table 53. (continued)

Setting	Description
	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 (extensions <1000) • 1,000,000 (extensions ≥1000) Maximum value: • 1,000,000 (extensions <1000) • 10,000,000 (extensions ≥1000)
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

Table 54.

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

Table 54. (continued)

Setting	Description
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

Table 55.

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: 90%
Recordings Preservation Days	Set the maximum number of days that recording files 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 recording files will be deleted. Default value: 0, which means no limit.

System Backup Files

Table 56.

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

Table 57.

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. 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

Table 58.

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

Table 59.

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

Table 60.

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 (extensions <1000) • 100 (extensions ≥1000)
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 Software Edition 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.
3. Select the checkbox of Access Files via FTP.

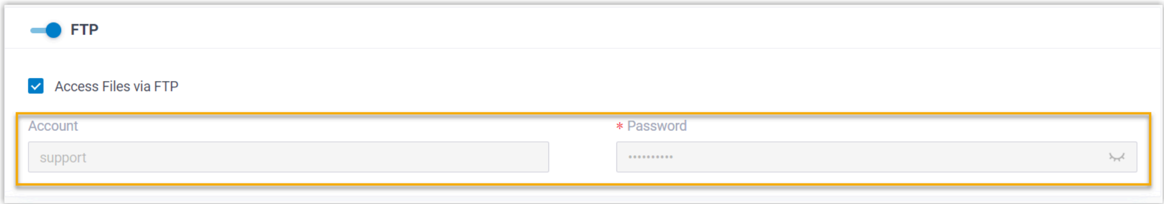
Note:

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.



FTP

☑ Access Files via FTP

Account: support

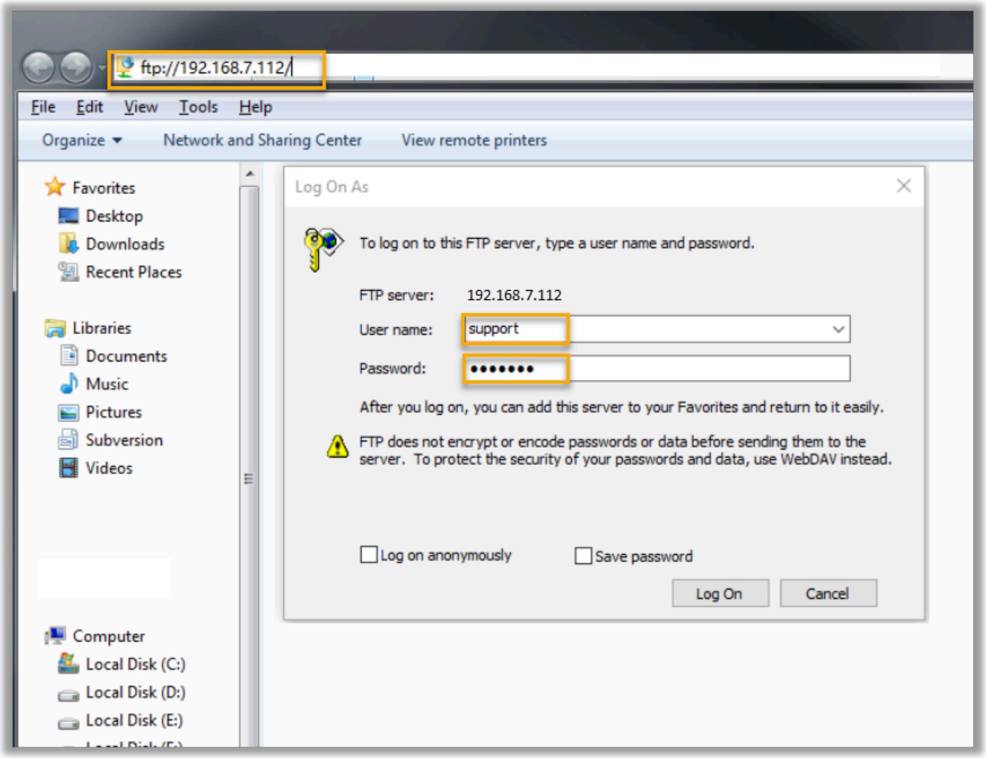
* Password: ••••••••••

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.



Log On As

To log on to this FTP server, type a user name and password.

FTP server: 192.168.7.112

User name: support

Password: •••••••

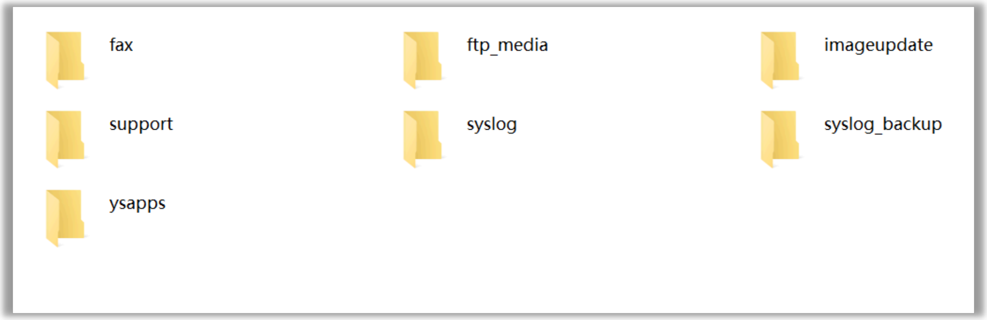
After you log on, you can add this server to your Favorites and return to it easily.

FTP does not encrypt or encode passwords or data before sending them to the server. To protect the security of your passwords and data, use WebDAV instead.

□ Log on anonymously □ Save password

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.



fax ftp_media imageupdate
support syslog syslog_backup
ysapps

4. Optional: Enter the folder `ftp_media` to check the files stored in PBX external storage.

   If you have connected a hard disk drive to the PBX, there will be a subfolder harddisk for the files stored in the hard disk.

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 Software Edition supports a file sharing feature, which allows you to access and share files that are stored in external storage devices (hard disk) 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

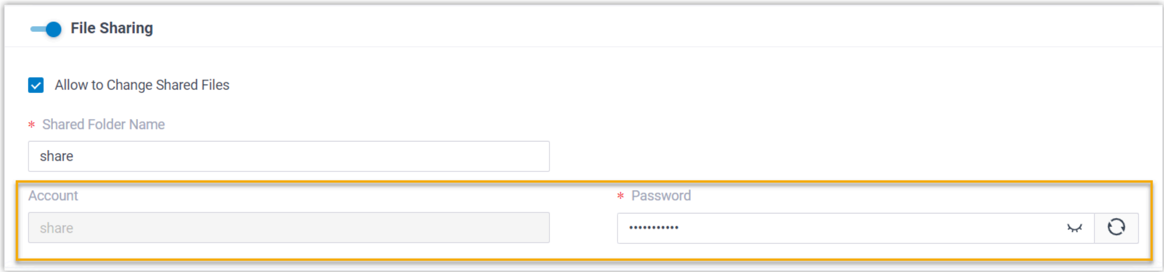
Step2. Access the shared files on PC

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.
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.



File Sharing

☑ Allow to Change Shared Files

* Shared Folder Name: share

Account: share

* Password: ••••••••••••

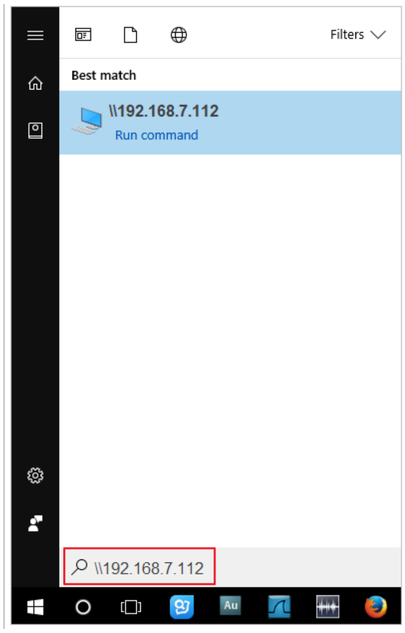
- Account: `share`.

> 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.

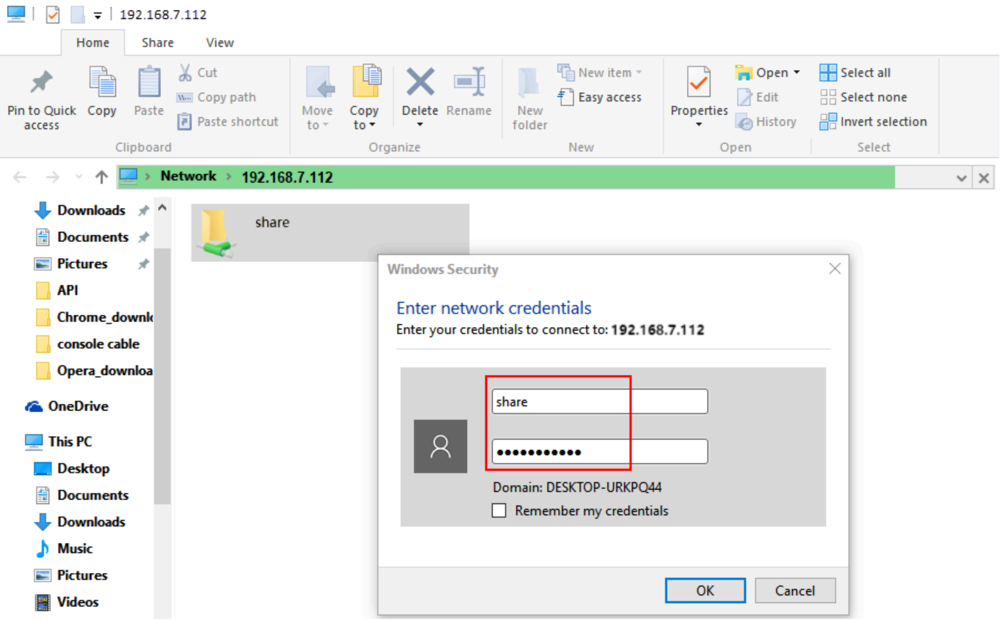
Step2. Access the shared files on PC

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.



Windows Security

Enter network credentials

Enter your credentials to connect to: 192.168.7.112

share

•••••••••••

Domain: DESKTOP-URKPQ44

□ Remember my credentials

a. Enter the user name and password.
   - User name: Enter `share`.
   - Password: Enter the password.

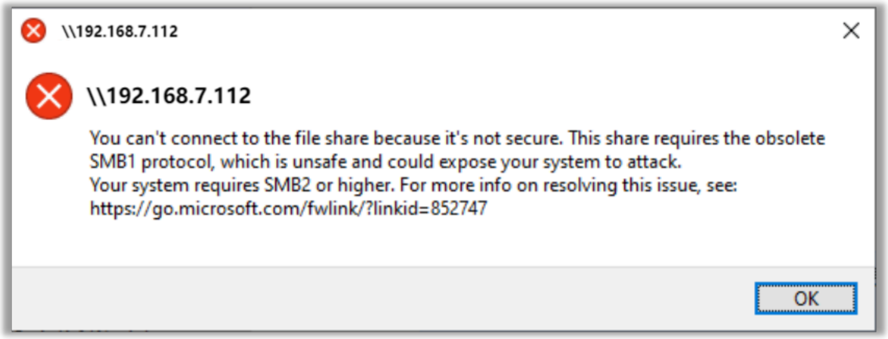
b. Click OK.

   You can now access the shared folder. If you have connected a hard disk drive to the PBX, there will be a subfolder harddisk for the files stored in the hard disk.

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.

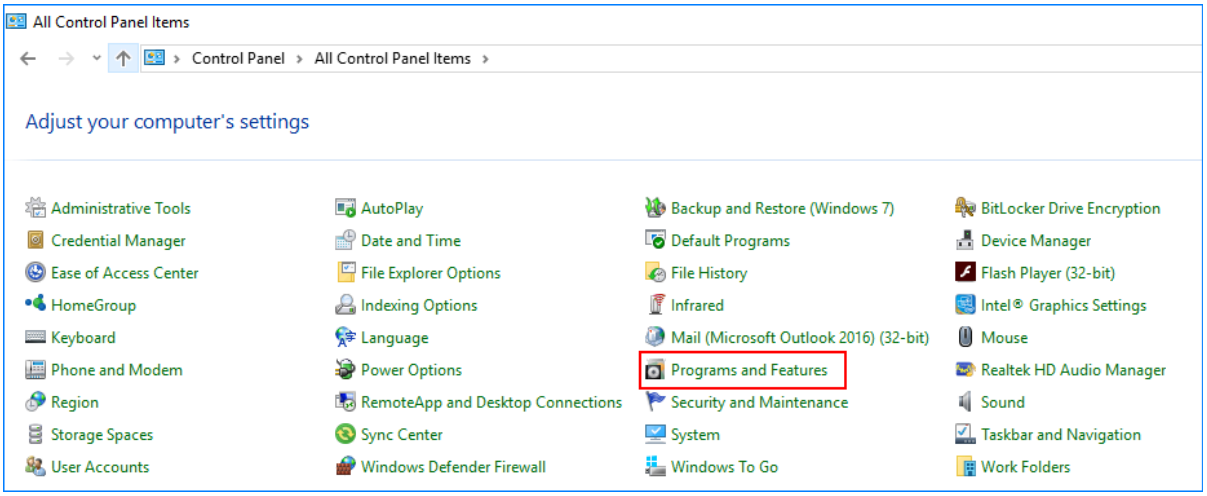


\\192.168.7.112

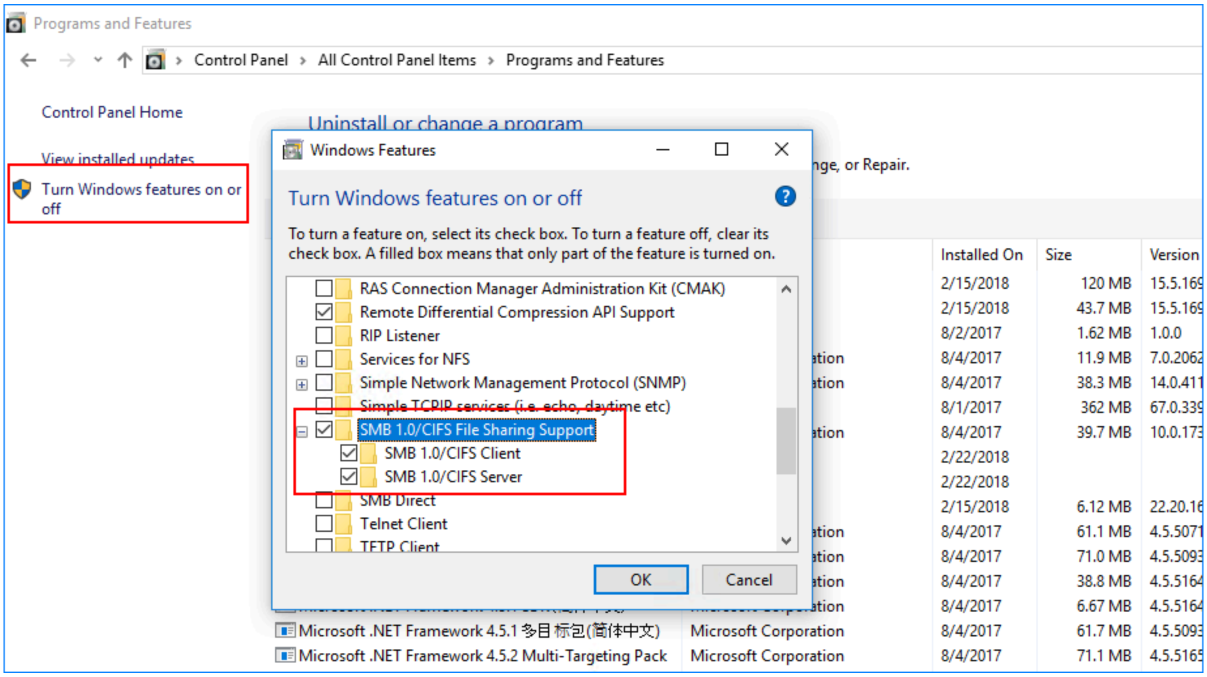
\\192.168.7.112

You can't connect to the file share because it's not secure. This share requires the obsolete SMB1 protocol, which is unsafe and could expose your system to attack.
Your system requires SMB2 or higher. For more info on resolving this issue, see:
https://go.microsoft.com/fwlink/?linkid=852747

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.


Programs and Features
Control Panel > All Control Panel Items > Programs and Features
Control Panel Home
View installed updates
Turn Windows features on or off
Uninstall or change a program
nge, or Repair.
Windows Features
OK
Cancel

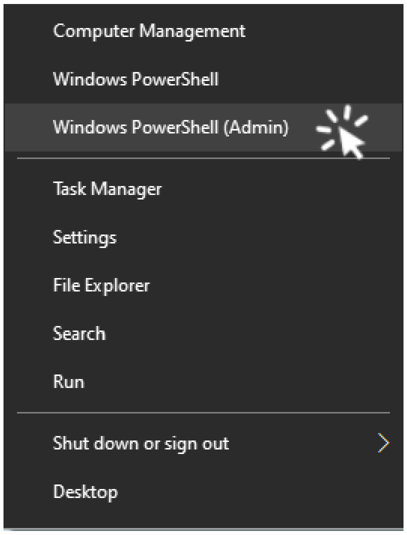
Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

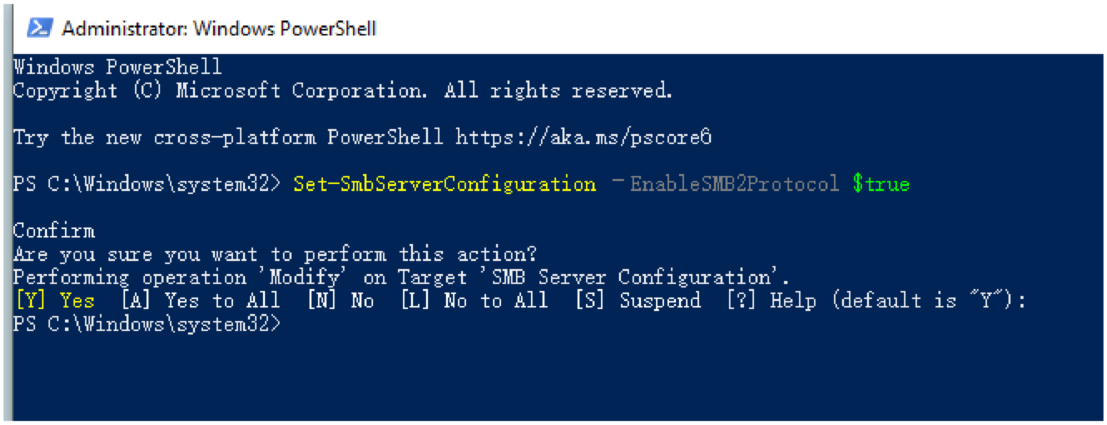
- ☐ RAS Connection Manager Administration Kit (CMAK)
- ☑ Remote Differential Compression API Support
- ☐ RIP Listener
- ☐ Services for NFS
- ☐ Simple Network Management Protocol (SNMP)
- ☐ Simple TCPIP services (i.e. echo, daytime etc)
- ☑ SMB 1.0/CIFS File Sharing Support
  - ☑ SMB 1.0/CIFS Client
  - ☑ SMB 1.0/CIFS Server
- ☐ SMB Direct
- ☐ Telnet Client
- ☐ TFTP Client

		Installed On	Size	Version
		2/15/2018	120 MB	15.5.169
		2/15/2018	43.7 MB	15.5.169
		8/2/2017	1.62 MB	1.0.0
	ation	8/4/2017	11.9 MB	7.0.2062
	ation	8/4/2017	38.3 MB	14.0.411
		8/1/2017	362 MB	67.0.339
	ation	8/4/2017	39.7 MB	10.0.173
		2/22/2018		
		2/22/2018		
		2/15/2018	6.12 MB	22.20.16
	ation	8/4/2017	61.1 MB	4.5.5071
	ation	8/4/2017	71.0 MB	4.5.5093
	ation	8/4/2017	38.8 MB	4.5.5164
	ation	8/4/2017	6.67 MB	4.5.5164
Microsoft .NET Framework 4.5.1 多目标包(简体中文)	Microsoft Corporation	8/4/2017	61.7 MB	4.5.5093
Microsoft .NET Framework 4.5.2 Multi-Targeting Pack	Microsoft Corporation	8/4/2017	71.1 MB	4.5.5165

4. Press Win + X, and select Windows Powershell(Admin).



5. In the pop-up window, enter `Set-SmbServerConfiguration –EnableSMB2Protocol $true`, and press Enter.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Set-SmbServerConfiguration -EnableSMB2Protocol $true

Confirm
Are you sure you want to perform this action?
Performing operation 'Modify' on Target 'SMB Server Configuration'.
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
PS C:\Windows\system32>
```

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 Software Edition can work as a TFTP server, you can upload or download desired files to/from a specific PBX file folder (/ysdisk/tftpboot) 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.
3. Click Save.

Result

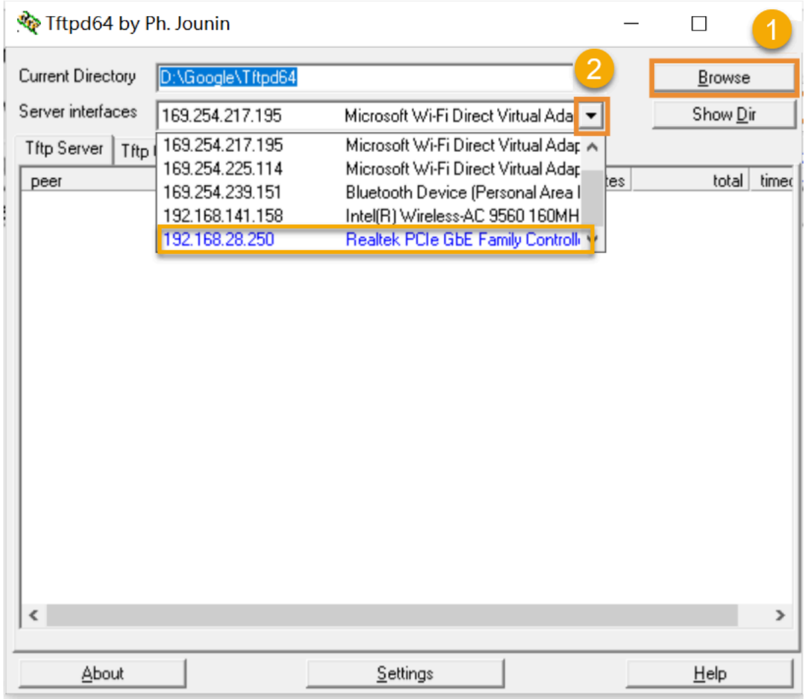
The PBX can now be used as a TFTP server, you can upload or download desired files to/ from the specific PBX file folder.

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.



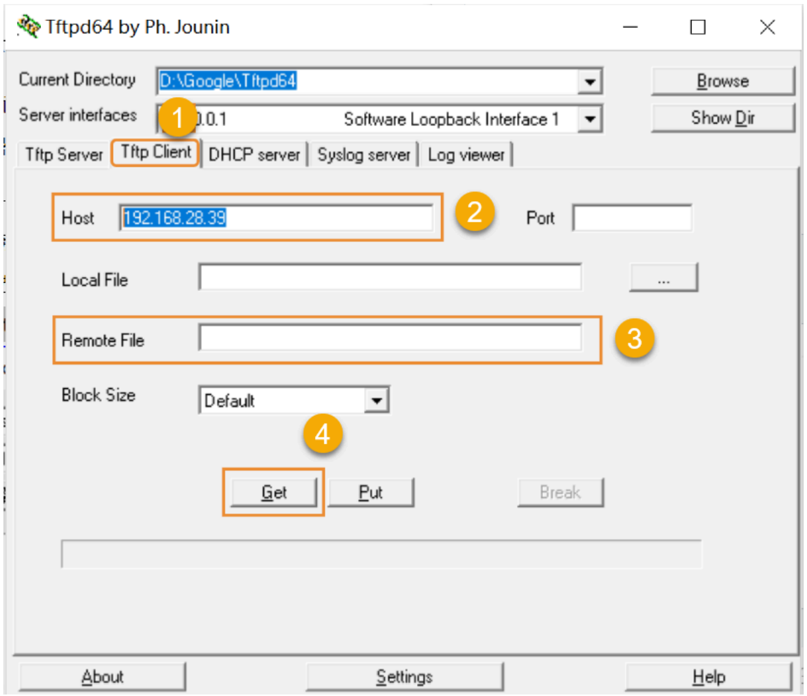
Current Directory D:\Google\Tftpd64

Server interfaces 169.254.217.195 Microsoft Wi-Fi Direct Virtual Ada

169.254.217.195	Microsoft Wi-Fi Direct Virtual Adap
169.254.225.114	Microsoft Wi-Fi Direct Virtual Adap
169.254.239.151	Bluetooth Device (Personal Area I
192.168.141.158	Intel(R) Wireless-AC 9560 160MH
192.168.28.250	Realtek PCIe GbE Family Controll

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.



Current Directory D:\Google\Tftpd64

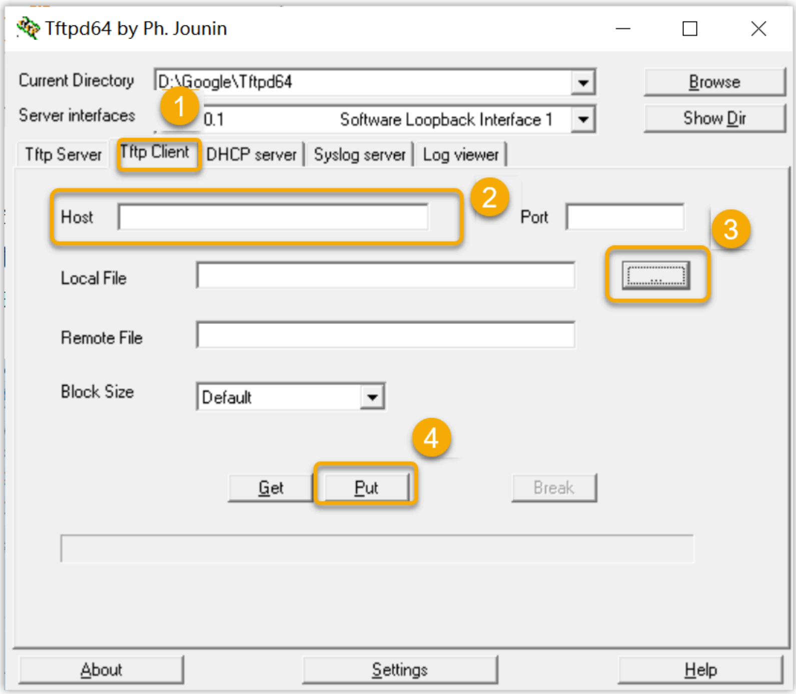
Server interfaces 0.0.1 Software Loopback Interface 1

Host 192.168.28.39

Block Size Default

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.



Event Notification

Event Notification Overview

Event Notification feature is designed to provide information about changes on Yeastar P-Series Software Edition 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 Software Edition supports the following event types:

- Operations
- Telephony
- System
- Security
- Reminder

Table 61. 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.
PBX Hot Standby Failover	A PBX failover has occurred, and the PBX system is taken over by the other server.
Secondary Server Takeover (For Only 30 Days)	The Primary Server was down and the Secondary Server has taken over the PBX system. The Secondary Server will take over the system for only 30 days.
Secondary Server Will Expire Soon	The Secondary Server that is taking over the PBX system is going to expire.
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.
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.

Table 62. 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 63. System

Event	Description
CPU Overload	CPU ran over 90% in 10s.
Memory Overload	Memory ran over 90% in 10s.
Storage Device Failure	Failed to write data to storage device.
Insufficient Storage	The storage ran out of 90%.
Lost Connectivity to Storage Device	Lost connection to storage device.
Auto Cleanup Reminder	Reach 90% of the allowed storage limit.
New System Firmware Detected	The PBX automatically detected a new firmware version.
System Upgrade Completed	The PBX was upgraded.
System Reboot	Either of the following situations triggered the event: • The PBX rebooted after configuration. • The PBX automatically rebooted after system crash.
System Restore	The PBX was restored.
Yeastar SMTP Server Error	Yeastar SMTP server failed to send emails.
Abnormal License Activation	Failed to connect to extranet License Activation Server.

Table 64. Security

Event	Description
Web User Locked Out	PBX blocked the source IP when either of the following situations was met:

Table 64. Security (continued)

Event	Description
	• 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: • 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.

Table 65. Reminder

Event	Description
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.
License Expiration Reminder	The current license will expire soon.

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 Software Edition 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 Software Edition 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.

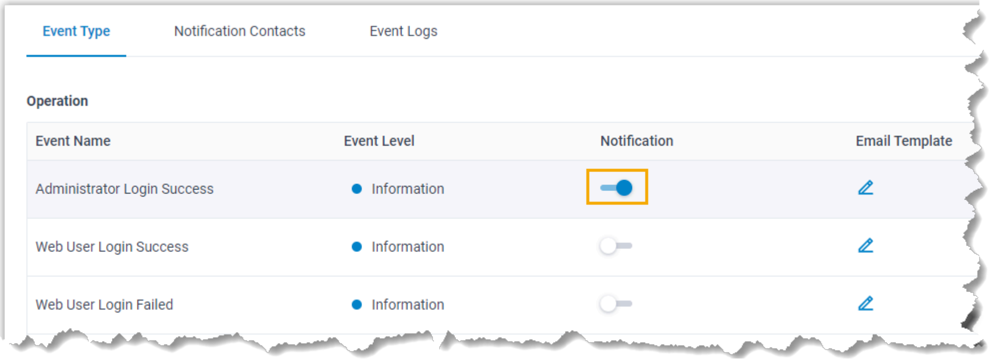
Configure Event Notifications

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.



Operation

Event Name	Event Level	Notification	Email Template
Administrator Login Success	● Information	●	✎
Web User Login Success	● Information	○	✎
Web User Login Failed	● Information	○	✎

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.

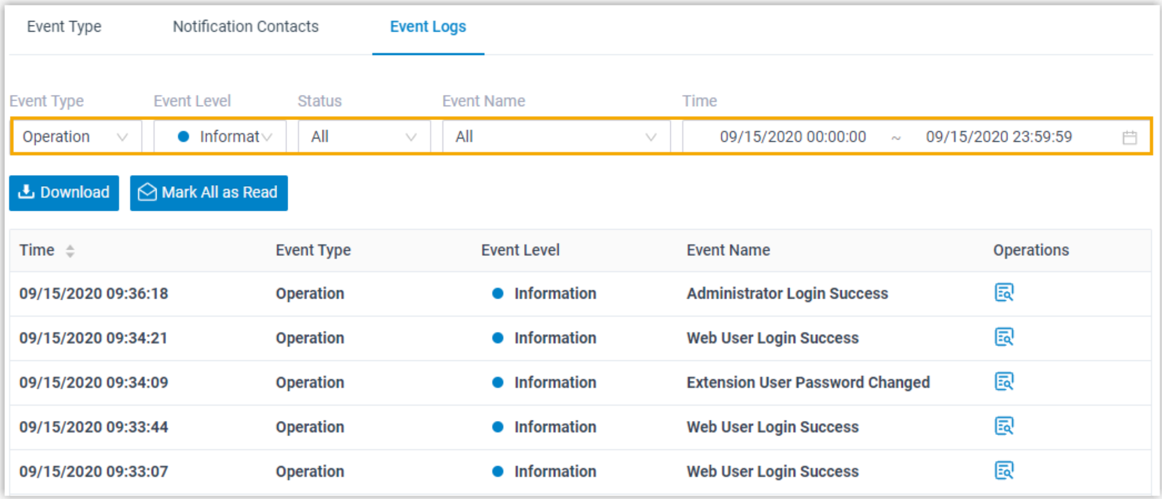
The contacts are removed from the list, and will not receive notifications when events occur.

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 | Notification Contacts | Event Logs

Event Type	Event Level	Status	Event Name	Time
Operation	● Informat	All	All	09/15/2020 00:00:00 ~ 09/15/2020 23:59:59

Download | Mark All as Read

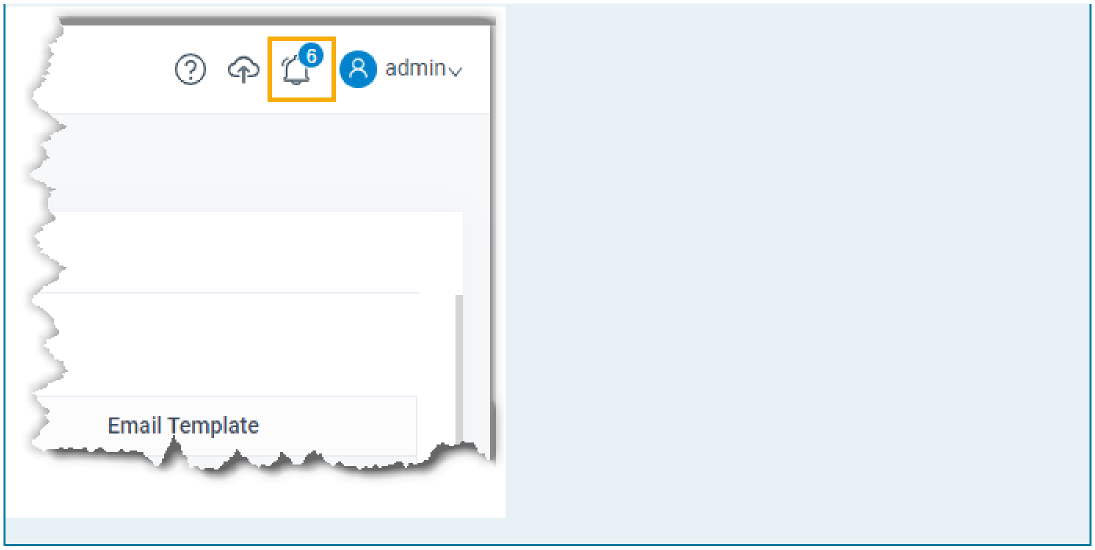
Time	Event Type	Event Level	Event Name	Operations
09/15/2020 09:36:18	Operation	● Information	Administrator Login Success	🔍
09/15/2020 09:34:21	Operation	● Information	Web User Login Success	🔍
09/15/2020 09:34:09	Operation	● Information	Extension User Password Changed	🔍
09/15/2020 09:33:44	Operation	● Information	Web User Login Success	🔍
09/15/2020 09:33:07	Operation	● Information	Web User Login Success	🔍

   - Event Type: Search all the event logs or search logs by a specific event type.
   - Event Level: Search all the event logs or search logs by a specific event level.
   - Status: Search all the event logs or search logs by a specific acknowledgement status.
   - Event Name: Search all the event logs or search a specific event.
   - Time: Set the start date and end date of the events.

   The matched events are displayed on the page.
3. Handle the searched events according to your needs.
   - To check log details, click 🔍 beside the desired event log.

     The event log will be marked as read.
   - To download all the searched logs, click Download.
   - To mark all the searched logs as read, click Mark All as Read.

> Note:
> At the top right corner, the number of unread events of the event level prompted on ⏰ will be cleared.



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 Software Edition to Yeastar Central Management Using Authentication Code
Device provider is responsible for routine maintenance of PBX system	Connect Yeastar P-Series Software Edition 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 Software Edition to Yeastar Central Management Using Authentication Code

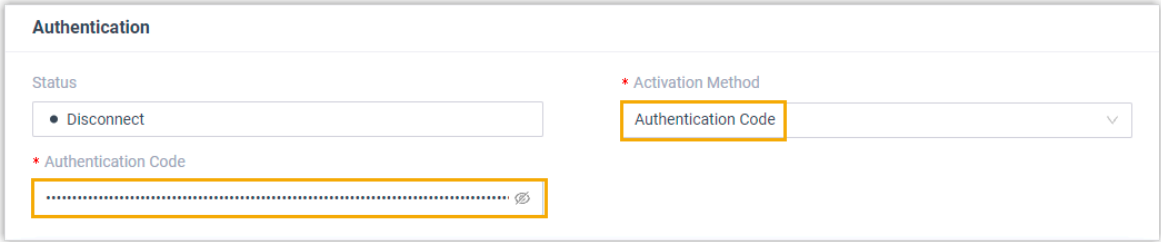
If you have in-house IT staff for routine maintenance of your PBX system, but the IT staff has difficulty handling specific system errors, you can connect PBX to Yeastar Central Management using an authentication code. In this way, device provider can help you troubleshoot issues.

Prerequisites

Make sure the version of your PBX system is 83.5.0.86 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:



Authentication

Status: ● Disconnect

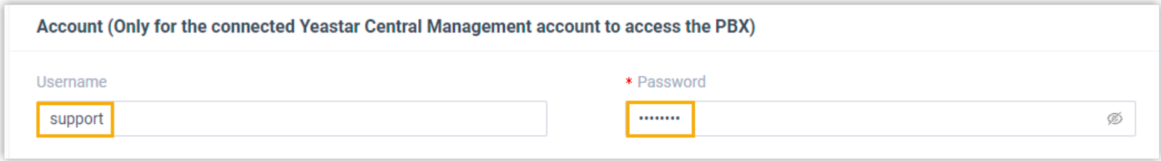
* Activation Method: Authentication Code

* Authentication Code: ••

   - 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 management 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.



Account (Only for the connected Yeastar Central Management account to access the PBX)

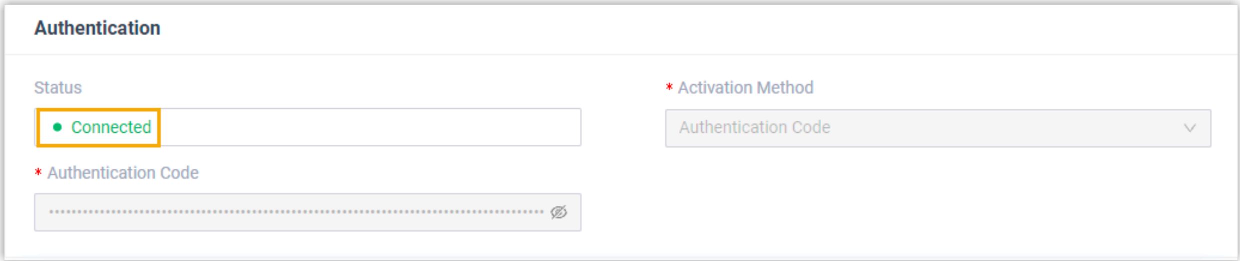
Username: support

* Password: ••••••••

5. Click Save.

Result

The status is displayed as Connected, which indicates that your PBX system is connected to Yeastar Central Management.



Authentication

Status: ● Connected

* Activation Method: Authentication Code

* Authentication Code: ••

Related information

[Connect Yeastar P-Series Software Edition to Yeastar Central Management Using Yeastar ID](#)
[Disconnect Yeastar P-Series Software Edition with Yeastar Central Management](#)

Connect Yeastar P-Series Software Edition 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.

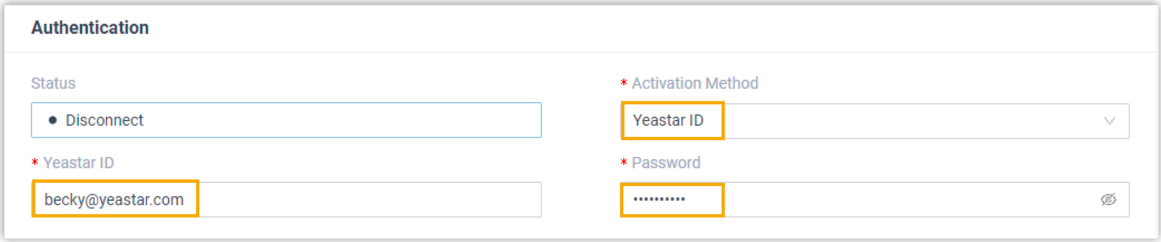
Prerequisites

Make sure the version of your PBX system is 83.5.0.86 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:



Authentication

Status: ● Disconnect

* Activation Method: Yeastar ID

* Yeastar ID: becky@yeastar.com

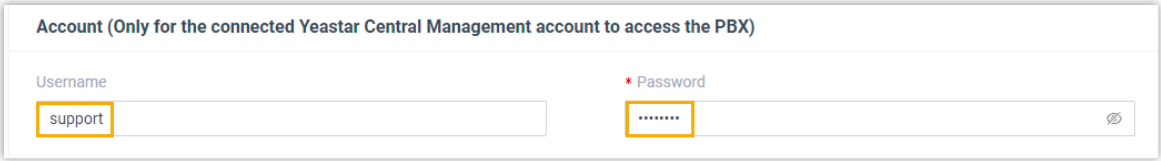
* Password: ••••••••••

- 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.

   Account (Only for the connected Yeastar Central Management account to access the PBX)

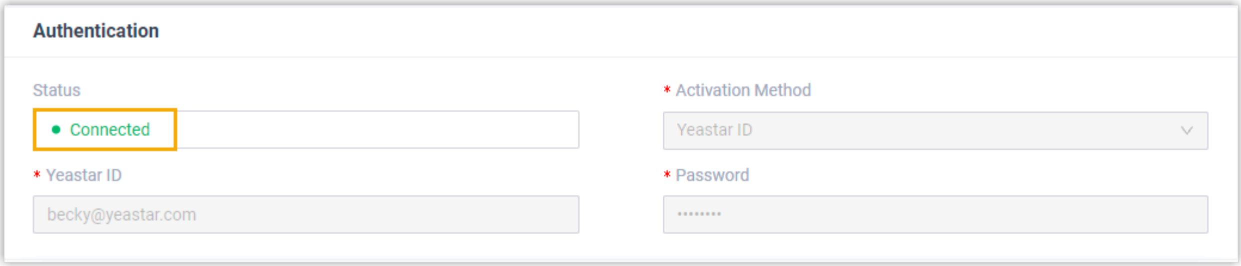
   Username: support

   * Password: ••••••••

4. Click Save.

Result

The status is displayed as Connected, which indicates that your PBX system is connected to Yeastar Central Management.



Authentication

Status: ● Connected

* Activation Method: Yeastar ID

* Yeastar ID: becky@yeastar.com

* Password: ••••••••

Related information

[Connect Yeastar P-Series Software Edition to Yeastar Central Management Using Authentication Code]

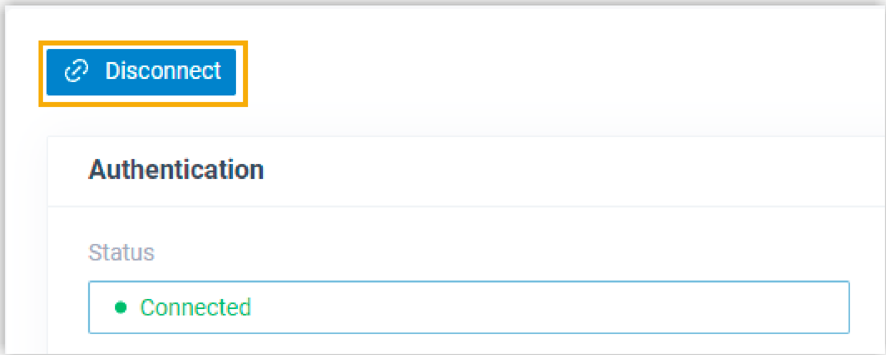
[Disconnect Yeastar P-Series Software Edition with Yeastar Central Management]

Disconnect Yeastar P-Series Software Edition 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.



Authentication

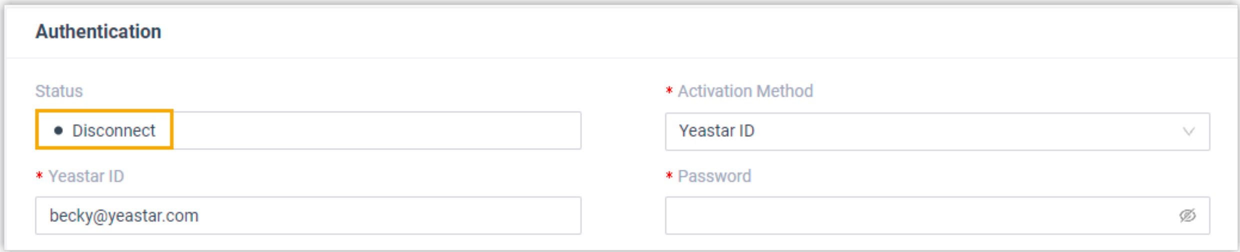
Status

● Connected

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.



Authentication

Status ● Disconnect	* Activation Method Yeastar ID
* Yeastar ID becky@yeastar.com	* Password

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.

Restriction

- PBX firmware: 83.6.0.24 or the later version
- Yeastar P-Series Software Edition 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).

- Hot Standby doesn't work in VPN network.

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 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.

Hot Standby status

The following table lists the Hot Standby status of the servers.

Table 66.

Status	Description
Running	The server is running.
Standby	The server is in standby mode now, and you can't not make any configuration changes on the server.
Abnormal	The server is down, and the Secondary Server has taken over the PBX system.

Related information

Set up Hot Standby Pair
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 services, thus minimizing downtime and data loss.

Restriction

- PBX firmware: 83.6.0.24 or the later version
- Yeastar P-Series Software Edition 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).

- Hot Standby doesn't work in VPN network.

Prerequisites

The Primary Server and Secondary Server in the failover pair must meet the following requirements:

Item	Requirement
Plan	The two PBXs have subscribed the same plan.
Serial Number (SN)	The SN of the secondary PBX server should be associated with the primary PBX server's. Note: To confirm this, contact your device provider.
System Capacity	The two PBXs have the same system capacity, including the number of extensions and concurrent calls.
Firmware	The firmware version of the two PBXs are the same.
IP address	The two PBXs both have static IP addresses.

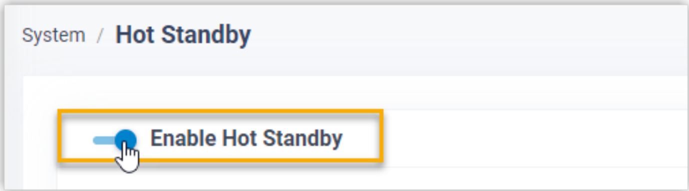
Scenarios

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

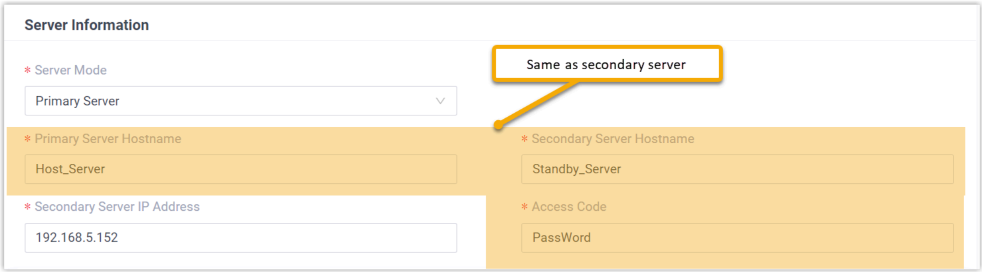
1. Log in to PBX web portal, go to System > Hot Standby.
2. On the top of the page, turn on the Enable Hot Standby switch.



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.



Server Information

* Server Mode: Primary Server

* Primary Server Hostname: Host_Server

* Secondary Server Hostname: Standby_Server

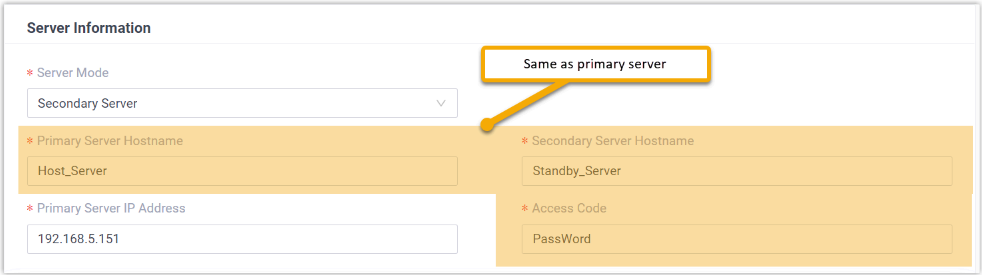
* Secondary Server IP Address: 192.168.5.152

* Access Code: PassWord

Same as secondary server

Set up Secondary Server

In the Hot Standby configuration page of the Secondary Server, complete the following settings.



Server Information

* Server Mode: Secondary Server

* Primary Server Hostname: Host_Server

* Secondary Server Hostname: Standby_Server

* Primary Server IP Address: 192.168.5.151

* Access Code: PassWord

Same as primary server

Settings

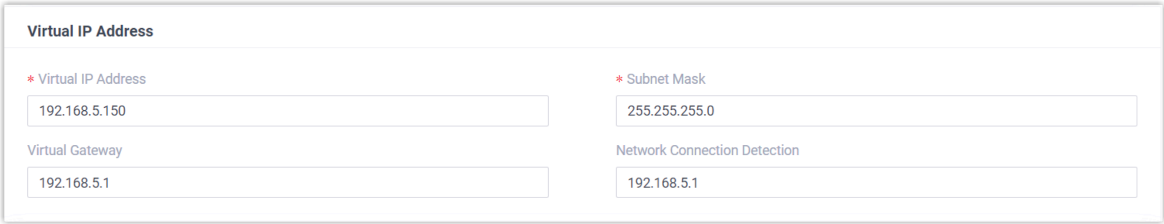
The detailed description of the settings are listed in the following table.

Table 67.

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`.

Setting	Description
	Note: The Secondary Server Hostname set in the Primary Server and Secondary 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.



Virtual IP Address

* Virtual IP Address: 192.168.5.150

* Subnet Mask: 255.255.255.0

Virtual Gateway: 192.168.5.1

Network Connection Detection: 192.168.5.1

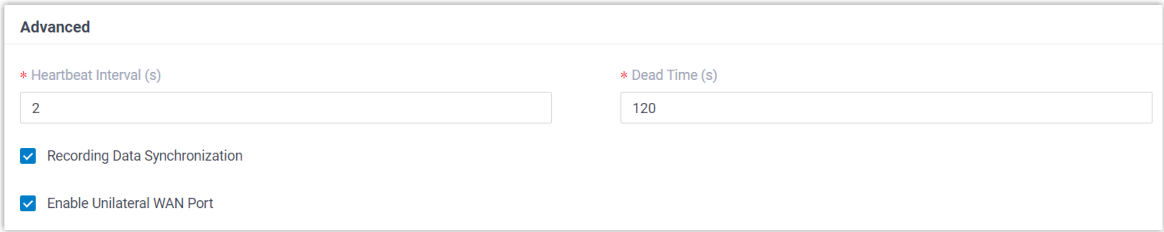
Note:
When you enter a virtual IP address, the corresponding information of Subnet Mask, Virtual Gateway and Network Connection Detection is automatically filled in.

Table 68.

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.

Setting	Description
	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 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.



Advanced

* Heartbeat Interval (s): 2

* Dead Time (s): 120

☑ Recording Data Synchronization

☑ Enable Unilateral WAN Port

Table 69.

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 de-

Setting	Description
	tect 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.
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.

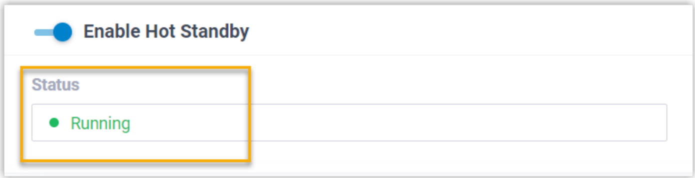
6. Click Save.

   The system prompts that you need to reboot the server to make Hot Standby take effect.

Result

Primary Server

- After the PBX is rebooted, the Status displays Running.



Enable Hot Standby

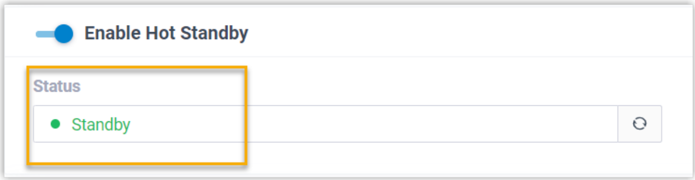
Status

● 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.

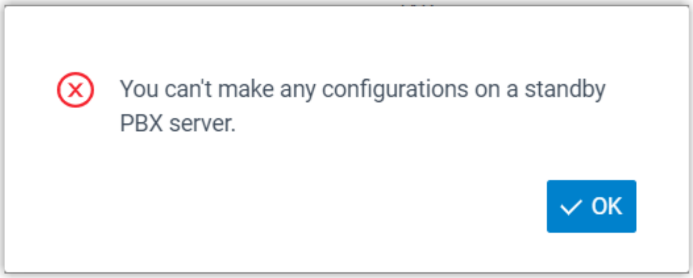


Enable Hot Standby

Status

● Standby

- When you try to make configuration on the Secondary Server, the system prompts "You can't make any configurations on a standby server".



You can't make any configurations on a standby PBX 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.

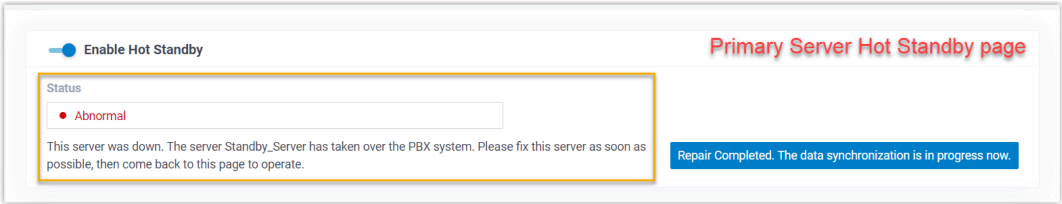
Background information

When the Primary Server fails, the Secondary Server will automatically take over the services, 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.


Enable Hot Standby
Repair Completed. The data synchronization is in progress now.

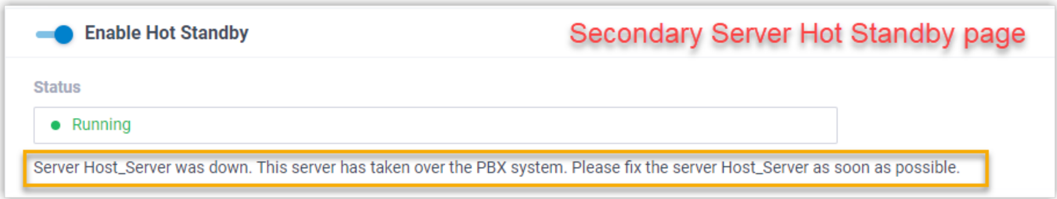
Primary Server Hot Standby page

Status: ● Abnormal

This server was down. The server Standby_Server has taken over the PBX system. Please fix this server as soon as possible, then come back to this page to operate.

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.



Secondary Server Hot Standby page

Status: ● Running

Server Host_Server was down. This server has taken over the PBX system. Please fix the server Host_Server as soon as possible.

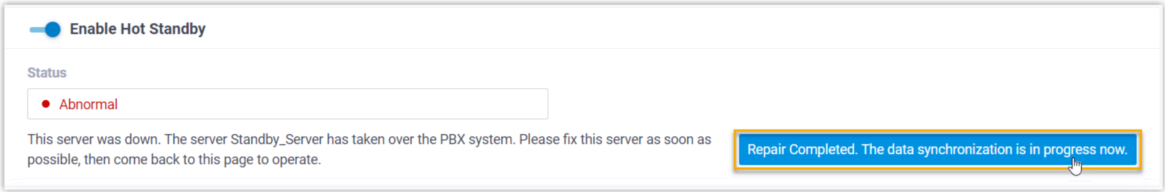
After you have repaired the Primary Server, you need to manually set up the Primary Server to take over the system from Secondary Server.

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.


Enable Hot Standby
Repair Completed. The data synchronization is in progress now.

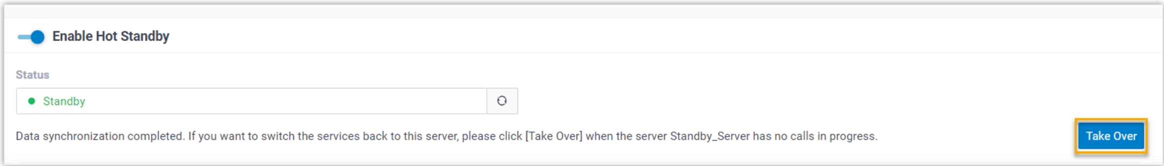
Status: ● Abnormal

This server was down. The server Standby_Server has taken over the PBX system. Please fix this server as soon as possible, then come back to this page to operate.

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.



Enable Hot Standby

Status

● Standby

Data synchronization completed. If you want to switch the services back to this server, please click [Take Over] when the server Standby_Server has no calls in progress.

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.

Security

Security Overview

Yeastar P-Series Software Edition provides robust security options to ensure a secure and reliable phone service to your business operation, such as static defense rules, auto defense rules, IP blocking and so on.

Static defense

Static defense rules are used to control and filter traffic sent to the PBX by IP address, domain, or MAC address.

Yeastar P-Series Software Edition has default static defense rules to ensure the communication among Yeastar server, Yeastar P-Series Software Edition, and devices in your local network.

By default, the PBX always accepts connections from the following addresses:

- Local network
    - 10.0.0.0/255.0.0.0
    - 172.16.0.0/255.240.0.0
    - 192.168.0.0/255.255.0.0
    - 169.254.0.0/255.255.0.0

    > Note:
    >
    > These rules can NOT be edited or deleted.
- Domain related with Yeastar
    - update.yeastar.com
    - rmtunnel.yeastar.com
    - ctltunnel.yeastar.com
    - tunnel.yeastar.com
    - appcenter.yeastar.com
    - mail.pbxsmtp.com
    - active.yeastar.com
- IP address of phones that have been auto provisioned

You can also set up new rules to accept, drop, or reject access to the PBX. The IP address that was denied access to the PBX would be blocked when trying to connect to the PBX. You can check the blocked IP address in Block IPs.

For more information, see Add a Static Defense Rule and Manage Blocked IP Addresses.

Auto defense

Auto defense rules are used to prevent massive connection attempts or brute force attacks. When a source address sends packets over the limit within the specified time period, the PBX will block the source address. You can check the blocked IP address in Block IPs.

Yeastar P-Series Software Edition has default auto defense rules as below:

Table 70.

Rule Name	Defense Object				
	Type	Port	Protocol	Number of IP Packets	Time Interval (s)
SSH	Service	8022	TCP	10	60s
SIP UDP	Service	5060	UDP	40	2s
SIP TCP	Service	5060	TCP	40	2s
HTTP	Service	80	Both	120	60s
HTTPS	Service	8088	Both	120	60s

You can also set up new rules according to your needs.

For more information, see Add an Auto Defense Rule.

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).

Console/SSH Access

Yeastar P-Series Software Edition 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 Software Edition 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.

For more information, see the following topics:

- Upload TLS certificates to the PBX
- Upload HTTPS Certificates to 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 Software Edition.

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.

Static Defense

Add a Static Defense Rule

Static defense rules are used to control and filter traffic sent to Yeastar P-Series Software Edition. 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 Software Edition 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 Software Edition 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 Software Edition. 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 Software Edition 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

Console/SSH Access

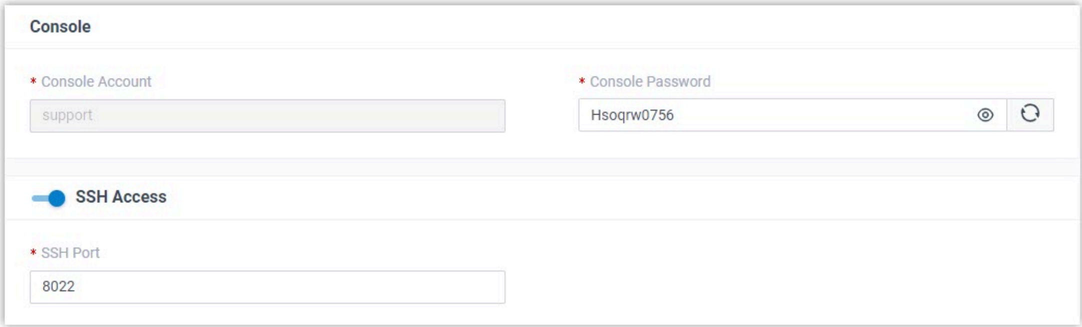
Access the System via SSH

This topic takes Putty as an example to introduce you how to access Yeastar P-Series Software Edition via SSH.

Procedure

1. Enable SSH, check SSH port, console account, and console password on the PBX.
    a. Log in to PBX web portal, go to Security > Security Settings > Console/SSH Access.
    b. Enable SSH Access.
    c. Check SSH port, console account, and console password.

    > Tip:
    >
    > Click to view the password.

    Console

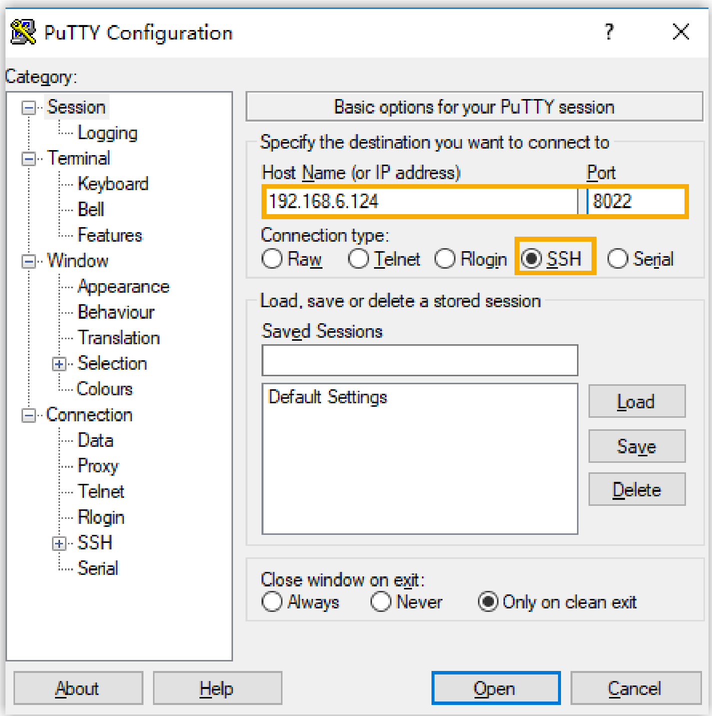
    * Console Account: support

    * Console Password: Hsoqrw0756

    SSH Access

    * SSH Port: 8022

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.



Specify the destination you want to connect to

Host Name (or IP address): 192.168.6.124

Port: 8022

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions

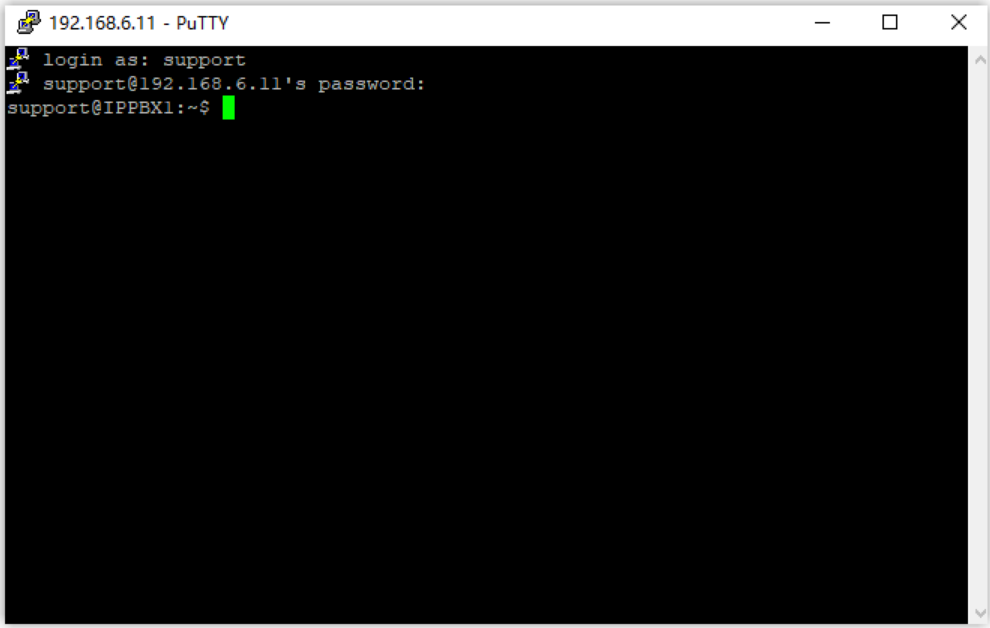
Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

3. Verify your account and password.
    a. In the login as field, enter support.
    b. Copy console password from PBX.
    c. In the password field, right click to paste the password.

Result

If the following figure shows, you can successfully access and debug the PBX.



```
login as: support
support@192.168.6.11's password:
support@IPPBX1:~$
```

Certificates

Upload TLS certificates to the PBX

Yeastar P-Series Software Edition supports TLS protocol to secure SIP messaging. Before using TLS protocol, you may need to upload a TLS certificate.

Background information

With TLS protocol enabled on the PBX, a TLS certificate may be required in the following situations:

- When the PBX acts as a server, a server certificate is required.

  If the PBX requires to verify TLS client (PBX Settings > SIP Settings > TLS > TLS Verify Client), you need to upload a client certificate to both PBX and TLS client, or the TLS connection would fail.
- When the PBX acts as a client, whether a client certificate is required depends on the server.

  If the PBX requires to verify TLS server (PBX Settings > SIP Settings > TLS > TLS Verify Server), you need to upload a server certificate.

Upload a TLS server certificate

Prerequisites

You have prepared a server certificate in `.pem` format.

Procedure

1. Log in to PBX web portal, go to Security > Security Settings > Certificates, click Upload.

   A window pops up, which requires you to select certificate type and upload a certificate.

   > Note:
   > You can ONLY upload 3 certificates.
2. In the Certificate Type drop-down list, choose PBX Certificate.
3. Click Browse to select the desired certificate.
4. Click Upload.

Result

The certificate is uploaded successfully, and is displayed on Certificates list.

Upload a TLS client certificate

Prerequisites

You have prepared a client certificate in `.cer` or `.crt` format.

Procedure

1. Log in to PBX web portal, go to Security > Security Settings > Certificates, click Upload.

   A window pops up, which requires you to select certificate type and upload a certificate.

   > Note:
   > You can ONLY upload 20 certificates.
2. In the Certificate Type drop-down list, choose Trusted Certificate.
3. Click Browse to select the desired certificate.
4. Click Upload.

Result

The certificate is uploaded successfully, and is displayed on Certificates list.

Upload HTTPS Certificates to the PBX

Yeastar P-Series Software Edition supports HTTPS protocol to secure SIP messaging when you access the PBX from web browser. Before using HTTPS protocol, you need to upload a PBX certificate.

Background information

When you access PBX from web browser, the PBX acts as a server and the web browser acts as a client. A certificate helps verify your PBX's IP address and secures your data transmission.

Prerequisites

You have prepared a server certificate in `.pem` format.

Procedure

1. Log in to PBX web portal, go to Security > Security Settings > Certificates, click Upload.

   A window pops up, which requires you to select certificate type and upload a certificate.

   > Note:
   >
   > You can ONLY upload 3 certificates.
2. In the Certificate Type drop-down list, choose PBX Certificate.
3. Click Browse to select the desired certificate.
4. Click Upload.

Result

The certificate is uploaded successfully, and is displayed on Certificates list.

Delete Certificates

This topic describes how to delete one or more certificates on Yeastar P-Series Software Edition.

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

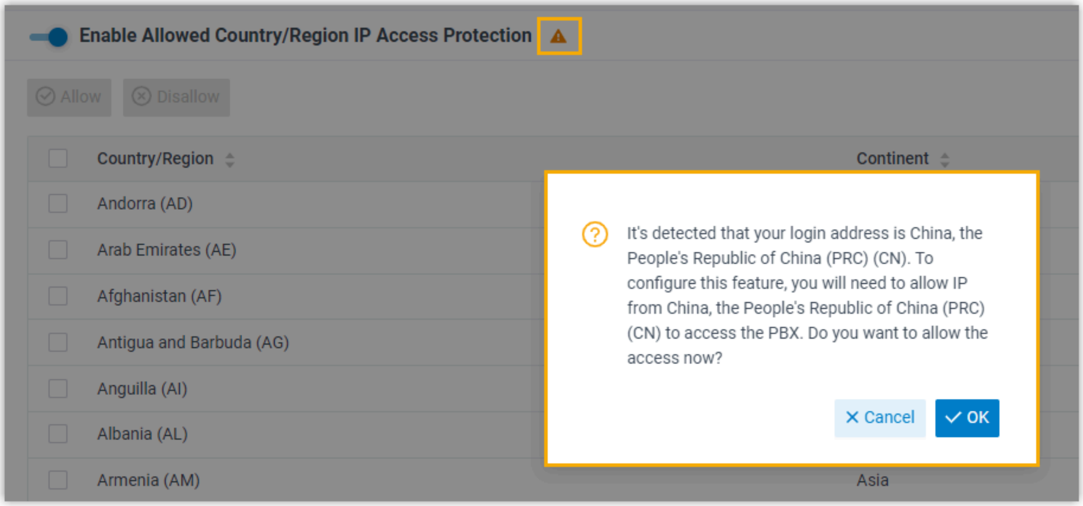
Restrict Specific Countries or Regions from Accessing Yeastar P-Series Software Edition

By default, all the countries and regions are allowed to access Yeastar P-Series Software Edition. 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.

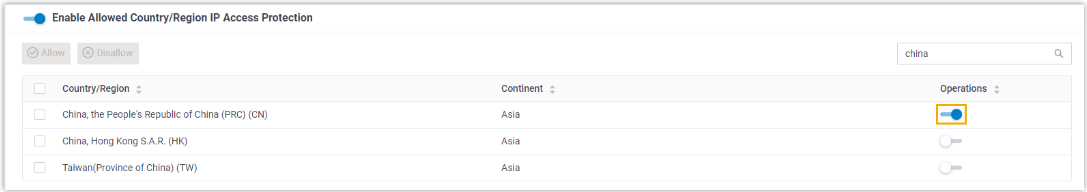
   The system tries to identify whether the connection from your current IP address is accepted in the Static Defense allowlist of your PBX.
3. If current IP address is not accepted in the Static Defense allowlist of your PBX, the system would try to identify the country/region from which your current IP 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.



□	Country/Region	Continent
□	Andorra (AD)	
□	Arab Emirates (AE)	
□	Afghanistan (AF)	
□	Antigua and Barbuda (AG)	
□	Anguilla (AI)	
□	Albania (AL)	
□	Armenia (AM)	Asia

It's detected that your login address is China, the People's Republic of China (PRC) (CN). To configure this feature, you will need to allow IP from China, the People's Republic of China (PRC) (CN) to access the PBX. Do you want to allow the access now?

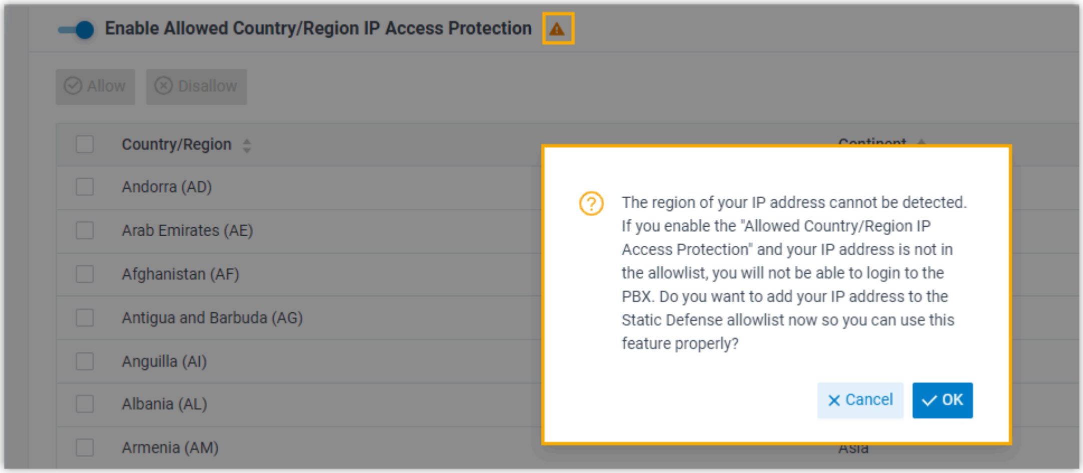
You should click OK to allow IPs from your current country/region to access the PBX. In doing so, the warning icon ⚠ is disappeared, and operation status of your country/region is changed to ● .



● Enable Allowed Country/Region IP Access Protection

□	Country/Region	Continent	Operations
□	China, the People's Republic of China (PRC) (CN)	Asia	●
□	China, Hong Kong S.A.R. (HK)	Asia	○
□	Taiwan(Province of China) (TW)	Asia	○

- 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.



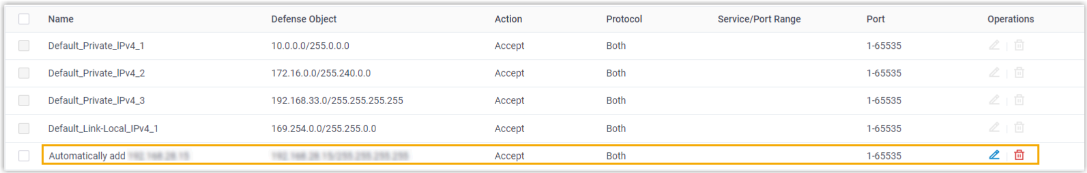
● Enable Allowed Country/Region IP Access Protection ⚠

□	Country/Region	Continent
□	Andorra (AD)	
□	Arab Emirates (AE)	
□	Afghanistan (AF)	
□	Antigua and Barbuda (AG)	
□	Anguilla (AI)	
□	Albania (AL)	
□	Armenia (AM)	Asia

The region of your IP address cannot be detected. If you enable the "Allowed Country/Region IP Access Protection" and your IP address is not in the allowlist, you will not be able to login to the PBX. Do you want to add your IP address to the Static Defense allowlist now so you can use this feature properly?

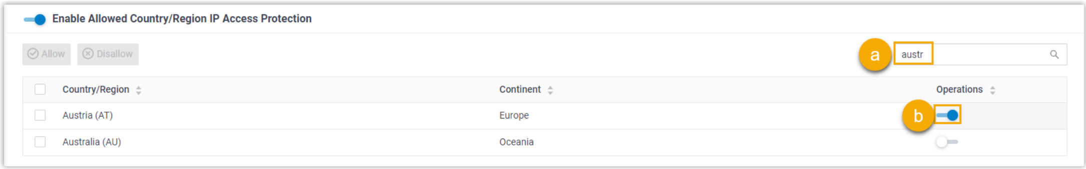
You should click OK to add your IP address to the Static Defense allowlist. In doing so, the warning icon ⚠ is disappeared, and connections from your IP address are accepted.

> **Tip:**
> You can check the added IP address on Security > Security Rules > Static Defense.



□	Name	Defense Object	Action	Protocol	Service/Port Range	Port	Operations
□	Default_Private_IPv4_1	10.0.0.0/255.0.0.0	Accept	Both		1-65535	
□	Default_Private_IPv4_2	172.16.0.0/255.240.0.0	Accept	Both		1-65535	
□	Default_Private_IPv4_3	192.168.33.0/255.255.255.255	Accept	Both		1-65535	
□	Default_Link-Local_IPv4_1	169.254.0.0/255.255.0.0	Accept	Both		1-65535	
□	Automatically add [redacted]	[redacted]	Accept	Both		1-65535	

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:

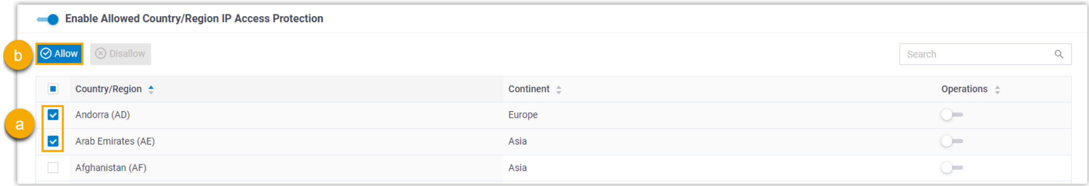


☐	Country/Region	Continent	Operations
☐	Austria (AT)	Europe	●
☐	Australia (AU)	Oceania	○

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:



■	Country/Region	Continent	Operations
☑	Andorra (AD)	Europe	○
☑	Arab Emirates (AE)	Asia	○
☐	Afghanistan (AF)	Asia	○

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.

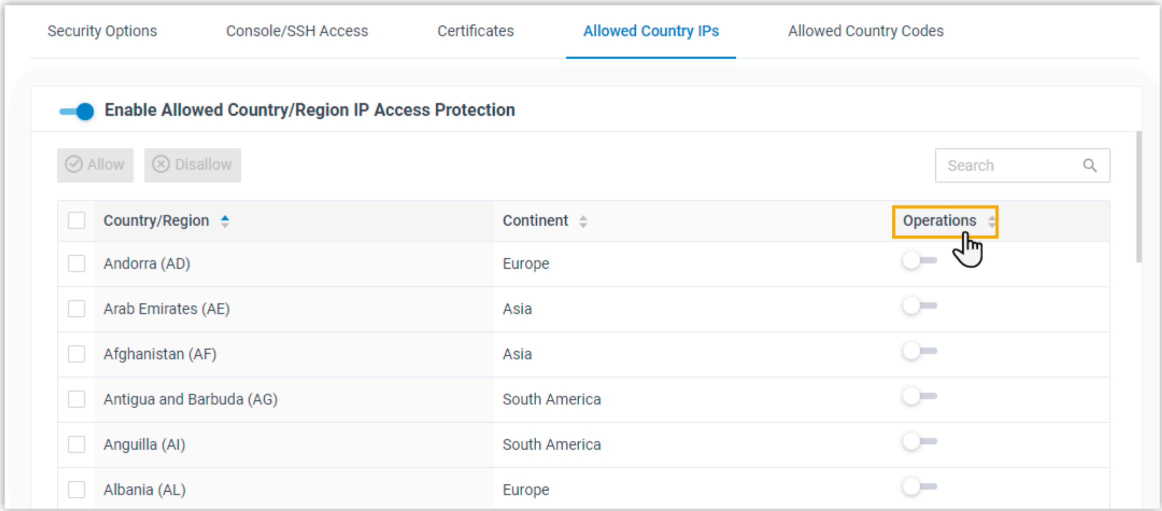
> Tip:
>
> For the disallowed countries or regions, if you want to allow a specific IP address to access the PBX, you can add a static defense rule to accept connections from the desired IP address. For more information, see Add a Static Defense Rule.

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 Software Edition 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.

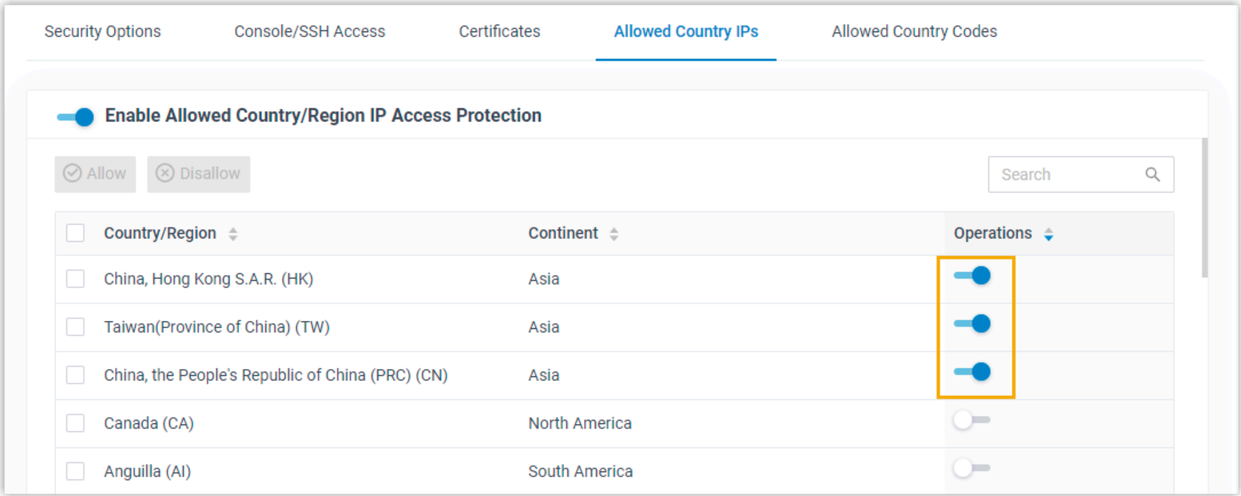


Enable Allowed Country/Region IP Access Protection ●

□	Country/Region	Continent	Operations
□	Andorra (AD)	Europe	○
□	Arab Emirates (AE)	Asia	○
□	Afghanistan (AF)	Asia	○
□	Antigua and Barbuda (AG)	South America	○
□	Anguilla (AI)	South America	○
□	Albania (AL)	Europe	○

Result

All the countries and regions that are allowed to access the PBX are moved to the top.



Enable Allowed Country/Region IP Access Protection ●

□	Country/Region	Continent	Operations
□	China, Hong Kong S.A.R. (HK)	Asia	●
□	Taiwan(Province of China) (TW)	Asia	●
□	China, the People's Republic of China (PRC) (CN)	Asia	●
□	Canada (CA)	North America	○
□	Anguilla (AI)	South America	○

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:

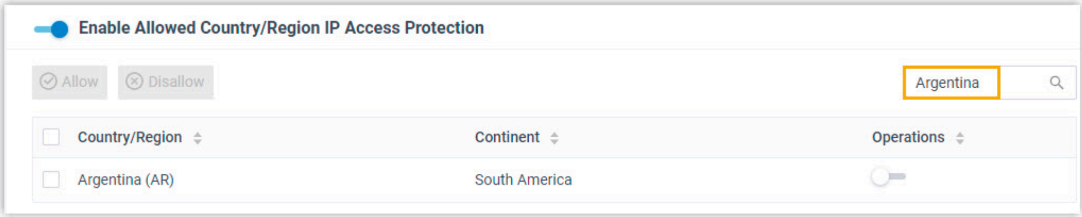
- Step1. Allow international calls to Argentina only
- Step2. Allow employees to make international calls

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.



Country/Region	Continent	Operations
Argentina (AR)	South America	

    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

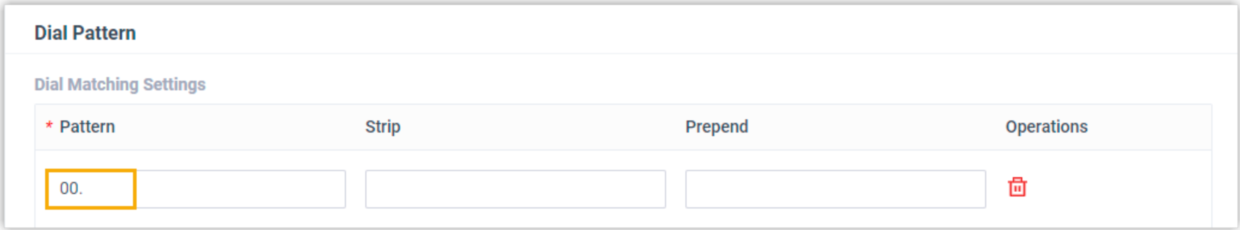
By default, after you enable country/region code dialing protection, all the users are not allowed to make international calls. To allow employees to make international calls, you need to grant permission to desired employees.

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:



Dial Pattern

Dial Matching Settings

* Pattern	Strip	Prepend	Operations
00.			🗑

When an authorized employee dials a number, PBX's outbound route will check if the dialing is valid:

- When an authorized employee dials 00541938384, the dialing is considered as valid.
- When an authorized employee dials 00621938384, the dialing is considered as invalid.
- When an authorized employee dials 541938384, it will not be considered as an international dialing, and the PBX will check if there is a matched outbound route to route the call out.

Block Outbound International Calls

To restrict users from making international calls, you can restrict dial pattern of outbound routes, or set up international dialing protection. This topic describes how to set up international dialing protection to block outbound international calls.

Procedure

1. Log in to PBX 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.

Maintenance

Upgrade

Check for Available Firmware Updates

This topic describes how to automatically or manually check for firmware updates.

Automatic check for firmware updates

Restrictions

This feature is available only when the number of PBX extensions is less than 1000.

Prerequisites

Make sure the PBX can access the Internet.

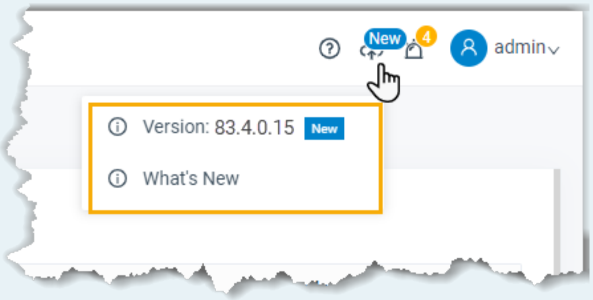
Procedure

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 Automatically check for updates at drop-down list, set when the system should check for new version. This can be a daily or weekly check.
4. Click Save.

Result

The system will regularly check for new firmware.

> Note:
>
> If a new firmware is detected, the followings can be achieved:
>
> - At the top-right corner of PBX web portal, New is displayed. Click New, 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

Restrictions

This feature is available only when the number of PBX extensions is less than 1000.

Prerequisites

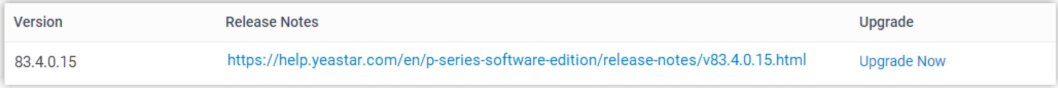
Make sure the PBX can access the Internet.

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
83.4.0.15	https://help.yeastar.com/en/p-series-software-edition/release-notes/v83.4.0.15.html	Upgrade Now

Schedule Automatic Firmware Upgrade

This topic describes how to schedule auto detection and upgrade of new firmware.

Restrictions

This feature is available only when the number of PBX extensions is less than 1000.

Prerequisites

- Make sure Yeastar P-Series Software Edition 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

Restrictions

This feature is available only when the number of PBX extensions is less than 1000.

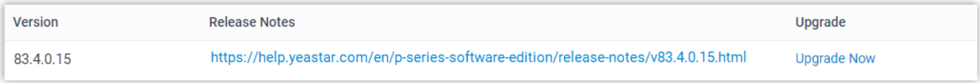
Prerequisites

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:

Version	Release Notes	Upgrade
83.4.0.15	https://help.yeastar.com/en/p-series-software-edition/release-notes/v83.4.0.15.html	Upgrade Now
2. Click the Release Notes link to check the update details of the new version.

3. Upgrade system firmware.
    a. Click Upgrade Now.

    > Important:
    > - Ensure the connection to Internet and power supply when the PBX is upgrading.
    > - Make sure there aren't ongoing calls, or the calls would be disconnected.

    b. In the pop-up dialog box, click OK.

Result

The PBX starts upgrading the firmware.

> Important:
> When the PBX is upgrading, do NOT turn off the power, or the system will get damaged.

Manually upgrade PBX via a local firmware file

Prerequisites

- Go to Yeastar Firmware Download Center to check and download the new firmware.
- We recommend that you create a backup file for PBX configurations before you start upgrading the PBX.

Procedure

1. Log in to PBX 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 Software Edition 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 Software Edition 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 Software Edition supports to back up the following configuration data:

- System Configuration: All the configurations on the system.
- Custom Prompts
- CDR
- Company Contacts and Phonebooks Settings

Backup locations

Backup files can be stored in the following locations:

- Local drive: The PBX's local drive.
- Hard disk drive
- 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, hard disk driveor network drive. If you want to save the file to hard disk driveor network drive, you need to set up a hard disk drive or add a network drive on the system first. For more information, see the following topics:
    - Set up a Hard Disk Drive
    - 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 hard disk driveor 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
3. Click Save.

Result

The created backup file is displayed in Backup and Restore list and is stored in the selected location.

Set up an Automatic Backup Schedule

Yeastar P-Series Software Edition 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, hard disk driveor network drive. If you want to save the file to hard disk driveor network drive, you need to set up a hard disk drive or add a network drive on the system first. For more information, see the following topics:
    - Set up a Hard Disk Drive
    - Add a Windows Network Drive
    - Add a Mac Network Drive
- What - Whether to back up custom prompts, CDR, or company contacts and phonebooks 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 backup.
        - Frequency: Choose to make a daily, weekly, or monthly backup.
            - Daily: If you choose the option, select a time from the drop-down list. The system backs up the settings at this time of the day.
            - Weekly: If you choose the option, choose a day of week and select a time from the drop-down list. The system backs up the settings at this time of the week.
            - Monthly: If you choose the option, choose a day and select a time from the drop-down list. The system backs up the settings on this day and time of the month.

            > Note:
            >
            > If you set the day to 31, but the month only has 29 or 30 days, the system will not make a backup.

    b. In the Storage Location drop-down list, select where you want to save the backup file.

    > Note:

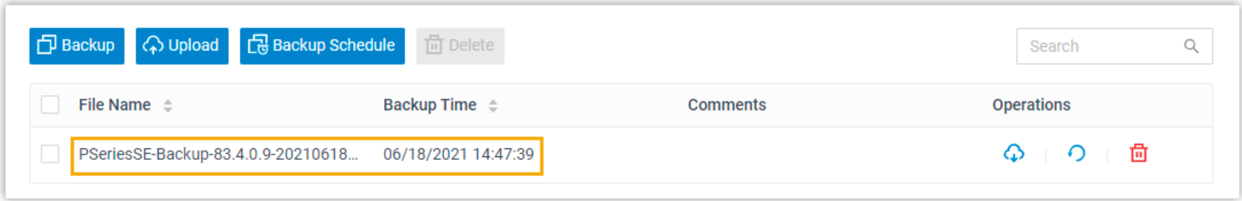
> To prevent backup failure in case of disconnection to hard disk driveor network drive, we recommend that you save the backup file on the local flash (LOCAL).

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

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.



□	File Name	Backup Time	Comments	Operations
□	PSeriesSE-Backup-83.4.0.9-20210618...	06/18/2021 14:47:39		

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 (v83.4.0.8) to PBX (v83.4.0.12) would work.
    - You can NOT restore a backup file that is created from a newer version of PBX.

      Example: Restoring a backup file (v83.4.0.12) to PBX (v83.4.0.8) 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 dialog box, click OK.
4. Reboot the PBX to take effect.

Result

The current configurations on your PBX are OVERWRITTEN with the backup data.

Related information

[Create an On-Demand Backup]
[Set up an Automatic Backup Schedule]

Reboot

Reboot Yeastar P-Series Software Edition on Web Interface

This topic describes how to reboot Yeastar P-Series Software Edition 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.

Shut Down Yeastar P-Series Software Edition

To shut down a running P-Series PBX system, you can not power off the server directly. The PBX should be shut down in a controlled manner, otherwise files might get lost or disk damage might occur.

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 Shut Down Now.
3. In the pop-up dialog box, click Yes to shut down the PBX.

Schedule Automatic Reboot

To ensure the stability and robustness of Yeastar P-Series Software Edition, 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 Software Edition.

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.

      > Note:
      >
      > If you set Date to 31, but the month only has 28, 29, or 30 days, the system will NOT reboot itself automatically.
4. Click Save.

Reset

Reset the System on Web Interface

This topic describes how to reset Yeastar P-Series Software Edition 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.

  > Important:
  > For PBX system installed on a cloud-based server, do NOT reset networking settings, or you can NOT access the PBX management portal.
- 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 Software Edition, 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 71.

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

Table 71. (continued)

Event Type	Event
	Outbound Call to a Disallowed Country

Manage Operation Logs

This topic describes how to view and download operation logs on Yeastar P-Series Software Edition.

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 Software Edition 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 Software Edition 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.

Activation

Overview of Yeastar P-Series Software Edition Activation

To access basic telephony features and advanced unified communication features, you need to contact your PBX provider to purchase a license from Yeastar and fill in the provided activation code on the system.

Licenses for Yeastar P-Series Software Edition

Table 72.

	Trial License	Commercial License
Extensions	100	Max. 10,000
Concurrent Calls	25	Max. 1,000
Validity	1 month	Annual Subscription
Activation Method	Online Activation	Online or Offline Activation

Activation methods

Based on the differences in network availability of Yeastar P-Series Software Edition, Yeastar provides two activation methods to adapt to your needs. Refer to the following table for details:

Table 73.

Method	Environment	Instruction
Online Activation	PBX can access the Internet	Activate the PBX online
Offline Activation	PBX can NOT access the Internet	Activate the PBX offline

Activation status

The following list helps you identify the activation status of your device:

- Not Activated: The system is inactivated. Contact your PBX provider to purchase a license from Yeastar.

- Activated: The system is activated. You can enjoy all the features that are supported by the license that you have purchased.
- Error: The system fails to connect to License Activation Server.
- Expired: The license is expired. Contact your device provider to extend license validity.

Activation expiration reminder

When it comes to 30 days and 7 days before the expiration date, or on the day, the system will display a banner at the top as well as sending an email to your mailbox for reminder. Contact your PBX provider to renew your license in time, or you can not use any call service of PBX.

Activate Yeastar P-Series Software Edition

If an activation code is not ready when you set up Yeastar P-Series Software Edition using the Installation Wizard, you can skip activation and finish the initial settings first, and then activate the system at any time when the activation code is ready.

Activate the PBX online

Prerequisites

- Yeastar P-Series Software Edition can access the Internet.
- Contact your PBX provider to purchase a license and get an activation code.

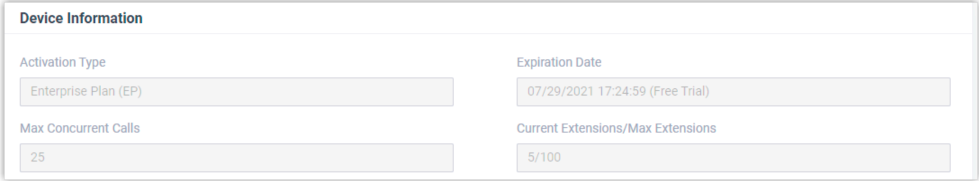
Procedure

1. Log in to the PBX web portal, go to Maintenance > Activation.
2. In the Activation Method drop-down list, select Online.
3. In the Activation Code field, enter the activation code.
4. Click Activate.

Result

It takes about one minute to reboot the PBX. After system reboot, you can check the followings:

- The Activation Status is displayed as Activated.
- In the Device Information section, you can check type and expiration date of the license that you have purchased, and the max concurrent calls and extensions of your system.



Device Information

Activation Type: Enterprise Plan (EP)

Expiration Date: 07/29/2021 17:24:59 (Free Trial)

Max Concurrent Calls: 25

Current Extensions/Max Extensions: 5/100

Activate the PBX offline

If your Yeastar P-Series Software Edition can NOT access the Internet, follow the instructions below to activate your system.

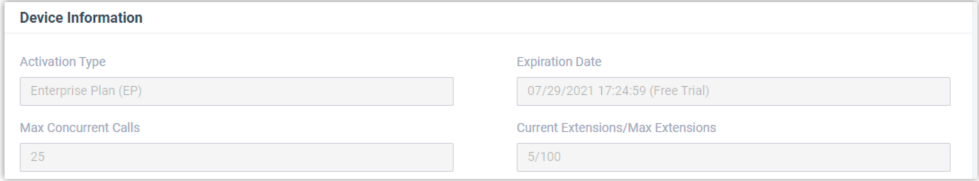
Procedure

1. Log in to the PBX web portal, go to Maintenance > Activation.
2. In the Activation Method drop-down list, select Offline.
3. Click Download Request File and send the request file to your PBX provider to get an activation code.
4. In the Activation Code field, enter the activation code.
5. Click Activate.

Result

It takes about one minute to reboot the PBX. After system reboot, you can check the followings:

- The Activation Status is displayed as Activated.
- In the Device Information section, you can check type and expiration date of the license that you have purchased, and the max concurrent calls and extensions of your system.



Device Information

Activation Type: Enterprise Plan (EP)

Expiration Date: 07/29/2021 17:24:59 (Free Trial)

Max Concurrent Calls: 25

Current Extensions/Max Extensions: 5/100

Update License of Yeastar P-Series Software Edition

If you want to extend the number of extensions or the validity of the license, or enjoy more advanced PBX features, you can contact your PBX provider to renew license, and update the new activation code on Yeastar P-Series Software Edition.

Prerequisites

Contact your PBX provider to purchase a new license.

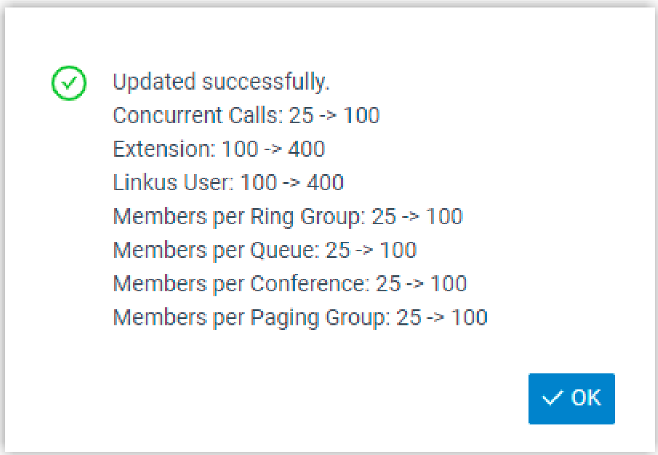
Procedure

1. Log in to the PBX web portal, go to Maintenance > Activation.
2. To update an online activation code, click Refresh.

   The system automatically obtains the license information from Yeastar Activation Server and updates the configurations that you have requested for update.
3. To update an offline activation code, do as follows:
   a. Click Update.
   b. In the pop-up window, enter the activation code.
   c. Click Save and OK.

Result

Changes of the configurations are displayed on the pop-up window and synchronized to Device Information section.



Updated successfully.
Concurrent Calls: 25 -> 100
Extension: 100 -> 400
Linkus User: 100 -> 400
Members per Ring Group: 25 -> 100
Members per Queue: 25 -> 100
Members per Conference: 25 -> 100
Members per Paging Group: 25 -> 100

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 Software Edition 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

Storage of system logs

System logs are saved in local storage, you can NOT change the storage location.

Auto cleanup of system logs

By default, the system automatically deletes the oldest system logs every 7 days, or when logs reach 10MB. You can change the maximum file size or days that logs can be retained. For more information, see Auto Cleanup Settings.

Configure Log Level

Yeastar P-Series Software Edition 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
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 Software Edition.

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.

CDR and Reports

CDR

Call Detail Record (CDR) Overview

The Call Detail Record (CDR) feature provides information about calls over Yeastar P-Series Software Edition. This topic describes parameters and auto cleanup of CDR.

CDR parameters

A CDR contains the following information:

- ID: A unique identifier for each call.
- Time: When the call was made or received.
- Call From: The number or the name of the caller.
- Call To: The number or the name of the callee.
- Call Duration: The time between the call started and the call ended.
- Ring Duration: The time between the call started and the call answered.
- Talk Duration: The time between the call answered and the call ended.
- Status: Call status.
  - ANSWERED
  - NO ANSWER
  - BUSY
  - FAILED
  - VOICEMAIL
- Reason: The reason why the call was ended.
- Source Trunk: The call was received via which trunk.
- Destination Trunk: The call was sent out via which trunk.
- Communication Type:
  - Internal
  - Outbound
  - Inbound
- DID/DDI: The phone number that the caller dialed.
- Outbound Caller ID: The phone number that was displayed on the callee's phone.
- Caller IP Address: The IP address of the caller's device.
- PIN Code: The PIN code entered when making a call via a restricted outbound route.
- Recording File: The call recording file.

CDR auto cleanup

By default, when the number of call logs reaches 200,000 (extensions $<$1000) or 1,000,000 (extensions ≥1000) , the system automatically deletes the oldest call logs (relevant recordings are retained.). You can change the maximum value, or you can also set the maximum preservation days.

For more information, see Auto Cleanup Settings.

Manage CDR

This topic describes how to view, download, and delete call logs.

View CDR

1. Log in to PBX web portal, go to Reports and Recordings > CDR.
2. Optional: Set the basic filter criteria.
    - Time: Set the start date and the end date.

      To specify a time period, click select time to set the start time and the end time.
    - Call From: Set the caller's number or name.
    - Call To: Set the callee's number or name.

      > Tip:
      >
      > To swap the callee for the caller, click ⇆.
    - Status: Select a call status.
        - 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.
    - Extension Group: Select an extension group. The system only queries group members' calls.
    - Ring Duration: Set how long the callee's phone rang before the call was answered.

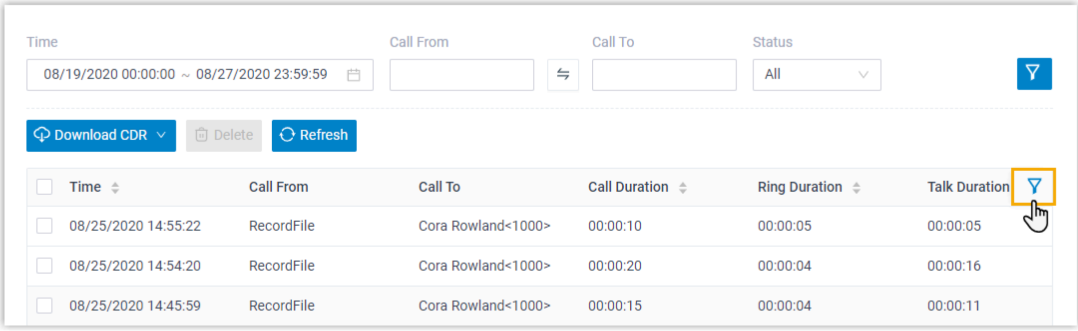
      > Note:
      >
      > Only numbers, -, =,<, <=, >, and >= are allowed.
    - Talk Duration: Set the time between the call was answered and the call was ended.

      > Note:
      >
      > Only numbers, -, =,<, <=, >, and >= are allowed.
    - Status: Select call status.

    - All
    - ANSWERED
    - NO ANSWER
    - BUSY
    - FAILED
    - VOICEMAIL
  - Communication Type: Select a type.
    - All
    - Internal
    - Outbound
    - Inbound
  - ID: Enter the unique identifier for a call.
  - Trunk: Select a trunk, which specifies the source or the destination trunk that the call went through.
  - Enable Number Fuzzy Search: Set whether to search for the fuzzy equivalent for the phone number.
  - PIN Code: Enter an existed PIN code, the system only queries the calls using this PIN code.

c. Scroll up to click ✕ to close the window.
   The filtered call logs are displayed on the page.

> **Note:**
>
> You can click ▽ to decide which item will be displayed.



Time: 08/19/2020 00:00:00 ~ 08/27/2020 23:59:59

Call From:

Call To:

Status: All

	Time	Call From	Call To	Call Duration	Ring Duration	Talk Duration
□	08/25/2020 14:55:22	RecordFile	Cora Rowland<1000>	00:00:10	00:00:05	00:00:05
□	08/25/2020 14:54:20	RecordFile	Cora Rowland<1000>	00:00:20	00:00:04	00:00:16
□	08/25/2020 14:45:59	RecordFile	Cora Rowland<1000>	00:00:15	00:00:04	00:00:11

Download CDR

1. Log in to PBX 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.

   Call logs 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.

Call Report

Call Reports Overview

Yeastar P-Series Software Edition 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.

Types of Call Reports

Yeastar P-Series Software Edition supports the following types of call reports:

- Extension Call Statistics
- Extension Call Activity
- Trunk Activity
- DID/Outbound Caller ID Activity
- 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

Methods of getting a call report

Yeastar P-Series Software Edition 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 Software Edition.

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 is a summary report displayed in pie chart, which makes it possible for you to query statistics of calls that have been made or received by a specific extension or extensions within a specific group/organization, and view percentage and proportional data of call statistics.

Report details

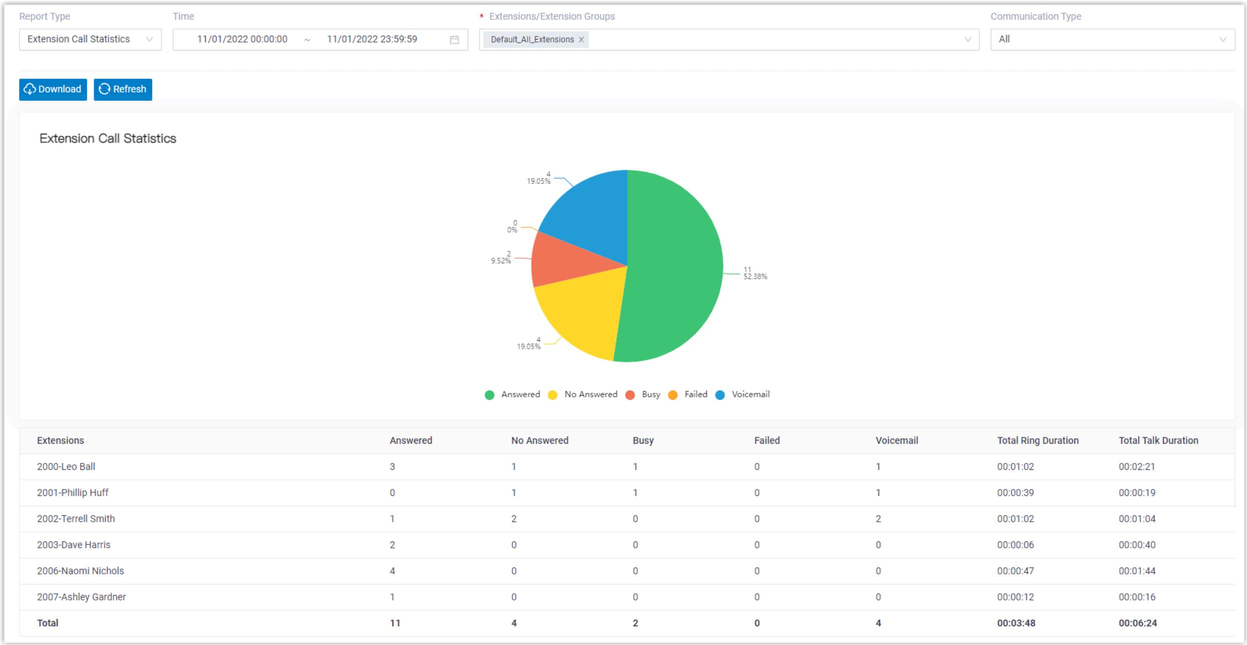
The following table lists the related parameters for Extension Call Statistics report.

Parameter	Description
Answered	The total number of calls that the extension answered.
No Answered	The total number of calls that were routed to the designated destination when the extension didn't answer the calls.

Parameter	Description
Busy	The total number of calls that were routed to the designated destination when the extension was busy.
Failed	The total number of calls that were failed to be made by the extension.
Voicemail	The total number of voicemails that the extension received.
Total Ring Duration	The total time between calls started and calls answered. Note: This parameter 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	The total number of calls for each extension. Note: This parameter is displayed only when you set Communication Type filter to Inbound/Outbound.

Report example

The following report shows call statistics of all the extensions in group Default_All_Extensions on 11/01/2022.



Report Type: Extension Call Statistics

Time: 11/01/2022 00:00:00 ~ 11/01/2022 23:59:59

* Extensions/Extension Groups: Default_All_Extensions

Communication Type: All

Extensions	Answered	No Answered	Busy	Failed	Voicemail	Total Ring Duration	Total Talk Duration
2000-Leo Ball	3	1	1	0	1	00:01:02	00:02:21
2001-Phillip Huff	0	1	1	0	1	00:00:39	00:00:19
2002-Terrell Smith	1	2	0	0	2	00:01:02	00:01:04
2003-Dave Harris	2	0	0	0	0	00:00:06	00:00:40
2006-Naomi Nichols	4	0	0	0	0	00:00:47	00:01:44
2007-Ashley Gardner	1	0	0	0	0	00:00:12	00:00:16
Total	**11**	**4**	**2**	**0**	**4**	**00:03:48**	**00:06:24**

Extension Call Activity Report

'Extension Call Activity' report is a summary report displayed in line graph, which makes it possible for you to query statistics of calls that have been made or received by a specific extension or extensions within a specific group/organization. The report allows you to track changes of call activity over a specific period of time, or compare changes over the same period of time.

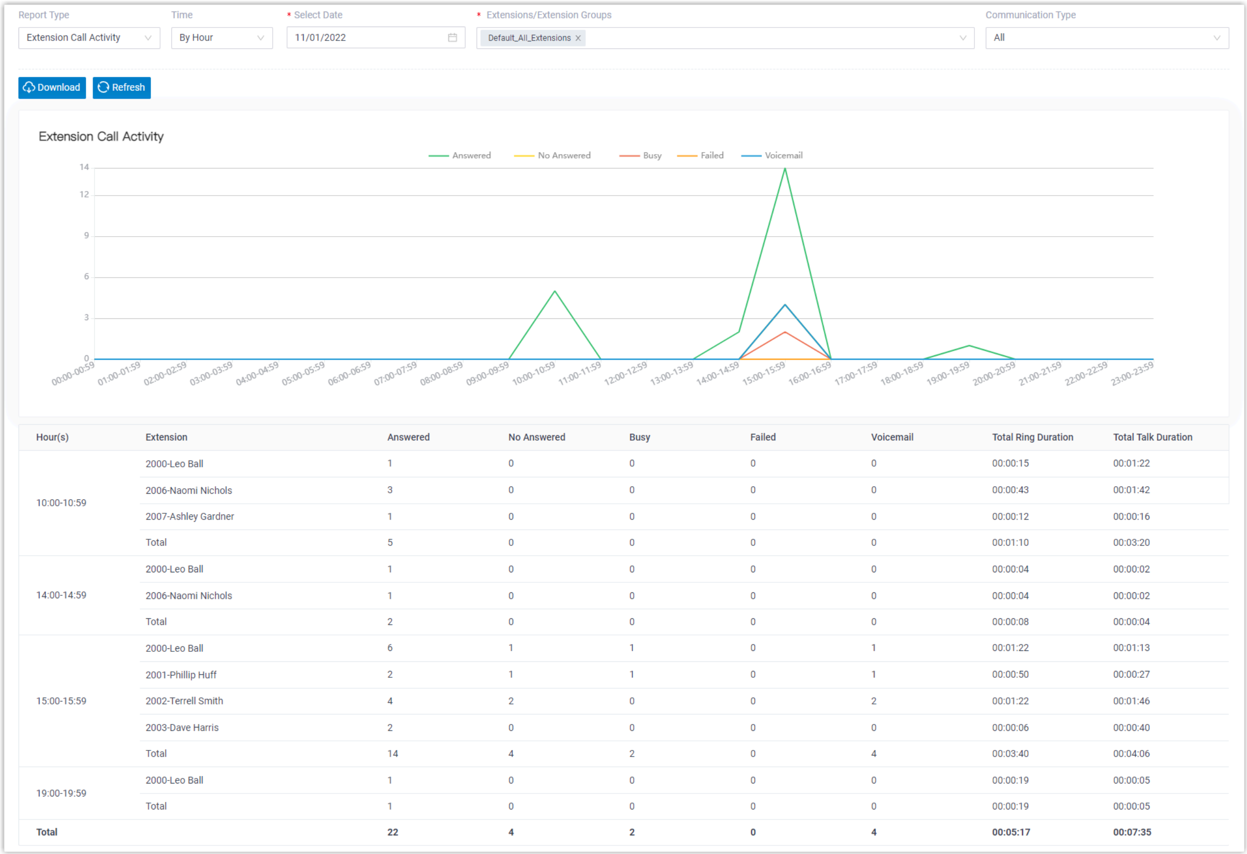
Report details

The following table lists the related parameters for Extension Call Activity report.

Parameter	Description
Answered	The total number of calls that the extensions answered.
No Answered	The total number of calls that were routed to the designated destination when the extensions didn't answer the calls.
Busy	The total number of calls that were routed to the designated destination when the extensions were busy.
Failed	The total number of calls that were failed to be made by the extensions.
Voicemail	The total number of voicemails that the extensions received.
Total Ring Duration	The time between the call started and the call answered.
Total Talk Duration	The time between the call answered and the call ended.

Report example

The following report shows hourly call statistics of all the extensions in group Default_All_Extensions on 11/01/2022.



Report Type: Extension Call Activity

Time: By Hour

* Select Date: 11/01/2022

* Extensions/Extension Groups: Default_All_Extensions

Communication Type: All

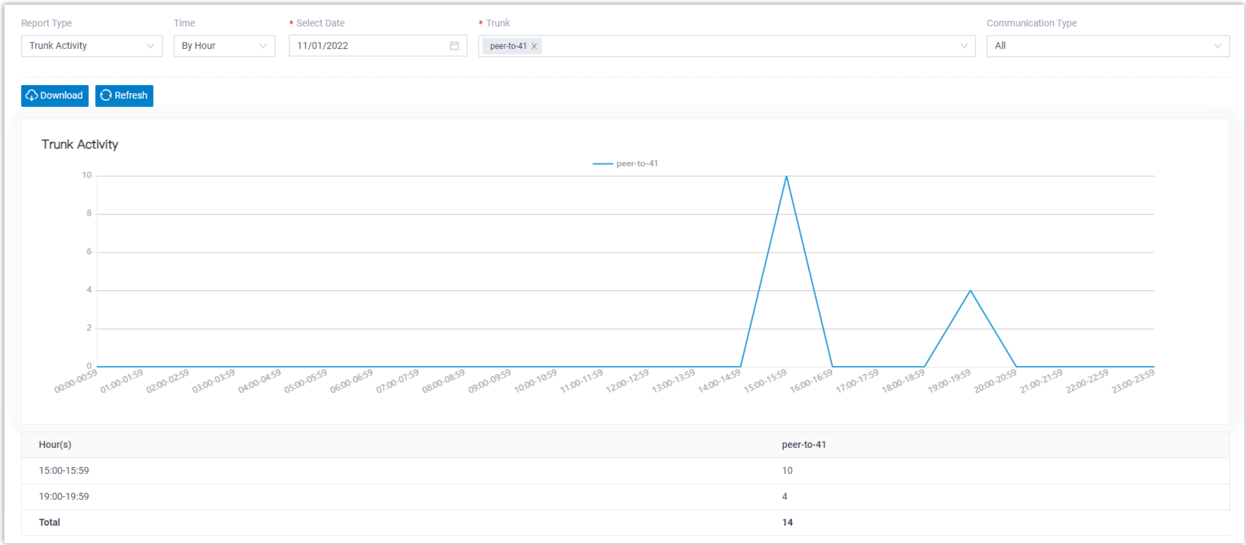
Hour(s)	Extension	Answered	No Answered	Busy	Failed	Voicemail	Total Ring Duration	Total Talk Duration
10:00-10:59	2000-Leo Ball	1	0	0	0	0	00:00:15	00:01:22
	2006-Naomi Nichols	3	0	0	0	0	00:00:43	00:01:42
	2007-Ashley Gardner	1	0	0	0	0	00:00:12	00:00:16
	Total	5	0	0	0	0	00:01:10	00:03:20
14:00-14:59	2000-Leo Ball	1	0	0	0	0	00:00:04	00:00:02
	2006-Naomi Nichols	1	0	0	0	0	00:00:04	00:00:02
	Total	2	0	0	0	0	00:00:08	00:00:04
15:00-15:59	2000-Leo Ball	6	1	1	0	1	00:01:22	00:01:13
	2001-Phillip Huff	2	1	1	0	1	00:00:50	00:00:27
	2002-Terrell Smith	4	2	0	0	2	00:01:22	00:01:46
	2003-Dave Harris	2	0	0	0	0	00:00:06	00:00:40
	Total	14	4	2	0	4	00:03:40	00:04:06
19:00-19:59	2000-Leo Ball	1	0	0	0	0	00:00:19	00:00:05
	Total	1	0	0	0	0	00:00:19	00:00:05
Total		**22**	**4**	**2**	**0**	**4**	**00:05:17**	**00:07:35**

Trunk Activity Report

'Trunk Activity' report is a summary report displayed in line graph, which makes it possible for you to query how many inbound and outbound calls have been received or made via a specific trunk. The report allows you to track changes of trunk activity by hour, by date, or by month.

Report example

The following report shows hourly call statistics of trunk peer-to-41 on 11/01/2022.



Report Type: Trunk Activity

Time: By Hour

* Select Date: 11/01/2022

* Trunk: peer-to-41

Communication Type: All

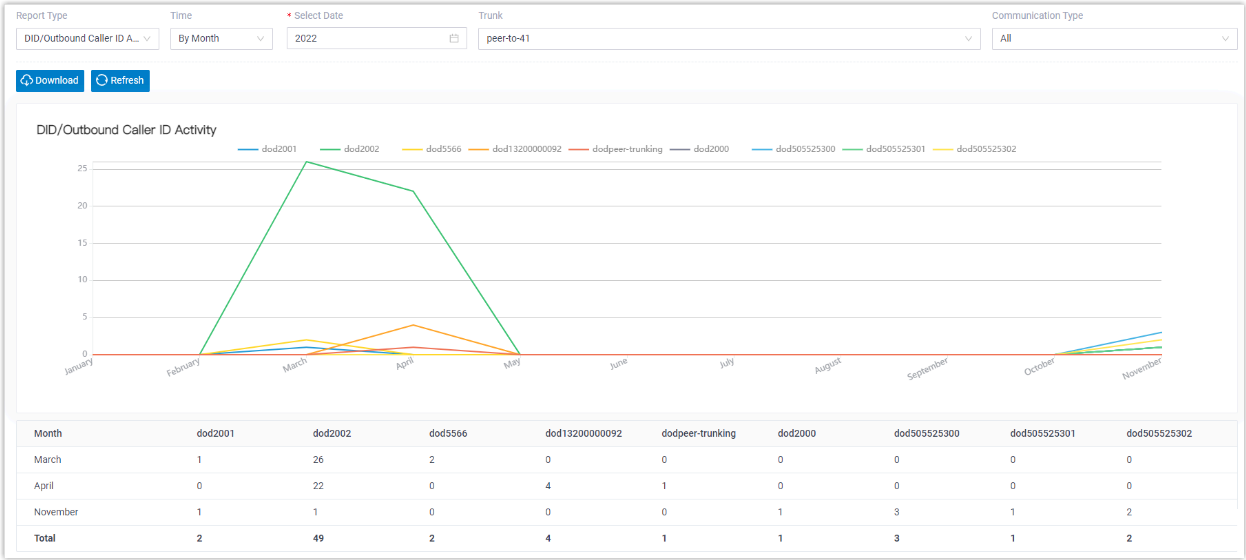
Hour(s)	peer-to-41
15:00-15:59	10
19:00-19:59	4
Total	**14**

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.



Report Type: DID/Outbound Caller ID A...

Time: By Month

* Select Date: 2022

Trunk: peer-to-41

Communication Type: All

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 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.

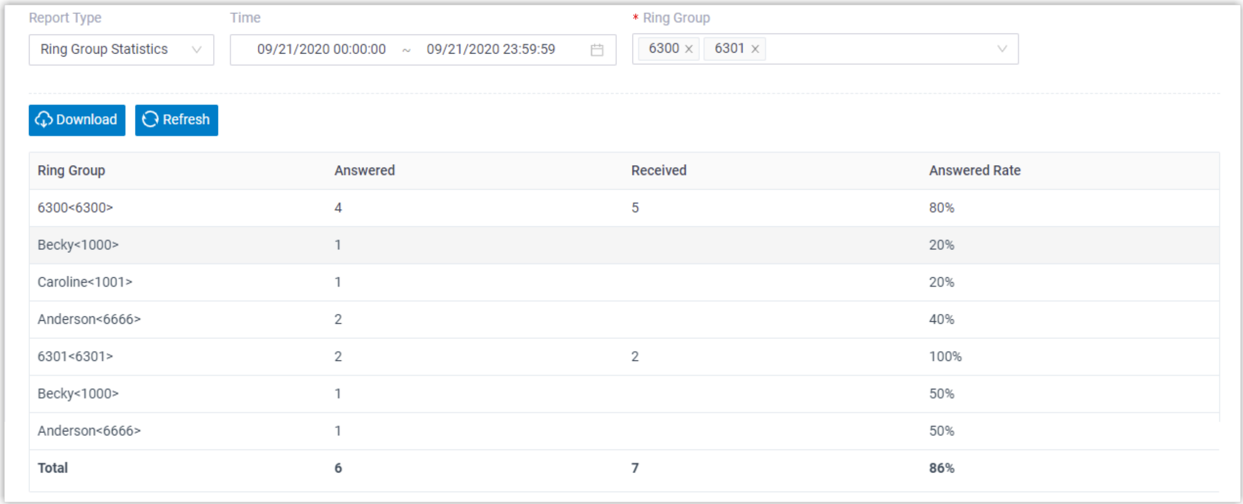
Report details

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.



Report Type: Ring Group Statistics

Time: 09/21/2020 00:00:00 ~ 09/21/2020 23:59:59

* Ring Group: 6300 × 6301 ×

Ring Group	Answered	Received	Answered Rate
6300<6300>	4	5	80%
Becky<1000>	1		20%
Caroline<1001>	1		20%
Anderson<6666>	2		40%
6301<6301>	2	2	100%
Becky<1000>	1		50%
Anderson<6666>	1		50%
Total	**6**	**7**	**86%**

Scheduled Reports

Schedule Call Reports

This topic describes how to schedule a call report to be sent to specific recipients' mailboxes at the specified time.

Background information

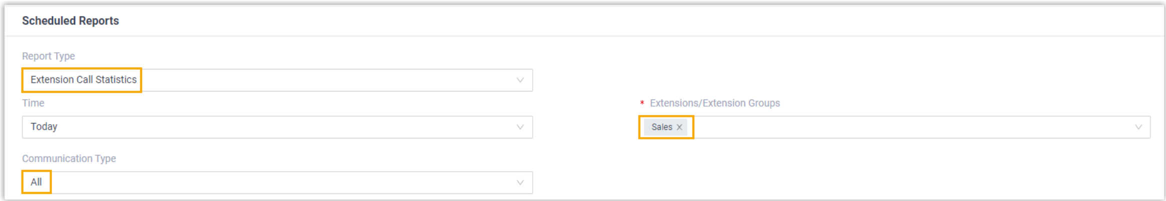
A scheduled call report is a diagram containing call statistics for the selected objects within a specific time frame. It automatically runs at a pre-defined frequency and is emailed to a specific address as a link and can be downloaded in CSV, XLS, or PDF.

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.



Scheduled Reports

Report Type: Extension Call Statistics

Time: Today

Communication Type: All

* Extensions/Extension Groups: Sales ×

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
  - Trunk Activity
  - DID/Outbound Caller ID Activity
- Short Abandoned Calls: Set a time. Calls abandoned within the specified time will not be included in report. You can use the parameter to filter call statistics in the following reports:
  - Queue Performance
  - Queue Performance Activity
  - Agent Missed Call Activity
  - Agent Performance
- 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

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 `;`.

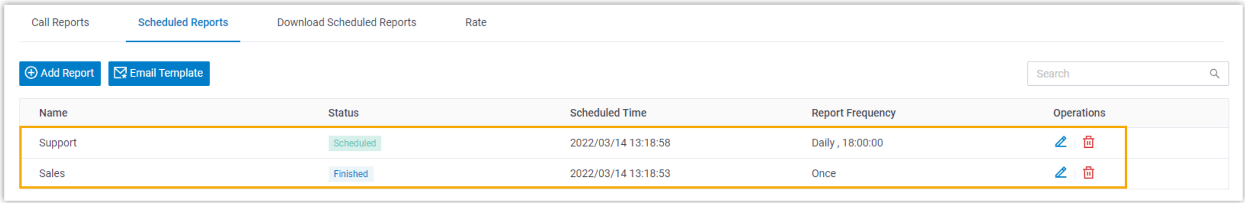
     > Note:
     >
     > You can set up to 10 email addresses.

     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.

       > Note:
       >
       > If you set the day to 31, but the month only has 29 or 30 days, the system will not send the report.
   - Format: Set in which format the report can be downloaded.
     - CSV
     - XLS
     - PDF
5. Click Save.

Result

On Scheduled Reports list, check status of the scheduled call report.



Name	Status	Scheduled Time	Report Frequency	Operations
Support	Scheduled	2022/03/14 13:18:58	Daily , 18:00:00	✎ 🗑
Sales	Finished	2022/03/14 13:18:53	Once	✎ 🗑

- 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 Software Edition 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.

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

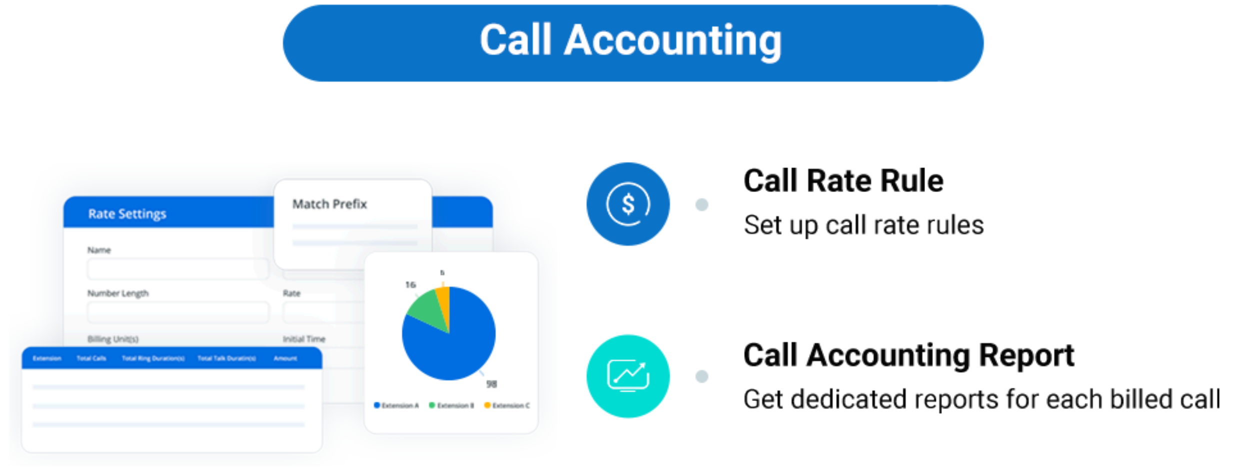
Tracking and analyzing telecom usage by individuals or departments help you manage and control telecommunication expenses, making the budgeting more accurate and efficient.

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.



Call Accounting

Call Rate Rule

Set up call rate rules

Call Accounting Report

Get dedicated reports for each billed call

1. [Add a Call Rate Rule]
2. [Extension Call Accounting Report]

Call Rate

Add a Call Rate Rule

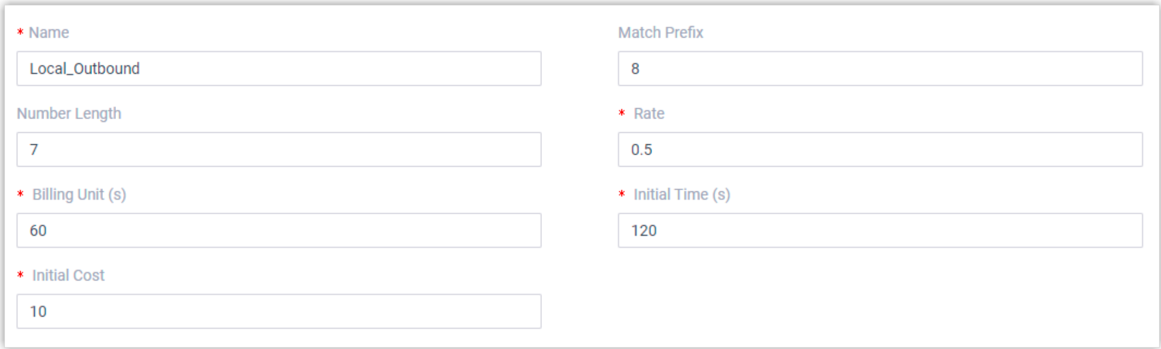
To monitor telecommunication costs for groups and individuals and prevent from potential fraudulent use of resources, you can add a call rate rule for outbound calls, such as local, long-distance, or international calls.

Restrictions

- A maximum number of 30,000 call rate rules is supported on Yeastar P-Series Software Edition.

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	Match Prefix
Local_Outbound	8
Number Length	* Rate
7	0.5
* Billing Unit (s)	* Initial Time (s)
60	120
* Initial Cost	
10	

- Name: Enter a name to help you identify the call rate rule. For example, enter `Local_Outbound`.
- Match Prefix: Optional. Define the prefix of outbound number to match the call rate rule.

  > Note:
  > The system matches call rate rules based on the outbound number instead of the dialed number.

  - If you leave this field blank, then all the outbound numbers will apply this rule.
  - If you set a specific value, then only outbound numbers starting with the prefix will apply this rule.
- Number Length: Optional. Define the length of the outbound number to match the call rate rule.
  - If you leave this field blank, then all the outbound numbers will apply this rule.
  - If you set a specific value, then only the outbound number whose length is shorter than or equal to the value will apply 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.

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 ⤒ ∧ ∨ ⤓ 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 Software Edition 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.

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 ⤒ ˄ ˅ ⤓ 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 you with an overview of bills of outbound calls that have been made by a specific extension or extensions within a specific group/organization via a specific trunk. The report allows you to track calling activities and monitor telecommunication usage within your company, eliminating the physical workload of tracking bills.

Prerequisites

- You have set up at least one call rate rule, or the system wouldn't know how to charge outbound calls.

  For more information, see Add a Call Rate Rule.

Get the report

You can get Extension Call Accounting Report in either of the following ways:

- Get instant report on PBX web portal (Path: Reports and Recordings > Call Reports > Call Reports).

  For more information, see View Call Reports.
- Get scheduled report via mailbox.

  > Tip:
  >
  > To achieve this, you need to schedule reports on PBX web portal (Path: Reports and Recordings > Call Reports > Scheduled Reports). For more information, see Schedule Call Reports.

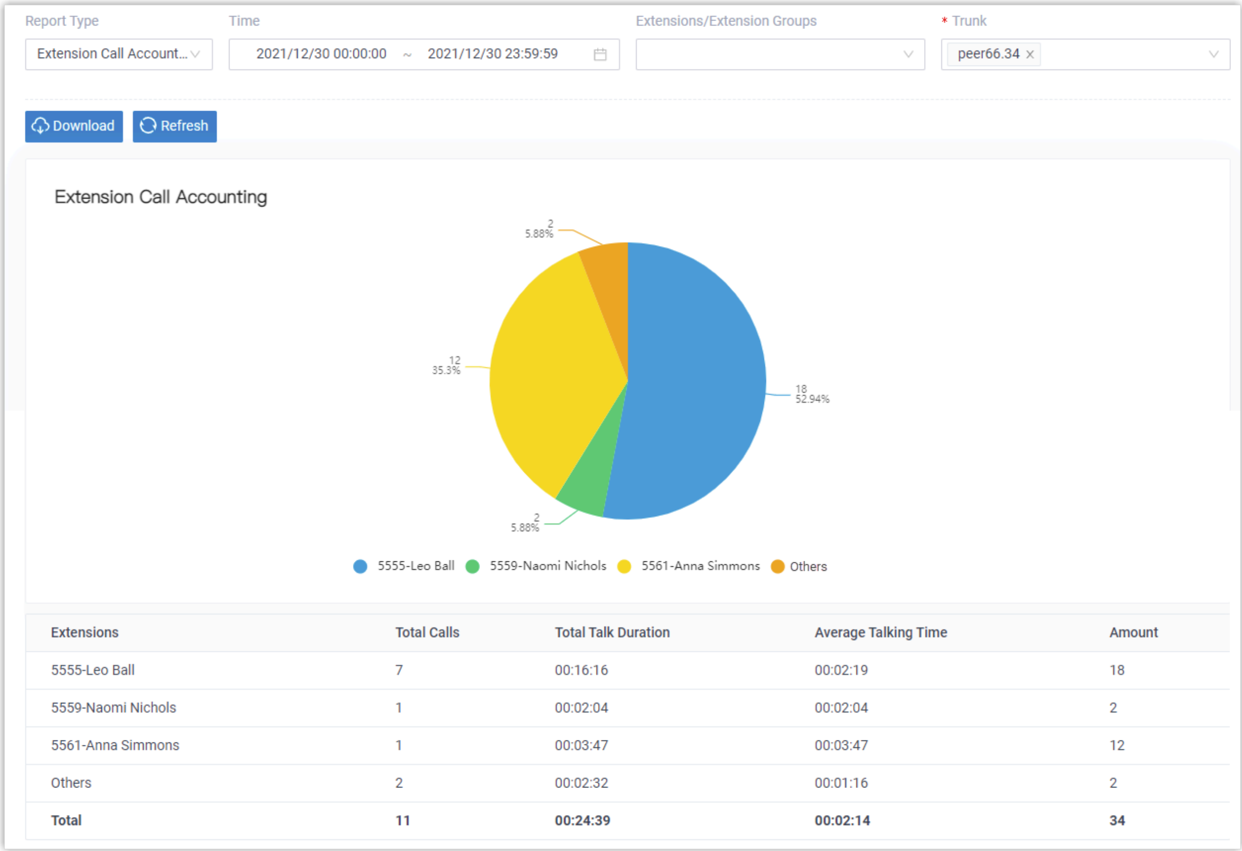
Report details

The following table lists the related parameters for Extension Call Accounting report.

Parameter	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.

Report example

The following report provides an overview of accounting statistics of outbound calls made by all the extensions through trunk peer 66.34 on 2021/12/30.



Report Type: Extension Call Account...

Time: 2021/12/30 00:00:00 ~ 2021/12/30 23:59:59

Extensions/Extension Groups:

* Trunk: peer66.34 ×

Download
Refresh
Extension Call Accounting
2
5.88%
12
35.3%
18
52.94%
2
5.88%
● 5555-Leo Ball ● 5559-Naomi Nichols ● 5561-Anna Simmons ● Others

Extensions	Total Calls	Total Talk Duration	Average Talking Time	Amount
5555-Leo Ball	7	00:16:16	00:02:19	18
5559-Naomi Nichols	1	00:02:04	00:02:04	2
5561-Anna Simmons	1	00:03:47	00:03:47	12
Others	2	00:02:32	00:01:16	2
Total	**11**	**00:24:39**	**00:02:14**	**34**

Related information

Extension Call Accounting Details Report

Extension Call Accounting Details Report

'Extension Call Accounting Details' report provides you with detailed information about bills of every outbound calls that have been made by a specific extension or extensions within a specific group/organization via a specific trunk. The report allows you to track calling activities and monitor telecommunication usage within your company, eliminating the physical workload of tracking bills.

Prerequisites

- You have set up at least one call rate rule, or the system wouldn't know how to charge outbound calls.

  For more information, see Add a Call Rate Rule.

Get the report

You can get the Extension Call Accounting Details Report in either of the following ways:

- Get instant report on PBX web portal (Path: Reports and Recordings > Call Reports > Call Reports).

  For more information, see View Call Reports.
- Get scheduled report via mailbox.

> Tip:
>
> To achieve this, you need to schedule reports on PBX web portal (Path: Reports and Recordings > Call Reports > Scheduled Reports). For more information, see Schedule Call Reports.

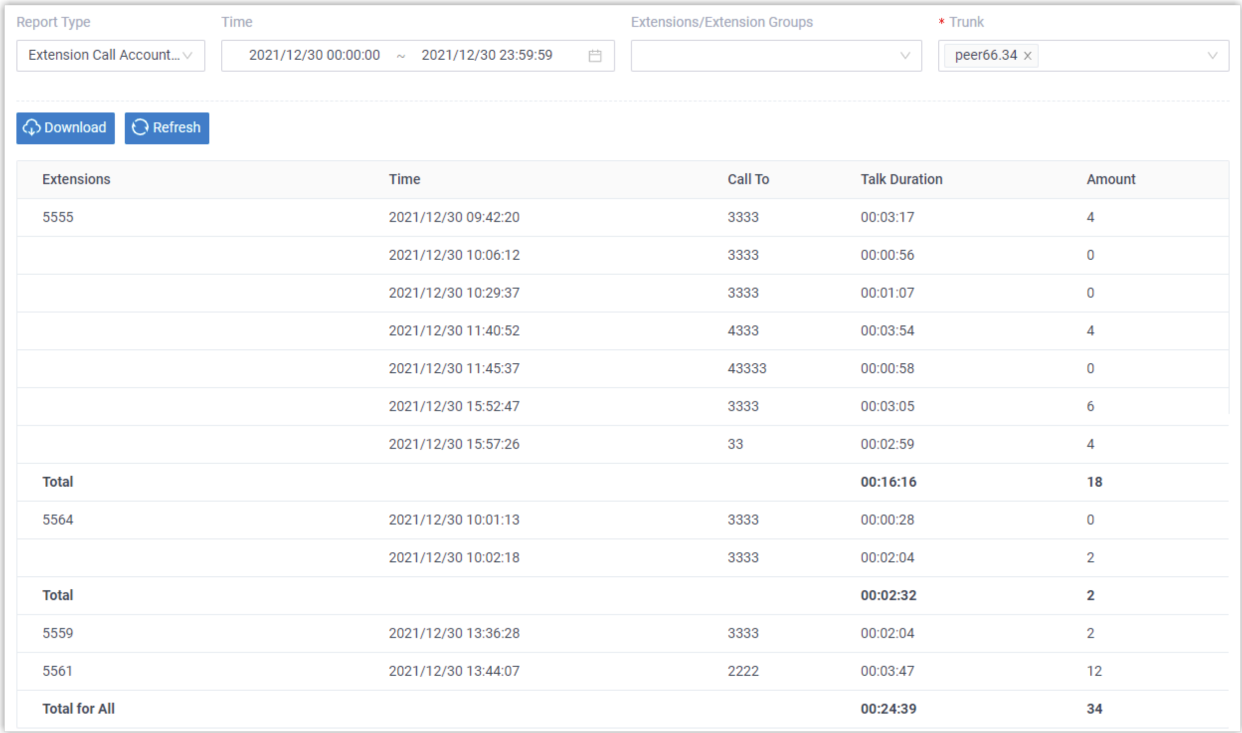
Report details

The following table lists the related parameters for Extension Call Accounting Details report.

Parameter	Description
Time	When the outbound call was made.
Call To	The callee number.
Talk Duration	The time between calls answered and calls ended.
Amount	The call cost.

Report example

The following report shows detailed accounting statistics of outbound calls made by all the extensions through trunk peer 66.34 on 2021/12/30.



Report Type	Time	Extensions/Extension Groups	* Trunk
Extension Call Account...	2021/12/30 00:00:00 ~ 2021/12/30 23:59:59		peer66.34

Extensions	Time	Call To	Talk Duration	Amount
5555	2021/12/30 09:42:20	3333	00:03:17	4
	2021/12/30 10:06:12	3333	00:00:56	0
	2021/12/30 10:29:37	3333	00:01:07	0
	2021/12/30 11:40:52	4333	00:03:54	4
	2021/12/30 11:45:37	43333	00:00:58	0
	2021/12/30 15:52:47	3333	00:03:05	6
	2021/12/30 15:57:26	33	00:02:59	4
Total			**00:16:16**	**18**
5564	2021/12/30 10:01:13	3333	00:00:28	0
	2021/12/30 10:02:18	3333	00:02:04	2
Total			**00:02:32**	**2**
5559	2021/12/30 13:36:28	3333	00:02:04	2
5561	2021/12/30 13:44:07	2222	00:03:47	12
Total for All			**00:24:39**	**34**

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 Software Edition allows you to use a third-party transcription service to implement the audio transcription.

Supported Service Platform

Yeastar P-Series Software Edition supports the following third-party transcription service:

> Note:
> The Speech to Text feature on Yeastar P-Series Software Edition 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 Software Edition with Google Cloud Speech-to-Text Service.

Applications

After STT integration is set up on the PBX, the speech recognition can be applied to Voicemail Transcription. Users can receive voicemails in the form of text on different platform:

Linkus Web Client and Linkus Mobile Client

Users can check the transcribed text for each voicemail on Linkus Web 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 Software Edition with Google Cloud Speech-to-Text Service

Before using Voicemail Transcription feature, you need to integrate Yeastar P-Series Software Edition 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 Software Edition.

Limitations

Audio length: 1 minute

The integration of Yeastar P-Series Software Edition 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 Software Edition 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.

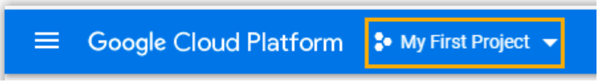
Procedure

1. Get the API key from Google Cloud Platform
2. Enable Speech to Text (STT) integration on Yeastar P-Series Software Edition

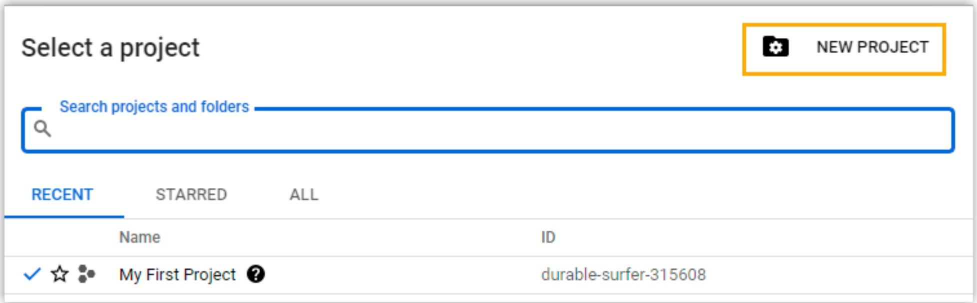
Get the API key from Google Cloud Platform

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.

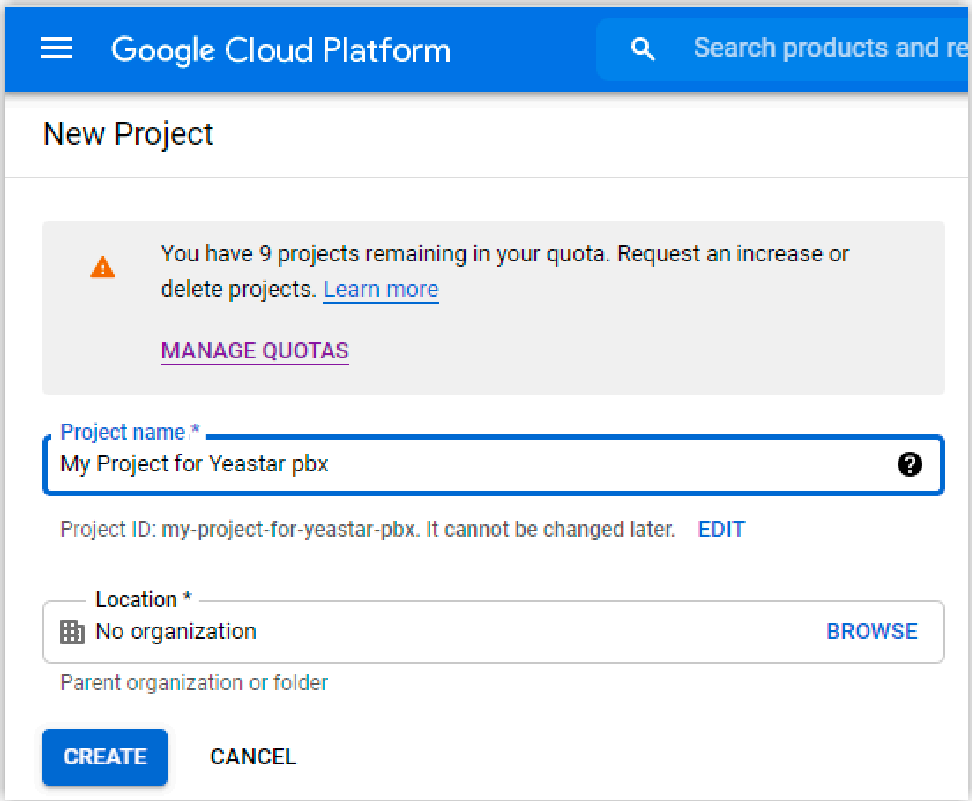


3. On the Select a project page, click NEW PROJECT in the top-right corner.



Name	ID
My First Project	durable-surfer-315608

4. On the New Project page, set a project name, and click CREATE.



You have 9 projects remaining in your quota. Request an increase or delete projects. Learn more

Project name *: My Project for Yeastar pbx

Project ID: my-project-for-yeastar-pbx. It cannot be changed later.

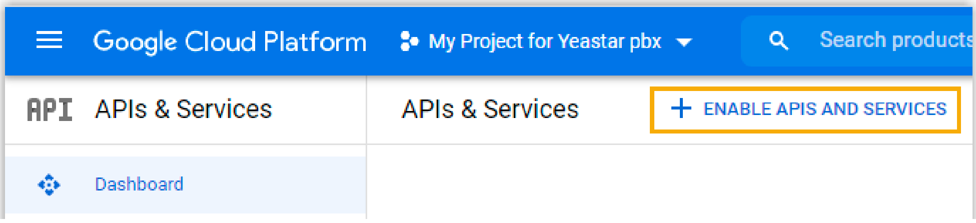
Location *: No organization

Parent organization or folder

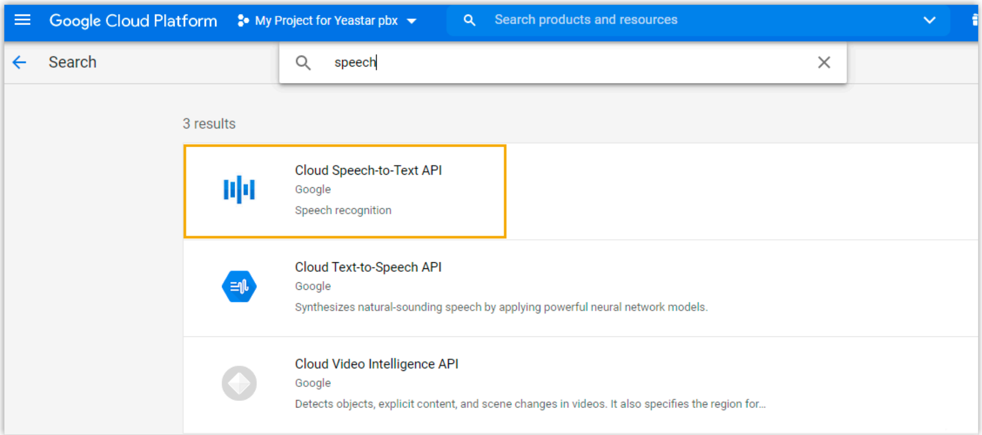
A new project is created, you can select the new project in the project list.

Step2. Enable Speech-to-Text API service on Google Cloud Platform

1. In the top-left conner, click ☰ to open the navigation menu, and go to API & Services > Dashboard.
2. Click ENABLE APIS AND SERVICES.



3. In the API Library, enter `speech` in the search box and select Cloud Speech-to-Text API.



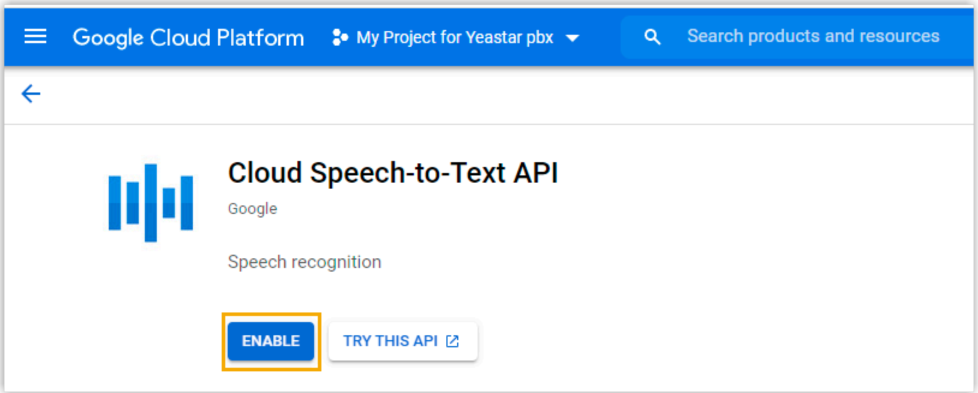
3 results

Cloud Speech-to-Text API
Google
Speech recognition

Cloud Text-to-Speech API
Google
Synthesizes natural-sounding speech by applying powerful neural network models.

Cloud Video Intelligence API
Google
Detects objects, explicit content, and scene changes in videos. It also specifies the region for...

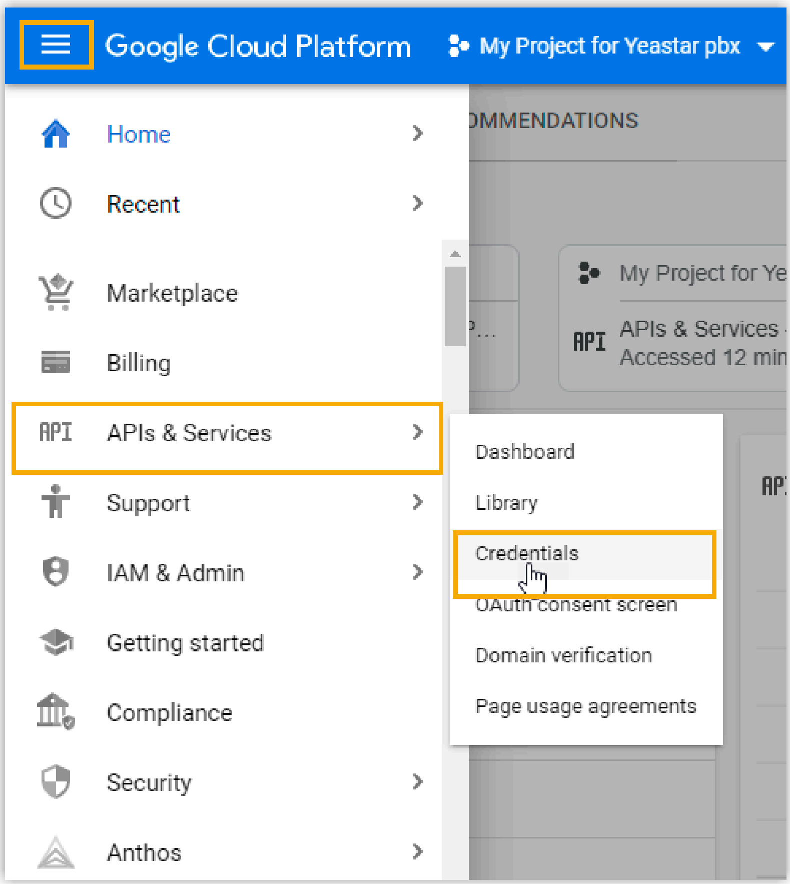
4. Click ENABLE button for the Cloud Speech-to-Text API.



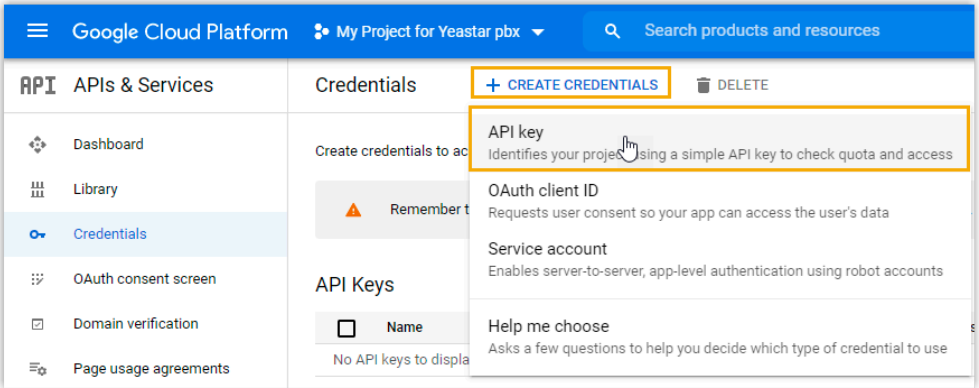
The Speech-to-Text service is enabled.

Step3. Create API credentials on Google Cloud Platform

1. In the left navigation panel, go to API & Services > Credentials.

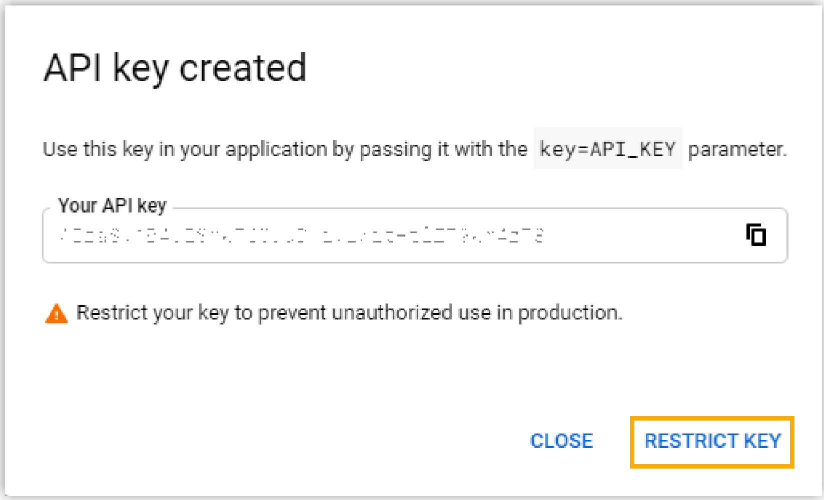


2. Click CREATE CREDENTIALS and select API key.


Google Cloud Platform
My Project for Yeastar pbx
Search products and resources
APIs & Services
Dashboard
Library
Credentials
OAuth consent screen
Domain verification
Page usage agreements
Credentials
+ CREATE CREDENTIALS
DELETE
Create credentials to ac
Remember t
API Keys
Name
No API keys to displa
API key
Identifies your project using a simple API key to check quota and access
OAuth client ID
Requests user consent so your app can access the user's data
Service account
Enables server-to-server, app-level authentication using robot accounts
Help me choose
Asks a few questions to help you decide which type of credential to use

3. In the pop-up window, click RESTRICT KEY.

Important:
For security purpose, you need to restrict your API key, ensuring only authorized requests are made with your API key.



API key created

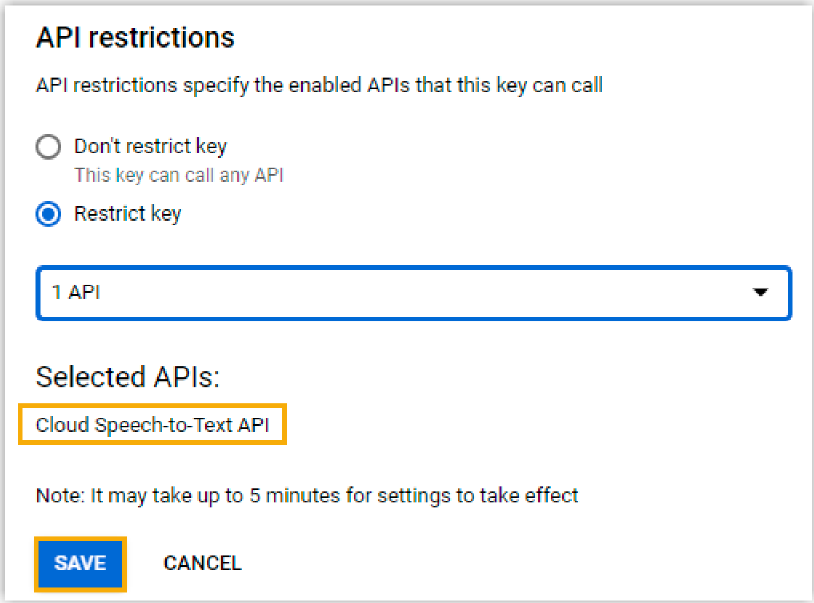
Use this key in your application by passing it with the `key=API_KEY` parameter.

Your API key

[redacted]

⚠ Restrict your key to prevent unauthorized use in production.

4. On the Restrict and rename API key page, complete the following configurations.
   a. In the Name field, specify the API key name.
   b. In the Application restrictions section, select None.
   c. In the API restrictions section, select Restrict key.
   d. Enter `speech` in the search box below to search and select the Cloud Speech-to-Text API, then click OK.
   e. Click Save to apply your configuration.



API restrictions

API restrictions specify the enabled APIs that this key can call

○ Don't restrict key
This key can call any API

● Restrict key

1 API

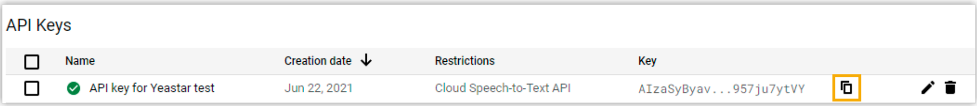
Selected APIs:

Cloud Speech-to-Text API

Note: It may take up to 5 minutes for settings to take effect

The API key is only allowed to call the Cloud Speech-to-Text API.

5. Go back to the Credentials page, in the API key section, click ⧉ to copy the restricted API key.

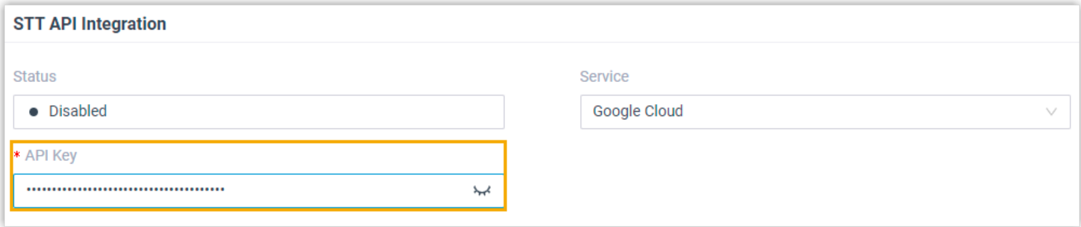


API Keys

□	Name	Creation date ↓	Restrictions	Key
□	✓ API key for Yeastar test	Jun 22, 2021	Cloud Speech-to-Text API	AIzaSyByav...957ju7ytVY

Enable Speech to Text (STT) integration on Yeastar P-Series Software Edition

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.

   STT API Integration

   Status: ● Disabled

   Service: Google Cloud

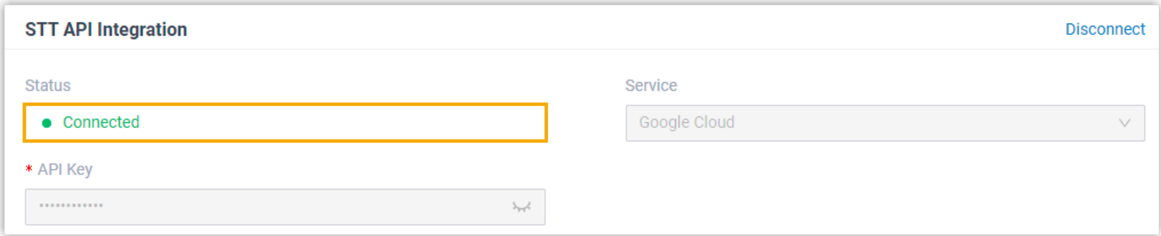
   * API Key: ••

3. In Settings section, select the transcription language.

   The audio messages will be transcribed to text in the selected language.

   Note:
   If the language of voicemail is different 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.

   STT API Integration

   Status: ● Connected

   Service: Google Cloud

   * API Key: ••••••••••••

What to do next

After the STT API integration succeeds, go to Call Features > Voicemail > Voicemail Settings to enable the Voicemail Transcription feature. For more information, see Enable or Disable Voicemail Transcription.

Related information

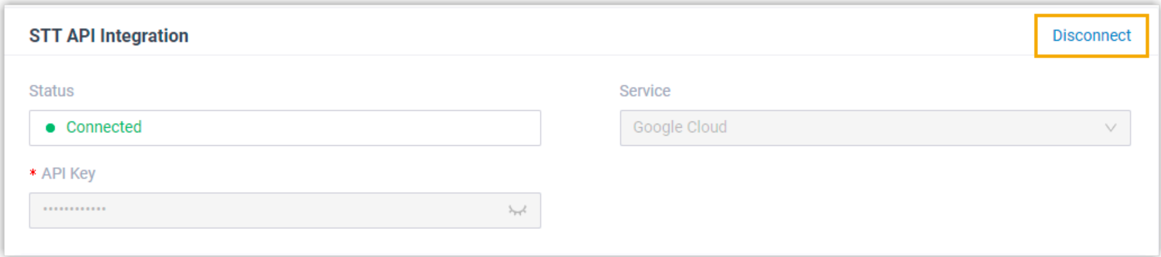
Speech to Text (STT) Overview
Disconnect Speech to Text (STT) API Integration

Disconnect Speech to Text (STT) API Integration

After the STT API integration is connected, you can directly disconnect the API service on PBX if you don't need the Speech to Text feature any more, or want to pause the API service.

Procedure

1. Log in to PBX web portal, go to Integrations > Speech to Text.
2. In the STT API Integration section, click Disconnect in the top-right corner.



STT API Integration

Disconnect

Status: ● Connected

Service: Google Cloud

* API Key: ••••••••••••

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 Software Edition supports AMI that allows you to connect an AMI client to Yeastar P-Series Software Edition.

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 Software Edition 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 Software Edition 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 Software Edition

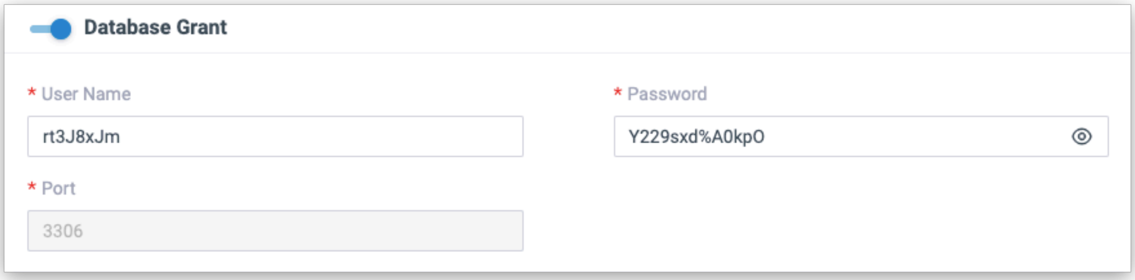
Yeastar P-Series Software Edition allows you to access the system database and get CDR data. This topic describes how to get CDR data from the PBX database via Navicat software.

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.



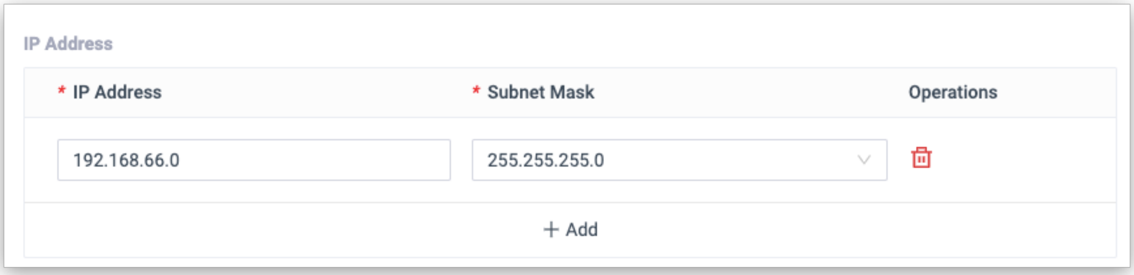
Database Grant

* User Name: rt3J8xJm

* Password: Y229sxd%A0kpO

* Port: 3306

   - User Name: Use the randomly generated user name or change the name.
   - Password: Use the randomly generated password or change password.
   - Port: Default port is 3306 and is unchangeable.
3. In the Permitted IP section, configure which IP addresses are allowed to access the database.



IP Address

* IP Address	* Subnet Mask	Operations
192.168.66.0	255.255.255.0	🗑

a. Click Add.
b. Enter the permitted IP address and subnet mask.

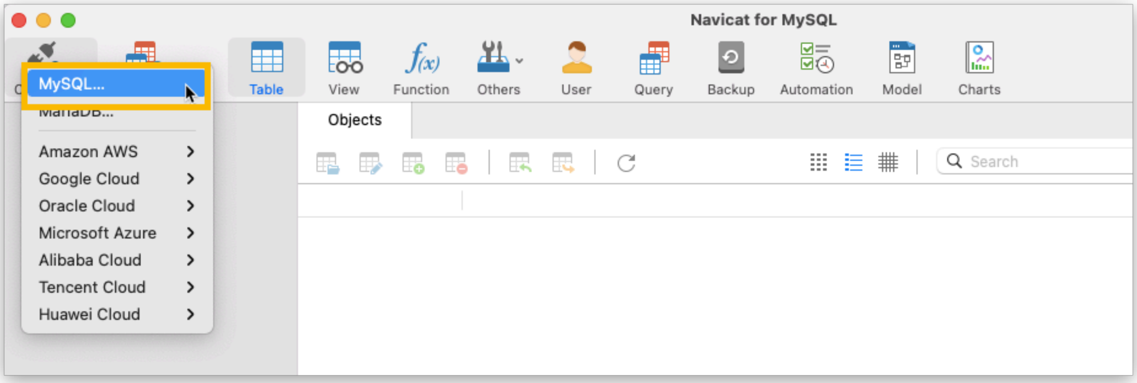
   In this example, enter IP address `192.168.66.0` and subnet mask `255.255.255.0` to allow all IP addresses in the segment 192.168.66.X to access the database.

   > 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`.

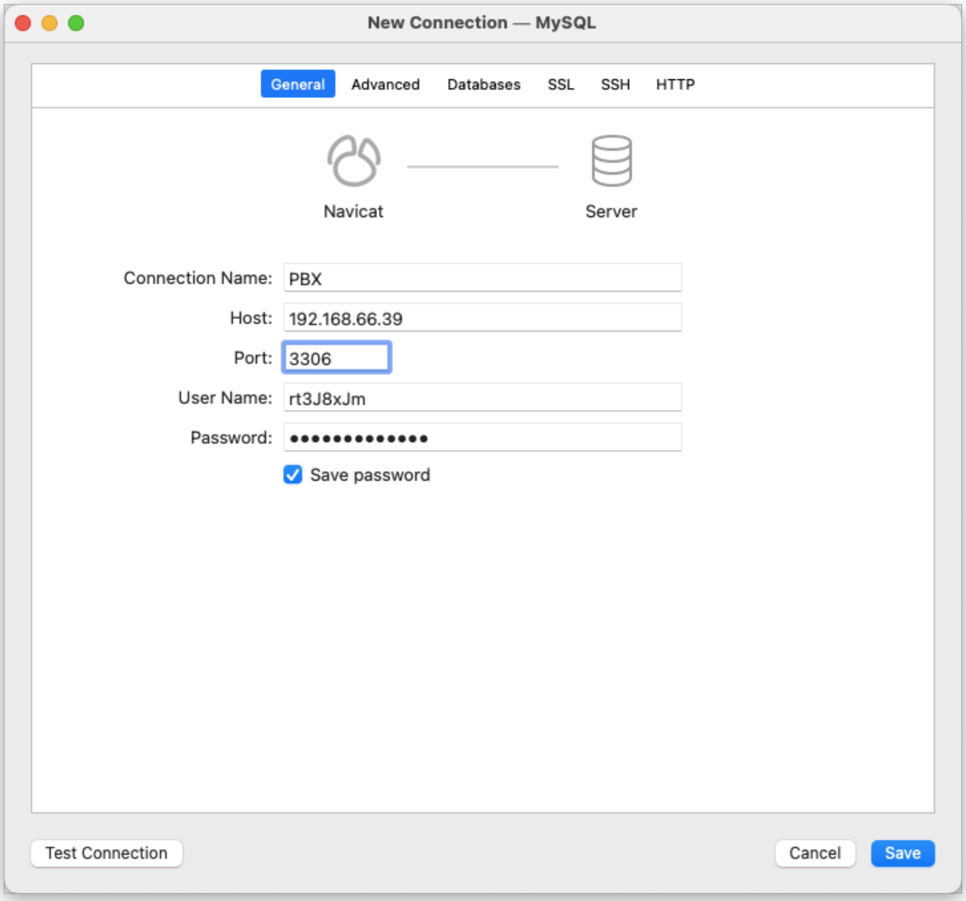
4. Click Save and Apply.

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: PBX

Host: 192.168.66.39

Port: 3306

User Name: rt3J8xJm

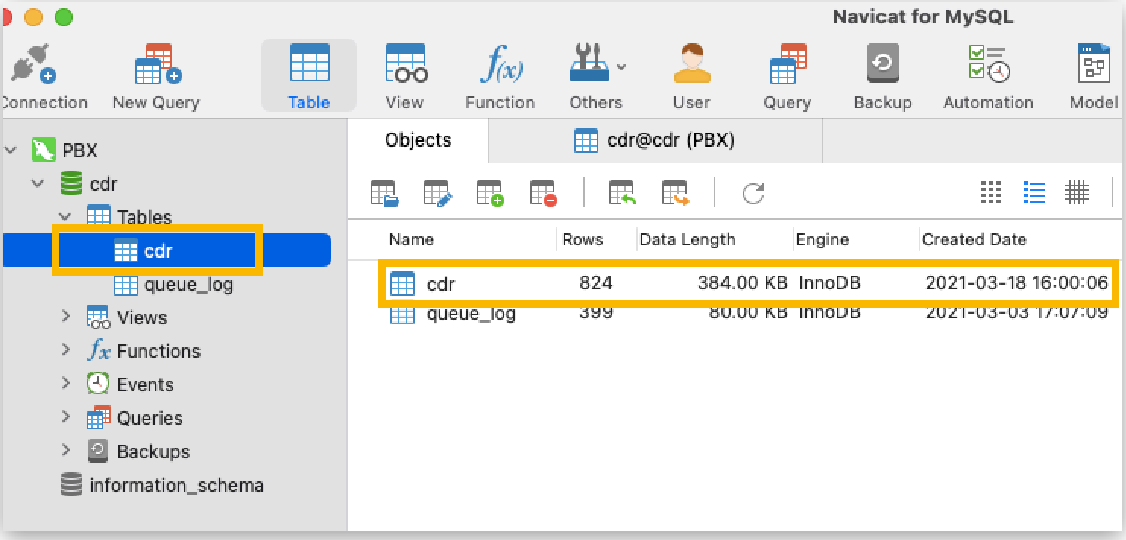
Password: ●●●●●●●●●●●●●●

☑ Save password

- 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.



Name	Rows	Data Length	Engine	Created Date
cdr	824	384.00 KB	InnoDB	2021-03-18 16:00:06
queue_log	399	80.00 KB	InnoDB	2021-03-03 17:07:09

cdr Table in the PBX Database

This topic describes details of cdr table stored in the database of Yeastar P-Series Software Edition.

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	System internal flag
uniqueid	System internal flag
didnumber	DID number
dodnumber	DOD number
recordfile	Recording file name
recordpath	Recordings path (with file name)
srcchanurl	Caller's SIP URI
dstchanurl	Callee's SIP URI
reasonpartya	System internal flag
reasonpartyb	System internal flag

Field	Descriptions
reasonpartyc	System internal flag
reasonpartyd	System internal flag
reasonpartye	System internal flag
reasonpartyf	System internal flag
displayonweb	System internal flag
src_del_cdr	System internal flag
dst_del_cdr	System internal flag
src_del_recording	System internal flag
dst_del_recording	System internal flag
srcnameprefix	System internal flag
dstnameprefix	System internal flag
misscall_isread	System internal flag
in2outbound	System internal flag
concurrentcalls	System internal flag
videocall	System internal flag
rascall	System internal flag
tryvideocall	System internal flag

Refereneces

System Capacity Comparison

This topic gives a comparison on the maximum value of the system capacity in different firmware versions.

Table 74.

Feature	Versions earlier than v83.6.0.63	v83.6.0.63 and the later version
Extension and Trunk		
Extension	500	10,000
Concurrent Call	125	1000
SIP Trunk	500	500 (extensions < 1000) 2000 (extensions ≥ 1000)
Contacts		
Company Contacts (total)	200,000	200,000 (extensions < 1000) 500,000 (extensions ≥ 1000)
Company Phonebooks	200	200 (extensions < 1000) 500 (extensions ≥ 1000)
Personal Contacts (per extensions)	100	100 (extensions < 1000) 500 (extensions ≥ 1000)
Call Control		
Inbound Route	500	500 (extensions < 1000) 1000 (extensions ≥ 1000)
Outbound Route	500	500 (extensions < 1000) 1000 (extensions ≥ 1000)
AutoCLIP Route list	100,000	100,000
Call Features		
IVR	64	64 (extensions < 1000)

Table 74. (continued)

Feature	Versions earlier than v83.6.0.63	v83.6.0.63 and the later version
		128 (extensions ≥ 1000)
Ring Group	32	32 (extensions < 1000) 128 (extensions ≥ 1000)
Queue	32	32 (extensions <1000) 128 (extensions ≥ 1000)
Conference	32	32 (extensions < 1000) 128 (extensions ≥ 1000)
Speed Dial Number	1024	1024
Paging Group	32	32 (extensions < 1000) 128 (extensions ≥ 1000)
PIN List	64	64 (extensions < 1000) 128 (extensions ≥ 1000)
Block Number List	256	256 (extensions < 1000) 512 (extensions ≥ 1000)
Allowed Number List	256	256 (extensions < 1000) 512 (extensions ≥ 1000)
PBX Settings		
MOH Playlist	32	32
Files per MOH Playlist	8	8
Custom Prompts	128	128
System		
Static Routes	500	500
Event Notification Contact	10	10
Network Drive	2	2
CDR Auto Cleanup	1,000,000	1,000,000 (extensions < 1000) 10,000,000 (extensions ≥ 1000)
Maintenance		

Table 74. (continued)

Feature	Versions earlier than v83.6.0.63	v83.6.0.63 and the later version
Backup and Restore	16	16
Video Conferencing		
Max. Duration per Video Meeting	120 min.	120 min.
Max. Participants per Video Meeting	5	5
Concurrent Meetings in PBX Server	4	4 (extensions ≤ 500) 8 (500 < extensions ≤ 3000) 10 (3000 < extensions ≤ 10,000)
Chat		
Group Chats Created (per extension)	100	100
Max. Group Members	200	200

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 Software Edition 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 Software Edition 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
- Speed Dial Number Parameters
- Emergency Number Parameters
- Trunk Parameters
- Trunk DIDs/DDIs Parameters
- Trunk Outbound Caller ID Parameters
- Inbound Caller ID Reformatting Rule Parameters
- Inbound Route Parameters
- Outbound Route Parameters
- Static Defense Rule Parameters
- Auto Defense Rule Parameters
- Outbound Call Frequency Restriction Rule Parameters
- 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

Parameter	Description	Importance	Restriction	Default Value
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: User Password will be generated randomly if you leave this field empty.	Generate Randomly
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 `/`. 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 "Sup-	Root organization, namely the Company Name.

Parameter	Description	Importance	Restriction	Default Value
			port 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 7.	N/A
Caller ID	The caller ID that is displayed on the callee's device.	Required	Numbers, letters, and special characters ( ) . - + * # are allowed. The maximum character length is 31. Note: Caller ID will be filled with default value Extension Number if you leave this field empty.	Extension Number
Registration Name	The registration name that is used to validate extension registration.	Required	The maximum character length is 63. Note: Registration Name will be generated randomly if you leave this field empty.	Generate Randomly

Parameter	Description	Importance	Restriction	Default Value
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. 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
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

Parameter	Description	Importance	Restriction	Default Value
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
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
After Notification	The way to handle voicemail message in mailbox after receiving the message	Required if Enable Voicemail = 1 & New Voicemail No-	Permitted value: • no: Do Nothing • mark_read: Mark as read • delete: Delete Voicemail	no

Parameter	Description	Importance	Restriction	Default Value
	notification via email.	tification = with_attach	Note: After Notification will be filled with default value no if you leave these fields empty.	
		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
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 be-	Required if Enable Voicemail = 1	Permitted value: • 0: Disable • 1: Enable	0

Parameter	Description	Importance	Restriction	Default Value
	fore playing the voicemail message.		Note: Play Message Duration will be filled with default value 0 if you leave this field empty.	
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: Send email notifications on missed calls will be filled with default value 0 if you leave this field empty.	0
Allow the extension to view recordings	Whether to allow users to view and manage their own recordings.	Required	Permitted value: • 0: Disable • 1: Enable Note: Allow the extension to view recordings will be filled with default value 1 if you leave this field empty.	1
Recording operation	Whether to allow users to switch their own recording	Required	Permitted value: • 0: No permission • 1: Pause/Resume	0

Parameter	Description	Importance	Restriction	Default Value
	status during a call.		• 2: Start/Pause/Resume Note: Recording operation will be filled with default value 0 if you leave this field empty.	
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
Call Popup URL	Whether to automatically open a custom URL (web page) upon receiving an incoming call.	Required	Permitted value: • 0: Disable • 1: Enable Note: Call Popup URL will be filled with default value 0 if you leave this field empty.	0
Popup URL	The address of third-party URL, followed by the variables that you want to pass.	Required if Call Popup URL = 1	The maximum character length is 255.	http://example.com/somepage.php?number={{.CallerNumber}}&name={{.CallerDisplayName}}
Communication type	The types of calls that will trigger the call popup.	Required if Call Popup URL = 1	Permitted value: Internal and Inbound. • For multiple types, enter values in order and use &	Inbound

Parameter	Description	Importance	Restriction	Default Value
			as a separator, e.g. Internal & Inbound. - If the value you enter is not permitted, it will be skipped.	
Trigger Event	When the call popup will be automatically triggered.	Required if Call Popup URL = 1	Permitted value: Ringing, Answered, and Call End. Note: Trigger Event will be filled with default value Ringing if you leave the field empty.	Ringing
Allow Being Monitored	Whether to allow the user's calls to be monitored.	Required	Permitted value: - 0: Disable - 1: Enable Note: Allow Being Monitored will be filled with default value 1 if you leave this field empty.	1
DTMF Mode	The mode for sending DTMF tones.	Required	Permitted value: rfc4733, info, inband or auto. Note: DTMF Mode will be filled with default value rfc4733 if you leave this field empty.	rfc4733
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 de-	Required	Permitted value: - 0: Disable - 1: Enable	1

Parameter	Description	Importance	Restriction	Default Value
	vice to check if the device is online.		Note: Qualify will be filled with default value1 if you leave this field empty.	
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
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:	0

Parameter	Description	Importance	Restriction	Default Value
			Allow Remote Registration will be filled with default value 0 if you leave this field empty.	
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 value 0 if you leave this field empty.	0
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	N/A

Parameter	Description	Importance	Restriction	Default Value
			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.	
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 with default value -1 if you leave these fields empty.	-1
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	Required	Permitted value: - 0: Disable - 1: Enable	1

Parameter	Description	Importance	Restriction	Default Value
	log in to Linkus Mobile Client.		Note: Linkus Mobile Client will be filled with default value 1 if you leave this field empty.	
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
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

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.	N/A

Parameter	Importance	Restriction	Default Value
		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`.	

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. 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.

Parameter	Importance	Restriction
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.

Parameter	Importance	Restriction
		For multiple phonebooks, enter the names and use & as a separator, e.g. phonebook_name1&phonebook_name2. Note: • 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

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. Emergency number cannot be duplicated.	N/A
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

Related information

Export and Import Emergency Numbers

Import and Export -FAQ

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	R
Name	The trunk name.	Required	The maximum character len Space and special character Trunk's name cannot be dup
Trunk Status	Whether to enable or disable the trunk.	Required	Permitted value: • 0: Disable • 1: Enable Note: Trunk Status will be filled wi field empty.
Trunk Type	Trunk type.	Required	Permitted value: • peer • register Note: • Importing Account Tru • Trunk Typewill be fillec leave this field empty.
Transport	The transport protocol that is provided by the ITSP.	Required	Permitted value: udp, tcp, tls Note: Transport will be filled with c fields empty.
Hostname/IP	The IP address or the domain of the ITSP.	Required	The maximum character len
Port	The trunk port.	Required	Only numbers between 0 anc
Domain	The domain in SIP URI of a specific header like From, To header. Note:	Required	The maximum character len

Parameter	Description	Importance	R
	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 len
Password	The password that is associated with the username.	Required if Trunk Type = register	The maximum character len
Authentication Name	The authentication name to register to the ITSP.	Optional	The maximum character len
Enable Outbound Proxy	Whether to enable or disable outbound proxy.	Required if Trunk Type = register	Permitted value: • 0: Disable • 1: Enable Note: Enable Outbound Proxy will l leave this field empty.
Outbound Proxy Server	The address of outbound proxy server.	Required if Enable Outbound Proxy = 1	The maximum character len
Port of Outbound Proxy Server	The port of outbound proxy server.	Required if Enable Outbound Proxy = 1	Only numbers between 1 anc
Codec Setting	The audio codec for trunk.	Required	Permitted value: ulaw, alaw, g722, g726, speex, adpcm, v For multiple Codec, please e separator, e.g. first_value1&s Note: If the value you enter is not p skipped.
DTMF Mode	The default mode for sending DTMF tones.	Required	Permitted value: rfc4733, inf Note: DTMF Mode will be filled wit this field empty.
DTMF FMTP	The value of the DTMF fmtp attribute when the DTMF mode is rfc4733.	Optional	Permitted value: 0-16, 0-15.

Parameter	Description	Importance	R
			Note: This field will be filled with d field 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 def empty.
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 wi field 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 filled wi field empty.
Inband Progress	Whether to enable or disable inband progress.	Required	Permitted value: • 0: Disable • 1: Enable Note: Inband Progress will be fillec field empty.
Ignore 183 Message without SDP	Whether to ignore 183 messages without SDP.	Required	Permitted value: • 0: Disable

Parameter	Description	Importance	R
			- 1: Enable Note: Ignore 183 Message withou 0 if you leave this field empt
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 len Note: Maximum Concurrent Calls you 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 o Note: Call Restriction Type will be you leave this field empty.
Default Outbound Caller ID	The caller ID that is displayed on the callee's device.	Optional	Numbers, letters, and chara The maximum character len Note: The outbound caller ID shou
Default Outbound Caller ID Name	The caller ID name that is displayed on the callee's device.	Optional	The maximum character len
Get Caller ID From	Decide from which header field will the trunk retrieve Caller ID.	Required	Permitted value: - follow_system: [Follow - from: From - contact: Contact - rpid: Remote-Party-ID - pai: P-Asserted-Identit - ppi: P-Preferred-Identit Note: Get Caller ID From will be fil if you leave this field empty.

Parameter	Description	Importance	R
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 • to: To • invite: Invite • diversion: Diversion • rpid: Remote-Party-ID • pai: P-Asserted-Identity • ppi: P-Preferred-Identit • pcpid: P-Called-Party-II Note: Get DID From will be filled w 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 Call • trunk_user: Trunk User Note: Only available when Tr • trunk_def_outbcid: Tru • ext_outbcid: Extension • outrounter_outbcid: Ou • originator_cid: Originat • A customized value. Note: Fill in a desired value c length is 31. Only num *, # are allowed. Note: From User Part will be filled 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: Extensic • trunk_def_outbcid_nar

Parameter	Description	Importance	R
			• ext_outbcid_name: Ext Trunk • originator_cid_name: O • A customized value. Note: Fill in a desired value o length is 63. Note: From Display Name Part will you leave this field empty.
Diversion	Define the parameters included in the Diversion SIP header.	Optional	Permitted value: • default: [Default] • ext_cid: Extension Call • trunk_user: Trunk User Note: Only available when Tr • trunk_def_outbcid: Tru • ext_outbcid: Extension • outrounter_outbcid: Ou • originator_cid: Originat • A customized value. Note: Fill in a desired value o length is 31. Only num *, # are allowed. Note: Leave Diversion field empty meter with SIP INVITE packe
Remote-Party-ID	Define the parameters included in the Remote-Party-ID SIP header.	Optional	Permitted value: • default: [Default] • ext_cid: Extension Call • trunk_user: Trunk User

Parameter	Description	Importance	R
			Note: Only available when Tr • trunk_def_outbcid: Tru • ext_outbcid: Extension • outrounter_outbcid: Ou • originator_cid: Originat • A customized value. Note: Fill in a desired value c length is 31. Only num *, # are allowed. Note: Leave Remote-Party-ID field this parameter with SIP INVI
P-Asserted-Identity	Define the parameters included in the P-Asserted-Identity SIP header.	Optional	Permitted value: • default: [Default] • ext_cid: Extension Call • trunk_user: Trunk User Note: Only available when Tr • trunk_def_outbcid: Tru • ext_outbcid: Extension • outrounter_outbcid: Ou • originator_cid: Originat • A customized value. Note: Fill in a desired value c length is 31. Only num *, # are allowed. Note: Leave P-Asserted-Identity fie this parameter with SIP INVI

Parameter	Description	Importance	R
P-Preferred-Identity	Define the parameters included in the P-Preferred-Identity SIP header.	Optional	Permitted value: • default: [Default] • ext_cid: Extension Call • trunk_user: Trunk User Note: Only available when Tr • trunk_def_outbcid: Tru • ext_outbcid: Extension • outrounter_outbcid: Ou • originator_cid: Originat • A customized value. Note: Fill in a desired value c length is 31. Only num *, # are allowed. Note: Leave P-Preferred-Identity fi this parameter with SIP INVI
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 len
Realm	Realm is a string displayed to users so they know which username and password to use.	Optional	The maximum character len
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 the header field of the SIP INVITE packet.	Required	Permitted value: • 0: Disable • 1: Enable
100rel	Whether to support 100rel or not.	Required	Permitted value:

Parameter	Description	Importance	R
			• 0: Disable • 1: Enable
Maxptime	Select the value of the Maxptime used when the PBX sends the INVITE packet.	Required	Permitted value: • default: PBX will send cording to the codec th • A customized value. Note: Fill in a desired value c ple of 10 ranging from Note: Maxptime will be filled with c 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

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.

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	Optional	The maximum character length is 127.	N/A

Parameter	Description	Importance	Restriction	Default Value
	to identify 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.	N/A

Parameter	Description	Importance	Restriction	Default Value
			• Then fill the extension range in Associated Extensions. The extension range and the outbound caller ID range must have the same amount of numbers.	
Outbound Caller ID Name	The caller ID that is displayed on the callee's device for specific extensions.	Optional	The maximum character length is 127.	N/A
Associated Extensions	The extensions that are associated with the Outbound Caller ID and Outbound Caller Name.	Required	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

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

Parameter	Description	Importance	Restriction	Default Value
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 Note: DID Matching Mode will be filled with default value patterns if you leave these fields empty.	patterns
DID Pattern	The DID pattern that is used to match callee number. Only when the callee number is matched will the inbound call go through this route.	Required if DID Matching Mode ≠ patterns	• If DID Matching Mode = patterns, you can enter one or more patterns. Numbers, letters X Z N, and characters [ ] * # ( ) . - + ! are allowed. The maximum character length is 31 (for each DID). Please use & as a separator for multiple patterns, e.g. 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 charac-	N/A

Parameter	Description	Importance	Restriction	Default Value
			ter + (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 end number with separator - in Number, e.g. 1001-1005.	
Caller ID Matching Mode	The Caller ID matching mode.	Required	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	• 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	N/A

Parameter	Description	Importance	Restriction	Default Value
			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) • pattern_to_ext: Match selected Extension (DID Matching Mode = pattern_to_ext) • ext_vm: Extension Voicemail • group_vm: Group Extension • ivr: IVR • ring_group: Ring Group • queue: Queue • conference: Conference	end_call

Parameter	Description	Importance	Restriction	Default Value
			• 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	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&extension_number2&extension_group_name3. Note: If the numbers or names you enter are not existing in PBX, Number of Default Destination will be skipped.	N/A

Parameter	Description	Importance	Restriction	Default Value
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 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 X Z N, and characters [ ] * # ( ) . - + ! are allowed. The maximum character length is 31. Note: Pattern will be filled with default value X. if you leave these fields empty.	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
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	Required	Permitted value: one or more trunk names existed in PBX. For multiple trunks, please enter trunk names and	N/A

Parameter	Description	Importance	Restriction	Default Value
	number matches the outbound route.		use & as a separator, e.g. name1&name2. Note: If the trunk you enter does not exist in PBX, it will be skipped.	
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, `Organization_Yeastar/Marketing Center/Training Team`. • For multiple extensions, extension	extension

Parameter	Description	Importance	Restriction	Default Value
			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 outbound calls through this route.	Required if Outbound Route Password is pin_list	Permitted value: The name of a PIN list existed in PBX. Note:	N/A

Parameter	Description	Importance	Restriction	Default Value
			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: • https • http • ssh • ftp • sip_udp • sip_tcp • sip_tls	N/A

Parameter	Description	Importance	Restriction	Default Value
			• outbound_sip • rtp • linkus	
Start Port	The start port.	Required if Service/Port Range = port_range	Only numbers between 1 and 65535 are allowed. Start port must be less than or equal to end port. 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, 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

Parameter	Description	Importance	Restriction	Default Value
			Service/Port Range will be filled with 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 • ftp • sip_udp • sip_tcp • sip_tls • outbound_sip • rtp • linkus	N/A
Start Port	The start port.	Required if Service/Port Range = port_range	Only numbers between 1 and 65535 are allowed. Start Port must be less than or equal to End Port. 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 a spe-	Required	Only numbers between 1 and 255 are allowed.	N/A

Parameter	Description	Importance	Restriction	Default Value
	cific 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 75.

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`. Variables:	N/A

Table 75. (continued)

Parameter	Description	Importance	Restriction	Default Value
			{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

Parameter	Importance	Restriction	Default Value
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. Only numbers 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 76.

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.	N/A

Table 76. (continued)

Parameter	Importance	Restriction	Default Value
		For multiple numbers or number patterns, use & as a separator, eg. number1&number2.	

Related information

[Import and Export -FAQ]

Blocked Numbers Parameters

Descriptions for parameters in exported and imported Blocked Numbers CSV files.

Table 77.

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