PROPOSTA DE PREÇOS

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO - DPRJ

Referência: PREGÃO ELETRÔNICO - PE 90009/2025

EMPRESA

Razão Social: CAM Tecnologia Ltda.

Inscrição Municipal: 0533626-0

CNPJ/MF: 14.438.757/0001-76

Inscrição Estadual: 86.603.969

Porte: Pequena Empresa

Regime: Simples Nacional

Endereço: Av. Pastor Martin Luther King Jr, nº 126

CEP: 20.765-000

Complemento: BL 9 Torre 2000, Sala 408

Cidade: Rio de Janeiro/RJ

E-mail: licitacao@camtecnologia.com.br

Tel/Fax: (21) 3189-1050

Banco: Itaú Agência: 0023 Nº. C/C: 22230-0

Dados do Representante Legal

Nome: Thiago Maluf Resende

CPF 103.068.457-09

Cargo: Sócio Proprietário

RG 113.214.589 DIC RJ

E-mail: thiago@camtecnologia.com.br

Tel: (21) 99700-9113

Dados do Responsável pela Proposta

Nome: Aline Hermes Klin

Cargo: Consultora Comercial

E-mail: aline.klin@camtecnologia.com.br

Tel: (11) 9 9600 8466

OBJETO

Contratação de empresa especializada para o fornecimento, configuração, manutenção de solução de central de atendimento (call center) para atendimento receptivo e ativo de telefonia, integrado aos bancos de dados da instituição, a fim de viabilizar o atendimento ao público da central de relacionamento com o cidadão, ouvidoria geral e service desk da secretaria de tecnologia da informação, incluindo o fornecimento de equipamentos do tipo headset e adaptador de áudio para o atendimento telefônico, bem como a gestão técnica completa

(configuração, monitoramento, manutenção e suporte) de equipamento gateway de propriedade da defensoria pública geral do estado do rio de janeiro (dprj).

ITEM	ESPECIFICAÇÃO	UF	QTD.	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
1	Solução de Call Center na modalidade SaaS (software como serviço) com hospedagem em nuvem (cloud).				
1.1	Locação de licenças de uso de software de Call Center (PBX-IP Virtual) com até 350 (trezentos e cinquenta) posições	Mensal	24	7,90	66.400,00
2	Equipamentos				
2.1	Fornecimento e manutenção de equipamento do tipo adaptador de áudio USB	Unidade	600	95,00	57.000,00
2.2	Fornecimento e manutenção de equipamento do tipo Headset	Unidade	1.200	106,00	127.200,00
3	Outros Serviços				
3.1	Banco de Horas de Consultoria	Horas	1.200	120,00	144.000,00
3.2	Serviço Continuado de Sustentação, Garantia e Suporte	Mensal	24	3.555,00	85.320,00
3.3	Treinamento de usuários gestores da solução de call center para até 20 pessoas	Serviço	1	5.118,80	5.118,80
3.4	Serviço de Operação Assistida	Mensal	1	4.561,20	4.561,20
3.5	Configuração, monitoramento, manutenção e suporte de equipamento Gateways com capacidade para até 16 (dezesseis)canais E1 de propriedade da DPRJ	Mensal	24	3.350,00	80.400,00
			VALOR TOTAL R$		**570.000,00**
(Quinhentos e setenta mil reais)					

O prazo de validade da proposta de preços é de 60 (sessenta) dias, contados da data da proposta.

Declaro que examinei, conheço e me submeto a todas as condições expressas na presente

contratação direta, bem como verifiquei todas as especificações contidas, não havendo quaisquer discrepâncias nas informações, nas condições de fornecimento e documentos que dele fazem parte dos serviços será de acordo com o estipulado no Termo de Referência.

Declaro que o preço ofertado compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes.

Declaro ainda que, estou ciente de todas as condições que possam de qualquer forma influir nos custos diretos ou indiretos, assumindo total responsabilidade por erros ou omissões existentes nesta proposta, bem como qualquer despesa relativa à realização integral de seu objeto.

Declaro que assumimos total responsabilidade pela manutenção, substituição, instalação e funcionamento integral dos equipamentos, fornecidos por nós, durante toda a vigência contratual.

Declaro que possuímos equipe técnica capacitada para o suporte e manutenção dos serviços fornecidos para este órgão.

Rio de Janeiro, 12 de dezembro de 2025.

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2025.12.12 11:57:29 -03'00'

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO - DPRJ

Referência: PREGÃO ELETRÔNICO - PE 90009/2025

DECLARAÇÃO DE EXEQUIBILIDADE

A CAM Tecnologia Ltda., inscrita no CNPJ nº 14.438.757/0001-76, por meio de seu representante legal infra-assinado, para fins de atendimento ao Edital Pregão Eletrônico nº 90009/2025, da Defensoria Pública do Estado do Rio de Janeiro, vem apresentar a presente DECLARAÇÃO DE EXEQUIBILIDADE, nos seguintes termos:

A proposta apresentada pela CAM é plenamente exequível, tendo em vista que a solução ofertada foi desenvolvida pela própria CAM em conjunto com a Yeastar, parceira tecnológica consolidada. Trata-se de uma solução já implantada e em plena operação em clientes da CAM, garantindo maturidade técnica, estabilidade e total aderência ao escopo definido no edital.

Toda a equipe técnica da CAM possui conhecimento avançado e experiência prática na implementação, operação, suporte e evolução desta solução, assegurando plena capacidade operacional para cumprir integralmente todas as exigências técnicas e prazos contratuais.

Ressalta-se ainda que a CAM possui sede na cidade Rio de Janeiro, o que reduz significativamente os custos de deslocamento quando necessário e contribui para a viabilidade econômica da proposta.

A solução ofertada é baseada em Asterisk, plataforma amplamente reconhecida e de código aberto, sem custos de licença, o que complementa a competitividade financeira da proposta sem comprometer qualidade, segurança e desempenho.

A CAM é uma Empresa de Pequeno Porte (EPP) optante pelo Simples Nacional, com estrutura tributária simplificada, o que permite otimização dos custos operacionais relacionados a pessoal, desenvolvimento, suporte e manutenção.

RACIONAL DE CUSTOS E LUCRATIVIDADE

O valor global ofertado de R$ 570.000,00 (quinhentos e setenta mil reais) para o período de 24 (vinte e quatro) meses foi estruturado a partir dos seguintes componentes:

- Custos operacionais diretos (mão de obra técnica, suporte especializado, monitoramento, gestão da solução): aproximadamente 55% do valor total.

- Custos de softwares, plataforma e infraestrutura de operação (incluindo manutenção da solução baseada em Asterisk, integrações, atualizações e suporte avançado): aproximadamente 25% do valor total.

- Locação de headsets e demais equipamentos operacionais relacionados ao escopo: aproximadamente 10% do valor total.

- Custos administrativos, deslocamentos presenciais quando necessários e despesas gerais: aproximadamente 5% do valor total.

- Margem de lucratividade prevista, compatível com o porte da empresa, riscos do projeto e natureza continuada dos serviços: aproximadamente 5% do valor total.

Essa composição garante que a proposta apresente sustentabilidade financeira, permitindo à CAM manter a qualidade, continuidade, disponibilidade técnica e atendimento integral das obrigações contratuais durante toda a vigência.

Por todo o exposto, a CAM declara que os valores apresentados são suficientes, coerentes e adequados para a perfeita execução do contrato, atendendo integralmente às especificações do edital e garantindo capacidade técnica, operacional e financeira para a plena prestação dos serviços durante os 24 meses previstos.

Termos em que,

Pede deferimento.

Rio de Janeiro, 12 de dezembro de 2025.

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2025.12.12 10:58:17 -03'00'

Yealink USB Wired Headset

UH34: Leather ear cushions UH34 Lite: Foamy ear cushions

The Yealink UH34/UH34 Lite, available in monaural (UH34/UH34 Lite Mono) and binaural (UH34/UH34 Lite Dual), is a professional USB wired headset with crystal clear audio. The UH34/UH34 Lite offers a lightweight form factor that is comfortable to wear, even for an entire workday. It's suitable for workers who spend a lot of time wearing headsets for voice communications. Provided with Yealink USB Connect software and Yealink Device Management Platform/ Cloud Service, you are easy to check the device information and upgrade the firmware of one or multiple UH34/UH34 Lite headsets.

UH34/UH34 Lite Mono Teams
UH34/UH34 Lite Mono UC

UH34/UH34 Lite Dual Teams
UH34/UH34 Lite Dual UC

Simple and Flexible Connectivity

Runs right out of box, a USB plug-and-play setup makes the connectivity to PC. You can enjoy a reliable call experience with soft clients. Perfect match with Yealink IP phones give you optimized audio quality.

Ultra-lightweight, All Day Wearing Comfort

Built for comfort with soft ear cushions and ultra-lightweight materials, the UH34/ UH34 Lite is 10%~30%* lighter than other headsets in the same range. Its ergonomic design makes this headset comfortable enough for long conference calls and all day use. (* Test data provided by Yealink Lab)

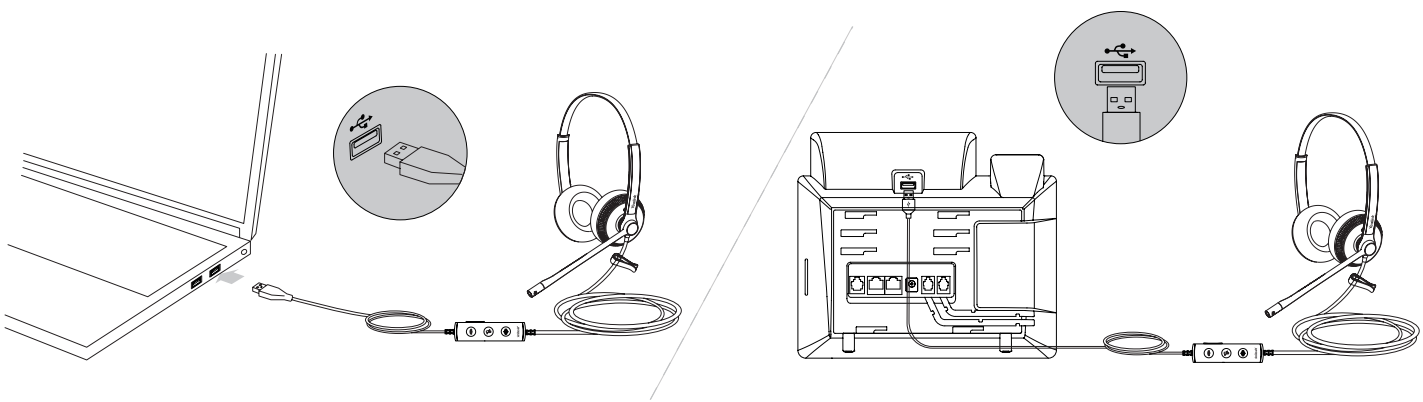
Unparallel Audio Experience

Made for calls and music, UH34/UH34 Lite is kitted out with a high signal-to-noise ratio speaker and independent cavity design. The passive noise cancellation creates a richer and clearer conversations with reduced background noise.

Intuitive Controller

The hand-held controller with LED indicator provides easier access to key call control capabilities, including answer call, end call, reject call, and mute/unmute.

Connection



* When you use UH34 in some uncertified communication platforms, as a minimum, it works as audio only.

Yealink

Specifications

Main Features

- Plug-and-play
  - USB connectivity to Yealink IP phones, including T41S/T42S/T46S/T48S/T42U/T43U/T46U/T48U/T53/T53W/T54W/T57W/T58A/VP59 (T41S/T42S/T46S/T48S should be upgraded to version 82 or higher)
- HD Voice/Wideband speaker performance
- Noise-canceling microphone and passive noise cancellation
- ActiveProtection technology safeguards users from acoustic injury
- Integrated LED indicator and warning tone
- 320° bendable boom arm for easy adjustment without breaking
- Optional connections for UH34: USB-C, 3.5mm jack

General

- Headset cable length: 1.2 m (from headset to call control unit)
- USB cable length: 0.9 m (from call control unit to USB plug)
- Supported operating systems:
  Microsoft Windows® 8/8.1/10, Apple Mac OS
- Color: Black
- Weight: UH34 Mono: 88 g / UH34 Dual: 118 g / UH34 Lite Mono: 84 g / UH34 Lite Dual: 110 g
- Storage temperature: -30 °C to +70 °C
- Operating temperature: -10 °C to +50 °C

Microphone

- Microphone type: Uni-Directional ECM
- Microphone frequency response range:
  100 Hz-8 kHz
- Microphone bandwidth: Wideband
- Microphone sensitivity: -44.0 dB re. 1 V/Pa

Speaker

- Speaker size: 28mm
- Speaker sensitivity: 93 dB SPL @1 kHz
- Speaker frequency response range: 20 Hz-20 kHz
- Speaker impedance: 32Ω, @1.0 kHz
- Speaker input power: max 10 mW
- Speaker bandwidth: Wideband

Easy Call Management

- Answer/End/Reject/Hold a call
- Volume up/down
- Microphone mute
- Redial last outgoing call

Package Features

- Package contents:
  - UH34 Mono Headset or UH34 Dual Headset or UH34 Lite Mono Headset or UH34 Lite Dual Headset
  (UH34 with leather ear cushions/UH34 Lite with foamy ear cushions)
  - Quick Start Guide
- Qty/CTN: 20 PCS
- N.W/CTN: UH34 Mono: 2.870 kg / UH34 Dual: 3.486 kg / UH34 Lite Mono: 2.790 kg / UH34 Lite Dual: 3.326 kg
- G.W/CTN: UH34 Mono: 3.576 kg / UH34 Dual: 4.202 kg / UH34 Lite Mono: 3.496 kg / UH34 Lite Dual: 4.042 kg
- Giftbox size: 170 mm*195 mm*63 mm
- Carton Meas: 345 mm*325 mm*400 mm

Compliance

CE FC IC

About Yealink

Yealink (Stock Code: 300628) is a global brand that specializes in video conferencing, voice communications and collaboration solutions with best-in-class quality, innovative technology and user-friendly experience. As one of the best providers in more than 140 countries and regions, Yealink ranks No.1 in the global market share of SIP phone shipments (Global IP Desktop Phone Growth Excellence Leadership Award Report, Frost & Sullivan, 2019).

Copyright

Technical Support

Visit Yealink WIKI (http://support.yealink.com/) for firmware downloads, product documents, FAQ, and more. For better service, we sincerely recommend you to use Yealink Ticketing system (https://ticket.yealink.com) to submit all your technical issues.

YEALINK(XIAMEN) NETWORK TECHNOLOGY CO., LTD.
Web: www.yealink.com
Addr: No.1 Ling-Xia North Road, High Tech Park,
Huli District, Xiamen, Fujian, P.R.C

Administrator Guide

Yeastar P-Series Software Edition

Version: 83.19.0.70
Date: 2025-06-09

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

Contents

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.

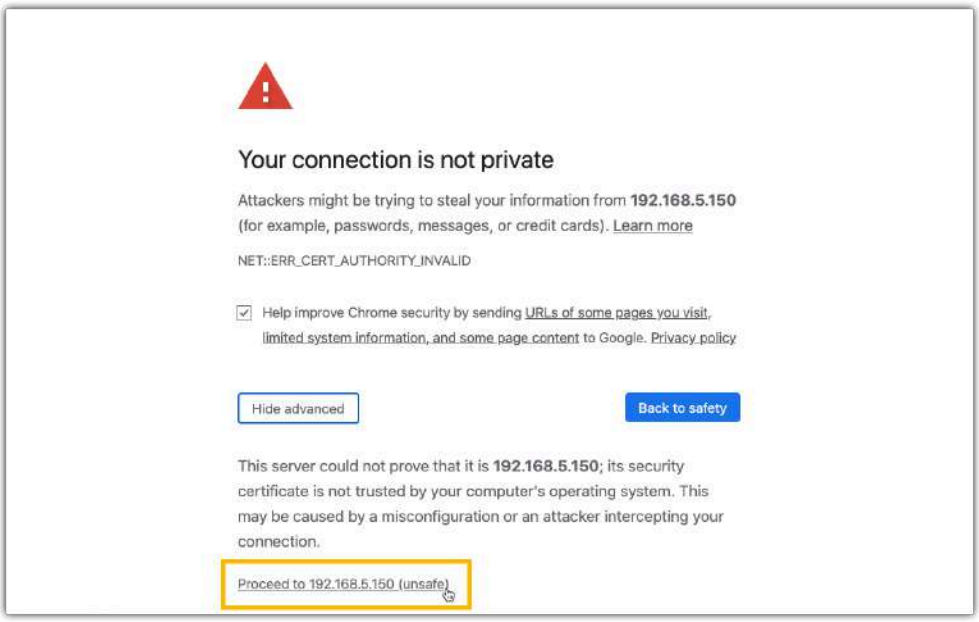
Procedure

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.

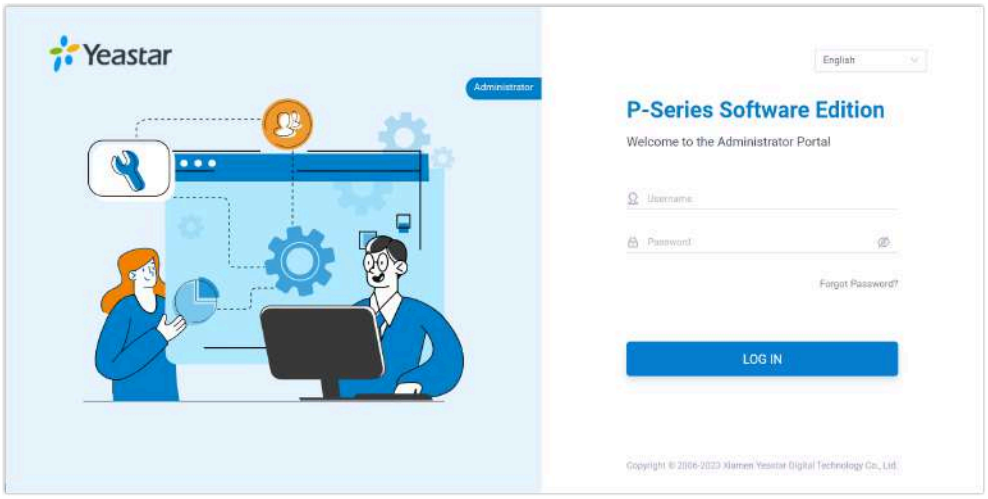
2. If a warning appears to remind you that the page is not secure, ignore the warning on the web page, expand the **Advanced** tab, and proceed to the PBX web.



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

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

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



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

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

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

c. Click **LOG IN**.

Log in to management portal

Prerequisite

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

Table 3.

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

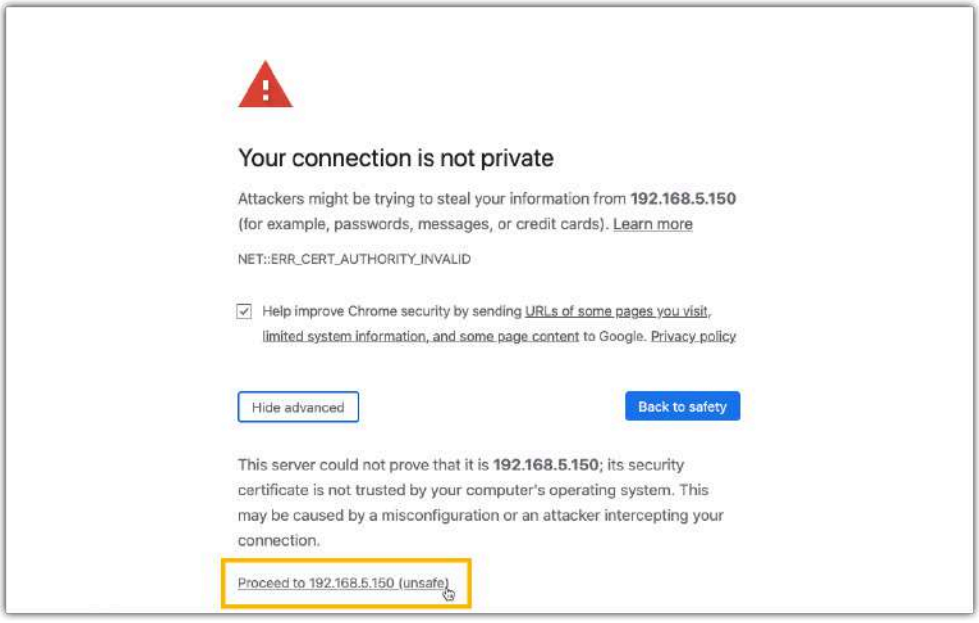
    - Support the resolution of 1366 x 768 or higher.
- If the PBX is installed on virtual machines or on-premise servers, make sure you have set the IP address of your PC.

  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.

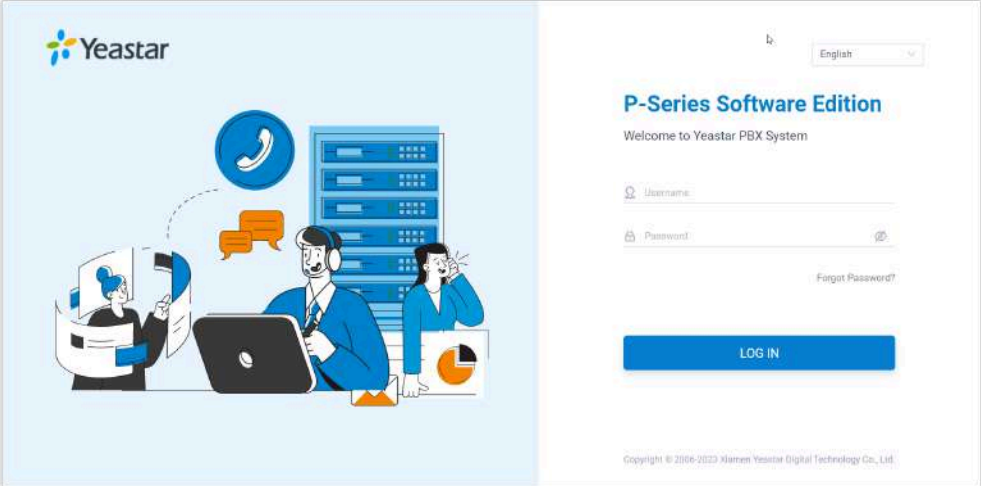
Procedure

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.



3. Enter the credential of the user account, then click **LOG IN**.

- **Username**: The **email address** or **extension number** of the user account.
- **Password**: The password of the user account.



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

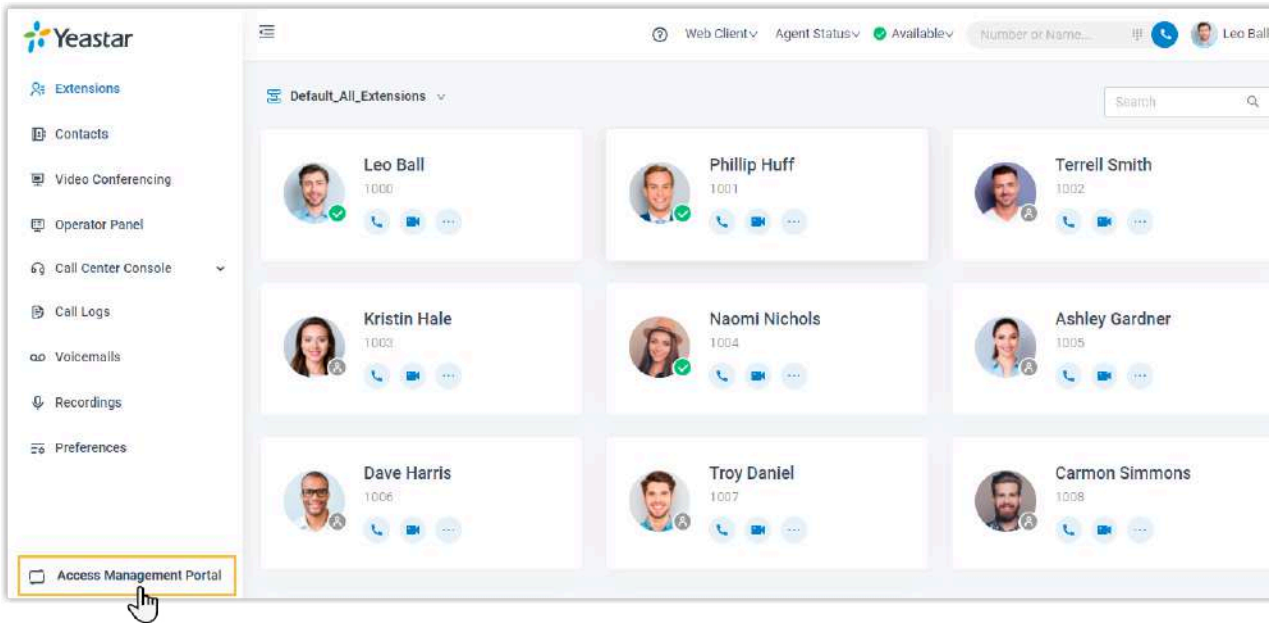
a. Enter the authentication code provided by an authenticator application or email.
b. **Optional:** Select the checkbox of **Trusted Device**.

> **Note:**
> For the device from which you log in most frequently, you can select the option to add it as a trusted device. In this

way, you don't have to re-enter an authentication code with this device for the next 180 days.

c. Click **LOG IN**.

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



Change the Password of Super Administrator

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

Background information

The username and password of super administrator are configured in Installation Wizard.

Important:

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

Procedure

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

Result

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

Reset the Password of Super Administrator

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

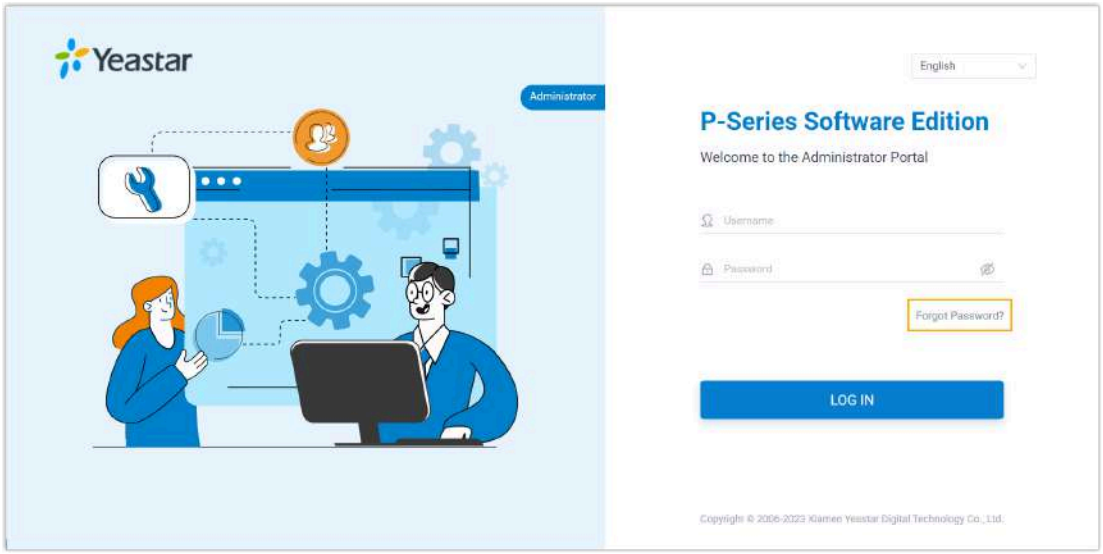
Prerequisites

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

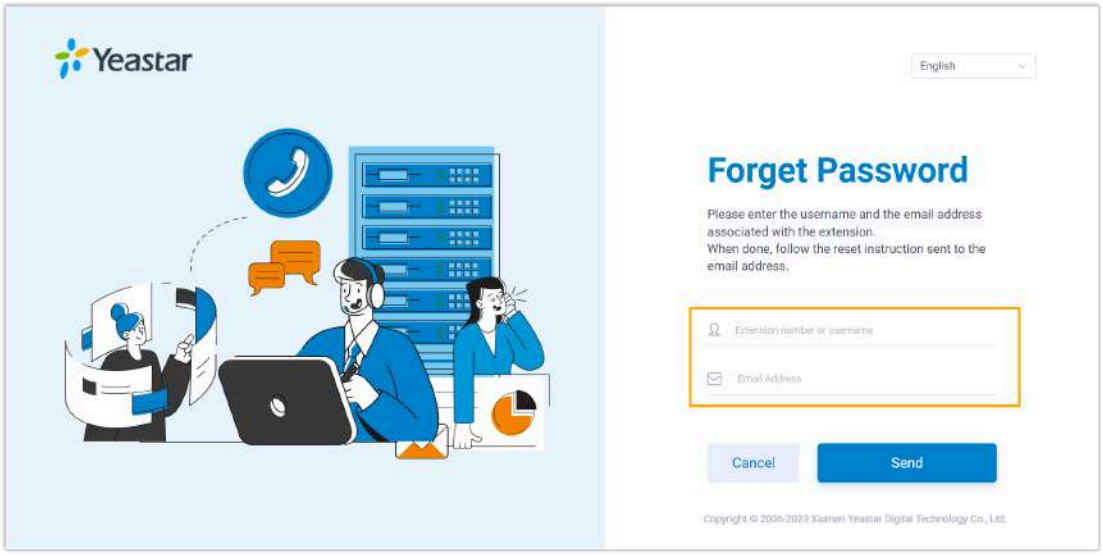
> **Important:**
> If you forget the username of super administrator, you need to reset the system to reconfigure a new username.

Procedure

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



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



3. Click **Send**.

   A password reset email is sent to super administrator's email address.
4. Check the password reset email, and click the link provided in the email to enter the **Reset Password** page.

Note:

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

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

Result

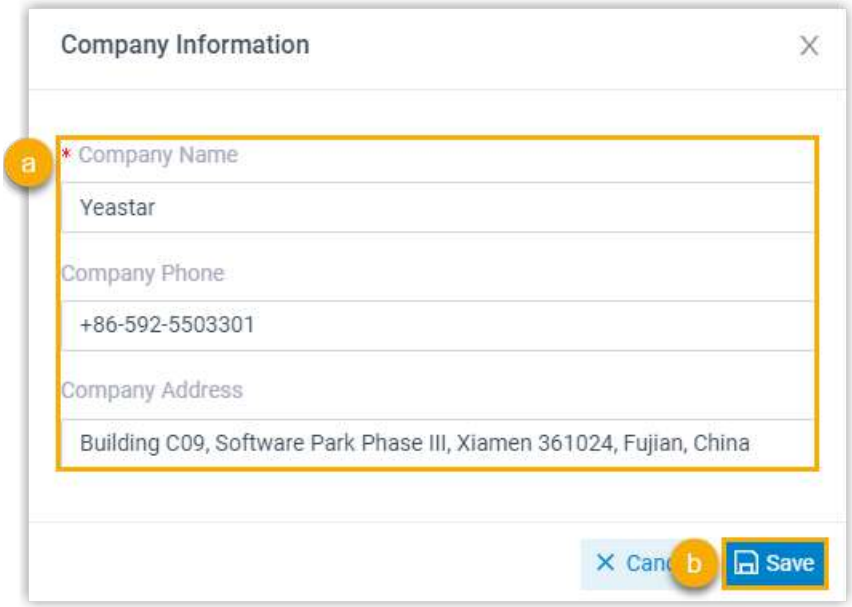
The password of super administrator is changed. You need to log in to PBX administrator portal by the new password next time.

Set up Company Information

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

Procedure

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



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

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

b. Click **Save**.

View System Information

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

Procedure

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

The following information is displayed:

- Network
- Device Name
- Product Model
- Serial Number
- 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

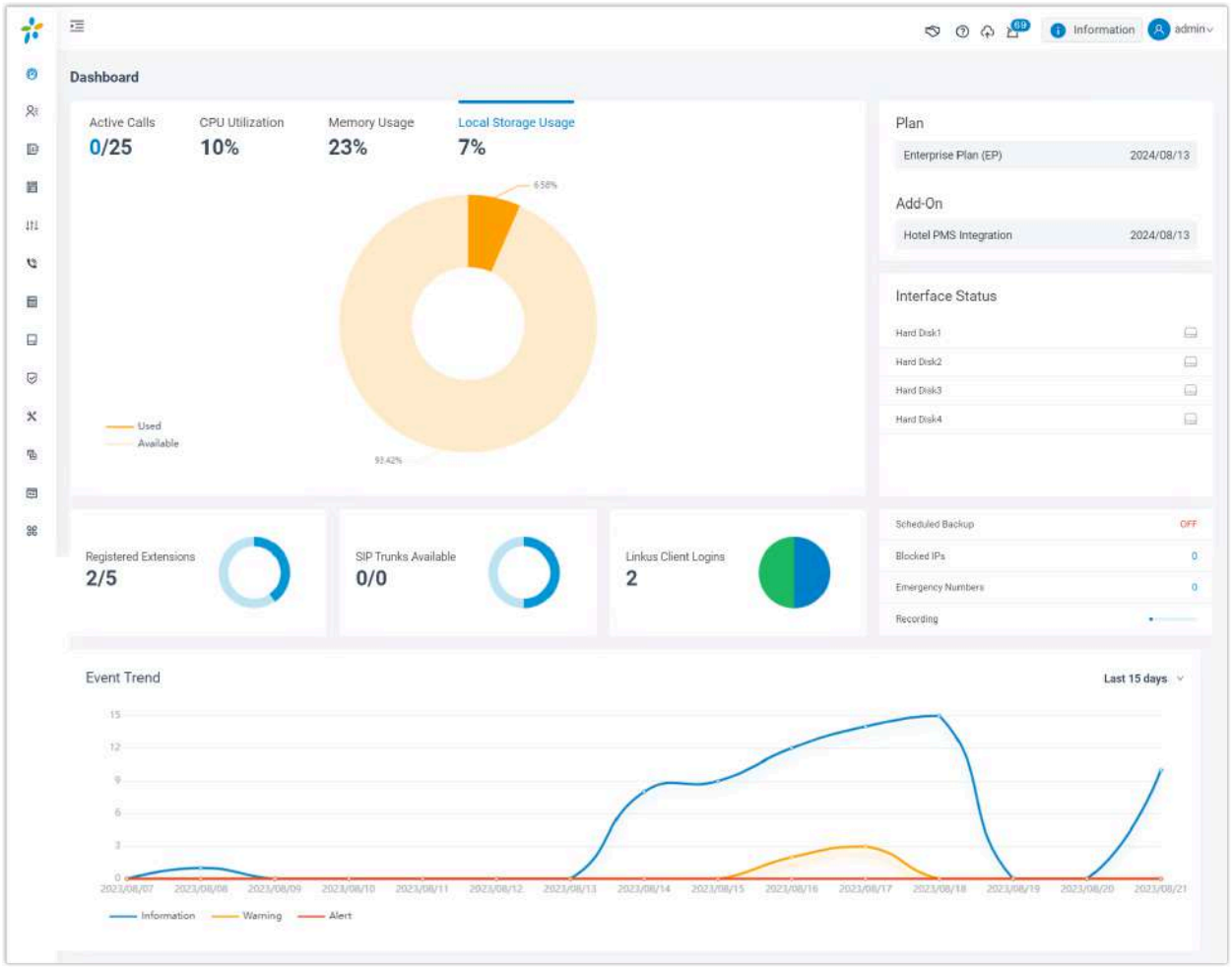
Yeastar P-Series Software Edition Dashboard gives you a historical and real-time view of what is happening on the PBX. This topic describes all the widgets on the Dashboard.

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
- Add-On
- Interface Status
- System status
- Event trend

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



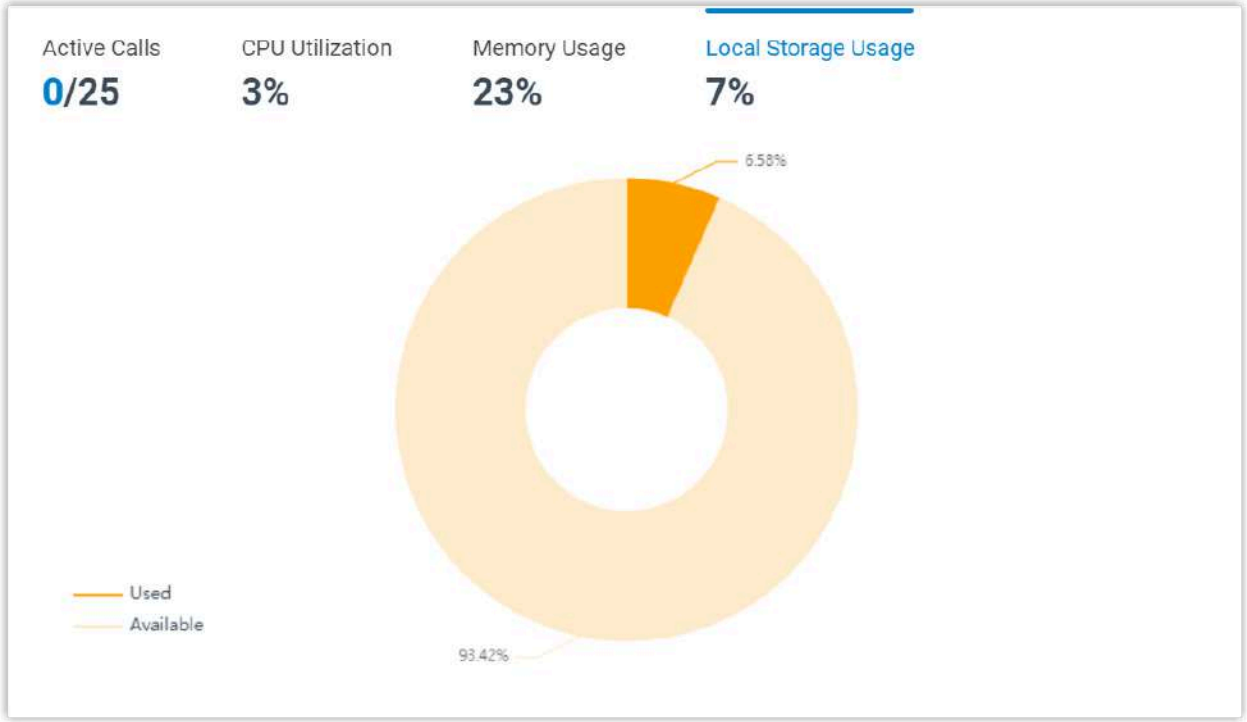
1. System performance
2. System information
3. Plan
4. Add-On
5. Interface status
6. System status
7. Event trend

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

System performance

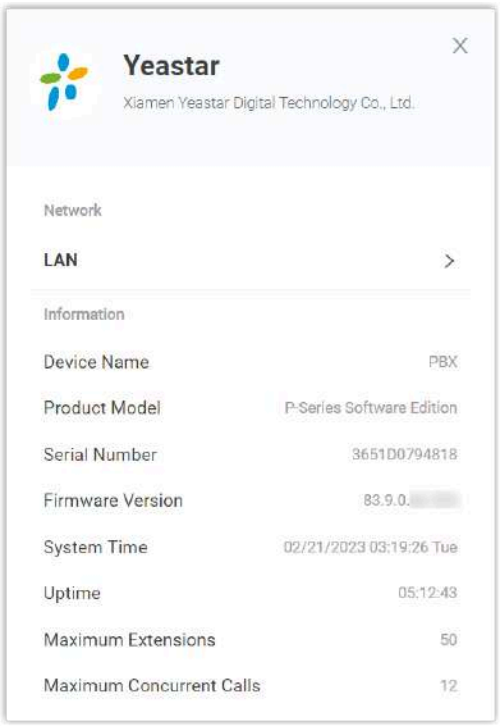
System performance displays the following information:

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



System information

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



Plan

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

Add-On

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

Interface status

Interface status displays connection status of 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.

System status

System status displays the following information:

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

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

Event trend

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

Extension

Extension Overview

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

Extension types

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

> **Note:**
> For security reasons, we recommend that you set a strong password. If you set weak passwords for these extensions, ⚠ will be displayed in front of these extensions on **Extension** page.

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

> **Note:**

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

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

     > **Tip:**
     > Configure voicemail notifications and play options according to your needs.

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

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

Result

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

What to do next

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

Set up Phones

Set up 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

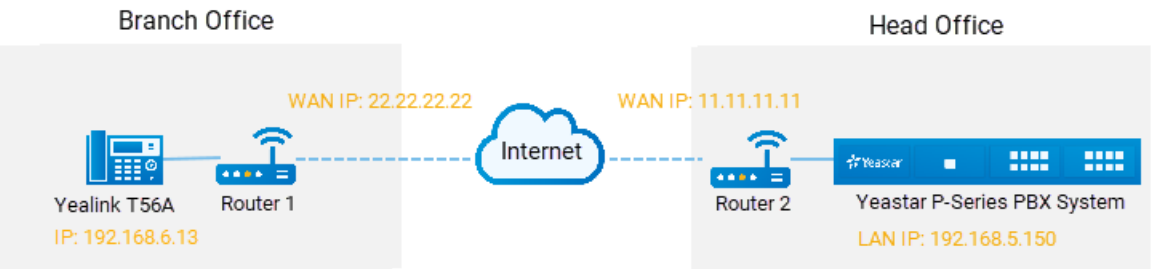
Set up a Remote SIP Phone via Public IP Address and Port
Set up a Remote SIP Phone via Yeastar FQDN

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**.

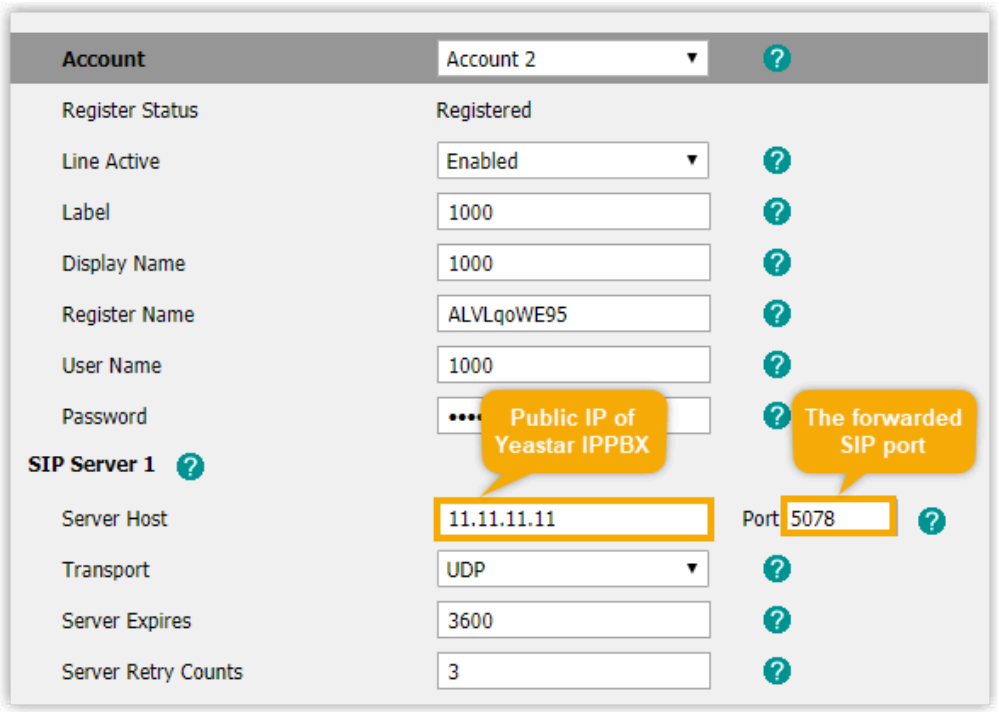
Step3. Set up an extension for remote access

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.



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

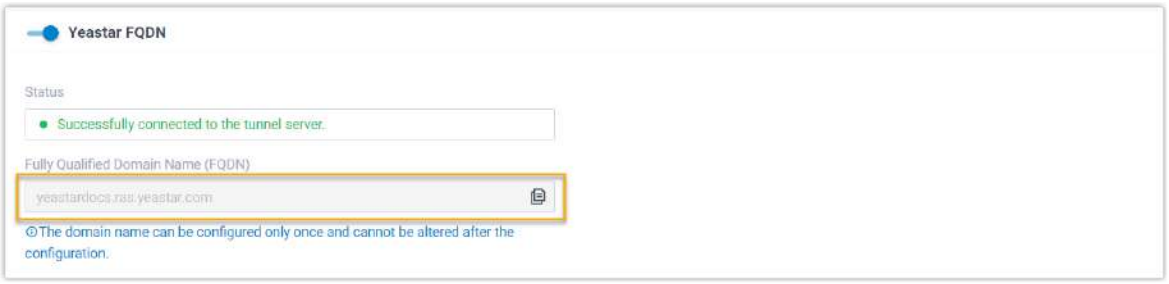
- Step 1. Gather information for extension registration
- Step 2. Register the extension on an IP phone
- Step 3. Confirm the extension's registration status

Step 1. Gather information for extension registration

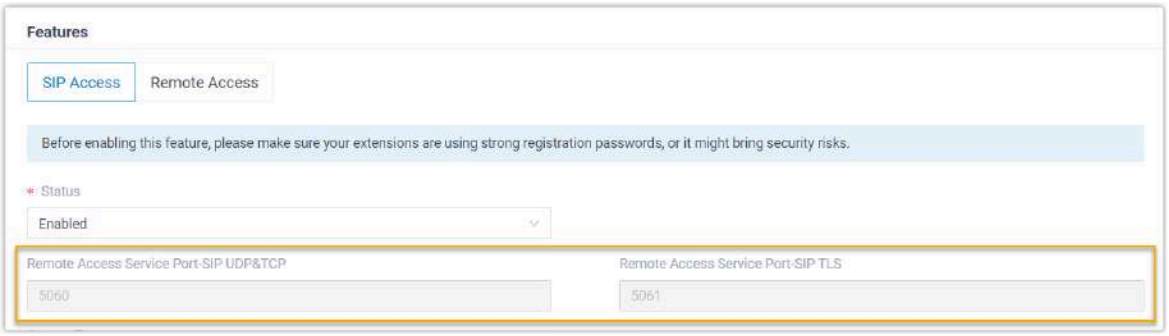
Log in to PBX web portal, and gather the required credentials.

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

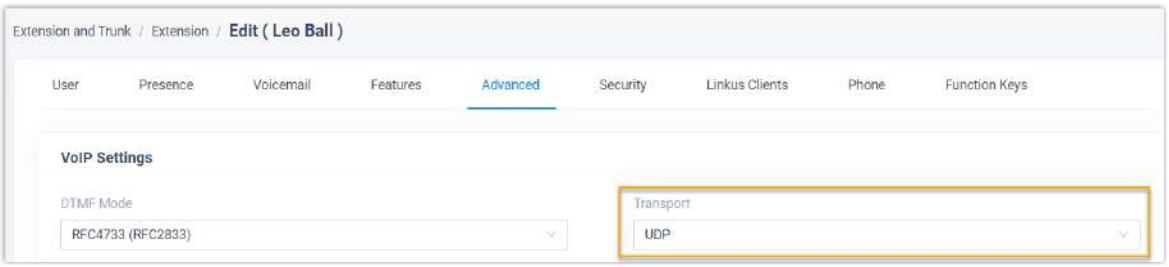
  In this example, the PBX FQDN is `yeastardocs.ras.yeastar.com`.



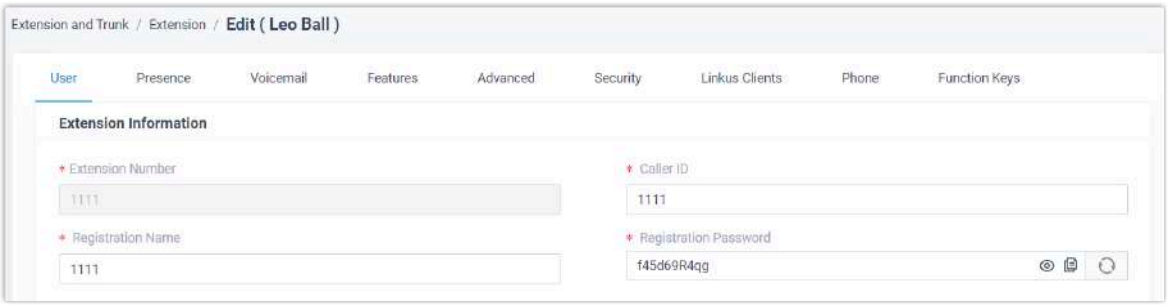
- Remote SIP registration port (Path: **System > Network > Yeastar FQDN > Features > SIP Access**)



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

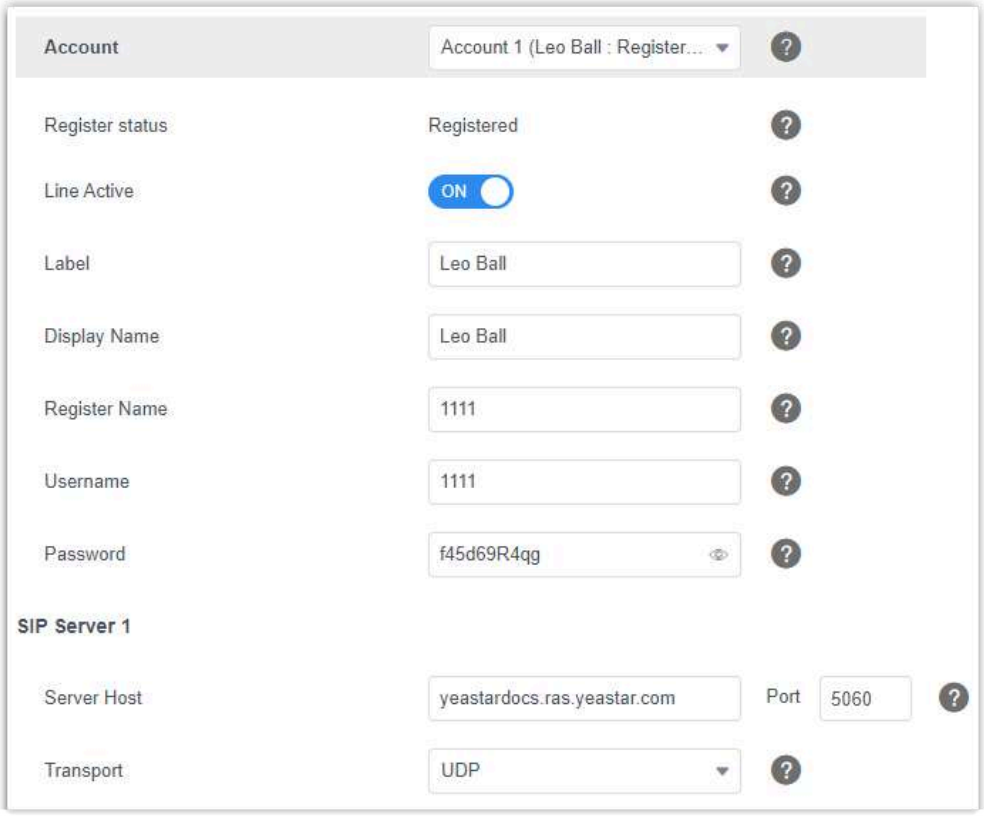


- Extension information (Path: **Extension and Trunk > Extension > User**)
  - Extension number
  - Registration name
  - Registration password



Step 2. Register the extension on an IP phone

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



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

5. Click **Confirm**.

Step 3. Confirm the extension's registration status

You can confirm the extension's registration status in one of the following ways:

- On the phone's web interface, check if the extension is registered.
- Log in to PBX web portal, go to **Extension and Trunk > > Extension**, check if the endpoint icon displays in the **Online Status** column.

Result

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

Extension Outbound Caller ID

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

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

Requirements

- The PBX version is 83.16.0.25 or later.
- Customizing outbound caller ID should be supported by the trunk provider.

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

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

1. Log in to PBX web portal, go to **Extension and Trunk > Trunk**, edit the desired trunk.
2. Click **Outbound Caller ID** tab.
3. In the **Outbound Caller ID List** section, click **Add**, and configure outbound caller IDs for extensions by different methods.
4. To associate one outbound caller ID with multiple extensions, select **Shared Outbound Caller ID** and configure the following settings:
    - **Outbound Caller ID**
    - **Outbound Caller ID Name**
    - **Associated Extensions**
    - **Default DOD Label**

5. To bind consecutive outbound caller IDs to consecutive extensions with one-to-one correspondence, select **Outbound Caller ID Range** and configure the following settings:
    - **Outbound Caller ID Range**
    - **Extension Range**
    - **Outbound Caller ID Name**
    - **Default DOD Label**
6. Click **Save** and **Apply**.

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

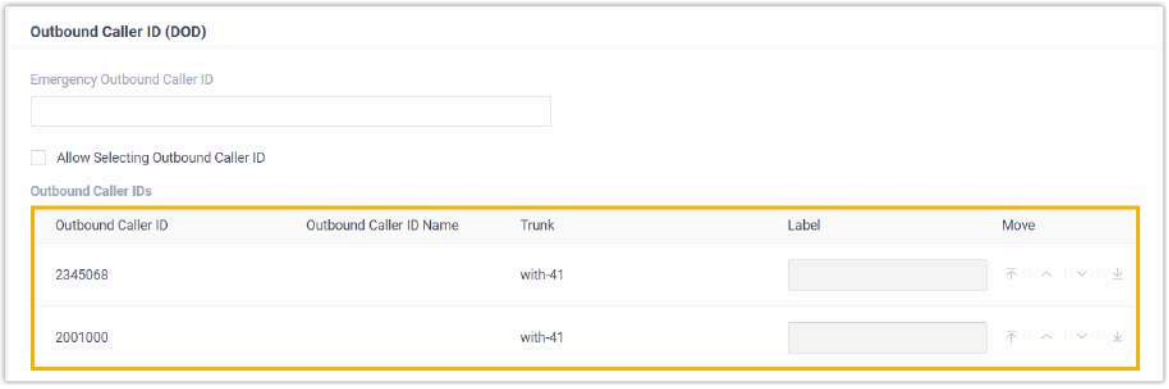
Set up an outbound route to allow extension users to dial out through the trunk that has been configured outbound caller IDs.

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

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

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

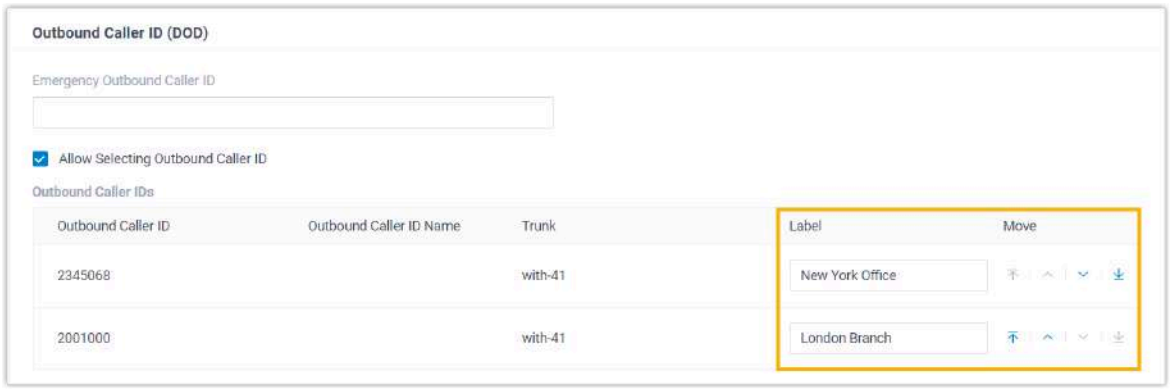
   The outbound caller IDs that have been associated with the extension are displayed on the **Outbound Caller IDs** list.



3. Select the checkbox of **Allow Selecting Outbound Caller ID**.

4. Customize how the DOD will be displayed on the extension's Linkus UC Clients as needed.

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

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

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

Result

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

> **Note:**
> To achieve this, extension user must upgrade his or her Linkus UC Clients to the specified version:
>
> - **Linkus Mobile Client**: 5.6.6 or later
> - **Linkus Desktop Client**: 1.6.0 or later

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

Extension Presence

Extension Presence Overview

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

What is presence

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

Yeastar P-Series Software Edition supports the following default statuses:

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

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

How presence benefits a user's work

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

- **Presence information**: Details about current presence.
- **Call forwarding**: Route internal and external calls to different destinations based on extension presence.
- **Ring strategy**: Adjust endpoints' ring strategy based on extension presence.

- **Ring timeout**: Adjust endpoints' ring timeout based on extension presence except **Do Not Disturb** status.
- **Ring the Mobile Number Simultaneously**: Whether to simultaneously ring mobile phone when a call reaches the extension number.
- **Accept push notifications**: Whether to receive Linkus push notifications on Linkus Mobile Client, such as missed calls, voicemails, etc.
- **Agent Status Auto Switch**: Adjust agent status automatically if the user is in a queue.
- **Voicemail greetings**: Adjust voicemail greetings based on extension presence.

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

Presence switch

There are two ways to switch extension presence:

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

  For more information, see Switch Presence on Linkus Client and Manually Switch Extension Presence.
- **Switch presence automatically**: Presence is switched based on Business Hours and Holidays.

  For more information, see Auto Switch Presence Status based on Business Hours and Holidays.

Presence Settings

This topic describes presence settings.

Background information

Yeastar P-Series 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

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

Call Forwarding

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

Setting	Description
Types of incoming calls	• **Internal Calls**: Set a call forwarding rule for incoming calls from colleagues. • **External Calls**: Set a call forwarding rule for incoming calls from external users.
Forwarding condition	Select a forwarding condition and configure a destination. • **Always**: Forward all incoming calls to the designated destination. • **No Answer**: Only forward unanswered calls to the designated destination. • **When Busy**: Only forward the calls that come in while the user is talking on the phone to the designated destination.

Ring Strategy

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

- **Extension Endpoint**: The IP phone or softphone to which the user's extension has registered.
- **Linkus Mobile Client**
- **Linkus Desktop Client (Softphone Only)**
- **Linkus Web Client (Web Client Mode Only)**
- **Linkus Pad Client (SDK)**

Note:

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

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

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

Ring Timeout

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

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

Options

Ring the Mobile Number Simultaneously

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

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

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

Accept Push Notifications

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

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

Accept calls from Ring Group

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

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

Agent Status Auto Switch

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

Setting	Description
Login	Log in to a queue. **Note:** The option is available ONLY in **Available** status.

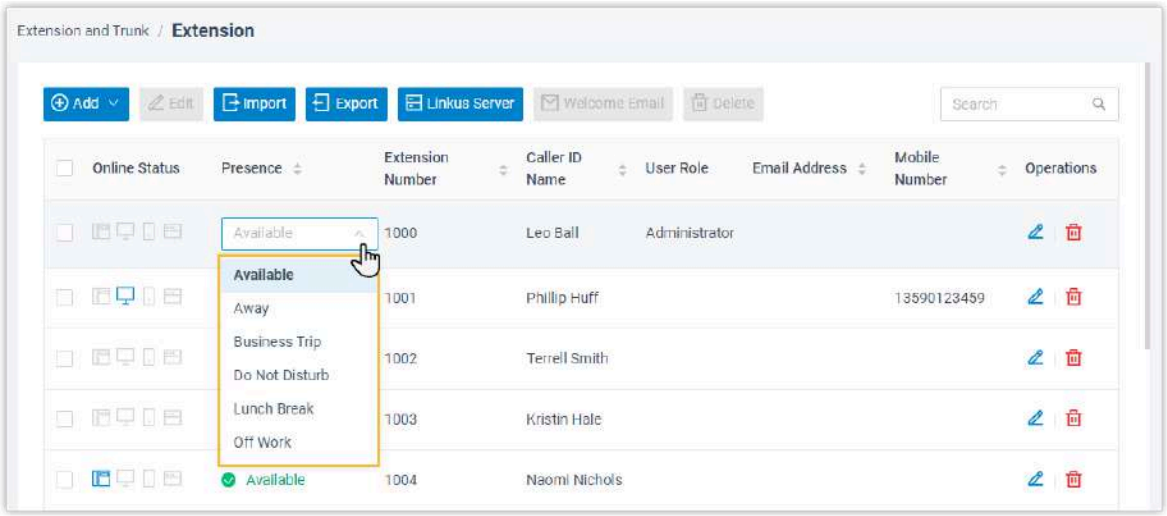
Setting	Description
Logout	Log out of a queue.
Pause	Pause receiving queue calls. **Note:** If you have set pause reasons for queue agents, you can select a specific pause reason in the **Pause Reason** drop-down list.
Do Nothing	Retain current status.

Manually Switch Extension Presence

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

Procedure

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



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

Result

New presence is synchronized on Linkus clients; presence settings related with the status take effect.

Related information

Automatically Switch Extension Presence Based on Time

Automatically Switch Extension Presence Based on Time

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

Background information

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

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

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

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the extensions that need to switch presence status automatically based on the time schedule.
2. Click the **Features** tab, and go to **Time-conditional Presence Auto Switch** section.
3. Configure the following presence based on the time:
   - **Business Hours**: Select a status to be displayed during office hours.

In this scenario, select **Available**.

- **Break Hours**: Select a status to be displayed during break time.

  In this scenario, select **Lunch Break**.
- **Holidays**: Select a status to be displayed during holiday.

  In this scenario, select **Off Work**.
- **Outside Business Hours**: Select a status to be displayed during non-office hours.

  In this scenario, select **Off Work**.

4. Click **Save**.

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

Result

Presence status will be switched automatically based on time.

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

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

Related information

Overview of Business Hours and Holidays
Manually Switch Extension Presence

Monitor Extension Status by BLF Key

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

Prerequisites

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

For more information, see the following topics:

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

Procedure

Step 1. Set up a function key for extension monitoring

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

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

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

Step 2. Apply the configuration to the IP phone

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

The system prompts you whether to reprovision the phone.

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

Result

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

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

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

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

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

Related information

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

Forward Incoming Calls to Another Destination

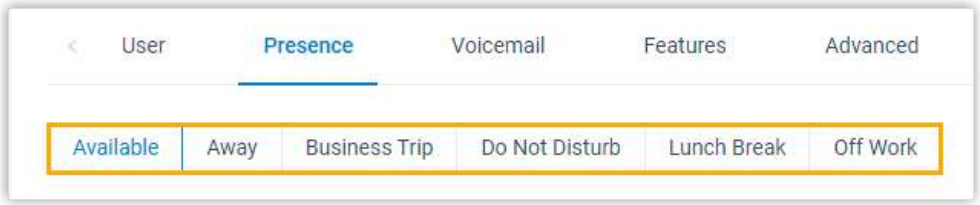
Yeastar P-Series Software Edition supports status-based call forwarding, which allows users to forward incoming calls to different destinations based on their presence status. This topic describes how to preconfigure call forwarding rules for extension users on PBX, and how to enable and configure feature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

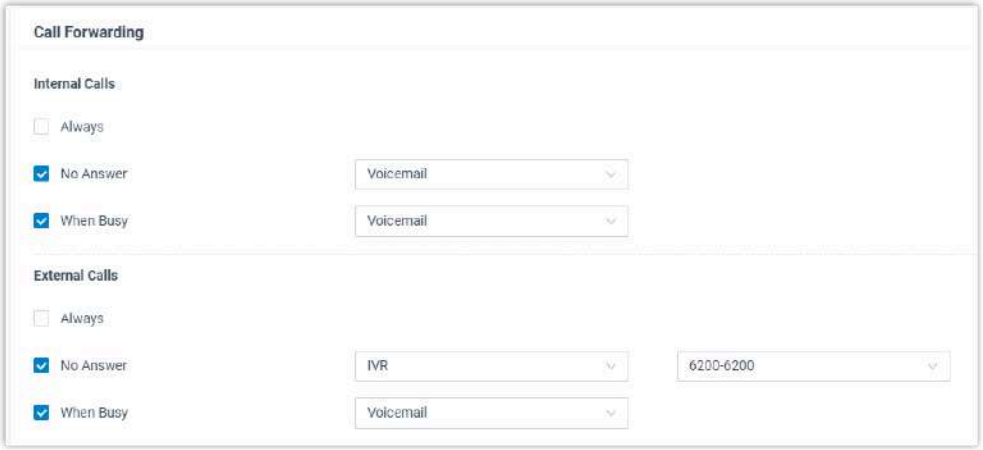
For each presence status of an extension, you can define a different destination to which the incoming calls will be forwarded. Every time the presence status changes, the incoming calls will be forwarded to the corresponding destination.

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.



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

Result

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

Enable feature code for call forwarding (destination immediate change)

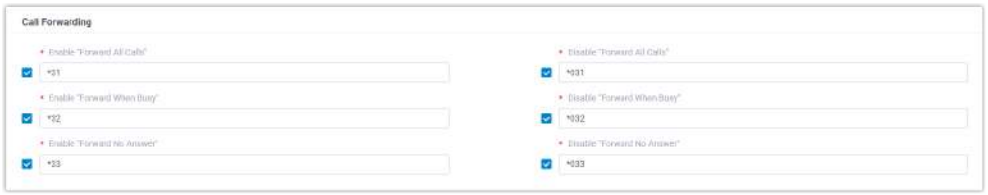
Extension users can change the preset call forwarding destinations on Linkus Web Client. For users with no access to Linkus Web Client, you can enable feature codes for call forwarding, so that these users can dial a feature code on their phones to change the call forwarding destinations.

Restrictions

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

Procedure

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



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

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

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

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

Result

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

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

Ring Office Phone and Mobile Phone Simultaneously

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

Scenario

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

Prerequisites

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

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
2. Click **Presence** tab.
3. In the status bar, select a status to which the strategy of simultaneous ring will be applied.
4. In the **Options** section, configure the following settings.

a. Select the checkbox of **Ring the Mobile Number Simultaneously**.

b. Click to configure mobile number.

c. **Optional:** In the **Prefix** field, enter the prefix of outbound route so that PBX can successfully send calls to your phone.

- If the **Strip** of outbound route is not set, you don't have to set the **Prefix**.
- If the **Strip** of outbound route is set, you need to set the **Prefix** according to the **Patterns** of outbound route.

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

Result

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

Extension Voicemail

Set up Extension Voicemail

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

Background information

Yeastar P-Series 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
- Email notifications
- Disallow voicemail messages
- Play options of voicemails
- Voicemail greetings
- Voicemail language

Procedure

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

     You can set the PIN number in the **Voicemail Access PIN** field.
   - **Disabled**: This user can access his or her voicemail messages directly.
4. In the **New Voicemail Notification** drop-down list, decide whether to send email notifications when the user receives a new voicemail.
   - To disable email notifications, select **Do Not Send Email Notifications**.
   - To enable email notifications, select one of the following options:
     - **Send Email Notifications with Attachment**: Send a notification email with the new voicemail message attached as a `.wav` file.
     - **Send Email Notifications without Attachment**: Send notification emails only.
5. If you enabled email notifications, configure the following settings as needed:

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

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

   The system will play voicemail greeting to the caller, and then hang up the call directly.
7. **Optional:** Set whether to play the following messages when playing a voicemail.
   - **Play Date and Time**: Enable this option to play date and time when the message is received.
     - **Time Display Format**: If **Play Date and Time** is enabled, you can specify the time format (12-hour or 24-hour) for announcing the message arrival time.
   - **Play Caller ID**: Enable this option to play caller ID information.
   - **Play Message Duration**: Enable this option to play duration of the message.
8. **Optional:** To customize voicemail greetings that will be played to callers when they reach the user's voice mailbox, see Record or Upload Voicemail Greetings.
9. Click **Save** and **Apply**.

Related information

Forward Voicemail Messages to Email
Check Voicemail Messages

Extension Function Keys

Set up Function Keys for Extensions Using a Template

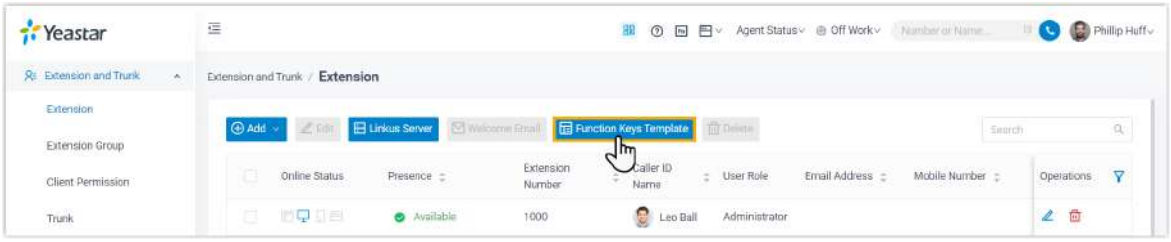
Yeastar P-Series Software Edition allows you to create function keys templates and apply them to multiple extensions at once, significantly reducing the time spent in configuring individual extensions. This topic describes how to set up a function keys template and apply the template to extensions.

Requirements

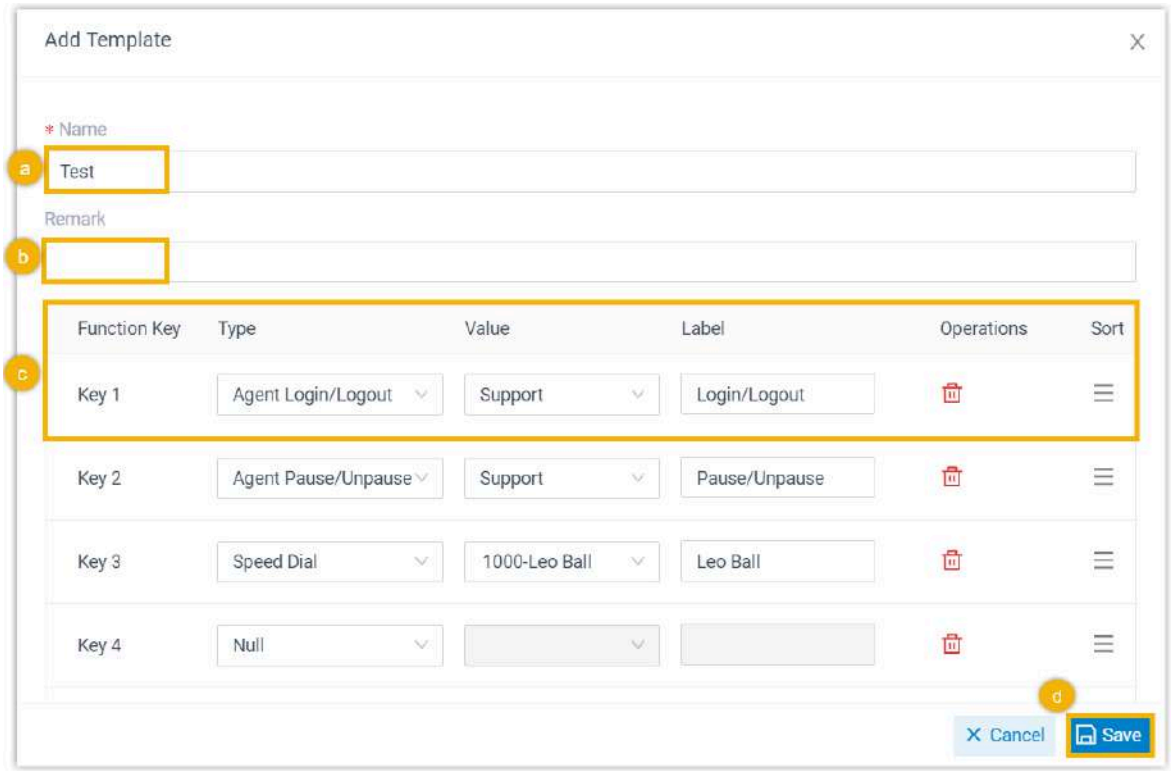
The firmware version of PBX server is 83.16.0.70 or later.

Step 1. Add a function keys template

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

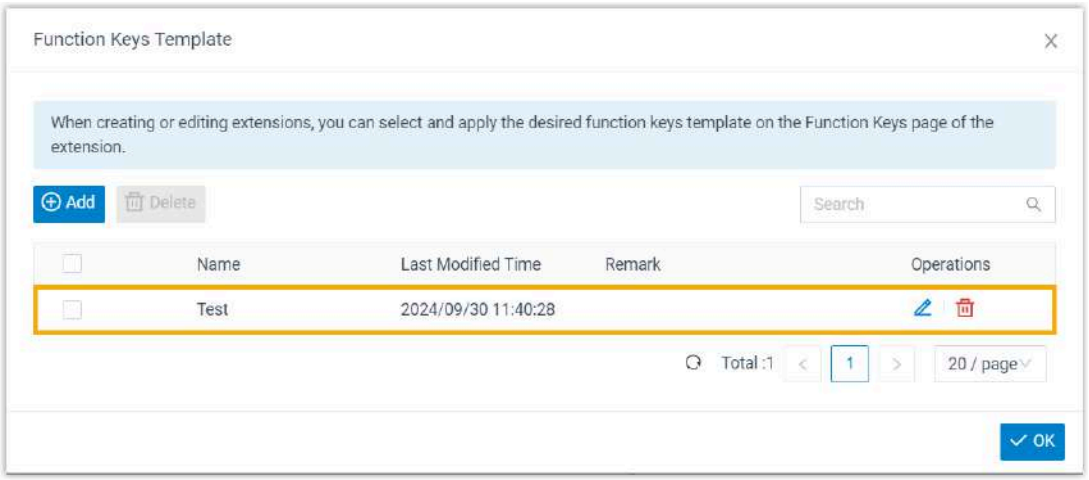


3. Click **Add** to add a function key template, then configure the following settings.



a. In the **Name** field, enter a name to help you identify the template.
b. **Optional:** In the **Remark** field, enter a short description about the template.
c. In the function keys list, configure function keys according to your needs.
   - **Type**: Select a key type.
   - **Value**: Configure a desired value based on the key type.
   - **Label**: Optional. Enter a value to help extension users identify the function key.
d. Click **Save**.

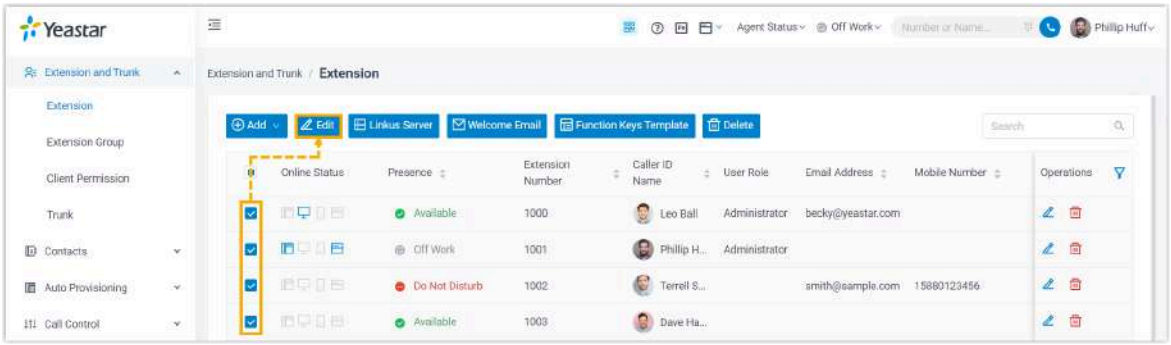
   The function key template is created and displayed on the list.



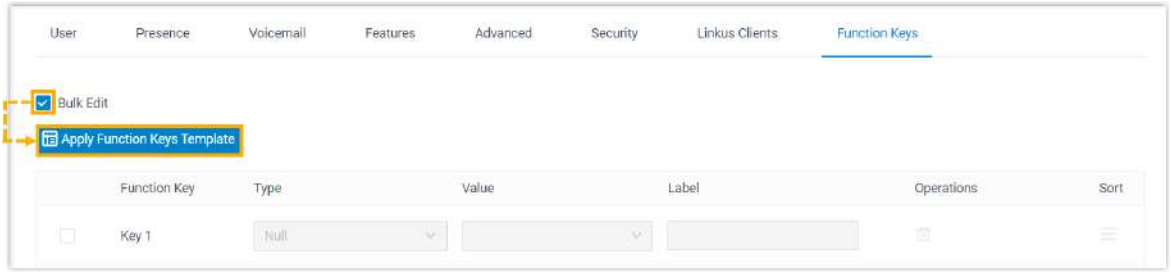
4. Click **OK**.

Step 2. Apply the function keys template to extensions

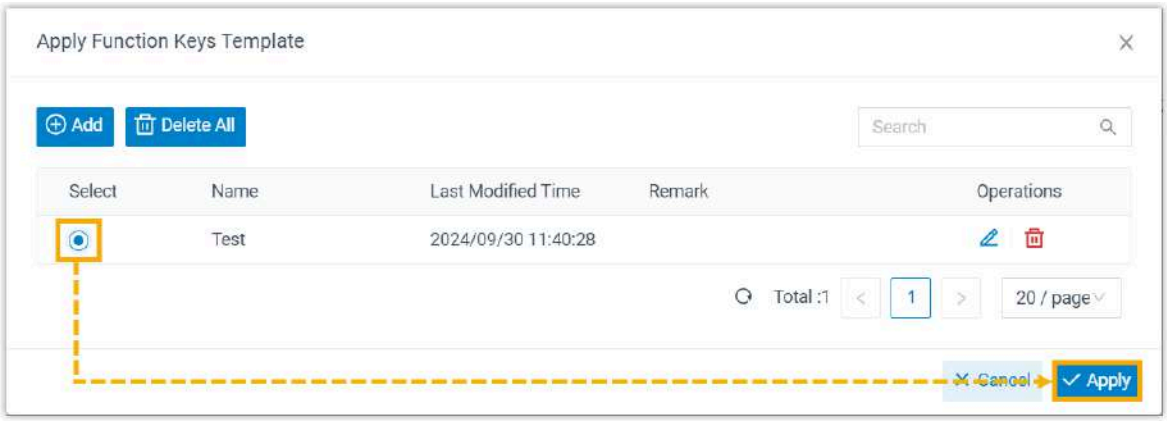
1. On the extension list, select the checkboxes of the desired extensions, then click **Edit**.



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



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



4. Click **Save**.

Result

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

Note:

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

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

Extension Features

Handle Incoming Calls Based on Caller ID

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

Procedure

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

2. Click **Features** tab.
3. In the **Call Handling Based on Caller ID** section, set up one or more rules according to your needs.
    a. Click **Add**.
    b. In the **Caller ID** field, enter a specific number or a number pattern.
        - To apply the rule to a specific number, enter a specific number.

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

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

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

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

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

    > **Note:**
    > For example, set the rule "Accept calls from 72837300" to a higher priority than the rule "Reject calls from numbers starting with 728373".
    > In this way, when receiving calls from 72837300, the system will send

> calls to the extension user. For other incoming calls from number starting with 728373, the system will hang up directly.

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

Result

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

Set up Email Notifications for Missed Calls

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

Prerequisites

- System email server is set up.
- An email address is associated with a desired extension.

Procedure

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

Result

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

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

Set up Email Notifications for User Password Change

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

Prerequisites

- System email server is set up.
- An email address is associated with a desired extension.

Procedure

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

Result

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

Customize Music on Hold for an Extension

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

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

Requirements

The firmware version of PBX server is 83.15.0.22 or later.

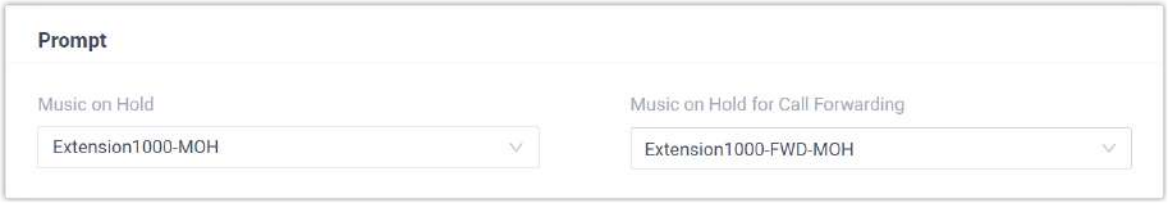
Prerequisites

You have prepared and uploaded music for the following scenarios:

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

Procedure

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



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

Allow Multiple Registrations for One Extension Number

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

Background information

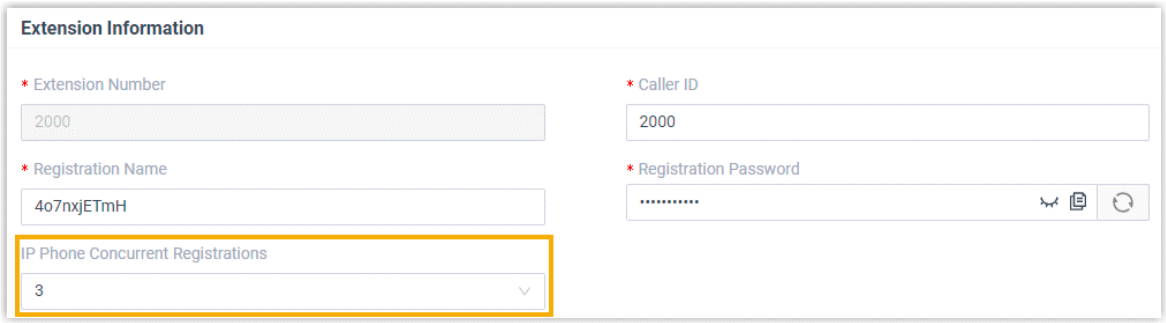
For employees who work flexibly anywhere, they can register their extensions on multiple SIP endpoints, such as an IP phone in their office, a softphone on computer, or a SIP client on mobile phone. In this way, an incoming call can ring all endpoints at the same time, and users can handle calls at anywhere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

Procedure

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

Note:

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



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

Result

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

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

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

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

Set Business Hours for an Extension

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

Requirements

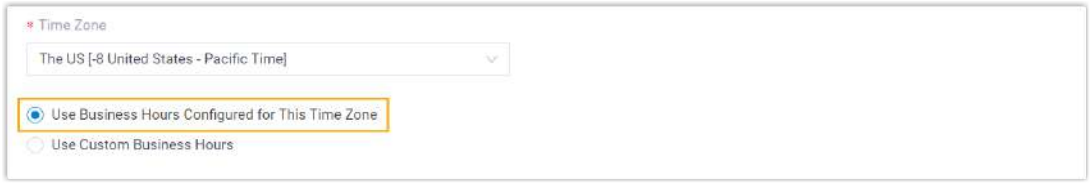
The firmware of Yeastar P-Series Software Edition is 83.18.0.59 or later.

Prerequisites

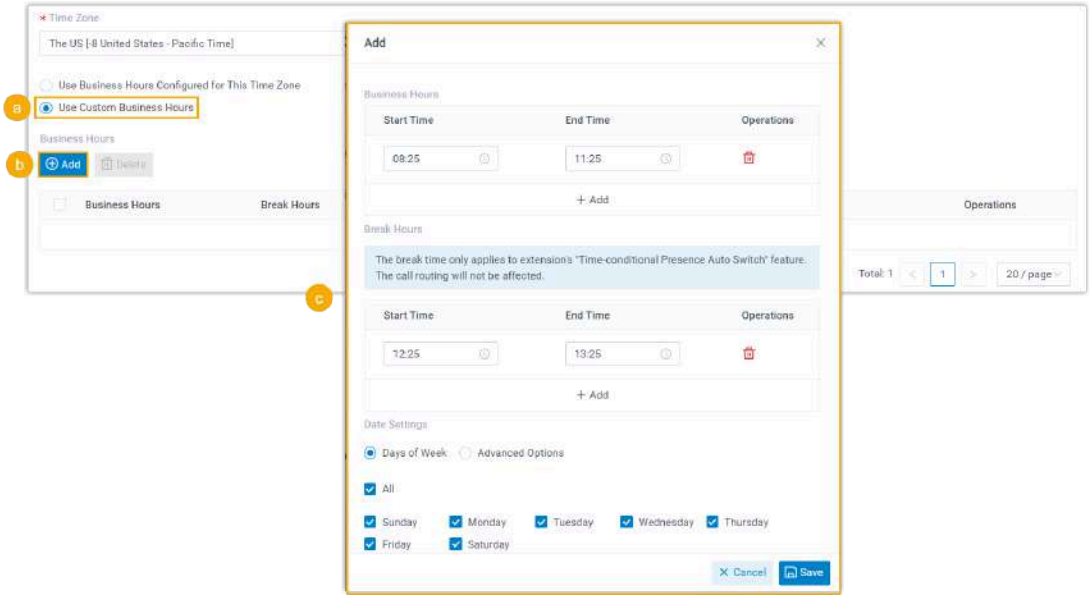
You have configured time zones and business hours for the system (Path: **Call Control > Business Hours and Holidays**).

Procedure

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



   - To use custom business hours, do as follows:



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

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

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

Results

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

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

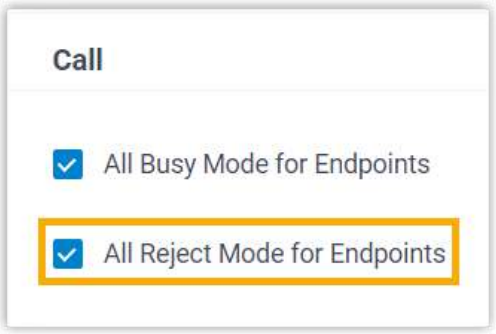
- If you customize business hours for extensions, the extension users can modify the business hours by their own on Linkus Web Client and Desktop Client (Path: **Preferences > Features > Business Hours**).

Stop Rejected Calls from Ringing Other Endpoints

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

Procedure

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



4. Click **Save**.

Result

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

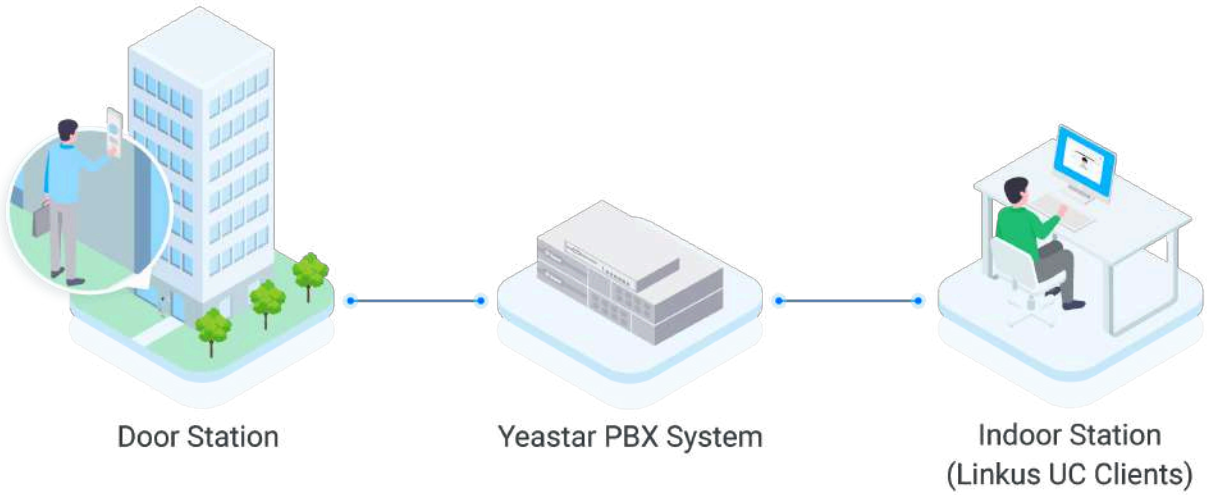
Enable Video Preview of Intercom Calls for Extensions

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

Scenario

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

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



Methods of previewing videos

Yeastar P-Series Software Edition supports the following two methods of previewing videos:

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

Requirements and restrictions

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

Requirements

- **PBX Version**: 83.10.0.30 or later
- **PBX Plan**: Ultimate Plan

Restrictions

- **Supported Door Station**: Fanvil

Note:

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

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

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

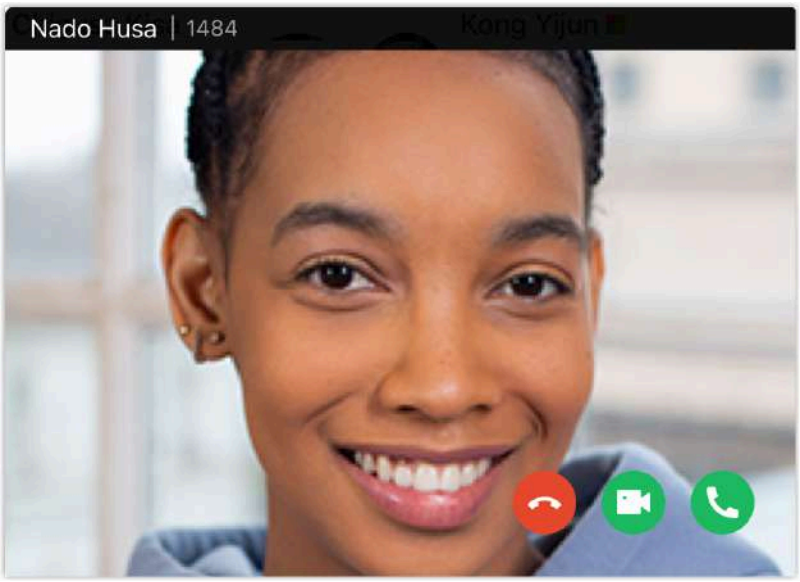
	Video Preview	Auto Preview
Linkus Mobile Client (iOS)	×	×
Linkus Mobile Client (Android)	√	√
Linkus Desktop Client (Windows)	√	× (Coming Soon)
Linkus Desktop Client (Mac)	√	× (Coming Soon)
Linkus Web Client	√	√

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

Procedure

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

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



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

Extension Advanced Settings

Advanced Settings of SIP Extension

This topic describes the advanced settings of a SIP extension.

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

Table 5.

Setting	Description
DTMF Mode	Set the mode for sending DTMF tones. • **RFC4733 (RFC2833)**: DTMF will be carried in the RTP stream in different RTP packets. • **Info**: DTMF will be carried in the SIP info messages. • **Inband**: DTMF will be carried in the audio signal. • **Auto**: If the device supports **RFC4733 (RFC2833)**, PBX will choose **RFC4733 (RFC2833)**, otherwise the PBX will choose **Inband**.
Transport	Set the transport protocol. • **UDP** • **TCP** • **TLS** **Note:** If you change the transport protocol, you must re-register the extension.
Qualify	Enable this option to send SIP OPTION packet to SIP device to check if the device is up.
T.38 Support	Enable or disable T.38 fax for the extension. **Note:** Enabling T.38 will add performance cost. We recommend that you disable T.38.
NAT	Enable this option when the PBX uses a public IP address. The feature is enabled by default.

Table 5. (continued)

Setting	Description
	Note: If you manually set up Linkus server, make sure the desired extension's NAT is enabled, or the extension user can not access Linkus when he or she is out of local network.
SRTP	Enable SRTP for voice encryption.

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.

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

Disable Outbound Calls

Restrict users from making outbound calls.

Disable Outbound Calls outside Business Hours

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

Disallow International Calls

Restrict users from making international calls.

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

Outbound Call Frequency Restriction

When an extension makes outbound calls and the number of calls exceeds the outbound call frequency restriction within specified time period, the system would restrict the extension from making outbound calls.

For more information, see Limit Outbound Call Frequency of an Extension.

Max Outbound Call Duration (s)

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

Outbound Route Permission

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

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

Login Security

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

Two-Factor Authentication

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

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

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

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

User must change password periodically

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

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

Restrict Outbound Calls for an Extension

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

Procedure

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

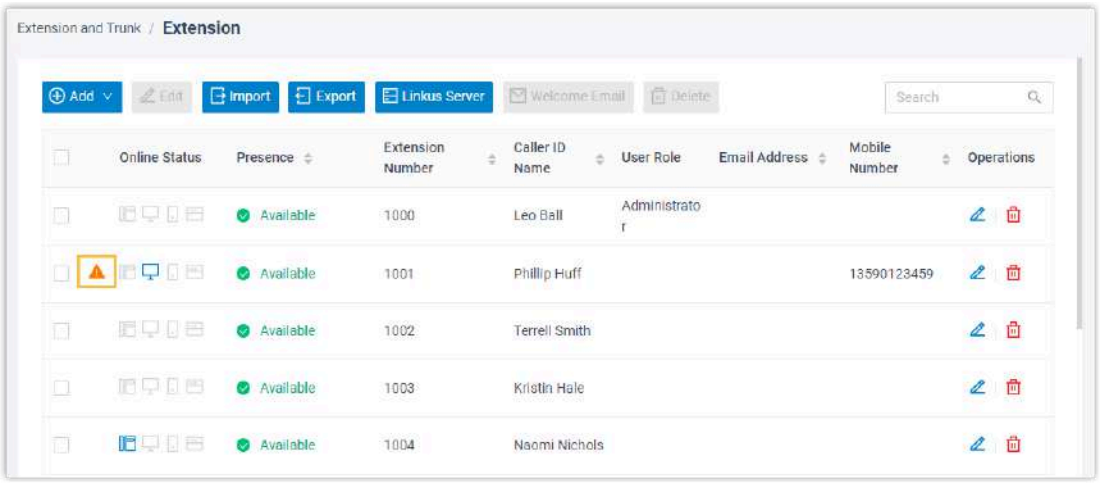
Result

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

  > **Note:**
  > Emergency Calls like 911 is not restricted.

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

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



Restrict Extension Registration Based on User Agent

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

Background information

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

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

When a SIP endpoint tries to register an extension to Yeastar P-Series 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

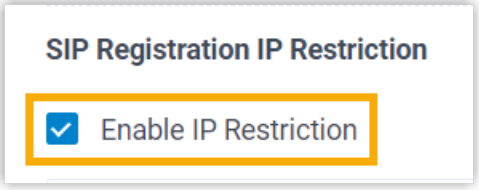
This topic describes how to allow devices with a specific IP address or in a specific IP section to register extensions on Yeastar P-Series Software Edition.

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 Registration IP Restriction** section, select the checkbox of **Enable IP Restriction**.



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

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

Result

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

Block Outbound Calls Outside Business Hours

This topic describes how to restrict an extension from making outbound calls outside the business hours of a specific time zone.

Prerequisites

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

Procedure

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

Result

The user can NOT make outbound calls during off-duty time and holidays defined in the time zone of the extension.

Limit Call Duration of an Outbound Call

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

Procedure

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

2. Click **Security** tab.
3. In the **Call Restrictions** section, select a value from the drop-down list of **Max Outbound Call Duration (s)**, or enter a value according to your needs.
4. Click **Save** and **Apply**.

Result

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

Limit Outbound Call Frequency of an Extension

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

Procedure

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

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

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

Result

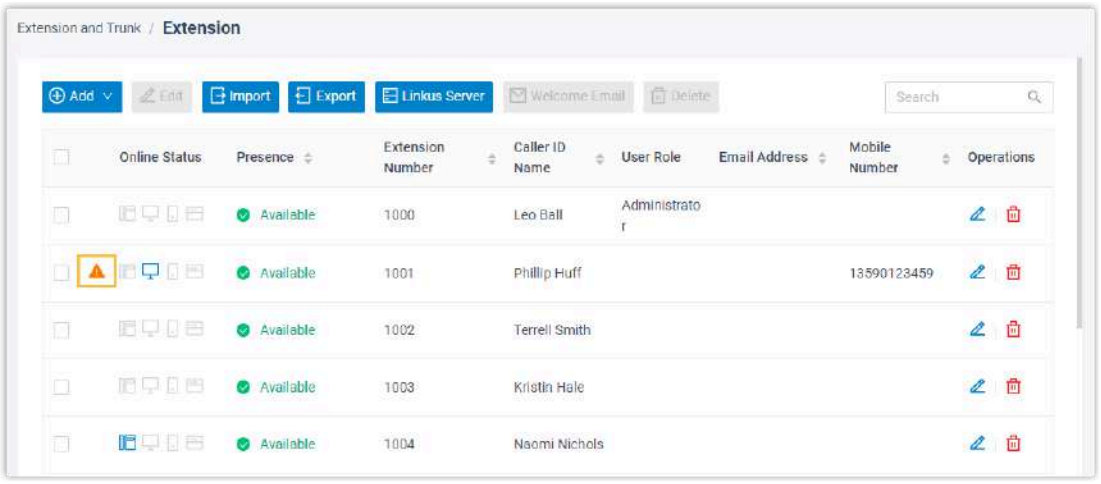
If an extension has exceeded the outbound call frequency restriction, the following things would happen.

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

> **Note:**
> Emergency Calls like 911 is not restricted.

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

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



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

Set up Periodic Password Changes for an Extension

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

Requirements

The version of PBX server is 83.18.0.102 or later.

Procedure

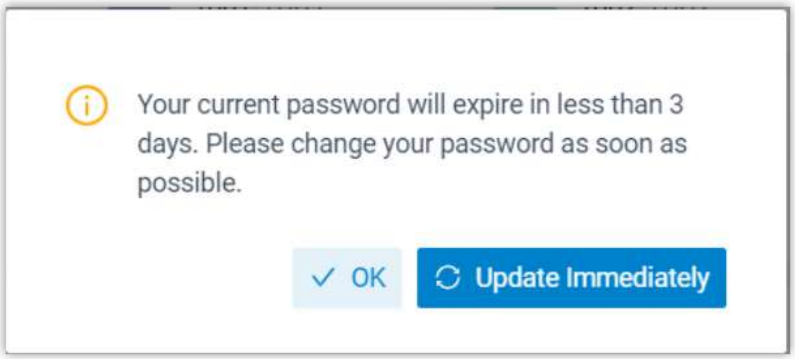
1. Log in to PBX administrator portal with super administrator account, go to **Extension and Trunk > Extension**.
2. Click to edit the desired extension.
3. Under **Security** tab, scroll down to **Login Security**, then configure the following settings.
   a. Select the checkbox of **User must change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

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

Result

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

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



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

- Linkus Desktop Client: Version 1.11.7 or later

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

Manage Extensions

Edit Extensions

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

Edit an extension

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

Bulk edit extensions

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

Reset an Extension's User Password

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

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Search and select the desired extension, click .

3. In the **User Information** section, delete the value in the **User Password** field, and enter a new password.
4. Click **Save**.

Result

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

Export and Import SIP Extensions

The SIP extensions configured on Yeastar P-Series 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

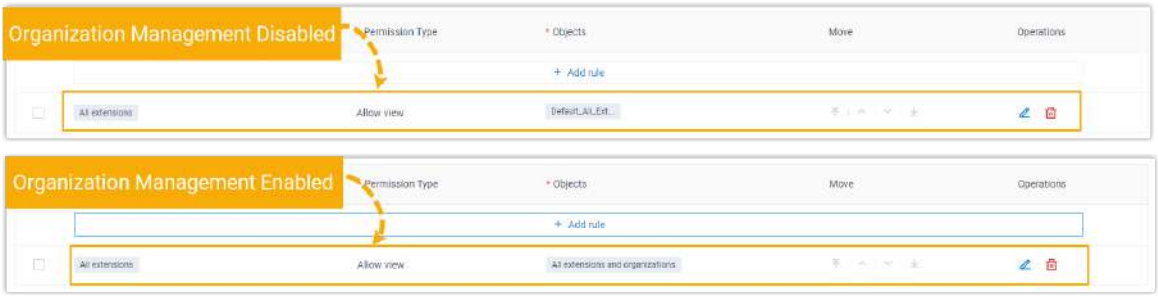
Set up Extension Visibility

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.

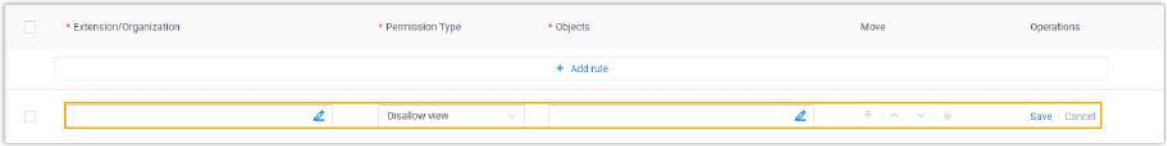
Procedure

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

   The default extension visibility rule is displayed.



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



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

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

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

b. Click **Save**.

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

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

Result

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

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

Manage Extension Visibility Rules

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

Edit an extension visibility rule

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

Delete extension visibility rules

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

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

Contacts

Contacts Overview

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

Contacts

Yeastar P-Series Software Edition supports two types of contacts:

Personal Contacts

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

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

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

Company Contacts

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

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

For more information, see the following topics:

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

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

Phonebook

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

Types of phonebooks

Yeastar P-Series Software Edition supports two types of phonebooks:

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

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

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

Visibility of phonebooks

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

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

For more information, see Set up Contact Visibility.

Restrictions

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

Number of contacts

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

Maximum Number of Extensions (N)	N < 1000	N ≥ 1000
Personal contacts (per extension)	3,000	3,000
Company contacts (total)	200,000	500,000
Company phonebooks	200	500

Available operations

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

The table below shows the operations available in each endpoint.

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

PBX-native Contacts

Add and Manage Company Contacts

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

Background information

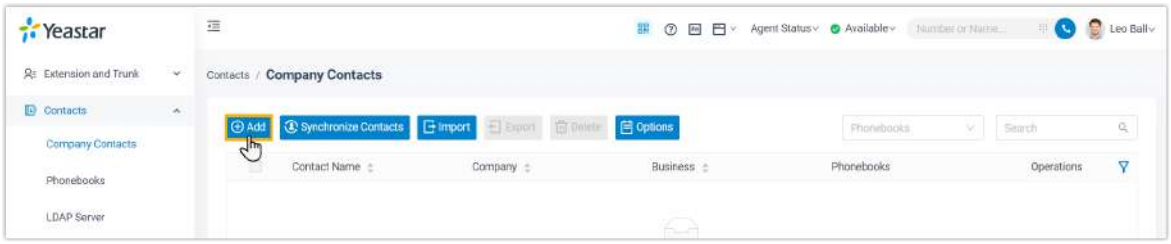
By default, only super administrator and extension users with **Administrator** role assigned can add and manage company contacts. Any other extension users can neither manage nor view any company contacts.

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

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

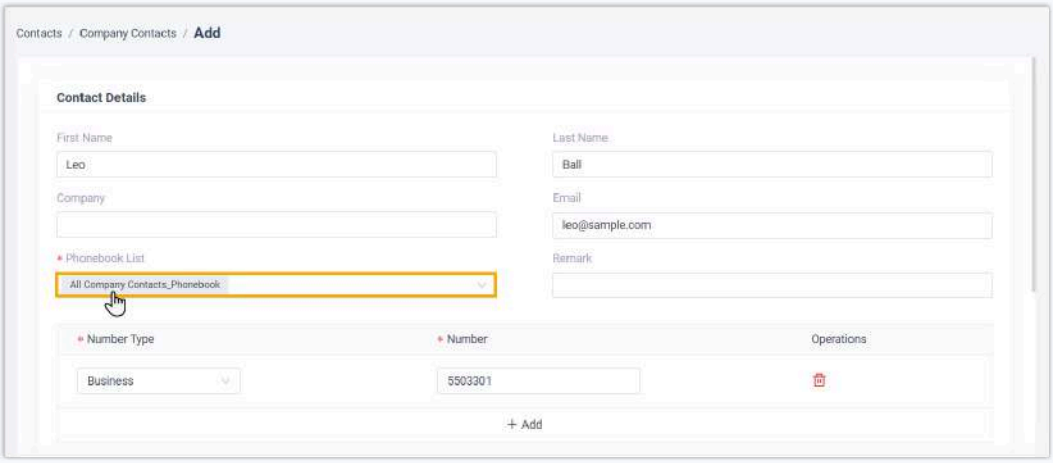
Add a company contact

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



3. Enter contact information.

> **Note:**
> The contact will be automatically added to the default **All Company Contacts_Phonebook**. You can group the contact into other organized phonebook(s) by selecting existing phonebook(s) from the drop-down list of **Phonebook List**.



4. Click **Save**.

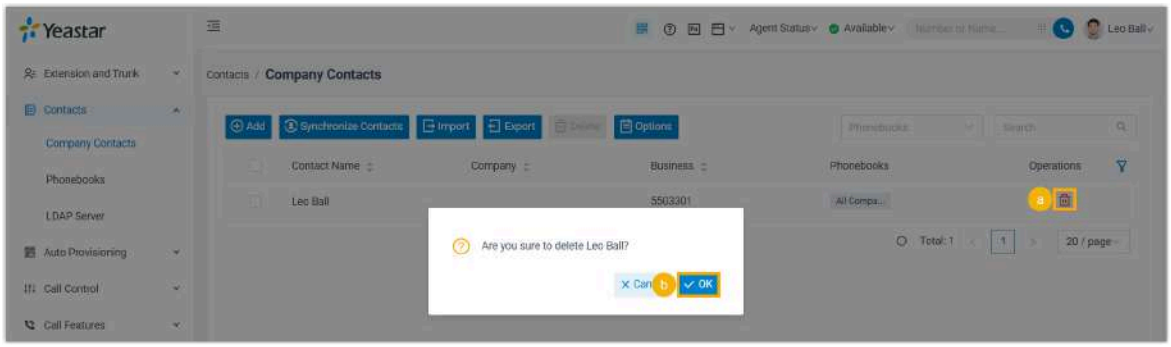
   The contact is stored as a company contact and shared among the authorized users from their Linkus UC Clients and IP phones.

Edit a company contact

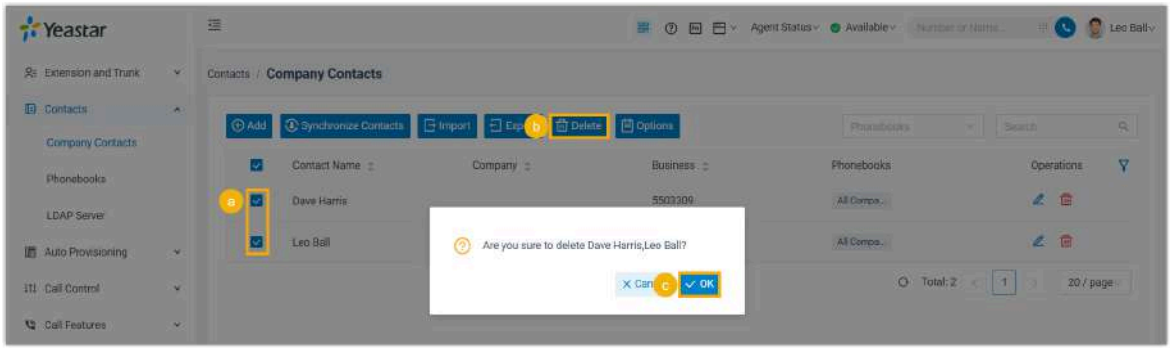
1. Log in to PBX web portal, go to **Contacts > Company Contacts**.
2. Click beside the desired contact.
3. Edit contact information as needed.
4. Click **Save**.

Delete company contacts

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



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



Export and Import Company Contacts

The company contacts configured on Yeastar P-Series 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

Third-party Contacts

Microsoft SQL

Microsoft SQL Integration Guide

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

Requirements

Item	Requirement
Yeastar PBX	• **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP) • **Firmware**: Version 83.16.0.70 or later
Microsoft SQL	No requirement. All versions of Microsoft SQL Server can integrate with Yeastar P-Series Software Edition.

Integration flow

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

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

Scenario: Caller ID name display

1. Integrate Yeastar P-Series Software Edition with Microsoft SQL

Scenario: Caller ID name display and contact synchronization

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

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

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

Integrate Yeastar P-Series Software Edition with Microsoft SQL

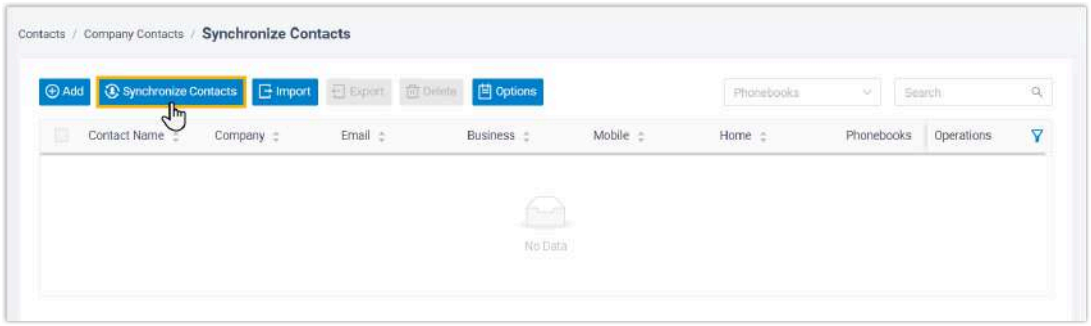
With the integration between Yeastar P-Series Software Edition and Microsoft SQL, inbound calls to PBX will automatically trigger contact lookup in your Microsoft SQL database and display the caller's name if a match is found.

Requirements

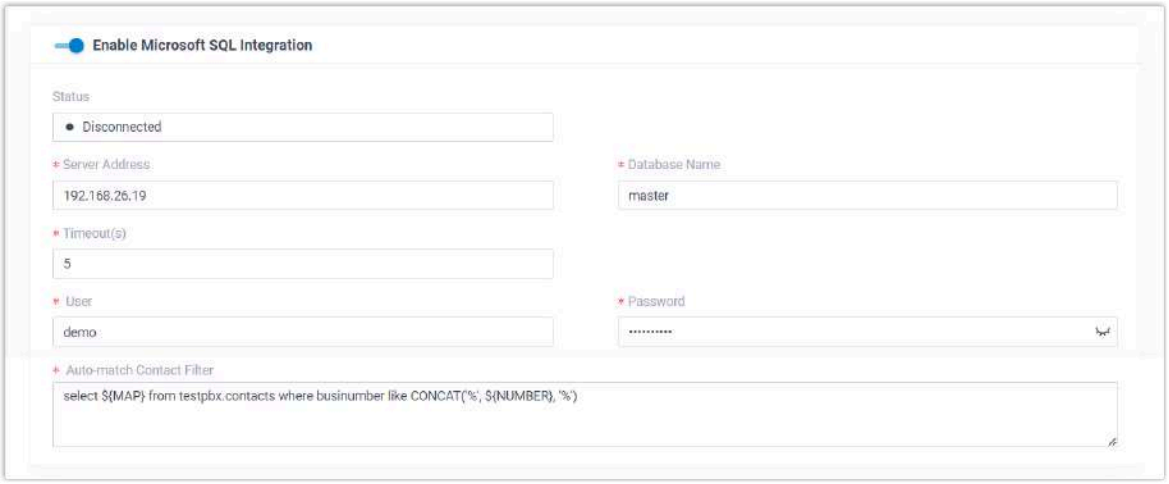
Item	Requirement
Yeastar PBX	• **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP) • **Firmware**: Version 83.16.0.70 or later
Microsoft SQL	No requirement. All versions of Microsoft SQL Server can integrate with Yeastar P-Series Software Edition.

Step 1. Enable Microsoft SQL integration

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



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

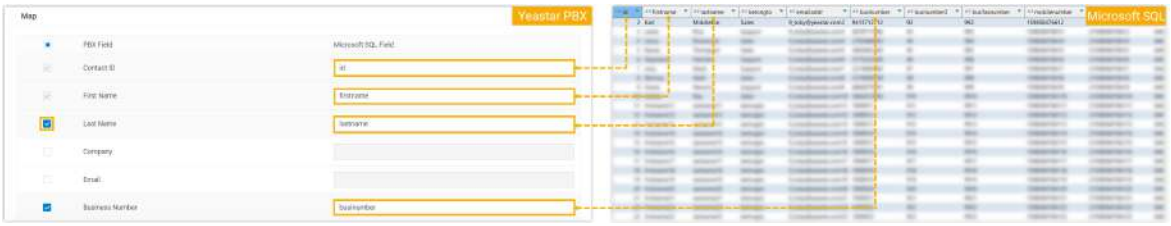


Item	Description
Server Address	Enter the address of Microsoft SQL server based on your situation. • If Microsoft SQL server runs on the default port `1433`, enter the server's IP address or domain name. For example, enter `192.168.26.19`. • If Microsoft SQL server runs on a non-default port, enter the server's IP address/domain name and port. For example, enter `192.168.26.19:2233`.
Database Name	Enter the name of the database.
Timeout(s)	Set the timeout for the connection to Microsoft SQL server.
User	Enter the username to connect to the database.
Password	Enter the password to connect to the database.

Item	Description
Auto-match Contact Filter	Enter a SELECT statement for contact caller ID matching, in the format **select ${MAP} from** *{schema_name}.{table_name}* **where** `{condition_to filter_number}`. **Example**: select ${MAP} from testpbx.contacts where businumber like CONCAT('%', ${NUMBER}, '%') • **select ${MAP}**: Specify the name of the column in the database that you want to display as the caller ID name. **Note:** *${MAP}* will be replaced by the field values corresponding to the PBX field (First Name, Last Name, or both) enabled in the **Map** section. • **from testpbx.contacts**: The table from which you want to select data, which must include two-part names (schema name and table name) in the format *{schema_name}*.*{table_name}*. • **where businumber like CONCAT('%', ${NUMBER}, '%')**: Retrieve the records where businumber contains the value of ${NUMBER} anywhere within it.

Step 2. Map contact fields between Yeastar P-Series Software Edition and Microsoft SQL

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



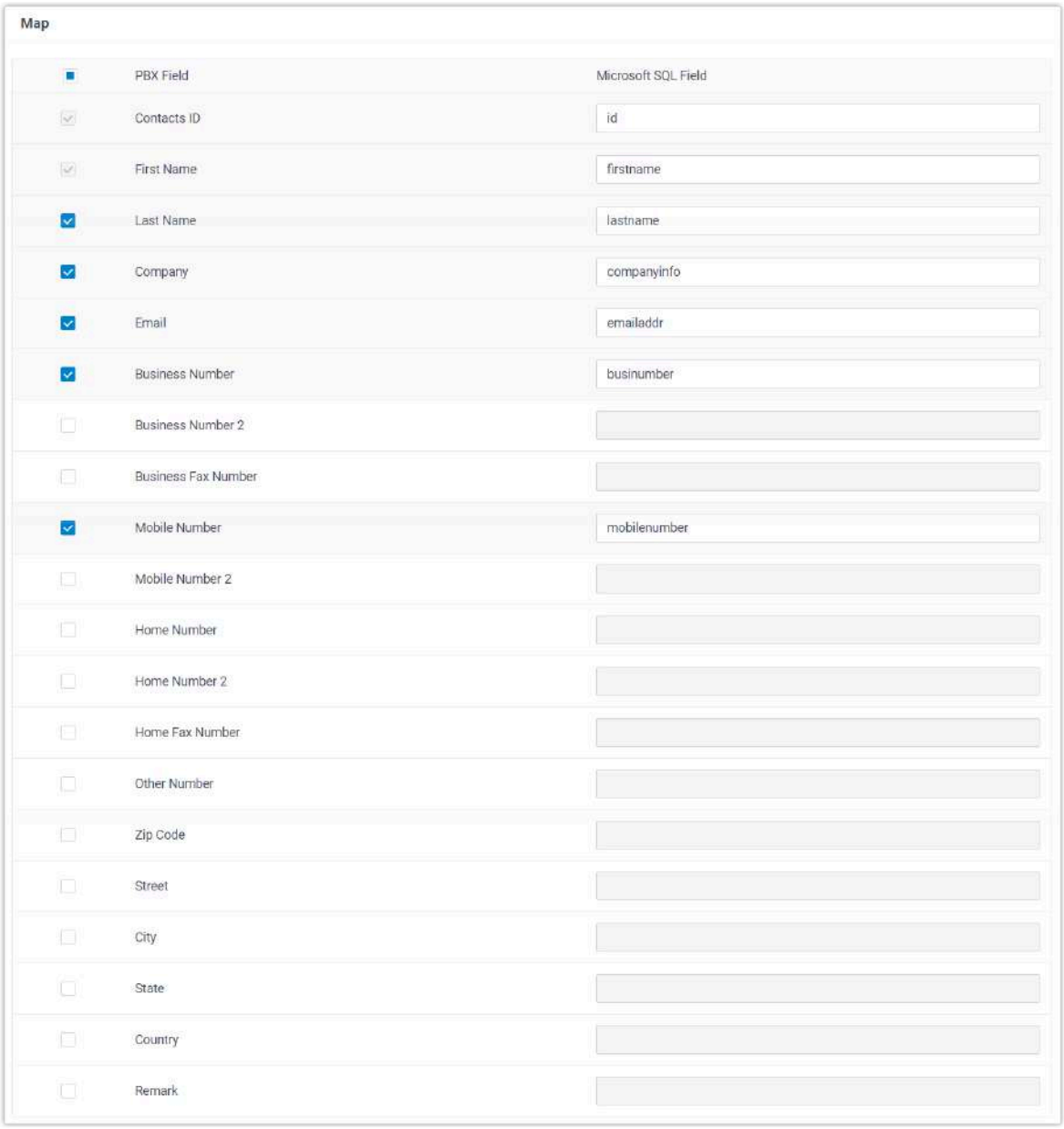
   a. For **Contacts ID**, **First Name**, and **Business Number**, enter the corresponding column name in Microsoft SQL contacts table.

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

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

b. **Optional:** To display contact's last name as well, select the checkbox of **Last Name**, then enter the corresponding column name in Microsoft SQL field.

3. If you want to synchronize Microsoft SQL contacts to PBX, enable and map the desired fields.



4. Click **Save**.

Result

- Yeastar P-Series Software Edition is connected to your Microsoft SQL server.

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

What to do next

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

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

Set up Contact Synchronization from Microsoft SQL

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

Restrictions

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

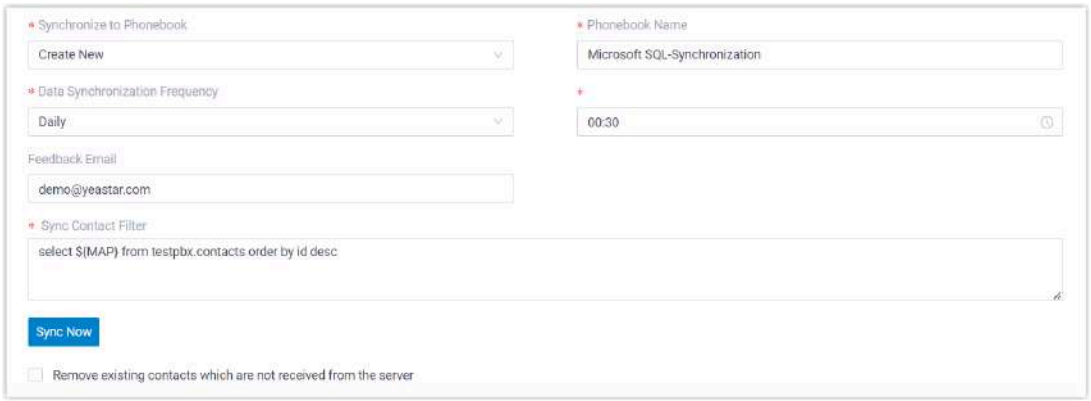
Maximum Number of Extensions (N)	N < 1000	N ≥ 1000
Company contacts (total)	200,000	500,000
Company phonebooks	200	500

Prerequisites

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

Procedure

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



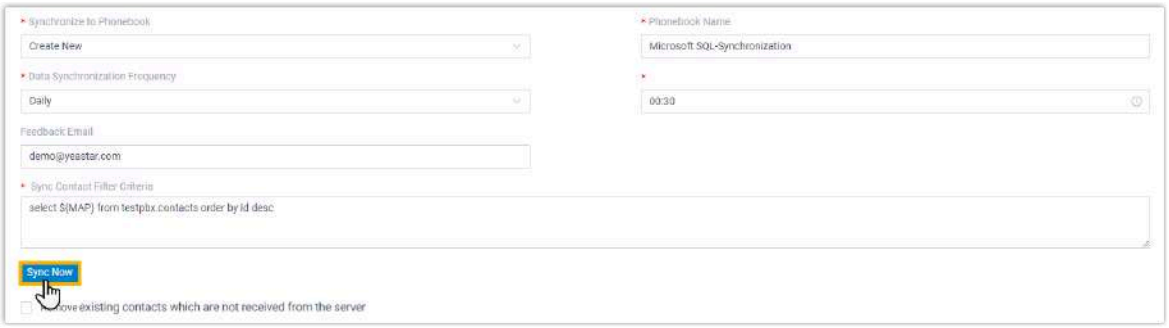
Item	Description
Synchronize to Phonebook	Select where to store the contacts that will be synchronized from your database. • **Create New**: Create a new phonebook from scratch to store the synced contacts. If you choose the option, enter the phonebook name in the **Phonebook Name** field. • **Read Specific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

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

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

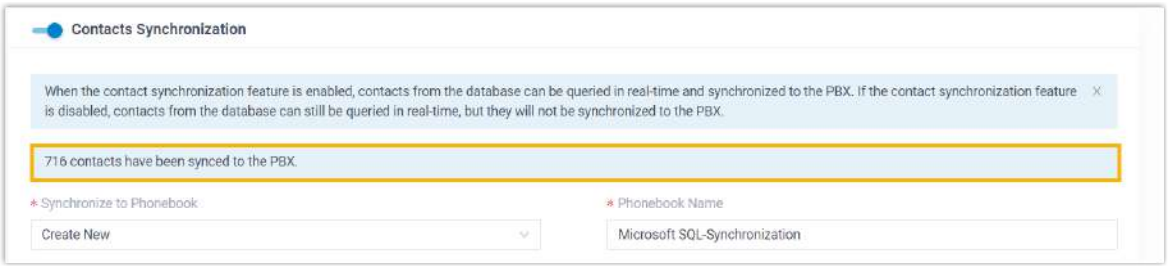
c. Click **Save**.

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



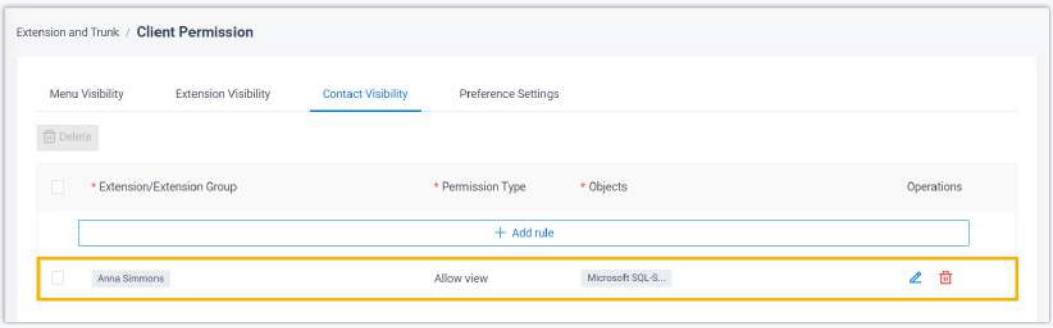
Result

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



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

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

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

What to do next

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

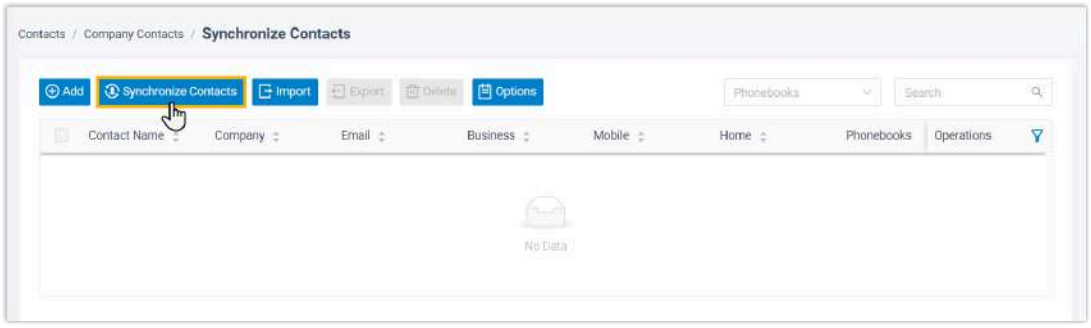
For more information, see Route Inbound Calls by Matched Phonebook Contacts.

Disable Microsoft SQL Integration

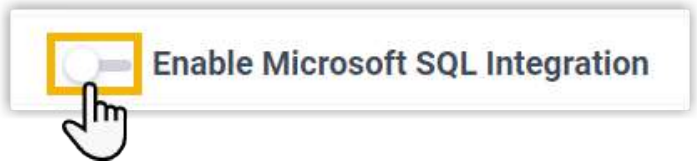
You can disable Microsoft SQL integration on Yeastar P-Series Software Edition at any time when you want to pause the database integration.

Procedure

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



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



3. Click **Save**.

Result

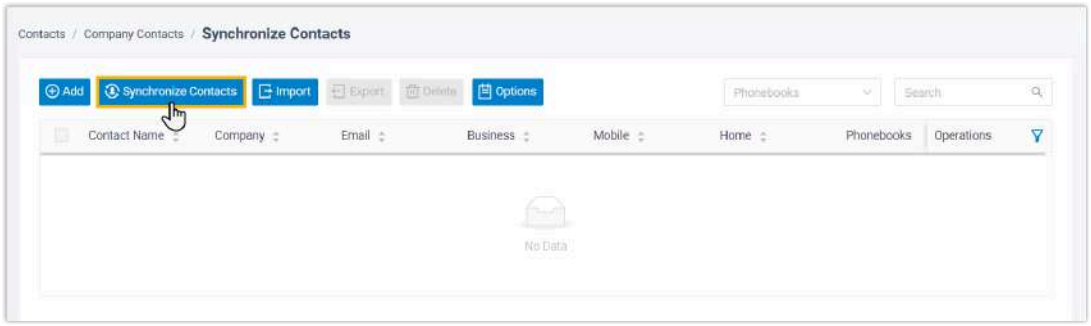
- The **Status** field displays **Disabled**.
- The Microsoft SQL configurations are retained, and can be used directly the next time the integration is enabled again.

Disconnect Microsoft SQL Integration

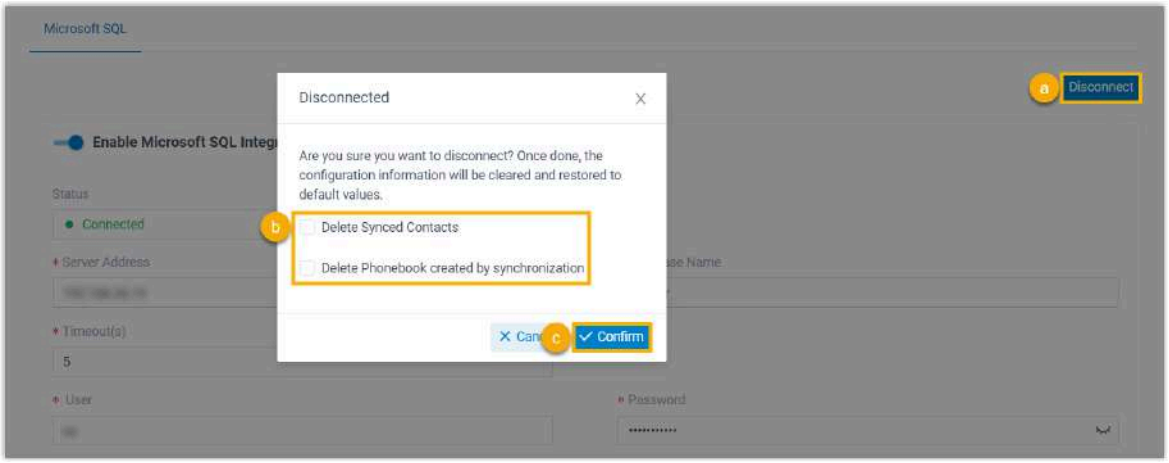
If you want to integrate with another database, you need to disconnect the current Microsoft SQL integration first.

Procedure

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



2. Disconnect Microsoft SQL integration.



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

Result

The Microsoft SQL integration is disconnected.

LDAP Server

LDAP Server Integration Guide

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

Requirements

Item	Requirement
Yeastar PBX	• **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP) • **Firmware**: Version 83.18.0.102 or later
Third-party LDAP Server	No requirement.

Integration flow

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

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

Scenario: Caller ID name display

1. Integrate Yeastar P-Series Software Edition with LDAP Server

Scenario: Caller ID name display and contact synchronization

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

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

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

3. Set up inbound routes based on phonebook matches

Integrate Yeastar P-Series Software Edition with LDAP Server

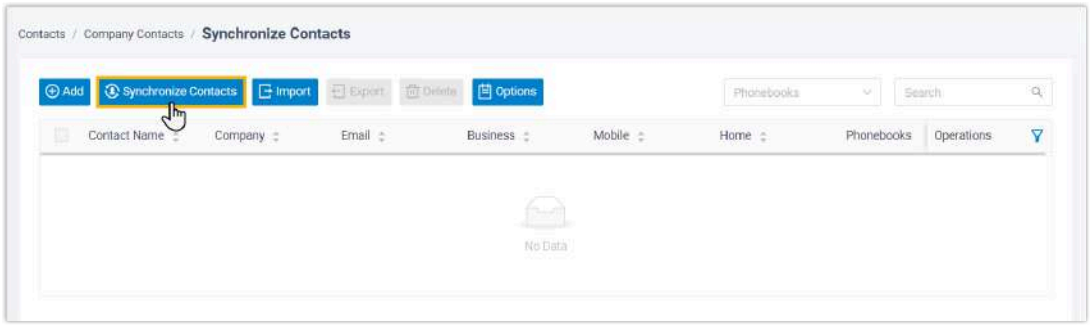
With the integration between Yeastar P-Series Software Edition and LDAP server, inbound calls to PBX will automatically trigger contact lookup in your LDAP server and display the caller's name if a match is found.

Requirements

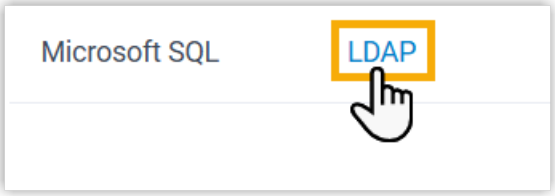
Item	Requirement
Yeastar PBX	• **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP) • **Firmware**: Version 83.18.0.102 or later
Third-party LDAP Server	No requirement.

Step 1. Enable LDAP integration

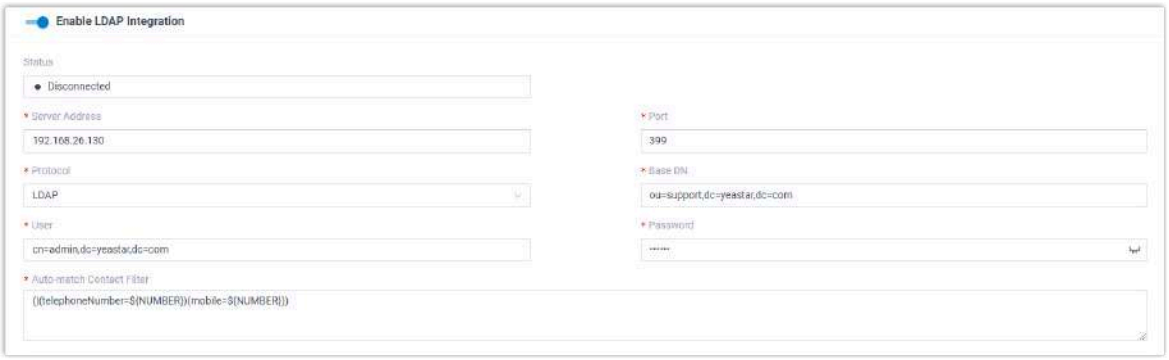
1. Access the LDAP configuration page.
   a. Log in to PBX web portal, go to **Contacts > Company Contacts**.
   b. At the top of the page, click **Synchronize Contacts**.



   c. Click **LDAP** tab.



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

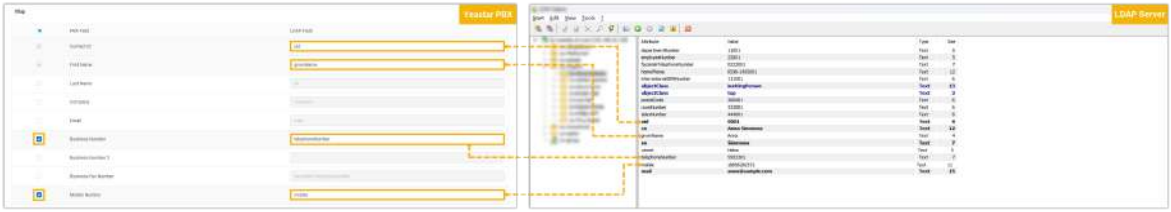


Item	Description
Server Address	Enter the address of LDAP server.
Port	Enter the port on which LDAP server is running.
Protocol	Select an LDAP protocol. • **LDAP**: Transmit data in plain text. • **LDAPS**: Use SSL (Secure Sockets Layer) or TLS (Transport Layer Security) to encrypt and authenticate the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

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

Step 2. Map contact fields between Yeastar P-Series Software Edition and LDAP server

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

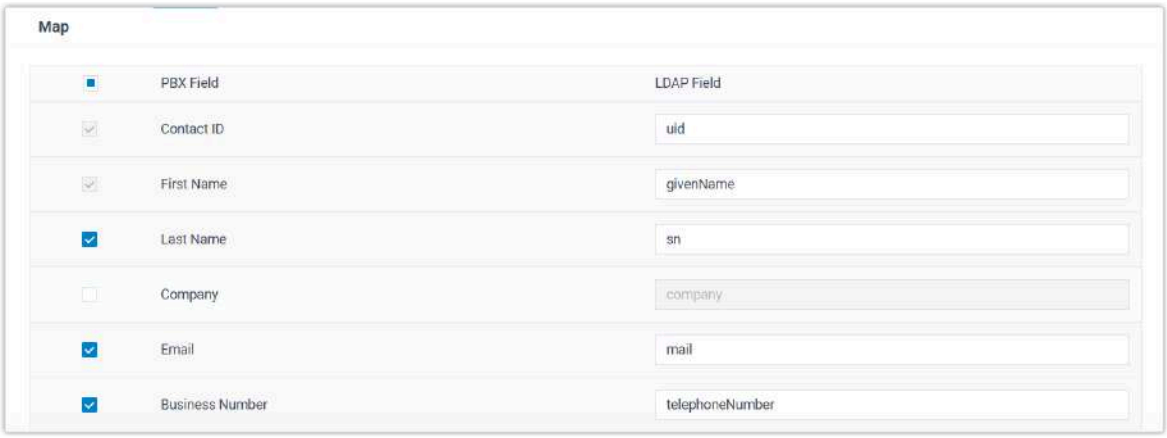


   a. For **Contact ID**, **First Name**, **Business Number**, and **Mobile Number**, enter the corresponding LDAP attribute name.

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

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

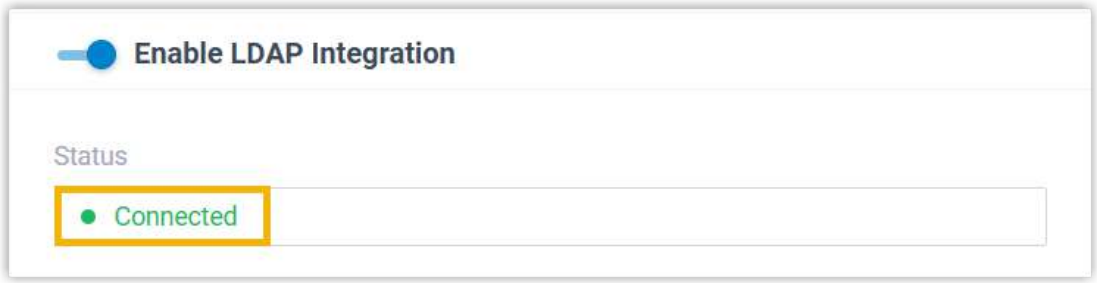
   b. **Optional:** To display contact's last name as well, select the checkbox of **Last Name**, then enter the corresponding LDAP attribute name.
3. If you want to synchronize LDAP contacts to PBX, enable and map the desired fields.



4. Click **Save**.

Result

- Yeastar P-Series Software Edition is connected to your LDAP server.



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

What to do next

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

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

Set up Contact Synchronization from LDAP Server

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

Restrictions

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

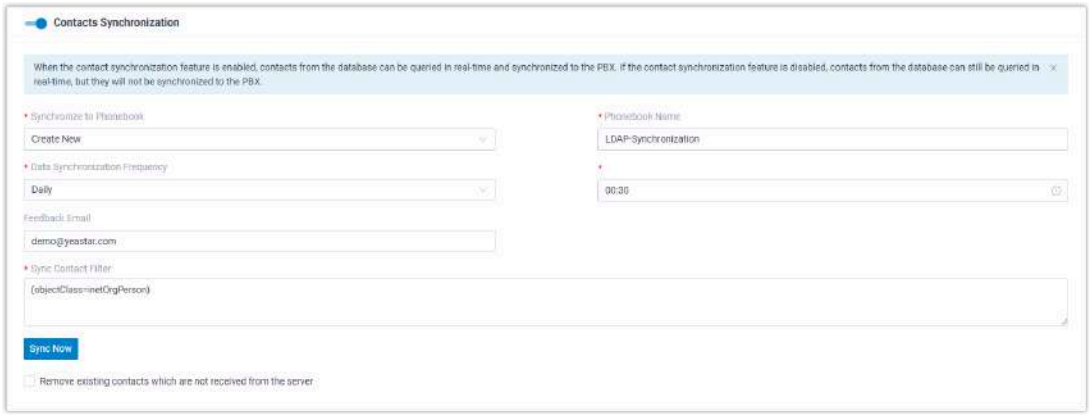
Maximum Number of Extensions (N)	N < 1000	N ≥ 1000
Company contacts (total)	200,000	500,000
Company phonebooks	200	500

Prerequisites

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

Procedure

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



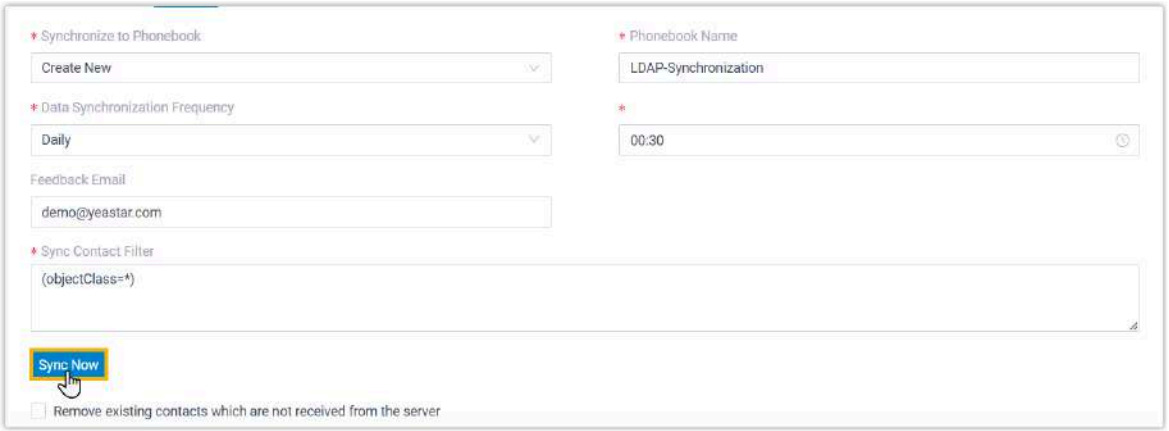
Item	Description
Synchronize to Phonebook	Select where to store the contacts that will be synchronized from LDAP server. • **Create New**: Create a new phonebook from scratch to store the synced contacts. If you choose the option, enter the phonebook name in the **Phonebook Name** field. • **Read Specific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

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

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

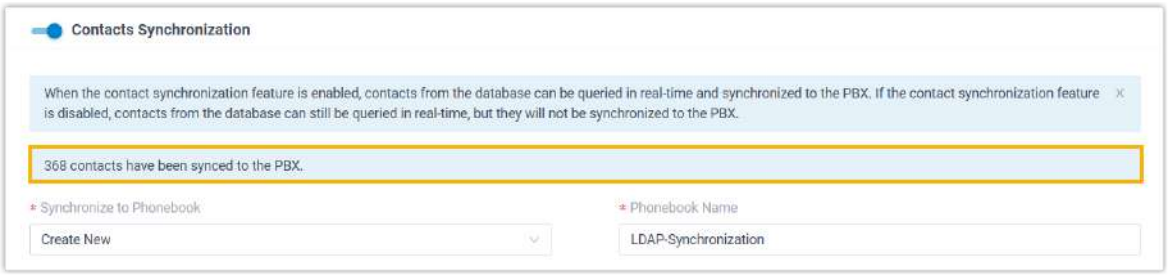
c. Click **Save**.

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



Result

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

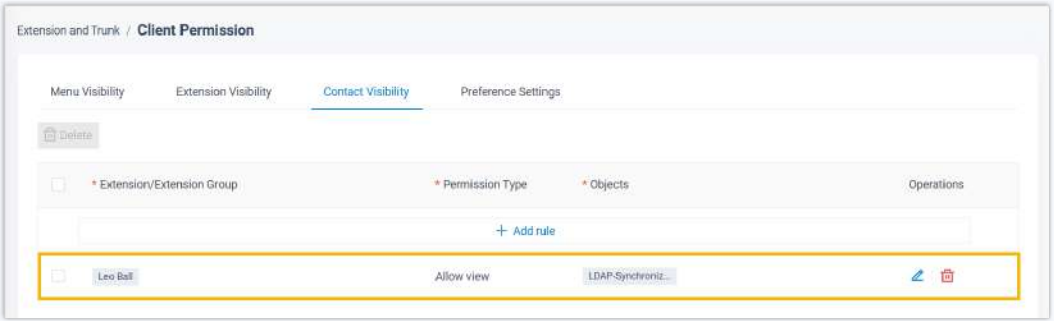


- You can check the synchronized contacts and the associated phonebook(s) in **Contacts > Company Contacts / Phonebooks**, which are tagged as LDAP.

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

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

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



What to do next

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

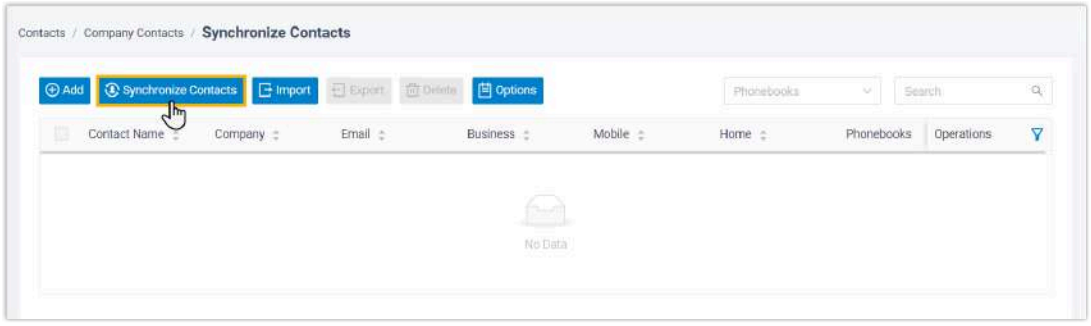
For more information, see Route Inbound Calls by Matched Phonebook Contacts.

Disable LDAP Integration

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

Procedure

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



   c. Click **LDAP** tab.

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

3. Click **Save**.

Result

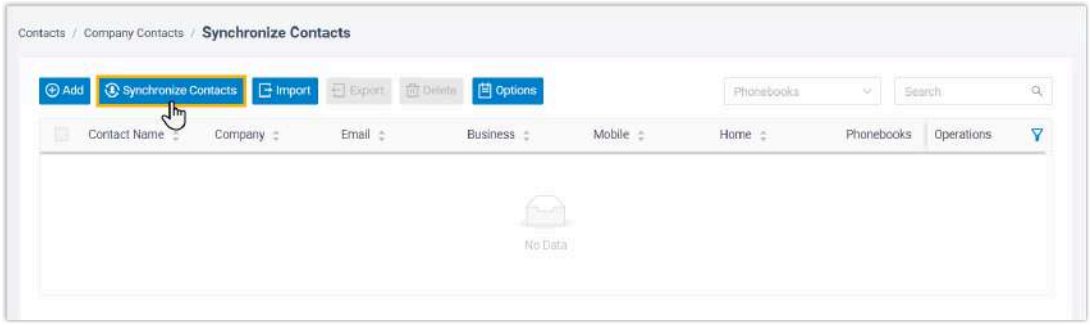
- The **Status** field displays **Disabled**.
- The LDAP configurations are retained, and can be used directly the next time the integration is enabled again.

Disconnect LDAP Integration

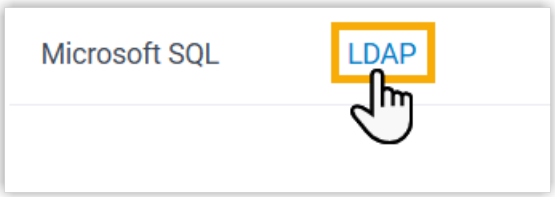
If you want to integrate with another database, you need to disconnect the current LDAP integration first.

Procedure

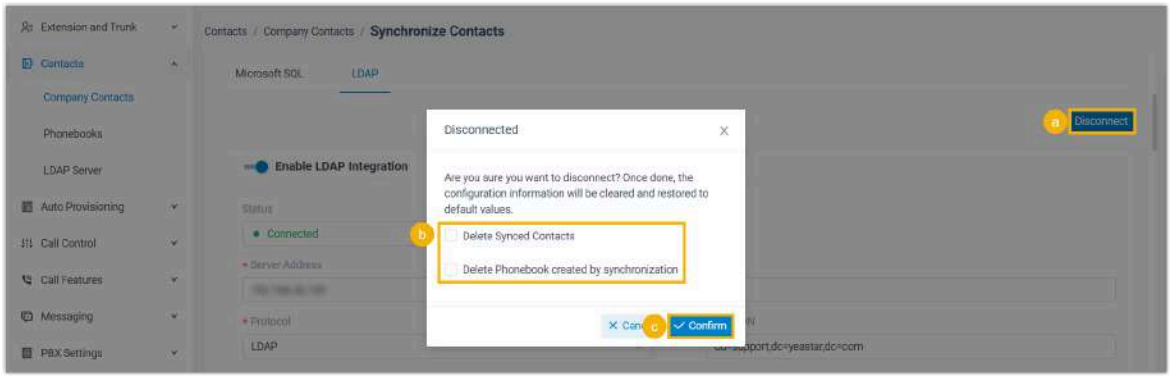
1. Access the LDAP configuration page.
   a. Log in to PBX web portal, go to **Contacts > Company Contacts**.
   b. At the top of the page, click **Synchronize Contacts**.



   c. Click **LDAP** tab.



2. Disconnect LDAP integration.



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

Result

The LDAP integration is disconnected.

Phonebook

Add and Manage Company Phonebooks

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

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 types of phonebooks:

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

  You can manually create phonebooks to group company contacts.
- **Third-party company phonebook**: The phonebooks that store company contacts synchronized from the third-party system integration.

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

Add a company phonebook

1. Log in to PBX web portal.
2. Go to **Contacts > Phonebooks**, click **Add**.
3. In the **Phonebook Name** field, enter a name to help you identify it.
4. In the **Members** section, select desired company contacts.

   Define a All Contacts phonebook

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

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

   Group specific contacts into a phonebook

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

Edit a company phonebook

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

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

Delete company phonebooks

1. Log in to PBX web portal, go to **Contacts > Phonebooks**.
2. To delete a phonebook, select the desired phonebook, click and **OK**.
3. To delete phonebooks in bulk, select the checkboxes of the desired phonebooks, click **Delete** and **OK**.
   The phonebooks are removed from PBX server and users' Linkus clients.

> **Note:**
> Company contacts in the phonebook are still kept in the system.

Related information

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

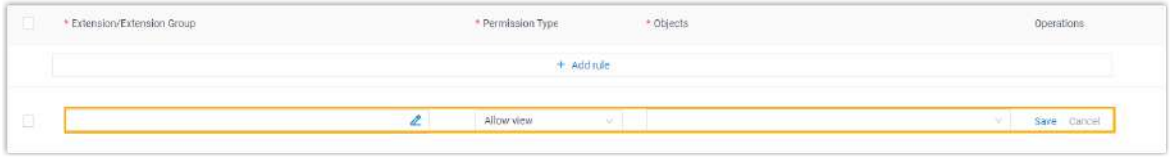
Contacts Visibility

Set up Contact Visibility

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

Procedure

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



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

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

b. Click **Save**.

Result

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

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

Manage Contact Visibility Rules

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

Edit a contact visibility rule

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

Delete contact visibility rules

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

Identify Callers from Contacts

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

Background information

Caller ID match is supported on all kinds of endpoints, including Linkus clients, desk phones, or softphones. Yeastar P-Series 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)
    - Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
    - Auto Provision IP Phones Remotely (Provision Link Method)
- If users' extensions have been associated with phones, reprovision the phones to take effect.
    a. Go to **Auto Provisioning > Phones**.
    b. Select the checkboxes of the desired phones, click **Reprovision**.

Result

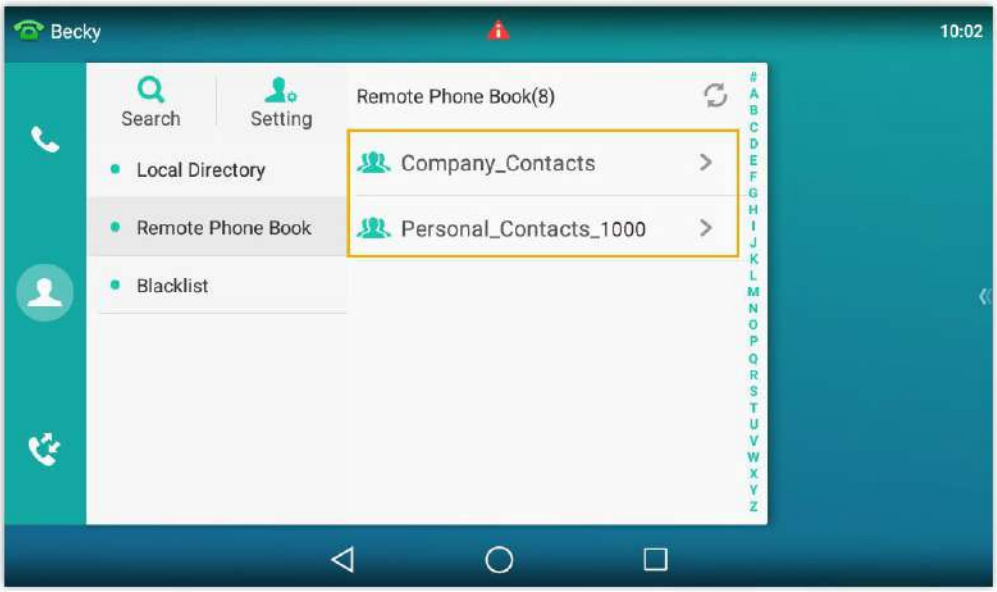
Contacts data are synchronized to IP phones' remote phonebooks. Users can query and place calls to contacts from the remote phonebook.

> **Note:**
> Two remote phonebooks from the PBX server are displayed on the IP phone:
>
> - **Company_Contacts**: Saves all the company shared contacts that you can view.
>
> > **Note:**
> > Company contacts on IP phones can NOT be grouped into phonebooks.
>
> - **Personal_Contacts_*{extension_number}***: Saves all your personal contacts.

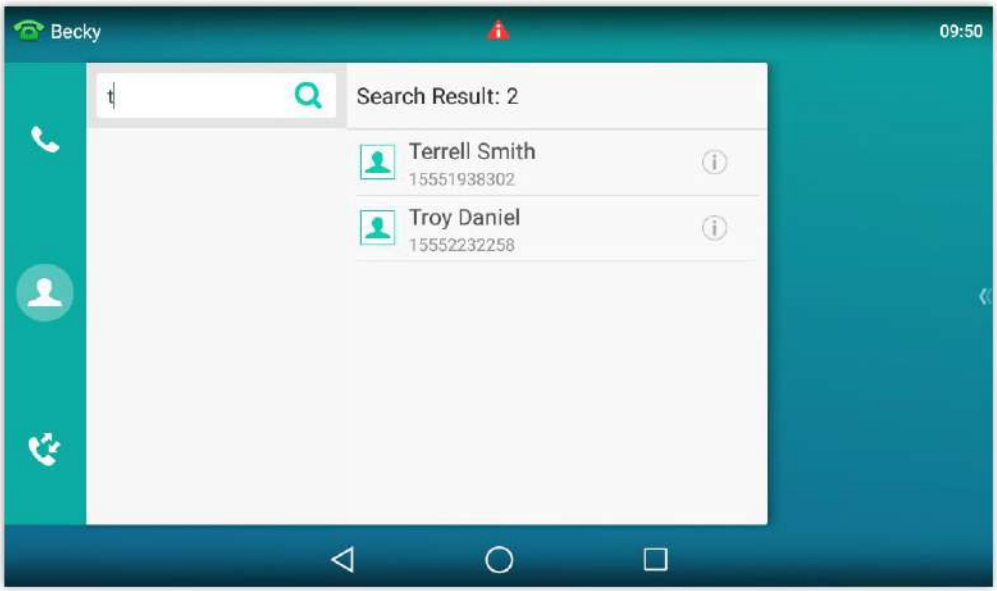
Example: Query contacts on Yealink T56A IP phone

1. Tap > **Remote Phonebook**.

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



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



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

Client Permission

Yeastar P-Series Software Edition Client Permissions

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

Linkus clients menu and operation permissions

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

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

For more information, seeSet up User Permissions of Linkus Clients .

Extension visibility permission

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

For more information, see Set up Extension Visibility.

Contact visibility permission

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

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

For more information, see Set up Contact Visibility.

LDAP Server

LDAP Server Overview

Yeastar P-Series 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.

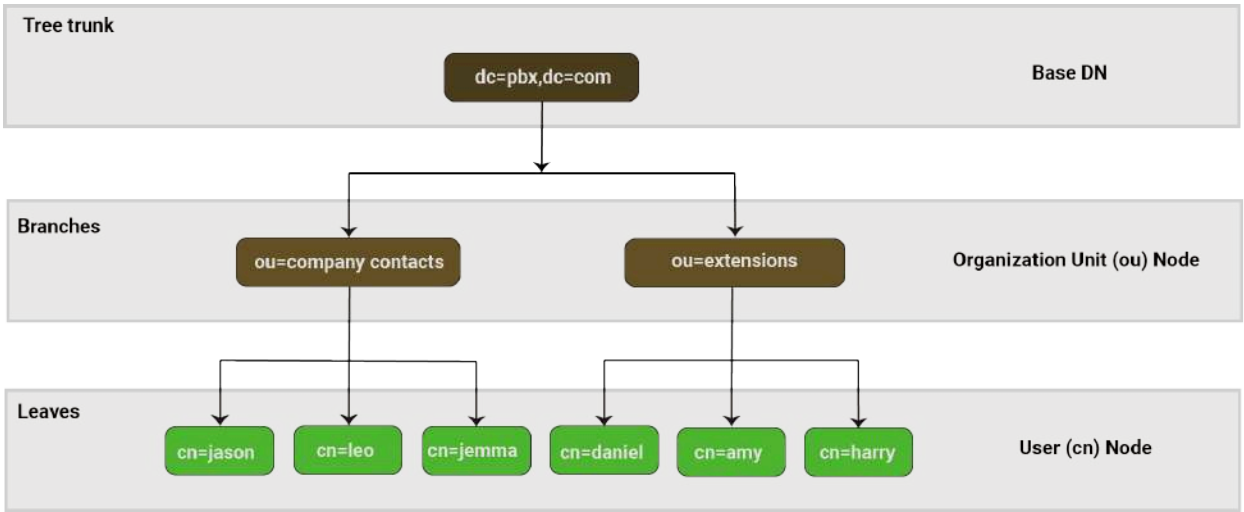
LDAP introduction

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`.

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

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

Object Classes

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

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

Related information

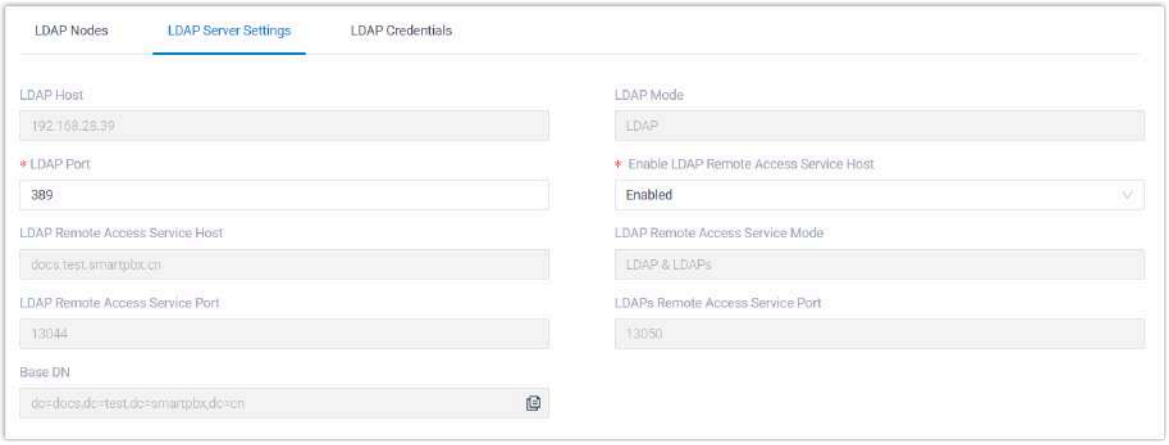
Set up Yeastar P-Series Software Edition as an LDAP Server

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.



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:**

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

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

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

Result

The Yeastar P-Series 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

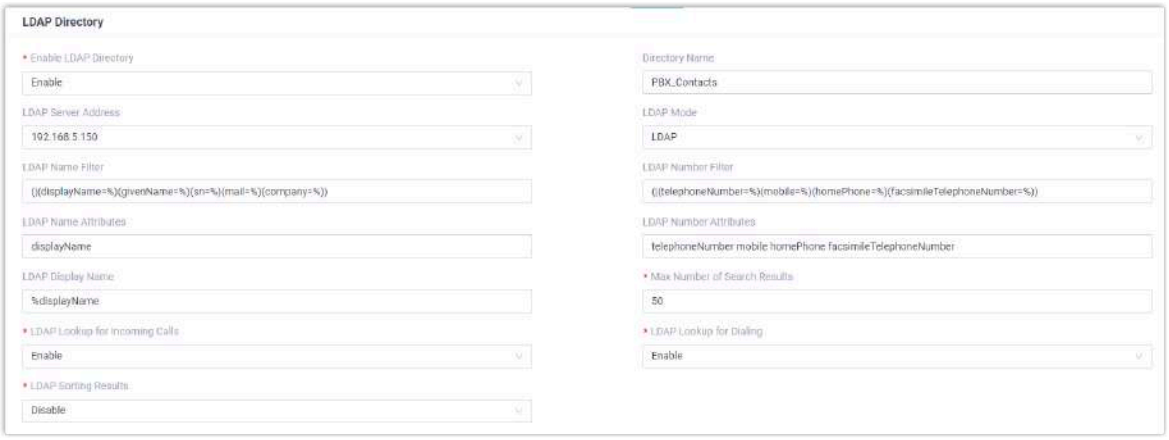
- Make sure the PBX version is 83.6.0.24 or later.
- You have set up the PBX as an LDAP server.
- The phone is connected to Yeastar P-Series Software Edition via Auto Provisioning, and has been assigned with an extension.

  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

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



Setting	Description	Example
Enable LDAP Directory	Enable or disable the LDAP directory feature.	Enable
Directory Name	Specify a name for the LDAP directory.	PBX_Contacts
LDAP Server Address	Enter the LDAP Server address of Yeastar P-Series 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.	(|(telephoneNumber=%)(mobile=%) (homePhone=%)(facsimileTelephoneNumber=%))

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

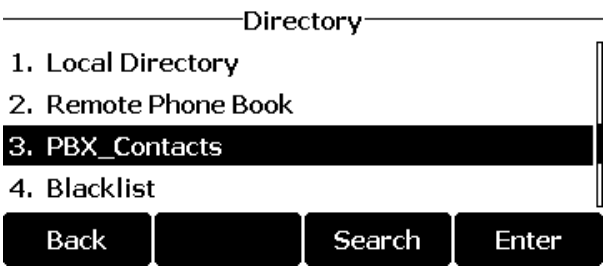
3. Click **Save**.

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

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

Result

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



Related information

Auto Provision Function Keys for Phones

Manual Configuration Examples

LDAP Configurations on Yealink Phones

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

Configuration example

The example configurations are set according to default settings of Yeastar P-Series 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 set up the PBX as an LDAP server.

Procedure

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

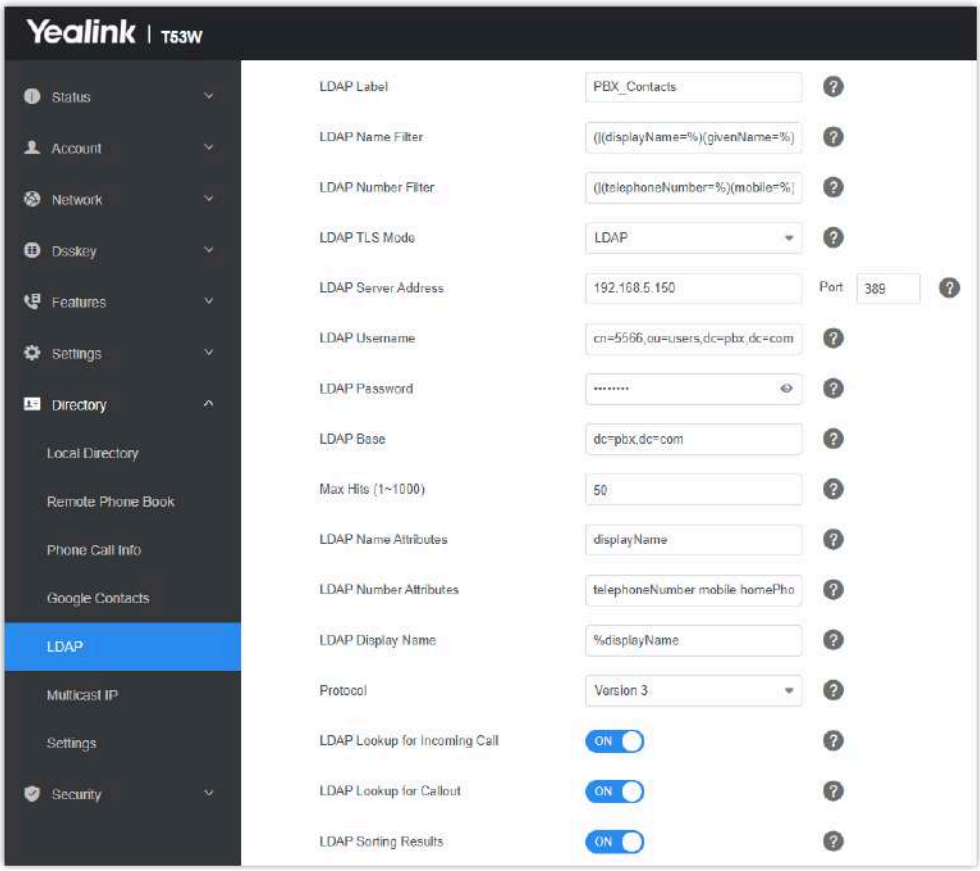


Table 6.

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.

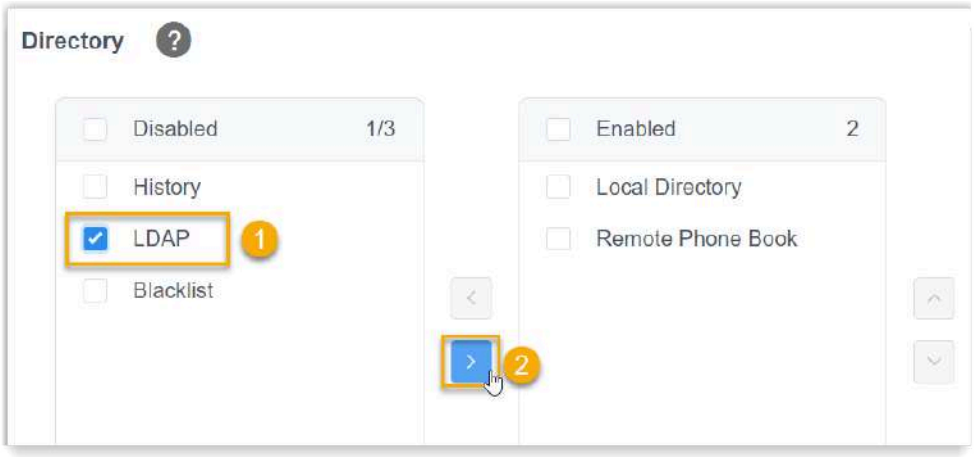
Result

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

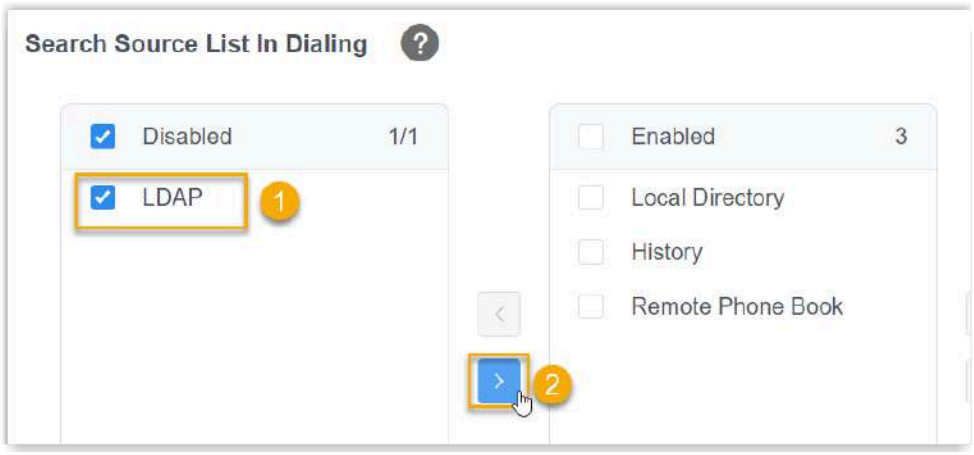
Search contacts via Directory

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.



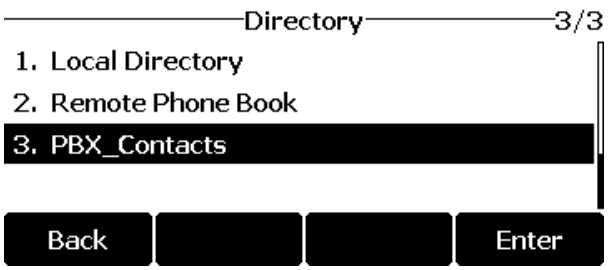
3. **Optional:** In the **Search Source List In Dialing** section, add **LDAP** from the **Disabled** box to the **Enabled** box.



4. Click **Confirm**.

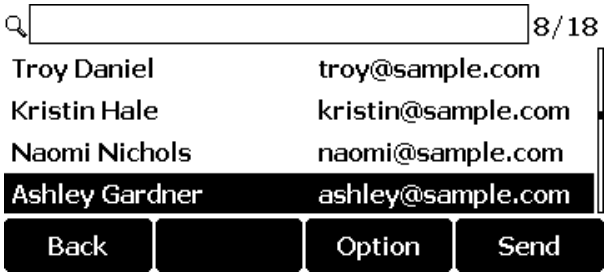
Search LDAP Contacts

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



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

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



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

Search contacts via LDAP key

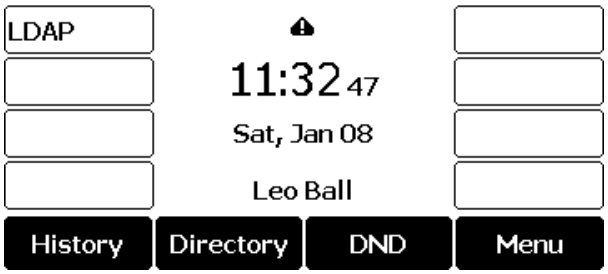
Set an LDAP Key on Yealink Phone

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

3. Click **Confirm**.

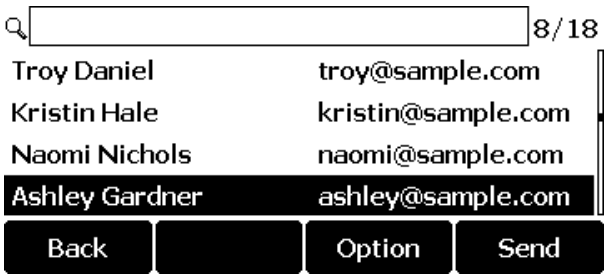
Search LDAP Contacts

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



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

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



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

Organization

Organization Overview

Organizational structure is the group of rules, roles, relationships, and responsibilities that outline how your company's activities are directed to meet its goals. Yeastar P-Series 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

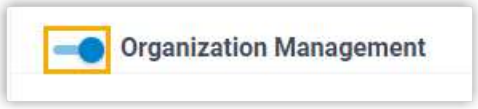
To group extension users into departments, you need to enable the **Organization Management** feature.

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.

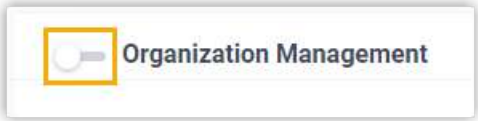
What to do next

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

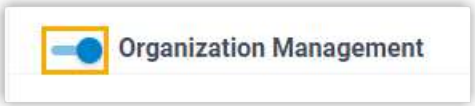
Maximum Number of Extensions (N)	N ≤500	N > 500
Layers of Departments	15	20
Number of Departments	100	1000

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.

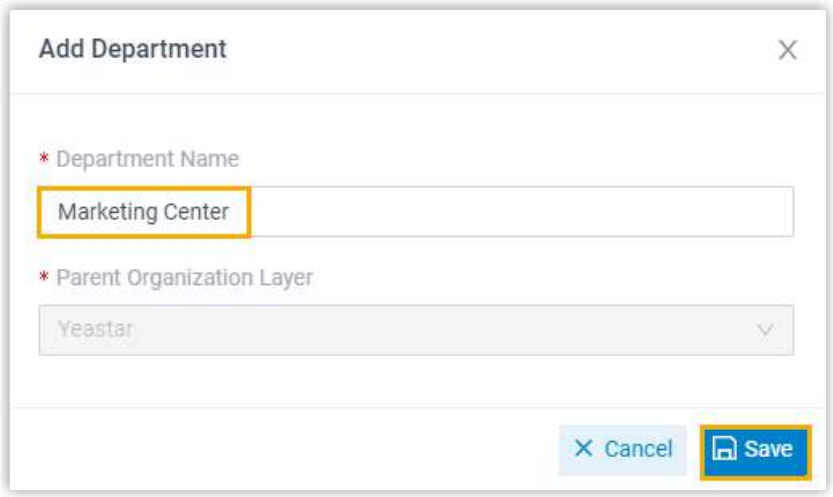
4. Click **Save** and **Apply**.

Step 2. Create departments

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

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

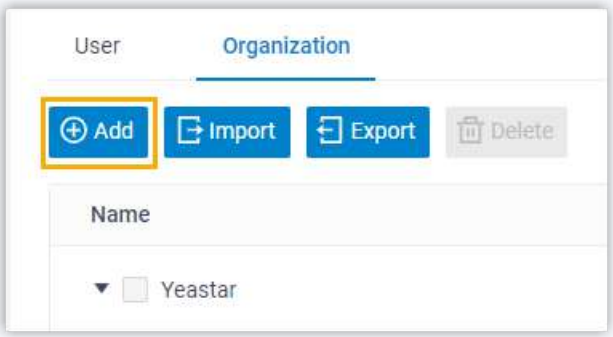
2. Click + beside the root organization.
3. In the pop-up window, configure the following information, then click **Save**.



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

Result

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

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

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

What to do next

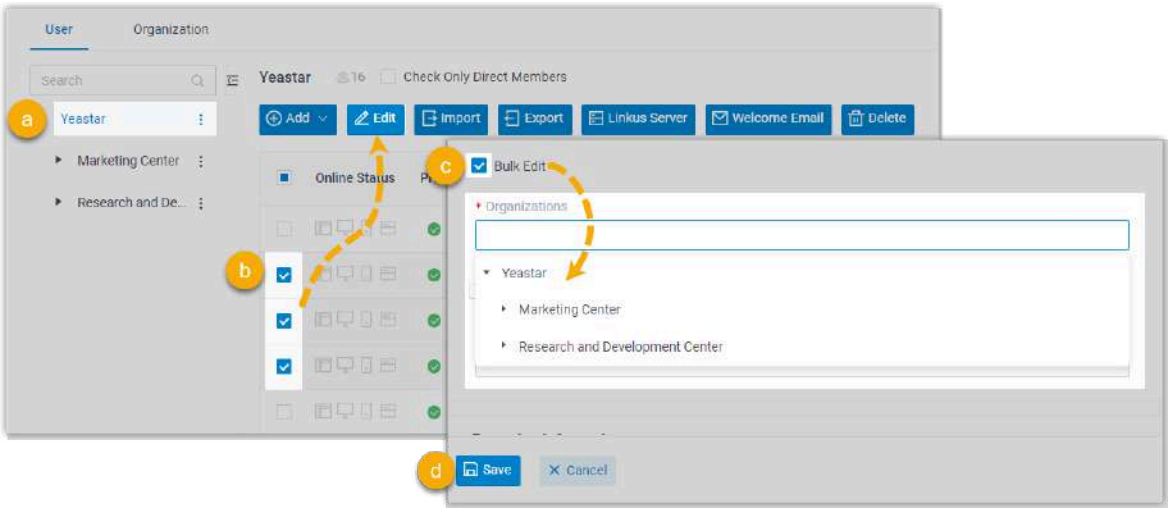
Add Users to Organizations.

Add Users to Organizations

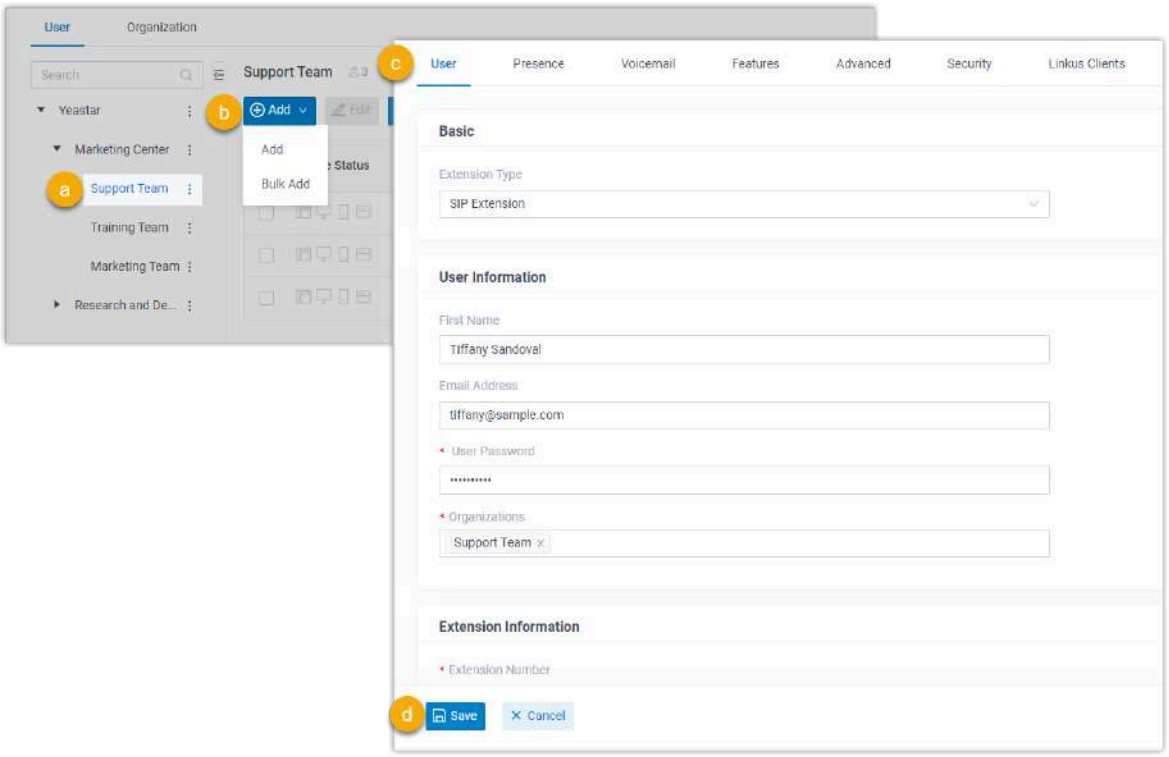
After setting up organizations, you need to group users into departments. This topic describes how to add users to departments.

Procedure

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



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



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

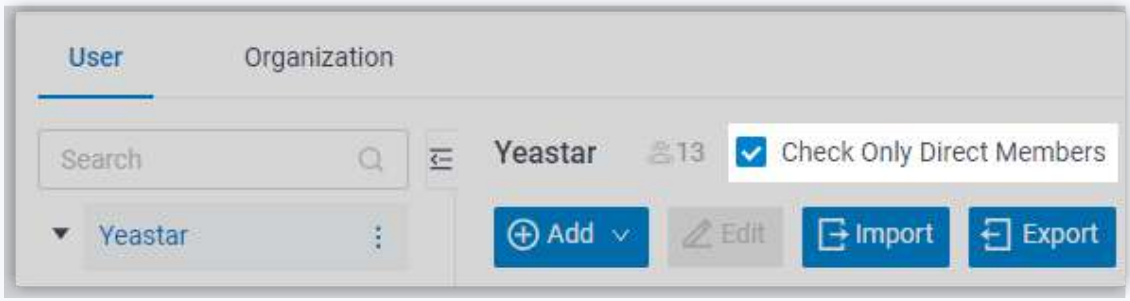
> **Note:**
> **Organization** is auto filled with the one that you have selected.

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

Result

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

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



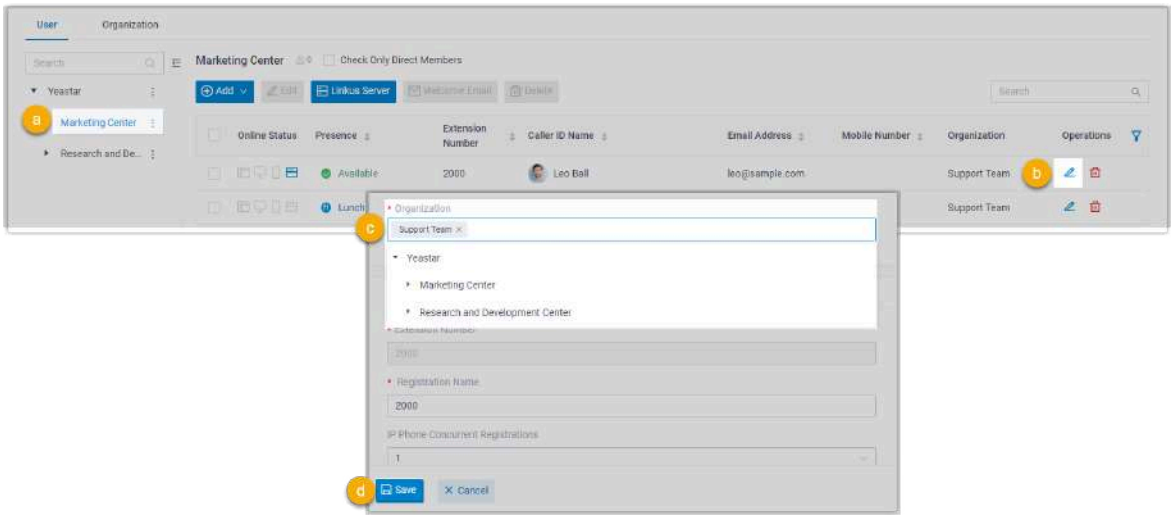
Manage Users within Organizations

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

Change users' departments

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

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



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

   All the extensions within the department are displayed.

b. Click beside a desired extension.

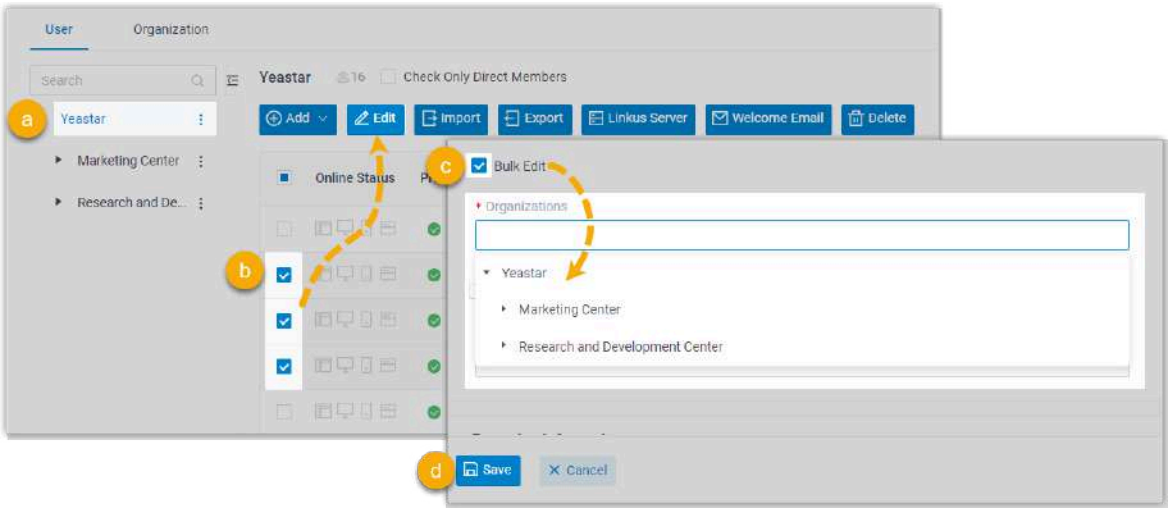
c. In the **Organization** field , change department as needed.

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

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

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

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



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

   All the extensions within the organization are displayed.

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

   The departments to which the extensions belong are cleared.

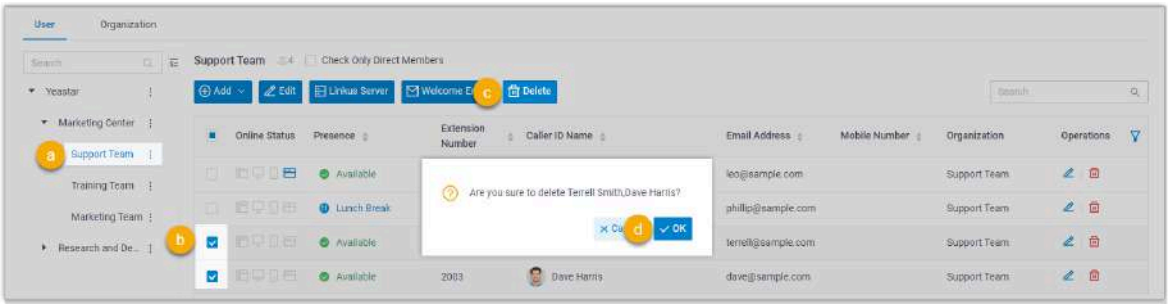
c. Select the checkbox of **Bulk Edit** for organization, then reselect departments.

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

Remove users from departments

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

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



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

   All the extensions within the department are displayed.

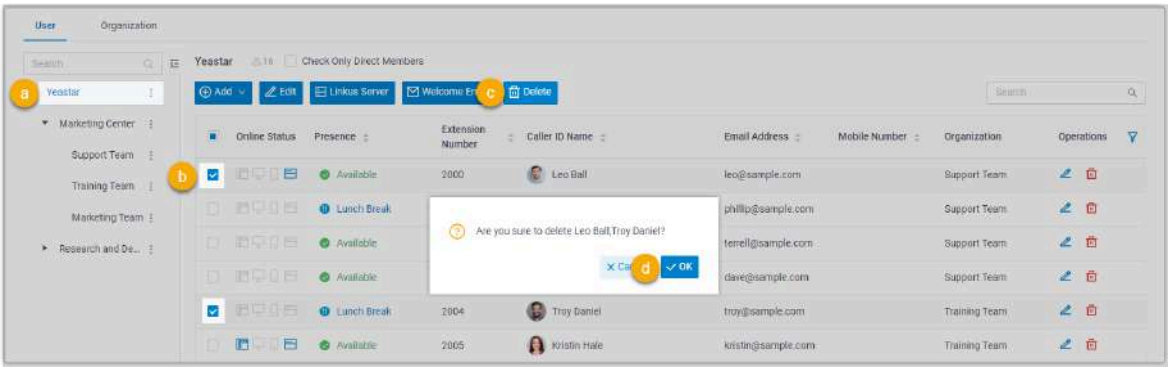
b. Select the checkboxes of desired extensions, then click **Delete**.

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

d. Click **Apply**.

   The selected extensions are deleted from the system.

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



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

   All the extensions within the organization are displayed.

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

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

d. Click **Apply**.

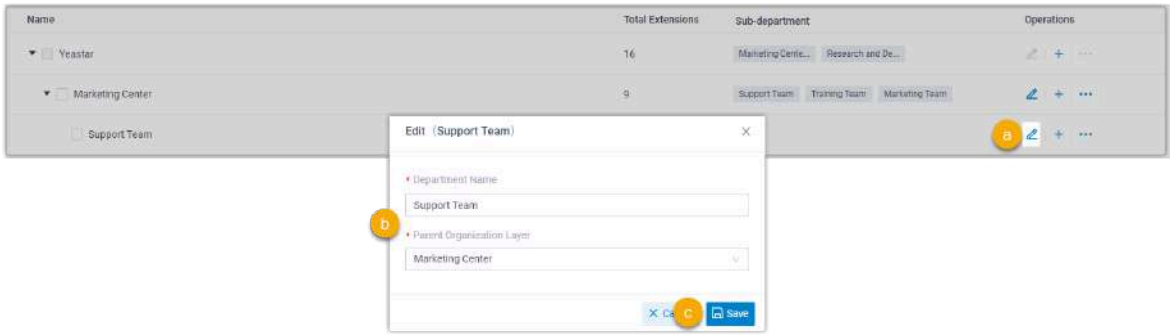
   The selected extensions are deleted from the system.

Manage Organizations

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

Procedure

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



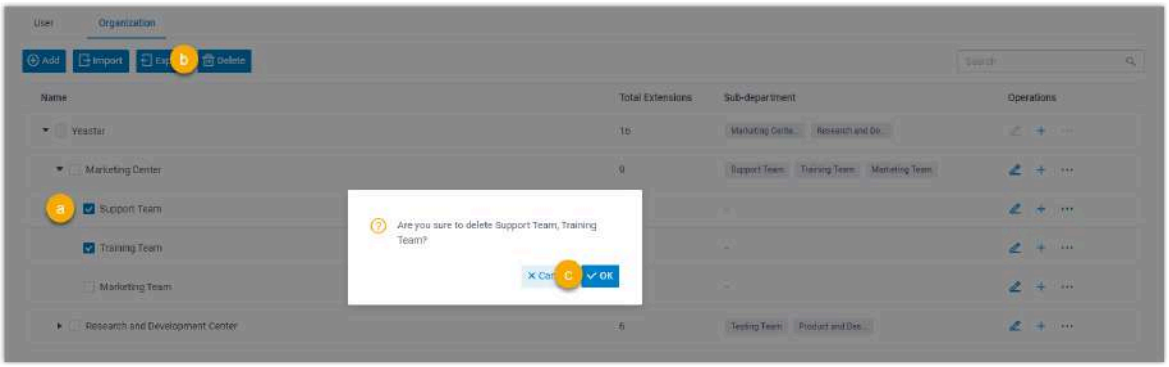
   a. Click beside the desired department.
   b. In the pop-up window, rename department or change parent organization layer.
   c. Click **Save**.
3. To adjust the order of departments, click , then select **Move Up** or **Move Down** to adjust the order.

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

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

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

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



Export and Import Organizations

The organizations configured on Yeastar P-Series 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 on Operator Panel and Extension Page. 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)	√	×

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

Module	Permission	Manager	User
	regardless of users' visibility permission for company contacts.		

Custom user type

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

For more information, see View or change permissions for a member with custom user type.

Default extension group

Yeastar P-Series 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

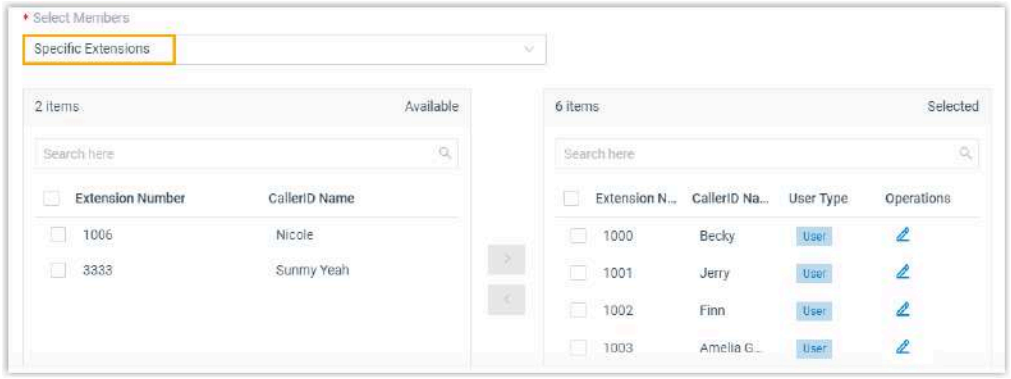
This topic describes how to create an extension group.

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.



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

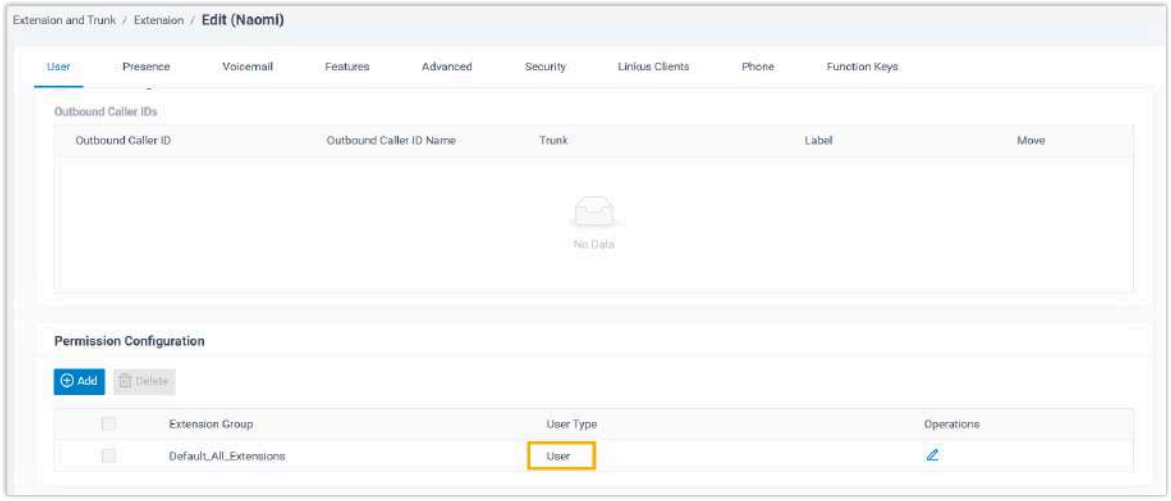
The member's user type and permissions in the group are updated.

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. In the **User** tab, scroll down to the **Permission Configuration** section, you can see all the groups to which the extension user belongs. Check the user's user type in each group in **User Type** column.



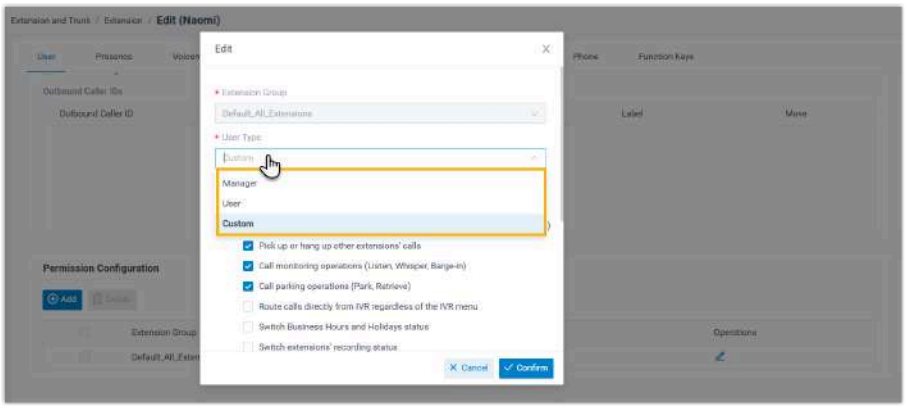
Change a member's user type in multiple groups

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

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, click beside desired extension.

2. In the **User** tab, scroll down to the **Permission Configuration** section, change the extension user's user type in a group.
    a. Click beside the desired extension group.
    b. In the **User Type** drop-down list, select a user type.
        - If you select **Manager** or **User**, the user has all the permissions that are granted to the user type.
        - If you select **Custom**, select the checkboxes of the desired permissions.



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

Result

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

Related information

Assign a User Type to a Group Member

View or Change Permissions for Group Members

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

View or change permissions for managers and users

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

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension Group**, edit the desired extension group.
2. Click **Group Permissions** tab.

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

        > **Note:**
        > To achieve this, you need to upgrade PBX to version 83.16.0.25 or later and extension users need to upgrade Linkus Desktop Client to version 1.6.0 or later.

   b. Click **Save** and **Apply**.

Result

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

What to do next

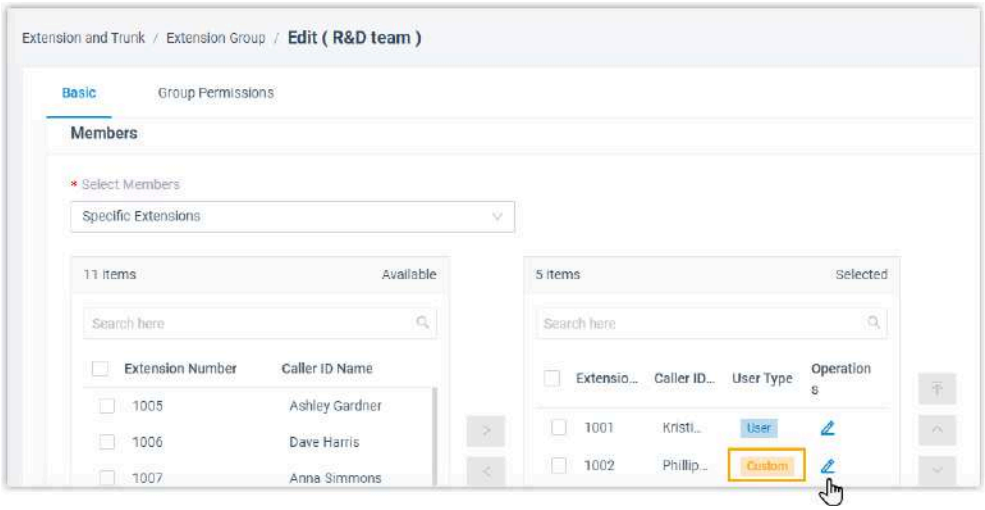
If you want to change members' user types to **Manager** or **User** in the group, see Assign a default user type to a group member.

View or change permissions for a member with custom user type

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

Procedure

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



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

Result

The member's permissions are updated.

Auto Provisioning

Auto Provisioning Overview

Auto Provisioning is a time-saving feature that helps you to manage and deploy IP phones and gateways centrally on Yeastar P-Series 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 four Auto Provisioning methods, you can select a method to provision your IP phones and gateways according to your network environment.

PnP (Plug and Play)

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

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

DHCP Option 66

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

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

RPS

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

Note:

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

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

Provision Link

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

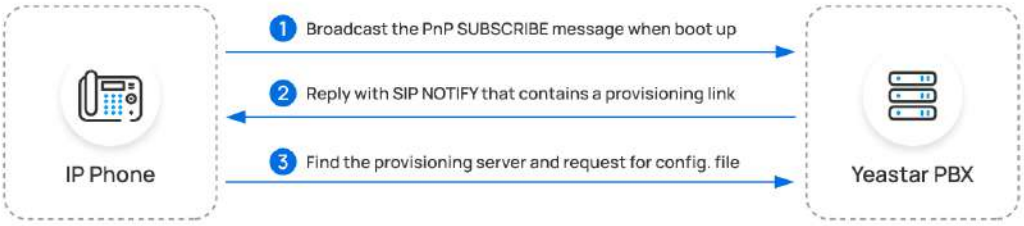
> **Note:**
> Cisco IP phones do not support Provision Link Auto Provisioning method.

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

How Auto Provisioning works

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

PnP Provisioning



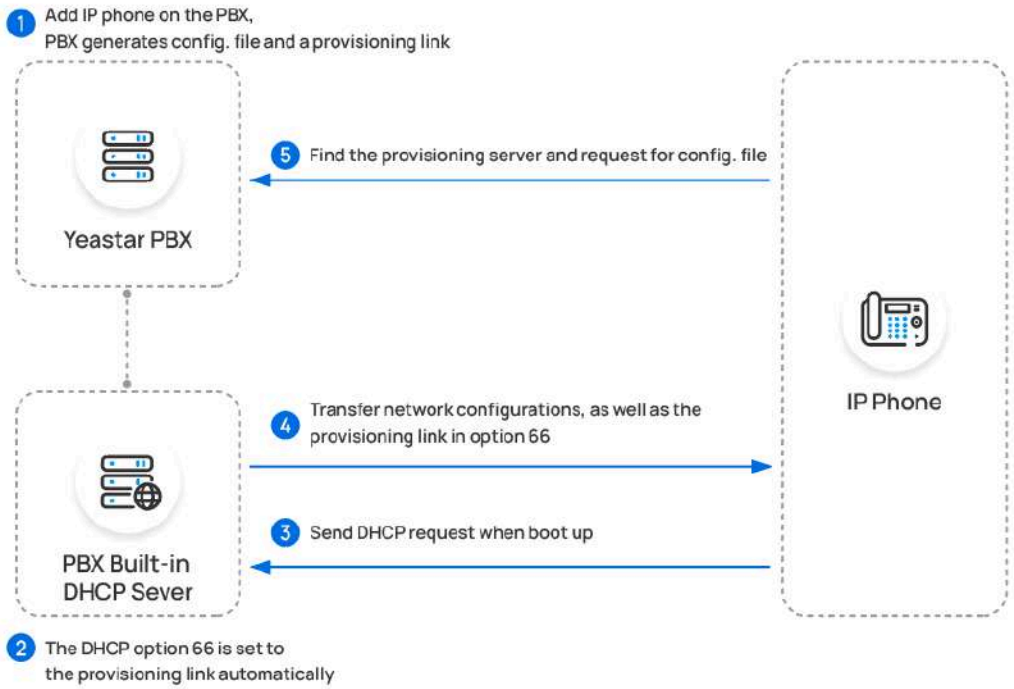
DHCP Provisioning

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

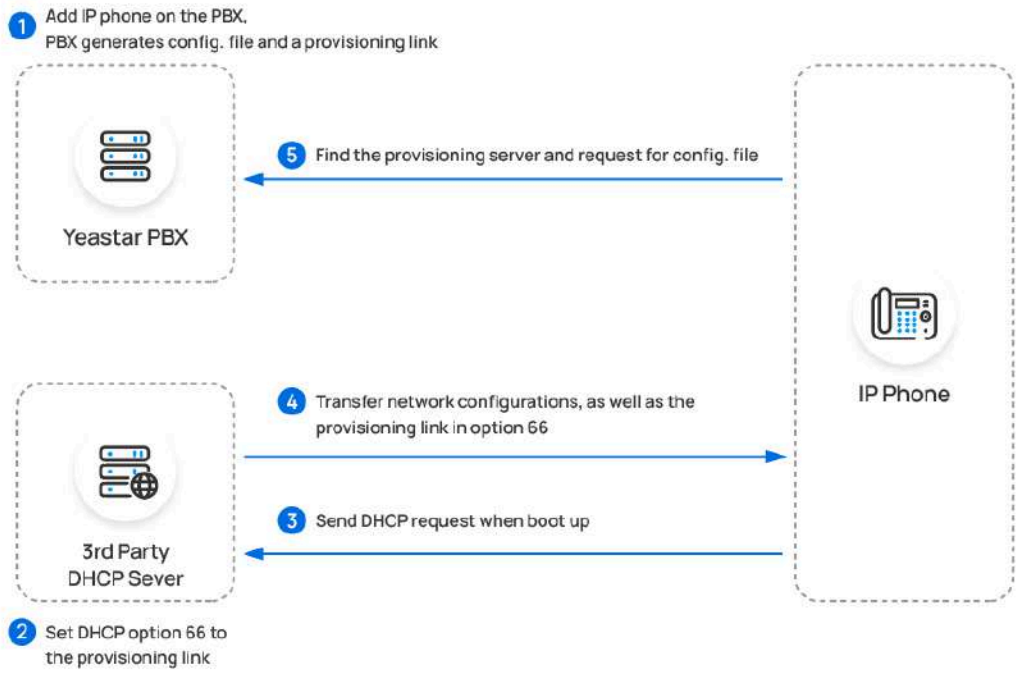
> **Note:**

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

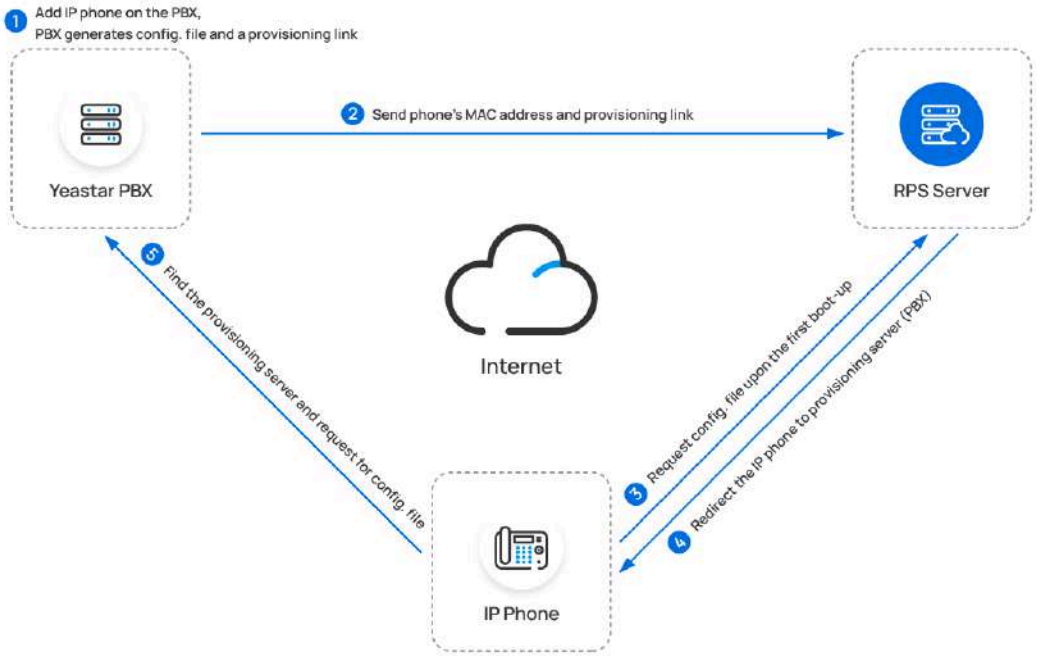
Using the PBX as a DHCP server



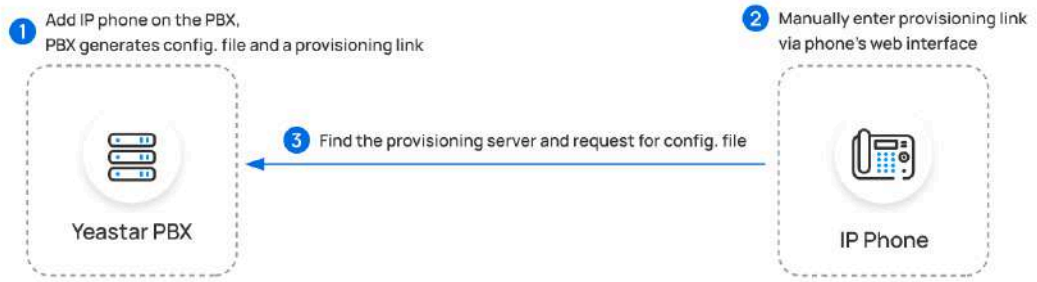
Using a third-party DHCP server



RPS Provisioning



Provision Link



Related information

IP Phone Configuration Guides

Provision IP Phones

Auto Provision IP Phones in Local Network (PnP Method)

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

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

Supported IP phones

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

Prerequisites

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

    IP: 192.168.5.150, Mask: 255.255.255.0

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

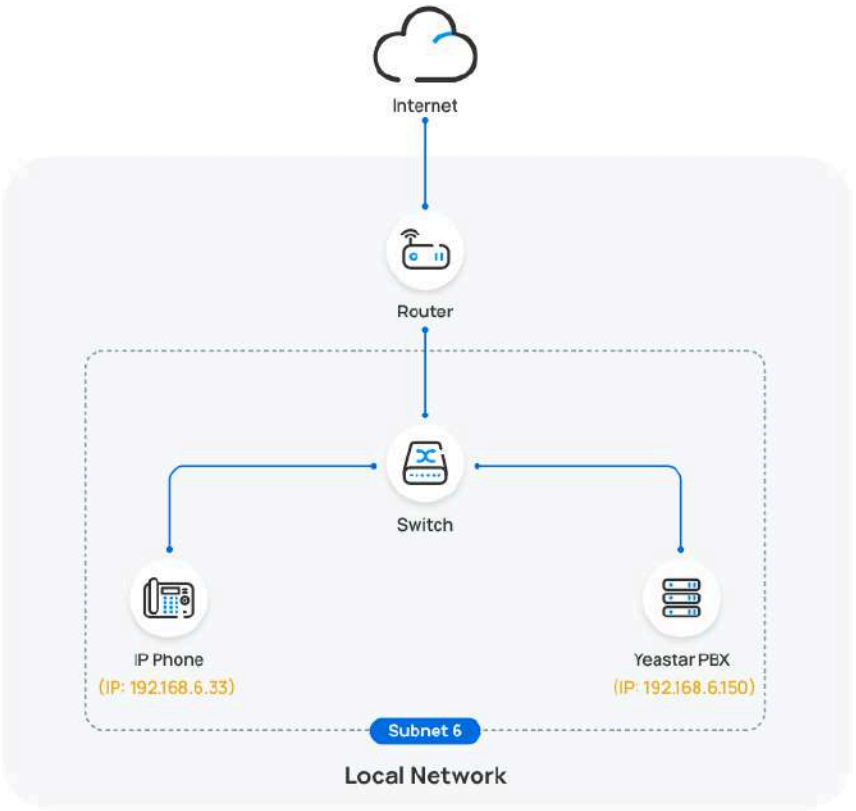
    IP: 192.168.5.150, Mask: 255.255.255.0

IP: 192.168.66.170, Mask: 255.255.255.0

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

Scenario

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



Procedure

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

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

> **Note:**
> - Only the supported devices can be discovered and displayed on the phone provisioning list.
> - Restart the phones if they are not discovered and displayed on the phone provisioning list.

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

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

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

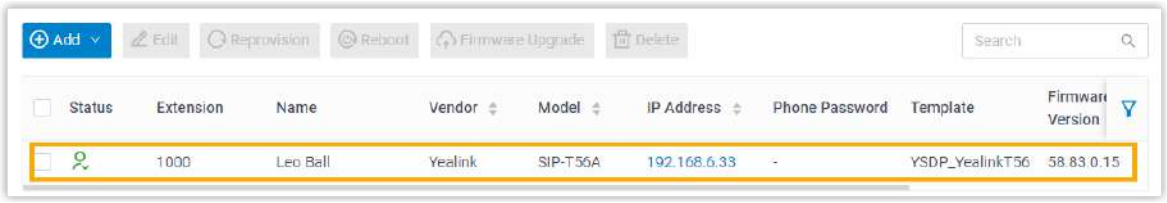
     A provisioning server URL is generated automatically and displayed on the web page.
6. In the **Assign Extension** section, assign an extension for the phone.

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

Result

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

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



Related information

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

Auto Provision IP Phones in Local Network (DHCP Method)

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

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

Supported IP phones

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

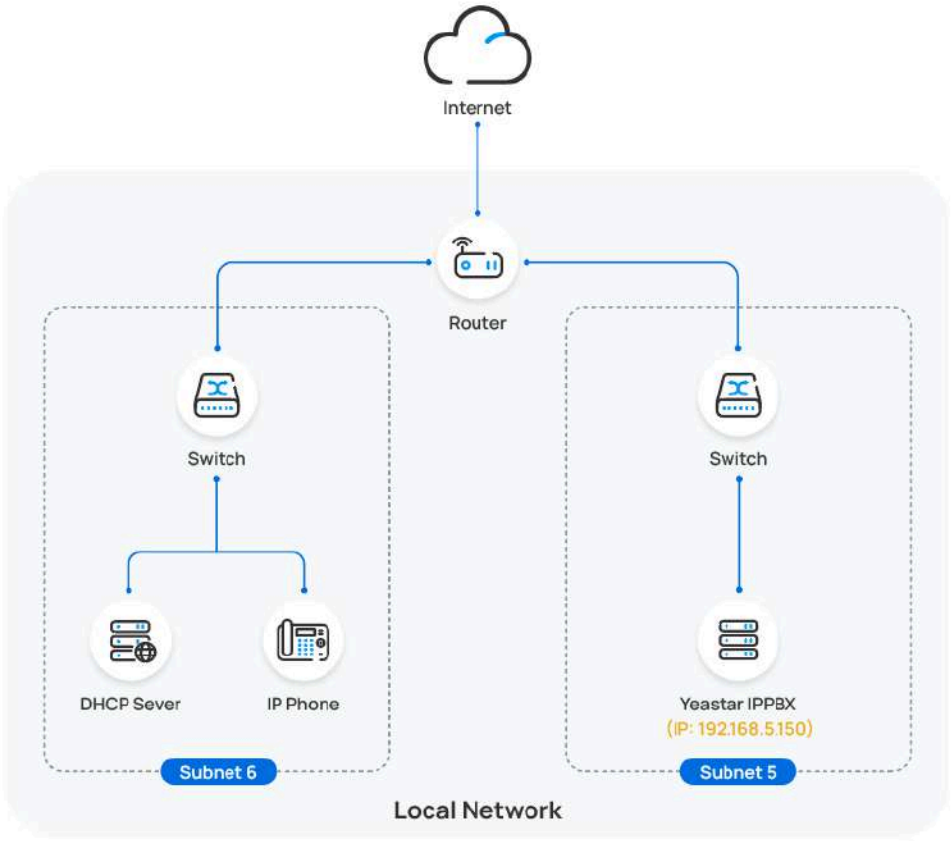
Prerequisites

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

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

Scenario

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



Procedure

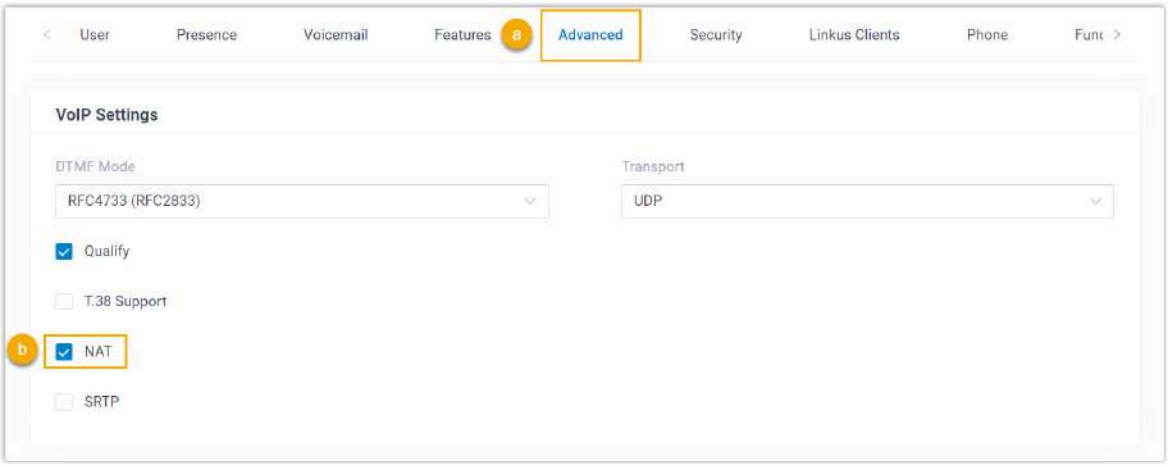
Step1. Set a remote extension

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

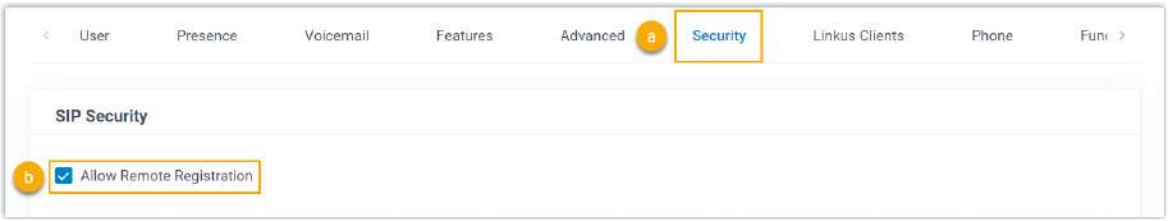
Step3. Set up a DHCP option 66

Step1. Set a remote extension

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



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



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

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

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

1. RESET the phone if it is previously used.
2. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
3. Click **Add** to add a phone to the PBX.
4. In the **IP Phone** section, configure phone information as follows:
    - **Vendor**: Select a phone vendor.
    - **Model**: Select a phone model.
    - **MAC Address**: Enter MAC address of the phone.
5. In the **Options** section, configure the following settings.

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

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

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

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

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

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

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

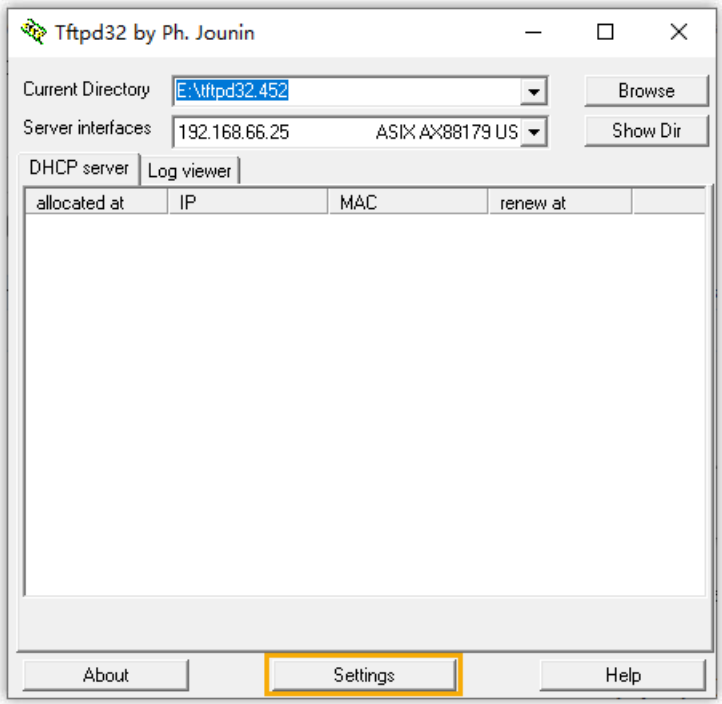
7. Click **Save**.

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

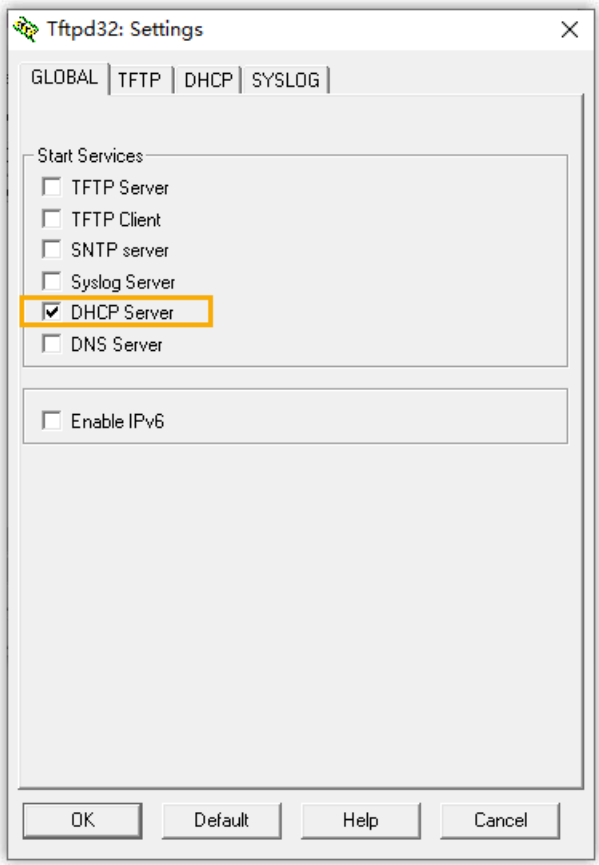
Step3. Set up a DHCP option 66

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

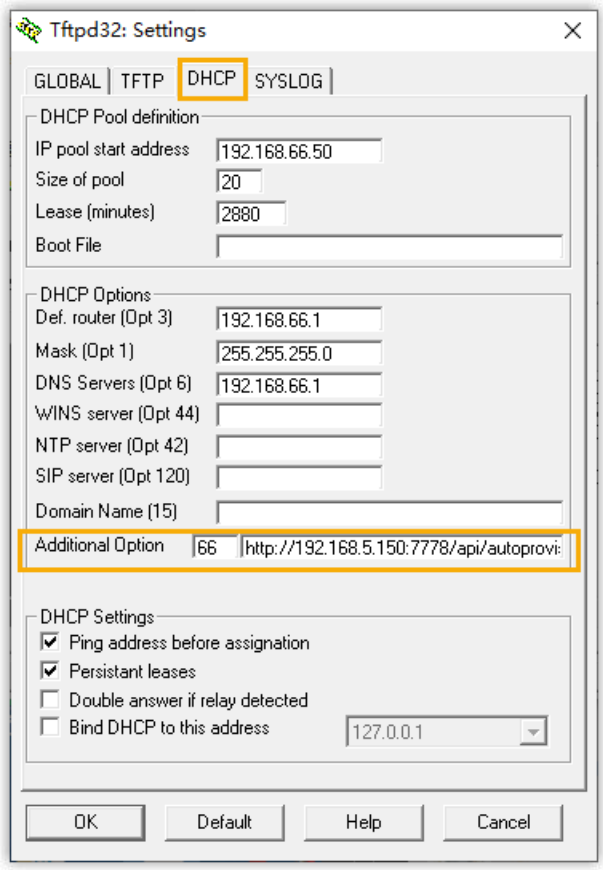
1. Run the Tftpd32 software, click **Settings** at the bottom of the window.



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



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



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

4. Click **OK**.

   The PC starts to work as a DHCP server.

Result

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

Auto Provision IP Phones Remotely (RPS FQDN Method)

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

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

Supported IP phones

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

Prerequisites

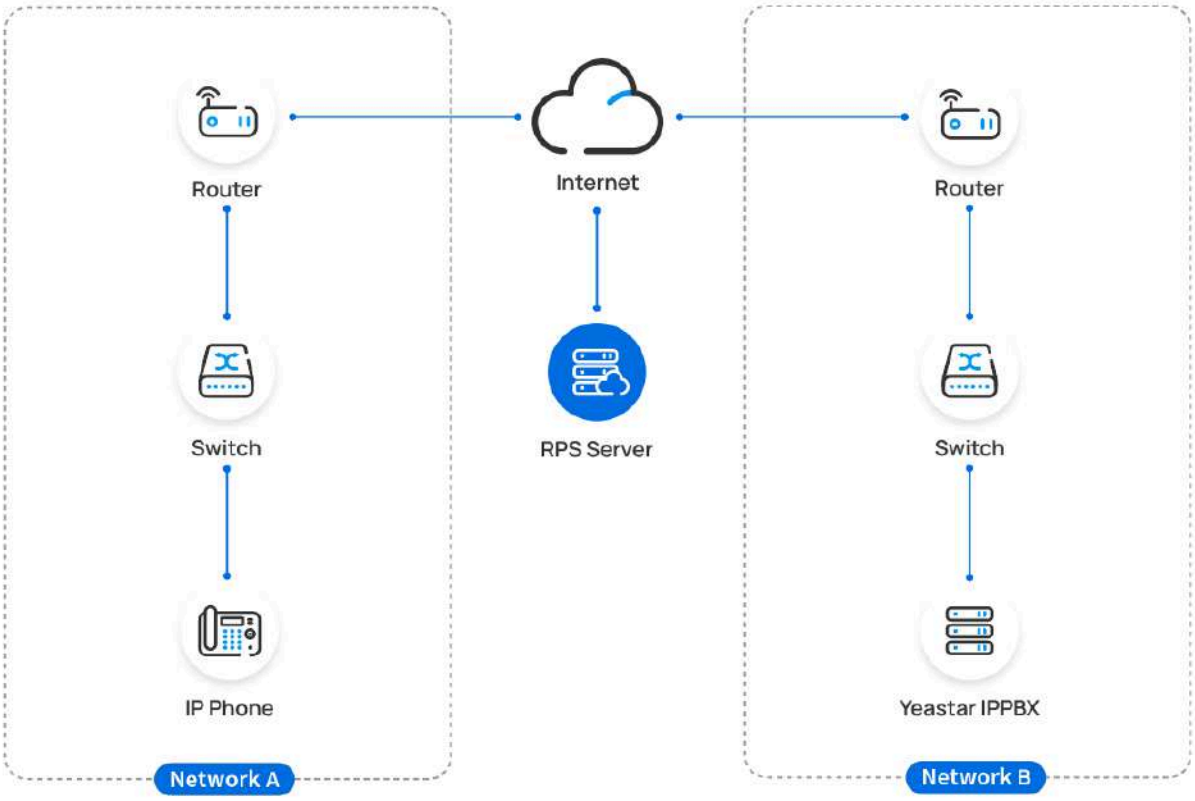
- Make sure the following required FQDN settings are ready.
  - The Yeastar FQDN domain name is available.

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

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

Scenario

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



Procedure

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

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

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

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

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

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

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

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

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

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

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

> **Tip:**

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

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

7. Click **Save**.

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

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

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

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

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

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

Result

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

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

Auto Provision IP Phones Remotely (RPS Method)

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

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

Supported IP phones

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

Prerequisites

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

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

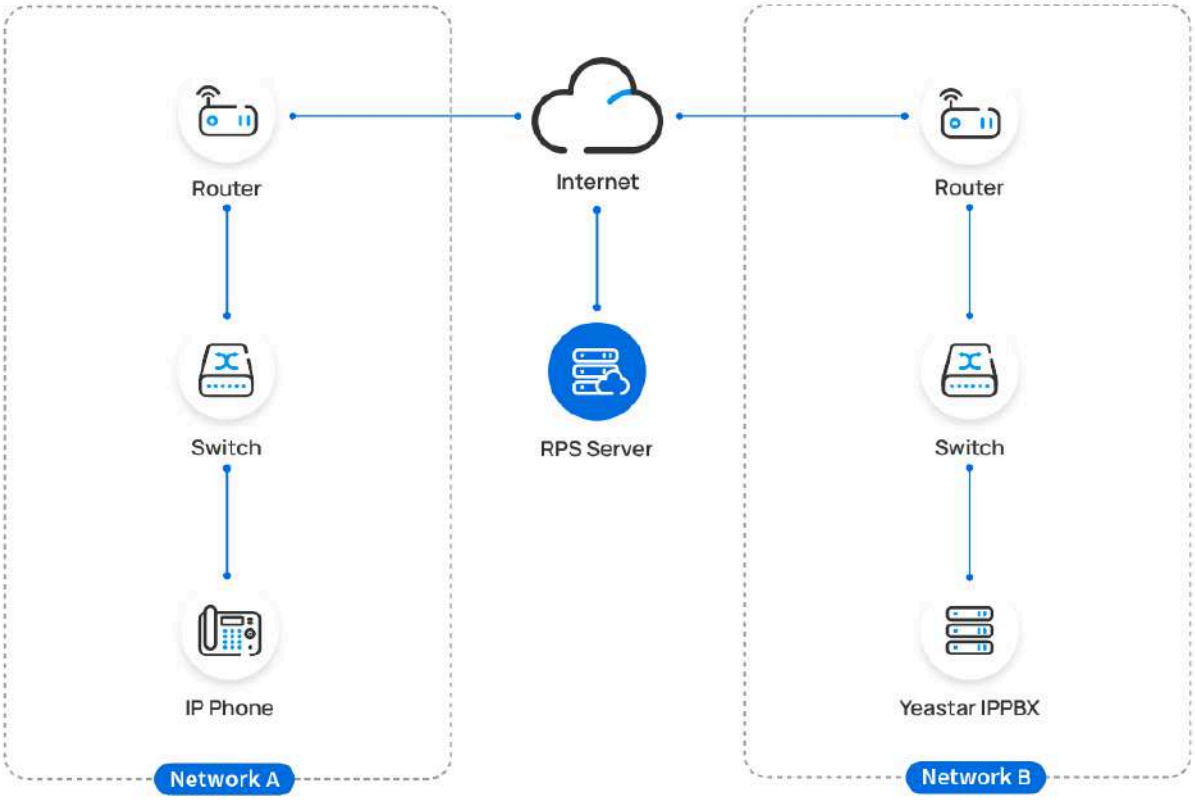
Important:
The following PBX ports must be forwarded.
- RTP ports
- SIP port
- Web Server port

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

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

Scenario

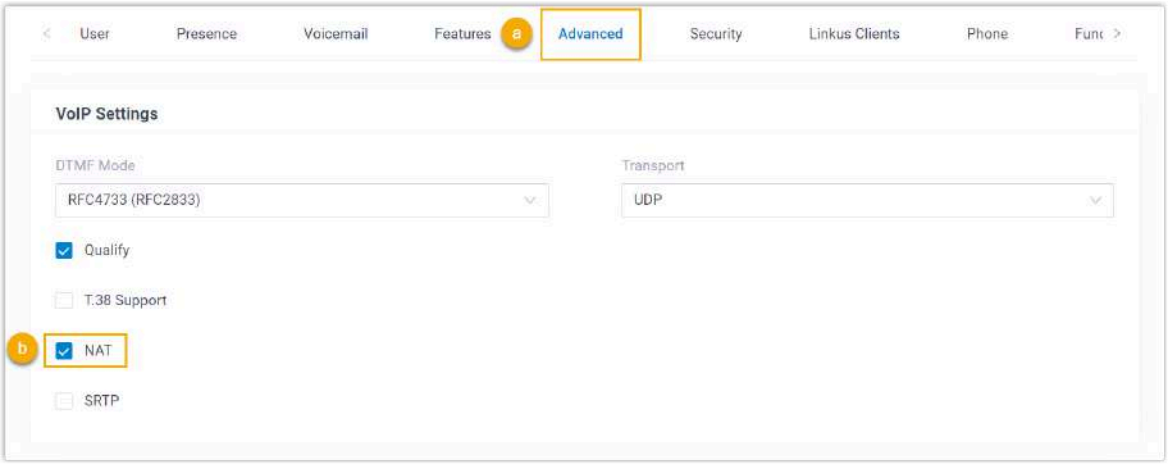
Yeastar P-Series Software Edition and IP phones are deployed in different networks. The PBX is behind a router and port forwarding is configured on the router.



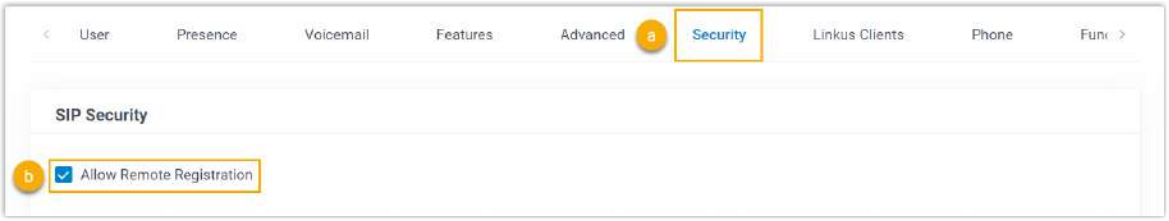
Procedure

Step 1. Set a remote extension

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



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



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

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

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

1. RESET the phone if it is previously used.
2. Log in to PBX web portal, go to **Auto Provisioning > Phones**.

3. Click **Add** to add an IP phone.
4. In the **IP Phone** section, configure phone information as follows:
    - **Vendor**: Select a phone vendor.
    - **Model**: Select a phone model.
    - **MAC Address**: Enter MAC address of the phone.
5. In the **Options** section, configure the following settings.
    - **Template**: Select a desired template from the drop-down list.

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

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

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

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

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

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

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

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

> • To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

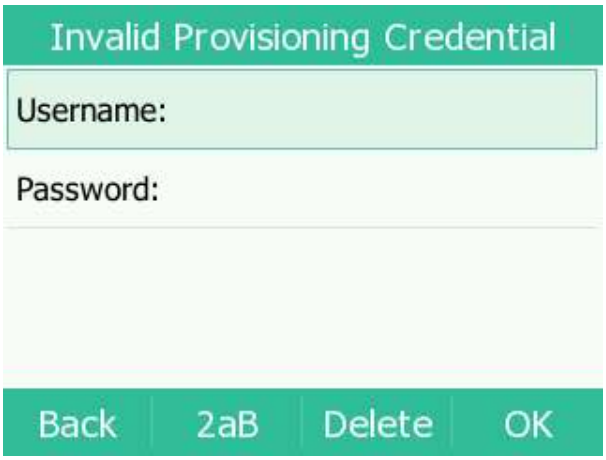
7. Click **Save**.

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

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

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

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



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

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

Result

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

- : The assigned extension is registered on the phone.

- : The assigned extension is unregistered on the phone.

Related information

Auto Provision IP Phones Remotely (RPS FQDN Method)

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

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

Supported IP phones

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

Prerequisites

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

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

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

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

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

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

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

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

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

7. Click **Save**.

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

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

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

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

Configure a DHCP server and set up option 66

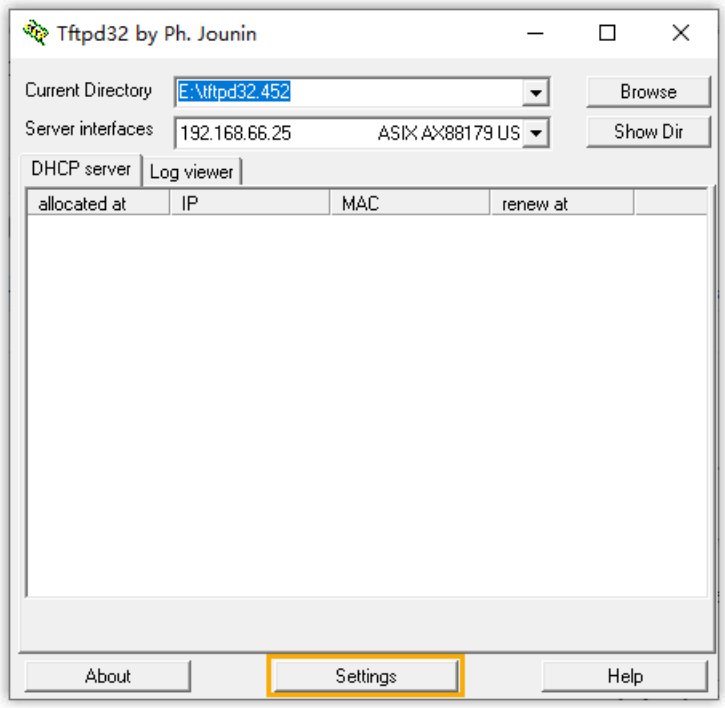
Configure a DHCP server and set up DHCP option 66 to the provisioning link. The IP phone will download configurations from PBX via the provisioning link, and apply the settings automatically.

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

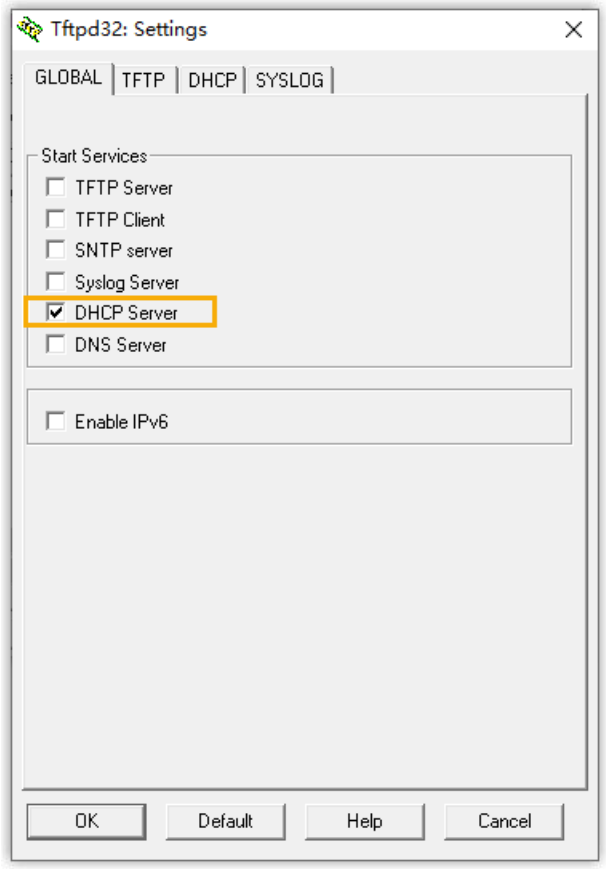
- If you use PBX as a DHCP server, the DHCP option 66 is set to the provisioning link automatically.
- If you use a third-party DHCP server, you need to set DHCP option 66.

  Here takes Tftpd32 DHCP server as an example.

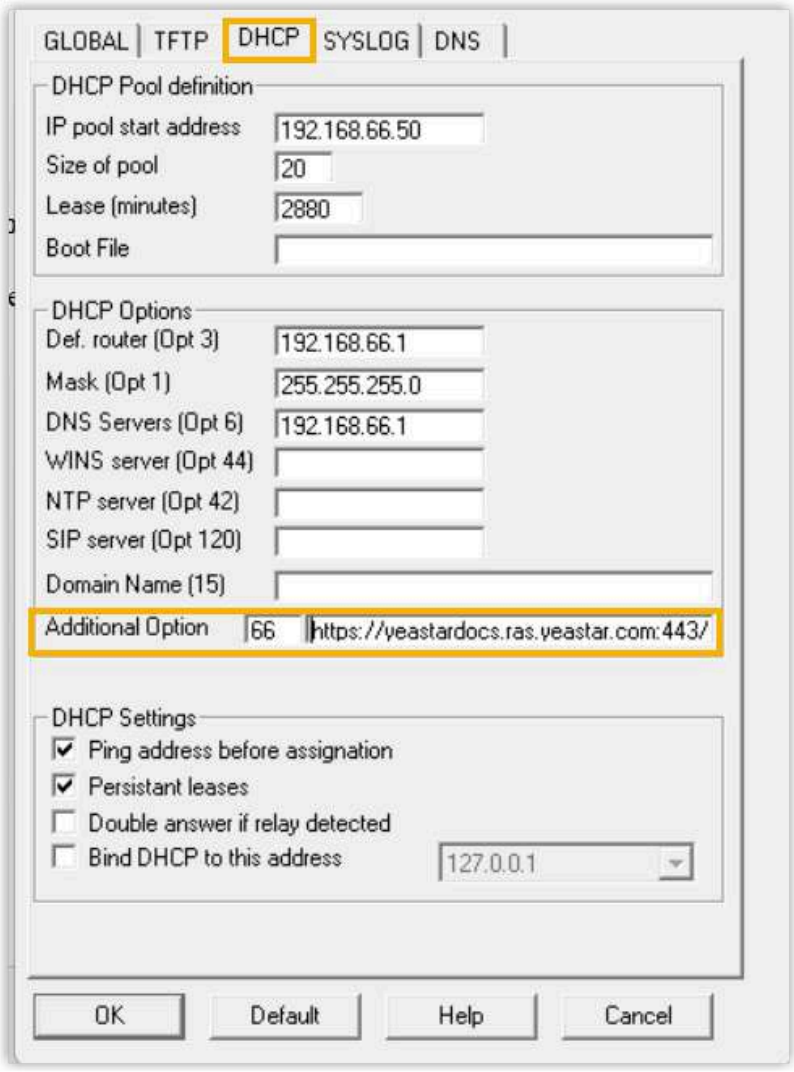
  1. Run the Tftpd32 software, click **Settings** at the bottom of the window.



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



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



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

4. Click **OK**.

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

Configure provisioning server address on the phone

Here takes the Yealink IP phone as an example.

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

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

Related information

Auto Provision IP Phones Remotely (Provision Link Method)

Auto Provision IP Phones Remotely (Provision Link Method)

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

Supported IP phones

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

Prerequisites

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

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

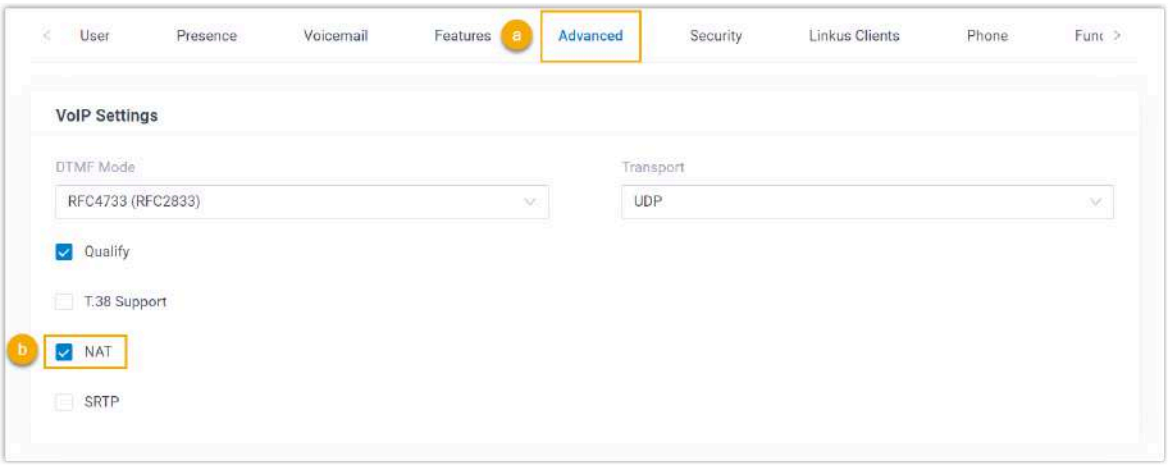
Important:
The following PBX ports must be forwarded.
- RTP ports
- SIP port
- Web Server port

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

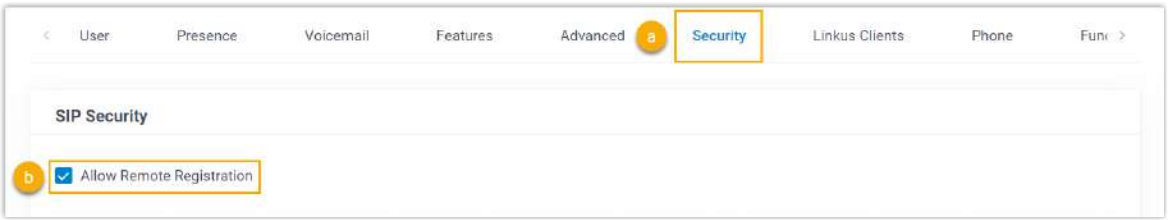
- Make sure that you have downloaded the template for the desired phone model (Path: **Auto Provisioning > Resource Repository > Default Templates**).
- Gather information of IP phone, including Vendor, Model, and MAC address.

Step 1. Set a remote extension

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



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



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

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

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

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

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

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

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

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

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

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

> • To associate an extension with multiple IP phones, see Allow Multiple Registrations for One Extension Number.

7. Click **Save**.

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

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

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

Configure a DHCP server and set up option 66

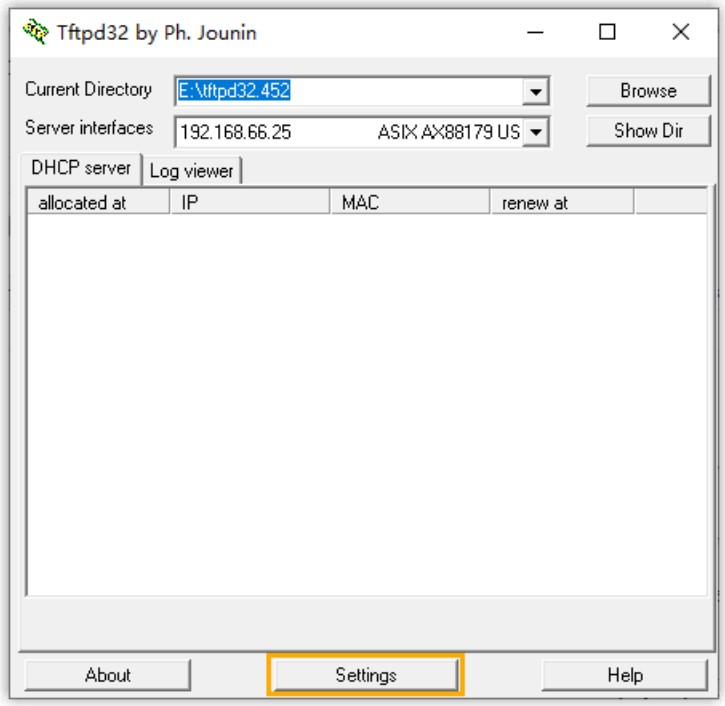
Configure a DHCP server and set up DHCP option 66 to the provisioning link. The IP phone will download configurations from PBX via the provisioning link, and apply the settings automatically.

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

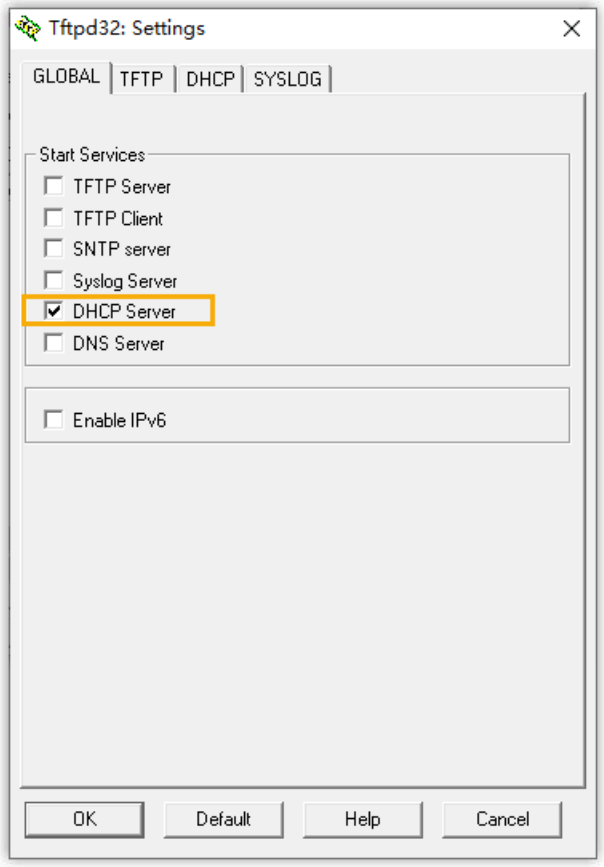
- If you use PBX as a DHCP server, the DHCP option 66 is set to the provisioning link automatically.
- If you use a third-party DHCP server, you need to set DHCP option 66.

  Here takes Tftpd32 DHCP server as an example.

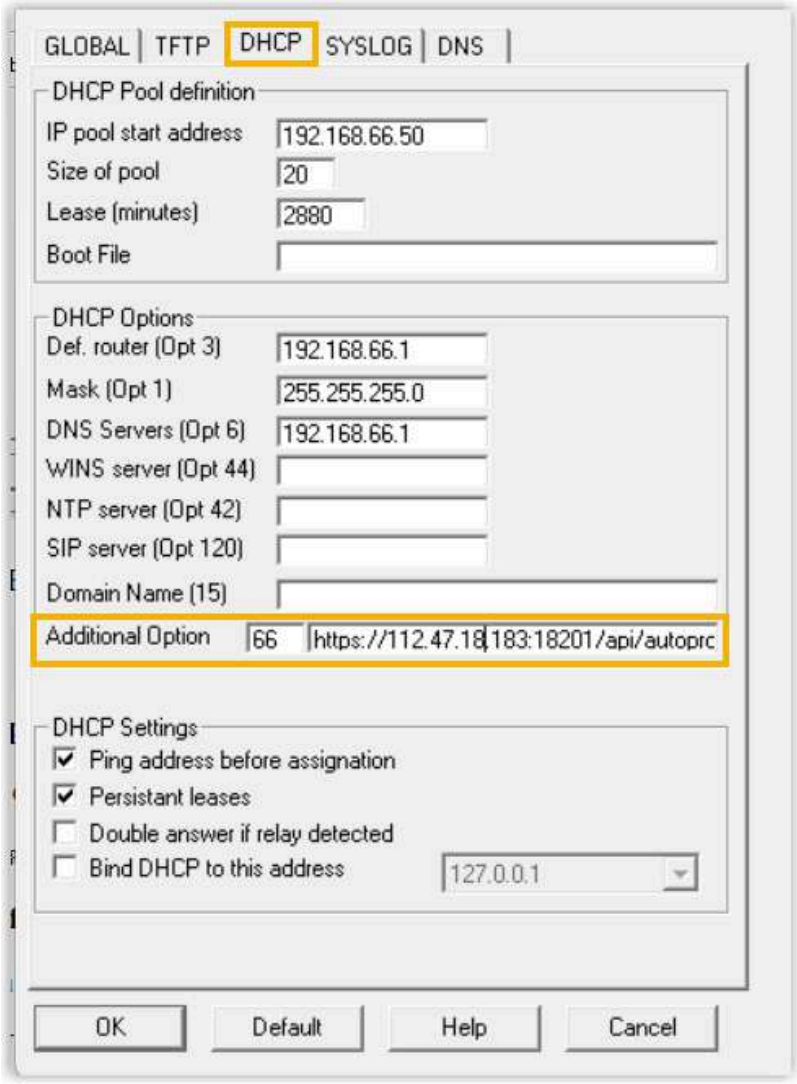
  1. Run the Tftpd32 software, click **Settings** at the bottom of the window.



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



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



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

4. Click **OK**.

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

Configure provisioning server address on the phone

Here takes the Yealink IP phone as an example.

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

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

Related information

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

Manually Provision an IP Phone

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

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

Supported IP phones

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

Prerequisites

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

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

Procedure

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

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

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

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

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

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

> **Tip:**

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

6. Click **Save**.

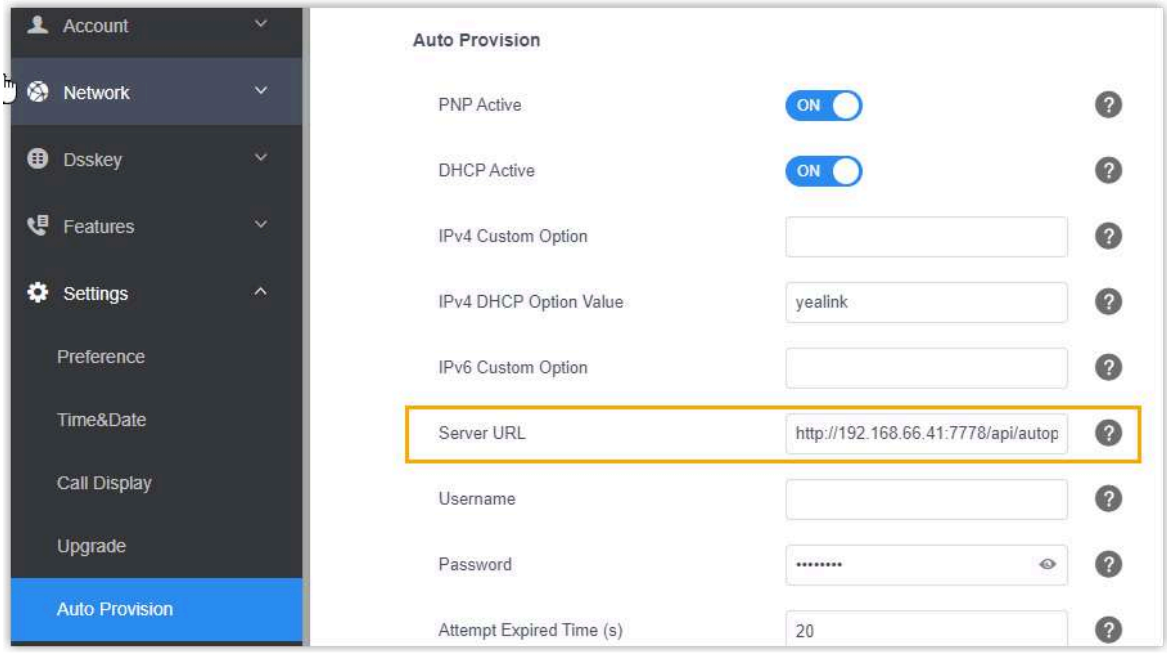
   A configuration file for the phone is generated in the PBX.

Step 2. Configure provisioning server address on the phone

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

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

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



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

Result

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

Provision Gateways

Auto Provision Yeastar TA FXS Gateways (PnP Method)

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

c. In the **Preference** section, configure the settings as needed.

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

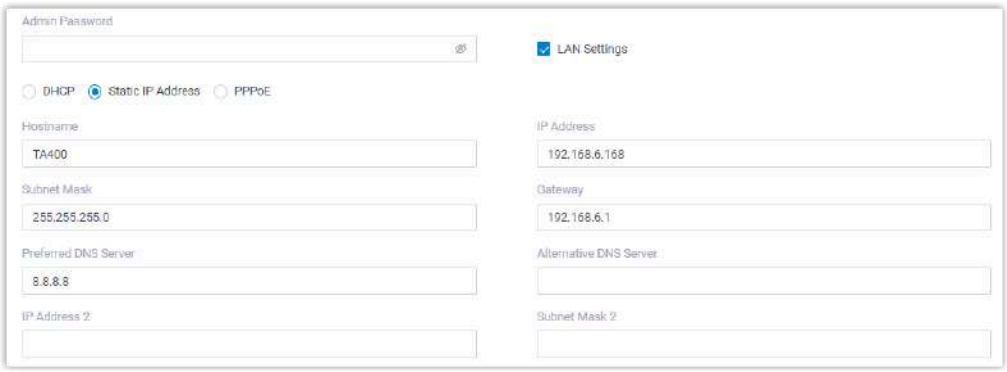
> **Note:**
> SIP VoIPServer IDX is not applicable for TA100 and TA200.

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

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

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

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



d. In the **Codecs** section, select your preferred codec list for the gateway.

5. Click **Save**.

   The PBX prompts you whether to reboot the gateway.

6. Click **OK** to reboot the gateway to apply the configurations.

Result

- The configurations will be automatically applied to the gateways after reboot:
  - The specified extensions will be registered on the corresponding ports of TA gateway.
- The extension registration status of provisioned phones is displayed on **Extension and Trunk > Extension**.
  - : The assigned extension is registered on the gateway.
  - : The assigned extension is unregistered on the gateway.

Related information

Modify a Provisioned Gateway Settings

Auto Provision Yeastar TA FXS Gateways (DHCP Method)

For the Yeastar TA FXS gateways that are located in different LAN subnet as the PBX, you can provision the gateways by DHCP method.

Supported gateway models

- TA100, TA200
- TA400, TA800
- TA1600, TA2400, TA3200

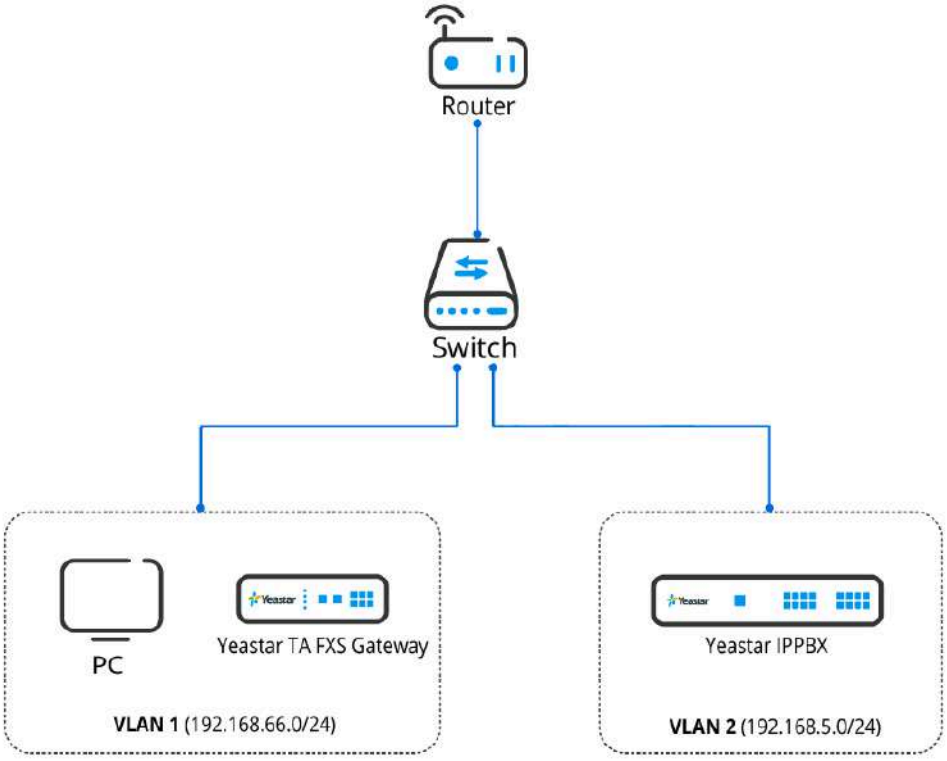
Prerequisites

- Make sure there is only one DHCP server, otherwise the gateway may fail to obtain an IP address.
- Gather information of Yeastar TA FXS gateway, including Model, and MAC address.

Scenario

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

- **Gateway**: Located in VLAN 1 (192.168.66.0/24)
- **PBX**: Located in VLAN 2 (192.168.5.0/24)



Procedure

Step1. Set a remote extension

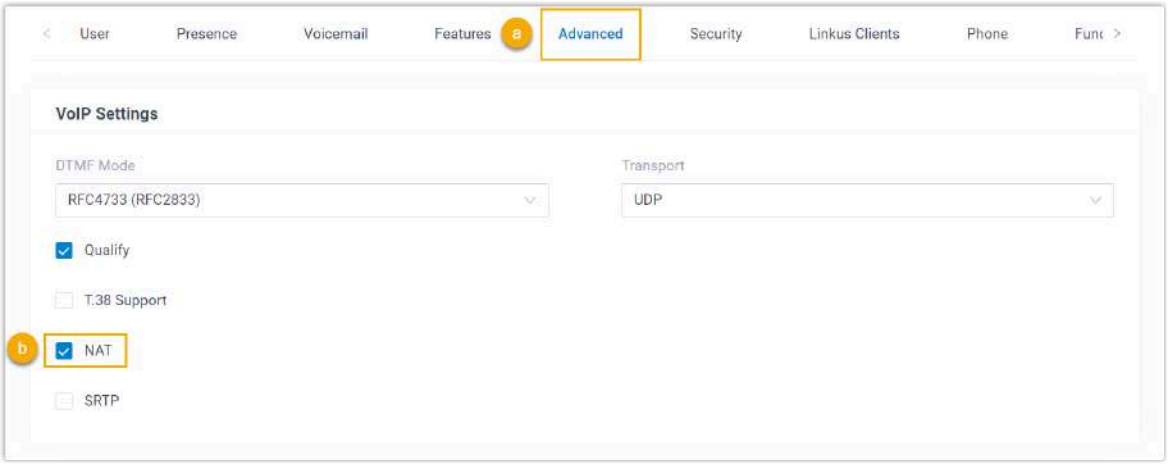
Step2. Add gateway's MAC address on the PBX

Step3. Set up a DHCP option 66

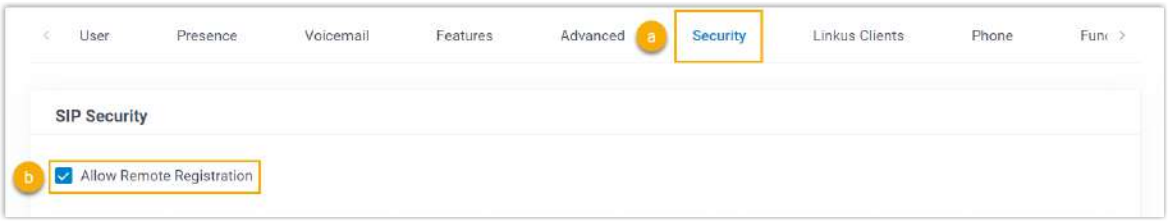
Step4. Enable DHCP provisioning on the gateway

Step1. Set a remote extension

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



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



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

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

Step2. Add gateway's MAC address on the PBX

1. RESET the TA gateway if it is previously used.
2. Log in to PBX web portal, go to **Auto Provisioning > Gateways**.
3. Click **Add** to add a gateway to the PBX.
4. In the **Gateway** section, configure gateway information as follows:
    - **Model**: Select a gateway model.
    - **MAC Address**: Enter MAC address of the gateway

5. In the **Options** section, configure the Auto Provisioning settings.
   - **Template**: Select a desired template from the drop-down list.

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

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

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

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

6. In the **Assign Extension** section, assign an extension for each port on gateway.
   a. In the **Port Range** field, select the port range to assign extensions.
   b. In the **Start Extension** and **End Extension** field, select the extension range to assign to the specified ports.
   c. Click **Assign Extension**.

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

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

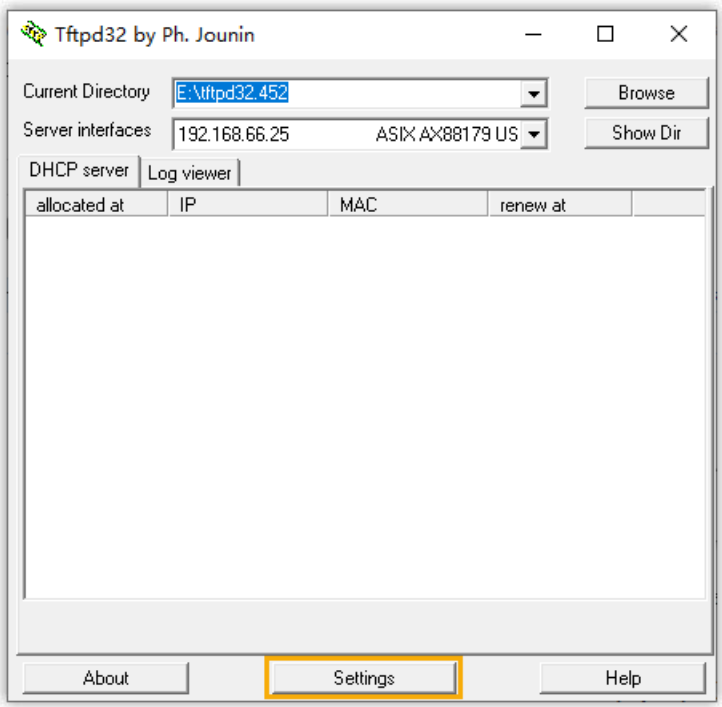
7. Click **Save**.

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

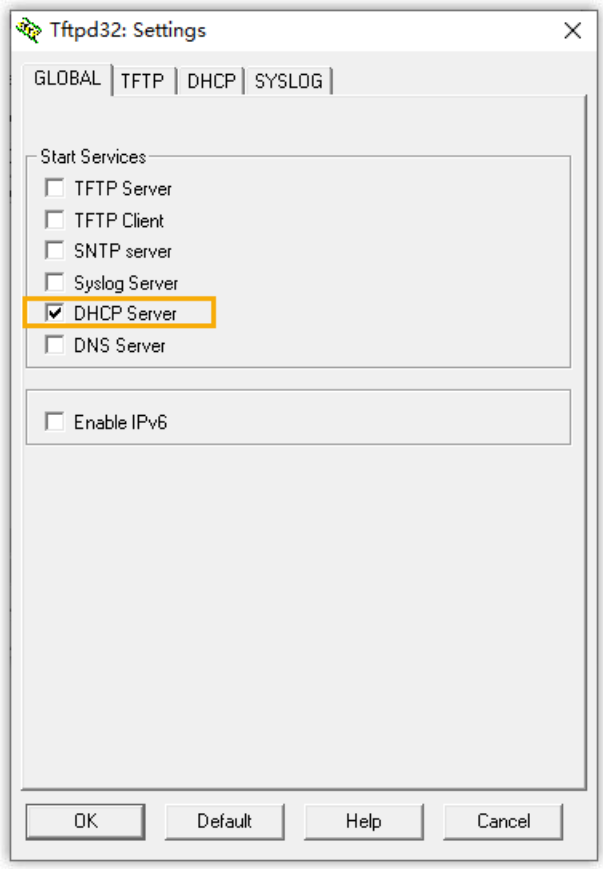
Step3. Set up a DHCP option 66

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

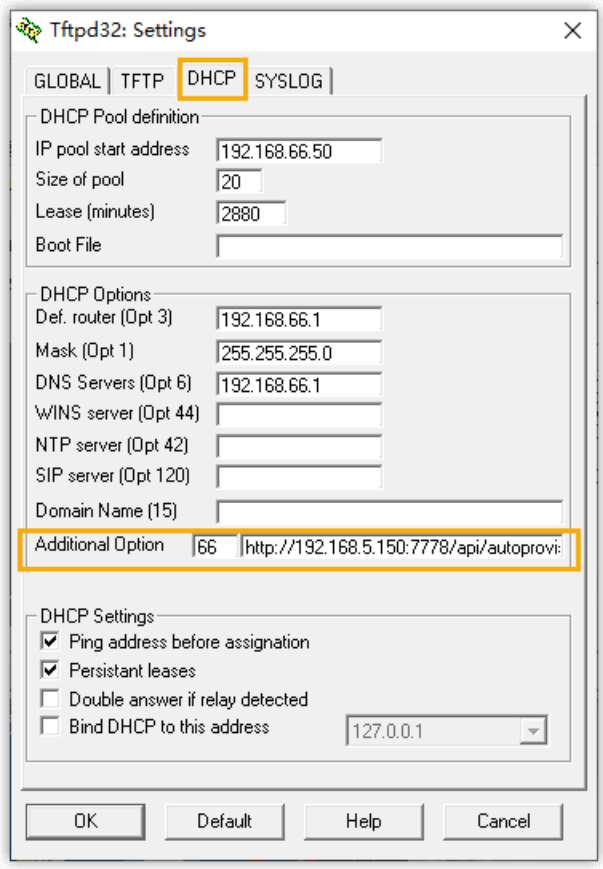
1. Run the Tftpd32 software, click **Settings** at the bottom of the window.



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



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



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

4. Click **OK**.

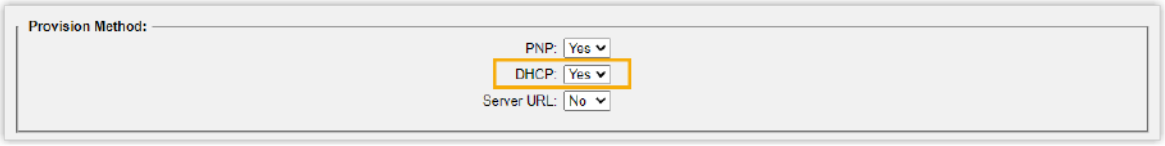
   The PC starts to work as a DHCP server.

Step4. Enable DHCP provisioning on the gateway

1. Reboot the gateway and get the IP address of the TA FXS gateway.

Connect an analog phone to any FXS port of the TA gateway, dial *** and follow the voice prompt to check the IP address.

2. Log in to the gateway web page by the IP address.
3. Go to **System > System Preferences > Auto Provision Settings**.
4. In the **Provision Method** section, enable the **DHCP** provisioning method.



5. Click **Save**, and then click **Apply Changes** appeared in the top-right corner.

Result

The extension registration status of provisioned analog phones is displayed on **Extension and Trunk > Extension**.

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

Auto Provision Yeastar TA FXS Gateway (Provision Link Method)

For Yeastar TA FXS gateways located in remote network, Yeastar P-Series Software Edition supports remote provisioning using the Provision Link method through public IP address/domain name and port. By generating a provisioning link on the PBX and entering it on the gateway, remote provisioning can be completed effortlessly.

Supported gateway models

- TA100, TA200
- TA400, TA800
- TA1600, TA2400, TA3200

Prerequisites

- Set up PBX to make it ready for the remote provisioning.
  - Upgrade PBX firmware to version 83.18.0.18 or later.
  - Configure port forwarding on router and SIP NAT on PBX for remote access.

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

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

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

- Configure transport protocol for Web server to HTTPS.

  For more information, see Change Web Server Protocol and Port.
- Download the latest template for Yeastar TA FXS gateway.

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

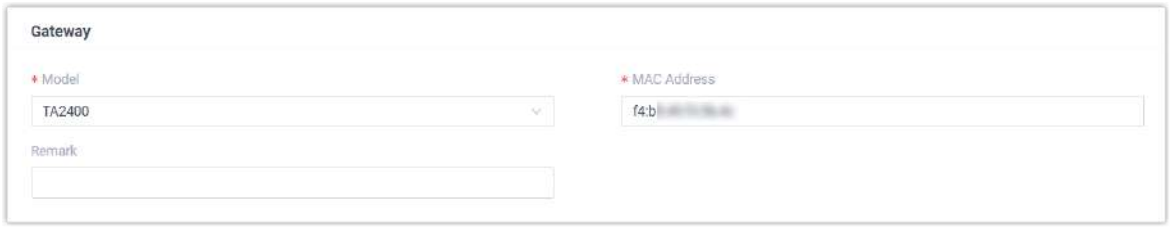
- Set up extension(s) to make them ready for the remote registration.

- Gather MAC address of TA FXS gateway.

Step 1. Generate configuration file for a gateway on the PBX

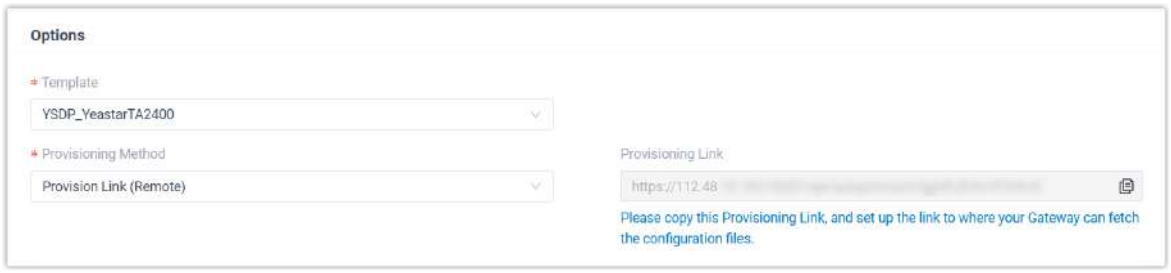
1. Log in to PBX web portal, go to **Auto Provisioning > Gateways**.
2. Click **Add** to add a gateway.

3. In the **Gateway** section, configure gateway information as follows:



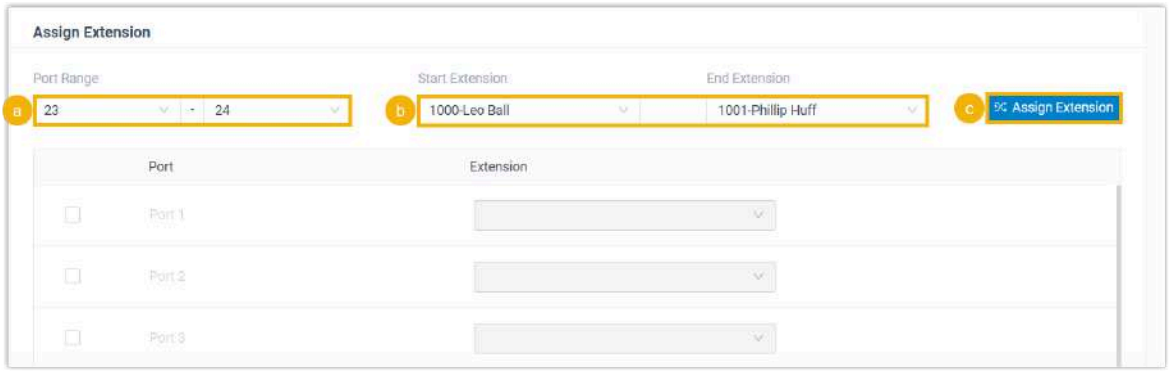
   - **Model**: Select a gateway model.
   - **MAC Address**: Enter MAC address of the gateway.
   - **Remark**: Optional. Add a short description about the gateway.

4. In the **Options** section, configure the following settings to generate a configuration file for the gateway.



   - **Template**: Select the corresponding template from the drop-down list.
   - **Provisioning Method**: Select **Provision Link (Remote)**.
   - **Provisioning Link**: Click to copy the provisioning link, as you will use it later.

5. In the **Assign Extension** section, assign extension(s) to the gateway port(s).

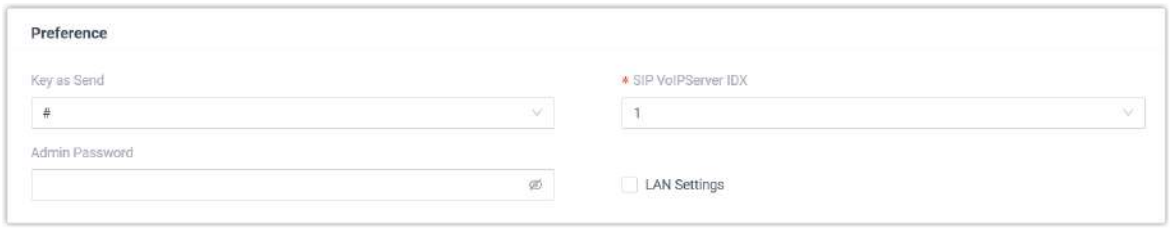


   a. In the **Port Range** field, select the port range to assign extension(s).
   b. In the **Start Extension** and **End Extension** field, select the extension range to assign the extensions to the specified ports.
   c. Click **Assign Extension**.

The ports with assigned extensions are displayed below.

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

6. **Optional:** In the **Preference** section, configure the settings as needed.

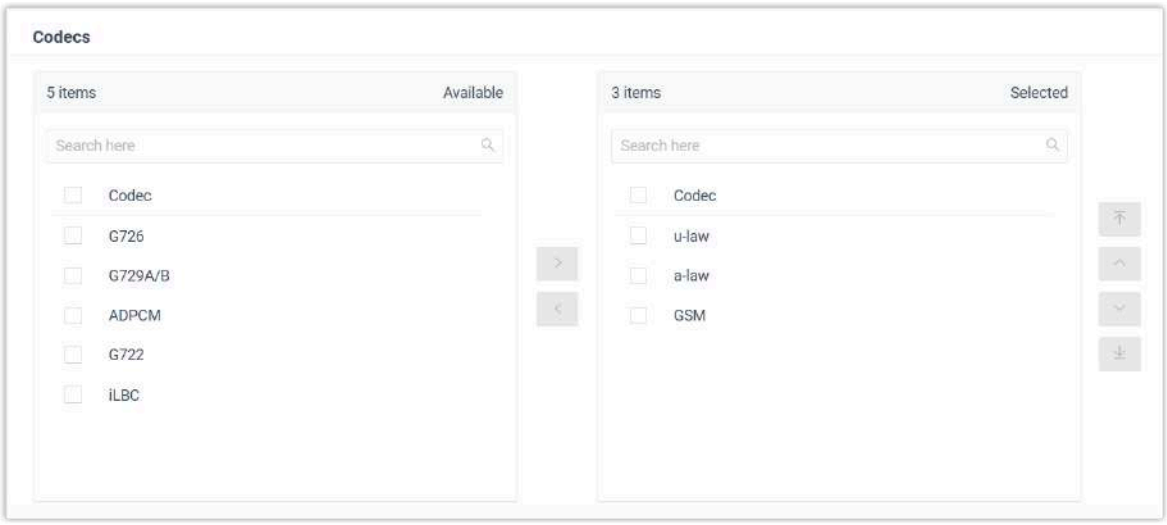


- **Key as Send**: Assign the pound key (“#”) or asterisk key (“*”) as the send key.
- **SIP VoIPServer IDX**: Select a VoIP server template ID to be provisioned.

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

- **Admin Password**: Set the password for logging in to the gateway web interface.
- **LAN Settings**: Keep it as default.

7. **Optional:** In the **Codecs** section, select your preferred codec list for the gateway.

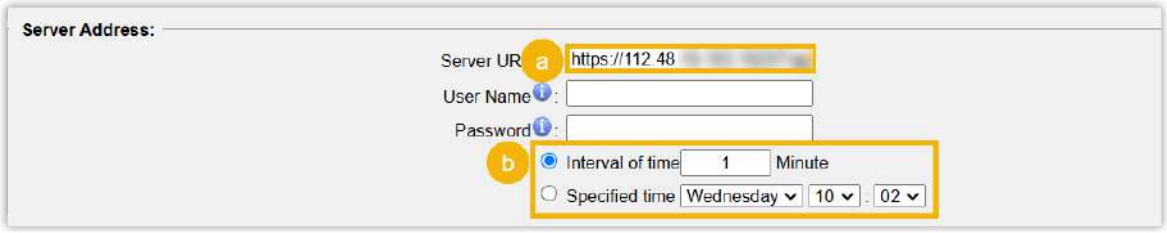


8. Click **Save**.

Step 2. Make the configuration file accessible to the gateway

1. Log in to the gateway web interface, go to **System > System Preferences > Auto Provision Settings**.
2. In the **Provision Method** section, set **Server URL** to **Yes**.

3. In the **Server Address** section, complete the following settings:



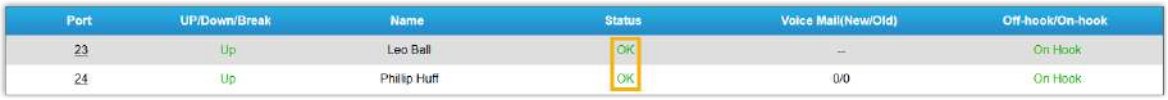
   a. In the **Server URL** field, paste the provisioning link that you have obtained from PBX.
   b. Set the time to perform auto provisioning.
4. Click **Save** and **Apply Changes**.

Result

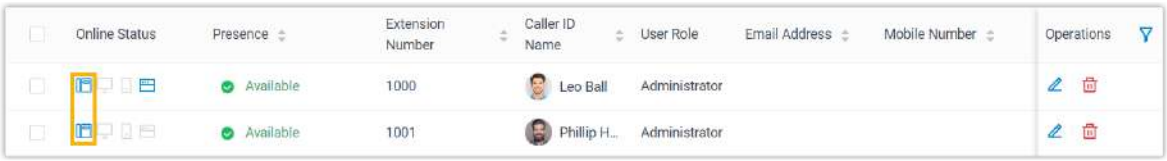
After the specified time, the configurations are applied to the gateway, and the specified extension(s) are registered on the corresponding port(s) of TA FXS gateway.

You can check extension registration status in the following ways:

- On gateway web interface, the port status is displayed as **OK** (Path: **Status > System Status > FXS Port Status**).



- On PBX web portal, the extension status is displayed as  (Path: **Extension and Trunk > Extension > Online Status**).



Auto Provision Yeastar TA FXS Gateway (Provision Link FQDN Method)

For Yeastar TA FXS gateways located in remote network, Yeastar P-Series Software Edition supports remote provisioning using the Provision Link FQDN method through Yeastar-supplied Fully Qualified Domain Name (FQDN). By generating a provisioning link on the PBX and entering it on the gateway, remote provisioning can be completed effortlessly.

Supported gateway models

- TA100, TA200
- TA400, TA800
- TA1600, TA2400, TA3200

Prerequisites

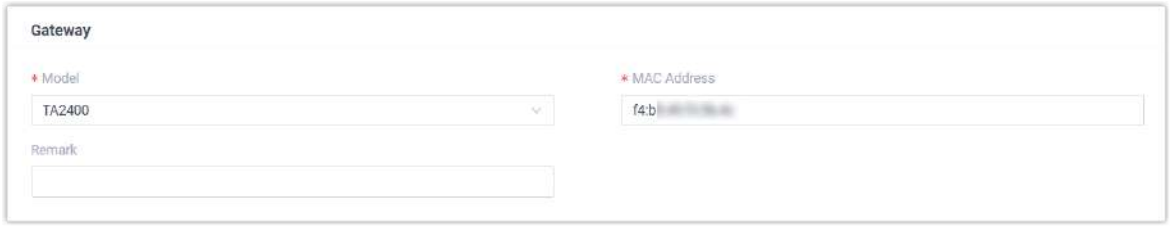
- Set up PBX to make it ready for the remote provisioning.
  - Upgrade PBX firmware to version 83.18.0.18 or later.
  - Configure Yeastar FQDN on PBX, and enable Web access and SIP access for the extension(s) to be assigned to gateway.

For more information, see Configure Network for Remote Web Access by a Yeastar FQDN and Configure Network for Remote SIP Access by a Yeastar FQDN.

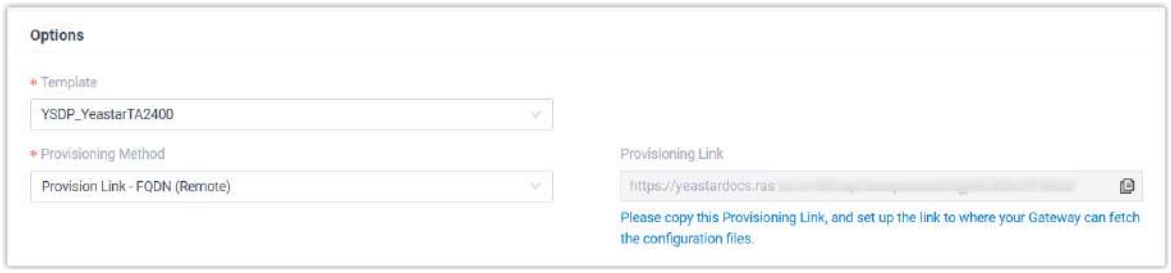
- Gather MAC address of TA FXS gateway.

Step 1. Generate configuration file for a gateway on the PBX

1. Log in to PBX web portal, go to **Auto Provisioning > Gateways**.
2. Click **Add** to add a gateway.
3. In the **Gateway** section, configure gateway information as follows:



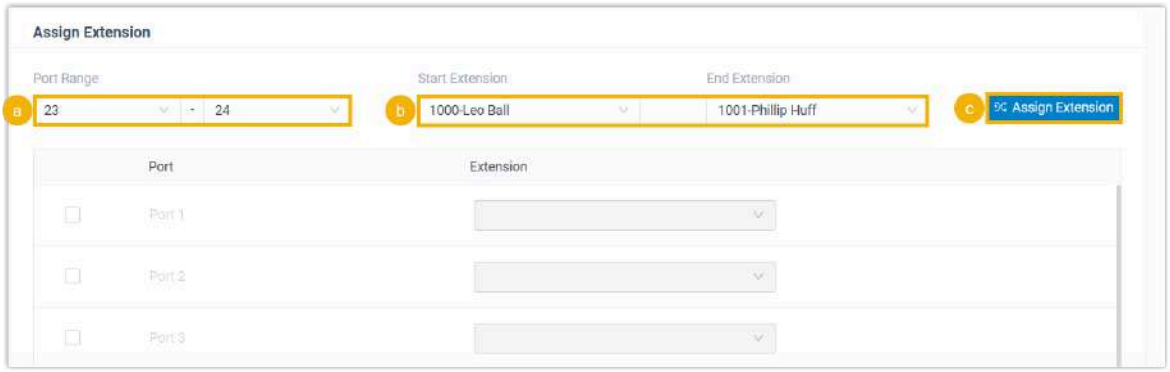
   - **Model**: Select a gateway model.
   - **MAC Address**: Enter MAC address of the gateway.
   - **Remark**: Optional. Add a short description about the gateway.
4. In the **Options** section, configure the following settings to generate a configuration file for the gateway.



   - **Template**: Select the corresponding template from the drop-down list.
   - **Provisioning Method**: Select **Provision Link - FQDN (Remote)**.

- **Provisioning Link**: Click to copy the provisioning link, as you will use it later.

5. In the **Assign Extension** section, assign extension(s) to the gateway port(s).

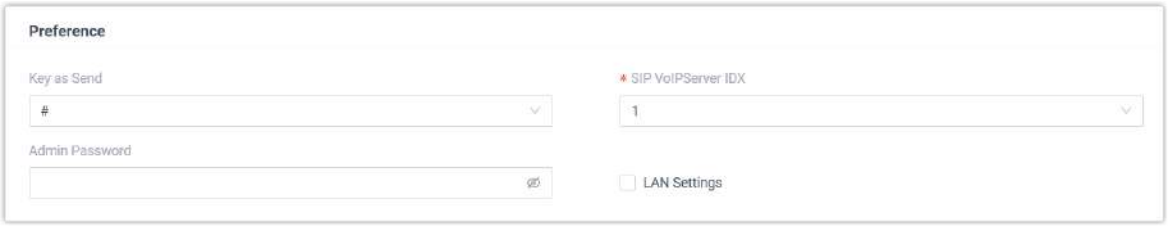


   a. In the **Port Range** field, select the port range to assign extension(s).
   b. In the **Start Extension** and **End Extension** field, select the extension range to assign the extensions to the specified ports.
   c. Click **Assign Extension**.

   The ports with assigned extensions are displayed below.

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

6. **Optional:** In the **Preference** section, configure the settings as needed.

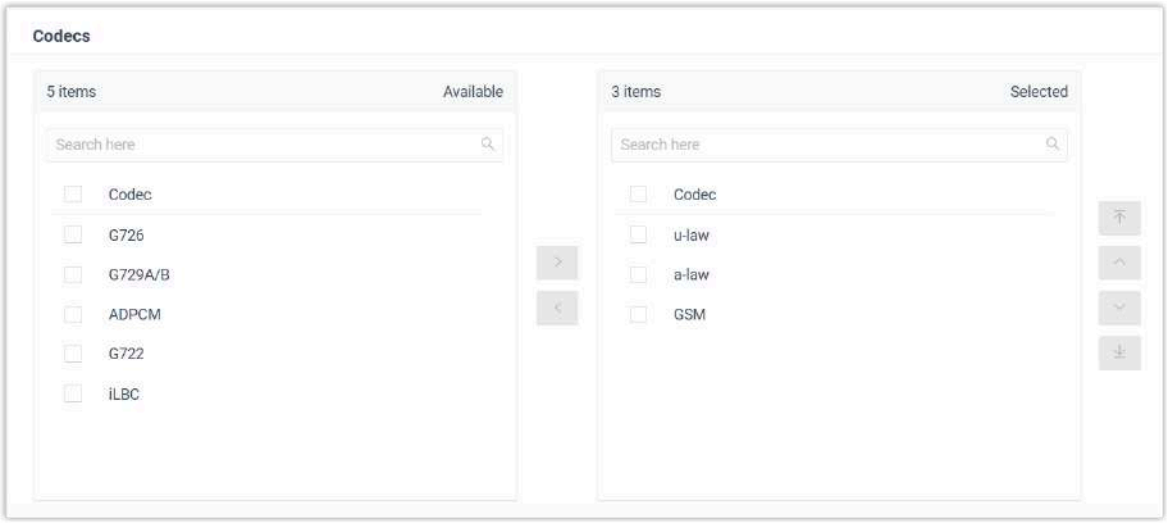


- **Key as Send**: Assign the pound key (“#”) or asterisk key (“*”) as the send key.
- **SIP VoIPServer IDX**: Select a VoIP server template ID to be provisioned.

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

- **Admin Password**: Set the password for logging in to the gateway web interface.
- **LAN Settings**: Keep it as default.

7. **Optional:** In the **Codecs** section, select your preferred codec list for the gateway.

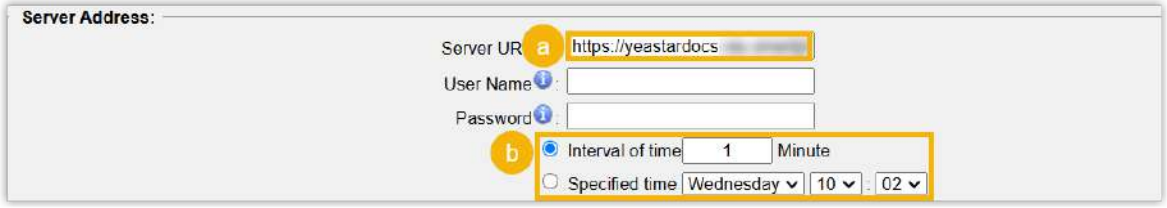


8. Click **Save**.

Step 2. Make the configuration file accessible to the gateway

1. Log in to the gateway web interface, go to **System > System Preferences > Auto Provision Settings**.
2. In the **Provision Method** section, set **Server URL** to **Yes**.

3. In the **Server Address** section, complete the following settings:



a. In the **Server URL** field, paste the provisioning link that you have obtained from PBX.
b. Set the time to perform auto provisioning.

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

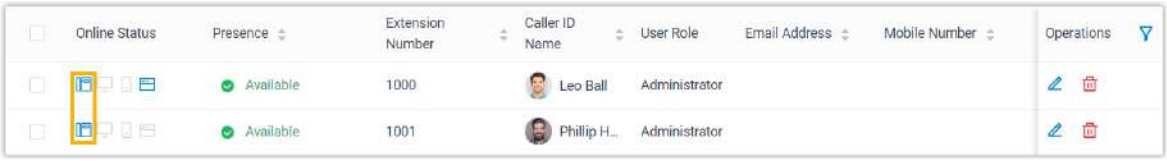
Result

After the specified time, the configurations are applied to the gateway, and the specified extension(s) are registered on the corresponding port(s) of TA FXS gateway.

You can check extension registration status in the following ways:

- On gateway web interface, the port status is displayed as **OK** (Path: **Status > System Status > FXS Port Status**).

- On PBX web portal, the extension status is displayed as (Path: **Extension and Trunk > Extension > Online Status**).



Manage Provisioned Devices

Remotely Access a Provisioned IP Phone / Gateway

Yeastar P-Series 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.

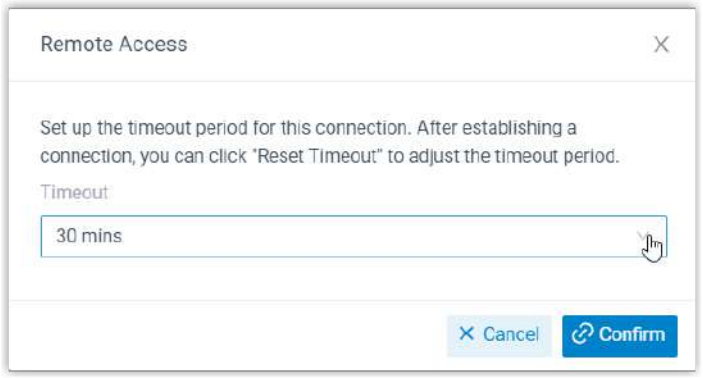
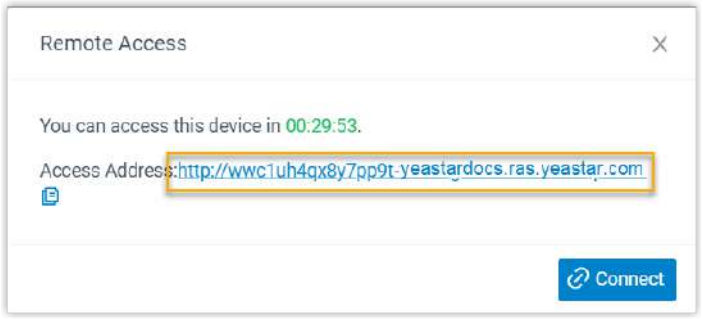
> **Tip:**
> To make sure of this, check if the private IP address of the IP phone / gateway is recognized and displayed in the **Auto Provisioning** device list.
>
> 
>

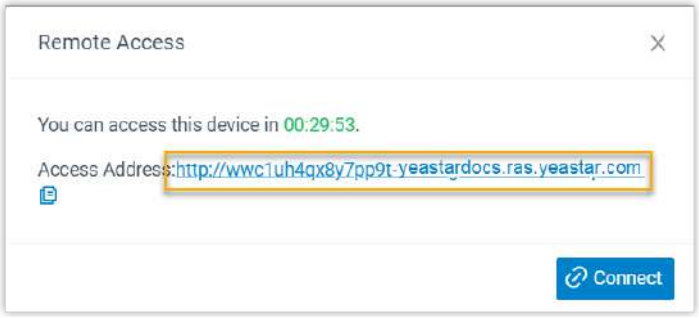
Remotely visit an IP phone on PBX

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

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

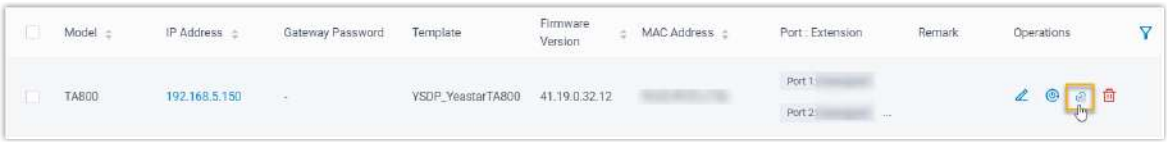
Table 7.

Method	Instruction
FQDN domain name	a. Set a connection timeout period. i. In the **Timeout** drop-down list of the pop-up window, set the timeout period.  ii. Click **Confirm**. The pop-up window displays a temporary remote access link and the connection time countdown; And the remote access icon turns to , indicating that the IP phone is connected.  b. Click **Connect** to visit the IP phone web interface.
Random PBX remote management link	The pop-up window directly displays a temporary link as well as the connection time countdown; And the remote access icon turns to , indicating that the IP phone is connected. **Note:** In this case, the time limit of IP phone remote access is synchronized with the remote management timeout of the PBX.

Method	Instruction
	 Click **Connect** to visit the IP phone web interface.

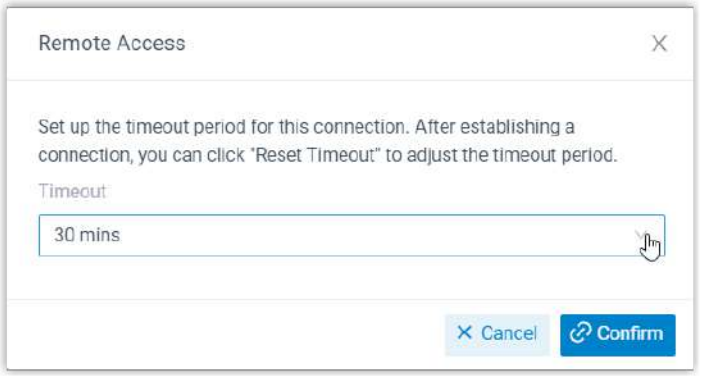
Remotely visit a gateway on PBX

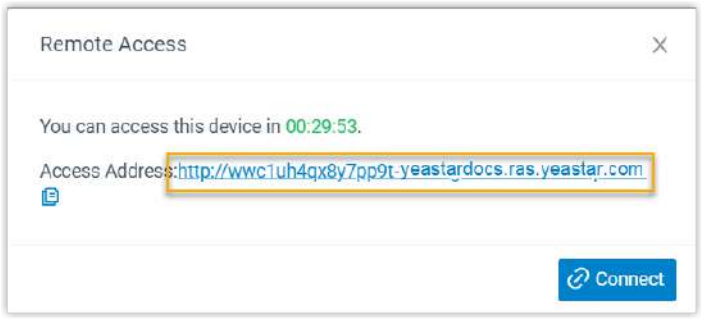
1. Log in to PBX web portal, go to **Auto Provisioning > Gateways**.
2. Click beside the desired gateway.

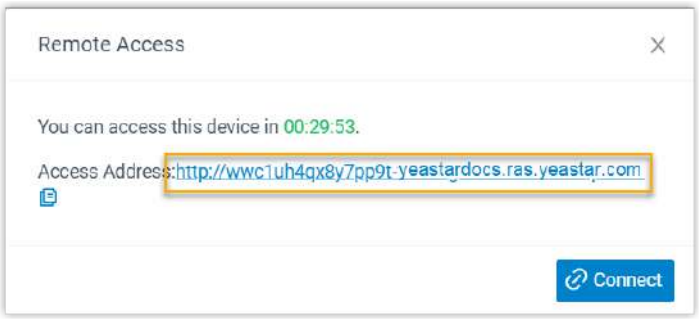


3. Connect to the gateway as the following instructions guide according to the method users visit the PBX.

Table 8.

Method	Instruction
FQDN domain name	a. Set a connection timeout period. i. In the **Timeout** drop-down list of the pop-up window, set the timeout period.  ii. Click **Confirm**.

<table>
<tr><th>Method</th><th>Instruction</th></tr>
<tr><td></td><td>The pop-up window displays a temporary remote access link and the connection time countdown; And the remote access icon turns to , indicating that the gateway is connected.
 

b. Click Connect to visit the gateway web interface.</td></tr>
<tr><td>Random PBX remote management link</td><td>The pop-up window directly displays a temporary link as well as the connection time countdown; And the remote access icon turns to , indicating that the gateway is connected.
Note:
In this case, the time limit of gateway remote access is synchronized with the remote management timeout of the PBX.
 

Click Connect to visit the gateway web interface.</td></tr>
</table>

FAQ

How to extend the IP phone / Gateway remote access time

After the connection is established, users can re-configure the timeout period to extend the connection time.

Note:

- Only when users access the PBX via the FQDN domain name can they reset the time limit of IP phone / gateway remote access on the PBX.
- If users access the PBX via a random visit link for PBX remote management, please contact the device provider to extend the remote access time.

1. On PBX web portal, go to **Remote Access** setting of the connected device.

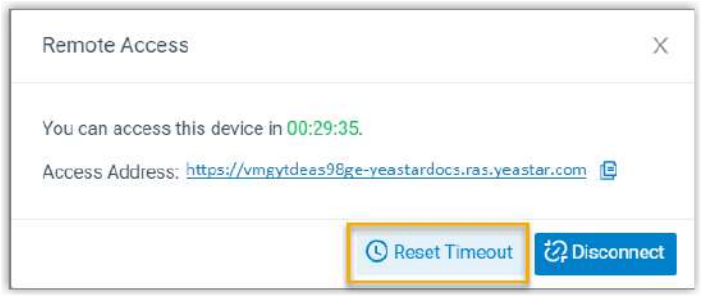
   IP Phone

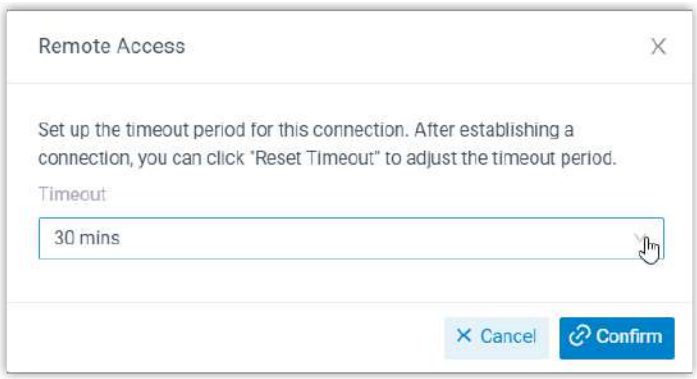
   Gateway

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

3. Reset the **Timeout** and click **Confirm**



The pop-up window displays the new countdown of connection time.

Reboot Provisioned IP Phones/Gateways

For some settings that need a device reboot to take effect, you can reboot the device remotely on PBX web portal if these devices have been auto provisioned on PBX.

Reboot provisioned IP phones

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

   The system prompts you whether to reboot the phones.
3. Click **OK**.

Reboot provisioned gateways

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

   The system prompts you whether to reboot the gateways.
3. Click **OK**.

Reassign an Extension to a Provisioned IP Phone/Gateway

If a phone is previously provisioned but the phone owner or gateway port has been changed, you can reassign an extension to the provisioned phone or gateway.

Reassign an extension to a provisioned IP Phone

Procedure

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

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

Result

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

Reassign an extension to a provisioned gateway

Procedure

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

   > **Tip:**

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

3. Click **Save**.

   The PBX generates a configuration file for gateway, and prompts you whether to reboot the gateway.
4. Click **OK** to reboot the gateway to apply the configurations.

Result

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

Release an Extension from a Provisioned IP Phone/Gateway

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

Release an extension from a provisioned phone

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

      The extension is released from the phone.
2. Reprovision the phone to de-register the extension.

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

Release an extension from a provisioned gateway

Procedure

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

    The extension is released from the gateway.
2. Reboot the gateway to apply the configurations.

Result

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

Remove IP Phones/Gateways from Provisioning List

The provisioning list always displays all the devices that are discovered. For the out-of-use devices, you can remove them from the phone/gateway provisioning list manually.

Remove phones from provisioning list

Procedure

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

Result

The system erases all configuration files for the phone and releases the assigned extension.

Remove gateways from provisioning list

Procedure

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

2. Remove gateways according to your needs:
   - To remove a gateway, click  beside the desired gateways.
   - To remove gateways in bulk, select the checkboxes of the desired gateways, and click **Delete**.
3. Click **OK**.

Result

The system erases all configuration files for the gateways and releases the assigned extension.

Export and Import Auto Provisioning Phone Information

The phones' information in the Auto Provisioning phone list can be exported and saved as a template. You can fill in the information of desired phones in the exported file, and import the file to PBX again, so as to add phones to the PBX in bulk conveniently. This topic describes how to export and import Auto Provisioning phone information.

Export Auto Provisioning phone information

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. At the top of the Auto Provisioning phone list, click **Export**.

   A CSV file is saved to your computer. To check and edit parameters in the CSV file, see Auto Provisioning Phone Information Parameters.

Import Auto Provisioning phone information

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

Prerequisites

Learn about the requirements of an imported file:

- **Format**: UTF-8.CSV
- **Size**: Less than 50 MB
- **File name**: Less than 127 characters
- **Import parameters**: Ensure that the import parameters meet requirements. For more information, see Auto Provisioning Phone Information Parameters.

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. At the top of the Auto Provisioning phone list, click **Import**.
3. In the pop-up window, click **Browse**, and select your CSV file.
4. Click **Import**.

   The phone information in the CSV file will be displayed in the Auto Provisioning phone list.

Related information

Import and Export -FAQ

Auto Provisioning Options

IP Phone Auto Provisioning Options

Yeastar P-Series 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)
- Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
- Auto Provision IP Phones Remotely (Provision Link Method)
- Reassign an Extension to a Provisioned IP Phone/Gateway

VLAN settings

Yeastar P-Series Software Edition allows you to configure VLAN settings for a provisioned phone (either for the WAN port or PC port), or set the phone to acquire VLAN ID through DHCP option.

For more information, see Configure VLAN for a Provisioned Phone.

Function key

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

For more information about the function keys, see Auto Provision Function Keys for Phones.

Device firmware

Yeastar P-Series 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.

Automatically Generate Random Passwords for Phones

Yeastar P-Series Software Edition supports to generate random and complex passwords for admin, user, and var accounts on auto provisioned phones, eliminating the need to manually change the default password for each phone. This topic describes how to enable this feature on PBX.

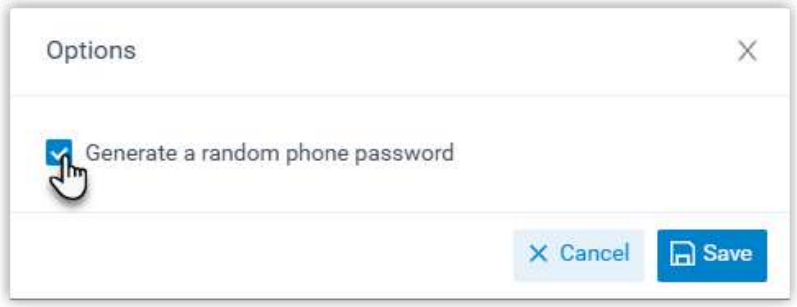
Requirements

The PBX firmware version is 83.18.0.102 or later.

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. At the top of the list, click **Options**.

3. In the pop-up window, select the checkbox of **Generate a random phone password**, then click **Save**.

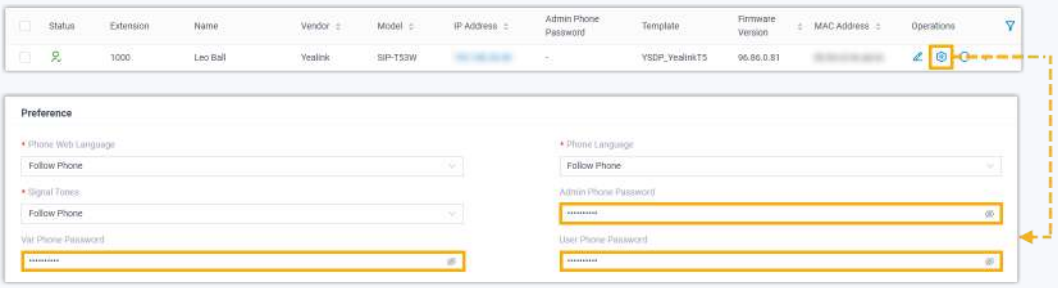


Result

When adding a phone, random phone password(s) are generated automatically.

Note:

- If you want to change the password, click , then edit the password in the corresponding fields.



- For DECT phones provisioned via PnP method, the default password will be used instead of a random one.

Configure VLAN for a Provisioned Phone

Yeastar P-Series Software Edition allows you to configure the VLAN settings for a provisioned phone, which helps to enhance the quality of VoIP calls. This topic describes how to configure the VLAN settings for a phone via Auto Provisioning.

Requirements

The PBX firmware version is 83.18.0.18 or later.

Prerequisites

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

For more information, see the following topics:

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

Procedure

- Step 1. Configure VLAN settings for the IP phone on PBX
- Step 2. Apply the configuration to IP phone

Step 1. Configure VLAN settings for the IP phone on PBX

> **Note:**
> The VLAN settings vary according to different phone models.

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**, then click to edit the desired phone.
2. Scroll down to the **VLAN** section, then complete the following settings as needed.
   - To configure VLAN for WAN port of the phone, do as follows:

     a. Select the checkbox of **WAN Port**.
     b. In the **VLAN ID** field, enter a VLAN ID.
     c. In the **Priority** drop-down list, select a priority value for the VLAN.

     The priority value is between `0` (lowest) to `7` (highest).
   - To configure VLAN for PC port of the phone, do as follows:

     a. Select the checkbox of **PC port**.
     b. In the **VLAN ID** field, enter a VLAN ID.
     c. In the **Priority** drop-down list, select a priority value for the VLAN.

     The priority value is between `0` (lowest) to `7` (highest).
   - To acquire VLAN ID through DHCP option, do as follows:

     a. Select the checkbox of **DHCP VLAN**.
     b. In the **Option** field, enter the DHCP option(s) from which the phone will obtain the VLAN ID.

     > **Note:**
     > Use a comma to separate multiple DHCP options.

3. Click **Save**.

Step 2. Apply the configuration to IP phone

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

   The system prompts you whether to reprovision the phone.
2. In the pop-up window, click **OK**.

Result

The phones automatically apply the changes. Check the VLAN settings on the phone to see if the changes are applied.

Auto Provision Function Keys for Phones

Function keys allow extension users to monitor status of specific objects or quickly perform specific operations from Linkus or IP phone. This topic describes how to provision function keys for extension users' IP phones.

Supported key types

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

Key type	Function
N/A	No functionality.
Line	Configure line keys.
BLF	• Extension ◦ Monitor the call status of a specific extension. ◦ Monitor the DND (Do Not Disturb) presence of a specific extension. ◦ Place a call to the monitored extension. ◦ Pick up calls ringing on the monitored extension. • Trunk ◦ Monitor the status of a specific trunk. ◦ Place an outbound call through the monitored trunk. • Queue ◦ Monitor specific pause status of a queue agent. For more information, see Auto Provision a function key for an IP phone.
Speed Dial	Place a call to the most commonly dialed numbers or extensions.

Key type	Function
Check Voicemail	• Monitor the status of voicemail. • Check voicemail messages.
Check Group Voicemail	• Monitor the status of group voicemail in shared mode. • Check group voicemail messages.
Park & Retrieve	• Monitor the status of a specific parking number. • Park a call on a specific parking number. • Retrieve a parked call from a specific parking number.
Intercom	Place an intercom call to the monitored extension to make an announcement.
DTMF	Send DTMF signals directly instead of manually entering the numbers each time.
Agent Login/Logout	• Monitor login status in a specific queue. • Log in to or log out of a specific queue.
Agent Pause/Unpause	• Monitor service status in a specific queue. • Pause or unpause receiving a call from a specific queue.
LDAP Directory	Quickly access the LDAP phonebook to query contact information. **Note:** This key type is only available for IP phone.
Boss-Secretary Feature	• For boss extensions: Monitor Secretary's Call Status. • For secretary extensions: Monitor Boss's Call Status.
Call Forward	Quickly enable or disable call forwarding. **Note:** The key type is only available for IP phone. For more information, see Forward All Incoming Calls to Another Destination by BLF Key.
Action URL	Quickly send an HTTP GET request to a specified URL for reporting specific events. **Note:** The key type is only available for IP phone.

Note:

If your desired function keys are not listed in the supported key types, you can create a custom Auto Provisioning template and apply the template to a provisioned IP phone.

Prerequisites

You have connected the IP phone to the PBX and associate it with an extension via auto provisioning. For more information about the configuration, see the following topics:

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

Auto Provision a function key for an IP phone

This section use the BLF function key as an example to show how to auto provision a specific function key to an IP phone.

1. Set up function key.
   a. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
   b. Click beside the desired phone.

      You are redirected to the setting page of the extension associated with the phone.
   c. Click the **Function keys** tab, then configure a BLF key according to your needs.
      - Monitor extension status by BLF key
      - Monitor trunk status by BLF key
      - Monitor agent status by BLF key

Monitor extension status by BLF key

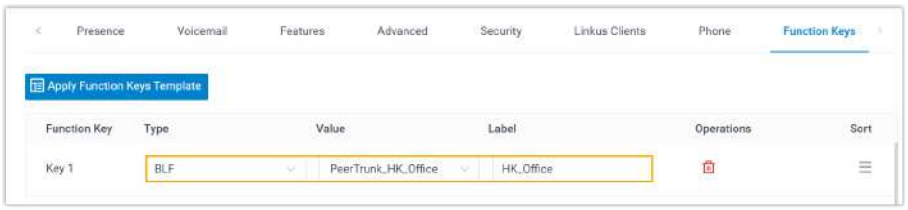
Configure a BLF key to monitor a specific extension's status in real time, make calls to it, or pick up its incoming calls with a single press.

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

Monitor trunk status by BLF key

Configure a BLF key to monitor a specific trunk's status in real time, and seize the trunk to make outbound calls with a single press.

> **Note:**
> To seize a trunk to call out by BLF key, make sure the extension has the permission to use the monitored trunk for outbound calls.

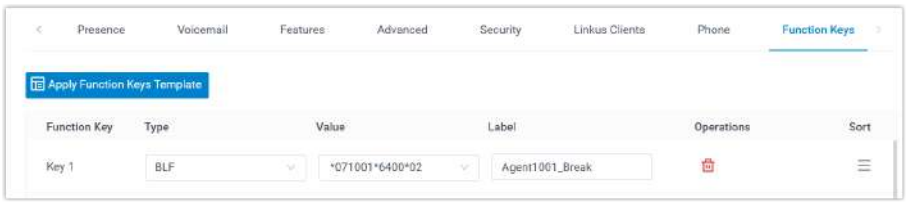


- **Type**: Select **BLF**.
- **Value**: Enter the name of the trunk to be monitored.
- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

Monitor agent status by BLF key

Configure a BLF key to monitor specific pause status of a queue agent.

> **Note:**
> Before you set up, you need to obtain the following feature codes:
>
> - Pause feature code (Path: **Call Features > Feature Code > Queue > Pause/Unpause**)
> - Pause Reason feature code (Path: **Call Features > Feature Code > Pause Reason**)



- **Type**: Select **BLF** key.
- **Value**: Enter the feature codes.

  The format should be `Pause feature code` + `extension number` + `*` + `queue number` + `pause reason feature code`. For example, `*071001*6400*01`.
- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

d. Click **Save**.

2. Reprovision IP phones with the extensions registered.

   a. Go to **Auto Provisioning > Phones**.

   b. Click beside the phone.

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

   The phone automatically applies the change, and the BLF key shows the real-time status of the monitored item.

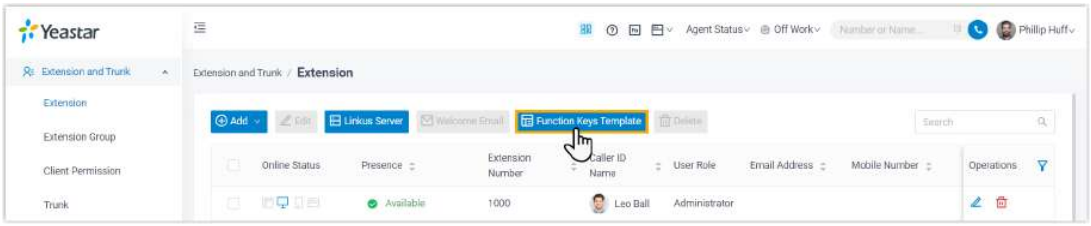
Scenario	BLF LED
Monitor extension status by BLF key	• **Solid Green**: The extension is being monitored, and the status is idle. • **Solid Red**: The extension is sending a call or is in a call; or the extension presence is DND (Do Not Disturb). **Note:** For Fanvil IP phones that support differentiated DND status indication, the DND status is indicated by a **Solid Yellow** LED light. • **Flashing Red**: The extension is ringing. • **LED off**: The extension is not registered, or the extension has been deleted from the PBX system. **Note:** You can press the BLF key on the phone to achieve the followings: • Place a call to the monitored extension.

Scenario	BLF LED
	• Pick up the monitored extension's incoming calls if the corresponding feature code is enabled on **Call Features > Feature Code > Call Pickup > Extension Pickup**.
Monitor trunk status by BLF key	• **Solid Green**: The trunk is being monitored, and the status is idle. • **Solid Red**: The trunk is busy. • **LED off**: The BLF key configuration failed. **Note:** You can press the BLF key to seize the trunk, then dial a number after a dial tone to call out.
Monitor agent status by BLF key	• **Solid Green**: The monitored agent is NOT in the specified pause status. • **Flashing Red**: The agent is in the specified pause status. • **LED off**: The BLF key configuration failed.

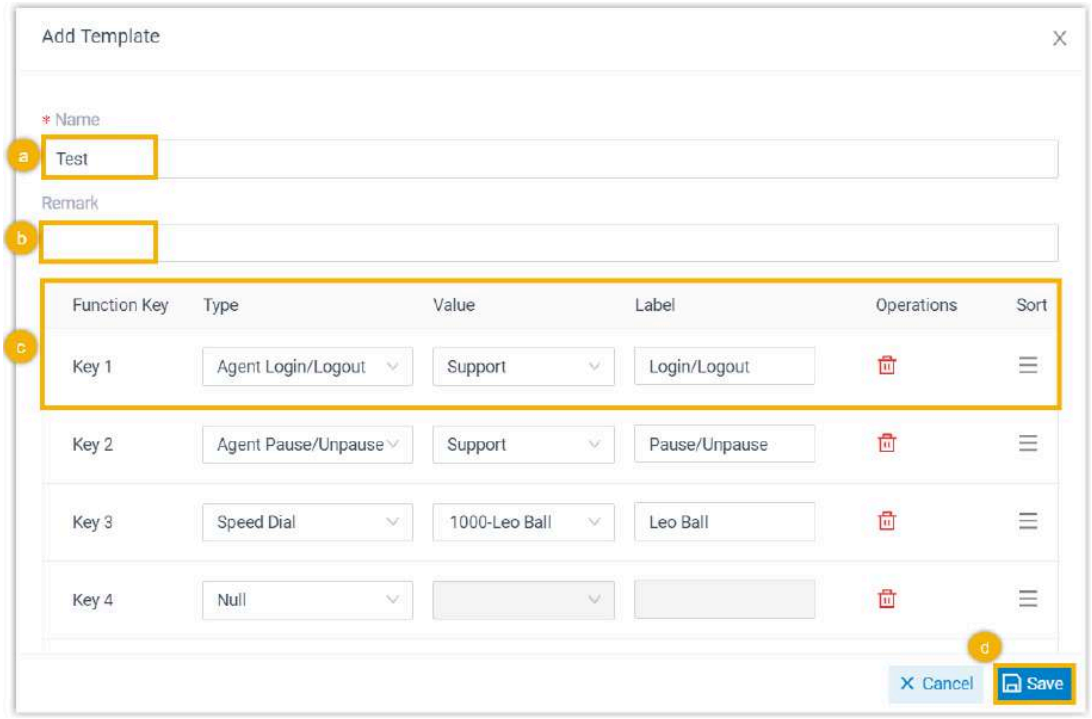
Auto Provision function keys for phones in bulk using a function key template

If you are managing many IP phones and want to simplify configuration while ensuring consistency across all phones, you can auto provision function keys in bulk using a function key template.

1. Add a function keys template.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
   b. Click **Function Keys Template**.



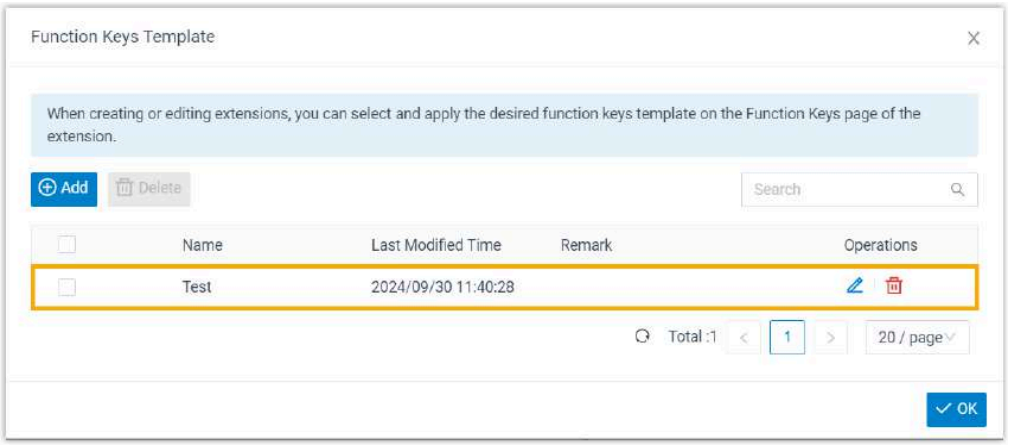
   c. Click **Add** to add a function key template, then configure the following settings.



Note:
The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the excess function keys cannot take effect. However, if the user's IP phone is connected with an expansion module, the excess function keys are automatically applied to the expansion module.

i. In the **Name** field, enter a name to help you identify the template.
ii. **Optional:** In the **Remark** field, enter a short description about the template.
iii. In the function keys list, configure function keys according to your needs.
   - **Type**: Select a key type.
   - **Value**: Configure a desired value based on the key type.
   - **Label**: Optional. Enter a value to help extension users identify the function key.
iv. Click **Save**.

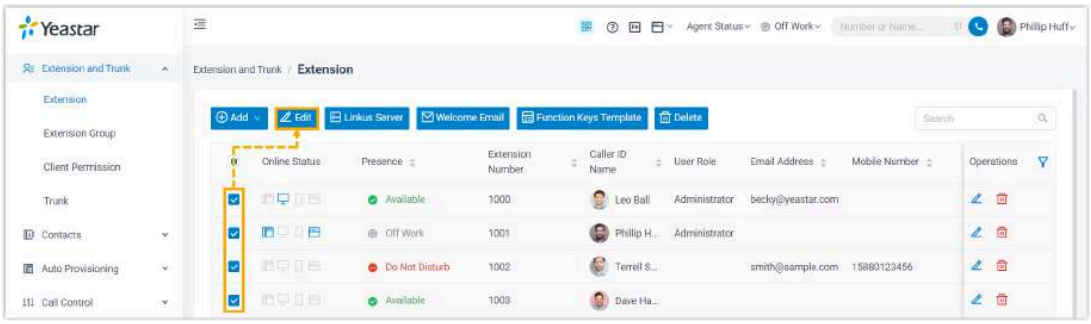
The function key template is created and displayed on the list.



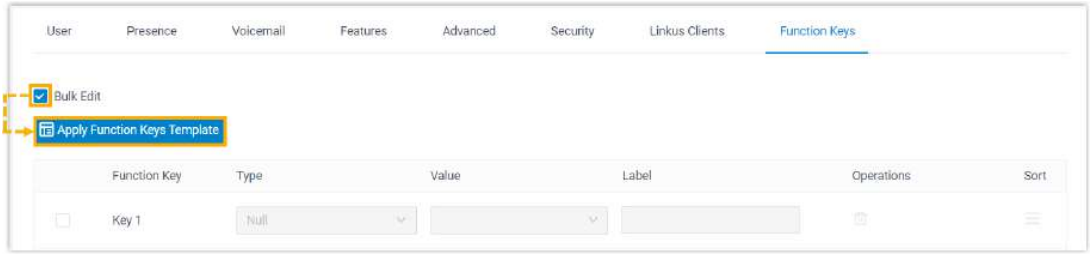
d. Click **OK**.

2. Apply the function keys template to extensions.

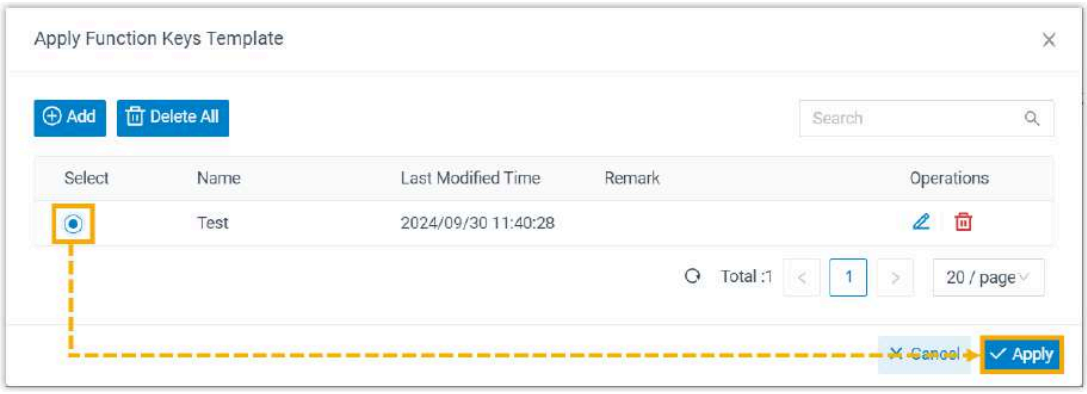
a. On the extension list, select the checkboxes of the desired extensions, then click **Edit**.



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

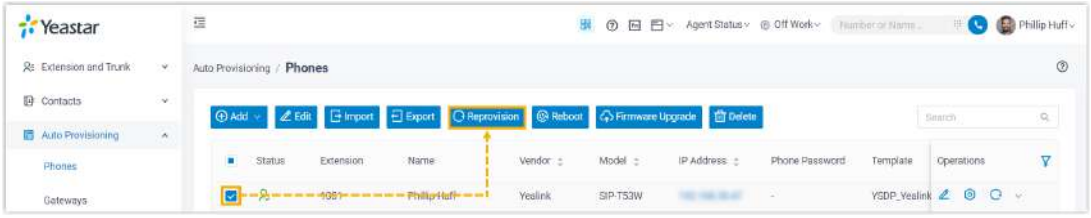


c. In the pop-up window, select the function keys template, then click **Apply**.



d. Click **Save**.

3. Reprovision IP phones with the extensions registered.
   a. Go to **Auto Provisioning > Phones**.
   b. Select the checkboxes of the desired phones, then click **Reprovision**.



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

   The phones automatically apply the changes. Check the function key status on the phones to see if the changes are applied.

Related information

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

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

- If you want to seize a trunk to call out by BLF key, make sure the extension assigned to the provisioned phone has the permission to use the monitored trunk for outbound calls.

Procedure

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

Step 1. Set up a function key for trunk monitoring

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

   The following figure shows a configuration example of monitoring the trunk `peer-trunk-66.41`.

   - **Type**: Select **BLF**.
   - **Value**: Enter the name of the trunk to be monitored. In this example, enter `peer-trunk-66.41`.
   - **Label**: Optional. Enter a value, which will be displayed on the phone screen.
4. Click **Save**.

Step 2. Apply the configuration to IP phone

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

The system prompts you whether to reprovision the phone.

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

Result

- The BLF key shows the real-time status of the monitored trunk:
  - **Green BLF LED**: The trunk is being monitored, and the status is idle.
  - **Red BLF LED**: The trunk is busy.
  - **BLF LED off**: The BLF key configuration failed.
- Press the BLF key to seize the trunk, you will get a dial tone, then dial the number that you want to call.

Forward All Incoming Calls to Another Destination by BLF Key

You can set up call forwarding for provisioned IP phones through Yeastar P-Series Software Edition. This topic describes how to set a BLF key on the IP phone via Auto Provisioning, so that users can quickly enable forwarding for all incoming calls by the BLF key.

> **Note:**
> This feature is independent of the extension's call forwarding settings based on presence or feature code. Call forwarding by BLF key is only available for IP phone and will forward all incoming calls to the predefined destination.

Prerequisites

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

For more information, see the following topics:

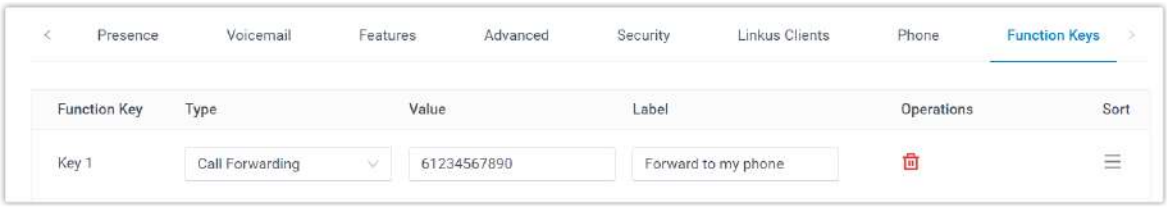
- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)
- Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
- Auto Provision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

Procedure

- Step 1. Set up a function key for call forwarding

Step 1. Set up a function key for call forwarding

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



   - **Type**: Select **Call Forwarding**.
   - **Value**: Enter the number to which you want to forward all calls.

     > **Note:**
     > If the number is an external number, make sure that the extension associated with the phone has permission to use the outbound route, or the call forwarding would fail.

   - **Label**: Optional. Enter a value, which will be displayed on the phone screen.
4. Click **Save**.

Step 2. Apply the configuration to IP phone

1. On PBX web portal, go to **Auto Provisioning > Phones**, click beside the associated IP phone.

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

Result

- The BLF key shows the current status of the call forwarding:
  - **Green BLF LED**: The call forwarding is enabled.

    - **BLF LED off**: The call forwarding is disabled.
- User can quickly enable the call forwarding by pressing the BLF key, and all incoming calls sent to the extension will be forwarded to the preset destination.

  In this example, all incoming calls sent to extension 2006 will be forwarded to an external number 61234567890.

Synchronize Phone Time with Yeastar P-Series 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 an extension.

For more information, see the following topics:

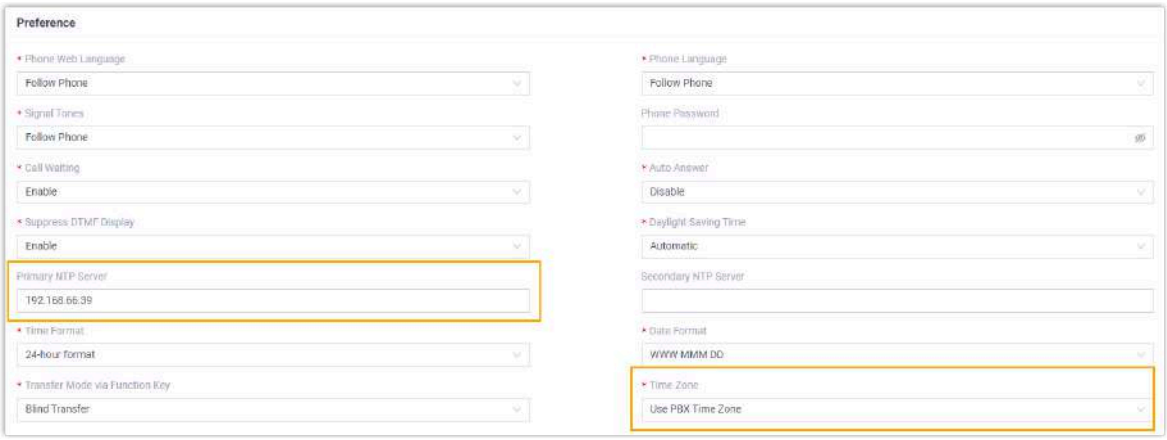
- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)
- Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
- Auto Provision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

Procedure

- Step 1. Set up PBX as NTP Server
- Step 2. Apply the configuration to IP phone

Step 1. Set up PBX as NTP Server

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the extension that is assigned to the phone.
2. Click the **Phone** tab.
3. Scroll down to the **Preference** section, complete the following settings.



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

4. Click **Save**.

Step 2. Apply the configuration to IP phone

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

   The system prompts you whether to reprovision the phone.
2. In the pop-up window, click **OK**.

Result

The phone time is now synchronized with the PBX.

Modify a Provisioned Phone Settings

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

Modify settings of a provisioned IP phone

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
2. Modify the phone that is associated with the extension.
   a. Click the **Phone** tab.
   b. Modify phone settings in the **Preference** and **Codecs** sections.

c. Click **Save**.

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

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

   The phone automatically applies the changes.

Modify settings of a provisioned DECT phone

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

   The phone automatically applies the changes.

Modify a Provisioned Gateway Settings

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

Procedure

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

> **Note:**
> If you want to change other settings, click the gateway IP address displayed on the provisioning list to access the gateway web interface, and change the configurations as your need.

The PBX prompts you whether to reboot the gateway.

3. Click **OK** to reboot the gateway to apply the configurations.

   The gateway will automatically apply the changes after reboot.

Manage Auto Provisioning Templates

Apply a New Template to a Provisioned IP Phone/Gateway

If you want to customize a device, you can create a custom template and apply the new template to the IP phone/gateway.

Apply a new template to a provisioned IP phone

Prerequisites

[Create a custom Auto Provisioning template](#).

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**, edit the desired phones.
2. In the **Options** section, select a desired template from the **Template** drop-down list.
3. Click **Save**.

Result

The configurations in the new template will be applied automatically to the phone.

Apply a new template to a provisioned gateway

Prerequisites

[Create a custom Auto Provisioning template](#).

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Gateways**, edit a desired gateway.

2. In the **Options** section, select a desired template from the **Template** drop-down list.
3. Click **Save**.

   The PBX prompts you whether to reboot the gateway.
4. Click **OK** to reboot the gateway to apply the configurations.

Result

The configurations in the new template will be applied automatically to the gateway.

Related information

Update Auto Provisioning template(s) to all applicable devices

View a Default Auto Provisioning Template

The default template of different models contains different parameters, you can view what configurations are included in the default template. This topic describes how to search and view a default template.

Background information

Yeastar P-Series 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.

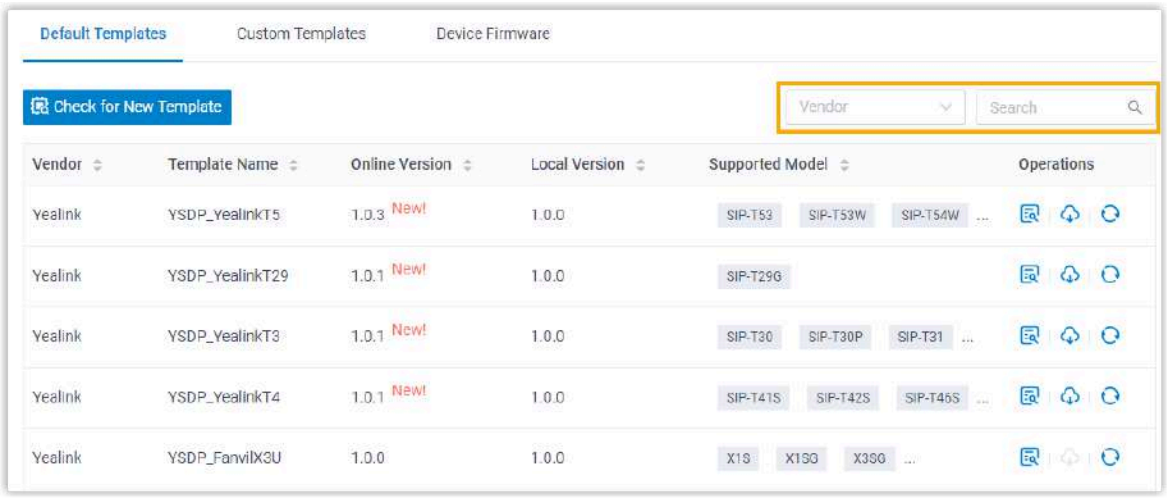
- **Variables**: Variables are attributes to which various values can be assigned. A variable starts with `{{.`, and ends with `}}`. For example, `{{.PhoneWebLanguage}}` means a variable of Phone Web Language setting. The phone web language varies on each phone according to specific phone configuration.
- **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.

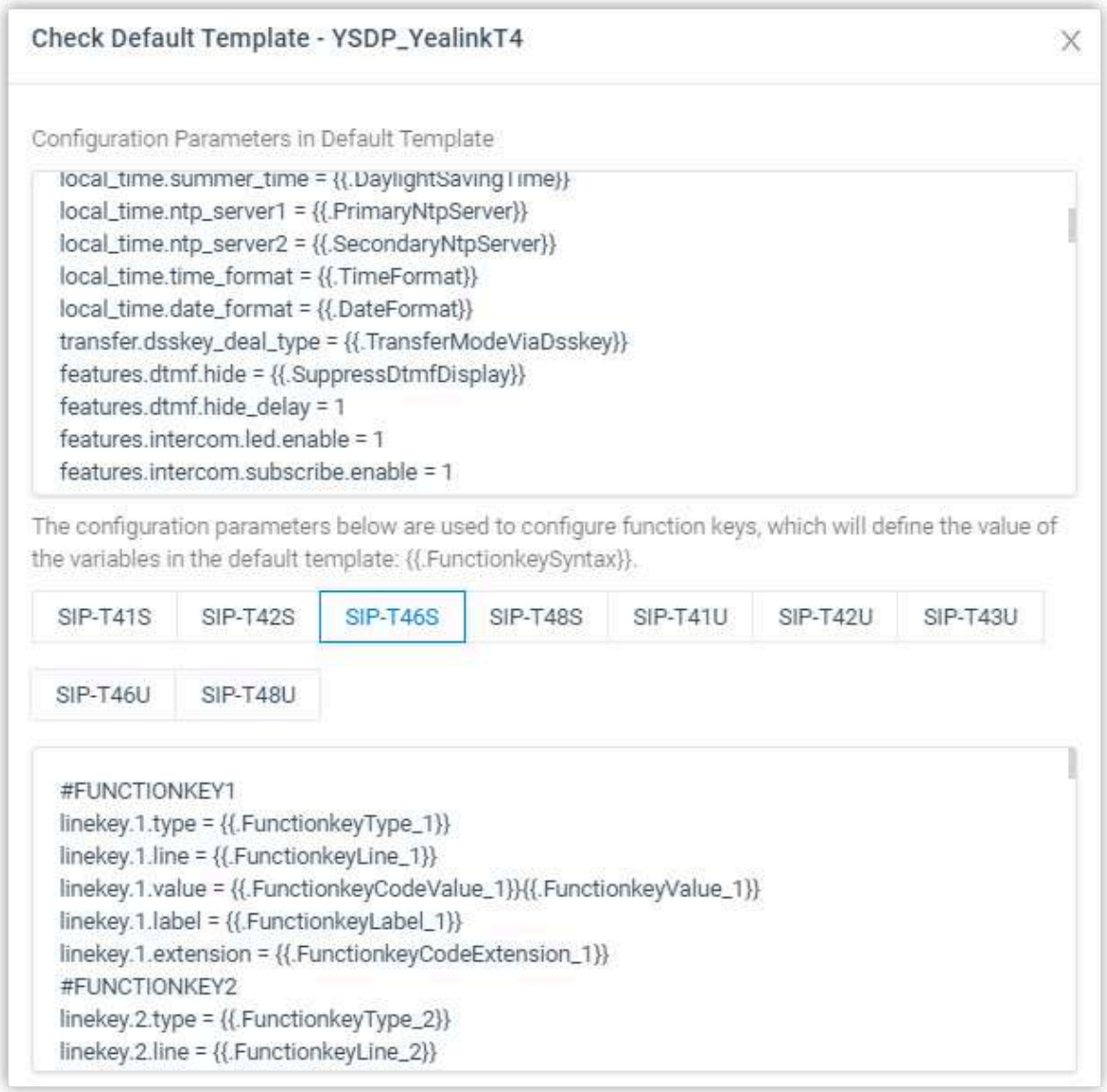
   You can search the template by vendor, provisioning template name, or device model.

   The search results are displayed automatically on the web page.



3. Click beside the desired template to view the default configurations.
   The following figure shows a default template of Yealink T56A. The default template consists of two parts:
   - **Configuration parameters in Default Template**: The pre-defined configuration parameters in this template are displayed in the first text box.
   - **Function keys of device model**: The pre-defined function keys supported by the device model are displayed in the second text box.

     You can click the device model tab to view the supported keys.



Related information

[Create a Custom Auto Provisioning Template]
[Manage Custom Auto Provisioning Templates]

Update a Default Auto Provisioning Template

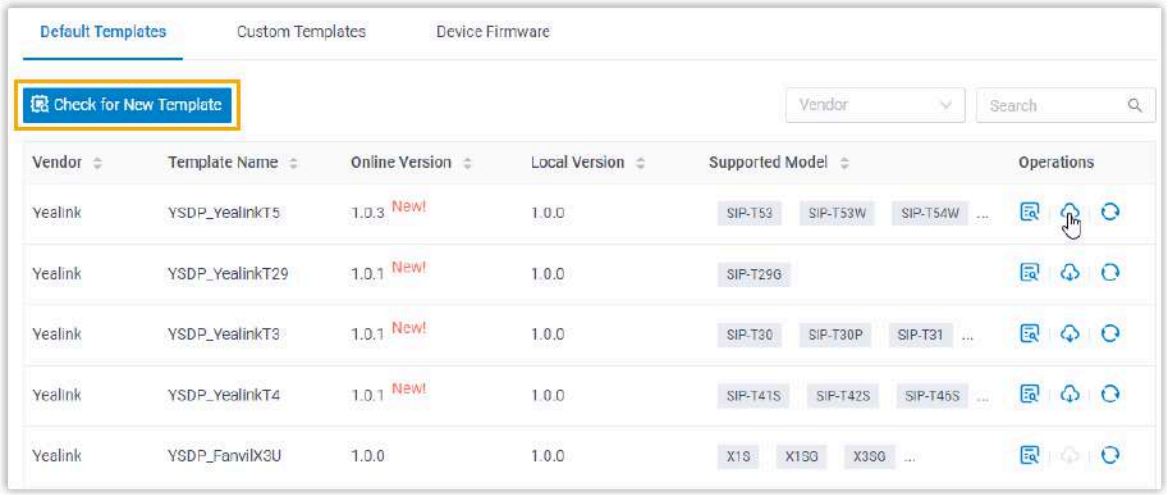
Yeastar P-Series Software Edition regularly provides new template versions to release new features and fix bugs. You can check if a new template is available, and decide whether to update the default template. This topic describes how to update a default template.

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.



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**, **Codecs** and **LDAP Directory** sections.
   - **Remark**: Optional. Enter a short description about this template.
4. In the **Preference** section, modify the preference settings that are provided by the source default template.
5. In the **Distinctive Ringtone** section, modify the settings according to your needs.
6. In the **Codecs** section, select a desired codec according to your needs.
7. In the **LDAP Directory** section, modify the settings according to your needs.
8. In the **VLAN** section, configure the VLAN settings according to your needs.
9. Click **Save**.

Create an advanced Auto Provisioning template

If the settings that you want to configure for your devices are not defined in the default provisioning template, you can create an advanced Auto Provisioning template.

1. Log in to PBX web portal, go to **Auto Provisioning > Resource Repository > Custom Templates**.
2. Click **Add**.
3. In the **Basic** section, set the basic information.
   - **Template Name**: Enter a name to help you identify it.
   - **Source Default Template**: Select a default template to customize.
   - **Template Type**: Select **Advanced**.

     The general settings that the source default template provides will be displayed in the **Preference**, **Distinctive Ringtone**, **Codecs** and **LDAP Directory** sections; A text box containing all configuration parameters will be displayed in the **Customize Configuration Parameters In Text** section.
   - **Remark**: Optional. Enter a short description about this template.
4. In the **Preference** section, modify the preference settings that are provided by the source default template.
5. In the **Distinctive Ringtone** section, modify the settings according to your needs.
6. In the **Codecs** section, select a desired codec according to your needs.
7. In the **LDAP Directory** section, modify the settings according to your needs.
8. In the **VLAN** section, configure the VLAN settings according to your needs.
9. Add additional parameters that are not provided by the source default template.

   > **Note:**
   > The general settings defined in source default template are assigned with variables. The variable that starts with `{{.` and ends with `}}` is associated with the configuration that can be configured on **Preference**, **Codecs**, and **Function Keys** sections. Please don't change the variable if you want to modify the settings from PBX web portal.

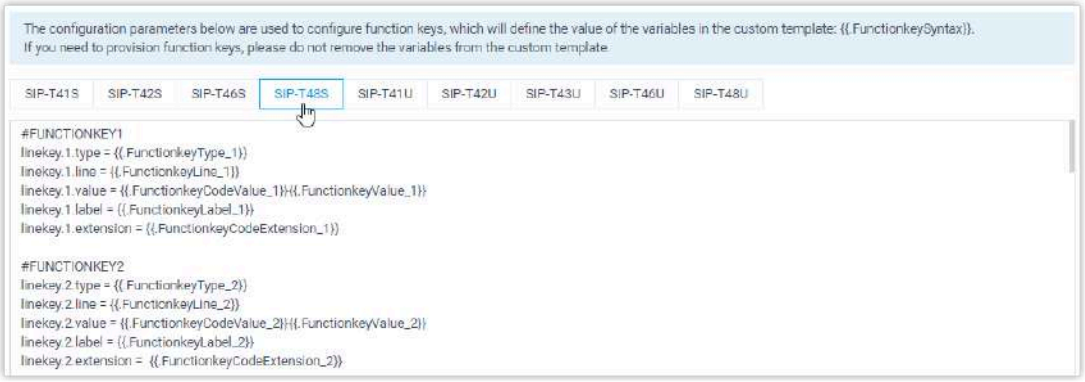
   a. In the **Customize Configuration Parameters In Text** section, add your configuration parameters in the first text box.

      > **Note:**

> Contact your vendor to make sure that the parameters are supported for the device model.

b. In the second text box, select which function keys to be applied according to the phone model.

You can also add your function key parameters in the second text box.



10. Click **Save**.

Related information

Edit a custom Auto Provisioning template
Update Auto Provisioning template(s) to all applicable devices

Manage Custom Auto Provisioning Templates

This topic describes how to edit or delete custom Auto Provisioning templates.

Edit a custom Auto Provisioning template

1. Log in to PBX web portal, go to **Auto Provisioning > Resource Repository > Custom Templates**.
2. Click beside a desired custom template.
3. Modify the device settings.
4. Click **Save**.
   The system prompts you whether to update the new configurations to devices that use this template.
   - **Yes**: The system generates new configuration files and immediately triggers provisioning for all devices that use this template.

- **No**: The system saves the changes to this template, and generates new configuration files for all devices that use this template. You can trigger provisioning manually for specific devices later.

Delete custom Auto Provisioning templates

1. Log in to PBX web portal, go to **Auto Provisioning > Resource Repository > Custom Templates**.
2. Delete custom templates according to your needs.
   - To delete a custom template, click  beside the desired template.
   - To delete custom templates in bulk, select the checkboxes of desired templates, click **Delete**.
3. In the pop-up dialog box, click **Yes**.

   If the template is in use, you need to release it from the devices that use the template first.

Update Auto Provisioning template(s) to all applicable devices

1. Log in to PBX web portal, go to **Auto Provisioning > Resource Repository > Custom Templates**.
2. Update the configurations to the devices:
   - To update the configuration of a specific template, click  beside the desired template.
   - To update the configuration of multiple templates, select the checkboxes of desired templates, click **Update to Device**.
3. Click **Yes** to trigger phone provisioning.

Download or upload custom Auto Provisioning templates

Yeastar P-Series Software Edition support downloading and uploading of auto provisioning custom templates, which allows template reuse across multiple PBXs without the need to recreate templates manually.

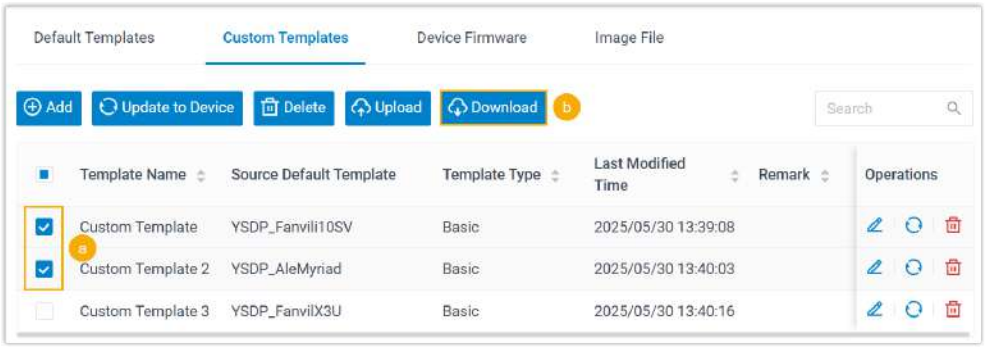
> **Important:**
> The downloaded template files are encrypted and cannot be opened directly; they can only be uploaded and parsed by the PBX.

Requirements

The firmware of Yeastar P-Series Software Edition is 83.19.0.70 or later.

Procedure

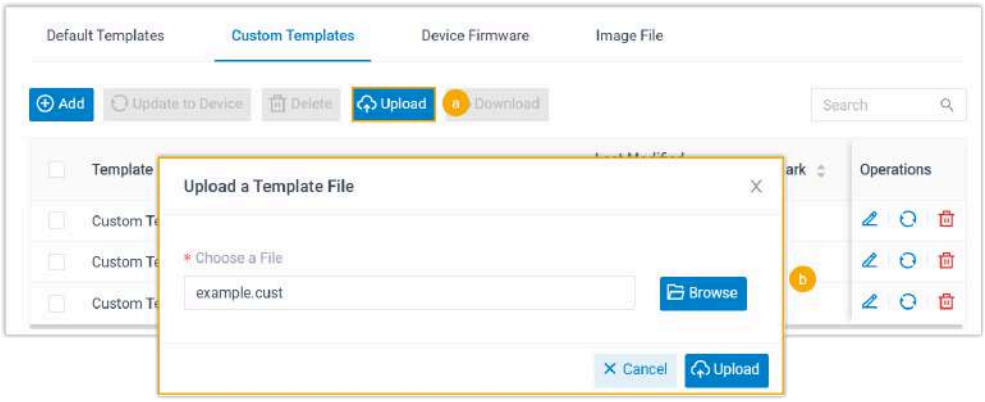
1. Log in to PBX web portal, go to **Auto Provisioning > Resource Repository > Custom Templates**.
2. To download custom auto provisioning templates, do as follows:



   a. Select one or more desired templates.
   b. At the top of the list, click **Download**.

      The template files are downloaded to your computer in `.cust` format.

3. To upload a custom auto provisioning template, do as follows:



   a. At the top of the list, click **Upload**.
   b. In the pop-up window, click **Browse** to select the downloaded `.cust` template file, then click **Upload**.

      The template is uploaded and displayed in the list.

Manage IP Phone Firmware

Update Phone Firmware via Auto Provisioning

This topic describes how to update phone firmware via Auto Provisioning.

Prerequisites

Upload the desired phone firmware to PBX. For more information, see Add a device firmware.

Update firmware to all applicable phones

1. Log in to PBX web portal, go to **Auto Provisioning > Resource Repository > Device Firmware**.
2. Click beside the desired firmware.
3. Click **Yes** to upgrade the phones.

Update firmware to specific phones

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Select the checkboxes of the desired phones.
3. Click **Firmware Upgrade**.
4. Select the firmware that you want to upgrade, click **Upgrade Now**.

Result

The phones automatically reboot and update their firmwares to the new version.

Manage Device Firmware Files

This topic describes how to manage device firmwares, including add, edit, and delete device firmware files.

Add a device firmware file

Note:
You can upload up to **3** device firmware files to PBX server.

1. Log in to PBX web portal, go to **Auto Provisioning > Resource Repository > Device Firmware**, click **Add**.
2. In the **Device** section, select a firmware vendor and device model.
3. In the **Firmware** section, upload the firmware.
    - **Firmware Version**: Enter a name (firmware version) to help you identify it.
    - **Upload Firmware File**: Click **Browse** and select the corresponding firmware.
    - **Remark**: Optional. Enter a short description about the firmware.
4. Click **Save**.

The uploaded firmware is displayed on the **Device Firmware** list. When you update phone firmware, the uploaded firmware can be detected and displayed for you to choose.

Edit a device firmware file

1. Log in to PBX web portal, go to **Auto Provisioning > Resource Repository > Device Firmware**.
2. Click  beside the desired firmware.
3. In the **Firmware** section, edit the firmware information or update the firmware file.
    - **Firmware Version**: Enter a name (firmware version) to help you identify it.
    - **Upload**: Click **Browse** and select the corresponding firmware.
    - **Remark**: Optional. Edit the note.
4. Click **Save**.

Delete device firmware files

1. Log in to PBX web portal, go to **Auto Provisioning > Resource Repository > Device Firmware**.
2. Delete device firmware files.
    - To delete a device firmware, click  beside the desired firmware.
    - To delete device firmwares in bulk, select the checkboxes of the desired firmware, and click **Delete**.
3. Click **OK**.

Auto Provisioning - Supported Devices

This topic lists the devices that are currently supported for Auto Provisioning by Yeastar P-Series Software Edition.

Yealink phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Yealink IP Phone with Yeastar P-Series Software Edition.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Yealink IP Phone with Yeastar P-Series Software Edition.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
AX83H	180.86.0.5 or later	83.16.0.25 or later	• PnP • DHCP • RPS • Provision Link
AX86R	180.86.0.5 or later	83.18.0.59 or later	• PnP • DHCP • RPS • Provision Link
CP920	78.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
CP925	148.86.0.5 or later	83.5.0.9 or later	• PnP • DHCP • RPS • Provision Link
CP960	73.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
CP965	143.86.0.5 or later	83.5.0.9 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
SIP-CP935W	149.86.0.5 or later	83.5.0.9 or later	• PnP • DHCP • RPS • Provision Link
SIP-T19P_E2	53.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T20P	9.73.0.50 or later	83.18.0.102 or later	• PnP • DHCP • RPS • Provision Link
SIP-T21_E2	52.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T21P_E2	52.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T22P	7.73.0.50 or later	83.18.0.102 or later	• PnP • DHCP • RPS • Provision Link
SIP-T23G	44.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T23P	44.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T26P	6.73.0.50 or later	83.18.0.102 or later	• PnP • DHCP • RPS • Provision Link
SIP-T27G	69.85.0.5 or later	83.4.0.17 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
SIP-T28P	2.73.0.50 or later	83.18.0.102 or later	• PnP • DHCP • RPS • Provision Link
SIP-T29G	46.83.0.120 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T30	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T30P	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T31	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T31G	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T31P	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T31W	124.86.0.75 or later	83.11.0.56 or later	• PnP • DHCP • RPS • Provision Link
SIP-T32G	32.70.0.125 or later	83.18.0.102 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
SIP-T33G	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T33P	124.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T34W	124.86.0.75 or later	83.12.0.23 or later	• PnP • DHCP • RPS • Provision Link
SIP-T38G	38.70.0.185 or later	83.18.0.102 or later	• PnP • DHCP • RPS • Provision Link
SIP-T40G	76.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T40P	54.84.0.125 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T41P	36.83.0.120 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T41S	66.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T41U	108.85.0.39 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T42G	29.83.0.120 or later	83.4.0.17 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
SIP-T42S	66.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T42U	108.85.0.39 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T43U	108.85.0.39 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T44U	108.86.0.90 or later	83.10.0.32 or later	• PnP • DHCP • RPS • Provision Link
SIP-T44W	108.86.0.90 or later	83.10.0.32 or later	• PnP • DHCP • RPS • Provision Link
SIP-T46G	28.83.0.120 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T46S	66.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T46U	108.85.0.39 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T48G	35.83.0.120 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T48S	66.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
SIP-T48U	108.85.0.39 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T52S	70.84.0.70 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T53	96.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T53W	96.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T54S	70.84.0.70 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T54W	96.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T56A	58.83.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T57W	96.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T58	58.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
SIP-T58W	150.86.0.5 or later	83.4.0.17 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
SIP-T73W	185.87.0.15 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T73U	185.87.0.15 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T74W	185.87.0.15 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T74U	185.87.0.15 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T77U	185.87.0.15 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T85W	185.87.0.15 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T87W	185.87.0.15 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T88W	192.87.0.5 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
SIP-T88V	192.87.0.5 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
T64LTE	132.86.0.25 or later	83.16.0.71 or later	• PnP • DHCP • RPS • Provision Link
T67LTE	132.86.0.35 or later	83.16.0.71 or later	• PnP • DHCP • RPS • Provision Link
VP59	91.85.0.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
W60B (W53P, W41P, W60P, CP930W-Base)	77.83.0.85 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
W70B (W79P, W76P, W73P)	146.85.0.20 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
W75DM	175.85.0.5 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
W80B	W80DM-103.83.0.80	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
W90DM	130.85.0.15 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link

Fanvil phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Fanvil IP Phone with Yeastar P-Series Software Edition.

- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Fanvil IP Phone with Yeastar P-Series Software Edition.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
A10	2.12.4 or later	83.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
A10W	2.12.4 or later	83.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
A308i	2.6.10.1177 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
A32	2.6.0.408 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
A32i	2.6.0.408 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
A320	2.6.0.1402 or later	83.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
A320i	2.6.0.1402 or later	83.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
FH-S01	2.12.8 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
H1	2.12.1 or later	83.10.0.32 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
H2U	2.4.7 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
H2U-V2	2.4.7.6 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
H3	2.12.1.7334 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
H3W	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
H4	1.0.8 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
H4W	1.0.8 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
H5	2.12.1.7334 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
H5W	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
H6	1.0.8 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
H6W	1.0.8 or later	83.14.0.26 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
H603W	2.14.0.11 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
i10	1.2.7 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i10D	1.2.7 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i10S	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i10SD	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i10SV	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i10V	1.2.7 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i11S	1.2.7 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i11SV	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
i12	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i16S	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i16SV	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i16V	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i18S	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i20S	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i23S	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i30	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i31S	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i32V	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
i33V	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i33VF	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i504	2.12.43.13 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i505	2.6.6.391 or later	83.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
i506W	2.12.43.13 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i507W	2.6.6.394 or later	83.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
i51	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i51W	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i52	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i52W	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
i53	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i53W	2.8.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i55A	1.0.0.45 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
i56A	0.3.0.21 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
i57A	1.0.0.46 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
i61	2.4.0 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i62	2.4.0 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i63	2.4.0 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i64	2.4.0 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
i68	2.8.40.22 or later	83.8.0.25 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
PA2	2.8.2.7009 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
PA2S	2.8.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
PA3	2.4.4 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
V50P	2.12.20.4 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V60P	2.12.20.3 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V60W	2.12.20.3 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V61G	2.12.18.8 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V61W	2.12.18.8 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V62	2.4.10 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
V62G	2.12.18.8 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V62W	2.12.18.8 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V62 Pro	2.12.18.2 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V63	2.12.16.19 or later	83.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
V64	2.4.10 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
V65	2.12.2.4 or later	83.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
V66	2.12.18.4 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V66 Pro	2.12.18.4 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
V67	2.6.0 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
W610W	2.12.0 or later	83.11.0.22 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
W611W	pvt-2.8 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
W710D	1.16.2 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
W710H	1.0.14.5 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
X1S / X1SP	2.2.12 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X1SG	2.2.12 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X2/X2P	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X2C/X2CP	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X210	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X210-V2	2.12.1.3 or later	83.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
X210i	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
X210i-V2	2.12.1.3 or later	83.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
X3SG	2.2.12 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X3S/X3SP/X3G	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X3S Lite / X3SP Lite	2.4.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X3S Pro / X3SP Pro	2.4.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X3SW	2.4.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X3SG Lite	2.4.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X3SG Pro	2.4.5 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X3U	2.2.12 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X3U Pro	2.4.5 or later	83.4.0.17 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
X301	2.12.2 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X301G	2.12.2 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X301W	2.12.2 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X303	2.12.2 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X303G	2.12.2 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X303W	2.12.2 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X303-2 WIRE	1.0.3 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
X305	2.12.1.6 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
X4/X4G	2.14.0.7386 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
X4U	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X4U-V2	2.12.1 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
X5U	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X5U-V2	2.12.1 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
X5S	2.2.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X6	2.2.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X6U	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X6U-V2	2.12.1 or later	83.6.0.24 or later	• PnP • DHCP • RPS • Provision Link
X7	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X7A	2.2.0.229 or later	83.4.0.17 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
X7C	2.2.11 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
X7-V2	2.12.1.3 or later	83.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
X7C-V2	2.12.1.3 or later	83.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
Y501	2.12.4 or later	83.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
Y501W	2.12.4 or later	83.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
Y501-Y	2.12.4 or later	83.11.0.22 or later	• PnP • DHCP • RPS • Provision Link
Y501W-Y	2.12.4 or later	83.11.0.22 or later	• PnP • DHCP • RPS • Provision Link

Grandstream phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Grandstream IP Phone with Yeastar P-Series Software Edition.

- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Grandstream IP Phone with Yeastar P-Series Software Edition.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
GXP1610	1.0.7.13 or later	83.4.0.17 or later	• PnP • DHCP • Provision Link
GXP1620	1.0.7.13 or later	83.4.0.17 or later	• PnP • DHCP • Provision Link
GXP1625	1.0.7.13 or later	83.4.0.17 or later	• PnP • DHCP • Provision Link
GXP1628	1.0.7.13 or later	83.4.0.17 or later	• PnP • DHCP • Provision Link
GXP1630	1.0.7.13 or later	83.4.0.17 or later	• PnP • DHCP • Provision Link
GXP2130	1.0.11.16 or later	83.4.0.17 or later	• PnP • DHCP • Provision Link
GXP2135	1.0.11.16 or later	83.4.0.17 or later	• PnP • DHCP • Provision Link
GXP2140	1.0.11.16 or later	83.4.0.17 or later	• PnP • DHCP • Provision Link
GXP2160	1.0.11.16 or later	83.4.0.17 or later	• PnP • DHCP • Provision Link
GXP2170	1.0.11.16 or later	83.4.0.17 or later	• PnP • DHCP • Provision Link
GAC2500	1.0.3.45 or later	83.11.0.22 or later	• PnP • DHCP • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
GAC2570	1.0.1.36 or later	83.11.0.22 or later	• PnP • DHCP • Provision Link
GRP2601	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2601P	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2602	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2602P	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2602G	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2602W	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2603	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2603P	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2604	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2604P	1.0.3.63 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2612	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2612P	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
GRP2612G	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2612W	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2613	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2614	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2615	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2616	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2624	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2634	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GRP2670	1.0.7.25 or later	83.7.0.51 or later	• PnP • DHCP • Provision Link
GHP610	1.0.1.71 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
GHP610W	1.0.1.71 or later	83.17.0.17 or later	• PnP • DHCP • Provision Link
GHP611	1.0.1.71 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
GHP611W	1.0.1.71 or later	83.17.0.17 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • Provision Link
GHP620	1.0.1.71 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
GHP620W	1.0.1.71 or later	83.17.0.17 or later	• PnP • DHCP • Provision Link
GHP621	1.0.1.71 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
GHP621W	1.0.1.71 or later	83.17.0.17 or later	• PnP • DHCP • Provision Link
GHP630	1.0.1.71 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
GHP630W	1.0.1.71 or later	83.17.017 or later	• PnP • DHCP • Provision Link
GHP631	1.0.1.40 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
GHP631W	1.0.1.71 or later	83.17.0.17 or later	• PnP • DHCP • Provision Link
WP825	1.0.11.67 or later	83.17.0.17 or later	• PnP • DHCP • Provision Link

Htek phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Htek IP Phone with Yeastar P-Series Software Edition.

- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Htek IP Phone with Yeastar P-Series Software Edition.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
UC803T	2.0.4.4.33 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC902	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC902S	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC903	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC912	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC912G	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC912E	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC921	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC921G	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 • Provision Link
UC923	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC923U	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC924	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC924E	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC924U	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC924W	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC926	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC926E	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UC926U	2.0.4.8.18 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
UCV10	5.42.1.6.30b58 or later	83.12.0.23 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
UCV20	5.42.1.6.30b79 or later	83.12.0.23 or later	• PnP • DHCP • RPS • Provision Link
UCV50	5.42.1.6.30b62 or later	83.12.0.23 or later	• PnP • DHCP • RPS • Provision Link
UCV52	5.42.1.6.30b68 or later	83.12.0.23 or later	• PnP • DHCP • RPS • Provision Link
UCV53	5.42.1.6.32R76 or later	83.12.0.23 or later	• PnP • DHCP • RPS • Provision Link

Gigaset phones

Note:
For more information about the auto provisioning configuration, see Auto Provision Gigaset DECT System with Yeastar P-Series Software Edition.

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 • Provision Link
N870 VI PRO	2.38.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
N670 IP PRO	2.38.1 or later	83.4.0.17 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
N610 IP PRO	2.52.0 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
Maxwell Basic PRO	3.18.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
Maxwell 2 PRO	3.18.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
Maxwell 3 PRO	3.18.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
Maxwell 4 PRO	3.18.1 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
P820 IP PRO	10.1.198.16 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
P850W IP PRO	10.1.198.16 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
P710 IP PRO	10.1.198.16 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link
P810 IP PRO	10.1.198.16 or later	83.19.0.70 or later	• PnP • DHCP • RPS • Provision Link

Snom phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Snom IP Phone with Yeastar P-Series Software Edition.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Snom IP Phone with Yeastar P-Series Software Edition.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
D120	10.1.54.13 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D140	10.1.148.1 or later	83.12.0.33 or later	• PnP • DHCP • RPS • Provision Link
D150	10.1.148.1 or later	83.12.0.33 or later	• PnP • DHCP • RPS • Provision Link
D315	10.1.73.16 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D335	10.1.73.16 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D385	10.1.73.16 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D710	8.9.3.80 or later	83.19.0.22 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
D712	8.9.3.61 or later	83.19.0.22 or later	• PnP • DHCP • RPS • Provision Link
D713	10.1.73.16 or later	83.6.0.46 or later	• PnP • DHCP • RPS • Provision Link
D715	10.1.33.33 or later	83.19.0.22 or later	• PnP • DHCP • RPS • Provision Link
D717	10.1.73.16 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D720	8.9.3.80 or later	83.19.0.22 or later	• PnP • DHCP • RPS • Provision Link
D725	10.1.175.16 or later	83.19.0.22 or later	• PnP • DHCP • RPS • Provision Link
D735	10.1.73.16 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D785	10.1.73.16 or later	83.4.0.17 or later	• PnP • DHCP • RPS • Provision Link
D812	10.1.184.14 or later	83.12.0.30 or later	• PnP • DHCP • RPS • Provision Link
D815	10.1.184.14 or later	83.12.0.30 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
D862	10.1.137.15 or later	83.9.0.22 or later	• PnP • DHCP • RPS • Provision Link
D865	10.1.137.15 or later	83.9.0.22 or later	• PnP • DHCP • RPS • Provision Link
HD100	1.0.0.3-0 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
HD101	1.0.0.3-0 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
HD300 (HD30L)	1.0.0.7 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
HD350W	1.0.0.3-0 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
HD351W	1.0.0.3-0 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
HM201	1.0.0.3-0 or later	83.14.0.26 or later	• PnP • DHCP • RPS • Provision Link
M100 KLE	1.0.5.7 or later	83.14.0.24 or later	• PnP • DHCP • RPS • Provision Link
M500	1.12.2 or later	83.14.0.24 or later	• PnP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• DHCP • RPS • Provision Link
M300	BSV530B2 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
M400	BSV610B5 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
M900	BSV530B7 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
SP800	10.1.169.15 or later	83.17.0.60 or later	• PnP • DHCP • RPS • Provision Link
PA1+	10.1.184.15 or later	83.17.0.60 or later	• PnP • DHCP • RPS • Provision Link

Flyingvoice phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Flyingvoice IP Phone with Yeastar P-Series Software Edition.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Flyingvoice IP Phone with Yeastar P-Series Software Edition.

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 • Provision Link
FIP11C	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP12WP	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP13G	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP14G	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP15G	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP15G Plus	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP16	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
FIP16 Plus	0.7.23.1 or later	83.8.0.25 or later	• PnP • DHCP • RPS • Provision Link
P10	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
P10P	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P10G	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P10W	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P10LTE	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P11	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P11P	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P11G	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P11W	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P11LTE	V0.7.56 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P20	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
P20P	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P20W	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P20G	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P21	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P21P	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P21W	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
flyphone	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P22P	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P22G	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P23G	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• RPS • Provision Link
P23GW	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
P24G	V0.7.57 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
i86Box_Basic	V0.0.16.1 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
i86Box_Indoor	V0.0.16.1 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
i86Box_2Line	V0.0.16.1 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
i86Box_PCBA	V0.0.16.1 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link
i86Box_NFC	V0.0.16.1 or later	83.9.0.20 or later	• PnP • DHCP • RPS • Provision Link

Alcatel-Lucent Enterprise phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Alcatel-Lucent Enterprise (ALE) IP Phone with Yeastar P-Series Software Edition.

- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Alcatel-Lucent Enterprise (ALE) IP Phone with Yeastar P-Series Software Edition.

Table 9.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
H2	2.10.00.0001083 or later	83.6.0.24 or later	• PnP • DHCP • Provision Link
H2P	2.10.00.0001083 or later	83.6.0.24 or later	• PnP • DHCP • Provision Link
H3P	2.12.43.010.2272 or later	83.5.0.9 or later	• PnP • DHCP • Provision Link
H3G	2.12.43.010.2272 or later	83.5.0.9 or later	• PnP • DHCP • Provision Link
H6	2.12.43.010.2272 or later	83.5.0.9 or later	• PnP • DHCP • Provision Link
M3	2.13.37.000.2202 or later	83.5.0.9 or later	• PnP • DHCP • Provision Link
M3s	2.15.10.000.3000 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
M5	2.13.37.000.2202 or later	83.5.0.9 or later	• PnP • DHCP • Provision Link
M5s	2.15.10.000.3000 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
M7	2.13.37.000.2202 or later	83.5.0.9 or later	• PnP • DHCP • Provision Link

Table 9. (continued)

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
M7s	2.15.10.000.3000 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
M7s-Pro	2.15.10.000.3000 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
M8	2.13.32.000.1535 or later	83.6.0.24 or later	• PnP • DHCP • Provision Link

Tiptel phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Tiptel IP Phone with Yeastar P-Series Software Edition.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Tiptel IP Phone with Yeastar P-Series Software Edition.

Table 10.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
3310	2.42.6.5.55 or later	83.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
3320	2.42.6.5.55 or later	83.7.0.16 or later	• PnP • DHCP • RPS • Provision Link
3330	2.42.6.5.55 or later	83.7.0.16 or later	• PnP • DHCP • RPS • Provision Link

Table 10. (continued)

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
3340	2.42.6.5.55 or later	83.7.0.16 or later	• PnP • DHCP • RPS • Provision Link

Dinstar phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Dinstar IP Phone with Yeastar P-Series Software Edition.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Dinstar IP Phone with Yeastar P-Series Software Edition.

Table 11.

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 • Provision Link
C60L	2.60.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP • Provision Link
C60U	2.60.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP • Provision Link
C61S	2.61.6.7.0/2.61.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP • Provision Link
C62S	2.62.6.7.0/2.62.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP • Provision Link
C62G	2.62.6.7.0/2.62.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP

Table 11. (continued)

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
C63S	2.63.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP • Provision Link
C63G	2.63.6.7.0/2.63.11.7.0 or later	83.6.0.24 or later	• PnP • DHCP • Provision Link
C64G	2.64.6.7.0 or later	83.6.0.24 or later	• PnP • DHCP • Provision Link
C66G	2.66.6.7.0 or later	83.6.0.24 or later	• PnP • DHCP • Provision Link

VTech phones

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
NG-S3211W	3.3.3.16-0 or later	83.13.0.29 or later	• PnP • DHCP • Provision Link
NG-S3311	3.3.3.16-0 or later	83.13.0.29 or later	• PnP • DHCP • Provision Link
NG-S3411W	3.3.3.16-0 or later	83.13.0.29 or later	• PnP • DHCP • Provision Link
S2211-SPK	3.3.3.16-0 or later	83.13.0.29 or later	• PnP • DHCP • Provision Link
S2210-X	3.3.3.16-0 or later	83.13.0.29 or later	• PnP • DHCP • Provision Link
S2411-X	3.3.3.16-0 or later	83.13.0.29 or later	• PnP • DHCP • Provision Link

Mitel phones

Note:

- For more information about the auto provisioning configuration, see Auto Provision Mitel IP Phone with Yeastar P-Series Software Edition.
- For phone models that are not in the list, you can manually register the IP phone with PBX. For more information, see Manually Register Mitel IP Phone with Yeastar P-Series Software Edition.

Table 12.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
6863i	R5.1.0SP6 or later	83.9.0.103 or later	• DHCP • Provision Link
6865i	R5.1.0SP6 or later	83.9.0.103 or later	• DHCP • Provision Link
6867i	R5.1.0SP6 or later	83.9.0.103 or later	• DHCP • Provision Link
6869i	R5.1.0SP6 or later	83.9.0.103 or later	• DHCP • Provision Link
6873i	R5.1.0SP6 or later	83.9.0.103 or later	• DHCP • Provision Link
6905	6.3 SP3 or later	83.17.0.17 or later	• DHCP • Provision Link
6910	6.3 SP3 or later	83.17.0.17 or later	• DHCP • Provision Link
6915	6.3 SP3 or later	83.17.0.17 or later	• DHCP • Provision Link
6920	6.3.1 SP1 or later	83.9.0.103 or later	• DHCP • Provision Link
6930	6.3.1 SP1 or later	83.9.0.103 or later	• DHCP • Provision Link
6940	6.3.1 SP1 or later	83.9.0.103 or later	• DHCP • Provision Link
RFP 44	9.1 or later	83.18.0.18 or later	• DHCP

Table 12. (continued)

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
RFP 45	9.1 or later	83.18.0.18 or later	• DHCP • Provision Link
RFP 47	9.1 or later	83.18.0.18 or later	• DHCP • Provision Link
RFP 48	9.1 or later	83.18.0.18 or later	• DHCP • Provision Link

Cisco phones

Note:
For more information about the auto provisioning configuration, see Auto Provision Cisco IP Phone with Yeastar P-Series Software Edition.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
3905	9.4(1)SR3 or later	83.12.0.23 or later	• DHCP
7821	14.2(1)SR1 or later	83.12.0.23 or later	• DHCP
7861	SIP78xx.14-2-1-0201-40 or later	83.13.0.29 or later	• DHCP
7911	SIP11.9-2-1S or later	83.17.0.17 or later	• DHCP
7942	SIP42.9-4-2SR3-1S or later	83.12.0.23 or later	• DHCP
7975	SIP75.9-3-1SR4-1S or later	83.17.0.17 or later	• DHCP
8811	SIP88xx.12-1-1SR1-4 or later	83.13.0.29 or later	• DHCP
8845	14.2(1)SR1 or later	83.12.0.23 or later	• DHCP
SPA501G	7.4.7 or later	83.19.0.22 or later	• DHCP
SPA502G	7.4.7 or later	83.19.0.22 or later	• DHCP
SPA504G	7.4.7 or later	83.19.0.22 or later	• DHCP
SPA508G	7.4.7 or later	83.19.0.22 or later	• DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
SPA509G	7.4.7 or later	83.19.0.22 or later	• DHCP
SPA512G	7.4.7 or later	83.19.0.22 or later	• DHCP
SPA514G	7.4.7 or later	83.19.0.22 or later	• DHCP
SPA301	7.4.7 or later	83.19.0.22 or later	• DHCP
SPA303	7.4.7 or later	83.19.0.22 or later	• DHCP
SPA525G2	7.4.7 or later	83.19.0.22 or later	• DHCP

Avaya phones

Note:
For more information about the auto provisioning configuration, see Auto Provision Avaya IP Phone with Yeastar P-Series Software Edition.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
J129	4.1.1.0.7 or later	83.12.0.23 or later	• DHCP • Provision Link
J139	4.1.1.0.7 or later	83.12.0.23 or later	• DHCP • Provision Link
J159	4.1.1.0.7 or later	83.12.0.23 or later	• DHCP • Provision Link
J169	4.1.1.0.7 or later	83.12.0.23 or later	• DHCP • Provision Link
J179	4.1.1.0.7 or later	83.12.0.23 or later	• DHCP • Provision Link
J189	4.1.1.0.7 or later	83.12.0.23 or later	• DHCP • Provision Link
9608	7.1.15.2.1 or later	83.14.0.26 or later	• DHCP • Provision Link

Poly phones

Note:

For more information about the auto provisioning configuration, see Auto Provision Poly IP Phone with Yeastar P-Series Software Edition.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
Edge_E100	8.0.0.15602 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E220	8.0.0.15602 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E300	8.0.0.15602 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E320	8.0.0.15602 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E350	8.0.0.15602 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E400	8.0.0.15602 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E450	8.0.0.15602 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E500	8.0.0.15602 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
Edge_E550	8.0.0.15602 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_101	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_201	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_301	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
VVX_310	5.9.8 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_311	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_401	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_410	5.9.8 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_411	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_501	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_601	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_150	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_250	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_350	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link
VVX_450	6.4.3.5059 or later	83.15.0.22 or later	• DHCP • RPS • Provision Link

Wildix phones

Note:

For more information about the auto provisioning configuration, see Auto Provision Wildix IP Phone with Yeastar P-Series Software Edition.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
WP410R2	50.145.6.169 or later	83.15.0.22 or later	• DHCP • Provision Link
WP480R2	55.145.6.111 or later	83.15.0.22 or later	• DHCP • Provision Link
WP480R3	63.145.10.168 or later	83.15.0.22 or later	• DHCP • Provision Link
WP480R4	65.145.6.38 or later	83.15.0.22 or later	• DHCP • Provision Link
WP490R2	59.145.6.148 or later	83.15.0.22 or later	• DHCP • Provision Link
WP490R3	67.145.8.107 or later	83.15.0.22 or later	• DHCP • Provision Link

Xenios phones

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
ICD012	23.12.20 or later	83.14.0.24 or later	• DHCP • Provision Link

Huawei phones

Note:
For more information about the auto provisioning configuration, see Auto Provision Huawei IP Phone with Yeastar P-Series Software Edition.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
eSpace 7910	V200R003C30SPCf00 or later	83.16.0.25 or later	• DHCP • Provision Link
eSpace 7950	V200R003C00SPCs00 or later	83.16.0.25 or later	• DHCP • Provision Link

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
IP Phone 7920	V600R019C10SPC200 or later	83.16.0.25 or later	• DHCP • Provision Link
IP Phone 7960	V600R019C10SPC202 or later	83.16.0.25 or later	• DHCP • Provision Link
eSpace 8950	V200R003C00SPCg00B015 or later	83.16.0.25 or later	• DHCP • Provision Link
eSpace 8950HK	V200R003C30SPCh20 or later	83.17.0.17 or later	• DHCP • Provision Link

NEC phones

Note:

- By default, DT700 series models are not displayed in the drop-down list. In case of need, contact Yeastar Support.
- For more information about the auto provisioning configuration, see Auto Provision NEC IP Phone with Yeastar P-Series Software Edition.

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
DT700 ITL-2E-1P	03.01.64.00 or later	83.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-6DE-1P	03.01.64.00 or later	83.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-12D-1P	03.01.64.00 or later	83.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-24D-1P	03.01.64.00 or later	83.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-8LD-1P	03.01.64.00 or later	83.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-8LDE-1P	03.01.64.00 or later	83.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-12DG-3P	03.01.64.00 or later	83.17.0.53 or later	• DHCP • Provision Link
DT700 ITL-12CG-3P	03.01.64.00 or later	83.17.0.53 or later	• DHCP

Model	Phone Requirement	PBX Requirement	Supported Auto Provisioning Method
			• Provision Link
DT820 ITY-6D-1P	04.04.28.14 or later	83.17.0.53 or later	• DHCP • Provision Link
DT820 ITY-8LDX-1P	04.04.28.14 or later	83.17.0.53 or later	• DHCP • Provision Link
DT820 ITY-8LCGX-1P	04.04.28.14 or later	83.17.0.53 or later	• DHCP • Provision Link
DT820 ITY-6DG-1P	04.04.28.14 or later	83.17.0.53 or later	• DHCP • Provision Link
DT820 ITY-32LDG-1P	04.04.28.14 or later	83.17.0.53 or later	• DHCP • Provision Link
DT820 ITY-32LCG-1P	04.04.28.14 or later	83.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-6D-1P	05.03.04.99 or later	83.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-12D-1P	05.03.04.03 or later	83.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-8LCX-1P	05.03.04.99 or later	83.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-8TCGX-1P	05.03.04.99 or later	83.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-6DG-1P	05.03.04.99 or later	83.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-12DG-1P	05.03.04.99 or later	83.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-32LCG-1P	05.03.04.99 or later	83.17.0.53 or later	• DHCP • Provision Link
DT900 ITK-32TCG-1P	05.03.04.99 or later	83.17.0.53 or later	• DHCP • Provision Link
DT900S ITK-6DGS-1P	05.03.04.99 or later	83.17.0.53 or later	• DHCP • Provision Link
DT900S ITK-32LCGS-1P	05.03.04.99 or later	83.17.0.53 or later	• DHCP • Provision Link
DT900S ITK-32TCGS-1P	05.03.04.99 or later	83.17.0.53 or later	• DHCP • Provision Link

Yeastar gateways

Note:
For more information about the auto provisioning configuration, see Auto Provision Yeastar TA FXS Gateways (PnP Method), Auto Provision Yeastar TA FXS Gateways (DHCP Method), Auto Provision Yeastar TA FXS Gateway (Provision Link Method), and Auto Provision Yeastar TA FXS Gateway (Provision Link FQDN Method).

Model	Gateway Requirement	PBX Requirement	Supported Auto Provisioning Method
TA100	44.19.86.30 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
TA200	44.19.86.30 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
TA400	41.19.0.32 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
TA800	41.19.0.32 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
TA1600	47.0.0.54 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
TA2400	47.0.0.54 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link
TA3200	47.0.0.54 or later	83.18.0.18 or later	• PnP • DHCP • Provision Link

Auto Provisioning - Variables in Templates

The provisioning templates make use of a set of variables that are replaced by the actual value when a device is provisioned. This topic shows you the variables used in the provisioning templates.

Variable	Description
Preference settings	
{{.PhoneWebLanguage}}	The language configured on phone web interface.
{{.PhoneLanguage}}	The language configured on phone interface.
{{.Tones}}	The default ringtone of the phone.
{{.CallWaiting}}	Enable or disable call waiting feature.
{{.PhoneUser}}	The user name for admin account to log in to the phone web interface.
{{.PhonePassword}}	The password for admin account to log in to the phone web interface.
{{.VarPassword}}	The password for var account to log in to the phone web interface.
{{.UserPassword}}	The password for user account to log in to the phone web interface.
{{.TimeZone}}	The time zone.
{{.TimeZoneName}}	The time zone name.
{{.DaylightSavingTime}}	The daylight saving time.
{{.PrimaryNtpServer}}	The primary NTP server address.
{{.SecondaryNtpServer}}	The second NTP server address.
{{.TimeFormat}}	The time format.
{{.DateFormat}}	The date format.
{{.DateSeparatorFormat}}	The date separator format.
{{.TransferModeViaDsskey}}	The transfer mode for function key.
{{.SuppressDtmfDisplay}}	Enable or disable the IP phone to suppress the display of DTMF digits.
{{.AutoProvisionServerUrl}}	The URL of provision server.
{{.AutoProvisionServerUrlWithoutProtocol}}	The URL of provision server without transport protocol.
{{.AutoProvisionServerProtocolUppercase}}	The uppercase representation of the transport protocol in the auto provisioning URL.
{{.AutoProvisionServerProtocolLowercase}}	The lowercase representation of the transport protocol in the auto provisioning URL.
{{.ProvisioningFile}}	The name of configuration file.
{{.FirmwareUrl}}	The URL of firmware.

Variable	Description
{{.FirmwareUrlWithoutProtocol}}	The URL of firmware without transport protocol.
{{.FirmwareFile}}	The name of firmware.
{{.FirmwareFullDownloadUrl}}	The full download URL of firmware.
{{.FirmwareVersion}}	The version of firmware.
{{.EnableUacsta}}	Enable or disable uaCSTA.
{{.AlertInfoText_X}}	The alert info text to trigger the IP phone to play a specific ring tone.
{{.AlertInfoRingtone_X}}	The specific ring tone corresponding to Alert info.
{{.WallpaperImageServerUrl}}	The URL of the wallpaper image for the phone.
{{.WallpaperFileName}}	The file name of the wallpaper image for the phone.
{{.ScreenSaverImageServerUrl}}	The URL of the ScreenSaver image for the phone.
{{.ScreensaverFileName}}	The file name of the ScreenSaver image for the phone.
{{.BootLogoImageServerUrl}}	The URL of the boot logo image for the phone.
{{.BootLogoFileName}}	The file name of the boot logo image for the phone.
VLAN settings for phones	
{{.WanVlanEnable}}	Enable or disable VLAN for the WAN port of the phone.
{{.WanVlanId}}	The VLAN ID for the WAN port of the phone.
{{.WanVlanPriority}}	The VLAN priority for the WAN port of the phone.
{{.PcVlanEnable}}	Enable or disable VLAN for the PC port of the phone.
{{.PcVlanId}}	The VLAN ID for the PC port of the phone.
{{.PcVlanPriority}}	The VLAN priority for the PC port of the phone.
{{.DhcpVlanEnable}}	Enable or disable acquiring the VLAN ID through DHCP option.
{{.DhcpVlanOption}}	The DHCP option(s) from which the phone will obtain the VLAN ID. **Note:** Use a comma to separate multiple DHCP options.
Contact settings for Yealink / Flyingvoice / Wildix/ Dinstar phones	
{{.CompanyPbUrl}}	The URL of company contact file.
{{.CompanyPbName}}	The name of company contact.

Variable	Description
{{.PersonalPbUrl}}	The URL of personal contact file.
{{.PersonalPbName}}	The name of personal contact.
Account settings for IP phones	
{{.EnbAccount}}	Enable or disable extension registration.
{{.AccountLabel}}	The extension label.
{{.AccountDisplayName}}	The display name of extension.
{{.AccountRegistrationName}}	The registration name of extension.
{{.AccountRegistrationExtNumber}}	The registration number of extension.
{{.AccountRegistrationPassword}}	The registration password of extension.
{{.AccountSipServerAddr}}	The URL of PBX server for extension registration.
{{.AccountSipServerPort}}	The port of PBX server for extension registration.
{{.AccountSipServerTransportType}}	The type of transport protocol for extension registration.
{{.AutoAnswer}}	Enable or disable auto answer feature.
{{.CheckVoicemail}}	The voicemail feature code.
Account settings for DECT phones(x is the handset ID)	
{{.EnbAccount_x}}	Enable or disable extension registration.
{{.SRTP_x}}	Enable or disable extension SRTP feature.
{{.AccountLabel_x}}	The extension label.
{{.AccountDisplayName_x}}	The display name of extension.
{{.AccountRegistrationName_x}}	The registration name of extension.
{{.AccountRegistrationExtNumber_x}}	The registration number of extension.
{{.AccountRegistrationPassword_x}}	The registration password of extension.
{{.AccountSipServerAddr_x}}	The URL of provisioning server for extension registration.
{{.AccountSipServerPort_x}}	The port of provisioning server for extension registration.
{{.AccountSipServerTransportType_x}}	The type of transport protocol for extension registration.
{{.HandsetIPUI_X}}	The IPUI number for extension registration.
{{.CheckVoicemail_x}}	The voicemail feature code.
SIP server template for Yealink W80B(x is the template ID, X=1, 2 or 3)	
{{.TemplateNamex}}	The template name.
{{.TemplateServerAddrx}}	The URL of PBX server for extension registration.
{{.TemplateServerPortx}}	The port of PBX server for extension registration.

Variable	Description
{{.AcountSipServerTemplate}}	The type of transport protocol for extension registration.
{{.HandsetIPUI_X}}	The IPUI number for extension registration.
Audio codec(x is the codec priority, X=1, 2, 3 or 4)	
{{.AccountAudioCodec_X}}	The priority of the audio codec.
{{.AudioCodecsPriorities}}	The priority of the audio codec.
{{.AccountCodecPcmu}}	Enable or disable PCMU audio codec.
{{.AccountCodecPcmu_Priority}}	The priority of the PCMU audio codec.
{{.AccountCodecPcma}}	Enable or disable PCMA audio codec.
{{.AccountCodecPcma_Priority}}	The priority of the PCMA audio codec.
{{.AccountCodecIlbc}}	Enable or disable iLBC audio codec.
{{.AccountCodecIlbc_Priority}}	The priority of the iLBC audio codec.
{{.AccountCodecIlbc_15_2_Kbps}}	Enable or disable iLBC_15_2 audio codec.
{{.AccountCodecIlbc_15_2_Kbps_Priority}}	The priority of the iLBC_15_2 audio codec.
{{.AccountCodecIlbc_13_33_Kbps}}	Enable or disable iLBC_13_33 audio codec.
{{.AccountCodecIlbc_13_33_Kbps_Priority}}	The priority of the iLBC_13_33 audio codec.
{{.AccountCodecG722}}	Enable or disable G722 audio codec.
{{.AccountCodecG722_Priority}}	The priority of the G722 audio codec.
{{.AccountCodecG729}}	Enable or disable G729 audio codec.
{{.AccountCodecG729_Priority}}	The priority of the G729 audio codec.
{{.AccountCodecG726_32}}	Enable or disable G726_32 audio codec.
{{.AccountCodecG726_32_Priority}}	The priority of the G726_32 audio codec.
{{.AccountCodecSpeex}}	Enable or disable Speex audio codec.
{{.AccountCodecSpeex_Priority}}	The priority of the Speex audio codec.
{{.AccountAdpcmCodec}}	Enable or disable Adpcm audio codec.
{{.AccountCodecAdpcm_Priority}}	The priority of the Adpcm audio codec.
{{.AccountCodecMpeg4}}	Enable or disable Mpeg4 audio codec.
{{.AccountCodecMpeg4_Priority}}	The priority of the Mpeg4 audio codec.
{{.AccountCodecGsm}}	Enable or disable GSM audio codec.
{{.AccountCodecGsm_Priority}}	The priority of the GSM audio codec.

Variable	Description
{{.AccountCodecOpus}}	Enable or disable Opus audio codec.
{{.AccountCodecOpus_Priority}}	The priority of the Opus audio codec.
Video codec(x is the codec priority, X=1, 2, 3 or 4)	
{{.AccountVideoCodec_X}}	The priority of the video codec.
{{.AccountCodecH264}}	Enable or disable H264 codec.
{{.AccountCodecH264_Priority}}	The priority of the H264 codec.
{{.AccountCodecH264_Hp}}	Enable or disable H264_Hp codec.
{{.AccountCodecH264_Hp_Priority}}	The priority of the H264_Hp codec.
{{.AccountCodecH263}}	Enable or disable H263 codec.
{{.AccountCodecH263_Priority}}	The priority of the H263 codec.
{{.AccountCodecH263_P}}	Enable or disable H263_P codec.
{{.AccountCodecH263_P_Priority}}	The priority of the H263_P codec.
{{.AccountCodecVp8}}	Enable or disable Vp8 codec.
{{.AccountCodecVp8_Priority}}	The priority of the Vp8 codec.
Function key (x is the function key ID)	
{{.FunctionkeyType_x}}	The type of function key.
{{.FunctionkeyType2_x}}	The type of function key (for Dynamic VPK).
{{.FunctionkeySubtype_x}}	The subtype of function key.
{{.FunctionkeyLine_x}}	The extension to which function key applies.
{{.FunctionkeyCodeValue_x}}	The feature code of function key.
{{.FunctionkeyValue_x}}	The object of function key.
{{.FunctionkeyExtension_x}}	The number where the call can be picked up by function key.
{{.FunctionkeyCodeExtension_x}}	The pickup code applied for function key.
{{.FunctionkeyLabel_x}}	The label of function key that is displayed on phone screen.
LDAP Directory (x is the template ID, X=1, 2 or 3)	
{{.EnableLdap_X}}	Enable LDAP directory.
{{.LdapName_X}}	Specify the name of LDAP directory.
{{.LdapMode_X}}	Set up the LDAP mode.
{{.LdapHost_X}}	The address of LDAP Server.

Variable	Description
{{.LdapNameFilter_X}}	The LDAP name filter.
{{.LdapNumFilter_X}}	The LDAP number filter.
{{.LdapNameAttr_X}}	The name attribute returned by LDAP Server.
{{.LdapNumAttr_X}}	The number attribute returned by LDAP Server.
{{.LdapDisplayName_X}}	The name of the search results displayed on IP phones.
{{.LdapMaxHit_X}}	The maximum number of search results to be returned by LDAP Server.
{{.LdapIncomingLookup_X}}	Enable or disable IP phone to perform an LDAP search when receiving an incoming call.
{{.LdapDialLookup_X}}	Enable or disable IP phone to perform an LDAP search when placing a call.
{{.LdapSort_X}}	Enable or disable IP phone to sort out search results in alphabetical and numerical order.
{{.LdapPort_X}}	The port of LDAP Server.
{{.LdapBase_X}}	The base entry of the LDAP directory.
{{.LdapUser_X}}	The user accessing the LDAP Server.
{{.LdapPassword_X}}	The password for accessing to the LDAP Server.
Gateway	
{{.KeyAsSend}}	Enable or disable Key as Send feature.
{{.SipVoipServerIdx}}	The VoIP server template ID.
{{.AdminPassword}}	The admin password.
{{.EnbLanSettings}}	Enable or disable LAN settings.
{{.Hostname}}	The host name.
{{.LanIpAddress}}	The primary IP address of LAN port.
{{.LanSubnetMask}}	The subnet mask of LAN port.
{{.LanGateway}}	The gateway of LAN Port.
{{.LanPrimaryDns}}	The primary DNS of LAN port.
{{.LanSecondaryDns}}	The secondary DNS of LAN Port.
{{.LanIpAddress2}}	The secondary IP address of LAN port.
{{.LanSubnetMask2}}	The secondary subnet mask of LAN port.
{{.PppoeUsername}}	The user name of PPPoE.
{{.PppoePassword}}	The password of PPPoE.

Variable	Description
Others	
{{.MacAddress}}	The MAC address of phone. **Note:** Here the value does not need a separator of `:`. For example, `09139876900e`.

User Role

User Roles and Permissions

Yeastar P-Series 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:

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.

Role	Permission
Employee	No access to PBX features.
Human Resource	View and manage all the extensions.
Accounting	Access and manage **Plan**.
Hotel Manager	Access and manage the following features: • **Hotel Settings** • **Room Management** • **Wake-up Service**

Related information

Create a User Role
Assign a Role to a User

Create a User Role

If the pre-defined roles can not meet your need, you can create a user role and grant permissions to the role. This topic describes how to create a user role.

Restrictions

Note:
Only system super administrator can create a user role.

Create a new role

Based on an employee's job duty, you can create a user role and grant corresponding permissions.

1. Log in to PBX web portal, go to **Extension and Trunk > Role**.
2. Click **Add** to create a new role.
3. In the **Role Name** field, enter a name to help you identify it.
4. Grant permissions to the user role.

   For permission details, see User Role Permissions.
5. Click **Save**.

Create a role by copying an existing role

You can create a role based on an existing user role, the new role automatically inherits permissions from the existing role. After copying permissions, you can add or remove permissions as needed.

1. Log in to PBX web portal, go to **Extension and Trunk > Role**.
2. Create a role.
    a. Click **Copy Role**.
    b. In the **Choose a role to copy** drop-down list, select a role.
    c. In the **Role Name** field, enter a name to help you identify the role.
    d. Click **Save**.

    The new role inherits permissions from the existing role.
3. Update permissions for the newly created role.
    a. On **Role** list, click  beside the role that you have created.
    b. Select or unselect the checkboxes of the desired permissions.

    For permission details, see User Role Permissions.
    c. Click **Save**.

What to do next

Assign a Role to a User.

Assign a Role to a User

This topic describes how to assign a role to a user.

Restrictions

> **Note:**
> Only system super administrator can assign a role to a user.

Prerequisites

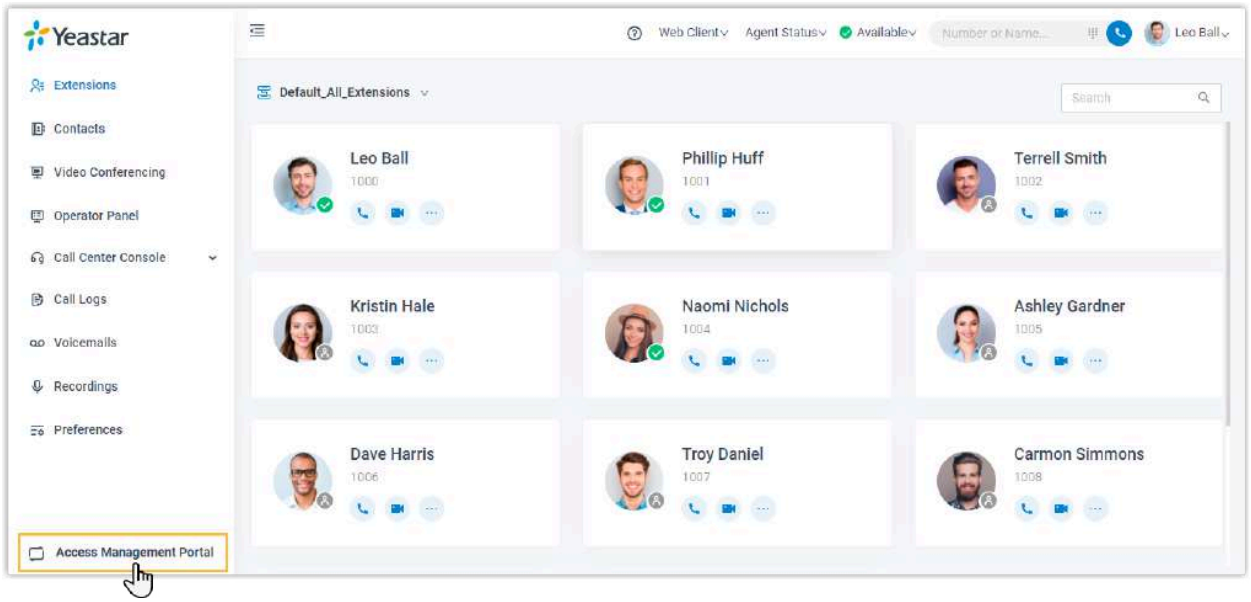
A user role is created.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. On **Extension** list, select an extension, click .
3. On the **User** page, select a role from the drop-down list of **User Role**.
4. Click **Save** and **Apply**.

Result

If specific permissions are granted to the role, after the user logs in to Linkus Web Client, the user can go to management portal, and access specific system features.



Manage User Roles

This topic describes how to edit or delete roles.

Restrictions

Note:
Only system super administrator can manage user roles.

Edit a role

After creating a role, you can edit role permissions according to your needs.

1. Log in to PBX web portal, go to **Extension and Trunk > Role**.
2. On **Role** list, select a role, click .
3. Edit the role name or change role permissions according to your needs.

   For permission details, see User Role Permissions.
4. Click **Save**.

Delete roles

If you don't need roles, you can delete them. After roles are deleted, users with the roles assigned will have no role definition.

1. Log in to PBX web portal, go to **Extension and Trunk > Role**.
2. Delete one or more roles according to your needs.
   - To delete a role, select a role, click and **OK**.
   - To delete roles in bulk, select the checkboxes of the desired roles, click **Delete** and **OK**.

User Role Permissions

This topic describes all the available permissions that can be granted to a role.

Available permissions on Yeastar P-Series Software Edition are as follows:

- Extension and Trunk
- Contacts
- Call Control
- Call Features
- Reports and Recordings
- Auto Provisioning
- Campaign Management
- Messaging
- PBX Settings
- Hotel Management
- System

- Security
- Maintenance
- Integration
- Plan

Extension and Trunk

Specify the extensions that users with the role assigned can manage, and whether users can manage extension group or trunks.

Module	Permission	
Extension	**Manage Extensions**	• **All Departments**: View and manage all the departments.
		• **All Extensions**: View and manage all the extensions. For example, grant the permission to a human resource. If there are changes of employees, the human resource can update extensions timely. • **All the other extensions of the same Extension Groups**: Manage or send Linkus welcome emails to all the other extensions in the same extension group except the one that contains all the extensions. For example, grant the permission to a supervisor. The supervisor can view and manage his or her subordinates' extensions. • **All other extensions of the same department**: Manage or send Linkus welcome emails to all the other extensions in the same department, excluding those in the associated sub-departments. • **Specific Extensions**: Manage or send Linkus welcome emails to specific extensions. For example, grant the permission to a leader. The leader can view and manage different departments' extensions. • **Extension itself only**: Manage or send Linkus welcome emails to his or her own extension.
	Manage Extension Operation Permission	Specify whether users with the role assigned can view and manage Linkus Client related settings of extensions. • **Linkus Clients**: Set whether users can view the **Linkus Clients** feature tab.

Module	Permission
	◦ **Linkus Mobile Client**: Set whether users can view and manage settings for Linkus Mobile Client. ◦ **Linkus Pad Client (SDK)**: Set whether users can view and manage Linkus SDK. **Note:** This option is available only when Linkus SDK (Path: **Integration > Linkus SDK**) is enabled. ◦ **Linkus Desktop Client**: Set whether users can view and manage settings for Linkus Desktop Client. ◦ **Linkus Web Client**: Set whether users can view and manage settings for Linkus Web Client.
Extension Group	Manage extension groups.
Client Permission	Manage users' permissions to view or manage specific extensions/contacts.
Trunks	Manage trunks.

Contacts

Specify whether users with the role assigned can manage the following features:

- **Company Contacts**
- **PhoneBooks**

- **LDAP Server**

Call Control

Specify whether users with the role assigned can manage the following features:

- **Inbound Route**
- **Outbound Route**
- **AutoCLIP Route**
- **Business Hours and Holidays**
- **Emergency Number**

- **Allow to edit Emergency Outbound Caller ID in Management Portal > Extension**: Specify whether users with the role assigned can configure emergency outbound caller ID for extensions (Path: **Management Portal > Extension and Trunk > Extension > User > Outbound Caller ID (DOD) > Emergency Outbound Caller ID**), which changes the number displayed to the called party when the extension users make an emergency call.

  > **Note:**
  > To specify whether the extension users can edit the emergency outbound caller ID on their own Linkus clients, go to **Management Portal > Client Permissions > Preference Settings**.

Call Features

Specify whether users with the role assigned can manage the following features:

- **Voicemail**
- **Feature Code**
- **IVR**
- **Ring Group**
- **Queue**
- **Conference**
- **Speed Dial**
- **Paging/Intercom**
- **Recording**
- **PIN List**
- **Call Disposition**
- **Blocked/Allowed Numbers**

Reports and Recordings

Specify users with the role assigned can view or manage which extensions' CDR and recordings, and whether users can access call reports and external chat logs.

Module	Permission
CDR	Specify users with the role assigned can view which extensions' CDR. • **All Extensions**: View all extensions' CDR.

Module	Permission	
	• **All the other extensions of the same Extension Groups**: View CDR of all the other extensions of the same group except the one that contains all the extensions. • **All other extensions of the same department**: View CDR of all the other extensions in the same department, excluding those in the associated sub-departments. • **Specific Extensions**: View CDR of specific extensions.	
	Specify how users with the role assigned can manage CDR. • **Download** • **Delete** • **Schedule Download**	
Recording Files	Specify users with the role assigned can view which extensions' recordings. • **All Extensions**: View all extensions' recordings. • **All the other extensions of the same Extension Groups**: View recordings of all the other extensions of the same group except the one that contains all the extensions. • **All other extensions of the same department**: View recordings of all the other extensions in the same department, excluding those in the associated sub-departments. • **Specific Extensions**: View recordings of specific extensions	
	Specify how users with the role assigned can manage recording files. • **Play** • **Download** • **Delete**	
Call Reports	**Call Report Operation Permission**	Specify how users with the role assigned can manage call reports. • **Download** • **Schedule Download** • **Rate**
	Call Report Data Permission	Specify users with the role assigned can view which call reports and the data scope. • **Queue Call Reports** • **Extension Call Reports** • **Other Call Reports**

Module	Permission
External Chat Logs	Specify whether users with the role assigned can access external chat logs.

Auto Provisioning

Specify whether users with the role assigned can manage **Auto Provisioning**.

Campaign Management

Specify whether users with the role assigned can manage **Campaign Management**.

Messaging

Specify whether users with the role assigned can manage the following features:

- **Message Channel**
- **Message Queue**

PBX Settings

Specify whether users with the role assigned can manage the following features:

- **Preferences**
- **Voice Prompt**
- **SIP Settings**
- **Jitter Buffer**

Hotel Management

Specify whether users with the role assigned can manage the following features:

- **Hotel Settings**
- **Room Management**
- **Wake-up Service**

System

Specify whether users with the role assigned can manage the following features:

- **Network**
- **Date and Time**
- **Email**

- **Storage**
- **Archive**
- **Event Notification**
- **Remote Management**

- **SNMP**

- **High Availability**
- **SD-WAN PBX Networking**

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:

- **Collaboration**
- **CRM**
- **Helpdesk**
- **PMS**
- **Speech to Text**
- **AMI**

- **API**
- **Database Grant**
- **Linkus SDK**

Plan

Specify whether users with the role assigned can buy or enable free trial of Yeastar-provided plan/add-on service.

Operator Panel

Manage Operator Panel

This topic describes instructions on setting up Operator Panel for extension user.

What is Operator Panel

Yeastar provides an embedded Operator Panel on Linkus Web Client and Desktop Client for call management. It is designed for employee who needs to manage and transfer a large number of calls, such as receptionist or agent manager.

> **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	√	√	√

Permission	Extension Group Manager	Extension Group User	Custom role of Extension Group
Call distribution management (Redirect, Transfer, Drag and Drop operation)	√	√	√
Pick up or hang up other extensions' calls	√	√	√
Call monitoring operations (Listen, Whisper, Barge-in)	√	√	√
Call parking operations (Park, Retrieve)	√	√	√
Route calls directly from IVR regardless of the IVR menu	√	√	√
Switch Business Hours and Holidays status	√	×	√
Switch 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
- Create a SIP Account Trunk

SIP Trunk status

Status	Description
	Disabled.
	Unreachable.
	Registration failed. • Authentication failed. • Transport type inconsistent. • Rejected.
	Registering.
	Registered.
	Unmonitored.

Status	Description
	Busy. Maximum channels reached.

Related information

WebRTC Trunk Overview

Create a SIP Trunk

Create a SIP Trunk from a Template

Yeastar has tested leading ITSP across the globe and provides configuration templates for the tested and certificated ITSP. If a template is provided for your ITSP on the PBX, you can quickly create a SIP Trunk by the template.

Prerequisites

- Check if your ITSP is tested and supported by Yeastar from ITSP partner page.
- Your PBX can connect to the ITSP.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Trunk**, click **Add**.
2. In the **Basic** section, configure the following settings:
   - **Name**: Enter a name to help you identify it.
   - **Trunk Status**: Select **Enabled**.
   - **Select ITSP Template**: Select your country.
   - **ITSP**: Select your ITSP.

   The trunk details are displayed automatically in the **Detailed Configuration** section.

   - If the trunk type is displayed as **Register Trunk**, configure the following settings:
     - **Username**: Enter the username provided by the ITSP.
     - **Password**: Enter the password provided by the ITSP.
     - **Authentication Name**: Optional. Authentication name is used for SIP authentication. If the ITSP provides an authentication name, enter the name.
   - If the trunk type is displayed as **Peer Trunk**, leave the settings as default.

3. **Optional:** If you have purchased DID numbers from the ITSP, click **DIDs/DDIs** tab to configure the DID numbers for the trunk.
    a. Click **Add**, then add DID number(s) according to your need.
        • To add a single DID number, do as follows:
            i. In the **Create Method** drop-down list, select **Single DID**.
            ii. Configure the following settings:
            ◦ **DID/DDI**: Enter the provided DID number.
            ◦ **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

            When the DID number is dialed, the name will be displayed on the called party's device.
        • To add a range of DID numbers, do as follows:
            i. In the **Create Method** drop-down list, select **DID Range**.
            ii. Configure the following settings:
            ◦ **DID Range**: Enter the start number and the end number of the DID range.
            ◦ **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

            When the DID number is dialed, the name will be displayed on the called party's device.
    b. Click **Confirm**.

> **Note:**
> For more information of DID configurations, see Configure DID Numbers on a Trunk.

4. Click **Save** and **Apply**.

Result

Go to **Extension and Trunk > Trunk** to check the trunk status on the trunk list page.

If the status shows , the trunk is registered successfully.

For more information of SIP trunk status, see SIP Trunk status.

What to do next

- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see Set up an Inbound Route.
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see Set up an Outbound Route.

Create a SIP Register Trunk

This topic gives a configuration example to describe how to create a general SIP Register Trunk, which can be applied to all kinds of SIP Register Trunk.

Background information

Assume that you have bought a SIP account from the ITSP ABC, and the trunk information is displayed as below.

- **Provider domain**: abc.provider.com
- **Protocol**: SIP
- **Registration Port**: 5060
- **Transport**: UDP
- **Username**: 254258255
- **Authentication name**: 254258255
- **Password**: 05JsOmsIS54SYh

Prerequisites

- You have purchased a SIP account from an ITSP and a username and a password are offered.
- Your PBX can connect to the ITSP.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Trunk**, click **Add**.
2. In the **Basic** section, configure the following settings:
    - **Name**: Enter a name to help you identify it.
    - **Trunk Status**: Select **Enabled**.
    - **Select ITSP Template**: Select **General**.

3. In the **Detailed Configuration** section, select the trunk type and enter the SIP information that is provided by the ITSP.
   - **Trunk Type**: Select **Register Trunk**.
   - **Transport**: Select the transport provided by the ITSP. In this example, select **UDP**.
   - **Hostname/IP**: Enter the domain name or IP address of the ITSP. In this example, enter *abc.provider.com*.
   - **Port**: Enter the provided registration port. In this example, enter *5060*.
   - **Domain**: Enter the domain in SIP URI of a specific header like From, To header. In this example, enter *abc.provider.com*.

     > **Note:**
     > If the domain is not provided by ITSP, enter the same value as **Hostname/IP**.

   - **Username**: Enter the provided user name. In this example, enter *254258255*.
   - **Password**: Enter the provided password. In this example, enter *05JsOmsIS54SYh*.
   - **Authentication Name**: Enter the provided authentication name. In this example, enter *254258255*.

     > **Note:**
     > In most cases, authentication name is the same as the user name.

   - **Enable Outbound Proxy**: Optional. If the trunk is configured to use an outbound proxy server, when users make outbound calls through this trunk, all the SIP packets will be sent to the outbound proxy server.

     > **Note:**
     > Contact your ITSP to check if outbound proxy is supported, then configure outbound proxy settings under the ITSP's guidance.

4. **Optional:** If you have purchased DID numbers from the ITSP, click **DIDs/DDIs** tab to configure the DID numbers for the trunk.
   a. Click **Add**, then add DID number(s) according to your need.
      - To add a single DID number, do as follows:
        i. In the **Create Method** drop-down list, select **Single DID**.
        ii. Configure the following settings:
        - **DID/DDI**: Enter the provided DID number.

- **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

  When the DID number is dialed, the name will be displayed on the called party's device.

- To add a range of DID numbers, do as follows:
  i. In the **Create Method** drop-down list, select **DID Range**.
  ii. Configure the following settings:
  - **DID Range**: Enter the start number and the end number of the DID range.
  - **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

    When the DID number is dialed, the name will be displayed on the called party's device.

b. Click **Confirm**.

> **Note:**
> For more information of DID configurations, see Configure DID Numbers on a Trunk.

5. **Optional:** Click **Advanced**, **Inbound Caller ID Reformatting**, **Outbound Caller ID**, or **SIP Headers** tab to configure other settings.
6. Click **Save** and **Apply**.

Result

Go to **Extension and Trunk > Trunk** to check the trunk status on the trunk list page.

If the status shows , the trunk is registered successfully.

For more information of SIP trunk status, see SIP Trunk status.

What to do next

- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see Set up an Inbound Route.
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see Set up an Outbound Route.

Create a SIP Peer Trunk

This topic gives a configuration example to describe how to create a general SIP Peer Trunk, which can be applied to all kinds of SIP Peer Trunk.

Background information

Assume that you have bought a SIP account from the ITSP ABC, and the trunk information is displayed as below.

- **Provider domain**: abc.provider.com
- **Protocol**: SIP
- **Registration Port**: 5060
- **Transport**: UDP

Prerequisites

- You have purchased a SIP account from an ITSP and no username and password is offered but only a domain name or IP address.
- Your PBX can connect to the ITSP.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Trunk**, click **Add**.
2. In the **Basic** section, configure the following settings:
    - **Name**: Enter a name to help you identify it.
    - **Trunk Status**: Select **Enabled**.
    - **Select ITSP Template**: Select **General**.
3. In the **Detailed Configuration** section, select the trunk type and enter the SIP information that is provided by the ITSP.
    - **Trunk Type**: Select **Peer Trunk**.
    - **Transport**: Select the transport provided by the ITSP. In this scenario, select **UDP**.
    - **Hostname/IP**: Enter the domain name or IP address of the ITSP. In this scenario, enter *abc.provider.com*.
    - **Port**: Enter the provided registration port. In this scenario, enter *5060*.
    - **Domain**: Enter the domain in SIP URI of a specific header like From, To header. In this example, enter *abc.provider.com*.

> **Note:**
> If the domain is not provided by ITSP, enter the same value as **Host-name/IP**.

- **Availability under Disaster Recovery**: Set the availability of the trunk.

> **Note:**
> This option is displayed only when Disaster Recovery is enabled on the PBX.

  - **Only available for Working Server**: The trunk can only be used for the Working Server. When the Working Server goes down and the Redundancy Server takes over, calls won't be routed through this trunk.
  - **Only available for Redundancy Server**: The trunk can only be used for the Redundancy Server. When the Working Server is in function, calls won't be routed through this trunk.
  - **Both**: The trunk can be used for both Working Server and Redundancy Server, and calls can always be routed through this trunk.

4. **Optional:** If you have purchased DID numbers from the ITSP, click **DIDs/DDIs** tab to configure the DID numbers for the trunk.
   a. Click **Add**, then add DID number(s) according to your need.
      - To add a single DID number, do as follows:
        i. In the **Create Method** drop-down list, select **Single DID**.
        ii. Configure the following settings:
          - **DID/DDI**: Enter the provided DID number.
          - **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

            When the DID number is dialed, the name will be displayed on the called party's device.
      - To add a range of DID numbers, do as follows:
        i. In the **Create Method** drop-down list, select **DID Range**.
        ii. Configure the following settings:
          - **DID Range**: Enter the start number and the end number of the DID range.
          - **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

When the DID number is dialed, the name will be displayed on the called party's device.

b. Click **Confirm**.

> **Note:**
> For more information of DID configurations, see Configure DID Numbers on a Trunk.

5. Click **Save** and **Apply**.

Result

Go to **Extension and Trunk > Trunk** to check the trunk status on the trunk list page.

If the status shows , the trunk is registered successfully.

For more information of SIP trunk status, see SIP Trunk status.

What to do next

- To receive inbound calls through the trunk, you need to select this trunk to one or more inbound routes. For more information, see Set up an Inbound Route.
- To make outbound calls through the trunk, you need to select this trunk to one or more outbound routes. For more information, see Set up an Outbound Route.

Create a SIP Account Trunk

A SIP Account is used for the other device to register with Yeastar P-Series 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, configure the following settings:

> **Note:**
> You can leave the default SIP information or edit the information according to your needs.

Setting	Description
Trunk Type	Select **Account Trunk**.
Transport	Select a transport. The following options are supported: • **UDP** • **TCP** **Note:** By default, SIP TCP port is disabled. If you select this option, go to **PBX Settings > SIP Settings > General > Basic**, enable **SIP TCP Port**, then reboot the PBX to make it take effect. • **TLS**
Username	Enter a username for the SIP account.
Password	Enter a password for the SIP account.
Authentication Name	Retain the default authentication name or enter a custom one. **Note:** If the device to be connected does NOT support the **Authentication Name** field, select **Use User Name as Account Trunk's Authentication Name**.

4. **Optional:** Click **Advanced**, **Inbound Caller ID Reformatting**, **Outbound Caller ID**, or **SIP Headers** to configure other settings.
5. Click **Save** and **Apply**.

What to do next

- Register the SIP Account Trunk on the third-party software or device. Depending on the network of the third-party software or device, you need to provide different information:

- **Same local network as Yeastar P-Series 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:**

Setting	Description
	If no SIP trunk template is provided for your ITSP, select **General**.
ITSP	Select your ITSP from the list of certified SIP trunk providers.

Detailed Configuration

Setting	Description
Trunk Type	Select a trunk type: • **Register Trunk** • **Peer Trunk** • **Account Trunk**
Register Trunk	
Transport	Select the transport that is provided by the ITSP. **Note:** If you select **TCP**, make sure SIP TCP Port is enabled (Path: **PBX Settings > SIP Settings > General > Basic > SIP TCP Port**.
Hostname/IP	Enter the IP address or the domain of the ITSP.
Port	Enter the SIP port provided by the ITSP.
Domain	Enter the domain in SIP URI of a specific header like From, To header. **Note:** If the domain is not provided by ITSP, enter the same value as **Hostname/IP**.
Username	Enter the username to register to the ITSP.
Password	Enter the password that is associated with the username.
Authentication Name	Enter the authentication name to register to the ITSP.
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.

Setting	Description
	Note: Contact your ITSP to check if they support outbound proxy, then configure outbound proxy settings under their guidance.
SBC Routing	If this option is enabled, all communication messages between the PBX and this trunk will be routed through the SBC. **Note:** • This setting is available only when Yeastar SBC is enabled (Path: **System > Yeastar SBC**). • Only supports UDP and TCP transport.
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**.
SBC Routing	If this option is enabled, all communication messages between the PBX and this trunk will be routed through the SBC. **Note:**

Setting	Description
	• This setting is available only when Yeastar SBC is enabled (Path: **System > Yeastar SBC**). • Only supports UDP and TCP transport.
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
- Trunk Network Interface Binding

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**.

Setting	Description
Qualify	Enable this option to send SIP OPTION packet to SIP device to check if the device is up.
Enable SRTP	Enable or disable SRTP (encrypted RTP) for the trunk.
T.38 Support	Enable or disable T.38 fax for this trunk. Enabling T.38 will add the performance cost. We suggest that you disable T.38.
Inband Progress	This Inband Progress setting applies to the extensions which make calls through this trunk. **Note:** To configure global Inband Progress setting, you need to contact Yeastar support to configure a custom config file. • **Check this option**: PBX will send a 183 Session Progress to the extension when told to indicate ringing and will immediately start sending ringing as audio. • **Uncheck this option**: PBX will send a 180 Ringing to the extension when told to indicate ringing and will NOT send it as audio.
Ignore 183 Message without SDP	This option determines the way PBX handles 183 messages without SDP. • **Check this option**: PBX will not forward 183 messages that don't contain SDP. • **Uncheck this option**: PBX will process all the 183 messages without SDP to those with SDP and forward them.
Forward the 180 (SDP) Message Following the Peer's Format	This option determines whether the PBX will forward a 180 message with SDP, depending on whether the 180 message received from the other party contains SDP. • **Check this option**: PBX will forward a 180 message if the 180 message received from the other party includes SDP. **Note:** This setting does not take effect when Inband Progress is enabled.

Setting	Description
	• **Uncheck this option**: PBX will not forward a 180 message with SDP even if the 180 message received from the other party contains SDP.
Enable RTP Keep-alive	Whether to send an RTP Comfort Noise (CN) frame. This helps to keep the NAT and firewall holes open during a call, so as to ensure the transmission of RTP traffic. **Note:** • This option is only available for register trunk and peer trunk. • When this option is enabled, if the PBX does not send an RTP packet to the trunk within 1 second, an RTP Comfort Noise (CN) frame will be sent.

Call Restriction

Setting	Description
Call Restriction Type	Specify based on which type of calls to restrict the max concurrent call number of this trunk. • **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.

Trunk Network Interface Binding

Specify which network interface the trunk will route through.

Note:

- This feature is only available when Dual mode is selected as the Ethernet mode in basic network settings (Path: **PBX > Network > Basic Settings**), and is available for IPv4 SIP register trunk and SIP peer trunk only.

- If you make the configuration, you need to reboot the PBX system to take effect.

Setting	Description
Follow Static Routes	The trunk's network will route following the static routing rules of the PBX system.
WAN	The trunk's network will route through the WAN interface. **Note:** If you enable Number of WAN Ports in basic network settings (Path: **System > Network > Basic Settings > Basic > Number of WAN Ports**), you can select the specific WAN to associate with.

DIDs/DDIs

Direct Inward Dialling (DID), also called Direct Dial-in (DDI), is a service offered by telephone companies. For more information of DID concepts, see DID Number Overview.

- DID numbers are usually configured on inbound routes to distinguish inbound calls.

  For more information, see Route Inbound Calls based on DID Numbers.
- For more instructions on configuring the DID numbers, see Configure DID Numbers on a Trunk.

Inbound Caller ID Reformatting

When a user calls in the PBX, the trunk provider may send a caller ID that is inconvenient for you to redial directly.

In this case, you can reformat inbound caller ID based on a trunk. The caller ID will be reformatted before it is sent to the called party.

For more information, see Reformat Inbound Caller ID based on a Trunk.

Outbound Caller ID

Outbound caller ID is the phone number or name that is displayed on the called party's device.

You can set up a global outbound caller ID for a trunk or assign caller IDs for extension users.

Note:
By default, each trunk has a default phone number that will be displayed on the called party's device. Outbound Caller ID configuration requires support from the trunk provider. Contact your trunk provider first before you configure Outbound Caller ID, or the settings won't take effect and outbound calls may fail.

If you set the caller ID number, when users make outbound calls through this trunk, the called party will see this caller ID number instead of the calling party's number.

For more information of outbound caller ID configurations, see Customize Outbound Caller IDs for Outbound Calls

SIP Headers

The SIP Headers settings require professional knowledge of SIP protocol. Incorrect configurations may cause calling issues. It is wise to leave the default settings provided on the SIP trunk page. However, for a few fields, you need to change them to suit your situation.

The following settings are included on the **SIP Headers** page.

- Inbound Parameters
- Outbound Parameters
- Other Settings

Inbound Parameters

Parameter	Description
Get Caller ID From	Decide from which header field will the trunk retrieve Caller ID. • **Follow System** The trunk will follow the global Get Caller ID From setting. • **From** • **Contact** • **Remote-Party-ID** • **P-Asserted Identify** • **P-Preferred-Identity**
Get DID From	Different devices or providers may contain DID numbers in different SIP headers. When an inbound call through a SIP trunk reaches the PBX, the PBX needs to retrieve a correct DID number, or the call will fail.

Parameter	Description
	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:

Parameter	Description
From User Part	Define the caller ID that will be used of a SIP From header. For more information, see Options of outbound parameters.
From Display Name Part	Define the caller ID name that will be used of a SIP From header. For more information, see Options of outbound parameters.
From Host Part	**Important:** • This parameter is only available for **Peer Trunks**. • Set the parameter according to the requirements of your SIP trunk provider, otherwise, it may cause call issues. Define the domain or IP address to be used in the **From** field of a SIP INVITE header.

Parameter	Description
	• **Default**: Use the domain or IP address configured in the **Domain** field when creating the Peer Trunk. • **Custom**: Use a custom domain or IP address. You can enter the custom value in the field next to the **Custom** drop-down list.
To Host Part	**Important:** • This parameter is only available for **Peer Trunks**. • Set the parameter according to the requirements of your SIP trunk provider, otherwise, it may cause call issues. Define the domain or IP address to be used in the **To** field of a SIP INVITE header. • **Default**: Use the domain or IP address configured in the **Domain** field when creating the Peer Trunk. • **Custom**: Use a custom domain or IP address. You can enter the custom value in the field next to the **Custom** drop-down list.
Diversion Remote-Party-ID P-Asserted-Identity P-Preferred-Identity	**Optional:** Define other parameters of a SIP INVITE header as needed. For more information, see Options of outbound parameters.
P-Asserted-Identity URI Format	**Note:** This parameter is available only when **P-Asserted-Identity** is not set to None. To assert and verify the identity of the caller, specify the format of P-Asserted-Identity: • SIP URI (sip:) • TEL URI (tel:)

Note:
For different types of SIP trunk, the optional items are different.

Table 13. Options of outbound parameters

Option	Description
[Default]	• For the **Diversion** outbound parameter, the system uses the original call destination number (DID number) as the parameter value when the call diversion occurs. • For the **Remote-Party-ID**, **P-Asserted-Identity** and **P-Preferred-Identity** outbound parameter, the system selects a parameter by the following priority from top to bottom: ◦ Outbound Route Outbound Caller ID ◦ Extension's Outbound Caller ID in Trunk ◦ Trunk Outbound Caller ID ◦ Trunk Username ◦ Extension Caller ID ◦ The Originator Caller ID
[None]	Do not send the parameter with the SIP INVITE packet.
Extension Caller ID	The caller ID configured on the extension.
Trunk Outbound Caller ID	The global outbound caller ID for the trunk (**Trunk > Outbound Caller ID > General**).
Extension's Outbound Caller ID in Trunk	The extension's associated outbound caller ID with the trunk. • If the extension selects a DOD to call out, the selected DOD number will be taken. • If the extension uses the default DOD to call out, the DOD number associated with the extension will be taken. When multiple DOD numbers are associated, the one with the highest priority in the extension's DOD list will be taken (**Extension and Trunk > Extension > User > Outbound Caller ID (DOD) > Outbound Caller IDs**).
Outbound Route Outbound Caller ID	The outbound caller ID configured on the outbound route that is used for the outbound calls.
Originator Caller ID	The Caller ID of the call originator (the first caller in the case that the call is transferred). • If the call originator is an external number, the external number will be taken. • If the call originator is an extension, the priority order will be Extension Outbound Caller ID → [Default].

Table 13. Options of outbound parameters (continued)

Option	Description
Trunk Username	The username configured on the trunk.
Custom	Define a custom value.

Other Settings

Setting	Description
User Agent	If the ITSP requires User Agent for authentication, enter the User Agent information that is provided by the ITSP.
Realm	Realm is a string displayed to users so they know which username and password to use. **Note:** If you don't know what to fill in, contact your service provider for further instructions.
100rel	Configure 100rel for this trunk. • **Required**: 100rel is required for this trunk. • **Supported**: 100rel is supported by this trunk. • **Disabled**: 100rel is disabled for this trunk.
Maxptime	Select the value of the maxptime used when the PBX sends the INVITE packet. **Note:** If you select **[Default]**, PBX will send a corresponding maxptime value according to the codec that is used for the outbound call.
Select which IP address to use in 'Contact'(SIP) and 'Connection'(SDP) fields	**Note:** This option is only available for register trunk and peer trunk. Select the option to decide which IP address will be used in 'Contact'(SIP) and 'Connection'(SDP) fields. • **Use Default Settings**: Use the IP address that the system provides by default. • **Use Custom IP Address**: Use the custom IP address specified in the **IP Address** field.

Setting	Description
	Note: The custom IP address will be used in 'Contact'(SIP) and 'Connection'(SDP) fields instead of IP addresses configured in the following features: ◦ **Public IP and Ports** (Path: **System > Network**) ◦ **Trunk Network Interface Binding** (Path: **Trunk > Register Trunk (or Peer Trunk) > Advanced**) ◦ **SBC Routing** (Path: **Trunk > Register Trunk (or Peer Trunk) > Basic**)
Send Privacy ID	Whether to send the Privacy ID in SIP header or not. The default is unchecked.
User Phone	Whether to add the parameter `user=phone` as a request line in the header field of the SIP INVITE packet. **Note:** Enable this option only when the SIP provider requires.
Send X-OpenAPI-Call-ID	Set whether to include a `X-OpenAPI-Call-ID` field in the SIP INVITE packet to carry the Call ID for inbound calls and outbound calls routed through the trunk.
Support P-Early-Media	Set whether the P-Early-Media field is included in the INVITE packet.
Send 183 Message with P-Early-Media Header	Set whether the PBX will include the `P-Early-Media` header with the value of `sendrecv` in the 183 message for inbound calls routed through the trunk.

WebRTC Trunk

WebRTC Trunk Overview

Yeastar P-Series Software Edition supports WebRTC trunk. Unlike traditional SIP trunks, WebRTC trunk uses WebRTC (Web Real-Time Communication) technology to implement real-time audio and video communication on web page. With a simple click on a call link pro-

vided by WebRTC trunk, your customers can make free calls directly from their browser to your company's phone system without the need for additional plug-ins or software. In addition, the audio call can be seamlessly switched to a video call for face-to-face communication, improving the customer service experience.

Requirements and restrictions

Requirements

- **Network**: PBX can be remotely accessed via a domain name.
  For more information about the domain configuration, see the following topics:
  - Configure Network for Remote Access by a Yeastar FQDN
  - Configure Network for Remote Access by a Yeastar Domain Name
  - Configure Network for Remote Access by a Domain Name
- **Plan**: If you need video calls, **Ultimate Plan** is required.
- **Firmware**: The version of Yeastar P-Series Software Edition is 83.19.0.70 or later.

Restrictions

- You can create up to **5** WebRTC trunks.
- A WebRTC trunk supports up to **10** concurrent calls.

Supported web browsers

The following table shows the compatible web browsers.

Web browser	Version
Google Chrome	Chrome 87 or later
Microsoft Edge	Edge 87 or later
Opera	Opera 72 or later

Related information

Set up WebRTC Click-to-Call

Set up WebRTC Click-to-Call

To implement WebRTC click-to-call, you need to create a WebRTC trunk on PBX to obtain a WebRTC call link, then embed the call link into your web page. In this way, your website visitors can make calls to your company's phone system with a click.

Prerequisites

- Make sure that the PBX can be remotely accessed via a domain name.
  For more information about the domain configuration, see the following topics:
  - Configure Network for Remote Access by a Yeastar FQDN
  - Configure Network for Remote Access by a Yeastar Domain Name
  - Configure Network for Remote Access by a Domain Name
- If you need video calls, **Ultimate Plan** is required.
- Make sure the version of Yeastar P-Series Software Edition is 83.19.0.70 or later.

Procedure

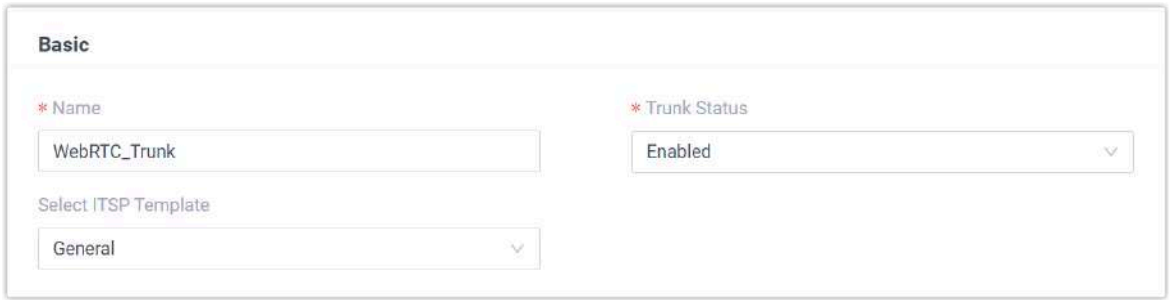
1. Create a WebRTC trunk
2. Set WebRTC inbound call destination
3. Test WebRTC Click-to-Call

Video Tutorial

Create a WebRTC trunk

Create a WebRTC trunk to obtain a WebRTC call link.

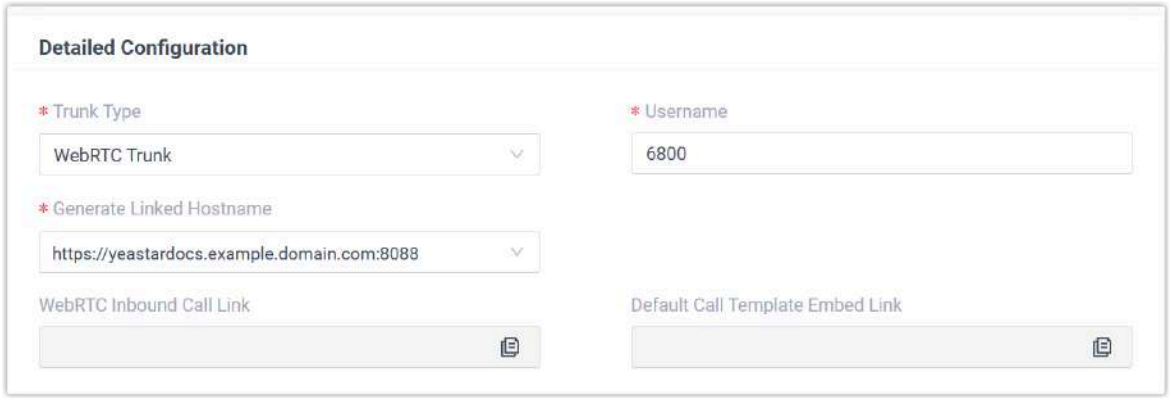
1. Log in to PBX web portal, go to **Extension and Trunk > Trunk**, then click **Add**.
2. In the **Basic** section, complete the following settings.



   - **Name**: Enter a name to help you identify it.

- **Trunk Status**: Select **Enabled**.
- **Select ITSP Template**: Select **General**.

3. In the **Detailed Configuration** section, complete the following settings.



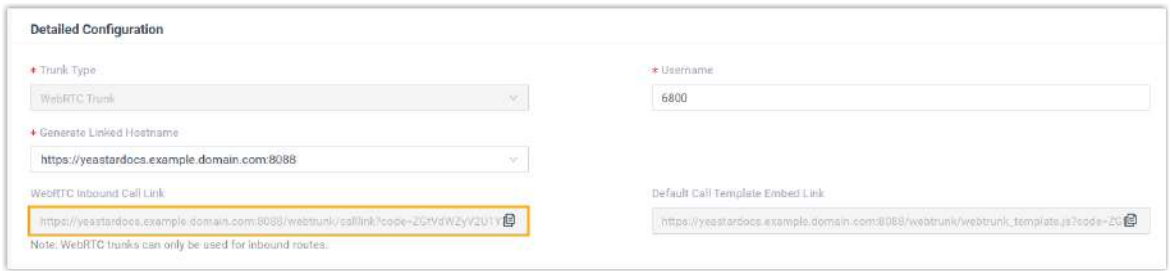
- **Trunk Type**: Select **WebRTC Trunk**.
- **Username**: Enter a username for the trunk.
- **Generate Linked Hostname**: Select the hostname for generating the WebRTC Inbound Call Link and the Default Call Template Embed Link.

4. **Optional:** Click the **Advanced** tab to configure advanced WebRTC trunk settings.
   a. In the **Codec Settings** section, configure your preferred codecs.
   b. In the **Call Restriction** section, set the maximum number of concurrent calls for the trunk.

> **Note:**
> The default number is **5**, you can set up to **10** concurrent calls.

5. Click **Save** and **Apply**.

A WebRTC trunk is displayed in the trunk list with the trunk status showing ; A WebRTC call link is generated and displayed in the **WebRTC Inbound Call Link** field of the trunk.



Set WebRTC inbound call destination

Set up an inbound route for the WebRTC trunk to route the WebRTC inbound calls to a desired destination.

1. Go to **Call Control > Inbound Route**, then click **Add** to add an inbound route.
2. In the **General** section, set a name for the inbound route.

3. In the **Trunk** section, select the WebRTC trunk from **Available** box to **Selected** box.

> **Note:**
> You can NOT select both WebRTC trunk and other types of trunk for an inbound route at the same time.

4. In the **Default Destination** section, set destination(s) for the WebRTC inbound calls.
   - If you want the inbound calls to always be routed to a destination, set the desired destination in the **Default Destination** drop-down list.

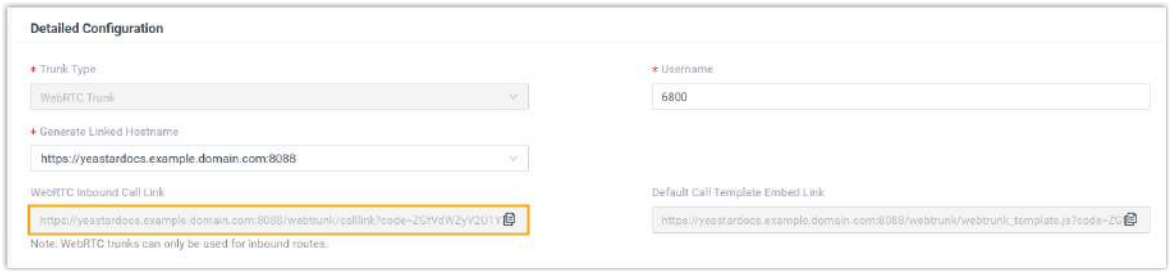
   - If you want the inbound calls to be routed to different destinations based on time, do as follows:
     a. Select the checkbox of **Time Condition**.
     b. In the **Time-based Routing Mode** drop-down list, select a time-based mode.
     c. Configure the corresponding destinations based on time.

     For more information of time-based inbound call routing, see the following topics:
     - Route Inbound Calls based on Business Hours
     - Route Inbound Calls based on Department Hours
     - Route Inbound Calls based on Employee Hours
5. Click **Save** and **Apply**.

Test WebRTC Click-to-Call

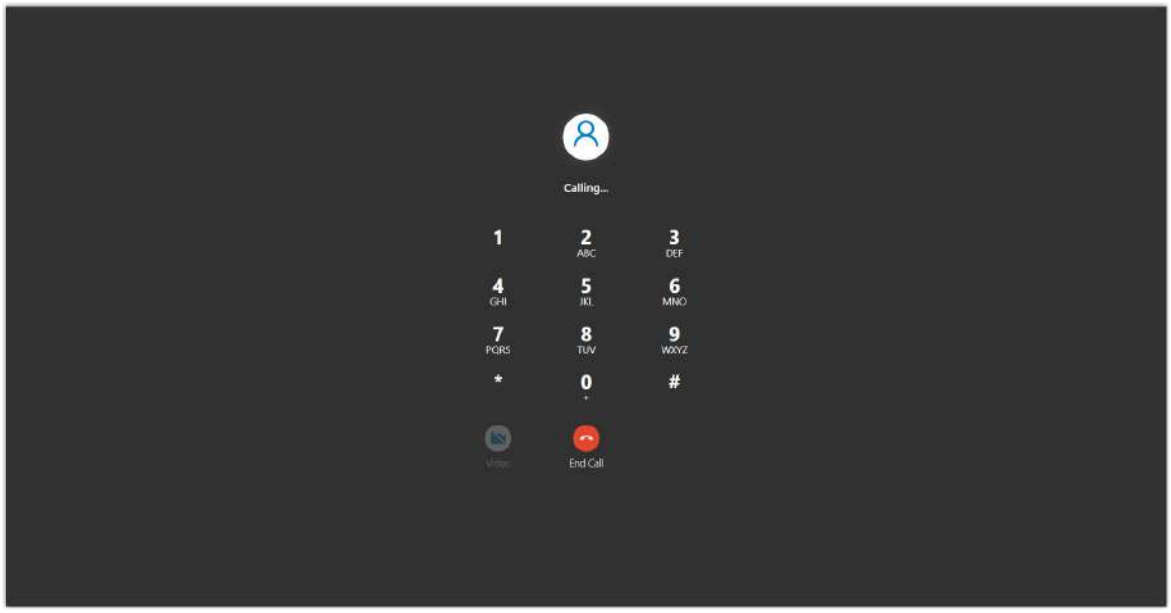
Test if the WebRTC inbound call can be routed to the given destination.

1. Go to **Extension and Trunk > Trunk**, click beside the WebRTC trunk.
2. In the **Detailed Configuration** section, copy the **WebRTC Inbound Call Link**.



3. Open a browser tab, paste the inbound call link in the address bar, then press **Enter**. A dialpad is displayed on the web page, and a call is placed to the pre-set call destination.

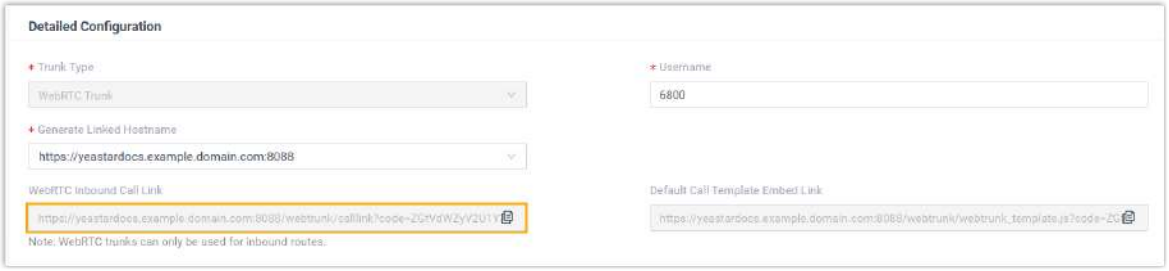
> **Tip:**
>
> During the call, you can switch to a video call by clicking at the bottom-left corner on the web page.



What to do next

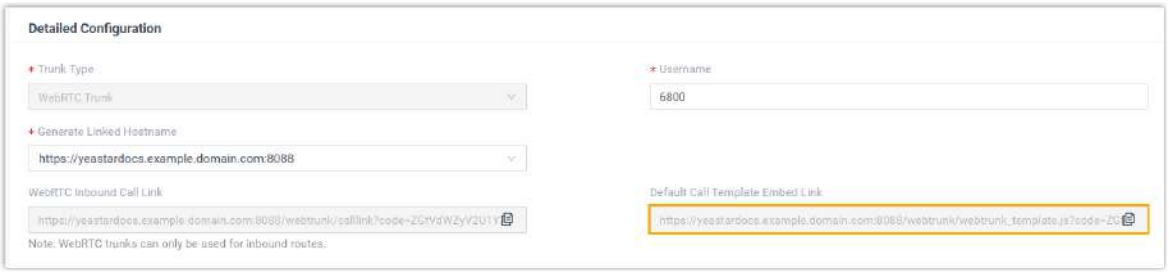
Embed the WebRTC inbound call link into your web page in either of the following ways:

- Customize a call button on your website, and set the button link to the WebRTC call link.

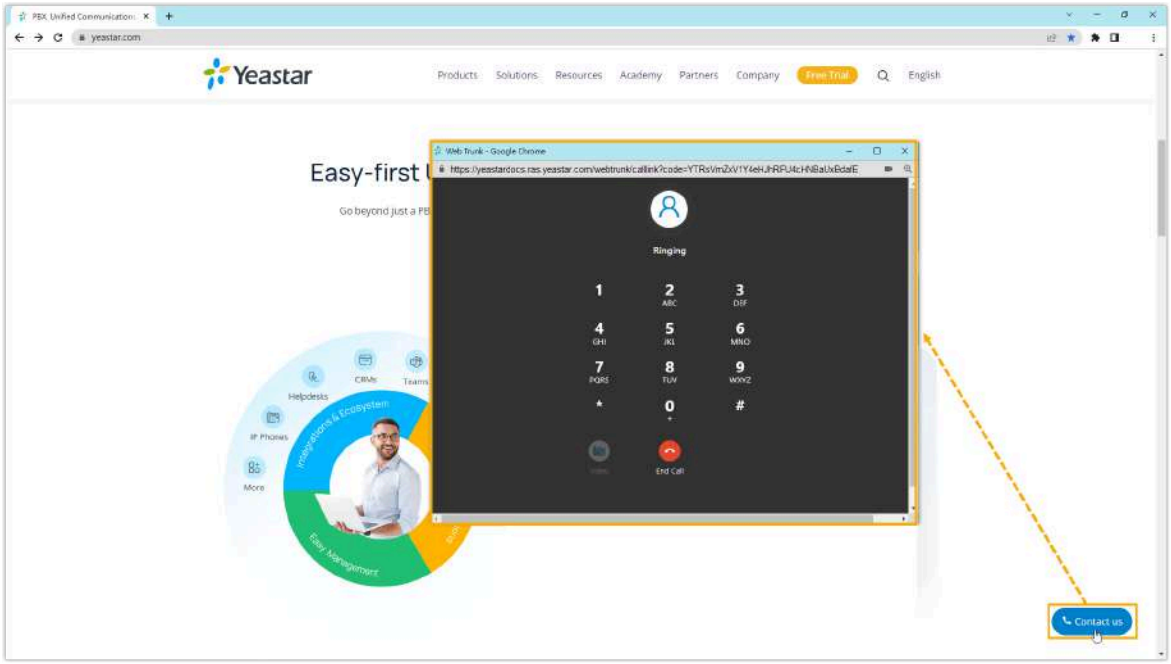


- Utilize the default call button template provided in the WebRTC trunk by referencing the embed link in your website using the following script:

```
<script src="{Default Call Template Embed Link}"></script>
```



The figure below shows the generated call button and the click-to-call effect:


Yeastar
Products
Solutions
Resources
Academy
Partners
Company
Free Trial
English
Easy-first
Web Trunk - Google Chrome
Ringing
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
*
0 +
#
End Call
Helpdesks
CRMs
Teams
IP Phones
More
Integrations & Ecosystem
Easy Management
Contact us

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. Under the **Outbound Rules** tab, configure trunks for emergency calls.

   Note:

> Emergency calls have the highest priority. If the selected trunk is occupied, PBX will terminate the ongoing call, and place the emergency call.

a. Click **Add**.
b. In the drop-down list of **Trunk**, select a trunk.
c. Leave the **Trunk's Emergency Outbound Caller ID** field blank.

> **Note:**
> Do not set emergency outbound caller ID for basic emergency calling, or the emergency calls may fail.

d. If the ITSP requires a prefix to place outbound calls, enter the provided prefix number in the **Prepend for Emergency Number** field.

   The prefix will be automatically added at the beginning of the dialed emergency number. For example, if you set the field to `1234`, when a user dials 911, the PBX system will add 1234 to the emergency number and call out 1234911.

> **Important:**
> Carefully configure the prefix according to the ITSP's requirements, or the emergency calls may fail.

e. **Optional:** Repeat **step a** - **step d** to add another trunk.

> **Note:**
> If the first trunk cannot work properly, the PBX will use the second trunk to make calls.

6. Click **Save** and **Apply**.

What to do next

After setting up an emergency calling, you may need to consider the following configurations:

- Set up a Route for PSAP Callbacks
- Add an Emergency Notification Contact

Set up Enhanced Emergency Calling

To ensure that users can make emergency calls for help when an accident occurs, you need to set up emergency calling in Yeastar P-Series 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. Under the **Outbound Rules** tab, configure trunks for emergency calls.

   > **Note:**
   > Emergency calls have the highest priority. If the selected trunk is occupied, PBX will terminate the ongoing call, and place the emergency call.

   a. Click **Add**.
   b. In the drop-down list of **Trunk**, select a trunk.

c. In the **Trunk's Emergency Outbound Caller ID** field, enter the Emergency Location Identification Number (ELIN) that you have purchased from the trunk provider.

d. If the ITSP requires a prefix to place outbound calls, enter the provided prefix number in the **Prepend for Emergency Number** field.

The prefix will be automatically added at the beginning of the dialed emergency number. For example, if you set the field to `1234`, when a user dials 911, the PBX system will add 1234 to the emergency number and call out 1234911.

> **Important:**
> Carefully configure the prefix according to the ITSP's requirements, or the emergency calls may fail.

e. **Optional:** Repeat **step a** - **step d** to add another trunk.

> **Note:**
> If the first trunk cannot work properly, the PBX will use the second trunk to make calls.

6. Click **Save** and **Apply**.

Assign ELINs for individual users

To provide the PSAP with the emergency caller's precise location, you may need to purchase multiple ELINs and assign these ELINs to extension users.

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, click to edit the desired extension.
2. On the extension **User** page, scroll down the page, enter the ELIN in the **Emergency Outbound Caller ID** field.
3. Click **Save** and **Apply**.

After the user dials an emergency number, the PSAP will locate the specific geographic location of the user by the extension user's ELIN.

What to do next

After setting up an emergency calling, you may need to consider the following configurations:

- Set up a Route for PSAP Callbacks
- Add an Emergency Notification Contact

Set up a Route for PSAP Callbacks

In case that the emergency caller is not available to answer the returned call from PSAP, you can set up an inbound route to forward the call to an on-site security personnel.

Procedure

1. Log in to PBX web portal, go to **Call Control > Inbound Route**.
2. Click **Add** to add an inbound route for PSAP callbacks.
3. In the **Name** field, specify a name to help you identify it.
4. In the **Caller ID Pattern** section, add all the emergency numbers that you have set on the PBX.
    a. Click **Add**.
    b. In the **Pattern** field, enter the emergency number.
    c. **Optional:** To add another emergency number, repeat **step a - b**.
5. In the **Trunk** section, select the trunks that are used for emergency calls to the **Selected** box.
6. In the **Default Destination** field, select **Extension**, and select the user who is responsible for answering the returned calls from PSAP.
7. Leave other fields as the default settings.
8. Click **Save** and **Apply**.

Result

When a PSAP operator calls back, the call will be forwarded to the extension user that is configured on the inbound route.

Related information

Set up Basic Emergency Calling
Set up Enhanced Emergency Calling

Manage Emergency Numbers

After you add emergency numbers, you can edit or delete them.

Edit an emergency number

1. Log in to PBX web portal, go to **Call Control > Emergency Number**, click beside the emergency number that you want to edit.
2. Edit information of emergency number.
3. Click **Save** and **Apply**.

Delete an emergency number

1. Log in to PBX web portal, go to **Call Control > Emergency Number**, click beside the emergency number that you want to delete.
2. In the pop-up dialog box, click **OK** to confirm.
3. Click **Apply**.

Export and Import Emergency Numbers

The emergency numbers configured on Yeastar P-Series 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.

Key Concepts

Time zones

Time zone is a standard time defined based on geographical regions, ensuring time synchronization across different areas and facilitating the coordination of business operations and communications.

Yeastar P-Series Software Edition allows you to use a default time zone or set multiple time zones to meet the specific needs of your business operations.

- **Default Time Zone**

  The system automatically assigns a default time zone based on the date and time settings of the PBX (Path: **System > Date and Time > Time Zone**). This default time zone is applied to system-wide time settings unless additional time zones are configured.
- **Additional Time Zone**

  For businesses operating across different regions, you can add multiple time zones to accommodate regional offices or customers in different regions, and set up business hours and holidays based on each region's local time.

  For more information, see Set Multiple Time Zones.

Business Hours

Business Hours is the working hours during which you conduct business. A rest break that allows an employee to rest for a short period of time during working days is also considered as Business Hours.

Yeastar P-Series 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 Business Hours and Route Inbound Calls based on Business Hours.

- **Custom Business Hours**

  Custom Business Hours is typically for departments with different hours from your main business hours. You need to create custom schedules that accommodate each department's unique hours and call handling needs.

  For more information, see Route Inbound Calls based on Department Hours.

- **Custom Time Periods**

  Custom Time Periods is typically for individual employees who have their own work schedules.

  For more information, see Route Inbound Calls based on Employee Hours.

Holidays

Holiday defines the days your business is closed due to a holiday. Holidays can be divided into two types:

- Fixed-date Holidays
- Moveable-date Holidays

You can add holidays by date, month, or week according to the holiday type, and set different prompts for different holidays. For more information, see Create a Holiday.

Outside Business Hours

Outside Business Hours is the time periods that are not defined as Business Hours or Holidays.

Application

After you configured Business Hours and Holidays feature, the time settings will be applied to various system features for user management and call handling. For detailed information

on the specific applications and how these time conditions are utilized, see Time Condition Overview.

Related information

- Set Business Hours
- Monitor Time Condition Status
- Create a Holiday
- Override Time Condition for Inbound Calls
- Automatic Reset of Time Condition

Time Zones

Set Multiple Time Zones

Yeastar P-Series Software Edition supports multiple time zones, enabling businesses to operate efficiently across different regions by managing calls and settings based on the local time. This topic describes how to set multiple time zones.

Scenarios

For businesses that operates across multiple time zones, or for multi-national companies with employees distributed across different regions, a single time zone setting is insufficient to meet daily operation needs. To ensure smooth collaboration and efficient call management, businesses need the flexibility to configure work hours tailored to each region's local time.

For example, if a business has offices in the US, the UK, and China, administrator can set the US Pacific time zone as the default, add additional time zones for the UK and China, and then configure business hours and holidays for the time zones accordingly. This ensures that staff can work and handle calls aligning with regional working hours, and customers can receive calls or services at appropriate times, improving work efficiency and customer satisfaction.

Requirements and restrictions

Requirements

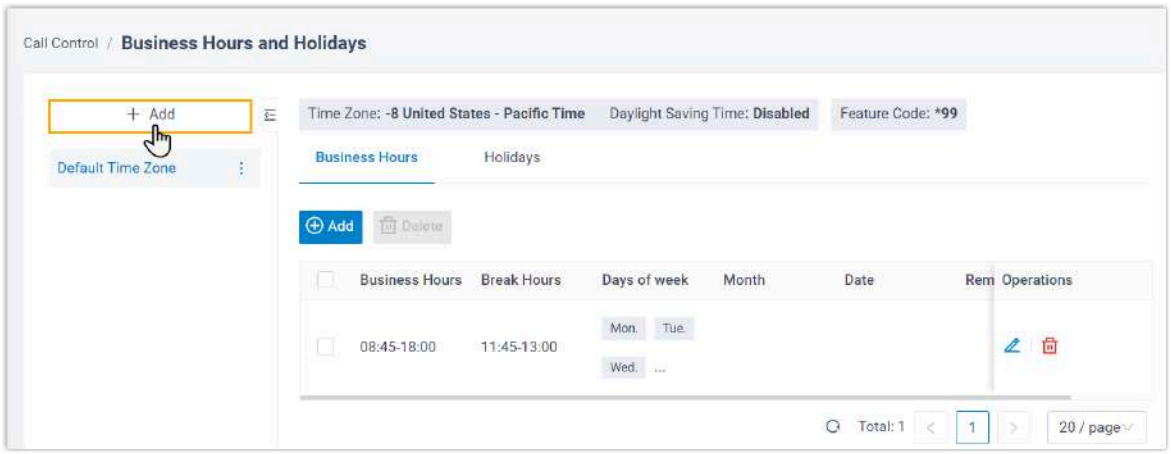
The firmware of Yeastar P-Series Software Edition is 83.18.0.59 or later.

Restrictions

Yeastar P-Series Software Edition supports up to **24** time zones (including the default time zone).

Procedure

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**.
2. On the side panel, click **Add**.



3. In the pop-up window, configure the time zone settings.

Setting	Description
Name	Set a name to help you identify the time zone.
Time Zone	Select the desired time zone.
Daylight Saving Time	Enable or disable Daylight Saving Time (DST) according to your needs.
Feature Code	This field is auto-populated with a system-generated feature code, which can be used to switch or subscribe to the Business Hours and Holidays status for the specific time zone. **Note:** The usage rules and user permissions follow the configurations on **Call Features > Feature Code > Switch Business Hours and Holidays Status**.
Assign to Extension	Optional. Assign the time zone to desired extensions in bulk. After assigned, the business hours and holidays configured in the time zone will be applied to the selected extensions. **Note:** You can change the time zone for extensions individually on **Extension and Trunk > Extension >** ✎ **> Features > Business Hours > Time Zone**.

4. Click **Save**.
5. Repeat step **2** - **4** to add more time zones as needed.
6. Reboot the PBX to take effect.

Results

The time zones are available in the system.

What to do next

Set Business Hours and Create a Holiday based on time zones.

Related information

Manage Time Zones

Manage Time Zones

This topic describes how to edit and delete the time zones that you've added on the PBX.

Edit a time zone

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**.
2. Click ⋮ beside the desired time zone, then click **Edit**.
3. In the pop-up window, change the time zone settings.
4. Click **Save** and **Apply**.
5. Reboot the PBX to take effect.

   The time zone settings are updated.

Delete a time zone

> **Note:**
> The default time zone can NOT be deleted.

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**.
2. Click ⋮ beside the desired time zone, then click **Delete**.
3. In the pop-up window, click **OK** and **Apply**.

   The time zone is deleted.

Business Hours

Set Business Hours

This topic describes how to set up Business Hours for a specific time zone.

Background information

Business Hours is the main working hours for your company, which may apply to most of the employees who have fixed work schedules.

For more information about different types of time in Yeastar P-Series 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**, and click the desired time zone.
2. On the **Business Hours** page, click **Add**, then complete the following time settings.
    a. In the **Business Hours** section, click **Add**, then specify the hours when your business is open.
    b. In the **Break Hours** section, click **Add**, then specify rest breaks during the working days.
    c. In the **Date Settings** section, select your working days.
        - **Days of Week**: If enabled, you can only use the **Days of Week** as the date condition for your business hours.
        - **Advanced Options**: If enabled, you can configure business hours more flexibly with a mixed condition of Week, Month, and Date.
    d. **Optional:** In the **Other Options** section, enter a note in the text field to help you identify the time group.
3. Click **Save** and **Apply**.

Result

- A time group is created to define the global business hours in the specific time zone.
- You can create more time groups according to your company's business hours based on different time zones. All the time groups created on the **Business Hours** page are regarded as your company's global business hours in the specific time zone.

What to do next

- To handle inbound calls based on the Global Business Hours, see Route Inbound Calls based on Business Hours.
- To limit users to make outbound calls based on the Global Business Hours, see Set up an Outbound Route.

Related information

Set Multiple Time Zones
Monitor Time Condition Status
Override Time Condition for Inbound Calls
Route Inbound Calls based on Business Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on Employee Hours

Manage Business Hours

This topic describes how to edit and delete the time groups that you've defined as your global business hours for a specific time zone.

Edit a time group of Global Business Hours

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Business Hours** page, select a desired time group, click  .
3. Change the time settings.
4. Click **Save** and **Apply**.

   The global business hours in the time zone is updated.

Delete a time group of Global Business Hours

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Business Hours** page, select a desired time group, click **Delete**.
3. In the pop-up dialog box, click **OK** to confirm.

   The time group is deleted from the global business hours in the time zone.

Related information

Set Business Hours
Overview of Business Hours and Holidays

Holidays

Create a Holiday

This topic describes how to create holidays for a specific time zone by date, week, and month.

Create a holiday by date

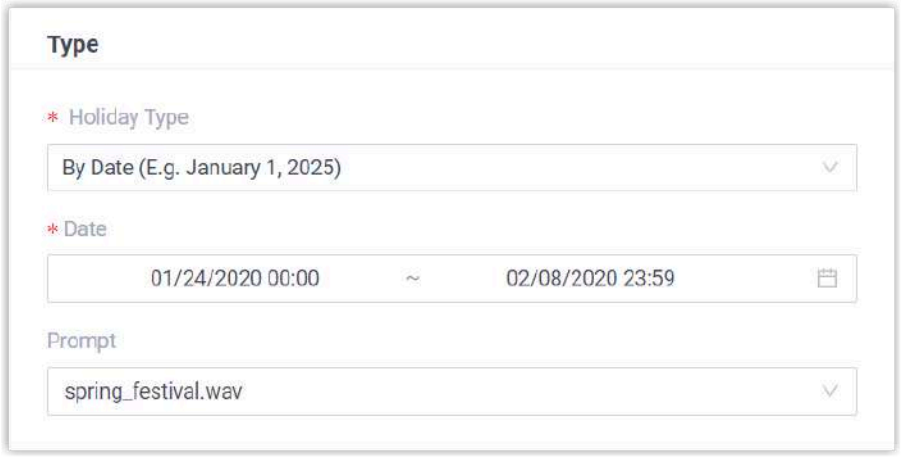
If the holiday date varies every year, you can create a holiday by date.

Example

Chinese Spring Festival varies every year, and 2020 Chinese Spring Festival falls on Jan. 24 to Feb. 8. You can set the holiday as follows.

Configuration Example

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Add**, then complete the following holiday settings.
   a. In the **Basic** section, enter `2020 Chinese Spring Festival` in the text field.
   b. In the **Type** section, set the type, date, and prompt of the holiday.



- **Holiday Type**: Select **By Date**.
- **Date**: Select the holiday start date and end date.
- **Prompt**: Optional. Select an existing prompt or click **Upload** to upload a prompt.

> **Note:**
> - Prompts in the drop-down list are synchronized from **PBX Settings > Voice Prompt > Custom Prompt**.
> - To play the prompt to callers when they call to the PBX during holidays, you need to enable **Play Holiday Prompt During Holidays** (Path: **Call Control > Inbound Route > Default Destination > Play Holiday Prompt During Holidays**) for the time-based inbound route.

3. Click **Save** and **Apply**.

Create a holiday by month

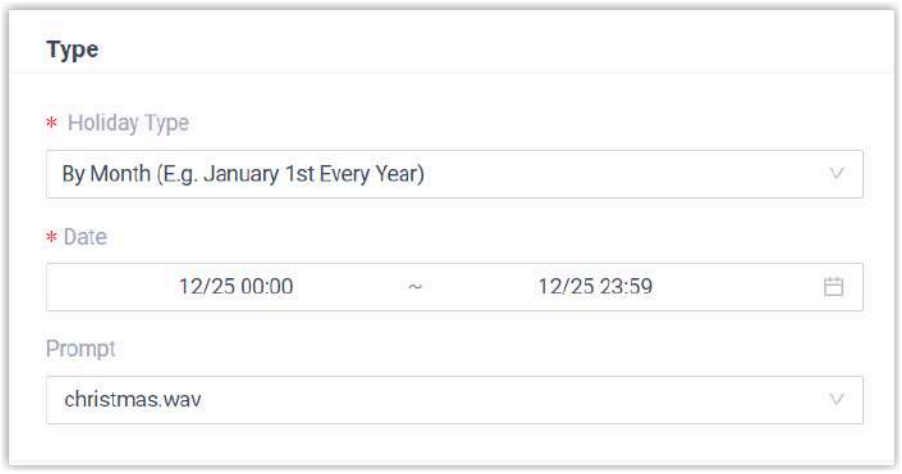
If the holiday always falls on the same date, you can set a holiday by month.

Example

The Christmas falls on Dec. 25 every year. You can set the holiday as follows.

Configuration Example

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Add**, then complete the following holiday settings.
   a. In the **Basic** section, enter `Christmas` in the text field.
   b. In the **Type** section, set the type, date, and prompt of the holiday.



- **Holiday Type**: Select **By Month**.
- **Date**: Select the holiday start date and end date.
- **Prompt**: Optional. Select an existing prompt or click **Upload** to upload a prompt.

> **Note:**
> - Prompts in the drop-down list are synchronized from **PBX Settings > Voice Prompt > Custom Prompt**.
> - To play the prompt to callers when they call to the PBX during holidays, you need to enable **Play Holiday Prompt During Holidays** (Path: **Call Control > Inbound Route > Default Destination > Play Holiday Prompt During Holidays**) for the time-based inbound route.

3. Click **Save** and **Apply**.

Create a holiday by week

If a holiday always falls on the specific week, you can set a holiday by week (which means the day of the specific week of the month).

> **Note:**

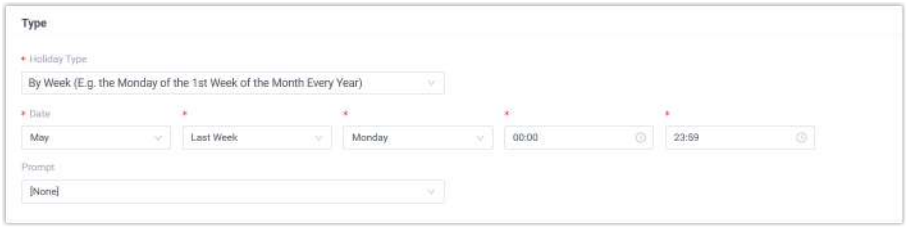
The system calculates the week as the period ending on and including Sunday, and the last week calculates from the last Monday.

Example

2024 Memorial Day falls on the Monday of the last week in May. You can set the holiday as follows.

Configuration Example

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Add**, then complete the following holiday settings.
   a. In the **Basic** section, enter `Memorial Day` in the text field.
   b. In the **Type** section, set the type, date, and prompt of the holiday.



   - **Holiday Type**: Select **By Week**.
   - **Date**: Select the month and the day of the specific week of the month.
   - **Prompt**: Optional. Select an existing prompt or click **Upload** to upload a prompt.

> **Note:**
> - Prompts in the drop-down list are synchronized from **PBX Settings > Voice Prompt > Custom Prompt**.
> - To play the prompt to callers when they call to the PBX during holidays, you need to enable **Play Holiday Prompt During Holidays** (Path: **Call Control > Inbound Route > Default Destination > Play Holiday Prompt**

During Holidays) for the time-based inbound route.

3. Click **Save** and **Apply**.

Create a holiday by weekday

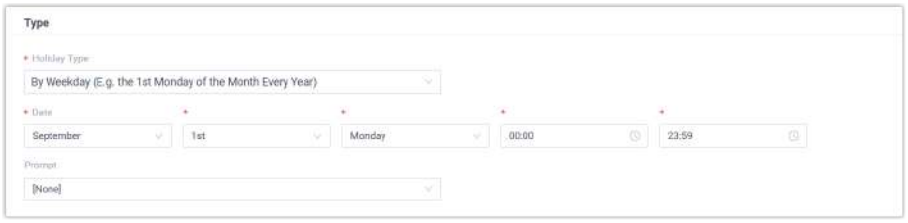
If a holiday always falls on the same weekday, you can set a holiday by weekday (which indicates the specific weekday of the month).

Example

Labor Day falls on the first Monday in September. You can set the holiday as follows.

Configuration Example

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Add**, then complete the following holiday settings.
   a. In the **Basic** section, enter `Labor Day` in the text field.
   b. In the **Type** section, set the type, date, and prompt of the holiday.



- **Holiday Type**: Select **By Weekday**.
- **Date**: Select the month and the weekday of the month.
- **Prompt**: Optional. Select an existing prompt or click **Upload** to upload a prompt.

Note:

- Prompts in the drop-down list are synchronized from **PBX Settings > Voice Prompt > Custom Prompt**.
- To play the prompt to callers when they call to the PBX during holidays, you need to enable **Play Holiday Prompt During Holidays**

> (Path: **Call Control > Inbound Route > Default Destination > Play Holiday Prompt During Holidays**) for the time-based inbound route.

3. Click **Save** and **Apply**.

What to do next

- To handle inbound calls based on Holidays, see Set up an Inbound Route.
- To limit users to make outbound calls during holidays, see Set up an Outbound Route.

Related information

Overview of Business Hours and Holidays
Set Multiple Time Zones
Set Business Hours
Manage Holidays
Export and Import Holidays

Manage Holidays

This topic describes how to edit and delete a holiday for a specific time zone.

Edit a holiday

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, select a desired holiday, click .
3. Change the holiday settings.
4. Click **Save** and **Apply**.

   The holiday list is updated.

Delete a holiday

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, select a desired holiday, click **Delete**.
3. In the pop-up dialog box, click **OK** to confirm.

The holiday is deleted from the holiday list.

Related information

Create a Holiday
Overview of Business Hours and Holidays
Export and Import Holidays

Export and Import Holidays

The holidays configured on Yeastar P-Series Software Edition can be exported and saved as a template. You can fill in desired holidays in the exported file, and import the file to PBX again. This topic describes how to export and import holidays.

Export holidays

You can export all holidays to a CSV file, and then make additions, removals, and changes to the file.

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Export**.

   A CSV file is saved to your computer. To check and edit parameters in the CSV file, see Holidays Parameters.

Import holidays

We recommend that you export holidays data to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- **Format**: UTF-8.CSV
- **Size**: Less than 50 MB
- **File name**: Less than 127 characters
- **Import parameters**: Ensure that the import parameters meet requirements. For more information, see Holidays Parameters.

Procedure

1. Log in to PBX web portal, go to **Call Control > Business Hours and Holidays**, then click the desired time zone.
2. On the **Holidays** page, click **Import**.
3. In the pop-up window, click **Browse**, and select your CSV file.
4. Click **Import**.

   The holidays in the CSV file will be displayed in the **Holidays** list.

Related information

Overview of Business Hours and Holidays
Create a Holiday
Manage Holidays

Time Condition

Time Condition Overview

Time Condition is the communication feature in Yeastar P-Series 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 the following features:

Apply to extension presence switch

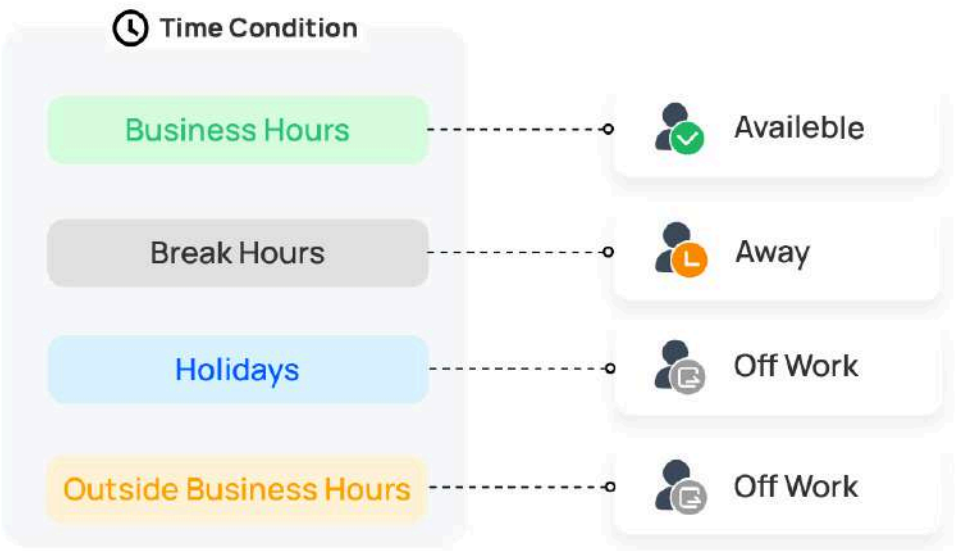
Extension presence status can be auto switched based on Time Condition. When time condition changes, extension presence status would be changed accordingly.

For example, when the PBX is in the time condition for Business Hours, the extension status is auto switched to **Available**.

Note:

- This feature should be configured on extension configuration page. For more information, see Automatically Switch Extension Presence Based on Time.

- In addition to the time group associated in the specific time zone, you can also customize business hours for an extension individually, which will be applied to the presence switch for the extension. For more information, see Set Business Hours for an Extension

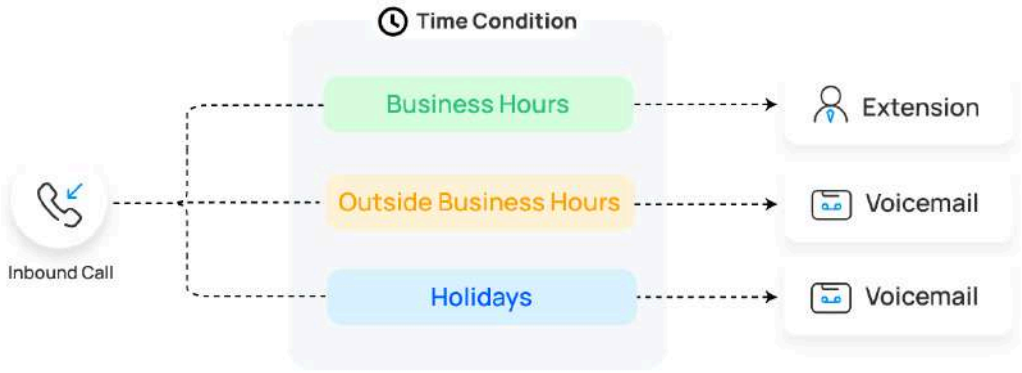


Apply to an Inbound Route

Time Condition can be used to control the destination of an inbound call based on date and time.

When a call reaches PBX, the system will check the date and time based on the specified time zone against the time group associated, and then route the call to corresponding destination.

For more information, see Set up an Inbound Route.

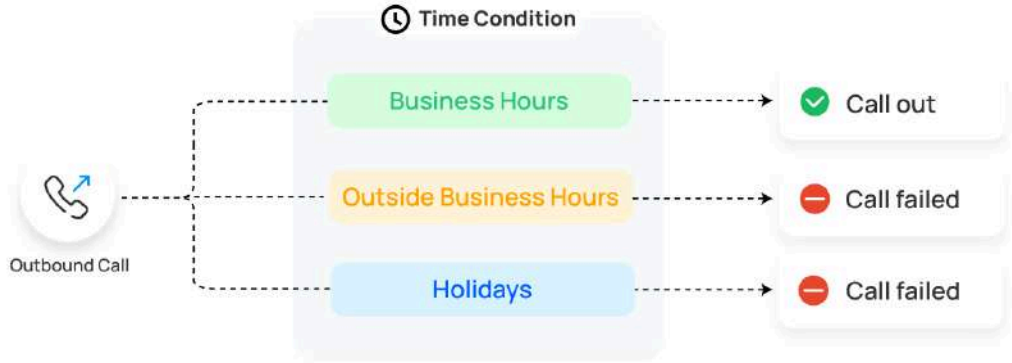


Apply to an Outbound Route

Time Condition can be used to limit the use of an Outbound Route based on date and time.

When a call is made, the system will check the date and time based on the specified time zone against the time group associated. Only when the time comes to the permitted time group can the outbound call be made.

For more information, see Set up an Outbound Route.

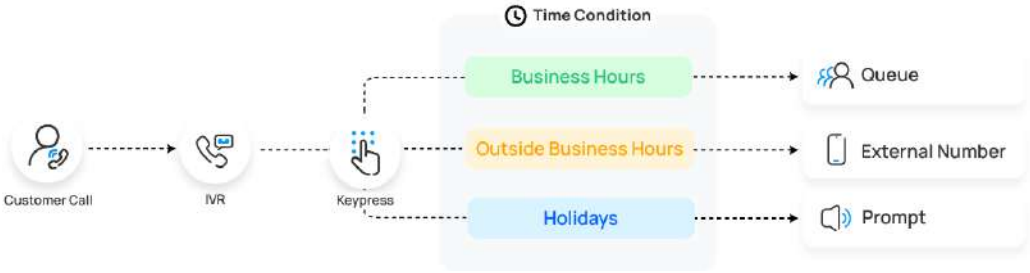


Apply to IVR

Time Condition can be used to control the destination of IVR key press event based on date and time.

When a caller calls an IVR and press a key, the system will check the date and time based on the specific time zone against the time group associated, and then route the call to corresponding destination.

For more information, see Set Key Events Based on Time Conditions.

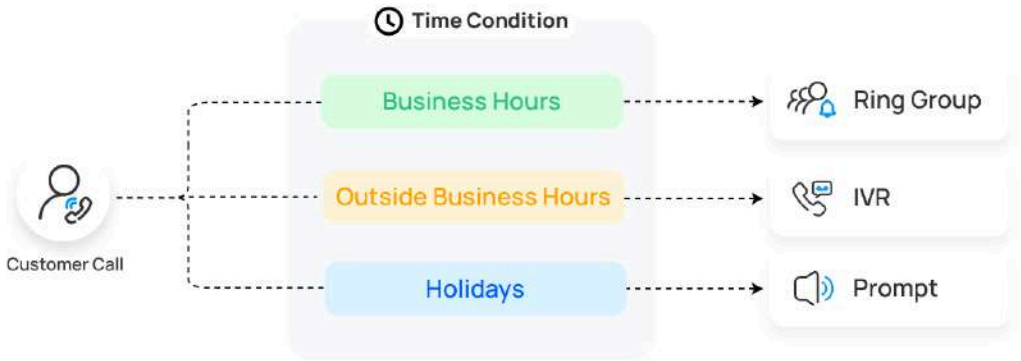


Apply to Ring Group

Time condition can be used to control the destination of calls sent to a ring group.

By default, the ring group receives incoming calls during all time periods. You can set the ring group to receive calls only during business hours, while routing calls to other destinations based on the specified time conditions.

For more information, see Create a Ring Group.

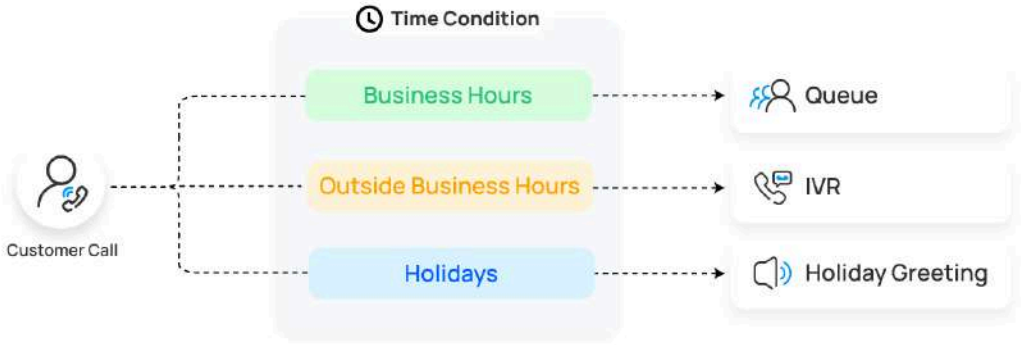


Apply to Call queue

Time condition can be used to control the destination of calls sent to a call queue.

By default, the call queue receives incoming calls during all time periods. You can set the call queue to receive calls only during business hours, while routing calls to other destinations based on the specified time conditions.

For more information Route Queue Call Based on Time Condition.



Time Condition override

For a time-based inbound route, the system routes inbound calls based on the system time. However, users may need to force open or close business occasionally. In this case, you can grant permissions to allow specific users to override time condition for inbound calls through the route. For more information, see Override Time Condition for Inbound Calls.

Note:

- If users do not manually clear time condition override, the system will automatically reset the time condition. For more information, see Automatic Reset of Time Condition.
- To keep the time condition after overriding, see Disable automatic reset of time condition.

Related information

Route Inbound Calls based on Business Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on Employee Hours
Set up an Outbound Route

Allow Users to Override Time Condition by Feature Code

By default, all the users can NOT override time condition. To allow users to override time condition by feature code, follow instructions in the topic to grant permissions to specific users.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. Scroll down the page, and configure the permission of time condition override in the **Switch Business Hours and Holidays Status** section.

   Table 14.

Setting	Feature Code	Permission
Switch Business Hours and Holidays Status (for Business Hours configured in the system's default time zone)	*99 **Note:** This feature code applies only to the system's default time zone. For additional time zones, you can check the corresponding feature code under the specific time zone settings (Path: **Call Control > Business Hours and Holidays**).	Select desired extensions.
Time Condition Switching Prefix (for Custom Business Hours and Custom Time Periods based on the system's default time zone)	Starting with prefix *8 **Note:** Feature codes starting with *8 would be generated for inbound routes that are based on Custom Business Hours or Custom Time Periods.	

3. Click **Save** and **Apply**.

Related information

Override Time Condition for Inbound Calls
Monitor Time Condition Status
Automatic Reset of Time Condition
Enable or Disable Automatic Reset of Time Condition

Allow Users to Override Time Condition on Operator Panel

By default, all the users can NOT override time condition. To allow users to override time condition on Operator Panel, follow instructions in the topic to grant permissions to specific users.

Restrictions

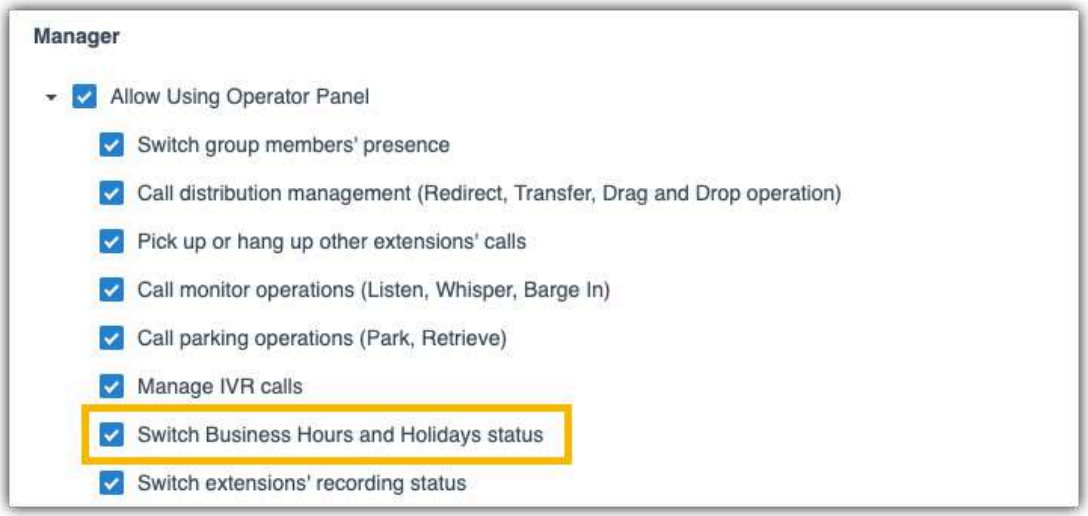
On Operator Panel, only time condition for Business Hours configured in the system's default time zone can be overridden.

Procedure

The permission of time condition override can only be assigned to extension group managers. Follow the instructions below to grant permission to extension group managers.

> **Note:**
> If you want to grant permissions to a specific user, you can assign a custom user type to the member, and customize permissions. For more information, see Assign a custom user type to a group member.

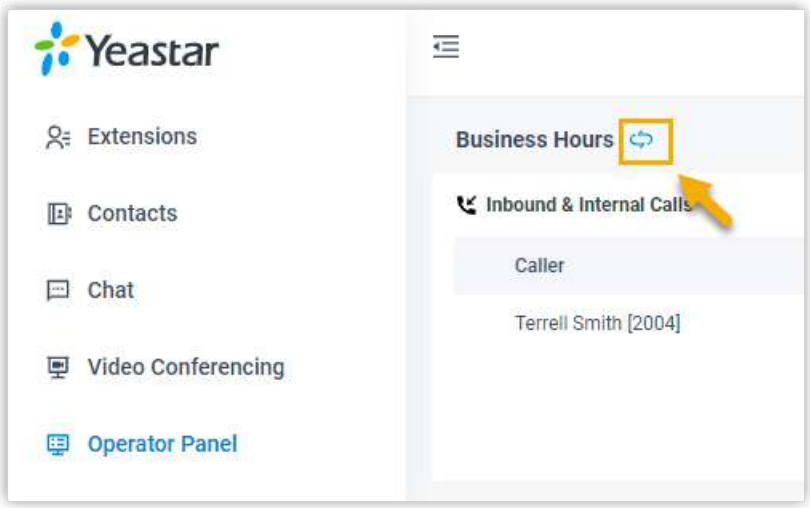
1. Log in to PBX web portal, go to **Extension and Trunk > Extension Group**.
2. Select an extension group, and click .
3. On the **Extension Group** page, click **Group Permissions** tab.
4. In the **Permission Configuration** section, select the checkbox of **Switch Business Hours and Holidays status**.



5. Click **Save** and **Apply**.

Result

On Operator Panel, the user whose user type is Manager can click to override time condition for Business Hours configured in the system's default time zone.



For more information, see Override Time Condition on Operator Panel.

Related information

Allow Users to Override Time Condition by Feature Code
Automatic Reset of Time Condition
Enable or Disable Automatic Reset of Time Condition

Override Time Condition for Inbound Calls

If you have configured a time-based inbound route, the system will automatically route calls to different destinations based on time. However, users may need to force open or close business occasionally. This topic describes how to achieve time condition override for inbound calls.

Background information

Users may need to override time condition in the following scenarios:

- **Temporary night shift**

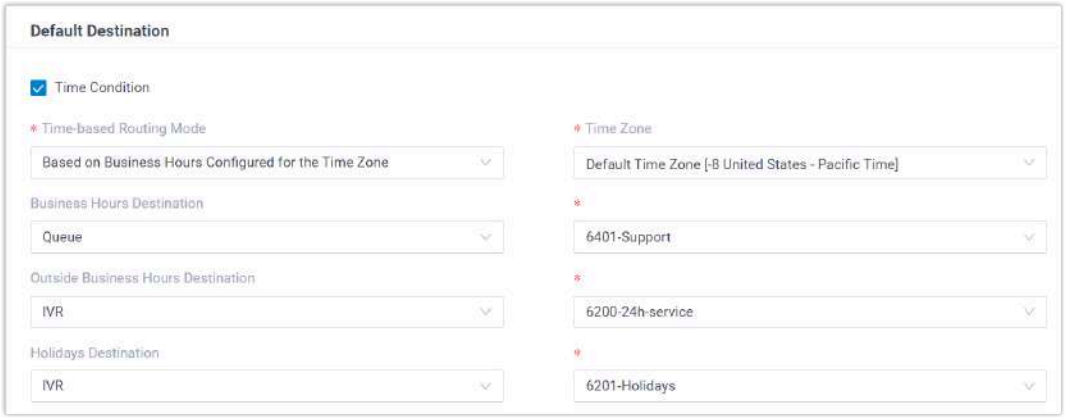
  After business hours, the employee who needs to work in the night can force open the business hours to provide communication services for customers.
- **Occasionally leaving**

  Your company may close the business earlier than usual on a special day. For example, your company will close the business one hour in advance on the Christmas day and you can force close business before you leave.

Override time condition for inbound calls (Global Business Hours)

Background information

An inbound route based on business hours configured in the system's default time zone is set up as follows:



Procedure

Follow the instructions below to achieve time condition override for inbound calls through the route:

1. Grant permission to allow specific users to override time condition.
2. To override time condition, the authorized users should dial corresponding feature code (default ***99**).

   Inbound calls would be routed to different destinations based on the time when users dial feature code.

   Table 15.

Operate Time	Result
Dial *99 during **Business Hours**	Inbound calls will be routed to **Outside Business Hours** destination (IVR 6200).
Dial *99 during **Outside Business Hours**	Inbound calls will be routed to **Business Hours** destination (Queue 6400).
Dial *99 during **Holidays**	Inbound calls will be routed to **Business Hours** destination (Queue 6400).

3. To clear time condition override, the authorized users should dial feature code (default: *99) again.

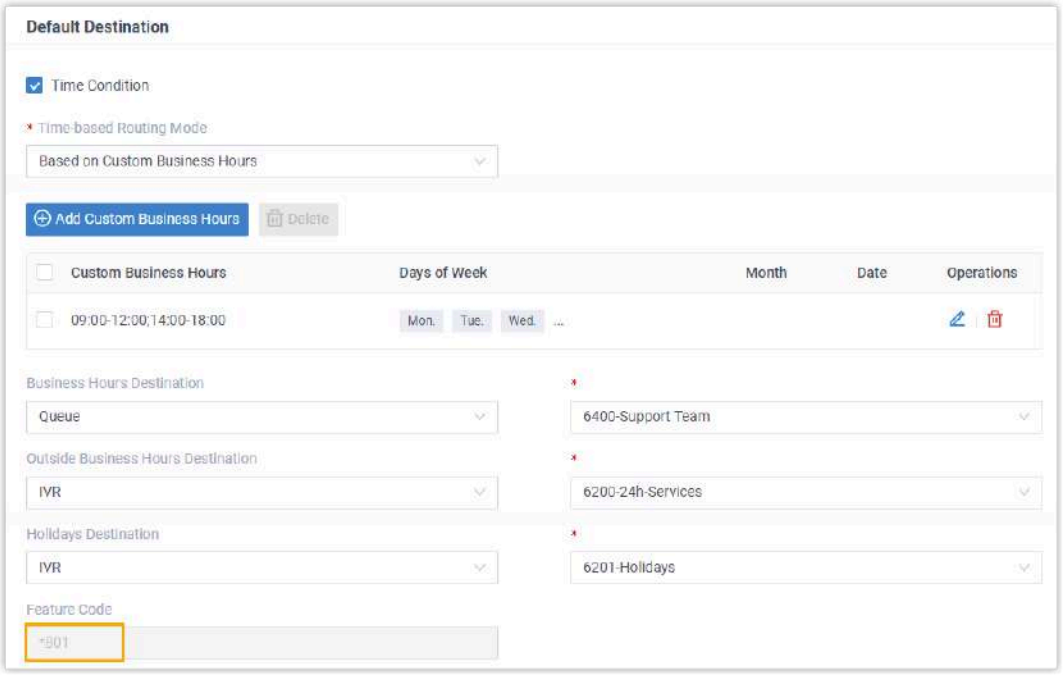
Note:

- If users do not manually clear time condition override, the system will automatically reset the time condition. For more information, see Automatic Reset of Time Condition.
- To keep the time condition after overriding, see Disable automatic reset of time condition.

Override time condition for inbound calls (Custom Business Hours)

Background information

An inbound route based on Custom Business Hours (follows the system's default time zone) is set up as follows:



Procedure

Follow the instructions below to achieve time condition override for inbound calls through the route:

1. Grant permission to allow specific users to override time condition.
2. To override time condition, the authorized users should dial feature code *801.

Inbound calls would be routed to different destinations based on the time when users dial feature code.

Table 16.

Operate Time	Result
Dial *801 during **Business Hours**	Inbound calls will be routed to **Outside Business Hours** destination (IVR 6200).
Dial *801 during **Outside Business Hours**	Inbound calls will be routed to **Business Hours** destination (Queue 6400).
Dial *801 during **Holidays**	Inbound calls will be routed to **Business Hours** destination (Queue 6400).

3. To clear time condition override, the authorized users should dial *801 again.

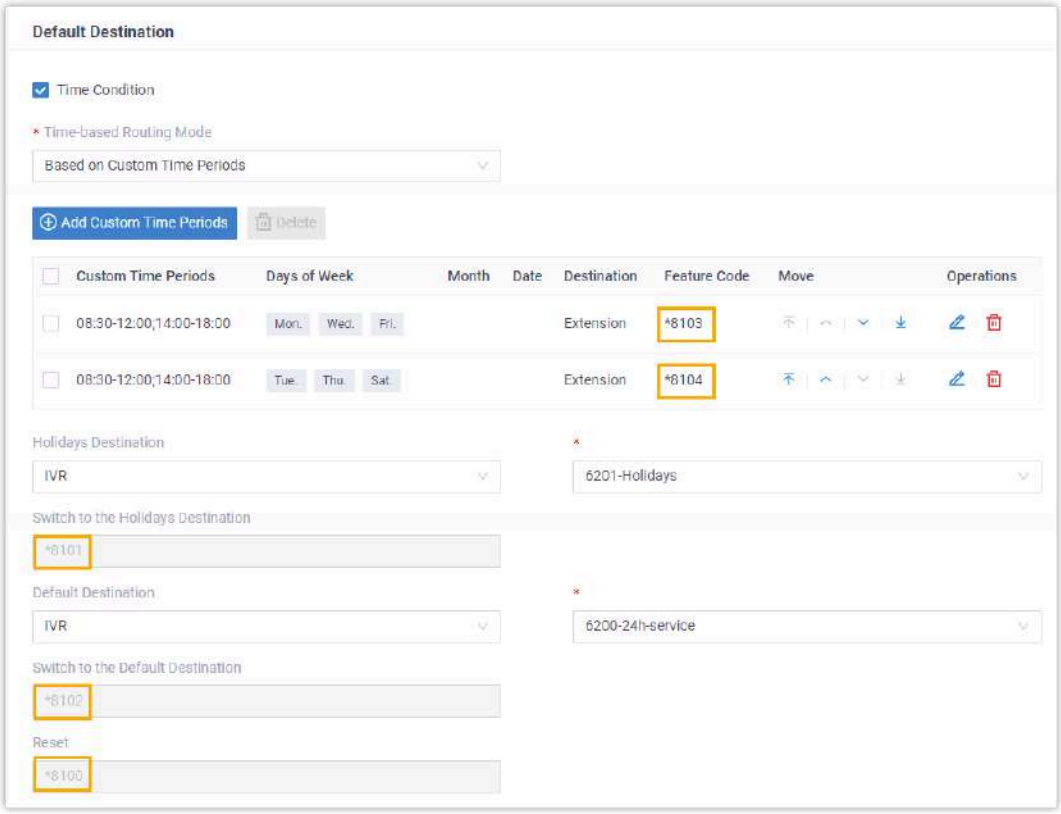
Note:

- If users do not manually clear time condition override, the system will automatically reset the time condition. For more information, see Automatic Reset of Time Condition.
- To keep the time condition after overriding, see Disable automatic reset of time condition.

Override time condition for inbound calls (Custom Time Periods)

Background information

An inbound route based on Custom Time Periods (follows the system's default time zone) is set up as follows:



Procedure

Follow the instructions below to achieve time condition override for inbound calls through the route:

1. Grant permission to allow specific users to override time condition.
2. To override time condition, the authorized users should dial a specific feature code.

   Inbound calls would be routed to corresponding destination based on the dialed feature code.

Table 17.

Time Group	Description	Destination	Feature Code
Time Period 1	Monday, Wednesday, Friday • 08:30 - 12:00 • 14:00 - 18:00	Extension (2000-Leo Ball)	*8103
Time Period 2	Tuesday, Thursday, Saturday	Extension	*8104

Time Group	Description	Destination	Feature Code
	• 08:30 - 12:00 • 14:00 - 18:00	(2004-Terrell Smith)	
Holidays		IVR (6201-Holidays)	*8101
Outside Business Hours		IVR (6200-24h-Services)	*8102

3. To clear time condition override, the authorized users should dial the **Reset** feature code *8100.

> **Note:**
> - If users do not manually clear time condition override, the system will automatically reset the time condition. For more information, see Automatic Reset of Time Condition.
> - To keep the time condition after overriding, see Disable automatic reset of time condition.

Related information

Allow Users to Override Time Condition by Feature Code
Allow Users to Override Time Condition on Operator Panel
Monitor Time Condition Status
Automatic Reset of Time Condition
Enable or Disable Automatic Reset of Time Condition

Monitor Time Condition Status

This topic describes how to set BLF keys on IP phones to monitor time condition status. In this way, users can know which time period the system is working and where inbound calls would be routed.

Background information

Users can monitor time condition status in the following ways:

Monitor time condition status on IP phone

For the users who want to monitor time condition status on their phones, you can set a BLF key for each user.

For more information, see the followings:

- Monitor time condition status for inbound calls (Global Business Hours)
- Monitor time condition status for inbound calls (Custom Business Hours)
- Monitor time condition status for inbound calls (Custom Time Periods)

Monitor time condition status on Operator Panel

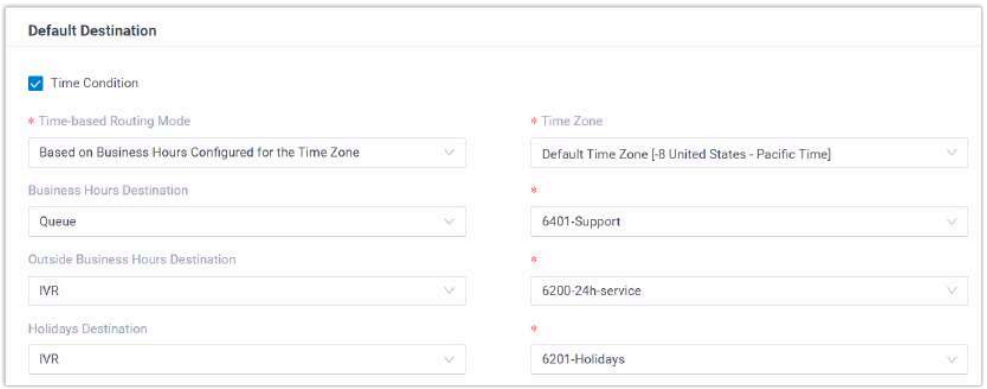
For the users who have permission to access Operator Panel, they can monitor time condition status on Operator Panel directly.

For more information, see Monitor Time Condition Status on Operator Panel.

Monitor time condition status for inbound calls (Global Business Hours)

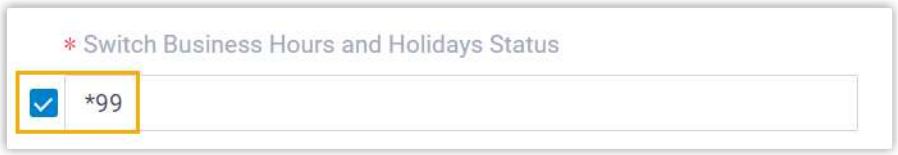
Background information

- An inbound route based on Business Hours configured in the system's default time zone is set up as follows:



- The feature code for **Switch Business Hours and Holidays Status** is *99.

> **Note:**
> This feature code applies only to the system's default time zone. For additional time zones, you can check the corresponding feature code under the specific time zone settings (Path: **Call Control > Business Hours and Holidays**).



Procedure

1. Assign function keys for extension users to monitor time condition status.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, click beside the desired extension.
   b. Click the **Function Keys** tab.
   c. Configure function keys.

   > **Note:**
   > The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

   - **Type**: Select **BLF**.
   - **Value**: Enter the feature code of **Switch Business Hours and Holidays Status**. In this example, enter `*99`.
   - **Label**: Optional. Enter a value, which will be displayed on the phone screen.

   d. Click **Save**.
2. If the extension has been provisioned and associated with a phone, reprovision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to this extension.
   c. In the pop-up window, click **OK** to reprovision the phone.
3. If the extension hasn't been associated with a phone, see the following topics to bind a phone with the extension.
   - Auto Provision IP Phones in Local Network (PnP Method)

- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

Result

The function key settings are automatically updated on the phone and different BLF LED indicates different status.

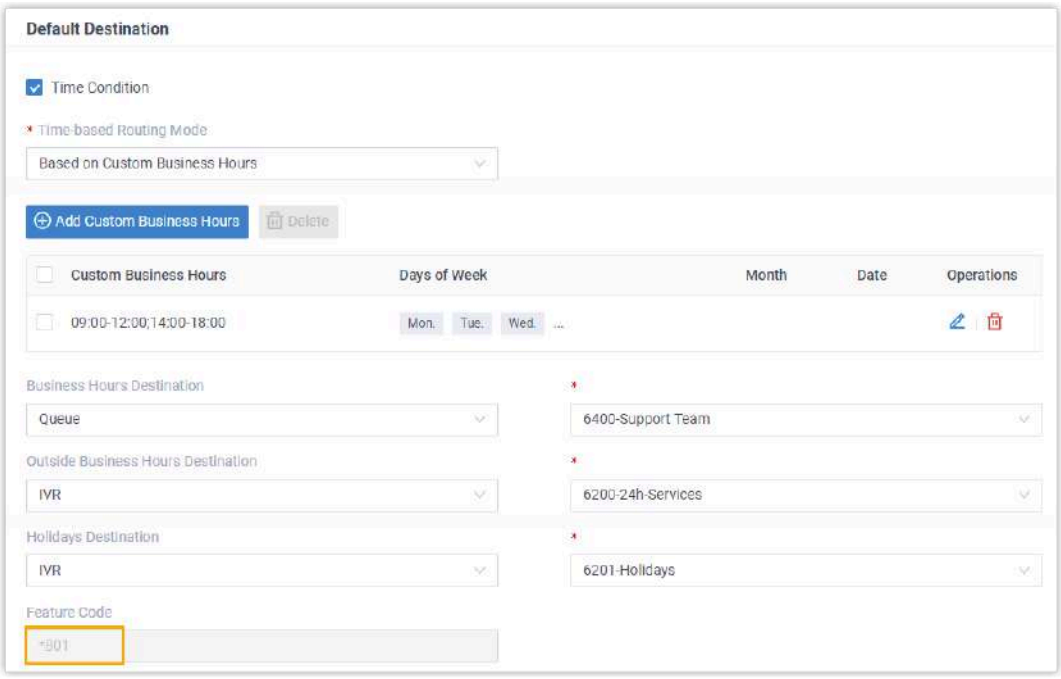
- **Red**: The system is in the status of **Business Hours**.
- **Green**: The system is in the status of **Outside Business Hours** or **Holidays**.
- **Off**: The BLF configurations are incorrect.

> **Note:**
> To change the BLF light color, go to **Call Features > Feature Code > Switch Business Hours and Holidays Status > BLF Light Color of Switching Global Business Hours Status**.

Monitor time condition status for inbound calls (Custom Business Hours)

Background information

An inbound route based on Custom Business Hours (follows the system's default time zone) is set up as follows:



Procedure

1. Assign function keys for extension users to monitor time condition status.
    a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, click beside the desired extension.
    b. Click the **Function Keys** tab.
    c. Configure function keys.

    > **Note:**
    > The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

    - **Type**: Select **BLF**.
    - **Value**: Enter feature code of the inbound route. In this example, enter `*801`.

- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

d. Click **Save**.

2. If the extension has been provisioned and associated with a phone, re-provision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to this extension.
   c. In the pop-up window, click **OK** to reprovision the phone.
3. If the extension hasn't been associated with a phone, see the following topics to bind a phone with the extension.
   - Auto Provision IP Phones in Local Network (PnP Method)
   - Auto Provision IP Phones in Local Network (DHCP Method)
   - Auto Provision IP Phones Remotely (RPS FQDN Method)
   - Auto Provision IP Phones Remotely (RPS Method)

Result

The function key settings are automatically updated on the phone and different BLF LED indicates different status.

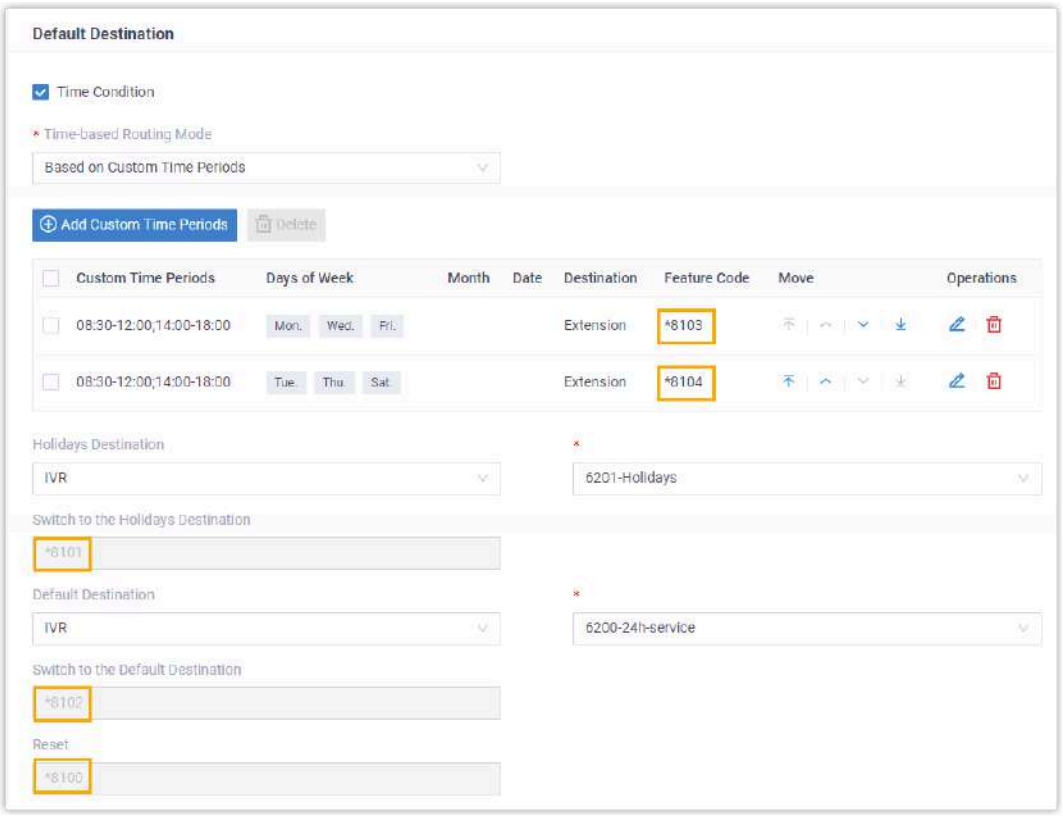
- **Red**: The system is in the status of **Business Hours**.
- **Green**: The system is in the status of **Outside Business Hours** or **Holidays**.
- **Off**: The BLF configurations are incorrect.

> **Note:**
> To change the BLF light color, go to **Call Features > Feature Code > Switch Business Hours and Holidays Status > BLF Light Color of Switching Global Business Hours Status**.

Monitor time condition status for inbound calls (Custom Time Periods)

Background information

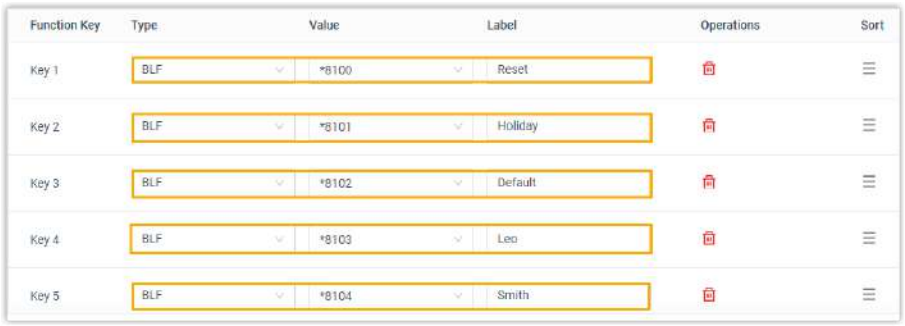
An inbound route based on Custom Time Periods (follows the system's default time zone) is set up as follows:



Procedure

1. Assign function keys for extension users to monitor time condition status.
    a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, click ✎ beside the desired extension.
    b. Click the **Function Keys** tab.
    c. Configure function keys.

> **Note:**
> The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.



- **Type**: Select **BLF**.
- **Value**: Enter the feature codes as needed.
- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

d. Click **Save**.

2. If the extension has been provisioned and associated with a phone, re-provision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to this extension.
   c. In the pop-up window, click **OK** to reprovision the phone.
3. If the extension hasn't been associated with a phone, see the following topics to bind a phone with the extension.
   - Auto Provision IP Phones in Local Network (PnP Method)
   - Auto Provision IP Phones in Local Network (DHCP Method)
   - Auto Provision IP Phones Remotely (RPS FQDN Method)
   - Auto Provision IP Phones Remotely (RPS Method)

Result

The function key settings are automatically updated on the phone and different BLF LED indicates different status.

- **Red**: The system is in the status of **Business Hours**.
- **Green**: The system is in the status of **Outside Business Hours** or **Holidays**.
- **Off**: The BLF configurations are incorrect.

> **Note:**
> - If the BLF key is set for **Reset** feature code, the BLF LED should be off.

◦ To change the BLF light color, go to **Call Features > Feature Code > Switch Business Hours and Holidays Status > BLF Light Color of Switching Global Business Hours Status**.

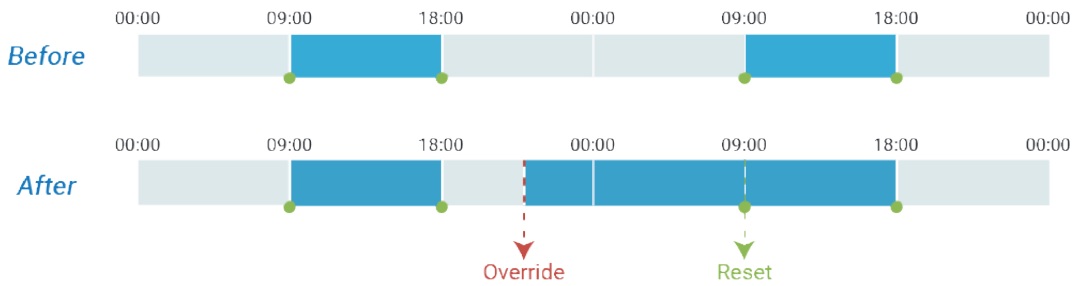
Automatic Reset of Time Condition

By default, if users have overridden time condition and don't clear the time condition override manually, PBX will automatically reset time condition in next period. The next period can be the starting point of business hours, outside business hours, or holidays. This topic gives examples to help you understand how the system automatically resets time condition.

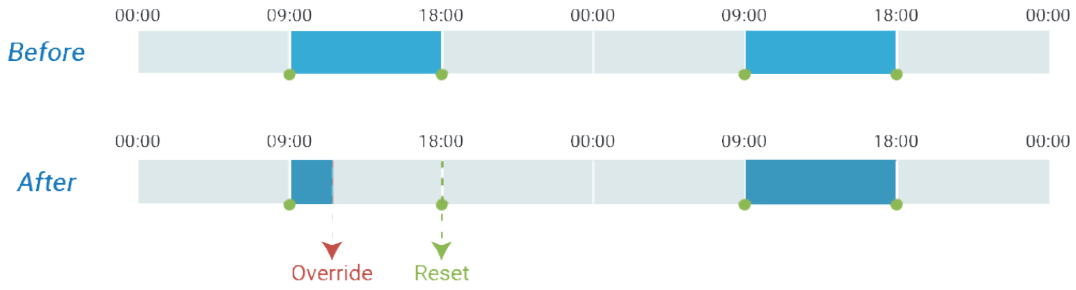
Examples for Global Business Hours/Custom Business Hours

	Business Hours
	Outside Business Hours
	Next hop of time condition: According to the time condition you configured, the system automatically switches the destination for incoming calls at the time point.
	Override time condition
	Automatically reset time condition

Example 1: Override to Business Hours



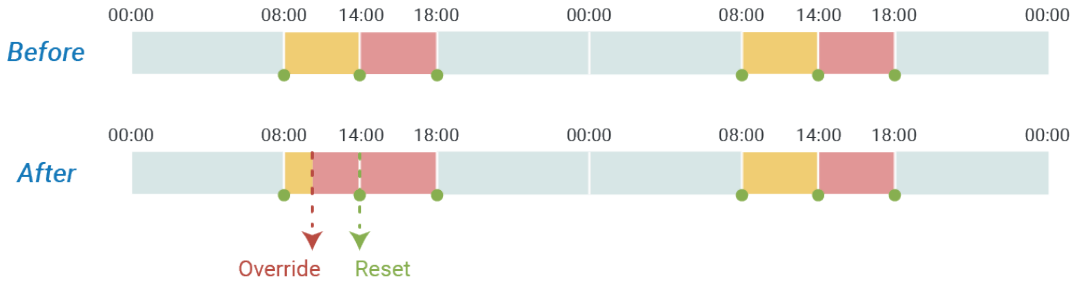
Example 2: Override to Outside Business Hours



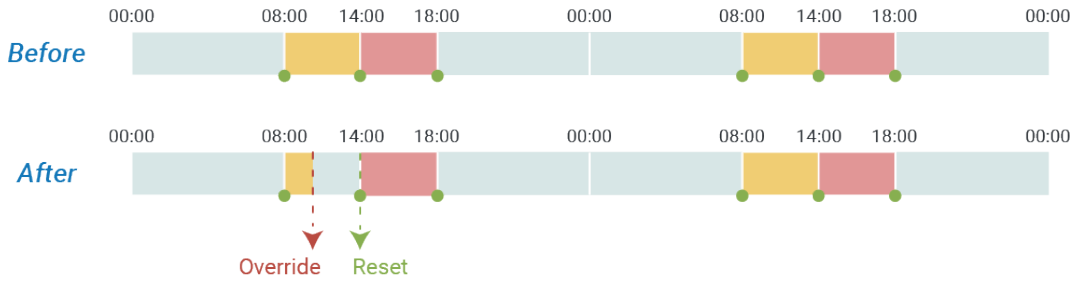
Examples for Custom Time Periods

	Time Period 1
	Time Period 2
	Outside Business Hours
	Next hop of time condition: According to the time condition you configured, the system automatically switches the destination for incoming calls at the time point.
	Override time condition
	Automatically reset time condition

Example 1: Override to Time Period 2



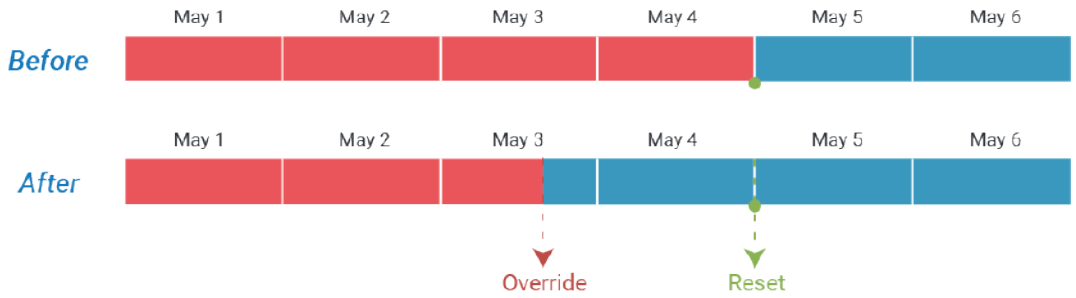
Example 2: Override to Outside Business Hours



Example for Holidays

	Business Hours
	Holidays
	Next hop of time condition (holiday or non-holiday): According to the time condition you configured, the system automatically switches the destination for incoming calls at the time point.
	Override time condition
	Automatically reset time condition

Example: Override to non-holiday



Related information

Enable or Disable Automatic Reset of Time Condition
Monitor Time Condition Status
Override Time Condition for Inbound Calls

Enable or Disable Automatic Reset of Time Condition

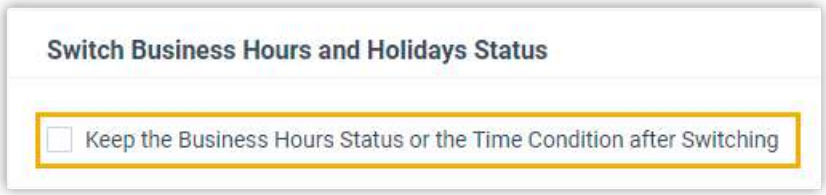
By default, if users have overridden time condition and don't clear the time condition override manually, PBX will automatically reset time condition in next period. You can decide whether to auto reset time condition or keep the time condition after overriding.

Enable automatic reset of time condition

To make the system go back to the normal schedule after users override time condition, follow the instructions below.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. Scroll down to **Switch Business Hours and Holidays Status** section.
3. Unselect the checkbox of **Keep the Business Hours Status or the Time Condition after Switching**.



4. Click **Save** and **Apply**.

Result

When it comes to the next starting point of business hours, outside business hours, or holidays, the system will reset time condition and go back to the normal schedule.

For more information, see Automatic Reset of Time Condition.

Disable automatic reset of time condition

To make the system keep the status after users override time condition, follow the instructions below.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. Scroll down to **Switch Business Hours and Holidays Status** section.

3. Select the checkbox of **Keep the Business Hours Status or the Time Condition after Switching**.

4. Click **Save** and **Apply**.

Result

After users override time condition, the system will stay in the state until someone manually clear the override.

> **Tip:**
> Tips for clearing the override:
>
> - For inbound route based on **Global Business Hours**, dial the feature code of **Switch Global Business Hours and Holidays Status**.
> - For inbound route based on **Custom Business Hours**, dial the feature code of corresponding inbound route.
> - For inbound route based on **Custom Time Periods**, dial the **Reset** feature code.

Related information

Override Time Condition for Inbound Calls
Monitor Time Condition Status

Inbound Route

Inbound Route Overview

An inbound route allows external callers to reach your system and routes the inbound calls to a specific destination based on the pre-configured rules and criteria.

Types of inbound call routing

Yeastar P-Series 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 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. In the **Trunk** section, select the desired trunks from **Available** box to **Selected** box.

   The PBX will route inbound calls through this inbound route when external users call the selected trunk number.
5. **Optional:** If you want to route inbound calls based on DID numbers, configure **DID Pattern**.

   The PBX will route inbound calls only when the callers dial the matched DID numbers.

   > **Note:**
   > Leave this field blank to match calls with any or no DID information.

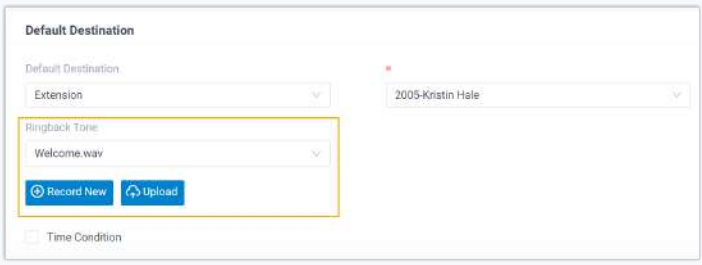
   For more information, see Route Inbound Calls based on DID Numbers.
6. **Optional:** If you want to route inbound calls based on Caller IDs, configure **Caller ID Pattern**.

   The PBX will route inbound calls only when the Caller IDs match the Caller ID pattern.

   > **Note:**
   > Leave this field blank to match calls with any or no Caller ID info.

   For more information, see Route Inbound Calls based on Caller ID.
7. Configure the inbound route destination.

   > **Note:**
   > When the destination is set to an extension, you can select or upload a music in the follow-up **Ringback Tone** field, which will be played to the caller before the extension user answers the call.



- If you want to route inbound calls to one destination whenever the calls reach the system, perform the following operations:
  a. Keep the **Time Condition** unselected.
  b. Configure the **Default Destination**.
- If you want to route inbound calls to different destinations based on the time, perform the following operations:
  a. Select the checkbox of **Time Condition**.
  b. Select an option from the drop-down list of **Time-based Routing Mode**.
  c. Configure the destinations based on the time.

     If an inbound call reaches the PBX during the time period, PBX will route the call to the selected destination.
  d. **Optional:** If you want to route inbound calls based on the business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**.

     Inbound calls during holiday will be distributed to other destinations according to your office hour setting.
  e. **Optional:** To play a prompt to callers before routing the inbound calls to the holiday destination, select the checkbox of **Play Holiday Prompt During Holidays**.

     Note:
     Make sure that you have set a prompt for the holiday (Path: **Call Control > Business Hours and Holidays > Holidays > Type > Prompt**). Otherwise, the inbound calls will be directly routed to the holiday destination without playing a prompt.

  For more information of inbound call routing based on time, see the following topics:

  - Route Inbound Calls based on Business Hours

    - Route Inbound Calls based on Department Hours
    - Route Inbound Calls based on Employee Hours

8. **Optional:** To receive faxes through this inbound route, enable **Fax Detection** and configure the fax destination.
    - **Extension**: The faxes will be sent to the selected extension. You need to register the extension on a SIP compatible fax machine.

      > **Note:**
      > If the selected extension is deleted, the fax destination will automatically jump to **Hang up**, and faxes cannot be received through this inbound route.

    - **Fax to Email**: The faxes will be converted to email attachments and be sent to an extension's email address.

      > **Note:**
      > Make sure the system email is configured correctly, or **Fax to Email** will fail to work.

    For more information of fax setting, see Fax Overview.
9. Click **Save** and **Apply**.

Time Based Inbound Routes

Route Inbound Calls based on Business Hours

This topic gives a configuration example to describe how to configure inbound route to control inbound calls based on Business Hours in a specific time zone, which can be applied to most of the employees.

Background information

Assume that your company's business hours are as follows:

- **Working days**: Monday to Friday
- **Business hours**: 09:00-12:00 and 14:00-18:00

When customers call in the trunk 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, and play a prompt "office_holiday".
- For other time periods, route inbound calls to a voicemail.

Prerequisites

- The trunk for inbound calling has been set up and is ready for use.
- Business Hours is configured according to your company's business hours.
- The desired destination of the inbound route has been configured on the system.

  In this scenario, an IVR for business hours, an IVR for holiday should be preconfigured.

  For more information of IVR, see Set up an IVR.
- If you want to play a prompt to customers when they make calls to the trunk during holidays, a prompt should be preconfigured.

  In this scenario, a prompt "office_holiday" is preconfigured.

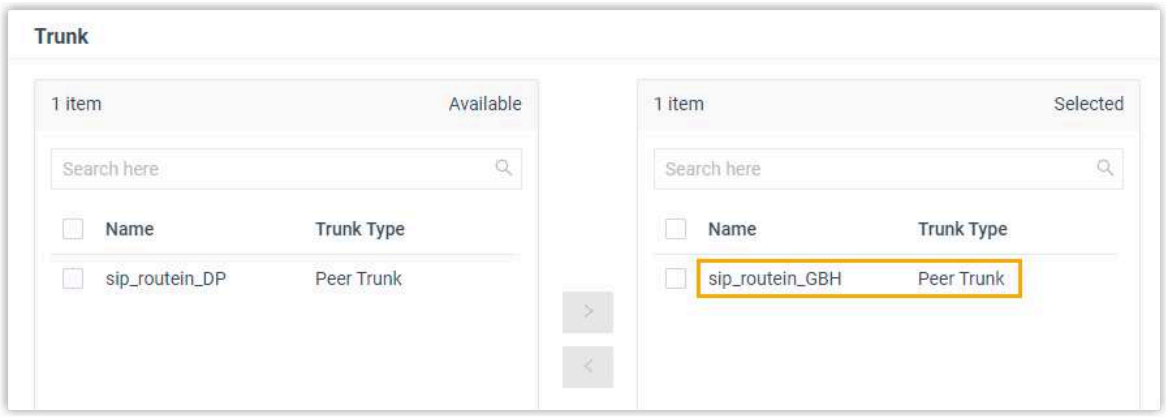
  For more information, see Create a Holiday.
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always directed to your desired destination.

  How to configure inbound route based on DID numbers, see Route Inbound Calls based on DID Numbers.

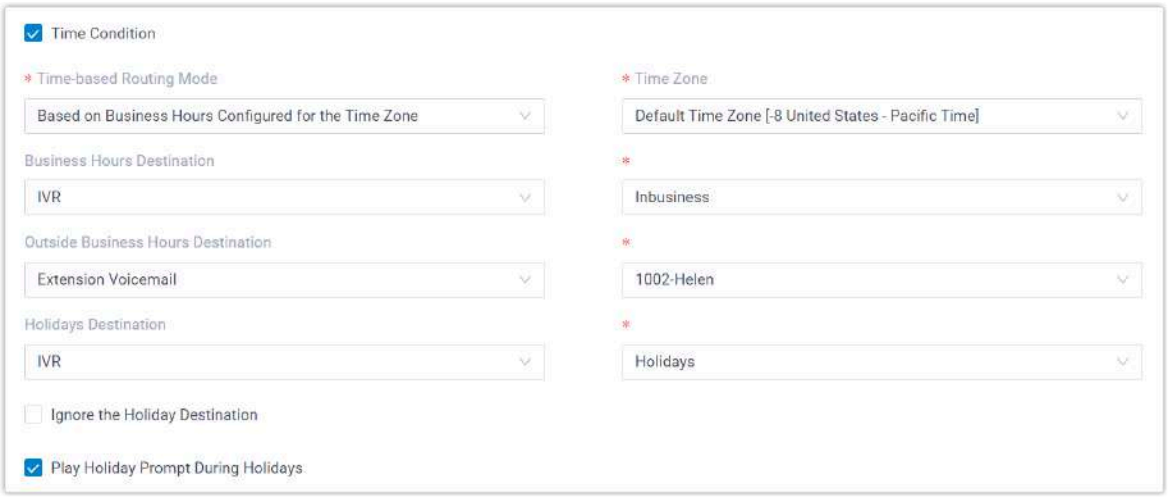
Procedure

1. Log in to PBX web portal, go to **Call Control > Inbound Route**, click **Add**.
2. In the **Name** field, enter a name to help you identify it.
3. In the **Trunk** section, select the desired trunks from **Available** box to **Selected** box.

   In this scenario, select the trunk 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 Business Hours Configured for the Time Zone**, then select the specific time zone.
   c. Configure the following destinations based on the time.
      - **Business Hours Destination**: Select the destination for inbound calls during the business hours configured for the selected time zone.

        In this scenario, select **IVR**, and select the IVR for business hours.
      - **Outside Business Hours Destination**: Outside Business Hours is the time periods that are not defined as Business Hours or Holidays.

        In this scenario, select **Extension Voicemail** then select an extension number.

- **Holidays Destination**: Select the destination for inbound calls during holidays configured for the selected time zone.

  In this scenario, select **IVR**, and select the IVR for holidays.

d. Select the checkbox of **Play Holiday Prompt During Holidays**.

   In this scenario, the system will play the prompt "office_holiday" before routing inbound calls to the holiday destination.

5. Click **Save** and **Apply**.

Result

When customers make calls to the phone number of the selected trunk 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 provides a configuration example on how to configure inbound routes for departments working in different time periods from the company's global business hours, based on the system's default time zone, and control the call destinations accordingly.

Scenarios

The employees in the branch office's support department have different business hours from the head office. The department hours is listed as below:

- **Working days**: Monday to Friday
- **Business hours**: 21:00 - 23:00 and 00:00 - 05:00

When customers call in the trunk 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, and play a prompt "office_holiday".

- For other time periods, route inbound calls to a voicemail.

Prerequisites

- The trunk for inbound calling has been set up and is ready for use.
- The desired destination of the inbound route should be configured on the system.

  In this scenario, a queue and an IVR for holiday should be preconfigured.

  For more information about the configurations of queue and IVR, see Create a Queue and Set up an IVR.
- If you want to play a prompt to customers when they make calls to the trunk during holidays, a prompt should be preconfigured.

  In this scenario, a prompt "office_holiday" is preconfigured.

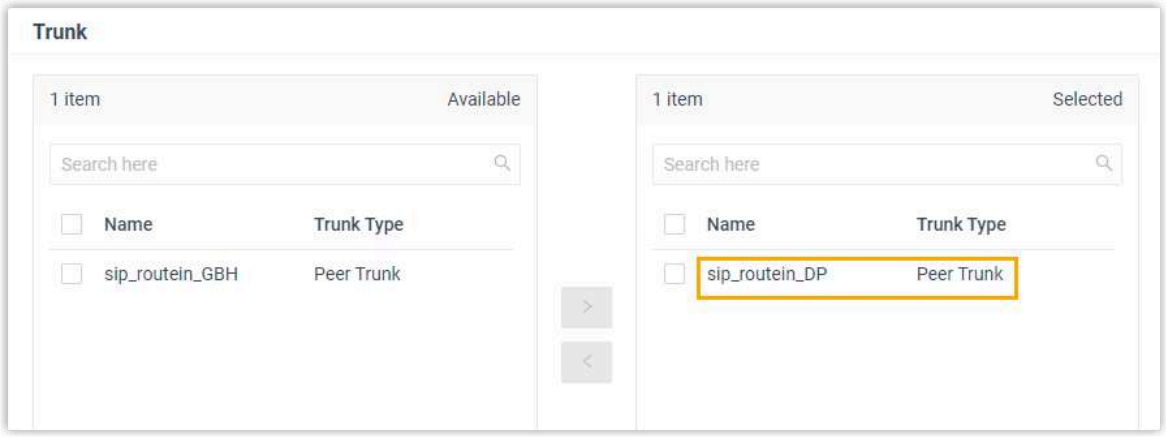
  For more information, see Create a Holiday.
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always directed to your desired destination.

  How to configure inbound route based on DID numbers, see Route Inbound Calls based on DID Numbers.

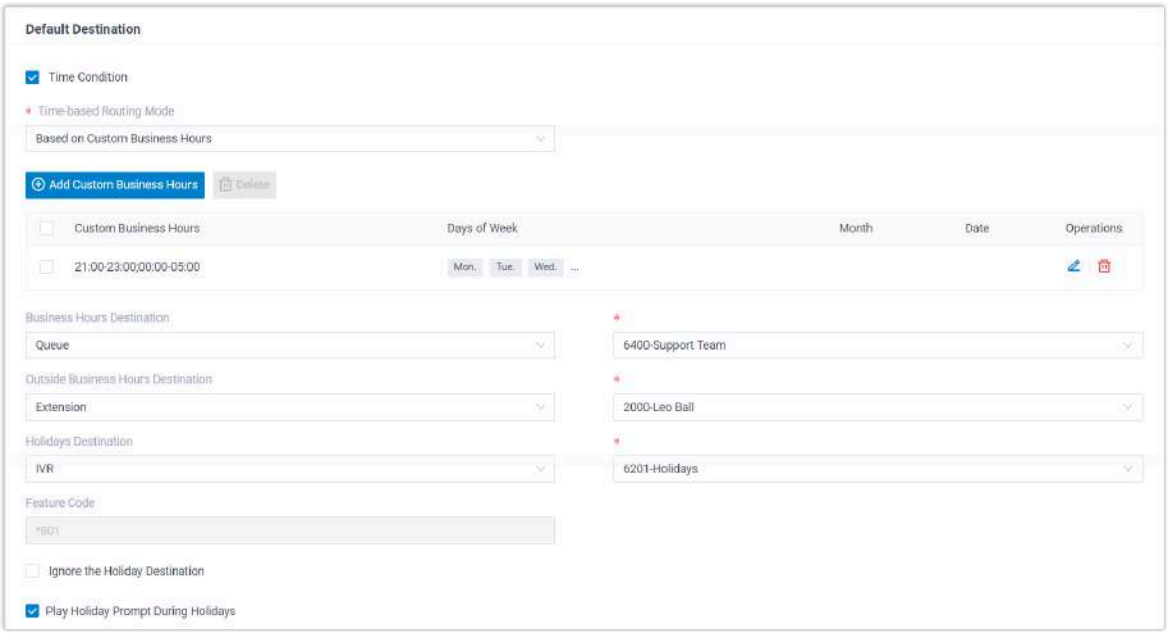
Procedure

1. Log in to PBX web portal, go to **Call Control > Inbound Route**, click **Add**.
2. In the **Name** field, enter a name to help you identify it.
3. In the **Trunk** section, select the desired trunks from **Available** box to **Selected** box.

   In this scenario, select the trunk sip_routein_DP.



4. In the **Default Destination** section, complete the following operations:



a. Select the checkbox of **Time Condition**.
b. In the drop-down list of **Time-based Routing Mode**, select **Based on Custom Business Hours**.
c. Configure custom business hours based on the system's default time zone.
    i. Click **Add Custom Business Hours**.
    ii. In the **Custom Business Hours** section, click **Add** to add business hours.

    In this scenario, add two business hours, 21:00 - 23:00 and 00:00 - 05:00.
    iii. In the **Date Settings** section, select working days.

    In this scenario, select **Days of Week** and select days from Monday to Friday.
    iv. Click **Confirm**.
d. Configure the following destinations based on the time.
    - **Business Hours Destination**: Select the destination for inbound calls during business hours set above.

      In this scenario, select **Queue**, and select the Queue "Support Team".
    - **Outside Business Hours Destination**: Outside Business Hours is the time periods that are not defined as Business Hours or Holidays.

      In this scenario, select **Extension Voicemail**, and select an extension.
    - **Holidays Destination**: Select the destination for inbound calls during holidays configured in the system's default time zone.

In this scenario, select **IVR**, and select the IVR for holidays.

e. Select the checkbox of **Play Holiday Prompt During Holidays**.

In this scenario, the system will play the prompt "office_holiday" before routing inbound calls to the holiday destination.

5. Click **Save** and **Apply**.

Result

- When customers make calls to the phone number of the selected trunk 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 Business Hours
Route Inbound Calls based on Employee Hours
Route Inbound Calls based on DID Numbers
Route Inbound Calls based on Caller ID
Route Inbound Calls by Matched Phonebook Contacts

Route Inbound Calls based on Employee Hours

This topic provides a configuration example on how to configure inbound route to control inbound calls for individual employees who have their own work schedules, based on the system's default time zone.

Scenarios

Duty doctors in a hospital are responsible for supporting emergency patient needs or arranging appointments for patients over phone calls.

- Each duty doctor has a different time schedule and will provide services based on the time schedule.
- During the time periods that no doctors are on duty or when it comes to a holiday, the incoming calls from patients will be routed to an IVR.

The following shows time schedule for the duty doctors.

Doctor Name	Time Schedule
Dr. Tommy Tse	Monday 07:00 -12:00 Friday 12:00 - 18:00
Dr. Eric Chan	Monday 00:00 - 07:00 Thursday 07:00 - 12:00

Prerequisites

- The trunk for inbound calling has been set up and is ready for use.
- The desired destination of the inbound route should be configured on the system.

  In this scenario, an IVR should be configured to ensure that patients can reach their desired services.

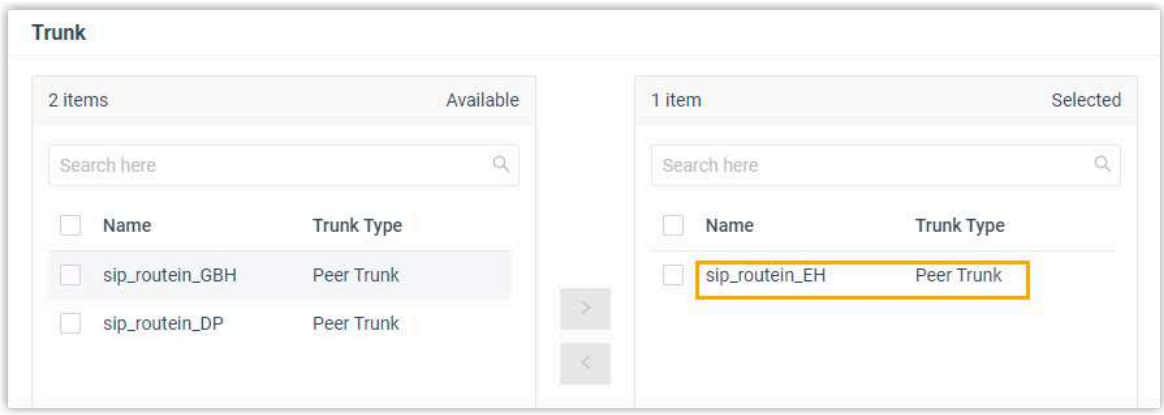
  For more information about IVR, see Set up an IVR.
- If you want to set up multiple inbound routes for different time schedules, each inbound route should be associated with a different trunk or a trunk with different DID numbers. In this way, the inbound calls can be always directed to your desired destination.

  How to configure inbound route based on DID numbers, see Route Inbound Calls based on DID Numbers.

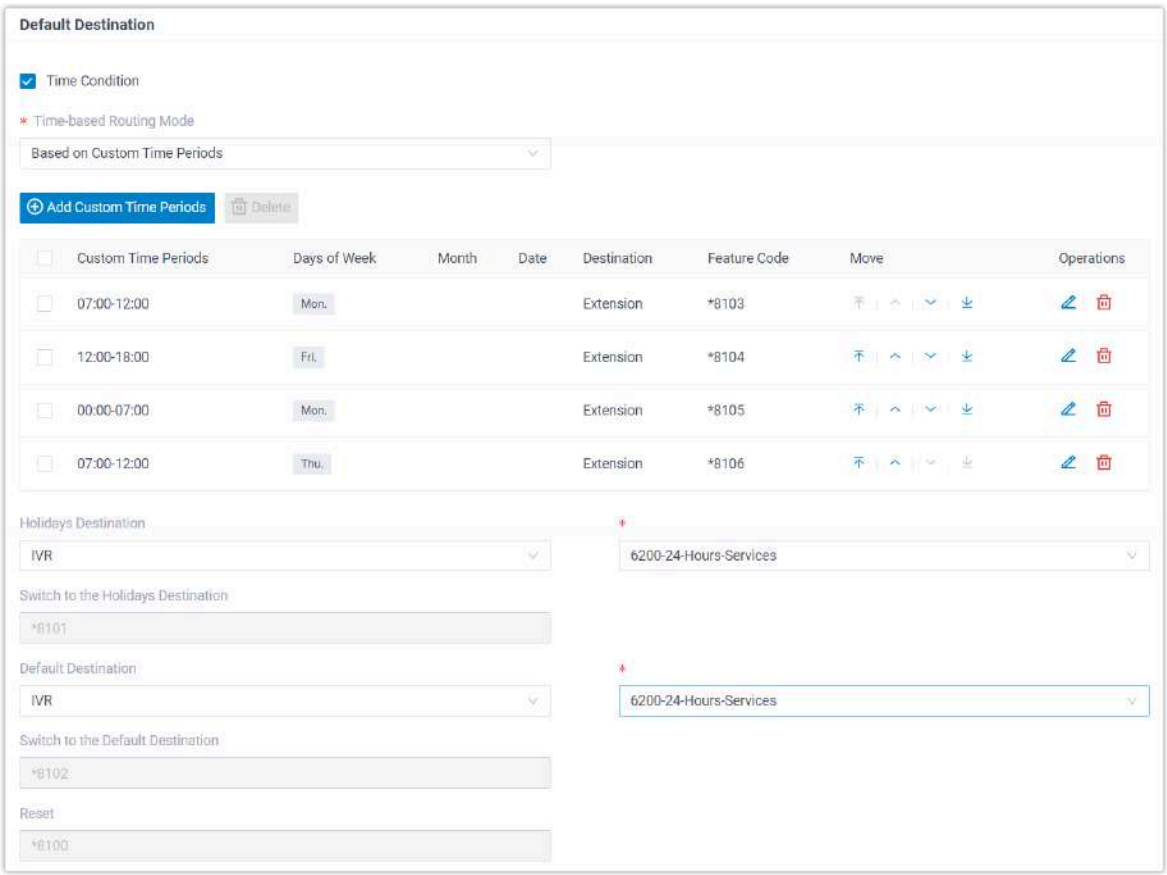
Procedure

1. Log in to PBX web portal, go to **Call Control > Inbound Route**, click **Add**.
2. In the **Name** field, enter a name to help you identify it.
3. In the **Trunk** section, select the desired trunks from **Available** box to **Selected** box.

   In this scenario, select the trunk sip_routein_EH.



4. In the **Default Destination** section, complete the following operations:



   a. Select the checkbox of **Time Condition**.
   b. In the drop-down list of **Time-based Routing Mode**, select **Based on Custom Time Periods**.
   c. Add time schedule for the duty doctors based on the system's default time zone.
      i. Click **Add Custom Time Periods**.

ii. In the pop-up window, click **Add** to add time periods, set relevant destinations, and select days of week.
iii. Click **Confirm**.
iv. Repeat **step i - iii** to add another time schedule.

In this scenario, add four time schedules as below.

Start Time	End Time	Days of Week	Destination
07:00	12:00	Monday	Tommy's extension
12:00	18:00	Friday	Tommy's extension
00:00	07:00	Monday	Eric's extension
07:00	12:00	Thursday	Eric's extension

d. Configure the **Holidays Destination**.

In this scenario, select **IVR**, and select an IVR to guide patients.

e. Configure the **Default Destination**.

In this scenario, select **IVR**, and select an IVR to guide patients.

5. Click **Save** and **Apply**.

Result

- When external users make calls to the selected trunk 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.

> **Tip:**
> The authorized users can dial a specific feature code to override time condition and route inbound calls to corresponding destinations. For more information, see Override Time Condition for Inbound Calls.

  - One feature code for each time period.

- A **Switch to the Holidays Destination** feature code that allows for switching destination of inbound calls to **Holidays**.
- A **Reset** feature code that allows for removing any overrides currently set.
- A **Switch to the Default Destination** feature code that allows for switching destination of inbound calls to the default destination.

Related information

Route Inbound Calls based on Business Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on DID Numbers
Route Inbound Calls based on Caller ID
Route Inbound Calls by Matched Phonebook Contacts

Caller ID/DID Based Inbound Routes

Route Inbound Calls based on DID Numbers

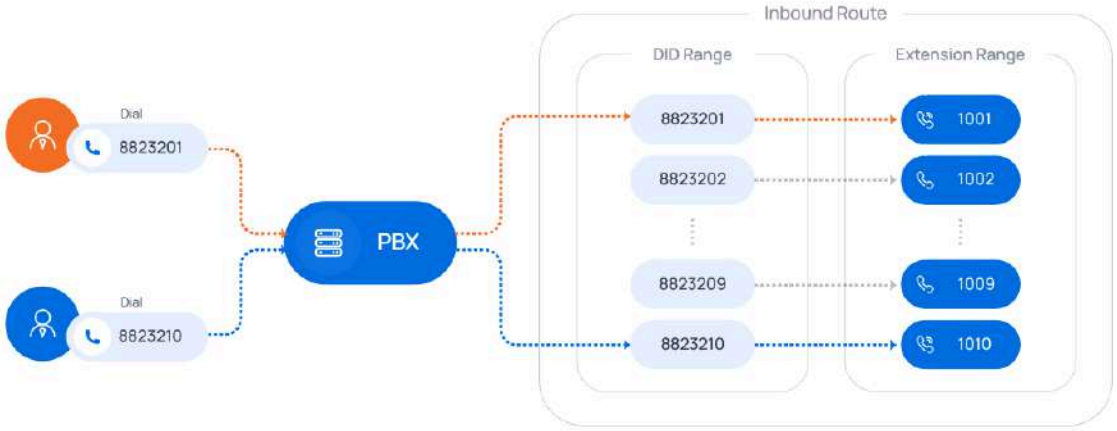
This topic gives configuration examples to describe how to route inbound calls based on the dialed numbers (also called DID numbers).

DID routing modes

Yeastar P-Series Software Edition provides four DID matching modes to help you route inbound calls based on DID numbers.

- **Match DID Range to Extension Range**

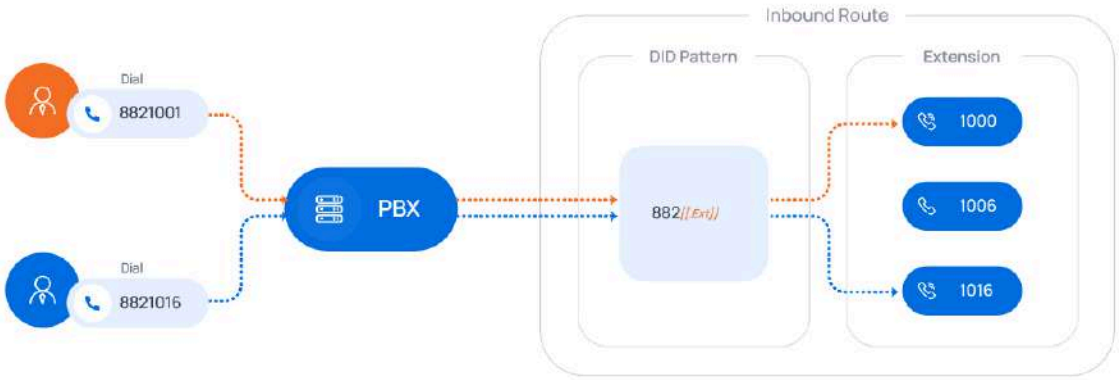
  Match DID Range and Extension Range in a one-to-one correspondence with sequential order.



For more information, see the configuration example Route calls to extension users by matching DID range.

- **Match DID Pattern to Extensions**

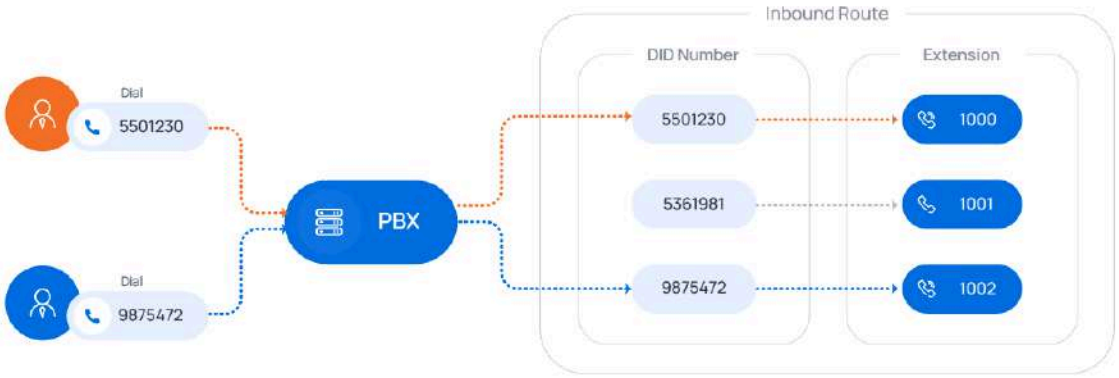
  Use the variable `{{.Ext}}` to match extension number in the DID pattern.



For more information, see the configuration example Route calls to extension users by matching DID patterns.

- **DID Number to Specific Extension**

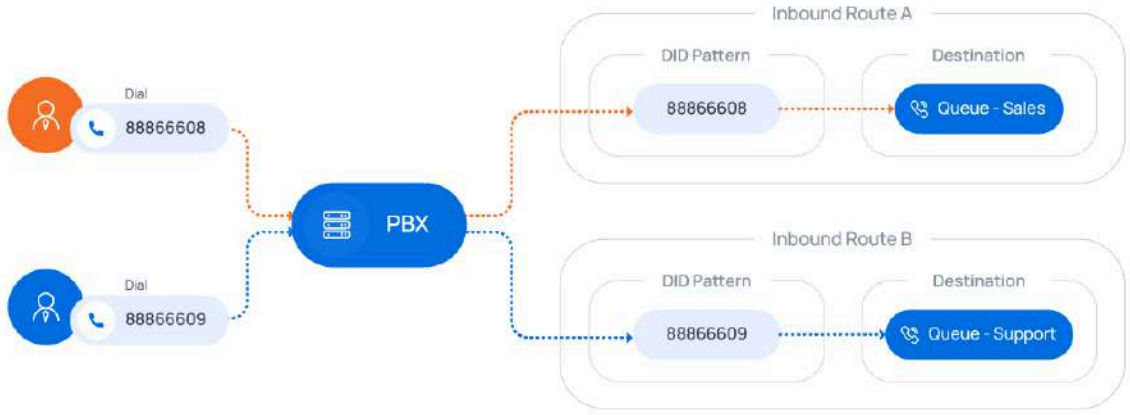
  The inbound calls that match the defined DID number(s) will be routed to the specified extension(s) in one-to-one correspondence.



For more information, see the configuration example Route calls to extension users by matching specific DID numbers.

- **DID Pattern**

  The inbound calls that match the defined DID number(s) or pattern(s) will be routed to a defined destination.



For more information, see the configuration example Route calls to different destinations by matching DID patterns.

Route calls to extension users by matching DID range

Scenario

Company ABC purchases a SIP trunk, and gets 10 DID numbers that are in order: 8823201-8823210.

The company wants to redirect inbound calls to specific extensions based on the provided DID numbers as follows:

Table 18.

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

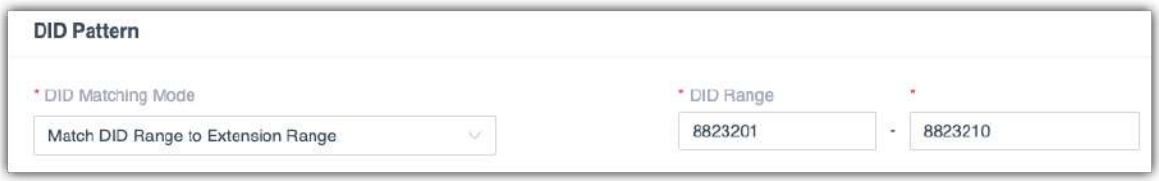
- You have purchased DID numbers from the trunk provider.
- The trunk for inbound calling has been set up and is ready for use.

Configuration example

According to this scenario, configure an inbound route based on the DID ranges as follows:

- **Name**: Enter a name to help you identify it.
- **Trunk**: Select the trunk that binds the DID numbers.
- **DID Pattern**:
  - **DID Matching Mode**: Select **Match DID Range to Extension Range**.
  - **DID Range**: Select or enter the start number and the end number of the DID range.

    In this scenario, enter *8823201* and *8823210*.



- **Caller ID Pattern**: Leave it blank, which means no limit on the inbound caller ID.
- **Default Destination**: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this scenario, route inbound calls to the default destination whenever the calls reach the system.

  - **Default Destination**: Select **Match Extension Range**, and enter the extension range *1001 - 1010*.

    > **Note:**
    > The DID range and extension range should have the same size (for example, DID range 991000-991003 and the extension range 1000-1003 have the same size).

  - **Time Condition**: Unselected.

- **Fax Detection**: Leave the settings as default.

Result

When an external user dials a number that is in the DID range, the user can reach a corresponding extension user directly.

For example, if an external user dials 8823201, the call goes to the extension 1001 directly.

Route calls to extension users by matching DID patterns

Scenario

Company ABC purchases a SIP trunk, and gets 3 DID numbers as follows.

- 8821001, 8821006, 8821016

The company wants to redirect inbound calls to specific extensions based on the provided DID numbers as follows:

Note:
The provided DIDs have the following characteristics:

- Not consecutive
- Each DID number consists of a string of fixed digits and a specific extension number.

Table 19.

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 DID patterns as follows:

- **Name**: Enter a name to help you identify it.
- **Trunk**: Select the trunk that binds the DID numbers.

  In this scenario, select **siptrunk**.
- **DID Pattern**:

  - **DID Matching Mode**: Select **Match DID Pattern to Extensions**.
  - **DID Pattern**: Enter the DID pattern according to the provided DIDs.

    In this scenario, enter *882{{.Ext}}*.

    > **Note:**
    > - *{{.Ext}}* is a variable that will match the destination extension.
    > - The wildcard `.` and `!` are not allowed.
    > - Only one DID pattern is allowed.

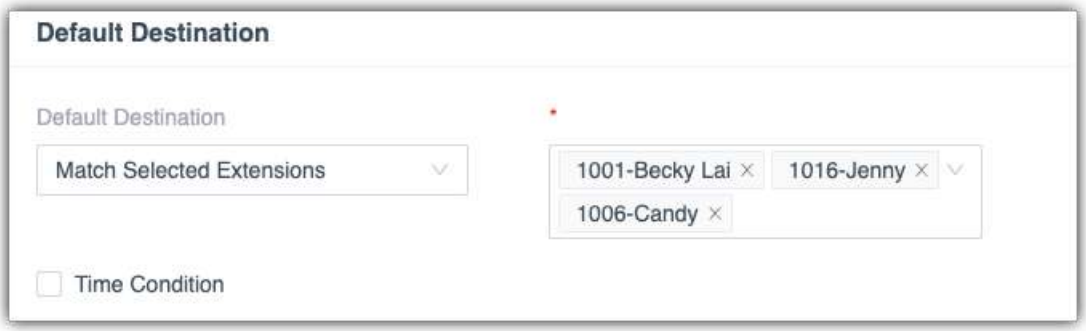
    

- **Caller ID Pattern**: Leave it blank, which means no limit of inbound caller ID.
- **Default Destination**: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this scenario, route inbound calls to the default destination whenever the calls reach the system.

  - **Default Destination**: Select **Match Selected Extensions**, and select extensions.

    In this scenario, select extension 1001, 1006, and 1016.
  - **Time Condition**: Unselected.

- **Fax Detection**: Leave the settings as default.

Result

When an external user dials a number that matches the DID pattern, the user can reach a specific extension user directly.

For example, if the external user dials 8821001, the call goes to the extension 1001 directly.

Route calls to extension users by matching specific DID numbers

Scenario

Company ABC purchases a SIP trunk, and gets 3 DID numbers as follows.

- 5501230, 5361981, 9875472

The company wants to redirect inbound calls to specific extensions based on the provided DID numbers as follows:

Table 20.

DID Number	Extension Number
5501230	1000
5361981	1001
9875472	1002

Prerequisites

- You have purchased DID numbers from the trunk provider.
- The trunk for inbound calling has been set up and is ready for use.

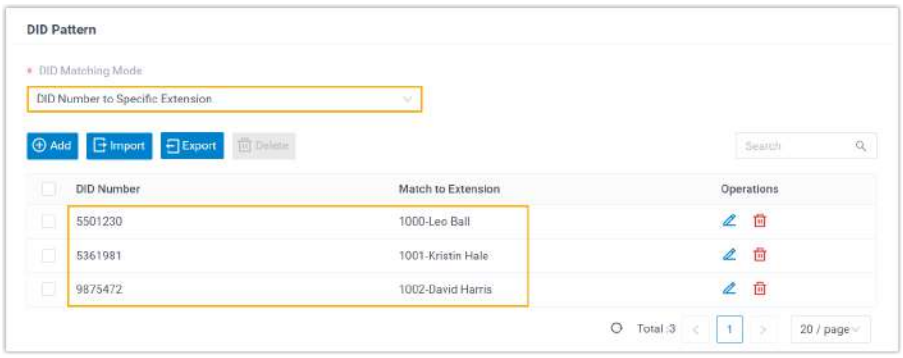
Configuration example

According to this scenario, configure an inbound route based on the specific DID numbers as follows:

- **Name**: Enter a name to help you identify it.
- **Trunk**: Select the trunk that binds the DID numbers.
- **DID Pattern**:
  - **DID Matching Mode**: Select **DID Number to Specific Extension**.
  - **DID Number**: Click **Add** and set up the DID number matching rules.

> **Tip:**
> You can also click **Export** to export the DID number matching rule to a CSV file first, use the file as a template to add DID number matching rules in bulk, then import the file into the inbound route. Refer to DID Number to Specific Extension Parameters to edit the parameters in the CSV file.

In this example, the configuration is as follows:



- **Caller ID Pattern**: Leave it blank, which means no limit on the inbound caller ID.
- **Default Destination**: Decide whether to route the inbound calls to different destinations based on time and configure the destinations.

  In this example, the configuration is as follows:

  - **Default Destination**: Select **DID Number to Specific Extension**.
  - **Time Condition**: Unselected.

- **Fax Detection**: Leave the settings as default.

Result

When an external user dials a number that equals to the DID number, the user can reach a specific extension user directly.

For example, if the external user dials 9875472, the call goes to the extension 1002 directly.

Route calls to different destinations by matching DID patterns

Scenario

Company ABC purchases a SIP trunk, and gets 2 DID numbers as follows.

- 88866608
- 88866609

The company wants to assign the two DID numbers to support team and sales team.

- When external users call 88866609, the calls go directly to support team.
- When external users call 88866608, the calls go directly to sales team.

Prerequisites

- You have purchased DID numbers from the trunk provider.
- The trunk for inbound calling has been set up and is ready for use.

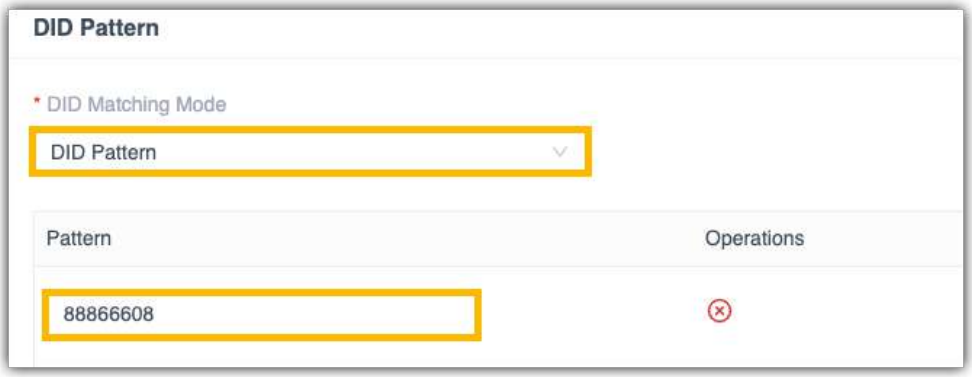
Configuration example

Set up two inbound routes to route calls to different destinations based on DID numbers.

Inbound Route for sales team

- **Name**: Enter a name to help you identify it.
- **Trunk**: Select the trunk that binds the DID numbers.
- **DID Pattern**:
  - **DID Matching Mode**: Select **DID Pattern**.
  - **DID Patterns**: Click **Add** and enter a DID pattern or a DID number.

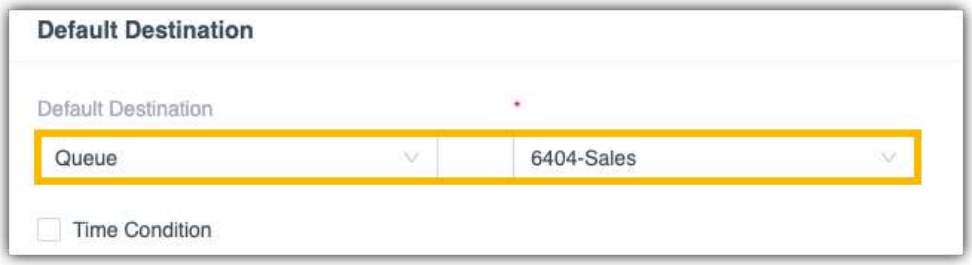
    In this scenario, enter *88866608*.



- **Caller ID Pattern**: Leave it blank, which means no limit of inbound caller ID.
- **Default Destination**: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this example, route inbound calls to the default destination whenever the calls reach the system.

  - **Default Destination**: Select the destination to the queue of sales team.
  - **Time Condition**: Unselected.

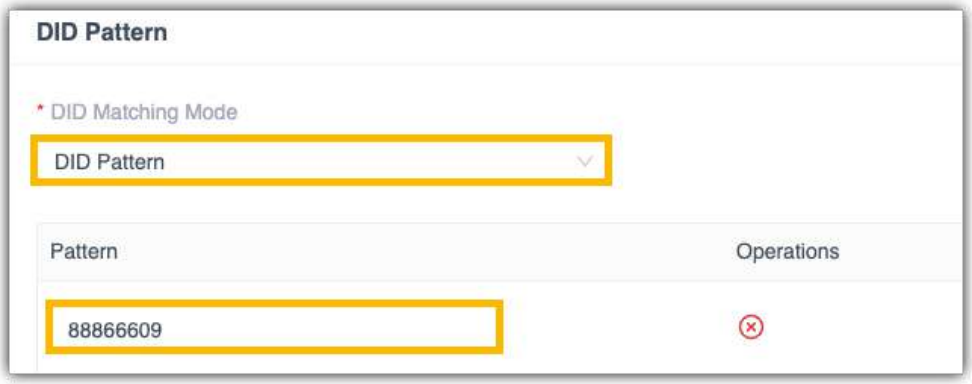


- **Fax Detection**: Leave the settings as default.

Inbound Route for support team

- **Name**: Enter a name to help you identify it.
- **Trunk**: Select the trunk that binds the DID numbers.
- **DID Pattern**:
  - **DID Matching Mode**: Select **DID Pattern**.
  - **DID Patterns**: Click **Add** and enter a DID pattern or a DID number.

    In this scenario, enter *88866609*.



- **Caller ID Pattern**: Leave it blank, which means no limit of inbound caller ID.
- **Default Destination**: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this example, route inbound calls to the default destination whenever the calls reach the system.

  - **Default Destination**: Select the destination to the queue of support team.
  - **Time Condition**: Unselected.

- **Fax Detection**: Leave the settings as default.

Result

External users will reach different teams according to the DID numbers they dial.

Related information

Route Inbound Calls based on Business Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on Employee Hours
Route Inbound Calls based on Caller ID
Route Inbound Calls by Matched Phonebook Contacts

Route Inbound Calls based on Caller ID

Caller ID routing connects external callers with the appropriate party quickly. This topic gives a configuration example to describe how to route calls by a caller-ID-based inbound route.

Scenarios

Company ABC is a Chinese company that provides consulting services around multiple cities.

For better customer experience, the company has a countrywide toll-free number 400-661-8815 and has multiple teams to provide professional services for customers from different regions.

For example, the following two teams will handle inbound calls based on different caller IDs.

Table 21.

Team	Responsible Region	Area Code
Team-A	Fujian	• 0591 • 0592 • 0593 • 0594 • 0595 • 0596 • 0597 • 0598 • 0599
Team-B	Guangdong	• 0662 • 0663 • 0668 • 0660

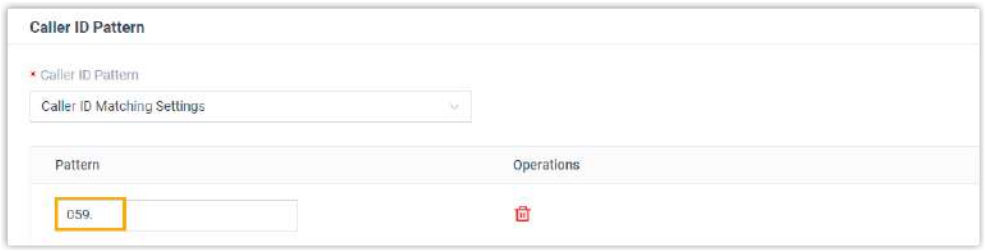
Configuration Example

Set up two inbound routes to route calls to different destinations based on caller IDs.

Inbound Route for Team-A

- **Name**: Enter a name to help you identify it.
- **DID Pattern**: Leave it blank, which means no limit of DID numbers.
- **Caller ID Pattern**: Select **Caller ID Matching Settings**, click **Add** and enter a Caller ID pattern or a full Caller ID.

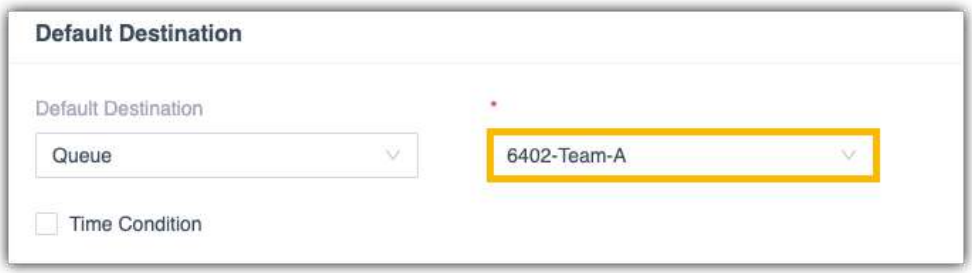
In this scenario, enter `059.`, which matches all inbound caller IDs that start with digit 059. For more information of Caller ID pattern, see DID Pattern and Caller ID Pattern.



- **Trunk**: Select the trunk that users will call in.
- **Default Destination**: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this example, route inbound calls to the default destination whenever the calls reach the system.

  - **Default Destination**: Select the destination to the queue of Team-A.
  - **Time Condition**: Unselected.

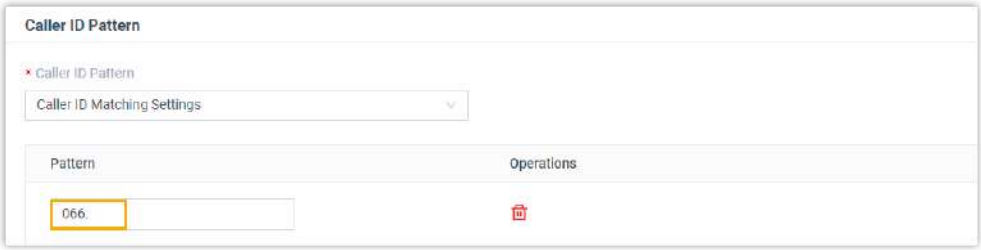


- **Fax Detection**: Leave the settings as default.

Inbound Route for Team-B

- **Name**: Enter a name to help you identify it.
- **DID Pattern**: Leave it blank, which means no limit of DID numbers.
- **Caller ID Pattern**: Select **Caller ID Matching Settings**, click **Add** and enter a Caller ID pattern or a full Caller ID.

  In this scenario, enter `066.`, which matches all inbound Caller IDs that start with digit 066. For more information of Caller ID pattern, see DID Pattern and Caller ID Pattern.

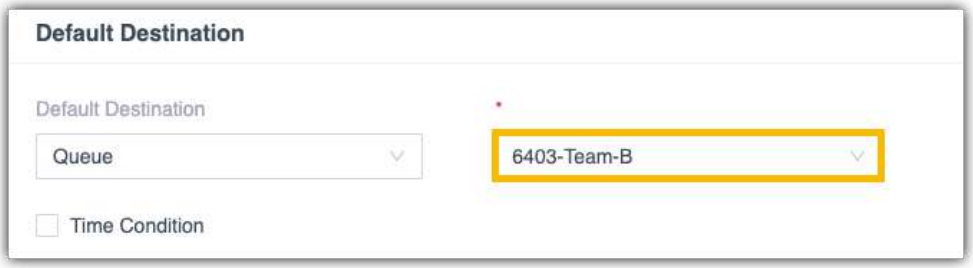


- **Trunk**: Select the trunk that users will call in.

  In this example, select **siptrunk**, whose phone number is 400-661-8815.
- **Default Destination**: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this example, route inbound calls to the default destination whenever the calls reach the system.

  - **Default Destination**: Select the destination to the queue of Team-B.
  - **Time Condition**: Unselected.



- **Fax Detection**: Leave the settings as default.

Result

- When users from Fujian dial the number 400-661-8815, agents in Team-A will handle the calls.
- When users from Guangdong dial the number 400-661-8815, agents in Team-B will handle the calls.

Related information

Route Inbound Calls based on Business Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on Employee Hours
Route Inbound Calls based on DID Numbers
Route Inbound Calls by Matched Phonebook Contacts

Route Inbound Calls by Matched Phonebook Contacts

After grouping company contacts into phonebooks, you can set up inbound routes to distribute inbound calls from contacts to different destinations based on phonebooks.

Prerequisites

- You have added phonebooks and enabled **Caller ID Match** feature.

  For more information, see Add and Manage Company Phonebooks and Identify Callers from Contacts.

Scenario

Company ABC has a Sales Team and a Support Team, both teams have their own customer groups. System administrator has added the customer information into two phonebooks.

Table 22.

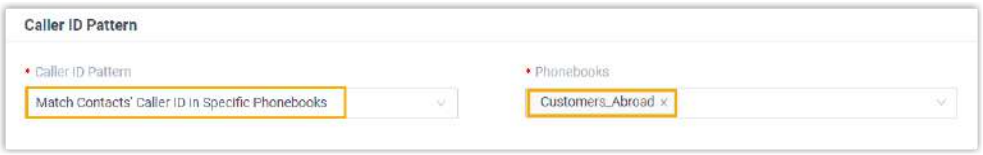
Team	Phonebook
Sales Team (Queue 6401)	Customers_Abroad
Support Team (Queue 6402)	Customers_China

Configuration Example

To distribute inbound calls from customers to corresponding team, you can set up two inbound routes to route calls by matching contacts in different phonebooks.

Inbound Route for Sales Team

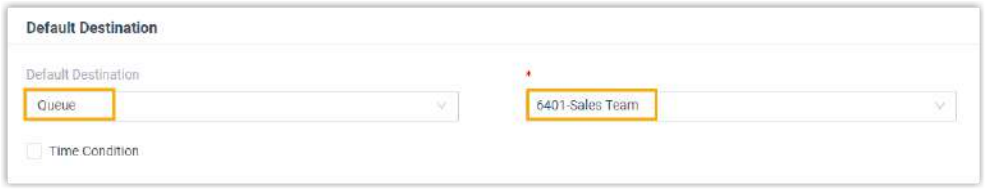
- **Name**: Enter a name to help you identify it.
- **DID Pattern**: Leave it blank, which means no limit of DID numbers.
- **Caller ID Pattern**: Select **Match Contacts' Caller ID in Specific Phonebooks** and select the phonebook **Customers_Abroad**.



- **Trunk**: Select the trunk that contacts will call in.
- **Default Destination**: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

In this example, route inbound calls to the default destination whenever the calls reach the system.

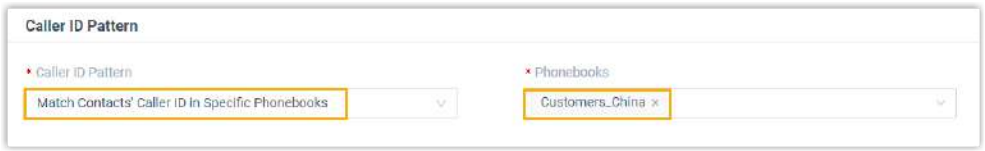
- **Default Destination**: Select the destination to **Queue** and select the Sales Team.
- **Time Condition**: Unselected.



- **Fax Detection**: Leave the settings as default.

Inbound Route for Support Team

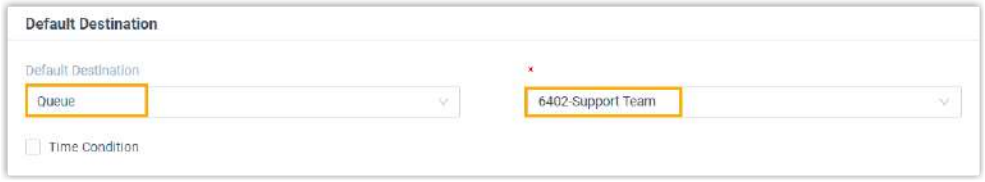
- **Name**: Enter a name to help you identify it.
- **DID Pattern**: Leave it blank, which means no limit of DID numbers.
- **Caller ID Pattern**: Select **Match Contacts' Caller ID in Specific Phonebooks** and select the phonebook **Customers_China**.



- **Trunk**: Select the trunk that contacts will call in.
- **Default Destination**: Decide whether to route inbound calls to different destinations based on time and configure the destinations.

  In this example, route inbound calls to the default destination whenever the calls reach the system.

  - **Default Destination**: Select the destination to **Queue** and select Support Team.
  - **Time Condition**: Unselected.



- **Fax Detection**: Leave the settings as default.

Result

- When customers from Phonebook 'Customers_Abroad' call to PBX, Sales Team will handle the calls.
- When customers from Phonebook 'Customers_China' call to PBX, Support Team will handle the calls.

Related information

Route Inbound Calls based on Caller ID
Route Inbound Calls based on DID Numbers
Route Inbound Calls based on Employee Hours
Route Inbound Calls based on Department Hours
Route Inbound Calls based on Business Hours

Manage Inbound Routes

After you create inbound routes, you can adjust the priority of the inbound routes. You can also edit or delete the inbound routes.

Adjust priority of inbound routes

A trunk can be selected to multiple inbound routes. When users call to a trunk that is selected in multiple inbound routes, the system will route inbound calls through the route with higher priority. You can adjust the priority of inbound routes according to your needs.

1. Log in to PBX web portal, go to **Call Control > Inbound Route**.
2. In the Inbound Route list, click  to adjust the priority of your inbound routes.

Edit an inbound route

1. Log in to PBX web portal, go to **Call Control > Inbound Route**.
2. Click  beside the inbound route that you want to edit.
3. Edit the inbound route.
4. Click **Save** and **Apply**.

Delete an inbound route

1. Log in to PBX web portal, go to **Call Control > Inbound Route**.

2. Click  beside the inbound route that you want to delete.
3. On the pop-up window, click **Yes** to confirm.
4. Click **Apply**.

Export and Import Inbound Routes

The inbound routes configured on Yeastar P-Series 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 **Call Control > Inbound Route**.
2. Click **Export**.

   A CSV file is saved to your computer. To check and edit parameters in the CSV file, see Inbound Route Parameters.

Import inbound routes

We recommend that you export inbound route data to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- **Format**: UTF-8.CSV
- **Size**: Less than 50 MB
- **File name**: Less than 127 characters
- **Import parameters**: Ensure that the import parameters meet requirements. For more information , see Inbound Route Parameters.

Procedures

1. Log in to PBX web portal, go to **Call Control > Inbound Route**.
2. Click **Import**.
3. In the pop-up window, click **Browse**, and select your CSV file.
4. Click **Import**.

The inbound routes in the CSV file will be displayed in the **Inbound Route** list.

Related information

Import and Export -FAQ

DID Pattern and Caller ID Pattern

This topic describes special characters that can be defined in a DID pattern or a Caller ID pattern, and provides examples to help you understand and configure the pattern.

Pattern

A **Pattern** field appears when you are configuring DID numbers or Caller IDs. The **Pattern** field allows you to enter a full number or special characters that will match specific numbers.

The following table shows descriptions of the allowed characters in the Pattern field.

Table 23.

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 24.

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 ⤒ ^ v ⤓ beside the **Selected** box to specify the default trunk sequence. By default, the system always selects an idle trunk from top to bottom, and uses the trunk to call out.
      - **Rrmemory Hunt**

        If the option **Rrmemory Hunt** is selected, the system will remember which trunk was used last time, and use the next idle trunk to call out.
   c. To enhance the outbound route security, configure the **Outbound Route Password**.
      - **Disable**: No password is required to call out through this outbound route.
      - **Single PIN**: Set a single PIN. All the users need to enter the same PIN to make outbound calls through this outbound route.
      - **PIN List**: Select a PIN list. Users are required to dial a password included in this list before an outbound call go through.

        > **Note:**
        > Generally, each user has a specific PIN code assigned by the administrator. For more information, see Add a PIN List.

5. Select which users are allowed to make calls through this outbound route.
   In the **Extension/Extension Group** section, select extensions, extension groups, or organizations from **Available** box to **Selected** box.

   > **Note:**
   > - Organizations are displayed only when you enable the **Organization Management** feature.
   > - By default, when you select an organization, its associated sub-organizations are selected. Be careful when selecting organizations.

6. **Optional:** In the **Time Condition** section, select an option from **Available Time** drop-down list to specify when this outbound route is available to use.
   - **Always**: This outbound route is available at any time for allowed extension users.
   - **Based on Business Hours Configured for the Time Zone**: Set up whether to allow this route in the following time separately:
     - **Business Hours**: Business Hours specified for the specific time zone.
     - **Holidays**: Holidays specified for the specific time zone.
     - **Outside Business Hours**: The time periods that are not defined as Business Hours or Holidays in the specific time zone.
   - **Based on Custom Business Hours**: Set up custom business hours and configure whether to allow this route in the following time:
     - **Business Hours**: The custom business hours based on the system's default time zone.
     - **Holidays**: Holidays specified for the system's default time zone in the system.
     - **Outside Business Hours**: The time periods that are not defined as Business Hours or Holidays for the system's default time zone.
   - **Based on Custom Time Periods**: Set up multiple time periods for this route based on the system's default time zone. You can also specify whether to allow this route in the Holidays configured for the default time zone.
7. Click **Save** and **Apply**.

What to do next

After you finish the outbound route configurations, you need to check and adjust the priority of your outbound routes, so that the system can match and route the call out through the proper outbound route.

For more information, see Adjust priority of outbound routes.

Restrict Outbound Calls by PIN Codes

To prevent the abuse of communication resources, you can restrict outbound calls by setting password for outbound routes to require callers to enter a PIN code before dialing out. Only when a valid PIN code is entered can the call be sent out through the outbound route. This topic describes how to configure either a single PIN code or a list of PIN codes for an outbound route.

Restrict outbound calls by a single PIN code

To allow only specific employees or departments to make outbound calls via a specific outbound route, you can set a unique PIN code for the route. In this way, only users with the correct PIN code are able to use the outbound route.

Procedure

1. Log in to PBX web portal, go to **Call Control > Outbound Route**.
2. Click beside the desired outbound route.
3. Scroll down to the **Trunk** section, set up a password for the outbound route.

   a. In the **Outbound Route Password** drop-down list, select **Single PIN**.
   b. In the **Single PIN** field, set a PIN code.

> **Note:**
> - Only allows numeric value.
> - The length of the PIN code is limited from 3 to 15.

4. Click **Save** and **Apply**.

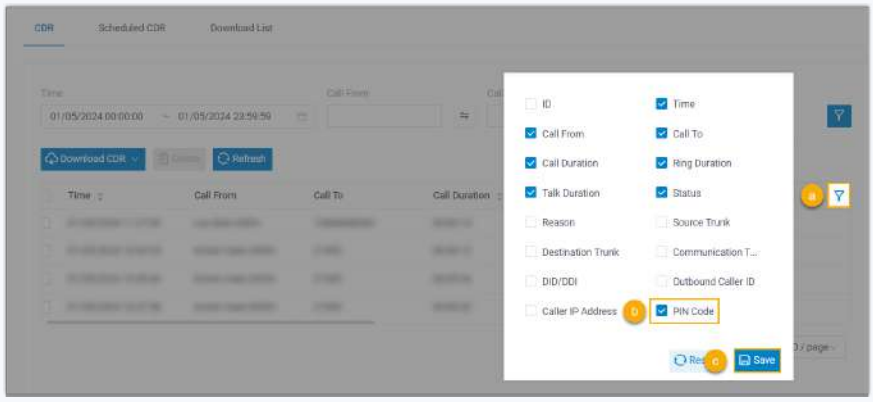
Result

- Users need to enter the PIN code when making outbound calls via the outbound route.

> **Note:**
> If a user enters a wrong PIN code for three times, the call will be hung up automatically.

- In the CDR, you can see the PIN code used in the outbound calls made via the outbound route (Path: **Reports and Recordings > CDR**).

> **Note:**
> Make sure that you have set the CDR to display the **PIN Code** column.



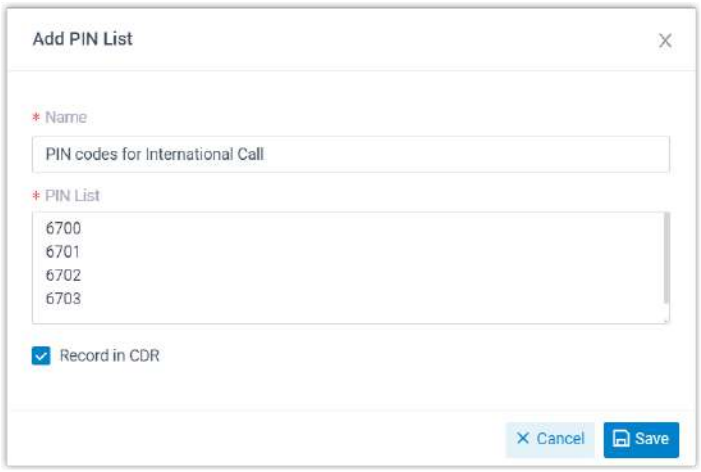
For more information about how extension users can use the PIN code for making outbound calls, see the usage example.

Restrict outbound calls by multiple PIN codes

In the scenario where a number of users share the same extension number across different endpoints to make outbound calls, it is difficult to track the calling activities of these users individually. In this case, you can set up a list of passwords for an outbound route and allocate them to users, so that users can make outbound calls via the outbound route, while you can track and distinguish their calls using the PIN codes.

Step 1. Add a PIN List

1. Log in to PBX web portal, go to **Call Features > PIN List**, click **Add**.
2. In the pop-up window, configure the following settings:



Setting	Description
Name	Enter a name to help you identify it.
PIN List	Enter PIN codes. **Note:** • Press the **Enter** key to separate multiple PIN codes. • Only allows numeric value. • The length of each PIN code is limited from 3 to 15.
Record in CDR	Enable this option. The system will record the PIN code in CDR when the PIN code has been used.

3. Click **Save**.

Step 2. Associate the PIN List with an outbound route

1. On PBX web portal, go to **Call Control > Outbound Route**.
2. Click beside the desired outbound route.
3. Scroll down to the **Trunk** section, set up passwords for the outbound route.

   a. In the **Outbound Route Password** drop-down list, select **PIN List**.

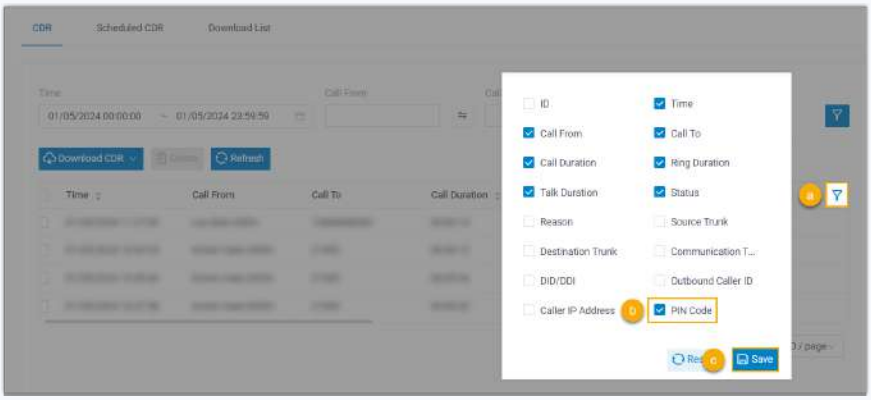
b. In the **PIN List** drop-down list, select an existing PIN list.

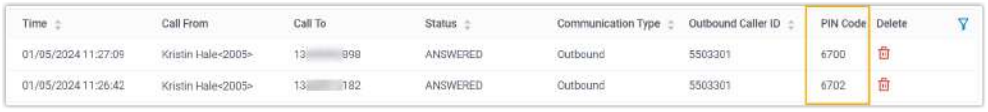
4. Click **Save** and **Apply**.

Result

- Users need to enter any PIN codes contained in the selected PIN list when making outbound calls via the outbound route.
- In the CDR, you can easily distinguish the users who made outbound calls via different PIN codes allocated to different users, even if they use the same extension to dial out (Path: **Reports and Recordings > CDR**).

Note:
Make sure that you have set the CDR to display the **PIN Code** column.





For more information about how extension users can use the PIN code for making outbound calls, see the usage example.

Usage example

We provide an example to help you understand the workflow of making outbound calls via a restricted outbound route using a PIN code.

1. An extension user 2000 dials an external number.

2. After hearing a voice prompt "Please enter your password followed by the pound key", the user enters a PIN code. When done, press # key.
    - If the PIN code is correct, the call will be successfully sent out through the outbound route.
    - If the PIN code is incorrect, the user will hear a voice prompt "password incorrect" and will be asked to enter a password again. If the user enters wrong password for three times, the call will be hung up automatically.

Manage Outbound Routes

After you create outbound routes, you can adjust the priority of the outbound routes. You can also edit or delete the outbound routes.

Adjust priority of outbound routes

When a user places a call, if the dialed number matches multiple dial patterns, the outbound route with the highest priority will be used. You can adjust the priority of outbound routes to route calls through proper outbound routes.

> **Note:**
> The route priority is important, especially if there is some overlap. For example, the number 5503305 matches both dial patterns of `ZXXXXXX` and `X.`, the PBX will send the call through the outbound route with the highest priority.

Example:

When users dial 05503301, both of the two outbound routes match 05503301:

- Outbound Route-Long-distance call: The dial pattern is `0XXXXXXX` and uses trunk 1.
- Outbound Route-Local call: The dial pattern is `X.` and uses trunk 2.

To call 5503301 through trunk 1, you need to prioritize the outbound route of "Long-distance call"; or PBX will match the outbound route of “Local call" and route the call out using trunk 2.

1. Log in to PBX web portal, go to **Call Control > Outbound Route**.
2. Click the buttons ⤒ ^ v ⤓ to adjust the priority of your outbound routes.

> **Note:**

PBX will match outbound route from top to bottom.

Edit an outbound route

1. Log in to PBX web portal, go to **Call Control > Outbound Route**.
2. Click beside the inbound route that you want to edit.
3. On the outbound route configuration page, edit the outbound route.
4. Click **Save** and **Apply**.

Delete an outbound route

1. Log in to PBX web portal, go to **Call Control > Outbound Route**.
2. Click beside the outbound route that you want to delete.
3. On the pop-up dialog box, click **OK** to confirm.
4. Click **Apply**.

Export and Import Outbound Routes

The outbound routes configured on Yeastar P-Series 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 **Call Control > Outbound Route**.
2. Click **Export**.

   A CSV file is saved to your computer. To check and edit parameters in the CSV file, see Outbound Route Parameters.

Import outbound routes

We recommend that you export outbound route data to a CSV file first, and use the file as a template to start with. In this way, you can save time and effort.

Prerequisites

Requirements of an imported file:

- **Format**: UTF-8.CSV
- **Size**: Less than 50 MB
- **File name**: Less than 127 characters
- **Import parameters**: Ensure that the import parameters meet requirements. For more information , see Outbound Route Parameters.

Procedure

1. Log in to PBX web portal, go to **Call Control > Outbound Route**.
2. Click **Import**.
3. In the pop-up window, click **Browse**, and select your CSV file.
4. Click **Import**.

   The outbound routes in the CSV file will be displayed in the **Outbound Route** list.

Related information

Import and Export -FAQ

Outbound Dial Pattern

This topic describes dial pattern settings of Outbound Route.

Dial Pattern components

A dial pattern comprises **Pattern**, **Strip**, and **Prepend**.

Pattern

Required.

Defines which dialed numbers will be matched.

The Pattern field allows a full number or special characters that will match specific numbers. The following table shows descriptions of the allowed characters in the Pattern field.

Pattern	Description
X	Match any digit from 0 -9.
Z	Match any digit from 1- 9.

Pattern	Description
`N`	Match any digit from 2 - 9.
`[###]`	Match any digit in the bracket. **Example**: `[123]` matches the numbers 1, 2, or 3. **Note:** Range of numbers can be specified with a dash, example `[136-8]` matches the numbers 1, 3, 6, 7, or 8.
`.`	Match one or more numbers. **Example**: `9011.` matches any numbers starting with digits 9011 (excluding 9011 itself).
`!`	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.

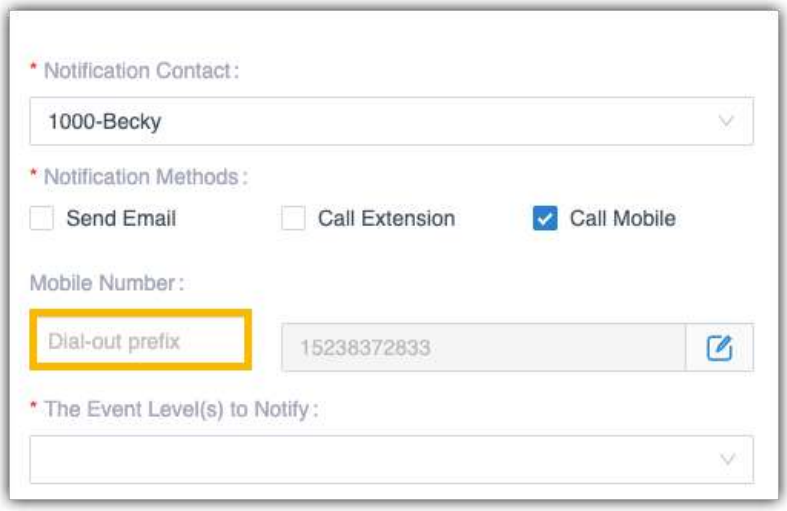
Prefix and Dial Pattern

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.



- External number for IVR keypress.

How to configure Prefix

You need to configure prefix according to the dial pattern settings on your outbound route. If the prefix is not configured correctly, the PBX cannot call to the external number successfully.

- **Leave Prefix setting blank**

  If the **Strip** of outbound route is not set, you don't have to add a prefix before the phone number.

  As the following figure shows, only the destination number that starts with digit *1* can be called out through this outbound route.

  For example, to call number 125451, you should dial the number 125451 directly.

- **Add prefix before a number**

If **Strip** is set on an outbound route, you need to set the prefix according to the **Pattern**.

As the following figure shows, to make calls through the outbound route, you need to add prefix *9* before the number, and the destination number should start with digit *1*.

For example, to call number 125451, you should add prefix 9 before the number 125451.

Dial Pattern Examples

This topic provides sample dial patterns to help you understand dial patterns of outbound route.

Local calls

In Xiamen, China, local numbers are all 7-digit numbers and the numbers do not start with 0, such as 5503305.

For the local calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
ZXXXXXX	Leave it blank.	Leave it blank.

Long distance calls

In Xiamen, China, users need to dial 4-digit area code and 7-digit local number to make a long distance call, such as 0595-7588123.

- Area code format: 0ZXX, the first digit is 0, and the second digit cannot be 0.
- Local number format: 7-digit number that does not start with 0.

For long distance calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
0ZXXZXXXXXX	Leave it blank.	Leave it blank.

Mobile calls

All mobile phone numbers in China are 11-digit numbers and start with digit 1, such as 15880260666.

For mobile calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
1XXXXXXXXXX	Leave it blank.	Leave it blank.

International calls

All international numbers start with digits 00.

For international calls, set dial pattern as the following table shows.

Pattern	Strip	Prepend
00.	Leave it blank.	Leave it blank.

AutoCLIP Route

AutoCLIP Route Overview

Yeastar provides AutoCLIP (Auto Calling Line Identification Presentation) feature, which is an intelligent call matching feature. You can configure AutoCLIP to route customer inbound calls to original extensions, which will promote your customer satisfaction and help your business be more efficient, and professional.

Restriction

The AutoCLIP list supports up to 100,000 records.

Scenarios

Assume that sales representatives in your company often make outbound calls to customers for promotion. More or less, some customers may miss the calls. When customers call back, the calls are routed to the receptionist or business auto attendant. Neither receptionist/business auto attendant nor the customers know who placed the call.

With AutoCLIP feature, the PBX can redirect the calls to the original extension users who placed the calls when customers call back. Using this feature, you can avoid the embarrassing situation that customers cannot find the person when they call back to the PBX.

How does the PBX redirect calls to original extensions?

1. When extension users make outbound calls, the PBX automatically stores the records to AutoCLIP list, including extension number, called number, and the used trunk.
2. When customers call back to the PBX system, PBX will compare the phone numbers with the records in the AutoCLIP list.
    - If there're matched records in AutoCLIP list, the calls will be routed to corresponding extensions, bypassing any receptionists or business auto attendant.
    - If there're not matched records in AutoCLIP list, the calls will be routed to the destination specified in inbound routes.

Route Inbound Calls to Original Extensions via AutoCLIP Route

With AutoCLIP feature, Yeastar P-Series 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.

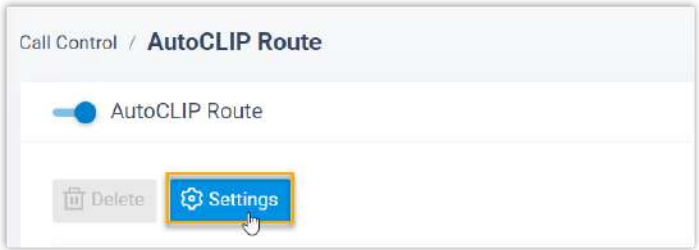
Prerequisites

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.

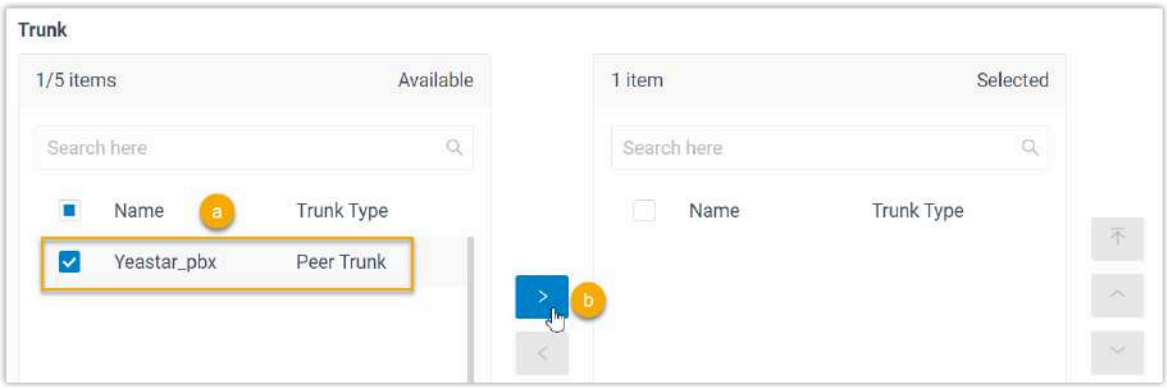


4. Configure the AutoCLIP settings according to your needs.

Table 25.

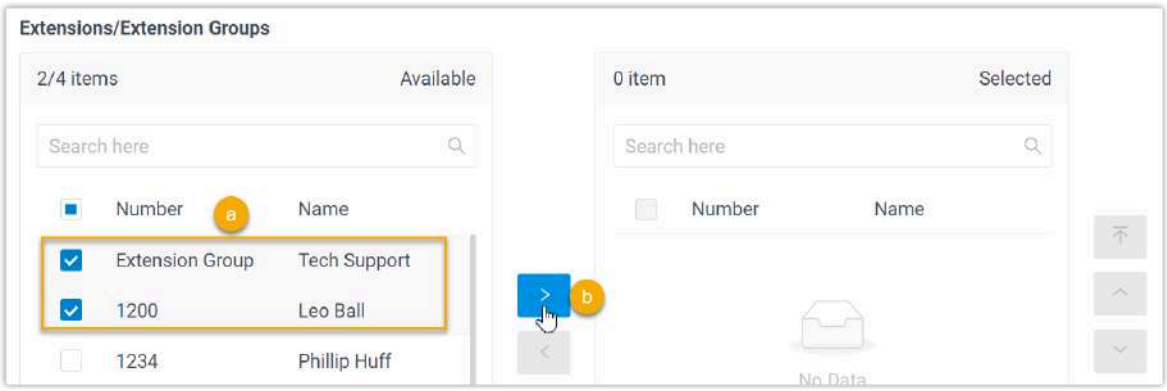
Setting	Description
Record Keep Time	Set how long records can be kept in AutoCLIP list. If keep time of a record exceeds the value, PBX will automatically delete the record. **Tip:** You can check the expiration time in the AutoCLIP record list directly.
Digits Match	Define how many digits from the last 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.



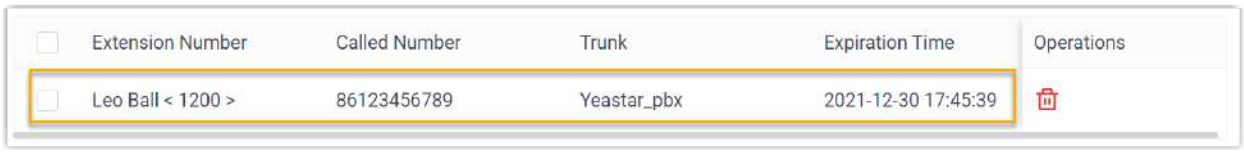
a. Select the desired extension(s)/extension group(s).
b. Add the extension(s)/extension group(s) from **Available** box to **Selected** box.

7. Click **Save**.

Result

When extension user uses the trunk with AutoCLIP feature to call external users out, PBX generates AutoCLIP records, including extension details, the numbers dialed and the used trunk. You can check the AutoCLIP record on **Call Control > AutoCLIP Route**.

Note:
If more than one extension user make outbound calls to the same external user, PBX will only match the last extension user that placed the call when the external user calls back.



Delete AutoCLIP Records

This topic describes how to delete AutoCLIP records.

Delete a record

1. Log in to PBX web portal, go to **Call Control > AutoCLIP Route**.
2. Click beside the record that you want to delete.
3. In the pop-up dialog box, click **OK**.

Bulk delete records

1. Log in to PBX web portal, go to **Call Control > AutoCLIP Route**.
2. Select the checkboxes of the desired records, and click **Delete**.
3. In the pop-up dialog box, click **OK**.

DID Number

DID Number Overview

This topic describes what is DID number and DID usages on Yeastar P-Series 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. Click **Add**, then add DID number(s) according to your need.
   - To add a single DID number, do as follows:
     a. In the **Create Method** drop-down list, select **Single DID**.
     b. Configure the following settings:
     - **DID/DDI**: Enter the provided DID number.
     - **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

       When the DID number is dialed, the name will be displayed on the called party's device.
   - To add a range of DID numbers, do as follows:
     a. In the **Create Method** drop-down list, select **DID Range**.
     b. Configure the following settings:
     - **DID Range**: Enter the start number and the end number of the DID range.
     - **DID/DDI Name**: Optional. Enter a name to distinguish inbound calls by DID numbers.

       When the DID number is dialed, the name will be displayed on the called party's device.
4. Click **Confirm**.
5. Click **Save** and **Apply**.

Delete DID numbers

1. Log in to PBX web portal, go to **Extension and Trunk > Trunk**, edit the desired trunk.
2. Click **DIDs/DDIs** tab.
3. On the **DIDs/DDIs** page, click  to delete a DID number.
4. To bulk delete DID numbers, select the checkboxes of DID numbers, click **Delete**.

5. Click **Save**.

Export and Import Trunk DIDs/DDIs Numbers

Trunk DIDs/DDIs numbers configured on Yeastar P-Series 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 for Outbound Calls.

Inbound caller ID

Inbound caller ID is an external user's phone number that will be displayed on an extension user's phone when the external user calls in Yeastar P-Series 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**: Leave it blank.
- **Prepend**: 0

Example 2

Company B wants all local numbers to be displayed without area code (0592).

For example, company B wants to display number 5503301 instead of 05925503301.

In this case, you can configure the reformatting rule as below:

- **Patterns**: 0592XXXXXXX
- **Strip**: 4
- **Prepend**: Leave it blank.

Export and Import Inbound Caller ID Reformatting Rules

The inbound caller ID reformatting rules configured on Yeastar P-Series 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 for Outbound Calls

This topic describes different ways to customize outbound caller IDs for standard outbound calls, which help customers recognize who's calling.

Background information

Before you start to customize outbound caller IDs, you may need to know the following concepts:

- Caller ID types
- Priority of outbound caller ID

Prerequisites

Customizing outbound caller ID should be supported by the trunk provider.

Customize outbound caller ID for a trunk

1. Log in to PBX web portal, go to **Extension and Trunk > Trunk**, edit the desired trunk.
2. Click **Outbound Caller ID** tab.

3. In the **General** section, configure a general **Outbound Caller ID** and **Outbound Caller ID Name** for the trunk.
4. Click **Save** and **Apply**.

   The general outbound caller ID and caller ID name will be displayed on the called party's device when users make outbound calls through this trunk.

Customize outbound caller IDs for extensions

You can set up an outbound caller ID for a specific extension based on a trunk, so that an associated caller ID is sent out when the user calls out.

1. Log in to PBX web portal, go to **Extension and Trunk > Trunk**, edit the desired trunk.
2. Click **Outbound Caller ID** tab.
3. In the **Outbound Caller ID List** section, click **Add**, and configure outbound caller IDs for extensions by different methods.
4. To associate one outbound caller ID with multiple extensions, select **Shared Outbound Caller ID** and configure the following settings:
   - **Outbound Caller ID**
   - **Outbound Caller ID Name**
   - **Associated Extensions**
   - **Default DOD Label**
5. To bind consecutive outbound caller IDs to consecutive extensions with one-to-one correspondence, select **Outbound Caller ID Range** and configure the following settings:
   - **Outbound Caller ID Range**
   - **Extension Range**
   - **Outbound Caller ID Name**
   - **Default DOD Label**
6. Click **Save** and **Apply**.

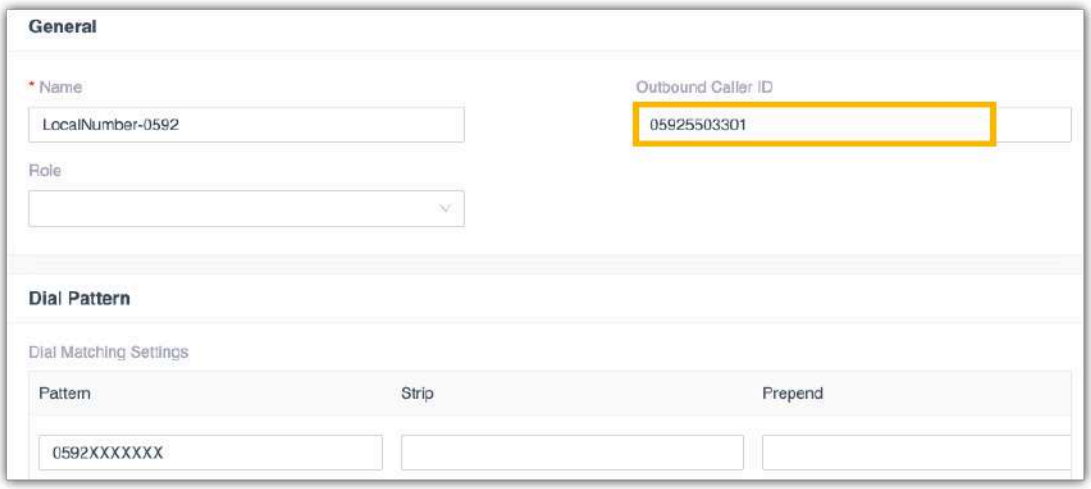
When extension users make outbound calls through the configured trunk, the associated outbound caller IDs will be displayed on the called party's device.

Customize outbound caller IDs based on dialed numbers

When calling to multiple areas, you may need to display pre-defined local number for the area code you are dialling. In this case, you can configure outbound caller IDs based on the dialed numbers.

The following instruction describes how to display a custom outbound caller ID 05925503301 when users call to local numbers that have area code 0592.

1. Log in to PBX web portal, go to **Call Control > Outbound Route**, edit the outbound route that is for local calls with area code 0592.
2. In the **General** section, enter the custom caller ID in the **Outbound Caller ID** field.



3. Click **Save** and **Apply**.

Related information

Customize Outbound Caller IDs for Outbound Campaigns

Customize Outbound Caller IDs for Outbound Campaigns

This topic describes how to customize the outbound caller ID for outbound campaigns based on trunks to display your company's phone number and name on recipients' devices. Primarily used in Yeastar outbound call center, this feature helps to achieve local presence for regional calls, improving answer rates and build trust with recipients.

Requirements

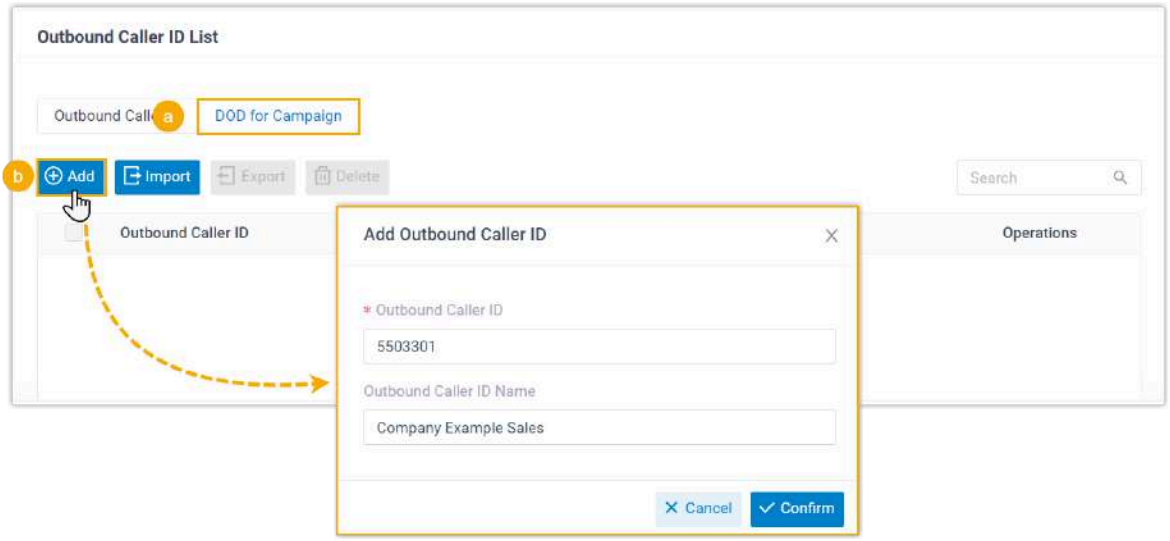
The firmware of Yeastar P-Series Software Edition is 83.18.0.59 or later.

Prerequisites

Customizing outbound caller ID should be supported by the trunk provider.

Procedure

1. Log in to PBX web portal, go to **Extensions and Trunk > Trunk**, edit the desired trunk.
2. In **Outbound Caller ID** page, scroll down to the **Outbound Caller ID List** section.
3. Click **DOD for Campaign** tab, then click **Add** to add an outbound caller ID.



   - **Outbound Caller ID**: Enter the phone number shown on the recipient's device.
   - **Outbound Caller ID Name**: Optional. Enter a name shown on the recipient's device.
4. Click **Confirm**.
5. Add more outbound caller IDs as needed.
6. Click **Save** and **Apply**.

Related information

Outbound Call Center Guide

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 outbound caller ID list

You can export the outbound caller ID list, either for standard outbound calls or for campaign outbound calls, into 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. Scroll down to the **Outbound Caller ID List** section, export the outbound caller ID list according to your needs.
   - To export outbound caller ID list for standard outbound calls, click **Export** at the top of the list.

   - To export outbound caller ID list for campaign outbound calls, click the **DOD for Campaign** tab, then click **Export** at the top of the list.

   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, import the outbound caller ID according to your needs.
   - To import outbound caller ID list for standard outbound calls, do as follows:
     a. Click **Import** at the top of the list.

     b. In the pop-up window, click **Browse**, and select your CSV file.
     c. Click **Import**.

        The outbound caller ids in the CSV file will be displayed in the **Outbound Caller ID List**.
   - To import outbound caller ID list for campaign outbound calls, do as follows:
     a. Click the **DOD for Campaign** tab, then click **Import** at the top of the list.

     b. In the pop-up window, click **Browse**, and select your CSV file.
     c. Click **Import**.

The campaign outbound caller ids 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

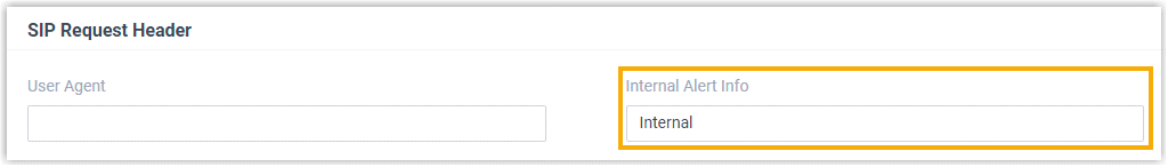
1. Set alert info for internal calls on the PBX.
2. Set a specific ringtone for a phone.

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`.



Set a specific ringtone for a phone

For users who want to play a specific ringtone for internal calls on their phones, you can set a specific ringtone for their phones by auto provisioning.

Note:
Users can also log in to phone web interface to set distinctive ringtone manually on their own IP phones. For more information, contact the phone manufacturer.

Prerequisites

Each user who wants distinctive ringtone has bound a phone with their extensions.
For more information, see the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

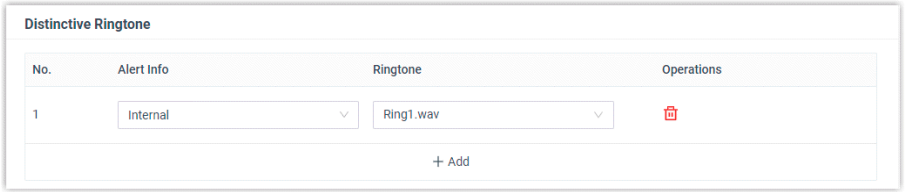
Procedure

1. Set a specific internal ringtone for a user's phone.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the user's extension.
   b. Click **Phone** tab to edit the phone associated with the extension.
   c. In the **Distinctive Ringtone** section, click **Add**.
   d. In the **Alert Info** field, select the alert info that is pre-defined for internal calls.

      In this example, select `Internal`.
   e. In the **Ringtone** field, select a ringtone for the internal calls.

      In this example, select `Ring1.wav`.

      Note:
      The available ringtones vary by phone models.

   f. Click **Save**.

2. Reprovision the phone to take effect.
    a. Go to **Auto Provisioning > Phones**.
    b. Click beside the phone assigned to the user's extension.

Result

The user's phone plays ringtone *Ring1.wav* when receiving internal calls.

Set Distinctive Ringtones for External Calls

You can set distinctive ringtones on different inbound routes. When an extension user hears the ringtone of an external incoming call, the user may notice the intention of the call.

Procedure

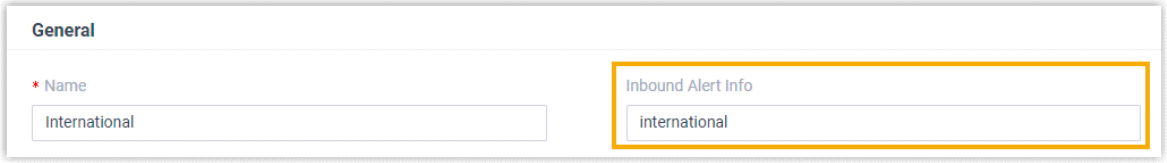
1. Set alert info for external calls on the PBX.
2. Set a specific ringtone for a phone.

Set alert info for external calls on the PBX

1. Log in to PBX web portal, go to **Call Control > Inbound Route**, edit a desired inbound route.
2. In the **General** section, enter an alert info in the **Inbound Alert Info** field.

    The alert info is used to trigger IP phones to play a specific ringtone when receiving external calls from the inbound route.

    In this example, set alert info to `international` to identify international calls.

3. Click **Save** and **Apply**.

Set a specific ringtone for a phone

For users who want to play a specific ringtone for external calls on their phones, you can set a specific tone for their extensions by auto provisioning.

Note:

Users can also log in to phone web interface to set distinctive ringtone manually on their own IP phones. For more information, contact the phone manufacturer.

Prerequisites

The user's extension should have been associated with a phone.

For more information, see the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

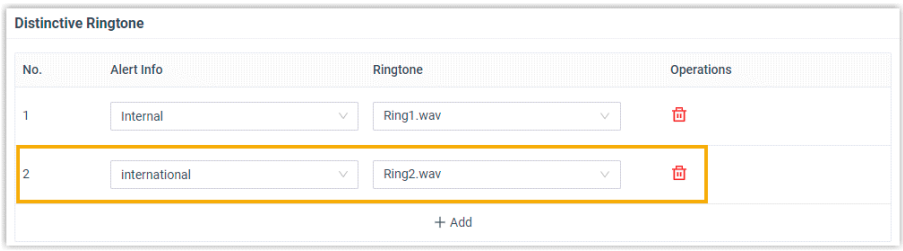
Procedure

1. Set distinctive ringtones for a user.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the user's extension.
   b. Click the **Phone** tab.
   c. In the **Distinctive Ringtone** section, click **Add**.
   d. In the **Alert Info** field, select the alert info that is pre-defined for external calls.

      In this example, select `international`.
   e. In the **Ringtone** field, select a specific ringtone for international calls.

      In this example, select `Ring2.wav`.

      Note:
      The available ringtones vary by phone models.



f. Click **Save**.

2. Reprovision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to user's extension.

Result

The user's phone plays ringtone *Ring2.wav* when receiving external calls from the specific inbound route.

Set Distinctive Ringtones for Queue Calls

You can set a unique ring tone per call queue so that the agents can easily identify who is calling. This is especially useful for the agents who are in multiple call queues to help them identify calls.

Procedure

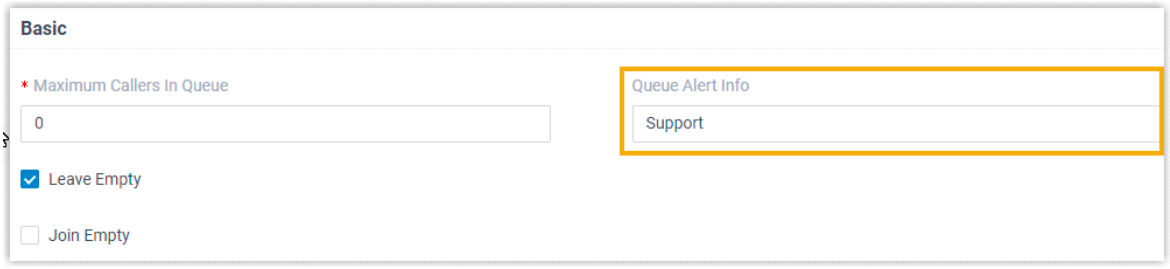
1. Set an alert info for queue calls on the PBX.
2. Set a specific ring tone for a phone.

Set an alert info for queue calls on the PBX

1. Log in to PBX web portal, go to **Call Features > Queue**, edit a desired queue.
2. Click the **Preferences** tab.
3. In the **Basic** section, enter an alert info in the **Queue Alert Info** field.

   The alert info is used to trigger IP phones to play a specific ring tone when receiving a call through this queue.

   In this example, set the alert info to `Support`.



Set a specific ring tone for a phone

For the agents who want to play unique ring tones for different queue calls on their phones, you can set distinctive ring tones for their phones by auto provisioning.

> **Note:**
> Users can also log in to phone web interface to set distinctive ring tone manually on their own IP phones. For more information, contact the phone manufacturer.

Prerequisites

The agent's extension should have been associated with a phone.

For more information, see the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

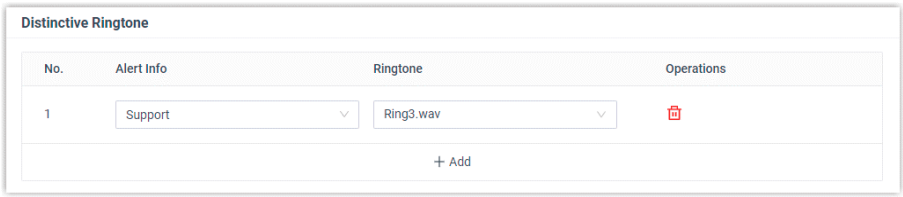
Procedure

1. Set a specific queue ring tone for an agent's phone.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the agent's extension.
   b. Click the **Phone** tab.
   c. In the **Distinctive Ringtone** section, click **Add**.
   d. In the **Alert Info** field, select the alert info that is pre-defined for queue calls.

      In this example, select `Support`.
   e. In the **Ringtone** field, select a specific ring tone for the queue calls.

      In this example, select `Ring3.wav`.

      > **Note:**
      > The available ring tones vary by phone models.



f. Click **Save**.

2. Reprovision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to agent's extension.

Result

The agent's phone plays ringtone *Ring3.wav* when receiving calls from the Support queue.

Set Distinctive Ringtones for Ring Group Calls

You can set a unique ringtone per ring group so that the members can easily identify who is calling. This is especially useful for the members who are in multiple ring groups to help them identify calls.

Procedure

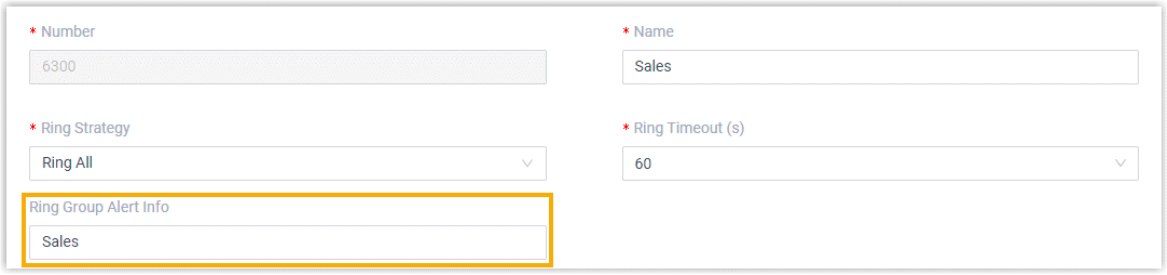
1. Set an alert info for ring group calls on the PBX.
2. Set a specific ringtone for a phone.

Set an alert info for ring group calls on the PBX

1. Log in to PBX web portal, go to **Call Features > Ring Group**, edit a desired ring group.
2. In the **Ring Group Alert Info** section, enter an alert info.

   The alert info is used to trigger IP phones to play a specific ringtone when receiving a call through this ring group.

   In this example, set alert info to `Sales`.



Set a specific ringtone for a phone

For ring group members who want to play a specific ringtone for ring group calls on their phones, you can set a specific tone for their extensions by auto provisioning.

> **Note:**
> Users can also log in to phone web interface to set distinctive ringtone manually on their own IP phones. For more information, contact the phone manufacturer.

Prerequisites

The ring group member's extension should have been associated with a phone.

For more information, see the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

Procedure

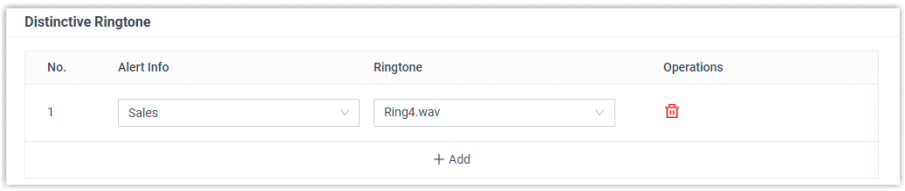
1. Set a specific ringtone for a ring group member.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit ring group member's extension.
   b. Click the **Phone** tab.
   c. In the **Distinctive Ringtone** section, click **Add**.
   d. In the **Alert Info** field, select the alert info that is pre-defined for ring group calls.

      In this example, we select `Sales`.

e. In the **Ringtone** field, select a specific ringtone for the ring group calls.

In this example, we select `Ring4.wav`.

> **Note:**
> The available ringtones vary by phone models.



f. Click **Save**.

2. Reprovision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to ring group member's extension.

Result

The ring group member's phone plays ringtone *Ring4.wav* when receiving calls from the Sales ring group.

Set Distinctive Ringtones for IVR Calls

You can set a unique ringtone per IVR so that the extension users can easily identify who is calling.

Procedure

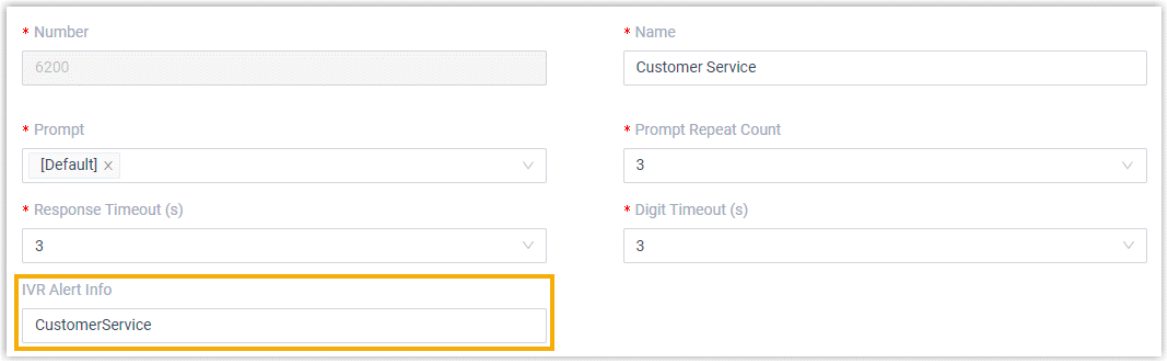
1. Set an alert info for IVR calls on the PBX.
2. Set a specific ringtone for a phone.

Set an alert info for IVR calls on the PBX

1. Log in to PBX web portal, go to **Call Features > IVR**.
2. In the **IVR Alert Info** field, enter an alert info.

The alert info is used to trigger IP phones to play a specific ringtone when receiving a call through this IVR.

In this example, set alert info to `CustomerService`.



Set a specific ringtone for a phone

For users who want to play a specific ringtone for IVR calls on their phones, you can set a specific tone for their extensions by auto provisioning.

> **Note:**
> Users can also log in to phone web interface to set distinctive ringtone manually on their own IP phones. For more information, contact the phone manufacturer.

Prerequisites

The user's extension should have been associated with a phone.

For more information, see the following topics:

- Auto Provision IP Phones in Local Network (PnP Method)
- Auto Provision IP Phones in Local Network (DHCP Method)
- Auto Provision IP Phones Remotely (RPS FQDN Method)
- Auto Provision IP Phones Remotely (RPS Method)

Procedure

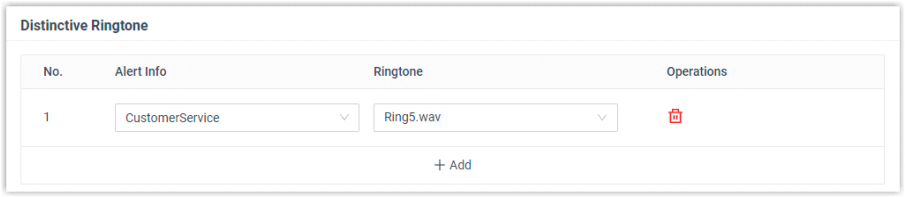
1. Set a specific ringtone for a user.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the user's extension.
   b. Click the **Phone** tab.

c. In the **Distinctive Ringtone** section, click **Add**.
d. In the **Alert Info** field, select the alert info that is pre-defined for IVR calls.

   In this example, select `CustomerService`.
e. In the **Ringtone** field, select a specific ringtone for the IVR calls.

   In this example, select `Ring5.wav`.

> **Note:**
> The available ringtones vary by phone models.



f. Click **Save**.

2. Reprovision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to user's extension.

Result

The user's phone plays ringtone *Ring5.wav* when receiving calls from CustomerService IVR.

Distinctive Caller ID Name

Distinctive Caller ID Name Overview

This topic describes what is Distinctive Caller ID Name, and an example of Distinctive Caller ID Name.

What is Distinctive Caller ID Name

Distinctive Caller ID Name allows employees to know where the incoming call is routed, and who is calling. Distinctive Caller ID Name is a string that will be displayed on employees' phones, which may include the followings (from the highest to the lowest):

1. Contact name that is stored in Company Contacts directory or Personal Contacts directory.

   > **Note:**
   > If the extension user does not have permission to view Company Contacts, the contact name stored in Company Contact will not be displayed on the extension user's phone.

2. Call feature name (the name of IVR, Ring Group, or Queue)

   > **Note:**
   > If an incoming call reaches an extension through multiple call features, the name of the last call feature will be displayed. For example, if a call reaches an IVR and then goes to a queue, the queue name will be displayed on agents' phones.

3. Trunk DID/DDI name
4. Caller Name (CNAM): CNAM is sent from the caller that displays the caller name or the caller's company name.

   > **Note:**
   > CNAM is configured by the caller's side.

An example of Distinctive Caller ID Name

Your company has a support team that is responsible for providing technical services for customers from China and America. The following settings are configured on your PBX to achieve your goal:

Queue

A queue named "Support" for support team.

SIP trunk

A SIP trunk with two DID numbers that are bound with their respective names.

Table 26.

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**.

3. Click **Save** and **Apply**.

Enable or disable the display of trunk DID/DDI name

1. Log in to PBX web portal, go to **PBX Settings > Preferences**.
2. In the **Distinctive Caller ID Name** section, configure the followings:
   - To display trunk DID/DDI name, select the checkbox of **Display DID/DDI Name**.
   - To hide trunk DID/DDI name, unselect the checkbox of **Display DID/DDI Name**.

3. Click **Save** and **Apply**.

Call Features

Voicemail

Voicemail Overview

Yeastar P-Series 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 language**: Custom language for system prompts played in group voicemails or extension voicemails. Callers accessing the voicemail will hear prompts in the selected language.
- **Voicemail greeting**: Custom greeting is available for global or a specific extension. The extension users can also customize their greetings based on presence.

  For more information, see Voicemail Greeting Overview.

- **Voicemail notification**: Various ways to get notified of new voicemail messages, including on IP phones, emails, or Linkus clients.

  For more information, see Voicemail Notification Overview.

- **Envelope playback**: Play optional envelope information before listening to voicemail message, including date and time, caller ID, and message duration.

  For more information, see Configure Message Envelope.
- **Caller experience**: User-friendly experience in leaving a message, such as allow the caller to review message, send a message without ringing extensions, break out of voicemail to operator, etc.
  For more information, see:
  - Allow Callers to Press a Key to Leave Messages
  - Allow Callers to Dial Extension from Voicemail
  - Allow Callers to Break out from Voicemail
  - Allow Callers to Review Voicemail Messages

Voicemail capacity and limitations

The default and adjustable capacity and limitations for each voicemail box are as follows:

- Message length: 1 to 15 minutes.

  The default minimum duration of a message is 2 seconds; the default maximum duration of a message is 10 minutes.

  To change the message length, see Limit Voicemail Message Length.

- Mailbox capacity: 1 to 500.

  The default max number of voicemail is 100.

  To change mailbox capacity, see Auto Cleanup Voicemail Messages.
- Storage time: Unlimited.

  The default is 0, which means no limit.

  To change the storage time, see Auto Cleanup Voicemail Messages.

Group Voicemail

Set up Group Voicemail for a Queue

You can set up a Group Voicemail for a queue. All agents of the queue will get notified when a group voicemail message is received.

Procedure

1. Log in to PBX web portal, go to **Call Features > Voicemail > Group Voicemail**.
2. Click **Add**.
3. Under **General** tab, complete the general settings:
   a. In the **Basic** section, configure the following settings.

Setting	Description
Type	Select **Queue**.
Queue	Select a queue.
Number	The Group Voicemail number is the queue number, and is not editable.
Name	The Group Voicemail name is the queue name, and is not editable.
Mode	Select the mode to handle received voicemail messages. • **Shared by Members**: The voicemail messages are saved in the group mailbox, and are shared by all members. Any members can manage the group voicemail messages. • **Broadcast to Members**: The voicemail messages are not stored in the group mailbox. Instead, the system broadcasts (copies and forwards) the

Setting	Description
	voicemail messages to the individual mailboxes of all the members.
Voicemail PIN Authentication	Enable or disable voicemail PIN authentication.
Voicemail Access PIN	If enable voicemail PIN authentication, enter a desired access PIN number.
Disallow Voicemail Messages	Optional. Enabling this option to restrict callers from leaving voicemail messages. The system will play voicemail greeting to the caller, and then hang up the call directly.
Play Date and Time	Optional. Play the date and time that the message was received before a voicemail message is played.
Play Caller ID	Optional. Play the caller ID information before a voicemail message is played.
Play Message Duration	Optional. Play the duration of the message before a voicemail message is played.
Custom Prompt Language	Optional. Enable this option and set the language of voicemail prompts heard by callers when they access the group voicemail. **Note:** • The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**). • If the group voicemail has set up a custom greeting, the custom greeting will be played to callers instead. In this case, the language setting will be ignored.

b. In the **Members** section, all the agents of the queue are selected, and the members are not editable.

> **Note:**
> If the queue agents are changed, the members of the group's voice mailboxes also change.

c. In the **Group Voicemail Greeting** section, select a voicemail greeting.

You can also click **Greeting Management** to customize a greeting or mange your custom greetings.

4. Under **Voicemail Announcement** tab, set up call alerts for new voicemail messages in the group voicemail.

> **Note:**
> This feature is only supported on the group voicemail with the **Mode** set to **Shared by Members**.

5. Click **Save** and **Apply**.

Related information

Enable or Disable Voicemail Access PIN
Change Voicemail Access PIN
Configure Message Envelope
Change Voicemail Greetings
Record or Upload Voicemail Greetings
Manage Group Voicemail Greetings

Set up Group Voicemail for a Ring Group

You can set up a Group Voicemail for a ring group. All members of the ring group will get notified when a group voicemail message is received.

Procedure

1. Log in to PBX web portal, go to **Call Features > Voicemail > Group Voicemail**.
2. Click **Add**.
3. Under **General** tab, complete the general settings:
   a. In the **Basic** section, configure the following settings:

Setting	Description
Type	Select **Ring Group**.
Ring Group	Select a ring group.
Number	The group voicemail number is the ring group number, and is not editable.
Name	The group voicemail name is the ring group name, and is not editable.
Mode	Select the mode to handle received voicemail messages.

Setting	Description
	• **Shared by Members**: The voicemail messages are saved in the group mailbox, and are shared by all members. Any members can manage the group voicemail messages. • **Broadcast to Members**: The voicemail messages are not stored in the group mailbox. Instead, the system broadcasts (copies and forwards) the voicemail messages to the individual mailboxes of all the members.
Voicemail PIN Authentication	Enable or disable voicemail PIN authentication.
Voicemail Access PIN	If enable voicemail PIN authentication, enter a desired access PIN number.
Disallow Voicemail Messages	Optional. Enabling this option to restrict callers from leaving voicemail messages. The system will play voicemail greeting to the caller, and then hang up the call directly.
Play Date and Time	Optional. Play the date and time that the message was received before a voicemail message is played.
Play Caller ID	Optional. Play the caller ID information before a voicemail message is played.
Play Message Duration	Optional. Play the duration of the message before a voicemail message is played.
Custom Prompt Language	Optional. Enable this option and set the language of voicemail prompts heard by callers when they access the group voicemail. **Note:** • The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**). • If the group voicemail has set up a custom greeting, the custom greeting will be played to callers instead. In this case, the language setting will be ignored.

b. In the **Members** section, all the members of the ring group are selected, and the members are not editable.

Note:

> If the ring group members are changed, the members of the group's voice mailboxes also change.

c. In the **Group Voicemail Greeting** section, select a voicemail greeting.

You can also click **Greeting Management** to customize a greeting or mange your custom greetings.

4. Under **Voicemail Announcement** tab, set up call alerts for new voicemail messages in the group voicemail.

> **Note:**
> This feature is only supported on the group voicemail with the **Mode** set to **Shared by Members**.

5. Click **Save** and **Apply**.

Related information

Enable or Disable Voicemail Access PIN
Change Voicemail Access PIN
Configure Message Envelope
Change Voicemail Greetings
Record or Upload Voicemail Greetings
Manage Group Voicemail Greetings

Set up Group Voicemail for a Custom Group

For a team whose members come from different departments, you can set up a Group Voicemail for the team members. All team members will get notified when a group voicemail message is received.

Procedure

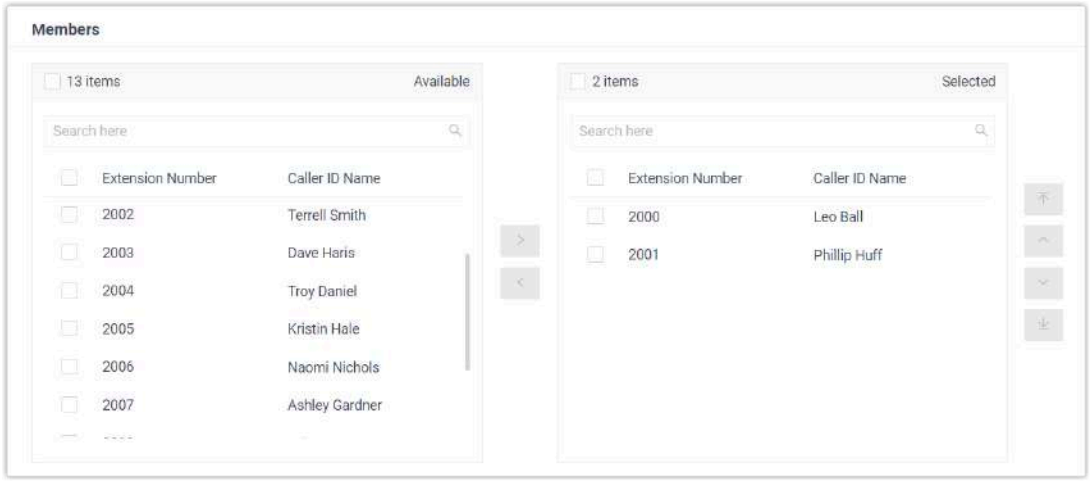
1. Log in to PBX web portal, go to **Call Features > Voicemail > Group Voicemail**.
2. Click **Add**.
3. Under **General** tab, complete the general settings:
   a. In the **Basic** section, configure the following settings:

Setting	Description
Type	Select **Custom**.

Setting	Description
Number	Specify a virtual number for callers to access the group voicemail.
Name	Enter a group voicemail name to help you identify it.
Mode	Select the mode to handle received voicemail messages. • **Shared by Members**: The voicemail messages are saved in the group mailbox, and are shared by all members. Any members can manage the group voicemail messages. • **Broadcast to Members**: The voicemail messages are not stored in the group mailbox. Instead, the system broadcasts (copies and forwards) the voicemail messages to the individual mailboxes of all the members.
Group voicemail to Email	Optional. Enter the desired email addresses to receive group voicemails. **Note:** A maximum of 5 email addresses is supported; Use semicolons ; to separate multiple email addresses.
Voicemail PIN Authentication	Enable or disable voicemail PIN authentication.
Voicemail Access PIN	If enable voicemail PIN authentication, enter a desired access PIN number.
Disallow Voicemail Messages	Optional. Enabling this option to restrict callers from leaving voicemail messages. The system will play voicemail greeting to the caller, and then hang up the call directly.
Play Date and Time	Optional. Play the date and time that the message was received before a voicemail message is played.
Play Caller ID	Optional. Play the caller ID information before a voicemail message is played.
Play Message Duration	Optional. Play the duration of the message before a voicemail message is played.
Custom Prompt Language	Optional. Enable this option and set the language of voicemail prompts heard by callers when they access the group voicemail. **Note:**

Setting	Description
	• The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**). • If the group voicemail has set up a custom greeting, the custom greeting will be played to callers instead. In this case, the language setting will be ignored.

b. In the **Members** section, select the desired extensions or extension groups from **Available** box to **Selected** box to receive group voicemails.



> **Note:**
> Group voicemails will be sent to the selected members and the specified email addresses if both are configured.

c. In the **Group Voicemail Greeting** section, select a voicemail greeting.

You can also click **Greeting Management** to customize a greeting or mange your custom greetings.

4. Under **Voicemail Announcement** tab, set up call alerts for new voicemail messages in the group voicemail.

> **Note:**
> This feature is only supported on the group voicemail with the **Mode** set to **Shared by Members**.

5. Click **Save** and **Apply**.

Related information

Enable or Disable Voicemail Access PIN
Change Voicemail Access PIN
Configure Message Envelope
Change Voicemail Greetings
Record or Upload Voicemail Greetings
Manage Group Voicemail Greetings

Set up Call Alerts for Group Voicemail

Yeastar P-Series Software Edition allows you to configure call alerts for new group voicemail messages. When a new voicemail message is left, the system will call the specified phone numbers in a pre-defined priority order until all the voicemail messages are read or the specified call cycles are reached.

Scenario

A company has a team of on-call agents responsible for after-hours emergency. Instead of answering incoming calls, the company wants the calls to be routed to voicemail while the agents can be alerted as soon as possible. In this case, the company can configure an inbound route for such emergency calls, routing the calls to a dedicated group voicemail, and then set up call alerts to notify the agents whenever a new voicemail message is left.

Requirements and restrictions

Before you begin, read through the requirements and restrictions for the feature:

Requirements

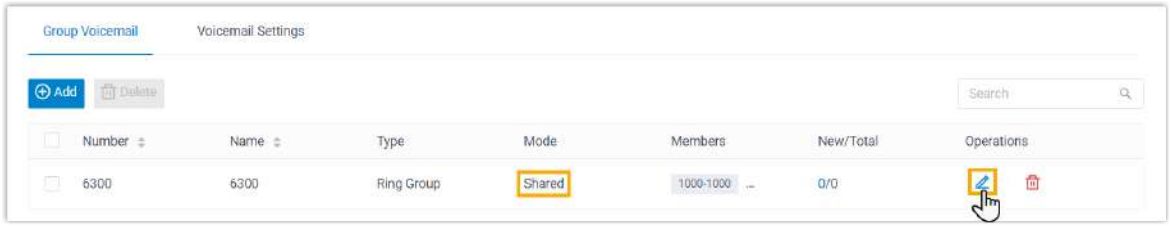
- **Version**: 83.13.0.25 or later
- **Plan**: Enterprise Plan or Ultimate Plan

Restrictions

- This feature is only available for the group voicemails that are **Shared by Members**.
- Allow calls to only **External Number** when there is a new voicemail message and only **5** external numbers are supported.

Procedure

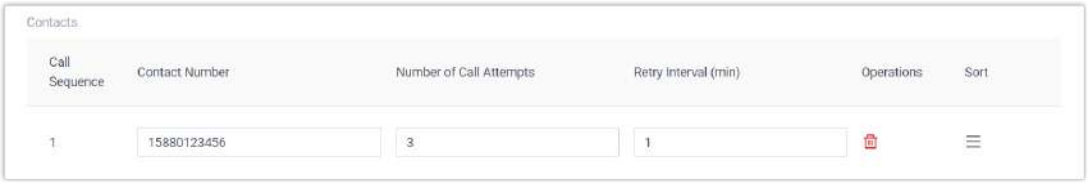
1. Log in to PBX web portal, go to **Call Features > Voicemail > Group Voicemail**, edit a group voicemail with the **Mode** displayed as **Shared**.



2. Click the **Voicemail Announcement** tab.
3. Turn on call notifications for new group voicemail messages, and set up the number and rule to call.
   a. Turn on the switch of **Voicemail Announcement**.
   b. In the **Max Number of Call Cycles** field, specify how many times you want to repeatedly call the contact list.

> **Note:**
> - The value you enter should not be greater than 30.
> - Notification calls will continue until the number of call cycle is reached or all voicemail messages have been read.

   c. In the **Contacts** section, click **Add** to configure the number to call and set up the rule.



- **Contact Number**: Enter an external number.

> **Note:**
> Notification calls to the number can be made via any matched outbound routes. Make sure that there are outbound routes that match the number, otherwise the notification call cannot be made.

- **Number of Call Attempts**: Specify the number of attempts to call the number if the callee doesn't answer the call or if the callee answers the call but does not listen to the new voicemail message.
- **Retry Interval (min)**: Specify the interval between the call attempts.

d. **Optional:** To add more contacts, repeat step c.

> **Note:**
> The system will call the external numbers from the top down. You can adjust the priority order using ☰.

4. Click **Save**.

Result

When the group voicemail receives a new message, the PBX will call the preset numbers in sequence. The callee can answer the call and follow the prompt to listen to the message or call the original caller back directly.

Related information

Extension Call Statistics Report
Extension Call Activity Report

Manage Group Voicemails

This topic describes how to edit a group voicemail, and delete group voicemails.

Edit a group voicemail

1. Log in to PBX web portal, go to **Call Features > Voicemail > Group Voicemail**.
2. Click ✎ beside the group voicemail that you want to edit.
3. Change the settings according to your needs.
   - Enable or Disable Voicemail Access PIN
   - Change Voicemail Access PIN
   - Configure Message Envelope
   - Change Voicemail Greetings
   - Record or Upload Voicemail Greetings
   - Manage Group Voicemail Greetings
4. Click **Save** and **Apply**.

Delete group voicemails

1. Log in to PBX web portal, go to **Call Features > Voicemail > Group Voicemail**.
2. To delete a group voicemail:
   a. Click beside the group voicemail that you want to delete.
   b. Click **Apply**.
3. To delete group voicemails in bulk:
   a. Select the checkboxes of the group voicemails that you want to delete, click **Delete**.
   b. Click **OK** and **Apply**.

Send and Receive Voicemail Messages

Forward Calls to Voicemail

Never miss a lead by allowing your customers to leave voicemail messages. This topic describes how to forward various kinds of calls to voicemail.

Background information

A growing business cannot afford to miss incoming calls. A missed call may make your customers impatient. Forwarding calls to voicemail automatically helps you to stay connected with customers and enhance the service.

In the following scenarios, you can consider a destination as voicemail, which helps the system to forward calls to voicemail:

- Forward extension users' calls to voicemail: The extension user is unavailable to answer a call.
- Set failover destination to voicemail for a ring group or queue: No members or agents are available to take a call or the call reaches the timeout.
- Allow users to leave voicemail messages by IVR: Give the customers an option to leave a voicemail message. When the customers cannot get the information from IVR, they can leave a message.
- Forward inbound calls to voicemail: Immediate phone support is not required.

Forward extension users' calls to voicemail

You can set call forwarding rules for each presence status as users' need, the system will forward extension users' calls to voicemail according to the presence status.

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
2. Click **Presence** tab, select a presence status to configure.
3. In the **Call Forwarding** section, configure call forwarding rules for internal calls (incoming calls from colleagues) and external calls (inbound calls from customers).
    a. Select the checkbox of a forwarding condition.
    b. Select a corresponding destination for the forwarding condition to one of the following options:
        - **Voicemail**: Forward calls to the extension's voicemail box.
        - **Group Voicemail**: Forward calls to a selected group mailbox.
4. Click **Save** and **Apply**.

Set failover destination to voicemail for a ring group or queue

1. Log in to PBX web portal, set failover destination to voicemail.
    - To set failover destination for a ring group, go to **Call Features > Ring Group**, edit the desired ring group.
    - To set failover destination for a queue, go to **Call Features > Queue**, edit the desired queue.
2. In the **Failover Destination** drop-down list, select a corresponding destination to one of the following options:
    - **Extension Voicemail**: Forward calls to the extension's voicemail box.
    - **Group Voicemail**: Forward calls to a selected group mailbox.
3. Click **Save** and **Apply**.

Allow users to leave voicemail messages by IVR

Prerequisites

Update your IVR prompt that would instruct callers to press a key to access voicemail.

Procedure

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. Click **Key Press Event** tab, select a corresponding destination to one of the following options:
    - **Extension Voicemail**: Forward calls to the extension's voicemail box.

- **Group Voicemail**: Forward calls to a selected group mailbox.

3. Click **Save** and **Apply**.

Forward inbound calls to voicemail

On non-working days, you can forward inbound calls to voicemail.

1. Log in to PBX web portal, go to **Call Control > Inbound Route**, edit the desired inbound route.
2. In the **Default Destination** section, select a corresponding destination to one of the following options:
   - **Extension Voicemail**: Forward calls to the extension's voicemail box.
   - **Group Voicemail**: Forward calls to a selected group mailbox.
3. Click **Save** and **Apply**.

Leave a Voicemail Message without Calling the User

This topic describes how to send a voicemail message without ringing extensions.

Background information

Although you can send a message by email or text, sometimes there is no replacement for the emotion, inflection, and sincerity of your voice. When you do not want to disturb someone or when you do not have time for a phone conversation, you can send a voicemail message without calling extension.

It is useful in a team work. When your partners are busy in a meeting or after work, but you have some information that need to share with them, you can send a voicemail message without calling them. It allows your partner to reflect prior to responding.

Prerequisites

This feature is only for internal extension users.

Procedure

1. To leave a voicemail message to a specific extension user, dial feature code (`*12`) followed by extension number (for example, *121001).
2. To leave a voicemail message to a queue, a ring group, or a custom group, dial feature code (`*12`) followed by group voicemail number (for example, *126100).
3. Follow the voice prompt to leave your message.
4. When done, hang up or press `#`.

Tip:
The default feature code for sending voicemail messages is `*12`. You can change, enable, or disable the code on PBX web portal: **Call Features > Feature Code > Voicemail > Leave a Voicemail for Extension/Group Voicemail**.

Forward Voicemail Messages to Email

Email is one of the most popular communication tools for business. Forwarding voicemail messages to email is an efficient business feature that allows employees to receive voicemail audio files as email attachments. This topic describes what you can do with voicemail to email and how to forward voicemail message to email for specific extension users.

Background information

Scenario

For employees who travel frequently and require an efficient way to keep up with voicemail and provide a quick response for the customers, it is an efficient way to get alert timely, listen to voicemails anywhere, and handle business over email.

Benefit

Each time the employees receive a voicemail message, they can receive an email with the new voicemail message attached as a .wav file, including caller ID, time of the call, and callback number.

- **Easy to identify**: In emails, the employees can quickly identify the person who left the message, and listen to voicemail message as they need.
- **Easy to listen**: The employees can check and listen to their voicemail messages via computer, smart phone or mobile device at convenience, instead of calling to voicemail box and navigating through the maze of voice prompts. They can also fast-forward or rewind to reach and repeat the important portion.
- **Easy to share**: The employees can forward emails to share voice messages with teammates to improve collaboration efficiency.
- **Easy to manage**: Managing the communications is easier since all the voicemail messages are in the email box. It is faster to sort, prioritize, scan, delete, and save voicemail message.

Prerequisites

- Make sure there is a valid email address assigned to each extension.
- Make sure the PBX system email works, or the PBX cannot forward the received voicemail to an extension user's email.

Procedure

1. Log in to PBX web portal, go to **Extension and trunk > Extension**, edit the desired extension.
2. Click **Voicemail** tab.
3. In the **New Voicemail Notification** drop-down list, select **Send Email Notifications with Attachment**.
4. In the **After Notification** drop-down list, set how to handle the voicemail message after the system has successfully notified the extension user by email.
5. Click **Save** and **Apply**.

Manage Voicemail Messages

Check Voicemail Messages

This topic describes how to check voicemail messages.

Background information

Methods

Extension users can get an instant voicemail notification when receiving a new voicemail message. There are multiple ways to check voicemail messages anytime and anywhere.

- On an IP phone
- On Linkus client
- Via Email
- Via IVR

Feature code

The default feature code for checking voicemail messages is *2. You can change, enable, or disable the code on PBX web portal: **Call Features > Feature Code > Voicemail > Check Voicemail/Subscribe Voicemail Status**.

Check voicemail messages on an IP phone

Check voicemail messages on a user's own phone

1. Dial feature code *2.
2. Follow the voice prompt to enter your PIN number followed by #.
3. Navigate through the voicemail menu to check your voicemail message.

Check voicemail messages from another phone

1. Dial feature code *2 followed by the extension number whose voicemail will be checked. (for example, to check voicemail of extension 1001, dial *21001).
2. Follow the voice prompt to enter your PIN number followed by #.
3. Navigate through the voicemail menu to check your voicemail message.

Check group voicemail messages from an IP phone

If the **Mode** of group voicemail is set to **Shared by Members**, the users can check the messages in group mailbox. If any users check the new messages, the status of messages will be set as read.

1. Dial feature code *2 followed by the group voicemail number (for example, *26100).
2. Navigate through the voicemail menu to check your voicemail message.

Check voicemail messages on Linkus client

If you have enabled **Linkus Clients** for extension users, the extension users can check voicemail messages on their Linkus clients.

Check voicemail messages via Email

If you have set up the feature of forwarding voicemail messages to email for extensions, the extension users can check their voicemail messages in their email boxes.

Check voicemail messages via IVR

If you have allowed extension users to dial in an IVR to check voicemail messages, the extension users can also check voicemail messages when they are out of office.

1. Dial in an IVR, follow the voice prompt.
2. Dial feature code *2 followed by extension number or group voicemail number, and then enter the PIN number.
3. Navigate through the voicemail menu to check voicemail messages.

Enable or Disable Voicemail Transcription

Yeastar P-Series 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

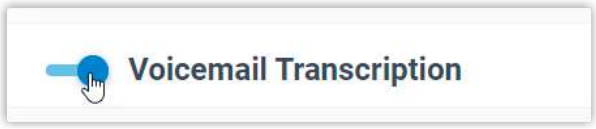
Prerequisites

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**.



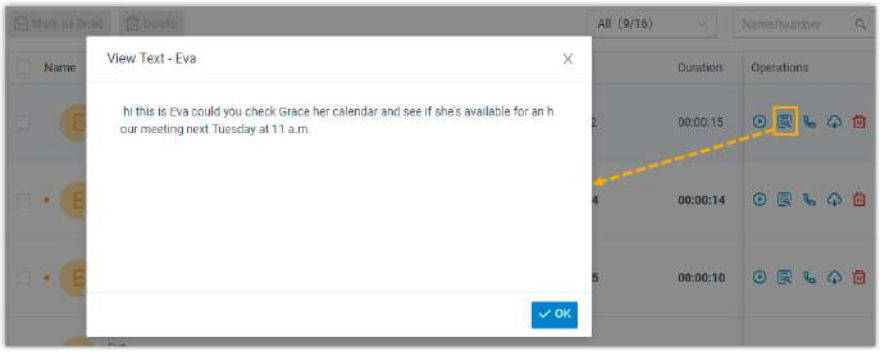
3. Click **Save**.

Result

The Voicemial Transcription feature is enabled, users can receive voicemails in the form of text on different platforms.

Linkus UC Clients

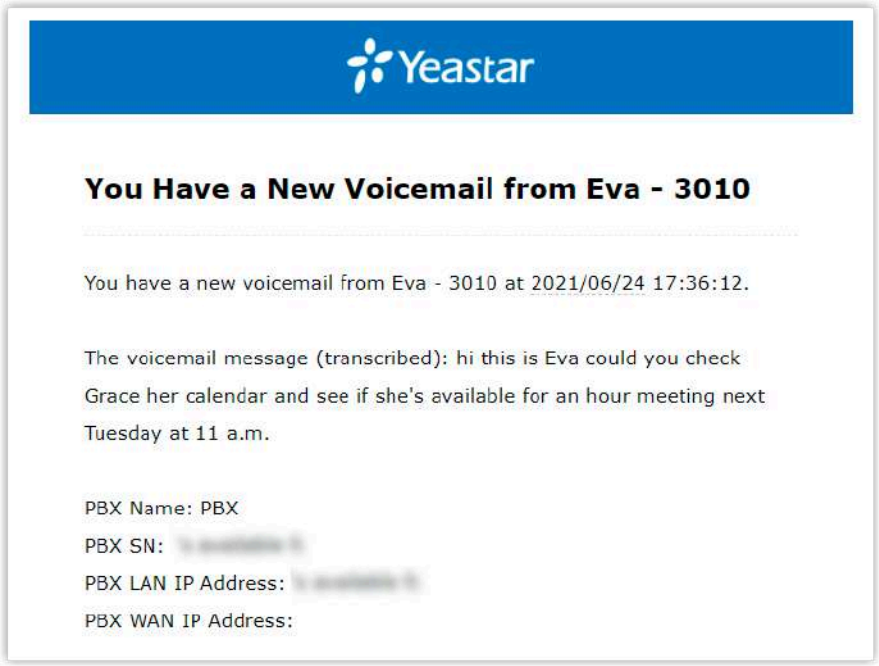
Users can check the transcribed text for each voicemail on Linkus Web Client, Desktop Client, and Mobile Client.



Email Client

If Voicemail to Email feature is enabled, the transcribed text will be displayed in the email content for received voicemails.

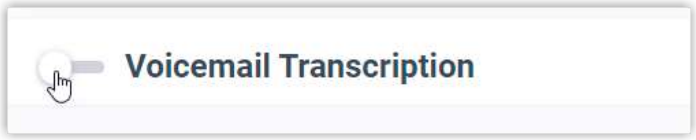
The figure below shows an example of voicemail notification email.



Disable Voicemail Transcription

Procedure

1. Log in to PBX web portal, go to **Call Features > Voicemail > Voicemail Settings**.
2. Scroll down to the bottom of the page, turn off **Voicemail Transcription**.



3. Click **Save**.

Result

The Voicemail Transcription feature is unavailable.

Configure Message Envelope

This topic describes how to enable or disable message envelope.

Background information

Message envelope is given before a voicemail message is played. Message envelop includes the following information:

- Date and Time that the message was received.
- Caller ID information.
- Duration of the message.

You can enable or disable envelope information separately according to user needs.

Configure message envelope for extension voicemail

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
2. Click **Voicemail** tab.
3. Decide whether to enable the following information for the message envelope:
    - **Play Date and Time**: Play the date and time that the message was received.

- **Play Caller ID**: Play the caller ID information.
- **Play Message Duration**: Play the duration of message.

4. Click **Save** and **Apply**.

Configure message envelope for group voicemail

1. Log in to PBX web portal, go to **Call Features > Voicemail > Group Voicemail**, edit the desired group voicemail.
2. In the **Basic** section, decide whether to enable the following information for the message envelope:
   - **Play Date and Time**: Play the date and time that the group voicemail message was received.
   - **Play Caller ID**: Play the caller ID information.
   - **Play Message Duration**: Play the duration of group voicemail message.
3. Click **Save** and **Apply**.

Limit Voicemail Message Length

Limiting voicemail message length is a good way to reduce invalid or lengthy voicemails. This topic describes how to specify the message length (max and min) for a caller to leave a voicemail message.

Procedure

1. Log in to PBX web portal, go to **Call Features > Voicemail > Voicemail Settings > Message Options**.
2. In the **Max Message Time(s)** drop-down list, select a number of seconds.

   Messages exceeding the maximum duration will be automatically cut off.
3. In the **Min Message Time(s)** drop-down list, select a number of seconds.

   Messages less than the minimal duration will be automatically discarded.
4. Click **Save** and **Apply**.

> **Tip:**
> You may need to inform the callers in the greeting to keep their messages brief or under the maximum duration.

Set up a Storage Location for Voicemail Messages

The voicemail messages are stored in Yeastar P-Series 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, decide whether to send email notifications when the user receives a new voicemail.
    - To disable email notifications, select **Do Not Send Email Notifications**.
    - To enable email notifications, select one of the following options:
        - **Send Email Notifications with Attachment**: Send a notification email with the new voicemail message attached as a `.wav` file.
        - **Send Email Notifications without Attachment**: Send notification emails only.
4. If you enabled email notifications, configure the following settings as needed:

Setting	Description
After Notification	Decide how to deal with voicemails after notification emails are sent out. • **Mark as Read**: Mark the voicemail message in mailbox as read. • **Delete Voicemail**: Delete the voicemail messages from mailbox. • **Do Nothing**: Keep the voicemail message in mailbox as unread.

Setting	Description
Send to	Specify the email address for receiving notification emails. • **User Email**: Send notification emails to the user's email address. • **Custom Email**: Send notification emails to a custom email address. Enter the desired email address in the **Custom Email Address** field.

5. Click **Save** and **Apply**.

Custom Voicemail Experience

Allow Callers to Press a Key to Leave Messages

This topic describes how to allow callers to press a key to leave messages.

Background information

By default, when the caller accesses a user's voicemail, PBX starts to record message automatically. It may make callers embarrassed when they are not ready to leave a message or they don't need to leave a message. Even if the caller hangs up directly, the voice mailbox still generates a lot of invalid information.

Procedure

1. Log in to PBX web portal, go to **Call Features > Voicemail > Voicemail Greetings**.
2. In the **Caller Options** section, select the checkbox of **Ask callers to press 5 for leaving a message**.
3. Click **Save**.

Result

The caller can choose whether to leave a message after listening to the greeting, and press 5 to leave a message after he or she is ready.

What to do next

If a custom greeting is used for voicemail, update the greeting that would instruct callers to press 5 for leaving a message.

Allow Callers to Dial Extension from Voicemail

This topic describes how to allow callers to dial extension from voicemail.

Background information

For the employees working in multiple places, they can record a greeting to prompt the caller to dial another extension to reach them. Instead of hanging up and calling again, you can allow the caller to dial extensions directly from voicemail.

It is also useful when the boss is unavailable to answer a call, instead of leaving a message in emergency, the caller can dial the secretary's extension, .

Procedure

1. Log in to PBX web portal, go to **Call Features > Voicemail**.
2. In the **Caller Options** section, select the checkbox of **Allow callers to dial extension**.
3. Select the extensions that can be dialed from the **Available** box to the **Selected** box.
4. Click **Save** and **Apply**.

Result

The caller can press * key to dial an extension.

What to do next

If a custom greeting is used for voicemail, update the greeting that would instruct callers to press * key for dialing an extension.

Allow Callers to Break out from Voicemail

This topic describes how to allow callers to break out from voicemail, and access the operator.

Background information

For technical support, doctor office or sales manager, they do need someone available in case of any emergencies after hours. When callers access the voicemail, it would be nice to allow the callers to press `0` to get to the operator directly in emergency. Otherwise, they have to hang up and redial.

Procedure

You can specify an IVR or an extension for answering such emergency calls.

1. Log in to PBX web portal, go to **Call Features > Voicemail**.
2. In the **Caller Options** section, select the checkbox of **Allow callers to press 0 to break out from voicemail**.
3. In the **Destination** drop-down list, select a destination.
    - **IVR**: Forward the call to an IVR.
    - **Extension**: Forward the call to the specific extension.
4. Click **Save** and **Apply**.

What to do next

If a custom greeting is used for voicemail, update the greeting that would instruct callers to press 0 to break out from voicemail.

Allow Callers to Review Voicemail Messages

Callers can review their voicemail messages after recording. This is important for callers to confirm whether the message is appropriate. This topic describes how to allow callers to review voicemail messages.

Procedure

1. Log in to PBX web portal, go to **Call Features > Voicemail**.
2. In the **Caller Options** section, select the checkbox of **Allow callers to review message**.
3. Click **Save** and **Apply**.

Global Voicemail Settings

The topic describes the global voicemail message settings, including caller options, message options, and greeting options.

Caller options

Setting	Description
Allow callers to press 0 to break out from voicemail	Allow callers to press 0 to exit the voicemail, and reach a specific IVR or an extension.
Allow callers to dial extension	Allow callers to dial other extensions.
Allow callers to press 5 for leaving a message	Allow callers to press 5 to leave a voicemail message after greeting, instead of auto starting recording immediately.
Allow callers to review message	Allow callers to review his/her voicemail message after recording.

Message options

Settings	Description
Max Message Time(s)	Set the maximum duration of one voicemail message. The default maximum voicemail duration that callers can leave is 600 seconds (10 minutes).
Min Message Time(s)	Set the minimum duration of one voicemail message. The default minimum voicemail duration that callers must leave is 2 seconds.

Greeting Options

Settings	Description
Max Greeting Time(s)	Set the maximum greeting duration that is played to caller. The default maximum greeting duration is 60 seconds (1 minute).
Global Voicemail Greeting	Select the greeting that is applied to all extensions.

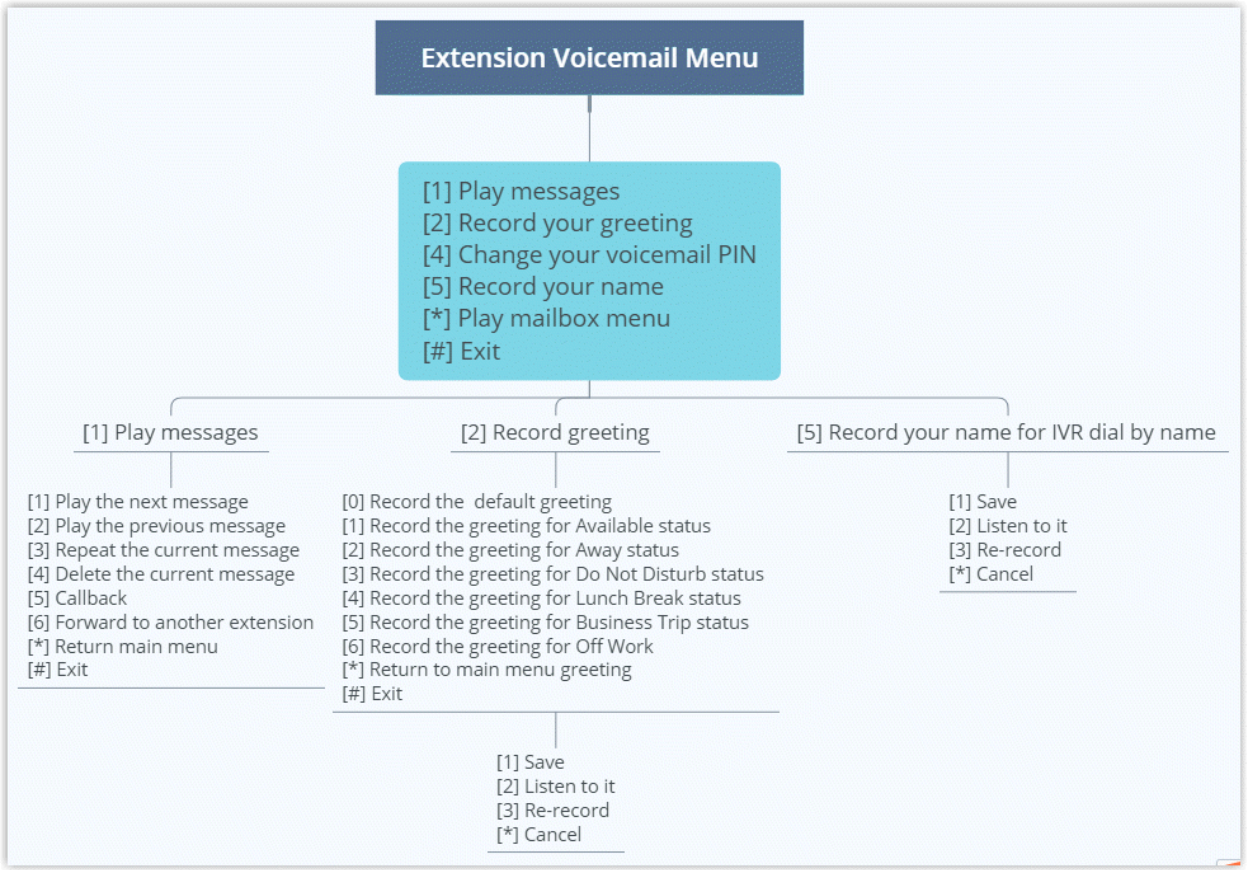
Voicemail Transcription

Decide to enable or disable Voicemail Transcription feature. For more information, see Enable or Disable Voicemail Transcription.

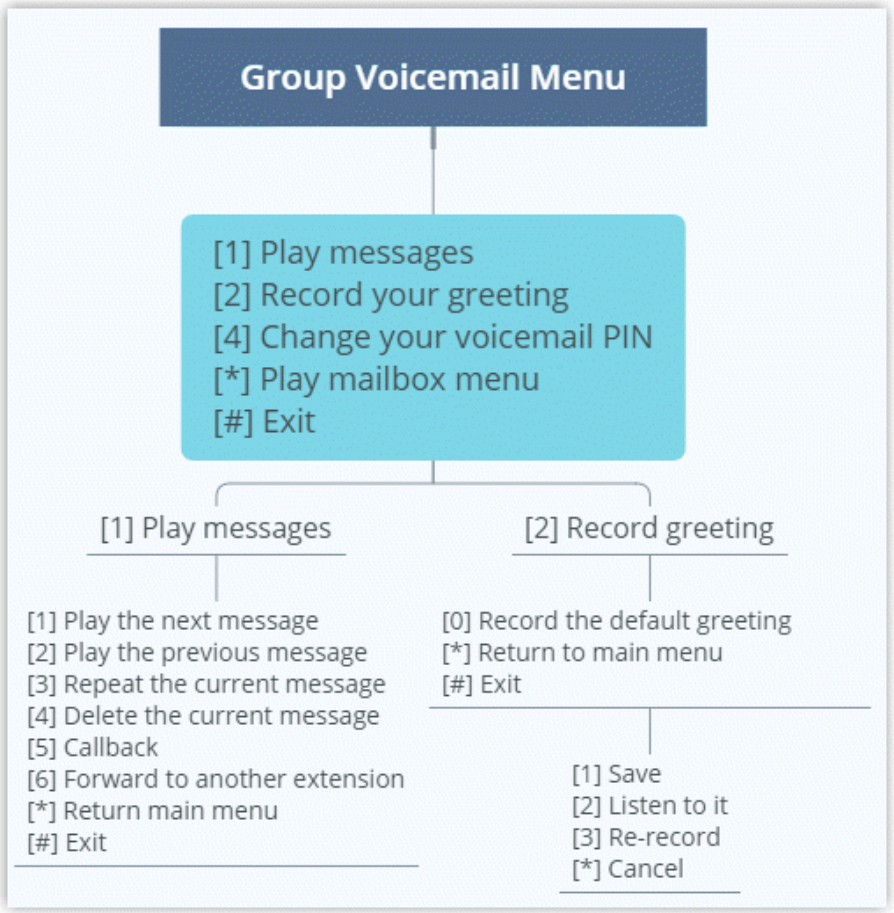
Voicemail Menu Options

This topic shows the quick reference of voicemail menu.

Extension voicemail menu



Group voicemail menu



Voicemail Capacity and Limitations

This topic describes the voicemail capacity and limitation for a voicemail.

Default capacity and limitations for each mailbox

Voicemail box capacity has a limit of 100 messages with maximum 10 minutes for each message. Once they hit that limit, the system auto deletes the old voicemail messages.

There is no limit of the time to keep the voicemail on PBX.

Adjust the capacity and limitations for each mailbox

- To adjust the capacity of voicemail box, see Auto Cleanup Voicemail Messages.
- To adjust the limitation of maximum message time, see Limit Voicemail Message Length.

IVR

Interactive Voice Response (IVR) Overview

Yeastar P-Series 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.
- Allow customers to dial ring group, queue, or conference numbers directly.

For employee

- Allow employees to make an outbound call via an IVR.
- Allow employees to check voicemail via an IVR.

- Allow employees to remotely change IVR prompt by dialing the feature code #9.

IVR keypress events

There are four types of keypress events:

- **Menu options**: The number keys, # key and * key for users to access a desired destination.
- **Invalid**: When an invalid key is pressed, route the call to a desired destination.
- **Timeout**: If no input is detected after the configured timeout, the PBX will forward the call based on the configuration.

Advanced settings

- **Time Condition**: Route inbound calls to different destinations based on time conditions.
- **Language**: Provide language options for callers and play system prompts in their preferred language.
- **Custom Key**: Route inbound calls to different destinations based on PIN code.

Keypress destination

The following options are available for you to assign to the keypress events:

- **Hang Up**: End the current call.
- **Extension**: Route the call to the specified extension.
- **Extension Voicemail**: Allow callers to leave a message for the specified extension.
- **Group Voicemail**: Allow callers to leave a message for a queue, a ring group, or a custom group.
- **IVR**: Allow callers to enter another IVR menu.
- **Ring Group**: Route the call to a specified ring group.
- **Queue**: Route the call to a specified queue.
- **Conference**: Route the call to a specified conference.
- **Dial by Name**: Allow callers to place a call by extension user's name.

  For more information, see Allow Callers to Dial by Name via IVR.
- **External Number**: Route the call to an external number.

- **Play Prompt and Exit**: Play a custom prompt, and then hang up the call.
- **Play Prompt and Return to IVR**: Play a custom prompt, and then back to the IVR.
- **Play IVR Prompt**: Play the IVR prompt, and then hang up the call.

> **Note:**
> - The option is only available for **Invalid Input Destination**.
> - When callers enter a DTMF digit that is not defined in the IVR, the system would repeat the IVR prompt. If the play counts of the IVR prompt reach the maximum number of times, the system would directly hang up the call.

Set up an IVR

Yeastar P-Series 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.
- **Allow Calling Numbers**: Whether to allow callers to dial ring group, queue, or conference numbers via IVR.
- **Dial Outbound Routes**: Whether to allow callers to make outbound calls via IVR.
- **Dial to Check Voicemail**: Whether to allow users to check voicemail via IVR.
- **Dial #9 to Modify IVR Prompt**: Whether to allow users to dial the feature code #9 to record and apply a new IVR prompt.

> **Note:**
> If the IVR prompt is replaced successfully, the previous voice prompt will be removed from the IVR prompt setting, and the new voice prompt will be retained.

3. Click the **Key Press Event** tab, set up an IVR menu.
   - To set key events to route calls to different destinations based on time, see Set Key Events Based on Time Conditions.
   - To set key events to route calls to different destinations based on PIN code, see Set up IVR Custom Key.

- To set key events to always route calls to the designated destination, do as follows:
    a. In the **Key Press** drop-down list, select a key event for each key: 0-9, *, and #.
    b. In the **Response Timeout** drop-down list, select a call routing destination if the caller remains inactive within the **Prompt Repeat Count**.
    c. In the **Invalid Input Destination** drop-down list, select a call routing destination if the caller enters a digit that is not defined in the IVR.
    d. **Optional:** Select the checkbox of **Allow Opt-out of Call Recording**.

    When the call is routed to the key press destination, the call would not be recorded even **Call Recording** is enabled.

4. Click **Save** and **Apply**.

What to do next

Set up an inbound route, and specify the destination to the IVR.

Related information

Allow Callers to Dial Extensions via IVR
Allow Callers to Dial Numbers via IVR
Allow Callers to Dial by Name via IVR
Allow Callers to Dial Outbound Calls via IVR
Allow Callers to Change IVR Prompt Remotely
Forward Incoming Calls to an External Number via IVR
Set up a Multi-language IVR
Set Key Events Based on Time Conditions
Set up IVR Custom Key

Set up IVR Prompts

A custom greeting and prompt allow you to provide a more personalized experience for your customers. This topic describes how to set up IVR prompts according to your IVR menu.

IVR prompt types

Generally, an IVR prompt consists of several pieces of information:

- **Welcome greeting**: Welcome greeting is the first message that callers hear when they call in an IVR.

  For example, "Thank you for calling Yeastar".

- **Menu prompt**: Present callers with a series of options.

  For example, "If you got something urgent, please press 1 to contact our support. To leave a voicemail, please press 2".
- **Goodbye greeting**: Play the greeting before ending a call.

Prepare audio files for IVR prompt

The PBX system has a default IVR prompt. You can customize IVR prompt using a single audio file or multiple audio clips.

Customize IVR prompt by a single audio file

You can record greeting, IVR menu, or any messages in a single audio file. It is easy to manage and reduce the number of prompts.

Customize IVR prompt by multiple audio clips

Yeastar IVR also allows you to specify up to 5 different audio files as IVR prompt. The system plays the audio files in order when a customer calls in IVR.

It is better to divide your IVR prompt into multiple audio clips in the following scenarios:

- Modify the IVR prompt frequently.

  Every time you modify the IVR menu, you need to update IVR prompt. Divide your IVR prompt into multiple audio clips according to the content, such as clip 1 for Welcome greeting, clip 2 for menu prompt, and so on. Next time, when you need to change the IVR prompt, just replace the specific clip.
- A single audio file exceeds the limit.

  The uploaded file should meet the audio file requirements. You can not upload an audio file larger than 8 MB. Divide the audio file into multiple audio clips to solve this issue.

Update the IVR prompts

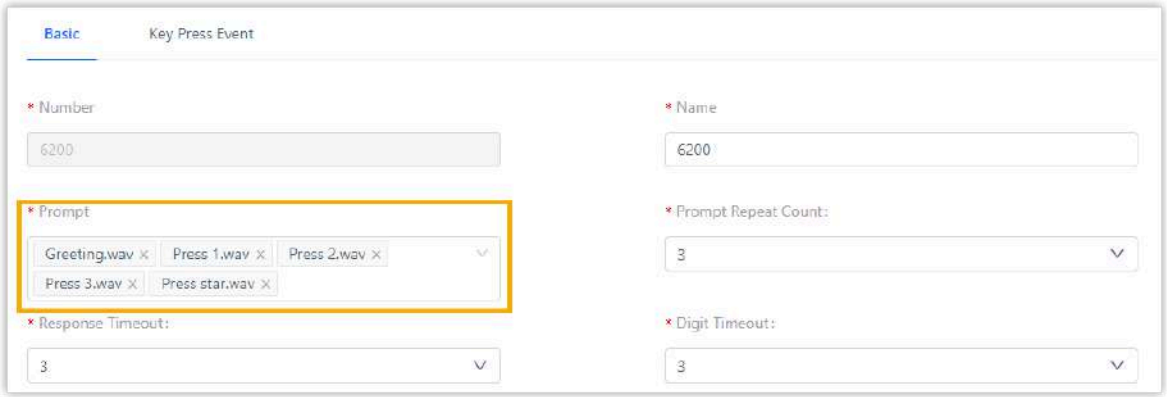
1. Log in to PBX web portal, go to **PBX Settings > Voice Prompt > Custom Prompt**, upload a custom prompt or record a custom prompt.

   Note:

> The uploaded file should meet the audio file requirements.

2. Go to **Call Features > IVR**, edit the desired IVR.
3. In the **Prompt** drop-down list, select your custom prompts.

   You can select up to 5 audio files, and the system plays the audio files in order.



4. In the **Prompt Repeat Count** drop-down list, select prompt repeat times.
5. Click **Save** and **Apply**.

Related information

Allow Callers to Change IVR Prompt Remotely

Allow Callers to Dial Extensions via IVR

This topic describes how to allow callers to dial extensions directly via an IVR.

Background information

For new customers, IVR can help them reach the desired employee or department. But for old customers, it is inconvenient for them to listen to audio prompts and make selections to reach the right employee or department, even they know the extension number.

For the callers who know the extension number, it is better to allow them to dial an extension number directly.

Prerequisites

Before you set up dialing extension directly via an IVR, update your IVR prompt that would instruct callers to dial an extension number.

Procedure

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. In the **Prompt** drop-down list, select the updated IVR prompt.
3. In the **Dial Extensions** drop-down list, select which extension as available or available for callers to dial.
    - **All Extensions**: The callers can dial all the extensions.
    - **Allowed Extensions**: The callers can dial the selected extensions.
    - **Restricted Extensions**: The callers can dial any extensions except the restricted extensions.
4. Click **Save** and **Apply**.

Allow Callers to Dial Numbers via IVR

When callers enter an IVR, if they know the number of a ring group, queue or conference room, they can dial the number directly to reach the destination. This topic describes how to allow callers to dial ring group, queue, or conference room numbers via an IVR.

Requirements

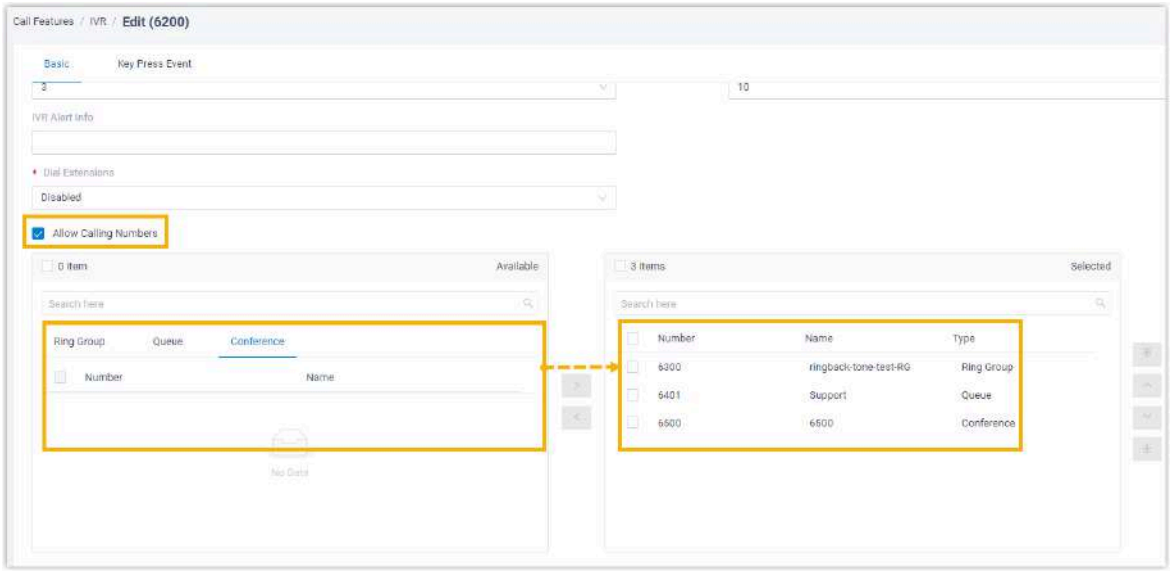
The firmware version of PBX server is 83.16.0.70 or later.

Prerequisites

- An IVR has already been set up, and ring group(s), queue(s) or conference(s) have been configured as you need.
- Upload or record an IVR prompt that would instruct customers to dial ring group, queue, or conference room numbers in an IVR.

Procedure

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. Select the checkbox of **Allow Calling Numbers**, then select the desired ring group, queue, or conference from the **Available** box to the **Selected** box.



3. Click **Save** and **Apply**.

Result

When callers enter an IVR, they can enter the number of ring group, queue or conference to reach the destination.

Allow Callers to Dial by Name via IVR

For the customers who don't remember an employee's extension number, you can allow them to reach the employee by entering the first three letters of the employee's first name or last name in an IVR. It is easier for customers to get to the right person.

Restrictions

The **Dial by Name** feature supports to search the extension users whose caller ID names are composed of English letters or Mandarin phonetic symbols.

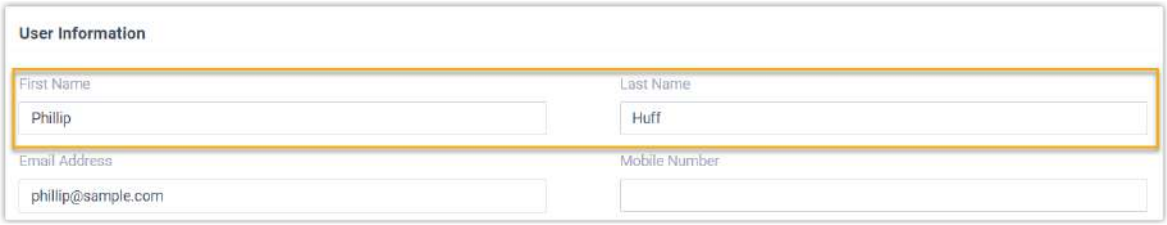
Procedure

1. Specify an extension's caller ID name
2. Set display format for extensions' caller ID name
3. Customize IVR prompt
4. Configure an IVR

Specify an extension's caller ID name

When using **Dial by Name**, the IVR performs a search on an extension's caller ID name, which is composed of the first name and last name of the extension user. Therefore, make sure you have configured the caller ID name for extensions.

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
2. In the **User Information** section, specify the **First Name** and **Last Name** for the extension.

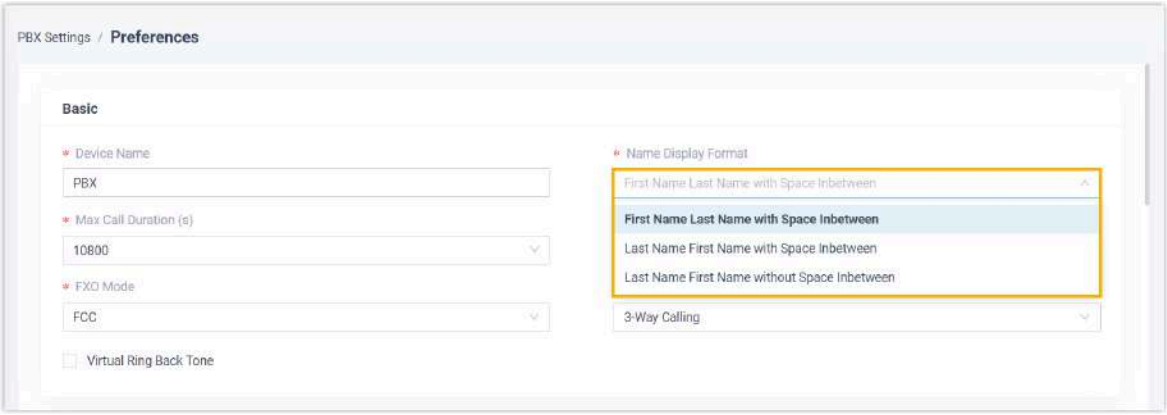


3. Click **Save** and **Apply**.

Set display format for extensions' caller ID name

When searching for extensions by name, the IVR starts from the beginning of extensions' caller ID name. By setting display format for extensions' caller ID name, you can determine how callers can reach employee - either by **First Name** or **Last Name**.

1. Log in to PBX web portal, go to **PBX Settings > Preferences**.
2. In the **Name Display Format** drop-down list, select a display format.



- To allow callers to reach extension users by first name, select **First Name Last Name with Space Inbetween**.
- To allow callers to reach extension users by last name, select **Last Name First Name with Space Inbetween** or **Last Name First Name without Space In-between**.

3. Click **Save** and **Apply**.

Customize IVR prompt

You need to prepare a custom IVR prompt, instructing the callers to press a specific key in an IVR to enter the **Dial by Name** feature.

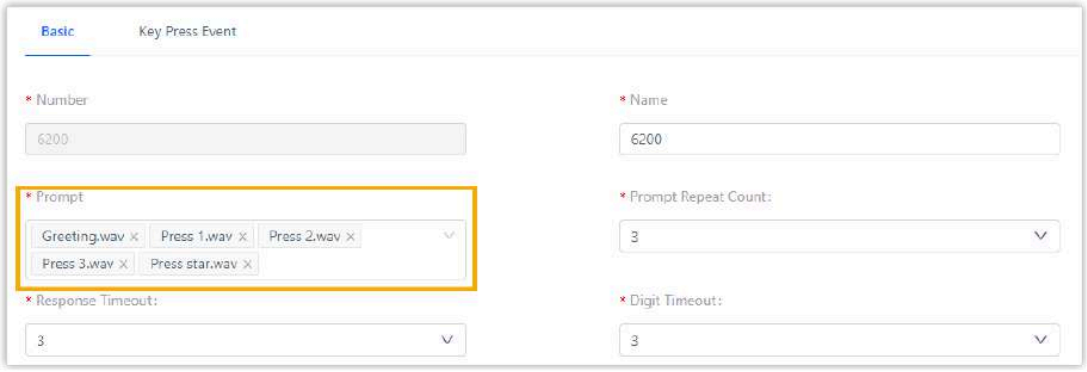
1. Log in to PBX web portal, go to **PBX Settings > Voice Prompt > Custom Prompt**.
2. Upload a custom prompt or record a custom prompt.

> **Note:**
> The uploaded file should meet the audio file requirements.

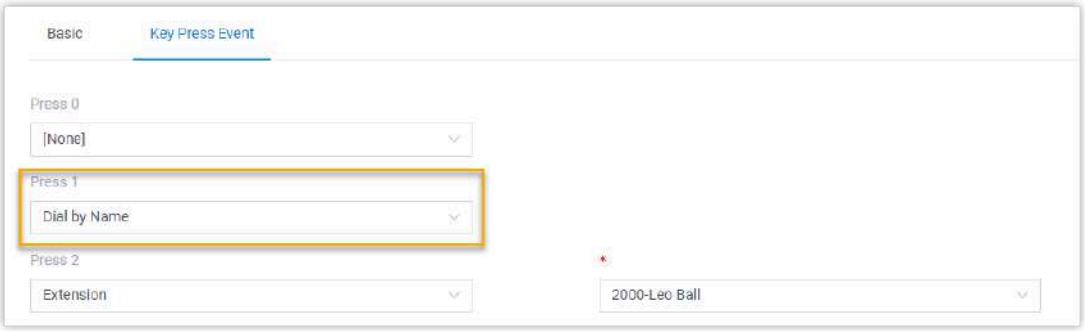
Configure an IVR

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. Update the IVR prompt.
   a. Go to the **Basic** tab.
   b. In the **Prompt** drop-down list, select your custom prompts.

   You can select up to 5 audio files, and the system plays the audio files in order.



3. Set up the IVR keypress destination.
   a. Go to the **Key Press Event** tab.
   b. In the drop-down list of a key press, select **Dial by Name**.



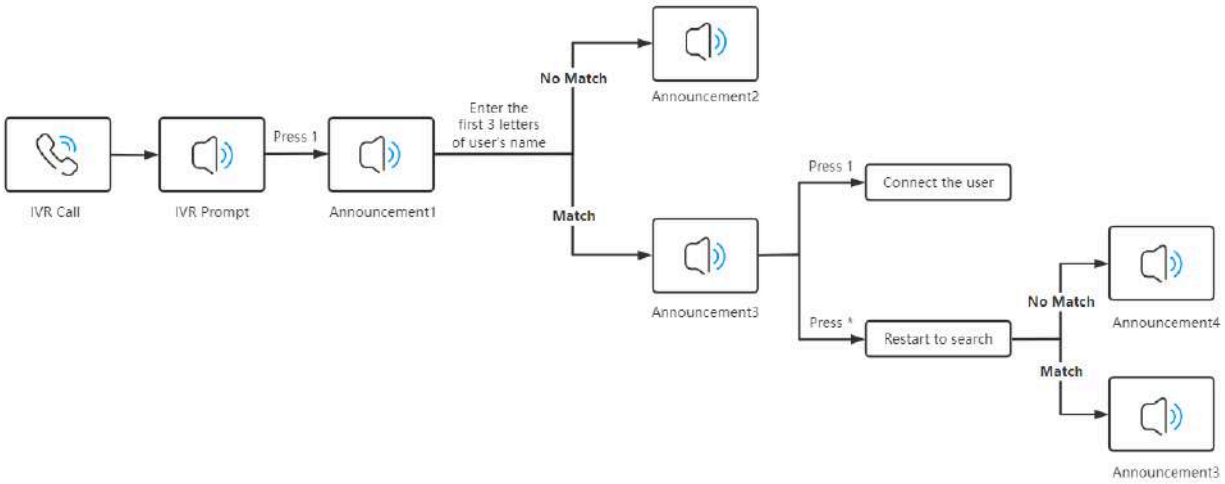
4. Click **Save** and **Apply**.

Result

Customers can call to the IVR, and quickly search the desired extension user by entering the first 3 letters of his/her name.

Example

We provide an example to help you understand the workflow of dial-by-name. In this example, the display format for extensions' caller ID name is set to **First Name Last Name with Space Inbetween** and the destination of key "1" is set to **Dial by Name**.



1. A caller calls into an IVR and hears the IVR prompt.
2. The caller presses "1" to enter the **Dial by Name** feature.
3. After hearing the announcement1, the caller enters the first 3 letters of an extension user's first name.

   For example, to search an extension user with the name "Phillips Huff", the caller needs to dial 7-4-4 (indicating `P H I`) on the phone's keypad.

4. The IVR will look for the best match and play the corresponding announcement.
   - If there is no matched user, the IVR plays announcement2.
   - If there is a matched user, the IVR plays announcement3, providing the extension user's name and extension number, as well as the following operation instructions:
     - **1**: If this is the person you are looking for, press 1 now.

       The IVR will send the call to the extension user.
     - *: Otherwise please press star now.

       The IVR will start a new search, and provide another matched user's information to the caller. If there is no more matched user, IVR will play announcement4.

Default announcement of Dial by Name

Yeastar provides the default announcements when the caller selects the **Dial by Name** option. An announcement is played in the following scenarios:

Announcement	scenario
Welcome to the directory. Please enter the first three letters of your party's first name, using your touch tone keypad, use the 7 key for Q, and the 9 key for Z.	Play when the caller presses a key to dial by name.
No directory entries match your search.	Play when there is no matching directory entries after the caller enters three letters.
[Name] extension [Number] If this is the person you are looking for, press 1 now, otherwise please press star now.	Play when there are matching directory entries after the caller enters three letters.
There are no more compatible entries in the directory.	Play when there are no more compatible entries in the directory after the caller presses * key to search.

Allow Callers to Dial Outbound Calls via IVR

This topic describes how to allow callers to dial outbound calls in an IVR.

Background information

Dialing outbound calls via an IVR is useful when you interconnect two PBXs between headquarters and branch, and only set an IVR on headquarters PBX. You can allow the customers to dial the headquarters' extension number to contact the employees or departments in branch directly.

Prerequisites

- Set up the appropriate outbound route and inbound route on the two interconnected PBXs.
- Upload or record IVR prompt that would instruct customers to dial an outbound call.

Procedure

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. In the **Prompt** drop-down list, select the updated IVR prompt.
3. Select the checkbox of **Dial Outbound Routes**.
4. Select the desired outbound route from the **Available** box to the **Selected** box.
5. Click **Save** and **Apply**.

Allow Callers to Change IVR Prompt Remotely

In case of emergency (e.g. the office needs to close early due to bad weather), you may need to change IVR prompt. Instead of logging in to PBX with a computer to change IVR prompt, you can just make a call to the IVR, then dial a specific feature code to record and apply a new IVR prompt.

Restrictions

- The number of custom prompts does NOT reach the maximum limit. Otherwise, users can NOT record new voice prompt for the IVR.
- A maximum of 2-minute recording time is allowed.

Procedure

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. In the **Basic** tab, select the checkbox of **Dial #9 to Modify IVR Prompt**.
3. In the **IVR Prompt Modify Password** field, enter a password for authentication.

   Callers need to enter the password to authenticate, so as to change the IVR prompt.
4. Click **Save** and **Apply**.

Result

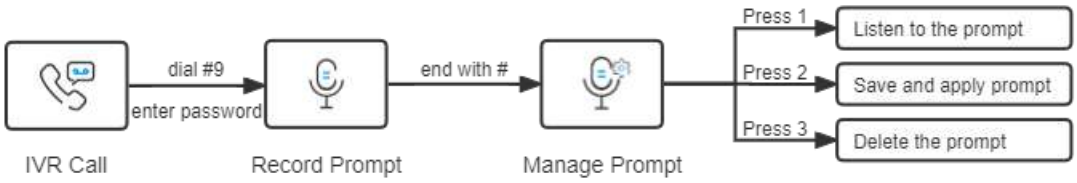
Users can call to an IVR, dial #9 and enter the password, then follow the voice prompt to record a new IVR prompt on their phones.

If IVR prompt is replaced successfully, the previous voice prompt will be removed from the IVR setting, and the new voice prompt will be retained.

Note:
The new voice prompt is save on **PBX Settings > Voice Prompt > Custom Prompt**, with a prompt name in the format of **IVR*{ivr_number}*Date*{date}*Number*{extension_number}***.

Example

We provide an example to help you understand the workflow of remotely changing IVR prompt.



1. In an IVR call, a caller dials #9, then enter the password to authenticate.
2. After hearing the beep tone, the caller starts recording the prompt. When done, press # key.
3. The caller can press a specific key to manage the prompt:
   - **1**: Listen to the prompt.
   - **2**: Save and apply the prompt to the IVR.
   - **3**: Delete the prompt.

Forward Incoming Calls to an External Number via IVR

This topic describes how to allow callers to reach a specific external number in an IVR.

Background information

Forward Incoming Calls to an External Number with IVR is typical and important for 24x7 services, such as Doctor Answering Services and IT Support Services.

For Doctor Answering Services

When a patient calls in an hospital IVR, the patient can press a key to reach the external Doctor Answering Service to schedule an appointment or ask health questions and medical questions.

For IT Support Services

When your customers call in your office IVR after hours, you can give them an option to connect to an emergency support line. This emergency support line can be a Maintenance Engineer's mobile phone number.

Prerequisites

Before you allow callers to reach a specific external number in an IVR, update your IVR prompt that would instruct callers to press a key to reach the external number.

Procedure

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. In the **Prompt** drop-down list, select the updated IVR prompt.
3. Click **Key Press Event** tab.
4. Select a key to set key press event to **External Number**.
5. **Optional:** In the **Prefix** field, enter the prefix of outbound route so that PBX can successfully route incoming calls to external number.
   - If the **Strip** of outbound route is not set, you don't have to set the **Prefix**.
   - If the **Strip** of outbound route is set, you need to set the **Prefix** according to the **Patterns** of outbound route.
6. Enter the external number, such as a Doctor Answering Service number or a mobile phone number.
7. Click **Save** and **Apply**.

IVR Configuration Example

This topic shows the examples of single IVR configuration and multi-level IVR configuration.

A Single IVR Configuration

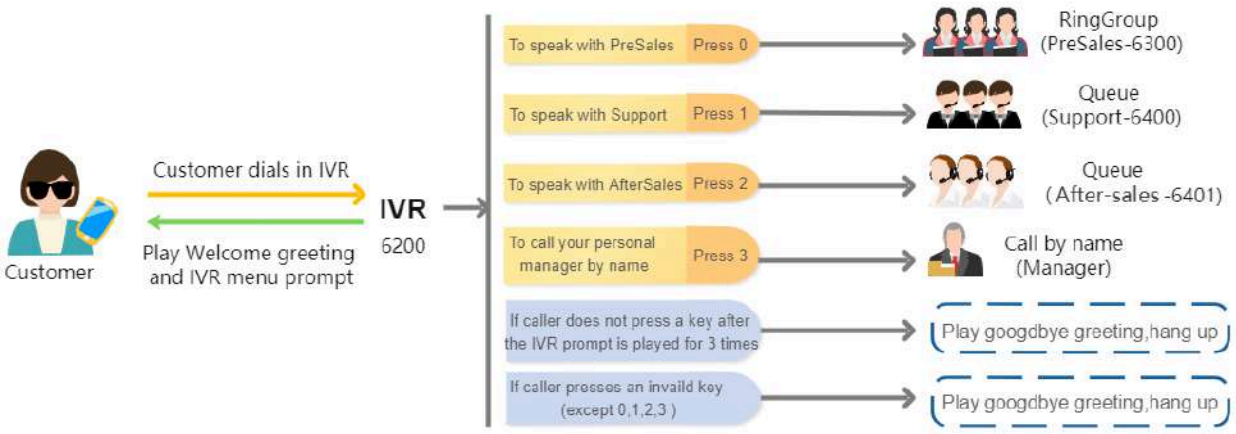
Background information

A company needs an IVR to redirect calls to Pre-sales, Support, After-sales, and personal manager.

We assume that all ring groups, call queues, audio prompts, and inbound routes used in this example are previously configured.

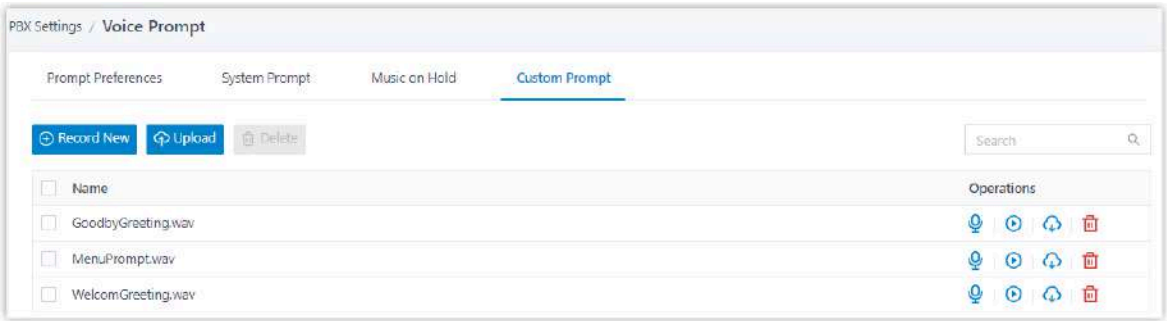
Step1. Design an IVR

When the customers dial in IVR (6200), they can access different service based on their business.



Step2. Upload IVR Prompts

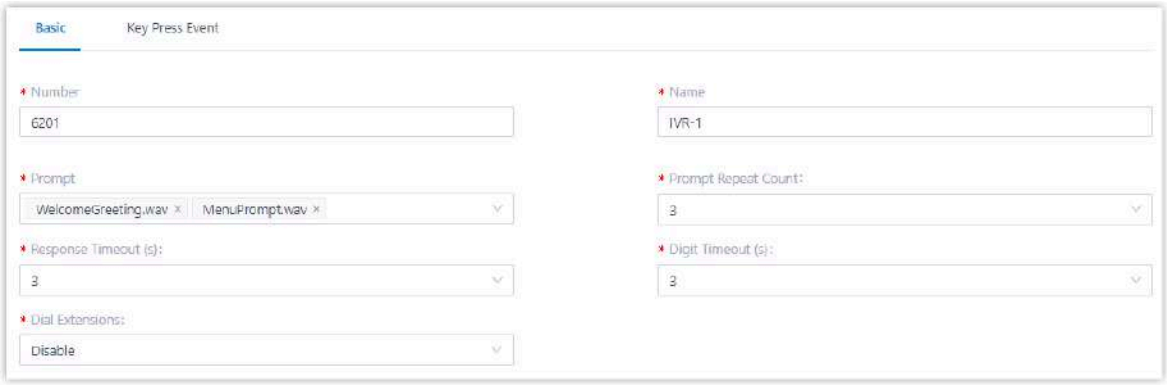
1. Go to **PBX Settings > Voice Prompt > Custom Prompts**, click **Upload**.
2. Select the audio files to upload.



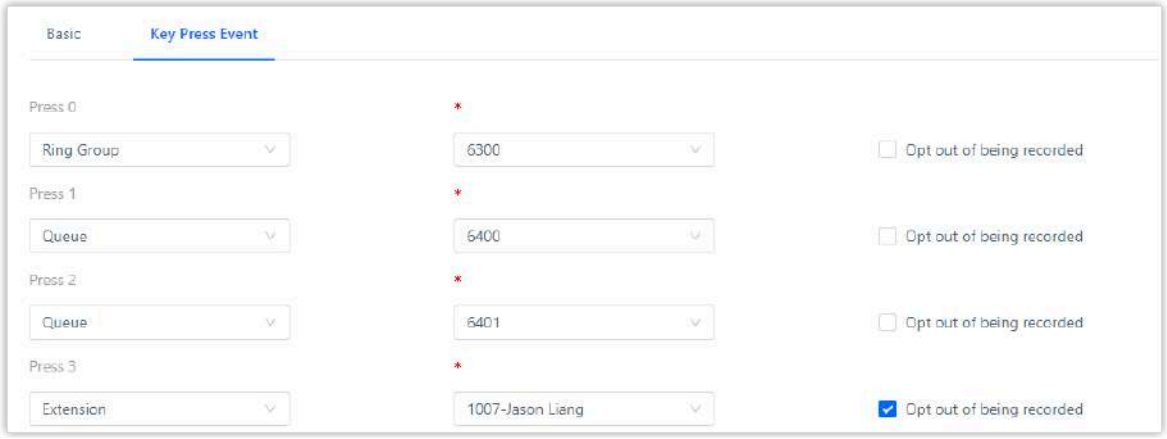
3. Click **Save** and **Apply**.

Step3. Set up an IVR

1. Go to **Call Features > IVR**, click **Add**.
2. In the **Basic** tab, set the basic settings of IVR.



3. In the **Key Press Event** tab, set up an IVR menu.



4. Click **Save** and **Apply**.

Multi-level IVR Configuration

Background information

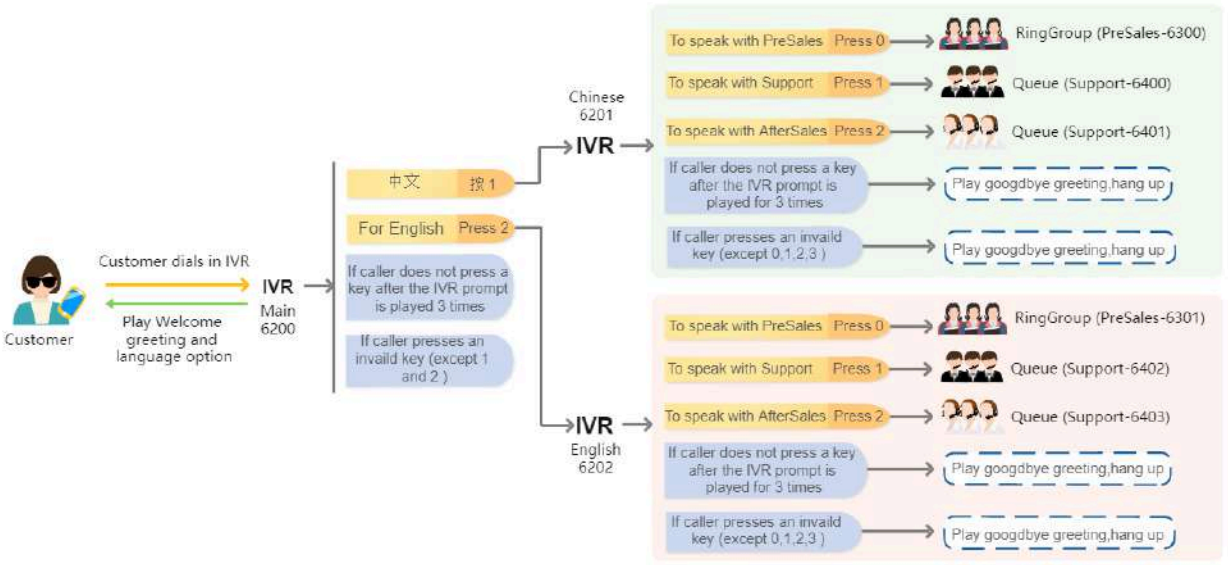
As business expands, the company needs to offer callers a bilingual auto-attendant feature based on their language selection. When the customer dials in to IVR, they can select a specific language to be used when playing prompts.

To achieve this, company needs to upgrade its IVR system allowing support of multi-language. We assume that all ring groups, call queues, extensions, audio prompts, and inbound routes used in this example are previously configured.

Step1. Design IVRs

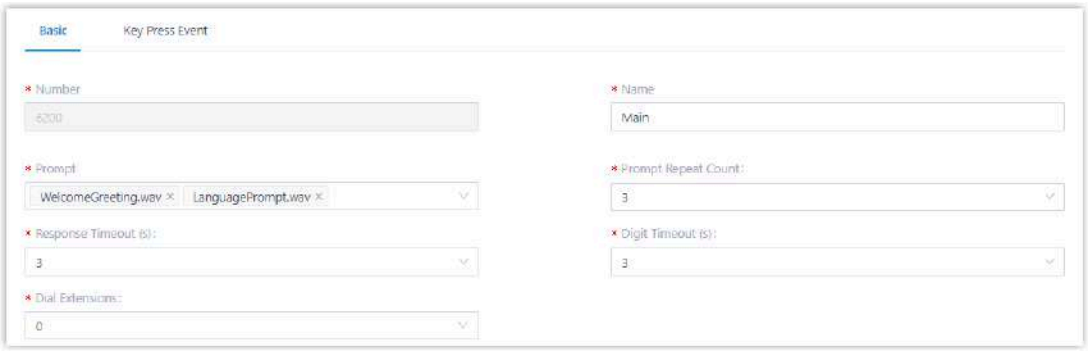
When the customers dial in to IVR-Main (6200), they can select a specific language to use.

- If customers select Chinese, the call will be redirected to IVR-Chinese (6201).
- If customers select English, the call will be redirected to IVR-English (6202).



Step2. Set up IVRs

1. Set up the different IVRs with the same configuration for different language as shown in a single IVR configuration.
   - IVR-1 (6201)
   - IVR-2 (6202)
2. Set up main IVR-Main (6200).
   a. In the **Basic** tab, set the basic settings of IVR.



b. In the **Key Press Event** tab, set up an IVR menu.

- Specify IVR-Chinese (6201) for key 1.
- Specify IVR-English (6202) for key 2.

3. Click **Save** and **Apply**.

   The following figure displays the different IVRs created.

Advanced IVR Settings

Set Key Events Based on Time Conditions

Yeastar P-Series Software Edition supports setting IVR key press events based on time conditions, enabling the routing of incoming calls to different destinations based on the

time they are received. You can apply a single time condition for all key press events or customize time conditions for each key press event.

Requirements

Yeastar P-Series Software Edition is 83.18.0.59 or later.

Apply the same time condition for all key press events

1. Log in to PBX web portal, go to **Call Features > IVR**.
2. Click  beside the desired IVR.
3. In the **Key Press Event** tab, configure key press events to route calls according to your needs.

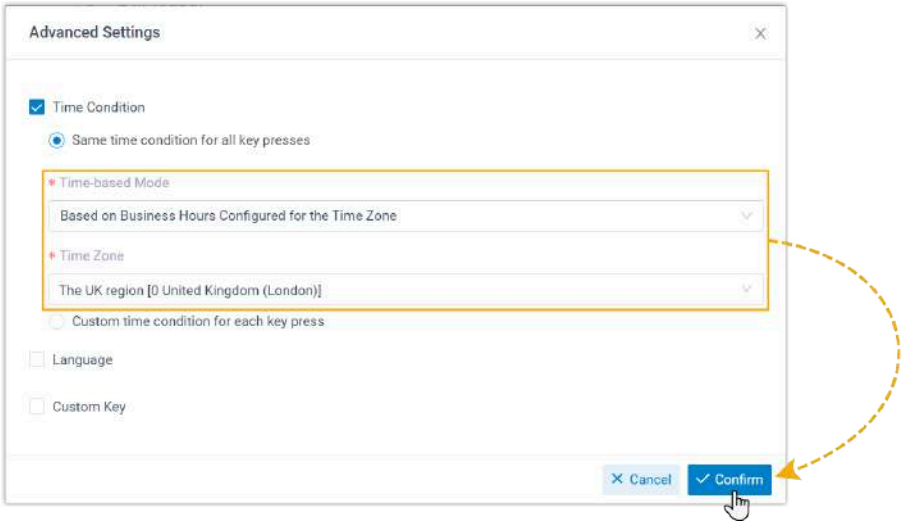
Scenario	Description
Route calls based on business hours configured in specific time zone	All key press events route calls to specified destinations based on the business hours, non-working hours, and holidays configured in a specific time zone (Defined on **Call Control > Business Hours and Holidays**). For detailed instructions, see Route calls based on business hours in specific time zone.
Route calls based on custom business hours	Create a custom business hours based on the system's default time zone, and all key press events route calls to specified destinations based on the custom business hours, non-working hours, and holidays. For detailed instructions, see Route calls based on custom business hours.
Route calls based on custom time periods	Create a custom time period based on the system's default time zone for each key press event, and route calls based on the custom time period accordingly. For detailed instructions, see Route calls based on custom time periods.

Route calls based on business hours in specific time zone

a. On the top-right corner, click **Advanced Settings**.

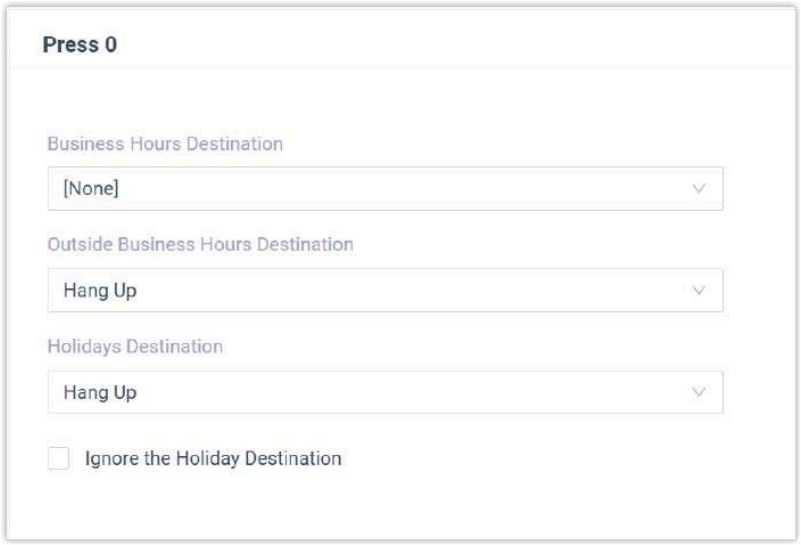
b. In the pop-up window, select the checkbox of **Time Condition**, and select **Same time condition for all key presses**.

c. In the **Time-based Mode** drop-down list, select **Based on Business Hours Configured for the Time Zone**, select the desired time zone, and click **Confirm**.



The global business hours is applied to all key press events in the IVR.

d. Specify call routing destinations for a key press event based on the global business hours.



- **Business Hours Destination**
- **Outside Business Hours Destination**
- **Holidays Destination**

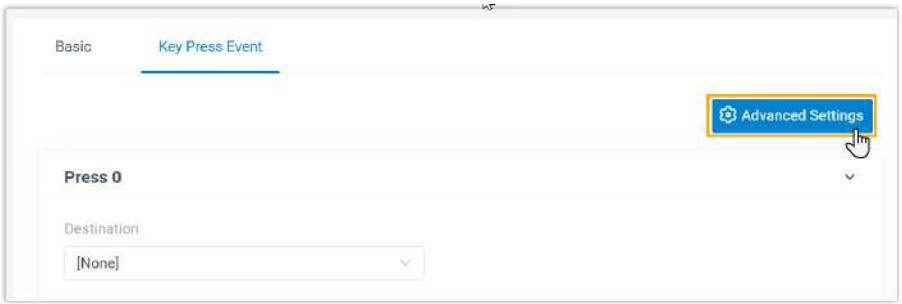
> **Note:**
> If you want to route calls based on global business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**.

e. Repeat step **d** for all the desired keys.

f. Click **Save** and **Apply**.

Route calls based on custom business hours

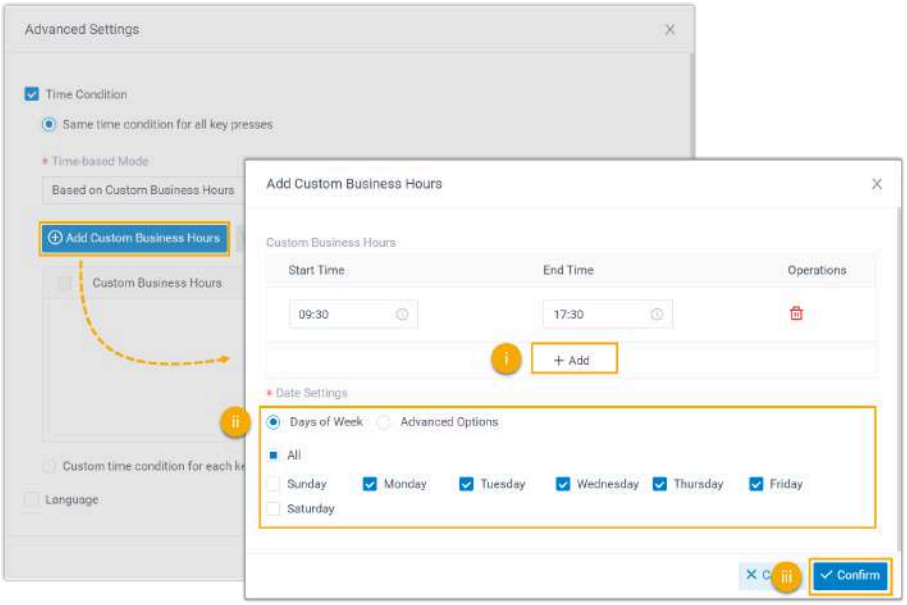
a. On the top-right corner, click **Advanced Settings**.



b. In the pop-up window, select the checkbox of **Time Condition**, and select **Same time condition for all key presses**.

c. In the **Time-based Mode** drop-down list, select **Based on Custom Business Hours**.

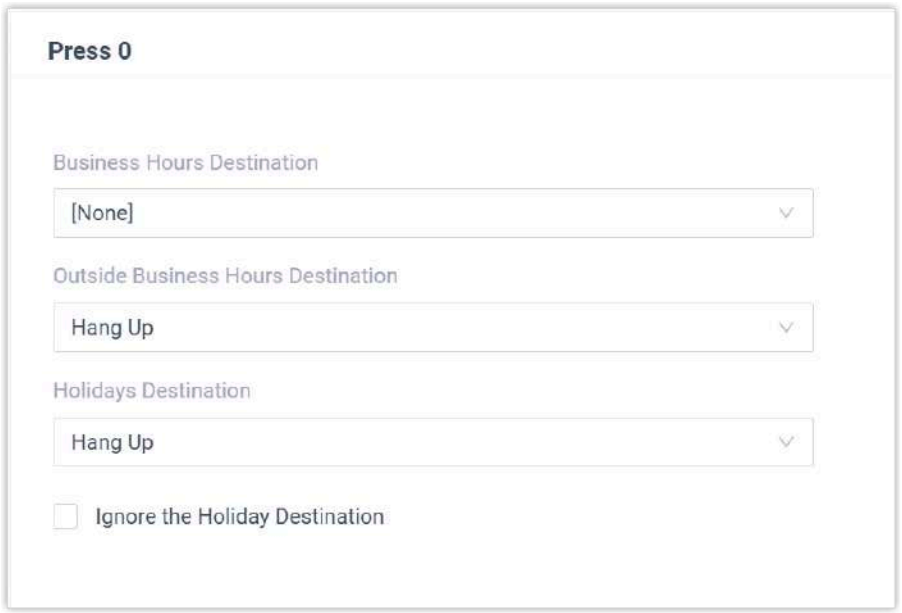
d. Click **Add Custom Business Hours** to create custom business hours based on the system's default time zone.



i. Click **Add** and specify the start time and end time.

ii. In the **Date Settings** section, specify the workdays.
iii. Click **Confirm**.

e. Click **Confirm** to apply this custom business hours to all key press events in the IVR.
f. Specify call routing destinations for a key press event based on the custom business hours.



- **Business Hours Destination**
- **Outside Business Hours Destination**
- **Holidays Destination**

> **Note:**
> If you want to route incoming calls based on custom business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**.

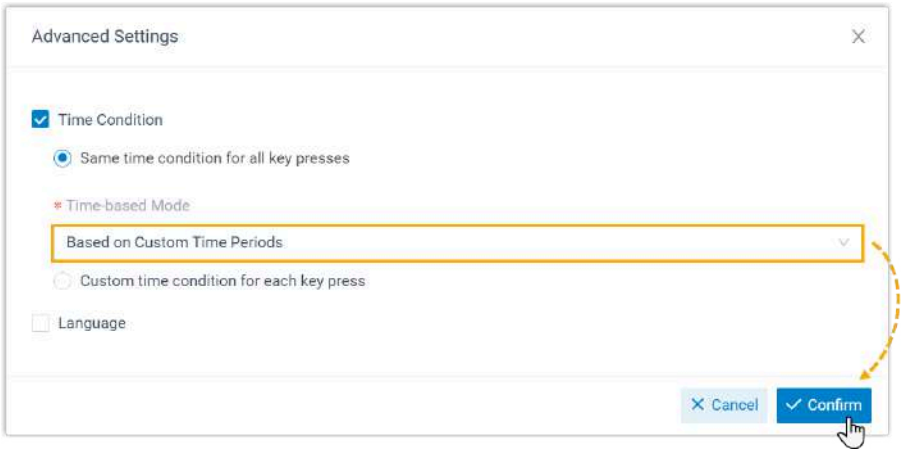
g. Repeat step **f** for all the desired keys.
h. Click **Save** and **Apply**.

Route calls based on custom time periods

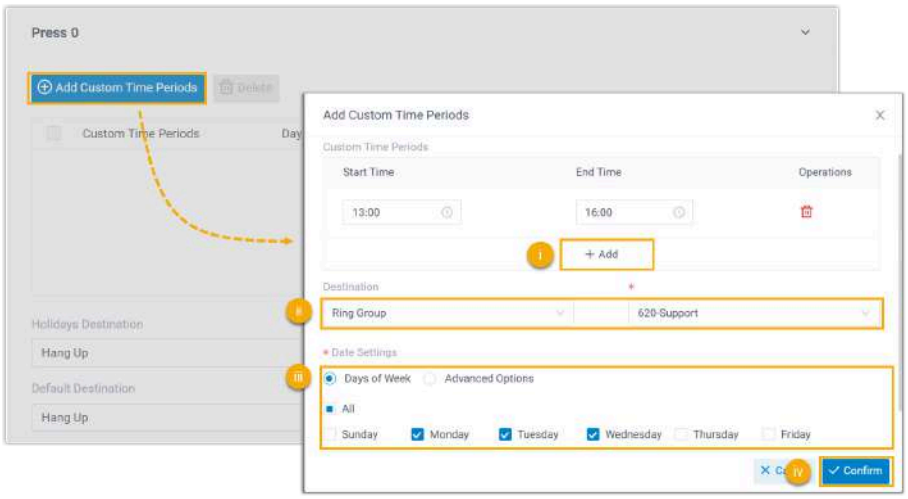
a. On the top-right corner, click **Advanced Settings**.

b. In the pop-up window, select the checkbox of **Time Condition**, and select **Same time condition for all key presses**.

c. In the **Time-based Mode** drop-down list, select **Based on Custom Time Periods**.



d. Under a key press event, click **Add Custom Time Periods** to create a custom time period based on the system's default time zone for the key.



i. Click **Add** and specify the start time and end time.
ii. In the **Destination** drop-down list, specify the destination for calls within the custom time periods.
iii. In the **Date Settings** section, specify the workdays.
iv. Click **Confirm**.

> **Note:**
> The specified custom time periods ONLY take effect for this key press event.

e. Specify the following call routing destinations for the key press event.

- **Holidays Destination**: Specify the call routing destination for calls during holidays.

> **Note:**

> If you want to route incoming calls based on custom time periods during holidays, select the checkbox of **Ignore the Holiday Destination**.

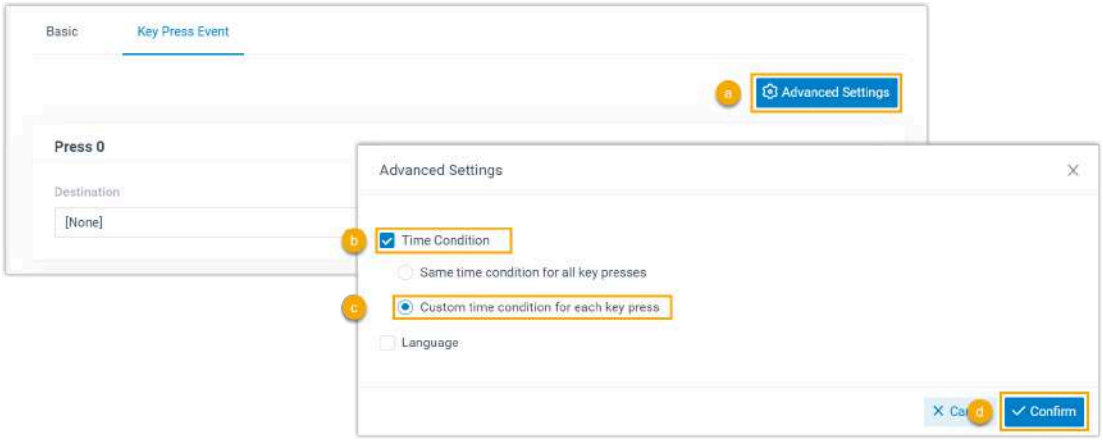
- **Default Destination**: Specify the call routing destination for calls outside the custom time periods.

f. Repeat step **d** - **e** for all the desired keys.

g. Click **Save** and **Apply**.

Apply different time conditions for each key press event

1. Log in to PBX web portal, go to **Call Features > IVR**.
2. Click beside the desired IVR.
3. In the **Key Press Event** tab, enable time-condition settings for this IVR.



a. On the top-right corner, click **Advanced Settings**

b. In the pop-up window, select **Time Condition**.

c. Select **Custom time condition for each key press**.

d. Click **Confirm**.

4. In the **Time-based Mode** drop-down list of a key, select the time condition and configure the call routing destinations.

Option	Description
All Time	Always route calls to the specified destination. For detailed instructions, see Route calls at all times.
Based on Business Hours Configured for the Time Zone	Route calls to specified destinations based on the business hours, non-working hours, and holidays of a specific time

Option	Description
	zone (Defined in **Call Control > Business Hours and Holidays**). For detailed instructions, see Route calls based on global business hours.
Based on Custom Business Hours	Create a custom business hours based on the system's default time zone, and route calls to specified destinations based on the custom business hours, non-working hours, and holidays. For detailed instructions, see Route calls based on custom business hours.
Based on Custom Time Periods	Create a custom time period based on the system's default time zone and route calls based on the custom time period. For detailed instructions, see Route calls based on custom time periods.

Route calls at all times

a. In the **Time-based Mode** drop-down list, select **All Time**.
b. In the **Destination** drop-down list, specify the destination.

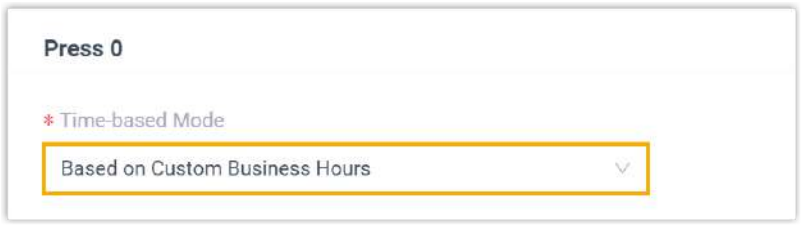
Route calls based on global business hours

a. In the **Time-based Mode** drop-down list, select **Based on Business Hours Configured for the Time Zone**, then select the desired time zone.
b. Specify call routing destinations for the key press event based on the global business hours.
    - **Business Hours Destination**
    - **Outside Business Hours Destination**
    - **Holidays Destination**

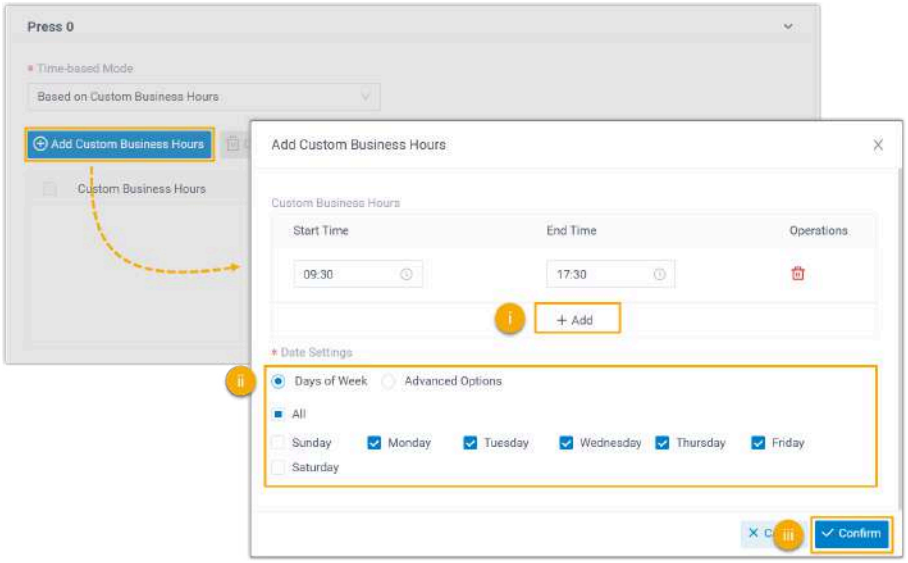
> **Note:**
> If you want to route incoming calls based on global business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**.

Route calls based on custom business hours

a. In the **Time-based Mode** drop-down list, select **Based on Custom Business Hours**.

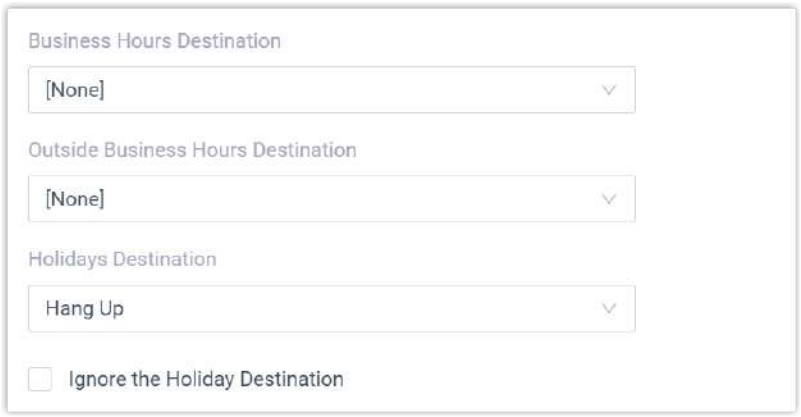


b. Click **Add Custom Business Hours** to create custom business hours based on the system's default time zone.



i. Click **Add** and specify the start time and end time.
ii. In the **Date Settings** section, specify the workdays.
iii. Click **Confirm**.

c. Specify call routing destinations for a key press event based on the custom business hours.



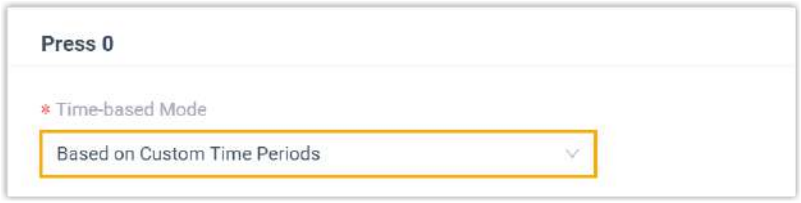
- **Business Hours Destination**

- **Outside Business Hours Destination**
- **Holidays Destination**

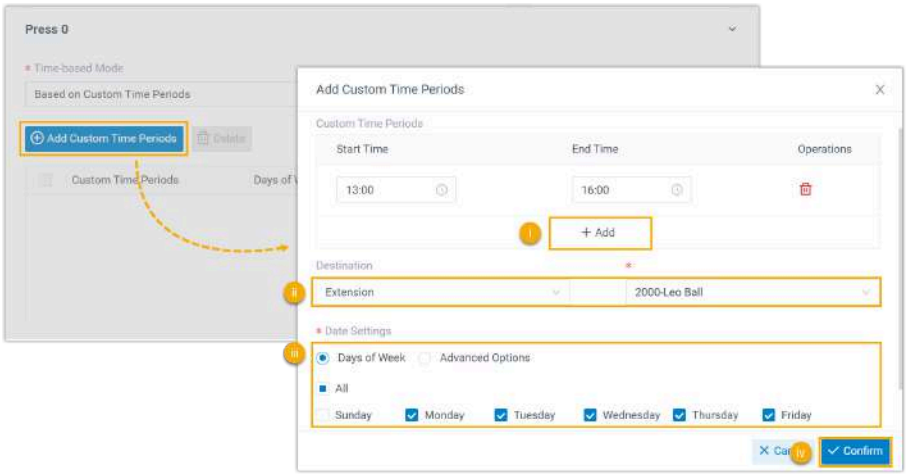
> **Note:**
> If you want to route incoming calls based on custom business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**.

Route calls based on custom time periods

a. In the **Time-based Mode** drop-down list, select **Based on Custom Time Periods**.

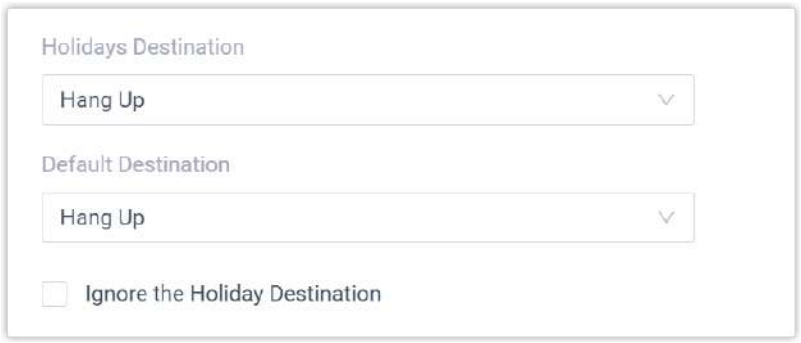


b. Click **Add Custom Time Periods** to create a custom time period based on the system's default time zone.



i. Click **Add** and specify the start time and end time.
ii. In the **Destination** drop-down list, specify the destination for calls within the custom time periods.
iii. In the **Date Settings** section, specify the workdays.
iv. Click **Confirm**.

c. Specify the following call routing destinations for the key event.



- **Holidays Destination**: Specify the call routing destination for calls during holidays.

> **Note:**
> If you want to route incoming calls based on custom time periods during holidays, select the checkbox of **Ignore the Holiday Destination**.

- **Default Destination**: Specify the call routing destination for calls outside custom time periods.

5. Repeat step **4** for all the desired keys.
6. Click **Save** and **Apply**.

Set up a Multi-language IVR

A multi-language IVR allows callers to select their language preferences and provides them with system prompts in their preferred language. You can set the IVR to route the callers to designated destinations based on different language selections, enabling better handling of customer calls and improved customer satisfaction.

Requirements

Yeastar P-Series Software Edition is 83.14.0.24 or later.

Step 1. Design a multi-language IVR

Design a multi-language IVR and outlines the following information:

- Language options the IVR supports
- Key for each language option
- Call routing destination for each language option

> **Note:**
> Make sure that you have created the respective destinations on PBX.

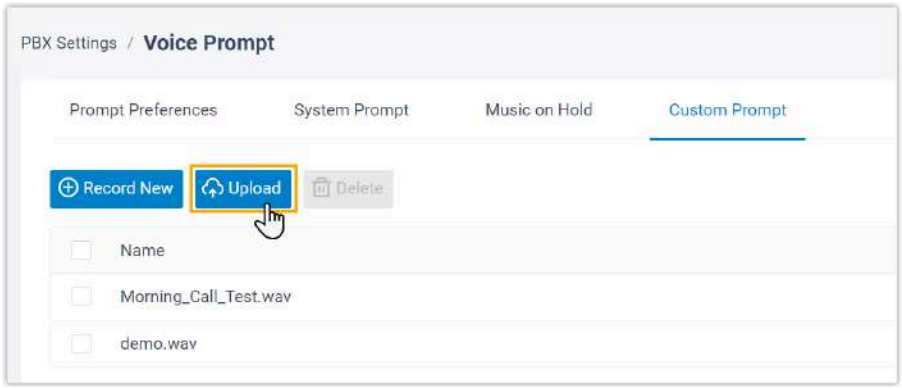
For example, design an IVR with 2 language options (English and Mandarin) supported.

Language Option	Key	Destination
English	key 1	IVR: English (6202)
Mandarin	key 2	Queue: Mandarin-agents (6400)

Step 2. Upload the IVR prompt

1. Prepare a voice prompt for the IVR to announce the available language options and their respective key actions.

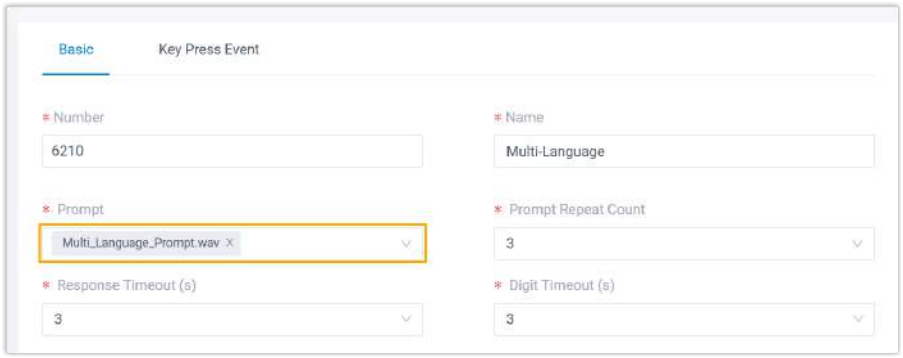
   For example, "Welcome. For English, please press 1. For Mandarin, please press 2".
2. Upload the voice prompt to the PBX system.
   a. Log in to PBX web portal, go to **PBX Settings > Voice Prompt > Custom Prompts**.
   b. Click **Upload**, and select the audio file to upload.



   c. Click **Save** and **Apply**.

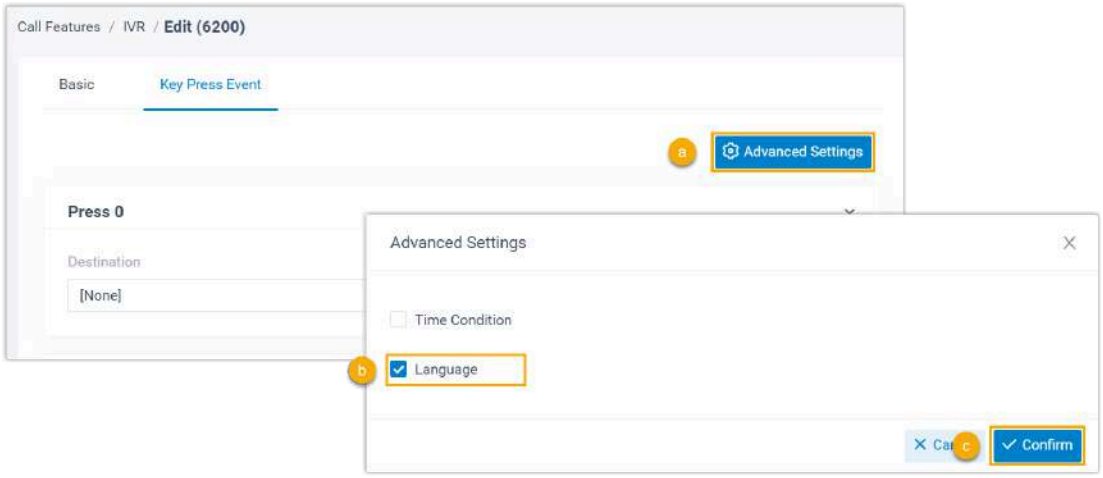
Step 3. Set up the multi-language IVR

1. On PBX web portal, go to **Call Features > IVR**, click **Add**.
2. In the **Basic** tab, configure the basic settings for the IVR.



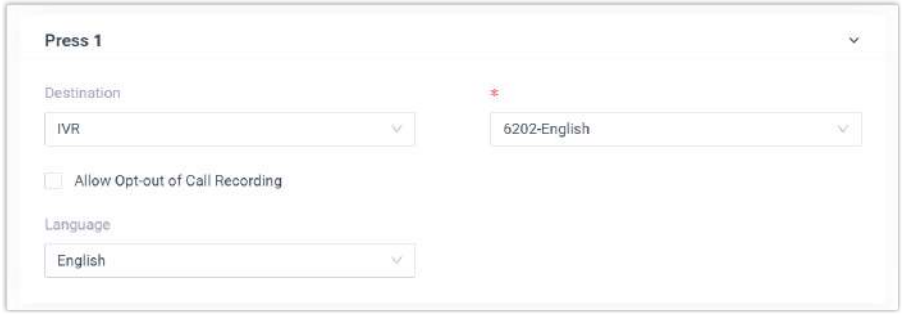
a. In the **Prompt** drop-down list, select the uploaded voice prompt.
b. Configure other settings as needed.

3. In the **Key Press Event** tab, enable multi-language setting for the IVR.



a. On the top-right corner, click **Advanced Settings**.
b. In the pop-up window, select the checkbox of **Language**.
c. Click **Confirm**.

4. Configure the corresponding key events based on your IVR design.



- **Destination**: Specify the call routing destination.

When callers press the key, the call will be routed to the specified destination.

- **Optional:** Select the checkbox of **Allow Opt-out of Call Recording**.

  If enabled, when the call is routed to the key press destination, the call would not be recorded even if **Call Recording** is enabled.
- **Language**: Select the system prompt language.

  > **Note:**
  > The displayed language options are synchronized from System Prompts (Path: **PBX Settings > Voice Prompt > System Prompt**).

  When callers press the key, all the subsequent system prompts will be played in the specified language.

5. Click **Save** and **Apply**.

Result

When calling into the IVR, callers hear the voice prompt for language preference selection. After they press the corresponding key, all subsequent system prompts (except the custom ones) will be played in the selected language, and the call will be routed to the respective key press destination.

Set up IVR Custom Key

Yeastar P-Series Software Edition allows you to add custom keys for IVR to authenticate callers with PIN codes (either a single PIN or a list of PINs) before routing them to specific destinations. This is particularly useful to differentiate inbound calls and ensure that only verified callers can access premium services or dedicated support lines. This topic describes how to set up IVR custom keys.

Requirements

The firmware version of PBX server is 83.16.0.70 or later.

Prerequisites

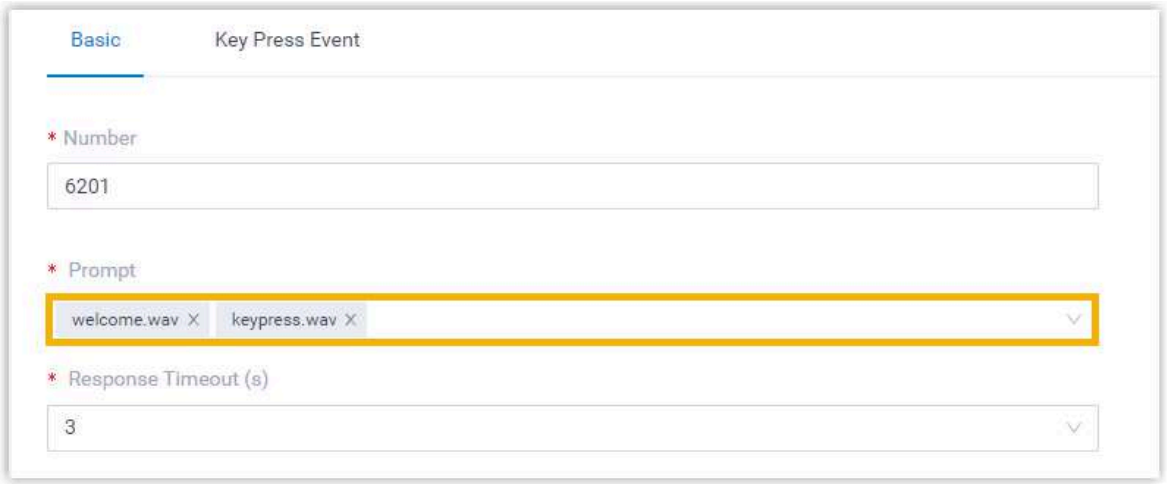
- Upload or record an IVR prompt that would instruct callers to press PIN codes to reach the corresponding destination.
- **Optional:** Add a PIN List that would authenticate callers before routing them to specific destinations.

> **Note:**
> If you prefer a single PIN for custom keys, you don't need to add a PIN list.

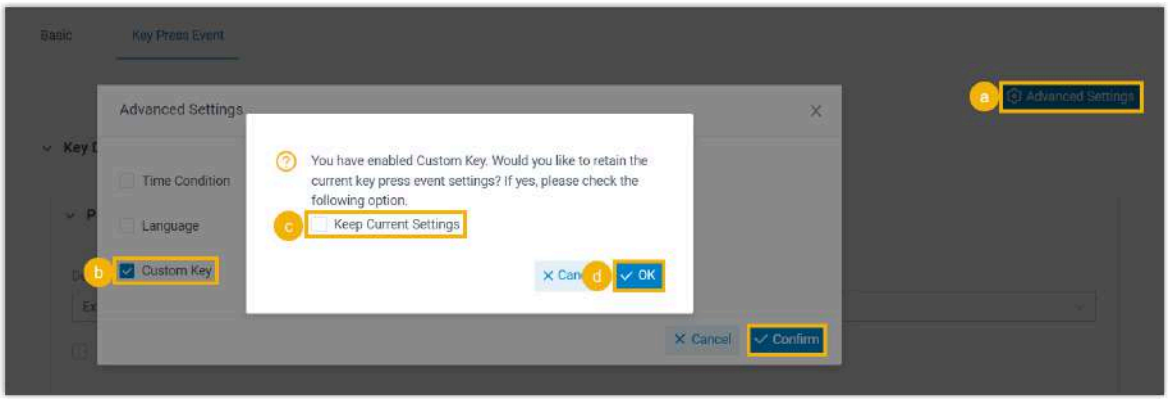
Procedure

1. Log in to PBX web portal, go to **Call Features > IVR**, edit the desired IVR.
2. Under **Basic** tab, select prompt(s) from the **Prompt** drop-down list to instruct callers to press custom key.

> **Note:**
> You can select up to 5 audio files, and the system plays the audio files in order.



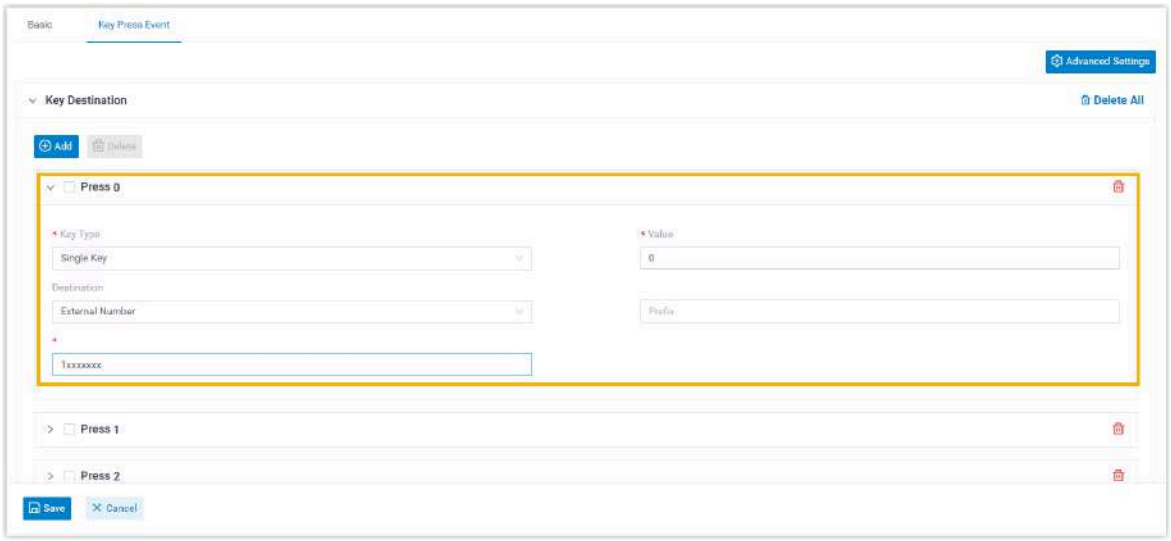
3. Under **Key Press Event** tab, enable custom keys.



   a. At the top-right corner, click **Advanced Settings**.

b. In the pop-up window, select the checkbox of **Custom Key**, then click **Confirm**.
c. **Optional:** Select the checkbox of **Keep Current Settings** to retain the current key press event settings.
d. Click **OK**.

4. Set up custom keys.



a. In the **Key Type** drop-down list, select a key type.
   - If you select **Single Key**, enter a PIN code in the **Value** field.

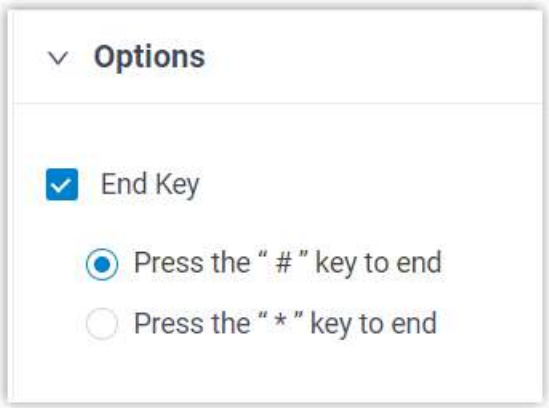
     > **Note:**
     > The length of PIN code should not be greater than 21.

   - If you select **PIN List**, select a PIN list from the **PIN List** drop-down list.

b. In the **Destination** drop-down list, specify a destination for the custom key.

5. **Optional:** Scroll down to the **Options** section, enable end key to allow callers to complete their input and be directed to the corresponding destination.

> **Note:**
> If **End Key** is enabled, `*` or `#` should not be included in your custom key.



a. Select the checkbox of **End Key**.
b. Select **Press the "#" key to end** or **Press the "*" key to end**.

6. Click **Save** and **Apply**.

Result

Callers who know the PIN code can press the key when enter an IVR and will be routed to the designated destination.

> **Note:**
> If you set key events based on time conditions, the PBX will match the key firstly when callers enter the IVR. If the key is right, calls will be routed to destinations according to time conditions; while it is wrong, calls will be routed to Response Timeout or Invalid Input Destination.

Call Recording

Call Recording Overview

Call recording is valuable to keep important conversations, help train employees, evaluate their performance, and provide them with feedback. This topic describes how does call recording work, recording types, recording prompt, and recording management.

How does call recording work

The system records the conversation automatically when a call is established. During call recording, the user can pause and resume recording to avoid the sensitive information

being recorded. After the call ends, the system converts the conversation into audio files (.wav) with a digital signature.

> **Note:**
> The digital signature ensures a recording is not altered in any way.

Recording types

You can set up call recording for extensions, trunks, conferences, and queues respectively.

- **Extensions**: Record all the calls of the specified extensions, including the internal calls and external calls.

  > **Note:**
  > Paging/Intercom call and voicemail on the specified extension would not be recorded.

- **Trunks**: Record all the calls on the specified trunks, including inbound calls and outbound calls.

  For example, for employees who use a dedicated trunk to deal with customer issues, the system only records all the calls on this trunk.
- **Conferences**: Record the conversation of all members who join the specified conference rooms.
- **Queues**: Record the calls based on the specified queues.

  For example, an agent logs in to two queues (Service and Support), and call recording is enabled for Service. The system can record all the calls from Service, but not record the calls from Support.

> **Note:**
> The system automatically records a queue call or a conference call only when you activate recording for a queue or conference. For example, extension 1000 is an agent of a queue, you activate recording for extension 1000, but not activate recording for the queue. When extension 1000 answers a queue call, the call is not recorded.

Recording prompts

By default, the system does not play any prompts when a call is being recorded.

To ensure that recordings are lawful and callers have given their consent, you can customize recording prompt for internal calls, inbound calls, and outbound calls respectively. The system plays the recording prompt before call recording begins.

Recording management

- **For users**: The users can monitor and switch call recording status on IP phones and Linkus Clients.
- **For administrator**: The administrator can set up a storage location for recording files, manage the recording files, and grant permission to other users.

Set up Call Recording

This topic describes how to set up call recording for extensions, trunks, conferences, and queues.

Prerequisites

Only when the storage location for recording files is configured will the recording function take effect. For more information, see manage storage locations.

Set up call recording for extensions

The system records the internal calls and external calls on the selected extensions.

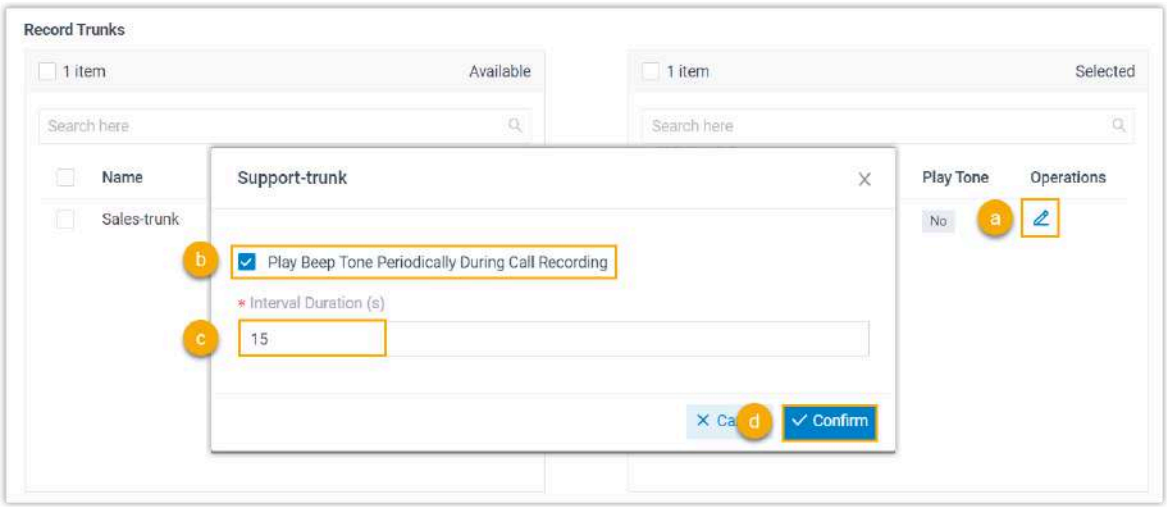
1. Log in to PBX web portal, go to **Call Features > Recording**.
2. **Optional:** Select the checkbox of **Enable Recording of Internal Calls** to automatically record the internal calls.
3. In the **Record Extensions** section, select the desired extensions from the **Available** box to the **Selected** box.
4. Click **Save** and **Apply**.

Set up call recording for trunks

The system automatically records the external calls on the selected trunks.

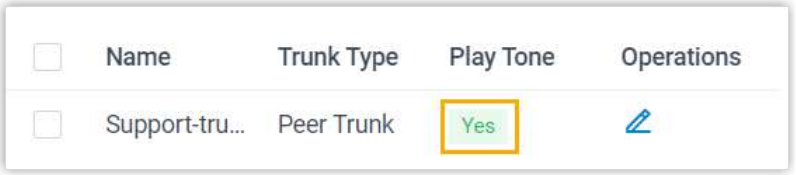
1. Log in to PBX web portal, go to **Call Features > Recording**.
2. In the **Record Trunks** section, select the desired trunks from the **Available** box to the **Selected** box.
3. **Optional:** To periodically play beep tones to inform both parties when the call on the selected trunk is being recorded, do as follows.

> **Note:**
> This setting will not take effect on the calls where multiple participants are involved, such as conference calls and multi-party calls.



a. In the **Selected** box, click beside a selected trunk.
b. In the pop-up window, select the checkbox of **Play Beep Tone Periodically During Call Recording**.
c. In the **Interval Duration (s)** field, specify the interval for playing the beep tone.
d. Click **Confirm**.

The **Play Tone** of the selected trunk displays **Yes**, indicating that periodic playback of beep tone is enabled for the trunk.



4. Click **Save** and **Apply**.

Set up call recording for conferences

The system automatically records the calls on the selected conferences.

1. Log in to PBX web portal, go to **Call Features > Recording**.

2. In the **Record Conferences** section, select the desired conferences from the **Available** box to the **Selected** box.
3. Click **Save** and **Apply**.

Set up call recording for queues

The system automatically records the calls on the selected queues.

1. Log in to PBX web portal, go to **Call Features > Recording**.
2. In the **Record Queues** section, select the desired queues from the **Available** box to the **Selected** box.
3. Click **Save** and **Apply**.

Set up Recording Prompts

This topic describes how to set up recording prompts for internal calls, inbound calls, and outbound calls respectively.

Set up recording prompt for internal calls

1. Log in to PBX web portal, go to **PBX Settings > Voice Prompt > Custom Prompt**, upload a custom prompt or record a custom prompt for internal calls.

   > **Note:**
   > The uploaded file should meet the audio file requirements.

2. Go to **Call Features > Recording**.
3. In the **Internal Call Being Recorded Prompt** drop-down list, select a prompt for internal calls.
4. Click **Save** and **Apply**.

Set up recording prompt for inbound calls

1. Log in to PBX web portal, go to **PBX Settings > Voice Prompt > Custom Prompt**, upload a custom prompt or record a custom prompt for inbound calls.

   > **Note:**
   > The uploaded file should meet the audio file requirements.

2. Go to **Call Features > Recording**.
3. In the **Inbound Call Being Recorded Prompt** drop-down list, select a prompt for inbound calls.
4. Click **Save** and **Apply**.

Set up recording prompt for outbound calls

1. Log in to PBX web portal, go to **PBX Settings > Voice Prompt > Custom Prompt**, upload a custom prompt or record a custom prompt for outbound calls.

   > **Note:**
   > The uploaded file should meet the audio file requirements.

2. Go to **Call Features > Recording**.
3. In the **Outbound Call Being Recorded Prompt** drop-down list, select a prompt for outbound calls.
4. Click **Save** and **Apply**.

Allow Users to Switch Call Recording Status

By default, if you set up call recording for extensions, trunks, conferences, or queues, the specified calls would be recorded as soon as they are established, and all the users can NOT switch call recording status. To avoid sensitive information being recorded or to allow users to start recording their calls when necessary, you can grant permissions to specific users, so that they can start, pause, or resume recording during a call.

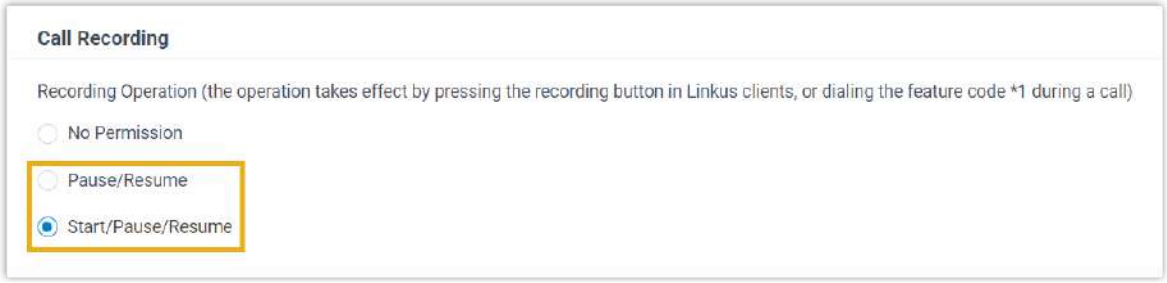
Restrictions

> **Note:**
> Extension users can NOT switch the recording status during a conference call, even if you have granted them permission.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit a desired extension.
2. Click **Features** tab.

3. In the **Call Recording** section, grant the operation permission of call recording to the extension user.



   - **Pause/Resume**: Allow the user to pause or resume recording during a call that is specified to be recorded.

     > **Tip:**
     > To specify the calls to be recorded, see Set up Call Recording.

   - **Start/Pause/Resume**: Allow the user to start, pause, or resume recording during any calls (except conference calls), be the calls specified to be recorded or not.
4. Click **Save** and **Apply**.

Result

- The user can switch call recording status in the following ways:
  - Press the recording button on Linkus Clients
  - Dial a feature code

  > **Note:**
  > The default feature code for switching call recording status is `*1`.
  > You can change, enable, or disable the code on PBX web portal (Path: **Call Features > Feature Code > Recording > Switch Extension's Recording Status**).
- By default, the user can view the call recording file that is generated when a call ends. To restrict the user from viewing recording files, see Restrict Users from Viewing Recording Files.

Monitor Call Recording Status on an IP phone

This topic describes how to set up a BLF key on an IP phone to monitor the call recording status.

Background information

For the users who want to know whether the call recording state is switched successfully or not, you can set a BLF key for each user by auto provisioning.

> **Note:**
> Users can also set function keys on their own IP phones. For more information, contact the phone manufacturer.

Procedure

1. Assign function keys for extension users to monitor agent status.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
      - If you want to assign function keys for a specific extension user, click beside the desired extension.
      - If you want to assign function keys for multiple extensions, select the checkboxes of the desired extensions, and click **Edit**.
   b. Click the **Function Keys** tab.
   c. Configure function keys.

      > **Note:**
      > The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

      - **Type**: Select **BLF**.
      - **Value**: Enter the code (`*1`) followed by extension number (for example *11000).
      - **Label**: Optional. Enter a value, which will be displayed on the phone screen.
   d. Click **Save**.

2. If the extension hasn't been associated with a phone, see the following topics to bind a phone with the extension.
   - Auto Provision IP Phones in Local Network (PnP Method)
   - Auto Provision IP Phones in Local Network (DHCP Method)
   - Auto Provision IP Phones Remotely (RPS FQDN Method)
   - Auto Provision IP Phones Remotely (RPS Method)
3. If the extension has been associated with a phone, reprovision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to this extension.

Result

The BLF key shows the real-time status of call recording.

- **Red**: An active call of the monitored extension is being recorded.
- **Green**: The monitored extension is not in a call or the call recording is paused.
- **Off**: The BLF key does not subscribe the recording status of this extension. Check if your configurations are correct.

> **Note:**
> The key LED status may vary by phone models.

Manage Call Recording Files

This topic describes how to manage call recording files, including searching, playing, downloading, or deleting the recording files.

Search recording files

You can search the recording files by time, caller number, callee number, or call ID.

1. Log in to PBX web portal, go to **Reports and Recordings > Recording Files**.
2. Set the search criteria.
   - **Time**: Set the start date and the end date.

     To specify a time period, click **select time** to set the start time and the end time.
   - **Call From**: Set the caller's number or name.
   - **Call To**: Set the callee's number or name.

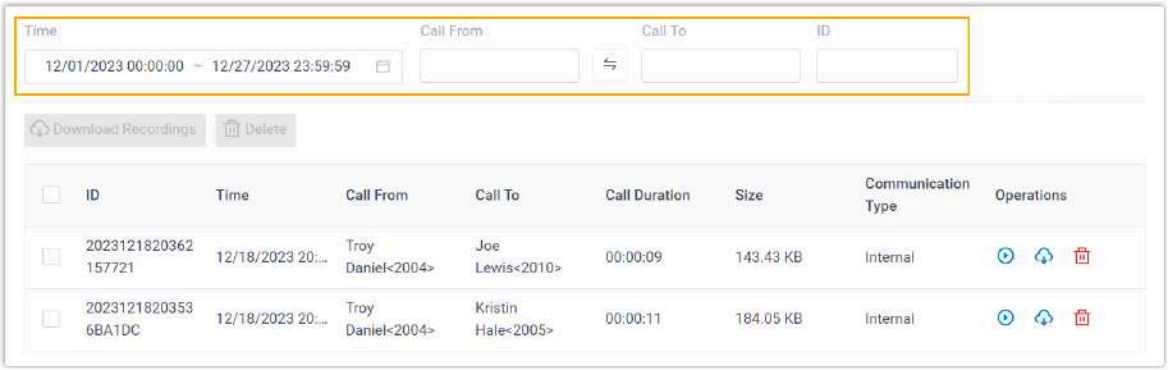
> **Tip:**
>
> To swap the callee for the caller, click ⇋.

- **ID**: Enter the unique identifier for the recording file.

The search results are displayed in the list.

Play recording files

1. Log in to PBX web portal, go to **Reports and Recordings > Recording Files**.
2. **Optional:** Set the criteria to filter the desired recordings.



3. Click ▶ beside the recording to which you want to listen.
   - **Play on Web**: Click ▶ to play the call recording on the web directly.
   - **Play to Extension**: Play the call recording on the phone.
     a. Select an extension, and click **Play**.

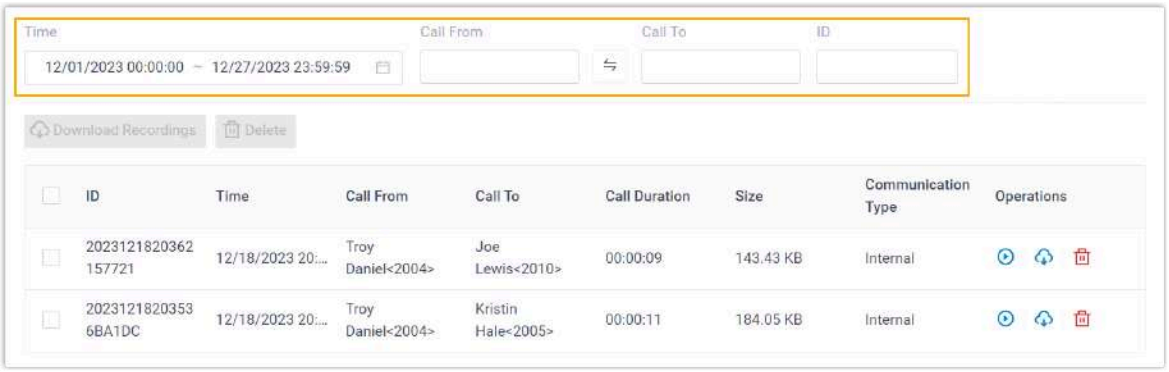
        The system places a call to the extension.
     b. Pick up the call to listen to the call recording on the phone.

Download recording files

You can download recording files to your local computer or to an external server (such as FTP server, SFTP server, Amazon S3, or Google Cloud Storage).

This section introduces how to download recording files to your local computer. For external server, see Yeastar P-Series Software Edition Remote Archiving Overview.

1. Log in to PBX web portal, go to **Reports and Recordings > Recording Files**.
2. **Optional:** Set the criteria to filter the desired recordings.



3. Download recording file(s) as needed.

> **Note:**
> You can download a maximum of 600 MB recording files or a maximum of 100 recording files at a time. The recordings that exceed the limit will not be downloaded.

Download a recording file

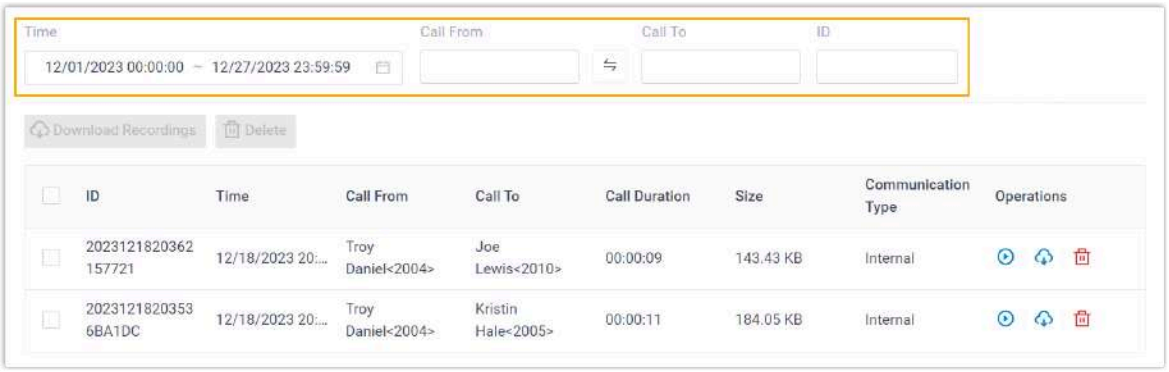
Click beside the recording file.

Download multiple recording files

Select the checkboxes of the recording files that you want to download, then click **Download Recordings**.

Delete recording files

1. Log in to PBX web portal, go to **Reports and Recordings > Recording Files**.
2. **Optional:** Set the criteria to filter the desired recordings.



3. Delete a recording file, or delete recording files in bulk.
    - **Delete a recording**: Select the recording file that you want to delete, click and **OK**.
    - **Delete recordings in bulk**: Select the checkboxes of the recording files that you want to delete, click **Delete** and **OK**.

Auto Clean up Recording Files

Clean up old recording files to free up space. When the storage device reaches 80% of its maximum storage capacity or reaches the maximum preservation days, the PBX automatically deletes the oldest recording files. You can customize the maximum usage of device and preservation days. This topic describes how to set up auto cleanup of recording files.

Procedure

1. Log in to PBX web portal, go to **System > Storage > Auto Cleanup > Recording Auto Cleanup**.
2. In the **Max Usage of Device (%)** field, enter a value to specify the maximum storage percentage of the device that is allowed to store recording files.
3. In the **Recordings Preservation Days** field, enter the maximum number of days that the recording files should be retained.

   The value `0` indicates no limit.
4. Click **Save** and **Apply**.

Note:
If **Auto Cleanup Reminder** is enabled, and the retained recording files reach 90% of threshold, the system sends you a notification email. If the old recording files

have continuing retention value, you can back up recording files or expand the retain limit in time.

Grant Manage Permission of Recording Files

By default, only the super administrator has permission to manage the call recording files. This topic describes how to grant manage permission to extension users.

Background information

As a super administrator, you can grant manage permission to a role, and assign the role to extension users. When the user logs in to the web client, he/she can manage recording files.

Procedure

1. Set up a user role.
    a. Log in to PBX web portal, go to **Extension and Trunk > Role**, edit a role.
    b. In the **Reports and Recordings** section, specify the manageable extensions and accessible permissions of recordings files for the role.
        - **Manage Extensions**: Specify the manageable extension range.
        - **Recording Files Operation Permission**: Specify the accessible permission, including **Play**, **Download**, and **Delete**.
    c. click **Save**.
2. Assign a role to a user.
    a. Go to **Extension**, edit the extension to which you want to grant recording permission.
    b. In the **User Information** section, select the role from the **User Role** drop-down list.
    c. Click **Save** and **Apply**.

Restrict Users from Viewing Recording Files

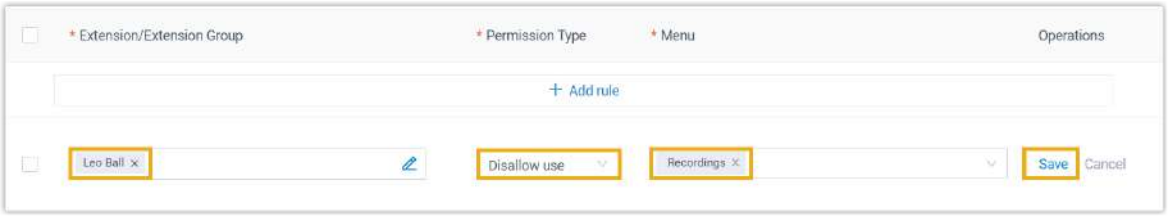
By default, all the users have access to viewing their own recording files. For security reasons, you can restrict specific users from view recording files.

Requirements

Server / Client	Version Requirement
PBX Server	Version 83.12.0.23 or later
Linkus Mobile Client	• **Linkus iOS Client**: Version 5.2.9 or later • **Linkus Android Client**: Version 4.13.16 or later
Linkus Desktop Client	• **Windows Desktop**: Version 1.2.14 or later • **Mac Desktop**: Version 1.2.10 or later

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Menu Visibility**.
2. Click **Add rule** to create a menu visibility rule.
3. Set up the rule, then click **Save**.



   - **Extension/Extension Group/Organization**: Click to select desired extensions, extension groups, or departments, for which you want to restrict the viewing permission of recordings.
   - **Permission Type**: Select **Disallow use**.
   - **Menu**: Select **Recordings**.

Result

The extension user can not view recording files on his or her Linkus UC Clients.

Ring Group

Ring Group Overview

Ring group is a feature to share the distribution of incoming calls among employees. This topic describes what is ring group, ring strategy, failover destination, and missed call alerts.

What is ring group

Ring group allows you to merge multiple extension numbers into a virtual number. The customers can dial the virtual number, and the calls ring through all the members to make sure that no call goes unanswered. It is often used to efficiently distribute calls to specific departments such as Sales, Support, and Accounting.

Ring strategy

Ring group can ring members in four ways:

- **Ring all simultaneously**: When receiving an incoming call, the system rings all the available members at the same time and stops ringing when any member in the group picks up the call. If no one answers the call within the ring time, the system routes the call to the failover destination.
- **Ring sequentially**: When receiving an incoming call, the system rings the first available member in the list. If no answer within the ring time, the system rings the next available member until the last one. If no one answers the call, the system routes the call to the failover destination.
- **Memory hunt**: When receiving an incoming call, the system rings the first available member in the list. If no answer within the ring time, the system rings the first and second available member. If still no answer within the ring time, the system rings the first, second, and third available member, and the like, until all available members in the list rang. If no one answers the call, the system routes the call to the failover destination.
- **Custom**: When receiving an incoming call, the system rings members according to their individually set delay times and stops ringing after their individual ring timeouts. If no one answers the call, the system routes the call to the failover destination.

Failover destination

When a call comes in to the ring group, and no one is available to answer the call, you can end the call or route the call to the following destinations:

- **Hang Up**
- **Extension**
- **Extension Voicemail**
- **Group Voicemail**
- **IVR**
- **Ring Group**

- **Queue**
- **External Number**
- **Play Prompt and Exit**

Missed call alerts

When there are missed calls from ring group, the system can record the missed calls and notify members via email.

To record missed calls from ring group, see Record Missed Calls.

To set up email alerts for missed calls from ring group, see Set up Email Notifications for Missed Calls.

Create a Ring Group

This topic describes how to create a ring group.

Procedure

1. Log in to PBX web portal, go to **Call Features > Ring Group**, click **Add**.
2. Configure the ring group.
   - **Number**: Enter a virtual number for callers to access the group.

     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.
     - **Custom**: Ring extensions according to their individual ring delays and stop ringing after their individual ring timeouts.

> **Note:**
> You can set ring delays and timeouts for each group member in the **Members** section.

- **Ring Timeout (s)**: Set a number of seconds that the system waits before ringing next member or routing the call to **Failover Destination**.

> **Note:**
> This option is available only when **Ring Strategy** is set to **Ring All**, **Ring Sequentially**, or **Memory Hunt**.

- **Join Announcement**: Optional. Set the announcement to be played to callers, which will be played only once.
  - **Play full Join Announcement to the caller before ringing extensions**: Set whether to play full join announcement to callers before ringing members.
- **Ringback Tone**: Optional. Specify a prompt that will be played to callers before members answer the call.

  You can select an existing prompt from the drop-down list, or click **Record New** / **Upload** to record or upload a new prompt.

> **Note:**
> - The Ringback Tone is played after the Join Announcement.
> - The existing prompts are synchronized from **PBX Settings > Voice Prompt > Music on Hold / Custom Prompt**. If you record or upload a new prompt here, it will also be synchronized to the location.

- **Music on Hold**: Optional. Specify the music that will be played to callers when the call is put on hold.

  You can select an existing MoH playlist from the drop-down list, or click **Create New** to add a new one.

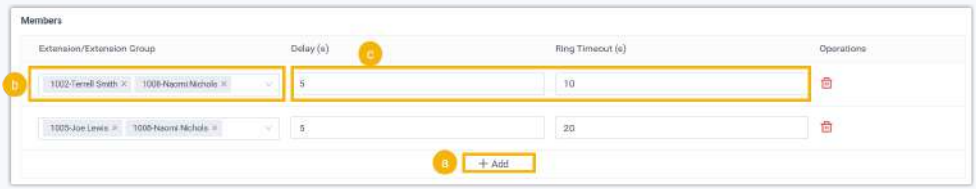
> **Note:**

The existing playlists are synchronized from **PBX Settings > Voice Prompt > Music on Hold**. If you create a new playlist here, it will also be synchronized to the location.

- **Ring Group Alert Info**: Optional. Set an "alert info text" to add to Alert-info header in INVITE request for ring group calls.

  When receiving a ring group call, the phone will inspect "Alert-Info" header to determine which ring tone it should use for ringing.
- **Members**: Select the desired extensions from the **Available** box to the **Selected** box.

Note:
If you set **Ring Strategy** to **Custom**, you can set ring delay and timeout for different extensions, as shown below.



a. Click **Add**.
b. Select extensions or extension groups from the drop-down list.

Note:
Each extension or extension group can be selected in at most 5 different member rules.

c. Configure ring delay and timeout for group members.
   - **Delay (s)**: Set the time delay in seconds (0 - 600, where 0 indicates ring immediately). The member will start ringing after the configured delay time.

     Note:
     If you select an extension group, all extensions within the group will ring simultaneously after the ring delay.
   - **Ring Timeout (s)**: Set the ring timeout in seconds (1 - 600). The member will stop ringing after the configured ring timeout. If all

members time out, the call will be routed to the Failover destination.

> **Note:**
> If you select an extension group, all extensions within the group will stop ringing simultaneously when the timeout is reached.

- **Failover Destination**: Select a destination to route the call when no member answers the call within ring time.
  - **Hang up**: End the current call.
  - **Extension**: Route the call to the specified extension.
  - **Extension Voicemail**: Route the call to voicemail box of the specified extension.
  - **Group Voicemail**: Route the call to voicemail box of a queue, a ring group, or a custom group.
  - **IVR**: Route the call to the specified IVR.
  - **Ring Group**: Route the call to another ring group.
  - **Queue**: Route the call to the specified queue.
  - **External Number**: Route the call to an external number.
  - **Play Prompt and Exit**: Play a custom prompt, and then hang up the call.
- **Record Missed Calls**: Decide whether to record missed calls from ring group.

> **Note:**
> - This option is available only when both **Ring Strategy** and **Failover Destination** are set to the followings:
>   - **Ring Strategy** is set to **Ring All**, **Memory Hunt**, or **Custom**.
>   - **Failover Destination** is set to **Extension**, **Queue**, or **Ring Group**.
> - You can also set up email alert on missed calls from ring group for members. To achieve this, enable this option, then turn on email notifications on missed calls for members. For more information, see Set up Email Notifications for Missed Calls.

- **Time Condition**: Decide whether to route the calls received in non-business hours to different destination based on the time in a specific time zone.

Setting	Description
Time Zone	Select a desired time zone. The business hours and holidays settings of the selected time zone (Path: **Call Control > Business Hours and Holidays**) will be applied to the ring group. **Note:** The ring group always receive calls in the business hours.
Outside Business Hours Destination	Select the destination for calls received during the time periods that are not defined as business hours or holidays in the selected time zone.
Holidays Destination	Select the destination for calls received during holidays defined in the selected time zone.
Ignore the Holiday Destination	If you want to route incoming calls based on the business hours and non-working hours during holidays, select the checkbox of **Ignore the Holiday Destination**. Incoming calls during holiday will be distributed to other destinations according to your office hour setting.
Play Holiday Prompt During Holidays	To play a prompt to callers before routing the inbound calls to the holiday destination, select the checkbox of **Play Holiday Prompt During Holidays**. **Note:** Make sure that you have set a prompt for the holiday (Path: **Call Control > Business Hours and Holidays > Holidays > Type > Prompt**). Otherwise, the inbound calls will be directly routed to the holiday destination without playing a prompt.

3. Click **Save** and **Apply**.

What to do next

Set up an inbound route, and specify the destination to the ring group.

Manage Ring Groups

This topic describes how to edit a ring group, and delete ring groups.

Edit a ring group

You can edit the group settings, including adding or removing a member, or change the ring strategy.

1. Log in to PBX web portal, go to **Call Features > Ring Group**.
2. Click  beside the ring group that you want to edit.
3. Change the ring group settings according to your needs.
4. Click **Save** and **Apply**.

Delete ring groups

1. Log in to PBX web portal, go to **Call Features > Ring Group**.
2. To delete a ring group, click  beside the ring group that you want to delete.
3. To delete ring groups in bulk, select the checkboxes of the ring groups that you want to delete, click **Delete**.
4. Click **OK** and **Apply**.

Call Queue

Call Queue Overview

Call queue is a method of handling large calls and provides callers with engaging holding experiences. This topic describes what is call queue, queue compositions, queue preference, and call center service.

What is call queue

A queue is like a virtual waiting room, in which callers wait in line to talk with the available agent. When the customer calls in PBX and reaches the queue, he/she can hear the hold music and announcement while the queue distributing the call to the available agents.

What is Call Center service

Call Center service is an additional service that drives faster call resolution and real-time call center monitoring, reporting, and management. It provides a powerful call center console, including a customizable Wallboard for proactive tracking of 16 key performance met-

rics, and a switchboard-type Queue Panel for real-time monitoring & control of queue activities, insightful call center reports, SLA and more.

Configuration guide

For more detailed information and configurations of call queue and Yeastar Call Center, see Call Center Administrator Guide.

Feature Code

Configure Feature Codes

Feature codes are a set of digits that the extension user can dial to activate a specific feature. This topic describes how to configure feature codes.

Background information

Yeastar P-Series 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.
Transfer Bounce Back (Applicable to Both	/	If enabled, when an extension user performs a blind transfer/semi-attended transfer and the transfer

Name	Default code	Usage
Blind/Semi-attended Transfer)		recipient doesn't answer, the call will be transferred back to the extension user.

Call Forwarding

Name	Default code	Usage
Enable "Forward All Calls"	*31	• Dial *31 to forward all calls to one's own voicemail. • Dial *311000 to forward all calls to extension 1000.
Disable "Forward All Calls"	*031	• Dial *031 to disable the automatic call forwarding of all calls.
Enable "Forward When Busy"	*32	• Dial *32 to forward calls to one's own voicemail when busy. • Dial *321000 to forward calls to extension 1000 when busy.
Disable "Forward When Busy"	*032	• Dial *032 to disable the automatic call forwarding when busy.
Enable "Forward No Answer"	*33	• Dial *33 to forward the no-answered calls to one's own voicemail. • Dial *331000 to forward the no-answered calls to extension 1000.
Disable "Forward No Answer"	*033	• Dial *033 to disable the automatic call forwarding of no-answered calls.

Call Pickup

Name	Default code	Usage
Group Call Pickup	*4	Dial *4 to pick up the ringing call for a group member.
Extension Pickup	*04	Dial *041000 to pick up the ringing call for extension 1000.

Call Parking

Name	Default code	Usage
Call Parking	*5	Dial *5 during a call to park a call.
Directed Call Parking	*05	Dial *056000 during a call to park a call to parking number 6000.

Call Monitoring

Name	Default code	Usage
Listen	*51	An authorized user dials *511001 to listen to the call of extension 1001 in real time. The authorized user can NOT talk with both parties.
Whisper	*52	An authorized user dials *521001 to listen to the call of extension 1001 in real time. The authorized user can talk with extension 1001 without being heard by the other party.
Barge-in	*53	An authorized user dials *531001 to listen to the call of extension 1001 in real time. The authorized user can talk with both parties.

Force Drop

Name	Default code	Usage
Call Force Drop	*54	• An authorized user dials *541001 to force drop the current call of extension 1001. • An authorized user dials *54 while monitoring the call of extension 1001 to force drop the call.

Intercom

Name	Default code	Usage
Intercom	*6	Dial *61001 to place an intercom call to extension 1001.

Queue

Name	Default code	Usage
Log in/Log out	*7	A dynamic agent dials *76400 to log in to or log out of queue 6400.
Pause/Unpause	*07	Dial *076400 to pause or unpause calls from queue 6400.

Hot Desking

Name	Default code	Usage
Guest In	*84	A user can dial *84 on a hot desking phone to register his or her extension to the phone.
Guest Out	*084	A user can dial *084 on a hot desking phone to de-register his or her extension from the phone.

Busy Camp-on

Name	Default code	Usage
Enable Busy Camp-on	*79	A user dials *791000 to camp on extension 1000 in case he or she gets a busy signal when dialing extension 1000. The PBX will automatically call the user back when extension 1000 becomes available.
Disable Busy Camp-on	*079	A user dials *079 to cancel all Busy Camp-on requests that he or she has initiated.

Speed Dial

Name	Default code	Usage
Speed Dial Prefix	*89	Specify a number to speed dial code 1, dial *891 to dial the specified number.

Presence Status

Name	Default code	Usage
Available	*91	Dial *91 to switch one's own presence status to **Available**.
Away	*92	Dial *92 to switch one's own presence status to **Away**.
Do Not Disturb	*93	Dial *93 to switch one's own presence status to **Do Not Disturb**.
Lunch Break	*94	Dial *94 to switch one's own presence status to **Lunch Break**.
Business Trip	*95	Dial *95 to switch one's own presence status to **Business Trip**.
Off Work	*96	Dial *96 to switch one's own presence status to **Off Work**.

Query my extension number

Name	Default code	Usage
Query my extension number	*97	If enabled, extension user can dial *97 to query the extension number registered on the current endpoint. The system will play the prompt "Your extension number is *{extension_number}*." twice, then hang up the call.
Line Status Detection Call	/	If enabled, the PBX system will initiate a line detection call to the extension after hanging up the number querying call, which detects whether the line functions normally or not. • If the line has no problem, the system will play the prompt "The line you are using is functioning normally.", and then hang up the call. • If the line has a problem, no line detection call will be sent to the extension.

Switch Business Hours and Holidays Status

Name	Default code	Usage
Keep the Business Hours Status or the Time Condition after switching	/	If enabled, keep the status after users switched the PBX's Business Hours status or dialed a feature code to switch the time condition of an inbound route.
Switch Business Hours and Holidays Status	*99	Dial *99 to override time condition for the Business Hours and Holidays configured in system's default time zone. **Note:** This feature code applies only to the system's default time zone. For additional time zones, you can check the corresponding feature code under the specific time zone settings (Path: **Call Control > Business Hours and Holidays**).
Time Condition Switching Prefix	*8	Dial a feature code starting with *8 to switch the time condition of inbound routes that are based on Custom Business Hours or Custom Time Periods.

Name	Default code	Usage
BLF Light Color of Switching Global Business Hours Status	/	Set the BLF light color to indicate whether being at the destination or not when in Business Hours or Outside Business Hours (or custom time conditions).

Hotel Management

Name	Default code	Usage
Room Status	*63	Dial *63 and room status feature code on hotel room phone to update the room status. **Note:** The room status feature code is automatically generated when adding room status in **Hotel Management > Room Management > Customize Room Status > Feature Code**.

PMS Integration

Name	Default code	Usage
Housekeeping Status	*61	Dial *611 on hotel room phone to update the room status to "Dirty/Vacant". **Note:** • The housekeeping status code is available only when the PBX is integrated with a PMS system using FIAS protocol. • The housekeeping status code must be used in conjunction with maid status code, in the format of `{housekeeping_status_code}{maid_status_code}`. The maid status codes specified by FIAS protocol are listed below: ◦ `1`: Dirty/Vacant ◦ `2`: Dirty/Occupied ◦ `3`: Clean/Vacant ◦ `4`: Clean/Occupied ◦ `5`: Inspected/Vacant

Name	Default code	Usage
		◦ 6: Inspected/Occupied
Minibar	*62	Depending on the **Minibar Billing Type** (Path: **Integrations > PMS**) set on the PBX, hotel staffs can dial specific feature codes on hotel room phone to post minibar charges. **Note:** The minibar feature code is available only when the PBX is integrated with a PMS system using FIAS protocol. • If **Minibar Billing Type** is set to **Based on Item and Quantity**, hotel staffs can dial *{minibar_feature_code}*{item_code}*{quantity}* on room phone to post the item consumed and its quantity to the guest's bill in PMS. For example, if a guest bought 2 cans of Coke (item code 4000), hotel staffs can dial `*62*4000*2`. • If **Minibar Billing Type** is set to **Based on Total Amount**, hotel staffs can dial *{minibar_feature_code}{total_amount}* on room phone to post the total minibar charge to the guest's bill in PMS. For example, if a guest bought 2 cans of Coke (unit price $3), hotel staffs can dial `*626`.

Boss-Secretary Feature

Name	Default code	Usage
Enable Boss-Secretary Feature	*59	**Note:** This feature code is only available for extensions set as the boss extension. Dial *59 to enable the Boss-Secretary feature.
Disable Boss-Secretary Feature	*059	**Note:**

Name	Default code	Usage
		This feature code is only available for extensions set as the boss extension. Dial *059 to disable the Boss-Secretary feature.

Pause Reason

Yeastar P-Series 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.

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.
  - **Custom Prompt Language**: Optional. Enable this option and set the language of system prompts heard by participants when they join the conference call.

    > **Note:**
    > The available languages are synchronized from System Prompt (Path: **PBX Settings > Voice Prompt > System Prompt**).

  - **Wait for Moderator**: Whether to forbid the participants to talk with each other till the moderator joins the conference call.
  - **Allow Extension Participants to Invite**: Whether to allow the extension participants to invite users to join the conference.
  - **Moderator(s)**: Select the moderators.

    The moderators can join the conference calls without any password.
3. Click **Save** and **Apply**.

What to do next

If the external participants want to join conference, you need to set an inbound route and specify the **Destination** to **Conference**.

Join a Conference Call

Both the PBX extension users and the external users can join the conference. This topic describes how to join a conference call.

Join as a conference participant

1. Dial the conference room number.
2. If participant password is required, enter the participant password.

   If you are the first participant in the conference call, the system plays a hold music to you.

Join as a conference moderator

For moderators

If you are a moderator specified by administrator, you can dial the conference room number to join the conference call.

If you are the first participant in the conference call, the system plays a hold music to you.

For participants who want to join conference as moderators

If you are not a moderator, and the moderator password is set for the conference room, you can also join conference call as a moderator

1. Dial the conference room number.
2. Enter the moderator password.

   If you are the first participant in the conference call, the system plays a hold music to you.

Invite Users to a Conference Call

By default, only the conference moderators can invite users to the conference. This topic describes how to allow participants to invite users and how to invite users to a conference call.

Allow participants to invite users

1. Log in to PBX web portal, go to **Call Features > Conference**, edit the desired conference.
2. Select the checkbox of **Allow Extension Participants to Invite**.
3. Click **Save** and **Apply**.

Invite users to a conference call

1. During a conference call, press the # key.

   You are forced out of the conference call temporarily.
2. Dial the number that you want to invite.

   After the invited user joins or rejects the conference call, you will return to the conference call.

Manage Conference Rooms

This topic describes how to edit conference room settings and delete conference rooms.

Edit a conference room

> **Note:**
> You can not change the conference room number after setting up a conference room.

1. Log in to PBX web portal, go to **Call Features > Conference**.
2. Click beside the conference room that you want to edit.
3. Change the conference room settings according to your needs.
4. Click **Save** and **Apply**.

Delete conference rooms

You can delete a conference room, or delete conference rooms in bulk.

1. Log in to PBX web portal, go to **Call Features > Conference**.
2. To delete a conference room, do the following:
   a. Click beside the conference room that you want to delete.
   b. Click **OK** and **Apply**.
3. Delete conference rooms in bulk, do the following:
   a. Select the checkboxes of the conference rooms that you want to delete, click **Delete**.
   b. Click **OK** and **Apply**.

Conference Voice Menu

This topic describes the conference voice menu.

During the conference call, the participants can manage the conference by pressing * key on their phones to access voice menu for conference room.

The following table shows the conference voice menu.

Key	Description	Moderator	Participant
1	Mute or unmute yourself.	√	√
2	Lock or unlock the conference.	√	×
3	Eject the last user.	√	×
4	Decrease the conference volume.	√	√

Key	Description	Moderator	Participant
6	Increase the conference volume.	√	√
7	Decrease your volume.	√	√
8	Exit the voice menu.	√	√
9	Increase your volume.	√	√

Speed Dial

Speed Dial Overview

Speed dial is often the easiest way to quickly connect with people and extensions that you dial frequently. This topic describes what is speed dial, and how to use speed dial.

What is speed dial

Speed dial is a feature that allows you to assign a speed dial code to a number that the users frequently dial. When dialing long strings of overseas numbers, the users do not have to remember or enter long telephone numbers on their phones.

How to use speed dial

You can create speed dial with a **Prefix** in front of the **Speed Dial Number** to avoid interference with your extensions.

- **Speed Dial Number**: The shorter number you assign to the phone number.
- **Prefix**: The code to access the speed dial feature. The default prefix is *89.

The users can dial {*prefix*}+{*speed_dial_number*} to call an assigned phone number. For example, assign `1` to phone number `5503302`, dial `*891` to place a call to `5503302`.

Set up Speed Dial Prefix

You need to dial the speed dial code with a prefix. The prefix is used to access the speed dial feature, and avoid interference with the extensions. This topic describes how to set up speed dial prefix.

Procedure

1. Log in to PBX web portal, go to **Call Features > Speed Dial**.
2. Click **Prefix**.
3. In the **Speed Dial Prefix** field, enter a prefix according to your needs.

   > **Note:**
   > - Only numbers and special characters `* #` are allowed.
   > - The maximum character length is 7.

   The default speed dial prefix is `*89`.
4. Click **Save** and **Apply**.

> **Tip:**
> To disable the speed dial prefix, go to **Call Features > Feature code > Speed Dial > Speed Dial Prefix**.

Add a Speed Dial Number

This topic describes how to add a speed dial number.

Background information

- Assume that you have an outbound route that allows you to dial an external number 15990234988, and you want to dial speed number 111 to reach an external number 15990234988 through the route.
- The speed dial prefix is enabled and set to `*89`.

Procedure

1. Log in to PBX web portal, go to **Call Features > Speed Dial**, click **Add**.
2. In the **Speed Dial Number** field, enter `111`.
3. In the **Phone Number** field, enter `15990234988`.
4. Click **Save** and **Apply**.

Result

Dial *89111 on your phone to call the external number 15990234988.

Manage Speed Dial Numbers

This topic describes how to edit a speed dial number, or delete speed dial numbers.

Edit a speed dial number

1. Log in to PBX web portal, go to **Call Features > Speed Dial**.
2. Click  beside the speed dial entry that you want to edit.
3. Change the **Speed Dial Number** or **Phone Number** according to your needs.
4. Click **Save** and **Apply**.

Delete speed dial numbers

You can delete a speed dial entry, or delete speed dial entries in bulk.

1. Log in to PBX web portal, go to **Call Features > Speed Dial**.
2. To delete a speed dial number, do as follows:
    a. Click  beside the speed dial entry that you want to delete.
    b. Click **OK** and **Apply**.
3. To delete speed dial numbers in bulk, do as follows:
    a. Select the checkboxes of the speed dial entries that you want to delete, click **Delete**.
    b. Click **OK** and **Apply**.

Export and Import Speed Dial Numbers

The speed dial numbers configured on Yeastar P-Series 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.
- **Transfer Bounce Back (Applicable to Both Blind/Semi-attended Transfer)**: If enabled, when an extension user performs a blind transfer/semi-attended transfer and the transfer recipient doesn't answer, the system sends the call back to the extension user.

Set up Call Transfer

This topic describes how to set up call transfer.

Set up attended transfer

1. Log in to PBX web portal, go to **Call Features > Feature code > Call Transfer**.

2. Select the checkbox of **Attended Transfer** to enable the attended transfer feature.

   If unselected, the extension users can not perform attended transfer by dialing the feature code.
3. Enter a code number according to your needs.
4. In the **Digit Timeout(s)** drop-down list, select a timeout for entering transfer recipient's number after you hear a dial tone.
5. In the **Attended Transfer Timeout(s)** field, enter a number of seconds for transfer recipient to take the transferring call.
6. Click **Save** and **Apply**.

Set up blind transfer

1. Log in to PBX web portal, go to **Call Features > Feature code > Call Transfer**.
2. Select the checkbox of **Blind Transfer** to enable the blind transfer feature.

   If unselected, the extension users can not perform blind transfer by dialing the feature code.
3. Enter a code number according to your needs.
4. In the **Digit Timeout(s)** drop-down list, select a timeout for entering transfer recipient's number after you hear a dial tone.
5. In the **Transfer Bounce Back (Applicable to Both Blind/Semi-attended Transfer)** option, set whether to transfer the call back to the transferor when the transfer recipient doesn't answer the call.
6. Click **Save** and **Apply**.

Perform an Attended Transfer

If you want to make sure someone is ready to take a transferred call or you need to explain something to the transfer recipient, you can perform an attended transfer. This topic describes how to perform an attended transfer.

Procedure

1. During a call, press the feature code of attended transfer (default *3).

   The original call is placed on hold, and the system prompts "transfer" and the dial tone.
2. Dial the phone number of the contact where you want the call to be transferred.
3. Wait for the call to be answered.

When the call is answered, talk to the transfer recipient.

4. Hang up the call directly to complete the call transfer.

   The original caller and the transfer recipient are connected.

Perform a Blind Transfer

If you do not need any interaction with the user who receives the call, you can perform a blind transfer. This topic describes how to perform a blind transfer.

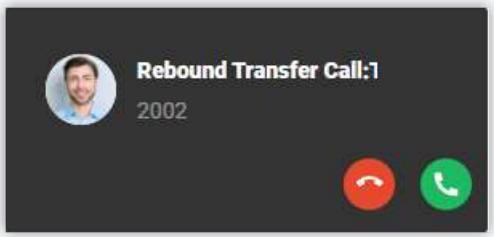
Procedure

1. During a call, press the feature code of blind transfer (default *03).

   The original call is placed on hold, and the system prompts "transfer" and the dial tone.
2. Dial the phone number of the contact where you want the call to be transferred.

   The call ends automatically, and the transfer recipient's phone rings.

   A new call between original caller and transfer recipient is established after transfer recipient answers.

> **Note:**
> By default, if the transfer recipient doesn't answer the call, the call will be routed to the call forwarding destination of the transfer recipient. If you have enabled **Transfer Bounce Back (Applicable to Both Blind/Semi-attended Transfer)**, the call will be transferred back to you with Caller ID displayed as **Rebound Transfer Call:** ***{caller_id_name}***.
>
> 
>

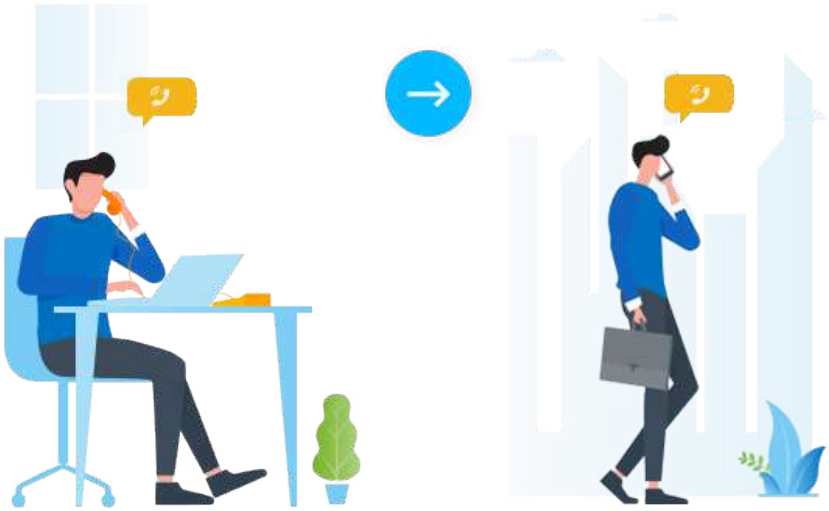
Call Flip

Call Flip Overview

Call Flip feature allows users to flip their ongoing calls from current device to another (with their extensions registered), without any interruption to the conversation.

Scenario

Assume that a sales representative is in a call with a customer on the desk phone, but has to get out of the office. In this case, the sales representative can flip the call to his mobile phone, keeping talking without customer knowing the switchover.



Methods of Call Flip

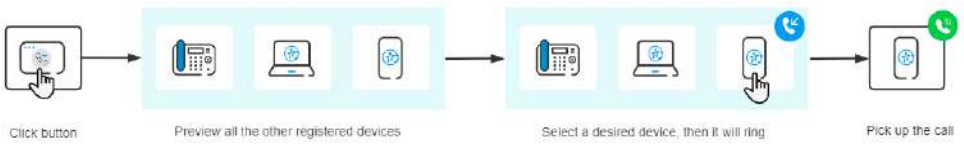
Extension users can flip an active call in the following ways:

- Flip an active call by clicking 'Call Flip' button
- Flip an active call by dialing 'Call Flip' feature code

Flip an active call by clicking 'Call Flip' button

With a simple click of the **Call Flip** button, users can preview all the other devices where their extensions are registered, and select a device to flip the call.

We provide a flowchart to help you understand the workflow:



This method is supported on the following endpoints:

- **Linkus Mobile Client**

  For more information, see Flip an Active Call between Devices.
- **Linkus Desktop Client**

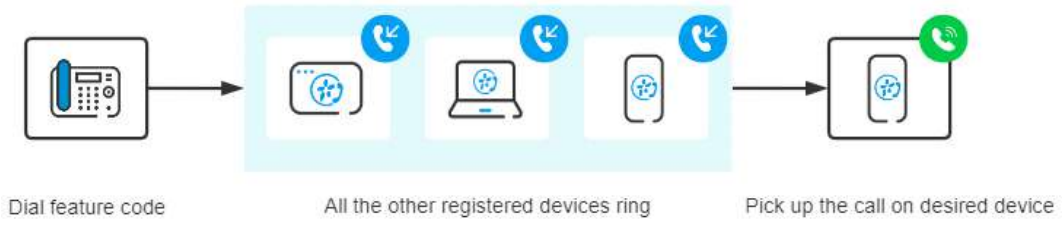
  For more information, see Flip an Active Call between Devices.
- **Linkus Web Client**
  For more information, see Flip an Active Call between Devices.

> **Note:**
> If Linkus Web Client is associated with 'Yeastar Linkus for Google', see Flip an Active Call between Devices.

Flip an active call by dialing 'Call Flip' feature code

By dialing the **Call Flip** feature code, all the other devices where users' extensions are registered will simultaneously ring. Users pick up the call on a desired device, then the call would be flipped.

We provide a flowchart to help you understand the workflow:



With the **Call Flip** feature code enabled on Yeastar P-Series 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.

3. Click **Save** and **Apply**.

   During a call, extension users can dial the feature code to flip the active call to another device where their extensions are registered. For more information, see Flip an Active Call by Dialing a Feature Code.

Disable 'Call Flip' feature code

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. In the **Call Flip** section, unselect the checkbox.

3. Click **Save** and **Apply**.

   Extension users can NOT flip an active call by dialing the feature code.

Flip an Active Call by Dialing a Feature Code

This topic describes how to flip an active call from current device to another (with the same extension registered) by dialing a feature code.

Requirements

- **PBX Server**: 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)
   - Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
   - Auto Provision IP Phones Remotely (Provision Link Method)
3. If the extension has been associated with a phone, reprovision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to this extension.

Result

- When extension group members receive a call, the user can press the Feature key directly to answer the call.

- When the call is picked up, the IP phones of other extension group members display a missed call.

Pick up a Call for a Specific Extension

This topic describes how to set up a BLF key on an IP phone to pick up a call for a specific extension.

Background information

For the users who want to monitor call status changes of a specific extension, and pick up the call on their phones, you can set a BLF key for each user by auto provisioning. Users can also set function keys on their own IP phones. For more information, contact the phone manufacturer.

> **Note:**
> The default feature code for picking up an extension call is `*04`. You can change, enable, or disable the code on PBX web portal: **Call Features > Feature Code > Call Pickup > Extension Pickup**.

Set up a BLF key

The following takes Yealink phone as an example to set a BLF key for call pickup.

1. Assign function keys for extension users to monitor agent status.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
      - If you want to assign function keys for a specific extension user, click beside the desired extension.
      - If you want to assign function keys for multiple extensions, select the checkboxes of the desired extensions, and click **Edit**.
   b. Click the **Function Keys** tab.
   c. Configure function keys.

> **Note:**
> The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

- **Type**: Select **BLF**.
- **Value**: Select the desired extension.
- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

d. Click **Save**.

2. If the extension hasn't been associated with a phone, see the following topics to bind a phone with the extension.
   - Auto Provision IP Phones in Local Network (PnP Method)
   - Auto Provision IP Phones in Local Network (DHCP Method)
   - Auto Provision IP Phones Remotely (RPS FQDN Method)
   - Auto Provision IP Phones Remotely (RPS Method)
   - Auto Provision IP Phones Remotely (Provision Link - FQDN Method)
   - Auto Provision IP Phones Remotely (Provision Link Method)
3. If the extension has been associated with a phone, reprovision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to this extension.

Result

- When the monitored extension receives an incoming all, the BLF key fast flashes red. The user can press the BLF key directly to answer the call.
- When the call is picked up, the IP phone where the monitored extension is registered displays a missed call.

Call Parking

Call Parking Overview

Call parking is a method of holding a call on a phone, anyone can retrieve the call on another phone. This topic describes what is call parking, parking number, parking types, parking recall, and parking code.

What is call parking

Traditionally, you can only retrieve the call on the same phone when you hold a call. Call parking allows you to hold a call on a parking number, and allows you to dial the parking number on any phone to retrieve the call.

Parking number

Parking number, also known as slot or orbit, is a virtual extension number that the system assigns to the parked call. One parked call occupies one parking number.

The maximum number of simultaneous parking number is 100.

Parking types

Yeastar P-Series 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 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**.

Set up Parking Timeout Destination

By default, if a parked call is not retrieved after 60 seconds, the call will be transferred back to the originator. You can set up the parking timeout and timeout destination. This topic describes how to set up parking timeout and timeout destination for an unretrieved call.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code > Call Parking**.
2. In the **Parking Timeout (s)** field, enter the number of seconds for the parked call.
3. In the **Timeout Destination** drop-down list, select a destination to receive the unretrieved call.

   A parked call will be routed to the designated destination when the call parking times out.

   - **Call Parking Initiator**: Route the call to the user who parks this call.
   - **Extension**: Route the call to the designated extension number.
   - **Extension Voicemail**: Route the call to the designated extension's voicemail.
   - **Group Voicemail**: Route the call to the voicemail box of a queue, a ring group, or a custom group.
   - **External Number**: Route the call to the designated external number.

> **Note:**
> Set the **Prefix** according to your outbound route so that PBX can successfully route incoming calls to external number.
> - If the **Strip** of outbound route is not set, you don't have to set the **Prefix**.
> - If the **Strip** of outbound route is set, you need to set the **Prefix** according to the **Patterns** of outbound route.

4. Click **Save** and **Apply**.

Set up Music on Hold for Call Parking

This topic describes how to customize music on hold for call parking on Yeastar P-Series Software Edition.

By default, the system plays a default music on hold (set on **PBX Settings > Voice Prompt > Prompt Preferences > Music on Hold**) to the parked party when a call is parked. You can refer to this topic to customize the music for call parking.

Requirements

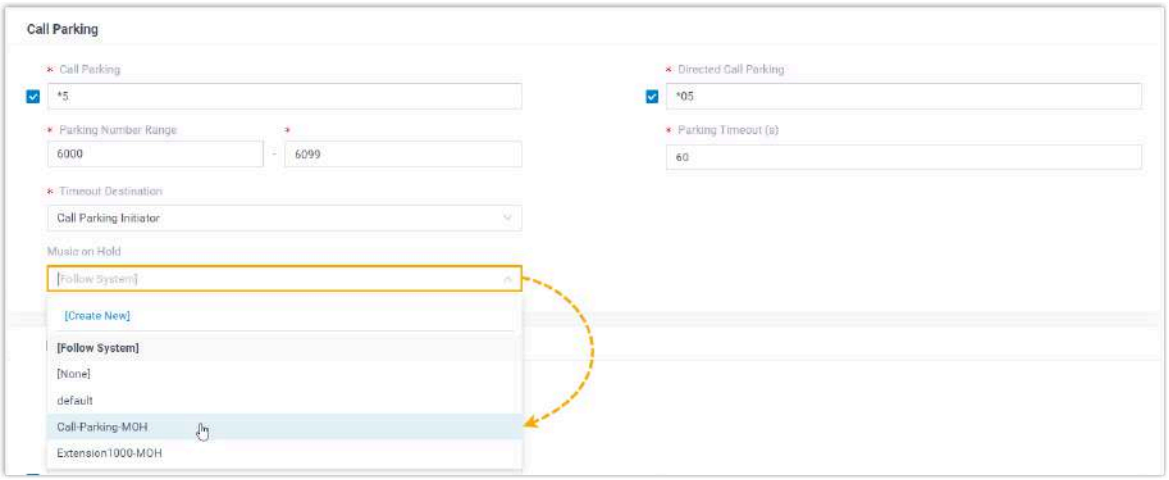
The firmware version of PBX server is 83.15.0.22 or later.

Prerequisites

You have prepared and uploaded a custom Music on Hold (MoH) playlist.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code > Call Parking**.
2. In the **Music on Hold** drop-down list, select the MoH playlist that you have uploaded.



3. Click **Save** and **Apply**.

Monitor a Parking Number on an IP Phone

This topic describes how to set up a function key on a user's phone to monitor a parking number.

Background information

For users who use directed call parking and want to monitor a specific parking number, you can set a function key for each user by auto provisioning.

> **Note:**
> Users can also set function keys on their own IP phones. For more information, contact the phone manufacturer.

> **Tip:**
> Agents can also press the function keys to park or retrieve a call.

Procedure

1. Assign function keys for extension users to monitor parking number.
   a. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
      - If you want to assign function keys for a specific extension user, click beside the desired extension.

- If you want o assign function keys for multiple extensions, select the checkboxes of the desired extensions, and click **Edit**.

b. Click the **Function Keys** tab.
c. Configure function keys.

> **Note:**
> The number of programmable keys varies by phone models. If the number of function keys you assign to an extension exceeds the number of programmable keys, the redundant function keys cannot take effect.

- **Type**: Select **Park & Retrieve**.
- **Value**: Select a parking number.
- **Label**: Optional. Enter a value, which will be displayed on the phone screen.

d. Click **Save**.

2. If the extension hasn't been associated with a phone, see the following topics to register the extension to a phone.
   - Auto Provision IP Phones in Local Network (PnP Method)
   - Auto Provision IP Phones in Local Network (DHCP Method)
   - Auto Provision IP Phones Remotely (RPS FQDN Method)
   - Auto Provision IP Phones Remotely (RPS Method)
3. If the extension has been associated with a phone, reprovision the phone to take effect.
   a. Go to **Auto Provisioning > Phones**.
   b. Click beside the phone assigned to this extension.

Result

The function key shows the real-time status of the parking number.

- **Green**: The parking number is idle.

  The user can press the function key to park an active call to the idle parking number.
- **Red**: The parking number is occupied.

  The user can press the function key to retrieve a parked call from the monitored parking number.

> **Note:**

The key LED status may vary by phone models.

Call Monitoring

Call Monitoring Overview

Call monitoring feature allows you to listen in on employee calls without interference or joining in the conversation as a third party. It helps you check on the quality of teams' sales calls, learn more about customer reactions and insights, and gain a better view for coaching and training the team.

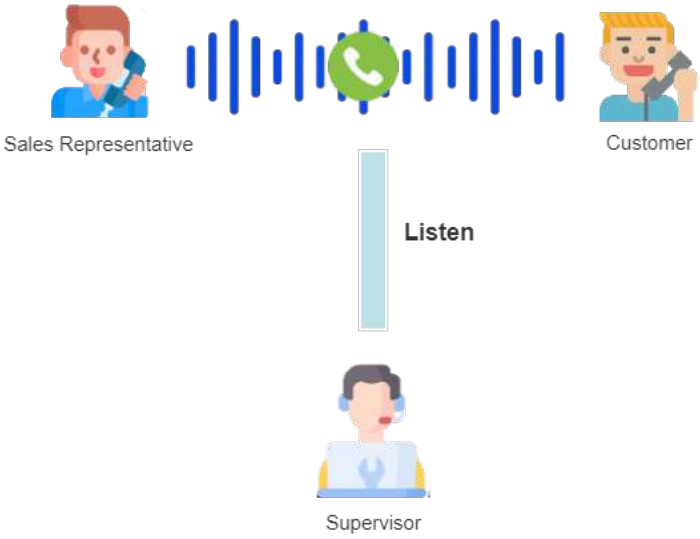
Modes of call monitoring

Yeastar P-Series 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.

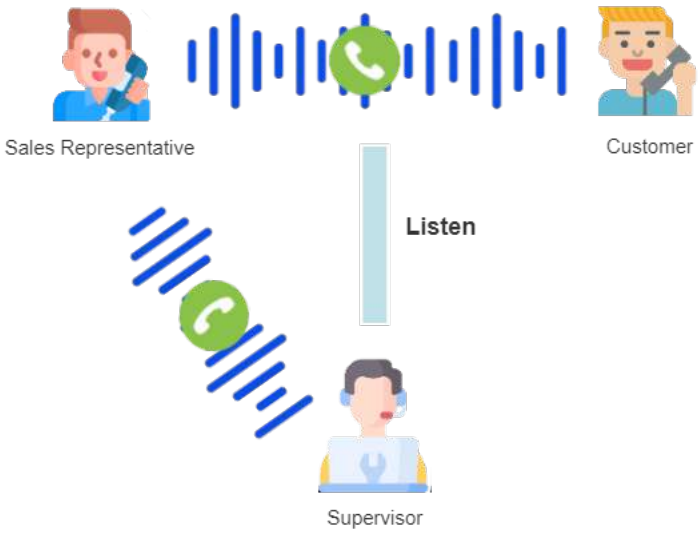
This mode is often used for supervisor to track the daily actions of sales representatives and evaluate their performance on the sales process.



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.

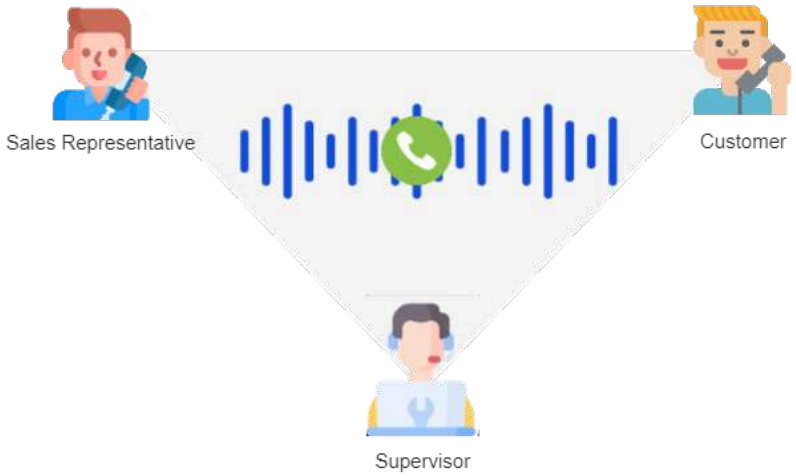
This mode is often used for supervisor to coach remote sales representatives and train them as they work on a sales call.



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

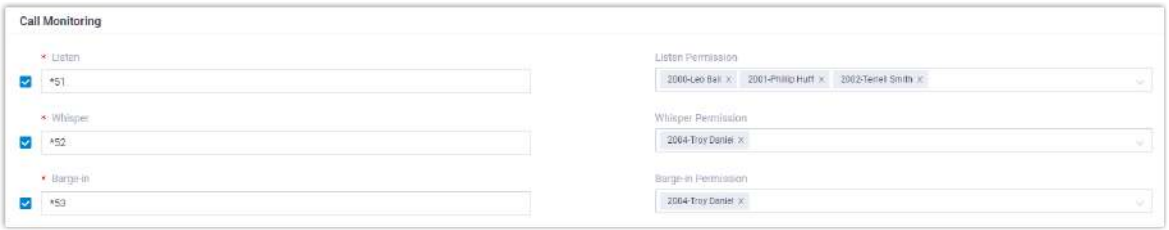
By default, all the extension users can NOT monitor others' calls by dialing a feature code, but their calls can be monitored instead.

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.



   a. Select the checkbox of a desired call monitoring mode, then configure the feature code.
      - **Listen**: Listen in on a call in real time, but can NOT talk with either party.

        The default feature code is *51.
      - **Whisper**: Listen in on a call in real time, and directly talk with the monitored extension without being heard by the other party.

        The default feature code is *52.
      - **Barge-in**: Listen in on a call in real time, and talk with both parties.

        The default feature code is *53.
   b. In the **Listen/Whisper/Barge-in Permission** drop-down list, select the allowed extensions for each call monitoring mode respectively.

3. Click **Save** and **Apply**.

Result

The authorized user can dial **Feature Code + Extension Number** to monitor the calls of the extensions that are allowed to be monitored.

Important:

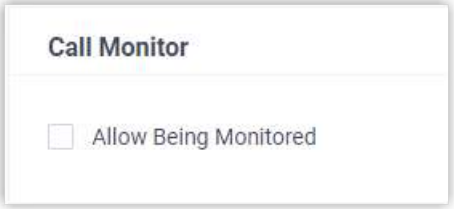
- Monitoring **Conference Calls** via feature code is NOT supported.
- Monitoring calls of extensions that are invisible on Linkus clients is NOT supported.
- During an internal call where one party allows being monitored while the other party disallows, the call can NOT be monitored even by the authorized user.

Disallow Users to be Monitored by Others

By default, all the extension users are allowed to be monitored. To keep specific users' calls private, you can disable the monitoring feature for users.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. To prevent an extension from being monitored, do as follows:
   a. Click beside the desired extension.
   b. Click **Features** tab.
   c. In the **Call Monitor** section, unselect the checkbox of **Allow Being Monitored**.



   d. Click **Save** and **Apply**.
3. To prevent multiple extensions from being monitored, do as follows:
   a. Select the checkboxes of the desired extensions, then click **Edit**.
   b. Click **Features** tab.

c. Select the checkbox of **Call Monitor**, then unselect the checkbox of **Allow Being Monitored**.

d. Click **Save** and **Apply**.

Result

The users' calls can NOT be monitored by anyone.

Call Force Drop

Allow Users to Force Drop Extensions' Calls

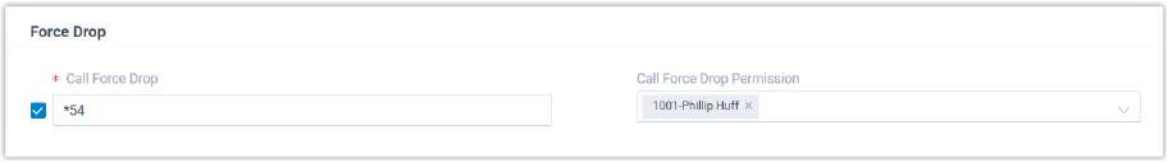
Call Force Drop feature allows the authorized users to force disconnect an extension's current call by dialing a feature code.

Requirements

The version of PBX is 83.16.0.25 or later.

Procedure

1. Log in to PBX web portal, go to **Call Features > Feature Code**.
2. Scroll down to the **Force Drop** section, then complete the following settings.



   - **Call Force Drop**: Retain the default feature code `*54` or change it as needed.
   - **Call Force Drop Permission**: Select the extensions that are allowed to force drop extensions' calls by dialing the feature code.
3. Click **Save** and **Apply**.

Result

The authorized users can dial *{feature_code}* + *{extension_number}* to force drop an extension's current call, or dial *{feature_code}* to force drop the monitored extension's current call.

For more information, see Force Drop an Extension's Call.

Force Drop an Extension's Call

This topic describes how an authorized user can force drop an extension's current call by dialing a feature code.

Prerequisites

The user to force drop calls has been assigned the **Call Force Drop** permission.

Procedure

- The authorized user dials *{feature_code}* + *{extension_number}* to force drop an extension's current call.

  For example, dial `*541000` to force drop the current call of extension 1000.
- The authorized user dials *{feature_code}* to force drop the monitored extension's current call.

  For example, while monitoring the current call of extension 1000, dial `*54` to force drop the call.

Result

- The authorized user who forces drop the call hears a prompt "Call force drop succeeded", then the call hangs up.
- The extension user whose call is forcibly disconnected hears a prompt "This call was forcibly dropped", then the call hangs up.
- The other party on the call is hung up directly.

Boss-Secretary

Set up Boss-Secretary Feature for Extensions

Yeastar Boss-Secretary feature allows the secretary to filter incoming calls for the boss. You can enable this feature on an extension to designate it a boss extension, then assign secretary extension(s) to it and set forwarding rule. After the setup, any incoming calls to the boss extension that meet the forwarding rule will be automatically forwarded to the secretary extension. The secretary can answer the call and decide whether to transfer it to the boss.

Video Tutorial

Prerequisites

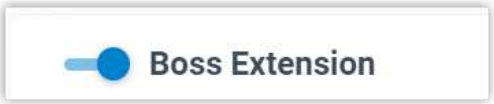
- If you want to assign multiple secretary extensions to one boss extension, you need to group all the secretary extensions into one ring group.

  For more information, see Create a Ring Group.

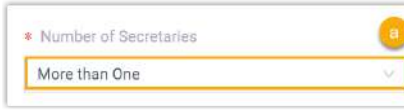
- If you want the boss extension to ring simultaneously when calls are forwarded to the secretary, you need to place both the boss extension and the secretary extension(s) into one ring group.

Procedure

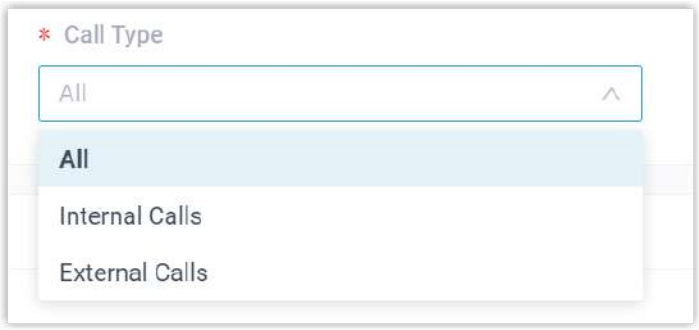
1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click beside the extension that you want to set as the 'Boss Extension'.
3. Click the **Features** tab.
4. In the **Boss Extension** section, turn on the switch to set the extension as the boss extension.

   The preselected **Enable Boss-Secretary Feature** option indicates the feature is enabled for this extension.
5. Specify secretary extension(s) for this boss extension.

One Secretary	Multiple Secretaries
	
a. In the **Number of Secretaries** drop-down list, select **Only One**. b. In the **Secretary Extension** drop-down list, select the desired extension.	a. In the **Number of Secretar** b. In the **Secretary Group** dro

6. In the **Call Type** drop-down list, decide which incoming calls to the boss extension need forwarding to the secretary extension(s).



- **All**: Forward all the incoming calls firstly to the secretary extension(s).
- **Internal Calls**: Forward only the internal incoming calls firstly to the secretary extension(s).
- **External Calls**: Forward only the external incoming calls firstly to the secretary extension(s).

> **Note:**
> If you set up Call Handling Based on Caller ID for the boss extension, the incoming calls that meet the call handling rule will be handled accordingly, instead of following the forwarding rule you set here.

7. Click **Save** and **Apply**.

Result

The extension is set up with the Boss-Secretary feature and designated as the boss extension.

The following features are achieved:

- Incoming calls of the selected call type to the boss extension will be automatically forwarded to the secretary extension(s). The secretary can answer the call and determine if it needs to be transferred to the boss.
- A call can be transferred between the boss and secretaries by putting it on hold and resuming it.
  When one party holds a call, the other party can resume and answer the call on the following endpoints:

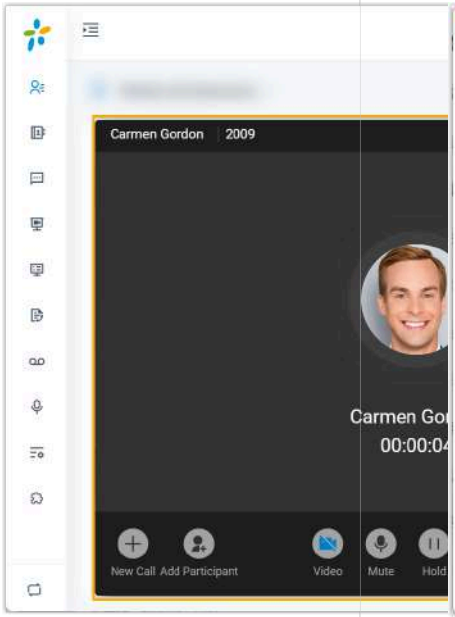
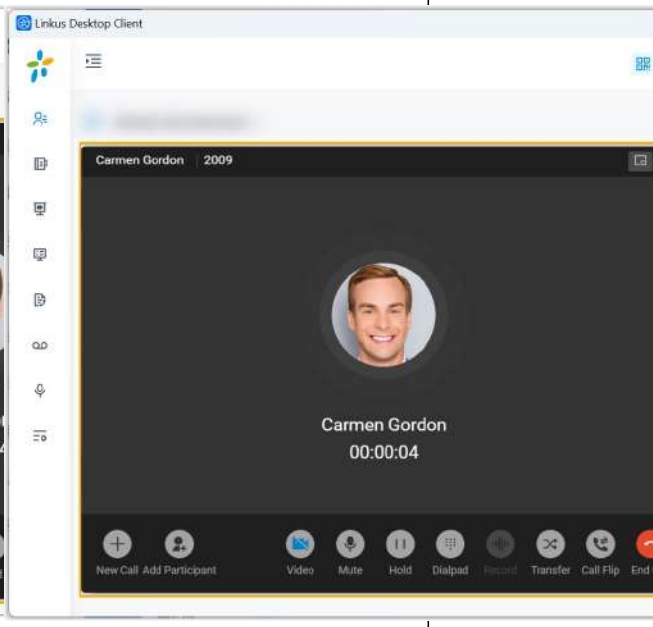
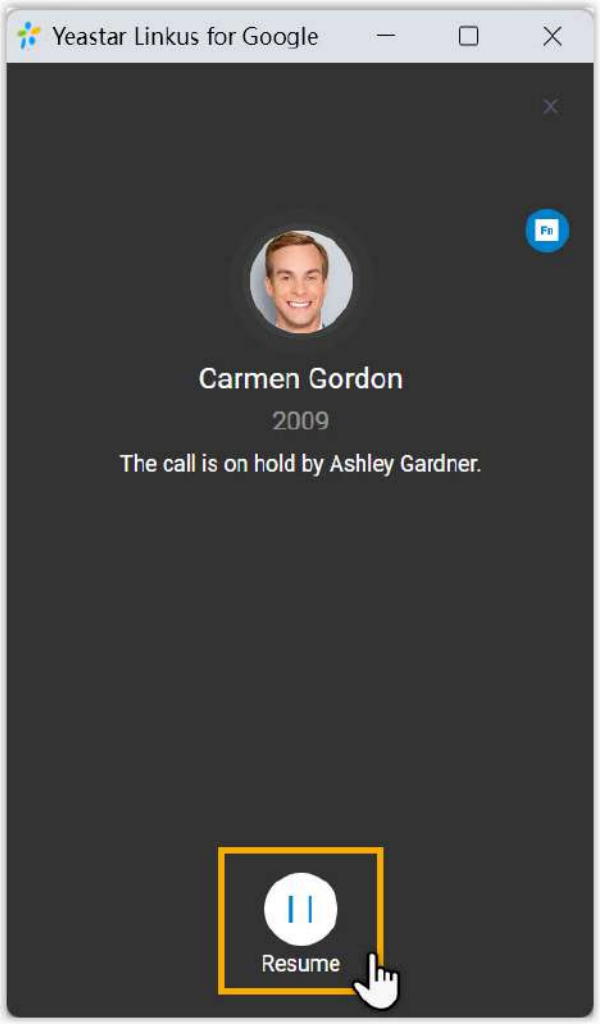
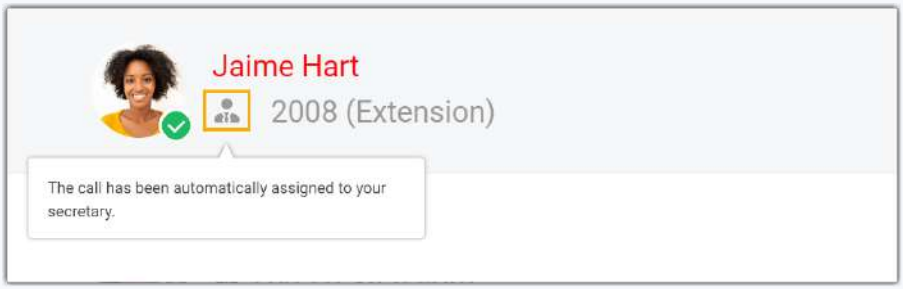
<table>
<tr><th>Endpoint</th><th>Description</th></tr>
<tr><td>Linkus Web Client & Linkus Desktop Client</td><td>Click Resume in the pop-up window to answer the call.
Note:
◦ To use this feature, ensure the Linkus Desktop Client meets the following version requirements:
▪ Windows Desktop: 1.1.2 or later.
▪ Mac Desktop: 1.1.2 or later.
◦ Linkus Mobile Client does NOT support resuming calls transferred from boss/secretary.
Figure 1. Linkus Web Client
 

Figure 2. Linkus Desktop Client
 
</td></tr>
<tr><td>Yeastar Linkus for Google</td><td>Click Resume in 'Yeastar Linkus for Google' to answer the call.</td></tr>
</table>

Endpoint	Description
	
IP phone	Press the BLF key on the IP phone to answer the call. **Important:** To resume the transferred calls via IP phones, you need to set up IP phones for the boss or secretary. ◦ To allow the boss to resume calls transferred from the secretary via an IP phone, see Monitor secretary's call status on an IP phone. ◦ To allow the secretary to resume calls transferred from the boss via an IP phone, see Monitor boss's call status on an IP phone.

Note:

- Boss can disable this feature or change the call type that needs forwarding on their Linkus Web Client or Linkus Desktop Client (path: **Preferences > Features > Boss Extension**), and the updated settings will be synchronized to PBX automatically.
- On the **Call Logs** page of the boss's Linkus clients, missed calls with icon indicate that the calls were automatically forwarded to the secretary extension, distinguishing them from the actual missed calls of the boss extension.



Monitor Call Status

Monitor Secretary's Call Status

With the Boss-Secretary feature enabled, you can set up function keys and configure the IP phone for the boss, allowing the boss to check if the secretary is currently handling his or her call by monitoring the secretary's call status through Linkus clients and IP phone.

Monitor secretary's call status on Linkus clients

By setting up function key(s) for the boss's extension, the boss can monitor secretary's call status through **Linkus Desktop Client**, **Linkus Web Client**, and **Yeastar Linkus for Google**.

Prerequisites

- You have Set up Boss-Secretary Feature for Extensions.
- Obtain the **Enable Boss-Secretary Feature** feature code.

Note:
The default feature code is `*59`. You can view or update the feature code on **Call Features > Feature Code > Boss-Secretary Feature > Enable Boss-Secretary Feature**.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, select the boss extension and click .
2. Click the **Function Keys** tab.
3. Configure the following settings to subscribe to the secretary's call status.

   - **Type**: Select **Boss-Secretary Feature**.
   - **Value**: Enter the **Enable Boss-Secretary Feature Code** and **Secretary Extension Number**.

     For example, the **Enable Boss-Secretary Feature Code** is `*59`, and the **Secretary Extension Number** is `2007`, then enter `*592007`.
   - **Label**: Optional. Enter a display name for this function key.
4. Click **Save**.

Result

The boss can monitor the secretary's call status by the icons in the **Function Keys** list of Linkus clients.

Icons & Descriptions

- : The secretary is NOT handling any calls for the boss.
- : The secretary is answering calls for the boss.
- : The secretary is putting a call on hold, waiting for the boss to answer.

Linkus clients

Figure 3. **Linkus Web Client & Linkus Desktop Client**

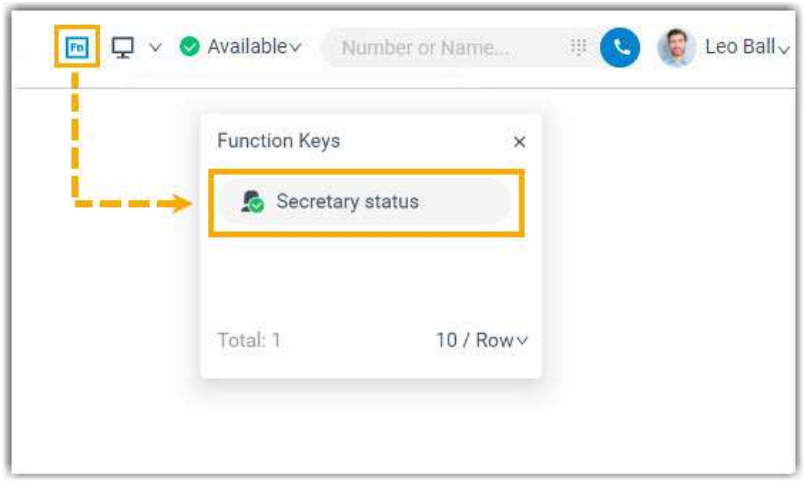


Figure 4. **Yeas**

Monitor secretary's call status on an IP phone

By setting up the boss's IP phone, the boss can monitor the secretary's call status by the BLF LED, and resume calls transferred from the secretary using the BLF key.

Prerequisites

- You have set up function keys for boss to monitor secretary's call status.
- Ensure that the IP phone is connected to Yeastar P-Series Software Edition via auto provisioning, and has been assigned to the boss extension.

> **Note:**
> For more information about auto provisioning, see the following topics:
> - Auto Provision IP Phones in Local Network (PnP Method)
> - Auto Provision IP Phones in Local Network (DHCP Method)
> - Auto Provision IP Phones Remotely (RPS FQDN Method)
> - Auto Provision IP Phones Remotely (RPS Method)

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Click beside the boss's phone.
3. In the pop-up window, click **OK**.

Result

The boss can monitor the secretary's call status through the BLF LED on his or her IP phone:

- **Solid Green**: The secretary is NOT handling any calls for the boss.
- **Solid Red**: The secretary is answering calls for the boss.
- **Flashing Red**: The secretary is putting a call on hold, waiting for the boss to answer. And the boss can press the BLF key to resume and answer the call.

> **Note:**
> If the boss is using a **Fanvil phone**, you need to set the **BLF Hold** LED to either **Slowblink** or **Fastblink**. Otherwise, the BLF LED will not flash when the secretary places a call on hold.

Monitor Boss's Call Status

With the Boss-Secretary feature enabled, you can set up function keys and configure the IP phone for the secretary, allowing the secretary to check if the boss is holding calls for him or her to resume by monitoring the boss's call status on Linkus clients and IP phone.

Monitor boss's call status on Linkus clients

By setting up function key(s) for the secretary's extension, the secretary can monitor the boss's call status through **Linkus Desktop Client**, **Linku Web Client**, and **Yeastar Linkus for Google**.

Prerequisites

- You have Set up Boss-Secretary Feature for Extensions.
- Obtain the **Enable Boss-Secretary Feature** feature code.

> **Note:**

> The default feature code is `*59`. You can view or update the feature code on **Call Features > Feature Code > Boss-Secretary Feature > Enable Boss-Secretary Feature**.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, select the secretary extension and click .
2. Click the **Function Keys** tab.
3. Configure the following settings to subscribe to the boss's call status.

   - **Type**: Select **Boss-Secretary Feature**.
   - **Value**: Enter the **Enable Boss-Secretary Feature Code** and **Boss Extension Number**.

     For example, the **Enable Boss-Secretary Feature Code** is `*59`, and the **Boss Extension Number** is `2010`, then enter `*592010`.
   - **Label**: Optional. Enter a display name for this function key.
4. Click **Save**.

Result

The secretary can check if the boss is currently holding a call by the icons in the **Function Keys** list of Linkus clients.

Icons & Descriptions

- : The boss is NOT holding any calls for the secretary to resume.
- : The boss is putting a call on hold, waiting for the secretary to resume.

Linkus clients

Figure 5. **Linkus Web Client & Linkus Desktop Client**

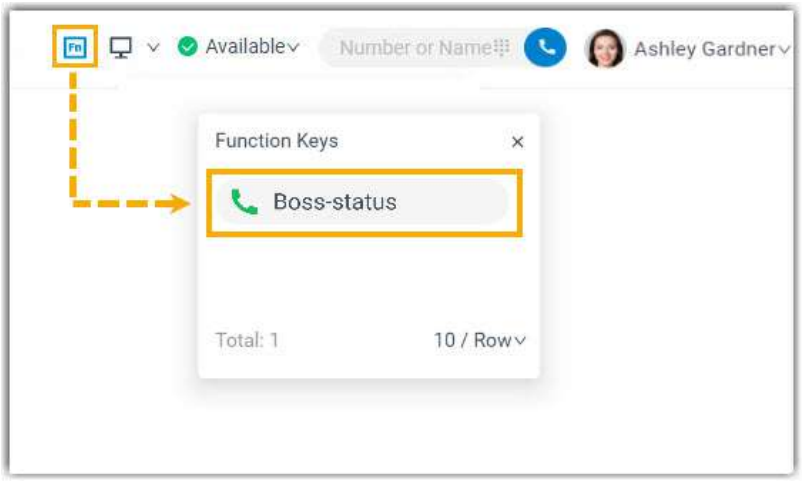


Figure 6. **Yeas**

Monitor boss's call status on an IP phone

By setting up the secretary's IP phone, the secretary can monitor the boss's call status by the BLF LED, and resume calls transferred from the boss using the BLF key.

Prerequisites

- You have set up function keys for secretary to monitor boss's call status.
- Ensure that the IP phone is connected to Yeastar P-Series Software Edition via auto provisioning, and has been assigned to the secretary extension.

> **Note:**
> For more information about auto provisioning, see the following topics:
> - Auto Provision IP Phones in Local Network (PnP Method)
> - Auto Provision IP Phones in Local Network (DHCP Method)
> - Auto Provision IP Phones Remotely (RPS FQDN Method)

◦ Auto Provision IP Phones Remotely (RPS Method)

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Click beside the secretary' phone.
3. In the pop-up window, click **OK**.

Result

The secretary can check if the boss is currently holding a call through the BLF LED on his or her IP phone:

- **Solid Green**: The boss is NOT holding any calls for the secretary to resume.
- **Flashing Red**: The boss is putting a call on hold, waiting for the secretary to resume. And the secretary can press the BLF key to resume the call.

Note:
If the secretary is using a **Fanvil phone**, you need to set the **BLF Hold** LED to either **Slowblink** or **Fastblink**. Otherwise, the BLF LED will not flash when the boss places a call on hold.

Hot Desking

Hot Desking Overview

Hot desking feature allows extension users to log in to a shared desk phone temporarily using their extension number and voicemail PIN, so that users can make and receive calls on the shared phone with their own extension numbers.

Scenario

The Hot Desking feature is ideal for shared offices, field teams, and call centers where employees have flexible schedules or work in shifts.

For example, call centers typically work in shifts to provide a 24-hour service, so employees may need to share a desk phone at different times. With hot desking feature, the employ-

ee can log in to a shared phone and answer incoming calls with his or her own extension during working hours. When the employee log out of the shared phone after work, the system automatically logs the user out of the queue, avoiding delays in responding to incoming calls. This not only optimizes the use of telephone hardware resources but also improves the economic benefits of the call center.

Requirements

- **PBX Server**: The firmware of Yeastar P-Series Software Edition is 83.10.0.30 or later.
- **IP Phone**: The model and firmware of the IP phone meets the requirements listed in Auto Provisioning - Supported Devices.

Process of setting up hot desking

To implement hot desking, you need to complete the following configurations:

Set up a hot desking phone

You need to set up a hot desking phone via auto provisioning according to your network environment.

For more information, see Set up a Hot Desking Phone.

Enable hot desking for extension users

You need to enable hot desking feature for specific extension users. Only the extension users with hot desking feature enabled can log in to a hot desking phone.

For more information, see Enable Hot Desking for an Extension User.

Methods of using hot desking

After you set up a hot desking phone, authorized users can log in to and log out of the hot desking phone in the following ways:

- Dial a Guest In / Guest Out feature code
- Press a Guest In / Guest Out key

Dial a Guest In / Guest Out feature code

By dialing a feature code on a hot desking phone, users can log in and use the phone with their own extension number, and log out after finish using the phone.

The default hot desking feature code is listed below:

- **Guest In**: *84
- **Guest Out**: *084

> **Tip:**
> You can change, enable, or disable the hot desking feature code on PBX web portal: **Call Features > Feature Code > Hot Desking**.

For more information, see dial a feature code to log in and dial a feature code to log out.

Press a Guest In / Guest Out key

The PBX system automatically assigns a **Guest In** and **Guest Out** key to a hot desking phone for login or logout. Users can press the BLF key on the phone to log in and use the phone with their own extension number, or log out after finish using the phone.

For more information, see press a BLF key to log in and press a BLF key to log out.

Set up Hot Desing

Set up a Hot Desking Phone

This topic describes how to set up a phone for hot desking via auto provisioning.

> **Important:**
> If the desired phone has been assigned to an extension, you need to delete the phone from auto provisioning phone list and RESET the phone first.

Supported devices

Hot desking is applicable on the IP phones listed in Auto Provisioning - Supported Devices.

Supported methods

According to your network environment, you can set up a hot desking phone on PBX web portal via the following methods:

- Set up a hot desking phone in local network (PnP method)

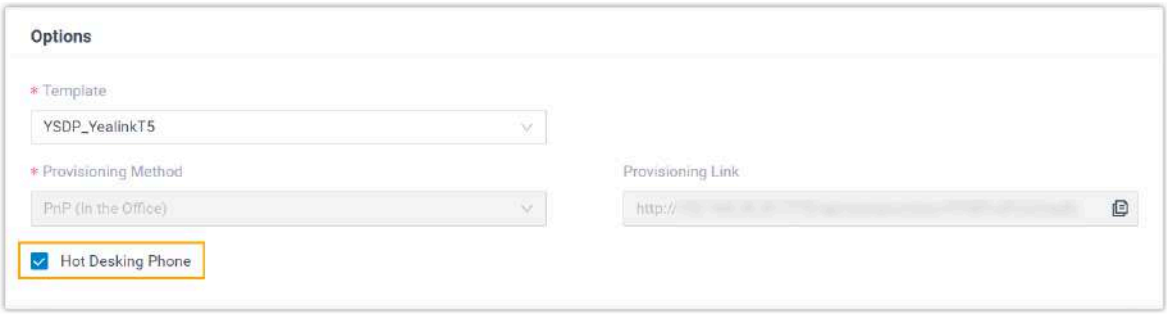
- Set up a hot desking phone in local network (DHCP method)
- Set up a hot desking phone in remote network (RPS FQDN / RPS method)

Set up a hot desking phone in local network (PnP method)

If the IP phone is in the same LAN subnet as the PBX, the PBX will detect the IP phone via PnP, and display the phone in the auto provisioning phone list. You can directly set an IP phone to a hot desking phone.

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Click beside an unassigned IP phone.

3. In the **Options** section, select the checkbox of **Hot Desking Phone**.



The phone is automatically assigned to a virtual extension named HostExt*{virtual_num}*.

4. Click **Save**.

Set up a hot desking phone in local network (DHCP method)

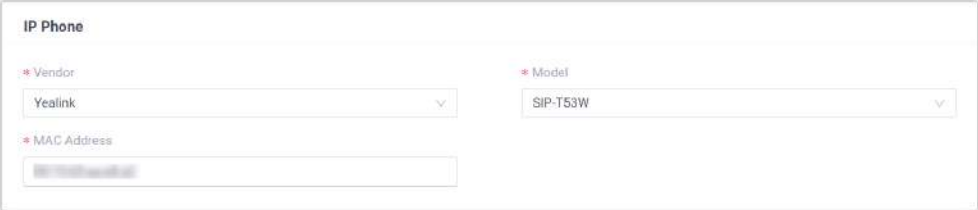
If the IP phone is in the same LAN subnet as the PBX server but doesn't support PnP provisioning method, or the IP phone is in different LAN subnet with the PBX server, you can set up the phone to a hot desking phone via DHCP provisioning method.

Prerequisites

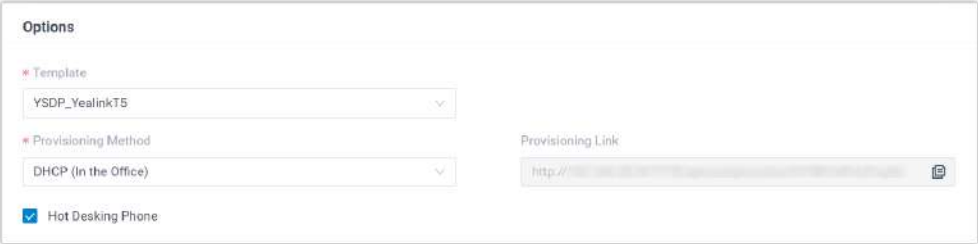
- Make sure the IP phone supports DHCP provisioning method.
- Gather information of IP phone, including Vendor, Model, and MAC address.

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Click **+Add > Add**.
3. In the **IP Phone** section, enter the phone's information:



   - **Vendor**: Select a phone vendor.
   - **Model**: Select a phone model.
   - **MAC Address**: Enter MAC address of the phone.
4. In the **Options** section, configure the following settings.



   - **Template**: Select a desired template for the phone from the drop-down list.
   - **Provisioning Method**: Select **DHCP (In the Office)**.

     A provisioning server URL is generated accordingly and displayed on the **Provisioning Link** field.
   - **Hot Desking Phone**: Enable the option to set the phone as a hot desking phone.

     The phone is automatically assigned to a virtual extension named HostExt*{virtual_num}*.

5. Click **Save**.
6. Configure the DHCP server.

> **Note:**
> Make sure there is only one DHCP server running on the network where the IP phone is located, otherwise the IP phone may fail to obtain an IP address.

Scenario	Instructions
The IP phone is in the same LAN as the PBX server, but doesn't support PnP provisioning	You can configure the DHCP server in either of the following ways: • Set up PBX as a DHCP server **Note:** The PBX built-in DHCP server will automatically obtain the provisioning link. • Set up option 66 on a third-party DHCP server with the provisioning link.
The IP phone is in different LAN with the PBX server	Set up DHCP option 66 on a third-party DHCP server with the provisioning link.

7. Reboot the IP phone manually.

Set up a hot desking phone in remote network (RPS FQDN / RPS method)

If the IP phone is deployed in a remote network, you can set up the phone to a hot desking phone via RPS FQDN or RPS method.

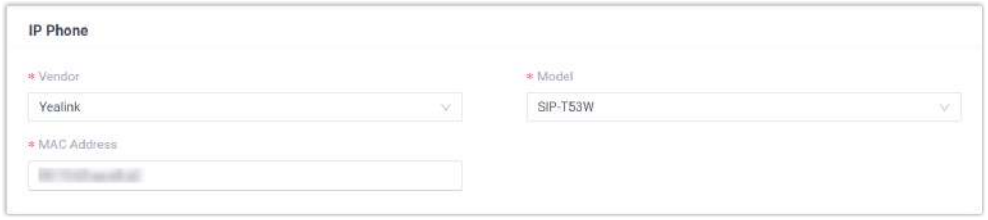
Prerequisites

Make sure that the following prerequisites are met according to your desired provisioning method.

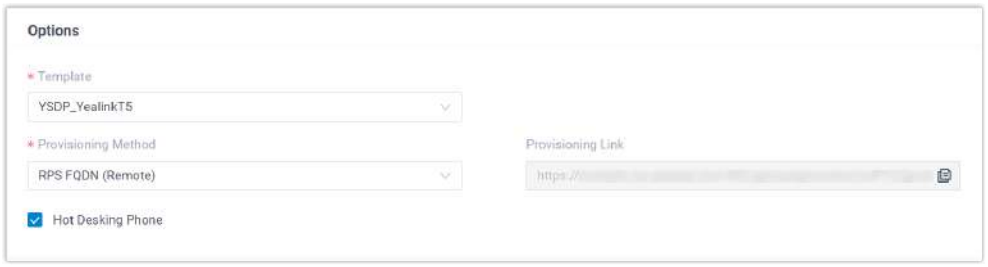
Method	Prerequisites
RPS FQDN	• You have subscribed **Enterprise Plan** or **Ultimate Plan**. • You have configured Yeastar FQDN for remote SIP access and remote web access. • Gather information of IP phone, including Vendor, Model, and MAC address.
RPS	• You have set up port forwarding on router (including RTP ports, SIP port, and Web Server port), and set up SIP NAT on the PBX to ensure remote registration. • Gather information of IP phone, including Vendor, Model, and MAC address.

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Click **+Add > Add**.
3. In the **IP Phone** section, enter the phone's information:



   - **Vendor**: Select a phone vendor.
   - **Model**: Select a phone model.
   - **MAC Address**: Enter MAC address of the phone.
4. In the **Options** section, configure the following settings:



   - **Template**: Select a desired template for the phone from the drop-down list.
   - **Provisioning Method**: Select a desired provisioning method.

A provisioning server URL is generated accordingly and displayed on the **Provisioning Link** field.

- **Hot Desking Phone**: Enable the option to set the phone as a hot desking phone.

  The phone is automatically assigned to a virtual extension named HostExt*{virtual_num}*.

5. Click **Save**.
6. Reboot the IP phone manually.

Result

The phone is connected to the PBX and set as a hot desking phone with the virtual extension registered. You can check the registration status from the phone list; The PBX system automatically assigns a **Guest In** key to the phone.

Note:
Users can only use the phone with virtual extension registered to make emergency calls. To use the phone for regular calling, users must either dial the **Guest In** feature code or press the **Guest In** BLF key to log in the phone.

What to do next

- Enable Hot Desking for an Extension User
- (Optional) Retain Configurations for Hot Desking Phones

Related information

IP Phone Configuration Guide

Enable Hot Desking for an Extension User

This topic describes how to enable hot desking for an extension user, so that the user can log in and use a hot desking phone with his or her own extension number.

Procedure

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click beside the desired extension, then click the **Features** tab.
3. Scroll down to the **Hot Desking** section, then turn on the switch.

4. Configure the following settings according to your needs.

Setting	Description
Log Out of Queue	Decide whether to automatically log out the dynamic agent from a queue. If enabled, the system will automatically log the extension user out of the queue when the user logs out of a hot desking phone.
Automatic Guest Out	Decide whether to automatically log out the extension user from a hot desking phone: • **Never**: Disable automatic logout. • **After**: Specify a time period to log the user out of a hot desking phone since the extension user logs in. • **At Daily**: Specify a fixed time to log the user out of a hot desking phone every day.

5. Click **Save** and **Apply**.

Related information

Log in to a Hot Desking Phone
Log out of a Hot Desking Phone
Manage Hot Desking feature

Retain Configurations for Hot Desking Phones

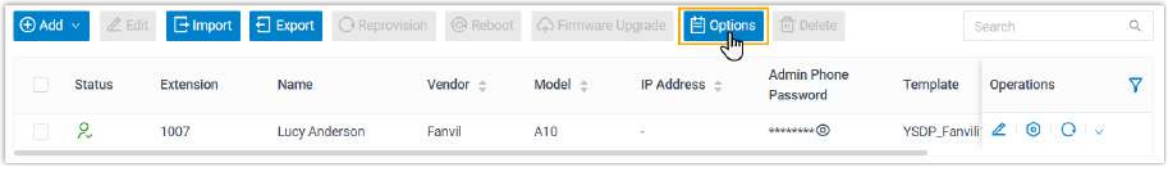
This topic describes how to configure retention of specific phone configurations on hot desking phones after guests log out.

Requirements

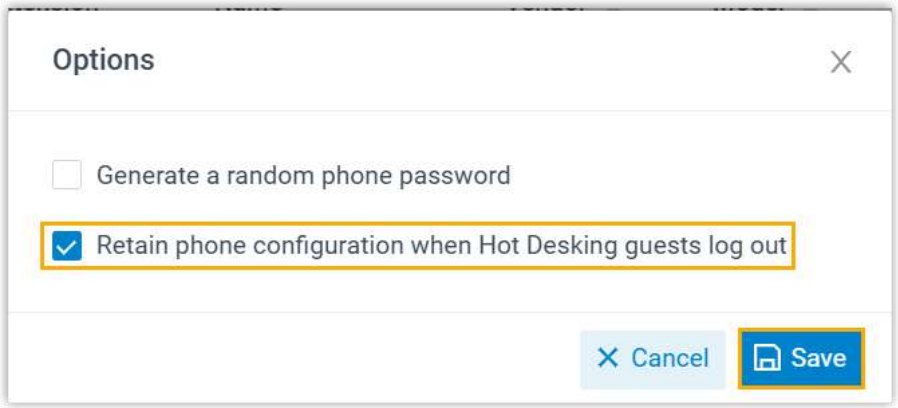
The firmware of Yeastar P-Series Software Edition is 83.19.0.70 or later.

Procedure

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. At the top of the list, click **Options**.



3. In the pop-up window, select the checkbox of **Retain phone configuration when Hot Desking guests log out**, then click **Save**.

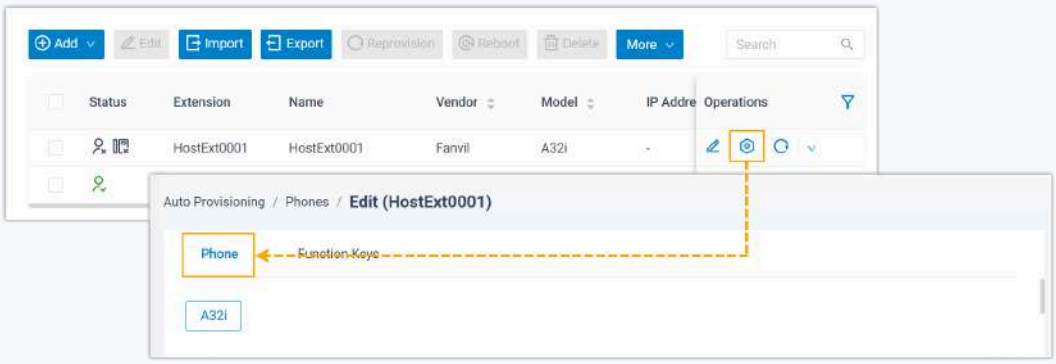


Result

When an extension user logs out of a Hot Desking phone, the general phone configurations will be retained.

Note:

- Only the general configurations will be retained (such as language, signal tones, distinctive ringtone, codecs, etc.), which are configured in the **Auto Provisioning > Phones >** ⚙ **> Phone**.



- The extension registration-related configurations, LDAP directory settings, and function key settings will be cleared.

Use Hot Desking

Log in to a Hot Desking Phone

This topic describes how extension users can log in to a hot desking phone.

Prerequisites

- You have set up a hot desking phone.
- You have enabled hot desking feature for desired extension users.
- If the users have their own phones, and may occasionally log in to a hot desking phone, you need to set concurrent registrations.

Procedure

Extension users can log in to a hot desking phone via either of the following methods:

Method	Instruction
Dial a feature code to log in	1. On a hot desking phone, dial the **Guest In** feature code. **Note:** The default **Guest In** feature code is `*84`. You can customize the feature code on **Call Features > Feature Code > Hot Desking > Guest In**. 2. Follow the voice prompt, enter the extension number followed by the `#` key (e.g. 2000#).

Method	Instruction
	3. Follow the voice prompt, enter the voicemail PIN followed by the # key (e.g. 8471#).
Press a BLF key to log in	After you set up a hot desking phone, the system automatically assigns a **Guest In** key to the phone, extension users can press the key to log in to the phone. 1. On a hot desking phone, press the **Guest In** key. 2. Follow the voice prompt, enter the extension number followed by the # key (e.g. 2000#). 3. Follow the voice prompt, enter the voicemail PIN followed by the # key (e.g. 8471#). **Troubleshooting:** If a user failed to log in to the hot desking phone by pressing the **Guest In** key, you can check if the **Guest In** feature code has been changed (Path: **Call Features > Feature Code > Hot Desking > Guest In**).

Result

- The user's extension configurations, including extension information and function key settings, are loaded onto the phone; The system automatically assigns a **Guest Out** key to the phone.
- The extension user can use the phone with his or her extension and implement the followings:
  - Make calls from the phone.
  - Receive calls on the phone.
  - Use the function keys of the extension.
  - Query contacts that are stored in the PBX on the IP phone via LDAP.

    Note:
    This requires you to configure the LDAP directory settings for the phone on **Auto Provisioning > Phones >** **> LDAP Directory**. For more information about the settings, see Auto Provision LDAP for IP Phones.
- You can monitor the hot desking phone status, and know who is working on the hot desking phone on **Auto Provisioning > Phones**.

Related information

[Log out of a Hot Desking Phone]

Log out of a Hot Desking Phone

This topic describes how extension users can log out of a hot desking phone.

Procedure

Extension users can log out of a hot desking phone using either of the following methods:

Method	Instruction
Dial a feature code to log out	On a hot desking phone, dial the **Guest Out** feature code. **Note:** The default **Guest Out** feature code is *084. If you want to customize the feature code, go to **Call Features > Feature Code > Hot Desking > Guest Out**.
Press a BLF key to log out	The system automatically assigns a **Guest Out** key to a hot desking phone when a user logged in. The user can press the key on the phone to quickly log out. **Troubleshooting:** If a user failed to log out by pressing the **Guest Out** key, you need to check if the **Guest Out** feature code has been changed (Path: **Call Features > Feature Code > Hot Desking > Guest Out**).

Result

The user's extension is logged out of the phone; the phone is reverted to the default settings and can only be used to make emergency calls.

Important:
The call logs are kept on the hot desking phone, the user needs to manually clear the data if necessary.

Note:

- If you have set up the system to retain configurations for hot desking phones, the general phone configurations (such as language, signal tones, distinctive ringtone, codecs, etc.) will be retained, which are configured in the **Auto Provisioning > Phones >** **> Phone**; while the extension registration-related configurations, LDAP directory settings, and function key settings will be cleared.
- If a user forgot to log out, after another user logs in to the hot desking phone, the previous user would be logged out automatically, or you can forcibly log the user out of the phone on PBX web portal.

Related information

Log in to a Hot Desking Phone

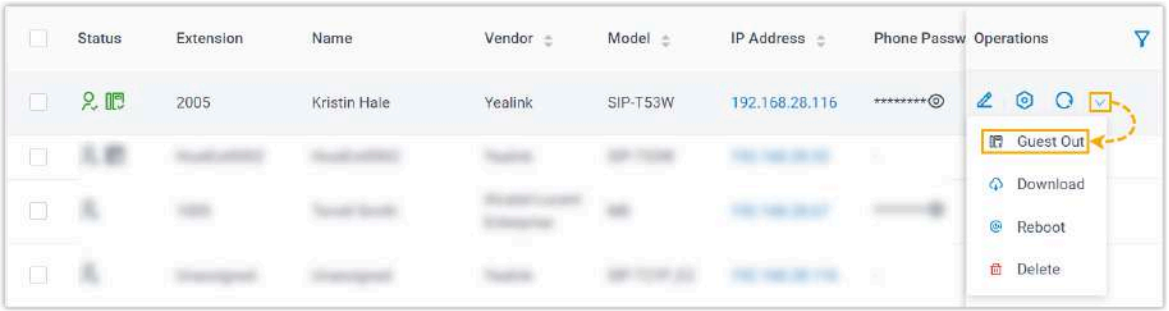
Manage Hot Desking feature

This topic describes how to manage the hot desking feature on PBX web portal, including forcibly log out a user, and disable hot desking for an extension user.

Forcibly log a user out of a hot desking phone

In case an extension user forgot to log out of a hot desking phone, you can forcibly log his or her extension out on PBX web portal, so as to prevent information disclosure or misuse of the extension.

1. Log in to PBX web portal, go to **Auto Provisioning > Phones**.
2. Hover your mouse over beside the desired phone, and click **Guest Out**.

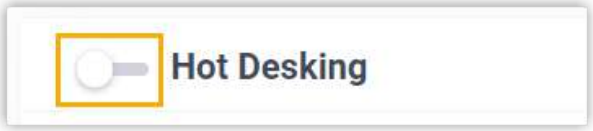


3. In the pop-up window, click **Confirm**.

The user is logged out of the hot desking phone.

Disable Hot Desking for an extension user

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click beside the desired extension, then click the **Features** tab.
3. Scroll down to the **Hot Desking** section, then turn off the switch.



4. Click **Save** and **Apply**.

   The extension user will not be able to log in to a hot desking phone.

Busy Camp-on

Camp on to a Busy Extension

Busy Camp-on feature allows a caller to place a call reservation when he or she makes a call to an extension and receives a busy signal. The PBX will automatically call the caller back as soon as the called extension becomes available.

Restrictions

- The Busy Camp-on feature is only applicable for the calls between extensions.
- The timeout for a Busy Camp-on request is **3600** seconds. This means that the PBX will not call the caller back if the called party is still unavailable 1 hour after the request is initiated.
- A maximum of **10** Busy Camp-on requests is available for each extension. If exceeds, the PBX will cancel the earliest requests.

Procedure

Assume that extension 1000 makes a call to extension 2000, but extension 2000 is in a call.

In this case, extension 1000 can hang up the call and camp on to extension 2000 by dialing a feature code. The PBX will call extension 1000 back and connect it to extension 2000 as soon as extension 2000 becomes available.

1. Extension 1000 dials *792000 to camp on to extension 2000.

   > **Tip:**
   > The default feature code for enabling Busy Camp-on is `*79`. You can change, enable, or disable the code on PBX web portal: **Call Features > Feature Code > Busy Camp-on > Enable Busy Camp-on**.

   A prompt "The Busy Camp-on has been enabled" is played and the call is hung up automatically.
2. As soon as extension 2000 becomes available, the PBX will call extension 1000.

   Extension 1000 receives an incoming call pop-up with caller ID displayed as **Busy Camp-on** ***{name_of_called_extension}{number_of_called_extension}*** and will hear a prompt "This call is connected via Busy Camp-on feature" after answering the call.
3. The PBX calls extension 2000.

   After extension 2000 answers the call, extension 2000 and extension 1000 are connected.

Cancel Busy Camp-on Requests

If extension users are not available to accept the automatic callback, they can cancel Busy Camp-on requests as shown in the topic.

> **Note:**
> We recommend that extension users think twice before proceeding, as this will cancel all the Busy Camp-on requests that they have initiated.

Procedure

Extension user dials *079 on the phone to cancel all the Busy Camp-on requests that he or she has initiated.

> **Tip:**
> The default feature code for disabling Busy Camp-on is `*079`. You can change, enable, or disable the code on PBX web portal: **Call Features > Feature Code > Busy Camp-on > Disable Busy Camp-on**.

Result

- A prompt "The Busy Camp-on has been disabled" is played and the call is hung up automatically.
- All Busy Camp-on requests from the extension user are cancelled.

Fax

Fax Overview

Yeastar P-Series 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.

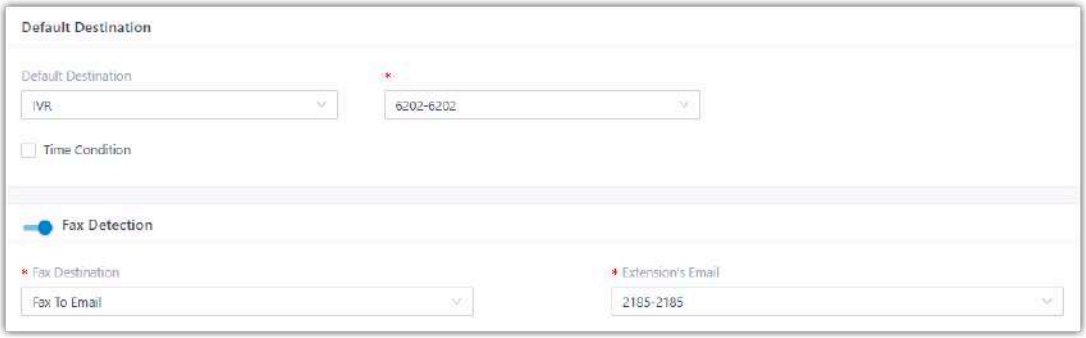
Prerequisites

- 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.

3. If you receive faxes through a shared line, go to **Fax Detection** section.
   a. In the **Fax Destination** drop-down list, select **Fax To Email**.
   b. In the **Extension's Email** drop-down list, select an extension user to receive faxes by email.



4. Click **Save** and **Apply**.

Result

When receiving a fax, PBX converts the received fax and simply forwards it to the email address as an PDF attachment.

Set up Fax over IP (FoIP)

Fax over IP (FoIP) is the process of using T.38 protocol to send a fax from a fax machine to another fax machine over the Internet. This topic describes how to enable T.38 for extension and trunk respectively, and how to change T.38 settings to improve the Fax transmission over VoIP network.

Enable T.38 protocol for SIP extension

If you want to register a SIP extension on a SIP compatible fax machine, you need to enable **T.38 Support** for this extension.

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**, edit the desired extension.
2. Go to **Advanced > VoIP Settings**.
3. Select the checkbox of **T.38 Support**.
4. Click **Save** and **Apply**.

Enable T.38 protocol for SIP trunk

If you want to use a SIP trunk to send or receive faxes, you need to enable **T.38 Support** for this trunk.

1. Log in to PBX web portal, go to **Extension and Trunk > Trunk**, edit the desired trunk.
2. Go to **Advanced > VoIP Settings**.
3. Select the checkbox of **T.38 Support**.
4. Click **Save** and **Apply**.

Change T.38 settings

If the Fax over IP doesn't work, you can change the T.38 settings.

1. Log in to PBX web portal, go to **PBX Settings > SIP Settings > T.38**.
2. Change the T.38 settings.

- **T.38 Max BitRate**: Set the maximum bit rate of the fax transmission.
- **No T.38 Attributes in re-INVITE SDP**: If enabled, SDP re-invite packet does not contain T.38 attributes.
- **Error Correction Mode**: If enabled, after receiving the packet for a complete fax page, PBX notifies the transmitting fax machine of the frames with errors. The transmitting fax machine then retransmits the specified frames.

  This process is repeated until all frames are received without errors.

3. Click **Save** and **Apply**.

Paging/Intercom

Overview of Paging and Intercom

This topic describes what is Paging and Intercom, scheduled paging call and intercom call.

What is Paging and Intercom

Yeastar P-Series 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

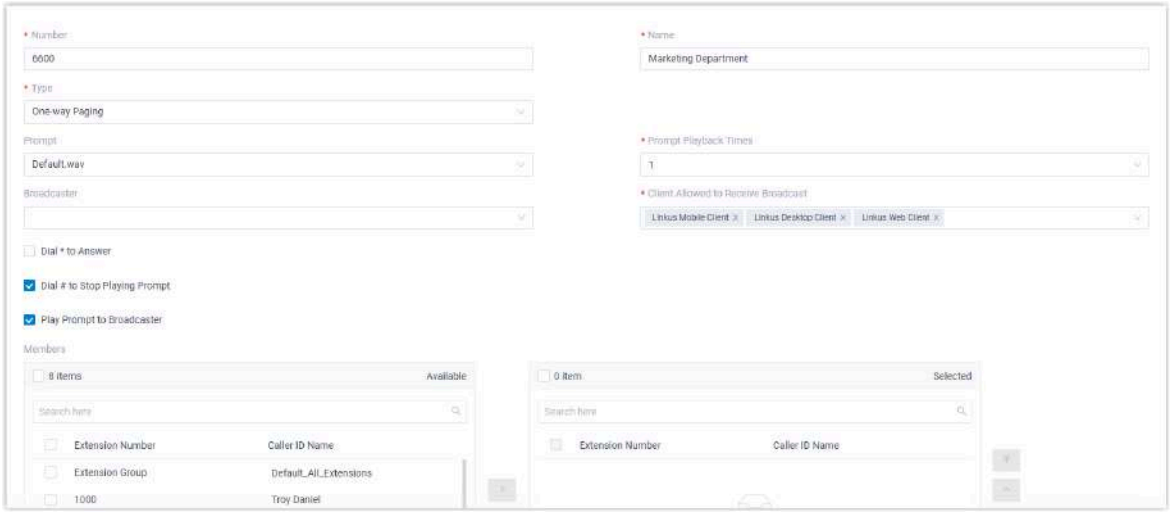
One-way Paging feature allows a broadcaster to make an announcement to users. The called parties' phones will not ring, but instead directly answering into speakerphone mode. This topic describes how to set up a one-way paging group.

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.



Item	Description
Number	Enter a number for the paging group. In this example, enter *6600*.
Name	Enter a name for the paging group. In this example, enter *Marketing Department*.
Type	Select **One-way Paging**.
Prompt	Optional. To play a prompt before making an announcement, you can select a custom prompt. In this example, select **Default.wav**. **Note:** To customize a prompt, see Record a Custom Prompt or Upload a Custom Prompt.
Prompt Playback Times	Specify how many times the prompt will be played and repeated. **Note:** Enter a value between 1 and 100, or select **Unlimited** to play the prompt in a loop.
Broadcaster	Optional. To restrict users from making an announcement to the paging group, select allowed extensions or extension

Item	Description
	groups from the drop-down list. In this example, leave it blank.
Client Allowed to Receive Broadcast	Select the desired clients for receiving broadcasts.
Dial * to Answer	Optional. To allow users to dial `*` to talk to the broadcaster privately, enable this option. In this example, keep the option disabled. **Note:** When a user dials `*`, announcement will terminate, and the user can have a private talk with the broadcaster.
Dial # to Stop Playing Prompt	Optional. If a prompt is selected, enabling this option allows the broadcaster to dial # during playback to stop the prompt.
Play Prompt to Broadcaster	Optional. To restrict the broadcaster from hearing the prompt, disable this option. In this example, disable this option. **Note:** This option is available only when a custom prompt is selected and is enabled by default.
Members	Select desired members from **Available** box to **Selected** box. In this example, select **Marketing Department**.

3. Click **Save** and **Apply**.

What to do next

When dialing the number of the paging group, the selected members will receive broadcast through the client(s) you have specified.

- For Linkus clients (Mobile/Desktop/Web), they will ring first, and users need to manually answer the call to listen to the broadcasts.

  Note:
  If necessary, you can set up user's Linkus clients to automatically answer paging calls. For more information, see Set up Auto Answer for Linkus UC Clients.

- For IP phones, they will automatically answer into speakerphone mode and play the broadcasts.

Related information

Schedule a Paging Call or an Intercom Call

Set up a One-way Multicast Paging Group

One-way Multicast Paging feature allows a broadcaster to make an announcement to the users who are listening to a specific multicast group on a specific channel. The called parties' phones will not ring, but instead directly answering into speakerphone mode. This topic describes how to set up a one-way multicast paging group.

Scenario

For a warehouse, the work flow in product line is closely connected and tends to be complex. For example, one zone is responsible for packaging goods, another zone is for dispatching goods. To facilitate supervisors in coordinating daily warehouse activities, you can set up paging groups for each zone.

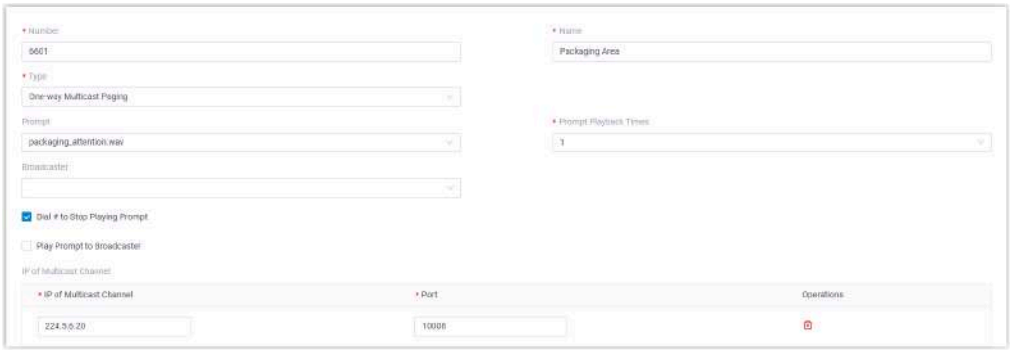
Requirements

The phone that will receive One-way Multicast Paging must support Multicast Paging feature, and is on the same local subnet as the PBX.

Procedure

Based on the above scenario, you need to create two paging groups on the PBX and set up multicast listening on two phones.

1. On Yeastar P-Series 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.



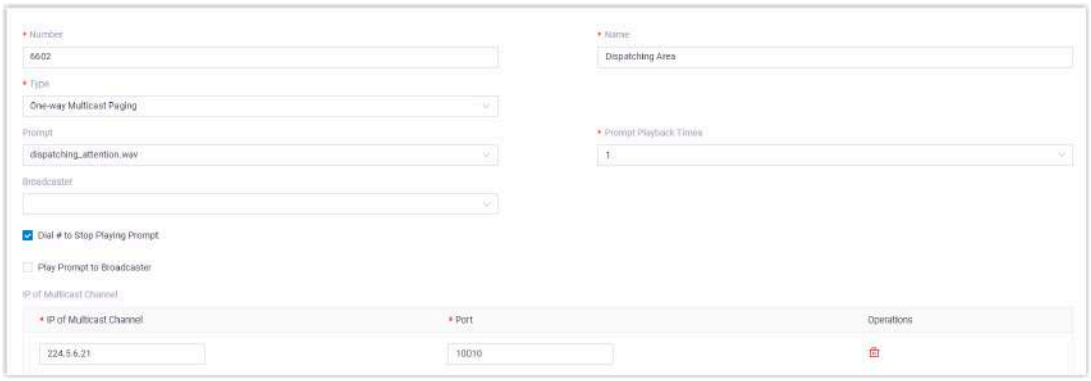
Item	Description
Number	Enter a number for the paging group. In this example, enter *6601*.
Name	Enter a name for the paging group. In this example, enter *Packaging Area*.
Type	Select **One-way Multicast Paging**.
Prompt	Optional. To play a prompt before making an announcement, you can select a custom prompt. In this example, select **packaging_attention.wav**. **Note:** To customize a prompt, see Record a Custom Prompt or Upload a Custom Prompt.
Prompt Playback Times	Specify how many times the prompt will be played and repeated. **Note:** Enter a value between 1 and 100, or select **Unlimited** to play the prompt in a loop.
Broadcaster	Optional. To restrict users from making an announcement to the paging group, select allowed extensions or extension groups from the drop-down list. In this example, leave it blank.
Dial # to Stop Playing Prompt	Optional. If a prompt is selected, enabling this option allows the broadcaster to dial # during playback to stop the prompt.
Play Prompt to Broadcaster	Optional. To restrict the broadcaster from hearing the prompt, disable this option. In this example, disable this option. **Note:** This option is available only when a custom prompt is selected and is enabled by default.
IP of Multicast Channel	Enter a multicast IP address and port. • **IP of Multicast Channel**: Enter a multicast IP address. In this example, enter *224.5.6.20*. • **Port**: Enter a multicast port. In this example, enter *10008*. **Note:**

Item	Description
	• The range of multicast IP address is 224.0.0.0 - 239.255.255.255. • You can add at most 30 IP addresses.

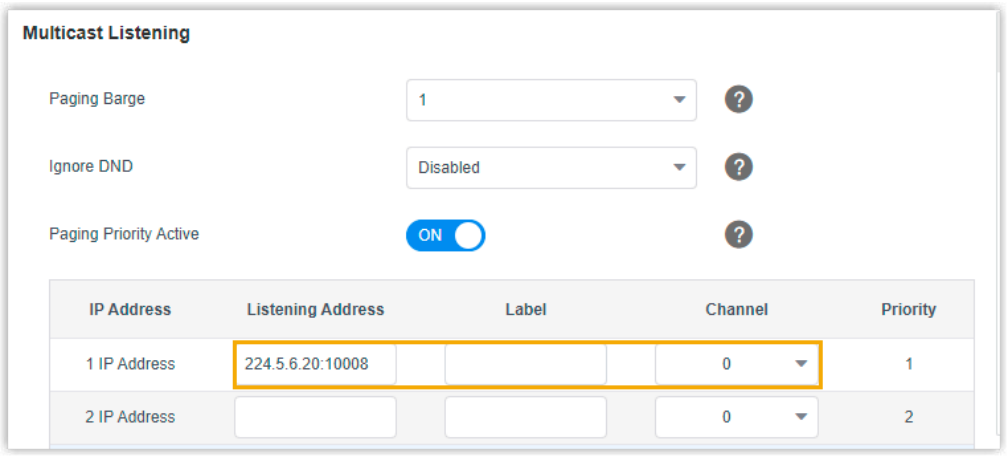
iii. Click **Save** and **Apply**.

b. Repeat step **a** to create another paging group 6602 for Dispatching Area.

> **Note:**
> Set a multicast IP address and port that are different from Packaging Area. For example, set **IP of Multicast Channel** to *224.5.6.21* and set **Port** to *10010*.



2. Set up multicast listening for the two phones in Packaging Area and Dispatching Area.
   a. Set up multicast listening for the phone in Packaging Area. In this example, we take Yealink T56A as an example.
      i. Log in to the phone web interface, go to **Directory > Multicast IP**.
      ii. In the **Listening Address** field, enter the same multicast IP address and port as the PBX. In this example, enter *224.5.6.20:10008*.

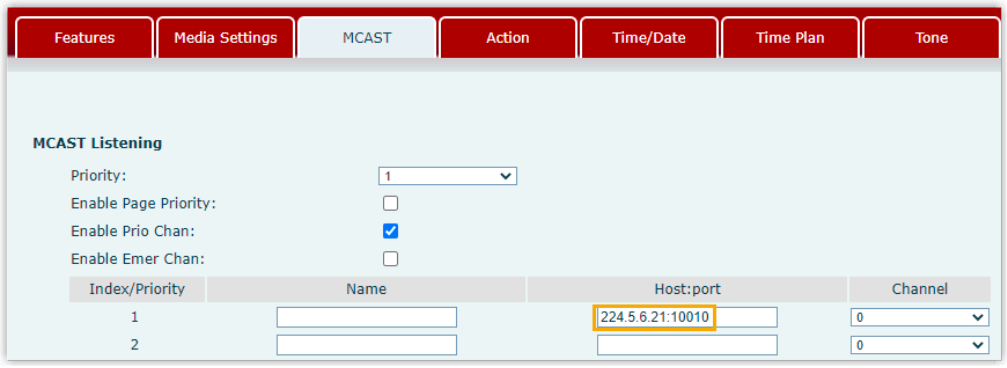


iii. Click **Confirm**.

b. Set up multicast listening for the phone in Dispatching Area. In this example, we take Fanvil X210 as an example.

i. Log in to the phone web interface, go to **Phone Settings > MCAST**.

ii. In the **Host:Port** field, enter the same multicast IP address and port as the PBX. In this example, enter *224.5.6.21:10010*.



iii. Click **Apply**.

What to do next

- Supervisor dials `6601` to reach employees in Packaging Area. Yealink T56A automatically answers into speakerphone mode.
- Supervisor dials `6602` to reach employees in Dispatching Area. Fanvil X210 automatically answers into speakerphone mode.

Related information

Schedule a Paging Call or an Intercom Call

Set up a Two-way Intercom Group

Two-way Intercom feature allows you to establish two-way communication with an individual user or a group of users. The called parties can respond without picking up the handset. This topic describes how to set up a two-way intercom group.

Background information

In office complexes, hospitals, or schools, there are either static guards or patrol guards to ensure safety within the workplace. The Two-way Intercom feature helps improve communication efficiency. For example, a security guard can ask for help when security incidents happen, a supervisor can flexibly dispatch employees in daily activities.

Yeastar P-Series 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**.

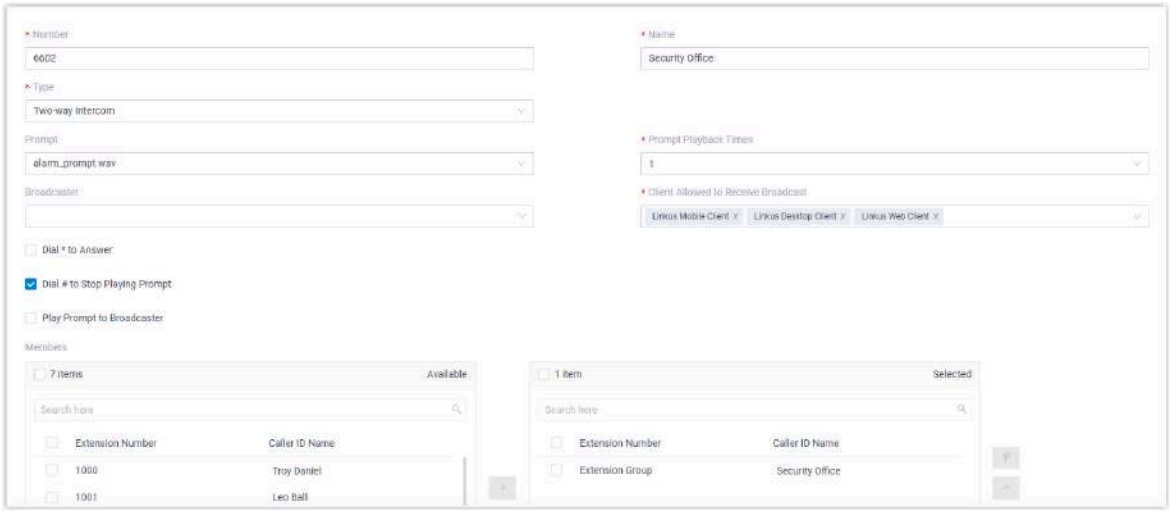
Place an intercom call to multiple users

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.



Item	Description
Number	Enter a number for the intercom group. In this example, enter *6602*.
Name	Enter a name for the intercom group. In this example, enter *Security Office*.
Type	Select **Two-way Intercom**.
Prompt	Optional. To play a prompt before making an announcement, you can select a custom prompt. In this example, select **alarm_prompt.wav**. **Note:** To customize a prompt, see Record a Custom Prompt or Upload a Custom Prompt.
Prompt Playback Times	Specify how many times the prompt will be played and repeated. **Note:** Enter a value between 1 and 100, or select **Unlimited** to play the prompt in a loop.
Broadcaster	Optional. To restrict users from placing an intercom call to the intercom group, select allowed extensions or extension groups from the drop-down list. In this example, leave it blank.
Client Allowed to Receive Broadcast	Select the desired clients for receiving intercom calls. **Note:**

Item	Description
	Intercom calls initiated by the feature code will NOT be restricted by this configuration and will call all the clients and extension endpoints of members simultaneously.
Dial * to Answer	Optional. To allow users to dial `*` to talk to the broadcaster privately, enable this option. When a user dials `*`, the call is ended from other users' side, and the user can have a private talk with the broadcaster.
Dial # to Stop Playing Prompt	Optional. If a prompt is selected, enabling this option allows the broadcaster to dial # during playback to stop the prompt.
Play Prompt to Broadcaster	Optional. To restrict the broadcaster from hearing the prompt, disable this option. In this example, disable this option. **Note:** This option is available only when a custom prompt is selected and is enabled by default.
Members	Select desired members from **Available** box to **Selected** box. In this example, select the group *Security Office*.

3. Click **Save** and **Apply**.

What to do next

When dialing the number of the intercom group, the selected members will receive the call through the client(s) you have specified.

- For Linkus clients (Mobile/Desktop/Web), they will ring first, and users need to manually answer the call to listen to the broadcasts.

  Note:
  If necessary, you can set up user's Linkus clients to automatically answer paging calls. For more information, see Set up Auto Answer for Linkus UC Clients.

- For IP phones, they will automatically answer into speakerphone mode.

Related information

Schedule a Paging Call or an Intercom Call

Manage Paging Groups and Intercom Groups

This topic describes how to edit or delete paging groups and intercom groups.

Edit a paging/intercom group

1. Log in to PBX web portal, go to **Call Features > Paging/Intercom**.
2. On **Paging/Intercom List** page, click beside desired group.
3. Edit group settings.
4. Click **Save** and **Apply**.

Delete a paging/intercom group

1. Log in to PBX web portal, go to **Call Features > Paging/Intercom**.
2. On **Paging/Intercom List** page, click beside desired group.
3. Click **OK** and **Apply**.

> **Note:**
> If you have scheduled a paging call or an intercom call for the group, the scheduled call will also be deleted.

Scheduled Paging/Intercom Call

Schedule a Paging Call or an Intercom Call

A scheduled paging call or intercom call allows Yeastar P-Series 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:

Item	Description
Paging	Select a pre-configured paging group from the drop-down list.
Caller	Select a broadcaster. • *{extension_user}*: The extension user will make the announcement. On the specified date and time, the PBX will place a call to the user. When the user answers the call, group members' phones directly answer into speakerphone mode. **Note:** If the user rejects the call, the announcement will be cancelled. • **None**: The PBX will make the announcement. On the specified date and time, the PBX will place a call to group members and play a specific custom prompt. After the prompt ends, the PBX hangs up. The option can be applied to school bells, church bells, etc. **Note:** The option is available only when a custom prompt is assigned to the selected paging group or intercom group.
Start Date	Set the start date of the scheduled paging call or intercom call.
Time	Set the start time of the scheduled paging call or intercom call. **Note:** You can set up to 8 timings, which means that the paging call or intercom call can be placed at different time on the same day.
Days of Week	Select the days of week. The scheduled paging call or intercom call will be weekly placed on the specified days of week.

   c. Click **Save** and **Apply**.

Manage Scheduled Paging Calls and Intercom Calls

This topic describes how to edit or delete scheduled paging calls and intercom calls.

Edit a scheduled paging/intercom call

1. Log in to PBX web portal, go to **Call Features > Paging/Intercom**.
2. On **Scheduled Paging/Intercom** page, click beside desired group.
3. Edit relevant settings.
4. Click **Save** and **Apply**.

Delete a scheduled paging/intercom call

1. Log in to PBX web portal, go to **Call Features > Paging/Intercom**.
2. On **Scheduled Paging/Intercom** page, click beside desired group.
3. Click **OK** and **Apply**.

   The announcement will not be made on the specified date and time.

PIN List

Add a PIN List

A PIN list allows you to define groups and then assign a list of passwords to each group. The PIN list can be used to restrict outbound routes to enhance communication security. Users need to enter a correct PIN code when making outbound calls through a restricted outbound route.

Procedure

1. Log in to PBX web portal, go to **Call Features > PIN List**, click **Add**.
2. In the pop-up window, configure the following settings:
   - **Name**: Specify a name to help you identify it.
   - **PIN List**: Enter the PIN codes. Press the **Enter** key to separate multiple PIN codes.

     Note:

> ◦ The PIN code only allows numeric value.
> ◦ The length of each PIN code is limited from 3 to 15.

- **Record in CDR**: Whether to record the PIN code in CDR when the PIN code has been used.

3. Click **Save**.

What to do next

1. Assign the PIN codes included in the PIN list to different users.
2. Select a PIN list in an outbound route to restrict outbound calls.

Call Disposition

Add Disposition Codes

Call Disposition feature allows you to define disposition code for call outcomes with custom labels and brief descriptions, which can be used to categorize and track business calls effectively. This topic describes how to add one or more disposition codes.

Requirements

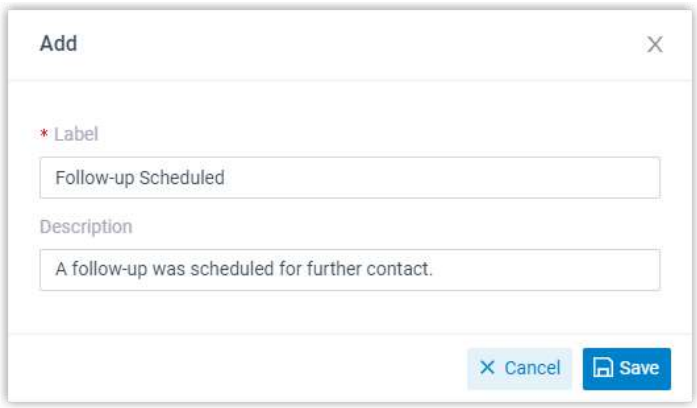
The firmware of Yeastar P-Series Software Edition is 83.18.0.59.

Limitations

Maximum Number of Extensions (N)	N ≤ 500	N > 500
Number of call disposition codes	20	30

Procedure

1. Log in to PBX web portal, go to **Call Features > Call Disposition**.
2. Click **Add**.
3. In the pop-up window, complete the following settings.



- **Label**: Enter a name to quickly identify the outcome of a call.
- **Description**: Optional. Enter a detailed explanation for the label.

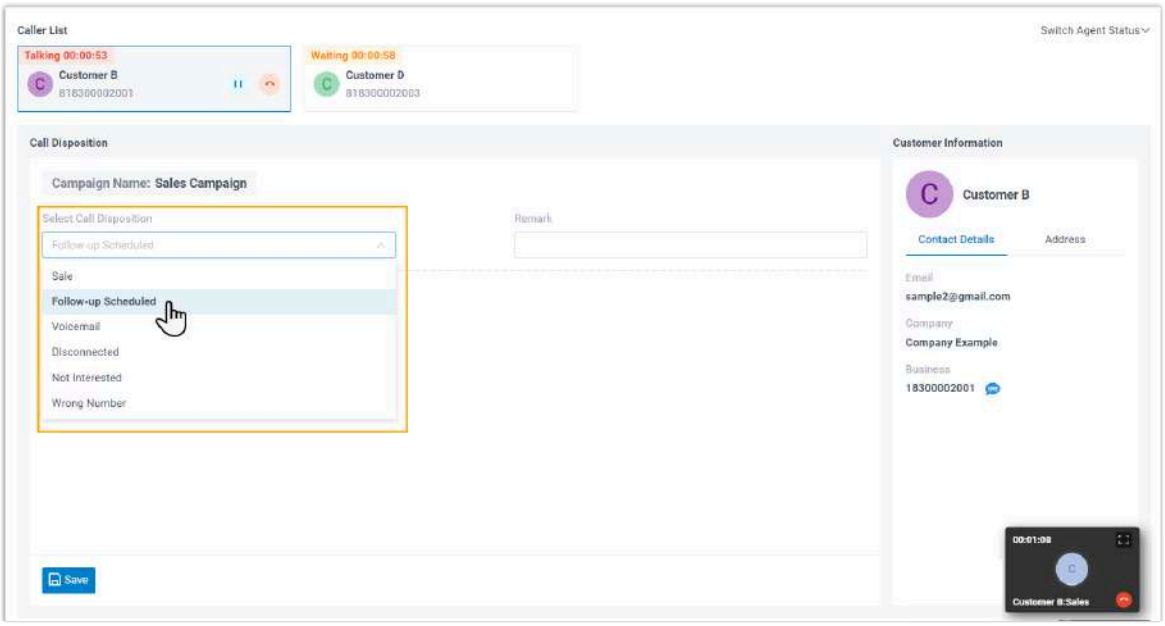
4. Click **Save**.
5. Repeat step **2** - **4** to add more disposition codes as needed.

Result

- Extension users can conveniently select these pre-defined codes when using call notes to mark and categorize their calls.

> **Note:**
> To achieve this, you need to allow users to use the call note feature. For more information, see Allow Users to Add Notes to Calls.

- For outbound call center, when agents handle outbound campaign calls on Inbox, they can quickly mark and categorize campaign calls with these pre-defined codes. For more information, see Handle Campaign Calls on Linkus Web Client and Handle Campaign Calls on Linkus Desktop Client.



Call Note

Allow Users to Add Notes to Calls

Call Note feature allows users to add tags and remarks to calls, capturing essential information or decisions made during the conversations. The call notes help users to keep track of calls, making it easier to reference information later or share it with others. This topic describes how to configure the call scenarios where users are allowed to add call notes.

Requirements

The firmware version of Yeastar P-Series Software Edition is 83.18.0.102 or later.

Procedure

1. Log in to PBX web portal, go to **PBX Settings > Preferences**.
2. Turn on the switch of **Call Note**.
3. Specify the call scenarios where users can add notes to calls.

Settings	Description
Calls from Queue	If enabled, inbound queue agents can access the call note feature to add tags and remarks during queue calls or in the

Settings	Description
	wrap-up time, and review or edit the call notes later in the corresponding call logs.
Calls from Ring Group	If enabled, ring group members can access the call note feature to add tags and remarks during ring group calls, and review or edit the call notes later in the corresponding call logs.
Calls to Voicemail	If enabled, extension users can access the call note feature to add tags and remarks to the calls that were sent to their extension's voicemails in the corresponding call log. **Note:** For calls sent to group voicemails, only administrators can add and edit call notes for the corresponding calls in the call detail records (CDR).
Calls to Extensions	If enabled, extension users can access the call note feature to add tags and remarks during the calls they receive, and review or edit the call notes later in the corresponding call logs.
Outbound Calls	If enabled, extension users can access the call note feature to add tags and remarks during outbound calls they initiate, and review or edit the call notes later in the corresponding call logs.

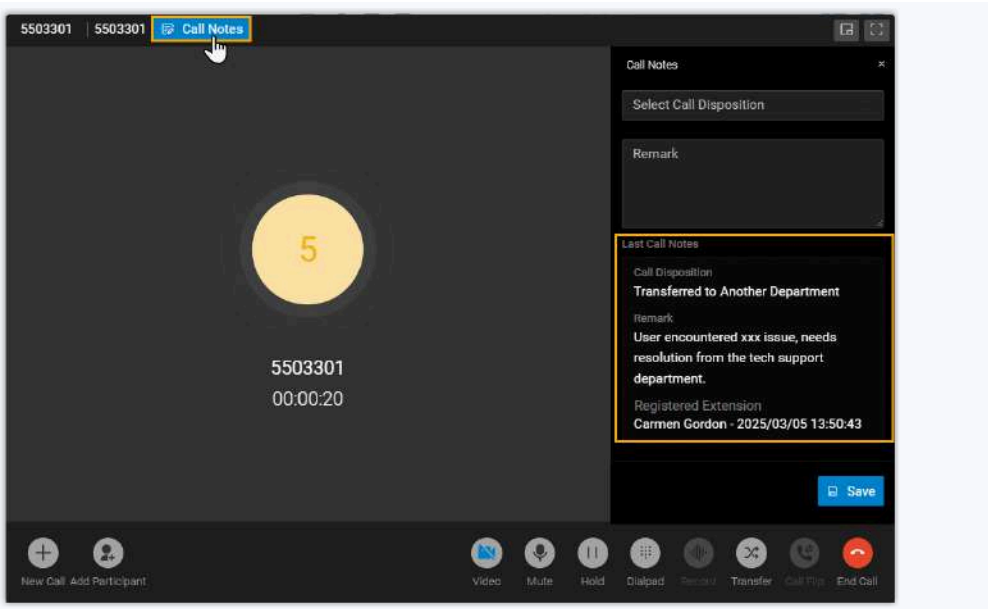
4. Click **Save**.

Result

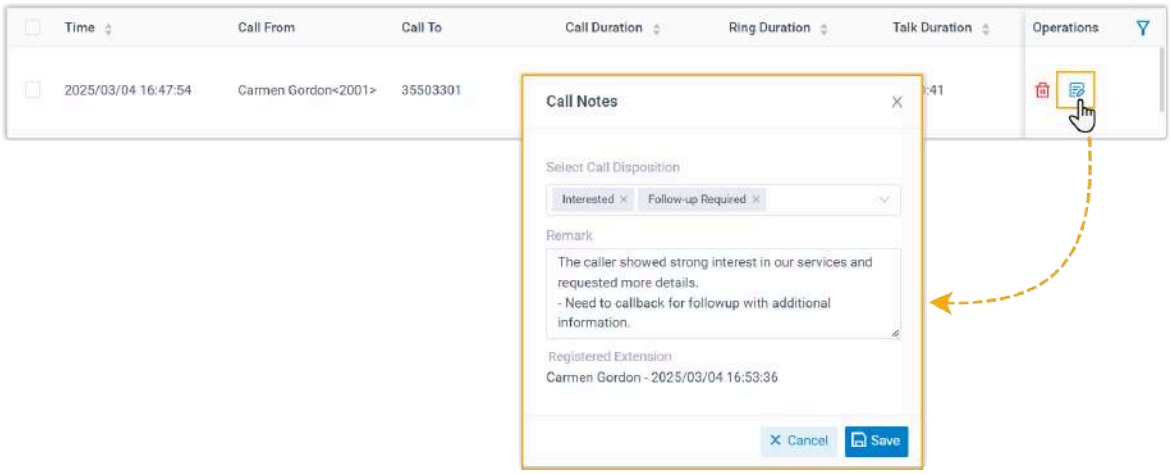
- The call note feature is enabled. During an active call on Linkus Clients, users can conveniently select pre-defined disposition codes as call tags, and add remarks for the call to note down essential information.

Note:

- To ensure that users can select pre-defined codes in call notes, you MUST configure the disposition codes in advance. For more information, see Add Disposition Codes.
- If a call is transferred to another user with access to the call note feature, he or she will be able to view the previous call notes after answering the call.



- You can review the call notes for calls in CDR, and edit the notes if necessary.



Blocked/Allowed Numbers

Block Calls To or From a Phone Number

Yeastar P-Series 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.

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

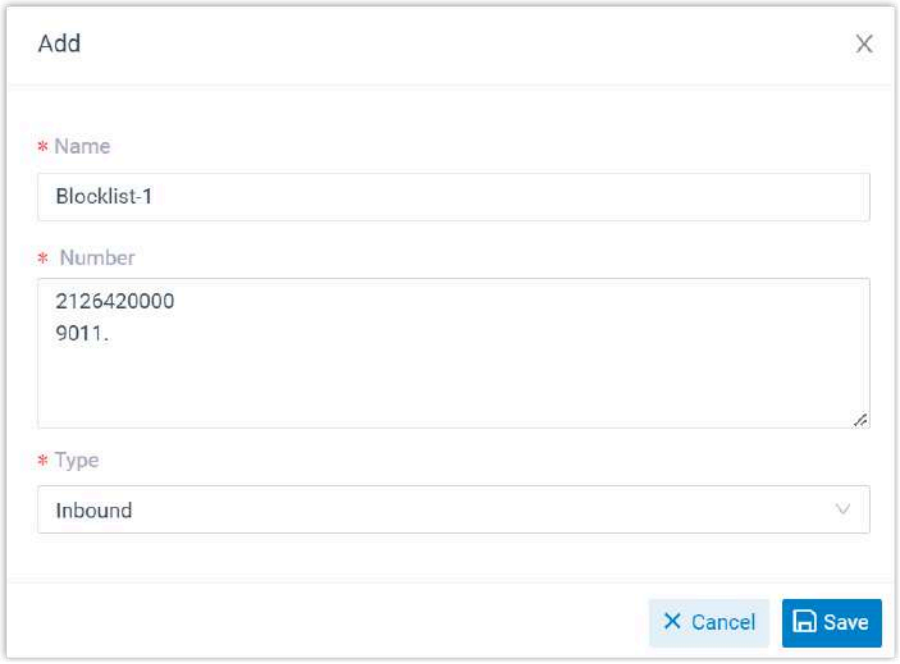
This feature makes it possible for blocking inbound and/or outbound calls to external users by phone number. If you list a phone number in the system blocklist, all the PBX extensions can NOT reach or be reached by the phone number.

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:



   - **Name**: Enter a name to help you identify the number(s) to be blocked.
   - **Number**: Enter a specific number or a number pattern per line.
     - To block a specific number, enter a specific number. For example, enter `2126420000`.
     - To block a range of numbers, enter a wildcard pattern. For example. enter `9011.` to block numbers starting with 9011.

       For more information about wildcard pattern, see DID Pattern and Caller ID Pattern.
   - **Type**: Select a type from the drop-down list.
     - **Inbound**: Block the number(s) from calling into the PBX.
     - **Outbound**: Block PBX extensions from calling the number(s).
     - **Both**: Block the number(s) from calling into the PBX and block the PBX extensions from calling the number(s).
4. Click **Save** and **Apply**.

Result

The blocked numbers list is displayed on the web page as the following figure shows. The added numbers will be blocked based on the type you selected.

Export and Import Blocked Numbers

The blocked numbers added on Yeastar P-Series 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:
   a. Select the checkbox of a desired list, then click  .
   b. In the pop-up window, click **OK**.
3. To bulk delete blocked numbers lists, do as follows:

a. Select the checkboxes of desired lists, then click **Delete**.
b. In the pop-up window, click **OK**.

The blocked numbers lists are deleted successfully. All the numbers in the deleted lists are no longer blocked, they can call into the PBX and be called by PBX extension users.

Allow Calls To or From a Phone Number

If trusted phone numbers happen to be listed in system blocklist, you can add the trusted phone numbers to system allowlist. Numbers in the allowlist are allowed to dial in, dial out, or both.

> **Note:**
> The **Allowed Number** has higher priority than the **Blocked Number**; Adding numbers in **Allowed Number** doesn't mean that PBX only allow these numbers to dial in or be dialed out.

Limitations

The maximum number of **Allowed Numbers Lists** and **Numbers per Allowed Numbers List** varies depending on the number of your extensions.

Maximum Number of Extensions (N)	Allowed Numbers Lists	Numbers per Allowed Numbers List
N < 1000	256	100
N ≥1000	512	200

Background information

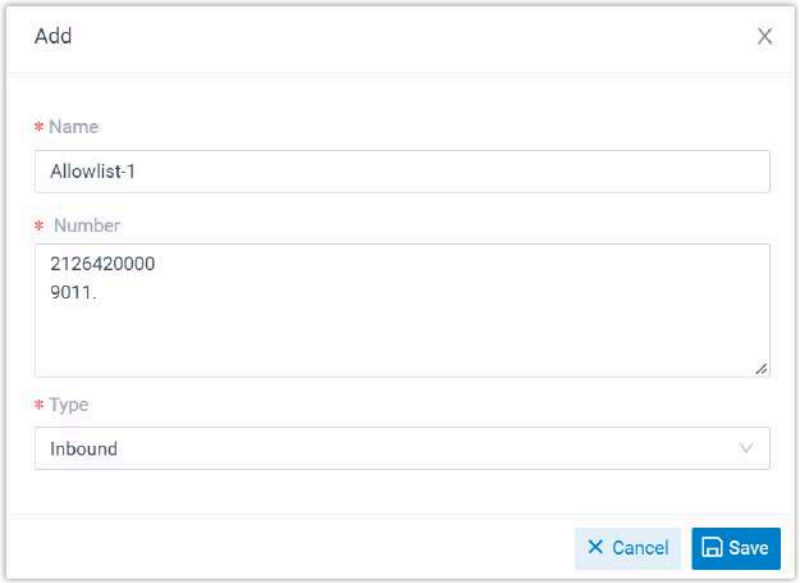
If your customers' phone numbers happen to be listed in system blocklist or individual blocklist, you can add trusted phone numbers to the allowlist.

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:



   - **Name**: Enter a name to help you identify the number(s) to be allowed.
   - **Number**: Enter a specific number or a number pattern per line.
     - To allow a specific number, enter a specific number. For example, enter `2126420000`.
     - To allow a range of numbers, enter a wildcard pattern. For example. enter `9011.` to allow numbers starting with 9011.

       For more information about wildcard pattern, see DID Pattern and Caller ID Pattern.
   - **Type**: Select a type from the drop-down list.
     - **Inbound**: Allow the number(s) to call into the PBX.
     - **Outbound**: Allow PBX extensions to call the number(s).
     - **Both**: Allow the number(s) to call into the PBX and allow PBX extensions to call the number(s).
4. Click **Save** and **Apply**.

Result

The allowed numbers list is displayed on the web page as the following figure shows. The added numbers can communicate with the PBX extensions based on the type you selected.

Export and Import Allowed Numbers

The allowed numbers added on Yeastar P-Series 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.

Messaging

Yeastar P-Series Software Edition Omnichannel Messaging Overview

Yeastar P-Series Software Edition offers omnichannel messaging feature, which allows a business to integrate different messaging channels with the business phone system. In this way, customers are able to reach the business through SMS and social media they prefer, while business agents can centrally receive and respond to customers' queries sent from different messaging channels on their Linkus UC Clients.

Requirements

- **Firmware**: Version 83.12.0.23 or later
- **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP)

Feature highlights

All-in-one Message Inbox

Agents are able to receive and respond to customers' queries from different messaging channels directly on their Linkus UC Clients, greatly saving their time by eliminating the need of switching between apps or services to check for messages. The messages are stored on the PBX server, providing a central record of all the messaging sessions.

Customer Contact using Business Number

Agents can contact customers using a business number, while keeping their own personal mobile number private. If necessary, the messaging session can be easily elevated to a call to reach the customer, so that the agent can resolve issues faster via voice call.

Seamless Collaboration across Agents

Agents can hand off customers' issue to another agent by transferring the conversation, the new agent can quickly review the whole chat history and take over the conversation without hassle.

Automatic Chat Assignment

Route your business messages from different messaging channels to agents, who can share the workload across teams to reduce customer service response time. The system automatically assigns chats to the first agent that picks up the session from the queue.

Configuration guide

For more detailed information and configurations of Omnichannel Messaging, see Omnichannel Messaging Administrator Guide.

PBX System

System Preferences

This topic describes the preference settings that will be applied globally to Yeastar P-Series Software Edition.

Go to **PBX Settings > Preferences** to configure preferences settings.

Basic preferences

Setting	Description
Device Name	Set a name for the PBX. The name will be used as the sender name when PBX sends emails out.
Name Display Format	Set display format for extension user's name and contact's name. • **First Name Last Name with Space Inbetween** • **Last Name First Name with Space Inbetween** • **Last Name First Name without Space Inbetween**
Max Call Duration (s)	Set the global maximum call duration for an active call. When the call duration reaches the limit, the call will be ended. The default value is **10800**. **Note:** For outbound calls, the **Max Call Duration (s)** setting of the caller's extension takes precedence.
Tone Region	Select your country or the nearest neighboring country to enable the default dial tone, busy tone, and ring tone.

Organization Management

Setting	Description
Organization Management	If enabled, you can arrange extension users into organizations.
Company Name	Set your company name, which will be used as the root organization name.

Internal Chat

Setting	Description
Internal Chat	The option is enabled by default. If disabled, extension users will NOT be able to access and use the internal chat feature (Instant Messaging, IM) on their Linkus UC clients. **Note:** The Linkus UC clients that can apply this setting are as listed below: • **Linkus Mobile Client** ◦ Linkus iOS Client: Version 5.2.9 or later ◦ Linkus Android Client: Version 4.13.16 or later • **Linkus Desktop Client** ◦ macOS Desktop: Version 1.2.10 or later ◦ Windows Desktop: Version 1.2.14 or later • **Linkus Web Client**

Distinctive Caller ID Name

Setting	Description
Display Call Feature Name	If enabled, the Caller ID will display the originated name when users receive a call from a ring group, queue, and IVR.
Display DID/DDI Name	If enabled, the Caller ID will display the DID name of the source trunk.

Masked Number

Specify the scenario(s) where external number will be masked. Once enabled, the number displayed in the call window and call logs will be masked.

Note:

- The masking rule applies when receiving and making calls using IP phones, softphones, or Linkus UC Clients. However, when using analog phones, the external numbers will not be masked.
- If the external number is shorter than 6 digits, it will not be masked.

- Callback to a masked number is not allowed.

Setting	Description
Calls initiated via "Open API"	If enabled, destination number will be masked when a third-party application initiates external calls through the API interface.
Calls initiated via "Speed Dial"	If enabled, destination number will be masked when extension users make external calls through Speed Dial.
Calls initiated via "Click to Call"	If enabled, when extension users initiate calls via click-to-call using 'Yeastar Linkus for Google' Chrome extension, destination number will be masked. **Note:** The version of the Chrome extension must be 4.11.1 or later.
Incoming Calls	If enabled, external numbers will be masked when extension users receiving inbound calls.

Call Notes

Specify the call scenarios where call notes can be used to add tags and remarks to calls.

Settings	Description
Calls from Queue	If enabled, inbound queue agents can access the call note feature to add tags and remarks during queue calls or in the wrap-up time, and review or edit the call notes later in the corresponding call logs.
Calls from Ring Group	If enabled, ring group members can access the call note feature to add tags and remarks during ring group calls, and review or edit the call notes later in the corresponding call logs.
Calls to Voicemail	If enabled, extension users can access the call note feature to add tags and remarks to the calls that were sent to their extension's voicemails in the corresponding call log. **Note:** For calls sent to group voicemails, only administrators can add and edit call notes for the corresponding calls in the call detail records (CDR).

Settings	Description
Calls to Extensions	If enabled, extension users can access the call note feature to add tags and remarks during the calls they receive, and review or edit the call notes later in the corresponding call logs.
Outbound Calls	If enabled, extension users can access the call note feature to add tags and remarks during outbound calls they initiate, and review or edit the call notes later in the corresponding call logs.

Presence

Customize presence status to indicate extension users' availability. The presence setting will be synchronized across Linkus UC Clients with the following versions:

- **Linkus iOS Client**: Version 5.15.8 or later
- **Linkus Android Client**: Version 5.15.4 or later
- **Linkus Windows Desktop**: Version 1.13.3 or later
- **Links Mac Desktop**: Version 1.13.3 or later

Note:
It's recommended to keep the default configuration for **Do Not Disturb** status. In this status, all incoming calls are always routed to the designated destination, and extension users will not receive calls from queues, ring groups, or paging groups.

DTMF

Setting	Description
DTMF Passthrough	If enabled, PBX will pass DTMF tones directly to the other end without processing the DTMF tones.
DTMF Duration (ms)	Set the duration (in millisecond) of DTMF audio signal sent by the PBX. The default value is **120**.
DTMF Gap (ms)	Set the interval (in millisecond) between two DTMF audio signals sent by the PBX. The default value is **120**.

Extension Preferences

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

Extension Type	Default Range
User Extension	1000 - 5999
Parking Extension	6000 - 6099
Group Voicemail Extension	6100 - 6199
IVR Extension	6200 - 6299
Ring Group Extension	6300 - 6399
Queue Extension	6400 - 6499
Conference Extension	6500 - 6599
Paging Extension	6600 - 6699
Account Trunk	6700 - 6799
WebRTC Trunk Number	6800 - 6899

The total of PBX extensions ＞ 6000

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
WebRTC Trunk Number	50800 - 50899

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.

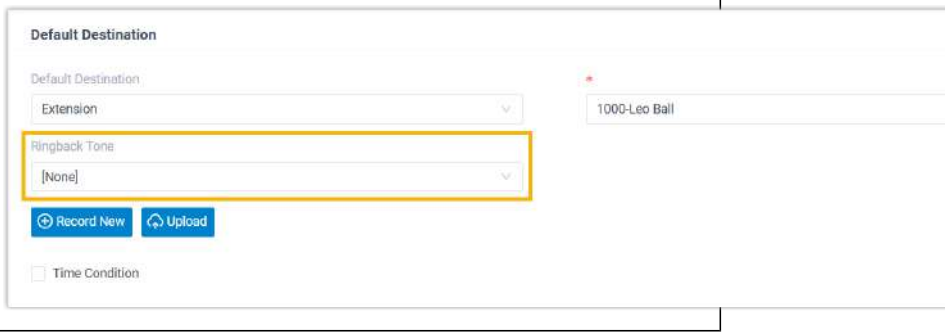
  You can use pre-defined music on hold, or customize your own music on hold.

  For more information, see Set up a Custom MoH Playlist.

Voice prompt preference settings

Navigation path: **PBX Settings > Voice Prompt > Prompt Preferences**.

Setting	Description
Music on Hold	The playlist to be played when a call is on hold. **Note:** The available playlists are synchronized with playlists in **Music on Hold**.
Music on Hold for Call Forwarding	The music to be played when the caller is put on hold during call forwarding. • **Music on Hold**: Play **Music on Hold** to the caller. • **Ringing Tone**: Play ringing tone to the caller.
Invalid Phone Number Prompt	The prompt to be played when a callee number is invalid. **Note:** The available prompts are synchronized with **Custom Prompt**.
Busy Line Prompt	The prompt to be played when a trunk is in use. **Note:** The available prompts are synchronized with **Custom Prompt**.
Call Failure Prompt	The prompt to be played when a call is failed to be sent out. **Note:** The available prompts are synchronized with **Custom Prompt**.
Event Notification Prompt	The prompt to be played when PBX places a call to notify callee that a specific event occurs. **Note:** The available prompts are synchronized with **Custom Prompt**.
Play Call Forwarding Prompt	Whether to inform the user that the current call will be forwarded.
Play Call Waiting Prompt	The prompt to be played when the caller is waiting to be connected to an extension user that is on a call.

Setting	Description
	• If the caller is an **extension user**, the system will play call waiting prompt "Sorry! Please hold on, the number you dialed is busy now.", then play ringing tone. • If the caller is an **external user**, the system will play call waiting prompt "Sorry! Please hold on, the number you dialed is busy now.", then play ringing tone or ringback tone (depending on whether you have configured ringback tone for the inbound route via which the caller is routed: **Call Control > Inbound Route > Default Destination > Ringback Tone**). 

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 **Tip:**

Item	Requirements
	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

> **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.

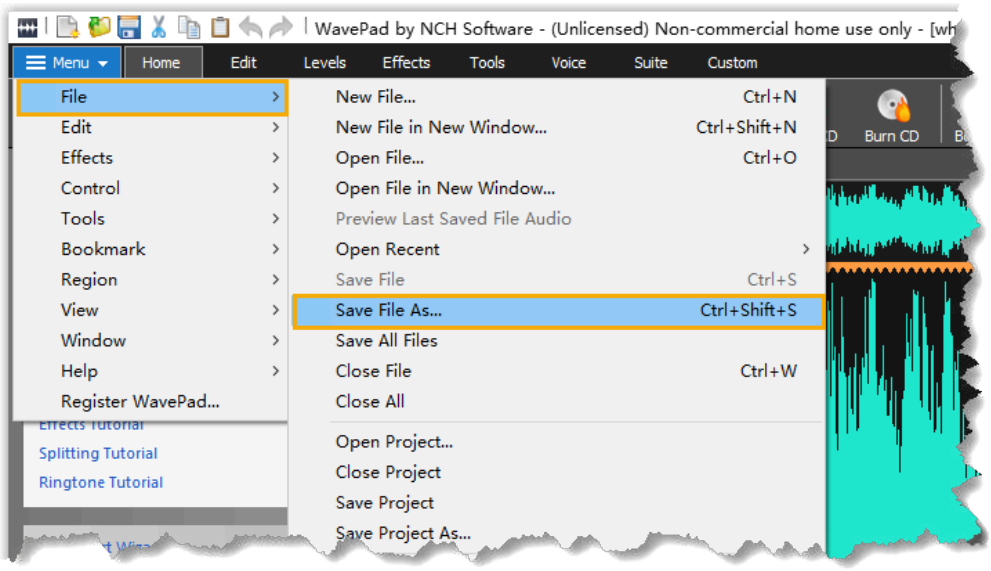
In this topic, we take the followings as examples to show you how to convert file format.

- Convert Audio Files via WavePad
- Convert Audio Files Online

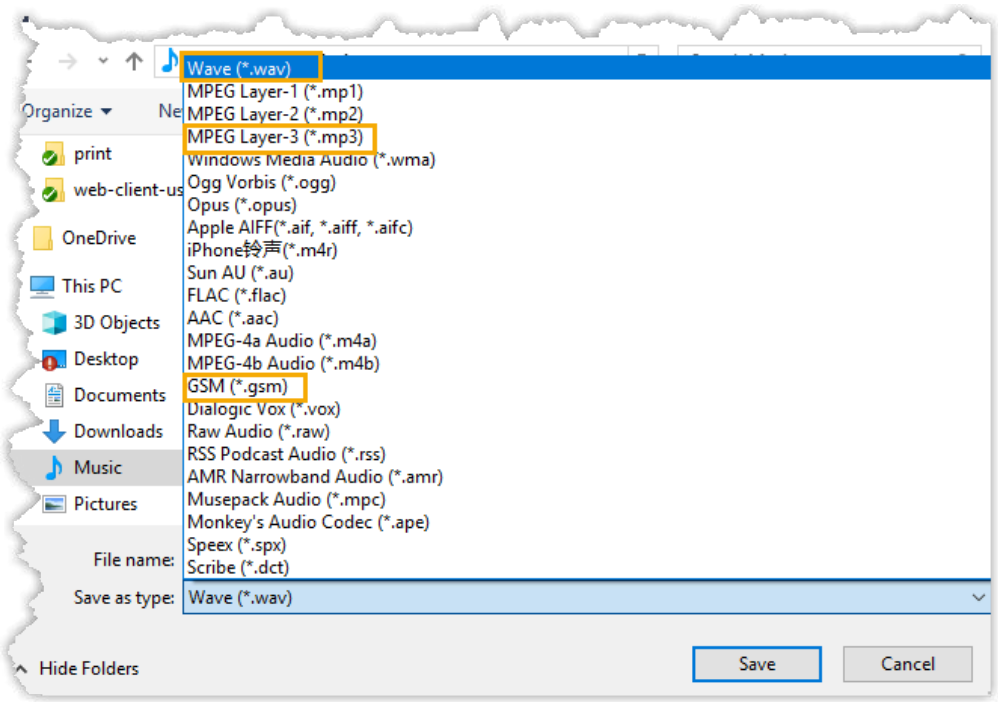
Convert audio files via WavePad

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**.

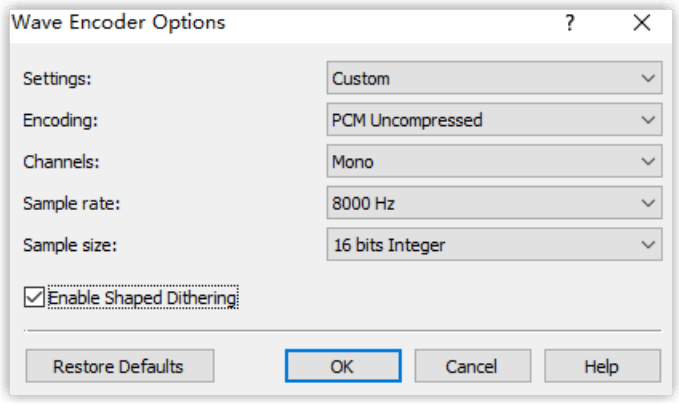


3. In the **Save as type** drop-down list, select `Wave(*.wav)`, `MPEG Layer-3(*.mp3)`, or `GSM(*.gsm)`, click **Save**.



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

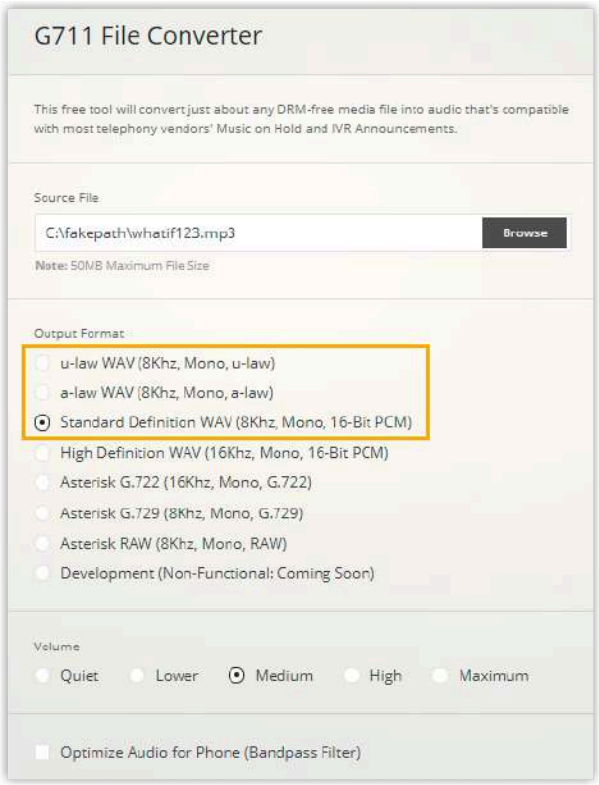


Convert audio files online

If you don't want to download an app, you can quickly convert your audio files via G711 File Converter online.

1. Go to g711.org.
2. Click **Browse** to upload your audio file.
3. Set the **Output Format**.

> **Note:**
> Select any one of **u-law WAV (8Khz, Mono, u-law)**, **a-law WAV (8Khz, Mono, a-law)**, and **Standard Definition WAV (8Khz, Mono, 16-Bit PCM)**.



4. Click **Submit** to start converting the file.

Audio Files Requirements

This topic describes the requirements for audio files to be uploaded to Yeastar P-Series 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.
File Format	`.wav`, `.mp3`, or `.gsm`. • PCM, 8Khz, 16bit, 128kbps • A-law (g.711), 8Khz, 8bit, 64kbps • u-law (g.711), 8Khz, 8bit, 64kbps

SIP Settings

This topic describes the SIP settings on the Yeastar P-Series 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 27.

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.

Table 27. (continued)

Setting	Description
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. • 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	

Table 27. (continued)

Setting	Description
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 28.

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**.

Setting	Description
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. • TLS V1.0 • TLS V1.2 **Note:** It's recommended to use the more secure TLS V1.2.
TLS Verify Server	Verify server certificate when PBX acts as a client. **Note:** If enabled, you need to upload a server certificate to the PBX.

Session Timer

A periodic refreshing of a SIP session that allows both user agent and proxy to determine if the SIP session is still active.

Setting	Description
Session Timer	Select a session timer mode. • **No**: Do not include “timer” value in any field. • **Supported**: Include “timer” value in Supported header. • **Required**: Include “timer” value in Required header. • **Forced**: Include “timer” value in both Supported and Required header.
Session-Expires (s)	The max refresh interval in seconds.
Min-SE (s)	The min refresh interval in seconds. The value should not be smaller than 90.

QoS

Quality of Service (QoS) is a major issue in VoIP implementations. The issue is how to guarantee that packet traffic for a voice or other media connection will not be delayed or dropped due to interference from other traffic of lower priority.

When the network capacity is insufficient, QoS can provide users with priority by setting the value.

Setting	Description
ToS (Type of Service)	
ToS SIP	Type of Service for SIP packets.
ToS Audio	Type of Service for RTP audio packets.
ToS Video	Type of Service for RTP video packets.
CoS (Class of Service)	
Cos SIP	Class of Service for SIP packets.
Cos Audio	Class of Service for RTP audio packets.
Cos Video	Class of Service for RTP video packets.

T.38

Adjust T.38 settings if T.38 Fax doesn't work.

Setting	Description
T.38 Max BitRate	Adjust the max BitRate for T.38 fax.
No T.38 Attributes in re-INVITE SDP	If enabled, SDP re-invite packet will not contain T.38 attributes.
Error Correction Mode	Enable or disable Error Correction for the fax.

Advanced SIP settings

Setting	Description
Incoming Caller ID/DID Retrieval	
Get Caller ID From	Decide the system will retrieve Caller ID from which header field. • From • Contact • Remote-Party-ID • P-Asserted-Identity

Setting	Description
	• P-Preferred-Identity
Get DID From	Decide the system will retrieve DID from which header field. • To • Invite • Diversion • Remote-Party-ID • P-Asserted-Identity • P-Preferred-Identity • P-Called-Party-ID **Note:** If **Remote-Party-ID** is selected but the SIP trunk doesn't support this, the system will retrieve DID from **Invite** header.
SIP Request Header	
User Agent	Set the user agent that will be included when sending SIP packages out.
Internal Alert Info	Set an "alert info text" to add to Alert-info header in INVITE request for internal calls. When receiving an internal call, the phone will inspect "Alert-Info" header to determine which ring tone it should use for ringing.
Other Options	
Allow Guest	If enabled, PBX will accept unknown calls.
Support Message Request	Whether to support SIP Message Request or not.
Inband Progress	Whether to enable inband progress or not. The Inband Progress setting applies to all the extensions. **Note:** To configure global Inband Progress setting, you need to contact Yeastar support to configure a custom configuration file. • **Check this option**: PBX will send a 183 Session Progress to the extension when told to indicate ringing and immediately start sending ringing as audio. • **Uncheck this option**: PBX will send a 180 Ringing to the extension when told to indicate ringing, but will NOT send it as audio.

Setting	Description
Enable uaCSTA Connection	If this option is enabled, the PBX will allow user agent Computer Supported Telecommunications Application (uaCSTA) to remotely control the IP phone via Linkus Web Client CTI or Linkus Desktop Client CTI. **Note:** Your IP phone should support uaCSTA standard to use this function.
Extension Forwarding with Diversion SIP Header	If this option is enabled, when an extension's call forwarding destination is another extension, a Diversion header will be included in the INVITE request to inform the destination of the source extension from which the call was forwarded.
P Asserted Identity	If this option is enabled, a `P Asserted Identity` field will be carried in the SIP header for calls that are transferred or forwarded to convey the identity of the call initiator. **Note:** This setting is only available for internal calls. For external calls, see SIP Headers settings for trunk.

Jitter Buffer

Jitter Buffer Overview

This topic describes what is and when to use jitter buffer, and introduces two jitter buffer types supported on Yeastar P-Series 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.

Internet protocols

Yeastar P-Series Software Edition supports the following Internet protocols:

- **IPv4 only**: The PBX can be configured with IPv4 address, and can communicate with the devices that support IPv4 protocol.
- **IPv4 / IPv6 dual stack**: The PBX can be configured with both IPv4 address and IPv6 address, and can communicate with a wide range of devices that support IPv4 protocol or IPv6 protocol.

IP address assignment

Yeastar P-Series 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.
- IPv6 over PPPoE is NOT supported.

Configure a Static IPv4 Address

This topic describes how to configure a static IPv4 address for Yeastar P-Series 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 and WAN port of Yeastar P-Series Software Edition to connect different networks, so that LAN/WAN uplinks can carry different services through separate ports, optimizing the utilization of network bandwidth. The IP information is as below:

LAN	WAN
• IP address: 192.168.6.124 • Subnet mask: 255.255.255.0 • Gateway address: 192.168.6.1 • DNS server: 192.168.1.1	• IP address: 10.0.0.50 • Subnet mask: 255.255.255.0 • Gateway address: 10.0.0.1 • DNS server: 8.8.8.8

Prerequisites

- PBX and PC are connected to the same local network.
- Your PC has ability to access the default network segment 192.168.5.X of the PBX.

Tip:
To access the PBX, you need to change your PC to the same network segment of the PBX.

Procedure

1. Log in to PBX web portal, go to **System > Network > Basic Settings**.
2. In the **Basic** section, configure the following settings:

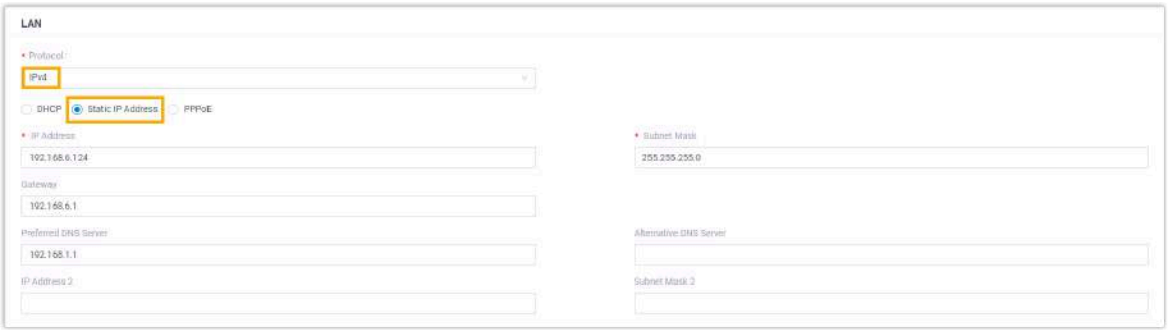
   - **Ethernet Mode**: Select the Ethernet mode. In this scenario, select **Dual**.
     - **Single**: Only the LAN port is used for up-link connection.
     - **Dual**: Both LAN and WAN are used for up-link connection.

     > **Note:**
     > The traffic will be routed to the default interface; you may need to add a static route to override the default route entries, routing the traffic from a specific IP address to the specified destination.

   - **Number of WAN Ports**: Optional. To connect more than one service providers, specify the number of WAN ports as needed.

     > **Note:**
     > This is only supported on P-Series Software Edition deployed on **Ubuntu**, and the PBX version must be 83.17.0.60 or later.

   - **Default Interface**: Select a default interface if select **Dual** mode. In this scenario, select **LAN**.
3. In the **LAN** section, select **IPv4** Internet protocol and select **Static IP Address**, then enter the network information for LAN port.

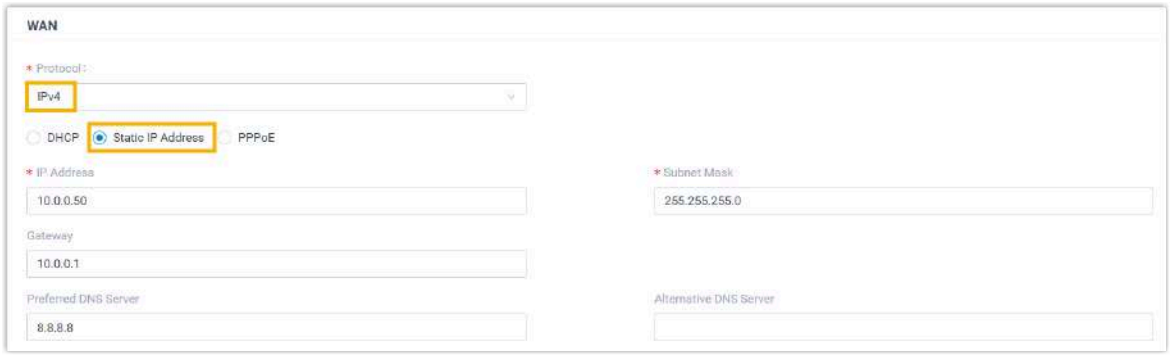


- **IP Address**: Enter the IP address that is assigned to the PBX.
- **Subnet Mask**: Enter the subnet mask.
- **Gateway**: Enter the gateway address.
- **Preferred DNS Server**: Enter the IP address of preferred DNS server.
- **Alternative DNS Server**: Optional. Enter the IP address of alternative DNS server.
- **IP Address 2**: Optional. Enter a second IP address for the PBX.

> **Note:**
> According to your network environment, you may need to set another IP address to allow users in different IP segment to access the PBX.

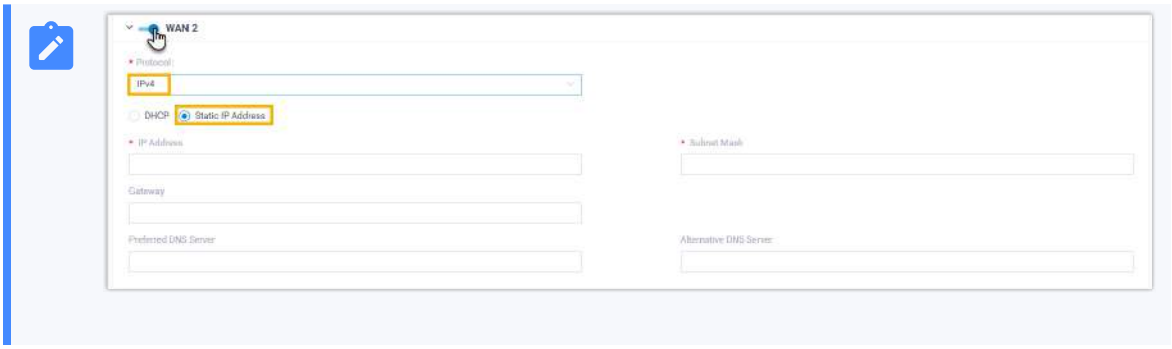
- **Subnet Mask 2**: Optional. Enter another subnet mask for the second IP address.

4. In the **WAN** section, select **IPv4** Internet protocol and select **Static IP Address**, then enter the network information for WAN port.



- **IP Address**: Enter the IP address that is assigned to the WAN interface.
- **Subnet Mask**: Enter the subnet mask.
- **Gateway**: Enter the gateway address.
- **Preferred DNS Server**: Enter the IP address of preferred DNS server.
- **Alternative DNS Server**: Optional. Enter the IP address of alternative DNS server.

> **Note:**
> If you specify the number of WAN ports, enable the WAN X (X refers to the specific number between 2 and 5) and configure related settings.



5. Click **Save** and reboot the PBX to take effect.

Result

After the PBX reboots, the LAN interface is changed to 192.168.6.124, and the WAN interface is changed to 10.0.0.50.

Different services will be sent through different ports. For example, LAN interface can be used to send and receive internal network traffic, while the WAN interface can be used to connect SIP providers.

What to do next

To access the PBX, change your PC's IP to the same network segment of the PBX, for example, 192.168.6.110.

Obtain an IP Address from a DHCP Server

This topic describes how to configure Yeastar P-Series Software Edition to automatically obtain an IPv4 address from a DHCP server running in your network.

Background information

If you choose this method to configure IP address for the PBX, the IP address assigned to the PBX may vary every time the PBX starts up. We suggest that you configure a static IP address for the PBX. For more information, see Configure a Static IPv4 Address.

The following instructions assume that you need to use LAN port and WAN port of Yeastar P-Series Software Edition to connect different networks, and need to obtain an IP address from the DHCP server.

Prerequisites

- DHCP feature is enabled on your router.

- Only one DHCP server in the local network, or the PBX cannot get the IP address.

Procedure

1. Log in to PBX web portal, go to **System > Network > Basic Settings**.
2. In the **Basic** section, configure the following settings:

   - **Ethernet Mode**: Select the Ethernet mode. In this scenario, select **Dual**.
     - **Single**: Only the LAN port will be used for up-link connection.
     - **Dual**: Both LAN and WAN can be used for up-link connection.

     > **Note:**
     > The traffic will be routed to the default interface; you may need to add a static route to override the default route entries, routing the traffic from a specific IP address to the specified destination.

   - **Number of WAN Ports**: Optional. To connect more than one service providers, specify the number of WAN ports as needed.

     > **Note:**
     > This is only supported on P-Series Software Edition deployed on **Ubuntu**, and the PBX version must be 83.17.0.60 or later.

   - **Default Interface**: Select a default interface if select **Dual** mode. In this scenario, select **LAN**.
3. In the **LAN** section, select **IPv4** Internet protocol, then select **DHCP**.

4. In the **WAN** section, select **IPv4** Internet protocol, then select **DHCP**.

Note:
If you specify the number of WAN ports, enable the WAN X (X refers to the specific number between 2 and 5) and configure related settings.

5. Click **Save** and reboot the PBX to take effect.

Result

The PBX will obtain new IP addresses from the DHCP server in your local network.

You need to log in to the web interface of your router to see assigned IP addresses.

Configure a PPPoE Connection

This topic describes how to configure a PPPoE connection on Yeastar P-Series Software Edition to obtain an IPv4 address when the PBX is in Dual network mode.

Note:
IPv6 over PPPoE is NOT supported.

Background information

A PPPoE client assigns a dynamic IP address to the PBX, the IP address of the PBX may vary every time the PBX starts up. In this case, you need to configure dual network, and configure a static IP address on the PBX to ensure that you can always access the PBX.

The following instructions assume that you need to connect LAN port to local network, connect WAN port to PPPoE. The network information is as the following:

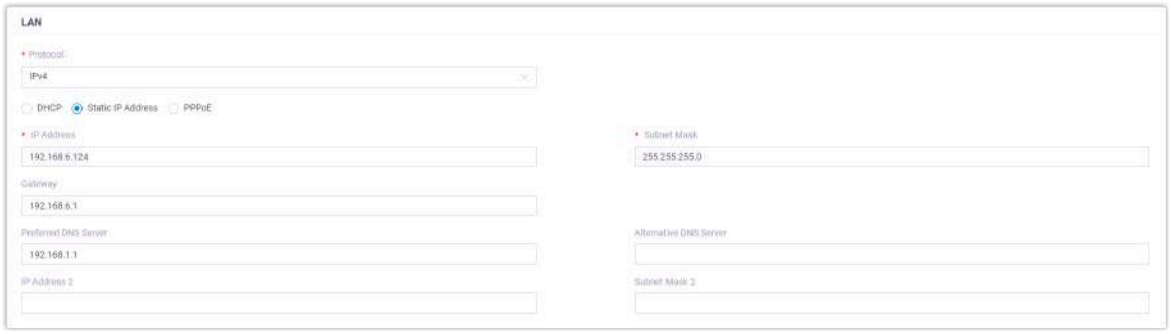
LAN	WAN
Static IP • IP address: 192.168.6.124 • Gateway address: 192.168.6.1 • Subnet mask: 255.255.255.0 • DNS: 192.168.1.1	**PPPoE** • Username: 059219383822 • Password: 19283772

Procedure

1. Log in to PBX web portal, go to **System > Network > Basic Settings**.
2. In the **Basic** section, configure the following settings:
   - **Ethernet Mode**: Select the Ethernet mode. In this scenario, select **Dual**.
     - **Single**: Only the LAN port will be used for up-link connection.
     - **Dual**: Both LAN and WAN can be used for up-link connection.

     > **Note:**
     > The traffic will be routed to the default interface; you may need to add a static route to override the default route entries, routing the traffic from a specific IP address to the specified destination.

   - **Default Interface**: Select the port where PPPoE is connected. In the scenario, select **WAN**.
3. In the **LAN** section, select an Internet protocol and select **Static IP Address**, then enter the network information for LAN port.



   - **IP Address**: Enter the IP address that is assigned to the PBX.
   - **Subnet Mask**: Enter the subnet mask.

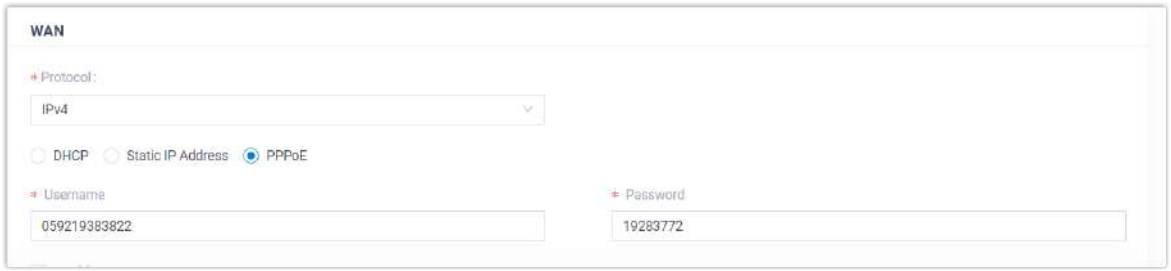
- **Gateway**: Enter the gateway address.
- **Preferred DNS Server**: Enter the IP address of preferred DNS server.
- **Alternative DNS Server**: Optional. Enter the IP address of alternative DNS server.
- **IP Address 2**: Optional. Enter a second IP address for the PBX.

> **Note:**
> According to your network environment, you may need to set another IP address to allow users in different IP segment to access the PBX.

- **Subnet Mask 2**: Optional. Enter another subnet mask for the second IP address.

4. In the **WAN** section, select **IPv4** and select **PPPoE**, then enter the **Username** and **Password**.

> **Note:**
> IPv6 over PPPoE is NOT supported.



5. Click **Save** and reboot the PBX to take effect.

Result

Both LAN and WAN are set up for the PBX.

- All network traffic will be sent and received by the WAN port (default network interface).
- You can access the PBX web portal by the LAN IP address to configure the PBX settings.

What to do next

If you want to route network traffic through LAN port, you need to add static routes on the PBX. For more information, see Add a Static Route.

Configure a VLAN on Yeastar P-Series Software Edition

This topic describes how to configure a VLAN on Yeastar P-Series Software Edition.

Background information

A VLAN subinterface is a virtual interface created by dividing one physical Ethernet interface (LAN or WAN) into multiple logical interfaces, enabling access to the VLAN configured by the switch or router.

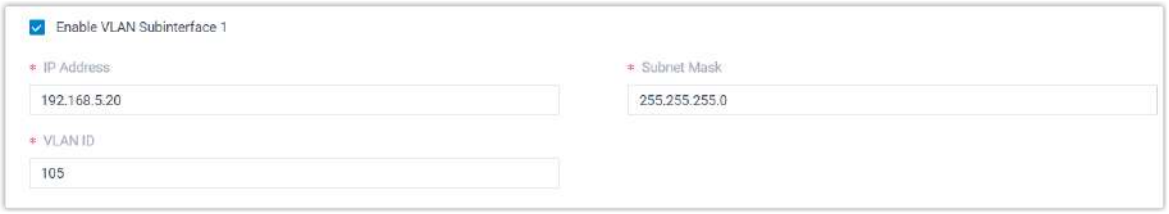
If the PBX has only one physical Ethernet interface, but needs to route traffic via multiple different subnets, you can add a VLAN subinterface with a different subnet and a different VLAN ID for the main interface (LAN or WAN). This allows the PBX to manage traffic for different VLANs or subnets using the same physical interface.

The following instructions assume that you need to add a VLAN subinterface for LAN interface.

- **Main interface (LAN)**: For network traffic in subnet 192.168.6.0/24.
- **Sub interface**: For network traffic in subnet 192.168.5.0/24.

Procedure

1. Log in the PBX web portal, go to **System > Network > Basic Settings**.
2. In the **LAN** section, select the checkbox of **Enable VLAN Subinterface 1** and configure the following settings.



   - **IP Address**: Assign an IP address that is in the subnet 192.168.5.0/24. For example, *192.168.5.20*.
   - **Subnet Mask**: Enter the subnet mask. In this scenario, enter *255.255.255.0*.
   - **VLAN ID**: Enter the VLAN ID that is configured on the switch or router. For example, enter *105*.

> **Note:**

> To know the VLAN ID configured on the switch or router, contact IT administrator of switch or router.

3. Click **Save** and reboot the PBX to take effect.

   The network traffic from subnet 192.168.5.0/24 and has VLAN ID 105 will be routed to the VLAN sub interface.

Web Server

Change Web Server Protocol and Port

This topic describes how to change the web protocol and port of Yeastar P-Series 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 an HTTPS port.
      - **HTTPS Certificate**: Select the default certificate or upload your own certificate.

- **Supported TLS Version**: Select the supported TLS version for handshake negotiation between PBX server and the connected client.
  - **TLS 1.2**: PBX server only supports TLS 1.2 for client-server communication.
  - **TLS 1.0, TLS 1.1, and TLS 1.2**: PBX server supports TLS 1.0/1.1/1.2 for client-server communication. The version that will be used depends on the highest supported TLS version on the connected client.
- **Redirect from HTTP 80 port**: Decide whether to allow requests to HTTP port 80.

  If the option is enabled, the requests to HTTP port 80 will be redirected to the respective HTTPS service.

c. If **HTTP** is selected, enter the HTTP port in the **HTTP Port** field.

3. Click **Save** and **Apply**.

Result

The next time, you need to access the PBX web portal by the configured protocol and port.

Change Automatic Logout Time

For security purposes, Yeastar P-Series 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
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.	10000-20000
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 29.

Feature	Description	Default Status	Usage Permission Setting
SIP Access	Support remote SIP registration via FQDN, including the registration of remote SIP extension and SIP account trunk. **Important:** The remote SIP access feature does NOT support the remote registration of SIP peer trunk.	Disabled.	• **Account**: Restrict or allow specific accounts to get access to the service via FQDN. **Note:** By default, all accounts are NOT allowed to use the remote SIP access feature. • **IP Address**: Only permit specific IP addresses to get access to the service via FQDN.
Web Access	Support remote access to the PBX web portal or Linkus Web Client via FQDN.	Enabled by default, and cannot be disabled.	• **Account**: Restrict or allow specific accounts to get access to the service via FQDN. **Note:** By default, the super administrator account is restricted from using the remote web access feature. • **IP Address**: Only permit specific IP addresses to get access to the service via FQDN.
Linkus Access	Support remote access to Linkus Clients via FQDN.	Enabled by default, and cannot be disabled.	• **IP Address**: Only permit specific IP addresses to get access to the service via FQDN.
LDAP Access	Support remote LDAP access via FQDN.	Disabled.	• **IP Address**: Only permit specific IP addresses to get access to the service via FQDN.
API Access	Support remote API access via FQDN.	Disabled.	• **IP Address**: Only permit specific IP addresses to get access to the service via FQDN.

For more detailed configurations, see the following topics:

Configure Network for Remote SIP Access by a Yeastar FQDN

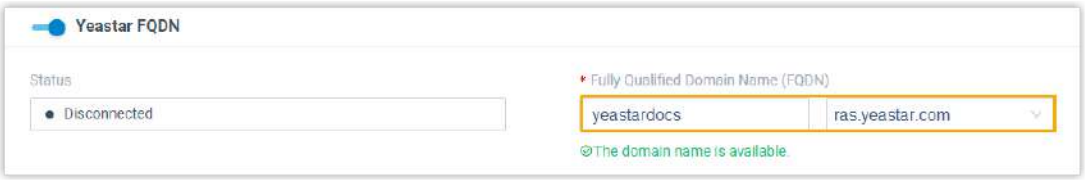
With a Yeastar FQDN, you can quickly establish a secure tunnel for remote registration of IP phones, alike SIP endpoints, and account trunks, without the need of configuring public IP and port forwarding for the PBX. This topic describes how to configure network for remote SIP access via FQDN.

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**.

4. Enable remote SIP access feature and grant usage permissions.

   > **Note:**
   > By default, all accounts are NOT allowed to use the remote SIP access feature. You need to grant the usage permission to desired accounts.

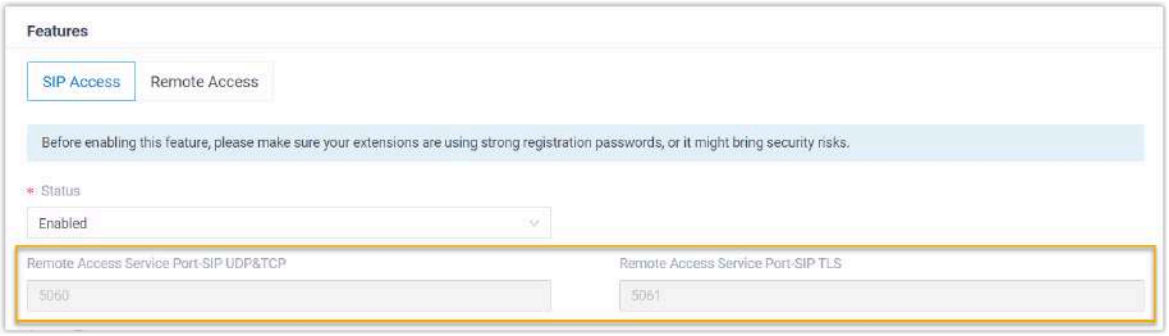
a. In the **Features** section, go to the **SIP Access** tab.
b. In the **Status** drop-down list, select **Enabled**.
c. In the **Access Type** drop-down list, select the account access restriction type.
   - **Allowed Account**: Only the selected accounts can get access to the service.
   - **Restricted Account**: All accounts except for the selected accounts can get access to the service.
d. Select the desired accounts from the **Available** box to the **Selected** box.
e. **Optional:** Select the checkbox of **Enable IP Restriction**, and add at least one permitted IP address and subnet mask.

   If you configure this option, only the permitted IP address(es) can use the remote access feature.

5. Click **Save** and **Apply**.

Result

- The Remote Access Service automatically assigns ports for remote SIP access, you can check the port in **Remote Access Service Port**.



- You can implement the followings:
  - Set up a Remote SIP Phone via Yeastar FQDN.
  - Perform remote registration of SIP Account trunk via Yeastar FQDN.

> **Important:**
> The remote registration of SIP peer trunk via Yeastar FQDN is NOT supported.

Related information

Auto Provision IP Phones Remotely (RPS FQDN Method)

Configure Network for Remote Web Access by a Yeastar FQDN

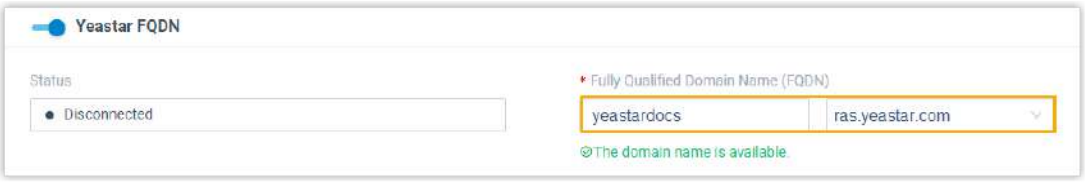
Yeastar FQDN provides secure remote access to PBX web portal or Linkus Web Client, without the need of configuring public IP and port forwarding. This topic describes how to configure network for remote web access via FQDN.

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.

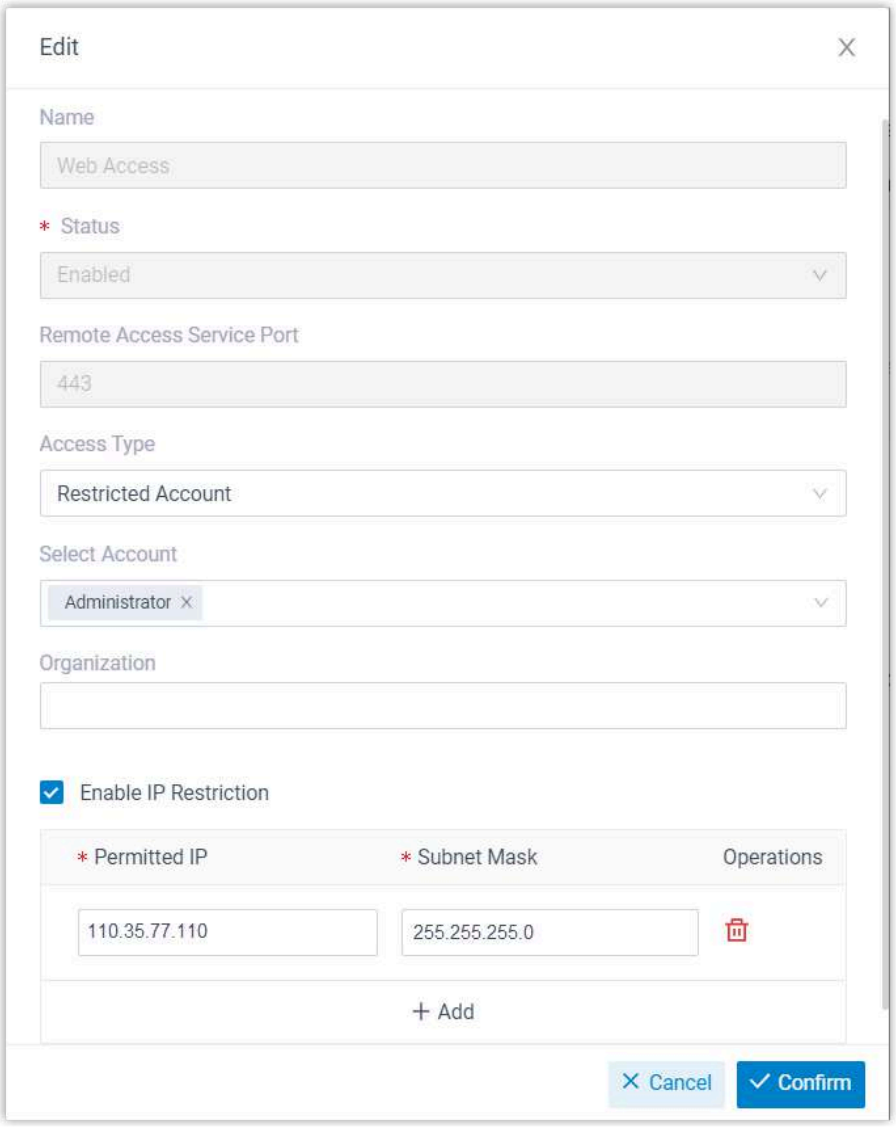
   For example, select domain name **ras.yeastar.com** and enter hostname `yeastardocs`, you will get an FQDN **yeastardocs.ras.yeastar.com**.

4. **Optional:** Configure remote web access usage permission.

   > **Note:**
   > By default, the super administrator account is restricted from using the remote web access feature.

   a. In the **Features** section, go to the **Remote Access** tab.
   b. Click beside the **Web Access**.
   c. In the pop-up window, complete the following settings according to your need.



- **Name**: Display the remote access feature name, and cannot be edited.
- **Status**: Enabled by default, and cannot be disabled.
- **Remote Access Service Port**: Display the remote web access port 443. The port is assigned by Remote Access Service automatically.
- **Access Type**: Define the account access restriction type.
    - **Allowed Account**: Only the selected accounts can get access to the service.
    - **Restricted Account**: All accounts except for the selected accounts can get access to the service.
- **Select Account**: Select the desired accounts that can or can not use the remote access feature.

- **Organization**: Select the desired organization(s) that can or can not use the remote access feature.

  > **Note:**
  > - This setting is available only when the **Organization Management** feature is enabled.
  > - By default, when you select an organization, its associated sub-organizations are selected. Be careful when selecting organizations.

- **Enable IP Restriction**: Select the checkbox of the option, and add at least one permitted IP address and subnet mask.

  If you configure this option, only the permitted IP address(es) can use the remote access feature.

d. Click **Confirm**.

5. Click **Save**.

Result

Network for remote web access is automatically configured, the authorized accounts can remotely access PBX web portal or Linkus Web Client via the FQDN.

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.

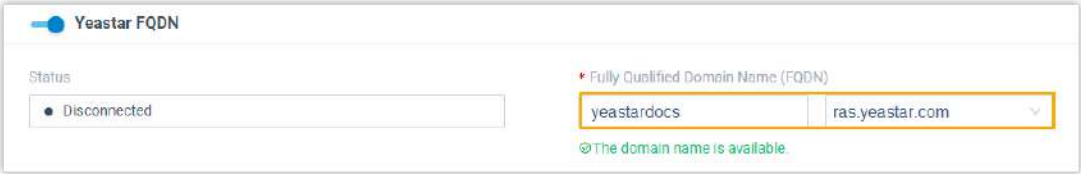
Procedure

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.

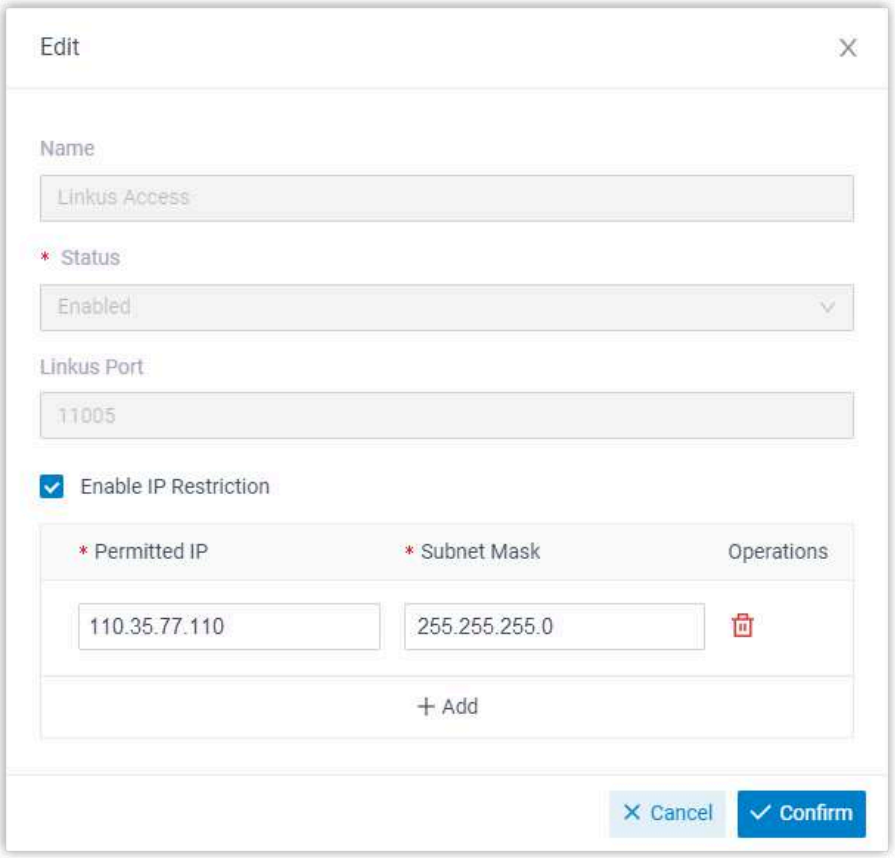
   > **Note:**

> 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**.



4. **Optional:** Configure remote Linkus access usage permission.
   a. In the **Features** section, go to the **Remote Access** tab.
   b. Click beside the **Linkus Access**.
   c. In the pop-up window, complete the following settings according to your need.



- **Name**: Display the remote access feature name, and cannot be edited.
- **Status**: Enabled by default, and cannot be disabled.

- **Linkus Port**: Display the remote Linkus access port 11005. The port is assigned by Remote Access Service automatically.
- **Enable IP Restriction**: Select the checkbox of the option, and add at least one permitted IP address and subnet mask.

  If you configure this option, only the permitted IP address(es) can use the remote access feature.

d. Click **Confirm**.

5. Click **Save**.

Result

Linkus Server is automatically set up for remote access, users can remotely log in to Linkus UC Clients via the FQDN.

> **Troubleshooting:**
> If a user can not access Linkus Web Client via the FQDN, check if you have allowed the user to use the remote web access service via FQDN.

Configure Network for Remote LDAP Access by a Yeastar FQDN

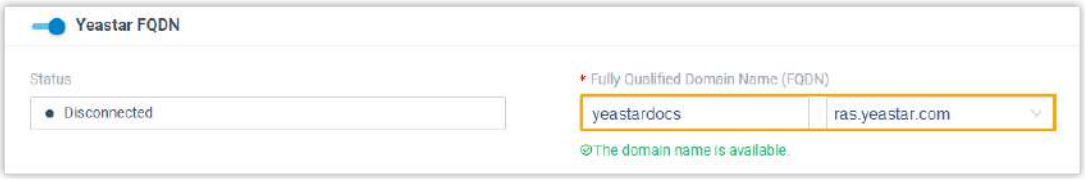
With a Yeastar FQDN, you can remotely access the LDAP server on PBX via secure LDAP connection without the need of configuring public IP and port forwarding for the PBX. This topic describes how to configure network for remote LDAP access via FQDN.

Procedure

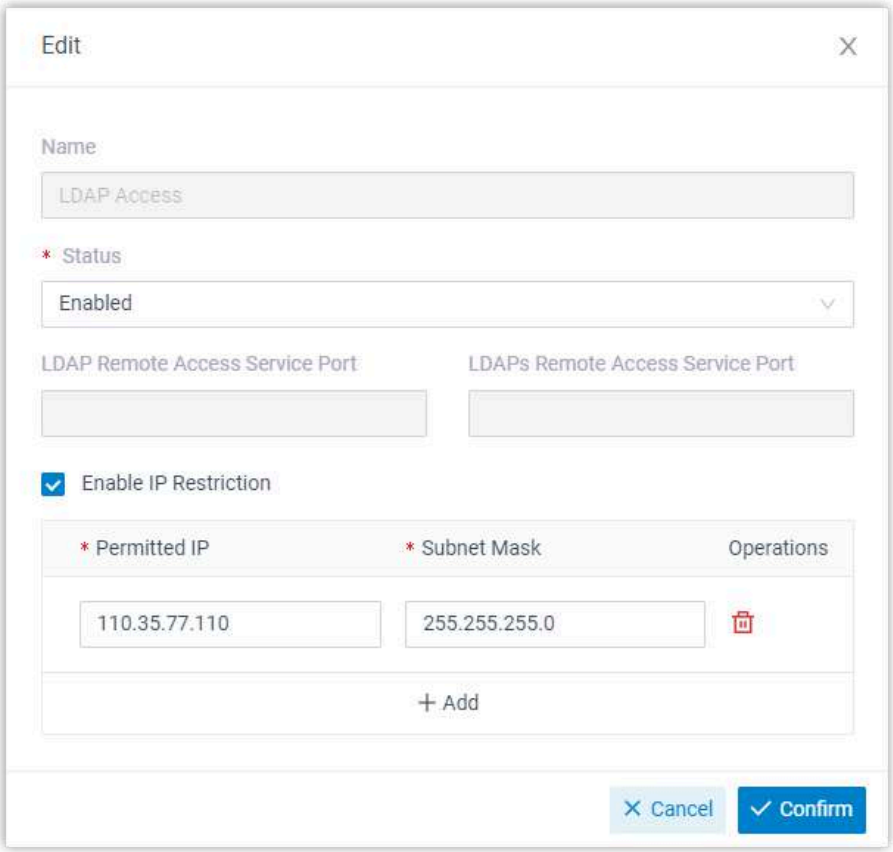
1. Log in to PBX web portal, go to **System > Network > Yeastar FQDN**.
2. Turn on **Yeastar FQDN**.
3. In the **Fully Qualified Domain Name (FQDN)** field, set up the FQDN domain name.
   a. Select a domain name from the drop-down list.
   b. Enter a host name in the first field.

   > **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**.



4. Enable remote LDAP access feature and configure usage permission.
   a. In the **Features** section, go to the **Remote Access** tab.
   b. Click beside the **LDAP Access**.
   c. In the pop-up window, complete the following settings according to your need.



- **Name**: Display the remote access feature name, and cannot be edited.
- **Status**: Select **Enabled**.
- **Remote Access Service Port**: The remote access ports will be assigned by Remote Access Service automatically.
- **Enable IP Restriction**: Optional. Select the checkbox of the option, and add at least one permitted IP address and subnet mask.

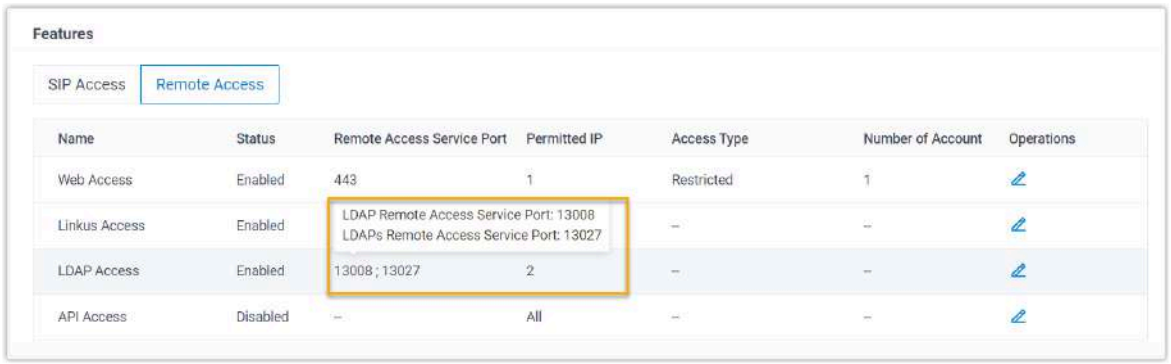
  If you configure this option, only the permitted IP address(es) can use the remote access feature.

d. Click **Confirm**.

5. Click **Save**.

Result

- The Remote Access Service automatically assigns ports for remote LDAP access.



- You can set up the PBX as an LDAP server via the FQDN, allowing an IP phone to remotely and securely query contacts' information within the PBX's directory. For more information of the remote LDAP settings, see Set up Yeastar P-Series Software Edition as an LDAP Server.

Configure Network for Remote API Access by a Yeastar FQDN

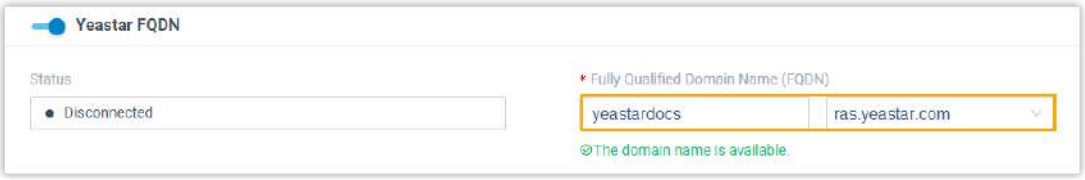
With a Yeastar FQDN, you can remotely access Yeastar P-Series APIs via a secure tunnel, without the need of configuring public IP and port forwarding for the PBX. This topic describes how to configure network for remote API access via FQDN.

Procedure

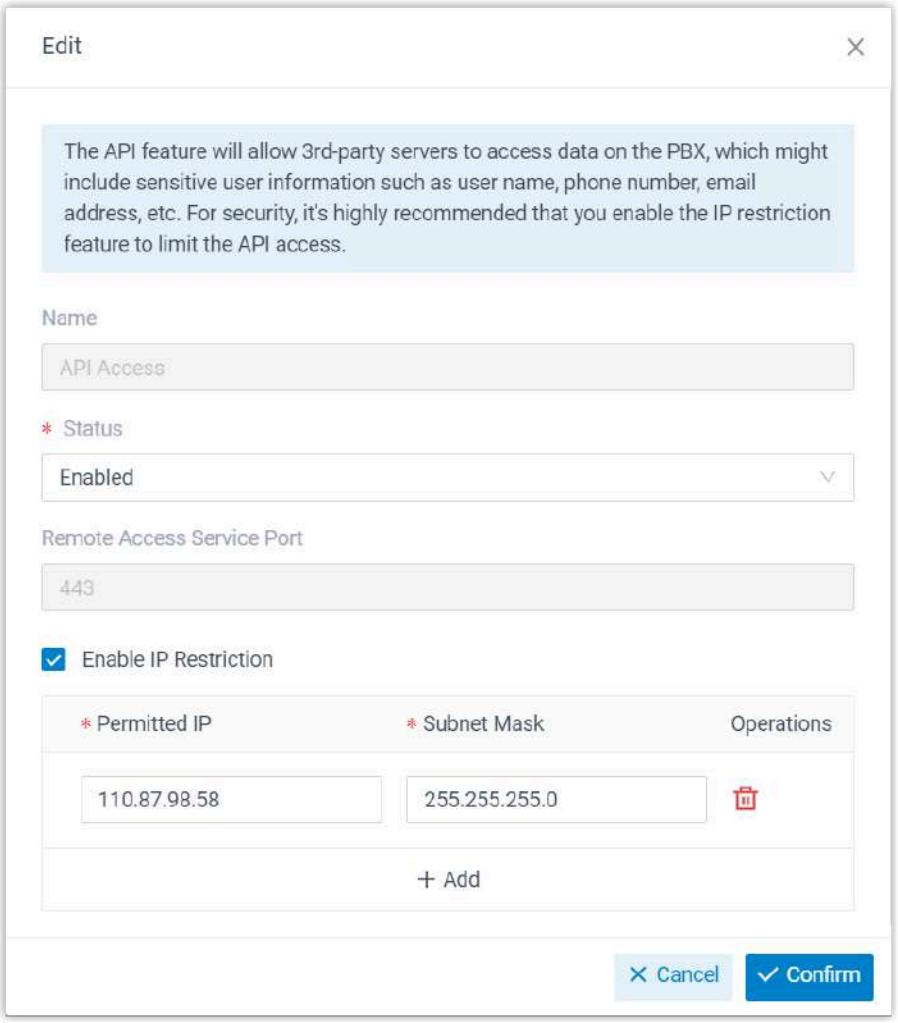
1. Log in to PBX web portal, go to **System > Network > Yeastar FQDN**.
2. Turn on **Yeastar FQDN**.
3. In the **Fully Qualified Domain Name (FQDN)** field, set up the FQDN domain name.
   a. Select a domain name from the drop-down list.
   b. Enter a host name in the first field.

> **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**.



4. Enable remote API access feature and configure usage permission.
   a. In the **Features** section, go to the **Remote Access** tab.
   b. Click ✎ beside the **API Access**.
   c. In the pop-up window, complete the following settings according to your need.



   - **Name**: Display the remote access feature name, and cannot be edited.
   - **Status**: Select **Enabled**.

- **Remote Access Service Port**: Display the remote API access port 443. The port is assigned by Remote Access Service automatically.
- **Enable IP Restriction**: Optional. Select the checkbox of the option, and add at least one permitted IP address and subnet mask.

  If you configure this option, only the permitted IP address(es) can use the remote access feature.

d. Click **Confirm**.

5. Click **Save**.

Result

You can now remotely access P-Series APIs via the FQDN.

Public IP and Ports

Public IP and Ports Overview

This topic describes when you need to configure the Public IP and Ports settings and introduces three functions of Public IP and Ports settings.

Applications

When your PBX is connected behind a router and needs to communicate with SIP devices on the external network, you need to set Public IP and Ports settings. Public IP and Port settings can be applied to different types of networks:

- Public IP Address
- External Host
- Yeastar Domain Name

Public IP Address

If your Internet Service Provider (ISP) provides a static public IP address, you can configure PBX network for remote access with the IP address.

For more information about the configurations, see Configure Network for Remote Access by a Public IP Address.

External Host

If static public IP address is not available in your network environment, you must have a registered domain name, and configure PBX network for remote access with the domain name.

For more information about the configurations, see Configure Network for Remote Access by a Domain Name.

Yeastar Domain Name

If you want to implement direct remote communication between the PBX server and the clients via a domain name but prefer a simplified domain setup, Yeastar offers a domain service that makes the process hassle-free. You only need to configure a Yeastar domain name, without having to configure DNS resolution and request certificates, the PBX can automatically complete the rest of the process and renew the domain certificates.

For more information about the configurations, see Configure Network for Remote Access by a Yeastar Domain Name.

Functions

Public IP and Ports settings have the following two functions to ensure that remote devices can access and communicate with the PBX via SIP protocol:

- Solve SIP NAT issue
- Provide PBX with information of Linkus remote access

Solve SIP NAT issue

If your PBX is connected behind a router, it can be said that the PBX is behind a Network Address Translation (NAT) router. To allow remote devices to access the PBX, you need to set up NAT rules and port forwarding on the router. In this way, the router will forward the right inbound packets from the internet to the PBX.

SIP-based communication does not reach devices in the Local Area Network (LAN) behind firewalls and NAT routers automatically. Public IP and Ports settings on the Yeastar P-Series 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.

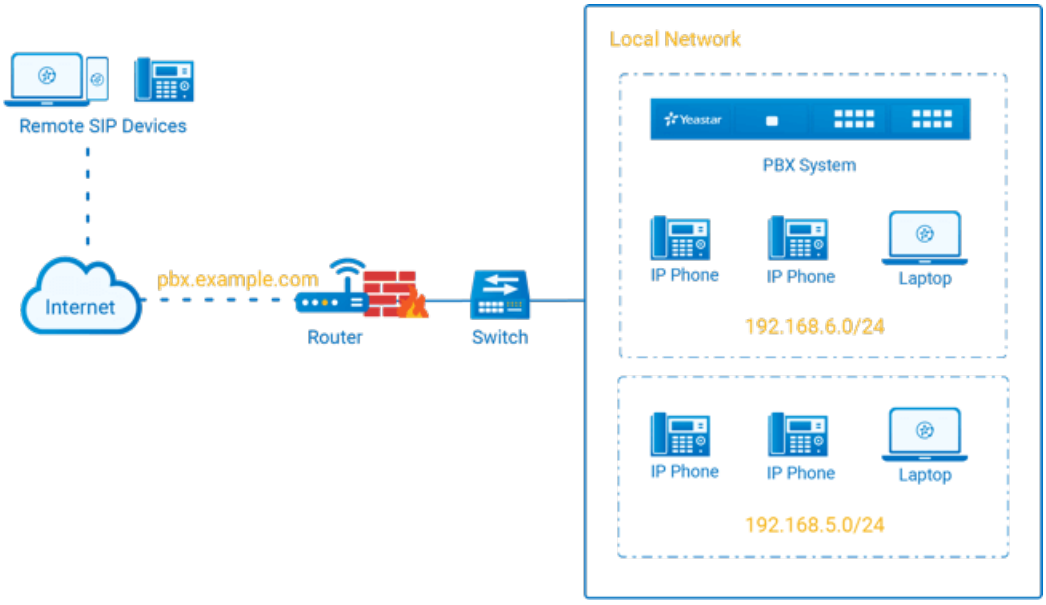
Configure Network for Remote Access by a Domain Name

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.

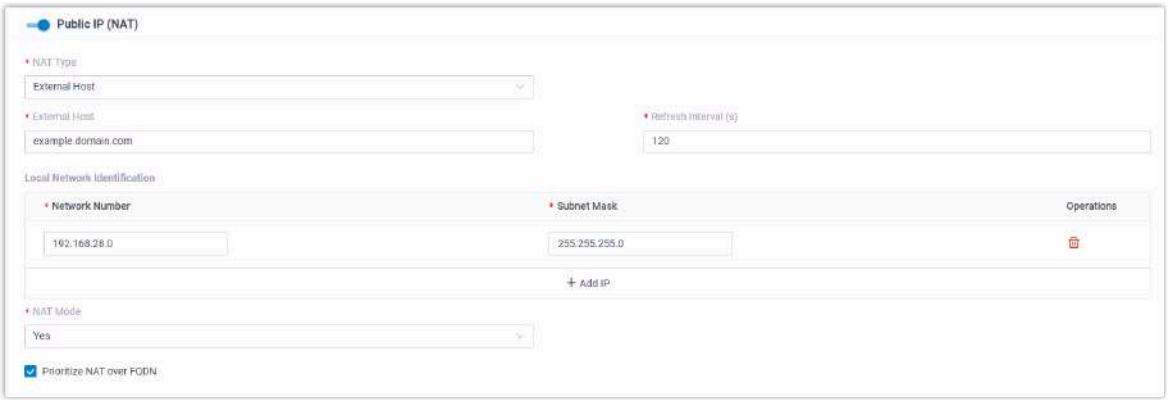
  In this scenario, forward the following ports:

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.

  > **Note:**
  > If a security notice pop-up appears, you can set up allowed country/region IP access protection to better secure remote access.

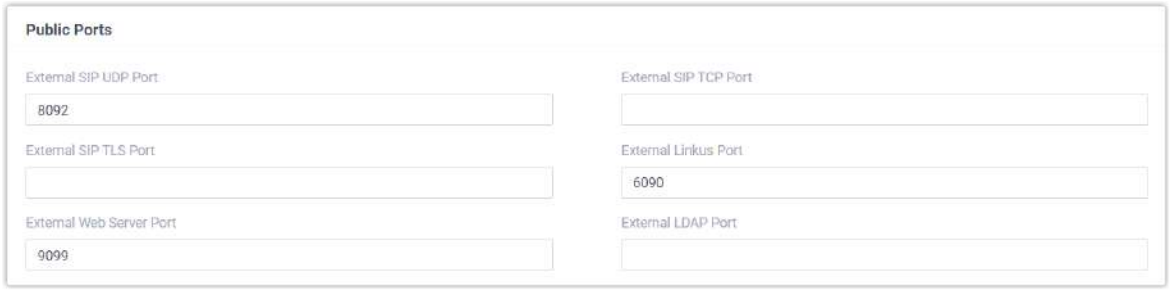
- **NAT Type**: Select **External Host**.
- **External Host**: Enter *example.domain.com*.
- **Refresh Interval (s)**: Leave the default setting or change the interval (in seconds) for PBX to request the external host for public IP.
- **Local Network Identification**: Add all your local network. This setting will allow all your local devices to communicate with the PBX by the local IP address instead of passing through the router.

  In this scenario, add the local network `192.168.28.0/255.255.255.0`.
- **NAT Mode**: Select a SIP NAT mode. In this scenario, select **Yes**.
  - **Yes**: Use NAT and ignore the address information in the SIP/SDP headers and reply to the sender's IP address and port.
  - **No**: Use NAT mode only according to RFC3581.
  - **Never**: Never attempt NAT mode or RFC3581 support.
  - **Route**: Use NAT but do not include Rport in headers.
- **Prioritize NAT over FQDN**: Optional. Specify whether NAT should take precedence over FQDN when both network settings are enabled.

  If this option is enabled, the system will use the NAT address instead of the FQDN when generating remote access URLs, such as Linkus login link, Live Chat embed code, etc.

3. In the **Public Ports** section, enter the external ports that you have forwarded on your router.

> **Note:**
> At least one of the following fields must be filled: **External SIP UDP Port**, **External SIP TCP Port**, or **External SIP TLS Port**.



- **External SIP UDP Port**: Enter *8092*.
- **External SIP TCP Port**: Leave it blank because SIP TCP protocol is not used in this scenario.
- **External SIP TLS Port**: Leave it blank because SIP TLS protocol is not used in this scenario.
- **External Linkus Port**: Enter *6090*.
- **External Web Server Port**: Enter *9099*.
- **External LDAP Port**: Leave it blank because LDAP protocol is not used in this scenario.

4. Click **Save**.

Result

- Users can remotely access the PBX web portal and log in to Linkus clients via the domain name.
- Remote devices based on SIP protocol can register to the PBX via the domain name.
- PBX will generate login links and QR codes for Linkus remote access based on the information provided on the **Public IP and Ports** page.

> **Note:**
> If you have configured network for remote access by a Yeastar FQDN, the login links and QR codes are generated based on the FQDN.

What to do next

To ensure secure communication and protect data integrity, either apply for an HTTPS certificate for the domain through the PBX directly or upload the certificate you have prepared.

Related information

Configure Network for Remote Web Access by a Yeastar FQDN
Configure Network for Remote Access by a Public IP Address
Set up a Remote SIP Phone via Public IP Address and Port

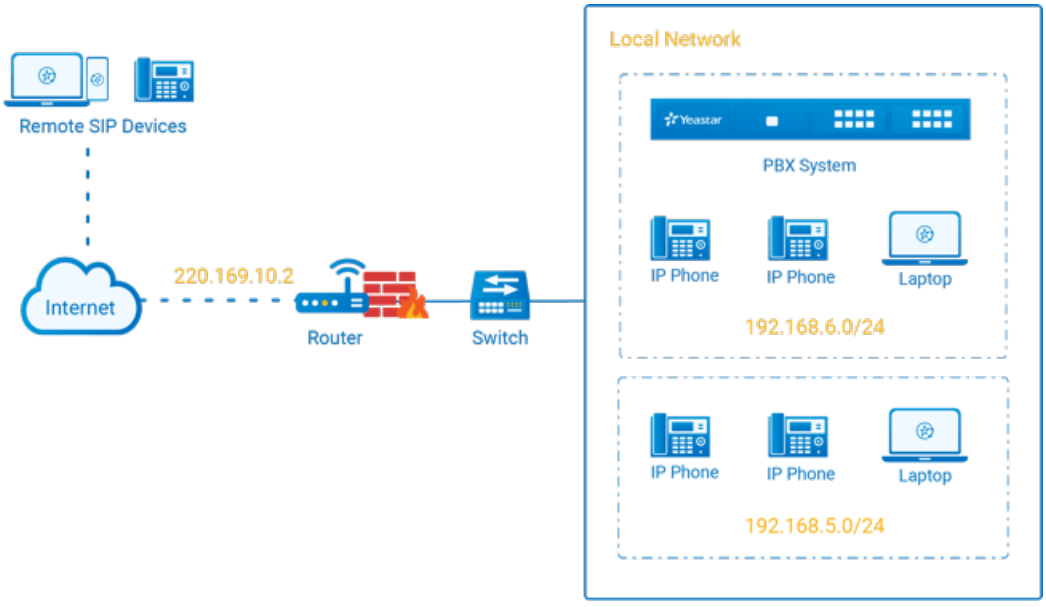
Configure Network for Remote Access by a Public IP Address

To ensure that remote Linkus clients and other SIP devices can communicate with Yeastar P-Series 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.

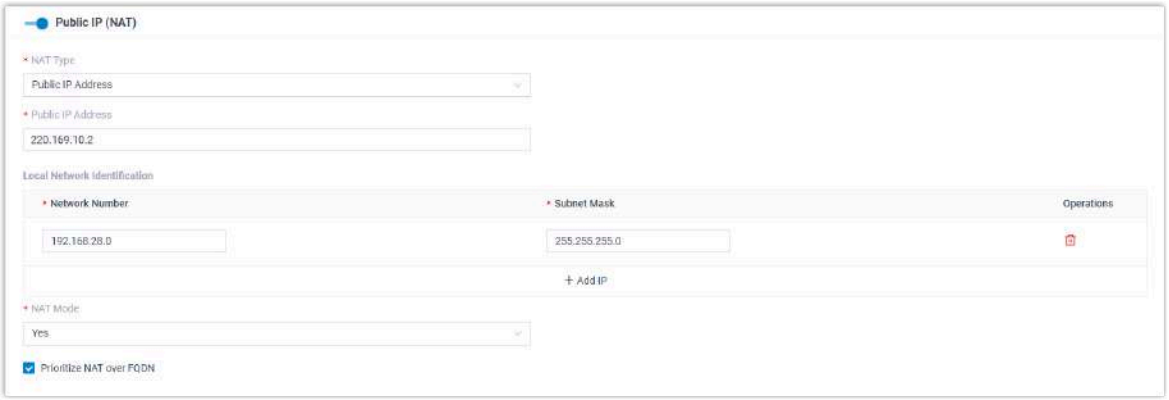
  In this scenario, forward the following ports:

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.

     > **Note:**
     > If a security notice pop-up appears, you can set up allowed country/region IP access protection to better secure remote access.

   - **NAT Type**: Select **Public IP Address** .
   - **Public IP Address**: Enter *220.169.10.2*.

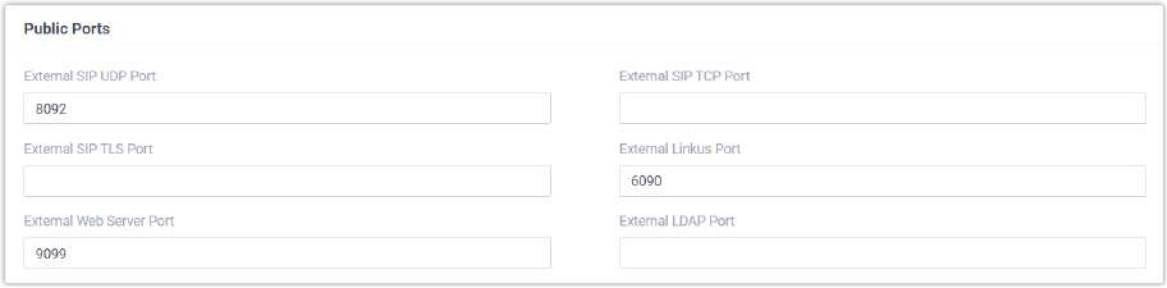
- **Local Network Identification**: Add all your local network. This setting will allow all your local devices to communicate with the PBX by the local IP address instead of passing through the router.

  In this scenario, add the local network `192.168.28.0/255.255.255.0`.
- **NAT Mode**: Select a SIP NAT mode. In this scenario, select **Yes**.
  - **Yes**: Use NAT and ignore the address information in the SIP/SDP headers and reply to the sender's IP address and port.
  - **No**: Use NAT mode only according to RFC3581.
  - **Never**: Never attempt NAT mode or RFC3581 support.
  - **Route**: Use NAT but do not include Rport in headers.
- **Prioritize NAT over FQDN**: Optional. Specify whether NAT should take precedence over FQDN when both network settings are enabled.

  If this option is enabled, the system will use the NAT address instead of the FQDN when generating remote access URLs, such as Linkus login link, Live Chat embed code, etc.

3. In the **Public Ports** section, enter the external ports that you have forwarded on your router.

> **Note:**
> At least one of the following fields must be filled: **External SIP UDP Port**, **External SIP TCP Port**, or **External SIP TLS Port**.



- **External SIP UDP Port**: Enter *8092*.
- **External SIP TCP Port**: Leave it blank because SIP TCP protocol is not used in this scenario.
- **External SIP TLS Port**: Leave it blank because SIP TLS protocol is not used in this scenario.
- **External Linkus Port**: Enter *6090*.
- **External Web Server Port**: Enter *9099*.

- **External LDAP Port**: Leave it blank because LDAP protocol is not used in this scenario.

4. Click **Save**.

Result

- Users can remotely access the PBX web portal and log in to Linkus clients via the public IP address.
- Remote devices based on SIP protocol can register to the PBX via the public IP address.
- PBX will generate login links and QR codes for Linkus remote access based on the information provided on the **Public IP and Ports** page.

> **Note:**
> If you have configured network for remote access by a Yeastar FQDN, the login links and QR codes are generated based on the FQDN.

Related information

Configure Network for Remote Access by a Domain Name
Configure Network for Remote Web Access by a Yeastar FQDN
Set up a Remote SIP Phone via Public IP Address and Port

Configure Network for Remote Access by a Yeastar Domain Name

To ensure that remote Linkus clients and other SIP devices can communicate with Yeastar P-Series Software Edition normally, you need to configure Public IP and Ports on the PBX. This topic provides a configuration example to describe how to easily implement remote connection by setting up a Yeastar-provided domain name.

Prerequisites

- The firmware version of Yeastar P-Series Software Edition is 83.18.0.102 or later.
- If SIP ALG option is provided in your router, disable it.
- You have configured the following settings on the router:
  - Configure a NAT rule to map the PBX server 's private IP address to a public IP address (static or dynamic) supplied by the Internet Service Provider (ISP).

◦ Set up port forwarding rules to forwarded the following ports to allow remote access of Linkus clients and other SIP devices.

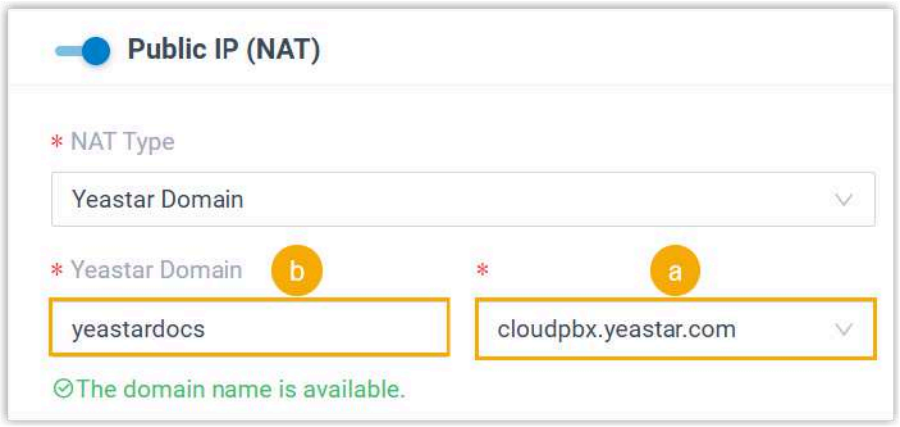
> **Note:**
> To check the relevant internal ports of your PBX, see Manage Service Ports of the PBX.

In this scenario, forward the following ports:

Service	Internal Port	External Port
SIP registration	UDP 5060 (default)	UDP 8092
RTP	UDP 10000-12000 (default)	UDP 10000-12000
Web server	TCP 8088 (default)	TCP 9099
Linkus server	TCP&UDP 8111 (default)	TCP&UDP 6090

Procedure

1. Log in to PBX web portal, go to **System > Network > Public IP and Ports**.
2. Turn on **Public IP (NAT)**.
3. In the **NAT Type** drop-down list, select **Yeastar Domain**.
4. In the **Yeastar Domain** section, set up the Yeastar domain name.



a. Select a domain suffix from the drop-down list.
b. Specify the subdomain in the first field.

> **Note:**

> Think twice before you enter the subdomain, as the Yeastar domain name cannot be changed after you save the configurations.

In this example, you will get a domain name `yeastardocs.cloudpbx.yeastar-.com`.

5. In the **Public IP Type** drop-down list, select the type of public IP address you use, and complete the related settings.
   - To use a static public IP address, do as follows:

     a. Select **Static Public IP Address (IP address does not change)**.
     b. In the **Public IP Address** field, enter your public IP address.
   - To use a dynamic public IP address, do as follows:

     a. Select **Dynamic Public IP Address (IP changes)**.
     b. **Optional:** In the **STUN Server** field, enter the address of your STUN server.

> **Note:**
> If left empty, Yeastar's STUN server will be used by default.

     c. In the **Refresh Interval (s)** field, specify the time interval for the PBX to request the STUN server for public IP.

     The default value is 120, and the available value should be an integer between 30 and 3600.
6. **Local Network Identification**: Add all your local network. This setting will allow all your local devices to communicate with the PBX by the local IP address instead of passing through the router.

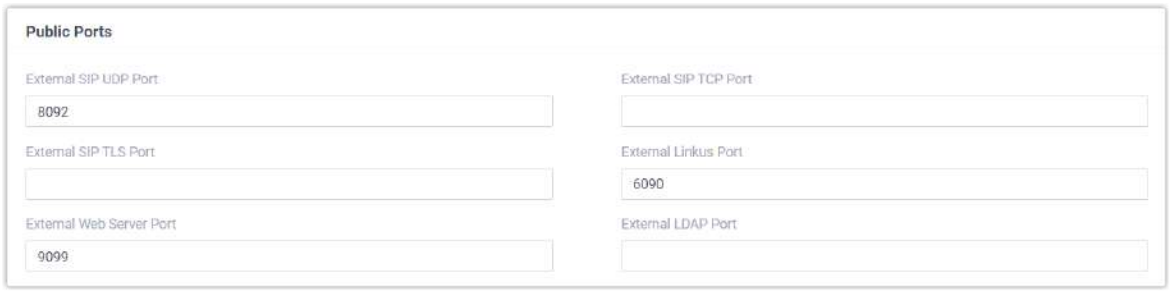
   In this scenario, add the local network `192.168.28.0/255.255.255.0`.
7. **NAT Mode**: Select a SIP NAT mode. In this scenario, select **Yes**.
   - **Yes**: Use NAT and ignore the address information in the SIP/SDP headers and reply to the sender's IP address and port.
   - **No**: Use NAT mode only according to RFC3581.

- **Never**: Never attempt NAT mode or RFC3581 support.
- **Route**: Use NAT but do not include Rport in headers.

8. **Prioritize NAT over FQDN**: Optional. Specify whether NAT should take precedence over FQDN when both network settings are enabled.

   If this option is enabled, the system will use the NAT address instead of the FQDN when generating remote access URLs, such as Linkus login link, Live Chat embed code, etc.
9. In the **Public Ports** section, enter the external ports that you have forwarded on your router.

   > **Note:**
   > At least one of the following fields must be filled: **External SIP UDP Port**, **External SIP TCP Port**, or **External SIP TLS Port**.

   - **External SIP UDP Port**: Enter *8092*.
   - **External SIP TCP Port**: Leave it blank because SIP TCP protocol is not used in this scenario.
   - **External SIP TLS Port**: Leave it blank because SIP TLS protocol is not used in this scenario.
   - **External Linkus Port**: Enter *6090*.
   - **External Web Server Port**: Enter *9099*.
   - **External LDAP Port**: Leave it blank because LDAP protocol is not used in this scenario.
10. Click **Save**.

Result

- Once the configuration is completed, the PBX will automatically apply for a certificate for the Yeastar domain name. The certificate can be check on **Security > Security Settings > Certificates**, and will be automatically renewed before it expires.

- The followings remote access features can be implemented:
  - Users can remotely access the PBX web portal and log in to Linkus clients via the Yeastar domain name.
  - Remote devices based on SIP protocol can register to the PBX via the domain name.
  - The login links and QR codes for Linkus remote access are generated based on the information provided on the **Public IP and Ports** page.

> **Note:**
> If you have configured network for remote access by a Yeastar FQDN, the login links and QR codes are generated based on the FQDN.

Static Route

Static Route Overview

This topic provides an overview of static route table and all associated system routes.

Route table

Yeastar P-Series 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

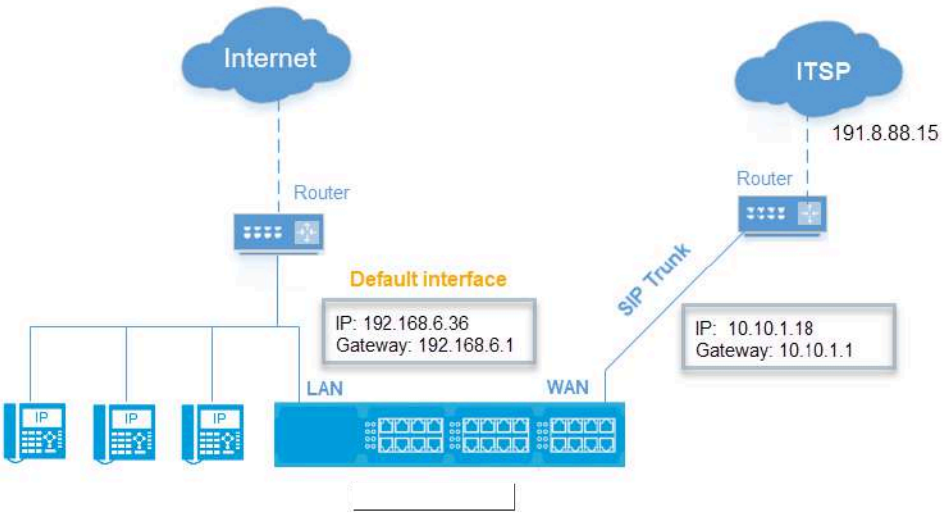
Adding custom static route is typically used in the "Dedicated SIP trunking" scenario.

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

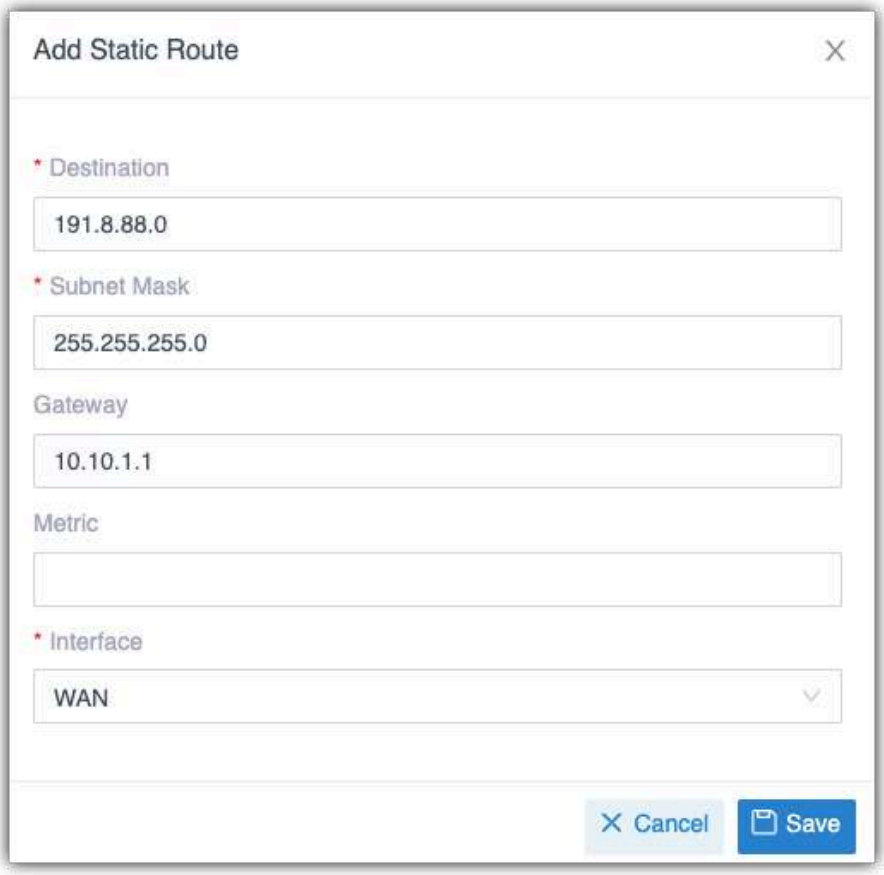
Setting	Value
Ethernet Mode	Dual
Default Interface	LAN
LAN	
IP Address	192.168.6.36
Subnet Mask	255.255.255.0
Gateway	192.168.6.1
Preferred DNS Server	192.168.1.1
WAN	
IP Address	10.10.1.18
Subnet Mask	255.255.255.0
Gateway	10.10.1.1
Preferred DNS Server	10.10.1.1

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:



- **Destination**: Enter the destination IP address or IP subnet for the PBX to reach using the static route.

  > **Note:**
  > To ensure that both SIP registration packets and SIP media packets can be routed to the desired destination, set the IP range of the SIP trunking. In this scenario, enter *191.8.88.0*.

- **Subnet Mask**: Enter the subnet mask for the destination address. In this scenario, enter *255.255.255.0*.
- **Gateway**: Enter the gateway address. The PBX will reach the destination address through this gateway. In this scenario, enter *10.10.1.1*.
- **Metric**: Optional.

  Routing metric is used to determine whether one route should be chosen over another.
- **Interface**: Select the network interface.

The PBX will reach the destination address using the static route through the selected network interface. In the scenario, select **WAN**.

3. Click **Save** and **Apply**.

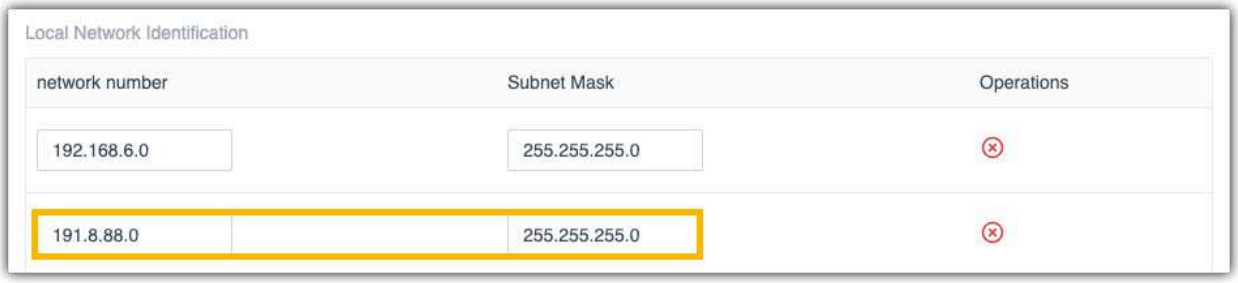
Result

After you set up a SIP trunk with the IP address 191.8.88.15 on the PBX, the SIP packets are sent and received by the WAN port, which ensure the communication between the PBX and the ITSP.

What to do next

To avoid SIP audio issues through the SIP trunk, you may need to add the network segment of the SIP trunk as a local network identification in PBX NAT settings.

In this scenario, add the IP segment 191.8.88.0/255.255.255.0 in the NAT settings as the following figure shows. For more information of NAT, see Configure Network for Remote Access by a Domain Name.



Manage Static Routes

After you add static routes on the Yeastar P-Series 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**: Specify the IP address of the default gateway for the DHCP server.
- **Subnet Mask**: Specify the subnet mask used to subdivide your IP address.
- **Preferred DNS Server**: Specify a DNS server for the DHCP server.
- **Alternative DNS Server**: Optional. Specify a secondary DNS server for the DHCP server.
- **DHCP Address Range**: Specify the IP address range that will be allocated to DHCP clients.

- **NTP Server**: Enter the IP address of an NTP server.

  > **Tip:**
  > The default value is the IP address of the PBX, which can synchronize the network time of the client devices with the PBX.

4. Click **Save**.

   The **Status** field displays **Running**, indicating the DHCP server is running.

Result

The PBX can now be used as a DHCP server and assign IP addresses, gateway, and other network configurations to the devices located in the local network.

Split DNS

Set up Split DNS

Split DNS allows extension users to seamlessly access and use their Linkus clients via the same domain name, whether they are inside the office or working remotely, which improves access speed and reliability. This topic describes how to set up split DNS in a typical company network.

Introduction

Split DNS allows the same domain name to be resolved to different IP addressed based on the user's network location:

- For external users, the domain resolves to the public IP address of the PBX system (e.g. `203.0.113.10`).

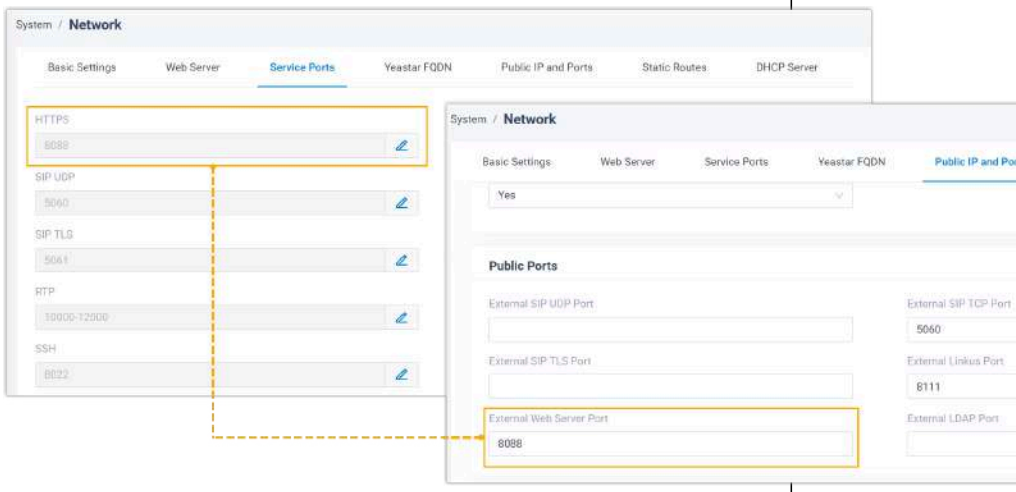
  This resolution is typically handled by public DNS servers, which rely on DNS records (such as A records) configured when the domain name is registered or managed with your domain registrar.
- For internal users, the domain resolves to the private IP address of the PBX system (e.g. `192.168.28.39`).

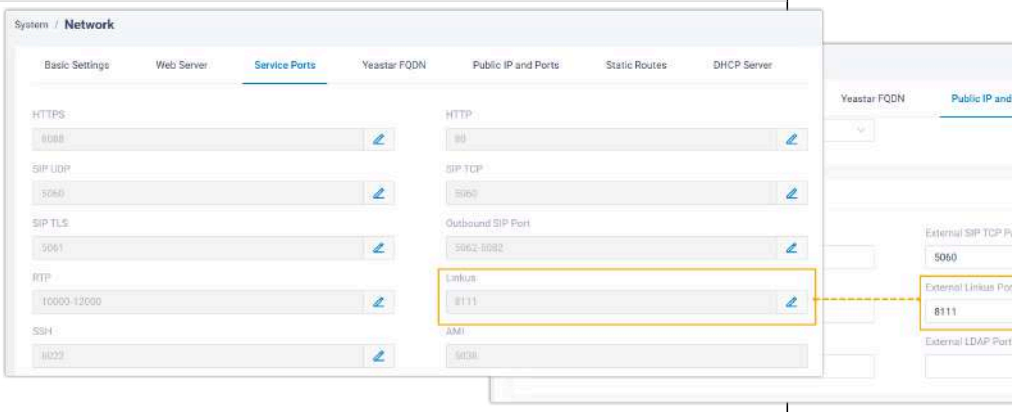
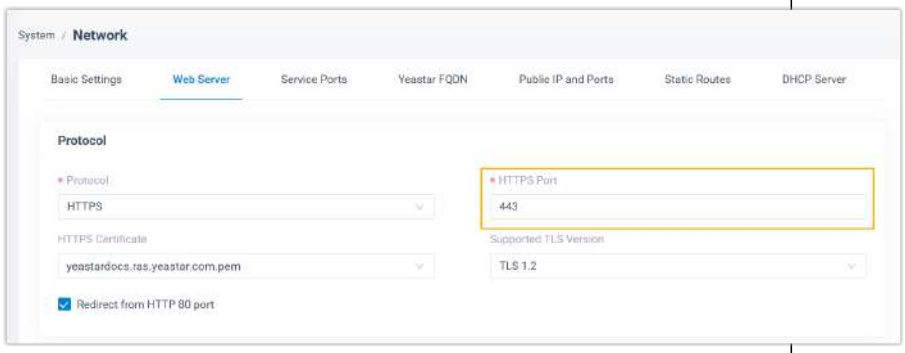
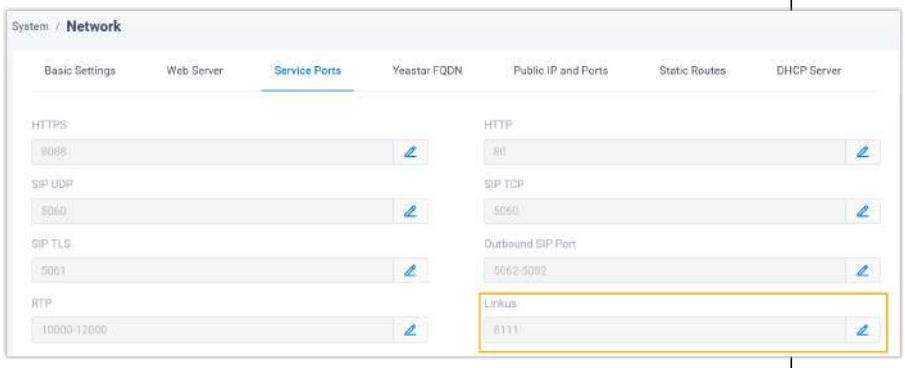
  This depends on your company's network configuration. It is recommended to implement this functionality on a firewall or router, if supported by the vendor. Alternatively, you can configure an internal DNS server to manage internal domain resolution. This

guide uses Microsoft DNS server as an example to demonstrate how to configure internal DNS resolution.

Prerequisites

To implement split DNS, make sure the followings are in place:

Item	Description
Domain	• You have a valid domain name (custom or Yeastar-provided) which will be used for both internal and external access. • The PBX has been configured for remote access via the domain name. For more information about the configurations, see the following topics: ◦ Configure Network for Remote Web Access by a Yeastar FQDN ◦ Configure Network for Remote Access by a Domain Name ◦ Configure Network for Remote Access by a Yeastar Domain Name
Port	Configure the ports for PBX server based on the domain type. • **For domains requiring NAT traversal (e.g. External Host & Yeastar Domain)** ◦ The external web server port should be mapped to the same port as the HTTPS port.  ◦ Ensure the external Linkus port is the same as the internal Linkus port.

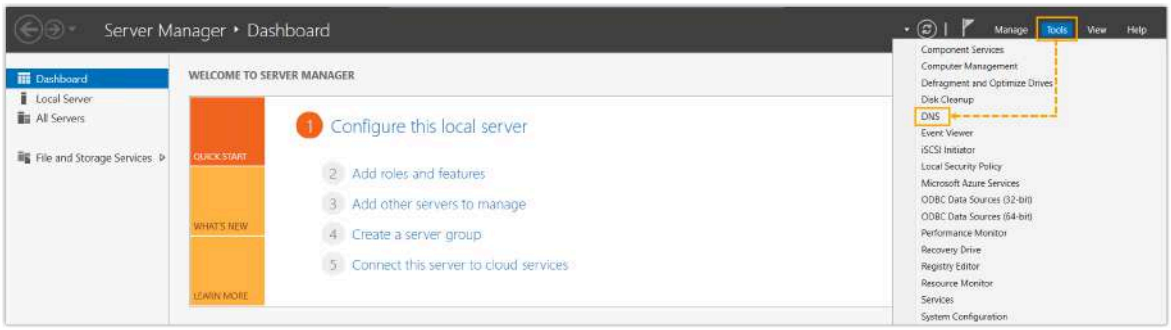
Item	Description
	 • **For Yeastar FQDN** ◦ The HTTPS port should be set to **443** for optimal performance (Path: **System > Network > Web Server > Protocol > HTTPS Port**).  ◦ Ensure the internal Linkus port is fixed at **8111** (Path: **System > Network > Service Ports > Linkus**). 
Internal DNS Server	A Microsoft DNS Server has been deployed within the company's internal network to handle internal domain resolution.

Procedures

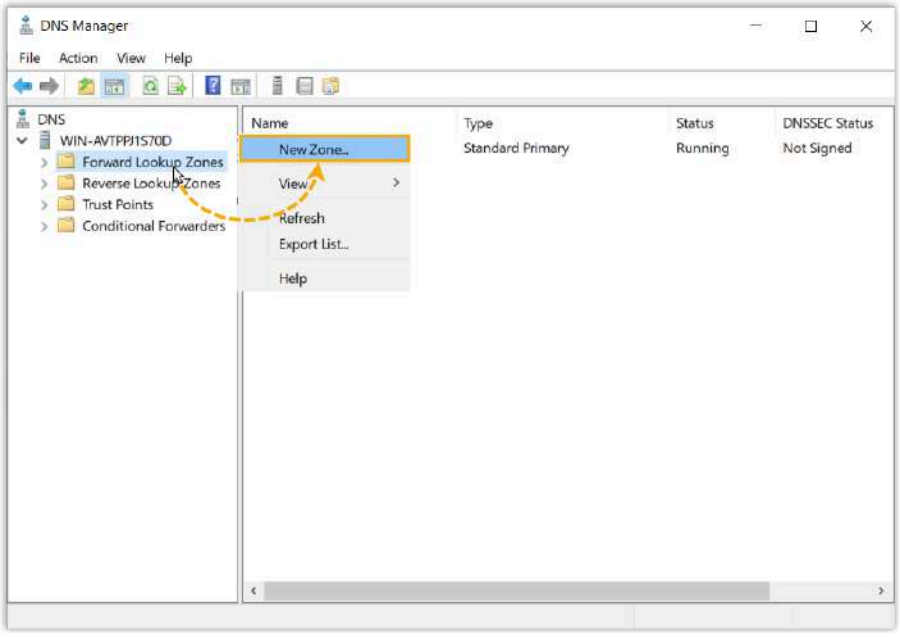
1. Create an internal DNS record
2. Verify internal DNS resolution
3. Enforce internal DNS usage for user devices

Create an internal DNS record

1. At the top-right of the Server Manager window on Windows Server, go to **Tools > DNS** to open the DNS manager.

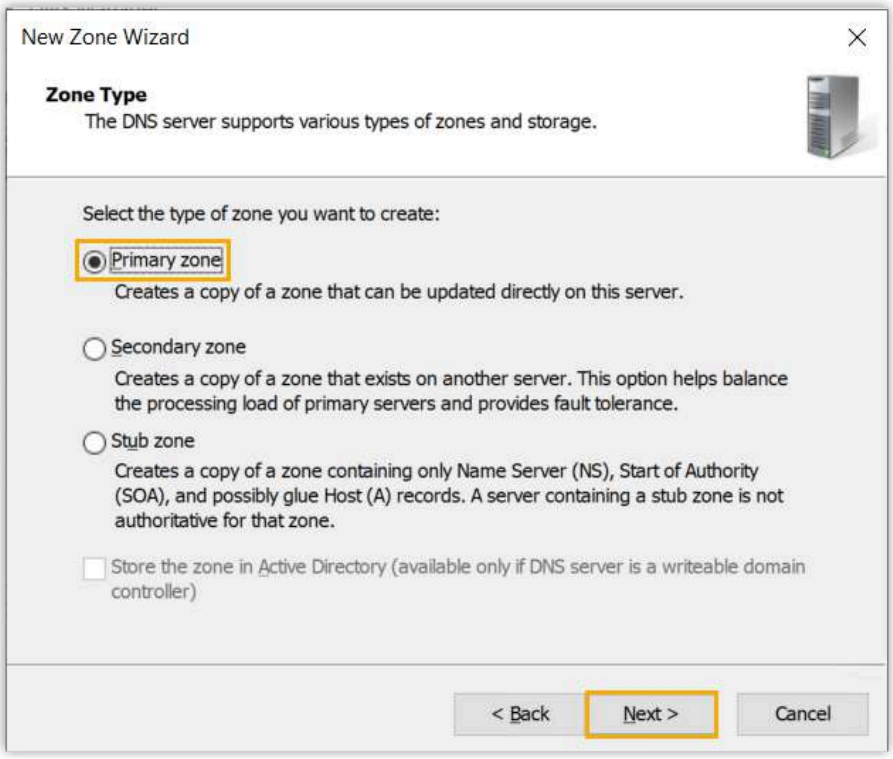


2. Add a Forward Lookup Zone.
   a. Right click **Forward Lookup Zones**, then select **New Zone...**.

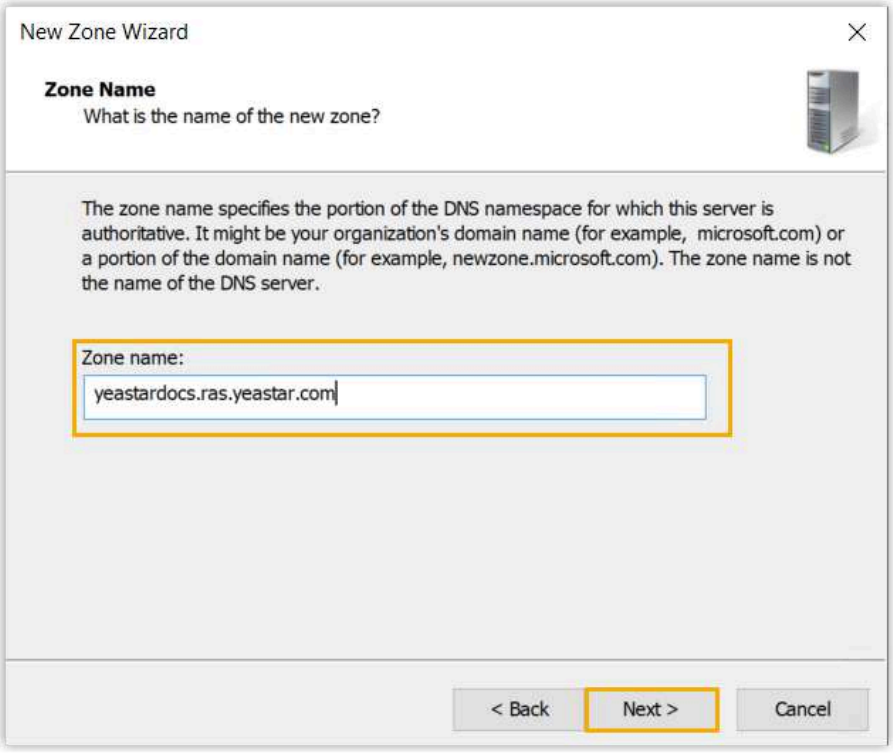


   The New Zone Wizard will open.
   b. On the wizard, click **Next** to continue.

c. In the **Zone Type** page, leave the default option **Primary zone** selected, then click **Next**.



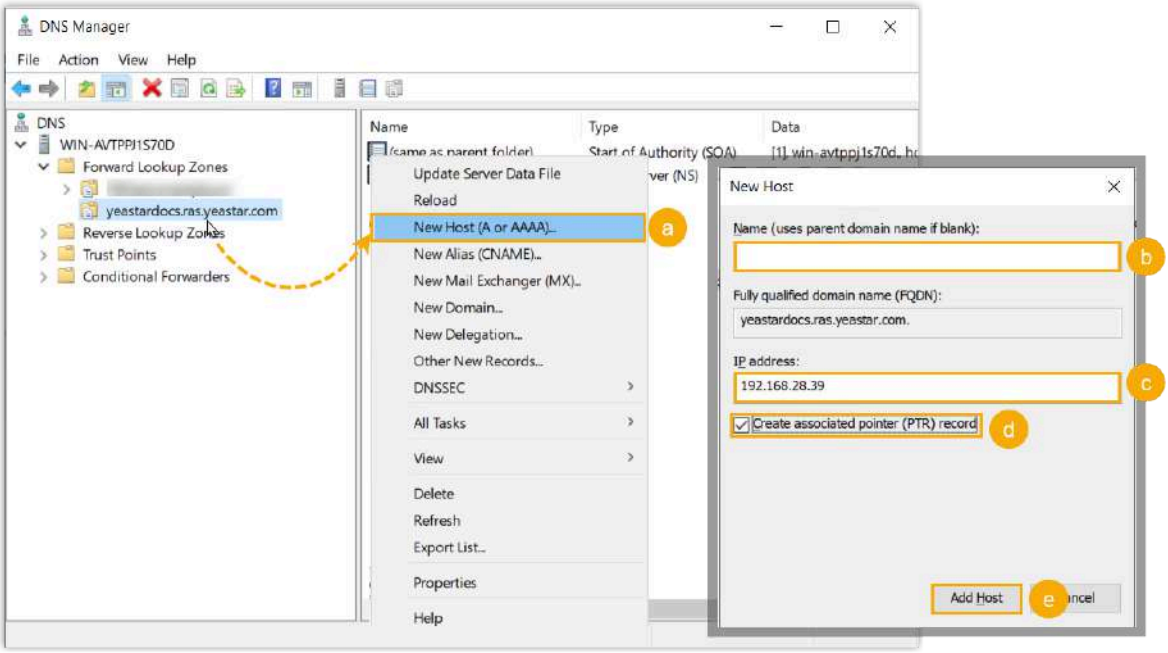
d. In the **Zone Name** page, enter the domain name of the PBX, then click **Next**.



e. On the remaining pages, keep the default settings and click **Next** until you reach the final step.

f. Click **Finish** to complete the setup.

3. Add a new host.

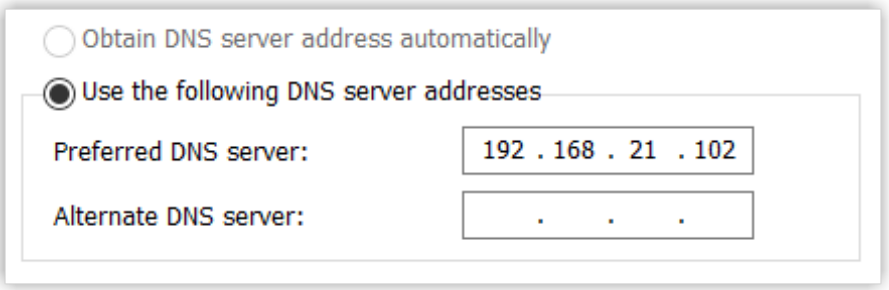


a. Right click on the domain name you added, then select **New Host (A or AAAA)...**.
b. Leave the **Name** field empty, which means the parent domain will be used.
c. In the **IP address** field, enter the private IP address of the PBX system.
d. **Optional:** To enable reverse DNS lookup, select the checkbox of **Create associated PTR record**.
e. Click **Add Host**.

   A dialog box pops up to indicate that the host record is successfully created, click **OK** to close.

Verify internal DNS resolution

1. Configure your computer to use the internal DNS server.
   a. On your computer, press **Win+R** to open the **Run** dialog box.
   b. Type `ncpa.cpl`, then press **Enter**.
   c. In the **Network Connections** window, right click your active network connection, then go to **Properties**.
   d. Double click the **Internal Protocol Version 4 (TCP/IPv4)**.
   e. Select **Use the following DNS server addresses**, then enter the IP address of the internal DNS server (E.g. `192.168.21.102`).



   f. Click **OK** to save the settings, then click **OK** again to close the window.
2. Test internal DNS resolution on your computer.

> **Tip:**
> For external DNS resolution, you can verify using an online DNS checker to see if the domain name is correctly resolved to the PBX's public IP address.

   a. On your computer, press **Win+R** to open the **Run** dialog box.
   b. Type `cmd`, then press **Enter**.

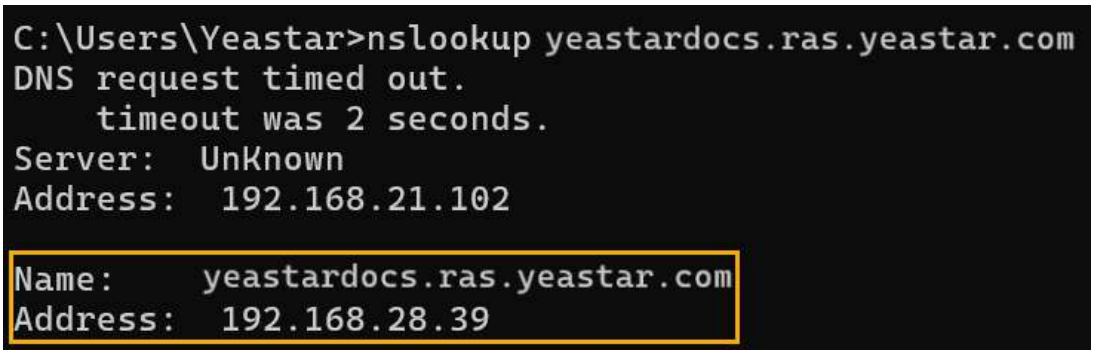
c. In the **Command Prompt** window, enter the following command and press **Enter**.

```
nslookup {your PBX's domain name}
```

For example,

```
nslookup yeastardocs.ras.yeastar.com
```

The output returns the private IP address of the PBX, indicating that the internal DNS resolution is configured successfully.



Enforce internal DNS usage for user devices

To ensure Split DNS works properly, user devices must use the internal DNS server when connected to the company network.

1. Configure DHCP server to assign internal DNS.

   Set the DHCP scope options to assign the IP address of the internal DNS server as the primary DNS for all devices connected to the corporate network.
2. **Optional:** Block external DNS requests on firewall.

   On the company's firewall, block outbound DNS requests (UDP/TCP port 53) to public DNS servers to prevent clients from bypassing the internal DNS.
3. Connect user devices to the company network.

Client Type	Connection Method
Linkus Web / Desktop Client	• Connect user's computer to the company's Wi-Fi to automatically obtain the internal DNS server via DHCP. **Note:** This method is recommended to avoid manual switching DNS settings when moving between different networks.

Client Type	Connection Method
	• If user's computer uses a static IP configuration, manually specify the internal DNS server address in the network settings.
Linkus Mobile Client	Connect to company's Wi-Fi to obtain internal DNS via DHCP.

Result

Extension users can access their Linkus clients using the same domain name from both internal and external networks, eliminating the need to manually switch between different addresses and ensuring a consistent login experience.

Date and Time

Change System Time Manually

In case you want to change system time when the PBX can not access the Internet, you can change system time manually. This topic describes how to manually change system time to your local time.

Background information

To ensure that the time of logs and CDRs generated on Yeastar P-Series 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.

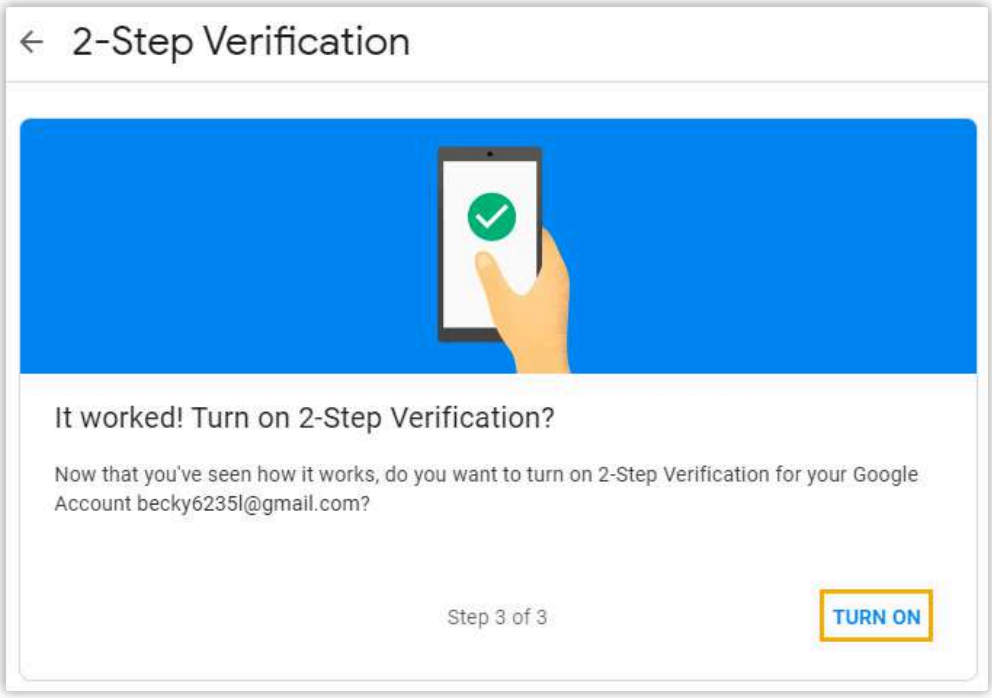
Prerequisites

Make sure Yeastar P-Series Software Edition can access Google Server.

Step1. Create an app password on Google Account

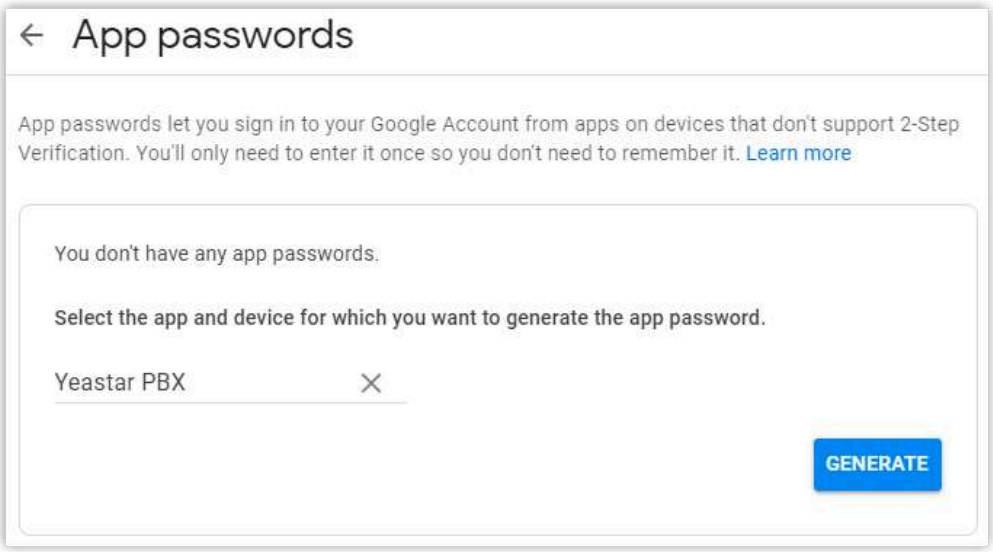
To ensure that the PBX can access Gmail server, you need to turn on 2-Step verification and create an app password as follows.

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.

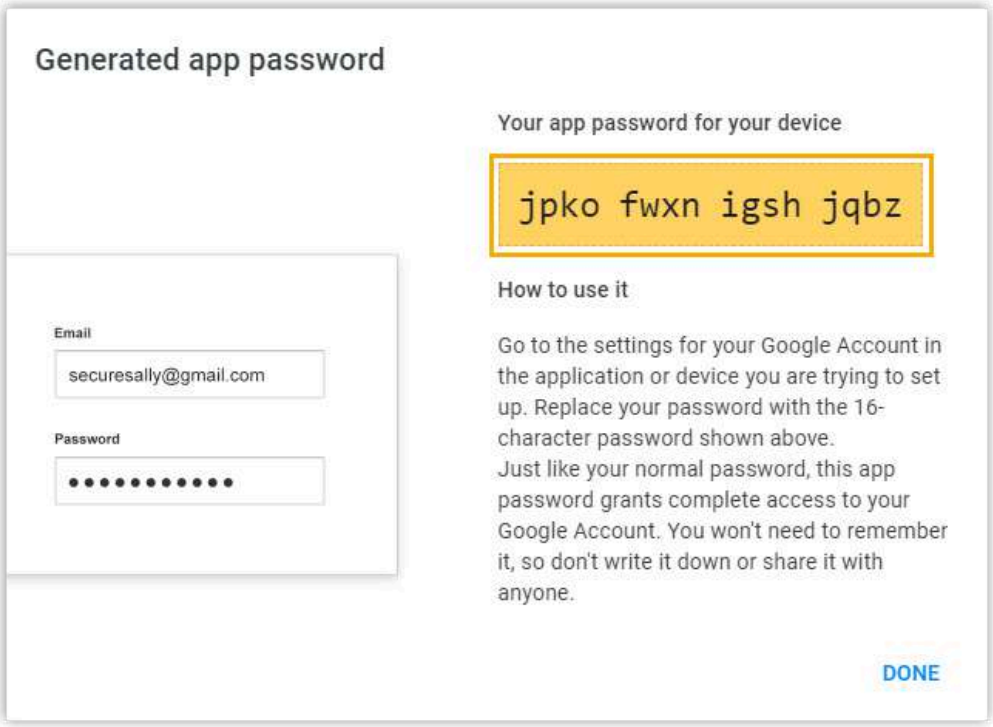


4. Right above the page, click ← to back to the security page.
5. Create an app password.
    a. In the **Signing in to Google** section, click **App passwords** and enter your Gmail password to verify your account.
    b. In the **Select app** drop-down list, select **Other (Custom name)**.

c. In the text field, enter a name to help you identify the app password. For example, enter *Yeastar PBX*.
d. Click **GENERATE**.



An app password is generated. Note down the password, which is used to verify your Gmail account when you configure Gmail as the mail server in the PBX.



Step2. Configure Gmail as mail server of Yeastar P-Series 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. In the **Select Email Server Provider** drop-down list, select **General**.
4. Configure email server settings.
    - **Sender Email Address**: Enter your Gmail address, which will appear as the From address for outgoing emails sent by the PBX.
    - **Email Address or Username**: Enter your Gmail address.
    - **Password**: Enter the 16-digit app password, which is used to access Gmail server.
    - **Outgoing Mail Server (SMTP)**: Retain the default value *smtp.gmail.com*.
    - **Port**: Retain the default value *587*.
    - **Enable TLS Encryption**: Keep the option unselected.
5. Test if the mail server can successfully send emails.
    a. Click **Test**.
    b. In the pop-up window, enter a recipient's email address in the **Email Address** field.
    c. Click **Test**.
6. Click **Save**.

Result

- If the test email is sent successfully, the page displays "Success" and the recipient's mailbox would receive the email.
- If the test email is failed to be sent, the page displays "Failed to send" and prompts you an error message. You can check the error in Email Sent Logs.

Set up Outlook as an Email Server

This topic describes how to set up Microsoft Outlook as the email server for Yeastar P-Series Software Edition using modern authentication. This allows the PBX to send and receive emails through your Microsoft account.

Requirements

Platform	Requirement
PBX server	• **Firmware**: Version 83.18.0.102 or later • **Plan**: Enterprise Plan (EP) or Ultimate Plan (UP) • The PBX can be remotely accessed. For more information about the configuration, see the following topics: ◦ Configure Network for Remote Access by a Yeastar FQDN ◦ Configure Network for Remote Access by a Yeastar Domain Name ◦ Configure Network for Remote Access by a Domain Name ◦ Configure Network for Remote Access by a Public IP Address
Microsoft 365	• A Microsoft account that meets the following requirements: **Note:** The account will be used as the designated email sender for the SMTP server. ◦ Assigned with the **Global Administrator** role. ◦ Assigned with **Microsoft 365 Business Standard** license. • The modern authentication is enabled in Microsoft 365 admin center.

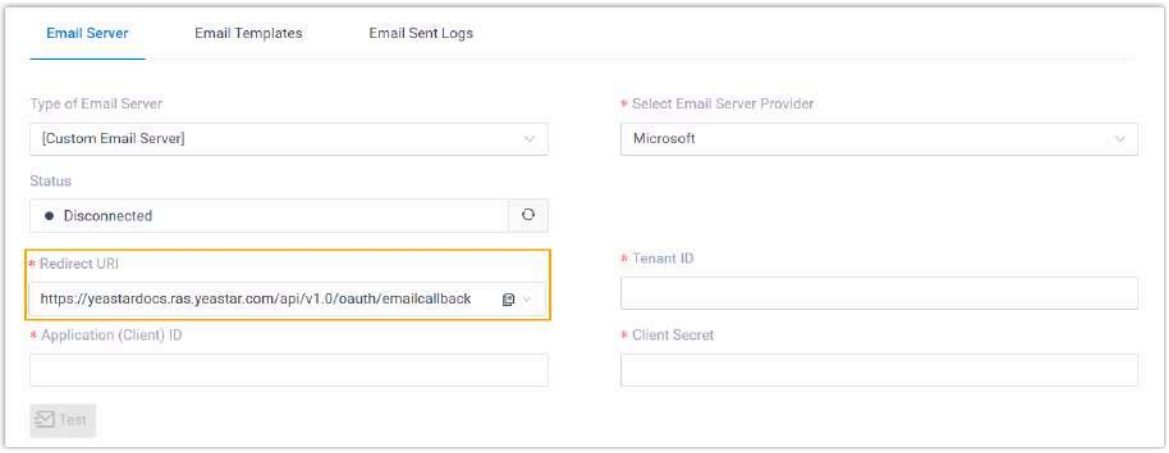
Procedure

- Step 1. Obtain redirect URI from PBX
- Step 2. Register an application on Microsoft Entra ID
- Step 3. Configure SMTP settings on PBX

Step 1. Obtain redirect URI from PBX

Obtain the redirect URI from Yeastar P-Series Software Edition, which will be required when registering a Microsoft Entra application later.

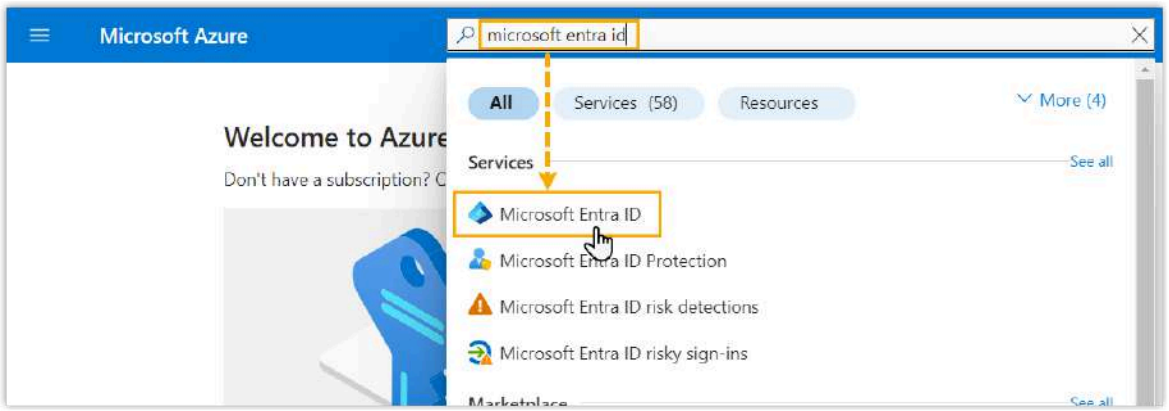
1. Log in to PBX web portal, go to **System > Email > Email Server**.
2. In the **Type of Email Server** drop-down list, select **Custom Email Server**.
3. In the **Select Email Server Provider** drop-down list, select **Microsoft**.
4. In the **Redirect URI** field, select and copy the desired redirect URI.



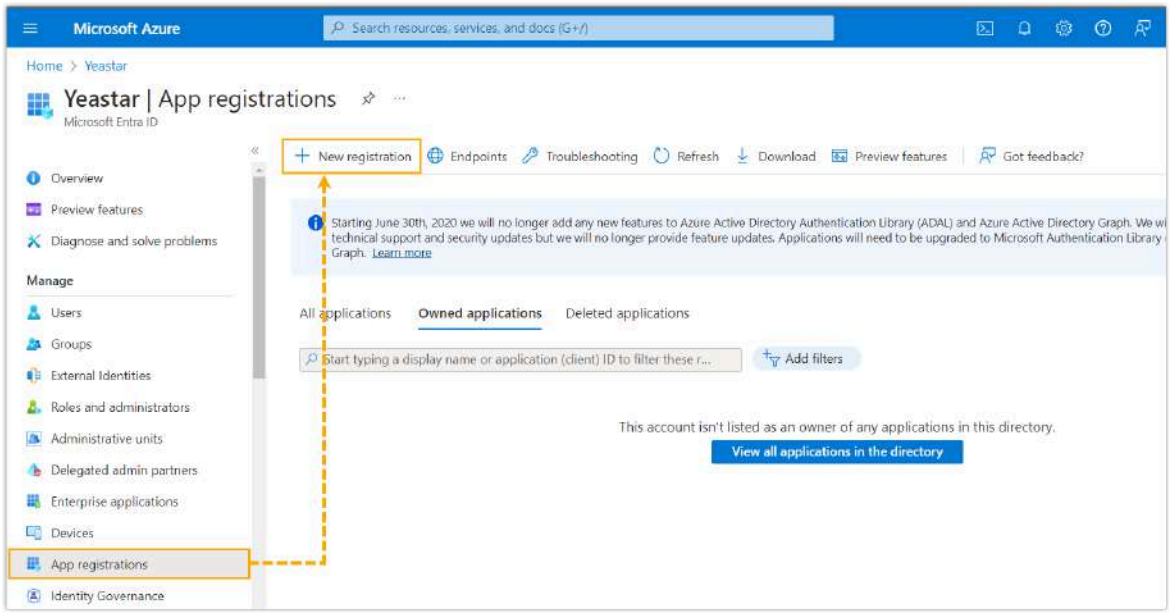
Step 2. Register an application on Microsoft Entra ID

Register an application on Microsoft Entra ID with the redirected URI provided by Yeastar PBX, then obtain the application authentication information for SMTP settings on PBX.

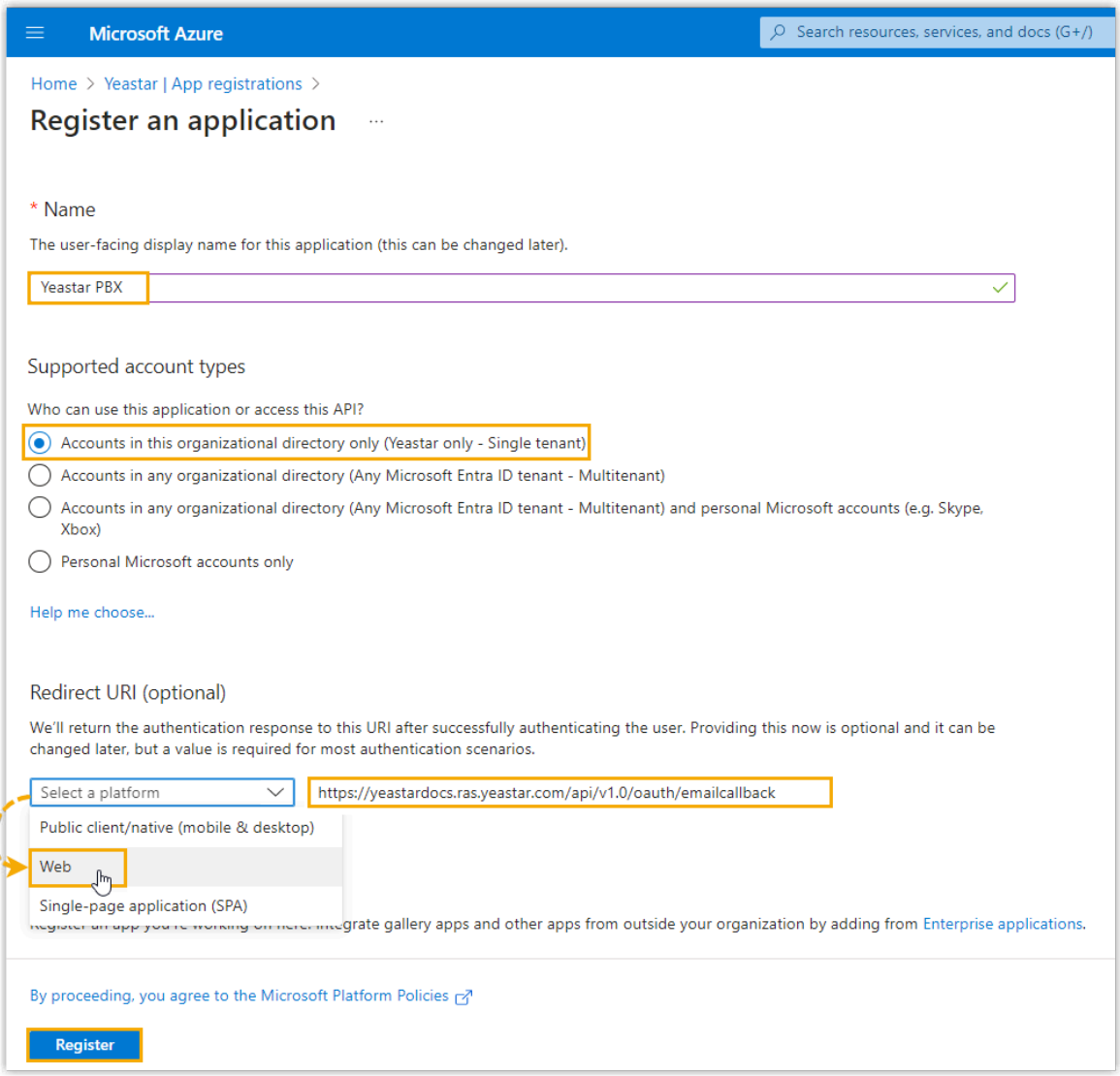
1. Log in to Microsoft Azure Portal with the Microsoft Administrator account.
2. In the search bar, search and select **Microsoft Entra ID** service to enter your organization's directory.



3. On the left navigation bar of organization's directory, go to **App registrations**, then click **New registration**.



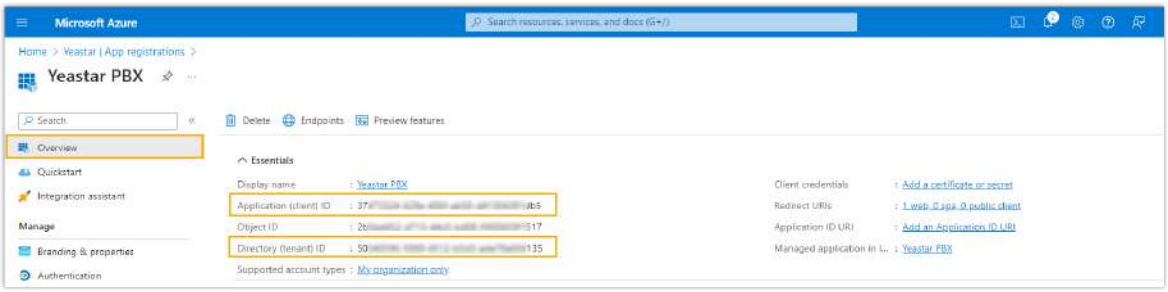
4. In the **Register an application** page, configure the registration information for the application, and click **Register**.



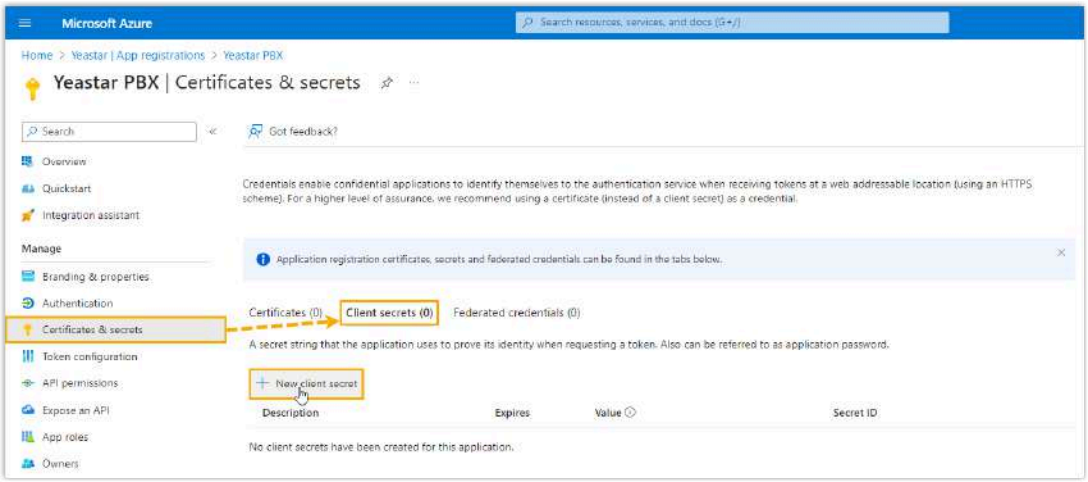
- **Name**: Specify a name to help you identify the application.
- **Supported account types**: Select **Accounts in this organizational directory only**.
- **Redirect URI**: In the **Select a platform** drop-down list, select **Web**, then paste the Redirect URI obtained from the PBX.

An application is registered successfully, you are redirected to the **Overview** page of the application.

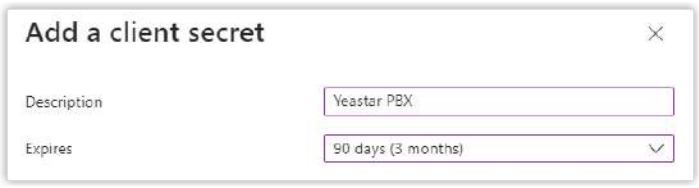
5. Note down the **Application (client) ID** and **Directory (tenant) ID** of the application, as you will need to fill them into the PBX later.



6. Generate a client secret for the application.
   a. On the left navigation bar of the application, go to **Certificates & secrets > Client secrets**, then click **New client secret**.



   b. In the **Add a client secret** page, add a description and set an expiration date for the client secret, then click **Add**.



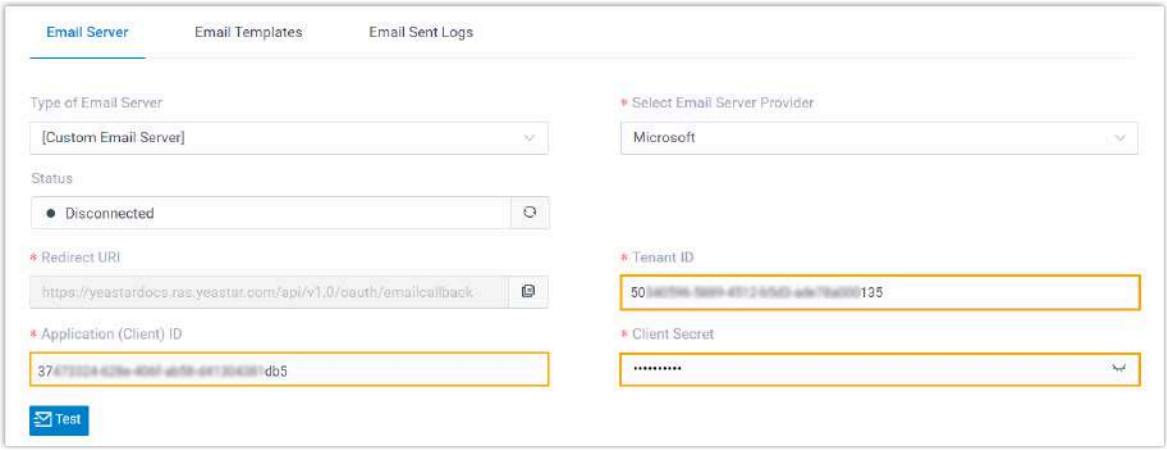
   A client secret is created and displayed in the **Client secrets** list.
   c. Note down the client secret's **Value** as you will need to fill it into the PBX later.

> **Important:**
> Record the client secret's value before leaving the page, as the key is only shown once. Otherwise, you will have to create a new client secret.

Step 3. Configure SMTP settings on PBX

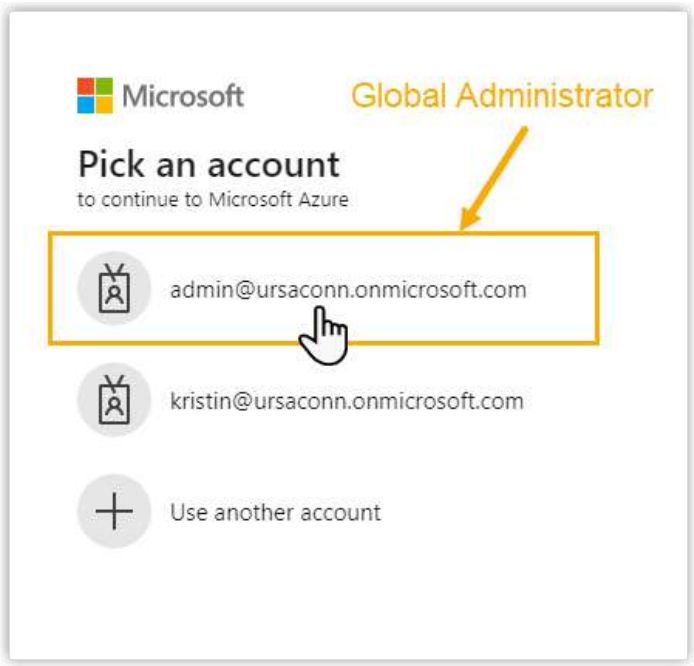
Configure the SMTP settings of the PBX with the authentication information obtained from the Microsoft Entra application, so as to set Microsoft Outlook as the PBX's email server.

1. Log in to PBX web portal, go to **System > Email > Email Server**.
2. In the **Type of Email Server** drop-down list, select **Custom Email Server**.
3. In the **Select Email Server Provider** drop-down list, select **Microsoft**.
4. Enter the following authentication information.

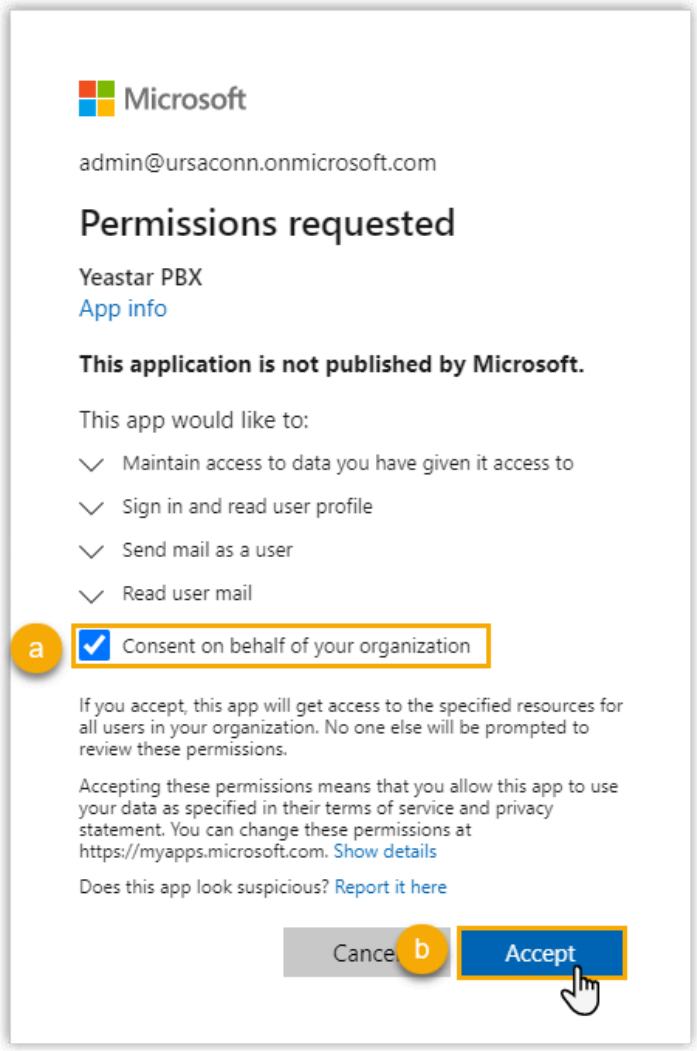


   - **Tenant ID**: Paste the Tenant ID of the Microsoft Entra application.
   - **Application (Client) ID**: Paste the Application ID of the Microsoft Entra application.
   - **Client Secret**: Paste the client secret of the Microsoft Entra application.
5. Click **Save**.

   You are redirect to the Microsoft Sign-in page.
6. Sign in with the Microsoft account that has **Global Administrator** privilege.



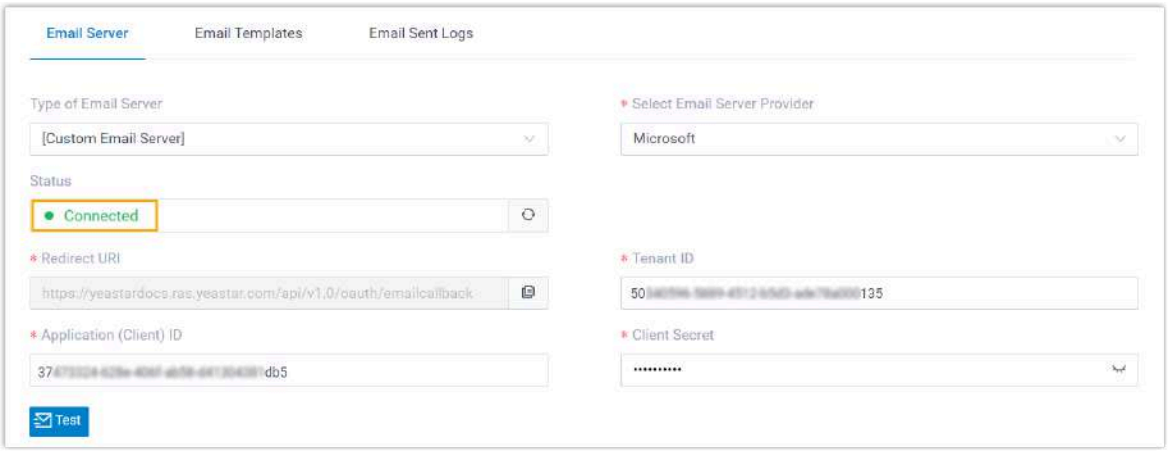
7. In the pop-up window, do as follows to confirm:



a. Select the checkbox of **Consent on behalf of your organization**.

b. Click **Accept**.

On the PBX configuration page, the **Status** field displays **Connected**, indicating that the Microsoft authentication is successful; The Microsoft Outlook is set up as the email server.



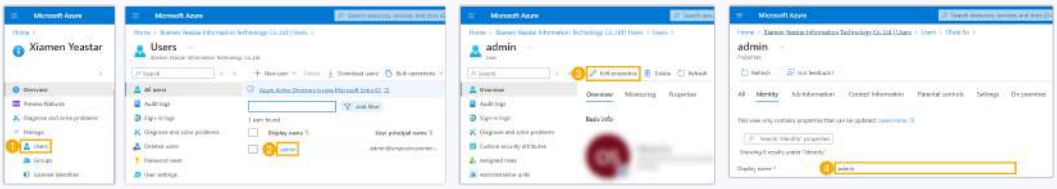
8. Test if the mail server can successfully send emails.
    a. Click **Test**.
    b. In the pop-up window, enter a recipient's email address in the **Email Address** field, then click **Test**.

Result

A test email is sent successfully using the Microsoft account; The page displays "Success" and the recipient's mailbox would receive the email where the sender name and email address are the Microsoft account's display name and user principal name respectively. For example, `admin<admin@ursaconn.onmicrosoft.com>`.

Note:

- If you want to change the sender name of the emails sent by the SMTP server, change the display name of the Microsoft account, as shown below:



- If the test email is failed to be sent, the page displays "Failed to send" and prompts you an error message.

Customize Email Templates

This topic describes how to customize email notification language and email templates.

Background information

If you have enabled notification for a specific event, and have chosen to send emails to notify contacts, the system will send emails in the pre-configured email template to inform contacts when the event is triggered.

Yeastar P-Series 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

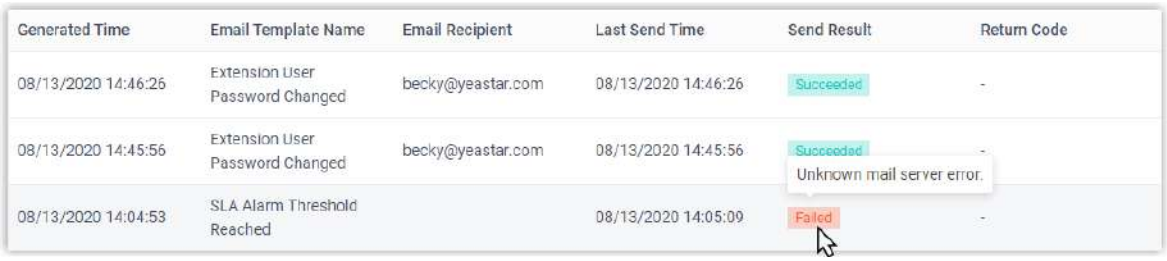
By default, when logs reach 50,000, the newest logs will replace the oldest logs. You can change the value, or restrict how long logs can be saved.

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.



Storage

Storage Overview

Yeastar P-Series Software Edition provides local storage and supports external storage and network drive storage.

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
- External Chat Files

- Backup files

For more information, see Manage Storage Locations.

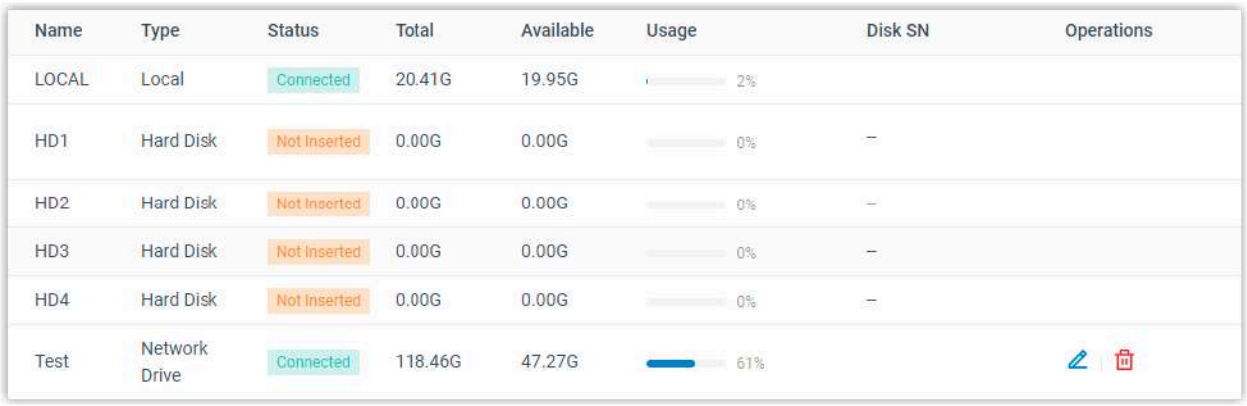
By default, data will be periodically cleared when it reaches the system limit. For more information, see Auto Cleanup Settings.

Storage devices

The **Storage Devices** section shows the local storage, external storage, and network drive. You can click specific icons to manage storage devices.

- Click to refresh the status.
- Click to edit network drive settings.
- Click to delete a network drive.
- Click to format 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

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.

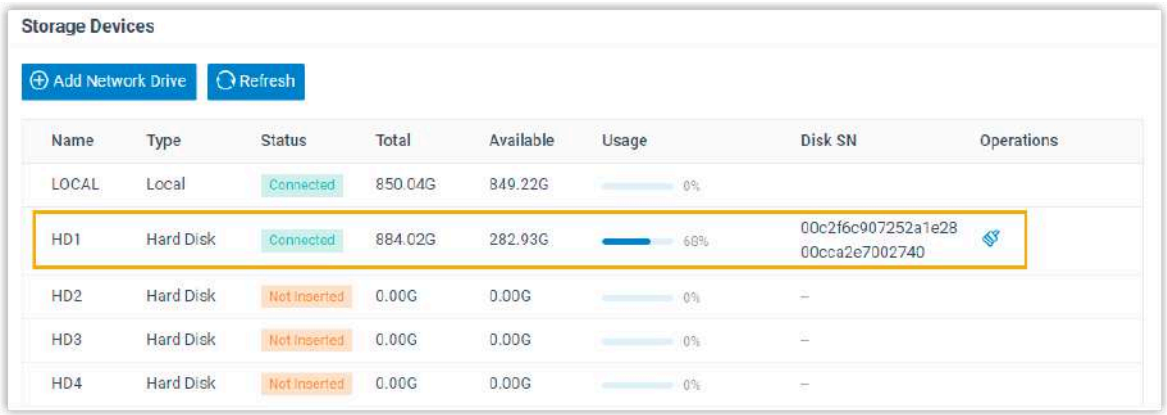
6. Install the front bezel.

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.



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

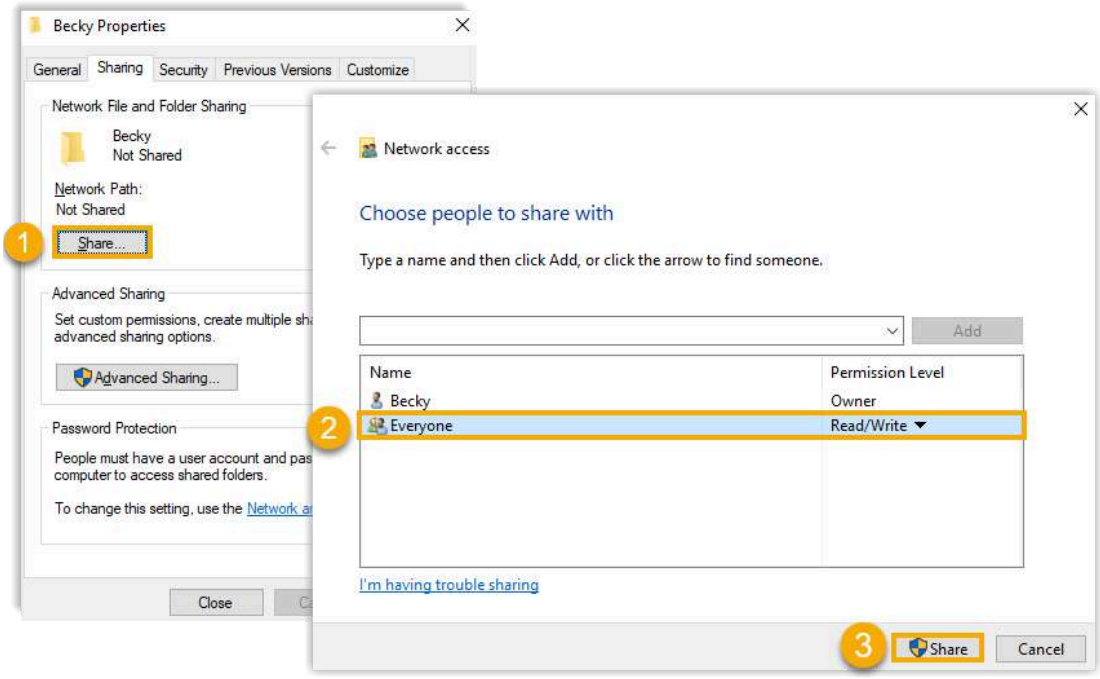
You can add up to 2 network drives.

Prerequisites

Make sure that the computer is always in service, or Yeastar P-Series Software Edition cannot add files to the shared folder.

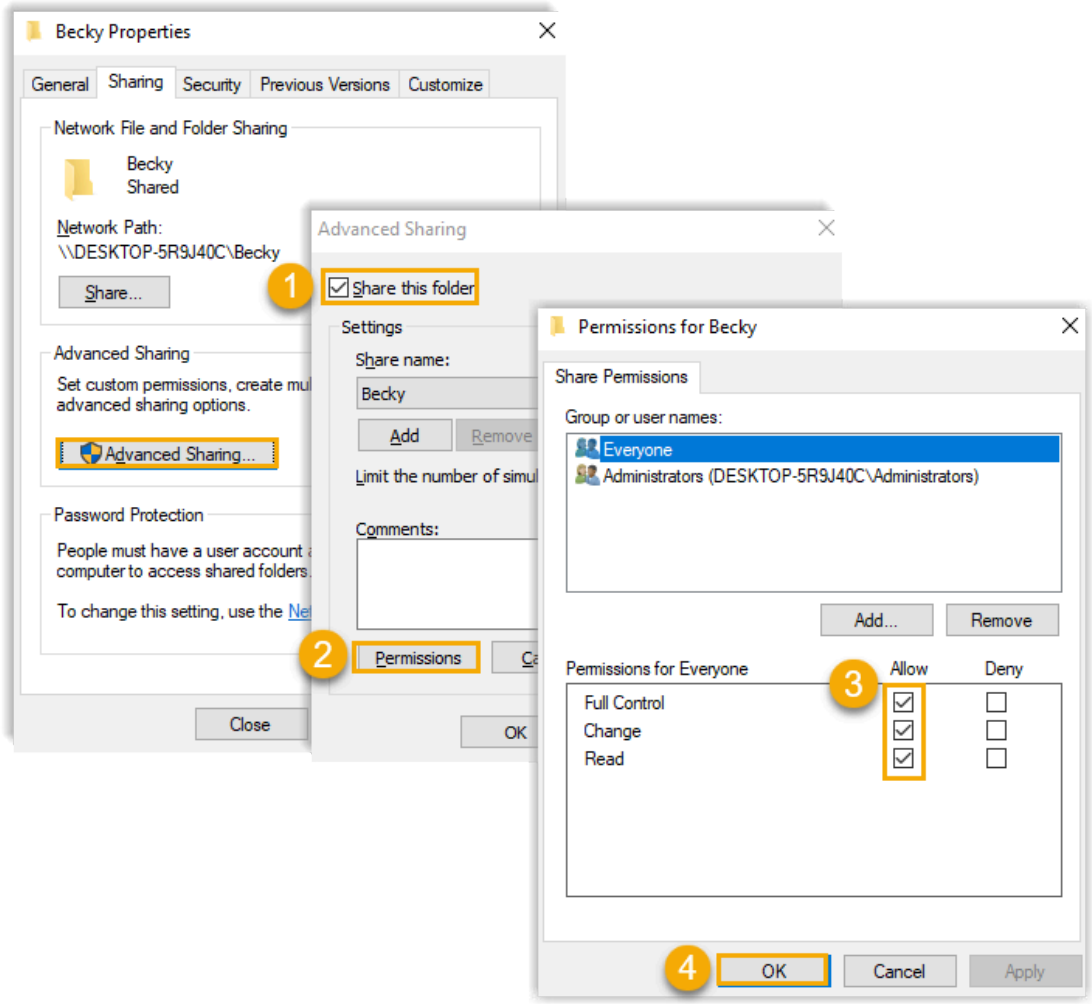
Step1. Create a shared folder in Windows 10

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.



a. Share the folder to **Everyone**.
b. In the **Permission Level** column, select **Read/Write** from the drop-down list.
c. Click **Share**.
d. In the pop-up dialog box, click **Done**.

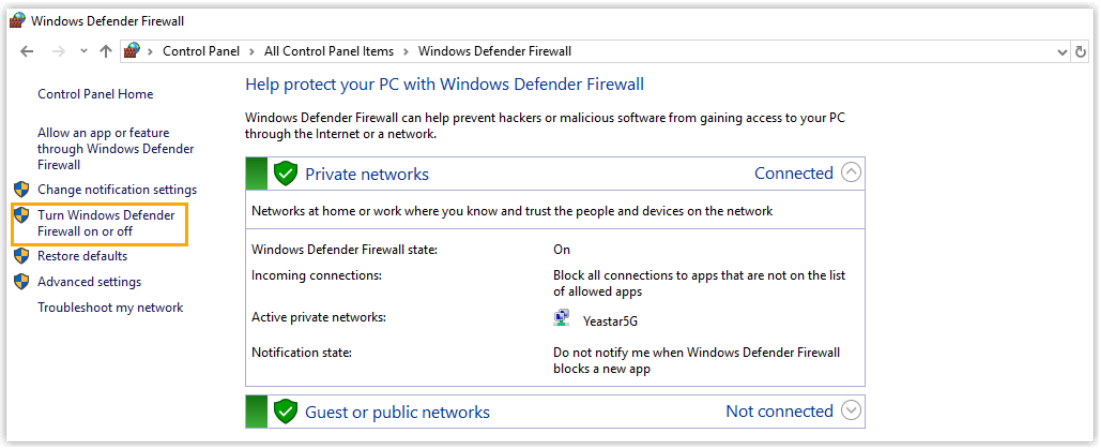
4. Click **Advanced Sharing...**, configure advanced Share properties.



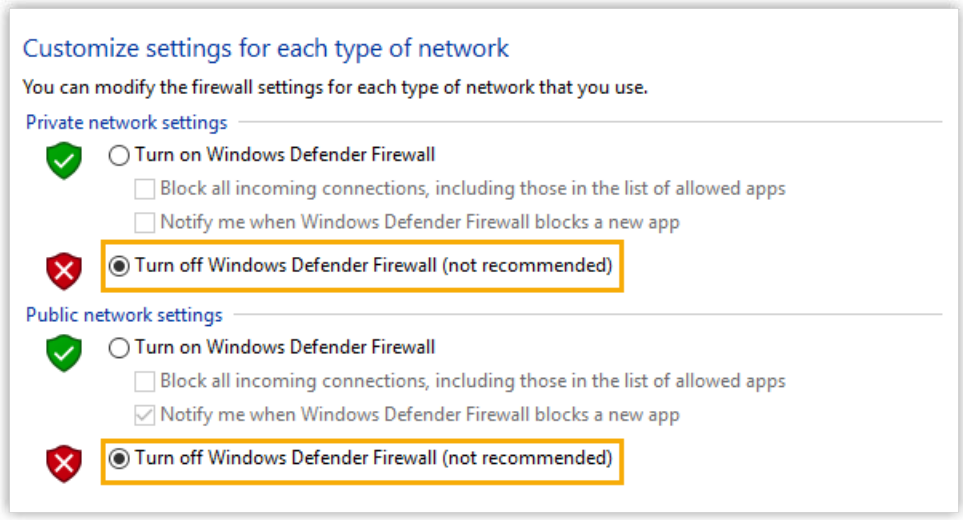
a. Select the checkbox of **Share this folder**.
b. Click **Permissions**.
c. In the pop-up window, allow all the permissions.
d. Click **OK**.

Step2. Turn off Windows Defender Firewall

1. On your computer, go to **Control Panel > Windows Defender Firewall**.
2. On the left navigation bar, click **Turn Windows Defender Firewall on or off**.



3. In both **Private network settings** and **Public network settings** sections, select **Turn off Windows Defender Firewall (not recommended)**.



4. Click **OK**.

Step3. Mount the shared folder to PBX

1. Log in to PBX web portal, go to **System > Storage > Storage Locations**.
2. In the **Storage Devices** section, click **Add Network Drive**.
3. In the pop-up window, configure the following settings.
   - **Name**: Specify a name to help you identify the network drive.
   - **Host/IP**: Enter the IP address of the Windows PC.
   - **Share Name**: Enter the name of the shared folder that you have created on the Windows PC.

> **Note:**
> To mount a subdirectory of the shared folder, enter *{share_folder_name}*/*{subdirectory_name}*. For example, `shared_folder/recording`.

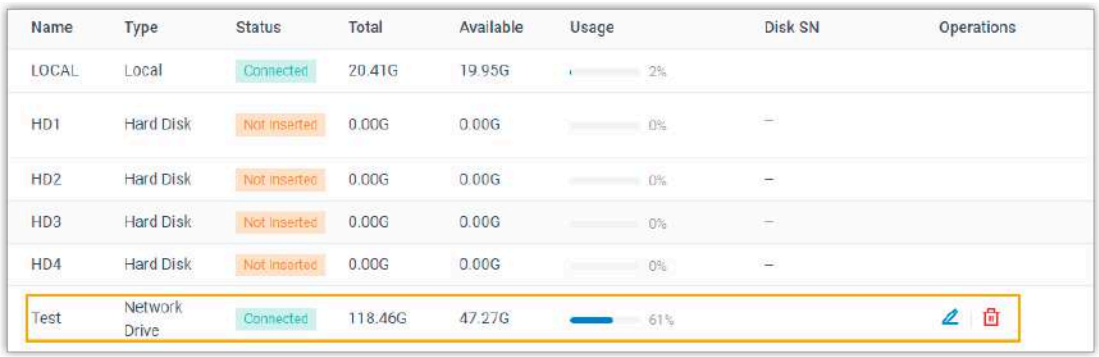
- **Access Username**: Enter the username to access the shared folder.
- **Access Password**: Enter the password to access the shared folder.
- **Work Group**: Optional. If you have set work group on your network drive, enter the name of the work group. If not, leave this field blank.
- **Samba Version**: Select the Samba version for the network drive. The default value is **Auto**.

4. Click **Save**.

Step4. Check connection status

In the **Storage Devices** section, check status of the network drive.

- **Connected**: The network drive is connected.
- **Unmounted**: No network drive is mounted.
- **Read Only**: Can NOT write data to the network drive.
- **Error**

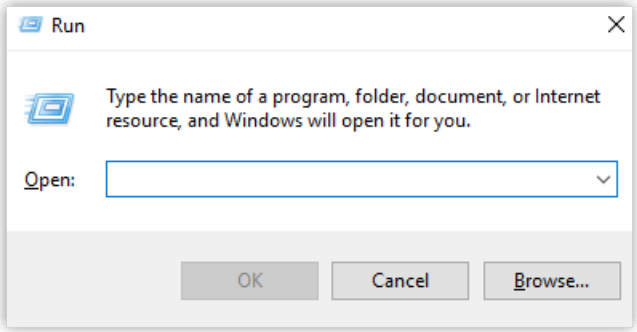


What to do next

Decide what data will be stored on the network drive. For more information, see Manage Storage Locations.

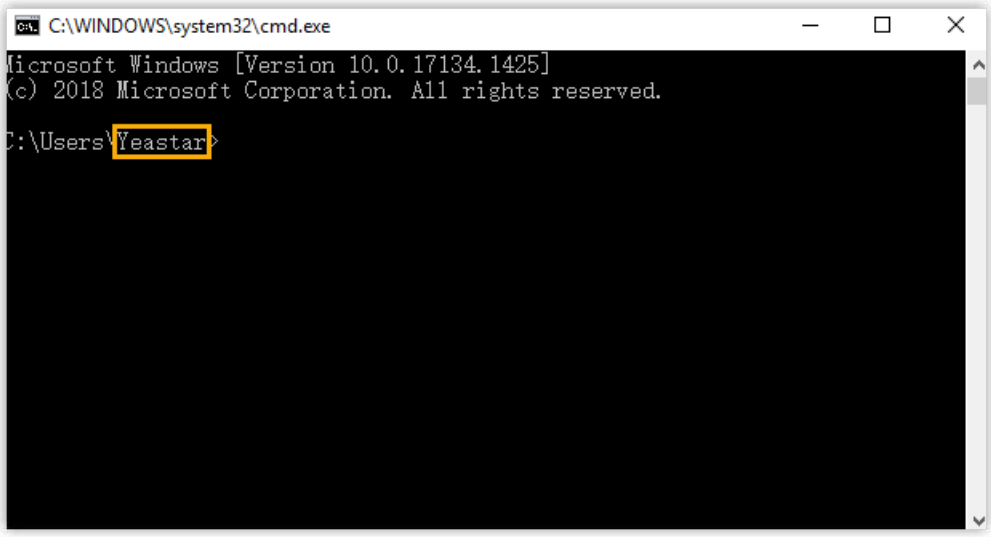
Network Drive FAQ

1. **How to check the user name that is used to access the shared folder?**
   a. On the Windows PC where the shared folder is created, press + **R** key to open the Run Window.



   b. Enter `cmd` and click **OK**.

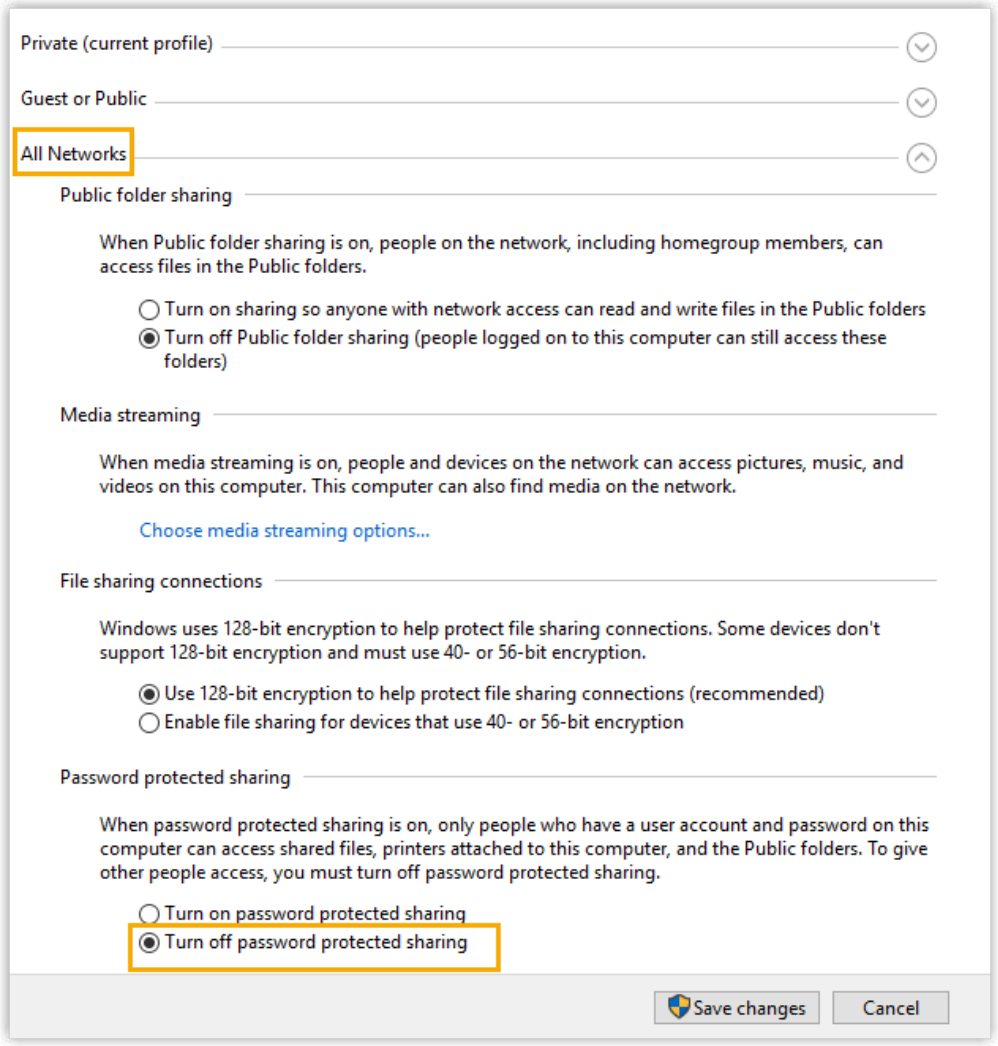
   The user name is displayed on the Command Prompt.



2. **How to configure Network Drive if no password is set on the Windows PC?**
   - We recommend that you set a password on the Windows PC.

     Enter the access password on PBX when you configure the Network Drive, then try to mount the network drive again.
   - If you want to leave the blank password on the Windows PC, configure the following settings, and try to mount the network drive again.
     a. On the Windows PC, go to **Control Panel > Network and Internet > Network and Sharing Center > Change advanced sharing settings**

> All Networks > Password protected sharing, select **Turn off password protected sharing**.



b. On the Network Drive configuration page, leave the **Username** and **Password** blank.

Add a Mac Network Drive

Network drive is used to extend storage space. You can save voicemails, recordings, and logs on a network drive. This topic describes how to add a shared folder on Mac and mount the shared folder to Yeastar P-Series Software Edition.

Restriction

You can add up to 2 network drives.

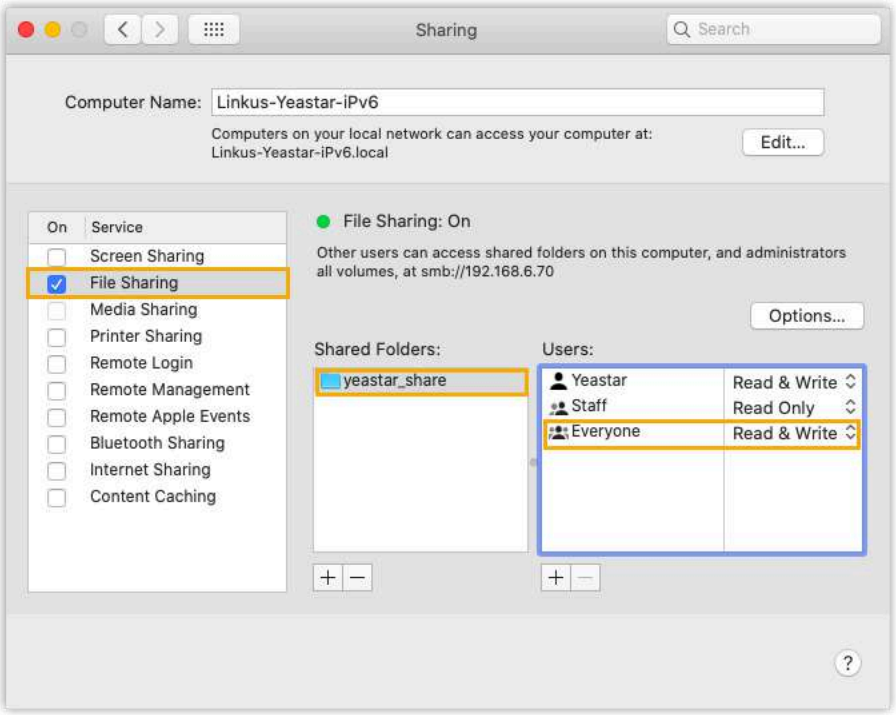
Prerequisites

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.

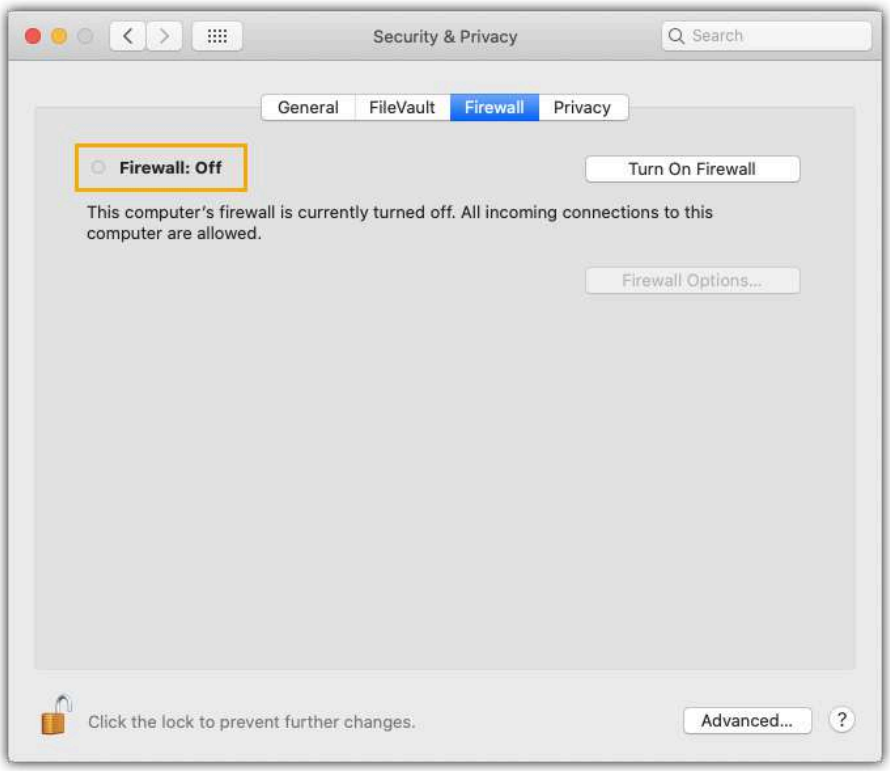
      i. Select the checkbox of **Share files and folders using SMB**.
      ii. In the **Windows File Sharing** section, enable the admin account and enter login password.
      iii. Click **Done**.
   c. In the **Shared Folders** section, click + to add the folder that you want to share.
   d. In the **Users** section, select **Everyone** and set permission level to **Read & Write**.
   e. Click to close the window.



Step2. Turn off Mac firewall

Firewall on Mac is disabled by default. Follow the instructions below to ensure that the firewall is disabled, or the shared folder on the Mac may not be accessed.

1. Go to **Apple menu** **> System Preferences > Security & Privacy**, click **Firewall** tab.
2. Make sure that firewall is disabled as follows.



Step3. Mount the shared folder to PBX

1. Log in to PBX web portal, go to **System > Storage > Storage Locations**.
2. In the **Storage Devices** section, click **Add Network Drive**.
3. In the pop-up window, configure the following settings.
    - **Name**: Specify a name to help you identify the network drive.
    - **Host/IP**: Enter the IP address of the Mac.
    - **Share Name**: Enter the name of the shared folder that you have created on the Mac.

      > **Note:**
      > To mount a subdirectory of the shared folder, enter subdirectory name.

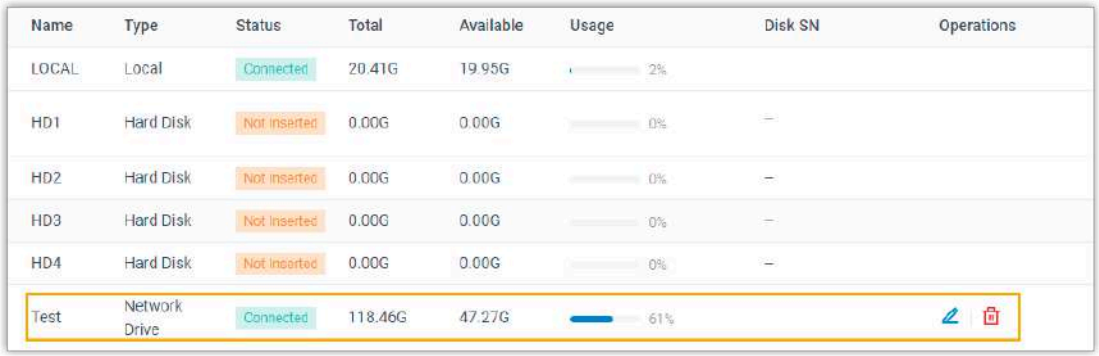
    - **Access Username**: Enter the username to access the shared folder.
    - **Access Password**: Enter the password to access the shared folder.
    - **Work Group**: Optional. If you have set work group on your network drive, enter the name of the work group. If not, leave this field blank.
    - **Samba Version**: Select the Samba version for the network drive. The default value is **Auto**.

4. Click **Save**.

Step4. Check connection status

In the **Storage Devices** section, check status of the network drive.

- **Connected**: The network drive is connected.
- **Unmounted**: No network drive is mounted.
- **Read Only**: Can NOT write data to the network drive.
- **Error**

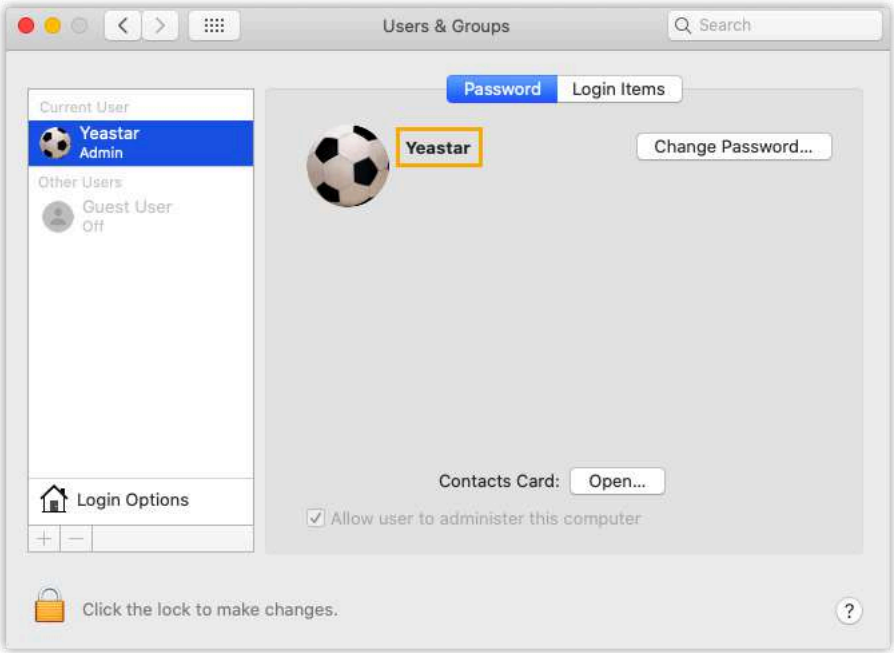


What to do next

Decide what data will be stored on the network drive. For more information, see Manage Storage Locations.

Network Drive FAQ

1. **How to check the user name that is used to access the shared folder?**
    a. Go to **Apple menu** > **System Preferences** > **Users & Groups**, check the current user name.



Manage Storage Locations

This topic describes how to manage storage locations for voicemail, logs, and recordings.

Prerequisites

- To store data on local flash, make sure there is enough storage space.
- To store data on external storage device or network drive, make sure the external device or network drive is connected.

  For more information, see the following topics:

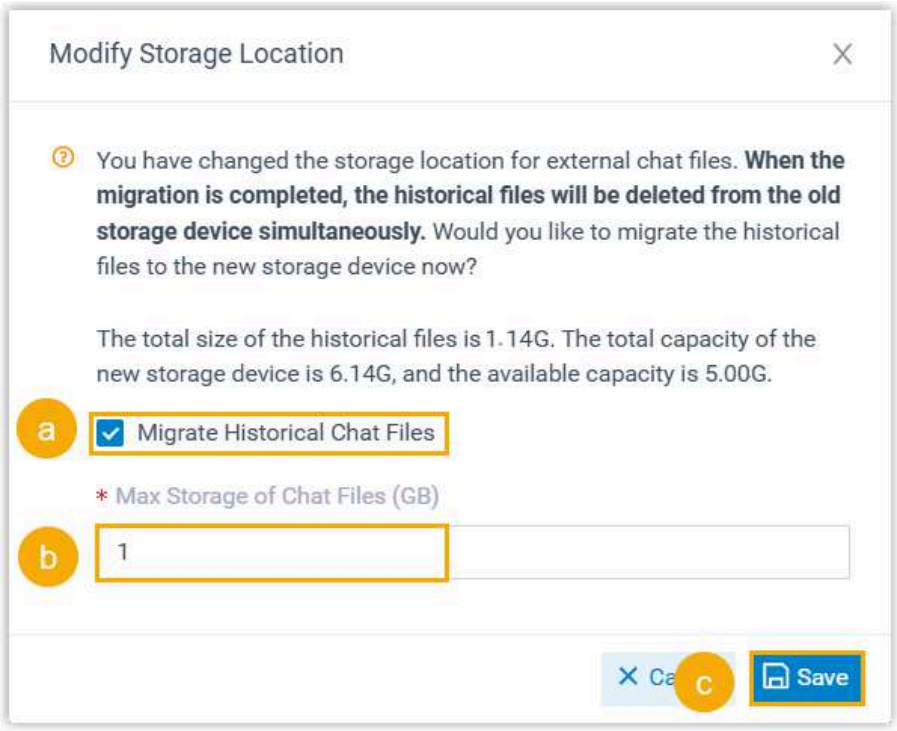
  -
  -
  - Set up a Hard Disk Drive
  - Add a Windows Network Drive
  - Add a Mac Network Drive

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.
- **External Chat Files**: Can be stored either on local flash or external device.

3. Click **Save**.
4. If you change the storage location for the external chat files, complete the further settings in the pop-up window.



a. If you want to migrate historical chat files to the new storage location, select the checkbox of **Migrate Historical Chat Files**.

> **Important:**
> Regardless of whether historical files are migrated or not, the files will be deleted from the original storage device after changing the storage location.

b. In the **Max Storage of Chat Files (GB)** field, set the maximum number of storage that external chat files could be retained.

> **Note:**
> The maximum storage for chat files set here will be synchronized to auto cleanup settings.

c. Click **Save**.

Result

New data will be stored on the specified location.

What to do next

Set the maximum number and preservation days that data can be stored. For more information, see Auto Cleanup Settings.

Auto Cleanup Settings

Auto Cleanup feature automatically and periodically cleans up your CDR, voicemails, recording files, backup files, and logs (including event logs, email sent logs, operation logs, and system logs). This topic describes relevant configuration parameters of auto cleanup.

CDR Auto Cleanup

Setting	Description
Max Number of CDR	Set the maximum number of CDR that should be retained. When it reaches 90% of the maximum number, the **Auto Cleanup Reminder** event will be triggered, the system will notify contacts concerned via specific methods. When it reaches the maximum number, the oldest CDR will be deleted. **Default value**: • 200,000 (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

Setting	Description
Max Number of Voicemail	Set the maximum number of voicemails that should be retained. When it reaches 90% of the maximum number, the **Auto Cleanup Reminder** event will be triggered, the system will notify contacts concerned via specific methods. When it reaches the maximum number, the oldest voicemails will be deleted. **Default value**: 100 **Maximum value**: 500
Voicemail Preservation Days	Set the maximum number of days that voicemails should be retained. When it reaches 90% of the maximum preservation days, the **Auto Cleanup Reminder** event will be triggered, the system will notify contacts concerned via specific methods. When it reaches the maximum preservation days, the oldest voicemails will be deleted. **Default value**: 0, which means no limit.

Recording Auto Cleanup

Setting	Description
Max Usage of Device (%)	Set the maximum storage percentage that the device is allowed to store recording files. When it reaches 90% of the maximum storage percentage, the **Auto Cleanup Reminder** event will be triggered, the system will notify contacts concerned via specific methods. When it reaches the maximum storage percentage, the oldest recording files will be deleted. **Default value**: 80% **Maximum value**: 99% **Note:** You can directly enter a value in this field to set the maximum storage percentage.
Recordings Preservation Days	Set the maximum number of days that recording files should be retained.

Setting	Description
	When it reaches 90% of the maximum preservation days, the **Auto Cleanup Reminder** event will be triggered, the system will notify contacts concerned via specific methods. When it reaches the maximum preservation days, the oldest recording files will be deleted. **Default value**: 0, which means no limit.

External Chat Data Auto Cleanup

Data Type	Setting	Description
Chat Logs	Max Number of External Chat Logs	Set the maximum number of external chat logs to store. When it reaches 90% of the maximum number, the **Auto Cleanup Reminder** event will be triggered, the system will notify contacts concerned via specific methods. When it reaches the maximum number, the oldest external chat logs will be deleted. **Default value**: 50,000 **Maximum value**: 100,000
	External Chat Data Preservation Days	Set the maximum number of days that external chat logs should be retained. When it reaches 90% of the maximum preservation days, the **Auto Cleanup Reminder** event will be triggered, the system will notify contacts concerned via specific methods. When it reaches the maximum preservation days, the oldest external chat logs will be deleted. **Default value**: 0, which means no limit.
Chat Files	Max Storage of Chat Files (GB)	Set the maximum number of storage that external chat files (including documents and images) should be retained. When it reaches 90% of the maximum number, the **Auto Cleanup Reminder** event will be triggered, the system will notify contacts concerned via specific methods. When it reaches the maximum number, the oldest external chat files will be deleted. **Default value**: 5

Data Type	Setting	Description
	External Chat Files Preservation Days	Set the maximum number of days that external chat files (including documents and images) should be retained. When it reaches 90% of the maximum preservation days, the **Auto Cleanup Reminder** event will be triggered, the system will notify contacts concerned via specific methods. When it reaches the maximum preservation days, the oldest external chat files will be deleted. **Default value**: 7 **Note:** Entering 0 means no limit.

System Backup Files Auto Cleanup

Setting	Description
Max Number of Files	Set the maximum number of backup files that should be retained. When it reaches 90% of the maximum number, the **Auto Cleanup Reminder** event will be triggered, the system will notify contacts concerned via specific methods. When it reaches the maximum number, the oldest backup files will be deleted. **Default value**: 5 **Maximum value**: 8

Event Logs Auto Cleanup

Setting	Description
Max Number of Logs	Set the maximum number of event logs that should be retained. When it reaches the maximum number, the oldest event logs will be deleted. **Note:** Some event logs are not allowed to be automatically cleaned up. When those logs reach 5,000, the oldest event logs will be deleted.

Setting	Description
	Default value: 50,000 **Maximum value**: 1,000,000
Logs Preservation Days	Set the maximum number of days that event logs should be retained. When it reaches the maximum preservation days, the oldest event logs will be deleted. **Default value**: 0, which means no limit.

Email Sent Logs Auto Cleanup

Setting	Description
Max Number of Logs	Set the maximum number of email sent logs that should be retained. When it reaches the maximum number, the oldest email sent logs will be deleted. **Default value**: 50,000 **Maximum value**: 1,000,000
Logs Preservation Days	Set the maximum number of days that email sent logs should be retained. When it reaches the maximum preservation days, the oldest email sent logs will be deleted. **Default value**: 0, which means no limit.

Operation Logs Auto Cleanup

Setting	Description
Max Number of Logs	Set the maximum number of operation logs that should be retained. When it reaches the maximum number, the oldest operation logs will be deleted. **Default value**: 50,000 **Maximum value**: 1,000,000
Logs Preservation Days	Set the maximum number of days that operation logs should be retained. When it reaches the maximum preservation days, the oldest operation logs will be deleted. **Default value**: 0, which means no limit.

System Logs Auto Cleanup

Setting	Description
Max Storage of Logs (MB)	Set the maximum file size for a system log package. When it reaches the maximum file size, the oldest logs in the package will be deleted. **Default value**: • 10 (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

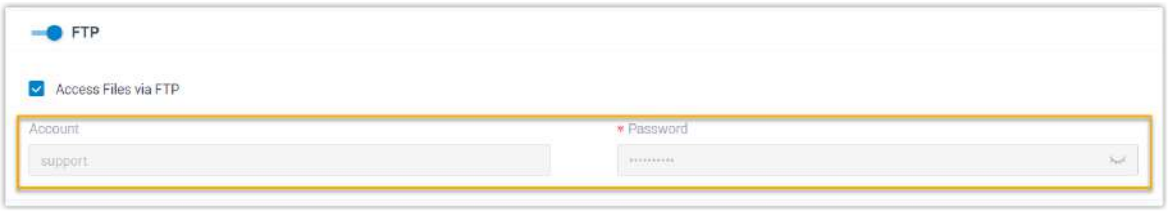
1. Log in to PBX web portal, go to **System > Storage > File Sharing**.
2. In the **FTP** section, enable **FTP** and click **OK** in the pop-up window.
3. Select the checkbox of **Access Files via FTP**.

> **Note:**
> Ensure this option is selected otherwise you can not access the files stored in PBX external storage.

4. Click **Save**.

   The PBX can now be used as an FTP server.

5. Check the **Account**, and click the to check and note down the **Password**.

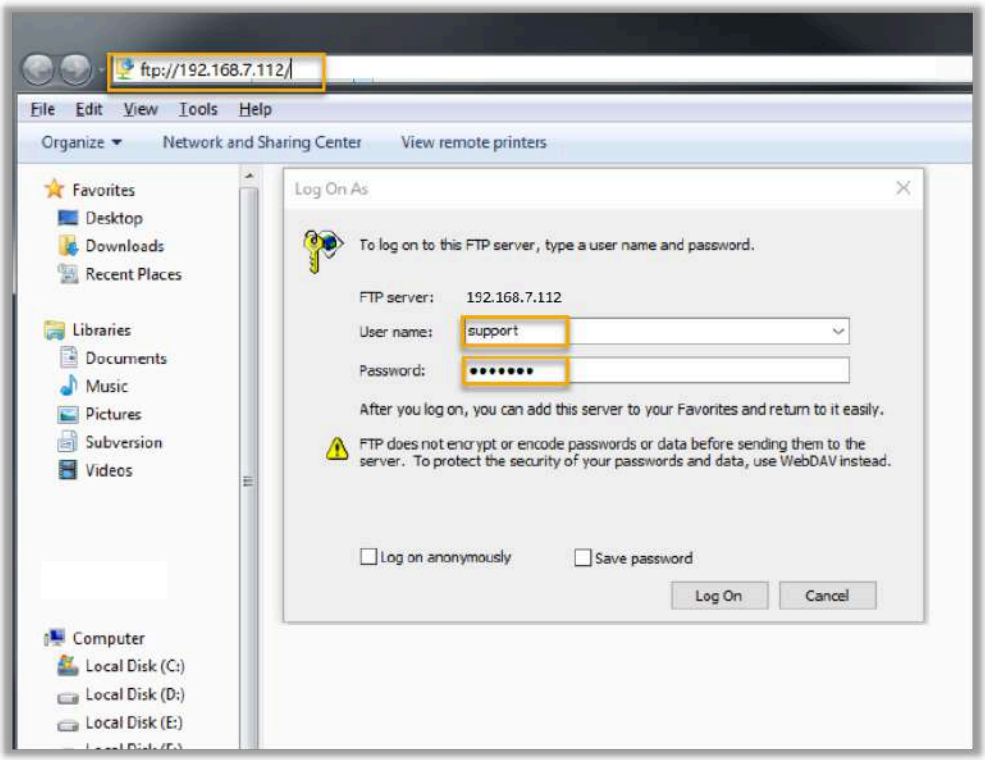


> **Note:**
> The FTP password is the same as the SSH password. If the SSH password is reset, the FTP password will be updated to the latest SSH password automatically.

Step2. Access the PBX files via FTP

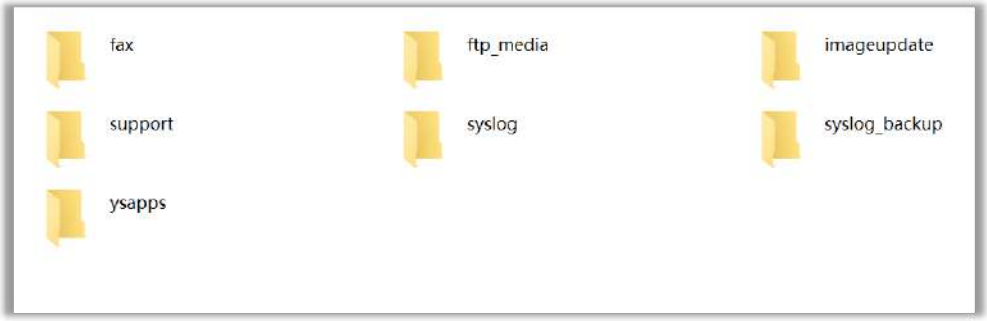
1. On a Windows PC, press **Win + E** to open a Windows Explorer window.
2. In the address bar, enter the FTP address of the PBX `ftp://{IP address of the PBX}`, then press **Enter**.

   For example, the IP address of the PBX is 192.168.7.112, then you should enter `ftp://192.168.7.112`.
3. In the pop-up window, enter the credentials to access the PBX files.



a. Enter the user name and password.
   - **User name**: Enter `support`.
   - **Password**: Enter the FTP password.

b. Click **Log On**.
   You will see the following folders that contain the files from PBX local storage and external storage.



4. **Optional**: Enter the folder `ftp_media` to check the files stored in PBX external storage.

   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 of PBX from a local computer.

Prerequisite

- You have set up external storage devices on PBX.
- You have stored desired data on external storage devices. For more information, see Manage Storage Locations.

Procedure

Step1. Enable File Sharing feature on the PBX

Step2. Access the shared files on PC

Step1. Enable File Sharing feature on the PBX

1. Log in to PBX web portal, go to **System > Storage > File Sharing**.
2. In the **File Sharing** section, enable **File Sharing** and click **OK** in the pop-up window.
3. Select the checkbox of **Allow to Change Shared Files**.

   > **Note:**
   > Ensure this option is selected otherwise you can not edit, upload or download the files in the shared file holder.

4. In the **Shared Folder Name** field, specify a folder name to help you identify it.
5. Click **Save**.
6. Check and note down the **Account** and **Password**.

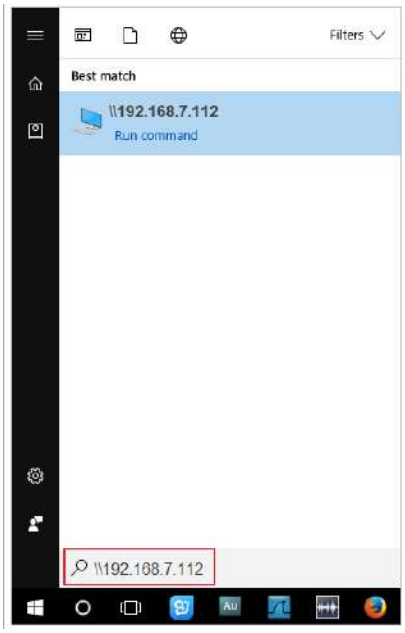
- **Account**: `share`.

> **Note:**
> The **Account** name can not be changed.

- **Password**: Auto-generated random password.
  - Click to check the password.
  - Click to generate a new random password.

Step2. Access the shared files on PC

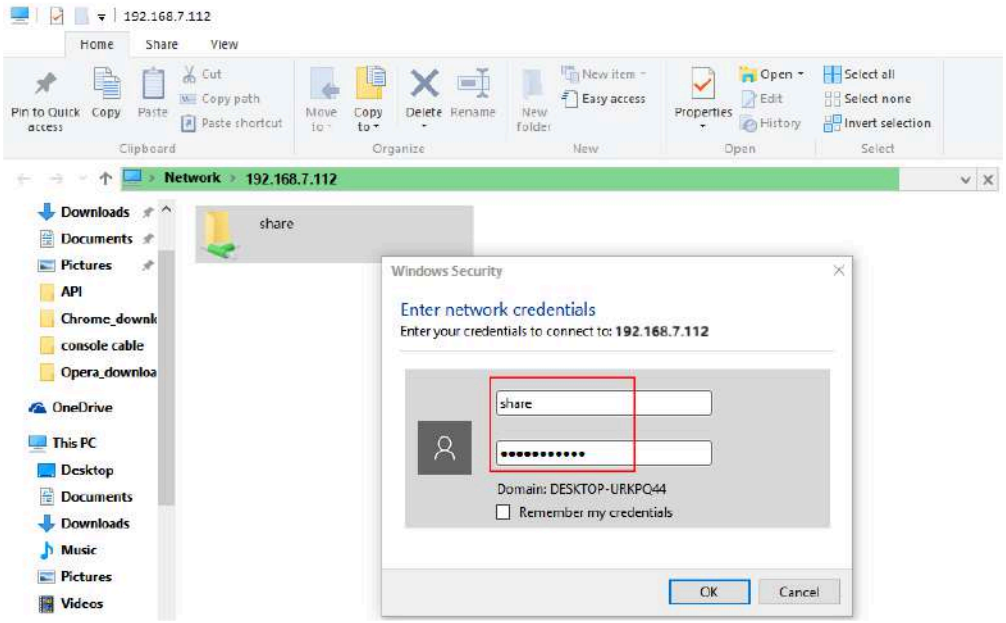
1. In the **Windows search** field, enter `\\{IP address of the PBX}`, then press **Enter**. For example, the IP address of the PBX is 192.168.7.112, then you should enter `\\192.168.7.112`.



2. Double-click the shared folder.

A pop-up window requires login credentials.

3. In the pop-up window, enter the credentials.



a. Enter the user name and password.

- **User name**: Enter `share`.
- **Password**: Enter the password.

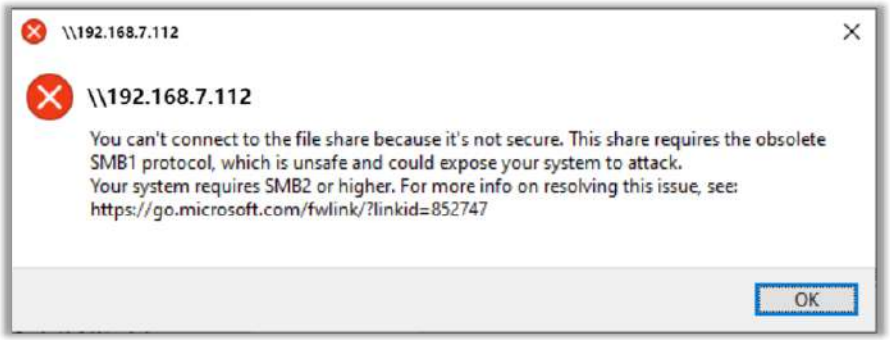
b. Click **OK**.

You can now access the shared folder. 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.

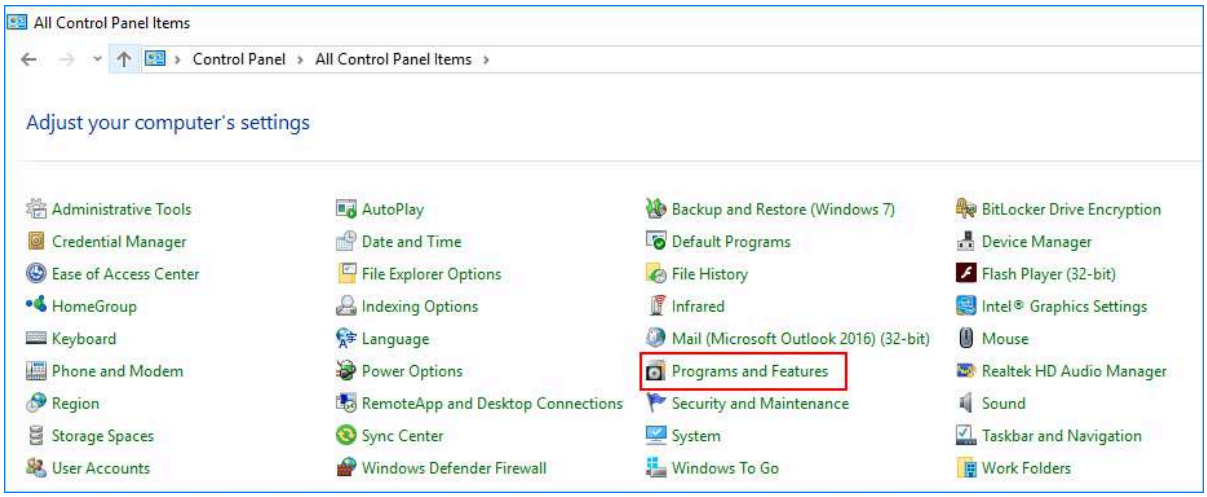
File Sharing FAQ

Windows 10 users cannot access the shared folder of the PBX

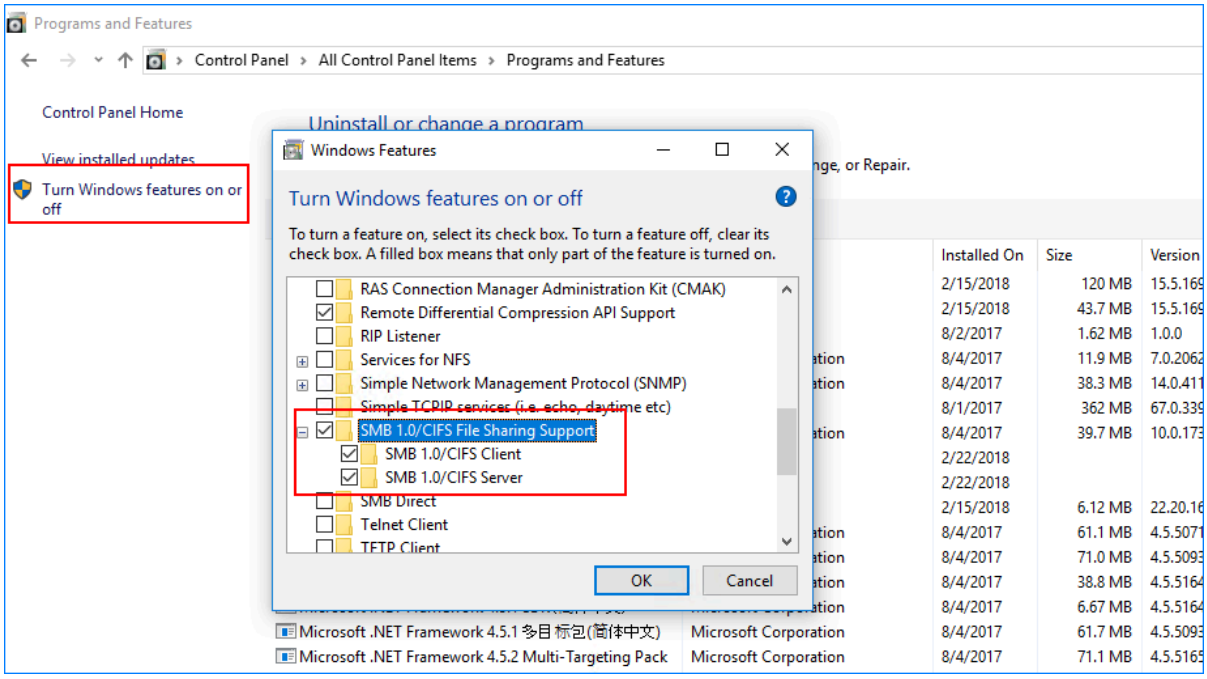
If you fail to access the shared folder and see the pop-up window shown as below, do as follows.



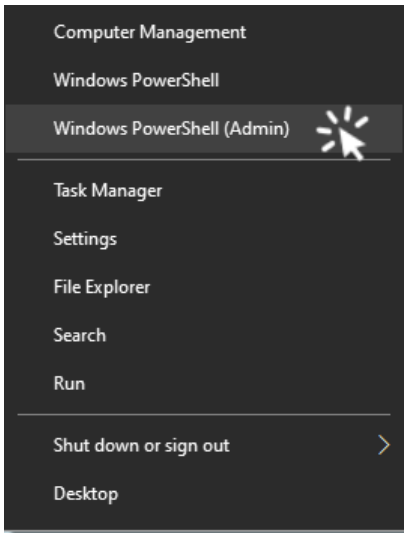
1. Go to **Control Panel > Programs and Features**.



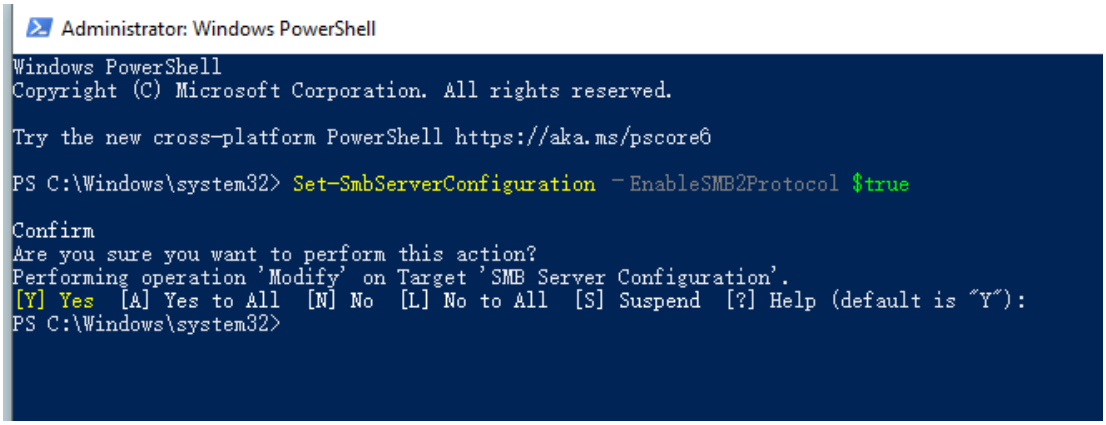
2. On the left column of the window, click **Turn Windows features on or off**.
3. In the pop-up window, check the option of **SMB 1.0/CIFS File Sharing Support**.



4. Press **Win** + **X**, and select **Windows Powershell(Admin)**.



5. In the pop-up window, enter `Set-SmbServerConfiguration –EnableSM-B2Protocol $true`, and press **Enter**.



6. Press **Enter** again to execute the command.
7. Reboot your computer and retry.

Set up PBX as a TFTP Server

By setting up the TFTP feature, Yeastar P-Series 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** and click **OK** in the pop-up window.
3. Click **Save**.

Result

The PBX can now be used as a TFTP server, you can upload or download desired files to/from the specific PBX file folder.

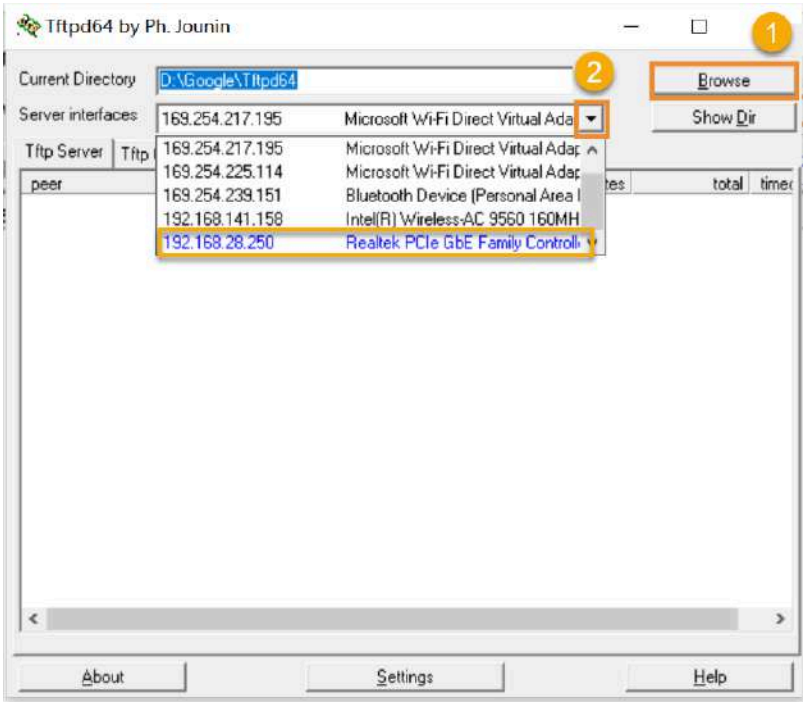
TFTP File Sharing examples

This section gives examples to show how to upload and download files in the specific PBX file holder using Tftpd64.

Configure a TFTP Client

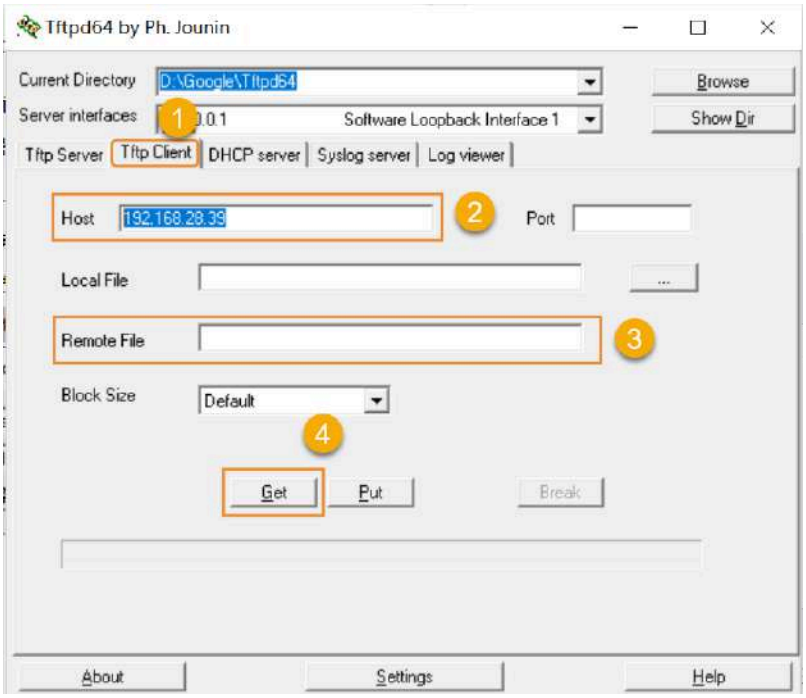
1. Download a Tftpd64 and run the software.
2. On the top of the window, click **Browse** to select the storage path for the shared files.

3. In the **Server interface** drop-down list, select the IP address of your computer.



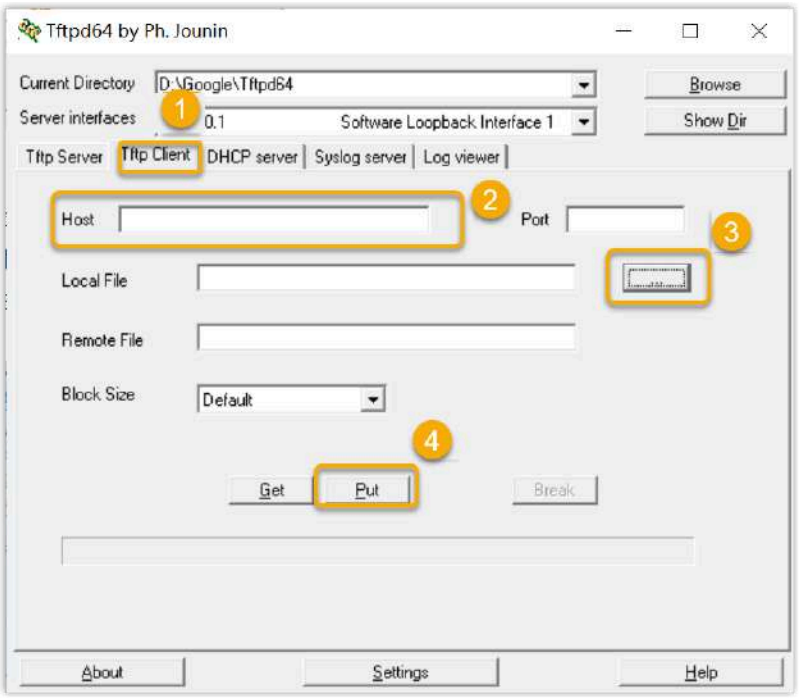
Download a file from PBX

1. In the Tftpd64, go to **Tftp Client** tab.
2. In the **Host** field, enter the IP address of the PBX.
3. In the **Remote File** field, enter the name of the desired file.
4. Click **Get** to download the file.



Upload a file to PBX

1. In the Tftpd64, go to **Tftp Client**.
2. In the **Host** field, enter the IP address of the PBX.
3. Click the ••• beside the **Local File** field to select the desired file.
4. Click **Put** to upload the file to the PBX.



Archive

Yeastar P-Series Software Edition Remote Archiving Overview

Yeastar P-Series Software Edition allows you to download and archive the system's call recordings and backup files to external servers via FTP, SFTP, Amazon S3, and Google Cloud Storage services, enabling less space occupying and minimized data loss risk on PBX, as well as easier file management on external server.

Requirements and restrictions

Requirements

- **PBX Firmware**: Version 83.18.0.59 or later
- **PBX Plan**: Enterprise Plan

Restrictions

- **Archive server**: 10
- **Archive task**: 200

Archive Files to FTP Server

Yeastar P-Series Software Edition supports archiving the system's call recordings and back-up files to FTP server, either on a regular interval or at any time you want. This topic describes how to add FTP server as an archive server and schedule tasks to archive the desired files.

Requirements and restrictions

Requirements

- **PBX Firmware**: Version 83.18.0.59 or later
- **PBX Plan**: Enterprise Plan

Restrictions

- **Archive server**: 10
- **Archive task**: 200

Prerequisites

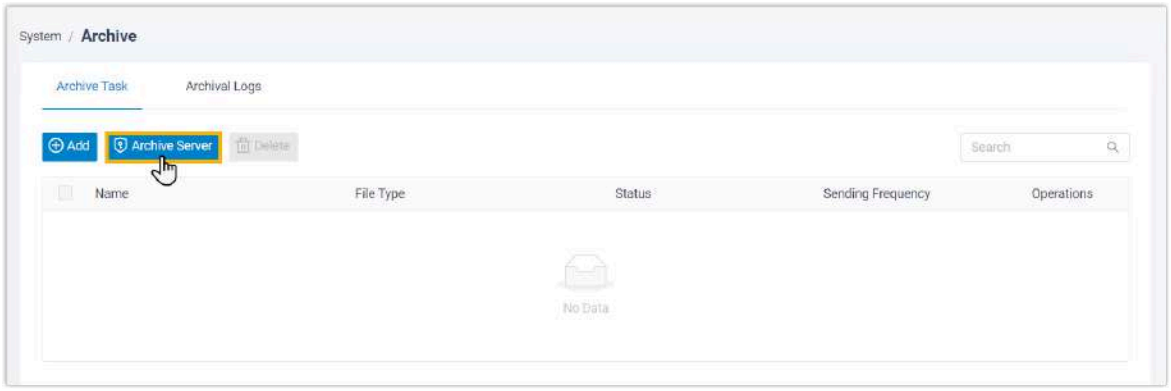
Before you begin, you need to prepare the following resources and collect the required information:

- Prepare an FTP server, and note down its **Domain/IP Address**, **Port**, and **File Transfer Protocol**.
- Prepare an FTP account with both read and write permissions, and note down its **Username** and **Password**.

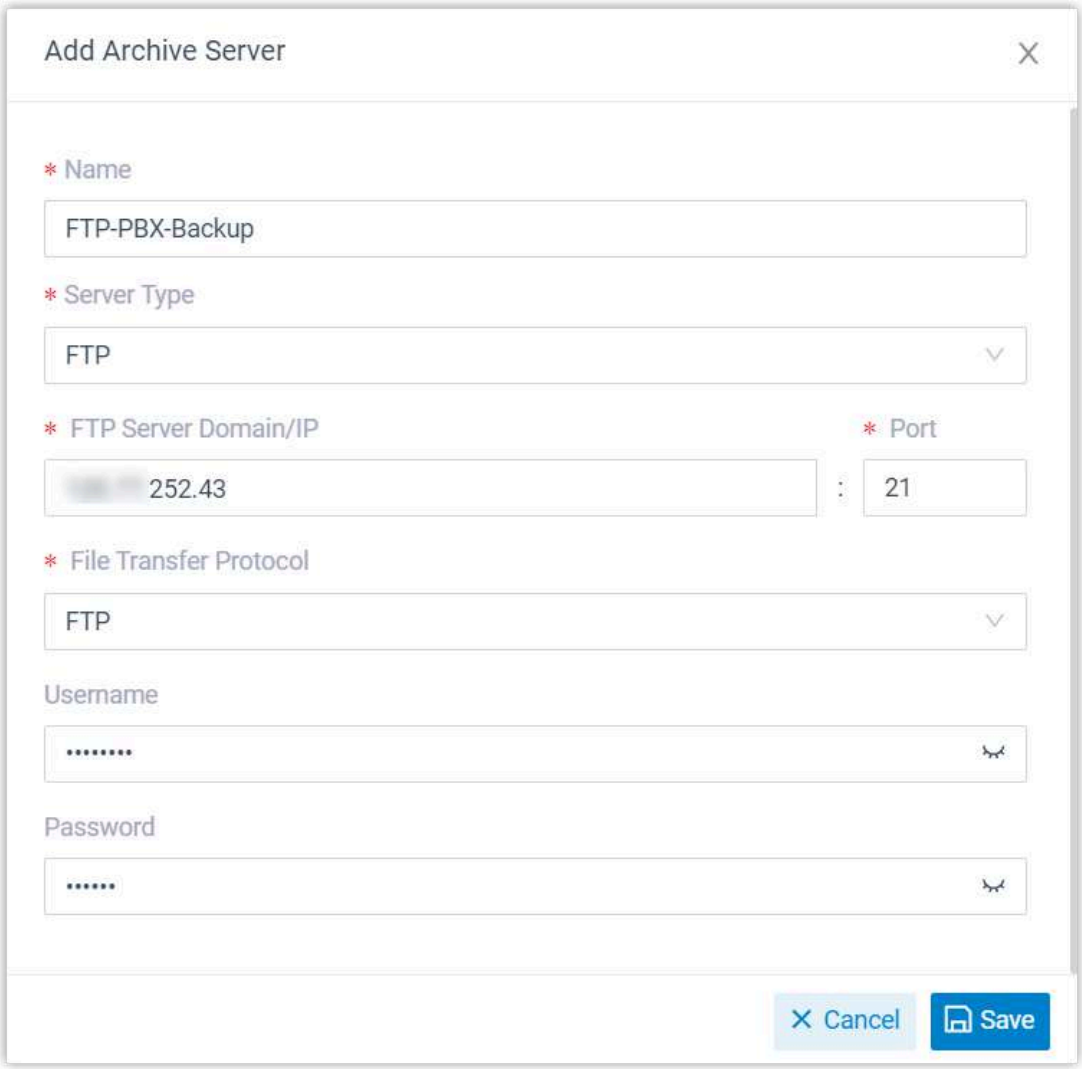
> **Note:**
> If you want old files to be automatically deleted from your FTP server, make sure the FTP account also has file deletion permission.

Step 1. Add FTP server as archive server

1. Log in to PBX web portal, go to **System > Archive**.
2. Under the **Archive Task** tab, click **Archive Server**.



3. Set up FTP server as the archive server.
    a. Click **Add**.
    b. In the pop-up window, complete the following settings.



Setting	Description
Name	Enter a name to help you identify the server.
Server Type	Select **FTP**.
FTP Server Domain/IP	Enter the address of your FTP server.
Port	Enter the port on which your FTP server is running. The default port is 21.
File Transfer Protocol	Select the transfer protocol supported by the FTP server. • **FTP**: Standard File Transfer Protocol. • **FTPES**: FTP over Explicit TLS/SSL. **Note:** ◦ The TLS feature on the FTP server must be enabled, and the encryption policy must be well-configured for security reason. ◦ The supported TLS protocol version is **TLS V1.2**.
Username	Enter the username for the FTP account.
Password	Enter the password associated with the username.

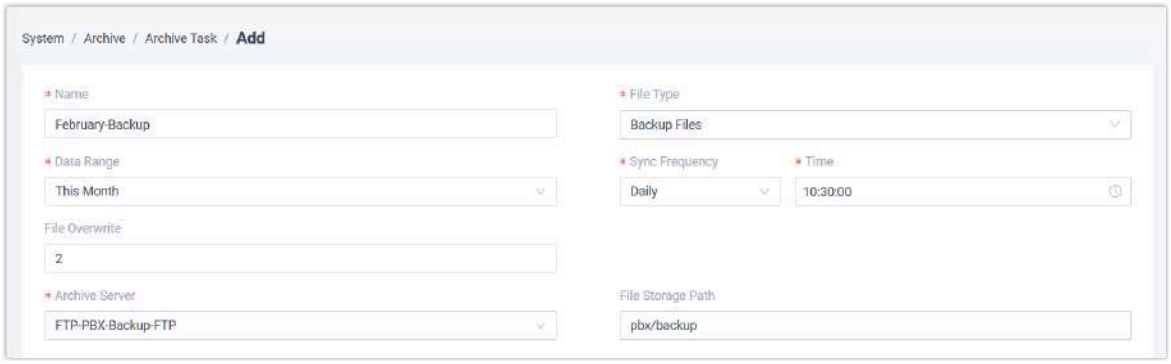
c. Click **Save**.

The FTP server is added as an archive server and displayed on the archive server list.

4. Click ✕ to close the window.

Step 2. Create a task to archive files to FTP server

1. Under **Archive Task** tab, click **Add**.
2. Create a one-time or recurring archive task.



Setting	Description
Name	Enter a name to help you identify the task.
File Type	Select **Recording Files** or **Backup Files** as needed.
Data Range	Specify a time range of the files to be archived. **Note:** You can archive files for up to 31 days at a time.
Sync Frequency	Set how often to archive files to FTP server. **Note:** As large amounts of data will consume PBX's CPU resources, we recommend that you schedule archive tasks during off-peak hours. • **Once**: If you choose the option, the system will archive files immediately after you save the task. • **Daily**: If you choose the option, select a time from the drop-down list. The system will archive files at this time of the day. • **Weekly**: If you choose the option, choose a day of week and select a time from the drop-down list. The system will archive files at this time of the week. • **Monthly**: If you choose the option, choose a day and select a time from the drop-down list. The system will archive files on this day and time of the month.
File Overwrite	Optional. Set the maximum number of files to be retained in the FTP server for the archive task. **Note:** • This option is available only when you schedule to archive backup files on a recurring basis.

Setting	Description
	• When it reaches the limit, the system will retain the latest backup files and delete the earlier ones.
Archive Server	Select the FTP server that you have added.
Select Folder/Path	Optional. Set the path to the folder in which you want to store archived files. For example, `pbx/backup/`. **Note:** If you leave this field blank, the files will be stored under the root directory.

3. Click **Save**.

Result

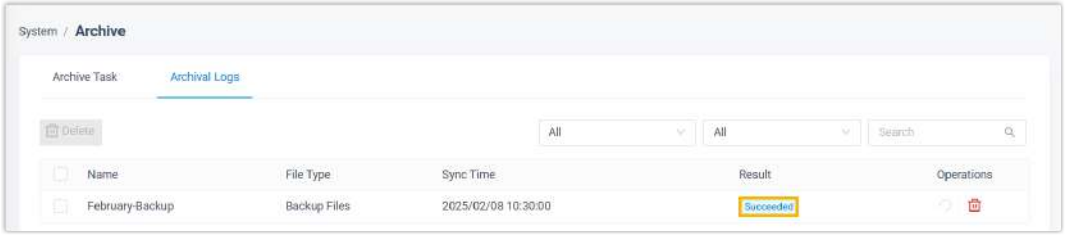
The specified files will be archived to the designated folder in your FTP server immediately or at the scheduled time.

Note:
The system executes only one task at a time to avoid affecting system performance. If there are multiple tasks, they will be queued up one after another.

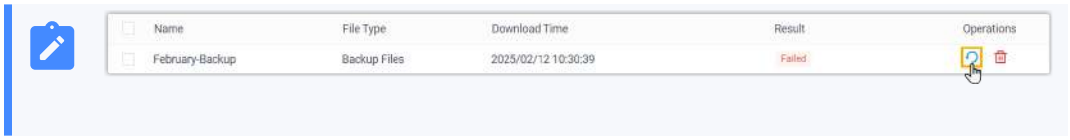
You can check the archive result in the following ways.

Check the archive result on PBX

On PBX web portal, go to **System > Archive > Archival Logs**. If the **Result** column of the task shows **Succeeded**, it indicates that the specified files have been successfully archived to the FTP server.

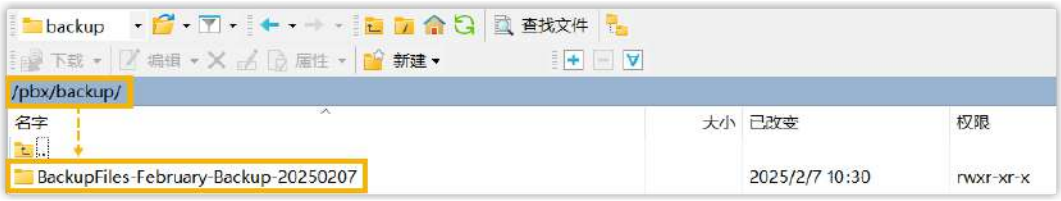


Note:
If the task is failed, the **Failed to Archive File(s)** event will be triggered; You can click to retry the task.



Check the archive result on FTP server

Go to the designated folder in FTP server. If the specified files appear in the list, it indicates that the archive is successful.



Archive Files to SFTP Server

Yeastar P-Series Software Edition supports archiving the system's call recordings and back-up files to SFTP server, either on a regular interval or at any time you want. This topic describes how to add SFTP server as an archive server and schedule tasks to archive the desired files.

Requirements and restrictions

Requirements

- **PBX Firmware**: Version 83.18.0.59 or later
- **PBX Plan**: Enterprise Plan

Restrictions

- **Archive server**: 10
- **Archive task**: 200

Prerequisites

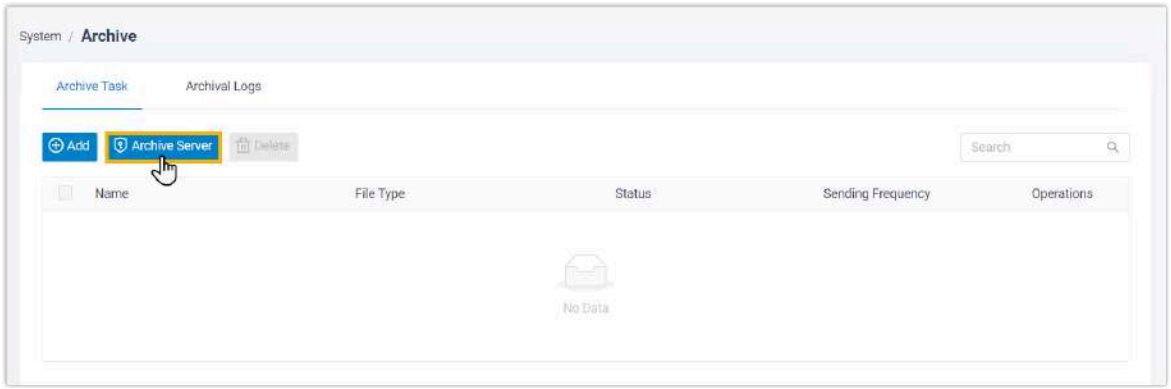
Before you begin, you need to prepare the following resources and collect the required information:

- Prepare an SFTP server and note down its **Domain/IP Address** and **Port**.
- Prepare an SFTP account with both read and write permissions, and note down its **Username** and **Password/Private Key**.

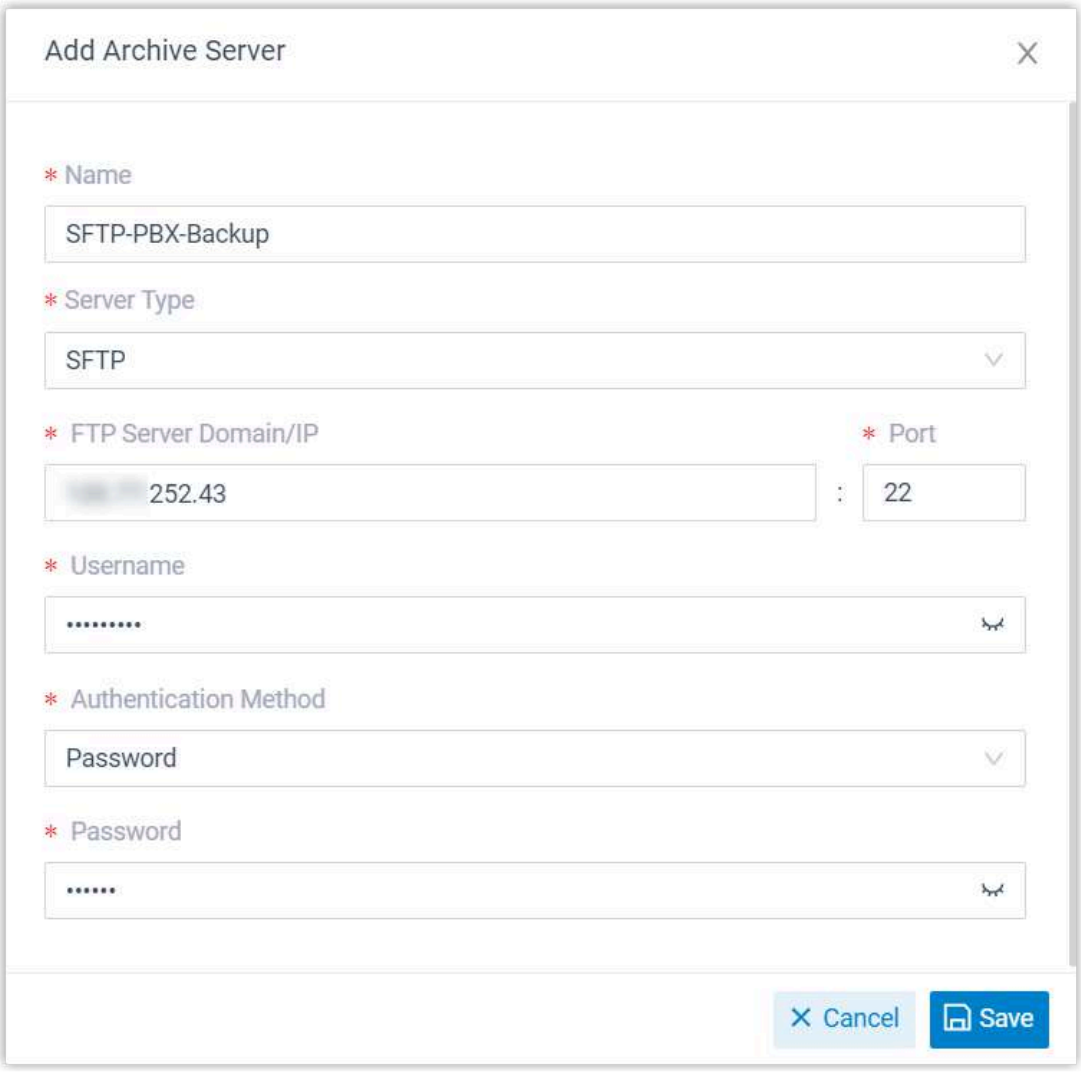
> **Note:**
> If you want old files to be automatically deleted from your SFTP server, make sure the SFTP account also has file deletion permission.

Step 1. Add SFTP server as archive server

1. Log in to PBX web portal, go to **System > Archive**.
2. Under the **Archive Task** tab, click **Archive Server**.



3. Set up SFTP server as the archive server.
    a. Click **Add**.
    b. In the pop-up window, complete the following settings.



Setting	Description
Name	Enter a name to help you identify the server.
Server Type	Select **SFTP**.
FTP Server Domain/IP	Enter the address of your SFTP server.
Port	Enter the port on which your SFTP server is running. The default port is 22.
Username	Enter the username for the SFTP account.
Authentication Method	Select an authentication method, then enter the credential.

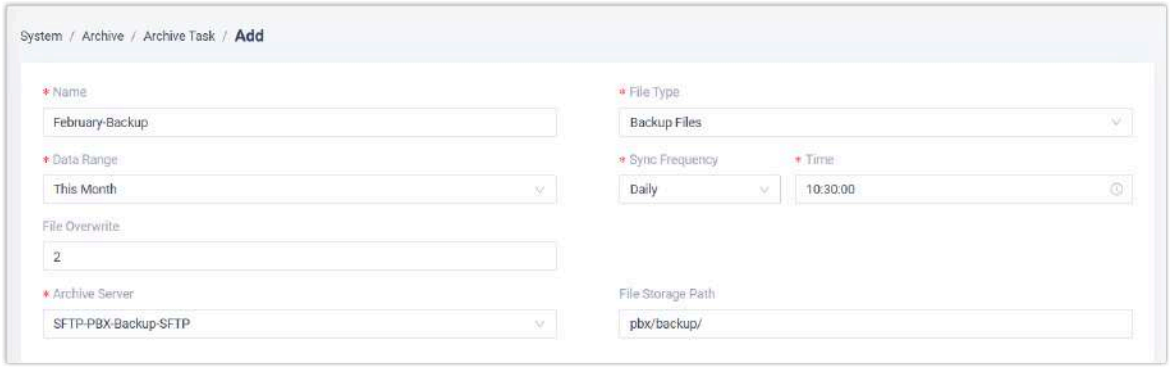
c. Click **Save**.

SFTP server is added as an archive server and displayed on the archive server list.

4. Click ✕ to close the window.

Step 2. Create a task to archive files to SFTP server

1. Under **Archive Task** tab, click **Add**.
2. Create a one-time or recurring archive task.



Setting	Description
Name	Enter a name to help you identify the task.
File Type	Select **Recording Files** or **Backup Files** as needed.
Data Range	Specify a time range of the files to be archived. **Note:** You can archive files for up to 31 days at a time.
Sync Frequency	Set how often to archive files to SFTP server. **Note:** As large amounts of data will consume PBX's CPU resources, we recommend that you schedule archive tasks during off-peak hours. • **Once**: If you choose the option, the system will archive files immediately after you save the task. • **Daily**: If you choose the option, select a time from the drop-down list. The system will archive files at this time of the day. • **Weekly**: If you choose the option, choose a day of week and select a time from the drop-down list. The system will archive files at this time of the week.

Setting	Description
	• **Monthly**: If you choose the option, choose a day and select a time from the drop-down list. The system will archive files on this day and time of the month.
File Overwrite	Optional. Set the maximum number of files to be retained in the SFTP server for the archive task. **Note:** • This option is available only when you schedule to archive backup files on a recurring basis. • When it reaches the limit, the system will retain the latest backup files and delete the earlier ones.
Archive Server	Select the SFTP server that you have added.
Select Folder/Path	Optional. Set the path to the folder in which you want to store archived files. For example, `pbx/backup/`. **Note:** If you leave this field blank, the files will be stored under the root directory.

3. Click **Save**.

Result

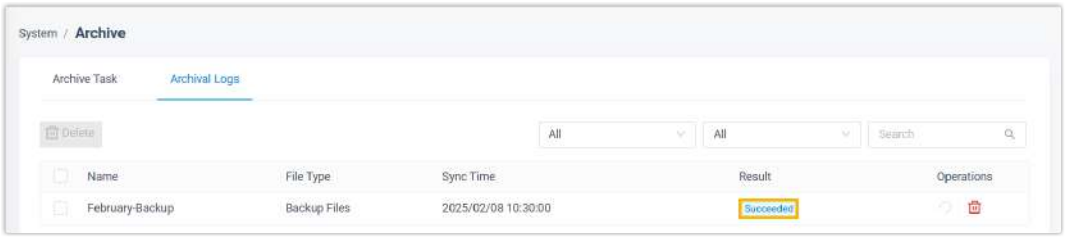
The specified files will be archived to the designated folder in your SFTP server immediately or at the scheduled time.

Note:
The system executes only one task at a time to avoid affecting system performance. If there are multiple tasks, they will be queued up one after another.

You can check the archive result in the following ways.

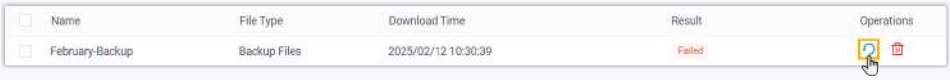
Check the archive result on PBX

On PBX web portal, go to **System > Archive > Archival Logs**. If the **Result** column of the task shows **Succeeded**, it indicates that the specified files have been successfully archived to SFTP server.



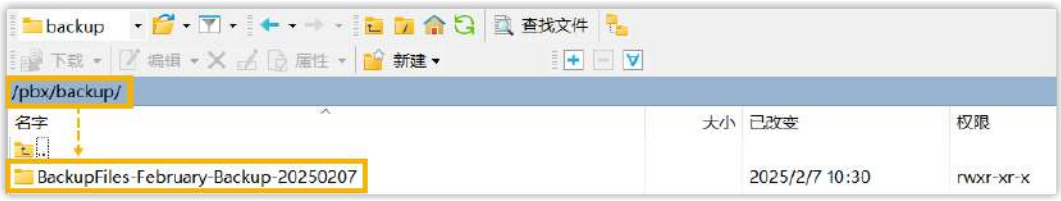
Note:

If the task is failed, the **Failed to Archive File(s)** event will be triggered; You can click to retry the task.



Check the archive result on SFTP server

Go to the designated folder in SFTP server. If the specified files appear in the list, it indicates that the archive is successful.



Archive Files to Amazon S3

Yeastar P-Series Software Edition supports archiving the system's call recordings and backup files to Amazon S3, either on a regular interval or at any time you want. This topic describes how to add Amazon S3 bucket as an archive server and schedule tasks to archive the desired files.

Requirements and restrictions

Requirements

- **PBX Firmware**: Version 83.18.0.59 or later
- **PBX Plan**: Enterprise Plan

Restrictions

- **Archive server**: 10
- **Archive task**: 200

Introduction

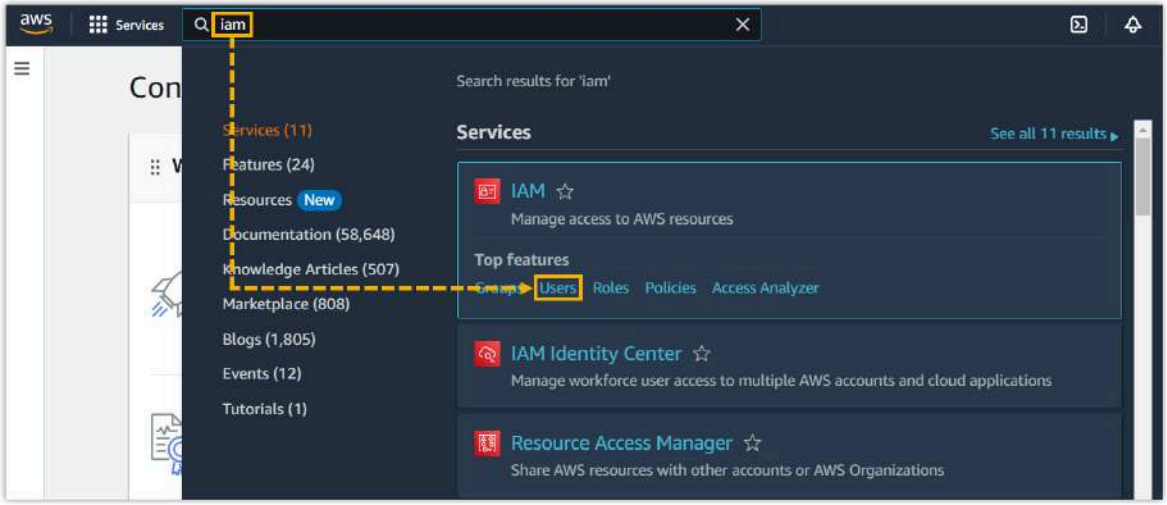
To archive PBX's call recordings and backup files to a specific bucket in Amazon S3, you need to complete the followings:

1. Prepare an eligible account and bucket on AWS.
   - An **IAM User** account that meets the requirements listed below:
     - Full access to Amazon S3 resources to archive PBX files
     - An access key pair (including an access key ID and a secret access key) to authenticate file archiving requests from PBX
   - An **S3 bucket** to store archived PBX files
2. Set up archive server and task on PBX.
   - Add the Amazon S3 bucket as an archive server
   - Create tasks to archive PBX files to Amazon S3

When it is time to execute the archive task, PBX will use the access key pair of the IAM user to send file archiving requests to Amazon S3. If the requests are considered authentic, the specified files will be archived to the designated bucket in Amazon S3.

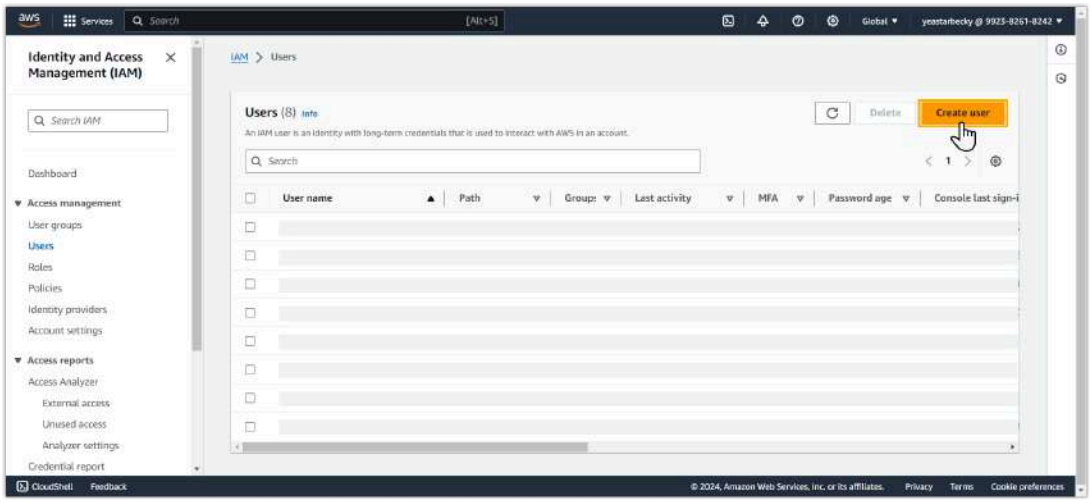
Step 1. Create an IAM user with full access to Amazon S3 bucket on AWS

1. Log in to AWS Management Console.
2. At the top of the console, search for IAM service and select **Users**.

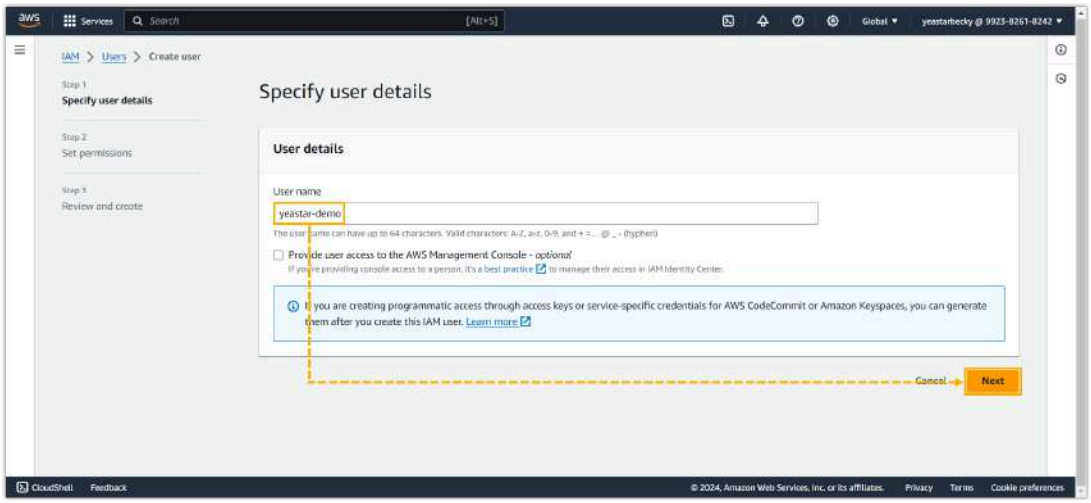


You are redirected to the IAM users page.

3. Create an IAM user and grant the user full access to Amazon S3 bucket.
   a. At the top-right corner, click **Create user**.

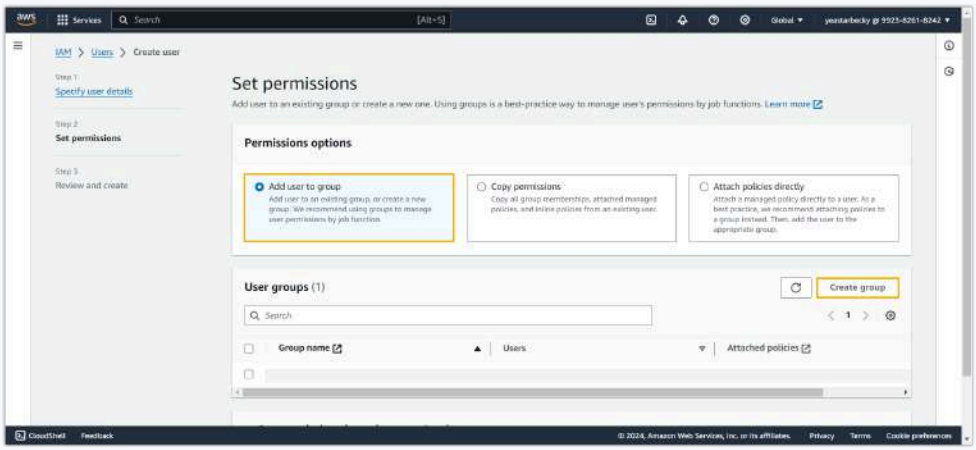


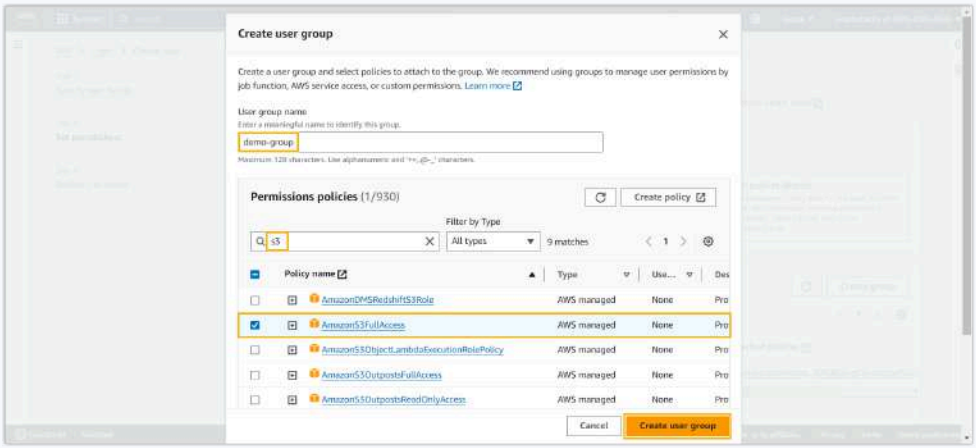
   b. On the **Specify user details** page, enter a name in the **User name** field to help you identify the IAM user, then click **Next**.

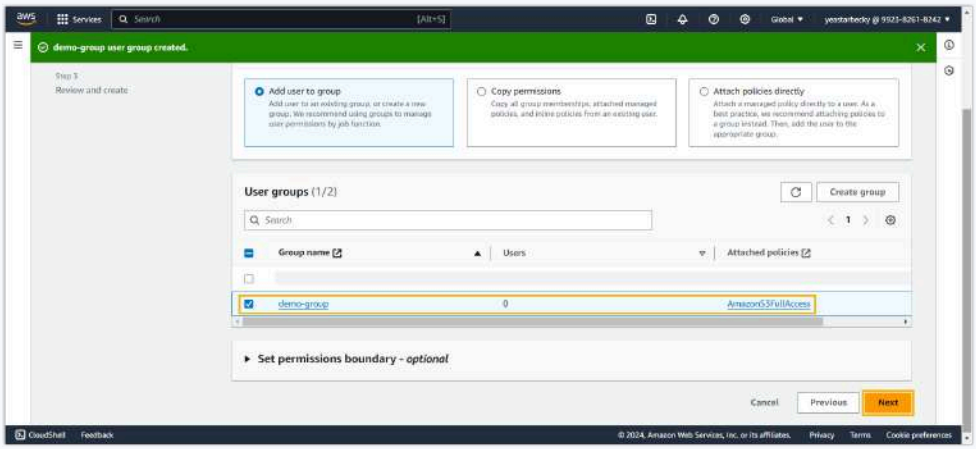


   c. On the **Set permissions** page, grant the user full access to Amazon S3 buckets, then click **Next**.

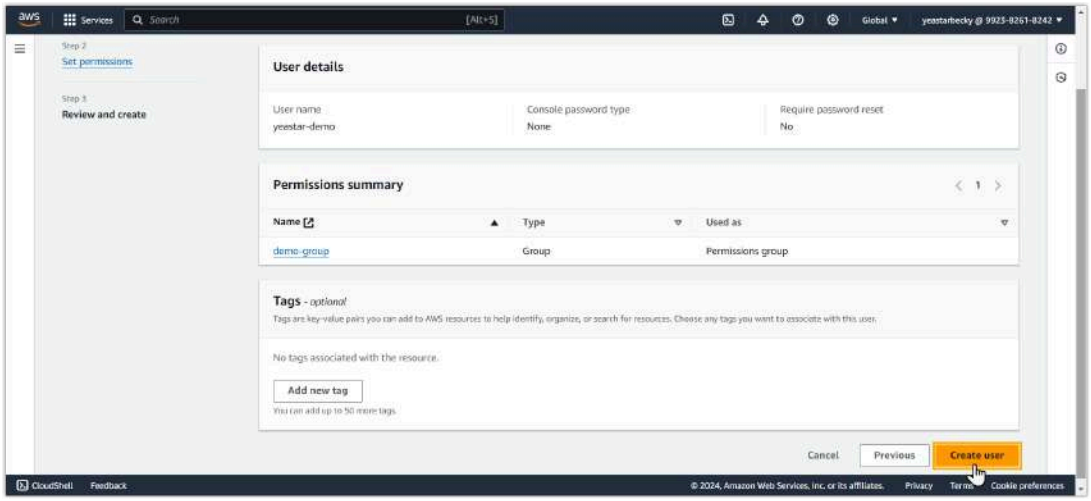
> **Note:**
> You can grant permission to the user by adding the user to an existing group, creating a new group, or attaching permission policy directly to the user.
>
> In this example, we create a new group with full Amazon S3 access permission and add the user to the group, as the following figure shows.





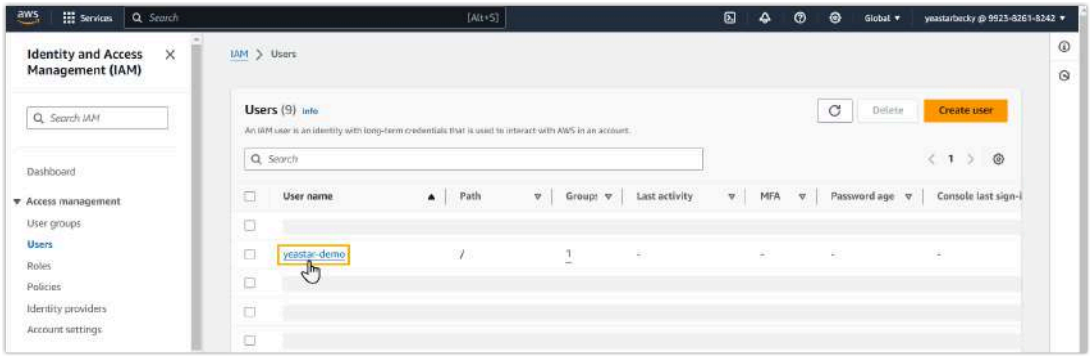


d. On the **Review and create** page, click **Create user**.

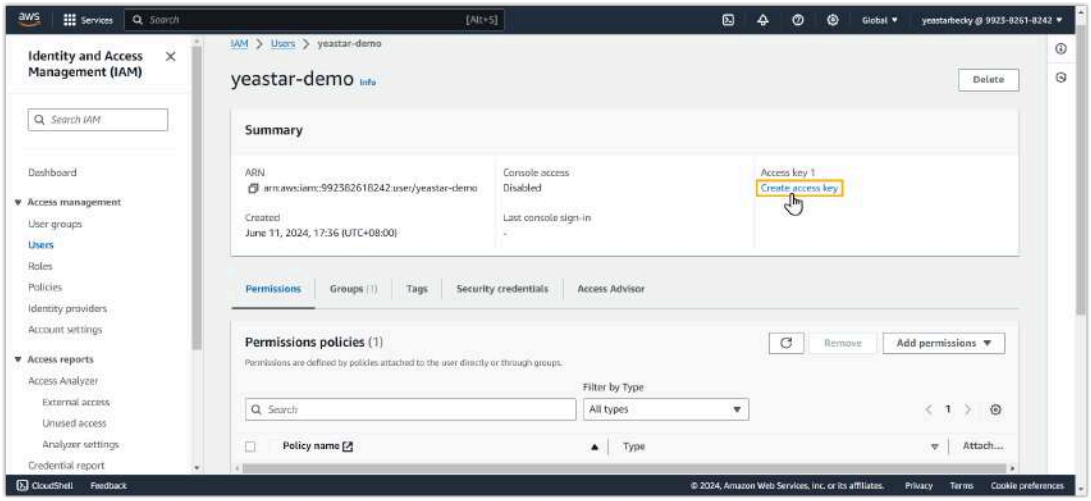


The IAM user with full access to Amazon S3 bucket is created and displayed on the users list.

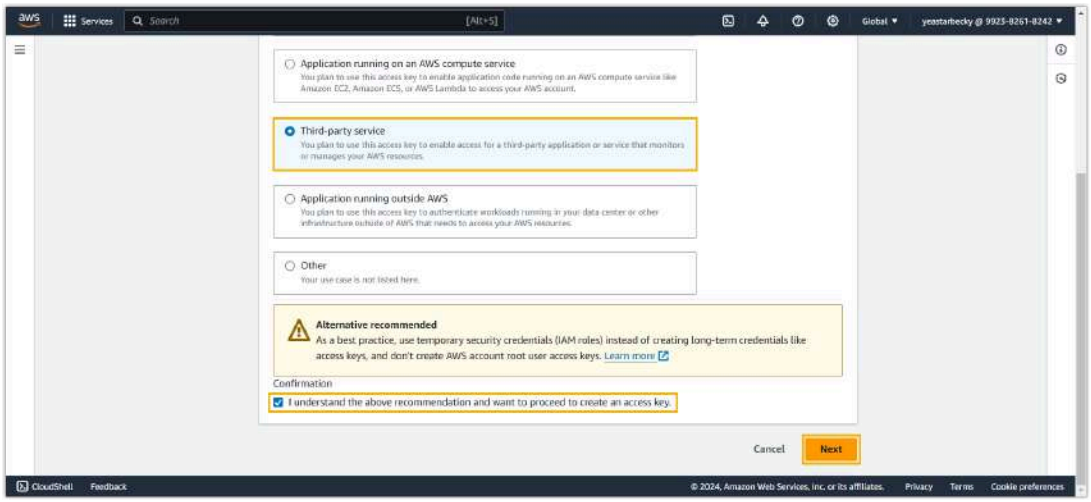
4. Create an access key for the IAM user.
   a. On the users list, click on the newly created IAM user to enter the details page.



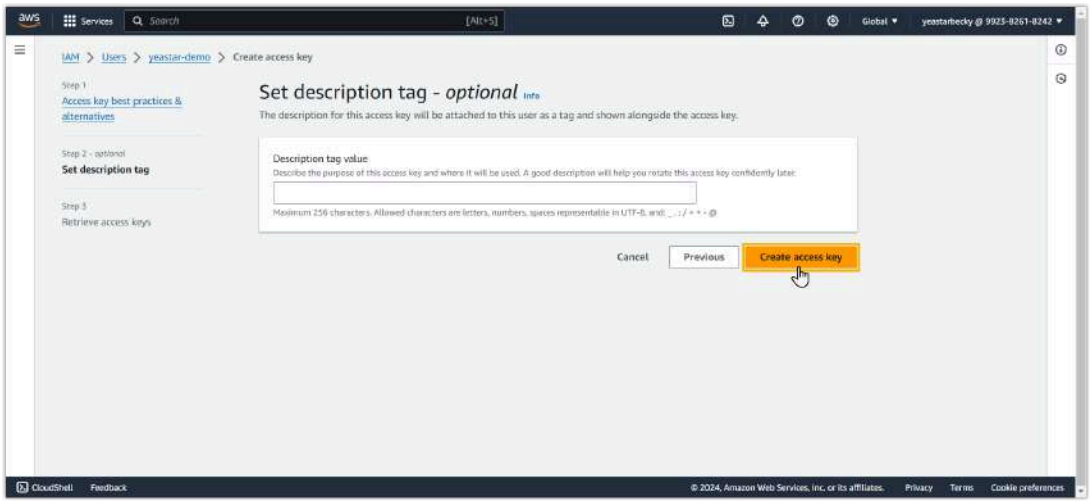
   b. In the **Summary** section, click **Create access key**.



c. On the **Access key best practices & alternatives** page, select **Third-party service**, confirm your operation, then click **Next**.

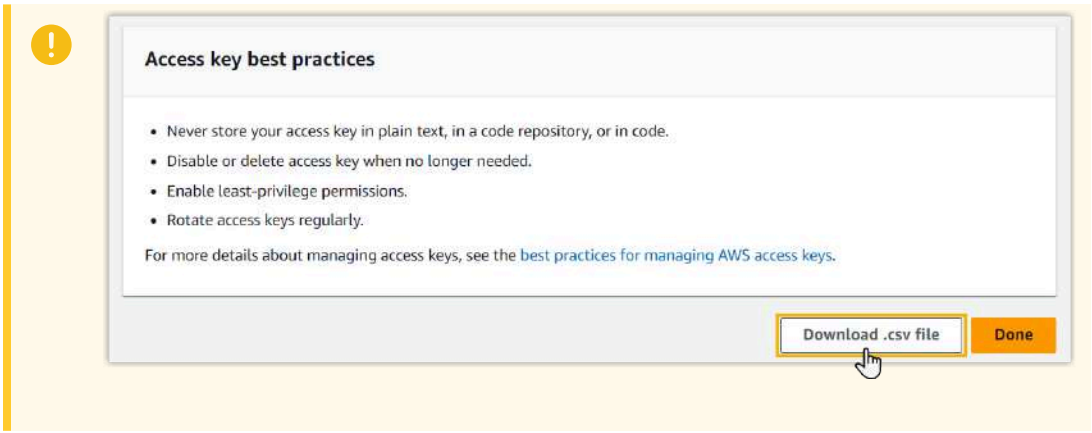


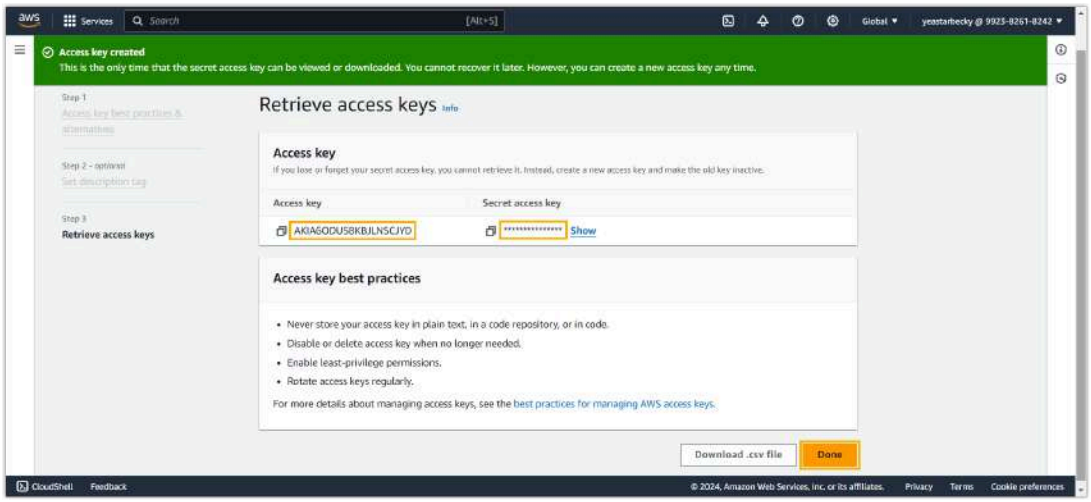
d. On the **Set description tag - optional** page, enter a description for the access key as needed, then click **Create access key**.



e. In the **Retrieve access keys** page, copy and note down the values of **Access key** and **Secret access key**, then click **Done**.

> **Important:**
> For **Secret access key**, the value is shown only ONCE, so make sure that you save the credential in a secure location before clicking **Done** to close the window. We recommend that you click **Download .csv file** to save the credential file to your computer.

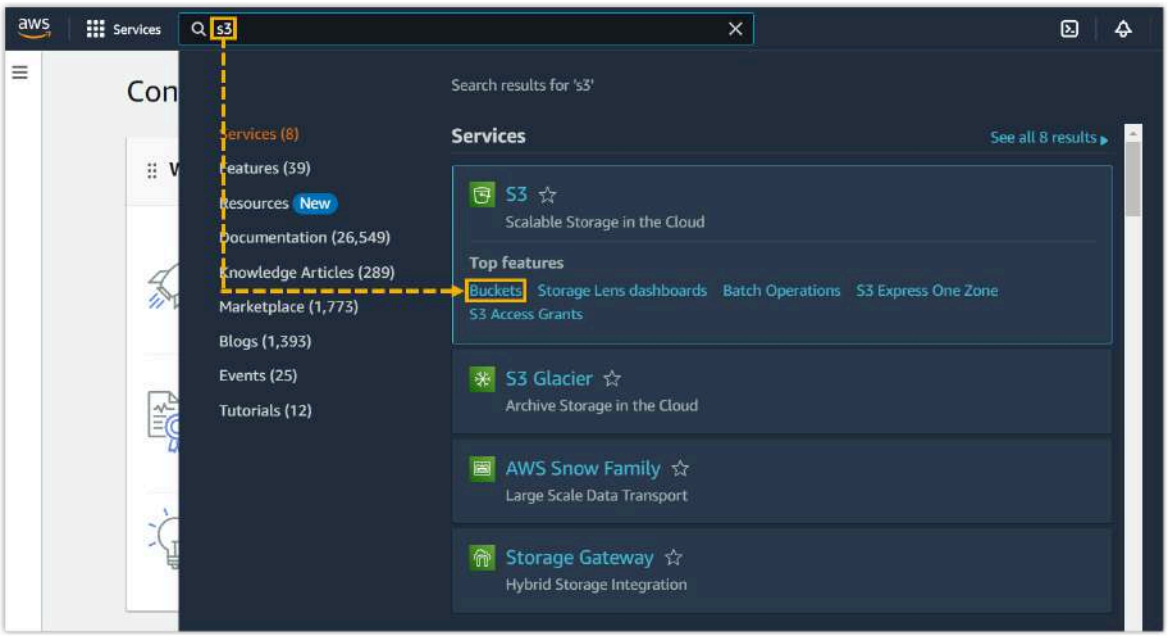




The access key is created and displayed on the access key list.

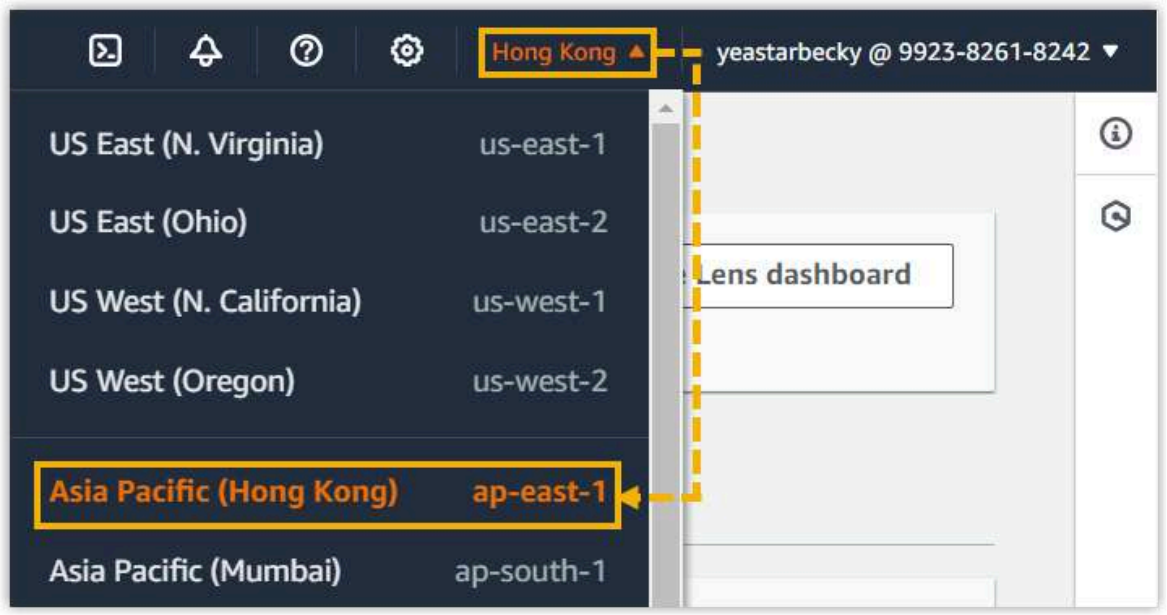
Step 2. Create an Amazon S3 bucket on AWS

1. On AWS Management Console, search for S3 service in the top-left search bar, then select **Buckets**.

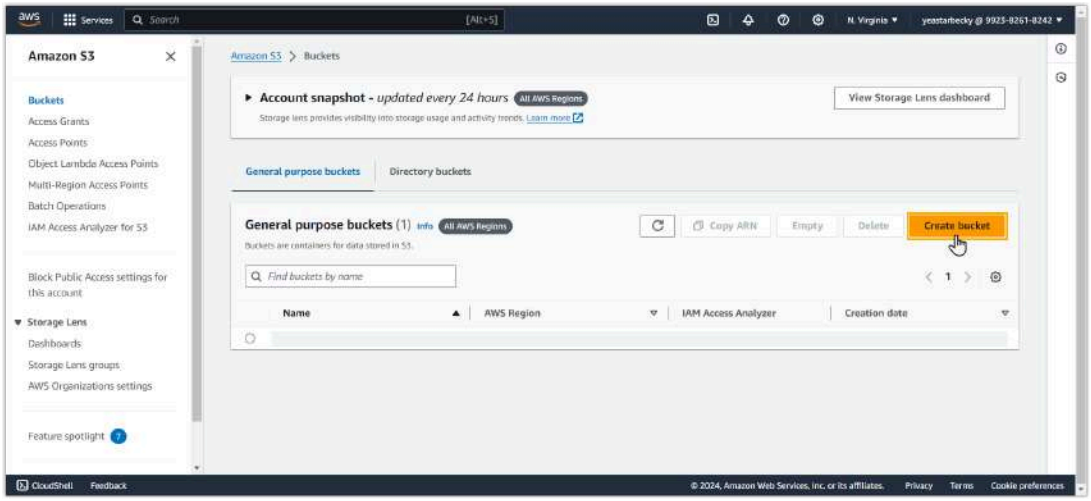


2. At the top-right corner, select the region in which you want to create an S3 bucket.

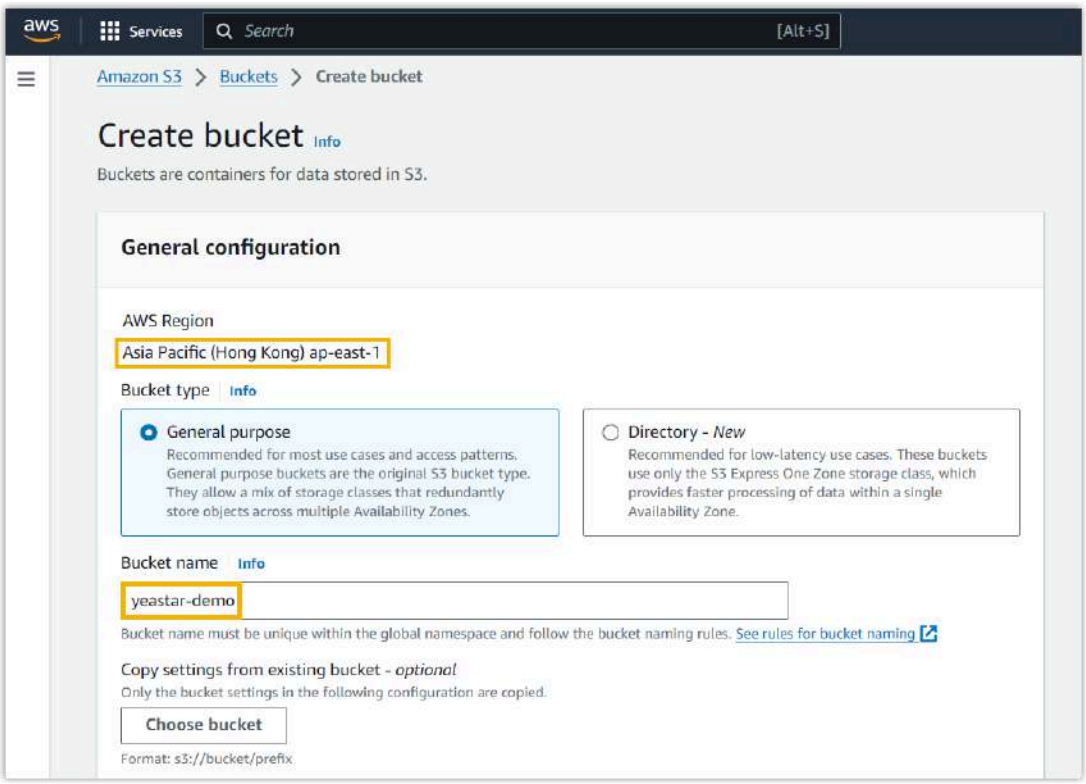
> **Note:**
> To minimize latency and costs and address regulatory requirements, choose a region that is closest to your PBX server.



3. Create an S3 bucket.
    a. On the right of the page, click **Create bucket**.



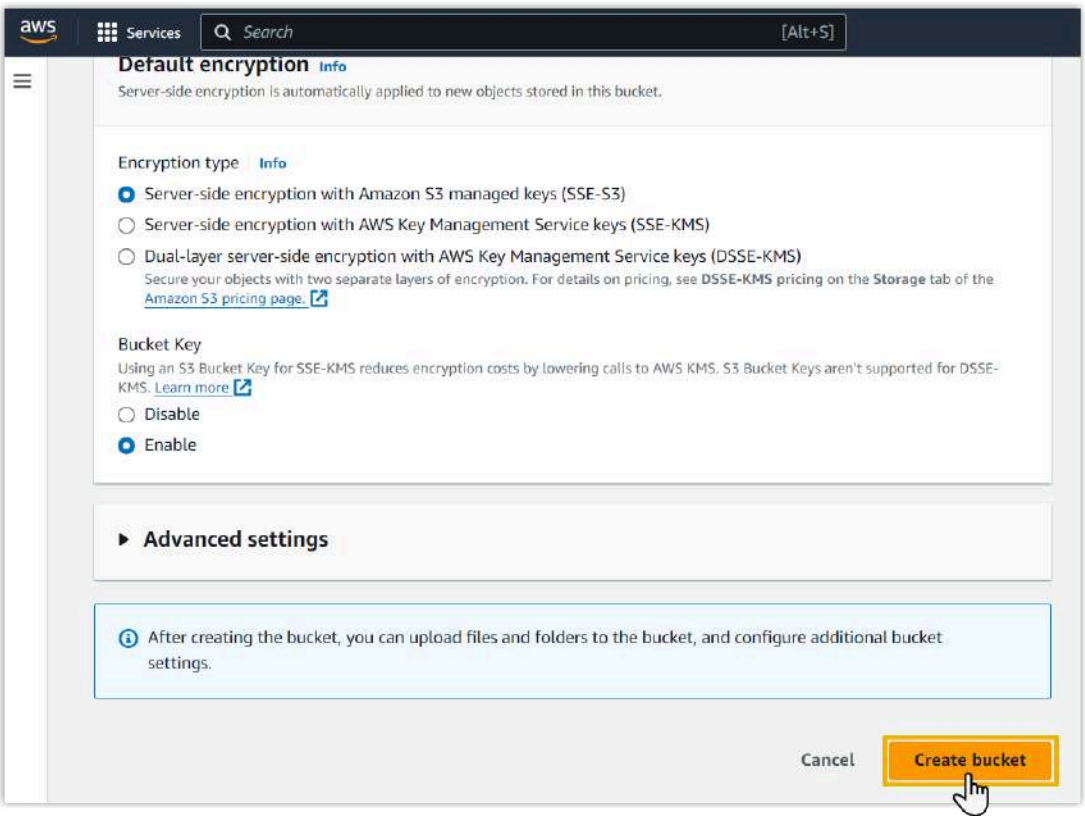
b. Check the region where the bucket will be created and specify a name for the bucket.



- **AWS Region**: Automatically show the region that you have selected.
- **Bucket name**: Enter a name to help you identify the bucket.

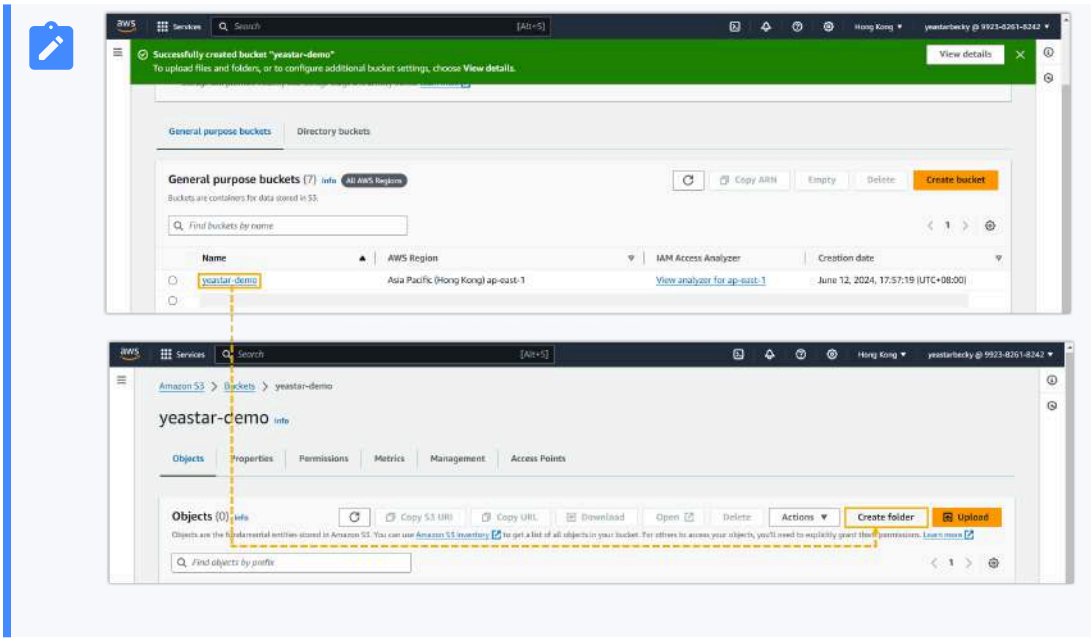
c. Configure other settings according to your needs.

d. At the bottom of the page, click **Create bucket**.



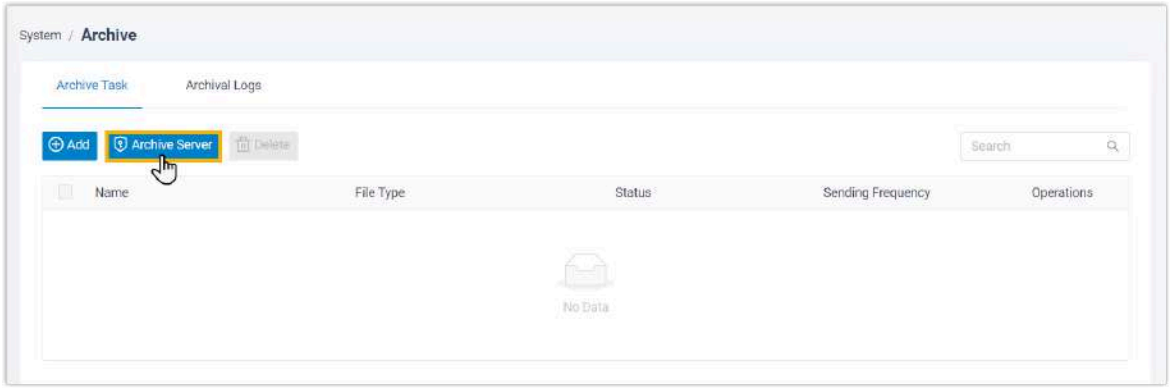
The S3 bucket is created and displayed on the buckets list.

Note:
If you want to group the archived PBX files in Amazon S3, you can create folders in the bucket. In this way, you can specify PBX files to be archived to the designated folder in the follow-up settings.

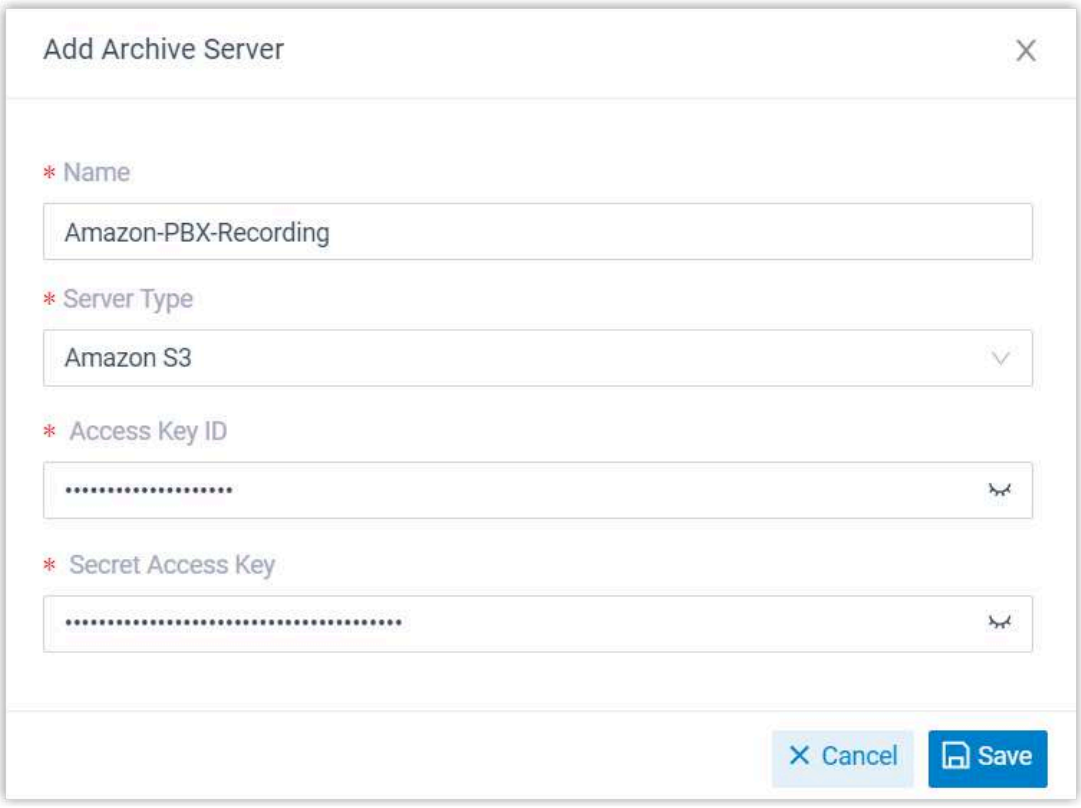


Step 3. Add Amazon S3 bucket as archive server on PBX

1. Log in to PBX web portal, go to **System > Archive**.
2. Under the **Archive Task** tab, click **Archive Server**.



3. Set up Amazon S3 bucket as an archive server.
    a. Click **Add**.
    b. In the pop-up window, complete the following settings.



Setting	Description
Name	Enter a name to help you identify the server.
Server Type	Select **Amazon S3**.
Access Key ID	Enter the access key that you have obtained from AWS.
Secret Access Key	Enter the secret access key that you have obtained from AWS.

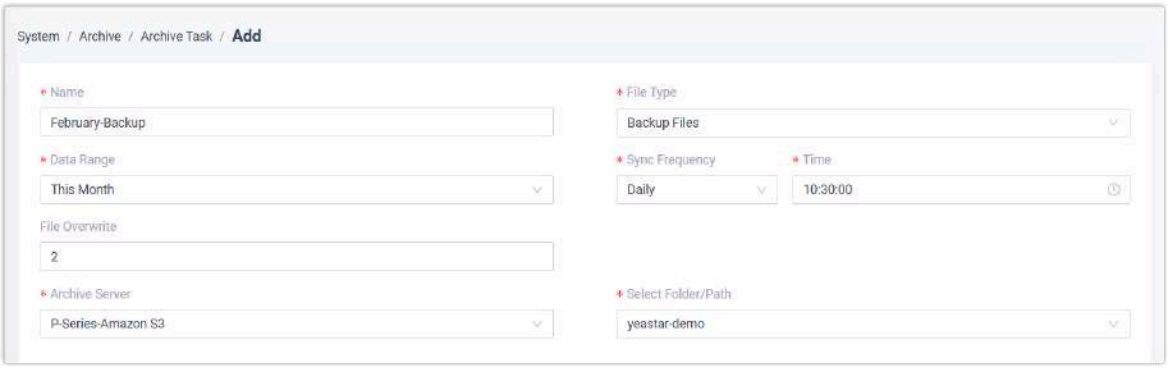
c. Click **Save**.

The Amazon S3 bucket is added as an archive server and displayed on the archive server list.

4. Click ✕ to close the window.

Step 4. Create a task to archive files to Amazon S3 on PBX

1. Under **Archive Task** tab, click **Add**.
2. Create a one-time or recurring archive task.



Setting	Description
Name	Enter a name to help you identify the task.
File Type	Select **Recording Files** or **Backup Files** as needed.
Data Range	Specify a time range of the files to be archived. **Note:** You can archive files for up to 31 days at a time.
Sync Frequency	Set how often to archive files to Amazon S3. **Note:** As large amounts of data will consume PBX's CPU resources, we recommend that you schedule archive tasks during off-peak hours. • **Once**: If you choose the option, the system will archive files immediately after you save the task. • **Daily**: If you choose the option, select a time from the drop-down list. The system will archive files at this time of the day. • **Weekly**: If you choose the option, choose a day of week and select a time from the drop-down list. The system will archive files at this time of the week. • **Monthly**: If you choose the option, choose a day and select a time from the drop-down list. The system will archive files on this day and time of the month.
File Overwrite	Optional. Set the maximum number of files to be retained in the Amazon S3 bucket for the archive task. **Note:** • This option is available only when you schedule to archive backup files on a recurring basis.

Setting	Description
	• When it reaches the limit, the system will retain the latest backup files and delete the earlier ones.
Archive Server	Select the Amazon S3 bucket that you have added.
Select Folder/Path	Select the bucket or the folder in which you want to store archived files.

3. Click **Save**.

Result

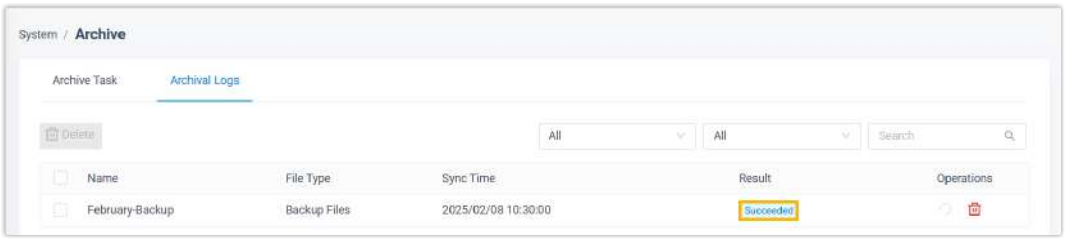
The specified files will be archived to the designated bucket or folder in Amazon S3 immediately or at the scheduled time.

Note:
The system executes only one task at a time to avoid affecting system performance. If there are multiple tasks, they will be queued up one after another.

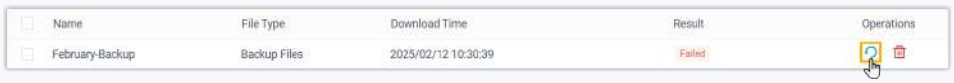
You can check the archive result in the following ways.

Check the archive result on PBX

On PBX web portal, go to **System > Archive > Archival Logs**. If the **Result** column of the task shows **Succeeded**, it indicates that the specified files have been successfully archived to Amazon S3.

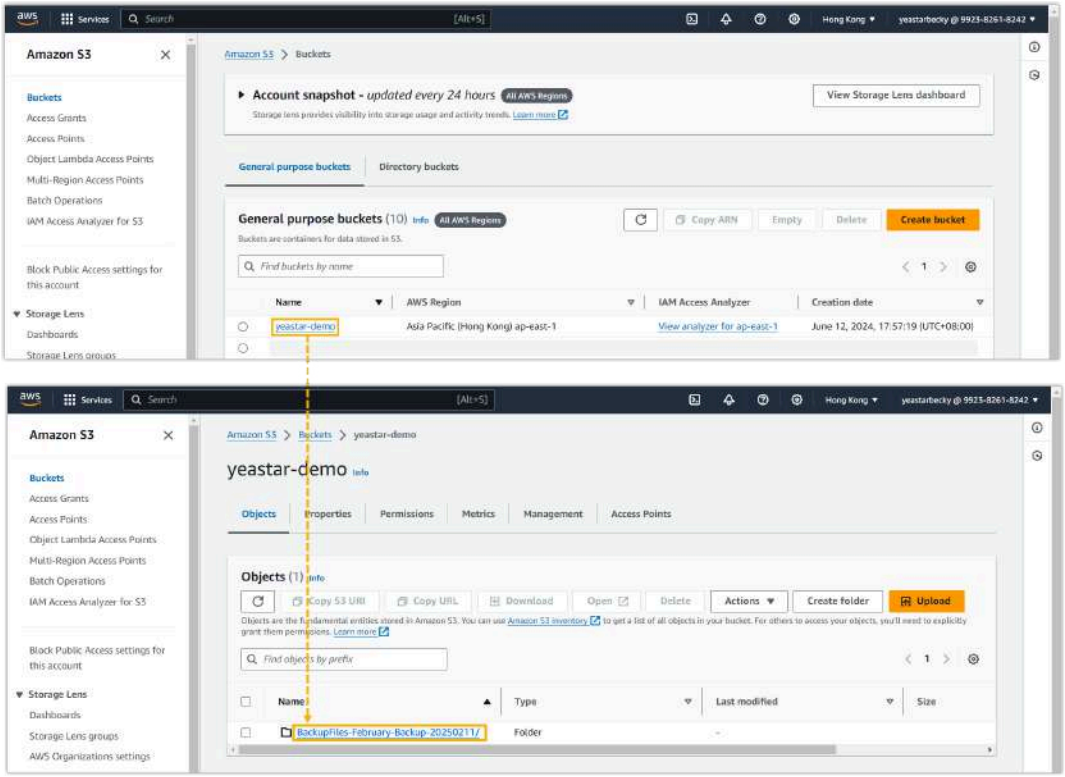


Note:
If the task is failed, the **Failed to Archive File(s)** event will be triggered; You can click to retry the task.



Check the archive result on AWS

On AWS Management Console, go to the created S3 bucket. If the specified files appear in the list, it indicates that the archive is successful.



Archive Files to Google Cloud Storage

Yeastar P-Series Software Edition supports archiving the system's call recordings and back-up files to Google Cloud Storage, either on a regular interval or at any time you want. This topic describes how to add Google Cloud Storage bucket as an archive server and schedule tasks to archive the desired files.

Requirements and restrictions

Requirements

- **PBX Firmware**: Version 83.18.0.59 or later
- **PBX Plan**: Enterprise Plan

Restrictions

- **Archive server**: 10
- **Archive task**: 200

Introduction

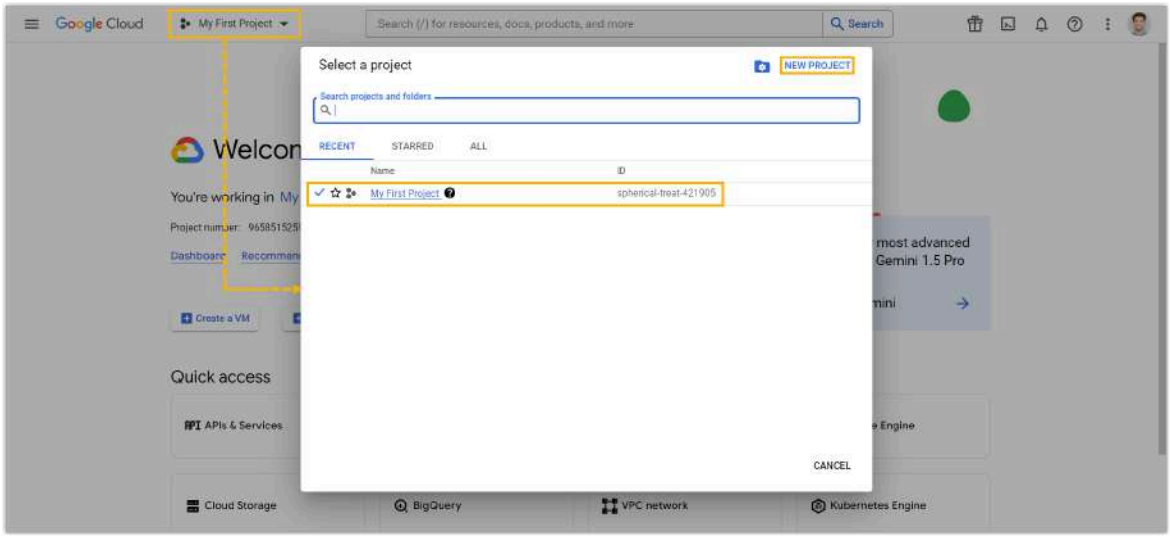
To archive PBX's call recordings and backup files to a specific bucket in Google Cloud Storage, you need to complete the followings:

1. Prepare an eligible account and bucket on Google Cloud.
   - A **service account** that meets the requirements listed below:
     - Full access to Google Cloud Storage resources to archive PBX files
     - An access key to authenticate file archiving requests from PBX
   - A **bucket** to store archived PBX files
2. Set up archive server and task on PBX.
   - Add the Google Cloud Storage bucket as an archive server
   - Create tasks to archive PBX files to Google Cloud Storage

When it is time to execute the archive task, PBX will use the access key of the service account to send file archiving requests to Google Cloud Storage. If the requests are considered authentic, the specified files will be archived to the designated bucket in Google Cloud Storage.

Step 1. Create a service account on Google Cloud

1. Log in to Google Cloud Console.
2. On the project selector page, select or create a Google Cloud project.

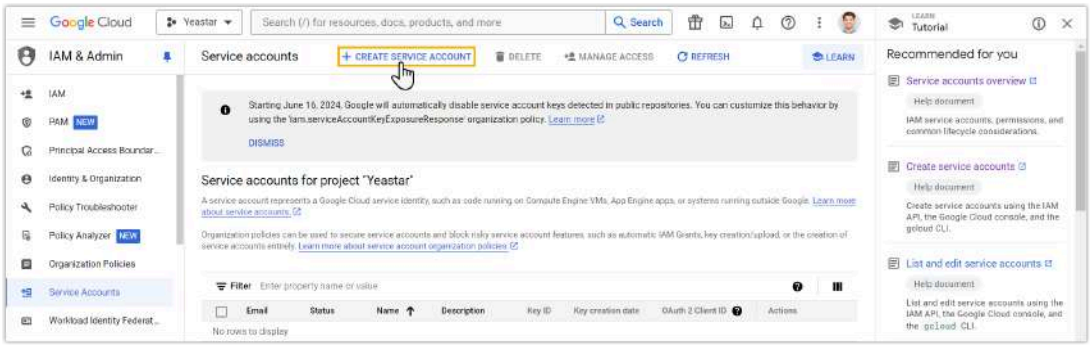


In this example, we create a new project "Yeastar".

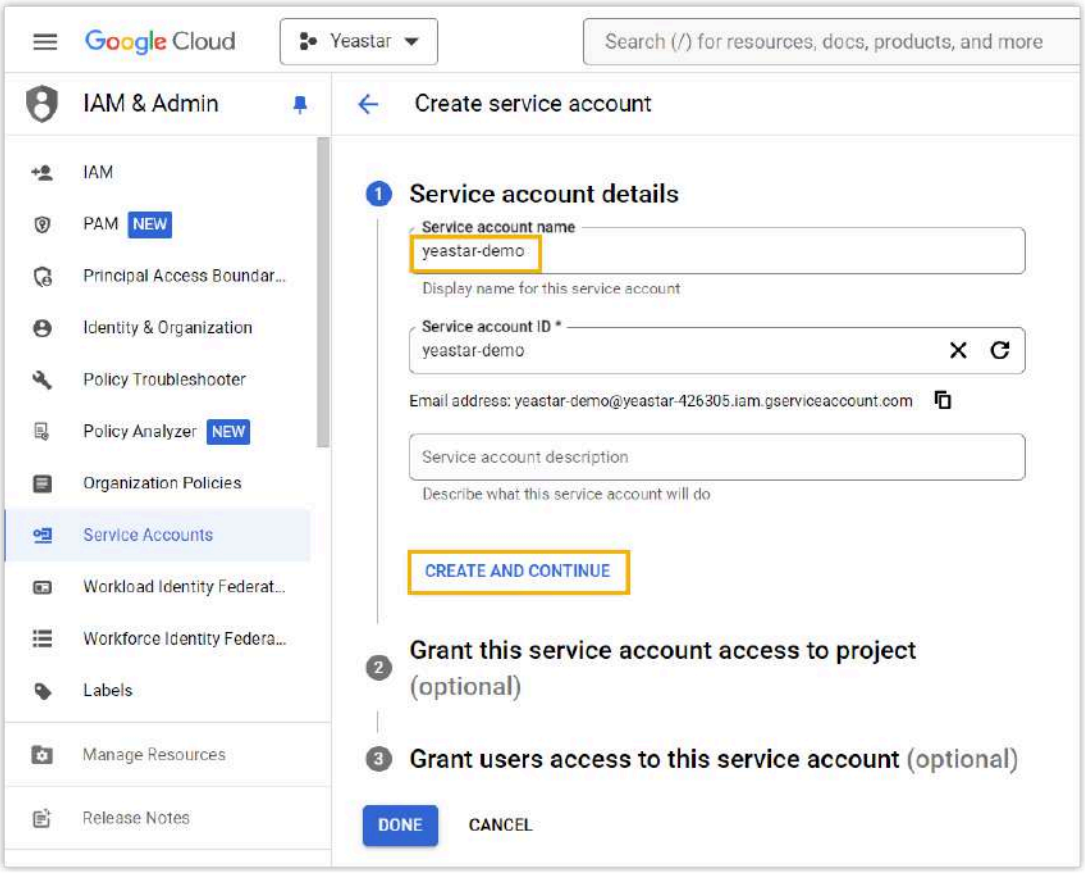
3. Create a service account.

   a. In the top search bar, search for and select **Service Accounts**.

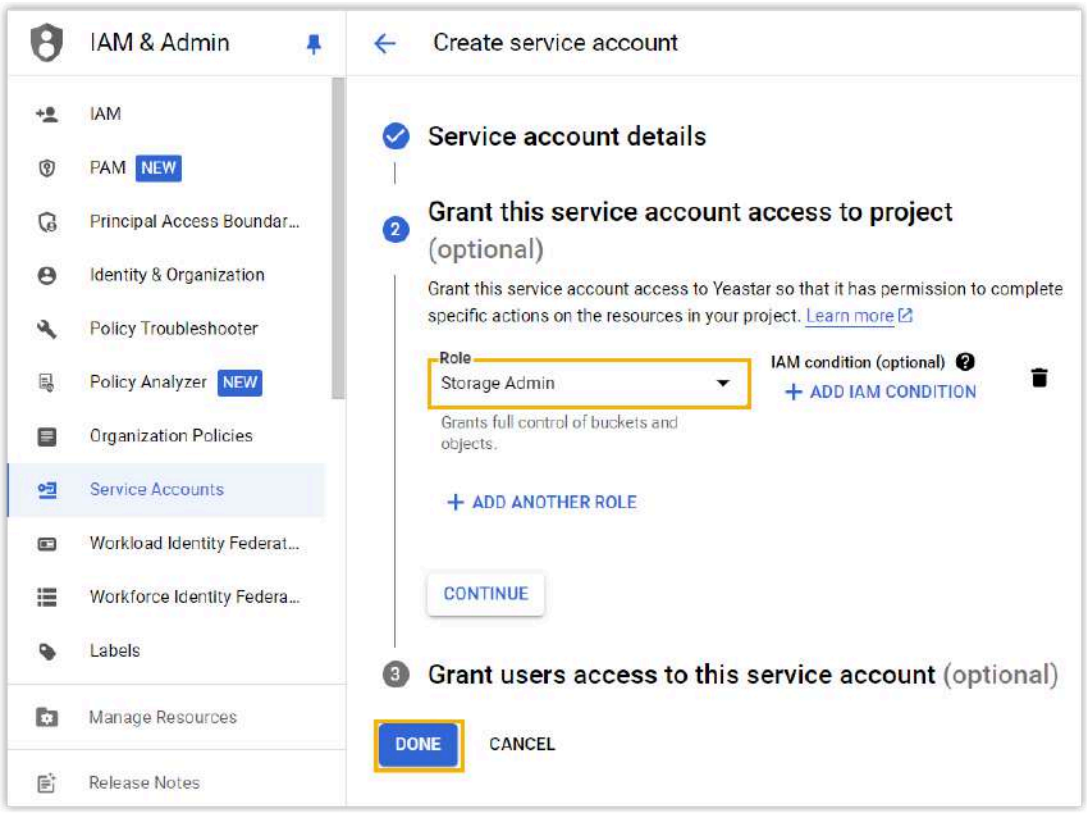
   b. In the top pane, click **CREATE SERVICE ACCOUNT**.



   c. In the **Service account details** section, enter a name in the **Service account name** field to help you identify the account, then click **CREATE AND CONTINUE**.



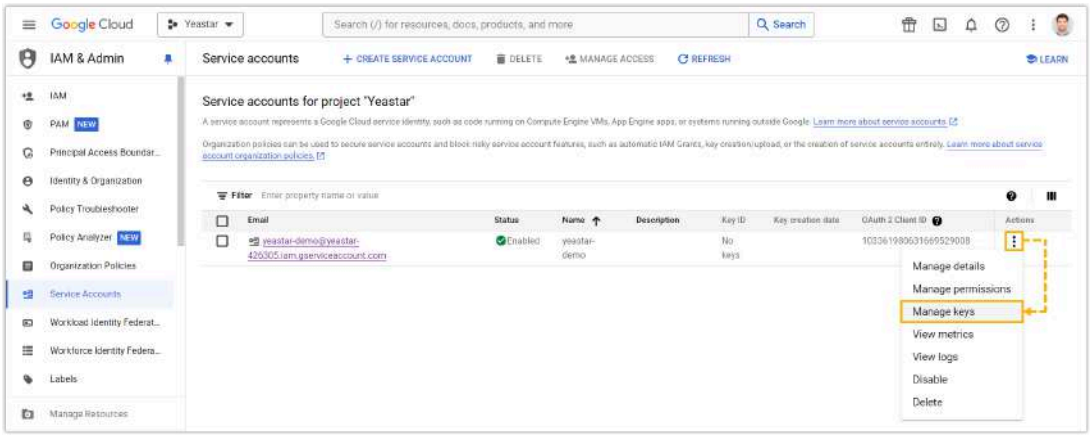
d. In the **Grant this service account access to project (optional)** section, search and select **Storage Admin** from the **Role** drop-down list, then click **DONE**.



The service account is created and displayed on the service accounts list.

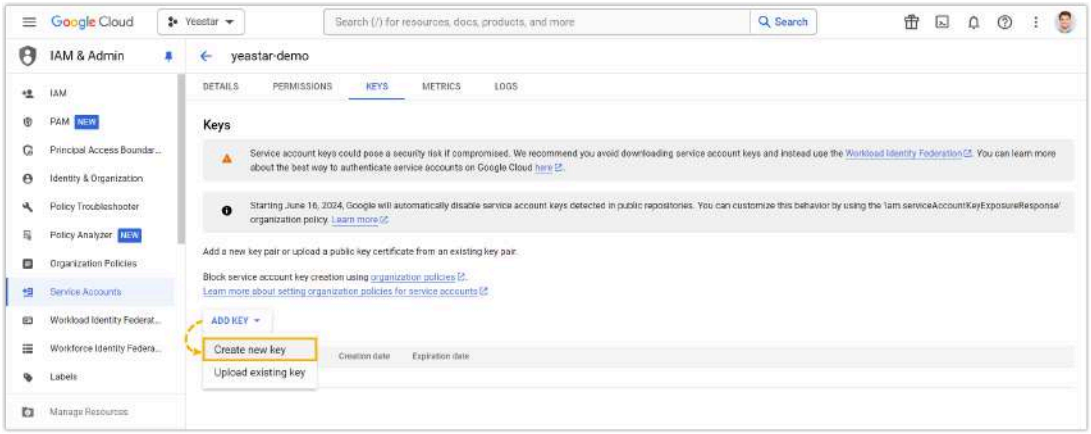
4. Create an access key for the service account.

   a. On the service accounts list, click ⋮ beside the service account that you have created, then select **Manage keys**.

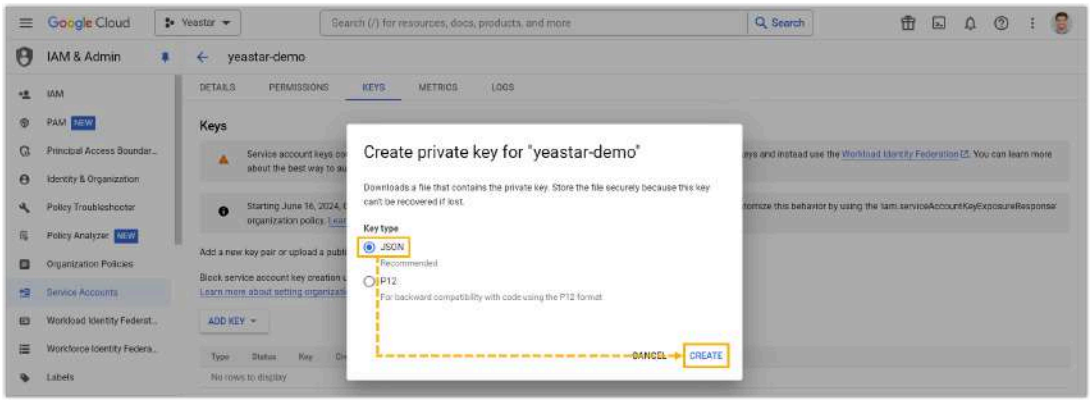


You are redirected to the key configuration page.

   b. Click **ADD KEY**, then select **Create new key** from the drop-down list.



c. Set **Key type** to **JSON**, then click **CREATE**.



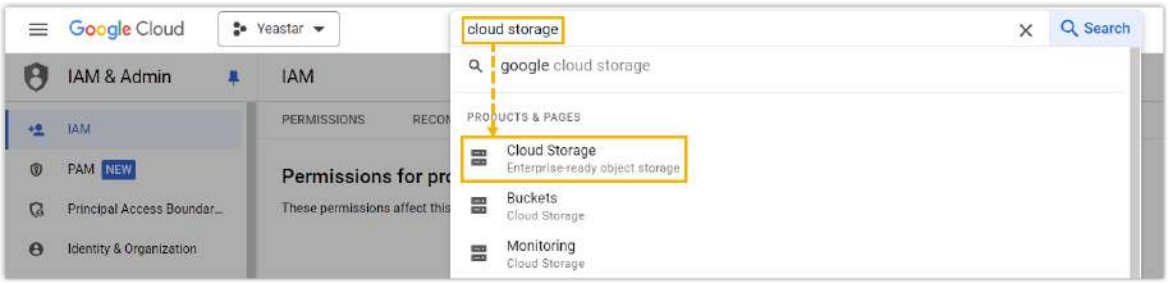
The access key is created and automatically downloaded to your computer as a JSON file.

> **Note:**
> Save the JSON file in a secure location, as you will need the file when setting up Google Cloud Storage bucket as archive server on PBX.

d. Click **CLOSE** to close the pop-up window.

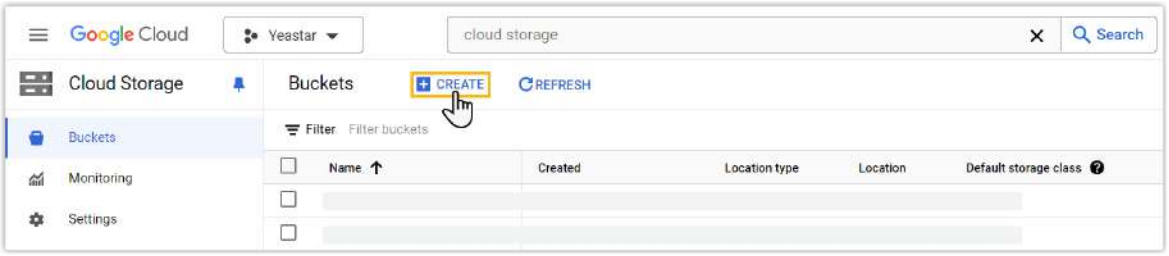
Step 2. Create a bucket on Google Cloud Storage

1. In the top search bar, search for and select **Cloud Storage**.

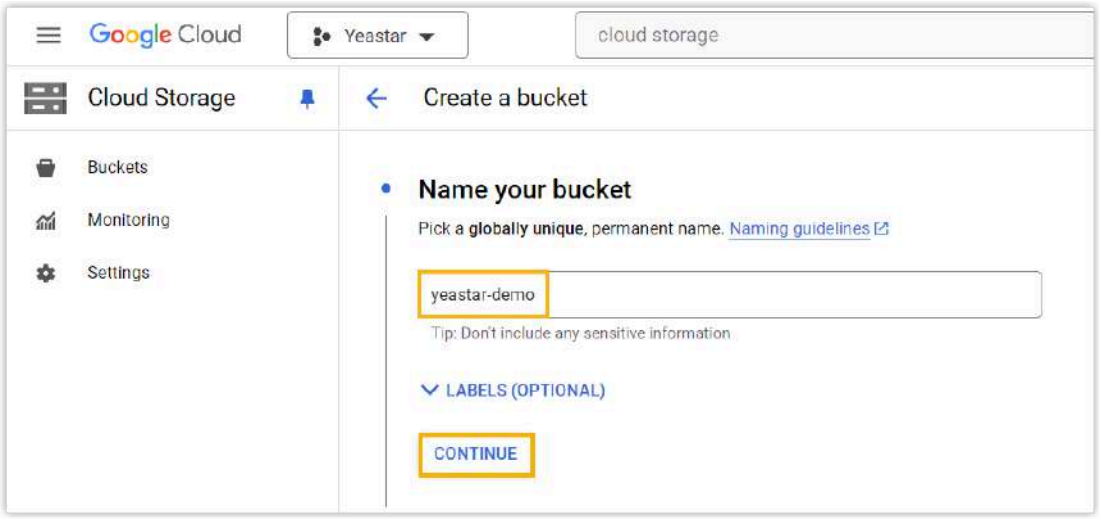


You are redirected to buckets configuration page.

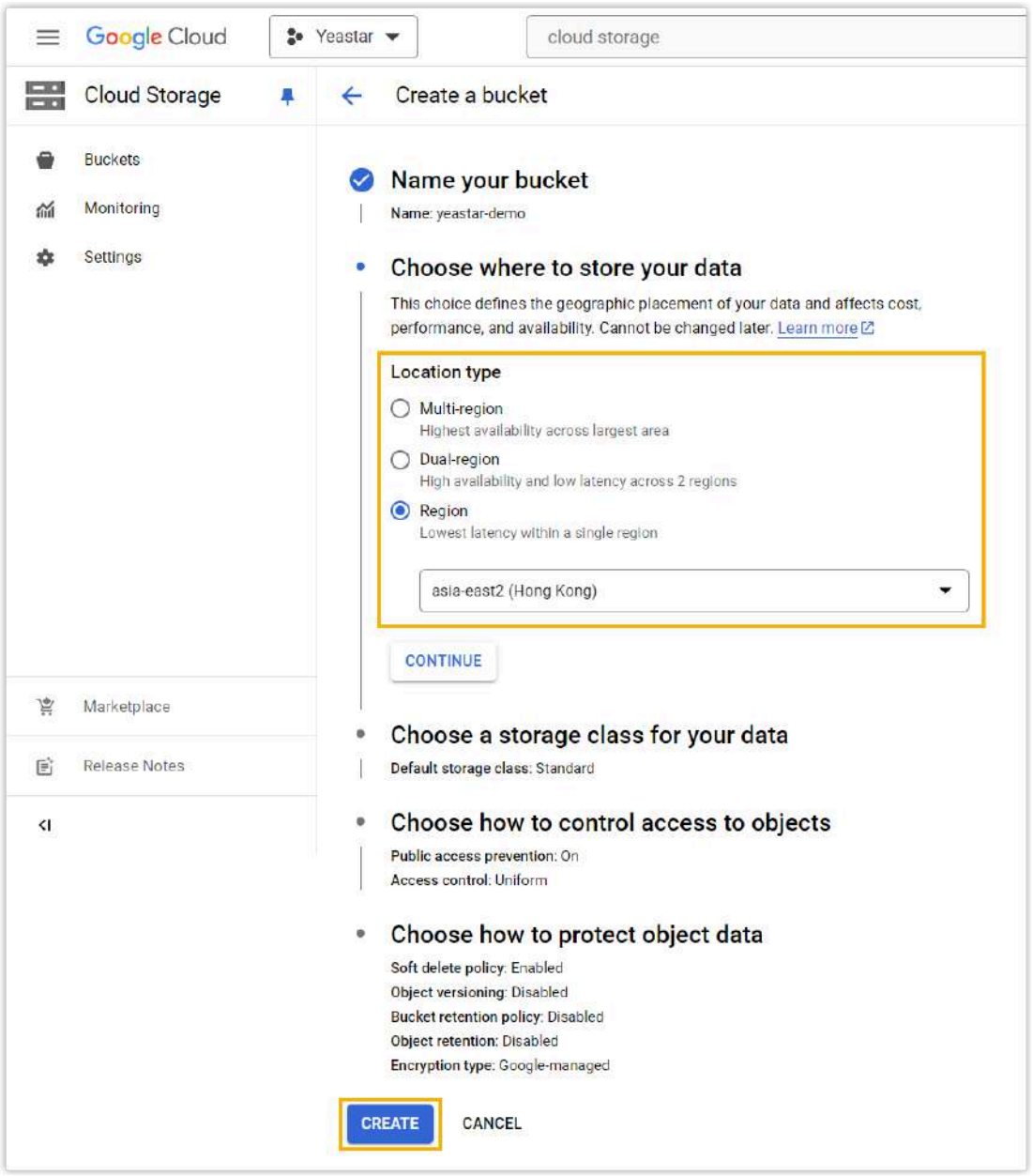
2. In the top pane, click **CREATE**.



3. In the **Name your bucket** field, enter a name to help you identify the bucket, then click **CONTINUE**.

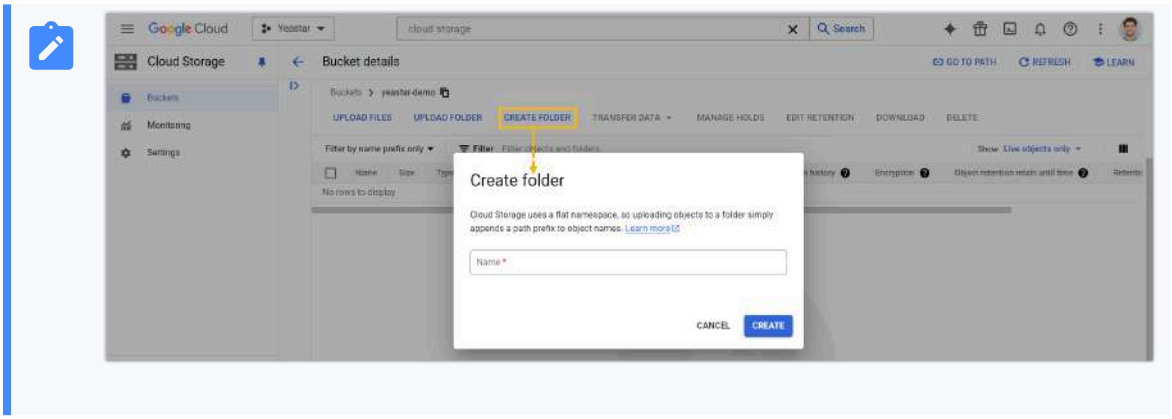


4. In the **Choose where to store your data** section, select the region in which you want to create a bucket, then click **CREATE**.



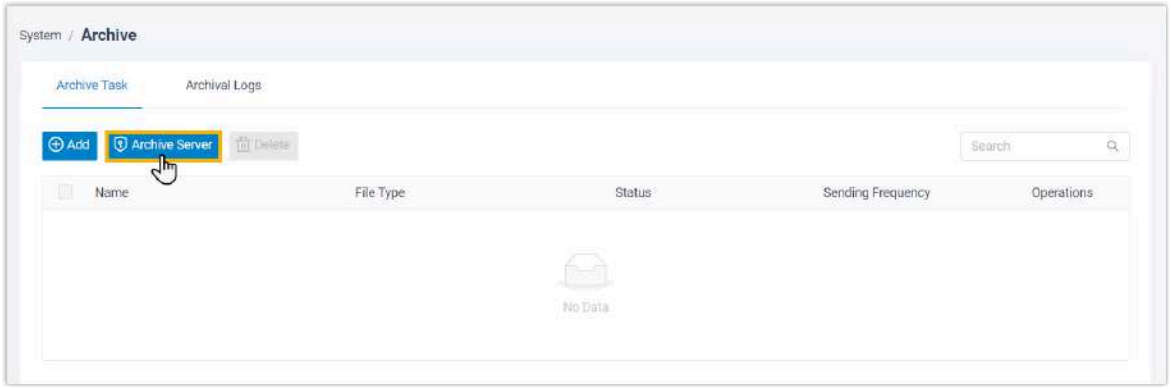
The bucket is created.

> **Note:**
> If you want to group the archived PBX files in Google Cloud Storage, you can create folders in the bucket. In this way, you can specify PBX files to be archived to the designated folder in the follow-up settings.

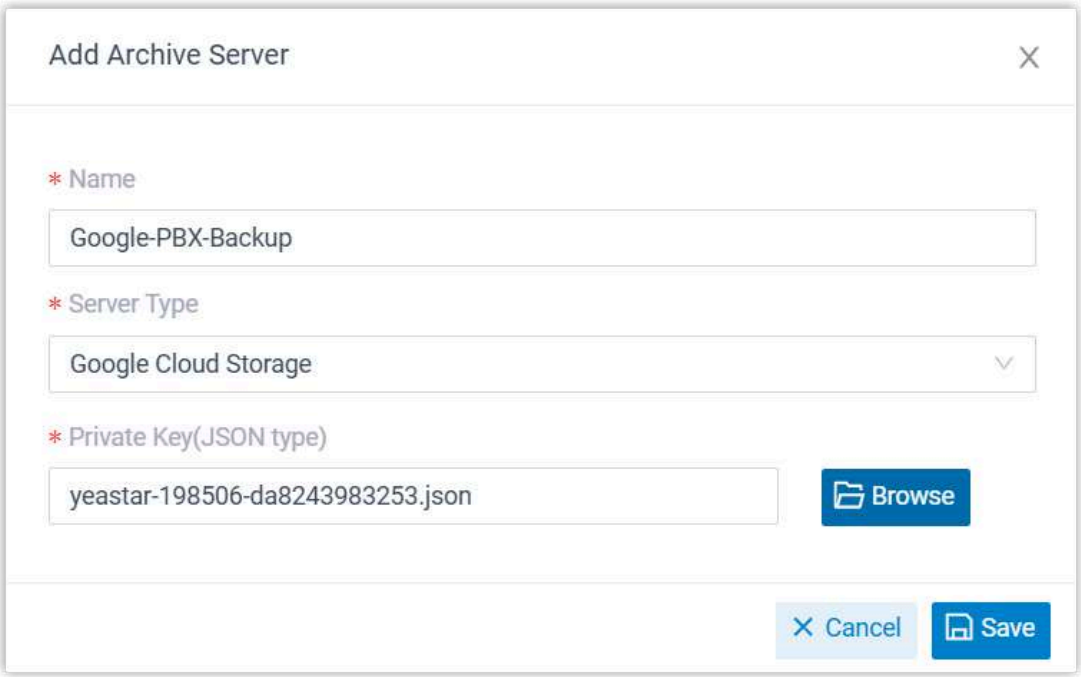


Step 3. Add Google Cloud Storage bucket as archive server on PBX

1. Log in to PBX web portal, go to **System > Archive**.
2. Under the **Archive Task** tab, click **Archive Server**.



3. Set up Google Cloud Storage bucket as an archive server.
    a. Click **Add**.
    b. In the pop-up window, complete the following settings.



Setting	Description
Name	Enter a name to help you identify the server.
Server Type	Select **Google Cloud Storage**.
Private Key(JSON type)	Click **Browse** to browse and upload the JSON file that you have downloaded in Google Cloud.

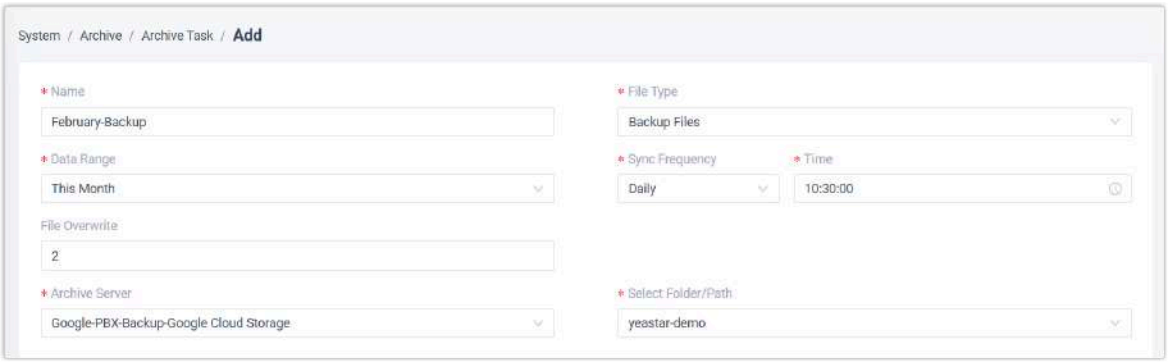
c. Click **Save**.

The Google Cloud Storage bucket is added as an archive server and displayed on the archive server list.

4. Click ✕ to close the window.

Step 4. Create a task to archive files to Google Cloud Storage on PBX

1. Under **Archive Task** tab, click **Add**.
2. Create a one-time or recurring archive task.



Setting	Description
Name	Enter a name to help you identify the task.
File Type	Select **Recording Files** or **Backup Files** as needed.
Data Range	Specify a time range of the files to be archived. **Note:** You can archive files for up to 31 days at a time.
Sync Frequency	Set how often to archive files to Google Cloud Storage. **Note:** As large amounts of data will consume PBX's CPU resources, we recommend that you schedule archive tasks during off-peak hours. • **Once**: If you choose the option, the system will archive files immediately after you save the task. • **Daily**: If you choose the option, select a time from the drop-down list. The system will archive files at this time of the day. • **Weekly**: If you choose the option, choose a day of week and select a time from the drop-down list. The system will archive files at this time of the week. • **Monthly**: If you choose the option, choose a day and select a time from the drop-down list. The system will archive files on this day and time of the month.
File Overwrite	Optional. Set the maximum number of files to be retained in Google Cloud Storage for the archive task. **Note:** • This option is available only when you schedule to archive backup files on a recurring basis.

Setting	Description
	• When it reaches the limit, the system will retain the latest backup files and delete the earlier ones.
Archive Server	Select the Google Cloud Storage bucket that you have added.
Select Folder/Path	Select the bucket or the folder in which you want to store archived files.

3. Click **Save**.

Result

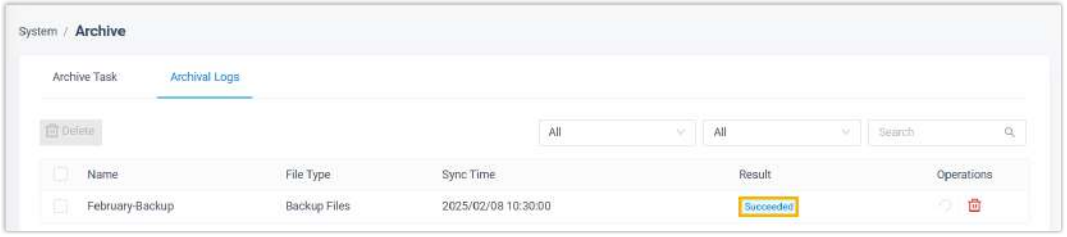
The specified files will be archived to the designated bucket or folder in your Google Cloud Storage immediately or at the scheduled time.

Note:
The system executes only one task at a time to avoid affecting system performance. If there are multiple tasks, they will be queued up one after another.

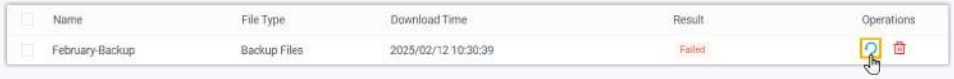
You can check the archive result in the following ways.

Check the archive result on PBX

On PBX web portal, go to **System > Archive > Archival Logs**. If the **Result** column shows **Succeeded**, it indicates that the specified files have been successfully archived to Google Cloud Storage.

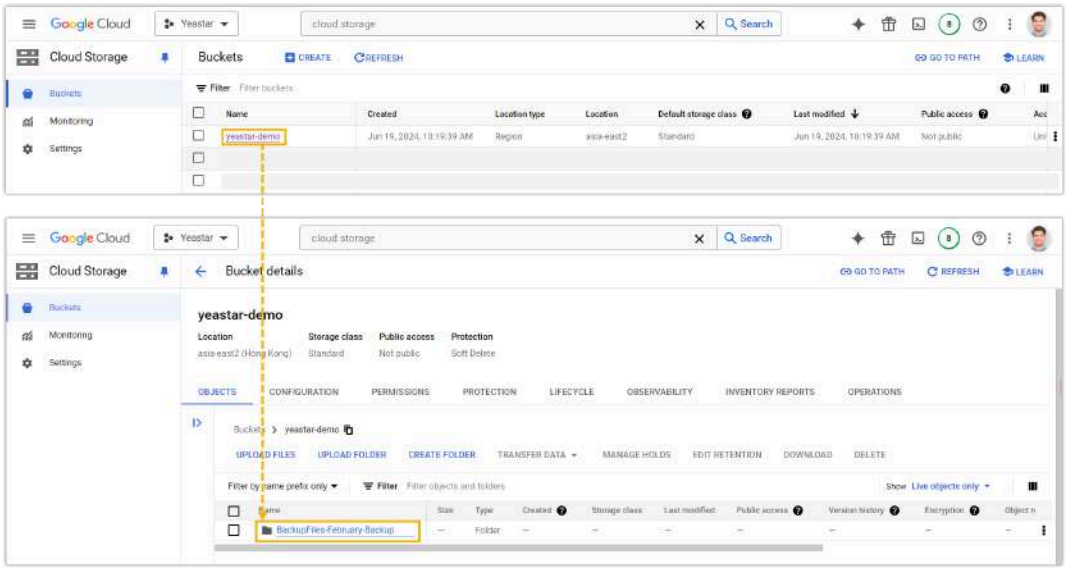


Note:
If the task is failed, the **Failed to Archive File(s)** event will be triggered; You can click to retry the task.



Check the archive result on Google Cloud Storage

On Google Cloud Console, go to the created bucket. If the specified files appear in the list, it indicates that the archive is successful.



Event Notification

Event Notification Overview

Event Notification feature is designed to provide information about changes on Yeastar P-Series 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 30. Operations

Event	Description
Administrator Login Success	The administrator successfully logged in to the PBX management portal.
Web User Login Success	A user successfully logged in to the PBX web portal or the Linkus Web Client.
Web User Login Failed	A user failed to log in to PBX web portal or the Linkus Web Client.
Linkus Client Login Failed	An extension user failed to log in to Linkus Mobile Client or Linkus Desktop Client.
Administrator Password Changed	The administrator's password was changed.
Extension User Password Changed	An extension user's user password was changed.
RPS Request Success	The RPS request of the IP Phone(s) succeeded.
RPS Request Failed	The RPS request of the IP Phone(s) failed.

Table 31. 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 32. 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.
System Reboot	Either of the following situations triggered the event: • The PBX rebooted after configuration. • The PBX automatically rebooted after system crash.

Table 32. System (continued)

Event	Description
System Restore	The PBX was restored.
New System Firmware Detected	The PBX automatically detected a new firmware version.
System Upgrade Completed	The PBX was upgraded.
PBX Hot Standby Failover	A PBX failover has occurred, and the PBX system is taken over by the other server.
Primary Server Data Restoration Completed	The Primary Server is fixed and the data synchronization is completed now.
Both PBX Servers Failed to Function	Both the Primary Server and the Scondary Server of your PBX system were down.
Data Synchronization Error Due to Server Missing	The data synchronization could not function properly as the opposite PBX server is not detected.
Yeastar SMTP Server Error	Yeastar SMTP server failed to send emails.
Abnormal License Activation	Failed to connect to extranet License Activation Server.
Data Synchronization Error Due to Storage Missing	The data synchronization could not function properly as the storage device of the opposite PBX server is not detected.
SD-WAN Network Joined Successfully	A PBX has successfully joined the SD-WAN network.
SD-WAN Network Exited	A PBX has exited the SD-WAN network.
SD-WAN Network Disconnected	A PBX has lost connection to the SD-WAN network.
SD-WAN Network Connection Switched	The Secondary Server in a Hot Standby pair has joined the SD-WAN network as it takes over the phone system from the Primary Server.
Abnormal Working Server	The Working Server is abnormal and the Redundancy Server will take over the telephony services.
Abnormal Redundancy Server	The Redundancy Server is abnormal, you need to fix the issue as soon as possible.
Disaster Recovery Fallback	A disaster recovery fallback was triggered and the Redundancy Server has taken over the telephony services.
Disaster Recovery Data Synchronization Error	The data synchronization between the Working Server and the Redundancy Server encounters an error.
Working Server Data Restoration Completed	The Working Server is repaired and the data synchronization from Redundancy Server is completed.
Abnormal Core Call Services	A deadlock issue has been detected in the core call process.

Table 32. System (continued)

Event	Description
Core Call Services Recovery Completed	The core call process has recovered successfully.

Table 33. Security

Event	Description
Web User Locked Out	PBX blocked the source IP when either of the following situations was met: • Web Login failure for more than 5 times in 24 hours. • More than 5 accounts were locked in 24 hours.
Linkus User Blocked Out	PBX blocked the source IP when either of the following situations was met: • Login failure (Linkus Mobile Client or Linkus Desktop Client) for more than 5 times in 24 hours. • More than 5 accounts were locked in 24 hours.
Extension Registration Blocked Out	PBX blocked the source IP when either of the following situations was met: • Registration failure for more than 20 times. • More than 3 accounts were locked.
Auto Defense IP Blocked Out	The monitored service or port reached the limit of **Number of Packets** during specific **Time Interval**.
Outbound Call Frequency Exceeded	An extension has exceeded the limit of **Number of Calls** during specified **Time Period** set in an Outbound Call Frequency Restriction rule.
Outbound Call to a Disallowed Country	An extension user made an outbound call to a disallowed country.
API Authentication Blocked Out	PBX blocked the source IP due to too many failed API authentication attempts.
Linkus SDK Authentication Blocked Out	PBX blocked the source IP due to too many failed Linkus SDK authentication attempts.

Table 34. Reminder

Event	Description
Video Conferencing Usage Has Reached 90% of Time Limit	Reach 90% of the annual time limit of video conferencing.

Table 34. Reminder (continued)

Event	Description
Video Conferencing Usage Limit Reached	Reach annual usage limit of video conferencing.
License Expiration Reminder	The current license will expire soon.
Failed to Archive File(s)	The task to archive recording files or backup files to an external server has failed.
Campaign Paused	The outbound campaign has been paused due to detected abnormalities with the associated trunk or a data issue.

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.

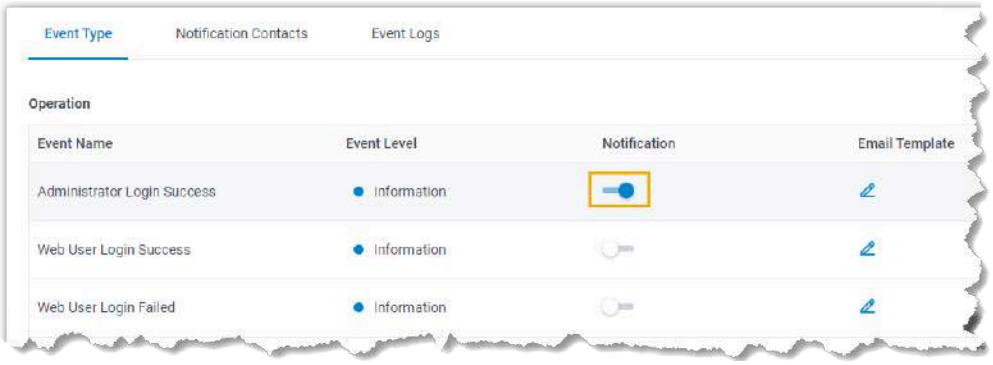
For more information, see Auto Cleanup Settings.

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.



3. Configure notification settings for a desired event.
   - **Event Level**: A proper level helps you identify seriousness of an event. Use default level or select a level from the drop-down list.
   - **Email Template**: To customize template of the email that will be sent to relevant contacts when the event occurs, click .

- **Notification Contacts**: Add notification contacts and select proper notification methods.

  For more information, see Manage Notification Contacts.

Result

When the event occurs, the followings can be achieved:

- The PBX sends notifications to relevant contacts via specific notification methods.
- On **Event Trend** section, the event is included in the statistics of corresponding event level.
- At the top right corner of the page, automatically adds 1 in the color that indicates the event level.

> **Note:**
> If default level for the event is **Error**, the system also gives you a pop-up reminder on the right of PBX web portal.

What to do next

At the top right corner, click to check event details.

Manage Notification Contacts

This topic describes how to add, edit, or delete a notification contact.

Add a notification contact

1. Log in to PBX web portal, go to **System > Event Notification > Notification Contacts**, click **Add**.
2. In the pop-up window, configure contact settings.
   - **Notification Contact**: Select an internal user or set an external user. If you choose **Custom**, enter a name in the **Contact Name** field.
   - **Notification Methods**: Set how to notify the contact when events occur.
     - **Call Extension**: The PBX will call the extension number of the contact when an event occurs.
     - **Send Email**: The PBX will send notifications to the email address of the contact when an event occurs.

    - **Call Mobile**: The PBX will call the mobile number of the contact when an event occurs.

      > **Note:**
      > To ensure that PBX can successfully call the mobile number, make sure that the **Prefix** is configured correctly according to the outbound route rule.

  - **The Event Levels to Notify**: Select the level of events that you want to notify the contact. The contact will only receive notifications when events at the level occur.
3. Click **Save**.

Edit a notification contact

1. Log in to PBX web portal, go to **System > Event Notification > Notification Contacts**.
2. Select a desired contact, click .

   > **Note:**
   > To edit the event notifications of super administrator, click the at the top-right corner and select **Administrator Settings**.
3. Change the notification methods and notification level according to your needs.
4. Click **Save**.

Delete notification contacts

1. Log in to PBX web portal, go to **System > Event Notification > Notification Contacts**.
2. Delete one or more contacts according to your needs.
   - To delete a contact, click beside the desired contact, click **OK**.
   - To delete contacts in bulk, select the checkboxes of the desired contacts, click **Delete** and **OK**.

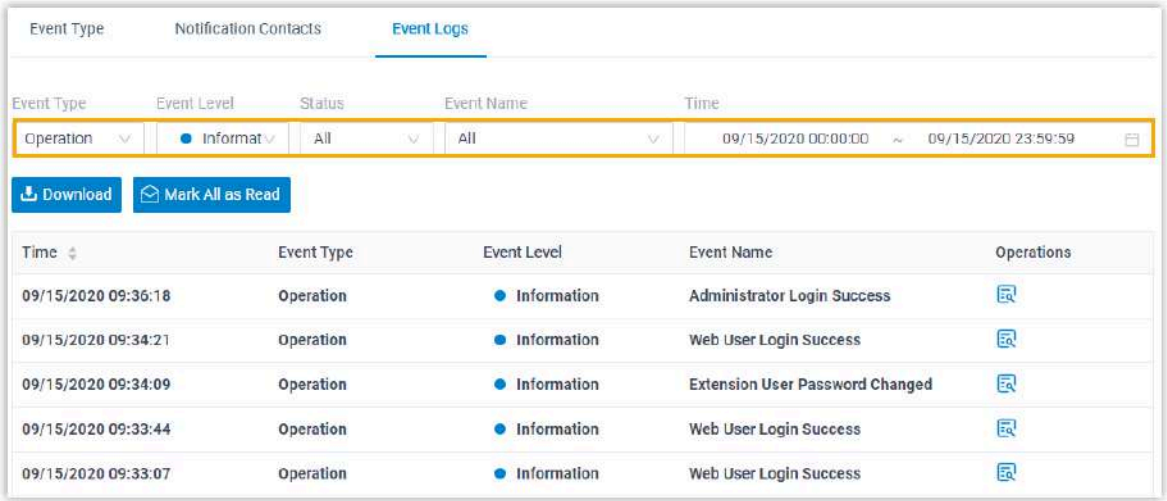
   The contacts are removed from the list, and will not receive notifications when events occur.

Manage Event Logs

All the occurred events are saved in event logs so that you can trace the events. This topic describes how to view, download, and mark event logs as read.

Procedure

1. Log in to PBX web portal, go to **System > Event Notification > Event Logs**.
2. Set the search criteria to search events.



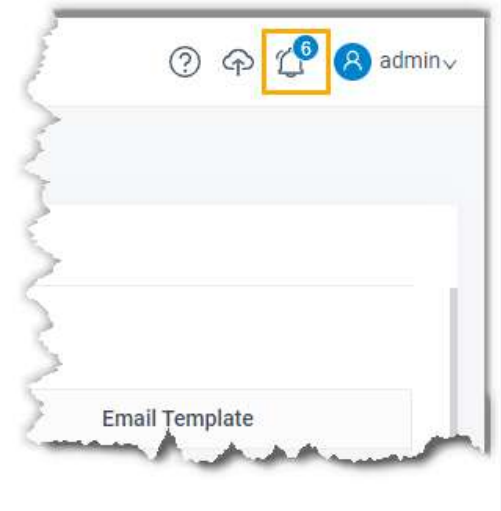
   - **Event Type**: Search all the event logs or search logs by a specific event type.
   - **Event Level**: Search all the event logs or search logs by a specific event level.
   - **Status**: Search all the event logs or search logs by a specific acknowledgement status.
   - **Event Name**: Search all the event logs or search a specific event.
   - **Time**: Set the start date and end date of the events.

   The matched events are displayed on the page.
3. Handle the searched events according to your needs.
   - To check log details, click beside the desired event log.

     The event log will be marked as read.
   - To download all the searched logs, click **Download**.
   - To mark all the searched logs as read, click **Mark All as Read**.

> **Note:**

At the top right corner, the number of unread events of the event level prompted on will be cleared.



Remote Management

Remote Management Overview

If you need remote technical support or troubleshooting, you can contact device provider to connect your PBX to Yeastar Central Management, which is a Yeastar-hosted platform for all the device providers to remotely access and manage devices. In this way, you can secure remote connection to your PBX, while reducing IT and maintenance costs.

Activation methods

User Scenario	Instruction
In-house IT staff is responsible for routine maintenance of PBX system	Connect Yeastar P-Series 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.
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

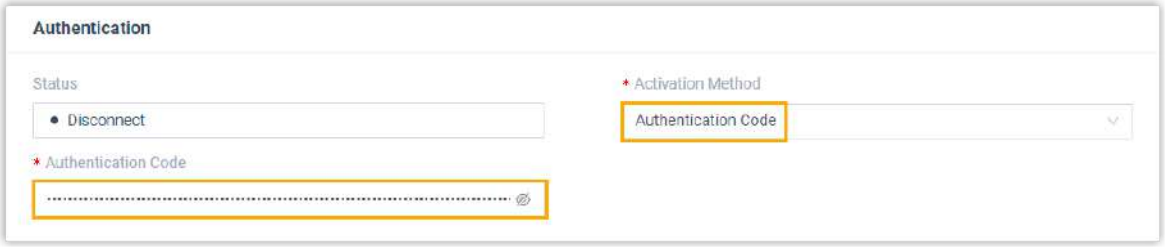
If you have in-house IT staff for routine maintenance of your PBX system, but the IT staff has difficulty handling specific system errors, you can connect PBX to Yeastar Central Management using an authentication code. In this way, device provider can help you troubleshoot issues.

Prerequisites

Make sure the version of your PBX system is 83.5.0.86 or later.

Procedure

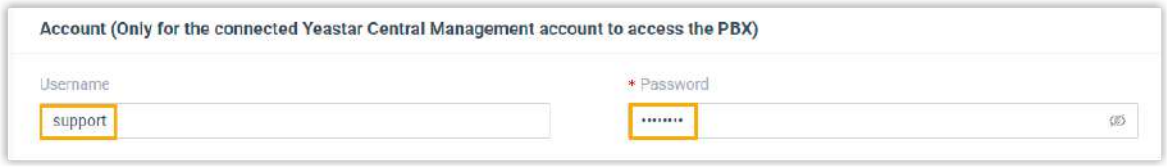
1. Contact device provider to obtain an authentication code.
2. Log in to PBX web portal, go to **System > Remote Management**.
3. In the **Authentication** section, complete the following settings:



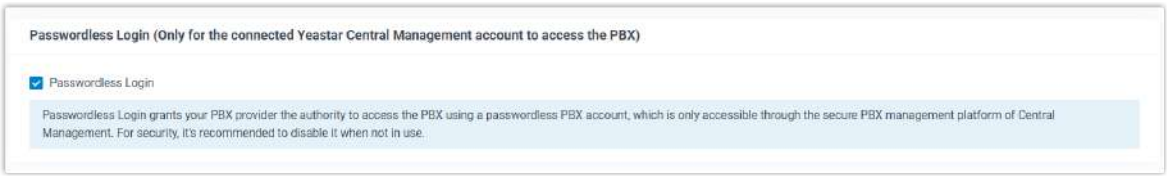
   - **Activation Method**: Select **Authentication Code**.
   - **Authentication Code**: Enter the authentication code that is provided by device provider.
4. If you don't want to expose your super administrator credential or extension credential, set a username and a password in the **Account** section.

Device provider can use the username and password to remotely log in to your PBX web portal.

> **Note:**
> - The **Username** can NOT duplicate with the name of super administrator or the email address of an extension.
> - Permissions of the account are the same as that of extensions with **Administrator** role assigned.



5. If you want to authorize device provider to log in to your PBX without entering username and password from Yeastar Central Management, select the checkbox of **Passwordless Login**.



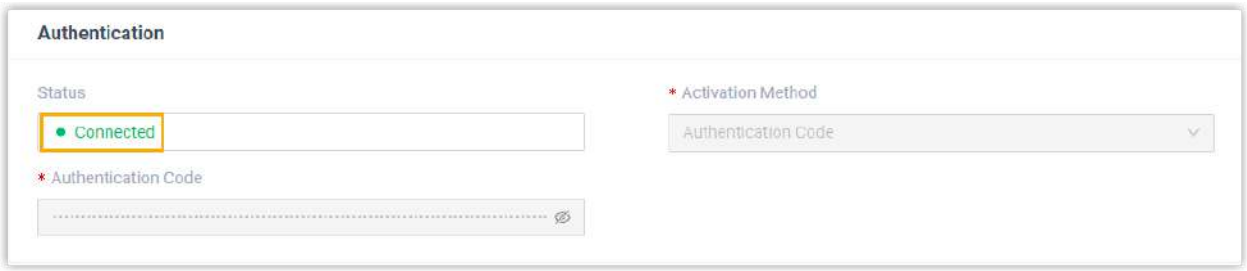
Device provider can log in to PBX management portal with a dedicated **Passwordless** account by clicking on the encrypted web access link from Yeastar Central Management.

> **Note:**
> - If the **Passwordless Login** feature is not available on your PBX, upgrade PBX to version 83.17.0.16 or later.
> - Permissions of the **Passwordless** account are the same as that of PBX super administrator.
> - The PBX system automatically logs out the account according to Auto Logout Time if no operation is performed on the web page.

6. Click **Save**.

Result

The status is displayed as **Connected**, which indicates that your PBX system is connected to Yeastar Central Management.



Related information

[Connect Yeastar P-Series 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.

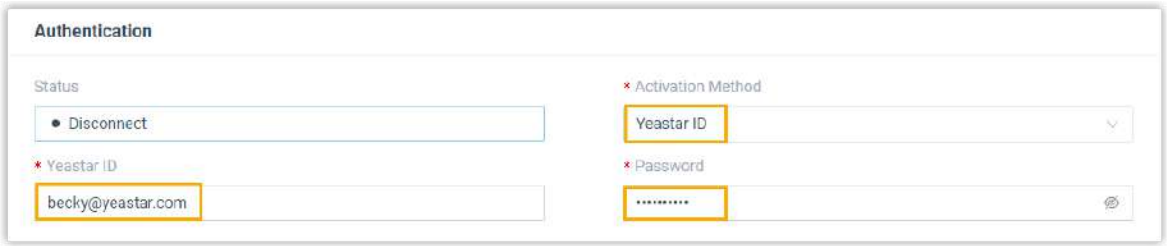
Prerequisites

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:

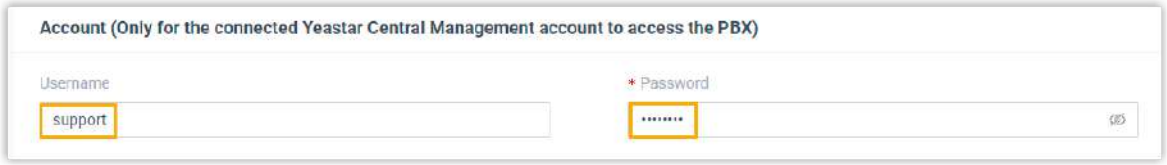


- **Activation Method**: Select **Yeastar ID**.
- **Yeastar ID**: Enter device provider's Yeastar ID.

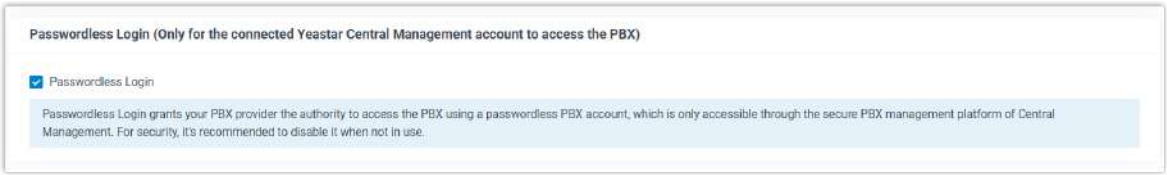
- **Password**: Enter device provider's password.

3. If you don't want to expose your super administrator credential or extension credential, set a username and a password in the **Account** section.
   Device provider can use the username and password to remotely log in to your PBX web portal.

> **Note:**
> - The **Username** can NOT duplicate with the name of super administrator or the email address of an extension.
> - Permissions of the account are the same as that of extensions with **Administrator** role assigned.



4. If you want to authorize device provider to log in to your PBX without entering username and password from Yeastar Central Management, select the checkbox of **Passwordless Login**.



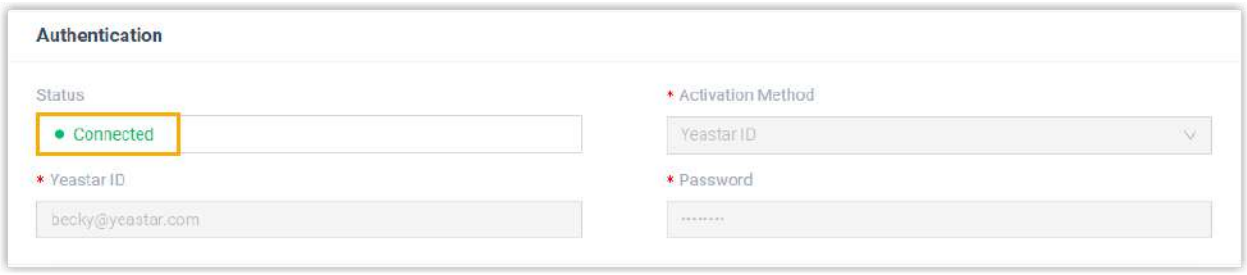
   Device provider can log in to PBX management portal with a dedicated **Passwordless** account by clicking on the encrypted web access link from Yeastar Central Management.

> **Note:**
> - If the **Passwordless Login** feature is not available on your PBX, upgrade PBX to version 83.17.0.16 or later.
> - Permissions of the **Passwordless** account are the same as that of PBX super administrator.
> - The PBX system automatically logs out the account according to Auto Logout Time if no operation is performed on the web page.

5. Click **Save**.

Result

The status is displayed as **Connected**, which indicates that your PBX system is connected to Yeastar Central Management.



Related information

Connect Yeastar P-Series 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.

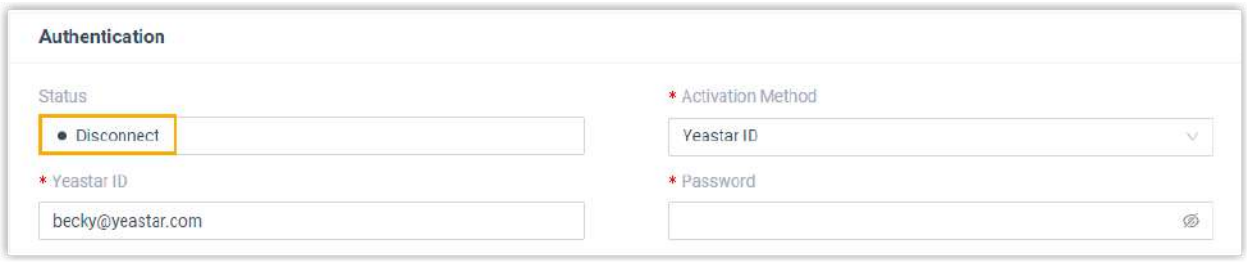
Procedure

1. Log in to PBX web portal, go to **System > Remote Management**.
2. Click **Disconnect**.

3. In the pop-up dialog box, click **OK**.

Result

The status is displayed as **Disconnect**, which indicates that your PBX system is disconnected with Yeastar Central Management.



SNMP

Yeastar P-Series Software Edition SNMP Overview

Simple Network Management Protocol (SNMP) is a standardized protocol for monitoring and managing network devices. By connecting Yeastar P-Series Software Edition to a Network Management System (NMS) through SNMP, network administrator can query PBX information and monitor PBX on NMS.

Requirements

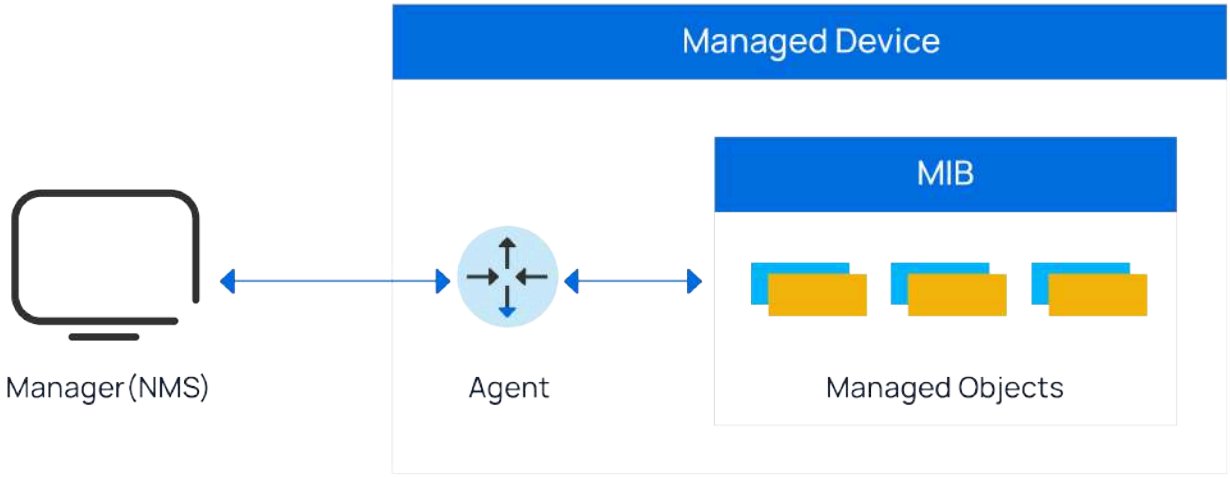
The version of Yeastar P-Series Software Edition is 83.17.0.60 or later.

SNMP components

An SNMP system consists of 4 key components:

- **Manager**: A centralized system used to monitor the SNMP network, also known as Network Management System (NMS).
- **Managed devices**: An SNMP-enabled network entity that is managed by the SNMP manager. These are usually routers, switches, servers, etc.
- **Agent**: A network-management software module that runs on each managed device. It maintains data on the managed device, responds to requests from the NMS, and returns data to the NMS.
- **MIB (Management Information Base)**: An information base that contains definitions and information about the properties of a managed device. The manageable features of the device is called managed objects (or just objects or variables).

We provide a typology to help you understand the connection and interaction of each SNMP component.



As the typology shows, each managed device contains an SNMP agent process, an MIB, and multiple managed objects. Upon receiving requests from NMS, the agent queries or modifies variables in the MIB, and returns operation result to the NMS; In addition, when the managed device triggers a trap event regarding the MIB, it will send trap messages to NMS.

Supported SNMP version

Yeastar P-Series Software Edition supports **SNMPv3**, which has all the functions of SNMPv1 and SNMPv2c. In addition, SNMPv3 provides secure access to devices by authenticating and encrypting data packets over the network.

Supported SNMP operation

Yeastar P-Series Software Edition supports two operations:

- **SNMP Get**: Allow network administrator to collect data from the managed device.

  The NMS sends a Get request to the SNMP agent, the SNMP agent queries variables from the MIB and returns the data to the NMS.
- **SNMP Trap**: The managed device sends unsolicited trap messages to notify NMS that an urgent and significant event has occurred on the managed device.

Set up SNMP on Yeastar P-Series Software Edition

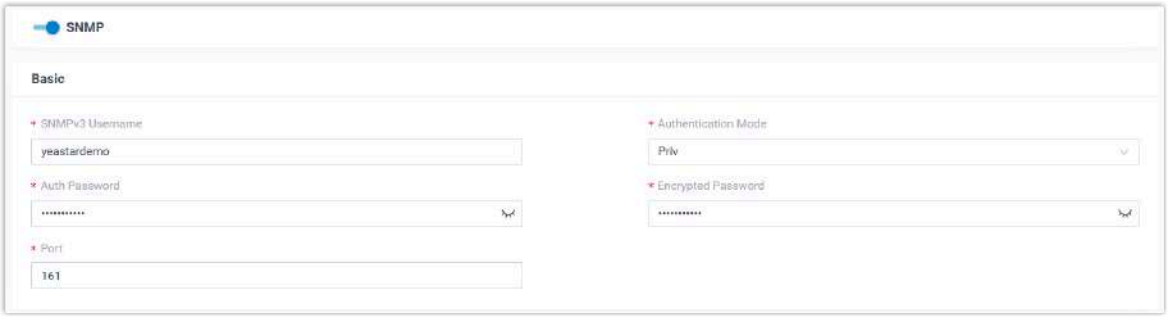
This topic describes how to enable SNMP and configure the related settings on Yeastar P-Series Software Edition.

Requirements

The version of Yeastar P-Series Software Edition is 83.17.0.60 or later.

Procedure

1. Log in to PBX web portal, go to **System > SNMP**.
2. In the **Basic** section, set up SNMP related settings that are required when adding the monitored device to the NMS.



   a. Turn on **SNMP**.
   b. Complete the following settings.

Setting	Description
SNMPv3 Username	Enter a user name for authentication on NMS.
Authentication Mode	Select an authentication method. • **NoAuth**: Provide access control based on the user name. • **Auth**: Provide access control based on the HMAC-MD5 authentication. • **Priv**: Provide access control based on the HMAC-MD5 authentication and data encryption by CBC-DES.
Auth Password	Retain the default authentication password, or enter a desired password. **Note:** This option is available only when **Authentication Mode** is set to **Auth** or **Priv**.
Encrypted Password	Retain the default encryption password, or enter a desired password. **Note:**

Setting	Description
	This option is available only when **Authentication Mode** is set to **Priv**.
Port	Retain the default SNMP port `161`, or enter a desired port number.

3. **Optional:** To enable the PBX to send SNMP trap messages to NMS when a pre-defined event occurs and triggers the trap, set up SNMP trap.

   a. Turn on **SNMP Trap**.
   b. Enter the IP address of the SNMP trap receiver and the port to which the SNMP traps will be sent.
4. Click **Save**.

Result

The SNMP feature on Yeastar P-Series Software Edition is set up.

What to do next

Connect Yeastar P-Series Software Edition with Network Management System (NMS) via SNMP.

Note:

- Enter the **IP Address** of your PBX on NMS, instead of the Yeastar FQDN (Fully Qualified Domain Name).
- We provide an example on how to connect Yeastar P-Series Software Edition with **Zabbix Server**.

  For more information, see Monitor Yeastar P-Series Software Edition through SNMP using Zabbix Server.

Monitor Yeastar P-Series Software Edition through SNMP using Zabbix Server

This topic takes Zabbix Server as an example to show you how to monitor Yeastar P-Series Software Edition through SNMP.

Prerequisites

- The version of Yeastar P-Series Software Edition is 83.18.0.18 or later.
- You have set up SNMP on Yeastar P-Series Software Edition.

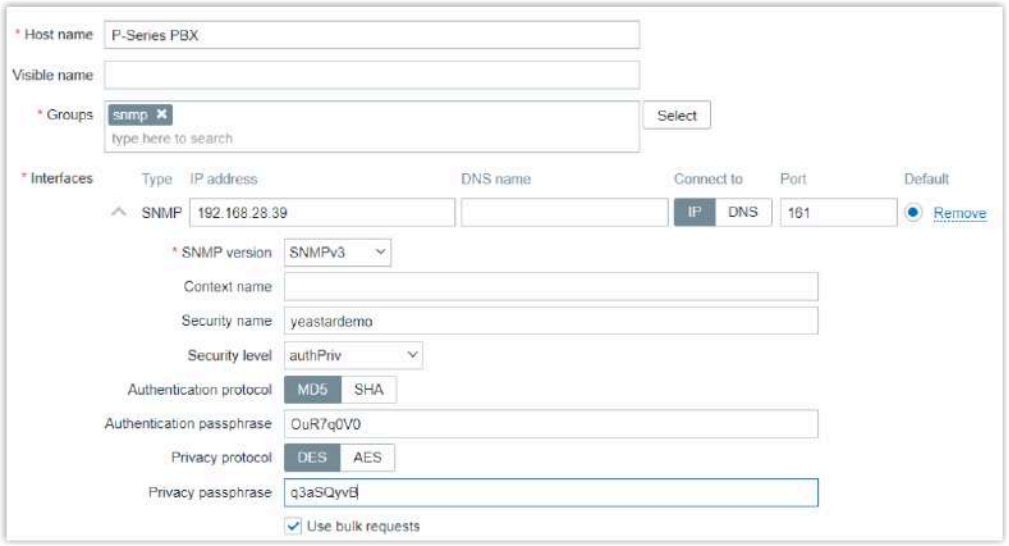
Procedure

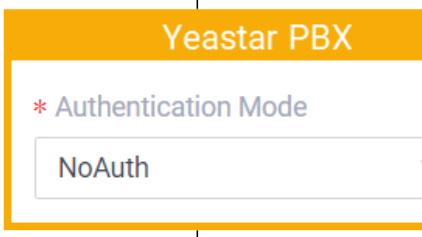
Step 1. Add a host to Zabbix Server

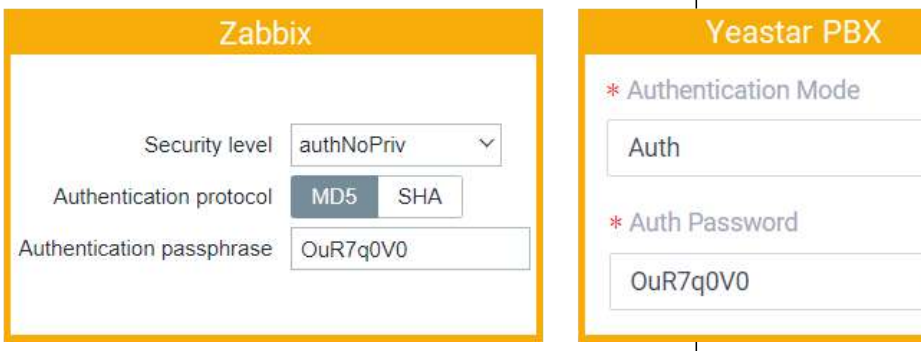
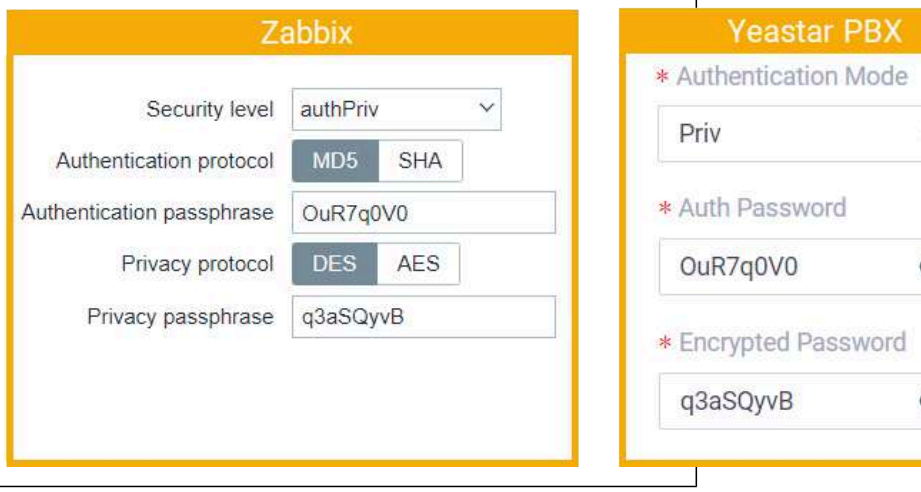
A host in Zabbix is a network entity (physical or virtual) that you want to monitor. In this example, we will add a host for Yeastar P-Series Software Edition on Zabbix Server.

1. On the left navigation bar, go to **Configuration > Hosts**.
2. At the top-right corner, click **Create host**.
3. Under the **Host** tab, complete the following settings.
    a. In the **Host name** field, enter a name to help you identify the host. In this example, enter `P-Series PBX`.
    b. In the **Groups** field, enter the name of an existing group or click **Select** to select a group.
    c. In the **Interfaces** section, remove the default agent, then add a host.
        i. Click **Remove** to remove the default agent.

        ii. Click **Add**, select **SNMP**, then complete the following settings:



Setting	Description
IP address	Enter the IP address of PBX. In this example, enter `192.168.28.39`.
Port	Enter the SNMP port that is configured on PBX. In this example, retain `161`.
SNMP Version	Select **SNMPv3**.
Security name	Enter the SNMPv3 username that is configured on PBX. In this example, enter `yeastardemo`.
Security level	Select the authentication mode that is specified on PBX. • **noAuthNoPriv**: This option corresponds to **NoAuth** on PBX.  

Setting	Description
	• **authNoPriv**: This option corresponds to **Auth** on PBX. If you choose this option, you need to set **Authentication protocol** to **MD5**, and enter the authentication passphrase.  • **authPriv**: This option corresponds to **Priv** on PBX. If you choose this option, you need to set **Authentication protocol** to **MD5** and **Privacy protocol** to **DES**, and enter the authentication passphrase and privacy passphrase. 

4. Click **Add**.

   The host is added successfully. You can check it on the **Hosts** list.

Step 2. Add monitoring items to the host

A monitoring item defines a single metric or what kind of data to collect from a host. In this example, we will add monitoring items to collect data from the PBX host.

You can add monitoring items in the following ways:

- Import monitoring items
- Manually add monitoring items

Import monitoring items

We provide a Yeastar PBX MIB file in both `.mib` and `.xml` formats, facilitating you to quickly import monitoring items into your Network Management System (NMS).

Download the file in the appropriate format, and follow the instructions below to import.

- Yeastar PBX MIB file in `.mib` format
- Yeastar PBX MIB file in `.xml` format

1. On the left navigation bar, go to **Configuration > Templates**.
2. At the top-right corner, click **Import**, select the MIB file, then click **Import**.

   You can check the imported template in the **Templates** list.

3. On the left navigation bar, go to **Configuration > Hosts**, search and find the PBX host, then go to the host detail page.
4. Click the **Templates** tab, search and select the imported template in the **Link new templates** field, then click **Update**.

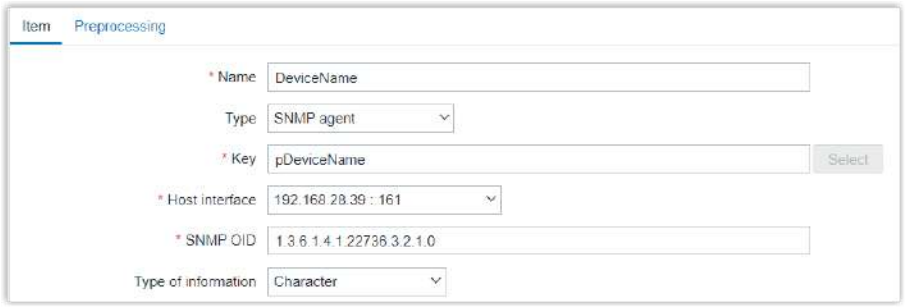
On the **Hosts** list, you will find the template and the items are linked with PBX host successfully.

Manually add monitoring items

We provide a list of MIB objects as a reference for manually adding items on NMS. Check against the Yeastar P-Series Software Edition MIB to add desired items.

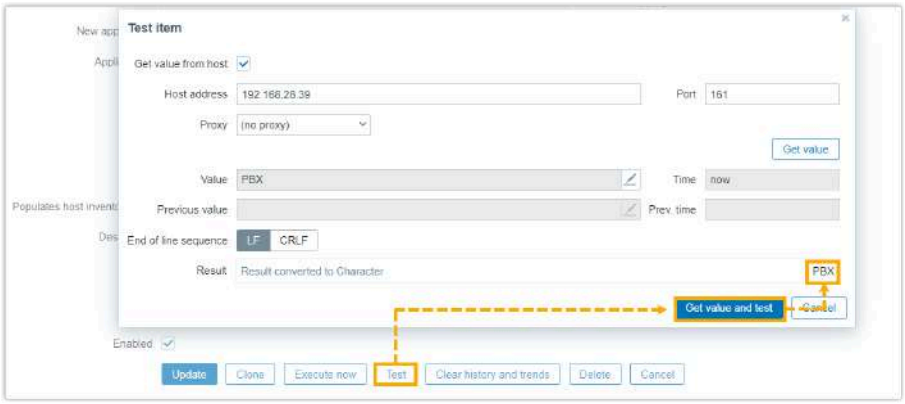
1. Go to the creation page of monitoring items.
   a. On **Configuration > Hosts**, search and find the PBX host.
   b. Click **Items** beside the host.

2. Add SNMP agent items to monitor and retrieve data from PBX.
   a. At the top-right corner, click **Create item**.
   b. Under **Item** tab, configure the following settings.



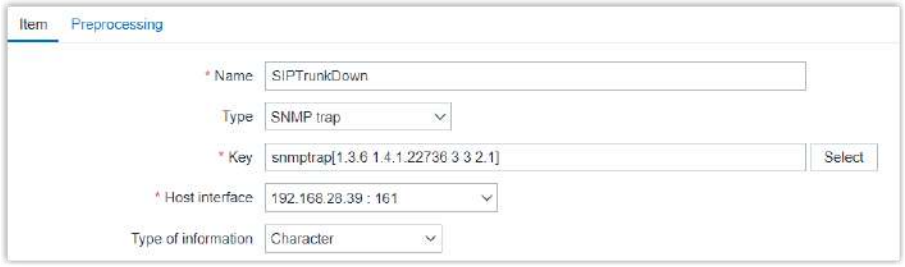
   - **Name**: Enter a name to help you identify the item. In this example, enter `DeviceName`.
   - **Type**: Select **SNMP agent**.
   - **Key**: Enter the name of the MIB object. In this example, enter `pDeviceName`.
   - **SNMP OID**: Enter the OID of the MIB object. In this example, enter `1.3.6.1.4.1.22736.3.2.1.0`.
   - **Type of information**: Select the information type. In this example, select **Character**.

   c. **Optional:** Click **Test > Get value and test** to test if the configuration works, then close the window.



d. Click **Add**.

3. Add SNMP trap items to monitor and receive trap messages from PBX.
   a. At the top-right corner, click **Create item**.
   b. Under **Item** tab, configure following settings.



- **Name**: Enter a name to help you identify the item. In this example, enter `SIPTrunkDown`.
- **Type**: Select **SNMP trap**.
- **Key**: Enter a key, in the format of `snmptrap[{snmp_oid}]`. In this example, enter `snmptrap[1.3.6.1.4.1.22736.3.3.2-.1]`.
- **Type of information**: Select the information type. In this example, select **Character**.

   c. Click **Add**.

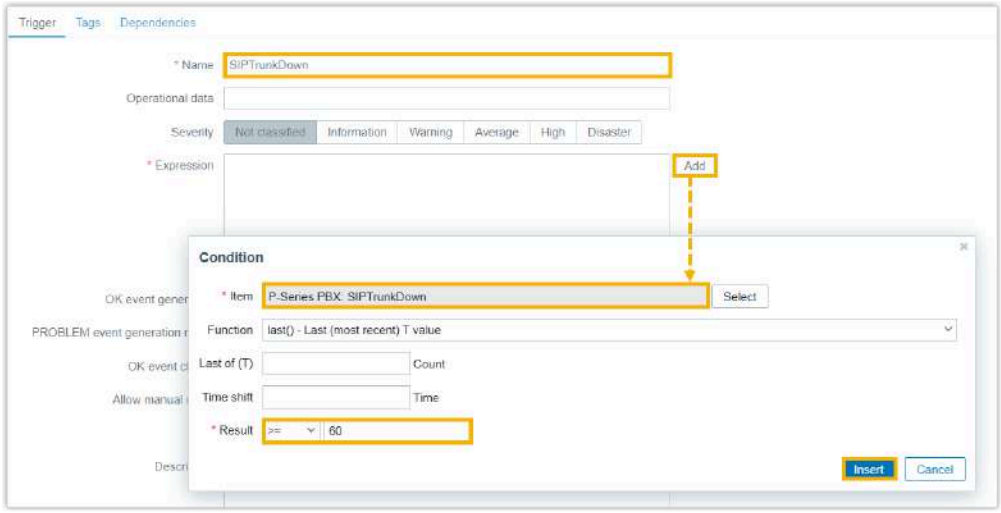
Step 3. Add triggers and actions

Add triggers and actions to receive timely alerts upon some condition change on PBX.

1. Add triggers to automatically evaluate whether the monitoring item reaches a threshold.
   a. Click **Triggers** beside the host.

b. At the top-right corner, click **Create trigger**.

c. Under **Trigger** tab, configure the trigger.

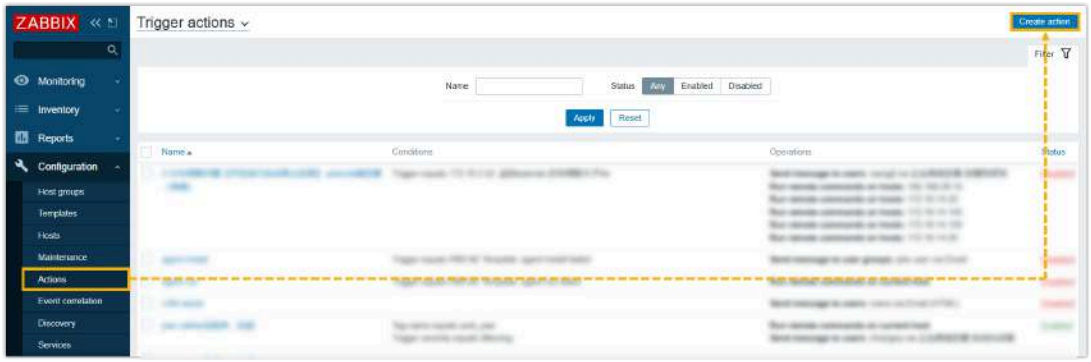


- **Name**: Enter a name to help you identify the trigger. In this example, enter `SIPTrunkDown`.
- **Expression**: Click **Add** to define the problem expression.

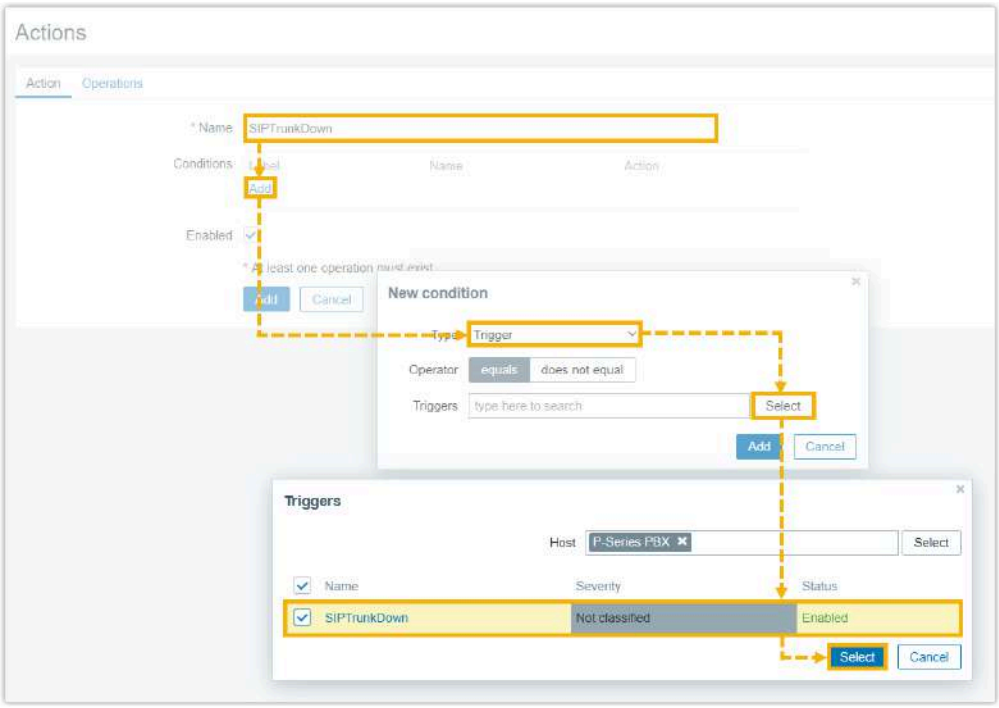
d. Click **Add**.

2. Add actions to send notifications when the monitoring item reaches a threshold.

a. On the left navigation bar, click **Actions**, then click **Create action**.

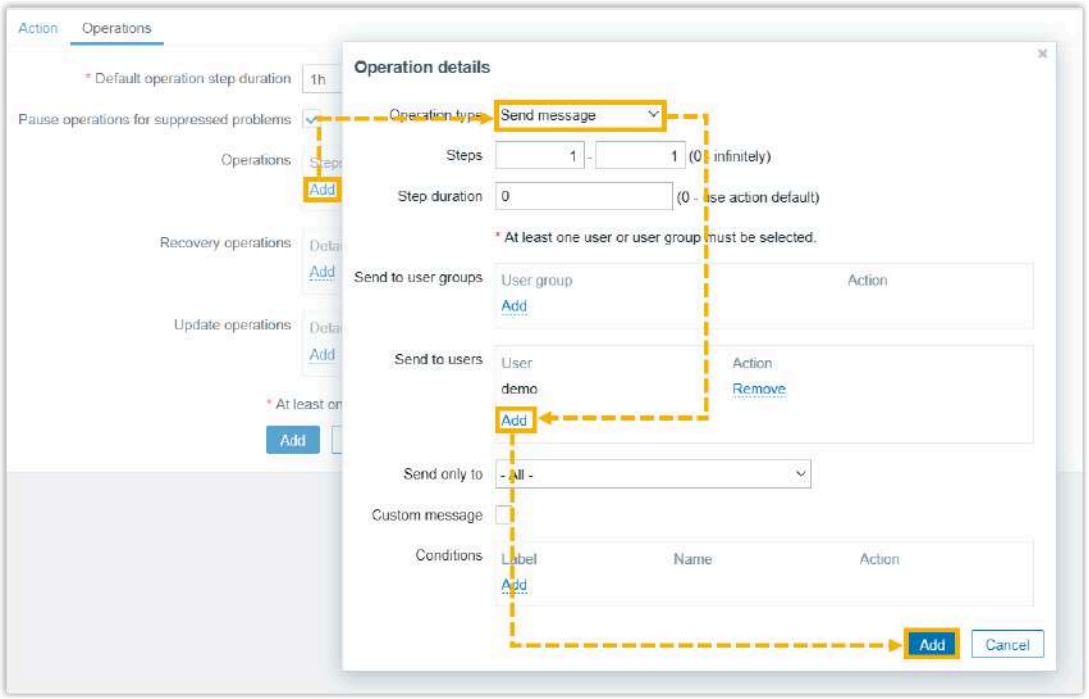


b. Under **Action** tab, set the conditions upon which operations will be carried out.



- **Name**: Enter a name to help you identify the action.
- **Condition**: Click **Add** to add a new condition for a trigger.

c. Under **Operations** tab, click **Add** to set the operations to carry out.



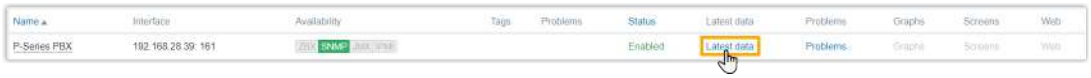
d. Click **Add**.

e. Click **Add**.

Result

- When a threshold is reached, notifications will be sent to the specified user.
- You can view the latest data collected by items on Zabbix.

1. On the left navigation bar, go to **Monitoring > Hosts**, search and find the PBX host.
2. Click **Latest data** beside the host.



You can view the latest data of the PBX.

Yeastar P-Series Software Edition MIB

This topic lists the Yeastar P-Series Software Edition MIB objects.

> **Tip:**
> To quickly add Yeastar P-Series Software Edition MIB objects to Network Management System (NMS), you can download the Yeastar PBX MIB file, and import the file to NMS.

System

Name	OID	Type	Description
pProductModel	1.3.6.1.4.1.22736.3.1.1.0	String	The product model of PBX.
pHardwareVersion	1.3.6.1.4.1.22736.3.1.2.0	String	The hardware version of PBX.

Name	OID	Type	Description
pFirmwareVersion	1.3.6.1.4.1.22736.3.1.3.0	String	The firmware version of PBX.
pSerialNumber	1.3.6.1.4.1.22736.3.1.4.0	String	The serial number of PBX.
pUptime	1.3.6.1.4.1.22736.3.1.5.0	String	The uptime of PBX.
pLocalStorageUsage	1.3.6.1.4.1.22736.3.1.6.0	String	The local storage usage of PBX.
pMemoryUsage	1.3.6.1.4.1.22736.3.1.7.0	String	The memory usage of PBX.
pCPUUtilization	1.3.6.1.4.1.22736.3.1.8.0	String	The CPU utilization of PBX.
pConcurrentCall	1.3.6.1.4.1.22736.3.1.9.0	Integer	The number of occupied concurrent calls.
pAvgCpuLoad	1.3.6.1.4.1.22736.3.1.10.0	String	The load average of CPU.
pAsteriskStatus	1.3.6.1.4.1.22736.3.1.11.0	String	The asterisk status.
pCpuTop10	1.3.6.1.4.1.22736.3.1.12.0	String	The top 10 CPU consumption processes.
pMemTop10	1.3.6.1.4.1.22736.3.1.13.0	String	The top 10 memory consumption processes.

Network

Name	OID	Type	Description
pDeviceName	1.3.6.1.4.1.22736.3.2.1.0	String	The device name of PBX.
pLanStatus	1.3.6.1.4.1.22736.3.2.2.0	String	The LAN status.
pLanMac	1.3.6.1.4.1.22736.3.2.3.0	String	The MAC address of LAN.
pLanConnectType	1.3.6.1.4.1.22736.3.2.4.0	String	The network connection type of LAN.
pLanIpaddress	1.3.6.1.4.1.22736.3.2.5.0	String	The IP address of LAN.

Name	OID	Type	Description
pLanSubnetMask	1.3.6.1.4.1.22736.3.2.6.0	String	The subnet mask of LAN.
pLanGateWay	1.3.6.1.4.1.22736.3.2.7.0	String	The gateway of LAN.
pLanPrimaryDns	1.3.6.1.4.1.22736.3.2.8.0	String	The primary DNS of LAN.
pLanSecondaryDns	1.3.6.1.4.1.22736.3.2.9.0	String	The secondary DNS of LAN.
pWanStatus	1.3.6.1.4.1.22736.3.2.10.0	String	The WAN Status.
pWanMac	1.3.6.1.4.1.22736.3.2.11.0	String	The MAC address of WAN.
pWanConnectType	1.3.6.1.4.1.22736.3.2.12.0	String	The network connection type of WAN.
pWanIpaddress	1.3.6.1.4.1.22736.3.2.13.0	String	The IP address of WAN.
pWanSubnetMask	1.3.6.1.4.1.22736.3.2.14.0	String	The subnet mask of WAN.
pWanGateWay	1.3.6.1.4.1.22736.3.2.15.0	String	The gateway of WAN.
pWanPrimaryDns	1.3.6.1.4.1.22736.3.2.16.0	String	The primary DNS of WAN.
pWanSecondaryDns	1.3.6.1.4.1.22736.3.2.17.0	String	The secondary DNS of WAN.

Data

Name	OID	Type	Description
Extension			
pExtObjects	1.3.6.1.4.1.22736.3.4.1	Integer	The extension objects.
pExtTable	1.3.6.1.4.1.22736.3.4.2	/	The table of extension information.
pExtEntry	1.3.6.1.4.1.22736.3.4.2.1	/	The information of extension.
pExtIndex	1.3.6.1.4.1.22736.3.4.2.1.1	Integer	The index of extension.

Name	OID	Type	Description
pExtNum	1.3.6.1.4.1.22736.3.4.2.1.2	String	The extension number.
pExtName	1.3.6.1.4.1.22736.3.4.2.1.3	String	The name of extension.
pExtStatus	1.3.6.1.4.1.22736.3.4.2.1.4	String	The status of extension.
Trunk			
pTrunkObjects	1.3.6.1.4.1.22736.3.4 3	Integer	The trunk objects.
pTrunkTable	1.3.6.1.4.1.22736 3.4.4	/	The table of trunk information.
pTrunkEntry	1.3.6.1.4.1.22736.3.4.4.1	/	The information of trunk.
pTrunkIndex	1.3.6.1.4.1.22736.3.4.4.1.1	Integer	The index of trunk.
pTrunkName	1.3.6.1.4.1.22736.3.4.4.1.2	String	The name of trunk.
pTrunkType	1.3.6.1.4.1.22736.3.4.4.1.3	String	The type of trunk.
pTrunkStatus	1.3.6.1.4.1.22736.3.4.4.1.4	String	The status of trunk.

Traps

Name	OID	Type	Description
pTraps	1.3.6.1.4.1.22736.3.3	String	All traps from PBX.
Extension			
pExtAbnormalTraps	1.3.6.1.4.1.22736.3.3.1	String	The trap of abnormal extensions.
pIPphoneDown	1.3.6.1.4.1.22736.3.3.1.1	String	The IP phone or softphone is disconnected.
pIPphoneUp	1.3.6.1.4.1.22736.3.3.1.2	String	The IP phone or softphone is reconnected.
pExtDown	1.3.6.1.4.1.22736.3.3.1.3	String	The extension loses registration with all the endpoints (Linkus UC Clients, IP phones, and softphones).
pExtUp	1.3.6.1.4.1.22736.3.3.1.4	String	The extension is re-registered on at least one endpoint after losing registration on all the endpoints.

Name	OID	Type	Description
Trunk			
pTrunkAbnormalTraps	1.3.6.1.4.1.22736.3.3.2	String	The trap of abnormal trunks.
pSIPTrunkDown	1.3.6.1.4.1.22736.3.3.2.1	String	The SIP trunk is disconnected.
pSIPTrunkUp	1.3.6.1.4.1.22736.3.3.2.2	String	The SIP trunk is reconnected.
pTrunkDown	1.3.6.1.4.1.22736.3.3.2.3	String	The trunk is disconnected.
pTrunkUp	1.3.6.1.4.1.22736.3.3.2.4	String	The trunk is reconnected.
Call			
pCallAbnormalTraps	1.3.6.1.4.1.22736.3.3.3	String	The trap of call anomalies.
pPBXMaxCCTraps	1.3.6.1.4.1.22736.3.3.3.1	String	The maximum Concurrent Calls (CC) of PBX is reached.
pPBXMaxCCTrapsRecovery	1.3.6.1.4.1.22736.3.3.3.2	String	The Concurrent Calls (CC) of PBX becomes available again after reaching the maximum capacity.
pTrunkMaxCCTraps	1.3.6.1.4.1.22736.3.3.3.3	String	The maximum Concurrent Calls (CC) allowed in the SIP trunk is reached.
pTrunkMaxCCTrapsRecovery	1.3.6.1.4.1.22736.3.3.3.4	String	The maximum number of Concurrent Calls (CC) allowed in the SIP trunkbecomes available again after reaching the maximum capacity.
pCallFailedTraps	1.3.6.1.4.1.22736.3.3.3.5	String	The traps of failed calls.
pAsteriskTraps	1.3.6.1.4.1.22736.3.3.3.6	String	The trap of abnormal Asterisk.
pAsteriskTrapsRecovery	1.3.6.1.4.1.22736.3.3.3.7	String	The Asterisk returns to normal status.

High Availability

Hot Standby

Hot Standby Overview

The high reliability and high availability performance of server plays a vital role in an application system. Once the key system is down, it may lead to significant losses in data and a variety of issues. Yeastar provides a Hot Standby solution, which can provide high system availability and prevent you from the unnecessary business loss caused by unexpected server failure.

Requirements and restrictions

Requirements

Two identical Yeastar P-Series Software Editions are required to set up a Hot Standby pair, and the servers in the Hot Standby pair must meet the following requirements.

Item	Requirement
Plan	Same plan for the two PBXs. **Note:** If you already have a PBX, provide your service provider with the PBX Serial Number (SN) to purchase another license for Secondary server. If you don't have a PBX, contact your service provider to purchase two licenses for the Hot Standby pair. The two PBXs will be automatically associated via SN.
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 (83.6.0.24 or later).
Network	The two PBXs use the same Internet Protocol, both assigned with static IP addresses, and are located in the same LAN subnet.

Restrictions

- Yeastar P-Series 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**).

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.

Set up Hot Standby Pair

This topic describes how to set up Hot Standby on the Primary Server and Secondary Server. When the Primary Server fails, the Secondary Server becomes active and takes over the entire phone system, thus minimizing downtime and data loss.

Requirements and restrictions

Requirements

Two identical Yeastar P-Series Software Editions are required to set up a Hot Standby pair, and the servers in the Hot Standby pair must meet the following requirements.

Item	Requirement
Plan	Same plan for the two PBXs. **Note:** If you already have a PBX, provide your service provider with the PBX Serial Number (SN) to purchase another license for Secondary server. If you don't have a PBX, contact your service provider to purchase two licenses for the Hot Standby pair. The two PBXs will be automatically associated via SN.
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 (83.6.0.24 or later).
Network	The two PBXs use the same Internet Protocol, both assigned with static IP addresses, and are located in the same LAN subnet.

Restrictions

- Yeastar P-Series 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**).

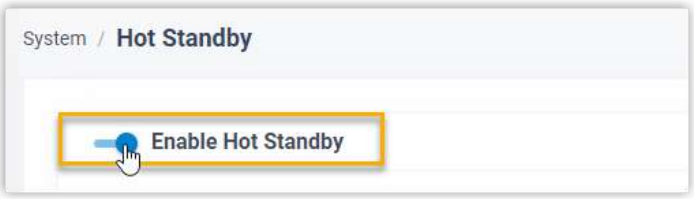
Scenarios

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

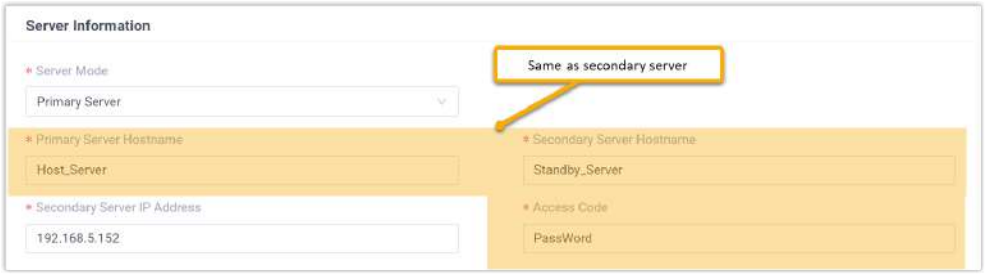
1. Log in to PBX web portal, go to **System > High Availability > Hot Standby**.
2. On the top of the page, turn on the **Enable Hot Standby** switch.



3. In the **Server Information** section, enter the information of the Primary Server and Secondary Server respectively.

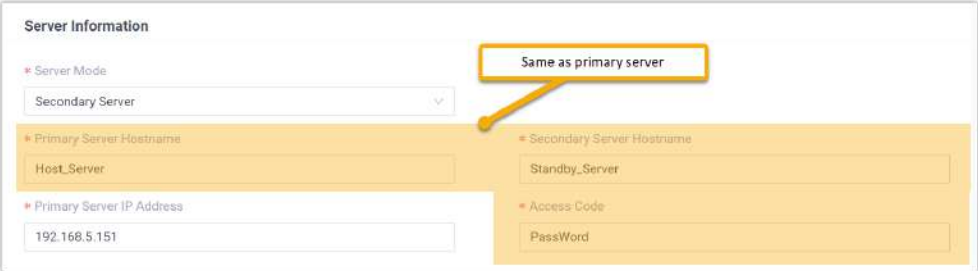
Set up Primary Server

In the **Hot Standby** configuration page of the Primary Server, complete the following settings.



Set up Secondary Server

In the **Hot Standby** configuration page of the Secondary Server, complete the following settings.



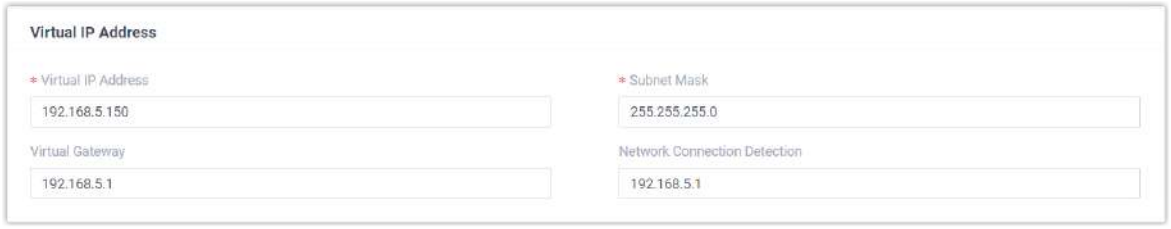
Settings

The detailed description of the settings are listed in the following table.

Setting	Description
Server Mode	In the drop-down list, select a server mode.
Primary Server Hostname	Enter a name to help you identify the Primary Server. In this example, enter `Host_Server`. **Note:** The **Primary Server Hostname** set in the Primary Server and Secondary Server should be the same to avoid confusion in the event notification.
Secondary Server Hostname	Enter a name to help you identify the Secondary Server. In this example, enter `Standby_Server`. **Note:** The **Secondary Server Hostname** set in the Primary Server and Secondary 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:**

Setting	Description
	The two PBXs must have the same access code to authenticate connection.

4. In the **Virtual IP Address** section, set up the network connection for the Hot Standby pair.

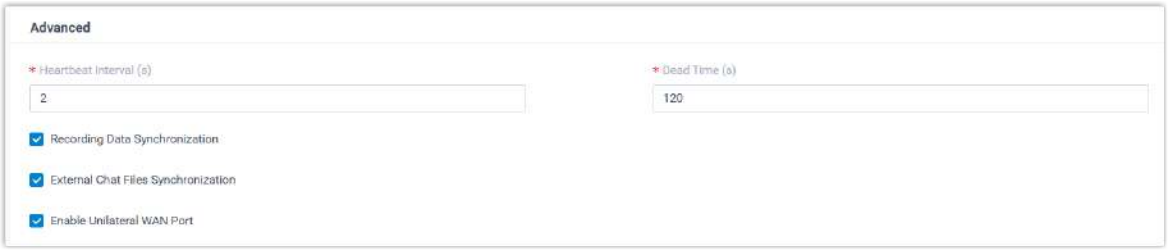


Note:
When you enter a virtual IP address, the corresponding information of **Subnet Mask**, **Virtual Gateway** and **Network Connection Detection** is automatically filled in.

Setting	Description
Virtual IP Address	Virtual IP address is an IP address that has not been assigned to other devices and will be the shared IP address for the two PBXs. The virtual IP always points to the active PBX server. **Note:** • Set the same virtual IP address on the Primary Server and Secondary Server. • After Hot Standby is enabled, you can access and operate the PBX system via the virtual IP. For example, use the virtual 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

Setting	Description
	system have abnormal internet connection. In this case, the PBX failover would not work.

5. In the **Advanced** section, complete the following settings.



Setting	Description
Heartbeat Interval (s)	Define the frequency to send heartbeat keep-alive packets. The default value is 2 seconds, which means that the Secondary Server sends packet every 2 seconds to detect whether the Primary Server is alive or not.
Dead Time (s)	Define the maximum time interval before the Primary Server responds to the Secondary Server. The default value is 120 seconds. If the Secondary Server receives no response after timeout, it will take over the PBX system automatically. **Note:** Set the **Dead Time** longer than the server rebooting time (about 2 minutes), or the Secondary Server will take over when the Primary Server is rebooting.
Recording Data Synchronization	If enabled, the Secondary Server will synchronize the call recording files in real-time.
External Chat Files Synchronization	If enabled, the secondary server will synchronize the external chat files in real time.
Enable Unilateral WAN Port	If enabled, only one WAN port of the Primary Server and Secondary Server will be enabled. When PBX Hot Standby failover occurs, the WAN IP address will remain unchanged and will be switched to the active PBX server.

6. Click **Save**.

   The system prompts that you need to reboot the server to make Hot Standby take effect.

Result

Primary Server

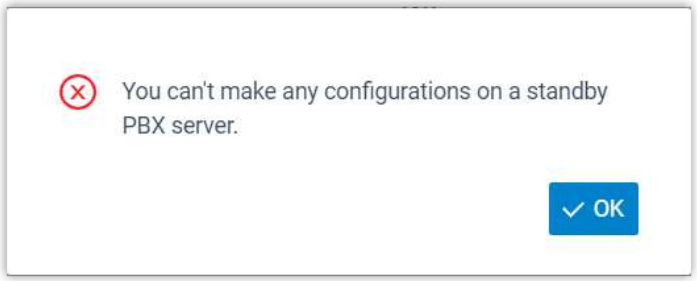
- After the PBX is rebooted, the **Status** displays **Running**.

- When you configure the Primary Server, the configuration will be synchronized to the Secondary Server.

Secondary Server

- After the PBX is rebooted, the **Status** of the Secondary Server displays **Standby**.

- When you try to make configuration on the Secondary Server, the system prompts "You can't make any configurations on a standby server".



What to do next

Test if Hot Standby works.

1. On Primary Server, create an extension, save and apply the changes.
2. On Secondary Server, check if the Hot Standby configurations are correct.

You can see the same extension is added automatically in the Secondary Server.

Primary Server Takes over the System from Secondary Server

The Secondary Server automatically takes over if the Primary Server goes down. You need to take over the PBX system on Primary Server after repairing. This topic describes how to take over the PBX system from the Secondary Server.

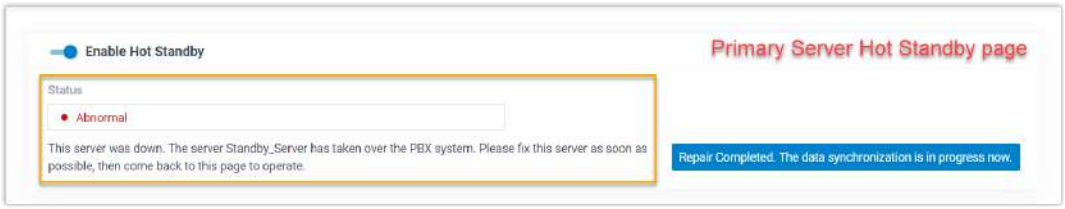
Background information

When the Primary Server fails, the Secondary Server will automatically take over the PBX system, and send a event notification of **PBX Hot Standby Failover** to the contacts concerned.

In this case, the Hot Standby status of Primary Server and Secondary Server is shown as below.

Primary Server

The Hot Standby status displays **Abnormal**, and the page prompts that the Secondary Server has taken over the PBX system, you need to repair the Primary Server as soon as possible.



Secondary Server

The hot standby status changes from **Standby** to **Running**, and the page prompts that the Secondary Server has taken over the PBX system, you need to fix the Primary Server as soon as possible.

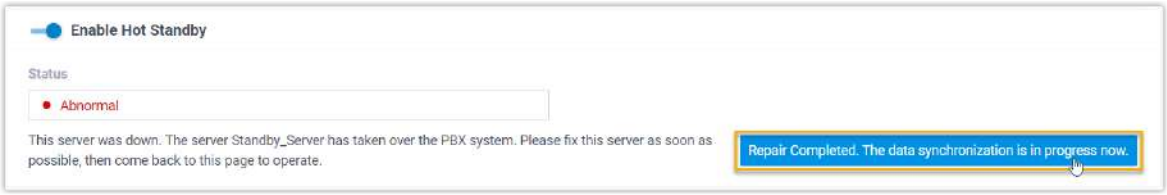
After you have repaired the Primary Server, you need to manually set up the Primary Server to take over the system from Secondary Server.

Prerequisites

- Make sure the firmwares of the Hot Standby pair are the same.
- Make sure there is no call in progress on the Secondary Server, or the call will be dropped.

Procedure

1. Log in to the PBX web portal of the Primary Server, go to **System > High Availability > Hot Standby**.
2. Click **Repair Completed. The data synchronization is in progress now**.

   The Hot Standby status of Primary Server becomes **Standby**, and the server starts to synchronize data from the Secondary Server.

   After data synchronization is completed, the PBX system will send an event notification of **Primary Server Data Restoration Completed** to the contacts concerned.
3. Click **Take Over**.

4. In the pop-up window, click **OK**.

Result

- The **Status** of the Primary Server changes to **Running**, indicating that the Primary Server has taken over the PBX system.
- The Secondary Server returns to standby state.

Secondary Server Takes over the System from Primary Server

If the Primary Server becomes abnormal and hot standby failover is not triggered, you can manually switch the system to the Secondary Server while it is in Standby mode.

Requirements

The firmware version of Secondary Server is 83.17.0.60 or later.

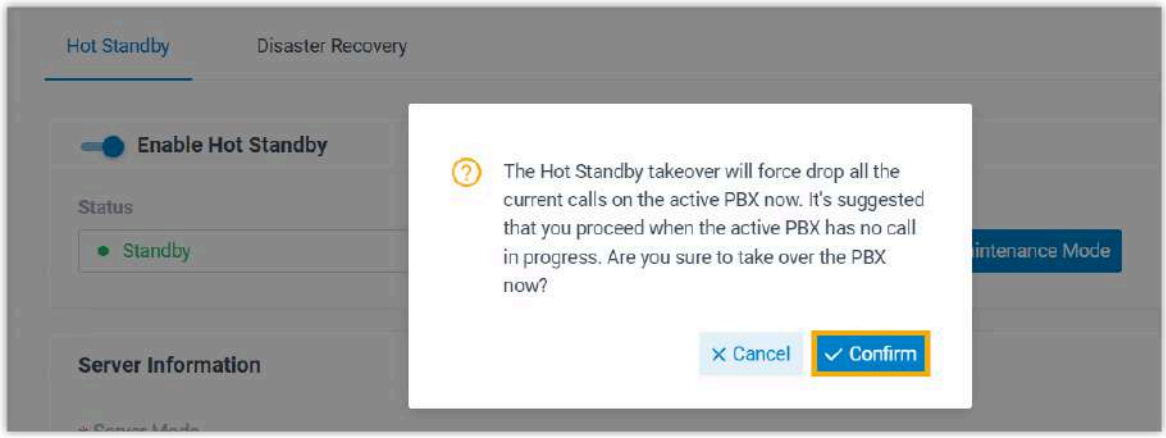
Prerequisites

Make sure there is no call in progress on the Primary Server, or the call will be dropped.

Procedure

1. Log in to the web portal of Secondary Server, go to **System > High Availability > Hot Standby**.
2. Click **Take Over**.

3. In the pop-up window, click **Confirm**.



Result

- The webpage displays "This server has taken over the system.", and the **Status** of the Secondary Server changes to **Running**.
- The system will send a event notification of **Secondary Server Takeover (For Only 30 Days)** to the contacts concerned.

Enable and Schedule Maintenance Mode on Secondary Server

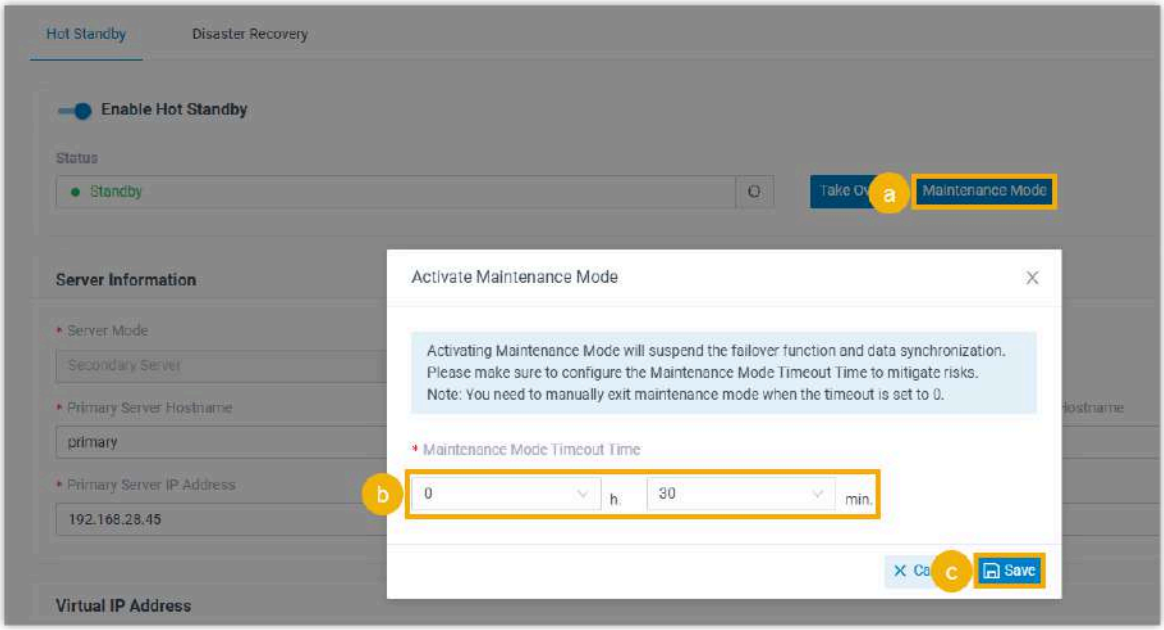
When Primary Server is under maintenance (e.g. firmware upgrade or system reboot), it may fail to respond to heartbeat packets from Secondary Server, which would trigger an unexpected takeover. To avoid this, you can enable and schedule Maintenance Mode on the Secondary Server to temporarily suspend health monitoring and prevent takeover during the maintenance window.

Requirements

The firmware version of Secondary Server is 83.19.0.70 or later.

Procedure

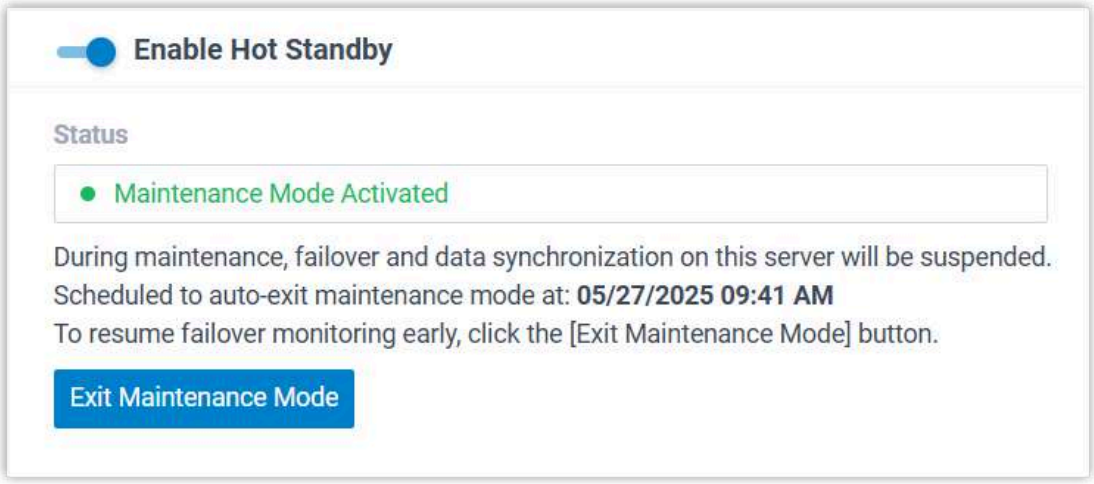
1. Log in to the web portal of Secondary Server, go to **System > High Availability > Hot Standby**.
2. Enable and schedule maintenance mode.



a. Click **Maintenance Mode**.
b. In the **Maintenance Mode Timeout Time** drop-down list, set the timeout.
c. Click **Save**.

Result

- The status displays **Maintenance Mode Activated**. During the maintenance window, failover and data synchronization are suspended.



- When the maintenance timeout is reached, the Secondary Server will automatically exit Maintenance Mode and resume failover monitoring as well as data synchronization.

> **Note:**
> - If the timeout is set to 0, you must click **Exit Maintenance Mode** to manually exit when the Primary Server is ready.
> - If a specific timeout is set, you can also exit manually in advance.

Disaster Recovery

Yeastar Disaster Recovery Overview

Yeastar Disaster Recovery allows you to deploy two Yeastar P-Series Software Editions in different locations as a disaster recovery pair. In the event that your local PBX fails, the telephony services will be automatically switched to the remote site, ensuring that your business calls can continue as usual.

What is Disaster Recovery?

Typically, Disaster Recovery refers to the establishment of a production system that similar to the local production system in different regions. It involves backing up critical data in

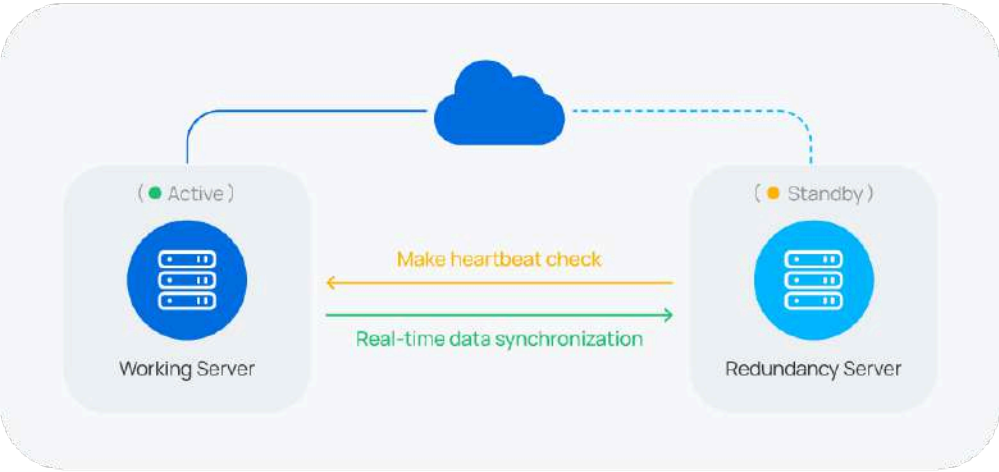
the remote regions, and using the backups to continue or resume business operations in the event of disaster.

Specially, Yeastar Disaster Recovery allows you to deploy a PBX in the main office and a replica PBX in a different region. When your PBX fails, the replica PBX will take over to support the continuity of all PBX telephony services.

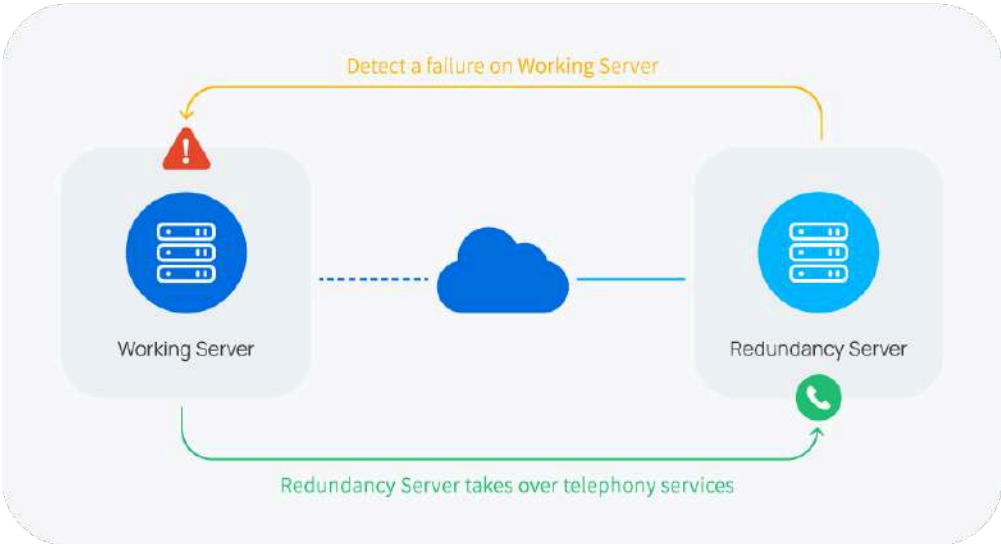
How does Yeastar Disaster Recovery work?

Yeastar Disaster Recovery ensures the continuous availability of telephony services by implementing an active-standby approach across two Yeastar P-Series Software Editions, one of which works as **Working Server** (active mode) while the other serves as **Redundancy Server** (standby mode).

Generally, all PBX functions are provided by the **Working Server**, while the **Redundancy Server** continuously monitors the health of **Working Server** via heartbeat mechanism and replicates telephony data from **Working Server** in real time.



Once the **Working Server** goes down, the telephony services would be automatically switched to the **Redundancy Server**, minimizing the downtime and ensuring business continuity.



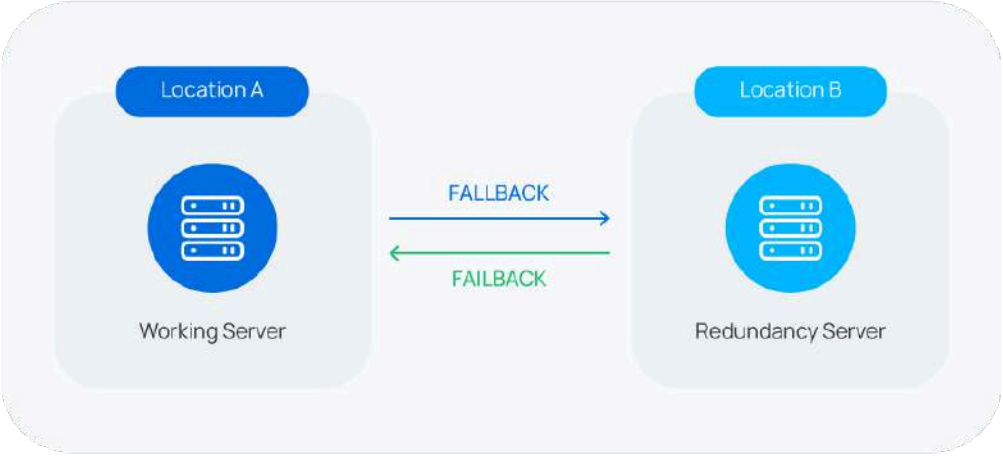
Which deployment environment can Yeastar Disaster Recovery work for?

Yeastar Disaster Recovery supports the following deployment environments:

1+1 Mode: One PBX works as Working Server, another PBX serves as Redundancy Server

In this deployment environment, the **Working Server** is deployed at Location A and the **Redundancy Server** is deployed at Location B.

When the **Working Server** at Location A fails, essential telephony services will automatically fall back to the **Redundancy Server**. After the **Working Server** is repaired, a manual failback is required to allow the **Working Server** to resume the telephony services.

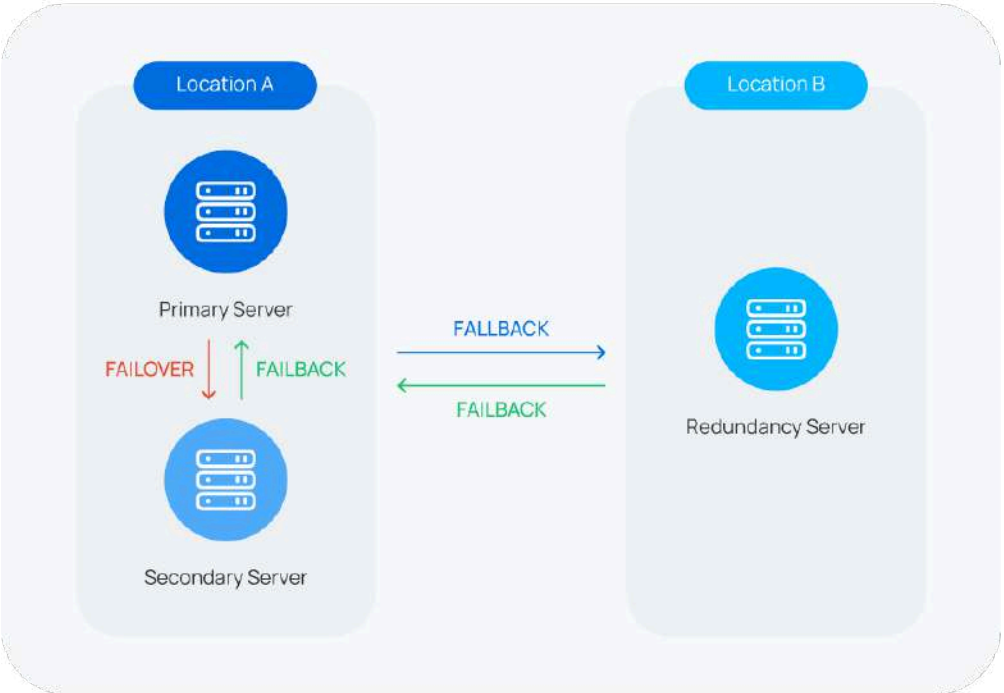


2+1 Mode: Two PBXs serve as Standby Server, One PBX works as Primary Server

In this deployment environment, two **Standby Server**s are deployed in different locations, one serving as a **Secondary Server** at Location A along with the **Primary Server** as a Hot Standby pair, the other serving as a **Redundancy Server** at Location B.

When the **Primary Server** at Location A fails, either **Secondary Server** or **Redundancy Server** will take over, depending on the status of **Secondary Server**.

- If the **Secondary Server** at Location A works normally, it will take over the entire phone system. Once **Primary Server** is repaired, a manual failback is required to allow **Primary Server** to take control of the phone system.
- If the **Secondary Server** is abnormal, **Redundancy Server** at Location B will take over the essential telephony services. Once **Primary Server** and **Secondary Server** are restored, a manual failback is required to resume the telephony services on **Primary Server**.



How to set up Yeastar Disaster Recovery?

Preparations

Prepare two Yeastar P-Series Software Editions that both meet the following requirements.

> **Note:**
> If you already have a PBX, provide your service provider with the PBX SN to purchase another license for Redundancy Server. If you don't have a PBX, contact your service provider to purchase two licenses for the disaster recovery pair.

Item	Requirement
Product Model	Yeastar P-Series Software Edition
Plan	Ultimate Plan
Version	Same firmware version and must be 83.12.0.57 or later.
Network	LAN port as the default Ethernet interface and a static IP address is required.

Item	Requirement
	Note: If you want to connect the two PBXs using Yeastar SD-WAN, make sure that the PBXs can access Yeastar SD-WAN node (sdwantunnel.yeastar.com).
External Storage	Identical storage device settings and mounting points.

Step 1. Connect two Yeastar P-Series Software Editions

Connect the two phone systems to the same virtual network using your own Site-to-site VPN or Yeastar SD-WAN for data transmission and synchronization.

Step 2. Set up disaster recovery on the two Yeastar P-Series Software Editions

Set up disaster recovery on the two phone systems. The setup method varies depending on how you connect the disaster recovery pair.

For more information, see Set up Disaster Recovery (Site-to-site VPN) and Set up Disaster Recovery (Yeastar SD-WAN).

Disaster Recovery (Site-to-site VPN)

Set up Disaster Recovery (Site-to-site VPN)

You can set up disaster recovery using your Site-to-site VPN connection between two Yeastar P-Series Software Editions, so as to ensure the continuous availability of essential telephony services in the event of a disaster.

Requirements

Both servers in a disaster recovery pair must meet the following requirements.

Item	Requirement
Product Model	Yeastar P-Series Software Edition
Plan	Ultimate Plan
Version	Same firmware version and must be 83.12.0.57 or later.
Network	LAN port as the default Ethernet interface and a static IP address is required.

Item	Requirement
External Storage	Identical storage device settings and mounting points.

Prerequisites

You have connected two Yeastar P-Series Software Editions using Site-to-site VPN, and they can communicate with each other.

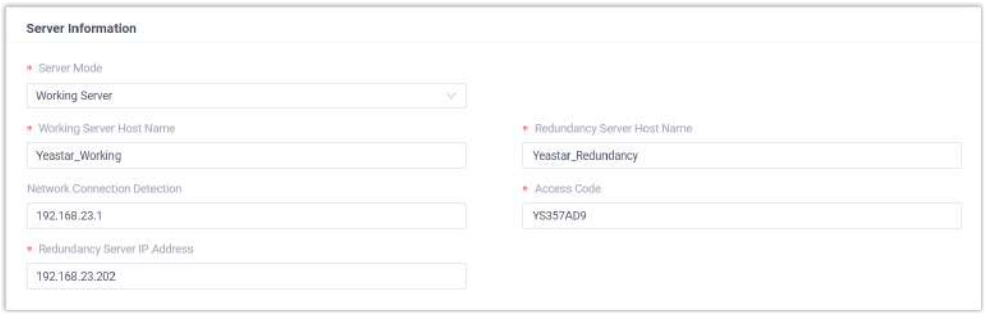
Procedure

To implement disaster recovery, you need to complete the following settings on both **Working Server** and **Redundancy Server**.

1. Log in to PBX web portal, go to **System > High Availability > Disaster Recovery**.
2. Enable disaster recovery and set the remote networking method.

   a. On the top of the page, turn on the **Enable Disaster Recovery** switch.
   b. In the **Remote Networking Method** drop-down list, select **Site-to-site VPN**.
3. Complete the following settings for the disaster recovery pair.

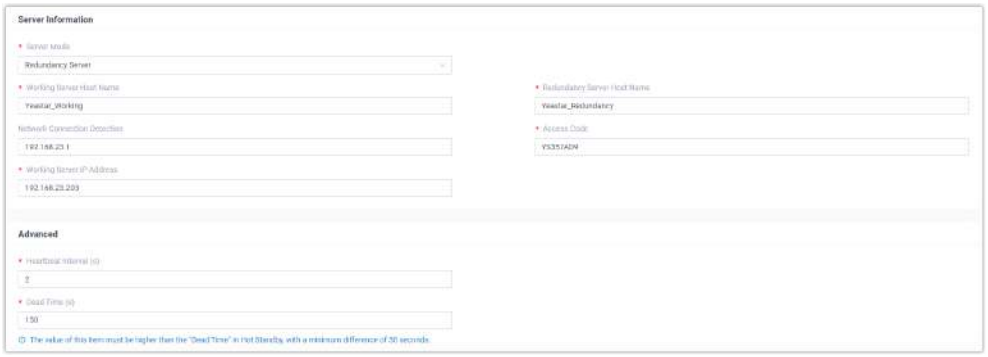
   Working Server



Setting	Description
Server Mode	Select **Working Server**. **Note:** If you have set up Hot Standby, only the **Primary Server** can act as **Working Server**.
Working Server Host Name	Enter a name to help you identify the Working Server when receiving event notifications. **Note:** The **Working Server Host Name** set in the Working Server and Redundancy Server should be the same to avoid confusion in event notifications.
Redundancy Server Host Name	Enter a name to help you identify the Redundancy Server when receiving event notifications. **Note:** The **Redundancy Server Host Name** set in the Working Server and Redundancy Server should be the same to avoid confusion in event notifications.
Network Connection Detection	Enter a network detection node (e.g. the gateway address of VPN router) to detect the Working Server's connection to the VPN. This helps prevent an unexpected takeover if the Redundancy Server doesn't receive heartbeat response from the Working Server.
Access Code	Set an access code.

Setting	Description
	Note: The two PBXs must have the same access code to authenticate connection.
Redundancy Server IP Address	Enter the IP address assigned to the Redundancy Server in your VPN network.

Redundancy Server



Setting	Description
Server Information	
Server Mode	Select **Redundancy Server**.
Working Server Host Name	Enter a name to help you identify the Working Server when receiving event notifications. **Note:** The **Working Server Host Name** set in the Working Server and Redundancy Server should be the same to avoid confusion in event notifications.
Redundancy Server Host Name	Enter a name to help you identify the Redundancy Server when receiving event notifications. **Note:** The **Redundancy Server Host Name** set in the Working Server and Redundancy Server should be the same to avoid confusion in event notifications.

Setting	Description
Network Connection Detection	Enter a network detection node to detect the Redundancy Server's connection to the VPN. This helps prevent an unexpected takeover if the Redundancy Server doesn't receive heartbeat response.
Access Code	Set an access code. **Note:** The two PBXs must have the same access code to authenticate connection.
Working Server IP Address	Enter the IP address based on the deployment environment of the Working Server. • If Hot Standby is enabled, enter the virtual IP. • If Hot Standby is disabled, enter the IP address assigned to the Working Server in your VPN network.
Advanced	
Heartbeat Interval (s)	Define the frequency to send heartbeat packets. The default value is 2 seconds, which means that the Redundancy Server sends packets every 2 seconds to detect whether the Working Server is alive or not.
Dead Time (s)	Define the maximum time interval before the Working Server responds to the Redundancy Server. The default value is 150 seconds. If the Redundancy Server receives no response after timeout, it will take over the telephony services automatically. **Note:** If you have set up Hot Standby, the value set here MUST be greater than the **Dead Time** in Hot Standby, with a minimum difference of 30 seconds.

4. Click **Save**.

   The system prompts that you need to reboot the PBXs to make disaster recovery take effect.

5. Click **Reboot Now**.

Result

After rebooting the PBXs, you can check the disaster recovery status on PBX web portal:

- On Working Server, the status is displayed as **Working**, indicating that the server is running to provide all PBX functions.

- On Redundancy Server, the status is displayed as **In Redundancy**, indicating that the server is in redundancy status. The Redundancy Server will now replicate data from the Working Server.

What to do next

Read Server Redundancy on SIP Trunks and WebRTC Trunks and Server Redundancy on SIP Devices and Linkus UC Clients to learn how server redundancy can be implemented on trunks and extension endpoints.

Server Redundancy on SIP Trunks and WebRTC Trunks

After setting up disaster recovery on Yeastar P-Series Software Edition, server redundancy can be implemented on SIP trunks and WebRTC trunks.

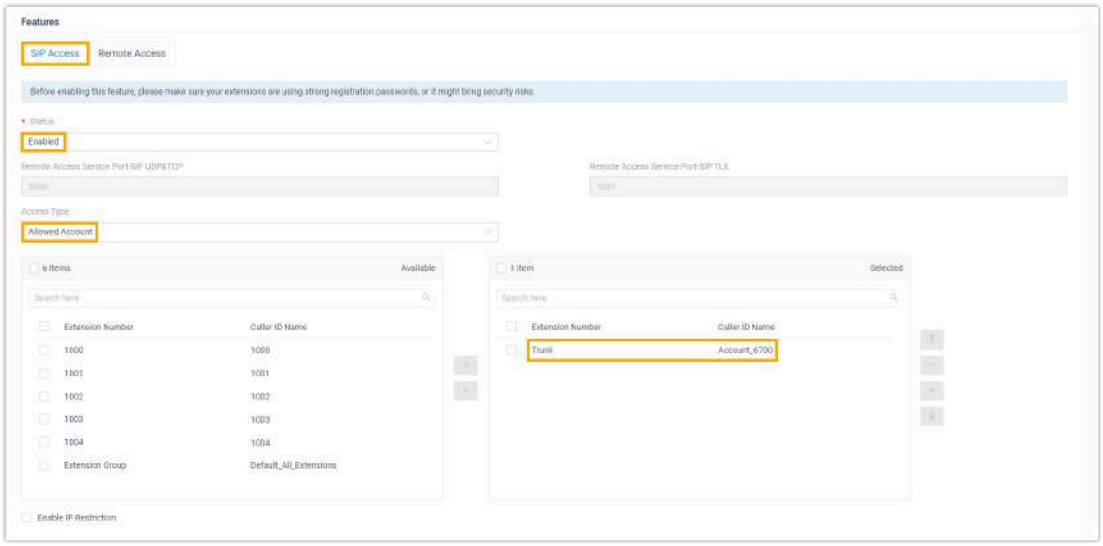
> **Note:**
> If you have extended physical trunks for Yeastar P-Series Software Edition, server redundancy will NOT be supported on these trunks.

Server redundancy on SIP account trunk

Yeastar Disaster Recovery implements server redundancy on SIP account trunks via **Yeastar FQDN**, which always points to the server in the disaster recovery pair that is in working status.

After you set up disaster recovery, server redundancy can be automatically implemented on the account trunks that meet both of the following criteria:

- The account trunk has been assigned the remote SIP access permission (Path: **System > Network > Yeastar FQDN > Features > SIP Access**).



- The account has been registered by the third-party software or device using Yeastar FQDN.

The account trunks that meet the above criteria are available regardless of which server is working, but the trunk status of the disaster recovery pair is different because only the server in working status can connect to the third-party software or device.

- When the Working Server works normally, the account trunk displays (**Registered**) on Working Server and displays (**Disabled**) on Redundancy Server.

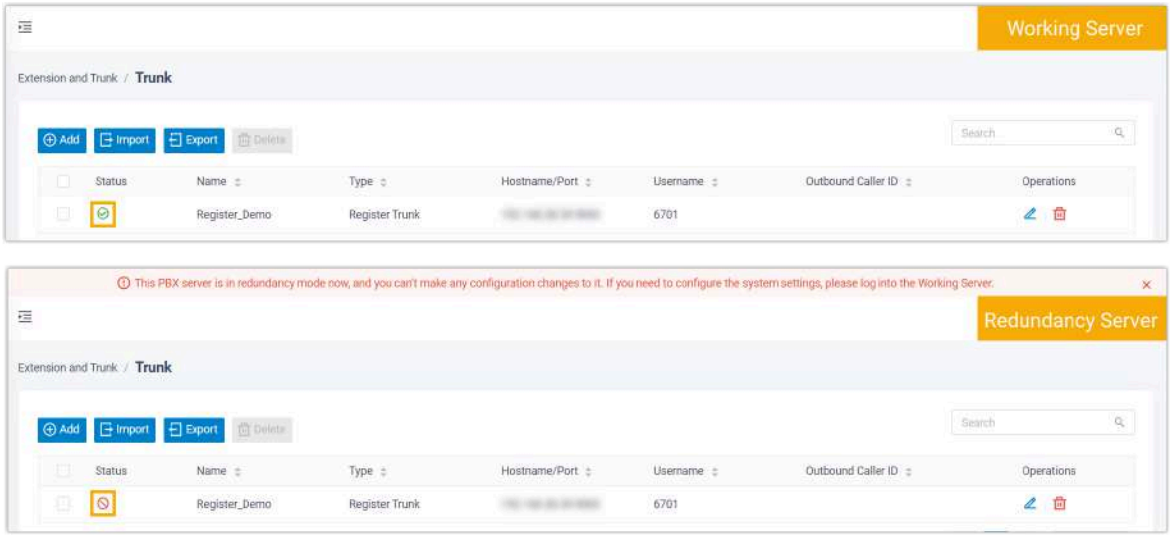
- When the Working Server goes down and the Redundancy Server takes over, the account trunk displays (**Registered**) on Redundancy Server.

Server redundancy on SIP register trunk

Yeastar Disaster Recovery automatically implements server redundancy on SIP register trunks, you don't need to perform any operations.

The register trunks are available regardless of which server is working, but the trunk status of the disaster recovery pair is different because only the server in working status can register with the ITSP (Internet Telephony Service Provider).

- When the Working Server works normally, the register trunk displays (**Registered**) on Working Server and displays (**Disabled**) on Redundancy Server.

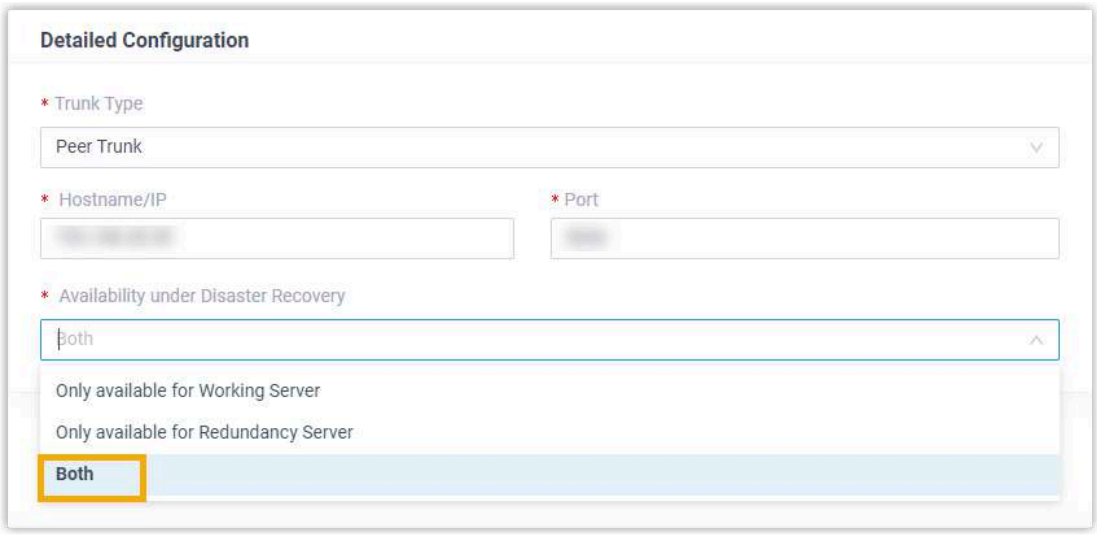


- When the Working Server goes down and the Redundancy Server takes over, the register trunk displays (**Registered**) on Redundancy Server.

Server redundancy on SIP peer trunk

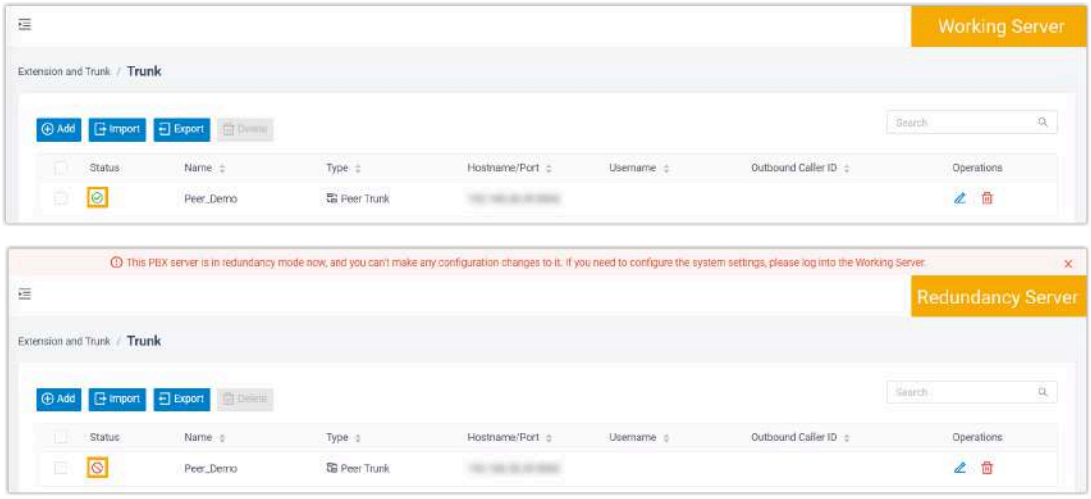
If the ITSP (Internet Telephony Service Provider) supports dual registration, server redundancy can be implemented on SIP peer trunks. To achieve this, you need to set the availability of SIP peer trunk as follows:

1. Go to **Extension and Trunk > Trunk**, edit the desired peer trunk.
2. In the **Detailed Configuration** section, select **Both** from the drop-down list of **Availability under Disaster Recovery**.

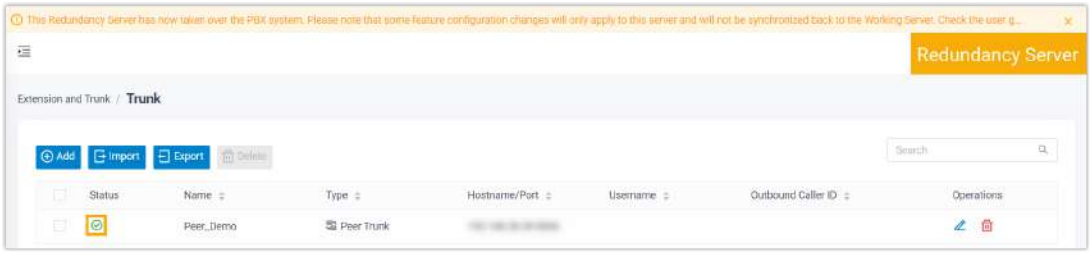


3. Click **Save** and **Apply**.
   The peer trunk is available regardless of which server is working, but the trunk status of the disaster recovery pair is different because only the server in working status can register with the ITSP.

   - When the Working Server works normally, the peer trunk displays (**Reachable**) on Working Server and displays (**Disabled**) on Redundancy Server.



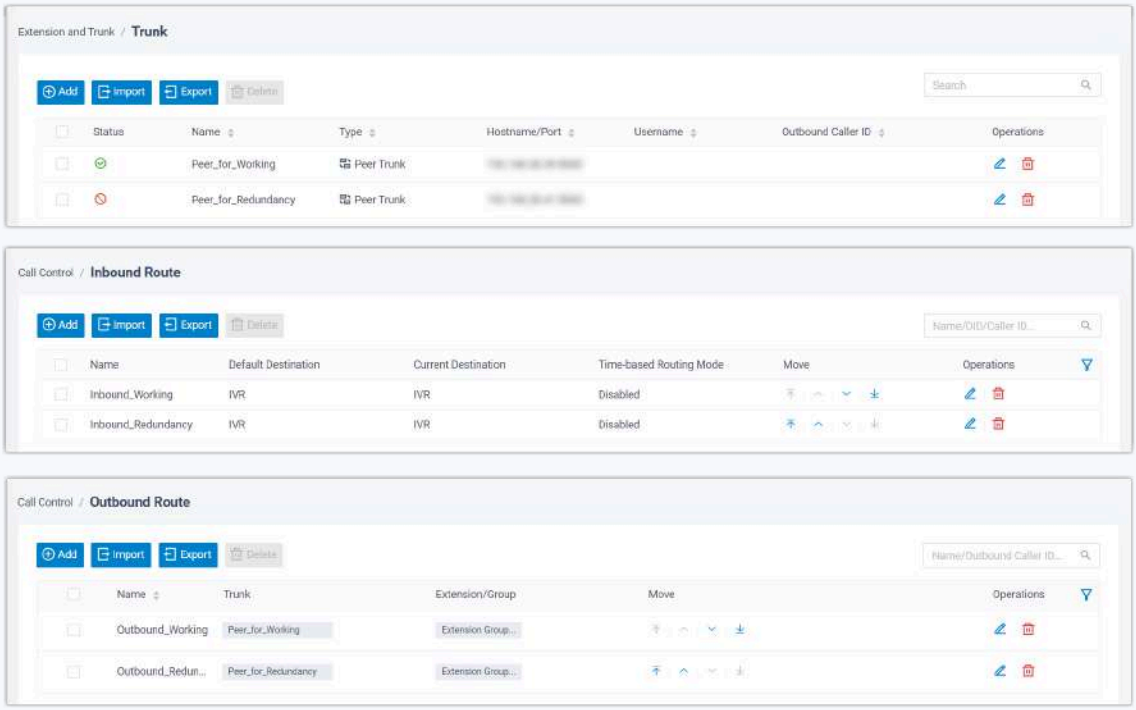
   - When the Working Server goes down and the Redundancy Server takes over, the peer trunk displays (**Reachable**) on Redundancy Server, and can be used for calls.



Note:

If the ITSP doesn't support dual registration, you can register both Working Server and Redundancy Server to the ITSP. In this way, extension users of Working Server can make and receive calls even if the Working Server goes down.

To achieve this, your need to create peer trunks on the Working Server to enable the disaster recovery pair to register to the ITSP. More importantly, set inbound routes and outbound routes to route calls through the trunks.



Server redundancy on WebRTC trunk

Yeastar Disaster Recovery implements server redundancy on WebRTC trunks via **Yeastar FQDN**, which always points to the server in the disaster recovery pair that is in working status.

As WebRTC trunks rely on Yeastar FQDN, so the sever redundancy is implemented automatically, you don't need to perform any operations. The WebRTC trunks are available regardless of which server is working, but the trunk status of the disaster recovery pair is different:

- When the Working Server works normally, the WebRTC trunk displays (**Available**) on Working Server and displays (**Disabled**) on Redundancy Server.

- When the Working Server goes down and the Redundancy Server takes over, the WebRTC trunk displays (**Available**) on Redundancy Server.

Server Redundancy (Site-to-site VPN) on SIP Devices and Linkus UC Clients

After setting up disaster recovery on Yeastar P-Series Software Edition, server redundancy can be implemented on **Auto Provisioned SIP Devices (IP phones and TA FXS gateways)** and **Linkus UC Clients**.

Server redundancy on IP phone

Yeastar Disaster Recovery implements server redundancy on auto provisioned IP Phones via **VPN IP / Virtual IP** or **Yeastar FQDN**, depending on whether Hot Standby is enabled on the Working Server and how you provision IP phones.

After you set up disaster recovery, the Yealink IP phones that have been provisioned will be automatically updated with the server information of the disaster recovery pair, as shown below.

> **Note:**
> To implement server redundancy on other IP phones that can be provisioned by Yeastar PBX, contact Yeastar Support.

Auto Provisioning Method	Description
PnP / DHCP	• **SIP Server 1**: The VPN IP (Hot Standby disabled) or the Virtual IP (Hot Standby enabled) of the Working Server. • **SIP Server 2**: The VPN IP of the Redundancy Server.
RPS FQDN	• **SIP Server 1**: The FQDN of the Working Server. In this scenario, IP phones register to PBX via FQDN, which always points to the server in the disaster recovery pair that is in working status.

Server redundancy on TA FXS gateway

Yeastar Disaster Recovery implements server redundancy on auto provisioned TA FXS gateways via **VPN IP**.

After you set up disaster recovery, you need to Reboot the auto provisioned gateways, so that they can obtain the server information of the disaster recovery pair, as shown below.

- **Hostname/IP**: The VPN IP of the Working Server.
- **Failover Hostname/IP**: The VPN IP of the Redundancy Server.

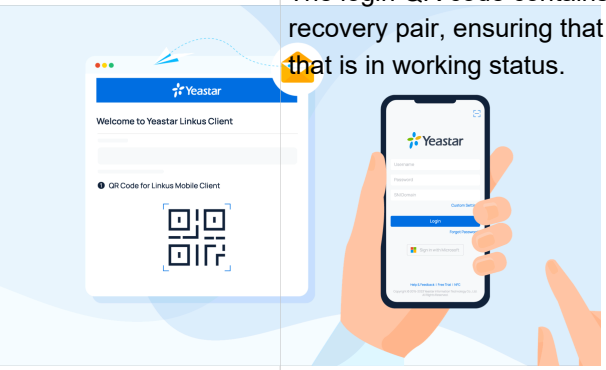
Server redundancy on Linkus Mobile Client

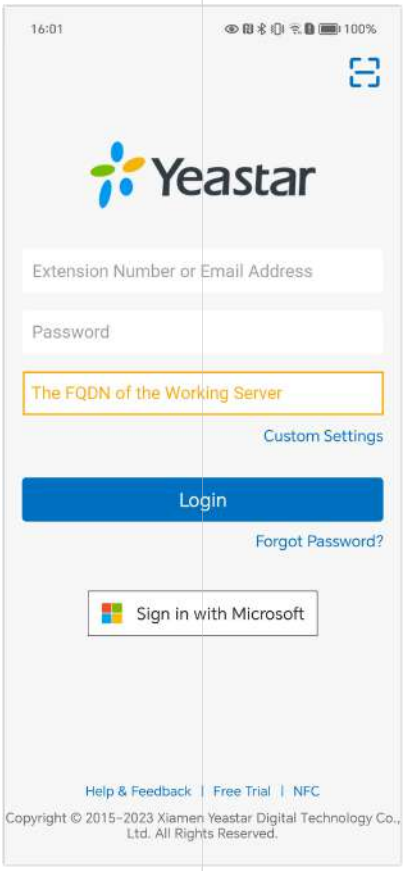
Yeastar Disaster Recovery implements server redundancy on Linkus Mobile Client via **VPN IP** or **Yeastar FQDN**.

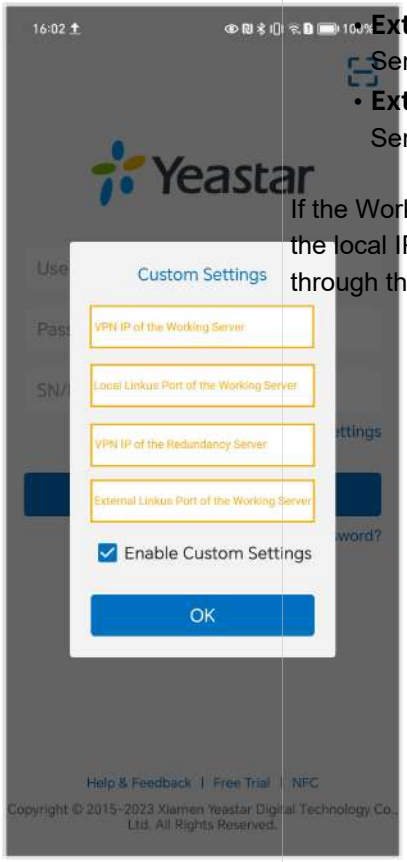
After you set up disaster recovery, users need to log in again to Linkus Mobile Client, so that Linkus can obtain the server information of the disaster recovery pair.

Note:
To achieve server redundancy, the version of Linkus Mobile Client must meet the following requirements:

- Linkus iOS Client: Version 5.2.9 or later
- Linkus Android Client: Version 4.13.16 or later

Scenario	Instruction
Figure 7. **Scan QR Code** 	Scan the login QR code to log in to Linkus Mobile Client. The login QR code contains the server information about the disaster recovery pair, ensuring that Linkus can always connect to the server that is in working status.
Figure 8. **Logining Domain** **Na**	Manually replace the server information with the FQDN of the Working Server in the **SN/Domain** field. The FQDN always points to the server in the disaster recovery pair that is in working status.

Scenario	Instruction
m **e**  	
Figure 9. **Log in using IP**	Manually replace the server information with the VPN IPs and Linkus port of the disaster recovery pair.

Scenario	Instruction
Address and Port 	• **Local Hostname/IP**: The VPN IP of the Working Server. • **Local Port**: The local Linkus port of the Working Server. • **External Hostname/IP**: The VPN IP of the Redundancy Server. • **External Port**: The external Linkus port of the Working Server. If the Working Server works normally, Linkus communicates through the local IP address and port. Otherwise, Linkus communicates through the external IP address and port.

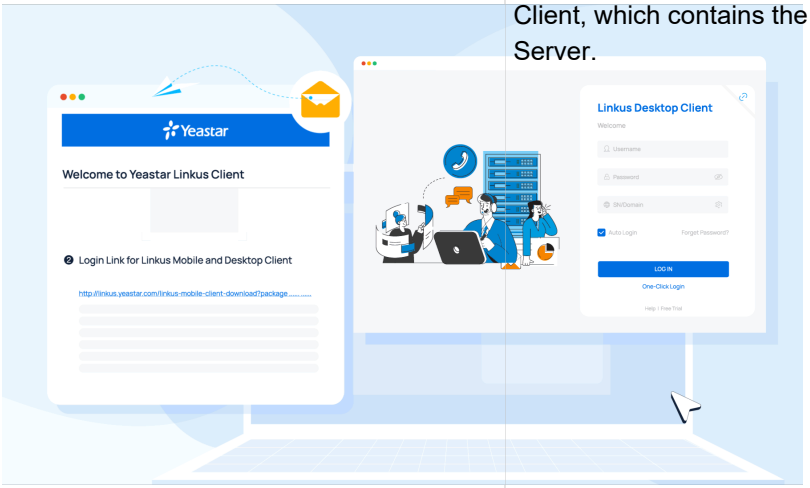
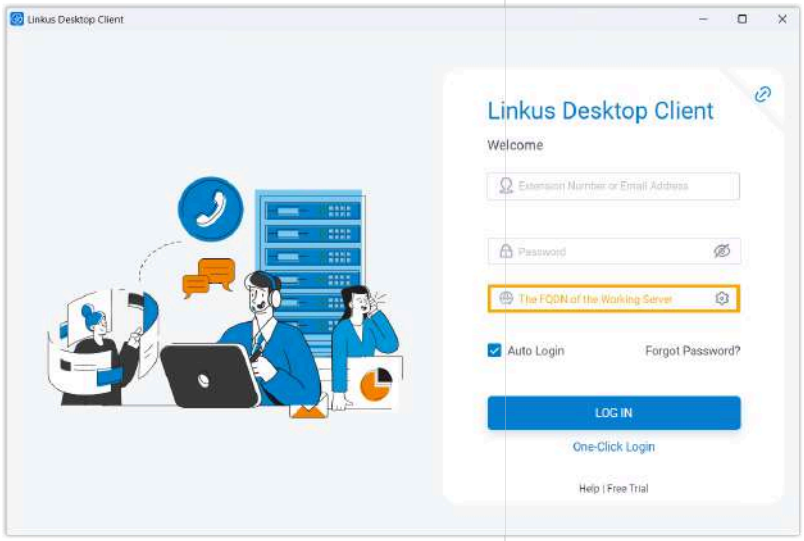
Server redundancy on Linkus Desktop Client

Yeastar Disaster Recovery implements server redundancy on Linkus Desktop Client via **Yeastar FQDN**, which always points to the server in the disaster recovery pair that is in working status.

After you set up disaster recovery, users need to log in again to Linkus Desktop Client via FQDN, as shown below.

Note:

- If the Working Server doesn't have a Yeastar FQDN, then when disaster occurs, users have to log in to Linkus Desktop Client using the VPN IP of the Redundancy Server so as to use telephony services.
- Server redundancy is NOT supported on Linkus Lite.

Scenario	Instruction
Figure 10. **Log in via Link** 	Paste the login link to log in to Linkus Desktop Client, which contains the FQDN of the Working Server.
Figure 11. **Log in using Domain Name** 	Manually replace the server information with the FQDN of the Working Server in the **Domain** field.

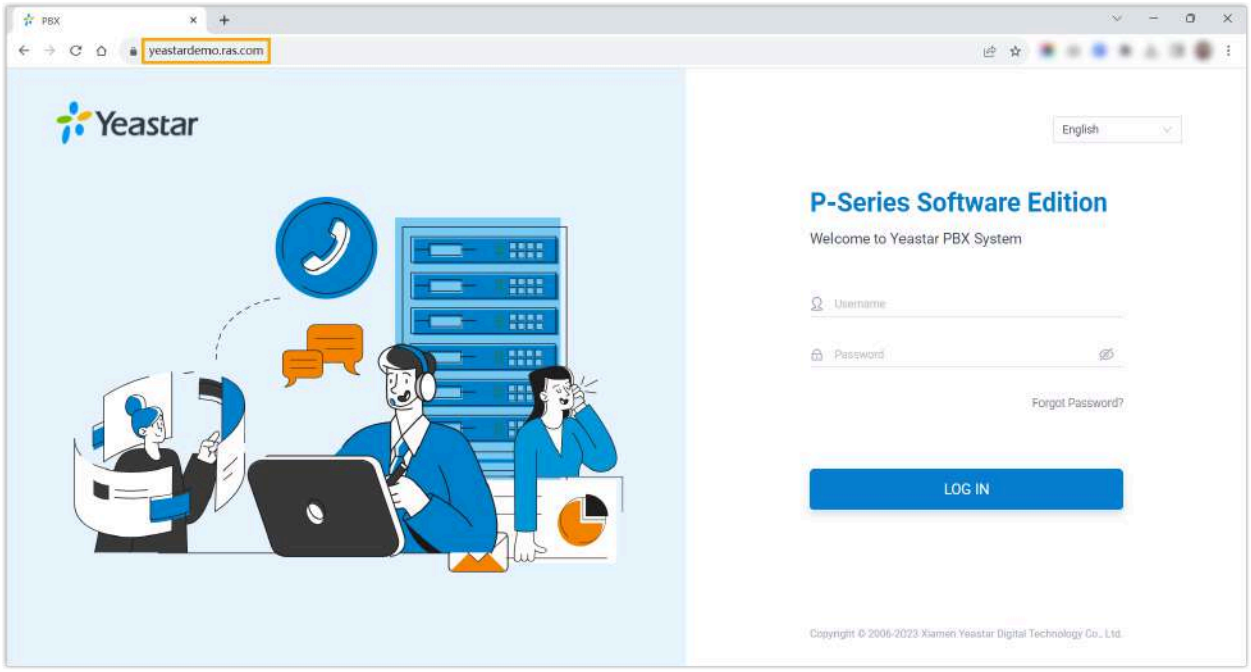
Server redundancy on Linkus Web Client

Yeastar Disaster Recovery implements server redundancy on Linkus Web Client via **Yeastar FQDN**, which always points to the server in the disaster recovery pair that is in working status.

After you set up disaster recovery, users need to access Linkus Web Client via the FQDN of the Working Server, as shown below.

Note:

If the Working Server doesn't have a Yeastar FQDN, then when disaster occurs, users have to log in to Linkus Web Client using the VPN IP of the Redundancy Server so as to use telephony services.



Restricted Configurations and Functions on Redundancy Server after Takeover

When the Redundancy Server takes over, you and your users will still be able to access the PBX management portal and Linkus UC Clients, but some configurations and functions are unavailable. This topic provides an overview of the restricted configurations and functions on PBX management portal and Linkus UC Clients.

Platform	Restricted configurations and functions
PBX Management Portal	**Note:** If you have integrated the Working Server with third-party Collaboration Tools (**Active Directory (AD)**, **Microsoft 365**, **Microsoft Teams**, or **Microsoft Outlook**), the configurations and data will be synchronized to the Redundancy Server, but you can NOT make changes to the configurations and data on the Redundancy Server.

<table>
<tr><th colspan="2">Platform</th><th>Restricted configurations and functions</th></tr>
<tr><td colspan="2"></td><td>Unavailable Configurations:

• CRM
• Helpdesk
• PMS

Available but Out-of-sync Configurations:

Important:
The changes you made to the following configurations will NOT be synchronized back to the Working Server.

• Speech to Text
• AMI
• Database Grant
• Auto Provisioning</td></tr>
<tr><td rowspan="3">Linkus UC Clients</td><td>Linkus Mobile Client</td><td>All the functions are supported except Chat.

Note:
The version of Linkus Mobile Client must meet the following requirements:

• Linkus iOS Client: Version 5.2.9 or later
• Linkus Android Client: Version 4.13.16 or later</td></tr>
<tr><td>Linkus Desktop Client</td><td>All the functions are supported except the followings:

• Chat
• Video Conferencing
• Call Center Console
• Greeting Management (Path: Preferences > Voicemail > Greeting Management)</td></tr>
<tr><td>Linkus Web Client</td><td>All the functions are supported except the followings:

• Chat
• Video Conferencing
• Call Center Console
• Greeting Management (Path: Preferences > Voicemail > Greeting Management)</td></tr>
</table>

Working Server Resumes Telephony Services after Redundancy Server Took Over

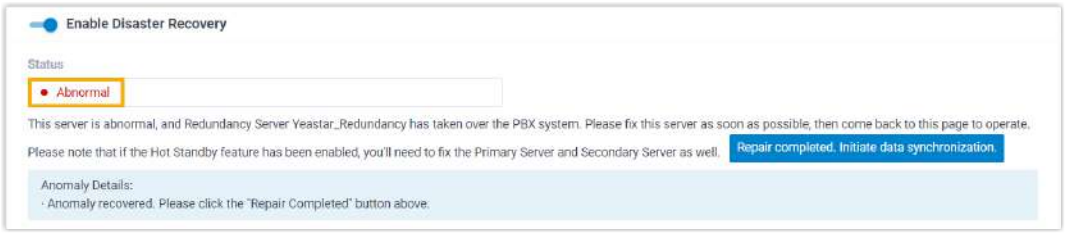
The Redundancy Server automatically takes over telephony services when the Working Server goes down. You need to resume the telephony services on Working Server after repairing.

Background information

When the Working Server fails and a fallback occurs, the system will send a **Disaster Recovery Fallback** event notification to relevant contacts, and update the Disaster Recovery status on PBX web portal as shown below.

Working Server

The Disaster Recovery status changes from **Working** to **Abnormal**, the page prompts that the Redundancy Server has taken over the PBX system and you need to repair the Working Server as soon as possible.



Redundancy Server

The Disaster Recovery status changes from **In Redundancy** to **Working**, the page prompts that the Redundancy Server has taken over the PBX system and you need to repair the Working Server as soon as possible.

After you repair the Working Server, you need to manually set up the Working Server to resume service.

Procedure

Important:

> Make sure there is no call in progress on the Redundancy Server, or the call will be dropped.

1. Log in to the PBX web portal of Working Server, go to **System > High Availability > Disaster Recovery**.
2. Click **Repair completed. Initiate data synchronization.**.

   The Disaster Recovery status of Working Server becomes **Recovering Data**, indicating that the server starts to synchronize data from the Redundancy Server.

   After data synchronization is completed, the Disaster Recovery status will change to **Data Recovered**, and relevant contacts of both servers will receive a **Working Server Data Restoration Completed** event notification.
3. Click **Take Over**.

4. In the pop-up window, click **OK**.

Result

- The **Status** of the Working Server changes to **Working**, indicating that the Working Server has resumed the telephony services.
- The Redundancy Server returns to the redundancy status.

Enable and Schedule Maintenance Mode on Redundancy Server

When Working Server is under maintenance (e.g. firmware upgrade or system reboot), it may fail to respond to heartbeat packets from Redundancy Server, which would trigger an

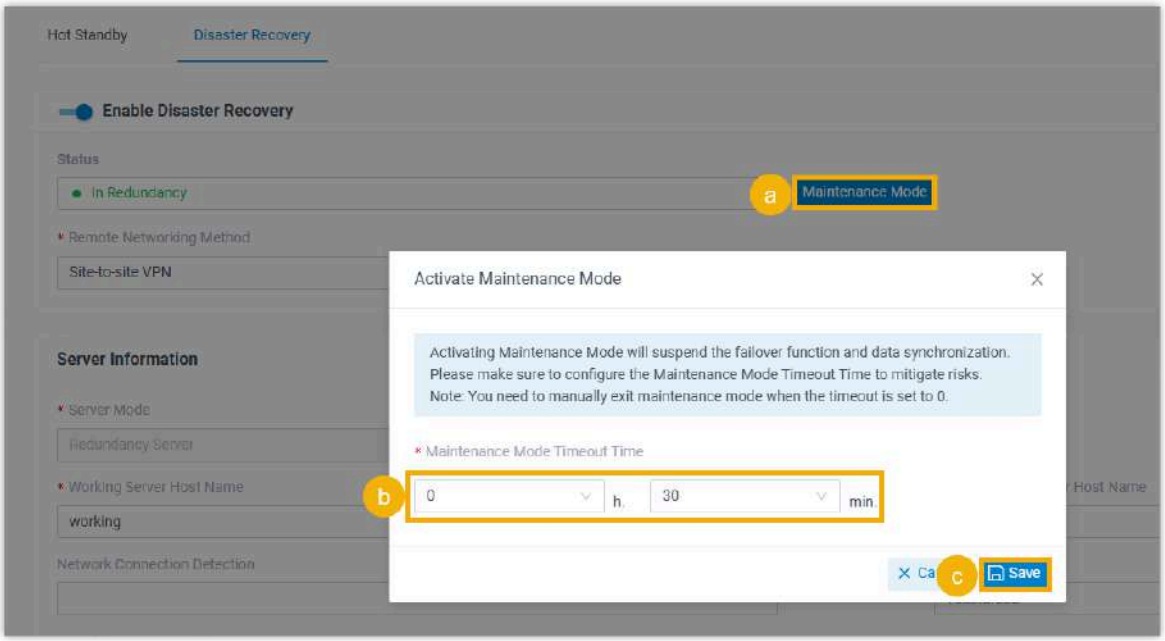
unexpected fallback. To avoid this, you can enable and schedule Maintenance Mode on the Redundancy Server to temporarily suspend health monitoring and prevent fallback during the maintenance window.

Requirements

The firmware version of Redundancy Server is 83.19.0.70 or later.

Procedure

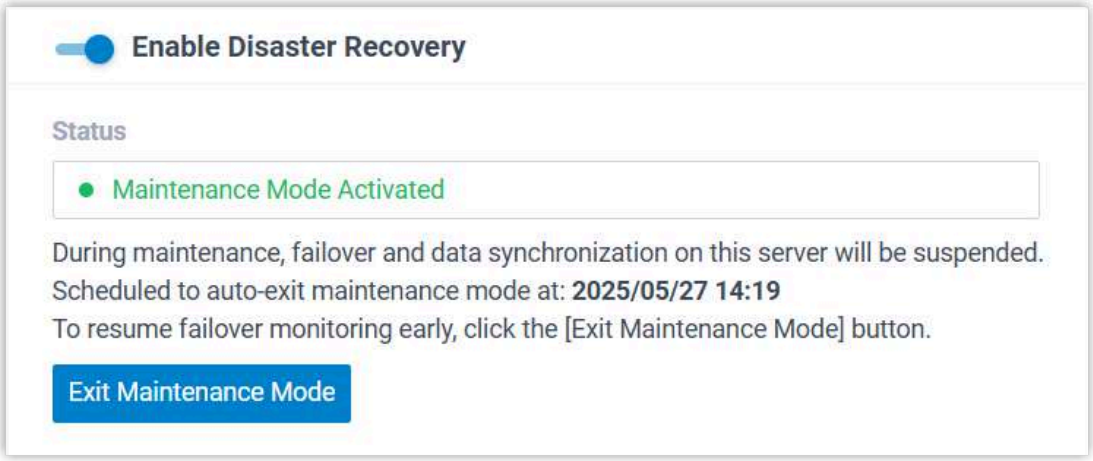
1. Log in to the web portal of Redundancy Server, go to **System > High Availability > Disaster Recovery**.
2. Enable and schedule maintenance mode.



   a. Click **Maintenance Mode**.
   b. In the **Maintenance Mode Timeout Time** drop-down list, set the timeout.
   c. Click **Save**.

Result

- The status displays **Maintenance Mode Activated**. During the maintenance window, telephony service fallback and data replication are suspended.



- When the maintenance timeout is reached, the Redundancy Server will automatically exit Maintenance Mode and resume fallback monitoring and data replication.

> **Note:**
> - If the timeout is set to 0, you must click **Exit Maintenance Mode** to manually exit when the Working Server is ready.
> - If a specific timeout is set, you can also exit manually in advance.

Disaster Recovery (Yeastar SD-WAN)

Set up Disaster Recovery (Yeastar SD-WAN)

If you have connected two Yeastar P-Series Software Editions in different locations using Yeastar SD-WAN, you can set up disaster recovery on the two PBXs to ensure the continuous availability of essential telephony services in the event of a disaster.

Requirements

Both servers in a disaster recovery pair must meet the following requirements.

Item	Requirement
Product Model	Yeastar P-Series Software Edition
Plan	Ultimate Plan
Version	Same firmware version and must be 83.12.0.57 or later.
Network	• LAN port as the default Ethernet interface and a static IP address is required.

Item	Requirement
	• Accessible to Yeastar SD-WAN node (sdwantunnel.yeastar.com).
External Storage	Identical storage device settings and mounting points.

Step 1. Connect two Yeastar P-Series Software Editions using Yeastar SD-WAN

Connect two Yeastar P-Series Software Editions to the same virtual network using Yeastar SD-WAN.

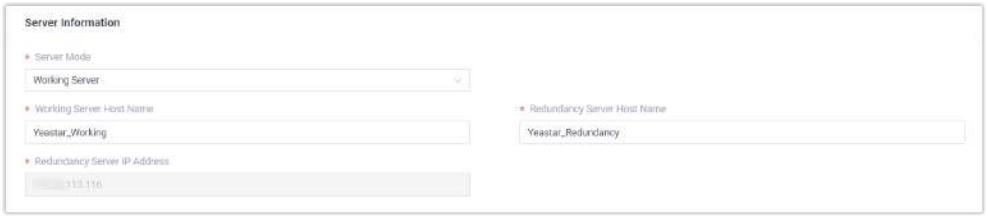
For more information, see Set up SD-WAN Network on Working Server and Join SD-WAN Network on Redundancy Server.

Step 2. Set up disaster recovery on the two Yeastar P-Series Software Editions

1. Log in to PBX web portal, go to **System > High Availability > Disaster Recovery**.
2. Enable disaster recovery and set the remote networking method.

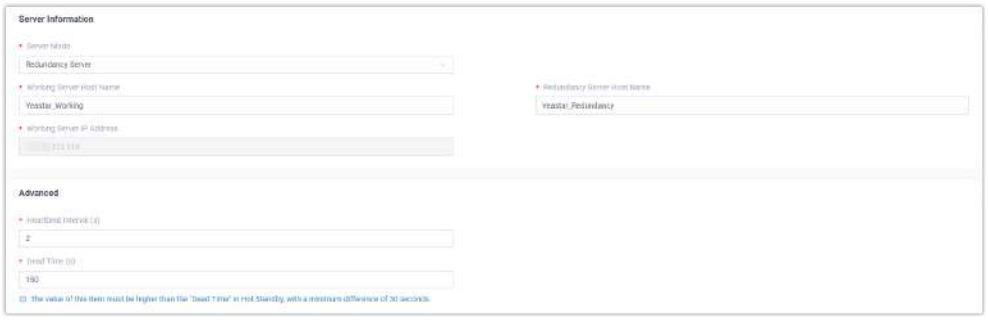
   a. On the top of the page, turn on the **Enable Disaster Recovery** switch.
   b. In the **Remote Networking Method** drop-down list, select **Yeastar SD-WAN**.
3. Complete the following settings for the disaster recovery pair.

   Working Server



Setting	Description
Server Mode	Select **Working Server**. **Note:** If you have set up Hot Standby, only the **Primary Server** can act as **Working Server**.
Working Server Host Name	Enter a name to help you identify the Working Server when receiving event notifications. **Note:** The **Working Server Host Name** set in the Working Server and Redundancy Server should be the same to avoid confusion in event notifications.
Redundancy Server Host Name	Enter a name to help you identify the Redundancy Server when receiving event notifications. **Note:** The **Redundancy Server Host Name** set in the Working Server and Redundancy Server should be the same to avoid confusion in event notifications.
Redundancy Server IP Address	Automatically synchronize the network IP assigned to the Redundancy Server within the SD-WAN network. 

Redundancy Server



Setting	Description
Server Information	
Server Mode	Select **Redundancy Server**.
Working Server Host Name	Enter a name to help you identify the Working Server when receiving event notifications. **Note:** The **Working Server Host Name** set in the Working Server and Redundancy Server should be the same to avoid confusion in event notifications.
Redundancy Server Host Name	Enter a name to help you identify the Redundancy Server when receiving event notifications. **Note:** The **Redundancy Server Host Name** set in the Working Server and Redundancy Server should be the same to avoid confusion in event notifications.
Working Server IP Address	Automatically synchronize the network IP assigned to the Working Server within the SD-WAN network. 
Advanced	

Setting	Description
Heartbeat Interval (s)	Define the frequency to send heartbeat packets. The default value is 2 seconds, which means that the Redundancy Server sends packets every 2 seconds to detect whether the Working Server is alive or not.
Dead Time (s)	Define the maximum time interval before the Working Server responds to the Redundancy Server. The default value is 150 seconds. If the Redundancy Server receives no response after timeout, it will take over the telephony services automatically. **Note:** If you have set up Hot Standby, the value set here MUST be greater than the **Dead Time** in Hot Standby, with a minimum difference of 30 seconds.

4. Click **Save**.

   The system prompts that you need to reboot the PBXs to make disaster recovery take effect.

Result

After rebooting the PBXs, you can check the disaster recovery status on PBX web portal:

- On Working Server, the status is displayed as **Working**, indicating that the server is running to provide all PBX functions.

- On Redundancy Server, the status is displayed as **In Redundancy**, indicating that the server is in redundancy status. The Redundancy Server will now replicate data from the Working Server.

What to do next

Read Server Redundancy on SIP Trunks and WebRTC Trunks and Server Redundancy on SIP Devices and Linkus UC Clients to learn how server redundancy can be implemented on trunks and extension endpoints.

Server Redundancy on SIP Trunks and WebRTC Trunks

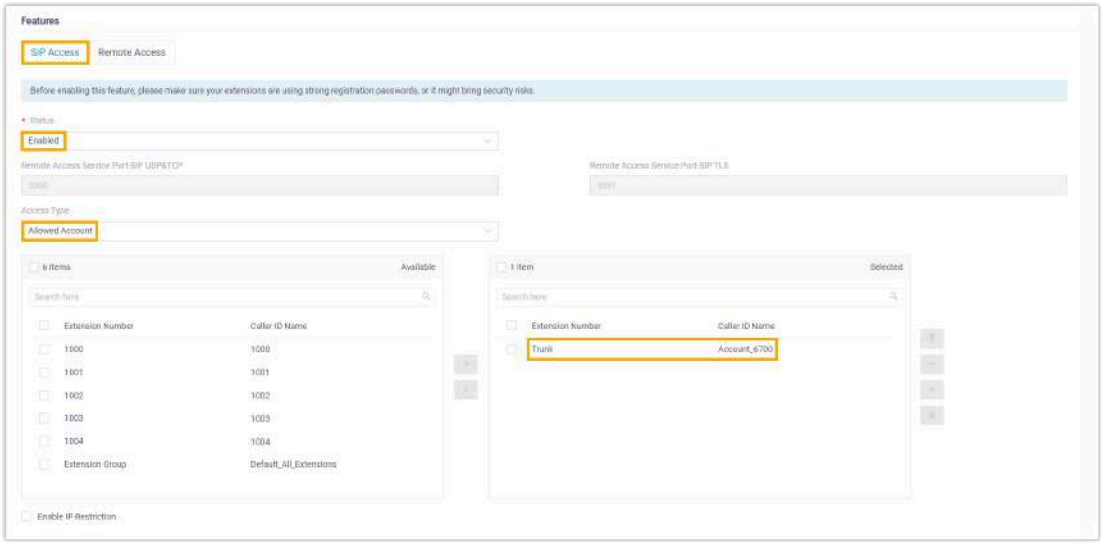
After setting up disaster recovery on Yeastar P-Series Software Edition, server redundancy can be implemented on SIP trunks and WebRTC trunks.

> **Note:**
> If you have extended physical trunks for Yeastar P-Series Software Edition, server redundancy will NOT be supported on these trunks.

Server redundancy on SIP account trunk

Yeastar Disaster Recovery implements server redundancy on SIP account trunks via **Yeastar FQDN**, which always points to the server in the disaster recovery pair that is in working status.
After you set up disaster recovery, server redundancy can be automatically implemented on the account trunks that meet both of the following criteria:

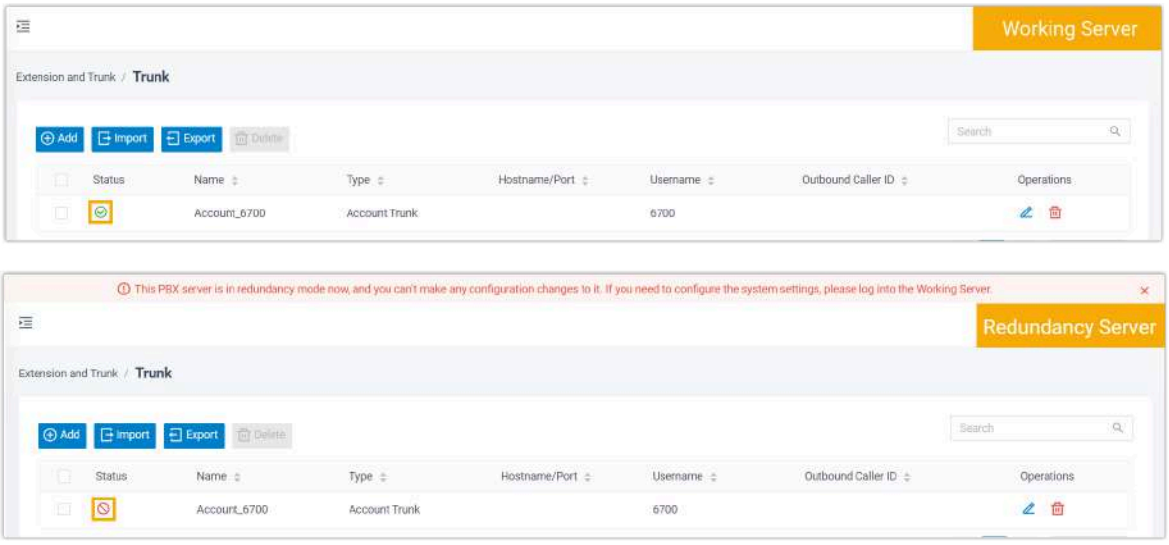
- The account trunk has been assigned the remote SIP access permission (Path: **System > Network > Yeastar FQDN > Features > SIP Access**).



- The account has been registered by the third-party software or device using Yeastar FQDN.

The account trunks that meet the above criteria are available regardless of which server is working, but the trunk status of the disaster recovery pair is different because only the server in working status can connect to the third-party software or device.

- When the Working Server works normally, the account trunk displays (**Registered**) on Working Server and displays (**Disabled**) on Redundancy Server.



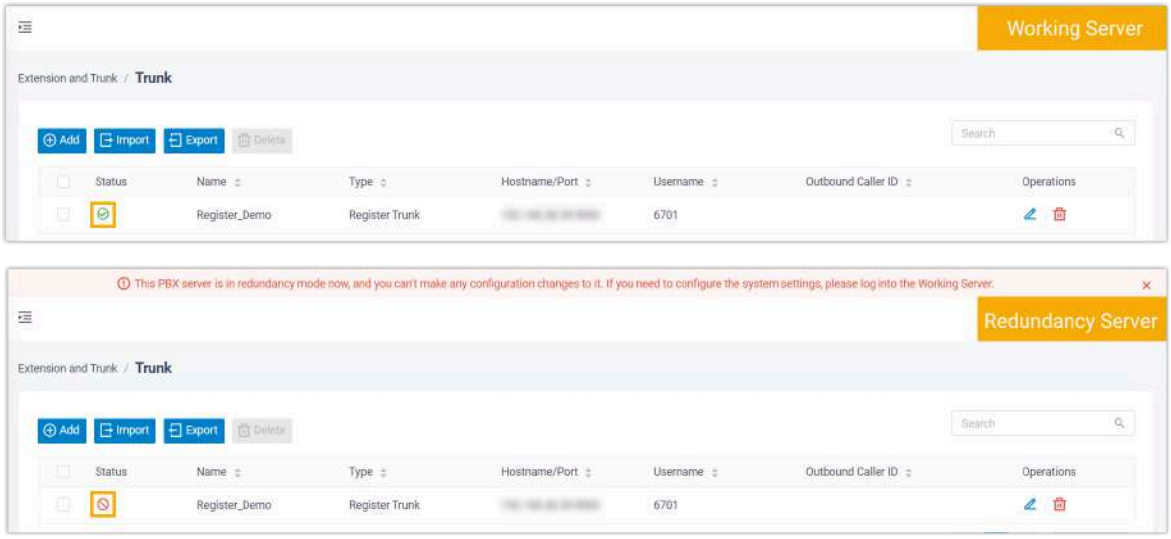
- When the Working Server goes down and the Redundancy Server takes over, the account trunk displays (**Registered**) on Redundancy Server.

Server redundancy on SIP register trunk

Yeastar Disaster Recovery automatically implements server redundancy on SIP register trunks, you don't need to perform any operations.

The register trunks are available regardless of which server is working, but the trunk status of the disaster recovery pair is different because only the server in working status can register with the ITSP (Internet Telephony Service Provider).

- When the Working Server works normally, the register trunk displays (**Registered**) on Working Server and displays (**Disabled**) on Redundancy Server.

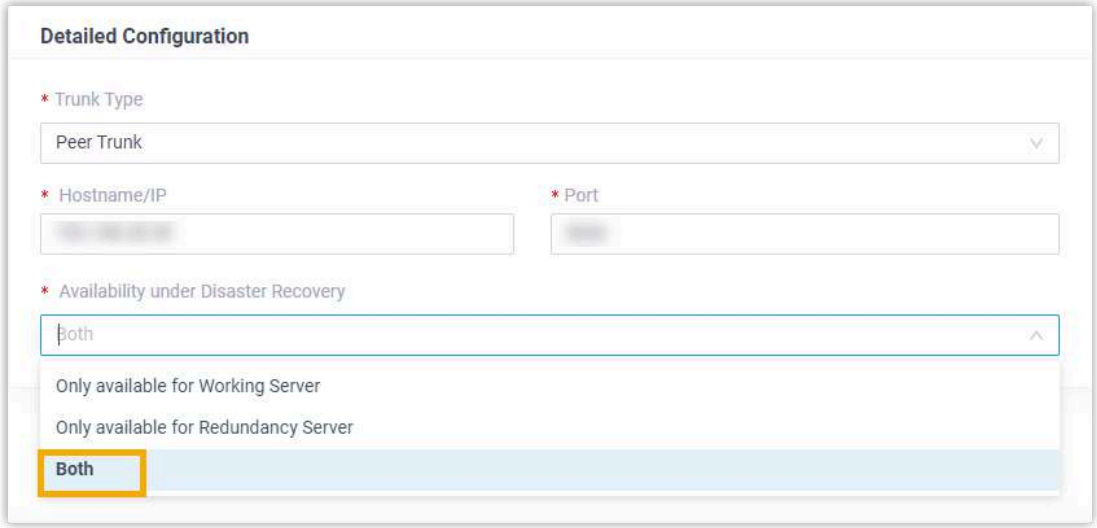


- When the Working Server goes down and the Redundancy Server takes over, the register trunk displays (**Registered**) on Redundancy Server.

Server redundancy on SIP peer trunk

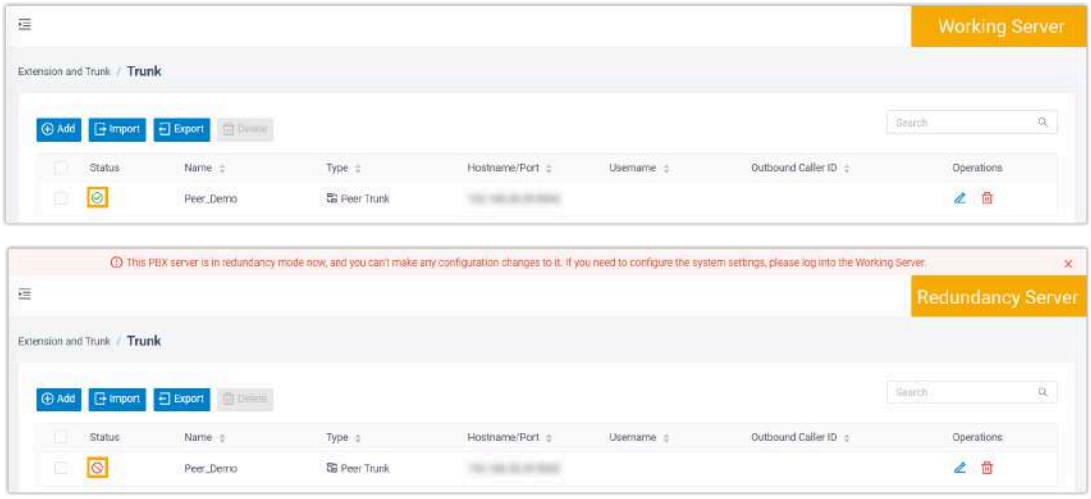
If the ITSP (Internet Telephony Service Provider) supports dual registration, server redundancy can be implemented on SIP peer trunks. To achieve this, you need to set the availability of SIP peer trunk as follows:

1. Go to **Extension and Trunk > Trunk**, edit the desired peer trunk.
2. In the **Detailed Configuration** section, select **Both** from the drop-down list of **Availability under Disaster Recovery**.



3. Click **Save** and **Apply**.
   The peer trunk is available regardless of which server is working, but the trunk status of the disaster recovery pair is different because only the server in working status can register with the ITSP.

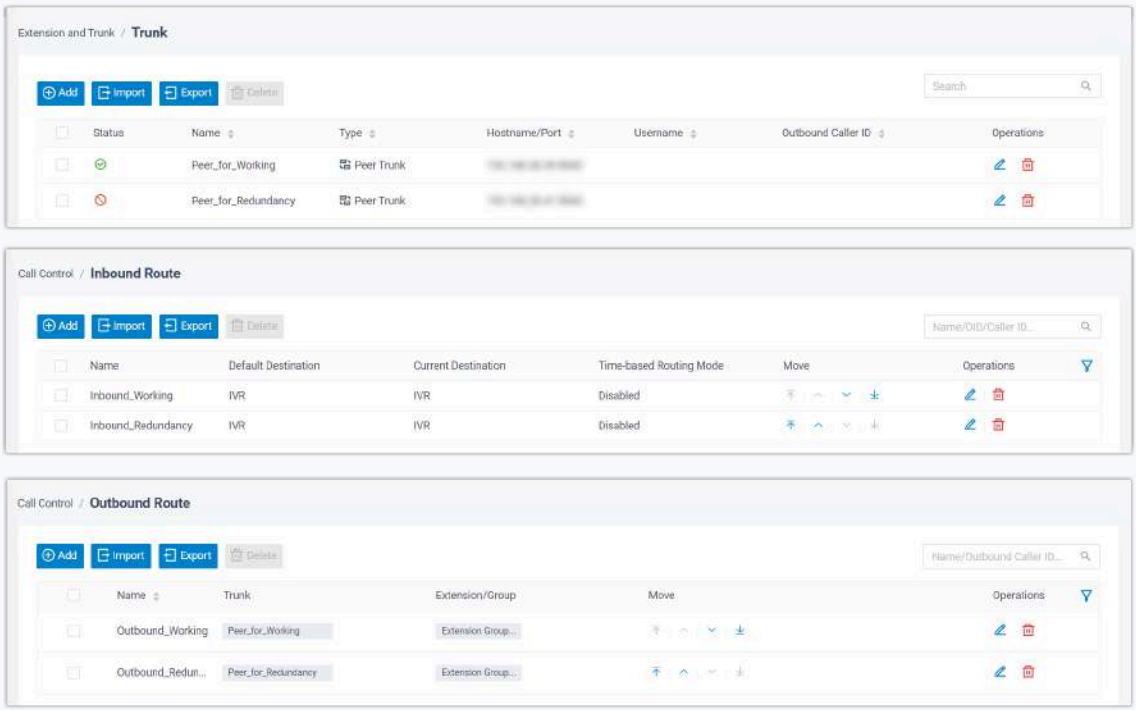
   - When the Working Server works normally, the peer trunk displays ✅ (**Reachable**) on Working Server and displays 🚫 (**Disabled**) on Redundancy Server.



- When the Working Server goes down and the Redundancy Server takes over, the peer trunk displays (**Reachable**) on Redundancy Server, and can be used for calls.

Note:
If the ITSP doesn't support dual registration, you can register both Working Server and Redundancy Server to the ITSP. In this way, extension users of Working Server can make and receive calls even if the Working Server goes down.

To achieve this, your need to create peer trunks on the Working Server to enable the disaster recovery pair to register to the ITSP. More importantly, set inbound routes and outbound routes to route calls through the trunks.



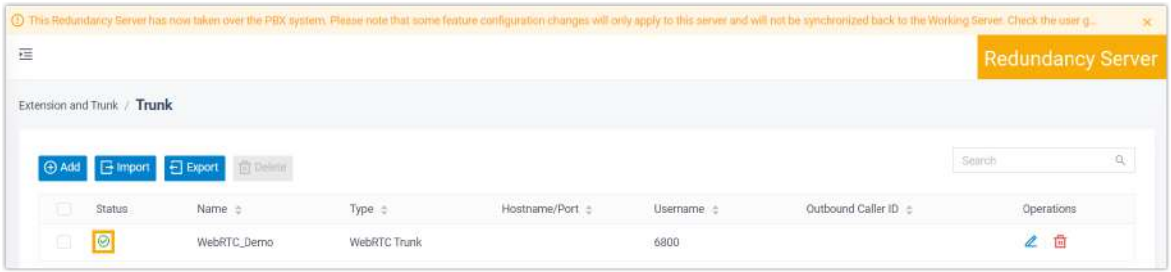
Server redundancy on WebRTC trunk

Yeastar Disaster Recovery implements server redundancy on WebRTC trunks via **Yeastar FQDN**, which always points to the server in the disaster recovery pair that is in working status.

As WebRTC trunks rely on Yeastar FQDN, so the sever redundancy is implemented automatically, you don't need to perform any operations. The WebRTC trunks are available regardless of which server is working, but the trunk status of the disaster recovery pair is different:

- When the Working Server works normally, the WebRTC trunk displays ✅ (**Available**) on Working Server and displays 🚫 (**Disabled**) on Redundancy Server.

- When the Working Server goes down and the Redundancy Server takes over, the Web-RTC trunk displays (**Available**) on Redundancy Server.



Server Redundancy (Yeastar SD-WAN) on SIP Devices and Linkus UC Clients

After setting up disaster recovery on Yeastar P-Series Software Edition, server redundancy can be implemented on **Auto Provisioned SIP Devices (IP phones and TA FXS gateways)** and **Linkus UC Clients**.

Server redundancy on IP phone

Yeastar Disaster Recovery implements server redundancy on auto provisioned IP phones via **LAN IP / Virtual IP** or **FQDN**, depending on whether Hot Standby is enabled on the Working Server and how you provision IP phones.

After you set up disaster recovery, the Yealink IP phones that have been provisioned will be automatically updated with the server information of the disaster recovery pair, as shown below.

Note:
To implement server redundancy on other IP phones that can be provisioned by Yeastar PBX, contact Yeastar Support.

Auto Provisioning Method	Description
PnP / DHCP	• **SIP Server 1**: The LAN IP (Hot Standby disabled) or the Virtual IP (Hot Standby enabled) of the Working Server. • **SIP Server 2**: The dedicated FQDN of the Working Server under disaster recovery, which always points to the Redundancy Server.
RPS FQDN	• **SIP Server 1**: The FQDN of the Working Server. In this scenario, IP phones register to PBX via FQDN, which always points to the server in the disaster recovery pair that is in working status.

Server redundancy on TA FXS gateway

Yeastar Disaster Recovery implements server redundancy on auto provisioned TA FXS gateways via **LAN IP / Virtual IP** and **FQDN**.

After you set up disaster recovery, you need to Reboot the auto provisioned gateways, so that they can obtain the server information of the disaster recovery pair, as shown below.

- **Hostname/IP**: The LAN IP (Hot Standby disabled) or the Virtual IP (Hot Standby enabled) of the Working Server.
- **Failover Hostname/IP**: The dedicated FQDN of the Working Server under disaster recovery, which always points to the Redundancy Server.

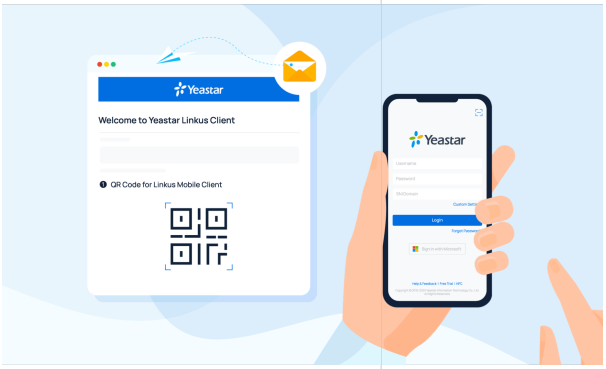
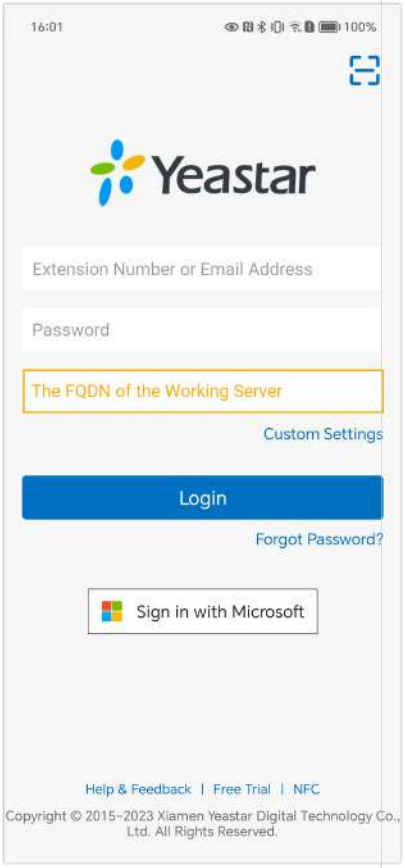
Server redundancy on Linkus Mobile Client

Yeastar Disaster Recovery implements server redundancy on Linkus Mobile Client via **Yeastar FQDN**, which always points to the server in the disaster recovery pair that is in working status.

After you set up disaster recovery, users need to log in again to Linkus Mobile Client via Yeastar FQDN, as shown below.

Note:
To achieve server redundancy, the version of Linkus Mobile Client must meet the following requirements:

- Linkus iOS Client: Version 5.2.9 or later
- Linkus Android Client: Version 4.13.16 or later

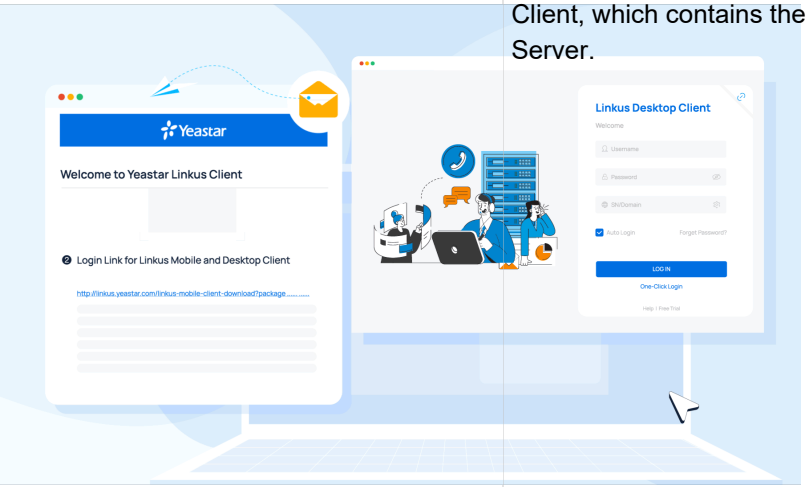
Scenario	Instruction
Figure 12. **Scan QR Code to log in** 	Scan the QR code to log in, which contains the FQDN of the Working Server.
Figure 13. **Log in using Domain Name** 	Manually replace the server information with the FQDN of the Working Server in the **SN/Domain** field.

Server redundancy on Linkus Desktop Client

Yeastar Disaster Recovery implements server redundancy on Linkus Desktop Client via **Yeastar FQDN**, which always points to the server in the disaster recovery pair that is in working status.

> **Note:**
> Server redundancy is NOT supported on Linkus Lite.

After you set up disaster recovery, users need to log in again to Linkus Desktop Client via FQDN, as shown below.

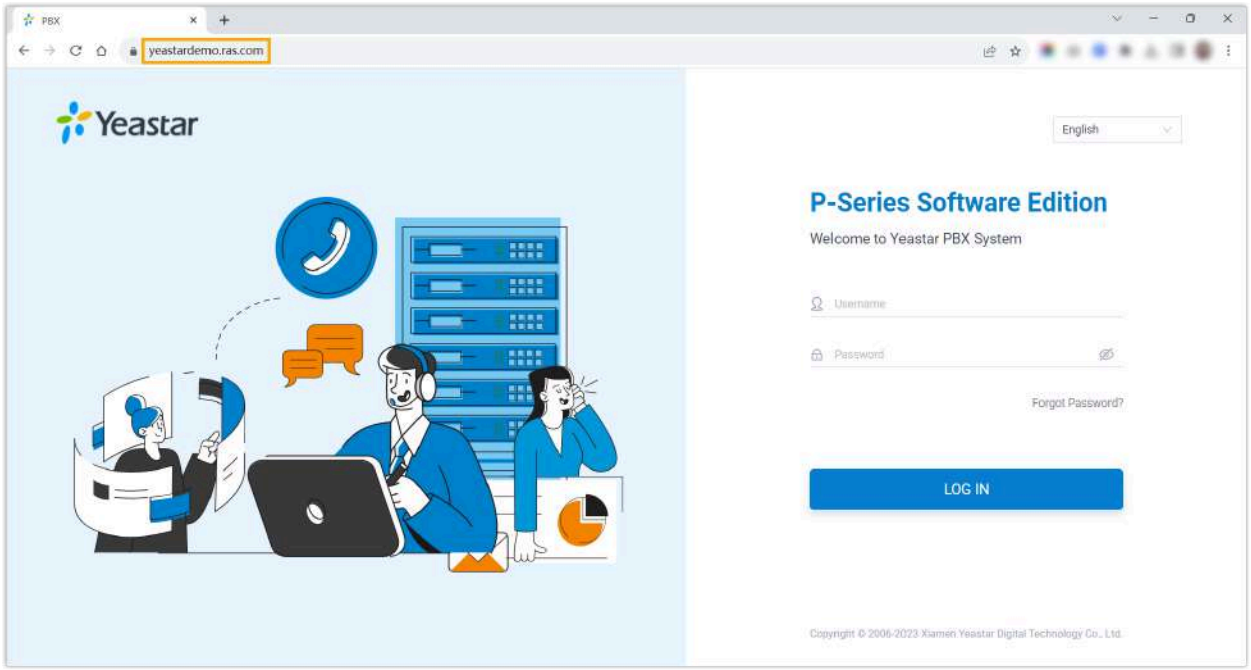
Scenario	Instruction
Figure 14. **Log in via Link** 	Paste the login link to log in to Linkus Desktop Client, which contains the FQDN of the Working Server.

Scenario	Instruction
Figure 15. **Log in using Domain Name** 	Manually replace the server information with the FQDN of the Working Server in the **Domain** field.

Server redundancy on Linkus Web Client

Yeastar Disaster Recovery implements server redundancy on Linkus Web Client via **Yeastar FQDN**, which always points to the server in the disaster recovery pair that is in working status.

After you set up disaster recovery, users need to access Linkus Web Client via the FQDN of the Working Server, as shown below.



Restricted Configurations and Functions on Redundancy Server after Takeover

When the Redundancy Server takes over, you and your users will still be able to access the PBX management portal and Linkus UC Clients, but some configurations and functions are unavailable. This topic provides an overview of the restricted configurations and functions on PBX management portal and Linkus UC Clients.

Platform	Restricted configurations and functions
PBX Management Portal	**Note:** If you have integrated the Working Server with third-party Collaboration Tools (**Active Directory (AD)**, **Microsoft 365**, **Microsoft Teams**, or **Microsoft Outlook**), the configurations and data will be synchronized to the Redundancy Server, but you can NOT make changes to the configurations and data on the Redundancy Server. **Unavailable Configurations**: • **CRM** • **Helpdesk** • **PMS**

<table>
<tr><th colspan="2">Platform</th><th>Restricted configurations and functions</th></tr>
<tr><td colspan="2"></td><td>Available but Out-of-sync Configurations:

Important:
The changes you made to the following configurations will NOT be synchronized back to the Working Server.

• Speech to Text
• AMI
• Database Grant
• Auto Provisioning</td></tr>
<tr><td rowspan="3">Linkus UC Clients</td><td>Linkus Mobile Client</td><td>All the functions are supported except Chat.

Note:
The version of Linkus Mobile Client must meet the following requirements:

• Linkus iOS Client: Version 5.2.9 or later
• Linkus Android Client: Version 4.13.16 or later</td></tr>
<tr><td>Linkus Desktop Client</td><td>All the functions are supported except the followings:

• Chat
• Video Conferencing
• Call Center Console
• Greeting Management (Path: Preferences > Voicemail > Greeting Management)</td></tr>
<tr><td>Linkus Web Client</td><td>All the functions are supported except the followings:

• Chat
• Video Conferencing
• Call Center Console
• Greeting Management (Path: Preferences > Voicemail > Greeting Management)</td></tr>
</table>

Working Server Resumes Telephony Services after Redundancy Server Took Over

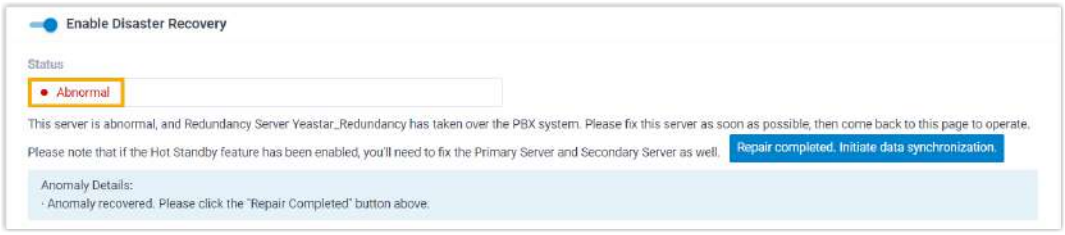
The Redundancy Server automatically takes over telephony services when the Working Server goes down. You need to resume the telephony services on Working Server after repairing.

Background information

When the Working Server fails and a fallback occurs, the system will send a **Disaster Recovery Fallback** event notification to relevant contacts, and update the Disaster Recovery status on PBX web portal as shown below.

Working Server

The Disaster Recovery status changes from **Working** to **Abnormal**, the page prompts that the Redundancy Server has taken over the PBX system and you need to repair the Working Server as soon as possible.



Redundancy Server

The Disaster Recovery status changes from **In Redundancy** to **Working**, the page prompts that the Redundancy Server has taken over the PBX system and you need to repair the Working Server as soon as possible.

After you repair the Working Server, you need to manually set up the Working Server to resume service.

Procedure

Important:

> Make sure there is no call in progress on the Redundancy Server, or the call will be dropped.

1. Log in to the PBX web portal of Working Server, go to **System > High Availability > Disaster Recovery**.
2. Click **Repair completed. Initiate data synchronization.**.

   The Disaster Recovery status of Working Server becomes **Recovering Data**, indicating that the server starts to synchronize data from the Redundancy Server.

   After data synchronization is completed, the Disaster Recovery status will change to **Data Recovered**, and relevant contacts of both servers will receive a **Working Server Data Restoration Completed** event notification.
3. Click **Take Over**.

4. In the pop-up window, click **OK**.

Result

- The **Status** of the Working Server changes to **Working**, indicating that the Working Server has resumed the telephony services.
- The Redundancy Server returns to the redundancy status.

Enable and Schedule Maintenance Mode on Redundancy Server

When Working Server is under maintenance (e.g. firmware upgrade or system reboot), it may fail to respond to heartbeat packets from Redundancy Server, which would trigger an

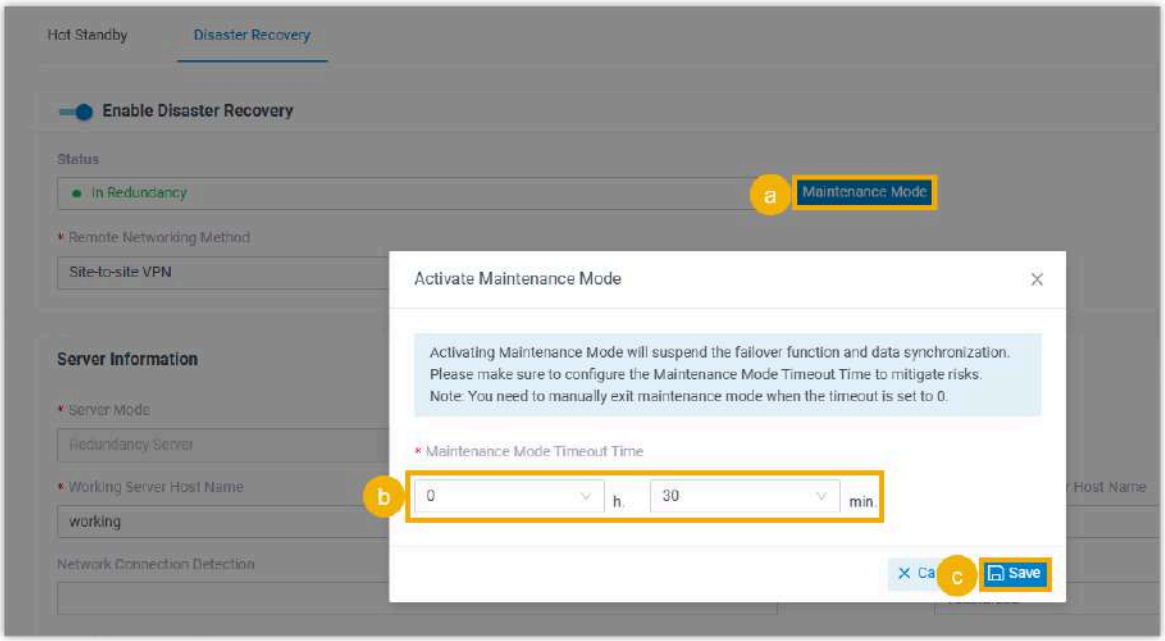
unexpected fallback. To avoid this, you can enable and schedule Maintenance Mode on the Redundancy Server to temporarily suspend health monitoring and prevent fallback during the maintenance window.

Requirements

The firmware version of Redundancy Server is 83.19.0.70 or later.

Procedure

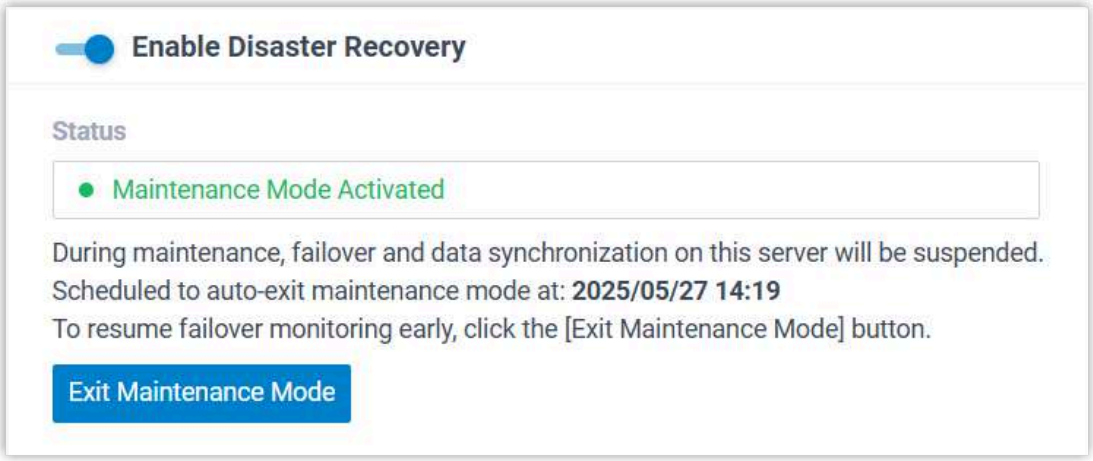
1. Log in to the web portal of Redundancy Server, go to **System > High Availability > Disaster Recovery**.
2. Enable and schedule maintenance mode.



   a. Click **Maintenance Mode**.
   b. In the **Maintenance Mode Timeout Time** drop-down list, set the timeout.
   c. Click **Save**.

Result

- The status displays **Maintenance Mode Activated**. During the maintenance window, telephony service fallback and data replication are suspended.



- When the maintenance timeout is reached, the Redundancy Server will automatically exit Maintenance Mode and resume fallback monitoring and data replication.

> **Note:**
> - If the timeout is set to 0, you must click **Exit Maintenance Mode** to manually exit when the Working Server is ready.
> - If a specific timeout is set, you can also exit manually in advance.

SD-WAN PBX Networking

Yeastar SD-WAN PBX Networking Overview

Yeastar SD-WAN PBX Networking leverages SD-WAN technology to build a secure and reliable Wide Area Network (WAN), without the need for dedicated lines or public IP addresses. It connects Yeastar P-Series Software Editions in different geographic locations and enhances the connectivity by intelligently routing traffic based on real-time network conditions, thus ensuring that users can access critical telephony services in the event of disaster.

What is SD-WAN?

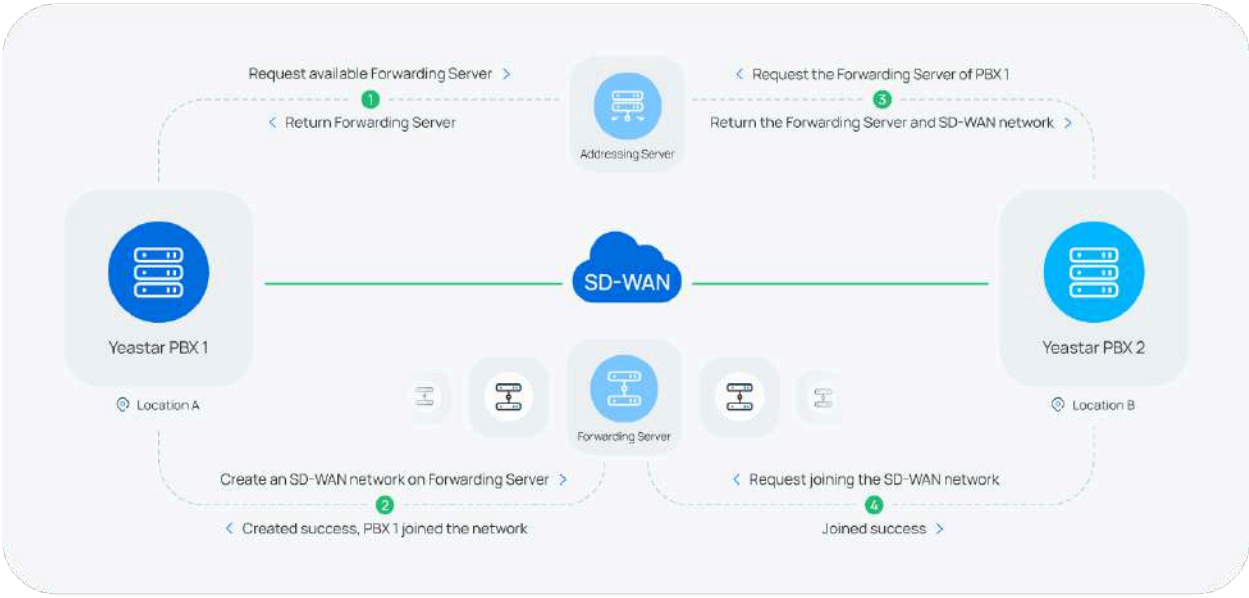
SD-WAN is a modern network architecture that provides flexible, secure, and efficient network connectivity, which can be used to create virtual connections between remote sites. Organizations can connect devices and networks across multiple locations through SD-WAN. In SD-WAN remote connection, each node is connected to the SD-WAN cloud control center, which can centrally manage and control all nodes. When a node needs to commu-

nicate with other nodes, the control center selects the best communication path based on proximity, network bandwidth, latency, and other factors, thus ensuring fast and secure data transmission.

How does SD-WAN enable Yeastar PBX Networking?

SD-WAN features plug-and-play and automated deployment to easily achieve multipoint remote network connection. All you need to do is to create an SD-WAN network on one Yeastar P-Series Software Edition, and join the network on another Yeastar P-Series Software Edition at the remote site, SD-WAN will automatically build the network using the **Addressing Server** and **Forwarding Server** hosted by Yeastar.

We provide a typology to help you better understand how Yeastar PBX networking is established using SD-WAN.



How to set up Yeastar SD-WAN PBX Networking and implement cross-region disaster recovery?

Yeastar PBX Networking with SD-WAN makes it possible to implement cross-region disaster recovery in case of regional service interruption. With the SD-WAN PBX networking and disaster recovery in place, if local server fails, traffic can be automatically re-routed to a remote server, ensuring the continuous availability of telephony services and minimizing downtime.

To achieve this, follow the instructions below:

Preparations

1. Prepare two Yeastar P-Series Software Editions as a disaster recovery pair and decide the role that they will play.

   One server will work as the **Working Server**, responsible for handling calls and providing all PBX functions, while the other server will serve as the **Redundancy Server**, working only when the **Working Server** fails.
2. Ensure both servers meet the requirements listed below.

> **Note:**
> If you already have a PBX, provide your service provider with the PBX SN to purchase another license for Redundancy Server. If you don't have a PBX, contact your service provider to purchase two licenses for the disaster recovery pair.

Item	Requirement
Product Model	Yeastar P-Series Software Edition
Plan	Ultimate Plan
Version	Same firmware version and must be 83.12.0.57 or later.
Network	• LAN port as the default Ethernet interface and a static IP address is required. • Accessible to Yeastar SD-WAN node (sdwantunnel.yeastar.com).
External Storage	Identical storage device settings and mounting points.

Step 1. Connect two Yeastar P-Series Software Editions using SD-WAN

Create an SD-WAN network on the **Working Server**, then join the SD-WAN network on the **Redundancy Server**.

For more information, see Set up SD-WAN Network on Working Server and Join SD-WAN Network on Redundancy Server.

Step 2. Enable and set up disaster recovery

Enable and set up disaster recovery on both **Working Server** and **Redundancy Server**.

For more information, see Set up Disaster Recovery (Yeastar SD-WAN).

Set up SD-WAN PBX Networking

Set up SD-WAN Network on Working Server

In a cross-region disaster recovery scenario, you can create an SD-WAN network on the Working Server and invite the Redundancy Server at a remote site to join the network. With disaster recovery in place, the Redundancy Server can replicate telephony data from Working Server and take over telephony services if the Working Server goes down.

Requirements and restrictions

Requirements

Both servers in a disaster recovery pair must meet the following requirements:

Item	Requirement
Product Model	Yeastar P-Series Software Edition
Plan	Ultimate Plan
Version	Same firmware version and must be 83.12.0.57 or later.
Network	• LAN port as the default Ethernet interface and a static IP address is required. • Accessible to Yeastar SD-WAN node (sdwantunnel.yeastar.com).
External Storage	Identical storage device settings and mounting points.

Restrictions

Item	Quantity
Max. SD-WAN network that can create or join (per PBX)	1
Max. redundancy member	1

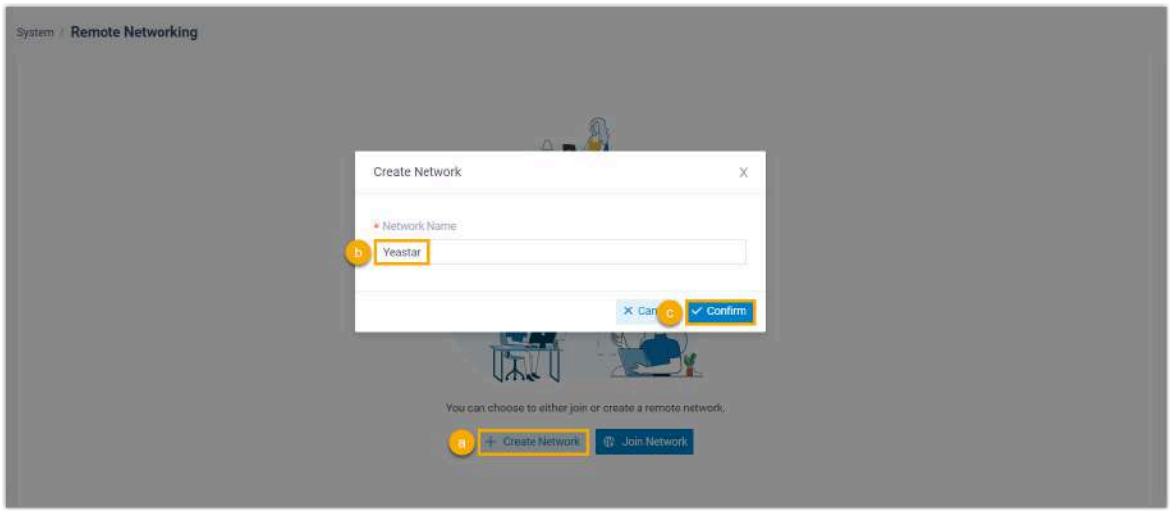
Prerequisites

- Contact your service provider for the Serial Number (SN) of the Redundancy Server.
- (Optional) Set up an email server if you want to share SD-WAN networking credential or send SD-WAN networking event notifications via email (Path: **System > Email > Email Server**).

For more information, see Email Server Overview.

Step 1. Create an SD-WAN network

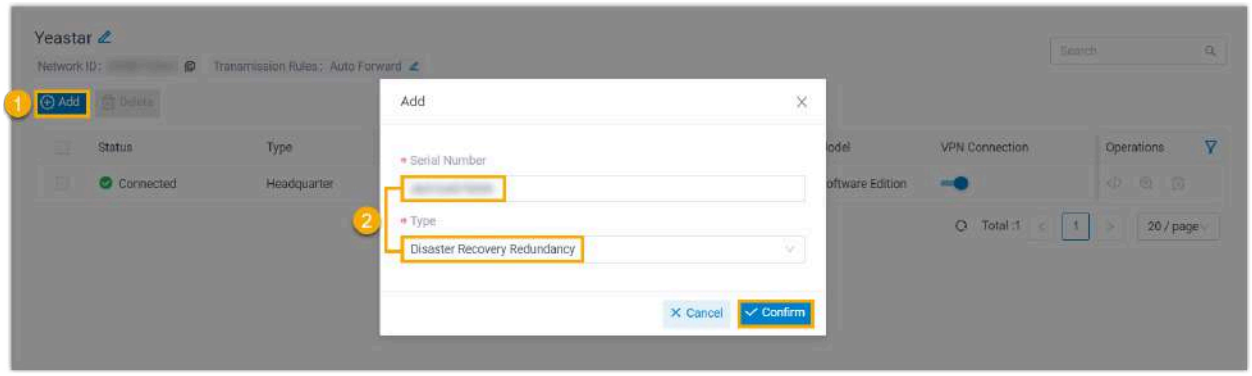
1. Log in to PBX web portal, go to **System > SD-WAN PBX Networking**.
2. Create an SD-WAN network.



   a. Click **Create Network**.
   b. In the **Network Name** field, enter a name to help you identify the network.
   c. Click **Confirm**.

An SD-WAN network is created; The Working Server has automatically joined and connected to the network, with the type displayed as **Headquarter**.

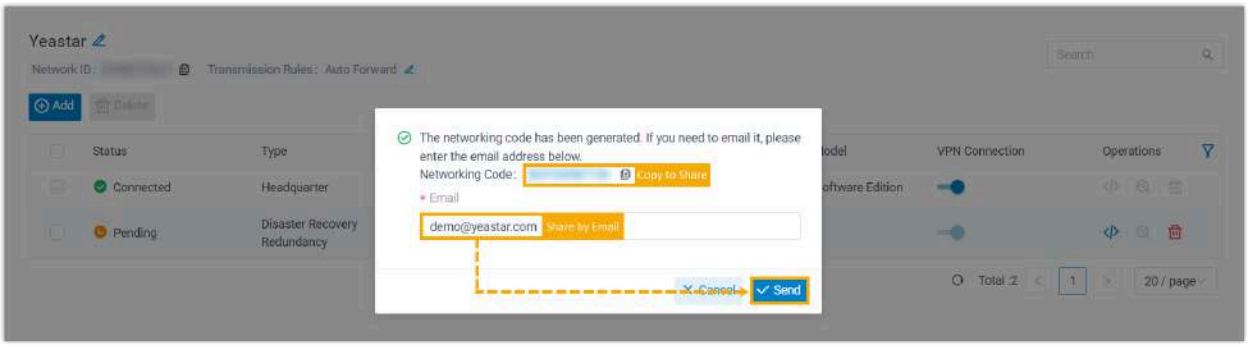
Step 2. Add Redundancy Server to the SD-WAN network



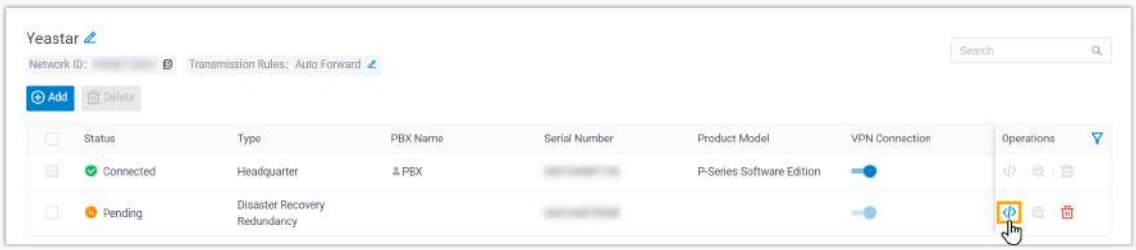
1. At the top-left corner, click **Add**.
2. In the pop-up window, configure the following settings, then click **Confirm**.
   - **Serial Number**: Enter the SN of the Redundancy Server.
   - **Type**: Select **Disaster Recovery Redundancy**.

The Redundancy Server is added to the list and a networking code (actually the SN of the Working Server) has been generated. You need to enter the networking code on the Redundancy Server so that it can connect to the SD-WAN network. You can click to copy the code and send it to the desired recipient, or share it by email.

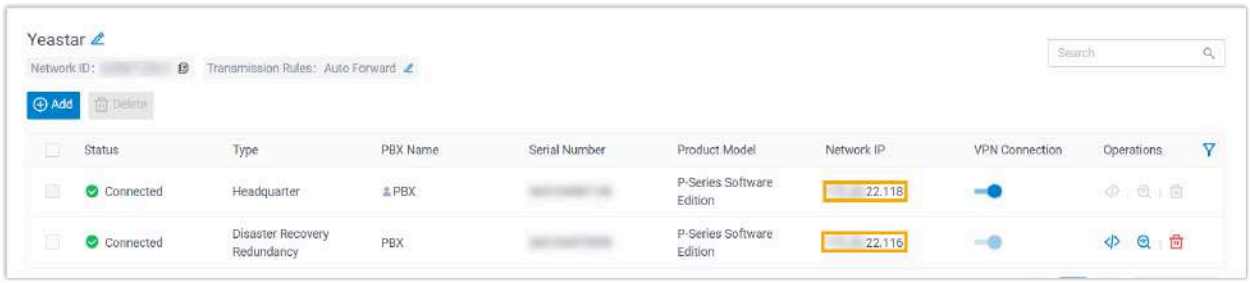
Note:
For more information about how the Redundancy Server can join the SD-WAN network using the code, see Join SD-WAN Network on Redundancy Server.



Tip:
To access the networking code after closing the window, click beside the Redundancy Server to check and share it again.

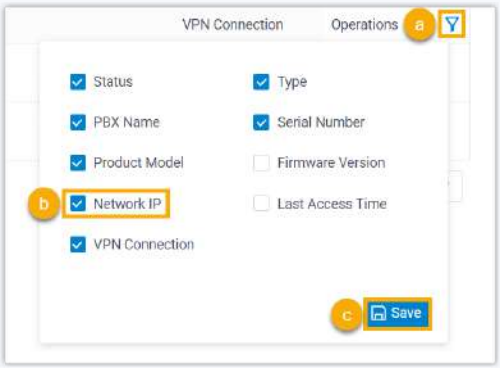


After the Redundancy Server joins the SD-WAN network, the specified contacts of both servers will receive a **SD-WAN Network Joined Successfully** event notification; Both servers have been assigned network IPs, which allow them to communicate with each other over the SD-WAN network.



Tip:

By default, the network IPs are hidden on the list. You can click at the top-right corner to set the **Network IP** column to display.



Related information

[Change Transmission Rule of SD-WAN Network]
[Test Network Connectivity between Two Servers in SD-WAN Network]
[Remove Redundancy Server from SD-WAN Network]
[Disconnect from SD-WAN Network]

Exit SD-WAN Network

Join SD-WAN Network on Redundancy Server

In a cross-region disaster recovery scenario, a Redundancy Server can join the SD-WAN network created by the Working Server. With disaster recovery in place, the Redundancy Server can replicate telephony data from Working Server and take over telephony services if the Working Server goes down.

Requirements and restrictions

Requirements

Both servers in a disaster recovery pair must meet the following requirements:

Item	Requirement
Product Model	Yeastar P-Series Software Edition
Plan	Ultimate Plan
Version	Same firmware version and must be 83.12.0.57 or later.
Network	• LAN port as the default Ethernet interface and a static IP address is required. • Accessible to Yeastar SD-WAN node (sdwantunnel.yeastar.com).
External Storage	Identical storage device settings and mounting points.

Restrictions

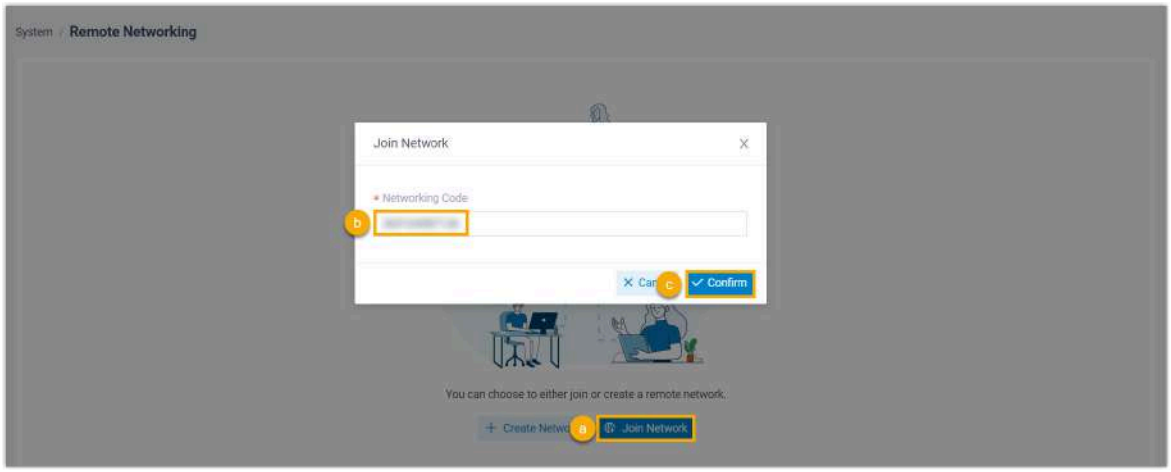
Item	Quantity
Max. SD-WAN network that can create or join (per PBX)	1

Prerequisites

You have received the networking code generated by the Working Server.

Procedure

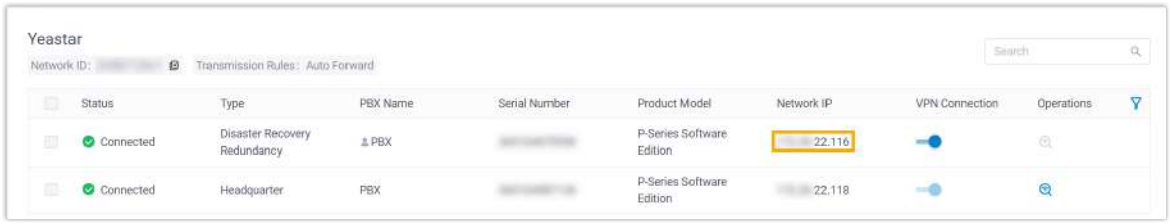
1. Log in to PBX web portal, go to **System > SD-WAN PBX Networking**.
2. Join an SD-WAN network.



a. Click **Join Network**.
b. In the **Networking Code** field, enter the networking code.
c. Click **Confirm**.

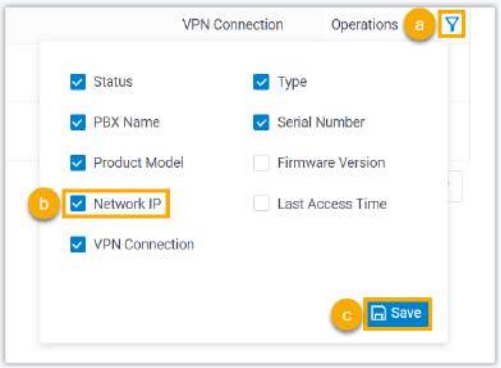
Result

- The Redundancy Server has joined and connected to the SD-WAN network, with the **Type** displayed as **Disaster Recovery Redundancy**.
- The Redundancy Server has been assigned a network IP through which it can communicate with the Working Server over the SD-WAN network.



Note:

- By default, the network IP is hidden on the list. You can click at the top-right corner to set the **Network IP** column to display.



- The network IP of the Working Server is also displayed, you can ping the IP address to test connectivity. For more information, see Test Network Connectivity between Two Servers in SD-WAN Network.

- The specified contacts of both servers will receive a **SD-WAN Network Joined Successfully** event notification.

Related information

Disconnect from SD-WAN Network
Exit SD-WAN Network

Manage SD-WAN PBX Networking

Change Transmission Rule of SD-WAN Network

In Yeastar SD-WAN network, traffic is automatically routed based on network conditions of the servers in the SD-WAN network. If necessary, you can change the transmission rule on the Working Server to force traffic to a preferred path.

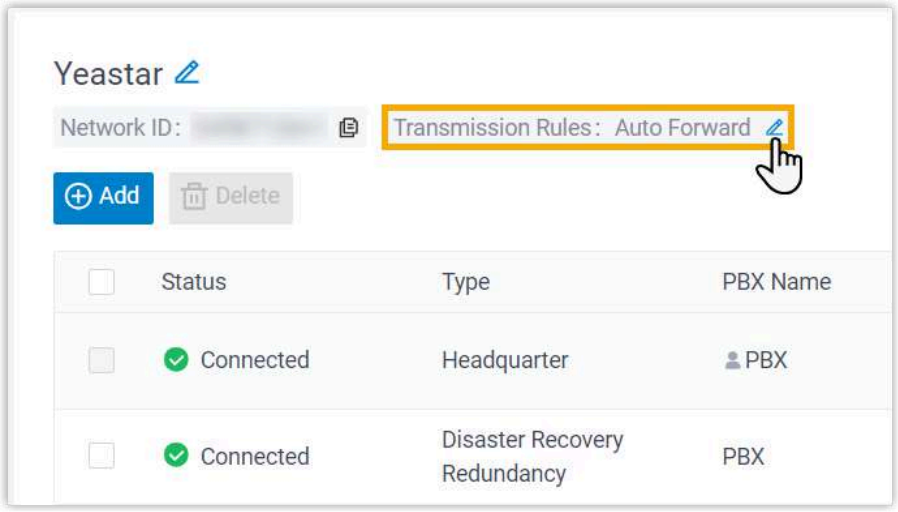
Background information

Yeastar SD-WAN PBX networking supports the following two transmission rules:

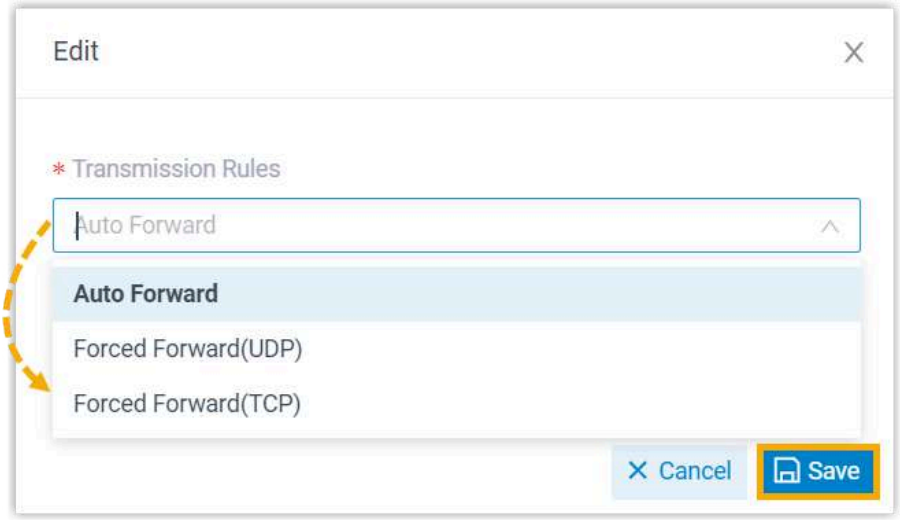
- **Auto Forward**: Intelligently choose between Peer-to-Peer (P2P) and Forwarding based on network conditions of the servers in the SD-WAN network to optimize traffic routing. When the servers are in good network condition, P2P is utilized for direct communication. Otherwise, traffic will be redirected through a dedicated Forwarding Server.
- **Forced Forward**: Prioritize and redirect TCP or UDP traffic through a dedicated Forwarding Server, this helps avoid potential network latency and slow data transmission when using **Auto Forward**, ensuring the delivery of critical data.

Procedure

1. Log in to the PBX web portal of the Working Server, go to **System > SD-WAN PBX Networking**.
2. At the top-left corner, click beside **Transmission Rules**.



3. In the pop-up window, select a transmission rule and click **Save**.

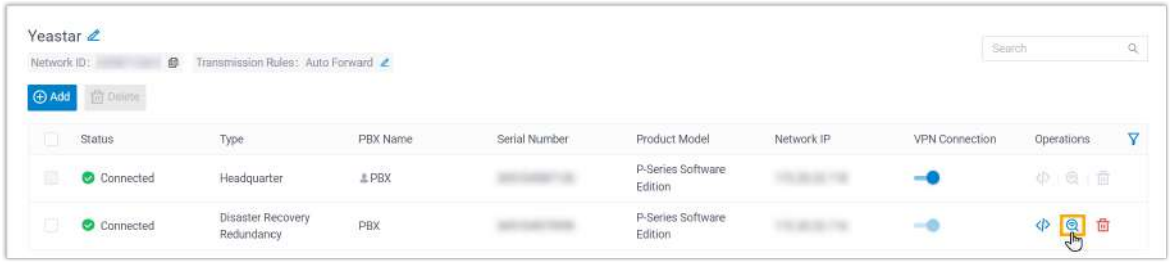


Test Network Connectivity between Two Servers in SD-WAN Network

After setting up or joining an SD-WAN network, you can ping the network IP of the other Yeastar P-Series Software Edition to test the connectivity.

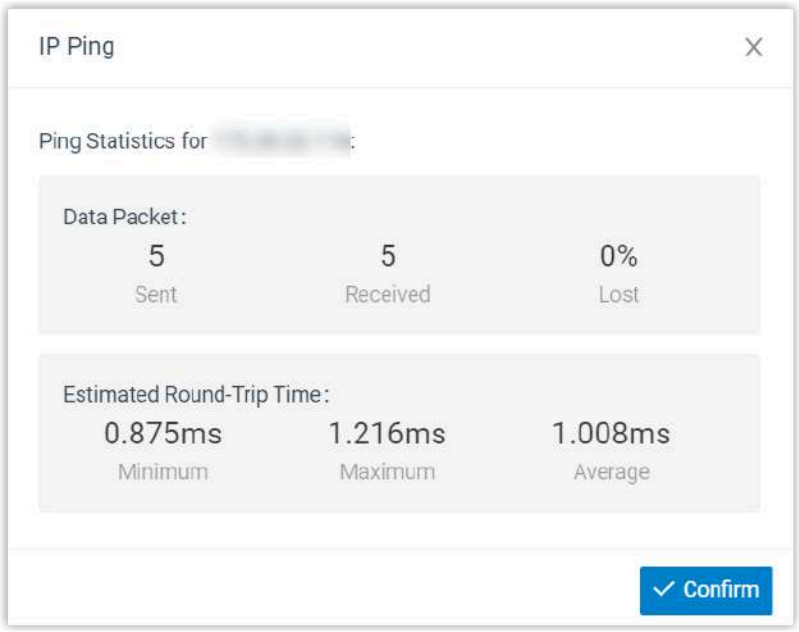
Procedure

1. Log in to PBX web portal, go to **System > SD-WAN PBX Networking**.
2. In the **Operations** column of the other server, click to ping the network IP.



Result

The network test result is displayed in the pop-up window.

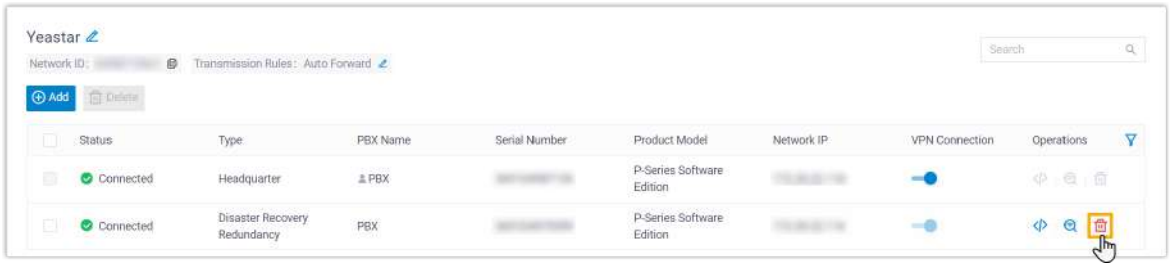


Remove Redundancy Server from SD-WAN Network

In some cases such as you want to replace the redundancy member in the SD-WAN network, you can remove the existing one on the Working Server.

Procedure

1. Log in to the PBX web portal of the Working Server, go to **System > SD-WAN PBX Networking**.
2. Click beside the Redundancy Server.



3. In the pop-up window, click **OK**.

Result

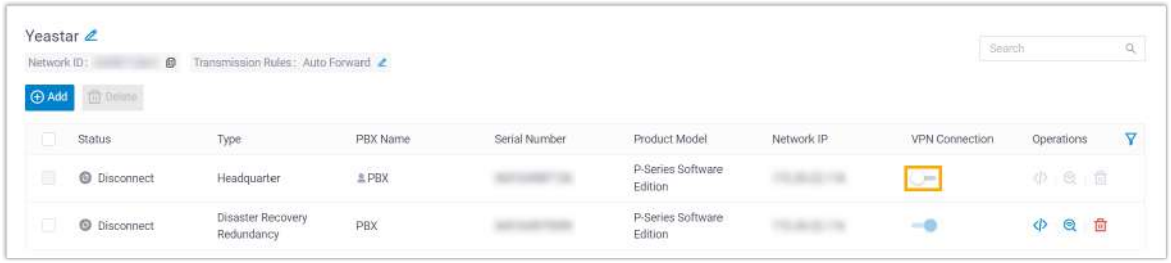
- The Redundancy Server is removed from the SD-WAN network.
- The specified contacts of both servers will receive a **SD-WAN Network Disconnected** event notification.

Disconnect from SD-WAN Network

In some cases, such as when there are network problems, you can pause the VPN connection from either Working Server or Redundancy Server to troubleshoot.

Procedure

1. Log in to PBX web portal, go to **System > SD-WAN PBX Networking**.
2. In the **VPN Connection** column of the server, turn off the switch.



Result

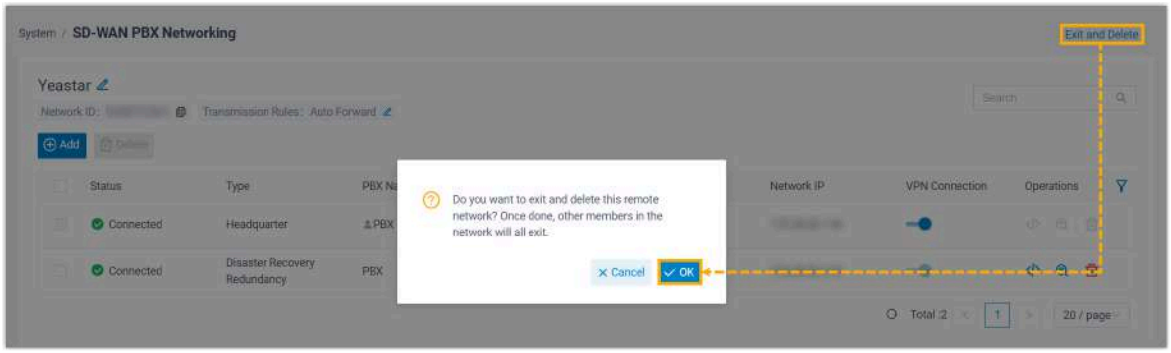
- The server is disconnected from the SD-WAN network, with status displayed as **Disconnected**.
- The specified contacts of both servers will receive a **SD-WAN Network Disconnected** event notification.

Exit SD-WAN Network

In some cases, such as when you don't need the SD-WAN network or want to replace the redundancy member, you can exit the SD-WAN network on Working Server or Redundancy Server.

Exit SD-WAN network for both Working Server and Redundancy Server

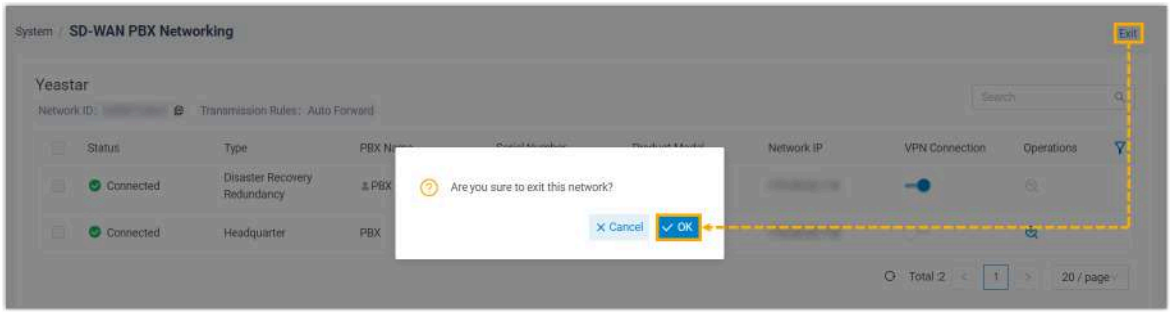
1. Log in to the PBX web portal of the Working Server, go to **System > SD-WAN PBX Networking**.
2. At the top-right corner, click **Exit and Delete**, then click **OK** in the pop-up window.



Both Working Server and Redundancy Server exit the SD-WAN network, and the SD-WAN network is deleted. The specified contacts of both servers will receive a **SD-WAN Network Exited** event notification.

Exit SD-WAN network for Redundancy Server

1. Log in to the PBX web portal of the Redundancy Server, go to **System > SD-WAN PBX Networking**.
2. At the top-right corner, click **Exit**, then click **OK** in the pop-up window.



The Redundancy Server exits from the SD-WAN network; The specified contacts of both servers will receive **SD-WAN Network Exited** event notification.

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 can control and filter traffic sent to the PBX based on IP address, domain, or MAC address.

Yeastar P-Series Software Edition has default static defense rules to accept connections from devices on local network, auto provisioned devices, and Yeastar servers. You can also set up new rules to accept, drop, or reject access to the PBX. The IP addresses that are denied access to the PBX would be blocked when trying to connect to the PBX, you can check the blocked IP address in **Block IPs**.

For more information, see Add a Static Defense Rule and Manage Blocked IP Addresses.

Auto defense

Auto defense rules can control and filter traffic sent to the PBX based on the frequency of packets sent, effectively preventing massive connection attempts or brute force attacks.

Yeastar P-Series Software Edition has default auto defense rules to protect SSH connection, SIP registration, and Web access. You can also set up new rules according to your needs. When a source address sends packets over the limit within the specified time period, the PBX will block the source address, you can check the blocked IP address in **Block IPs**.

For more information, see Add an Auto Defense Rule and Manage Blocked IP Addresses.

Blocked IPs

The blocked IP addresses would be listed in the **Blocked IPs**. If a trusted IP address was blocked, you can go to **Blocked IPs** to delete the IP address.

For more information, see Manage Blocked IP Addresses.

Outbound Call Frequency Restriction

Outbound Call Frequency Restriction rule is used to limit the number of outbound calls over specified time period.

The PBX has a default rule to limit extension users to make maximum 5 outbound calls in 1 second.

You can also set up new rules according to your needs. For more information, see Add an 'Outbound Call Frequency Restriction' Rule.

Security options

The PBX provides additional options so that you can flexibly adjust your security scheme:

Disable Auto Defense

If the option is enabled, the auto defense feature will not work.

Disable Extension Registration Defense

If the option is enabled, the SIP security settings will not work.

Drop All but Accepted IPs in Static Defense

If the option is enabled, the PBX will drop all the packets and connections from other hosts except the accepted addresses defined in static defense rules.

> **Note:**
> We recommend that you create a backup on the PBX before you enable the feature.

Drop IP Ping Request

If the option is enabled, the PBX will disable Ping response (ICMP echo).

Download Global Anti-hacking IP Blocklist

If the option is enabled, Yeastar Global Anti-hacking IP Blocklist will be downloaded to the PBX. Any connections from the IP addresses in the blocklist will be dropped.

Report PBX's IP Blocklist

If the option is enabled, the IP addresses that are permanently blocked by the PBX will be reported to Yeastar Global Anti-hacking IP Blocklist.

Two-Factor Authentication

Yeastar P-Series Software Edition supports to set two-factor authentication for super administrator account to ensure login security.

For more information, see Two-factor Authentication (2FA) Overview.

Enable IP Restriction for Administrator Login

Yeastar P-Series Software Edition supports to add IP restrictions to specify the IP addresses from which super administrator are allowed to access administrator portal.

For more information, see Restrict Access to Administrator Portal by IP Addresses.

Console/SSH Access

Yeastar P-Series 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, or directly apply for a certificate on the PBX.

For more information, see the following topics:

- Manage TLS certificates on the PBX
- Manage HTTPS Certificates on the PBX

Allowed Country IPs

You can set up **Allowed Country IPs** to only allow specific countries or regions to access your phone system, thus preventing the situations that hackers remotely access your phone system to make international and long-distance calls, monitor conversations, or do other operations that may cause security threats to your phone system.

For more information, see Restrict Specific Countries or Regions from Accessing Yeastar P-Series 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.

Global Anti-hacking IP Blocklist Program

Download Yeastar Global Anti-hacking IP Blocklist

Yeastar Global Anti-hacking IP Blocklist is a central database of IP addresses that have been blocked by Yeastar PBX systems worldwide or that are suspected of malicious activity or attack. After downloading Yeastar Global Anti-hacking IP Blocklist, any connections to your PBX from the IP addresses in the blocklist will be dropped, reducing the risk of cyber attacks.

Procedure

1. Log in to PBX web portal, go to **Security > Security Settings**.
2. Click **Security Options** tab.
3. In the **Join Global Anti-hacking IP Blocklist Program** section, select the checkbox of **Download Global Anti-hacking IP Blocklist**.
4. Click **Save**.

Result

The IP blocklist is downloaded to the PBX; Any connections from the IP addresses in the blocklist will be dropped.

> **Note:**
> The IP blocklist will be automatically updated every 7 days to obtain the latest blocked IPs from Yeastar.

Report PBX's IP Blocklist to Yeastar Global Anti-hacking IP Blocklist

Yeastar Global Anti-hacking IP Blocklist is a central database of IP addresses that have been blocked by Yeastar PBX systems worldwide or that are suspected of malicious activity or attack. If you would like to contribute to the IP blocklist, you can share with Yeastar by reporting your system's IP blocklist. Yeastar security team will evaluate and analyze the reported addresses to ensure that only the malicious ones are added to the global blocklist.

Procedure

1. Log in to PBX web portal, go to **Security > Security Settings**.
2. Click **Security Options** tab.
3. In the **Join Global Anti-hacking IP Blocklist Program** section, select the checkbox of **Report PBX's IP Blocklist**.
4. Click **Save**.

Result

Permanent IP Blocklist of the PBX will be reported to Yeastar Global Anti-hacking IP Blocklist daily.

Note:

- Permanent IP Blocklist indicates the IP addresses on **Security > Security Rules > Blocked IPs**, which meet both of the following requirements:
  - **Block Type**: Block IP
  - **Expiration Date**: 12/30/2099 23:59:59
- To avoid legitimate VoIP servers or carriers being blocked, Yeastar security team will evaluate and analyze the IP addresses reported, then add the malicious ones to the global blocklist. The newly added IP addresses will be shared with all the users participating in the Yeastar Global Anti-hacking IP Blocklist Program.

Static Defense

Add a Static Defense Rule

Static defense rules are used to control and filter traffic sent to Yeastar P-Series 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

Restrict Administrator Login

Restrict Access to Administrator Portal by IP Addresses

As a super administrator, you can add IP restrictions to specify the IP addresses from which super administrator are allowed to access administrator portal.

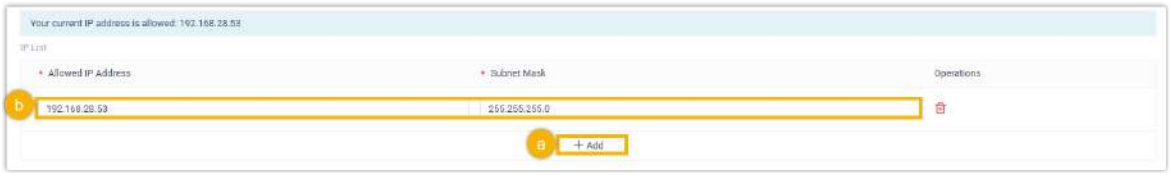
Requirements

The firmware version of PBX server is 83.16.0.70 or later.

Procedure

1. Log in to PBX administrator portal, go to **Security > Security Settings > Security Options**.
2. Turn on the option **Enable IP Restriction for Administrator Login**.

   You are prompted that your current IP address is not allowed to log in to administrator portal.
3. Add one or more IPs.



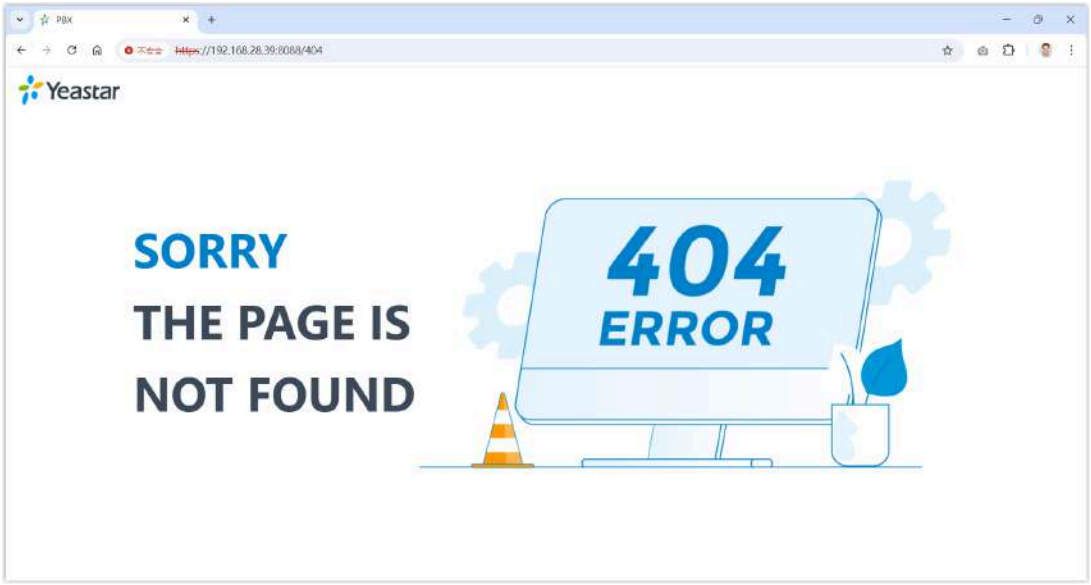
a. Click **Add**.
b. Enter the allowed IP address and the subnet mask.

> **Note:**
> The maximum number of allowed IP rule is 10.

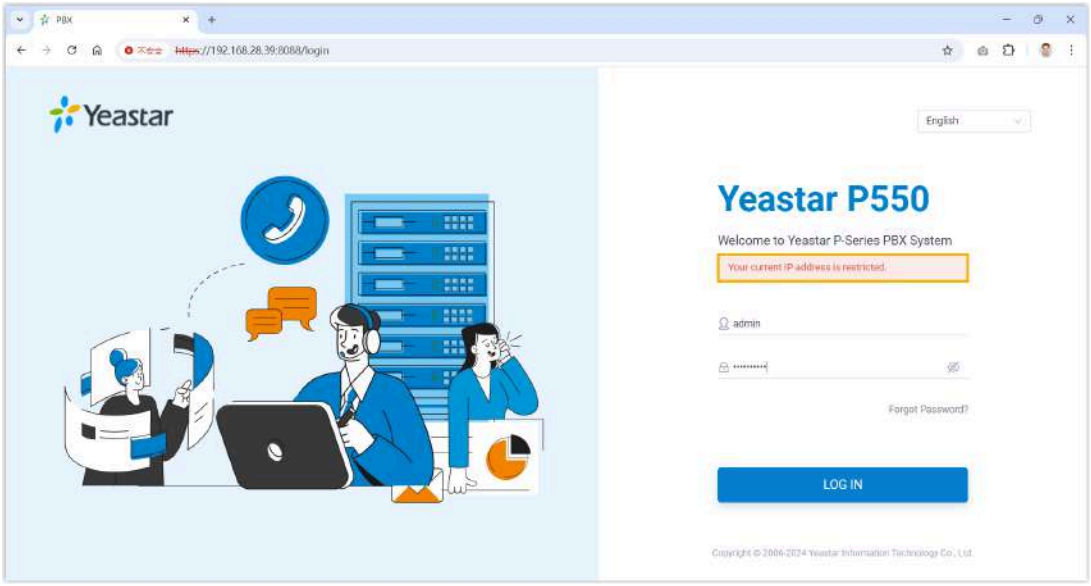
4. Click **Save**.

Result

- Only the allowed IP addresses can access PBX administrator portal, and the settings will take effect next time users log in. Users attempting to log in as super administrator from disallowed IP addresses will receive different prompts depending on the address they visit:
  - If a user logs in as super administrator using `PBX IP address/admin/login`, he or she will be prompted that the page is not found.



  - If a user logs in as super administrator using `PBX IP address/login`, he or she will be prompted that "Your current IP address is restricted".



- The IP address(es) are added to the system's static defense rules. You can check it on **Security > Security Rules > Static Defense**.

> **Note:**
> Changes made to the static defense will not be synchronized to the allowed IP list here.

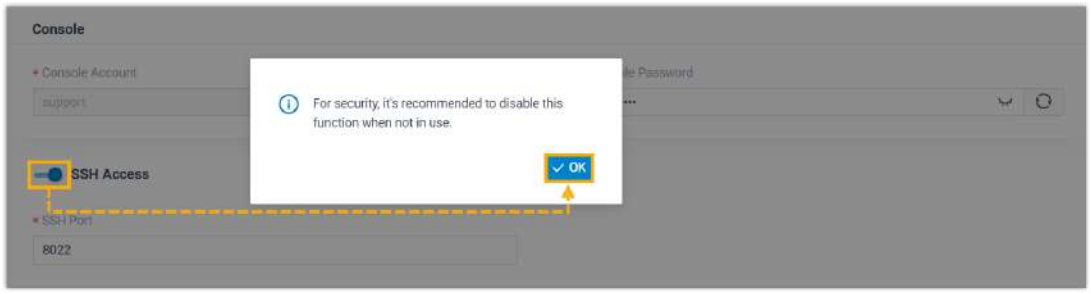
Console/SSH Access

Access the System via SSH

This topic takes Putty as an example to introduce how to access Yeastar P-Series Software Edition via SSH.

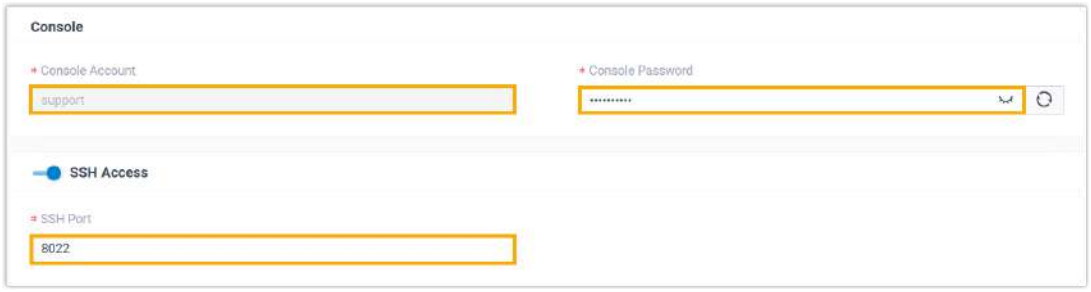
Procedure

1. Enable SSH access on the PBX.
   a. Log in to PBX web portal, go to **Security > Security Settings > Console/SSH Access**.
   b. Turn on the switch of **SSH Access**, then click **OK**.

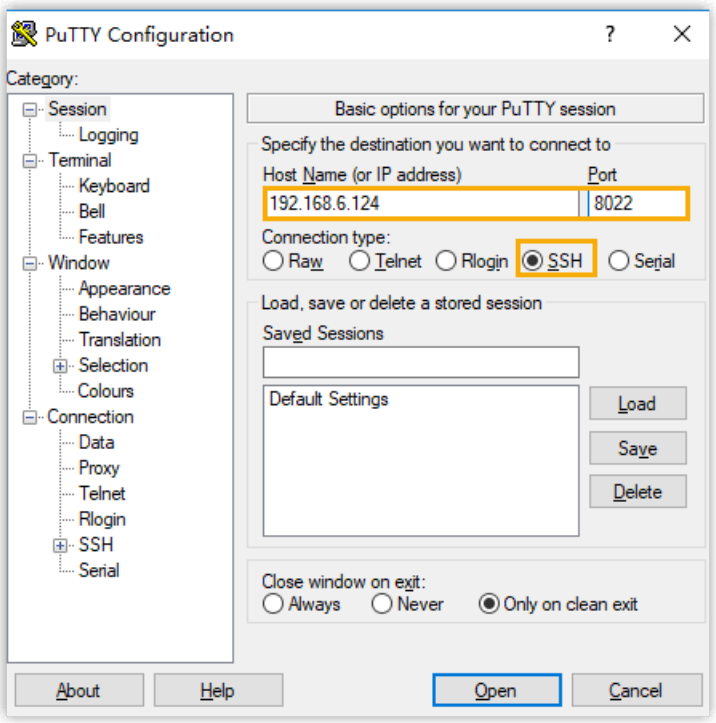


   c. Check and note down the SSH credentials.

> **Note:**
> If you manually install PBX on Ubuntu system, you may be asked to set a normal user during the installation process. You can also use the normal user's credentials to access the PBX via SSH.



2. Enter access information on Putty.
   a. In the **Connection type** field, choose **SSH**.
   b. In the **Host Name (or IP address)** field, enter your PBX's IP address.
   c. In the **Port** field, enter SSH port that you have configured on the PBX.
   d. **Optional:** On the left navigation bar, click **Window > Lines of scrollback**, set a scrollback line number, so that you can get sufficient lines of log for debug analysis.
   e. Click **Open**.



3. Verify your account and password.
    a. In the **login as** field, enter the username.
    b. In the password field, enter the password.

Result

If the following figure shows, you can successfully access and debug the PBX.

Certificates

Manage TLS certificates on the PBX

Yeastar P-Series Software Edition supports TLS protocol to secure SIP messaging. Before using TLS protocol, you may need to upload or apply for a TLS certificate on the PBX.

Background information

With TLS protocol enabled on the PBX, a TLS certificate may be required in the following situations:

- When the PBX acts as a server, a server certificate is required.

  If the PBX requires to verify TLS client (**PBX Settings > SIP Settings > TLS > TLS Verify Client**), you need to upload a client certificate to both PBX and TLS client, or the TLS connection would fail. For more information, see Upload a TLS client certificate.
- When the PBX acts as a client, whether a client certificate is required depends on the server.

If the PBX requires to verify TLS server (**PBX Settings > SIP Settings > TLS > TLS Verify Server**), you need to upload or apply for a server certificate. For more information, see Upload a TLS server certificate or Apply for a TLS server certificate.

Upload a TLS server certificate

Prerequisites

You have prepared a server certificate in `.pem` format.

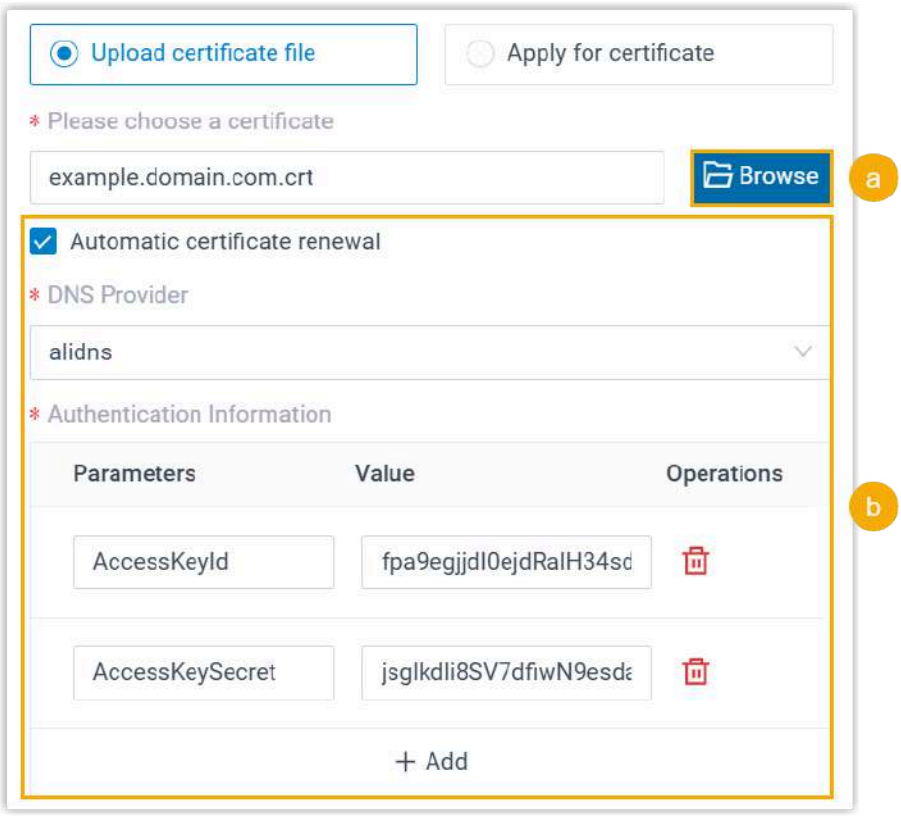
Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Certificates**, click **Add**.

   A window pops up, which requires you to select certificate type and upload a certificate.

   > **Note:**
   > You can ONLY upload or apply for 3 PBX certificates in total.

2. In the **Certificate Type** drop-down list, choose **PBX Certificate**.
3. Select **Upload certificate file**, and complete the following settings.



a. In the **Please choose a certificate** section, click **Browse** to select the desired certificate.
b. If you want the PBX to automatically renew the certificate, select the checkbox of **Automatic certificate renewal**, and provide the DNS provider information.

> **Note:**
> Only Let's Encrypt certificates can be automatically renewed. If the certificate is a non-Let's Encrypt certificate, the PBX will directly apply for a new Let's Encrypt certificate.

- **DNS Provider**: Search and select your desired DNS provider from the drop-down list.
- **Authentication Information**: Add one or more required authentication parameters, and enter the corresponding value.

> **Note:**
> For the specific authentication information of the DNS providers, see Supported DNS Providers.

4. Click **Save**.

Result

- The certificate is uploaded successfully, and is displayed on **Certificates** list.
- If you enable automatic certificate renewal, the system will automatically renew the certificate through the configured DNS provider 7 days before it expires.

Apply for a TLS server certificate

You can directly apply for a TLS server certificate on the PBX.

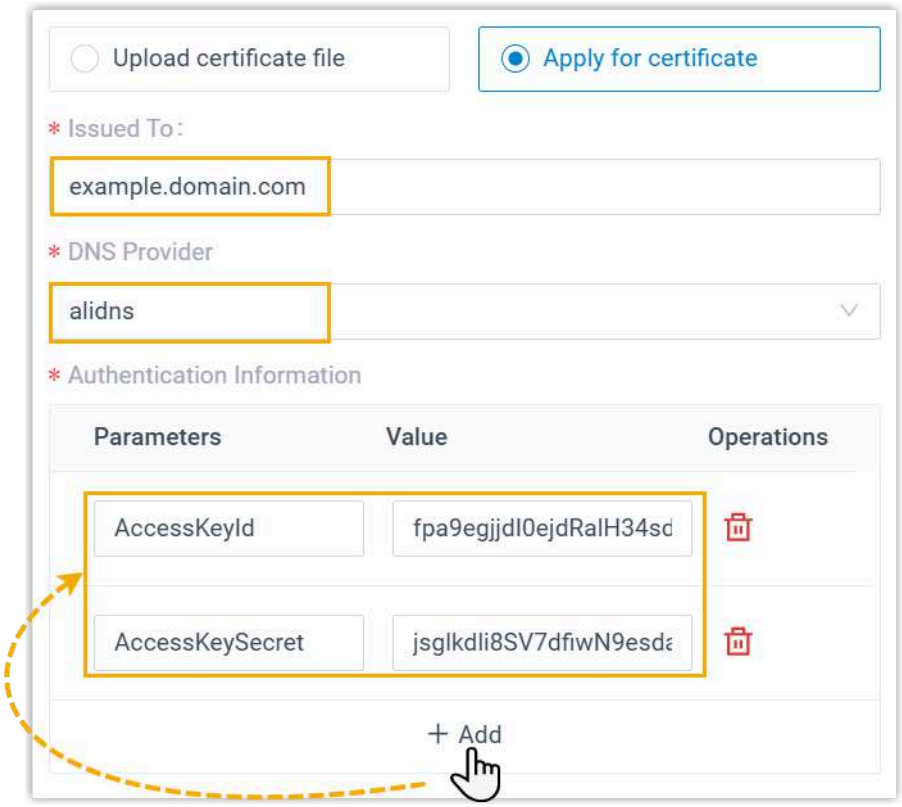
Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Certificates**, click **Add**.

   A window pops up, which requires you to select certificate type and upload a certificate.

   > **Note:**
   > You can ONLY upload or apply for 3 PBX certificates in total.

2. In the **Certificate Type** drop-down list, choose **PBX Certificate**.
3. Select **Apply for certificate**, and complete the following settings.



- **Issued To:**: Enter the domain name for which you want to apply for the certificate.
- **DNS Provider**: Search and select your desired DNS provider from the drop-down list.
- **Authentication Information**: Add one or more required authentication parameters, and enter the corresponding value.

> **Note:**
> For the specific authentication information of the DNS providers, see Supported DNS Providers.

4. Click **Save**.

Result

- PBX will request a domain certificate from Let's Encrypt through the configured DNS provider. The obtained certificate files are named after the domain name.

- If the certificate is applied successfully, the **Application status** displays "-".

Upload a TLS client certificate

Prerequisites

You have prepared a client certificate in `.cer` or `.crt` format.

Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Certificates**, click **Add**.

   A window pops up, which requires you to select certificate type and upload a certificate.

   > **Note:**
   > You can ONLY upload 20 trusted certificates.

2. In the **Certificate Type** drop-down list, choose **Trusted Certificate**.
3. Click **Browse** to select the desired certificate.
4. Click **Upload**.

Result

The certificate is uploaded successfully, and is displayed on **Certificates** list.

Manage HTTPS Certificates on the PBX

Yeastar P-Series 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 or apply for a PBX certificate.

Background information

When you access PBX from web browser, the PBX acts as a server and the web browser acts as a client. A certificate helps verify your PBX's IP address and secures your data transmission.

Upload an HTTPS certificate

Prerequisites

You have prepared a server certificate in `.pem` format.

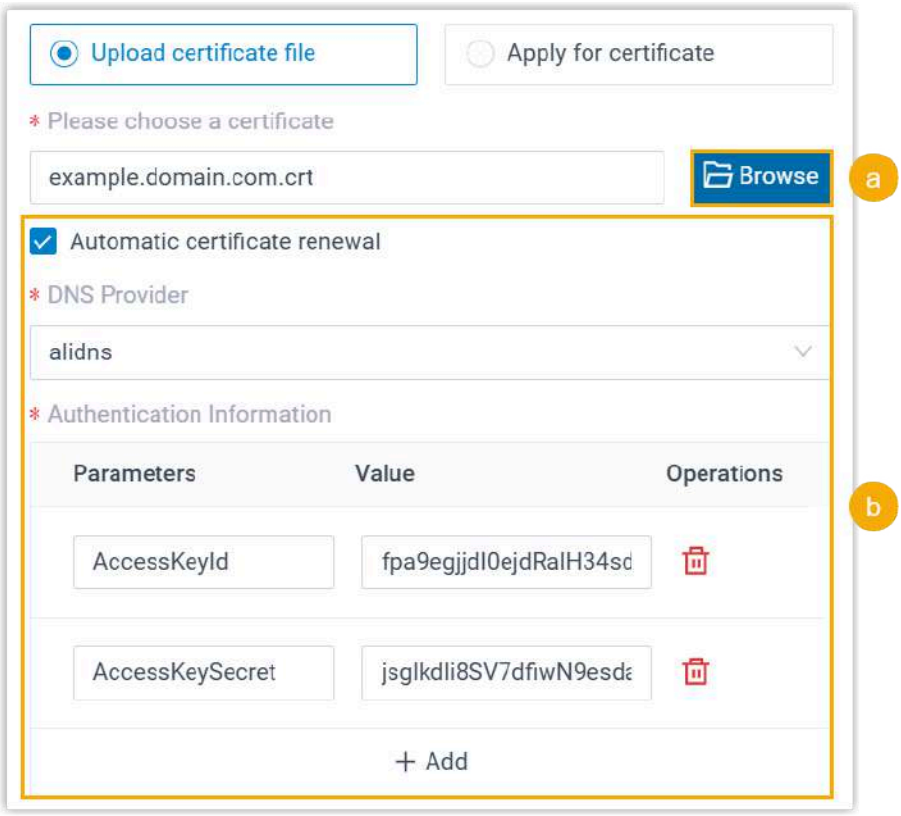
Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Certificates**, click **Add**.

   A window pops up, which requires you to select certificate type and upload a certificate.

   > **Note:**
   > You can ONLY upload or apply for 3 PBX certificates in total.

2. In the **Certificate Type** drop-down list, choose **PBX Certificate**.
3. Select **Upload certificate file**, and complete the following settings.



   a. In the **Please choose a certificate** section, click **Browse** to select the desired certificate.

b. If you want the PBX to automatically renew the certificate, select the checkbox of **Automatic certificate renewal**, and provide the DNS provider information.

> **Note:**
> Only Let's Encrypt certificates can be automatically renewed. If the certificate is a non-Let's Encrypt certificate, the PBX will directly apply for a new Let's Encrypt certificate.

- **DNS Provider**: Search and select your desired DNS provider from the drop-down list.
- **Authentication Information**: Add one or more required authentication parameters, and enter the corresponding value.

> **Note:**
> For the specific authentication information of the DNS providers, see Supported DNS Providers.

4. Click **Save**.

Result

- The certificate is uploaded successfully, and is displayed on **Certificates** list.
- If you enable automatic certificate renewal, the system will automatically renew the certificate through the configured DNS provider 7 days before it expires.

Apply for an HTTPS certificate

You can directly apply for a HTTPS certificate on the PBX.

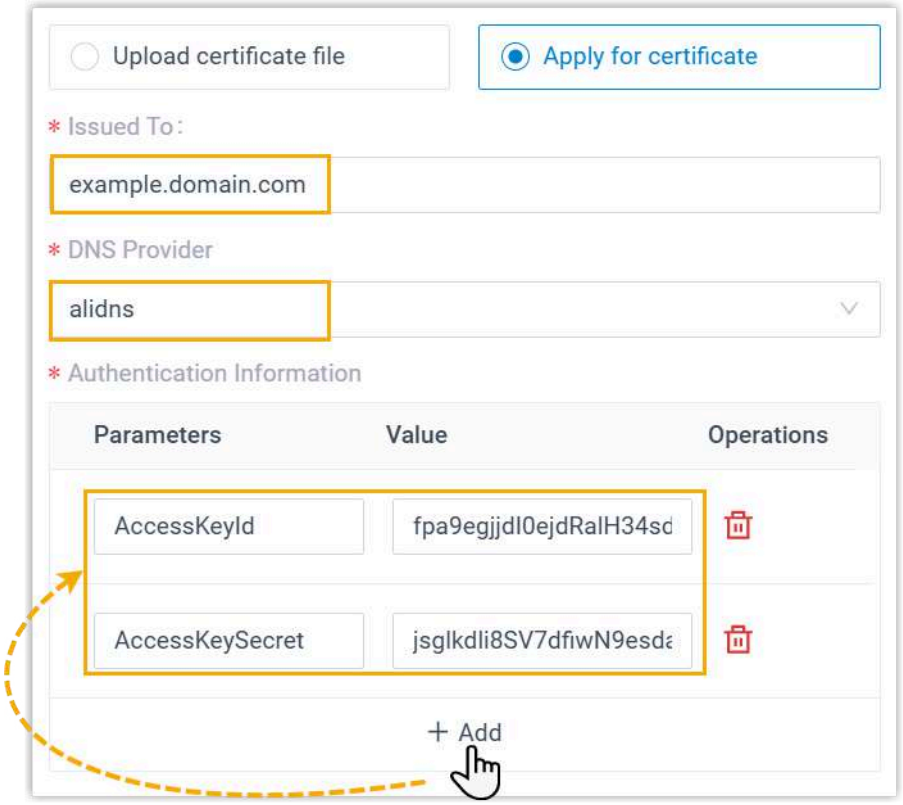
Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Certificates**, click **Add**.

   A window pops up, which requires you to select certificate type and upload a certificate.

> **Note:**
> You can ONLY upload or apply for 3 PBX certificates in total.

2. In the **Certificate Type** drop-down list, choose **PBX Certificate**.
3. Select **Apply for certificate**, and complete the following settings.



- **Issued To:**: Enter the domain name for which you want to apply for the certificate.
- **DNS Provider**: Search and select your desired DNS provider from the drop-down list.
- **Authentication Information**: Add one or more required authentication parameters, and enter the corresponding value.

> **Note:**
> For the specific authentication information of the DNS providers, see Supported DNS Providers.

4. Click **Save**.

Result

- PBX will request a domain certificate from Let's Encrypt through the configured DNS provider. The obtained certificate files are named after the domain name.
- If the certificate is applied successfully, the **Application status** displays "-".

Supported DNS Providers

This topic lists the DNS providers supported by PBX for automatic certificate request and renewal, and provides the description for their required authentication information parameters.

Note:

- You can use the flag name to search for the corresponding DNS provider.
- For parameters with default values, if a parameter is not specified, the system will automatically use its default value.

Provider Name	Flag Name	Supported Parameter
Akamai EdgeDNS	edgedns	• `Host`: API endpoint hostname, managed by the Akamai EdgeGrid client. • `ClientToken`: EdgeGrid client token, generated in the Akamai Control Center. • `ClientSecret`: EdgeGrid client secret, generated in the Akamai Control Center. • `AccessToken`: Access token, managed by the Akamai EdgeGrid client. • `PropagationTimeout`: Time between DNS propagation check in seconds. The default value is 15. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Alibaba Cloud DNS	alidns	• `AccessKeyId`: AccessKey ID. • `AccessKeySecret`: AccessKey secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
all-inkl	allinkl	• `Login`: KAS login username for authentication. • `Password`: KAS password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 60. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Amazon Route 53	route53	• `AccessKeyId`: AWS IAM Access Key ID. • `SecretAccessKey`: AWS IAM Secret Access Key. • `Region`: AWS region name (e.g., `us-east-1`). • `HostedZoneId`: Override the target hosted zone ID. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 120. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 10.
ArvanCloud	arvancloud	• `APIKey`: API key for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
Aurora DNS	auroradns	• `APIKey`: API key for authentication. • `Secret`: API secret paired with the API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Autodns	autodns	• `Username`: Autodns account username. • `Password`: Password for the Autodns account. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.

Provider Name	Flag Name	Supported Parameter
Azure DNS	azuredns	• `ResourceGroup`: Name of the resource group containing the DNS zone. • `TenantID`: Azure Active Directory tenant ID. • `ClientID`: Application (client) ID. • `ClientSecret`: Client secret for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Bindman	bindman	• `ManagerAddress`: Full URL of Bindman-DNS Manager server including scheme, hostname, and port (if required). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Bluecat	bluecat	• `ServerURL`: Full URL of BlueCat BAM server including scheme, hostname, and port. • `UserName`: API username. • `Password`: API password. • `DNSView`: Name of the external DNS view where records will be modified. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Bunny	bunny	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Checkdomain	checkdomain	• `Token`: API token for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Civo	civo	• `Token`: API token for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 30. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
Cloud.ru	cloudru	• `ServiceInstanceID`: Unique ID of the DNS service instance (parentId). • `KeyID`: API key ID (login credential). • `Secret`: API secret key for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
CloudDNS	clouddns	• `ClientID`: API Client ID. • `Email`: Account email. • `Password`: Account password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
Cloudflare	cloudflare	• `DnsApiToken`: API token with DNS:Edit permissions; can also be provided via `CF_DNS_API_TOKEN` environment variable. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
ClouDNS	cloudns	• `AuthID`: Main account ID (numeric) for API authentication. • `AuthPassword`: The password for the API user. • `SubAuthID`: Sub-account ID. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
ConoHa v2	conoha	• `Region`: Target region code (Default: `tyo1`). • `TenantID`: Project (tenant) ID. • `Username`: API username with DNS management permissions. • `Password`: API password for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Constellix	constellix	• `APIKey`: User API key. • `SecretKey`: Secret key paired with the API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Core-Networks	corenetworks	• `Login`: API account username with DNS management privileges. • `Password`: Corresponding account password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
CPanel/WHM	cpanel	• `Mode`: API type (`cpanel` = per-account, `whm` = server-wide). The default is `cpanel`. • `Username`: cPanel account username (for `cpanel` mode) or WHM root username (for `whm` mode). • `Token`: API authentication token. • `BaseURL`: Server API endpoint. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Derak Cloud	derak	• `APIKey`: Account authentication key. • `WebsiteID`: Explicitly specify target zone ID (override auto-detection) • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
deSEC.io	desec	• `Token`: Domain-specific API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Digital Ocean	digitalocean	• `BaseURL`: API endpoint URL. • `AuthToken`: Authentication token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 10.
DirectAdmin	directadmin	• `BaseURL`: The URL of the API. • `Username`: API username. • `Password`: API password. • `ZoneName`: The domain name (DNS zone) where the TXT record will be added. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 10.
DNS Made Easy	dnsmadeeasy	• `APIKey`: The API key. • `APISecret`: The API secret. • `Sandbox`: Activate the sandbox (boolean, the default value is `false`). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
dnsHome.de	dnshomede	• `Credentials`: Comma-separated list of `domain:password` credential pairs. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5.
DNSimple	dnsimple	• `AccessToken`: Your DNSimple API access token used for authentication. • `BaseURL`: The base URL for the DNSimple API. E.g. `https://api.dnsimple.com`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Domain Offensive (do.de)	dode	• `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5.
Domeneshop	domeneshop	• `APIToken`: API token. • `APISecret`: API secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 20.
DreamHost	dreamhost	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 3600. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 60.
Duck DNS	duckdns	• `Token`: Your DuckDNS account token used for authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5.

Provider Name	Flag Name	Supported Parameter
Dyn	dyn	• `CustomerName`: Your Dyn customer account name. • `UserName`: Your Dyn Managed DNS username. • `Password`: The password associated with your Dyn Managed DNS username. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Dynu	dynu	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
EasyDNS	easydns	• `Endpoint`: (Optional) The base URL of the EasyDNS API server. • `Token`: API token. • `Key`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Efficient IP	efficientip	• `Username`: API username. • `Password`: Password associated with the API username. • `Hostname`: The Fully Qualified Domain Name (FQDN) of the DNS record to be managed. E.g. `foo.example.com`. • `DNSName`: The name of the DNS zone where the record resides. E.g. `dns.smart`. • `ViewName`: The DNS view name associated with the zone. E.g. `external`. • `InsecureSkipVerify`: Whether to skip SSL certificate verification when connecting to the EfficientIP API (Boolean, the default value is `false`, which means certificate verification is enabled to ensure secure connections). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Epik	epik	• `Signature`: Epik API signature. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Gandi	gandi	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 2400. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 60. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Gandi Live DNS (v5)	gandiv5	• `PersonalAccessToken`: Personal access token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 20. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Glesys	glesys	• `APIUser`: API username. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 20. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Go Daddy	godaddy	• `ApiKey`: API key. • `ApiSecret`: API secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
Google Cloud	gcloud	• `ServiceAccount`: Your Google Cloud service account. • `Project`: The Google Cloud project ID. If not specified, it will be automatically detected using the metadata server.

Provider Name	Flag Name	Supported Parameter
		• `ZoneID`: The managed zone name. Providing this skips automatic zone detection. • `AllowPrivateZone`: Allows the use of private DNS zones. This is supported only with a private ACME server (Boolean, the default value is `false`). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 5. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Google Domains	googledomains	• `AccessToken`: Access token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Hetzner	hetzner	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Hosting.de	hostingde	• `APIKey`: API key. • `ZoneName`: The DNS zone name in ACE (ASCII Compatible Encoding) format. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Hosttech	hosttech	• `APIKey`: API login key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 120. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
http.net	httpnet	• `APIKey`: API key. • `ZoneName`: The DNS zone name in ACE (ASCII Compatible Encoding) format.

Provider Name	Flag Name	Supported Parameter
		• `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Huawei Cloud	huaweicloud	• `AccessKeyId`: Huawei Cloud API access key ID. • `SecretAccessKey`: The secret key associated with your access key ID. • `Region`: Huawei Cloud region where your DNS service is located. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Hurricane Electric DNS	hurricane	• `Credentials`: List of TXT record names and corresponding tokens required to complete the DNS-01 challenge. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
IBM Cloud (SoftLayer)	ibmcloud	• `Username`: Username. • `APIKey`: API key for accessing the Classic Infrastructure services. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
IIJ DNS Platform Service	iijdpf	• `Token`: API token. • `ServiceCode`: The service code for IIJ Managed DNS Service. • `Endpoint`: The API endpoint URL. Defaults to `https://api.dns-platform.jp/dpf/v1`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Infoblox	infoblox	• `Host`: The base URI of the Infoblox grid manager API. • `Port`: Port number used to connect to the Infoblox grid manager. The default value is 443. • `Username`: Username for account authentication. • `Password`: Password for the account. • `DNSView`: The DNS view where the TXT records are managed. The default value is `External`. • `WapiVersion`: Version of the Infoblox WAPI (Web API) in use. The default value is `2.11`. • `SSLVerify`: Whether to verify the TLS certificate or not (Boolean, the default value is `true`). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Infomaniak	infomaniak	• `APIEndpoint`: Your infomaniak API endpoint URL. The default value is `https://api.infomaniak.com`. • `AccessToken`: Access token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Internet Initiative Japan	iij	• `AccessKey`: API access key. • `SecretKey`: API secret key. • `DoServiceCode`: The service code for IIJ Managed DNS. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Internet.bs	internetbs	• `APIKey`: API key. • `Password`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
INWX	inwx	• `Username`: Your account username. • `Password`: The password for your account. • `SharedSecret`: The shared secret key used for two-factor authentication (2FA). • `Sandbox`: Activate the sandbox (Boolean, the default value is `false`). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Ionos	ionos	• `APIKey`: API key in the format `prefix.secret`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
IPv64	ipv64	• `APIKey`: Account API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
iwantmyname	iwantmyname	• `Username`: API username. • `Password`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Joker	joker	• `APIKey`: API key, used only in DMAPI mode. • `Username`: Your Joker account username. • `Password`: Your Joker account password. • `APIMode`: API mode, either `DMAPI` or `SVC`. Default is `DMAPI`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Liara	liara	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Lima-City	limacity	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Linode (v4)	linode	• `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Liquid Web	liquidweb	• `BaseURL`: Liquid Web API endpoint URL. • `Username`: Liquid Web API username. • `Password`: Liquid Web API password. • `Zone`: DNS zone name. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Loopia	loopia	• `BaseURL`: API endpoint URL. E.g. `https://api.loopia.se/RPCSERV` (default) or `https://api.loopia.rs/RPCSERV`. • `APIUser`: API username. • `APIPassword`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 2400. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
LuaDNS	luadns	• `APIUsername`: Your username, which is your email address. • `APIToken`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Mail-in-a-Box	mailinabox	• `Email`: Email address. • `Password`: Password. • `BaseURL`: Base URL of the API (e.g. `https://box.example.com`). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
ManageEngine CloudDNS	manageengine	• `ClientID`: Client ID. • `ClientSecret`: Client secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Metaname	metaname	• `AccountReference`: The four-digit identifier for your Metaname account. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
mijn.host	mijnhost	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.

Provider Name	Flag Name	Supported Parameter
Mittwald	mittwald	• `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
MyDNS.jp	mydnsjp	• `MasterID`: Master ID. • `Password`: Password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
MythicBeasts	mythicbeasts	• `UserName`: Username. • `Password`: Password. • `APIEndpoint`: The API endpoint (must support v2). • `AuthAPIEndpoint`: The endpoint for Mythic Beasts' Authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Name.com	namedotcom	• `Username`: Username. • `ApiToken`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 20. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Namecheap	namecheap	• `BaseURL`: Your Namecheap API base URL. • `APIUser`: API user. • `APIKey`: API key. • `ClientIP`: The IP address authorized to access the API. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Namesilo	namesilo	• `ApiKey`: API key.

Provider Name	Flag Name	Supported Parameter
		• `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
NearlyFreeSpeech.NET	nearlyfreespeech	• `APIKey`: API key used for authenticating API requests. • `Login`: Username associated with your NearlyFreeSpeech.NET account. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Netcup	netcup	• `Key`: API key. • `Password`: API password. • `Customer`: Your Netcup customer number. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Netlify	netlify	• `Token`: Token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Nicmanager	nicmanager	• `Login`: Your login name for username-based authentication. • `Username`: Alternate field for username-based login (used interchangeably with `Login`). • `Email`: Email address used for email-based login. • `Password`: The account password. • `OTPSecret`: TOTP (Time-based One-Time Password) secret for two-factor authentication. • `Mode`: DNS mode, either `anycast` (default) or `zone`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 900.
NIFCloud	nifcloud	• `BaseURL`: The base URL for the NIFCloud API. • `AccessKey`: Access key. • `SecretKey`: Secret access key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Njalla	njalla	• `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Nodion	nodion	• `APIToken`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
NS1	ns1	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Open Telekom Cloud	otc	• `IdentityEndpoint`: The endpoint URL for identity authentication. • `DomainName`: The domain name associated with your account. • `ProjectName`: The name of the project under your account. • `UserName`: Username. • `Password`: Password.

Provider Name	Flag Name	Supported Parameter
		• `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Oracle Cloud	oraclecloud	• `CompartmentID`: The OCID of your Oracle Cloud compartment. • `Tenancy`: The OCID of your tenancy. • `User`: The OCID of your user account. • `Region`: The Oracle Cloud region to use. • `Fingerprint`: The fingerprint of your API public key. • `PrivateKey`: Path to your API private key file. • `PrivateKeyPassphrase`: The passphrase for the private key, if set. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
OVH	ovh	• `APIEndpoint`: Endpoint URL, typically `ovh-eu` or `ovh-ca`. • `ApplicationKey`: Application key used for Application Key authentication. • `ApplicationSecret`: Application secret used for Application Key authentication. • `ConsumerKey`: Consumer key used for Application Key authentication. • `OAuth2ClientID`: Client ID used for OAuth2 authentication. • `OAuth2ClientSecret`: Client secret used for OAuth2 authentication. • `AccessToken`: Access token for OAuth2 authentication. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
plesk.com	plesk	• `BaseURL`: Base URL of the Plesk server. • `Username`: API username. • `Password`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Porkbun	porkbun	• `APIKey`: API key. • `SecretAPIKey`: Secret API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
PowerDNS	powerdns	• `ApiUrl`: API URL. • `ApiKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Rackspace	rackspace	• `APIUser`: API user. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Rain Yun	rainyun	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
RcodeZero	rcodezero	• `APIToken`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.

Provider Name	Flag Name	Supported Parameter
reg.ru	regru	• `Username`: API username. • `Password`: API password • `TLSCert`: Authentication certificate. • `TLSKey`: Authentication private key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
Regfish	regfish	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
RFC2136	rfc2136	• `Nameserver`: Network address in the format `host` or `host:port`. • `TSIG`: Path to the key file generated by `tsig-keygen`. • `TSIGAlgorithm`: TSIG algorithm. Refer to here for supported values. To disable TSIG authentication, leave `RFC2136_TSIG_KEY` or `RFC2136_TSIG_SECRET` unset. • `TSIGKey`: Name of the secret key as defined in DNS server configuration. To disable TSIG authentication, leave `RFC2136_TSIG_KEY` unset. • `TSIGSecret`: Secret key value. To disable TSIG authentication, leave `RFC2136_TSIG_SECRET` unset. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
RimuHosting	rimuhosting	• `APIKey`: User API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Sakura Cloud	sakuracloud	• `Token`: Access token. • `Secret`: Access token secret.

Provider Name	Flag Name	Supported Parameter
		• `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Scaleway	scaleway	• `ProjectID`: Project ID. • `AccessKey`: Access key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Selectel	selectel	• `BaseURL`: API endpoint URL. • `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Selectel v2	selectelv2	• `BaseURL`: API endpoint URL. • `Username`: Openstack username. • `Password`: Password for the OpenStack username. • `Account`: Selectel account ID (integer). • `ProjectID`: Cloud project ID (UUID). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
SelfHost.(de|eu)	selfhostde	• `Username`: Username. • `Password`: Password. • `RecordsMapping`: Mapping of record IDs to domains. E.g. `"example.com":["123","456"],"example.org":["789"],"foo.example.com":["147"]`.
Servercow	servercow	• `Username`: API username. • `Password`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200.

Provider Name	Flag Name	Supported Parameter
		• `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Shellrent	shellrent	• `Username`: Username. • `Token`: Token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.
Simply.com	simply	• `AccountName`: Account name. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Sonic	sonic	• `UserID`: User ID. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Stackpath	stackpath	• `ClientID`: Client ID. • `ClientSecret`: Client Secret. • `StackID`: Stack ID. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Technitium	technitium	• `BaseURL`: Server base URL. • `APIToken`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.

Provider Name	Flag Name	Supported Parameter
		• `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Tencent Cloud DNS	tencentcloud	• `SecretId`: Access key ID. • `SecretKey`: Access Key secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 0. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 0.
Timeweb Cloud	timewebcloud	• `AuthToken`: Authentication token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
TransIP	transip	• `AccountName`: Account name. • `PrivateKey`: Path to the private key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 10.
UKFast SafeDNS	safedns	• `AuthToken`: Authentication token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Ultradns	ultradns	• `Username`: API username. • `Password`: API password. • `Endpoint`: API endpoint URL, defaults to `https://api.ultradns.com/`. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Variomedia	variomedia	• `APIToken`: API token.

Provider Name	Flag Name	Supported Parameter
		• `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
VegaDNS	vegadns	• `BaseURL`: API endpoint URL. • `APIKey`: API key. • `APISecret`: API secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 10.
Vercel	vercel	• `AuthToken`: Authentication token. • `TeamID`: Team ID (E.g. `team_xxxx`) • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Versio.[nl|eu|uk]	versio	• `BaseURL`: The endpoint URL of the API Server,optional, defaults to `https://www.versio.nl/api/v1/`. • `Username`: Basic authentication username. • `Password`: Basic authentication password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
VinylDNS	vinyldns	• `AccessKey`: The VinylDNS API key. • `SecretKey`: The VinylDNS API Secret key. • `Host`: The VinylDNS API URL. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 30.
VK Cloud	vkcloud	• `ProjectID`: String ID of project in VK Cloud. • `Username`: Email of VK Cloud account. • `Password`: Password for VK Cloud account.

Provider Name	Flag Name	Supported Parameter
		• `DNSEndpoint`: URL of DNS API. Defaults to `https://mcs.mail.ru/public-dns` but can be changed for private clouds. • `IdentityEndpoint`: URL of OpenStack Auth API, Defaults to `https://infra.mail.ru:35357/v3/` but can be changed for usage with private clouds. • `DomainName`: Openstack users domain name. Defaults to `users` but can be changed for private clouds. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Volcano Engine	volcengine	• `AccessKeyId`: Access key ID (AK). • `SecretAccessKey`: Secret access key (SK). • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 300. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 10. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
Vscale	vscale	• `BaseURL`: API endpoint URL. • `Token`: API token. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Vultr	vultr	• `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 120.
Webnames	webnames	• `APIKey`: Domain API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4.
Websupport	websupport	• `APIKey`: API key.

Provider Name	Flag Name	Supported Parameter
		• `Secret`: API secret. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 600.
WEDOS	wedos	• `Username`: Username is the same as the admin account. • `Password`: Password must be generated and the IP address allowed in the admin interface. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 300.
West.cn	westcn	• `Username`: Username. • `Password`: API password. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Yandex 360	yandex360	• `OAuthToken`: The OAuth Token. • `OrgID`: The organization ID. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 21600.
Yandex Cloud	yandexcloud	• `IamToken`: The base64-encoded JSON containing IAM token info of a service account with `dns.admin` permissions. • `FolderID`: The string ID of the folder (i.e. project) in Yandex Cloud. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.

Provider Name	Flag Name	Supported Parameter
Yandex PDD	yandex	• `PddToken`: Basic authentication username. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 21600.
Zone.ee	zoneee	• `Endpoint`: API endpoint URL. • `Username`: API user. • `APIKey`: API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 60.
Zonomi	zonomi	• `APIKey`: User API key. • `PropagationTimeout`: Maximum wait time for DNS propagation in seconds. The default value is 1200. • `PollingInterval`: Time between DNS propagation check in seconds. The default value is 4. • `TTL`: The TTL of the TXT record used for the DNS challenge in seconds. The default value is 3600.

Delete Certificates

This topic describes how to delete one or more certificates on Yeastar P-Series 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

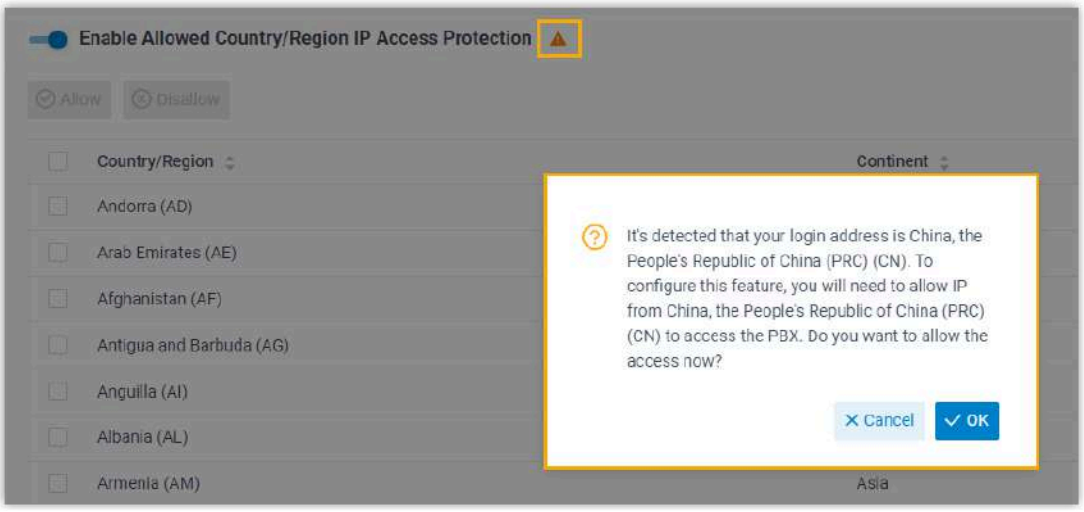
Restrict Specific Countries or Regions from Accessing Yeastar P-Series Software Edition

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

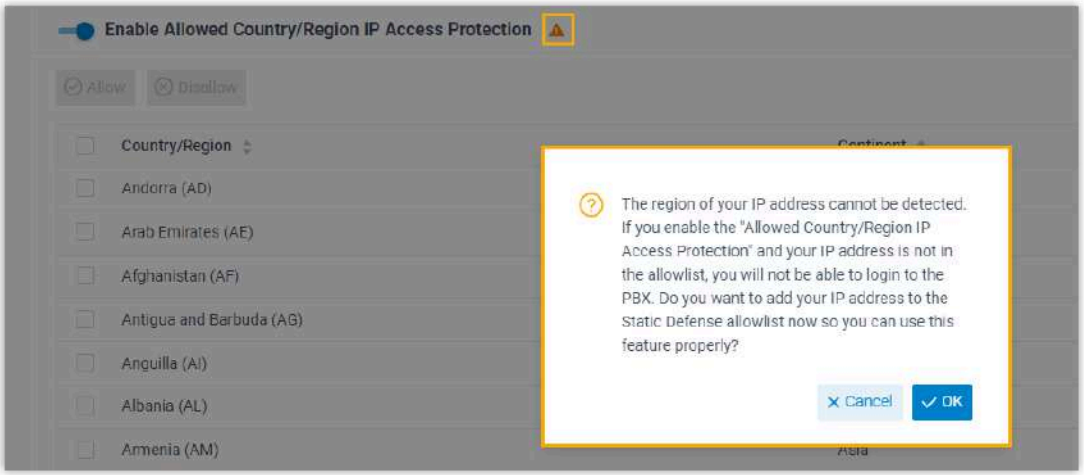
1. Log in to PBX web portal, go to **Security > Security Settings > Allowed Country IPs**.
2. Turn on the option **Enable Allowed Country/Region IP Access Protection**.

   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.



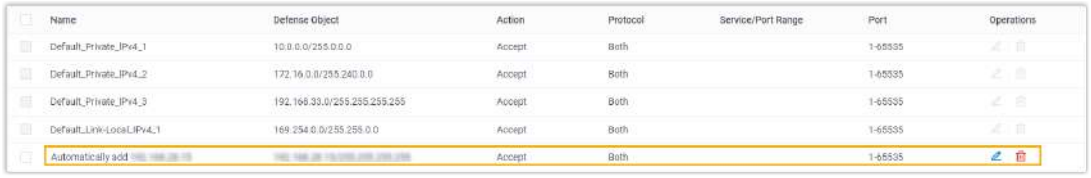
You should click **OK** to allow IPs from your current country/region to access the PBX. In doing so, the warning icon is disappeared, and operation status of your country/region is changed to .

- If the system fails to detect your country/region, a warning icon and a pop-up window will be displayed, prompting you to allow access for your current IP address.



You should click **OK** to add your IP address to the Static Defense allowlist. In doing so, the warning icon ⚠ is disappeared, and connections from your IP address are accepted.

> **Tip:**
> You can check the added IP address on **Security > Security Rules > Static Defense**.



4. To allow desired countries/regions to access the PBX, do as follows:
   - To allow a country/region to access the PBX, do as follows:

     a. In the search box, enter a desired country or region.
     b. In the **Operations** column, set the status to .
   - To allow multiple countries/regions to access the PBX, do as follows:

     a. Select the checkboxes of desired countries or regions.
     b. Click **Allow**.

     The status will be changed to .
5. Click **Apply**.

Result

Only the devices with IP addresses originating from the allowed countries or regions can access the PBX.

Tip:
For the disallowed countries or regions, if you want to allow a specific IP address to access the PBX, you can add a static defense rule to accept connections from the desired IP address. For more information, see Add a Static Defense Rule.

Check Allowed Country/Region IP

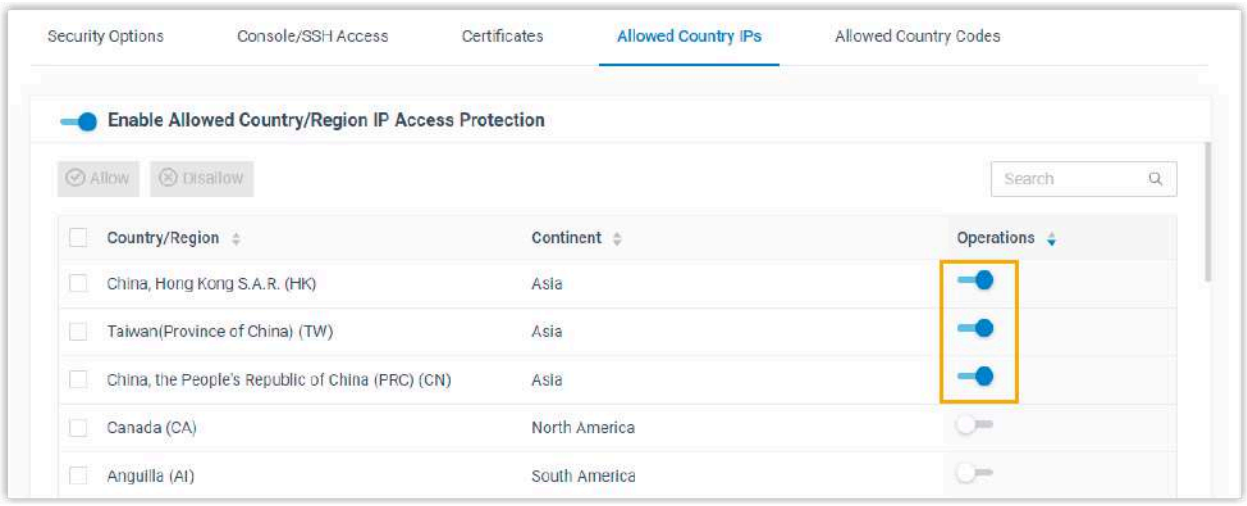
By default, all the countries and regions are displayed in ascending (A to Z) alphabetical order, whether they are allowed to access Yeastar P-Series Software Edition or not. To check the allowed country/region IP, you need to sort all the countries and regions again.

Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Allowed Country IPs**.
2. Click ▼ beside **Operations**.

Result

All the countries and regions that are allowed to access the PBX are moved to the top.



Allowed Country Codes

Restrict International Calls to Specific Countries or Regions

If there is an outbound route on your PBX that allows outbound international calls, the authorized users can make international calls to all the countries and regions. To prevent toll fraud, you can restrict users from making international calls to specific countries or regions.

Scenario

A manufacturer has a factory in Mexico, and his or her target customers are in Argentina. The manufacturer wants to restrict employees from making international calls to countries and regions except Argentina (country code 54).

Procedure

Based on the above scenario, you need to follow the instructions below to realize restrictions on international dialing:

- Step1. Allow international calls to Argentina only
- Step2. Allow employees to make international calls

Step1. Allow international calls to Argentina only

1. Log in to PBX web portal, go to **Security > Security Settings > Allowed Country Codes**.

2. Enable international dialing protection, and set international dialing code.
    a. Turn on the option **Enable Allowed Country/Region Code Dialing Protection**.
    b. In the **International Dialing Code** field, enter the prefix of international call according to your country. In the scenario, enter *00*.
    When an employee tries to call a number starting with 00, the PBX's outbound route will identify this call as an international call.

    > **Note:**
    > Make sure there is at least one outbound route that matches with the international dialing code to route international calls out.

    c. Click and **Apply**.
3. Set the countries or regions to which employees can make international calls.
    a. In the search box, enter a desired country or region. In the scenario, enter *Argentina*.

    b. In the **Operations** column, set the status to .

    > **Note:**
    > Some countries or regions share the same code (e.g. the country code for Canada and America is 1). If you allow international dialing to a country or a region, employees can also make calls to the countries or regions that share the same code.

    c. Click **Apply**.

Step2. Allow employees to make international calls

By default, after you enable country/region code dialing protection, all the users are not allowed to make international calls. To allow employees to make international calls, you need to grant permission to desired employees.

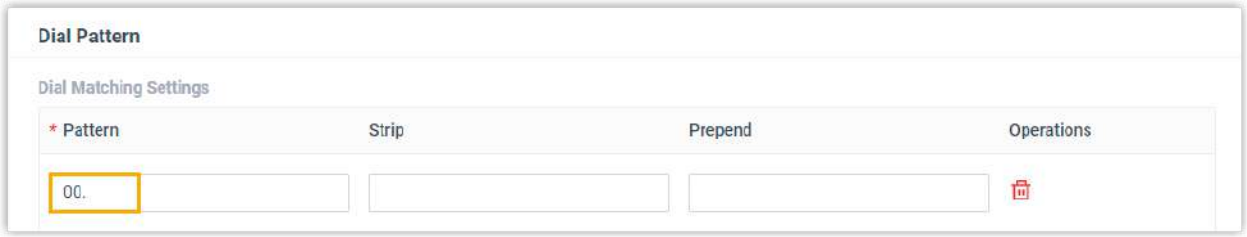
1. Go to **Extension and Trunk > Extension**.

2. Select the checkboxes of desired extensions, click **Edit**.
3. Click **Security** tab.
4. In the **Call Restrictions** section, select the checkbox of **Bulk Edit** and unselect the checkbox of **Disallow International Calls**.
5. Click **Save** and **Apply**.

Result

Authorized employees can make international calls to Argentina (country code 54).

The PBX has an outbound route configured as follows:



When an authorized employee dials a number, PBX's outbound route will check if the dialing is valid:

- When an authorized employee dials 00541938384, the dialing is considered as valid.
- When an authorized employee dials 00621938384, the dialing is considered as invalid.
- When an authorized employee dials 541938384, it will not be considered as an international dialing, and the PBX will check if there is a matched outbound route to route the call out.

Block Outbound International Calls

To restrict users from making international calls, you can restrict dial pattern of outbound routes, or set up international dialing protection. This topic describes how to set up international dialing protection to block outbound international calls.

Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Allowed Country Codes**.
2. Turn on the option **Enable Allowed Country/Region Code Dialing Protection**.
3. In the **International Dialing Code** field, enter the prefix of international call according to your country.

4. Click and **Apply**.

Result

All the extension users can NOT make international calls.

Two-Factor Authentication (2FA)

Two-factor Authentication (2FA) Overview

Yeastar P-Series Software Edition supports to configure two-factor authentication (2FA) for super administrator account. With 2FA enabled, both the account password and an additional authentication code are required for login, which adds an extra layer of security to the PBX. This topic provides an overview of the supported two-factor authentication methods.

> **Note:**
> Extension users can also configure two-factor authentication for their own accounts on Linkus **Web Client** or **Desktop Client**, and the configuration will be applied to all their Linkus clients.
>
> For more information, see Two-factor Authentication (2FA) on Linkus Web Client and Two-factor Authentication (2FA) on Linkus Desktop Client.

Requirements

Yeastar P-Series Software Edition is 83.10.0.30 or later.

Two-factor authentication by authenticator application

This method requires you to install an authenticator application on your mobile phone. The supported applications are listed below:

- Google Authenticator
- FreeOTP
- Twilio Authy
- Microsoft Authenticator

After installing an authenticator application, you need to add your account to the application, via which you can obtain authentication codes for two-factor authentication. When you log in to the super administrator account, both account password and the authentication code generated by the authenticator application are required.

For more information about the configuration, see Configure Two-factor Authentication using Authenticator Application.

Two-factor authentication by Email

This method allows you to receive authentication codes for two-factor authentication via the email associated with the super administrator account. When you log in to the super administrator account, both account password and the authentication code sent to your email are required.

For more information about the configuration, see Configure Two-factor Authentication using Email.

Configure Two-factor Authentication using Authenticator Application

This topic describes how to configure two-factor authentication for super administrator account using an authenticator application on your mobile phone.

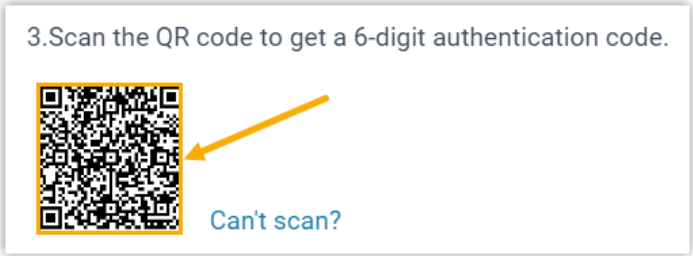
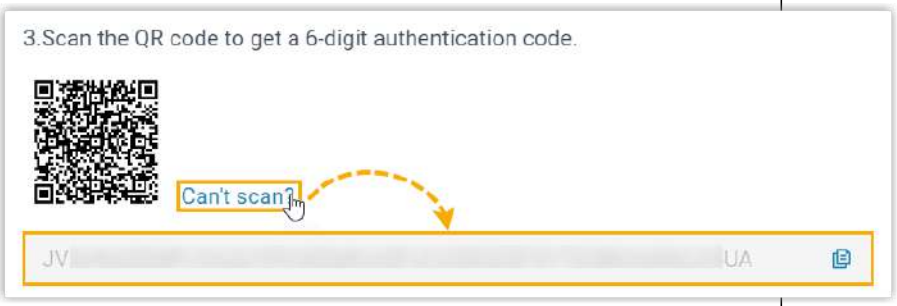
Prerequisites

You have installed one of the following supported authenticator applications on your mobile phone.

- Google Authenticator
- FreeOTP
- Twilio Authy
- Microsoft Authenticator

Procedure

1. Log in to PBX web portal, click your account at the top-right corner, then go to **Change Password & Security > Security Settings**.
2. Select the checkbox of **Two-Factor Authentication**.
3. In the pop-up **Password** window, enter your account password and click **Confirm** to verify your operation.
4. Select **Authenticated by Authenticator**.
5. Add your account to the authenticator application via either of the following methods.

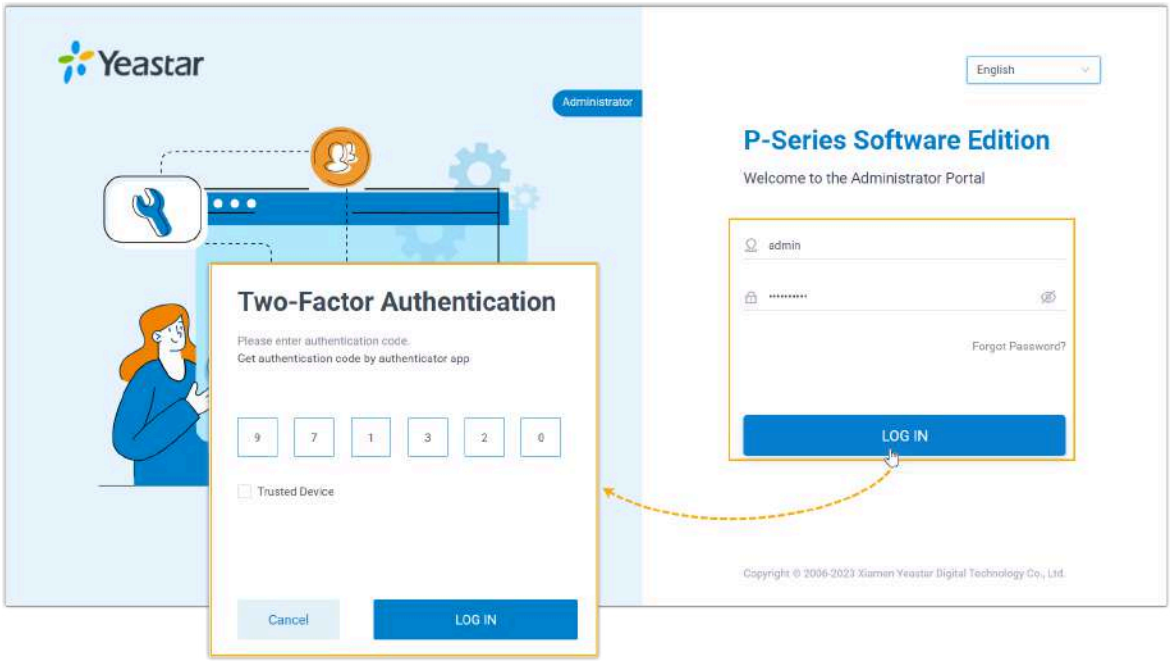
Method	Instruction
Scan QR Code to quickly add the account	You can quickly add your account to the authenticator application by scanning the QR code provided by PBX. a. On your mobile phone, open the authenticator application, and select to scan QR code. b. Scan the QR code shown on PBX web portal.  Your account is added to the application automatically, a 6-digit authentication code is shown.
Manually add the account	In case you can not scan QR code, you can manually add your account and enter the secret key provided by PBX. a. On PBX web portal, click **Can't scan** beside the QR code. PBX will generate a secret key, note it down for later use.  b. On your mobile phone, open the authenticator application, and select to manually add an account. c. Enter the relevant information, and paste the secret key. **Note:** If you need to complete more configurations for the secret key, you should set **SHA1** as the algorithm for **TOTP** protocol, and set to generate **6-digit** code with an interval of **30** seconds. Your account is added to the application, a 6-digit authentication code is shown.

6. On PBX web portal, enter the 6-digit authentication code in the **Authentication Code** field.
7. Click **Save**.

Result

- The webpage prompts a message "Edited successfully.", which means that you have successfully set up two-factor authentication.
- Next time you log in to PBX web portal, you need to enter an authentication code additionally.

> **Note:**
> For the device from which you log in most frequently, you can select the checkbox of **Trusted Device** to add it as a trusted device. In this way, you don't have to re-enter an authentication code with this device for the next 180 days.



> **Troubleshooting:**
> **What if my extension users fail to log in with two-factor authentication?**

You can disable two-factor authentication for their extension accounts, so that they can directly log in with their username and password.

Related information

Manage Two-factor Authentication of Super Administrator Account

Configure Two-factor Authentication using Email

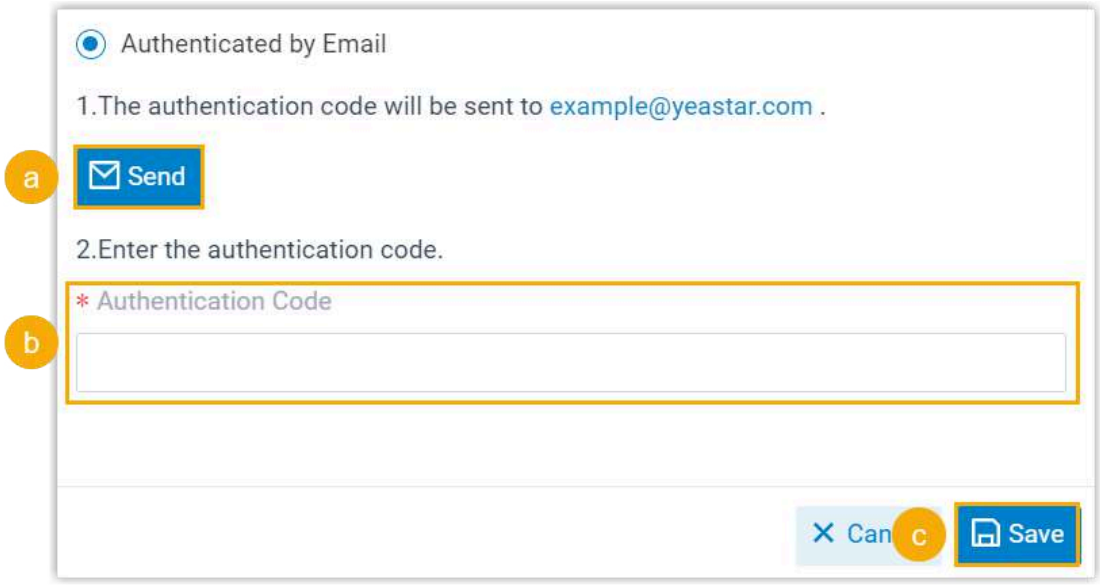
This topic describes how to configure two-factor authentication for super administrator account using email.

Prerequisites

System email server is set up.

Procedure

1. Log in to PBX web portal, click your account at the top-right corner, then go to **Change Password & Security > Security Settings**.
2. Select the checkbox of **Two-Factor Authentication**.
3. In the pop-up **Password** window, enter your account password and click **Confirm** to verify your operation.
4. Select **Authenticated by Email**, and complete the following settings:



a. Click **Send**.
An email containing a 6-digit authentication code is sent to the email address that is associated with the super administrator account.

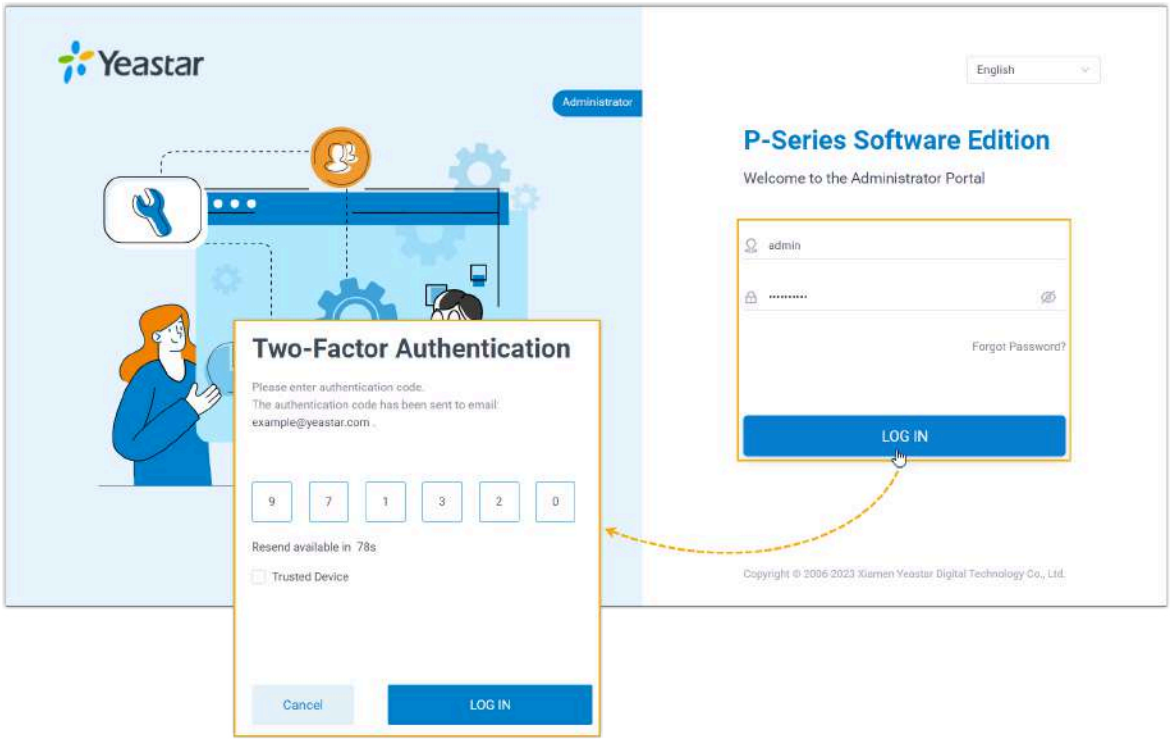
> **Note:**
> The code expires 5 minutes after the email is sent.

b. In the **Authentication Code** field, enter the authentication code.
c. Click **Save**.

Result

- The webpage prompts a message "Edited successfully.", which means that you have successfully set up two-factor authentication.
- Next time you log in to PBX web portal, you need to enter an authentication code additionally.

> **Note:**
> For the device from which you log in most frequently, you can select the checkbox of **Trusted Device** to add it as a trusted device. In this way, you don't have to re-enter an authentication code with this device for the next 180 days.



Troubleshooting:
What if my extension users fail to log in with two-factor authentication?

You can disable two-factor authentication for their extension accounts, so that they can directly log in with their username and password.

Related information

Manage Two-factor Authentication of Super Administrator Account

Manage Two-factor Authentication of Super Administrator Account

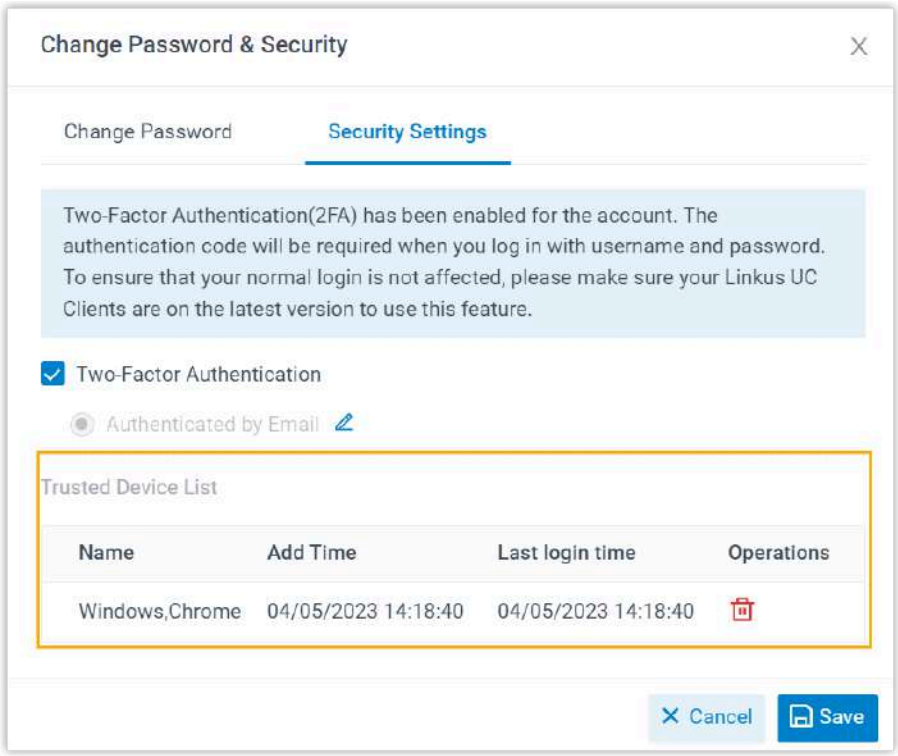
This topic describes how to manage the two-factor authentication feature for super administrator account, including removing trusted devices, changing authentication method, and disabling the two-factor authentication feature.

Remove a trusted device

As a super administrator, in case you lost access to a trusted device, you can remove it from the list if necessary.

1. Log in to PBX administrator portal with super administrator account, click your account at the top-right corner, then go to **Change Password & Security > Security Settings**.

   The trusted devices are displayed in the **Trusted Device List** section.



2. Click 🗑 beside the device that you want to remove.
3. In the pop-up window, click **OK**.

Change two-factor authentication method

You can change the two-factor authentication method for your super administrator account as needed.

1. Log in to PBX administrator portal with super administrator account, click your account at the top-right corner, then go to **Change Password & Security > Security Settings**.

2. Click beside the current authentication method.
3. Select the desired method, then complete the follow-up settings accordingly.

Disable two-factor authentication

Disable two-factor authentication for your account

You can disable two-factor authentication for your super administrator account at any time.

1. Log in to PBX administrator portal with super administrator account, click your account at the top-right corner, then go to **Change Password & Security > Security Settings**.
2. Unselect the checkbox of **Two-Factor Authentication**.
3. In the pop-up **Password** window, enter your account password and click **Confirm** to verify your operation.
4. In the **Security Settings** tab, click **Save**.

   The webpage prompts a message "Edited successfully.", which means that you have successfully disabled two-factor authentication.

Disable two-factor authentication for your extension user

If your extension user lost access to their two-factor authentication (e.g. they lost their authenticator device or could not receive authentication code via email), you can disable the two-factor authentication for their extension accounts, so that they can directly log in with username and password.

1. Log in to PBX web portal, go to **Extension and Trunk > Extension**.
2. Click beside the extension, then click the **Security** tab.
3. Scroll down to the **Login Security** section, then unselect the checkbox of **Two-Factor Authentication**.
4. In the pop-up **Password** window, enter your account password and click **Confirm** to verify your operation.
5. Click **Save**.

   The two-factor authentication of the extension account is disabled.

Related information

Configure Two-factor Authentication using Authenticator Application
Configure Two-factor Authentication using Email

Enforce Two-factor Authentication for All Extension Users

Enforce Two-factor Authentication for All Extension Users

To enhance security for users' accounts, you can make Two-Factor Authentication (2FA) mandatory for all extension users. In this way, users will be required to go through two-factor authentication when logging in using their extension username and password, thus preventing unauthorized access.

Requirements

- Yeastar P-Series Software Edition is 83.14.0.24 or later.
- Linkus Desktop Client is 1.4.9 or later.

Procedure

1. Log in to PBX web portal, go to **Security > Security Settings > Security Options**.
2. In the **Two-Factor Authentication** section, select the checkbox of **Make Two-Factor Authentication Mandatory for All Extensions**.

3. Click **Save**.

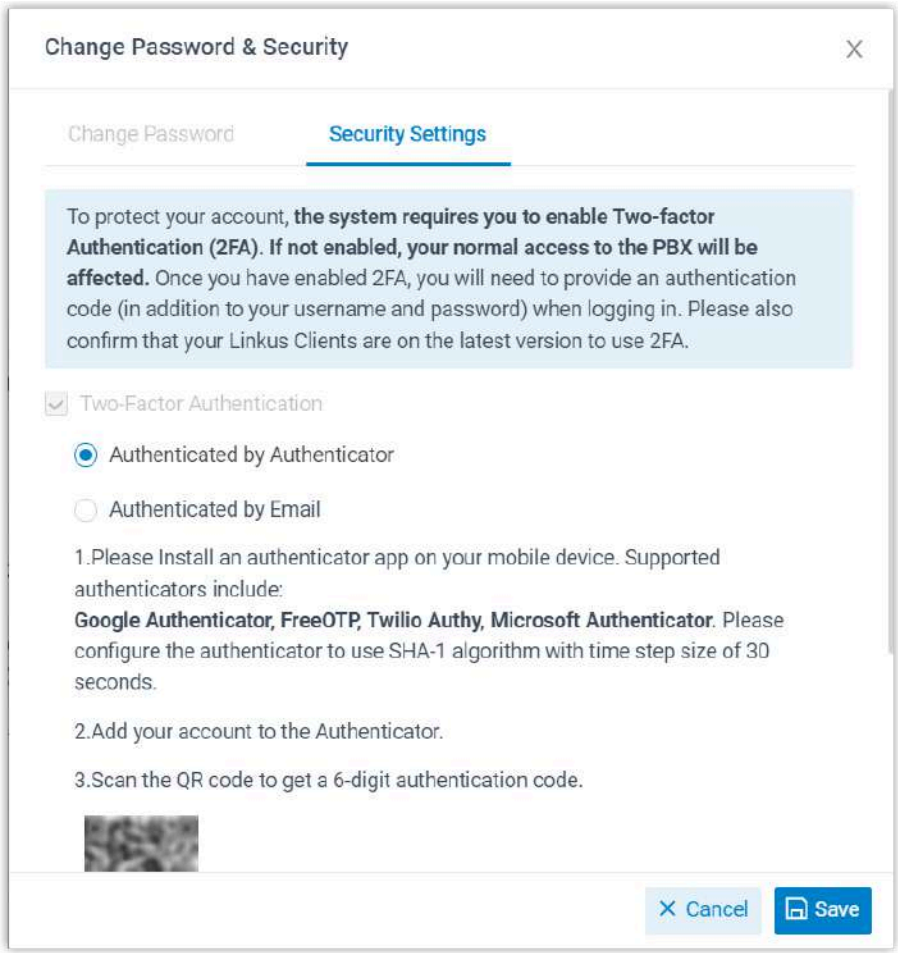
Result

The result varies depending on whether the two-factor authentication (2FA) feature is enabled on user's Linkus clients:

- **2FA is already enabled on users' Linkus clients**

  These users will not experience any interruption in using Linkus.
- **2FA is disabled on users' Linkus clients**

Users who attempt to log in or are already logged in Linkus Web Client or Desktop Client using their extension username and password, the two-factor authentication setup window will pop up, requiring the users to complete the 2FA setup for their accounts. Otherwise, their accounts will be automatically logged out.



Maintenance

Upgrade

Check for Available Firmware Updates

This topic describes how to automatically or manually check for firmware updates.

Automatic check for firmware updates

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.

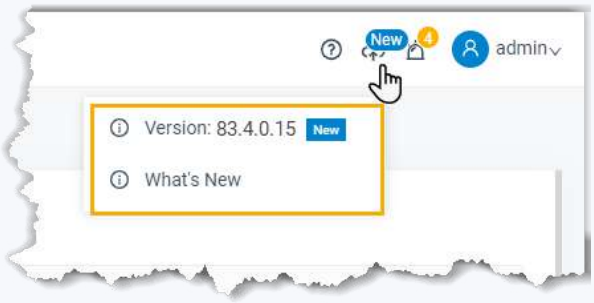
Procedure

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, 
>
> is displayed. Click 
>
> , click **What's New** to check release notes for the new version or click **Version** to go to upgrade page.



- The system will notify you via specific notification methods if you have enabled notification for **New System Firmware Detected** event.

Manual check for firmware updates

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.

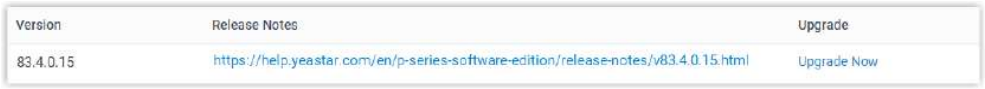
Prerequisites

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:

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**
- **Chat Data for External Chat**
- **License Code and FQDN 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 drive or 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**
     - **Chat Data for External Chat**
     - **License Code and FQDN Settings**

3. Click **Save**.

Result

The created backup file is displayed in **Backup and Restore** list and is stored in the selected location.

> **Tip:**
> You can archive the backup file to external servers via FTP, SFTP, Amazon S3, and Google Cloud Storage services for less space occupying and minimized data loss risk on PBX, as well as easier file management on external server. For more information, see Yeastar P-Series Software Edition Remote Archiving Overview.

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 drive or 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 back-up.
        - **Frequency**: Choose to make a daily, weekly, or monthly backup.
            - **Daily**: If you choose the option, select a time from the drop-down list. The system backs up the settings at this time of the day.
            - **Weekly**: If you choose the option, choose a day of week and select a time from the drop-down list. The system backs up the settings at this time of the week.
            - **Monthly**: If you choose the option, choose a day and select a time from the drop-down list. The system backs up the settings on this day and time of the month.
    b. In the **Storage Location** drop-down list, select where you want to save the backup file.

        > **Note:**
        > To prevent backup failure in case of disconnection to 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**
        - **Chat Data for External Chat**
        - **License Code and FQDN 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.

Tip:
You can archive the backup file to external servers via FTP, SFTP, Amazon S3, and Google Cloud Storage services for less space occupying and minimized data loss risk on PBX, as well as easier file management on external server. For more information, see Yeastar P-Series Software Edition Remote Archiving Overview.

Restore Your System from a Backup

In case of data loss or system failure, you can restore the PBX from a backup. This topic describes how to restore data on the PBX.

Prerequisites

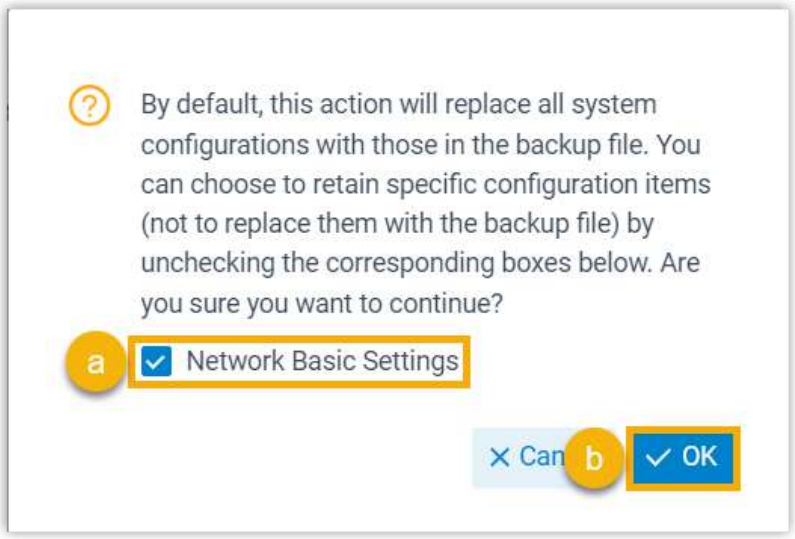
- Make sure that you have backed up system configurations and required files, such as custom prompts and CDR.
- Read and understand restrictions for data restoration.
  - You can restore a backup file that is created from an older version of PBX.

    Example: Restoring a backup file (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 window, do as follows:



a. If you want to retain existing network basic settings (the settings on **System > Network > Basic Settings**), unselect the checkbox of **Network Basic Settings**.
b. Click **OK**.

4. Reboot the PBX to take effect.

Result

The current configurations on your PBX are OVERWRITTEN with the backup data.

Related information

Create an On-Demand Backup
Set up an Automatic Backup Schedule

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.
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 35.

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 35. (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.

Enable Core Call Service Anomaly Detection

Anomaly in core call service will cause registration dropouts and call failures. Yeastar P-Series Software Edition can minimize the impact by automatically detecting the health of core call service and initiating a recovery process when any abnormalities are detected.

Requirements

The firmware version of Yeastar P-Series Software Edition is 83.15.0.22 or later.

Procedure

1. Log in to PBX web portal, go to **Maintenance > Troubleshooting > Advanced**.
2. Turn on the option **Core Call Service Anomaly Detection**, then configure the following settings:
   - **Detection Interval (s)**: Enter the interval between each detection to determine how frequently the system will check for core call service anomaly.

     > **Note:**
     > The value you enter should not be smaller than 10.

   - **Anomaly Confirmation Delay (s)**: Enter the waiting time before confirming a core call service anomaly after it is detected.

     > **Note:**
     > The value you enter should not be smaller than 30.

3. **Optional:** To allow the system to automatically initiate a recovery process after confirming a core call service anomaly, select the checkbox of **Automatic Recovery from Abnormality**.

   > **Note:**
   > During the recovery, all ongoing calls will be disconnected.

4. Click **Save** and **Apply**.

Result

The system will periodically check for the health of core call service.

- If core call service is found abnormal, the **Abnormal Core Call Services** event will be triggered to notify the relevant contacts.
- If automatic recovery is enabled, the system will automatically initiate a recovery process when any abnormalities are detected. Once the core call service is successfully recovered, the **Core Call Services Recovery Completed** event will be triggered to notify the relevant contacts.

> **Note:**
> If the core call service is not recovered, you can download system logs and contact Yeastar for support.

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 36.

	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 37.

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.

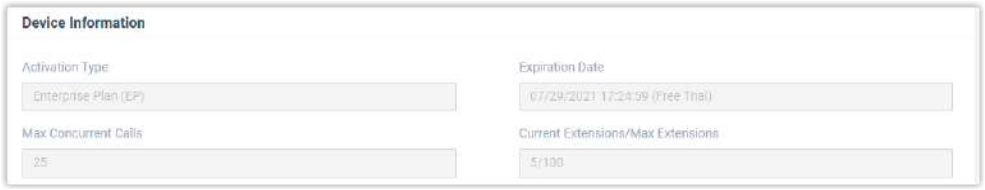
Procedure

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.



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

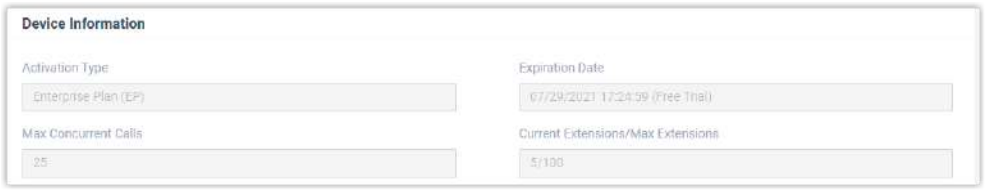
1. Log in to the PBX web portal, go to **Maintenance > Activation**.
2. In the **Activation Method** drop-down list, select **Offline**.
3. Click **Download Request File** and send the request file to your PBX provider to get an activation code.
4. In the **Activation Code** field, enter the activation 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.



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.

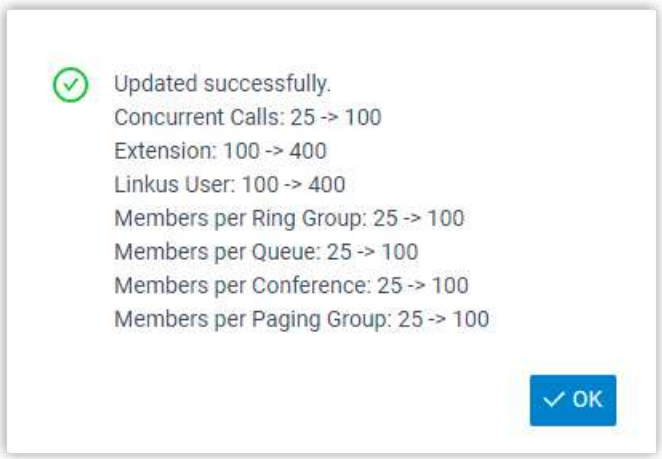
Procedure

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.



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**
- **Enable OpenAPI Event Notification Message Debug**

Storage of system logs

System logs are saved in local storage, you can NOT change the storage location.

Auto cleanup of system logs

By default, the system automatically deletes the oldest system logs every 7 days, or when logs reach 10MB. You can change the maximum file size or days that logs can be retained. For more information, see Auto Cleanup Settings.

Related information

Configure Log Level
Manage System Logs
Forward System Logs to a Third-party Syslog Server

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**
     - **Enable OpenAPI Event Notification Message Debug**
4. Click **Save** and **Apply**.

Result

The system will generate logs of the specified levels every day.

Related information

Forward System Logs to a Third-party Syslog Server

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**.

Related information

Forward System Logs to a Third-party Syslog Server

Forward System Logs to a Third-party Syslog Server

By default, PBX system automatically and periodically deletes the oldest system logs. To ensure comprehensive logging for routine troubleshooting and incident handling, you can con-

figure the PBX to forward system logs to a third-party syslog server (either local or remote) via Syslog protocol over UDP, TCP, or TLS, thus guarantee centralized logging and long-term storage.

Requirements

Yeastar P-Series Software Edition is 83.17.0.60 or later.

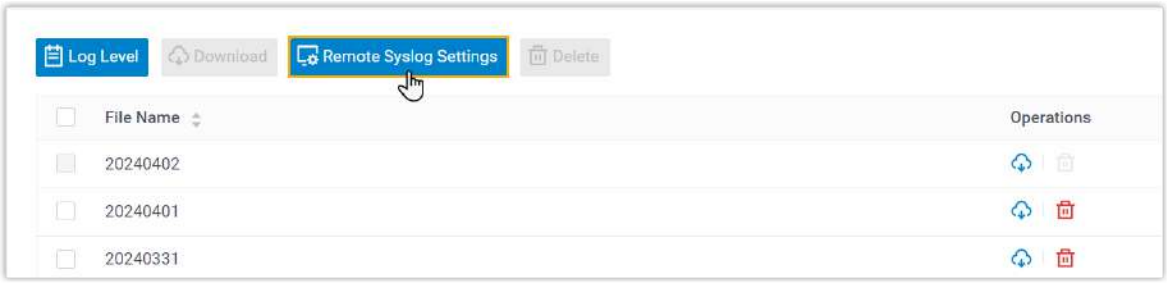
Prerequisites

You have set up a syslog server, and obtain the following information of the server:

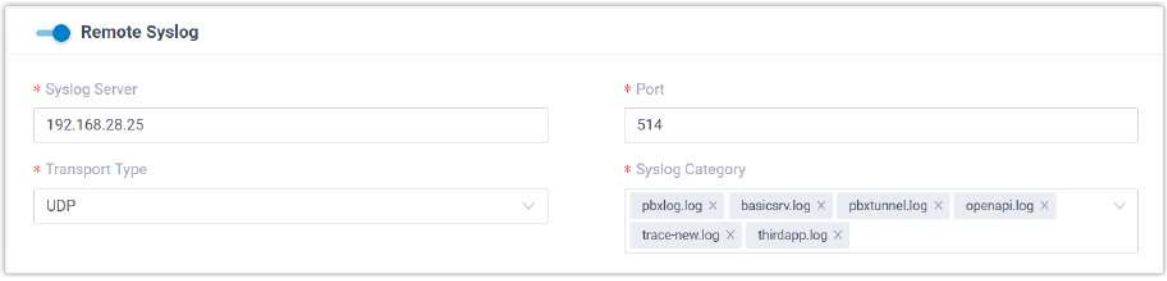
- IP address or hostname
- Supported transport protocol and the corresponding port

Procedure

1. Log in to PBX web portal, go to **Maintenance > System Logs**.
2. In the top menu, click **Remote Syslog Settings**.



3. Turn on the switch of **Remote Syslog**, and complete the following settings.



   - **Syslog Server**: Enter the IP address or hostname of the syslog server.
   - **Port**: Enter the port number to connect to the syslog server.
   - **Transport Type**: In the drop-down list, select the transport type that the syslog server supports.

> **Note:**

To forward system logs over TLS, you must enable TLS encryption, and upload the required certificate and key on the syslog server.

- **Syslog Category**: In the drop-down list, select the log categories to forwarded to the syslog server.

Note:
The information contained in the system logs depends on the log level settings (Path: **Maintenance > System Logs > Log Level**).

The following table lists the supported system log categories and the information they include.

Category	Description
pbxlog.log	Logs that provide detailed information about extension registration and PBX calls (call establishment, dialling rule matching, and call duration, etc.). These logs can be used to analyze call quality and investigate call issues.
basicsrv.log	Logical logs of using PBX features, such as Operator Panel, Queue Panel, Hot Standby, and other non-call related features. These logs can be used to track system operating behavior, detect abnormal situations, and conduct performance analysis.
pbxtunnel.log	Logs about the Yeastar PBX FQDN tunnel, including connection establishment and heartbeat detection. These logs can be used to monitor tunnel connection status, and troubleshoot connection issues.
openapi.log	Logs about API calls in the system, including interface requests, parameter transmission, and response results. These logs can be used to track API calls, troubleshoot interface issues, and analyze interface performance.
trace-new.log	Logs of system process status, including startup, shutdown, and abnormal exit of guardian processes, as well as inter-process communication and collaboration. These logs can be used for debugging and tracing purposes.
thridapp.log	Logs of third-party integrations, including the process and results of the integration with third-party systems or services. For example, CRM-related logs record the data interaction between the CRM system and PBX system.

Category	Description
	These logs can be used to monitor data synchronization and exchange, troubleshoot integration issues, etc.
apigateway.log	Logs of API Gateway that records the internal process of API Gateway, which involves rate limiting and circuit breaking when the PBX system receives large amounts of API requests. These logs can be used to monitor traffic management and actions of circuit breaking.

4. Click **Save**.

Result

PBX system starts to forward the selected system logs to the syslog server in real time.

CDR and Reports

CDR

Call Detail Record (CDR) Overview

The Call Detail Record (CDR) feature provides information about calls over Yeastar P-Series Software Edition. This topic describes parameters and auto cleanup of CDR.

CDR parameters

A CDR contains the following information:

Item	Description
ID	A unique identifier for each call.
Time	When the call was made or received.
Call From	The number or the name of the caller.
Call To	The number or the name of the callee.
Call Duration	The time between the call started and the call ended.
Ring Duration	The time between the call started and the call answered.
Talk Duration	The time between the call answered and the call ended.
Status	Call status. • **ANSWERED** • **NO ANSWER** • **BUSY** • **FAILED** • **VOICEMAIL**
Reason	The reason why the call was ended.
Call Notes	The call notes added for each call.
Source Trunk	The call was received via which trunk.
Destination Trunk	The call was sent out via which trunk.
Communication Type	Communication Type. • **Internal** • **Outbound**

Item	Description
	• **Inbound**
DID/DDI	The phone number that the caller dialed.
Outbound Caller ID	The phone number that was displayed on the callee's phone.
Caller IP Address	The IP address of the caller's device.
PIN Code	The PIN code entered when making a call via a restricted outbound route.
Recording File	The call recording file.

CDR auto cleanup

By default, when the number of call logs reaches 200,000 (extensions <1000) or 1,000,000 (extensions ≥1000) , the system will automatically delete the oldest call logs (relevant recordings are retained.). You can change the maximum value, or you can also set the maximum preservation days. For more information, see Auto Cleanup Settings.

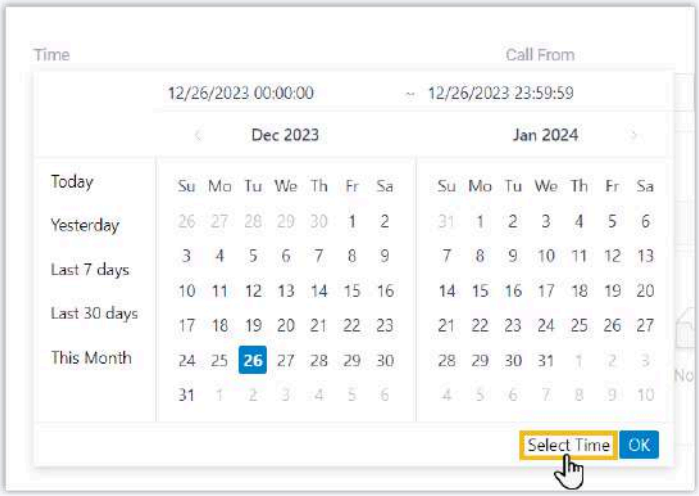
View and Manage CDR

This topic describes how to view, download, and delete CDR.

View CDR

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. **Optional:** Set the basic filter criteria.

Filter	Description
Time	Set the start date and the end date. **Note:** To specify a time period of a day, click **Select Time** to set the start time and the end time.

Filter	Description
	
Call From	Enter the caller's number or name.
Call To	Enter the callee's number or name. **Tip:** To swap the callee for the caller, click ⇋.
Status	Select a call status. • **All** • **ANSWERED** • **NO ANSWER** • **BUSY** • **FAILED** • **VOICEMAIL**

3. **Optional:** Set the advanced filter criteria.

   a. Click .

   b. On the **Filter** page, set the advanced criteria.

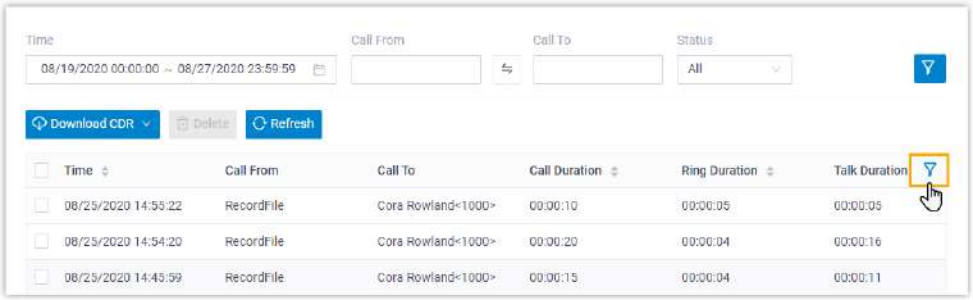
Option	Description
Queue	Select a queue. The system only queries the queue's calls.
Extension Group	Select an extension group. The system only queries the group members' calls.
Call Disposition	Select call disposition code(s).

Option	Description
Remark	Enter the remark added for the call.
Ring Duration	Enter how long the callee's phone rang before the call was answered. **Note:** Only numbers, `-`, =,<, <=, >, and >= are allowed.
Talk Duration	Enter the time between the call was answered and the call was ended. **Note:** Only numbers, `-`, =,<, <=, >, and >= are allowed.
Status	Select call status. • **All** • **ANSWERED** • **NO ANSWER** • **BUSY** • **FAILED** • **VOICEMAIL**
Communication Type	Select communication type. • **All** • **Internal** • **Outbound** • **Inbound**
ID	Enter the unique ID for a call.
Trunk	Select a trunk. The system only queries calls that are sent or received via the trunk.
Enable Number Fuzzy Search	Set whether to search for the fuzzy equivalent for the phone number.
DID	Select a DID number. The system only queries the calls that match this DID number.
PIN Code	Enter an existing PIN code. The system only queries the calls using this PIN code.

c. Scroll up to click ✕ to close the window.
The filtered call logs are displayed on the page.

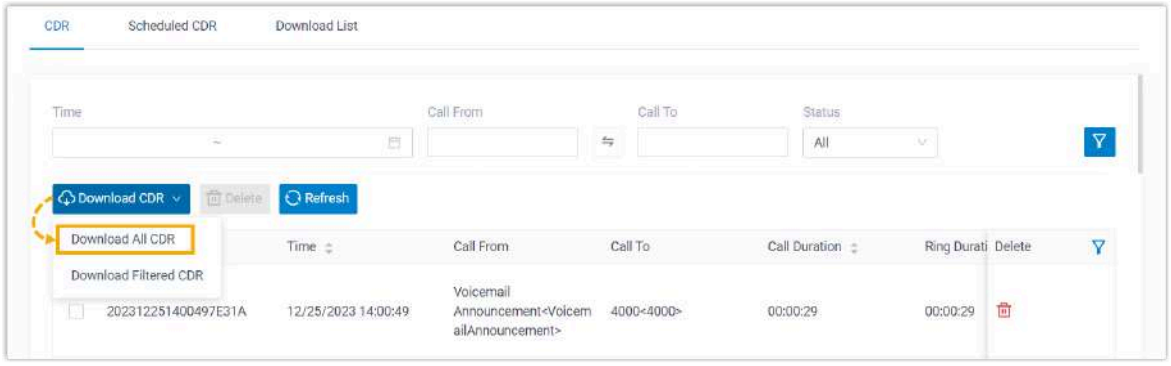
Note:

You can click to decide which item will be displayed.

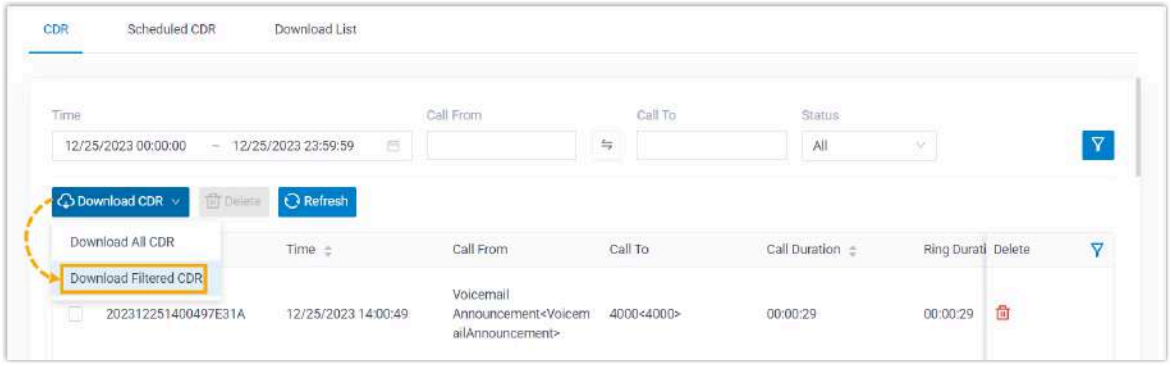


Download CDR

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. To download all the call logs, select **Download All CDR** from the drop-down list of **Download CDR**.



3. To download the filtered call logs, set the filter criteria and select **Download Filtered CDR** from the drop-down list of **Download CDR**.



CDR are exported to a CSV file.

Delete CDR

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. **Optional:** Filter call logs.
3. Select the checkboxes of the desired call logs, click **Delete** and **OK**.

> **Important:**
> The relevant recording files will also be deleted.

Both call logs and recording files are deleted.

Scheduled CDR

Schedule CDR to Email

Yeastar P-Series Software Edition allows you to schedule CDR to be sent to specific recipients' mailboxes at the specified time. The recipients can access the CDR via a link attached in the email and download it as a CSV, XLS, or PDF file.

Restrictions

- Only super administrator and the authorized users can schedule CDR to email.
- The maximum number of CDR that can be downloaded at one time varies depending on the file format of the downloaded CDR.
  - **CSV**: 10,000 (Extension < 1000) or 100,000 (Extension ≥ 1000)
  - **XLS**: 10,000 (Extension < 1000) or 100,000 (Extension ≥ 1000)
  - **PDF**: 5,000

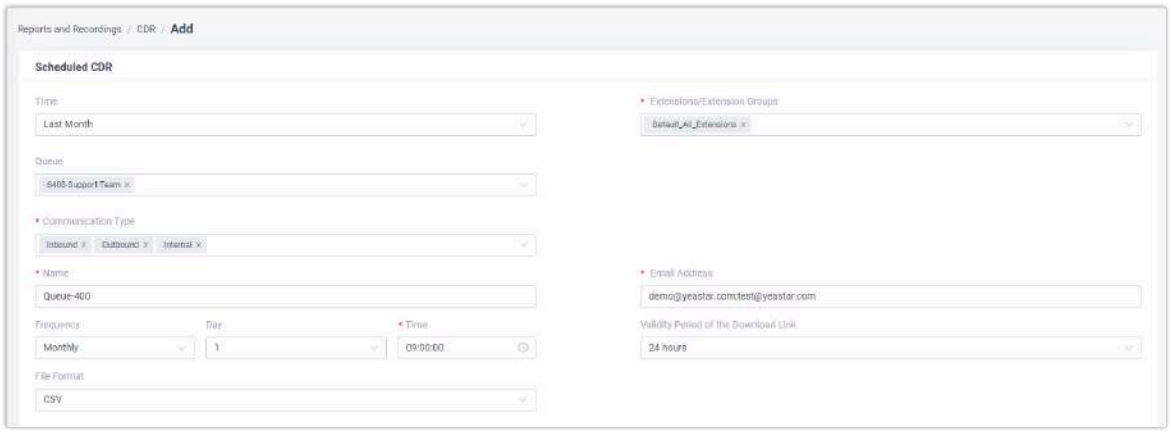
Prerequisites

Make sure email server works.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. Under the **Scheduled CDR** tab, click **Add**.

3. Schedule a task to send CDR via email.



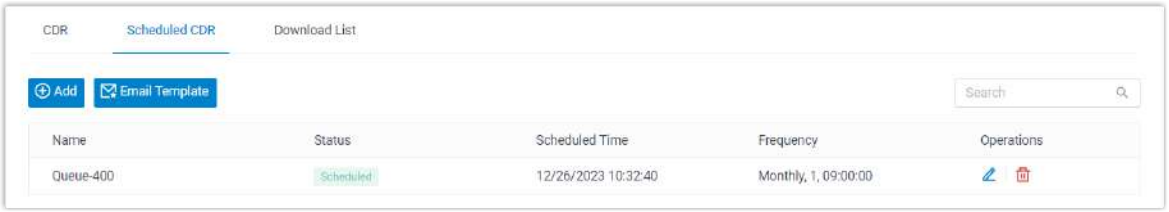
Setting	Description
Time	Select a time range to filter CDR.
Extensions/Extension Groups	Select extension(s) or extension group(s) to filter CDR.
Organization	Select department(s) to filter CDR.
Queue	Select call queue(s) to filter CDR.
Communication Type	Select communication type(s) to filter CDR.
DID	Select DID number(s) to filter CDR.
Name	Enter a name to help you identify the task.
Email Address	Enter recipients' email addresses. **Note:** You can set up to 10 email addresses; Separate multiple email addresses by semicolon `;`.
Frequency	Set how often to send CDR. • **Once**: If selected, the system will send the CDR immediately after you save the task. • **Daily**: If selected, choose a specific time from the drop-down list. The system will send the CDR at the selected time each day. • **Weekly**: If selected, choose a specific day of the week and select a specific time from the drop-down list. The system will send the CDR at the selected day and time each week. • **Monthly**: If selected, choose a specific day of the month and select a specific time from the drop-down list.

Setting	Description
	The system will send the CDR on the selected day and time each month.
Validity Period of the Download Link	Set the validity period of the download link for the scheduled CDR. After the link expires, the recipients can NOT access and download the CDR via the link.
File Format	Set in which file format the CDR can be downloaded. • **CSV** • **XLS** • **PDF**

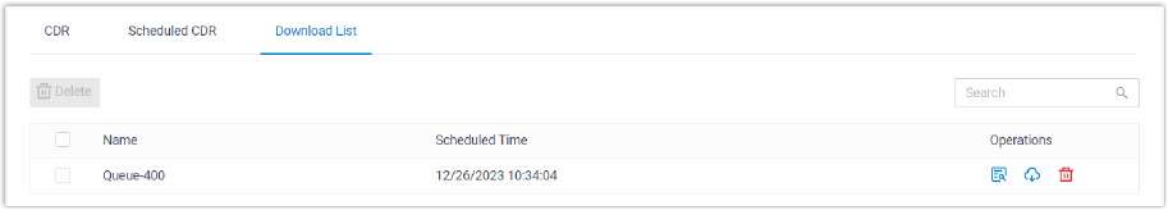
4. Click **Save**.

Result

- The task is scheduled and displayed in the list.



- When it comes to the scheduled time, the specified CDR will be automatically sent to the specified recipients' mailboxes; You can also check the CDR in the **Download List** tab, either by clicking to preview the CDR online, or by clicking to download the CDR for offline viewing.



Related information

Manage Scheduled CDR Tasks
Customize Email Template for Scheduled CDR

Manage Scheduled CDR Tasks

This topic describes how to edit and delete scheduled CDR tasks.

Edit a scheduled CDR task

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. Under the **Scheduled CDR** tab, click beside the desired task.
3. Edit the task according to your needs.
4. Click **Save**.

Delete a scheduled CDR task

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. Under the **Scheduled CDR** tab, do as follows:
   a. Click beside the desired task.
   b. In the pop-up window, click **OK**.

Download Scheduled CDR on PBX Web Portal

After the system sends scheduled CDR to recipients' mailboxes, the recipients can preview and download the CDR via an attached link, while you can also view and download the CDR on PBX web portal. This topic describes how to download scheduled CDR on PBX web portal.

Prerequisites

A scheduled CDR task has been performed successfully.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. Under **Download List** tab, click beside the desired scheduled CDR task.

Result

The CDR is downloaded to your computer in the pre-defined file format.

Customize Email Template for Scheduled CDR

This topic describes how to customize the email template for scheduled CDR.

Background information

By default, Yeastar P-Series Software Edition sends scheduled CDR in the pre-defined language and in a default email template.

The language is what you have set in system email template, and the default email template contains the following information:

- A download link for CDR.
- Soft reminder of the download link.
  - The validity period of the download link.
  - If the PBX hasn't configured Yeastar FQDN or a public IP address, the download link can only be accessed over the same local network as the PBX.
- System information, including PBX name, PBX serial number, PBX LAN IP address, and PBX WAN IP address.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > CDR**.
2. Under the **Scheduled CDR** tab, click **Email Template**.
3. Configure template settings.
   a. In the **Template** drop-down list, select **Custom**.
   b. Edit email subject and content according to your needs.
   c. Click **Save**.

Result

The PBX will send scheduled CDR using the customized email template.

Call Report

Call Reports Overview

Yeastar P-Series 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
- IVR Report
- Unreturned Missed Call Report
- Queue AVG Waiting & Talking Time
- Queue Performance
- Queue Performance Activity
- Queue Callback Summary
- Queue Callback Activity
- Satisfaction Survey
- Satisfaction Survey Details
- Agent Login Activity
- Agent Pause Activity
- Agent Missed Call Activity
- Agent Performance
- Agent Call Summary
- Ring Group Statistics
- Extension Call Accounting
- Extension Call Accounting Details

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

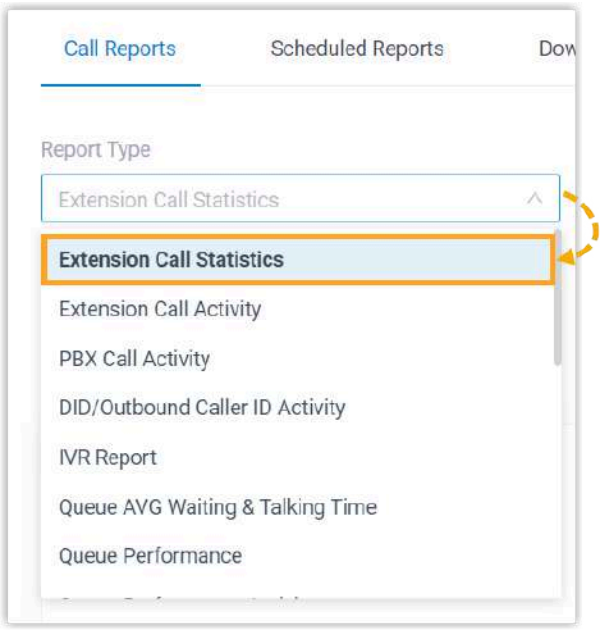
Relevant call statistics are displayed on the page.

Extension Call Statistics Report

Extension Call Statistics report provides a quick overview of the number of calls that have been made and received by extension(s), and can be broken down to specific extensions, groups of extensions, or organizations of extensions. This topic introduces how to access the report and explains the key metrics in detail.

Access Extension Call Statistics report

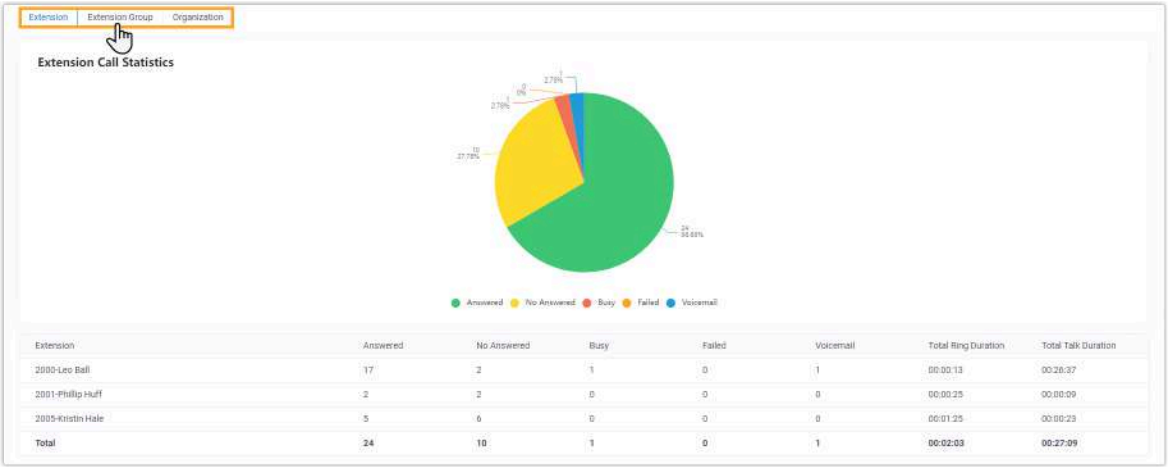
1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Extension Call Statistics**.



3. Filter data by system time, extension(s), extension group(s), organization(s), or communication type.

> **Note:**
> **Organization** filter is displayed only when you enable **Organization Management** feature (Path: **PBX Settings > Preferences**).

A report that meets the filter criteria is displayed on the page, as shown below.



Note:

- You can click the tab at the top-left corner to switch between the break-down reports.
- If you filter data by organization(s), the report data will include the selected organization and its subordinate departments.

Report details

We take the above report as an example to introduce the key metrics for **Extension Call Statistics** report.

Metric	Description
Answered	The total number of calls that the extension(s) answered.
No Answered	The total number of calls that were routed to the designated destination when the extension(s) didn't answer the calls.
Busy	The total number of calls that were routed to the designated destination when the extension(s) was busy.
Failed	The total number of calls that were failed to be made by the extension(s).
Voicemail	The total number of voicemails that the extension(s) received.
Total Ring Duration	The total time between calls started and calls answered. **Note:** This metric is displayed only when you set **Communication Type** filter to **All**, **Inbound**, **Outbound**, or **Internal**.
Total Talk Duration	The total time between calls answered and calls ended.
Total (displayed in row)	The sum of all the values in each column. **Note:** • This metric is only available for extension and extension group. • If you select multiple extension groups and one of the extensions belongs to two or more extension groups, the call statistics for the extension will be calculated more than once.
	The total number of calls for each communication type.

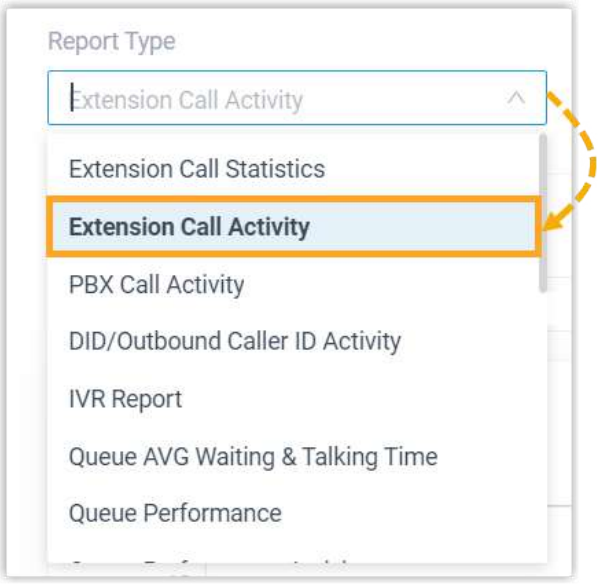
Metric	Description
Total (displayed in column)	**Note:** This metric is displayed only when you set **Communication Type** filter to **Inbound/Outbound**.

Extension Call Activity Report

Extension Call Activity report provides granular insights into the hourly, daily, and monthly breakdown of the number of calls that have been made or received by extension(s), and can be broken down to specific extensions, groups of extensions, or organizations of extensions. This topic introduces how to access the report and explains the key metrics in detail.

Access Extension Call Activity report

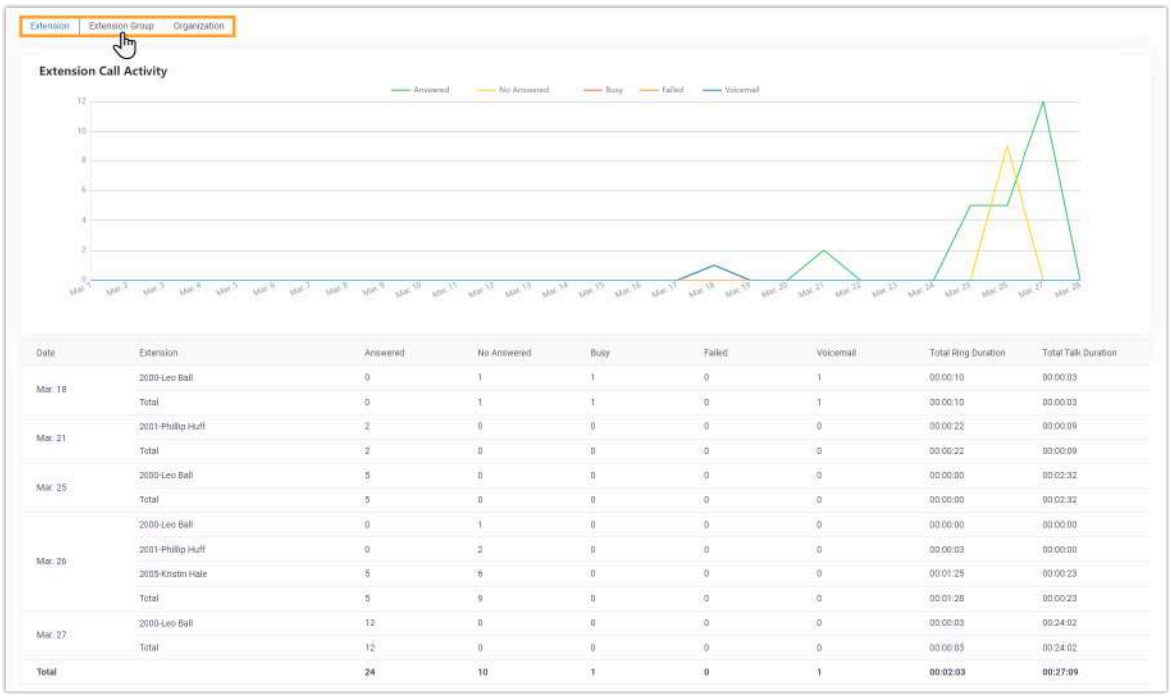
1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Extension Call Activity**.



3. Filter data by system date and time, extension(s), extension group(s), organization(s), or communication type.

> **Note:**
> **Organization** filter is displayed only when you enable **Organization Management** feature (Path: **PBX Settings > Preferences**).

A report that meets the filter criteria is displayed on the page, as shown below.



Note:

- You can click the tab at the top-left corner to switch between the break-down reports.
- If you filter data by organization(s), the report data will include the selected organization and its subordinate departments.

Report details

We take the above report as an example to introduce the key metrics for **Extension Call Activity** report.

Metric	Description
Answered	The total number of calls that the extension(s) answered.
No Answered	The total number of calls that were routed to the designated destination when the extension(s) didn't answer the calls.
Busy	The total number of calls that were routed to the designated destination when the extension(s) was busy.

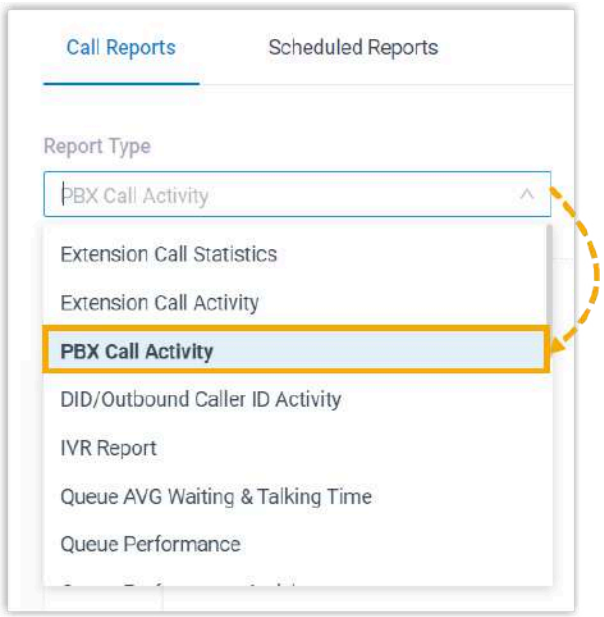
Metric	Description
Failed	The total number of calls that were failed to be made by the extension(s).
Voicemail	The total number of voicemails that the extension(s) received.
Total Ring Duration	The total time between calls started and calls answered.
Total Talk Duration	The total time between calls answered and calls ended.
Total (displayed in row)	The sum of all the values in each column. **Note:** • This metric is only available for extension and extension group. • If you select multiple extension groups and one of the extensions belongs to two or more extension groups, the call statistics for the extension will be calculated more than once.

PBX Call Activity Report

PBX Call Activity report provides granular insights into the hourly, daily, and monthly break-down of internal calls and external calls. This topic introduces how to access the report and explains the key metrics in detail.

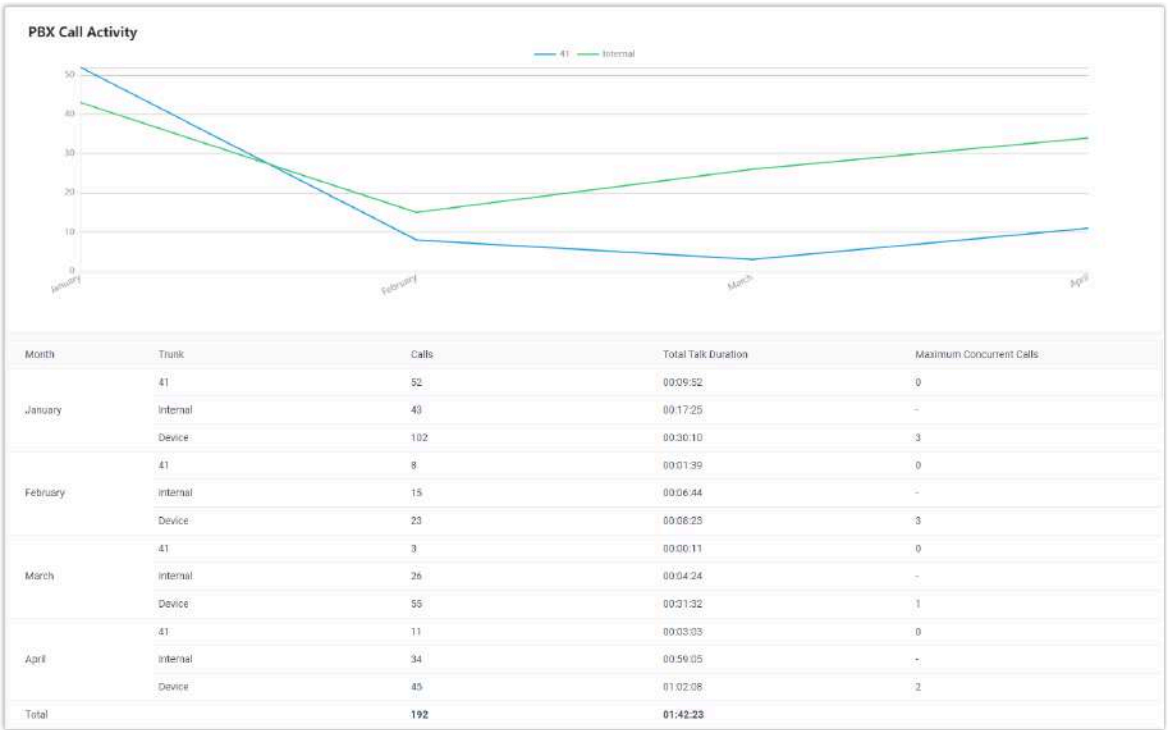
Access PBX Call Activity report

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **PBX Call Activity**.



3. Filter data by system time, trunks, call type, or communication type.

A report that meets the filter criteria is displayed on the page, as shown below.



Month	Trunk	Calls	Total Talk Duration	Maximum Concurrent Calls
January	41	52	00:09:52	0
	Internal	43	00:17:25	-
	Device	102	00:30:10	3
February	41	8	00:01:39	0
	Internal	15	00:06:44	-
	Device	23	00:08:25	3
March	41	3	00:00:11	0
	Internal	26	00:04:24	-
	Device	55	00:31:32	1
April	41	11	00:03:03	0
	Internal	34	00:59:05	-
	Device	45	01:02:08	2
Total		192	01:42:23	

Report details

We take the above report as an example to introduce the key metrics for **PBX Call Activity** report.

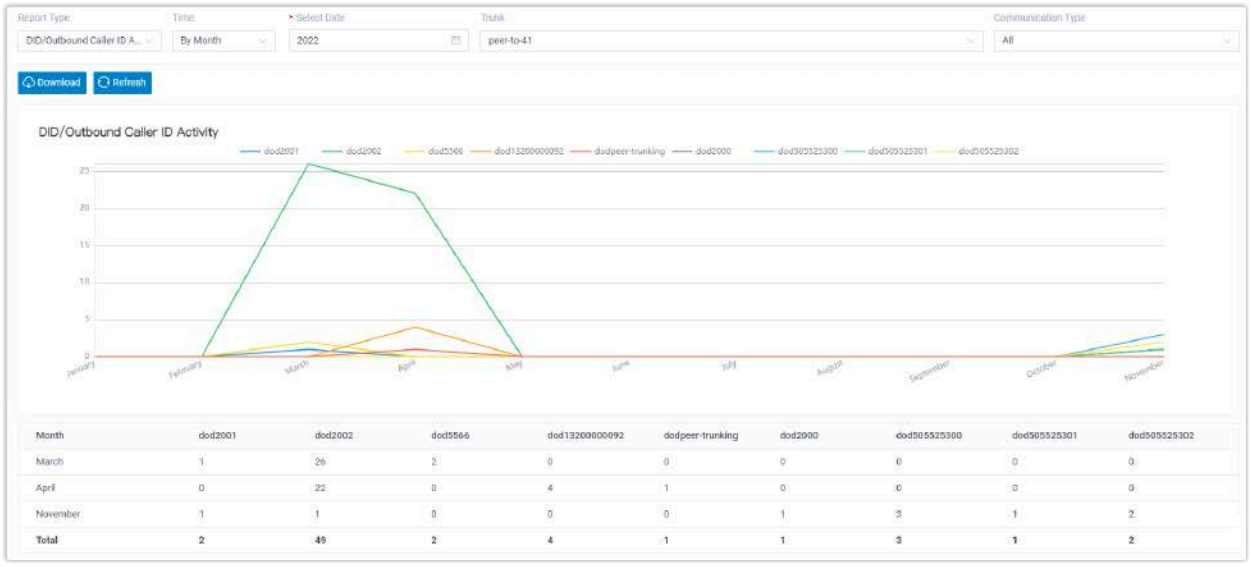
Metric	Description
Trunk	Trunk name. • *{trunk_name}*: Calls that are made or received via trunks. • **Internal**: Calls that are made between extensions. • **Device**: Calls of the entire system (including internal calls, inbound and outbound calls on all the trunks). **Note:** This value is displayed only when **Communication Type** filter is set to **All**.
Calls	The total number of calls that were made or received.
Total Talk Duration	The total time between calls answered and calls ended.
Maximum Concurrent Calls	The maximum number of concurrent calls within the time frame. **Note:** • Calls between extensions and the calls received from WebRTC trunks do NOT support the calculation of maximum concurrent calls. • For **Trunk** displayed as **Device**, it calculates the maximum concurrent calls for the entire phone system.
Total (displayed in row)	Total number of calls and total talk duration. **Note:** This shows the sum of the data for internal calls and the selected trunks, excluding the data for the entire phone system (namely the data for **Trunk** displayed as **Device**).

DID/Outbound Caller ID Activity Report

DID/Outbound Caller ID Activity report is a summary report displayed in line graph, which allows you to track changes of DID/Outbound Caller ID activity by hour, by date, or by month.

Report example

The following report shows monthly DID/Outbound Caller ID statistics of the trunk **peer-to-41** on 2022.



Month	dod2001	dod2002	dod5566	dod13209000092	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.

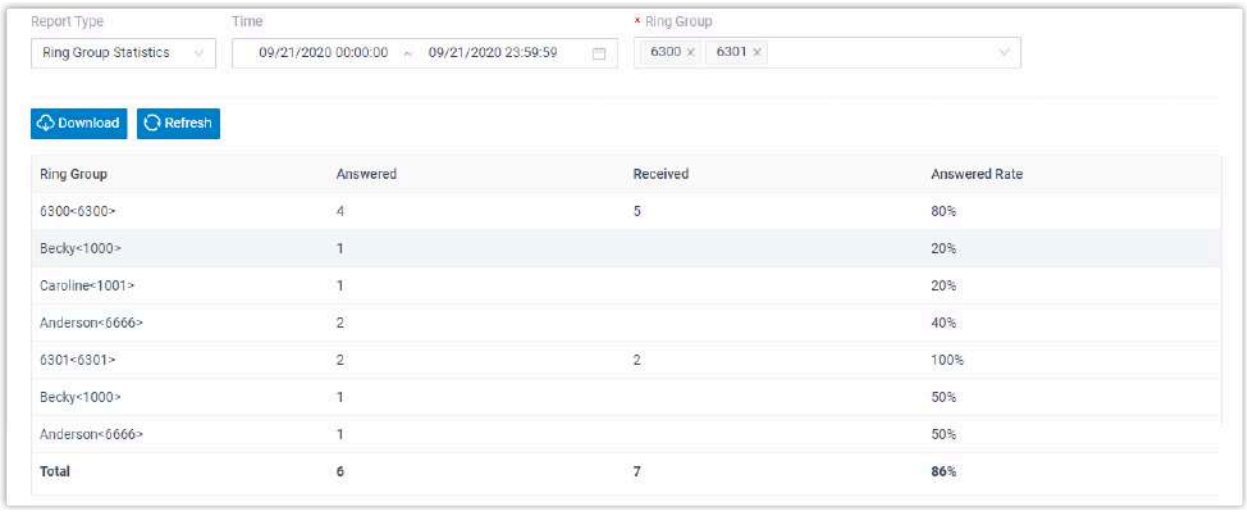
Report details

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.



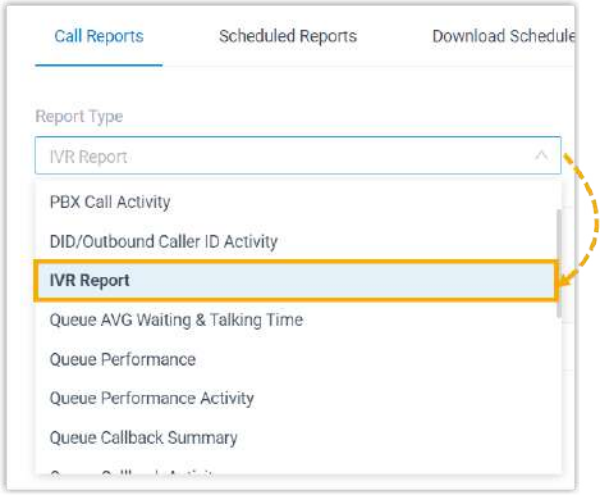
Ring Group	Answered	Received	Answered Rate
6300<6300>	4	5	80%
Becky<1000>	1		20%
Caroline<1001>	1		20%
Anderson<6666>	2		40%
6301<6301>	2	2	100%
Becky<1000>	1		50%
Anderson<6666>	1		50%
Total	**6**	**7**	**86%**

IVR Report

IVR report provides a quick overview of the keypress events for IVR as well as granular insights into the associated IVR calls. This topic introduces how to access the report and explains the key metrics in detail.

Access IVR Report

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **IVR Report**.

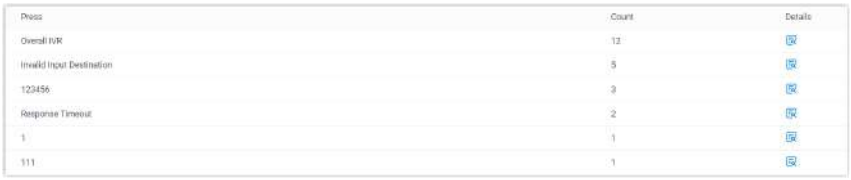


3. Filter data by system time, key type, and IVR(s).

A report that meets the filter criteria is displayed on the page, as shown below.

Figure 16. IVR with standard keys

Figure 16. IVR with custom keys



Report details

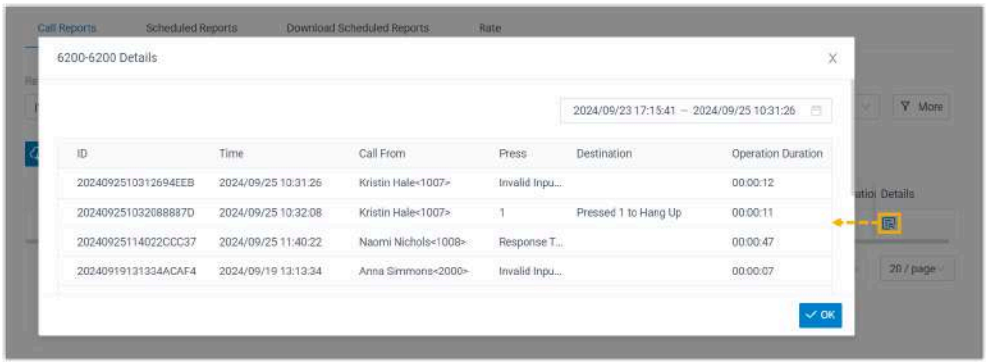
We take the above reports as examples to introduce the key metrics for **IVR** report.

IVR with standard keys

- **Metrics for IVR (with standard keys)**

Metric	Description
Press*key_pressed*	The number of times that the key was pressed.
Response Timeout	The number of times that IVR calls were routed to the timeout destination. **Note:** IVR calls will be routed to response timeout destination if no key was pressed after reaching the maximum **Prompt Repeat Count**.
Invalid Input Destination	The number of times that IVR calls were routed to the invalid input destination. **Note:** IVR calls will be routed to invalid input destination if callers repeatedly entered a DTMF digit that is not defined for the IVR after reaching the maximum **Prompt Repeat Count**.

- **Metrics for IVR call (with standard keys)**



Metric	Description
ID	A unique ID for the call.
Time	When the call was received.
Call From	The number and the name of the caller.
Press	The keypress event.
Destination	The destination of the call.
Operation Duration	The time between the caller called into the IVR and exited the IVR.

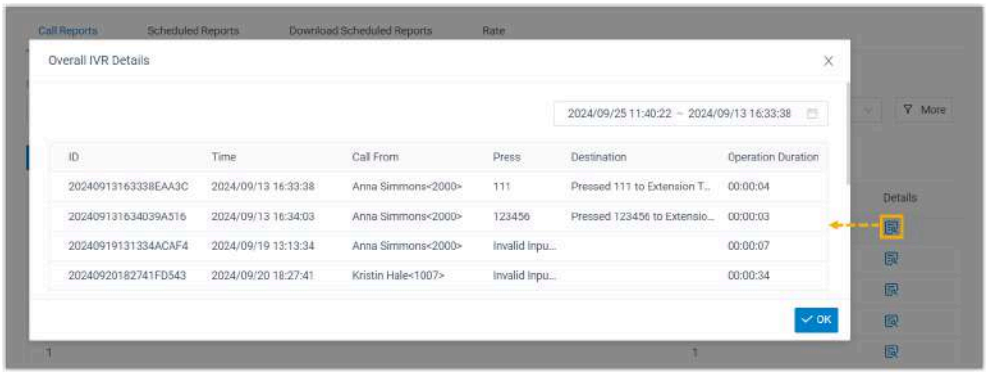
IVR with custom keys

- **Metrics for IVR (with custom keys)**

Metric	Description
Overall IVR	The number of times that all key press events in the IVR were triggered.
{key_pressed}	The number of times that the key was pressed.
Response Timeout	The number of times that IVR calls were routed to the timeout destination. **Note:**

Metric	Description
	IVR calls will be routed to response timeout destination if no key was pressed after reaching the maximum **Prompt Repeat Count**.
Invalid Input Destination	The number of times that IVR calls were routed to the invalid input destination. **Note:** IVR calls will be routed to invalid input destination if callers repeatedly entered a DTMF digit that is not defined for the IVR after reaching the maximum **Prompt Repeat Count**.

- **Metrics for IVR call (with custom keys)**



Metric	Description
ID	A unique ID for the call.
Time	When the call was received.
Call From	The number and the name of the caller.
Press	The keypress event.
Destination	The destination of the call.
Operation Duration	The time between the caller called into the IVR and exited the IVR.

Unreturned Missed Call Report

Unreturned Missed Call report provides a comprehensive overview of all the missed inbound calls, including callback status and details, which helps track missed call activities

and follow-up actions. This topic introduces how to access and download the report and explains the key metrics in detail.

Access Unreturned Missed Call Report

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Unreturned Missed Call Report**.

3. Filter data by the following criteria.

A report that meets the filter criteria is displayed on the page, as shown below.

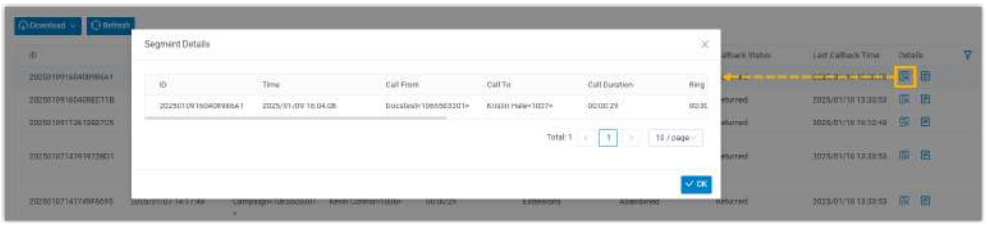
To understand each metric, refer to the following tables.

- Metrics for unreturned missed call
- Metrics for unreturned missed call details (segment details)
- Metrics for unreturned missed call details (callback details)

Metrics for unreturned missed call

Metric	Description
ID	A unique ID for the call.
Time	The time when the call was received.
Call From	The number or the name of the caller.
Call To	The number or the name of the callee.
Ring Duration	The time between the call started and the call answered.
Call Destination	The type of the destination to which the inbound call was routed. • Extension • Ring Group • Queue
Missed Call Type	The type of the missed call. • No Answered • Abandoned • Busy
Callback Status	Whether the missed call was returned or not. • Returned • Unreturned
Last Callback Time	The last time that the callback was made.

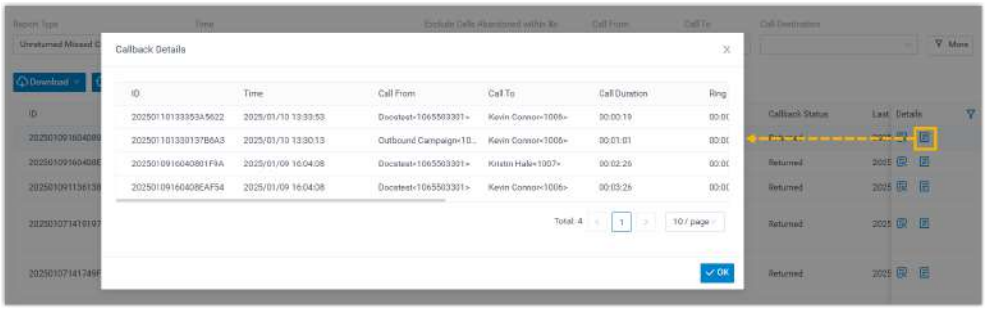
Metrics for unreturned missed call details (segment details)



Metric	Description
ID	A unique ID for the call.
Time	The time when the call was received.
Call From	The number or the name of the caller.

Metric	Description
Call To	The number or the name of the callee.
Call Duration	The time between the call started and the call ended.
Ring Duration	The time between the call started and the call answered.
Talk Duration	The time between the call was answered and the call ended.
Status	Whether the call was answered or not.
Reason	The reason why the call was missed.
Communication Type	The type of the call.

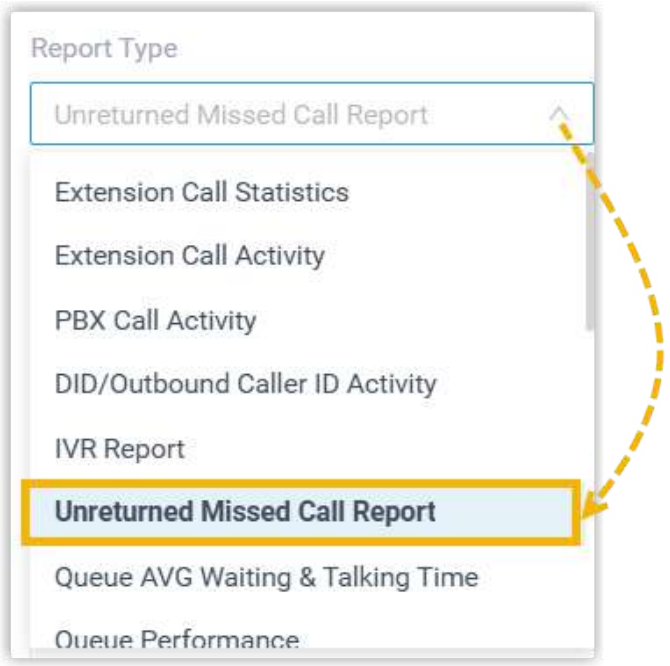
Metrics for unreturned missed call details (callback details)



Metric	Description
ID	A unique ID for the call.
Time	The time when the call was received.
Call From	The number or the name of the caller.
Call To	The number or the name of the callee.
Call Duration	The time between the call started and the call ended.
Ring Duration	The time that the callee's phone rang before the call was answered or disconnected.
Talk Duration	The time between the call was answered and the call ended.
Status	Whether the call was successful or not.
Reason	The reason why the call ended.
Communication Type	The type of the call.

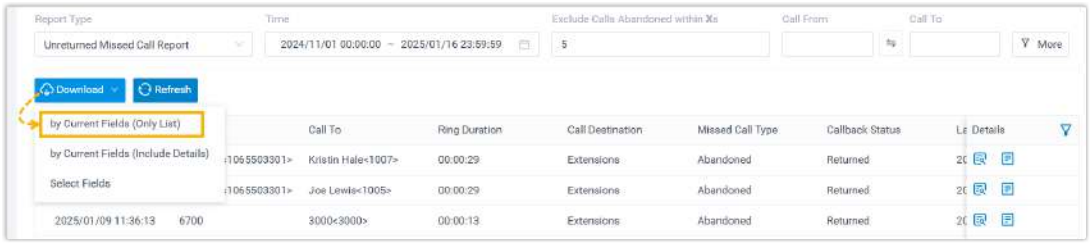
Download Unreturned Missed Call Report

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Unreturned Missed Call Report**.

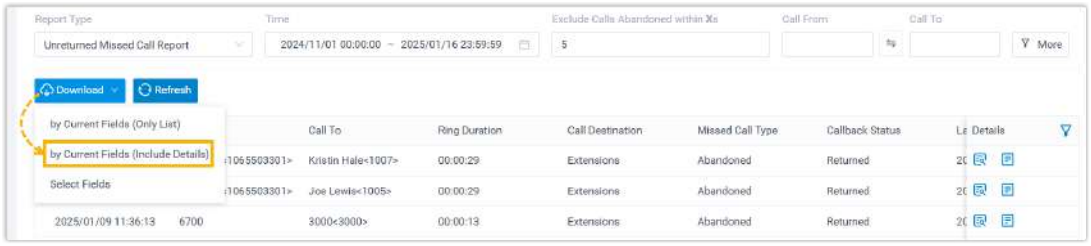


3. Filter data by the following criteria.

4. Download the report according to your needs.
   - To download the current displayed list of the report excluding details, do as follows:



     a. At the top of the list, click **Download**.
     b. In the drop-down list, select **by Current Fields (Only List)**.
   - To download the current displayed list of the report including details, do as follows:

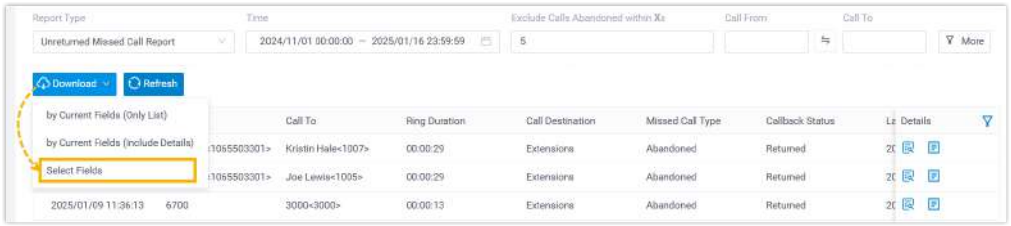


a. At the top of the list, click **Download**.

b. In the drop-down list, select **by Current Fields (Include Details)**.

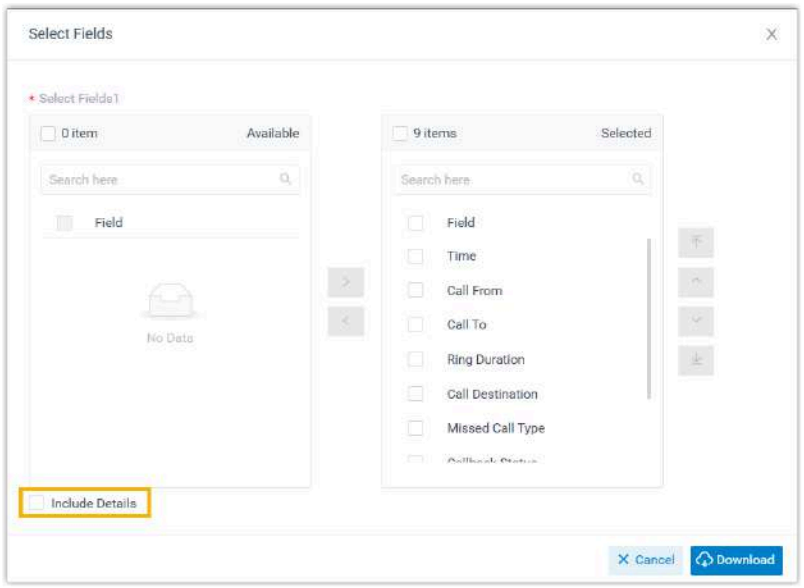
- To download reports with customized display fields, do as follows:

  a. At the top of the list, click **Download**, then select **Select Fields** from the drop-down list.



  b. In the pop-up window, select the desired fields which you want to display in the report, and decide whether to include details as needed.

> **Note:**
> By default, all fields will be displayed in the report.



  c. Click **Download**.

The unreturned missed call report is exported to a CSV file.

Scheduled Reports

Schedule Call Reports

This topic describes how to schedule a call report to be sent to specific recipients' mailboxes at the specified time.

Background information

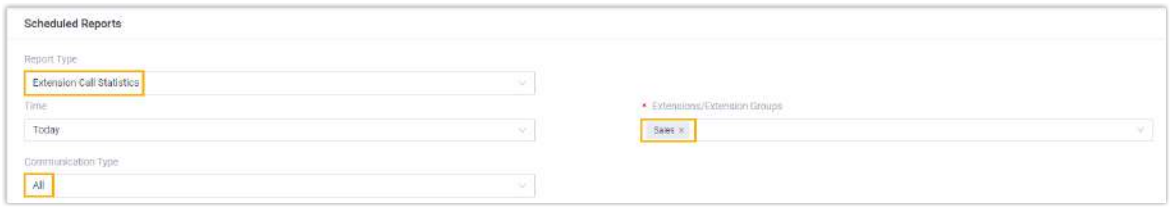
A scheduled call report is a diagram containing call statistics for the selected objects within a specific time frame. It automatically runs at a pre-defined frequency and is emailed to a specific address as a link and can be downloaded in CSV, XLS, or PDF.

Prerequisites

- Make sure email server works.
- Customize Email Template for Scheduled Reports.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. Under **Scheduled Reports** tab, click **Add Report**.
3. In the **Report Type** drop-down list, choose the desired report, and select one or more objects that you want to query.



Note:
Descriptions for specific parameters:

- **Communication Type**: Select a communication type from **Inbound**, **Outbound**, **Internal**, **Inbound/Outbound**, or **All**. You can use the parameter to filter call statistics in the following reports:
  - **Extension Call Statistics**

- **Extension Call Activity**
- **PBX Call Activity**
- **DID/Outbound Caller ID Activity**

- **Exclude Calls Abandoned within Xs**: Set a time. Calls abandoned within the specified time will not be included in report. You can use the parameter to filter call statistics in the following reports:
  - **Queue Performance**
  - **Queue Performance Activity**
  - **Agent Performance**
  - **Unreturned Missed Call Report**
- **Organization**: Select one or more departments. Calls of the department and its sub-departments will be included in the report.

  Note:
  This option is available only when you enable the **Organization Management** feature.
  You can use the parameter to filter call statistics in the following reports:
  - **Extension Call Statistics**
  - **Extension Call Activity**
  - **Extension Call Accounting**
  - **Extension Call Accounting Details**
- **Type**: Select a type from **Standard** or **Custom**. You can use the parameter to filter call statistics in **IVR Report**.

4. Schedule the report.
   - **Time**: Set a time frame that the desired report covers.
   - **Report Name**: Enter a name to help you identify it.
   - **Email Address**: Enter recipients' email addresses, separated by semicolon `;`.

     Note:
     You can set up to 10 email addresses.

     The report will be sent to the email address at the specified time.
   - **Report Frequency**: Set how often to send the report.
     - **Once**: If you choose the option, the system sends the report immediately after you save the setting.

    - **Daily**: If you choose the option, select a time from the drop-down list. The system sends the report at this time of the day.
    - **Weekly**: If you choose the option, choose a day of week and select a time from the drop-down list. The system sends the report at this time of the week.
    - **Monthly**: If you choose the option, choose a day and select a time from the drop-down list. The system sends the report on this day and time of the month.
- **Validity Period of the Download Link**: Set the validity period of the download link for the scheduled report.

  After the link expires, you can NOT download the report via the link.
- **File Format**: Set in which format the report can be downloaded.
    - **CSV**
    - **XLS**
    - **PDF**
- **Send Attachment**: Optional. If enabled, a file attachment will be included in the email sent to the specific email address.

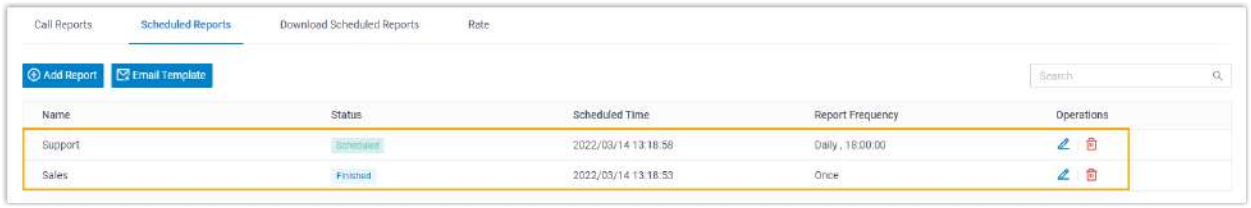
  > **Note:**
  > This option is only available when the scheduled file format is set to **CSV** or **XLS**.
- **Select Fields**: Optional. If you want to customize the display fields in your scheduled report, adjust the desired fields in the **Selected** box.

  > **Note:**
  > This option is only available in the following reports:
  >
  > - **Unreturned Missed Call Report**
  > - **Queue Performance**
  > - **Queue Performance Activity**
  > - **Agent Performance**
  > - **Agent Call Summary**

5. Click **Save**.

Result

On **Scheduled Reports** list, check status of the scheduled call report.



- **Finished**: The one-off call report was sent to the recipients' email addresses.
- **Scheduled**: The call report is scheduled and valid. The system will send the report to the recipients' email addresses at the specified time.
- **Paused**: The scheduled call report is on hold because the Call Center Service expired. To renew it, go to Yeastar P-Series Enterprise Plan or Ultimate Plan.

Manage Scheduled Reports

This topic describes how to edit and delete scheduled reports.

Edit scheduled reports

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**, click **Scheduled Reports**.
2. Select the desired report, click .
3. Edit the scheduled report according to your needs.
4. Click **Save**.

Delete scheduled reports

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**, click **Scheduled Reports**.
2. Select the desired report, click .
3. In the pop-up dialog box, click **OK**.

Download Scheduled Reports on Web Interface

After the system sends scheduled reports to recipients' mailboxes, the recipients can download reports via attached links and system administrator can view and download reports on PBX web portal. This topic describes how to download scheduled reports on PBX web portal.

Prerequisites

A scheduled report was sent out.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**, click **Download Scheduled Reports** tab.
2. Select the desired call report, click  .

   The report contains a snapshot of data for the time frame you have selected.
3. At the top-right corner, click **Download**.

Result

The report is downloaded to your computer in the pre-defined format.

Customize Email Template for Scheduled Reports

This topic describes how to customize email template for scheduled reports.

Background information

By default, Yeastar P-Series 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.

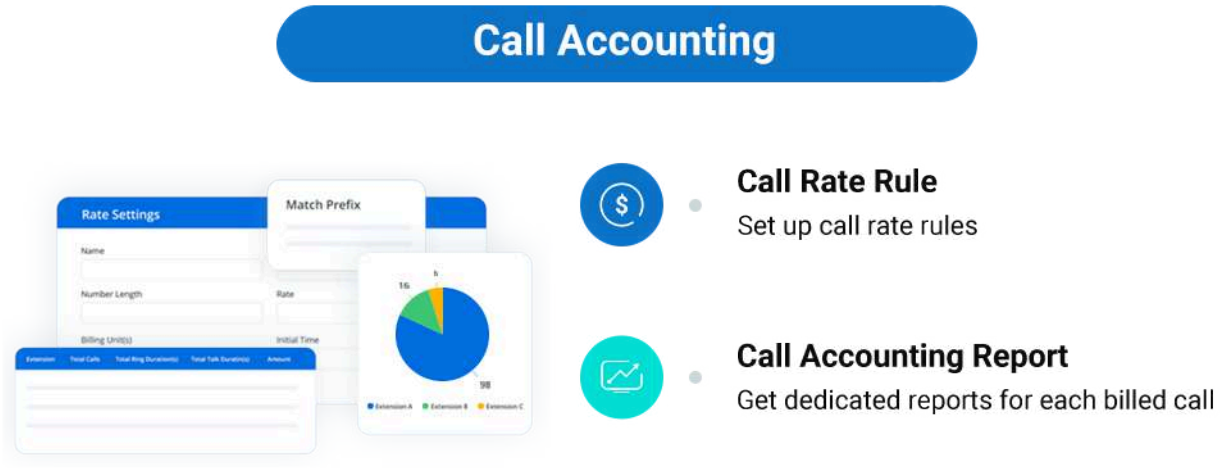
Improve telecom budget planning

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.



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**: Enter a name to help you identify the call rate rule. For example, enter `Local_Outbound`.
- **Match Prefix**: Optional. Define the dialing prefix to match the call rate rule.

  > **Note:**
  > Only outbound calls matching the dialing prefix will apply this rate.

- **Number Length**: Optional. Define the length of the dialed number to match the call rate rule.

  > **Note:**
  > Only the dialed number whose length is shorter than or equal to the value will match this rule.

- **Rate**: Enter a call rate. After the initial time, each billing unit will be charged with this rate.
- **Billing Unit (s)**: Define the time increment (in seconds) that will be used to calculate the fee for a call after the initial time. The default value is 60 seconds.

  For example, set **Rate** to 0.5 and **Billing Unit** to 60 seconds. In this way, the fee for a call will increase by 0.5 every 60 seconds.
- **Initial Time (s)**: Define the initial period of time (in seconds) during which the call will be charged with the initial cost.
- **Initial Cost**: Define the fixed cost incurred over the preset initial time.

For example, set **Initial Time** to 120 seconds and **Initial Cost** to 2. In this case, it costs 2 for the call within 2 minutes. After 2 minutes, the call will be charged with the preset rate.

4. Click **Save** and **Apply**.

Result

- The call rate rule is created. Any outbound calls matching the rule will be charged with the call rate as the following formula from now on.

```
Amount = Initial Cost + [(Talk Duration - Initial Time) / Billing Unit] * Rate
```

> **Note:**
> If the value to be multiplied by rate has decimals, it will be rounded upwards to the nearest integer.

- If you create more than one call rate rules in the list, the system will match outbound calls with these rules from the top down. You can click ⤒ ^ v ⤓ 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 ⤒ ^ v ⤓ to adjust the priority of call rate rules.

3. Click **Apply**.

Edit a call rate rule

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. Under **Rate** tab, click beside a call rate rule.
3. Edit the call rate rule.

> **Important:**
> Modifying the rate would affect the newly generated call billing statistics.

4. Click **Save** and **Apply**.

Delete call rate rules

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. Click **Rate** tab.
3. To delete a call rate rule, do as follows:
   a. On the right of a desired call rate rule, click .
   b. In the pop-up window, click **OK**.
4. To bulk delete call rate rules, do as follows:
   a. Select the checkboxes of desired call rate rules, then click **Delete**.
   b. In the pop-up window, click **OK**.

Export and Import Call Rate Rules

The call rate rules configured on Yeastar P-Series 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 ⤒ ^ v ⤓ to adjust the priority of call rate rules.

Related information

Import and Export -FAQ

Call Accounting Report

Extension Call Accounting Report

Extension Call Accounting report provides a quick overview of the bills for outbound calls made by extensions via specific trunks, and can be broken down to specific extensions, groups of extensions, or organizations of extensions. This topic introduces how to access the report and explains the key metrics in detail.

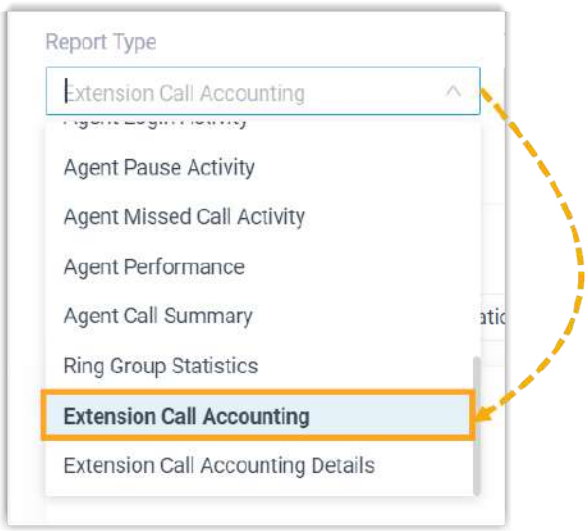
Prerequisites

You have set up at least one call rate rule, otherwise the system wouldn't know how to charge outbound calls.

For more information, see Add a Call Rate Rule.

Access Extension Call Accounting report

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Extension Call Accounting**.



3. Filter data by system time, extension(s), extension group(s), organization(s), or trunk.

> **Note:**
> **Organization** filter is displayed only when you enable **Organization Management** feature (Path: **PBX Settings > Preferences**).

A report that meets the filter criteria is displayed on the page, as shown below.

Note:

- You can click the tab at the top-left corner to switch between the break-down reports.
- If you filter data by extension group(s), the report will NOT include the call statistics from unknown source (the record where **Extension** column is displayed as **Other**).
- If you filter data by organization(s), the report data will include the selected organization and its subordinate departments, but will NOT include the call statistics from unknown source (the record where **Extension** column is displayed as **Other**).

Report details

We take the above report as an example to introduce the key metrics for **Extension Call Accounting** report.

Metric	Description
Total Calls	The total number of outbound calls made where a call rate rule is applied.
Total Talk Duration	The total time between calls answered and calls ended.
Average Talking Time	The average time between calls answered and calls ended.
Amount	The call cost.

Metric	Description
Total (displayed in row)	The sum of all the values in each column. **Note:** • This metric is only available for extension and extension group. • If you select multiple extension groups and one of the extensions belongs to two or more extension groups, the call statistics for the extension will be calculated more than once.

Related information

Extension Call Accounting Details Report

Extension Call Accounting Details Report

Extension Call Accounting Details report provides granular insights into the bills for each outbound call made by extensions via specific trunks. This topic introduces how to access the report and explains the key metrics in detail.

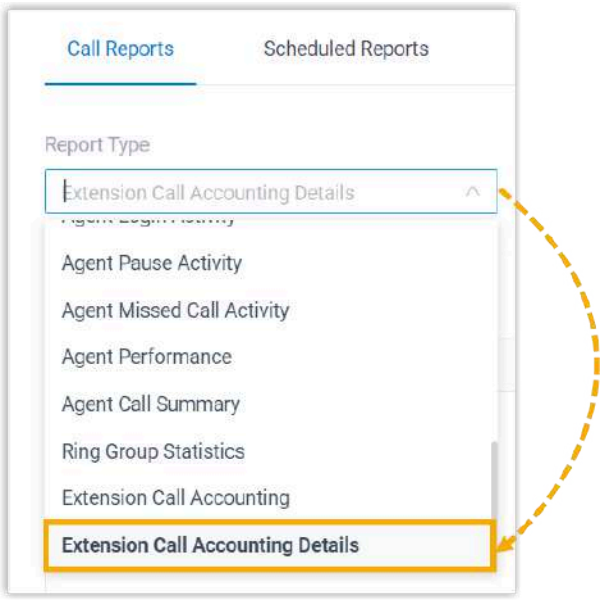
Prerequisites

You have set up at least one call rate rule, otherwise the system wouldn't know how to charge outbound calls.

For more information, see Add a Call Rate Rule.

Access Extension Call Accounting Details report

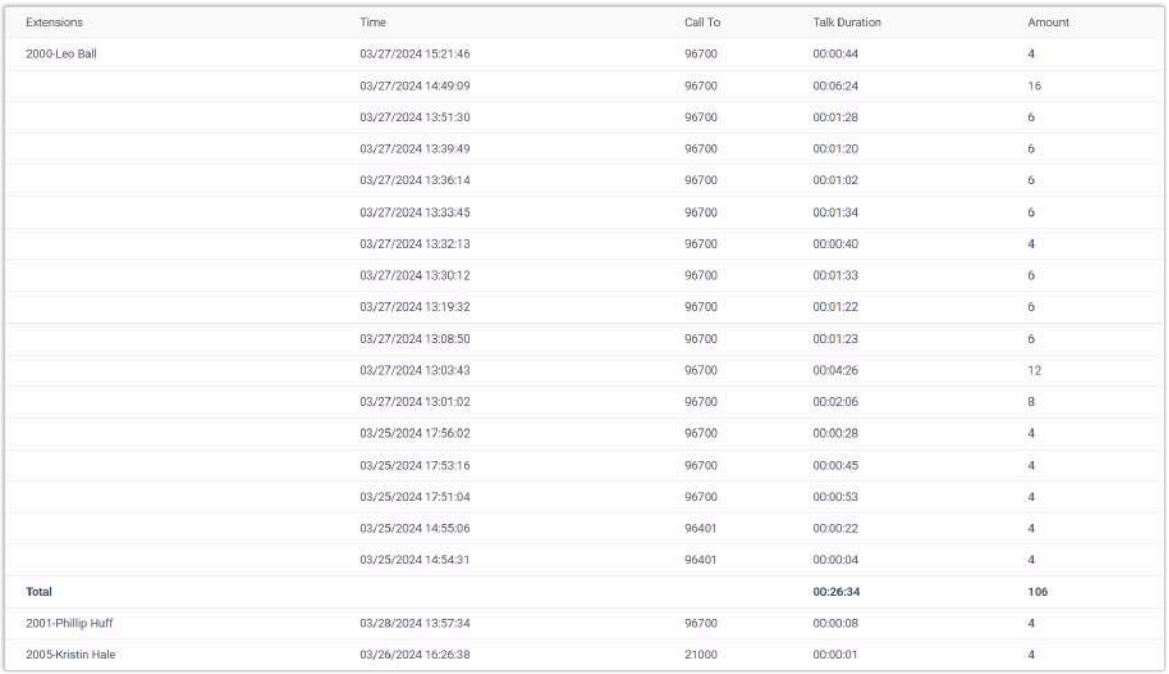
1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports**.
2. In the **Report Type** drop-down list, select **Extension Call Accounting Details**.



3. Filter data by system time, extension(s), extension group(s), organization(s), or trunk.

> **Note:**
> **Organization** filter is displayed only when you enable **Organization Management** feature (Path: **PBX Settings > Preferences**).

A report that meets the filter criteria is displayed on the page, as shown below.



Extensions	Time	Call To	Talk Duration	Amount
2000-Leo Ball	03/27/2024 15:21:46	96700	00:00:44	4
	03/27/2024 14:49:09	96700	00:06:24	16
	03/27/2024 13:51:30	96700	00:01:28	6
	03/27/2024 13:39:49	96700	00:01:20	6
	03/27/2024 13:36:14	96700	00:01:02	6
	03/27/2024 13:33:45	96700	00:01:34	6
	03/27/2024 13:32:13	96700	00:00:40	4
	03/27/2024 13:30:12	96700	00:01:33	6
	03/27/2024 13:19:32	96700	00:01:22	6
	03/27/2024 13:08:50	96700	00:01:23	6
	03/27/2024 13:03:43	96700	00:04:26	12
	03/27/2024 13:01:02	96700	00:02:06	8
	03/25/2024 17:56:02	96700	00:00:28	4
	03/25/2024 17:53:16	96700	00:00:45	4
	03/25/2024 17:51:04	96700	00:00:53	4
	03/25/2024 14:55:06	96401	00:00:22	4
	03/25/2024 14:54:31	96401	00:00:04	4
Total			**00:26:34**	**106**
2001-Phillip Huff	03/28/2024 13:57:34	96700	00:00:08	4
2005-Kristin Hale	03/26/2024 16:26:38	21000	00:00:01	4

Report details

We take the above report as an example to introduce the key metrics for **Extension Call Accounting Details** report.

Metric	Description
Time	When the outbound call was made.
Call To	The callee number.
Talk Duration	The time between call answered and call ended.
Amount	The call cost.
Total	Total talk duration and amount for extensions that make two or more outbound calls.
Total for All	Total talk duration and amount for the selected extensions. **Note:** This metric is displayed only when you set **Trunk** filter to a specific trunk.

Related information

Extension Call Accounting Report

Integration

Speech to Text (STT)

Speech to Text (STT) Overview

Speech to Text, also known as speech recognition, enables transcription of audio messages into texts. Yeastar P-Series 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 UC Clients

Users can check the transcribed text for each voicemail on Linkus Web Client, Linkus Desktop Client, and Linkus Mobile Client.

Email Client

If Voicemail to Email feature is enabled, the transcribed text will be displayed in the email content for received voicemails.

Related information

Enable or Disable Voicemail Transcription

Integrate with Speech to Text (STT) API

Integrate Yeastar P-Series 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

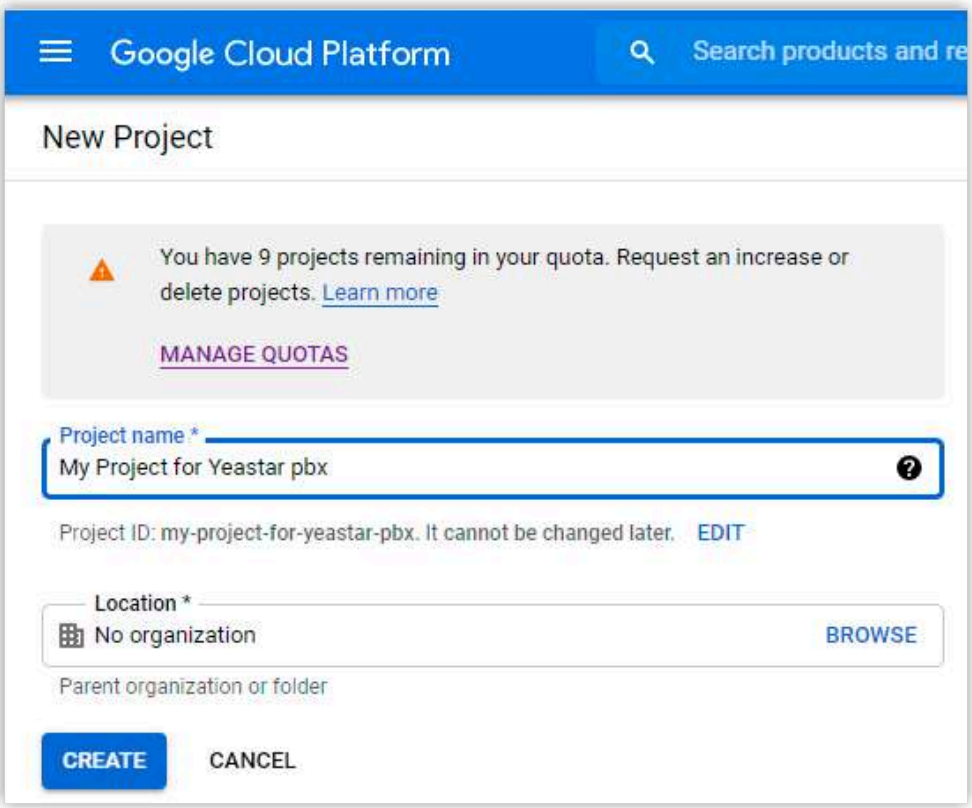
Get the API key from Google Cloud Platform

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.

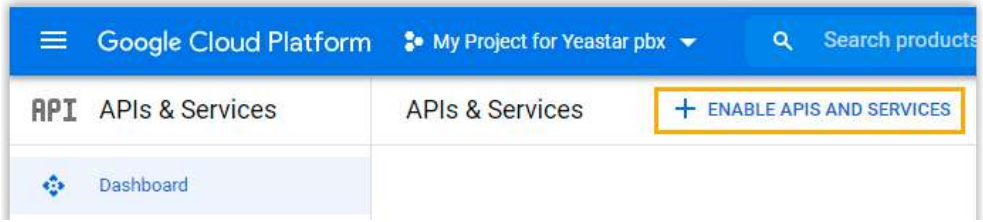
4. On the **New Project** page, set a project name, and click **CREATE**.



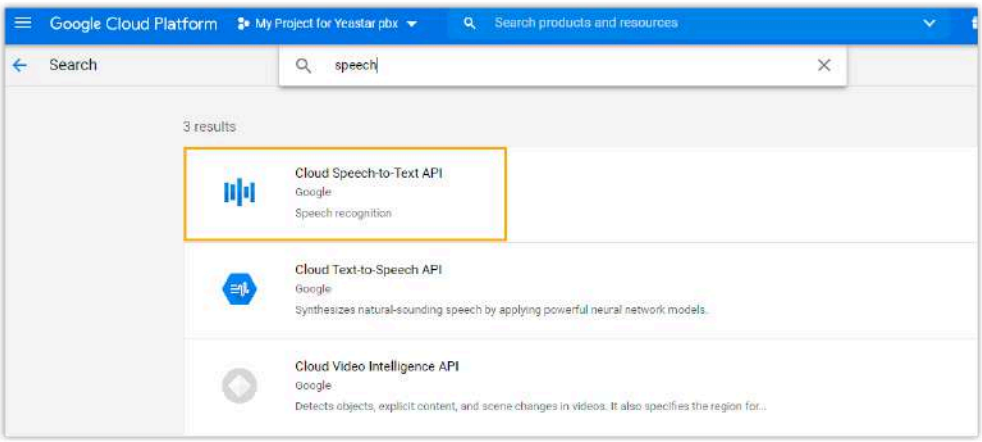
A new project is created, you can select the new project in the project list.

Step2. Enable Speech-to-Text API service on Google Cloud Platform

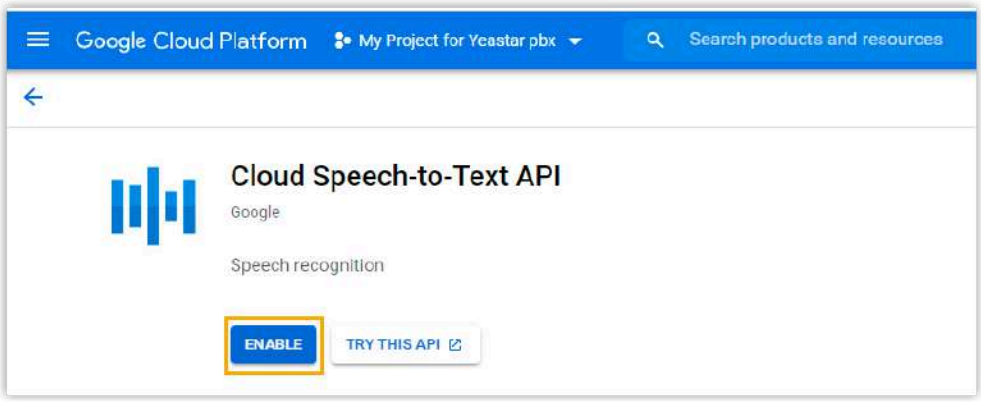
1. In the top-left conner, click ☰ to open the navigation menu, and go to **API & Services > Dashboard**.
2. Click **ENABLE APIS AND SERVICES**.



3. In the API Library, enter speech in the search box and press **Enter**, then select **Cloud Speech-to-Text API**.



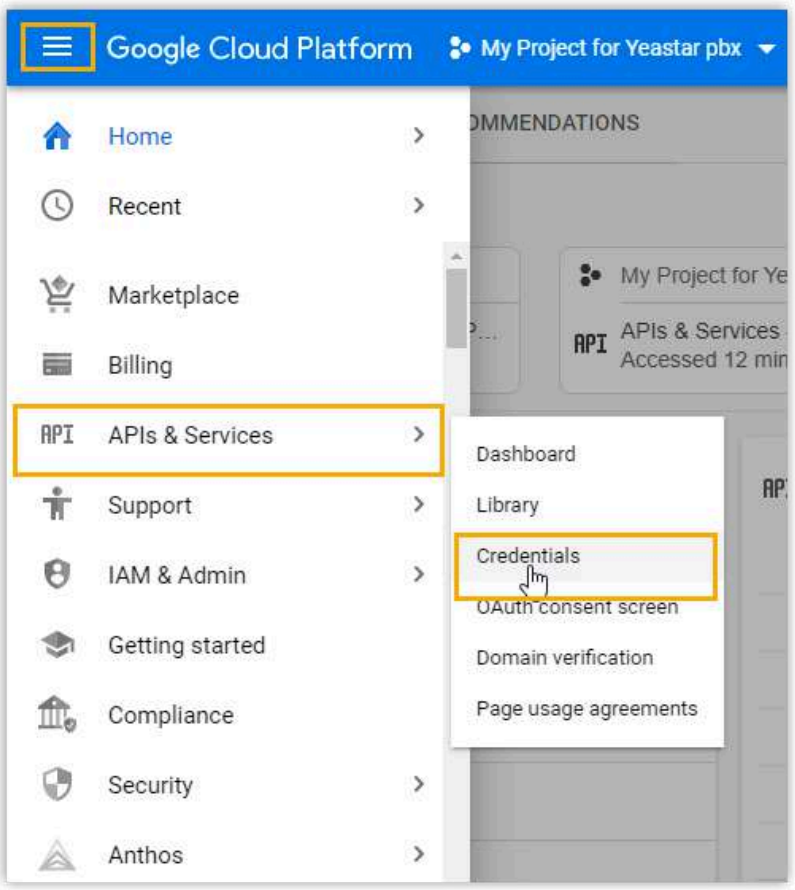
4. Click **ENABLE** button for the **Cloud Speech-to-Text API**.



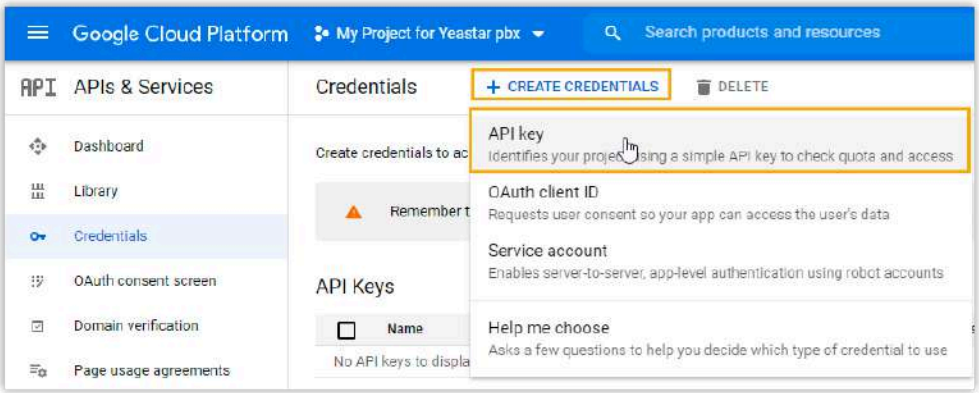
The Speech-to-Text service is enabled.

Step3. Create API credentials on Google Cloud Platform

1. In the left navigation panel, go to **API & Services > Credentials**.



2. Click **CREATE CREDENTIALS** and select **API key**.

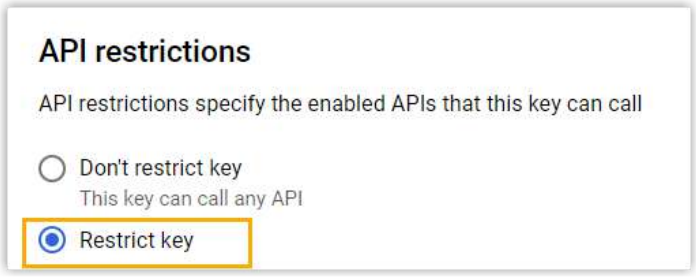


3. In the pop-up window, click **Edit API key** to edit and set restrictions for the key.

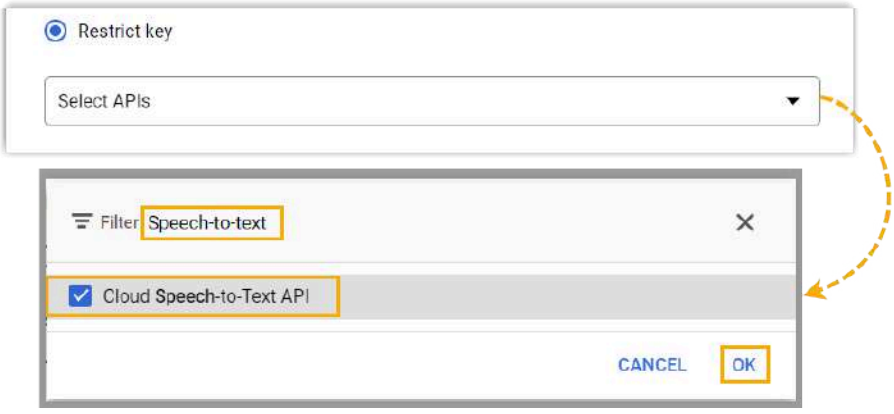
> **Important:**
> For security purpose, you need to restrict your API key, ensuring only authorized requests are made with your API key.

4. In the **Edit API key** page, complete the following configurations.
   a. In the **Name** field, set a name to help you identify the API key.

   b. In the **API restrictions** section, select **Restrict key**.



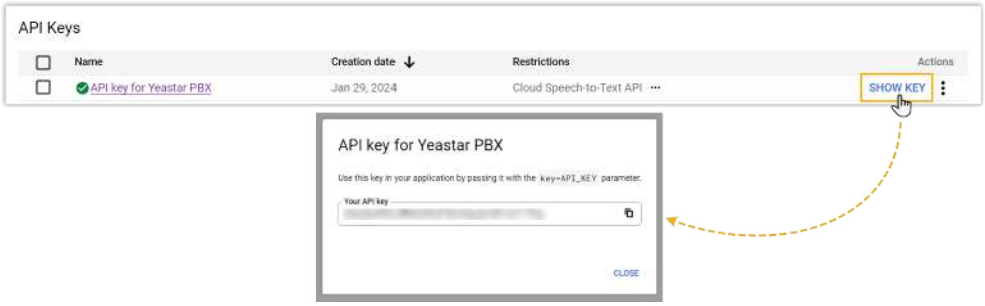
   c. In the **Select APIs** drop-down list, search and select the **Cloud Speech-to-Text API**, then click **OK**.



d. At the bottom of the page, click **SAVE** to apply your configuration.

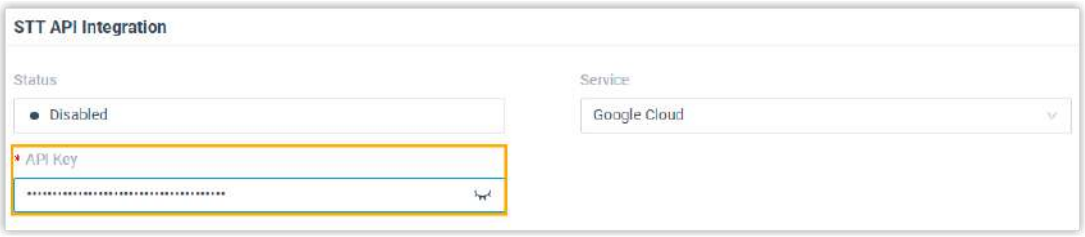
The API key is now only allowed to call the Cloud Speech-to-Text API.

5. In the **Credentials** page, click **SHOW KEY** beside the restricted API key, then in the pop-up window to copy the key.



Enable Speech to Text (STT) integration on Yeastar P-Series 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.



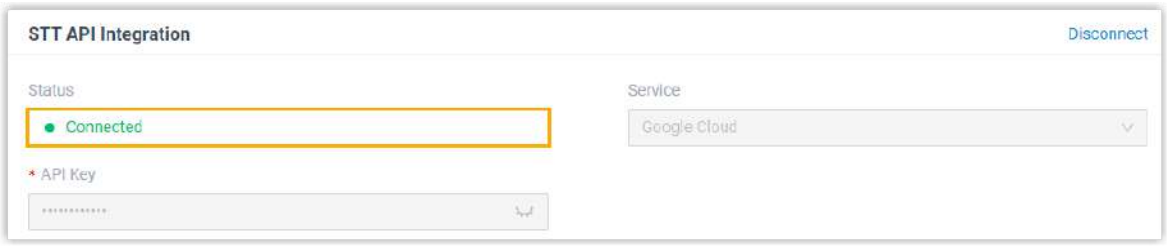
3. In **Settings** section, select the transcription language.

   The audio messages will be transcribed to text in the selected language.

> **Note:**
> If the language of voicemail is different from the selected language, the transcribed text will be inaccurate.

4. Click **Save**.

   If the integration succeeds, the **Status** in the **STT API Integration** section will display **Connected**.



What to do next

After the STT API integration succeeds, go to **Call Features > Voicemail > Voicemail Settings** to enable the Voicemail Transcription feature. For more information, see Enable or Disable Voicemail Transcription.

Related information

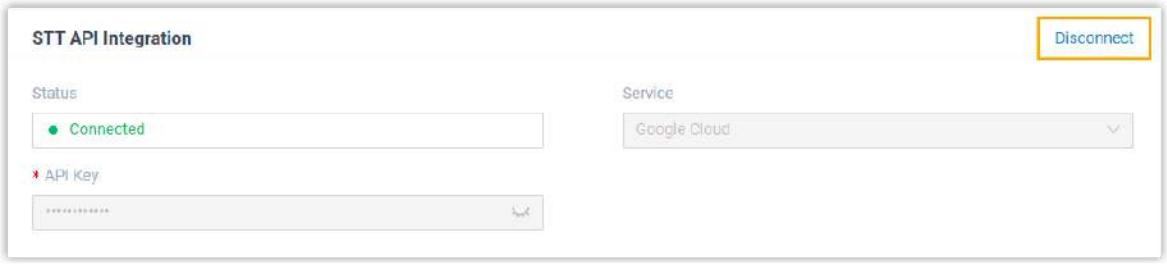
Speech to Text (STT) Overview
Disconnect Speech to Text (STT) API Integration

Disconnect Speech to Text (STT) API Integration

After the STT API integration is connected, you can directly disconnect the API service on PBX if you don't need the Speech to Text feature any more, or want to pause the API service.

Procedure

1. Log in to PBX web portal, go to **Integrations > Speech to Text**.
2. In the **STT API Integration** section, click **Disconnect** in the top-right corner.



3. In the pop-up dialog box, click **Confirm** to disconnect the API service.

   The API integration is disconnected, and the **Status** displays **Disabled**.

Result

The Voicemail Transcription feature is unavailable.

Asterisk Manager Interface (AMI) Overview

The Asterisk Manager Interface (AMI) is a system monitoring and management interface provided by Asterisk. Yeastar P-Series 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

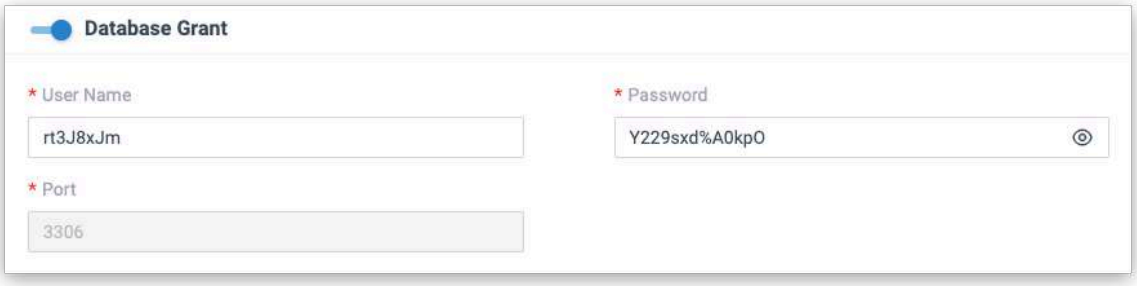
Yeastar P-Series Software Edition allows you to access the system database and get CDR data. This topic describes how to get CDR data from the PBX database via Navicat software.

Procedure

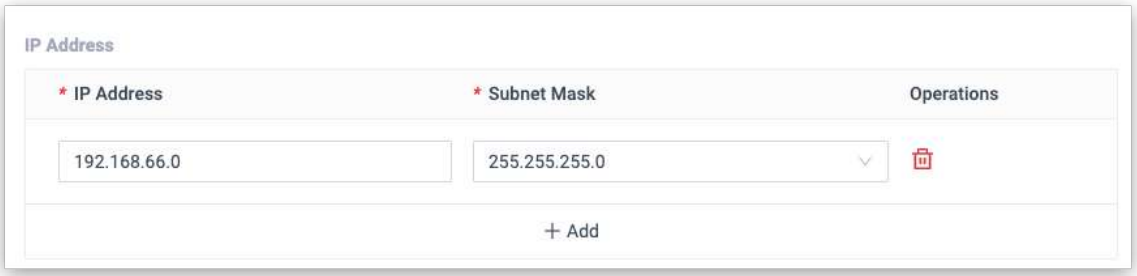
1. Grant access to the PBX database
2. Access the PBX database via Navicat software

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.



   - **User Name**: Use the randomly generated user name or change the name.
   - **Password**: Use the randomly generated password or change password.
   - **Port**: Default port is 3306 and is unchangeable.
3. In the **Permitted IP** section, configure which IP addresses are allowed to access the database.



   a. Click **Add**.
   b. Enter the permitted IP address and subnet mask.

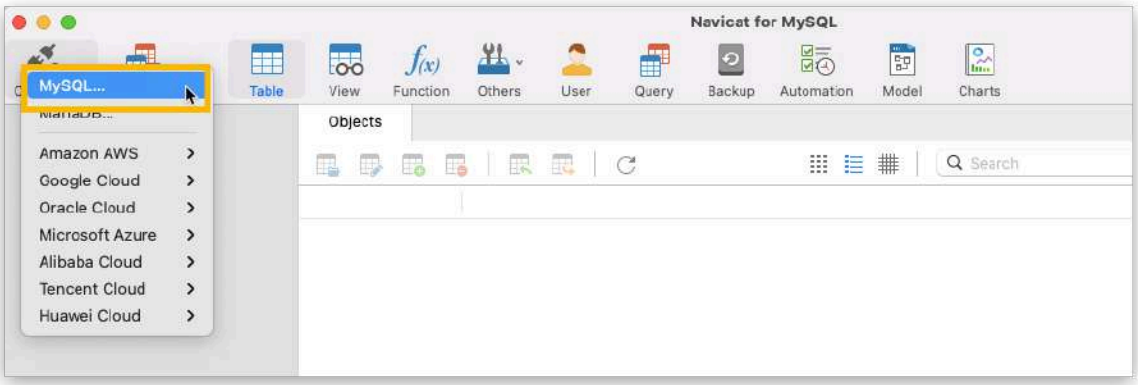
      In this example, enter IP address `192.168.66.0` and subnet mask `255.255.255.0` to allow all IP addresses in the segment 192.168.66.X to access the database.

> **Note:**
> Restricted from MySQL database, only the two subnet masks are allowed to be filled in: `255.255.255.255` and `255.255.255.0`.

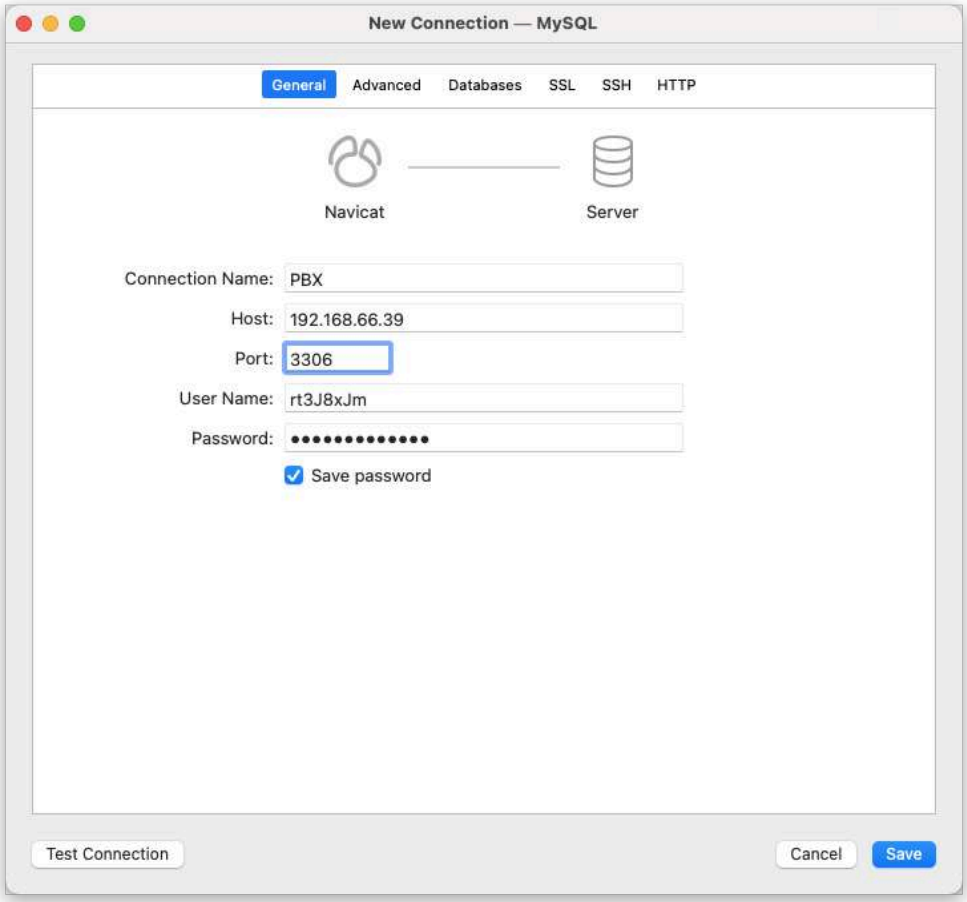
4. Click **Save** and **Apply**.

Access the PBX database via Navicat software

1. Launch Navicat for MySQL on the PC that has IP address being in the segment 192.168.66.X.
2. On the Navicat for MySQL, click **Connection** and select **MySQL**.



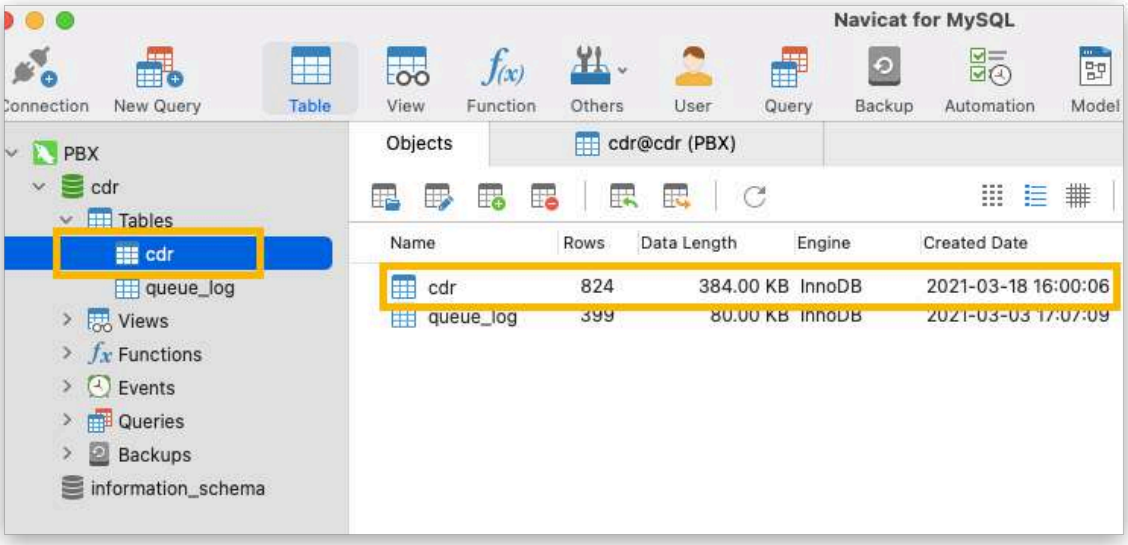
3. In the pop-up window, enter the following information:



- **Connection Name**: Enter a connection name to help you identify it.
- **Host**: Enter the IP address of PBX.
- **Port**: Enter `3306`.
- **User Name**: Enter the user name that is configured on the PBX. In this example, enter `rt3J8xJm`.
- **Password**: Enter the password that is configured on the PBX. In this example, enter `Y229sxd%A0kpO`.

4. Click **Save**.
5. To check CDR data, double click the new connection, and select cdr table.

   For more information about the cdr table, see cdr Table in the PBX Database.



cdr Table in the PBX Database

This topic describes details of cdr table stored in the database of Yeastar P-Series 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	Pin code
uniqueid	System internal flag
didnumber	DID number
dodnumber	DOD number
recordfile	Recording file name
recordpath	Recordings path (with file name)
srcchanurl	Caller's SIP URI
dstchanurl	Callee's SIP URI
reasonpartya	System internal flag
reasonpartyb	System internal flag
reasonpartyc	System internal flag
reasonpartyd	System internal flag
reasonpartye	System internal flag

Field	Descriptions
reasonpartyf	System internal flag
displayonweb	System internal flag
src_del_cdr	System internal flag
dst_del_cdr	System internal flag
src_del_recording	System internal flag
dst_del_recording	System internal flag
srcnameprefix	System internal flag
dstnameprefix	System internal flag
misscall_isread	System internal flag
in2outbound	System internal flag
concurrentcalls	System internal flag
videocall	System internal flag
rascall	System internal flag
tryvideocall	System internal flag

References

System Capacity Comparison

This topic gives a comparison on the maximum value of the system capacity in different firmware versions.

Table 38.

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) **128** (extensions ≥ 1000)
Ring Group	32	**32** (extensions < 1000)

Table 38. (continued)

Feature	Versions earlier than v83.6.0.63	v83.6.0.63 and the later version
		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		
Backup and Restore	16	16
Video Conferencing		
Max. Duration per Video Meeting	120 min.	120 min.

Table 38. (continued)

Feature	Versions earlier than v83.6.0.63	v83.6.0.63 and the later version
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

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.	N/A

Parameter	Description	Importance	Restriction	Default Value
			The maximum character length is 255.	
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
System Prompt Language	The language of the system prompts heard by the extension during a call.	Optional	Permitted value: `follow_system` or one of the prompt language existed in PBX System Prompt (e.g. `German`). **Note:** **System Prompt Language** will be filled with default value *`follow_system`* if the language you enter does not exist in PBX, or if you leave this field empty.	follow_system
Email Language	The language of email notifications for the extension.	Optional	Permitted value: `follow_system` or one of the email language that existed in PBX (e.g. `German`). **Note:** **Email Language** will be filled with default value *`follow_system`* if the language you enter does not exist in PBX, or if you leave this field empty.	follow_system
Organization	The organization to which the	Optional	Permitted value: The organization names that existed in PBX.	Root organization, namely the

Parameter	Description	Importance	Restriction	Default Value
	extension user belongs.		**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 "Support Team", enter `Yeastar/Marketing Center/Support Team`. • If belong to multiple organizations, enter `Yeastar/Marketing Center&Yeastar/Product Management Center`.	Company Name.
User Role	The role for extension user with PBX management permission.	Required	Permitted value: `0` or one of the role names defined in the PBX. `0` means [None]. **Note:** **User Role** will be filled with default value `0` if you leave this field empty.	0

Parameter	Description	Importance	Restriction	Default Value
Extension Number	The extension's number.	Required	Extension Number cannot be duplicated, and only numbers are allowed. The maximum character length is 8.	N/A
Caller ID	The caller ID that is displayed on the callee's device.	Required	Numbers, letters, and special characters `( ) . - + * #` are allowed. The maximum character length is 31. **Note:** **Caller ID** will be filled with default value `Extension Number` if you leave this field empty.	Extension Number
Registration Name	The registration name that is used to validate extension registration.	Required	The maximum character length is 63. **Note:** **Registration Name** will be generated randomly if you leave this field empty.	Generate Randomly
Registration Password	The password for the user to register the SIP extension.	Required	The minimum character length is 8 and the maximum is 63. **Note:** **Registration Password** will be generated randomly if you leave this field empty.	Generate Randomly
IP Phone Concurrent Registrations	How many SIP phones are allowed to register with the extension.	Required	Permitted value: • `1`: Allow one phone to register with the extension. • `2`: Allow two phones to register with the extension. • `3`: Allow three phones to register with the extension. • `4`: Allow four phones to register with the extension. • `5`: Allow five phones to register with the extension.	1

Parameter	Description	Importance	Restriction	Default Value
			Note: **IP Phone Concurrent Registrations** will be filled with default value *1* if you leave this field empty.	
Emergency Outbound Caller ID	The outbound Caller ID for the extension when it makes emergency calls.	Optional	Numbers, letters, and characters *( ) . - + * #* are allowed. The maximum character length is 31.	N/A
Enable Voicemail	Whether to enable or disable voicemail feature.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Enable Voicemail** will be filled with default value *1* if you leave this field empty.	1
Voicemail PIN Authentication	Whether to enable or disable voicemail PIN authentication.	Required if **Enable Voicemail** = *1*	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Voicemail PIN Authentication** will be filled with default value *1* if you leave this field empty.	1
Voicemail Access PIN	The PIN for authentication when accessing voicemail box.	Required if **Enable Voicemail** = *1* & **Voicemail PIN Authentication** = *1*	Only numbers are allowed. The minimum character length is 3 and the maximum is 15. **Note:** **Voicemail Access PIN** will be generated randomly if you leave this field empty.	Generate Randomly

Parameter	Description	Importance	Restriction	Default Value
Voicemail Language	The language of the system prompts heard by caller when they access the extension's voicemail box.	Optional	Permitted value: `follow_system` or one of the prompt language existed in PBX System Prompt (e.g. `German`). **Note:** **Voicemail Language** will be filled with default value *`follow_system`* if the language you enter does not exist in PBX, or if you leave this field empty.	follow_system
New Voicemail Notification	The notification type for new voicemail.	Required if **Enable Voicemail** = *`1`*	Permitted value: • *`no`*: No Email Notifications • *`with_attach`*: Send Email Notifications with Attachment • *`without_attach`*: Send Email Notifications without Attachment **Note:** **New Voicemail Notification** will be filled with default value *`no`* if you leave this field or Email Address empty.	no
Send to	Specify the email address for receiving notification emails about new voicemails.	Required if **Enable Voicemail** = *`1`* & **New Voicemail Notification** = *`with_attach`* or *`without_attach`*	Permitted value: • *`user Email`*: Send notification emails to the user's email address. • *`custom Email`*: Send notification emails to a custom email address.	user Email
Voicemail Email Address	Enter a custom email address for receiving	Required if **Enable Voicemail**	Only numbers, letters, and characters *`@ _ - .`* are allowed. Must start with a number, letter, or character _ and	N/A

Parameter	Description	Importance	Restriction	Default Value
	notification emails about new voicemails.	= *1* & **New Voicemail Notification** = *with_attach* or *without_attach* & **Send to** = *custom Email*	follow the email address format XXX@XXX.XX. The maximum character length is 255.	
After Notification	The way to handle voicemail message in mailbox after receiving the message notification via email.	Required if **Enable Voicemail** = *1* & **New Voicemail Notification** = *with_attach*	Permitted value: • *no*: Do Nothing • *mark_read*: Mark as read • *delete*: Delete Voicemail **Note:** **After Notification** will be filled with default value *no* if you leave these fields empty.	no
		Required if **Enable Voicemail** = *1* & **New Voicemail Notification** = *without_attach*	Permitted value: • *no*: Do Nothing • *mark_read*: Mark as read **Note:** **After Notification** will be filled with default value *no* if you leave these fields empty.	no
Play Date and Time	Whether to announce arrival time of the message before playing the voicemail message.	Required if **Enable Voicemail** = *1*	Permitted value: • *0*: Disable • *1*: Enable **Note:**	0

Parameter	Description	Importance	Restriction	Default Value
			Play Date and Time will be filled with default value `0` if you leave this field empty.	
Time Display Format	The time format for announcing the message arrival time.	Required if **Play Date and Time** = `1`	Permitted value: • `Follow System` • `12-hour format` • `24-hour format` **Note:** **Time Display Format** will be filled with default value if you leave this field empty.	Follow System
Play Caller ID	Whether to announce caller ID of the party that left the message before playing the voicemail message.	Required if **Enable Voicemail** = `1`	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Play Caller ID** will be filled with default value `0` if you leave this field empty.	0
Play Message Duration	The duration of the message (in minutes) will be announced before playing the voicemail message.	Required if **Enable Voicemail** = `1`	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Play Message Duration** will be filled with default value `0` if you leave this field empty.	0
Send email notification when the User Password is changed	Whether to send email notification when the User Password is changed.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:**	1

Parameter	Description	Importance	Restriction	Default Value
			Send email notification when the User Password is changed will be filled with default value `1` if you leave this field empty.	
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
Recording operation	Whether to allow users to switch their own recording status during a call.	Required	Permitted value: • `0`: No permission • `1`: Pause/Resume • `2`: Start/Pause/Resume **Note:** **Recording operation** will be filled with default value `0` if you leave this field empty.	0
All Busy Mode for Endpoints	Whether to forward a new incoming call to the Busy destination when one of the endpoints with extension registered is busy in a call.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **All Busy Mode for Endpoints** will be filled with default value `0` if you leave this field empty.	0
All Reject Mode for Endpoints	Whether to stop the incoming call from ringing other	Required	Permitted value: • `0`: Disable	0

Parameter	Description	Importance	Restriction	Default Value
	endpoints and forward to the Busy destination when it was rejected on an endpoint.		• *1*: Enable **Note:** **All Reject Mode for Endpoints** will be filled with default value *0* if you leave this field empty.	
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
Video Preview	Whether to allow other extension users to click a specific button to preview the extension's video when receiving a call from the extension.	Optional	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Video Preview** will be filled with default value *0* if you leave this field empty.	0
Auto Preview	Whether to allow other extension users to automatically preview the extension's video when receiving a call from the extension.	Optional	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Auto Preview** will be filled with default value *0* if you leave this field empty.	0
Hot Desking	Whether to allow the extension to log in to a hot desking phone.	Optional	Permitted value: • *0*: Disable • *1*: Enable	0

Parameter	Description	Importance	Restriction	Default Value
			Note: **Hot Desking** will be filled with default value *0* if you leave this field empty.	
Log out of Queue	Whether to automatically log out the dynamic agent from the queue when the user log out of a hot desking phone.	Optional	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Log out of Queue** will be filled with default value *0* if you leave this field empty.	0
Automatic Guest Out	Whether to automatically log out the extension from a hot desking phone.	Optional	Permitted value: • `0`: Never • `1`: After • `2`: At Daily **Note:** **Automatic Guest Out** will be filled with default value `0` if you leave this field empty.	0
After hr.	The hour of the specified time period for automatically logging out the extension from a hot desking phone.	Required if **Automatic Guest Out** = *1*	Permitted value: 00 - 23 **Note:** **After hr.** will be filled with default value `08` if you leave this field empty.	08
After min.	The minute of the specified time period for automatically logging out the extension from a hot desking phone.	Required if **Automatic Guest Out** = *1*	Permitted value: 00 - 59 **Note:** **After min.** will be filled with default value `00` if you leave this field empty.	00

Parameter	Description	Importance	Restriction	Default Value
At Daily	The time for automatically logging out the extension from a hot desking phone on a daily basis.	Required if **Automatic Guest Out** = *2*	Time Format: HH:MM (e.g. 13:30) **Note:** The End Time must be later than the Start Time.	N/A
DTMF Mode	The mode for sending DTMF tones.	Required	Permitted value: *rfc4733*, *info*, *inband* or *auto*. **Note:** **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 device to check if the device is online.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Qualify** will be filled with default value *1* if you leave this field empty.	1
T.38 Support	Whether to support T.38 fax for this extension.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **T.38 Support** will be filled with default value `0` if you leave this field empty.	0

Parameter	Description	Importance	Restriction	Default Value
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:** **Allow Remote Registration** will be filled with default value `0` if you leave this field empty.	0
Disable Outbound Calls	Whether to restrict the user from making outbound calls.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Disable Outbound Calls** will be filled with default value `0` if you leave this field empty.	0

Parameter	Description	Importance	Restriction	Default Value
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 exist in PBX, it will be skipped. • For multiple outbound routes, please enter outbound route names and use `&` as a separator, e.g. name1&name2.	N/A

Parameter	Description	Importance	Restriction	Default Value
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 log in to Linkus Mobile Client.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Linkus Mobile Client** will be filled with default value `1` if you leave this field empty.	1

Parameter	Description	Importance	Restriction	Default Value
Call Waiting (for Mobile Client)	Whether to receive another call while the extension user is on the phone.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Call Waiting (for Mobile Client)** will be filled with default value `1` if you leave this field empty.	1
Auto Answer (for Mobile Client)	Whether to automatically answer non-paging/intercom calls.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Auto Answer (for Mobile Client)** will be filled with default value `0` if you leave this field empty.	0
Auto Answer Delay Time(s) (for Mobile Client)	The delay time in seconds before automatically answering non-paging/intercom calls.	Required if **Auto Answer (for Mobile Client)** = `1`	Only numbers are allowed. The maximum allowed input is 60. **Note:** **Auto Answer Delay Time(s) (for Mobile Client)** will be filled with default value `0` if you leave this field empty.	0
Play Auto Answer Tone (for Mobile Client)	Whether to play a tone to alert the extension user when non-paging/intercom calls are auto answered.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Play Auto Answer Tone (for Mobile Client)** will be	1

Parameter	Description	Importance	Restriction	Default Value
			filled with default value `1` if you leave this field empty.	
Auto Answer Paging/Intercom Call (for Mobile Client)	Whether to automatically answer paging/intercom calls.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Auto Answer Paging/Intercom Call (for Mobile Client)** will be filled with default value `0` if you leave this field empty.	0
Paging/Intercom Barge (for Mobile Client)	Whether to automatically answer the paging/intercom call when the extension user is already on the phone.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Paging/Intercom Barge (for Mobile Client)** will be filled with default value `0` if you leave this field empty.	0
Play Auto Answer Tone for Paging/Intercom Call (for Mobile Client)	Whether to play a tone to alert the extension user when paging/intercom calls are auto answered.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Play Auto Answer Tone for Paging/Intercom Call (for Mobile Client)** will be filled with default value `1` if you leave this field empty.	1
Linkus Desktop Client	Whether to allow the extension user to log in to Linkus Desktop Client.	Required	Permitted value: • `0`: Disable • `1`: Enable	1

Parameter	Description	Importance	Restriction	Default Value
			Note: **Linkus Desktop Client** will be filled with default value *1* if you leave this field empty.	
Call Waiting (for Desktop Client)	Whether to receive another call while the extension user is on the phone.	Optional	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Call Waiting (for Desktop Client)** will be filled with default value *1* if you leave this field empty.	1
Auto Answer (for Desktop Client)	Whether to automatically answer non-paging/intercom calls.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Auto Answer (for Desktop Client)** will be filled with default value *0* if you leave this field empty.	0
Auto Answer Delay Time(s) (for Desktop Client)	The delay time in seconds before automatically answering non-paging/intercom calls.	Required if **Auto Answer (for Desktop Client)** = *1*	Only numbers are allowed. The maximum allowed input is 60. **Note:** **Auto Answer Delay Time(s) (for Desktop Client)** will be filled with default value *0* if you leave this field empty.	0
Play Auto Answer Tone (for Desktop Client)	Whether to play a tone to alert the extension user when	Optional	Permitted value: • *0*: Disable • *1*: Enable	1

Parameter	Description	Importance	Restriction	Default Value
	non-paging/intercom calls are auto answered.		**Note:** **Play Auto Answer Tone (for Desktop Client)** will be filled with default value `1` if you leave this field empty.	
Auto Answer Paging/Intercom Call (for Desktop Client)	Whether to automatically answer paging/intercom calls.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Auto Answer Paging/Intercom Call (for Desktop Client)** will be filled with default value `0` if you leave this field empty.	0
Paging/Intercom Barge (for Desktop Client)	Whether to automatically answer the paging/intercom call when the extension user is already on the phone.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Paging/Intercom Barge (for Desktop Client)** will be filled with default value `0` if you leave this field empty.	0
Play Auto Answer Tone for Paging/Intercom Call (for Desktop Client)	Whether to play a tone to alert the extension user when paging/intercom calls are auto answered.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Play Auto Answer Tone for Paging/Intercom Call (for Desktop Client)** will be filled with default value `1` if you leave this field empty.	1

Parameter	Description	Importance	Restriction	Default Value
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
Call Waiting (for Web Client)	Whether to receive another call while the extension user is on the phone.	Optional	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Call Waiting (for Web Client)** will be filled with default value *1* if you leave this field empty.	1
Auto Answer (for Web Client)	Whether to automatically answer non-paging/intercom calls.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Auto Answer (for Web Client)** will be filled with default value *0* if you leave this field empty.	0
Auto Answer Delay Time(s) (for Web Client)	The delay time in seconds before automatically answering non-paging/intercom calls.	Required if **Auto Answer (for Web Client)** = *1*	Only numbers are allowed. The maximum allowed input is 60. **Note:** **Auto Answer Delay Time(s) (for Web Client)** will be filled with default	0

Parameter	Description	Importance	Restriction	Default Value
			value `0` if you leave this field empty.	
Play Auto Answer Tone (for Web Client)	Whether to play a tone to alert the extension user when non-paging/intercom calls are auto answered.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Play Auto Answer Tone (for Web Client)** will be filled with default value `1` if you leave this field empty.	1
Auto Answer Paging/Intercom Call (for Web Client)	Whether to automatically answer paging/intercom calls.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Auto Answer Paging/Intercom Call (for Web Client)** will be filled with default value `0` if you leave this field empty.	0
Paging/Intercom Barge (for Web Client)	Whether to automatically answer the paging/intercom call when the extension user is already on the phone.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Paging/Intercom Barge (for Web Client)** will be filled with default value `0` if you leave this field empty.	0
Play Auto Answer Tone for Paging/Interc	Whether to play a tone to alert the extension user when paging/intercom	Optional	Permitted value: • `0`: Disable • `1`: Enable	1

Parameter	Description	Importance	Restriction	Default Value
om Call (for Web Client)	calls are auto answered.		**Note:** **Play Auto Answer Tone for Paging/Intercom Call (for Web Client)** will be filled with default value `1` if you leave this field empty.	
Linkus Pad Client (SDK)	Whether to allow the extension user to log in to Linkus Pad Client (SDK).	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** • This parameter only takes effect when Linkus SDK is enabled (Path: **Integrations > Linkus SDK**). • **Linkus Pad Client (SDK)** will be filled with default value `1` if you leave this field empty.	1
Linkus Mobile Client Codec	Specify the audio codec for this user's Linkus Mobile Client.	Optional	Permitted value: • `ulaw` • `alaw` • `ilbc` • `g722` • `g729` • `opus`	N/A
Linkus Mobile Client - ICE	Whether to enable ICE (Interactive Connectivity Establishment) for this user's Linkus Mobile Client.	Optional	Permitted value: • `0`: Disable • `1`: Enable	N/A

Related information

Export and Import SIP Extensions
Import and Export -FAQ

Organization Parameters

Descriptions for parameters in exported and imported Organization CSV file.

Parameter	Importance	Restriction	Default Value
Organization Name	Required	The maximum character length is 127.	N/A
Parent Organization	Required	Permitted value: The full path of parent organization. For multiple organizations, please use `&` to separate. Examples are shown as below: • If belong to root organization "Yeastar", enter `Yeastar`. • If belong to first-layer organization "Marketing Center", enter `Yeastar/Marketing Center`. • If belong to second-layer organization "Support Team", enter `Yeastar/Marketing Center/Support Team`. • If belong to multiple organizations, enter `Yeastar/Marketing Center&Yeastar/Product Management Center`.	N/A

Related information

Export and Import Organizations
Import and Export -FAQ

Contacts Parameters

Descriptions for parameters in exported and imported Company Contacts CSV file and Personal Contacts CSV file.

Parameter	Importance	Restriction
First Name	At lease one is required	The maximum character length is 127 (63 for first name and 63 for last name).

Parameter	Importance	Restriction
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.
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

Holidays Parameters

Descriptions for parameters in exported and imported Holidays CSV file.

Parameter	Importance	Restriction	Default Value
Name	Required	The maximum character length is 127. The holiday name can not be duplicated.	N/A
Holiday Type	Required	Permitted value: • `By Date` • `By Month` • `By Week` **Note:** **Holiday Type** will be filled with default value `By Date` if you leave this field empty.	By Date

<table>
<tr><th>Parameter</th><th>Importance</th><th>Restriction</th><th>Default Value</th></tr>
<tr><td>Start Date (By Date)</td><td rowspan="2">Required if Holiday Type = By Date</td><td rowspan="2">Format: DD/MM/YYYY HH:MM
E.g. 25/10/2020 13:30

Note:
The End Date must be later than the Start Date.</td><td>N/A</td></tr>
<tr><td>End Date (By Date)</td><td>N/A</td></tr>
<tr><td>Start Date (By Month)</td><td rowspan="2">Required if Holiday Type = By Month</td><td rowspan="2">Format: DD/MM HH:MM
E.g. 31/10 13:30

Note:
The End Date must be later than the Start Date.</td><td>N/A</td></tr>
<tr><td>End Date (By Month)</td><td>N/A</td></tr>
<tr><td>Month (By Week)</td><td rowspan="3">Required if Holiday Type = By Week</td><td>Permitted value:

• January
• February
• March
• April
• May
• June
• July
• August
• September
• October
• November
• December</td><td>N/A</td></tr>
<tr><td>Week (By Week)</td><td>Permitted value:

• First Week
• Second Week
• Third Week
• Fourth Week
• Last Week</td><td>N/A</td></tr>
<tr><td>Day (By Week)</td><td>Permitted value:

• Sunday
• Monday
• Tuesday
• Wednesday
• Thursday
• Friday</td><td>N/A</td></tr>
</table>

Parameter	Importance	Restriction	Default Value
		• *Saturday*	
Start Time (By Week)		Format: HH:MM E.g. 13:30	N/A
End Time (By Week)		**Note:** The End Time must be later than the Start Time.	N/A

Related information

Export and Import Holidays

Speed Dial Number Parameters

Descriptions for parameters in exported and imported Speed Dial Number CSV file.

Parameter	Importance	Restriction
Speed Dial Number	Required	The maximum character length is 4. Only numbers and characters * # are allowed. Speed dial number cannot be duplicated.
Phone Number	Required	The maximum character length is 31. Numbers, letters, and characters ( ) . - + * # are allowed.

Related information

Export and Import Speed Dial Numbers
Import and Export -FAQ

Emergency Number Parameters

Descriptions for parameters in exported and imported Emergency Number CSV file.

Parameter	Importance	Restriction	Default Value
Name	Required	The maximum character length is 63. Characters ; " , \ are not allowed.	N/A

Parameter	Importance	Restriction	Default Value
		Emergency number's name cannot be duplicated.	
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
Prepend for Emergency Number	Optional	The maximum character length is 10. Numbers, letters, and characters `( ) . - + * #` are allowed.	N/A

Related information

Export and Import Emergency Numbers
Import and Export -FAQ

Auto Provisioning Phone Information Parameters

Descriptions for parameters in exported and imported Auto Provisioning Phone Information CSV file.

Parameter	Description	Importance	Restriction	Default Value
Vendor	Phone vendor.	Required	Refer to the permitted value for the supported phone vendor.	N/A
Model	Phone model.	Required	Refer to the permitted value for the supported phone model of various phone vendors.	N/A
MAC Address	MAC address of the phone.	Required	Only numbers `0` - `9`, letters `A` - `Z` or `a` - `z`, hyphens `-` and colons `:` are allowed. The maximum character length is 17, where you can enter a combination of letters or numbers with a total of 12 characters. Examples are given below: • FA-B5-49-1A-2B-3C • FA:B5:49:1A:2B:3C • FAB5491A2B3C	N/A
Template	The configuration template used to provision the phone.	Required	The name of default or custom template. **Tip:** To obtain the value for this parameter, go to **Auto Provisioning > Resource Repository > Default Templates / Custom Templates**, then copy the name in the **Template Name** column.	N/A
Provisioning Method	The method that is used to provision the phone.	Required	Refer to the permitted value for the supported provisioning method of different phone models.	N/A
Hot Desking Phone	Whether to set the phone as a hot desking phone.	Optional	Permitted value: • `0`: Disable. • `1`: Enable. **Note:**	0

Parameter	Description	Importance	Restriction	Default Value
			• **Hot Desking Phone** will be filled with default value `0` if you leave this field empty. • Do NOT set this parameter to `1` for DECT phones, or it will cause error when importing.	
Authentication First-time	Whether to require users to enter authentication information on the phone before triggering the first-time provisioning.	Optional	**Note:** • This parameter only takes effect on the phones that support **RPS** or **RPS FQDN** provisioning method. • If **Hot Desking Phone** is set to `1`, this parameter MUST be `0`, or it will cause error when importing. Permitted value: • `0`: Disable. • `1`: Enable. **Note:** **Authentication First-time** will be filled with a default value if you leave this field empty.	If **Hot Desking Phone** = `0`, the default value will be `1`. Otherwise, the default value will be `0`.
Assign Extension	The extension to be assigned to the phone.	Required if **Hot Desking Phone** = `0`.	**Note:** Do NOT set this parameter if **Hot Desking**	N/A

Parameter	Description	Importance	Restriction	Default Value
			Phone = `1`, or it will cause error when importing. Only numbers are allowed. For IP phones, the maximum character length is 7. For DECT phones, the maximum character length is 1024, and the format should be *`Handset Number`*:*`Extension Number`*. **Note:** Use `&` to separate multiple handsets. For example, `1:1002&2:1005&3:1006`.	

Related information

Export and Import Auto Provisioning Phone Information
Import and Export -FAQ

Auto Provisioning Phone Information Parameters - Permitted Value

This topic provides the permitted values of the import and export Auto Provisioning phone information parameters, including Vendor, Model, and Provisioning Method.

Vendor	Model	Provisioning Method
Yealink	• AX83H, AX86R • CP920, CP925 • SIP-CP935W, SIP-CP960, SIP-CP965 • SIP-T19P_E2, SIP-T20P, SIP-T21_E2,SIP-T21P_E2, SIP-T22P • SIP-T23G, SIP-T23P, SIP-T26P, SIP-T27G, SIP-T28P, SIP-T29G, SIP-T32G, SIP-T38G • SIP-T30, SIP-T30P, SIP-T31, SIP-T31G, SIP-T31P, SIP-T31W, SIP-T33G, SIP-T33P, SIP-T34W • SIP-T40G, SIP-T40P, SIP-T41P, SIP-T41S, SIP-T41U, SIP-T42G, SIP-T42S, SIP-T42U, SIP-T43U, SIP-T44U, SIP-T44W, SIP-T46G, SIP-T46S, SIP-T46U, SIP-T48G, SIP-T48S, SIP-T48U	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn

Vendor	Model	Provisioning Method
	• SIP-T52S, SIP-T53, SIP-T53W, SIP-T54S, SIP-T54W, SIP-T56A, SIP-T57W, SIP-T58, SIP-T58W, SIP-T73W, SIP-T73U, SIP-T74W, SIP-T74U, SIP-T77U, SIP-T85W, SIP-T87W, SIP-T88W, SIP-T88V • SIP-W60B, W70B, SIP-W75DM, SIP-W80DM, SIP-W90DM • VP59 • T64LTE, T67LTE	
Fanvil	• A10, A10W, A308i, A32, A32i, A320, A320i • FH-S01 • H1, H2U, H2U-V2, H3, H3W, H4, H4W, H5, H5W, H6, H6W, H603W • i10, i10D, i10S, i10SD, i10SV, i10V, i11S, i11SV, i12, i16S, i16SV, i16V, i18S • i20S, i23S • i30, i31S, i32V, i33V, i33VF • i504, i505, i506W, i507W, i51, i51W, i52, i52W, i53, i53W, i55A, i56A, i57A • i61, i62, i63, i64, i68 • PA2, PA2S, PA3 • V50P, V60P, V60W, V61G, V61W, V62, V62 Pro, V62G, V62W, V63, V64, V65, V66, V66 Pro, V67 • W610W, W611W, W710D, W710H • X1S/X1SP, X1SG, X2, X2C, X210, X210-V2, X210i, X210i-V2 • X3SG, X3S, X3S(P) Lite, X3S(P) Pro, X3SW, X3SG Lite, X3SG Pro, X3U, X3U Pro, X301, X301G, X301W, X303, X303G, X303W, X305, X303-2 WIRE • X4, X4U, X4U-V2, X5U, X5U-V2, X5S • X6, X6U, X6U-V2 • X7, X7A, X7C, X7-V2, X7C-V2 • Y501, Y501W, Y501-Y, Y501W-Y	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Grandstream	• GAC2500, GAC2570 • GRP2601, GRP2601P, GRP2602, GRP2602P, GRP2602G, GRP2602W, GRP2603, GRP2603P, GRP2604, GRP2604P • GRP2612, GRP2612P, GRP2612G, GRP2612W, GRP2613, GRP2614, GRP2615, GRP2616 • GRP2624, GRP2634, GRP2670 • GXP1610, GXP1620, GXP1625, GXP1628, GXP1630 • GXP2130, GXP2135, GXP2140, GXP2160, GXP2170	• pnp • dhcp • provision_link • provision_link_fqdn

Vendor	Model	Provisioning Method
	• GHP610, GHP610W, GHP611, GHP611W, GHP620, GHP620W, GHP621, GHP621W, GHP630, GHP630W, GHP631, GHP631W • WP825	
Htek	• UC803T • UC902, UC902S, UC903 • UC912, UC912G, UC912E • UC921, UC921G, UC923, UC923U, UC924, UC924E, UC924U, UC924W, UC926, UC926E, UC926U • UCV10, UCV20, UCV50, UCV52, UCV53	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Gigaset	• Gigaset N610 IP PRO, Gigaset N670 IP PRO • Gigaset N870 IP PRO, Gigaset N870 VI PRO • GigasetP82x, GigasetP85x, GigasetP710, GigasetP810 • Maxwell Basic PRO • Maxwell 2 PRO, Maxwell 3 PRO, Maxwell 4 PRO	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Snom	• HD100, HD101, HD300, HD350W, HD351W, HM201 • M100KLE, M500 • snomD120, snomD140, snomD150 • snomD315, snomD335, snomD385 • snom710, snom712, snomD713, snom715, snomD717, snom720, snom725, snomD735, snomD785 • snomD812, snomD815, snomD862, snomD865 • snomM300, snomM400, snomM900 • snomSP800 • snomPA1P	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Flyingvoice	• FIP10, FIP11C, FIP12WP, FIP13G, FIP14G, FIP15G, FIP15GPlus, FIP16, FIP16Plus • P10, P10P, P10G, P10W, P10LTE, P11, P11P, P11G, P11W, P11LTE • P20, P20P, P20W, P20G, P21, P21P, P21W, P22P, P22G, P23G, P23GW, P24G • flyphone • i86Box_Basic, i86Box_Indoor, i86Box_2Line, i86Box_PCBA, i86Box_NFC	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Alcatel-Lucent Enterprise	• H2, H2P, H3P, H3G, H6 • M3, M3s, M5, M5s, M7, M7s, M7s-Pro, M8	• pnp • dhcp

Vendor	Model	Provisioning Method
		• provision_link • provision_link_fqdn
Tiptel	• 3310, 3320, 3330, 3340	• pnp • dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Dinstar	• C60S, C60L, C60U, C61S, C62S, C62G, C63S, C63G, C64G, C66G	• pnp • dhcp • provision_link • provision_link_fqdn
Vtech	• CTM-S2211-SPK, CTM-S2210-X, CTM-S2411-X • NG-S3211W, NG-S3311, NG-S3411W	• pnp • dhcp • provision_link • provision_link_fqdn
Mitel	• 6863i, 6865i, 6867i, 6869i, 6873i • 6920, 6930, 6940, 6905, 6910, 6915 • RFP 44, RFP 45, RFP 47, RFP 48	• dhcp • provision_link • provision_link_fqdn
Cisco	• Cisco3905 • Cisco7821 • Cisco7861 • Cisco7911 • Cisco7942 • Cisco7975 • Cisco8811 • Cisco8845 • SPA501G, SPA502G, SPA504G, SPA508G, SPA509G, SPA512G, SPA514G, SPA301, SPA303, SPA525G2	• dhcp
Avaya	• J129, J139, J159, J169, J179, J189	• dhcp

Vendor	Model	Provisioning Method
	• 9608	• provision_link • provision_link_fqdn
Poly	• Edge_E100, Edge_E220,Edge_E300, Edge_E320, Edge_E350, Edge_E400, Edge_E450, Edge_E500, Edge_E550 • VVX_101, VVX_201, VVX_301, VVX_310, VVX_311, VVX_401, VVX_410, VVX_411, VVX_501, VVX_601, VVX_150, VVX_250, VVX_350, VVX_450	• dhcp • rps • rps_fqdn • provision_link • provision_link_fqdn
Wildix	• WP410R2, WP480R2, WP480R3, WP480R4, WP490R2, WP490R3	• dhcp • provision_link • provision_link_fqdn
Xenios	• ICD012	• dhcp • provision_link • provision_link_fqdn
Huawei	• eSpace 7910, eSpace 7950, eSpace 8950, eSpace 8950HK • IP Phone 7920, IP Phone 7960	• dhcp • provision_link • provision_link_fqdn
NEC	• DT700 ITL-2E-1P, DT700 ITL-6DE-1P, DT700 ITL-12D-1P, DT700 ITL-24D-1P, DT700 ITL-8LD-1P, DT700 ITL-8LDE-1P, DT700 ITL-12DG-3P, DT700 ITL-12CG-3P • DT820 ITY-6D-1P, DT820 ITY-8LDX-1P, DT820 ITY-8LCGX-1P, DT820 ITY-6DG-1P, DT820 ITY-32LDG-1P, DT820 ITY-32LCG-1P • DT900 ITK-6D-1P, DT900 ITK-12D-1P, DT900 ITK-8LCX-1P, DT900 ITK-8TCGX-1P, DT900 ITK-6DG-1P, DT900 ITK-12DG-1P, DT900 ITK-32LCG-1P, DT900 ITK-32TCG-1P, DT900S ITK-6DGS-1P, DT900S ITK-32LCGS-1P, DT900S ITK-32TCGS-1P	• dhcp • provision_link • provision_link_fqdn

Trunk Parameters

Descriptions for parameters in exported and imported Trunk CSV file.

> **Note:**
> Only SIP Peer Trunk and Register Trunks can be exported and imported.

Parameter	Description	Importance	
Name	The trunk name.	Required	The maximum character length is Space and special characters are Trunk's name cannot be duplicate
Trunk Status	Whether to enable or disable the trunk.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Trunk Status** will be filled empty.
Trunk Type	Trunk type.	Required	Permitted value: • `peer` • `register` **Note:** • Importing Account • **Trunk Type**will be leave this field emp
Transport	The transport protocol that is provided by the ITSP.	Required	Permitted value: `udp`, `tcp`, `tls`, or **Note:** **Transport** will be filled wi fields empty.
Hostname/IP	The IP address or the domain of the ITSP.	Required	The maximum character length is

Parameter	Description	Importance	
Port	The trunk port.	Required	Only numbers between 0 and 655
Domain	The domain in SIP URI of a specific header like From, To header. **Note:** If the domain is not provided by ITSP, enter the same value as **Hostname/IP**.	Required	The maximum character length is
Username	The username to register to the ITSP.	Required if **Trunk Type** = *register*	The maximum character length is
Password	The password that is associated with the username.	Required if **Trunk Type** = *register*	The maximum character length is
Authentication Name	The authentication name to register to the ITSP.	Optional	The maximum character length is
Enable Outbound Proxy	Whether to enable or disable outbound proxy.	Required if **Trunk Type** = *register*	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Enable Outbound Proxy** leave this field empty.
Outbound Proxy Server	The address of outbound proxy server.	Required if **Enable Outbound Proxy** = *1*	The maximum character length is
Port of Outbound Proxy Server	The port of outbound proxy server.	Required if **Enable Outbound Proxy** = *1*	Only numbers between 1 and 655
SBC Routing	Whether all communication messages between the PBX and this trunk will be routed through the SBC.	Optional	Permitted value: • *0*: Disable • *1*: Enable **Note:** **SBC Routing** will be filled empty.
Codec Setting	The audio codec for trunk.	Required	Permitted value: *ulaw*, *alaw*, *g729*, *g726*, *speex*, *adpcm*, *vp8*, or *mpeg*

Parameter	Description	Importance	
			For multiple Codec, please enter e.g. first_value1&second_value2. **Note:** If the value you enter is nc skipped.
DTMF Mode	The default mode for sending DTMF tones.	Required	Permitted value: *rfc4733*, *info*, * **Note:** **DTMF Mode** will be filled field empty.
DTMF FMTP	The value of the DTMF fmtp attribute when the DTMF mode is *rfc4733*.	Optional	Permitted value: *0-16*, *0-15*. **Note:** This field will be filled with empty.
Qualify	Whether to send SIP OPTION packet to check if the SIP device is up.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Qualify** will be filled with
Enable SRTP	Whether to enable or disable SRTP (encrypted RTP) for the trunk.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Enable SRTP** will be filled empty.
T.38 Support	Whether to enable or disable T.38 fax.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:**

Parameter	Description	Importance	
			T.38 Support will be fille empty.
Inband Progress	Whether to enable or disable inband progress.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Inband Progress** will be field empty.
Ignore 183 Message without SDP	Whether to ignore 183 messages without SDP.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Ignore 183 Message wit** if you leave this field empt
Forward the 180 (SDP) Message Following the Peer's Format	Whether the PBX will send a 180 message with SDP, depending on whether the 180 message received from the other party contains SDP.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Forward the 180 (SDP)** will be filled with default va
Enable RTP Keep-alive	Whether to enable or disable RTP keep-alive.	Optional	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Enable RTP Keep-alive** leave this field empty.
Maximum Concurrent Calls	Specify the maximum number of concurrent calls allowed in the trunk.	Required	Only numbers are allowed. Specially, 0 means unlimited. The maximum character length is

Parameter	Description	Importance	
			Note: **Maximum Concurrent C** leave this field empty.
Call Restriction Type	Specify based on which type of calls to define the maximum number of concurrent calls for this trunk.	Required	Permitted value: *outbound* or *all* **Note:** **Call Restriction Type** wi you leave this field empty.
Default Outbound Caller ID	The caller ID that is displayed on the callee's device.	Optional	Numbers, letters, and characters The maximum character length is **Note:** The outbound caller ID sh
Default Outbound Caller ID Name	The caller ID name that is displayed on the callee's device.	Optional	The maximum character length is
Get Caller ID From	Decide from which header field will the trunk retrieve Caller ID.	Required	Permitted value: • *follow_system*: [Follow S • *from*: From • *contact*: Contact • *rpid*: Remote-Party-ID • *pai*: P-Asserted-Identity • *ppi*: P-Preferred-Identity **Note:** **Get Caller ID From** will b you leave this field empty.
Get DID From	Different devices or providers may contain DID numbers in different SIP headers. When an inbound call through a SIP trunk reaches the PBX, the PBX needs to retrieve a correct DID number, or the call will fail. Adjust the setting after analysis of the SIP packets sent from the trunk provider.	Required	Permitted value: • *follow_system*: [Follow S • *to*: To • *invite*: Invite • *diversion*: Diversion • *rpid*: Remote-Party-ID • *pai*: P-Asserted-Identity • *ppi*: P-Preferred-Identity • *pcpid*: P-Called-Party-ID

Parameter	Description	Importance	
			Note: **Get DID From** will be fille leave this field empty.
From User Part	A From header contains caller ID and caller ID name. **From User Part** indicates caller ID.	Required	Permitted value: • `default`: [Default] • `ext_cid`: Extension Caller • `trunk_user`: Trunk Userna **Note:** Only available whe • `trunk_def_outbcid`: Trun • `ext_outbcid`: Extension's • `outrounter_outbcid`: Ou • `originator_cid`: Originat • A customized value. **Note:** Fill in a desired val is 31. Only number are allowed. **Note:** **From User Part** will be fil this field empty.
From Display Name Part	A From header contains caller ID and caller ID name. **From Display Name Part** indicates caller ID name.	Required	Permitted value: • `default`: [Default] • `ext_cid_name`: Extension • `trunk_def_outbcid_name` • `ext_outbcid_name`: Exten • `originator_cid_name`: O • A customized value. **Note:** Fill in a desired val is 63. **Note:**

Parameter	Description	Importance	
			From Display Name Par you leave this field empty.
Diversion	Define the parameters included in the Diversion SIP header.	Optional	Permitted value: • *default*: [Default] • *ext_cid*: Extension Caller • *trunk_user*: Trunk Usern **Note:** Only available whe • *trunk_def_outbcid*: Trun • *ext_outbcid*: Extension's • *outrounter_outbcid*: Ou • *originator_cid*: Originat • A customized value. **Note:** Fill in a desired val is 31. Only number allowed. **Note:** Leave **Diversion** field em parameter with SIP INVIT
Remote-Party-ID	Define the parameters included in the Remote-Party-ID SIP header.	Optional	Permitted value: • *default*: [Default] • *ext_cid*: Extension Caller • *trunk_user*: Trunk Usern **Note:** Only available whe • *trunk_def_outbcid*: Trun • *ext_outbcid*: Extension's • *outrounter_outbcid*: Ou • *originator_cid*: Originat • A customized value. **Note:**

Parameter	Description	Importance	
			Fill in a desired val is 31. Only number allowed. **Note:** Leave **Remote-Party-ID** this parameter with SIP IN
P-Asserted-Identity	Define the parameters included in the P-Asserted-Identity SIP header.	Optional	Permitted value: • *default*: [Default] • *ext_cid*: Extension Caller • *trunk_user*: Trunk Usern **Note:** Only available whe • *trunk_def_outbcid*: Trun • *ext_outbcid*: Extension's • *outrounter_outbcid*: Ou • *originator_cid*: Originat • A customized value. **Note:** Fill in a desired val is 31. Only number allowed. **Note:** Leave **P-Asserted-Identi** this parameter with SIP IN
P-Preferred-Identity	Define the parameters included in the P-Preferred-Identity SIP header.	Optional	Permitted value: • *default*: [Default] • *ext_cid*: Extension Caller • *trunk_user*: Trunk Usern **Note:** Only available whe • *trunk_def_outbcid*: Trun • *ext_outbcid*: Extension's

Parameter	Description	Importance	
			• `outrounter_outbcid`: Ou • `originator_cid`: Originat • A customized value. **Note:** Fill in a desired val is 31. Only number allowed. **Note:** Leave **P-Preferred-Iden** this parameter with SIP IN
From Host Part	Define the domain or IP address to be used in the **From** field of a SIP INVITE header.	Required	**Note:** This parameter is only req Permitted value: • `default`: [Default] • A customized value. **Note:** Fill in a desired val is 255.
To Host Part	Define the domain or IP address to be used in the **To** field of a SIP INVITE header.	Required	**Note:** This parameter is only req Permitted value: • `default`: [Default] • A customized value. **Note:** Fill in a desired val is 255.
User Agent	If the ITSP requires User Agent for authentication, enter the User Agent information that is provided by the ITSP.	Optional	The maximum character length is

Parameter	Description	Importance	
Realm	Realm is a string displayed to users so they know which username and password to use.	Optional	The maximum character length is
Send Privacy ID	Whether to send the Privacy ID in SIP header or not.	Required	Permitted value: • *0*: Disable • *1*: Enable
User Phone	Whether to add the parameter `user=phone` as a request line in the header field of the SIP INVITE packet.	Required	Permitted value: • *0*: Disable • *1*: Enable
Send X-OpenAPI-Call-ID	Set whether to include a `X-OpenAPI-Call-ID` field in the SIP INVITE packet to carry the Call ID for inbound calls and outbound calls routed through the trunk.	Required	Permitted value: • *0*: Disable • *1*: Enable
100rel	Configure 100rel for this trunk.	Required	Permitted value: • *Required*: 100rel is require • *Supported*: 100rel is supp • *Disabled*: 100rel is disabl
Maxptime	Select the value of the Maxptime used when the PBX sends the INVITE packet.	Required	Permitted value: • *default*: PBX will send a the codec that is used for t • A customized value. **Note:** Fill in a desired val of 10 ranging from **Note:** **Maxptime** will be filled wi field empty.
Support P-Early-Media	Set whether the P-Early-Media field is included in the INVITE packet.	Required	Permitted value: • *0*: Disable • *1*: Enable

Parameter	Description	Importance	
Select which IP address to use in 'Contact'(SIP) and 'Connection'(SDP) fields	Decide which IP address will be used in 'Contact'(SIP) and 'Connection'(SDP) fields.	Required	Permitted value: • `default_settings`: Use tl default. • `custom_ip`: Use the custo **Note:** • Only available whe • **Select which IP a 'Connection'(SDF** `default_settings`
IP Address	The custom IP address that will be used in 'Contact'(SIP) and 'Connection'(SDP) fields.	Required if **Select which IP address to use in 'Contact'(SIP) and 'Connection'(SDP) fields** = `custom_ip`	IP address in IPv4 or IPv6 format

Related reference

Trunk DIDs/DDIs Parameters

Related information

Export and Import SIP Trunks

Import and Export -FAQ

Trunk DIDs/DDIs Parameters

Descriptions for parameters in exported and imported Trunk DIDs/DDIs CSV file.

Parameter	Description	Importance	Restriction	Default Value
DID/DDI	A virtual number that is used to identify which path of the trunk is passing the call.	Required	Numbers, letters, and characters `[ ] * # ( ) . - + !` are allowed. The maximum character length is 31.	N/A
DID/DDI Name	The name of DID/DDI that is used to identify	Optional	The maximum character length is 127.	N/A

Parameter	Description	Importance	Restriction	Default Value
	which path of the trunk is passing the call.			

Related information

Export and Import Trunk DIDs/DDIs Numbers
Import and Export -FAQ

Trunk Outbound Caller ID Parameters

Descriptions for parameters in exported and imported Trunk Outbound Caller ID CSV file.

Check the parameter descriptions for the following types of trunk outbound caller IDs according to your needs.

- Outbound Caller ID for standard outbound calls
- Outbound Caller ID for campaign outbound calls

Outbound Caller ID for standard outbound calls

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	N/A

Parameter	Description	Importance	Restriction	Default Value
			ID and the end caller ID with separator -, e.g. 5503301-5503310. • The start number and the end number must have the same amount of digits and both contain character + or neither. The range of start number and end number cannot exceed 500. • Then fill the extension range in Associated Extensions. The extension range and the outbound caller ID range must have the same amount of numbers.	
Outbound Caller ID Name	The caller ID that is displayed on the callee's device for specific extensions.	Optional	The maximum character length is 127.	N/A
Default DOD Label	The default label for the outbound caller ID that is displayed when extension users selecting a DOD to dial out.	Optional	The maximum character length is 127.	N/A
Associated Extensions	The extensions that are associated with the Outbound Caller ID and Outbound Caller Name.	Required	Permitted value: one or more extension numbers and extension group names existed in PBX. • For multiple extensions or groups, please enter the numbers or names and use & as a separator, e.g. extension_number1&extension_number2&extension_group_name3. • If the extensions or groups you enter are not existing in PBX, it will be skipped. • For extension range, please fill in the start extension number and the end extension number with separator -, e.g. 1001-1010.	N/A

Parameter	Description	Importance	Restriction	Default Value
			The maximum number length is 7 (for each number).	

Outbound Caller ID for campaign outbound calls

Parameter	Description	Importance	Restriction	Default Value
Outbound Caller ID	The caller ID that is displayed on the callee's device.	Required	The maximum character length is 31(for each caller ID). Only numbers are allowed	N/A
Outbound Caller ID Name	The caller ID that is displayed on the callee's device.	Optional	The maximum character length is 127.	N/A

Related information

Export and Import Trunk Outbound Caller IDs
Import and Export -FAQ

Inbound Caller ID Reformatting Rule Parameters

Descriptions for parameters in exported and imported 'Inbound Caller ID Reformatting Rule' CSV file.

Parameter	Description	Importance	Restriction	Default Value
Patterns	The inbound caller ID that matches this pattern will be reformatted.	Required	Numbers, letters, and characters `[ ] * # ( ) . - + !` are allowed. The maximum character length is 31.	N/A
Strip	Specify how many digits will be stripped from the beginning of the inbound caller ID.	Optional	Only numbers are allowed. The maximum character length is 2.	N/A
Prepend	Specify the digits that will be prepended to the inbound caller ID.	Optional	Numbers, letters, and characters `( ) . - + * #` are allowed. The maximum character length is 31.	N/A

Related information

Export and Import Inbound Caller ID Reformatting Rules
Import and Export -FAQ

DID Number to Specific Extension Parameters

Descriptions for parameters in exported and imported 'DID Number to Specific Extension' CSV file.

Parameter	Description	Importance	Restriction	Default Value
DID Number	The specific DID number that is used to match the callee number. Only when the callee number is equal to the DID number will the inbound call go through the inbound route.	Required if **DID Matching Mode** = `pattern_to_ext_list`	The maximum character length is 31. Only numbers, letters, and characters `( ) . - + * #` are allowed.	N/A
Extension Matched	The destination of the specific DID number. The DID number and the extension is in one-to-one correspondence.	Required if **DID Matching Mode** = `pattern_to_ext_list`	Permitted value: Extension numbers	N/A

Related information

Import and Export -FAQ

Inbound Route Parameters

Descriptions for parameters in imported and exported Inbound Route CSV file.

Parameter	Description	Importance	Restriction	Default Value
Name	The name of inbound route.	Required	Space and special characters are not allowed. Inbound route's name cannot be duplicated.	N/A

Parameter	Description	Importance	Restriction	Default Value
			The maximum character length is 63.	
Inbound Alert Info	The Alert Info field is used to configure distinctive ring tones for incoming calls.	Optional	Only numbers and letters are allowed. The maximum character length is 31.	N/A
DID Matching Mode	The DID matching mode.	Optional	Permitted value: • *patterns*: DID Patterns • *pattern_to_ext*: DID Pattern to Extensions • *range_to_ext*: DID Range to Extension Range • pattern_to_ext_list: DID Number to Specific Extension **Note:** **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, 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	N/A

Parameter	Description	Importance	Restriction	Default Value
			allowed. The maximum character length is 31. The **Default Destination** must be *pattern_to_ext*, then fill multiple extension numbers with separator *&* in Number. • If **DID Matching Mode** = *range_to_ext*, only numbers and character + (before numbers) are allowed. The maximum character length is 16 (for each DID). Please enter the start DID and the end DID with separator -, e.g. 5503301-5503305. The **Default Destination** must be *range_to_ext*, then fill the start number and the end number with separator - in Number, e.g. 1001-1005.	
Caller ID Matching Mode	The Caller ID matching mode.	Required	**For Enterprise/Ultimate Plan**: Permitted value: • *patterns*: Caller ID Matching Settings • *phonebook*: Match Contacts' Caller ID in Specific Phonebooks **Note:** **Caller ID Matching Mode** will be filled with default value *patterns* if you leave this fields empty.	patterns
Caller ID Pattern	The pattern used to match caller ID. Only when the caller ID matches the pattern can	Optional	• If **Caller ID Matching Mode** = *patterns*, the maximum character length is 31 (for each pattern). Numbers,	N/A

Parameter	Description	Importance	Restriction	Default Value
	user dials in through this route.		letters, characters `[ ] * # ( ) . - + !` are allowed. For multiple patterns, enter patterns and use `&` as a separator, e.g. pattern1&pattern2. • If **Caller ID Matching Mode** = `phonebook`, the permitted value is one or more phonebook names existed in PBX. For multiple phonebook names, enter names and use `&` as a separator, e.g. name1&name2. If the phonebook you enter does not exist in PBX, it will be skipped.	
Trunks	The trunks that incoming calls will be routed by this inbound route. The PBX will route inbound calls through this route when external users call the selected trunk number.	Required	Permitted value: one or more trunk names existed in PBX. For multiple trunks, please enter trunk names and use `&` as a separator, e.g. name1&name2. **Note:** If the trunks you enter are not existing in PBX, Trunks will be skipped.	N/A
Default Destination	The default destination to receive inbound calls.	Required	Permitted value: • `end_call`: Hang up • `extension`: Extension • `range_to_ext`: Match extension Range (DID Matching Mode = range_to_ext) • `pattern_to_ext`: Match selected Extension (DID Matching Mode = pattern_to_ext)	end_call

Parameter	Description	Importance	Restriction	Default Value
			• `pattern_to_ext_list`: DID number match specific extension (DID Matching Mode = pattern_to_ext_list) • *`ext_vm`*: Extension Voicemail • *`group_vm`*: Group Extension • *`ivr`*: IVR • *`ring_group`*: Ring Group • *`queue`*: Queue • *`conference`*: Conference • *`fax_to_email`*: Fax to Email **Note:** **Default Destination** will be filled with default value *`end_call`* if you leave these fields empty.	
Number of Default Destination	The destination number to receive inbound calls.	Required if **Default Destination** ≠ *`end_call`* or *`pattern_to_ext_list`*	Permitted value: • If **Default Destination** = *`Extension`*, *`Extension Email`*, *`Group Voicemail`*, *`IVR`*, *`Ring Group`*, *`Queue`*, *`Conference`*, or *`Fax to Email`*, please fill in a number. • If **Default Destination** = *`Match extension Range`*, please fill in a range of extension, e.g. 1000-1010. The maximum number length is 7 (for each number). • If **Default Destination** = *`Match selected Extension`*, please fill in numbers or names and use *`&`* as a separator, e.g. extension_number1&extension_number2&extension_group_name3.	N/A

Parameter	Description	Importance	Restriction	Default Value
			Note: If the numbers or names you enter are not existing in PBX, Number of Default Destination will be skipped.	
Enable Fax Detection	Whether to enable or disable FAX detection.	Required	Permitted value: • `0`: Disable • `1`: Enable **Note:** **Enable Fax Detection** will be filled with default value `0` if you leave this field empty.	0
Fax Destination	The destination to receive fax.	Required if **Enable Fax Detection** = `1`	Permitted value: • `end_call`: Hang Up • `extension`: Extension • `fax_to_email`: Fax to Email **Note:** **Fax Destination** will be filled with default value `extension` if you leave this field empty.	extension
Number of Fax Destination	The destination number to receive fax.	Required if **Fax Destination** ≠ `end_call`	Permitted value: extension numbers existed in PBX. • If **Fax Destination** = `Extension`, fax will be sent to extension number. • If **Fax Destination** = `Fax to Email`, fax will be sent to extension's email address.	N/A

Related reference

DID Number to Specific Extension Parameters

Related information

Export and Import Inbound Routes

Import and Export -FAQ

Outbound Route Parameters

Descriptions for parameters in exported and imported Outbound Route CSV file.

Parameter	Description	Importance	Restriction	Default Value
Name	The name of outbound route.	Required	Space and special characters are not allowed. Outbound route's name cannot be duplicated. The maximum character length is 63.	N/A
Outbound Caller ID	The caller ID that is displayed on the callee's device.	Optional	Numbers, letters, and characters `[ ] ( ) . - + * #` and placeholder `{{.Ext}}` are allowed. The maximum character length is 31.	patterns
Pattern	The pattern used to match a callee number. Only when the callee number is matched will the outbound call go through this route.	Required	Numbers, letters, and characters `[ ] * # ( ) . - + !` are allowed. The maximum character length is 31. **Note:** **Pattern** will be filled with default value `X.` if you leave these fields empty.	X.
Strip	The number of digits that will be stripped from the front of callee number before the call is placed.	Optional	Only numbers 1 - 16 are allowed.	N/A
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

Parameter	Description	Importance	Restriction	Default Value
Trunks	The trunks that can be used to dial out. The PBX will route outbound calls through this trunk when the dialed number matches the outbound route.	Required	Permitted value: one or more trunk names existed in PBX. For multiple trunks, please enter trunk names and use *&* as a separator, e.g. name1&name2. **Note:** If the trunk you enter does not exist in PBX, it will be skipped.	N/A
Rrmemory Hunt	Whether to remember which trunk was used last time, and then use the next available trunk to call out.	Required	Permitted value: • *0*: Disable • *1*: Enable **Note:** **Rrmemory Hunt** will be filled with default value *0* if you leave this field empty.	0
Extensions	The extensions that are allowed to make outbound calls through this route.	Optional	Permitted value: one or more extension numbers, extension group names, or organization names existed in PBX. **Format**: • When entering the organization name, you must enter the complete path with parent organization(s) connected by character `/`, and with the prefix `Organization_`, i.e. `Organization_{Parent Organization}/{Organization Name}`. For example, `Organization_Yeastar/Marketing Center/Training Team`. • For multiple extensions, extension groups, or	extension

Parameter	Description	Importance	Restriction	Default Value
			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:** If the PIN list name you entered is not existing in PBX, it will be skipped.	N/A

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:** **Action** will be filled with default value *accept* if you leave this field empty.	accept
Object Type	The type of the source traffic.	Required	Permitted value: *ip*, *domain*, or *mac*. **Note:**	ip

Parameter	Description	Importance	Restriction	Default Value
			Object Type will be filled with default value *ip* if you leave this field empty.	
Source IP Address	The source IP address.	Required if **Object Type** = *ip*	Must be IPv4 address format XXX.XXX.XXX.XXX.XXX: 0 - 255	N/A
Subnet Mask	The subnet mask.	Required if **Object Type** = *ip*	Must be IPv4 address format XXX.XXX.XXX.XXX.XXX: 0 - 255	N/A
Domain	The domain name.	Required if **Object Type** = *domain*	The maximum character length is 255.	N/A
MAC Address	The MAC address.	Required if **Object Type** = *mac*	Only numbers, letters *A* to *F*, *a* to *f* and character *-:* are allowed. The character length must be 12 or 17.	N/A
Service/Port Range	The type of defense objects.	Required if **Action** = *drop* or *reject* (leave it empty if **Action** = *accept*)	Permitted value: *service* or *port_range*. **Note:** **Service/Port Range** will be filled with default value *service* if you leave this field empty.	service
Service	The service to which the rule is applied.	Required if **Service/Port Range** = *service*	Permitted value: • *sip* • *web* • *linkus* • *ssh* • *ami* • *database_grant* • *ldap* • *ftp* • *tftp*	N/A
Start Port	The start port.	Required if **Service/Port Range** = *port_range*	Only numbers between 1 and 65535 are allowed. Start port must be less than or equal to end port.	1
End Port	The end port.	Required if **Service/Port**	**Note:**	65535

Parameter	Description	Importance	Restriction	Default Value
		Range = *port_range*	**Start Port** and **End Port** will be filled with default port range if you leave these fields empty.	
Protocol	The protocol to which the rule is applied.	Required	Permitted value: *both*, *udp*, or *tcp*. **Note:** **Protocol** will be filled with default value *both* if you leave this field empty.	both

Related information

Export and Import Static Defense Rules
Import and Export -FAQ

Auto Defense Rule Parameters

Descriptions for parameters in exported and imported 'Auto Defense Rule' CSV file.

Parameter	Description	Importance	Restriction	Default Value
Name	The name of defense rule.	Required	The maximum character length is 127. Auto defense's name cannot be duplicated.	N/A
Service/Port Range	The type of defense objects.	Required	Permitted value: *service* or *port_range*. **Note:** **Service/Port Range** will be filled with default value *service* 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* • *sip_udp*	N/A

Parameter	Description	Importance	Restriction	Default Value
			• *sip_tcp* • *sip_tls* • *outbound_sip* • *rtp* • *linkus* • *ami* • *database_grant* • *ldap* • *ftp* • *tftp*	
Start Port	The start port.	Required if **Service/Port Range** = *port_range*	Only numbers between 1 and 65535 are allowed. Start Port must be less than or equal to End Port.	1
End Port	The end port.	Required if **Service/port Range** = *port_range*	**Note:** **Start Port** and **End Port** will be filled with default port range if you leave these fields empty.	65535
Protocol	The protocol to which the rule is applied.	Required	Permitted value: • *both* • *udp* • *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 specific time interval.	Required	Only numbers between 1 and 255 are allowed.	N/A
Time Interval(s)	The time interval (in seconds) to receive IP packets.	Required	Only numbers are allowed. The maximum character length is 5.	N/A

Related information

Export and Import Auto Defense Rules
Import and Export -FAQ

Outbound Call Frequency Restriction Rule Parameters

Descriptions for parameters in exported and imported 'Outbound Call Frequency Restriction' CSV file.

Table 39.

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**: *{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.	N/A

Table 39. (continued)

Parameter	Description	Importance	Restriction	Default Value
			{time_unit}: Permitted value: *second* or *minute*.	

Related information

Export and Import 'Outbound Call Frequency Restriction' Rules
Import and Export -FAQ

Rate Parameters

Descriptions for parameters in exported and imported Rate CSV file.

Parameter	Importance	Restriction	Default Value
Name	Required	The maximum character length is 127.	N/A
Match Prefix	Optional	The maximum character length is 31. Numbers, letters, and characters *[]*#().-+!* are allowed.	N/A
Number Length	Optional	The maximum character length is 2. Only numbers are allowed.	N/A
Rate	Required	The maximum character length is 7. Only numbers and characters . are allowed.	0
Billable Unit(s)	Required	The maximum character length is 3. Only numbers are allowed.	60
Initial Time(s)	Required	The maximum character length is 3. Only numbers are allowed.	0
Initial Cost	Required	The maximum character length is 7. Only numbers and characters . are allowed.	0

Related information

Export and Import Call Rate Rules
Import and Export -FAQ

Allowed Numbers Parameters

Descriptions for parameters in exported and imported Allowed Numbers CSV files.

Table 40.

Parameter	Importance	Restriction	Default Value
Name	Required	The maximum character length is 127.	N/A
Type	Required	Permitted value: • *inbound*: Allow the number(s) to call into the PBX. • *outbound*: Allow PBX extensions to call the number(s). • *both*: Allow the number(s) to call into the PBX and allow PBX extensions to call the number(s). **Note:** **Type** will be filled with default value *inbound* if you leave this field empty.	inbound
Number	Required	Numbers, letters, and characters `[ ] * # ( ) . - + !` are allowed. For multiple numbers or number patterns, use *&* as a separator, eg. number1&number2.	N/A

Related information

Import and Export -FAQ

Blocked Numbers Parameters

Descriptions for parameters in exported and imported Blocked Numbers CSV files.

Table 41.

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

Hotel Management Guide

Yeastar P-Series Software Edition

Version: 83.18.0.18
Date: 2025-01-14

+86-592-5503309 sales@yeastar.com www.yeastar.com

Contents

Hotel Management Overview

Yeastar P-Series Software Edition comes with a built-in hotel module, enabling hotels to deliver communication services and manage business operations seamlessly from a single platform.

Yeastar's hospitality-focused solutions

Yeastar offers a comprehensive suite of hospitality solutions tailored to hotels of different sizes, empowering hotels to streamline service delivery and enhance guest experience.

Yeastar P-Series Software Edition supports the following solutions:

Built-in Hotel Management module

The hotel management module enables hotels to deliver hospitality features together with a rich set of telephony features on a single platform, eliminating the need to switch between different systems. Leveraging the robust service panels from Linkus Desktop/Web Client, guest check-ins/outs, rooms assignments, wake-up calls, etc. can be completed with just a few clicks.

FIAS-based PMS integration

Easy integration with Oracle Hospitality Opera, Micros Fidelio, and other PMS supporting FIAS protocol. Hoteliers can retain their current PMS system while benefiting from reliable communication services powered by Yeastar PBX.

For more information, see Hotel PMS Integration Guide.

Custom integration using Open API

Custom integration with current hotel management system via PBX's inbuilt open APIs.

For more information, see Hotel APIs.

Requirements

PBX

Item	Requirement
Subscription	Enterprise Plan or Ultimate Plan
Version	83.18.0.18 or later

Linkus Desktop Client

The version of Linkus Desktop Client is 1.9.3 or later.

Key takeaways

Below are the key takeaways to help you get started with hotel management module.

Hotel Manager

1. Plan numbering and complete the setup.
   - **Service number(s) for hotel service** (such as 24-hour front desk, laundry service, restaurant, etc.): All guests can call service number(s) from their room phones, regardless of check-in status.

     To create service number, see Extension Overview.
   - **Emergency number for emergency calling**: All guests can call emergency number from their room phones, regardless of check-in status.

     To add emergency number, see Emergency Calling Overview.
   - **Extension numbers for room phones**: Extension number needs to be registered on the room phone, so that guests can make calls.

     To create extension number, see Extension Overview.
   - **Wake-up number for alarms**: All guests can call this number to query, add, or delete their own wake-up calls from room phone.

     The number is available to set when you enable and set up hotel service on PBX.
2. Set up Hotel Service on Yeastar P-Series Software Edition.
3. Enable co-management for the hotel service.
   - Grant hotel management permission to enable co-management of the hotel service.
   - Grant call management permission to enable staffs to manage guest calls.
   - Grant guest room management permission to enable staffs to assist in room operations such as check-ins/outs, room assignments, wake-up calls, etc.
4. Set up hotel calling and tracking.
   - Grant room-to-room and outbound call permission to guests.
   - Set up call rate to bill guests for outbound calls.
   - Schedule call reports to track call activities

Front Desk

Front desk can efficiently manage day-to-day hotel operations from the robust service panels on Linkus Desktop/Web Client.

The supported operations are listed below:

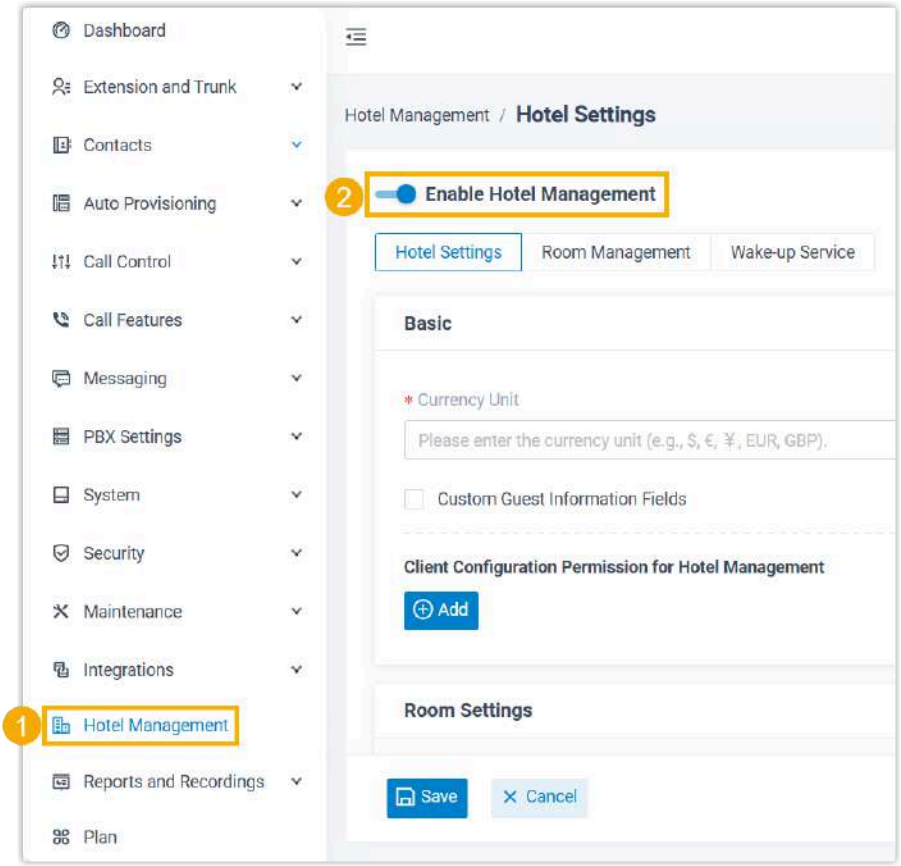
- Check in
- Move Rooms
- Set Do Not Disturb (DND)
- Change Room Status
- Schedule and manage wake-up calls
    - Schedule Wake-up Calls
    - Query Scheduled Wake-up Calls
    - Update Scheduled Wake-up Calls
    - Delete Scheduled Wake-up Calls
    - Check Wake-up Call Logs
- Check out
- Manage Guest Calls
- View and Manage Guest Stay History
- Check Guest Bills and Invoices

Hotel Manager

Set up Hotel Service on Yeastar P-Series Software Edition

This topic describes how to enable and set up hotel service on Yeastar P-Series Software Edition.

Step 1. Enable hotel service



1. Log in to PBX web portal, go to **Hotel Management**.
2. Turn on the switch **Enable Hotel Management**.

Step 2. Configure basic hotel settings

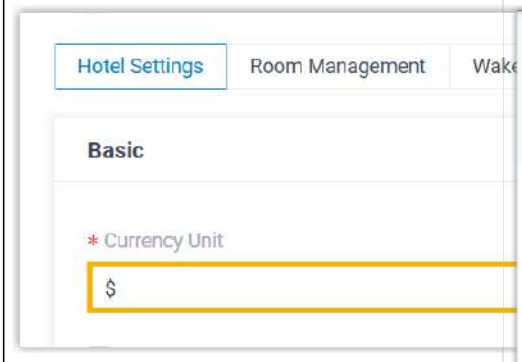
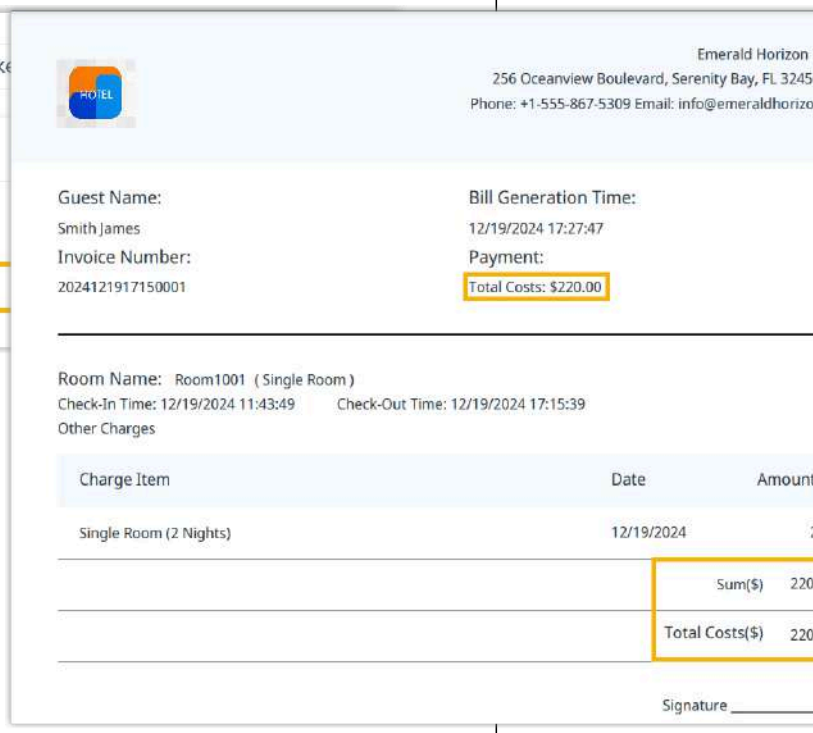
Go to **Hotel Settings** tab to configure currency preference, guest information fields, staff privilege for room operations, guest room policy, and hotel information.

Currency Preference

Currency Unit is required and will be used in all billing and invoicing transactions.

You need to enter currency unit in the **Currency Unit** field.

Refer to the following table to see how the currency unit setting on PBX is presented on the guest bill.

Setting	Effect
	

Guest Information Field

Guest Information Field is used to collect additional information from guests during check-in.

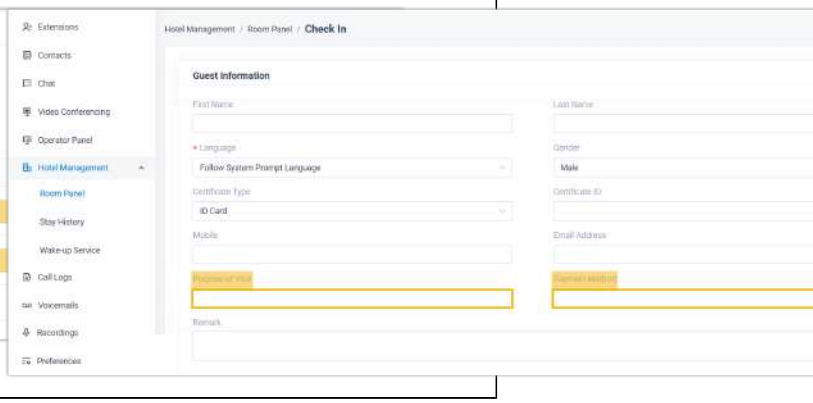
By default, the following basic information can be collected when a guest checks into your hotel:

Category	Item
Guest Information	• First Name • Last Name • Certificate ID • Mobile Number • Email Address
Guest Address	• Zip Code • Street • City • State • Country

If you want to collect more guest information, enable **Custom Guest Information Fields**, then click **Add** to add the desired fields.

> **Note:**
> A maximum of 10 custom fields are supported.

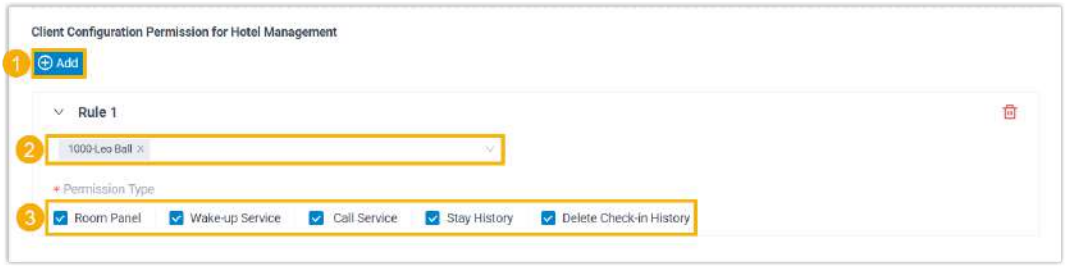
Refer to the following table to see how the guest information field settings are reflected in the check-in form.

Setting	Effect
	

Staff Privilege for Room Operation

Client Configuration Permission for Hotel Management enables you to grant specific room operation privileges to staff members (e.g. front desk). The authorized staff member(s) will be able to perform these operations on their Linkus Desktop/Web Client.

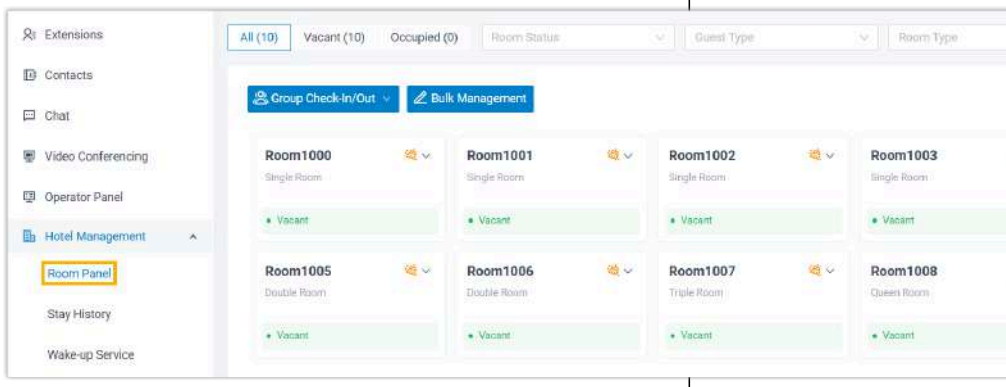
You can click **Add** to add permission rule(s).

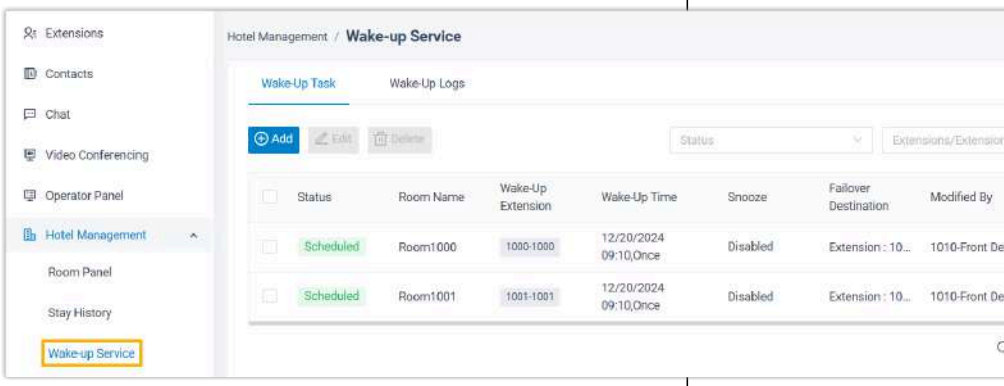
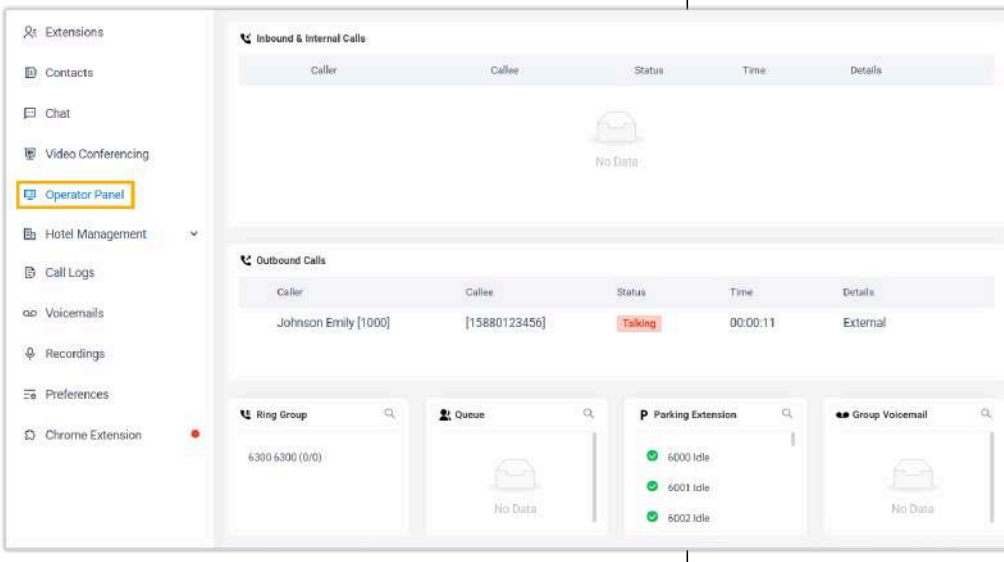


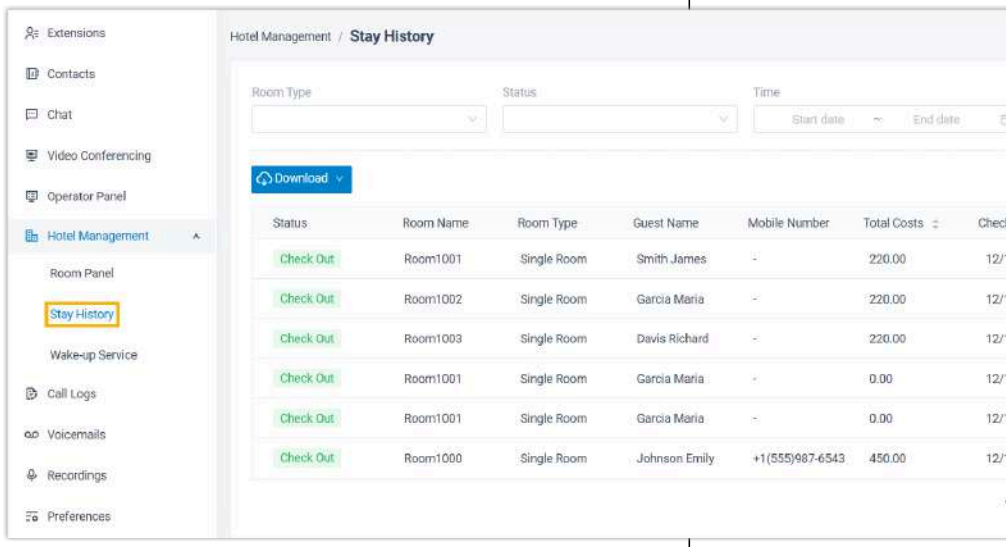
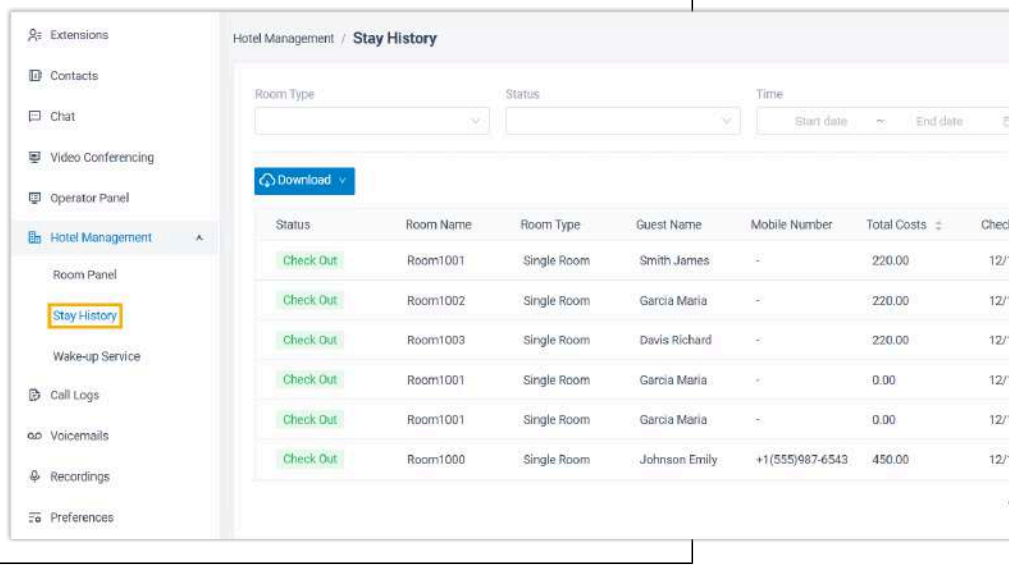
Note:

- A maximum of 10 permission rules are supported.
- This doesn't grant the management permission of hotel service to staff member. To achieve this, you can assign the **Hotel Manager** role to the desired member. For more information, see Grant Hotel Management Permission.

Refer to the following table to see how the authorized staff members can access and perform operations on Linkus Desktop/Web Client based on their assigned privileges.

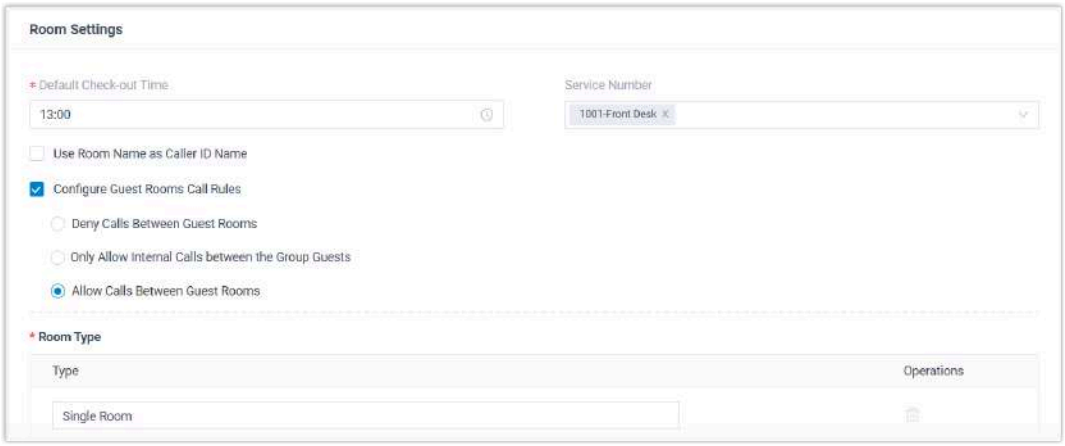
Permission	Description
Room Panel	The authorized staff member can access **Room Panel** on Linkus Desktop/Web Client (Path: **Hotel Management > Room Panel**) to perform operations such as check-in, move rooms, set Do Not Disturb (DND), change room status, add wake-up calls, check out, etc. 
Wake-up Service	The authorized staff member can access **Wake-up Service** (Path: **Hotel Management > Wake-up Service**)

Permission	Description
	on Linkus Desktop/Web Client to perform operations such as schedule wake-up tasks and review the wake-up log. 
Call Service	The authorized staff member can manage guest calls from Operator Panel on Linkus Desktop/Web Client. **Tip:** Refer to Call Management Permission to learn more. 
Stay History	The authorized staff member can access **Stay History** on Linkus Desktop/Web Client (Path: **Hotel Management > Stay History**) to review guest stay history.

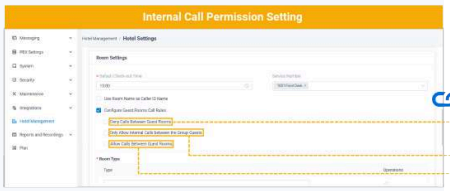
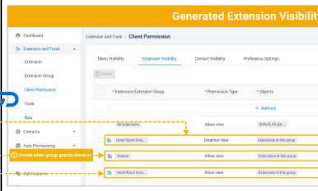
Permission	Description
	
Delete Check-in History	The authorized staff member can access **Stay History** on Linkus Desktop/Web Client (Path: **Hotel Management > Stay History**) to delete guest stay history. 

Guest Room Policy

Guest Room Policy is required, where you need to configure the general settings for guest rooms.



Setting	Description
Default Check-out Time	Set the default check-out time.
Service Number	Service Number is the extension number assigned to hotel services, such as 24-hour front desk, laundry service, restaurant, etc. All guests can call this number from their room phones, regardless of check-in status. Select one or more service numbers from the drop-down list to allow guests to call.
Use Room Name as Caller ID Name	By default, when guests make internal calls from a room phone, the guest name registered at check-in is displayed as the Caller ID name, according to the name display format set in **PBX Settings > Preferences > Basic > Name Display Format**.   To display the room name (as configured in **Hotel Management > Room Management > Room Name**) as the Caller ID name, enable the option **Use Room Name as Caller ID Name**.  

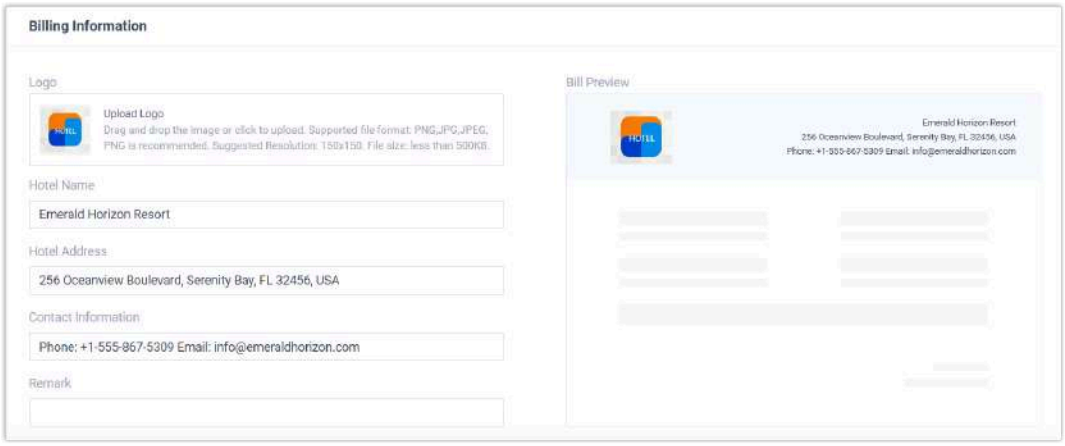
Setting	Description
Configure Guest Rooms Call Rules	By default, guests are NOT allowed to make internal calls between rooms. You can configure internal call permission for guest rooms as needed. **Note:** • For Yeastar PBX, internal call permission is associated with extension visibility. After you configure the internal call permission, PBX will create the corresponding extension visibility rules on **Extension and Trunk > Client Permission > Extension Visibility**.   • If **Organization Management** (Path: **PBX Settings > Preferences**) is enabled on Yeastar PBX, this feature is DISABLED by default. To configure internal call permission, see Enable internal call permission (Department-based structure). • **Deny Calls Between Guest Rooms** • **Only Allow Internal Calls between the Group Guests** • **Allow Calls Between Guest Rooms** **Note:** When internal calls are enabled on room phones, only guests in checked-in rooms can make calls. Otherwise, only the emergency number, service number, and housekeeping feature code can be dialed.

Setting	Description
Room Type	Set room types. **Note:** A maximum of 10 room types are supported.

Hotel Information

Hotel Information will be used in all billing and invoicing transactions.

You can fill in the hotel information in the **Billing Information** section.

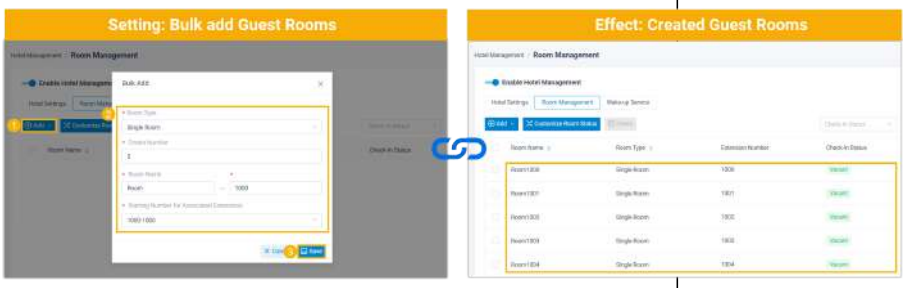


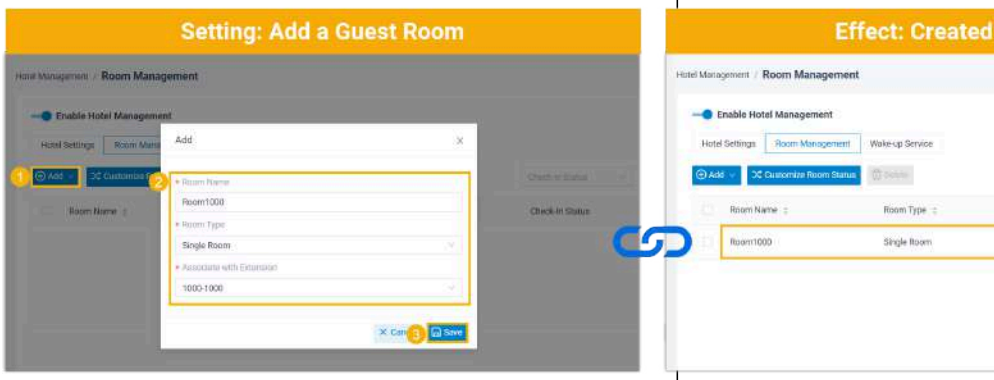
Step 3. Set up guest room

Go to **Room Management** tab to set room status and add guest rooms.

Add Guest Room

Add guest rooms in bulk or one by one as needed.

Scenario	Instruction
Add guest rooms in bulk	 1. Click **Add > Bulk Add**.

Scenario	Instruction
	2. In the pop-up window, configure the following settings: • **Room Type**: Select a room type. • **Create Number**: Set the number of guest rooms that you want to create. **Note:** Enter a value between 1 and 99. • **Room Name**: Set a prefix and a suffix for the room name. ◦ **Prefix**: Any letter or number. ◦ **Suffix**: A number between 0 and 9999. For example, set prefix as "Room" and suffix as "1000", the room name will be Room1000. • **Starting Number for Associated Extensions**: Select an extension from the drop-down list. PBX will automatically assign available extension numbers to the created guest rooms, starting from the number you specify here. 3. Click **Save**.
Add guest rooms one by one	 1. Click **Add > Add**. 2. In the pop-up window, configure the following settings: • **Room Name**: Set the room name. • **Room Type**: Select a room type. • **Associate with Extension**: Select an extension from the drop-down list to associate with the guest room.

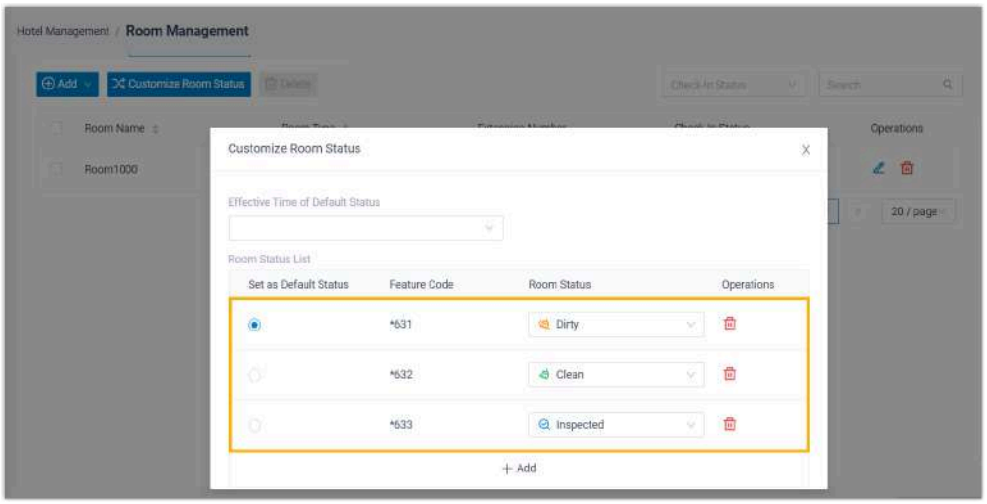
Scenario	Instruction
	3. Click **Save**.

Set Room Status

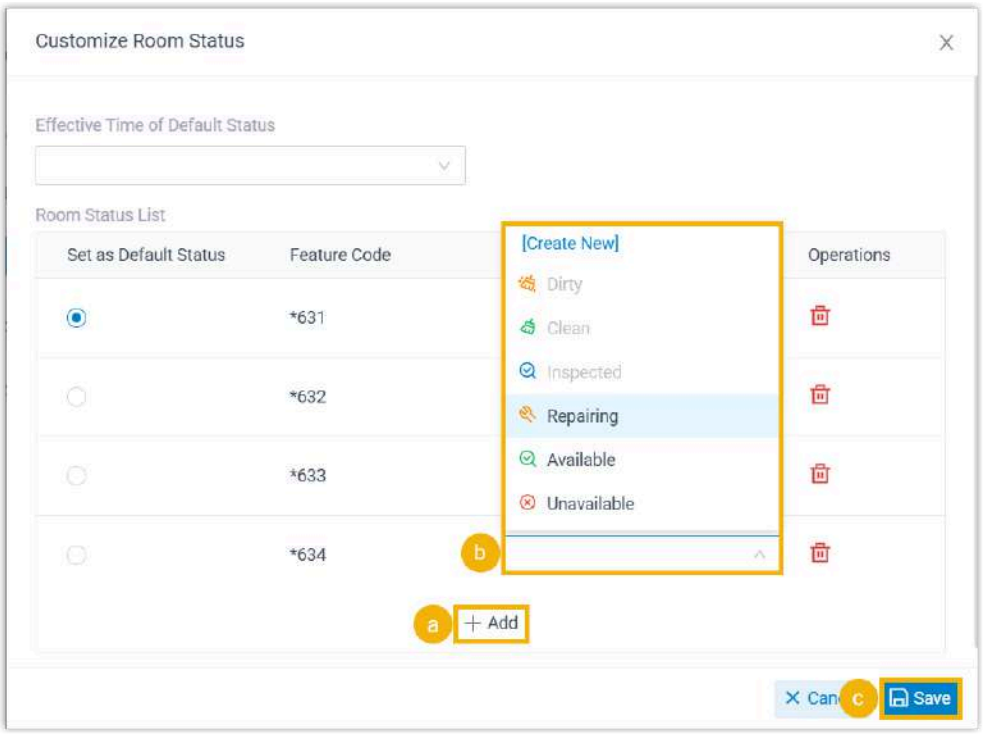
Yeastar provides 6 built-in room status - **Dirty**, **Clean**, **Inspected**, **Repairing**, **Available**, and **Unavailable**, along with feature codes to facilitate housekeeping management. You can also customize desired room status as needed, as shown below.

1. Click **Customize Room Status**.

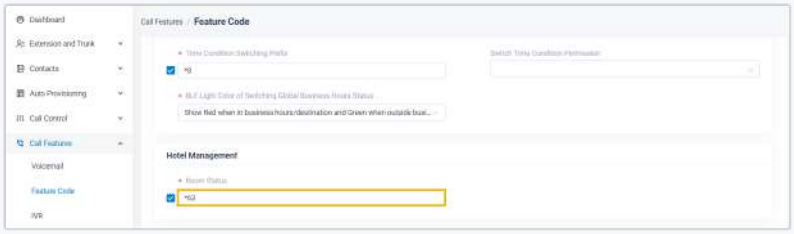
   The default 3 room status rules are displayed on the list.



2. Add room status.



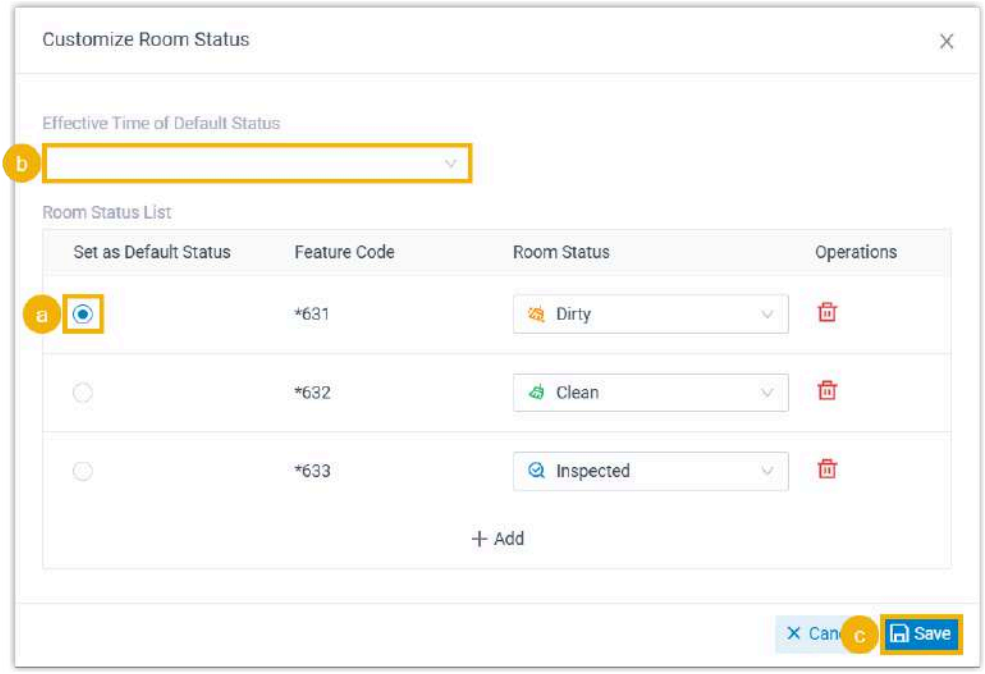
a. Click **Add**.
   A feature code is automatically generated for the room status, allowing housekeepers to dial the code from room phone to change room status.

> **Note:**
> The feature code consists of a default room status code (*63) followed by a sequential number. To use a different room status code, go to **Call Features > Feature Code > Hotel Management > Room Status** to change it.
>
> 

b. In the **Room Status** drop-down list, select an existing status or click **Create New** to create a room status.

> **Note:**
> A maximum of 26 room statuses are supported, including 6 built-in statuses and 20 custom statuses.

3. Set the default room status and specify the scenario for resetting room status to default.



   a. In the **Set as Default Status** column, select the default room status.
   b. **Optional:** In the **Effective Time of Default Status** drop-down list, select another scenario where room status will be reset.
      - **At Check-In**: Reset room status to the default when guests check in.
      - **Automatically Reset Every X Days**: Periodically reset room status to the default.

        If you choose this option, select the interval (in days) from the drop-down list.
   c. Click **Save**.

Step 4. Set up wake-up service

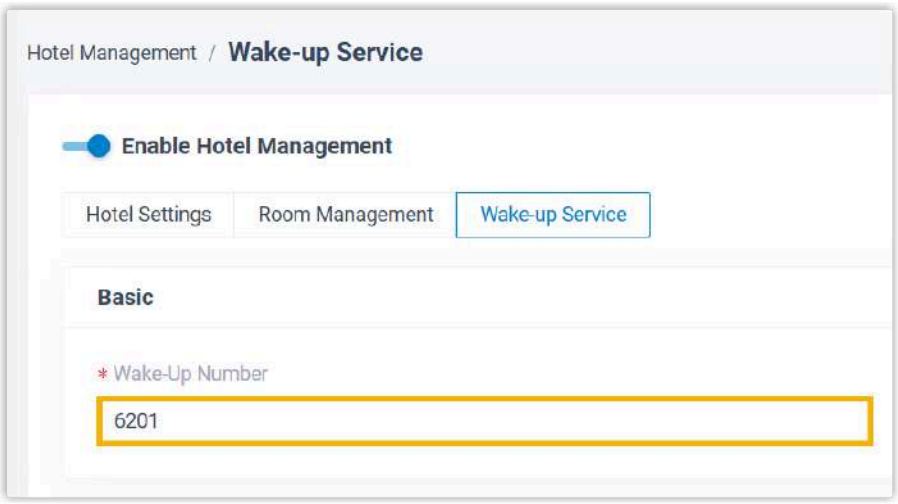
Go to **Wake-up Service** tab to configure wake-up number and wake-up rules.

Wake-up Number

Wake-up Number is an internal number that guests can call to set wake-up calls.

You can use the default wake-up number, or enter a desired number in the **Wake-Up Number** field.

> **Note:**
>
> - You can enter any number, as long as it doesn't conflict with existing numbers in the PBX.
> - Once you save the number, it can NOT be changed.



Wake-Up Rule

Customize the rule for wake-up calls.

Setting	Description
Ring Timeout (s)	Set the time for a wake-up call to ring before it times out (**Unit**: Second). **Valid value**: 5-300
Snooze	Set the number of times to repeat the call if guests don't answer the wake-up call, and the interval between each repeat.
Voice Prompt	Select the voice prompt to be played when guests answer wake-up calls. **Note:** Prompts in the drop-down list are synchronized from **PBX Settings > Voice Prompt > Custom Prompt**.
Failover Destination	Set the failover destination in case guests don't answer the wake-up call. • **Hang Up** • **Extension** • **Ring Group**

Result

- Hotel service is set up on Yeastar P-Series Software Edition.
- An extension group **Hotel Room Group** is created, and all extensions assigned to guest rooms are automatically added to the group for centralized call management.

Call Management

Grant Call Permission to Guest Rooms

By default, guests can call the service number and emergency number, while room-to-room and outbound calls are disabled. This topic describes how to grant internal and external call permission to guest rooms.

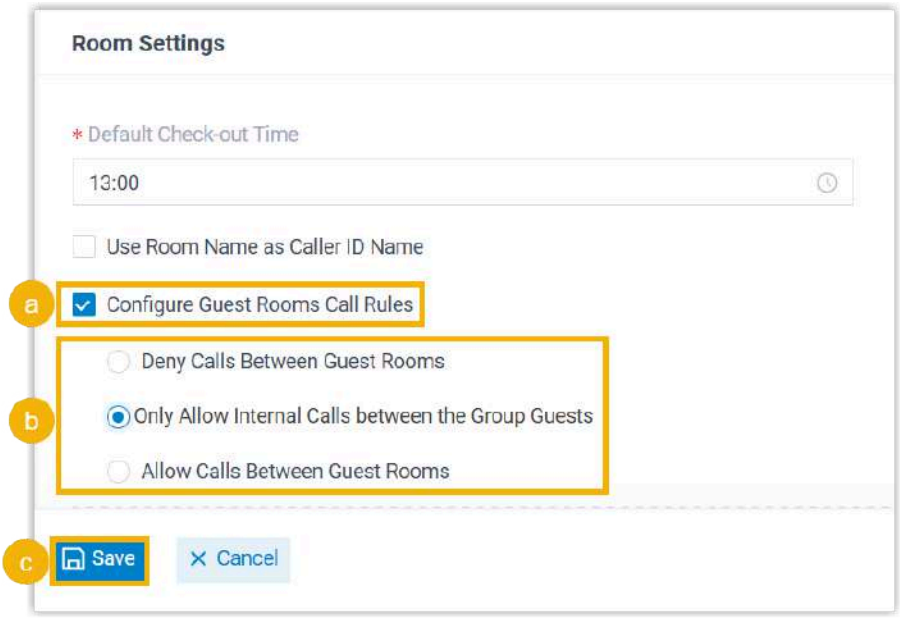
Enable internal calls between guest rooms

For Yeastar PBX, internal call permission is associated with extension visibility rules. To put it simply, guests can make calls between rooms only if their room extensions are allowed to view the called extension. By default, there are no rules to allow room-to-room calls.

To enable internal calls between guest rooms, you can proceed from the **Extension Visibility** or the **Hotel Management** configuration page. The available way depends on how your company's structure is organized - whether it is group-based or department-based.

Enable internal call permission (Group-based structure)

1. Log in to PBX web portal, go to **Hotel Management**.
2. Under **Hotel Settings** tab, scroll down to the **Room Settings** tab.
3. Set up the call rule.



a. Select the checkbox of **Configure Guest Rooms Call Rules**.
b. Select the desired call rule.
c. Click **Save**.

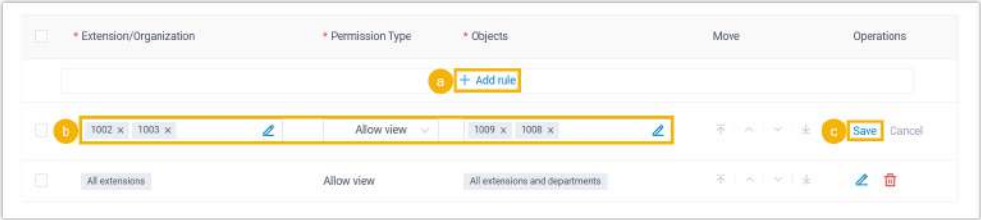
The corresponding visibility rule will be created in **Extension and Trunk > Client Permission > Extension Visibility**.

Internal Call Permission Setting	Generated Extension Visibility Rule
	
Deny Calls Between Guest Rooms	**Hotel Room Group Disallow view** Extensions in this group
Only Allow Internal Calls between the Group Guests **Note:** If you select this option, whenever a tour group checks	***{tour_group}*** **Allow view** Extensions in this group

Internal Call Permission Setting	Generated Extension Visibility Rule
in to your hotel, the system will create a temporary extension group, containing all extensions associated with the rooms assigned to the tour guests. This group will be automatically deleted when the tour group checks out.	
Allow Calls Between Guest Rooms	**Hotel Room Group Allow view** Extensions in this group

Enable internal call permission (Department-based structure)

1. Log in to PBX web portal, go to **Extension and Trunk > Client Permission > Extension Visibility**.
2. Add a visibility rule.



   a. Click **Add rule**.
   b. Set up the visibility rule.
      - **Extension/Organization**: Select the member(s) to which you want to grant the viewing permission.
      - **Permission Type**: Select **Allow view**.
      - **Objects**: Select the member extension(s) that are allowed to be viewed.
   c. Click **Save**.

   The selected member(s) can make calls to the member extensions.

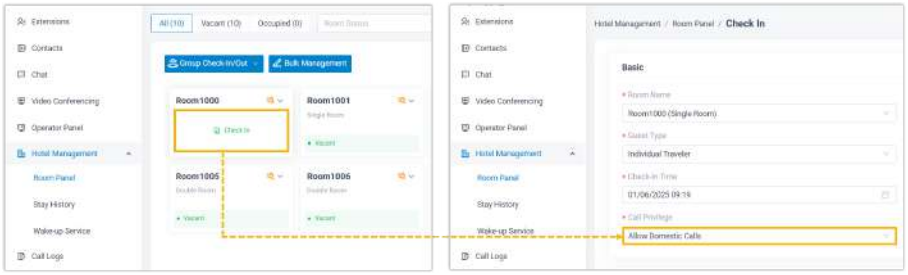
Enable outbound calls from guest rooms

By default, outbound calls from room phones are blocked. As a best practice, you should avoid enabling outbound calling for all guest rooms. Instead, grant access only to the guests who request it.

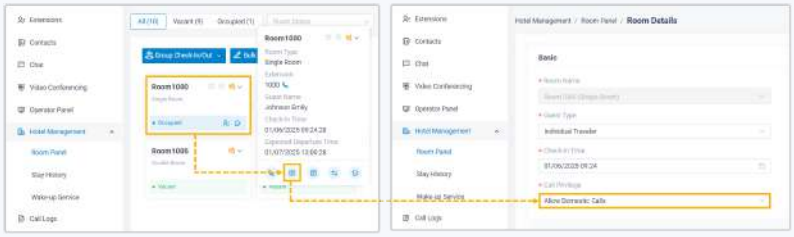
To accommodate guest requests for outbound calls, you can configure the outbound calling settings in advance and grant permission to guest(s) during check-in.

Enable domestic outbound calling

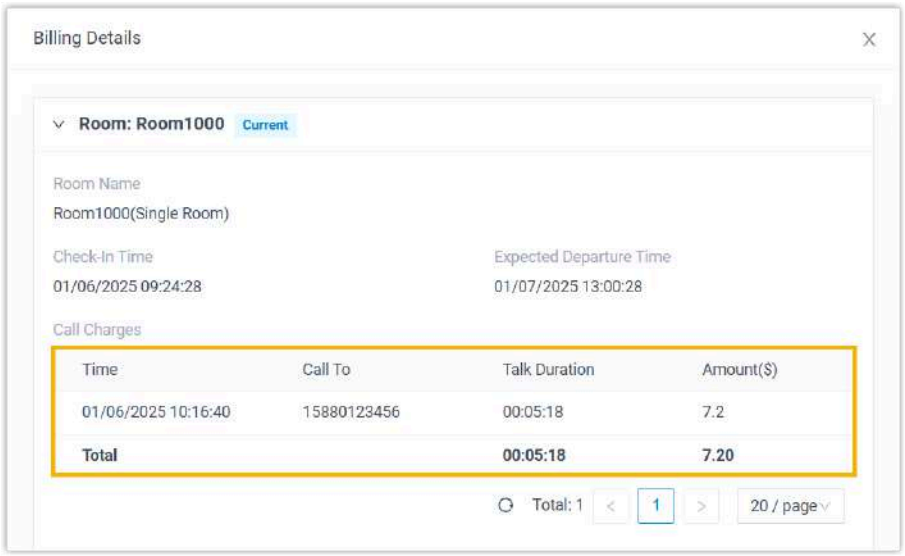
1. Configure domestic outbound calling settings.
    a. Set up a trunk for outbound calls.
    b. Create an outbound route to route calls to external numbers.
    c. Add a call rate rule to bill guest calls.
2. Grant domestic outbound calling permission to guest(s) during check-in.
    a. On the check-in page, select **Allow Domestic Calls** from the drop-down list of **Call Privilege**.



    b. Click **Save**.

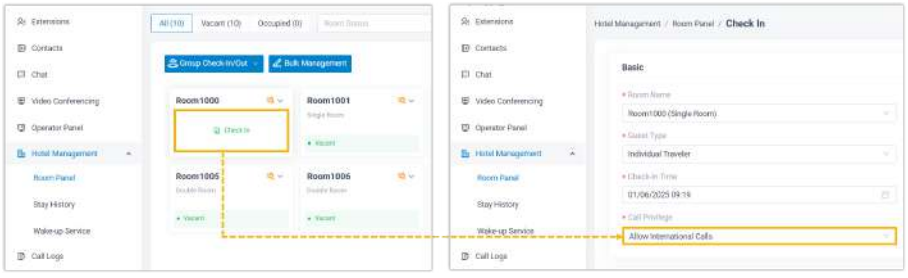
> **Note:**
> If guest(s) request domestic outbound calling permission after check-in, you can grant the permission from room page, as shown below.
>
> 

The guest can make domestic outbound calls from room phone. After a call ends, the PBX system will calculate the charge based on the applicable rate, and post the charge to the guest's bill.



Enable international outbound calling

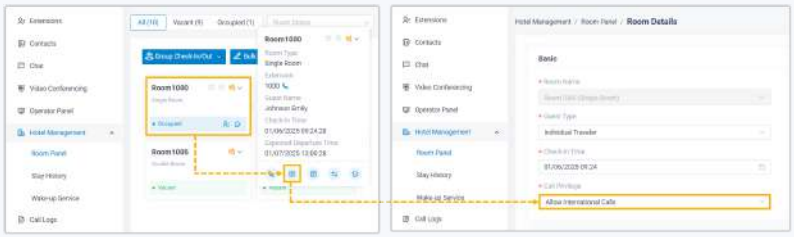
1. Configure international outbound calling settings.
    a. Set up a trunk for outbound calls.
    b. Set up international dialing code to help the system identify international calls, and restrict international calls only to the trusted countries and regions.
    c. Create an outbound route to route calls to external numbers.
    d. Add a call rate rule to bill guest calls.
2. Grant international outbound calling permission to guest(s) during check-in.
    a. On the check-in page, select **Allow International Calls** from the drop-down list of **Call Privilege**.



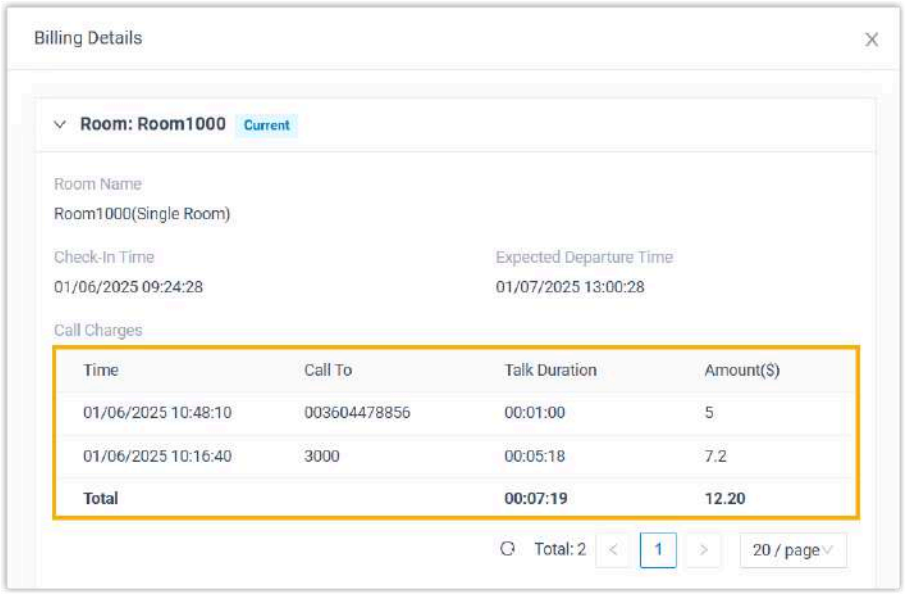
    b. Click **Save**.

> **Note:**

If guest(s) request international outbound calling permission after check-in, you can grant the permission from room page, as shown below.



The guest can make both international and domestic outbound calls from room phone. After a call ends, the PBX system will calculate the charge based on the applicable rate, and post the charge to the guest's bill.



Set up Call Rate for Guest Call Billing

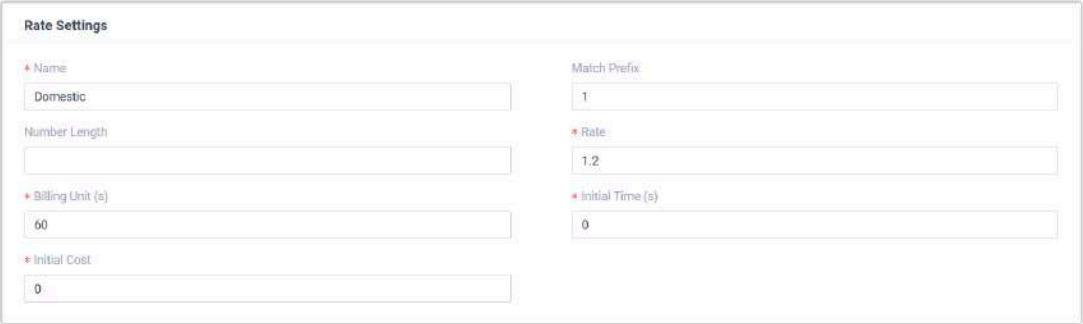
Yeastar P-Series Software Edition incorporates a built-in call accounting feature that automates billing for guest outbound calls. You can create one or more call rate rules to define the rate deck. After a guest completes an outbound call, the PBX system calculates the charge based on the applicable rate, and posts it to the guest's bill. This topic describes how to add a call rate rule for outbound calls.

Note:

Yeastar Call Accounting allows you to set call rates based on dialing prefix and number length, which are closely tied to the outbound route settings, as the applicable rate is determined by the number sent by PBX, instead of the number dialed by guest. Therefore, ensure that your call rate settings align with the outbound route configuration.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports > Rate**.
2. Add a call rate rule.
    a. Click **Add**.
    b. Fill in the following information to set up the rule.



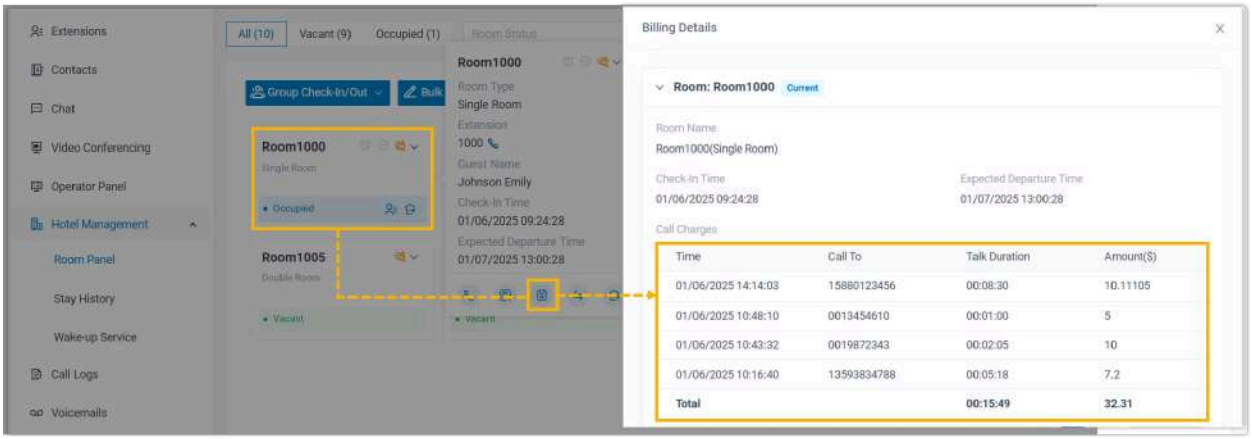
Item	Description
Name	Enter a name to help you identify the call rate rule.
Match Prefix	Optional. Define the dialing prefix to match the call rate rule. **Note:** This rate rule applies only to outbound calls that match the dialing prefix and is based on the number sent by the PBX, rather than the number dialed by guest.
Number Length	Optional. Define the dialing length to match the call rate rule. **Note:** This rate rule applies only to outbound calls with a number length equal to or shorter than the specified value and is based on the number sent by the PBX, rather than the number dialed by guest.
Rate	Enter the call rate.

Item	Description
	After the initial time, each billing unit will be charged with this rate. **Note:** Up to 5 decimal places are supported.
Billing Unit (s)	Define the time increment (in seconds) that will be used to calculate the charge 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 charge for a call will increase by 0.5 every 60 seconds.
Initial Time (s)	Define the initial period of time (in seconds) during which a 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.

c. Click **Save**.

Result

After a guest completes an outbound call, the PBX system calculates the charge based on the applicable rate, and posts the charge to the guest's bill, as shown below.



Note:

PBX bills each outbound call with up to 5 decimal places of precision, and rounds the subtotal to 2 decimal places.

Schedule Call Reports to Track Call Activity

A list of call reports is available to provide actionable insights into guest calls with detailed analysis. To make call tracking and analysis easier, you can schedule call reports to be generated on a recurring basis and automatically sent to specific email address(es). This topic describes how to schedule call reports to be sent to a specific address.

The following is a list of call reports related to hotel call activities. Refer to the table below for details on the information each report provides.

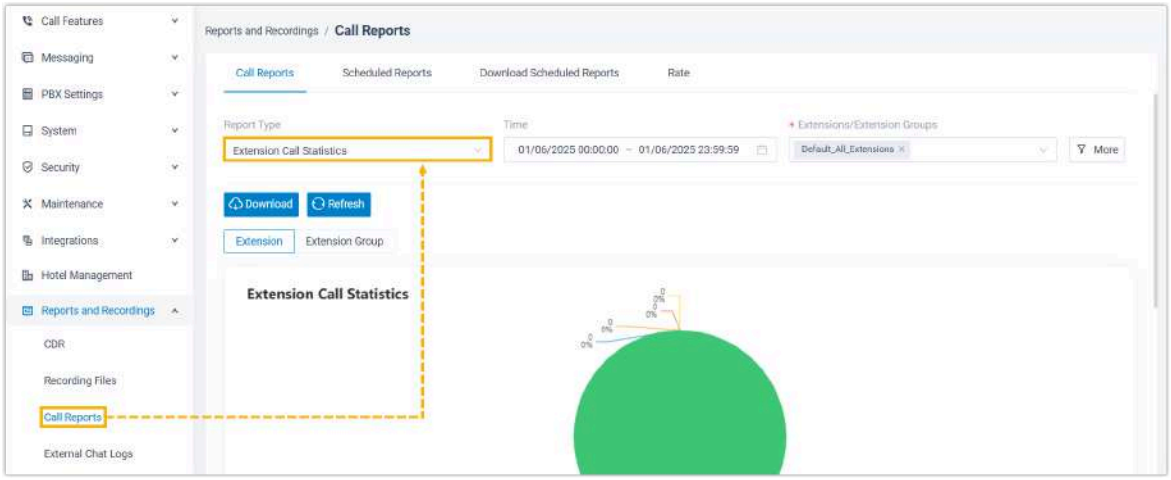
Note:
For more call reports, see Call Reports Overview.

Report	Description
Extension Call Statistics	Provide a quick overview of the number of calls that have been made and received on room extensions.
Extension Call Activity	Provide granular insights into the hourly, daily, and monthly breakdown of the number of calls that have been made and received on room extensions.
PBX Call Activity	Provide granular insights into the hourly, daily, and monthly breakdown of total external calls on specific trunks and internal calls.
Extension Call Accounting	Provide a quick overview of the bills for outbound calls made from room extensions over specific trunks.
Extension Call Accounting Details	Provide granular insights into the bills for each outbound call made from room extensions over specific trunks.

You can explore the above call reports in two ways:

- Access the call reports directly from PBX web portal.

  To achieve this, proceed as below.

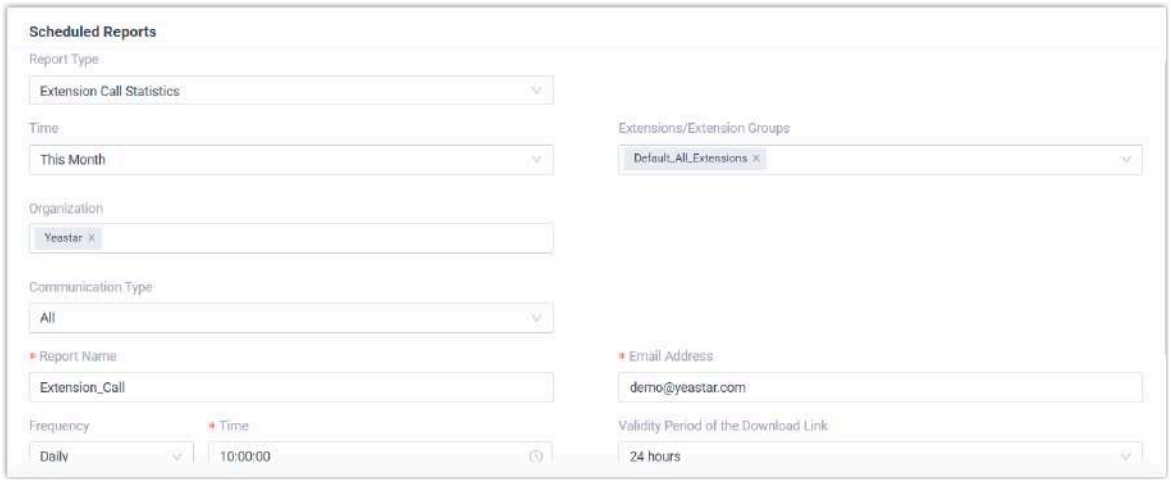


- Schedule call reports to be automatically sent to the specified email address(s) on a recurring basis.

  To achieve this, refer to the instructions below.

Procedure

1. Log in to PBX web portal, go to **Reports and Recordings > Call Reports > Scheduled Reports**.
2. Click **Add Report**.
3. Complete the following settings to schedule a report.



Setting	Description
Report Type	Select a call report.
Time	Select a time frame that the report will cover.

Setting	Description
Extensions/Extension Groups	Select one or more objects of call data you want to query.
Report Name	Enter a name to help you identify the report.
Email Address	Enter email address(es) to receive the report. **Note:** You can specify up to 10 email addresses. For multiple email addresses, separate them with semicolon `;`.
Frequency	Set how often to send the report.
Validity Period of the Download Link	Set the validity period of the download link for the scheduled report. After the link expires, the email recipient(s) can NOT download the report via the link.
File Format	Set in which format the report can be downloaded. • **CSV** • **XLS** • **PDF**
Send Attachment	If enabled, the call report will also be sent as an attached file. **Note:** This option is available only when the file format is set to **CSV** or **XLS**.

4. Click **Save**.

Result

PBX system will send the report to the specified email recipient(s) at the scheduled time.

User Management

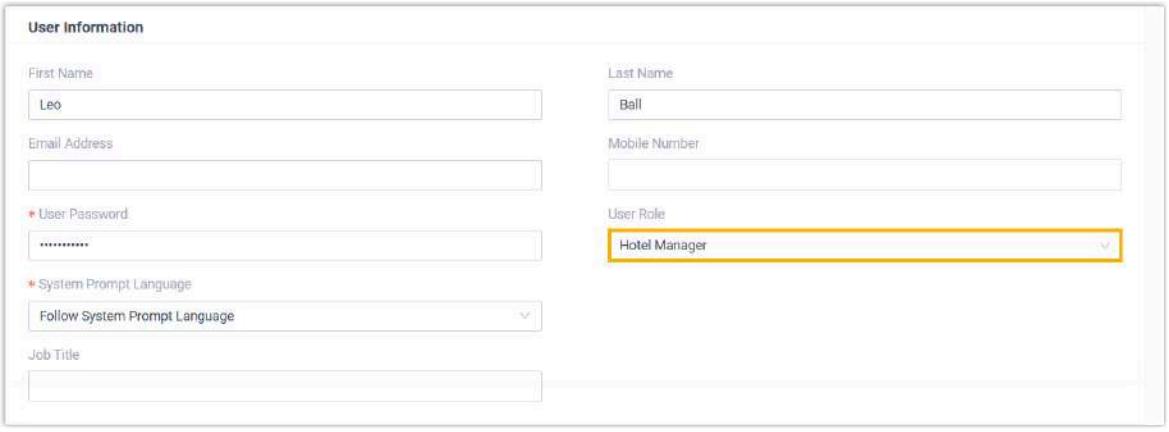
Grant Hotel Management Permission

Grant hotel management permission to specific hotel staff(s), allowing them to access the hotel service configuration page (Path: **Hotel Management**) for co-management.

Yeastar P-Series Software Edition has a built-in role **Hotel Manager** with exclusive access to manage the hotel service. To enable colleagues to co-manage the hotel service, you can assign the role to the desired extension user(s).

Assign the Hotel Manager role to a single user

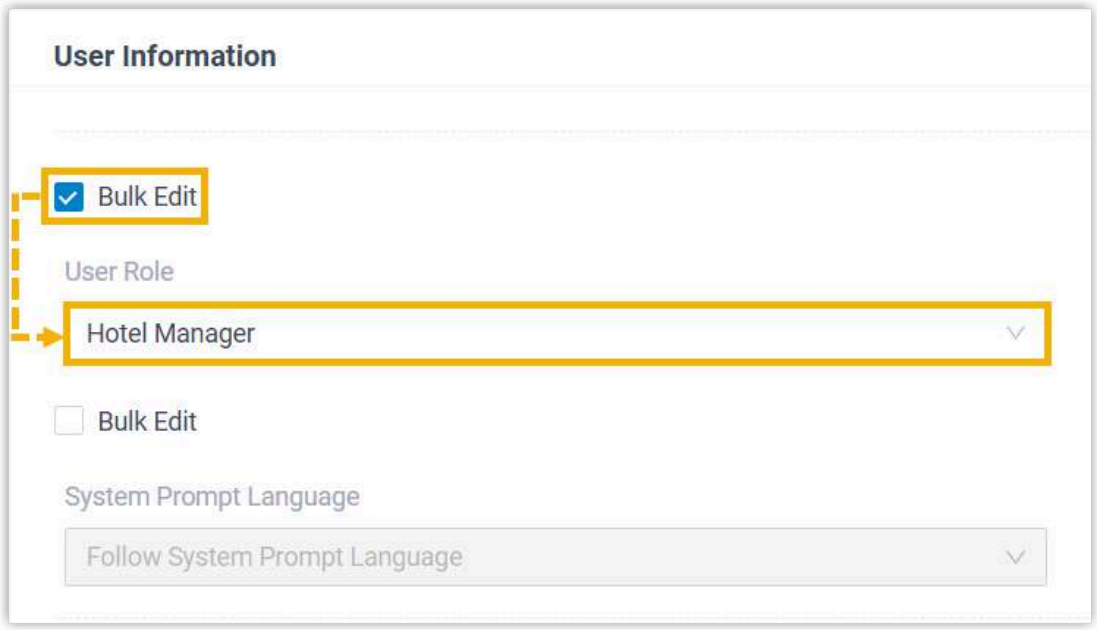
1. Log in to PBX administrator portal, go to **Extension and Trunk > Extension**.
2. Click beside a desired extension.
3. In the **User Information** section, select **Hotel Manager** from the **User Role** drop-down list.



4. Click **Save** and **Apply**.

Assign the Hotel Manager role to multiple users

1. Log in to PBX administrator portal, go to **Extension and Trunk > Extension**.
2. Select the checkboxes of the desired extensions, then click **Edit**.
3. In the **User Information** section, select the checkbox of **Bulk Edit**, then select **Hotel Manager** from the drop-down list.



4. Click **Save** and **Apply**.

Grant Call Management Permission

Grant call management permission to specific hotel staff(s), allowing them to manage guest calls from Linkus Desktop/Web Client.

Background information

Yeastar P-Series Software Edition implements group-based control over users' call management permissions. After you enable hotel management on PBX, an extension group **Hotel Room Group** is automatically created, and all extensions assigned to guest rooms will be added to the group.

This extension group has 3 built-in user types, each with different default permissions:

Note:

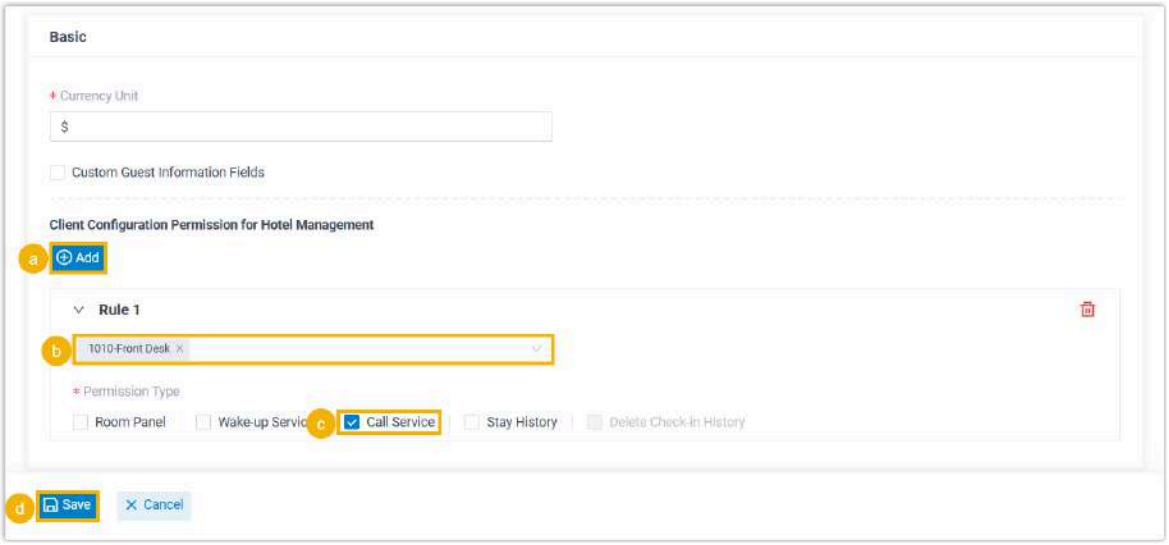
> You can change the default permissions as needed. For more information, see View or Change Permissions for Group Members.

- **Manager**: Allow to access **Extensions** page and **Operator Panel** on Linkus Desktop/Web Client to perform the following operations on calls:
  - **Extensions** page: Redirect, transfer, park, or retrieve internal calls
  - **Operator Panel**: Redirect, transfer, park, or retrieve calls; drag and drop calls to another destination within your organization; route calls directly from IVR regardless of the IVR menu; switch extension presence
- **User**: No access to manage calls.
- **Custom**: Customizable permissions to tailor your business needs.

By default, all room extensions are assigned the **User** user type, and no one can manage guest calls. You can designate specific staff members (e.g. front desk) as the **Manager** by granting them the call service permission , who will then be able to manage guest calls from Linkus Desktop/Web Client.

Procedure

1. Log in to PBX web portal, go to **Hotel Management**.
2. Under **Hotel Settings** tab, add a permission rule.

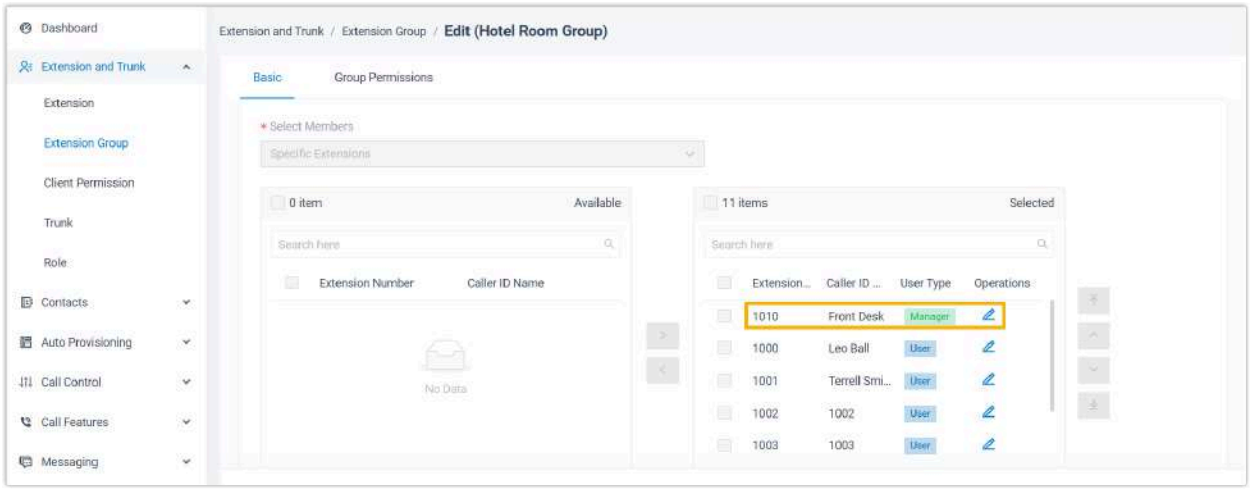


   a. In the **Client Configuration Permission for Hotel Management** section, click **Add**.

b. In the **Extension** drop-down list, select the extension(s) to which you want to grant call service permission.
c. In the **Permission Type** section, select the checkbox of **Call Service**.
d. Click **Save**.

Result

The selected extension(s) become the manager of the hotel extension group and can manage calls on Linkus Desktop/Web Client.



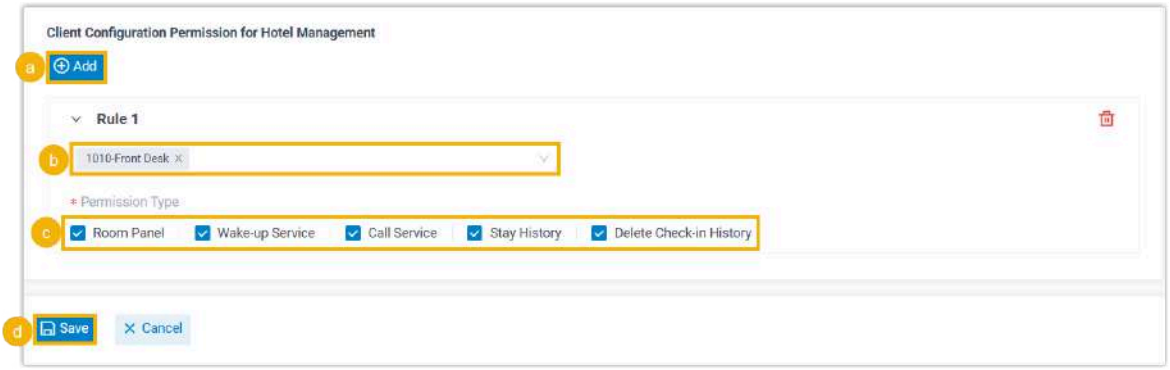
> **Note:**
> For more information about how to manage calls on Linkus Desktop/Web Client, see Manage Guest Calls.

Grant Room Management Permission

Grant room management permission to front desk(s), allowing them to handle guest check-ins and check-outs, room assignments, wake-up calls and more, directly from Linkus Desktop/Web Client.

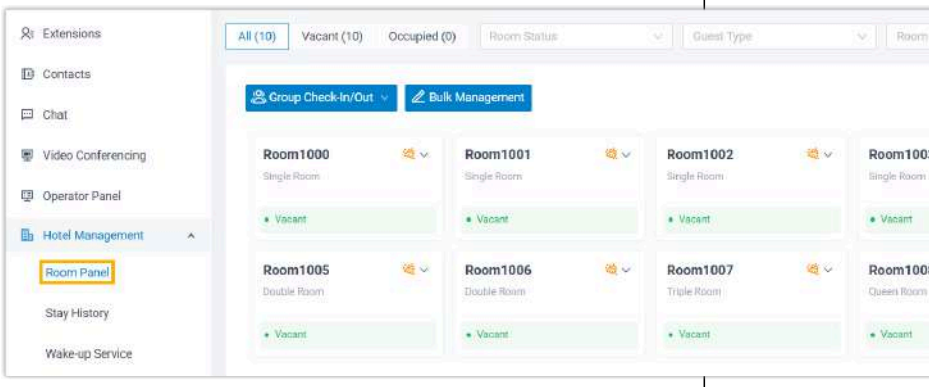
Procedure

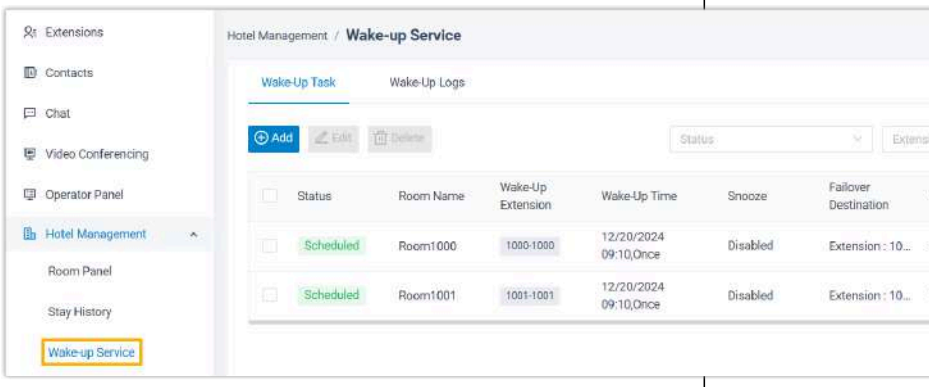
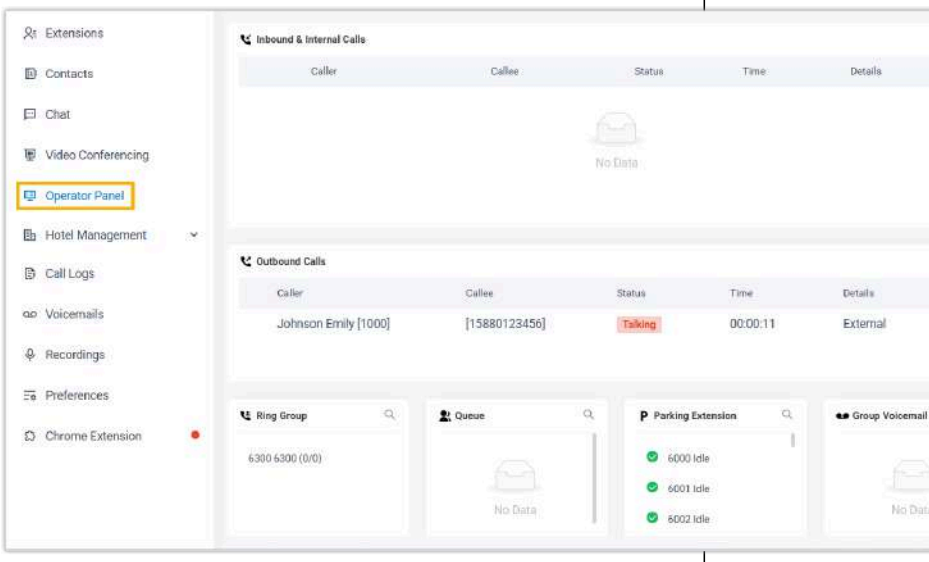
1. Log in to PBX web portal, go to **Hotel Management**.
2. Under **Hotel Settings** tab, add a permission rule.

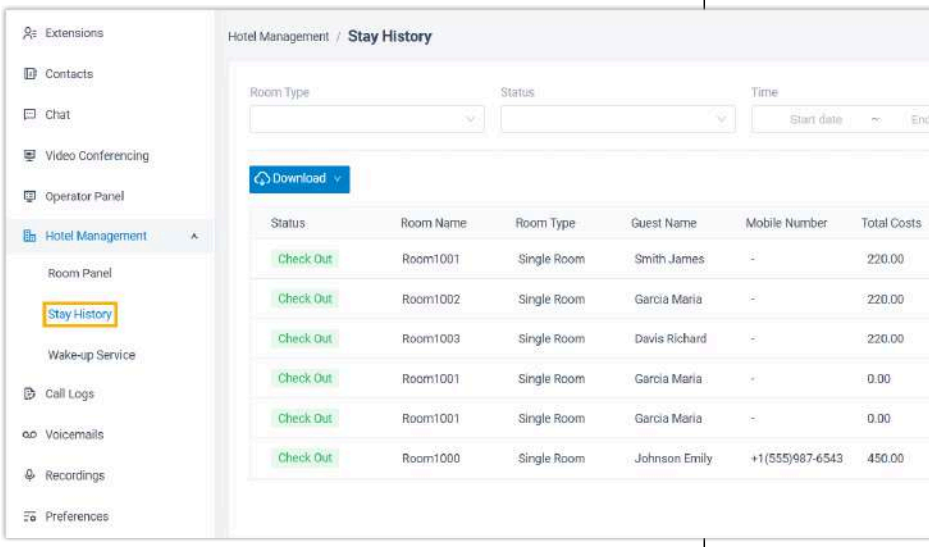
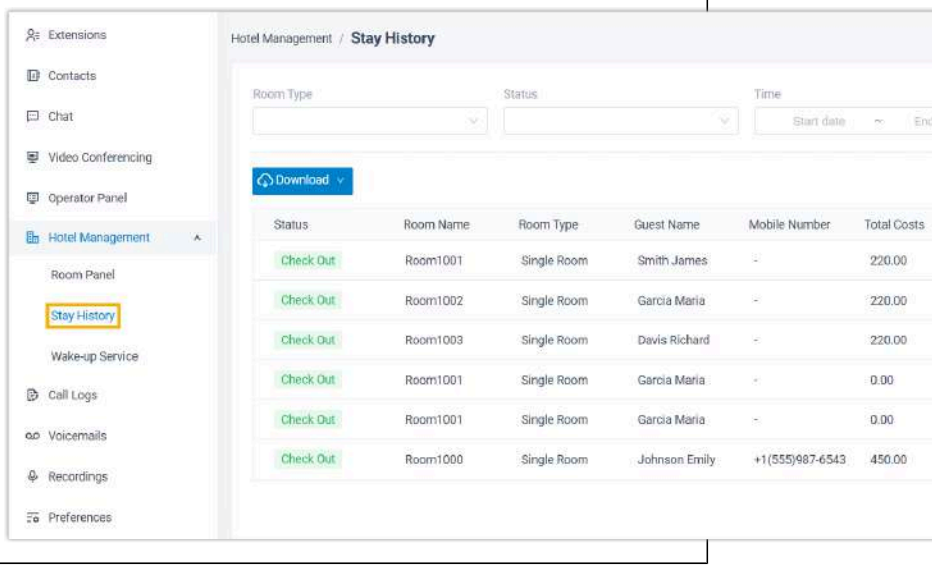


a. In the **Client Configuration Permission for Hotel Management** section, click **Add**.
b. In the **Extension** drop-down list, select the extension(s) to which you want to grant permission.
c. In the **Permission Type** section, select permissions.

   Refer to the following table to see how the authorized extension(s) can access and perform operations on Linkus Desktop/Web Client based on the corresponding privilege.

Permission	Description
Room Panel	The authorized staff member can access **Room Panel** on Linkus Desktop/Web Client (Path: **Hotel Management > Room Panel**) to perform operations such as check-in, move rooms, set Do Not Disturb (DND), change room status, add wake-up calls, check out, etc. 
Wake-up Service	The authorized staff member can access **Wake-up Service** (Path: **Hotel Management > Wake-up Service**) on Linkus Desktop/Web Client to perform operations such as schedule wake-up tasks and review the wake-up log.

Permission	Description
	
Call Service	The authorized staff member can manage guest calls from Operator Panel on Linkus Desktop/Web Client. **Tip:** Refer to Call Management Permission to learn more. 
Stay History	The authorized staff member can access **Stay History** on Linkus Desktop/Web Client (Path: **Hotel Management > Stay History**) to review guest stay history.

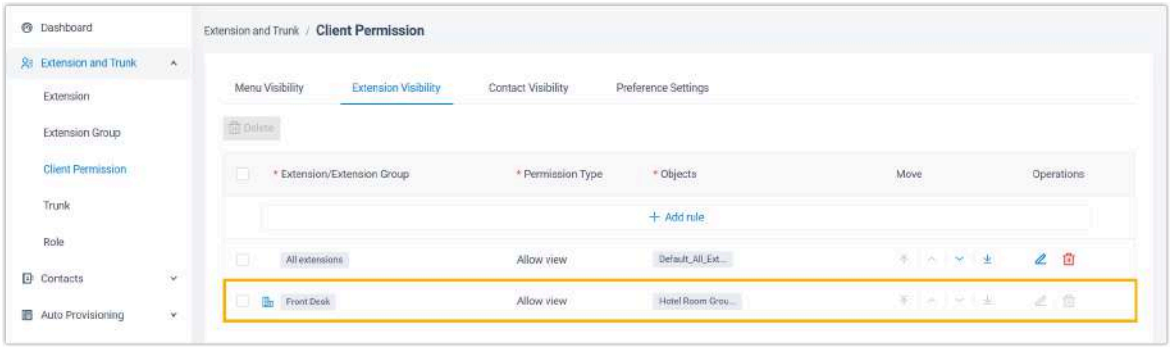
Permission	Description
	
Delete Check-in History	The authorized staff member can access **Stay History** on Linkus Desktop/Web Client (Path: **Hotel Management > Stay History**) to delete guest stay history. 

d. Click **Save**.

Result

- The selected extension(s) can access and perform operations on Linkus Desktop/Web Client based on their assigned privileges.

- If you grant any of the **Room Panel**, **Wake-up Service**, or **Call Service** permissions to extension(s), an extension visibility rule will be created on the PBX to allow the selected extension(s) to make calls to the guest rooms.



Front Desk

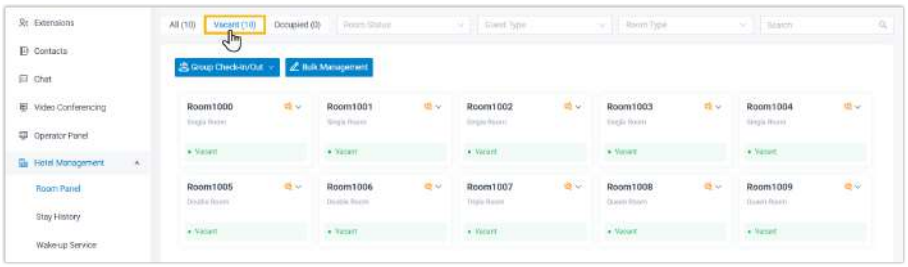
Check in

When guests arrive at the hotel, the front desk can complete the check-in process for them on Linkus Desktop/Web Client.

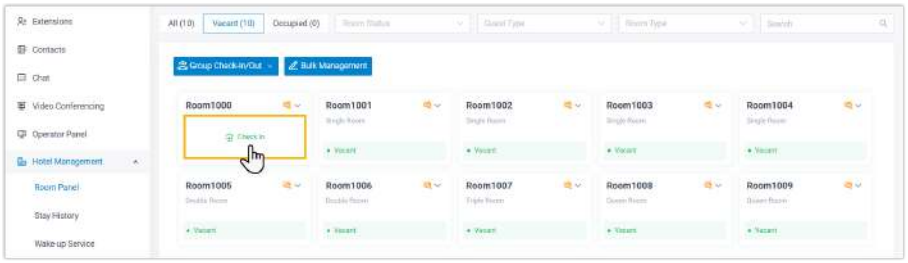
Individual guest check-in

Procedure

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. Filter vacant rooms and find a suitable one.
   a. Click **Vacant** tab to filter available guest rooms.

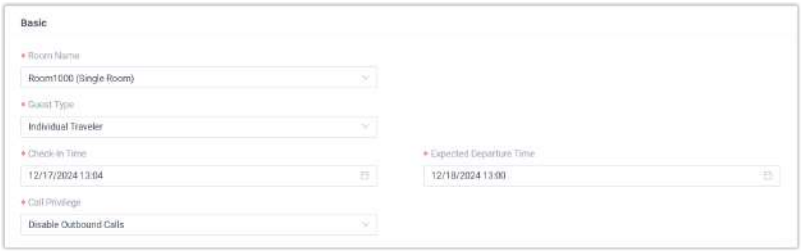


   b. Hover your mouse over a guest room, then click **Check In**.



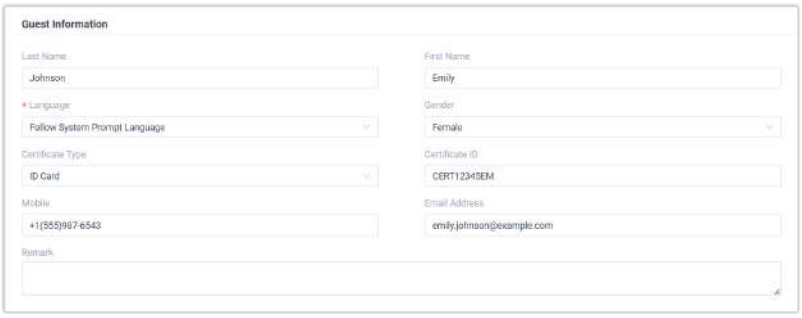
3. Fill in the following information for guest accommodation.

   Basic



Setting	Description
Room Name	This field is automatically filled in with the guest room that you have selected.
Guest Type	Select **Individual Traveler**.
Check-In Time	Keep the current time as check-in time, or change it as needed.
Expected Departure Time	Keep the default check-out time, or change it as needed.
Call Privilege	Set whether the guest can make outbound calls from the room phone. • **Disable Outbound Calls** (default value) • **Allow Domestic Calls** • **Allow International Calls** **Note:** • If you allow the guest to make outbound calls, ensure that you have configured the proper trunk and outbound route. • Outbound call permission is assigned to guest rather than guest room. This means that each time a guest checks out or moves room, PBX will reset the guest room's outbound call permission to **Disable Outbound Calls**.

Guest Information



> **Note:**
> **Language** determines the language in which system prompts (e.g. wake-up call, voicemail, or IVR) will be played to the guest.

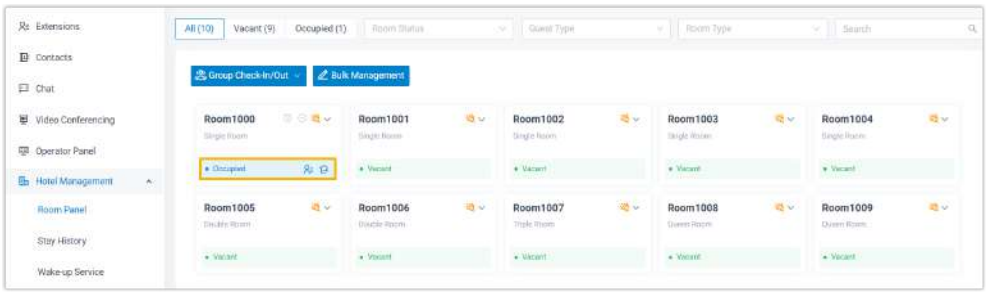
Guest Address

4. Click **Save**.

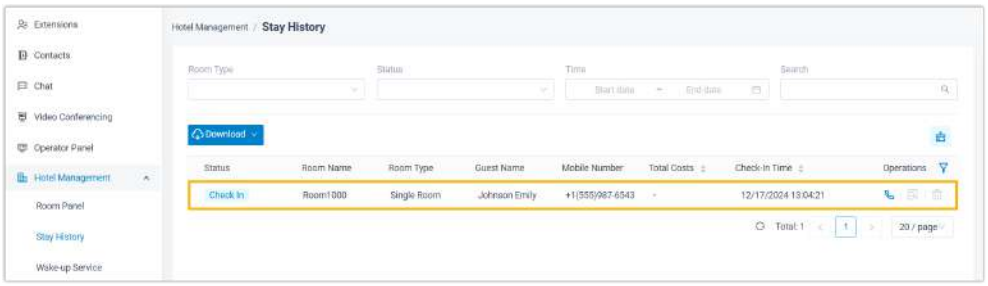
Result

You have checked the guest into the guest room, and the followings are achieved:

- The room status is changed to **Occupied**.



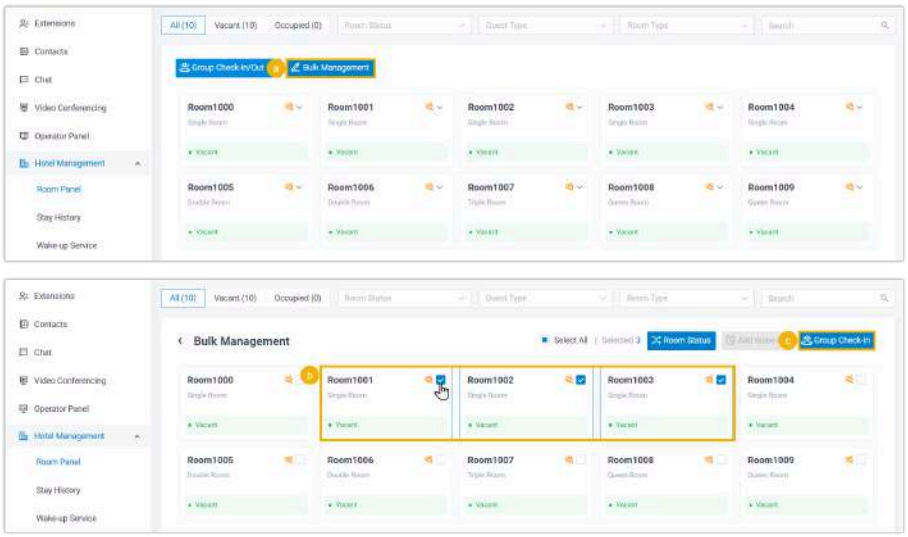
- A history of the stay is created for tracking purposes.



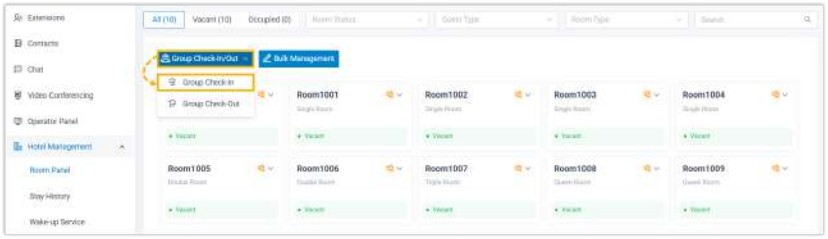
Tour group check-in

Procedure

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. Go to the group check-in page.
   - To pre-select guest rooms, do as follows:

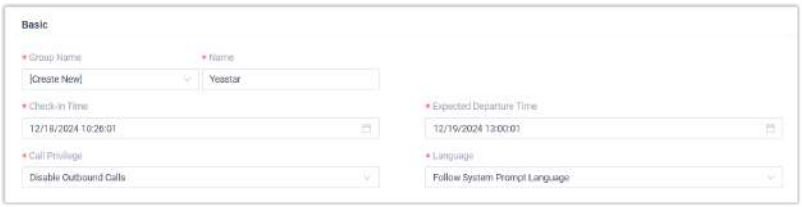


     a. At the top-left corner, click **Bulk Management**.
     b. Select the checkboxes of the desired guest rooms.
     c. At the top-right corner, click **Group Check-In**.
   - To select guest rooms during check-in, do as follows:
     a. At the top-left corner, click **Group Check-In/Out**, then select **Group Check-In**.



3. Fill in the following information for guest accommodation.

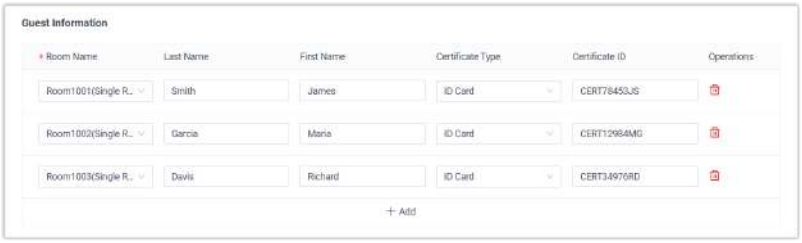
Basic



Setting	Description
Group Name	Click **Create New** to create a group.
Check-In Time	Keep the current time as check-in time, or change it as needed.
Expected Departure Time	Keep the default check-out time, or change it as needed.
Call Privilege	Set whether the tour group can make outbound calls from the room phones. • **Disable Outbound Calls** (default value) • **Allow Domestic Calls** • **Allow International Calls** **Note:** • If you allow the tour group to make outbound calls, ensure that you have configured the proper trunk and outbound route. • Outbound call permission is assigned to guest rather than guest room. This means that each time a guest checks out or moves

Setting	Description
	room, PBX will reset the guest room's outbound call permission to **Disable Outbound Calls**.
Language	Select the language in which system prompts (e.g. wake-up call, voicemail, or IVR) will be played to the group guests.

Guest Information



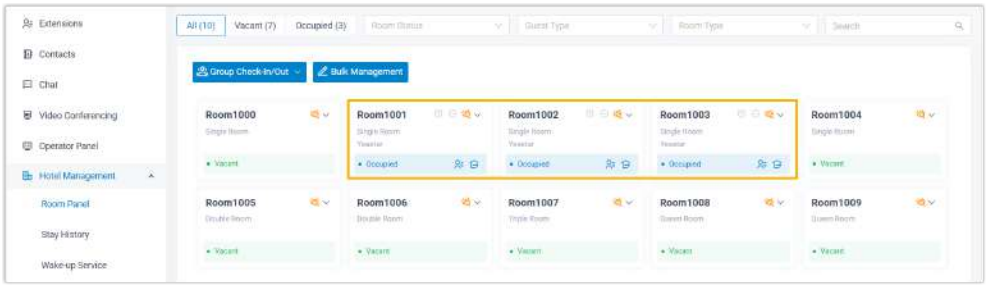
> **Note:**
> A maximum of 64 guests are supported to check in at the same time.

4. Click **Save**.

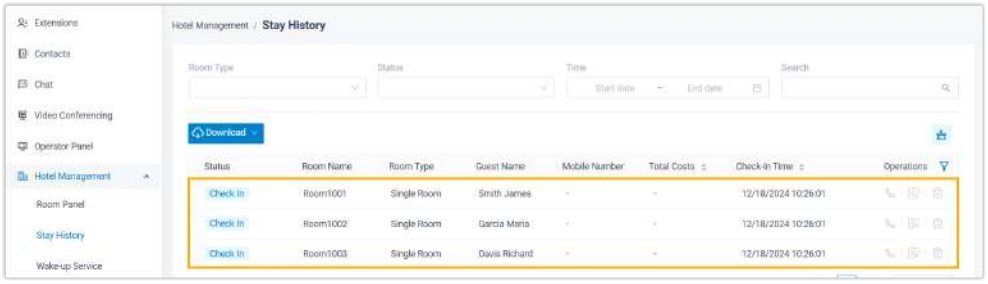
Result

You have checked the tour group into the guest rooms, and the followings are achieved:

- The room status is changed to **Occupied**.



- Multiple histories of the stay are created for tracking purposes.



- A temporary extension group is automatically created, and all extensions associated with the guest rooms assigned to the tour group are added to it for centralized call permission assignment.

Move Rooms

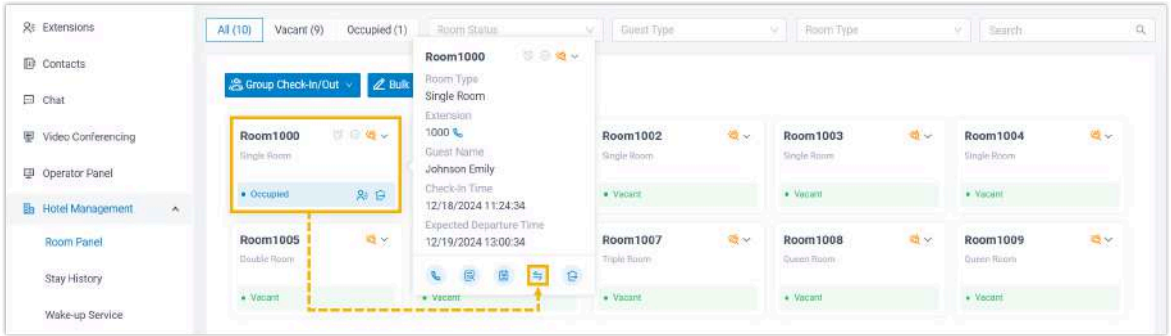
When guests request to move rooms, the front desk can handle it with just a few clicks.

Restrictions

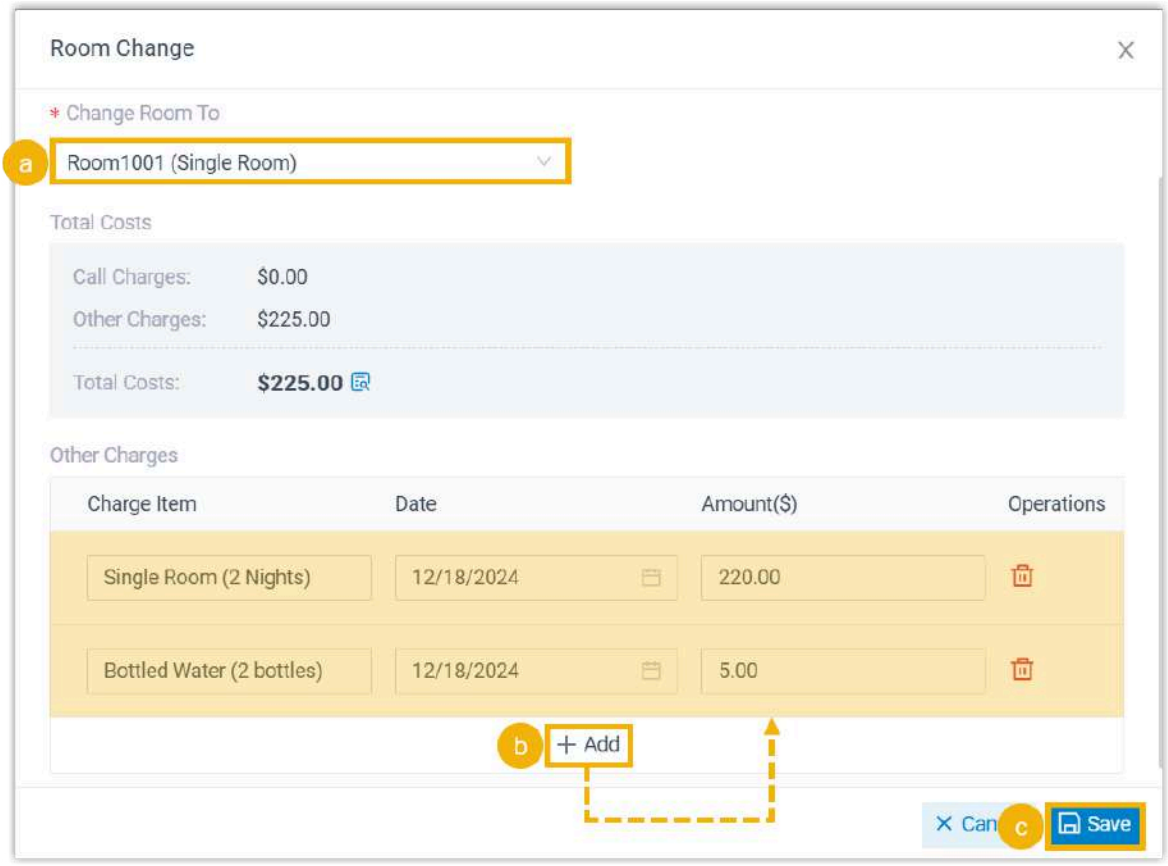
A guest can move to a maximum of 10 different rooms.

Procedure

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. Click the room where the guest has checked in, then click ⇋.



3. In the pop-up window, perform the following operations to move the guest to a new room.



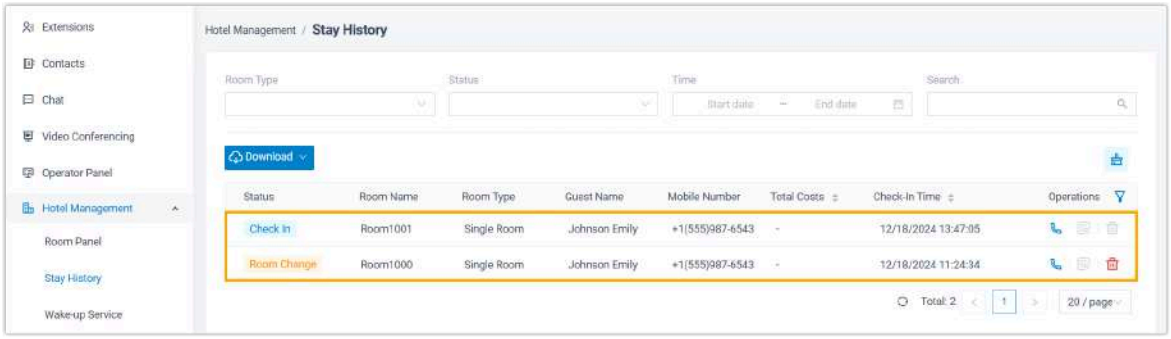
   a. In the **Change Room To** drop-down list, select a new room.
   b. In the **Other Charges** section, click **Add** to add charge items for the current room.

> **Note:**
> The charges will be transferred to the new room.

   c. Click **Save**.

Result

- The guest is moved to the new room.
- The history of the previous stay is marked as **Room Change**, and a new history of the current stay is created and marked as **Check In**.

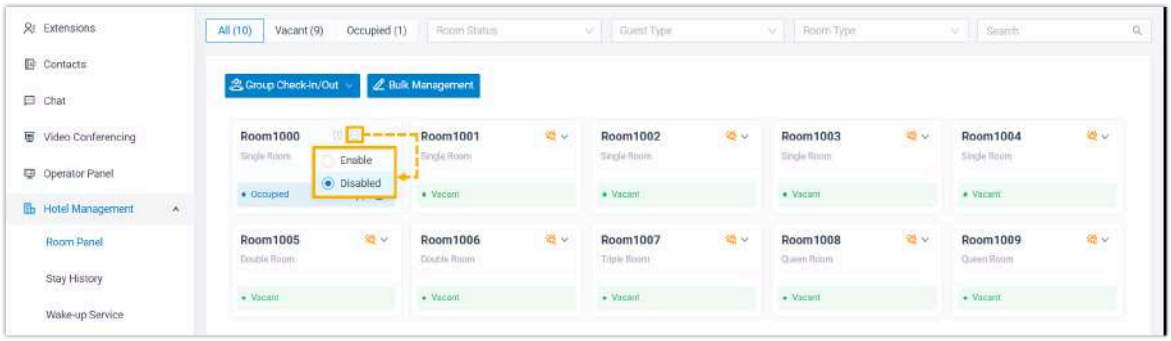


Set Do Not Disturb (DND)

Front desk can enable DND for room phones when guests do not want to be disturbed, and disable DND when guests are ready to answer calls.

Procedure

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. At the top-right corner of a checked-in room, click ⊖, then select an option to enable or disable DND for the room phone.



Result

The DND setting is applied to the room phone, and the presence status of the associated extension is updated accordingly.

- When DND is enabled, extension presence is set to **Do Not Disturb**, and the room extension will not receive any calls.
- When DND is disabled, extension presence will be set to **Available**, and the room extension can receive calls.

Change Room Status

This topic describes how to change the status of guest rooms from Room Panel on Linkus Desktop/Web Client, so as to stay updated on rooms' condition.

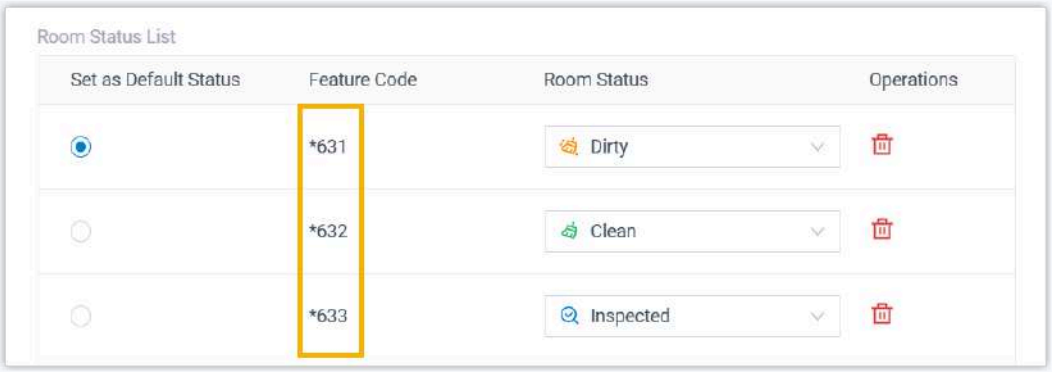
Background information

Yeastar P-Series Software Edition supports two ways to change the status of guest rooms:

- Front desk can click to change room status from the visualized **Room Panel** on Linkus Desktop/Web Client.

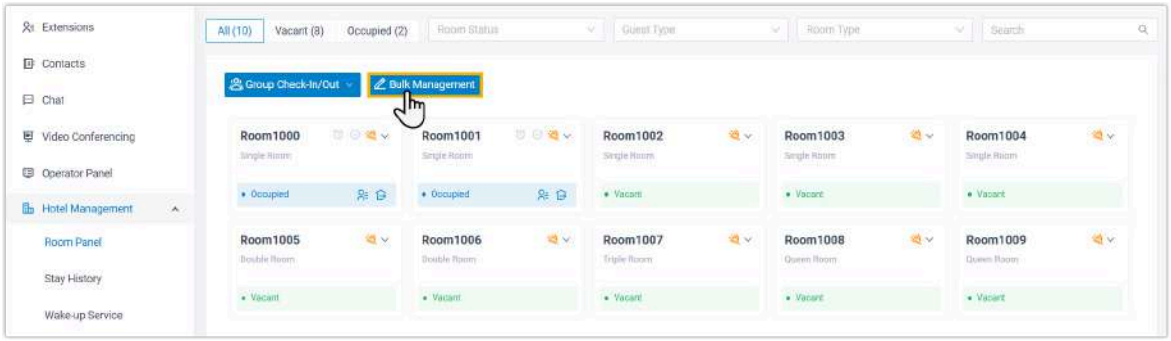
  For detailed instructions, see Change the status of multiple rooms and Change the status of a single room.
- Housekeeper can dial the room status feature code from room phone to change room status.

Note:
For the feature code, contact hotel manager, as the feature codes are automatically generated when hotel manager customizes the room status.

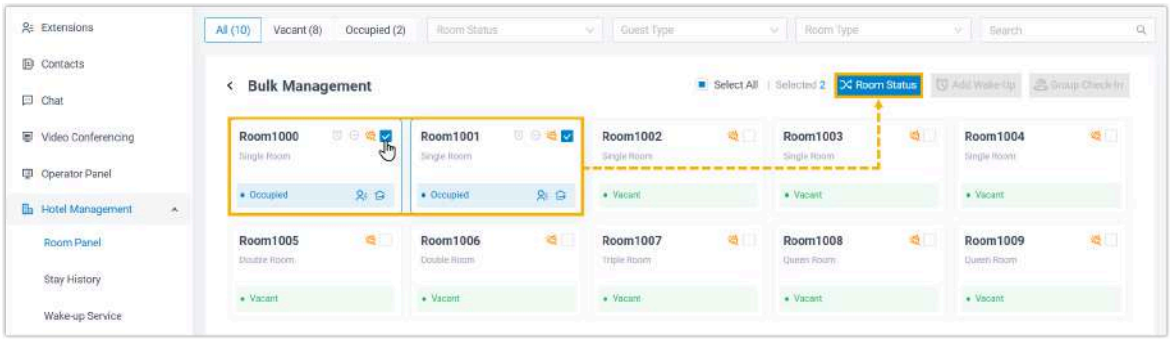


Change the status of multiple rooms

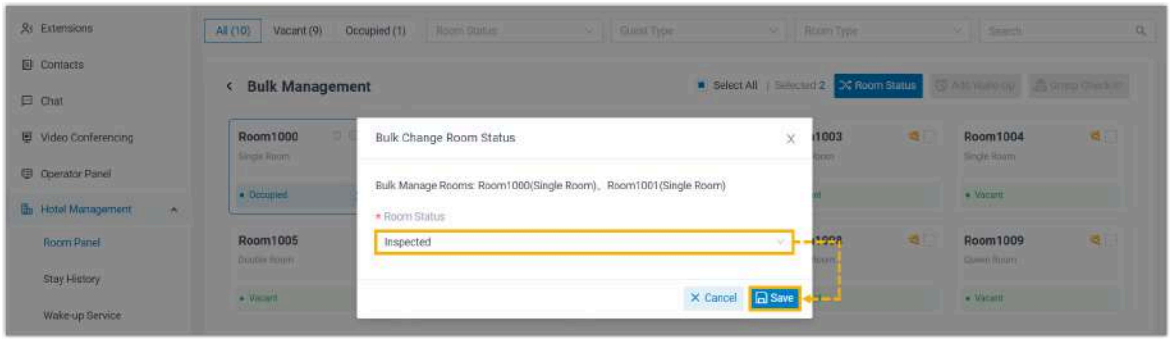
1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. At the top-left corner, click **Bulk Management**.



3. Select the checkboxes of the desired rooms, then click **Room Status**.

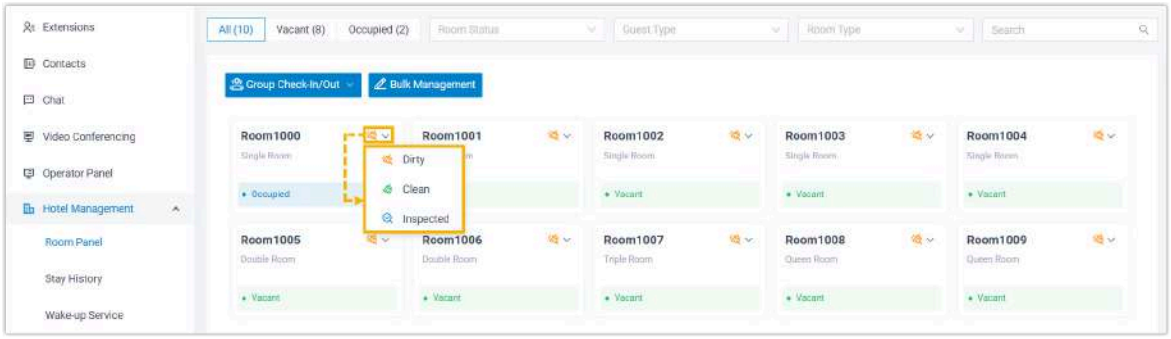


4. In the pop-up window, select a new status from the drop-down list of **Room Status**, then click **Save**.



Change the status of a single room

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. At the top-right corner of a room, click the room status icon, then select a status from the drop-down list.



Wake-up Call

Schedule Wake-up Calls

When guests request alarms, front desk can schedule wake-up calls on Linkus Desktop/Web Client. Alternatively, guests can schedule their own wake-up calls from their room phones.

Restriction

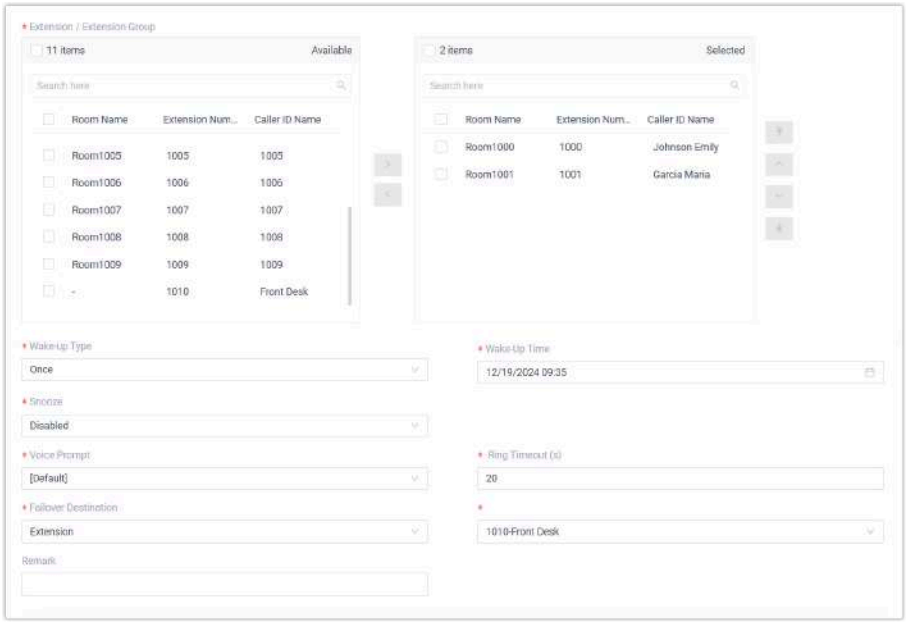
A guest can have up to 23 pending wake-up calls.

Schedule a wake-up task from Wake-up Service panel

You can schedule wake-up tasks from the Wake-up Service panel, a dedicated panel for delivering wake-up call service, ideal for adding alarms for multiple guests at a time.

Procedure

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Wake-up Service**.
2. Under **Wake-Up Task** tab, add a wake-up task.
    a. At the top-left corner, click **Add**.
    b. Complete the following settings to schedule the task.



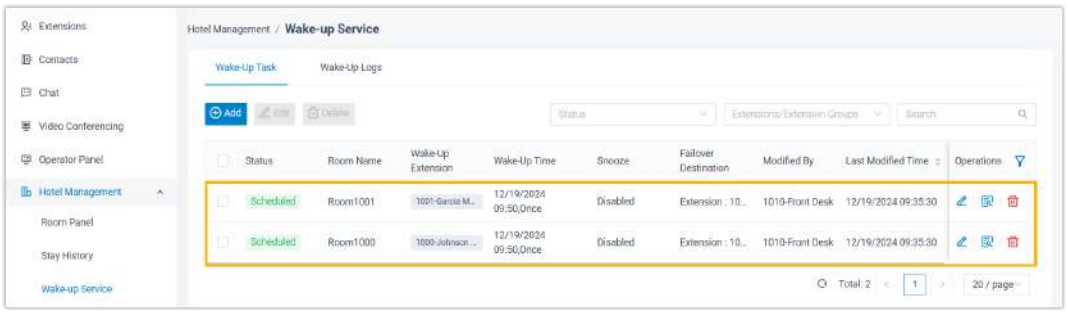
Setting	Description
Extension / Extension Group	Select the guest room(s) for which you want to schedule wake-up calls.
Wake-up Type	Select the frequency of the wake-up task. • **Once** • **At Daily** • **Week** • **Month**
Wake-Up Time	Select a wake-up time.
Snooze	Set the number of times to repeat the call if the guest(s) don't answer the wake-up call, as well as the interval between each repeat.
Voice Prompt	Select the voice prompt to be played when the guest(s) answer the wake-up call. **Note:** The available prompts are configured by hotel manager under custom prompts (Path: **PBX Settings > Voice Prompt > Custom Prompt**).
Ring Timeout (s)	Set the time for the wake-up call to ring before it times out (**Unit**: Second).

Setting	Description
	Valid value: 5 - 300
Failover Destination	Set the failover destination if the guest(s) don't answer the wake-up call. • **Hang Up** • **Extension** • **Ring Group**
Remark	Add additional information.

c. Click **Save**.

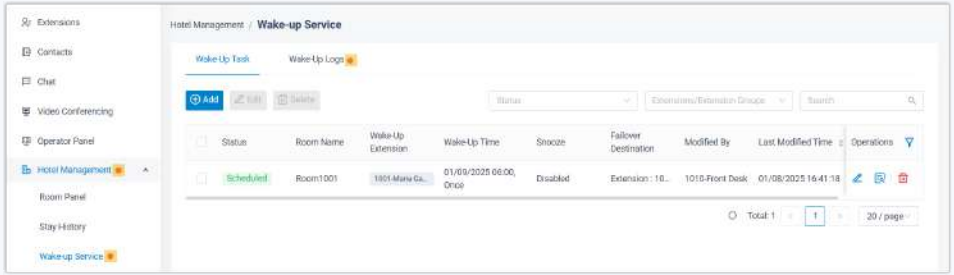
Result

The wake-up task is scheduled and displayed on the list.

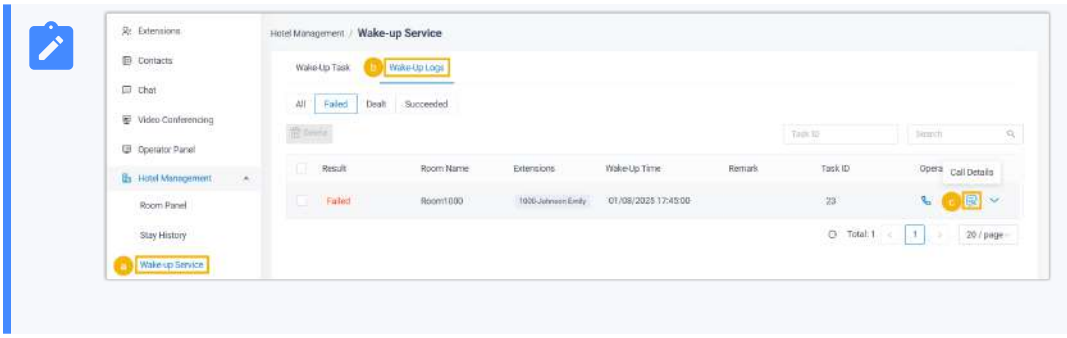


When it reaches the wake-up time, the PBX will make a call to the room phone(s). After the guest(s) answer the call, the system will play the specified voice prompt, then hang up the call.

Note:
If the wake-up task fails, red dot badges will appear to alert you.



You can access the **Wake-Up Logs** page to check the reason for the failure.



Schedule a wake-up task from Room Panel

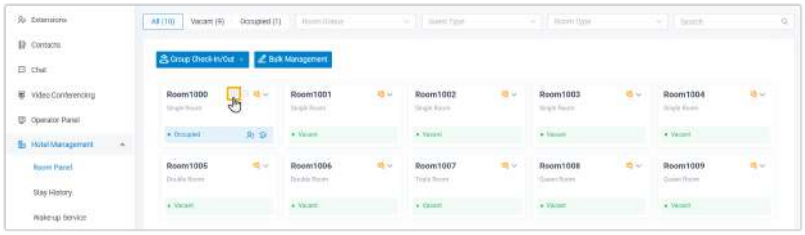
You can schedule wake-up tasks from the Room Panel, a room-based panel that visualizes all guest rooms, ideal for adding alarms for one or multiple guests.

Procedure

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. Access the wake-up call configuration page of the desired guest rooms.

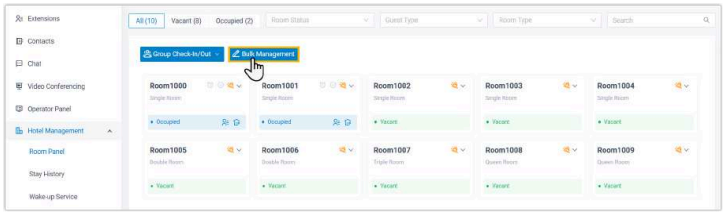
For a Single room

At the top-right corner of a checked-in room, click .

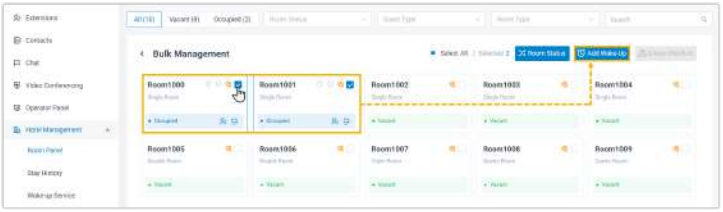


For multiple rooms

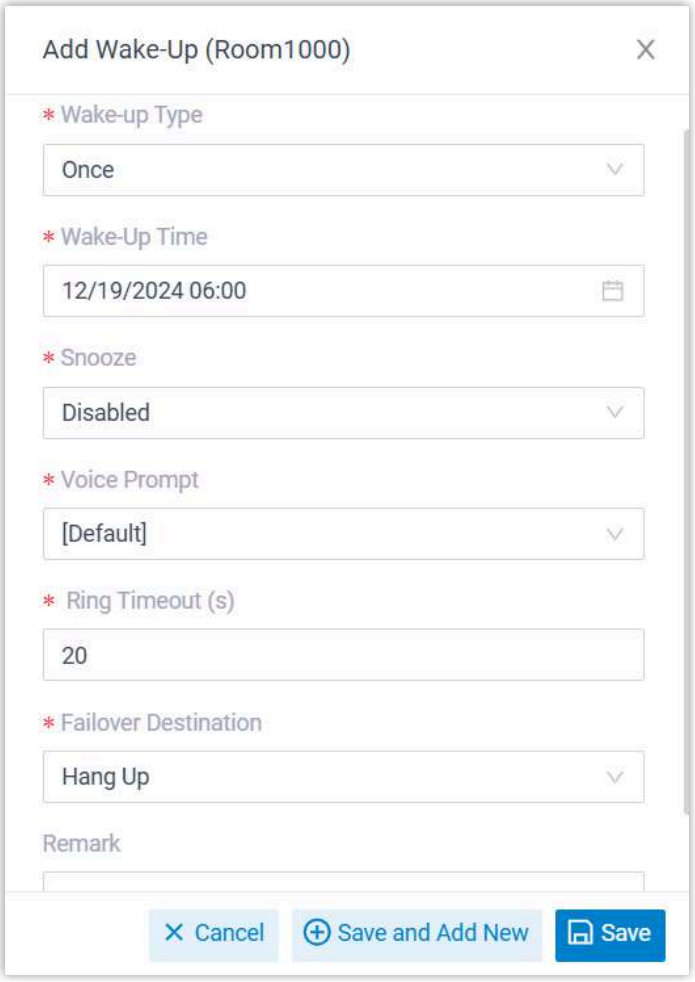
a. At the top-left corner, click **Bulk Management**.



b. Select the checkboxes of the checked-in rooms, then click **Add Wake-Up**.



3. In the pop-up window, schedule a wake-up call, then save the configuration.

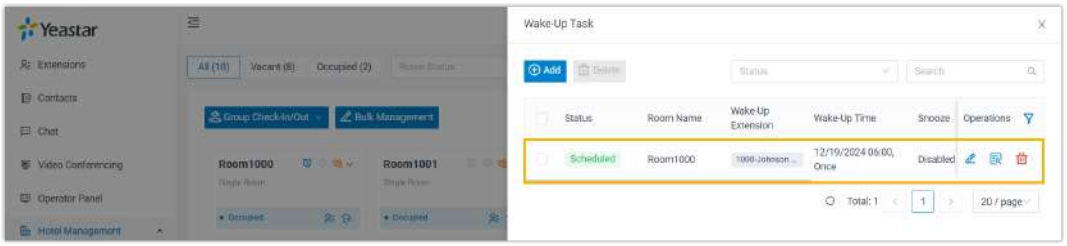


Setting	Description
Wake-up Type	Select the frequency of the wake-up call. • **Once** • **At Daily** • **Week** • **Month**
Wake-Up Time	Select a wake-up time.

Setting	Description
Snooze	Set the number of times to repeat the call if the guest(s) don't answer the wake-up call, as well as the interval between each repeat.
Voice Prompt	Select the voice prompt to be played when the guest(s) answer the wake-up call. **Note:** The available prompts are configured by hotel manager under custom prompts (Path: **PBX Settings > Voice Prompt > Custom Prompt**).
Ring Timeout (s)	Set the time for the wake-up call to ring before it times out (**Unit**: Second). **Valid value**: 5 - 300
Failover Destination	Set the failover destination if the guest(s) don't answer the wake-up call. • **Hang Up** • **Extension** • **Ring Group**
Remark	Add additional information.

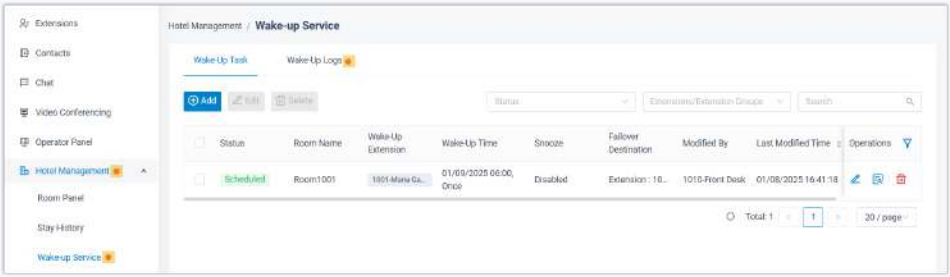
Result

The wake-up task is scheduled and displayed on the list.

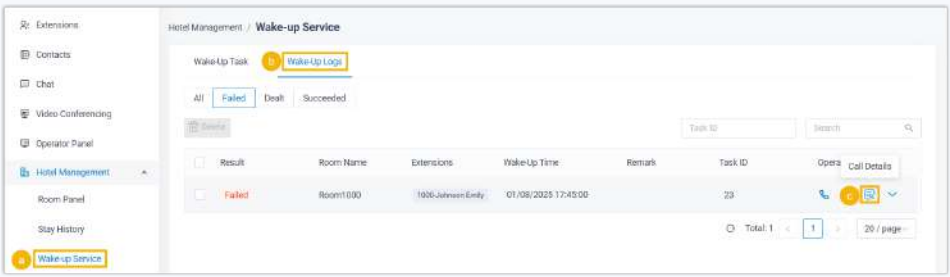


When it reaches the wake-up time, the PBX will make a call to the room phone(s). After the guest(s) answer the call, the system will play the specified voice prompt, then hang up the call.

Note:
If the wake-up task fails, red dot badges will appear to alert you.



You can access the **Wake-Up Logs** page to check the reason for the failure.



Schedule a wake-up task from room phone

Guests can schedule their own wake-up calls directly from their room phones, without having to contact the front desk. To achieve this, you need to obtain the wake-up number from hotel manager, provide the number to guests, and instruct them to set a wake-up call by following the audio instructions.

We provide an example to show you how to schedule a wake-up call for **tomorrow at 06:00 AM** from room phone.

1. Dial the wake-up number from room phone.

   The system prompt "Please choose your operation. Press 1 to add wake-up calls. Press 2 to query wake-up calls. Press 3 to delete wake-up calls. Press 0 to delete all wake-up calls. Press # to exit." will be played to the guest.
2. Press `1` to add a wake-up call.

   The system prompt "Please choose the date for your wake-up call. Press 1 to choose today. Press 2 to choose tomorrow. Press 3 to set custom date." will be played to the guest.
3. Press `2` to set the date of the wake-up call to tomorrow.

   The system prompt "Please enter your wake-up call time in a 24-hour format. For example, 1400 means 2:00 PM." will be played to the guest.

4. Press `0600` to set the time of the wake-up call to 06:00 AM.

   The system prompt "Operate Successfully. Your wake-up call is set for *{wakeup_time}* will be played to the guest.
5. Hang up the call, or repeat steps 2-4 to add another wake-up call.

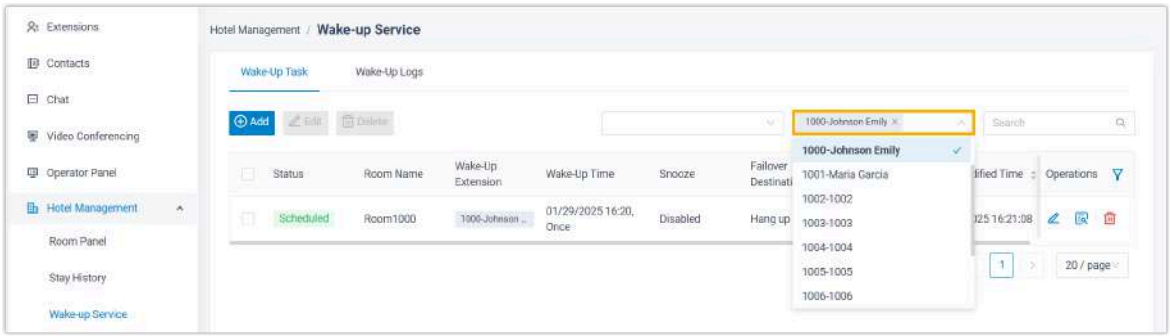
Query Scheduled Wake-up Calls

In case of need, front desk can query the scheduled wake-up calls for guests on Linkus Desktop/Web Client. Alternatively, guests can query their own scheduled wake-up calls from their room phones.

Query scheduled wake-up tasks from Wake-up Service panel

You can query scheduled wake-up calls for one or multiple guests from the dedicated Wake-up Service panel.

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Wake-up Service > Wake-Up Task**.
2. Filter the room(s) assigned to the desired guest(s).

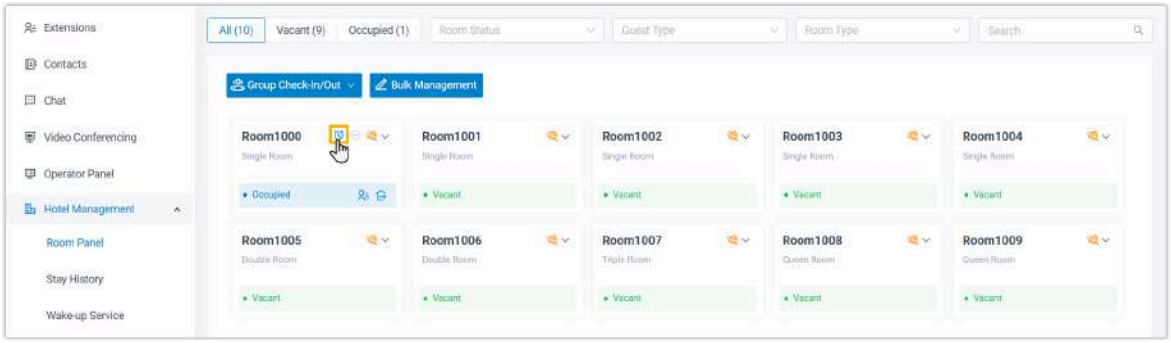


   The scheduled wake-up tasks for the selected guest room(s) are displayed on the list.

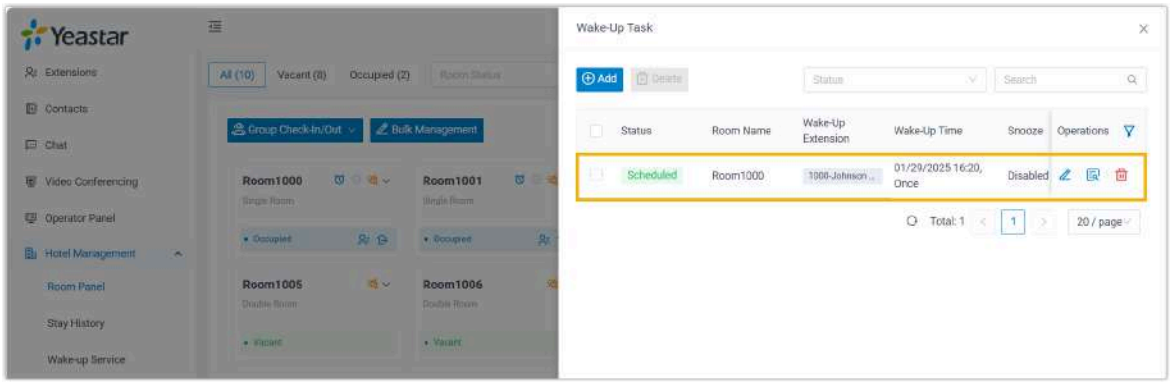
Query scheduled wake-up tasks from Room Panel

You can query scheduled wake-up calls for an individual guest from the Room Panel.

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. At the top-right corner of a desired room, click .



The scheduled wake-up task for the guest room is displayed on the list.



Query scheduled wake-up tasks from room phone

Guests can query their own scheduled wake-up calls directly from their room phones, without having to contact the front desk. To achieve this, you need to obtain the wake-up number from hotel manager, provide the number to guests, and instruct them to query wake-up calls by following the audio instructions.

We provide an example to show you how to query the scheduled wake-up calls from room phone.

1. Dial the wake-up number from room phone.

   The system prompt "Please choose your operation. Press 1 to add wake-up calls. Press 2 to query wake-up calls. Press 3 to delete wake-up calls. Press 0 to delete all wake-up calls. Press # to exit." will be played to the guest.
2. Press `2` to query wake-up calls.

   The system prompt "You have *`{number}`* wake-up calls. First *`{wakeup_time}`*..." will be played to the guest.
3. Hang up the call, or press a number to proceed.

Update Scheduled Wake-up Calls

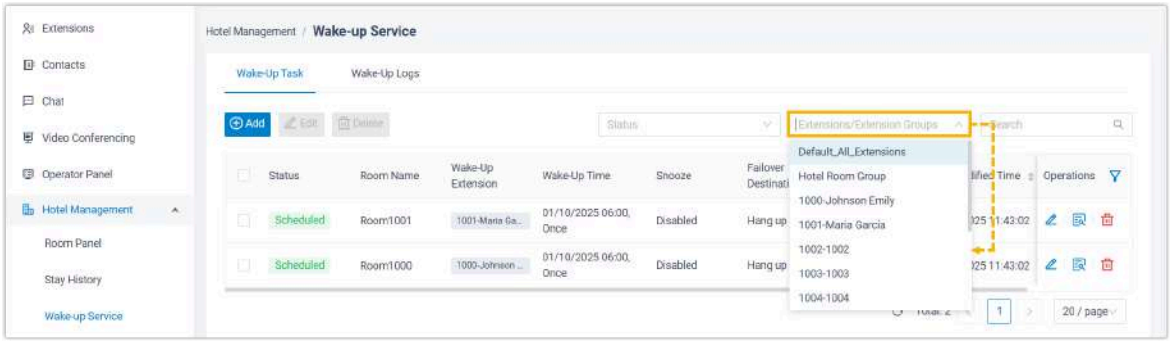
When guests need to update their scheduled wake-up calls, front desk can handle the request on Linkus Desktop/Web Client.

> **Note:**
> Guests can NOT update their scheduled wake-up calls from their room phones.

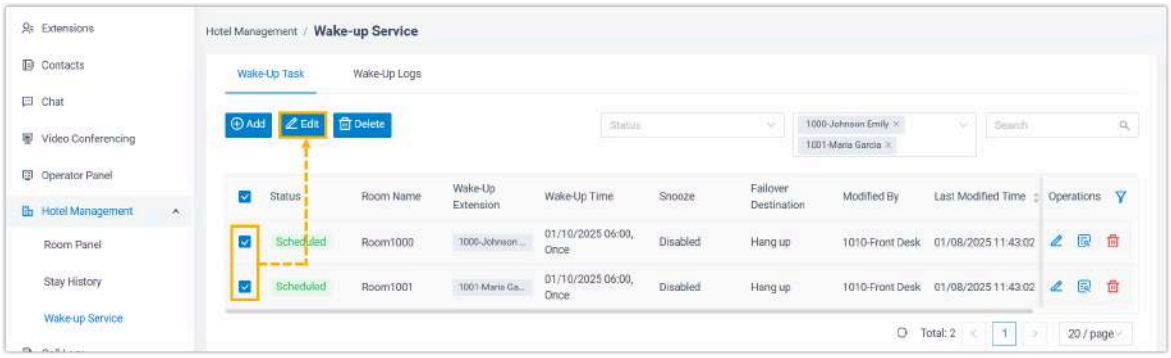
Update scheduled wake-up tasks from Wake-up Service panel

You can update scheduled wake-up calls for one or multiple guests from the dedicated Wake-up Service panel.

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Wake-up Service > Wake-Up Task**.
2. Filter the rooms assigned to the desired guest(s).



3. Select the checkboxes of the desired tasks, then click **Edit** to edit the tasks as needed.

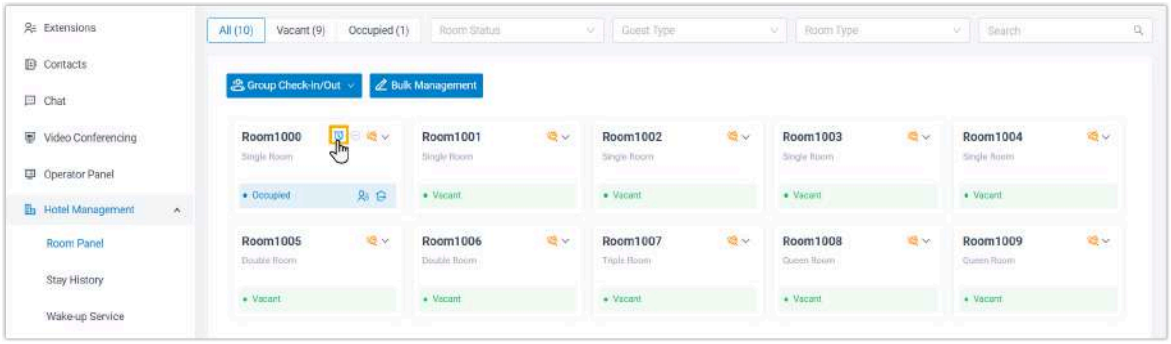


4. Click **Save**.

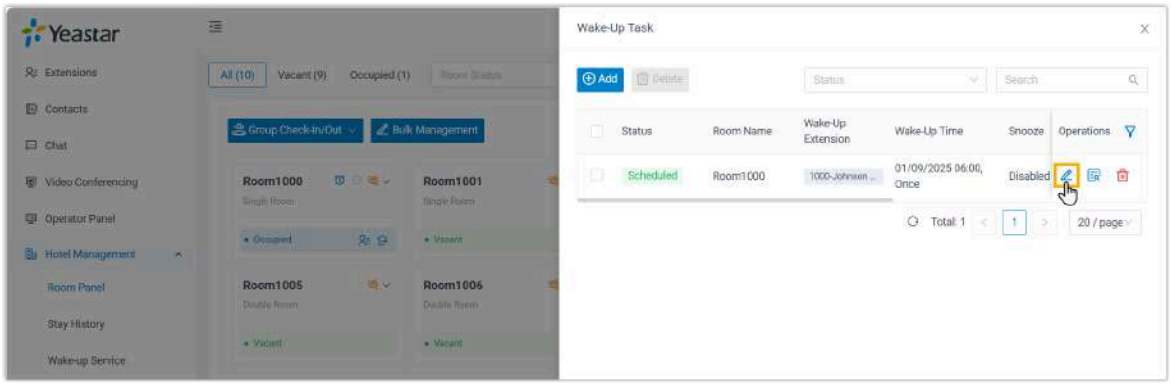
Update scheduled wake-up tasks from Room panel

You can update scheduled wake-up calls for an individual guest from the Room Panel.

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. At the top-right corner of a desired room, click .



3. On the right panel, click to edit the wake-up task as needed.



4. Click **Save**.

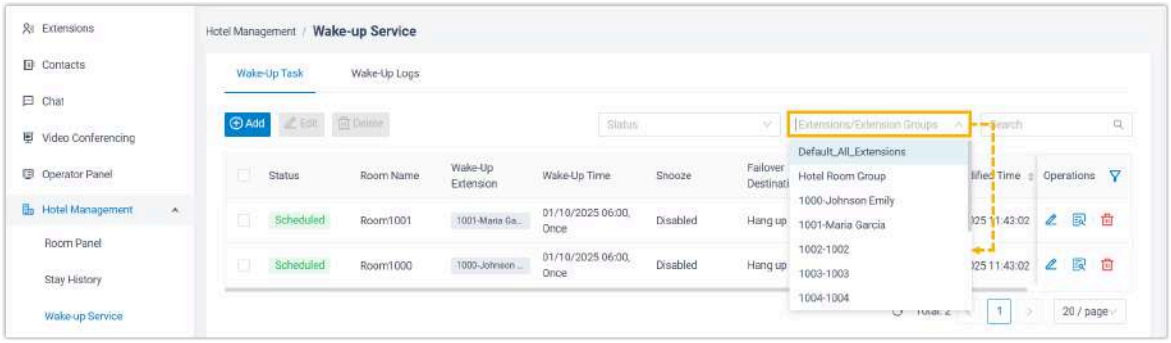
Delete Scheduled Wake-up Calls

If guests need to cancel alarms, front desk can delete wake-up calls on Linkus Desktop/Web Client. Alternatively, guests can delete their own wake-up calls from their room phones.

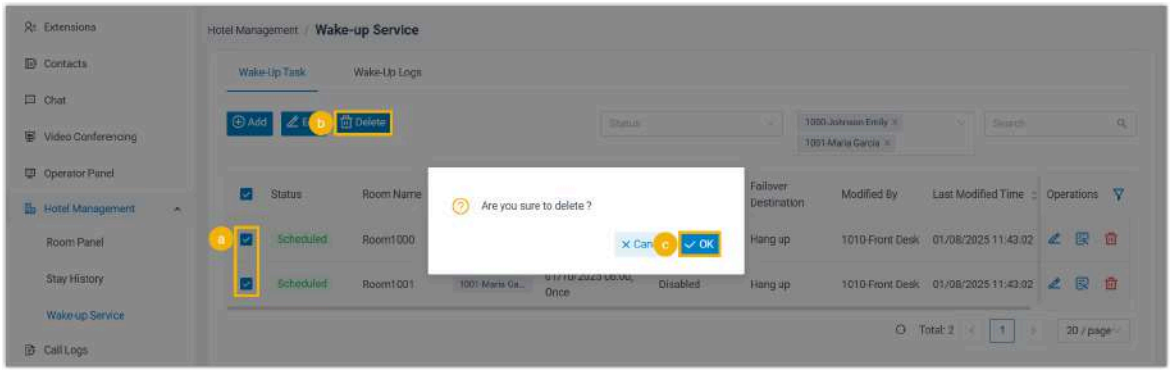
Delete scheduled wake-up tasks from Wake-up Service panel

You can delete scheduled wake-up calls for one or multiple guests from the dedicated Wake-up Service panel.

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Wake-up Service > Wake-Up Task**.
2. Filter the rooms assigned to the desired guest(s).



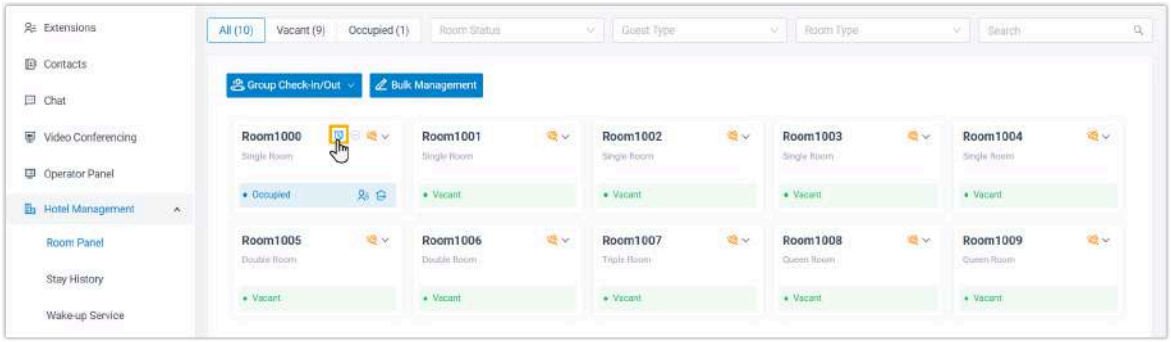
3. Select the checkboxes of the desired tasks, click **Delete**, then click **OK**.



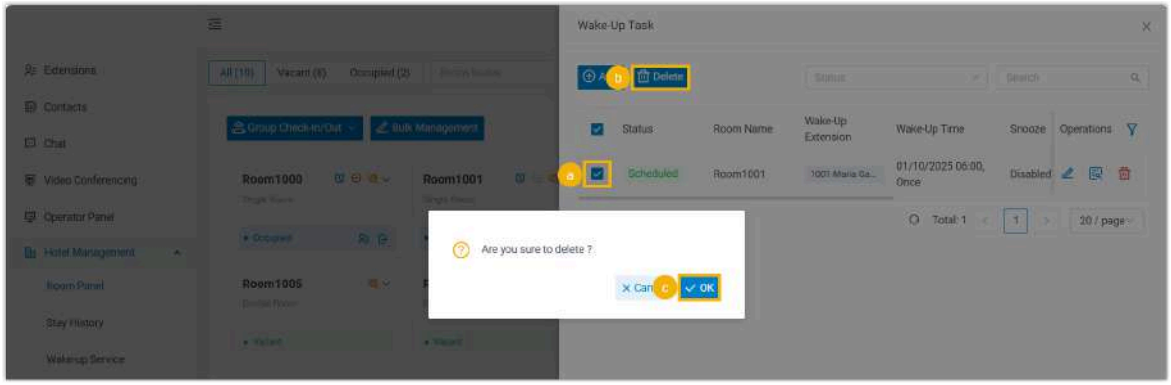
Delete scheduled wake-up tasks from Room Panel

You can delete scheduled wake-up calls for an individual guest from the Room Panel.

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. At the top-right corner of a desired room, click .



3. On the right panel, select the checkboxes of the desired tasks, click **Delete**, then click **OK**.



Delete scheduled wake-up tasks from room phone

Guests can delete their own wake-up calls directly from their room phones, without having to contact the front desk. To achieve this, you need to obtain the wake-up number from hotel manager, provide the number to guests, and instruct them to delete wake-up calls by following the audio instructions.

We provide two examples to show you how to delete wake-up calls from room phone.

Delete one or multiple wake-up calls

1. Dial the wake-up number from room phone.

   The system prompt "Please choose your operation. Press 1 to add wake-up calls. Press 2 to query wake-up calls. Press 3 to delete wake-up calls. Press 0 to delete all wake-up calls. Press # to exit." will be played to the guest.
2. Press `3` to delete a wake-up call.

   The system prompt "You have *`{number}`* wake-up calls. First *`{wakeup_time}`*... Please enter the number of the wakeup call you want to delete. Or, Press 0 to delete all wakeup calls. Press * to cancel." will be played to the guest.
3. Press a number to delete the corresponding wake-up call.

   The system prompt "Operate Successfully." will be played to the guest.
4. Hang up the call, or repeat steps 2-4 to delete another wake-up call.

Delete all wake-up calls

1. Dial the wake-up number from room phone.

   The system prompt "Please choose your operation. Press 1 to add wake-up calls. Press 2 to query wake-up calls. Press 3 to delete wake-up calls. Press 0 to delete all wake-up calls. Press # to exit." will be played to the guest.
2. Press `0` to delete all wake-up calls.

   The system prompt "Press 1 to delete all wake-up calls. Or, Press * to cancel." will be played to the guest.
3. Press `1` to confirm the deletion.

   The system prompt "Operate Successfully." will be played to the guest.
4. Hang up the call.

Check Wake-up Call Logs

Each time a wake-up task is executed, the activity will be logged for tracking purposes. In the event that a wake-up task fails, front desk can review the log for details.

Restriction

A maximum of 100,000 wake-up call logs can be stored.

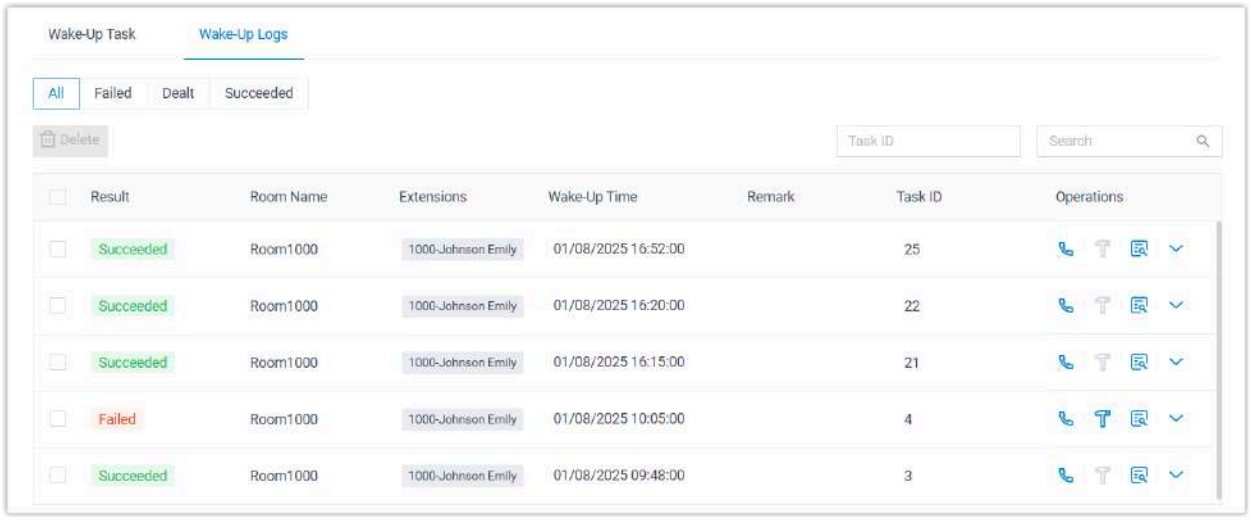
> **Note:**
> When it reaches the maximum number, the oldest logs will be deleted automatically.

Procedure

Log in to Linkus Desktop/Web Client, go to **Hotel Management > Wake-up Service > Wake-Up Logs**.

Result

All the wake-up call logs are displayed on the list.



Note:

For a failed wake-up task, you can click to view the reason for the failure and take appropriate actions. When done, you can click to mark the task as dealt.

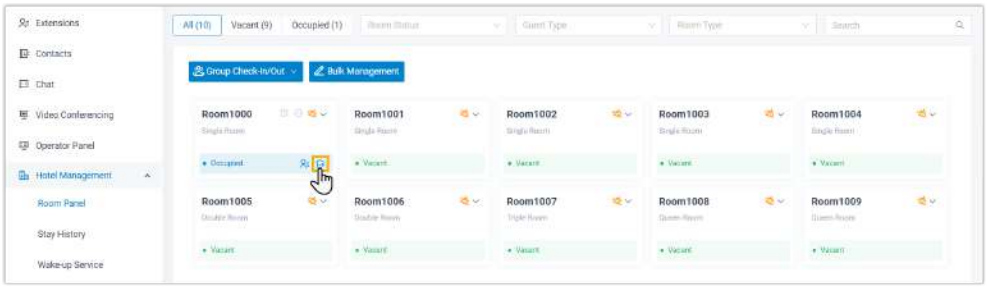
Check out

When guests are ready to leave, front desk can complete the check-out process for them.

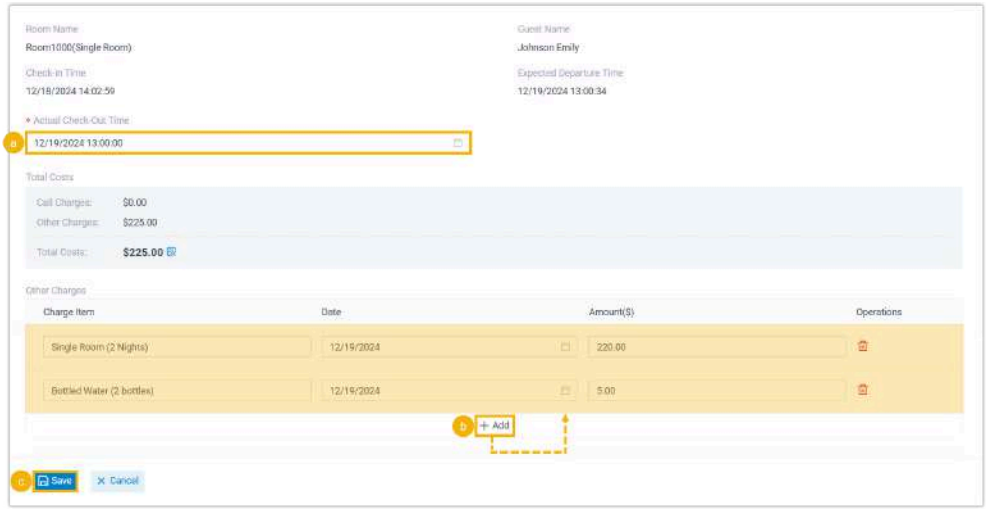
Individual guest check-out

Procedure

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. At the bottom-right corner of a checked-in room, click .



3. Perform the following operations to check the guest out of the room.



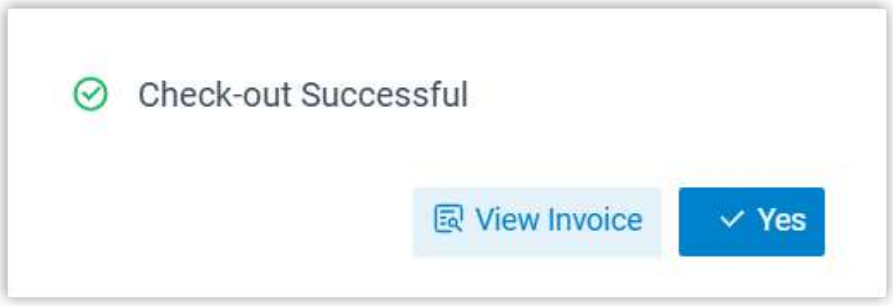
a. In the **Actual Check-Out Time** drop-down list, keep the current time as the check-out time, or change it as needed.
b. In the **Other Charges** section, click **Add** to add charge items for the room.

> **Note:**
> A maximum of 10 charge items can be added.

c. Click **Save**.

Result

- A window pops up, prompting that the checkout is successful. You can click **View Invoice** to view the invoice and provide it to the guest.



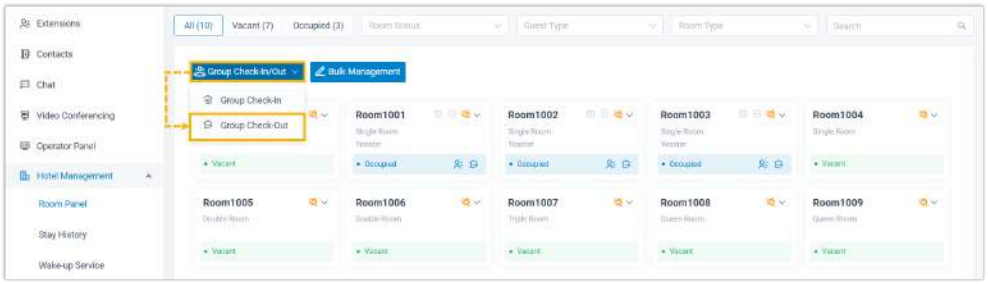
- The guest room is marked as **Vacant** and its status is reset to the default setting.
- The room extension is reset to the default settings and existing data is cleared:

- **Clear the data**: First Name, Mobile Number, Email Address, Voicemail Messages, Call Recordings, Call Logs, Internal Chat histories, Personal Contacts, Video Conferences, Wake-up Calls
- **Reset call permission**: Restrict the extension from making outbound calls and international calls
- **Reset extension presence**: Reset extension presence to **Available**
- **Reset extension setting**: Reset **Last Name** to extension number

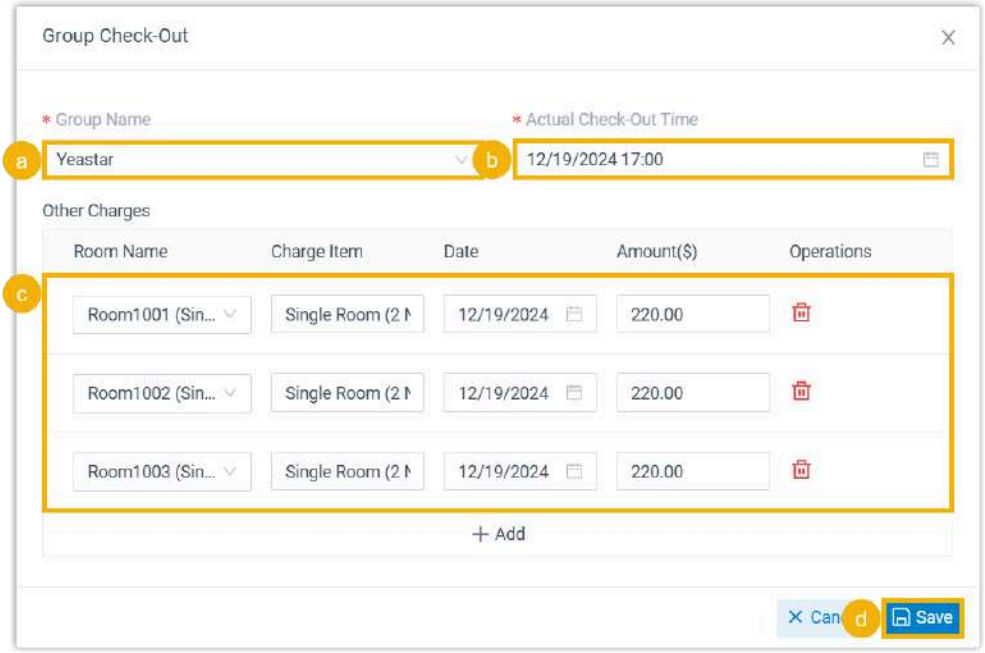
Tour group check-out

Procedure

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. At the top-left corner, click **Group Check-In/Out**, then select **Group Check-Out**.



3. Perform the following operations to check a tour group out of the rooms.



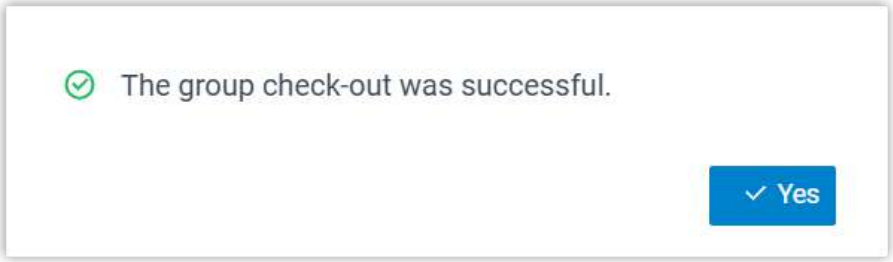
a. In the **Group Name** drop-down list, select a tour group.
b. In the **Actual Check-Out Time** drop-down list, keep the current time as the check-out time, or change it as needed.
c. In the **Other Charges** section, click **Add** to add charge items for the tour group.

> **Note:**
> A maximum of 640 charge items can be added.

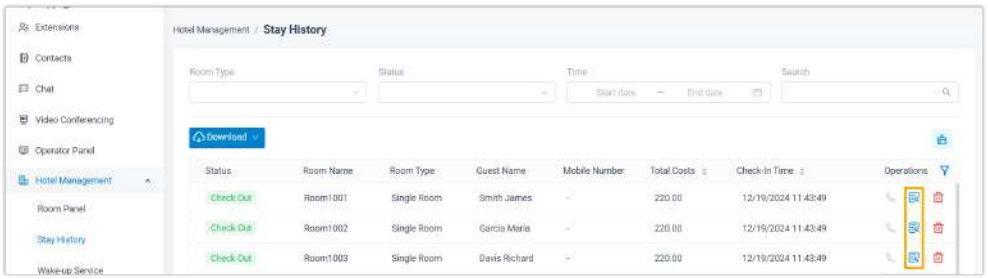
d. Click **Save**.

Result

- A window pops up, prompting that the checkout is successful.



You can view the invoices in **Hotel Management > Stay History** and send them to guests.



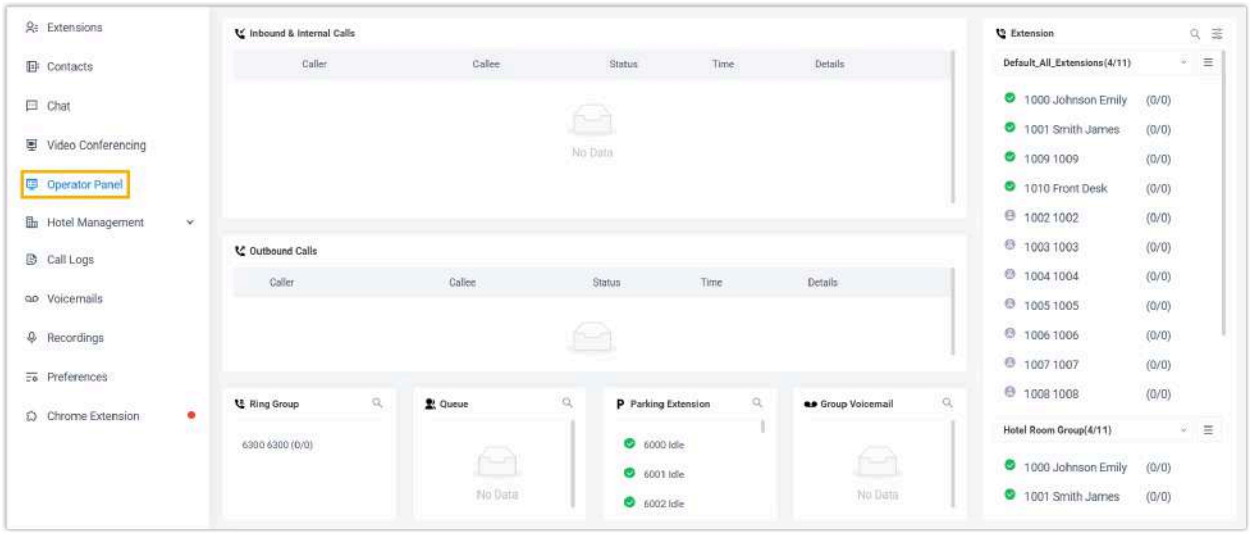
- The temporary extension group for the tour group is removed from PBX.
- The guest rooms are marked as **Vacant** and their statuses are reset to the default setting.
- The room extensions are reset to the default settings and existing data is cleared:
  - **Clear the data**: First Name, Mobile Number, Email Address, Voicemail Messages, Call Recordings, Call Logs, Internal Chat histories, Personal Contacts, Video Conferences, Wake-up Calls
  - **Reset call permission**: Restrict the extension from making outbound calls and international calls
  - **Reset extension presence**: Reset extension presence to **Available**
  - **Reset extension setting**: Reset **Last Name** to extension number

Manage Guest Calls

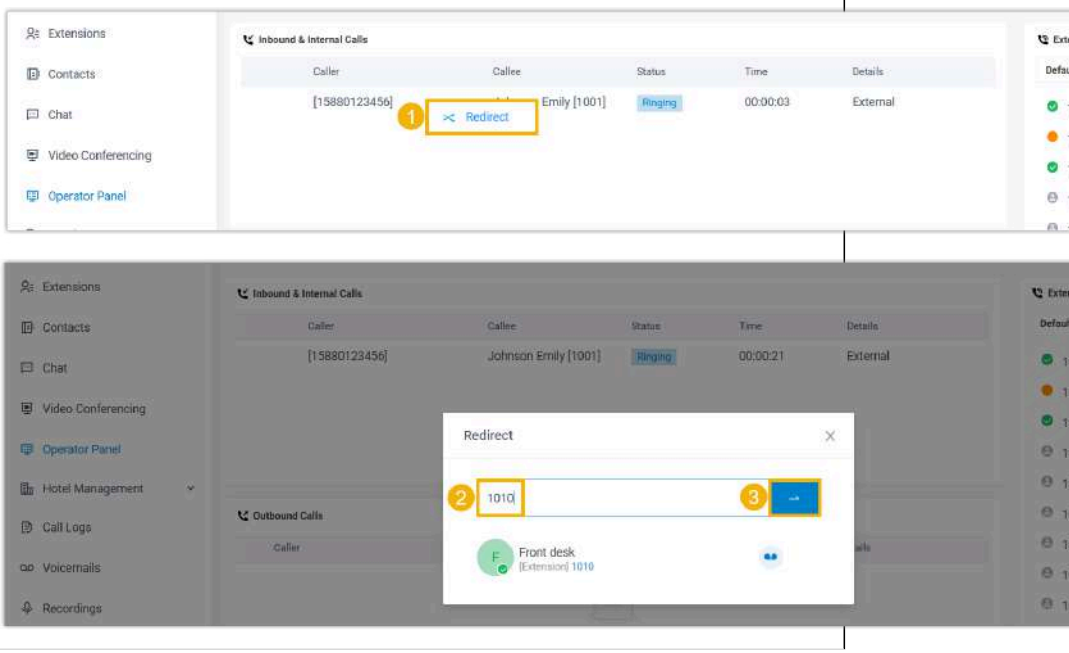
In some cases, front desk may need to manage guest calls, such as transferring calls to another room. This topic describes how front desk can manage guests calls from Operator Panel.

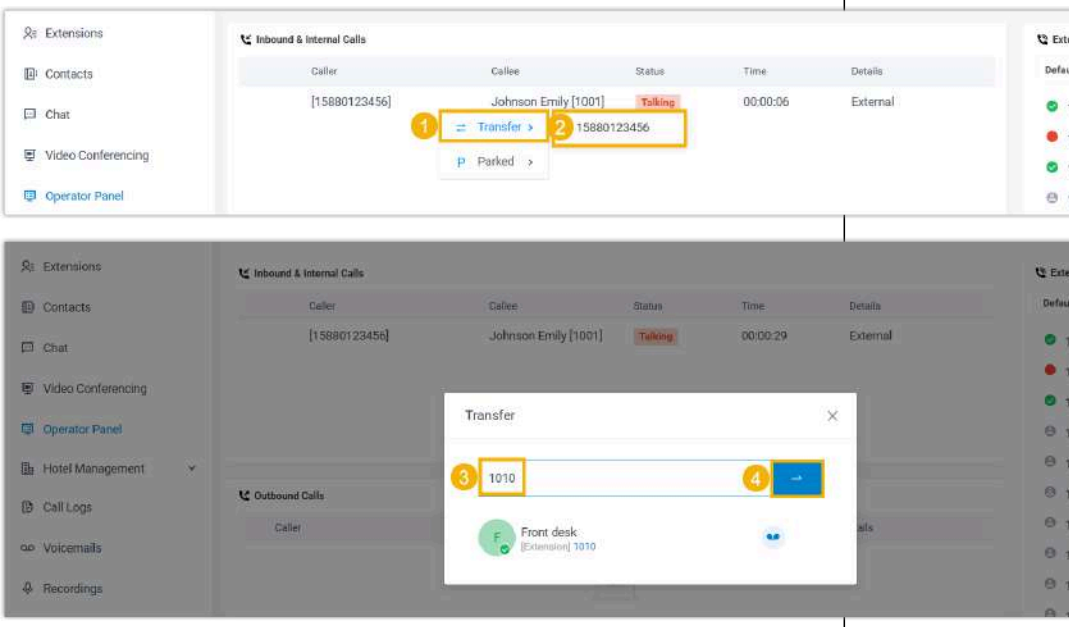
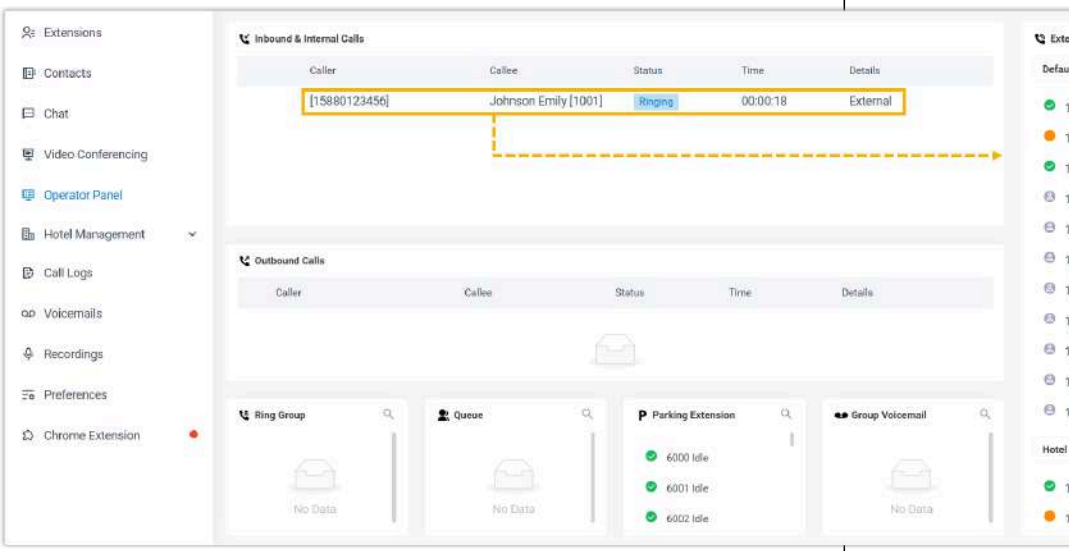
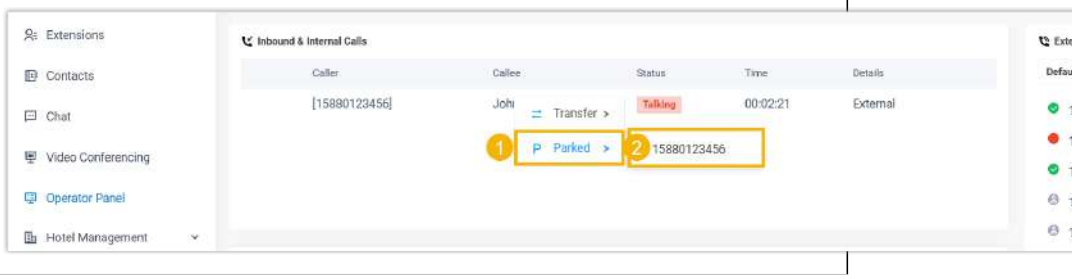
> **Note:**
> This topic provides instructions on how to manage guest calls based on the default privileges assigned by hotel manager. If hotel manager assigns you more privileges, refer to Operator Panel User Guide for detailed instructions.

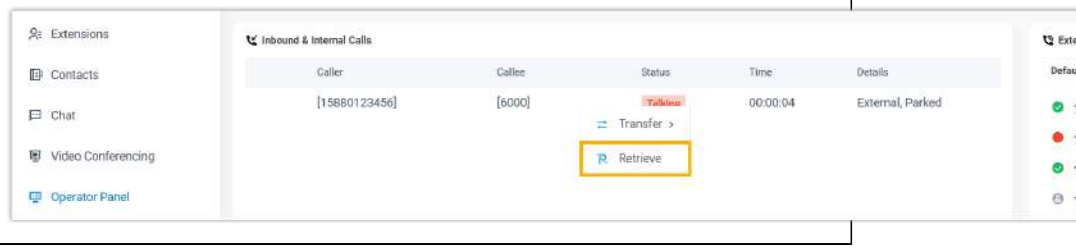
On Linkus Desktop/Web Client, go to **Operator Panel**.



Refer to the following table to see how to manage guests calls according to the assigned privileges.

Privilege	Instruction
Redirect a call	

Privilege	Instruction
Transfer a call	
Drag a call and drop to extension	
Park a call	

Privilege	Instruction
Retrieve a call	

View and Manage Guest Stay History

Guest Stay History provides quick information on the visits of guests. This topic describes how front desk can view, download, and delete guest stay histories.

Restriction

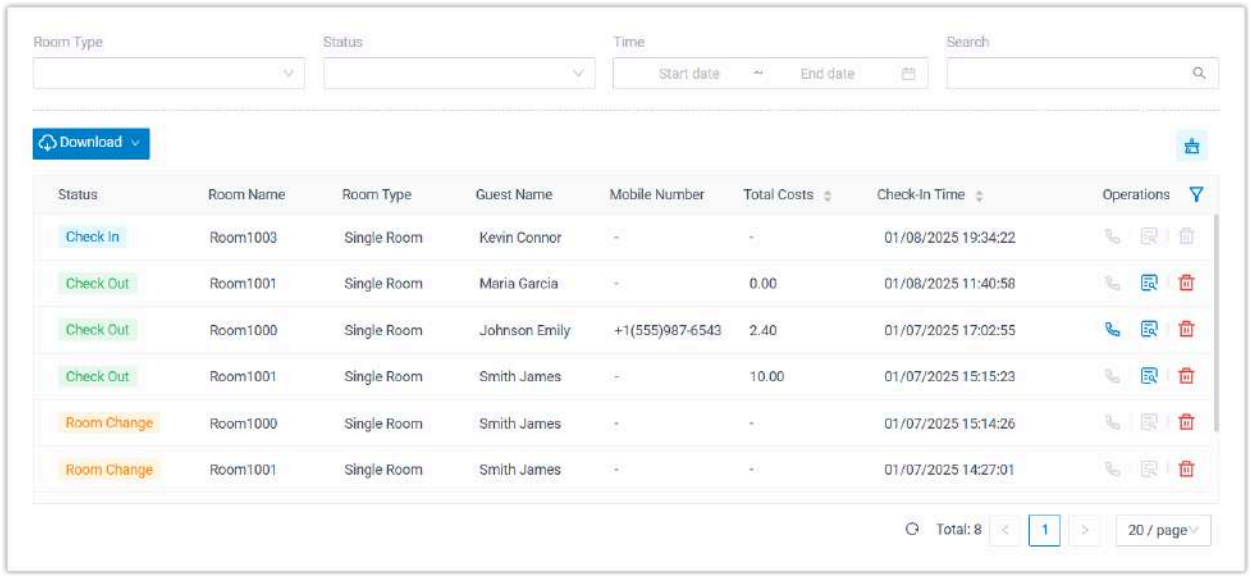
A maximum of 100,000 guest stay histories can be stored.

> **Note:**
> When it reaches the maximum number, the oldest histories will be deleted automatically.

View guest stay history

Log in to Linkus Desktop/Web Client, go to **Hotel Management > Stay History**.

All the guest stay histories are displayed on the list.



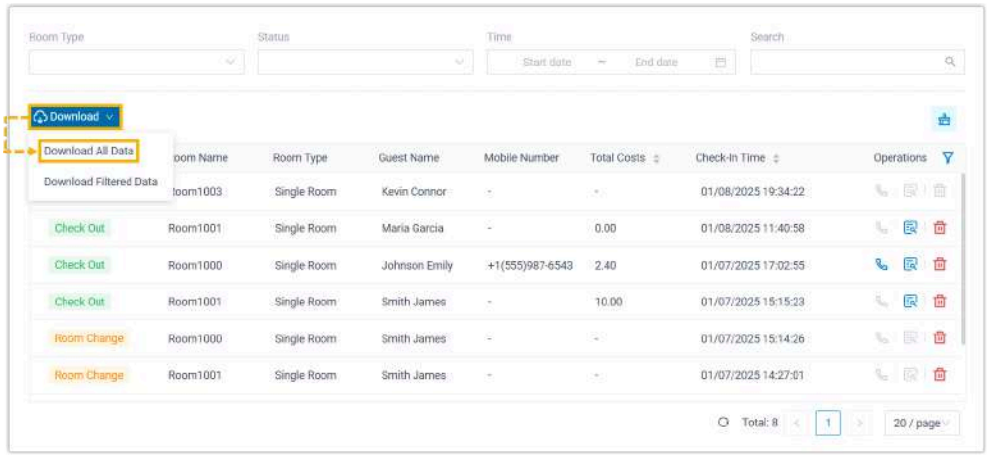
Download guest stay history

You can download all guest stay histories, or filter and download only the histories you need.

> **Note:**
> Invoices are NOT included in the download. To download invoices, see Check guest invoices.

Download all guest stay histories

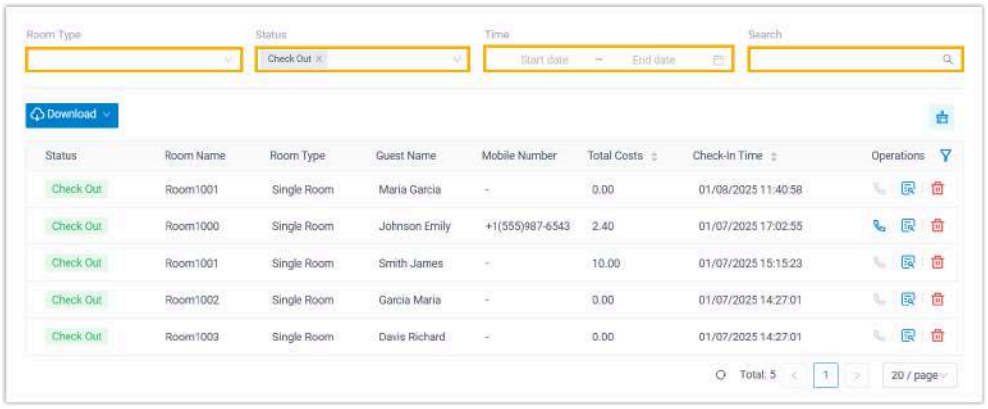
1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Stay History**.
2. Click **Download**, then select **Download All Data**.



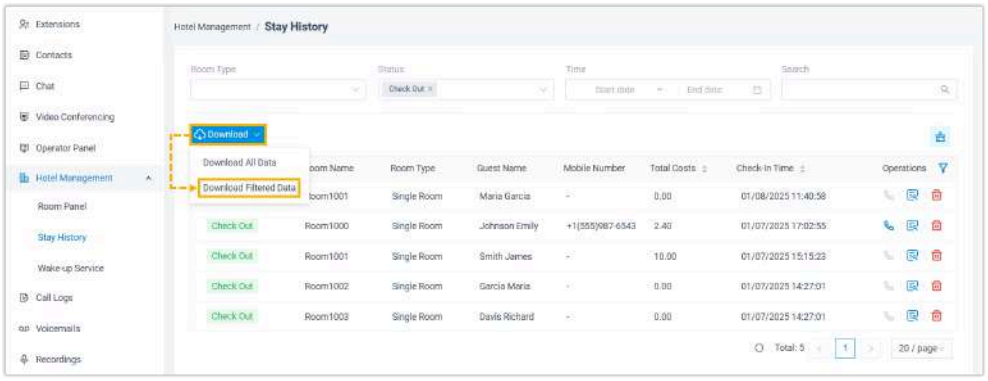
All guest stay histories will be downloaded to your computer as a `.csv` file.

Download specific guest stay histories

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Stay History**.
2. Filter out the desired guest stay histories.



3. Click **Download**, then select **Download Filtered Data**.



The filtered guest stay histories will be downloaded to your computer as a `.csv` file.

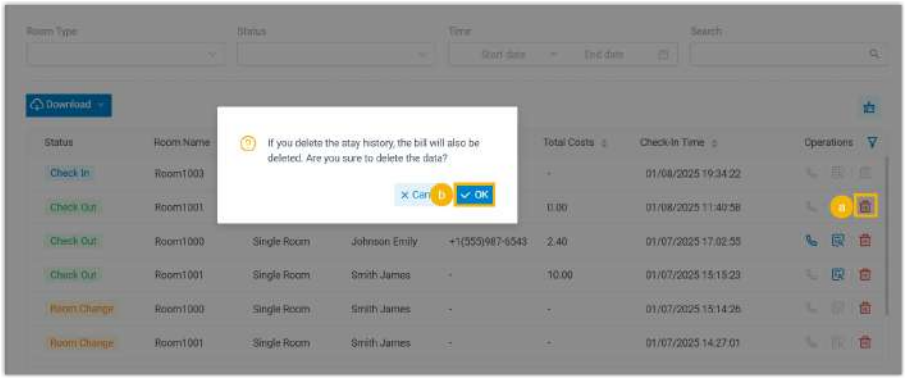
Delete guest stay history

Restriction

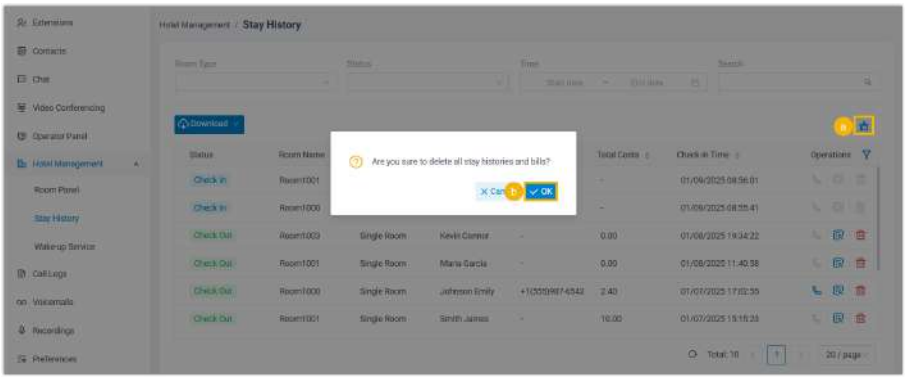
Only guest histories with **Check Out** or **Room Change** status can be deleted.

Procedure

1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Stay History**.
2. Delete guest stay histories as needed.
    - To delete specific histories, click , then click **OK**.



    - To delete all histories, click , then click **OK**.



Result

The guest histories as well as the invoices are deleted from the PBX.

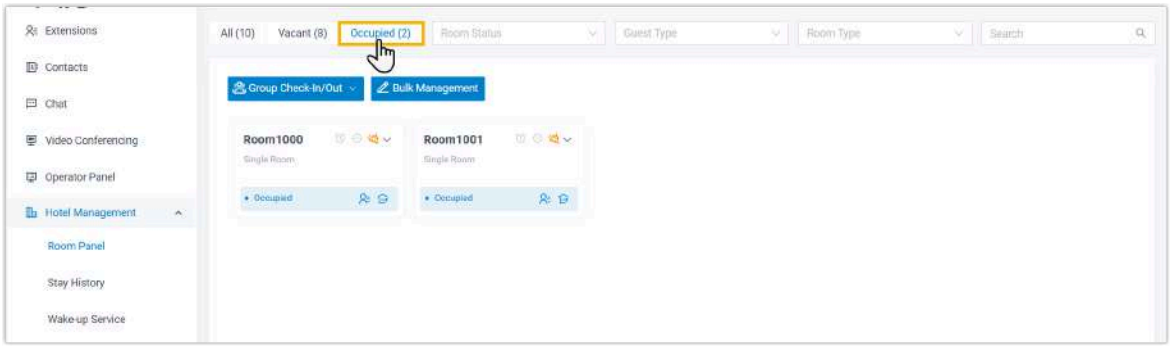
Check Guest Bills and Invoices

When guests check in to the hotel, a bill is created to track the charges incurred by the guests during their stay. Upon check-out, an invoice is generated and can be issued to guests. This topic describes how front desk can check guest bills and invoices.

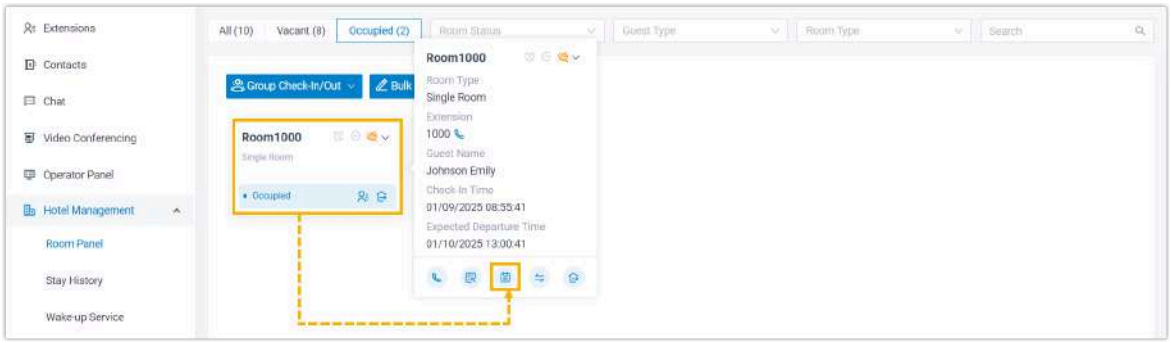
Check guest bills

During a guest's stay, you can review the charges incurred from Room Panel.

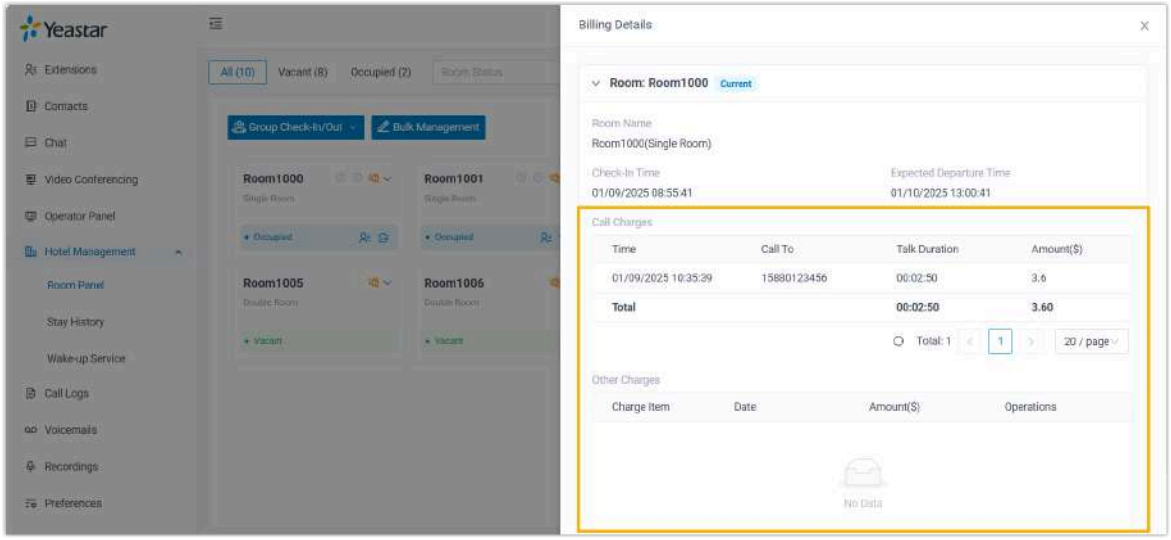
1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Room Panel**.
2. **Optional:** Click **Occupied** tab to filter the checked-in rooms.



3. Click on the desired room, then click .



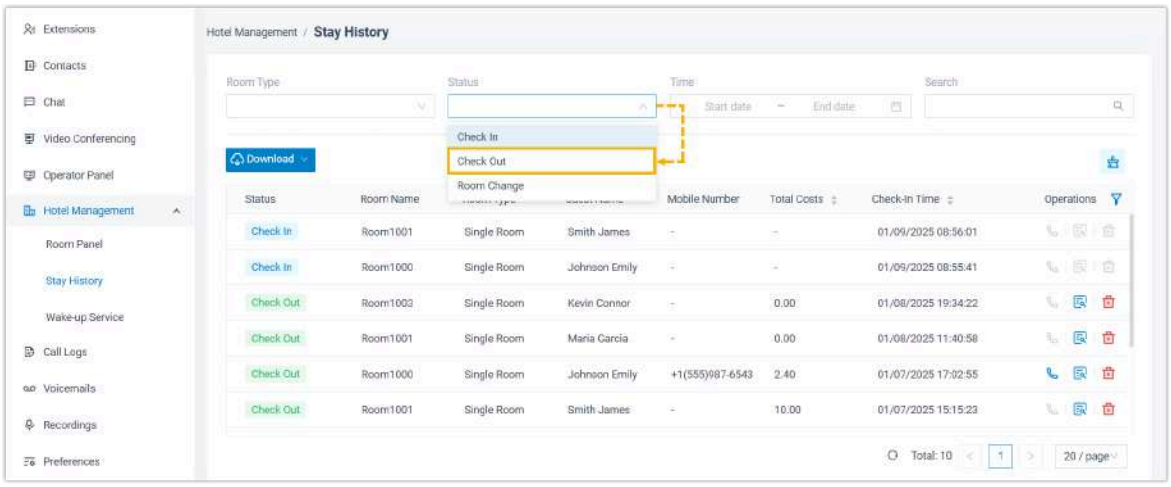
The bill for the guest room is displayed on the right panel.



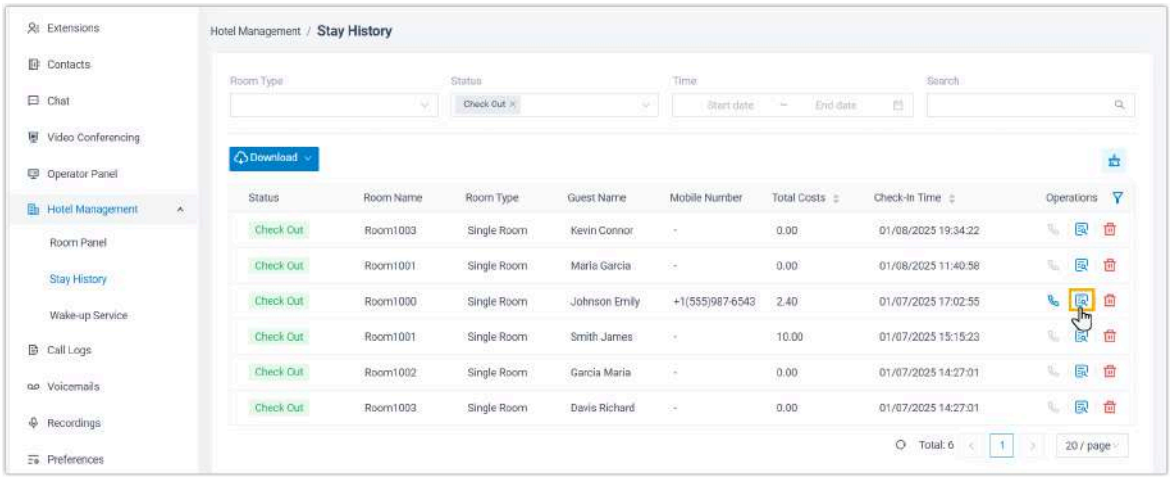
Check guest invoices

When a guest checks out, you can access the guest's invoice from Stay History panel and provide it to the guest.

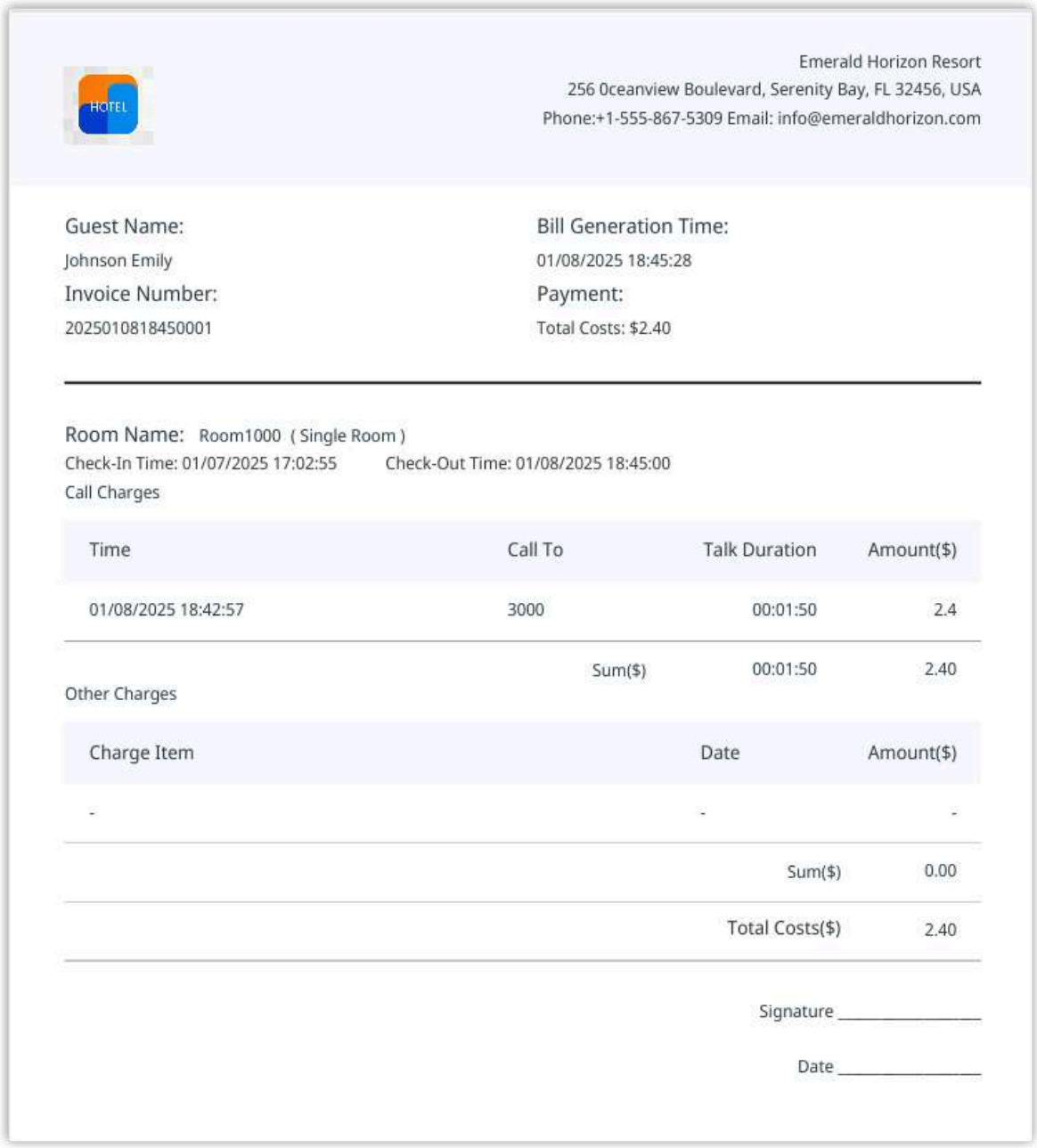
1. Log in to Linkus Desktop/Web Client, go to **Hotel Management > Stay History**.
2. **Optional:** In the **Status** drop-down list, select **Check Out** to filter the checkout histories.



3. Click beside a desired history to view the invoice.



The invoice is opened in a new browser tab.



Emerald Horizon Resort
256 0ceanview Boulevard, Serenity Bay, FL 32456, USA
Phone:+1-555-867-5309 Email: info@emeraldhorizon.com

Guest Name:
Johnson Emily

Bill Generation Time:
01/08/2025 18:45:28

Invoice Number:
2025010818450001

Payment:
Total Costs: $2.40

Room Name: Room1000 (Single Room)
Check-In Time: 01/07/2025 17:02:55 Check-Out Time: 01/08/2025 18:45:00
Call Charges

Time	Call To	Talk Duration	Amount($)
01/08/2025 18:42:57	3000	00:01:50	2.4
	Sum($)	00:01:50	2.40

Other Charges

Charge Item	Date	Amount($)
-	-	-
	Sum($)	0.00
	Total Costs($)	2.40

Signature _____

Date _____

You can download it to your computer as a `.pdf` file and provide it to guest.

Linkus Overview

Yeastar Linkus is designed to keep users connected with colleagues, business partners, and customers anywhere and anytime. To help you quickly understand how to set up and use Yeastar Linkus, we provide an overview on it, including information on Linkus server, Linkus UC clients, and Linkus event notifications.

Linkus server

You need to configure Linkus server according to the users' needs for using Linkus.

- If users only need to use Linkus within the company's Local Area Network (LAN), you need to complete the following settings on Linkus Server:
  1. Enable Linkus clients for users
  2. Send Linkus login credentials to users
- If users need to use Linkus outside the company, you should set up Linkus server for remote access. Yeastar P-Series Software Edition provides the following two remote working solutions to help you set up a remote Linkus server.

Remote Access Service (RAS)

Remote Access Service is a subscription-based service designed for remote working, which is included in **Enterprise Plan** and **Ultimate Plan**. After you subscribe to the plan to get Remote Access Service, you can bind a Yeastar FQDN to the PBX, and enjoy the following benefits:

- Secure connection
- Network Address Translation (NAT) for Linkus service auto configured
- Linkus server for remote access auto configured
- Remote access to Linkus Mobile Client, Desktop Client, and Web Client
- Advanced Linkus features, such as Instant Messaging (IM), video call, and video conferencing

If you choose this solution, refer to the following topics to complete the setup.

1. Set up Linkus server with Remote Access Service
2. Enable Linkus clients for users
3. Send Linkus login credentials to users

Manual configuration

If you don't subscribe to **Remote Access Service** and users need to use Linkus in external network, you have to go through complicated server and network settings, such as port forwarding, NAT and public IP address configuration, so as to implement remote access to Linkus.

Note:

- Weak network protection will cause SIP attacks.
- Incorrect configurations may cause one-way audio issue.

If you choose this solution, refer to the following topics to complete the setup.

1. Manually set up Linkus server
2. Enable Linkus clients for users
3. Send Linkus login credentials to users

Linkus client

Linkus client types

Yeastar P-Series Software Edition supports Linkus Mobile Client, Desktop Client, and Web Client.

The following table lists the requirements for using Linkus clients, as well as the corresponding download links and user guides.

Linkus Client		Requirement
Linkus Mobile Client	iOS	• iOS 11.0 or later
	Android	• Android 6.0 or later

Linkus Client		Requirement
Linkus Desktop Client	Windows	• Windows 7 or later • Minimum 2 GHz (32-bit or 64-bit) processor • Minimum 4 GB memory • Minimum 300 MB free hard drive space
	macOS	• OS X 10.11 El Capitan or later
Linkus Web Client	Browser	• Google Chrome 87 or later • Microsoft Edge 87 or later • Opera 72 or later

Linkus client user permissions

By default, users can access all the menus and configure all the settings within Linkus clients. You can set up permission rules to restrict users' access and configuration permission:

- **Menu Visibility Permission**: Restrict users from specific menus within Linkus clients.
- **Operation Permission**: Restrict users from specific settings within Linkus clients.

For more information, see Set up User Permissions of Linkus Clients.

Linkus client login methods

Yeastar P-Series Software Edition allows users to log in to Linkus clients using different methods, including quick login via a login link or QR code, and manual login with login information.

Quick login

You can send login credentials to users via Linkus welcome emails. In this way, the users can quickly and easily log in to Linkus clients with the QR code or login link provided in the email.

For more information, see Send Linkus Welcome Emails to Users for Quick Login.

Manual login

In case users fail to receive Linkus welcome emails or access their mailboxes, you can provide login information (the username and password of extension account as well as Linkus server network information) for users. In this way, users can manually enter the login information and log in to Linkus clients.

For more information, see Send Linkus Login Information to Users for Manual Login.

Linkus events

Yeastar P-Series Software Edition provides event notification feature. When the following Linkus events occur, the system will record events in logs and notify relevant contacts via specific notification methods.

Event	Description
Operations-related event	
Web User Login Success	An extension user successfully logged in to Linkus Web Client.
Web User Login Failed	An extension user failed to log in to Linkus Web Client.
Linkus Client Login Failed	An extension user failed to log in to Linkus Mobile Client or Linkus Desktop Client.
Extension User Password Changed	An extension user's user password was changed.
Security-related event	
Web User Blocked Out	A specific source IP address was blocked by the system due to too many failed login attempts to Linkus Web Client.
Linkus User Blocked Out	A specific source IP address was blocked by the system due to too many failed login attempts to Linkus Mobile Client or Linkus Desktop Client.

You can customize the event level, notification email template or manage relevant contacts on **System** > (and then)**Event Notification**.

For more information, see Configure Event Notifications and Manage Notification Contacts.

CAMBOX

com

TARIFADOR, MIDIAS e RELATÓRIOS

Datasheet do PABX IP / CALL CENTER / CONTROLE DE ACESSO

Versão do documento: 4.4 - 2023

1. Características do CAMBOX

CAMBOX
SEU PABX IP INTELIGENTE

O CAMBOX é o que há de mais inovador em tecnologia de telecomunicações. Implementado como um Soft-switch, o CAMBOX tem funções antes só disponíveis em equipamentos de grande porte, em uma configuração de pequeno porte, mas, de grande capacidade. Com o CAMBOX, qualquer empresa poderá dispor de unidade de resposta audível, distribuidor automático de chamadas (call center), controle de acesso, gravação de chamadas, fax e correio de voz integrados ao e-mail, interface amigável via web, além de uma infinidade de outras aplicações.

O CAMBOX incorpora as últimas tendências da telefonia sobre protocolo IP, sendo compatível com os principais protocolos de VoIP tais como: SIP, H.323 e IAX2. Com centenas de funções telefônicas, protocolos padronizados e os CODECS mais utilizados no mundo VoIP, o CAMBOX é a melhor relação custo-benefício do mercado de telecomunicações.

Com o uso de placas de interface com as linhas de comunicação das operadoras tradicionais de telefonia (interfaces telefônicas analógicas, Interface E1 G.703), o CAMBOX convive com o mundo tradicional e com as operadoras de VoIP, permitindo à sua empresa uma economia sem precedentes.

O CAMBOX pode ser configurado como um servidor VPN, fechando um túnel criptografado com os aparelhos de telefonia IP no qual toda a informação entre o aparelho telefônico e o servidor é transmitida de forma criptografada, garantindo o sigilo total na comunicação.

Através de sua interface de operação, manutenção e configuração em ambiente web, qualquer pessoa poderá realizar as tarefas comuns de administração do PABX sem a necessidade de um técnico especializado.

2. Principais Características do CAMBOX

- Atendimento Eletrônico automático (URA)
- Distribuidor Automático de Chamadas (DAC)
- Gerenciamento via Web
- Suporte a Interfaces Telefônicas Analógicas e Digitais
- Suporte aos protocolos SIP, IAX e H.323
- Suporte aos Canais TDM via KHOMP, DIGIVOICE, ALIGERA e DIGIUM (DAHDI)
- Solução de alta-disponibilidade com servidores redundantes e funcionamento Ativo-Ativo
- Suporte a Cancelamento de Eco
- Suporte a:
    - CAMBOX em Nuvem

      Suporte a 10.000 Ramais, 1.000 Troncos e a capacidade de tratar 2.000 chamadas simultâneas.
    - CAMBOX Virtualizado

      Suporte a 10.000 Ramais, 1.000 Troncos e a capacidade de tratar 2.000 chamadas simultâneas.
    - CAMBOX Light

      Suporte a 200 Ramais, 50 Troncos e a capacidade de tratar 50 chamadas simultâneas.
    - CAMBOX Server

      Suporte a 1.000 Ramais, 100 Troncos e a capacidade de tratar 200 chamadas simultâneas.
    - CAMBOX Pró

      Suporte a 10.000 Ramais, 1.000 Troncos e a capacidade de tratar 2.000 chamadas simultâneas.
- Slot para instalação de Placas de Interface TDM
- Correio de Voz e Fax para todos os ramais
- Recepção e envio de fax para todos os ramais
- Identificação do assinante chamador (BINA) em todos os ramais
- Bilhetagem de todas as chamadas feita em banco de dados SQL
- Mesa de Operadora implementada em ambiente Web
- Suporte a aparelhos telefônicos VoIP de Mercado

- Suporte a conexão a PABX tradicionais para ampliação e funcionamento conjunto
- Sistema de fácil instalação e operação
- Equipamento de pequenas dimensões
- Baixo consumo de energia
- Compatível com as principais operadoras VoIP nacionais e internacionais
- Provisionamento automático com telefones SIP
- Autenticação via Oauth2, OpenLDAP e Microsoft AD
- Sistema integrado a plataformas de comunicação, como: URA VoIP Interativa, Microsoft Teams, Facebook, Telegram, WhatsApp, Instagram, Messenger, SMS e outros.
- Sistema capacitado para realizar a robotização de funções de acordo com a configuração - BOT
- Tarifador integrado ao PABX IP
- Suporte a Sinalização e Mídia Criptografados: SIP Seguro e SRTP
- Suporte a virtualização em Soluções: VmWARE, Microsoft Hyper-V, KVM, XEN Server, XCP-NG e ProxMox

3. Descrição técnica do Softphone para PC (Desktop) ou dispositivo móvel

a) Sistema Operacional suportado para PC (Desktop)
   a. Windows: Windows 7 ou superior (x86/32 bits ou x86/64 bits)
   b. Linux (x86/64 bits)
   c. OS X (x86/64 bits)

b) Sistema Operacional para dispositivos móveis
   a. Android 4.1.3 ou superior
   b. IOS 12.0 ou superior

c) Suporte a interfaces de Áudios
   a. Windows: WASAPI ou MME
   b. Linux: Pulse
   c. Android: OpenSL/ES e AAudio
   d. OS X: CoreAudio
   e. IOS: CoreAudio

d) Suporte a interfaces de vídeo
    a. Windows: DirectShow
    b. iOS: CoreMedia
e) Codecs de Áudio suportados: G.711, G.729, GSM, iLBC, Speex, G.722 e OPUS
f) Codecs de Vídeos suportados: H.264 e VP8
g) Funcionalidades de áudio:
    a. Cancelamento de eco acústico
    b. Controle de ganho automático
    c. Supressão de ruído e geração de ruído de conforto
    d. Buffer de Jitter adaptativo com compensação automática
    e. Mascará e ocultar perda de pacotes
    f. Detecção de atividade da voz
    g. Audioconferência para até 3 participantes
    h. Música em espera
    i. DTMF
h) Suporte a Recomendações associadas ao protocolo SIP (conforme item 7)
i) Suporte a comunicação segura via Open VPN, SRTP, ZRTP e/ou SIP/TLS
j) Características do softphone:
    a. Suporte a receber e realizar chamadas e vídeo chamadas
    b. Integração com catálogo telefônico externo via LDAP ou WebService
    c. Histórico das últimas 2.000 chamadas realizadas/recebidas
    d. Provisionamento e configuração do softphone via QRCODE

4. Descrição técnica do Softphone via Web

a) Browsers suportados
    a. Windows: Chrome, Edge e Firefox
    b. Linux: Chrome e Firefox
    c. OS X: Chrome, Safari e Firefox
b) Solução baseada em WebRTC
c) Codecs de Áudio suportados: G.711, G.729, GSM, iLBC, Speex, G.722 e OPUS
d) Codecs de Vídeos suportados: H.264 e VP8

e) Funcionalidades de áudio:
    a. Cancelamento de eco acústico
    b. Controle de ganho automático
    c. Supressão de ruído e geração de ruído de conforto
    d. Buffer de Jitter adaptativo com compensação automática
    e. Mascará e ocultar perda de pacotes
    f. Detecção de atividade da voz
    g. Conferência
    h. Música em espera
    i. DTMF
f) Suporte a Recomendações associadas ao protocolo SIP (conforme item 7)
g) Suporte a comunicação segura via OpenVPN, SRTP, ZRTP e/ou SIP/TLS
h) Características do softphone:
    a. Suporte a receber e realizar chamadas e vídeo chamadas
    b. Integração com catálogo telefônico externo via LDAP ou WebService
    c. Histórico das últimas 2.000 chamadas realizadas/recebidas
    d. Acesso via login/senha individual

5. Lista de todas as características do CAMBOX

1. Sistema de Menus na tela do telefone
2. Recebimento de Alarmes
3. Autenticação de Usuário
4. Atendente Eletrônica
5. Transferência de Chamada
6. CDR em BD Relacional (MySQL/ODBC)
7. Transferência em caso de ocupado
8. Transferência em caso de não atendimento
9. Monitoramento de Chamada
10. Estacionamento de Chamada
11. Filas de Chamada
12. Gravação de Chamadas
13. Roteamento de Chamadas (DDR, horário, filas etc.)
14. Transferência de Chamada

15. Chamada em Espera
16. Bina (Caller ID)
17. Bloqueio pelo Caller ID
18. DISA
19. Aplicação de Calling Card
20. Conferência ilimitada
21. Integração com BD
22. Unified Messaging
23. Distinctive Ring
24. Não Perturbe
25. Fax embutido integrado ao email
26. Flexible Extension Logic
27. Serviço de Diretório por voz
28. URA (Interactive Voice Response)
29. DAC - Agentes de Atendimento Locais Remotos
30. Macros
31. Música de Espera nos formatos: Wav, GSM e MP3
32. Flexible Mp3-based System
33. Predictive Dialer
34. Conversão de Protocolos (SIP-H.323- MGCP)
35. Suporte a Escritórios Remotos
36. Ramais em Roaming
37. Roteamento por Caller ID
38. Mensagens SMS
39. Transferência Supervisionada
40. Videoconferência
41. Text-to-Speech (via Festival)
42. Chamada a três
43. Relógio com Data e Hora faladas
44. Transcodificação
45. Conexão a VoIP Gateways
46. Correio de Voz Integrado ao email

47. Indicador visual ou sonoro de Nova Mensagem
48. Grupos de Correio de Voz
49. Interface Web
50. Computer-Telephony Integration
51. Gerenciamento das Chamadas pela Web
52. Acesso a BDs durante as Chamadas
53. Interface de Gerência via TCP/IP
54. Escalabilidade:
    a. Via TDMoE
    b. Conexão Direta de vários PABX
    c. Latência Zero
    d. Usa hardware Ethernet Comum
55. Voice-over IP:
    a. Reduz Custos de Interurbanos
    b. Integra PABX de locais remotos
    c. Usa conexões normais de dados
    d. Dialplan integrado para vários locais
56. Codecs de áudio
    a. G.711 PCMU
    b. G.711 PCMA
    c. G.722
    d. GSM
    e. G.729
    f. OPUS
    g. ILBC
    h. G.723
    i. G.726
    j. Speex
57. Codecs de Vídeo
    a. H.263
    b. H.264

58. Protocolos Suportados
    a. DHCP
    b. DNS
    c. SNMP
    d. RTP/RTCP/SRTP: RFC 3550; RTCP-X; RTCP-XR
    e. SIP UDP/SIP TCP/SDP/SIP Seguro; RFC 3261; RFC 2976; RFC 3715; RFC 4028; RFC 2327; RFC 3264
    f. WebRTC
59. Integração
    a. Processos Organizacionais
    b. Web Service
    c. Base de Dados de ERP e/ou CRM
    d. Gestão Automática do Serviço
    e. Nativo para o fone@RNP

6. Características do Tarifador CAM

1. Multi linguagem (português do Brasil, inglês e Espanhol);
2. Não é um componente *core* de comunicação. Qualquer indisponibilidade do serviço de tarifação não afeta o sistema de comunicação;
3. Não perde o registro das chamadas mesmo que a comunicação entre o Tarifador e a Solução de Comunicação caia. Assim que a comunicação for restabelecida, o sistema é capaz de recuperar todos os registros não contabilizados;
4. Permite a conexão a múltiplos servidores PBX;
5. *Seguro* - Acesso seguro (HTTPS) com autenticação via Web a partir de qualquer navegador moderno (Google Chrome, Mozilla Firefox);
6. *Cloud ready* - Pode ser implantado em um ambiente de nuvem pública ou privada por ser implantado em um contêiner “Docker”;
7. Customização de tarifas de acordo com o local e operadora de saída (tronco);
8. Compatível com soluções Asterisk (e derivadas como Issabel 4);
9. Extrato de ligações em tempo real;
10. Extrato de ligações incompletas;
11. Emissão de relatórios de chamadas em PDF e Microsoft Excel (csv):
    a. Diário;

b. Diário/usuário;

c. Diário/tronco;

d. Mensal;

e. Mensal/usuário;

f. Mensal/tronco;

g. Por usuário;

h. Por tronco;

12. Licenciamento livre de limitações de usuário, servidores PBX ou tronco.

7. Lista de RFCs atendidas pelo PABX IP CAMBOX e softphone Web, Desktop ou Mobile

a) SIP

a. RFC 2976: The SIP INFO Method
b. RFC 3261: SIP: Session Initiation Protocol
c. RFC 3263: SIP: Locating SIP Servers
d. RFC 3313: Private SIP Extensions for Media Authorization (Partial)
e. RFC 3325: Private Extensions to SIP for Asserted Identity within Trusted Networks (Partial)
f. RFC 3326: The Reason Header Field for SIP
g. RFC 3329: Security Mechanism Agreement for SIP (Partial)
h. RFC 3428: SIP Extension for Instant Messaging
i. RFC 3515: SIP Refer Method
j. RFC 3581: rport An Extension to SIP for Symmetric Response Routing
k. RFC 3842: MWI A Message Summary and Message Waiting Indication Event Package for SIP
l. RFC 3891: SIP "Replaces" Header
m. RFC 3892: SIP Referred-By Mechanism
n. RFC 4028: Session Timers in SIP
o. RFC 4235: BLF (SIP dialog event package, partial support)
p. RFC 4320: Actions Addressing Identified Issues with SIP's Non-INVITE Transaction
q. RFC 4483: A Mechanism for Content Indirection in SIP Messages

r. RFC 4488: Suppression of SIP REFER Method Implicit Subscription
s. RFC 5589: SIP Call Control - Transfer
t. RFC 5922: Domain Certificates in the Session Initiation Protocol

b) Extensões do Protocolo SIP
   a. KPML
   b. SIMPLE/PUBLISH (SIP Presence)
   c. RFC 2278: A Model for Presence and Instant Messaging
   d. RFC 2779: Instant Messaging / Presence Protocol Requirements
   e. RFC 3856: A Presence Event Package for SIP
   f. RFC 3857: A Watcher Information Event Template-Package for SIP
   g. RFC 3859: Common Profile for Presence
   h. RFC 3863: PIDF: Presence Information Data Format
   i. RFC 3903: SIP Extension for Event State Publication
   j. RFC 4479: A Data Model for Presence
   k. RFC 4827: XCAP Usage for Manipulating Presence Document Contents
   l. RFC 5025: Presence Authorization Rules

c) SDP
   a. RFC 2327: SDP: Session Description Protocol
   b. RFC 3264: An Offer/Answer Model with SDP
   c. RFC 4566: SDP: Session Description Protocol

d) RTP
   a. RFC 1889: RTP: A Transport Protocol for Real-Time Applications obsolete
   b. RFC 2429: RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video H.263
   c. RFC 2435: RTP MJPEG, RTP Payload Format for JPEG
   d. RFC 2833: RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
   e. RFC 3550: RTP: Real-Time Protocol
   f. RFC 3551: RTP/AVP (audio and video profile)
   g. RFC 3555: RTP Payload Formats
   h. RFC 3952: RTP Payload Format for iLBC Speech

i. RFC 4629: H.263 RTP Payload Format

j. RFC 4733: RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals

k. RFC 5574: RTP Payload Format for the Speex Codec

e) Diversos

a. SRTP: RFC 4568: SDES: SDP Security Descriptions for Media Streams

b. ZRTP: RFC 6189: ZRTP: Media Path Key Agreement for Unicast Secure RTP

c. STUN: RFC 3489: STUN Simple Traversal of UDP Through NATs

8. Relatórios Estatísticos CAMBOX

Relatórios estatísticos baseados na utilização de cada serviço disponível, segregados diariamente por hora.

É possível efetuar o acesso e a impressão de todos os relatórios bem como a importação deles para planilhas eletrônicas do mercado através da rede interna ou internet.

➲ Relatórios básicos (analíticos e sintéticos):

- ✓ Chamadas atendidas;
- ✓ Chamadas abandonadas (sem as ligações que foram atendidas pela URA);
- ✓ Estatísticas de utilização por hora, dia e mês.
- ✓ Estatísticas para cada tipo de serviço oferecido pela Central de atendimento;
- ✓ Relatórios por TMA (Tempo Médio de Atendimento), por desempenho, bloqueio, login e outros (atendentes);
- ✓ Relatórios por TME (Tempo Médio de Espera em Fila).

9. Atendimento Omnichannel

Sistema de atendimento multicanal para plataformas de Whatsapp, Instagram, Facebook Messenger, Telegram e WebChat.

Funcionalidades inclusas:

- ✓ Auditoria de Atendimento
- ✓ Pesquisa de Satisfação
- ✓ Integração com ERPs
- ✓ Mensagem Modelo
- ✓ Gestão de usuários
- ✓ Atendimento Automático
- ✓ Tabulação de Atendimento
- ✓ Mensagem automática
- ✓ Gestão de Departamentos
- ✓ Mensagens Ilimitadas
- ✓ Relatórios de atendimentos

Sistema Telefônico Série P

Vá além com comunicações unificadas fáceis de usar.

Fácil de usar | Fácil de gerenciar | Fácil de integrar | Fácil de adotar | Fácil de expandir

Comunicações modernas impulsionando a produtividade empresarial

Focando em oferecer "Comunicações Unificadas Fáceis de Usar", o Sistema Telefônico Série P da Yeastar proporciona às empresas de todos os tamanhos um pacote completo para chamadas, vídeo, mensagens e integrações, pronto para uso.

Com gerenciamento visual de chamadas embutido, videoconferência integrada, recursos avançados de contact center e integrações prontas com SMS, WhatsApp, Microsoft Teams, CRMs e mais, o P-Series aumenta a produtividade em todos os níveis e oferece tudo em aplicativos simples para desktop, smartphone e navegador.

Disponível em Software e Cloud, a Série P oferece opções de implantação flexíveis, permitindo que a instale localmente ou na nuvem. Equilibrando custos e crescimento futuro, ele requer um menor custo total de aquisição, menos treinamento e menos esforços de gerenciamento, seja fazendo uma transição de sistema telefônico ou começando do zero.

- **Mais que um Sistema:** Unifique PABX, central de atendimento, chat ao vivo, mensagens omnichannel, videoconferências e integrações de terceiros em uma solução simples.
- **Opções de Implantação Flexíveis:** Na nuvem, local ou híbrido, com mínima dificuldade de configuração.
- **Interoperabilidade Líder:** Suporte à auto-configuração de mais de 300 modelos de telefones populares e troncos SIP de mais de 130 Provedores de Serviços de Internet (ITSPs) em todo o mundo.
- **Administração Fácil:** Administração baseada em painel, permissões granulares, relatórios avançados e mais, tornando tudo simples.
- **Tranquilidade:** Altamente confiável e seguro, o Série P reduz ameaças de segurança, fraudes de tarifas e tempo de inatividade por meio de uma arquitetura robusta e segurança em múltiplas camadas.

Recursos

Basic Telephony		Enterprise	Ultimate
Call Routing	●	●	●
Call Forwarding	●	●	●
Call Parking / Pickup	●	●	●
Call Transfer (Attended/Blind)	●	●	●
Call Waiting	●	●	●
Call Flip/Switch	●	●	●
Call Recording[1]	●	●	●
Ring Group	●	●	●
Paging & Intercom	●	●	●
Caller ID	●	●	●
Dial by Name	●	●	●
Speed Dial	●	●	●
AutoCLIP	●	●	●
CID/DID-based Call Routing	●	●	●
Direct Inward/Outward Dialing	●	●	●
DNIS	●	●	●
DND (Do Not Disturb)	●	●	●
Custom Prompts	●	●	●
Distinctive Ringtone	●	●	●
Music on Hold	●	●	●
MOH Playlist & Streaming	●	●	●
CDR & Basic Call Reports	●	●	●
Business			
Call Operator Panel	●	●	●
Desk Phone Control (CTI)	●	●	●
Function Keys	●	●	●
Feature Code	●	●	●
BLF Support	●	●	●
Busy Camp-on	●	●	●
Business Hours & Holidays	●	●	●
Boss-Secretary	●	●	●
Hot Desking	●	●	●
Emergency Calling	●	●	●
LDAP Server	●	●	●
TAPI Driver	●	●	●
Call Accounting		●	●

Unified Communications		Enterprise	Ultimate
Linkus UC Clients	●	●	●
- Web Client	●	●	●
- Mobile: iOS & Android	●	●	●
- Desktop: Windows & MacOS	●	●	●
- Google Chrome Extension	●	●	●
Presence & Custom Messages	●	●	●
Team Chat & File Sharing	●	●	●
Audio Conferencing	●	●	●
T.38 Fax	●	●	●
Fax to Email	●	●	●
Voicemail	●	●	●
Voicemail to Email	●	●	●
Voicemail Transcription[2]	●	●	●
Group Voicemail	●	●	●
Personal & Company Contacts	●	●	●
Call Pop-up URL	●	●	●
Voicemail Announcement		●	●
Phonebooks		●	●
Video Calls & Conferencing			●
Door Phone Video Preview			●
Integration			
Open APIs	●	●	●
CRM & Helpdesk Integration Zoho CRM, Salesforce, HubSpot, Bitrix 24, Odoo, Zoho Desk, Zendesk		●	●
Messaging Channel SMS, WhatsApp, Facebook		●	●
Microsoft 365 Integration Teams, Outlook, Azure AD (Entra ID)		●	●
File Remote Archiving[3] Google Storage, Amazon S3, FTP, SFTP		●	●
Database Contacts Sync Microsoft SQL		●	●
Active Directory Integration			●
Linkus SDKs			●
Hotel PMS Integration[4]	Optional	Optional	Optional

Advanced Business	Enterprise	Ultimate
Remote Access Service (FQDN)[5]	•	•
Remote SIP Service (WebRTC Trunk & Effortless Offsite SIP)[6]	•	•
Call Center		
IVR	•	•
Call Queue	•	•
Listen/Whisper/Barge Monitoring	•	•
Prority Queue & Acceleration	•	•
Queue Announcement	•	•
Queue Call Logs	•	•
Missed Call Disposition	•	•
Queue Callback	•	•
Skill-based Routing	•	•
Queue Panel	•	•
Wallboard	•	•
SLA Monitoring & Alerts	•	•
Post Call Survey	•	•
Call Center Reports	•	•
CRM & Helpdesk Integration	•	•
Live Chat & Messaging		
Live Chat (Chat & Call)	•	•
WhatsApp Integration	•	•
Facebook Integration	•	•
SMS & MMS Integration	•	•
Central Inbox & Message Queue	•	•
External Call Logs	•	•

Administration	Enterprise	Ultimate
Web Admin Portal	•	•
Real-time Dashboard	•	•
Extension Group & Organization	•	•
User Role & Permission	•	•
IP Phone Auto Provisioning	•	•
Headset Integration	•	•
SIP Forking	•	•
PIN List	•	•
Event Logs & Notficatoins	•	•
Troubleshooting	•	•
Backup and Restore	•	•
Built-in SMTP Server	•	•
AMI (Asterisk Manager Interface)	•	•
Network Drive	•	•
SNMP Support	•	•
Hot Standby [7]	Optional	Optional
Disaster Recovery [8]		Optional
Security		
SRTP & TLS Call Encryption	•	•
Auto & Static Defense	•	•
Global Anti-hacking IP Blocklist	•	•
Allowed Country IP's & Codes	•	•
Call Allow/Block List	•	•
Outbound Call Frequency Restriction	•	•
Password Policy Enforcement	•	•
Two-factor Authentication (2FA)	•	•

Modo de Planejamento e Implantação

	Plano Enterprise	Plano Ultimate
Método de Implantação	Software, Nuvem	Software, Nuvem

1 **Gravação de chamadas:** O recurso de gravação de chamadas é gratuito na Edição Dispositivo e Software. Quanto à Edição Nuvem, cada instância de PABX vem com 500 minutos de gravação gratuitos e mais podem ser adquiridos adicionalmente, se necessário.

2 **Transcrição de Correio de Voz:** Requer integração com o Serviço Google Cloud Speech-to-Text.

3 **Arquivo Remoto de Arquivos:** Requer Plano Ultimate para a Edição em Nuvem; Requer Plano Enterprise para a Edição de Dispositivo e Software.

4 **Hotel Integração PMS:** Compatível com a Edição Software.

5 **Serviço de acesso remoto, serviço SIP remoto:** Como a Edição em Nuvem é intrinsecamente acessível de qualquer lugar, o Serviço de Acesso Remoto e o Serviço de SIP Remoto são apenas para a Edição de Appliance e Software.

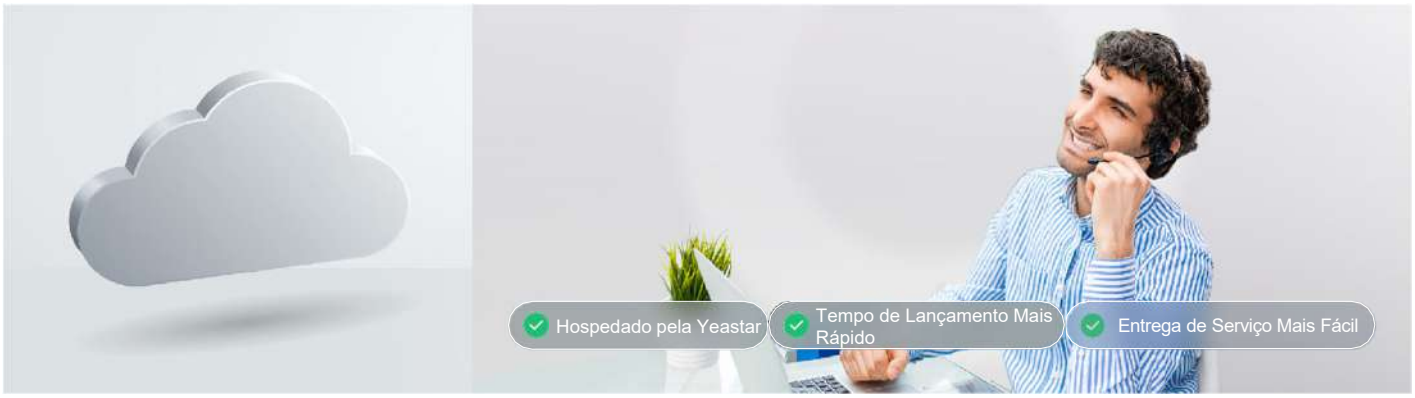
6 **Registro fácil de terminais SIP remotos:** Registre seus telefones IP remotos, PABXs de filiais, gateways VoIP e terminais SIP remotos semelhantes no PBX facilmente, como se estivessem implantados na intranet do seu PABX.

7 **Hot Standby:** Only supported by the Appliance and Software Edition. Requires an additional PBX redundancy server to function.

8 **Recuperação de Desastres:** Suportado pela Edição Software e requer um servidor de redundância de PABX adicional para funcionar.

Cloud Edition

O aumento do interesse em UCaaS está criando enormes oportunidades para MSP, VAR e outros parceiros de canal. O Yeastar Edição Série P Cloud oferece uma solução pronta para uso, permitindo que você inicie rapidamente o negócio de PABX na nuvem com apenas alguns cliques e sem configurar seu próprio servidor. Com custos iniciais e conhecimento técnico mínimos, você pode fornecer UCaaS de alto nível com confiança e manter a propriedade total dos clientes. Para os parceiros que buscam mais controle, a Edição Série P Cloud também suporta BYOI (Bring Your Own Infrastructure), permitindo que você hospede toda a plataforma de gerenciamento e fornecimento de serviços de UCaaS em sua própria nuvem.



Mude de CapEx para OpEx

Para aqueles que desejam evitar as complexidades da infraestrutura em nuvem, essa solução pronta para uso elimina o incômodo e o gasto inicial de configurar seus próprios servidores, reduzindo assim o risco de introduzir um novo serviço. Basta comprar pacotes de hospedagem através do Portal de parceiros da Yeastar e você estará pronto para vender aos clientes imediatamente.

No topo de uma arquitetura de alta disponibilidade

Com servidores redundantes para replicação em tempo real e failover contínuo, infraestrutura com balanceamento para a máxima utilização de recursos, SBC e outros mecanismos de segurança protegendo contra ataques maliciosos, não há necessidade de gastar tempo, esforço e despesas extras na manutenção e manutenção do ambiente de entrega.

Acelere a implementação do seu serviço

A Yeastar Central Management (YCM) é uma plataforma de fornecimento de serviço construída para esse propósito. São necessários alguns cliques para criar instâncias de PABX de diferentes recursos. Com diversos nós em todo o mundo, você pode selecionar servidores hospedados mais próximos de seus clientes e o PABX estará funcionando imediatamente, seja para atender a um pequeno número de usuários, ou mesmo a milhares.

Personalize e dimensione sob demanda

Como uma excelente oportunidade de crescimento, essa solução também permite que você crie seus próprios pacotes de serviços, agrupe telefones IP e outros hardwares, além de adicionar troncos SIP e outros serviços. Além disso, é fácil aumentar ou reduzir os serviços e atualizar os planos de assinatura para atender a diversas necessidades, o que, por sua vez, leva a um relacionamento mais sólido com o cliente.

Uma interface para conveniência operacional

Além de visualizar todas as instâncias de PABX e clientes em uma exibição de lista, você pode editá-los diretamente e criar tarefas para executar atualizações e outras operações automaticamente. As informações em tempo real de PABXs em nuvem, tarefas, alarmes e muito mais também são exibidas em um painel dinâmico baseado em widget para que você possa acompanhar rapidamente o andamento dos serviços.

Identifique problemas antes que os clientes o façam

Com a YCM monitorando automaticamente o status de todas as instâncias de PABX dos seus clientes, você recebe alertas instantâneos quando ocorrem ameaças, riscos relacionados à segurança ou qualquer outro problema crítico do sistema, podendo diagnosticá-los e solucioná-los rapidamente antes que afetem seus resultados. Isso garante um serviço mais contínuo, tirando muito peso de seus ombros.

Edição Software

Especificações gerais e requisitos do servidor

Edição de Software & Especificações Gerais			
Max. Extension	10,000	Operating System	Ubuntu 20.04 LTS, Debian 12
Max. Concurrent Calls	1000	Activation Method	Online /Offline Activation
Recommended Server Environmen	**On-premise**: VMware Workstation 15.1.0 or later; VMware ESXi 6.0 or later; Hyper-V 10.0.17134.1 or later; KVM; Proxmox VE 7.0 or later; Dell EMC PowerEdge; **Cloud**: Amazon Web Service (AWS); Microsoft Azure; Google Cloud; Amazon Lightsail; Digital Ocean; OVHcloud; HETZNER; Vultr, etc.		

Requisitos de ambiente virtual e de nuvem					
Extension Number (Concurrent Calls)	**1-20** (1-5)	**21-50** (6-13)	**51-250** (14-63)	**251-500** (64-125)	**501-1000** (126-250)
vCPU	2	2	4	6	8
CPU Frequency	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz	3.0 GHz
CPU Family	Intel i3 (Gen.8) or equivalent	Intel i3 (Gen.8) or equivalent	Intel i5 (Gen.8) or equivalent	Intel i7 (Gen.8) or equivalent	Intel Xeon E5 v4 or equivalent
Memory	2 GB	4 GB	4 GB	8 GB	16 GB
Storage (Call Recording Disabled)	40 GB	40 GB	50 GB	100 GB	200 GB
Storage (Call Recording Enabled)	Recommended: 1 TB The capacity requirement depends on your total recording volume, 1000 mins = 1GB				

Requisitos do servidor de nuvem					
Extension Number (Concurrent Calls)	**1-20** (1-5)	**21-50** (6-13)	**51-250** (14-63)	**251-500** (64-125)	**501-1000** (126-250)
vCPU	2	2	4	6	8
Memory	2 GB	4 GB	4 GB	8 GB	16 GB
Storage (Call Recording Disabled)	40 GB	40 GB	50 GB	100 GB	200 GB
Storage (Call Recording Enabled)	Recommended: 1 TB The capacity requirement depends on your total recording volume, 1000 mins = 1GB				

Requisitos de Servidor de Hardware			
Extension Number (Concurrent Calls)	**500-1000** (125-250)	**1001-2000** (251-500)	**2001-4000** (501-1000)
Recommended Server	Dell EMC PowerEdge R350	Dell EMC PowerEdge R350	Dell EMC PowerEdge R750
CPU	• CPU: Intel(R) Xeon(R) E-2374G • CPU Frequency: 3.70GHz • CPU Count: 1 • Cores: 4 • Threads: 8	• CPU: Intel (R) Xeon (R) E-2386G • CPU Frequency: 3.50GHz • CPU Count: 1 • Cores: 6 • Threads: 12	• CPU: Intel (R) Xeon (R) Gold 6346 • CPU Frequency: 3.10GHz • CPU Count: 2 • Cores: 16 • Threads: 32
Memory	16 GB	16 GB	32 GB
Hard Disk	1 TB	1 TB	1 TB

Para os requisitos de servidor para **PABX com mais de 1.000 chamadas simultâneas**, entre em contato com Yeastar para obter mais detalhes.

Yeastar

sales@yeastar.com
+86-592-5503301

Building C09, Software Park Phase III,
Xiamen 361024, Fujian, China

NIRE (DA SEDE OU DA FILIAL QUANDO A SEDE FOR EM OUTRA UF)

33.2.1235536-5

Tipo Jurídico

Sociedade empresária limitada

Porte Empresarial

Microempresa

Nº do Protocolo

2023/00977396-9

JUCERJA

Útimo arquivamento:
33212355365 - 07/12/2022
NIRE: 33.2.1235536-5
CAM TECNOLOGIA LTDA

Boleto(s):

Hash: 4E070085-0DFF-43B5-B77F-C463152D56BB

Orgão	**Calculado**	**Pago**
Junta	439,00	439,00
DNRC	0,00	0,00

TERMO DE AUTENTICAÇÃO

Nome

CAM TECNOLOGIA LTDA

Código Ato

002

Eventos

Cód	Qtde.	Descrição do Ato / Evento
021	1	Alteração / Alteração de Dados (Exceto Nome Empresarial)
xxx	xx	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxx	xx	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxx	xx	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxx	xx	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

CERTIFICO O DEFERIMENTO POR ANDRÉ RODRIGUES MARQUES DE SOUZA SILVA SOB O NÚMERO E DATA ABAIXO:

NIRE / Arquivamento	CNPJ	Endereço / Endereço completo no exterior	Bairro	Municipio	Estado
00005914907	14.438.757/0001-76	Avenida Pastor Martin Luther King Jr. 126	Del Castilho	Rio de Janeiro	RJ
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx
xxxxxxxxxxx	xx.xxx.xxx/xxxx-xx	xxxxxxxxxxxxxxxxxxxxxxx	xxxxxxxxxxxxxxxxxxx	xxxxxxxxxx	xx

Deferido em 30/11/2023 e arquivado em 30/11/2023

Gabriel Oliveira de Souza Voi
SECRETÁRIO GERAL

Nº de Páginas	Capa Nº Páginas
6	1/1

Observação:

Junta Comercial do Estado do Rio de Janeiro
Empresa: CAM TECNOLOGIA LTDA
NIRE: 332.1235536-5 Protocolo: 2023/00977396-9 Data do protocolo: 29/11/2023
CERTIFICO O ARQUIVAMENTO em 30/11/2023 SOB O NÚMERO 00005914907 e demais constantes do termo de autenticação.
Autenticação: 32D2F45CA1EA56B7148A3D149C402E43FAF96816FE748F4D22A547A9AE326F4B
Para validar o documento acesse https://www.jucerja.rj.gov.br/servicos/chanceladigital, informe o nº de protocolo.

JUCERJA assinado digitalmente

NIRE (DA SEDE OU DA FILIAL QUANDO A SEDE FOR EM OUTRA UF)

33.2.1235536-5

Tipo Jurídico

Sociedade empresária limitada

Porte Empresarial

Microempresa

Nº do Protocolo

2023/00977396-9 29/11/2023 12:16:31

JUCERJA

Último arquivamento:

33212355365 - 07/12/2022

NIRE: 33.2.1235536-5

CAM TECNOLOGIA LTDA

Boleto(s): 104556102

Hash: 4E070085-0DFF-43B5-B77F-C463152D56BB

Orgão	Calculado	Pago
Junta	439,00	439,00
DREI	0,00	0,00

REQUERIMENTO

Ilmo Sr. Presidente da Junta Comercial do Estado do Rio de Janeiro

CAM TECNOLOGIA LTDA

requer a v. sa o deferimento do seguinte ato:

Código do Ato	Código Evento	Qtde.	Descrição do ato / Descrição do evento
002	021	1	Alteração / Alteração de Dados (Exceto Nome Empresarial)
	xxx	xxx	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
	xxx	xxx	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
	xxx	xxx	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
	xxx	xxx	xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Requerente

Nome:	Rodrigo Villaça Gorgulho
Assinatura:	ASSINADO DIGITALMENTE O Requerente DECLARA, sob sua responsabilidade pessoal, sem prejuízo das sanções administrativas, cíveis e penais, a veracidade dos documentos e assinaturas apresentados no presente processo
Telefone de contato:	2122401780
E-mail:	rodrigo@unicon.rio
Tipo de documento:	Digital
Data de criação:	29/11/2023
Data da 1ª entrada:	

Rio de Janeiro

Local

29/11/2023

Data

2023/00977396-9

4ª Alteração Contratual
"CAM TECNOLOGIA LTDA"
CNPJ: 14.438.757/0001-76
Nire: 33212355365

Pelo presente instrumento particular, que entre si fazem,

THIAGO MALUF RESENDE, brasileiro, casado pelo regime de comunhão parcial de bens, Analista de Sistemas, nascido em 28/08/1985 portador da carteira de identidade n°11.321.458-9 expedida pelo DIC/RJ, inscrito no CPF sob o n°. 103.068.457-09, residente e domiciliado Rua Fortunato de Brito, 345 bloco 3 Apto 104 Freguesia - CEP: 22.750-300 – Rio de Janeiro – RJ.

na condição de titular da empresa **CAM TECNOLOGIA LTDA**, situada na Avenida Pastor Martin Luther King Jr, 126 BLC 9 Sal 408 Tor 2 Del Castilho CEP: 20765-000 – Rio de Janeiro- RJ, com seu ato constitutivo registrado na JUCERJA sob o Nire: 33212355365, resolve, na melhor forma de direito alterar o Contrato Social nas seguintes resoluções:

1) Alterar o objeto social para: 1- Desenvolvimento de programas de computador sob encomenda; 2- Suporte Técnico, análise, projeto, manutenção, gerencia de sistemas de informação e para internet; 3- Serviços de suporte e manutenção de máquinas e equipamentos, materiais de escritório e informática; 4- Treinamento em gestão da tecnologia da informação e telecomunicação; 5- Outros serviços em tecnologia da informação; 6- Comércio de produtos e equipamentos de informática e telecomunicações; 7- Representação Comercial de produtos em geral de informática e telecomunicações; 8- Aluguel de máquinas e equipamentos de informática e telecomunicações; 9- Serviços de comunicação multimídia – SCM; 10- Provedores de voz sobre protocolo internet – VOIP; 11- Serviços de telefonia fixa comutada – STFC.

2) Em virtude das modificações ora ajustadas, consolida-se o contrato social com a seguinte redação.

ATO CONSTITUTIVO
CAM TECNOLOGIA LTDA

CLÁUSULA PRIMEIRA

A sociedade empresária limitada tem a denominação de **CAM TECNOLOGIA LTDA.** Usará o nome fantasia **CAM TECNOLOGIA.**

CLÁUSULA SEGUNDA

A sociedade tem sua sede na Avenida Pastor Martin Luther King Jr, 126 BLC 9 Sal 408 Tor 2 Del Castilho CEP: 20765-000 – Rio de Janeiro- RJ, podendo abrir, manter e encerrar filiais, escritórios e repartições em qualquer localidade do país ou do exterior, por deliberação de quotistas representando a maioria do capital social.

CLÁUSULA TERCEIRA

O capital social, totalmente subscrito e integralizado é de R$ 100.000,00 (cem mil reais) dividido em quotas nominais e indivisíveis de R$ 1,00 (um real) cada uma, todas pertencentes ao sócio **THIAGO MALUF RESENDE**.

CLÁUSULA QUARTA

A sociedade tem por objeto específico: 1- Desenvolvimento de programas de computador sob encomenda; 2- Suporte Técnico, análise, projeto, manutenção, gerencia de sistemas de informação e para internet; 3- Serviços de suporte e manutenção de máquinas e equipamentos, materiais de escritório e informática; 4- Treinamento em gestão da tecnologia da informação e telecomunicação; 5- Outros serviços em tecnologia da informação; 6- Comércio de produtos e equipamentos de informática e telecomunicações; 7- Representação Comercial de produtos em geral de informática e telecomunicações; 8- Aluguel de máquinas e equipamentos de informática e telecomunicações; 9- Serviços de comunicação multimídia – SCM; 10- Provedores de voz sobre protocolo internet – VOIP; 11- Serviços de telefonia fixa comutada – STFC.

CLÁUSULA QUINTA

O prazo de duração da sociedade é indeterminado.

CLÁUSULA SEXTA

As cotas são indivisíveis e não poderão ser cedidas ou transferidas a terceiros sem o consentimento do outro sócio, a quem fica assegurado, em igualdade de condições e preço, direito de preferência para a sua aquisição, se postas a venda, formalizando, se realizada a cessão delas, a alteração contratual pertinente.

CLÁUSULA SÉTIMA

A responsabilidade de cada sócio é restrita ao valor de suas cotas, mas todos respondem solidariamente pela integralização do Capital Social.

CLÁUSULA OITAVA

A empresa será administrada pelo sócio **THIAGO MALUF RESENDE**, a quem caberá a representação ativa e passiva, judicial e extrajudicial da sociedade.

Parágrafo Único – O Administrador pode ser substituído, destituído e admitido a qualquer tempo, por ato apartado, sem necessidade de alteração contratual.

CLÁUSULA NONA

Ao término de cada exercício social, em 31 de dezembro de cada ano, o administrador prestará contas justificadas de sua administração, procedendo à elaboração do inventário, balanço patrimonial e do balanço de resultado econômico, cabendo aos sócios, na proporção de suas cotas, os lucros ou perdas apuradas.

CLÁUSULA DÉCIMA

Nos quatro meses seguintes ao término do exercício social, os sócios deliberarão as contas e designarão administrador, quando for o caso.

CLÁUSULA DÉCIMA PRIMEIRA

Os Sócios poderão de comum acordo, fixar uma retirada mensal, a título de Pró-Labore, em favor dos sócios administradores, observadas as disposições regulamentares pertinentes.

CLÁUSULA DÉCIMA SEGUNDA

Falecendo ou interditado qualquer sócio, a sociedade continuará suas atividades com os herdeiros sucessores e o incapaz. Não sendo possível ou inexistindo interesse destes ou dos sócios remanescentes, o valor de seus haveres será apurado e liquidado com base na situação patrimonial da sociedade, à data de resolução, verificada em balanço especialmente levantado, no prazo de 30 (trinta) dias contados a do evento, os quais serão pagos aos herdeiros, sucessores ou representante legal, da seguinte forma: 30% (trinta por cento) 30 (trinta) dias após a elaboração do Balanço Patrimonial e os outros 70% (setenta por cento) restantes em 10 (dez) parcelas mensais, iguais e sucessivas, vencendo-se a primeira 30 (trinta) dias após o pagamento da parcela inicial.

Parágrafo Único – O mesmo procedimento será adotado em outros casos em que a sociedade se resolva em relação a seu sócio.

CLÁUSULA DÉCIMA TERCEIRA

Declaração de Desimpedimento: Os sócios e Administrador, declaram sob as penas da Lei, de que não estão impedidos de exercer a administração da sociedade, pôr Lei especial ou em virtude de condenação criminal ou pôr se encontrar sob os efeitos dela, a pena que vede, ainda que temporariamente, o acesso a cargos públicos; ou pôr crime falimentar de prevaricação, peita ou suborno, concussão, peculato ou contra a economia popular, contra o sistema financeiro nacional, contra normas de defesa da concorrência, contra as relações de consumo, fé pública, ou a propriedade.

CLÁUSULA DÉCIMA QUARTA

A sociedade empresária limitada unipessoal declara, sob as penas da Lei, que se enquadra na condição de MICROEMPRESA, nos termos da Lei Complementar nº 123, de 14/12/2006.

CLÁUSULA DÉCIMA QUINTA

Fica eleito o foro da cidade do Rio de Janeiro - RJ para o exercício e o cumprimento dos direitos e obrigações resultantes deste contrato renunciando-se a qualquer outro pôr mais privilegiado que seja.

E, pôr estar em perfeito acordo em tudo, o quanto neste instrumento particular foi lavrado, obriga-se a cumpri-lo, tanto pôr si como seus herdeiros e sucessores, firmando-o em 01 (uma) via.

Rio de Janeiro, 05 de novembro de 2023.

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2023.11.09 16:00:26 -03'00'

THIAGO MALUF RESENDE

IDENTIFICAÇÃO DOS ASSINANTES

CERTIFICO QUE O ATO DA CAM TECNOLOGIA LTDA, NIRE 33.2.1235536-5, PROTOCOLO 2023/00977396-9, ARQUIVADO EM 30/11/2023, SOB O NÚMERO (S) 00005914907, FOI ASSINADO DIGITALMENTE.

CPF/CNPJ	Nome
071.012.347-71	RODRIGO VILLAÇA GORGULHO

30 de novembro de 2023.

Gabriel Oliveira de Souza Voi
Secretário Geral

REPÚBLICA FEDERATIVA DO BRASIL

CADASTRO NACIONAL DA PESSOA JURÍDICA

NÚMERO DE INSCRIÇÃO	COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL	DATA DE ABERTURA
14.438.757/0001-76 **MATRIZ**		**10/10/2011**

NOME EMPRESARIAL
CAM TECNOLOGIA LTDA

TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA)	PORTE
CAM TECNOLOGIA REDES E SERVICOS	**ME**

CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL
47.51-2-01 - Comércio varejista especializado de equipamentos e suprimentos de informática

CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS
47.52-1-00 - Comércio varejista especializado de equipamentos de telefonia e comunicação
61.10-8-01 - Serviços de telefonia fixa comutada - STFC
61.10-8-03 - Serviços de comunicação multimídia - SCM
61.10-8-99 - Serviços de telecomunicações por fio não especificados anteriormente
61.20-5-99 - Serviços de telecomunicações sem fio não especificados anteriormente
61.90-6-02 - Provedores de voz sobre protocolo internet - VOIP
61.90-6-99 - Outras atividades de telecomunicações não especificadas anteriormente
62.01-5-01 - Desenvolvimento de programas de computador sob encomenda
62.09-1-00 - Suporte técnico, manutenção e outros serviços em tecnologia da informação
63.11-9-00 - Tratamento de dados, provedores de serviços de aplicação e serviços de hospedagem na internet
77.33-1-00 - Aluguel de máquinas e equipamentos para escritórios
77.39-0-99 - Aluguel de outras máquinas e equipamentos comerciais e industriais não especificados anteriormente, sem operador
95.11-8-00 - Reparação e manutenção de computadores e de equipamentos periféricos

CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA
206-2 - Sociedade Empresária Limitada

LOGRADOURO	NÚMERO	COMPLEMENTO
AV PASTOR MARTIN LUTHER KING JR.	**00126**	**BLC 9 SAL 408 TOR 2**

CEP	BAIRRO/DISTRITO	MUNICÍPIO	UF
20.765-000	**DEL CASTILHO**	**RIO DE JANEIRO**	**RJ**

ENDEREÇO ELETRÔNICO	TELEFONE
CONTATO@CAMTECNOLOGIA.COM.BR	**(21) 3189-1050**

ENTE FEDERATIVO RESPONSÁVEL (EFR)
*****

SITUAÇÃO CADASTRAL	DATA DA SITUAÇÃO CADASTRAL
ATIVA	**10/10/2011**

MOTIVO DE SITUAÇÃO CADASTRAL

SITUAÇÃO ESPECIAL	DATA DA SITUAÇÃO ESPECIAL
********	********

Aprovado pela Instrução Normativa RFB nº 2.119, de 06 de dezembro de 2022.

Emitido no dia **08/10/2025** às **15:51:32** (data e hora de Brasília). Página: **1/1**

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Declaração

Declaramos para os fins exigidos na legislação, conforme documentação registrada no SICAF, que a situação do fornecedor no momento é a seguinte:

Dados do Fornecedor

CNPJ:	**14.438.757/0001-76**	DUNS®:	**90*****86**
Razão Social:	**CAM TECNOLOGIA LTDA**		
Nome Fantasia:	**CAM TECNOLOGIA REDES E SERVICOS**		
Situação do Fornecedor:	**Credenciado**	Data de Vencimento do Cadastro:	**01/12/2026**
Natureza Jurídica:	**SOCIEDADE EMPRESÁRIA LIMITADA**		
MEI:	**Não**		
Porte da Empresa:	**Micro Empresa**		

Ocorrências e Impedimentos

Ocorrência:	**Consta**
Impedimento de Licitar:	**Nada Consta**

Níveis cadastrados:

Automática: a certidão foi obtida através de integração direta com o sistema emissor. Manual: a certidão foi inserida manualmente pelo fornecedor.

I - Credenciamento

II - Habilitação Juridica

III - Regularidade Fiscal e Trabalhista Federal

Receita Federal e PGFN		Validade:	**14/04/2026**	**Automática**
FGTS		Validade:	**01/01/2026**	**Automática**
Trabalhista	**(http://www.tst.jus.br/certidao)**	Validade:	**09/06/2026**	**Automática**

IV - Regularidade Fiscal Estadual/Distrital e Municipal

Receita Estadual/Distrital	Validade:	**26/01/2026**
Receita Municipal	Validade:	**01/01/2026**

VI - Qualificação Econômico-Financeira

	Validade:	**30/06/2026**

Esta declaração é uma simples consulta e não tem efeito legal

CPF: 103.XXX.XXX-09 Nome: THIAGO MALUF RESENDE

Ass: _____

Secretaria de Estado de Fazenda

Sistema Integrado de Cadastro de Contribuintes do ICMS do Estado do Rio de Janeiro

Comprovante de Inscrição e de Situação Cadastral

CNPJ/CPF	Inscrição Estadual	Data da concessão da inscrição
14.438.757/0001-76	86.603.96-9	20/12/2013

Nome empresarial

CAM TECNOLOGIA LTDA

Título do estabelecimento

Natureza Jurídica	Tipo de unidade principal
Sociedade Empresária Limitada	Unidade Operacional
Regime de apuração	**Situação do Sublimite do Simples Nacional**
Simples nacional - Não Optante Simei	ICMS no Simples Nacional

Endereço do estabelecimento

AVENIDA Pastor Martin Luther King Jr., 126 BLC 9 SAL 408 TOR 2
DEL CASTILHO - RIO DE JANEIRO RJ 20.765-000

Situação cadastral	Data da situação cadastral
Habilitada	20/12/2013

Atividades econômicas (CNAE)

Principal

47.51-2/01 - COMÉRCIO VAREJISTA ESPECIALIZADO DE EQUIPAMENTOS E SUPRIMENTOS DE INFORMÁTICA

Secundárias

47.52-1/00 - COMÉRCIO VAREJISTA ESPECIALIZADO DE EQUIPAMENTOS DE TELEFONIA E COMUNICAÇÃO
61.10-8/01 - SERVIÇOS DE TELEFONIA FIXA COMUTADA - STFC
61.10-8/03 - SERVIÇOS DE COMUNICAÇÃO MULTIMÍDIA - SCM
61.10-8/99 - SERVIÇOS DE TELECOMUNICAÇÕES POR FIO NÃO ESPECIFICADOS ANTERIORMENTE
61.20-5/99 - SERVIÇOS DE TELECOMUNICAÇÕES SEM FIO NÃO ESPECIFICADOS ANTERIORMENTE
61.90-6/02 - PROVEDORES DE VOZ SOBRE PROTOCOLO INTERNET - VOIP
61.90-6/99 - OUTRAS ATIVIDADES DE TELECOMUNICAÇÕES NÃO ESPECIFICADAS ANTERIORMENTE
62.01-5/01 - Desenvolvimento de programas de computador sob encomenda
62.09-1/00 - SUPORTE TÉCNICO, MANUTENÇÃO E OUTROS SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO
63.11-9/00 - TRATAMENTO DE DADOS, PROVEDORES DE SERVIÇOS DE APLICAÇÃO E SERVIÇOS DE HOSPEDAGEM NA INTERNET
77.33-1/00 - ALUGUEL DE MÁQUINAS E EQUIPAMENTOS PARA ESCRITÓRIO
77.39-0/99 - ALUGUEL DE OUTRAS MÁQUINAS E EQUIPAMENTOS COMERCIAIS E INDUSTRIAIS NÃO ESPECIFICADOS ANTERIORMENTE, SEM OPERADOR
95.11-8/00 - REPARAÇÃO E MANUTENÇÃO DE COMPUTADORES E DE EQUIPAMENTOS PERIFÉRICOS

Unidade de cadastro	Tipo da Inscrição
AFR 64.12 - Capital	Contribuinte Pessoa Jurídica do RJ - obrigatória

Comprovante emitido nos termos da Resolução SEFAZ nº 720/2014, Parte II, Anexo I , em 04/04/2025 10:11:07.

Secretaria de Estado de Fazenda

Sistema Integrado de Cadastro de Contribuintes do ICMS do Estado do Rio de Janeiro

Comprovante de Inscrição e de Situação Cadastral

Observação

Contribuinte optante do Simples Nacional desde 20/12/2013. Em regra, documentos fiscais emitidos não geram crédito de ICMS.

Comprovante emitido nos termos da Resolução SEFAZ nº 720/2014, Parte II, Anexo I , em 04/04/2025 10:11:07.

Prefeitura da Cidade do Rio de Janeiro

Secretaria Municipal de Fazenda

FICHA DE INFORMAÇÕES CADASTRAIS (SUBSTITUI O CARTÃO DE INSCRIÇÃO MUNICIPAL)

INSCRIÇÃO MUNICIPAL	GRLF	DIV ISS	CPF/CNPJ	INÍCIO DE ATIVIDADE ECONÔMICA	DATA DE EMISSÃO	TIPO DE ESTABELECIMENTO
0533626-0	6	04	14438757000176	25/01/2012	05/07/2018	UNICO

NOME / FIRMA / RAZÃO SOCIAL
CAM TECNOLOGIA EIRELI ME

ENDEREÇO
Avenida Pastor Martin Luther King Jr., 00126, BLC 9 SAL 326 TOR 2, Del Castilho

CATEGORIA DO CONTRIBUINTE
FIRMA INDIVIDUAL C/ CNPJ

CÓDIGO E DESCRIÇÃO DE ATIVIDADES ECONÔMICAS (CAE)

2.26.64.5	GERAÇÃO DE PROGRAMAS DE COMPUTADOR SOB ENCOMENDA
2.17.17.4	ALUGUEL DE MÁQUINAS APARELHOS E EQUIPAMENTOS
2.26.45.9	PROCESSAMENTO DE DADOS
4.16.10.0	MAQUINAS E SUPRIMENTOS PARA PROCESSAMENTO DE DADOS - COMERCIO VAREJISTA
2.26.18.1	BUREAU DE SERV E CENTRO DE PROCESSAMENTO DE DADOS
2.10.43.9	INTERMEDIAÇÃO COMERCIAL
2.17.04.2	ALUGUEL DE MÁQUINAS PARA PROCESSAMENTO DE DADOS
2.17.03.4	ALUGUEL DE MÁQUINAS PARA ESCRITÓRIO
2.43.05.1	REPARAÇÃO DE MÁQUINAS DE PROCESSAMENTO DE DADOS
2.10.49.8	AGENCIAMENTO EM CONSIGNAÇÃO

CADASTRO DE SÓCIOS - 10 MAIORES PARTICIPAÇÕES

NOME: **THIAGO MALUF RESENDE**
PARTICIPAÇÃO: **0.00%**
IDENTIDADE: **113214589**
CPF/CNPJ: **10306845709**
QUALIFICAÇÃO: **Sócio/Diretor**
ENDEREÇO: **VINTE E QUATRO DE MAIO 859 AP 202 BL 1 ENGENHO NOVO RIO DE JANEIRO 20950091 RJ 105**

NOME:
PARTICIPAÇÃO:
IDENTIDADE:
CPF/CNPJ:
QUALIFICAÇÃO:
ENDEREÇO:

NOME:
PARTICIPAÇÃO:
IDENTIDADE:
CPF/CNPJ:
QUALIFICAÇÃO:
ENDEREÇO:

NOME:
PARTICIPAÇÃO:
IDENTIDADE:
CPF/CNPJ:
QUALIFICAÇÃO:
ENDEREÇO:

NOME:
PARTICIPAÇÃO:
IDENTIDADE:
CPF/CNPJ:
QUALIFICAÇÃO:
ENDEREÇO:

NOME:
PARTICIPAÇÃO:
IDENTIDADE:
CPF/CNPJ:
QUALIFICAÇÃO:
ENDEREÇO:

NOME:
PARTICIPAÇÃO:
IDENTIDADE:
CPF/CNPJ:
QUALIFICAÇÃO:
ENDEREÇO:

NOME:
PARTICIPAÇÃO:
IDENTIDADE:
CPF/CNPJ:
QUALIFICAÇÃO:
ENDEREÇO:

NOME:

PARTICIPAÇÃO:

IDENTIDADE:

CPF/CNPJ:

QUALIFICAÇÃO:

ENDEREÇO:

NOME:

PARTICIPAÇÃO:

IDENTIDADE:

CPF/CNPJ:

QUALIFICAÇÃO:

ENDEREÇO:

GOVERNO DO ESTADO DO RIO DE JANEIRO
SECRETARIA DE ESTADO DE FAZENDA

CERTIDÃO DE REGULARIDADE FISCAL Nº: 10-2025/3143482

Código de verificação de autenticidade: 512be8e74fff0d7e03785793b425c68f

CERTIDÃO NEGATIVA DE DÉBITOS - CND

IDENTIFICAÇÃO DO REQUERENTE	
Raiz de CNPJ: 14.438.757	CAD-ICMS: Ativo
RAZÃO SOCIAL: CAM TECNOLOGIA LTDA	

CERTIFICAMOS, para os fins de direito, e de acordo com as informações registradas nos Sistemas Corporativos da Secretaria de Estado de Fazenda e Planejamento, que, até a presente data,
NÃO CONSTAM DÉBITOS perante a RECEITA ESTADUAL para o requerente acima identificado, ressalvado o direito de a Receita Estadual cobrar e inscrever as dívidas de sua responsabilidade, que vierem a ser apuradas.

EMITIDA EM: 28/10/2025 ÀS 11:15:25

VÁLIDA ATÉ: 26/01/2026

Certidão emitida com base na Resolução SEFAZ nº 109 de 04/08/2017

OBSERVAÇÕES

De acordo com o § 2º, do Art. 3° da Resolução SEFAZ 109/2017, esta certidão abrangerá a regularidade fiscal de todos os estabelecimentos do requerente que possuam a mesma raiz de CNPJ, inscritos ou não no Cadastro de Contribuintes do ICMS do Estado do Rio de Janeiro.

Esta certidão deve estar acompanhada da Certidão Negativa da Dívida Ativa, emitida pelo órgão próprio da Procuradoria Geral do Estado, nos termos da Resolução Conjunta PGE/SER nº 33/2004.

A autenticidade desta certidão pode ser confirmada pela Internet (https://fisco-facil.fazenda.rj.gov.br/SATI-FiscoFacil/publico/autenticidadeHashCertidao/consultaAutenticidadeHash.xhtml).

A verificação de débitos é efetuada pelo CNPJ do requerente, abrangendo sua regularidade fiscal e de estabelecimentos que porventura possuir com mesma raiz de CNPJ. A razão social, quando indicada, é informação apenas ilustrativa.

O campo CAD-ICMS atesta a situação do CNPJ do requerente no Cadastro Estadual de Contribuintes do ICMS: ATIVO - estabelecimento inscrito e ativo; DESATIVADO - estabelecimento inscrito e desativado; NÃO INSCRITO - estabelecimento sem qualquer inscrição. No caso de estabelecimento inscrito no CAD-ICMS, sua identificação deverá ser obtida pelo Comprovante de Inscrição e de Situação Cadastral (www.fazenda.rj.gov.br).

A condição de não-inscrito ou desativado não desobriga o requerente de possuir inscrição ativa no Cadastro de Contribuintes do ICMS do Estado do Rio de Janeiro caso exerça atividade relacionada no artigo 20 do Anexo I da Parte II da Resolução SEFAZ nº 720/2014.

Procuradoria Geral do Estado do Rio de Janeiro

Procuradoria de Dívida Ativa (PG05)

Procuradoria de Dívida Ativa (PG05)

CERTIDÃO POSITIVA DE DÉBITOS EM DÍVIDA ATIVA, COM EFEITOS DE NEGATIVA.

Certifico, tendo em vista as informações fornecidas pelo Sistema da Dívida Ativa, que no período de 1977 até 29/10/2025, conforme solicitado no nos autos do procedimento administrativo n.º **SEI-140001/012663/2025,** por **CAM TECNOLOGIA LTDA ME** , CNPJ nº **14.438.757/0001-76**, **CONSTA(M) 01 DÉBITO(S)**, relacionado(s) à requerente, para empresas com mesmo Nome, CNPJ ou raiz de CNPJ corporificados nas inscrições listadas no relatório de pesquisa cadastral em anexo, extraído do Sistema da Dívida Ativa.

O(s) referido(s) débito(s) se encontra(m) na situação prevista no art. 4º da Resolução PGE nº 5002 de 23 de outubro de 2023, o que determina a expedição da presente certidão, nos termos do art. 206 do CTN em relação a tal(is) débito(s).

A presente certidão, lavrada em 01 (uma) lauda e 01 (uma) lauda(s) de anexo, todas com informações somente no anverso, tem validade de 180 (cento e oitenta) dias, conforme artigo 17 da Resolução nº 5002 de 23/10/2023.

Para maiores informações: https://pge.rj.gov.br/divida-ativa

Rio de Janeiro, 29 de outubro de 2025.

_____

PAOLO HENRIQUE SPILOTROS COSTA
Procurador Chefe da Procuradoria
da Dívida Ativa - PG-5

Documento assinado eletronicamente por **Gustavo Areal Pires**, **Procurador**, em 30/10/2025, às 12:00, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

R. do Carmo, 27, - Bairro Centro, Rio de Janeiro/RJ, CEP 20011-020
Telefone: (21) 2332-6015 - https://www.pge.rj.gov.br/

Voltar Imprimir

CAIXA ECONÔMICA FEDERAL

Certificado de Regularidade do FGTS - CRF

Inscrição: 14.438.757/0001-76

Razão Social: CAM TECNOLOGIA LTDA

Endereço: AV PASTOR MARTIN LUTHER KING JR 00126 BLC 9 SAL 408 / DEL CASTILHO / RIO DE JANEIRO / RJ / 20765-000

A Caixa Econômica Federal, no uso da atribuição que lhe confere o Art. 7, da Lei 8.036, de 11 de maio de 1990, certifica que, nesta data, a empresa acima identificada encontra-se em situação regular perante o Fundo de Garantia do Tempo de Servico - FGTS.

O presente Certificado não servirá de prova contra cobrança de quaisquer débitos referentes a contribuições e/ou encargos devidos, decorrentes das obrigações com o FGTS.

Validade:03/12/2025 a 01/01/2026

Certificação Número: 2025120317081875097464

Informação obtida em 11/12/2025 15:02:27

A utilização deste Certificado para os fins previstos em Lei esta condicionada a verificação de autenticidade no site da Caixa: **www.caixa.gov.br**

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO

CERTIDÃO NEGATIVA DE DÉBITOS TRABALHISTAS

Nome: CAM TECNOLOGIA LTDA (MATRIZ E FILIAIS)
CNPJ: 14.438.757/0001-76
Certidão nº: 64322045/2025
Expedição: 28/10/2025, às 10:54:46
Validade: 26/04/2026 - 180 (cento e oitenta) dias, contados da data de sua expedição.

Certifica-se que **CAM TECNOLOGIA LTDA (MATRIZ E FILIAIS)**, inscrito(a) no CNPJ sob o nº **14.438.757/0001-76**, **NÃO CONSTA** como inadimplente no Banco Nacional de Devedores Trabalhistas.
Certidão emitida com base nos arts. 642-A e 883-A da Consolidação das Leis do Trabalho, acrescentados pelas Leis ns.° 12.440/2011 e 13.467/2017, e no Ato 01/2022 da CGJT, de 21 de janeiro de 2022.
Os dados constantes desta Certidão são de responsabilidade dos Tribunais do Trabalho.
No caso de pessoa jurídica, a Certidão atesta a empresa em relação a todos os seus estabelecimentos, agências ou filiais.
A aceitação desta certidão condiciona-se à verificação de sua autenticidade no portal do Tribunal Superior do Trabalho na Internet (http://www.tst.jus.br).
Certidão emitida gratuitamente.

INFORMAÇÃO IMPORTANTE
Do Banco Nacional de Devedores Trabalhistas constam os dados necessários à identificação das pessoas naturais e jurídicas inadimplentes perante a Justiça do Trabalho quanto às obrigações estabelecidas em sentença condenatória transitada em julgado ou em acordos judiciais trabalhistas, inclusive no concernente aos recolhimentos previdenciários, a honorários, a custas, a emolumentos ou a recolhimentos determinados em lei; ou decorrentes de execução de acordos firmados perante o Ministério Público do Trabalho, Comissão de Conciliação Prévia ou demais títulos que, por disposição legal, contiver força executiva.

PREFEITURA DA CIDADE DO RIO DE JANEIRO
SECRETARIA MUNICIPAL DE FAZENDA
Coordenadoria do ISS e Taxas

Nº AUTENTICAÇÃO: 9937930327
ÓRGÃO: FP/REC-RIO/CIS/F
CONTROLE: 919612031

VALIDADE: 01/01/2026

CERTIDÃO DE REGULARIZAÇÃO DO IMPOSTO SOBRE SERVIÇOS DE QUALQUER NATUREZA

Nome: CAM TECNOLOGIA LTDA
CNPJ: 14.438.757/0001-76

A presente certidão, válida para todas as inscrições sediadas no Município do Rio de Janeiro, vinculadas aos oito primeiros dígitos do CNPJ ou CPF acima, serve como prova perante qualquer órgão público ou privado.

Esta certidão possui os **mesmos efeitos da certidão negativa**, por apontar créditos não vencidos, em curso de cobrança executiva em que tenha sido efetivada a penhora, ou cuja exigibilidade esteja suspensa, nos termos do Art 206 da Lei nº 5.172/1966 (Código Tributário Nacional).

Em relação ao contribuinte acima qualificado, consta(m) a(s) seguinte(s) ocorrência(s):

Débitos em Cobrança na Secretaria Municipal de Fazenda

Processo	AI/NL	Situação	Processo	AI/NL	Situação
043904892024	--------	PARCELAMENTO EM DIA			

Débitos em Cobrança na Procuradoria de Dívida Ativa da Procuradoria Geral do Município

Processo	Nº CDA	Situação	Processo	Nº CDA	Situação

Certidão emitida pela Internet - Em 3/10/2025 10:53:39

Certidão expedida com base na Resolução SMFP nº 3.390, de 29/11/2024.

Rio de Janeiro, 3 de OUTUBRO de 2025. Hora: 10:53

I - A autenticidade desta certidão deverá ser confirmada no portalCarioca Digital, no endereço carioca.rio.
II - O presente documento não certifica inexistência de débitos de ISS declarados pelo contribuinte no âmbito do Simples Nacional. Caso o contribuinte seja ou tenha sido optante pelo Simples nos últimos 5 (cinco) anos, a presente certidão deverá ser complementada por certidão de situação fiscal fornecida pela Receita Federal do Brasil.
III - A situação de cada CDA é retirada diretamente do sistema DAM da Procuradoria de Dívida Ativa da Procuradoria Geral do Município. Inconsistências relativas a essa situações devem ser questionadas junto àquele órgão.

Sistema Nacional de Registro de Empresas Mercantis - SINREM

GOVERNO DO ESTADO RIO DE JANEIRO

Governo do Estado do Rio de Janeiro
Secretaria Estadual de Desenvolvimento Econômico, Indústria, Comércio e Serviços
Junta Comercial do Estado do Rio de Janeiro

CERTIDÃO SIMPLIFICADA

Certidão Simplificada para Sociedades Empresárias, exceto as Anônimas, e suas filiais

Certificamos que as informações abaixo constam dos documentos arquivados nesta Junta Comercial e são vigentes na data da sua expedição.

Nome da empresa:
CAM TECNOLOGIA LTDA

Tipo Jurídico: Sociedade empresária limitada **Natureza Jurídica:** Sociedade Empresária Limitada

Número de Identificação do Registro de Empresas (NIRE)	CNPJ	Data de Arquivamento do Ato Constitutivo	Data de inícios das atividades
332.1235536-5	14.438.757/0001-76	10/10/2011	10/10/2011

Endereço:
AV Pastor Martin Luther King Jr., 126, BLC 9 SAL 408 TOR 2, Del Castilho, Rio de Janeiro, RJ, 20.765-000

Capital Social:	Prazo de Duração	Microempresa ou Empresa de Pequeno Porte
R$100.000,00 (CEM MIL REAIS)		
Capital Integralizado: 100.000,00 (CEM MIL REAIS)	Indeterminado	ME

Último Arquivamento:
Alteração/Alteração de Dados (Exceto Nome Empresarial)

Data	Número	Ato/eventos
30/11/2023	00005914907	002/021

Situação
Registro Ativo

Status
Transformada

Objeto:
MAQUINAS E SUPRIMENTOS PARA PROCESSAMENTO DE DADOS - COMERCIO VAREJISTA; APARELHOS DE TELECOMUNICAÇÃO-COMERCIO VAREJISTA; POSTAGEM E TELEGRAFIA, SERVIÇOS DE; TELEFONIA, SERVIÇOS DE; TELECOMUNICAÇÃO; GERAÇÃO DE PROGRAMAS DE COMPUTADOR SOB ENCOMENDA; CONSULTORIA TÉCNICA; PROCESSAMENTO DE DADOS; PROVIMENTO DE ACESSO E INFORMAÇÕES JUNTO À INTERNET; ALUGUEL DE MÁQUINAS PARA PROCESSAMENTO DE DADOS; ALUGUEL DE MÁQUINAS APARELHOS E EQUIPAMENTOS; REPARAÇÃO DE MÁQUINAS DE PROCESSAMENTO DE DADOS;

Atividades Econômicas:

- **4751201 Comércio Varejista Especializado de Equipamentos e Suprimentos de Informática**
- 9511800 Reparação e Manutenção de Computadores e de Equipamentos Periféricos
- 7739099 Aluguel de Outras Máquinas e Equipamentos Comerciais e Industriais não Especificados Anteriormente, sem Operador
- 7733100 Aluguel de Máquinas e Equipamentos para Escritório
- 6311900 Tratamento de Dados, Provedores de Serviços de Aplicação e Serviços de Hospedagem na Internet
- 6209100 Suporte Técnico, Manutenção e Outros Serviços em Tecnologia da Informação
- 6201501 Desenvolvimento de Programas de Computador Sob Encomenda
- 6190699 Outras Atividades de Telecomunicações não Especificadas Anteriormente
- 6190602 Provedores de Voz Sobre Protocolo Internet - Voip
- 6120599 Serviços de Telecomunicações sem Fio não Especificados Anteriormente
- 6110899 Serviços de Telecomunicações por Fio não Especificados Anteriormente
- 6110803 Serviços de Comunicação Multimídia - Scm
- 6110801 Serviços de Telefonia Fixa Comutada - Stfc
- 4752100 Comércio Varejista Especializado de Equipamentos de Telefonia e Comunicação

Sócios:

THIAGO MALUF RESENDE
CPF/CNPJ: 103.068.457-09 Participação no capital: 100.000,00
Condição: Sócio

THIAGO MALUF RESENDE
CPF/CNPJ: 103.068.457-09 Participação no capital: 0,00
Condição: Administrador

Filial(ais) nesta Unidade da Federação ou fora dela:
NIRE: XXXXXXX CNPJ: XXXXXXX XXXXXXX

Observações:

Sistema Nacional de Registro de Empresas Mercantis - SINREM

GOVERNO DO ESTADO RIO DE JANEIRO

Governo do Estado do Rio de Janeiro
Secretaria Estadual de Desenvolvimento Econômico, Indústria, Comércio e Serviços
Junta Comercial do Estado do Rio de Janeiro

CERTIDÃO SIMPLIFICADA

Certidão Simplificada para Sociedades Empresárias, exceto as Anônimas, e suas filiais

Certificamos que as informações abaixo constam dos documentos arquivados nesta Junta Comercial e são vigentes na data da sua expedição.

Ordens Judiciais:

Número: xxx **Data:** xx/xx/xxxx **Protocolo** xx-xxxx/xxxxxx-x

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Nomes Anteriores:

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Atos Arquivados:

CERTIFICO A EXISTÊNCIA DE TODOS OS ATOS ARQUIVADOS ATÉ A PRESENTE DATA:

07/12/2022 - 33212355365 - 002 - 30/11/2023 - 00005914907 - 002 -

Art.1029 - Notificação de Retirada:

CPF/CNPJ: xxxxxxxxx-xx **Participação no capital:** R$ 0,00
Condição: xxxxxxxxxxxxxxxxxxxx **Data da Notificação:** xx/xx/xxxx

Liquidante:

CPF/CNPJ: xxxxxxxxx-xx **Participação no Capital:** 0.00
Condição: xxxxxxxxxxxxxxxxxxxx

2025/00703346-5

Local, data
Rio de Janeiro, 11 de Julho de 2025

Gabriel Oliveira de Souza Voi
SECRETÁRIO GERAL - JUCERJA

Documento Assinado por meio digital, conforme MP 2200-2 de 24/08/2001, que institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP Brasil, em vigor consoante E.C nº32 de 11/09/2001 - Art.2º.
Art 1º. Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP Brasil, para garantir autenticidade, integridade e validade jurídica de documentos em forma

PREFEITURA DA CIDADE DO RIO DE JANEIRO
Procuradoria Geral do Município
Procuradoria da Dívida Ativa

Código de Controle

BCC8191MCC

CERTIDÃO NEGATIVA

Ressalvado o direito de o Município do Rio de Janeiro cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo identificado neste documento que vierem a ser apuradas, A PROCURADORIA DA DÍVIDA ATIVA DO MUNICÍPIO DO RIO DE JANEIRO, após analisar o cadastro dos créditos sob sua administração, relativamente a **CAM TECNOLOGIA LTDA** , inscrito(a) no cadastro nacional de pessoas jurídicas - CNPJ sob o nº 14.438.757/0001-76, inscrição municipal nº 0.533.626-0, com endereço no(a) AV PST MARTIN L K JR, nº 0 - RJ Cep: 20765-000, certifica que

NÃO FORAM APURADAS INSCRIÇÕES EM DÍVIDA ATIVA

Observações Complementares

Esta certidão compõe-se de 1 folha(s) e é válida por 120 dias, a contar desta data.

Observações

Rio de Janeiro, RJ, 13/10/2025

1. Esta certidão refere-se exclusivamente à situação fiscal do(s) contribuinte(s) acima indicado(s) perante a dívida ativa do Município do Rio de Janeiro.

2. A situação fiscal do(s) contribuinte(s) quanto a créditos não inscritos em dívida ativa deve ser certificada pelos órgãos responsáveis pelas respectivas apurações.

3. Esta certidão poderá ser renovada a partir de 27/01/2026. A certidão de situação fiscal é expedida no prazo de 10 dias, contados da data de seu requerimento perante a Procuradoria da Dívida Ativa . Não são aceitos pedidos de urgência.

4. O requerimento de certidão de situação fiscal perante a Procuradoria da Dívida Ativa pode ser feito pela própria pessoa física ou jurídica interessada, gratuitamente e sem a necessidade de nomeação de procurador.

5. Regularize sua situação fiscal imediatamente: efetue o pagamento ou parcelamento das dívidas apontadas nesta certidão, apresente os comprovantes de pagamento ou de início de parcelamento (originais, inclusive honorários, quando devidos) e obtenha em dois dias úteis sua certidão de situação fiscal regular.

6. O destinatário poderá confirmar a autenticidade desta certidão, informando o número do Código de Controle impresso acima no endereço **daminternet.rio.rj.gov.br**

7. A certidão é valida para matriz e filial(is).

Diogo Henriques Ferreira Mendes
Procurador-Chefe
Procuradoria da Dívida Ativa
Mat. 11/297.773-4

MINISTÉRIO DA FAZENDA
Secretaria da Receita Federal do Brasil
Procuradoria-Geral da Fazenda Nacional

CERTIDÃO POSITIVA COM EFEITOS DE NEGATIVA DE DÉBITOS RELATIVOS AOS TRIBUTOS FEDERAIS E À DÍVIDA ATIVA DA UNIÃO

Nome: CAM TECNOLOGIA LTDA
CNPJ: 14.438.757/0001-76

Ressalvado o direito de a Fazenda Nacional cobrar e inscrever quaisquer dívidas de responsabilidade do sujeito passivo acima identificado que vierem a ser apuradas, é certificado que:

1. constam débitos administrados pela Secretaria da Receita Federal do Brasil (RFB) com exigibilidade suspensa nos termos do art. 151 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional (CTN), ou objeto de decisão judicial que determina sua desconsideração para fins de certificação da regularidade fiscal, ou ainda não vencidos; e

2. constam nos sistemas da Procuradoria-Geral da Fazenda Nacional (PGFN) débitos inscritos em Dívida Ativa da União (DAU) com exigibilidade suspensa nos termos do art. 151 do CTN, ou garantidos mediante bens ou direitos, ou com embargos da Fazenda Pública em processos de execução fiscal, ou objeto de decisão judicial que determina sua desconsideração para fins de certificação da regularidade fiscal.

Conforme disposto nos arts. 205 e 206 do CTN, este documento tem os mesmos efeitos da certidão negativa.

Esta certidão é válida para o estabelecimento matriz e suas filiais e, no caso de ente federativo, para todos os órgãos e fundos públicos da administração direta a ele vinculados. Refere-se à situação do sujeito passivo no âmbito da RFB e da PGFN e abrange inclusive as contribuições sociais previstas nas alíneas 'a' a 'd' do parágrafo único do art. 11 da Lei nº 8.212, de 24 de julho de 1991.

A aceitação desta certidão está condicionada à verificação de sua autenticidade na Internet, nos endereços <http://rfb.gov.br> ou <http://www.pgfn.gov.br>.

Certidão emitida gratuitamente com base na Portaria Conjunta RFB/PGFN nº 1.751, de 2/10/2014.
Emitida às 10:20:38 do dia 13/10/2025 <hora e data de Brasília>.
Válida até 11/04/2026.
Código de controle da certidão: **E90C.767A.F0A8.832C**
Qualquer rasura ou emenda invalidará este documento.

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa CAM TECNOLOGIA EIRELI ME, situada na Avenida Pastor Martin Luther King Júnior, nº 126, Torre 2000, sala 326, no Bairro de Del Castilho, Rio de Janeiro/RJ, CEP nº 20.765-000, inscrita no CNPJ 14.438.757/0001-76, atendeu-nos a contento, não havendo nada que a desabone a Prestação do Serviço de Locação dos seguintes equipamentos:

- *02 unidades de PABX IP – CAMBOX físico com suporte para até 500 (quinhentos Ramais) com função de High Availability*
- *321 unidades de aparelhos telefônicos IP Grandstream GXP 1610*
- *01 Unidade de Concentrador Ótico GPON Mikrotik CCR1072*
- *65 Unidades do Modem Ótico GPON Fiberhome FD511*

A prestação de serviço contemplou a instalação, configuração dos mesmos, suporte e treinamento VOIP com foco em Protocolo SIP, SIPS, RTP, SRTP e UDP; conceitos sobre CODEC, qualidade de voz, ASTERISK e Gateways de voz. O treinamento foi aplicado para 06 (seis) alunos, com duração de 20h e ministrado pelo instrutor Thiago Maluf Resende, em nossas dependências.

Agudos, 20 de Agosto de 2020

Matheus Lourenzoni Dias

SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
STO/DITEL/COINF/DTI/PF

ATESTADO DE CAPACIDADE TÉCNICA

A CAM TECNOLOGIA EIRELI ME,

O STO/DITEL/COINF/DTI/PF - Serviço Técnico Operacional, no âmbito da POLÍCIA FEDERAL, com sede em Brasília, no Endereço SAIS Quadra 7- Lote 23 Edifício DTI – Setor Policial Sul Brasília - DF, CEP nº 70610-902, CNPJ 00394494/0080-30, representado pelo senhor Joelson Murilo Coelho da Silva vem por meio desta atestar que a empresa CAM TECNOLOGIA EIRELI ME, situada na A. Pastor Martin Luther King Jr, 126, Torre 200, sala 326, no Bairro de Del Castilho, Rio de Janeiro/RJ, CEP nº 20.765-000 e inscrita no CNPJ 14.438.757/0001-76, atendeu-nos a contento, não havendo nada que a desabone no fornecimento de Central Telefônica IP, contendo Gateways físicos (14) e Virtual Machine (1), incluindo o serviço de instalação presencial e o treinamento sobre conceitos em telefonia IP e Central PABX IP, cumprido rigorosamente prazos de entrega e faturamento, de acordo com a Ordem de Fornecimento nº 400/2019 e *Pregão Eletrônico 07/2018.*

Brasília, 06 de Novembro de 2019.

Joelson Murilo Coelho da Silva
Agente de Telecomunicações - Mátricula 12.849
Chefe do STO/DITEL - Serviço Técnico Operacional

Referência: Processo nº 08206.002544/2019-20 SEI nº 12930330

SERVIÇO PÚBLICO FEDERAL
MSP - POLÍCIA FEDERAL
SETOR DE APOIO ADMINISTRATIVO - SAD/DTI/PF

EDITAL Nº 07/2018 - DTI/PF - CENTRAL TELEFÔNICA/2018-SAD/DTI/PF

Processo nº 08206.300573/2016-10

PREGÃO ELETRÔNICO Nº 07/2018
(Processo Administrativo n°08206300573201610)

Torna-se público, para conhecimento dos interessados, que a Polícia Federal, por meio do(a) Diretoria de Tecnologia da Informação e Inovação da Polícia Federal, sediada no SAIS Quadra 07, Lote 23, Edifício CGTI, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, **do tipo menor preço,** nos termos da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 5.450, de 31 de maio de 2005, da Instrução Normativa SLTI/MPOG nº 02, de 11 de outubro de 2010, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993, e as exigências estabelecidas neste Edital.

Data da sessão: 14/11/2018
Horário: 10h
Local: Portal de Compras do Governo Federal – www.comprasgovernamentais.gov.br

1. DO OBJETO

1.1. O objeto da presente licitação é a escolha da proposta mais vantajosa para a aquisição de software e equipamentos de Telefonia IP baseada em software livre, com o fim de ampliação e posterior substituição do atual sistema, incluindo o fornecimento e instalação dos equipamentos necessários conforme descrito no Termo de Referência, como também treinamento, implementação e configuração**,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será dividida em GRUPO 1 contendo oito itens, e itens 9, 10, 11 e 12, conforme tabela constante no item 4.1 do Termo de Referência, facultando-se ao licitante a participação em quantos grupos forem de seu interesse, devendo oferecer proposta para todos os itens que o compõem.

ITENS		Descrição	Quantidade
GRUPO 1	01	Central Telefônica IP/PABX IP com redundância (*Software*, baseado em *open source*, com suporte para mínimo de 4.000 ramais/usuários a ser instalado em VM - Virtual *Machine*) - Implantação, Configuração	01
	02	Gateway com 04 E1 - Implantação, Configuração	02
	03	Gateway com 02 E1, 04 FXO, 08 FXS - Implantação, Configuração	02
	04	Gateway com 02 E1 - Implantação, Configuração	08
	05	Gateway GSM 16 portas	01
	06	Gateway SBC	01
	07	Configuração dos intens 09, 10, 11 e 12	2370
	08	Treinamento	01
09		Aparelho Telefônico IP - Tipo 1	500
10		Aparelho Telefônico IP - Tipo 2	500
11		Aparelho Telefônico IP - Tipo 3	1300
12		Aparelho Vídeo Fone IP	70

2. DOS RECURSOS ORÇAMENTÁRIOS

2.1. As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento da União para o exercício de 2017, na classificação abaixo:

Gestão/Unidade: 0001

Fonte: TESOURO – RECURSOS ORDINARIOS

Programa de Trabalho: 06.122.2112.2000.0001

Elemento de Despesa: 3917

PI: PF99900AG18

3. DO CREDENCIAMENTO

3.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

3.2. O cadastro no SICAF poderá ser iniciado no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, com a solicitação de login e senha pelo interessado.

3.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4. O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema, ou ao órgão ou entidade responsável por esta licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

3.5. A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso.

4. DA PARTICIPAÇÃO NO PREGÃO.

4.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no §3º do artigo 8º da Instrução Normativa SLTI/MPOG nº 2, de 11.10.10.

4.2. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as, nos limites previstos da Lei Complementar nº 123, de 2006.

4.3. Não poderão participar desta licitação os interessados:

4.3.1. proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

4.3.2. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.3.3. que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

4.3.4. que estejam sob falência, concurso de credores, , em processo de dissolução ou liquidação;

4.3.5. entidades empresariais que estejam reunidas em consórcio;

4.4. Como condição para participação no Pregão, a licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:

4.4.1. que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;

4.4.1.1. a assinalação do campo “não” apenas produzirá o efeito de a licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que seja qualificada como microempresa ou empresa de pequeno porte;

4.4.2. que está ciente e concorda com as condições contidas no Edital e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no Edital;

4.4.3. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

4.4.4. que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

4.4.5. que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MPOG nº 2, de 16 de setembro de 2009.

5. DO ENVIO DA PROPOSTA

5.1. O licitante deverá encaminhar a proposta por meio do sistema eletrônico até a data e horário marcados para abertura da sessão, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas.

5.2. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

5.3. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

5.4. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.5. Até a abertura da sessão, os licitantes poderão retirar ou substituir as propostas apresentadas.

5.6. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

5.6.1. Valor unitário e total do item;

5.6.2. Marca;

5.6.3. Fabricante;

5.6.4. Descrição detalhada do objeto: indicando, no que for aplicável, o modelo, prazo de validade ou de garantia;

5.7. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

5.8. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.

5.9. O prazo de validade da proposta não será inferior a 60 (sessenta) dias**,** a contar da data de sua apresentação.

5.10. O licitante deverá declarar, para cada item, em campo próprio do sistema COMPRASNET, se o produto ofertado é manufaturado nacional beneficiado por um dos critérios de margem de preferência indicados no Termo de Referência.

6. DA FORMULAÇÃO DOS LANCES E DO JULGAMENTO DAS PROPOSTAS

6.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

6.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

6.2.1. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

6.2.2. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

6.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

6.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

6.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

6.5.1. O lance deverá ser ofertado pelo valor total do item ou grupo.

6.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

6.7. O licitante somente poderá oferecer lance inferior ao último por ele ofertado e registrado pelo sistema.

6.7.1. O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20) segundos e o intervalo entre lances não poderá ser inferior a três (3) segundos

6.8. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

6.9. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

6.10. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

6.11. Se a desconexão perdurar por tempo superior a 10 (dez) minutos, a sessão será suspensa e terá reinício somente após comunicação expressa do Pregoeiro aos participantes.

6.12. O Critério de julgamento adotado será o menor preço, conforme definido neste Edital e seus anexos.

6.13. A etapa de lances da sessão pública será encerrada por decisão do Pregoeiro. O sistema eletrônico encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado pelo sistema, findo o qual será automaticamente encerrada a recepção de lances.

6.14. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta e, na hipótese de desistência de apresentar outros lances, valerá o último lance por ele ofertado, para efeito de ordenação das propostas.

6.15. Encerrada a etapa de lances será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as licitantes qualificadas como microempresas ou empresas de pequeno porte, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentado pelo Decreto nº 8.538, de 2015.

6.16. Caso a melhor oferta válida tenha sido apresentada por empresa de maior porte, as propostas de licitantes qualificadas como microempresas ou empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da proposta ou lance de menor preço serão consideradas empatadas com a primeira colocada.

6.17. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

6.18. Caso a licitante qualificada como microempresa ou empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes qualificadas como microempresa ou empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

6.18.1. Quando houver propostas beneficiadas com as margens de preferência em relação ao produto estrangeiro, o critério de desempate será aplicado exclusivamente entre as propostas que fizerem jus às margens de preferência, conforme regulamento.

6.19. Para a aquisição de bens comuns de informática e automação, definidos no art. 16-A da Lei n° 8.248, de 1991, será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010.

6.19.1. Nas contratações de bens e serviços de informática e automação, nos termos da Lei nº 8.248, de 1991, as licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

6.20. Para produtos abrangidos por margem de preferência, caso a proposta de menor preço não tenha por objeto produto manufaturado nacional, o sistema automaticamente indicará as propostas de produtos manufaturados nacionais que estão enquadradas dentro da referida margem, para fins de aceitação pelo Pregoeiro.

6.20.1. Nesta situação, a proposta beneficiada pela aplicação da margem de preferência tornar-se-á a proposta classificada em primeiro lugar.

7. DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

7.1. Encerrada a etapa de lances e depois da verificação de possível empate, o Pregoeiro examinará a proposta classificada em primeiro lugar quanto ao preço, a sua exequibilidade, bem como quanto ao cumprimento das especificações do objeto.

7.2. Será desclassificada a proposta ou o lance vencedor com valor superior ao preço máximo fixado ou que apresentar preço manifestamente inexequível.

7.3. Considera-se inexequível a proposta que apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

7.4. O Pregoeiro poderá convocar o licitante para enviar documento digital, por meio de funcionalidade disponível no sistema, estabelecendo no “chat” prazo razoável para tanto, sob pena de não aceitação da proposta.

7.4.1. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, tais como marca, modelo, tipo, fabricante e procedência, além de outras informações pertinentes, a exemplo de catálogos, folhetos ou propostas, encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo Pregoeiro, sem prejuízo do seu ulterior envio pelo sistema eletrônico, sob pena de não aceitação da proposta.

7.4.1.1. O prazo estabelecido pelo Pregoeiro poderá ser prorrogado por solicitação escrita e justificada do licitante, formulada antes de findo o prazo estabelecido, e formalmente aceita pelo Pregoeiro.

7.5. Caso a proposta classificada em primeiro lugar tenha se beneficiado da aplicação da margem de preferência, o Pregoeiro solicitará ao licitante que envie imediatamente, por meio eletrônico, com posterior encaminhamento por via postal, o documento comprobatório da caracterização do produto manufaturado nacional, nos termos do Decreto n° 7.174/2010.

7.6. O licitante que não apresentar o documento comprobatório, ou cujo produto não atender aos regulamentos técnicos pertinentes e normas técnicas brasileiras aplicáveis, não poderá usufruir da aplicação da margem de preferência, sem prejuízo das penalidades cabíveis.

7.6.1. Nessa hipótese, bem como em caso de inabilitação do licitante, as propostas serão reclassificadas, para fins de nova aplicação da margem de preferência.

7.7. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

7.8. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “*chat*” a nova data e horário para a continuidade da mesma.

7.9. O Pregoeiro poderá encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.

7.9.1. Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

7.9.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.10. Sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

8. DA HABILITAÇÃO

8.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

8.1.1. SICAF;

8.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);

8.1.3. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php).

8.1.4. Lista de Inidôneos, mantida pelo Tribunal de Contas da União – TCU;

8.1.5. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

8.1.6. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

8.2. Os licitantes deverão apresentar a seguinte documentação relativa à Habilitação Jurídica, à Regularidade Fiscal e trabalhista:

8.3. **Habilitação jurídica:**

8.3.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

8.3.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

8.3.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

8.3.4. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

8.3.5. No caso de microempresa ou empresa de pequeno porte: certidão expedida pela Junta Comercial ou pelo Registro Civil das Pessoas Jurídicas, conforme o caso, que comprove a condição de microempresa ou empresa de pequeno porte, segundo determinado pelo Departamento de Registro Empresarial e Integração – DREI.

8.3.6. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

8.3.7. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

8.4. **Regularidade fiscal e trabalhista:**

8.4.1. prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

8.4.2. prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

8.4.3. prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

8.4.4. prova de inexistência de débitos inadimplidos perante a justiça do trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

8.4.5. prova de inscrição no cadastro de contribuintes estadual, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

8.4.6. prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante**;**

8.4.7. caso o fornecedor seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Estadual do domicílio ou sede do fornecedor, ou outra equivalente, na forma da lei;

8.4.8. caso o licitante detentor do menor preço seja qualificado como microempresa ou empresa de pequeno porte deverá apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, sob pena de inabilitação.

8.5. **Qualificação Econômico-Financeira**,

8.5.1. certidão negativa de falência expedida pelo distribuidor da sede da pessoa jurídica;

8.5.2. balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

8.5.2.1. No caso de fornecimento de bens para pronta entrega, não será exigido da licitante qualificada como microempresa ou empresa de pequeno porte, a apresentação de balanço patrimonial do último exercício financeiro. (Art. 3º do Decreto nº 8.538, de 2015);

8.5.2.2. no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

8.5.3. A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), resultantes da aplicação das fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

8.5.4. As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor estimado da contratação ou do item pertinente.

8.6. As empresas, deverão comprovar, ainda, a qualificação técnica, por meio de:

8.6.1. Comprovação de aptidão para o fornecimento de bens em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado, conforme previsto no item 10 do Termo de Referência, anexo I do edital.

8.7. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

8.8. Os documentos exigidos para habilitação relacionados nos subitens acima, deverão ser apresentados em meio digital pelos licitantes, por meio de funcionalidade presente no sistema (upload), no prazo de até **2 (duas) horas**, após solicitação do Pregoeiro no sistema eletrônico. Somente mediante autorização do Pregoeiro e em caso de indisponibilidade do sistema, será aceito o envio da documentação por meio do e-mail cpl.cti@dpf.gov.br. Posteriormente, os documentos serão remetidos em original, por qualquer processo de cópia reprográfica, autenticada por tabelião de notas, ou por servidor da Administração, desde que conferidos com o original, ou publicação em órgão da imprensa oficial, para análise, no prazo de **2 (dois) dias úteis**, após solicitação do pregoeiro por meio de funcionalidade no sistema.

8.8.1. Não serão aceitos documentos com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

8.9. Em relação às licitantes cadastradas no Sistema de Cadastro Unificado de Fornecedores – SICAF, o Pregoeiro consultará o referido Sistema em relação à habilitação jurídica, à regularidade fiscal e trabalhista conforme o disposto nos arts. 4º, caput, 8º, § 3º, 13 a 18 e 43, III, da Instrução Normativa SLTI/MPOG nº 2, de 11.10.10.

8.9.1. Também poderão ser consultados os sítios oficiais emissores de certidões, especialmente quando o licitante esteja com alguma documentação vencida junto ao SICAF.

8.9.2. Caso o Pregoeiro não logre êxito em obter a certidão correspondente através do sítio oficial, ou na hipótese de se encontrar vencida no referido sistema**,** o licitante será convocado a encaminhar, no prazo de 2 (duas) horas, documento válido que comprove o atendimento das exigências deste Edital, sob pena de inabilitação, ressalvado o disposto quanto à comprovação da regularidade fiscal das licitantes qualificadas como microempresas ou empresas de pequeno porte, conforme estatui o art. 43, § 1º da LC nº 123, de 2006.

8.10. A existência de restrição relativamente à regularidade fiscal não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

8.10.1. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

8.11. Caso a proposta mais vantajosa seja ofertada por licitante qualificada como microempresa ou empresa de pequeno porte, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

8.12. A não-regularização fiscal no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, com a reabertura da sessão pública.

8.13. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

8.14. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

8.15. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

8.16. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

9. DA REABERTURA DA SESSÃO PÚBLICA

9.1. A sessão pública poderá ser reaberta:

9.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

9.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

9.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

9.2.1. A convocação se dará por meio do sistema eletrônico (“chat”), e-mail, ou, ainda, fac-símile, de acordo com a fase do procedimento licitatório.

9.2.2. A convocação feita por e-mail ou fac-símile dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de 2 (duas) horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

10.1.1. ser redigida em língua portuguesa, digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

10.1.2. conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

10.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

10.2.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

11. DOS RECURSOS

11.1. Declarado o vencedor e decorrida a fase de regularização fiscal da licitante qualificada como microempresa ou empresa de pequeno porte, se for o caso, será concedido o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

11.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

11.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

11.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

11.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

11.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

12.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

12.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

13. DA GARANTIA DE EXECUÇÃO

13.1. O adjudicatário, no prazo de até 10 (dez) dias após a assinatura do Termo de Contrato ou aceite do instrumento equivalente, prestará garantia no valor correspondente a 5% (cinco por cento) do valor do Contrato, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 56 da Lei nº 8.666, de 1993, desde que cumpridas as obrigações contratuais.

13.1.1. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, até o máximo de 2% (dois por cento).

13.1.2. O atraso superior a 30 (trinta) dias autoriza a Contratante a promover a retenção dos pagamentos devidos à Contratada, até o limite de 5% (cinco por cento) do valor do contrato a título de garantia, a serem depositados junto à Caixa Econômica Federal, com correção monetária, em favor da Contratante.

13.2. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

13.2.1. prejuízos advindos do não cumprimento do objeto do contrato;

13.2.2. prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

13.2.3. as multas moratórias e punitivas aplicadas pela Contratante à Contratada;

13.3. A garantia em dinheiro deverá ser efetuada em favor da Contratante, na Caixa Econômica Federal, com correção monetária, em favor do contratante.

13.4. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

13.5. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

13.6. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

13.7. Será considerada extinta a garantia:

13.7.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

13.7.2. no prazo de três meses após o término da vigência, caso a Contratante não comunique a ocorrência de sinistros.

14. DO TERMO DE CONTRATO

14.1. Após a homologação da licitação, será firmado Termo de Contrato. O prazo de vigência da contratação é de 12 (doze) meses contados da assinatura do contrato prorrogável na forma do art. 57, § 1°, da Lei n° 8.666/93.

14.2. Previamente à contratação, a Administração promotora da licitação realizará consulta ao SICAF para identificar eventual proibição da licitante adjudicatária de contratar com o Poder Público.

14.2.1. A adjudicatária terá o prazo de até 10 (dez) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar o instrumento equivalente, conforme o caso, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

14.2.2. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite da Adjudicatária, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado ou aceito no prazo de 10 (dez) dias, a contar da data de seu recebimento.

14.3. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

14.4. Antes da assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração realizará consulta “on line” ao SICAF, bem como ao Cadastro Informativo de Créditos não Quitados – CADIN, cujos resultados serão anexados aos autos do processo.

14.4.1. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias, sob pena de aplicação das penalidades previstas no edital e anexos.

15. DO PREÇO

15.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

16. DA ENTREGA E DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

16.1. Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Termo de Referência.

17. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

17.1. As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência.

18. DO PAGAMENTO

18.1. O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir da data final do período de adimplemento a que se referir, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

18.2. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

18.3. O pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor competente na nota fiscal apresentada.

18.4. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

18.5. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

18.6. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

18.7. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

18.8. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

18.9. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

18.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

18.11. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante, não será rescindido o contrato em execução com a contratada inadimplente no SICAF.

18.12. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

18.12.1. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

18.13. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \qquad I = \frac{(6 / 100)}{365} \qquad I = 0,00016438$$

TX = Percentual da taxa anual = 6%

19. DAS SANÇÕES ADMINISTRATIVAS.

19.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

19.1.1. não aceitar/retirar a nota de empenho, ou não assinar o termo de contrato, quando convocado dentro do prazo de validade da proposta;

19.1.2. apresentar documentação falsa;

19.1.3. deixar de entregar os documentos exigidos no certame;

19.1.4. ensejar o retardamento da execução do objeto;

19.1.5. não mantiver a proposta;

19.1.6. cometer fraude fiscal;

19.1.7. comportar-se de modo inidôneo;

19.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

19.3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

19.3.1. Multa de até 10% (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante, conforme previsto no item 23 do Termo de Referência.

19.3.2. Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;

19.4. A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.

19.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

19.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

19.7. As penalidades serão obrigatoriamente registradas no SICAF.

19.8. As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

20. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

20.1. Até 02 (dois) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

20.2. A impugnação poderá ser realizada por forma eletrônica, pelo e-mail cpl.cti@dpf.gov.br, ou por petição dirigida ou protocolada no endereço SAIS Quadra 07 Lote 23 Edifício CGTI, no setor de Protocolo.

20.3. Caberá ao Pregoeiro decidir sobre a impugnação no prazo de até vinte e quatro horas.

20.4. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

20.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.

20.6. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

20.7. As respostas às impugnações e os esclarecimentos prestados pelo Pregoeiro serão entranhados nos autos do processo licitatório e estarão disponíveis para consulta por qualquer interessado.

21. DAS DISPOSIÇÕES GERAIS

21.1. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário pelo Pregoeiro.

21.2. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

21.3. A homologação do resultado desta licitação não implicará direito à contratação.

21.4. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

21.5. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

21.6. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

21.7. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

21.8. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

21.9. O Edital está disponibilizado, na íntegra, no endereço eletrônico cpl.cti@dpf.gov.br, e também poderão ser lidos e/ou obtidos no endereço SAIS Quadra 07 Lote 23 Edifício CGTI, nos dias úteis, no horário das 09:00 horas às 16:30 horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

21.10. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

21.10.1. ANEXO I - Termo de Referência

21.10.2. ANEXO II – Valores Máximos Admitidos para Contratação

21.10.3. ANEXO III – Minuta de Termo de Contrato

Brasília/DF, 31 de outubro de 2018

Willian Marcel Murad
Diretor de Tecnologia da Informação e Inovação
Polícia Federal

Documento assinado eletronicamente por **WILLIAM MARCEL MURAD**, **Delegado(a) de Polícia Federal**, em 31/10/2018, às 15:05, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.dpf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **8814684** e o código CRC **E0F6A787**.

Referência: Processo nº 08206.300573/2016-10 SEI nº 8814684

SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
SETOR DE APOIO ADMINISTRATIVO - SAD/CGTI/DLOG/PF

LICI. TERMO DE REFERÊNCIA Nº 4997378/2017-SAD/CGTI/DLOG/PF

Processo nº 08206.300573/2016-10

1. FUNDAMENTOS LEGAIS

1.1. A aquisição do objeto deste Termo de Referência tem amparo legal na Lei nº 10.520 de 17 de julho de 2002, publicada no DOU de 18 de julho de 2002, no decreto nº 5.450 de 31 de maio de 2005 – "Pregão Eletrônico" e subsidiariamente nas normas da Lei nº 8.666/93 e suas alterações.

1.2. O presente documento foi elaborado em consonância com o Plano Diretor de Tecnologia da Informação e com os princípios contidos nos instrumentos legais vigentes referentes a contratações no âmbito da Administração Pública Federal, notadamente, a Instrução Normativa n° 04, de 11 de setembro de 2014, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão.

1.3. Os Licitantes eventualmente interessados em participar deste certame licitatório deverão observar rigorosamente todas as especificações constantes do Termo de Referência e seus anexos.

1.4. Desse modo, o planejamento aqui descrito contém os elementos essenciais fixados nas referidas normas, descritos de forma a subsidiar a instrução do procedimento licitatório e a participação dos interessados em concorrer no certame.

2. DO OBJETO

2.1. O objeto deste Termo de Referência é aquisição de software e equipamentos de Telefonia IP baseada em software livre, com o fim de ampliação e posterior substituição do atual sistema, incluindo o fornecimento e instalação dos equipamentos necessários conforme descrito neste Termo de Referência, como também treinamento, implementação e configuração.

3. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

3.1. O atual sistema telefônico da Polícia Federal (PF) em Brasília é composto por 01 (uma) central telefônica de marca AASTRA ERICSSON, Modelo MD110, Versão TSW BC13, e 07 (sete) Módulos (LIMs) remotos, divididos em: LIM principal (SAS Quadra 2, Bloco A) e LIMs remotos (CGTI, INI, INC, SUDOESTE, DSG, ANP, SR/DF).

3.2. A versão de software utilizada no equipamento é antiga e não são mais comercializadas novas licenças, fato que impossibilita o aumento de ramais e acréscimo de novas funcionalidades. Com esta configuração, a PF se encontra com uma central telefônica desatualizada e com capacidade insuficiente para atender as demandas de comunicação por voz para novos servidores, novos Setores ou novas Unidades da PF em Brasília/DF.

3.3. A implantação do sistema de Telefonia IP, baseado em software livre, proporcionará uma significativa redução de custos, além de uma gestão mais ágil, segura e eficiente, com respostas rápidas às diversas demandas dos usuários. Ressalte-se ainda a melhor qualidade das ligações, a disponibilidade imediata de informações gerenciais para suporte à tomada de decisões, bem como outras inúmeras facilidades de comunicação não disponíveis no sistema atual, tais como conferência, escolha automática das rotas mais econômicas de ligações, entroncamento com unidades remotas, dentre outras.

3.4. Desta forma, a contratação dos serviços descritos neste termo visa assegurar as condições ideais de funcionamento do sistema de telefonia da PF possibilitando o acompanhamento da evolução tecnológica dos serviços de telecomunicações existentes no mercado.

4. ESPECIFICAÇÃO DO OBJETO

4.1. Relação de itens que compõem o Sistema de Telefonia IP:

GRUPO	ITEM	Descrição	Quantidade
01	01	Central Telefônica IP/PABX IP com redundância (*Software*, baseado em *open source*, com suporte para mínimo de 4.000 ramais/usuários a ser instalado em VM - Virtual *Machine*) - Implantação, Configuração	01

	02	Gateway com 04 E1 - Implantação, Configuração	02
	03	Gateway com 02 E1, 04 FXO, 08 FXS - Implantação, Configuração	02
	04	Gateway com 02 E1 - Implantação, Configuração	08
	05	Gateway GSM 16 portas	01
	06	Gateway SBC	01
	07	Configuração dos intens 09, 10, 11 e 12	2370
	08	Treinamento	01
02	09	Aparelho Telefônico IP - Tipo 1	500
03	10	Aparelho Telefônico IP - Tipo 2	500
04	11	Aparelho Telefônico IP - Tipo 3	1300
05	12	Aparelho Vídeo Fone IP	70

4.1.1. O quantitativo do item 01 corresponde à necessidade de um PABX IP com redudância.

4.1.2. O quantitativo dos itens 02, 03 e 04 equivalem as unidades da Polícia Federal onde serão instalados, inicialmente, de forma a garantir a sobrevivencia local, ou seja, 12 (doze), conforme item 4.1.24.

4.1.3. O quantitativo do item 05 e 06 refere-se as facilidades de acesso remoto e chamadas para celulares com rota de menor custo.

4.1.4. O quantitativo do item 07 correspodem a soma total dos aparelhos a serem instalados.

4.1.5. O quantitativo dos itens 09 ao 12 correspondem ao atendimento das demandas iminentes, de ampliação e expansão, quantitativo dos ramais ativos (existem atualmente 1700 ramais ativos), bem como dos aparelhos relativos à videoconferência atual.

4.1.6. A criação de GRUPO, se dá pelo motivo de que há necessidade de total compatibilidade das funcionalidades e padronização entre os itens que compõem cada grupo:

4.1.6.1. **ESPECIFICAÇÕES COMUNS AOS ITENS DO GRUPO 01:**

a) Sobrevivência local - SAS, com no mínimo as seguintes funcionalidades:

1. Encaminhamento de chamadas entrantes e saintes;
2. Transferência com e sem consulta;
3. Fallback automático de proxy;
4. Mínimo 03 portas de rede gigabit (100/1000 Mbps), que permita conecção com redes distintas;
5. Alimentação tipo Full Range 110-240 Vac – 50/60 Hz.
6. Garantia de fábrica de 3 anos;

b) Protocolos Voip:

1. SIP (Session Initiation Protocol) – RFC 3261;
2. Suporte a SIP sobre UDP e TCP
3. Configuração de porta SIP
4. Suporte a envio e recebimento de SIP OPTIONS para monitoramento de status(keep-alive)
5. RFC 2976 – The SIP INFO Method
6. RFC 3515 – The Session Initiation Protocol (SIP) REFER Method
7. RFC 4028 – Session Timers in the Session Initiation Protocol (SIP)
8. SDP (Session Description Protocol) – RFC 2327 e RFC 3264

c) Protocolos de Mídia VoIP:

1. RTP (Real-Time Transport Protocol) – RFC 3550
2. Configuração de porta RTP
3. RTCP (Real-Time Transport Control Protocol) – RFC 3550
4. Manipulação de número de destino (to) e número de origem (from)
5. Adição e remoção de x-headers

d) Processamento de Chamdas:

1. A quantidade de chamadas simultâneas deve ser igual a quantidade de
2. canais de voz solicitados
3. O número de canais DSPs (processadores digitais de sinal) deve ser igual
4. ao número de canais de voz
5. O equipamento ofertado deve possuir capacidade de processamento da
6. capacidade máxima de tráfego em qualquer situação, sem perda ou atraso na
7. comunicação
8. O equipamento deve possuir a capacidade de manusear no mínimo 200 CAPS (tentativas de chamadas por segundo)

e) Facilidades de Voz/Mídia:

1. Codecs:

- Devem ser implementados por DSP (Digital Signal Processor) em hardware
- Suporte a G.711 (a-law e u-law) e G.729 A/B
- Suportar priorização de codecs e auto-negociação
- Utilização independente por canal de voz
- Detecção de Atividade de Voz (Voice Activity Detection - VAD) com supressão de silêncio e geração de ruído de conforto em G.711 e G.729
- Geração de Ruído de Conforto (Comfort Noise Generation - CNG)
- Possuir buffer de jitter
- Cancelamento de eco de linha – Line echo canceller (LEC) ITU G.165/G.168 de 64ms 512 TAPS
- Detecção e geração de DTMF:
- In-band EIA/TIA-464B
- Out-of-band padrão RFC2833
- Detecção automática de tipo de chamada: voz, fax e modem.

f) Suporte a Fax:

1. Suporte fax T.30 Grupo 3
2. FoIP – Fax over IP:
3. G.711 Fax Pass-Through
4. Deverá desabilitar automaticamente a supressão de silêncio e o cancelamento de eco no canal utilizado para FAX
5. T.38 – Real-Time Fax over IP (Fax Relay)
6. Deverá suportar fallback para G.711 Fax Pass-Through caso ocorra falha na negociação do T.38.

g) Facilidades da Rede:

1. Ethernet mínimo de 3 interfaces Ethernet
2. Conector padrão RJ-45

3. Switch integrado de 8 portas para interligação de interfaces TDM. (KMG 3200)
4. IEEE 802.3 10Base-T / IEEE 802.3u 100Base-TX
5. Suporte a auto-negociação conforme padrão ANSI/IEEE 802.3 Nway
6. IPv4 (Internet Protocol – RFC 0791)
7. DNS (Domain Name System – RFC 1034)
8. Configuração de IP, máscara, DNS e gateway:
9. Estática
10. DHCP – RFC 2131
11. Redundância de rede através de DNS SRV
12. Suporte VLAN tagging IEEE 802.1Q
13. NAT / Suporte a Firewall:
14. Suporte a NAT (Network Address Translation) – RFC 1631
15. Suporte a travessia de NAT através de IETF STUN – RFC 3489
16. Pode ser usado para interligar diferentes redes
17. Configuração de IP externo
18. STUN

h) Facilidades de Segurança:

1. Encriptação de sinalização de chamada SIP com TLS (Transport Layer Security) – RFC 2246
2. Suporte a SIPS URI scheme
3. Encriptação de mídia com SRTP (Secure Real Time Protocol) – RFC 3711
4. Deverá suportar a encriptação em todos os canais simultaneamente
5. Suporte ao protocolo de troca de chaves SDES – RFC 4568
6. SIP Digest Authentication: implementação da RFC2617 - HTTP
7. Authentication: Basic and Digest Access Authentication conforme descrito na
8. RFC3261 capítulo 22
9. Register authorization
10. Prevenção de fraudes: bloqueio de chamadas por destino e origem
11. DoS/DDoS prevention
12. Topology hiding
13. SIP TLS
14. SRTP (SDES e DTLS)
15. ACL (whitelist e blacklist)
16. Malformed packet protection
17. Rogue RTP protection

i) Facilidades de Chamada:

1. Deve suportar a participação nos seguintes casos:
2. Retenção de chamada (Call Hold)
3. Chamada em espera (Call Waiting)
4. Desvio de chamadas incondicional, por não atendimento e por
5. ocupado (Call Forward)
6. Transferência com e sem consulta (Call Transfer)
7. Conferência a 3 (3-Way Conference Call)
8. Identificação do número chamador (Caller ID)
9. Habilitar e desabilitar identificação de chamador (Caller ID)
10. Detecção e geração de identificação de chamador (Caller ID)

j) Deve ser possível a programção dos seguintes tons (Tons de Chamdada de Andamento):

1. Tom de discagem – dial tone
2. Tom de ocupado – busy tone
3. Tom de chamada em espera – call waiting tone
4. Tom de congestionamento – congestion/reorder tone
5. Tom de retenção – holding tone

6. Tom de chamada – ringback tone

k) Plano de Numeração:

1. Suporte a numeração E.164
2. Suporte a planos de numeração pública e privada, definidas pelo usuário
3. Suporte a planos de discagem que permitam direcionar as ligações para
4. interfaces de telefonia diretamente conectadas, para outros gateways e para SIP Server
5. Possuir facilidades para manipulação da numeração, como reescrita de
6. números, códigos de escape e adição e remoção de prefixos.
7. Roteamento de chamadas com base no número discado, no número chamador, horário e priorização
8. Failover retry baseado nas causas das falhas utilizando routing scripting.
9. Possuir funcionalidades de balanceamento de carga em caso de instalação de mais de um equipamento.
10. Possuir limitação de chamadas simultâneas por rede

l) Administração:

1. Acesso remoto via Web(HTTP/HTTPS) com autenticação de usuário
2. Deverão ser fornecidos manuais de usuário e administrador em formato digital
3. Acesso remoto via Telnet, SSH ou através de software cliente com autenticação de usuário
4. Prover métodos para debug e diagnóstico do sistema, através da geração de arquivos ou mensagens de logs com conteúdo cuja interpretação não necessite de conhecimentos detalhados da arquitetura ou implementação interna do sistema.
5. Caso os arquivos ou mensagens de logs não sejam em texto plano, eles devem suportar serem abertos ou interpretados por softwares em ambiente Linux
6. Caso a abertura ou interpretação dos logs necessite de softwares proprietários estes deverão ser fornecidos sem custo adicional.
7. Atualização de firmware e backup das configurações para arquivo via FTP, TFTP, HTTP, HTTPS, DHCP ou BootP.

m) Monitoramento:

1. Suporte SNMP v.1/v.2c/v.3
2. Suporte à MIB II (SNMP)
3. Caso o equipamento trabalhe com MIBs proprietárias, estas deverão ser fornecida pelo fabricante.
4. Status do sistema via web
5. Status dos troncos e canais via web

n) Especificações Adicionais:

1. Suporte a contabilização de recursos (incluindo tráfego gerado e tempo de utilização), com o uso de monitoramento baseado em CDR (Call Detail Record) customizavel.
2. Geração de registros CDR, com suporte a exportação automática e envio para dos bilhetes para sistema centralizado.
3. Contadores de ligações por canal
4. Opções de download em arquivo CSV (compatível com Microsoft Excel)
5. Equipamento deve permitir integração com interface de monitoramento de telefonia utilizando RADIUS para coleta de CDR´s

o) Características Físicas:

1. Tipo "appliance".
2. Fonte de alimentação interna dual hot swap, que opere na faixa de 100 a 240 V / 60Hz
3. Base de processamento com 1 U de altura, 19” de largura
4. Módulos de expansão TDM com 1 U de altura.
5. Deve ser fornecido com todo o hardware e licenças de softwares, cabos e acessórios necessários para a sua montagem e operação de suas funcionalidades como requeridas nesta especificação.
6. Deverá conter LEDs de status para indicação de status dos seguintes itens:

- Indicador de energia
- Status/Alarme
- Indicador de status do Link/ACT
- Portas WAN / LAN

p) Obrigações, Conformidade e Certificações:

1. Deverá ser entregue com o último release de software disponível na data da aquisição
2. Deverá ser fornecida toda a documentação necessária para a administração, configuração e manutenção, juntamente com os equipamentos, em português ou inglês e sem restrições de tempo e uso
3. Deverá acompanhar manual de usuário em português, cabos,acessórios necessários a sua instalação e uso, e licenças de uso de software por tempo indeterminado
4. O suporte técnico na instalação e solução de problemas de hardware e/ou software com relação a possíveis incompatibilidades deverá ser prestado gratuitamente pelo fornecedor
5. Deve estar obrigatoriamente em conformidade com as normas técnicas brasileiras em vigor, controladas pela ANATEL – Agência Nacional de Telecomunicações, no que concerne a interligação com a rede pública de telefonia, devendo ser apresentado o respectivo Certificado de Homologação emitido pela ANATEL.

q) Os itens de 02 a 06 devem acompanhar sistema de nobreak de alimentação, com autonomia de no mínimo 02 (duas) horas.

4.1.6.2. **ESPECIFICAÇÕES COMUNS AOS ITENS DO GRUPOS 02 A 05:**

a) Características Físicas:

1. Fonte de alimentação automática, entrada 100-240 VCA;
2. 01 “path cord CAT 5E” na cor cinza ou preta, e com comprimento de 2,5 metros;
3. Deverá permitir o mínimo de dois ângulos de posições diferentes;
4. Compatibilidade com Headset Conector RJ 9, compatível com EHS;
5. Deverá ser compatível com o padrão IEEE 802.3af (POWER OVER ETHERNET – POE);
6. Suporte de parede.

b) Obrigações, Conformidade e Certificações:

1. Garantia de fábrica de 1 ano;
2. Possuir certificação da ANATEL.
3. Possuir manual em Português.

c) Os aparelhos dos itens 09, 10 e 11, respectivamente dos grupos 02, 03 e 04, deverão dispor da funcionalidade de captura dos pacotes na interface web para avaliação e debug das atividades de registro e realização da chamada dos mesmos.

4.1.7. **DETALHAMENTO E CARACTERÍSTICAS DO ITEM 01:**

4.1.7.1. Arquitetura:

a) Deverá ser 100% baseada em software livre, que também possua capacidade para atender a todo o projeto de telefonia VoIP sem permitir degradação na qualidade das ligações, mesmo nos momentos de pico;

b) A solução deverá prover disponibilidade de 99,999%. A infraestrutura proposta deverá ser **redundante** em VM (máquinas virtuais) oferecida pela contratante e um dos servidores deve suportar toda a carga de tráfego de voz do sistema sem degradação do serviço prestado, considerando que a infraestrutura da contratante, que esta fora do escopo deste edital, esteja disponível 100%.

c) Os dois controladores (servidores em máquinas virtuais) da Central Telefônica VoIP (Principal e Redundante) deverão apresentar as mesmas características funcionais e operarem de forma ativoativo, garantindo que na falha de um deles não interrompa o pleno funcionamento da solução, ou ocasione pausas no sistema para sincronismos de informações.

d) Em caso de indisponibilidade de um servidor, o outro servidor, automaticamente e transparentemente, deve assumir o processamento, sem interrupção das chamadas IP em curso, com toda a garantia de serviços redundantes em modo ativo-ativo. Caso um servidor falhe, a transação deve ser completamente transparente para os usuários, de modo que não haja uma degradação da rede com a solicitação de registro de todos os telefones.

e) Outra funcionalidade solicitada é a de no caso de falha do servidor primário, a solução possibilitar o administrador gerar mudanças ou atualizações nas configurações do sistema, de forma que, no reestabelecimento do servidor primário, as configurações realizadas no servidor secundário sejam mantidas.

f) O sistema deve permitir o registro simultâneo de ramais IP aos servidores principal e secundário, possibilitando a sobrevivência do ramal no caso de uma falha em um dos servidores ou na conectividade da rede.

g) Deverá permitir o funcionamento em topologias de múltiplas localidades (multi-site) integrando um único sistema distribuído.

h) O sistema, quando operante em topologia multi-site, deverá possuir gestão e configuração centralizada e distribuição de recursos, tais como: interfaces analógicas e digitais (E1, FXS, FXO, etc.), conferência (DSP), fonte de música em espera, comutação de chamadas local, armazenamento e atualização de firmwareem servidor da solução.

i) A Central Telefônica VoIP deverá atuar também como SIP Proxy Server em modo stateful e SIP Register Server, conforme RFC 3261, possibilitando o registro de gateways e roteamento de chamadas de qualquer entidade SIP (terminais SIP, gateways de qualquer fabricante, etc).

j) Deverá tratar toda a comutação entre dispositivos SIP, como usuários e gateways, sem que o payload passe pelo central (peer-to-peer), controlando apenas o registro e a sinalização entre os dispositivos.

k) A Contratante poderá utilizar a qualquer momento telefones e/ou softwares de qualquer fabricante integrados à Central Telefônica VoIP, incluindo smartphones, tablets, etc., desde que operem no protocolo SIP -RFC3261, mantendo no mínimo as funcionalidades de Comunicação de áudio e vídeo, Transferência, Conferência e Chamada em espera.

l) A solução deve implementar criptografia tanto da sinalização, através do protocolo TLS, quanto da media, através do protocolo SRTP.

m) Possibilitar que as chaves de criptografia do fluxo de voz sejam trocadas a cada chamada e sejam distribuídas através de um canal também criptografado.

n) Deverá possuir licenciamento centralizado permitindo ao usuário de ramal IP se registrar em qualquer ponto da rede para garantia de mobilidade e utilização de um único número de ramal.

o)

p) Conformidade do Sistema proposto com as normas técnicas brasileiras em vigor, editadas pela ANATEL – Agência Nacional de Telecomunicações e pela ABNT – Associação Brasileira Normas Técnicas, no que se refere a possuir características funcionais básicas e características técnico-operacionais para Centrais Telefônicas IP;

q) Deverá ser constituído de arquitetura IP com suporte à integração de telefonia TDM através de gateways integrados à solução, permitindo transparência de funcionalidades entre os ramais de diferentes tecnologias pertencentes ao mesmo sistema;

r) Deverá possuir, de forma integrada, comutação TDM e VoIP (Voz sobre IP);

s) Suportar cancelamento de eco segundo padrão G.165 ou G.168;

t) O Sistema de Telefonia IP deve funcionar utilizando **SIP** (Session Initiation Protocol - **RFC 3261**) como protocolo padrão;

u) A Central Telefônica IP deverá possibilitar a programação de grupos de linhas de troncos analógicas, através de simples configuração de seu software de sistema, sem acréscimo de hardwares, de forma que se possa configurar algumas linhas para só realizarem ou receberem ligações externas (unidirecionais), outras para receberem e realizarem ligações externas (bidirecionais), e outras para atuar como troncos executivos em aparelhos telefônicos IP;

v) Plano de numeração dos ramais compostos por no mínimo 4 (quatro) dígitos;

w) Acesso remoto com proteção por senha e outros mecanismos de segurança;

x) Permitir a seleção e encaminhamento de chamadas para diferentes operadoras de longa distância, com facilidade de supressão do código da operadora;

y) A desconexão das ligações deverá ser do tipo simples, ou seja, a ligação será desfeita pelo primeiro que repor o monofone no gancho, ou no caso de comunicação de dados, pela primeira porta que receber um código de desconexão;

z) Possuir sistema de proteção contra falhas que evite a perda de suas programações de controle e da base de dados utilizada em sua programação;

aa) A Central Telefônica IP, como um todo, deverá apresentar máxima confiabilidade de funcionamento, através de utilização de mecanismos e procedimentos de segurança adequados e garantir o sigilo absoluto das comunicações entre seus componentes internos.

ab) Deverá dispor de recursos capazes de fornecer interconexão com Rede Pública de Telefonia Comutada, Telefonia IP e roteamento com a rede WAN, fornecendo suporte de comunicação para a plataforma e comunicação de telefonia local;

ac) Suportar sinalizações de entroncamento MFC R2 digital, ISDN (RDSI) PRI e BRI, CAS, QSIG (ETSI), SIP e H.323;

ad) Permitir livre configuração de todos os recursos de telefonia, incluindo-se definição de plano de encaminhamento de chamadas, configurações de rotas, supressão de Código de Seleção de Prestadora - CSP, além de facilidades e permissões de usuários, através da interface web de gerenciamento e administração;

ae) Prever um Plano de Numeração transparente para o usuário, de modo que se indique o devido roteamento das chamadas telefônicas, sem intervenção dos usuários, mas permitindo critérios configuráveis;

af) Permitir configuração de rotas alternativas, isto é, em caso de falha na conexão com a rede corporativa os equipamentos deverão operar normalmente entre seus ramais e com acesso à rede pública de telefonia, devendo garantir ainda que telefones IP, localizados em redes remotas, continuem sua operação em caso de falha do circuito WAN;

ag) Interceptar e encaminhar, automaticamente, para a rota VoIP (caso exista) as chamadas realizadas utilizando-se Código de Seleção de Prestadora – CSP quando deveriam ter sido realizadas pela rede corporativa. Se, no momento do encaminhamento, todos os canais da rota estiverem ocupados ou com problemas que impeçam o devido encaminhamento, a chamada deverá cursar pela rede pública;

ah) Deverá possibilitar, para todas as interligações, a utilização de rota alternativa (caso exista), caso a rota principal esteja congestionada;

ai) Permitir a implantação de rotas com interfaces celulares (“troncos celulares”) para o encaminhamento de tráfego para as prestadoras de telefonia celulares contratadas. Em caso de indisponibilidade destas rotas, a chamada deverá cursar pela rede de telefonia fixa;

aj) Possuir capacidade para gerenciar e manusear todas as chamadas e funcionalidades previstas neste Termo, tanto para a sua capacidade inicial como para a capacidade final ofertada pela licitante, inclusive nos horários de maior movimento, sem degradação do serviço;

ak) Permitir o registro de ramais/terminais IP baseados no protocolo SIP, H.323 e IAX2;

al) Suportar SIP Trunk;

am) Suportar IAX2 Trunk;

an) Permitir registro de telefones através do protocolo DHCP;

ao) Permitir registro de telefones através da configuração de endereçamento IP ESTÁTICO;

ap) Permitir o bloqueio e/ou liberação do registro de ramais através do endereçamento de rede;

aq) Suportar a mobilidade de ramal por usuário de forma que o mesmo possa utilizá-lo em qualquer ponto de rede da estrutura interna desta Instituição;

ar) Permitir o bloqueio de chamadas para códigos de acesso compostos de no mínimo 8 dígitos. A inclusão de números não permitidos deverá ser realizada pelo administrador do sistema;

as) Permitir para todas as rotas a manipulação (inserção ou retirada de prefixos, substituição de dígitos, etc.) dos números de origem e de destino, alterando todos os campos do cabeçalho SIP;

at) Possuir agenda telefônica interna com no mínimo 500 (quinhentos) números cadastrados;

au) Suportar, os padrões de mercado de CODECs de compressão de voz G711, G711a, G.711µ, G729, G729a, e G722;

av) Suportar o envio de FAX através do padrão T.38 e recebimento de fax convertido para PDF e enviado por e-mail;

aw) Suportar cancelamento de eco;

ax) Suportar os CODECs H.263 ou H.264 ou outro padrão de compressão para vídeo;

ay) Suportar facilidade de DDR (Discagem Direta Ramal), sem uso de hardware externo adicional;

az) Suportar sinalização DTMF (RFC 2833);

ba) Suportar música de espera no padrão MP3 ou WAV, sem a necessidade de uso de hardwares externo adicional;

bb) Possuir interface WEB na qual disponibilizará acesso seguro (HTTPS) ao servidor a partir de qualquer ponto da rede. Através dessa interface o administrador do sistema poderá operar e configurar os softwares instalados no servidor. O acesso WEB deverá ser controlado mediante usuário e senha;

bc) Deverá permitir a configuração de backup automático das bases de dados, cuja periodicidade, hora de início e caminho de destino, inclusive unidade de rede mapeada, possa ser programada pelo administrador do sistema;

bd) Todas as funcionalidades requeridas neste Termo deverão ser implementadas utilizando o mesmo protocolo de sinalização entre o telefone IP e o IPBX, ofertados pela licitante;

be) A CONTRATANTE poderá utilizar a qualquer momento, telefones e/ou softwares de qualquer fabricante, integrados à SOLUÇÃO DE TELEFONIA, incluindo smartphones, tablets, etc., desde que operem no protocolo SIP – RFC 3261, mantendo no mínimo as seguintes funcionalidades:

1. Comunicação de áudio;
2. Transferência;
3. Conferência;
4. Chamada em espera.

bf) Open Source (Asterisk 1.8.18 ou superior);

bg) Suporte a Banco de Dados MySQL;

bh) Integração do Asterisk com banco de dados em realtime;

bi) Extensões SIP e IAX2;

bj) Interface web de Administração em PHP e JavaScript.

4.1.7.2. Plano de Numeração:

a) O PABX IP deverá exercer a função de Central Local – CL, para cursar os tráfegos originados e terminados entre os seus próprios ramais, entre estes e a Rede Pública, e entre estes e a rede WAN da unidade;

b) A PABX IP deverá possibilitar a implantação de um plano de numeração específico, de acordo com a faixa de DDR disponibilizada pela concessionária na localidade do campus e solicitação da unidade.

4.1.7.3. Interface Web de Administração contendo:

a) Cadastros de Ramais, Grupos e Filas de Atendimento;

b) Configurações específicas de filas: música de espera, estratégia de distribuição, máximo de ligações na fila, tempo máximo de toque para o operador, cadastro de membros das filas;

c) Cadastro dos Agentes;

d) Análise do CDR (Call detail record): Relatório de chamdas, Bilhetagem de chamadas por ramal, Relatórios Estatísticos, Estatísticas de utilização por ramal, Estatísticas de utilização por tronco ou grupo, Tráfego geral de chamadas por período (dia,hora e acompanhamento mensal), Exportação de relatório para CSV e PDF;

e) Gráficos: Utilização diária e ocupação por horário; Utilização Mensal; Taxa de ocupação de troncos;

f) Monitoramento: Monitoramento de Filas;

g) Painel de Monitoramento de Filas: operadores, chamadas em espera, tempos de espera, status de operadores;

h) Monitoramento de Status do Sistemas: Espaço em disco; Memória; Processamento; Usuários conectados; Versões de softwares principais;

i) Painel de Visualização de: Status Ramais; Status de Tronco; Status de Agentes; Status de Filas de Atendimento;

j) Configuração de áudios do Sistema: Configuração de Mensagens da URA de pré-atendimento; Gerenciamento de Músicas de Espera;

4.1.7.4. Funcionalidades Operacionais:

a) Bloqueio de chamdas conforme rementente, Bloquei de chamada a cobrar;

b) Transbordo de chamadas entre troncos;

c) Controle de Chamadas com senha;

d) Bloqueio de chamadas por rota;

e) Definição de categoria de ramal;

f) Chamada em espera;

g) Siga-me quando não atende;

h) Siga-me quando ocupado;

i) Siga-me;

j) Enfileiramento de chamadas;

k) Estacionamento de chamadas;

l) Identificação de chamadas;

m) Monitoramento de chamadas em curso;

n) Rediscagem automática;

o) Registro de Chamadas;

p) Roteamento de chamadas;

q) Toque diferencial por chamada;

r) Transferência Assistida de Chamadas;

s) Transferência cega;

t) Música de Espera;

u) Música de Transferência;

v) Captura de Chamadas;

w) Captura de chamadas por grupo;

x) Não perturbe;

y) Desvio de chamadas conforme horário.

4.1.7.5. Sistema integrado de Unidade de Resposta Audível de Pré - Atendimento (URA):

a) Atendimento Automatizado;

b) Distribuição de Chamadas para ramais;

c) Distribuição de Chamadas para filas;

d) Distribuição de Chamadas para grupos de ramais;

e) Permitir autoatendimento para que possam ser digitadas opções no atendimento eletrônico. Automatiza algumas ou todas as interações dos seus clientes, utilizando recursos de conversão de digito em voz (“text-to-speech”) integrados para obter informação do cliente e fazer a comparação com os sistemas de informação para, automaticamente, atender às questões e solicitações dos clientes.

f) Deverá possuir capacidade mínimo 30 canais;

g) Atendimento telefônico com menus e sub-menus;

h) Diferenciação de atendimento por períodos determinados por dia, hora ou canal de atendimento;

i) Armazenar frases digitalizadas em formato de alta qualidade;

j) Possibilitar a gravação de mensagens de voz em estúdio profissional;

k) Possibilitar a interrupção do menu de opções (Cut-Thru), caso o usuário conheça o passo seguinte;

l) Flexibilidade na implementação de novos serviços (customizações);

m) Possibilita transformar cada canal de atendimento em multi aplicações, tratando-os na estratégia determinada, distribuídas no tempo;

n) Ter modularidade que permite o crescimento do sistema de acordo com a demanda;

o) Comunicar-se com aplicações externas;

p) Fazer captura de dados;

q) Caixas postais, em quantidade ilimitada, para armazenamento de mensagens de voz;

4.1.7.6. Sistema integrado de Distribuição Automática de Chamadas (DAC):

a) Permitir que chamadas atendidas assim que elas chegam na fila de atendimento inteligentemente sejam direcionadas aos agentes disponíveis com base em: Número Discado pelo Cliente (“Dialed Number Identification Service” - DNIS), na Identificação do originador da chamada (“Automatic Number Identification” - ANI), agentes disponíveis, perfil do cliente, níveis de serviço ou regras de negócio definidas pelo usuário. O DAC também ajuda gerenciar redirecionamentos de transbordo, redirecionamento de chamadas baseado em estatísticas de fila, recuperação de chamadas abandonadas e encaminhamento de chamadas entre múltiplas localidades. O recurso de “Intelligent Network Routing” interliga múltiplas localidades, para tirar vantagem das estatísticas de tempo real, centralizadas permitindo reencaminhamento automático de chamadas de uma localidade para outra.

4.1.7.7. Permitir que as funcionalidades de URA e DAC possam ser utilizadas em conjunto para obter informações do cliente e encaminhar a chamada para o agente mais habilitado. Nas campanhas ativas via URA, a mesma disca para os clientes, toca mensagem para os mesmos assim que eles atenderem ao telefone, responde automaticamente algumas perguntas pré-definidas, e encaminha o cliente para um agente humano se necessário.

4.1.7.8. Salas de Conferência:

a) Salas de Conferência;

b) Salas privadas com senha;

c) Salas públicas.

4.1.7.9. Entroncamentos:

a) Suporte a entroncamento Digital TDM E1 com protocolo R2 ou ISDN;

b) Suporte a entroncamento VoIP SIP;

c) Suporte a entroncamento VoIP IAX2;

d) Suporte a entroncamento TDM GSM;

e) Suporte a entroncamento TDM analógico;

f) Suporte a entroncamento VoIP H.323;

g) O sistema deve permitir criação de troncos Digitais, Analógicos, GSM e VoIP;

h) O sistema deve permitir total integração com equipamentos GATEWAYS (com interface Digital, Analógica ou GSM) através do protocolo SIP ou através de drivers do equipamento devidamente fornecidos pelos fabricantes ou disponibilizados através de seus sites;

i) Permitir configuração de quantidade de canais simultâneos;

j) Permitir transbordo de chamadas para outro tronco quando atingiu uma quantidade de minutos previamente configurados;

k) Permitir configuração de Codec preferencial diretamente da interface web, no caso de tronco VoIP;

l) Permitir o monitoramento de todos os canais (Digitais, Analógicos, GSM e VoIP), com opção de desligar uma chamada em andamento, inclusive informando o status de cada canal (se ocupado, livre ou indisponível).

4.1.7.10. Digitalização de documentos e Fax:

a) Recebimento automático de FAX via E1.

b) Permitir o cadastro ilimitado de fax virtuais;

c) Permitir o recebimento dos fax em PDF diretamente na caixa de e-mail;

d) Permitir o armazenamento de cópia dos fax recebidos com possibilidade de visualizar e/ou reenviar para o e-mail cadastrado;

e) Permitir o envio de fax diretamente da interface do sistema, com notificação de entrega;

f) Permitir o envio de fax através de um cliente de e-mail.

4.1.7.11. Outras Facilidades do sistema:

a) Possuir no mínimo 10 (dez) classes de serviços de ramais, de maneira a atribuir diferentes níveis de restrição para acessar as funções, bem como autorização de tráfego.

b) Possibilitar backup de programas e dados alteráveis (data base) a cada mudança na base de dados do sistema.

c) Possibilidade de definir diferentes rotas para chamadas de entrada e/ou saída, bem como definição de privilégio para obtenção de rotas em função de categorização do ramal.

d) As rotas de saída devem possibilitar: discagem direta por multifrequencial, pós discagem.

e) Todas as informações apresentadas no “display” dos aparelhos telefônicos e consoles/terminais de telefonista devem ser obrigatoriamente em português.

f) A Central Telefônica IP deverá possibilitar o bloqueio automático de recebimento de ligações a cobrar – DDC e de realização de chamadas a serviços especiais (0900, 0300, 0700, auxílio à lista, etc.), em todas as linhas de tronco da central. A implementação deste recurso deverá ser pela programação da central telefônica, sem uso de “hardware” adicional.

g) A Central Telefônica IP deverá possuir circuitos discriminadores de chamadas interurbanas (IU) de modo a viabilizar a categorização de diferentes tipos de acesso dos ramais às redes telefônicas local, regional, nacional e internacional.

h) Os circuitos discriminadores IU utilizados deverão atender às definições e características funcionais, elétricas e de transmissão previstas na Prática TELEBRÁS nº 220-600-703 - Especificações Gerais de Discriminador IU para Central Telefônica IP tipo PABX.

i) A Central Telefônica IP deverá possibilitar a implementação da seguinte categorização de ramais:

1. Irrestrito: poderão efetuar chamada local, nacional (DDD) e internacional (DDI) para terminais fixo ou celular, após a discagem de código de acesso;
2. Impedido de acesso ao tráfego ddi: somente poderão efetuar chamadas locais e nacionais (DDD) para terminais fixo ou celular, após a discagem de código de acesso;
3. Impedido de acesso ao tráfego ddi e restrição ao tráfego DDD: somente poderão efetuar chamadas locais para terminais fixo e celular e para áreas nacionais – DDD previamente definidas, com ou sem bloqueio a celular, após a discagem de código de acesso;
4. Impedido de acesso ao tráfego ddi e DDD: somente poderão efetuar chamadas locais para terminais fixo ou celular, após a discagem de código de acesso;
5. Impedido de acesso ao tráfego ddi e ddd com restrição a celular: somente poderão efetuar chamadas locais para terminais fixo, após a discagem de código de acesso;
6. Semi-restrito: somente poderão efetuar chamadas internas e, via telefonista, chamadas externas;
7. Restrito: somente poderão efetuar chamadas entre os ramais do Sistema.

j) A programação dos parâmetros do Sistema deve ser realizada através de terminal de serviço baseado em microcomputador;

k) Possuir toques de campainha diferenciados para chamadas internas, chamadas externas e rechamada automática;

l) Permitir que um usuário habilite através de código PIN (Personal Identification Number), todas as características de seu ramal de origem, em qualquer ponto do Sistema proposto, sendo sempre bilhetado pelo seu código de origem, e não ao ramal físico onde se fez a ligação;

m)O Sistema deve possibilitar serviço noturno de modo que as chamadas externas encaminhadas através das telefonistas ausentes, sejam automaticamente dirigidas a ramal ou grupos de ramais pré-determinados;

n) Possuir agenda de nomes que possibilite a indicação de número e nome, associados a todos os ramais do Sistema, quando em chamadas internas dirigidas a aparelhos telefônicos IP;

o) A Central Telefônica IP deverá possibilitar que ramais para fax sejam programados especificamente para lidar com as informações enviadas por fax;

p) A Central Telefônica IP deverá estar dotada de dispositivo interno que gere música sintética para uso em chamadas retidas pela telefonista/usuário, quando em processo de consulta, retenção e transferência entre ramais. Deverá ser possível ainda a implementação de fonte externa de música por meio de rádio, tocador de CD ou porta USB que suporte leitura de áudio de um dispositivo de armazenamento USB;

q) A Central Telefônica IP deverá ser dotada de hardware e software necessário à bilhetagem em tempo real para todas as suas linhas de entrada (digitais e analógicas), através da detecção da inversão de polaridade nos fios "A" e "B" ou de qualquer outra sinalização que indique que o número chamado atendeu à ligação.

4.1.7.12. Facilidade a ramais:

a) Chamada para a telefonista – acesso à telefonista através do dígito “9”. Obs.: pode mudar de acordo com o plano de numeração local;

b) Interligação automática entre ramais – acesso automático a qualquer ramal do Sistema;

c) Transferência de chamada – capacidade de transferir ligações internas ou externas a outro ramal, antes ou após o ramal chamado atender;

d) Captura de chamada – as chamadas destinadas para um ramal podem ser capturadas por outros ramais independente de pertencer ou não ao grupo do ramal chamado;

e) Redirecionamento automático de chamadas – redirecionamento automático de chamadas para outro ramal, por não atendimento, ausente ou ocupado;

f) Rediscagem do último número discado – rediscagem, por meio de uma única tecla, do último número discado (interno ou externo);

g) Chamada em espera para ramal ocupado - com indicação por tom especial ou display e com possibilidade de proteção contra chamada em espera;

h) Retorno automático de chamadas (ramal ocupado ou não atende) – as pessoas que efetuarem chamadas para um ramal ocupado ou que não atende podem solicitar o retorno automático da chamada;

i) Estacionamento de chamadas – chamadas em curso poderão ser “estacionadas” temporariamente, para posterior retomada ou captura por outro ramal;

j) Rechamada – após um período predeterminado, as chamadas que foram estacionadas ou transferidas sem resposta, voltam a chamar o ramal inicial. As chamadas transferidas para ramal ocupado também devem retornar ao ramal inicial;

k) Rechamada automática para ramal – reserva automática de um ramal quando ocupado ou não atende, através de uma chamada de retorno automática;

l) Consulta – consultar um outro destino nas chamadas externas de entrada e saída, e internas. Parte retida com música em espera;

m) Consulta Pendular - possibilidade de alternar entre dois participantes (interno e/ou externo) através de código de 1 (hum) dígito ou tecla específica; parte retida com música em espera;

n) Conferência a três – entre participantes internos e/ou externos, com tom de advertência;

o) Conferência múltipla entre ramais;

p) Acesso a duas linhas - atendimento simultâneo de duas chamadas, com uma sendo colocada em espera;

q) Siga-me – redirecionar uma chamada de entrada de um ramal ou grupo de ramais, para um número designado, interno ou externo;

r) Proteção para transmissão de dados – os ramais de dados deverão ser protegidos contra intercalação, de maneira fixa ou iniciado através de código;

s) Grupos de usuários – formação de grupos de usuários por ramais analógicos ou IP;

t) Grupos chefe/secretária – agrupamento de ramais multi-chefe / multi-secretária;

u) Busca em grupo – grupo de ramais podendo ser acessado de maneira cíclica, hierárquica, fixa ou pré- definida, através de um número comum de grupo ou por seus números individuais;

v) Cadeado Eletrônico – Possibilidade de qualquer ramal do Sistema ser habilitado ou desabilitado pelo seu usuário para efeito de estabelecimento de chamadas externas;

w) O sistema deve permitir a criação de agendas numéricas, para serem utilizadas na tradução dos números para nome/número nos relatórios das chamadas;

x) Permitir hot dial, que é a discagem automática para um número quando o usuário tira o telefone do gancho;

y) Permitir discagem direta a ramal (DDR) ou direct inward dialing (DID), permitindo direcionar as ligações externas diretamente aos ramais, por meio dos troncos DDR sem passar pela telefonista;

z) Permitir a opção de não perturbe. Uma vez habilitado, o telefone não poderá emitir sinal sonoro.

4.1.7.13. Comunicação Unificada:

a) Deverá ser fornecida juntamente com a solução de telefonia ofertada um serviço que possibilite a comunicação unificada que contemple sistema de correio de voz integrado ao correio eletrônico mensagem instantânea, presença e ainda softphone com capacidade de efetuar chamadas de voz e vídeo, tanto para as estações de trabalho quanto para os dispositivos móveis com as seguintes características:

b) Software de Comunicação Unificada para estações de trabalho de todos os usuários IP, com as seguintes características:

1. Utilizar no login as mesmas credenciais - usuário e senha -usadas pelos telefones IP na autenticação.
2. Efetuar chamadas de áudio e vídeo.

3. Possuir softphone integrado com sinalização e mídia criptografados no mínimo (128 bits) para as chamadas de voz e vídeo.
4. Informar acerca do estado de múltiplos dispositivos: telefones IPs, softphones e software cliente de comunicações unificadas de tal modo a indicar a disponibilidade dos usuários (por ícones, imagens ou cores), como por exemplo: Off-line, Disponível, Ausente, Ocupado e Não perturbe.
5. Ao receber uma chamada, o sistema possa direcioná-la aos dispositivos conectados ao sistema.
6. Suportar a facilidade de número único para realizar e receber chamadas, fazendo o roteamento das chamadas de acordo com as preferências do usuário.
7. Permitir a criação de conferências selecionando os contatos e clicando num botão específico para esse fim.
8. Permitir que o criador da conferência tenha o controle de adicionar ou retirar usuários, retirar ou devolver o áudio do microfone de um participante, encerrar a conferência e/ou transferi-la para outro usuário.
9. Permitir que o usuário cadastre dispositivos/telefones de contato.
10. Permitir o envio de mensagens instantâneas e indicação de presença.

c) Deverão ser fornecidos softwares de Comunicação Unificada para dispositivos móveis compatível com sistemas operacionais iOS e Android, com as seguintes características:

1. Utilizar no login as mesmas credenciais - usuários e senhas - usadas pelos usuários na autenticação dos telefones IP.
2. Efetuar chamadas de áudio.
3. Possuir softphone integrado com sinalização e mídia criptografados no mínimo (128 bits) para as chamadas de voz.
4. Informar acerca do estado de múltiplos dispositivos: telefones IPs, softphones e software cliente de comunicações unificadas de tal modo a indicar a disponibilidade dos usuários (por ícones, imagens ou cores), como por exemplo: Off-line, Disponível, Ausente, Ocupado e Não perturbe.
5. Ao receber uma chamada, o sistema possa direcioná-la aos dispositivos conectados ao sistema.
6. Suportar a facilidade de número único para realizar e receber chamadas, fazendo o roteamento das chamadas de acordo com as preferências do usuário.
7. Permitir a criação de conferências selecionando os contatos e clicando num botão específico para esse fim.
8. Permitir que o criador da conferência tenha o controle de adicionar ou retirar usuários, retirar ou devolver o áudio do microfone de um participante, encerrar a conferência e/ou transferi-la para outro usuário.
9. Permitir que o usuário cadastre dispositivos/telefones de contato.
10. Permitir o envio de mensagens instantâneas e indicação de presença.

d) Deverá ser entregue solução de correio de voz com caixa postal independente para cada ramal IP do sistema com as seguintes características:

1. Deverá realizar atendimento automático de chamadas que possibilite a gravação e recuperação de mensagens, quando o ramal chamado estiver ocupado, com seu usuário ausente ou por comando do usuário para redirecionamento das chamadas.
2. O Sistema de correio de voz deve ser centralizado e atender a todos os usuários do sistema de telefonia IP.
3. Permitir a associação de uma caixa postal a qualquer licença de usuário do sistema de telefonia IP.
4. Implementar os codecs G.711 a-law/µ-law ou G.729.
5. Deverá implementar protocolo IMAP4 e SMTP para integração com sistema de e-mail existente no CONTRATANTE.
6. Deverá prover indicação visual nos telefones IP de mensagem existente na caixa postal.
7. Deverá permitir uma caixa postal de fax individualizada para cada usuário que possua um correio de voz no sistema.
8. Suportar formato TIF para recebimento de fax.
9. Permitir a indicação de forma audível em terminais analógicos da existência de mensagens na caixa postal.
10. O sistema deve implementar mecanismo de login e senha para acesso às caixas postais.
11. Permitir definir no sistema a quantidade mínima de 8 (oito) dígitos para a senha de acesso a caixa postal.
12. O Sistema deve possuir a facilidade de menu de voz para pré-atendimento individual, configurável pelo usuário da caixa postal, com possibilidade de desvio para ramais internos e números externos. Deverá ser possível montar um menu para chamadores internos e outra para chamadores externos.
13. O sistema deve permitir o usuário acionar mensagem de ausência temporária.
14. Deverá permitir, através da interface de gerenciamento, a inclusão e exclusão de usuários, cancelamentos de senhas, indicação de ocupação do sistema. Este acesso ao gerenciamento deve ser controlado por senha.
15. Deverá permitir gravação de saudações, devendo ser possível usar saudação padrão ou personalizada pelo usuário. A gravação das mensagens de saudação deve ser feita por meio do telefone.
16. Permitir ao usuário salvar, deletar, responder e encaminhar as mensagens de voz através do próprio telefone.
17. Deverá ser disponibilizada uma caixa de correio de voz para cada ramal do sistema.

e) Permitir a agregação de no mínimo 3 terminais IP, de forma que no recebimento de chamadas telefônicas a ligação possa tocar no mínimo em três dispositivos simultaneamente, (ex. cliente SIP para celular, telefone IP e cliente SIP para desktop) sendo interrompido após o primeiro atendimento.

4.1.7.14. Facilidade para Secretária:

a) Atendimento seletivo de chamadas;

b) Indicação de chamada em espera;

c) Transferência rápida de chamadas (sem anúncio);

d) Transferência de chamadas com anúncio;

e) Rediscagem do último número discado;

f) Preparação de discagem sem retirada do monofone do gancho;

g) Discagem abreviada de números através da agenda;

h) Intercalação quando o ramal e/ou tronco está ocupado;

i) Permitir retenção de chamada de entrada para efetuar consultas e transferências;

j) Identificação dos números chamadores na fila de espera;

k) Estacionamento de chamadas;

l) Rechamada em ramal ocupado;

m) Conferência;

n) Comutação manual para serviço noturno.

4.1.7.15. Controles:

a) Controle de minutagem por ramal;

b) Controle de consumo por operadora, em minutos e valores.

4.1.7.16. Administração de Cadastro:

a) Cadastro de Ramais;

b) Cadastro de Voicemail;

c) Cadastro de Centro de Custos;

d) Cadastro de Agentes.

4.1.7.17. Mesa Virtual de Telefonista:

a) Status de Ramais (Registrados, Livres, Ocupados e Tocando);

b) Status das chamadas entrantes da fila de atendimento;

c) Campo de comentário nos registros de ligações;

d) Teclas de funções básicas do pabx ip.

e) A Console para Telefonista deve ser integrável numa mesma rede local.

f) Possibilidade de utilização em conjunto com aparelho IP com monofone e fone de cabeça, e com fone de cabeça conectado diretamente ao computador.

g) Deverá funcionar em ambiente MS Windows, de forma que outros recursos de informática (p/ex. Correio Eletrônico) possam ser compartilhados e integrados num mesmo ambiente de trabalho.

h) Deverá ser fornecido um conjunto, para cada console de telefonista, incluindo 1 (um) aparelho telefônico IP tipo 2, conforme especificação definida nesta especificação.

i) Será de responsabilidade da contratante fornecer o microcomputador/desktop, sistema operacional MS Windows, suíte de software MS Office, mouse, teclado e monitor, mas será de responsabilidade da contratada informar os requisitos mínimos necessários para funcionamento adequado do Console para Telefonista.

j) Permitir a visualização em tela das seguintes informações, importantes para o processamento de chamadas: número do ramal e nome do usuário e status do ramal.

k) Permitir reter a chamada de entrada para efetuar breves consultas e transferências.

l) Quando não for possível à telefonista transferir a ligação imediatamente, deverão haver 04 (quatro) posições de estacionamento de chamadas, cujas ligações estacionadas poderão ser recuperadas de forma seletiva, visualizadas em tela.

m) Permitir transbordo para outros grupos.

n) Possuir sinalização visual das chamadas internas e externas da telefonista, permitindo a ela atender às chamadas de maneira seletiva.

o) Possuir a facilidade de proteção contra a transferência não autorizada.

p) Permitir a visualização da data e/ou hora real do sistema.

q) Acesso à lista telefônica centralizada, com capacidade para 04 (quatro) campos de informação do ramal por registro (nome, setor, empresa, cargo, etc). Os critérios de pesquisa para localização de registros devem ao menos pelo o número do ramal, o nome e o setor.

r) A lista deve ser integrada com a tela da telefonista, de forma a trazer para esta os resultados da pesquisa. O resultado da pesquisa deverá ser aproveitado automaticamente na seleção do destino correspondente.

s) A lista telefônica deverá ter a facilidade de poder ser importada de bancos de dados externos, bem como exportada.

t) Permitir o acesso à discagem abreviada comum.

u) A console para telefonista deverá permitir a chamada dos correspondentes, interno e externo, de acordo com o sobrenome, o primeiro nome ou as iniciais, independente do seu status de comunicação (chamada direta, transferência). O usuário terá acesso ao serviço pelo teclado do PC, pois o uso amigável é uma exigência.

v) Os softwares adicionais com licença (p.ex. SQL Server, etc) necessário para a completa instalação da mesa operadora deverá ser cotado pelos proponentes.

w) Permitir a visualização do status (ocupado ou disponível) de no mínimo 2.000 ramais de usuários.

x) Possuir manual em Português.

4.1.7.18. Gerenciamento de Tarifação de chamadas:

a) Cadastro de Tarifa por operadoras;

b) Cadastro de Centro de Custos;

c) Relatório detalhado e resumido por ramais;

d) Relatório modelo fatura;

e) Relatório por Centro de Custos, Detalhado e Sumário;

f) Gráfico de acompanhamento de consumo por operadora: Diário, Mensal e Anual;

g) A SOLUÇÃO DE TELEFONIA IP deverá implementar geração e gerenciamento de bilhetes detalhados (CDR) de todas as chamadas, além de permitir sua exportação para PDF e CSV;

h) Permitir a parametrização das tarifas contratadas via web;

i) Permitir criação de rotas de saídas associadas às tarifas previamente configuradas (rotas de menor custo).

j) Geração de alarme quando houver falha no sistema de geração, coleta ou armazenamento de bilhetes, com envio de mensagem eletrônica;

k) Permitir a coleta de bilhetes da Central PABX via porta ethernet;

l) Permitir agendamento de coleta em intervalos diferenciados em relação ao armazenamento das informações em banco de dados;

m) Os bilhetes gerados deverão conter no mínimo os seguintes campos:

1. Número do Nó de origem ou informação equivalente;
2. Número do assinante chamado;
3. Número do ramal que originou a chamada;
4. Identificação do entroncamento;
5. Identificação do usuário que efetuou a chamada;
6. Data de início da chamada;
7. Hora de início da chamada;
8. Duração da chamada;
9. Número do ramal ou assinante de destino em caso de transferência de chamadas;
10. Identificação de ligação de transferência.

n) Deverá permitir a exportação de dados para programas editores de texto, em formatos previamente configuráveis pelo usuário do sistema;

o) Deverá gerar a totalização automática diária, durante o horário noturno, das seguintes informações do dia anterior: quantidade e valor de chamadas e minutos por central, por operadora, por usuário e por tipo de ligação;

p) Deverá gerar a totalização automática e mensal das informações totalizadas diariamente, e permitir que estas informações sejam exportadas para planilhas eletrônicas e arquivos em formato PDF ou HTML;

q) Deverá permitir a definição de critérios para emissão de relatórios através do uso de filtros, tais como data, hora, ramal, tipo de chamada, centro de custo, valor da chamada, ligações particulares ou a negócios, duração da ligação, troncos, número do nó, localidade, número discado, operadora, código de projeto;

r) Os relatórios deverão ser apresentados em língua portuguesa (Brasil);

s) Deverá ser possível acessar os relatórios totalizados a partir de qualquer computador na rede Intranet ou Internet, via acesso Web-Browser, através de uso de senha de autenticação, permitindo acessos simultâneos ao gerenciador do sistema;

t) Deverá ser possível enviar, por meio de mensagem eletrônica pela Intranet da CONTRATANTE, os relatórios totalizados diários e mensais para usuários pré-cadastrados em uma linha de distribuição;

u) O sistema de tarifação deverá permitir a observação de dados de tráfego, de tal forma que possibilite a medição e registros diários, relatório de tráfego na hora de Maior Movimento, em forma de relatórios específicos para análise de custos, ocupação de tronco, duração de chamadas e avaliação da carga de serviço em períodos pré-determinados;

v) Os relatórios poderão ser configurados pelo administrador, de forma que o logotipo da CONTRATANTE possa ser inserido no início de cada página;

w) Possibilitar o envio de relatórios via e-mail, com ou sem compactação de arquivo, nos formatos RTF (Word), HTML, PDF, XLS (Excel) e Texto;

x) Permitir a personalização do corpo do e-mail no envio de relatórios;

y) Possibilitar o compartilhamento de relatórios para consulta via Web por outros usuários e grupos de usuários específicos;

z) Permitir que cada ramal seja associado a um ou mais endereços de e-mail assim como cada centro de custo. Ao emitir um relatório de conta telefônica, os relatórios de cada ramal devem ser automaticamente enviados aos respectivos e-mails;

aa) O agendamento de tarefas poderá ser programado para realização diária, semanal, mensal ou em dias específicos da semana ou do mês;

ab) Permitir exportação de ligações via arquivo texto, periódica e automaticamente, visando possibilitar integração com sistemas gerenciais e/ou de terceiros;

ac) Possibilitar análise de desempenho no atendimento das ligações por ramal e/ou centro de custo;

ad) Centro de Custo - Fornecer de maneira sintética quanto cada centro de custo gastou, indicando, inclusive, os gastos dos ramais associados;

ae) Conta Telefônica - Totalizar por RAMAL ou por CENTRO DE CUSTO as ligações locais, DDD, DDI e celulares além de indicar as ligações particulares baseadas na lista telefônica;

af) Estatística da Central - Emitir relatório que sumariza as ligações por gasto, tempo ou número de ligações levando em conta diversos critérios (por Ramal, por Tronco ou Número Discado), imprimindo os registros em ordem crescente ou decrescente, indicando quais os ramais que gastaram mais ou menos, os números mais discados ou os troncos menos utilizados;

ag) Fluxo de ligações - Sumarizar por dia ou por hora o número de ligações, tempo utilizado e custo das ligações;

ah). Pela Lista telefônica particular - Sumarizar por dia ou por hora o número de ligações, tempo utilizado e custo das ligações efetuadas para números cadastrados na lista telefônica;

ai) Tráfego Telefônico - Relatórios gerenciais, incluindo análise do tráfego;

aj) Relatório de Análise de Operadoras, permitindo que sejam analisados, além dos gastos reais por operadora, as possibilidades de economia se fossem utilizadas outras operadoras do mercado. O relatório deverá aplicar os dados reais de utilização telefônica em uma simulação das tarifas reais de outras operadoras;

ak) Relatório que permita análise anual de gastos por ramal e por tipo de ligação, com respectivos gráficos;

al) É necessário que o Sistema de Tarifação permita o cadastramento de cotas de consumo máximo por ramal e/ou centro de custo, de forma que uma vez atingida a cota, seja emitido um aviso e mensagem via correio eletrônico;

am) As cotas podem ser definidas por valor ou por duração das ligações;

an) Controle de cotas equivalente ao controle de conta corrente bancária;

ao) Possibilidade de bloquear o ramal cuja cota foi atingida quando houver disponibilização de acesso ao PABX;

ap) O desbloqueio de ramal poderá ser efetuado pelos gestores e/ou pelo Gerente responsável pelo usuário do ramal;

aq) Emitir relatórios de extrato e saldo de conta corrente, para controle de utilização das cotas concedidas;

ar) Possuir aplicativo de identificação de ligações particulares via interface web, para que os usuários possam interagir com os gestores na autorização de débitos com ligações particulares;

as) Trabalhar em ambiente Windows;

at) Utilizar os protocolos SMTP ou IMAP para envio de e-mails;

au) Interface única para cadastramento, configurações, manutenção e emissão de relatórios;

av) Deverá ser fornecido todo o Hardware, Software (Ex. sistema operacional), licenças e outros materiais necessários ao pleno funcionamento do Sistema de Tarifação;

aw) Deverá possuir capacidade para tarifar no mínimo 4.000 ramais.

4.1.7.19. Análise de contas:

a) O sistema deve controlar faturas das principais operadoras do mercado;

b) O sistema deve controlar faturas de operadoras de telefonia móvel e fixa;

c) O sistema deve ser instalado na nuvem, mantido pelo contratante (as especificações necessárias para a nuvem devem ser informadas pela contratada);

d) O sistema deve disponibilizar pelo menos os últimos seis meses de informações;

e) Permitir controle de inventário de Chip e Dispositivos;

f) Permitir associar as linhas telefônicas (acesso) e seus responsáveis, esta informação deverá ser traduzida em todo o sistema;

g) Permitir gestão e auditoria da fatura conforme descrito abaixo:

1. Verificação da conformidade;
2. Comparação dos serviços e tarifas cobradas pelas operadoras com o valor contratado e serviço realmente realizado;
3. Análise de utilização das linhas para decisões estratégicas (necessidade de expansão ou subutilização de recursos).

h) O sistema deve permitir criar agendamentos para lembrar sobre vencimento de fatura, comodato e protocolo, com opção para finalizar o alerta diretamente da tela do aviso;

i) Permitir a parametrização das datas e seus vencimentos para gerar alertas na tela do sistema;

j) Permitir criar alerta para renovação de linhas telefônicas;

k) Permitir parametrização por plano;

l) Permitir parametrização por VC1, VC2 e VC3;

m) Permitir configurar se o plano é compartilhado ou não compartilhado;

n) Informar o valor cobrado dentro da mesma operadora;

o) Informar o limite em minutos para outras operadoras;

p) Informar valor a ser pago dentro ou fora do limite de minutos;

q) Permitir parametrização por pacote de dados;

r) Permite informar o limite de dados a ser trafegado informando o valor dentro ou fora do limite;

s) Permitir parametrização por SMS por limite de mensagens, valor dentro do limite e valor fora do limite;

t) Permite informar o limite de SMS enviados e o valor a ser cobrado dentro ou fora do limite;

u) Permitir verificar a conta telefônica para identificar se o valor cobrado está de acordo com o contratado, comparando o "valor cobrado x valor cobrado errado";

v) Permitir parametrização dos valores contratados com a operadora, especificando por plano serviços, pacotes etc;

w) Permitir exportação para Excel;

x) Visualizar resumo por acesso;

y) Permitir consolidar várias faturas, desta forma gerar relatórios por bimestre, trimestre, semestre, etc;

z) Permitir visualizar relatórios de faturas por acesso, centro de custos e total;

aa) Permitir visualizar total de chamadas, duração e gasto, por operadora, por VC1, VC2 e VC3, por on-net (chamadas para números dentro do mesmo grupo) e off-net (chamadas para números fora do grupo);

ab) Permitir visualizar o valor cobrado do minuto falado;

ac) Permitir visualizar o total de SMS enviados, o valor total cobrado e o valor pago por SMS;

ad) Permitir visualizar a quantidade de SMS enviados e o valor pago, por operadora;

ae) Permitir visualizar o top custo e os acessos que menos gastaram;

af) Permitir detalhamento por acesso contendo total gasto, valor da assinatura, valor do consumo de chamadas e demais valores**;**

ag) Permitir controle dos dispositivos (celulares), com possibilidade e cadastrar nota fiscal, marca/modelo/IMEI do aparelho, valor, parcelas se houver, data de recebimento e calcular valor residual automaticamente;

ah) Permitir controle de protocolo, possibilitando adicionar prazo e tipo do protocolo se solicitação ou contestação.

4.1.7.20. Integrações:

a) A Plataforma PABX IP deverá permitir integração com a Central Telefônica atual;

b) A Plataforma PABX IP deverá integrar-se com este sistema de gestão, permitindo que o mesmo efetue ações programadas de discagem, recebimento de chamadas com acionamento de tela e login de agentes de atendimento, envio de SMS;

c) A Plataforma PABX IP deverá integrar-se com a funcionalidade de URA (Unidade de Resposta Audível) e que permita a importação e consultas de informações na base de dados do sistema ativo atual.

d) A Plataforma PABX IP deverá permitir integração ou substuição dos componentes que compõem o Sistema de Video Conferência atual ativo (Marca POLYCOM) composto de: 01 MCU/RMX2000, 01 RSS 2000 (Gravador / Streaming), 01 CMA 5000 (Gatekeeper), 01 VBP (Nat Travesal), 01 Sala de Telepresença - TPX1, 64 Televisores LCD de 42, 39 CODEC PESSOAL OU EXECUTIVO DE VIDEOCONFERENCIA, 32 CODEC DE SALA OU GRUPO DE VIDEOCONFERENCIA e Software para Videoconferência(Licença) com 300 licenças.

4.1.7.21. Sistema Integrado de Videoconferência:

a) Permitir salas virtuais com mínimo de 150 usuários;

b) Oferecer escalabilidade para o mínimo de 1.500 usuários simultâneos em múltiplas salas virtuais;

c) Acompanhar os softwares de video conferência correspondentes a quantidade informada acima;

d) Permitir expansão da infraestrutura para atender a um número maior de usuários simultâneos;

e) Ser acessível a partir do navegador web em Desktop (suporte a pelo menos Google Chrome e Mozilla Firefox);

f) Ser acessível a partir de dispositivos Android e iOS via aplicativo nativo;

g) Permitir compartilhamento de múltiplos áudios e múltiplos vídeos dentro de uma sala virtual, de maneira que todos os usuários enxerguem e ouçam todos os outros;

h) Permitir compartilhamento de apresentações e documentos (suporte a pelo menos os formatos PDF, ODF, JPEG e PPT);

i) Permitir anotações sobre a apresentação através de quadro branco;

j) Possuir área de texto colaborativo dentro da sala virtual (bloco de notas);

k) Permitir compartilhamento da tela do apresentador para visualização em tempo real pelos participantes;

l) Permitir que o moderador da sala defina o papel dos participantes dentro da sala;

m) Possuir batepapo público e privado;

n) Permitir que o moderador da sala restrinja o acesso a câmera, microfone, batepapo e layout dos participantes;

o) Permitir que o moderador controle os segmentos da reunião que serão gravados;

p) Possuir gravação em formato HTML5 com indexação através dos slides;

q) Possuir gravação em formato em vídeo compatível com plataformas como YouTube ou Vimeo;

r) Suportar armazenamento de até 3.000 gravações;

s) Possuir suporte a autenticação LDAP, OAuth2 e Shibboleth, além de autenticação local.

4.1.7.22. Gravação das Chamadas

a) Permitir que as ligações sejam gravadas em disco nas seguintes formas:

1. Contínua: grava todas as ligações do início ao fim;
2. Seletiva: você define os ramais que irão serem gravados;
3. Controle manual: os usuários dos ramais acionam a gravação por teclado quando há necessidade de gravação daquela conversação.

b) Permitir consultar as chamadas por período, número ou contato previamente cadastrado na agenda, efetuadas e/ou recebidas, com a opção de baixar (download) o arquivo de áudio no computador, na extensão. WAV, para ouvir a qualquer momento sem a necessidade de estar conectado a Internet;

c) Permitir consulta das ligações gravadas via web;

d) Permitir consulta das gravações por grupo de ramais;

e) Permitir buscar as gravações por duração;

f) Permitir buscar as gravações por DDD;

g) Permitir o envio da gravação diretamente para um aparelho telefônico, podendo ser analógico, GSM, sem a necessidade de internet, utilizando uma ligação convencional;

h) Permitir enviar a gravação para um ou mais endereço de e-mail;

i) Permitir buscar as gravações por tronco de entrada;

j) Permitir adicionar um comentário na gravação;

k) Permitir exportar gravações, por período ou filtro de busca;

l) Permitir que durante uma chamada seja possível ingressar pessoas para participarem da conversação. Essas pessoas podem estar dentro ou fora da empresa;

m) O Sistema deve permitir que as gravações das chamadas sejam associadas ao usuário.

4.1.8. **DETALHAMENTO E CARACTERÍSTICAS DO ITEM 02:**

4.1.8.1. Gateway E1 para telefonia IP compatível com Asterisk:

a) 04 nterfaces digitais E1 (por equipamento):

1. Protocolos de rede: ISDN PRI e R2D/MFC.
2. A interface E1 deverá funcionar com uma rede privada (PABX) utilizando os seguintes protocolos de sinalização de usuário: QSIG, CAS EL7 e Line Side.
3. Cancelamento de eco de no mínimo 64ms (512 TAPS) por canal;
4. Compatível com as normas ITUT G.165 e G.168;
5. Deve atuar em todos os canais simultaneamente, independentemente ao uso de outros recursos do concentrador.
6. Deverá ter o recurso de desabilitar automaticamente o cancelador de eco em um canal, quando for detectado o tom de fax (2100Hz)
7. Compatível com Asterisk;
8. 30 Canais de voz de 64Kbps com possibilidade de expansão para 120 canais de voz de 64 Kbps por modulo de expansão;
9. O equipamento devera ser capaz de efetuar ou receber chamadas em todos os canais;
10. Simultaneamente, sem perda de ligações;
11. O equipamento deverá possuir cancelamento de eco em hardware, no nível da operadora (Carrier grade) de até 64ms (512 Taps) em todos os canais simultaneamente, independente de outros recursos;
12. O cancelamento de eco deverá permitir convergência e ajuste automático de delay durante toda a duração da conexão;
13. O cancelamento de eco deverá ser compatível com as normas ITU-T G165 e G.168;
14. Protocolos de rede: ISDN e R2 Digital (com até 120 trocadores de sinalização MFC). É possível configurar protocolos diferentes em cada um dos links;
15. Protocolos de PABX: EL7, Line Side, LC e QSIG (SSCT e CT);
16. Todos os recursos de voz disponíveis simultaneamente em todos os canais;
17. DSPs para executar o processamento de áudio e CODECs;
18. Troca MFC (sinalização R2);
19. Detecção e geração de dígitos DTMF, tons de fax, 425Hz (dialtone) e mensagens TDD (Telecommunications Device for the Deaf);
20. Geração de tons programáveis (beep);
21. Detecção de silêncio e presença de áudio antes e depois do atendimento;
22. Detecção de tons de interceptação (caixa postal, chamada a cobrar, etc.);
23. Detecção de sinal de fax e de caixa postal com sinalização padrão: 600Hz/450ms – 1000Hz/450ms ou 300Hz/250ms;
24. Detecção de frequências programáveis (por exemplo: tom de portabilidade, caixas postais fora do padrão, etc);
25. Supressão de DTMF;
26. Controle de volume manual e automático (AGC);
27. Cancelamento de eco em hardware;
28. Carrier grade (nível de operadora);
29. Até 64ms (512 TAPS) em todos os canais simultaneamente, independente de outros recursos;
30. Convergência e ajuste de delay automáticos durante toda a ligação;
31. Compatível com as normas ITU-T G165 e G.168 (2000 e 2002);
32. Detecção de chamada a cobrar por reconhecimento de tons, sinalização ou duplo atendimento;
33. Call progress para geração de eventos de call control em interfaces FXO e protocolos de PABX;
34. Classificação de atendimento de chamadas (Call Analyzer);
35. Interfaces (G.703) com conector BNC ou RJ-45 (no caso do RJ-45, deverá ser entregue com o respectivo adaptador balun BNC/ RJ-45);

b) Configuração, monitoração, administração e diagnóstico via Web:

c) Status dos troncos e canais via web;

d) Status do sistema via web;

e) Diagnóstico detalhado do link E1;

f) Suporte a SNMP;

g) Pode ser usado para interligar diferentes redes;

h) Configuração de IP externo;

4.1.9. **DETALHAMENTO E CARACTERÍSTICA DO ITEM 03:**

4.1.9.1. Gateway com 02 E1, 04 FXO e 08 FXS para telefonia IP compatível com Asterisk:

a) 02 nterfaces digitais E1:

1. Protocolos de rede: ISDN PRI e R2D/MFC.
2. A interface E1 deverá funcionar com uma rede privada (PABX) utilizando os seguintes protocolos de sinalização de usuário: QSIG, CAS EL7 e Line Side.
3. Cancelamento de eco de no mínimo 64ms (512 TAPS) por canal;
4. Compatível com as normas ITUT G.165 e G.168;
5. Deve atuar em todos os canais simultaneamente, independentemente ao uso de outros recursos do concentrador.
6. Deverá ter o recurso de desabilitar automaticamente o cancelador de eco em um canal, quando for detectado o tom de fax (2100Hz)
7. Compatível com Asterisk;
8. 30 Canais de voz de 64Kbps com possibilidade de expansão para 120 canais de voz de 64 Kbps por modulo de expansão;
9. O equipamento devera ser capaz de efetuar ou receber chamadas em todos os canais;
10. Simultaneamente, sem perda de ligações;
11. O equipamento deverá possuir cancelamento de eco em hardware, no nível da operadora (Carrier grade) de até 64ms (512 Taps) em todos os canais simultaneamente, independente de outros recursos;
12. O cancelamento de eco deverá permitir convergência e ajuste automático de delay durante toda a duração da conexão;
13. O cancelamento de eco deverá ser compatível com as normas ITU-T G165 e G.168;
14. Protocolos de rede: ISDN e R2 Digital (com até 120 trocadores de sinalização MFC). É possível configurar protocolos diferentes em cada um dos links;
15. Protocolos de PABX: EL7, Line Side, LC e QSIG (SSCT e CT);
16. Todos os recursos de voz disponíveis simultaneamente em todos os canais;
17. DSPs para executar o processamento de áudio e CODECs;
18. Troca MFC (sinalização R2);
19. Detecção e geração de dígitos DTMF, tons de fax, 425Hz (dialtone) e mensagens TDD (Telecommunications Device for the Deaf);
20. Geração de tons programáveis (beep);
21. Detecção de silêncio e presença de áudio antes e depois do atendimento;
22. Detecção de tons de interceptação (caixa postal, chamada a cobrar, etc.);
23. Detecção de sinal de fax e de caixa postal com sinalização padrão: 600Hz/450ms – 1000Hz/450ms ou 300Hz/250ms;
24. Detecção de frequências programáveis (por exemplo: tom de portabilidade, caixas postais fora do padrão, etc);
25. Supressão de DTMF;
26. Controle de volume manual e automático (AGC);
27. Cancelamento de eco em hardware;
28. Carrier grade (nível de operadora);
29. Até 64ms (512 TAPS) em todos os canais simultaneamente, independente de outros recursos;
30. Convergência e ajuste de delay automáticos durante toda a ligação;
31. Compatível com as normas ITU-T G165 e G.168 (2000 e 2002);
32. Detecção de chamada a cobrar por reconhecimento de tons, sinalização ou duplo atendimento;
33. Call progress para geração de eventos de call control em interfaces FXO e protocolos de PABX;
34. Classificação de atendimento de chamadas (Call Analyzer);
35. Interfaces (G.703) com conector BNC ou RJ-45 (no caso do RJ-45, deverá ser entregue com o respectivo adaptador balun BNC/ RJ-45);

b) 04 interfaces FXO:

1. Protocolos de rede: FXO (Foreign eXchange Office).
2. O equipamento deverá possuir XX (xxxx) canais FXO (Foreign eXchange Office) para interligação analógica com linhas telefônicas convencionais;
3. E deverá atender com Call progress; gravação full duplex, detecção de discagem DTMF e decádica, detecção de silêncio e presença de áudio, geração de sinais de beeb 425Hz e DTMF;
4. Deverá ter o recurso de desabilitar automaticamente o cancelador de eco em um canal, quando for detectado o tom de fax (2100Hz);

5. Cancelamento de eco de no mínimo 64ms (512 TAPS) por canal;
6. Compatível com as normas ITUT G.165 e G.168;
7. Deve atuar em todos os canais simultaneamente, independentemente ao uso de outros recursos do concentrador.
8. Deverá ter o recurso de desabilitar automaticamente o cancelador de eco em um canal, quando for detectado o tom de fax (2100Hz)
9. Detecção de sinais de discagem do tipo DTMF no dispositivo;
10. Detecção de sinais de fax e caixa postal dentro do intervalo padrão 600 Hz/450 ms – 1000 Hz/450 ms no dispositivo;
11. Os protocolos de sinalização devem fazer parte do produto;
12. O tratamento de sinalização acústica deve ser feito pelo hardware, através de DSPs.

c) 08 interfaces FXS:

1. Protocolos de rede analógia: FXS (*Foreign eXchange Subscriber*)
2. Cancelamento de eco de no mínimo 64ms (512 TAPS) por canal;
3. Cancelamento de eco compatível com as normas ITUT G.165 e G.168;
4. O cancelamento de eco deve atuar em todos os canais simultaneamente, independentemente ao uso de outros recursos do concentrador.
5. Deverá ter o recurso de desabilitar automaticamente o cancelador de eco em um canal, quando for detectado o tom de fax (2100Hz)
6. Detecção de sinais de discagem do tipo DTMF no dispositivo;
7. Detecção de sinais de fax e caixa postal dentro do intervalo padrão 600 Hz/450 ms – 1000 Hz/450 ms no dispositivo;
8. Os protocolos de sinalização devem fazer parte do produto;
9. O tratamento de sinalização acústica deve ser feito pelo hardware, através de DSPs.

d) Configuração, monitoração, administração e diagnóstico via Web:

e) Status dos troncos e canais via web;

f) Status do sistema via web;

g) Diagnóstico detalhado do link E1;

h) Suporte a SNMP;

i) Pode ser usado para interligar diferentes redes;

j) Configuração de IP externo;

4.1.10. **DETALHAMENTO E CARACTERÍSTICA DO ITEM 04:**

4.1.10.1. Gateway E1 para telefonia IP compatível com Asterisk:

a) 02 nterfaces digitais E1 (por equipamento):

1. Protocolos de rede: ISDN PRI e R2D/MFC.
2. A interface E1 deverá funcionar com uma rede privada (PABX) utilizando os seguintes protocolos de sinalização de usuário: QSIG, CAS EL7 e Line Side.
3. Cancelamento de eco de no mínimo 64ms (512 TAPS) por canal;
4. Compatível com as normas ITUT G.165 e G.168;
5. Deve atuar em todos os canais simultaneamente, independentemente ao uso de outros recursos do concentrador.
6. Deverá ter o recurso de desabilitar automaticamente o cancelador de eco em um canal, quando for detectado o tom de fax (2100Hz)
7. Compatível com Asterisk;
8. 30 Canais de voz de 64Kbps com possibilidade de expansão para 120 canais de voz de 64 Kbps por modulo de expansão;
9. O equipamento devera ser capaz de efetuar ou receber chamadas em todos os canais;
10. Simultaneamente, sem perda de ligações;
11. O equipamento deverá possuir cancelamento de eco em hardware, no nível da operadora (Carrier grade) de até 64ms (512 Taps) em todos os canais simultaneamente, independente de outros recursos;
12. O cancelamento de eco deverá permitir convergência e ajuste automático de delay durante toda a duração da conexão;
13. O cancelamento de eco deverá ser compatível com as normas ITU-T G165 e G.168;
14. Protocolos de rede: ISDN e R2 Digital (com até 120 trocadores de sinalização MFC). É possível configurar protocolos diferentes em cada um dos links;
15. Protocolos de PABX: EL7, Line Side, LC e QSIG (SSCT e CT);
16. Todos os recursos de voz disponíveis simultaneamente em todos os canais;
17. DSPs para executar o processamento de áudio e CODECs;

18. Troca MFC (sinalização R2);
19. Detecção e geração de dígitos DTMF, tons de fax, 425Hz (dialtone) e mensagens TDD (Telecommunications Device for the Deaf);
20. Geração de tons programáveis (beep);
21. Detecção de silêncio e presença de áudio antes e depois do atendimento;
22. Detecção de tons de interceptação (caixa postal, chamada a cobrar, etc.);
23. Detecção de sinal de fax e de caixa postal com sinalização padrão: 600Hz/450ms – 1000Hz/450ms ou 300Hz/250ms;
24. Detecção de frequências programáveis (por exemplo: tom de portabilidade, caixas postais fora do padrão, etc);
25. Supressão de DTMF;
26. Controle de volume manual e automático (AGC);
27. Cancelamento de eco em hardware;
28. Carrier grade (nível de operadora);
29. Até 64ms (512 TAPS) em todos os canais simultaneamente, independente de outros recursos;
30. Convergência e ajuste de delay automáticos durante toda a ligação;
31. Compatível com as normas ITU-T G165 e G.168 (2000 e 2002);
32. Detecção de chamada a cobrar por reconhecimento de tons, sinalização ou duplo atendimento;
33. Call progress para geração de eventos de call control em interfaces FXO e protocolos de PABX;
34. Classificação de atendimento de chamadas (Call Analyzer);
35. Interfaces (G.703) com conector BNC ou RJ-45 (no caso do RJ-45, deverá ser entregue com o respectivo adaptador balun BNC/ RJ-45);
36. Alimentação tipo Full Range 110-240 Vac – 50/60 Hz.

b) Configuração, monitoração, administração e diagnóstico via Web:

c) Status dos troncos e canais via web;

d) Status do sistema via web;

e) Diagnóstico detalhado do link E1;

f) Suporte a SNMP;

g) Pode ser usado para interligar diferentes redes;

h) Configuração de IP externo;

4.1.11. **DETALHAMENTO E CARACTERÍSTICA DO ITEM 05:**

4.1.11.1. Gateway GSM para telefonia IP compatível com Asterisk:

a) 16 nterfaces/portas:

1. Capacidade para 2 SIM Cards de qualquer operadora por canal, sendo um ativo e outro stand-by;
2. Permite diferentes operadoras no mesmo módulo;
3. Interface 3G GSM 6-band: 800/850/900/1700/1900/2100 MHz;
4. Fallback para 2G quad-band: 850/900/1800/1900 MHz;
5. Canais VoIP: 8 canais SIP. Possibilidade de expansão de canais SIP sob aquisição de licenças adicionais;
6. Protocolos de rede: GSM;
7. Envio e recebimento de SMS: Suporte ao envio e recepção de mensagens SMS via dialplan ou interface AMI;
8. Recebe confirmação de entrega de SMS;
9. Informações de sinalização e estado dos canais reportados via interface AMI;
10. Detecção de atendimento disponível via dialplan e interface AMI;
11. Comandos específicos de sinalização disponibilizados via interfaces AMI e AGI;
12. Compatível com Asterisk;
13. Todos os recursos de voz disponíveis simultaneamente em todos os canais;
14. DSPs para executar o processamento de áudio;
15. Detecção e geração de tons (DSP);
16. Detecção e geração de dígitos DTMF, tons de fax, 425Hz (dialtone) e mensagens TDD (Telecommunications Device for the Deaf);
17. Geração de tons programáveis (beep);
18. Detecção de silêncio e presença de áudio antes e depois do atendimento;

19. Detecção de tons de interceptação (caixa postal, chamada a cobrar, etc.);
20. Detecção de sinal de fax e de caixa postal com sinalização padrão: 600Hz/450ms – 1000Hz/450ms ou 300 Hz/250ms;
21. Detecção de frequências programáveis (por exemplo: tom de portabilidade, caixas postais fora do padrão, etc)
22. Supressão de DTMF;
23. Controle de volume manual e automático (AGC);
24. Cancelamento de eco em hardware;
25. Carrier grade (nível de operadora);
26. Até 64ms (512 TAPS) em todos os canais simultaneamente, independente de outros recursos;
27. Convergência e ajuste de delay automáticos durante toda a ligação;
28. Compatível com as normas ITU-T G165 e G.168 (2000 e 2002) Sinalização e tratamento de chamadas:
29. Detecção de chamada a cobrar por reconhecimento de tons, sinalização ou duplo atendimento;
30. Call progress para geração de eventos de call control em interfaces FXO e protocolos de PABX;
31. Classificação de atendimento de chamadas (Call Analyzer) Alta Disponibilidade;

b) Mínimo 02 portas Ethernet para conexão com servidor (redundância de rede);

c) Redundância de servidores (suporte a IP virtual);

d) Instalador automatizado para atualização e implantação de novos sistemas;

e) Sistema web para configuração, monitoração e diagnóstico;

f) Integração nativa com SNMP;

g) Analisador de sinalização;

h) Monitoramento remoto em tempo real (via web);

i) Interface web para controle, visualização e download de logs Características Físicas

j) Conectores: SMA para antenas;

k) Acompanha 1 antena 3dB com fio por canal GSM;

l) Módulo padrão 1U e 1/2 rack 19";

m) Garantia de fábrica de 3 anos;

n) Certificação Anatel;

o) Indústria Certificada ISO 9001;

4.1.12. **DETALHAMENTO E CARACTERÍSTICA DO ITEM 06:**

4.1.12.1. Para permitir o acesso remoto dos usuários através de dispositivos móveis, PC e telefones IPs de forma segura e a conexão com troncos SIP de rede publica telefônica, faz-se necessário o fornecimento solução de SBC (Session Border Controller) compatível com Asterisk.

4.1.12.2. Por questões de segurança o SBC deverá ser implementado em appliance ou servidor distinto do controlador de voz SIP.

4.1.12.3. Deverá implementar todas as funcionalidades descritas na RFC 5853.

4.1.12.4. Deverá permitir o registro de no mínimo 3.000 (três mil) usuários externos.

4.1.12.5. Deverá suportar no mínimo 500 ligações simultâneas.

4.1.12.6. Deverá ser aderente e homologado pelo fabricante do equipamento de telefonia proposto e totalmente compatível com a solução.

a) Serviços:

1. Amplamente escalável baseada na plataforma;
2. Soluções de alta disponibilidade com failover dinâmico;
3. Deep Packet Inspection (Sinalização e Mídia);
4. Proteção DoS / DDoS;
5. Lista ACL / bloqueio ou liberação por IP;
6. Normalização SIP;

7. Controle de Admissão de Chamadas;
8. Marcação QoS;
9. Manipulação DTMF;
10. Travessia NAT;
11. Compatível com RFC 5853;
12. Trabalhador remoto: valida e suporta de forma segura os usuários remotos / móveis para ampliação da capacidade dos PABX;
13. Sem VPN;
14. Travessia NAT da ponta remota e local;
15. Suporta hard e soft IP Phones;
16. Serviços de criptografia;
17. SIP TLS para TCP, UDP;
18. SRTP para RTP.

b) Características de Segurança:

1. Deep Packet Inspection (Sinalização e Mídia)
2. Proteção DoS / DDoS
3. Lista ACL / bloqueio ou liberação por IP
4. Normalização SIP
5. Controle de Admissão de Chamada
6. Manipulação de DTMF
7. Travessia NAT da ponta remota e local
8. Topology Hiding
9. Compatível com RFC 5853

c) Sinalização/Protocolos suportados:

1. RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication;
2. RFC 2833 - RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals (somente Telephony Signals);
3. RFC 3204 - MIME media types for ISUP and QSIG Objects;
4. RFC 3262 - Protocolo Session Initiation Protocol (SIP);
5. RFC 3262 - Reliability of Provisional Responses in the Session Initiation Protocol (SIP);
6. RFC 3264 - An Offer/Answer Model with the Session Description Protocol (SDP);
7. RFC 3311 - The Session Initiation Protocol (SIP) UPDATE Method;
8. RFC 3323 - A Privacy Mechanism for the Session Initiation Protocol (SIP);
9. RFC 3325 - Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks;
10. RFC 3326 - The Reason Header Field for the Session Initiation Protocol (SIP);
11. RFC 3489 - STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs);
12. RFC 3515 - The Session Initiation Protocol (SIP) Refer Method;
13. RFC 3550 - RTP: A Transport Protocol for Real-Time Applications;
14. RFC 3551 - RTP Profile for Audio and Video Conferences with Minimal Control;
15. RFC 3581 - An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing;
16. RFC 3711 - The Secure Real-time Transport Protocol (SRTP);
17. RFC 3891 - The Session Initiation Protocol (SIP) "Replaces" Header;
18. RFC 3892 - The Session Initiation Protocol (SIP) Referred-By Mechanism;
19. RFC 4028 - Session Timers in the Session Initiation Protocol (SIP);
20. RFC 4145 - TCP-Based Media Transport in the Session Description Protocol (SDP);
21. RFC 4244 - An Extension to the Session Initiation Protocol (SIP) for Request History Information;
22. RFC 4566 - SDP: Session Description Protocol;
23. RFC 4568 - Session Description Protocol (SDP) Security Descriptions for Media Streams;
24. RFC 4571 - Framing Real-time Transport Protocol (RTP) and RTP Control Protocol (RTCP) Packets over Connection-Oriented Transport;
25. RFC 4572 - Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP);
26. RFC 4961 - Symmetric RTP / RTP Control Protocol (RTCP);
27. RFC 5009 - Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media;
28. RFC 5124 - Extended Secure RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/SAVPF);
29. RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2;
30. RFC 5245 - Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols;

31. RFC 5389 - Session Traversal Utilities for NAT (STUN);
32. RFC 5502 - The SIP P-Served-User Private-Header (P-Header) for the 3GPP IP Multimedia (IM) Core Network (CN) Subsystem;
33. RFC 5589 - Session Initiation Protocol (SIP) Call Control - Transfer;
34. RFC 5761 - Multiplexing RTP Data and Control Packets on a Single Port;
35. RFC 5764 - Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP);
36. RFC 5806 - Diversion Indication in SIP;
37. RFC 6050 - A Session Initiation Protocol (SIP) Extension for the Identification of Services;
38. RFC 6086 - Session Initiation Protocol (SIP) INFO Method and Package Framework;
39. RFC 6347 - Datagram Transport Layer Security Version 1.2;
40. RFC 7118 - The WebSocket Protocol as a Transport for the Session Initiation Protocol (SIP);
41. RFC 7315 - Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP;
42. draft-ietf-sip-183-00 - SIP 183 Session Progress Message;
43. draft-kaplan-dispatch-info-dtmf-package-00 - A Session Initiation Protocol (SIP) INFO Package for Dual-Tone Multi-Frequency (DTMF) Events.

4.1.13. **DETALHAMENTO E CARACTERÍSTICAS DO ITEM 07:**

4.1.13.1. Os aparelhos telefônicos deverão ser instalados e configurados, nas unidades informadas no item 4.1.24, com as facilidades previstas nos subitens do item 4.1.7, ativas.

4.1.13.2. Os videofones deverão ser instalados e configurados, nas unidades informadas no item 4.1.24, com as facilidades previstas nos subitens do item 4.1.7, ativas.

4.1.14. **DETALHAMENTO E CARACTERÍSTICAS DO ITEM 08:**

4.1.14.1. Treinamento oficial ministrado, pelo fabricante ou por empresa por ele credenciada, com emissão de certificado, para 15 (quinze) treinandos, onde deverá contemplar, no mínimo:

4.1.14.2. Instalação e desinstalação, manutenção e operação do sistema, incluindo os sistemas de gerenciamento e manutenção;

4.1.14.3. Instalação do software;

4.1.14.4. Configuração de ramais;

4.1.14.5. Configuração de rotas;

4.1.14.6. Configuração de remote extension;

4.1.14.7. Configuração de todas as facilidades do sistema;

4.1.14.8. Reconhecimento das indicações de alarmes, localização de falhas e substituição de gateways;

4.1.14.9. Capacitação para gerência, instalação, configuraçao e operação do sistema de tarifação, videoconferência, telefonista;

4.1.14.10. Starts e restarts;

4.1.14.11. Sistemas gerais de gerenciamento;

4.1.14.12. Backup / restore e safety backup;

4.1.14.13. Inserção e remoção de cartões/módulos;

4.1.14.14. Adição de gateways;

4.1.14.15. Instalação do LINUX, voltado para o para o software da Central Telefônica;

4.1.14.16. Sistema de arquivos do LINUX;

4.1.14.17. Permissão de acesso e atributos de arquivos.

4.1.14.18. As licitantes deverão estar aptas a promover o treinamento técnico para 15 (quinze) servidores do contratante, a fim de dotá-lo de condições técnicas para acessar o sistema PABX IP, para Administração, Manutenção e operação, bem como difundir entre os usuários as facilidades técnicas oferecidas pelo sistema;

4.1.14.19. As despesas com passagens, hospedagem, deslocamentos no destino e alimentação ficarão a cargo da CONTRATADA caso o curso não seja realizado em Brasília;

4.1.14.20. A contratada deverá fornecer todo material didático necessário para os treinamentos.

4.1.15. **DETALHAMENTO E CARACTERÍSTICA DO ITEM 09:**

4.1.15.1. Aparelho Telefônico IP tipo 01: Telefone de mesa para atender demandas de usuários que desempenham atividades de secretária ou atendentes.

4.1.15.2. Características:

a) 12 teclas de memória/programáveis ou mais;

b) LCD de 128 x 64 pixels ou superior, 02 linhas ou mais; com luz de fundo;

c) Tamanho mínimo da tela: 6 x 3 cm;

d) HD Voice;

e) Disponível com alimentação via Ethernet (PoE) integrado;

f) Deverá possuir no mínimo 02 (duas) portas Ethernet (RJ 45) de 10/100/1000 Mbps com detecção automática;

g) Suporte a IPv4 e IPv6;

h) Comutador duplo;

i) Deverá suportar a configuração via DHCP e IP fixo;

j) Suporte aos seguintes padrões e protocolos: SIP RFC 3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP/RARP, ICMP, DNS (registro A, SRV, NAPTR), DHCP, PPPoE, SSH, TFTP, NTP, STUN, SIMPLE, LLDP-MED, LDAP, TR-069, 802.1x, TLS, SRTP;

k) Qualidade de serviço (QoS) de camada 2 (802.1Q, 802.1P) e camada 3 (ToS, DiffServ, MPLS);.

l) 02 (duas) teclas de linhas com LED em duas cores e 02 (duas) contas SIP;

m) Minimo de 03 (três) sensíveis ao contexto com programação XML;

n) Minimo de 05 (cinco) teclas de navegação/menu;

o) Teclas de função exclusivas para:

1. Ajuste de volume;
2. Interrupção de som (MUTE);
3. Fone de ouvido (HEADSET);
4. Transferência;
5. Conferência;
6. Rediscagem (REDIAL);
7. Viva-Voz;
8. Agenda;
9. Espera (HOLD);
10. Início (HOME);
11. Enviar (SEND);

p) Deverá suportar os seguintes codecs: G.711µ/a, G.722, G.723, G.729 A/B, DTMF em banda e fora de banda; (em áudio, RFC2833, SIP INFO);

q) Agenda para download (XML, LDAP, mínimo de 300 itens);

r) Histórico de chamadas (mínimo de 30 registros);

s) Deverá possuir interface gráfica em inglês e português brasileiro;

t) Controle de acesso de usuário e administrador, autenticação baseada em MD5 e MD5-sess, arquivo de configuração com criptografia AES de 256 bits, TLS, SRTP, HTTPS, controle de acesso à mídia 802.1x;

u) Áudio em HD, aparelho e viva-voz com suporte e áudio em banda larga;

v) Inglês, Espanhol, Português;

w) Compatibilidade com Headset Conector RJ 9, compatível com EHS;

x) Deverá ser compatível com o padrão IEEE 802.3af (POWER OVER ETHERNET – POE);

y) Fonte de alimentação automática entrada 100-240 VCA;

z) Deverá permitir o mínimo de dois ângulos de posições diferentes;

aa) Suporte de parede;

ab) Upgrade de firmware via TFTP/HTTP/HTTPS, provisionamento em massa usando um arquivo de configuração XML com criptografia AES ou TR-069;

ac) Indicador de status das linhas;

ad) Encaminhamento (incondicional/sem resposta/ocupado);

ae) Correio de voz, prompt de voz, mensagem de voz;

af) Discagem rápida;

ag) Chamada em espera;

ah) Chamada em espera para conferência/captação de chamadas;

ai) Conferência de três vias, SIP MESSAGE (Instant Message);

aj) Exibição de chamadas compartilhadas (SCAm shared call appearance)/exibição de linhas transferidas (BLA, bridged line appearance);

ak) Discagem automática com aparelho ocupado;

al) Agenda para download (XML, LDAP, mínimo de 300 itens);

am) Resposta automática;

an) Histórico de chamadas (mínimo de 100 registros);

ao) Rediscagem;

ap) Plano de discagem flexível, uso compartilhado de recursos;

aq) Toques musicais personalizados;

ar) Redundância de servidores e failover;

as) Discagem rápida;

4.1.16. **DETALHAMENTO E CARACTERÍSTICA DO ITEM 10:**

4.1.16.1. Aparelho Telefônico IP tipo 02: Telefone de mesa para atender demandas de usuários que desempenham atividades de Chefia, Diretoria, Coordenação, Administrador, Gerente.

4.1.16.2. Características:

a) Display LCD de 128 x 64 pixels ou superior, 02 linhas ou mais; com luz de fundo;

b) Tamanho mínimo da tela: 6 x 3 cm;

c) Deverá possuir no mínimo 02 (duas) portas Ethernet (RJ 45) de 10/100/1000 Mbps com detecção automática;

d) Suporte a IPv4 e IPv6;

e) Comutador duplo;

f) PoE integrado;

g) Deverá suportar a configuração via DHCP e IP fixo;

h) Suporte aos seguintes padrões e protocolos: SIP RFC 3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP/RARP, ICMP, DNS (registro A, SRV, NAPTR), DHCP, PPPoE, SSH, TFTP, NTP, STUN, SIMPLE, LLDP-MED, LDAP, TR-069, 802.1x, TLS, SRTP;

i) Qualidade de serviço (QoS) de camada 2 (802.1Q, 802.1P) e camada 3 (ToS, DiffServ, MPLS);

j) 02 (duas) teclas de linhas com LED em duas cores e 02 (duas) contas SIP;

k) Mínimo de 03 (três) sensíveis ao contexto com programação XML;

l) Teclas programáveis para mínimo 04 (quatro) números de memória;

m) Mínimo de 05 (cinco) teclas de navegação/menu;

n) Possuir teclas individuais para as seguintes funções: Ajuste de volume, interrupção de som (mute), fone de ouvido (headset), Transferência, Rediscagem (redial), Conferência, Viva-Voz, Agenda, Início (home), Espera (hold), Enviar (send);

o) Deverá suportar os seguintes codecs: G.711μ/a, G.722, G.723, G.729 A/B, G.726-32, DTMF em banda e fora de banda (em áudio, RFC2833, SIP INFO), VAD, CNG, AEC, PLC;
p) Agenda para download (XML, LDAP, mínimo de 300 itens);
q) Histórico de chamadas (mínimo de 30 registros);
r) Deverá possuir interface gráfica em português brasileiro;
s) Controle de acesso de usuário e administrador, autenticação baseada em MD5 e MD5-sess, arquivo de configuração com criptografia AES de 256 bits, TLS, SRTP, HTTPS, controle de acesso à mídia 802.1x;
t) Áudio em HD, aparelho e viva voz com suporte e áudio em banda larga;
u) Compatibilidade com Headset Conector RJ 9, compatível com EHS;
v) Deverá ser compatível com o padrão IEEE 802.3af (POWER OVER ETHERNET – POE);
w) Fonte de alimentação automática entrada 100-240 VCA;
x) Deverá permitir o mínimo de dois ângulos de posições diferentes;
y) Upgrade de firmware via TFTP/HTTP/HTTPS, provisionamento em massa usando um arquivo de configuração XML com criptografia AES ou TR-069;
z) Indicador de status das linhas;
aa) Transferência;
ab) Espera;
ac) Encaminhamento (incondicional/sem resposta/ocupado);
ad) Correio de voz, prompt de voz, mensagem de voz;
ae) Discagem rápida;
af) Chamada em espera;
ag) Chamada em espera para conferência/captação de chamadas;
ah) Conferência de três vias, SIP MESSAGE (Instant Message);
ai) Exibição de chamadas compartilhadas (SCAm shared call appearance)/exibição de linhas transferidas (BLA, bridged line appearance);
aj) Discagem automática com aparelho ocupado;
ak) Agenda para download (XML, LDAP, mínimo de 300 itens);
al) Resposta automática;
am) Histórico de chamadas (mínimo de 100 registros);
an) Rediscagem;
ao) Plano de discagem flexível, uso compartilhado de recursos;
ap) Toques musicais personalizados;
aq) Redundância de servidores e failover;
ar) Discagem rápida.

4.1.17. **DETALHAMENTO E CARACTERÍSTICA DO ITEM 11:**

4.1.17.1. Aparelho Telefônico IP tipo 03: Telefone de mesa para atender demandas de usuários que desempenham atividades consideradas comuns, que não correspondem aos itens 07 e 08.

4.1.17.2. Características:

a) Display LCD gráfico com resolução de 128 x 64, ou superior, com luz de fundo;
b) Tamanho mínimo da tela: 6 x 2 cm;
c) Deverá possuir no mínimo 02 (duas) portas Ethernet de 10/100/1000 Mbps com detecção automática;
d) Suporte a IPv4 e IPv6;

e) Comutador duplo;

f) PoE integrado;

g) Deverá suportar a configuração via DHCP e IP fixo;

h) Suporte aos seguintes padrões e protocolos: SIP RFC 3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP/RARP, ICMP, DNS (registro A, SRV, NAPTR), DHCP, PPPoE, SSH, TFTP, NTP, STUN, SIMPLE, LLDP-MED, LDAP, TR-069, 802.1x, TLS, SRTP;

i) Qualidade de serviço (QoS) de camada 2 (802.1Q, 802.1P) e camada 3 (ToS, DiffServ, MPLS);

j) 02 (duas) teclas de linhas com LED em duas cores e 02 (duas) contas SIP;

k) Mínimo de 03 (três) sensíveis ao contexto com programação XML;

l) Teclas programáveis para 08 (oito) ramais com BLF ou lista telefônica;

m) Mínimo de 05 (cinco) teclas de navegação/menu;

n) Possuir teclas individuais para as seguintes funções: Ajuste de volume, interrupção de som (mute), fone de ouvido (headset), Transferência, Rediscagem (redial), Conferência, Viva-Voz, Agenda, Início (home), Espera (hold), Enviar (send);

o) Deverá suportar os seguintes codecs: G.711μ/a, G.722, G.723, G.729 A/B, G.726-32, DTMF em banda e fora de banda (em áudio, RFC2833, SIP INFO), VAD, CNG, AEC, PLC;

p) Agenda para download (XML, LDAP, mínimo de 300 itens);

q) Histórico de chamadas (mínimo de 30 registros);

r) Deverá possuir interface gráfica em português brasileiro;

s) Controle de acesso de usuário e administrador, autenticação baseada em MD5 e MD5-sess, arquivo de configuração com criptografia AES de 256 bits, TLS, SRTP, HTTPS, controle de acesso à mídia 802.1x;

t) Áudio em HD, aparelho e viva voz com suporte e áudio em banda larga;

u) Compatibilidade com Headset Conector RJ 9, compatível com EHS;

v) Deverá ser compatível com o padrão IEEE 802.3af (POWER OVER ETHERNET – POE);

w) Fonte de alimentação automática entrada 100-240 VCA;

x) Deverá permitir o mínimo de dois ângulos de posições diferentes;

y) Upgrade de firmware via TFTP/HTTP/HTTPS, provisionamento em massa usando um arquivo de configuração XML com criptografia AES ou TR-069;

z) FCC: Part 15 (CFR 47) Class B, CE : EN55022 Class B, EN55024, EN61000-3-2, EN61000-3-3, EN60950-1, RCM: AS/ACIF S004; AS/NZS CISPR22/24; AS/NZS 60950; AS/NZS 60950.1;

aa) Indicador de status das linhas;

ab) Encaminhamento (incondicional/sem resposta/ocupado);

ac) Correio de voz, prompt de voz, mensagem de voz;

ad) Discagem rápida;

ae) Chamada em espera para conferência/captação de chamadas;

af) Conferência de três vias, SIP MESSAGE (Instant Message);

ag) Exibição de chamadas compartilhadas (SCAm shared call appearance)/exibição de linhas transferidas (BLA, bridged line appearance);

ah) Discagem automática com aparelho ocupado;

ai) Agenda para download (XML, LDAP, mínimo de 300 itens);

aj) Resposta automática;

ak) Histórico de chamadas (mínimo de 100 registros);

al) Rediscagem;

am) Plano de discagem flexível, uso compartilhado de recursos;

an) Toques musicais personalizados;

ao) Redundância de servidores e failover;

ap) Discagem rápida.

4.1.18. **DETALHAMENTO E CARACTERÍSTICA DO ITEM 12:**

4.1.18.1. Aparelho Video Fone IP: Aparelho Video Fone de mesa para atender demandas de usuários que utilizam com frequência o serviço de Videoconferência.

4.1.18.2. Características:

a) Deverá possuir 02 (duas) portas, suportando switch entre as portas, com velocidade de 10/100/1000 MBPS Giga Ethernet.

b) Deverá possuir interface de rádio para rede wireless interno conforme o IEEE 802.11 a/b/g/n, 6.3.

c) Deverá possuir interface Bluetooth 4.0 suportando conexão e utilização com headset que suportem esta tecnologia.

d) Deverá suportar a redundância no servidor de chamadas.

e) Deverá salvar Log de eventos em servidor.

f) Deverá suportar QoS segundo IEEE 802.1p/Q tagging (VLAN), Layer 3 TOS e DSCP.

g) Deverá suportar provisionamento através de protocolos seguros como HTTPS ou outro.

h) Deverá possuir relatório de status e estatísticas de funcionamento.

i) Deverá suportar a configuração IP manualmente e via DHCP.

j) Deverá suportar sincronismo de tempo com o sistema central de telefonia.

k) Deverá implementar o protocolo LLDP e LLDP-MED.

l) Deverá possuir identificação de presença, mostrando no display o status de outros usuários, tais como: Off-line, Disponível, Ausente, Ocupado e Não perturbe.

m) Deverá suportar assinatura de arquivos de firmware.

n) Deverá possuir Login via senha de usuário.

o) Deverá suportar Transport Layer Security (TLS) para trafego de sinalização e SRTP para tráfego de voz e vídeo.

p) Deverá suportar a autenticação e criptografia das chamadas telefônicas de voz e vídeo, de forma nativa e com indicação no display destas funcionalidades.

q) Deverá implementar chaves de criptografia no padrão AES de no mínimo 128bits.

r) Deverá suportar provisionamento seguro.

s) Deverá possuir interface RJ-09 dedicada para conexão com a headsets, não sendo aceito o compartilhamento desta interface com o Handset.

t) Deverá possibilitar conexão com monitor externo, através de interface HDMI.

u) Deverá possuir câmera de vídeo acoplada ao videofone para realização de vídeo chamadas, com resolução “Full HD” (1080p 30fps).

v) A câmera poderá ser integrada ao telefone ou acopladas, fixando-se perfeitamente ao aparelho. Neste último caso, a câmera deverá constar na documentação oficial do telefone.

w) Permitir o usuário desabilitar a câmera durante uma chamada, mantendo apenas o envio do áudio.

x) Deverá possuir Certificação da ANATEL.

y) Deverá suportar temperatura de operação entre +10ºC a +40°C.

z) Deverá suportar humidade relativa de 20% a 80% sem condensação.

aa) Deverá ser do mesmo fabricante Central Telefônica VoIP Redundante, ou deverá ser homologado pelo mesmo para esta função, não sendo aceitos sistemas de terceiros. Isto visa garantir uma melhor integração de todo o ecossistema de telefonia e gerência.

ab) Deverá ser compatível o padrão IEEE 802.3at (Power Over Ethernet +) até classe3 sendo desejável Classe 4.

ac) Deverá possuir 03 (três) linhas (Protocolo SIP IETF RFC 3261) com tecla dedicada no display sensível ao toque, para seleção de linhas e indicação de chamada e ocupação com display.

ad) Possuir display do tipo matriz gráfica de LCD colorido com ajuste de ângulo, do tipo “touch screen” (sensível ao toque) com tecnologia capacitiva, com resolução de 1280x800 pixels, tamanho de 7 polegadas (medida diagonal), com o vídeo da chamada sendo apresentada neste display, e com informações no idioma Português.

ae) Deverá possuir web browser, sendo desejável o suporte a HTML5.

af) Deverá possuir integração de calendário com sistema de correio eletrônico, de forma a permitir a visualização dos compromissos na tela do aparelho telefônico.

ag) Deverá possuir viva-voz full-duplex.

ah) Deverá possuir Resposta de Frequência de 150 Hz – 7000 Hz para operação com monofone, headset e viva-voz.

ai) Deverá suportar os codecs G.711, G.729 e G.722, com as codificações e compressões de voz sempre ocorrendo diretamente no aparelho.

aj) Deverá suportar pelo menos o codec H.264 BP, sendo desejável H.264 AVC e H.264 High Profile, suportando no mínimo as resoluções (pixels) 1280x720 e 1920x1080, e com as codificações e compressões de vídeo sempre ocorrendo diretamente no aparelho.

ak) Deverá suportar detecção de atividade de voz (VAD).

al) Deverá suportar geração de ruído de conforto.

am) Deverá suportar Geração de DTMF e transmissão de DTMF pelo tráfego RTP.

an) Deverá suportar transmissão dos pacotes de áudio com baixo delay.

ao) Deverá suportar jitter e buffer adaptativo para compensar as condições de rede.

ap) Deverá possuir dispositivo para compensar a perda de pacotes.

aq) Deverá suportar cancelamento de eco.

ar) Deverá suportar supressão de ruídos de fundo.

as) Devera suportar temporizador de chamada.

at) Deverá suportar toque de chamada diferenciado.

au) Deverá suportar login/logout do telefone.

av) Deverá suportar transferência de chamada.

aw) Deverá suportar chamada em espera.

ax) Deverá suportar audioconferência a seis participantes.

ay) Deverá possuir discagem rápida e rediscagem.

az) Deverá possuir notificação de chamadas perdidas.

ba) Deverá suportar desvio de chamada quando ocupado, de chamada quando não atendida, e desvio incondicional de chamadas.

bb) Deverá suportar estacionamento de chamadas.

bc) Deverá suportar captura de chamadas em grupo e de ramal específico.

bd) Deverá suportar a opção de não perturbe.

be) Deverá possuir display de relógio.

bf) Deverá possuir histórico de chamadas e lista de contatos.

bg) Deverá possuir 03 (três) teclas para linhas diretamente no display sensível ao

bh) Deverá possuir sinalização de nova mensagem no correio de voz.

bi) Deverá possuir teclas de controle de volume (Up and down).

bj) Deverá possuir tecla de seleção de headset com Led.

bk) Deverá possuir tecla de viva-voz com Led.

bl) Deverá possuir tecla “mudo” para áudio com Led.

bm) Deverá possuir tecla “mudo” para vídeo com Led.

bn) Deverá possuir tecla de histórico e contatos.

4.1.19. A Empresa CONTRATADA deve fornecer todos os códigos fonte e acessos aos programas, servidores e equipamentos para total controle do Sistema de Telefonia, permitindo a CONTRATANTE gerência e controle global para, caso necessário, configurar, ampliar, remover, integrar o Sistema, sem, contudo, fazer aquisição de licenças e ou autorização junto a Empresa CONTRATADA.

4.1.20. A CONTRATADA deve fornecer mão de obra especializada para instalação e programação do sistema com fornecimento de materiais e softwares necessários.

4.1.21. Deve garantir a continuidade de uso dos equipamentos de voz, a fim de que sejam equipados para o funcionamento integrado via rede IP com a Central Telefônica Marca ERICSSON, Modelo MD 110, Versão BC13-TSW, como se fosse um único PABX com transparência total de facilidades básicas, até a sua total substituição.

4.1.22. Deverá ser elaborado pela CONTRATADA em até 15 (quinze) dias a contar da data de emissão da Ordem de Serviço pela Fiscalização, um cronograma de implantação da solução que deverá ser elaborado em conjunto com a Divisão de Telecomunicações - DITEL da PF;

4.1.23. Toda instalação e ampliação da central deve ser visto como um projeto único e integrado, devendo compor um sistema completo de telefonia híbrida (IP e TDM), a ser implementado gradualmente;

4.1.24. Os softwares, hardware e demais componentes deverão ser instalados nas unidades da PF em Brasília/DF:

4.1.24.1. SR - Superintêndia da Pólicia Federal;

4.1.24.2. CGTI - Coordenação Geral de Tecnologia da Informação;

4.1.24.3. COT - Coordenação de Operações Táticas;

4.1.24.4. DIP - Diretoria de Inteligência Policial;

4.1.24.5. DAT - Divisão Antiterrorismo;

4.1.24.6. INI - Instituto Nacional de Identificação;

4.1.24.7. INC - Instituto Nacional de Criminalística;

4.1.24.8. DSG - Divisão de Serviços Gerais;

4.1.24.9. CAOP - Coordenação de Aviação Operacional;

4.1.24.10. CGCI - Coordenação Geral de Cooperação Internacional;

4.1.24.11. ANP - Academia Nacional de Polícia;

4.1.24.12. DG - Direção Geral (Edifício Sede)

4.1.25. Os Gateways IPs deverão ser instalados nas salas de equipamentos dos prédios das unidades da PF em Brasília/DF;

4.1.26. A conexão dos troncos E1 do equipamento com a RTPC deverá ser realizada nas Unidades da PF em Brasília/DF, configurados de forma a permitir que, em caso de falha ou queda da conexão IP entre essas Unidades, os ramais possam realizar e receber ligações externas (sobrevivência local);

4.1.27. Ficarão por conta da proponente vencedora todas as despesas de transporte, estadias, alimentação, etc, necessárias para atendimento do item objeto desta licitação;

4.1.28. Caberá à Divisão de Telecomunicações - DITEL julgar a qualidade dos serviços executados, podendo a qualquer momento impugnar parte ou totalidade destes serviços que não estejam de acordo com as disposições técnicas previamente aprovadas;

4.1.29. As instalações das soluções deverão ocorrer em horários que não compreendam o horário comercial, inclusive em finais de semana e feriado, ficando a critério desta Administração que realizará o agendamento com a CONTRATADA. A execução das atividades fora do horário comercial não implicará custos adicionais para esta Coordenação/Divisão;

4.1.30. Todo o material, que se fizer necessário, será de responsabilidade da Proponente;

4.1.31. A solução de telefonia IP deverá implementar seleção de rota de menor custo (LCR - LeastCostRoute) para chamadas de longa distância, sem a necessidade de digitar um código de rota específico;

4.1.32. A solução de telefonia IP deverá implementar seleção de rota de menor custo (LCR - LeastCostRoute) para chamadas de longa distância, sem a necessidade de digitar um código de rota específico;

4.1.33. Deverá fornecer rotas alternativas para as chamadas, em caso de indisponibilidade do destino, de forma totalmente transparente ou informativa ao usuário (podendo ser configurada pelo administrador do sistema esta funcionalidade). Deste modo, caso a solução de telefonia IP detecte que o número de destino se encontra indisponível, não registrado, ou de insuficiência de recursos para realização da chamada através da rede WAN, o mesmo deverá encaminhar automaticamente a chamada para a RPTC;

4.1.34. O plano de numeração hoje existente não deverá ser alterado, e deverá ficar em pleno funcionamento mesmo durante a implantação do projeto;

4.1.35. A solução de telefonia IP deve ter a capacidade de permitir a mobilidade de usuários, mediante a digitação de conta e senha, habilitando todas as funcionalidades de seu ramal de origem, em qualquer outro ponto do sistema proposto, sendo sempre tarifado pelo código de origem, e não pelo ramal físico onde foi realizada a ligação;

4.1.36. A solução deve possibilitar a centralização, em um único ponto da rede das chamadas telefônicas, mesmo DDR, sendo encaminhadas aos usuários finais de forma automática;

4.1.37. A solução deverá ser fornecida com suporte a QSIG;

4.1.38. A CONTRATADA será responsável pela elaboração, execução e acompanhamento de cronograma de instalação dos equipamentos e seus respectivos componentes que fazem parte da proposta da CONTRATADA;

4.1.39. Deverá ser realizada uma reunião entre a CONTRATADA e a PF para discussão do cronograma de instalação/ampliação;

4.1.40. A instalação de todos os itens será executada pela CONTRATADA com apoio e supervisão da PF.

4.1.41. Dos testes:

4.1.41.1. Quando do término das instalações, a CONTRATADA deverá realizar, na presença de um representante da PF, os testes de funcionamento dos sistemas;

4.1.41.2. Durante 05 (cinco) dias úteis após a instalação de toda a solução, a CONTRATADA deverá realizar o suporte assistido, devendo para isso manter um técnico residente por 4 (quatro) horas diárias nas instalações da PF, a fim de sanar qualquer problema que venha a ocorrer no novo sistema telefônico proveniente da instalação e ampliação.

5. ESPECIFICAÇÕES DOS SERVIÇOS E ENTREGA DOS EQUIPAMENTOS

5.1. Os serviços de instalação e expansão objeto deste Termo de Referência caracterizam-se pela aplicação de mão-de-obra especializada, com técnicos treinados e certificados por entidade reconhecida ou pelo fornecedor da central telefônica, para implementação de tecnológica contemplando ampliação e instalação de Software, Hardware e demais componentes necessários.

5.2. Os serviços de instalação e expansão deverão ser compatíveis com o sistema de telefonia existente e instalado na Polícia Federal em Brasília/DF;

5.3. Os serviços de instalação e expansão deverão ser efetuados, obrigatoriamente, de forma a não afetar o funcionamento dos sistemas, recursos e/ou equipamentos atualmente em operação, nem impedir ou interromper por períodos prolongados a rotina de trabalho dos servidores da PF.

5.3.1. Havendo necessidade de interrupção de outros sistemas, recursos, equipamentos e/ou rotinas dos trabalhos da PF, em decorrência dos serviços, esta alteração deverá estar devidamente planejada e acordada anteriormente com a Administração.

5.4. Os materiais a serem empregados e os serviços a serem executados deverão obedecer rigorosamente:

5.4.1. Às normas e especificações constantes deste Termo de Referência;

5.4.2. Às normas da ABNT;

5.4.3. Às prescrições e recomendações dos fabricantes dos equipamentos e peças;

5.4.4. Às normas internacionais, na falta de normas da ABNT (ITU-T, ISSO, ANSI, IEEE, EIA/TIA, etc).

5.5. Deverá atender aos requisitos técnicos mínimos das Normas Técnicas da ABNT e ANATEL vigentes relativos às Centrais Privadas de Comutação Telefônica (CPCT) tipo PABX CPA-T;

5.6. Todos os equipamentos, materiais, peças, componentes e acessórios a serem utilizados nos serviços deverão ser novos e originais e farão parte do acervo patrimonial do CONTRATANTE, a partir do seu recebimento definitivo;

5.7. A CONTRATADA deverá realizar toda a instalação dos equipamentos, incluindo suas configurações, meio físico, cabeamento em VOICE PANEL, instalação interna e externa, obras eventuais para a acomodação do meio físico e/ou equipamentos e quaisquer outras providências que tenham relação direta ou indireta com a instalação dos mesmos. A CONTRATANTE fornecerá apenas o local e alimentação elétrica para a instalação dos equipamentos.

5.8. Caso a licitante necessite fornecer hardwares e/ou softwares adicionais não especificados nominalmente nesse edital, mas necessários para atender as funcionalidades e capacidades exigidas nas especificações previstas, o custo desses deverão estar inseridos no preço total ofertado.

5.9. Os equipamentos dos itens 09, 10, 11 e 12 compreendem apenas fornecimento dos aparelhos telefônicos e videofones. A instalação e configuração dos aparelhos telefônicos e videofones indicados nos itens 09, 10, 11 e 12 será de responsabilidade da empresa vencedora dos itens do grupo 01, da tabela exposta no item 4.1, conforme orientações do item 22.

5.9.1. Os equipamentos dos intens 09 ao 12 devem ser entregues conforme demanda apresentada pela contratante.

6. DA CLASSIFICAÇÃO DOS BENS E SERVIÇOS

6.1. Trata-se de processo para prestação de serviços de ampliação, modernização e atualização, com substituição de hardware e software, do sistema telefônico instalado nas Unidades da Polícia Federal em Brasília/DF, classificados, respectivamente, como serviços e bens comuns, nos termos do parágrafo único do art. 1º da Lei nº 10.520/02, visto que os padrões de desempenho e qualidade do objeto podem ser objetivamente definidos pelo edital, por meio de especificações usuais do mercado.

6.2. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto n° 2.271, de 1997, constituindo-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal do órgão licitante, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

6.3. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

7. DO TIPO DE LICITAÇÃO

7.1. A estratégia é de realização de licitação na modalidade **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO POR LOTE**, para os itens **01, 02, 03, 04, 05, 06, 07 e 08 (grupo 01)**, e a realização de licitação na modalidade de **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO POR ITEM**, para os itens 09, 10, 11 e 12.

7.2. Os itens 01, 02, 03, 04, 05, 06, 07 e 08 (grupo 01) comporão um LOTE ÚNICO, mediante contrato único, já que são serviços complementares pelo qual a CONTRATADA será a única responsável.

7.3. Os itens 09, 10, 11 e 12, visando aumentar a competitividade do certame, serão licitados **por itens**.

8. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

AVALIAÇÃO TECNICA

8.1. Serão desclassificadas as propostas que não apresentem a habilitação técnica na forma e conteúdo exigidos neste Termo de Referência.

8.2. Serão desclassificadas as propostas que não atendam às demais exigências deste Termo de Referência, de seus Anexos e da Legislação vigente.

8.3. Serão desclassificadas, ainda, as propostas que sejam omissas, vagas ou apresentem irregularidades e defeitos capazes de dificultar o julgamento objetivo.

AVALIAÇÃO DE PREÇO

8.4. Será considerada vencedora a licitante que atender todas as regras do termo de referência, do edital, dos seus anexos e apresentar o MENOR PREÇO PARA CADA ITEM.

8.5. Será assegurada, como critério de desempate, preferência de contratação para as microempresas e empresas de pequeno porte, conforme previsto no Capítulo V da Lei Complementar nº 123, de 2006.

9. PROPOSTA

9.1. A apresentação da proposta implicará em plena aceitação, por parte da licitante, das condições estabelecidas neste instrumento.

9.2. A validade da proposta não poderá ser inferior a 60 (sessenta) dias consecutivos, contados da entrega.

9.3. São itens obrigatórios da proposta:

9.3.1. Razão social, nome fantasia, CNPJ, endereço completo, telefone e endereço eletrônico da licitante proponente;

9.3.2. Nome, documento de identificação, endereço completo, telefone, endereço eletrônico, cargo, função e tipo de vínculo com a empresa, do responsável pela apresentação da proposta;

9.3.3. Valor unitário e valor total da proposta, expressos em moeda corrente nacional, em algarismo e por extenso, neles incluídos todos os impostos, taxas, salários, encargos sociais e trabalhistas, contribuições previdenciárias e demais obrigações e despesas de qualquer natureza, necessárias à perfeita execução dos serviços especificados neste instrumento.

9.3.4. Prazo de validade da proposta, não inferior a 60 (sessenta) dias consecutivos, contados a partir da data de apresentação da proposta.

9.3.5. Assinatura do responsável pela apresentação da Proposta.

9.3.6. Assinatura do representante legal da empresa.

9.4. Será desclassificada a proposta elaborada em desacordo com este Termo de Referência, que se oponha a qualquer dispositivo legal vigente, que contenha preços excessivos ou manifestamente inexequíveis, preços simbólicos ou irrisórios, ou ainda, vantagens ou preços baseados nas ofertas dos demais licitantes. Também não serão consideradas as propostas que impuserem condições diferentes das dispostas no edital de licitação, que apresentarem irregularidades ou defeitos capazes de dificultar o julgamento ou que não atenderem aos requisitos mínimos discriminados no edital.

9.5. A proposta deverá conter as especificações do objeto de forma clara, descrevendo detalhadamente as características técnicas dos serviços ofertados, incluindo especificação de marca, soluções, procedência e outros elementos que de forma inequívoca identifiquem e constatem as configurações cotadas, comprovando-os através de certificados, manuais técnicos, folders e demais literaturas editadas pelo fabricante.

9.6. Na proposta deverão ser apresentadas quaisquer outras informações afins, que a proponente julgar necessárias ou convenientes.

9.7. As propostas que não atenderem à totalidade das características obrigatórias serão desclassificadas.

9.8. O preço deve ser apresentado segundo o modelo contido no ANEXO I deste Termo de Referência.

9.9. Havendo divergência entre as características técnicas descritas na proposta da Licitante e as disponibilizadas pelo fabricante (como informes técnicos, manual técnico que descreve os serviços e ferramentas, folders ou prospectos técnicos), prevalecerão os informes do fabricante, salvo os casos específicos em que o Licitante esclareça os motivos da divergência e que sejam aceitos pela CONTRATANTE.

10. QUALIFICAÇÃO TÉCNICA

10.1. As licitantes deverão apresentar pelo menos 1 (um) Atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, comprovando que prestou ou está prestando serviços compatíveis em características, com mínimo de 50% das quantidades e prazos com o objeto ora licitado;

10.2. A empresa vencedora deste processo licitatório, para a assinatura do contrato, deverá comprovar que possui em seu quadro técnico pessoal com as certificações abaixo:

10.2.1. Certificação DCAP – Digium Certified Asterisk Professional;

10.2.2. Certificação DCAA – Digium Certified Asterisk Administration;

10.2.3. O responsável técnico deverá apresentar registro no CREA;

10.3. A eventual substituição do responsável técnico será realizada mediante solicitação prévia ao CONTRATANTE, e o novo profissional deverá atender aos requisitos mínimos definidos no item 10.2.

11. VISTORIA TÉCNICA

11.1. É aberta aos licitantes a vistoria ao local do serviço, antes da apresentação de suas propostas;

11.2. A vistoria deverá ser agendada em dia útil com servidor da Divisão de Telecomunicações (DITEL), por meio do telefone (61) 2024-9999;

11.3. Qualquer dúvida ou irregularidade observada durante a vistoria deverá ser previamente esclarecida junto ao CONTRATANTE, por escrito, visto que, depois de apresentada a proposta, não se acolherá nenhuma reivindicação intempestiva;

11.4. A vistoria técnica será obrigatória, assim a CONTRATADA será detentora de pleno conhecimento das condições e peculiaridades inerentes à natureza dos serviços, assumindo total responsabilidade por esse fato, evitando portanto, quaisquer questionamentos futuros que ensejem avenças técnicas ou financeiras com o CONTRATANTE.

12. DA SUBCONTRATAÇÃO

12.1. Não será admitida a subcontratação do objeto licitatório.

13. ALTERAÇÃO SUBJETIVA

13.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

14. OBRIGAÇÕES DA CONTRATADA

14.1. A CONTRATADA deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

14.1.1. Providenciar junto ao CREA-DF a Anotação de Responsabilidade Técnica (ART) referente ao objeto deste Termo de Referência, nos termos da Lei n° 6.496/77;

14.1.2. Solicitar previamente a autorização para os serviços executados nos Edifícios das Unidades, bem como o acesso dos trabalhadores, os quais serão submetidos à autorização da Instituição, ora CONTRATANTE.

14.1.3. Solicitar previamente a execução de serviços fora do expediente e nos finais de semana, não ensejando custos adicionais à CONTRATANTE.

14.1.4. Responsabilizar-se integralmente pelo fiel cumprimento do objeto contratado;

14.1.5. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia;

14.1.6. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

14.1.7. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

14.1.8. Comunicar à CONTRATANTE, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

14.1.9. Indicar preposto para representá-la durante a execução do contrato.

14.1.10. Manter o empregado nos horários predeterminados pela Administração;

14.1.11. Responsabilizar-se pela aprovação do Projeto nos Órgãos Competentes;

14.1.12. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica, normas e legislação;

14.1.13. Agendar durante o período de garantia, com o Gestor do Contrato, visita trimestral, a fim de realizar manutenção preventiva nos equipamentos;

14.1.14. Fornecer toda documentação técnica em português (em mídia ou papel) necessária à manutenção e operação do sistema;

14.1.14.1. A documentação a ser fornecida deverá conter, no mínimo: documentação sobre a operação e manutenção do sistema, que contenha as especificações físicas, operacionais e de manutenção / descrição funcional de comandos e alarmes / procedimentos de carga / inicialização e localização de defeitos / manual de diagnose para interpretação de relatórios de falhas / manual de operação dos sistemas de gerenciamento / documentação do projeto que contenha as condições de alimentação elétrica e ambientais de funcionamento, disposição física e especificações operacionais.

14.1.15. Fornecer o Certificado de Homologação de Produtos de Telecomunicações dos equipamentos expedido pela Agência Nacional de Telecomunicações – ANATEL;

14.1.16. Fornecer os produtos nas suas condições de fabricação, operação, manutenção, funcionamento, alimentação e instalação que obedeçam integralmente as normas e recomendações em vigor, baixadas pelos órgãos oficiais competentes ou entidades autônomas reconhecidas na área (ANATEL, ABNT, Ministério das Comunicações) e de entidade geradoras de padrões reconhecidas internacionalmente (ITU-T/CCITT, IETF, ISO, EIA-TIA, IEEE, CCIR, etc.), no que for aplicável;

14.1.17. Apresentar um cronograma que deverá estabelecer os prazos das etapas de entrega dos projetos e dos materiais, instalação dos equipamentos, e período de funcionamento;

14.1.18. Apresentar ao Gestor do contrato um cronograma detalhado da instalação e migração do sistema, definindo todos os produtos e serviços ofertados e sua atuação/interligação, todos os componentes adicionais, incluindo a metodologia para a migração gradual e transparente, bem como a sua implantação, no prazo máximo de cinco dias úteis após a instalação do sistema;

14.1.19. Realizar todos os ensaios, verificações e testes dos materiais, equipamentos fornecidos, instalações e serviços executados, bem como dos reparos necessários à entrega dos serviços em perfeitas condições;

14.1.20. Substituir os equipamentos instalados por novos, primeiro uso, equivalentes e totalmente compatíveis, durante o período de garantia, sempre que apresentarem três ou mais defeitos que comprometam o seu uso normal, dentro de um período de trinta dias corridos;

14.1.21. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, mantendo seu pessoal equipado disponibilizando, às suas expensas, materiais e equipamentos, ferramentas e utensílios necessários à execução dos serviços;

14.1.22. Utilizar empregados habilitados e com conhecimentos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

14.1.23. Apresentar os empregados devidamente uniformizados e identificados por meio de crachá, tendo suas funções legalmente registradas em carteira de trabalho;

14.1.24. Quando necessário à execução dos serviços, utilizar equipamentos de proteção individual (EPI);

14.1.25. Apresentar à CONTRATANTE a relação nominal dos empregados que adentrarão o órgão para a execução do serviço;

14.1.26. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;

14.1.27. Substituir imediatamente, de modo a não interromper o andamento dos serviços, qualquer empregado cuja atuação, permanência e/ou comportamento sejam julgados prejudiciais, inconvenientes e/ou insatisfatórios pela CONTRATANTE;

14.1.28. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a CONTRATADA relatar à CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

14.1.29. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE;

14.1.30. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

14.1.31. Não transferir a outrem, no todo ou em parte, o objeto da presente especificação, sem prévia e expressa anuência da CONTRATANTE;

14.1.32. Responsabilizar-se por qualquer atendimento médico de seus empregados, por acidente ou mal súbito, ocorrido dentro da área de local de trabalho;

14.1.33. Prestar todos os esclarecimentos solicitados pela FISCALIZAÇÃO, atendendo prontamente todas as reclamações ou solicitações;

14.1.34. Cumprir os prazos estipulados pela FISCALIZAÇÃO. Caso haja necessidade de maior prazo, a CONTRATADA deverá formalizar imediata comunicação ao CONTRATANTE, justificando as causas e propondo novos prazos;

14.1.35. Responsabilizar-se pela qualidade dos serviços, devendo corrigir às suas expensas os serviços que o CONTRATANTE julgar insatisfatórios;

14.1.36. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

14.1.37. Responsabilizar-se por quaisquer serviços executados em desacordo com as normas técnicas vigentes e pelas consequências resultantes de tais serviços;

14.1.38. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, causados diretamente ou indiretamente ao CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços, ficando a CONTRATANTE autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos;

14.1.39. Não modificar as especificações dos serviços sem autorização por escrito da FISCALIZAÇÃO. Os casos não abordados serão definidos pelo CONTRATANTE, de maneira a manter o padrão de qualidade previsto para os serviços em questão;

14.1.40. Comunicar imediatamente à FISCALIZAÇÃO qualquer fato extraordinário ou anormal que ocorra durante a execução dos serviços, para a adoção de medidas cabíveis, bem como, comunicar, por escrito e de forma detalhada, todo tipo de acidente que eventualmente venha a ocorrer;

14.1.41. Executar os serviços sem prejuízo do funcionamento normal das atividades do CONTRATANTE, devendo adotar todas as medidas de proteção necessárias, com vistas ao livre trânsito das áreas;

14.1.42. Executar os serviços com o máximo esmero, devendo ser imediatamente refeitos aqueles que a juízo do CONTRATANTE, não forem julgados em condições satisfatórias ou forem constatados vícios, defeitos, imperfeições ou incorreções, sem que caiba qualquer acréscimo no preço contratado, ainda que em decorrência se torne necessário ampliar o horário da prestação dos serviços, conforme previsto no art. 69 da Lei nº 8.666/93;

14.1.43. Deixar, após os serviços, as instalações com bom aspecto, não sendo admitidos desalinhamentos, desleixo nas instalações, que não inspirem segurança e que sejam desagradáveis à vista e ao uso;

14.1.44. Remover entulho, sobras de materiais não utilizados e fazer a limpeza completa após a finalização dos serviços, despejando-os em local permitido pelas autoridades competentes, sem ônus para o CONTRATANTE;

14.1.45. Recolocar em seus respectivos lugares, móveis e equipamentos, quando retirados para execução de serviços;

14.1.46. Responsabilizar-se por danos causados ao patrimônio do CONTRATANTE ou a terceiros, ocasionados por seus profissionais por dolo ou culpa, durante a execução do objeto contratado, arcando com todas as despesas necessárias ao restabelecimento das condições originais;

14.1.47. Cuidar para que os serviços a serem executados acarretem a menor perturbação possível aos serviços públicos, às vias de acesso, e a todo e qualquer bem, público ou privado, adjacente ao prédio do CONTRATANTE. Também providenciará toda e qualquer sinalização e/ou isolamento das áreas de serviço;

14.1.48. Solicitar previamente à FISCALIZAÇÃO autorização para movimentar equipamentos ou modificar elementos existentes no prédio, a fim de facilitar a execução de seus serviços;

14.1.49. Atender às instruções da FISCALIZAÇÃO quanto à execução e horários de realização dos serviços, permanência e circulação de pessoas nas dependências do CONTRATANTE.

14.1.50. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

14.1.51. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

14.1.52. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

15. OBRIGAÇÕES DO CONTRATANTE

15.1. Além das obrigações previstas no presente termo, deverá o CONTRATANTE:

15.1.1. Relacionar-se com a CONTRATADA, exclusivamente, por meio de pessoa por ela credenciada;

15.1.2. Assegurar o livre acesso dos empregados da CONTRATADA, quando devidamente identificados e/ou uniformizados, aos locais em que devam executar suas tarefas;

15.1.3. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos empregados da CONTRATADA;

15.1.4. Comunicar à CONTRATADA, de imediato, qualquer irregularidade ou falha verificada nos materiais ou na execução dos serviços, para que sejam adotadas as medidas corretivas necessárias;

15.1.5. Acompanhar e fiscalizar a execução do Contrato, por Representante da Administração, especificamente designado por Portaria, que atestará as Notas Fiscais para fins de pagamento, comprovado o fornecimento de materiais e a prestação dos serviços de instalação de forma correta;

15.1.6. Efetuar, com pontualidade, os pagamentos à CONTRATADA, após o cumprimento das formalidades legais;

15.1.7. Fornecer à CONTRATADA todos os esclarecimentos e informações necessárias à execução dos serviços ora contratados;

15.1.8. Exigir o cumprimento de todos os compromissos assumidos pela Contratada;

15.1.9. Determinar o imediato afastamento de qualquer empregado integrante da equipe designada para a execução dos serviços que esteja sem uniforme ou sem crachá, ou cuja permanência na área for julgada inconveniente;

15.1.10. Recusar qualquer material, produto ou equipamento que não atenda satisfatoriamente. Os serviços rejeitados deverão ser refeitos pela CONTRATADA sem nenhum ônus adicional para o CONTRATANTE;

15.1.11. Notificar a Contratada, por escrito, sobre imperfeições.

16. FORMALIZAÇÃO E PRAZO DE VIGÊNCIA DO CONTRATO

16.1. A Polícia Federal convocará a adjudicatária para assinar o contrato, a qual terá o prazo de 05 (cinco) dias úteis, a contar do recebimento da notificação, para comparecer à Administração, sob pena de decair do direito à contratação, sem prejuízo das penalidades previstas em Edital;

16.2. Na assinatura do contrato será exigida a comprovação das condições de habilitação consignadas no Edital, as quais deverão ser mantidas pela adjudicatária durante a vigência do contrato;

16.3. Se a adjudicatária não fizer a comprovação referida no subitem anterior ou quando, injustificadamente, recusar-se a assinar o contrato, poderá a Administração convocar outra LICITANTE, desde que respeitada a ordem de classificação, para, depois de comprovados os requisitos habilitatórios e feita a negociação, assinar o contrato, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais aplicáveis à adjudicatária que deixou de assinar o instrumento;

16.4. O prazo estabelecido para assinatura do Contrato poderá ser prorrogado uma única vez, por igual período, quando solicitado pela adjudicatária durante o seu transcurso e desde que ocorra motivo justificado e aceito pela Administração;

16.5. Será formalizado contrato administrativo, com vigência de doze meses, contados da sua assinatura, nos termos da Lei 8.666/93;

17. GARANTIA E INSTALAÇÃO DE NOVAS VERSÕES DE SOFTWARE/FIRMWARE

17.1. Os equipamentos, infraestrutura, serviços e materiais acessórios e necessários para o funcionamento do sistema deverão possuir garantia integral pelo período mínimo de 36 meses, contados a partir do recebimento definitivo. A garantia do sistema deverá englobar todas as falhas de peças e mão de obra, de fabricação e defeitos na instalação dos equipamentos por meio de manutenção preventiva e corretiva.

17.2. Entende-se como manutenção preventiva a totalidade de serviços, ajustes, testes, substituição de peças, executadas de forma periódica ou preditiva, de forma a manter a continuidade dos serviços em perfeitas condições de funcionamento. A CONTRATADA deverá apresentar um plano completo de manutenção preventiva do sistema, a qual deve ser efetuada por mão-de-obra qualificada e treinada de acordo com as recomendações do fabricante. A periodicidade da manutenção e testes deverá estar em conformidade com os procedimentos recomendados pelos fabricantes.

17.3. Entende-se como manutenção corretiva, a realização dos consertos, reparos e substituições de peças ou de componentes dos elementos do sistema, para corrigir falhas ou defeitos.

17.4. Durante o período de garantia, a CONTRATADA deverá manter os equipamentos em perfeito estado de funcionamento.

17.5. Como parte dos serviços de manutenção, preventiva e corretiva, ficarão por conta da CONTRATADA:

17.5.1. A desmontagem, o transporte e a remontagem de qualquer componente do sistema que deva ser reparado, dentro ou fora das dependências da PF;

17.5.2. O fornecimento do material de consumo necessário à execução dos serviços de manutenção.

17.6. Durante o prazo de vigência da garantia, todos os eventuais erros ou falhas, locomoções, trocas de equipamentos, atualizações e todos os serviços para execução da garantia deverão ser corrigidos/fornecidos pela CONTRATADA, sem ônus para a CONTRATANTE.

17.7. As visitas para prestação dos serviços de manutenções corretiva, durante o período da garantia e independentemente da quantidade necessária, não implicarão em custos adicionais para a PF.

17.8. Eventuais despesas de custeio com deslocamento de técnicos da CONTRATADA ao local de prestação do serviço de garantia, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos ficam a cargo exclusivo da CONTRATADA.

17.9. Para o serviço de manutenção corretiva, a CONTRATADA deverá atender aos prazos máximo constantes nas respectivas tabelas do item 18.

17.10. Durante o período da garantia, a CONTRATADA deverá disponibilizar toda e qualquer atualização de software ou firmware dos equipamentos fornecidos, sem ônus adicional ao CONTRATANTE.

17.11. Os equipamentos, componentes ou partes dos equipamentos entregues ou equipamentos substituídos em garantia deverão ser originais, novos, de primeiro uso, estarem em linha de produção e possuir configuração igual ou superior ao do componente substituído.

17.12. O prazo de garantia deverá ser respeitado pela CONTRATADA mesmo após o término do prazo de vigência do contrato.

17.13. A contratada deverá comprometer-se a prestar a garantia estabelecida nas especificações técnicas constantes neste Termo de Referência.

18. NÍVEIS MÍNIMOS DE SERVIÇO, GARANTIA E ENTREGA DOS EQUIPAMENTOS

18.1. Os serviços descritos neste termo serão realizados nas Unidades da Polícia Federal, indicados no item 4.1.24;

18.2. Em atendimento a Instrução Normativa SLTI/MP n° 4/2014, e suas alterações, o nível mímino de execução dos serviços de intalação e configuração dos itens do grupo 01 da tabela do item 4.1 será da forma descrita nas tabela abaixo .

18.2.1. A TABELA representa a relação entre o tempo, em dias úteis, para execução do serviço, e as respectivas sanções administrativas aplicáveis para cada caso:

EXECUÇÃO DOS SERVIÇOS INSTALAÇÃO E CONFIGURAÇÃO DO GRUPO 01	
TEMPO PARA EXECUÇÃO	CLASSIFICAÇÃO DO ATENDIMENTO/SANÇÃO
Tempo de execução ≤ 45 dias (úteis)	Aceito
45 dias (uteis) < Tempo para execução ≤ 50 dias (corridos)	Advertência
50 dias (uteis) < Tempo para execução ≤ 60 dias (corridos)	Multa de 3% sobre o valor do contrato
Tempo para execução > 70 dias(uteis)	Demais Sanções ADMINISTRATIVAS previstas no item 23 deste Termo de Referência.

18.2.2. A CONTRATADA deverá apresentar PROJETO DA ESTRUTURA E FUNCIONAMENTO da solução de acordo com a demanda da CONTRATANTE, dentro do prazo estabelecido na tabela acima, não sendo oferecido prazo a mais.

18.2.3. O Treinamento deverá ser ministrado (de acordo com as especificações no item 4), após a finalização da instalação e configuração dos equipamentos do grupo 01, conforme prazos da tabela abaixo:

18.2.3.1. A TABELA representa a relação entre o tempo, em dias úteis, para iniciação do curso, e as respectivas sanções administrativas aplicáveis para cada caso:

MINISTRAÇÃO DO TREINAMENTO	
TEMPO PARA INICIAR EXECUÇÃO APÓS EMISSÃO DA ORDEM DE EXECUÇÃO	CLASSIFICAÇÃO DO ATENDIMENTO/SANÇÃO
Tempo para início ≤ 30 dias (uteis)	Aceito
30 dias (uteis) < Tempo para início ≤ 50 dias (corridos)	Advertência
50 dias (uteis) < Tempo para início ≤ 60 dias (corridos)	Multa de 3% sobre o valor do contrato
Tempo para início > 70 dias(uteis)	Demais Sanções ADMINISTRATIVAS previstas no item 23 deste Termo de Referência.

18.2.4. A configuração e instalação dos itens dos grupos 02, 03, 04 e 05 será de acordo com as demandas apresentadas pela contratante, limitado em até 180 dias da total instalação e configuração dos itens do grupo 01, conforme descrição da tabela abaixo:

18.2.4.1. A TABELA representa a relação entre o tempo, em dias úteis, para execução do serviço, e as respectivas sanções administrativas aplicáveis para cada caso:

EXECUÇÃO DOS SERVIÇOS INSTALAÇÃO E CONFIGURAÇÃO DO GRUPO 02, 03, 04 E 05	
TEMPO PARA EXECUÇÃO APÓS EMISSÃO DA ORDEM DE EXECUÇÃO	CLASSIFICAÇÃO DO ATENDIMENTO/SANÇÃO
Tempo de execução ≤ 03 dias (úteis)	Aceito
05 dias úteis < 07 dias úteis	Advertencia – Formalizada
07 dias (úteis) < Tempo de Solução ≤ 12 dias (úteis), com advertência anterior	Multa de 3% do valor do equipamento ou suprimento por solução de garantia atendida neste prazo.
12 dias (úteis) < Tempo de Solução ≤ 15 dias úteis	Multa de 10% do valor do equipamento ou suprimento por solução de garantia atendida neste prazo
A partir do 15° dia útil	Multa de 30% do valor do equipamento ou suprimento + Multa de 1% do valor do equipamento ou suprimento ou dia de atraso até a entrega da solução (dias corridos). Limitado ao valor total do equipamento ou suprimento
A partir da aplicação da multa do valor total do equipamento ou suprimento	Demais sanções ADMINISTRATIVAS previstas no item 23 deste Termo de Referência.

18.2.5. Após o prazo disposto no item 18.2.1, se a contratante não apresentar demanda para instalação e configuração será dado por encerrado e concluído o serviço;

18.2.6. A contratada deverá instalar e eonfigurar o quantitativo, de aprelhos telefônicos e video fones indicados nos referidos itens.

18.3. Haverá um período de funcionamento experimental mínimo de 30 dias após a instalação e completo funcionamento da central.

18.4. Horário de funcionamento da central de atendimento telefonico da CONTRATADA ou fabricante dos equipamentos para atendimento dos chamados de garantia realizados pela contrantatne: 08 as 19h (horáro oficial de Brasília), em dias úteis de segunda a sexta-feira.

18.5. O atendimento do serviço de garantia de produto deverá ser executado de acordo com as seguintes regras:

18.5.1. Após o registro do incidente na central de atendiemento telefonico da CONTRATADA, os técncnico da CONTRATADA deverão ser deslocados para o local onde estiver o equipamento, devendo resolver o(s) problema(s) técnico(s) em até 05 (cinco) dias úteis.

18.5.2. No caso de vícios insanáveis no equipamento e sempre que determinado pela CONTRATADA ou pela rede oficial de atendimento do fabricante, o equipamento e/ou suprimento deverá ser substituído por um novo com características similares ou superiores devidamente avaliados pela equipe técnica da Polícia Federal.

18.6. Em atendimento a Instrução Normativa SLTI/MP n° 4/2014, e suas alterações, o nível de serviço mínimo para Garantia de todos equipamentos e suprimentos descritos neste Termo será dado pela TABELA abaixo:

18.6.1. A TABELA representa a relação entre o tempo, em dias úteis, para resolução do chamado, e as respectivas sanções administrativas aplicáveis para cada caso:

ATENDIMENTO DOS CHAMADOS EM GARANTIA	
TEMPO PARA SOLUÇÃO NOS ACIONAMENTOS DA GARANTIA DE EQUIPAMENTO	CLASSIFICAÇÃO DO ATENDIMENTO/SANÇÃO
Tempo de Solução ≤ 02 dias	Aceito

(úteis)	
02 dias úteis < 04 dias úteis	Advertencia – Formalizada
04 dias (úteis) < Tempo de Solução ≤ 7 dias (úteis), com advertência anterior	Multa de 3% do valor do equipamento ou suprimento por solução de garantia atendida neste prazo.
7 dias (úteis) < Tempo de Solução ≤ 12 dias úteis	Multa de 10% do valor do equipamento ou suprimento por solução de garantia atendida neste prazo
A partir do 12° dia útil	Multa de 30% do valor do equipamento ou suprimento + Multa de 1% do valor do equipamento ou suprimento ou dia de atraso até a entrega da solução (dias corridos). Limitado ao valor total do equipamento ou suprimento.
A partir da aplicação da multa do valor total do equipamento ou suprimento	Demais sanções ADMINISTRATIVAS previstas no item 23 deste Termo de Referência.

18.7. O objetivo é restabelecer as condições ideais de funcionamento dos equipamentos, eliminando os defeitos e/ ou desgastes decorrentes do uso normal.

18.8. Os serviços de atendimento técnico poderão ser solicitados por chamada interurbana a cobrar ou por discagem direta gratuita.

18.9. Durante a garantia, de 36 meses, a contratada deverá manter o Sistema funcionando, dispondo de:

18.9.1. Serviço mínimo que permita a reconfiguração dos parâmetros de funcionamento da solução de telefonia IP, de forma concomitante com a transferência de conhecimento a equipe técnica da contratante.

18.9.2. Configuração e reconfiguração da solução já implantada e em operação, caso necessário.

18.9.3. Configuração e reconfiguração de todas as interfaces de rede IP.

18.9.4. Configuração e reconfiguração de ramais, sendo estes de tecnologia analógico ou IP, incluindo todas as facilidades de ramal, tais como grupos de captura, espera telefônica, chefe/secretária, classes de restrições de chamadas, correio de voz e fax, integrações de comunicação unificada, CDR.

18.9.5. Configuração e reconfiguração de rotas e troncos, sendo estes de tecnologia digital, analógico ou IP, incluindo todas as funcionalidades de rotas, tais como plano de numeração, tratamento do encaminhamento de chamadas, rotas de menor custo, CDR.

18.9.6. O serviço deverá ser realizado por técnico qualificado da contratada. O Serviço poderá ocorrer de forma “on-site” e/ou através de acesso VPN a ser disponibilizado pela contratante.

18.10. Em atendimento a Instrução Normativa SLTI/MP n° 4/2014, e suas alterações, o nível de serviço mínimo para Entrega de todoss equipamentos e suprimentos descritos será dado pela TABELA a seguir:

18.10.1. A TABELA representa a relação entre o tempo, em dias úteis, para entrega dos equipamentos, e as respectivas sanções administrativas aplicáveis para cada caso:

ENTREGA APÓS EMISSÃO DA ORDEM DE FORNECIMENTO	
TEMPO PARA ENTREGA DOS EQUIPAMENTOS DOS GRUPOS 01, 02, 03, 04 E 05 APÓS EMISSÃO DA ORDEM DE FORNECIMENTO	CLASSIFICAÇÃO DO ATENDIMENTO/SANÇÃO
Tempo para Entrega ≤ 45 dias (corridos)	Aceito
45 dias (corridos) < Tempo para Entrega ≤ 50 dias (corridos)	Advertência
50 dias (corridos) < Tempo para Entrega ≤ 60 dias (corridos)	Multa de 3% sobre o valor do contrato.
Tempo para Entrega > 70 dias(corridos)	Demais Sanções ADMINISTRATIVAS previstas no item 23 deste Termo de Referência.

18.11. A entrega de aparelhos telefônicos e equipamentos que compõem a solução deverá ocorrer no Almoxarifado, localizado no Setor Policial Sul, Área 7, Lote 23 - Edifício CGTI, Brasília/DF, no horário de 12h às 19h;

18.11.1. O Almoxarifado fará o recebimento provisório, e após exemplares serem testados e inspecionados, comprovando suas plenas funcionalidades, poderão receber o tombamento e o Recebimento Definitivo.

19. ACOMPANHAMENTO E FISCALIZAÇÃO

19.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da CONTRATANTE, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993, e do art. 6º do Decreto nº 2.271, de 1997.

19.2. A fiscalização do objeto deste termo será feita por equipe de servidores designados pelo CONTRATANTE, através de Portaria, que deverá dirimir as dúvidas que surgirem no curso da execução, dando ciência à CONTRATADA, nos termos do art. 67 da Lei nº 8.666/93, a qual não exclui nem reduz a responsabilidade da CONTRATADA.

19.3. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados;

19.4. Os equipamentos entregues serão testados, fiscalizados e atestados por servidores designados pela CONTRATANTE, que também verificarão o exato cumprimento de todas as cláusulas e condições, conforme prevê o art. 67 da Lei nº 8.666/93, além de atestar as faturas apresentadas pela CONTRATADA;

19.5. O recebimento de material de valor superior a R$ 80.000,00 (oitenta mil reais) será confiado a uma comissão de, no mínimo, 3 (três) membros, designados pela autoridade competente;

19.6. Os serviços prestados serão acompanhados, fiscalizados e atestados pela Comissão de Gestão e Fiscalização do Contrato, composta por:

19.6.1. Gestor do Contrato: servidor que realizará o processo de gestão do contrato, indicado por autoridade competente;

19.6.2. Fiscal Técnico do Contrato: servidor representante da Área Técnica, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato;

19.6.3. Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos;

19.6.4. Fiscal Requisitante do Contrato: servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação.

19.7. Compete à Comissão de Fiscalização do Contrato, a fiscalização do cumprimento dos requisitos técnicos, administrativos e financeiros do Contrato. Também verificarão o exato cumprimento de todas as cláusulas e condições, conforme prevê o art. 67 da Lei nº 8.666/93, além de atestar as faturas apresentadas pela CONTRATADA.

19.8. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

19.9. A execução do contrato deverá ser acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam a mensuração dos aspectos mencionados no art. 34 da Instrução Normativa SLTI/MPOG nº 02, de 2008.

19.10. O fiscal ou gestor do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do artigo 65 da Lei nº 8.666, de 1993.

19.11. Compete aos Fiscais Técnico e Requisitante do Contrato a avaliação da qualidade dos serviços realizados, de acordo com os critérios de aceitação definidos em contrato.

19.12. Compete ao Fiscal Administrativo do Contrato a verificação de aderência aos termos contratuais, bem como a verificação das regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento.

19.13. Compete aos Fiscais Administrativo e Técnico do Contrato a verificação da manutenção das condições referentes à habilitação técnica.

19.14. Compete ao Gestor do Contrato o encaminhamento de indicação de sanções do Contrato para a deliberação do Ordenador de Despesas.

19.15. Compete aos Fiscais Técnico e Requisitante do Contrato aprovarem o relatório de disponibilidade e desempenho e providenciar o atesto da fatura para fins de encaminhamento para pagamento.

19.16. Compete ao Gestor do Contrato o encaminhamento, ao Ordenador de Despesas, de eventuais pedidos de modificação contratual.

19.17. Compete ao Gestor do Contrato a manutenção do Histórico de Gerenciamento do Contrato, contendo registros formais de todas as ocorrências positivas e negativas da execução do Contrato, por ordem histórica.

19.18. O Representante Técnico da CONTRATANTE deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato.

19.19. A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da CONTRATADA que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência e na proposta, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

19.20. A Comissão de Gestão e Fiscalização se reserva o direito de rejeitar, no todo ou em parte, a prestação do serviço, se em desacordo com o Contrato.

19.21. Os Fiscais anotarão em registro próprio todas as ocorrências relacionadas com o fornecimento dos serviços, determinando o que for necessário à regularização das faltas ou defeitos observados.

19.22. O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de penalizações e/ou sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 80 da Lei nº 8.666, de 1993.

19.23. As disposições previstas nesta cláusula não excluem o disposto no Anexo IV (Guia de Fiscalização dos Contratos de Terceirização) da Instrução Normativa SLTI/MPOG nº 02, de 2008, aplicável no que for pertinente à contratação.

19.24. A fiscalização pela Comissão de Gestão e Fiscalização do Contrato não exclui nem reduz a responsabilidade da CONTRATADA quanto aos danos causados diretamente ao CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo na execução do Contrato ou, ainda, resultante de imperfeições técnicas, vício redibitório ou emprego de material inadequado ou de qualidade inferior. A ocorrência de qualquer dessas hipóteses não implica em corresponsabilidade da CONTRATANTE ou de seus agentes, conforme dispõe o art. 70 da Lei nº 8.666, de 1993.

19.25. Quaisquer exigências da fiscalização inerentes ao objeto deste Termo de Referência deverão ser prontamente atendidas pela CONTRATADA.

19.26. A CONTRATADA deverá indicar representantes oficiais para representá-la na execução do Contrato.

20. ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

20.1. O objeto será recebido nos termos do Art. 73 da Lei n.º 8.666/93, após a execução dos serviços:

20.1.1. Provisoriamente, pelo responsável por seu acompanhamento e fiscalização, mediante termo circunstanciado, assinado pelas partes em até 15 (quinze) dias da comunicação escrita da CONTRATADA;

20.1.2. Definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo de observação, ou vistoria que comprove a adequação do objeto aos termos contratuais, observado o disposto no Art. 69 da Lei n.º 8.666/93.

20.2. O prazo a que se refere o item 20.1.2 será de até 90 (noventa) dias, contados a partir da emissão do Termo de Recebimento Provisório.

20.3. O objeto será recebido nos termos do Art. 73 da Lei n.º 8.666/93, em se tratando do fornecimento dos bens:

20.3.1. Provisoriamente, para efeito de posterior verificação da conformidade do material com a especificação;

20.3.2. Definitivamente, após a verificação da qualidade e quantidade do material e consequente aceitação.

20.4. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança da obra ou do serviço, nem ético-profissional pela perfeita execução do Contrato, dentro dos limites estabelecidos pela lei ou pelo Contrato;

20.5. Poderá ser exigido do licitante provisoriamente classificado que apresente, no local de entrega dos equipamentos, no prazo de 5 dias uteis, amostra(s) do(s) item(ns), para a verificação de compatibilidade com as especificações deste Termo de Referência e consequentemente aceitação da proposta.

20.6. A amostra deverá estar devidamente identificada com o nome do licitante, conter os respectivos prospectos e manuais, se for o caso, e dispor na embalagem de informações quanto às suas características, quantidade de produto, sua marca, número de referência, código do produto (part-number) e modelo.

20.7. Os exemplares colocados à disposição da Administração serão tratados como protótipos, podendo ser manuseados, desmontados ou instalados pela equipe técnica responsável pela análise, bem como conectados a equipamentos e submetidos aos testes necessários.

20.8. Os licitantes deverão colocar à disposição da Administração todas as condições indispensáveis à realização de testes e fornecer, sem ônus, os manuais impressos, necessários ao seu perfeito manuseio, quando for o caso.

20.9. A responsabilidade sobre a entrega e recolhimento dos equipamentos ficam a cargo da licitante, que deverá recolher os equipamentos em até 5 dias úteis após avaliação da Administração.

21. TESTE E INSPEÇÃO

21.1. Em atendimento a Instrução Normativa SLTI/MP n° 4/2014, e suas alterações, os procedimentos de teste e inspeçao de todos equipamentos e suprimentos descritos neste Termo será dado pela TABELA abaixo:

ITENS	CRITÉRIO DE VALIAÇÃO E JULGAMENTO
Central Telefônica IP/PABX IP (*Software*, baseado em *open source*, com suporte para mínimo de 4.000 ramais/usuários a ser instalado em uma VM - Virtual *Machine*) - Implantação, Configuração	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o equipamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência. No ato do recebimento da Central IP, o fiscal técnico do contrato emitirá o Termo de Recebimento Provisório, mediante verificação do equipamento em conjunto com o fiscal administrativo, de modo a verificar se o equipamento entregue está em acordo com o objeto aceito na fase de seleção do fornecedor e com o termo de referência.

ITENS	CRITÉRIO DE VALIAÇÃO E JULGAMENTO
Gateway com 04 E1 - Implantação, Configuração	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o equipamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência. No ato do recebimento do gateway, o fiscal técnico do contrato emitirá o Termo de Recebimento Provisório, mediante verificação do equipamento em conjunto com o fiscal administrativo, de modo a verificar se o equipamento entregue está em acordo com o objeto aceito na fase de seleção do fornecedor e com o termo de referência.
Gateway com 02 E1, 04 FXO, 08 FXS - Implantação, Configuração	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o equipamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência. No ato do recebimento do gateway, o fiscal técnico do contrato emitirá o Termo de Recebimento Provisório, mediante verificação do equipamento em conjunto com o fiscal administrativo, de modo a verificar se o equipamento entregue está em acordo com o objeto aceito na fase de seleção do fornecedor e com o termo de referência.
Gateway com 02 E1 - Implantação, Configuração	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o equipamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência. No ato do recebimento do gateway, o fiscal técnico do contrato emitirá o Termo de Recebimento Provisório, mediante verificação do equipamento em conjunto com o fiscal administrativo, de modo a verificar se o equipamento entregue está em acordo com o objeto aceito na fase de seleção do fornecedor e com o termo de referência.
Gateway GSM 16 portas	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o equipamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência. No ato do recebimento do gateway, o fiscal técnico do contrato emitirá o Termo de Recebimento Provisório, mediante verificação do equipamento em conjunto com o fiscal administrativo, de modo a verificar se o equipamento entregue está em acordo com o objeto aceito na fase de seleção do fornecedor e com o termo de referência.
Gateway SBC	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o equipamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência. No ato do recebimento do gateway, o fiscal técnico do contrato emitirá o Termo de Recebimento Provisório, mediante verificação do equipamento em conjunto com o fiscal administrativo, de modo a verificar se o equipamento entregue está em acordo com o objeto aceito na fase de seleção do fornecedor e com o termo de referência.

ITENS	CRITÉRIO DE VALIAÇÃO E JULGAMENTO
Configuração e instalação dos Aparelhos Telefônicos IP - Tipo 1, 2, 3 e Videofones	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o equipamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência.
Treinamento	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o Treinamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência. No ato do recebimento, o fiscal técnico do contrato emitirá o Termo de Recebimento Provisório, mediante verificação em conjunto com o fiscal administrativo, de modo a verificar se o treinamento está em acordo com o objeto aceito na fase de seleção do fornecedor e com o termo de referência.
Aparelho Telefônico IP - Tipo 1	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o equipamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência. No ato do recebimento do telefone, o fiscal técnico do contrato emitirá o Termo de Recebimento Provisório, mediante verificação do equipamento em conjunto com o fiscal administrativo, de modo a verificar se o equipamento entregue está em acordo com o objeto aceito na fase de seleção do fornecedor e com o termo de referência.
Aparelho Telefônico IP - Tipo 2	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o equipamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência. No ato do recebimento do telefone, o fiscal técnico do contrato emitirá o Termo de Recebimento Provisório, mediante verificação do equipamento em conjunto com o fiscal administrativo, de modo a verificar se o equipamento entregue está em acordo com o objeto aceito na fase de seleção do fornecedor e com o termo de referência.
Aparelho Telefônico IP - Tipo 3	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o equipamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência. No ato do recebimento do telefone, o fiscal técnico do contrato emitirá o Termo de Recebimento Provisório, mediante verificação do equipamento em conjunto com o fiscal administrativo, de modo a verificar se o equipamento entregue está em acordo com o objeto aceito na fase de seleção do fornecedor e com o termo de referência.

ITENS	CRITÉRIO DE VALIAÇÃO E JULGAMENTO
Aparelho Vídeo Fone IP	Analisar no processo de seleção de amostra em conjunto com a equipe de compras se o equipamento ofertado atende a todas as características técnicas exigidas no item 4 deste Termo de Referência. Verificar em conjunto com a equipe de compras se os documentos referentes a garantia e todas as exigências referentes à mesma estão em acordo com as exigências estabelecidas no Termo de Referência. No ato do recebimento do telefone, o fiscal técnico do contrato emitirá o Termo de Recebimento Provisório, mediante verificação do equipamento em conjunto com o fiscal administrativo, de modo a verificar se o equipamento entregue está em acordo com o objeto aceito na fase de seleção do fornecedor e com o termo de referência.
Recebimento Definitivo	

21.2. Os itens constantes na tabela acima correspondem aos itens da tabela do item 4.1.

22. MODELO DE EXECUÇÃO

22.1. Após a assinatura do Contrato, a CONTRATANTE deverá emitir a(s) Ordem(ns) de Fornecimento de Bens/Serviço.

22.2. O prazo para entrega dos equipamentos/serviços será contabilizado a partir do atesto de recebimento da Ordem de Fornecimento de Bens/Serviço pela CONTRATADA.

22.3. Todas as Ordens de Fornecimento de Bens deverão ser atendidas pela CONTRATADA em um prazo máximo de 45 (quarenta e cinco) dias corridos.

22.4. O prazo para execução dos serviços será da forma descrita abaixo, a contar da data de emissão da Ordem de Serviço pela Fiscalização:

22.5. 30 dias para entrega do projeto;

22.6. 45 dias para entrega dos materiais;

22.7. 60 dias para instalação dos equipamentos;

22.8. Período de funcionamento experimental mínimo de 30 dias após a instalação e completo funcionamento da central.

22.9. Os serviços descritos neste termo serão realizados nas Unidades da Polícia Federal, indicados no item 4.1.24;

22.10. A entrega de aparelhos telefônicos deverá ocorrer no Almoxarifado, localizado no Setor Policial Sul, Área 7, Lote 23 - Edifício CGTI, Brasília/DF, no horário de 12h às 19h;

22.11. O Almoxarifado fará o recebimento provisório, e após os exemplares serem testados na Central MX One, comprovando suas plenas funcionalidades, poderão receber o tombamento e o Recebimento Definitivo.

22.12. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 (cinco) dias úteis, a contar da notificação da CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades.

22.13. Os bens serão recebidos definitivamente no prazo de 20 (vinte) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado.

22.14. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

22.15. Os serviços serão recebidos provisoriamente no prazo de 15 (quinze) dias, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

22.16. Os serviços serão recebidos definitivamente no prazo de 90 dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do serviço executado e materiais empregados, com a consequente aceitação mediante termo circunstanciado.

22.16.1. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

22.17. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

22.18. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do contrato.

22.19. Durante o período em que a Administração estiver realizando a inspeção de aceitação, será suspensa a contagem do prazo de recebimento definitivo, a qual será restabelecida apenas após a conclusão da referida inspeção, através da sua comunicação formal ao fornecedor.

22.20. Os horários de trabalho serão acordados entre a CONTRATADA e a Divisão de Telecomunicações (DITEL), conforme já especificado acima a ordem e quando de sua execução. A autorização deve ser dada por escrito e encaminhada uma cópia à DITEL/CGTI/DLOG/PF.

22.21. O pagamento será efetuado em única parcela, acompanhado de Fatura (Nota Fiscal) discriminada de acordo com a Nota de Empenho, após conferência de quantidade e qualidade do(s) serviço/bens por gestor a ser designado pelo Departamento de Administração da Polícia Federal;

22.22. O pagamento será creditado em favor do fornecedor mediante ordem bancária, devendo para isto, ficar explicitado na proposta o nome e número da agência e o número da conta corrente em que deverá ser efetivado o crédito, após a aceitação do produto e registrado no patrimônio da Polícia Federal.

23. DAS SANÇÕES ADMINISTRATIVAS

23.1. Comete infração administrativa, nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

23.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

23.1.2. ensejar o retardamento da execução do objeto;

23.1.3. fraudar na execução do contrato;

23.1.4. comportar-se de modo inidôneo;

23.1.5. cometer fraude fiscal;

23.1.6. não mantiver a proposta.

23.2. A CONTRATADA que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

23.2.1. Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a CONTRATANTE, que deverá ser feita através de notificação por meio de ofício, mediante contra-recibo do representante legal da CONTRATADA, estabelecendo prazo para cumprimento das obrigações assumidas;

23.2.2. Multa de até 10% (dez por cento) sobre o valor total da contratação, quando for constatado o descumprimento de qualquer obrigação prevista no Edital, no Termo de Referência e/ou Contrato, ressalvadas aquelas obrigações para as quais tenham sido fixadas penalidades específicas;

23.2.3. Pelo atraso injustificado para fornecimento/substituição dos equipamentos, multa de 0,33% (zero vírgula trinta e três por cento) incidente sobre o valor total da contratação, por dia de atraso, a ser cobrada pelo período máximo de 30 (trinta) dias. A partir do 31º (trigésimo primeiro) dia de atraso, o contrato será rescindido;

23.2.4. Pela inobservância dos demais prazos atrelados à execução dos serviços vinculados à garantia/assistência técnica, multa de 0,33% (zero vírgula trinta e três por cento) incidente sobre o valor total da contratação, por dia de atraso, conforme o SLA previsto no Termo de Referência, a ser cobrada pelo período máximo de 30 (trinta) dias. A partir do 31º (trigésimo primeiro) dia de atraso, o contrato será rescindido;

23.2.5. Multa de 10% (dez por cento) sobre o valor total da contratação, nos casos de rescisão do contrato por culpa da CONTRATADA.

23.2.6. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

23.2.7. Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

23.2.8. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

23.2.9. Em se tratando de inobservância do prazo fixado para apresentação da garantia prevista na cláusula 24- DA GARANTIA DE EXECUÇÃO CONTRATUAL, ainda que seja para reforço, aplicar-se-á multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, observado o máximo de 2% (dois por cento), de modo que o atraso superior a 25 (vinte e cinco) dias autorizará a Administração contratante a promover a rescisão do contrato;

23.3. A aplicação das sanções previstas no Contrato não exclui a possibilidade de aplicação de outras, previstas na Lei nº 8.666/1993 e no art. 28, do Decreto nº 5.450/2005, inclusive a responsabilização da CONTRATADA por eventuais perdas e danos causados à CONTRATANTE.

23.4. A multa deverá ser recolhida no prazo máximo de 10 (dez) dias corridos, a contar da data do recebimento da comunicação enviada pela CONTRATANTE.

23.5. A multa, aplicada após regular processo administrativo, será descontada da garantia ou do pagamento eventualmente devido pela CONTRATANTE, ou, ainda, cobrada judicialmente. Havendo aplicação de multa em valor superior ao montante da garantia prestada, além da perda desta, responderá a CONTRATADA pela sua diferença, a qual será descontada dos pagamentos devidos pela CONTRATANTE ou ainda, quando for o caso, cobrada judicialmente;

23.6. Conforme o disposto no art. 28 do Decreto nº 5.450, de 31/05/2005, aquele que, convocado dentro do prazo de validade de sua proposta, não assinar o contrato, deixar de entregar documentação exigida no edital, apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar no fornecimento e/ou prestação do serviço, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantido o direito à ampla defesa, ficará impedida de licitar e de contratar com a União, e será descredenciado no SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas no edital e no contrato e das demais cominações legais.

23.7. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

23.7.1. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

23.7.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

23.7.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

23.8. As penalidades previstas poderão ser suspensas no todo ou em parte, quando o atraso no cumprimento das obrigações for devidamente justificado pela empresa Contratada, por escrito, no prazo máximo de 05 (cinco) dias úteis e aceito pela Contratante.

23.9. As sanções previstas no Contrato são independentes entre si, podendo ser aplicadas de forma isolada ou cumulativamente, sem prejuízo de outras medidas cabíveis.

23.10. Não será aplicada multa se, justificada e comprovadamente, o atraso na entrega dos equipamentos e/ou na execução dos serviços advier de caso fortuito ou de força maior.

23.11. As sanções serão obrigatoriamente registradas no SICAF e, no caso de suspensão do direito de licitar, o licitante deverá ser descredenciado, por igual período, sem prejuízo das multas previstas no Edital, no Contrato e das demais cominações legais.

23.12. Em qualquer hipótese de aplicação de sanções, serão assegurados à CONTRATADA o contraditório e a ampla defesa.

24. DA GARANTIA DE EXECUÇÃO CONTRATUAL

24.1. Para a execução das obrigações assumidas, a CONTRATANTE exigirá da CONTRATADA vencedora do lote único, até 10 (dez) dias após a assinatura do Contrato, prestação de garantia correspondente a 5% (cinco por cento) do seu valor total, em uma das modalidades previstas no art. 56 da Lei nº 8.666/93, que será liberada ou restituída somente após o término da vigência contratual e desde que não haja pendências.

24.2. O valor da garantia poderá ser utilizado para corrigir as imperfeições verificadas na execução dos serviços, bem como nos casos decorrentes de inadimplemento contratual e de indenização por danos causados ao patrimônio da União ou de terceiros;

24.3. O valor da garantia se reverterá em favor da PF, integralmente ou pelo saldo que apresentar, no caso de rescisão contratual por culpa exclusiva da CONTRATADA, sem prejuízo das perdas e danos porventura verificados;

24.4. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

24.5. Será considerada extinta a garantia:

24.5.1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato;

24.5.2. No prazo de três meses após o término da vigência, caso a CONTRATANTE não comunique a ocorrência de sinistros.

25. DO PAGAMENTO

25.1. O pagamento deverá ser feito por meio de crédito em conta corrente, mediante a apresentação da respectiva nota fiscal/fatura, onde deverá constar o número do contrato, acompanhada do termo de aceite correspondente, sendo que:

25.1.1. Os pagamentos relativos às entregas dos equipamentos mencionados nos itens 08, 09, 10 e 11 serão efetuados em até 30 (trinta) dias após a assinatura do Termo de Aceite Definitivo dos equipamentos e apresentação da respectiva nota fiscal/fatura.

25.1.2. Os pagamentos relacionados aos serviços especificados nos itens 01, 02, 03, 04, 05, 06 e 07, bem como ao serviço de instalação dos equipamentos discriminados nos itens 08, 09, 10 e 11 serão efetuados em até 30 (trinta) dias após a assinatura do Termo de Aceite Definitivo e apresentação da respectiva nota fiscal/fatura.

25.1.3. Deverá ser assinado Termo de Aceite Definitivo e apresentada nota fiscal/fatura para a parcela de serviço prestado em cada uma das unidades descritas no subitem 4.1.24.

25.2. O pagamento será efetuado à CONTRATADA, no prazo de até 30 (trinta) dias contados a partir da data de apresentação das Notas Fiscais / Faturas, observado Art. 40 Inc. XIV, “a” da Lei 8.666/1993. As Notas Fiscais / Faturas serão pagas após serem devidamente atestadas pelo Fiscal, designado em documentação própria, podendo a CONTRATANTE descontar eventuais multas, glosas e penalizações que tenham sido impostas à CONTRATADA.

25.3. Será procedida consulta “ON LINE” junto ao SICAF antes de cada pagamento ser efetuado à CONTRATADA, para verificação da situação da CONTRATADA quanto às condições de habilitação e qualificação exigidas na licitação.

25.4. Nenhum pagamento será efetuado à CONTRATADA enquanto estiver pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de aplicação de penalidade ou inadimplência decorrente do presente processo.

25.5. As notas fiscais contendo incorreções serão devolvidas à CONTRATADA, no prazo de até cinco dias úteis, com as razões da devolução apresentadas formalmente, para as devidas retificações, e permanecerá pendente até que todas as medidas saneadoras sejam tomadas.

25.6. O ônus decorrente das eventuais devoluções de nota fiscal previstas no item anterior são de inteira responsabilidade da CONTRATADA.

25.7. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes formulas:

$$I = (TX/100)$$

EM = I x N x VP

Onde:

I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

25.8. O presente critério aplica-se aos casos de compensações financeiras por eventuais atrasos de pagamentos e aos casos de descontos por eventuais antecipações de pagamento.

25.9. A CONTRATANTE poderá deduzir do montante a pagar os valores correspondentes a multas, glosas, penalizações ou indenizações devidas pela CONTRATADA, nos termos deste documento.

26. DA DOTAÇÃO ORÇAMENTÁRIA

26.1. As despesas decorrentes da contratação do objeto deste Termo de Referência correrão à conta dos recursos consignados no Orçamento Geral da União para a Polícia Federal, cujos programas de trabalho e elemento de despesas especificadas constarão da respectiva Nota de Empenho.

27. DA SUSTENTABILIDADE AMBIENTAL – IN Nº. 01/2010-SLTI/MPOG

27.1. A empresa contratada adotará as seguintes práticas de sustentabilidade na execução dos serviços, quando couber:

27.1.1. Usar produtos de limpeza e conservação de superfícies e objetos inanimados que obedeçam às classificações e especificações determinadas pela ANVISA;

27.1.2. Adotar medidas para evitar o desperdício de água tratada, conforme instituído no Decreto nº 48.138, de 8 de outubro de 2003;

27.1.3. Observar a Resolução CONAMA nº 20, de 7 de dezembro de 1994, quanto aos equipamentos de limpeza que gerem ruído no seu funcionamento;

27.1.4. Fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços;

27.1.5. Realizar um programa interno de treinamento de seus empregados, nos três primeiros meses de execução contratual, para redução de consumo de energia elétrica, de consumo de água e redução de produção de resíduos sólidos, observadas as normas ambientais vigentes;

27.1.6. Respeitar as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos;

27.1.7. Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;

27.1.8. Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

27.1.9. Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

28. DAS DISPOSIÇÕES FINAIS

28.1. A participação no certame importa em total, irrestrita e irretratável aceitação, pelos proponentes, das condições deste Termo de Referência, impedindo-os de alegar desconhecimento, não entendimento ou interpretação errônea das condições do certame fixadas neste documento.

28.2. Este certame poderá ser revogado por interesse público, em decorrência de fato superveniente devidamente comprovado, pertinente e suficiente para justificar o ato, ou anulado por vício ou ilegalidade, a modo próprio ou por provocação de terceiros, sem que as partes tenham direito a qualquer indenização, obedecendo ao disposto no Art. 18 do Decreto nº 3.555/2000, ressalvado o disposto no § 2º do mesmo artigo.

28.3. Os proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase do certame.

Brasília-DF, 09 de agosto de 2017.

29. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		
Integrante Técnico	**Integrante Administrativo**	**Integrante Requisitante**
Henderson Dias de Oliveira Agente de Telecomunicações e Eletricidade Matrícula DPF 15.162 DITEL/CGTI/DLOG/PF **Welington Rodrigues Silva** Agente de Telecomunicações e Eletricidade Matrícula DPF 13.369 DITEL/CGTI/DLOG/PF **Jose Doniseth Dantas de Oiveira** Agente de Telecomunicações e Eletricidade Matrícula DPF 12.823 DITEL/CGTI/DLOG/PF **Nilson Luiz Cavallin** Agente de Polícia Federal Matrícula DPF 15.162 DITEL/CGTI/DLOG/PF	**Paulo Rodrigo Brito e Silva** Agente Adminstrativo Matrícula DPF 15.162 SAD/CGTI/DLOG/PF **Edivaldo Sacramento Borges** Agente Adminstrativo Matrícula DPF 15.162 DITEL/CGTI/DLOG/PF	**Alilton Moreira de Assis** Agente de Telecomunicações e Eletricidade Matrícula DPF 14.648 Chefe da DITEL/CGTI/DLOG/PF
Brasília/DF, 09 de agosto de 2017.		

ANEXO I

PLANILHA PARA FORMAÇÃO DE PREÇO

Item	Descrição	Quantidade Estimada	Valor Unitário (R$)	Valor Total (R$)
01	Instalação e Configuração de Central PABX IP e serviços agregados: Sistema telefônico, baseado em software livre (open source), Asterisk, com as respectivas soluções integradas conforme TR (Termo de Referência), a ser instalado em VM (Máquina Virtual) com redundância.	01		
02	Gateway com 04 E1	02		
03	Gateway com 02 E1, 04 FXO, 08 FXS	02		
04	Gateway com 02 E1	08		
05	Gateway GSM 16 portas	01		
06	Gateway SBC	01		
07	Configuração dos intens 09, 10, 11 e 12	2370		
08	Treinamento	01		
09	Aparelho Telefônico IP - Tipo 1	500		
10	Aparelho Telefônico IP - Tipo 2	500		
11	Aparelho Telefônico IP - Tipo 3	1300		
12	Aparelho Vídeo Fone IP	70		
	TOTAL			

ANEXO II - DECLARAÇÃO DE VISTORIA

Declaramos, para fins de Pregão Eletrônico nº ...../2017 – CGTI/DITEL/PF, que a empresa .....(nome ou razão social da empresa)....., CNPJ/MF nº ....., representada por seu Responsável Técnico .....(nome do responsável)....., CPF nº ....., em visita realizada às instalações da Coordenação – Geral de Tecnologia da Informação da Polícia Federal (CGTI/DLOG/PF), está ciente das condições atuais de infraestrutura, bem como das quantidades, marcas e configurações dos equipamentos de informática e ainda dos *softwares* utilizados pelo órgão, e que recebeu instruções e informações necessárias ao atendimento do objeto e demais condições do Edital. Não havendo, portanto, nenhuma dúvida que prejudique a apresentação de uma proposta completa e com todos os detalhes.

Declaramos, ainda, que a supramencionada empresa está ciente do compromisso assumido de manter sigilo sobre todas as informações às quais teve acesso em decorrência da vistoria realizada nesta data.

Brasília, ... de ..... de 2017.

(Assinatura e carimbo)

NOME COMPLETO

Cargo

Matrícula PF

_____

(Responsável técnico da empresa)

ANEXO III - MODELO DO TERMO DE SIGILO

O(a) Sr.(a) ..... CPF nº..... endereço....., profissional responsável pela execução do contrato nº _____/_____, **DECLARA**, sob as penalidades da lei, que está ciente das normas de segurança vigentes na CGTI/DLOG/PF e que se compromete:

1. a não divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto;

2. a não utilizar as informações confidenciais a que tiver acesso, para gerar benefício exclusivo e/ou unilateral, presente ou futuro, para si ou para terceiros;

3. a não efetuar nenhuma gravação ou cópia do código fonte ou das informações confidenciais a que tiver acesso;

4. a não apropriar-se para si ou para outrem do material confidencial e/ou sigiloso oriundo das informações confidenciais às quais tiver acesso;

5. a não repassar o conhecimento das informações confidenciais, responsabilizando-se por todas as pessoas que vierem a ter acesso a tais informações por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e/ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

Neste Termo, as seguintes expressões serão assim definidas:

Informação Confidencial significará toda e qualquer informação pertencente exclusivamente à Polícia Federal e seus afiliados, de natureza técnica, operacional, comercial, jurídica, know-how, processos, projetos, métodos e metodologia, fluxogramas, sistemas de logística e layouts, planos de negócios (business plans), documentos, contratos, papéis, pareceres, dados e código fonte, que forem disponibilizados a mim sob a forma escrita, verbal ou por quaisquer outros meios.

Não se configuram informações confidenciais:

a. aquelas já disponíveis ao público em geral sem minha culpa;
b. aquelas que não são mais consideradas confidenciais pela coordenação do projeto e pelo Departamento de Tecnologia da Informação da Polícia Federal;
c. os conhecimentos de ferramentas e tecnologias de terceiros, não vinculados à Polícia Federal, adquiridos por mim durante o projeto.

A vigência da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste termo, terá a validade enquanto a informação não for tornada de conhecimento público por qualquer outra pessoa, ou mediante autorização escrita, concedida à minha pessoa pela coordenação do projeto.

A multa aplicável em caso de quebra deste termo de sigilo, será aquela enunciada no subitem 23.2.2 do Termo de Referência.

Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

E, por ser verdade, firmamos o presente.

Local e Data

_____

Nome:
CPF:
Endereço – telefone – fax:
E-mail:

ANEXO IV - MODELO DO TERMO DE CIÊNCIA

Contrato nº			
Objeto:			
Gestor do Contrato:		**Mat.:**	
Contratante:			
Contratada:		**CNPJ:**	
Preposto da Contratada:		**CPF:**	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o Termo de Responsabilidade e Sigilo e das normas de segurança vigentes na Polícia Federal.

Também declaram que estão cientes de que a estrutura computacional disponibilizada pela Contratante não poderá ser utilizada para fins particulares e que a navegação em sítios da internet e as correspondências em meio eletrônico utilizando o endereço eletrônico da Contratante, ou acessados a partir dos seus equipamentos poderão ser auditadas. Declaram, ainda, que não farão uso em benefício próprio de nenhum dos recursos disponíveis na Polícia Federal, tais como: telefones, impressoras, e-mail, acesso à internet, entre outros.

_____, _____ de _____ de 20_____

CIÊNCIA

Funcionários da Contratada	
Nome: Matrícula:	Assinatura:
Nome: Matrícula:	Assinatura:
Nome: Matrícula:	Assinatura:
Nome: Matrícula:	Assinatura:
Nome: Matrícula:	Assinatura:
Nome: Matrícula:	Assinatura:
Nome: Matrícula:	Assinatura:
Nome: Matrícula:	Assinatura:
Nome: Matrícula:	Assinatura:
Nome: Matrícula:	Assinatura:

ANEXO V - EXEMPLO DE ORDEM DE SERVIÇO - OS

Data do Envio:

dd/mm/aaaa hh:mm:ss

De:

PF/cgti@dpf.gov.br

Para:

Preposto da CONTRATADA

Assunto:

Projeto x - Ordem de Serviço para apoio gerencial a projeto.

Mensagem:

Apoiar a elaboração e a execução do projeto referido neste protocolo.

Documento assinado eletronicamente por **PAULO RODRIGO BRITO E SILVA**, **Agente Administrativo**, em 13/09/2018, às 16:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **HENDERSON DIAS DE OLIVEIRA**, **Agente de Telecomunicações e Eletricidade**, em 13/09/2018, às 17:04, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **WELINGTON RODRIGUES SILVA**, **Agente de Telecomunicações e Eletricidade**, em 14/09/2018, às 08:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **JOSE DONISETH DANTAS DE OLIVEIRA**, **Agente de Telecomunicações e Eletricidade**, em 14/09/2018, às 08:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **ALILTON MOREIRA DE ASSIS**, **Agente de Telecomunicações e Eletricidade**, em 11/10/2018, às 07:12, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.dpf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **8238376** e o código CRC **F6FE1110**.

Referência: Processo nº 08206.300573/2016-10 SEI nº 8238376

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO - PARANÁ
SLC – (41) 3310-7344 – slc@trt9.jus.br
Av. Vicente Machado, 147, 10º andar – Curitiba – PR, CEP 80420-905

ATESTADO DE CAPACIDADE TÉCNICA Nº 47/2024

Referência: Pregão 2/2023 (Processo PROAD 3762/2022)

Instrumento de Contrato: Contrato nº 22/2023

Prazo de vigência contratual: 21/6/2023 a 20/12/2025.

Contratada: CAM TECNOLOGIA EIREI LTDA., inscrita no CNPJ sob o nº 14.438.757/0001-76.

Objeto: Contratação de solução de telefonia institucional totalmente IP com alta disponibilidade e escalabilidade - PABX IP, com licença para 2700 ramais e 25 PAs, incluindo atualização, manutenção e suporte**.**

Item	Descrição	Quantidade
1	Solução de telefonia institucional totalmente IP com alta disponibilidade e escalabilidade - PABX IP, com licença para pelo menos 2700 ramais e 25 PAs, incluindo atualização, manutenção e suporte	28 meses, considerando o início após a conclusão do item 2
2	Projeto/Instalação/Configuração	1
3	Treinamento no sistema de comunicação PABX com tecnologia VoIP, turma com 6 vagas	1
4	SBC para 100 sessões SIP simultâneas, com HA, virtualizado em VM separada do PBX, incluindo atualização, manutenção e suporte.	1

A solução implantada abrange **todas as unidades do TRT9 no estado do Paraná**, e inclui:

1. **Sistema de telefonia totalmente IP com alta disponibilidade e escalabilidade (PABX IP)**, com:
    - **Licença para 2700 ramais** e **25 PAs (Posições de Atendimento)**;
    - **Manutenção**, **suporte técnico** e **atualizações contínuas**;
    - Gerenciamento e **provisionamento de aparelhos IP** de diferentes fabricantes, garantindo interoperabilidade e compatibilidade entre diversos modelos;
    - **Softphones para desktops e dispositivos móveis**, tanto para sistemas Android quanto iOS, assegurando mobilidade e flexibilidade aos usuários.
2. **Entroncamentos digitais E1** para integrar as unidades, permitindo comunicação eficiente entre os diversos pontos do Tribunal;
3. **SBC (Session Border Controller)** com suporte para **100 sessões SIP simultâneas**, virtualizado em ambiente separado do PABX, assegurando segurança e estabilidade no tráfego de voz;

4. **Projeto, instalação e configuração** da solução de telefonia para todas as unidades, cobrindo desde a fase de concepção até a implementação final;
5. **Treinamento técnico** para as equipes do TRT9, incluindo capacitação de 6 participantes no uso e gestão da solução VoIP.

ATESTAMOS, de acordo com as informações prestadas pela unidade gestora da contratação, a empresa vem executando satisfatoriamente a contratação, não havendo qualquer fato que a desabone.

Curitiba, *data da assinatura digital/eletrônica*.

(assinado digitalmente)
Nome: PAULO CELSO GERVA
Cargo/Função: Diretor da Secretaria de Licitações e Contratos
Conforme autorização delegada pela Portaria GP 22/2022

Embrapa Solos

Atestado de Capacidade Técnica

A EMBRAPA (EMPRESA BRASILEIRA DE AGROPRECUÁRIA) CNPS / SOLOS, com sede em RIO DE JANEIRO na Rua JARDIM BOTÂNICO nº 1024 Bairro JARDIM BOTÂNICO, CEP nº 22.460-000, CNPJ 00.348.003/0012-73, representada pelo senhor FLAVIO ARTHUR SOUZA DA COSTA, vem por meio desta atestar que a empresa CAM TECNOLOGIA EIRELI ME, situada na Avenida Pastor Martin Luther King Jr, 126 sala 326 Bloco 9 Torre Office 2000 no Bairro de Del Castilho, Rio de Janeiro/RJ, CEP nº 20.765-000 e inscrita no CNPJ 14.438.757/0001-76 atendeu-nos a contento não havendo nada que a desabone no fornecimento da prestação de serviços de implantação do PABX IP virtualizado CAMBOX para 150 ramais integrado transparentemente ao serviço fone@RNP, sendo responsável pela implantação, gestão e suporte do PABX IP CAMBOX para até 150 ramais, Gateway SIP/E1 EBS SERVER SPX 300 e o ambiente de virtualização VMWARE com atendimento presencial e/ou remoto, cumprido rigorosamente o nível de serviço e faturamento estabelecido no Pregão Eletrônico 07/2017 empenho 2017NE800118 e processo administrativo 16.00.21.00.400, desde o dia 05/12/2017 até o presente momento.

Rio de Janeiro, 22 de Janeiro de 2020.

FLAVIO ARTHUR SOUZA DA COSTA
SETOR DE INFRAESTRUTURA DE LOGÍSTICA DA EMBRAPA SOLOS
Assinatura Eletrônica

MARISA TEIXEIRA MATTIOLI
CHEFE ADJUNTO DE ADMINISTRAÇÃO DA EMBRAPA SOLOS
Assinatura Eletrônica

Documento assinado eletronicamente por **Flavio Arthur Souza da Costa**, **Supervisor**, em 23/01/2020, às 11:12, conforme art. 6º, parágrafo 1º do Decreto 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Marisa Teixeira Mattioli**, **Chefe-Adjunto**, em 24/01/2020, às 09:25, conforme art. 6º, parágrafo 1º do Decreto 8.539, de 8 de outubro de 2015.

A autenticidade do documento pode ser conferida no site https://sei.sede.embrapa.br/sei/controlador_externo.php?

acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **3773911** e o código CRC **6BA1B2EE**.

Referência: Processo nº 21201.400255/2017-39 SEI nº 3773911

Governo do Estado do Rio de Janeiro

Departamento de Trânsito do Estado do Rio de Janeiro

Diretoria de Apoio Operacional

Of.DETRAN/DIRAPOIO SEI Nº13 Rio de Janeiro, 13 de agosto de 2021
À CAM TECNOLOGIA EIRELI - ME
Avenida Pa stor Martin Luther King Júnior, nº 126, Torre 2000, sala 408 - Del Castilho
CEP nº 20.765-000 – Rio de Janeiro/RJ

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos para os devidos fins que a empresa CAM TECNOLOGIA EIRELI - ME, situada na Avenida Pa stor Martin Luther King Júnior, nº 126, Torre 2000, sala 408, no Bairro de Del Castilho, Rio de Janeiro/RJ, CEP nº 20.765-000, inscrita no CNPJ 14.438.757/0001-76, atendeu-nos a contento, não havendo nada que a desabone, no fornecimento da solução detalhada a seguir:

• Implementação de Solução Tecnológica para a Central de Atendimento (Call Center) com capacidade para 400 operadores simultâneos;
• 16 Troncos E1;
• URA Inteligente integrada ao Web Service para acesso à base de dados;
• 210 aparelhos VoIP Grandstream GXP2170;
• Instalação e treinamento;
• Suporte e manutenção.

A Solução foi adquirida através do Pregão Eletrônico nº 08/2020 e Contrato 060/2020 DETRAN/RJ, respeitando todos os prazos de entrega determinados.

RANDAL FARAH
Diretor Geral - Diretoria de Apoio Operacional
DETRAN/RJ - Id: 4398172-0

Documento assinado eletronicamente por **Randal Farah de Oliveira Leão**, **Diretor Geral**, em 13/08/2021, às 11:21, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **20909771** e o código CRC **B76E5A40**.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº SEI-150153/000998/2021 SEI nº 20909771

INSTITUTO
Pedro Ruiz
O Nascer de um novo olhar

ATESTADO DE CAPACIDADE TÉCNICA

INSTITUTO PEDRO RUIZ, com sede na cidade de São Paulo, no Endereço Av. Nova Independência, 1087 – Brooklin –, CNPJ 12.138.769/0001-50, representada pelo senhor RACHID DIEGO OLIVEIRA TEIXEIRA vem por meio desta atestar que a empresa CAM TECNOLOGIA LTDA, situada na Av. Pastor Martin Luther King Jr, 126, Torre 2000, sala 408, no Bairro de Del Castilho, Rio de Janeiro/RJ, CEP nº 20.765-000 e inscrita no CNPJ 14.438.757/0001-76, atende-nos a contento, não havendo nada que a desabone no fornecimento de serviço de PABX em nuvem, baseado em tecnologia de voz sobre IP, em infraestrutura baseada em datacenter TIER3, na modalidade serviço, com 20 ramais, DID/DDR, Telefones IP's e fornecimento de Minutos (fixo e móvel Brasil)..

Informamos ainda que o serviço é prestado, de forma continuada, tendo seu início ocorrido em 12/2023.

São Paulo, 30 de julho de 2024.

Rachid Diego Oliveira Teixeira
075.156.656-02

RACHID DIEGO OLIVEIRA TEIXEIRA

CEO

CPF: 075.156.656-02

ESTADO DE GOIÁS
GOIÁS TURISMO - AGÊNCIA ESTADUAL DE TURISMO
SUPERVISÃO DA TECNOLOGIA DA INFORMAÇÃO

ATESTADO DE CAPACIDADE TÉCNICA Nº: 3/2024 - GOIASTURISMO/SUPTI-12098

GOIANIA, 03 de outubro de 2024.

Atestamos para os devidos fins que a empresa CAM TECNOLOGIA LTDA, situada na Avenida Pastor Martin Luther King Júnior, nº 126, Torre 2000, sala 408, no Bairro de Del Castilho, Rio de Janeiro/RJ, CEP nº 20.765-000, inscrita no CNPJ 14.438.757/0001-76, atendeu-nos a contento no fornecimento da solução contratada através da Dispensa Eletrônica nº 105001/2024 – Contrato nº 22/2024, conforme detalhamento a seguir:

- SOLUÇÃO PABX IP EM NUVEM PARA 35 RAMAIS COM LICENÇA, CONFIGURAÇÃO, IMPLANTAÇÃO, TREINAMENTO E SERVIDOR;
- SERVIÇOS DE TELEFONIA, ENTRONCAMENTO DIGITAL E1 (R2D/ISDN) COM 30 CANAIS E A PORTABILIDADE DE 100 RAMAIS DDR COM TRÁFEGO FIXO-FIXO E FIXO-MÓVEL NACIONAL ILIMITADO.
- FORNECIMENTO EM COMODATO DE 35 (TRINTA E CINCO) APARELHOS TELEFÔNICOS IP MODELO GXP1630 - GRANDSTREAM

Atestamos ainda que a citada empresa desempenha suas atividades com a mais relevante responsabilidade, cumprindo assim todas as cláusulas pertinentes ao contrato e que nada consta, até a presente data, em nossos arquivos que possa desaboná-la moral e profissionalmente.

(documento assinado eletronicamente)
JÂNIO GUILHERME SOARES JÚNIOR
Gestor do Contrato nº 22/2024
Responsável pelas informações

Documento assinado eletronicamente por **JANIO GUILHERME SOARES JUNIOR**, **Supervisor (a)**, em 04/10/2024, às 07:34, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1** informando o código verificador **65711299** e o código CRC **EA72FB4F**.

SUPERVISÃO DA TECNOLOGIA DA INFORMAÇÃO
RUA 30 , s/n, Bl. A, 2º Andar do Centro de Convenções de Goiânia - Bairro SETOR CENTRAL - GOIANIA - GO - CEP 74015-180 - 32018122.

Referência:
Processo nº 202400027000826

SEI 65711299

ATESTADO DE CAPACIDADE TÉCNICA

Curvelo, 17 de Março de 2025.

Atestamos para os devidos fins que a empresa **CAM TECNOLOGIA LTDA - ME**, situada na **Avenida Pastor Martin Luther King Jr., nº 126, Bloco 9, Sala 408, Torre 2, Del Castilho, Rio de Janeiro/RJ, CEP 20.765-000**, inscrita no **CNPJ 14.438.757/0001-76**, atendeu-nos satisfatoriamente na execução dos serviços contratados por meio da **Dispensa de Licitação nº 030/2024 – Contrato nº 103/2024**, conforme detalhamento a seguir:

SERVIÇOS EXECUTADOS

- **Fornecimento de Serviço de Telefonia Fixa Comutada (STFC) via SIP** para **150 números** da Prefeitura Municipal de Curvelo/MG;
- **Portabilidade de 150 números fixos e 1 número 0800** utilizados nas diversas Unidades Administrativas do Município;
- **Configuração, ativação e operacionalização completa de 30 canais de entrada para chamadas simultâneas**;
- **Suporte técnico especializado e atendimento remoto 24/7 para casos emergenciais**;
- **Implementação de troncos SIP para chamadas locais e de longa distância nacional (fixo-fixo e fixo-móvel)**;
- **Ativação e integração dos números portados à infraestrutura telefônica do município**;
- **Treinamento básico aos responsáveis pelo uso do sistema**.

Atestamos ainda que a referida empresa desempenhou suas atividades com total responsabilidade e competência, cumprindo todas as cláusulas contratuais pertinentes. Não há, até a presente data, qualquer registro em nossos arquivos que possa desaboná-la técnica ou profissionalmente.

Nome do Responsável: **Vitor Augusto Assis Barcelos**
Cargo: **Secretário Municipal de Administração, Políticas Sociais e Desenvolvimento Sustentável**
Município de Curvelo – MG

PREFEITURA DA CIDADE DO RIO DE JANEIRO

Secretaria Municipal de Fazenda

ALVARÁ DE LICENÇA PARA ESTABELECIMENTO

INSCRIÇÃO MUNICIPAL	CNPJ / CPF	PROCESSO DE CONCESSÃO	ÚLTIMO PROCESSO DE DEFERIMENTO	IRLF/GRLF
0533626-0	14.438.757/0001-76	04/745.634/2011	04/919.244/2023	GRLF6 - Meier

CONCEDIDO A

CAM TECNOLOGIA LTDA

PARA SE ESTABELECER NO

Avenida Pastor Martin Luther King Jr., 00126, BLC 9 SAL 408 TOR 2, Del Castilho

COM AS SEGUINTES ATIVIDADES DO CÓDIGO DE ATIVIDADES ECONÔMICAS (CAE)

4.16.10.0 - MAQUINAS E SUPRIMENTOS PARA PROCESSAMENTO DE DADOS - COMERCIO VAREJISTA
4.19.01.0 - APARELHOS DE TELECOMUNICAÇÃO-COMERCIO VAREJISTA
2.19.32.0 - POSTAGEM E TELEGRAFIA, SERVIÇOS DE
2.56.05.6 - TELEFONIA, SERVIÇOS DE
2.56.06.4 - TELECOMUNICAÇÃO
2.26.64.5 - GERAÇÃO DE PROGRAMAS DE COMPUTADOR SOB ENCOMENDA
2.27.12.9 - CONSULTORIA TÉCNICA
2.26.45.9 - PROCESSAMENTO DE DADOS
2.26.69.6 - PROVIMENTO DE ACESSO E INFORMAÇÕES JUNTO À INTERNET
2.17.04.2 - ALUGUEL DE MÁQUINAS PARA PROCESSAMENTO DE DADOS
2.17.17.4, 2.43.05.1

COM AS SEGUINTES RESTRIÇÕES

VEDADOS INCOMODOS E PREJUIZOS A VIZINHANCA
VEDADA A PRESTACAO DE SERVICOS NO LOCAL
VEDADO O EXERCICIO DA ATIVIDADE NO LOCAL
VEDADA A CIRCULACAO DE MERCADORIAS NO LOCAL
SIMPLES ESCRITORIO

OBSERVAÇÕES

A concessão deste Alvará não importa, entre outros, no reconhecimento de regularidade do estabelecimento quanto a quaisquer normas aplicáveis ao seu funcionamento, especialmente as de proteção da saúde, condições de edificação, instalação de máquinas e equipamentos, prevenção contra incêndios e exercício de profissões.

Códigos CNAE's: 4751-2/01, 4752-1/00, 6110-8/99, 6110-8/01, 6110-8/03, 6120-5/99, 6190-6/02, 6190-6/99, 6201-5/01, 6209-1/00, 6311-9/00, 7733-1/00, 7739-0/99, 9511-8/00

Rio de Janeiro, 30 de Novembro de 2023	Deferido automaticamente conforme decreto 41827/2016

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES

ATO Nº 17433, DE 18 DE DEZEMBRO DE 2023

O GERENTE DE OUTORGA E LICENCIAMENTO DE ESTAÇÕES DA AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, no uso das atribuições que lhe foram conferidas pelo art. 183, do Regimento Interno da Anatel, aprovado pela Resolução nº 612, de 29 de abril de 2013, e

CONSIDERANDO o disposto na Portaria n.º 1.919, de 20 de setembro de 2019, que delega competência à Gerência de Outorga e Licenciamento de Estações para outorgar autorização para exploração de serviços de telecomunicações e de autorização de uso de radiofrequências, não decorrentes de procedimentos licitatórios, bem como decidir pela adaptação, prorrogação e extinção, exceto por caducidade, e

CONSIDERANDO o disposto no Regulamento dos Serviços de Telecomunicações, aprovado pela Resolução nº 73, de 25 de novembro de 1998;

CONSIDERANDO que, conforme dispõe o § 1º do art. 3º do Regulamento Geral de Outorgas, aprovado pela Resolução nº 720, de 10 de fevereiro de 2020, a autorização para a exploração de serviço de telecomunicações será expedida por prazo indeterminado e a título oneroso, e independerá de licitação, salvo em caso de impossibilidade técnica ou, excepcionalmente, quando o excesso de competidores puder comprometer a prestação de uma modalidade de serviço de interesse coletivo;

CONSIDERANDO o constante dos autos do processo nº 53500.110605/2023-38,

RESOLVE:

Art. 1º Expedir autorização à CAM TECNOLOGIA LTDA, CNPJ/MF nº 14.438.757/0001-76, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, sem caráter de exclusividade, e tendo como área de prestação de serviço todo o território nacional.

Parágrafo único. O uso de radiofrequência, quando necessário, tendo ou não caráter de exclusividade, dependerá de prévia outorga da Agência, mediante autorização, nos termos da regulamentação e da respectiva consignação, que se dará mediante ato da Superintendência de Outorga e Recursos à Prestação desta Agência.

Art. 2º Estabelecer que o preço devido pelo direito de exploração do serviço de que trata o art. 1º deste Ato é de R$ 400,00 (quatrocentos reais), de acordo com a Resolução nº 720, de 10 de fevereiro de 2020, da Anatel.

Art. 3º Estabelecer que os equipamentos que compõem as estações de telecomunicações do serviço devem ter certificação expedida ou aceita pela Anatel, segundo as normas vigentes.

Art. 4º Este Ato entra em vigor na data de publicação de seu extrato no Diário Oficial da União.

Documento assinado eletronicamente por **Renato Sales Bizerra Aguiar**, **Gerente de Outorga e Licenciamento de Estações**, em 19/12/2023, às 10:28, conforme horário oficial de Brasília, com fundamento no art. 23, inciso II, da Portaria nº 912/2017 da Anatel.

A autenticidade deste documento pode ser conferida em http://www.anatel.gov.br/autenticidade, informando o código verificador **11287652** e o código CRC **0B31D084**.

Referência: Processo nº 53500.110605/2023-38 SEI nº 11287652

Nº 17.092 - Processo nº 53500.109143/2023-14. Outorga Autorização de Uso de Radiofrequência à Universidade Federal de Pernambuco, CNPJ 24.134.488/0001-08, executante do Serviço de Radiodifusão Sonora em Onda Média, na localidade de Recife/PE.

Nº 17.093 - Processo nº 53500.109420/2023-81. Outorga Autorização de Uso de Radiofrequência à RÁDIO DIFUSORA DE SÃO JOÃO NEPOMUCENO LTDA-ME, CNPJ 24.801.367/0001-72, executante do Serviço de Radiodifusão Sonora em Frequência Modulada, na localidade de São João Nepomuceno/MG.

RENATO SALES BIZERRA AGUIAR
Gerente

ATOS DE 11 DE DEZEMBRO DE 2023

Nº 17.098 - Processo nº 53500.097062/2023-56. Outorga Autorização de Uso de Radiofrequência à CAMARA DOS DEPUTADOS, CNPJ 00.530.352/0001-59, executante do Serviço de Radiodifusão Sonora em Frequência Modulada, na localidade de Caxias do Sul/RS.

Nº 17.099 - Processo nº 53500.097947/2023-55. Outorga Autorização de Uso de Radiofrequência à CAMARA DOS DEPUTADOS, CNPJ 00.530.352/0001-59, executante do Serviço de Radiodifusão Sonora em Frequência Modulada, na localidade de Luís Eduardo Magalhães/BA.

Nº 17.100 - Processo nº 53500.106490/2023-87. Outorga Autorização de Uso de Radiofrequência à SISTEMA TRANSRIO DE COMUNICACAO LTDA, CNPJ 30.913.990/0001-10, executante do Serviço de Radiodifusão Sonora em Frequência Modulada, na localidade de Rio de Janeiro/RJ.

Nº 17.101 - Processo nº 53500.109767/2023-23. Outorga Autorização de Uso de Radiofrequência à EMPRESA DE RADIODIFUSAO TUPINAMBAS LTDA, CNPJ 24.614.471/0001-58, executante do Serviço de Radiodifusão Sonora em Frequência Modulada, na localidade de Dourados/MS.

Nº 17.102 - Processo nº 53500.109797/2023-30. Outorga Autorização de Uso de Radiofrequência à Radio Eldorado de Lagarto Ltda, CNPJ 13.002.084/0001-44, executante do Serviço de Radiodifusão Sonora em Frequência Modulada, na localidade de Lagarto/SE.

RENATO SALES BIZERRA AGUIAR
Gerente

ATOS DE 13 DE DEZEMBRO DE 2023

Nº 17.250 - Processo nº 53500.101474/2023-06. Outorga Autorização de Uso de Radiofrequência à SOCIEDADE WM DE COMUNICACAO S/C LTDA, CNPJ 00.097.163/0001-34, executante do Serviço de Retransmissão de Radiodifusão de Sons e Imagens - Digital, na localidade de Cambé/PR.

Nº 17.251 - Processo nº 53500.110094/2023-54. Outorga Autorização de Uso de Radiofrequência à RADIO, TV E JORNAL IMPRESSO AMAZONIA LTDA, CNPJ 08.776.018/0001-91, executante do Serviço de Radiodifusão Sonora em Frequência Modulada, na localidade de Acrelândia/AC.

Nº 17.252 - Processo nº 53500.107959/2023-03. Outorga Autorização de Uso de Radiofrequência à FUNDACAO CANDIDO GARCIA, CNPJ 04.166.662/0001-97, executante do Serviço de Retransmissão de Radiodifusão de Sons e Imagens - Digital, na localidade de Guaíra/PR.

Nº 17.253 - Processo nº 53500.109418/2023-10. Outorga Autorização de Uso de Radiofrequência à FUNDACAO JOAO XXIII, CNPJ 20.599.387/0001-51, executante do Serviço de Radiodifusão Sonora em Frequência Modulada, na localidade de Governador Valadares/MG.

Nº 17.254 - Processo nº 53500.110388/2023-86. Outorga Autorização de Uso de Radiofrequência à FUNDACAO CRUZEIRENSE DE JORNALISMO E RADIODIFUSAO, CNPJ 45.387.222/0001-47, executante do Serviço de Radiodifusão Sonora em Frequência Modulada, na localidade de Cruzeiro/SP.

RENATO SALES BIZERRA AGUIAR
Gerente

ATOS DE 14 DE DEZEMBRO DE 2023

Nº 17.279 - Processo nº 53500.110689/2023-18. Outorga Autorização de Uso de Radiofrequência à NASCENTE COMUNICACOES LTDA, CNPJ 02.374.730/0001-88, executante do Serviço de Radiodifusão Sonora em Frequência Modulada, na localidade de Mongaguá/SP.

Nº 17.280 - Processo nº 53500.110290/2023-29. Outorga Autorização de Uso de Radiofrequência à TELEVISAO INDEPENDENTE DE SAO JOSE DO RIO PRETO LTDA, CNPJ 61.413.092/0001-26, executante do Serviço de Retransmissão de Radiodifusão de Sons e Imagens - Digital, na localidade de Nova Era/MG.

Nº 17.285 - Processo nº 53500.098314/2023-64. Expede autorização à DIGITAL TELECOM PROVEDOR DE INTERNET LTDA, CNPJ/MF nº 35.560.038/0001-01, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

Nº 17.289 - Processo nº 53500.110096/2023-43. Expede autorização à ENTECH TELECOM LTDA, CNPJ/MF nº 44.705.769/0001-80, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

RENATO SALES BIZERRA AGUIAR
Gerente

ATOS DE 17 DE DEZEMBRO DE 2023

Nº 17.372 - Processo nº 53500.107002/2023-59. Expede autorização à WAVECOM TECNOLOGIA LTDA, CNPJ/MF nº 33.910.293/0001-01, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

Nº 17.373 - Processo nº 53500.110749/2023-94. Expede autorização à CH2 TELECOM LTDA, CNPJ/MF nº 26.961.509/0001-94, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

Nº 17.374 - Processo nº 53500.110233/2023-40. Expede autorização à VOXBIT LTDA, CNPJ/MF nº 52.590.019/0001-39, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

Nº 17.375 - Processo nº 53500.074123/2023-15. Declara extinta, por renúncia, a partir de 08/09/2023, a autorização outorgada a NET MARIANA INFORMÁTICA LTDA, CNPJ/MF nº 20.395.768/0001-19, por intermédio do Ato nº 4334, de 13/08/2020, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

RENATO SALES BIZERRA AGUIAR
Gerente

ATOS DE 18 DE DEZEMBRO DE 2023

Nº 17.382 - Processo nº 53500.110221/2023-15. Expede autorização à L DE MOURA BORBA QUEIROZ LTDA, CNPJ/MF nº 46.110.017/0001-00, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

Nº 17.383 - Processo nº 53500.110196/2023-70. Expede autorização à VENN BRASIL LTDA, CNPJ/MF nº 53.107.768/0001-25, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

Nº 17.385 - Processo nº 53500.007409/2021-15. Extingue, por cassação, a autorização para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, expedida à SRMINAS LTDA, CNPJ nº 13.266.344/0001-99, por meio do Ato nº 4334, de 13/08/2020, tendo em vista a perda de condição indispensável à manutenção da autorização, com fulcro nos arts. 133 e 139 da Lei nº 9472, de 16/07/1997.

Nº 17.403 - Processo nº 53500.110714/2023-55. declara extinta, por renúncia, a partir de 07/12/2023, a autorização outorgada à AVATO DATACENTER S.A., CNPJ/MF nº 12.495.265/0001-97, por intermédio do Ato nº 4334, de 13/08/2020, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

Nº 17.432 - Processo nº 53500.110243/2023-85. Expede autorização à VOEE TELECOM COMUNICACOES LTDA, CNPJ/MF nº 46.770.237/0001-52, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

Nº 17.433 - Processo nº 53500.110605/2023-38. Expede autorização à CAM TECNOLOGIA LTDA, CNPJ/MF nº 14.438.757/0001-76, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

Nº 17.434 - Processo nº 53500.111087/2023-70. Expede autorização à CONNECT PLUS SERVICOS DE TELEFONIA LTDA, CNPJ/MF nº 48.100.442/0001-36, para explorar Serviços de Telecomunicações de Interesse Coletivo e de Interesse Restrito, por prazo indeterminado, em todo o território nacional.

RENATO SALES BIZERRA AGUIAR
Gerente

ATO Nº 17.478, DE 19 DE DEZEMBRO DE 2023

Processo n° 53500.109529/2023-18. Outorga autorização de uso de radiofrequência(s) à Brisanet Serviços de Telecomunicações S.A., CNPJ nº 04.601.397/0001-28, associada à autorização para execução do Serviço Móvel Pessoal.

RENATO SALES BIZERRA AGUIAR
Gerente

Ministério da Cultura

SECRETARIA DO AUDIOVISUAL

PORTARIA Nº 85, DE 18 DE DEZEMBRO DE 2023

O(A) SECRETÁRIA DO AUDIOVISUAL, no uso de suas atribuições legais, que lhe confere a Portaria nº 1.408, de 31 de janeiro de 2023 e o art. 1º da Portaria nº 1.201, de 18 de dezembro de 2009, resolve:

Art. 1º - Aprovar a complementação de valor em favor do(s) projeto(s) cultural(is) relacionado(s) no(s) anexo(s) desta Portaria, para o(s) qual (is) o(s) proponente(s) fica(m) autorizado(s) a captar recursos, mediante doações ou patrocínios, na forma prevista no § 1º do artigo 18 e no artigo 26 da lei n.º 8.313, de 23 de dezembro de 1991, alterada pela Lei nº 9.874, de 23 de novembro de 1999.

221659 - ECOCINE ITINERANTE 3ª EDIÇÃO
JK PROJETOS ESPORTIVOS E CULTURAIS LTDA
CNPJ/CPF: 27.501.490/0001-66
Cidade: Brasília - DF;
Valor Complementado: R$ 49.912,66
Valor total atual: R$ 449.657,00

Art. 2º - Aprovar o(s) projeto(s) cultural(is), relacionado(s) no(s) anexo(s) desta Portaria, para o(s) qual(is) o(s) proponente(s) fica(m) autorizado(s) a captar recursos, mediante doações ou patrocínios, na forma prevista no § 1º do artigo 18 e no artigo 26 da Lei n.º 8.313, de 23 de dezembro de 1991, alterada pela Lei nº 9.874, de 23 de novembro de 1999.

Art. 3º - Esta portaria entra em vigor na data de sua publicação.

JOELMA OLIVEIRA GONZAGA

ANEXO I
Artigo 18 , § 1º

2310233 - Cine Form(ação)
LUIZ GUSTAVO BRASILEIRO PEIXOTO DE MORAES 41311767851
CNPJ/CPF: 32.153.253/0001-91
Processo: 01400029072202393
Cidade: Jacareí - SP;
Valor Aprovado: R$ 512.325,00
Prazo de Captação: 19/12/2023 à 31/12/2023
Resumo do Projeto: O projeto "Cine Form(ação)" consiste em 12 ações de exibições públicas de obras audiovisuais, com enfoque em 4 eixos temáticos: Cine Formação, Cine Diversidade, Cine Mulher e Cineclubinho. O objetivo é utilizar o cinema como plataforma de reflexão e promover debates sobre questões de relevância contemporânea. Atualmente contamos com uma parceria estratégica com a Mostra Ecofalantes e a Aliança Francesa (Taubaté) para a criação da curadoria das ações.

2310243 - TEATRO NA TELA - UMA EXPERIÊNCIA DIFERENTE
Porto e Stein Produções Ltda.-ME.
CNPJ/CPF: 11.144.407/0001-09
Processo: 01400029082202329
Cidade: Vitória - ES;
Valor Aprovado: R$ 524.159,11
Prazo de Captação: 19/12/2023 à 31/12/2023
Resumo do Projeto: Exibição gratuita de registros audiovisuais de espetáculos teatrais em formato itinerante.

2310426 - O Voo da Águia - O Filme
ALINE CRISTINA PEREIRA DOS REIS
CNPJ/CPF: 387.622.078-57
Processo: 01400029267202333
Cidade: São José dos Campos - SP;
Valor Aprovado: R$ 895.395,60
Prazo de Captação: 19/12/2023 à 31/12/2023
Resumo do Projeto: "O Voo da Águia - O Filme" é um projeto cinematográfico que revela a história e paixão do São José Esporte Clube. O media metragem de 1 hora explora bastidores e momentos marcantes do time.

CREA-RJ

Conselho Regional de Engenharia e Agronomia do Estado do Rio de Janeiro

CERTIDÃO DE REGISTRO PROFISSIONAL

50013/2025

VÁLIDA ATÉ: 31/12/2025

Certificamos que o profissional abaixo citado encontra-se registrado neste Conselho, nos termos da Lei Federal número 5.194, de 24 de dezembro de 1.966. Certificamos ainda, face ao estabelecido nos artigos 68 e 69 da referida Lei, que o interessado não se encontra em débito com o Crea-RJ.

DADOS DO REGISTRO

Nome:	THIAGO FRENSCH		
Registro:	2014112104	Data de Registro:	22/05/2014
Carteira:	RJ-/D	Emitida em:	22/05/2014
CPF:	106.027.417-50		
RNP:	2013262108		

Título: ENGENHEIRO DE TELECOMUNICAÇÕES
Atribuições:
RES 218/73 - ART 08(AT.01 A 18)
RES 218/73 - ART 09(AT.01 A 18)
Formado pelo(a): UNIVERSIDADE FEDERAL FLUMINENSE
Data colação de grau: 14/03/2010

FINALIDADE DA CERTIDÃO: PARA FINS DE LICITAÇÃO

Certidão de Registro Profissional nº 50013/2025
Emitida às: 02/04/2025 18:53 (hora de Brasília)
Código de controle do comprovante: 0.8007640594533515

A autencididade e a validade desta certidão deve ser confirmada no site do Crea-RJ (www.crea-rj.org.br).

A falsificação deste documento constitui crime previsto no Código Penal Brasileiro, sujeitando o autor à respectiva ação penal.

Esta certidão perderá a validade caso ocorra qualquer alteração posterior dos elementos cadastrais nela contidos desde que não representem a situação correta ou atualizada do registro.

Válida em todo território nacional.

CREA-RJ

Conselho Regional de Engenharia e Agronomia do Estado do Rio de Janeiro

CERTIDÃO DE REGISTRO DE PESSOA JURÍDICA

50016/2025

VÁLIDA ATÉ: 31/12/2025

Certificamos que a Pessoa Jurídica, abaixo citada, encontra-se registrada neste Conselho, nos termos da Lei Federal Nº 5194, de 24 de dezembro de 1966, não apresentando débitos para com o Crea-RJ até a presente data, assim como seus responsáveis técnicos. As atividades da empresa estão restritas ao(s) ramo(s) especificado(s) nesta CERTIDÃO e somente podem ser exercidas com a participação efetiva do(s) respectivo(s)responsável(eis) técnico(s).

DADOS DO REGISTRO

Registro:	2016201124
Razão Social:	CAM TECNOLOGIA LTDA
CNPJ:	14.438.757/0001-76
Data Registro:	26/09/2016
Endereço	AVENIDA PASTOR MARTIN LUTHER KING JR 126 BLOCO 9 TORRE 2000 SALA 326 DEL CASTILHO - RIO DE JANEIRO - RJ , CEP: 20765-000

RAMOS ATIVIDADE :

2030-0	OBRAS E SERVICOS DE ENGENHARIA ELETRONICA / OS ENG ELETRONICA
2040-0	OBRAS E SERVICOS DE ENGENHARIA DE TELECOMUNICACOES / OS ENG DE TELECOMUNICACOES

CAPITAL SOCIAL:

R$ 100.000,00 (MATRIZ)

OBJETO SOCIAL:

1-DESENVOLVIMENTO DE PROGRAMAS DE COMPUTADOR SOB ENCOMENDA; 2-SUPORTE TÉCNICO, ANÁLISE, PROJETO, MANUTENÇÃO, GERÊNCIA DE SISTEMAS DE INFORMAÇÃO E PARA INTERNET E TREINAMENTO; 3-OUTROS SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO; 4-COMÉRCIO DE PRODUTOS E EQUIPAMENTOS DE INFORMÁTICA.

CLASSE:

A - EXECUCAO DE OBRA, PRESTACAO DE SERVICOS, DESENVOLVIMENTO DE ATIVIDADE TECNICA

RESPONSÁVEL(EIS) TÉCNICO(S):

THIAGO FRENSCH

RNP: 2013262108 Registro: 2014112104 expedido em 22/05/2014

TÍTULO: ENGENHEIRO DE TELECOMUNICAÇÕES

Atribuições: RES 218/73 - ART 08(AT.01 A 18)
RES 218/73 - ART 09(AT.01 A 18)

Inclusão como QT: 26/09/2016 Inclusão como RT: 26/09/2016

Ramo Atividade: OBRAS E SERVICOS DE ENGENHARIA ELETRONICA / OS ENG ELETRONICA

Inclusão como QT: 26/09/2016 Inclusão como RT: 26/09/2016

Ramo Atividade: OBRAS E SERVICOS DE ENGENHARIA DE TELECOMUNICACOES / OS ENG DE TELECOMUNICACOES

CREA-RJ

Conselho Regional de Engenharia e Agronomia do Estado do Rio de Janeiro

CERTIDÃO DE REGISTRO DE PESSOA JURÍDICA

50016/2025

VÁLIDA ATÉ: 31/12/2025

(Continuação da Certidão de Registro de Pessoa Jurídica Nº 50016/2025)

FINALIDADE DA CERTIDÃO: Fins de concorrência publica

Certidão de Registro de Pessoa Jurídica nº 50016/2025

Emitida às: 02/04/2025 18:54 (hora de Brasília)

Código de controle do comprovante: 0.8411275128164487

A capacidade técnico profissional da empresa é comprovada pelo conjunto dos acervos técnicos dos profissionais constantes de seu quadro técnico.

A autencidade e a validade desta certidão deve ser confirmada no site do Crea-RJ (www.crea-rj.org.br).

A falsificação deste documento constitui crime previsto no Código Penal Brasileiro, sujeitando o autor à respectiva ação penal.

Esta certidão perderá a validade caso ocorra qualquer alteração posterior dos elementos cadastrais nela contidos desde que não representem a situação correta ou atualizada do registro.

Fica reservado ao Crea-RJ o direito de cobrar qualquer importância que venha a ser considerada devida.

Válida em todo território nacional.


CAM TECNOLOGIA LTDA
14/07/2025
Issabel
PARTNER
CERTIFIED

YEASTAR

CERTIFIED CLOUD ASSOCIATE

This is to certify that

Thiago Maluf

Has been conferred the "Yeastar Certified Cloud Associate" Certificate
for P-Series PBX System Cloud Edition

Issued on: Mar 13th, 2025
Valid until: Mar 13th, 2028

DATE

Nick Chen
CEO

SIGNATURE

Certification No.: CCA26250300277

2020080409KM

KHOMP
ACADEMY

CERTIFICADO

THIAGO MALUF RESENDE

PARTICIPOU DO TREINAMENTO TÉCNICO AVANÇADO ABAIXO:
"LINHA VSBC ONE",
Realizado no período de: **10 de março de 2023**
Carga Horária: **04 horas**

KHOMP

Giancarlo Granzotto Macedo
Diretor Presidente

2020080409KM

KHOMP
ACADEMY

CERTIFICADO

FÁBIO CARVALHOSA SANCHEZ

PARTICIPOU DO TREINAMENTO TÉCNICO AVANÇADO ABAIXO:
"LINHA VSBC ONE",
Realizado no período de: **10 de março de 2023**
Carga Horária: **04 horas**

KHOMP

Giancarlo Granzotto Macedo
Diretor Presidente

2020080409KM

KHOMP
ACADEMY

CERTIFICADO

FÁBIO CARVALHOSA SANCHEZ

PARTICIPOU DO TREINAMENTO TÉCNICO AVANÇADO ABAIXO:
"LINHA KMG ONE",
Realizado no período de: **10 de março de 2023**
Carga Horária: **08 horas**

KHOMP

Giancarlo Granzotto Macedo
Diretor Presidente

2020080409KM

KHOMP
ACADEMY

CERTIFICADO

THIAGO MALUF RESENDE

PARTICIPOU DO TREINAMENTO TÉCNICO AVANÇADO ABAIXO:
"LINHA KMG ONE",
Realizado no período de: **10 de março de 2023**
Carga Horária: **08 horas**

KHOMP

Giancarlo Granzotto Macedo
Diretor Presidente

2o. Ofício do Registro de Distribuição

RUA DO CARMO, 8 - 3o. ANDAR

CERP: 2025.5342525.799-1

REQUERIDA EM: 06/10/2025

967831
01/49 Pag: 0001

MODELO(C)>> CERTIFICA A a B <<

PARA FINS DE: LICITACAO

Paulo Felippe de Oliveira Silva - Responsável pelo Expediente

CERTIDÃO DE REGISTRO DE DISTRIBUIÇÃO DE FEITOS AJUIZADOS

O REGISTRADOR DO 2o. OFÍCIO DO REGISTRO DE DISTRIBUIÇÃO DA CIDADE E COMARCA DO RIO DE JANEIRO, CAPITAL DO ESTADO DO RIO DE JANEIRO.

C E R T I F I C A e D Á F É

QUE REVENDO OS LIVROS E ASSENTAMENTOS DAS DISTRIBUIÇÕES EM CURSO OU ANDAMENTO SOBRE:

A - Ações de Falência ou Concordata; demais ações e precatorias distribuídas as Varas Empresariais, bem como, Inqueritos Judiciais Falimentares ou Falências Dolosas as Varas Criminais ou outras (art.186 da Lei de Falências), Recuperações Judiciais;

B - Interdições previstas pela Lei no. 6024 desde 13/03/1974, que trata da intervenção e Liquidação Extrajudicial de Instituições Financeiras pelo Banco Central,do Brasil ou Ministério da Fazenda, desde:

DOIS DE OUTUBRO DE DOIS MIL E CINCO ATÉ DOIS DE OUTUBRO DE DOIS MIL E VINTE E CINCO (02/10/2005 a 02/10/2025) dele(s).-

.-.-.-.-.-.-.-.NADA CONSTA.-.-.-.-.-.-.-.-

Relativamente ao Nome de CAM TECNOLOGIA LTDA Qualificação: 14438757000176 (conforme requerido).-.

EMITIDA EM: 07/10/2025, RIO DE JANEIRO, COMARCA DA CAPITAL

EU REGISTRADOR ASSINO. **T O T A L R$: 0.00**

Senhor usuário, se necessário, é possível obter certidão que abranja outros períodos de consulta para além do pesquisado. Informe-se com o cartório do distribuidor.

Poder Judiciário - TJERJ
Corregedoria Geral de Justiça
Codigo Identificador de Certidao
CACR50648-GJM
Consulte a validade do CIC em:
http://www4.tjrj.jus.br/Portal-Extrajudicial/

Esta certidão eletrônica estará disponível para download e validação no Portal Exrtajudicial (acesso pela página do TJRJ/Corregedoria/Extrajudicial/Portal Extrajudicial) pelo período de 90 (noventa) dias após sua emissão.

A autenticidade desta certidão deverá ser confirmada na - TJRJ (http://www4.tjrj.jus.br/Portal-Extrajudicial/consultaselo/)
A certidão eletrônica estará disponível para download pelo período de 90 (noventa) dias após a sua emissão.

COEFICIENTES DE ANÁLISES EM 31/12/2024

Coeficiente	Fórmula	Valor	Resultado
Índice de Liquidez Geral	Ativo Circulante + Realizável Longo Prazo	2.045.859,19 + 0,00	1,99
	Passivo Circulante + Passivo Não-Circulante	1.029.458,43 + 0,00	
Índice de Liquidez Corrente	Ativo Circulante	2.045.859,19	1,99
	Passivo Circulante	1.029.458,43	
Índice de Solvência Geral	Ativo	2.045.859,19	1,99
	Passivo Circulante + Passivo Não-Circulante	1.029.458,43 + 0,00	
Índice de Endividamento Geral	Passivo Circulante + Passivo Não-Circulante	1.029.458,43 + 0,00	0,50
	Passivo Total	2.045.859,19	

JOAO PAULO DE AZEVEDO ROSA:11364632756

Assinado de forma digital por JOAO PAULO DE AZEVEDO ROSA:11364632756
Dados: 2025.07.01 16:47:51 -03'00'

TERMOS DE ABERTURA E ENCERRAMENTO

Entidade:	CAM TECNOLOGIA LTDA		
Período da Escrituração:	01/01/2024 a 31/12/2024	CNPJ:	14.438.757/0001-76
Número de Ordem do Livro:	14		

TERMO DE ABERTURA

Nome Empresarial	CAM TECNOLOGIA LTDA
NIRE	
CNPJ	14.438.757/0001-76
Número de Ordem	14
Natureza do Livro	LIVRO DIARIO
Município	RIO DE JANEIRO
Data do arquivamento dos atos constitutivos	17/01/2024
Data de arquivamento do ato de conversão de sociedade simples em sociedade empresária	
Data de encerramento do exercício social	31/12/2024
Quantidade total de linhas do arquivo digital	10547

TERMO DE ENCERRAMENTO

Nome Empresarial	CAM TECNOLOGIA LTDA
Natureza do Livro	LIVRO DIARIO
Número de ordem	14
Quantidade total de linhas do arquivo digital	10547
Data de inicio	01/01/2024
Data de término	31/12/2024

Este documento é parte integrante de escrituração cuja autenticação se comprova pelo recibo de número 8B.2C.B3.62.54.CC.C6.61.66.12.5A.5C.50.DC.CC.12.6C.7E.DF.39-2, nos termos do Decreto nº 9.555/2018.

Este relatório foi gerado pelo Sistema Público de Escrituração Digital – Sped

BALANÇO PATRIMONIAL

Entidade:	CAM TECNOLOGIA LTDA
Período da Escrituração:	01/01/2024 a 31/12/2024
CNPJ:	14.438.757/0001-76
Número de Ordem do Livro:	14
Período Selecionado:	01 de janeiro de 2024 a 31 de dezembro de 2024

Descrição	Nota	Saldo Inicial	Saldo Final
ATIVO		R$ 1.477.392,66	R$ 2.045.859,19
ATIVO CIRCULANTE		R$ 1.477.392,66	R$ 2.045.859,19
DISPONÍVEL		R$ 893.307,15	R$ 615.813,21
CAIXA		R$ 22.140,41	R$ 0,00
CAIXA GERAL		R$ 22.140,41	R$ 0,00
BANCOS CONTA MOVIMENTO		R$ 679.843,39	R$ 357.442,21
BANCO DO BRASIL		R$ 2.000,00	R$ 0,00
CAIXA ECONÔMICA FEDERAL		R$ 352.168,32	R$ 352.168,32
ITAU		R$ 192.605,36	R$ 1,00
BANCO BRADESCO		R$ 1.478,51	R$ 4.350,00
BANCO CONTA AZUL		R$ 96.199,11	R$ 0,00
BANCO NUBANK		R$ 35.392,09	R$ 922,89
APLICAÇÕES FINANCEIRAS LIQUIDEZ IMEDIATA		R$ 191.323,35	R$ 258.371,00
APLICAÇÃO FINANCEIRA		R$ 10.098,45	R$ 0,00
APLICAÇÃO FINANCEIRA BB		R$ 0,00	R$ 117.885,40
APLICAÇÃO FINANCEIRA ITAÚ		R$ 181.082,95	R$ 140.485,63
APLICAÇÃO FINANCEIRA BRADESCO		R$ 141,95	R$ (0,03)
CLIENTES		R$ 53.018,15	R$ 184.932,28
DUPLICATAS A RECEBER		R$ 53.018,15	R$ 184.932,28
CLIENTES DIVERSOS		R$ 53.018,15	R$ 184.932,28
OUTROS CRÉDITOS		R$ 127.037,36	R$ 807.727,92
ADIANTAMENTOS A FORNECEDORES		R$ 0,00	R$ 241.150,64
ADIANTAMENTO A FORNECEDOR		R$ 0,00	R$ 241.150,64
EMPRÉSTIMO A TERCEIROS		R$ 127.037,36	R$ 566.577,28
EMPRÉSTIMO A TERCEIROS		R$ 127.037,36	R$ 566.577,28
ESTOQUE		R$ 404.030,00	R$ 444.574,32
MERCADORIAS, PRODUTOS E INSUMOS		R$ 404.030,00	R$ 444.574,32
MERCADORIAS PARA REVENDA		R$ 404.030,00	R$ 444.574,32
ANTECIPAÇÃO DE LUCROS		R$ 0,00	R$ 0,00
ANTECIPAÇÃO DE LUCROS		R$ 0,00	R$ 0,00
ANTECIPAÇÃO DE DISTRIBUIÇÃO DE LUCROS		R$ 0,00	R$ 0,00
CONTA TRANSITÓRIA		R$ 0,00	R$ (7.188,54)
CONTA TRANSITÓRIA		R$ 0,00	R$ (7.188,54)
CONTA TRANSITÓRIA BANCÁRIA		R$ 0,00	R$ (7.188,54)
ATIVO NÃO-CIRCULANTE		R$ 0,00	R$ 0,00
IMOBILIZADO		R$ 0,00	R$ 0,00
MÓVEIS E UTENSÍLIOS		R$ 9.930,00	R$ 9.930,00
MÓVEIS E UTENSÍLIOS		R$ 9.930,00	R$ 9.930,00
MÁQUINAS, EQUIPAMENTOS E FERRAMENTAS		R$ 77.548,50	R$ 77.548,50
MÁQUINAS E EQUIPAMENTOS		R$ 77.548,50	R$ 77.548,50
(-) (-) DEPRECIAÇÕES, AMORT. E EXAUS. ACUMUL		R$ (87.478,50)	R$ (87.478,50)
(-) (-) DEPRECIAÇÕES DE MÓVEIS E UTENSÍLIOS		R$ (9.930,00)	R$ (9.930,00)
(-) (-) DEPRECIAÇÕES DE MÁQUINAS, EQUIP. FER		R$ (77.548,50)	R$ (77.548,50)
PASSIVO		R$ 1.477.392,66	R$ 2.045.859,19
PASSIVO CIRCULANTE		R$ 1.201.829,17	R$ 1.029.458,43
EMPRÉSTIMOS E FINANCIAMENTOS		R$ 479.959,62	R$ 439.534,15
EMPRÉSTIMOS		R$ 479.959,62	R$ 439.534,15
EMPRÉSTIMO		R$ 479.959,62	R$ 439.534,15
FORNECEDORES		R$ 47.222,69	R$ 122.983,28
FORNECEDORES		R$ 47.222,69	R$ 122.983,28
FORNECEDOR NACIONAL		R$ 47.222,69	R$ 122.983,28
OBRIGAÇÕES TRIBUTÁRIAS		R$ 634.390,64	R$ 421.708,87
IMPOSTOS E CONTRIBUIÇÕES A RECOLHER		R$ 634.390,64	R$ 421.708,87
IMPOSTOS E CONTRIBUIÇÕES		R$ 118.624,71	R$ 272.641,95
ICMS A RECOLHER		R$ 56.534,52	R$ 0,00
ISS A RECOLHER		R$ 20.020,32	R$ 0,00
IRRF A RECOLHER		R$ 3.038,70	R$ 2.908,64
PARCELAMENTO ICMS		R$ 0,00	R$ 60.959,54
PARCELAMENTO ISS		R$ 0,00	R$ 18.619,90
PARCELAMENTO SIMPLES NACIONAL		R$ 436.172,39	R$ 66.578,84
OBRIGAÇÕES TRABALHISTA E PREVIDENCIÁRIA		R$ 32.255,73	R$ 20.032,13
OBRIGAÇÕES COM O PESSOAL		R$ 22.074,59	R$ 12.154,13
SALÁRIOS E ORDENADOS A PAGAR		R$ 22.074,59	R$ 12.154,13
FÉRIAS A PAGAR		R$ 0,00	R$ 0,00
RESCISÕES A PAGAR		R$ 0,00	R$ 0,00
13º SALÁRIO A PAGAR		R$ 0,00	R$ 0,00
PENSÃO ALIMENTICIA		R$ 0,00	R$ 0,00
OBRIGAÇÕES SOCIAIS		R$ 10.181,14	R$ 7.878,00
INSS A RECOLHER		R$ 4.890,78	R$ 4.500,44
FGTS A RECOLHER		R$ 5.290,36	R$ 3.377,56
OUTRAS OBRIGAÇÕES		R$ 8.000,00	R$ 25.200,00
CONTAS A PAGAR		R$ 8.000,00	R$ 25.200,00
HONORÁRIOS CONTÁBEIS A PAGAR		R$ 8.000,00	R$ 25.200,00
PENSÃO ALIMENTICIA A DEPOSITAR		R$ 0,00	R$ 0,00
DIVIDENDOS, PART. E JURO SOBRE O CAPITAL		R$ 0,49	R$ 0,00
DIVIDENDOS		R$ 0,49	R$ 0,00
DIVIDENDOS A PAGAR		R$ 0,49	R$ 0,00
PATRIMÔNIO LÍQUIDO		R$ 275.563,49	R$ 1.016.400,76
CAPITAL SOCIAL		R$ 100.000,00	R$ 100.000,00
CAPITAL SUBSCRITO		R$ 100.000,00	R$ 100.000,00
CAPITAL SOCIAL		R$ 100.000,00	R$ 100.000,00
LUCROS OU PREJUÍZOS ACUMULADOS		R$ 175.563,49	R$ 916.400,76
LUCROS OU PREJUÍZOS ACUMULADOS		R$ 175.563,49	R$ 916.400,76
LUCROS ACUMULADOS		R$ 175.563,49	R$ 2.628.633,44
LUCRO DO PERIODO		R$ 0,00	R$ (1.712.232,68)

DEMONSTRAÇÃO DE RESULTADO DO EXERCÍCIO

Entidade:	CAM TECNOLOGIA LTDA		
Período da Escrituração:	01/01/2024 a 31/12/2024	CNPJ:	14.438.757/0001-76
Número de Ordem do Livro:	14		
Período Selecionado:	01 de janeiro de 2024 a 31 de dezembro de 2024		

Descrição	Nota	Saldo anterior	Saldo atual
RECEITA BRUTA		R$ 2.459.926,22	R$ 2.990.172,10
VENDA DE MERCADORIAS		R$ 0,00	R$ 933.816,17
SERVIÇOS PRESTADOS		R$ 0,00	R$ 2.056.355,93
(-) DEDUÇÕES		R$ (428.832,67)	R$ (397.479,73)
(-) (-) DEVOLUÇÃO DE VENDA DE MERCADORIAS		R$ (0,00)	R$ (88.499,99)
(-) (-) SIMPLES NACIONAL		R$ (0,00)	R$ (308.979,74)
RECEITA LÍQUIDA		R$ 2.031.093,55	R$ 2.592.692,37
LUCRO BRUTO		R$ 1.886.243,49	R$ 2.592.692,37
(-) DESPESAS OPERACIONAIS		R$ (1.392.643,37)	R$ (1.398.540,12)
(-) DESPESAS COM VENDAS		R$ (0,00)	R$ (668.004,40)
(-) SALÁRIOS E ORDENADOS		R$ (0,00)	R$ (415.211,73)
(-) 13º SALÁRIO		R$ (0,00)	R$ (31.759,16)
(-) FGTS		R$ (0,00)	R$ (37.752,81)
(-) ASSISTÊNCIA MÉDICA E SOCIAL		R$ (0,00)	R$ (104.970,67)
(-) COMISSÕES		R$ (0,00)	R$ (8.500,00)
(-) AMOSTRAS GRÁTIS		R$ (0,00)	R$ (13.478,31)
(-) PUBLICIDADE - LOCACAO DE EQUIPAMENTO		R$ (0,00)	R$ (918,90)
(-) FRETES E CARRETOS		R$ (0,00)	R$ (17.708,62)
(-) VIAGENS TERRESTRES		R$ (0,00)	R$ (30.599,71)
(-) TELEFONE		R$ (0,00)	R$ (6.663,56)
(-) DESPESAS POSTAIS E TELEGRÁFICAS		R$ (0,00)	R$ (100,18)
(-) COMBUSTÍVEL		R$ (0,00)	R$ (60,00)
(-) BONIFICAÇÕES ENVIADAS		R$ (0,00)	R$ (280,75)
(-) DESPESAS ADMINISTRATIVAS		R$ (1.392.643,37)	R$ (730.535,72)
(-) PLANO DE SAÚDE EMPREGADOS		R$ (0,00)	R$ (11.541,88)
(-) PATROCÍNIO		R$ (0,00)	R$ (55.000,00)
(-) SALÁRIOS E ORDENADOS		R$ (0,00)	R$ (39.050,14)
(-) 13º SALÁRIO		R$ (0,00)	R$ (39.029,97)
(-) FÉRIAS		R$ (0,00)	R$ (51.353,20)
(-) INSS		R$ (0,00)	R$ (44.571,28)
(-) FGTS		R$ (0,00)	R$ (3.690,15)
(-) INDENIZAÇÕES E AVISO PRÉVIO		R$ (0,00)	R$ (15.925,04)
(-) VALE TRANSPORTE		R$ (0,00)	R$ (6.018,17)
(-) ALUGUÉIS DE IMÓVEIS		R$ (0,00)	R$ (38.311,71)
(-) IPTU		R$ (0,00)	R$ (309,80)
(-) TAXAS DIVERSAS		R$ (0,00)	R$ (6.870,46)
(-) ENERGIA ELÉTRICA		R$ (0,00)	R$ (10.392,37)
(-) ÁGUA E ESGOTO		R$ (0,00)	R$ (414,89)
(-) TELEFONE		R$ (0,00)	R$ (49.933,82)
(-) SEGUROS		R$ (0,00)	R$ (2.508,90)
(-) MATERIAL DE HIGIENE E LIMPEZA		R$ (0,00)	R$ (28,05)
(-) ASSISTÊNCIA CONTÁBIL		R$ (0,00)	R$ (39.199,98)
(-) SERVIÇOS PRESTADOS POR TERCEIROS		R$ (0,00)	R$ (179.274,06)
(-) DEPRECIAÇÕES E AMORTIZAÇÕES		R$ (0,00)	R$ (363,80)
(-) DESPESAS LEGAIS E JUDICIAIS		R$ (0,00)	R$ (12.980,06)
(-) ALIMENTAÇÃO		R$ (0,00)	R$ (864,60)
(-) CONDOMINIO E TAXAS		R$ (0,00)	R$ (28.167,63)
(-) SOFTWARE		R$ (0,00)	R$ (60.708,80)
(-) JUROS PASSIVOS		R$ (0,00)	R$ (24.914,39)
(-) TARIFA BANCARIA		R$ (0,00)	R$ (5.522,84)
(-) PROVISÕES P/ PERDAS E A JUSTES DE ATIVOS		R$ (0,00)	R$ (3.589,73)
OUTRAS RECEITAS OPERACIONAIS		R$ 0,00	R$ 1.169,40
BONIFICAÇÕES RECEBIDAS		R$ 0,00	R$ 1.169,40
RESULTADO OPERACIONAL		R$ 321.470,14	R$ 1.195.321,65
(-) DESPESAS NÃO OPERACIONAIS		R$ (210.059,05)	R$ (316.014,09)
(-) OUTRAS DESPESAS NÃO OPERACIONAIS		R$ (0,00)	R$ (316.014,09)
RESULTADO ANTES DO IR E CSLL		R$ 111.411,09	R$ 879.307,56
LUCRO LÍQUIDO DO EXERCÍCIO		R$ 111.411,09	R$ 879.307,56

MINISTÉRIO DA FAZENDA
SECRETARIA DA RECEITA FEDERAL DO BRASIL
SISTEMA PÚBLICO DE ESCRITURAÇÃO DIGITAL – Sped Versão: 10.3.3

RECIBO DE ENTREGA DE ESCRITURAÇÃO CONTÁBIL DIGITAL

IDENTIFICAÇÃO DO TITULAR DA ESCRITURAÇÃO

NIRE	CNPJ	
	14.438.757/0001-76	

NOME EMPRESARIAL
CAM TECNOLOGIA LTDA

IDENTIFICAÇÃO DA ESCRITURAÇÃO

FORMA DA ESCRITURAÇÃO CONTÁBIL	PERÍODO DA ESCRITURAÇÃO
Livro Diário (Completo - sem escrituração Auxiliar)	01/01/2024 a 31/12/2024
NATUREZA DO LIVRO	**NÚMERO DO LIVRO**
LIVRO DIARIO	14

IDENTIFICAÇÃO DO ARQUIVO (HASH)
8B.2C.B3.62.54.CC.C6.61.66.12.5A.5C.50.DC.CC.12.6C.7E.DF.39

ARQUIVOS SUBSTITUÍDOS (HASH)

ESTE LIVRO FOI ASSINADO COM OS SEGUINTES CERTIFICADOS DIGITAIS:

QUALIFICAÇÃO DO SIGNATARIO	CPF/CNPJ	NOME	Nº SÉRIE DO CERTIFICADO	VALIDADE	RESPONSÁVEL LEGAL
Contador	11364632756	JOAO PAULO DE AZEVEDO ROSA:11364632756	892826394669204097 43392	28/05/2025 a 28/05/2026	Não
Pessoa Jurídica (e-CNPJ ou e-PJ)	14438757000176	CAM TECNOLOGIA LTDA:14438757000176	128750722980866436 6	07/01/2025 a 07/01/2026	Sim

NÚMERO DO RECIBO:

8B.2C.B3.62.54.CC.C6.61.66.12.5A.5C.
50.DC.CC.12.6C.7E.DF.39-2

Escrituração recebida via Internet
pelo Agente Receptor SERPRO

em 20/06/2025 às 18:54:41

25.3B.14.35.2C.47.66.DC
23.B8.37.A1.6D.C7.71.42

Considera-se autenticado o livro contábil a que se refere este recibo nos termos do Decreto nº 9.555/2018, dispensando-se qualquer outra forma de autenticação. Este recibo comprova a autenticação.

TERMOS DE ABERTURA E ENCERRAMENTO

Entidade:	CAM TECNOLOGIA LTDA		
Período da Escrituração:	01/01/2023 a 31/12/2023	CNPJ:	14.438.757/0001-76
Número de Ordem do Livro:	13		

TERMO DE ABERTURA

Nome Empresarial	CAM TECNOLOGIA LTDA
NIRE	33600407362
CNPJ	14.438.757/0001-76
Número de Ordem	13
Natureza do Livro	LIVRO DIARIO
Município	RIO DE JANEIRO
Data do arquivamento dos atos constitutivos	26/10/2016
Data de arquivamento do ato de conversão de sociedade simples em sociedade empresária	
Data de encerramento do exercício social	31/12/2023
Quantidade total de linhas do arquivo digital	9995

TERMO DE ENCERRAMENTO

Nome Empresarial	CAM TECNOLOGIA LTDA
Natureza do Livro	LIVRO DIARIO
Número de ordem	13
Quantidade total de linhas do arquivo digital	9995
Data de inicio	01/01/2023
Data de término	31/12/2023

BALANÇO PATRIMONIAL

Entidade:	CAM TECNOLOGIA LTDA		
Período da Escrituração:	01/01/2023 a 31/12/2023	CNPJ:	14.438.757/0001-76
Número de Ordem do Livro:	13		
Período Selecionado:	01 de Janeiro de 2023 a 31 de Dezembro de 2023		

Descrição	Nota	Saldo Inicial	Saldo Final
ATIVO		R$ 1.740.407,72	R$ 1.477.392,17
CIRCULANTE		R$ 1.740.407,72	R$ 1.477.392,17
DISPONIVEL		R$ 454.451,66	R$ 893.306,66
CAIXA		R$ 235.998,11	R$ 22.140,41
Caixa		R$ 235.998,11	R$ 22.140,41
BANCO CONTA MOVIMENTO		R$ 218.453,55	R$ 679.843,39
Banco do Brasil		R$ 0,00	R$ 2.000,00
Banco Itau		R$ 233.752,24	R$ 192.605,36
Banco Bradesco		R$ 67,15	R$ 1.478,51
(-) Caixa Economica Federal		R$ (15.956,62)	R$ 352.168,32
Receba Facil Boletos		R$ 0,00	R$ 96.199,11
Nubank		R$ 590,78	R$ 35.392,09
APLICACOES FINANCEIRAS - M. FIXO		R$ 0,00	R$ 191.322,86
Aplicacao Banco do Brasil		R$ 0,00	R$ 0,00
Aplicacao Banco Itau		R$ 0,00	R$ 181.082,46
Aplicacao Banco Bradesco		R$ 0,00	R$ 141,95
Outras Aplicacoes Financeiras		R$ 0,00	R$ 10.098,45
CONTAS A RECEBER - CLIENTES		R$ 247.083,22	R$ 53.018,15
CONTAS A RECEBER - CLIENTES		R$ 247.083,22	R$ 53.018,15
Contas a Receber Clientes		R$ 247.083,22	R$ 53.018,15
OUTRAS CONTAS A RECEBER		R$ 598.277,57	R$ 127.037,36
OUTRAS CONTAS A RECEBER		R$ 598.277,57	R$ 127.037,36
Mutuo - Partes Relacionadas		R$ 307.813,89	R$ 0,00
Mutuo - Partes Não Relacionadas		R$ 290.463,68	R$ 127.037,36
ESTOQUES		R$ 440.595,27	R$ 404.030,00
ESTOQUES DE MERCADORIAS		R$ 440.595,27	R$ 404.030,00
Mercadorias Para Revenda		R$ 440.595,27	R$ 404.030,00
IMPOSTOS A RECUPERAR OU COMPENSAR		R$ 0,00	R$ 0,00
IMPOSTOS A RECUPERAR OU COMPENSAR		R$ 0,00	R$ 0,00
INSS a Recuperar		R$ 0,00	R$ 0,00
IMOBILIZADO		R$ 0,00	R$ 0,00
ATIVO FIXO - AQUISICAO		R$ 87.478,50	R$ 87.478,50
Moveis e Utensilios		R$ 9.930,00	R$ 9.930,00
Equipamentos Informatica		R$ 77.548,50	R$ 77.548,50
(-) ATIVO FIXO - DEPRECIACAO		R$ (87.478,50)	R$ (87.478,50)
(-) Depreciacao Moveis e Utensilios		R$ (9.930,00)	R$ (9.930,00)
(-) Depreciacao Equipamentos de Informatica		R$ (77.548,50)	R$ (77.548,50)
PASSIVO		R$ 1.740.407,72	R$ 1.477.392,17
CIRCULANTE		R$ 938.065,15	R$ 1.201.828,68
FORNECEDORES		R$ 78.966,37	R$ 55.222,69
FORNECEDORES		R$ 78.966,37	R$ 55.222,69
Fornecedores		R$ 78.966,37	R$ 47.222,69
Honorários a Pagar		R$ 0,00	R$ 8.000,00
EMPRESTIMOS E FINANCIAMENTOS		R$ 462.639,95	R$ 479.959,62
EMPRESTIMOS		R$ 462.639,95	R$ 479.959,62
Emprestimo Banco Itau		R$ 6.824,49	R$ 73.526,64
Emprestimo Banco Bradesco		R$ 70.447,76	R$ 36.614,22
Emprestimo Caixa Economica Federal		R$ 385.367,70	R$ 369.818,76
IMPOSTOS E CONTRIBUICOES A RECOLHER		R$ 363.153,24	R$ 634.390,64
IMPOSTOS E CONTRIBUICOES A RECOLHER		R$ 0,00	R$ 195.179,55
ICMS a Recolher		R$ 0,00	R$ 56.534,52
ISS a Recolher		R$ 0,00	R$ 20.020,32
Simples Nacional - DAS a Recolher		R$ 0,00	R$ 118.624,71
IMPOSTOS E CONTRIBUICOES RETIDOS		R$ 2.202,52	R$ 3.038,70
IR Retido - Folha de Pagamento		R$ 2.202,52	R$ 3.038,70
PARCELAMENTOS		R$ 360.950,72	R$ 436.172,39
Parcelamento Impostos Federais		R$ 360.950,72	R$ 436.172,39
SALARIOS, PROVENTOS E ENCARGOS		R$ 33.305,59	R$ 32.255,73
SALARIOS E PROVENTOS		R$ 26.441,68	R$ 22.074,59
Salarios e Remuneraçoes a Pagar		R$ 26.175,40	R$ 22.074,59
Pensão Alimentícia a Pagar		R$ 266,28	R$ 0,00
ENCARGOS SOCIAIS		R$ 6.863,91	R$ 10.181,14
INSS - Folha de Pagamento		R$ 4.550,02	R$ 4.890,78
FGTS a Recolher		R$ 2.313,89	R$ 5.290,36
PATRIMONIO LIQUIDO		R$ 802.342,57	R$ 275.563,49
CAPITAL SOCIAL		R$ 802.342,57	R$ 275.563,49
CAPITAL SOCIAL REALIZADO RESIDENTE NO PAÍS		R$ 100.000,00	R$ 100.000,00
Capital Subscrito De Residente No País		R$ 100.000,00	R$ 100.000,00
LUCROS/PREJUIZOS ACUMULADOS		R$ 702.342,57	R$ 175.563,49
Lucros Acumulados		R$ 702.342,57	R$ 175.563,49

DEMONSTRAÇÃO DE RESULTADO DO EXERCÍCIO

Entidade:	CAM TECNOLOGIA LTDA
Período da Escrituração:	01/01/2023 a 31/12/2023
CNPJ:	14.438.757/0001-76
Número de Ordem do Livro:	13
Período Selecionado:	01 de Janeiro de 2023 a 31 de Dezembro de 2023

Descrição	Nota	Saldo anterior	Saldo atual
RECEITA BRUTA		R$ 3.806.460,71	R$ 2.459.926,22
Receita Revenda de Produtos		R$ 1.697.225,00	R$ 519.034,97
Receita de Prestacao de Servicos		R$ 2.022.736,09	R$ 1.789.907,27
Receita de Locacao		R$ 86.499,62	R$ 150.983,98
(-) DEDUÇÕES		R$ (489.069,27)	R$ (428.832,67)
(-) ICMS		R$ (0,00)	R$ (67.438,18)
(-) ISS		R$ (0,00)	R$ (89.494,25)
(-) Simples Nacional - DAS		R$ (489.069,27)	R$ (271.900,24)
RECEITA LÍQUIDA		R$ 3.317.391,44	R$ 2.031.093,55
(-) CMV		R$ (776.306,79)	R$ (144.850,06)
(-) Custo Revenda de Produtos		R$ (776.306,79)	R$ (144.850,06)
LUCRO BRUTO		R$ 2.541.084,65	R$ 1.886.243,49
(-) DESPESAS OPERACIONAIS		R$ (1.495.830,00)	R$ (1.392.643,37)
(-) DESPESAS ADMINISTRATIVAS		R$ (1.495.830,00)	R$ (1.392.643,37)
(-) Despesas Propaganda e Publicidade		R$ (13.200,00)	R$ (7.200,00)
(-) Frete sobre Venda e Devolucao		R$ (6.188,06)	R$ (16.479,93)
(-) Salarios e Remuneracoes		R$ (432.978,32)	R$ (408.468,64)
(-) Horas Extras		R$ (3.281,75)	R$ (4.224,70)
(-) Ferias		R$ (67.529,10)	R$ (68.313,41)
(-) Decimo Terceiro Salario		R$ (41.978,45)	R$ (40.669,90)
(-) Verbas Rescisorias		R$ 2.869,09	R$ (83,33)
(-) Ajuda De Custo		R$ (0,00)	R$ (35.607,43)
(-) INSS		R$ (764,22)	R$ (0,00)
(-) FGTS		R$ (41.774,48)	R$ (40.439,80)
(-) Vale Transporte		R$ (7.379,21)	R$ (2.254,81)
(-) Auxilio Alimentacao/Refeição		R$ (124.359,15)	R$ (96.050,11)
(-) Assistencia Medica e Odontologica		R$ (86.469,25)	R$ (93.046,72)
Tiquete Combustivel		R$ 0,00	R$ 222,00
(-) Provisao de Ferias - Principal		R$ 82.684,23	R$ (0,00)
(-) Provisao de Ferias - FGTS		R$ 5.887,59	R$ (0,00)
(-) Provisao Decimo Terceiro Salario - Principal		R$ 38.672,57	R$ (0,00)
(-) Provisao Decimo Terceiro Salario - FGTS		R$ 3.093,78	R$ (0,00)
(-) Estagiarios e Temporarios		R$ (10.500,00)	R$ (7.500,00)
(-) Aluguel de Imoveis		R$ (76.909,36)	R$ (0,00)
(-) Energia Elétrica		R$ (17.119,91)	R$ (15.466,16)
(-) Telefone e Internet		R$ (29.159,25)	R$ (36.403,83)
(-) Correios e Malote		R$ (0,00)	R$ (5.030,96)
(-) Seguros		R$ (1.884,19)	R$ (1.636,89)
(-) Viagens e Estadias		R$ (62.165,03)	R$ (44.154,60)
(-) Combustivel		R$ (0,00)	R$ (53.574,00)
(-) Lanches e Refeicoes		R$ (19.706,98)	R$ (5.795,33)
(-) Servicos prestados PJ		R$ (51.143,02)	R$ (88.550,12)
(-) IPTU e Outras Taxas Prediais		R$ (1.257,30)	R$ (1.582,49)
(-) Outros Tributos e Contribuicoes		R$ (449,04)	R$ (0,00)
(-) Multas Compensatorias		R$ (12.379,29)	R$ (4.852,02)
(-) Outras Despesas		R$ (520.461,90)	R$ (315.480,19)
RECEITAS FINANCEIRAS		R$ 79,15	R$ 26,75
Receitas em Operações de Renda Fixa		R$ 79,15	R$ 26,75
(-) OUTRAS DESPESAS OPERACIONAIS		R$ (158.257,98)	R$ (172.156,73)
(-) Juros e Despesa Bancarias		R$ (158.257,98)	R$ (172.156,73)
RESULTADO OPERACIONAL		R$ 887.075,82	R$ 321.470,14
(-) DESPESAS NÃO OPERACIONAIS		R$ (0,00)	R$ (210.059,05)
(-) Outras Despesas Financeiras		R$ (0,00)	R$ (210.059,05)
RESULTADO ANTES DO IR E CSLL		R$ 887.075,82	R$ 111.411,09
LUCRO LÍQUIDO DO EXERCÍCIO		R$ 887.075,82	R$ 111.411,09

MINISTÉRIO DA FAZENDA
SECRETARIA DA RECEITA FEDERAL DO BRASIL
SISTEMA PÚBLICO DE ESCRITURAÇÃO DIGITAL – Sped Versão: 10.2.0

RECIBO DE ENTREGA DE ESCRITURAÇÃO CONTÁBIL DIGITAL

IDENTIFICAÇÃO DO TITULAR DA ESCRITURAÇÃO

NIRE	CNPJ	
33600407362	14.438.757/0001-76	

NOME EMPRESARIAL
CAM TECNOLOGIA LTDA

IDENTIFICAÇÃO DA ESCRITURAÇÃO

FORMA DA ESCRITURAÇÃO CONTÁBIL	PERÍODO DA ESCRITURAÇÃO
Livro Diário (Completo - sem escrituração Auxiliar)	01/01/2023 a 31/12/2023
NATUREZA DO LIVRO	**NÚMERO DO LIVRO**
LIVRO DIARIO	13

IDENTIFICAÇÃO DO ARQUIVO (HASH)
BE.78.50.46.59.B6.FA.25.D2.81.64.EB.D0.A4.35.07.7A.AC.31.E8

ESTE LIVRO FOI ASSINADO COM OS SEGUINTES CERTIFICADOS DIGITAIS:

QUALIFICAÇÃO DO SIGNATARIO	CPF/CNPJ	NOME	Nº SÉRIE DO CERTIFICADO	VALIDADE	RESPONSÁVEL LEGAL
Contabilista	18435718700	CARLOS ALBERTO DOMINGUES DA SILVA:18435718700	470412440787971348 3	27/04/2023 a 27/04/2026	Não
Pessoa Jurídica (e-CNPJ ou e-PJ)	28005155000130	UNICON CONSULTORIA FINANCEIRA LTDA:28005155000130	794763759161380967 3	14/12/2023 a 13/12/2024	Sim

NÚMERO DO RECIBO:

BE.78.50.46.59.B6.FA.25.D2.81.64.EB.
D0.A4.35.07.7A.AC.31.E8-7

Escrituração recebida via Internet
pelo Agente Receptor SERPRO

em 28/05/2024 às 12:46:59

C9.E6.9F.19.69.41.B8.A1
23.AF.3A.15.32.31.03.16

Considera-se autenticado o livro contábil a que se refere este recibo, dispensando-se a autenticação de que trata o art. 39 da Lei nº 8.934/1994. Este recibo comprova a autenticação.

BASE LEGAL: Decreto nº 1.800/1996, com a alteração do Decreto nº 8.683/2016, e arts. 39, 39-A, 39-B da Lei nº 8.934/1994 com a alteração da Lei Complementar nº 1247/2014.

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO - DPRJ

Referência: PREGÃO ELETRÔNICO - PE 90009/2025

DECLARAÇÃO DE CONTRATOS FIRMADOS

COM A INICIATIVA PRIVADA E A ADMINISTRAÇÃO PÚBLICA

Eu, Thiago Maluf Resende, CPF nº 103068457-09, representante legal da empresa CAM Tecnologia Ltda, com sede na Av. Pastor Martin Luther King Jr, nº 126 Nova América Offices, Torre 2000, Sala 408, Bairro Del Castilho, CEP: 20.765-000, Cidade do Rio de Janeiro, RJ, inscrita no CNPJ sob o nº 14.438.757/0001-76, DECLARO, sob as penas da Lei, os seguintes contratos firmados com a iniciativa privada e a Administração Pública:

NOME	ENDEREÇO / TELEFONE	VIGÊNCIA DO CONTRATO	VALOR MENSAL DO CONTRATO (R$)	VALOR ANUAL DO CONTRATO (R$)	VALOR TOTAL DO CONTRATO (R$)
POLICIA FEDERAL CONTRATO 09/2025	Setor Policial Sul, Brasília/DF. (61) 99276-8173	26/06/2028	0,00	605.645,42	605.645,42
PREFEITURA BOTUCATU/SP CONTRATO 278/2025	Centro, Botucatu/SP (14) 99722-0293	04/09/2030	6.888,20	82.658,40	415.292,00
PREFEITURA CURVELO/MG CONTRATO 19/2025	Centro, Curvelo/MG (38) 99958-5418	18/03/2030	6.034,00	72.408,00	362.040,00

PRODAM/SP Contrato 18.07/2025	Rua Libero Padaró, Centro, São Paulo/SP (11) 98268-3034	04/08/2026	22.075,00	264.900,00	264.900,00
RNP - Rede Nacional de Ensino e Pesquisa Contrato ADC 10571	Rua Lauro Muller, Botafogo, Rio de Janeiro/RJ.	09/01/2027	24.493,90	264.900,00	264.900,00
Prefeitura São Vicente/SP Contrato 22/2025	Centro, São Vicente/SP	19/05/2026	19.531,00	234.372,00	234.372,00
Prefeitura Volta Redonda/RJ Contrato 240/2023	Centro, Volta Redonda/RJ	02/08/2027	8.782,50	105.390,00	105.390,00
SR/AP – Polícia Federal do Amapá Contrato 25/2025	Macapá/AP	39/09/2030	2.291,66	27.499,92	137.499,60
EMBRAPA Pantanal/MS Contrato 2260023/00399	Corumbá/MS	31/05/2026	3.000,00	36.000,00	99.000,00

SAS Barbacena Contrato 058/SAS/2025	Barbacena/MG	27/11/2029	1.612,50	19.350,00	96.750,00
EMBRAPA SEDE Contrato 3500624/00010	Brasília/DF	28/10/2026	7.989,94	95.879,28	95.879,28
CRM/MG Contrato 25/2025	Belo Horizonte/MG	05/05/2025	5.824,75	69.897,00	69.897,00

1. FÓRMULA DO PATRIMÔNIO LÍQUIDO (item 9.13.1.11)

Fórmula de cálculo:

- Patrimônio Líquido: R$ 1.016.400,76
- Multiplicado por 12: R$ 1.016.400,76 × 12 = R$ 12.196.809,12
- Soma total dos Contratos: R$ 2.751.565,30
- Resultado: R$ 12.196.809,12 > R$ 2.751.565,30

2. FÓRMULA DA RECEITA BRUTA (item 9.13.1.13)

- Receita Bruta (DRE 2024): R$ 2.990.172,10
- Cálculo: (2.990.172,10 - 2.751.565,30) x 100 / 2.990.172,10
- Cálculo = 7,98%

Rio de Janeiro, 12 de dezembro de 2025.

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2025.12.12 10:31:57 -03'00'

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO - DPRJ

Referência: PREGÃO ELETRÔNICO - PE 90009/2025

DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA

Eu Thiago Maluf Resende, CPF nº 103068457-09, representante legal da empresa CAM Tecnologia Ltda., com sede na Av. Pastor Martin Luther King Jr, nº 126 Nova América Offices, Torre 2000, Sala 408, Bairro Del Castilho, CEP: 20.765-000, Cidade do Rio de Janeiro, RJ, inscrita no CNPJ sob o nº 14.438.757/0001-76, doravante denominado LICITANTE, para fins do disposto no Edital do Pregão Eletrônico nº PE 90009/25, declara, sob as penas da lei, em especial o art. 299 do código Penal Brasileiro, que:

a) A proposta anexa foi elaborada de maneira independente, e que o conteúdo da proposta anexa não foi, no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de qualquer outro participante potencial ou de fato do presente certame, por qualquer meio ou por qualquer pessoa;

b) A intenção de apresentar a proposta anexa não foi informada a, discutida com ou recebida de qualquer outro participante potencial ou de fato do presente certame, por qualquer meio ou qualquer pessoa;

c) Que não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato do presente certame, quanto a participar ou não da referida licitação;

d) Que o conteúdo da proposta anexa não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro participante potencial ou de fato, antes da adjudicação do objeto da referida licitação;

e) Que o conteúdo da proposta anexa não foi no todo ou em parte, direta ou indiretamente, informado a, discutido com ou recebido de DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO antes da abertura oficial das propostas e;

f) Que está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

Rio de Janeiro, 12 de dezembro de 2025.

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2025.12.12 10:33:05 -03'00'

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO - DPRJ

Referência: PREGÃO ELETRÔNICO - PE 90009/2025

DECLARAÇÃO DE EMPRESA DE PEQUENO PORTE

Eu Thiago Maluf Resende, CPF nº 103068457-09, representante legal da empresa CAM Tecnologia Ltda., com sede na Av. Pastor Martin Luther King Jr, nº 126 Nova América Offices, Torre 2000, Sala 408, Bairro Del Castilho, CEP: 20.765-000, Cidade do Rio de Janeiro, RJ, inscrita no CNPJ sob o nº 14.438.757/0001-76, DECLARO, sob as penas da lei, para fins do disposto no Edital Pregão Eletrônico nº PE 90009/25, sob as sanções administrativas cabíveis e sob as penas da lei, que esta empresa, na presente data, é considerada:

( ) MICROEMPRESA, conforme Inciso I do artigo 3º da Lei Complementar nº 123, de 14/12/2006;

(X) EMPRESA DE PEQUENO PORTE, conforme Inciso II do artigo 3º da Lei Complementar nº 123, de 14/12/2006. Declara ainda que a empresa está excluída das vedações constantes do parágrafo 4º do artigo 3º da Lei Complementar nº 123, de 14 de dezembro de 2006.

Declaro também, no ano-calendário de realização da licitação, ainda não ter celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, na forma do artigo 4º, § 2º da Lei Nº 14.133/21.

Rio de Janeiro, 12 de dezembro de 2025.

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2025.12.12 10:32:43 -03'00'

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO - DPRJ

Referência: PREGÃO ELETRÔNICO - PE 90009/2025

DECLARAÇÃO DE CUMPRIMENTO DO DISPOSTO NA LEI 7.258/2016

Eu Thiago Maluf Resende, CPF nº 103068457-09, representante legal da empresa CAM Tecnologia Ltda., com sede na Av. Pastor Martin Luther King Jr, nº 126 Nova América Offices, Torre 2000, Sala 408, Bairro Del Castilho, CEP: 20.765-000, Cidade do Rio de Janeiro, RJ, inscrita no CNPJ sob o nº 14.438.757/0001-76, DECLARO, sob as penas da lei, que atendemos ao disposto da Lei 7.258/2016, apresentando um efetivo de 8 (oito) empregados.

Rio de Janeiro, 12 de dezembro de 2025.

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2025.12.12 10:32:19 -03'00'

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO - DPRJ

Referência: PREGÃO ELETRÔNICO - PE 90009/2025

Prezados,

A CAM Tecnologia LTDA., inscrita no CNPJ 14.438.757/0001-76, vem, respeitosamente, apresentar a devida comprovação da localização dos datacenters utilizados na prestação dos serviços contratados.

1. Infraestrutura de Nuvem no Brasil e Zonas de Disponibilidade

A CAM Tecnologia adota a infraestrutura da Huawei Cloud Brasil, garantindo que toda a prestação dos serviços de PABX em Nuvem ocorra em datacenters localizados exclusivamente no Brasil.

A Huawei Cloud segue um modelo de infraestrutura baseado em Zonas de Disponibilidade (Availability Zones – AZs), que são datacenters fisicamente distintos dentro de uma mesma região, cada um operando com seus próprios sistemas independentes de energia, conectividade e segurança. Esse modelo de arquitetura garante alta disponibilidade e resiliência, minimizando riscos de falha e interrupção do serviço.

No Brasil, a Huawei Cloud possui três (03) Zonas de Disponibilidade (AZs) no estado de São Paulo, distribuídas de forma estratégica para garantir redundância e continuidade operacional.

2. Baixo Tempo de Latência e Qualidade da Conectividade

Além da alta disponibilidade, a infraestrutura utilizada pela **CAM Tecnologia** proporciona tempo de latência extremamente baixo, essencial para a qualidade da telefonia IP e da comunicação em tempo real.

Teste prático: A latência pode ser validada através de testes de ping aos seguintes servidores da infraestrutura da CAM Tecnologia:

SBC (Session Border Controller) → sbc.cambox.cloud

Roteador de Telefonia → router.cambox.cloud

Os testes demonstram baixíssimos tempos de resposta, garantindo que as chamadas de voz e

os serviços de comunicação operem com alta qualidade, sem atrasos perceptíveis e sem degradação da experiência do usuário.

A Huawei Cloud oferece conectividade direta com os principais backbones de internet do Brasil, reduzindo significativamente o tempo de resposta e garantindo estabilidade e desempenho de nível empresarial.

3. Sigilo e Segurança da Infraestrutura

Por razões de segurança da informação e política global de proteção de infraestrutura crítica, a Huawei não divulga os endereços físicos exatos de seus datacenters, uma prática comum entre grandes provedores de nuvem, como Microsoft Azure, AWS e Google Cloud. No entanto, confirmamos que a infraestrutura utilizada está 100% localizada no Brasil, conforme pode ser verificado nos casos de sucesso de clientes no site oficial:

https://www.huaweicloud.com/intl/pt-br/cases.html

4. Atendimento a Clientes de Grande Porte

Os datacenters da Huawei Cloud Brasil atendem instituições renomadas, como o Banco Itaú, além de diversas organizações públicas e privadas. Essa robustez operacional reforça a confiabilidade, segurança e conformidade da infraestrutura utilizada pela CAM Tecnologia.

5. Certificações de Segurança e Conformidade

A infraestrutura da Huawei Cloud no Brasil possui certificações reconhecidas internacionalmente, garantindo altos padrões de segurança, disponibilidade e conformidade regulatória, incluindo:

ISO 27001 (Gestão de Segurança da Informação);

TIER III e TIER IV (Certificação de datacenters pela Uptime Institute);

Conformidade com a LGPD (Lei Geral de Proteção de Dados – Lei nº 13.709/2018).

Colocamo-nos à disposição para quaisquer esclarecimentos adicionais que se façam necessários.

Atenciosamente,

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2025.12.12 10:31:29 -03'00'

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO - DPRJ

Referência: PREGÃO ELETRÔNICO - PE 90009/2025

DECLARAÇÃO EM ATENDIMENTO AO § 1°, ART. 63 DA LEI FEDERAL 14.133/2021

Eu Thiago Maluf Resende, CPF nº 103068457-09, representante legal da empresa CAM Tecnologia Ltda., com sede na Av. Pastor Martin Luther King Jr, nº 126 Nova América Offices, Torre 2000, Sala 408, Bairro Del Castilho, CEP: 20.765-000, Cidade do Rio de Janeiro, RJ, inscrita no CNPJ sob o nº 14.438.757/0001-76, DECLARO, sob as penas da Lei, possui aptidão financeira para a execução do CONTRATO e que a sua PROPOSTA DE PREÇO compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, conforme § 1°, Art. 63 de Lei Federal 14.133/2021.

Declara ainda que está plenamente ciente do teor e da extensão desta Declaração, bem como detém plenos poderes e informações para firmá-la.

Rio de Janeiro, 12 de dezembro de 2025.

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2025.12.12 10:31:06 -03'00'

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO - DPRJ

Referência: PREGÃO ELETRÔNICO - PE 90009/2025

DECLARAÇÃO DE INEXISTÊNCIA DE PENALIDADE

Eu Thiago Maluf Resende, CPF nº 103068457-09, representante legal da empresa CAM Tecnologia Ltda., com sede na Av. Pastor Martin Luther King Jr, nº 126 Nova América Offices, Torre 2000, Sala 408, Bairro Del Castilho, CEP: 20.765-000, Cidade do Rio de Janeiro, RJ, inscrita no CNPJ sob o nº 14.438.757/0001-76, DECLARO, sob as penas da Lei, que não foram aplicadas penalidades de suspensão temporária da participação em licitação, impedimento de contratar ou declaração de inidoneidade para licitar e contratar por qualquer Ente ou Entidade da Administração Federal, Estadual, Distrital e Municipal cujos efeitos ainda vigorem.

Rio de Janeiro, 12 de dezembro de 2025.

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2025.12.12 10:33:47 -03'00'

DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO - DPRJ

Referência: PREGÃO ELETRÔNICO - PE 90009/2025

DECLARAÇÃO DE O DE CUMPRIMENTO DO DISPOSTO NO INCISO XXXIII DO ART. 7° DA CONSTITUIÇÃO FEDERAL

Eu Thiago Maluf Resende, CPF nº 103068457-09, representante legal da empresa CAM Tecnologia Ltda., com sede na Av. Pastor Martin Luther King Jr, nº 126 Nova América Offices, Torre 2000, Sala 408, Bairro Del Castilho, CEP: 20.765-000, Cidade do Rio de Janeiro, RJ, inscrita no CNPJ sob o nº 14.438.757/0001-76, DECLARO, sob as penas da lei, para os fins do disposto no Inciso VI do art. 68 da Lei 14.133/2021, que não empregamos menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não empregamos menos de 16 (dezesseis) anos.

Rio de Janeiro, 12 de dezembro de 2025.

THIAGO MALUF RESENDE:10306845709

Assinado de forma digital por THIAGO MALUF RESENDE:10306845709
Dados: 2025.12.12 10:33:26 -03'00'

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Declaração

Declaramos para os fins exigidos na legislação, conforme documentação registrada no SICAF, que a situação do fornecedor no momento é a seguinte:

Dados do Fornecedor

CNPJ:	**14.438.757/0001-76**	DUNS®:	**901065486**
Razão Social:	**CAM TECNOLOGIA LTDA**		
Nome Fantasia:	**CAM TECNOLOGIA REDES E SERVICOS**		
Situação do Fornecedor:	**Credenciado**	Data de Vencimento do Cadastro:	**01/12/2026**
Natureza Jurídica:	**SOCIEDADE EMPRESÁRIA LIMITADA**		
MEI:	**Não**		
Porte da Empresa:	**Micro Empresa**		

Ocorrências e Impedimentos

Ocorrência:	**Consta**
Impedimento de Licitar:	**Nada Consta**
Ocorrências Impeditivas indiretas:	**Nada Consta**
Vínculo com "Serviço Público":	**Nada Consta**

Níveis cadastrados:

Automática: a certidão foi obtida através de integração direta com o sistema emissor. Manual: a certidão foi inserida manualmente pelo fornecedor.

I - Credenciamento

II - Habilitação Juridica

III - Regularidade Fiscal e Trabalhista Federal

Receita Federal e PGFN		Validade:	**14/04/2026**	**Automática**
FGTS		Validade:	**01/01/2026**	**Automática**
Trabalhista	**(http://www.tst.jus.br/certidao)**	Validade:	**09/06/2026**	**Automática**

IV - Regularidade Fiscal Estadual/Distrital e Municipal

Receita Estadual/Distrital	Validade:	**26/01/2026**
Receita Municipal	Validade:	**01/01/2026**

VI - Qualificação Econômico-Financeira

	Validade:	**30/06/2026**

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Relatório de Ocorrências Ativas

Dados do Fornecedor

CNPJ:	**14.438.757/0001-76** DUNS®: **901065486**
Razão Social:	**CAM TECNOLOGIA LTDA**
Nome Fantasia:	**CAM TECNOLOGIA REDES E SERVICOS**
Situação do Fornecedor:	**Credenciado**

Ocorrência 1:

Tipo Ocorrência:	**Advertência - Lei nª 8666/93, art. 87, inc. I**
UASG Sancionadora:	**389320 - CONSELHO FEDERAL DE ENFERMAGEM**
Data Aplicação:	**05/09/2018**
Número do Processo:	**688/2016**
Descrição/Justificativa:	**O recurso da defesa prévia foi parcialmente procedente, a empresa foi desclassificada do Pregão Eletrônico nª 46/2016 por não manter a proposta, sendo assim, será penalizada com ADVERTÊNCIA, com base no Art. 87, inciso I da Lei 8.666/93.**

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Relatório de Ocorrências Ativas Impeditivas de Licitar

Dados do Fornecedor

CNPJ: **14.438.757/0001-76** DUNS®: **901065486**
Razão Social: **CAM TECNOLOGIA LTDA**
Nome Fantasia: **CAM TECNOLOGIA REDES E SERVICOS**
Situação do Fornecedor: **Credenciado**

Nenhum registro de Ocorrência Ativa encontrado para o fornecedor

Sistema de Cadastramento Unificado de Fornecedores - SICAF

Relatório de Prováveis Ocorrências Impeditivas Indiretas do Fornecedor

Dados do Fornecedor

CNPJ: **14.438.757/0001-76** DUNS®: **901065486**
Razão Social: **CAM TECNOLOGIA LTDA**
Nome Fantasia: **CAM TECNOLOGIA REDES E SERVICOS**
Situação do Fornecedor: **Credenciado**

Nenhum registro de Ocorrência Impeditiva Indireta encontrado para o fornecedor.

CONTROLADORIA-GERAL DA UNIÃO

Certidão Negativa Correcional - Entes Privados (ePAD, CGU-PJ, CEIS, CNEP e CEPIM)

Consultado: **CAM TECNOLOGIA LTDA**

CPF/CNPJ: **14.438.757/0001-76**

Certifica-se que, em consulta aos sistemas ePAD e CGU-PJ e aos cadastros CEIS, CNEP e CEPIM, mantidos pela Corregedoria-Geral da União, **NÃO CONSTAM** registros de penalidades vigentes ou de procedimentos acusatórios em andamento, relativos ao CPF/CNPJ consultado.

Destaca-se que, nos termos da legislação vigente, os referidos cadastros consolidam informações prestadas pelos entes públicos, de todos os Poderes e esferas de governo.

Os Sistemas ePAD e CGU-PJ consolidam os dados sobre o andamento dos processos administrativos de responsabilização de entes privados no Poder Executivo Federal.

O Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) apresenta a relação de empresas e pessoas físicas que sofreram sanções que implicaram a restrição de participar de licitações ou de celebrar contratos com a Administração Pública.

O Cadastro Nacional de Empresas Punidas (CNEP) apresenta a relação de empresas que sofreram quaisquer das punições previstas na Lei nº 12.846/2013 (Lei Anticorrupção).

O Cadastro de Entidades Privadas sem Fins Lucrativos Impedidas (CEPIM) apresenta a relação de entidades privadas sem fins lucrativos que estão impedidas de celebrar novos convênios, contratos de repasse ou termos de parceria com a Administração Pública Federal, em função de irregularidades não resolvidas em convênios, contratos de repasse ou termos de parceria firmados anteriormente.

Certidão emitida às 10:41:42 do dia 15/12/2025 , com validade até o dia 14/01/2026.

Link para consulta da verificação da certidão https://certidoes.cgu.gov.br/

Código de controle da certidão: zovd9dAMEvMa0NwTL9iO

Qualquer rasura ou emenda invalidará este documento.