Admin Guide

Yeastar S1000-P IPPBX

Version: 80.13.53.34.45
Date: 2022-12-16

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

Yeastar Information Technology Co.Ltd.

Contents

Admin Guide

Admin Guide for Yeastar S1000-P IPPBX.

About this guide

In this guide, we describe every detail on the functionality and configuration of the Yeastar S1000-P IPPBX. We begin by assuming that you are familiar with networking and other IT disciplines.

Product covered

- Yeastar S1000-P IPPBX

Audience

This guide is for administrators who need to prepare for, configure, and operate Yeastar S1000-P IPPBX.

Getting Started

Log in to the PBX Web Interface

Yeastar S1000-P IPPBX provides a web management portal that allows you to quickly set up and manage the system. This topic describes how to log in to the PBX web interface.

Prerequisites

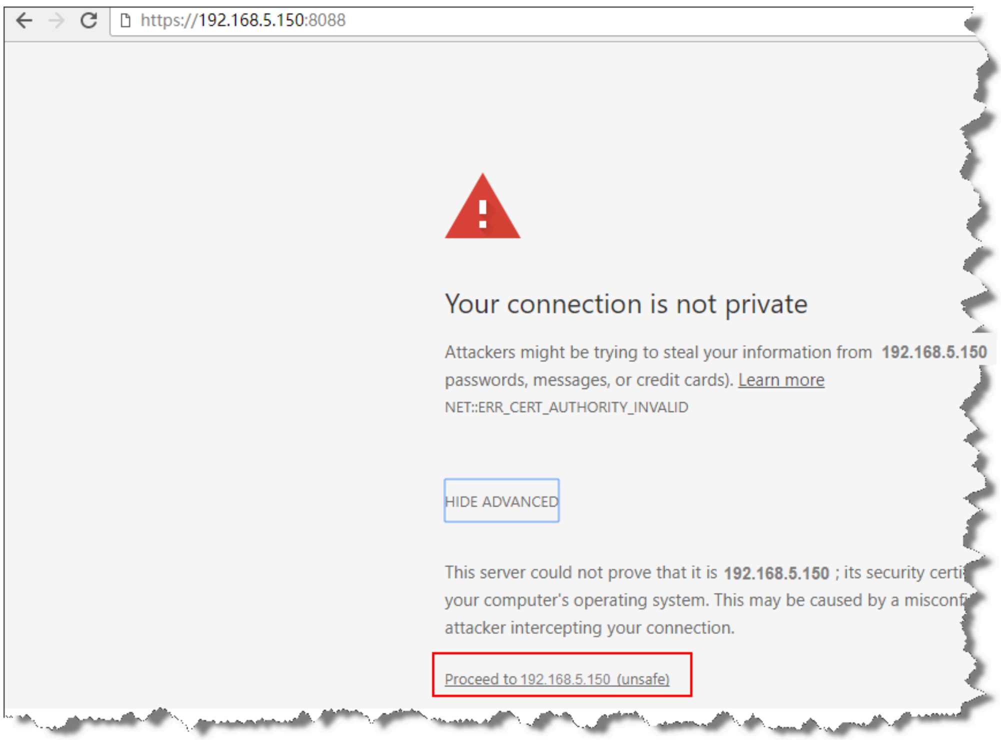
- You have connected the network cable to the PBX.
- The IP address of the PC must be on the same network segment as that of the PBX and cannot conflict with IP addresses of other devices.

> Note:
> - The default IP address of Yeastar S1000-P IPPBX is 192.168.5.150, and the default gateway address is 192.168.5.1.
> - If you fail to access the PBX web interface, contact your network administrator to check if your PC can communicate with the IP address 192.168.5.150.

Procedure

1. Open web browser, enter the PBX' IP address (default: 192.168.5.150) 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 interface.

> Note:
> Your connection is secure. The warning is caused by the certificate that is installed for remote management. You can purchase a trusted third party certificate to avoid this message.



3. Enter the administrator username and password, click Login.
    - Username(default): admin
    - Password(default): password

What to do next

Follow the Configuration Wizard to set up your PBX.

Initial Setup Using the Installation Wizard

The configuration wizard will run you through the most basic PBX configurations to get your phone system started.

Step1. Change default password

For security reasons, we recommend that you change the default password.

1. In the Old Password field, enter the default password.
2. In the New Password and Retype New Password fields, enter your new password.
3. Click Next.

Step2. Bind administrator email

Bind an email address with the Administrator account. The email will be used to retrieve your account password and receive notification from PBX Event Center.

1. In the Email Address field, enter your email address.
2. Click Next.

Step3. Configure email server

Set up your email server, which will be used to send password recovery emails and event notification emails.

1. In the Sender Email Address field, enter the sender email address, which will appear as the address of FROM for outgoing emails.
2. In the Email Address or Username field, enter the account to log in to the email server.

   > Note:
   > Generally, enter the same address as the Sender Email Address. If the email server provides a unique user name, enter the user name.

3. In the Password field, enter the password to log in to the email server.
4. In the Outgoing Mail Server (SMTP) field, enter the outgoing mail address and port.
5. In the Incoming Mail Server (POP3) field, enter the incoming mail address and port.
6. If the email sending server needs to authenticate the sender, you need to select the checkbox of Enable TLS.

   For more information of email server settings, see Email (on page 205).

Step4. Configure network

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

1. Select the Ethernet mode and default interface.
    - Mode: Select an Ethernet mode.
        - Single: Only LAN port is used for connection, WAN port is disabled.
        - Dual: Both LAN port and WAN port are used for connection.

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

    For more information of network settings, see Basic Network Overview (on page 150).

Step5. Configure date and time

Configure the time zone and daylight saving time, and set up the date and time manually or synchronize with a NTP server.

1. In the Time Zone drop-down list, select your time zone.
2. In the Daylight Saving Time drop-down list, select a setting as your need.
3. Synchronize system time with a NTP server or set a date and time manually.

    For more information of date and time settings, see Date and Time (on page 204).

Step6. Configure extension preferences

Change the extension range according to your needs.

Step7. Configure extensions

Create extensions for your users to register and have calls. The default extension user passwords are created randomly by the system.

For more information of extensions, see Extension Overview (on page 6).

Step8. Configure trunks

Configure your trunk(s) which will be used to get inbound calls and make outbound calls.

For more information of trunks, see Trunk (on page).

Step9. Configure time conditions

Time conditions are used to control call flow based upon date and time. It can be applied to inbound route(s) to direct calls to different destinations upon different date and time. Or used for outbound route(s) to bar outbound calls within a specified date and time.

For more information of time conditions, see Time Conditions Overview (on page 53).

Step10. Configure inbound routes

Configure your inbound route(s). An inbound route is used to tell the PBX where to route inbound calls based on the phone number or DID dialed.

For more information of inbound routes, see Inbound Route Overview (on page 63).

Step11. Configure outbound routes

Configure your outbound route(s). An outbound route works like a traffic cop giving directions to road users to use a predefined route to reach a predefined destination.

For more information of outbound routes, see Outbound Route Overview (on page 81).

Step12. Configure event center

Event Center records and notifies the PBX's system abnormal events. If you wish the PBX to send notification when a specific abnormal event occurred, please set up Notification Contact and turn on the Notification option for the event.

For more information of event notifications, see Event Center (on page 208).

Change Web Interface Language

Switch the web interface language according to your needs.

Procedure

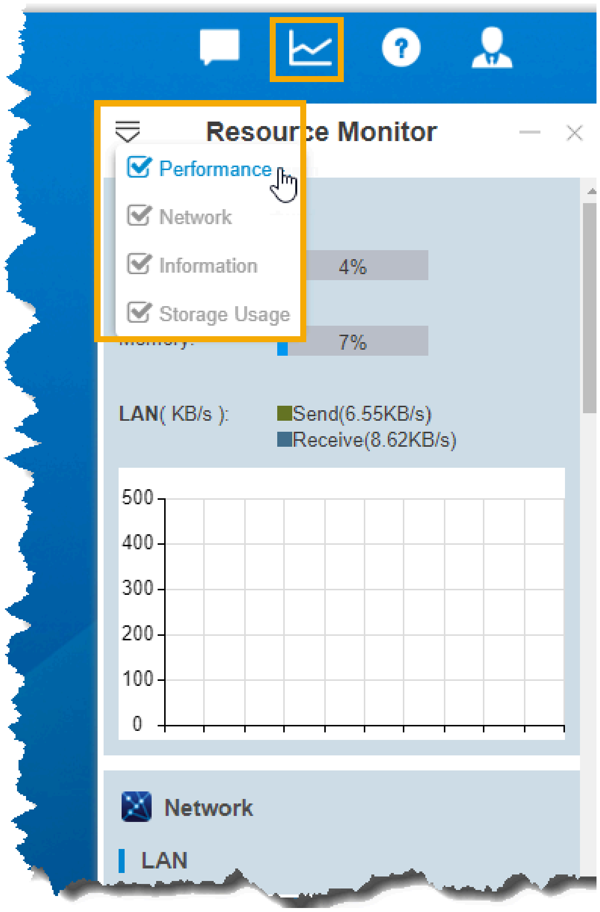
1. At the top-right conner of the web page, click .
2. Select Language and select your desired language.

   The web interface is switched to the selected language immediately.

View System Information

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

1. At the top-right conner of the web page, click .
2. Select the information that you want to view.



Extensions

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 type

Yeastar S1000-P IPPBX supports SIP extension, which is based on SIP protocol.

To use a SIP extension, you need to enter the extension credentials on an IP phone or a soft-phone. After the extension is registered on a phone, you can make and receive calls.

Extension format

Yeastar S1000-P IPPBX supports 1-digit to 7-digit extension format. The default extension format is 4-digit number.

Before you create extensions, you can go to Settings > PBX > General > Preferences > Extension Preferences > User Extensions to change the extension format and range.

Extension Basic Setup

Create Extensions

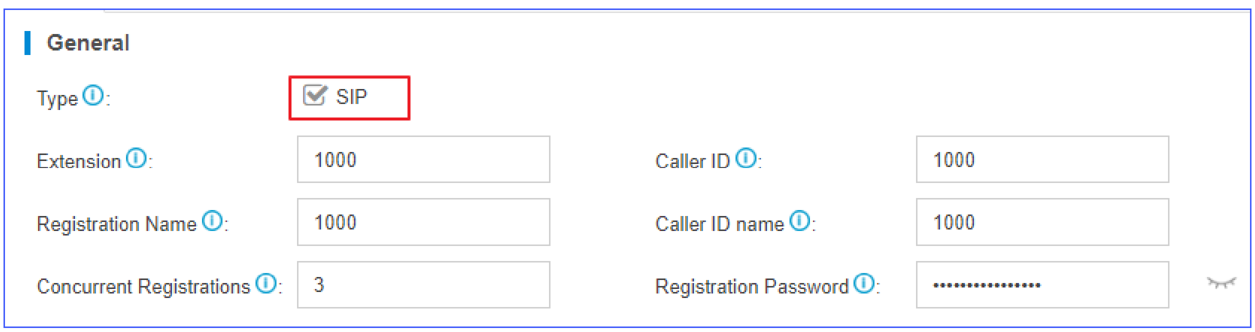
Extension Creation Overview

Yeastar S1000-P IPPBX supports SIP forking, which enables an extension number to register on multiple SIP phones simultaneously.

Set one extension number for multiple devices

You can link your office phone, softphone, and analog phone through a universal extension number. When a call reaches the extension number, all phones will ring simultaneously, you won't miss any business calls.

On extension configuration page, you can select multiple types for the extension.



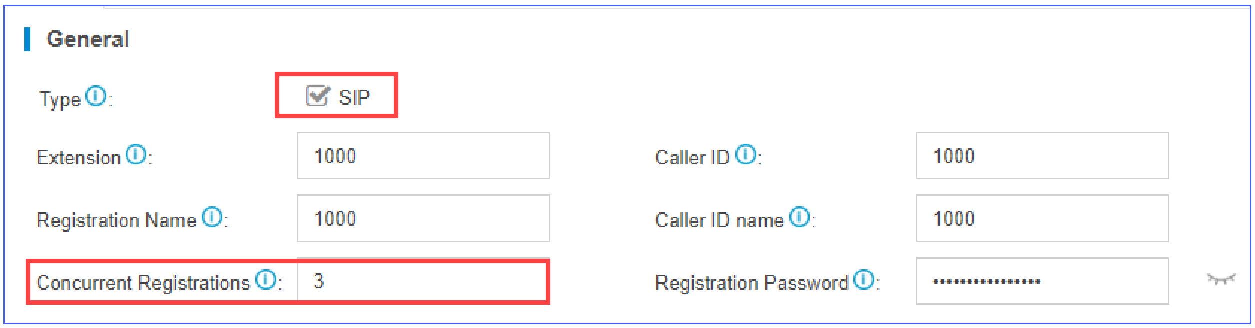
SIP Forking

Yeastar S1000-P IPPBX supports SIP forking, which enables an extension number to be registered by multiple SIP phones. When a call reaches the extension, all registered phones will ring simultaneously, and you can take the call from any device easily.

You can configure SIP Forking on the extension configuration page. The value of Concurrent Registrations limits how many SIP phones the extension can be registered.

Note:

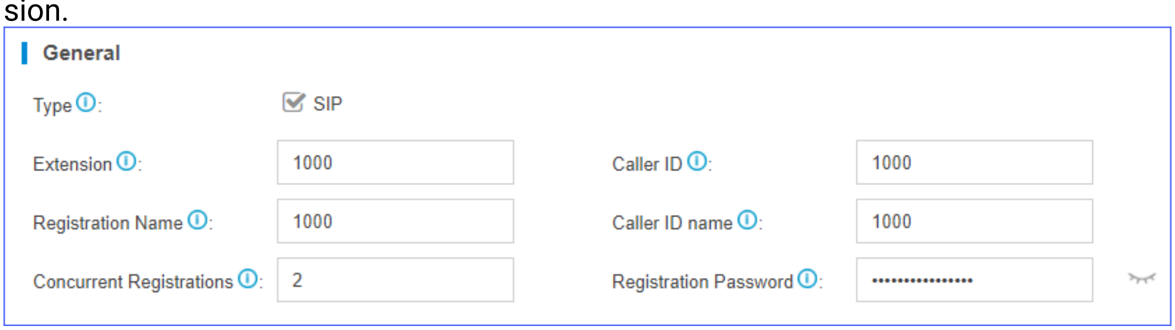
- The limit of concurrent registrations is 5.
- By default, if one SIP phone is busy, other SIP phones still can receive calls when calls reach the extension. To restrict other phones from receiving calls when the extension is busy, you can enable All Busy Mode for SIP Forking (Settings > PBX > General > SIP > Advanced).



Create a SIP Extension

Yeastar S1000-P IPPBX supports Session Initiation Protocol (SIP). SIP is used in VoIP communications allowing users to make and receive voice calls for free over the Internet. Before registering a SIP account on phones, you need to create a SIP account.

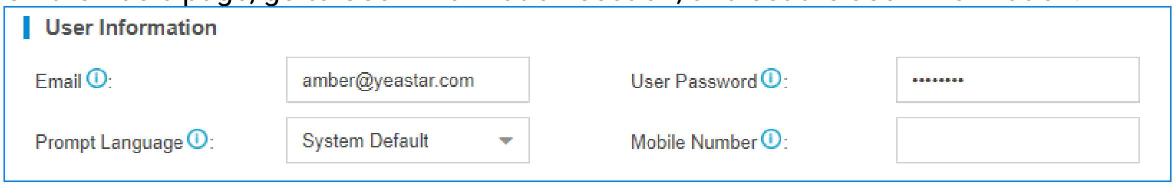
1. Go to Settings > PBX > Extensions, click Add.
2. On the Basic page, go to General section, and set the general settings of the extension.



    - Type: Select the checkbox of SIP.
    - Extension: Enter the extension number.
    - Caller ID: Enter the caller ID number. The called party will see this caller ID number when the extension user makes an outgoing call.
    - Registration Name: The name used to register a SIP extension.
    - Caller ID name: Enter the caller ID name. The called party will see this caller ID name when the extension user makes an outgoing call.

- Concurrent Registrations: Yeastar S1000-P IPPBX supports to register one SIP extension number on multiple phones. When a call reaches the extension number, all phones will ring. The maximum number of concurrent registrations is 5.
- Registration Password: The password is used to register the extension.

3. On the Basic page, go to User Information section, and set the user information.



- Email: Extension user can reset his/her login password, receive voicemails, faxes, or PBX notifications via this email address.
- User Password: Extension user can log in to the PBX web interface by the user password.
- Prompt Language: The language of voice prompts. The default prompt language is the same as the system language. If the extension user speaks foreign language, you can set a specific system prompt.

> Note:
> Before selecting other system prompts, go to Settings > PBX > Voice Prompts > System Prompt to download online prompts.

- Mobile Number: Extension user can receive the PBX notifications or forwarded calls on this mobile number.

4. Optional: Click Features, Advanced, or Call Permission tab to configure other settings (on page 33).
5. Click Save and Apply.

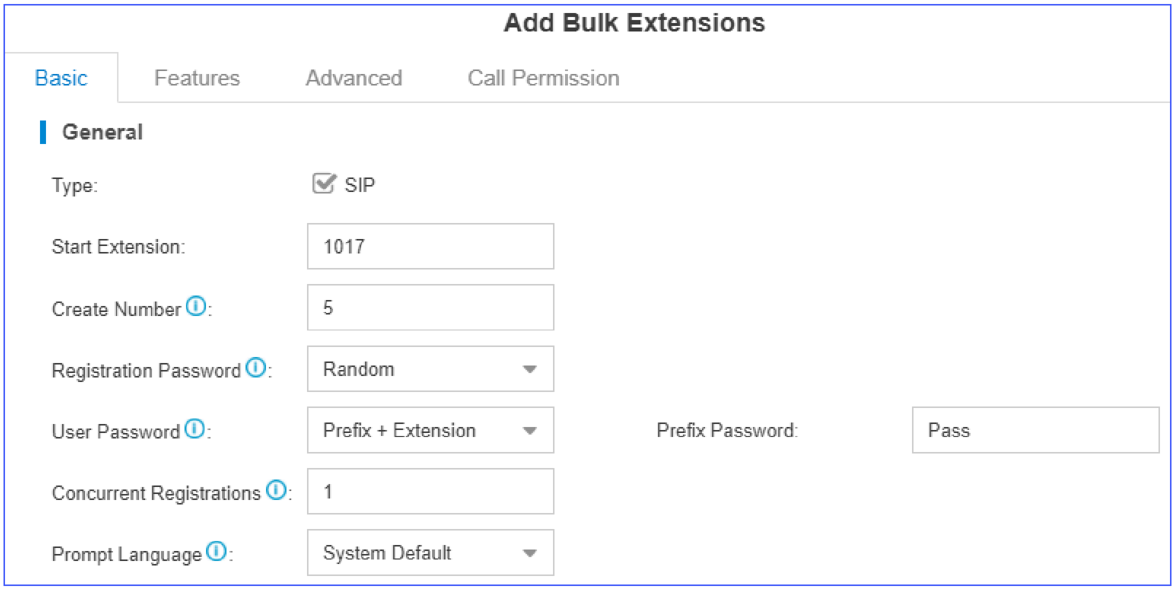
Related information
Register a SIP Extension (on page 11)

Bulk Create Extensions

Yeastar S1000-P IPPBX supports to add SIP extensions in bulk.

1. Go to Settings > PBX > Extensions, click Bulk Add.
2. On the Basic page, configure the following settings:

> Note:
> If you want to edit the Registration Password and User Password for multiple extensions, you need to go to Settings > System > Security > Service, select the checkbox of Allow Weak Password.



- Type: Select the extension type.
- Start Extension: Enter the first extension number. The system will create extensions in bulk starting with the extension number.
- Create Number: Enter the number of extensions that will be created.
- Registration Password: Specify which type of registration password will be created.
    - Random: If you choose the option, a random password will be generated for each extension.
    - Fixed: If you choose the option, enter a password in the Fixed Password field. All the newly created extensions use the same registration password.
    - Prefix+Extension: If you choose the option, enter a prefix in the Prefix Password field. The password will be the prefix plus extension number.
- User Password: Specify which type of user password will be created.
    - Fixed: If you choose the option, enter a password in the Fixed Password field. All the newly created extensions use the same user password.
    - Prefix+Extension: If you choose the option, enter a prefix in the Prefix Password field. The password will be the prefix plus extension number.
- Concurrent Registrations: Yeastar S1000-P IPPBX supports to register one extension number on multiple phones. When a call reaches the extension number, all phones will ring.
- Prompt Language: The language of voice prompts. The default prompt language is the same as the system language. If the extension user speaks foreign language, you can set a specific system prompt.

> **Note:**
> Before selecting other system prompts, go to Settings > PBX > Voice Prompts > System Prompt to download online prompts.

3. Optional: Click Features, Advanced, or Call Permission tab to configure other settings.
4. Click Save and Apply.

Related information
Bulk Edit Extension Names and Emails (on page 15)
Register a SIP Extension (on page 11)

Register Extensions

Register a SIP Extension

To make and receive calls from a SIP extension, you need to register the SIP extension on an IP phone or soft phone.

1.Gather information of extension registration

For most SIP phones, the following items are needed for the SIP phone to register with Yeastar S1000-P IPPBX.

- IP address of PBX
- SIP registration port: The default port is 5060 on Yeastar S1000-P IPPBX.
- Extension information
  - Extension Number
  - Registration Name
  - Registration Password
  - Caller ID Name
  - Transport

2.Register the extension on a phone

Log in to the phone web interface, fill in and save the required items to register the SIP extension.

3.Confirm registration status

You can do one of the followings to check if the extension is registered.

- On the phone web interface, check if the status indicates that the extension is registered.
- Log in to PBX web interface, go to PBX Monitor > Extensions to check if the status shows .

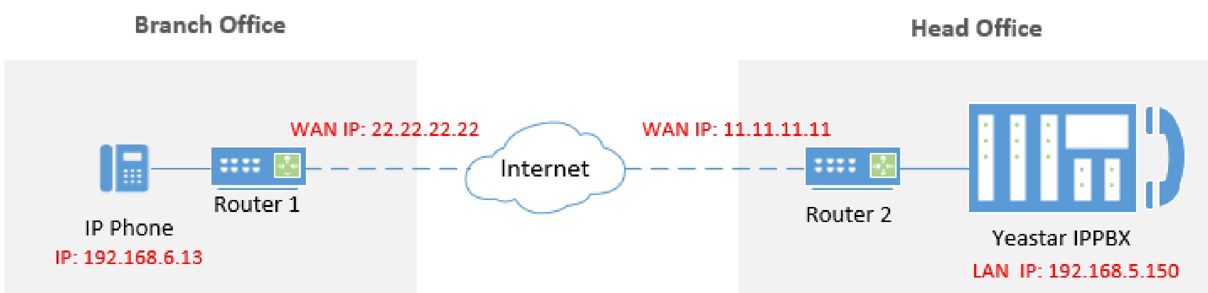
Related information
Register Yealink Phone with Yeastar S1000-P IPPBX (on page)
Register Htek Phone with Yeastar S1000-P IPPBX (on page)
Register Cisco Phone with Yeastar S1000-P IPPBX (on page)
Register Fanvil Phone with Yeastar S1000-P IPPBX (on page)
Register Snom Phone with Yeastar S1000-P IPPBX (on page)

Register a Remote Extension

When you are out of the office, you can register a remote extension on a softphone or an IP phone.

Scenario

The instructions provided in this topic are based on the following scenario: PBX and IP phone are in different IPv4 network with their own private IP address.



Procedure

For IPv4 network

1. Forward the required ports on router (on page 12)
2. Configure SIP NAT settings on PBX (on page 13)
3. Set up an extension for remote access (on page 13)
4. Register the extension on the phone (on page 14)

For IPv6 network

1. Forward the required ports on router (on page 12)
2. Set up an extension for remote access (on page 13)
3. Register the extension on the phone (on page 14)

Forward the required ports on router

Forward the following default ports on the Router 2, 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).

> Tip:
> You can change the default ports on Settings > PBX > General > SIP > General.

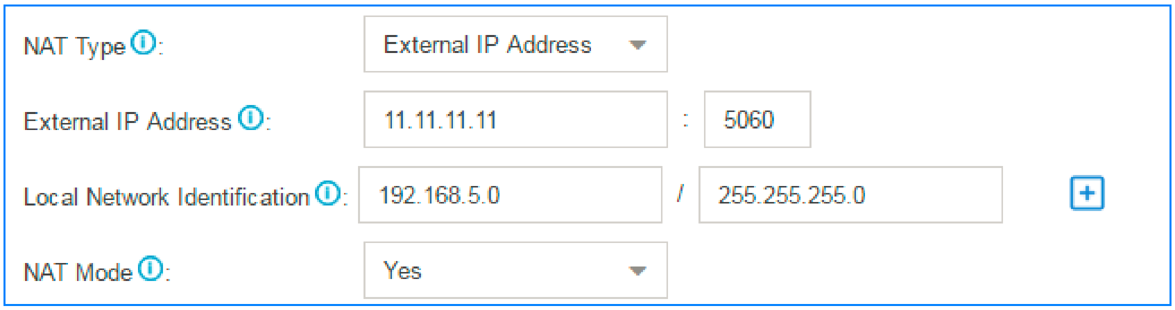
- SIP Registration Port: UDP 5060 (default)
- RTP Port Range: UDP 10000-12000 (default)

Configure SIP NAT settings on PBX

> **Note:**
> If IPv6 network is used, skip this step.

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

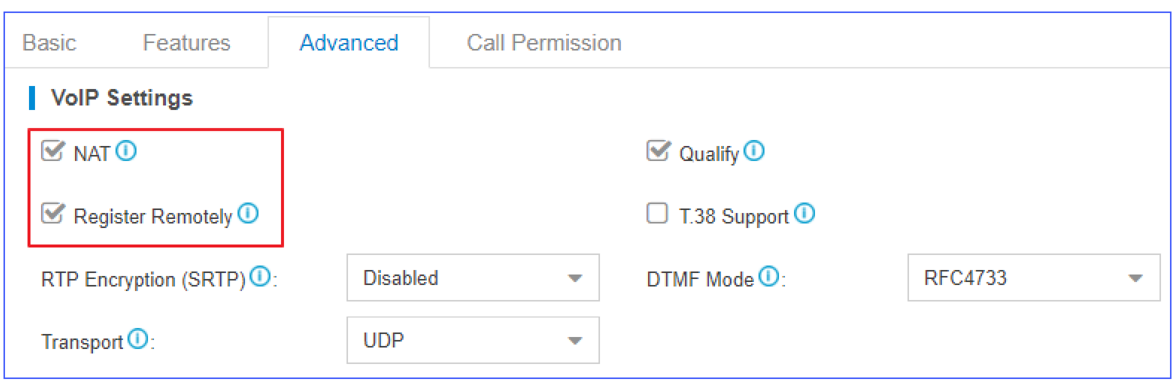
1. Log in to PBX web interface, go to PBX > General > SIP > NAT.
2. Configure NAT settings:



   a. In the NAT Type drop-down list, select External IP Address.
   b. In the External 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.
   d. In the NAT Mode drop-down list, select Yes.
3. Click Save and Apply.

Set up an extension for remote access

1. Log in to PBX web interface, go to PBX > Extensions, edit the desired extension.
2. Click Advanced tab.
3. Select the checkbox of NAT and Register Remotely.

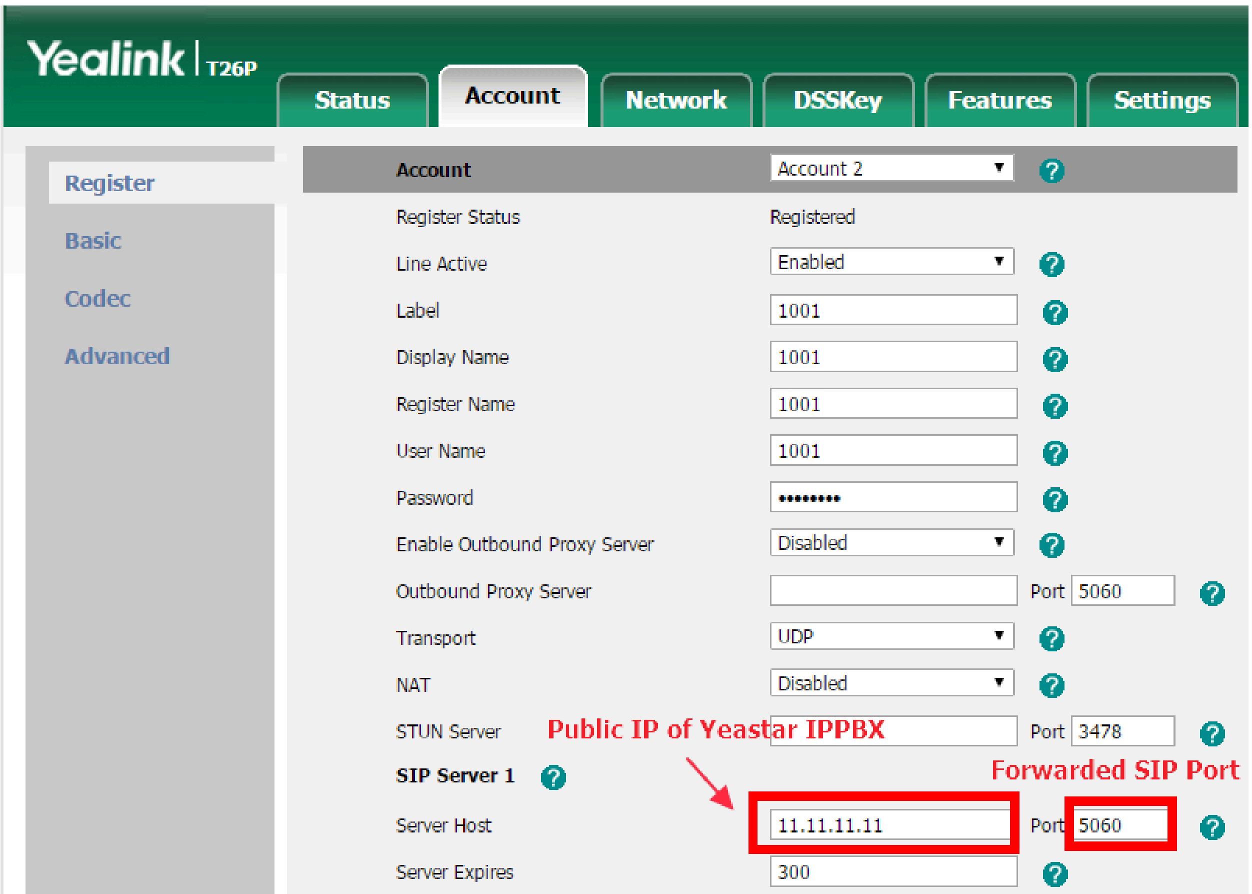


4. Click Save and Apply.

Register the extension on the phone

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

> Note:
> Use the public IP address or hostname of the PBX and the forwarded SIP port to register the remote extension.



Manage Extensions

Change Extension Range

The default extension range is from 1000 to 5999. Before you create extensions, you can change the extension range according to your needs.

1. Log in to the PBX web interface, go to Settings > PBX > General > Preferences > Extension Preferences.
2. Change the range of User Extensions.
3. Click Save and Apply.

Edit Extensions

After creating extensions, you may need to change extension settings. You can edit an extension, or edit extensions in bulk.

Edit an Extension

1. Log in to the PBX web interface, go to Settings > PBX > Extensions.
2. On Extensions page, click beside the extension that you want to edit.
3. Change extension settings according to your needs.
4. Click Save and Apply.

Bulk Edit Extensions

1. Log in to the PBX web interface, go to Settings > PBX > Extensions.
2. On Extensions page, select the checkboxes of the desired extensions, click Edit.
3. Change extension settings according to your needs.
4. Click Save and Apply.

Bulk Edit Extension Names and Emails

To bulk edit the extension names and emails, you need to export the extensions from Yeastar S1000-P IPPBX first, edit the extension names and email addresses in the CSV file, then import the file to the PBX.

1. Log in to the PBX web interface, go to Settings > PBX > Extensions, click Export to export all the extensions.
2. Edit the CSV file, enter the users' names and email addresses, then save the file.

	A	B	C	D	E	F	G	H	I	J	K	L
1	type	username	fullname	callerid	registerr	registerp	loginpass	vmsecret	hasvoicem	enablevm	email	ringtimec
2	SIP	1000	carol	1000	1000	XbY-?01S_@NWOYPP		1000	yes	no	carol@yeastar.com	30
3	SIP	1001	eve	1001	1001	tIf?1@YjretXYPVY		1001	yes	no	eve@yeastar.com	30
4	SIP	1002	ina	1002	1002	??F-52ivj745omnr		1002	yes	no	ina@yeastar.com	30
5	SIP	1003	apple	1003	1003	k1QCFN-~GOUWTARO		1003	yes	no	apple@yeastar.com	30
6	SIP	1004	david	1004	1004	3kGSY@@~?onxJM7O		1004	yes	no	david@yeastar.com	30
7	SIP	1005	amber	1005	1005	_4Q3-a~C40INC_0P		1005	yes	no	amber@yeastar.com	30
8	SIP	1006	alan	1006	1006	i_TU_G2J~_~@^YFP		1006	yes	no	alan@yeastar.com	30
9	SIP	1007	jason	1007	1007	@*?4rF*-S1*M_HKG		1007	yes	no	jason@yeastar.com	30
10	SIP	1008	ramon	1008	1008	@-N81AlTKIGIXJTE		1008	yes	no	ramon@yeastar.com	30
11	SIP	1009	harry	1009	1009	?*0es*tuGIN@-hsg		1009	yes	no	harry@yeastar.com	30
12	SIP	1010	pixy	1010	1010	D*2-*_to16408512		1010	yes	no	pixy@yeastar.com	30
13	SIP	1011	rose	1011	1011	^F2?65otv2plerrj		1011	yes	no	rose@yeastar.com	30
14	SIP	1012	hermy	1012	1012	@T1u*?1UG_~KsrVR		1012	yes	no	hermy@yeastar.com	30
15	SIP	1013	gary	1013	1013	W~h-~6x??-^?_?^_		1013	yes	no	gary@yeastar.com	30
16	SIP	1014	jerry	1014	1014	712rx_?BUAmobLLG		1014	yes	no	jerry@yeastar.com	30
17												

- fullname: Enter the user's name. The fullname stands for the Caller ID Name.
- email: Enter the user's email address.

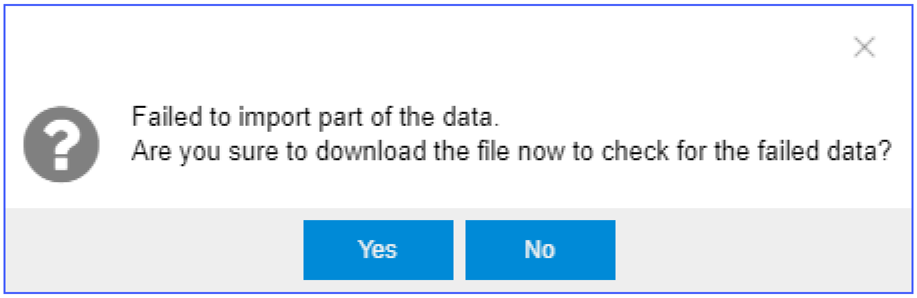
3. Import the CSV file to the PBX.

   a. Go to Settings > PBX > Extensions, click Import.

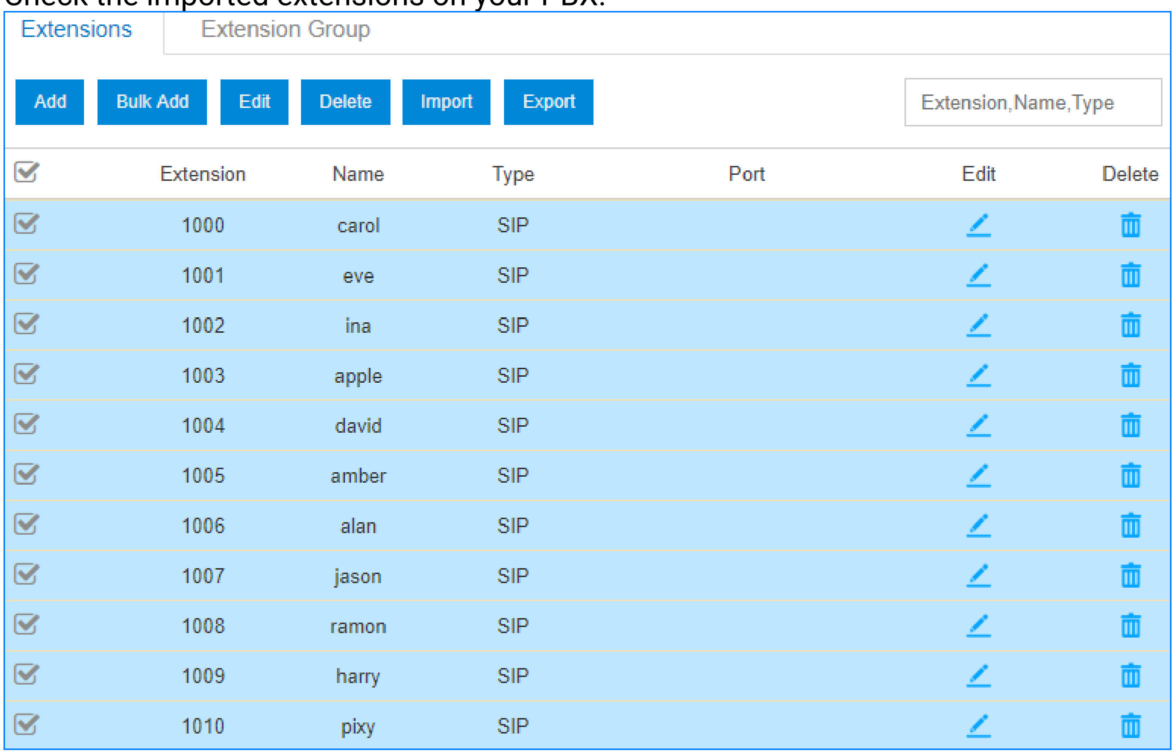
   b. In the pop-up window, click Browse, select your CSV file.

c. Click Import.
   If you get an error prompt like the following figure, click Yes to check the log.

> **Note:**
> Ignore the error if the Error Cause displays "username[1000]: The imported record is existing, the record has been overwritten".



4. Check the imported extensions on your PBX.



Delete Extensions

When an employee leaves or an extension is no longer needed, you can delete the extension from the Yeastar S1000-P IPPBX.

Delete an Extension

1. Log in to the PBX web interface, go to Settings > PBX > Extensions.
2. On Extensions page, click beside the extension that you want to delete.
3. In the pop-up dialog box, click Yes.
4. Click Apply.

Bulk Delete Extensions

1. Log in to the PBX web interface, go to Settings > PBX > Extensions.
2. On Extensions page, select the checkboxes of the desired extensions, and click Delete.
3. In the pop-up dialog box, click Yes.
4. Click Apply.

Import or Export Extensions

The extensions configured on Yeastar S1000-P IPPBX can be exported and saved as a template. You can fill in desired extension information and import the CSV file to PBX again.

Export Extensions

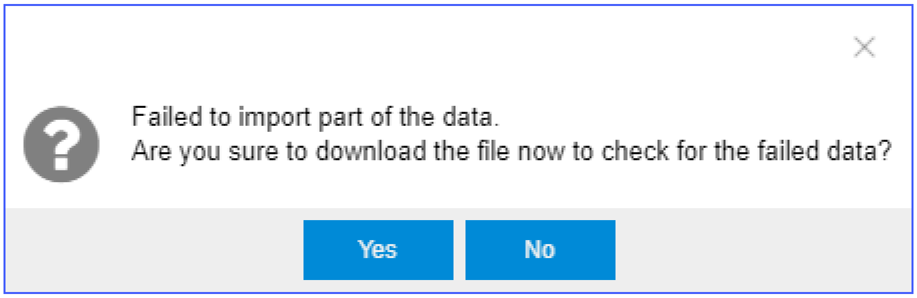
1. Log in to the PBX web interface, go to Settings > PBX > Extensions.
2. Click Export to export the extensions to a CSV file.

Import Extensions

> Tip:
> You can export extensions first, and use the CSV file as a template.

1. Log in to the PBX web interface, go to Settings > PBX > Extensions.
2. Refer to the Import Parameters - Extensions (on page), and edit your CSV file.
3. Click Import.
4. In the pop-up window, click Browse to select your CSV file.
5. Click Import.
   If you get an error prompt like the following figure, click Yes to check the log.

> Note:
> Ignore the error if the Error Cause displays "username[1000]: The imported record is existing, the record has been overwritten".

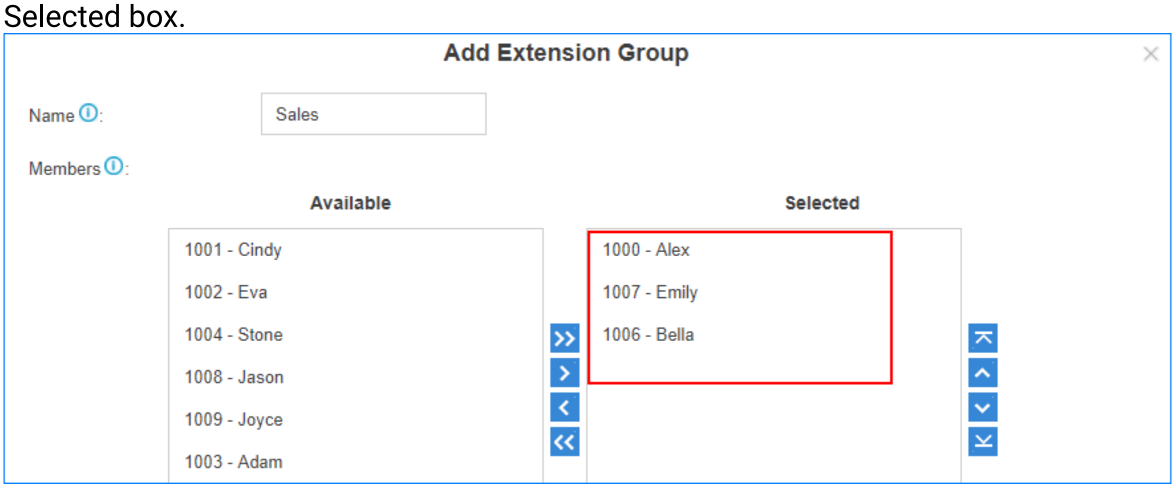


Extension Groups

Create an Extension Group

You can assign and categorize extensions in different groups. Extension groups simplify the configuration process.

1. Go to Settings > PBX > Extensions > Extension Group, click Add.
2. Set the Name to help you identify the group.
3. In the Members section, select the desired extensions from the Available box to the Selected box.



4. Click Save.

Manage Extension Groups

Edit extension groups

You can edit the group name, add more extensions to the group or remove extensions from the group.

1. Go to Settings > PBX > Extensions, click Extension Group tab.
2. Click beside the desired extension group.
3. Edit group settings according to your needs.
4. Click Save and Apply.

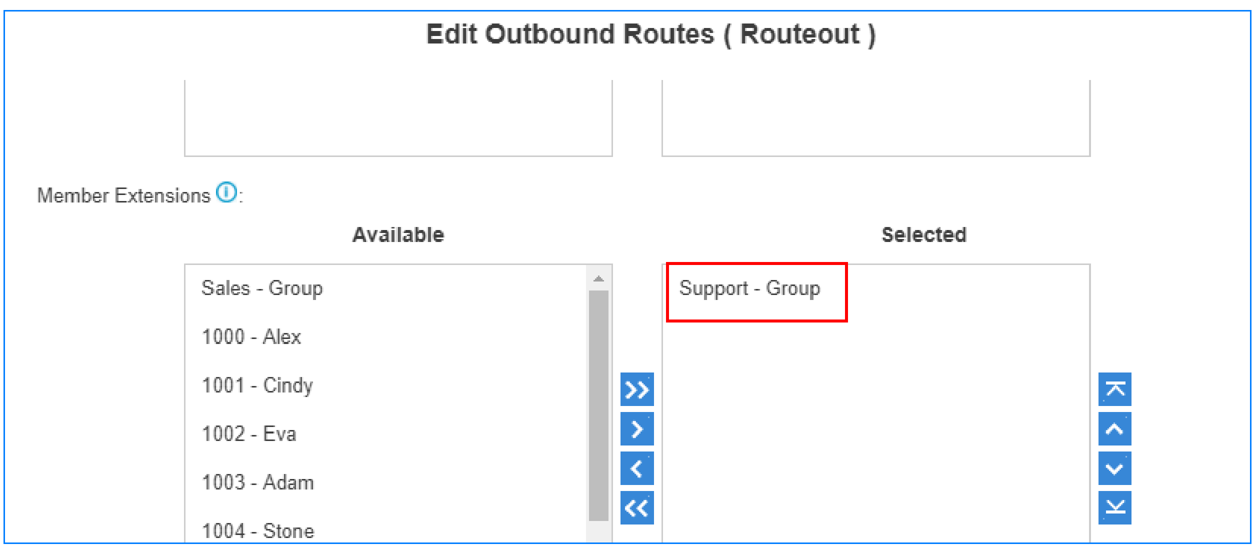
Delete extension group

1. Go to Settings > PBX > Extensions > Extension Group, search and find the desired extension group, click .
2. Click Yes and Apply.

Extension Groups Application

You can use the extension groups when you need to assign outbound routes, ring groups, or queues for extensions.

To set up an outbound route that only allows members in Support Department to make outbound calls, you can assign the outbound route to the department instead of manually assigning to members one by one, which simplifies the configuration process.



Voicemail

Voicemail Overview

Yeastar S1000-P IPPBX integrates a free voicemail system. Voicemail is a modern kind of answering machine that allows the callers to leave audio messages in case of unavailability.

Enable/Disable Voicemail Function

By default, the voicemail is enabled for all extension users. You can disable the Voicemail function if the user doesn't need it.

1. Go to Settings > PBX > Extensions, search and find the desired extension, click beside the desired extension.
2. Click Features tab.
3. Change the Voicemail settings.
    - To enable voicemail, select the checkbox of Enable Voicemail.
    - To disable voicemail, unselect the checkbox of Enable Voicemail.
4. Click Save and Apply.

Change Voicemail PIN/Password

Extension users can dial voicemail feature code (default *2) on their phones to access their voicemails. To enhance the extension security, you can change the voicemail PIN on PBX web interface.

1. Go to Settings > PBX > Extensions, click beside the desired extension.
2. Click Features tab.
3. In the Voicemail Access PIN field, enter a numeric PIN/password.
4. Click Save and Apply.

Configure Voicemail to Email

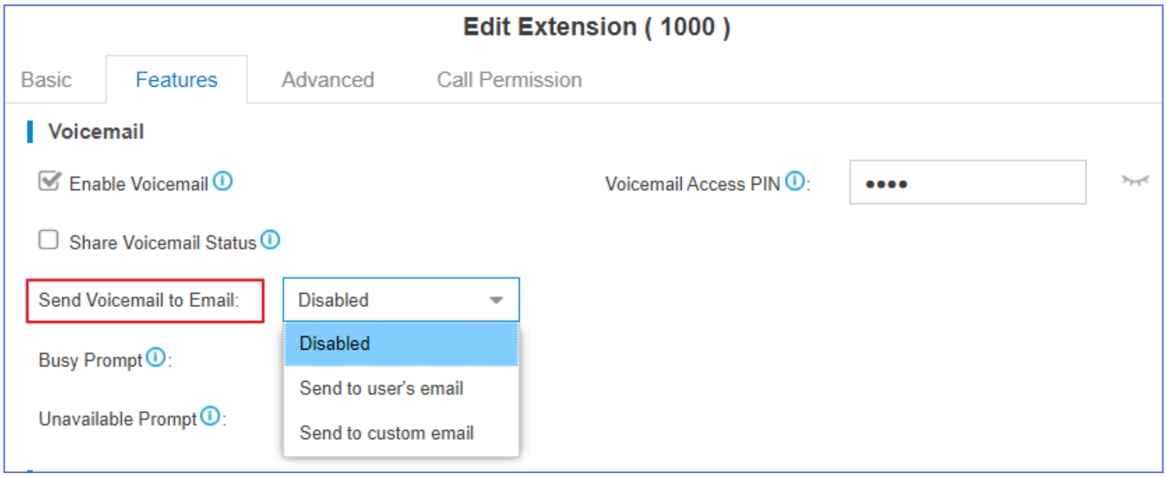
The Voicemail to Email feature of Yeastar S1000-P IPPBX allows extension users to receive voicemail audio files as email attachments and quicken response time when they are out of office.

Enable Voicemail to Email

Voicemail to Email function is disabled by default. If an extension user wants to check voicemail messages via email, you need to enable Voicemail to Email for his/her extension.

> **Note:**
> To receive voicemail via email successfully, make sure the system email (on page 205) is working.

1. Go to Settings > PBX > Extensions, click beside the desired extension.
2. Click Features tab.
3. In the Send Voicemail to Email drop-down list, select an email type.

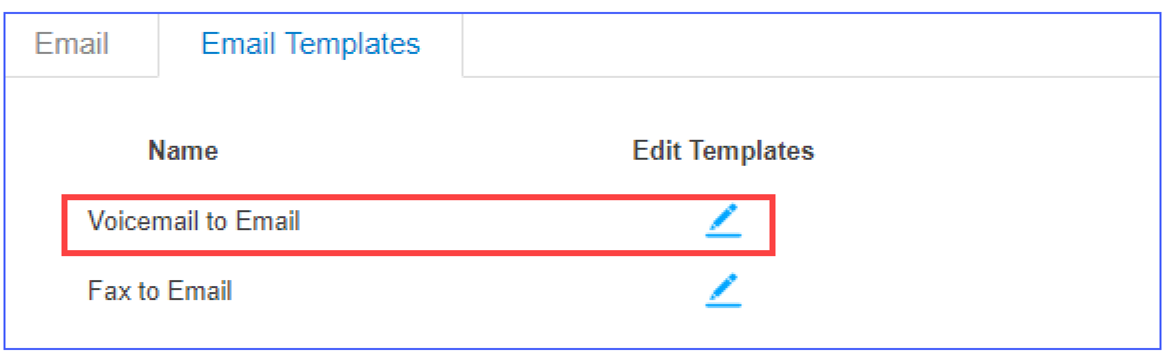


   - Send to user's email: Send voicemail to the extension user's email address.
   - Send to custom email: Send voicemail to a custom email address.
4. Click Save and Apply.

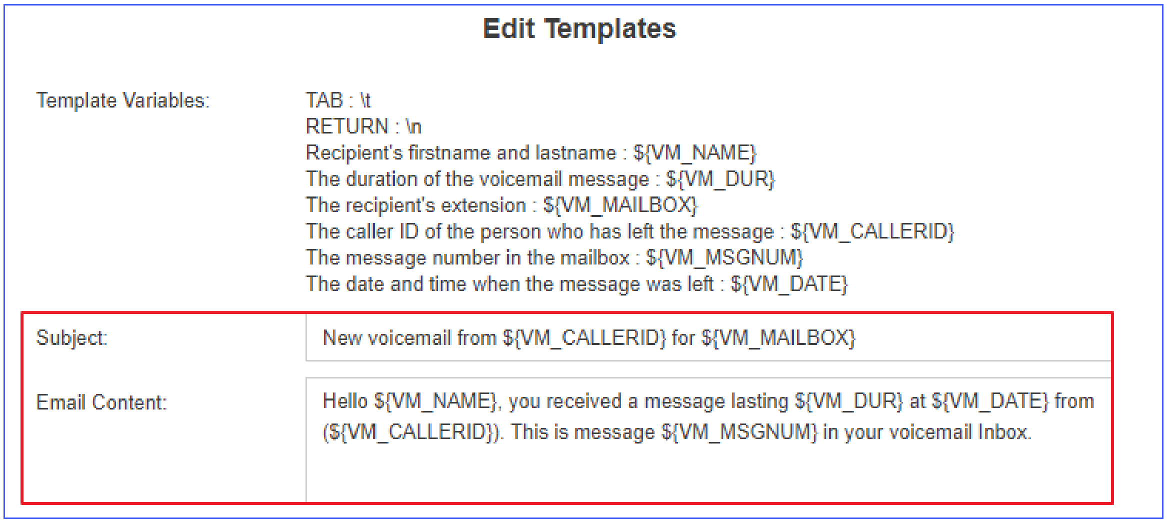
Email template of 'Voicemail to Email'

The PBX has a default email template for Voicemail to Email. You can edit the template according to your needs.

1. Go to Settings > System > Email > Email Templates, click beside Voicemail to Email.



2. Edit the email subject and email contents.



3. Click Save and Apply.

Check Voicemail Messages

Extension users have multiple ways to check their voicemail messages.

Check Voicemail on a Phone

- Dial feature code *2 on a phone

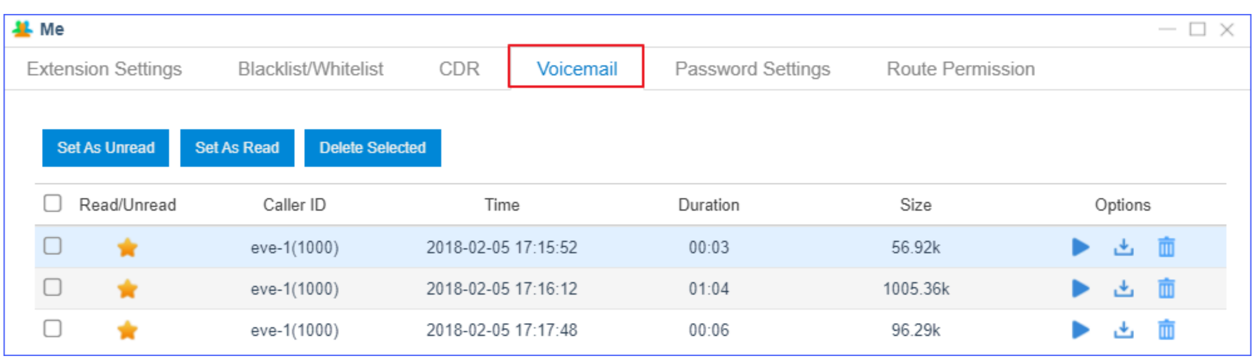
  A user can dial *2 on his/her own phone to check voicemail.
- Dial feature code *02 on a phone

  A user can dial *02 on another user's phone to enter the voicemail main menu, then enter his/her extension number and voicemail PIN to check voicemail.

Check Voicemail on Web Interface

Extension users can log in to the PBX web interface to check their own voicemails.

- User name: The extension user's extension number or email address.
- Password: The extension's User Password.



Check Voicemail via Email

If voicemail to email (on page 20) is enabled for an extension user, the user can check voicemails in his/her mailbox.

Check Voicemail via IVR

If you check the option Dial to Check Voicemail for an IVR, users can access the IVR to check their voicemails. This solution is for the users who are outside the office to check their voicemails.

Change Voicemail Greetings

You can change the global voicemail greetings for all the extension users or change voice-mail greeting for a specific extension.

Components of a Voicemail Greeting

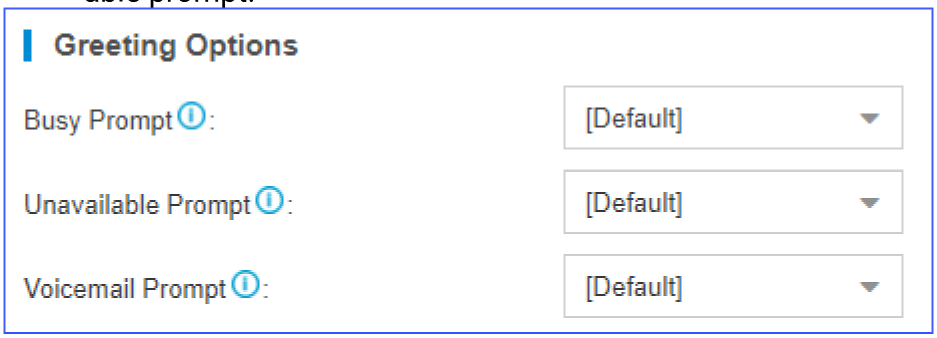
When an extension user is unavailable, the voicemail greeting consists of 3 audio clips: Un-available Prompt + Voicemail Prompt + "Di".

When an extension is busy on a phone, the voicemail greeting consists of 3 audio clips: Busy Prompt + Voicemail Prompt + "Di"

- Default Unavailable Prompt: The person at the extension XXXX is unavailable.
- Default Busy Prompt: The person at the extension XXXX is busy.
- Default Voicemail Prompt: Please leave your message after the tone, when done hang up or press the pound key (#)."

Change global voicemail greetings

1. Prepare your custom prompt files (on page 145), and upload to the PBX.
2. Go to Settings > PBX > General > Voicemail > Greeting Options.
3. Change the global voicemail greetings.
    - Busy Prompt: Select the prompt that will be played when the extension is busy.
    - Unavailable Prompt: Select the prompt that will be played when the extension is unavailable.
    - Voicemail Prompt: Select the prompt that will be played after Busy or Unavailable prompt.



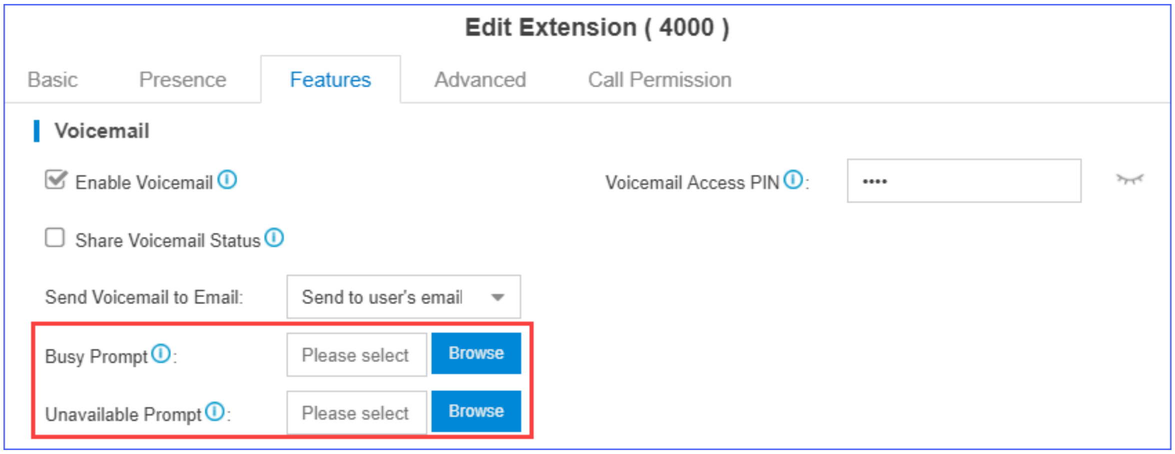
4. Click Save and Apply.

Change voicemail greetings for a specific extension

By default, the global busy prompt and global unavailable prompt are applied to all extensions. If an extension user wants to use his/her personal greetings, you can change the prompts for the extension.

> Note:
> The greeting prompt file format should be ".wav", ".WAV" or ".gsm" file.
>
> The file size must not be larger than 8 MB.
>
> Supported Format: PCM: 8K, 16bit, 128kbps; A-law(g.711): 8k, 8bit, 64kbps; u-law (g.711): 8k, 8bit, 64kbps; gsm: 6.10, 8k, 13kbps.

1. Go to Settings > PBX > Extensions, click beside the desired extension.
2. Click Features tab.
3. Click Browse to upload a prompt file.



4. Click Save and Apply.

Manage Voicemail Messages Centrally

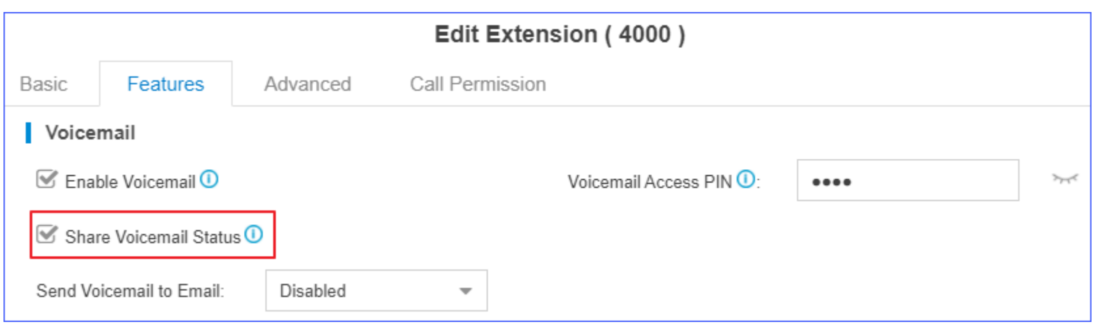
In Yeastar S1000-P IPPBX, you have two options to manage voicemail messages centrally and efficiently: subscribe BLF keys on a phone to monitor multiple extensions' voicemail status; receive multiple extensions' voicemail messages from one mailbox.

Monitor voicemail status by BLF keys

By default, an extension's voicemail status cannot be monitored by other users. To monitor an extension's voicemail status, you need to enable Share Voicemail Status on the extension.

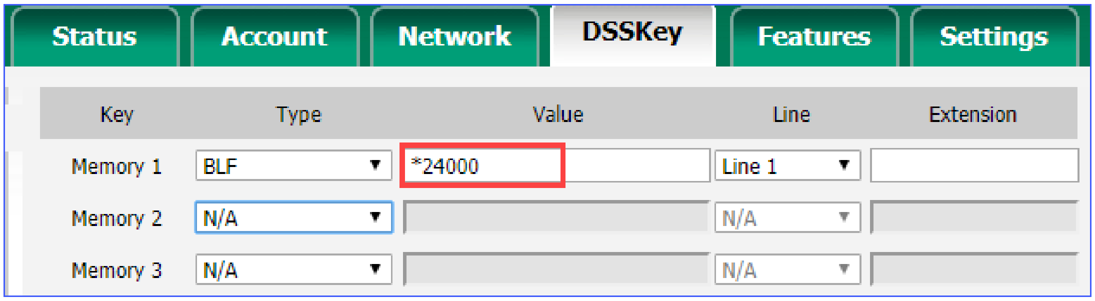
We take Yealink T27G v69.82.0.20 as an example to introduce how to monitor voicemail status of extension 4000 by extension 1000.

1. Enable voicemail status sharing feature of extension 4000.
    a. Log in to the PBX web interface, go to Settings > PBX > Extensions, edit the extension 4000.
    b. On the Features page, enable Share Voicemail Status.



    c. Click Save and Apply.
2. Set BLF key to monitor the voicemail status.
    a. Log in to the IP phone where extension 1000 is registered, go to Dsskey.
    b. Set a BLF key to monitor voicemail status of extension 4000.

- Type: Select BLF.
- Value: Enter *2{ext_num}. In this example, enter *24000.
- Line: Select the line where extension 1000 is registered.



c. Click Confirm.

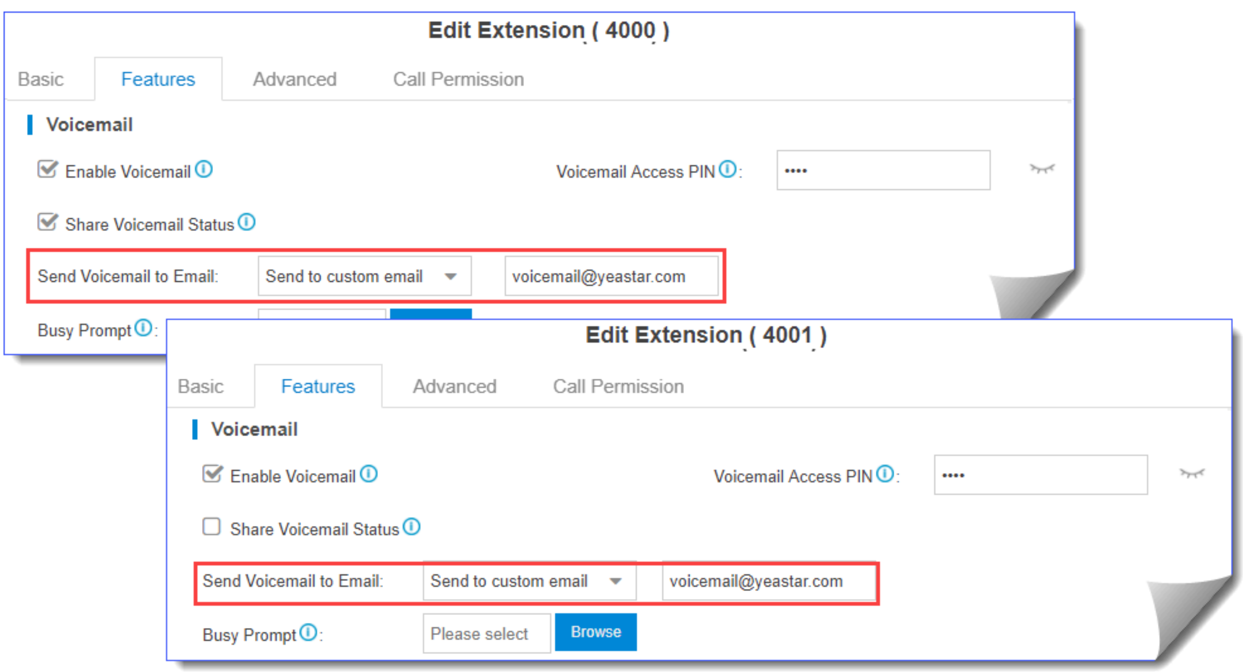
Result:

- Green BLF LED: The extension 4000 has NO unread voicemail messages.
- Red BLF LED: The extension 4000 has unread voicemail messages.

Receive voicemail from a mailbox

To receive multiple extensions' voicemail messages from one mailbox, you can configure sending voicemail to the same custom email address for these extensions.

For example, to receive multiple extensions' voicemail messages from the mailbox voicemail@yeastar.com. Set Send Voicemail to Email to the same custom email address voicemail@yeastar.com for these extensions.



Global Voicemail Settings

You can change message settings and playback settings for global voicemail according to your needs.

The global voicemail settings will be applied to all the extensions.

Navigation path: Settings > PBX > General > Voicemail.

Table 1. Global Voicemail settings

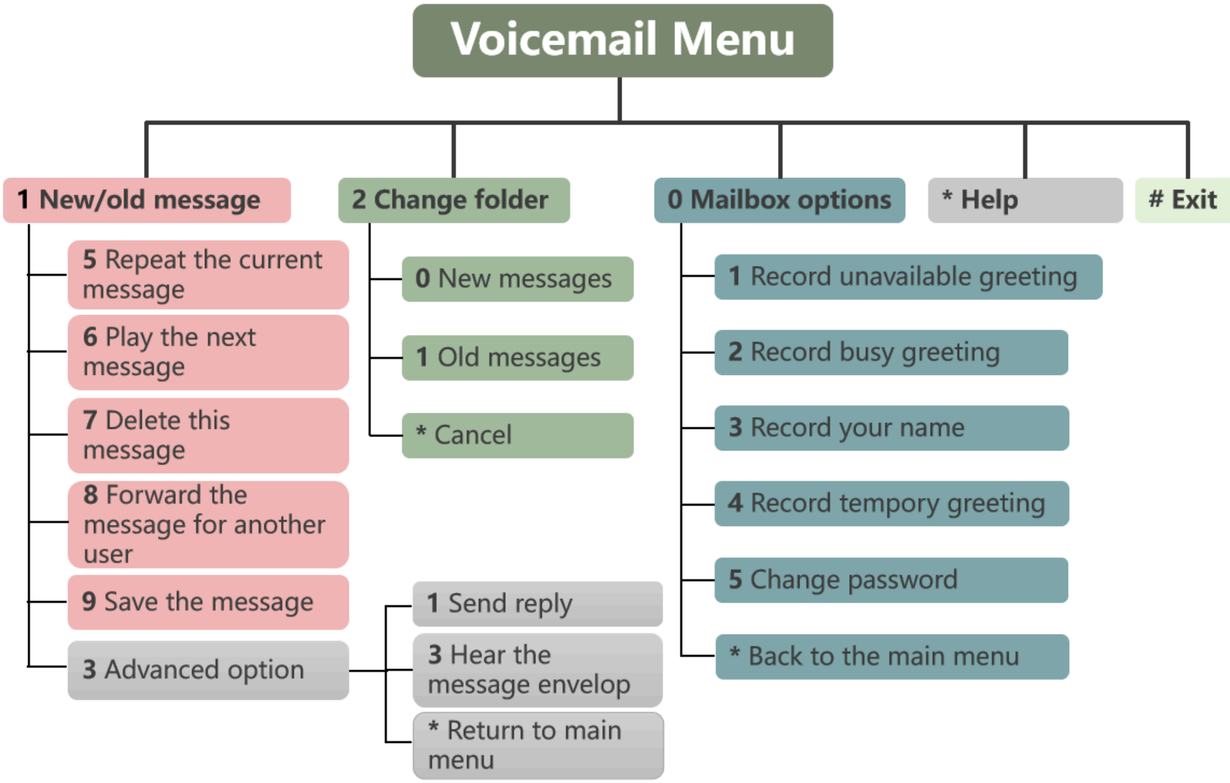
Setting	Description
Message Options	
Max Messages per Folder	Each extension user has a Read voicemail folder and an Un-read folder. You can set the maximum number of messages per folder.
Max Message Time	Set the maximum time of one message.
Min Message Time	Set the minimum time of one message.
Delete Voicemail	This function will work if you enable Send Voicemail to Email. If the voicemail is forwarded to the user's email, PBX will delete voicemails from the user's voicemail folder.
Ask Caller to Dial 5	By default, when the caller accesses a user's voicemail, PBX starts to record message automatically. If you want to prompt the caller first, you can enable this option. The caller needs to dial 5 first, then starts to record message.
Operator Breakout from Voicemail	If enabled, the users can dial `0` to exit from the voicemail destination of an IVR.
Greeting Options	
Busy Prompt	Select the greeting that will be played when the extension is busy. Note: To use a custom prompt, you need to upload your audio file to the Custom Prompt (on page 145) page first.
Unavailable Prompt	Select the greeting that will be played when the extension is unavailable.

Table 1. Global Voicemail settings (continued)

Setting	Description
	Note: To use a custom prompt, you need to upload your audio file to the Custom Prompt (on page 145) page first.
Voicemail Prompt	Select the greeting that will be played before the caller leaves a message. Note: To use a custom prompt, you need to upload your audio file to the Custom Prompt (on page 145) page first.
Playback Options	
Announce Message Caller ID	If enabled, the PBX will announce who left the message.
Announce Message Duration	If enabled, the PBX will announce the message duration.
Announce Message Arrival Time	If enabled, the PBX will announce when the message was received.
Allow Users to Review Messages	If enabled, the users can review their recorded messages, and then send the messages.

Voicemail Menu

You can dial *2 on your phone to access the voicemail menu. Below is the detailed voicemail menu.



Mobility Extension

Yeastar Mobility Extension allows you to stay in contact with colleagues and customers using either office phone or mobile phone with the same extension number.

Scenarios

When you're out of office or on a business trip, the mobility extension allows your mobile phone to have the same permissions as the office phone and frees you from missing any business calls. With mobility extension feature, you can achieve the followings.

- Place free calls to your colleagues.
- Call external numbers using the trunks on the PBX.
- Receive calls using your mobile phone wherever and whenever calls reach your extension number.

Configure Mobility Extension

1. Log in to the PBX web interface, go to Settings > Extensions, click beside the extension that you want to edit.
2. Click Features tab.
3. In the Mobility Extension section, configure as follows:

   a. Select the checkbox of Enable Mobility Extension.
   b. Set the mobile number and prefix.
      - Set Mobile Number: Enter your mobile number to associate your mobile number with extension number.
      - Prefix: Optional. Enter prefix of outbound route (on page 82) so that PBX can successfully route incoming calls to your mobile phone.
   c. Select the checkbox of Ring Simultaneously.

      When a call reaches your office phone, your mobile phone will ring simultaneously.
4. Click Save and Apply.

Use Mobility Extension

After configuring mobility extension, you can use your mobile phone to call in the PBX as follows.

1. Dial a trunk number of the PBX.

   You will hear a voice prompt asking you to dial a phone number that you want to call.
2. Dial an extension number or an external number.
   - Dial an extension number

     The called party will see caller ID "mobile_number <extension_number>".
   - Dial an external number

     The called party will see caller ID "mobile_number".

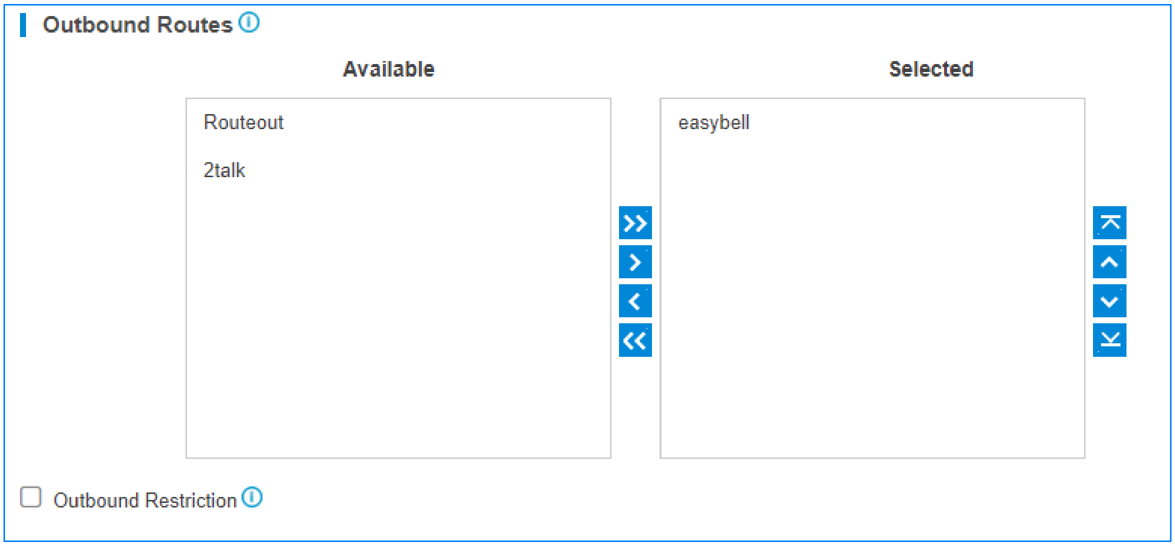
> Note:
> - Make sure the prefix of mobile number matches the dial patterns of outbound route.
> - Make sure at least two trunks are available on PBX. When you use your mobile phone to call in the PBX, the trunk that routes your incoming call to PBX will be occupied, PBX needs another trunk to call the external number out.

Call Permission

Set Outbound Call Permission of an Extension

On the Extension configuration page, you can set the outbound call permissions for the extension user.

1. Go to Settings > PBX > Extensions, click beside the desired extension.
2. On the configuration page, click Call Permission tab.
3. Select outbound routes for the extension from Available box to Selected box.



4. Click Save and Apply.

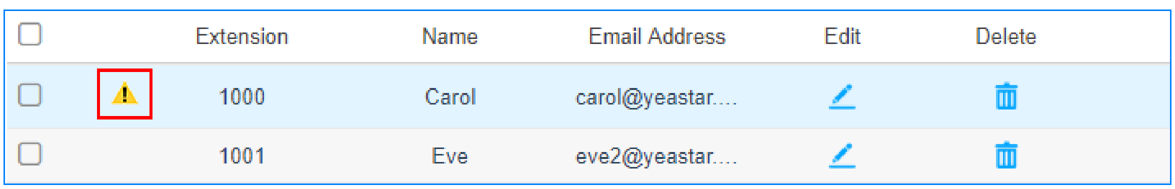
   The extension user can make outbound calls through the selected outbound routes.

Outbound Restriction

- Prohibit Outbound Calls

  Select the checkbox of Outbound Restriction to restrict this extension from making outbound calls.

  On the Extensions page, the extension will be locked and the extension status will show .



- Cancel Restriction for Outbound Calls

  Double click or unselect the checkbox of Outbound Restriction to allow this extension to make outbound calls.

Bar an Extension From Making and Receiving Any Calls

If you want to prohibit an extension from making or receiving calls, you can set up call barring feature of the extension.

Procedure

1. Log in to the PBX web interface, go to Settings > PBX > Extensions, click beside the desired extension.
2. On the configuration page, click Call Permission tab.
3. In the Call Barring section, select the checkbox of Bar Calls.
4. Click Save and Apply.

Result

- The extension(s) can NOT make or receive any calls except emergency calls.
- On the Extension page, the extension status shows .

		Extension	Name	Type	Edit	Delete
		1000	1000	SIP		
		1001	1001	SIP		

Note:
When the call barring feature is enabled, other features related to the extension will also be affected. For example:

- If the extension is set as an IVR destination, the caller will hear a busy tone, which indicates the call transferred to this destination fails.
- If the extension is set as a Queue member or Ring Group member, the extension will be directly ignored.

Set Call Priority for an Extension

In most cases, if the concurrent call limit is reached on the system, users can NOT dial out. To ensure that important calls can be sent out in case of emergency, you can set call priority for extension users.

Scenario

As control over railway traffic increasingly becomes centralised, the distance among traffic controller, traffic driver, and customer service personnel working on board grows. Instead of physically meeting each other at the train stations, they use telephone for communication.

Upon realizing potentially severe incidents, personnel concerned may need to make calls to Operations Control Center (OCC). To ensure that such important calls can be made and answered as soon as possible, you can set up call priority for extensions.

Procedure

1. Log in to the PBX web interface.
2. Enable call priority settings.
    a. Go to Settings > PBX > General > Preferences.
    b. Select the checkbox of Enable Call Priority Settings.
    c. Click Save.
    d. In the pop-up dialog box, click Yes to reboot the PBX server.
3. Set call priority for a specific extension.
    a. Go to Settings > Extensions, click beside the desired extension.
    b. Click Call Permission tab.
    c. In the Call Priority Settings section, select a value from the drop-down list.

    > Note:
    > The supported priority levels are as follows:
    > - 0: Low priority
    > - 1: Medium priority
    > - 2: High priority

    d. Click Save and Apply.

Result

If an extension is trying to make a call when the concurrent call limit is reached on the system, the system will compare the extension's call priority with that of ongoing calls. Whether the call can be made out or not depends on the followings:

- If there are one or more calls of lower call priority, the system will randomly cut off a call, and the extension user can dial out.
- If there is no call of lower call priority, the extension user can NOT dial out.

> Important:
> Emergency call always has the highest priority, which means that whatever call priority an extension is assigned, the user can always make an emergency call.

Extension Settings

SIP Extension Settings

This reference describes all settings on a SIP extension.

Basic Settings

Navigation path: Settings > PBX > Extensions, edit a SIP extension on the Basic tab.

General Settings

Setting	Description
Type	Select SIP.
Extension	Enter the extension number.
Caller ID	If you set the caller ID number, the called party will see this caller ID number when the extension user makes an outgoing call.
Registration Name	The name used to register a SIP extension.
Caller ID name	If you set the caller ID name, the called party will see this caller ID name when the extension user makes an outgoing call.
Concurrent Registrations	Yeastar S1000-P IPPBX supports to register one extension number on multiple phones. When a call reaches the extension number, all phones will ring.
Registration Password	The password is used to register a SIP extension. The password is generated randomly by default.

User Information Settings

Setting	Description
Email	Enter the email address. Extension user can reset his/her login password, receive voice mails, faxes, or PBX notifications via this email address.
User Password	The password is used to log in to the PBX. The password is generated randomly by default.
Prompt Language	The language of voice prompt. The default prompt language is the same as the system language. If the extension user speaks foreign language, you can set a specific system prompt.
Mobile Number	Enter the mobile number. Extension user can receive PBX notifications or forwarded calls on this mobile number.

Features Settings

You can configure voicemail, call forwarding, mobility extension, and other settings under the Features tab.

Navigation path: Settings > PBX > Extensions, edit a SIP extension under the Features tab.

Voicemail Settings

Setting	Description
Enable Voicemail	Enable voicemail feature.
Voicemail Access PIN	Password used to access voicemail.
Share Voicemail Status	Enable this option to share voicemail status with other extensions.
Send Voicemail to Email	Whether to send voicemail to the designated Email address or not. • Disabled: Do not send voicemail to the designated Email address. • Send to user's mail: Send voicemail to the email address of the extension user. • Send to custom mail: Customize an email address, and the PBX will send the voicemail to the designated Email address.
Busy Prompt	Set the prompt that will be played when the extension user is busy in a call.
Unavailable Prompt	Set the prompt that will be played when the extension user is unavailable.

Call Forwarding Settings

You can forward calls to a specific destination or a specific extension user to avoid missing calls.

Setting	Description
Always	Forward all calls to the designated destination.
No Answer	Only forward the unanswered calls to the designated destination.
When Busy	Only forward the calls that come in while you are talking on the phone to the designated destination.

Mobility Extension Settings

Yeastar Mobility Extension allows you to stay in contact with colleagues and customers using either office phone or mobile phone with the same extension number.

Setting	Description
Ring Simultaneously	Enable this option to allow both extension and the associated mobile number ring simultaneously when anyone calls in the extension number.
Enable Mobility Extension	Enable this option to allow your mobile number to have the same permission as the office phone when you use the associated mobile number to call in the PBX.
Mobility Extension	• Set Mobile Number: Set the associated mobile number. • Prefix: Set prefix of the mobile number according to the outbound route.

Manager Extension Settings

Setting	Description
Enable Manager Extension	Enable this option to forward all incoming calls to the secretary extension. Note: • To enable this feature, you must select a secretary extension. • Once enabled, you can directly dial a feature code to disable (default *076) or enable (default *76) this feature. For more information, see Manager and Secretary (on page 119).

Busy Camp-on Settings

Setting	Description
Enable Busy Camp-on	If enabled, the caller can camps the call on PBX when the callee's phone is busy. The PBX informs the caller as soon as the callee's phone becomes available.

Calling Line Identification Service Settings

Setting	Description
Calling Line Identification Presentation	If enabled, the user can see the caller ID number of the caller when receiving an inbound call.

Setting	Description
Calling Line Identification Restriction	If enabled, the extension's caller ID number will be hidden when making an outbound call.

Other Settings

Setting	Description
Ring Timeout (s)	Set the timeout in seconds. Phone will stop ringing after timeout.
Max Call Duration (s)	Set the maximum call duration in seconds for every call of this extension. Note: The precedence of Max Call Duration(s) (Global (on page 174) v.s. Extension): • For internal calls: The Max Call Duration(s) setting of the caller's extension takes precedence. • For outbound calls: The Max Call Duration(s) setting of the caller's extension takes precedence. • For inbound calls: The global Max Call Duration(s) setting takes precedence.
DND	If enabled, the user will NOT receive any calls.
Send email notification when extension user password is changed	Enable this option to send email notification when extension user password is changed.
Call Waiting	If enabled, the user can still receive a call while he/she is already on the line with someone else.

Advanced Settings

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

Navigation path: Settings > PBX > Extensions, edit an extension under the Advanced tab.

VoIP Settings

Setting	Description
NAT	Enable this option when the PBX is using the public IP address. NAT is a process where public IP address is translated into local IP address and vice versa.
Qualify	Enable this option to send SIP OPTION packet to SIP device to check if the device is up.
Register Remotely	Enable or disable the registration of remote extension.
T.38 Support	Enable or disable T.38 fax for the extension.
RTP Encryption (SRTP)	Enable SRTP encryption to ensure the security of voice and data transmission on terminals. • Disabled: Disable SRTP encryption. • Optional: Negotiate the type of encryption and authentication to use for the session with the other terminal. • Compulsory: Enable SRTP encryption for all session with the other terminal.
DTMF Mode	Set the default mode for sending DTMF tones. • RFC4733: 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: The PBX will detect if the device supports RFC4733 DTMF. If RFC4733 is supported, PBX will choose RFC4733, or the PBX will choose Inband.
Transport	Set the transport protocol. • UDP • TCP • TLS

Enable User Agent Registration Authorization Settings

Setting	Description
Enable User Agent Registration Authorization	Whether to restrict user agents from registering to the extension.
User Agent	Enter the name of user agent. If the prefix of the user agent does not match the value, the registration will fail.

IP Restriction Settings

Setting	Description
Enable IP Restriction	This option is used for IP access control. Only the IP address or IP section that matches the settings can register the extension number.
Permitted IP	• If IPv4 network is used, enter the IPv4 address and subnet mask. • If IPv6 network is used, enter the IPv6 address and IPv6 prefix.

Call Permission Settings

You can set the call permissions for the SIP extension.

Navigation path: Settings > PBX > Extensions, edit a SIP extension under the Call Permission tab.

Outbound Routes Settings

Setting	Description
Outbound Routes	Select outbound routes that the extension user is allowed to use.
Outbound Restriction	Enable this option to restrict this extension from making outbound calls.

Call Barring Settings

Setting	Description
Bar calls	If enabled, this extension will not be able to make and receive any calls except emergency calls.

Trunks

Trunk Overview

Making and receiving calls between internal extensions is one thing, but if you want to receive and make calls to the outside world, you need at least a trunk to the outside world.

VoIP Trunks

VoIP Trunks Introduction

VoIP Trunks are phone lines that transmit calls over the Internet. A VoIP provider can assign a local number to one or more cities or countries and route it to the PBX phone system. Usually VoIP trunks are cheaper than traditional PSTN trunks.

VoIP Trunk Types

Yeastar S1000-P IPPBX supports the following VoIP trunk types:

- VoIP Register Trunk: Registration based VoIP trunk. VoIP Register Trunk uses the username and password for registration with SIP providers.
- VoIP Peer Trunk: IP based VoIP trunk. Uses the IP address and port of PBX for authentication.
- VoIP Account Trunk: Account Trunk is designed for connection between Yeastar S1000-P IPPBX and other devices. Yeastar S1000-P IPPBX will act as a VoIP account provider, the other device should register this account to connect to Yeastar S1000-P IPPBX.

Create a VoIP Trunk

Create a VoIP Register Trunk

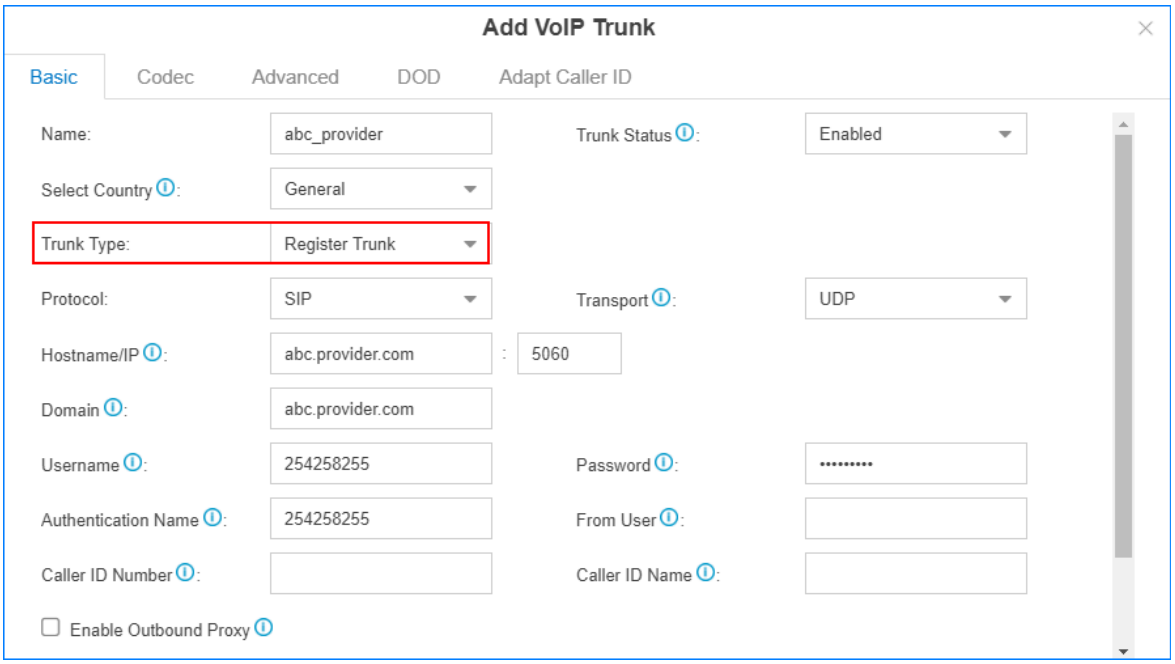
If you have got a VoIP account with user name and password, you can set up a Register Trunk on Yeastar S1000-P IPPBX.

Assume that you bought a SIP trunk from the VoIP provider, and the trunk information is displayed as below. We will introduce how to set up a Register Trunk according to the trunk information.

Provider address	abc.provider.com
Protocol	SIP
SIP Port	5060
Transport	UDP
Username	254258255
Authenticate name	254258255
Password	05JsOmsIS54SYh

Provided DID numbers	5503301 / 5503302 / 5503303

1. Go to Settings > PBX > Trunks, click Add.
2. In the Name field, enter a trunk name.
3. In the Trunk Status drop-down list, select Enabled.
4. In the Select Country drop-down list, select General or your country.
5. In the Trunk Type drop-down list, select Register Trunk.



6. In the Protocol drop-down list, select SIP.
7. In the Transport drop-down list, select the transport provided by the VoIP provider.
8. Enter the trunk information that is provided by the VoIP provider:
    - Hostname/IP: Enter the IP address or the domain of the VoIP provider (e.g.abc-.provider.com).
    - Domain: Enter the IP address or the domain of the VoIP provider (e.g. abc.provider.com).
    - Username: Enter the username to register to the VoIP provider (e.g. 254258255).
    - Password: Enter the password that is associated with the username (e.g. 05Js-OmsIS54SYh).
    - Authentication Name: Enter the authentication name to register to the VoIP provider (e.g. 254258255).
    - From User: Enter the same name as Username (e.g. 254258255).
9. If the trunk DID number is different from the trunk authentication name, you need to set the DID number.
    a. Click Advanced tab, enter the DID Number which is provided by the VoIP provider (e.g. 5503301).
    b. Optional: Select the checkbox of DNIS Name, enter a DNIS name for the DID number.

When users call the DID number, the DNIS name will be displayed on ringing phone.

c. Optional: Click ⊞ to add other DID numbers.

10. Optional: Configure other VoIP trunk settings (on page 44) as your need.
11. Click Save and Apply.

    You can check the trunk status in PBX Monitor. If the trunk status shows ✔, the trunk is ready for use.

Related information
Add an Outbound Route (on page 83)
Add an Inbound Route (on page 64)
Set up DOD Numbers for VoIP Trunk (on page)

Create a VoIP Peer Trunk

If your ITSP only provides an IP address or domain for your purchased VoIP account, you can set up a Peer Trunk on the Yeastar S1000-P IPPBX.

Assume that you bought a SIP trunk from the ITSP, and the trunk information is displayed as below. We will introduce how to set up a Peer Trunk according to the trunk information.

Provider address	peer.sip.com
Protocol	SIP
SIP Port	5060
Transport	UDP

1. Go to Settings > PBX > Trunks, click Add.
2. In the Name field, enter a trunk name.
3. In the Trunk Status drop-down list, select Enabled.
4. In the Select Country drop-down list, select General or your country.
5. In the Trunk Type drop-down list, select Peer Trunk.
6. In the Protocol drop-down list, select SIP.
7. In the Transport drop-down list, select the transport provided by the VoIP provider.
8. Enter the trunk information that is provided by the VoIP provider.
    - Hostname/IP: Enter the IP address or the domain of the VoIP provider (e.g.peer-.sip.com).
    - Domain: Enter the IP address or the domain of the VoIP provider (e.g. peer.sip.com).
9. Optional: Configure other VoIP trunk settings (on page 44) as your need.
10. Click Save and Apply.

    You can check the trunk status in PBX Monitor. If the trunk status shows ✔, the trunk is ready for use.

Related information
Add an Outbound Route (on page 83)
Add an Inbound Route (on page 64)
Set up DOD Numbers for VoIP Trunk (on page)

Create a VoIP Account Trunk

Create a VoIP Account Trunk on the Yeastar S1000-P IPPBX, and provide this account for the other device to register. In this way, Yeastar S1000-P IPPBX and the other device are connected.

1. Go to Settings > PBX > Trunks, click Add.
2. In the Name field, enter a trunk name.
3. In the Trunk Status drop-down list, select Enabled.
4. In the Trunk Type drop-down list, select Account Trunk.
5. In the Protocol drop-down list, select SIP.
6. In the Transport drop-down list, select the transport provided by the VoIP provider.
7. Enter the account information as your need:
    - Username: Use the default or change the number.
    - Password: Use the default or change the number.
    - Authentication Name: Use the default or change the number.

    > Note:
    > The other device should use the provided trunk information to connect to the Yeastar S1000-P IPPBX.
8. Optional: Configure other VoIP trunk settings (on page 44) as your need.
9. Click Save and Apply.

    After the Account Trunk is registered on the other device, you can check the trunk status in PBX Monitor. If the trunk status shows ✔, the trunk is ready for use.

Related information
Add an Outbound Route (on page 83)
Add an Inbound Route (on page 64)

Manage VoIP Trunks

Import the VoIP register Trunks

You can create multiple VoIP register trunks by importing a UTF-8 `.csv` file.

For requirements of the import parameters, see Import Parameters - Trunks (on page).

1. Go to Settings > PBX > Trunks, click Import.
2. Click Download the Template, add the VoIP register trunks information in the template file.
3. Click Browse to upload the template file, and then click Import.

Edit the VoIP Trunk

1. Go to Settings > PBX > Trunks.
2. Search and find your VoIP Trunk, click .
3. Click the desired tab to edit the VoIP Trunk Settings (on page 44) as your need.
4. Click Save and Apply.

Delete the VoIP Trunk

1. Go to Settings > PBX > Trunks.
2. Search and find your VoIP Trunk, click .
3. Click Yes to confirm the deletion.

VoIP Trunk Settings

When you configure a VoIP trunk, you may need to configure some of the advanced settings. This reference describes all the settings on a VoIP trunk.

Basic Settings

Navigation path: Settings > PBX > Trunks, edit a trunk on the Basic tab.

Settings	Description
Name	Give this trunk a name to help you identify it.
Trunk Status	Enable or disable the trunk.
Select Country	Select the country that the VoIP provider operates in.
Trunk Type	Select a trunk type.
Protocol	Select the protocol that is provided by the VoIP provider.
Transport	Select the transport that is provided by the VoIP provider.
Hostname/IP	Enter the IP address or the domain of the VoIP provider.
Domain	Enter the IP address or the domain of the VoIP provider.
Username	Enter the username to register to the VoIP provider.
Authentication Name	Enter the authentication name to register to the VoIP provider.

Settings	Description
Password	Enter the password that is associated with the username.
From User	Enter a name. All the outgoing calls from this trunk will use this name in From header of the SIP invite package.
Caller ID Number	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. This feature requires support from the VoIP provider.
Caller ID Name	If you set the caller ID name, when users make outbound calls through this trunk, the called party will see this caller ID name instead of the calling party's name. This feature requires support from the VoIP provider.
Enable Outbound Proxy	Set the outbound proxy if the VoIP provider needs.
Enable SLA	After enabling SLA (on page 94), users can share this trunk to make outbound calls and receive inbound calls by BLF keys on their phones. In this way, Inbound Route settings and Outbound Route settings for the trunk is invalid.

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 VoIP trunk page. However, for a few fields, you need to change them to suit your situation.

Navigation path: Settings > PBX > Trunks, edit a trunk on the Advanced tab.

VoIP Settings

Settings	Description
RTP Encryption(SRTP)	Enable SRTP encryption to ensure the security of voice and data transmission on terminals. • Disabled: Disable SRTP encryption. • Optional: Negotiate the type of encryption and authentication to use for the session with the other terminal. • Compulsory: Enable SRTP encryption for all session with the other terminal.

Settings	Description
Qualify	Enable this option to send SIP OPTION packet to SIP device to check if the device is up.
DTMF Mode	Set the default mode for sending DTMF tones. • RFC4733 (RFC2833): DTMF will be carried in the RTP stream in different RTP packets 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). If RFC4733(RFC2833) is supported, PBX will choose RFC4733(RFC2833), or the PBX will choose Inband.
Send Privacy ID	Whether to send the Privacy ID in SIP header or not.
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.
User Phone	Whether to add the parameter `user=phone` in the SIP INVITE packet. Note: Enable this option if the SIP provider requires.

DID Settings

Settings	Description
DID Number	Direct Inward Dialing (DID) number, can be used to distinguish incoming calls. Note: For Register Trunk, if the trunk DID number is different from the trunk authentication name, you need to enter the DID number.
DNIS Name	Dialed Number Identification Service (DNIS) is a telephony service, used to identify which number was dialed.

Settings	Description
	Bind a DNIS name for a DID number, when users call the DID number, the DNIS name will be displayed on ringing phone.

Inbound Parameters

Settings	Description
Get DID From	Decide from which header field will the trunk retrieve DID header. • [Follow System] The trunk will follow the global Get DID From (on page 182) setting. • To • Invite • 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 • Diversion • P-Called-Party-ID • P-Preferred-Identity
Get Caller ID From	Decide from which header field will the trunk retrieve Caller ID header. • [Follow System] The trunk will follow the global Get Caller ID From (on page 182) setting. • From • Contact • Remote-Party-ID • P-Asserted-Identify • P-Preferred-Identity

Outbound Parameters

Configure SIP parameters for outbound calls.

- Default: The same as the value in "From".
- Trunk Username: The username you configured for the trunk.
- Extension Number: The extension number.
- DOD Number: The DOD number that you configured to associate with the extension. If the extension doesn't have an associated DOD number, the Caller ID Number of the trunk will be taken instead.
- From User: The From User value that you configured for the trunk.
- None: Do not send the parameter with the SIP INVITE packet.

Settings	Description
Remote Party ID	Select which Remote Party ID value should be contained in the SIP INVITE headers when making an outbound call.
P Asserted Identity	Select which P Asserted Identity value should be contained in the SIP INVITE headers when making an outbound call.
Diversion	Select which Diversion value should be contained in the SIP INVITE headers when making an outbound call.
P Preferred-Identity	Select which P Preferred Identity value should be contained in the SIP INVITE headers when making an outbound call.

Transfer Parameters

Configure the SIP parameters for transferred calls.

- Default: The same as the value in "From".
- Trunk Username: The username you configured for the trunk.
- Extension Number: The extension number.
- DOD Number: The DOD number that you configured to associate with the extension. If the extension doesn't have an associated DOD number, the Caller ID Number of the trunk will be taken instead.
- The Originator Caller ID: The Caller ID Number of the first caller in cases that the call is transferred.
- From User: The From User value that you configured for the trunk.
- None: Do not send Remote Party ID with the SIP INVITE packet.

Settings	Description
From	Select which From value should be contained in the SIP INVITE headers when the call is transferred.

Settings	Description
Diversion	Select which Diversion value should be contained in the SIP INVITE headers when the call is transferred.
Remote Party ID	Select which Remote Party ID value should be contained in the SIP INVITE headers when the call is transferred.
P Asserted Identity	Select which P Asserted Identity value should be contained in the SIP INVITE headers when the call is transferred.
P Preferred Identity	Select which P Preferred Identity value should be contained in the SIP INVITE headers when the call is transferred.

Other Settings

Settings	Description
Maximum Channels	Set the maximum number of concurrent calls on the trunk. Note: The value `0` means unlimited.
Realm	SIP Realms, also known as domains within SIP networks. Realm is a component within SIP that is used to authenticate users within the SIP registration process. Note: By default, the Realm setting is unnecessary. Contact your service provider if you want to configure Realm.
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.

Settings	Description
	• 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.

Codec Settings

Each new created VoIP trunk has a default preferred codec list. However, the default codec list may not match the codecs supported by your VoIP provider. In order to maximize the quality of calls and the amount of bandwidth used for calls, you'll want to choose and configure your preferred codec list to match the settings that your VoIP provider supports.

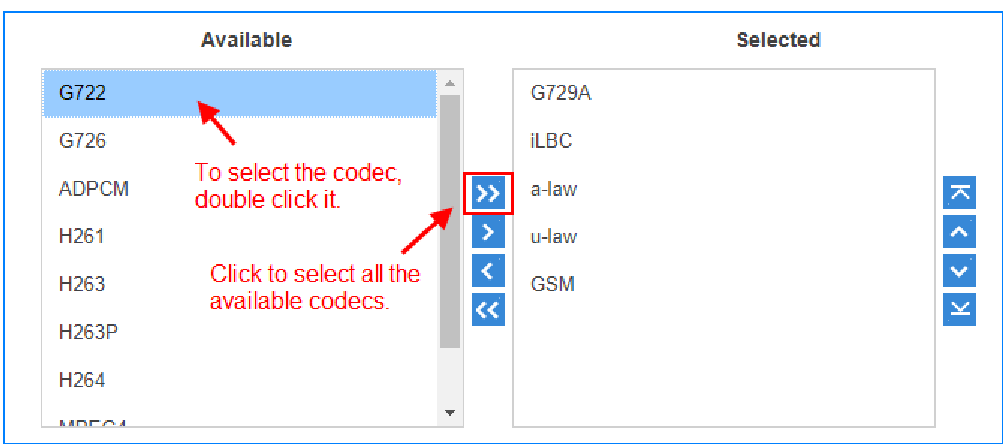
Yeastar S1000-P IPPBX supports the following codecs:

Disabled by default	Enabled by default
GSM, SPEEX, G722, G726, ADPCM, H261, H263, H263P, H264, MPEG4, iL-BC, opus	G729A, a-law, u-law

Navigation path: Settings > PBX > Trunks, edit a trunk on the Codec tab.

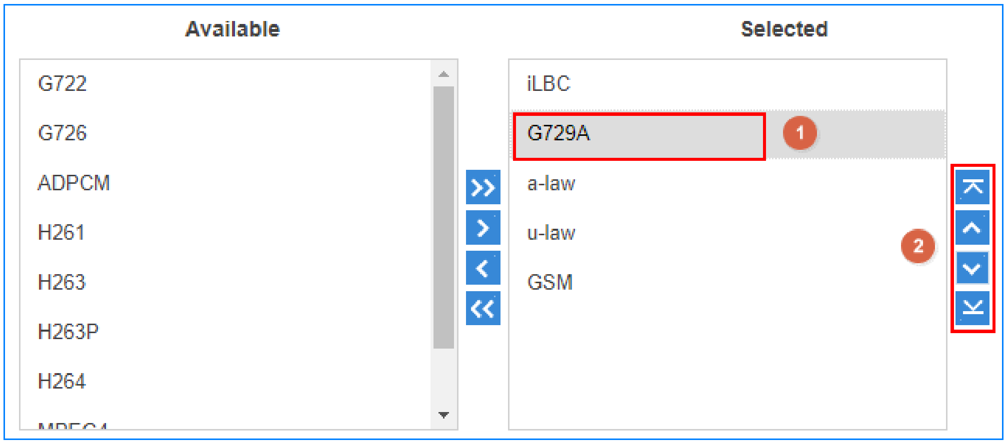
Select Codec

In the Available box, double click a codec, the selected codec will appear in the Selected box.



Set the Codec Priority

In the Selected box, click a codec, and click to change the priority.



Adapt Caller ID

The incoming caller ID that matches the adaptation pattern will be adapted, so that you can press the call record directly on your phone to call back a number.

For more information, see Change Inbound Caller ID (on page 67).

Navigation path: Settings > PBX > Trunks, edit a trunk on the Adapt Caller ID tab.

Settings	Description
Patterns	The following characters have special meanings: • X matches the numbers 0-9; • Z matches the numbers 1-9; • N matches the numbers 2-9; • [12345-9] matches the numbers in the bracket (in this example, 1, 2, 3, 4, 5, 6, 7, 8, 9); • Wildcard matches one or more numbers. E.g. "9011." matches anything starting with 9011 (excluding 9011 itself); • Wildcard "!" matches none or more than one numbers. E.g. "9011!" matches anything starting with 9011 (including 9011 itself);
Strip	Strip allows you to specify the number of digits that will be stripped from the front of the Caller ID before the call is displayed. For example, if the incoming Caller ID is 05929999999, but you need to dial number 5929999999 to call back, one digit should be stripped.
Prepend	These digits will be prepended to the Caller ID before the call is displayed. For example, if the incoming caller ID is 5929999999, but you need to dial digit 0 before the number to call back, 0 should be prepended.

Call Control

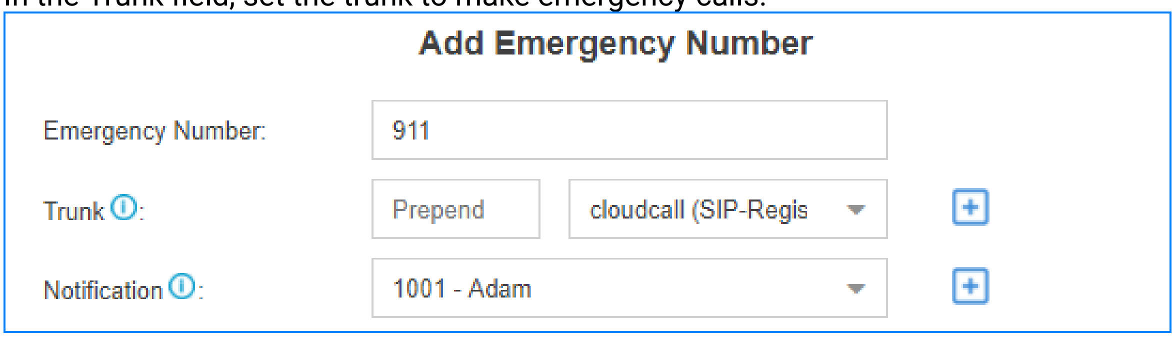
Emergency Numbers

Add an Emergency Number

To ensure that the extension users can make emergency calls at any time, you need to add emergency numbers on Yeastar S1000-P IPPBX. You can also set an alert to notify the emergency contacts that an emergency call has been dialed.

> Note:
> Emergency calls have the highest priority. If the trunk used to make emergency calls is busy, the PBX will terminate the ongoing call, and place the emergency call.

1. Go to Settings > PBX > Emergency Number, click Add.
2. In the Emergency Number field, enter the emergency number.
3. In the Trunk field, set the trunk to make emergency calls.



    a. In the drop-down list, select a trunk.

    b. Optional: If the selected trunk needs a prepended number before the emergency number, enter a prepended number in the Prepend field.
    For example, if your trunk needs a prepended number 0 before the emergency number 911, users should dial 0911 to make the emergency call. To comply with the user's dialing habit, you can set the Prepend as `0`. In this way, users can dial 911 as they usually do.

    c. Optional: Click ⊞ to add another trunk.

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

4. In the Notification drop-down list, select the notification contact.

If someone makes emergency calls through the PBX, the contacts will receive notification calls on their extensions.
   a. In the drop-down list, select a contact.
   b. Optional: Click to add another contact.
5. Click Save and Apply.

Manage Emergency Numbers

After you add emergency numbers, you can edit or delete them.

Edit an emergency number

1. Go to Settings > PBX > 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. Go to Settings > PBX > Emergency Number, click beside the emergency number that you want to delete.
2. In the pop-up window, click Yes to delete the selected emergency number.
3. Click Apply.

Time Conditions

Time Conditions Overview

A Time Condition is a time group, which can be applied to outbound routes and inbound routes. You can use Time Condition to control calls based on date and time.

What is a Time Condition used for?

A Time Condition contains a time group.

- Apply Time Condition to an Inbound Route

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

  You can select a Time Condition and set a corresponding destination for an inbound route. When a call reaches the PBX, PBX will route the call to the destination when the current system time matches the time defined in the Time Condition.

- Apply Time Condition to an Outbound Route

  You can also apply Time Condition to an outbound route to limit when the users can use the outbound route.

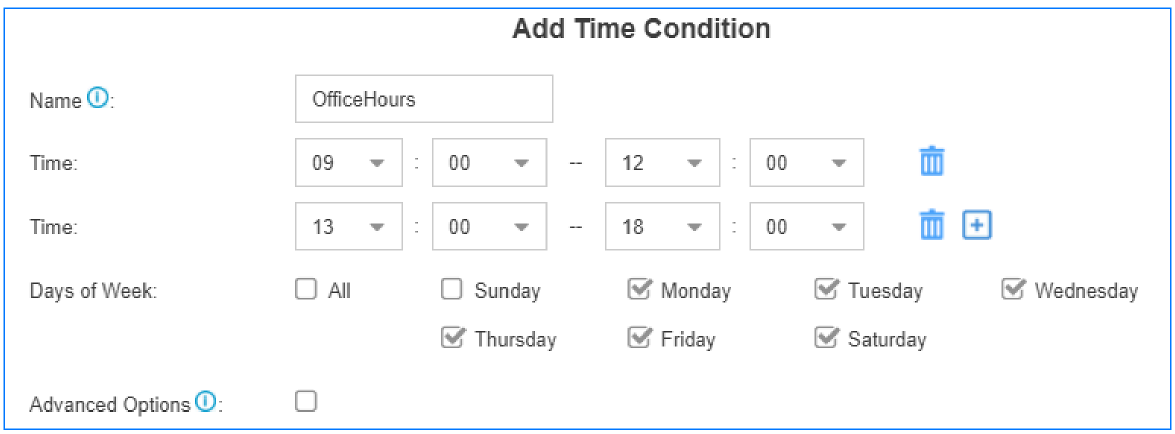
Set Time Conditions

A Time Condition is a time group, which can be applied to outbound routes and inbound routes. This topic describes how to set office hours, non-office hours, and holidays on Yeastar S1000-P IPPBX.

Set office hours

Add a Time Condition according to your office hours. Apply this Time Condition to inbound routes to route incoming calls during office hours to the corresponding destination.

1. Go to Settings > PBX > Call Control > Time Conditions > Time Conditions, click Add.
2. In the Name field, enter a name to help you identify it.
3. In the Time field, set the time according to your office time.
4. Click to add another time period.
5. In the Days of Week field, select your office days.



6. Optional: If you want to apply the time period(s) to specific dates, select the checkbox of Advanced Options, and set the month and the days of month.

> Note:
> Advanced Options is disabled by default, which means that the time period(s) will be applied throughout the year.

7. Click Save and Apply.

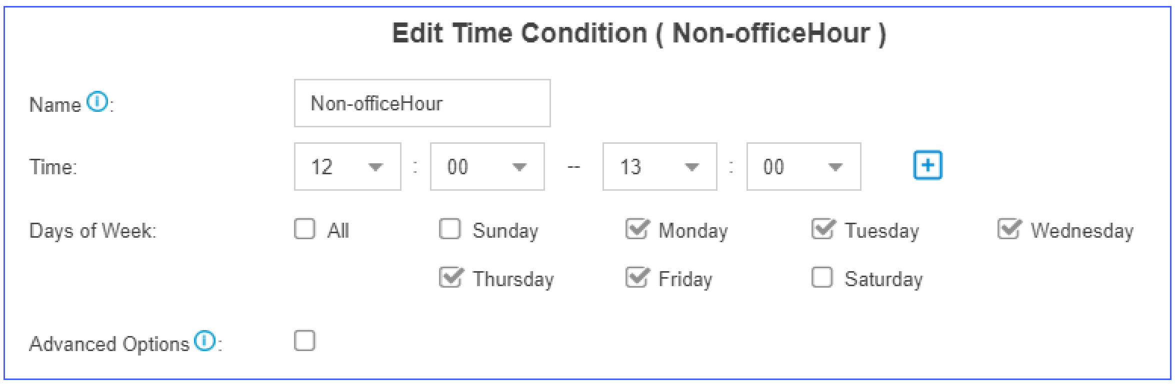
Set non-office hours

PBX has a default Time Condition - Other Time. Generally, when you're configuring an inbound route, you can set one destination for office hours, and set the other destination for Other Time.

However, you may need to add another Time Condition to route incoming calls to other destinations due to company's schedule. For example, you want all incoming calls during lunch break to be routed to the receptionist. In this way, employees can enjoy nap time without missing any important calls.

In this case, you can add another Time Condition for non-office hours.

1. Go to Settings > PBX > Call Control > Time Conditions > Time Conditions, click Add.
2. In the Name field, enter a name to help you identify it.
3. In the Time field, set the time according to your non-office time.
4. Optional: Click to add another time period.
5. In the Days of Week field, select your office days.



6. Optional: If you want to apply the time period(s) to specific dates, select the checkbox of Advanced Options, and set the month and the days of month.

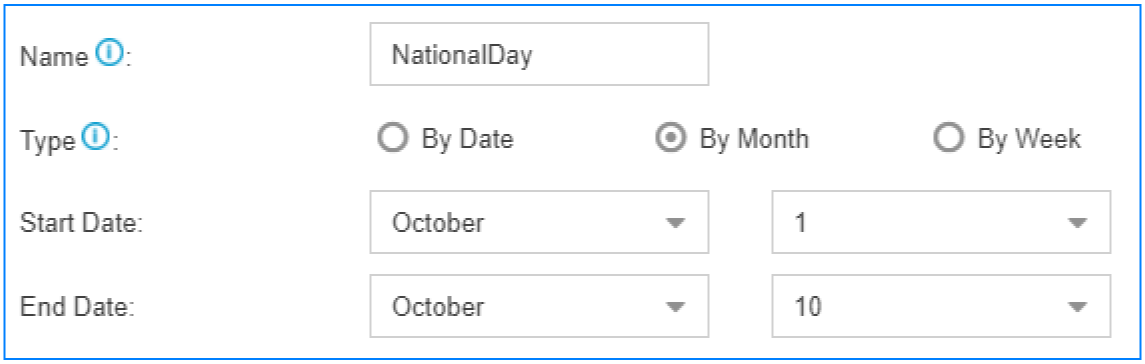
> Note:
> Advanced Options is disabled by default, which means that the time period(s) will be applied throughout the year.

7. Click Save and Apply.

Set holidays

You can add a group of holidays and set a Time Condition destination like an IVR for the holidays on your inbound route. When a customer calls to your company during holidays, the PBX will route the call to the IVR and inform your customers that you are on vacation.

1. Go to Settings > PBX > Call Control > Time Conditions > Holiday, click Add.
2. In the Name field, enter a name to help you identify it.
3. In the Type field, select a type.



- By Date: If the holiday varies every year, select this type.
- By Month: If the holiday always falls on the same calendar date, select this type.
- By Week: If the holiday always falls on the same week, select this type.

4. In the Start Date field, select the start date of the holiday.
5. In the End Date field, select the end date of the holiday.
6. Click Save and Apply.

Manage Time Conditions

After you create Time Conditions, you can apply them to inbound routes or outbound routes. You can also edit or delete the Time Conditions.

Apply a Time Condition to an Inbound Route

You can apply a Time Condition to an inbound route to route inbound calls to different destinations according to your business hours and schedule.

1. Go to Settings > PBX > Call Control > Inbound Routes, click beside the inbound route that you want to edit.
2. On the Inbound Route page, select the checkbox of Enable Time Condition.
3. Click , and select a Time Condition from the drop-down list.
4. Select destination from the drop-down list.

   Inbound calls will be routed to the pre-configured destination if the date and time of the calls match the time condition.
5. Click Save and Apply.

Apply a Time Condition to an Outbound Route

You can apply a Time Condition to an outbound route to limit when the extension users can make outbound calls.

1. Go to Settings > PBX > Call Control > Outbound Routes, click beside the outbound route that you want to edit.
2. On the Outbound Routes page, select the Time Condition which will be applied to the outbound route.

Only in this time period can extension users make outbound calls via this outbound route.

3. Click Save and Apply.

Edit a Time Condition

1. Go to Settings > PBX > Call Control > Time Conditions, click beside the Time Condition that you want to edit.
2. Change Time Condition settings according to your needs.
3. Click Save and Apply.

Delete a Time Condition

1. Go to Settings > PBX > Call Control > Time Conditions, click beside the Time Condition that you want to delete.
2. On the pop-up window, click Yes and Apply.

   After deleting a Time Condition, related configurations of the Time Condition in both inbound routes and outbound routes will be deleted automatically.

Time Condition Examples

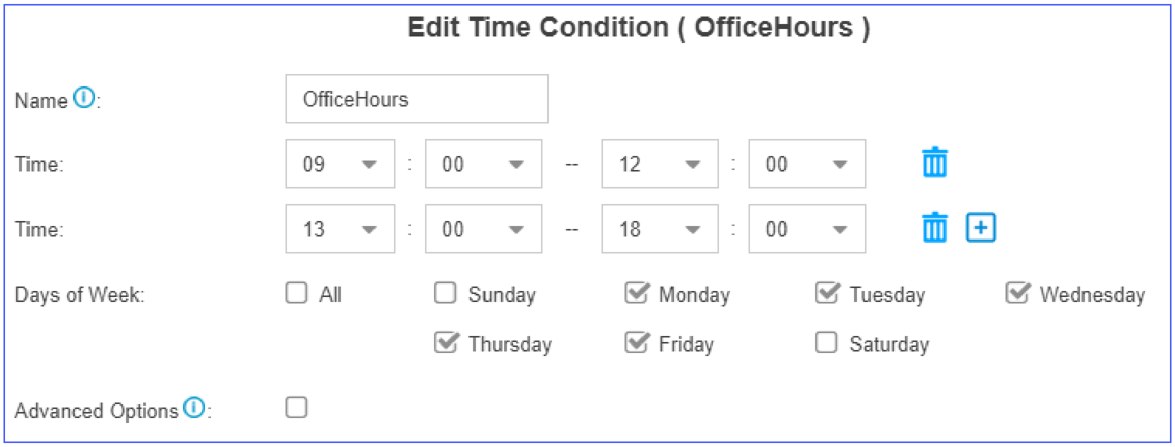
In this topic, we offer you configuration examples of Time Conditions to help you understand how to set office hours, non-office hours, holidays and apply these Time Conditions to inbound routes and outbound routes.

Office hours & non-office hours example

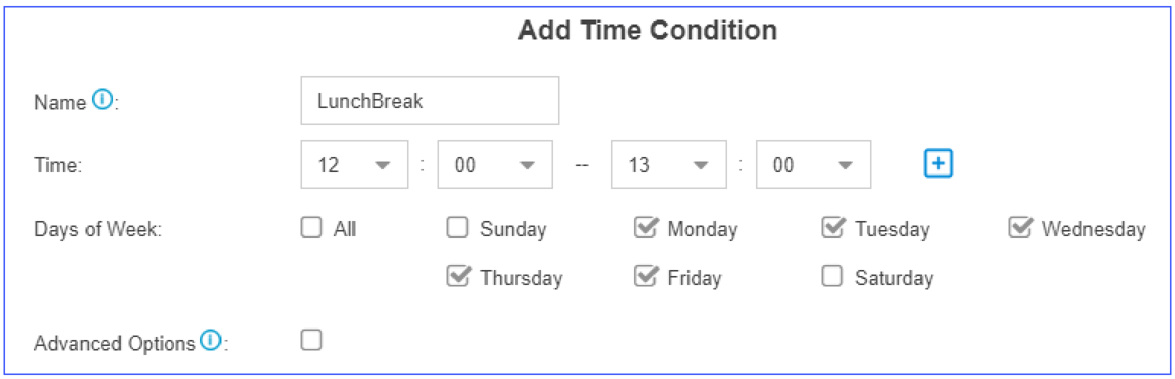
Assume that your office hours are Monday - Friday from 9:00 to 18:00, and the lunch break starts from 12:00 to 13:00.

According to your office hours, you can set two Time Conditions as follows..

- Office hours



- Lunch break



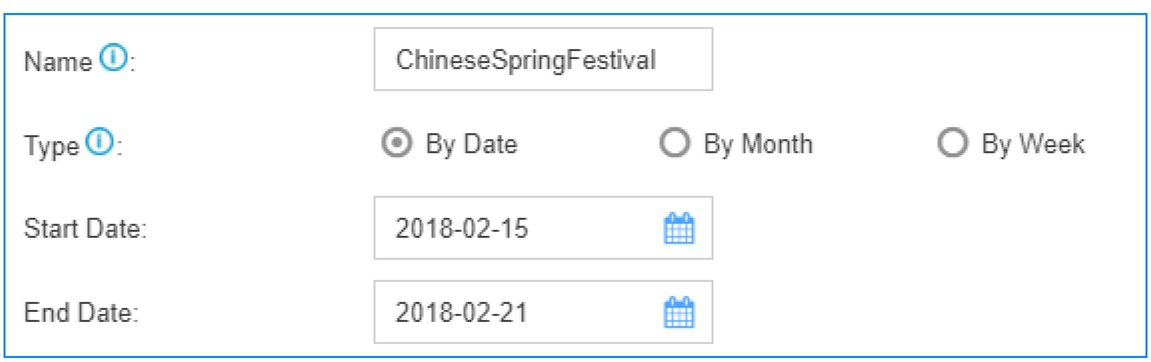
Holiday examples

Yeastar S1000-P IPPBX supports 3 types of holidays.

- Set a Holiday by Date

  If date of a holiday varies every year, you can set a holiday by date.

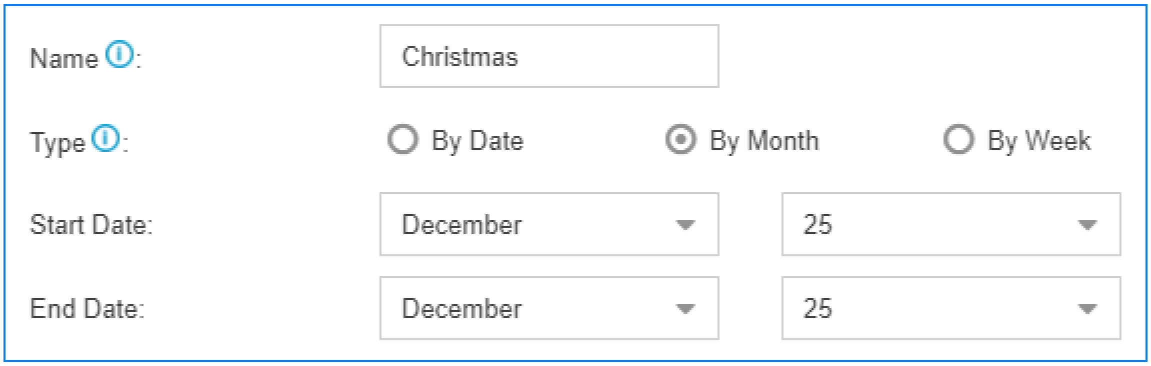
  For example, Chinese Spring Festival falls on February 15th-21st. You can set the holiday as follows.



- Set a Holiday by Month

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

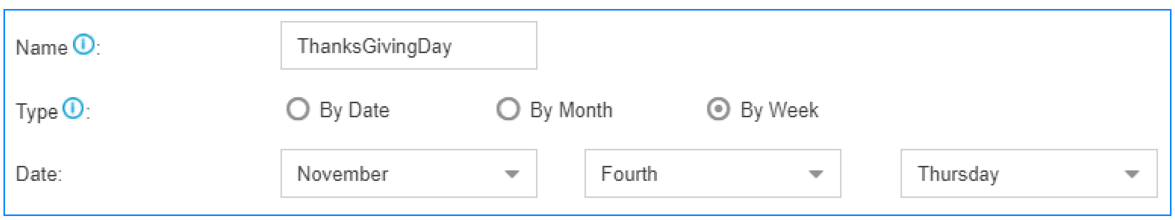
  For example, Christmas falls on December 25th every year. You can set the holiday as follows.



- Set a Holiday by Week

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

  For example, Thanksgiving Day falls on the 4th week of November. You can set the holiday as follows.



Route inbound calls based on Time Conditions

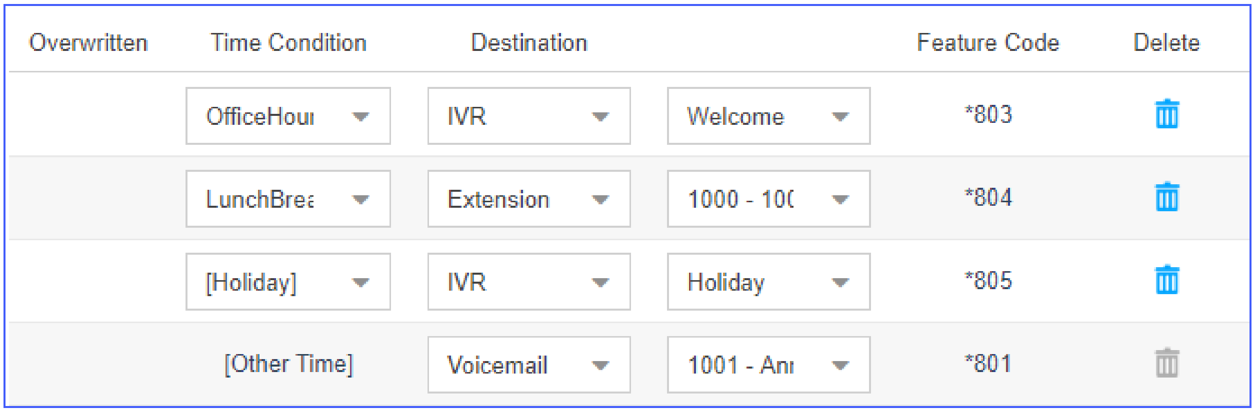
On Inbound Route page, enable Enable Time Condition, click + to add Time Conditions, and set corresponding destinations.

For example, the following table is a schedule of Time Conditions for a company.

Time Condition	Destination
Office hours	IVR
Lunch break	Extension 1000
Holiday	Holiday IVR
Other time	Voicemail

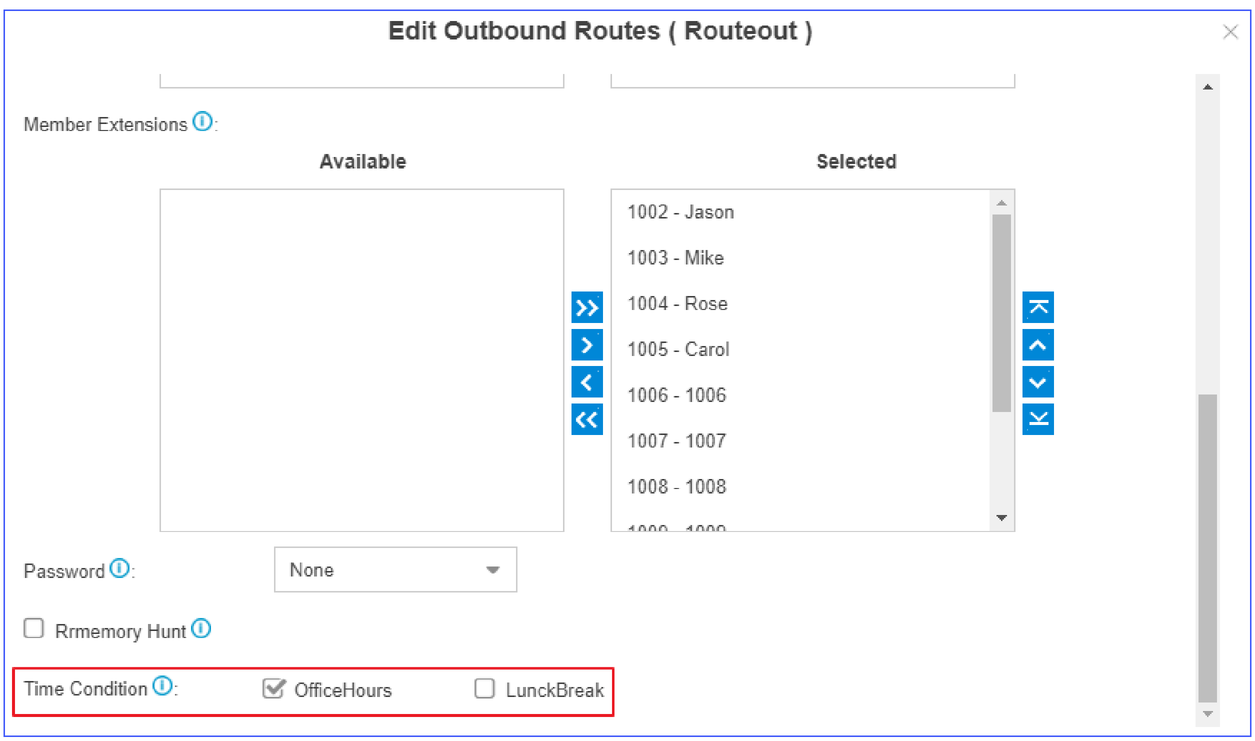
> **Note:**
> All holidays will be integrated into one Holiday, you don't have to select holidays one by one from Time Condition on inbound routes.

You can set Time Conditions as follows.



Restrict when to make outbound calls

On Outbound Routes page, select Time Condition, which means that only in this time period can extension users make outbound calls via this outbound route.



Time Condition Override

The Time Condition Override function is used to switch the inbound call routing against the Time Condition. An authorised user can dial Time Condition feature code to override the time condition.

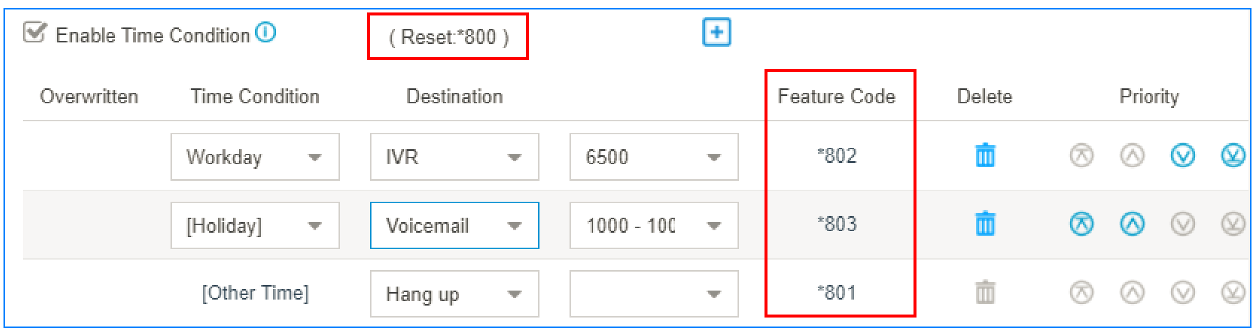
Scenarios

Company A sets day time condition and night time condition in an inbound route with different destinations.

The staffs occasionally leave early or someone needs to enable the night time condition manually. In this scenario, the staffs can dial override feature code to override the time condition.

Time Condition feature code

When you enable and add Time Condition on an inbound route, you will see the default generated feature code for the Time Condition. If you want to disable Time Condition Override, dial the Reset feature code *800.

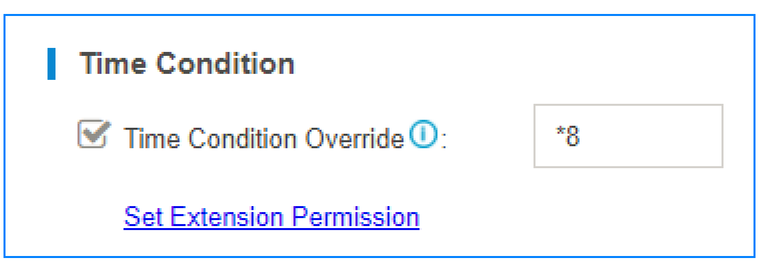


You can go to Settings > PBX > General > Feature Code > Time Condition to change the feature code prefix.

Set extension permission to override Time Condition

By default, users have no permission to override Time Condition. You can set which extension users can override Time Condition.

1. Go to Settings > PBX > General > Feature Code > Time Condition, click Set Extension Permission.



2. Select the desired extensions from Available box to Selected box.
3. Click Save and Apply.

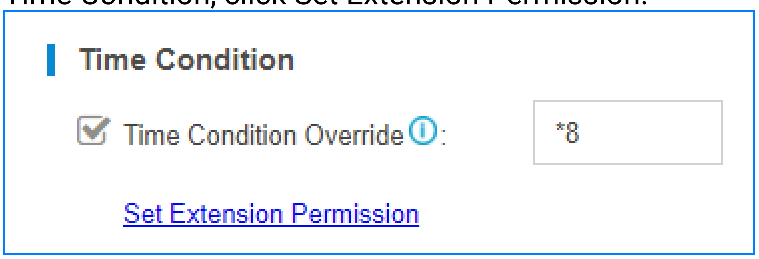
Monitor Time Condition State

You can set a BLF key on your phone to quickly override Time Condition and monitor the Time Condition state.

We take Yealink T53W v95.0.0.0.0.0.1 as an example to explain how to set BLF keys to monitor Time Condition state.

1. Set Time Condition Override permission for the extension that is registered on the IP phone.

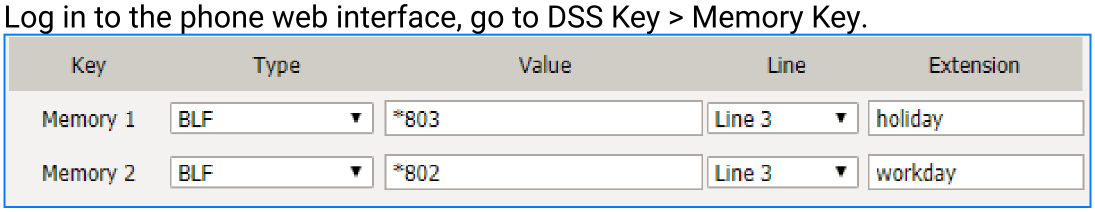
    a. Log in to PBX web interface, go to Settings > PBX > General > Feature Code > Time Condition, click Set Extension Permission.

    b. Select the desired extension from Available box to Selected box.

    c. Click Save and Apply.
2. Set BLF keys on the phone where the extension is registered.

    a. Log in to the phone web interface, go to DSS Key > Memory Key.

    b. Set Key Type as BLF.

    c. Set Key Value as feature code of Time Condition.

    d. Select the Line as the extension registered line.

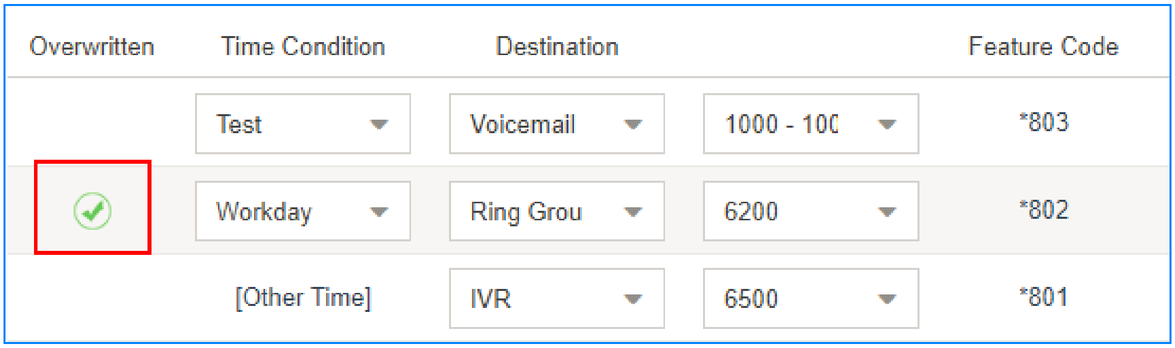
    e. Optional: In the Extension field, enter a description of the key.

    f. Click Confirm.

    The BLF LED will show the Time Condition state.

   - Red: The PBX is using this Time Condition; inbound calls go to the destination of the Time Condition.
   - Green: This Time Condition is not in use.
3. Press a BLF key to override Time Condition, the BLF LED turns to red.

   You can also log in to the PBX web interface, and check the Time Condition state on configuration page of Inbound Routes. If the state shows , it indicates that the PBX is using the Time Condition, and route all incoming calls to destination of the Time Condition.



Inbound Routes

Inbound Route Overview

An inbound route is used to tell the PBX where to route inbound calls based on the caller's phone number or the DID number. Inbound routes are often used in conjunction with time conditions and an IVR.

DID routing & Caller ID routing

Yeastar S1000-P IPPBX allows two specific types of inbound routing: DID Routing and Caller ID Routing. You can set both DID routing and Caller ID routing for an inbound route, or set one of the routing types.

If you don't specify DID numbers and Caller ID numbers on the inbound route, the inbound route will match and route all inbound calls to a pre-configured internal destination on the PBX.

Inbound routes can send inbound calls to destinations as follows:

- Hang up

- Extension
- Extension Range
- Voicemail
- IVR
- Ring Group
- Queue

- Conference
- External Number
- DISA
- Callback
- Outbound Route
- Fax to Email

Add an Inbound Route

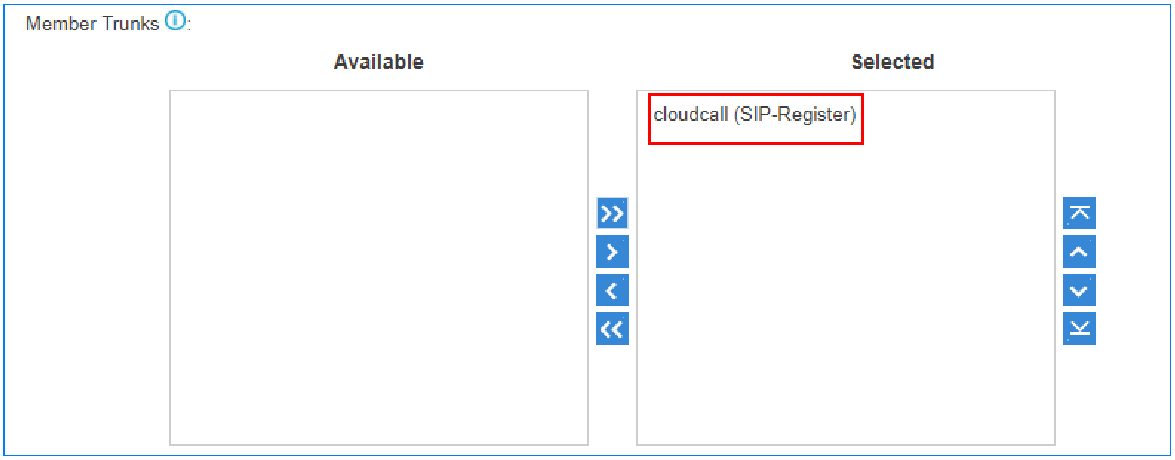
To receive external calls on Yeastar S1000-P IPPBX, you need to set up at least one inbound route.

The PBX has a default inbound route. When users call to the selected trunk, the PBX will route the call to an IVR. You can delete the default inbound route, then add a new one to configure settings according to your needs.

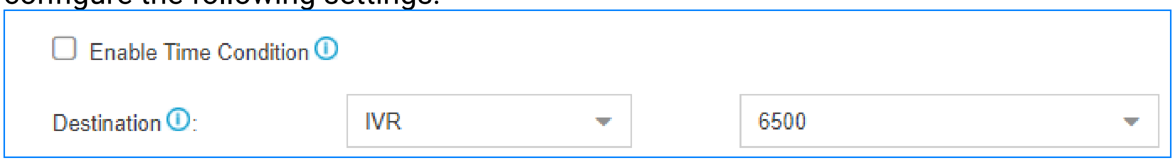
1. Go to Settings > PBX > Call Control > Inbound Routes, click Add.
2. In the Name field, enter a name to help you identify it.
3. Optional: In the DID Pattern field, enter a DID number or a DID pattern if you want to route inbound calls based on DID numbers.
   The PBX will route the call only when the caller dials the matched numbers.

   > Note:
   > Leave this blank to match calls with any or no DID info.
4. Optional: In the Caller ID Pattern field, enter a Caller ID or a Caller ID pattern if you want to route inbound calls based on Caller IDs.
   The PBX will route the call only when the caller ID number matches the Caller ID Pattern.

   > Note:
   > Leave this blank to match calls with any or no caller ID info.
5. In the Member Trunks field, select the desired trunk from Available box to the Selected box.
   The PBX will route the inbound call when the caller calls the number of the selected trunk.

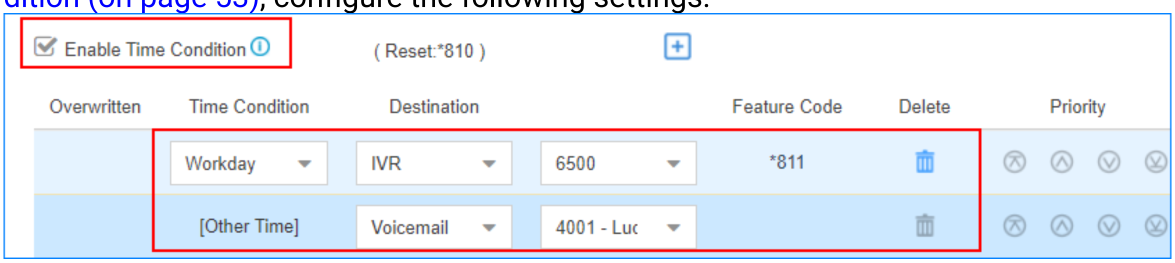


6. If you allow the inbound calls to be routed to a desired destination without time limit, configure the following settings:



    a. Uncheck the checkbox of Enable Time Condition.
    b. Select the Destination.

7. If you allow the inbound calls to be routed to different destinations based on time condition (on page 53), configure the following settings:



    a. Select the checkbox of Enable Time Condition.

    b. Click [+], select a Time Condition and the destination.

    If an inbound call reaches the PBX during the time period, PBX will route the call to the selected destination.

    c. Optional: Click [+] to set another time condition and destination.

    d. Set the destination for Other Time.

    If an inbound call reaches the PBX beyond the time periods that are defined in the above Time Conditions, PBX will route the call to the selected destination.

8. Optional: In the Distinctive Ringtone field, enter the ringtone name. Distinctive Ringtone (on page 78) helps users recognize where the call is from.

> Note:
> Distinctive Ringtone feature needs support from the IP phones.

For example, the IP phone has a ringtone called "Family". You can enter "Family" in the Distinctive Ringtone field. When a call reaches the IP phone through this inbound route, the IP phone plays the "Family" ringtone.

9. Optional: Select the checkbox of Enable Fax Detection. PBX will send the fax to Fax Destination if a fax tone is detected.
    - Extension: PBX will send the fax to Fax Destination if a fax tone is detected.
    - Fax to Email: PBX will send the fax as an attachment to the specified email address. An email address can be associated with extensions or be customized address.

    > Note:
    > If you want to send fax to email, make sure system email (on page 205) is configured correctly.
10. Click Save and Apply.

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 the selected trunk, the PBX will route the call through the inbound route with higher priority. You can adjust the priority of inbound routes according to your needs.

1. Go to Settings > PBX > Call Control > Inbound Routes.
2. Click to adjust the priority of your inbound routes.

Edit an inbound route

1. Go to Settings > PBX > Call Control > Inbound Routes.
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. Go to Settings > PBX > Call Control > Inbound Routes.
2. Click beside the inbound route that you want to delete.
3. On the pop-up window, click Yes and Apply.

Import Inbound Routes

You can import inbound routes to quickly set up inbound routing on Yeastar S1000-P IPPBX.

1. Go to Settings > PBX > Call Control > Inbound Routes, click Import.
2. Click Download the Template, add the inbound routes information in the template file.

> Note:
> - The imported file should be a UTF-8 `.csv` file.
> - For requirements of the import parameters, refer to Import Parameters - Inbound Routes (on page).

3. Click Browse to upload the template file.
4. Click Import.

Change Inbound Caller ID

By default, the Inbound caller ID on Yeastar S1000-P IPPBX displays the caller's phone number, you can change the inbound caller ID with Adapt Caller ID feature.

Adapt Caller ID feature is supported on each trunk. Go to Settings > PBX > Trunks, click Adapt Caller ID tab on the trunk edit page to configure the settings.

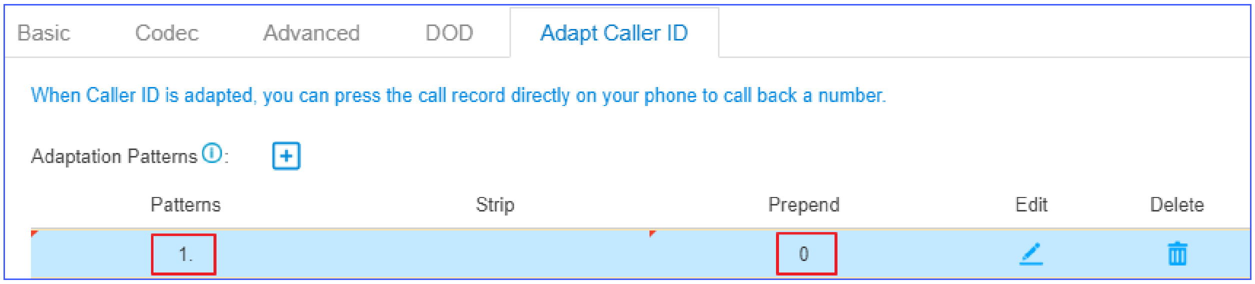
Example 1

Company A wants to add a digit 0 to the 11-digit incoming caller ID number that begins with digit 1 for quick redial purposes.

For example, company A wants to display 012345678910 instead of 12345678910.

In this case, you can configure Adapt Caller ID on trunk 1, and set the rules as follows:

- Patterns: 1.
- Strip: Leave it blank.
- Prepend: 0



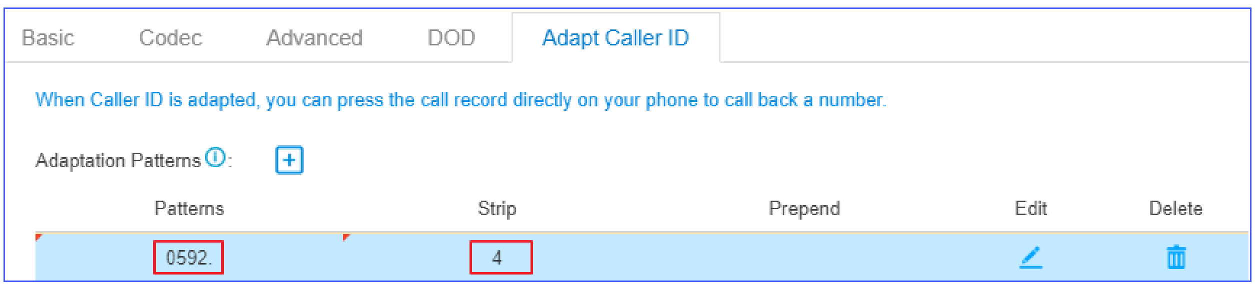
Example 2

Company B wants all Xiamen numbers to be displayed as local number without Xiamen area code (0592) that is received through the trunk 2.

For example, company B wants to display number 5503301 instead of 05925503301.

In this case, you can configure Adapt Caller ID on trunk 2, and set the rules as follows:

- Patterns: 0592.
- Strip: 4
- Prepend: Leave it blank.



Inbound Route Examples

Inbound Route Examples

This topic provides sample configurations that will help you understand DID setting and Caller ID setting of inbound routes.

> **Note:**
> The following examples ignore time condition (on page 53), you can set time condition according to your needs.

Inbound route without limit

Any calls to the selected trunk will be routed to the inbound route destination. You can set an inbound route as follows:

- Name: Set a name to help you identify it.
- Member Trunks: Select desired trunk(s).
- Destination: Set the destination.

  Leave all other fields blank.

Inbound route based on a DID number

If a trunk has multiple DID numbers, you can add multiple inbound routes that based on different DID numbers. When users dial different DID numbers, they will be routed to different destinations.

The following example shows an inbound route based on DID number 5503301.

- Name: Set a name to help you identify it. For DID routes, you can set the name as the DID number, which helps you identify the route.
- DID Pattern: 5503301
- Member Trunks: Select the trunk that has the DID number.
- Destination: Set the destination.

  Leave all other fields blank.

Inbound route based on consecutive DID numbers

If a trunk has multiple consecutive DID numbers, you can quickly set the DID number range in an inbound route to route calls to different destinations based on the DID numbers.

The following example shows an inbound route based on DID range 5503301-5503305, which will route calls to extension 1001-1005.

- Name: Set a name to help you identify it.
- DID Pattern: 5503301-5503305
- Member Trunk: Select the trunk that has the DID numbers.
- Destination: Select Extension Range, and enter the extension range 1001-1005.

  Leave all other fields blank.

Inbound route based on Caller ID

By default, PBX routes inbound calls without limit. If you set Caller ID Pattern, PBX will route calls only when the users' caller ID numbers match the Caller ID Pattern.

In the following example, the inbound route will route caller ID numbers that start with digit 1 to the destination. For example, number 532352584 that doesn't start with digit 1 can not call in the system through this inbound route.

- Name: Set a name to help you identify it.
- Caller ID Pattern: 1.
- Member Trunks: Select desired trunk(s).

- Destination: Select a destination.

  Leave all other fields blank.

Inbound route based on Caller ID and DID numbers

If you set both DID pattern and Caller ID pattern for an inbound route, PBX will check if the DID numbers and the user's caller ID number match the DID pattern and Caller ID pattern. Only the matched incoming calls can be routed to the pre-configured destination.

In the following example, when users dial 5503301 with phone number starting with digit 1, the inbound call will be routed to the destination.

- Name: Set a name to help you identify it.
- DID Pattern: 5503301
- Caller ID Pattern: 1.
- Member Trunk: Select desired trunk(s).
- Destination: Select a destination.

  Leave all other fields blank.

Route Inbound Calls Based on DID

This topic describes what is DID numbers and how to configure inbound routes on Yeastar S1000-P IPPBX to route inbound calls based on DID.

DID numbers

Direct Inward Dialing (DID) is a telephone service that allows outside users to reach a certain destination instead of going to a receptionist or a queue and needing to dial an extension number.

DID numbers are provided by the trunk provider.

The trunk provider usually assigns a range of numbers to the VoIP trunk. There is an extra charge for the DID numbers. Contact your trunk provider for more information about DID numbers.

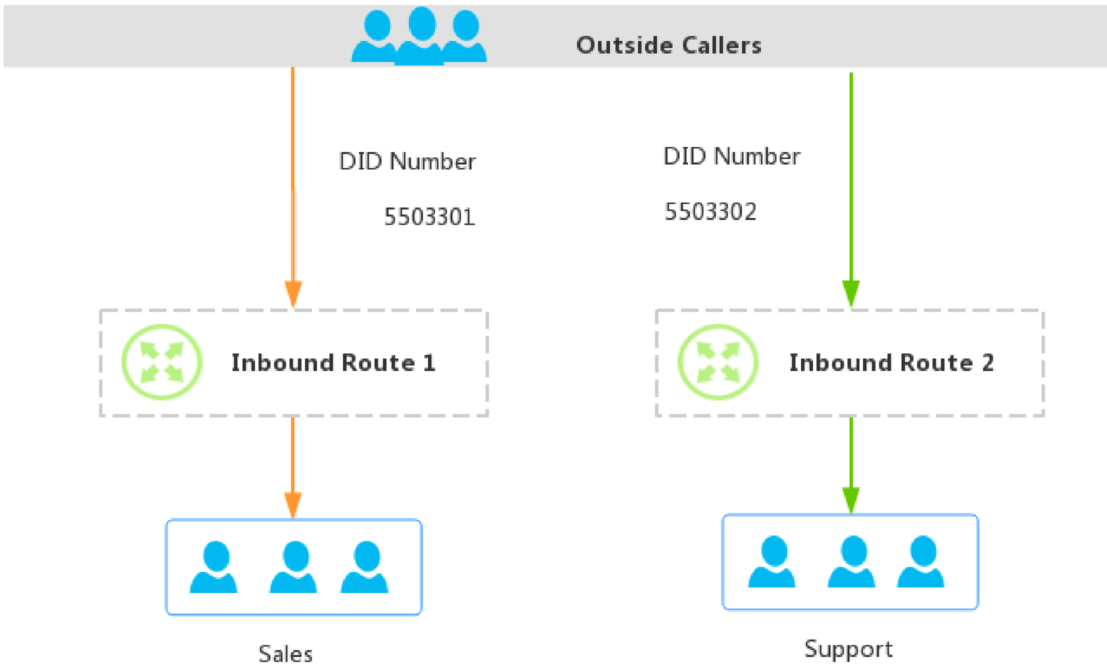
Configure DID routing - single DID

Bind a DID number to an inbound destination.

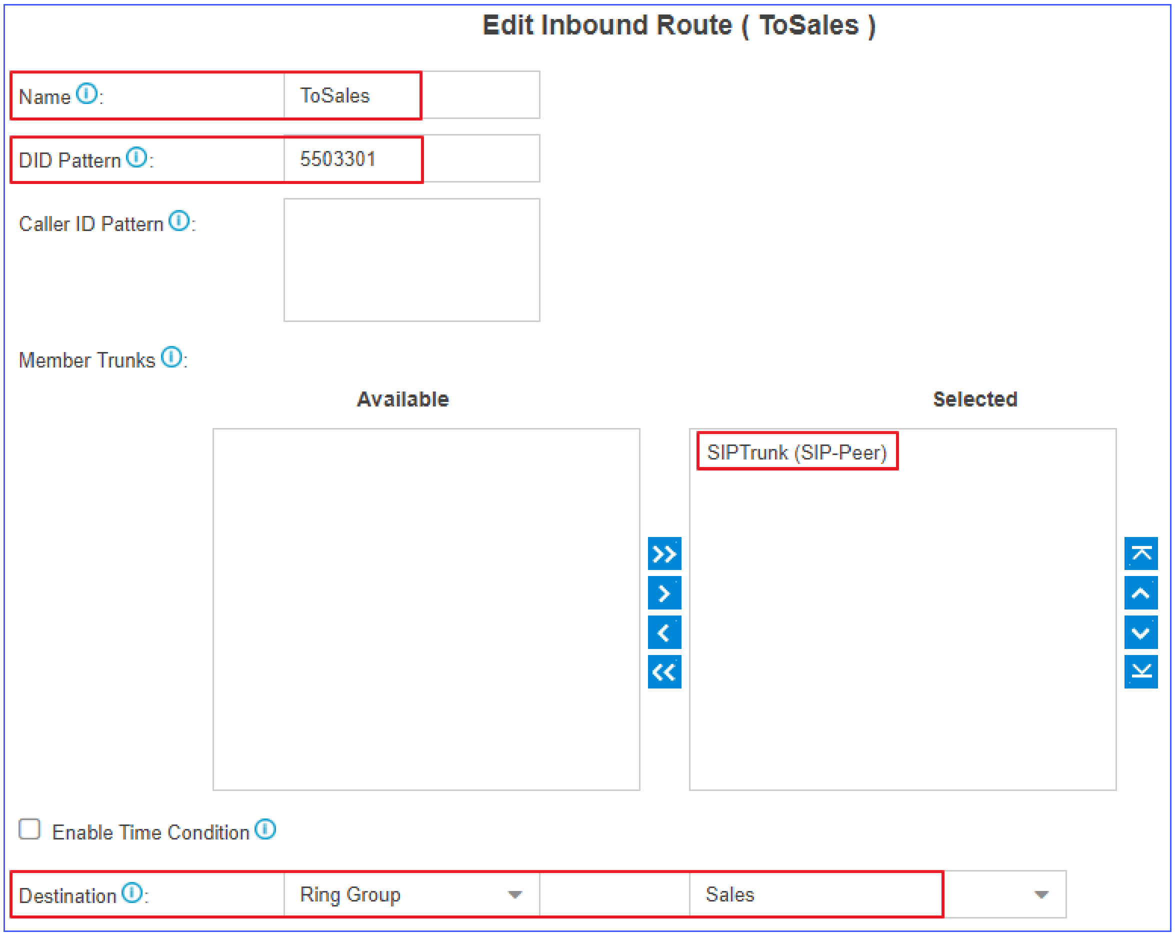
Example:

You purchased two DID numbers from the SIP trunk provider: 5503301 and 5503302.

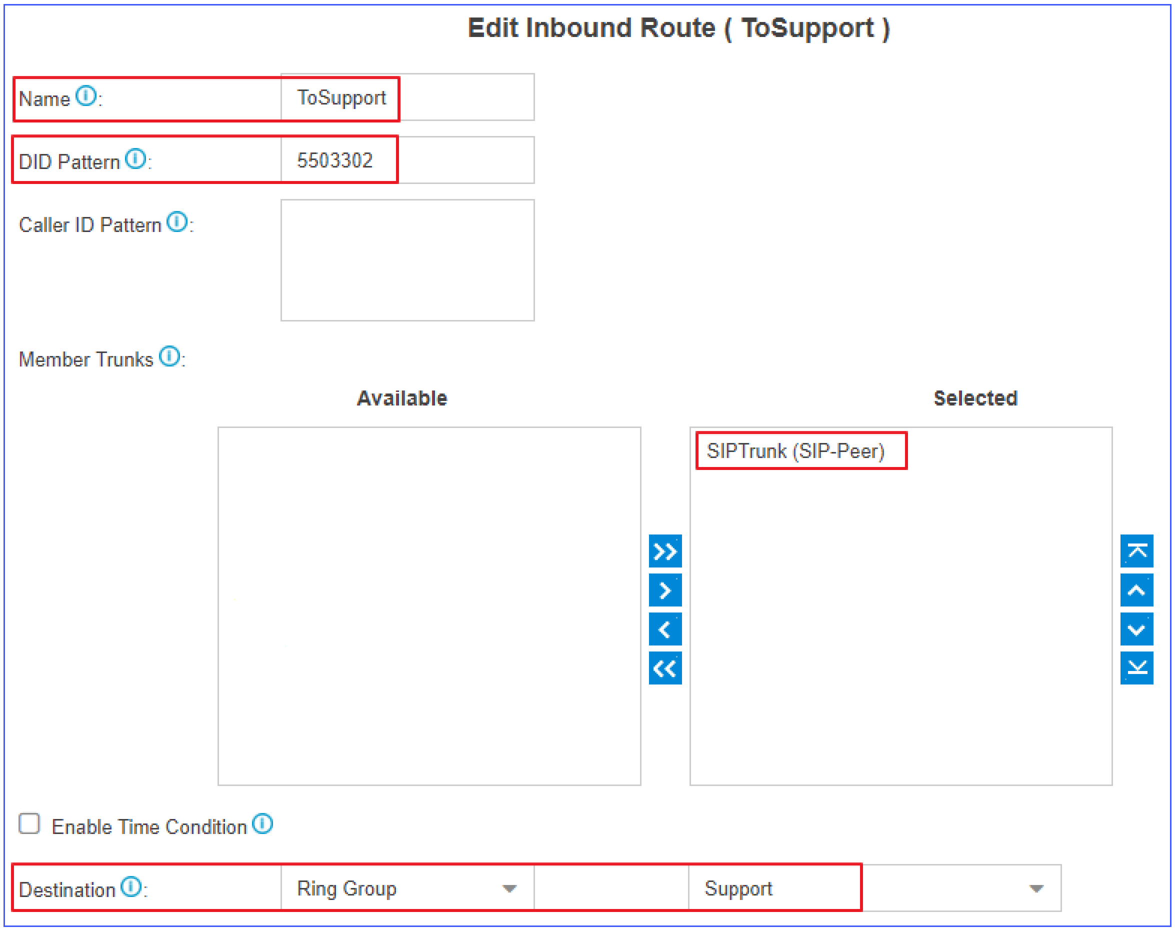
To route inbound calls to different destinations based on different DID numbers, you can set up two inbound routes for the two DID numbers.


Outside Callers
DID Number
5503301
DID Number
5503302
Inbound Route 1
Inbound Route 2
Sales
Support

1. Inbound Route ToSales for DID number 5503301.



   - Name: Set a name to help you identify it.
   - DID Pattern: Enter the DID number 5503301.
   - Caller ID Pattern: Leave it blank, which means no limit on caller's Caller ID.
   - Member Trunks: Select the trunk that is bound with the DID number.
   - Destination: Select the desired destination. When users dial the DID number 5503301, the call will be routed to the destination.
2. Inbound Route ToSupport for DID number 5503302.



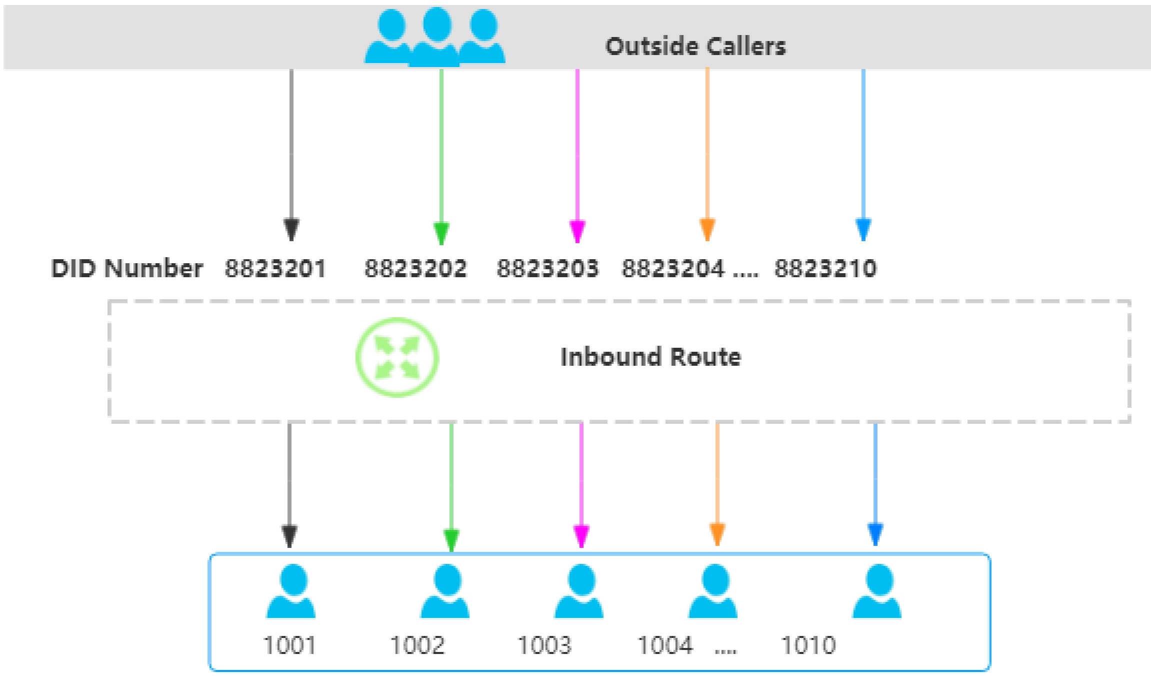
- Name: Set a name to help you identify it.
- DID Pattern: Enter the DID number 5503302.
- Caller ID Pattern: Leave it blank, which means no limit on caller's Caller ID.
- Member Trunks: Select the trunk that is bound with the DID number.
- Destination: Select the desired destination. When users dial the DID number 5503302, the call will be routed to the destination.

Configure DID routing - multiple DIDs

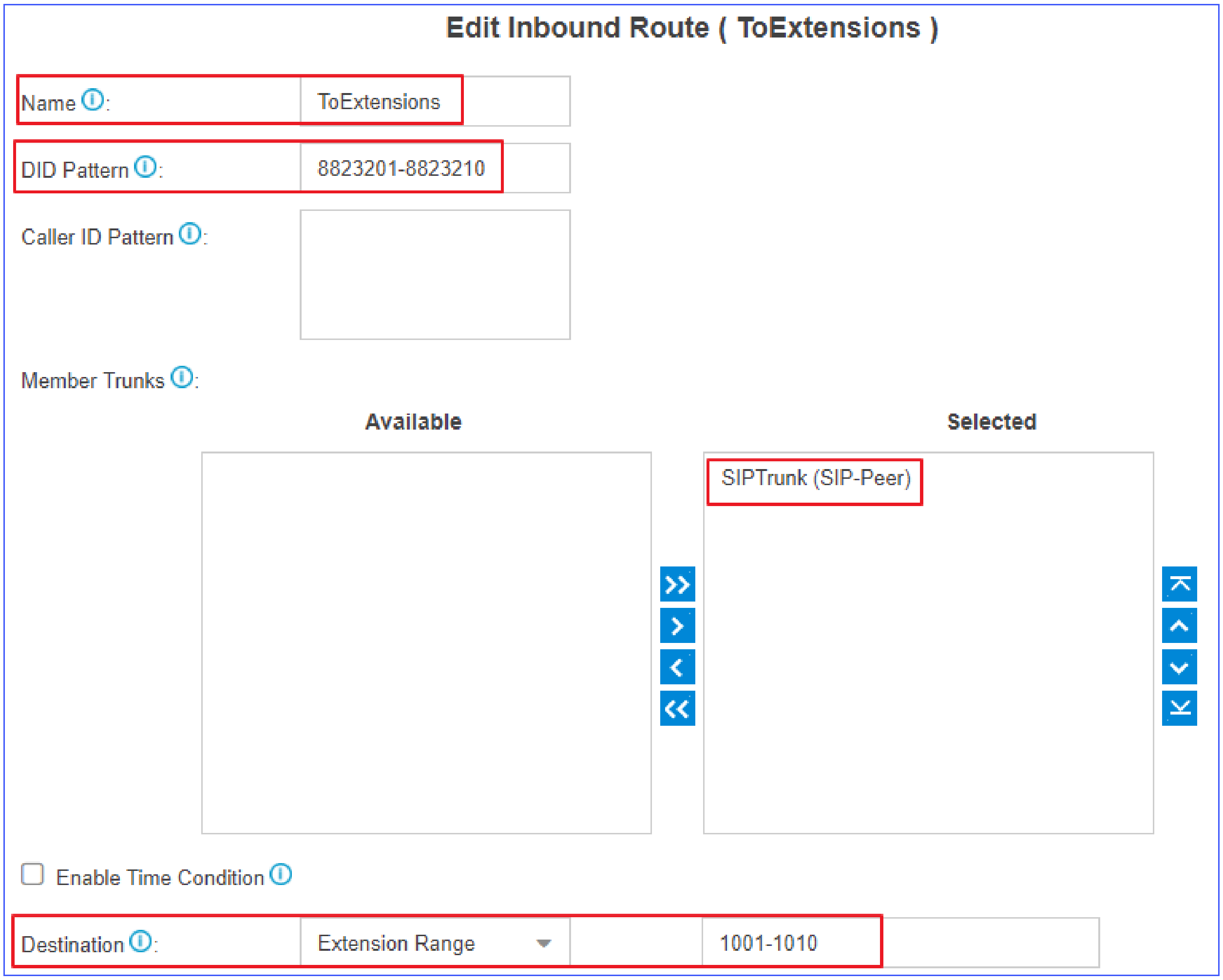
You can assign DID numbers to extension users one by one. When an outside user dials an DID number, the user can reach a specific extension directly.

> **Note:**
> The DID numbers should be consecutive DID numbers.

Example: You purchased 10 DID numbers from the SIP trunk provider: 8823201-8823210.



To assign the DID numbers one by one to extension 1001-1010 , you can configure the inbound route as follows.



- Name: Set a name to help you identify it.

- DID Pattern: Enter the DID range 8823201-8823210.
- Caller ID Pattern: Leave it blank, which means no limit on caller's Caller ID.
- Member Trunks: Select the trunk that is bound with the DID numbers.
- Destination: Select Extension Range, and enter the extension range 1001-1010.

> Note:
> The number of extensions and DID numbers must be the same.

Route Inbound Calls Based on Caller ID

This topic describes what is Caller ID routing and how to configure inbound routes on Yeastar S1000-P IPPBX to route inbound calls based on Caller ID.

Caller ID routing

Caller Identification (Caller ID) is a telephone service that displays a caller's phone number on the called party's phone device before the call is answered.

Caller ID routing allows users to accept or reject calls based on the caller's phone number. Inbound calls which match the Caller ID pattern on PBX will be routed to the pre-configured destination. For those unmatched, calls can not be established.

Scenarios

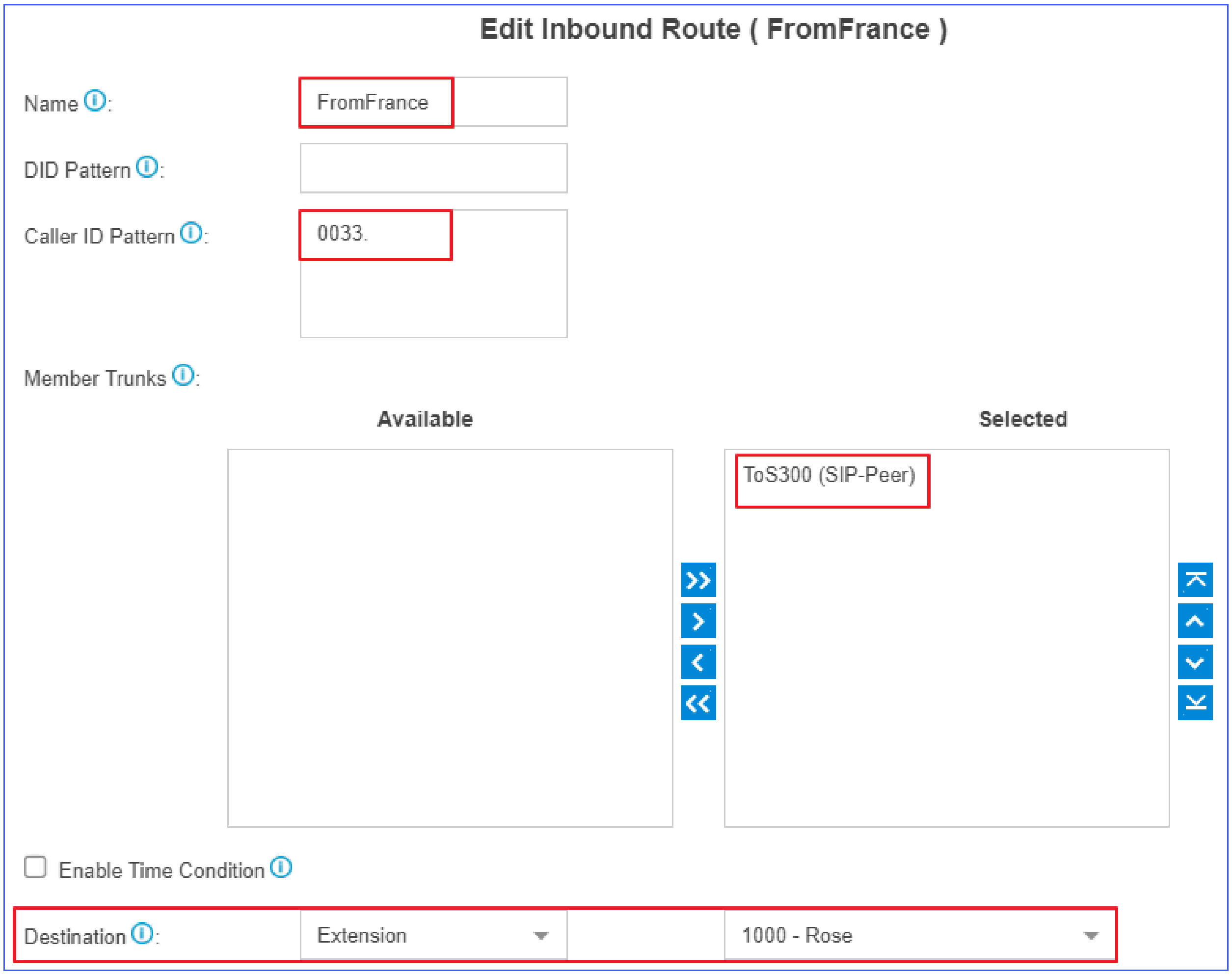
A company is dedicated to offering targeted service for different regions, the company hopes that the Caller ID of inbound calls can be identified and the calls can be routed to responsible employees. In this case, you can set Caller ID patterns for inbound routes.

Configuration Example

Company A assigns pre-sales business in France to Rose, and pre-sales business in America to Mike. Refer to the following table and related configuration figures.

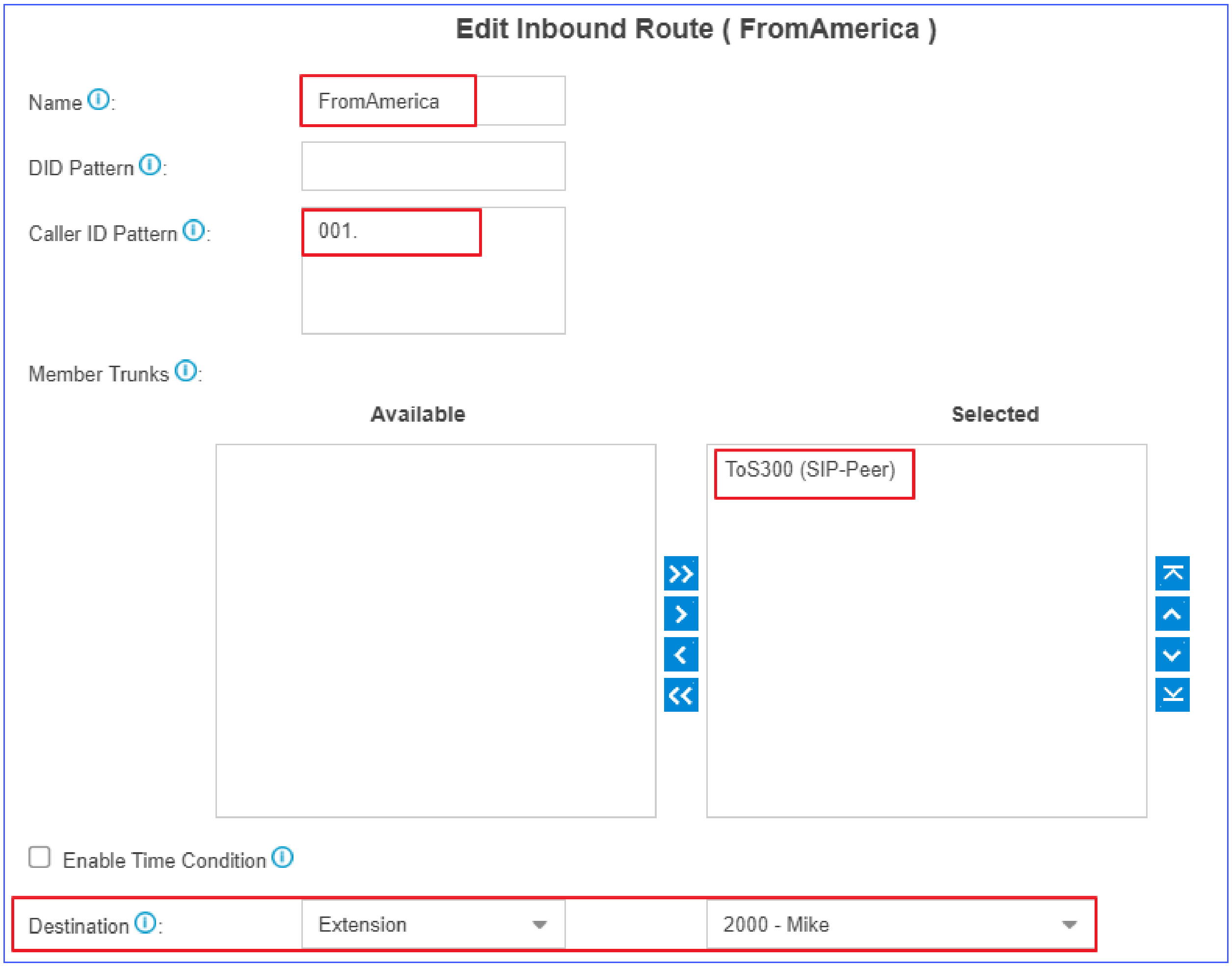
Name	Extension	Responsible Country	Area Code
Rose	1000	France	0033
Mike	2000	America	001

Configure Caller ID pattern for Rose



- Name: Set a name to help you identify it.
- Caller ID Pattern: Enter the caller ID pattern 0033..
- Member Trunks: Select the trunk that is bound with the caller ID pattern.
- Destination: Select the desired destination. When a caller calls to the trunk with the caller ID starting with 0033, the call will be routed to extension 1000.

Configure Caller ID pattern for Mike



- Name: Set a name to help you identify it.
- Caller ID Pattern: Enter the caller ID pattern 001..
- Member Trunks: Select the trunk that is bound with the caller ID pattern.
- Destination: Select the desired destination. When a caller calls to the trunk with the caller ID starting with 001, the call will be routed to extension 2000.

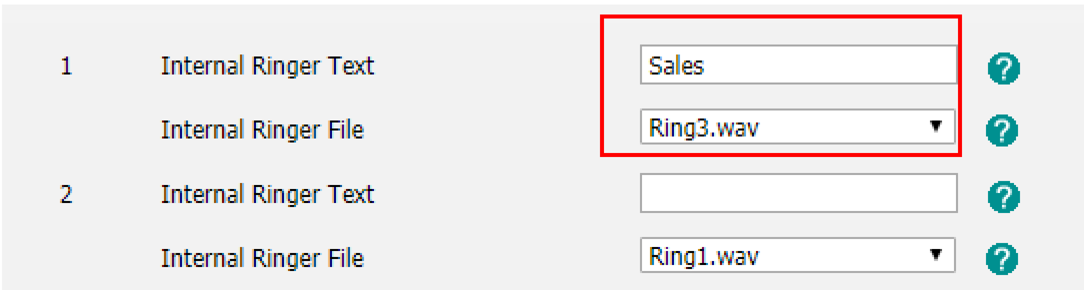
Distinguish Inbound Calls

Distinguish Inbound Calls by Ring Tones

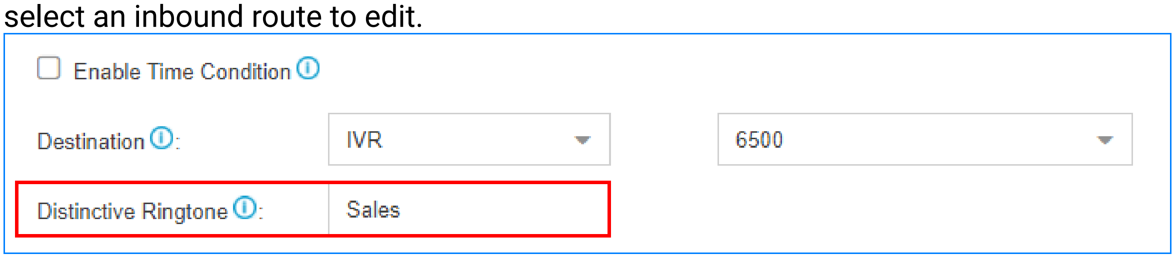
Distinctive ringtone distinguishes calls from different inbound routes. You can set distinctive ringtones on different inbound routes. When a user hears the ringtone of an incoming call, he/she may notice the intention of the call.

> Note:
> Distinctive Ringtone feature needs support from the IP phones. We take Yealink phone as an example.

1. Log in to the phone web interface, go to Settings > Ring, select a ringtone and set the name.



   a. In the Internal Ringer Text field, enter the ringtone name.
   b. In the Internal Ringer File drop-down list, select a ringtone file.
   c. Click Confirm to save the settings.
2. Log in to the PBX web interface, go to Settings > PBX > Call Control > Inbound Routes, select an inbound route to edit.



   a. In the Distinctive Ringtone field, enter the ringtone name that is configured on IP phone.
   b. Click Save and Apply.

When a call comes through the inbound route, the phone will play corresponding ringtone.

Distinguish Inbound Calls by DNIS Name

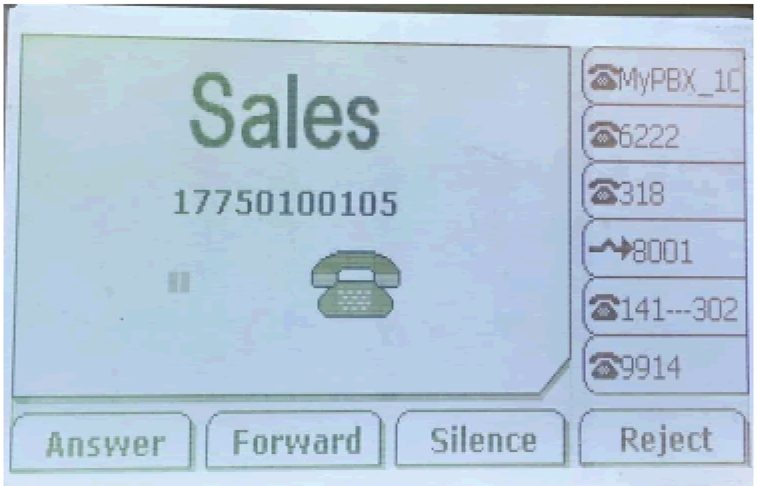
Dialed Number Identification Service (DNIS) is used to identify where the incoming call is from. You can set different DNIS names for different trunks or set different DID numbers and DNIS names for a trunk. When external users make calls to PBX, extension users can identify incoming call by DNIS name.

1. Go to Settings > PBX > Trunks, click beside the trunk that you want to edit.
2. On the trunk edit page, click Advanced tab.
3. In the DID Settings section, select the checkbox of DNIS Name, then set the name.
4. If the trunk has another DID number, click to add a DID number and set a DNIS name.

For example, a VoIP trunk has 3 DID numbers. 5503301 for Support, 5503302 for Sales, and 5503303 for Marketing. When external users dial a DID number, extension users can notice the intention by DNIS name displayed on an IP phone.

5. Click Save and Apply.

Make a call to the trunk of the PBX, the user who receives the call will see the incoming caller ID and the DNIS name of the trunk.



Distinguish Inbound Calls by Caller ID

When inbound calls are routed from a ring group/queue or an IVR, Yeastar S1000-P IPPBX can display the name of ring group/queue/IVR. When the extension user receives a call from the ring group/queue/IVR, he/she may notice the intention of the inbound call.

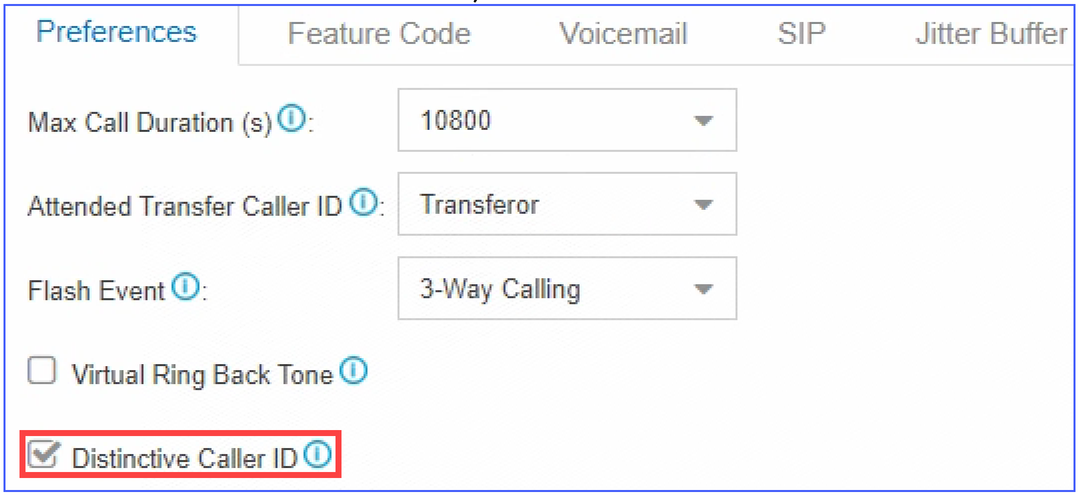
For example:

Set up two Ring Groups according to your organization, one is named as Sales, the other is named as Support.

You can set up two inbound routes to route incoming calls to different destinations by different trunks, and enable Distinctive Caller ID feature.

- When external users call to PBX, and IP phones of Sales members ring, "Sales" will be displayed on IP phones.
- When external users call to PBX, and IP phones of Support members ring, "Support" will be displayed on IP phones.

1. Go to PBX > General > Preferences, select the checkbox of Distinctive Caller ID.



2. Click Save and Apply.

Outbound Routes

Outbound Route Overview

An outbound route is used to tell the PBX which extension users are allowed to make outbound calls and which trunk to use for the outbound calls.

How does an outbound route work?

Every time user dials a number, PBX will do the following in strict order:

1. Examine the number user dialed.
2. Compare the dialed number with the pattern that you have defined in route 1.
    - If it matches, PBX will route the call out using the associated trunk.
    - If it does not match, PBX will match the number with the pattern that you have defined in route 2, and so on .

Dial Patterns of Outbound Route

This topic describes dial pattern settings of Outbound Route to help you understand and configure the dial patterns of Outbound Route.

Pattern

A pattern specifies routing rules to route a call based on the digits dialed by a user. The PBX matches a dial pattern and routes the call out based on the dial pattern.

Pattern	Description
X	Refers to any digit between 0 and 9.

Pattern	Description
Z	Refers to any digit between 1 and 9.
N	Refers to any digit between 2 and 9.
[###]	Refers to any digit in the brackets, example [123] would match the numbers 1, 2, or 3. Range of numbers can be specified with a dash, example [136-8] would match the numbers 1, 3, 6, 7, and 8.
.	Wildcard . matches one or more numbers. Example 9011. matches any numbers starting with 9011 (excluding 9011 itself).
!	• Wildcard ! matches none or more than one characters. Example 9011! matches any numbers starting with 9011 (including 9011 itself).

Strip

Strip is an optional setting, it defines how many digits will be stripped from the front of the dialed number before the call is placed.

Example:

Set Pattern as 9. and set Strip as 1.

If a user wants to call number 1588902923, he/she should dial 91588902923. The PBX will strip digit 9 from the dialed number, and call the number 1588902923.

Prepend

Prepend is an optional setting. The prepend will be added to the beginning of a successful match. If the dialed number matches the Pattern, the prepend will be added to the beginning of the number before placing the call.

Example:

If a trunk requires 10-digit dialing, but users are more comfortable with 7-digit dialing, you can prepend a 3-digit area code to all 7-digit phone numbers before the calls are placed.

Prefix and dial patterns

Scenarios

Prefix setting appears when you are configuring the following settings:

- Mobility Extension (on page 29)
- Mobile phone number for Notification Contacts (on page 209)
- External number for IVR keypress (on page 105)

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.

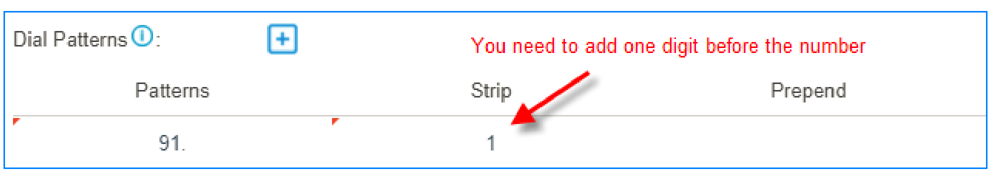
  For example, to call number 125451, you should dial the number 125451 directly.

- Add prefix before a number

  If Strip is set, you need to set the prefix according to the Patterns.

  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.



Related information
Outbound Route Examples (on page 85)

Add an Outbound Route

To allow users to make outbound calls through trunks, you need to set up at least one outbound route on the PBX.

The PBX 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.

1. Go to Settings > PBX > Call Control > Outbound Routes, click Add.
2. On the configuration page, configure an outbound route according to your needs.
    - Name: Enter a name to help you identify it.
    - Dial Patterns: Used to match the digits that users dial. When the dialed numbers match a dial pattern (on page 81), PBX will route the call out through matched outbound route.

Pattern	Description
X	Refers to any digit between 0 and 9.
Z	Refers to any digit between 1 and 9.
N	Refers to any digit between 2 and 9.
[###]	Refers to any digit in the brackets.
.	Wildcard . matches one or more numbers.
!	Wildcard ! matches none or more than one characters.

    - Member Trunks: Select a trunk to make outbound calls. If the dialed number matches a dial pattern of the outbound route, PBX will route the call out through selected trunk.
    - Member Extensions: Select which extensions are allowed to use this outbound route.
    - Password: Optional. Set a password for the outbound route. If a password is set, users are required to enter a password when they try to make outbound calls through this route.
        - None: No password is needed.
        - PIN List: Select a PIN list. Users are required to enter a password in the PIN list when they try to make outbound calls through this outbound route.
        - Single Pin: Enter a password. Users are required to enter the password when they try to make outbound calls through this outbound route.
    - Rrmemory Hunt: Optional.
        - If the feature is enabled, PBX will remember which trunk was used last time, and then use the next available trunk to call out.

          For example, PBX uses the first trunk to call out, then it will use the second trunk to call out next time.
        - If the feature is disabled, PBX will use trunks orderly to call out.
    - Time Condition (on page 53): Optional. You can define during which time period can users use this outbound route. By default, users can call out through the outbound route at any time.
3. Click Save and Apply.

> Note:
> After you finish the outbound route configurations, you need to check and adjust the priority of your outbound routes, so that PBX can match and route the call out through the proper outbound route.

Related information

Dial Patterns of Outbound Route (on page 81)
Outbound Route Examples (on page 85)

Outbound Route Examples

This topic provides sample configurations that will help you understand dial patterns of outbound route.

Route Name: Domestic

In Xiamen, China, local numbers are all 7-digit numbers and the numbers do not start with 0, such as 5503305.

For long-distance calls, you need to dial the 4-digit area code and local numbers, such as 0595-5503305. The area code in China is in the format of 0ZXX, the first digit is 0, and the second digit cannot be 0.

<table>
<tr><th>Pattern</th><th>Strip</th><th>Prepend</th><th>Description</th></tr>
<tr><td>90ZXX.</td><td>1</td><td>Leave it blank.</td><td>This is for a long-distance call.
The long-distance number starts with 0, and users should dial 9 before the number.
Note:
Before placing the call, PBX will strip the leading digit 9.
Example: To call number 05955503303, the user should dial 905955503303.</td></tr>
<tr><td>9ZXXXXXX</td><td>1</td><td>Leave it blank.</td><td>This is for a local call.
The local number starts with digit 1-9, and users should dial 9 before the number.
Note:
Before placing the call, PBX will strip the leading digit 9.</td></tr>
</table>

Pattern	Strip	Prepend	Description
			Example: To call number 5503301, the user should dial 95503301.

Route Name: Mobile

All mobile phone numbers in China are 11-digit numbers and start with digit 1, such as 15880260666.

Pattern	Strip	Prepend	Description
1XXXXXXXXXX	Leave it blank.	Leave it blank.	Users can dial the mobile number as they usually do. Example: To call number 15880260666, dial 15880260666.

Route Name: International_Call

All international numbers start with digits 00.

Pattern	Strip	Prepend	Description
00.	Leave it blank.	Leave it blank.	Numbers start with digits 00 will go through this outbound route. Example: To call number 16262023379, dial 001626202379.

Import Outbound Routes

You can import outbound routes to quickly set up outbound routing on Yeastar S1000-P IPP-BX.

1. Go to Settings > PBX > Call Control > Outbound Routes, click Import.
2. Click Download the Template, add the outbound routes information in the template file.

> Note:
> - The imported file should be a UTF-8 `.csv` file.
> - For requirements of the import parameters, refer to Import Parameters - Outbound Routes (on page).

3. Click Browse to upload the template file.
4. Click Import.

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, greatly saving calling cost for your company.

> Note:
> The route priority is important, especially if there is some overlap. For example, the number 5503305 matches both a dial pattern of `ZXXXXXX` and `X.`, the PBX will send the call through the outbound route with the highest priority.

Example:

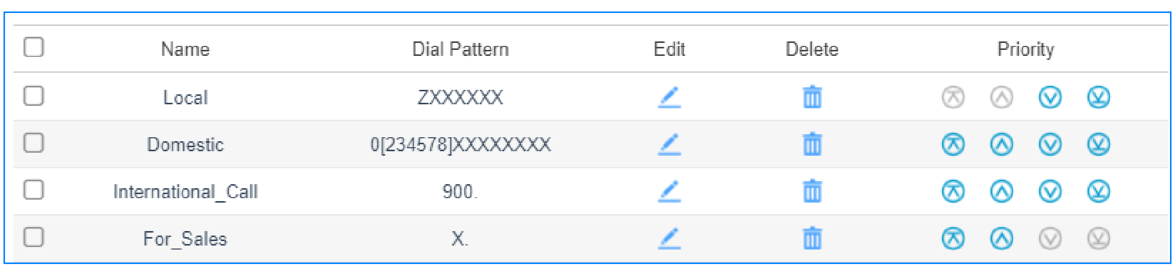
When users dial 05503301, both of the two outbound routes match 05503301:

- 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. Go to Settings > PBX > Call Control > Outbound Routes.
2. Click the buttons to adjust the priority of your outbound routes.

> Note:
> PBX will match outbound route from top to bottom.



	Name	Dial Pattern	Edit	Delete	Priority
	Local	ZXXXXXX			
	Domestic	0[234578]XXXXXXXX			
	International_Call	900.			
	For_Sales	X.			

- : Put this outbound route at the top.
- : Move this outbound route upward.

- : Move this outbound route downward.
- : Put this outbound at the bottom.

Edit an outbound route

1. Go to Settings > PBX > Call Control > Outbound Routes.
2. Click beside the outbound route that you want to edit.
3. Edit the outbound route.
4. Click Save and Apply.

Delete an outbound route

1. Go to Settings > PBX > Call Control > Outbound Routes.
2. Click beside the outbound route that you want to delete.
3. On the pop-up window, click Yes and Apply.

> Note:
> After you delete the outbound route, extension users can not make outbound calls through this outbound route.

Outbound Restriction

Outbound Restriction Overview

Outbound Restriction is used to limit how many outbound calls extension users can make within specified time period.

Scenarios

Avoid toll fraud

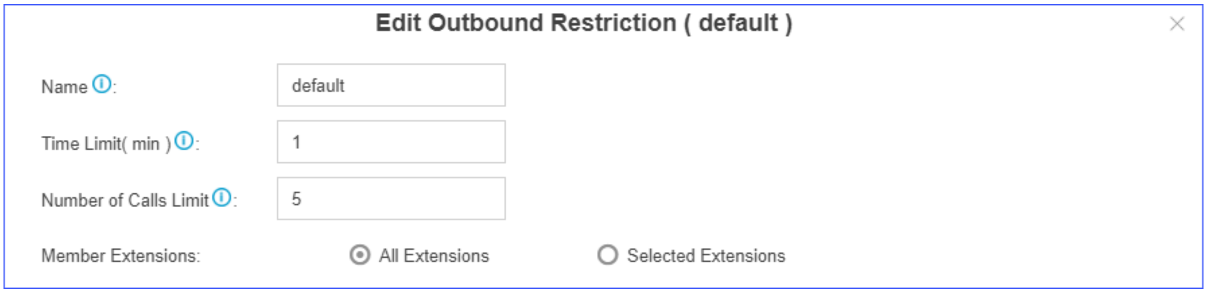
Most toll fraud is committed from the outside. Hackers may attack the system by registering to extensions and making outbound calls frequently.

With the Outbound Restriction rules, if extension users make outbound calls over the limited frequency, the extensions will be blocked and unable to make outbound calls.

Default outbound restriction rule

The PBX has a default rule to limit users to make maximum 5 outbound calls in 1 minute. You can add another Outbound Restriction rule according to your needs.

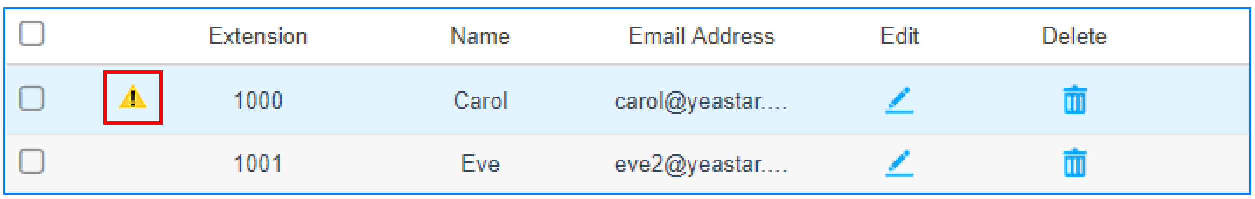
> **Note:**
> We recommend that you keep the default Outbound Restriction rule.



Cancel restriction of outbound calls

If a user makes outbound calls over the limit, the extension will be locked and prohibited from making outbound calls. On Extensions list, the extension status will display .

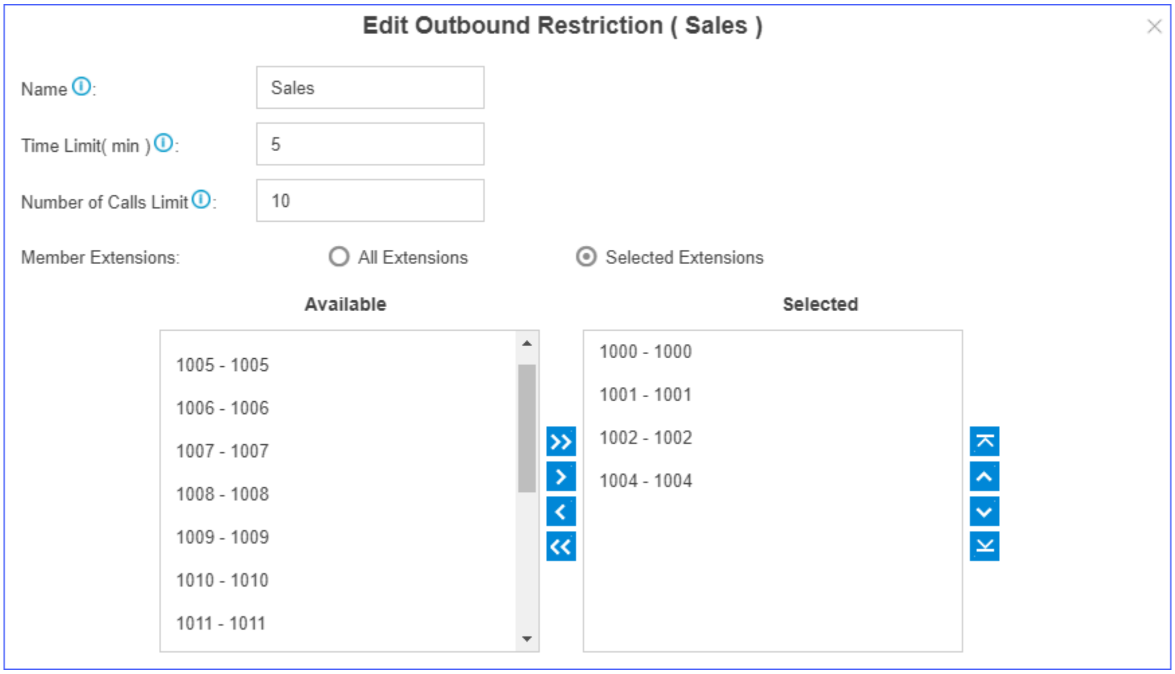
Double click the icon , the extension will be able to make outbound calls again.



Add a Rule to Restrict Outbound Calls

The PBX has a default rule to limit users to make maximum 5 outbound calls in 1 minute. You can add an Outbound Restriction rule to define how many outbound calls the extension users can make during a period of time.

1. Go to Settings > PBX > Call Control > Outbound Restriction, click Add.
2. On the configuration page, configure an outbound restriction rule according to your needs.



- Name: Enter a name to help you identify it.
- Time Limit(min): Set time in minutes to limit the number of outbound calls during the time period.
- Number of Calls Limit: Set the number of outbound calls during the specified time period. For example, set Time Limit(min) to 5, Number of Calls Limit to 10. It means if the selected extension users make outbound calls over 10 times in 5 minutes, the extension(s) will be locked and can not make outbound calls.
- Member Extensions: Select extensions which will be restricted by the rule.

3. Click Save and Apply.

Manage Outbound Restriction Rules

After you create restriction rules, you can edit or delete them.

Edit an outbound restriction rule

1. Go to Settings > PBX > Call Control > Outbound Restriction.
2. Click beside the outbound restriction rule that you want to edit.
3. Edit the outbound restriction rule.
4. Click Save and Apply.

Delete an outbound restriction rule

1. Go to Settings > PBX > Call Control > Outbound Restriction.
2. Click beside the outbound restriction rule that you want to delete.
3. On the pop-up window, click Yes and Apply.

AutoCLIP Routes

AutoCLIP Overview

Auto Calling Line Identity Presentation (AutoCLIP) is an intelligent call matching feature. You can configure AutoCLIP to route inbound calls to original extensions, which will promote your customer satisfaction and work efficiency.

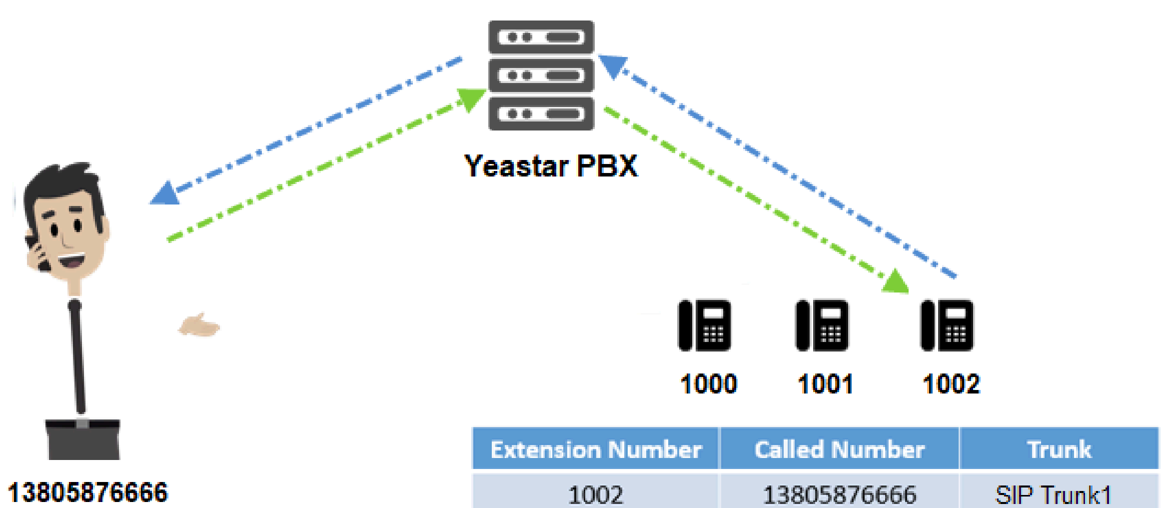
Scenarios

Assume 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 reception or business auto attendant. Neither reception/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.

How does the PBX redirect calls to original extensions?

1. When extension users make outbound calls, the PBX automatically stores the records to AutoCLIP routing table.
2. When customers call in the PBX, PBX will search the phone numbers from the AutoCLIP routing table.
    - If there're matched records in AutoCLIP routing table, the calls will be routed to corresponding extensions.
    - If there're not matched records in AutoCLIP routing table, the calls will be routed to the destination specified in inbound routes.



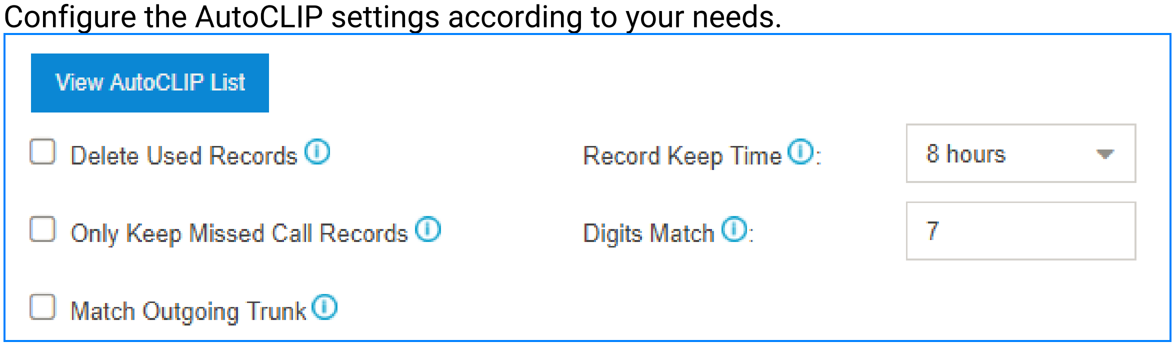
Configure AutoCLIP to Route Inbound Calls to Original Extensions

With AutoCLIP feature on Yeastar S1000-P IPPBX, the PBX can route inbound calls from customers to original extensions users who placed the calls. This intelligent call matching feature can greatly improve work efficiency and customer satisfaction.

> **Note:**
>
> - Enable caller ID feature for the trunk that you want to configure AutoCLIP routes, or the PBX can not distinguish the caller ID and perform AutoCLIP.
> - If many extension users 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.

1. Go to Settings > PBX > Call Control > AutoCLIP Routes.
2. In the Member Trunks section, select the trunk(s) from Available box to the Selected box.

3. Configure the AutoCLIP settings according to your needs.



- Delete Used Records: Select this option, PBX will perform AutoCLIP as follows:
    a. When receiving an external call from customer A, the PBX will search the record from AutoCLIP list, and redirect the call to the original extension user that placed the call.
    b. PBX will delete the AutoCLIP record.

c. When receiving an external call from customer A again, PBX will always route the call to the destination specified by the inbound route instead of searching the record from AutoCLIP list.
d. If extension users make outbound calls to customer A again, PBX will generate AutoCLIP record again.

> Note:
> To restrict PBX from routing all inbound calls from a certain customer to the same extension user, select Delete Used Records.

- Record Keep Time: Set how long records can be kept in AutoCLIP list. If keep time of a certain record over the value, PBX will automatically delete the record.
- Only Keep Missed Call Records: Select this option. Only unconnected outbound calls (missed calls on the called party) will be recorded in AutoCLIP list.
- Digit Match: The default value is 7, which means if the digit of caller ID is less than or equal to 7, the PBX will match the whole phone number with all phone numbers in AutoCLIP list. If the digit of caller ID over 7, the PBX will match the last 7 digits of phone number with all phone numbers in AutoCLIP list.

  Example:

  a. Extension user 2000 makes an outbound call to customer 15880270666, and an AutoCLIP record is generated.
  b. When the customer calls in the PBX, the caller ID displays +8615880270666, where +86 stands for country code. To make sure the PBX can exactly match the phone number in AutoCLIP list, you should set Digit Match to 11.
  c. If the last 11 digits of +8615880270666 exactly match the phone number in AutoCLIP list, the PBX will route the call to extension 2000.
- Match Outgoing Trunk: Select this option. The PBX will route the call to the original extension only when the trunk number dialed by external users matches the trunk that used to place the call earlier.

  Example:

  Extension user (1000) uses trunk1 to call external user (15880273600). PBX will route the call to extension (1000) only when the external user (15880273600) calls the phone number of trunk1.

4. Click Save and Apply.
5. Test AutoCLIP routes.

   Extension user uses the trunk with AutoCLIP feature to call external users out.

PBX generates an AutoCLIP record when extension user uses the trunk with AutoCLIP feature to call external users out. On the AutoCLIP Routes page, click View AutoCLIP List to view AutoCLIP record.

SLA Stations

SLA Overview

Shared Line Appearance (SLA) feature helps users share and monitor SIP trunks. After enabling SLA feature for a trunk, the trunk works as the exclusive line for SLA station and is unavailable in both inbound routes and outbound routes.

SLA trunk refers to the trunk with SLA feature enabled. SLA station refers to an extension which is bound with an SLA trunk.

- When an SLA station makes an outbound call through SLA trunk, other members sharing the SLA trunk can monitor the trunk state by BLF keys LED on phone devices.
- When receiving an external call from SLA trunk, all extensions sharing the SLA trunk will ring.

> Note:
> If Allow Barge feature is enabled on an SLA trunk, all members can place and join multi-party calls.

SLA Sample Configuration

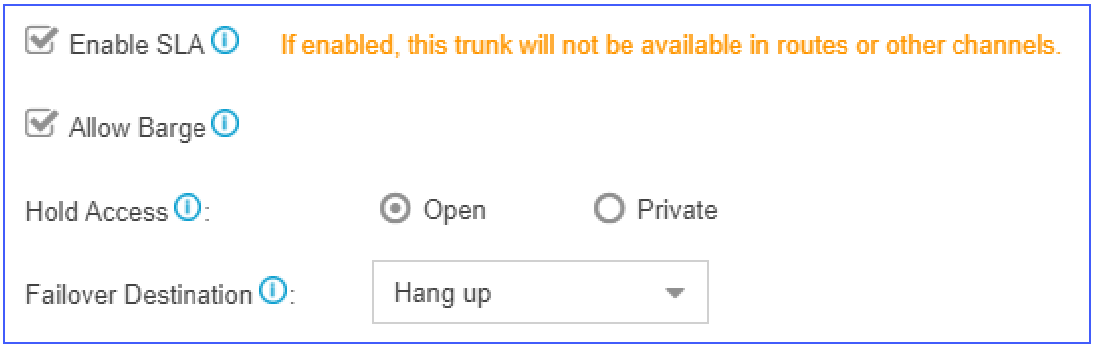
In a boss-assistant scenario, sometimes assistant needs to answer calls for the boss. So boss and assistant need to share a trunk. In this topic, we introduce how to configure SLA trunk and SLA station on Yeastar S1000-P IPPBX based on a boss-assistant scenario.

Assume that the boss's phone is extension 2000 and the assistant's phone is extension 1000. The shared trunk name is "sipabc" and the trunk number is 5503305.

> Note:
> SLA feature should be used in conjunction with BLF keys on phone devices.

You can set up a shared trunk as follows.

1. Enable SLA feature.
    a. Go to Settings > PBX > Trunks, click beside the trunk that you want to enable SLA.
    b. On the Basic page, select Enable SLA and configure the SLA settings.



- Enable SLA: Select this option to enable SLA on the trunk.
- Allow Barge: Optional. Whether to allow other SLA stations that share the trunk to join the ongoing call by pressing the BLF key on phone devices.
- Hold Access: Whether to allow any SLA stations to retrieve a call that's put on hold.
    - Open: Any SLA stations that share the trunk can retrieve the call.
    - Private: The call can be retrieved only by the SLA station that previously put the call on hold.
- Failover Destination: The unanswered calls will be routed to the destination.
    - Hang up
    - Extension
    - Voicemail
    - IVR
    - Ring Group
    - Queue

c. Click Save and Apply.

2. Add two SLA stations for the same SLA trunk. One SLA station for the boss's extension 2000, the other SLA station for the assistant's extension 1000.
    a. Go to Settings > PBX > Call Control > SLA, click Add.
    b. On the SLA Station configuration page, set SLA station for the boss.

- Station Name: Set a name to help you identify it.
- Station: Select the boss's extension 2000.
- Associated SLA Trunks: Select SLA trunk from the Available box to the Selected box.
- Ring Timeout(s): Set the timeout in seconds. When receiving an inbound call, the phone of the SLA station will ring until timeout. The default value is 30s.
- Ring Delay(s): Set the time delay in seconds. Phone of the SLA station will delay ringing after the time defined. The time of Ring Delay(s) can not be longer than the time of Ring Timeout(s). The default value is 0.
- Hold Access:Whether to allow any SLA stations to retrieve a call that's put on hold.
  - Open: Any SLA stations that share the line can retrieve the call.
  - Private: The call can be retrieved only by the SLA station that previously put the call on hold.

c. Click Save and Apply.
d. Repeat steps a to c to set the other SLA station for the assistant.

> **Note:**
> In the Station field, select the assistant's extension 1000.
>
> 
>

3. On the boss's IP phone (extension 2000), configure a BLF key to monitor SLA trunk.

> **Note:**
> We take an Yealink IP phone as an example.
> a. Log in to the phone web interface, go to DSS key > Line Key to set a BLF key for the boss.
> b. Select a key to configure.
>
> 
>
> | Key | Type | Value | Label | Line | Extension |
> |---|---|---|---|---|---|
> | Line Key1 | BLF | 2000_sipabc | | Line1 | |
>
> - Type: Select BLF.
> - Value: Enter `{ext_num}_{trunk_name}`. In this example, enter 2000_sipabc.
>
> > **Note:**
> > - {ext_num} stands for extension number.
> > - {trunk_name} stands for trunk name.

> - Line: Select the line which the extension registers to.
> - Extension: Optional. You can enter the key name to help you identify it.
>
> c. Click Confirm.

4. On the assistant's IP phone (extension 1000), configure a BLF key to monitor SLA trunk.

> Note:
> We take an Yealink IP phone as an example.

   a. Log in to the phone web interface, go to DSS key > Line Key to set a BLF key for the assistant.
   b. Select a key to configure.

Key	Type	Value	Label	Line	Extension
Line Key1	BLF	1000_sipabc		Line1	

   - Type: Select BLF.
   - Value: Enter `{ext_num}_{trunk_name}`. In this example, enter 1000_sipabc.

> Note:
> - {ext_num} stands for extension number.
> - {trunk_name} stands for trunk name.

   - Line: Select the line which the extension registers to.
   - Extension: Optional. You can enter the key name to help you identify it.

   c. Click Confirm.

If the configuration is correct, you can see the BLF key LED is on.

- Green: The trunk is available.
- Red: The trunk is busy.

The boss and assistant can share the trunk by SLA.

Related information
Share Trunks by SLA (on page 98)

Share Trunks by SLA

After setting up SLA stations on PBX and configuring BLF keys on IP phones, users can monitor SLA trunks, receive calls from SLA trunks, and make outbound calls through SLA trunks.

Make outbound calls

SLA station can monitor the status of SLA trunk according to BLF keys status.

> Note:
> For different phone models, there may be some difference in the status of BLF keys.

- If the BLF key used to monitor SLA trunk turns green, it indicates that the trunk is available, and the associated SLA station can make outbound calls through this trunk.

  To make outbound calls, the SLA station should press BLF key first, and dial the external number after hearing a dial tone.
- If the BLF key used to monitor SLA trunk turns red, it indicates that the trunk is in use. Other SLA stations can not use the trunk to make outbound calls now.

Handle incoming calls

When an external call reaches the SLA trunk, all phones of associated SLA stations will ring, and BLF keys on phone devices will flash in red. Any SLA stations can answer the call by pressing BLF keys.

Barge-in an active call

If Allow Barge (on page 95) is enabled for an SLA trunk, other SLA stations are allowed to join an active call.

When an SLA station is in a call with other users using this SLA trunk, other SLA stations can join the active call by pressing the BLF key.

Hold and retrieve calls

During the call, the SLA station can press the BLF key to hold and retrieve the call. Whether an SLA station can retrieve a call or not depends on the Hold Access.

> Note:
> Hold Access of SLA station has a higher priority than the Hold Access of a trunk.

- If Hold Access is set to Open, other stations that share the trunk can press BLF key to retrieve the call.
- If Hold Access is set to Private, the call can be retrieved only by the station that previously put the call on hold.

Related information

SLA Sample Configuration (on page 94)

Call Features

Call Forwarding

Set Call Forwarding Rules

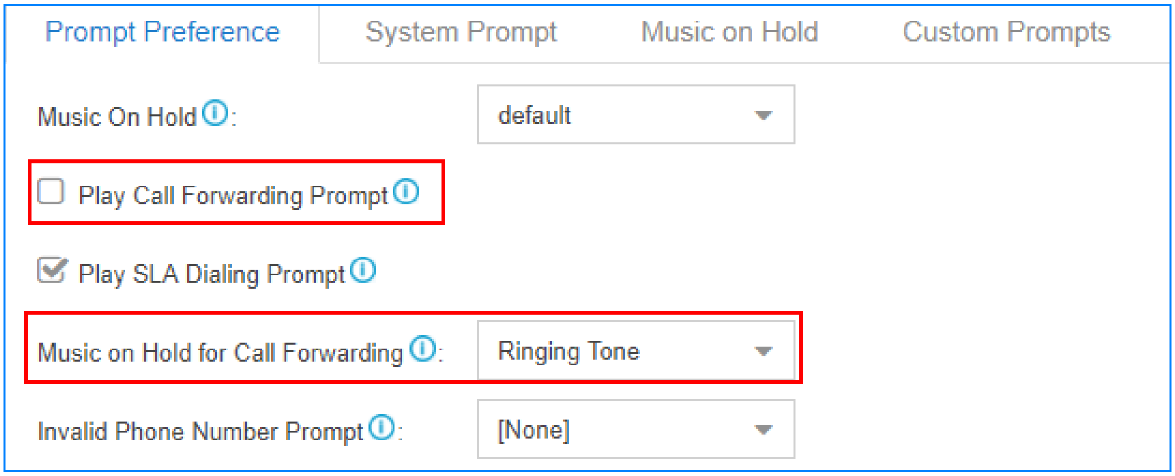
Call forwarding rules allow users to automatically forward an incoming call to voicemail, another extension, mobile, etc.

1. Go to Settings > PBX > Extensions, search and find the desired extension, click ✎.
2. Click Features tab.
3. In the Call Forwarding section, set call forwarding rules for the extension.
    a. Select a forwarding option.
        - Always: All the incoming calls will be forwarded to the destination.
        - No Answer: Only the unanswered calls will be forwarded to the destination.
        - When Busy: Only the calls that come in while you are talking on the phone will be forwarded.
    b. Select a forwarding destination from the drop-down list.
4. Click Save and Apply.

Set Call Forwarding Prompt

By default, when the 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 when the caller is waiting. You can disable the call forwarding prompt and change the MoH music to a normal ringtone. In this way, the caller will not realize that the call is forwarded.

1. Go to Settings > PBX > Voice Prompts > Prompt Preference.
2. Unselect the checkbox of Play Call Forwarding Prompt.
3. In the Music on Hold for Call Forwarding drop-down list, select Ringing Tone.

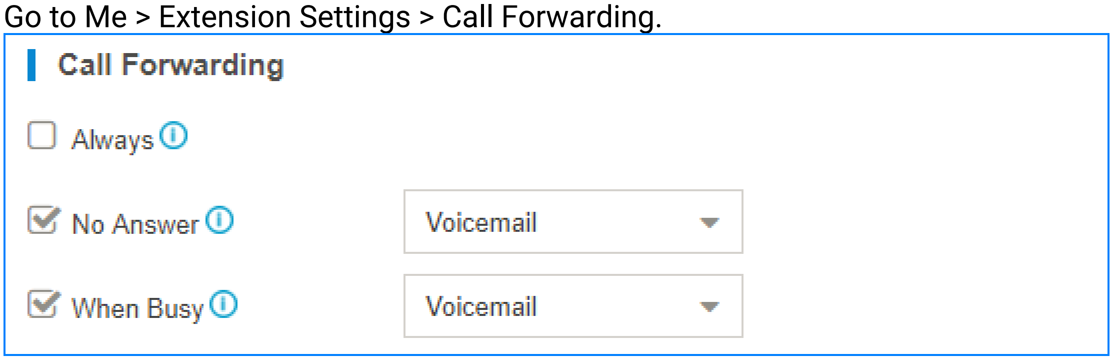


4. Click Save and Apply.

Set up Call Forwarding for Your Extension

Log in to the Extension User Portal to change the call forwarding settings for your extension.

1. Go to Me > Extension Settings > Call Forwarding.



2. Select a forwarding option.
    - Always: All the calls will be forwarded regardless of your state.
    - No Answer: Calls will be forwarded if you don't answer the call.
    - When Busy: Calls will be forwarded when you are busy in a call.
3. Select the destination for the forwarding condition.
4. Click Save and Apply.

IVR

Like most organisations, where possible, we would like to route incoming calls an Auto Attendant. You can create one or more IVR (Auto Attendant) on the system to achieve it.

When calls are routed to an IVR, the system will play a recording prompting them what options the callers can enter such as “Welcome to XX, for sales press 1, for Technical Support press 2”.

Set up an IVR

Set up your own IVR if you need to route incoming calls via an auto attendant.

1. Go to Settings > PBX > Call Features > IVR, click Add to add an IVR or edit the default IVR.
2. Edit the Basic settings of the IVR.
    - Number: PBX treats IVR as an extension; you can dial this extension number to reach the IVR from internal extensions.
    - Name: Set a name for the IVR.
    - Prompt: Use the default IVR prompt or select your custom IVR prompt (on page 103).
    - Prompt Repeat Count: Set how many times the prompt will be played.
    - Response Timeout(s): Set how long the PBX will wait for the caller to operate.
    - Digit Timeout(s): After the user enters a digit, the user needs to enter the next digit within the timeout.
    - Dial Extensions: Whether to allow callers to dial extension numbers via IVR.
    - Dial Branches' Extensions if Multisite Interconnect is enabled: When the PBX is connected to other PBX systems via Multisite Interconnect (on page) feature, callers can make a direct dial to the extensions of other PBX systems connected.
    - Dial Outbound Routes: Whether to allow callers to dial outbound calls via IVR.

      > Note:
      > This option is useful if you interconnect two PBXs. The callers can dial the other PBX's extension number via the IVR. In this solution, you need to configure the appropriate outbound route and inbound route in both of the two connected PBXs.
    - Dial to Check Voicemail: Whether to allow users to check voicemail via IVR.

      > Note:
      > This option is for the users who work out of the office. They can call in the PBX and check their voicemail messages via the IVR.
3. Click Key Press Event tab, set the destination based on callers' key presses.
   The following Key Press destination are supported:
    - Hang up
    - Extension
    - Voicemail
    - IVR
    - Ring Group
    - Queue
    - Conference
    - External Number
    - DISA

- Callback
- Fax to Email
- Dial by Name
- Custom Prompt

4. On the Key Press Event page, set the Timeout destination and the Invalid Destination.

- Timeout: If callers do not make an entry within the Prompt Repeat Count, they will be transferred to the Timeout destination.
- Invalid: If callers enter a digit that is not defined in the IVR, they will be transferred to the Invalid destination.

5. Click Save and Apply.

Set an IVR Prompt

When users call in the PBX IVR, the users would operate following the IVR prompt. The PBX system has one default IVR prompt, you can change the IVR prompt to your audio file.

1. Upload a custom prompt or record a custom prompt on the PBX web interface.
2. Go to Settings > PBX > Call Features > IVR, edit your IVR.
3. Select the Prompt to your custom prompt.
4. Set the Prompt Repeat Count.
5. Click Save and Apply.

Related information

[Upload a Custom Prompt (on page 145)]
[Record a Custom Prompt (on page 146)]
[Convert Audio Files Online (on page 148)]
[Convert Audio Files via WavePad (on page 148)]

Change IVR Prompt Clip

If you need to change one audio clip in the IVR prompt frequently, you can divide your IVR prompt to multiple audio clips, and change the desired audio clip when you need to change the IVR prompt.

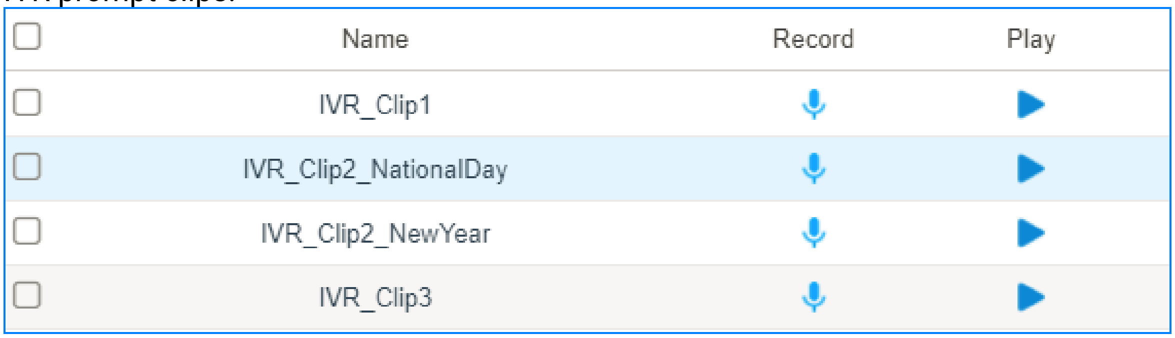
For example, your IVR prompt is like the following:

" Thank you for calling Yeastar. We are currently closed in observance of `Holiday Name`. We will return on `Date`. If you got something urgent, please press 1 to contact our support. To leave a voicemail, please press 2."

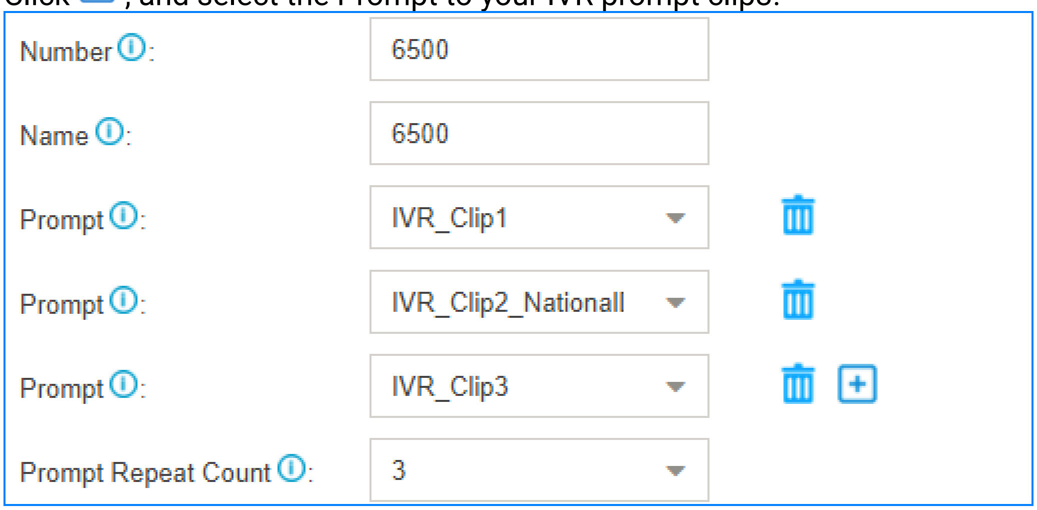
The second sentence is what your would change frequently. You can divide the IVR prompt to 3 clips.

- Clip 1: Thank you for calling Yeastar.
- Clip 2: We are currently closed in observance of `Holiday Name`. We will return on `Date`.
- Clip 3: If you got something urgent, please press 1 to contact our support. To leave a voicemail, please press 2.

1. Go to Settings > PBX > Voice Prompts > Custom Prompts, click Upload to upload your IVR prompt clips.



2. Go to Settings > PBX > Call Features > IVR, edit your IVR.
3. Select the Prompt to the IVR prompt clip1.
4. Click , and select the Prompt to your IVR prompt clip2.
5. Click , and select the Prompt to your IVR prompt clip3.



6. Click Save and Apply.

Next time, when you want to change the IVR prompt, you can change the desired prompt clip instead of changing the whole IVR prompt.

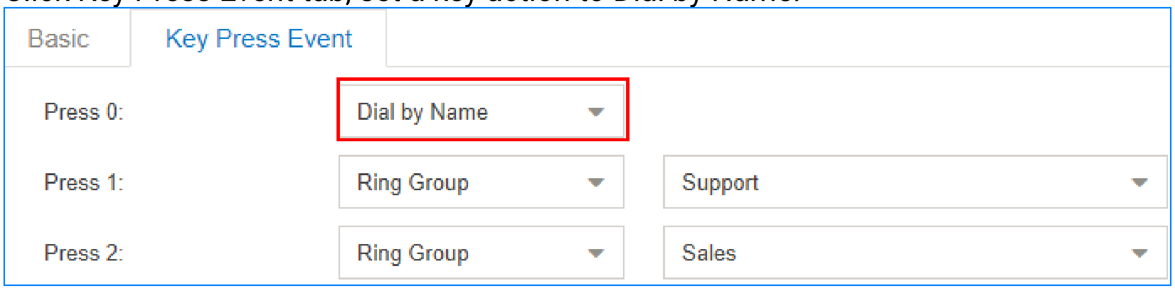
Dial by Name

You can set the IVR Keypress to "Dial by Name", which will allow the callers to find the person by entering the first 3 letters of extensions' first name.

To use Dial by Name, you need to do the followings:

- Specify names for extensions on the PBX.
- Better to instruct the callers to use the feature in the IVR prompt.

1. Go to Settings > PBX > Call Features > IVR, edit your IVR.
2. Click Key Press Event tab, set a key action to Dial by Name.



3. Click Save and Apply.

Forward Incoming Calls to an External Number with IVR

Set the IVR Keypress destination to an external number to route calls from IVR to an external number.

Scenarios

Forward Incoming Calls to an External Number with IVR is typical and important for 24×7 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.

Before you begin

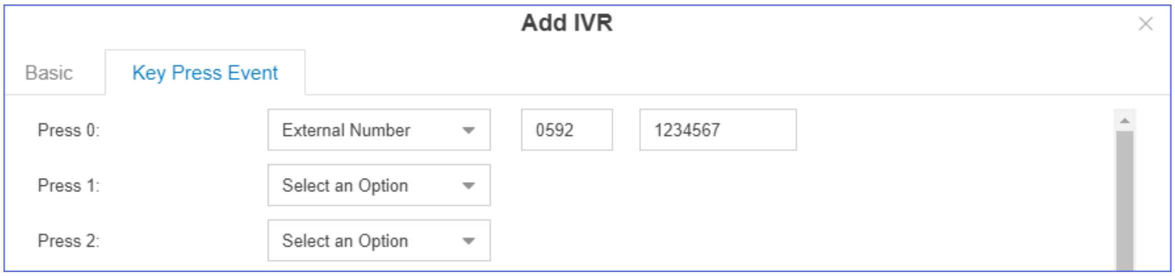
Update your IVR prompt that would instruct callers to press a key to the external number.

To update your IVR prompt, you can upload custom prompt (on page 145) or record custom prompt (on page 146).

Procedures

1. Log in to PBX web interface, go to Settings > PBX > Call Features > IVR, edit your IVR.
2. In the Basic tab, select the updated IVR prompt.

3. In the Key Press Event tab, select a key to set keypress destination to External Number.
4. In the Prefix field, enter prefix of outbound route (on page 82) 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.
5. Enter the external number, such as a Doctor Answering Service number or a mobile phone number.



6. Click Save and Apply.

Ring Group

A ring group helps you to ring a group of extensions in a variety of ring strategies. For example, you could define all the technical support guys' extensions in a ring group and ring the support guys one by one.

Add a Ring Group

1. Go to Settings > PBX > Call Features > Ring Group, click Add.
2. Configure the ring group.
    - Number: Use the default number or change the number.
    - Name: Give a name for the ring group to help you identify it.
    - Ring Strategy:
        - Ring All: Ring all the available extensions simultaneously.
        - Sequentially: Ring each extension in the group one at a time.
    - Seconds to ring each member (s): Define how long the system will wait to ring next member.
    - Members: Select the desired extensions to the Selected box.
    - Failover Destination: Define what will happen if none of the members in the ring group answer the call in the defined time.
3. Click Save and Apply.

Queue

Queues are designed to receiving calls in a call center.

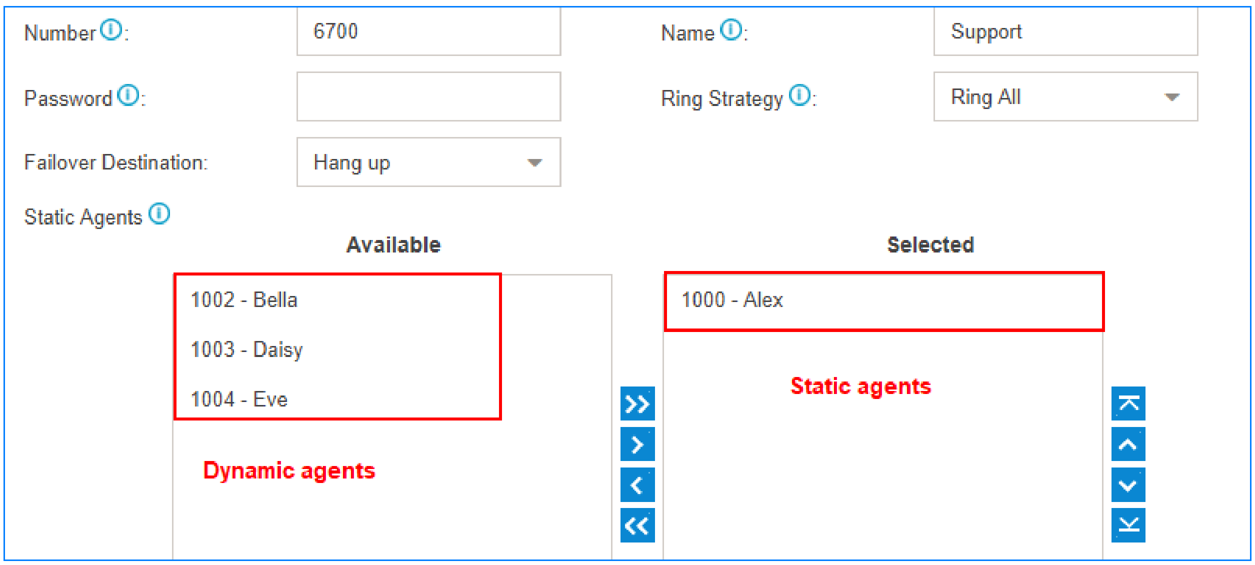
A queue is like a virtual waiting room, in which callers wait in line to talk with the available agent. Once the caller called in PBX and reached the queue, he/she will hear hold music and prompts, while the queue sends out the call to the logged-in and available agents. A number of configuration options on the queue help you to control how the incoming calls are routed to the agents and what callers hear and do while waiting in the line.

Queue Agents

Yeastar S1000-P IPPBX supports dynamic agents and static agents.

- Static Agent: A static agent always stays in a queue to receive incoming calls.
- Dynamic Agent: A dynamic agent can log in a queue or log out a queue at any time.

On the Queue configuration page, the unselected agents act as dynamic agents.



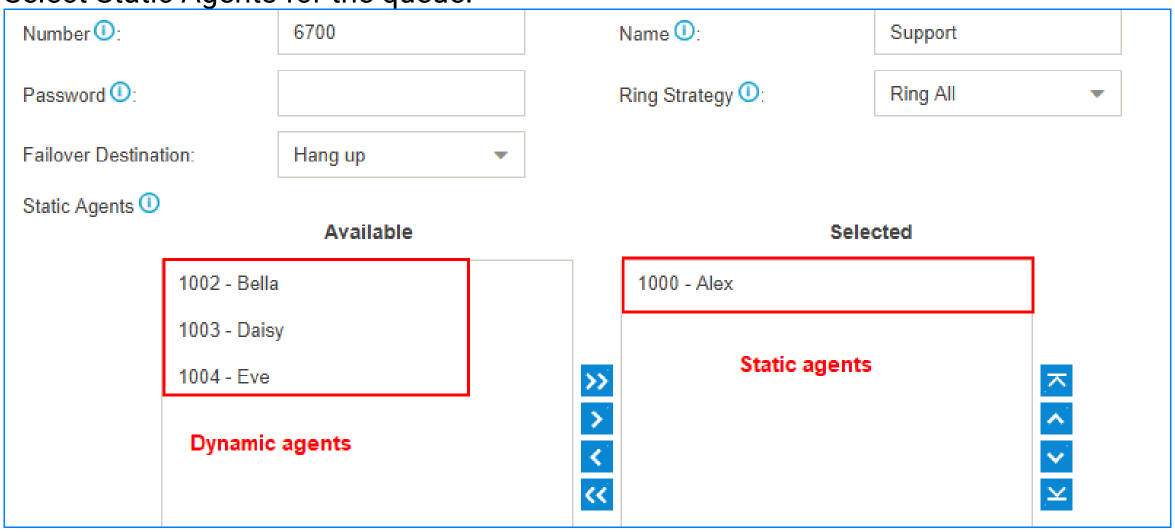
Add a Queue

Add a simple call queue.

1. Go to Settings > PBX > Call Features > Queue, click Add.
2. Specify a Number and Name for the queue.
3. Optional: In the Password field, enter a password for dynamic agent to log in and log out of the queue.
4. Select a Ring Strategy for the call.
    - Ring All: Ring All available Agents simultaneously until one answers.
    - Least Recent: Ring the Agent which was least recently called.
    - Fewest Calls: Ring the Agent with the fewest completed calls.
    - Random: Ring a Random Agent.

- Rrmemory: Ring agents in a round-robin fashion, remembering where it left off in the last ring pass.
- Linear: Ring agents in the order specified in the configuration file, always starting at the beginning of the list.

5. Select Failover Destination, define what should happen if the call does not get answered by an agent.
6. Select Static Agents for the queue.



- Dynamic agents: A dynamic agent can log in or log out a queue at any time.
- Static agents: A static agent will always stay in the queue.

7. Set the Agent Timeout, define how long the phone should keep ringing before it considers the call unanswered by that agent.
8. Click Save and Apply.

It is done for a simple call queue, for more information of queue settings, refer to Queue Settings (on page 108).

Queue Settings

References of basic queue settings and caller experience settings.

Basic Queue Settings

Option	Description
Number	Use this number to dial into the queue, or transfer callers to this number to put them into the queue.
Name	Give this queue a brief name to help you identify it.
Password	You can request agents to enter a password before they can log in to this queue.
Ring Strategy	This option sets the Ring Strategy for this Queue.

Option	Description
	• Ring All: Ring All available Agents simultaneously until one answers. • Least Recent: Ring the Agent which was least recently called. • Fewest Calls: Ring the Agent with the fewest completed calls. • Random: Ring a Random Agent. • Rrmemory: Ring agents in a round-robin fashion, remembering where it left off in the last ring pass. • Linear: Ring agents in the order specified in the configuration file, always starting at the beginning of the list.
Failover Destination	Set the failover destination.
Static Agents	Select static agent of the queue. The static agents will always stay in the queue. Note: • The static agent is not allowed to log in and log out the queue. • The unselected users are dynamic agents.
Agent Timeout	The number of seconds an agent's phone can ring before we consider it a timeout. If you wish to customize, enter the value in the text box directly.
Ring In Use	If unchecked, the queue will avoid sending calls to members whose devices are known to be “in use”.
Agent Announcement	Announcement played to the Agent prior to bridging in the caller.
Retry	The number of seconds to wait before trying all the phones again. If you wish to customize, enter the value in the text box directly.
Wrap-up Time	How many seconds after the completion of a call an Agent will have before the Queue can ring them with a new call .If you wish to customize, enter the value in the text box directly. Input 0 for no delay.

Call Experience Settings

<table>
<tr><td colspan="2">Caller Settings</td></tr>
<tr><td>Music On Hold</td><td>Select the “Music on Hold” playlist for this Queue.</td></tr>
<tr><td>Caller Max Wait Time</td><td>Select the maximum number of seconds a caller can wait in a queue before being pulled out. If you wish to customize, enter the value in the text box directly. Input 0 for unlimited.</td></tr>
<tr><td>Leave When Empty</td><td>If enabled, callers already on hold will be forced out of a queue when no agents available.</td></tr>
<tr><td>Join Empty</td><td>If enabled, callers can join a queue that has no agents.</td></tr>
<tr><td>Join Announcement</td><td>Announcement played to callers once prior to joining the queue.</td></tr>
<tr><td>Agent ID Announcement</td><td>Announcement played to the callers to prompt the agent ID. The agent is who will answer the call.

• [None]: The system will not announce the agent ID.
• [Default]: The system will play the prompt “{extension_number} will be connected. Please wait”. The {extension_number} is the extension number of the agent.
• Custom Prompt: If you choose your custom prompt. The system will play "{extension_number}" + your custom prompt.</td></tr>
<tr><td>Satisfaction Survey Prompt</td><td>When the agent hangs up, the system will play the prompt to ask the caller to rate their satisfaction scale.</td></tr>
<tr><td colspan="2">Caller Position Announcements</td></tr>
<tr><td>Announce Position</td><td>Announce position of caller in the queue.</td></tr>
<tr><td>Announce Hold Time</td><td>Enabling this option causes PBX to announce the hold time to the caller periodically based on the frequency timer. Be this option enabled or not, hold time will be announced after one minute.</td></tr>
<tr><td>Frequency</td><td>How often to announce queue position and estimated hold time.</td></tr>
<tr><td colspan="2">Periodic Announcements</td></tr>
<tr><td>Prompt</td><td>Select a prompt file to play periodically.</td></tr>
<tr><td>Frequency</td><td>How often to play the periodic announcements.</td></tr>
<tr><td colspan="2">Events</td></tr>
</table>

Caller Settings	
Key	Once the events settings are configured, the callers are able to press the key to enter the destination you set. Usually, a prompt should be set on Periodic Announcements to guide the callers to press the key.

Log in/out a Queue

A dynamic agent can log in or log out a queue at any time.

Log in/out a Queue by Feature Code

> **Note:**
> If the static agents try to log out a queue, the system will play a prompt "Agent logged out, goodbye"; But actually, the agent is still in the queue.

- To log in a queue, dial {queue_number}`*`.

  For example, dynamic agent 1000 dials `6700*` to log in the queue 6700.
- To log out a queue, dial {queue_number}`*`.

  For example, dynamic agent 1000 dials `6700*` to log out the queue 6700.

- Dial `*75`queue_number to log in a queue.

  For example, dynamic agent dials `*756700` to log in the queue 6700.
- Dial `*75`{queue_number} again to log out a queue.

  For example, dynamic agent dials `*756700` again to log out the queue 6700.

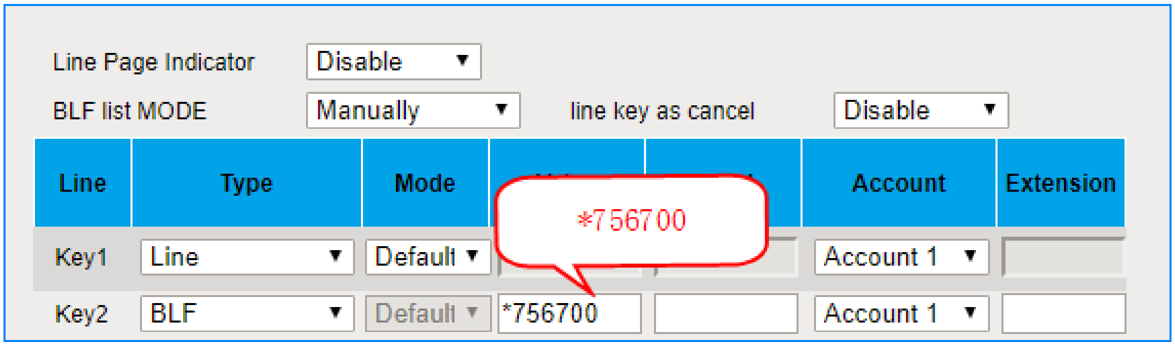
Log in/out a Queue by BLF Key

A dynamic agent can set a BLF key on his/her IP phone to quickly log in or log out a queue.

For example, on the phone of a dynamic agent, set a BLF key to quickly log in or log out queue 6700.

The following instructions are based on the Htek UC912 v2.0.4.4.33.

1. Log in to the phone web interface, go to Function Keys > Line Key.
2. Set a BLF key to log in or log out queue 6700.



  - Type: Set to BLF.
  - Value: The BLF key format is `*75`{queue_number}. In this example, set to `*756700`.
  - Account: Select the account that is registered to the extension number of the agent.
3. Click SaveSet.

Now, the agent can press the BLF key to switch his/her status in the queue.

- When the prompt "agent logged out, goodbye." is played, the agent is logged out of the queue.
- When the prompt "agent logged in, goodbye." is played, the agent is logged in the queue.

Monitor Agent Status by BLF

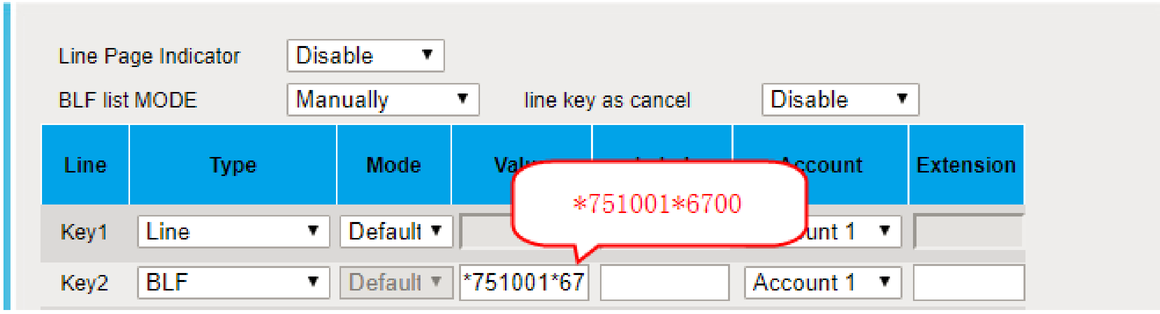
In a call center scenario, a supervisor can set BLF keys to monitor if the agents are in a specific queue. An agent can also set a BLF key to monitor his own status.

This topic is based on the Htek UC912 v2.0.4.4.33.

> Note:
> Monitoring agent status is supported in the firmware version 30.8.0.8 or later.

We will set a BLF key to monitor if the agent 1001 is in the queue 6700 or not.

1. Log in to the phone web interface, go to Function Keys > Line Key.
2. Set a BLF key to monitor extension 1001.



- Type: Set to BLF.
- Value: The BLF key format is `*75`{extension_number`*`{queue_number}. In this example, set to `*751001*6700`.
- Account: Select the account that has an extension registered to the PBX.

3. Click SaveSet.
   Check the BLF LED status:

> Note:
> Different brands of IP phone may have different LED indications.

- Green LED: The agent 1001 is not in the queue 6700.
- Red LED: The agent 1001 is in the queue 6700.
- BLF LED is off: Check if your configurations are correct.

Conference

Conference calls increase employee efficiency and productivity, and provide a more cost-effective way to hold meetings.

Conference members can dial `*` to access the settings options and the admin can kick the last user out and lock the conference room.

Add a Conference

To make a conference call, you should add a conference on the PBX first.

1. Go to Settings > PBX > Call Features > Conference, click Add.
2. On the configuration page, configure the Conference.
   - Number: The extension users need to dial this number to join the conference.
   - Name: Set a name for the conference.
   - Participant Password: Optional. If the password is set, users need to input the correct PIN to join this conference.
   - Wait for Moderator: If this option is checked, the conference participants could not hear each other until the moderator joins the conference.
   - Sound Prompt: Select the sound prompt used for the login and logout of conference members.

    - Allow Participant to Invite: Whether to allow the participants to invite users to join the conference.
    - Moderator Password: The moderator doesn't need to enter a password to join the conference. If a user enters this password to join the conference, he/she will act as the conference moderator.
    - Member Moderators: Select the conference moderators.
3. Click Save and Apply.

Join a Conference

Both the PBX extension users and the external users can join the conference.

1. For the PBX extension users, dial the conference number to join the conference room.
2. For the external users, you need to set the inbound route destination to a conference first, then the external users call to the PBX, their calls will be routed to the conference.

Call Pickup

Call Pickup is a feature that allows a user to answer an incoming call that rings on a telephone other than the user's own.

Extension Call Pickup

When a user wants to pick up a call that is ringing at the other extension that is not in the same pickup group, the user can dial "Extension Pickup feature code (default *04) + Extension Number" to pick up the call.

Extension Call Pickup Feature Code

The default Extension Call Pickup feature code is *04.

You can change the code on Settings > PBX > General > Feature Code > Extension Pickup.

Operation

Dial `*04`{extension_number} to pick up a call.

For example, the ringing extension number is 1000, you should dial *041000 to pick up the call.

Pick up an Extension's Call by BLF

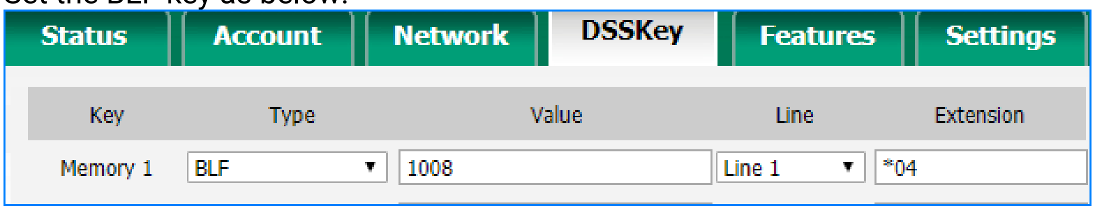
You can set a BLF key of Extension Call Pickup on your phone. The BLF key will show the real-time status of the extension. When the extension is ringing, you can press the BLF key to pick up the call.

We take Yealink T27G v69.82.0.20 as an example below.

1. Set a BLF key to monitor and pick up an extension.

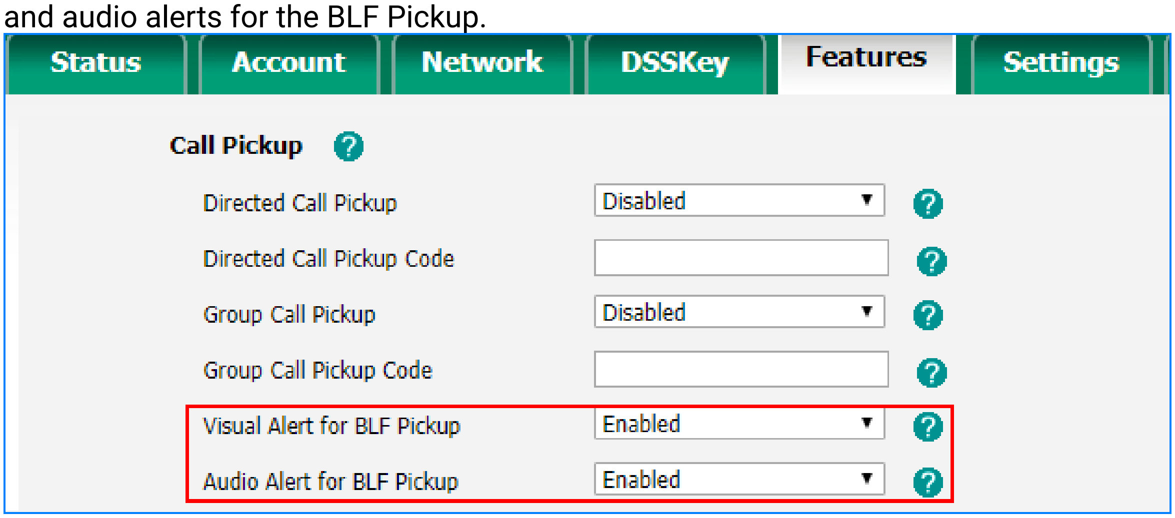
   a. Log in to the phone web interface, go to Dsskey page.

   b. Set the BLF key as below.



   - Type: Select BLF.
   - Value: Enter the extension number that you want to monitor.
   - Line: Choose the line where your extension is registered.
   - Extension: Enter the feature code of extension pickup. The default code is *04.

   c. Click Confirm.
2. To get notified when the monitored extension has an incoming call, set visual alerts and audio alerts for the BLF Pickup.



   a. On the phone web page, go to Phone > Features > Call Pickup.

   b. In the Visual Alert for BLF Pickup, select Enabled.
   When a call reaches the monitored extension, you can see the incoming caller ID on your phone.

c. In the Audio Alert for BLF Pickup, select Enabled.

A “beep” sound will remind you of an incoming call for the monitored extension.

d. Click Confirm.

If your configuration is correct, the BLF LED will turn green.

When the monitored extension has an incoming call, the followings occur on your phone, press BLF key to pick up the call.

- The phone plays a warning tone.
- The BLF LED turns red.

Group Call Pickup

If extension users are in the same pickup group, they can dial the Group Call Pickup feature code (default *4) to pick up group members' incoming call.

Group Call Pickup Feature Code

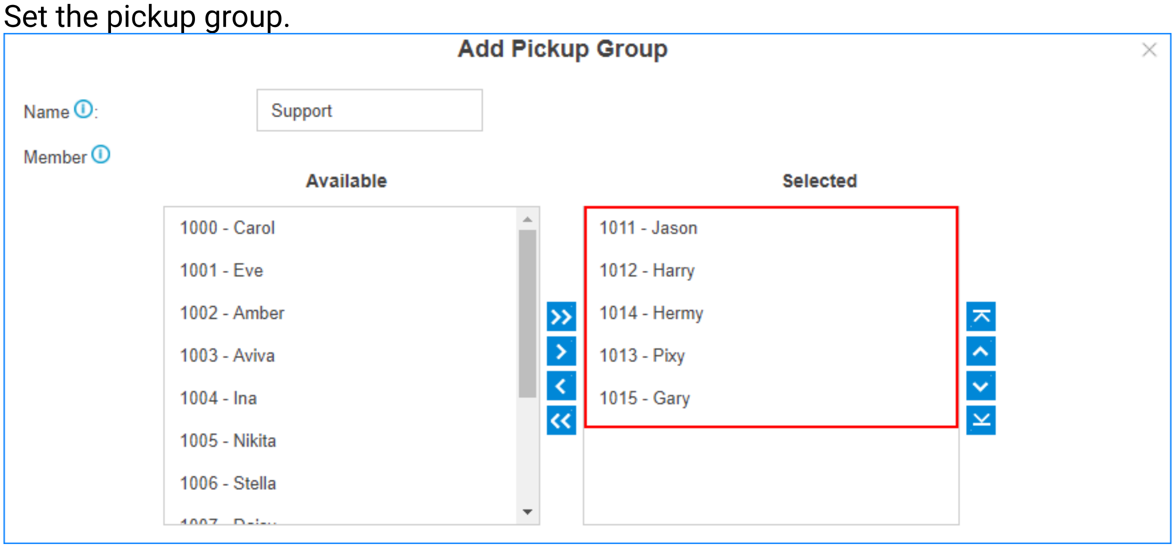
The default Group Pickup feature code is *4.

You can change the code on Settings > PBX > General > Feature Code > Call Pickup.

Add a Pickup Group

Generally, You can set the extension users who are in the same department in a pickup group.

1. Go to Settings > PBX > Call Features > Pickup Group, click Add.
2. Set the pickup group.



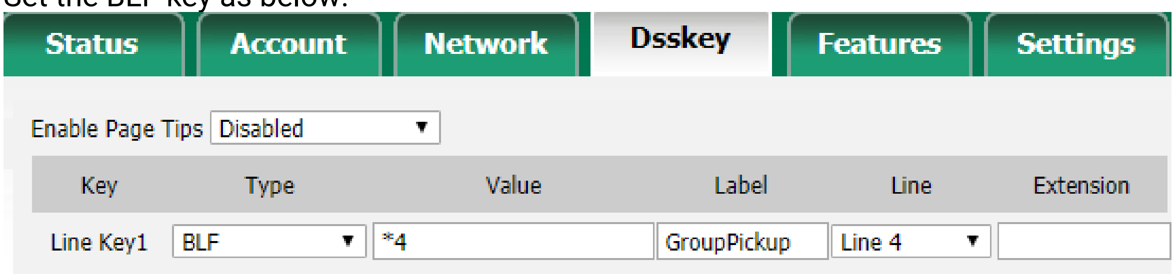
    - Name: Give the group a name to help you identify it.
    - Member: Select the desired extensions from Available box to Selected box.
3. Click Save and Apply.

Pick up A Group Member's Call by BLF

You can set a BLF key for Group Call Pickup on your IP phone. When your group member's phone is ringing, you can press the BLF key to quickly pick up the call.

We take Yealink T27G v69.82.0.20 as an example below.

1. Log in to the phone web interface, go to Dsskey page.
2. Set the BLF key as below.



    - Type: Set to BLF.
    - Value: Enter the feature code of group pickup. The default code is *4.
    - Label: Set a label that you want to display on the phone screen.
    - Line: Choose the line where your extension is registered.
3. Click Confirm.
   If your configuration is correct, the BLF LED will turn green.

Call Transfer

Yeastar S1000-P IPPBX supports Attended Transfer and Blind Transfer, users can dial the feature code to transfer a call on their phones.

Attended Transfer (Default feature code *3)

An attended transfer, also called consult transfer or warm transfer, is when you speak with the new person before the call is transferred. You can tell the new person about the caller's issue and give any background information before transferring the call (without the caller hearing).

Blind Transfer (Default feature code *03)

A blind transfer is when you transfer the caller to another person without speaking to the new person first.

Attended Transfer

If you want to tell the new person about the caller's issue and give any background information before transferring the call, you can choose attended transfer.

Scenario: You (B) are talking with A, then transfer the call to C.

1. During the call with person A, dial *3 on your phone.
   You will hear the prompt "transfer" and the dial tone.
2. Dial C's number.
   C's phone is ringing. After C answers the call, the call between you and C is established. In this time, the call between you and A is held.
3. Hang up your call, the call between A and C is established.

Blind Transfer

If you don't need to consult the new person who you want to transfer the call to, you can perform a blind transfer. Your call will be ended after you transfer the call.

Scenario: You (B) are talking with A, then transfer the call to C.

1. During the call with person A, dial *03 on your phone.
   You will hear the prompt "transfer" and the dial tone.
2. Dial C's number and hang up.
   C's phone is ringing. After C answers the call, the call between A and C is established.

Busy Camp-on

Busy Camp-on is a busy-call handling method. When the callee's phone is busy, the caller can camp the call on PBX, the PBX informs the caller as soon as the callee's phone becomes available, and re-establishes the call to save the caller's waiting time.

Prerequisites

- The Busy Camp-on feature is only applicable to the call between extensions.
- Call Forwarding When Busy (on page 35) is disabled for the callee's extension.
- Call Waiting (on page 37) is not enabled for the callee's extension.

Enable Busy Camp-on for extension

1. Log in to the PBX web interface, go to Settings > PBX > Extensions, edit a desired extension.
2. Click Features tab.
3. Select the checkbox of Enable Busy Camp-on.
4. Click Save and Apply.

Sample Application

John and Tom are in different offices, John uses extension 1000, and Tom uses extension 1001.

1. John calls Tom.

   Tom is busy in a call or cannot answer the incoming call
2. John hears a busy prompt, and presses 1 to camp on the call.

   > Tip:
   > If John hangs up the call directly, John can also dial “*791001” to camp the call on; and dial "*079" to cancel.
3. The PBX calls John as soon as Tom hangs up and his extension becomes available.
4. When John answers the call from PBX, the PBX will recall Tom.
5. Tom answers the call from PBX. The call will be established between John and Tom.

Busy Camp-on code

The caller can also dial camp-on code followed by the callee number to camp on a call.

Log in to the PBX web interface, go to Settings > PBX > General > Feature Code, you can view or change the busy camp-on code.

The default busy camp-on code:

- Enable Busy Camp-on code: *79
- Disable Busy Camp-on code: *079

Manager and Secretary

Yeastar Manager and Secretary feature allows the secretary to filter the calls for the manager. The secretary can answer incoming calls on behalf of a manager, and transfer the calls to the manager if he/she agrees to answer.

Assign a secretary to a manager

Procedure

1. Log in to the PBX web interface, go to Settings > PBX > Extensions, edit the manager's extension.
2. Click Features tab.
3. In the Manager Extension Settings section, select the checkbox of Enable Manager Extension.
4. In the Secretary Extension drop-down list, select the secretary's extension.
5. Click Save and Apply.

Result

All incoming calls to the manager's extension will be forwarded to the secretary's extension.

The secretary answers the call and decides if the call is important enough to disturb the manager. The secretary can perform an attended transfer to contact with the manager if he/she is available to take the call. If the manager is available to take the call, the secretary can transfer the call to the manager directly.

Manager and Secretary feature code

After enabling the Manager and Secretary feature and assign a secretary extension to the manager extension on the extension configuration page, you can dial the feature code of Manager Extension Settings on the manager extension to directly enable or disable this feature.

Log in to the PBX web interface, go to Settings > PBX > General > Feature Code, you can view or change the Manager extension feature code.

The default Manager and Secretary feature codes are as follows:

- Enable Manager Extension: *76
- Disabled Manage Extension: *076

After a beep tone, the feature status is successfully changed.

Callback

Callback feature allows callers to hang up and get called back to the PBX. Callback feature could reduce the cost for the users who work out of the office using their own mobile phones.

Set up Callback

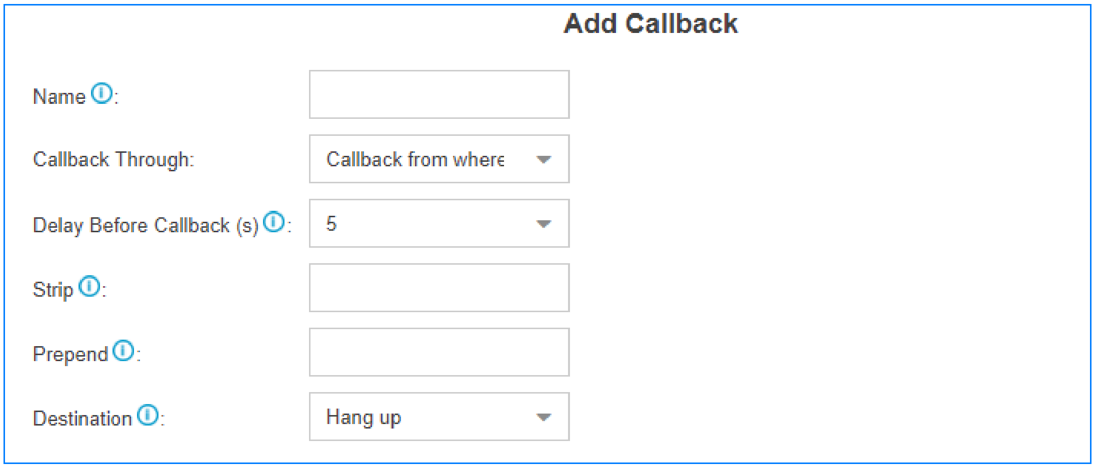
Add a Callback rule and set Inbound Route destination to the Callback rule.

> Note:
> Make sure that the Caller ID service is enabled on the callback trunk. If the PBX cannot recognize the inbound caller ID, callback will fail.

1. Add a Callback rule.

    a. Go to Settings > PBX > Call Features > Callback, click Add.

    b. On the Callback configuration page, finish the callback settings.



- Name: Set a name for the Callback.
- Callback Through: Select which trunk to use when calling back.

> Note:
> Make sure that you have set up an outbound route for the trunk, or callback would fail. If the Register-Trunk is used for Callback, make sure the From User is configured, or callback would fail.

- Delay Before Callback: How long to wait before calling back the caller.
- Strip: Optional. How many digits will be stripped from the call in number before the callback is placed.

> Note:
> You do not need to configure Strip if the trunk supports calling back with the Caller ID directly.
>
> For example, user 5503301 calls in the PBX, the caller ID displays 05503301. To call back to the user, you should set strip 1 digit so that the PBX will call back to 5503301.

- Prepend: Optional. The digits to prefix to the callback number before the callback is placed.

> Note:
> You do not need to configure Prepend if the trunk supports calling back with the Caller ID directly.
>
> For example, user 15880232154 calls in the PBX, the caller ID displays 15880232154. To call back to the long-distance number 15880232154 through the selected trunk, you should add digit 9 before the number. In this case, set Prepend to 9.

- Destination: Where the callback will direct the caller.

c. Click Save and Apply.

2. Set Inbound Route destination to callback.

a. Go to Settings > PBX > Call Control > Inbound Route, edit your inbound route.

b. Set the Inbound Destination to the Callback.

c. Click Save and Apply.

3. Test callback.
Make an inbound call to the PBX trunk, after you hear the ring tone, hang up the call, the PBX will call back to you.

Speed Dial

Sometimes you may just need to call someone quickly without having to look up his/her phone number. You can achieve this by simply defining a shortcut number. You can use Speed Dial feature to place a call by pressing a reduced number of keys.

Add a Speed Dial Number

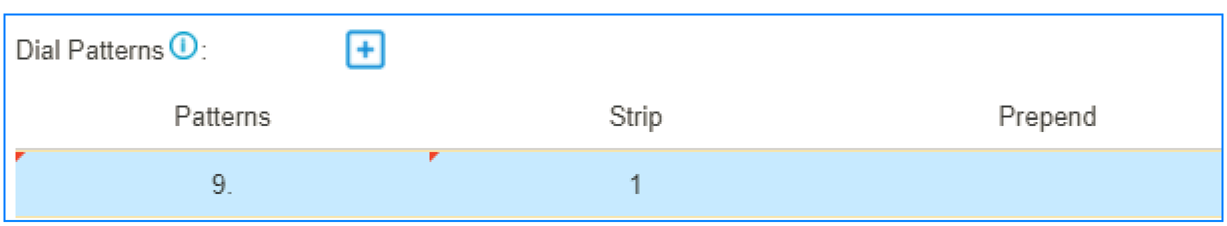
1. Go to Settings > PBX > Call Features > Speed Dial, click Add.
2. On the configuration page, configure the Speed Dial.
   - Speed Dial Code: Speed dialing number.
   - Phone Number: The phone number that you want to call.

> Note:
> You need to add the outbound dial prefix before the phone number if you want to call an external number.

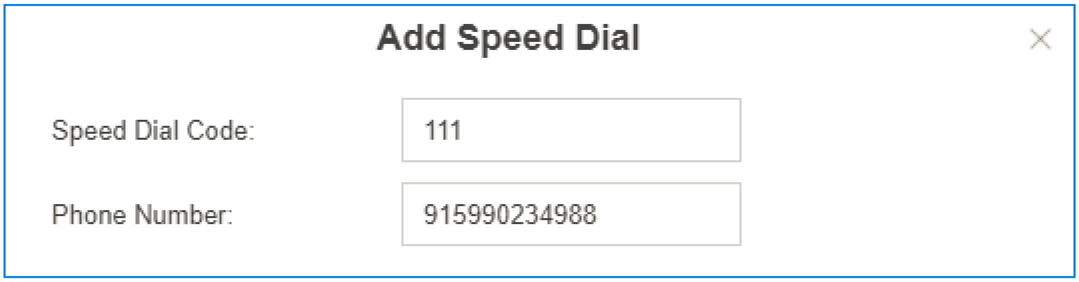
3. Click Save and Apply.

Speed Dial Example

Assume that you have an outbound route set as below, and you will dial speed number 111 to reach an external number 15990234988 through the route.



You need to set the Speed Dial as below:



Dial *99111 on your phone to call the number 15990234988. *99 is the default feature code for speed dial.

DISA

Direct Inward System Access (DISA) allows users outside the office to make calls through the PBX's trunks. For the staffs who are outside the office, they can use DISA feature to take advantage of lower long-distance rates that are provided by the PBX trunks.

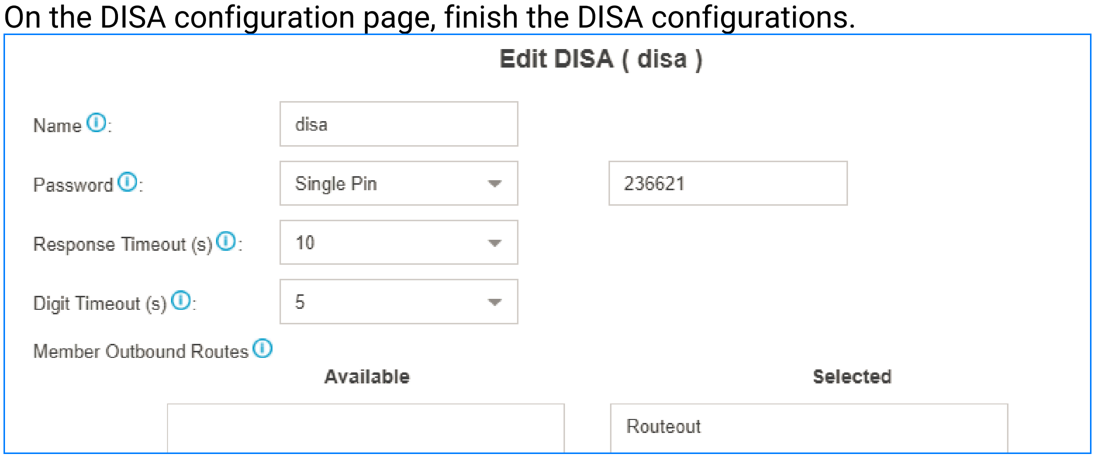
Set up DISA

Add a DISA and set the Inbound Route destination to DISA.

1. Add a DISA.

    a. Go to Settings > PBX > Call Features > DISA, click Add.

    b. On the DISA configuration page, finish the DISA configurations.



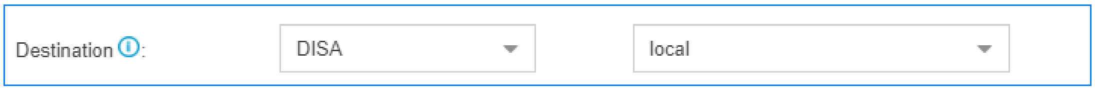
- Name: Set the DISA name.
- Password: Set password for the DISA.
- Response Timeout: The maximum amount of time it will wait before hanging up if the user has dialed an incomplete or invalid number.

        - Digit Timeout: The maximum amount of time permitted between digits.
        - Member Outbound Routes: Select the outbound routes that can be accessed from the DISA.

    c. Click Save and Apply.
2. Set Inbound Route destination to DISA.

    a. Go to Settings > PBX > Call Control > Inbound Route, edit your inbound route.

    b. Set the Inbound Destination to the DISA.



    c. Click Save and Apply.
3. Test DISA.
    a. Make an inbound call to the PBX, you will get a dial tone after inputting a correct DISA pin code.
    b. Dial the external number that you want to call.

Intercom/Paging

The Paging and Intercom features allow you to make an announcement to a group of extensions. The called parties do not need to pick up the handset as the audio will be played via the phone speakers.

Set up 1-Way Paging

Paging is used to make an announcement over the speakerphone to a phone or group of phones. The called parties will not ring, but instead answer immediately into speakerphone mode.

> Note:
> Paging is typically one way for announcements only.

1. Go to Settings > PBX > Call Features > Paging/Intercom > Paging/Intercom, click Add.
2. Set a 1-Way paging group.
    - Number: Use the default or specify a number for the paging group.
    - Name: Enter a name for the paging group.
    - Type: Choose 1-Way Paging.
    - Dial * to Answer: This feature is NOT supported for 1-Way paging. If this option is checked, the group announcement will be terminated directly when a member dials `*`.
    - Member: Choose the group members to the Selected box.
3. Click Save and Apply.

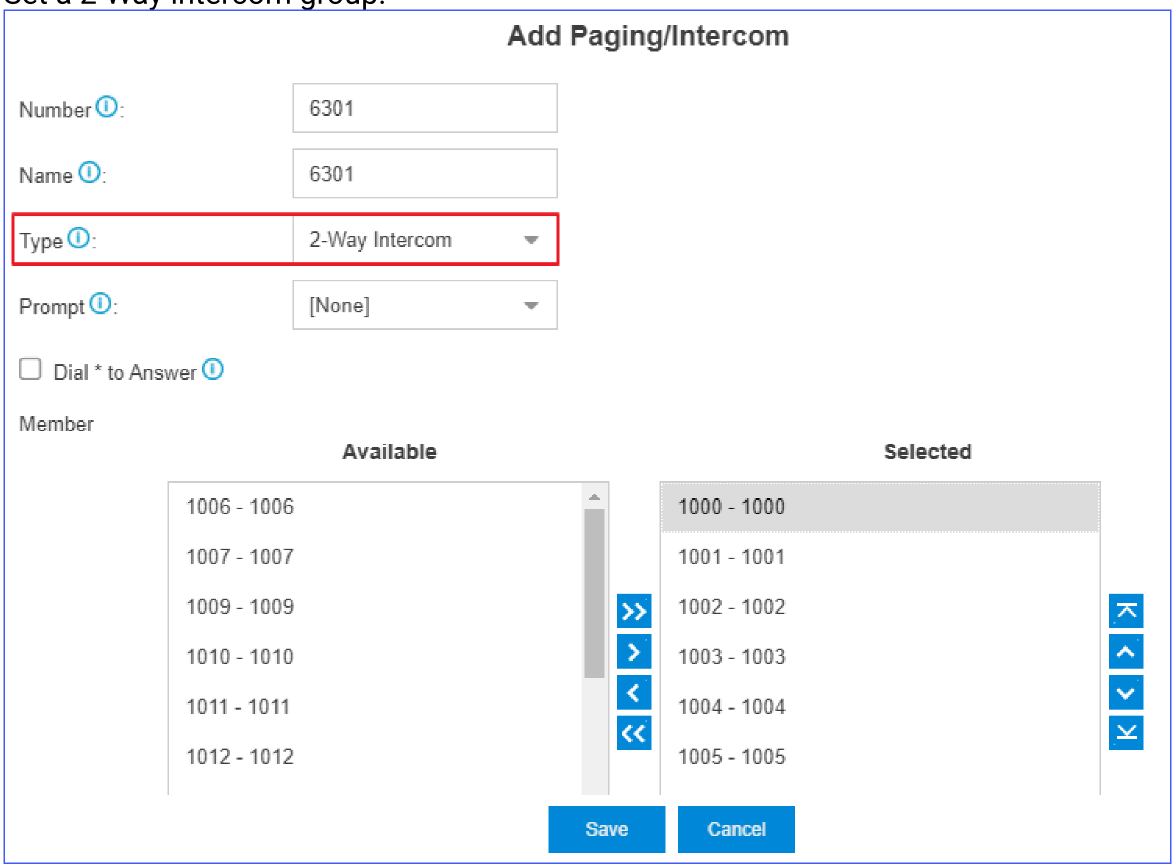
When you dial the paging group number, the members in the group will hear the announcement.

Set up 2-Way Intercom

2-way intercom is used to make a multi-party conference. The called parties will automatically answer the call into speakerphone mode and join the conference.

> Note:
> Intercom allows all users in the group to talk and be heard by all.

1. Go to Settings > PBX > Call Features > Paging/Intercom > Paging/Intercom, click Add.
2. Set a 2-Way intercom group.



- Number: Use the default or specify a number for the intercom group.
- Name: Enter a name for the intercom group.
- Type: Choose 2-Way Intercom.
- Dial * to Answer: If this option is checked, the intercom group members can dial `*` to talk to the intercom initiator.

> **Note:**
> When a member dials `*`, the group announcement will terminate, and the member who dials `*` can have a private call with the intercom initiator.

- Member: Choose the group members to the Selected box.

3. Click Save and Apply.

When you dial the intercom group number, the members in the group will automatically join the conference by speakerphone mode.

Set up 1-Way Multicast Paging

Multicast Paging allows you to easily and quickly broadcast instant audio announcements to phone users who are listening to the same multicast IP address of the PBX.

When you make a Multicast Paging, the PBX sends Real-time Transport Protocol (RTP) streams to the IP phones without involving SIP signaling. The phones that receive the RTP streams don't need to register SIP extensions.

> **Note:**
>
> - The IP phone that will receive 1-way multicast paging should support Multicast Paging feature.
> - The Multicast Paging is one-way audio call.
> - IPv6 network does NOT support this feature.

1. Set a 1-way Multicast Paging on the PBX.

    a. Go to Settings > PBX > Call Features > Paging/Intercom > Paging/Intercom, click Add.

    b. Set a 1-Way multicast paging.

- Number: Use the default or specify a number for the paging group.
- Name: Enter a name for the paging group.
- Type: Choose 1-Way Multicast Paging.
- IP of Multicast Channel: Enter the multicast IP address and port (e.g. 224.255.255.255:1000).

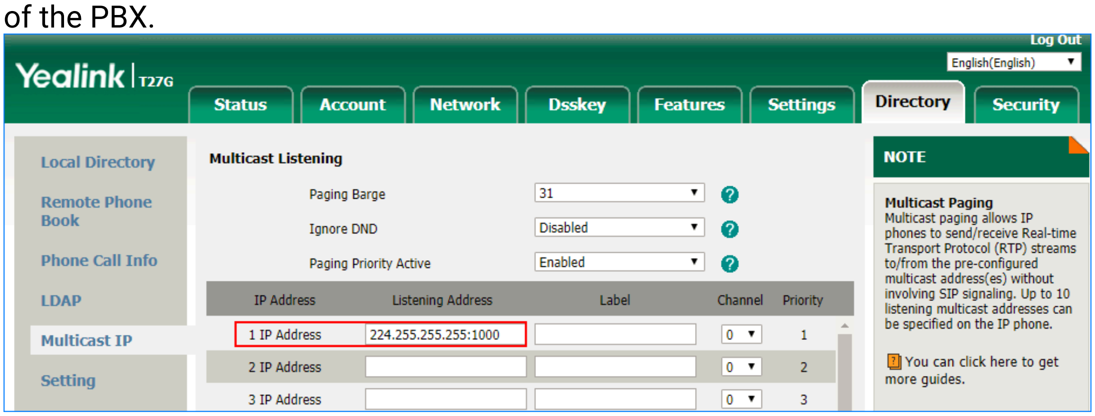
> Note:
> The range of multicast IP address is 224.0.0.0 - 239.255.255.255.

c. Click Save and Apply.

2. Set Multicast Paging on each of your IP phone.
   In the following, we take Yealink T27G as an example.

   a. Log in to the phone web interface, go to Directory > Multicast IP.

   b. In the Multicast Listening section, enter the same multicast IP address and port of the PBX.



   c. Click Confirm.

When you dial the paging group number, the members in the group will automatically answer the call into speakerphone mode.

> Note:
> If the multicast paging doesn't work, check the following:
>
> - Multicast IP address and port are in the correct range.
> - If the PBX and IP phones are in different IP segments (e.g. PBX is in `192.168.5.X` IP segment, IP phones are in `192.168.3.X` IP segment), check if your router supports IP Multicast in different IP segments.

Make an Announcement to a Specific User

Extension users can dial the intercom feature code to make an intercom to a specific extension, the called party can respond immediately without picking up the handset.

The default Intercom feature code is *5.

> Note:
> In this way, the audio is two way, both the caller and called party can hear each other.

Extension user 2000 makes an intercom call to extension user 1000.

1. Dial `*51000` on the phone of extension 2000.

   The call on extension 1000 will be answered automatically.

Call Parking

Call Parking is a feature that allows you to suspend a call for an extended period of time and then retrieve that call from any extension.

Scenario

During a call with clients, extension users may need to check information somewhere else. In such case, extension users can park the call temporarily and retrieve the call by any extensions when getting things done.

Settings of Call Parking

Go to Settings > PBX > General > Feature Code > Call Parking, you can modify the feature code, parking extension range, and parking time.

We provide default settings of call parking as follows.

Settings	Descriptions
Call Parking	The default feature code is `*6`. During a call, dial `*6` on your phone, the system will automatically assign a parking slot number to the call.
Directed Call Parking	The default feature code is `*06`. During a call, dial "`*06`+parking slot number", the call will be parked to the designated parking slot number.
Parking Extension Range	Specify the range of parking extension where a call will be parked. The default value is 6900-6999. Note: The rang of parking extension must be different from existing extension ranges (Settings > PBX > General > Preferences > Extension Preferences).
Parking Timeout (s)	Specify the time that a call can be parked before it is retrieved by other extensions. The default value is 60s. Note: Parking Timeout must be longer than 30s.
Timeout Destination	If a parked call hasn't been retrieved before the parking timeout, PBX will route the call to the designated destination. • Original Parker: The call will be routed to the user who parks this call. • Extension: The call will be routed to the designated extension number. • Extension's Voicemail: The call will be routed to the designated extension's voicemail. • Custom Number: The call will be routed to the designated number.

Call Parking (Default feature code: *6)

You can dial the feature code of Call Parking to get the parking slot number, then dial the parking slot number on another phone to retrieve the call.

Example:

1. During a call, dial *6 on your phone, the system will prompt you that the parking slot number is 6900.
2. Dial 6900 on another phone to retrieve the call.

Direct Call Parking (Default feature code: *06)

If you get a parking slot number from your administrator, you can dial the “feature code of Direct Call Parking + parking slot number" to park the call to the slot.

Example:

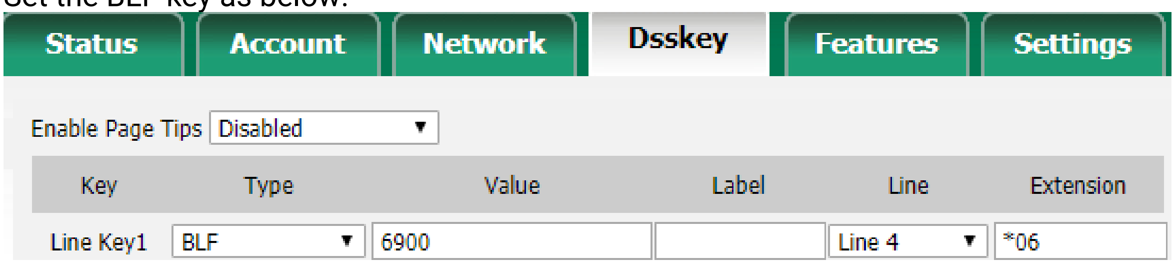
1. During a call, dial *066900 to park the call to slot 6900.
2. Dial 6900 on another phone to retrieve the call.

Park Calls by BLF

You can set a BLF key of Call Parking on your phone. The BLF key will show the real-time status of the parking slot. If the parking slot is vacant, you can press the BLF key to park a call to the parking slot.

We take Yealink T27G v69.82.0.20 as an example below.

1. Log in to the phone web interface, go to Dsskey page.
2. Set the BLF key as below.



    - Type: Select BLF.
    - Value: Enter the parking slot number.
    - Line: Select the line where your extension is registered.
    - Extension: Enter the feature code of Direct Call Parking. The default code is *06.
3. Click Confirm.

- When the parking slot is vacant, the BLF LED is green.

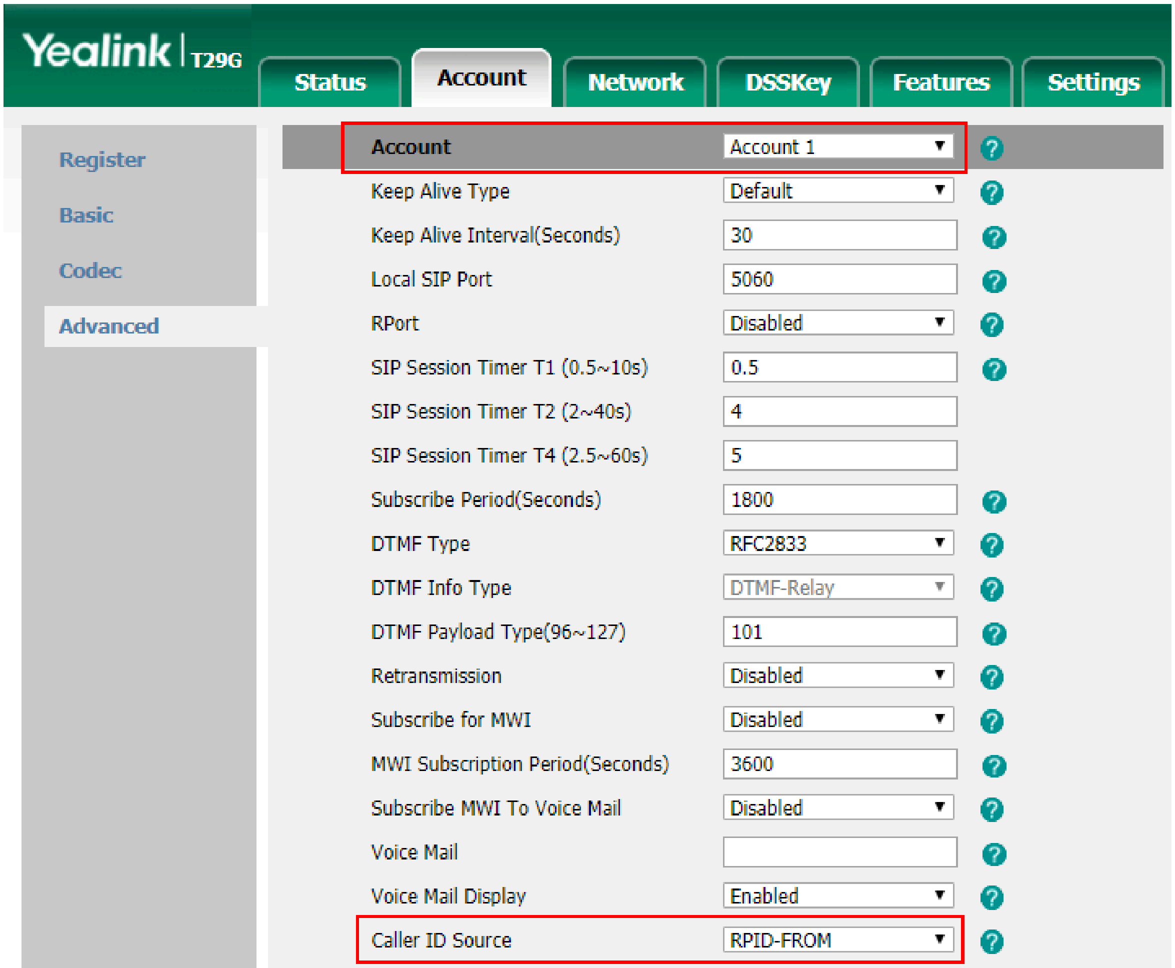
  Press the BLF key to park a call to the parking slot.
- When the parking slot is occupied, the BLF LED is red.

Configure Call Parking Caller ID

By default, when you retrieve a parked call, the call-park slot number (e.g. 6900) will be displayed on the phone. To display the original caller ID of the user who you were talking to, you need to configure SIP settings to get caller ID from Remote- Party-ID SIP header.

1. On PBX, enable Send Remote Party ID.
    a. Go to Settings > PBX > General > SIP > Advanced.
    b. Check the option Send Remote Party ID.
    c. Click Save and Apply.
2. On the IP phone that you will use to retrieve a parked call, configure the Caller ID Source.

> Note:
> We take Yealink T29G v46.83.0.50 as an example below.

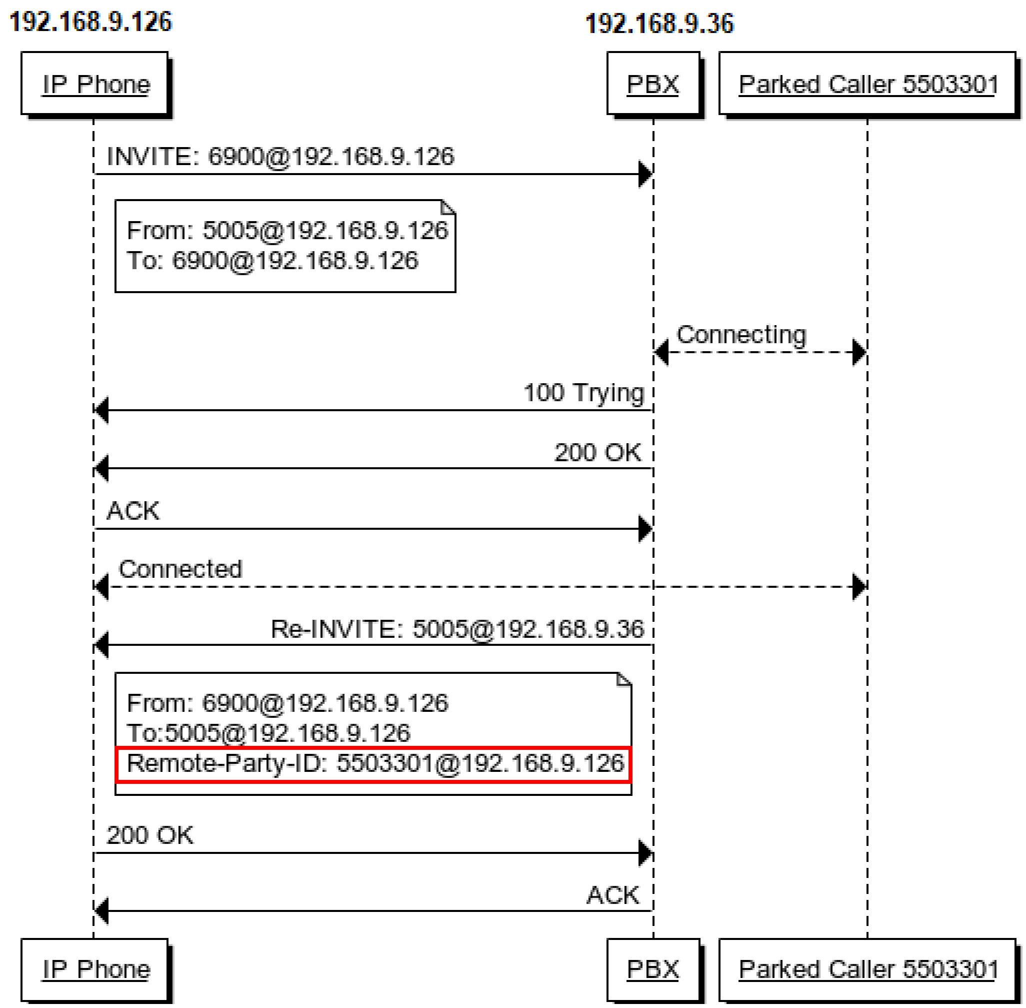


    a. Log in to the phone web interface, go to Account > Advanced.
    b. In the Account drop-down list, select the account where the extension is registered.
    c. In the Caller ID Source field, select RPID-FROM.
    d. Click Confirm.

Test call parking. When you retrieve the parked call from the IP phone, the phone screen will display the parking slot number for 1 or 2 seconds, then display the original caller ID.

The following call flow shows how the IP phone gets caller ID when a user retrieves a parked call.

1. A user dials parking slot number 6900 on IP phone to retrieve a parked call.
2. PBX sends a Re-INVITE packet that contains Remote-Party-ID.
3. The IP phone gets the caller ID from the Remote-Party-ID header.



Fax

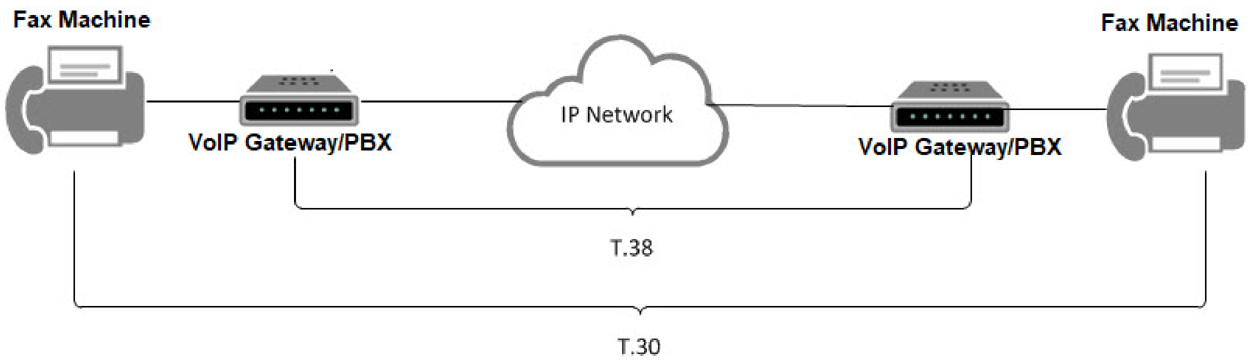
Yeastar S1000-P IPPBX supports Fax over IP. You can send or receive a fax via a physical fax machine or receive a fax over the network.

What is T.38 Fax over IP?

T.38 is a protocol for sending faxes over a Voice over IP (VoIP) network or the Internet in re-al time.

T.38 protocol defines the transport of data (a fax) between PSTN fax terminals through a fax gateway, between two Internet-aware fax terminals, or from a PSTN fax terminal through a fax gateway to an Internet-aware fax terminal. A T.38 stream is sometimes referred to as Fax over IP (FoIP).

PSTN fax terminals traditionally use the T.30 protocol to send analog data. To exchange analog fax data with a PSTN terminal over the Internet, the T.38 protocol first converts analog data into digital data. The protocol then converts the data back to analog on the receiving end if the receiver is a PSTN fax terminal.



T.38 Fax Settings

If the Fax over IP doesn't work, you can go to Settings > PBX > General > SIP > T.38 to change the T.38 settings.

- No T.38 Attributes in Re-invite SDP

  If this option is enabled, no T.38 attributes will be added in re-invite SDP packet.

- Error Correction

  Error Correction Mode (ECM) for the Fax.

- T.38 Max BitRate

  T38 Max Bit Rate.

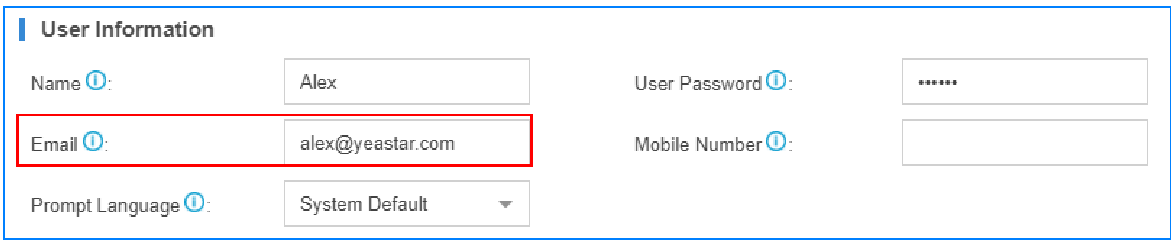
Fax to Email

Fax to Email feature helps you receive faxes on your smart phone or computer. Yeastar S1000-P IPPBX will convert the received fax and forward it to an extension user's email.

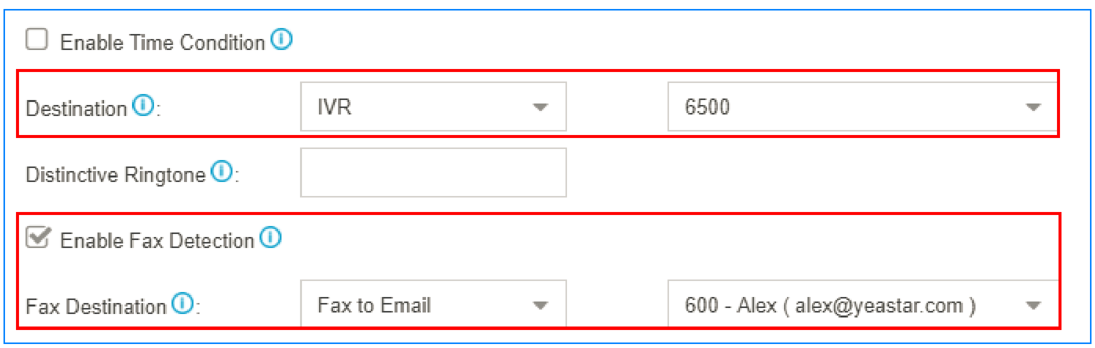
Steps to Configure 'Fax to Email'

1. Configure the PBX System Email.

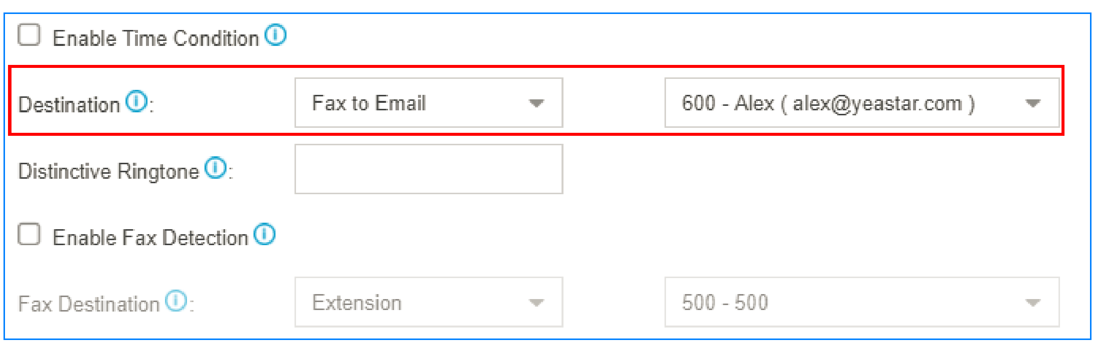
   Make sure the PBX system email works, or the PBX cannot forward the received faxes to an extension user's email.
2. Check if the extension user's email is configured.



3. Configure the destination of your inbound route.
   - If you want to receive fax via fax detection (on page 135), set the Destination to IVR, and set Fax Destination to Fax to Email.



   - If you want to receive fax through a private trunk (on page 135), set the Destination to Fax to Email.



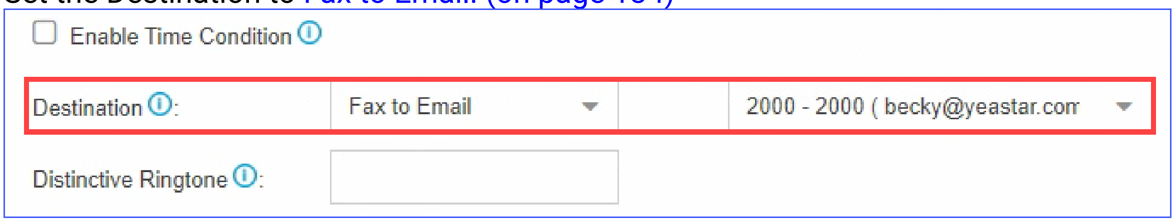
Receive Fax through a Dedicated Trunk

You can assign one or more trunks to receive faxes, and tell your customers to send faxes to the dedicated trunk number.

1. Go to Settings > PBX > Call Control > Inbound Route, click Add.
2. On the configuration page, select the dedicated trunk to the Selected box.

> Note:
> The selected trunk will be used to receive faxes only, users cannot make audio calls through the selected trunk.

3. Set the Destination to Fax to Email. (on page 134)



4. Click Save and Apply.

Users can dial the number of the dedicated trunk, then send fax to the PBX.

Receive Fax via Fax Detection

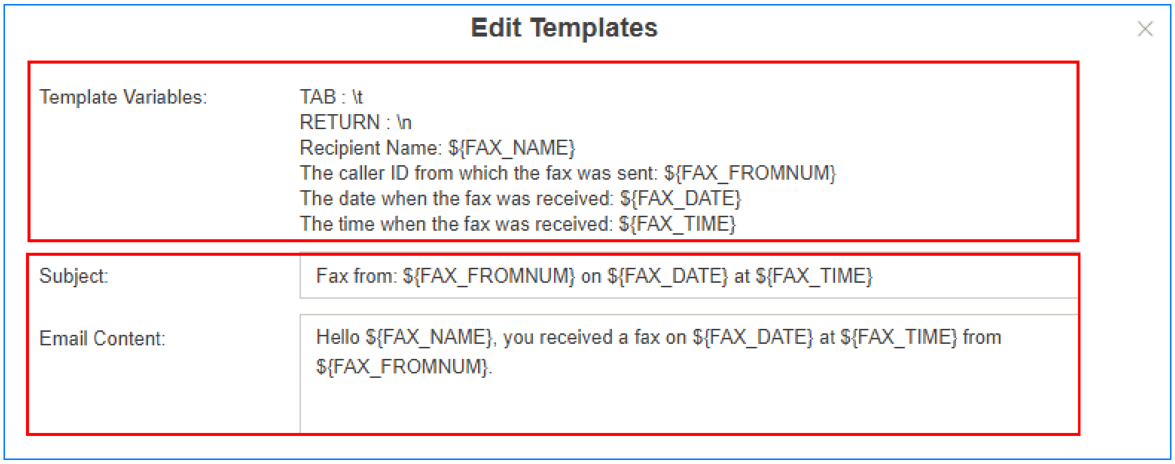
If you want to receive calls and also receive faxes through a trunk, you can set fax detection on your inbound route.

1. Go to Settings > PBX > Call Control > Inbound Route, configure your inbound route.
2. Select the trunk to the Selected box.
3. Set the Destination to `IVR`.
4. Select the checkbox of Enable Fax Detection.
5. Set the Fax Destination to Fax to Email (on page 134).
6. Click Save and Apply.

Edit 'Fax to Email' Template

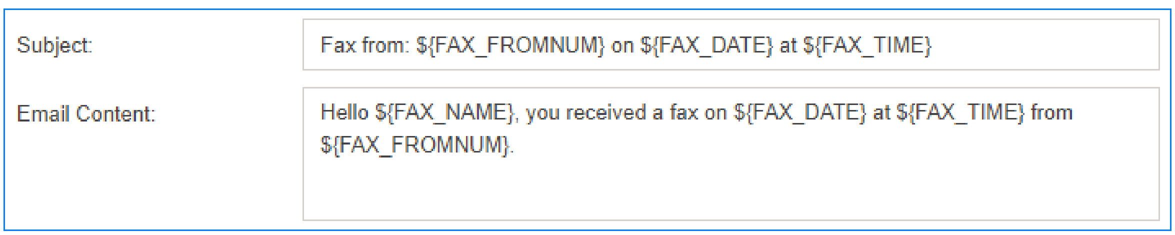
The PBX has a default email template for Fax to Email. You can edit the template according to your needs.

1. Go to Settings > System > Email > Email Templates, click beside Fax to Email.
   On the Edit Template page, the description of variables and the default email contents are displayed.



2. Edit the email subject and email contents.

> **Note:**
> The variable names are unchangeable.



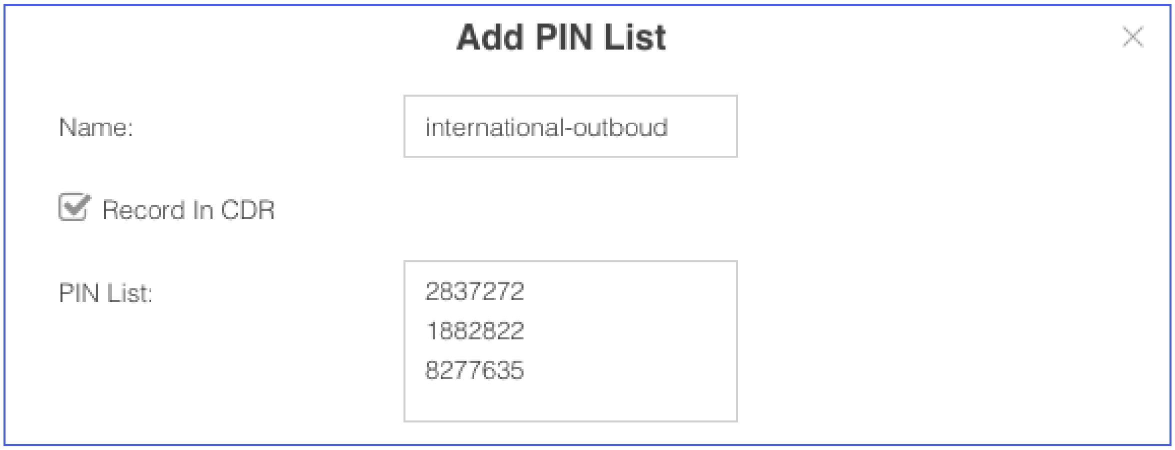
3. Click Save and Apply.

PIN List

PIN List is used to manage lists of PINs (numerical passwords) that can be used to access restricted features such as outbound route (on page 81) and DISA (on page 123).

Add a PIN list

1. Go to Settings > PBX > Call Features, click More to display more call features.
2. Click PIN List.
3. On the Add PIN List page, configure the following settings:

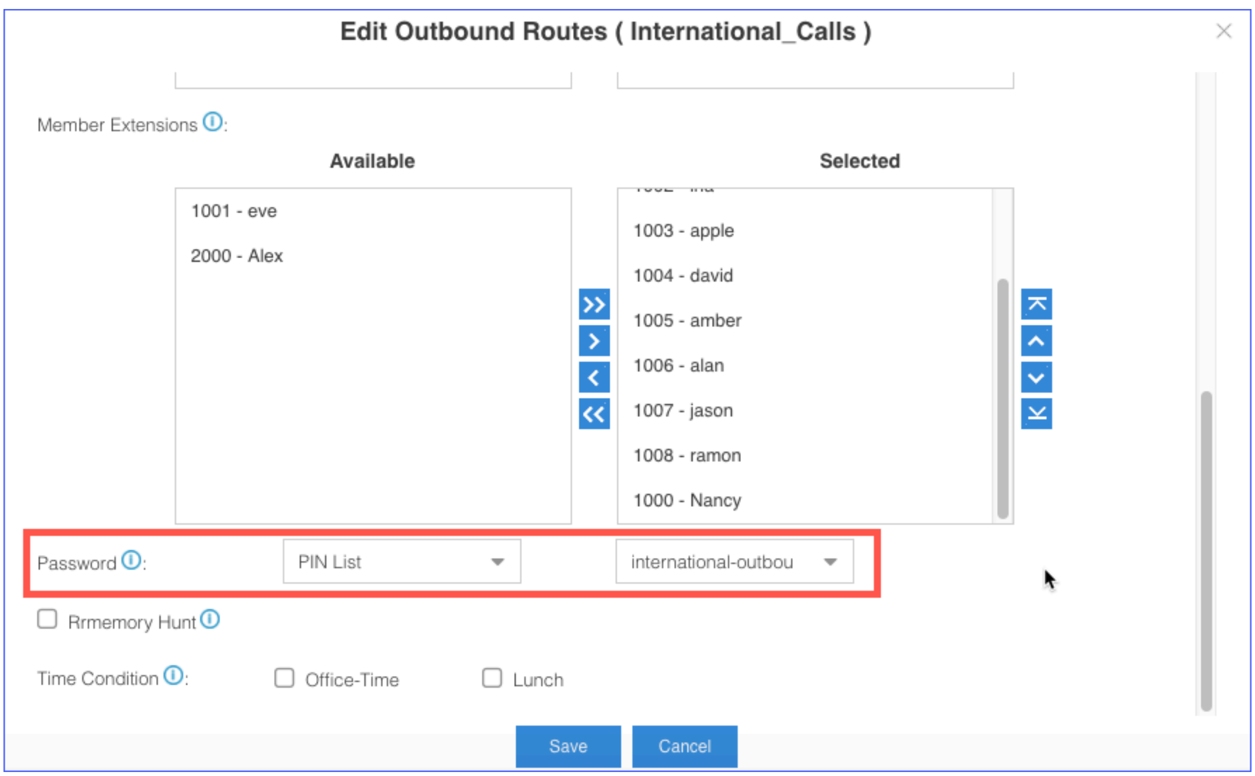


- Name: Set a name for the PIN list.
- Record In CDR: When a PIN code has been used, whether to display the PIN code in the relevant CDR.
- PIN List: Enter the PIN codes. Press Enter key to add multiple PIN codes.

4. Click Save and Apply.

Apply a PIN list

You can apply a PIN list to an outbound route or a DISA to restrict users from dialling outbound calls. When a PIN list is applied to an outbound route or a DISA, users need to dial the correct PIN to place the outbound calls.



Blacklist/Whitelist

Yeastar S1000-P IPPBX allows you to blacklist and whitelist IP addresses. This article briefly introduces the definitions and basic settings of blacklist and whitelist, and provides related configuration examples.

What is Blacklist and Whitelist

We briefly introduce the definitions of blacklist and whitelist as follows.

- Blacklist

  The blacklist is used to filter phone numbers. If a phone number is added to the blacklist, the system blocks incoming or outgoing calls for the phone number.
- Whitelist

  The whitelist is used to add trusted phone numbers. If a phone number is added to the whitelist, the system allows incoming or outgoing calls for the phone number.

  > Note:
  > The whitelist has a higher priority than the blacklist.

Blacklist/Whitelist Setting

Yeastar S1000-P IPPBX supports system blacklist/whitelist and personal blacklist/whitelist. You can set a global system blacklist/whitelist to apply to all extensions. Extension users can also log in to the PBX web interface by their accounts, and set blacklist/whitelist for their own extensions.

- System Blacklist and Whitelist

  Log in the PBX web interface as an administrator, and go to Settings > PBX > Call Features > Blacklist/Whitelist to set blacklist and whitelist.

  Yeastar S1000-P IPPBX supports to block or allow three types of numbers:
  - Inbound: If blacklist type is set to Inbound, the number can not call in the system; if whitelist type is set to Inbound, the number can call in the system.
  - Outbound: Extension users can not call the number whose blacklist type is Outbound; extension users can call the number whose whitelist type is Outbound.
  - Both: Neither inbound calls nor outbound calls are allowed for the number whose blacklist type is Both; both inbound calls and outbound calls are allowed for the number whose whitelist type is Both.

- Personal Blacklist and Whitelist

  Log in to the PBX web interface by extension accounts, the extension users can view the system blacklist and whitelist that is set by the administrator.

  > **Note:**
  > Extension users can add personal blacklist and whitelist for their extensions according to their needs.

- Blacklist/Whitelist Priority

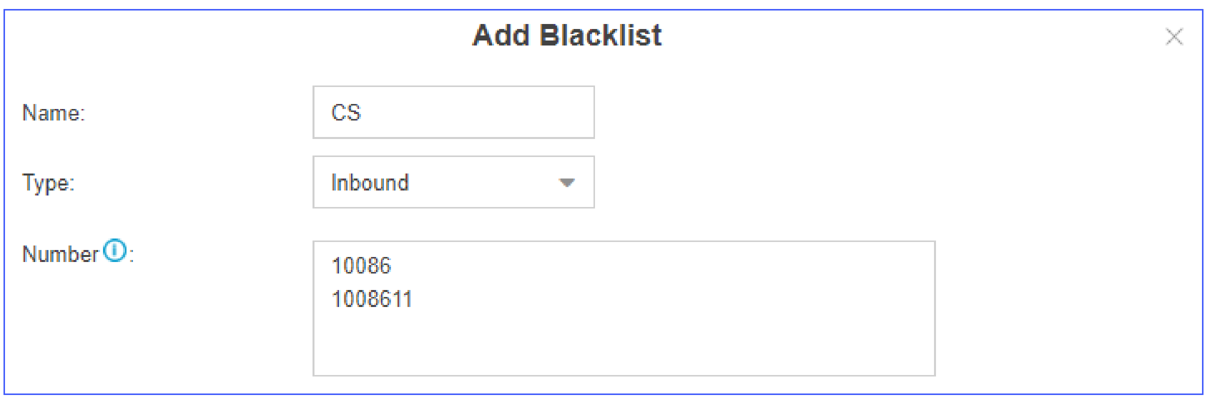
  Priority of blacklist/whitelist: system whitelist > system blacklist> personal whitelist > personal blacklist.

Blacklist Example

We demonstrate a few examples of blacklist as follows.

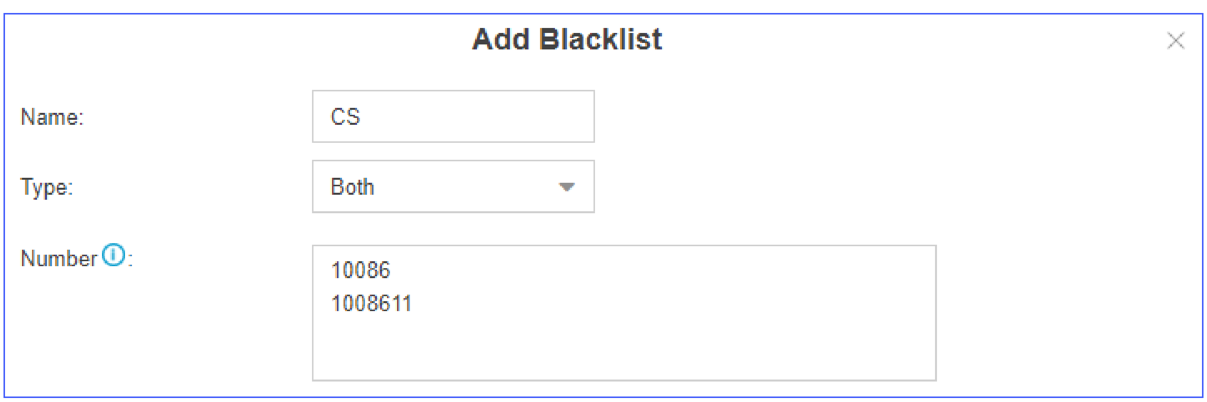
Prohibit inbound calls from external numbers

For example, 10086 and 1008611 are not allowed to call in PBX. You can add the two numbers to blacklist as follows.



Prohibit inbound calls and outbound calls

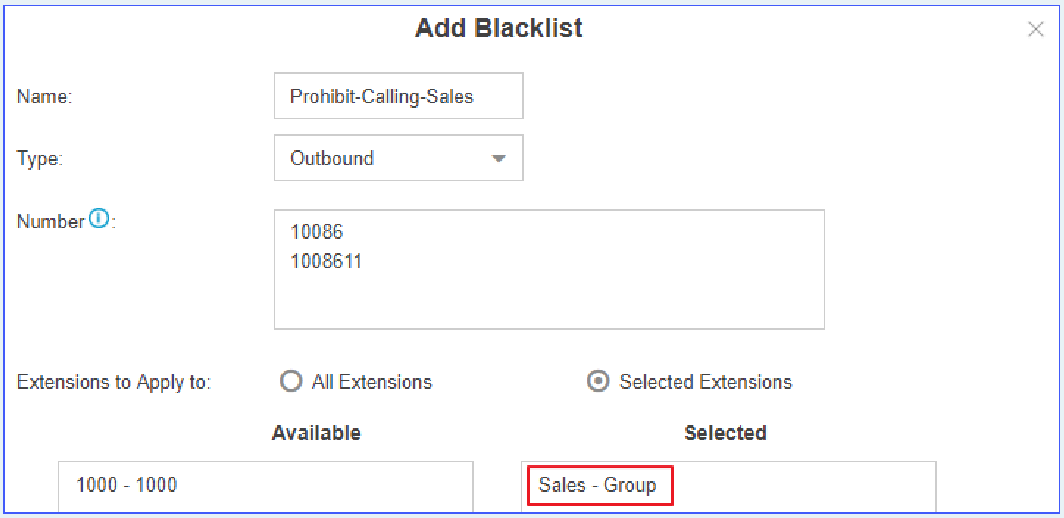
For example, 10086 and 1008611 are not allowed to call in PBX, and all extensions on PBX are not allowed to call out 10086 and 1008611.



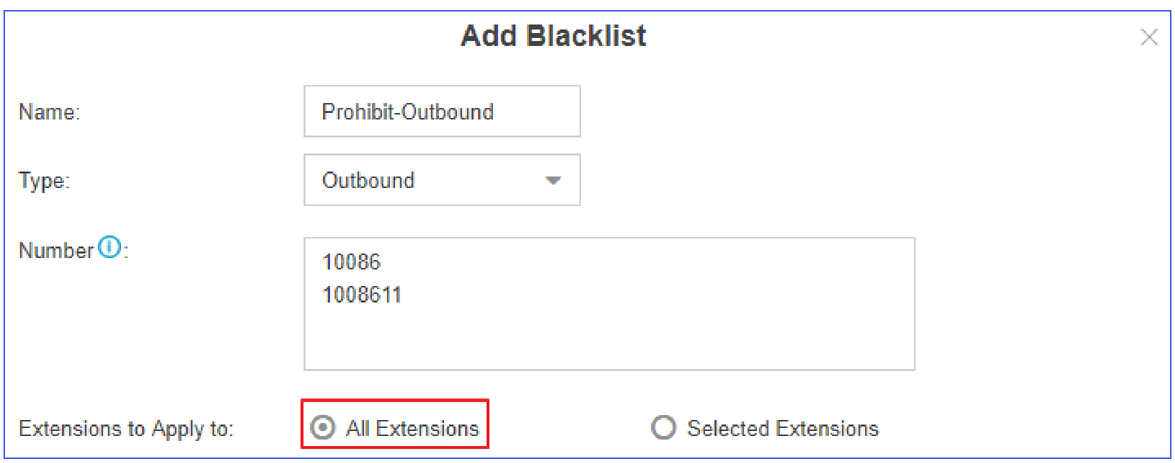
Prohibit selected extensions or extension groups from calling certain numbers

- Prohibit extension group (Sales) from calling 10086 and 1008611.

> **Note:**
> You can add an extension group (on page 18) in advance for quick selection.

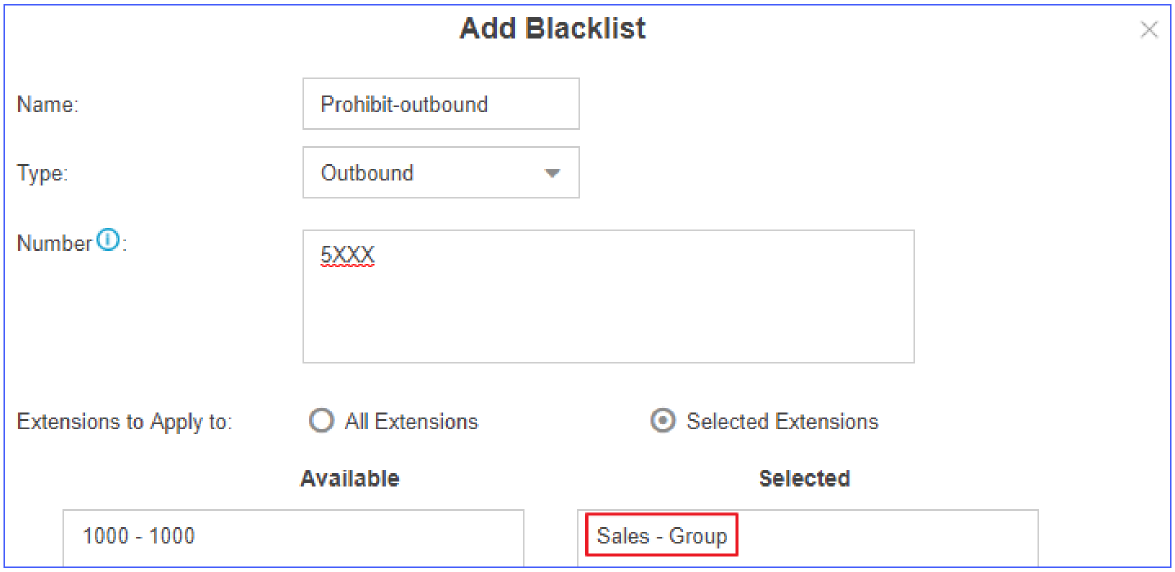


- Prohibit all extensions from calling 10086 and 1008611.



• Prohibit extensions from calling numbers with specified extension format

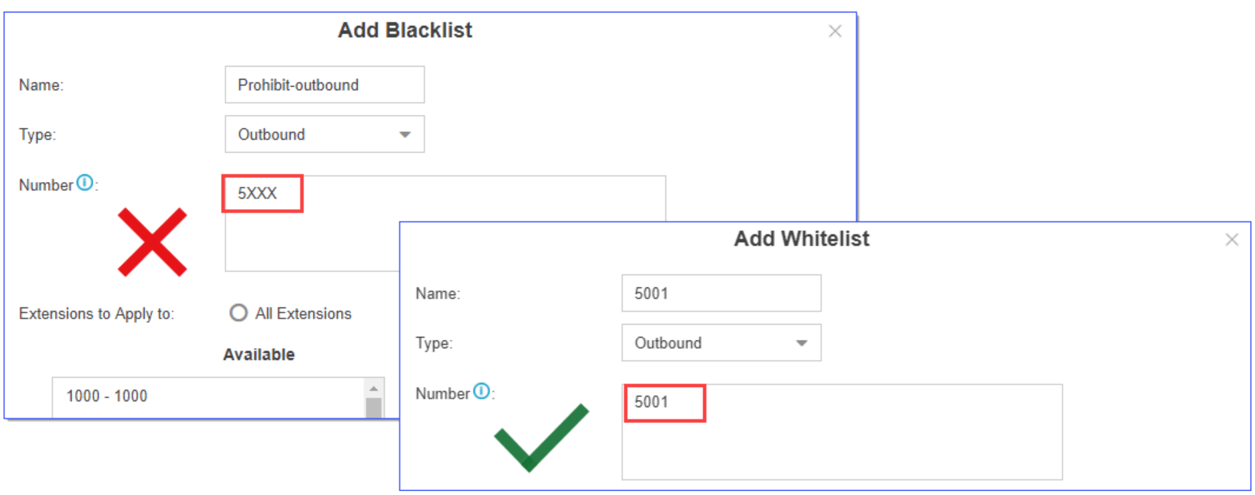
For example, prohibit extension group (sales) from calling R&D team (all extension numbers are in the format 5XXX).



Whitelist Example

The whitelist has a higher priority than the blacklist, so you can use whitelist to filter trusted phone numbers from blacklist, and allow inbound/outbound calls for the phone numbers.

For example, assume you've added 5XXX (extension numbers of R&D team) to blacklist to prohibit sales from calling R&D teams, but you want to allow sales to call extension 5001. In this case, you can add 5001 to whitelist as follows.



Voice Prompts

System Prompt

The default system prompt language is Greek. You can change the global system prompt, and if an extension user works in a foreign language, you can set a different system prompt for the user.

Change System Prompt

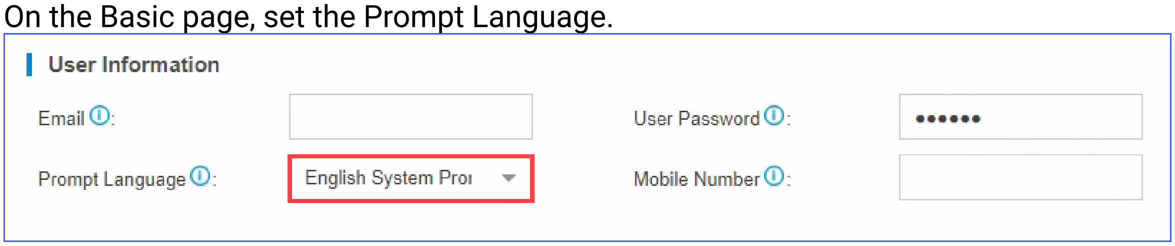
This topic describes how to change to the desired system prompt.

1. Go to Settings > PBX > Voice Prompts > System Prompt.
2. In the Prompt List section, set the desired prompt as default in the Default column.

Change an Extension's System Prompt

If a user works in a foreign language, you can set a different system prompt for the extension user.

1. Go to Settings > PBX > Extensions, select the desire extension, click .
2. On the Basic page, set the Prompt Language.

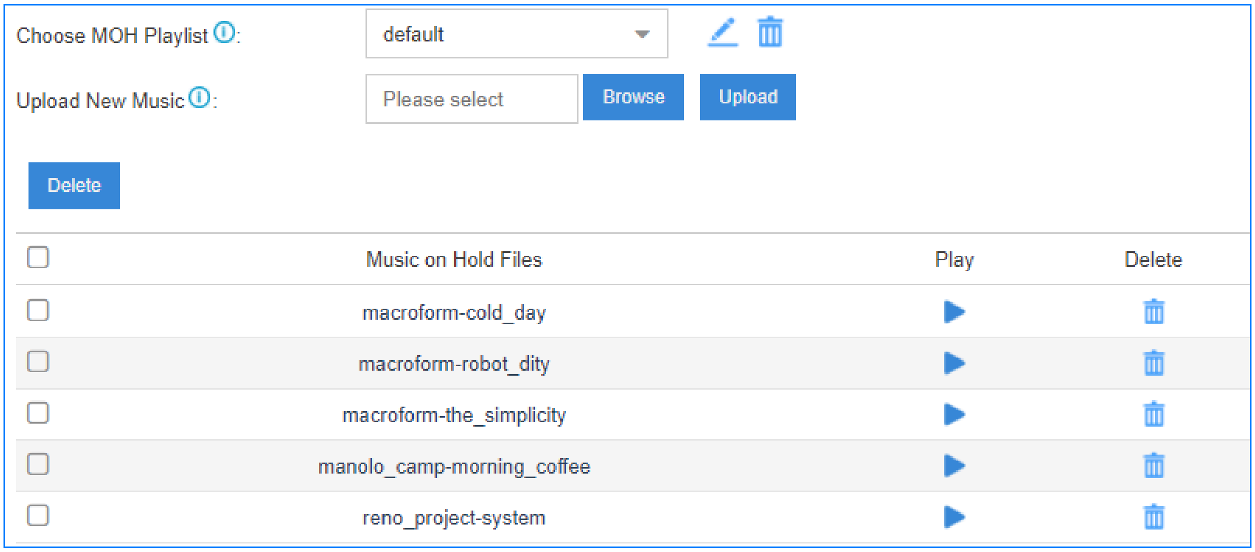


3. Click Save and Apply.

Music on Hold (MoH)

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.

The PBX has a default MoH playlist, you can add MoH playlists and upload music files to the PBX.

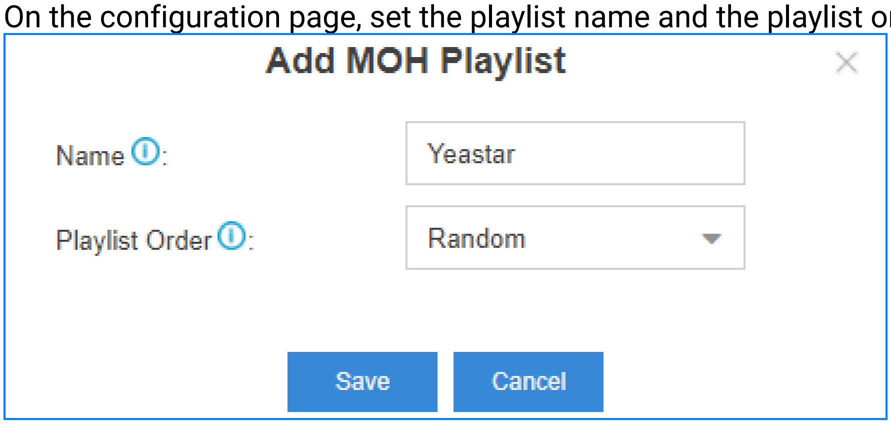


Notice:
The default MoH files are distributed under the Creative Commons Attribution-ShareAlike3.0 license through explicit permission from their authors.

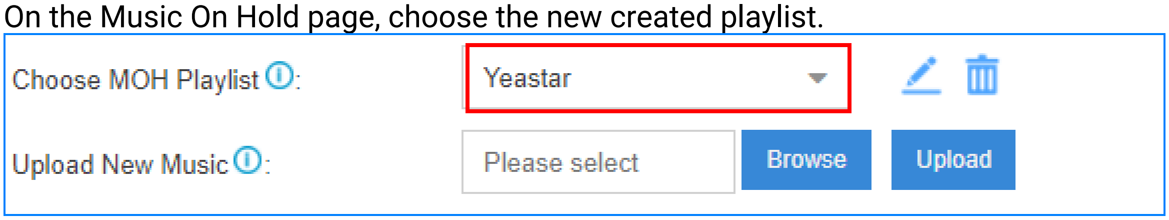
Add a Custom MoH Playlist

You can add a custom MoH playlist and upload your audio files to the PBX.

1. Go to Settings > PBX > Voice Prompts > Music on Hold, click Create New Playlist.
2. On the configuration page, set the playlist name and the playlist order, click Save.



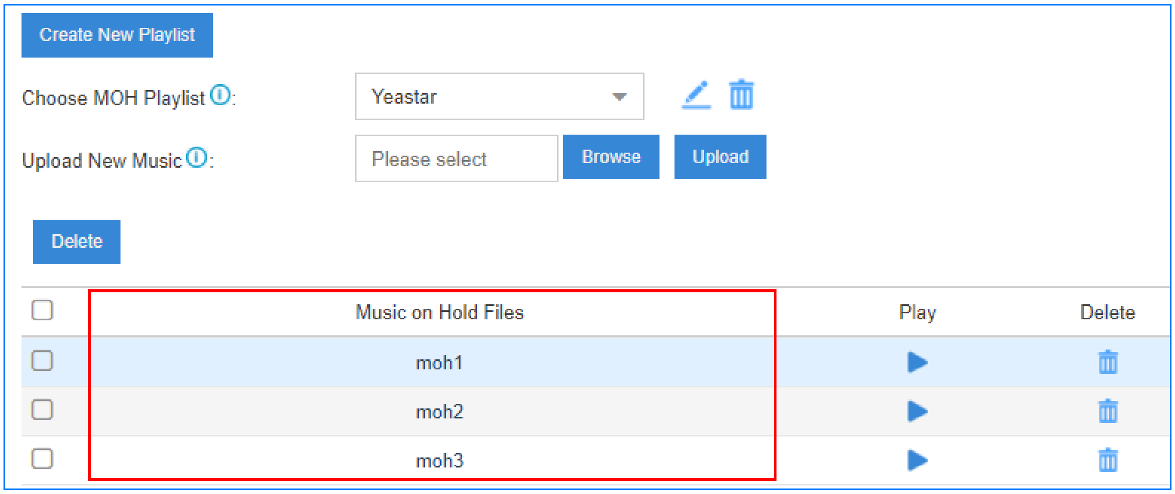
3. On the Music On Hold page, choose the new created playlist.



4. Click Browse to choose an audio file from your local PC, then click Upload.

> Note:
> The uploaded file should meet the audio file requirements (on page 145).

5. Repeat step 4 to add another audio file.
   You can see the uploaded audio files in the MoH list.

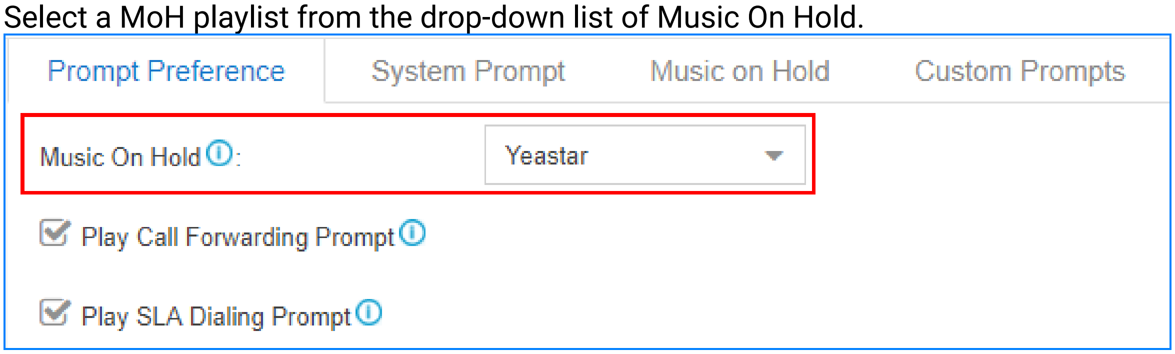


Related information
Change the MoH Playlist (on page 144)
Requirements of Custom Audio Files (on page 145)
Convert Audio Files via WavePad (on page 148)
Convert Audio Files Online (on page 148)

Change the MoH Playlist

To change the MoH playlist, you need to first add a MoH playlist and upload your audio files to the PBX.

1. Go to Settings > PBX > Voice Prompts > Prompt Preference.
2. Select a MoH playlist from the drop-down list of Music On Hold.



The PBX will play the selected MoH playlist when a user is held in a call.

Related information
Add a Custom MoH Playlist (on page 143)

Custom Prompt

The default voice prompts and announcements in the system are suitable for almost every situation.

However, you may want to use your own voice prompt to make it more meaningful and suitable for your case. In this case, you need to upload a custom prompt to the system or record a new prompt and apply it to the place you want to change.

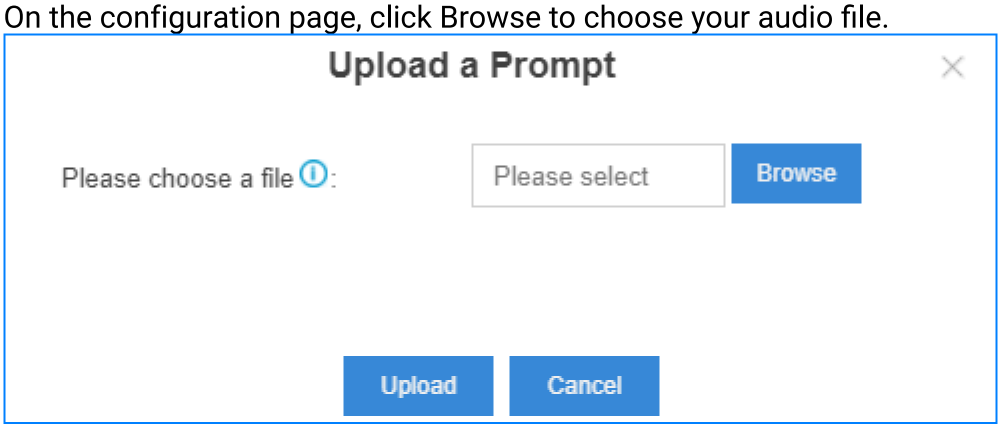
Requirements of Custom Audio Files

You can upload your audio file to the PBX, the audio file should meet the following requirements.

Option	Requirement
File Format	`.WAV`, `.wav`, or `.gsm` file. • gsm 6.10 8kHz, Mono, 1Kb/s • alaw 8kHz, Mono, 1Kb/s • ulaw 8kHz, Mono, 1Kb/s • pcm 8kHz, Mono, 16Kb/s
File Name	Should NOT contain special characters.
File Size	Smaller than 8 MB.

Upload a Custom Prompt

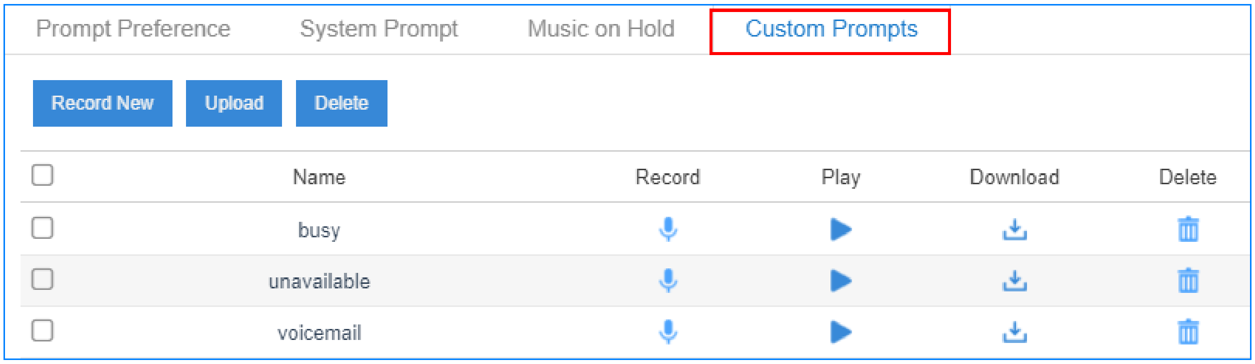
1. Go to Settings > PBX > Voice Prompts > Custom Prompts, click Upload.
2. On the configuration page, click Browse to choose your audio file.



> **Note:**
> The uploaded file should meet the audio file requirements (on page 145).

3. Click Upload to start uploading the file.

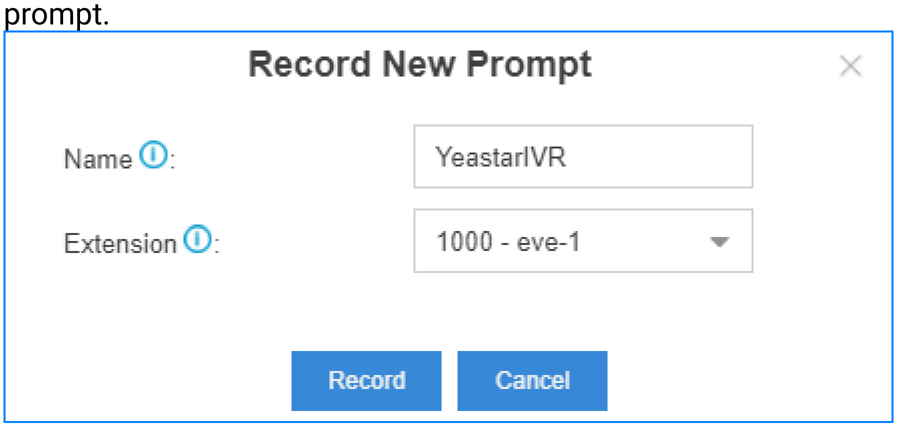
After the file is uploaded, you can see the file on the Custom Prompts page.



Record a Custom Prompt

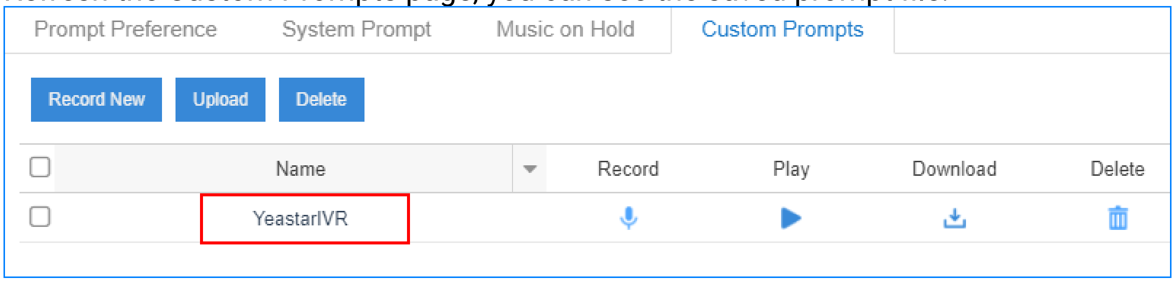
You can use an extension to record custom prompts.

1. Go to Settings > PBX > Voice Prompts > Custom Prompts, click Record New.
2. On the configuration page, set the prompt name and select an extension to record the prompt.



3. Click Save.
   The selected extension will ring.
4. Record your prompt on the phone. When done, press the # key or hang up.

5. Refresh the Custom Prompts page, you can see the saved prompt file.



You can click to play the prompt, and decide whether to save it or not. If you are not satisfied with the prompt, click to record again.

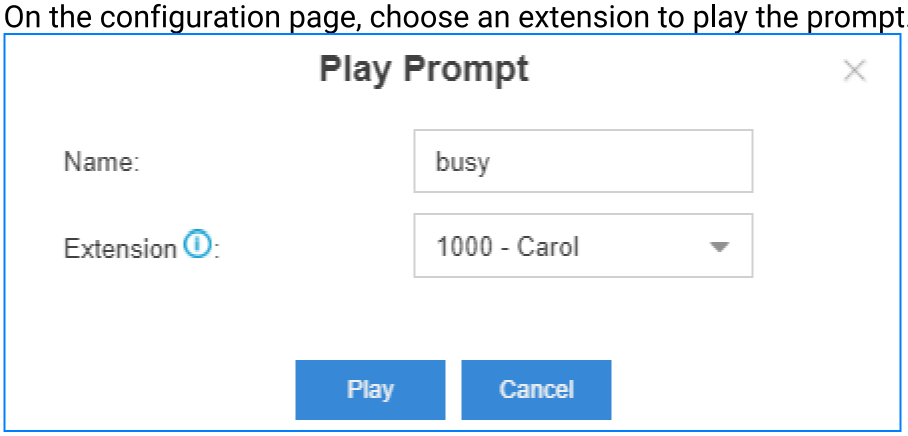
Related information
Play a Custom Prompt (on page 147)

Play a Custom Prompt

After you upload a custom prompt or record a custom prompt, you can select an extension to play the prompt.

> **Note:**
> We recommend that you play your custom prompts before you apply the custom prompts to IVR, MoH, or other places.

1. Go to Settings > PBX > Voice Prompts > Custom Prompts.
2. In the Custom Prompts list, choose a prompt, click .
3. On the configuration page, choose an extension to play the prompt.



4. Click Play.
   The selected extension will ring.
5. Pick up the phone to listen to the prompt.

Related information

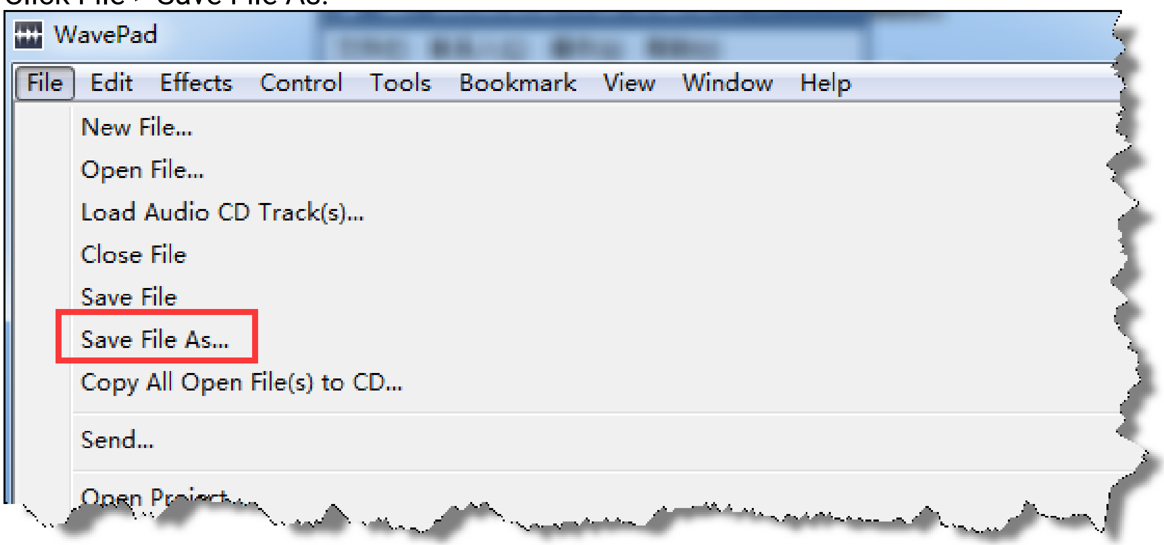
Upload a Custom Prompt (on page 145)

Record a Custom Prompt (on page 146)

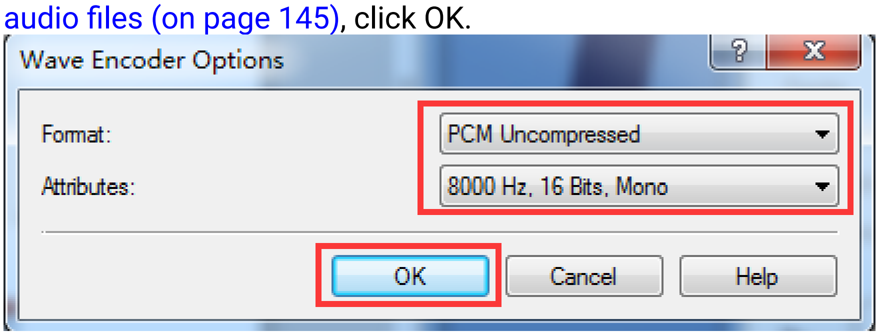
Convert Audio Files via WavePad

WavePad is audio editing software, you can convert audio files via WavePad, then upload the audio files to your PBX.

1. Launch WavePad, open your audio file.
2. Click File > Save File As.



3. Set the Save as type to `.wav` or `.gsm`, click Save.
4. For the `.wav` type, set the encoder options according to the requirements of custom audio files (on page 145), click OK.



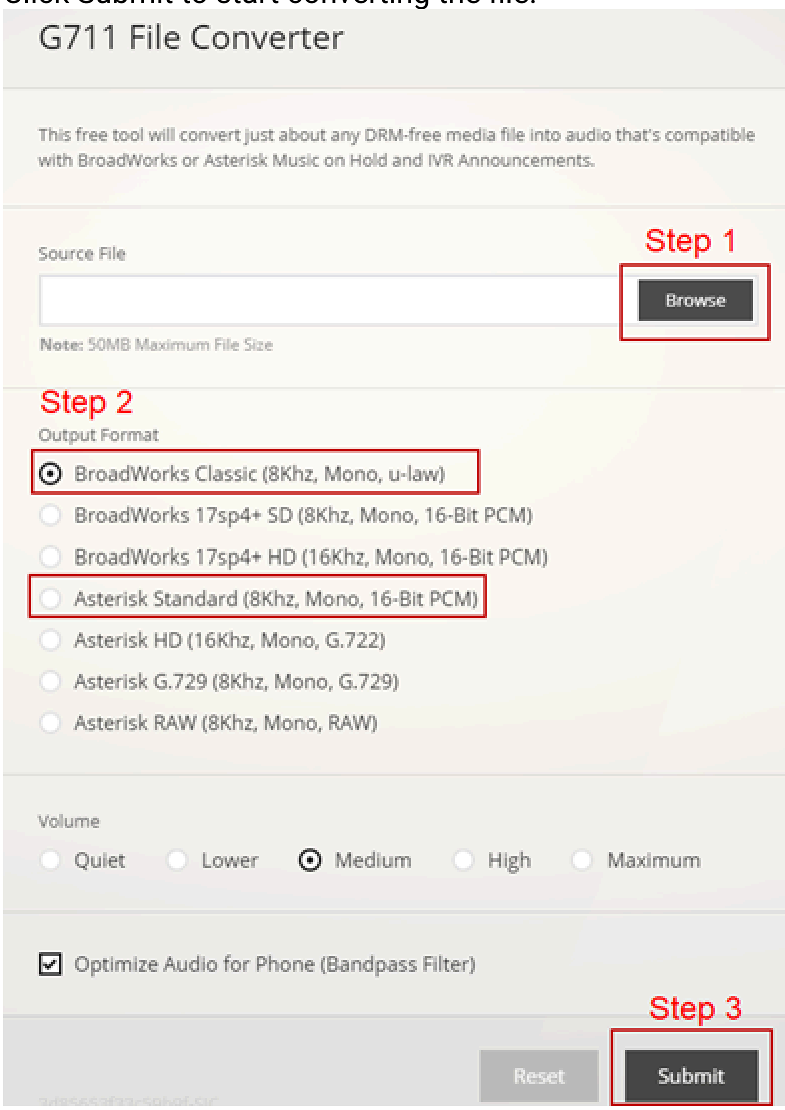
Related information

Convert Audio Files Online (on page 148)

Convert Audio Files Online

You can quickly convert your audio files via G711 File Converter online.

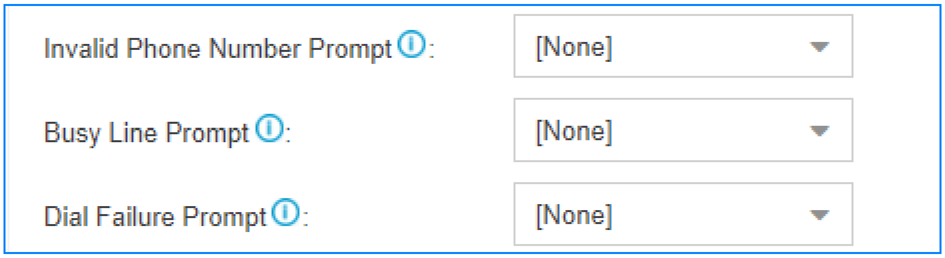
1. Visit g711.org.
2. Click Browse to upload your audio file.
3. Set the Output Format.
   We recommend BroadWorks Classic or Asterisk Standard.
4. Click Submit to start converting the file.



Set Prompts for Failed Calls

A user may fail to make outbound calls due to many reasons, such as the trunk is busy, no trunk available, or invalid number. You can set different prompts to inform the user why the call fails.

1. Go to Settings > PBX > Voice Prompts > Prompt Preference.
2. Set the prompts for different type of failed calls.



- Invalid Phone Number Prompt: The PBX will play the prompt when the dialed number is invalid.
- Busy Line Prompt: The PBX will play the prompt when the trunk used is busy.
- Dial Failure Prompt: The PBX will play the prompt if no trunk is available to call out.

Network

Basic Network

Basic Network Overview

Before using the Yeastar S1000-P IPPBX in your network, you must configure the basic network.

Network interfaces

Yeastar S1000-P IPPBX supports LAN interface and WAN interface. By default, the LAN interface is enabled, and the WAN interface is disabled.

According to your network environment, you may need to use dual network interfaces.

If you use dual network interface, the system route entries are automatically created for the default network interface. To properly route the network traffic through the desired network interface, you need to add a static route (on page 172) on the PBX.

Ethernet modes

Yeastar S1000-P IPPBX supports two Ethernet modes:

- Single: Only LAN port will be used for connection, WAN port is disabled.
- Dual: Both LAN port and WAN port can be used for connection.
  If you use Dual mode, you need to choose a default network interface for the PBX.

> Note:
> The traffic will be routed to the default interface; you need to add a static route (on page 172) to override the default route entries, routing the traffic from a specific IP address to the specified destination.

IP address assignment

Yeastar S1000-P IPPBX supports three types of IP address assignment:

- Assign a static IP address

  Contact your network administrator to assign an IP address to the PBX. Then you need to manually configure settings such as the IP address, subnet mask, default gateway, and DNS servers on the PBX.
- Obtain an IP address from a DHCP server

  You can configure the PBX to automatically obtain its 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 the IP address.

Configure Static IP Address

This topic describes how to assign a static IP address to the LAN network interface when the PBX is in Single network mode.

1. Go to Settings > Systems > Network > Basic Settings.
2. In the Hostname field, enter a host name.
3. In the Mode field, select Single mode.
4. In the LAN section, click IPv4 Address or IPv6 Address tab based on your network environment, select Static IP Address, and enter the network information as follows.

   > Note:
   > - Consult your network administrator to get the network information.
   > - If you use both IPv4 address and IPv6 address, the PBX selects a protocol stack according to the domain name or IP address of the destination device. Avoid mapping the domain name to both IPv4 address and IPv6 address. If the destination device only supports IPv4, the connection would fail as IPv6 address has higher priority.

   Table 2. IPv4 address

Setting	Description
IP Address	Enter the IP address that is assigned to the PBX.

Setting	Description
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.

Table 3. IPv6 address

Setting	Description
IP Address	Enter the IP address that is assigned to the PBX.
IP Prefix Length	Enter the IPv6 prefix.
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.
IP 2 Prefix Length	Optional. Enter another IPv6 prefix for the second IP address.

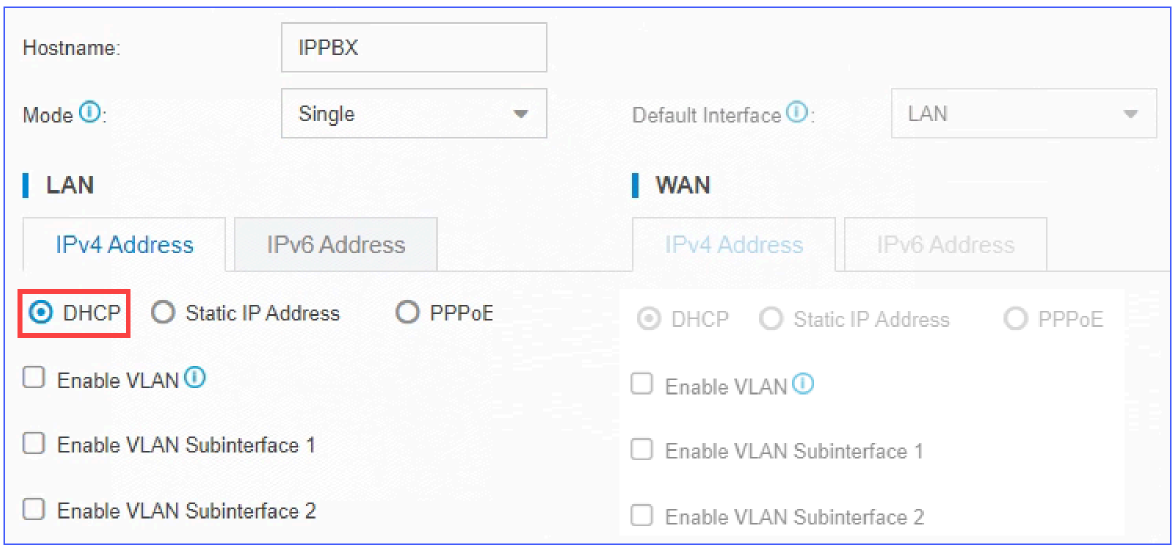
5. Click Save and reboot the PBX to take effect.

Obtain an IP Address from a DHCP Server

You can configure Yeastar S1000-P IPPBX to automatically obtain an IP address 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. We suggest that your configure a static IP address for the PBX.

1. Go to Settings > System > Network > Basic Settings.
2. In the Hostname field, enter a host name.
3. In the Mode field, select Single mode.
4. In the LAN section, click IPv4 Address or IPv6 Address tab based on your network environment, select DHCP to obtain an IP address from a DHCP server.



5. Click Save and reboot the PBX to take effect.

   You can check the IP address of the PBX from your router.

Configure a PPPoE Connection

This topic describes how to configure a PPPoE connection on Yeastar S1000-P IPPBX to obtain an IP address when the PBX is in Dual network mode.

Scenario

A PPPoE client assigns a dynamic IP address to the PBX, the IP address of the PBX may vary every time the PBX is started up.

Due to the IP address from PPPoE varies, you need to configure dual network, and configure a local network on the PBX for you to access the PBX.

Configuration Example

The following takes the configuration of Static IP address on LAN port and PPPoE on WAN port as an example.

1. Go to Settings > Systems > Network > Basic Settings.
2. In the Hostname field, enter a host name.
3. In the Mode field, select Dual mode.
4. In the LAN section, click IPv4 Address or IPv6 Address tab based on your network environment, select Static IP Address, and enter the network information as follows:

Table 4. IPv4 address

Setting	Description
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.

Table 5. IPv6 address

Setting	Description
IP Address	Enter the IP address that is assigned to the PBX.
IP Prefix Length	Enter the IPv6 prefix.
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.

Setting	Description
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.
IP 2 Prefix Length	Optional. Enter another IPv6 prefix for the second IP address.

5. In the WAN section, click IPv4 Address or IPv6 Address tab based on your network environment, select PPPoE, and configure the username and password.
    - Username: Enter the username that is provided by the ISP.
    - Password: Enter the password that is provided by the ISP.
6. Click Save and reboot the PBX to take effect.

OpenVPN Client

OpenVPN Client Overview

Yeastar S1000-P IPPBX supports OpenVPN version 2.0.5. Yeastar S1000-P IPPBX can act as an OpenVPN client to establish a connection with the VPN server access to VPN services.

OpenVPN is a software based on VPN protocol. OpenVPN uses VPN techniques to secure point-to-point and site-to-site connections. You can use VPN connection to bypass geographic restrictions and government censorship by hiding your real IP address on the Internet. Also, OpenVPN encrypts your Internet data and traffic to keep it from being monitored and threatened by hackers.

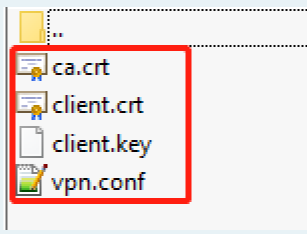
Connect Yeastar S1000-P IPPBX to OpenVPN Server

You can connect Yeastar S1000-P IPPBX to the OpenVPN server by manual configuration or OpenVPN files package.

Note:
IPv6 network does NOT support this feature.

- Manual Configuration: If your VPN provider provides you with the information of OpenVPN server settings, certification files and key files, you can manually configure the OpenVPN client on Yeastar S1000-P IPPBX and connect to OpenVPN Server.
- Upload OpenVPN Package: If your VPN provider provides you with a connection file, certification files and key files, you can compress these files, upload the package to Yeastar S1000-P IPPBX and connect to OpenVPN Server.

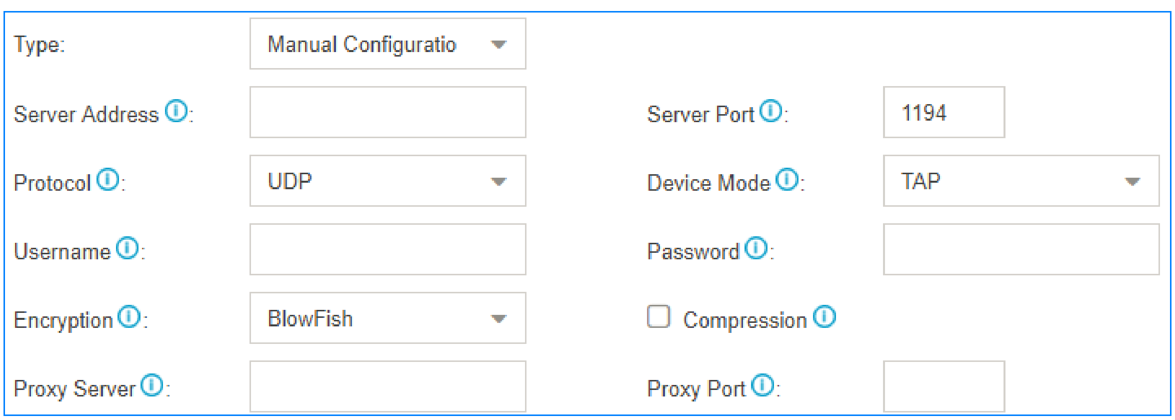
Note:
- The name of OpenVPN connection file should be `vpn.conf`.
- You need to save the certification files and key files in the root directory, and compress them into a `.tar` package.



- The new option `remote-cert-tls server` is not supported on the S-Series VoIP PBX, you need to change it to `ns-cert-tls server`.

Manual Configuration on Yeastar S1000-P IPPBX

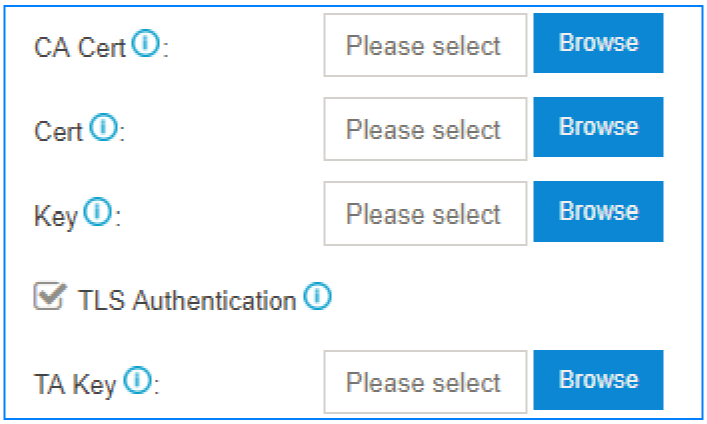
1. Go to Settings > System > Network > OpenVPN, select the checkbox of Enable OpenVPN.
2. In the drop-down list of Type, select Manual Configuration.
3. Set the OpenVPN client settings according to the OpenVPN server.



- Server Address: Enter the IP address of the OpenVPN server.
- Server Port: Enter the port of the OpenVPN server.
- Protocol: Select the same protocol as the OpenVPN server.
- Device Mode: Select the same mode as the OpenVPN server.
- Username: Optional. Enter the username to access the VPN server.
- Password: Optional. Enter the username to access the VPN server.

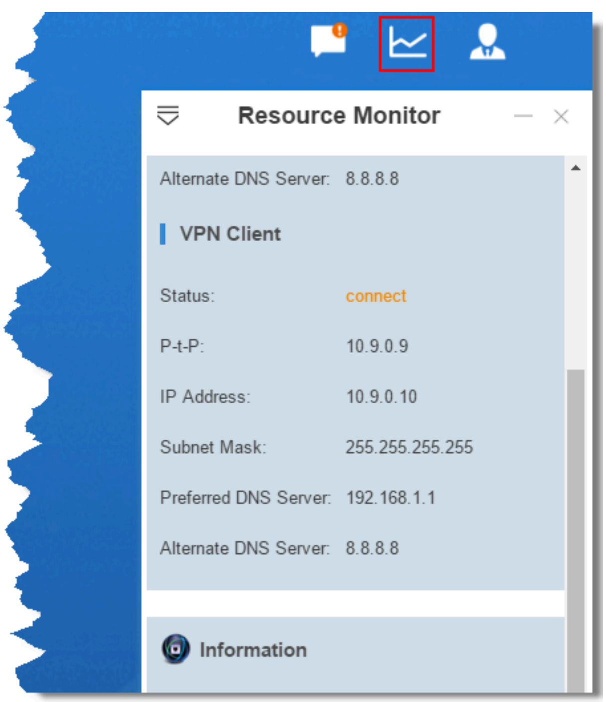
- Encryption: Select the same type as the OpenVPN server.
- Compression: Enable or disable compression for data stream. The server and client should be the same setting.
- Proxy Server: If the PBX is connected through an HTTP proxy to reach the OpenVPN server, enter the proxy server.
- Proxy Port: If the PBX is connected through an HTTP proxy to reach the OpenVPN server, enter the proxy port.

4. Upload certificates and keys.



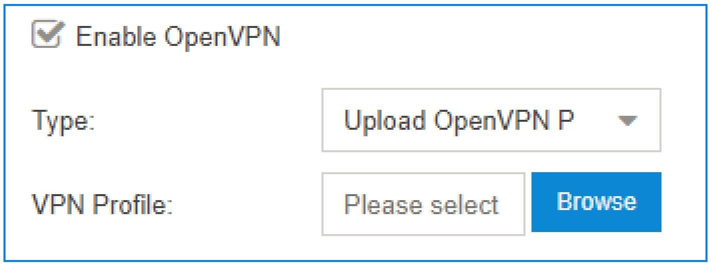
- CA Cert: Upload a CA certificate.
- Cert: Upload a Client certificate.
- Key: Upload a Client key.
- TLS Authentication: Enable or disable TLS authentication.
- TA Key: If you enable TLS Authentication, upload a TA key.

5. Click Save and click the at the right-top corner to check the VPN client status.

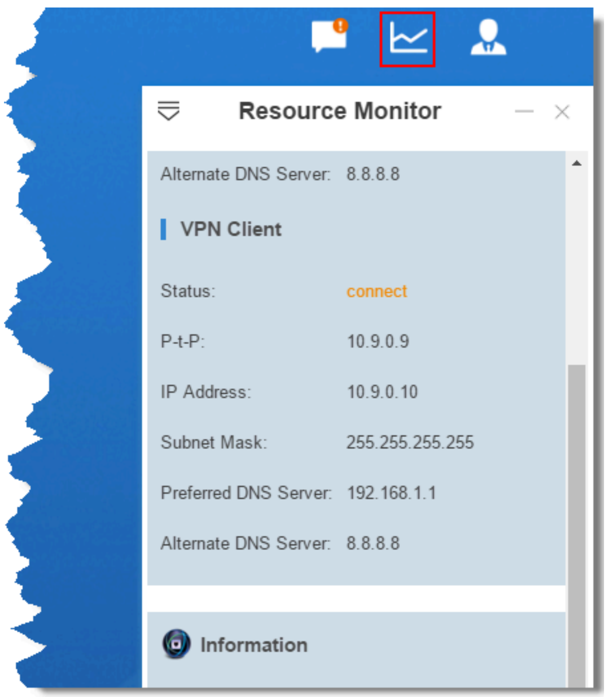


Upload OpenVPN Package

1. Go to Settings > System > Network > OpenVPN, select the checkbox of Enable Open-VPN.
2. In the drop-down list of Type, select Upload OpenVPN Package.
3. Click Browse, select the OpenVPN package.



4. Click Save and click the at the right-top corner to check the VPN client status.



DDNS

DDNS Overview

Dynamic DNS (DDNS) is a method of updating a Domain Name System (DNS) to point to a changing IP address on the Internet.

> Note:
> IPv6 network does NOT support this feature.

When do you need a DDNS?

If your ISP assigns dynamic IP addresses to you, the remote extensions, or other remote devices can not keep connected to your PBX.

To ensure the successful remote connection with your PBX, you need to set up dynamic DNS service. Dynamic DNS keeps track of the dynamic IP address, so the remote devices can access the PBX even the IP address is changing from time to time.

Supported DDNS providers

You can set up DDNS on your router or Yeastar S1000-P IPPBX. Yeastar S1000-P IPPBX supports the following DDNS providers:

- dyndns.org
- freedns.afraid.org
- www.no-ip.com
- www.zoneedit.com
- www.oray.com (For Chinese users)
- 3322.org (For Chinese users)

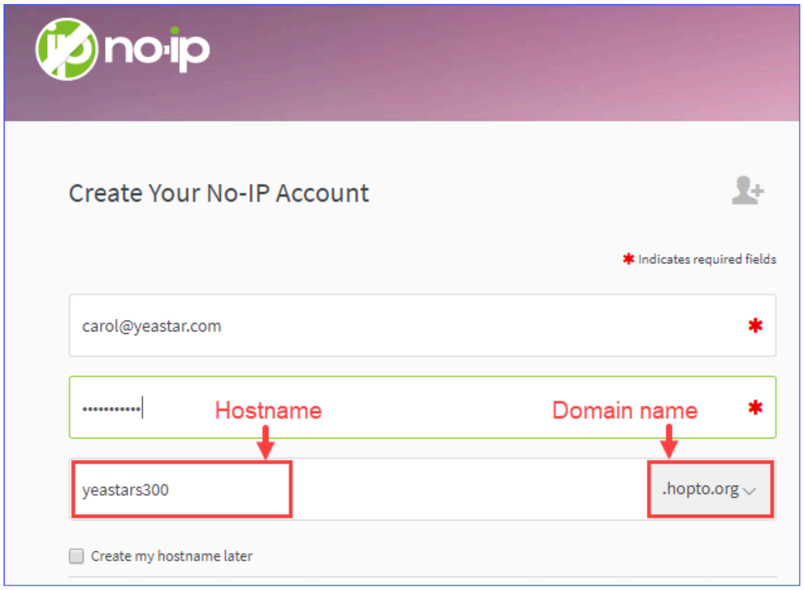
Set up No-IP DDNS on Yeastar S1000-P IPPBX

If your ISP doesn't provide a static public IP address for you, you can create a No-IP DDNS account, and set up DDNS on Yeastar S1000-P IPPBX.

> Note:
> IPv6 network does NOT support this feature.

Step 1. Create a No-IP account

1. Go to the No-IP Sign Up page.
2. On the new account form, fill in the required fields.
    - Email: Enter your email address as the No-IP account.
    - Password: Set the password of the No-IP account.
    - Hostname: Select your desired domain name, and enter your desired hostname.

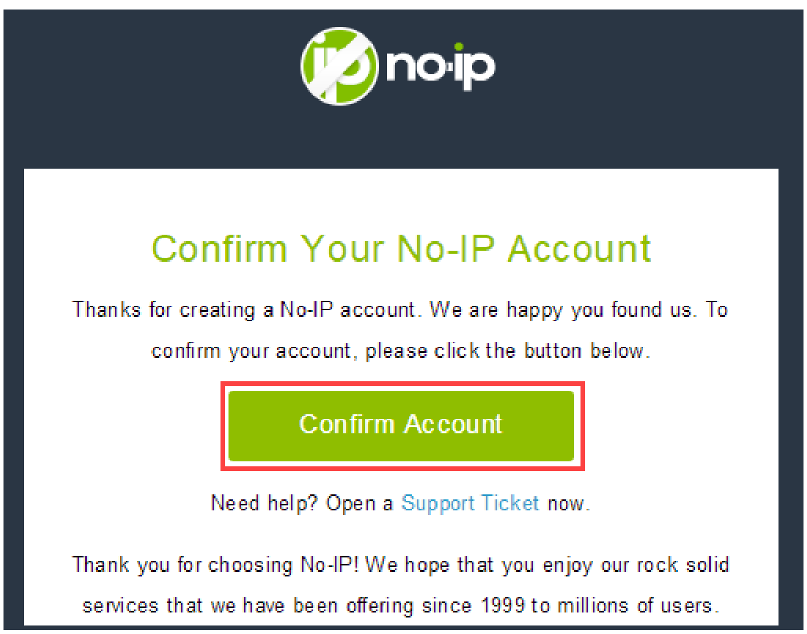


3. At the bottom of the page, click Free Sign Up.

   No-IP will send a confirmation email to your email address.

Step 2. Confirm your No-IP account

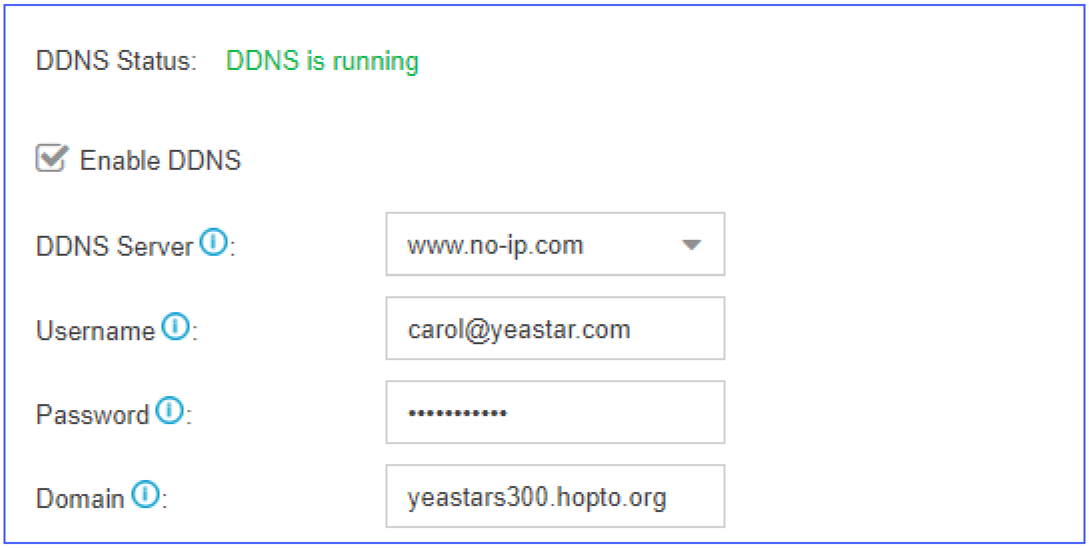
Check your email from No-IP, click Confirm Account. Your No-IP account is activated.



Step 3. Set up No-IP DDNS on PBX

1. Log in to the PBX web interface, go to Settings > System > Network > DDNS Settings.
2. Select the checkbox of Enable DDNS.
3. In the DDNS Server drop-down list, select www.no-ip.com.

4. Enter your No-IP account information and the fully qualified domain name.
5. Click Save and Apply.



Step 4. Set up Port Forwarding and NAT

- If your PBX is behind a router, you need to set up Port Forwarding on the router (on page 163) to allow external devices to access the PBX.
- To ensure that the external traffic packets can be sent to the correct destination, you need to set NAT (on page 165) on your PBX.

> **Important:**
> To enhance the security of your PBX, we suggest you to change the default ports.

Table 6. Common ports on Yeastar S1000-P IPPBX

Service	Default Port
Web	8088
SIP	5060
RTP	10000-12000

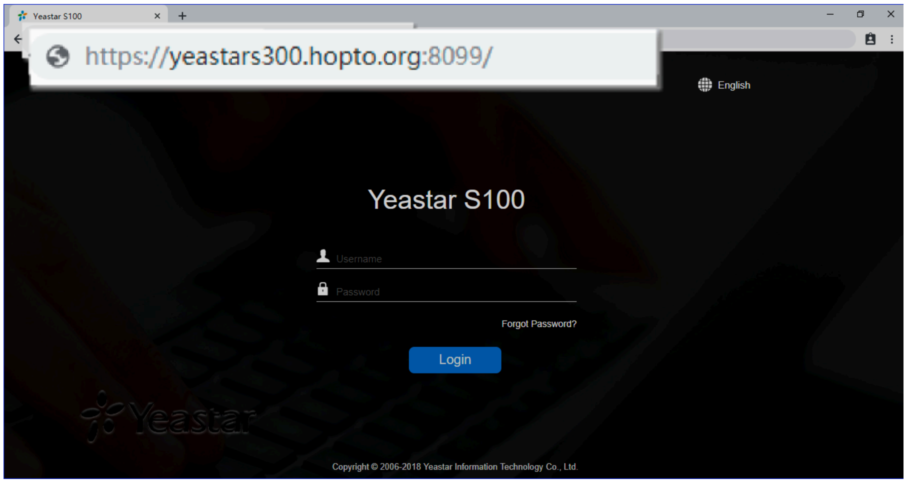
> **Tip:**
> To verify that you have set up your router correctly, you can visit the website www.portchecktool.com.

Step 5. Check the DDNS connection

To check the connection of an external device from the Internet, enter the domain name and external port to access the PBX.

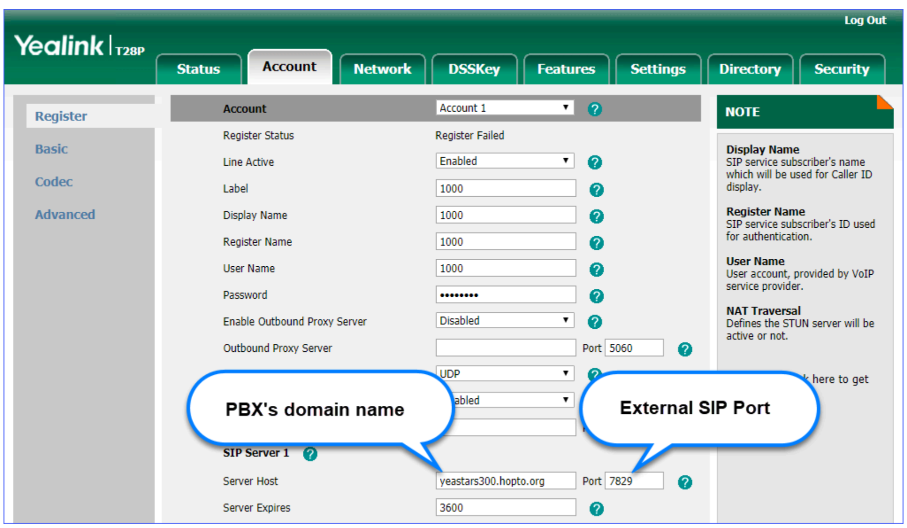
Example: Access PBX by DDNS

On a PC that is NOT in the PBX's network, enter the domain name and external web port to access the PBX web interface.



Example: Register a remote extension by DDNS

On an IP phone that is NOT in the PBX's network, enter the domain name and external SIP port to register a remote extension.



Port Forwarding

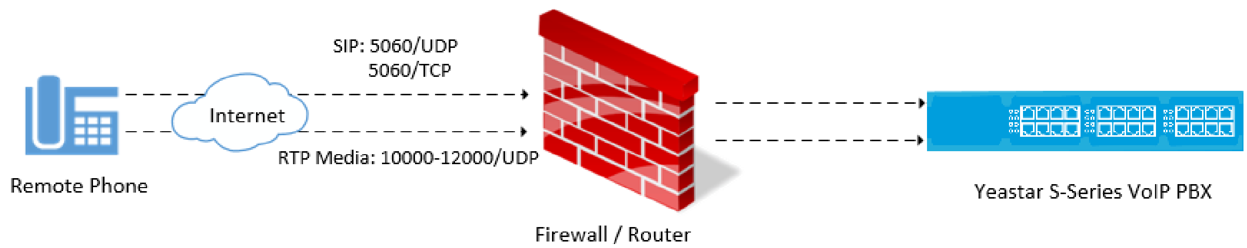
Port Forwarding Overview

If Yeastar S1000-P IPPBX is behind a router, you need to set up port forwarding on the router to allow external devices to access the PBX. The router directs the appropriate traffic from the Internet to the PBX.

Forward Ports for Remote Extensions

If you want to register remote extensions to the PBX, forward the following ports on your router:

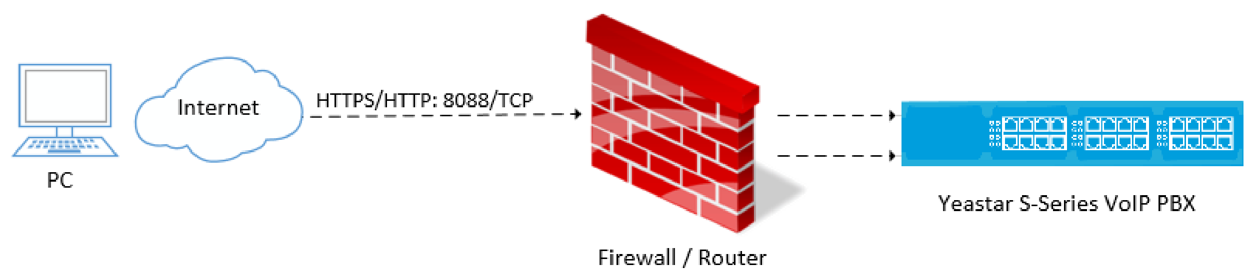
- Port 5060 (inbound, UDP)
- Port 5060 (inbound, TCP) — if you use TCP for SIP registration
- Port 10000 - 12000 (inbound, UDP) for RTP



Forward Ports for Remote Web Login

If you want to log in the PBX web interface remotely, you need to forward the following ports:

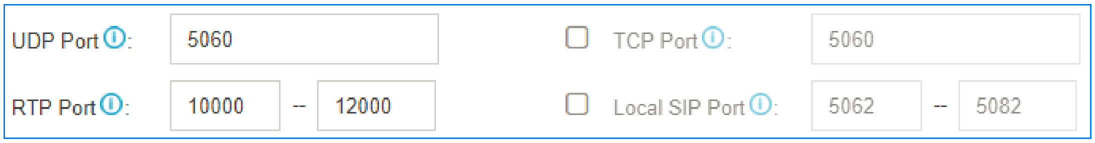
- Port 8088 (inbound, TCP)



Set up Port Forwarding on Mikrotik Router

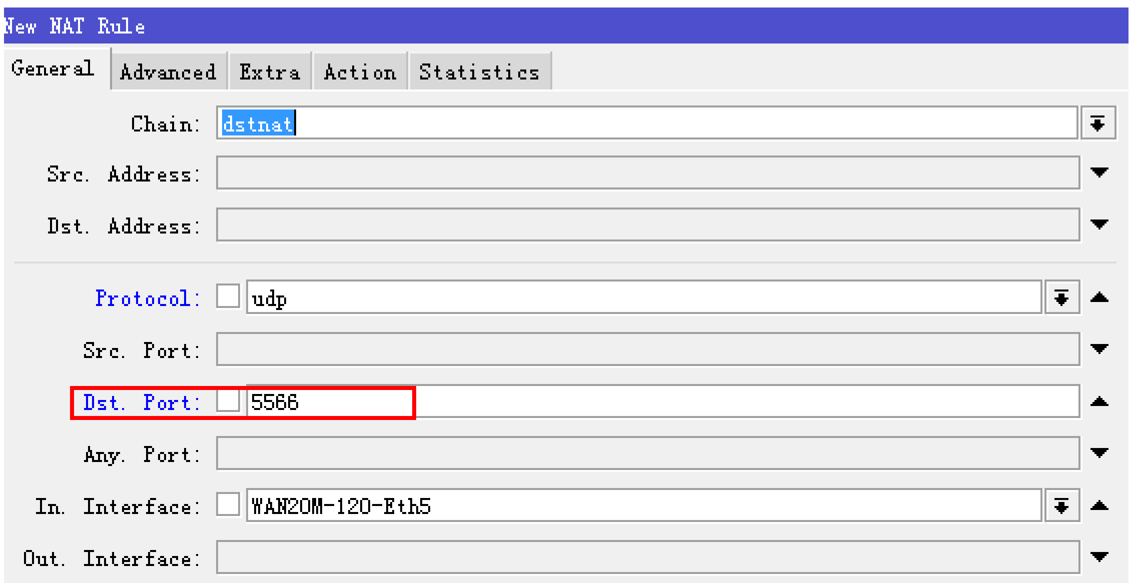
This topic provides a configuration example of port forwarding on Mikrotik router.

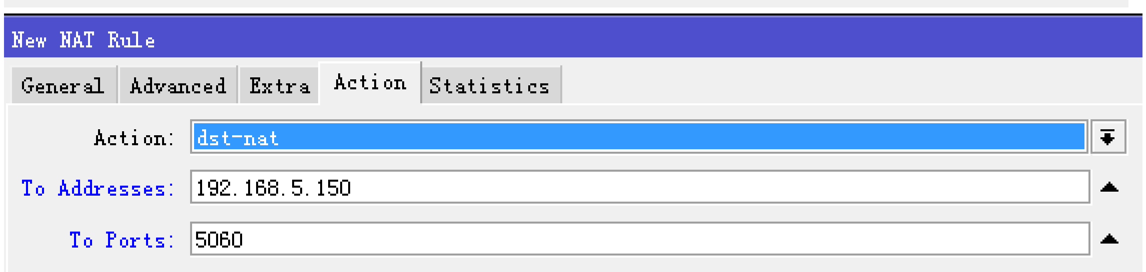
1. Check the SIP UDP port and RTP port on Yeastar S1000-P IPPBX.
    a. Log in to the PBX web interface, go to Settings > PBX > General > SIP > General.
    b. Note down the default port or change the default port.



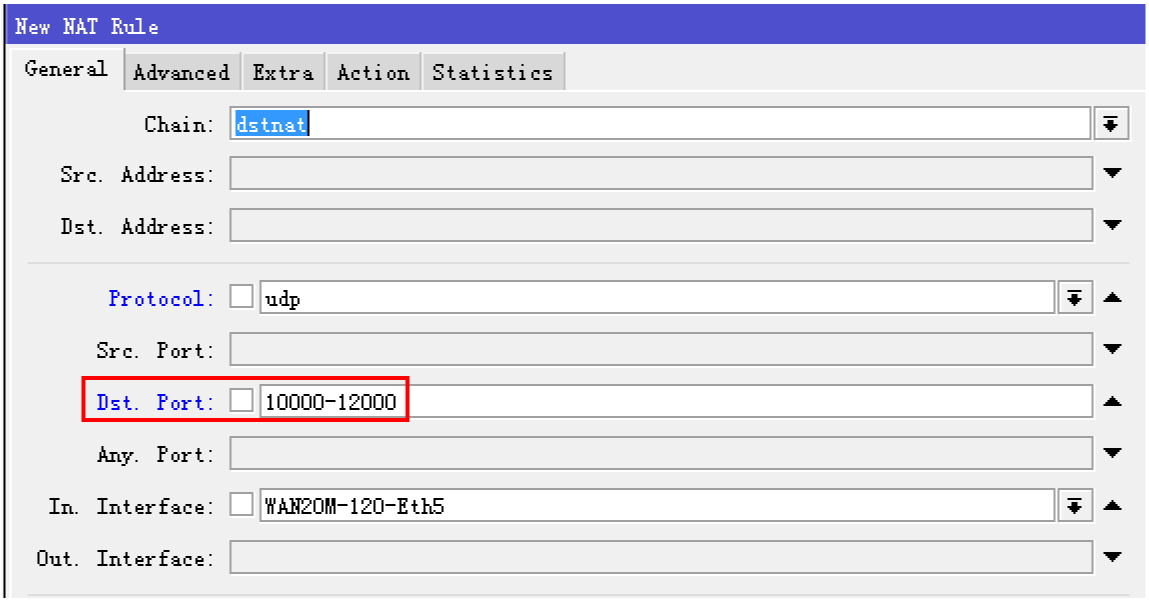
2. Forward SIP UDP 5060 on Mikrotik Router.
    As the following figure shows, we forward port 5060 to 5566.

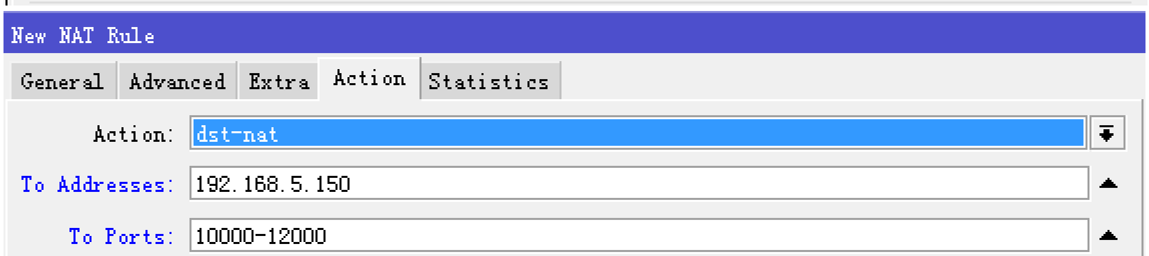
> Note:
> To enhance the PBX security, we highly suggest you not to forward the SIP port 5060 to 5060.





3. Forward RTP ports 10000-12000 on Mikrotik Router.
    As the following figure shows, we forward ports 10000-12000 to 10000-12000.



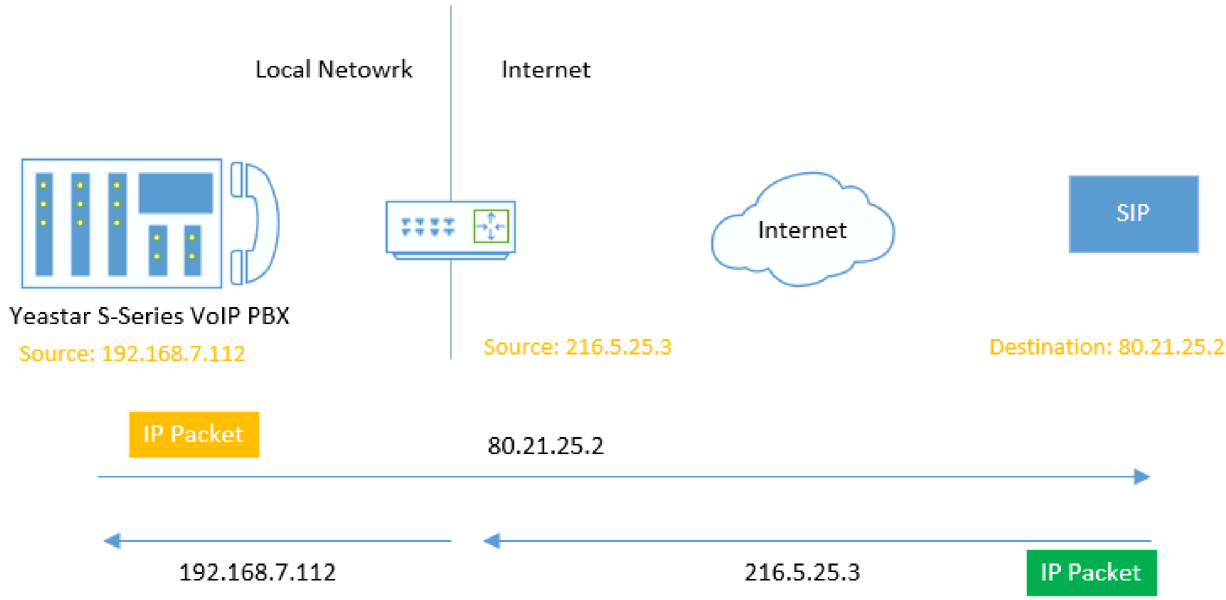


NAT

NAT Overview

Network Address Translation (NAT) is a method of translating the private (not globally unique) address in Internet Protocol (IP) into legal address. NAT is used to limit the number of public IP addresses for security purpose..

> Important:
> IPv6 network does NOT support this feature.



When do you need to configure NAT?

If your PBX is operating in a network connected to the Internet through a single router, your PBX is behind NAT.

The NAT device has to be instructed to forward the right inbound packets (from Internet) to the PBX server. You need to configure NAT settings in the following situations:

- Register a remote extension to the PBX
- Connect a device to the PBX via SIP trunk

> Note:
> Problems like "One way audio" or "Call drops after XX seconds" are mostly caused by incorrect NAT settings.

NAT types

Yeastar S1000-P IPPBX provides three types of NAT configurations, you can select a type to configure NAT according to your network environment.

- External IP Address: If your PBX has a private IP address and is connected to a router that has a static public IP address, you can set NAT with External IP Address.

  Your PBX will communicate with the external devices with the static public IP address. When the router gets packets back from the external devices, the router can redirect the packet to the PBX.

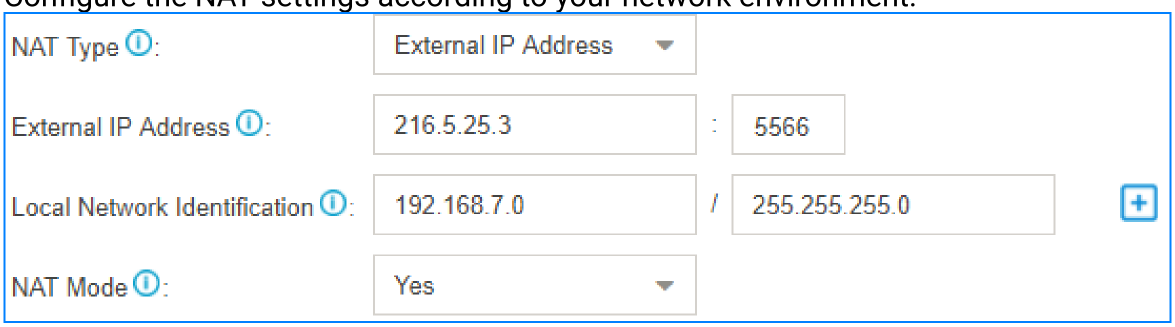
- External Host: If your PBX has a private IP address and is connected to a router that doesn't have a static public IP address, you can set NAT with External Host.
- STUN: If your PBX has no static public IP address and domain name, you can set the NAT with STUN (Simple Traversal Utilities for NAT). STUN is a simple protocol for discovering the public IP address.

Set NAT with External IP Address

If your PBX has a private IP address and is connected to a router that has a static public IP address, you can set NAT with External IP Address.

> Important:
> IPv6 network does NOT support this feature.

1. Forward the required ports on your router. (on page 163)
2. Log in to the PBX web interface, go to Settings > PBX > General > SIP > NAT.
3. In the drop-down list of NAT Type, select External IP Address.
4. Configure the NAT settings according to your network environment.



   - External IP Address: Enter the static IP address of the router and enter the forwarded destination port of SIP.
   - Local Network Identification: Enter the local network segment and the subnet mask. This setting will allow all your local devices to communicate with the PBX by the local IP address instead of passing through the router.

   > Note:
   > If you have multiple local network segments, click to add another Local Network Identification.

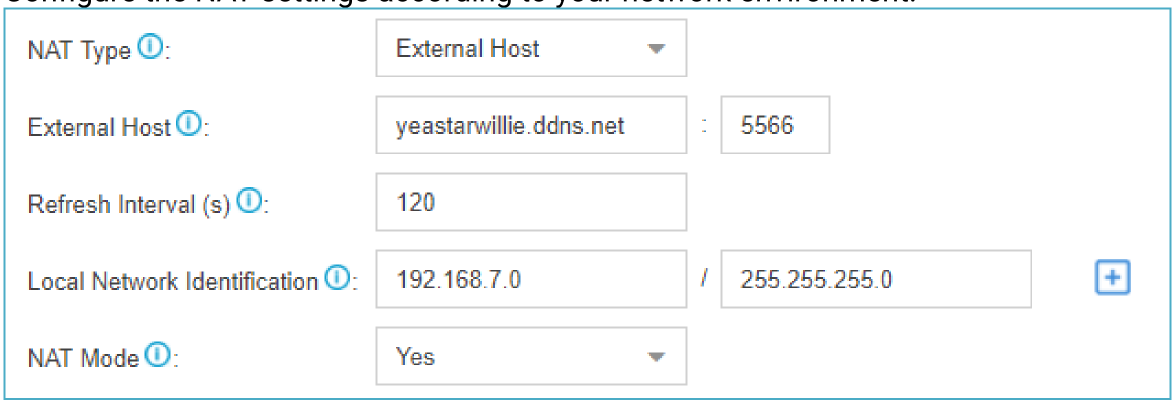
   - NAT Mode: Set to Yes.
5. Click Save and reboot the PBX to take effect.

Set NAT with External Host

If your PBX has a private IP address and is connected to a router that doesn't have a static public IP address, you can set NAT with External Host.

Important:
IPv6 network does NOT support this feature.

1. Set up DDNS on the PBX (on page 158) or set up DDNS on your router.
2. Forward the required ports on your router. (on page 163)
3. Log in to the PBX web interface, go to Settings > PBX > General > SIP > NAT.
4. In the drop-down list of NAT Type, select External Host.
5. Configure the NAT settings according to your network environment.



    - External Host: Enter the domain of the PBX and enter the external SIP port.
    - Local Network Identification: Enter the local network segment and the subnet mask. This setting will allow all your local devices to communicate with the PBX by the local IP address instead of passing through the router.

    Note:
    If you have multiple local network segments, click to add another Local Network Identification.

    - NAT Mode: Set to Yes.
6. Click Save and reboot the PBX to take effect.

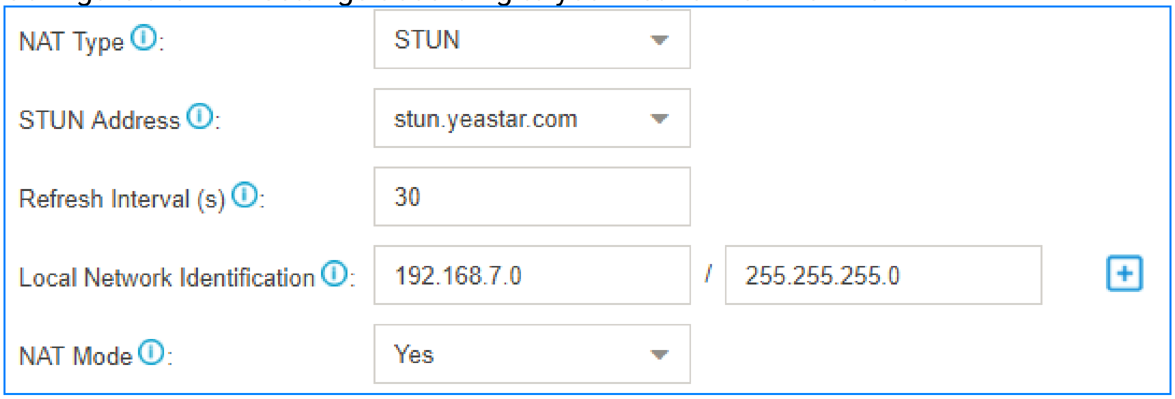
Set NAT with STUN

If your PBX has no static public IP address and domain name, you can set the NAT with STUN (Simple Traversal Utilities for NAT). STUN is a simple protocol for discovering the public IP address.

Important:
IPv6 network does NOT support this feature.

1. Forward the required ports on your router. (on page 163)
2. Log in to the PBX web interface, go to Settings > PBX > General > SIP > NAT.
3. In the drop-down list of NAT Type, select STUN.

4. Configure the NAT settings according to your network environment.



- STUN Address: Select the Yeastar STUN or customize a STUN.
- Local Network Identification: Enter the local network segment and the subnet mask. This setting will allow all your local devices to communicate with the PBX by the local IP address instead of passing through the router.

> Note:
> If you have multiple local network segments, click to add another Local Network Identification.

- NAT Mode: Set to Yes.

5. Click Save and reboot the PBX to take effect.

Static Route

Static Route Overview

Yeastar S1000-P IPPBX automatically adds system route entries to the routing table after you configure IP addresses on the PBX network interface. If you set the PBX network mode to Dual, you need to add a static route to override the default route entries, routing the packets from specific IP address to the specified destination.

System Route Entries

The system route entries are added to the routing table after you configure the PBX network interface.

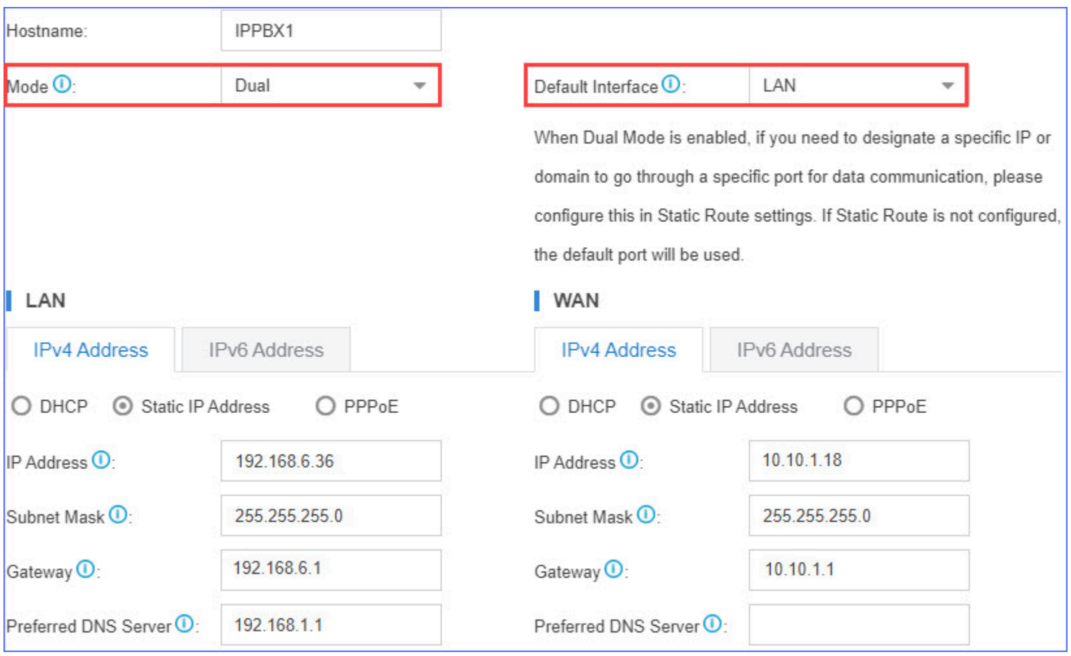
In the routing table, you can check the original rule after configuring the network settings:

- 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.
- A route entry for broadcast packets. The broadcast packets can be sent directly to the destination.

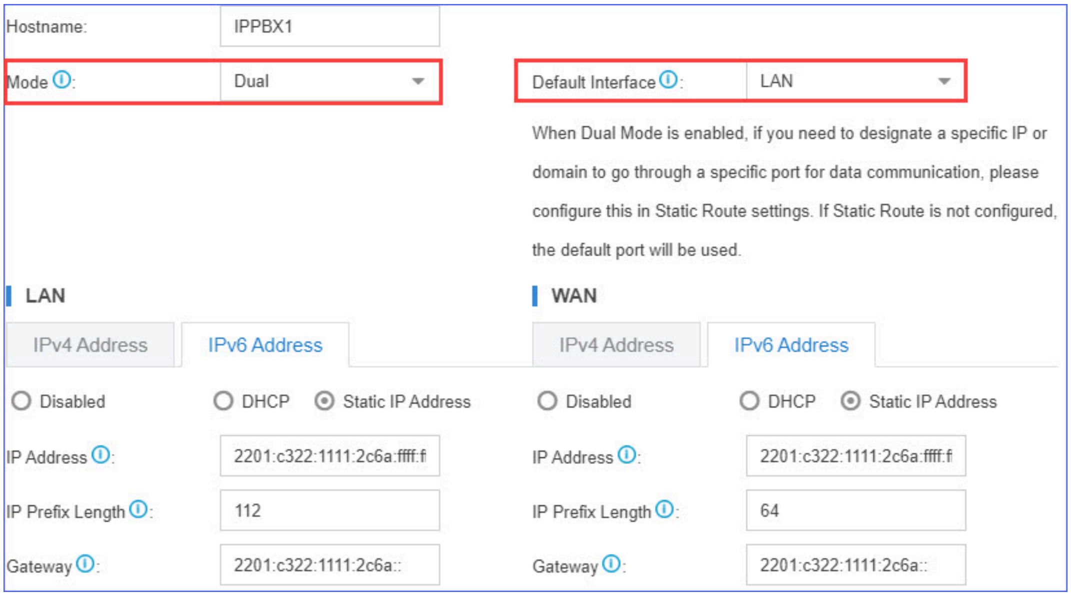
> **Note:**
> You cannot delete the default route entries from the routing table.

For example, you enable both LAN interface and WAN interface, and set LAN as the default network interface.

IPv4 address



IPv6 address



You can go to Settings > System > Network > Static Routes > Routing Table to check the routing entries.

The following route entries are automatically added to the routing table of the PBX.

IPv4 routing table

Destination	Subnet Mask	Gateway	Metric	Interface
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
224.0.0.0	224.0.0.0	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.
- The route entry with the Destination of `224.0.0.0` is the route entry that is automatically added for broadcast packets. The broadcast packets can be sent directly to the destination.

IPv6 routing table

Destination	IP Prefix Length	Gateway	Metric	Interface
default	0	2201:c322:1111:2c6a::	1	WAN
2201:c322:1111:2c6a::	64	::	256	WAN
2201:c322:1111:2c6a::	64	::	256	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 `2201:c322:1111:2c6a::` through WAN interface.
- The route entry with the Destination of `2201:c322:1111:2c6a::` is the route entry that is automatically added for WAN interface.

  The packets for the network `2201:c322:1111:2c6a::` 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 `2201:c322:1111:2c6a::` is the route entry that is automatically added for LAN interface.

  The packets for the network `2201:c322:1111:2c6a::` don't need to be routed. The network is locally connected, so packets can be sent directly to the destination.

Add a Static Route

If you set the network mode of Yeastar S1000-P IPPBX to Dual, you need to add a static route to override the default route entries, routing the traffic from specific IP address to the specified destination.

1. Go to Settings > System > Network > Static Routes > Static Routes.
2. Click IPv4 or IPv6 tab based on your network environment, then click Add.
3. In the pop-up dialog box, configure the route entry according to the following information.
    - Destination: Enter the destination IP address or IP subnet for the PBX to reach using the static route.
    - Subnet Mask: If IPv4 network is used, enter the subnet mask for the destination address.
    - IP Prefix Length: If IPv6 network is used, enter the IPv6 prefix for the destination address.
    - Gateway: Enter the gateway address. The PBX will reach the destination address through this gateway.
    - 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.
4. Click Save and Apply.

The static route is added to the routing table. Go to Settings > System > Network > Static Routes > Routing Table to check the routing table.

Manage the Static Routes

After you add static routes on the Yeastar S1000-P IPPBX, you can edit or delete them.

Edit a static route

1. Go to Settings > System > Network > Static Routes > 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. Go to Settings > System > Network > Static Routes > Static Routes.
2. Click beside the static route that you want to delete.
3. Click Yes to confirm the deletion.

System Management

System General Settings

The system general settings can be applied globally to Yeastar S1000-P IPPBX

System Preference

Configure the preferences settings that will be applied globally to the system.

Go to Settings > PBX > General > Preferences to configure the system preferences.

General Preference

Table 7. Description of General Preference

Option	Description
Max Call Duration	Select the global maximum call duration. Note: The precedence of Max Call Duration(s) (Global v.s. Extension (on page 37)): • For internal calls: The Max Call Duration(s) setting of the caller's extension takes precedence. • For outbound calls: The Max Call Duration(s) setting of the caller's extension takes precedence. • For inbound calls: The global Max Call Duration(s) setting takes precedence.
Attended Transfer Caller ID	The Caller ID that will be displayed on the recipient's phone. For example, Phone A (transferee) calls Phone B (transferor), and Phone B transfers the call to Phone C (recipient). If set to Transferor, the Caller ID displayed will be Phone B's number; if set to Transferee, Phone A's number will be displayed.
Distinctive Caller ID	When the incoming call is routed from Ring Group, Queue, or IVR, the Caller ID would display where it comes.
Match Route Permission When Seizing a Line	If checked, when users seize a line to place an outbound call, the call will succeed only when the route permission is matched.
Enable Call Priority Settings	If enabled, extension with higher call priority will cut off the call of lower one to dial out when the concurrent call limit is reached on the system.

Extension Preference

Below are default extension ranges. You can change the extension range according to your needs.

Note:
PBX treats Ring Group, Paging Group, Conference, Queue as extensions. Extension users can dial the extension numbers to reach them directly.

Extension Type	Default Range
User Extensions	1000 - 5999
Account Trunks	6100 - 6199
Ring Group Extensions	6200 - 6299
Paging Group Extensions	6300 - 6399
Conference Extensions	6400 - 6499
IVR Extensions	6500 - 6599
Queue Extensions	6700 - 6799

Feature Code

Feature codes are used to enable and disable certain features available in the Yeastar S1000-P IPPBX. Extension users can dial feature codes on their phones to use that particular feature.

Go to Settings > PBX > General > Feature Code to view or change the feature code settings.

- Feature Code Digits Timeout: The timeout to input next digit. The default is 4000 ms.

Default Feature Codes

Call Forwarding	
Reset to Defaults	*70
Enable Forward All Calls	*71
Disable Forward All Calls	*071
Enable Forward When Busy	*72
Disable Forward When Busy	*072
Enable Forward No Answer	*73
Disable Forward No Answer	*073
Extension's Voicemail	
Check Voicemail	*2

Call Forwarding	
Voicemail for Extension	**
Voicemail Main Menu	*02
Transfer	
Blind Transfer	*03
Attended Transfer	*3
DND	
Enable Do Not Disturb	*74
Disable Do Not Disturb	*074
Queue	
Switch the status of dynamic agents	*75
Call Pickup	
Call Pickup	*4
Extension Pickup	*04
Busy Camp-on	
Enable Busy Camp-on	*79
Disable Busy Camp-on	*079
Time Condition	
Time Condition Override	*8
Intercom	
Intercom	*5
Call Parking	
Call Parking	*6
Directed Call Parking	*06
Manager Extension Settings	
Enable Manager Extension	*76
Disabled Manage Extension	*076

SIP Settings

The SIP configurations require professional knowledge of SIP protocol, incorrect configuration may cause calling issues on the SIP extensions and SIP trunks.

Go to Settings > PBX > General > SIP to configure the SIP settings.

SIP General Settings

Option	Description
UDP Port	UDP Port used for SIP registrations. The default is 5060.
RTP Port	RTP Port for transmitting data. The From-port should start from 10000. From-port and To-port should have a difference value between 100 and 10000. The default is 10000-12000.
TCP Port	TCP Port used for SIP registrations. The default is 5060.
Local SIP Port	A random port in the port range will be used when sending packets to SIP server. The default range is 5062-5082.
Registration Timers	
Max Registration Time	Maximum duration (in seconds) of incoming registrations and subscriptions. The default is 3600 seconds.
Min Registration Time	Minimum duration (in seconds) of incoming registrations and subscriptions. The default is 60 seconds.
Qualify Frequency	How often to send SIP OPTIONS packet to SIP device to check if the device is up. The default is 30 per second.
Outbound SIP Registrations	
Registration Attempts	The number of registration attempts before giving up (0 for no limit).
Default Incoming/Outgoing Registration Time	Default duration (in seconds) of incoming/outgoing registration. The default is 120 seconds. Note: The actual duration needs to minus 10 seconds from the value you filled in.
Subscription Timers	
Max Subscription Time	Maximum duration (in seconds) of incoming subscriptions. The default is 3600 seconds.

Option	Description
Min Subscription Time	Minimum duration (in seconds) of incoming subscriptions. The default is 90 seconds.

NAT Settings

If your PBX is operating in a network connected to the internet through a single router, your PBX is behind NAT.

The NAT device has to be instructed to forward the right inbound packets (from internet) to the PBX server.

> Note:
> You need to configure NAT settings when you want to register a remote extension to the PBX or when you need to connect to the PBX via SIP trunk.

Yeastar S1000-P IPPBX supports 3 methods to configure NAT.

- Set NAT with External Host (on page 167)
- Set NAT with External IP Address (on page 167)
- Set NAT with STUN (on page 168)

SIP Codec

A codec is a compression or decompression algorithm that used in the transmission of voice packets over a network or the Internet.

Codec Selection

Yeastar S1000-P IPPBX supports G711 a-law, u-law, GSM, H261, H263, H263P, H264, SPEEX, G722, G726, ADPCM, G729A, MPEG4, opus and iLBC.

> Note:
>
> - You need to choose at least one same code on the PBX and on your phones, or there may be a problem of the call.
> - If you want to make video calls, you need to select H261, H263, H263P, H264, or MPEG4 codec on the PBX and on your phones.

iLBC Settings

The iLBC codec supports two modes: 20ms and 30ms frame length modes.

To get better voice quality, you need to set the iLBC mode according to your SIP endpoints.

TLS Settings

Option	Description
Enable TLS	Select the checkbox to enable TLS.
TLS Port	TLS Port used for SIP registrations. The default is 5061.
Certificate	Choose the TLS certificates.
TLS Verify Server	If set to `no`, don't verify the server certificate when acting as a client. If you don't have the server's CA certificate, you can set this and it will connect without requiring TLS CA file. The default is `no`.
TLS Verify Client	If set to `yes`, verify certificate when acting as server. The default is `no`.
TLS Client Method	Specify protocol for outbound client connections. The default is sslv2.

Session Timer

A periodic refreshing of a SIP session that allows both the user agent and proxy to determine if the SIP session is still active.

Option	Description
Session-timers	Choose the session timers mode on the system: • No: Do not include “timer” value in any field. • Supported: Include “timer” value in Supported header. • Require: Include “timer” value in Require header. • Forced: Include “timer” value in both Supported and Required header. The default is Supported.
Session-Expires	The max refresh interval in seconds.
Min-SE	The min refresh interval in seconds, it must not be less 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 could provide priority for users by setting the value.

Option	Description
ToS SIP	Type of Service for SIP packets.
ToS Audio	Type of Service for RTP audio packets.
ToS Video	Type of Service for RTP video packets.
CoS 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 don't work.

Option	Description
No T.38 Attributes in Re-invite SDP	If this option is selected, SDP re-invite packet will not contain T.38 attributes.
Error Correction	Enable or disable Error Correction for the fax.
T.38 Max BitRate	Adjust the max BitRate for T.38 fax.

Advanced SIP Settings

Option	Description
PBX Transmits Media Stream	When enabled, the media stream of the SIP terminal will be forwarded through the PBX. When disabled, the media streams will be sent directly between the terminals without being forwarded through the PBX. Note: If disabled, the Call Parking and Transfer feature will not be available.
User Agent	Change the User-Agent field.
Send Remote Party ID	Whether to send Remote-Party-ID in SIP header or not.

Option	Description
	Note: This configuration only takes effect on internal calls. To set up for external calls, configure the Advanced settings of SIP trunk.
Send P Asserted Identify	Whether to send P-Asserted-Identity in SIP header or not. Note: This configuration only takes effect on internal calls. To set up for external calls, configure the Advanced settings of SIP trunk.
Send Diversion ID	Whether to send Diversion in SIP header or not. If this option is selected, the Diversion value will be extension number. Note: This configuration only takes effect on internal calls. To set up for external calls, configure the Advanced settings of SIP trunk.
Support Early Media	Whether to support Early Media or not.
All Busy Mode for SIP Forking	• Check this option: When one of the terminals that register the same extension number is busy in a call, other terminals will not receive calls. • Uncheck this option: When one terminal is busy, other terminals will still be able to make and receive calls.
Inband Progress	This 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 config file.

Option	Description
	• 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.
Get Caller ID From	Decide the system will retrieve Caller ID from which header field.
Get DID From	Decide the system will retrieve DID from which header field. Note: If Remote-Party-ID is selected but the SIP trunk doesn't support this, the system will retrieve DID fron INVITE header.
100rel	Whether to support 100rel or not.
Allow Guest	If this option is selected, PBX will accept the unknown calls.
Support Message Request	Whether to support SIP Message Request or not.
Maxptime	Select or enter the Maxptime value.
Notify Caller ID	If checked, when extension A has an inbound call, PBX will send the call's Caller ID information to the extension that has subscribed to the A's call status. Displaying caller ID information can be useful to help an agent decide whether to pick up an incoming call. This option is disabled by default.
DTMF Passthrough	If DTMF Passthrough is enabled, PBX will not process the DTMF tones, and pass DTMF tones transparently to the other end.

Jitter Buffer Settings

A jitter buffer is used at the receiving equipment to store incoming RTP packets, re-align them in terms of timing and check whether they are in the correct order. If some arrive slightly out-of-sequence, provided it is large enough, the jitter buffer can put them back into the right sequence. However, for this to work, the receiving device must delay the audio very slightly while it checks and reassembles the packet stream.

Jitter Buffer Settings

Go to Settings > PBX > General > Jitter Buffer to enable and configure jitter buffer settings.

Option	Description
Enable Jitter Buffer	Whether to enable jitter buffer.
Select which trunk(s) to enable Jitter Buffer	Enable jitter buffer for the selected trunks. The outbound audio through the selected trunk will be dejittered by jitter buffer on the other side.
Select which extension(s) to enable Jitter Buffer	Enable jitter buffer for the selected extensions. The received audio on the selected extension will be dejittered by jitter buffer. Note: In the following conditions, jitter buffer will not work for the selected extensions: • In an internal call, the audio is received from an analog phone. • In an external call, the other side sends audio through a non-SIP trunk, and jitter buffer is not enabled for the trunk.
Implementation	The implementation of jitter buffer. • Fixed: The length of jitter buffer will always be the size defined by Jitter Buffer Size. • Adaptive: The length of jitter buffer will vary in size within the range of min size and max size based on current network condition.
Adaptive Adjustment Size	The size of each adaptive adjustment of jitter buffer. The default is 50ms. If set by default, the jitter buffer size will be adjusted dynamically based on current network condition. It will start from 0 ms and grows at a size of 50 ms each time.

Option	Description
Max Jitter Buffer Size	The maximum value of adaptive jitter buffer.

Security

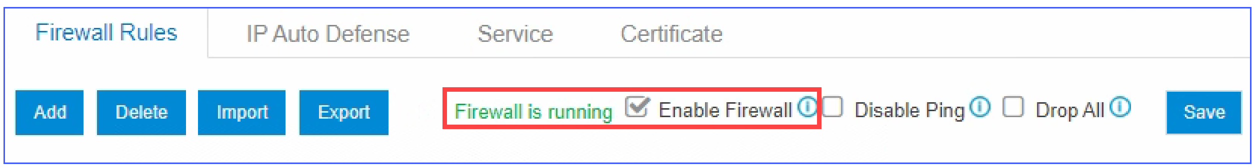
Firewall Rules

We strongly recommend that you enable and configure firewall on the PBX to prevent attack fraud or call loss.

Enable Firewall on the PBX

Go to Settings > System > Security > Firewall Rules, select the checkbox of Enable Firewall.

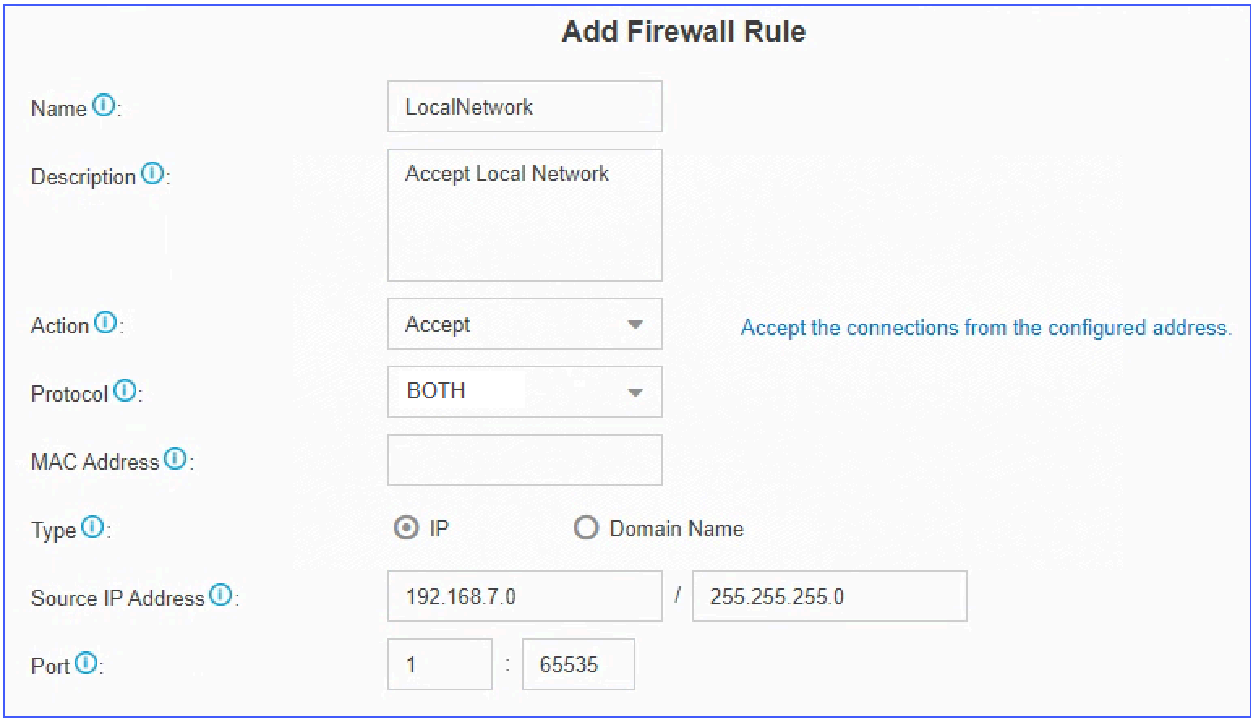
If firewall is enabled, the page will show "Firewall is running", and the firewall rules will work to protect your PBX.



Firewall Rules

Firewall rules are pre-configured rules to control and filter traffic that are sent to the PBX. You can create firewall rules to filter specific source IP address or domain name, ports, MAC address.

Go to Settings > System > Security > Firewall Rules to configure the firewall rules.



- Name: Set a name to identify the firewall rule.
- Description: Optional. Description for this firewall rule.
- Action: Choose the action for the firewall rule.
    - Accept
    - Drop
    - Reject
- Protocol: Choose the protocol that is applied to the rule.
    - UDP
    - TCP
    - BOTH: Both TCP and UDP.
- MAC Address: Optional. The MAC address that is applied to the rule.

  The format of MAC address is `XX:XX:XX:XX:XX:XX`.
- Type: Choose the network type of the source traffic.
- Source IP Address: Enter the network information of source traffic.
    - If IPv4 address is used, enter IPv4 address and subnet mask.
    - If IPv6 address is used, enter IPv6 address and IPv6 prefix.
- Domain Name: The domain name of the source traffic.
- Port: The port of the source traffic.

Additional Firewall Settings

The PBX provides additional firewall settings to enhance the system security.

- Disable Ping: The PBX will disable Ping response (ICMP echo).
- Drop All: The PBX will drop all the packets and connections from other hosts except the accepted/trusted IP address/domain that is defined in the firewall rules.

> Note:
> To avoid that you cannot access the PBX:
> - Create a backup on the PBX before you enable Drop All.

Examples of Firewall Rules

In this topic, we provide configuration examples of firewall rules under different scenarios. We recommend that you configure firewall rules according to the network environment of your PBX.

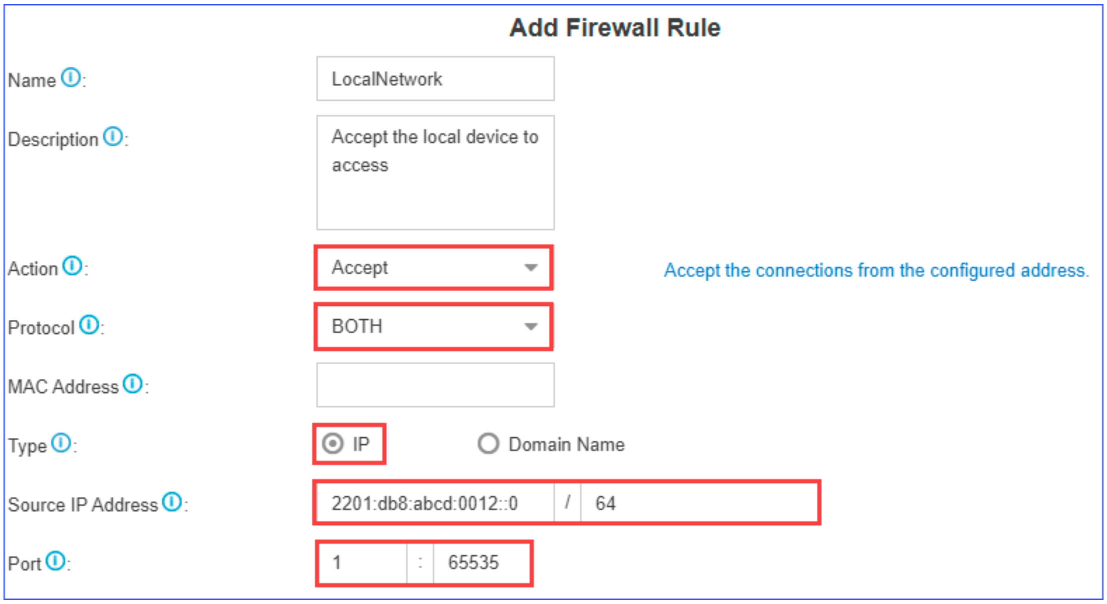
Log in to the PBX web interface, go to Settings > System > Security > Firewall Rules, and configure firewall rules as follows.

- Add a trusted IP address to whitelist, or PBX may blacklist the IP address as it frequently sends packets.
- Add an untrusted IP address to blacklist, preventing the IP address from accessing PBX.

Accept access of local network

If PBX often blacklists local phones which are under the same network segment, you can configure a firewall rule to allow all IP addresses under the same network segment to access the PBX.

For example, the range of local IP address is 2201:0DB8:ABCD:0012:0000:0000:0000:0000 - 2201:0DB8:ABCD:0012:FFFF:FFFF:FFFF:FFFF. You can set a firewall rule as follows.



Accept remote extensions and remote web access

If you want to remotely access PBX web page or register extensions, you can add the public IP address to the whitelist, or PBX may blacklist the public IP address as it frequently sends packets.

For example, the trusted public IP address is 2001:c322:1111:2c6a:ffff:ffff:ffff:2000. Set the firewall rule as follows.

> **Note:**
> If the remote place doesn't have a static public IP address, you can set a firewall rule for the trusted domain name.

Accept traffic of VoIP Provider

Accept the traffic of SIP registration port and RTP media ports from the VoIP provider.

For example, the IP address of the VoIP provider is 2408:824c:200::2b8b:336f:cc9c; port of SIP registration is 5630; the range of RTP ports is 10000-12000. You need to set two firewall rules for the VoIP provider.

- Accept traffic of the SIP registration port

- Accept traffic of the RTP ports

Accept traffic of NTP, SMTP, POP, STUN

We recommend that you accept traffic of NTP, SMTP, POP, STUN, and keep the default auto defense rules (on page 191).

For example, the IP address of the NTP server is 2001:0db8::4101. Set the firewall rule as the following figure.

Block untrusted web access

After you have added firewall rules to accept access of local network (on page 186) and remote web access (on page 187), you can add a firewall rule to block untrusted web access.

> **Note:**
> Many attacks are caused by web access. We recommend that you block the untrusted web access.

For example, the IP address is ::; subnet mask is 0; the port of web access is 8088, which indicate that PBX denies all web access.

Allow trusted web access with Drop All enabled

If Drop All is enabled, PBX will block web access that does not comply with the preconfigured rules. You can add trusted IP addresses to the whitelist to accept the web access.

> **Note:**
> Enable Drop All with caution, or Web, SSH feature may fail to work.

If PBX is mapped to public network, and only local IP and the specified WAN IP can access the PBX, you need to configure firewall rules as follows.

1. Enable Drop All.
2. Add a firewall rule to accept access of local network (on page 186).
3. Add a firewall rule to allow the specified WAN IP to access the PBX.

   For example, the IP address of VoIP provider is 2001:DB8:A00:1::1; port of SIP registration is 5060, you should configure a firewall rule to allow the traffic of SIP registration port from VoIP provider as follows.

The following ports are in common use, you should configure ports according to the actual scenario.

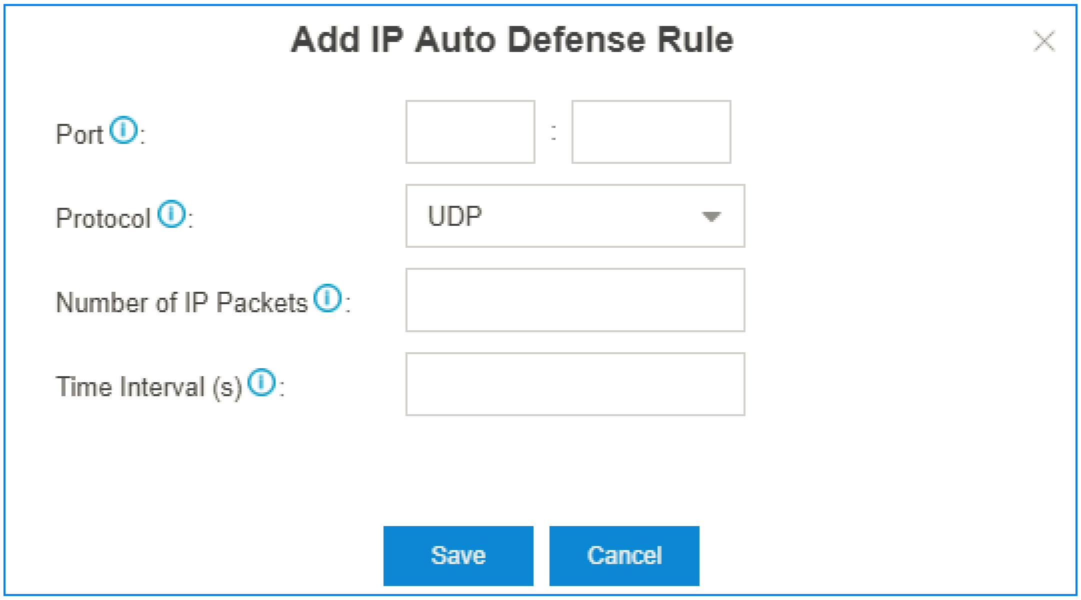
Description	Port	Protocol
SIP port	5060	UDP & TCP
Web access port	80/8088	TCP
SSH port	8022	TCP
RTP port	10000-12000	UDP

IP Auto Defense

Yeastar S1000-P IPPBX has default auto defense rules to prevent massive connection attempts or brute force attacks.

> **Important:**
>
> - Do NOT delete the default IP defense rules.
> - Change the default IP defense rules under the instruction of Yeastar support.

Go to Settings > System > Security > IP Auto Defense > Auto Defense Rules to configure auto defense rules.



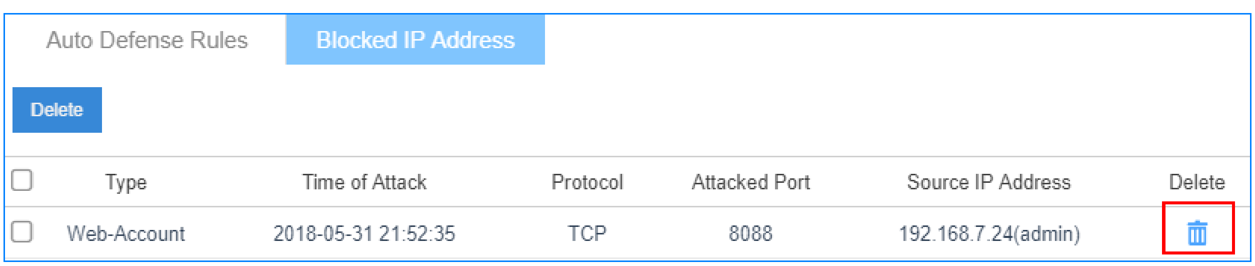
- Port: The auto defense port.
- Protocol: The protocol of the auto defense port.
- Number of IP Packets: The number of IP Packets permitted within a specific time interval.
- Time Interval: The time interval to receive IP Packets.

  For example, Number of IP Packets is `90` and Time Interval is `60`; The PBX will block the IP that sends more than 90 IP packets in 60 seconds.

Blocked IP Address

The PBX will block an IP address for too many failed login attempts or too many failed registration attempts.

The blocked IP addresses would be listed in the Blocked IP Address table. If a trusted IP address was blocked by the PBX, you can go to Settings > System > Security > IP Auto Defense > Blocked IP Address to delete the IP address.



Service

All the PBX service statuses and ports are displayed on the security service page.

Go to Settings > System > Security > Service to configure the service settings.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Auto Logout Time (min)</td><td>After the set time of inactivity, the session will automatically log out. The default time is 15 minutes.</td></tr>
<tr><td>Web Login Mode</td><td>Users can log in to the web interface with extension number, email address or both.
Extension: Use an extension number as the username to log in.
Email: Use an email address as the username to log in. The email address is associated with extension number.
Note:
Users are not allowed to log in to web interface if neither Extension nor Email is checked.
The super administrator can always log in to the web interface by the username "admin".</td></tr>
<tr><td>Allow Weak Password</td><td>By default, strong password is required for Extension Registration Password and Extension User Password.
If weak password is enabled, the PBX will allow a weaker password to be configured.
Note:
Reconsider it before you enable Weak Password. A weak password will make your PBX system easily be attacked by brute force methods.</td></tr>
<tr><td>Protocol</td><td>Select the web protocol. The default web protocol is HTTPS.</td></tr>
<tr><td>Port</td><td>Select the web port. The default port is 8088.
Note:
The port 8090 is reserved port which can't be assigned.</td></tr>
</table>

Option	Description
Redirect from port 80	If the option is enabled, when you access the PBX using HTTP with port 80, it will be redirected to HTTPS with port 8088.
Certificate	Select a certificate for HTTPS. The default is None.
Enable SSH	SSH port is used to access the PBX underlying configurations to debug the system. The default SSH port is 8022. Note: Disable SSH port if you don't need to debug the system.
SIP UDP Port	SIP registration port. The default SIP UDP port is 5060.
Enable SIP TCP	Whether to enable SIP TCP or not. The default port is 5060.
Enable SIP TLS	Whether to enable SIP TLS or not. The default port is 5061.

Set up Yeastar S1000-P IPPBX with HTTPS

Yeastar S1000-P IPPBX supports HTTPS protocol to secure SIP messaging. 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 address and secures your data transmission.

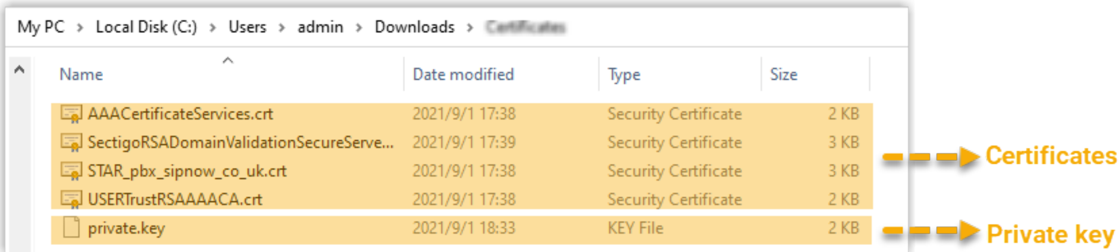
In this article, we assume that you have set up Dynamic DNS (DDNS) on the PBX system, and you can access the system via a domain name. Refer to the following instructions to set up your PBX system with HTTPS.

Procedure

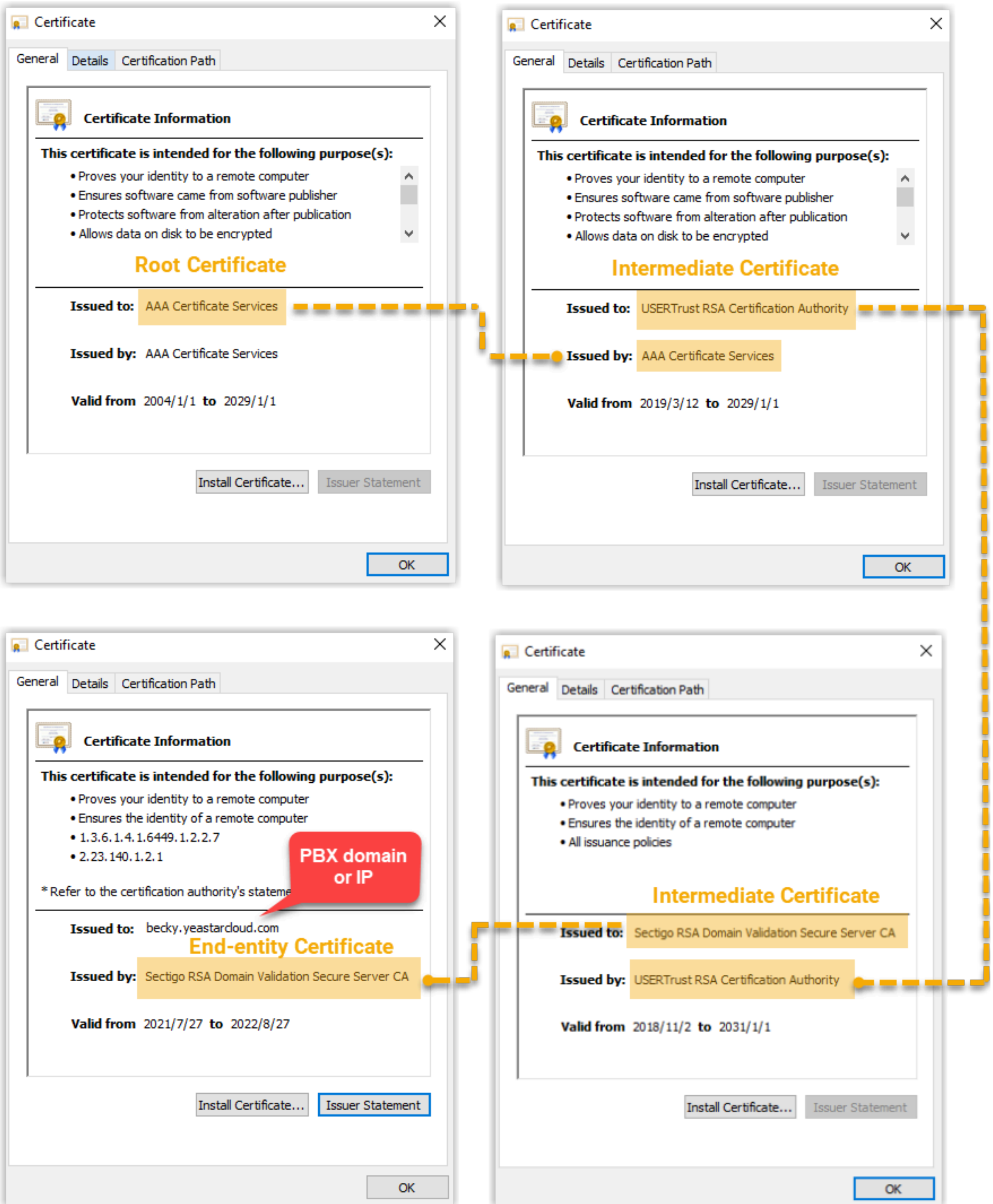
1. Buy a Wildcard SSL certificate from a Certified Authority (CA).

   > Tip:
   > A Wildcard SSL certificate is a single certificate with a wildcard character (*) in the domain name field. This allows the same certificate to be shared across multiple hosts within your organization. For example, a wildcard certificate for `*.(domainname).com` can be used for `www.(domainname).com`, `mail.(domainname).com`, `store.(domainname).com`.

   You may get a root certificate, intermediate certificate, end-entity certificate, and private key.

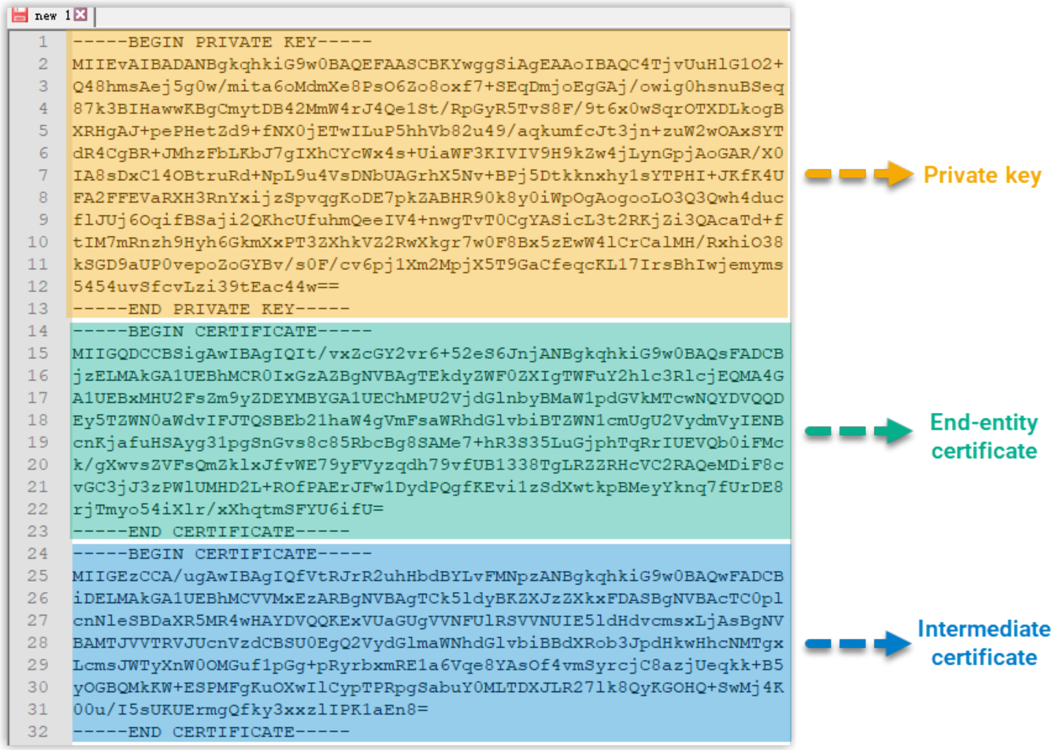


2. Double click certificates to check certificate type and identify the SSL certificate chain.
    - Root Certificate: A self-signed certificate used to sign other certificates.
    - Intermediate certificate: A certificate that is signed by either a Root Certificate or another Intermediate Certificate, and that signs either End-entity Certificate or other Intermediate Certificate.
    - End-entity Certificate: A certificate that can not be used to sign other certificates.

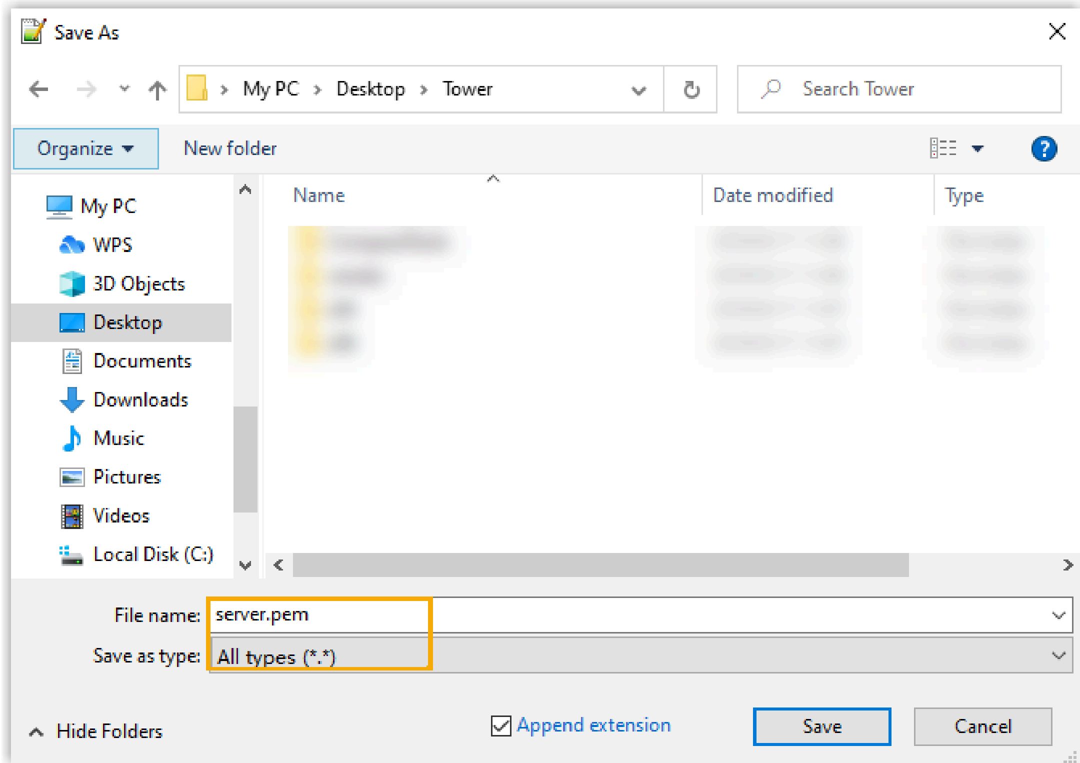


3. Create a `.pem` file to store the certificates and private key.
    a. Open a text editor (e.g. Notepad++).
    b. Click File > New.
    c. Copy and paste your certificates and private key in the following order (from the top down):

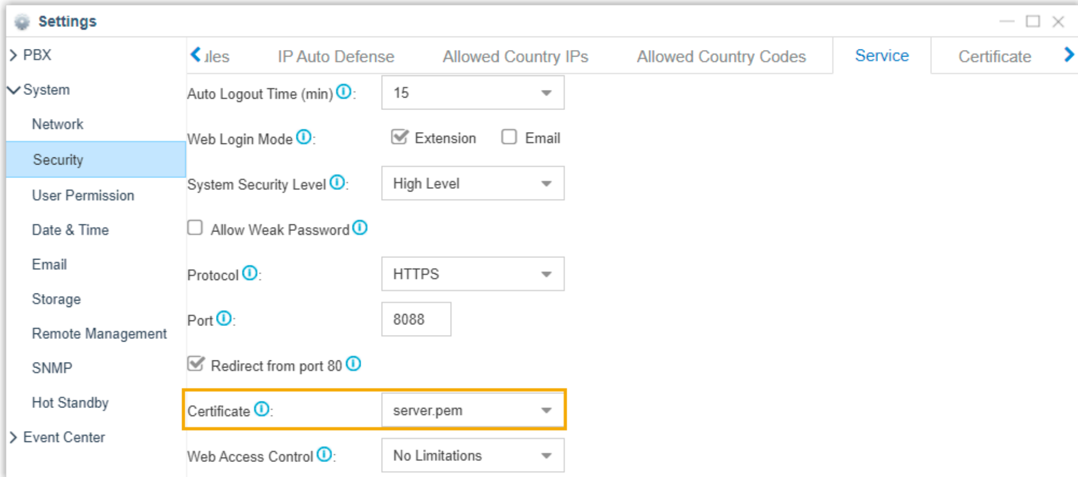
- Private Key
- End-entity Certificate
- Intermediate Certificate that issues the End-entity Certificate



d. Click File > Save as, set Save as type to All types (*.*), and set File name to `server.pem`, then click Save.



4. Upload the `.pem` certificate file to the PBX web interface.
    a. Log in to the PBX web interface, go to Settings > System > Security.
    b. Under Certificate tab, click Upload.
    c. In the pop-up window, select PBX Certificate from the drop-down list of Type, and browse to the `server.pem` file.
    d. Click Upload and OK.
    e. Reboot the PBX to take effect.
5. Set the `.pem` certificate file as the certificate for HTTPS protocol.
    a. Go to Settings > System > Security.
    b. Under Service tab, select the `.pem` certificate file from the drop-down list of Certificate.



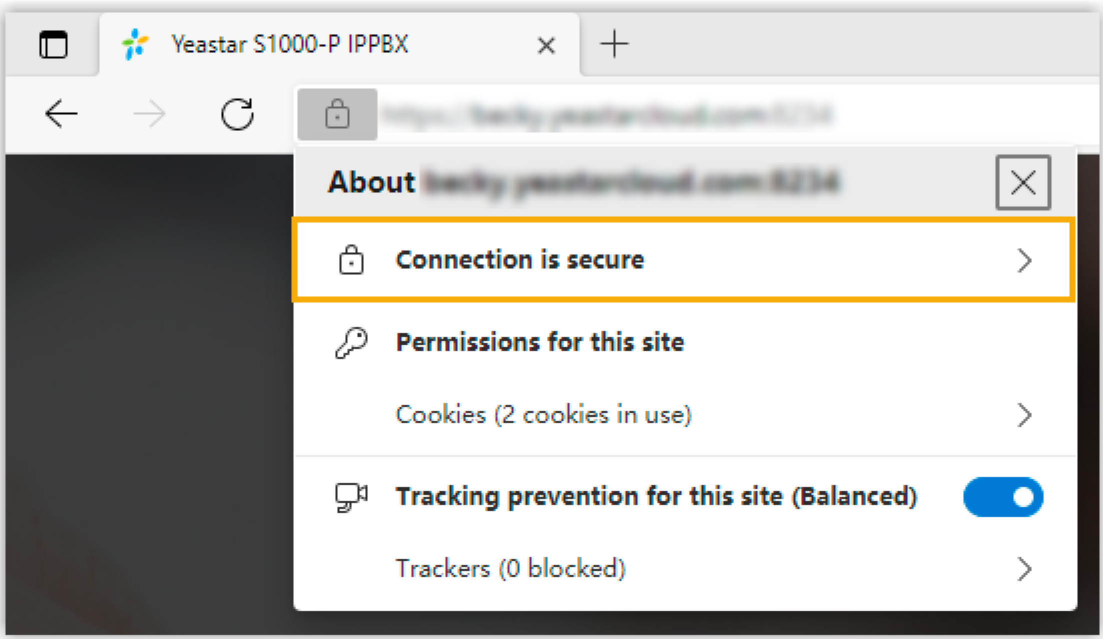
c. Click Save.

6. Refresh the web page.

Result

On the address bar, connection to your PBX system is displayed as "secure".

> Note:
> If it still displays "Not secure", try to clear your web browser's cache, then refresh the web page.



Upload TLS Certificates to Yeastar S1000-P IPPBX

Yeastar S1000-P IPPBX supports TLS protocol to secure SIP messaging.

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 (Settings > General > SIP > TLS > TLS Verify Client), you need to upload a client certificate to both PBX and TLS client, or the TLS connection would fail.
- When the PBX acts as a client, whether a client certificate is required depends on the server.

  If the PBX requires to verify TLS server (Settings > General > SIP > TLS > TLS Verify Server), you need to upload a server certificate.

Upload a TLS server certificate

Prerequisites

You have prepared a server certificate in `.pem` format.

Procedure

1. Log in to PBX web interface, go to Settings > System > Security > > Certificate.
2. Click Upload.
3. In the Type drop-down list, choose PBX Certificate.
4. Click Browse to select the desired certificate.
5. Click Upload.
6. Click Yes to reboot the system.

Upload a TLS client certificate

Prerequisites

You have prepared a client certificate in `.cer` or `.crt` format.

Procedure

1. Log in to PBX web interface, go to Settings > System > Security > > Certificate.
2. Click Upload.
3. In the Type drop-down list, choose Trusted Certificate.
4. Click Browse to select the desired certificate.
5. Click Upload.

Result

The certificate is uploaded successfully, and is displayed on Certificate list.

Ports Used on Yeastar S1000-P IPPBX

This topic lists all the ports used on Yeastar S1000-P IPPBX.

Port	Status	Protocol	Service	Changeable	Description
80/8088	Enabled	TCP	HTTP/ HTTPS	8088 is changeable at the path Settings > System > Security > Service > Port.	Used to access the PBX web interface.
8022	Disabled	TCP	SSH	8022 is changeable at the path Settings > System > Security > Service > Enable SSH.	Used to access the PBX underlying configurations to debug the system.
123	Enabled	UDP	NTP	Unchangeable.	Used for NTP service.
3306	Enabled	TCP	MySQL	Unchangeable.	Used for MySQL service.
873	Disabled	TCP	Rsync	Unchangeable.	Used for Hot Standby.
6088	Disabled	UDP	heartbeat	Unchangeable.	Used for Hot Standby.
5038	Disabled	TCP	AMI	Unchangeable.	Used for Asterisk Manager Interface (AMI).
5060	Enabled	TCP & UDP	SIP	5060 is changeable at the path Settings > System > Security > Service > SIP UDP Port & Enable SIP TLS.	Used for SIP registration.
5061	Disabled	TCP	SIP	5061 is changeable at the path Settings > System > Security > Service > Enable SIP TLS.	Used for SIP TLS service.

Port	Status	Protocol	Service	Changeable	Description
5062-5082	Disabled	TCP & UDP	SIP	5062-5082 are changeable at the path PBX > General > SIP > General > Local SIP Port	Random ports are used when sending packets to SIP server.
10000-20000	Enabled	UDP	RTP	RTP ports are changeable at the path Settings > PBX > General > SIP > RTP Port.	Used for handling media during a call.
1194	Disabled	TCP & UDP	OpenVPN	1194 is changeable at the path Settings > System > Network > OpenVPN > Server Port.	Used to connect OpenVPN clients to PBX VPN Server.
8094	Disabled	TCP	OpenVPN	Unchangeable.	Used for OpenVPN.
8090	Disabled	TCP & UDP	Remote Management	Unchangeable.	Used for Remote Management.
139	Disabled	TCP	Network Drive	Unchangeable.	Used for storing recording files on Network Drive.
445	Disabled	TCP	Network Drive	Unchangeable.	Used for storing recording files on Network Drive.
8090	Disabled	UDP & TCP	Cwmp-client	Unchangeable.	Used for Remote Management.
2222	Disabled	UDP	Cwmp-client	Unchangeable.	Used for Remote Management (STUN).

User Permission

By default, the extension users can log in to the system and check their own settings and CDR. You can set different permission to the users according to their roles and duty.

User Types on the PBX

Super Admin

Super Admin has the highest privilege. The super administrator can access all pages on the web and make all the configurations on the system.

- Username: `admin`

Administrator or Custom User

Administrator or Custom User is created by the Super Admin. The Super Admin sets the privileges for those users according to their roles and duty.

- Username: The extension number or the email address of the extension user.

> Note:
>
> - Administrator and Custom User can have the same permission. The difference between the two role types is shown below:
>   - Administrator: All permissions are enabled by default.
>   - Custom User: No permission is enabled by default.
> - Administrator and Custom User do not have permission to configure User Permission.

Configure User Permission

To grant more privileges for a user or change a user's privilege, you need to configure the User Permission on PBX.

Scenarios

In the following scenarios, you may need to add permissions for the extension users according to their roles.

- For an HR, he/she may need the permission to add extension, configure extension's outbound route privilege when there are new staffs.
- For a supervisor, he/she will have permission to check the CDR, but have no permission to configure the system or other extensions.

Procedures

1. Log in to the PBX web interface by `admin` account, go to Settings > System > User Permission, click Add.
2. On the configuration page, select the User.
3. Set the Set Privilege As.
    - Administrator: All the permissions are enabled for the user by default.
    - Custom: No permission is enabled for the user by default.

4. Click Settings, CDR, Monitor, Application, or Others tab, and check or uncheck the relevant options for the user.
5. Click Save and Apply.

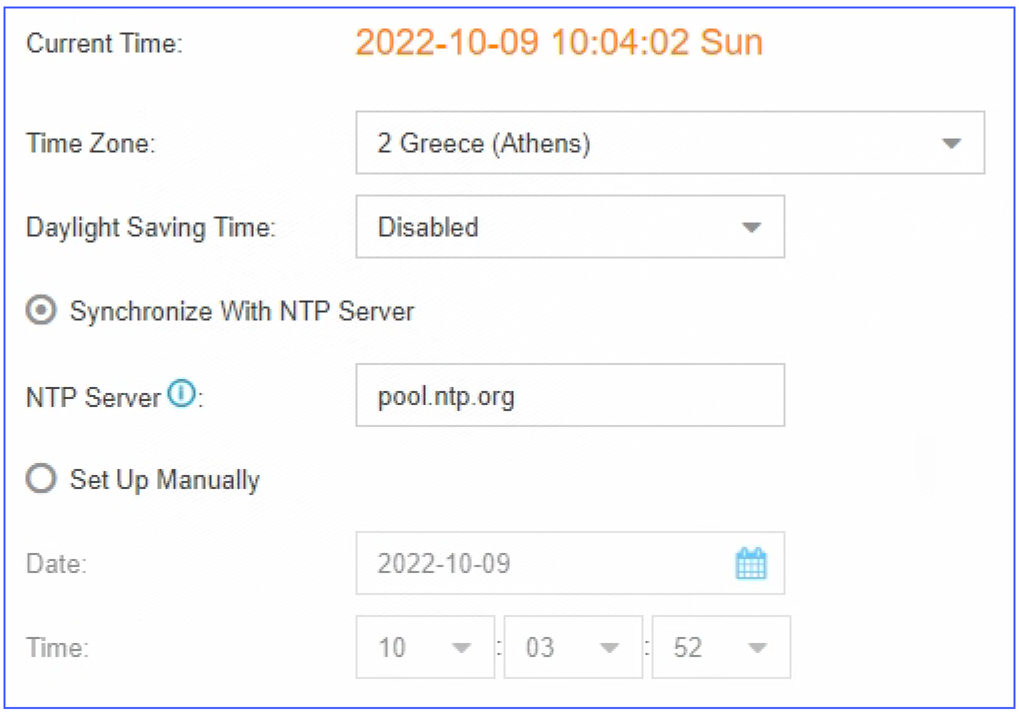
   Results: When the user logs in to the PBX web interface by the extension user account, he/she can access the permitted configuration page.

Date and Time

To ensure that the time of logs and CDR is consistent with your local time , you need to adjust the date and time of the PBX.

On the Date & Time configuration page, you can see the current time of the PBX.

You can set the PBX time to be synchronized with an NTP server or set the time manually.



Change the PBX Time

1. Go to Settings > System > Date & Time.
2. Select your current and correct Time Zone.
3. Enable Daylight Saving Time if you need it in your place.
4. Select Set Up Manually and set the Date and Time according to your local time.
5. Click Save.
6. Reboot the PBX to take effect.

Synchronize PBX Time with NTP Server

If you synchronize the PBX time with an external NTP server, the PBX will adjust its internal clock to a central network server.

> Note:
> Make sure that the PBX can access the Internet, or the PBX cannot synchronize its time from the NTP server.

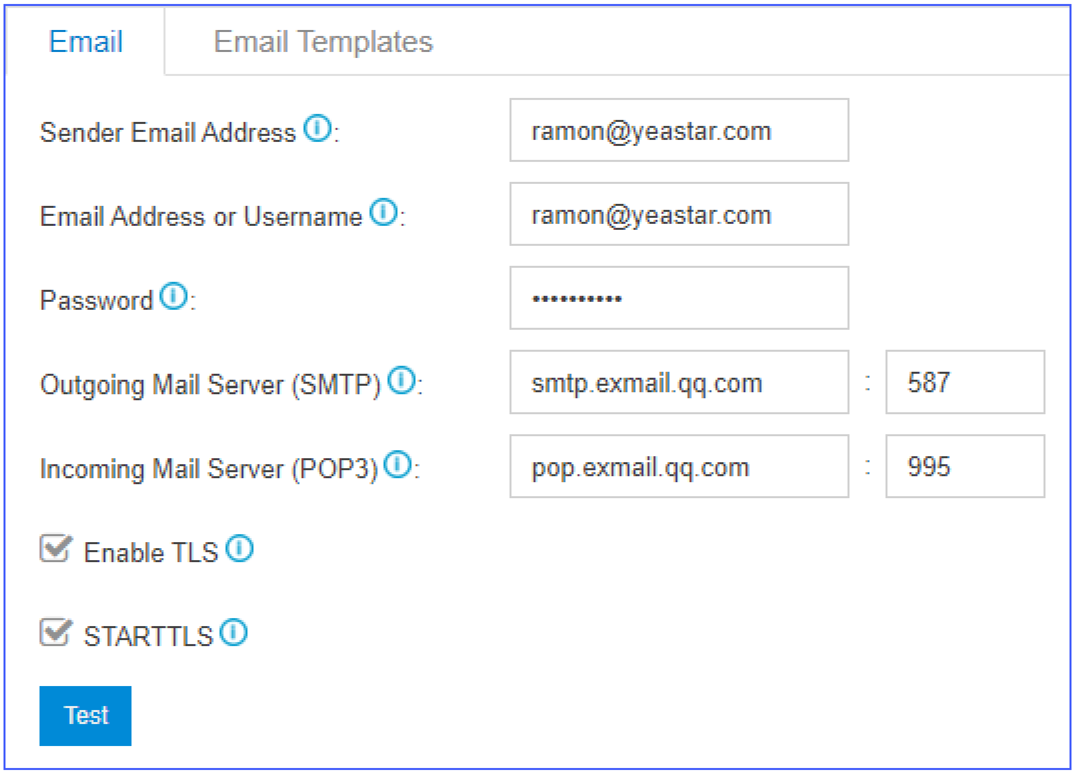
1. Go to Settings > System > Date & Time.
2. Select your current and correct Time Zone.
3. Enable Daylight Save Time if you need it in your place.
4. Select Synchronize With NTP Server and set the NTP Server.
5. Click Save.
6. Reboot the PBX to take effect.

Email

The system email can be used to reset password, send voicemail to email, send alert event emails, and send fax to email. To make these features work, you need to set up the PBX system email.

Set up System Email

1. Go to Settings > System > Email to set up the system email.



- Sender Email Address: Enter an available email address.
- Email Address or Username: If the email server supports User Name, enter user name. If not,enter the email address.
- Password: Enter the login password of the email address.
- Outgoing Mail Server (SMTP): Enter the outgoing mail server and port according to the email server.
- Incoming Mail Server (POP3): Enter the incoming mail server and port according to the email server.
- Enable TLS: Enable or disable TLS during transferring/submitting your Email to another SMTP server.

> Note:
> For Gmail or Exchange server, you need to enable TLS.

- STARTTLS: If you enable TLS, the STARTTLS is enabled by default . If the mail server doesn't support STARTTLS, do not select this option.

2. Click Test to check if the email works.
3. Click Save to save the email settings.

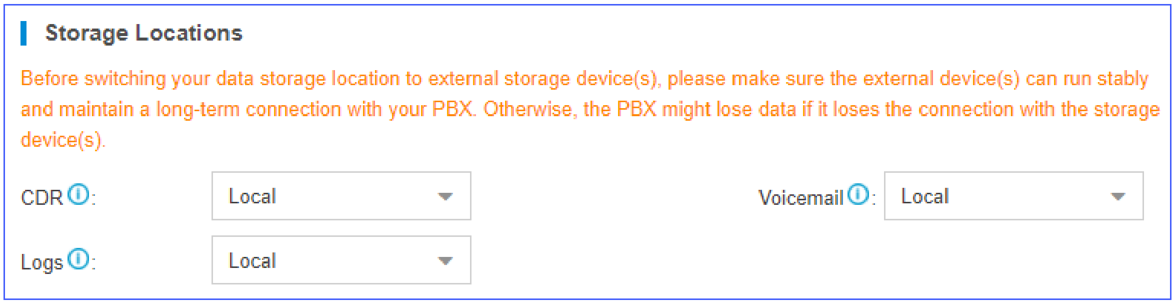
Storage

Yeastar S1000-P IPPBX provides local storage and supports . You can choose where to store the CDR, voicemail, logs, and backup files.

Storage Locations

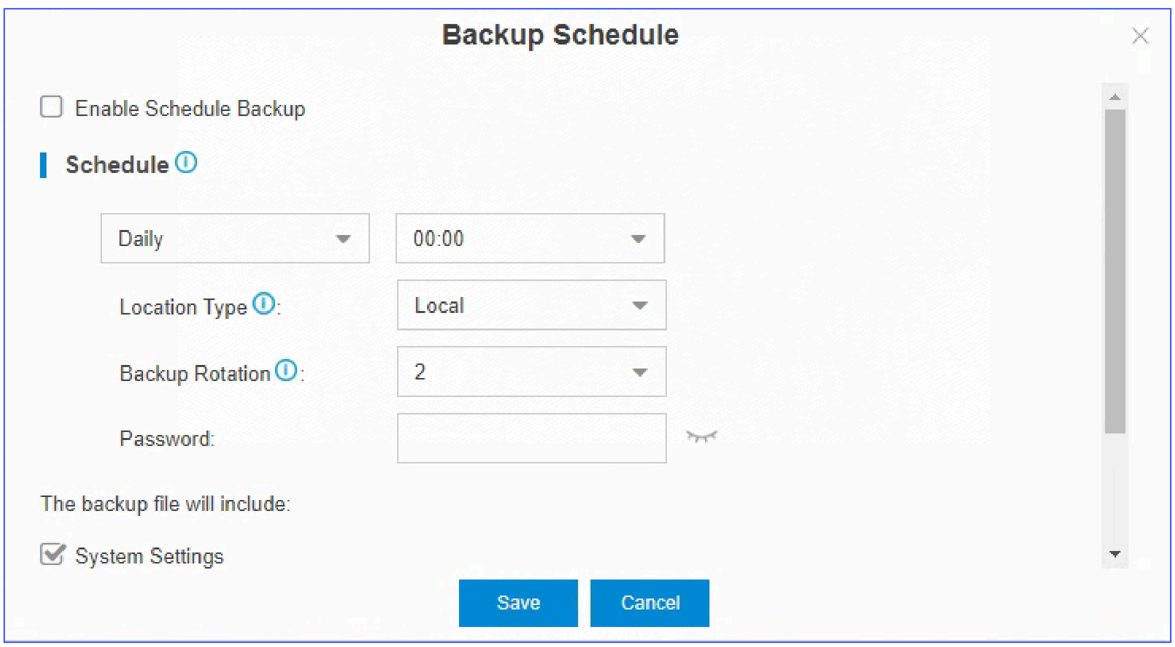
- CDR, Voicemail, and Logs

  Go to Settings > System > Storage > Preference to change the storage locations for CDR, Voicemail, and Logs.



- Backup Files

  When you set a backup schedule, you can choose the storage location of the backup files.



Storage Devices

The Storage Devices section shows the local storage. You can click to check or configure the storage device.

Auto Cleanup

Auto Cleanup is a feature that can auto clean your CDR, voicemail, and logs periodically.

Table 8. Configuration Parameters of Auto Cleanup

CDR Auto Cleanup	
Max Number of CDR	Set the maximum number of CDR that should be retained. The old CDR will be deleted when the threshold is reached.
CDR Preservation Duration	Set the maximum number of days that CDR should be retained.
Voicemail Auto Cleanup	
Max Number of Files	Set the maximum number of voicemail that should be retained. The old voicemail will be deleted when the threshold is reached.
Files Preservation Duration	Set the maximum number of minutes that voicemails should be retained.
Logs Auto Cleanup	
Max Size of Total Logs	Limit the total size of pbxlog files in syslog. The old logs will be deleted when the threshold is reached.
Logs Preservation Duration	Set the maximum number of days that system logs should be retained respectively.
Max Number of Logs	Set the maximum number of event logs and operation logs that should be retained. The old logs will be deleted when the threshold is reached.

Event Center

You can set the PBX to send notifications when specific events or errors occur, notifying you via email.

For example, the system can automatically send a notification when the network connection is lost, VoIP trunk registration is failed, storage volume is running out of space, or the administrator password is changed.

Event Settings

Go to Settings > Event Center > Event Settings to configure the event settings.

- Record

  indicates that Record function is enabled. When the event occurs, the PBX will record the event in Event Log.

  indicates that Record function is disabled.

- Notification

  indicates that Notification function is enabled. When the event occurs, the PBX will send notification to the Notification Contacts.

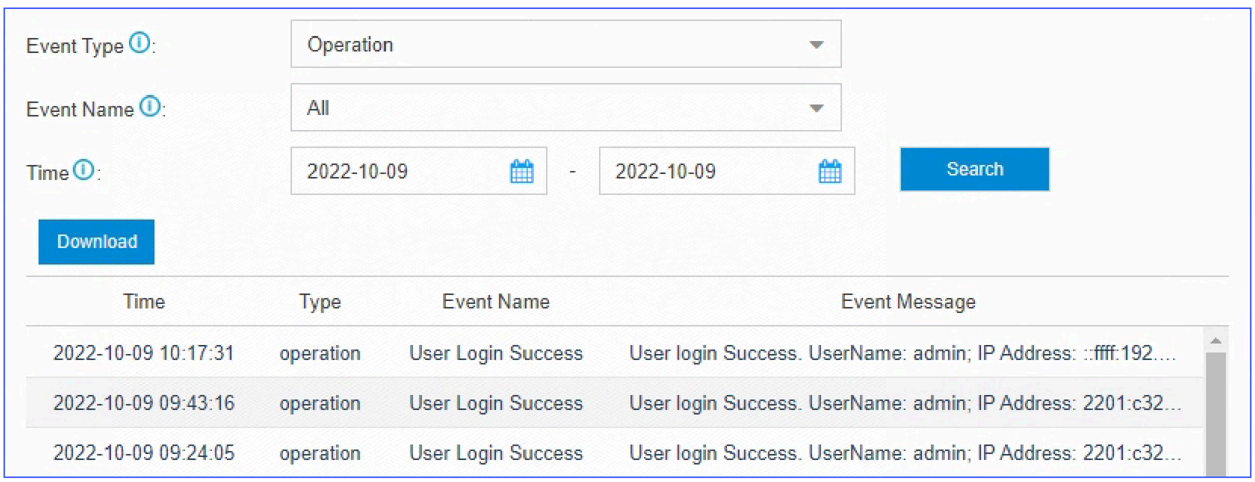
  indicates that Notification function is disabled.

- Edit Notification

  Click to edit the template of notification email.

Event Log

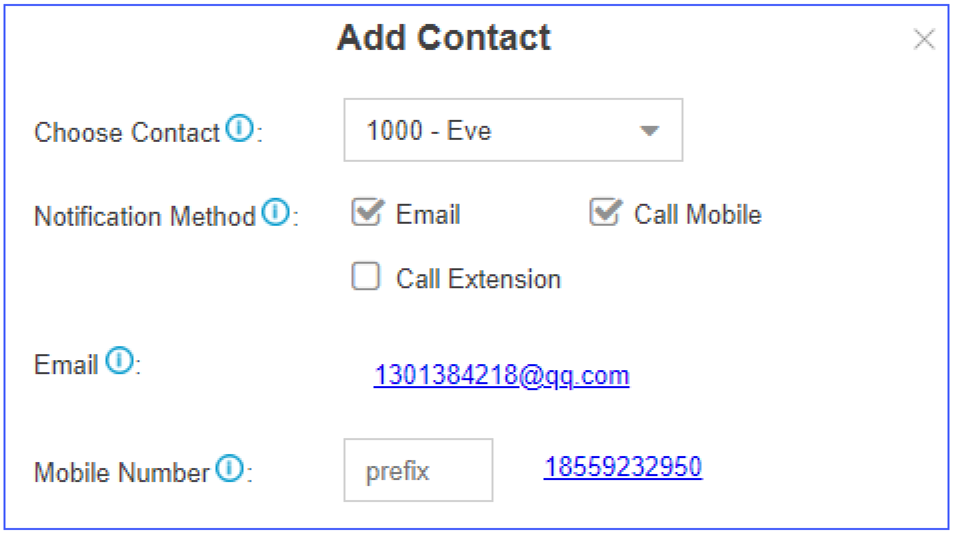
Go to Settings > Event Center > Event Log to search and check event logs.



Add Notification Contacts

You can set the PBX to send notifications when specific events or errors occur, notifying you via email, extension, or mobile devices.

1. Go to Settings > Event Center > Event Settings > Notification Contacts, click Add.
2. On the configuration page, choose a contact and set the notification method.



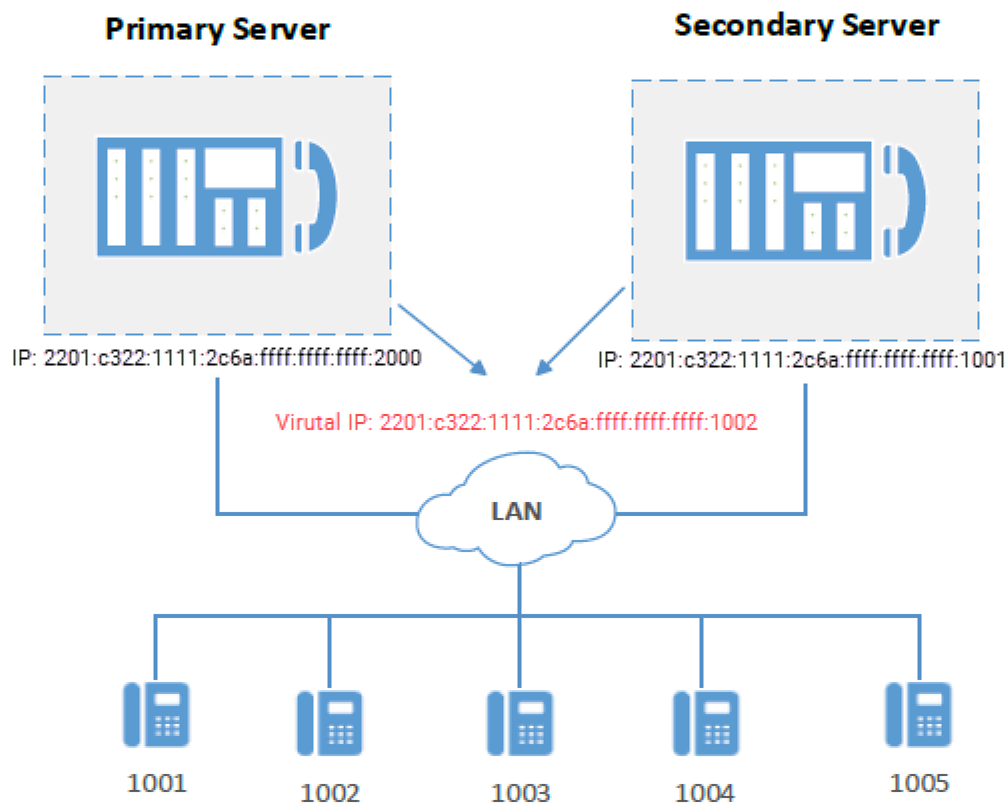
- Choose Contact: Choose an extension user or choose Custom to add an external contact.
- Notification Method: Select how to notify the contact when the event occurs.
    - Email: The PBX will send notifications to the email address of the contact.
    - Call Extension: The PBX will call the extension number of the contact when the event occurs.
    - Call Mobile: The PBX will call the mobile number of the contact when the event occurs.
- Email: If you choose Notification Mode to Email, you need to set the email address of the contact.
- Mobile Number: If you choose Notification Mode to Call Mobile, you need to set the mobile number of the contact and set the Prefix according to the outbound route pattern (on page 81) on the PBX.

3. Click Save and Apply.

Hot Standby

The Hot Standby solution provides high system availability to prevent you from the unnecessary business loss caused by unexpected server failure.

The solution consists of two PBXs with the same hardware and software, one works in the "active" state and the other works in the "standby" state. The configuration of primary server is synchronized to the secondary server in real time so that both systems contain identical information. When the primary server goes down, the secondary server can automatically and instantly take over.



Set up Hot Standby

This topic describes how to set hot standby on the primary server and secondary server.

Prerequisites

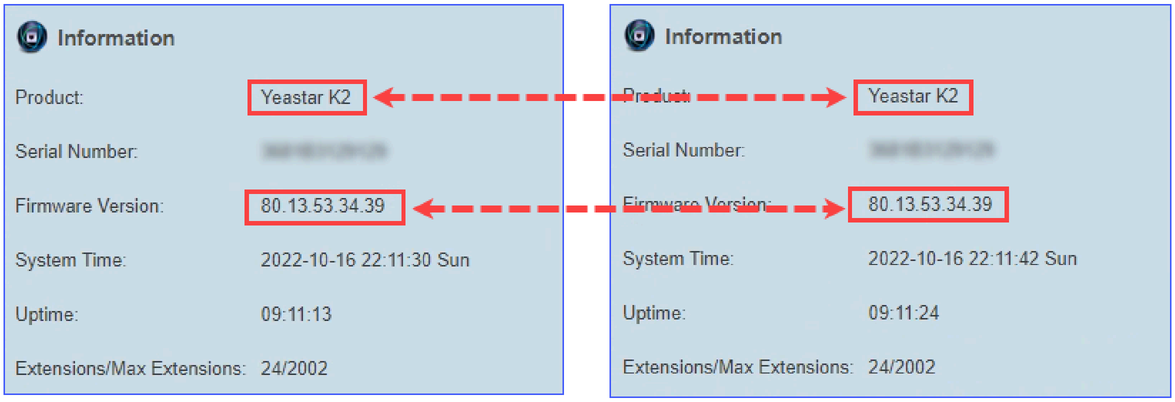
The primary server and secondary server in the failover pair must meet the following requirements:

- Same model
- Same firmware version

Step1. Check the basic information of the two PBXs

1. Log in to the PBX web interface, click Resource Monitor icon at the top-right corner to check PBX information.

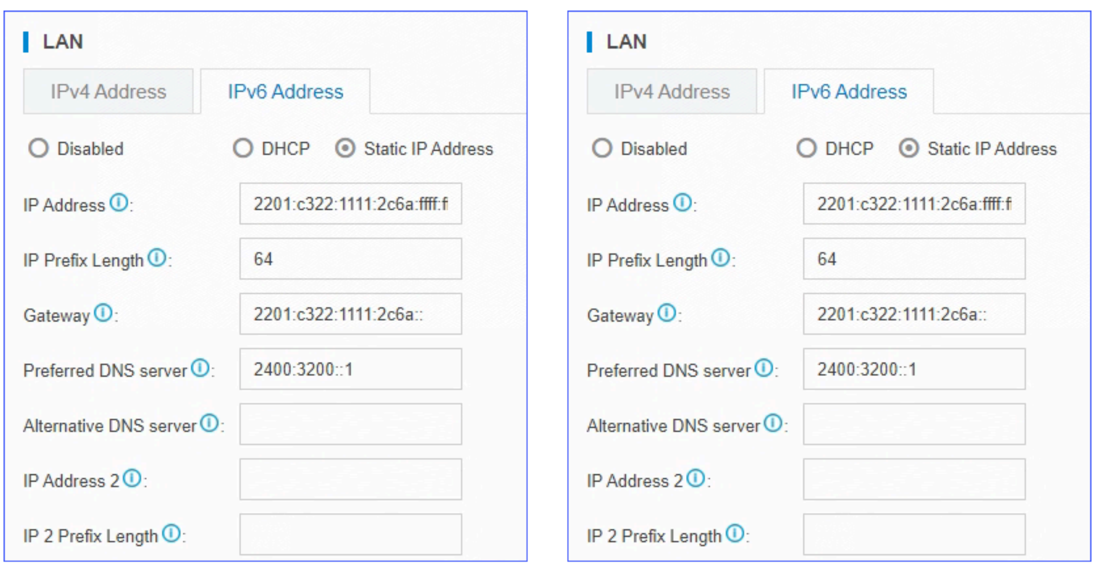
   Make sure the Product model and Firmware Version are the same.



2. Check the network information of the two PBXs.
    a. Go to Settings > System > Network > Basic Settings.
    b. Note down the network information of the two PBXs.

> Note:
> - Hot standby only works for LAN port. If the network Mode of the PBX is Dual, set the default interface to LAN port.
> - Hot standby doesn't work in VPN network.

In this example, the network information of the primary server and the secondary server is shown as below:



Primary **Secondary**

Step2. Set up hot standby for primary server and secondary server

Go to Settings > System > Hot Standby, set up hot standby for the two servers respectively.

Set up primary server

In the Hot Standby page, configure the network information of secondary server.

Set up secondary server

In the Hot Standby page, configure the network information of primary server.

Hot standby settings

Setting	Description
Enable Hot Standby	Check this option to enable hot standby.
Mode	Select a server mode.
Server Information	• Primary Server Hostname: Enter the hostname of the primary PBX. It's used in the event notification to help you identify the server. • Secondary Server Hostname: Enter the hostname of the secondary PBX. It's used in the event notification to help you identify the server.

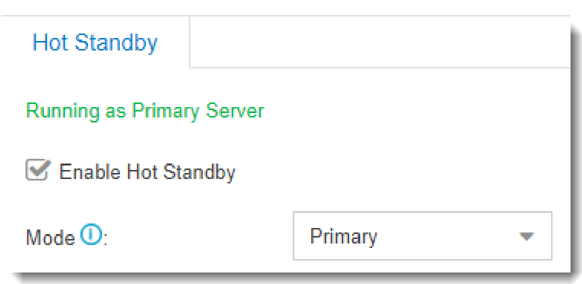
Setting	Description
	• Primary Server IP Address: Enter the IP address of the primary server. • Secondary Server IP Address: Enter the IP address of the secondary server. • Access Code: Enter an access code. Note: The two PBXs must have the same access code to authenticate connection.
Virtual IP Address	• Virtual IP Address: Virtual IP address is a shared IP for the two PBXs. The virtual IP always points to the on-site PBX. Note: ◦ Set the same virtual IP address on the primary server and secondary server. ◦ Use the virtual IP address as server IP address when registering extensions in the local network. • Subnet Mask / IPv6 Prefix: Enter subnet mask (for IPv4 network) or IPv6 prefix (for IPv6 network). • Virtual Gateway: Enter a gateway address for the virtual IP network. If left blank, the interactions between the PBX server and the virtual IP network would fail when they are under different network segments. • 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 and the secondary server of your PBX system have abnormal internet connection. In this case, the PBX failover would not work. Note: We recommend that you enter the gateway address.

Setting	Description
Advanced	Advanced settings only work when the server runs as a standby system. • Keep Alive(s): Define the frequency to send heartbeat keep-alive packets. The default value is 2 seconds, which means that the standby server sends packets 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 standby server. The default value is 120 seconds. If the standby server receives no response after timeout, it takes over automatically. Note: Set the Dead Time longer than the server rebooting time, or the standby server will take over when the primary server is rebooting.

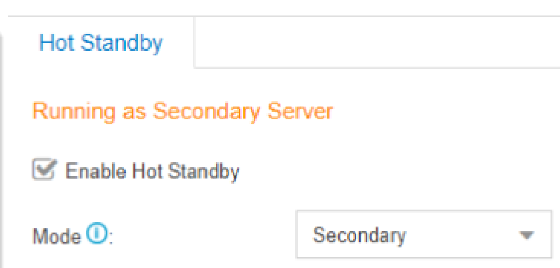
Step3. Test if hot standby works

1. Reboot the two servers to make hot standby take effect.
2. Log in to the PBX web interface, check the status of the primary server and secondary server.

> Note:
> The password setting is also synchronized, so you need to log in to the secondary server using the same login password as the primary server.



Primary



Secondary

3. Test if hot standby works.
    a. On primary server, create an extension, save and apply the changes.
    b. On secondary server, check if the hot standby configurations are correct.

        You can see the same extension is added automatically in the secondary server.

> Note:
> - The extensions and trunks created on the secondary server are invalid, because the secondary server is in the "standby" state.
> - If you want to upgrade the PBX firmware, you must DISABLE hot standby feature first.

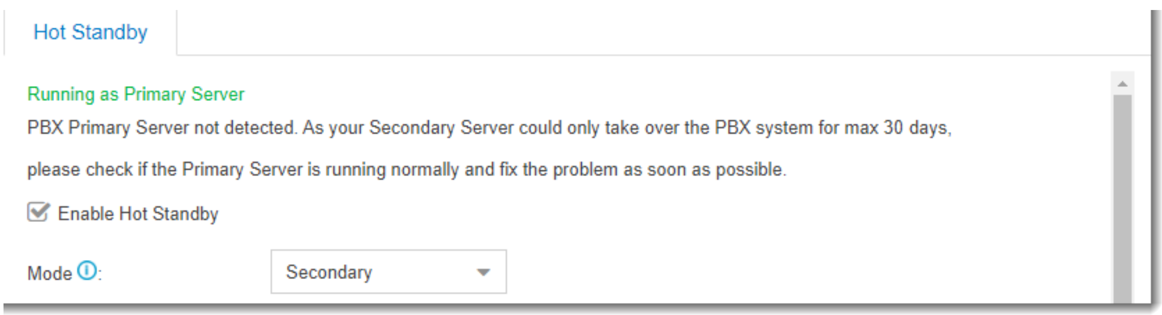
Primary Server Takes over the System from Secondary Server

The secondary server automatically and instantly takes over if the primary server goes down. As your secondary server could only take over the PBX system for max 30 days, you should repair the primary server as soon as possible. The primary server can take over after repairing. This topic describes how to take over the PBX system from the secondary server.

Prerequisites

- You have repaired the primary server.
- The secondary server has taken over the PBX system and runs as primary server.

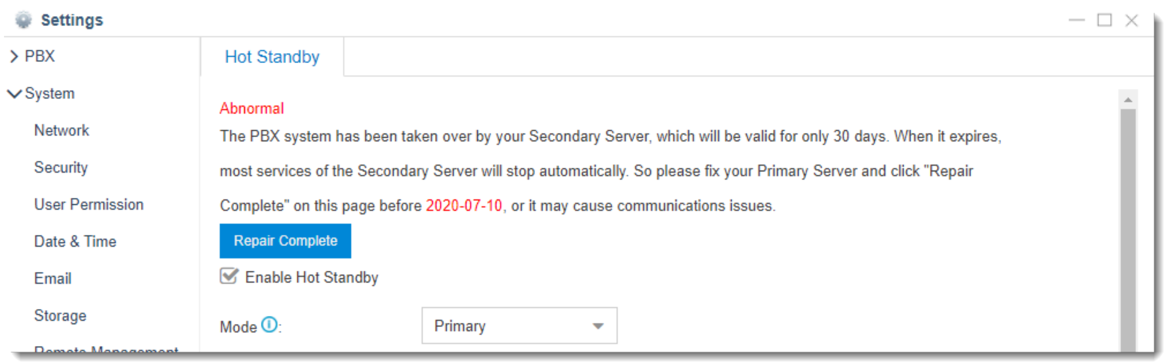
    The following figure shows the status of the secondary server.



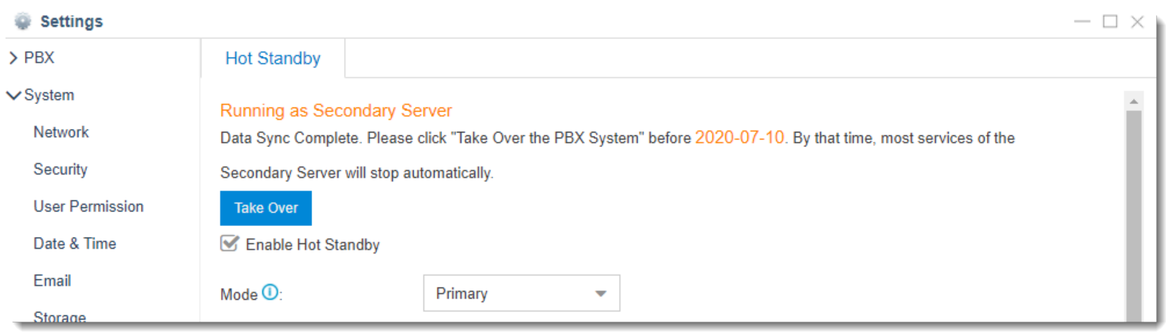
Procedure

1. Log in to the web interface of the primary server, go to Settings > System > Hot Standby.
2. Click Repair Complete.

    The primary server starts synchronizing data, and runs as the secondary server.



3. After data synchronization completes, click Take Over.



4. In the pop-up dialog box, select Yes.

   After the primary server takes over the PBX system, the secondary server reboots and runs as secondary server.

Set Event Notification of Hot Standby

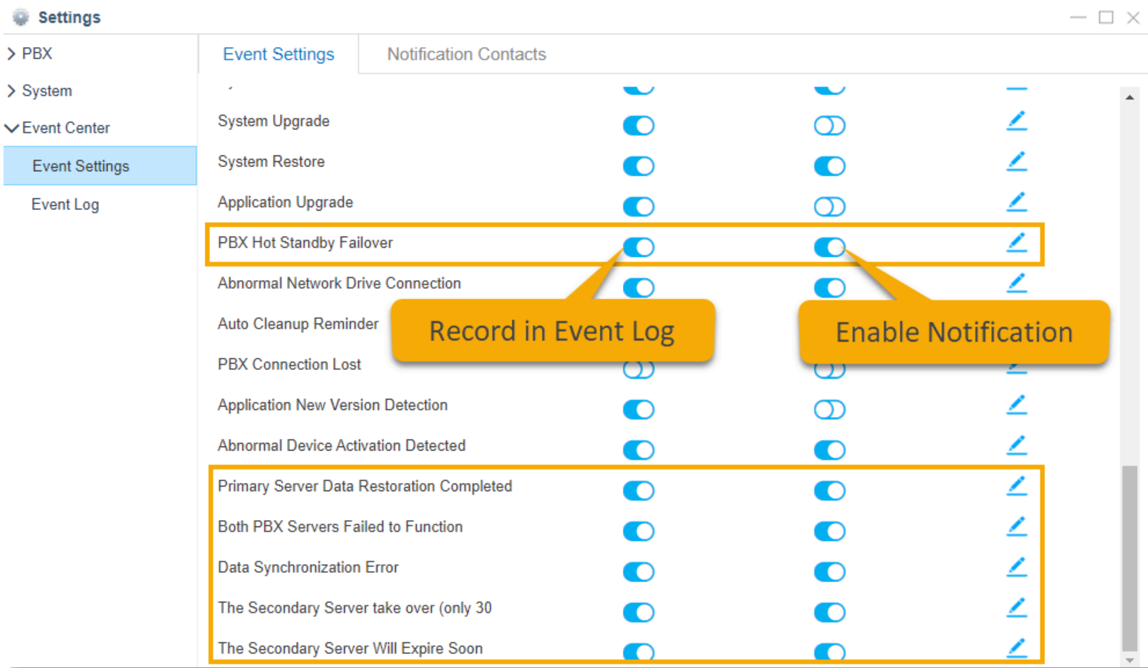
To keep informed of the hot standby status of the primary server and secondary server, you can enable the event notification. If the PBX server is abnormal, you can receive notifications by a phone call or email.

Notification events

- PBX Hot Standby Failover
- Both PBX Servers Failed to Function
- Data Synchronization Error
- Primary Server Data Restoration Completed
- The Secondary Server take over (only 30 days)
- The Secondary Server Will Expire Soon

Set event notification of hot standby

1. Log in to the PBX web interface, go to Settings > Event Center > Event Settings.
2. Enable notification for the events.



3. Click the Notification Contacts tab, add contacts to receive the notifications.
    a. Click Add, set the way to receive the notifications.

> Note:
> Make sure that the selected notification method has been configured.
>
> | Notification methods | Prerequisites |
> |---|---|
> | Email | Set up system email (on page 205) |
> | Call Mobile | • Set Mobile Number for the notified contact.
• Set the Prefix according to the outbound route pattern (on page 81) on the PBX. |

    b. Click Save and Apply.

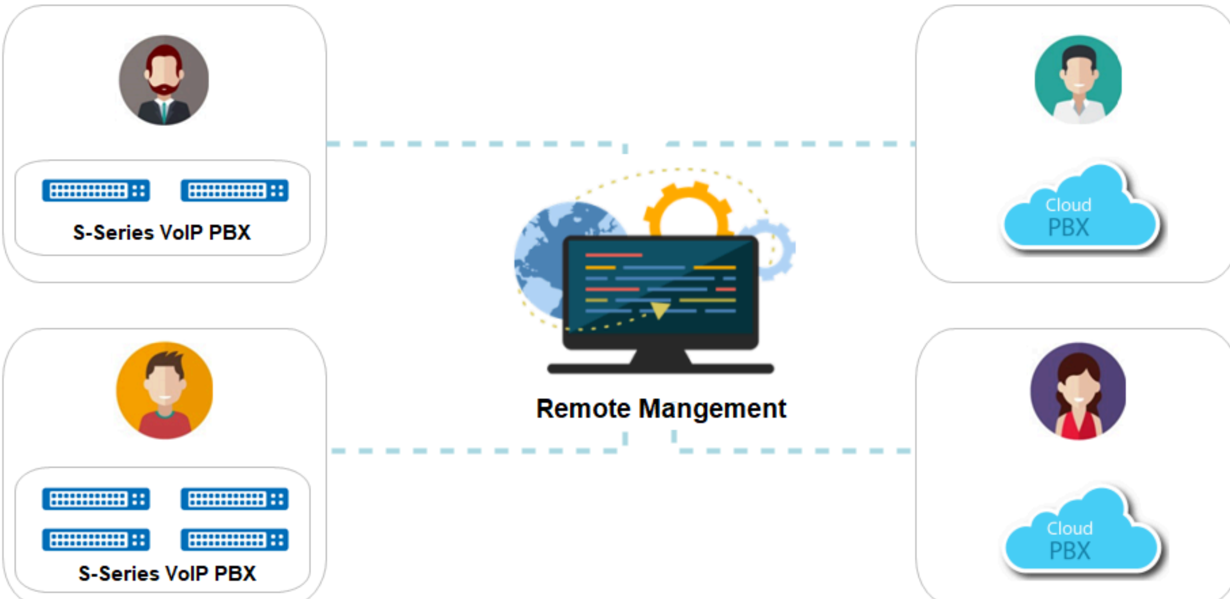
Remote Management

Remote Management

Yeastar Remote Management provides an affordable, low maintenance solution for easily deploying Yeastar VoIP PBX and VoIP gateways across multiple locations, reducing complexity and providing deep visibility and control.

Remote Management Guide

How to manage Yeastar products on the Remote Management platform, refer to the Remote Management Guide.



Maintenance

Maintenance gives you access to upgrade PBX firmware, check logs and troubleshooting.

Upgrade Firmware

Note:

- Back up the PBX configurations before you start updating the PBX firmware.
- If Reset Configuration to Factory Default is enabled, the system will reset to factory default settings after upgrading.
- When updating the firmware, please don't turn off the power, or the system will get damaged.

Related information

Create a Backup File (on page 221)

Browse a Local File to Upgrade

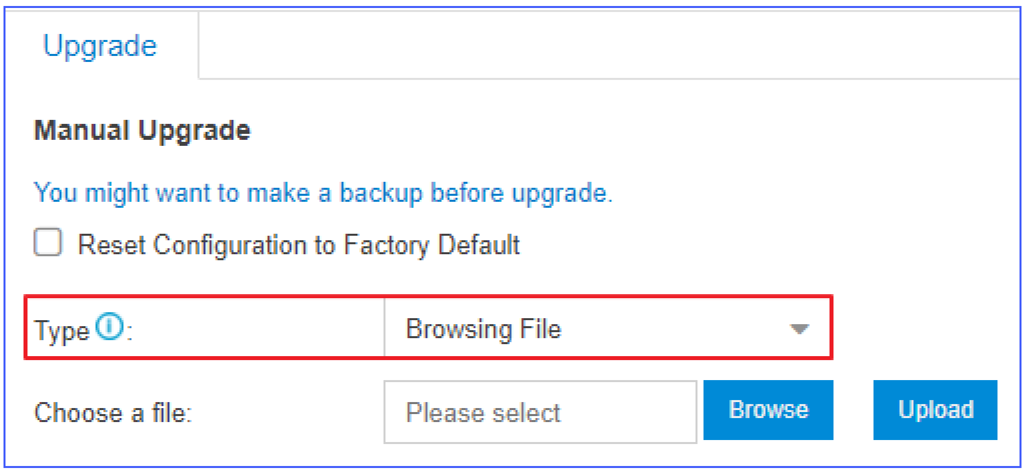
Upload the PBX firmware file from your local PC, then upgrade the PBX firmware.

This upgrade method is suitable when the PBX cannot access the Internet.

1. Go to Maintenance > Upgrade > Upgrade.
2. Optional: If you want to reset the configuration to factory defaults, select the check-box of Reset Configuration to Factory Default.

   > Important:
   > If you check this option, all your PBX configurations will be erased. We don't recommend you reset the PBX before upgrading firmware.

3. Set Type to Browsing File.

4. Click Browse to choose your local firmware file.

   > Note:
   > The firmware file format should be `.bin`, and the file name should not have special characters.

5. Click Upload.
   The PBX starts uploading the file and upgrading the firmware automatically.

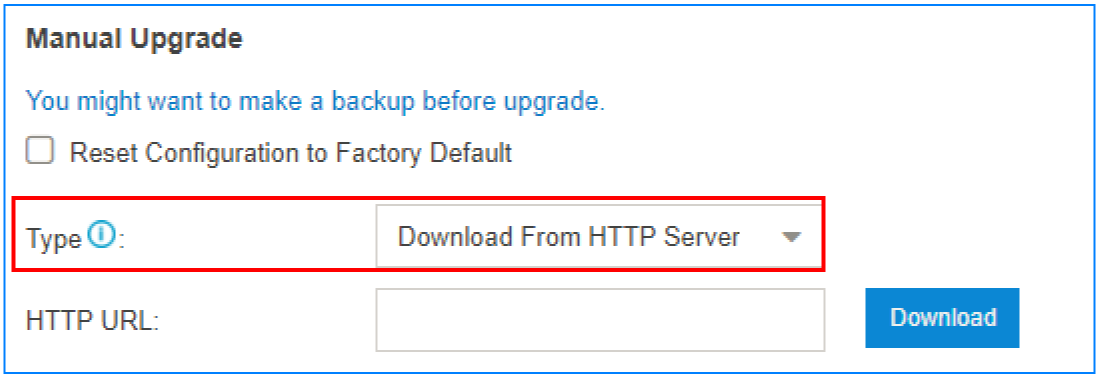
   > Note:
   > When the PBX is upgrading the firmware, do NOT turn off the power, or the system will get damaged.

Upgrade Firmware by HTTP Method

Make sure that the PBX could access the Internet, or the upgrade will fail.

1. Go to Maintenance > Upgrade > Upgrade.
2. If you want to reset the configuration to factory defaults, select the checkbox of Reset Configuration to Factory Default.

   Important:
   If you check this option, all your PBX configurations will be erased. We don't recommend you reset the PBX before upgrading firmware.
3. Set Type to Download From HTTP Server.

4. Enter the firmware download link in the HTTP URL field.

   Note:
   The URL should be a download link for a `.bin` file.
5. Click Download.
   The PBX starts downloading file from the HTTP server, and upgrading the firmware automatically.

   Note:
   When the PBX is upgrading the firmware, do NOT turn off the power, or the system will get damaged.

Backup and Restore

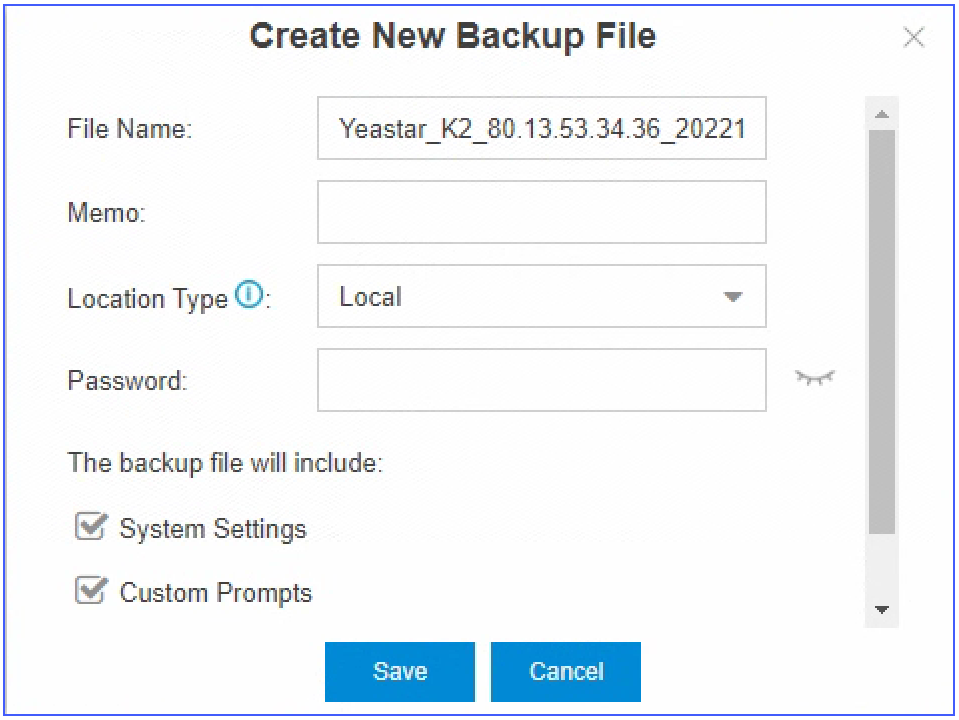
Go to Maintenance > Backup and Restore, then you can back up all configurations of PBX. Once backed up, back up file will be displayed in the list. You can upload backup file from local client to PBX, or you can choose from backup list and restore.

Create a Backup File

You can create a backup file of the PBX settings on the PBX web interface.

Note:
The backup file does NOT contain voicemail files.

1. Go to Maintenance > Backup and Restore, click Backup.



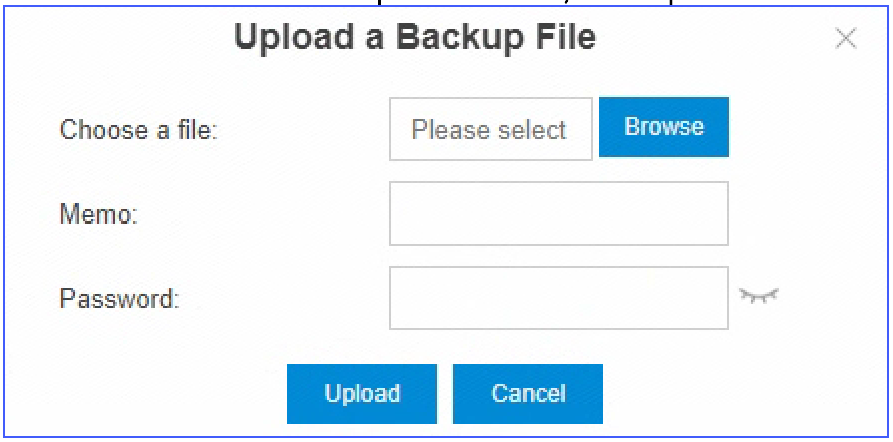
2. Set the File Name.
   The default file name contains the PBX model, firmware version, and backup date.
3. Optional: In the Memo field, enter notes for the backup file.
4. Select where to store the backup file.
5. Enter a password to encrypt the backup file. If set, anyone who wants to restore a PBX from the backup file must enter the password.
6. Select which configurations and files to back up.
7. Click Save.
   The created backup file appears on the Backup and Restore page.

Upload a Backup File

You can select a backup file from your local PC, and upload the file to the PBX.

Note:
The file format is `.bak` and the file name should not contain special characters.

1. Go to Maintenance > Backup and Restore, click Upload.



2. Click Browse, and select your backup file to upload.
3. In the Memo field, enter notes for the backup file.
4. In the Password field, enter the password of the backup file.
5. Click Upload.

   The uploaded backup file appears on the Backup and Restore page.

Restore a Backup File

After restoring a backup file, the current configurations on your PBX will be OVERWRITTEN with the backup data.

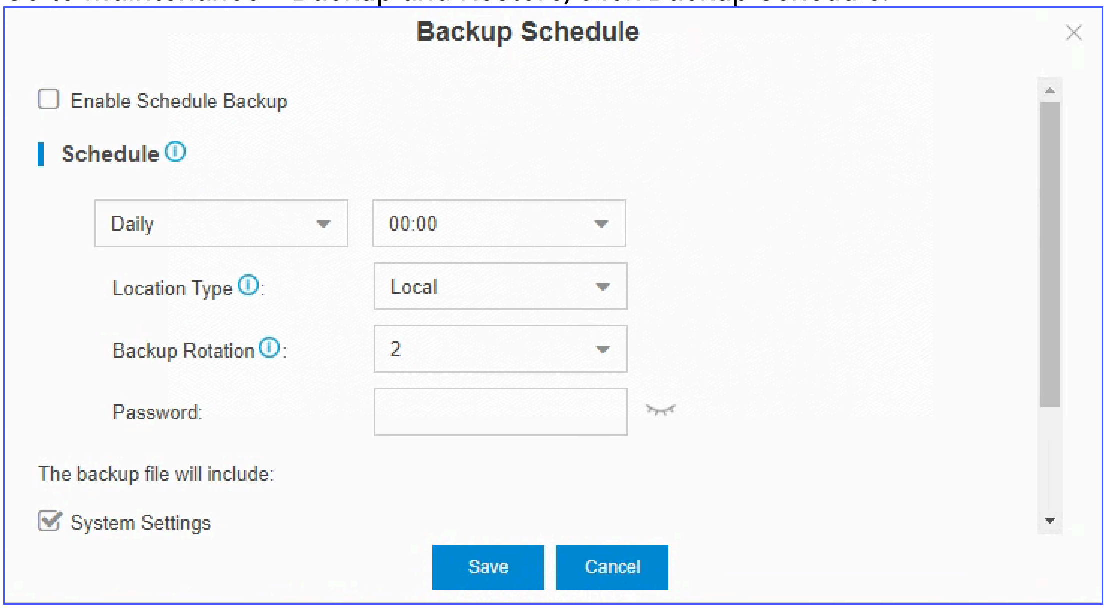
> Note:
>
> - You cannot restore a backup file that is downloaded from a different PBX model.
> - If a backup file is created from a newer version of PBX, you cannot restore this backup file. For example, restore a backup file (v30.14.53.34.76) to PBX (v30.14.53.34.65) would not work.
> - You can restore a backup file that is created from a older version of PBX. For example, restore a backup file (v30.14.53.34.65) to PBX (v30.14.53.34.76) would work.

1. Go to Maintenance > Backup and Restore.
2. Choose a backup file, click .
3. In the pop-up window, click Yes to reboot the PBX.

   The PBX starts to restore data from the backup file.

Schedule Auto Backup

1. Go to Maintenance > Backup and Restore, click Backup Schedule.



2. Select the checkbox of Enable Schedule Backup.
3. Set the backup Schedule settings.
    - Frequency and time: Select the backup frequency and when to make the back-up.
    - Location Type: Select where to store the backup file.
    - Backup Rotation: Set the maximum number of backup files that is stored in the selected location. When the number of backup files exceeds the set value, the oldest file will be replaced with the newest.
    - Password: Optional. Enter a password to encrypt the backup file.

      If set, anyone who wants to restore a PBX from the backup file must enter the password.
4. Set which configurations and files to back up.
5. Click Save.

Related information
Storage (on page 207)

Reboot the PBX

Reboot the PBX immediately on the PBX web interface or schedule auto reboot to keep the system running smoothly.

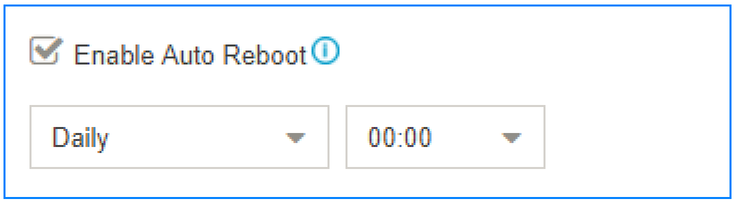
> **Note:**
> When the PBX is rebooting, all the on-going calls will be terminated.

Reboot the PBX Immediately

1. Go to Maintenance > Reboot, click Reboot.
2. In the pop-up window, click Yes.

Schedule Auto Reboot

1. Go to Maintenance > Reboot, check the option Enable Auto Reboot.

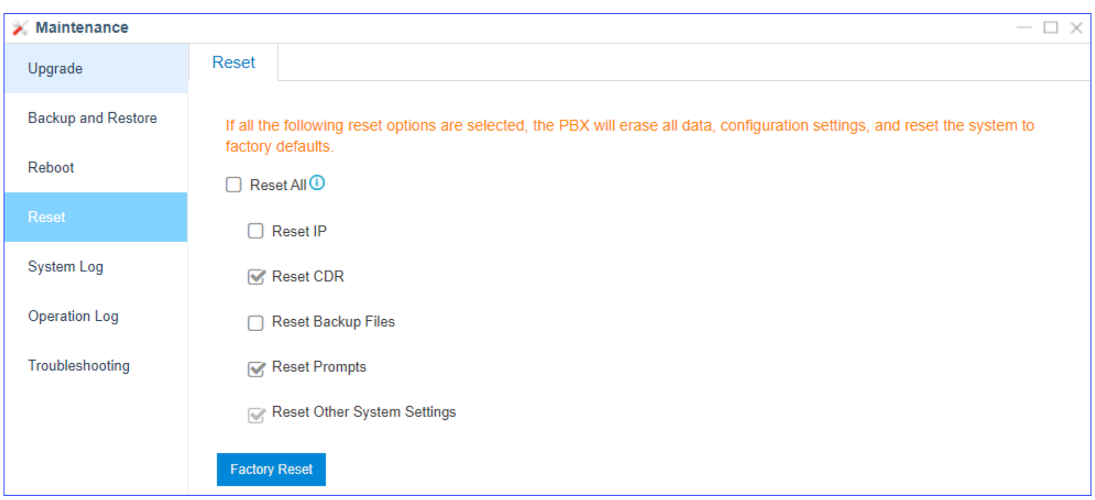


2. Set the frequency and time of auto reboot.
3. Click Save.

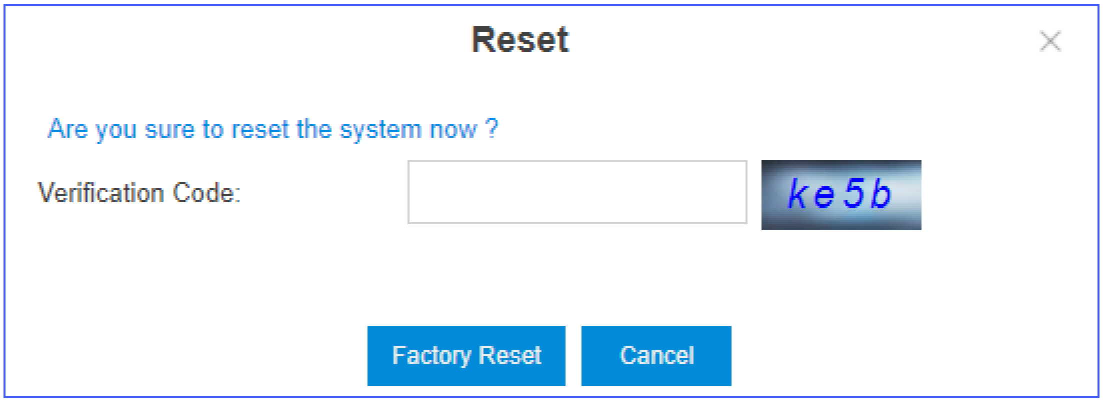
Reset the PBX

If you want to erase all the configurations on your PBX, you can reset the PBX to the factory defaults.

1. Go to Maintenance > Reset.
2. Select which data that you want to reset.
    - Reset All: Factory reset all the data and configurations on the PBX.
    - Reset IP: Reset the PBX's IP address to 192.168.5.150.
    - Reset CDR: Delete CDR that are stored in the Local flash of PBX.
    - Reset Backup Files: Delete the backup files that are stored in the Local flash of PBX.
    - Reset Prompts: Delete the custom prompts.
    - Reset Other System Settings: Reset all the configurations except IP address settings, and delete system logs, event logs, and operation logs.



3. Click Factory Reset



4. Enter the verification code.
5. Click Reset.

System Log

The PBX automatically traces the PBX information, notices, warnings, errors, debug logs, and web logs, then generates log files. You can download the system logs on the PBX web interface, and check the logs.

Go to Maintenance > System Log to trace real-time logs or download the generated system logs.

System Log Settings

The PBX traces different levels of log.

- Information: Basic information.
- Notice: NOTICE information.
- Warning: WARNING information.
- Error: ERROR information.
- DTMF: DTMF information.
- Time Log: Add time stamp of system logs.
- Debug: Select the following checkboxes to decide which type of debug logs to trace:
    - Enable SIP Debug
    - Enable RTP Debug

System Log

The PBX generates system logs everyday. The system logs are compressed into a tar file. You can check the system logs on the System Log page.

Click Download to download the log file and open the log file by `Notepad++` or other editor software to check the logs.

The PBX provides the following kinds of system logs:

- PBX firmware version
- Asterisk guard logs
- Module update logs
- SSH connection logs
- PnP logs
- Web logs

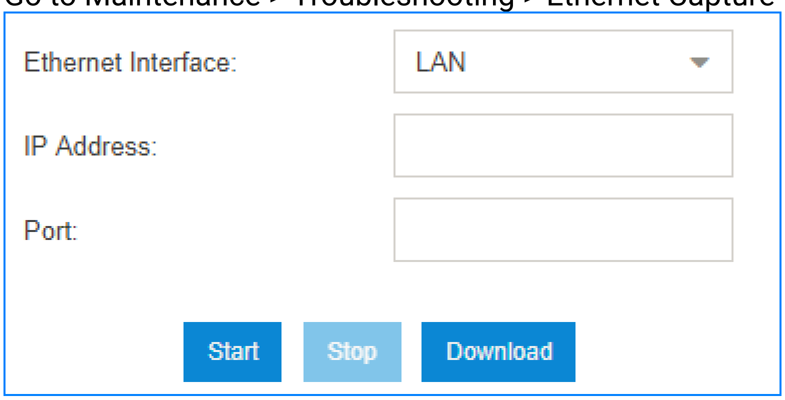
Troubleshooting

Yeastar S1000-P IPPBX Ethernet Capture Tool, IP Ping and Traceroute can be used to debug and capture packets.

Capture Ethernet Packets

When there is a problem on the VoIP extensions or trunks, you can use the Ethernet Capture Tool to capture Ethernet packet, and download the packet to analyze it.

1. Go to Maintenance > Troubleshooting > Ethernet Capture Tool.



2. Choose the Ethernet Interface where the packet will go through.
3. Optional: In the IP Address field, enter the target 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 the target port.

> Note:
> If you don't set a port, the PBX will capture packets for all the ports.

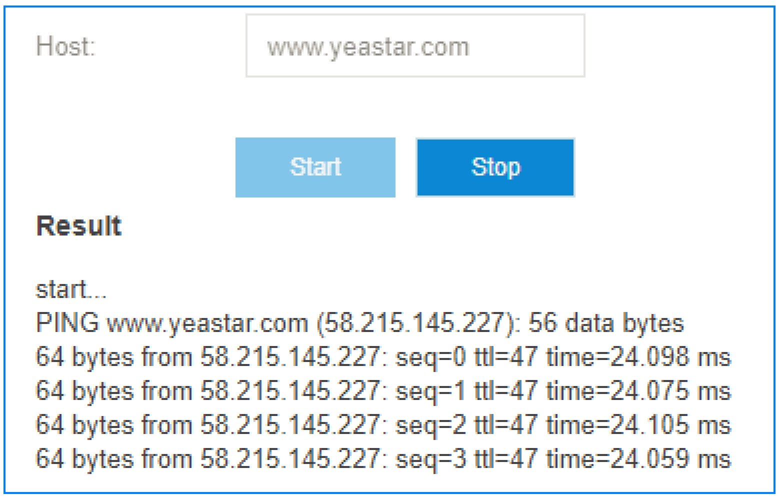
5. Click Start.
   The PBX starts to capture the Ethernet packet. During this time, you should duplicate the problem of your VoIP trunks or extensions.
6. Click Stop to stop capturing packets.

7. Click Download to download the captured packet.
8. Decompress the `.tar`file and use `Wireshark` software to open the packet file.

Ping IP Address

A ping utility sends test messages from the local client to a remote target over the TCP/IP network connection. You can use IP Ping tool to test if the PBX can access the target IP address.

1. Go to Maintenance > Troubleshooting > IP Ping.
2. In the Host field, enter the target domain name or IP address.
3. Click Start and check the result.

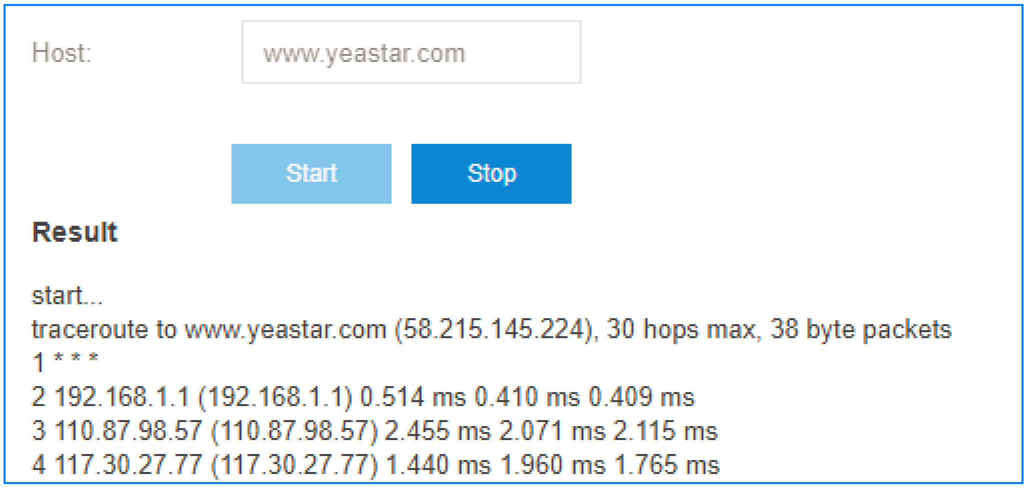


4. Click Stop to stop ping.

Traceroute

Traceroute is a common diagnostic tool for displaying the route (path) and measuring transit delays of packets across a network.

1. Go to Maintenance > Troubleshooting > Traceroute.
2. In the Host field, enter the target domain name or IP address.
3. Click Start and check the result.

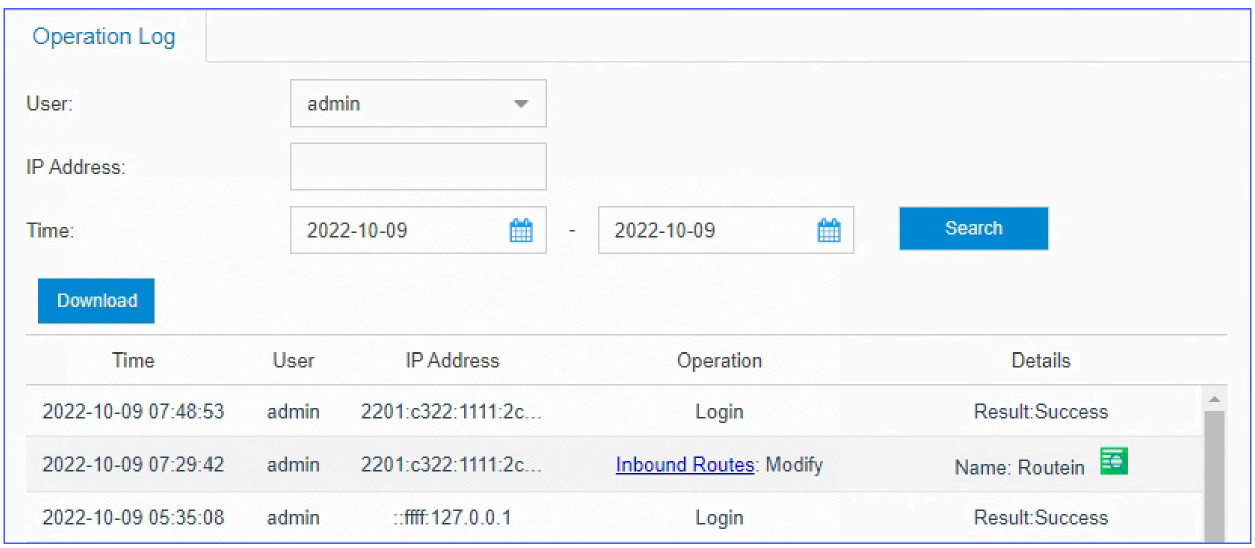


4. Click Stop to stop traceroute.

Operation Log

The PBX records all the users' operations, and keeps the logs in Operation Log.

Go to Maintenance > Operation Log to search and check the operation logs.



PBX Monitor

The PBX monitors the status of Trunks, Extensions, Concurrent Call, Conference.

You can log in to the PBX web interface, go to PBX Monitor to check the real-time status of your trunks, extensions, and conferences.

Extension Status

Table 9.

Status	Description
	The extension is idle.
	The extension is ringing.
	The extension is unavailable.
	The extension is busy.
	The extension is held.

VoIP Trunk Status

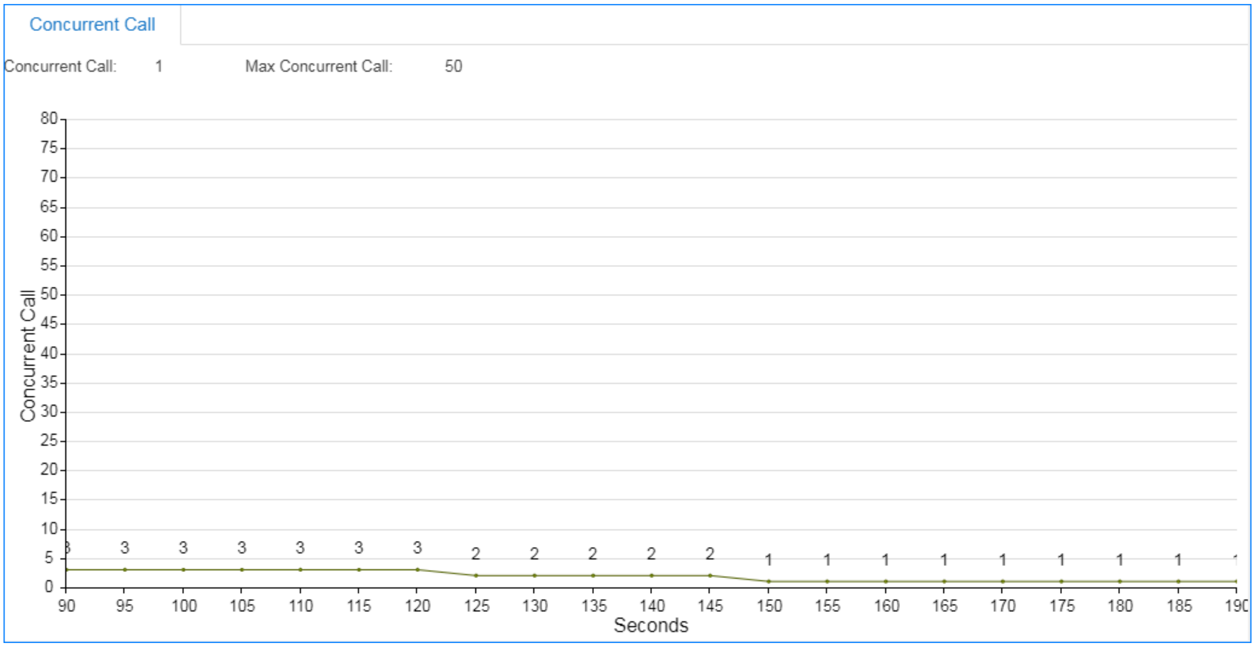
Table 10.

Status	Description
	Registered
	Registering

	• Unreachable
	• Registration failed, caused by:
	  ◦ wrong password
	  ◦ wrong authentication name
	  ◦ wrong user name
	  ◦ transport type inconsistent

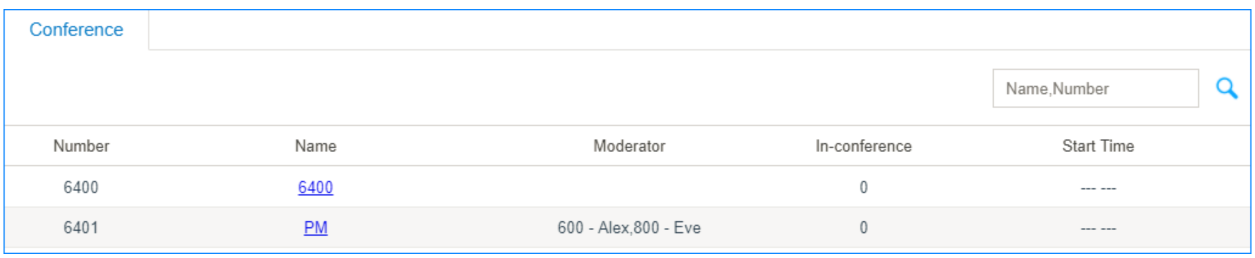
Concurrent Call

Check the maximum supported concurrent calls and the real-time concurrent calls on the PBX.



Monitor Conference

Check how many conferences are created on the PBX, and monitor the status of the conferences.



Conference

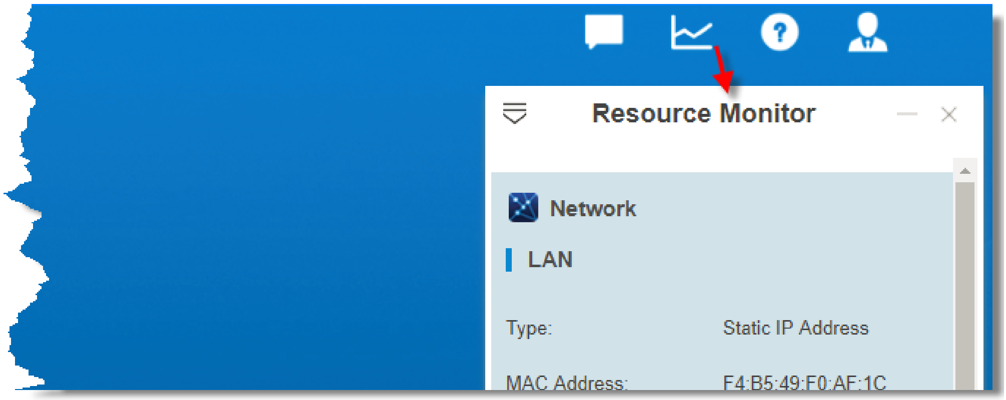
Name,Number

Number	Name	Moderator	In-conference	Start Time
6400	6400		0	--- ---
6401	PM	600 - Alex,800 - Eve	0	--- ---

Resource Monitor

Monitor the CPU usage, memory usage, disk utilization, and network flow.

You can go to Resource Monitor or click the shortcut icon at the right-top corner to check the information.



Performance

Check the performance of CPU, Memory, and local network.

Network

Check the status of local network and VPN network.

Information

Check the basic information of the PBX.

- Product
- Serial Number
- Firmware Version
- System Time: The current time on the PBX.
- Uptime: The system up time since the last reboot.
- Extensions/Max Extensions: The number of added extensions/The maximum number of extensions allowed to be added.

Storage Usage

Check the usage of local storage in the PBX.

CDR

Call Detail Record (CDR) is a data record that contains various attributes of the call, such as time, duration, call status, source number, and destination number, etc. You can check CDR on the PBX web interface.

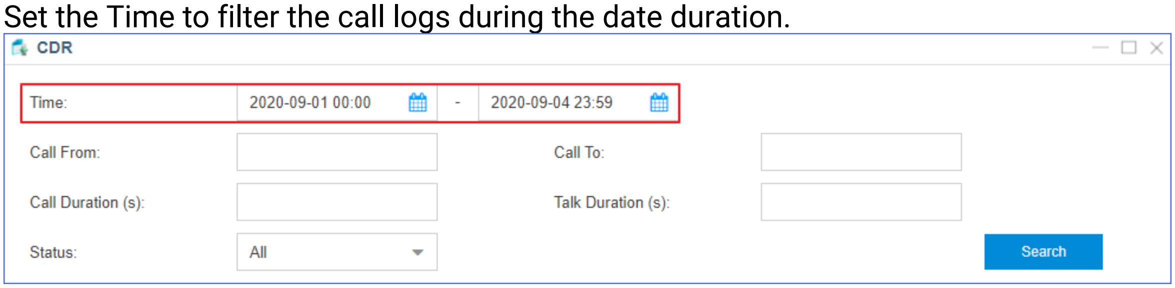
Searching Criteria

You can search CDR by the following criteria:

- Time: Set the start date and the end date to filter the call logs that are in the date duration.
- 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. Enter a value to filter the call logs that have call duration equal or greater than this value.
- Talk Duration: The time between the call answered and the call ended. Enter a value to filter the call logs that have talk duration equal or greater than this value.
- Status: Call status, including Answered, No Answer, Busy, Failed and Voicemail.
- Communication Type: Communication type, including Inbound, Outbound, Internal, Multisite Interconnect, Callback, Transfer, and Warning.
- Source Trunk: The call was received from which trunk.
- Destination Trunk: The call was sent out via which trunk.
- PIN Code: The PIN code to access voicemails.
- DID: The phone number that the caller dialed.
- DOD: The phone number that is displayed on the callee's device.
- Caller IP Address: The address of the caller's device.
- Emergency Call: Whether the call is an emergency call or not.

Search CDR

1. Log in to the PBX web interface, go to CDR.
2. Set the Time to filter the call logs during the date duration.

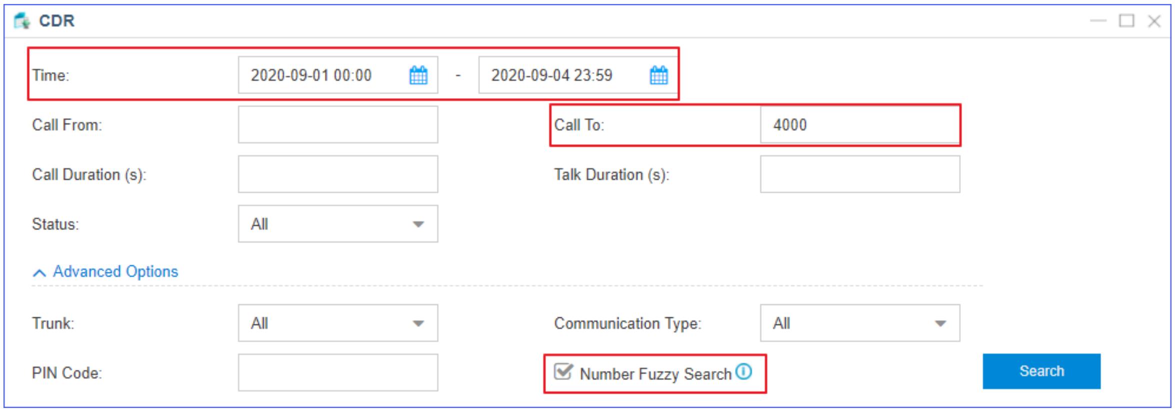


3. Set other searching criteria.
4. Click Search.
   The filtered call logs will display.

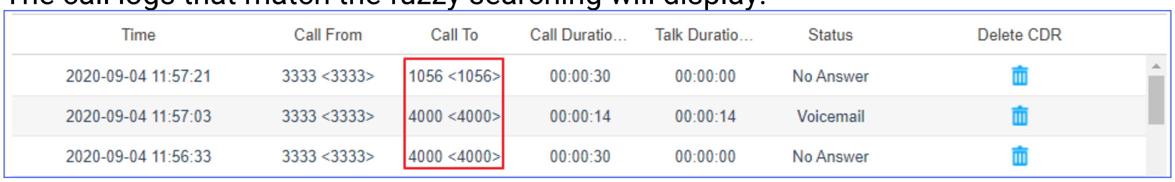
Fuzzy Search CDR

By default, you need to enter an exact and complete phone number in the relevant searching criteria, or you cannot get the search result. If you cannot remember the exact number or the name, you can use Fuzzy Search feature.

1. Go to CDR.
2. Set the Time to filter the call logs during the date duration.
3. Enter a desired number or letters in Call From field or Call To field.
4. Click Advanced Options, select the checkbox of Number Fuzzy Search.



5. Optional: Set other searching criteria.
6. Click Search.
   The call logs that match the fuzzy searching will display.



Download CDR

You can download the searched CDR to your local PC.

1. Go to CDR.
2. Search the CDR (on page 233).
3. Click Download CDR.

Conference Panel

Conference Panel App allows you to establish a multiparty call, monitor and manage the conference call on web pages.

Features

- Instant conference
- Dial-in conference
- Check conference status
- Add/Delete conference members
- Change status of conference members
- Phonebook

Manage Conference Contacts

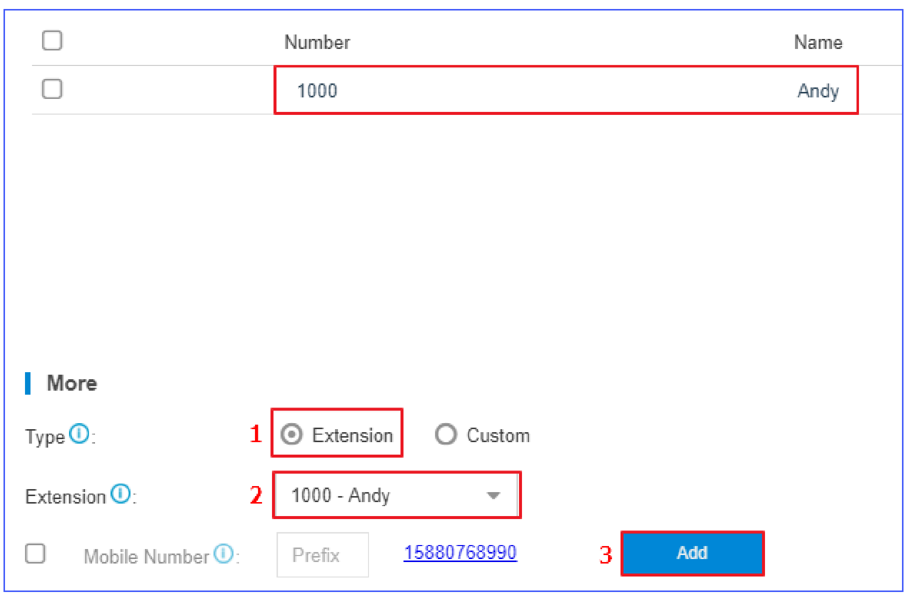
Phonebook allows you to quickly select contacts before initiating a conference call. You can add a phonebook on Conference Panel or save members' information as a new phonebook after a conference is concluded.

Add a phonebook

1. Log in to Conference Panel.
2. Click Conference Contacts tab, and click Add to create a phonebook and add contacts.
3. In the Group Name field, enter a name to help you identify it.

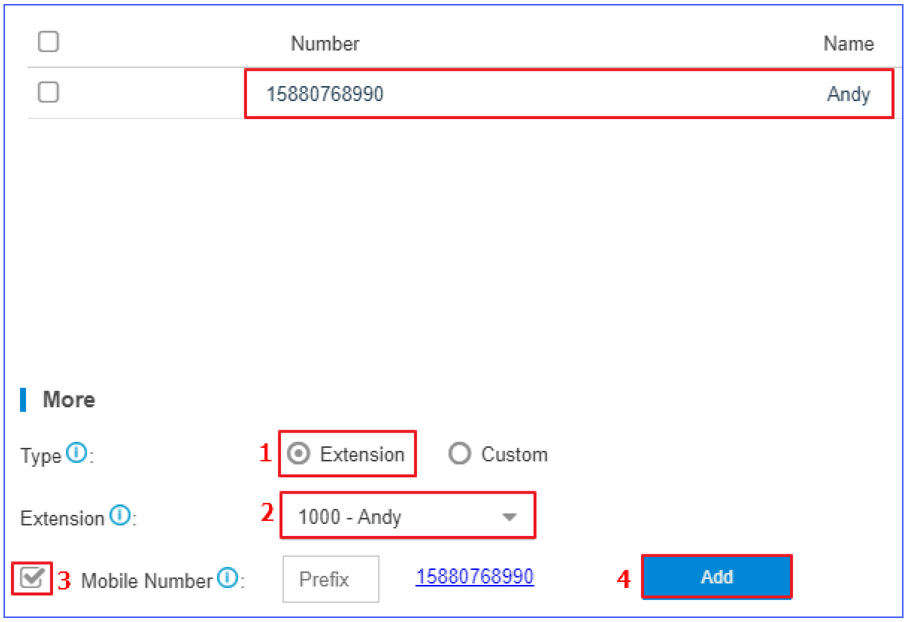
> **Note:**
> Special characters like `&""\<>'|$` are not allowed.

4. On More section, select the type of phone number and add a contact, then click Add.
    - Extension: Select an internal contact on PBX. For the internal contact, you can select either an extension number or an associated phone number.
        - Extension: The extension number will be saved on the phonebook.



- Mobile Number: Select the checkbox of Mobile Number. The mobile number will be saved on the phonebook while extension number will not be displayed.

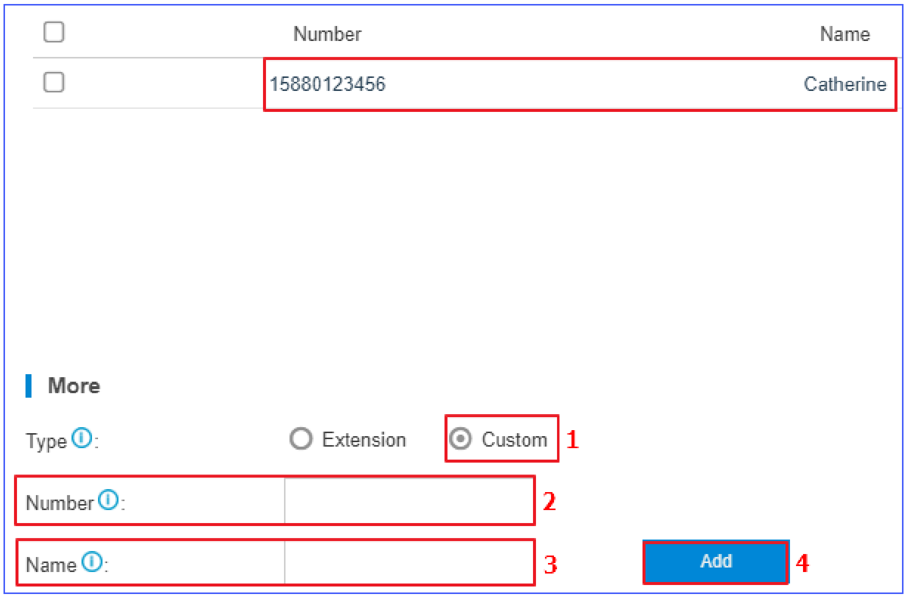
> **Note:**
> If a prefix is specified for the outbound route that is available to the extension, you should set the corresponding prefix for mobile number.



- Custom: Add an external contact to phonebook by mobile number.

  Select Custom, enter Number and Name, and click Add.

> Note:
> If a prefix is specified for the outbound route that is used to dial external numbers out, you should set the corresponding prefix for the phone number.



5. Click Save to save the phonebook.

Save a phonebook

If you invite a contact who is not available on the phonebook to the conference, you can save the contact as a new phonebook. You can quickly select the contact from phonebook next time you want to initiate another conference.

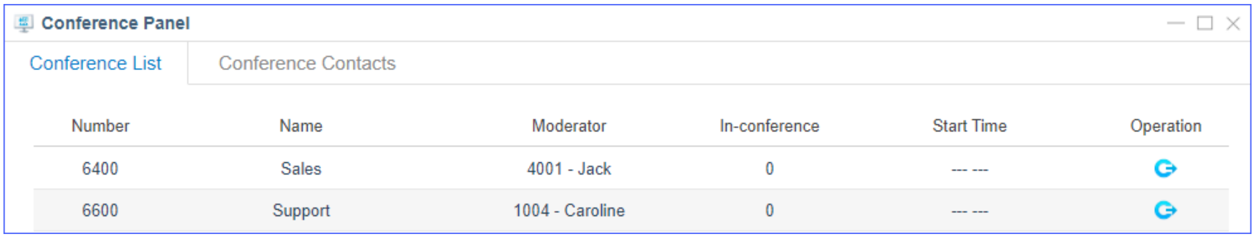
1. Log in to Conference Panel.
2. Select a conference, and click to enter the specific conference page, which displays all members in the conference.
3. Click Save Contacts, system saves all members in the conference as the phonebook by default.
   You can delete members who are not required to join the follow-up conference.
   - Delete one by one: Click beside the contact who you want to delete.
   - Bulk delete: Select the contacts who you want to delete, and click Delete.
4. In the Group Name field, enter a name to help you identify it.

> Note:
> Special characters like &""\<>'|$ are not allowed.

5. Click Save.

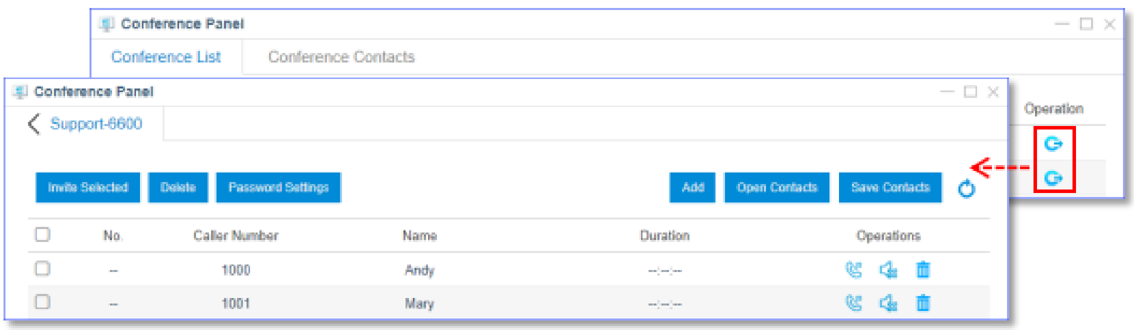
Conference List

Click Conference List tab, you can view the created conference, in-conference members, and start time of each conference. You can also go to the specific conference page to monitor and manage conference.



Go to the specific conference page

1. Log in to PBX web interface, and go to Conference Panel.
2. Click Conference List tab.
3. Select a conference, and click  to go to the specific conference page.



Dial-in Conferencing

You can set up a meeting in advance. Members can dial the conference number at the scheduled time to join the conference.

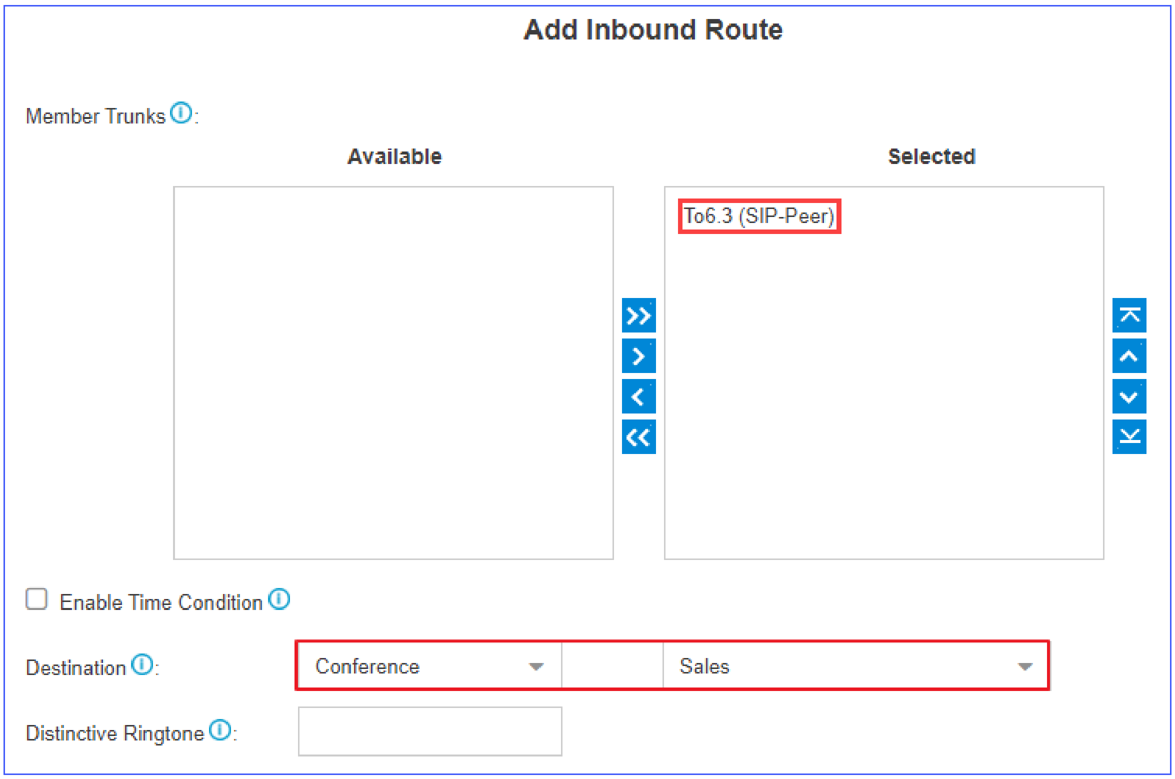
An internal user joins the conference

An internal user can directly dial the conference number to join the conference. For example, an extension user can dial 6400 to join conference 6400. If a participant password is required, extension users should enter the password. Only when password is authenticated can extension users join the conference.

An external user joins the conference

To allow external users to join the conference, you should set the destination of an inbound route to conference, and inform external users of the phone number for the trunk that is used in the inbound route. External users will be routed to the conference after dialing the trunk number.

1. Log in to the PBX web interface, go to Settings > PBX > Call Control > Inbound Routes, add an inbound route.
2. In the Name field, enter the inbound route name.
3. Select the desired trunk from Available box to Selected box.
4. In the Destination drop-down list, select Conference and select a specific conference.



5. Click Save and Apply.

   External users can dial phone number of the selected trunk to join the conference.

Dial-out Conferencing

You can place a conference call on Conference Panel to invite contacts to join the conference.

Log in to the PBX web interface and go to Conference Panel to add phone number of the contact who you want to invite. Select the contact and click Invite Selected to place the conference call. The contact joins the conference when he/she answers the call.

1. Log in to the PBX web interface, go to Conference Panel.
2. Click Conference List tab.
3. Select a conference, and click  to enter the specific conference page.
4. Click Open Contacts, and select contacts who you want to invite from phonebook.

- Select the checkbox of a phonebook, then all contacts will be selected.
- Click to unfold the phonebook, and select the desired contacts.

5. Click OK to add contacts to the current conference.
6. Optional: Click Add to add contacts who are not available on the phonebook.
7. Invite contacts to join the conference.

   Password Settings: Click Password Settings, you can change participant password. By default, the field is null, which means that users are not required to enter password when they join the conference.

   - To invite all members, select all members and click Invite Selected.

   - To invite a member, click beside the contact who you want to invite.

   Phones of the selected members will ring, and the conference number is displayed as caller ID. When the call is answered, members will be prompted that they are invited to the conference call.

Control Online Conferences

During a conference call, the administrator can manage the conference either on Conference Panel App or on phones.

Control conferences on web pages

: Click the icon to mute the member.

: Click the icon to unmute the member.

: Click the icon to kick the member out of the conference.

: Click the icon to remove the member from the conference list.

Control conferences on phones

During a conference call, members can press `*` to enter conference voice menu, and operate according to the voice prompt.

Administrator - Voice Menu	
1	Mute or unmute a member.
2	Lock or unlock a conference.
3	Kick out the last member to join the conference call.
4	Turn down the conference volume.
6	Turn up the conference volume.
7	Turn down your own volume.
8	Exit from voice menu.
9	Turn up your own volume.
Other Conference Members - Voice Menu	
1	Mute or Unmute.
4	Turn down conference volume.
6	Turn up conference volume.
7	Turn down your own volume.
8	Exit from voice menu.
9	Turn up your own volume.

Appendix

We provide detailed information about the user name and password, the personal data, and the communication matrix that are used or collected when you use Yeastar S1000-P IPPBX, as well as how to harden security of Yeastar S1000-P IPPBX.

For more information, see the followings:

- Appendix 1: User Name & Password, Personal Data, Communication Matrix
- Appendix 2: Security Hardening Policy

S1000-P Security Hardening Policy

Change History

Date	Version	Description
2021.10.25	Rev1.0	First version.
2022.12.12	Rev1.1	1. In Chapter 2.2, added 'Fix Host Vulnerability'. 2. In Chapter 2.4, added IPv6 screenshot. 3. In Chapter 2.11, added restrictions for account login. 4. In Chapter 2.12, added restrictions for mounting options. 5. In Chapter 3.6, added IPv6 screenshot. 6. In Chapter 3.3, updated boa patch. 7. In Chapter 4.1, updated the description of upgrading Mysql database to 5.7.40. 8. In Chapter 5.1, updated Applibs upgrade; In Chapter 5.3, updated patch list; In Chapter 5.2, added source code compilation options.

Content

1 Before You Begin

Check the colors below, which would help you identify the changes made in this document.

Blue - Add

Red - Update

Gray - Delete

2 Ubuntu Security

2.1 Upgrade Ubuntu from 14.04 to 18.04

```
root@IPPBX:~# uname -a
Linux IPPBX 4.15.0-161-generic #169-Ubuntu SMP Fri Oct 15 13:41:54 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
root@IPPBX:~# cat /etc/os-release
NAME="Ubuntu"
VERSION="18.04.4 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.4 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
```

2.2 Fix Host Vulnerability

- **Upgrade and uninstall APP when creating ISO file**

  apt install --only-upgrade linux-image-generic

  apt install --only-upgrade grub-efi-amd64

  apt install --only-upgrade vim vim-common vim-runtime

  apt install --only-upgrade squashfs-tools

  apt install --only-upgrade unzip

  apt install --only-upgrade tar

  apt install --only-upgrade libsqlite3-0

  apt install --only-upgrade libp11-kit0

  apt install --only-upgrade gnupg

  apt install git

  apt install --only-upgrade busybox-initramfs busybox-static

  apt install --only-upgrade apport python3-apport

  apt install accountsservice libaccountsservice0

  apt install --only-upgrade apt

  apt install --only-upgrade ca-certificates

  apt install --only-upgrade dbus libdbus-1-3

  apt install --only-upgrade libssl1.1

  apt install python3-apt

  apt install python3-software-properties software-properties-common

  apt install python3-urllib3

  apt install --only-upgrade liblz4-1

  apt install --only-upgrade python-apport

  apt install --only-upgrade libnettle6

  apt install --only-upgrade libx11-6

  apt install --only-upgrade isc-dhcp-client

  apt install --only-upgrade libglib2.0-0

apt install --only-upgrade dnsmasq-base dnsmasq-utils
apt install intel-microcode
apt install --only-upgrade libxml2
apt install libxml2-utils
apt-get purge curl libcurl3-gnutls libcurl4 （Use openssl-1.1.11 in applibs）
apt-get purge isc-dhcp-server
apt install --only-upgrade vim vim-common vim-runtime
apt install --only-upgrade busybox-initramfs busybox-static
apt install --only-upgrade libssl1.1 libssl1.0.0
apt install --only-upgrade libexpat1
apt install --only-upgrade rsync zlib1g
apt install --only-upgrade login passwd
apt install uidmap
apt install ruby2.5
apt install --only-upgrade klibc-utils libklibc
apt install --only-upgrade dpkg libdpkg-perl
apt install --only-upgrade libc6
apt install --only-upgrade cron
apt install --only-upgrade bash
apt install --only-upgrade dbus libdbus-1-3
apt install --only-upgrade libxslt1.1
apt install --only-upgrade binutils binutils-multiarch
apt install --only-upgrade libpython3.6-stdlib libpython3.7-stdlib libpython3.8-stdlib
apt install --only-upgrade policykit-1
apt install --only-upgrade snapd snap-confine
apt install --only-upgrade e2fsck-static e2fslibs e2fsprogs fuse2fs
apt install --only-upgrade rsyslog
apt install --only-upgrade ntfs-3g
apt install --only-upgrade heimdal-kcm heimdal-kdc heimdal-servers libgssapi3-heimdal libkdc2-heimdal libkrb5-26-heimdal samba
apt install --only-upgrade libpcre3
apt install --only-upgrade libgmp-dev libgmp10 libgmpxx4ldbl libgmpxx4ldbl
apt install --only-upgrade ntfs-3g ntfs-3g-dev
apt install --only-upgrade python-twisted python-twisted-bin python-twisted-bin python3-twisted python3-twisted-bin
apt install --only-upgrade libxml2 libxml2-utils
apt install --only-upgrade icu-devtools libicu60 libiculx60
apt install --only-upgrade tar
apt install --only-upgrade libglib2.0-0 libglib2.0-bin libglib2.0-data libglib2.0-dev (time-consuming)
apt install --only-upgrade apport python3-apport
apt install --only-upgrade libgnutls30
apt install --only-upgrade unzip
apt install --only-upgrade apport dnsmasq dnsmasq-base dnsmasq-utils
apt install --only-upgrade gzip xz-utils
apt install --only-upgrade intel-microcode
apt install --only-upgrade systemd
apt install --only-upgrade libfribidi-bin libfribidi-dev libfribidi0

apt install --only-upgrade isc-dhcp-client isc-dhcp-server

apt install --only-upgrade networkd-dispatcher

apt install --only-upgrade ca-certificates

apt install --only-upgrade linux-image-generic linux-image-4.15.0-157-generic

apt install lib32z1 libx32z1

apt install libxslt1.1

apt install sosreport

apt install open-vm-tools

apt install --only-upgrade gnupg

apt install --only-upgrade libruby2.5

apt install rsync

apt remove libcrack2

- **Run /home/install/etc/rc.local.app, then proceed as follows:**

```
if [ ! -f "/sbin/ifenslave" ];then
        if [ -f "/ysdisk/ubuntu18" ];then
                dpkg -i --force-overwrite /home/install/ifenslave_2.4ubuntu1.2_all.deb << EOF
Y
EOF
                dpkg -i --force-overwrite /home/install/ifenslave-2.6_2.4ubuntu1.2_all.deb << EOF
Y
EOF
        else
                dpkg -i --force-overwrite /home/install/ifenslave_2.4ubuntu1.2_all.deb
                dpkg -i --force-overwrite /home/install/ifenslave-2.6_2.4ubuntu1.2_all.deb
        fi
fi
if [ -f "/usr/bin/telnet" ];then
        dpkg --purge telnet
fi
if [ -f "/usr/bin/strace" ];then
        rm /usr/bin/strace*
fi
if [ -f "/usr/sbin/tcpdump" ]; then
        dpkg --purge tcpdump
        dpkg --purge libpcap0.8
        ln -s /home/install/bin/tcpdump /bin/tcpdump
fi
dpkg --purge ldap-utils
dpkg --purge isc-dhcp-server
dpkg --purge sssd
if [ -f "/usr/bin/curl" ];then
        apt-get --purge remove curl << EOF
Y
EOF
        apt-get --purge remove libcurl3-gnutls << EOF
Y
EOF
        apt-get --purge remove libcurl4 << EOF
Y
EOF
```

2.3 Disable Debugging Tools

apt-get purge gdb

apt-get purge gcc

apt-get purge cpp

apt-get purge gdbserver

apt-get purge cpp-7

apt-get purge netcat-openbsd

rm /sbin/regdbdump

rm /usr/sbin/cppw

rm /usr/bin/x86_64-linux-gnu-readelf

rm /usr/bin/readelf

rm /usr/bin/vgdb

rm /usr/bin/strace*

2.4 SSH Security

- **Prohibit the root user from directly logging in to the system in SSH mode.**

Add –w in /etc/inetd.conf

```
ls@yf@IPPBX:~# vi /etc/network/lan.conf
ls@yf@IPPBX:~# cat /etc/inetd.conf
ssh     stream tcp nowait root /bin/dropbear -w -L super -i
ls@yf@IPPBX:~#
```

Rollback policy:

a. Remove –w from /etc/inetd.conf

b. Restart inetd service: killall -9 inetd && /bin/inetd &

➢ **Brute-force Attack Prevention**

The systimetask checks */ysdisk/syslog/ssh.log* every 15 seconds. When the number of maximum password retry attempts reaches 10, use iptable (iptables -C INPUT -p tcp -s %s --dport %s -j DROP) to restrict SSH login of the source IP address for 1800 seconds.

The password error in *ssh.log* is shown as below:

```
Oct 24 19:38:59 (none) authpriv.warn dropbear[1077]: Failed loading /etc/dropbear/dropbear_ecdsa_host_key
Oct 24 19:38:59 (none) authpriv.warn dropbear[1077]: Failed loading /etc/dropbear/dropbear_ed25519_host_key
Oct 24 19:38:59 (none) authpriv.info dropbear[1077]: Child connection from 192.168.12.131:39754
Oct 24 19:39:00 (none) authpriv.warn dropbear[1077]: Bad password attempt for 'ls@yf' from 192.168.12.131:39754
```

After the source IP address is blocked, you can run different commands to check firewall rules based on your network environment:

For IPv4, run iptable -L

```
^C
ls@yf@IPPBX:~# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            tcp spt:53
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0            udp spt:53
DROP       tcp  --  192.168.12.131       0.0.0.0/0            tcp dpt:22
DROP       all  --  192.168.12.213       0.0.0.0/0
ACCEPT     all  --  127.0.0.1            127.0.0.1
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
           tcp  --  0.0.0.0/0            0.0.0.0/0            tcp dpt:8022 state NEW recent: SET name
```

For IPv6, run ip6table -L

```
root@IPPBX:~# ip6tables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source                                   destination
DROP       tcp      2201:c311:2222:eeee:eeee:eeee:eeee:120f   ::/0                 tcp dpt:22
```

Block rule configuration:

```
mysql> select * from syscore.sshblockconfig\G;
*************************** 1. row ***************************
                 id: 1
             enable: yes
  scanned_line_number: 182
   scanned_first_line: Oct 24 17:17:34 (none) authpriv.err sudo: PAM (other) illegal module type: @include

        block_seconds: 1800
failed_times_to_block: 9
```

Rollback policy:

1. Database: update *syscore.sshblockconfig enable='no';*
2. Restart systimetask: killall -9 systimetask&& /ysbin/systimetask&

➢ **Disable Insecure Algorithms**

1. -oKexAlgorithms=diffie-hellman-group1-sha1
2. -oHostKeyAlgorithms=ssh-ed25519
3. -m hmac-sha2-256 -c aes256-cbc
4. -m hmac-md5 -c aes256-ctr

The supported algorithms are shown as below:

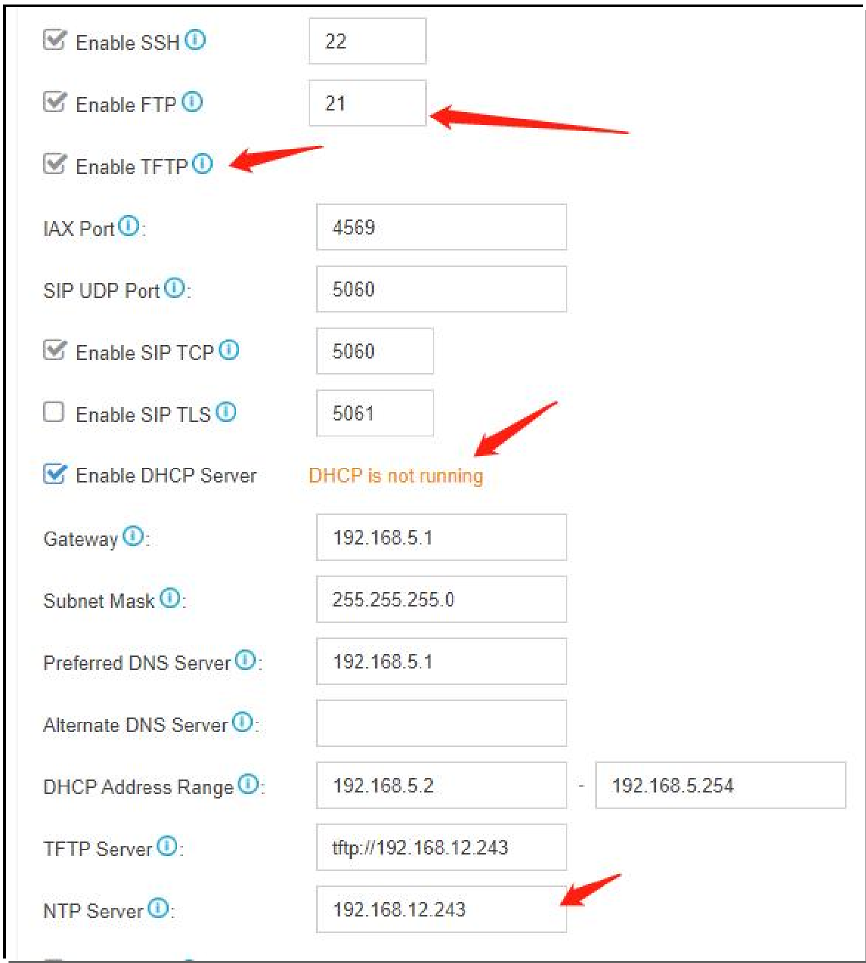
key exchange：

curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,kexguess2@matt.ucc.asn.au

host key type：

rsa-sha2-256,ssh-rsa,ssh-dss
Cipher：
chacha20-poly1305@openssh.com,aes128-ctr,aes256-ctr
MAC：
hmac-sha1,hmac-sha2-256
Rollback policy :
1. Copy *dropbearmulti-s1000* to */tmp/*
2. *killall -9 inetd*
3. Remove *–w* from */etc/inetd.conf*
4. *cp /tmp/dropbearmulti-s1000 /home/install/sbin/dropbearmulti*
5. */bin/inetd &*

2.5 Disable Insecure Services



➢ **Disable DHCP Server**

1. Run *apt-get purge isc-dhcp-server*, you would find DHCP Server is disabled.

```
dpkg-buildflags                 dpkg-deb                 dpkg-genbuil
root@IPPBX:~# dpkg -l |grep dhcp
ii  isc-dhcp-client                             4.3.5-3ubuntu7.3
ii  isc-dhcp-common                             4.3.5-3ubuntu7.3
root@IPPBX:~#
```

2. Remove third-party *dhcp-4.1-ESV-R16-P1* that was compiled by applibs.
dhcpd executable program was removed from */sbin* directory.

- **Disable FTP Server**

1. Do not compile third-party *vsftpd-3.0.4*. In this way, *vsftpd* program would not be stored in */bin* directory of PBX.
2. Make sure */etc/inetd.conf* does NOT contain the followings. In this way, FTP Server can not be started using inetd.

```
192.168.12.131 | serial-com1 | 192.168.12.209 (3) | 192.168.12.131 (1)
ssh      stream tcp nowait root /bin/dropbear -L super -i
ftp      stream tcp nowait root /bin/vsftpd
tftp     dgram  udp wait root /bin/atftpd --no-timeout --log
~
~
```

- **Disable TFTP Server**

1. Do not compile third-party atftp-0.7.4. In this way, atftpd program would not be stored in /bin directory of PBX.
2. Make sure */etc/inetd.conf* does NOT contain the followings. In this way, TFTP Server can not be started using inted.

```
ssh      stream tcp nowait root /bin/dropbear -L super -i
ftp      stream tcp nowait root /bin/vsftpd
tftp     dgram  udp wait root /bin/atftpd --no-timeout --logfile /ysdisk/syslog/tftp3681A1870530.log --logsize 5120 /ysdisk/tftpboot
~
~
~
```

- **Disable NTP Server**

1. Do not compile third-party *atftp-0.7.4*. In this way, *atftpd* program would not be stored in */bin* directory of PBX.
2. Remove */bin/ntpd -4 -c $1 -g -n &* from */etc/init.d/ntpd.sh*

2.6 Run External Program as Non-root User

- **Boa (Web Server)**

```
ii  isc-dhcp-common                          4.3.5-3ubuntu7.3                    amd64
root@IPPBX:~# ps aux |grep boa
root       4085  0.0  0.0  29880  4956 ?       D    Oct21   0:00 /bin/boa -c/ysdisk/etc/boa
www-data   4094  0.0  0.0  29880  4956 ?       S    Oct21   0:00 /bin/boa -c/ysdisk/etc/boa
root      32539  0.0  0.0  11472  1148 pts/0   S+   21:55   0:00 grep --color=auto boa
root@IPPBX:~#
```

1. In */ysdisk/etc/boa/boa.conf*, set *user* and *group*.
2. To run background service such as *syscore* and *pbxcore* via *cgi*, you need to configure the followings in */etc/sudoers*:

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
%www-data  ALL=(ALL) NOPASSWD:/ysbin/syscore,/ysbin/operlog,/ysdisk/ysapps/pbxcenter/bin/*,/ysdi
sk/ysapps/billing/bin/billing,/ysdisk/ysapps/conferencepanel/bin/conferencepanel,/ysdisk/ysapps/
pbxcenter/boot/*,/ysbin/ybkcrypt,/ysbin/pc_firmware_opt,/ysbin/eventadd,/bin/cp,/bin/touch,/bin/
chown
~
```

   In this way, cgi could execute program via *sudo -uroot /ysbin/syscore* without entering password.
3. Make sure *www-data* account could read, write, and execute */var/run/mysqld/mysql.sock* as cgi is connected using */var/run/mysqld/mysql.sock* instead of *host 127.0.0.1*.
4. Owner of directories concerning Boa operations shall be changed to *www-data*.

```
chown www-data:www-data /ysdisk//gui_backups/ -R
chown www-data:www-data /ysdisk/etc/boa/ -R
chown www-data:www-data /ysdisk/www/ -R
chown www-data:www-data /ysdisk/cache/ -R
chown www-data:www-data /ysdisk/syslog/ -R
chown www-data:www-data /ysdisk/webupload/ -R
```

5. Owner of the files that were downloaded from PBX web page shall be changed to *www-data*. In this way, cgi can read the files and run *printf* to display the files on PBX web page.

- **Asterisk (PBX Voice Service)**

```
root@IPPBX:/var/run/lock# ps aux |grep asterisk
www-data  5485  0.1  0.4 4796552 32556 ?      Sl   Oct21   7:09 /ysdisk/ysapps/pbxcenter/bin/asterisk -vvvvvvvvvv
root      6212  0.0  0.0  11472  1032 pts/0   S+   22:20   0:00 grep --color=auto asterisk
```

1. In */etc/asterisk/asterisk.conf*, set *runuser* and *rungroup*.
2. In */etc/sudoers*, configure as follows:

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
%www-data  ALL=(ALL) NOPASSWD:/ysbin/syscore,/ysbin/operlog,/ysdisk/ysapps/pbxcenter/bin/* /ysdisk/ysapps/billing/bin/billing,/ysdisk/ysapps/conferencepanel/bin/conferencepanel,/ysdisk/ysapps/pbxcenter/boot/*,/y
c_firmware_opt,/ysbin/eventadd,/bin/cp,/bin/touch,/bin/chown
~
~
```

3. In */ysdisk/ysapps/pbxcenter/start*, set the permission of asterisk */run* directory.

```
chmod 664 /ysdisk/var/lib/asterisk/astdb.sqlite3
chmod 771 /var/run/asterisk/
chown www-data:www-data /etc/asterisk/*
chown www-data:www-data /ysdisk/ysapps/pbxcenter/etc/codec.conf
chown www-data:www-data /ysdisk/ysapps/pbxcenter/etc/faxlib.conf
chown www-data:www-data /ysdisk/ysapps/pbxcenter/etc/usb_modules.conf
chown www-data:www-data -R /ysdisk/ysapps/pbxcenter/etc/asterisk
chown www-data:www-data -R /ysdisk/ysapps/pbxcenter/var/lib/asterisk
chown www-data:www-data -R /ysdisk/ysapps/pbxcenter/var/spool
chown www-data:www-data -R /ysdisk/var/lib/asterisk/
if [ 0 -ne 0 ];then
```

- **cwmpclient (Remote Management)**
  1. In */ysdisk/etc/cwmp/cwmp.conf*, set *user* and *group*.
  2. In */etc/sudoers*, configure as follows:

     add /ysdisk/ysapps/pbxcenter/bin/, /ysbin/ybkcrypt, /ysbin/pc_firmware_opt in %www-data,*
  3. Change directory permission

     chown www-data:www-data /ysdisk/gui_backups/ -R

- **Hot Standby**
  1. External data is forwarded from *rinetd* to *heartbeat*.

     Run *rinetd* as *www-data* account and use 127.0.0.1 to listen on heartbeat.

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:873           0.0.0.0:*               LISTEN      5426/rsync
tcp        0      0 0.0.0.0:6090            0.0.0.0:*               LISTEN      6177/rinetd
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      2181/mysqld
tcp        0      0 127.0.0.1:5038          0.0.0.0:*               LISTEN      4063/asterisk
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      6887/boa
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      934/systemd-resolve
```

```
root@IPPBX224:/ysdisk/support#
root@IPPBX224:/ysdisk/support# ps aux |grep rinted
root      10381  0.0  0.0  14436  1016 pts/0    S+   01:11   0:00 grep --color=auto rinted
root@IPPBX224:/ysdisk/support# ps aux |grep rinetd
www-data   [illegible]  0.0  0.0   4752    72 ?        Ss   01:05   0:00 /bin/rinetd
root      10441  0.0  0.0  14436  1016 pts/0    S+   01:11   0:00 grep --color=auto rinetd
root@IPPBX224:/ysdisk/support#
```

  2. In /ysdisk/etc/rinetd.conf, set up port forwarding:

0.0.0.0	6088/udp	127.0.0.1	6089/udp
::	6088/udp	127.0.0.1	6089/udp
0.0.0.0	6090	127.0.0.1	873
::	6090	127.0.0.1	873

     Heartbeat port 6089 -> 6088（rinetd external）

     Rsync port: 873-> 6090（rinetd external）

2.7 File System

- **Update umask**

  Add *umask 027* in */etc/profile*
- **Change permissions of existing files to 755**

  chmod 751 -R /ysdisk/ysapps/*

  chmod 755 /ysdisk/ysapps

  chmod 775 ./ysdisk

chmod 755 -R ./ysdisk/syslog
chmod -R 750 /home/install/etc/ysmodules/
chmod -R 750 /home/install/ysdisk/www/webfile/
chmod 755 -R /ysdisk/ysapps/pbxcenter/usr/lib/asterisk/modules
chmod 664 /ysdisk/var/lib/asterisk/astdb.sqlite3
chmod 771 /var/run/asterisk/
chmod 755 /ysdisk/support/add.sh
chmod 755 /ysdisk/support/rc_stop.sh

```
chmod -R 750 /home/install/etc/ysmodules/
chmod -R 750 /home/install/ysdisk/www/webfile/
chmod o-w /home/install/ysdisk/imageupdate
chmod o-w /home/install/ysdisk/support/customcfg
chmod o-w /home/install/ysdisk/tftpboot
chmod o-w /home/install/ysdisk/ftp_media
chmod o-w /run/mysqld
chown root:root /boot/grub/grub.cfg
chmod u-wx,go-rwx /boot/grub/grub.cfg

groupadd sugroup
chown root:root /etc/crontab
chmod og-rwx /etc/crontab
chown root:root /etc/cron.hourly/
chmod og-rwx /etc/cron.hourly/
chown root:root /etc/cron.daily/
chmod og-rwx /etc/cron.daily/
chown root:root /etc/cron.weekly/
chmod og-rwx /etc/cron.weekly/
chown root:root /etc/cron.monthly/
chmod og-rwx /etc/cron.monthly/
chown root:root /etc/cron.d/
chmod og-rwx /etc/cron.d/
rm /etc/cron.deny
touch /etc/cron.allow
chown root:root /etc/cron.allow
chmod g-rwx,o-rwx /etc/cron.allow
rm /etc/at.deny
touch /etc/at.allow
chown root:root /etc/at.allow
chmod g-wx,o-rwx /etc/at.allow
```

2.8 Encryption Root Key

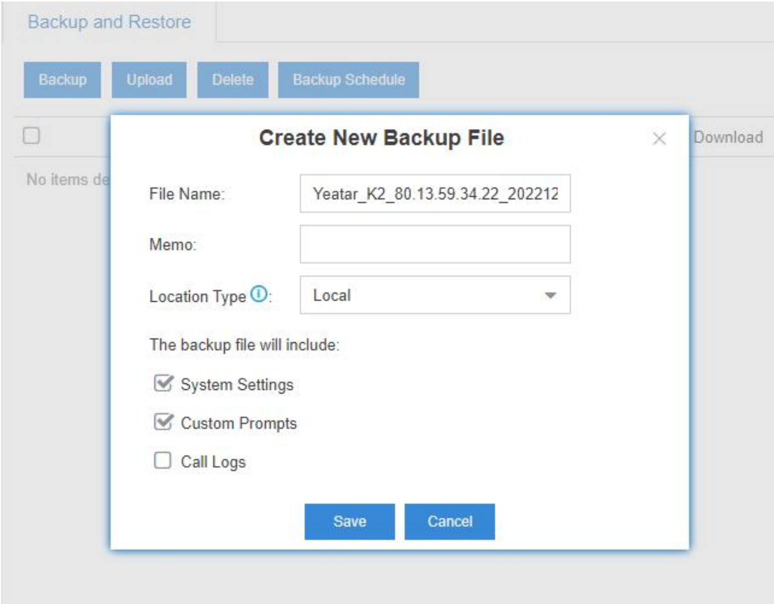
1. Use random algorithm (RAND_bytes in OpenSSL) to generate root key, encrypt the key with pbkdf2, and set file permission to 600.

```
root@IPPBX:/ysdisk/etc# ls -al .db* .pwd* .root*
-rw------- 1 www-data www-data 64 Oct 19 17:07 .db_k
-rw------- 1 www-data www-data 44 Oct 19 17:07 .pwd_k
-rw------- 1 www-data www-data 20 Oct 19 17:07 .root_k
root@IPPBX:/ysdisk/etc#
root@IPPBX:/ysdisk/etc#
```

2. Use *GET_DB_PASSWORD* to get a password instead of hard coding. The password is composed of root password and salt, which are obtained from *.pwd_k* and *.root_k*, and is encrypted with pbkdf2.
3. Encrypt the followings using AES-128-CBC algorithm and key:
   Database Password
   Encryption activation server
   Hot Standby verification key

Voicemail PIN
Email password
Openvpn password
DNSS client password
API password
Extension registration password
Voicemail box login password
The key is encrypted using pbkdf2 and is composed of root password and salt, which are obtained from *.db_k* and *.root_k* files.

4. For the PBX backup file, users shall enter a password on PBX web page to encrypt the file.



2.9 Disable md5 Encryption and md5sum Commands

1. Use SHA-512 to encrypt support account and root account.

2. When running */ysbin/sshpass* to reset SSH password of support account, the password must be encrypted with SHA-512.
3. Use SHA256sum instead of md5sum to validate the downloaded file when interacting with Remote Management.

2.10 Audit Log

```
audisp/ audit/
root@IPPBX:/ysdisk/etc# cd /etc/audit/rules.d
root@IPPBX:/etc/audit/rules.d# ls -al
total 76
drwxr-xr-x 2 root root 4096 Oct 18 23:48 .
drwxr-xr-x 3 root root 4096 Oct 18 23:48 ..
-rw-r--r-- 1 root root   76 Oct 18 23:48 50-MAC-policy.rules
-rw-r--r-- 1 root root  554 Oct 18 23:48 50-access.rules
-rw-r--r-- 1 root root  208 Oct 18 23:48 50-actions.rules
-rw-r--r-- 1 root root  230 Oct 18 23:48 50-delete.rules
-rw-r--r-- 1 root root  175 Oct 18 23:48 50-identity.rules
-rw-r--r-- 1 root root  109 Oct 18 23:48 50-logins.rules
-rw-r--r-- 1 root root  167 Oct 18 23:48 50-modules.rules
-rw-r--r-- 1 root root  160 Oct 18 23:48 50-mounts.rules
-rw-r--r-- 1 root root  752 Oct 18 23:48 50-perm_mod.rules
-rw-r--r-- 1 root root 4486 Oct 18 23:48 50-privileged.rules
-rw-r--r-- 1 root root   65 Oct 18 23:48 50-scope.rules
-rw-r--r-- 1 root root  100 Oct 18 23:48 50-session.rules
-rw-r--r-- 1 root root  306 Oct 18 23:48 50-system-locale.rules
-rw-r--r-- 1 root root  306 Oct 18 23:48 50-time-change.rules
-rw-r--r-- 1 root root    5 Oct 18 23:48 99-finalize.rules
-rw-r----- 1 root root  240 Oct 18 23:48 audit.rules
root@IPPBX:/etc/audit/rules.d#
```

Audit log provides information about the operations that have been performed on the system。

2.11 Set up login restrictions

Restrict all accounts from logging in except ls@yf and support .

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
support:x:222:222:yeastar:/ysdisk/support:/bin/sh
lxd:x:105:65534::/var/lib/lxd/:/bin/false
landscape:x:107:115::/var/lib/landscape:/usr/sbin/nologin
mysql:x:64001:64001:MySQL Server:/var/lib/mysql:/sbin/nologin
```

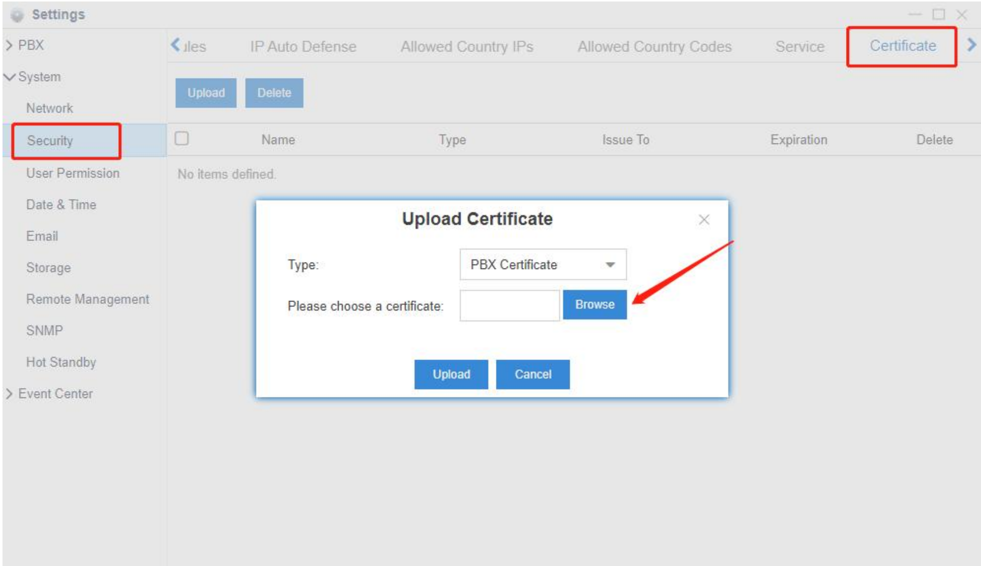
2.12 Deny mounting with nodev, noexec, and nosuid

1. Deny mounting /dev/shm and /tmp with nodev, noexec, and nosuid
2. Deny mount /home with nodev, noexec, and nosuid

3 Web Security

3.1 Encryption and Replacement of Certificates

1. Upload a certificate on PBX web page to replace.



2. The certificate is encrypted with AES-128-CBC algorithm, and then passed to the boa server via shared memory.

3.2 Use HTTPS Protocol

➢ **Upgrade openssl to 1.1.11**

```
root@IPPBX:/home/install/usr/bin# ldd /bin/boa
        linux-vdso.so.1 (0x00007fff54f79000)
        libssl.so.1.1 => /usr/lib/x86_64-linux-gnu/libssl.so.1.1 (0x00007f4f2fd09000)
        libcrypto.so.1.1 => /usr/lib/x86_64-linux-gnu/libcrypto.so.1.1 (0x00007f4f2f816000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f4f2f425000)
        libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007f4f2f206000)
        libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007f4f2f002000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f4f301b9000)
```

➢ **Use TLS 1.2 and disable insecure protocols (CBC\SHA)**

1. boa calls TLSv1_2_server_method to use HTTPS protocol.
2. Update /ysdisk/etc/boa/boa.conf as follows to support secure protocols:

SSLciphers HIGH:MEDIUM:!aNULL:!MD5:!RC4:!DES:!IDEA:!3DES:!SHA1:!SHA256:!ECDHE-RSA-AES256-SHA384:!ECDHE-RSA-CAMELLIA256-SHA384

For more information about corresponding algorithms, see: https://www.openssl.org/docs/man1.1.0/man1/ciphers.html

3.3 Boa Patch Upgrade

Version: 0.94.14rc21
CVE-2018-21027 & CVE-2018-21028

Patch link:

https://github.com/gpg/boa/pull/1/commits/e139b87835994d007fbd64eead6c1455d7b8cf4e

Commit 2c4e908f authored 2 years ago by qhm Committed by csq6074 2 years ago

Browse files | Options

ID1017240 boa: 修复内存溢出漏洞

https://www.tapd.cn/32809406/bugtrace/bugs/view?bug_id=1132809406001017240

parent b7b82be8 T1.0.27-0.2 ...

No related merge requests found

Changes 4

Showing 4 changed files with 17 additions and 4 deletions

Hide whitespace changes | Inline | Side-by-side

src/apps/boa-new/extras/scandir.c +11 -2 View file @2c4e908f

```
@@ -56,17 +56,26 @@ scandir(const char *dir, struct dirent ***namelist,

     while (NULL != readdir(d))
         count++;
+    closedir(d);

     names = malloc(sizeof (struct dirent *) * count);
+    if (!names) {
+        return -1;
+    }

-    closedir(d);
     d = opendir(dir);
-    if (NULL == d)
+    if (NULL == d) {
+        free(names);
         return -1;
+    }

     while (NULL != (current = readdir(d))) {
         if (NULL == select || select(current)) {
             struct dirent *copyentry = malloc(current->d_reclen);
+            /* FIXME: OOM, silently skip it?*/
+            if (!copyentry) {
+                continue;
```

src/apps/boa-new/src/index_dir.c +4 -1

```
@@ -376,6 +376,9 @@ int main(int argc, char *argv[])
     timeptr = gmtime(&timep);
 #endif
     now = strdup(asctime(timeptr));
+    if (!now) {
+        return -1;
+    }
     now[strlen(now) - 1] = '\0';
 #ifdef USE_LOCALTIME
     printf("</table>\n<hr noshade>\nIndex generated %s %s\n"
@@ -386,6 +389,6 @@ int main(int argc, char *argv[])
            "<!-- This program is part of the Boa Webserver Copyright (C) 1991-2002
 >\n"
            "</body>\n</html>\n", now);
 #endif
-
+    free(now);
     return 0;
 }
```

src/apps/boa-new/src/sublog.c +1 -0

```
@@ -142,6 +142,7 @@ int main(int argc, char *argv[])
             exit(EXIT_FAILURE);
         }
     }
+    close(fd);
     return 0;
 }
 #endif
```

Yeastar

3.4 Prevent Clickjacking

Add *X-Frame-Options DENY* to */ysdisk/etc/boa/boa.conf*

3.5 Logs about Operations on PBX Web Page

1. All the operations on PBX web page are recorded in operlog. You can run select * from operlog.operlog; to check.
2. Anonymize sensitive data.

Options	Value
Extension	1006
Email	7650*********.com
Address	福建省厦**********************************号楼0abc
Mobile Number	861******3731
Title	TCG-高**********************师0026

3.6 Lockout for Failed Login Attempts

1. Use iptable to block the IP address with too many failed login attempts.
2. Record the failed login attempts in syscore.autherror.

IPV4:

```
3 rows in set (0.01 sec)

mysql> select * from syscore.autherror;
+----+------+---------------+---------+---------------------+---------------------+--
| id | type | IP            | Account | LockTime            | UnLockTime          | T
+----+------+---------------+---------+---------------------+---------------------+--
|  2 | 3    | 192.168.12.69 | 1004    | 2021-10-21 02:05:36 | 2022-10-16 02:05:36 |
|  3 | 3    | 192.168.12.49 |         | 2021-10-21 02:05:37 | 2022-10-16 02:05:37 |
|  4 | 3    | 192.168.12.79 | 1004    | 2021-10-21 02:06:38 | 2022-10-16 02:06:38 |
+----+------+---------------+---------+---------------------+---------------------+--
```

IPV6:

```
mysql> select * from autherror;
+----+------+----------------------------------------------+---------+---------------------+-----------
--------+-------+--------------+-------+----------+---------+---------+
| id | type | IP                                           | Account | LockTime            | UnLockTime
       | Times | account_to_ip | State | others1 | others2 | dstport |
+----+------+----------------------------------------------+---------+---------------------+-----------
--------+-------+--------------+-------+----------+---------+---------+
| 11 | 0    | 2201:c311:2222:eeee:eeee:eeee:eeee:120f  admin    | 2022-12-12 15:56:59 | 2022-12-12 1
6:06:59 |       | 1            | 4     |          |         |         |
+----+------+----------------------------------------------+---------+---------------------+-----------
--------+-------+--------------+-------+----------+---------+---------+
```

3.7 File Upload Validation

Item	Format	Validation Method
Custom Prompt	wav or gsm	Run Asterisk –vvvvr to check if file format can be converted.
Image file	bin	/bin/pc_firmware_opt Validate the sha256sum

Backup File	bak	Use the user-defined password to decrypt the backup file.
Certificate	pem	Use openssl to validate the certificate. If the format is incorrect, you can't successfully upload the certificate.
Extension, Trunk, Inbound Route, and Outbound Route	csv	Validate file content.

4 Database Security

4.1 Upgrade mysql from 5.1.6 to 5.7.40

```
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)
root@IPPBX:~# mysql -V
mysql  Ver 14.14 Distrib 5.7.40, for Linux (x86_64) using  EditLine wrapper
root@IPPBX:~#
```

4.2 mysql Monitoring and IP Restriction

1. Add *bind-address= 127.0.0.1* in */etc/my.cnf*.
2. Only local access to *127.0.0.1* is allowed.

```
mysql> select host,user from mysql.user;
+-----------+---------------+
| host      | user          |
+-----------+---------------+
| localhost | mypbx_sys_user |
| localhost | mysql.session |
| localhost | mysql.sys     |
| localhost | root          |
+-----------+---------------+
4 rows in set (0.00 sec)
```

3. Prevent duplicate user names

Delete multiple hosts existing in the same user name. Use select user,count(*) from user group by user having count(*) > 1; to check if the hosts still exist.

4.3 Disable mysql History

rm ~/.mysql_history
ln -s /dev/null ~/.mysql_history

4.4 Run mysql as Non-root User and Set Account Restriction

1. Use mysql to run mysql service.

```
root@IPPBX:/etc# ps aux |grep mysql
root      1870  0.0  0.0  21480  3784 ?      S    Oct21   0:00 /bin/sh /home/install/usr/bin/mysqld_safe --datadir=/var/lib/mysql/ --pid-file=/var/run/mysqld/mysqld.pid
mysql     2225  0.0  1.1 2107672 90040 ?     Sl   Oct21   0:57 /home/install/usr/libexec/mysqld --basedir=/home/install/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/plu
le=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysql.sock --port=3306
root     26089  0.0  0.0  11472  1072 pts/0   S+   23:49   0:00 grep --color=auto mysql
root@IPPBX:/etc#
```

2. Restrict mysql account from logging in to PBX system.

usermod -s /bin/false mysql
usermod -s /sbin/nologin mysql

4.5 Allow Changes to Password of Mysql Root Account

Run mysqladmin -uroot -pH@db*902020 password {new_password}

4.6 Enable Error Logs

```
mysql>
mysql> show variables like 'log_error';
+---------------+---------------------+
| Variable_name | Value               |
+---------------+---------------------+
| log_error     | /var/log/mysqld.log |
+---------------+---------------------+
1 row in set (0.00 sec)

mysql> quit
Bye
root@IPPBX:/etc# cat /etc/my.cnf
[mysqld]
port=3306
bind-address= 127.0.0.1
datadir=/var/lib/mysql/
basedir=/home/install/usr
default-storage-engine=MyISAM
socket=/var/run/mysqld/mysql.sock
server-id=1
log-bin=mysql-bin
log-error=/var/log/mysqld.log
pid-file=/var/run/mysqld/mysqld.pid
lower_case_table_names=1
plugin-dir=/usr/lib/plugin
sql-mode=STRICT_TRANS_TABLES,ERROR_FOR_DIVISION_BY_ZERO,NO_ENGINE_SUBSTITUTION,STRICT_ALL_
performance_schema = 0
symbolic-links=0
local-infile=0
user=mysql
innodb_temp_data_file_path = ibtmp1:12M:autoextend:max:100M
innodb_buffer_pool_size=2M
innodb_data_file_path = ibdata1:12M:autoextend:max:100M
language=/home/install/usr/share/mysql/english/
root@IPPBX:/etc#
```

5 Third-party Library Scanning

5.1 Upgrade applibs

The third-party libraries currently in use are as follows:

Components Scanned		
Component	**Version**	**Publish Date**
berkeleydb	6.2.32	
boa	0.94.14	
busybox	1.33.1	
coreutils	8.32	
curl	7.79.0	2021.09.15
curl	7.78	
curl	7.77.0	
dhcpcd	9.4.0	
dropbear	2020.81	
dropbear ssh server and client	2020.81	
editline library - libedit	5.7.33 (mysql key word)	
ethtool	1.8	

ethtool	5	
glib	2.68.2	
gmp	5.1.3	2013.09.30
ipset	6.34	
iptables	1.8.7	
jansson	2.13.1	2020.05.07
libcap-ng	1.3.0	
libdb	6.2.32	
libedit	3.1	
libevent	2.1.12	2020.07.05
libffi	3.3	2019.11.23
libiconv	1.13.1	2009.07.12
libmnl	1.0.4	2016.07.02
libnet	1.1.6	
libpcap	1.10.1	
libpcap	1.10.0	2020.12.30
libpng	1.6.37	2019.04.14
libsrtp	1.5.4	
libtiff	4.3.0	
libtiff	4.2.0	2020.12.19
libxml2	2.9.12	2021.05.14
mysql	5.7.33	
mysql database server	5.733 (mysql key word)	
mysql-client	5.7.33 (mysql key word)	
ncurses	6.2	2020.02.12
nghttp2	1.41.0	2020.06.02
ntp	4.2.8p15	2020.06.23
openlitespeed	0.94.14 (boa key word)	

openssl	1.1.11	2021.08.24
openssl	1.0.2u	
openssl	1.1.11	
openvpn	2.5.3	
openvpn	2.6	
opus	1.3.1	2019.04.12
pcre	2.68.2	
popt	3.2.3 (rsync key word)	
ppp	2.4.9	2021.01.05
rp_pppoe	3.3	
rsync	3.2.3	
spandsp	0.0.6	
spdylay	1.41.0	
speex	1.2beta2	
speex	1.2.0	2016.12.08
speexdsp	1.2.0	2019.05.29
sqlite	3.35.5	
sqlite3	3.36.0	2021.06.18
ssmtp	2.60	
tcpdump	4.99.0	2020.12.30
tomcrypt	2020.81	
util-linux	2.37	
wget	1.21.1	
wxsqlite3	3.36.0	
zlib	1.2.11	2017.01.15

5.2 Source Code Compilation

Both native codes and third-party library codes support compilation, including BIND_NOW, NX, PIC, PIE, RELRO, SP, NO Rpath, Runpath and Strip.

5.3 Install Vulerability Patch

- **busybox CVE-2022-28391**

  Patch link:

  https://git.alpinelinux.org/aports/plain/main/busybox/0001-libbb-sockaddr2str-ensure-only-printable-characters-.patch

```
diff --git a/src/apps/busybox-1.33.2/libbb/xconnect.c b/src/apps/busybox-1.33.2/libbb/xconnect.c
index 5dd9cfd..e85fa75 100644
--- a/src/apps/busybox-1.33.2/libbb/xconnect.c
+++ b/src/apps/busybox-1.33.2/libbb/xconnect.c
@@ -15,6 +15,7 @@
 # include <linux/netlink.h>
 #endif
 #include "libbb.h"
+#include "yeastar_app.h"

 int FAST_FUNC setsockopt_int(int fd, int level, int optname, int optval)
 {
@@ -506,11 +507,19 @@ static char* FAST_FUNC sockaddr2str(const struct sockaddr *sa, int flags)
        if (rc)
                return NULL;
        if (flags & IGNORE_PORT)
+#ifdef YEASTAR_CSQ_BUSYBOX_PATCH_CVE-2022-28391
+               return xstrdup(printable_string(NULL, host));
+#else
                return xstrdup(host);
+#endif
 #if ENABLE_FEATURE_IPV6
        if (sa->sa_family == AF_INET6) {
                if (strchr(host, ':')) /* heh, it's not a resolved hostname */
+               #ifdef YEASTAR_CSQ_BUSYBOX_PATCH_CVE-2022-28391
+                       return xasprintf("%s:%s", printable_string(NULL, host), serv);
+               #else
                        return xasprintf("[%s]:%s", host, serv);
+               #endif
                /*return xasprintf("%s:%s", host, serv);*/
                /* - fall through instead */
        }
```

- **Libtiff CVE-2022-3570**

  Patch link:

  https://gitlab.com/libtiff/libtiff/-/commit/bd94a9b383d8755a27b5a1bc27660b8ad10b094c

```
diff --git a/src/apps/tiff-4.4.0/tools/tiffcrop.c b/src/apps/tiff-4.4.0/tools/tiffcrop.c
index 1f827b2..453e5e8 100644
--- a/src/apps/tiff-4.4.0/tools/tiffcrop.c
+++ b/src/apps/tiff-4.4.0/tools/tiffcrop.c
@@ -111,9 +111,17 @@
  * Note:    The (-X|-Y), -Z and -z options are mutually exclusive.
  *          In no case should the options be applied to a given selection successively.
  */
+#ifndef YEASTAR_CSQ_SYNC_CVE_2022_3570
+#define YEASTAR_CSQ_SYNC_CVE_2022_3570
+#endif

+#ifdef YEASTAR_CSQ_SYNC_CVE_2022_3570
+static   char tiffcrop_version_id[] = "2.5.2";
+static   char tiffcrop_rev_date[] = "22-08-2022";
+#else
 static   char tiffcrop_version_id[] = "2.5";
 static   char tiffcrop_rev_date[] = "02-09-2022";
+#endif

 #include "tif_config.h"
 #include "libport.h"
@@ -210,6 +218,12 @@ static   char tiffcrop_rev_date[] = "02-09-2022";

 #define TIFF_DIR_MAX  65534

+#ifdef YEASTAR_CSQ_SYNC_CVE_2022_3570
+/* Some conversion subroutines require image buffers, which are at least 3 bytes
+ * larger than the necessary size for the image itself. */
+#define NUM_BUFF_OVERSIZE_BYTES   3
+#endif
+
 /* Offsets into buffer for margins and fixed width and length segments */
 struct offset {
   uint32_t  tmargin;
@@ -231,7 +245,11 @@ struct offset {
  */

 struct  buffinfo {
+#ifdef YEASTAR_CSQ_SYNC_CVE_2022_3570
+       uint64_t size;            /* size of this buffer */
+#else
   uint32_t size;           /* size of this buffer */
+#endif
   unsigned char *buffer; /* address of the allocated buffer */
 };

@@ -805,8 +823,13 @@ static int readContigTilesIntoBuffer (TIFF* in, uint8_t* buf,
   uint32_t dst_rowsize, shift_width;
   uint32_t bytes_per_sample, bytes_per_pixel;
   uint32_t trailing_bits, prev_trailing_bits;
+#ifdef YEASTAR_CSQ_SYNC_CVE_2022_3570
+       tmsize_t tile_rowsize  = TIFFTileRowSize(in);
+       tmsize_t src_offset, dst_offset;
+#else
   uint32_t tile_rowsize  = TIFFTileRowSize(in);
   uint32_t src_offset, dst_offset;
+#endif
   uint32_t row_offset, col_offset;
   uint8_t *bufp = (uint8_t*) buf;
   unsigned char *src = NULL;
@@ -856,7 +879,11 @@ static int readContigTilesIntoBuffer (TIFF* in, uint8_t* buf,
       TIFFError("readContigTilesIntoBuffer", "Integer overflow when calculating buffer size.");
       exit(EXIT_FAILURE);
   }
+#ifdef YEASTAR_CSQ_SYNC_CVE_2022_3570
:
```

- **gmp CVE-2021-43618**

  Patch link: https://gmplib.org/repo/gmp-6.2/rev/561a9c25298e

```
root@yeastar1-B250M-D2V:/home/S/ipv6/applibs# git diff src/libs/gmp-5.1.3/mpz/inp_r
diff --git a/src/libs/gmp-5.1.3/mpz/inp_raw.c b/src/libs/gmp-5.1.3/mpz/inp_raw.c
index 0da0c61..e5b9083 100644
--- a/src/libs/gmp-5.1.3/mpz/inp_raw.c
+++ b/src/libs/gmp-5.1.3/mpz/inp_raw.c
@@ -21,6 +21,7 @@ along with the GNU MP Library.  If not, see http://www.gnu.org/li
 #include "gmp.h"
 #include "gmp-impl.h"

+#define YEASTAR_CSQ_PATCH_CVE_2021_43618

 /* NTOH_LIMB_FETCH fetches a limb which is in network byte order (ie. big
    endian) and produces a normal host byte order result. */
@@ -81,8 +82,17 @@ mpz_inp_raw (mpz_ptr x, FILE *fp)

   abs_csize = ABS (csize);

+#ifdef YEASTAR_CSQ_PATCH_CVE_2021_43618
+       if (UNLIKELY (abs_csize > ~(mp_bitcnt_t) 0 / 8))
+               return 0;  /* Bit size overflows */
+#endif
+
   /* round up to a multiple of limbs */
+#ifdef YEASTAR_CSQ_PATCH_CVE_2021_43618
+       abs_xsize = BITS_TO_LIMBS ((mp_bitcnt_t) abs_csize * 8);
+#else
   abs_xsize = (abs_csize*8 + GMP_NUMB_BITS-1) / GMP_NUMB_BITS;
+#endif

   if (abs_xsize != 0)
     {
root@yeastar1-B250M-D2V:/home/S/ipv6/applibs#
```

- **pjsip CVE-2017-16872**

  Patch: https://trac.pjsip.org/repos/changeset/5682

```
修改:      src/pjproject-2.6/pjlib/build/pjlib.vcproj
修改:      src/pjproject-2.6/pjlib/build/pjlib.vcxproj
修改:      src/pjproject-2.6/pjlib/build/pjlib.vcxproj.filters
修改:      src/pjproject-2.6/pjlib/include/pj/compat/os_win32.h
修改:      src/pjproject-2.6/pjlib/include/pj/string.h
修改:      src/pjproject-2.6/pjlib/include/pj/types.h
修改:      src/pjproject-2.6/pjlib/src/pj/string.c
修改:      src/pjproject-2.6/pjlib/src/pj/timer.c
修改:      src/pjproject-2.6/pjsip/include/pjsip/sip_parser.h
修改:      src/pjproject-2.6/pjsip/src/pjsip/sip_parser.c
修改:      src/pjproject-2.6/pjsip/src/pjsip/sip_transaction.c
修改:      src/pjproject-2.6/pjsip/src/pjsip/sip_transport.c
```

```
@@ -284,6 +338,13 @@ static pj_status_t init_parser()
                                     &PJSIP_SYN_ERR_EXCEPTION);
     PJ_ASSERT_RETURN(status == PJ_SUCCESS, status);

+/*
+        * Invalid value exception.
+*/
+        pj_assert (PJSIP_EINVAL_ERR_EXCEPTION == -2);
+        status = pj_exception_id_alloc("PJSIP invalid value error",
+                                                            &PJSIP_EINVAL_ERR_EXCEPTION);
+        PJ_ASSERT_RETURN(status == PJ_SUCCESS, status);
     /*
      * Init character input spec (cis)
      */
@@ -502,6 +563,9 @@ void deinit_sip_parser(void)
        /* Deregister exception ID */
        pj_exception_id_free(PJSIP_SYN_ERR_EXCEPTION);
        PJSIP_SYN_ERR_EXCEPTION = -1;
+
+       pj_exception_id_free(PJSIP_EINVAL_ERR_EXCEPTION);
+       PJSIP_EINVAL_ERR_EXCEPTION = -2;
     }
     pj_leave_critical_section();
 }
@@ -766,8 +830,7 @@ PJ_DEF(pjsip_msg *) pjsip_parse_rdata( char *buf, pj_size_t size,
 }

 /* Determine if a message has been received. */
-PJ_DEF(pj_bool_t) pjsip_find_msg( const char *buf, pj_size_t size,
-                                  pj_bool_t is_datagram, pj_size_t *msg_size)
+PJ_DEF(pj_status_t) pjsip_find_msg( const char *buf, pj_size_t size, pj_bool_t is_datagram, pj_size_t *msg_size)
 {
 #if PJ_HAS_TCP
     const char *hdr_end;
@@ -776,6 +839,7 @@ PJ_DEF(pj_bool_t) pjsip_find_msg( const char *buf, pj_size_t size,
     const char *line;
     int content_length = -1;
     pj_str_t cur_msg;
+    pj_status_t status = PJ_SUCCESS;
     const pj_str_t end_hdr = { "\n\r\n", 3};

     *msg_size = size;
@@ -836,9 +900,15 @@ PJ_DEF(pj_bool_t) pjsip_find_msg( const char *buf, pj_size_t size,
                 pj_scan_get_newline(&scanner);

                 /* Found a valid Content-Length header. */
-                content_length = pj_strtoul(&str_clen);
+                strtoi_validate(&str_clen, PJSIP_MIN_CONTENT_LENGTH, PJSIP_MAX_CONTENT_LENGTH, &content_length);
             }
             PJ_CATCH_ANY {
+                int eid = PJ_GET_EXCEPTION();
+                if (eid == PJSIP_SYN_ERR_EXCEPTION) {
+                        status = PJSIP_EMISSINGHDR;
+                } else if (eid == PJSIP_EINVAL_ERR_EXCEPTION) {
+                        status = PJSIP_EINVALIDHDR;
+                }
                 content_length = -1;
             }
```

- **pjsip CVE-2017-16875**

  Patch: https://trac.pjsip.org/repos/ticket/2055

```
\ No newline at end of file
diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index 8a836c0..a0e5e62 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -202,4 +202,12 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_5740_PATCH
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_5680_PATCH
+/*****************************************************************
+* 2021.08.12 同步https://trac.pjsip.org/repos/changeset/5680
+* Cannot register ioqueue key after double key unregistration
+****************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_5680_PATCH
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjlib/src/pj/activesock.c b/src/pjproject-2.6/pjlib/src/pj/activesock.c
index b9dee42..431639d 100644
--- a/src/pjproject-2.6/pjlib/src/pj/activesock.c
+++ b/src/pjproject-2.6/pjlib/src/pj/activesock.c
@@ -296,17 +296,37 @@ PJ_DEF(pj_status_t) pj_activesock_create_udp( pj_pool_t *pool,

 PJ_DEF(pj_status_t) pj_activesock_close(pj_activesock_t *asock)
 {
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_5680_PATCH
+       pj_ioqueue_key_t *key;
+       pj_bool_t unregister = PJ_FALSE;
+#endif
     PJ_ASSERT_RETURN(asock, PJ_EINVAL);
     asock->shutdown = SHUT_RX | SHUT_TX;
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_5680_PATCH
+       /* Avoid double unregistration on the key */
+       key = asock->key;
+       if (key) {
+               pj_ioqueue_lock_key(key);
+               unregister = (asock->key != NULL);
+               asock->key = NULL;
+               asock->key = NULL;
+       }
+
+       if (unregister) {
+               pj_ioqueue_unregister(key);
+#else
     if (asock->key) {
        pj_ioqueue_unregister(asock->key);
+#endif

 #if defined(PJ_IPHONE_OS_HAS_MULTITASKING_SUPPORT) && \
     PJ_IPHONE_OS_HAS_MULTITASKING_SUPPORT!=0
        activesock_destroy_iphone_os_stream(asock);
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_5680_PATCH
        asock->key = NULL;
+#endif
     }
     return PJ_SUCCESS;
 }
diff --git a/src/pjproject-2.6/pjlib/src/pj/ioqueue_epoll.c b/src/pjproject-2.6/pjlib/src/pj/ioqueue_epoll.c
index 3af7758..9865b9b 100644
--- a/src/pjproject-2.6/pjlib/src/pj/ioqueue_epoll.c
+++ b/src/pjproject-2.6/pjlib/src/pj/ioqueue_epoll.c
:
```

- **pjsip CVE-2018-1000098**

  Patch link: https://trac.pjsip.org/repos/ticket/2093

```
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -210,4 +210,12 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_5680_PATCH
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_5741_PATCH
+/*****************************************************************
+* 2021.08.12 同步https://trac.pjsip.org/repos/changeset/5741
+* Crash when parsing SDP with an invalid media format description
+*****************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_5741_PATCH
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjmedia/src/pjmedia/sdp.c b/src/pjproject-2.6/pjmedia/src/
index 0df0a8b..3e63ec6 100644
--- a/src/pjproject-2.6/pjmedia/src/pjmedia/sdp.c
+++ b/src/pjproject-2.6/pjmedia/src/pjmedia/sdp.c
@@ -1529,11 +1529,20 @@ PJ_DEF(pj_status_t) pjmedia_sdp_validate2(const pjmedia_sdp_sessi
              * RTC based programs sends "null" for instant messaging!
              */
            if (pj_isdigit(*m->desc.fmt[j].ptr)) {
+       #ifdef YEASTAR_CSQ_SYNC_PJSIP_5741_PATCH
+               unsigned long pt;
+               pj_status_t status = pj_strtoul3(&m->desc.fmt[j], &pt, 10);
+       #else
               unsigned pt = pj_strtoul(&m->desc.fmt[j]);
+       #endif

               /* Payload type is between 0 and 127.
                */
+       #ifdef YEASTAR_CSQ_SYNC_PJSIP_5741_PATCH
+               CHECK( status == PJ_SUCCESS && pt <= 127, PJMEDIA_SDP_EINPT);
+       #else
               CHECK( pt <= 127, PJMEDIA_SDP_EINPT);
+       #endif

               /* If port is not zero, then for each dynamic payload type, an
                * rtpmap attribute must be specified.
```

- **pjsip CVE-2018-1000099**

  Patch link: https://trac.pjsip.org/repos/changeset/5740

```
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -194,4 +194,12 @@
 #define YEASTAR_CBS_READ_PEM_FROM_MEMORY
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_5740_PATCH
+/**************************************************************
+* 2021.08.12 同步https://trac.pjsip.org/repos/changeset/5740
+* Crash when receiving SDP with invalid fmtp attribute
+**************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_5740_PATCH
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjmedia/src/pjmedia/sdp.c b/src/pjproject-2.6/pjmedia/src/pjmedia/sdp.c
index 711c854..d000aea 100644
--- a/src/pjproject-2.6/pjmedia/src/pjmedia/sdp.c
+++ b/src/pjproject-2.6/pjmedia/src/pjmedia/sdp.c
@@ -257,6 +257,10 @@ PJ_DEF(pj_status_t) pjmedia_sdp_attr_get_rtpmap( const pjmedia_sdp_attr *attr,
     PJ_ASSERT_RETURN(pj_strcmp2(&attr->name, "rtpmap")==0, PJ_EINVALIDOP);

     PJ_ASSERT_RETURN(attr->value.slen != 0, PJMEDIA_SDP_EINATTR);
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_5740_PATCH
+       if (attr->value.slen == 0)
+               return PJMEDIA_SDP_EINATTR;
+#endif

     init_sdp_parser();

@@ -341,6 +345,10 @@ PJ_DEF(pj_status_t) pjmedia_sdp_attr_get_fmtp( const pjmedia_sdp_attr *attr,

     PJ_ASSERT_RETURN(pj_strcmp2(&attr->name, "fmtp")==0, PJ_EINVALIDOP);

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_5740_PATCH
+       if (attr->value.slen == 0)
+               return PJMEDIA_SDP_EINATTR;
+#endif
     /* fmtp BNF:
      * a=fmtp:<format> <format specific parameter>
      */
@@ -379,6 +387,10 @@ PJ_DEF(pj_status_t) pjmedia_sdp_attr_get_rtcp(const pjmedia_sdp_attr *attr,

     PJ_ASSERT_RETURN(pj_strcmp2(&attr->name, "rtcp")==0, PJ_EINVALIDOP);

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_5740_PATCH
+       if (attr->value.slen == 0)
+               return PJMEDIA_SDP_EINATTR;
+#endif
     init_sdp_parser();
```

- **pjsip CVE-2021-37706**

  Patch link:

  https://github.com/pjsip/pjproject/commit/15663e3f37091069b8c98a7fce680dc04bc8e865

```
+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-37706
+/**************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/15663e3f37091069b8c98a7fce680dc04bc8e865
+* In affected versions if the incoming STUN message contains an ERROR-CODE attribute,
+* the header length is not checked before performing a subtraction operation,
+* potentially resulting in an integer underflow scenario
+**************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-37706
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjnath/src/pjnath/stun_msg.c b/src/pjproject-2.6/pjnath/src/pjnath/stun_msg.c
index a504f6f..1cbfa25 100644
--- a/src/pjproject-2.6/pjnath/src/pjnath/stun_msg.c
+++ b/src/pjproject-2.6/pjnath/src/pjnath/stun_msg.c
@@ -1760,7 +1760,12 @@ static pj_status_t decode_errcode_attr(pj_pool_t *pool,
     /* Get pointer to the string in the message */
     value.ptr = ((char*)buf + ATTR_HDR_LEN + 4);
     value.slen = attr->hdr.length - 4;
-
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-37706
+       /* Make sure the length is never negative */
+       if (value.slen < 0) {
+               value.slen = 0;
+       }
+#endif
     /* Copy the string to the attribute */
```

- **pjsip CVE-2021-41141**

  Patch link:

  https://github.com/pjsip/pjproject/commit/1aa2c0e0fb60a1b0bf793e0d834073ffe50fb196

```
GIT_RELEASE_PATH=/home/projects/git_appsoft/s_series/release
iff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
ndex 6adad7d..78193aa 100644
-- a/src/pjproject-2.6/pjlib/include/yeastar.h
++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@ -237,4 +237,13 @@
#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-37706
#endif

#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-41141
/*************************************************************
* 2022.10.25 https://github.com/pjsip/pjproject/commit/1aa2c0e0fb60a1b0bf793e0d834073ffe50fb196
* when error/failure occurs, it is found that the function returns without releasing the currently held
* This could result in a system deadlock
*************************************************************/
#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-41141
#endif

#endif
iff --git a/src/pjproject-2.6/pjmedia/src/pjmedia-codec/ipp_codecs.c b/src/pjproject-2.6/pjmedia/src/pjm
ndex f3e58c6..736cd7a 100644
-- a/src/pjproject-2.6/pjmedia/src/pjmedia-codec/ipp_codecs.c
++ b/src/pjproject-2.6/pjmedia/src/pjmedia-codec/ipp_codecs.c
@ -939,6 +939,9 @@ static pj_status_t ipp_alloc_codec( pjmedia_codec_factory *factory,
    }
    if (idx == -1) {
       *p_codec = NULL;
#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-41141
       pj_mutex_unlock(ipp_factory.mutex);
#endif
       return PJMEDIA_CODEC_EFAILED;
    }

iff --git a/src/pjproject-2.6/pjmedia/src/pjmedia-codec/opus.c b/src/pjproject-2.6/pjmedia/src/pjmedia-c
ndex 78d15bb..1ac09a0 100644
-- a/src/pjproject-2.6/pjmedia/src/pjmedia-codec/opus.c
++ b/src/pjproject-2.6/pjmedia/src/pjmedia-codec/opus.c
@ -679,6 +679,9 @@ static pj_status_t  codec_open( pjmedia_codec *codec,
                         OPUS_APPLICATION_VOIP);
    if (err != OPUS_OK) {
       PJ_LOG(2, (THIS_FILE, "Unable to create encoder"));
#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-41141
       pj_mutex_unlock (opus_data->mutex);
#endif
       return PJMEDIA_CODEC_EFAILED;
    }

@ -723,6 +726,9 @@ static pj_status_t  codec_open( pjmedia_codec *codec,
                          attr->info.channel_cnt);
    if (err != OPUS_OK) {
       PJ_LOG(2, (THIS_FILE, "Unable to initialize decoder"));
#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-41141
       pj_mutex_unlock (opus_data->mutex);
#endif
       return PJMEDIA_CODEC_EFAILED;
    }

iff --git a/src/pjproject-2.6/pjmedia/src/pjmedia-codec/passthrough.c b/src/pjproject-2.6/pjmedia/src/pj
ndex 0c75691..7a9b192 100644
-- a/src/pjproject-2.6/pjmedia/src/pjmedia-codec/passthrough.c
++ b/src/pjproject-2.6/pjmedia/src/pjmedia-codec/passthrough.c
```

- **pjsip CVE-2021-43299**

  Patch link:

  https://github.com/pjsip/pjproject/commit/d979253c924a686fa511d705be1f3ad0c5b20337

```
-GIT_RELEASE_PATH=/home/projects/git_appsoft/s_series/release
diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index 78193aa..da45676 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -246,4 +246,13 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-41141
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+/*****************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/d979253c924a686fa511d705be1f3ad0c5b20337
+* An attacker-controlled 'filename' argument may cause a buffer overflow since it
+* is copied to a fixed-size stack buffer without any size validation
+*****************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c b/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist
index a215539..663b457 100644
--- a/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c
+++ b/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c
@@ -257,8 +257,14 @@ PJ_DEF(pj_status_t) pjmedia_wav_playlist_create(pj_pool_t *pool,
     /* Be sure all files exist */
     for (index=0; index<file_count; index++) {

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+       PJ_ASSERT_RETURN(file_list[index].slen >= 0, PJ_ETOOSMALL);
+       if (file_list[index].slen >= PJ_MAXPATH) {
+           return PJ_ENAMETOOLONG;
+       }
+#else
        PJ_ASSERT_RETURN(file_list[index].slen < PJ_MAXPATH, PJ_ENAMETOOLONG);
-
+#endif
        pj_memcpy(filename, file_list[index].ptr, file_list[index].slen);
        filename[file_list[index].slen] = '\0';

diff --git a/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c b/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
index b84c550..ddebe0d 100644
--- a/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
+++ b/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
@@ -1034,6 +1034,11 @@ PJ_DEF(pj_status_t) pjsua_player_create( const pj_str_t *filename,
     if (pjsua_var.player_cnt >= PJ_ARRAY_SIZE(pjsua_var.player))
        return PJ_ETOOMANY;

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+       if (filename->slen >= PJ_MAXPATH) {
+               return PJ_ENAMETOOLONG;
+       }
:
```

- **pjsip CVE-2021-43300**

  Patch link:

  https://github.com/pjsip/pjproject/commit/d979253c924a686fa511d705be1f3ad0c5b20337


```
-GIT_RELEASE_PATH=/home/projects/git_appsoft/s_series/release
diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index 78193aa..da45676 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -246,4 +246,13 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-41141
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+/*****************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/d979253c924a686fa511d705be1f3ad0c5b20337
+* An attacker-controlled 'filename' argument may cause a buffer overflow since it
+* is copied to a fixed-size stack buffer without any size validation
+*****************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c b/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist
index a215539..663b457 100644
--- a/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c
+++ b/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c
@@ -257,8 +257,14 @@ PJ_DEF(pj_status_t) pjmedia_wav_playlist_create(pj_pool_t *pool,
     /* Be sure all files exist */
     for (index=0; index<file_count; index++) {

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+       PJ_ASSERT_RETURN(file_list[index].slen >= 0, PJ_ETOOSMALL);
+       if (file_list[index].slen >= PJ_MAXPATH) {
+           return PJ_ENAMETOOLONG;
+       }
+#else
        PJ_ASSERT_RETURN(file_list[index].slen < PJ_MAXPATH, PJ_ENAMETOOLONG);
-
+#endif
        pj_memcpy(filename, file_list[index].ptr, file_list[index].slen);
        filename[file_list[index].slen] = '\0';

diff --git a/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c b/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
index b84c550..ddebe0d 100644
--- a/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
+++ b/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
@@ -1034,6 +1034,11 @@ PJ_DEF(pj_status_t) pjsua_player_create( const pj_str_t *filename,
     if (pjsua_var.player_cnt >= PJ_ARRAY_SIZE(pjsua_var.player))
        return PJ_ETOOMANY;

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+       if (filename->slen >= PJ_MAXPATH) {
+               return PJ_ENAMETOOLONG;
+       }
:
```

- **pjsip CVE-2021-43301**

  Patch link: https://github.com/pjsip/pjproject/security/advisories/GHSA-qcvw-h34v-c7r9

```
-GIT_RELEASE_PATH=/home/projects/git_appsoft/s_series/release
diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index 78193aa..da45676 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -246,4 +246,13 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-41141
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+/*************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/d979253c924a686fa511d705be1f3ad0c5b20337
+* An attacker-controlled 'filename' argument may cause a buffer overflow since it
+* is copied to a fixed-size stack buffer without any size validation
+*************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c b/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist
index a215539..663b457 100644
--- a/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c
+++ b/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c
@@ -257,8 +257,14 @@ PJ_DEF(pj_status_t) pjmedia_wav_playlist_create(pj_pool_t *pool,
     /* Be sure all files exist */
     for (index=0; index<file_count; index++) {

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+       PJ_ASSERT_RETURN(file_list[index].slen >= 0, PJ_ETOOSMALL);
+       if (file_list[index].slen >= PJ_MAXPATH) {
+           return PJ_ENAMETOOLONG;
+       }
+#else
        PJ_ASSERT_RETURN(file_list[index].slen < PJ_MAXPATH, PJ_ENAMETOOLONG);
-
+#endif
        pj_memcpy(filename, file_list[index].ptr, file_list[index].slen);
        filename[file_list[index].slen] = '\0';

diff --git a/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c b/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
index b84c550..ddebe0d 100644
--- a/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
+++ b/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
@@ -1034,6 +1034,11 @@ PJ_DEF(pj_status_t) pjsua_player_create( const pj_str_t *filename,
     if (pjsua_var.player_cnt >= PJ_ARRAY_SIZE(pjsua_var.player))
        return PJ_ETOOMANY;

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+       if (filename->slen >= PJ_MAXPATH) {
+               return PJ_ENAMETOOLONG;
+       }
:
```

- **pjsip CVE-2021-43302**

  Patch link: https://github.com/pjsip/pjproject/security/advisories/GHSA-qcvw-h34v-c7r9

```
-GIT_RELEASE_PATH=/home/projects/git_appsoft/s_series/release
diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index 78193aa..da45676 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -246,4 +246,13 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-41141
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+/***************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/d979253c924a686fa511d705be1f3ad0c5b20337
+* An attacker-controlled 'filename' argument may cause a buffer overflow since it
+* is copied to a fixed-size stack buffer without any size validation
+***************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c b/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist
index a215539..663b457 100644
--- a/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c
+++ b/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c
@@ -257,8 +257,14 @@ PJ_DEF(pj_status_t) pjmedia_wav_playlist_create(pj_pool_t *pool,
      /* Be sure all files exist */
     for (index=0; index<file_count; index++) {

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+        PJ_ASSERT_RETURN(file_list[index].slen >= 0, PJ_ETOOSMALL);
+        if (file_list[index].slen >= PJ_MAXPATH) {
+            return PJ_ENAMETOOLONG;
+        }
+#else
        PJ_ASSERT_RETURN(file_list[index].slen < PJ_MAXPATH, PJ_ENAMETOOLONG);
-
+#endif
        pj_memcpy(filename, file_list[index].ptr, file_list[index].slen);
        filename[file_list[index].slen] = '\0';

diff --git a/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c b/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
index b84c550..ddebe0d 100644
--- a/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
+++ b/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
@@ -1034,6 +1034,11 @@ PJ_DEF(pj_status_t) pjsua_player_create( const pj_str_t *filename,
     if (pjsua_var.player_cnt >= PJ_ARRAY_SIZE(pjsua_var.player))
        return PJ_ETOOMANY;

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+        if (filename->slen >= PJ_MAXPATH) {
+                return PJ_ENAMETOOLONG;
+        }
:
```

- **pjsip CVE-2021-43303**

Patch link: https://github.com/pjsip/pjproject/security/advisories/GHSA-qcvw-h34v-c7r9


```
-GIT_RELEASE_PATH=/home/projects/git_appsoft/s_series/release
diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index 78193aa..da45676 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -246,4 +246,13 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-41141
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+/***************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/d979253c924a686fa511d705be1f3ad0c5b20337
+* An attacker-controlled 'filename' argument may cause a buffer overflow since it
+* is copied to a fixed-size stack buffer without any size validation
+***************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c b/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist
index a215539..663b457 100644
--- a/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c
+++ b/src/pjproject-2.6/pjmedia/src/pjmedia/wav_playlist.c
@@ -257,8 +257,14 @@ PJ_DEF(pj_status_t) pjmedia_wav_playlist_create(pj_pool_t *pool,
      /* Be sure all files exist */
     for (index=0; index<file_count; index++) {

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+        PJ_ASSERT_RETURN(file_list[index].slen >= 0, PJ_ETOOSMALL);
+        if (file_list[index].slen >= PJ_MAXPATH) {
+            return PJ_ENAMETOOLONG;
+        }
+#else
        PJ_ASSERT_RETURN(file_list[index].slen < PJ_MAXPATH, PJ_ENAMETOOLONG);
-
+#endif
        pj_memcpy(filename, file_list[index].ptr, file_list[index].slen);
        filename[file_list[index].slen] = '\0';

diff --git a/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c b/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
index b84c550..ddebe0d 100644
--- a/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
+++ b/src/pjproject-2.6/pjsip/src/pjsua-lib/pjsua_aud.c
@@ -1034,6 +1034,11 @@ PJ_DEF(pj_status_t) pjsua_player_create( const pj_str_t *filename,
     if (pjsua_var.player_cnt >= PJ_ARRAY_SIZE(pjsua_var.player))
        return PJ_ETOOMANY;

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43299
+        if (filename->slen >= PJ_MAXPATH) {
+                return PJ_ENAMETOOLONG;
+        }
:
```


- **pjsip CVE-2021-43304**

Patch link:

https://github.com/pjsip/pjproject/commit/8b621f192cae14456ee0b0ade52ce6c6f258af1e

```
+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43804
+/*****************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/8b621f192cae14456ee0b0ade52ce6c6f258af1e
+* In affected versions if the incoming RTCP BYE message contains a reason's length,
+* this declared length is not checked against the actual received packet size,
+* potentially resulting in an out-of-bound read access.
+*****************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43804
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjmedia/src/pjmedia/rtcp.c b/src/pjproject-2.6/pjmedia/src/pjmedia/rtcp.c
index cf53c05..13f2093 100644
--- a/src/pjproject-2.6/pjmedia/src/pjmedia/rtcp.c
+++ b/src/pjproject-2.6/pjmedia/src/pjmedia/rtcp.c
@@ -753,6 +753,9 @@ static void parse_rtcp_bye(pjmedia_rtcp_session *sess,
     if (size > 8) {
         reason.slen = PJ_MIN(sizeof(sess->stat.peer_sdes_buf_),
                              *((pj_uint8_t*)pkt+8));
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43804
+        reason.slen = PJ_MIN(reason.slen, size-9);
+#endif
        pj_memcpy(sess->stat.peer_sdes_buf_, ((pj_uint8_t*)pkt+9),
```

- **pjsip CVE-2017-16872**

  Patch link:

  https://github.com/pjsip/pjproject/commit/f74c1fc22b760d2a24369aa72c74c4a9ab985859

```
+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43845
+/*****************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/f74c1fc22b760d2a24369aa72c74c4a9ab985859
+* if incoming RTCP XR message contain block, the data field is not checked against the received packet size,
+* potentially resulting in an out-of-bound read access.
+*****************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43845
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjmedia/src/pjmedia/rtcp_xr.c b/src/pjproject-2.6/pjmedia/src/pjmedia/rtcp_xr.c
index 1dcd286..313123e 100644
--- a/src/pjproject-2.6/pjmedia/src/pjmedia/rtcp_xr.c
+++ b/src/pjproject-2.6/pjmedia/src/pjmedia/rtcp_xr.c
@@ -436,16 +436,40 @@ void pjmedia_rtcp_xr_rx_rtcp_xr( pjmedia_rtcp_xr_session *sess,
         if (rb_len) {
             switch (rb_hdr->bt) {
                 case BT_RR_TIME:
+                #ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43845
+                        if ((char*)rb_hdr + sizeof(*rb_rr_time) <= (char*)pkt + size) {
+                                rb_rr_time = (pjmedia_rtcp_xr_rb_rr_time*)rb_hdr;
+                        }
+                #else
                     rb_rr_time = (pjmedia_rtcp_xr_rb_rr_time*) rb_hdr;
+                #endif
                     break;
                 case BT_DLRR:
+                #ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43845
+                        if ((char*)rb_hdr + sizeof(*rb_dlrr) <= (char*)pkt + size) {
+                                rb_dlrr = (pjmedia_rtcp_xr_rb_dlrr*)rb_hdr;
+                        }
+                #else
                     rb_dlrr = (pjmedia_rtcp_xr_rb_dlrr*) rb_hdr;
+                #endif
                     break;
                 case BT_STATS:
+                #ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43845
+                         if ((char*)rb_hdr + sizeof(*rb_stats) <= (char*)pkt + size) {
+                                rb_stats = (pjmedia_rtcp_xr_rb_stats*)rb_hdr;
+                        }
+                #else
                     rb_stats = (pjmedia_rtcp_xr_rb_stats*) rb_hdr;
+                #endif
                     break;
                 case BT_VOIP_METRICS:
+                #ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2021-43845
+                        if ((char*)rb_hdr + sizeof(*rb_voip_mtc) <= (char*)pkt + size) {
:
```

- **pjsip CVE-2022-21722**

  Patch link:

  https://github.com/pjsip/pjproject/commit/22af44e68a0c7d190ac1e25075e1382f77e9397a

```
+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21722
+/*****************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/22af44e68a0c7d190ac1e25075e1382f77
+* there are various cases where it is possible that certain incoming RTP/RTCP packets car
+*****************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21722
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjmedia/src/pjmedia/rtcp.c b/src/pjproject-2.6/pjmedia/src/
index 13f2093..9a748be 100644
--- a/src/pjproject-2.6/pjmedia/src/pjmedia/rtcp.c
+++ b/src/pjproject-2.6/pjmedia/src/pjmedia/rtcp.c
@@ -496,12 +496,26 @@ static void parse_rtcp_report( pjmedia_rtcp_session *sess,

     /* Parse RTCP */
     if (common->pt == RTCP_SR) {
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21722
+       if (sizeof (pjmedia_rtcp_common) + sizeof (pjmedia_rtcp_sr) > size) {
+               TRACE_((sess->name, "Discarding RTCP SR due to truncated size "
+                                   "%d bytes", size));
+               return;
+       }
+#endif
        sr = (pjmedia_rtcp_sr*) (((char*)pkt) + sizeof(pjmedia_rtcp_common));
        if (common->count > 0 && size >= (sizeof(pjmedia_rtcp_sr_pkt))) {
           rr = (pjmedia_rtcp_rr*)(((char*)pkt) + (sizeof(pjmedia_rtcp_common)
                                + sizeof(pjmedia_rtcp_sr)));
        }
     } else if (common->pt == RTCP_RR && common->count > 0) {
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21722
+       if (sizeof (pjmedia_rtcp_common) + sizeof (pjmedia_rtcp_rr) > size) {
+               TRACE_((sess->name, "Discarding RTCP RR due to truncated size "
+                                   "%d bytes", size));
+               return;
+       }
+#endif
        rr = (pjmedia_rtcp_rr*)(((char*)pkt) + sizeof(pjmedia_rtcp_common));
 #if defined(PJMEDIA_HAS_RTCP_XR) && (PJMEDIA_HAS_RTCP_XR != 0)
     } else if (common->pt == RTCP_XR) {
@@ -776,10 +790,27 @@ PJ_DEF(void) pjmedia_rtcp_rx_rtcp( pjmedia_rtcp_session *sess,
     p = (pj_uint8_t*)pkt;
     p_end = p + size;
     while (p < p_end) {
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21722
+       pjmedia_rtcp_common *common = NULL;
+#else
        pjmedia_rtcp_common *common = (pjmedia_rtcp_common*)p;
+#endif
        unsigned len;

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21722
+       if (p + sizeof(pjmedia_rtcp_common) > p_end) {
+               TRACE_((sess->name, "Receiving truncated RTCP packet (1)"));
+               break;
+       }
+       common = (pjmedia_rtcp_common*)p;
+#endif
       len = (pj_ntohs((pj_uint16_t)common->length)+1) * 4;
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21722
+       if (p + len > p_end) {
+               TRACE_((sess->name, "Receiving truncated RTCP packet (2)"));
```

- **pjsip CVE-2022-21723**

  Patch link:

  https://github.com/pjsip/pjproject/commit/077b465c33f0aec05a49cd2ca456f9a1b112e896

```
index a8c939d..efdb555 100644
--- a/src/pjproject-2.6/pjlib-util/src/pjlib-util/scanner.c
+++ b/src/pjproject-2.6/pjlib-util/src/pjlib-util/scanner.c
@@ -441,16 +441,35 @@ PJ_DEF(void) pj_scan_get_n( pj_scanner *scanner,

 PJ_DEF(int) pj_scan_get_char( pj_scanner *scanner )
 {
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21723
+        register char *s = scanner->curptr;
+        int chr;
+#else
     int chr = *scanner->curptr;
+#endif

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21723
+        if (s >= scanner->end || !*s) {
+#else
     if (!chr) {
+#endif
        pj_scan_syntax_err(scanner);
        return 0;
     }

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21723
+        chr = *s;
+#else
     ++scanner->curptr;
+#endif

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21723
+        ++s;
+        scanner->curptr = s;
+        if (PJ_SCAN_CHECK_EOF(s) && PJ_SCAN_IS_PROBABLY_SPACE(*s) && scanner->skip_ws) {
+#else
     if (PJ_SCAN_IS_PROBABLY_SPACE(*scanner->curptr) && scanner->skip_ws) {
+#endif
        pj_scan_skip_whitespace(scanner);
     }
     return chr;
diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index b4e570a..5930843 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -282,4 +282,12 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21722
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21723
+/*************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/077b465c33f0aec05a49cd2ca456f9a1b112e896
+* parsing an incoming SIP message that contains a malformed multipart can potentially cause out-of-bound read
+************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21723
```

- **pjsip CVE-2022-23608**

  Patch link:

  https://github.com/pjsip/pjproject/commit/db3235953baa56d2fb0e276ca510fefca751643f

```
+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-23608
+/*****************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/db3235953baa56d2fb0e276ca
+* when in a dialog set (or forking) scenario, a hash key shared by multiple UAC
+* The issue may cause a dialog set to be registered in the hash table multiple t
+*****************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-23608
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjsip/src/pjsip/sip_ua_layer.c b/src/pjproject-2.6
index d1a4d2a..999af85 100644
--- a/src/pjproject-2.6/pjsip/src/pjsip/sip_ua_layer.c
+++ b/src/pjproject-2.6/pjsip/src/pjsip/sip_ua_layer.c
@@ -64,7 +64,10 @@ struct dlg_set

     /* This is the buffer to store this entry in the hash table. */
     pj_hash_entry_buf ht_entry;
-
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-23608
+        /* Entry key in the hash table */
+        pj_str_t ht_key;
+#endif
     /* List of dialog in this dialog set. */
     struct dlg_set_head  dlg_list;
 };
@@ -321,17 +324,24 @@ PJ_DEF(pj_status_t) pjsip_ua_register_dlg( pjsip_user_agent
          * Create the dialog set and add this dialog to it.
          */
         dlg_set = alloc_dlgset_node();
+       #ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-23608
+               dlg_set->ht_key = dlg->local.info->tag;
+       #endif
        pj_list_init(&dlg_set->dlg_list);
        pj_list_push_back(&dlg_set->dlg_list, dlg);

        dlg->dlg_set = dlg_set;

        /* Register the dialog set in the hash table. */
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-23608
+              pj_hash_set_np_lower(mod_ua.dlg_table, dlg_set->ht_key.ptr, (unsi
+#else
:
```

- **pjsip CVE-2022-24754**

  Patch link:

  https://github.com/pjsip/pjproject/commit/d27f79da11df7bc8bb56c2f291d71e54df8d2c47

```
root@yeastar1-B250M-D2V:/home/k2/ipv6/pjsip# git diff src/pjproject-2.6/pjlib/include/yeastar.h
diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index 233ac16..8d7025a 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -326,4 +326,13 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-31031
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24754
+/*****************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/d27f79da11df7bc8bb56c2f291d71e54df8d2c47
+* a stack buffer overflow vulnerability affects PJSIP users that use STUN in their applications,
+* either by: setting a STUN server in their account/media config in PJSUA/PJSUA2 level, or directly usi
+*****************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_ CVE-2022-24754
+#endif
+
```

- **pjsip CVE-2022-24763**

  Patch link:

  https://github.com/pjsip/pjproject/commit/856f87c2e97a27b256482dbe0d748b1194355a21

```
-GIT_RELEASE_PATH=/home/projects/git_appsoft/s_series/release
diff --git a/src/pjproject-2.6/pjlib-util/src/pjlib-util/xml.c b/src/pjproject-2.6/pjlib-util/src/pjlib-util/xml.c
index 3d4d16f..b1c900b 100644
--- a/src/pjproject-2.6/pjlib-util/src/pjlib-util/xml.c
+++ b/src/pjproject-2.6/pjlib-util/src/pjlib-util/xml.c
@@ -150,6 +150,9 @@ static pj_xml_node *xml_parse_node( pj_pool_t *pool, pj_scanner *scanner)
        pj_scan_get_until_ch(scanner, ']', &node->content);
        while (pj_scan_strcmp(scanner, "]]>", 3)) {
            pj_str_t dummy;
+       #ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24763
+               pj_scan_advance_n(scanner, 1, PJ_FALSE);
+       #endif
            pj_scan_get_until_ch(scanner, ']', &dummy);
        }
        node->content.slen = scanner->curptr - node->content.ptr;
diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index 5930843..dfb0214 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -290,4 +290,13 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-21723
 #endif


+
+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24763
+/*************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/856f87c2e97a27b256482dbe0d748b1194355a21
+* contain a denial-of-service vulnerability that affects PJSIP users that consume PJSIP's XML parsing in their apps.
+*************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24763
+#endif
+
 #endif
root@yeastar1_B250M_D2V:/home/k2/ipv6/pjsip#
```

- **pjsip CVE-2022-24764**

  Patch link: https://trac.pjsip.org/repos/changeset/5740

```
+
+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24764
+/*************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/560a1346f87aabe126509bb24930106dea292b00
+* a stack buffer overflow vulnerability that affects PJSUA2 users or users that call the API `pjm
+* Applications that do not use PJSUA2 and do not directly call `pjmedia_sdp_print()` or `pjmedia_
+*************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24764
+#endif
+
 #endif
diff --git a/src/pjproject-2.6/pjmedia/src/pjmedia/sdp.c b/src/pjproject-2.6/pjmedia/src/pjmedia/s
index 3e63ec6..4f56d21 100644
--- a/src/pjproject-2.6/pjmedia/src/pjmedia/sdp.c
+++ b/src/pjproject-2.6/pjmedia/src/pjmedia/sdp.c
@@ -650,12 +650,30 @@ static int print_media_desc( pjmedia_sdp_media *m, char *buf, int len)
     pj_memcpy(p, m->desc.transport.ptr, m->desc.transport.slen);
     p += m->desc.transport.slen;
     for (i=0; i<m->desc.fmt_count; ++i) {
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24764
+       if (end-p > m->desc.fmt[i].slen) {
+               *p++ = ' ';
+               pj_memcpy(p, m->desc.fmt[i].ptr, m->desc.fmt[i].slen);
+               p += m->desc.fmt[i].slen;
+       } else {
+               return -1;
+       }
+}
+
+       if (end-p >= 2) {
+               *p++ = '\r';
+               *p++ = '\n';
+       } else {
+               return -1;
+       }
+#else
        *p++ = ' ';
        pj_memcpy(p, m->desc.fmt[i].ptr, m->desc.fmt[i].slen);
        p += m->desc.fmt[i].slen;
     }
     *p++ = '\r';
     *p++ = '\n';
:
```

- **pjsip CVE-2022-24786**

  Patch link:

  https://github.com/pjsip/pjproject/commit/11559e49e65bdf00922ad5ae28913ec6a198d508

```
+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24786
+/************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/11559e49e65bdf00922ad5ae28913ec6a198d508
+* do not parse incoming RTCP feedback RPSI (Reference Picture Selection Indication) packet,
+* but any app that directly uses pjmedia_rtcp_fb_parse_rpsi() will be affected.
+************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24786
+#endif
 #endif
diff --git a/src/pjproject-2.6/pjmedia/include/pjmedia/rtcp.h b/src/pjproject-2.6/pjmedia/include/pjmedia/rtcp.h
index 6584f63..2c30ee7 100644
--- a/src/pjproject-2.6/pjmedia/include/pjmedia/rtcp.h
+++ b/src/pjproject-2.6/pjmedia/include/pjmedia/rtcp.h
@@ -225,6 +225,18 @@ typedef struct pjmedia_rtcp_stat
 } pjmedia_rtcp_stat;


+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24786
+/**
+ * RTCP feedback common header.
+ */
+typedef struct pjmedia_rtcp_fb_common
+{
+    pjmedia_rtcp_common rtcp_common;
+    pj_uint32_t             ssrc_src;   /**< SSRC media source      */
+} pjmedia_rtcp_fb_common;
+#endif
+
+
 /**
  * RTCP session is used to monitor the RTP session of one endpoint. There
  * should only be one RTCP session for a bidirectional RTP streams.
@@ -234,7 +246,9 @@ typedef struct pjmedia_rtcp_session
    char                  *name;       /**< Name identification.        */
    pjmedia_rtcp_sr_pkt          rtcp_sr_pkt;/**< Cached RTCP SR packet.        */
    pjmedia_rtcp_rr_pkt          rtcp_rr_pkt;/**< Cached RTCP RR packet.        */
-
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24786
+       pjmedia_rtcp_fb_common  rtcp_fb_com;/**< Cached RTCP feedback common header packet.*/
+#endif
    pjmedia_rtp_seq_session seq_ctrl;  /**< RTCP sequence number control.  */
    unsigned              rtp_last_ts;/**< Last timestamp in RX RTP pkt.  */
:
```

- **pjsip CVE-2022-24792**

  Patch link:

  https://github.com/pjsip/pjproject/commit/947bc1ee6d05be10204b918df75a503415fd3213

```
-GIT_RELEASE_PATH=/home/projects/git_appsoft/s_series/release
diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index 233ac16..7ae99d9 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -326,4 +326,12 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-31031
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24792
+/****************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/947bc1ee6d05be10204b918df75a503415fd3213
+* A denial-of-service vulnerability affects applications on a 32-bit systems that use PJSIP versions 2
31-bit integers. The vulnerability does not affect 64-bit apps and should not affect apps that only pla
+***************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_ CVE-2022-24792
+#endif
+
 #endif
root@yeastar1_B250M_D2V:/home/k2/ipv6/pjsip#
```

- **pjsip CVE-2022-24793**

  Patch link:

  https://github.com/pjsip/pjproject/commit/9fae8f43accef8ea65d4a8ae9cdf297c46cfe29a

```
+GIT_RELEASE_PATH=/home/projects/git_appsort/s_series/release
diff --git a/src/pjproject-2.6/pjlib-util/src/pjlib-util/dns.c b/src/pjproject-2.6/pjlib-util/src/pjlib-util/dns.c
index d7736c9..331cbce 100644
--- a/src/pjproject-2.6/pjlib-util/src/pjlib-util/dns.c
+++ b/src/pjproject-2.6/pjlib-util/src/pjlib-util/dns.c
@@ -160,7 +160,17 @@ static pj_status_t get_name_len(int rec_counter, const pj_uint8_t *pkt,
            unsigned label_len = *p;

            /* Check that label length is valid */
+       #ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24793
+                /* Check that label length is valid.
+            * Each label consists of an octet length (of size 1) followed
+            * by the octet of the specified length (label_len). Then it
+            * must be followed by either another label's octet length or
+            * a zero length octet (that terminates the sequence).
+            */
+                if (p+1+label_len+1 > max)
+       #else
            if (pkt+label_len > max)
+       #endif
                return PJLIB_UTIL_EDNSINNAMEPTR;

            p += (label_len + 1);
@@ -223,7 +233,17 @@ static pj_status_t get_name(int rec_counter, const pj_uint8_t *pkt,
            unsigned label_len = *p;

            /* Check that label length is valid */
+       #ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24793
+                 /* Check that label length is valid.
+            * Each label consists of an octet length (of size 1) followed
+            * by the octet of the specified length (label_len). Then it
+            * must be followed by either another label's octet length or
+            * a zero length octet (that terminates the sequence).
+            */
+                if (p+1+label_len+1 > max)
+       #else
            if (pkt+label_len > max)
+       #endif
                return PJLIB_UTIL_EDNSINNAMEPTR;

            pj_memcpy(name->ptr + name->slen, p+1, label_len);
@@ -234,9 +254,10 @@ static pj_status_t get_name(int rec_counter, const pj_uint8_t *pkt,
                *(name->ptr + name->slen) = '.';
                ++name->slen;
            }
-
+       #ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24793
            if (p >= max)
                return PJLIB_UTIL_EDNSINSIZE;
+       #endif
```

- **pjsip CVE-2022-31031**

  Patch link: https://trac.pjsip.org/repos/changeset/5740

```
diff --git a/src/pjproject-2.6/pjlib-util/src/pjlib-util/stun_simple.c b/src/pjproject-2.6/pjlib-util/src/pjlib-util/stun_simple.c
index bec8681..2b1f994 100644
--- a/src/pjproject-2.6/pjlib-util/src/pjlib-util/stun_simple.c
+++ b/src/pjproject-2.6/pjlib-util/src/pjlib-util/stun_simple.c
@@ -54,6 +54,9 @@ PJ_DEF(pj_status_t) pjstun_parse_msg( void *buf, pj_size_t buf_len,
 {
     pj_uint16_t msg_type, msg_len;
     char *p_attr;
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-31031
+       int attr_max_cnt = PJ_ARRAY_SIZE(msg->attr);
+#endif

     PJ_CHECK_STACK();

@@ -83,7 +86,11 @@ PJ_DEF(pj_status_t) pjstun_parse_msg( void *buf, pj_size_t buf_len,
     msg->attr_count = 0;
     p_attr = (char*)buf + sizeof(pjstun_msg_hdr);

+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-31031
+        while (msg_len > 0 && msg->attr_count < attr_max_cnt) {
+#else
     while (msg_len > 0) {
+#endif
        pjstun_attr_hdr **attr = &msg->attr[msg->attr_count];
        pj_uint32_t len;
        pj_uint16_t attr_type;
@@ -111,7 +118,11 @@ PJ_DEF(pj_status_t) pjstun_parse_msg( void *buf, pj_size_t buf_len,
        p_attr += len;
        ++msg->attr_count;
     }
-
+#ifdef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-31031
+       if (msg->attr_count == attr_max_cnt) {
+               PJ_LOG(4, (THIS_FILE, "Warning: max number attribute %d reached.", attr_max_cnt));
+       }
+#endif
     return PJ_SUCCESS;
 }

diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index 655e868..233ac16 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -316,4 +316,14 @@
 ****************************************************************/
 #define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-24793
 #endif
+
+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-31031
+/***************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/450baca94f475345542c6953832650c390889202
+* a stack buffer overflow vulnerability affects PJSIP users that use STUN in their applications,
+* either by: setting a STUN server in their account/media config in PJSUA/PJSUA2 level, or directly using `pjlib-util/stun_simple`
+****************************************************************/
:
```

- **pjsip CVE-2022-39244**

  Patch link:

  https://github.com/pjsip/pjproject/commit/c4d34984ec92b3d5252a7d5cddd85a1d3a8001ae

```
@@ -1 +0,0 @@
-GIT_RELEASE_PATH=/home/projects/git_appsoft/s_series/release
diff --git a/src/pjproject-2.6/pjlib/include/yeastar.h b/src/pjproject-2.6/pjlib/include/yeastar.h
index 233ac16..df8883c 100644
--- a/src/pjproject-2.6/pjlib/include/yeastar.h
+++ b/src/pjproject-2.6/pjlib/include/yeastar.h
@@ -326,4 +326,12 @@
 #define YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-31031
 #endif

+#ifndef YEASTAR_CSQ_SYNC_PJSIP_CVE-2022-39244
+/***************************************************************
+* 2022.10.25 https://github.com/pjsip/pjproject/commit/c4d34984ec92b3d5252a7d5cddd85a1d3a8001ae
+* the PJSIP parser, PJMEDIA RTP decoder, and PJMEDIA SDP parser are affeced by a buffer overflow vu
 master branch and will be included in releases 2.13 and later.
+**************************************************************/
+#define YEASTAR_CSQ_SYNC_PJSIP_ CVE-2022-39244
+#endif
+
 #endif
```

- **asterisk CVE-2021-32588**

  Patch link: http://downloads.asterisk.org/pub/security/AST-2021-008-13.diff

```
--- a/src/asterisk-13.7.0/channels/chan_iax2.c
+++ b/src/asterisk-13.7.0/channels/chan_iax2.c
@@ -4172,6 +4172,9 @@ static void __get_from_jb(const void *p)
        long ms;
        long next;
        struct timeval now = ast_tvnow();
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2021_32588
+       struct ast_format *voicefmt;
+#endif

        /* Make sure we have a valid private structure before going on */
        ast_mutex_lock(&iaxsl[callno]);
@@ -4191,10 +4194,16 @@ static void __get_from_jb(const void *p)

        ms = ast_tvdiff_ms(now, pvt->rxcore);

+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2021_32588
+       voicefmt = ast_format_compatibility_bitfield2format(pvt->voiceformat);
+       if (voicefmt && ms >= (next = jb_next(pvt->jb))) {
+               ret = jb_get(pvt->jb, &frame, ms, ast_format_get_default_ms(voicefmt));
+#else
        if(ms >= (next = jb_next(pvt->jb))) {
                struct ast_format *voicefmt;
                voicefmt = ast_format_compatibility_bitfield2format(pvt->voiceformat);
                ret = jb_get(pvt->jb, &frame, ms, voicefmt ? ast_format_get_default_ms(voicefmt) : 20);
+#endif
                switch(ret) {
                case JB_OK:
                        fr = frame.data;
@@ -6655,8 +6664,18 @@ static int decode_frame(ast_aes_decrypt_key *dcx, struct ast_iax2_full_hdr *fh,
                f->frametype = fh->type;
                if (f->frametype == AST_FRAME_VIDEO) {
                        f->subclass.format = ast_format_compatibility_bitfield2format(uncompress_subclass(fh->csub & ~
+               #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2021_32588
+                       if (!f->subclass.format) {
+                               f->subclass.format = ast_format_none;
+                       }
+               #endif
                } else if (f->frametype == AST_FRAME_VOICE) {
                        f->subclass.format = ast_format_compatibility_bitfield2format(uncompress_subclass(fh->csub));
+               #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2021_32588
+                       if (!f->subclass.format) {
+                               f->subclass.format = ast_format_none;
+                       }
+               #endif
                } else {
                        f->subclass.integer = uncompress_subclass(fh->csub);
                }
@@ -10480,8 +10499,13 @@ static int socket_process_meta(int packet_len, struct ast_iax2_meta_hdr *meta, s
                } else if (iaxs[fr->callno]->voiceformat == 0) {
                        ast_log(LOG_WARNING, "Received trunked frame before first full voice frame\n");
                        iax2_vnak(fr->callno);
+       #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2021_32588
+               } else if ((f.subclass.format = ast_format_compatibility_bitfield2format(
+                                                       iaxs[fr->callno]->voiceformat))) {
+       #else
                } else {
                        f.subclass.format = ast_format_compatibility_bitfield2format(iaxs[fr->callno]->voiceformat);
+       #endif
                        f.datalen = len;
                        if (f.datalen >= 0) {
                                if (f.datalen)
@@ -10724,11 +10748,21 @@ static int socket_process_helper(struct iax2_thread *thread)
```

- **asterisk CVE-2021-26712**

  Patch link: https://downloads.asterisk.org/pub/security/AST-2021-003-13.diff

```
root@yeastar1-B250M-D2V:/home/k2/ipv6/astcore# git diff src/asterisk-13.7.0/res/res_rtp_asterisk.c
diff --git a/src/asterisk-13.7.0/res/res_rtp_asterisk.c b/src/asterisk-13.7.0/res/res_rtp_asterisk.c
index 971168f..7d85c88 100644
--- a/src/asterisk-13.7.0/res/res_rtp_asterisk.c
+++ b/src/asterisk-13.7.0/res/res_rtp_asterisk.c
@@ -117,6 +117,9 @@ enum strict_rtp_state {
 };

 #define DEFAULT_STRICT_RTP STRICT_RTP_CLOSED
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2021_26712
+#define DEFAULT_SRTP_REPLAY_PROTECTION 1
+#endif
 #define DEFAULT_ICESUPPORT 1

 extern struct ast_srtp_res *res_srtp;
@@ -139,6 +142,9 @@ static int nochecksums;
 #endif
 static int strictrtp = DEFAULT_STRICT_RTP; /*< Only accept RTP frames from a defined source. If we rec
 static int learning_min_sequential = DEFAULT_LEARNING_MIN_SEQUENTIAL; /*< Number of sequential RTP fra
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2021_26712
+static int srtp_replay_protection = DEFAULT_SRTP_REPLAY_PROTECTION;
+#endif
 #ifdef HAVE_PJPROJECT
 static int icesupport = DEFAULT_ICESUPPORT;
 static struct sockaddr_in stunaddr;
@@ -2334,7 +2340,11 @@ static int __rtp_recvfrom(struct ast_rtp_instance *instance, void *buf, size_t s
        }
 #endif

+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2021_26712
+       if ((*in & 0xC0) && res_srtp && srtp && res_srtp->unprotect(srtp, buf, &len, (rtcp || rtcp_mux(
+#else
        if ((*in & 0xC0) && res_srtp && srtp && res_srtp->unprotect(srtp, buf, &len, rtcp) < 0) {
+#endif
           return -1;
        }

@@ -6171,6 +6181,9 @@ static int rtp_reload(int reload)
        dtmftimeout = DEFAULT_DTMF_TIMEOUT;
        strictrtp = DEFAULT_STRICT_RTP;
        learning_min_sequential = DEFAULT_LEARNING_MIN_SEQUENTIAL;
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2021_26712
+       srtp_replay_protection = DEFAULT_SRTP_REPLAY_PROTECTION;
+#endif

        /** This resource is not "reloaded" so much as unloaded and loaded again.
         * In the case of the TURN related variables, the memory referenced by a
@@ -6238,6 +6251,11 @@ static int rtp_reload(int reload)
                                DEFAULT_LEARNING_MIN_SEQUENTIAL);
                        }
                }
+       #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2021_26712
+               if ((s = ast_variable_retrieve(cfg, "general", "srtpreplayprotection"))) {
+               srtp_replay_protection = ast_true(s);
+       }
+       #endif
 #ifdef HAVE_PJPROJECT
                if ((s = ast_variable_retrieve(cfg, "general", "icesupport"))) {
                        icesupport = ast_true(s);
root@yeastar1-B250M-D2V:/home/k2/ipv6/astcore# 
```

- **asterisk CVE-2019-18610**

  Patch link: http://downloads.asterisk.org/pub/security/AST-2019-007-13.diff

```
index ecbe576..3a9f5ae 100644
--- a/src/asterisk-13.7.0/main/manager.c
+++ b/src/asterisk-13.7.0/main/manager.c
@@ -5807,6 +5807,9 @@ static int action_originate(struct mansession *s, const struct message *m)
                                                 EAGI(/bin/rm,-rf /)       */
                        strcasestr(app, "mixmonitor") ||  /* MixMonitor(blah,,rm -rf)  */
                        strcasestr(app, "externalivr") || /* ExternalIVR(rm -rf)       */
+               #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2019_18610
+                       strcasestr(app, "originate") ||   /* Originate(Local/1234,app,System,rm -rf) */
+               #endif
                        (strstr(appdata, "SHELL") && (bad_appdata = 1)) ||       /* NoOp(${SHELL(rm -rf /)})  */
                        (strstr(appdata, "EVAL") && (bad_appdata = 1))           /* NoOp(${EVAL(${some_var_containing_SHELL})}) */
                        )) {
root@yeastar1-B250M-D2V:/home/k2/ipv6/astcore#
root@yeastar1-B250M-D2V:/home/k2/ipv6/astcore#
```

- **asterisk CVE-2019-18976**

  Patch link: http://downloads.asterisk.org/pub/security/AST-2019-008-13.diff

```
diff --git a/src/asterisk-13.7.0/res/res_pjsip_session.c b/src/asterisk-13.7.0/res/res_pjsip_session.c
index 60b0405..5021b58 100644
--- a/src/asterisk-13.7.0/res/res_pjsip_session.c
+++ b/src/asterisk-13.7.0/res/res_pjsip_session.c
@@ -263,6 +263,14 @@ static int handle_incoming_sdp(struct ast_sip_session *session, const pjmedia_sd
                        continue;
                }
 #endif
+       #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2019_18976
+               /* If we have a port of 0, ignore this stream */
+               if (!sdp->media[i]->desc.port) {
+                       ast_debug(1, "Declining incoming SDP media stream '%s' at position '%d'\n",
+                               session_media->stream_type, i);
+                       continue;
+               }
+       #endif
```

- **asterisk CVE-2021-15639**

  Patch link: http://downloads.asterisk.org/pub/security/AST-2019-005-13.diff

```
root@yeastar1-B250M-D2V:/home/k2/ipv6/astcore/src/asterisk-13.7.0/main#
root@yeastar1-B250M-D2V:/home/k2/ipv6/astcore/src/asterisk-13.7.0/main# git diff translate.c
diff --git a/src/asterisk-13.7.0/main/translate.c b/src/asterisk-13.7.0/main/translate.c
index 4b9ffe6..67eca84 100644
--- a/src/asterisk-13.7.0/main/translate.c
+++ b/src/asterisk-13.7.0/main/translate.c
@@ -413,7 +413,14 @@ static int framein(struct ast_trans_pvt *pvt, struct ast_frame *f)
        pvt->f.seqno = f->seqno;

        if (f->samples == 0) {
-               ast_log(LOG_WARNING, "no samples for %s\n", pvt->t->name);
+       #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2019_15639
+               /* Do not log empty audio frame */
+               if (!f->src || strcasecmp(f->src, "ast_prod"))
+       #endif
+                       ast_log(LOG_WARNING, "no samples for %s\n", pvt->t->name);
+       #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2019_15639
+               }
+       #endif
        }
        if (pvt->t->buffer_samples) {   /* do not pass empty frames to callback */
               if (f->datalen == 0) { /* perform native PLC if available */
```

- **asterisk CVE-2018-17281**

  Patch link: http://downloads.asterisk.org/pub/security/AST-2018-009-13.diff

```
+++ b/src/asterisk-13.7.0/res/res_http_websocket.c
@@ -718,7 +718,12 @@ static void websocket_bad_request(struct ast_tcptls_session_instance *ser)
 int AST_OPTIONAL_API_NAME(ast_websocket_uri_cb)(struct ast_tcptls_session_instance *ser, const struct ast_http_uri *urih, const char *ur
 {
        struct ast_variable *v;
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2018_17281
+       const char *upgrade = NULL, *key = NULL, *key1 = NULL, *key2 = NULL, *protos = NULL;
+       char *requested_protocols = NULL, *protocol = NULL;
+#else
        char *upgrade = NULL, *key = NULL, *key1 = NULL, *key2 = NULL, *protos = NULL, *requested_protocols = NULL, *protocol = NULL;
+#endif
        int version = 0, flags = 1;
        struct ast_websocket_protocol *protocol_handler = NULL;
        struct ast_websocket *session;
@@ -737,16 +742,35 @@ int AST_OPTIONAL_API_NAME(ast_websocket_uri_cb)(struct ast_tcptls_session_instan
        /* Get the minimum headers required to satisfy our needs */
        for (v = headers; v; v = v->next) {
                if (!strcasecmp(v->name, "Upgrade")) {
+               #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2018_17281
+                       upgrade = v->value;
+               #else
                        upgrade = ast_strip(ast_strdupa(v->value));
+               #endif
                } else if (!strcasecmp(v->name, "Sec-WebSocket-Key")) {
+               #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2018_17281
+                       key = v->value;
+               #else
                        key = ast_strip(ast_strdupa(v->value));
+               #endif
                } else if (!strcasecmp(v->name, "Sec-WebSocket-Key1")) {
+               #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2018_17281
+                       key1 = v->value;
+               #else
                        key1 = ast_strip(ast_strdupa(v->value));
+               #endif
                } else if (!strcasecmp(v->name, "Sec-WebSocket-Key2")) {
+               #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2018_17281
+                       key2 = v->value;
+               #else
                        key2 = ast_strip(ast_strdupa(v->value));
+               #endif
                } else if (!strcasecmp(v->name, "Sec-WebSocket-Protocol")) {
+               #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2018_17281
+               #else
                        requested_protocols = ast_strip(ast_strdupa(v->value));
                        protos = ast_strdupa(requested_protocols);
+               #endif
                } else if (!strcasecmp(v->name, "Sec-WebSocket-Version")) {
                        if (sscanf(v->value, "%30d", &version) != 1) {
                                version = 0;
@@ -760,7 +784,11 @@ int AST_OPTIONAL_API_NAME(ast_websocket_uri_cb)(struct ast_tcptls_session_instan
                        ast_sockaddr_stringify(&ser->remote_address));
                ast_http_error(ser, 426, "Upgrade Required", NULL);
                return 0;
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2018_17281
+       } else if (ast_strlen_zero(protos)) {
+#else
        } else if (ast_strlen_zero(requested_protocols)) {
+#endif
                /* If there's only a single protocol registered, and the
                 * client doesn't specify what protocol it's using, go ahead
                 * and accept the connection */
@@ -781,10 +809,20 @@ int AST_OPTIONAL_API_NAME(ast_websocket_uri_cb)(struct ast_tcptls_session_instan
                return 0;
```

- **asterisk CVE-2018-7284**

  Patch link: http://downloads.asterisk.org/pub/security/AST-2018-004-13.diff

```
index fb6aef6..7908de4 100644
--- a/src/asterisk-13.7.0/res/res_pjsip_pubsub.c
+++ b/src/asterisk-13.7.0/res/res_pjsip_pubsub.c
@@ -681,10 +681,17 @@ static struct ast_sip_pubsub_body_generator *subscription_get_generator_from_rda
        char accept[AST_SIP_MAX_ACCEPT][64];
        size_t num_accept_headers = 0;

+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2018_7284
+       while ((accept_header = pjsip_msg_find_hdr(rdata->msg_info.msg, PJSIP_H_ACCEPT, accept_header->next)) && (num_accept_headers < AST_SIP_MAX_ACCEPT))
+#else
        while ((accept_header = pjsip_msg_find_hdr(rdata->msg_info.msg, PJSIP_H_ACCEPT, accept_header->next))) {
+#endif
                int i;
-
+       #ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2018_7284
+               for (i = 0; i < accept_header->count && num_accept_headers < AST_SIP_MAX_ACCEPT; ++i) {
+       #else
                for (i = 0; i < accept_header->count; ++i) {
+       #endif
                        if (!exceptional_accept(&accept_header->values[i])) {
                                ast_copy_pj_str(accept[num_accept_headers], &accept_header->values[i], sizeof(accept[num_accept_headers]));
                                ++num_accept_headers;
root@yeastar1-B250M-D2V:/home/k2/ipv6/astcore#
```

- **asterisk CVE-2017-17090**

  Patch link: http://downloads.asterisk.org/pub/security/AST-2017-013-13.diff

```
root@yeastar1-B250M-D2V:/home/k2/ipv6/astcore# git diff src/asterisk-13.7.0/channels/chan_skinny.c
diff --git a/src/asterisk-13.7.0/channels/chan_skinny.c b/src/asterisk-13.7.0/channels/chan_skinny.c
index 5cdfe1b..dbafb88 100644
--- a/src/asterisk-13.7.0/channels/chan_skinny.c
+++ b/src/asterisk-13.7.0/channels/chan_skinny.c
@@ -7413,6 +7413,11 @@ static void destroy_session(struct skinnysession *s)
        }
        ast_mutex_unlock(&s->lock);
        ast_mutex_destroy(&s->lock);
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27452
+       if (s->t != AST_PTHREADT_NULL) {
+               pthread_detach(s->t);
+       }
+#endif
        ast_free(s);
 }

@@ -7497,10 +7502,12 @@ static void *skinny_session(void *data)
        int eventmessage = 0;
        struct pollfd fds[1];

+#ifndef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27452
        if (!s) {
               ast_log(LOG_WARNING, "Bad Skinny Session\n");
               return 0;
        }
+#endif

        ast_log(LOG_NOTICE, "Starting Skinny session from %s\n", ast_inet_ntoa(s->sin.sin_addr));

@@ -7662,6 +7669,9 @@ static void *accept_thread(void *ignore)
               s->keepalive_timeout_sched = -1;

               if (ast_pthread_create(&s->t, NULL, skinny_session, s)) {
+              #ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27452
+                      s->t = AST_PTHREADT_NULL;
+              #endif
                      destroy_session(s);
               }
        }
root@yeastar1-B250M-D2V:/home/k2/ipv6/astcore#
```

- **asterisk CVE-2017-16671**

Patch link: http://downloads.asterisk.org/pub/security/AST-2017-010-13.diff

```
diff --git a/src/asterisk-13.7.0/main/cdr.c b/src/asterisk-13.7.0/main/cdr.c
index 023ff6f..8b03e9c 100755
--- a/src/asterisk-13.7.0/main/cdr.c
+++ b/src/asterisk-13.7.0/main/cdr.c
@@ -5184,7 +5184,11 @@ static int cdr_object_update_party_b_userfield_cb(void *obj, void *arg, int flag
                }
                if (it_cdr->party_b.snapshot
                        && !strcasecmp(it_cdr->party_b.snapshot->name, info->channel_name)) {
+               #ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27337
+                       ast_copy_string(it_cdr->party_b.userfield, info->userfield, sizeof(it_cdr->party_b.userfield));
+               #else
                        strcpy(it_cdr->party_b.userfield, info->userfield);
+               #endif
                }
        }
        return 0;
@@ -5206,8 +5210,8 @@ void ast_cdr_setuserfield(const char *channel_name, const char *userfield)
                        if (it_cdr->fn_table == &finalized_state_fn_table) {
                                continue;
                        }
-               #ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_26897
-                       ast_copy_string(it_cdr->party_a.userfield, userfield, AST_MAX_USER_FIELD);
+               #ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27337
+                       ast_copy_string(it_cdr->party_a.userfield, userfield, sizeof(it_cdr->party_a.userfield));
                #else
                        strcpy(it_cdr->party_a.userfield, userfield);
                #endif
```

- **asterisk CVE-2017-14603**

Patch link: https://issues.asterisk.org/jira/browse/ASTERISK-27274

```
        STRICT_RTP_OPEN = 0, /*! No RTP packets should be dropped, all source
        STRICT_RTP_LEARN,    /*! Accept next packet as source */
        STRICT_RTP_CLOSED,   /*! Drop all RTP packets not coming from source
};

#ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27274
#define STRICT_RTP_LEARN_TIMEOUT        1500    /*!< milliseconds */
#define DEFAULT_STRICT_RTP -1   /*!< Enabled */
#else
#define DEFAULT_STRICT_RTP STRICT_RTP_CLOSED
#endif
#define DEFAULT_ICESUPPORT 1

extern struct ast_srtp_res *res_srtp;
```

- **asterisk CVE-2017-14100**

Patch link: http://downloads.asterisk.org/pub/security/AST-2017-005-13.diff

```
diff --git a/src/asterisk-13.7.0/apps/app_minivm.c b/src/asterisk-13.7.0/apps/app_minivm.c
index 45d04d8..3d22806 100644
--- a/src/asterisk-13.7.0/apps/app_minivm.c
+++ b/src/asterisk-13.7.0/apps/app_minivm.c
@@ -1757,11 +1757,39 @@ static int play_record_review(struct ast_channel *chan, char *playfile, char *re
 /*! \brief Run external notification for voicemail message */
 static void run_externnotify(struct ast_channel *chan, struct minivm_account *vmu)
 {
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2017_14100
+       char fquser[AST_MAX_CONTEXT * 2];
+       char *argv[5] = { NULL };
+       struct ast_party_caller *caller;
+       char *cid;
+       int idx;
+#else
        char arguments[BUFSIZ];
+#endif

        if (ast_strlen_zero(vmu->externnotify) && ast_strlen_zero(global_externnotify))
                return;

+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_CVE_2017_14100
+       snprintf(fquser, sizeof(fquser), "%s@%s", vmu->username, vmu->domain);
+       caller = ast_channel_caller(chan);
+       idx = 0;
+       argv[idx++] = ast_strlen_zero(vmu->externnotify) ? global_externnotify : vmu->externnotify;
+       argv[idx++] = fquser;
+       cid = S_COR(caller->id.name.valid, caller->id.name.str, NULL);
+       if (cid) {
+               argv[idx++] = cid;
+       }
+       cid = S_COR(caller->id.number.valid, caller->id.number.str, NULL);
+       if (cid) {
+               argv[idx++] = cid;
+       }
+       argv[idx] = NULL;
+
+       ast_debug(1, "Executing: %s %s %s %s\n",
+               argv[0], argv[1], argv[2] ?: "", argv[3] ?: "");
+       ast_safe_execvp(1, argv[0], argv);
+#else
        snprintf(arguments, sizeof(arguments), "%s %s@%s %s %s&",
                ast_strlen_zero(vmu->externnotify) ? global_externnotify : vmu->externnotify,
                vmu->username, vmu->domain,
@@ -1772,6 +1800,7 @@ static void run_externnotify(struct ast_channel *chan, struct minivm_account *vm

        ast_debug(1, "Executing: %s\n", arguments);
        ast_safe_system(arguments);
+#endif
 }
```

- **asterisk CVE-2017-14099**

  Patch link: http://downloads.asterisk.org/pub/security/AST-2017-005-13.diff

```
--- a/src/asterisk-13.7.0/res/res_rtp_asterisk.c
+++ b/src/asterisk-13.7.0/res/res_rtp_asterisk.c
@@ -201,6 +201,9 @@ static AST_LIST_HEAD_STATIC(ioqueues, ast_rtp_ioqueue_thread);
 struct rtp_learning_info {
 	int max_seq;	/*!< The highest sequence number received */
 	int packets;	/*!< The number of remaining packets before the source is accepted */
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27103
+	struct timeval received; /*!< The time of the last received packet */
+#endif
 };

 #ifdef HAVE_OPENSSL_SRTP
@@ -287,8 +290,9 @@ struct ast_rtp {
 	 * but these are in place to keep learning mode sequence values sealed from their normal counterparts.
 	 */
 	struct rtp_learning_info rtp_source_learn;	/* Learning mode track for the expected RTP source */
+#ifndef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27103
 	struct rtp_learning_info alt_source_learn;	/* Learning mode tracking for a new RTP source after one
-
+#endif
 	struct rtp_red *red;

 	ast_mutex_t lock;		/*!< Lock for synchronization purposes */
@@ -2470,6 +2474,9 @@ static void rtp_learning_seq_init(struct rtp_learning_info *info, uint16_t seq)
 {
 	info->max_seq = seq - 1;
 	info->packets = learning_min_sequential;
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27103
+	memset(&info->received, 0, sizeof(info->received));
+#endif
 }

 /*!
@@ -2484,6 +2491,15 @@ static void rtp_learning_seq_init(struct rtp_learning_info *info, uint16_t seq)
  */
 static int rtp_learning_rtp_seq_update(struct rtp_learning_info *info, uint16_t seq)
 {
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27103
+	if (!ast_tvzero(info->received) && ast_tvdiff_ms(ast_tvnow(), info->received) < 5) {
+		/* During the probation period the minimum amount of media we'll accept is
+		 * 10ms so give a reasonable 5ms buffer just in case we get it sporadically.
+		 */
+		return 1;
+	}
+#endif
+
 	if (seq == info->max_seq + 1) {
 		/* packet is in sequence */
 		info->packets--;
@@ -2492,6 +2508,9 @@ static int rtp_learning_rtp_seq_update(struct rtp_learning_info *info, uint16_t
 		info->packets = learning_min_sequential - 1;
 	}
 	info->max_seq = seq;
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27103
+	info->received = ast_tvnow();
+#endif

 	return (info->packets == 0);
 }
@@ -2656,10 +2675,16 @@ static int ast_rtp_new(struct ast_rtp_instance *instance,
 	/* Set default parameters on the newly created RTP structure */
 	rtp->ssrc = ast_random();
 	rtp->seqno = ast_random() & 0xffff;
+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_27103
:
```

- **asterisk CVE-2016-7551**

  Patch link: https://issues.asterisk.org/jira/secure/attachment/54224/ASTERISK-26272-11.patch

```
root@yeastar1-B250M-D2V:/home/k2/ipv6/astcore/src/asterisk-13.7.0# git diff channels/chan_sip.c
diff --git a/src/asterisk-13.7.0/channels/chan_sip.c b/src/asterisk-13.7.0/channels/chan_sip.c
index b30a343..105bf3f 100644
--- a/src/asterisk-13.7.0/channels/chan_sip.c
+++ b/src/asterisk-13.7.0/channels/chan_sip.c
@@ -5704,6 +5704,36 @@ static void set_t38_capabilities(struct sip_pvt *p)
        }
 }

+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_26272
+static void dialog_clean_rtp(struct sip_pvt *p)
+{
+       if (p->rtp) {
+               ast_rtp_instance_destroy(p->rtp);
+               p->rtp = NULL;
+       }
+
+       if (p->vrtp) {
+               ast_rtp_instance_destroy(p->vrtp);
+               p->vrtp = NULL;
+       }
+
+       if (p->trtp) {
+               ast_rtp_instance_destroy(p->trtp);
+               p->trtp = NULL;
+       }
+
+       if (p->srtp) {
+               sip_srtp_destroy(p->srtp);
+               p->srtp = NULL;
+       }
+
+       if (p->tsrtp) {
+               sip_srtp_destroy(p->tsrtp);
+               p->tsrtp = NULL;
+       }
+}
+#endif
+
 static void copy_socket_data(struct sip_socket *to_sock, const struct sip_socket *from_sock)
 {
        if (to_sock->tcptls_session) {
@@ -5770,6 +5800,11 @@ static int dialog_initialize_rtp(struct sip_pvt *dialog)
               return 0;
        }

+#ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_26272
+       /* Make sure previous RTP instances/FD's do not leak */
+       dialog_clean_rtp(dialog);
+#endif
+
```

- **asterisk CVE-2017-7617**

  Patch link:

  https://issues.asterisk.org/jira/secure/attachment/55270/0001-CDR-Protect-from-data-overflow-in-ast_cdr_setuserfie.patch

```
diff --git a/src/asterisk-13.7.0/main/cdr.c b/src/asterisk-13.7.0/main/cdr.c
index 9b3d044..023ff6f 100755
--- a/src/asterisk-13.7.0/main/cdr.c
+++ b/src/asterisk-13.7.0/main/cdr.c
@@ -5206,7 +5206,11 @@ void ast_cdr_setuserfield(const char *channel_name, const char *userfield)
                       if (it_cdr->fn_table == &finalized_state_fn_table) {
                               continue;
                       }
+              #ifdef YEASTAR_CSQ_SYNC_ASTERISK_JIRA_26897
+                      ast_copy_string(it_cdr->party_a.userfield, userfield, AST_MAX_USER_FIELD);
+              #else
                       strcpy(it_cdr->party_a.userfield, userfield);
+              #endif
               }
               ao2_unlock(cdr);
        }
```