K2 VoIP PBX

Administrator Guide

Sales Tel: +86-592-5503309
E-mail: sales@yeastar.com
Support Tel:+86-592-5503301
E-mail: support@yeastar.com
Web: http://www.yeastar.com

Version: 80.0.0.5
Revised: April 6, 2017

Copyright

Declaration of Conformity

Hereby, Yeastar Information Technology Co., Ltd. declares that Yeastar K2 IP PBX is in conformity with the essential requirements and other relevant provisions of the CE, FCC.

Warranty

The information in this document is subject to change without notice.
Yeastar Information Technology Co., Ltd. makes no warranty of any kind with regard to this guide, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Yeastar Information Technology Co., Ltd. shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance or use of this guide.

WEEE Warning

In accordance with the requirements of council directive 2002/96/EC on Waste of Electrical and Electronic Equipment (WEEE), ensure that at end-of-life you separate this product from other waste and scrap and deliver to the WEEE collection system in your country for recycling.

Contents

About This Guide

Thanks for choosing Yeastar K2 VoIP PBX. This guide is intended for administrators who need to prepare for, configure and operate K2 VoIP PBX. In this guide, we describe every detail on the functionality and configuration of the PBX. We begin by assuming that you are interested in K2 VoIP PBX and familiar with networking and other IT disciplines.

Related Documents

The following related documents are available on Yeastar website: http://www.yeastar.com.

Document	Description
Yeastar K2 VoIP PBX Extension User Guide	Users could refer to the manual for instructions on how to login the user portal, and how to configure their accounts, listen to call recordings, check voicemail messages, etc.

Safety when working with electricity

- Do not use a 3rd party power adaptor.
- Do not power on the device during the installation.
- Do not work on the device, connect or disconnect cables when lightning strikes.

K2 Overview

This chapter provides the following sections:

- Introduction
- Feature Highlights
- Hardware Overview

Introduction

Yeastar K2 VoIP PBX is designed for medium and large enterprises, supporting up to 2000 users and 500 concurrent calls. Yeastar K2 delivers exceptional cost savings, productivity and efficiency improvements, delivering power, performance, quality and peace of mind.

The all new K2 is engineered for the communications needs of today and tomorrow, and with the Yeastar unique modular design future proofs your investment choice.

Hardware Overview

By default, the K2 VoIP PBX is installed with a 1T hard disk. Please contact us if you want to install a different hard disk.

Front Panel

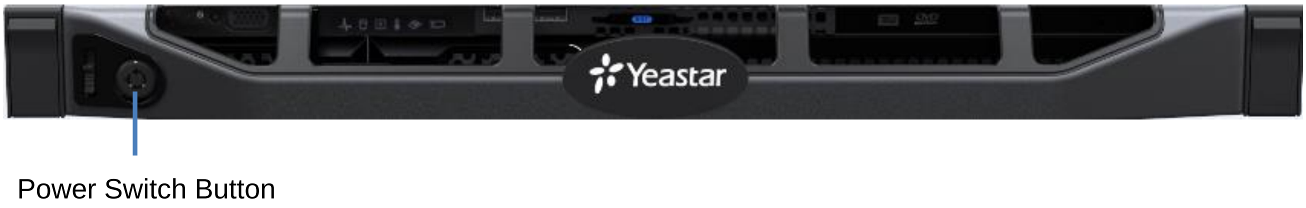


Figure 1-1 Yeastar K2 VoIP PBX Front Panel

Rear Panel

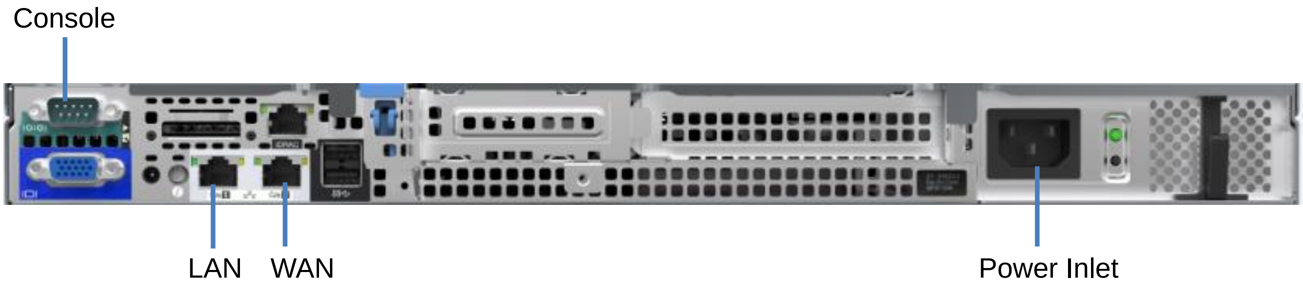


Figure 1-2 Yeastar K2 VoIP PBX Rear Panel

Port Description

Table 1-1 Yeastar K2 VoIP PBX Port Description

Ports	Description
Console	Connect to the RS-232 Cable to debug to system.
LAN	10/100M adaptive RJ45 Ethernet port.
WAN	10/100/1000M adaptive RJ45 Ethernet port.
Power Inlet	Connect the supplied power supply to the port.
Power Switch	Press this button to switch on/off the device.

Getting Started

This chapter explains how to log in Yeastar K2 Web GUI, use the taskbar and widgets, and open applications with the Main Menu.

- Accessing Web GUI
- Activating and Upgrading Yeastar K2
- Web Configuration Desktop
- Make Your First Call

Accessing Web GUI

Yeastar K2 provides web-based configuration interface for administrator and extension users. The administrator can manage the device by logging in the Web interface. Check the factory defaults below:

IP address: https://192.168.5.150:8088
User Name: admin
Default Password: password

To log in K2:

1 Connect the network cable to the K2 PBX's LAN port, connect the power cord to PBX's power inlet, switch on the device.

2 Make sure your computer is connected to the same network as the K2 VoIP PBX.

3 Start a web browser on your PC, enter the IP address, press **Enter** on your keyboard.

4 Enter your user name and password, click **Login**.

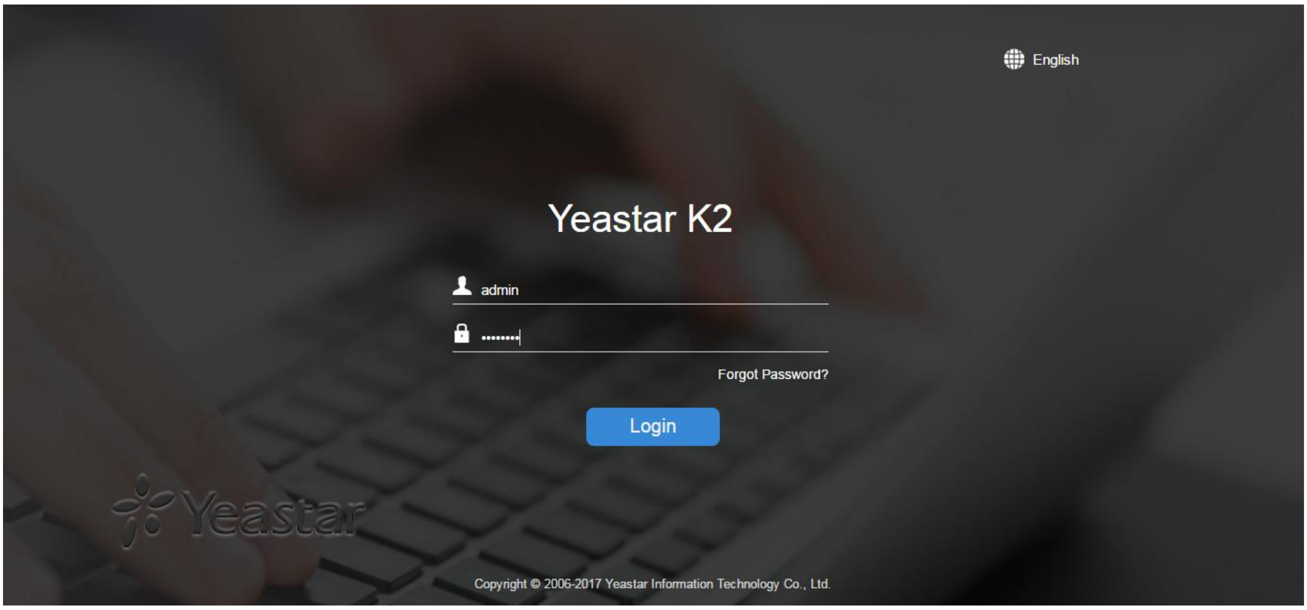

English
Yeastar K2
admin
••••••••
Forgot Password?
Login
Yeastar
Copyright © 2006-2017 Yeastar Information Technology Co., Ltd.

Figure 2-1 K2 Web Configuration Panel Login Page

Note: to ensure your connection to the K2 Web GUI runs smoothly, please use the following browsers:

- **Chrome**
- **Firefox**
- **Internet Explorer:** 11.0 or later

Activating and Upgrading Yeastar K2

You can try out all the features on Yeastar K2 free without time limit. However the Yeastar K2 trial version has a limit on the number of extensions, concurrent calls, VoIP trunks, ring groups, etc.

Table 2-1 Yeastar K2 Trail Version Limits

Feature	Max Number
Extension	10
Concurrent Call	5
VoIP Trunk	2
Ring Group/Queue/Conference/Pickup Group/Paging/Intercom/Callback/DISA	1

Follow the steps below to activate or upgrade Yeastar K2

1. Log in Yeastar K2 web interface, go to **Maintenance > Activate**, click **Apply for Activation**.
2. Contact Yeastar to buy the license, tell us how many extensions and concurrent calls you want to activate on your Yeastar K2 device.
3. Yeastar will generate the license according to your needs.
4. Log in your Yeastar K2 web interface, go to **Maintenance > Activate**, click **Update Activation Code**, the page will show the device has been activated.
5. If you want to extend your extensions or concurrent calls, you need to contact Yeastar to buy a new license, then go to the **Maintenance > Activate**, click **Update Activation Code**.

Web Configuration Desktop

When you log in Yeastar K2 Web GUI, you will see the desktop. From here, you can manage settings and view system resource information.

Desktop

The desktop is where your application windows are displayed.

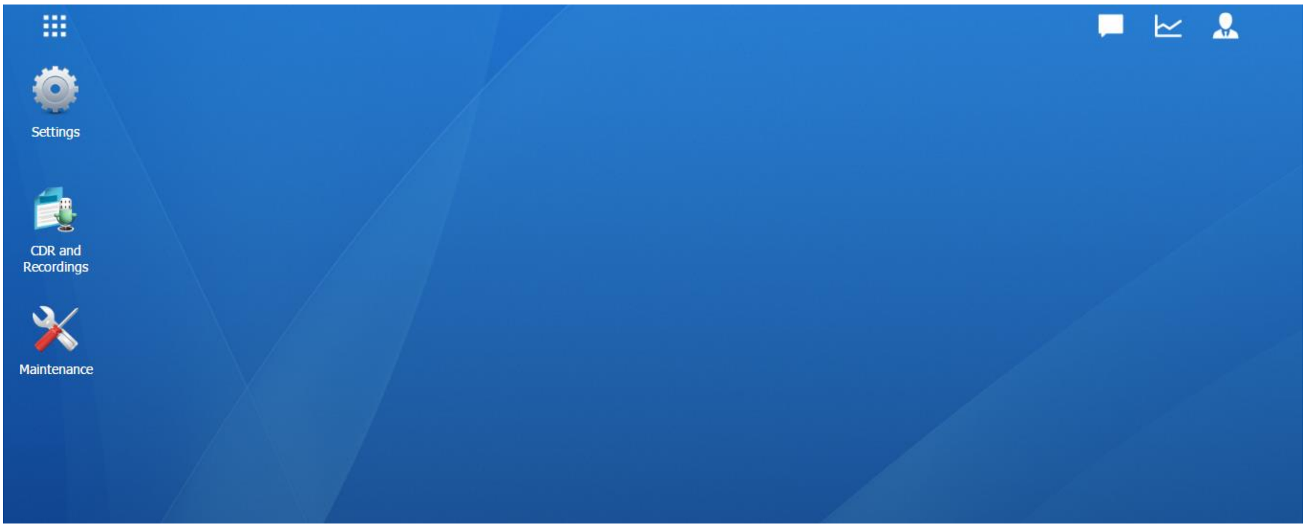


Figure 2-2 Desktop

Taskbar

The taskbar at the top of the desktop includes the following items:

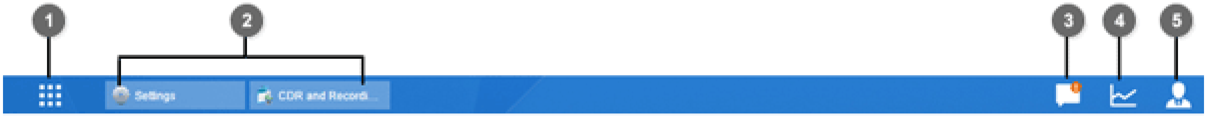


Figure 2-3 Taskbar

1 **Main Menu:** view and open applications installed on your K2 system. Right-click an application icon, you can add the application to desktop.

2 **Open Application**

- Click the icon of an application to show or hide its window on the desktop.
- Right-click the icon and choose from the shortcut menu to manage the application window (**Maximize**, **Minimize**, **Restore**, **Close**).

3 **Notifications:** displays notifications, like errors, status updates, and app installation notifications.

4 **Resource Monitor:** click the icon to check the system information, network status and storage usage.

5 **Options**: logout, change Web language or modify personal account options.

Main Menu

Click the **Main Menu** ▦ at the top-left of the desktop, you can find all the installed applications on your K2 system.

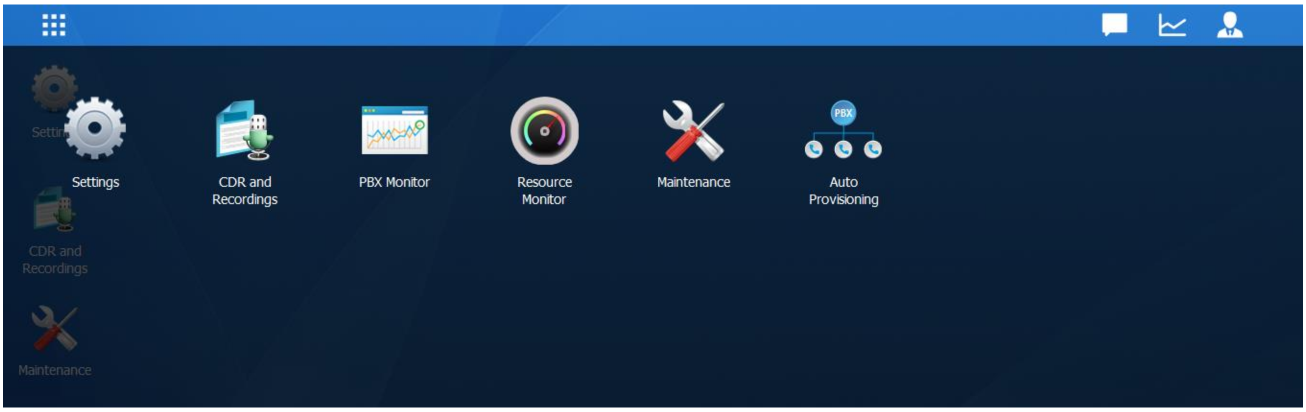


Figure 2-4 Main Menu

Options

Click the options icon 👤 to logout, change Web language or modify your account settings.

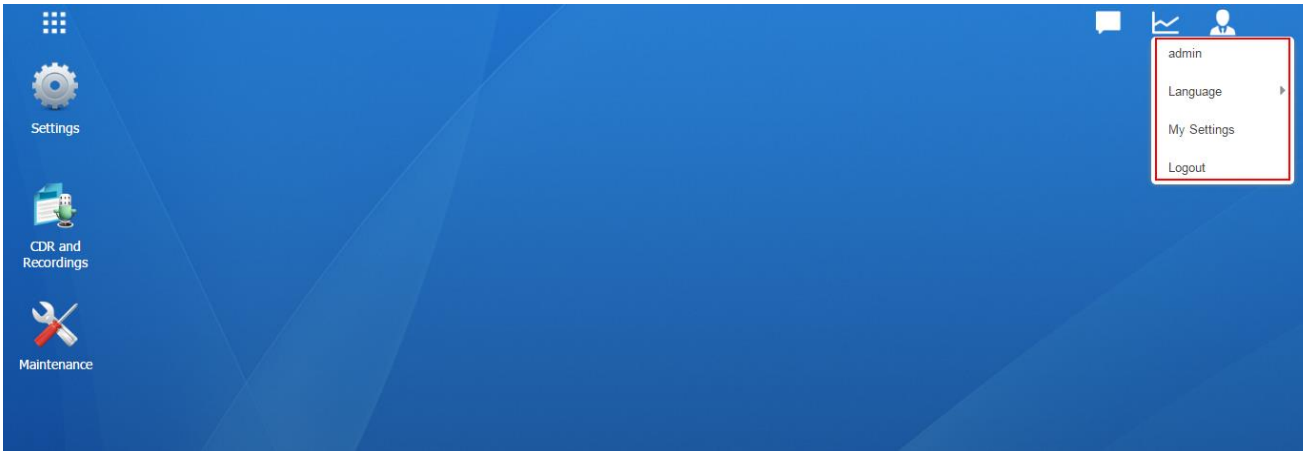
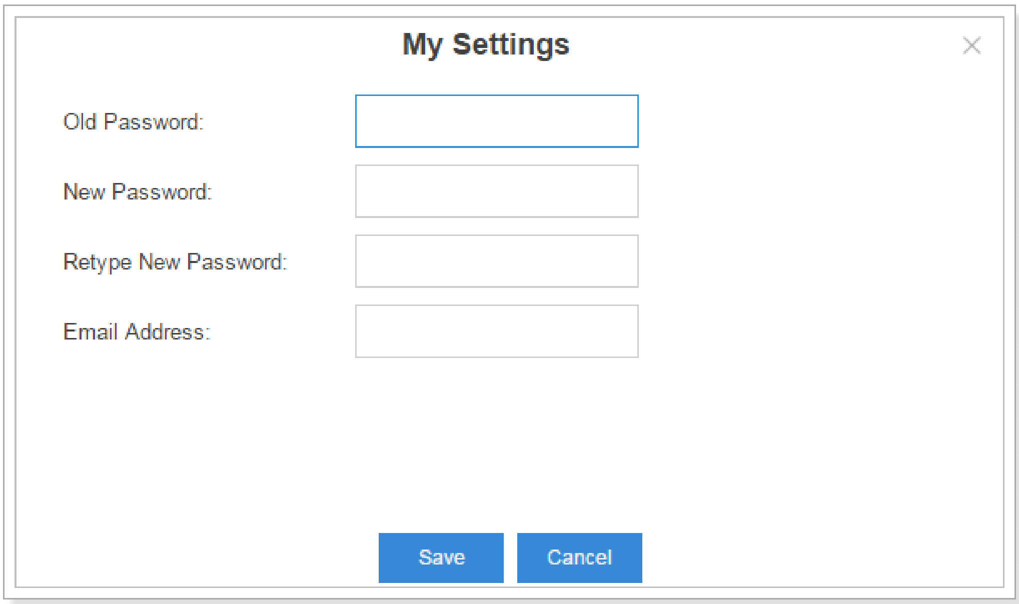


Figure 2-5 Options

- **Language**
  Select Language to change web language.
- **My Settings**
  Click My Settings to modify your account settings. Here you can change the login password and bind your email address with the account.



My Settings

Old Password:

New Password:

Retype New Password:

Email Address:

Figure 2-6 My Settings

- **Logout**

  Click Logout to log out the Web GUI.

Save and Apply Changes

Click **Save** button after your configurations on the K2 system, do not forget to click **Apply** button on the upper right of the desktop to submit all the changes. If the change requires reboot to take effect, the system will prompt you with a pop-up window.

Make Your First Call

Connect your IP phone and K2 device to the same network. Then register an extension to the IP phone and make your first call through K2 system.

1. Log in your K2 Web GUI, go to **Settings > PBX > Extensions**.
2. Click **Add** to create a new extension, set the type as "SIP". You will need the Registration Name and Registration Password to register the extension later.
3. Register the extension on your phone with the Registration Name and Registration Password, the SIP server address is your K2 IP address.
4. When the extensions is registered to K2, you can dial *2 to access your voicemail box. The default password to enter the voicemail box is your extension number.
5. Once entering the voicemail box, you are connected to the K2 system!

System Settings

This chapter explains system settings on K2. Go to **Settings > System** to check the system settings.

- Network
- Security
- User Permission
- Date & Time
- Email
- Storage

Network

After successfully logging in the K2 Web GUI for the first time with the factory IP address, users could go to **Settings > System > Network** to configure the network for K2.

Basic Settings

Please check the basic network settings below.

Table 3-1 Network Basic Settings Description

Basic Settings	
Hostname	Set the hostname for the system.
Mode	Select the Ethernet mode. The default mode is Single. ● Single: only LAN port will be used for uplink, WAN port is disabled. ● Dual: the two Ethernet interfaces will use different IP addresses. Assign two IP addresses in this mode.
Default Interface	In Dual mode, you need to choose the default interface.
LAN/WAN Settings (DHCP Mode)	
If you choose this mode, the system will act as DHCP client to get an available IP address from your local network.	
LAN/WAN Settings (Static IP Address)	
IP Address	Enter the IP address (xxx.xxx.xxx.xxx).
Subnet Mask	Enter the subnet mask (xxx.xxx.xxx.xxx). For example, 255.255.255.0
Gateway	Enter the gateway address (xxx.xxx.xxx.xxx).
Preferred DNS Server	Enter the IP address of the preferred DNS server (xxx.xxx.xxx.xxx).
Alternate DNS Server	Enter the IP address of the alternative DNS server (xxx.xxx.xxx.xxx).
LAN/WAN Settings (PPPoE)	
Username	Enter the PPPoE username.
Password	Enter the PPPoE password.

OpenVPN

K2 supports OpenVPN. The system provides detailed VPN configurations on the Web GUI and you can also upload the VPN configuration package to the system to make it work.

Before using OpenVPN feature, please Enable OpenVPN first, then choose the Type to configure OpenVPN:

- Manual Configuration
- Upload OpenVPN Package

Check the VPN configurations parameters below.

Table 3-2 OpenVPN Manual Configuration Parameters Description

OpenVPN Configuration	
Server Address	Enter the server address of OpenVPN.
Server Port	Enter the server port of OpenVPN. The default is 1194.
Protocol	Select the protocol type. The server and client must use the same protocol.
Device	Select the network device. The client and server must use the same setting. ● TUN: a TUN device is a virtual point-to-point IP link. ● TAP: a TAP device is a virtual Ethernet adapter.
Username	Specify the username.
Password	Specify the password.
Encryption	Select the encryption method. The server and client must use the same setting.
Compression	Enable or disable compression for data stream. The server and client must use the same setting.
Proxy Server	Specify the proxy server.
Proxy Port	Specify the proxy port.
CA Cert	Upload a CA certificate.
Cert	Upload a Client certificate.
Key	Upload a Client key.
TLS Authentication	Enable or disable TLS authentication. If enabled, please upload a TA key via **Settings > System> Security>Certificate**.

DDNS Settings

Dynamic DNS or DDNS is a method of updating, in real time, a Domain Name System (DNS) to point to a changing IP address on the Internet. This is used to provide a persistent domain name for a resource that may change location on the network. DDNS is usually configured on router. If your router cannot support DDNS, we can set up DDNS on Yeastar system.

Yeastar K2 supports the following DDNS servers:

- dyndns.org
- freedns.afraid.org
- www.no-ip.com
- www.zoneedit.com

- www.oray.com
- 3322.org

Check the DDNS configuration parameters below.

Table 3-3 DDNS Configuration Parameters Description

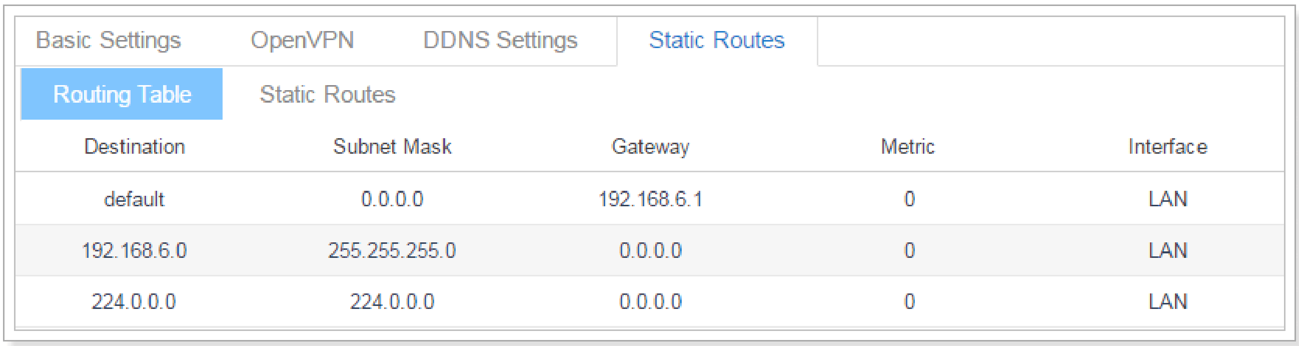
DDNS	
DDNS Status	This shows the current DDNS status of the device.
Enable DDNS	Check this box to enable DDNS.
Server	Choose a DDNS provider from the list.
Username	Enter the username of your DDNS account.
Password	Enter the password of you DDNS account.
Hash	Enter your string of Hash as provided by freedns.afraid.org.
Domain	Enter the domain name.

Static Route

In computer networking, a routing table is a data table stored in a router or a networked device that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. Static routes are entries made in a routing table by non-automatic means and which are fixed rather than being the result of some network topology “discovery” procedure.
Static route on the system is used to configure to route the connection, packets to particular network destinations, usually a specific gateway.

- **Routing Table**

All the static routes are displayed on the Routing Table.



Destination	Subnet Mask	Gateway	Metric	Interface
default	0.0.0.0	192.168.6.1	0	LAN
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

Figure 3-1 Routing Table

- **Static Routes**

Click Static Routes tab, you can add static routes here.

Click Add to add a static route.

- Click ✎ to edit the static route.

- Click 🗑 to delete the static route.

Check the Static route settings below.

Table 3-4 Static Routes Settings Description

Static Route	
Destination	Enter the destination IP address or IP subnet for the K2 to reach using the static route. **Example:** • IP address: *192.168.6.120* • IP subnet: *192.168.6.0*
Subnet Mask	Enter the subnet mask for the destination address. **Example:** *255.255.255.255*
Gateway	Enter the gateway address. The K2 system will reach the destination address via this gateway. **Example:** *192.168.6.1*
Metric	The cost of a route is calculated using what are called routing metric. Routing metrics are assigned to routes by routing protocols to provide measurable values that can be used to judge how useful (how cost) a route will be.
Interface	Select the network interface. The system will reach the destination address using the static route through the selected network interface.

Security

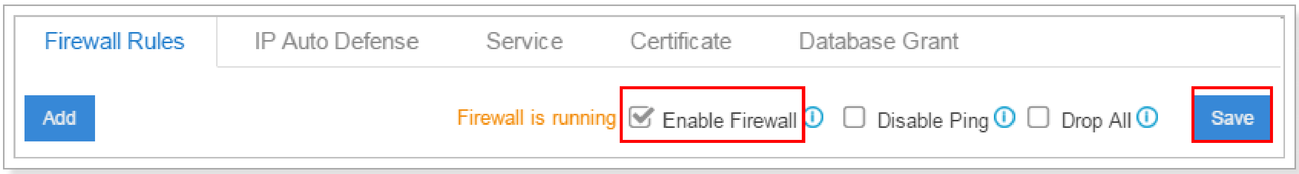
VoIP attack, although not an everyday occurrence does exist. When using VoIP, system security is undoubtedly one of the issues we care about most. With appropriate configuration, and some basic safety habits, we can improve the security of the telephone system. Moreover, the powerful built-in firewall function in Yeastar system is adequate to enable the system to run safely and stably.

We strongly recommend that you configure firewall and other security options to prevent the attack fraud and the system failure or calls loss.

Firewall Rules

Users could add rules to accept or reject traffic through the system. Go to **Settings** > **System** > **Security** > **Firewall Rules** to configure firewall for the system.

Before adding firewall rules, please check the option **Enable Firewall**, then click **Save** to enable the firewall.



Firewall Rules | IP Auto Defense | Service | Certificate | Database Grant

Add

Firewall is running ☑ Enable Firewall ⓘ □ Disable Ping ⓘ □ Drop All ⓘ Save

Figure 3-2 Firewall Rules

- Click Add to add a new rule.
- Click ✎ to edit the rule.
- Click 🗑 to delete the rule.

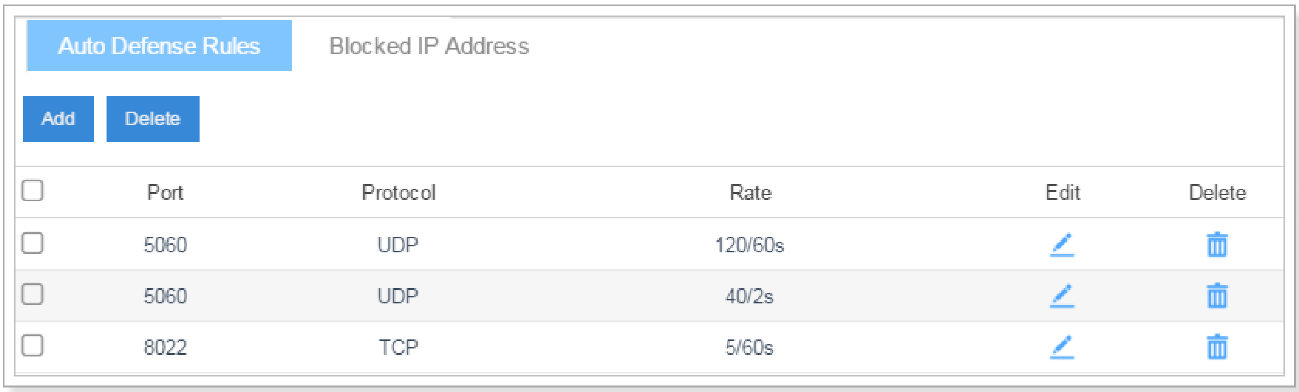
Check the firewall configuration parameters below.

Table 3-5 Firewall Configuration Parameters Description

Firewall	
Enable Firewall	Enable Firewall to protect the system from malicious attack. Click Save icon to apply the changes.
Disable Ping	Enable this item, net ping from remote hosts will be dropped. Click Save icon to apply the changes.
Drop All	When you enable Drop All feature, the system will drop all packets and connections from other hosts if there are no other rules defined. To avoid locking the device, at least one TCP Accept common rule must be created for port used for SSH access and port used for HTTP access.
Firewall Rules	
Name	Specify a name to identify the firewall rule.
Description	Description for this firewall rule.
Action	Select the action for the firewall rule: • Accept • Ignore • Reject
Protocol	Select the protocol applied for the rule: • UDP • TCP • BOTH
Source IP address/ Subnet mask	The IP address for this rule. **Example:** 192.168.5.100/255.255.255.255 means this rule is for 192.168.5.100. 192.168.5.100/255.255.255.0 is for IP from 192.168.5.0 to 192.168.5.100.
Port	Set the port for the firewall rule. The end port must be equal to or greater than start port.

IP Auto Defense

Users could create auto defense rules, then the system will prevent massive connection attempts or brute force attacks. The IP addresses would be listed in the **Blocked IP Address** table. There are 3 default auto defense rules, we recommend you keep the rules there.



□	Port	Protocol	Rate	Edit	Delete
□	5060	UDP	120/60s	✎	🗑
□	5060	UDP	40/2s	✎	🗑
□	8022	TCP	5/60s	✎	🗑

Figure 3-3 Auto Defense Rules

Please check the auto defense rule configuration parameters below.

Table 3-6 IP Auto Defense Rule Configuration

IP Auto Defense Rule	
Port	Auto defense port, for example, 8022.
Protocol	Select auto defense protocol: ● UDP ● TCP
The 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 sets 90 and Time Interval sets 60 mean 90 IP packets are allowed in 60 seconds.

Service

The service page displays all the service status and port on K2.

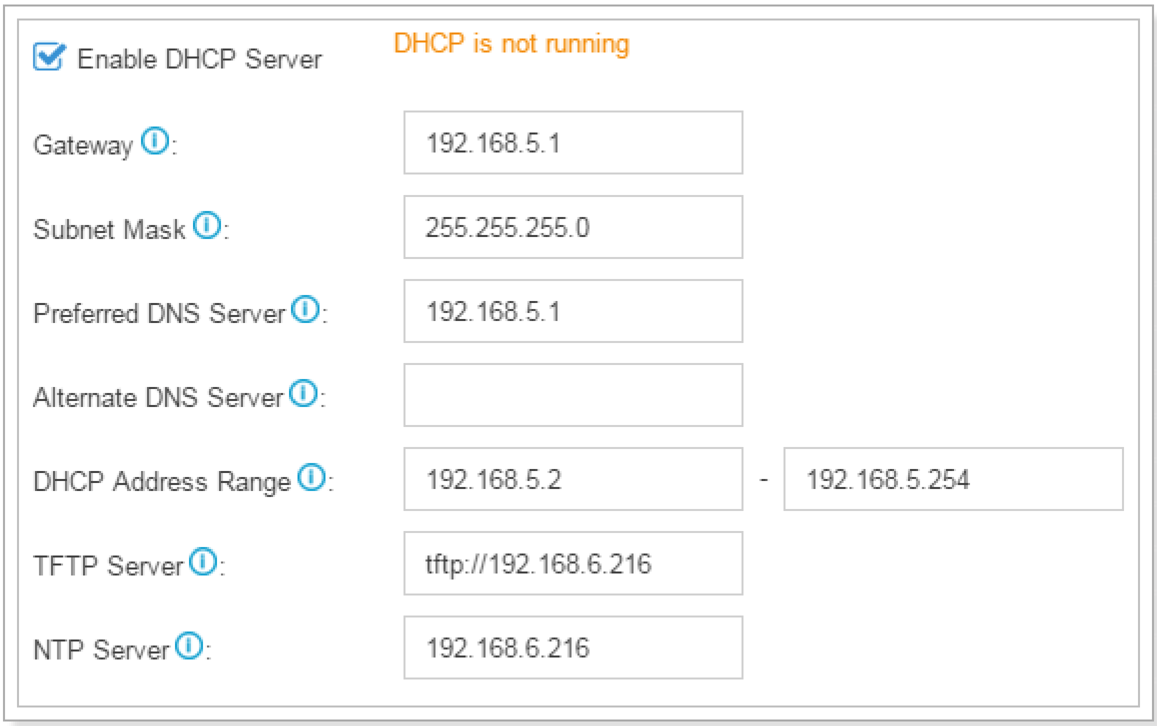
Table 3-7 Service Configuration

Protocol or Service	Description
Auto Logout Time(min)	After the set time of inactivity, the session will automatically log out. The default time is 15 minutes.
HTTPS	The default access protocol is HTTPS and the port is 8088.
Redirect from port 80	If the option is enabled, when you access K2 using HTTP with port 80, it will be redirected to HTTPS with port 8088.
Certificate	If you have uploaded HTTPS certificates to K2, select it from the drop-down menu.
HTTP	The default port for HTTP is 80.

SSH	SSH port is used to access K2 underlying configurations to debug the system. The default port is 8022. We recommend you disable SSH port if you do not need it.
FTP	With FTP service, you can connect to PBX via web browser. The default port is 21.
TFTP	To upload files to K2 through TFTP, you need to enable this option.
IAX	The default port is 4569.
SIP UDP	The default port is 5060.
SIP TCP	The default port is 5060.
SIP TLS	The default port is 5061.

DHCP

Check the box **Enable DHCP Server**, K2 will acts as a DHCP server. This feature is used when you do phone provisioning through DHCP mode.



☑ Enable DHCP Server

DHCP is not running

Gateway: 192.168.5.1

Subnet Mask: 255.255.255.0

Preferred DNS Server: 192.168.5.1

Alternate DNS Server:

DHCP Address Range: 192.168.5.2 - 192.168.5.254

TFTP Server: tftp://192.168.6.216

NTP Server: 192.168.6.216

Figure 3-4 DHCP Server

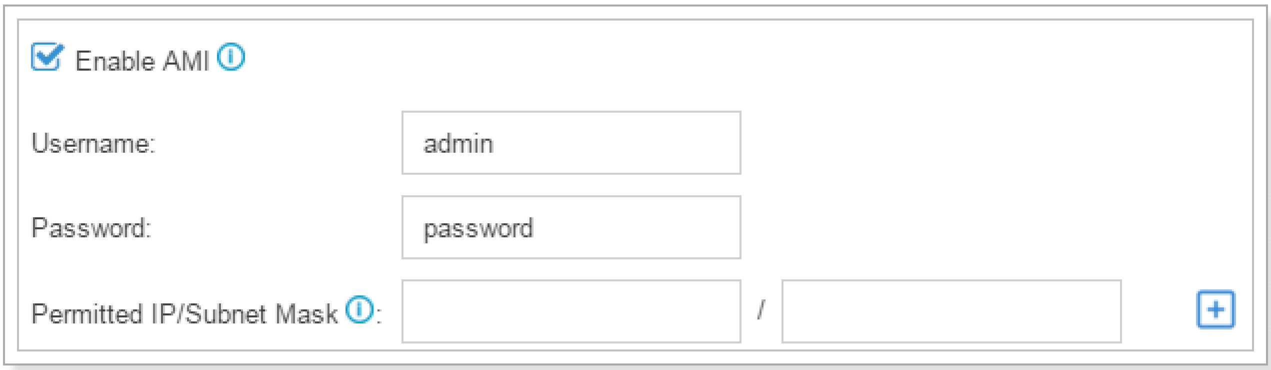
- **Gateway**: enter the gateway IP address.
- **Subnet Mask**: enter the subnet mask.
- **Preferred DNS Server**: enter the preferred DNS server.
- **Alternate DNS Server**: enter the alternate DNS server.
- **Allow IP Address**: this sets the IP address that the DHCP server can assign to network devices. Start IP address is on the left and end IP on the right.
- **TFTP Server**: this option is for Phone Provisioning feature. So IP phones can get configuration file from this address. For Grandstream and Panasonic phones, enter the PBX’s IP address, for example: 192.168.5.150. For other IP phones, remember to specify the protocol, for example,

tftp://192.168.5.150.

- **NTP Server**: the PBX can be a NTP server. By default, it is the PBX's IP address.

AMI

The Asterisk Manager Interface (AMI) is a system monitoring and management interface provided by Asterisk. The 3rd party software can work with K2 using AMI interface. The default port is 5038.



☑ Enable AMI

Username: admin

Password: password

Permitted IP/Subnet Mask: /

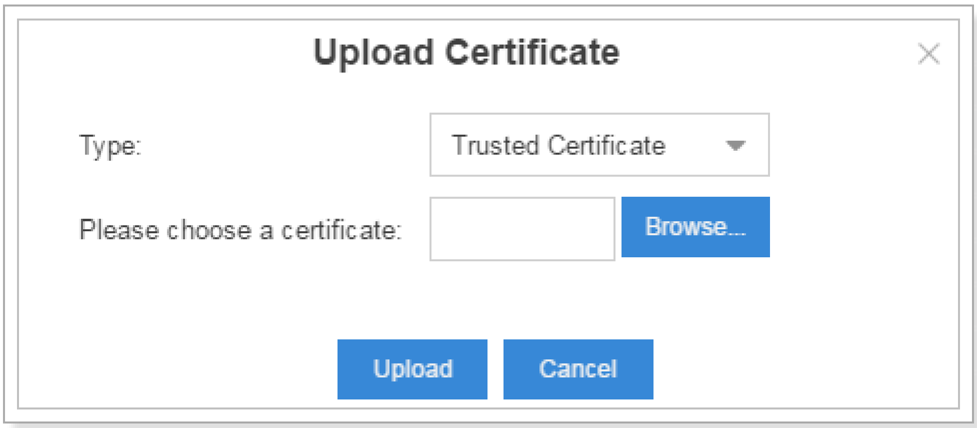
Figure 3-5 AMI Settings

- **Username**: specify a name for the AMI user.
- **Password**: specify a password for the user to connect to AMI.
- **Permitted IP/Subnet mask**: configure permitted IP address and subnet mask that would be allowed to authenticate as the AMI user. If you do not set this option, all IPs will be denied.

Certificate

K2 supports TLS and HTTPS protocols. Before using these two protocols, you need to upload the relevant certificates to the system.

Click Upload to upload a certificate.



Upload Certificate

Type: Trusted Certificate

Please choose a certificate:

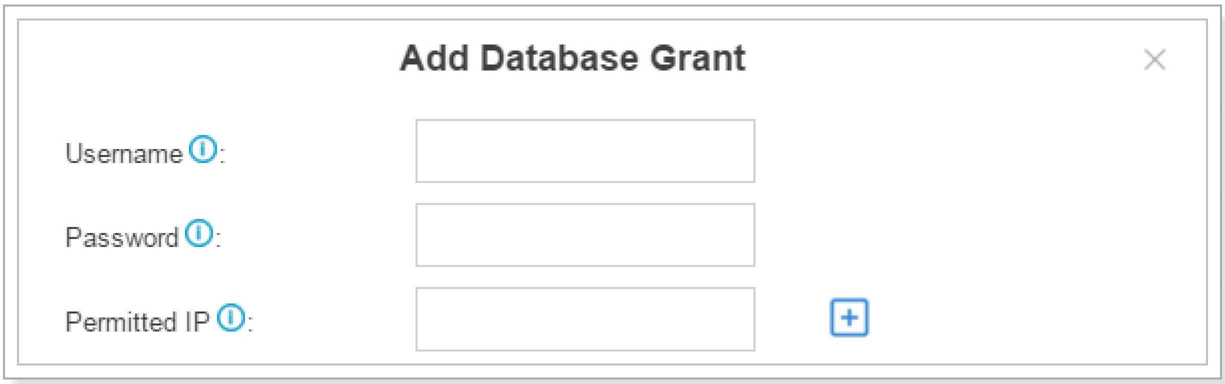
Figure 3-6 Certificate

- **Trusted Certificate**: This certificate is a CA certificate. When selecting "TLS Verify Client" as "Yes", you should upload a CA. The relevant TLS client (i.e. IP phone) should also have this certificate.
- **PBX Certificate**:
  This certificate is server certificate. No matter selecting "TLS Verify Client" as "Yes" or "NO", you

should upload this certificate to K2. If TLS client (i.e. IP phone) enables “TLS Verify server”, you should also upload the relevant CA certificate on IP phone.

Database Grant

Yeastar K2 is using MySQL database. The 3rd party software can access MySQL via the Internet. Before that, you need to grant the authority to the database user. Go to Database Grant page, click Add to add a database user, specify the username and password.



Add Database Grant

Username ⓘ:

Password ⓘ:

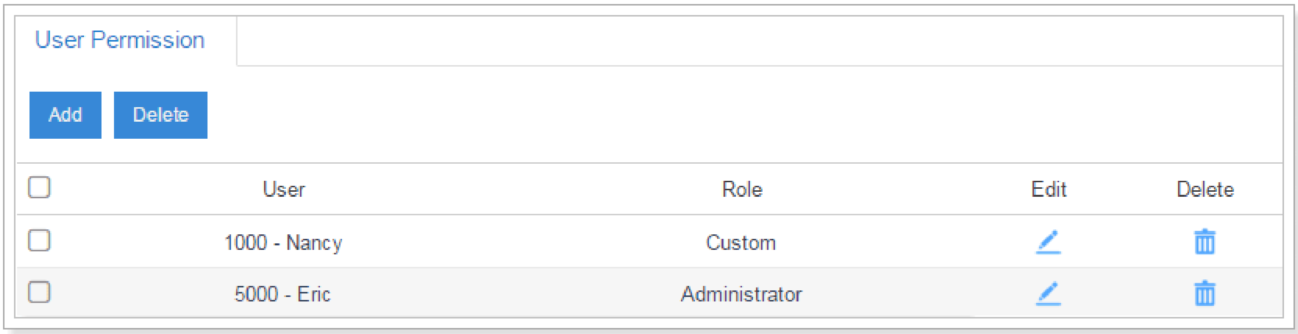
Permitted IP ⓘ:

Figure 3-7 Add Database Grant

- **Username**: configure the username which can be used by third party to access the database of PBX.
- **Password**: configure the password which can be used by third party to access the database of PBX.
- **Permitted IP**: enter the permitted IP address.

User Permission

The system has one default administrator account, which has the highest privileges. Here the administrator is referred as Super Admin. The system will automatically create user accounts when new extensions are created. By default, the extension users can log in the system and check their own settings and CDR. The Super Admin can grant more privileges for extension users. All the created users will be displayed on the User Permission page.



User Permission

Add Delete

□	User	Role	Edit	Delete
□	1000 - Nancy	Custom	✎	🗑
□	5000 - Eric	Administrator	✎	🗑

Figure 3-8 User Permission

- **Super Admin** has the highest privilege. The super administrator can access all pages on K2 Web and make all the configurations on the system.

Username: admin

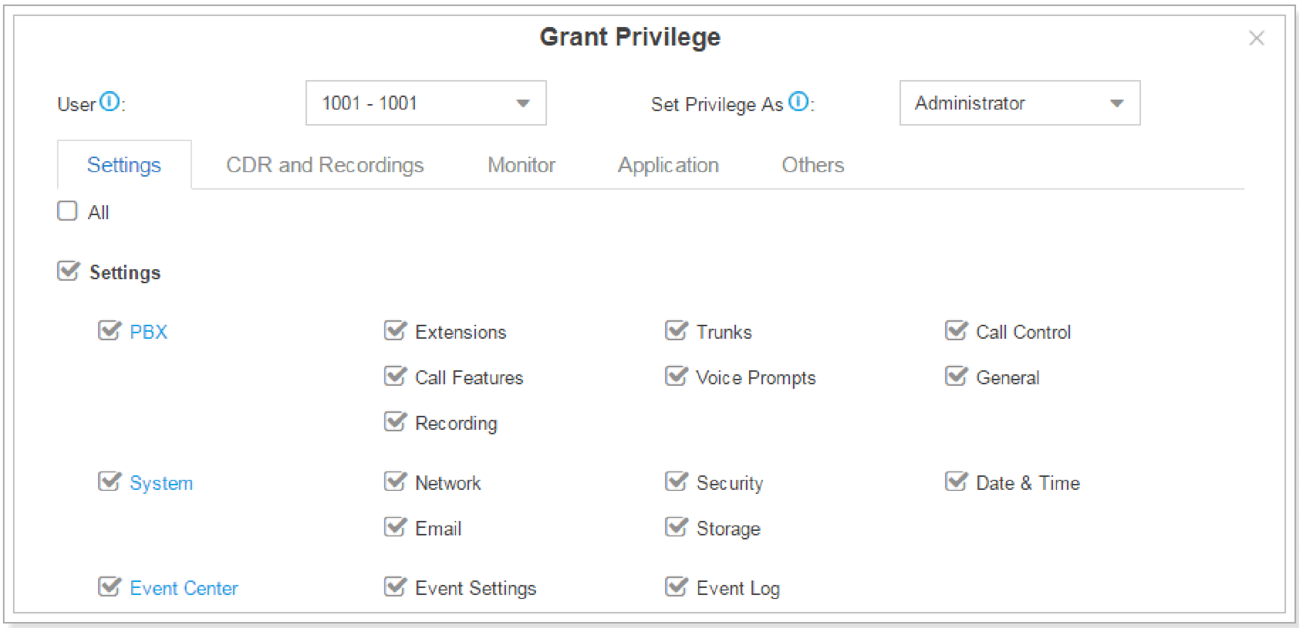
Default Password: password

- **Administrator** is created by the Super Admin. The administrator has all the privileges but cannot create new users for login.
- **Custom User** is created by the Super Admin. The Super Admin sets the privileges for those users according to different situations.

Add New User Permission

Log in the K2 Web GUI with the Super Admin account, go to **Settings > System > User Permission**.

Click Add to add a new User Permission. The following window prompts. Choose the user and privilege type, then check the options to enable the privileges for the user.



Grant Privilege ×

User ⓘ: 1001 - 1001 ▾

Set Privilege As ⓘ: Administrator ▾

Settings | CDR and Recordings | Monitor | Application | Others

☐ All

☑ Settings

☑ PBX	☑ Extensions	☑ Trunks	☑ Call Control
	☑ Call Features	☑ Voice Prompts	☑ General
	☑ Recording		
☑ System	☑ Network	☑ Security	☑ Date & Time
	☑ Email	☑ Storage	
☑ Event Center	☑ Event Settings	☑ Event Log	

Figure 3-9 Add New User Permission

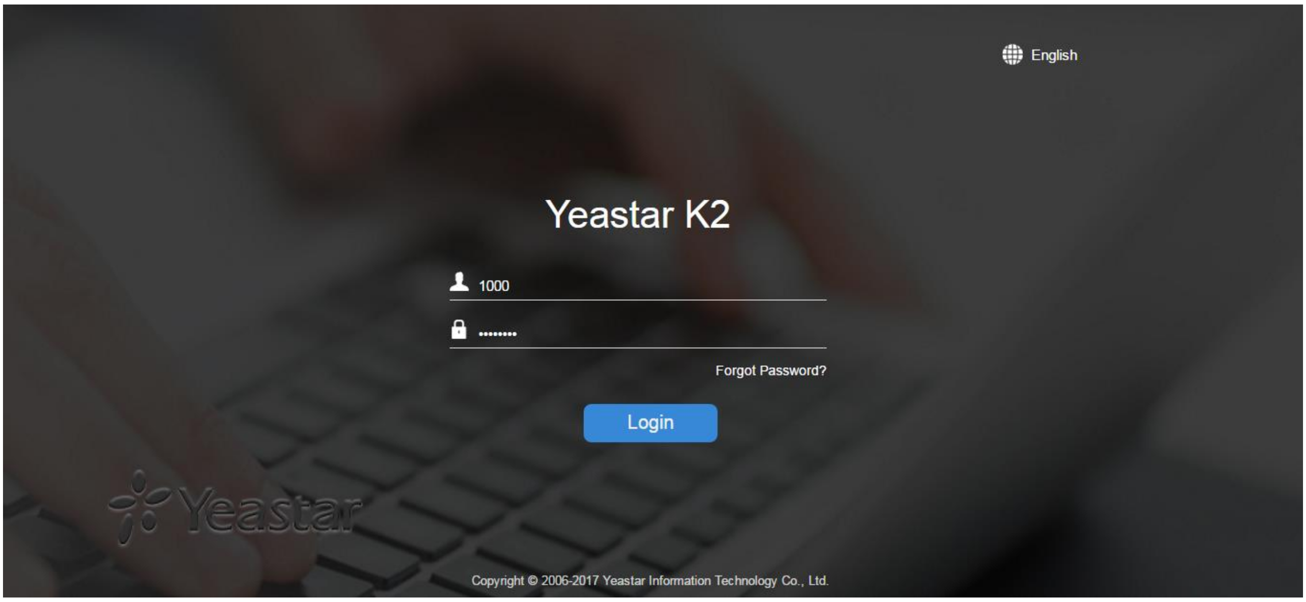
Once created, the Super Admin can edit the users by clicking ✎ or delete the users by clicking 🗑.

User Portal

The extension user could log in K2 Web GUI with the extension username and password. The extension user account is created automatically when an extension is created on the system.

- **Username**: extension number (i.e. 1000)
- **Default password**: “pass” plus extension number (i.e. pass1000)

Below is an example of login page using extension number 1000.

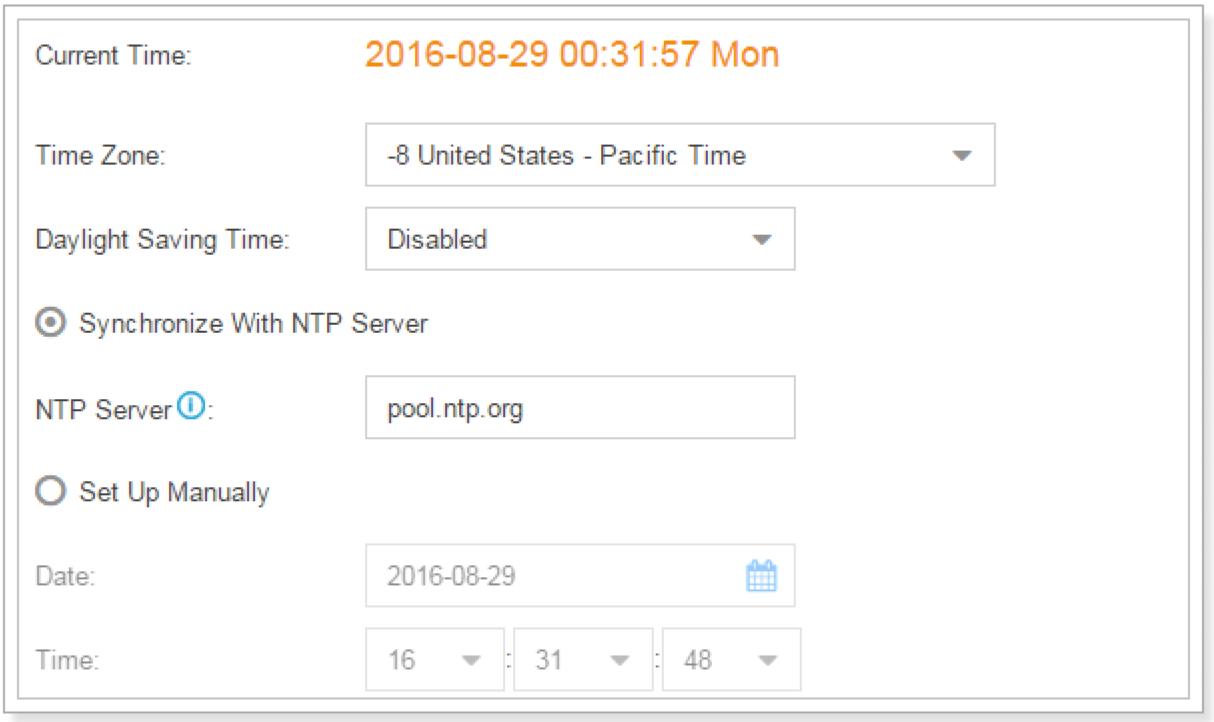


English
Yeastar K2
1000
....
Forgot Password?
Login
Yeastar
Copyright © 2006-2017 Yeastar Information Technology Co., Ltd.

Figure 3-10 User Portal

Date & Time

Go to **Settings > System > Date & Time** to check the current time on the system. Here you can adjust time of the system (including time zone) to your local time.



Current Time: 2016-08-29 00:31:57 Mon

Time Zone: -8 United States - Pacific Time

Daylight Saving Time: Disabled

● Synchronize With NTP Server

NTP Server: pool.ntp.org

○ Set Up Manually

Date: 2016-08-29

Time: 16 : 31 : 48

Figure 3-11 Date & Time

- **Time Zone**: select your current time zone.
- **Daylight Saving Time**: the option is disabled by default. Enable it when necessary.
- **Synchronize With NTP Server**: if you choose this mode, the system will adjust its internal clock to a central network server. Please note K2 should be able to access the Internet if you choose

this mode.

    - NTP Server: enter a NTP server.
- **Set Up Manually**: if you choose this mode, you need to set the time manually.
    - Date: choose the date.
    - Time: choose the time.

Email

Set the system's email to send voicemail to email, alert event emails, and fax to email. Go to **Settings > System > Email** to configure the system email.
Check the email settings parameters below.

Table 3-8 Email Settings

Option	Description
Email Address	Enter the email address.
Password	Enter the password.
Outgoing Mail Server (SMTP)	Enter SMTP server and port. **Example**: *smtp.sina.com:25*
Incoming Mail Server (POP3)	Enter the POP3 server and port. **Example**: *pop.sina.com:110*
Enable TLS	Use TLS to send secure message to server .If the email sending server needs to authenticate the sender, you need to select the checkbox. Note: if you use Gmail or Exchange, you need enable this option.

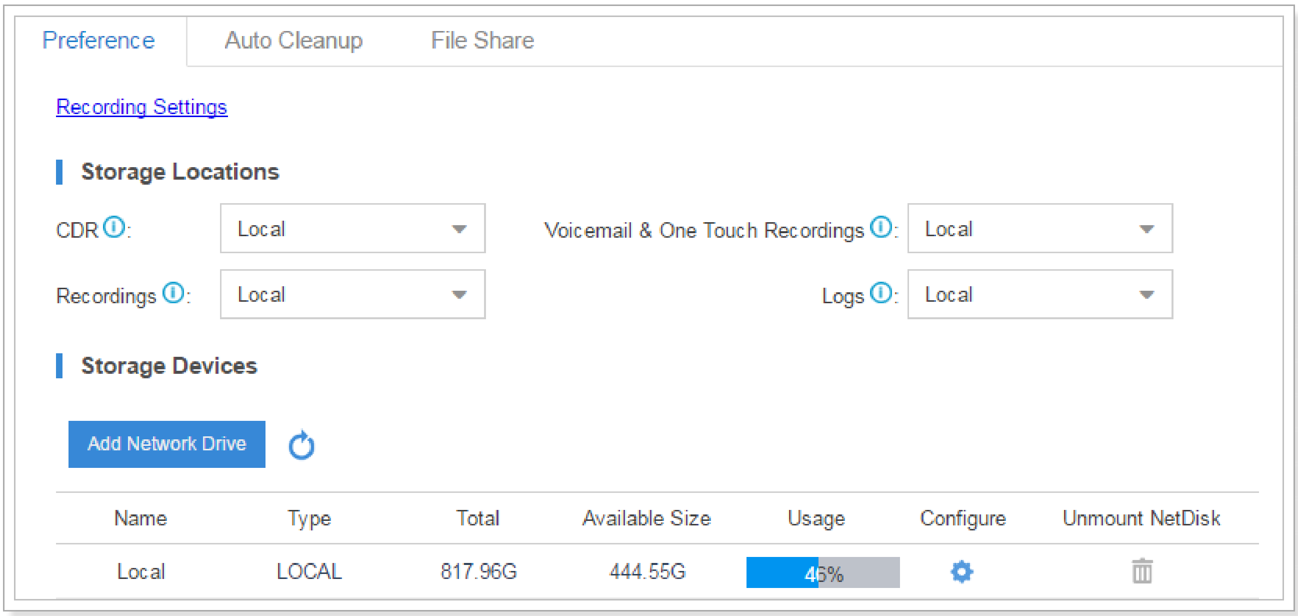
After finishing the configuration, click Test to test the email. In the prompt, fill in an email address to send a test email to verify the Email settings.

Storage

Yeastar K2 provides local storage (Flash) and supports external storage TF/SD card. Users could choose where to store the voicemails, CDR, recordings and logs.

Storage Devices

Go to **Settings > System > Storage** to configure the storage. This page shows all the storage devices. The local type device refers to the installed hard disk.



Storage Locations

CDR: Local

Voicemail & One Touch Recordings: Local

Recordings: Local

Logs: Local

Storage Devices

Name	Type	Total	Available Size	Usage	Configure	Unmount NetDisk
Local	LOCAL	817.96G	444.55G	46%	⚙	🗑

Figure 3-12 Storage Devices

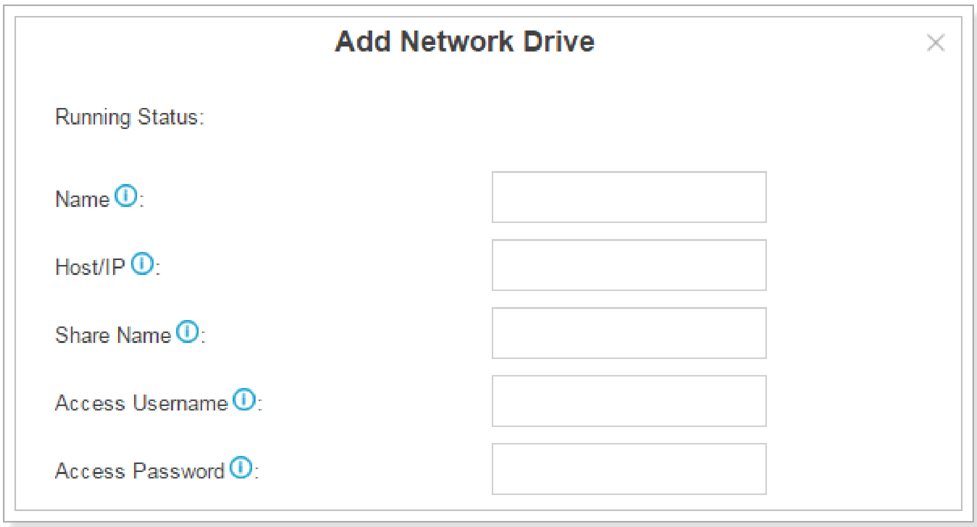
To format a storage device:

1. Click ⚙.
2. Click Format on the pop-up window to start formatting.

To add Network Drive:

The Network Drive feature is used to extend storage space. Before network drive can be properly configured, an SMB share folder accessible from Yeastar system must be set up on a Windows based machine. Once that has been set up, please follow the following instructions to configure network drive:

1. Choose a window-based computer that is always in service.
2. Create a folder.
3. Share this folder to Everyone.
4. Click Add Network Drive and input the Net-Disk information in Yeastar K2:



Add Network Drive

Running Status:

Name ⓘ:

Host/IP ⓘ:

Share Name ⓘ:

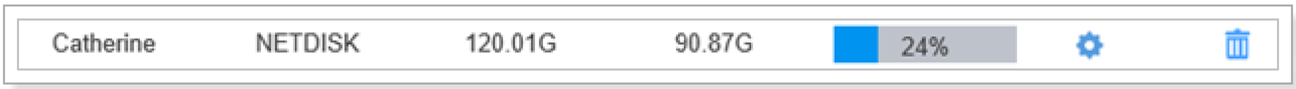
Access Username ⓘ:

Access Password ⓘ:

Figure 3-13 Add Network Disk

- **Name**: give this network drive a name to help you identify it.
- **Host/IP**: set the IP address where the recordings will be stored.
- **Share Name**: the shared folder name where the recordings will be stored.
- **Access User Name**: the User name used to log in the Network share. Leave this blank if it is not required. In general, you use the administrator account on PC as a user name here.
- **Access Password**: the password used to log into the network share. Leave this blank if it is not required.

5. If the configuration is correct, you can see the NETDISK status shown as below.

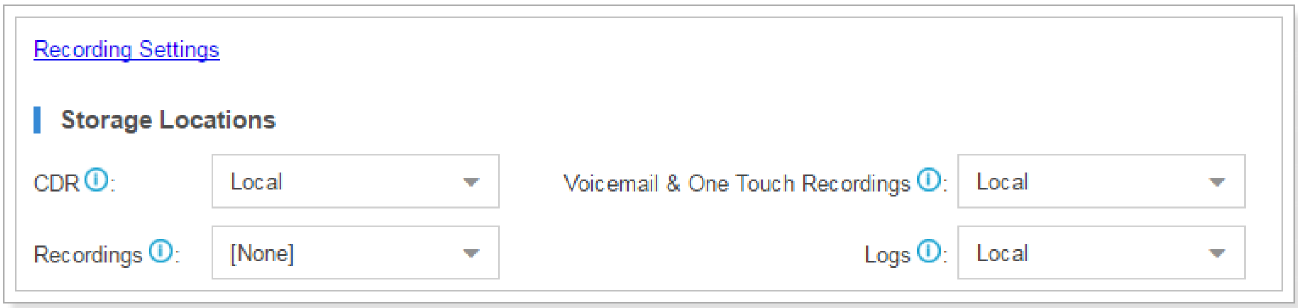


Catherine	NETDISK	120.01G	90.87G	24%	⚙	🗑

Figure 3-14 Network Drive Status

Storage Locations

When the storage devices are configured and ready to use, you can select where to store CDR, Recordings, Voicemail, one-touch recordings, logs.



Recording Settings

Storage Locations

CDR ⓘ: Local

Voicemail & One Touch Recordings ⓘ: Local

Recordings ⓘ: [None]

Logs ⓘ: Local

Figure 3-15 Storage Locations

Auto Cleanup

Yeastar K2 supports auto clean for CDR, logs, voicemails, one-touch recordings and recordings.

Table 3-9 Auto Cleanup Settings

CDR Auto Cleanup	
Max Number of CDR	Set the maximum number of CDR that should be retained. The default is 500,000. 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. The default is left blank.
Voicemail and One Touch Recording Auto Cleanup	
Max Number of Files	Set the maximum number of voicemail and one touch recording files that should be retained. The default is 50. The old CDR will be deleted when the threshold is reached.
Files Preservation Duration	Set the maximum number of minutes that voicemails and one touch recordings should be retained. The default is left blank.
Recordings Auto Cleanup	
Max Usage of Device	Set the maximum storage percentage the device is allowed to store. The default is 80%. The recordings will be deleted when the threshold is reached.
Recordings Preservation Duration	Set the maximum number of days that recording files should be retained. The default is left blank.
Logs Auto Cleanup	
Logs Preservation Duration	Set the maximum number of days that logs should be retained. “Logs Preservation Duration”. The default is 7. This setting is for system log.
Max Number of Logs	Set the maximum number of logs that should be retained. The default is unlimited. The old logs will be deleted when the threshold is reached. This setting is for operation logs.

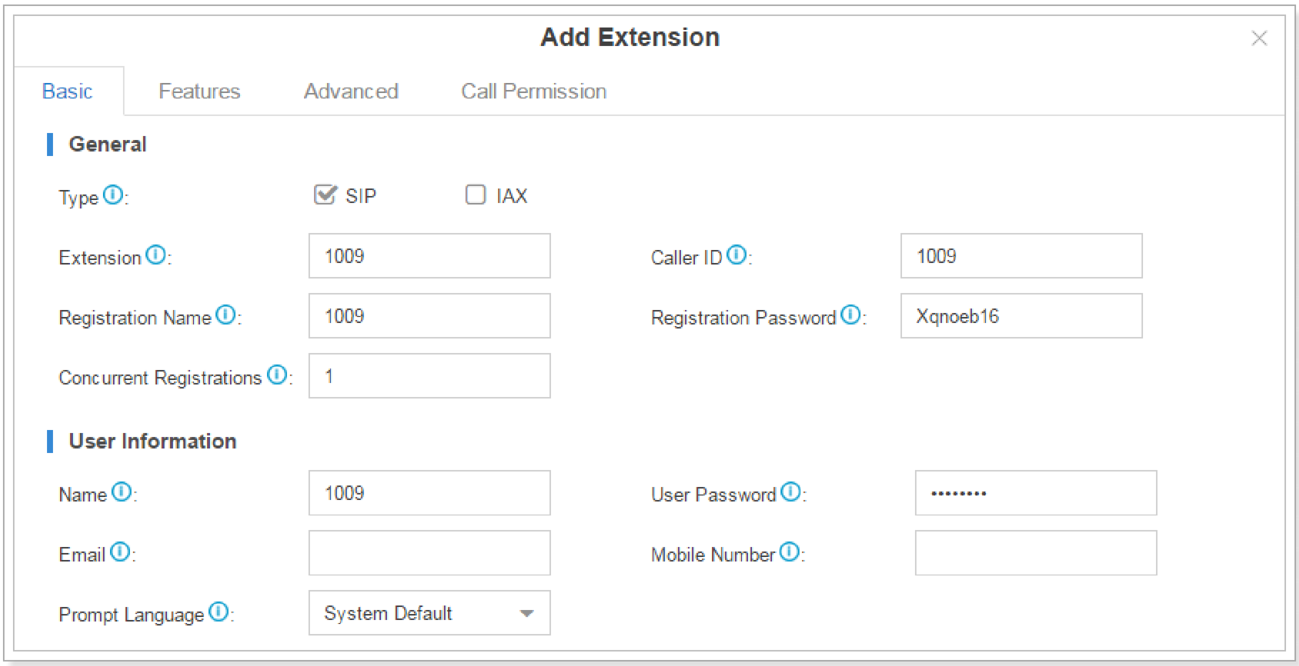
Extensions

This chapter explains how to create and configure extensions on K2. Yeastar K2 supports SIP and extensions. An extension can be set to the 2 types and be registered to different devices. Go to **PBX > Extensions** page to configure the extensions.

- Add New Extension
- Add Bulk Extensions
- Search and Edit Extensions
- Import and Export Extensions
- Extension Group

Add New Extension

Click Add to add a new extension, you will see the pop-up window appear as below.



Add Extension

General

Type: ☑ SIP ☐ IAX

Extension:	1009	Caller ID:	1009
Registration Name:	1009	Registration Password:	Xqnoeb16
Concurrent Registrations:	1		

User Information

Name:	1009	User Password:	••••••••
Email:		Mobile Number:	
Prompt Language:	System Default		

Figure 4-1 Add New Extension

Extension settings are divided to 4 categories:

- Basic
- Feature
- Advanced
- Call Permission

Click on the tab to view or edit the relevant settings. Check the configuration parameters below.

Note: different settings would appear for different types of extension.

- **Basic Settings**

Table 4-1 Extension Configuration Parameters – Basic

General	
Type	Check the box to set the extension type. You can set the extension to multiple types. ● SIP ● IAX
Extension	The extension number that will be associated with this particular user or phone.
Caller ID	The Caller ID string that appears on outbound calls for this extension.
Registration Name	For extension registration validation.
Registration Password	The password for the user to register the SIP or IAX account. For example, 12t3f6.
Concurrent Registrations	Yeastar K2 IP PBX supports SIP forking. **SIP forking** refers to the process of “forking” a single SIP call to multiple SIP endpoints. The value of Concurrent Registrations limits how many SIP endpoints the extension can be registered.
User Information	
Name	A character-based name for this user. For example, Bob Jones.
User Password	The password for this extension user to log in the system. For example, 12t3f6.
Email	Email address of this extension user. The email will be used to recover password, receive forwarding voicemails, receive fax as an attachment, and receive event notifications.
Mobile Number	Mobile Number of this user. The number can receive forwarded calls and event notifications.
Prompt Language	The language of voice prompts. The default is the same with system language. If more language options are needed, please download it from "System Prompts" under "Voice Prompts".

- **Features**

Table 4-2 Extension Configuration Parameters – Features

Voicemail	
Enable Voicemail	Check this box to enable voicemail for this extension.
Send Voicemail to Email	Check this box to send voicemail to the user's email address. Note: to use this feature, "Email Settings" under "System" need to be configured correctly.
Voicemail Access PIN	Voicemail password used to access Voicemail system. This password can contain only numbers.
Call Forwarding	

Always	Always redirect the call to the designated destination. • Voicemail: redirect the caller to leave a voice message. • Extension: redirect the caller to another extension. • Users' Mobile Number: redirect the caller to the mobile number filled in User Information. • Custom Number: fill in the number manually and redirect the caller to this number.
No Answer	Redirect the call to the designated destination when it is not answered.
When Busy	Redirect the call when the extension is busy.
Mobility Extension	
Enable Mobility Extension	If you enable this setting, when the User's Mobile Number dial into the system, the phone will have the same user permission with the desktop extension. So the mobile number will be able to reach the other extension, dial out with the trunk, and play voicemail.
Mobility Extension	It is the same with the User's Mobile Number. A prefix matching the outbound route also needs to be filled in.
Ring Simultaneously	When the extension has an incoming call, it rings the mobile number simultaneously.
Monitor Settings	
Allow Being Monitored	Check this option to allow this user to be monitored.
Monitor Mode	Decide how you will monitor another extension's current call. • None: you will not be allowed to monitor other's call. • Extensive: all the following 3 modes will be available to use. • Listen: you can only listen to the call, but can't talk (default feature code: *90). • Whisper: you can talk to the extension you're monitoring without being heard by the other party (default feature code: *91). • Barge-in: you can talk to both parties (default feature code: *92).
Other Settings	
Ring Timeout	Customize the timeout in seconds. Phone will stop ringing over the time defined.
Max Call Duration	Select the maximum call duration in seconds for every call of this extension. If you wish to customize, enter the value in the text box directly. This option is valid only for outbound calls. If you choose “Follow System”, it would be equal to the “Max Call Duration” value in the “General” page.
Call Waiting	Check this option if the extension should have Call Waiting capability. If this option is checked, the “When busy” call forwarding options will not be available. The call waiting function of IP phone has higher priority than MyPBX call waiting function.

DND	Don’t Disturb. When DND is enabled for an extension, the extension will not be available.

- **Advanced Settings**

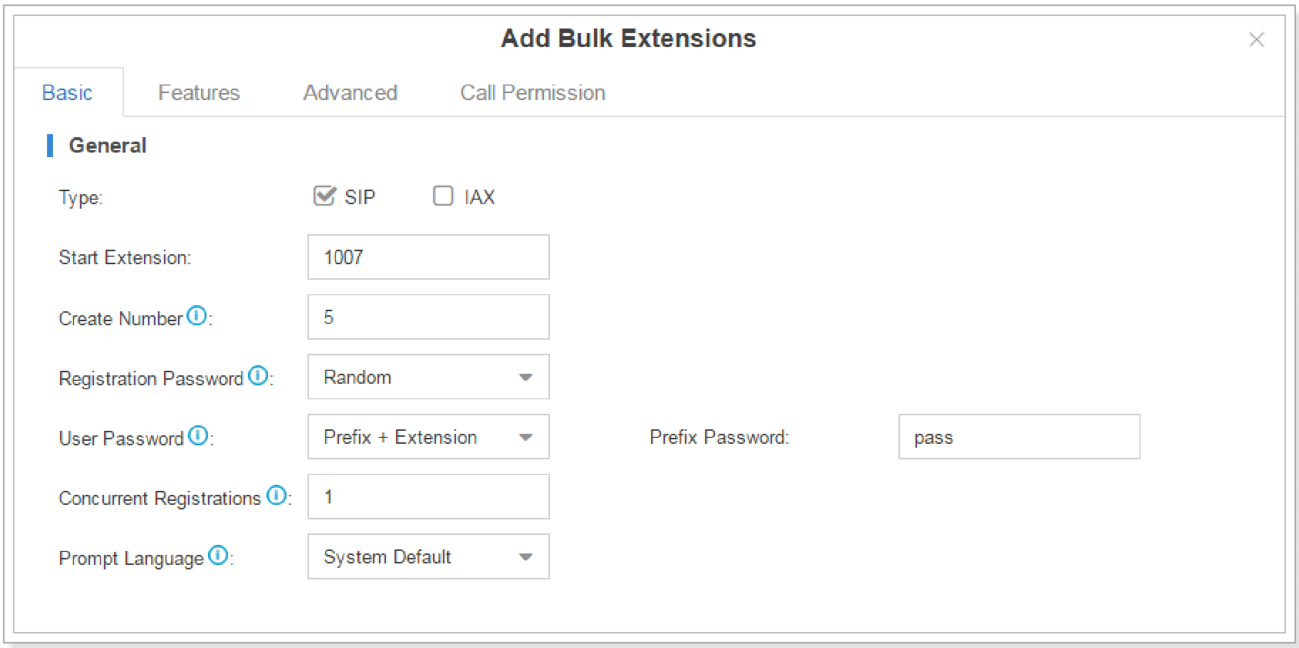
Table 4-3 Extension Configuration Parameters – Advanced

VoIP Settings	
NAT	This setting should be used when the system is using a public IP address, communicating with devices hidden behind a NAT device (such as a broadband router). If you have one-way audio problems, you usually have problems with your NAT configuration or your firewall's support of SIP and/or RTP ports.
Qualify	Check the box to send SIP OPTIONS regularly to the device to check if the device is still online.
Enable SRTP	Enable SRTP for voice encryption.
Register Remotely	Check the box to allow registration of a remote extension.
Transport	Select the allowed transport.
DTMF Mode	Set the default mode for sending DTMF tones. ● RFC4733: 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: will use RFC4733 or Info automatically. RFC4733 is the default mode.
IP Restriction	
Enable IP Restriction	This option is used for IP access control. Check this option to enhance the VoIP security. Once enabled, only the IP address or IP section match the settings will be able to register this extension number.
Permitted IP/Subnet mask	Define the IP address or IP section which is allowed to register to the PBX. The input format should be IP address/Subnet mask. **Example:** ● 192.168.5.100/255.255.255.255 means only the device whose IP address is 192.168.5.100 is allowed to register this extension number; ● 192.168.5.0/255.255.255.0 means only the device whose IP section is 192.168.5.XXX is allowed to register this extension number.

- **Call Permission**
  Choose the outbound routes the user is allowed to use.

Add Bulk Extensions

You can batch add SIP/IAX extensions on the system, which help you add a large amount of extensions quickly. Click Bulk Add to add extensions in bulk.



Add Bulk Extensions

General

Type: ☑ SIP ☐ IAX

Start Extension: 1007

Create Number: 5

Registration Password: Random

User Password: Prefix + Extension

Prefix Password: pass

Concurrent Registrations: 1

Prompt Language: System Default

Figure 4-3 Add Bulk Extensions

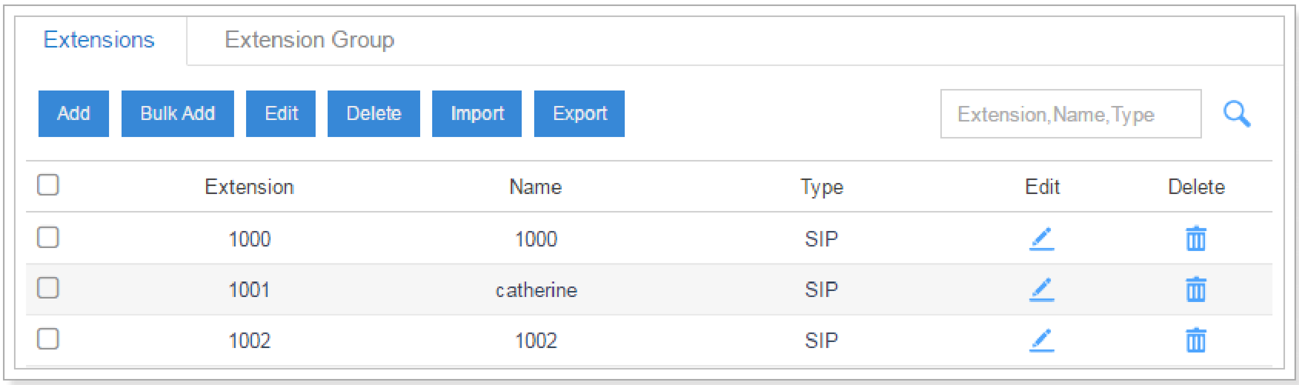
Table 4-4 Bulk Add Extensions Configuration Parameters

General	
Type	Choose the type for the extensions: • SIP • IAX
Start Extension	Set the starting extension number of the batch of extensions to be added.
Create Number	The number of extensions to be created.
Register Password	Decide which type of registration password will be used. There are 3 options. • Random: generate a random password for each extension. • Fixed: use the text filled in as the password for all extensions. • Prefix + extension number: fill in a prefix and the password will be the text plus the extension's number.
User Password	Decide which type of user password will be used. There are 3 options. • Extension: use extension number as password for each extension. • Fixed: use the text filled in as the password for all extensions. • Prefix + extension number: fill in a prefix and the password will be the text plus the extension’s number.

Concurrent Registrations	Set the max concurrent registrations for SIP extensions.
Prompt Language	Set the language of voice prompt for extensions.

Search and Edit Extensions

All the extensions are listed on the extension page. Each extension has a checkbox for you to edit or delete in bulk. Also, you can edit or delete per extension by clicking ✎ or 🗑.



□	Extension	Name	Type	Edit	Delete
□	1000	1000	SIP	✎	🗑
□	1001	catherine	SIP	✎	🗑
□	1002	1002	SIP	✎	🗑

Figure 4-4 Extensions List

- **Search Extension**
  You can search extensions by entering the extension number, name or type.
- **Edit an Extension**

  Click ✎ to edit the desired extension.
- **Delete an Extension**

  Click 🗑 to delete the desired extension.
- **Bulk Edit Extensions**

  Select the checkbox for the extensions, click Edit to edit the extensions.
- **Bulk Delete Extensions**

  Select the checkbox for the extensions, click Delete to delete the extensions.

Importing and Exporting Extensions

Users could import and export extension configurations, which helps you manage extensions easily.

To Import Extensions

1. Click Import, you will see a dialog window shown as below.

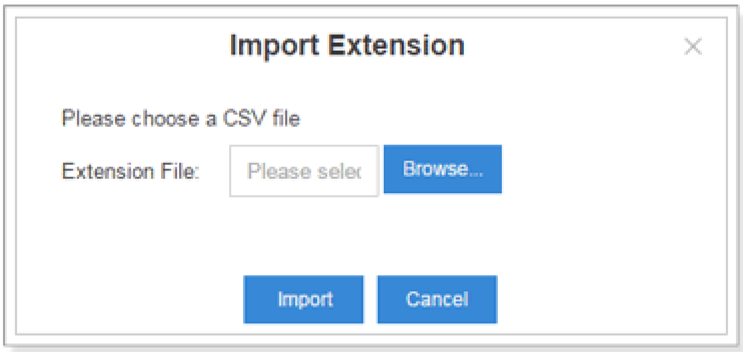
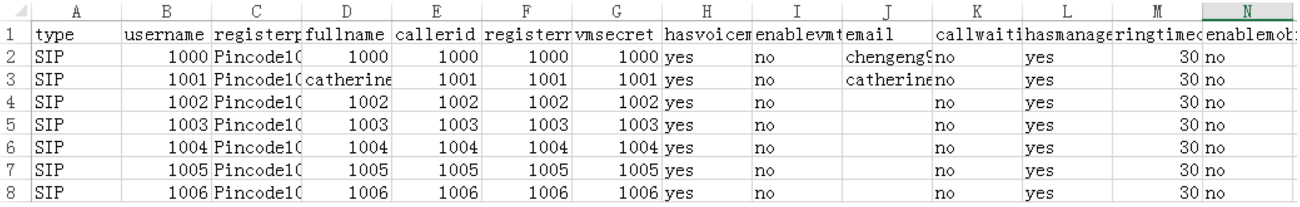


Figure 4-5 Import Extensions

2. Click **Browse** and select the file to start uploading. The file must be a .csv file. Check the sample file below. You can export an extension file from the PBX and use it as a sample to start with.

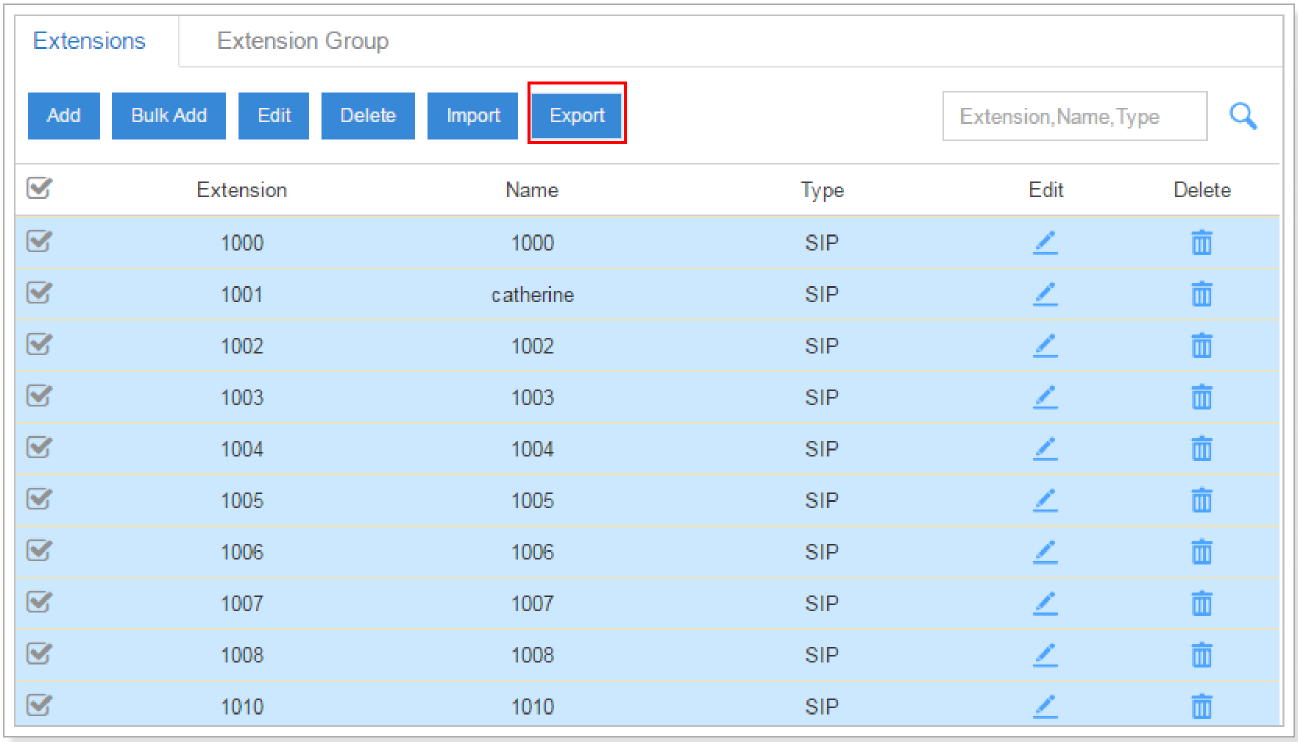


	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	type	username	registerp	fullname	callerid	registerr	vmsecret	hasvoicem	enablevmt	email	callwaiti	hasmanage	ringtimec	enablemob
2	SIP	1000	Pincode1(	1000	1000	1000	1000	yes	no	chengeng§	no	yes	30	no
3	SIP	1001	Pincode1(	catherine	1001	1001	1001	yes	no	catherine	no	yes	30	no
4	SIP	1002	Pincode1(	1002	1002	1002	1002	yes	no		no	yes	30	no
5	SIP	1003	Pincode1(	1003	1003	1003	1003	yes	no		no	yes	30	no
6	SIP	1004	Pincode1(	1004	1004	1004	1004	yes	no		no	yes	30	no
7	SIP	1005	Pincode1(	1005	1005	1005	1005	yes	no		no	yes	30	no
8	SIP	1006	Pincode1(	1006	1006	1006	1006	yes	no		no	yes	30	no

Figure 4-6 Sample Extension File

To Export Extensions

Select the checkbox of the extensions, click Export, the selected extensions would be exported to your local PC.



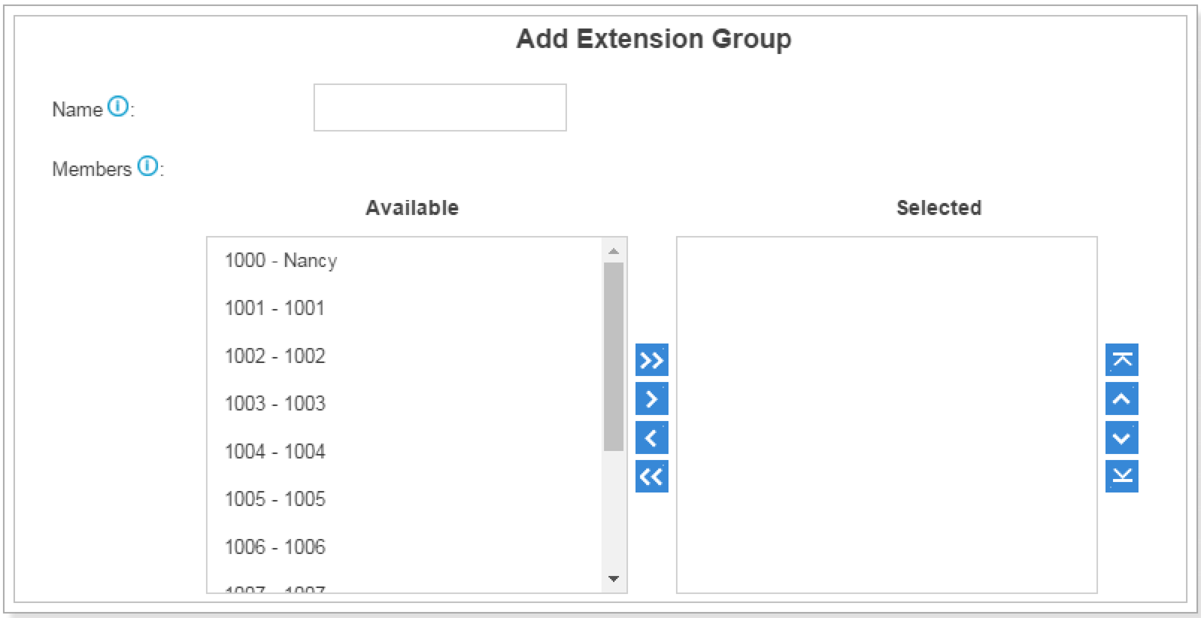
☑	Extension	Name	Type	Edit	Delete
☑	1000	1000	SIP	✎	🗑
☑	1001	catherine	SIP	✎	🗑
☑	1002	1002	SIP	✎	🗑
☑	1003	1003	SIP	✎	🗑
☑	1004	1004	SIP	✎	🗑
☑	1005	1005	SIP	✎	🗑
☑	1006	1006	SIP	✎	🗑
☑	1007	1007	SIP	✎	🗑
☑	1008	1008	SIP	✎	🗑
☑	1010	1010	SIP	✎	🗑

Figure 4-8 Export Extensions

Extension Group

Extension Group feature allows you to assign and categorize extensions in different groups, which helps you to better manage the configurations in the system. For example, you can create Support and Sales groups, when configuring Outbound Route, you can select an extension group instead of each extension. This feature simplifies the configuration process.

Click Add to create an extension group.



Add Extension Group

Name ⓘ:

Members ⓘ:

Available

1000 - Nancy
1001 - 1001
1002 - 1002
1003 - 1003
1004 - 1004
1005 - 1005
1006 - 1006
1007 - 1007

Selected

Figure 4-9 Add Extension Group

Trunks

Yeastar K2 supports VoIP trunk. In this chapter, we give a simplified guide of setting up VoIP trunks.

VoIP Trunk

Yeastar K2 supports SIP and IAX protocols and provides 2 types of VoIP trunks:

- **Register Trunk:** registration based VoIP trunk. A Register Trunk requires K2 to register with the provider using an authentication name and password.
- **Peer Trunk:** IP based VoIP trunk. A Peer VoIP trunk does not require K2 to register with the provider. The IP address of K2 needs to be configured with the provider, so that it knows where calls to your number should be routed.

Go to **Settings > PBX > Trunks** to add a VoIP trunk.

Note:

- Choosing different trunk protocol would have different settings.

1) Basic Settings

Table 5-1 SIP Register Trunk Configuration Parameters - Basic

SIP Register Trunk	
Trunk Status	Enable or disable the trunk. If the trunk is disabled, it would be unavailable in K2 PBX.
Protocol	Set the trunk protocol "SIP".
Trunk Type	Choose the trunk type "Register Trunk".
Provider Name	Give this trunk a name to help you identify this trunk.
Transport	Set the transport method used by the trunk. If Hostname/IP Address is the PBX's Hostname and the port is 0 or blank, NAPTR and SRV lookup will be executed to search for transport, port and server. If Hostname/IP Address is a legal IP address or a designated port, then UDP will be used.
Hostname/IP	Service provider's hostname or IP address. The default SIP port is 5060.
Domain	VoIP provider's server domain name. If the provider has no domain name, fill in the IP address instead.
User Name	The username used to register to the trunk from the VoIP provider.
Password	The password to register to the trunk from the VoIP provider.
From User	All outgoing calls from the SIP trunk will use the From User (in this case the account name for SIP Registration) in From Header of the SIP Invite package. Keep this field blank if not needed.

Authentication Name	Used for SIP authentication. In most cases, it is the same with the username.
Enable Outbound Proxy	A proxy that receives requests from a client. Even though it may not be the server resolved by the Request-URI.
Outbound Proxy Server	Configure the address of outbound proxy server. The address can be domain name or IP address.
Enable SLA	If enabled, this trunk will not be available in routes or other channels.
Allow Barge	Whether to allow other SLA stations to join a call by pressing the SLA key.
Hold Access	Specify hold permission for the station. ● **Open:** other stations that share the same line could retrieve the call. ● **Private:** the call can be retrieved only by the station that previously put the call on hold, not by others sharing the same line.

Table 5-2 SIP Peer Trunk Configuration Parameters - Basic

SIP Peer Trunk	
Protocol	Set the trunk protocol as "SIP".
Trunk Type	Choose the trunk type "Peer Trunk".
Provider Name	Give this trunk a name to help you identify this trunk.
Transport	Set the transport method used by the trunk. If Hostname/IP Address is the PBX's Hostname and the port is 0 or blank, NAPTR and SRV lookup will be executed to search for transport, port and server. If Hostname/IP Address is a legal IP address or a designated port, then UDP will be used.
Hostname/IP	Service provider's hostname or IP address. The default SIP port is 5060.
Domain	VoIP provider's server domain name. If the provider has no domain name, fill in the IP address instead.
Enable SLA	If enabled, this trunk will not be available in routes or other channels.
Allow Barge	Whether to allow other SLA stations to join a call by pressing the SLA key.
Hold Access	Specify hold permission for the station. ● **Open:** other stations that share the same line could retrieve the call. ● **Private:** the call can be retrieved only by the station that previously put the call on hold, not by others sharing the same line.

Table 5-3 IAX Register Trunk Configuration Parameters - Basic

IAX Register Trunk	
Protocol	Set the trunk protocol “IAX”.
Trunk Type	Choose the trunk type “Register Trunk”.
Provider Name	Give this trunk a name to help you identify this trunk.
Hostname/IP	Service provider’s hostname or IP address. The default IAX port is 4569.
User Name	The username used to register to the trunk from the VoIP provider.
Password	The password to register to the trunk from the VoIP provider.

Table 5-4 IAX Peer Trunk Configuration Parameters - Basic

IAX Peer Trunk	
Protocol	Set the trunk protocol “IAX”.
Trunk Type	Choose the trunk type “Peer Trunk”.
Provider Name	Give this trunk a name to help you identify this trunk.
Hostname/IP	Service provider’s hostname or IP address. The default IAX port is 4569.
Domain	VoIP provider’s server domain name. If the provider has no domain name, fill in the IP address instead.

2) **Codec**

Select codec for the VoIP trunk. Yeastar K2 supports the codecs: a-law, u-law, GSM, iLBC, SPEEX, G722, G726, ADPCM, G729A, H261, H263, H263P, H264, MPEG4 and iLBC.

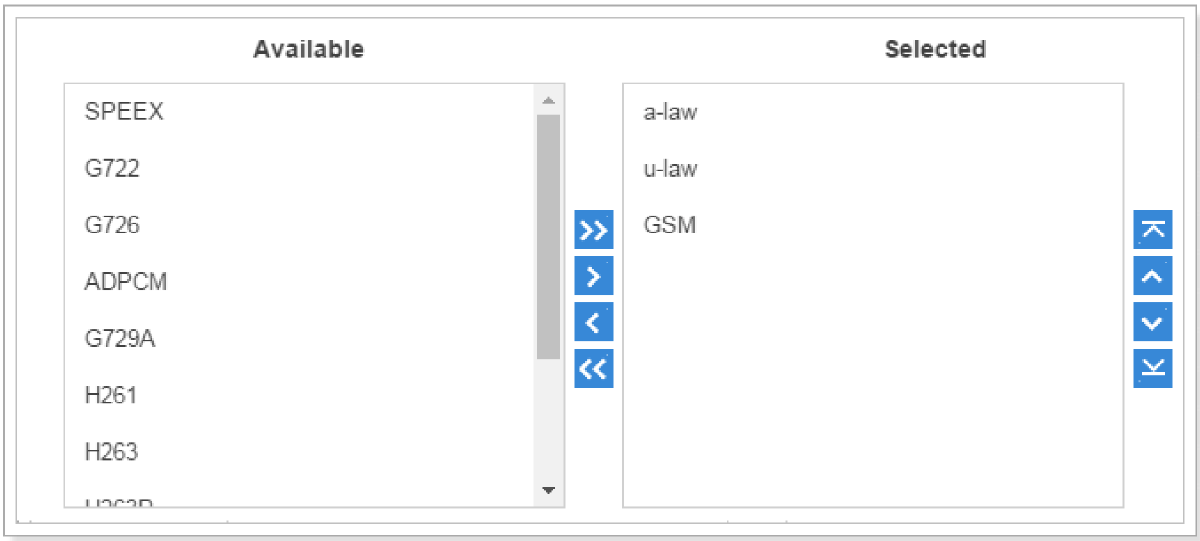


Figure 5-1 VoIP Trunk Codec

3) Advanced

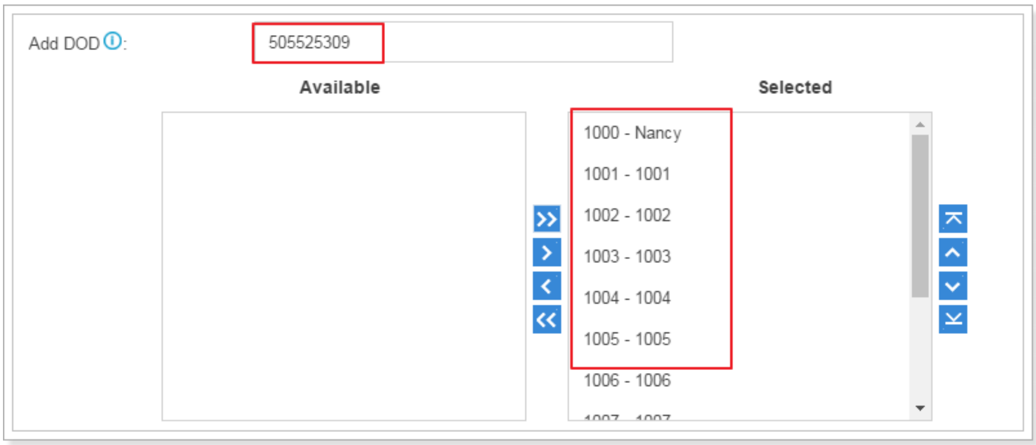
Table 5-12 VoIP Trunk Configuration Parameters - Advanced

VoIP Settings	
Qualify	Enable this to send SIP OPTIONS packet to SIP device to check if the device is up.
Enable SRTP	This option enables or disable SRTP (encrypted RTP) for the trunk.
T.38 Support	Whether to enable T.38 fax for the trunk.
DTMF Mode	Set the default mode for sending DTMF tones. • RFC4733: 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: will attempt to detect if the device supports RFC4733 DTMF. If so, it will choose RFC4733; if not, it will choose Inband. RFC4733 is the default mode.
Other Settings	
Realm	Realm is a string to be displayed to users so they know which username and password to use. If you don’t know what to fill in, contact your service provider for further instructions.
Send Privacy ID	Check this checkbox to send privacy ID.
Enable DNIS	Dialed Number Identification Service is a telephone service that enables a company to identify which telephone number was dialed. Users could configure DNIS to allow the IP phones to display which trunk is passing the call.
DID Number	This number is used to identify which line of the trunk is passing the call.
DNIS Name	A name for this DNIS, when a call reaches the selected trunk, the name will be displayed on the ringing phone.

4) DOD

DOD (Direct Outward Dialing) means the caller ID displayed when dialing out. Before configuring this, please make sure the provider supports this feature.

- **Global DOD**
  Configure Global direct outward dialing number. DOD (Direct Outward Dialing) is the caller ID displayed when dialing out. Before configuring this, please make sure the carrier supports this feature.
- **Add One DOD with Multiple Extensions**
  Enter one DOD number and select multiple extensions.



Add DOD: 505525309

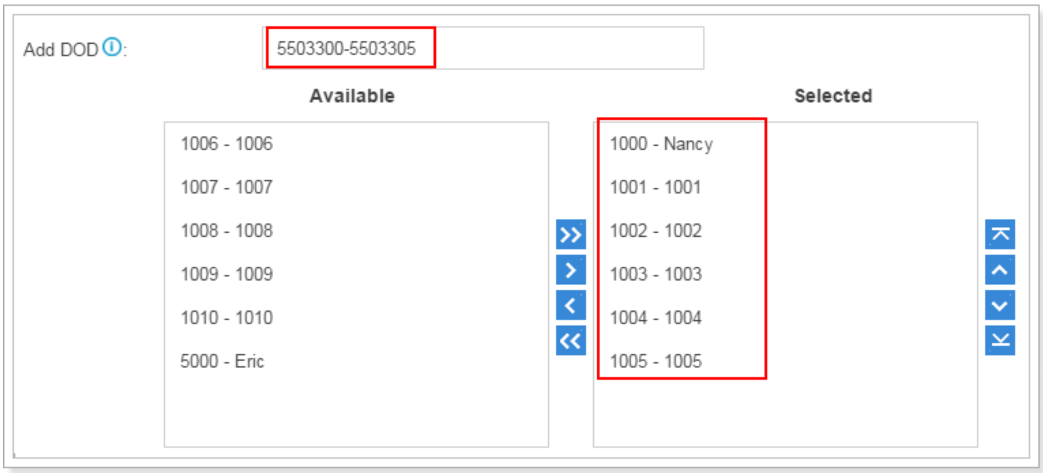
Available

Selected

1000 - Nancy
1001 - 1001
1002 - 1002
1003 - 1003
1004 - 1004
1005 - 1005
1006 - 1006

Figure 5-2 Add One DOD with Multiple Extensions

- **Bind Consecutive DOD Numbers to Multiple Extensions**
  Enter the DOD number range and select the extensions.



Add DOD: 5503300-5503305

Available

1006 - 1006
1007 - 1007
1008 - 1008
1009 - 1009
1010 - 1010
5000 - Eric

Selected

1000 - Nancy
1001 - 1001
1002 - 1002
1003 - 1003
1004 - 1004
1005 - 1005

Figure 5-3 Bind Consecutive DOD Numbers to Multiple Extensions

Call Control

This chapter shows you how to control outgoing calls and incoming calls.

- Inbound Routes
- Outbound Routes
- Auto CLIP Routes
- SLA
- Time Conditions

Inbound Routes

When a call comes into K2 from the outside, K2 needs to know where to direct it. It can be directed to an extension, a ring group, a queue or a digital Receptionist (IVR) etc.

Go to **Settings** > **PBX** > **Call Control** > **Inbound Routes** to edit inbound routes.
Please check the inbound route configuration parameters below.

1) **Route Name**
   Give this inbound route a brief name to help you identify it.
2) **DID Pattern**
   Match the DID Pattern in this field to pass incoming call through. Leave this blank to match calls with any or no DID info. You can use a pattern match to map a range of numbers. In patterns, the following characters have special meanings:

Table 6-1 DID Patterns Description

Patterns	
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, example [123] is 1 or 2 or 3. Note that multiple numbers can be separated by commas and ranges of numbers can be specified with a dash ([1.3.6-8]) would match the numbers 1,3,6,7 and 8.
. (dot)	Wildcard. Match any number of anything.
!	Used to initiate call processing as soon as it can be determined that no other matches are possible.

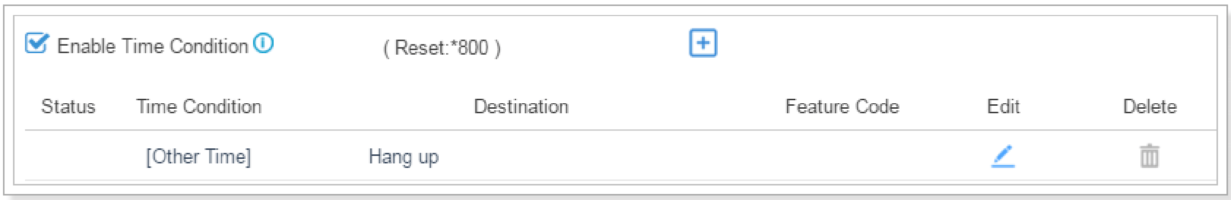
If you want to route consecutive DID numbers to a range of consecutive extensions directly through SIP, SIP Peer to Peer, IAX Peer to Peer trunk, you need to enter the DID number range (separate the first number and the last number by "-"), choose the Destination as Extension Range, and fill in the relevant extension numbers (separated by "-").

3) **Caller ID Pattern**
Define the Caller ID Number that is allowed to call in through this inbound route. Leave this field blank to match any or no CID info. You can also use patterns match to map a range of numbers. Press Enter to input multiple patterns.

4) **Member Trunks**
Select which trunks will be used in this route. To make a trunk a member of this route, please move it to the "Selected" box.

5) **Enable Time Condition**
Decide if you want to route incoming calls based on Time Condition.

- If disabled, all calls will be routed to the Destination.
- If enabled, you could route calls to different destinations at different time. Calls that do not match the time periods will be routed to "Other Time" destination. The system will assign each Time Condition with a feature code, so you could use this code to force change the destination of a Time Condition and restore to its original destination.



☑ Enable Time Condition ⓘ (Reset:*800) ⊞

Status	Time Condition	Destination	Feature Code	Edit	Delete
	[Other Time]	Hang up		✎	🗑

Figure 6-1 Time Condition

6) **Distinctive Ring Tone**
The system supports mapping to custom ring tone files. For example, if you configure the distinctive ringing for custom ring tone to "Family", the ring tone will be played if the phone receives the incoming call.

7) **Fax Detection**
Decide if you want to enable Fax Detection.

- If disabled, the system will not detect fax tone nor will it send fax tone.
- If enabled, the system will send the fax to Fax Destination if a fax tone is detected.

Fax Destination
Sets the destination where to send the fax to. You can set it to:

- Extension: send the fax to the designated extension. If it is a FXS extension, the fax will be sent to the FXS fort (fax machine).
- Fax to Email: sent the fax as an email attachment to the designated email address, which could be associated to an extension or a custom one.
  Note: please make sure the sender email address is correctly configured in "System > Email".

Outbound Routes

An outbound route works like a traffic cop giving directions to road users to use a predefined route to reach a predefined destination. Outbound routes are used to specify what numbers are allowed to go out a particular route. When a call is placed, the actual number dialed by the user is compared with the dial patterns in each route (from highest to lowest priority) until a match is found. If no match is found, the call fails. If the number dialed matches a pattern in more than one route, only the rules with the highest priority in the route are used.

Note:

- Yeastar K2 compares the number with the pattern that you have defined in your route 1. If matches, it will initiate the call using the selected trunks. If it does not, it will compare the number with the pattern you have defined in route 2 and so on. The outbound route which is in a higher position will be matched firstly.
- Adjust the outbound route sequence by clicking these buttons ⤒ ⋀ ⋁ ⤓.

Go to **Settings** > **PBX** > **Call Control** > **Outbound Routes** to edit outbound routes.
Please check the outbound route configuration parameters below.

1) **Route Name**
   Give this outbound route a brief name to help you identify it.
2) **Dial Patterns**
   Outbound calls that match this dial pattern will use this outbound route.

Table 6-2 Dial Patterns Description

Patterns	
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, example [123] is 1 or 2 or 3. Note that multiple numbers can be separated by commas and ranges of numbers can be specified with a dash ([1.3.6-8]) would match the numbers 1,3,6,7 and 8.
. (dot)	Wildcard. Match any number of anything.
!	Used to initiate call processing as soon as it can be determined that no other matches are possible.
Strip	
Allow the users to specify the number of digits that will be stripped from the front of the phone number before the call is placed. For example, if users must press 0 before dialing a phone number, one digit should be stripped from the dial string before the call is placed.	
Prepend	
Digits to prepend to a successful match. If the dialed number matches the patterns, then this will be prepended before sending to the trunks. For example if a trunk requires 10-digit dialing, but users are more comfortable with 7-digit dialing, this field could be used to prepend a 3-digit area code to all 7-digit phone numbers before the calls are placed. When using analog trunks, a “w” character may also be prepended to provide a slight delay before dialing.	

3) **Member Trunks**
Select which trunks will be used in this route.

4) **Member Extensions**
Select extensions that will be permitted to use this outbound route.

5) **Password**
You can prompt users for a password before allowing calls to progress. The options are:

- None
- PIN List: select a list of PIN
- Password: enter a single password which will be needed when dialing through this outbound route

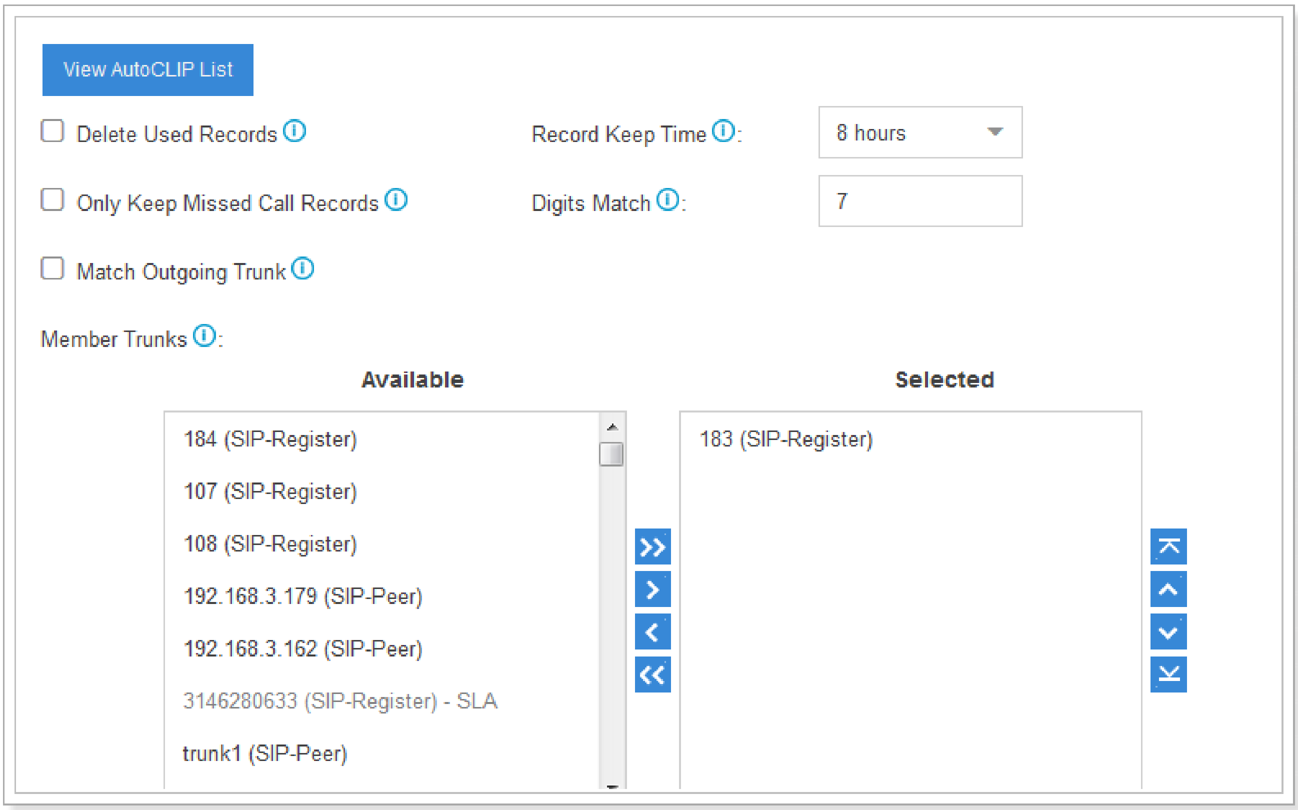
6) **Rrmemory Hunt**
Round robin with memory, remembers which trunk was used last time, and then use the next available trunk to call out.

7) **Time Condition**
This defines the time conditions to use this outbound route.

Auto CLIP Routes

The system automatically stores information about outgoing calls to the AutoCLIP routing table. When a person calls back the call is routed directly to the original number.

Go to **Settings** > **PBX** > **Call Control** > **Auto CLIP Routes** to configure Auto CLIP:



☐ Delete Used Records ⓘ

Record Keep Time ⓘ: 8 hours

☐ Only Keep Missed Call Records ⓘ

Digits Match ⓘ: 7

☐ Match Outgoing Trunk ⓘ

Member Trunks ⓘ:

Available	Selected
184 (SIP-Register)	183 (SIP-Register)
107 (SIP-Register)	
108 (SIP-Register)	
192.168.3.179 (SIP-Peer)	
192.168.3.162 (SIP-Peer)	
3146280633 (SIP-Register) - SLA	
trunk1 (SIP-Peer)	

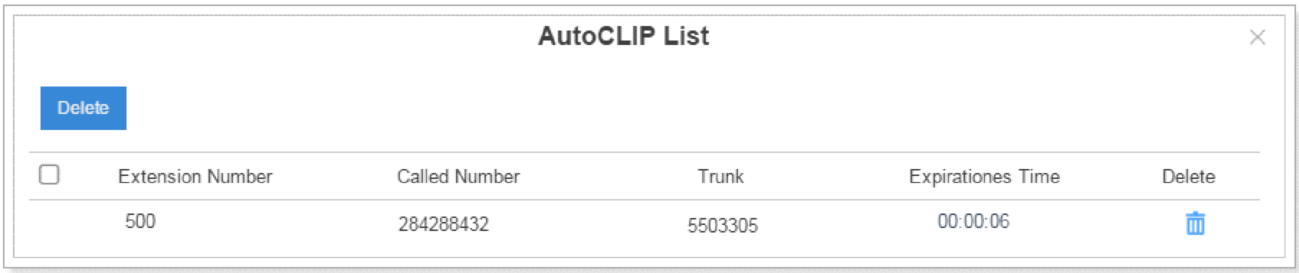
Figure 6-2 Auto CLIP Route

- **Delete Used Records:** when an AutoCLIP record is matched, the record will be automactically deleted afterwards.
- **Record Keep Time:** set the time duration for which records should be kept in the AutoCLIP List. Default is 8 hours.
- **Only Keep Missed Call Records:** the system will only keep records of calls that are not answered in AutoCLIP list.

- **Digits Match:** define how many digits from the last digit of the incoming phone number will be used to match the AutoCLIP record. For example, you need to set this option if the incoming phone number has a prefix '+'.

- **Match Outgoing Trunk:** if enabled, only the incoming call that came to the PBX through the same trunk which made the call will be match against the AutoCLIP List.
- **Member Trunks:** choose the trunks, AutoCLIP Route will apply to the selected trunks.

Click **View AutoCLIP List** to view the records. In the AutoCLIP List you can see the AutoCLIP records.



□	Extension Number	Called Number	Trunk	Expirationes Time	Delete
	500	284288432	5503305	00:00:06	🗑

Figure 6-3 Auto CLIP List

As the above figure shows, when the user (284288432) has a missed call and returns the call, he will be directly forwarded to extension 500 as shown in the AutoCLIP List.

SLA

Shared Line Appearance (SLA) feature helps users share SIP trunks. It also helps monitor the status of the shared line. SLA feature works with BLF key on IP phones.

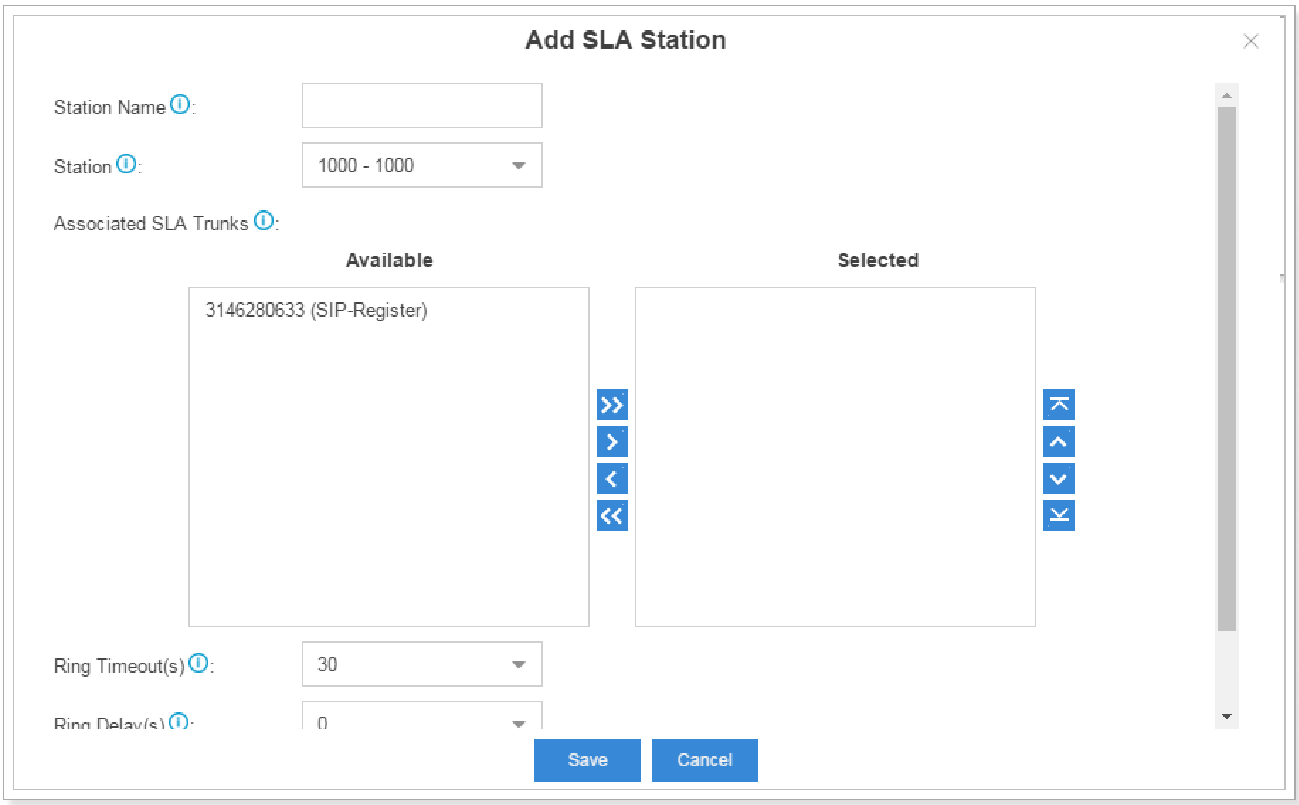
- When an incoming call is received, all the SLA stations are informed of it and may join it if the shared line allows to barge in.
- When an outgoing call is made by one SLA station, all members shared with the same line are informed about the call, and will be blocked from this line appearance until the line goes back to idle or the call is put on hold.

To use SLA, you need do the following:

✓ Enable SLA feature on a VoIP trunk.

- ✓ Create SLA Stations.
- ✓ Configure BLF keys for the shared line on the stations' IP phones. The BLF key value is "**extension number_trunkname**".

Go to **Settings** > **PBX** > **Call Control** > **SLA**, click Add to create SLA stations.



Add SLA Station

Station Name ⓘ:

Station ⓘ: 1000 - 1000

Associated SLA Trunks ⓘ:

Available	Selected
3146280633 (SIP-Register)	

Ring Timeout(s) ⓘ: 30

Ring Delay(s) ⓘ: 0

Figure 6-4 Add SLA Station

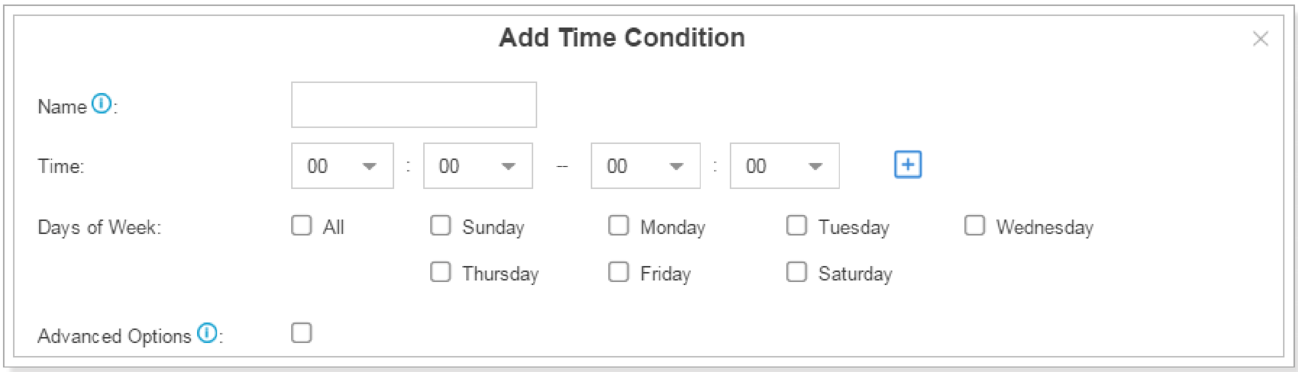
- **Station Name:** set a name for the SLA name.
- **Station:** choose a SIP extension to monitor and use the SLA trunks.
- **Associated SLA Trunks:** choose the SLA trunks.
- **Ring Timeout:** set the ring timeout in seconds, phone will stop ringing after the time defined.
- **Ring Delay:** set the delay time in seconds. Phone will delay ringing after the time defined. This time couldn't be longer than "Ring Timeout".
- **Hold Access:** specify hold permission for the station.
  - **Open:** any station can place this trunk on hold and any other station is allowed to take it back off of hold.
  - **Private:** only the station that placed the trunk on hold is allowed to take it back off of hold.

Time Conditions

On Time Condition page, you can create time groups. A time group is a list of times against which incoming or outgoing calls are checked. The rules specify a time range, by the time, day of the week, day of the month, and month of the year. Time conditions can be assigned to an inbound route, which control the destination of a call based on the time. Time conditions can also be assigned to an outbound route in order to limit the use of that route.

Add Time Condition

Go to **Settings** > **PBX** > **Call Control** > **Time Conditions**, click Add Time Condition to add time condition.



Add Time Condition ×

Name ⓘ:

Time: 00 ▾ : 00 ▾ -- 00 ▾ : 00 ▾ ⊞

Days of Week: □ All □ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

Advanced Options ⓘ: □

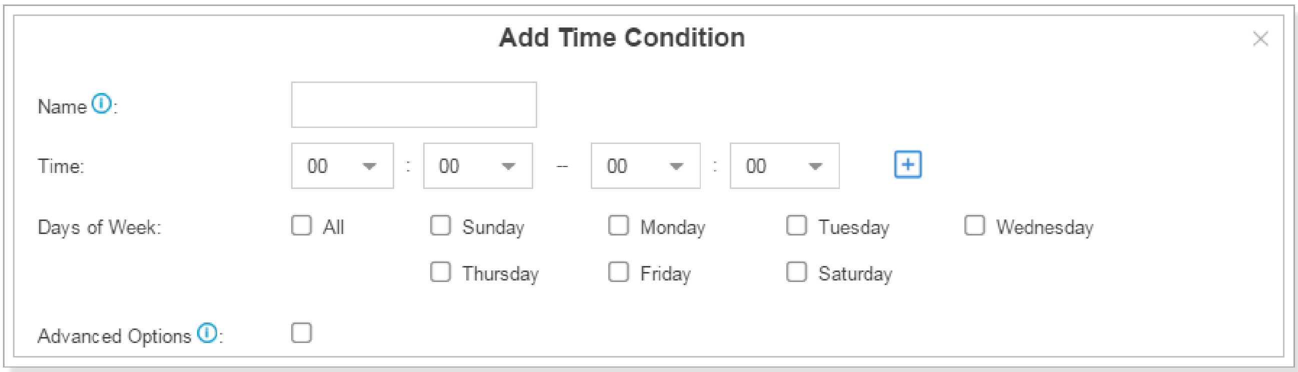
Figure 6-5 Add Time Condition

- **Name**: give this Time Condition a brief name to help you identify it.
- **Time**: this is where you will define a time range. You can define multiple ranges in the same time group by clicking ⊞.
- **Days of Week**: select a week day, month day, and/or month range in which you want this time range to apply.
- **Advanced Options**: this option is disabled by default. If it is enabled, you need to set the month and the day of the month. If it is disabled, it means that the time range defined above will apply to every day of the month, every month of the year.

Add a Holiday

After you have defined your office time conditions, you may need to create a holiday time groups. For example, you want to create a Holiday for Chinese National Day, from October 1st to October 5th.

Click Add Holiday to add a holiday.



Add Time Condition ×

Name ⓘ:

Time: 00 ▾ : 00 ▾ -- 00 ▾ : 00 ▾ ⊞

Days of Week: □ All □ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

Advanced Options ⓘ: □

Figure 6-6 Add Holiday

Assigning Time Conditions to Inbound Routes

The created Time Conditions will become available for selection in the Inbound Routes.

Assigning Time Conditions to Outbound Routes

You can also assign Time Conditions to outbound routes, which may help you to control the route can be used. For example, you can limit the users to make outbound calls when your office is closed.

Call Features

This chapter explains various call features on Yeastar K2.

- IVR
- Ring Group
- Queue
- Conference
- Pickup Group
- Speed Dial
- Callback
- DISA
- Blacklist/Whitelist
- Pin List
- Paging/Intercom

IVR

Like most organizations, where possible, we would like to route incoming calls an Auto Attendant. You can create one or more IVR (Auto Attendant) on K2 to achieve it. When calls are routed to an IVR, K2 will play a recording prompting them what options the callers can enter such as "Welcome to XX, press 1 for Sales and press 2 for Technical Support".

Go to **Settings** > **PBX** > **Call Features** > **IVR** to configure IVR.

- Click Add to add a new IVR.
- Click Delete to delete the selected IVR.
- Click ✎ to edit one IVR.
- Click 🗑 to delete one IVR.

Please check the IVR configuration parameters below.

Table 7-1 IVR Configuration Parameters

Basic Settings	
Number	Yeastar K2 treats IVR as an extension; you can dial this extension number to reach the IVR from internal extensions.
Name	Give this IVR a brief name to help you identify it.
Prompt	The prompt that will be played when the caller reaches this IVR.
Prompt Repeat Count	The number of times that the selected IVR prompt will be played.
Response Timeout	The number of seconds to wait for a digit input after prompt.

Digit Timeout	How long (in seconds) we wait for the caller to enter an option on their phone keypad before we consider it timed out and it follows the Timeout Destination as defined below.
Dial Extension	If this option is enabled, the callers can enter a user's extension number when entering the IVR to go direct to the users.
Dial Outbound Routes	Allow the caller to dial through outbound routes.
Keypress Events	
Key Press Event 0 1 2 3 4 5 6 7 8 9 # * Timeout Invalid	Select the destination for each key pressing: digits 0-9, "#", "*", Timeout and Invalid. When the callers press the corresponding key, the call will be routed to: • Extension • Voicemail • Ring Group • IVR • Conference Room • Queues • Faxes • Dial by Name • Custom Prompt • Hangup

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.

Go to **Settings** > **PBX** > **Call Features** > **Ring Group** to configure ring groups.

- Click Add to add a new ring group.
- Click Delete to delete the selected ring groups.
- Click ✎ to edit one ring group.
- Click 🗑 to delete one ring group.

Please check the ring group configuration parameters below.

Table 7-2 Ring Group Configuration Parameters-General Settings

Option	Description
Number	The extension number dialed to reach this ring group.
Name	Give this ring group a brief name to help you identify it.
Ring Strategy	Select an appropriate ring strategy for this ring group. • Ring All Simultaneously: ring all the available extensions simultaneously. • Ring Sequentially: ring each extension in the group one at a time.
Seconds to ring each member	Set the number of seconds to ring a single extension before moving to the next one.
Members	Choose the member of this ring group
Destination If No Answer	Choose the failover destination.

Queue

Queues are designed to receive 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 K2 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.

Go to **Settings** > **PBX** > **Call Features** > **Queue** to configure queue.

- Click Add to add a new queue.
- Click Delete to delete the selected queues.
- Click ✎ to edit one queue.
- Click 🗑 to delete one queue.

Please check the queue configuration parameters below.

1) Basic Settings

Table 7-3 Queue Configuration Parameters - Basic Settings

Basic Settings	
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 require agents to enter a password before they can login to this queue.
Ring Strategy	This option sets the Ringing Strategy for this Queue. The options are: • Ringing All: ring all available agents simultaneously until one answer. • 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. - Rememory: Round Robin with Memory, remembers where it left off in the last ring pass. - Linear: rings agents in the order specified in the configuration file.
Failover Destination	Set the failover destination.
Static Agents	This selection shows all users. Selecting a user here makes them a dynamic agent of the current queue. The dynamic agent is allowed to log in and log out the queue at any time. - Dial "Queue number" + "*" to log in the queue. - Dial "Queue number" + "**" to log out the queue.
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.
Agent Announcement	Announcement played to the Agent prior to bridging in the caller.
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.
Ring In Use	If set to “no”, unchecked, the queue will avoid sending calls to members whose device are known to be “in use”.
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.

2) Caller Experience Settings

Table 7-4 Queue Configuration Parameters – Caller Experience Settings

Caller Settings	
Music On Hold	Select the “Music on Hold” playlist for this Queue.
Caller Max Wait Time	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.
Leave When Empty	If enabled, callers already on hold will be forced out of a queue when no agents available.
Join Empty	If enabled, callers can join a queue that has no agents.
Join Announcement	Announcement played to callers once prior to joining the queue.
Caller Position Announcements	
Announce Position	Announce position of caller in the queue.
Announce Hold Time	Enabling this option causes PBX to announce the hold time to the caller periodically based on the frequency timer. Either yes or no; hold time will be announced after one minute.
Frequency	How often to announce queue position and estimated hold time.
Periodic Announcements	

Prompt	Select a prompt file to play periodically.
Frequency	How often to play the periodic announcements.
Events	
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.	

Conference

Conference Calls increase employee efficiency and productivity, and provide a more cost-effective way to hold meetings. Conference agents can dial * to access to the settings options and the admin can kick the last user out and can lock the conference room.

Go to **Settings** > **PBX** > **Call Features** > **Conference** to configure conferences.

- Click Add to add a new conference.
- Click Delete to delete the selected conferences.
- Click ✎ to edit one conference.
- Click 🗑 to delete one conference.

Please check the conference configuration parameters below.

Table 7-5 Conference Configuration Parameters

Options	Description
Number	Use this number to dial into the conference room.
Name	Give the conference a brief name to help you identify it.
Administrator	Admin can kick the users out and lock the conference. Also you can set none.
PIN#	You can require callers to enter a password before they can enter this conference. This setting is optional.

Join a Conference Room

Users on K2 could dial the conference extension to join the conference room. If a password is set for the conference, users would be prompted to enter a PIN.

How to join the conference room if I am calling from outside (i.e. calling from my mobile phone)?
In this case, an inbound route for conferences should be set on K2. A trunk should be selected in the inbound route and destination should be set to a conference room. When the outside users dial in the trunk number, the call will be routed to the conference room.

Manage the Conference

During the conference call, the users could manage the conference by pressing * key on their phones

to access voice menu for conference room.
Please check the options for the voice menu.

Table 7-6 Conference Voice Menu

Conference Administrator IVR Menu	
1	Mute/ un-mute yourself.
2	Lock /unlock the conference.
3	Eject the last user.
4	Decrease the conference volume.
6	Increase the conference volume.
7	Decrease your volume.
8	Exit the IVR menu.
9	Increase your volume.
Conference Users IVR Menu	
1	Mute/ un-mute yourself.
4	Decrease the conference volume.
6	Increase the conference volume.
7	Decrease your volume.
8	Exit the IVR menu.
9	Increase your volume.

Pickup Group

Call pickup allows one to answer someone else's call. You can add pickup group. The default call pickup for Group Call Pickup is *4. It allows you to pick up a call from a ringing phone which is in the same group as you.

Go to **Settings** > **PBX** > **Call Features** > **Pickup Group** to add pickup group.

- Click Add to add a new pickup group.
- Click Delete to delete the selected pickup groups.
- Click ✎ to edit one pickup group.
- Click 🗑 to delete one pickup group.

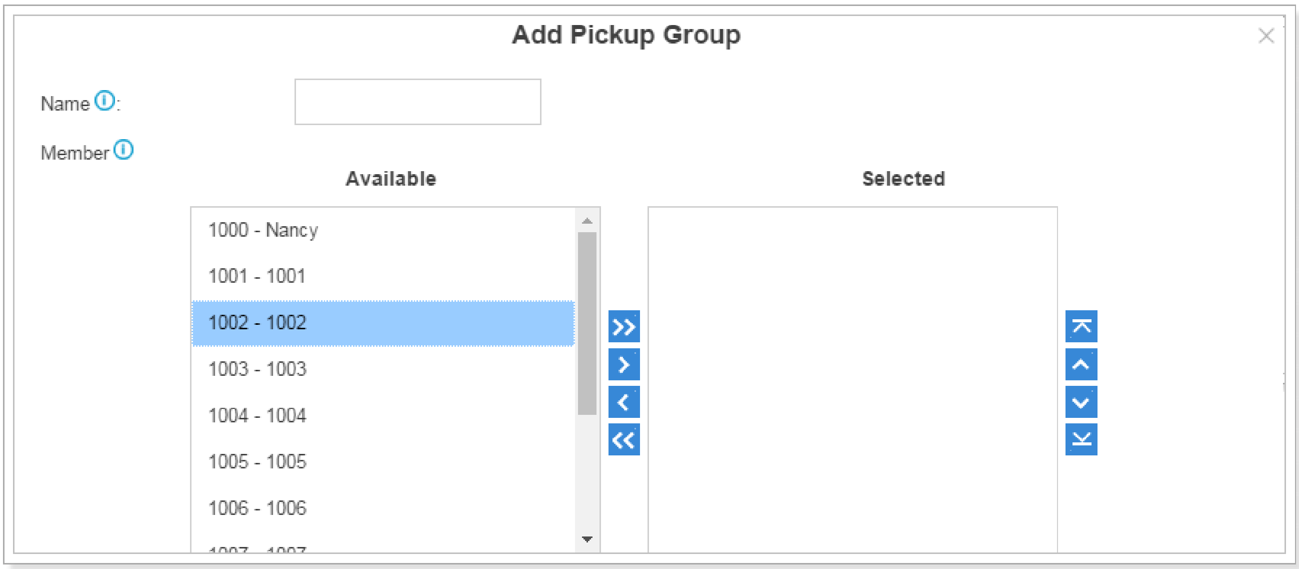


Figure 7-1 Add Pickup Group

Speed Dial

Sometimes you may just need to call someone quickly without having to look up his/her phone number. You can by simply define a shortcut number. Speed Dial feature is available on Yeastar K2 that allowing you to place a call by pressing a reduced number of keys.

1) **Add Speed Dial**

Click Add to add a speed dial.

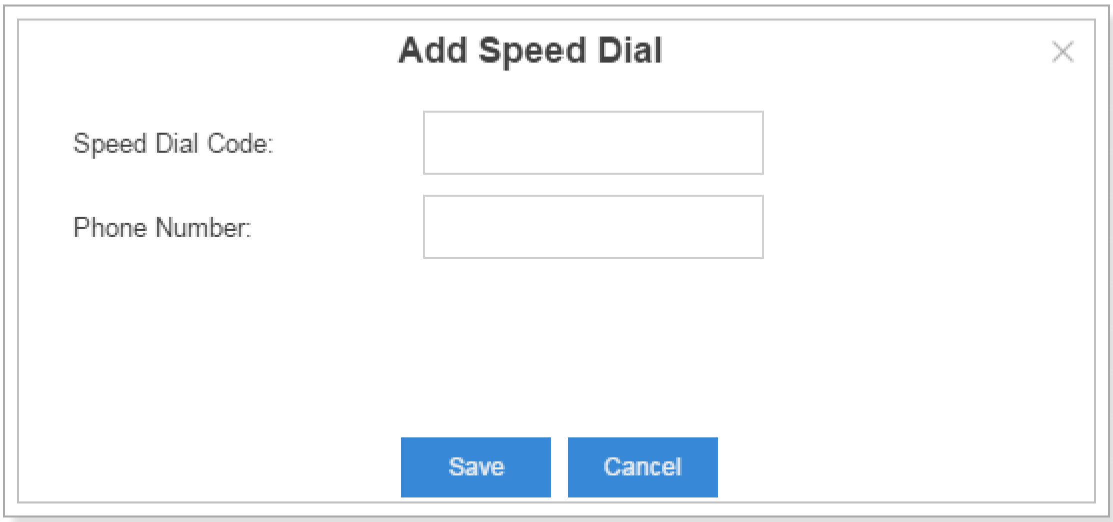
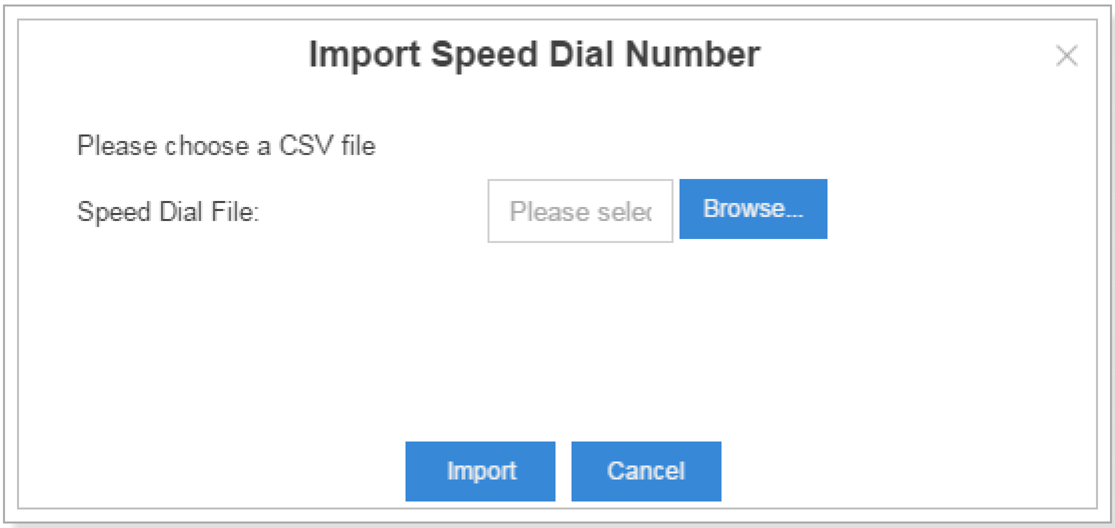


Figure 7-2 Add Speed Dial

- **Speed Dial Code**: enter the speed dial code.
- **Phone Number**: enter the number you want to call.

2) **Import Speed Dial**

Click Import, you will see a dialog window shown as below.



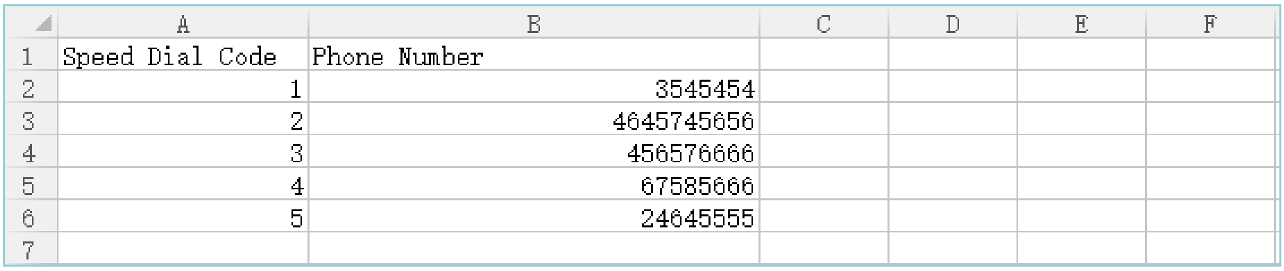
Import Speed Dial Number

Please choose a CSV file

Speed Dial File: Please selec

Figure 7-3 Import Speed Dial Number

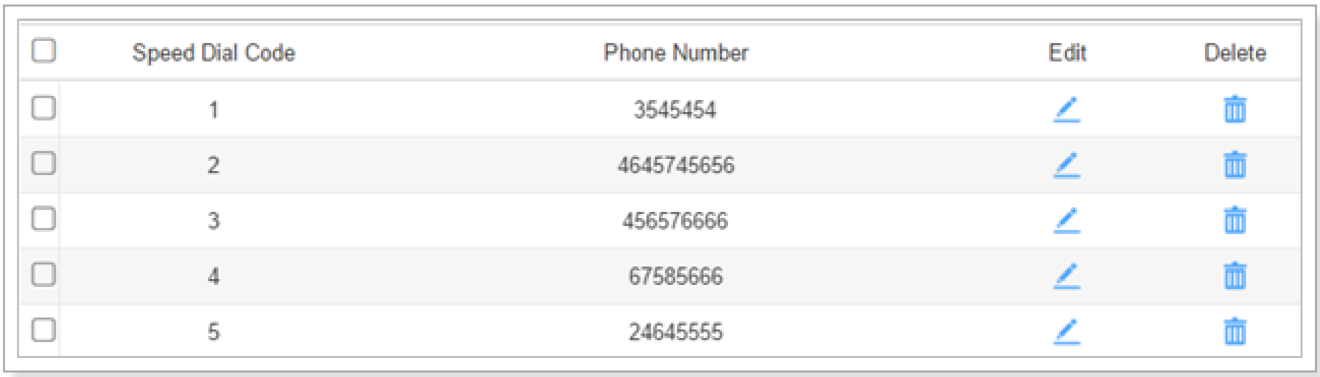
Click Browse and select the file to start uploading. The file must be a .csv file. Check the sample file below. You can export a speed dial file from K2 and use it as a sample to start with.



	A	B	C	D	E	F
1	Speed Dial Code	Phone Number				
2	1	3545454				
3	2	4645745656				
4	3	456576666				
5	4	67585666				
6	5	24645555				
7						

Figure 7-4 Speed Dial File

The sample csv file will result in the following speed dial in Yeastar K2.

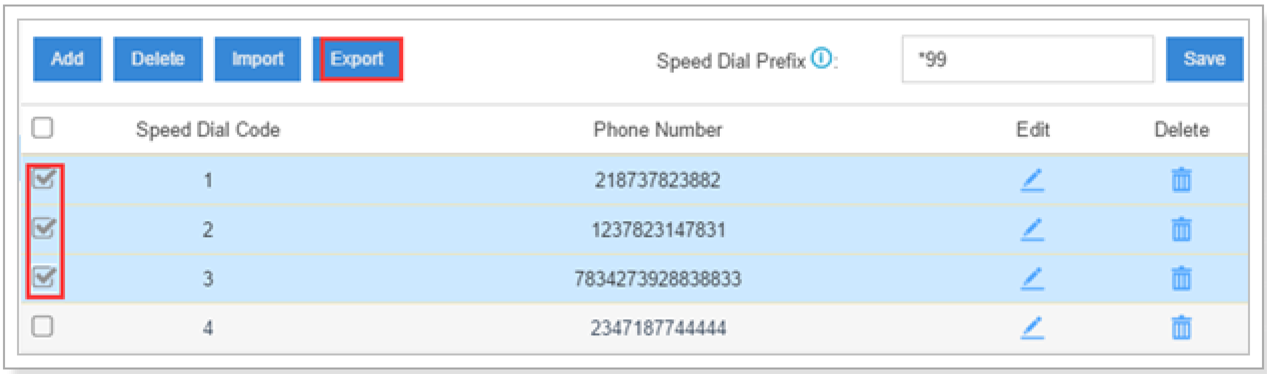


□	Speed Dial Code	Phone Number	Edit	Delete
□	1	3545454	✎	🗑
□	2	4645745656	✎	🗑
□	3	456576666	✎	🗑
□	4	67585666	✎	🗑
□	5	24645555	✎	🗑

Figure 7-5 Speed Dial Codes

3) Export Speed Dial

Select the checkbox of the speed dial, click Export, the selected speed dial will be exported to your local PC.



Add Delete Import Export Speed Dial Prefix ⓘ: *99 Save

☐	Speed Dial Code	Phone Number	Edit	Delete
☑	1	218737823882	✎	🗑
☑	2	1237823147831	✎	🗑
☑	3	7834273928838833	✎	🗑
☐	4	2347187744444	✎	🗑

Figure 7-6 Export Speed Dial

Callback

Callback feature allows callers to hang up and get called back to Yeastar K2 Callback feature could reduce the cost for the users who work out of the office using their own mobile phones.

Go to **Settings** > **PBX** > **Call Features** > **Callback** to configure Callback.

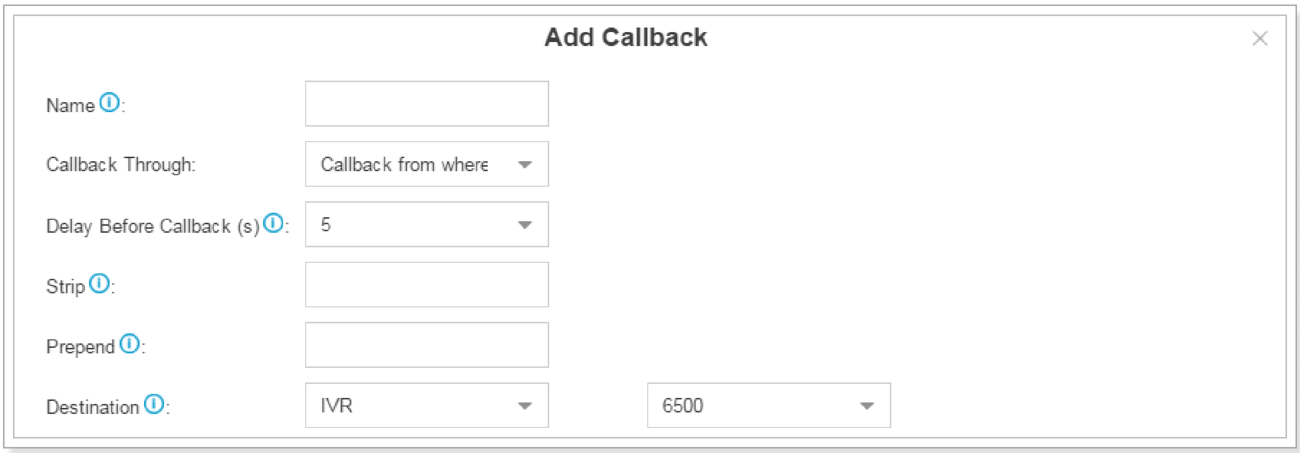
- Click Add to add a new callback.
- Click Delete to delete the selected callbacks.
- Click ✎ to edit one callback.

Note:

- You don't need to configure "Strip" and "Prepend" options if the trunk supports call back with the caller ID directly.

To use callback feature, you need to select callback as destination on the inbound route.

Please check the callback configuration parameters below.



Add Callback

Name ⓘ:		
Callback Through:	Callback from where	
Delay Before Callback (s) ⓘ:	5	
Strip ⓘ:		
Prepend ⓘ:		
Destination ⓘ:	IVR	6500

Figure 7-7 Add Callback

Table 7-7 Call Back Configuration Parameters

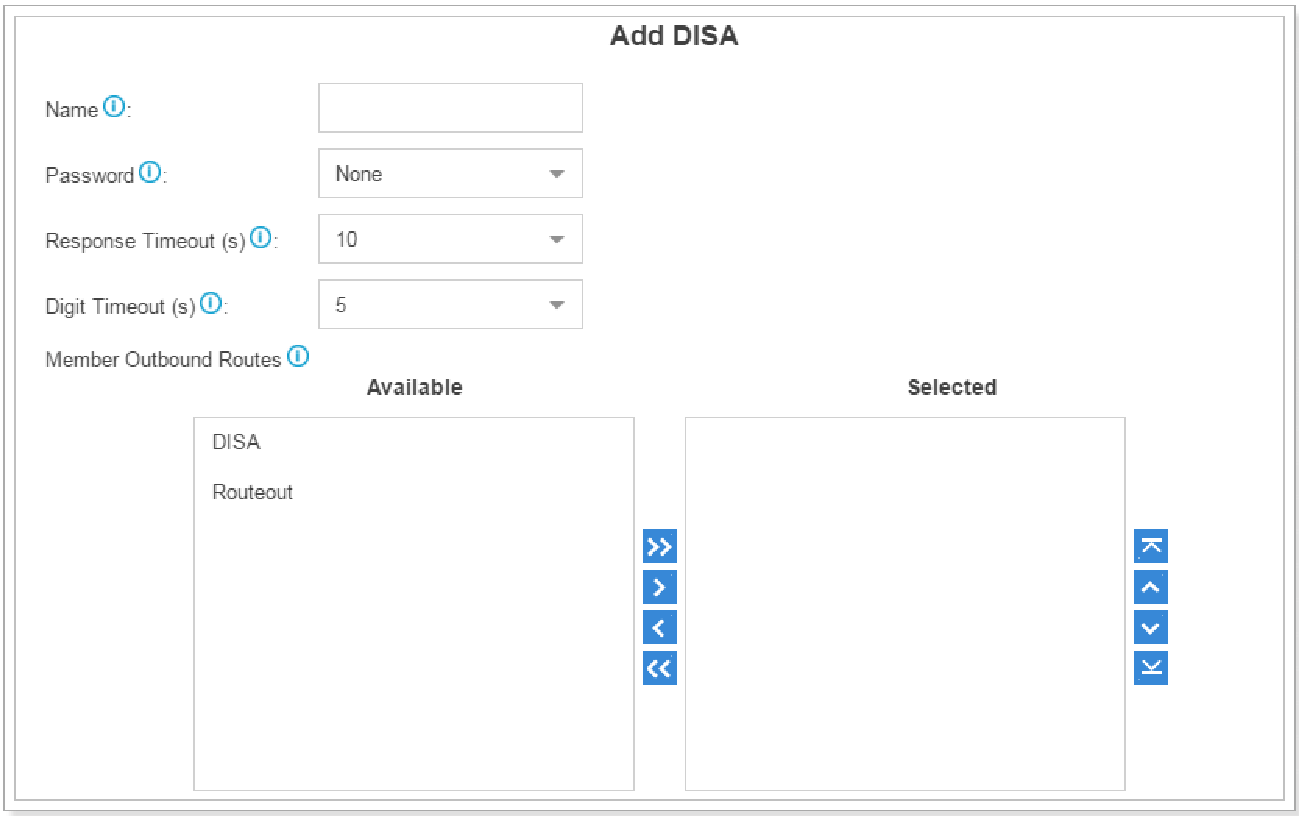
Option	Description
Name	Give this Callback a brief name to help you identify it.
Callback Through	Choose a trunk, the call will be called back through the selected trunk.
Delay Before Callback	Set the number of seconds before calling back a caller.
Strip	Defines how many digits will be stripped from the call in number before the callback is placed.
Prepend	Defines digits added before a callback number before the callback is placed.
Destination	The destination which the callback will direct the caller to.

DISA

DISA (Direct Inward System Access) allows someone calling in from outside Yeastar K2 to obtain an "internal" system dial tone and make calls as if they were using one of the extensions of K2.

To use DISA, a user calls a DISA number, which invokes the DISA application. The DISA application in turn requires the user to enter a PIN number, followed by the pound key (#). If the PIN number is correct, the user will hear dial tone on which a call may be placed.

Please check the callback configuration parameters below.



Add DISA

Name:	
Password:	None
Response Timeout (s):	10
Digit Timeout (s):	5

Member Outbound Routes

Available	Selected
DISA Routeout	

Figure 7-8 Add DISA

Table 7-8 DISA Configuration Parameters

Option	Description
Name	Give this DISA a brief name to help you identify it.
Password	The password for this DISA.
Response Timeout	The maximum amount of time the system will wait before hanging up the call if the user has dialed an incomplete or invalid number. The default value is 10s.
Digit Timeout	The maximum amount of time permitted between each digit when the user is dialing an extension number. The default value is: 5s.
Member Outbound Routes	Defines the outbound routes that can be accessed from this DISA.

Blacklist/Whitelist

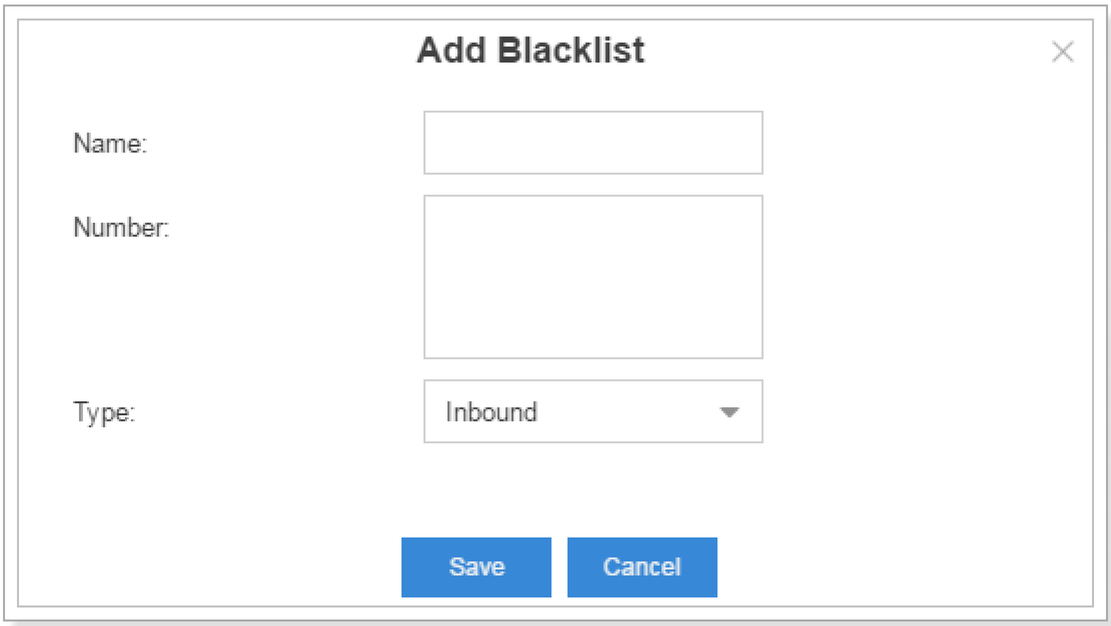
Blacklist is used to block an incoming/outgoing call. If the number of incoming or outgoing call is listed in the number blacklist, the caller will hear the following prompt: “The number you have dialed is not in service. Please check the number and try again”. The system will then disconnect the call.
Whitelist is used to allow incoming/outgoing numbers.

The system supports to block or allow 3 types of numbers:

- **Inbound**: the number would be disallowed or allowed to call in the system.
- **Outbound**: users are disallowed or allowed to call the number out from the system.
- **Both**: both inbound and outbound calls are disallowed or allowed.

1) Add Blacklist/Whitelist

Select Blacklist or Whitelist tag, click Add to add a number to Blacklist or Whitelist.



Add Blacklist

Name:

Number:

Type: Inbound

Figure 7-9 Add Blacklist

- **Name**: give a name for the blacklist/whitelist.
- **Number**: enter the numbers, one number per row.

- **Type**: choose the type.

2) Import Blacklist/Whitelist

Click Import, you will see a dialog window shown as below.

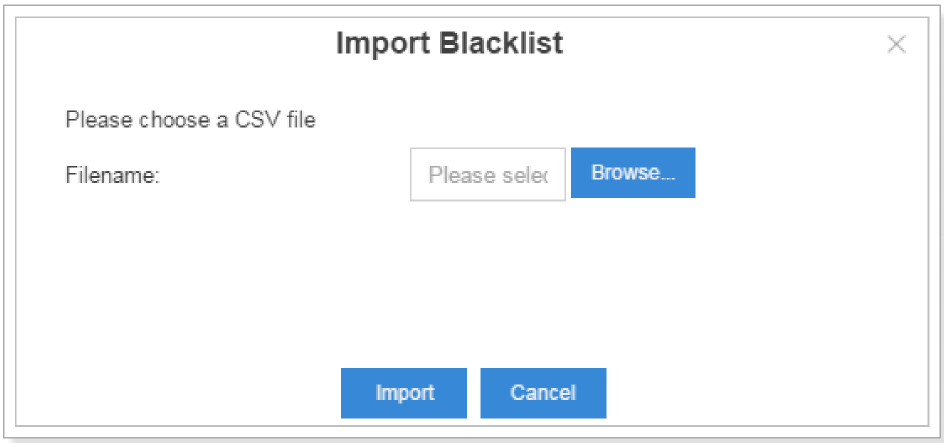
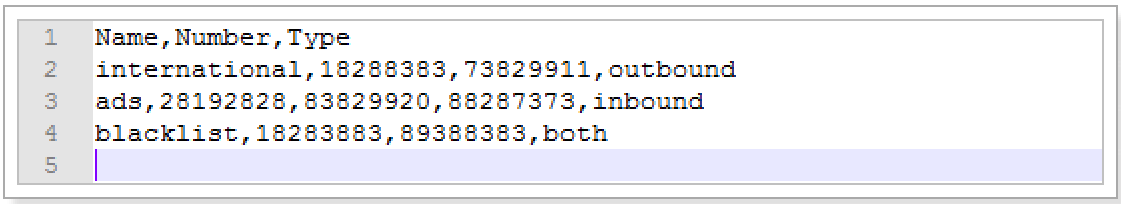


Figure 7-10 Import Blacklist

Click Browse and select the file to start uploading. The file must be a .csv file. Open the file with notepad, check the sample below. You can export a blacklist/whitelist file from K2 and use it as a sample to start with.

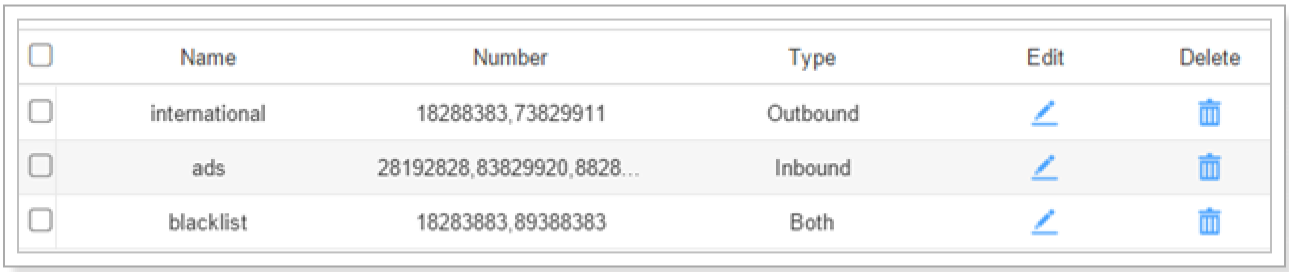


```
Name,Number,Type
international,18288383,73829911,outbound
ads,28192828,83829920,88287373,inbound
blacklist,18283883,89388383,both

```

Figure 7-11 Blacklist/Whitelist File

The sample csv file will result in the following blacklist/whitelist in Yeastar K2.



□	Name	Number	Type	Edit	Delete
□	international	18288383,73829911	Outbound	✎	🗑
□	ads	28192828,83829920,8828...	Inbound	✎	🗑
□	blacklist	18283883,89388383	Both	✎	🗑

Figure 7-12 Blacklist/Whitelist

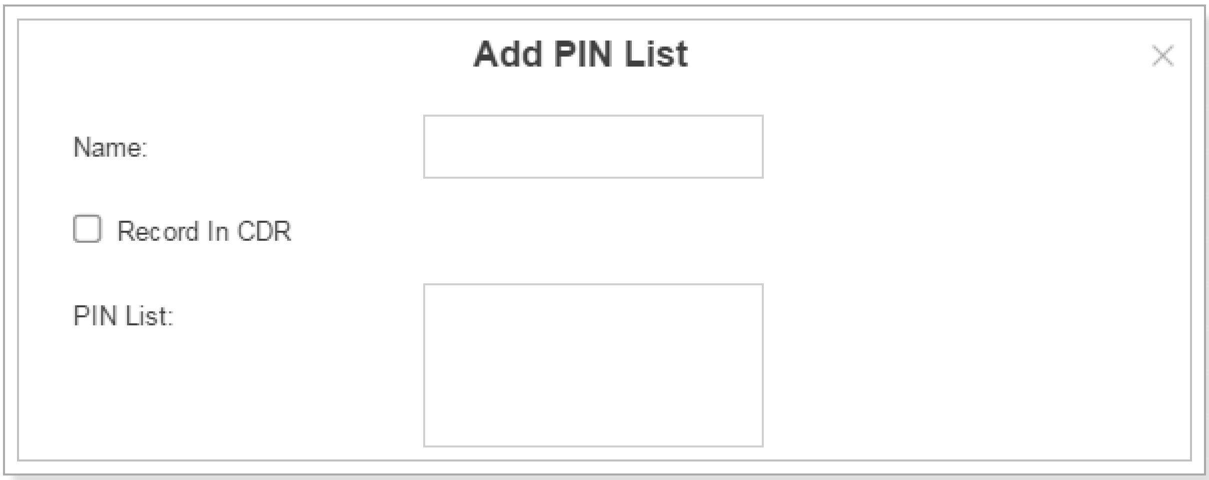
3) Export Blacklist/Whitelist

Select the checkbox of the blacklist/whitelist, click Export, the selected blacklist/whitelist will be exported to your local PC.

Pin List

PIN List is used to manage lists of PINs (numerical passwords) that can be used to access restricted features such as outbound routes. The PIN can also be presented in the CDR record.

Go to **Settings** > **PBX** > **Call Features** > **Pin List** and click Add to add Pin list.


Add PIN List

Name:

□ Record In CDR

PIN List:

Figure 7-13 Add PIN List

Linking a PIN List to Outbound Routes/DISA

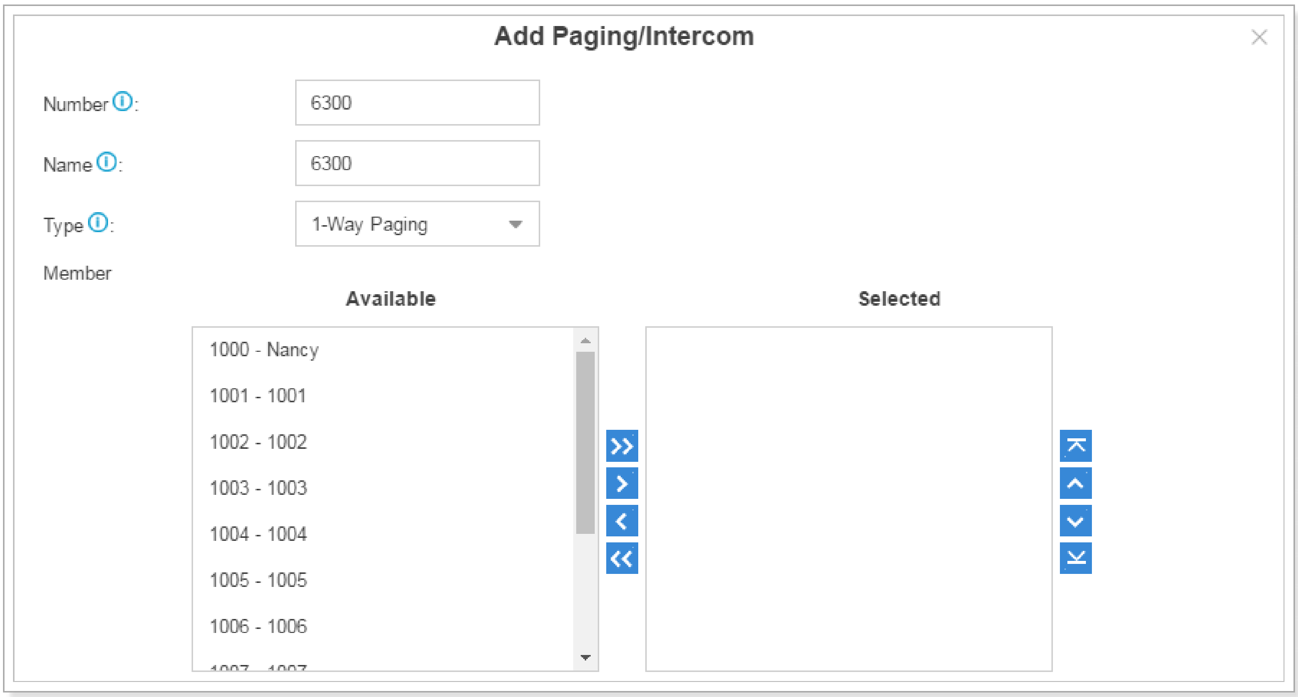
After creating PIN lists, you can link the PIN lists to Outbound Routes or DISA. On outbound route/DISA edit page, you can select the PIN list from the **Password** drop-down menu.

Paging/Intercom

Intercom is a feature that allows you to make an announcement to one extension via a phone speaker. The called party does not need to pick up the handset. It is can be achieved by pressing the feature code on your phone and it is a two-way audio call.
The default Intercom feature code is *5. To make an announcement to a specific extension, you need to dial *5+ extension number on your phone. For example, make an announcement to extension 500, you need to dial *5500, then the extension 500 will be automatically picked up.

Paging is used to make an announcement over the speakerphone to a phone or group of phones. Targeted phones will not ring, but instead answer immediately into speakerphone mode. Paging is typically one way for announcements only, but you can set the paging group as a duplex mode to allow all users in the group to talk and be heard by all.

Go to **Settings > PBX > Call Features > Paging/Intercom**, click Add to add a paging group.



Add Paging/Intercom

Number ⓘ: 6300

Name ⓘ: 6300

Type ⓘ: 1-Way Paging

Member

Available

1000 - Nancy
1001 - 1001
1002 - 1002
1003 - 1003
1004 - 1004
1005 - 1005
1006 - 1006
1007 - 1007

Selected

Figure 7-14 Add Paging Group

- **Number**: the extension number dialed to reach this Paging Group.
- **Name**: give this Paging Group a brief name to help you identify it.
- **Type**: select the mode of paging group.
  a) 1-Way Paging: typically one way for announcement only.
  b) 2-Way Paging: make paging duplex, allowing all users in the group to talk and be heard by all.
- **Member**: select the members of the group.

Voice Prompts

In this chapter, we introduce how to manage voice on Yeastar K2, including the following sections:

- Prompt Preference
- System Prompt
- Music on Hold
- Custom Prompts

Prompt Preference

Select prompt files for the relevant options on this page.

Table 8-1 Prompt Preference Configuration Parameters

Option	Description
Music On Hold	The music to play when a call is being held.
Play Call Forwarding Prompt	If enabled, system will play a prompt before transferring the call. Otherwise, the call will be transferred directly without any prompt.

	It is enabled by default.
Music On Hold for Call Forwarding	This decides what to play when the caller is put on hold during call forwarding. The options are: • Music, which will be the same with the one selected in Music on Hold. • Ringing Tone The default is to play Music.
Invalid Phone Number Prompt	The prompt to play when the dialed phone number is invalid.
Busy Line Prompt	The prompt to play when the dialed phone number is busy.
Dial Failure Prompt	The prompt to play when a dial failed due to conjunction and lack of available trunks.
Event Center Prompt	The prompt to play when there is a notification call from “Event Center”.
One Touch Recording Start Prompt	The prompt to play when the one touch recording starts.
One Touch Recording End Pormpt	The prompt to play when the one touch recording ends.

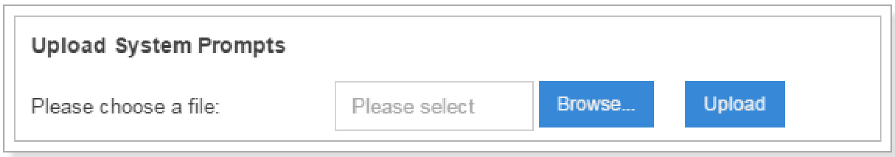
System Prompt

Yeastar K2 ships with a US English prompt set by default. The system supports multiple languages. You could update the system prompt from the cloud server directly. Also, upload system prompt from local PC is supported.

Go to **Settings** > **PBX** > **Voice Prompt** > **System Prompt** to update the system prompt.

Upload System Prompts

Click Browse to select the system prompt file from local computer, then click Upload to start uploading.



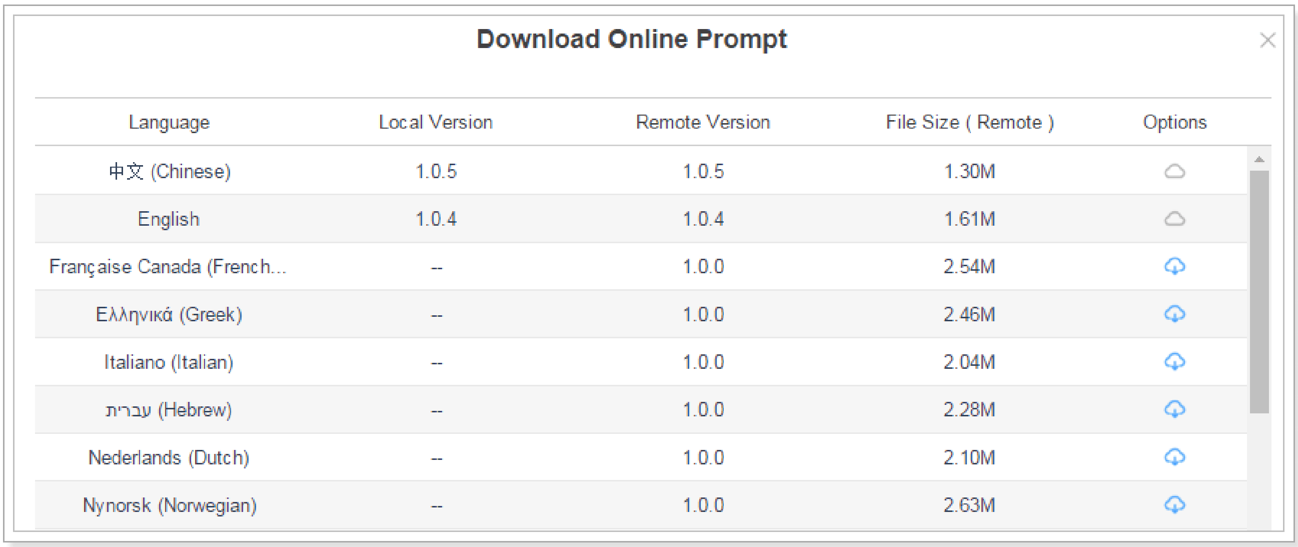
Upload System Prompts

Please choose a file: Please select

Figure 8-1 Upload System Prompts

Download Online Prompt

Click Download Online Prompt, a dialog window appears as the following figure. All the available system prompts are listed on the window.



Download Online Prompt

Language	Local Version	Remote Version	File Size (Remote)	Options
中文 (Chinese)	1.0.5	1.0.5	1.30M	☁
English	1.0.4	1.0.4	1.61M	☁
Française Canada (French...	--	1.0.0	2.54M	☁↓
Ελληνικά (Greek)	--	1.0.0	2.46M	☁↓
Italiano (Italian)	--	1.0.0	2.04M	☁↓
עברית (Hebrew)	--	1.0.0	2.28M	☁↓
Nederlands (Dutch)	--	1.0.0	2.10M	☁↓
Nynorsk (Norwegian)	--	1.0.0	2.63M	☁↓

Figure 8-2 Download Online Prompt

Click ☁↓ to download the latest prompts. The new downloaded system prompt will be displayed once installed successfully. You can select the prompt to apply in the K2 system or delete it.

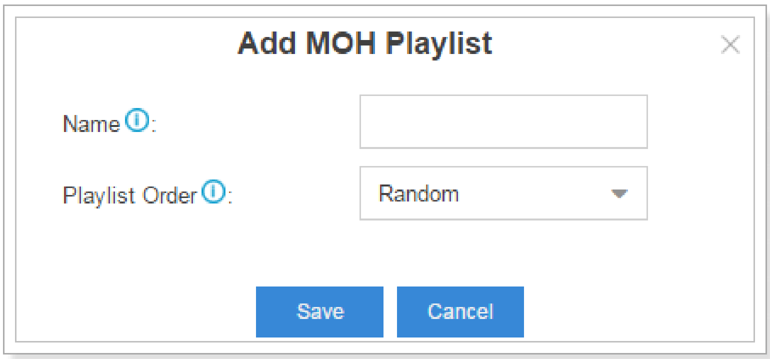
Music on Hold

Music on hold (MOH) is the business practice of playing recorded music to fill the silence that would be heard by callers who have been placed on hold. Users could configure Music on Hold Folder and upload music files to the system. The "default" Music on Hold Playlist includes 3 music files for users to use.

Go to **Settings** > **PBX** > **Voice Prompts** > **Music on Hold**.

1) Create New Playlist

Click Create New Playlist to create a new playlist.



Add MOH Playlist

Name ⓘ:

Playlist Order ⓘ: Random

Figure 8-3 Add Playlist

- **Name:** give this playlist a name to help you identify it.
- **Play Sort:** select the playing order of the playlist.

2) Upload New Music

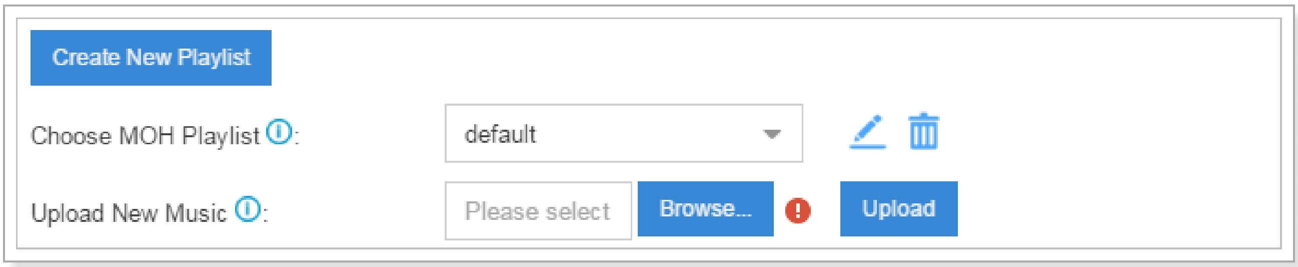


Figure 8-4 Upload New Music

Choose MOH Playlist from the drop-down menu.

Click Browse to select music file from your local computer, click Upload to start uploading.

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.

Go to **Settings > PBX > Voice Prompts > Custom Prompts** to record and upload custom prompts.

1) Upload Custom Prompt

Click Upload, the following dialog window appears. Click Browse... to choose a music file from your computer. Click Upload to start uploading.

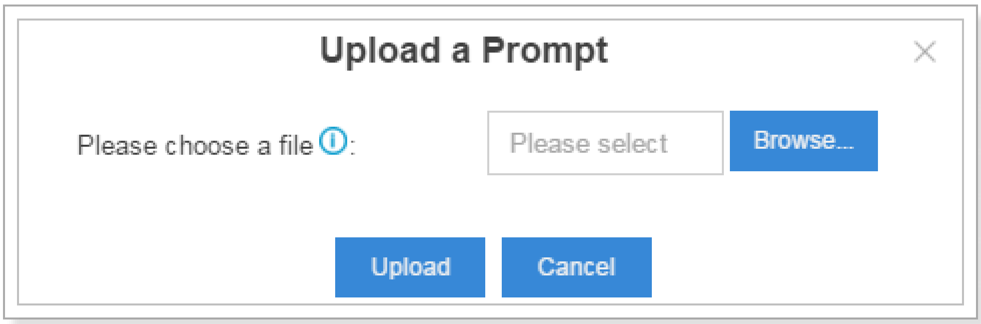


Figure 8-5 Upload a Prompt

2) Record Custom Prompt

Click Record New, the following dialog window shows. Specify the name and choose an extension to make the record.

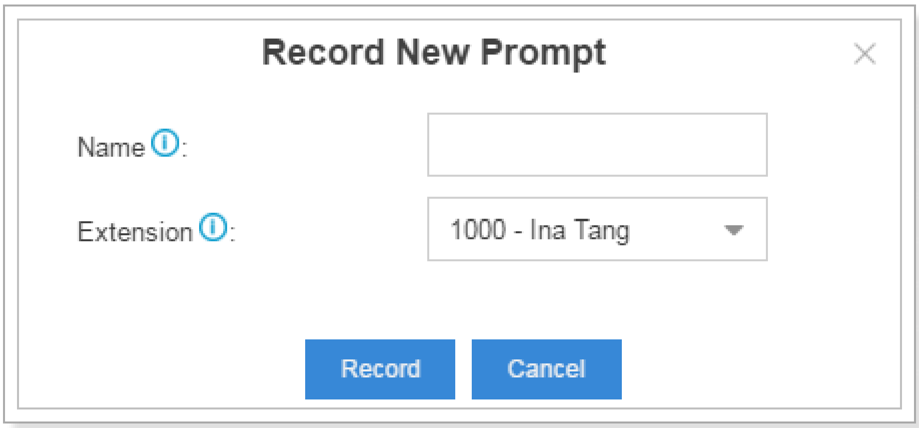


Figure 8-6 Record New Custom Prompt

Click Record, the selected extension will ring, pick up the call to start recording.

General

This chapter explains general settings in the system, which can be applied globally to Yeastar K2.

- Preference
- Feature Code
- Voicemail
- SIP
- IAX

Preference

Table 9-1 Preference Configuration Parameters

Option	Description
Max Call Duration	Select the absolute maximum number of seconds permitted for a call. If you wish to customize, enter the value in the text box directly. Input 0 disables the timeout.
Attended Transfer Caller ID	The Caller ID that will be displayed on the recipient's phone. For example, Phone A (transferee) calls Phone B (transfer), and Phone B transfers the call to Phone C (recipient). If set to Transfer, the Caller ID displayed will be Phone B's number; if set to Transferee, Phone A's number will be displayed.
Virtual Ring Back Tone	Once enabled, when the caller calls out with cellular trunks, the caller will hear the virtual ring back tone generated by the system before the callee answers the call.
Distinctive Caller ID	When the incoming call is routed from Ring Group, Queue or IVR, the Caller ID would display where it comes from.
Extension Preferences	
User Extensions	Specify the user extension range. The default range is 1000-5999.
Ring Group Extensions	Specify the Ring Group extension range. The default range is 6200-6299.
Paging Group Extensions	Specify the Paging Group extension range. The default range is 6300-6399.
Conference Extensions	Specify the Conference extension range. The default range is 6400-6499.
IVR Extensions	Specify the IVR extension range. The default range is 6500-6599.
Queue Extensions	Specify the Queue extension range. The default range is 6600-6699.

Feature Code

Feature Codes are used to enable and disable certain features available in the system. The K2 local users can dial feature codes on their phones to use a particular feature.

The default feature codes can be checked and changed via **Settings > PBX > General > Feature Code**.

Table 9-2 Feature Code

Feature Code	
Feature Code Digits Timeout	The timeout to input next digit (in milliseconds). The default is 4000.
Recording	
One Touch Record	The feature code that is used to start or stop call recording. The default feature code is *1.
Voicemail	
Check Voicemail	The feature code that is used to check voicemail. The system will prompt you for password. The default feature code is *2.
Voicemail for Extension	You can leave a voicemail to other extensions by dialing feature code on their phone or forward an incoming call to an extension's voicemail directly. The default feature code is #. For example, dial "#501" to leave a message for Ext. 501.
Voicemail Main Menu	The feature code that is used to access voicemail main menu. The default feature code is *02.
Transfer	
Blind Transfer	Dial this feature code and an extension number to blind transfer the call. The default feature code is *03.
Attended Transfer	Dial this feature code and an extension number to transfer the call. Hang up after contacting the destination. The default feature code is *3.
Attended Transfer Timeout	The timeout to transfer a call, in seconds. The default is 15 seconds.
Call Pickup	
Call Pickup	This feature code allows you to answer another ringing phone that is in the same pickup group. The default feature code is *4.
Extension Pickup	Dial this feature code and an extension number to pick up a call that is ringing at the extension. The default feature code is *04.
Intercom	
Intercom	Dial this feature code and an extension number to page that extension. The default feature code is *5.
Call Parking	
Call Parking	Dial this feature code to put a call on hold and park the call at an

	extension number directed by the system. Any other phone can dial this extension number to resume the conversation. The default feature code is *6.
Directed Call Parking	Dial this feature code and an extension number to park the call at that extension. Any other phone can dial this extension number to resume the conversation. The default feature code is *6. Note: if the directed extension number is occupied, the call parking will fail.
Parking Extension Range	A range of extensions where the call will be parked.
Parking Timeout	This defines the number of seconds that a call can be parked before it is recalled by an extension.
Call Forwarding	
Reset to Defaults	Dial this feature code to restore call forwarding to the following default settings: • Always Forward: disabled • Busy Forward to Voicemail: enabled • No Answer Forward to Voicemail: enabled • Do Not Disturb: disabled. The default feature code is *70.
Enable Forward All Calls	Dial this feature code to forward all calls to voicemail or a designated number. For example: dial *71 to forward all calls to voicemail, and dial *71500 to forward all calls to number 500 (this number does cont include prefix, if you are required to dial with prefix, you need to configure it in Call Forwarding in Edit Extension window).
Disable Forward All Calls	Dial this feature code to disable forwarding of all calls. The default feature code is *071.
Enable Forward When Busy	Dial this feature code to forward calls to voicemail or a designated number when busy. For example: dial *72 to forward calls to voicemail when busy, and dial *72500 to forward all calls to number 500 when busy (this number does cont include prefix, if you are required to dial with prefix, you need to configure it in Call Forwarding in Edit Extension window). The default feature code is *72.
Disable Forward When Busy	Dial this feature code to disable when busy call forwarding. The default feature code is *072.
Enable Forward No Answer	Dial this feature code to forward calls to voicemail or a designated number when no answer. For example: dial *73 to forward calls to voicemail when no answer, and dial *73500 to forward all calls to number 500 when no answer (this number does cont include prefix, if you are required to dial with prefix, you need to configure it in Call Forwarding in Edit Extension window). The default feature code is *73.

Disable Forward No Answer	Dial this feature code to disable no answer call forwarding. The default feature code is *073.
Call Monitor	
Listen	Dial this feature code and the monitored extension number to initiate Listen monitoring. In this mode, the monitor can only listen to the call but can't talk. The default feature code is *90. Note: to monitor an extension, you need to configure the Monitor Settings for this extension first.
Whisper	Dial this feature code and the monitored extension number to initiate Whisper monitoring. In this mode, the monitor can listen to and talk with the monitored extension without being heard by the other party. The default feature code is *91. Note: to monitor an extension, you need to configure the Monitor Settings for this extension first.
Barge-in	Dial this feature code and the monitored extension number to initiate Barge-in monitoring. In this mode, the monitor can listen to and talk with both parties. The default feature code is *92. Note: to monitor an extension, you need to configure the Monitor Settings for this extension first.
DND	
Enable Do Not Disturb	Dial this feature code to put the extension in Do Not Disturb state. The default feature code is *74.
Disable Do Not Disturb	Dial this feature code to take the extension out of Do Not Disturb state. The default feature doe is *074.

Voicemail

The configurations of voicemail can be globally set up and managed on the Voicemail page. Go to **Settings > PBX > General > Voicemail**, you can configure the Message Options, Greeting Options and Playback Options.

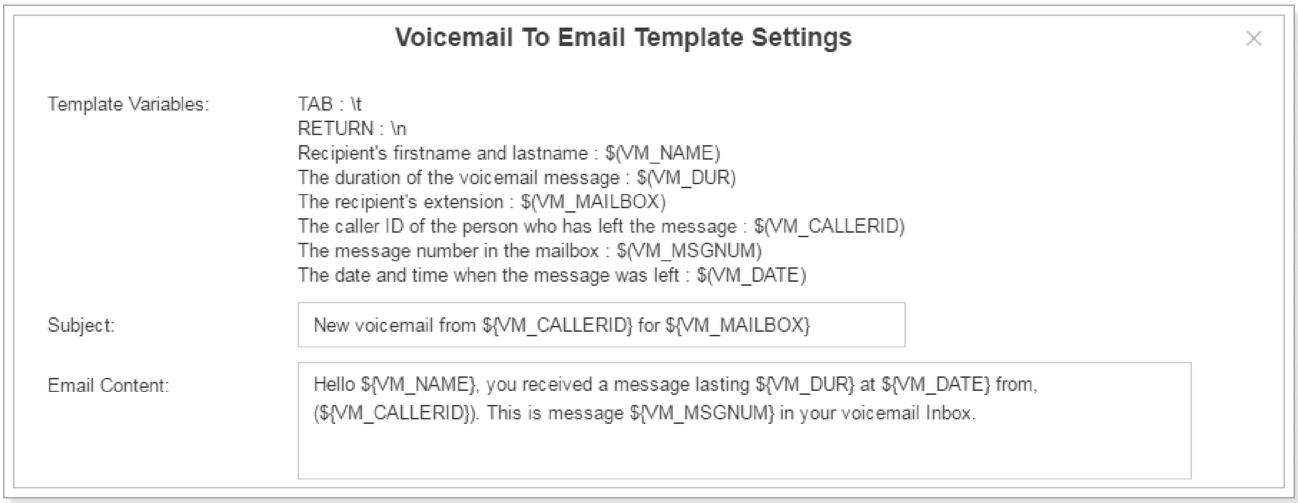
Table 9-3 Voicemail Configuration Parameters

Message Options	
Max Messages per Folder	This sets the maximum number of messages that can be stored in a single folder of voicemail.
Max Message Time	This sets the maximum length of a single voicemail message (in seconds).
Min Message Time	This sets the minimum length of a single voicemail message (in seconds). Messages below this threshold will be automatically

	deleted.
Ask Caller to Dial 5	If this option is enabled, the caller will be prompted to press 5 before leaving a message.
Operator Breakout from Voicemail	If this option is set, the caller can jump out of the voicemail and go to the pre-configured destination by dialing 0.
Destination	This sets the breakout destination.
Greeting Options	
Busy Prompt	Greeting played when the extension is busy.
Unavailable Prompt	Greeting played when the extension is unavailable.
Leave a Message Prompt	Greeting played when dial 5.
Playback Options	
Announce Message Caller ID	If this option is enabled, the caller ID of the party that left the message will be announced before the voicemail message begins playing.
Announce Message Duration	If this option is enabled, the duration of the message in minutes will be announced before the voicemail message begins playing.
Announce Message Arrival Time	If this option is enabled, the arrival time of the message will be played back before the voicemail message begins playing.
Allow Users to Review Messages	Allow the callers to review their recorded messages before sending them to the voicemail box.

Voicemail to Email Template

You can customize the Voicemail Email contents by clicking Voicemail To Email Template Settings.



Voicemail To Email Template Settings

Template Variables:

TAB : \t
RETURN : \n
Recipient's firstname and lastname : $(VM_NAME)
The duration of the voicemail message : $(VM_DUR)
The recipient's extension : $(VM_MAILBOX)
The caller ID of the person who has left the message : $(VM_CALLERID)
The message number in the mailbox : $(VM_MSGNUM)
The date and time when the message was left : $(VM_DATE)

Subject: New voicemail from ${VM_CALLERID} for ${VM_MAILBOX}

Email Content: Hello ${VM_NAME}, you received a message lasting ${VM_DUR} at ${VM_DATE} from, (${VM_CALLERID}). This is message ${VM_MSGNUM} in your voicemail Inbox.

Figure 9-1 Voicemail To Email Template Settings

SIP

Go to **Settings > PBX > General > SIP** to configure SIP settings. It is wise to leave the default setting as provided on this page. However, for a few fields, you need to change them to suit your situation.

General

Table 9-4 General Settings

UDP Port	UDP Port used for SIP registrations. The default is 5060.
TCP Port	TCP 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.
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.
Register Timers	
Max Registration/Subscription Time	Maximum duration (in seconds) of incoming registrations and subscriptions. The default is 3600 seconds.
Min Registration/Subscription Time	Minimum duration (in seconds) of incoming registration 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	
Register Attempts	The number of registration attempts before giving up (0 for no limit).

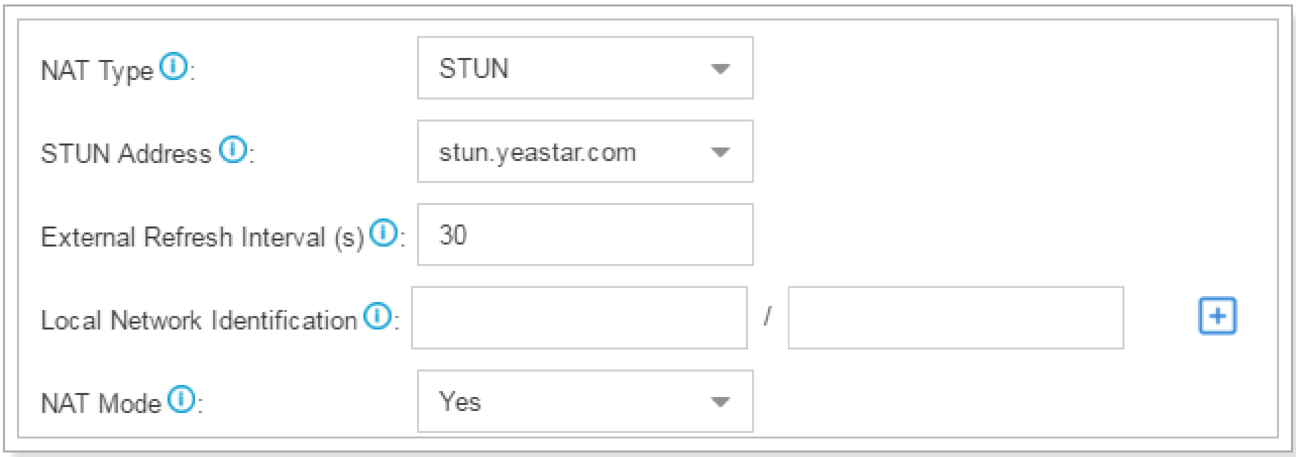
Default Incoming/ Outgoing Registration Time	Default duration (in seconds) of incoming/outgoing registration. The default is 120 seconds. Note: the actual duration needs to minus 10 seconds from the value you filled in.

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. Usually you have to configure NAT settings when you want to register a remote extension to the PBX or when you need connect to the PBX via SIP trunk.

Yeastar K2 supports 3 methods to configure NAT: STUN, External IP Address and External Host. You can select one method to configure NAT or disable NAT.

1) STUN



NAT Type: STUN

STUN Address: stun.yeastar.com

External Refresh Interval (s): 30

Local Network Identification: /

NAT Mode: Yes

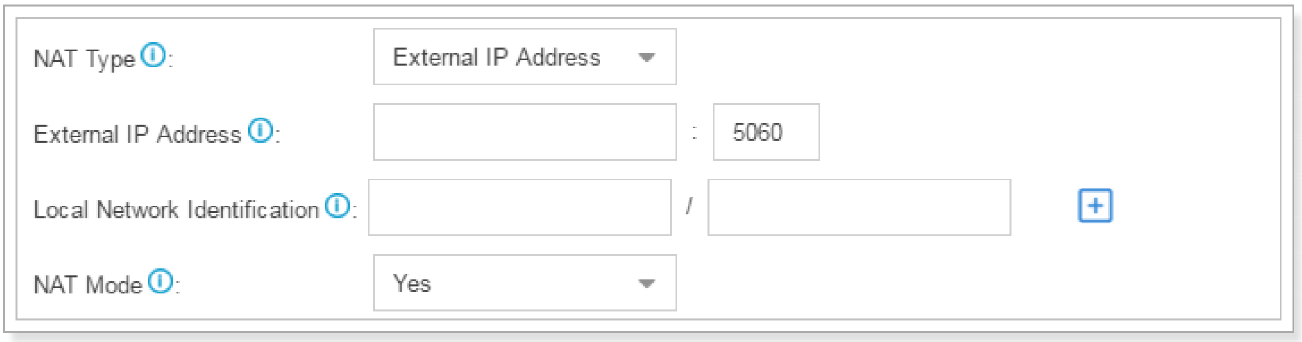
Figure 9-2 STUN

Table 9-5 STUN Configuration Parameters

Option	Description
STUN Address	Choose a STUN address in the drop-down list or customize with a STUN address and STUN port.
External Refresh Interval	If an external host has been supplied, you may specify how often the system will perform a DNS query on this host. This value is specified in seconds.
Local Network Identification	Used to identify the local network using a network number/subnet mask pair when the system is behind a NAT or firewall. Some examples are as follows: “192.168.0.0/255.255.0.0”, “10.0.0.0/255.0.0.0”, and “172.16.0.0/12”.

NAT Mode	Global NAT configuration for the system. The options are as follows: • Yes: use NAT and ignore the address information in the SIP/SDP headers and reply to the sender's IP address/port. • No: use NAT mode only according to RFC3581. • Never: never attempt NAT mode or RFC3581 support. • Route: use NAT but do not include rport in headers.

2) External IP Address



NAT Type: External IP Address

External IP Address: : 5060

Local Network Identification: /

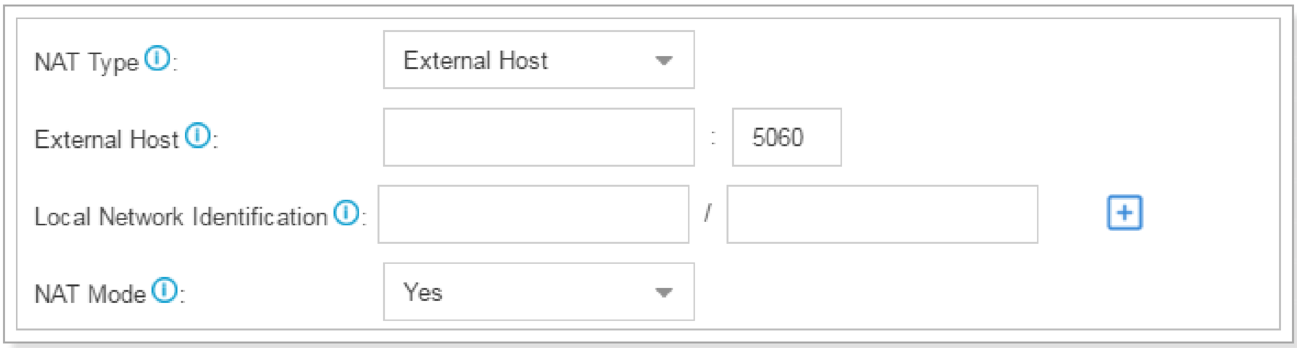
NAT Mode: Yes

Figure 9-3 NAT Settings – External IP Address

Table 9-6 External IP Address Configuration Parameters

Option	Description
External IP Address	The IP address that will be associated with outbound SIP messages if the system is in a NAT environment.
Local Network Identification	Used to identify the local network using a network number/subnet mask pair when the system is behind a NAT or firewall. Some examples are as follows: “192.168.0.0/255.255.0.0”, “10.0.0.0/255.0.0.0”, and “172.16.0.0/12”.
NAT Mode	Global NAT configuration for the system. The options are as follows: • Yes: use NAT and ignore the address information in the SIP/SDP headers and reply to the sender's IP address/port. • No: use NAT mode only according to RFC3581. • Never: never attempt NAT mode or RFC3581 support. Route: use NAT but do not include rport in headers.

3) External Host



NAT Type: External Host

External Host: : 5060

Local Network Identification: /

NAT Mode: Yes

Figure 9-4 NAT Settings – External Host

Table 9-7 External Host Configuration Parameters

Option	Description
External Host	Alternatively you can specify an external host, and the system will perform DNS queries periodically. This setting is only required when your external IP address is not static. It is recommended that a static public IP address be used with this system. Please contact your ISP for more information.
External Refresh Interval	If an external host has been supplied, you may specify how often the system will perform a DNS query on this host. This value is specified in seconds.
Local Network Identification	Used to identify the local network using a network number/subnet mask pair when the system is behind a NAT or firewall. Some examples are as follows: "192.168.0.0/255.255.0.0", "10.0.0.0/255.0.0.0", and "172.16.0.0/12".
NAT Mode	Global NAT configuration for the system. The options are as follows: • Yes: use NAT and ignore the address information in the SIP/SDP headers and reply to the sender's IP address/port. • No: use NAT mode only according to RFC3581. • Never: never attempt NAT mode or RFC3581 support. Route: use NAT but do not include rport in headers.

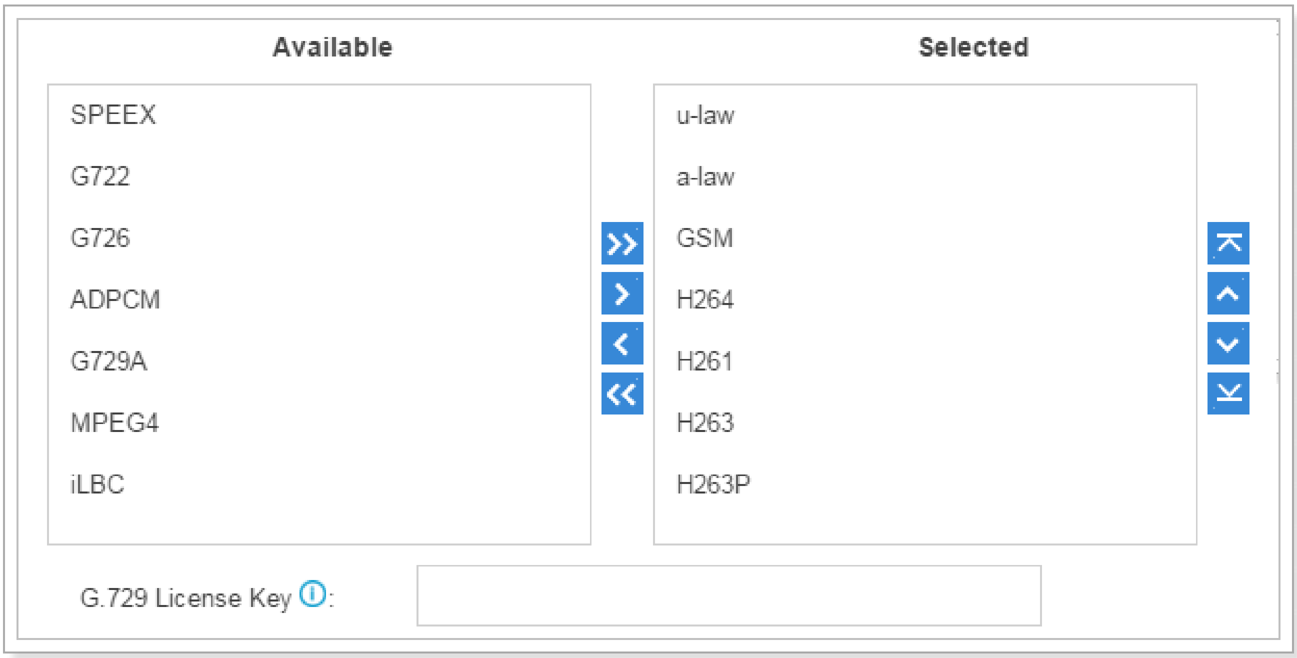
Codec

A codec is a compression or decompression algorithm that used in the transmission of voice packets over a network or the Internet. K2 supports G711 a-law, u-law, GSM, H261, H263, H263P, H264, SPEEX, G722, G726, ADPCM, G719A, MPEG4 and iLBC.

Note:

- If you would like to use G.729, please enter your license. The system have embedded the G729, you can test it directly without purchasing license. But for copyright protection, we suggest you to buy it after testing it successfully. After you buy the license from DIGIUM, you should enter G729 license at the "G729 License Key".

If you would like to use G.729, please enter your license. The system have embedded the G729, you can test it directly without purchasing license. But for copyright protection, we suggest you to buy it after testing it successfully. After you buy the license from DIGIUM, you should enter G729 license at the "G729 License Key".



Available	Selected
SPEEX	u-law
G722	a-law
G726	GSM
ADPCM	H264
G729A	H261
MPEG4	H263
iLBC	H263P

G.729 License Key ⓘ:

Figure 9-5 Codec Settings

TLS

Yeastar K2 supports TLS protocol, to use TLS, you need enable TLS via **Settings > PBX > General > SIP > TLS**. Check the TLS configuration parameters below.

Table 9-8 TLS Configuration Parameters

Option	Description
Enable TLS	Check 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 servers 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 Ignore Common Name	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

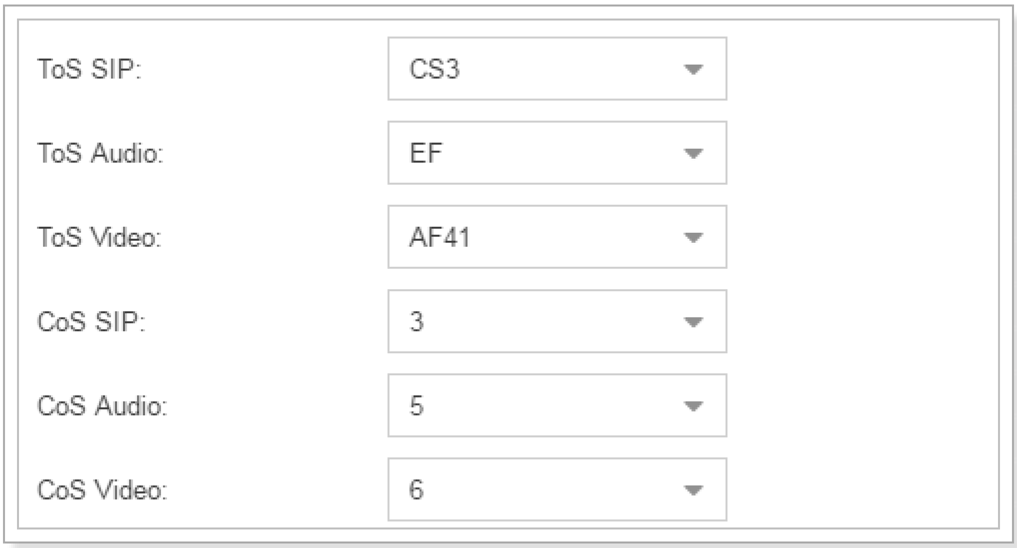
A periodic refreshing of a SIP session that allows both the user agent and proxy to determine if the SIP session is still active.

Table 9-9 Session Timer Configuration Parameters

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.
Session-minse	The min refresh interval in seconds, it must not be less than 90.

QOS

QoS (Quality of Service) 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 interference from other lower priority traffic. When the network capacity is insufficient, QoS could provide priority to users by setting the value.



ToS SIP: CS3

ToS Audio: EF

ToS Video: AF41

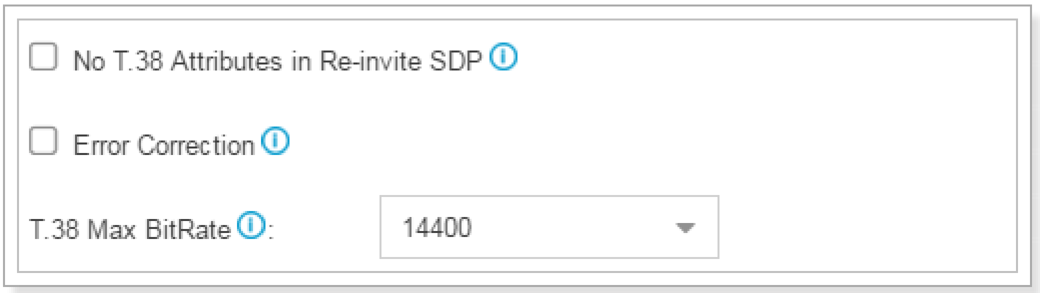
CoS SIP: 3

CoS Audio: 5

CoS Video: 6

Figure 9-6 QOS

T.38



□ No T.38 Attributes in Re-invite SDP ⓘ

□ Error Correction ⓘ

T.38 Max BitRate ⓘ: 14400

Figure 9-7 T.38

- **Re-invite SDP Not Add T.38 Attribute**
  If set to yes, SDP in re-invite packet will not add T.38 attributes.
- **Error Correction**
  This sets the Error Correction Mode (ECM) for the Fax.
- **T.38 Max BitRate**
  T38 Max Bit Rate.

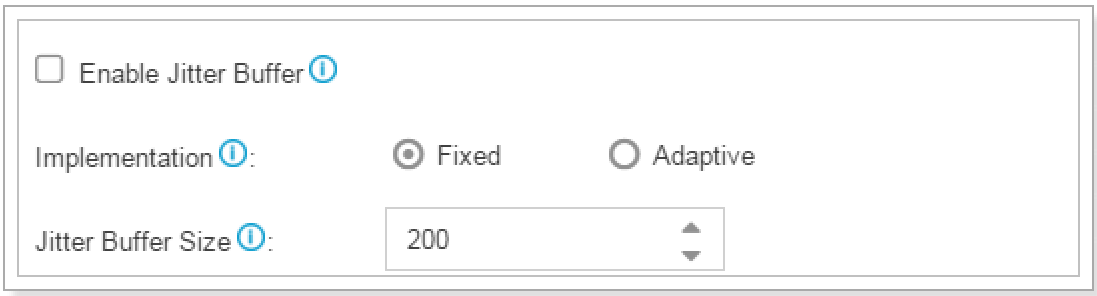
Advanced

Table 9-10 SIP Advanced Settings

Option	Description
Allow RTP Re-invite	By default, the system will route media steams from SIP endpoints through itself. Enabling this option causes the system to attempt to negotiate the endpoints to route packets to each other directly, bypassing the system. It is not always possible for the system to negotiate endpoint-to-endpoint media routing.
Get Caller ID From	This decides the system will pull Caller ID header from which header field.
User Agent	This allows you to change the User-Agent field.
Get DID From	This decides the system will pull DID from which header field. If Remote-Party-ID is selected but the line does not support this, DID will be pulled from Invite header.
Send Remote Party ID	Whether to send the Remote-Party-ID in SIP header or not. The Default is no.
Send P Asserted Identify	Whether to send the P-Asserted-Identify in SIP header or not. The Default is no.
100rel	Check the option to enable 100rel.
Send Diversion ID	Whether to send the Diversion ID in SIP header or not. The Default is no.
Allow Guest	If enabled, it will allow the unauthorized INVITE coming into the PBX and the calls can be made. The default is no.

Jitter Buffer

Jitter is the variation in the time between packets arriving on a VoIP system. These variations can be caused by network congestion, timing drift or route changes. Jitter buffers are used to counter delay or latency, dropped packets, and jitter. They temporarily store arriving packets to minimize jitter and discard packets that arrive too late.



□ Enable Jitter Buffer

Implementation: ● Fixed ○ Adaptive

Jitter Buffer Size: 200

Figure 9-8 Jitter Buffer

Configure the Jitter Buffer settings on K2 PBX will improve the call quality through VoIP. Jitter buffers must be correctly configured to be effective.

- **Enable Jitter Buffer**: check to enable this feature.
- **Implementation:** choose the implementation of jitter buffer.
  - ✓ **Fixed:** the length of jitter buffer will always be the size defined by “Jitter Buffer Size”. The default is 200 ms.
  - ✓ **Adaptive:** the length of jitter buffer will vary in size within the range of min size and max size based on current network condition. The default is from 100 ms to 200 ms.
- **Jitter Buffer Size:** set a fixed jitter buffer size.
- **Min Jitter Buffer Size:** the minimum jitter buffer size.
- **Max Jitter Buffer Size:** the maximum jitter buffer size.

IAX

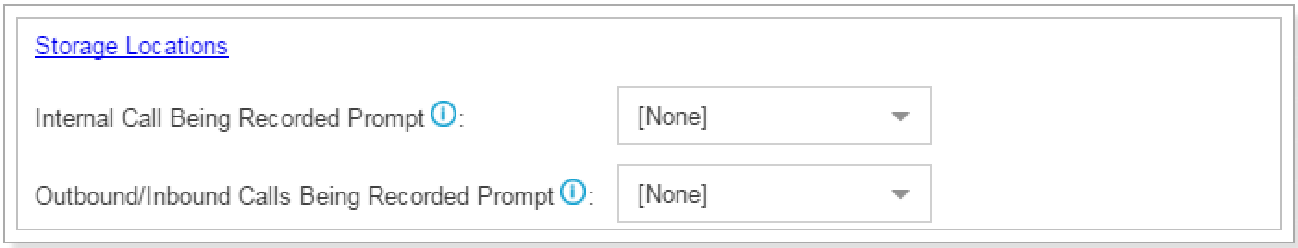
Table 9-11 IAX Configuration Parameters

Option	Description
UDP Port	UDP port used for IAX2 registrations. The default is 4569.
Bandwidth	Control which codecs to be used based on bandwidth consumption.
Maximum Registration/ Subscription Time	Maximum duration (in seconds) of an IAX registration. The default is 1200 seconds.
Minimum Registration/ Subscription Time	Minimum duration (in seconds) of an IAX registration. The default is 60 seconds.
Codec	Choose the codec.

Recording

This chapter explains how to configure auto recording on Yeastar K2.

Yeastar K2 supports auto recording for an established call. Go to **Settings > PBX > Recording** to configure auto recording settings.



Storage Locations

Internal Call Being Recorded Prompt ⓘ: [None]

Outbound/Inbound Calls Being Recorded Prompt ⓘ: [None]

Figure 10-1 Recording Prompt Settings

Table 10-1 Recording Configuration Parameters

General Preferences	
Storage Location	Click the option to link the **Storage** settings. In the storage settings, you can configure where to store recording files.
Internal Call Being Recorded Prompt	If the internal call has enabled call recording, this prompt will notify the called party that the call will be recorded.
Outbound/Inbound Call Being Recorded Prompt	If the external call (outbound/inbound/callback) has enabled call recording, this prompt will notify the called party that the call will be recorded.
Record Trunks	When a call reaches the selected trunk, it will be recorded.
Record Extensions	The selected extensions will be recorded.
Record Conferences	The selected conferences will be recorded.

Event Center

Yeastar K2 can monitor system events and logs, then send email notifications to the specified contacts.

Event Settings

The system events are divided into three categories:

Operation

- ✓ Modify Administrator Password
- ✓ User Login Success
- ✓ User Login Failed
- ✓ User Locked

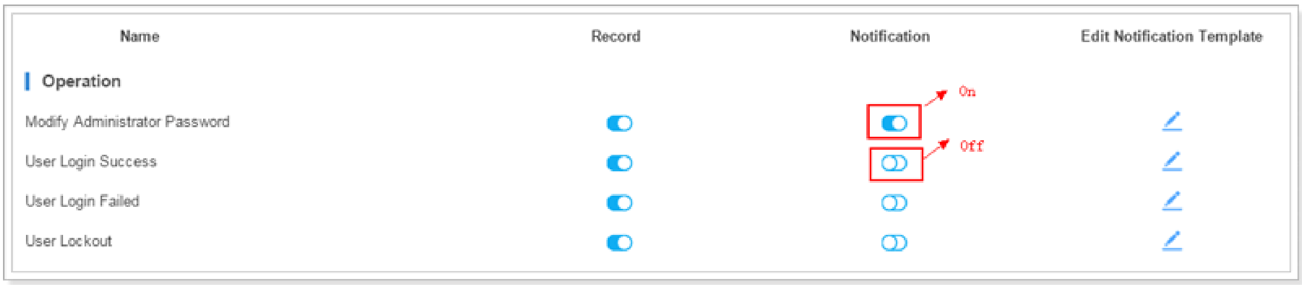
Telephony

- ✓ Register SIP Trunk Failed
- ✓ Service Provider Unreachable
- ✓ Outgoing Call Failed

System

- ✓ CPU Overload
- ✓ Memory Overload
- ✓ Concurrent Calls Overload
- ✓ Disk Failure
- ✓ Storage Space Full
- ✓ Network Attacked
- ✓ System Reboot
- ✓ System Upgrade
- ✓ System Restore

- Turn on ● **Record** to decide whether to record the event.
- Turn on ● **Notification** to decide whether to send notification.
- Click ✎ to edit the notification template.



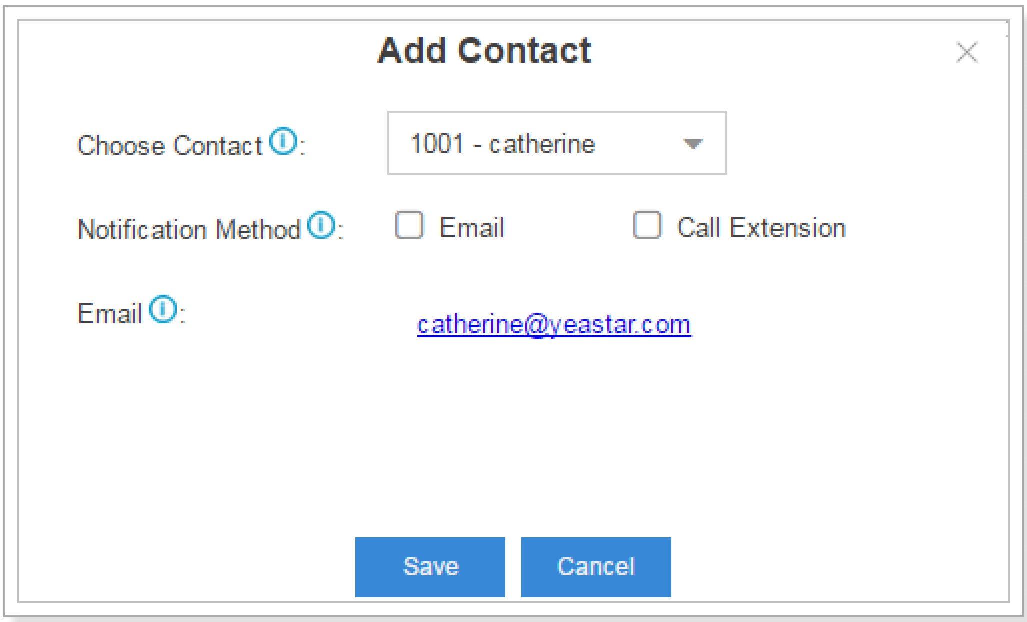
Name	Record	Notification	Edit Notification Template
Operation			
Modify Administrator Password	●	●	✎
User Login Success	●	○	✎
User Login Failed	●	○	✎
User Lockout	●	○	✎

Figure 11-1 Event Settings

Notification Contacts

The administrator could add contacts here to define where to send the notifications. The system supports to send Email notification and Call notification.

Click Add to add a contact.



Add Contact

Choose Contact ⓘ: 1001 - catherine

Notification Method ⓘ: □ Email □ Call Extension

Email ⓘ: catherine@yeastar.com

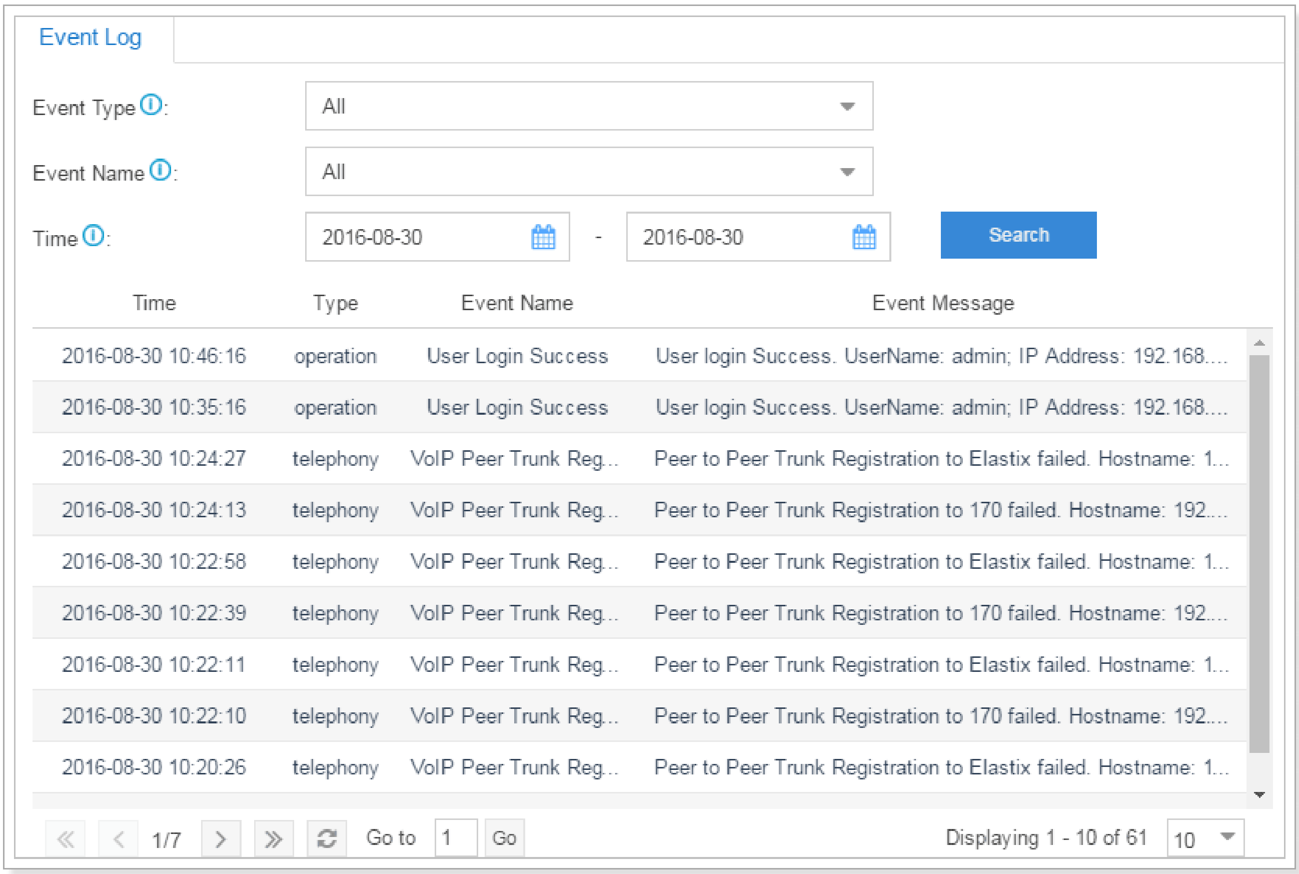
Figure 11-2 Notification Contacts

Table 11-1 Notification Contact Configuration Parameters

Option	Description
Choose Contact	Choose a contact from the drop-down menu. The selected contact will receive alert email or calls.
Notification Method	Select how to notify the contact when the event occurs. • Email • Call Extension • Call Mobile
Email	When events occur, send notification emails to this address. If the Notification Method is Email, this field must be entered.

Event Log

Go to **Settings > Event Center > Event Log** to check the event log.
You can filter the event logs by selecting a event type, event name, and specifying a certain time period. Click Search, the matching results will be displayed.



Event Type: All

Event Name: All

Time: 2016-08-30 - 2016-08-30

Time	Type	Event Name	Event Message
2016-08-30 10:46:16	operation	User Login Success	User login Success. UserName: admin; IP Address: 192.168....
2016-08-30 10:35:16	operation	User Login Success	User login Success. UserName: admin; IP Address: 192.168....
2016-08-30 10:24:27	telephony	VoIP Peer Trunk Reg...	Peer to Peer Trunk Registration to Elastix failed. Hostname: 1...
2016-08-30 10:24:13	telephony	VoIP Peer Trunk Reg...	Peer to Peer Trunk Registration to 170 failed. Hostname: 192....
2016-08-30 10:22:58	telephony	VoIP Peer Trunk Reg...	Peer to Peer Trunk Registration to Elastix failed. Hostname: 1...
2016-08-30 10:22:39	telephony	VoIP Peer Trunk Reg...	Peer to Peer Trunk Registration to 170 failed. Hostname: 192....
2016-08-30 10:22:11	telephony	VoIP Peer Trunk Reg...	Peer to Peer Trunk Registration to Elastix failed. Hostname: 1...
2016-08-30 10:22:10	telephony	VoIP Peer Trunk Reg...	Peer to Peer Trunk Registration to 170 failed. Hostname: 192....
2016-08-30 10:20:26	telephony	VoIP Peer Trunk Reg...	Peer to Peer Trunk Registration to Elastix failed. Hostname: 1...

Figure 11-3 Event Log

CDR and Recording

In CDR and Recording center, you can check all the call logs and recordings on the system. You can run reports against the logs and filter on the following:

- Time
- Call From
- Call To
- Call Duration
- Talk Duration
- Status
- Trunk
- Communication Type
- Account Code

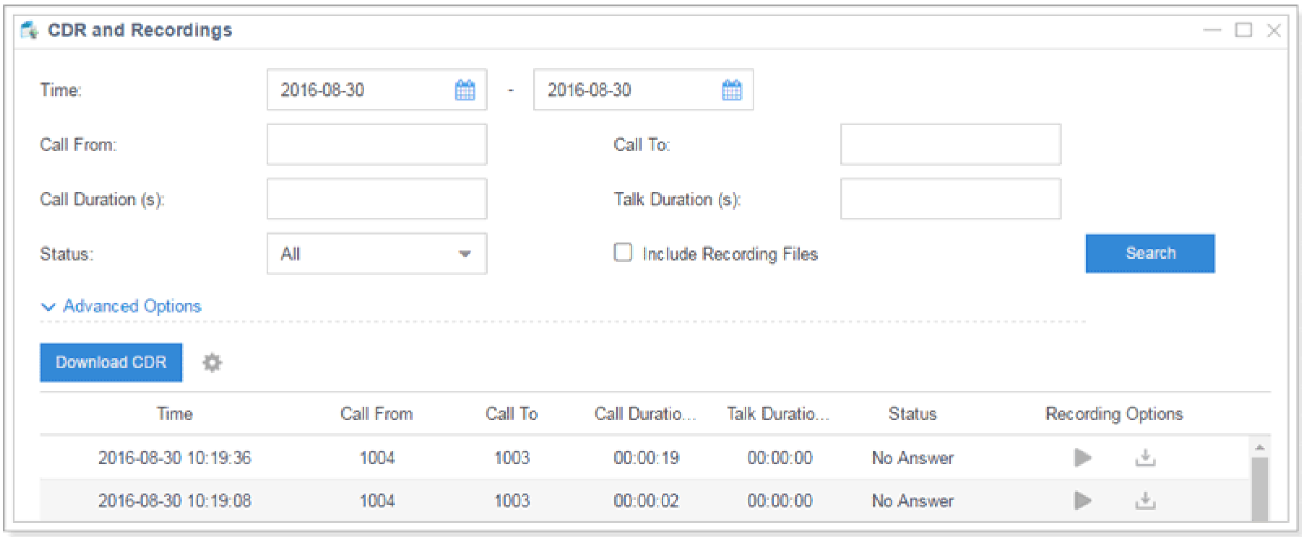
You can perform the following operations on the filtered call report:

- **Download Searched Result**
  Click Download the Records to download the searched records.
- **Edit List Options**

  Click ⚙ to choose which options will be displayed on the logs page.
- **Play Recording File**

  Click ▶ to play the recording file.
- **Download Recording File**

  Click ⭳ to play the recording file.



CDR and Recordings

Time:	2016-08-30	-	2016-08-30
Call From:		Call To:	
Call Duration (s):		Talk Duration (s):	
Status:	All	□ Include Recording Files	Search

Advanced Options

Download CDR ⚙

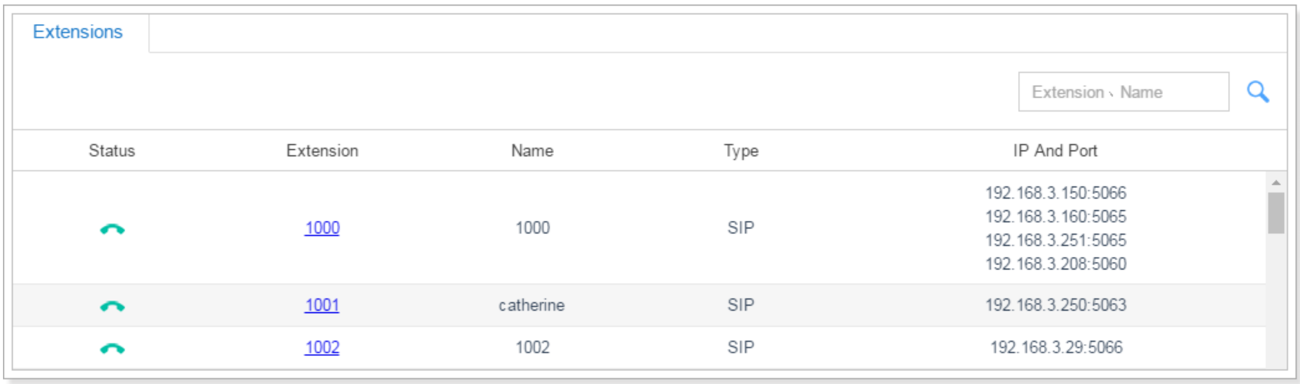
Time	Call From	Call To	Call Duratio...	Talk Duratio...	Status	Recording Options
2016-08-30 10:19:36	1004	1003	00:00:19	00:00:00	No Answer	▶ ⭳
2016-08-30 10:19:08	1004	1003	00:00:02	00:00:00	No Answer	▶ ⭳

Figure 12-1 CDR and Recording

PBX Monitor

The PBX monitors the status of Extensions, Trunks and Concurrent Call. Go to **PBX Monitor** to check the real time status.

Extension Status



Extensions

Extension、Name

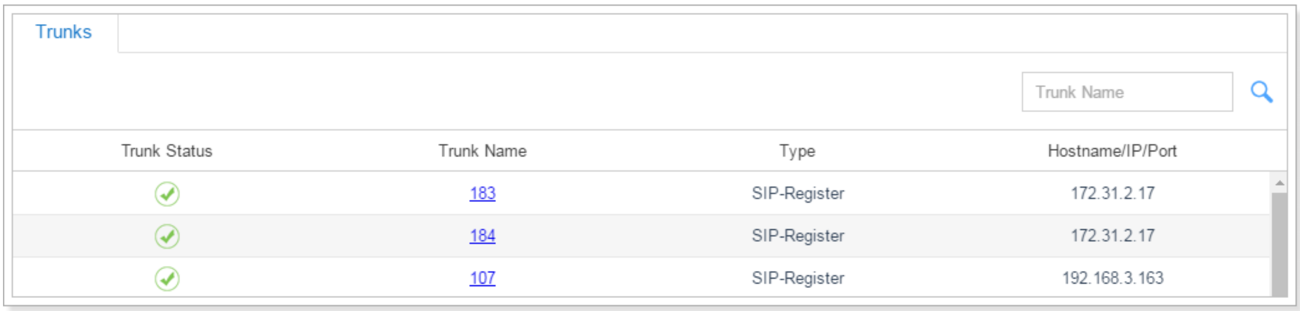
Status	Extension	Name	Type	IP And Port
☎	1000	1000	SIP	192.168.3.150:5066 192.168.3.160:5065 192.168.3.251:5065 192.168.3.208:5060
☎	1001	catherine	SIP	192.168.3.250:5063
☎	1002	1002	SIP	192.168.3.29:5066

Figure 13-1 Extension Status

Table 13-1 Extension Status Description

Status	Description
☎	The extension is idle.
☎	The extension is ringing.
☎	The extension is unavailable.
☎	The extension is busy.
☎	The extension is on hold.

Trunk Status



Trunks

Trunk Name

Trunk Status	Trunk Name	Type	Hostname/IP/Port
✓	183	SIP-Register	172.31.2.17
✓	184	SIP-Register	172.31.2.17
✓	107	SIP-Register	192.168.3.163

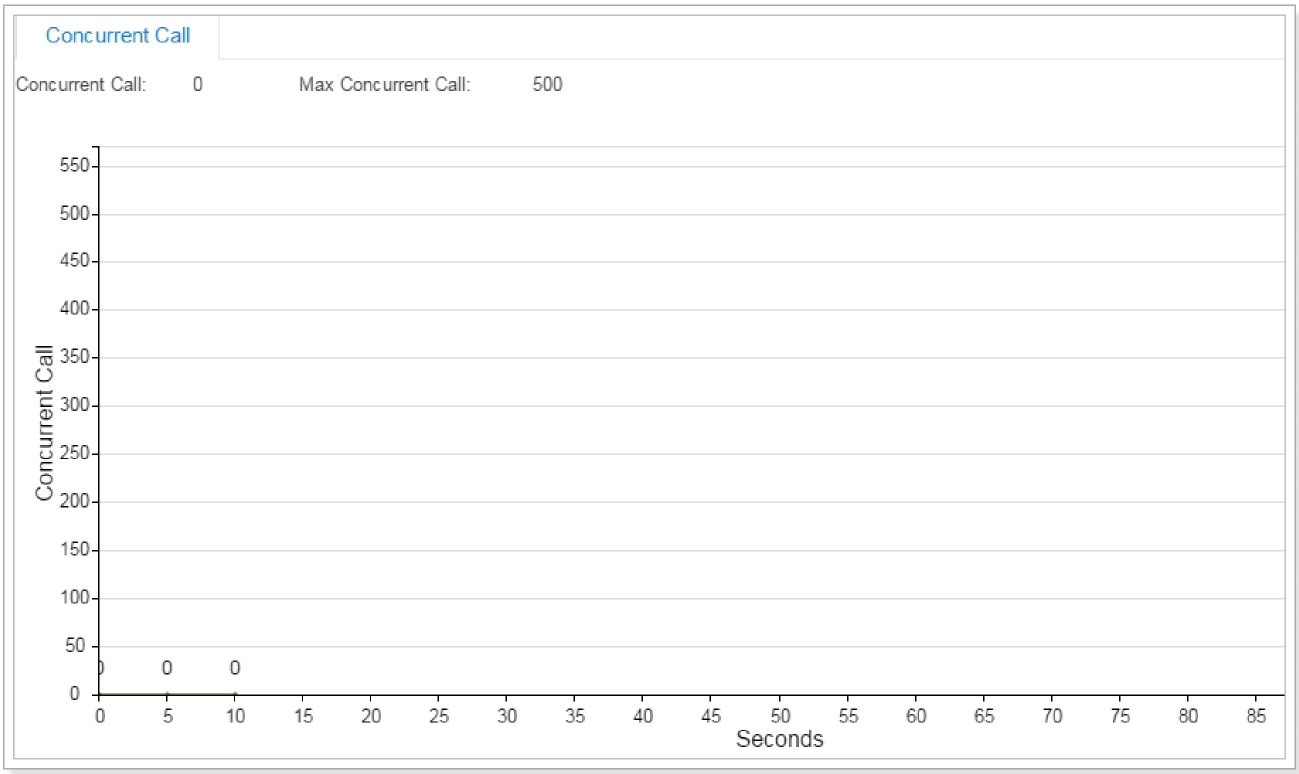
Figure 13-2 Trunk Status

Table 13-5 VoIP Trunk Status Description

VoIP Trunk Status	
✓	1. Registered 2. Unmonitored
↺	Registering.
⊗	1. Unreachable 2. Registration failed, caused by: ● wrong password ● wrong authentication name ● wrong username ● transport type inconsistent

Concurrent Call

Monitor the concurrent calls on the system.

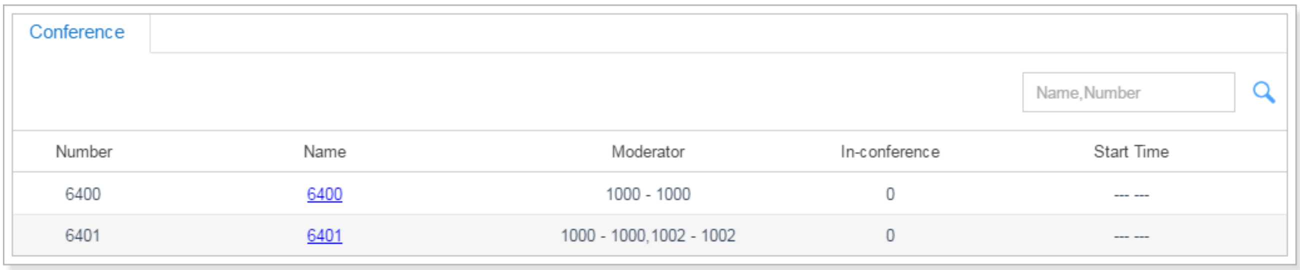


Concurrent Call: 0 Max Concurrent Call: 500

Figure 13-3 Concurrent Call

Conference

You can check the conference moderator, how many members in the conference, when the conference starts.

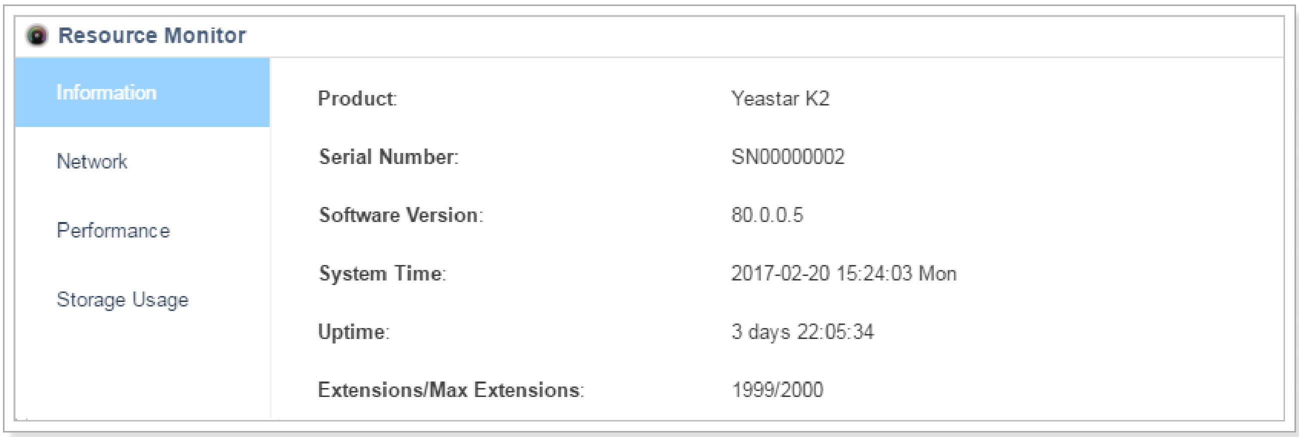


Number	Name	Moderator	In-conference	Start Time
6400	6400	1000 - 1000	0	--- ---
6401	6401	1000 - 1000,1002 - 1002	0	--- ---

Figure 13-4 Conference

Resource Monitor

Resource Monitor allows you to check device information and monitor the disk utilization and network flow.



Product:	Yeastar K2
Serial Number:	SN00000002
Software Version:	80.0.0.5
System Time:	2017-02-20 15:24:03 Mon
Uptime:	3 days 22:05:34
Extensions/Max Extensions:	1999/2000

- **Information**

  On this page, you can check the system information, including Product, SN, Hardware version, Software version etc.

- **Network**

  Click on **Network** tab to view the system's network status.

- **Performance**

  Click on **Performance** tab to view the resource utilization data. The information of the chart will be shown upon mouseover.

- **Storage Usage**

  Click on **Storage Usage** tab to check hard disk storage usage.

Maintenance

This chapter describes system maintenance settings including the followings:

- Upgrade
- Backup and Restore
- Reboot and Reset
- System Log
- Operation Log
- Trouble Shooting

Upgrade

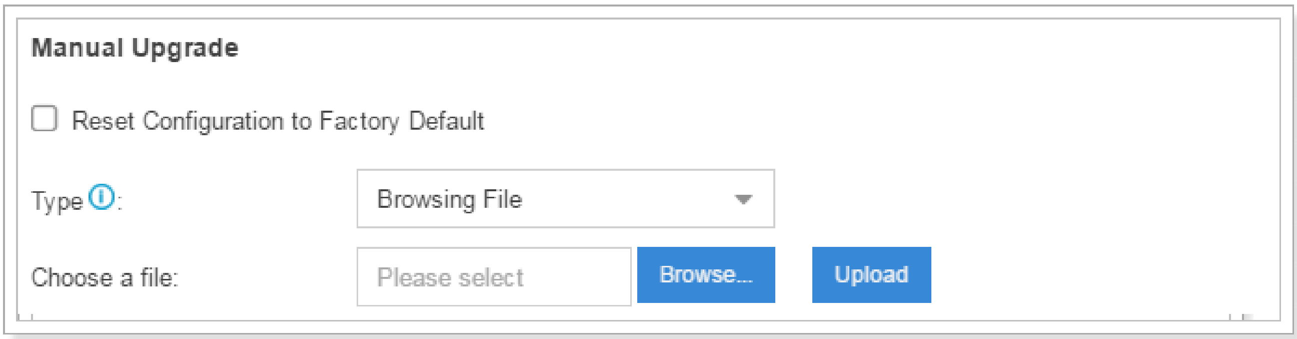
Yeastar K2 supports upgrading through TFTP, HTTP, also supports browsing firmware file from local PC. Go to **Maintenance > Upgrade** to do upgrade.

Note:

- If “Reset configuration to Factory Defaults” is enabled, the system will reset to factory default settings.
- When update the firmware, please don’t turn off the power. Or the system will get damaged.
- If you are trying to upgrade through HTTP or do auto upgrade, please make sure that the system is able to visit the Internet, or it cannot access Yeastar website to get the firmware file, causing the upgrade fail.

Browsing File from Local PC to Upgrade

1. Choose **Type** "Browsing File".
2. Click Browse, select the firmware file from your local PC. Note that the file should be a BIN file.
3. Click Upload to start uploading.



Manual Upgrade

□ Reset Configuration to Factory Default

Type ⓘ: Browsing File

Choose a file: Please select

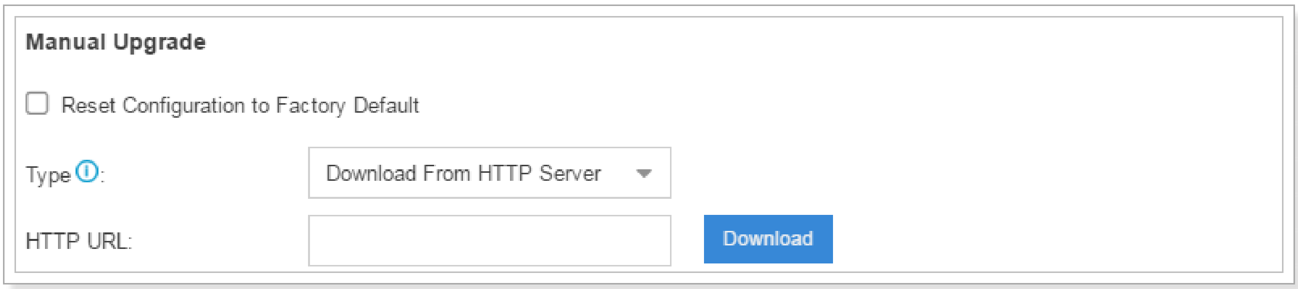
Figure 15-1 Upgrade Manually – Browsing File

Upgrade through HTTP

1. On the Firmware Upgrade page, choose **“**Download From HTTP Server”.

2. Enter the HTTP URL.
   Note: the HTTP URL should be a **BIN** file download link.

3. Click Download to start downloading the file from Yeastar HTTP server.



Manual Upgrade

□ Reset Configuration to Factory Default

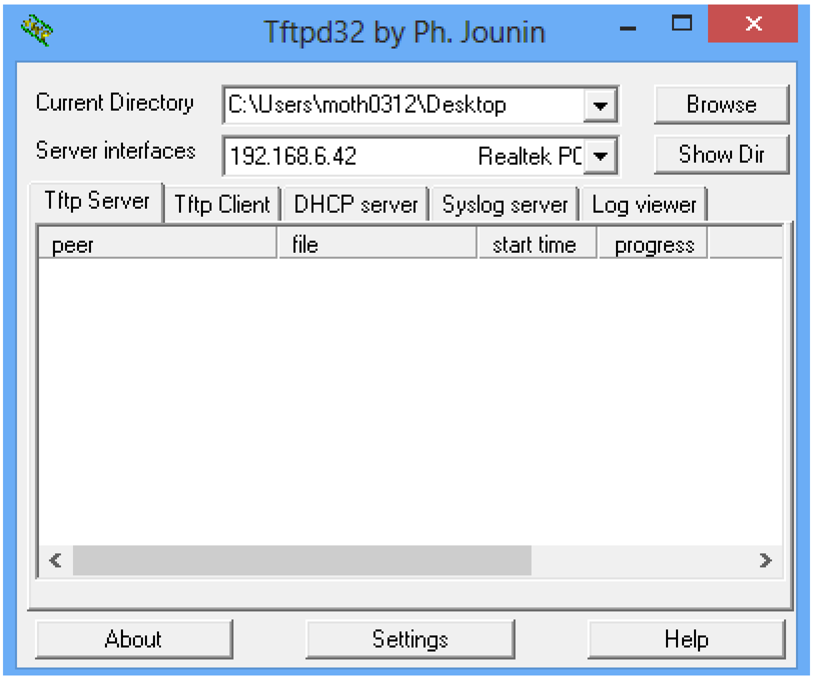
Type: Download From HTTP Server

HTTP URL:

Figure 15-2 Upgrade Manually - HTTP

Upgrade through TFTP

1. Download firmware file from Yeastar website to your local PC.
2. Create a tftp server, here take Tftpd32 for example.
3. Configure tftp server. Click **Browse** button to select the firmware file upgraded patch.



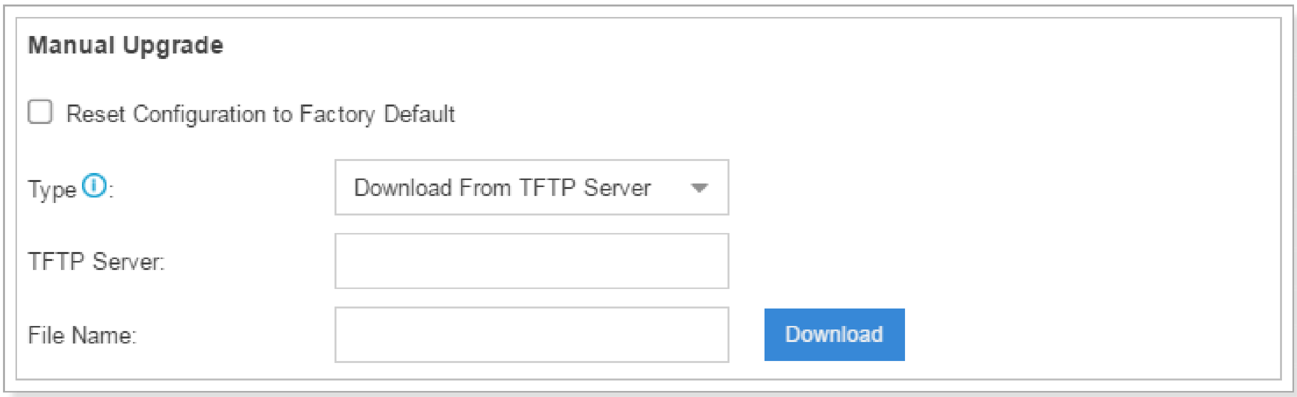
Tftpd32 by Ph. Jounin

Current Directory: C:\Users\moth0312\Desktop

Server interfaces: 192.168.6.42 Realtek PC

Figure 15-3 TFTP32 Settings

4. Go to Yeastar system upgrade page, select **Type** as "Download From TFTP Server".
5. Fill in the **TFTP Server IP**, the IP should be the local PC's IP address.
6. Fill in the name of firmware update. It should be a BIN file name.
7. Click **Download** to download the file and start to upgrade.



Manual Upgrade

□ Reset Configuration to Factory Default

Type ⓘ: Download From TFTP Server ▾

TFTP Server:

File Name:

Download

Figure 15-4 Upgrade Manually – TFTP

Backup and Restore

Yeastar K2 provides Backup and Restore feature, which allows you to create a complete backup of the system configurations to a file.

Note:

- When you have updated the firmware version, it's not recommended to restore using old package.
- Backup from an later version cannot be restored on the system of an earlier version.

- **Create a New Backup**

  Click Backup to create a new backup.

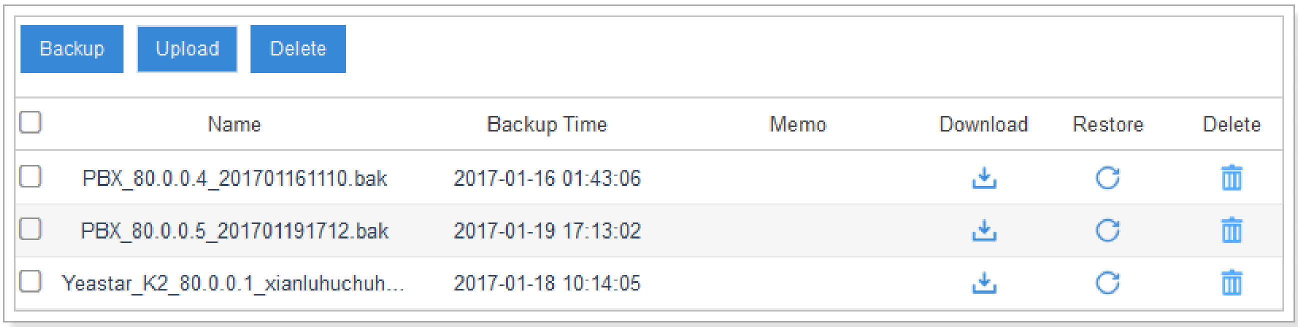
- **Upload a Backup**

  Click Upload to upload a backup.

- **Restore**

  To restore the configuration data, select a backup and click ↻. Reboot the system to take effect.

  Note: the current configurations will be OVERWRITTEN with the backup data.



Backup Upload Delete

□	Name	Backup Time	Memo	Download	Restore	Delete
□	PBX_80.0.0.4_201701161110.bak	2017-01-16 01:43:06		⭳	↻	🗑
□	PBX_80.0.0.5_201701191712.bak	2017-01-19 17:13:02		⭳	↻	🗑
□	Yeastar_K2_80.0.0.1_xianluhuchuh...	2017-01-18 10:14:05		⭳	↻	🗑

Figure 15-5 Restore Backup File

Reset and Reboot

Users could reset and reboot the system via **Maintenance > Reset and Reboot**.

- Click Reboot to reboot the system
- Click Reset to reset the system to factory configurations.

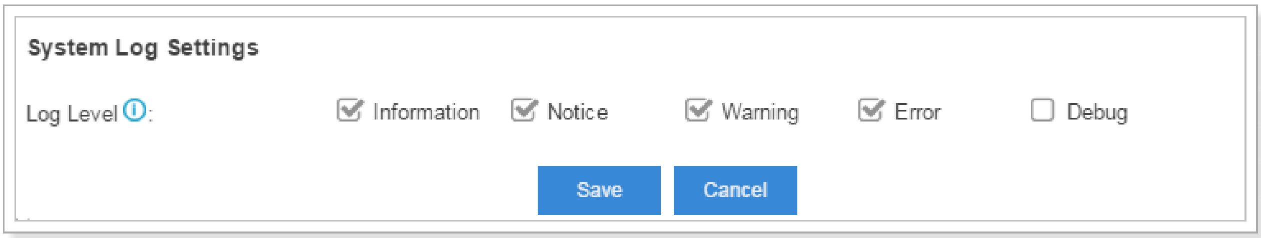
System Log

Users could check system logs under **Maintenance > System Log**.

The system logs will be generated everyday automatically and a log file will be listed in the System Log.

1) **System Log Settings**

   You can set the debug level by checking/unchecking the options "Info", "Notice", "Warning", "Error" and "Debug", click Save and Apply to save the changes.



System Log Settings

Log Level ⓘ: ☑ Information ☑ Notice ☑ Warning ☑ Error □ Debug

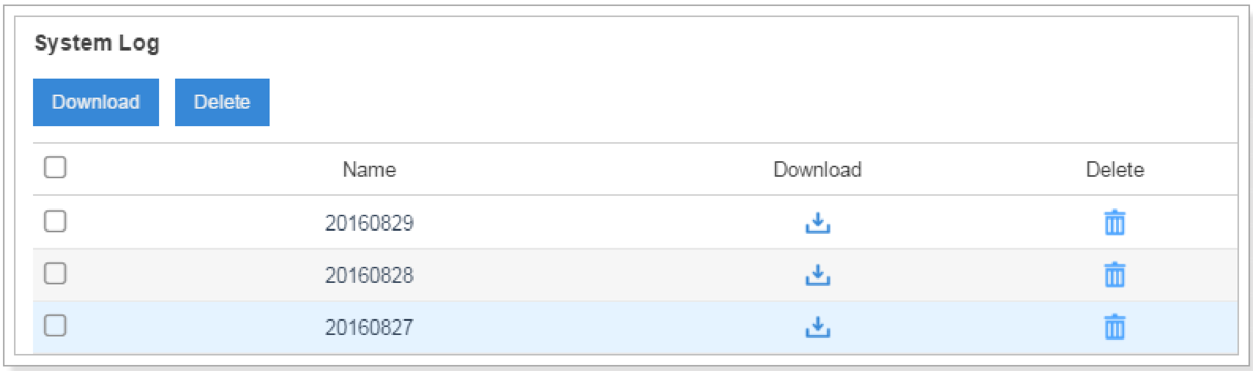
Save Cancel

Figure 15-6 System Log Settings

2) **System Log**

   Click ⭳ to download the file to your local PC.

   Click 🗑 to delete the log file.

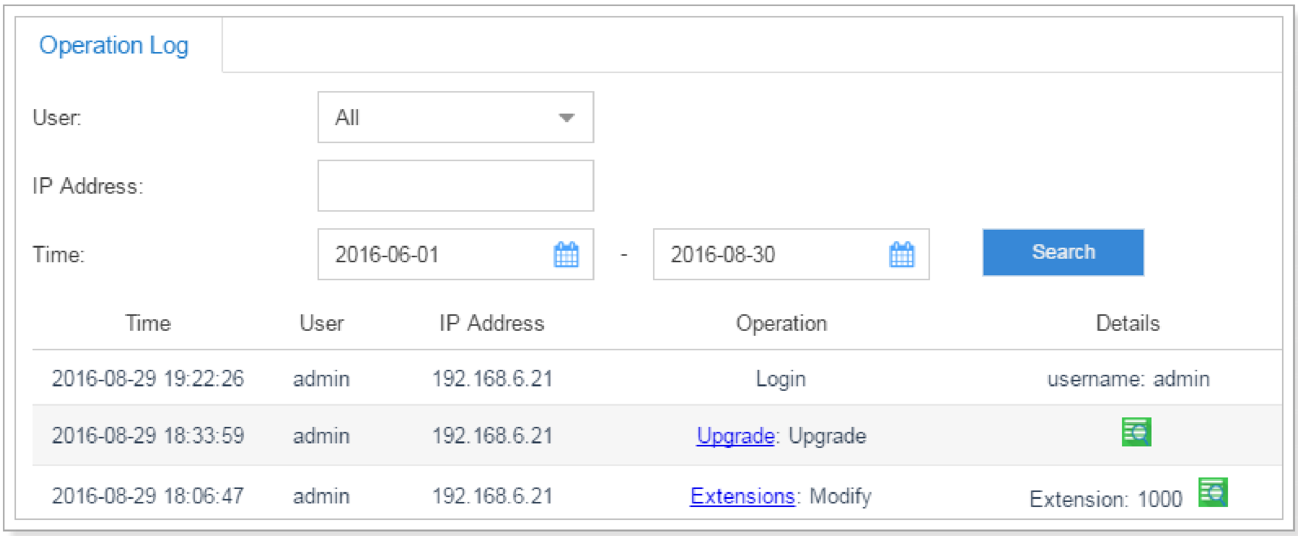


□	Name	Download	Delete
□	20160829	⬇	🗑
□	20160828	⬇	🗑
□	20160827	⬇	🗑

Figure 15-7 System Log

Operation Log

Go to **Maintenance > Operation Log** to check the operation log.
You can filter the logs by user, IP address, and specifying a certain time period. Click Search, the matching results will be displayed.



User: All

IP Address:

Time: 2016-06-01 - 2016-08-30

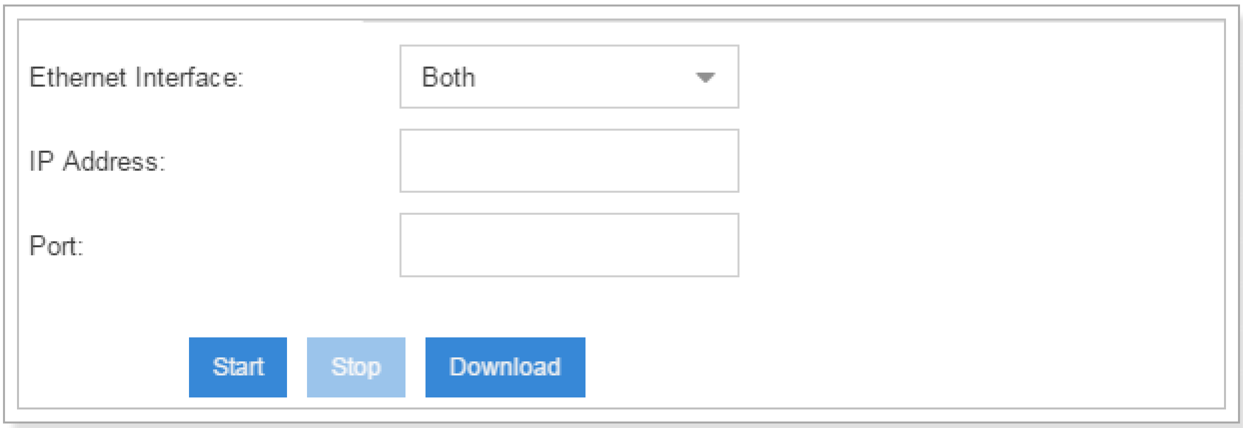
Time	User	IP Address	Operation	Details
2016-08-29 19:22:26	admin	192.168.6.21	Login	username: admin
2016-08-29 18:33:59	admin	192.168.6.21	Upgrade: Upgrade	🔍
2016-08-29 18:06:47	admin	192.168.6.21	Extensions: Modify	Extension: 1000 🔍

Figure 15-8 Operation Log

Troubleshooting

Yeastar K2 provides multiple tools on the Web GUI for you to do troubleshooting. Go to **Maintenance > Troubleshooting** to check the tools.

Ethernet Capture Tool



Ethernet Interface: Both

IP Address:

Port:

Figure 15-9 Ethernet Capture Tool

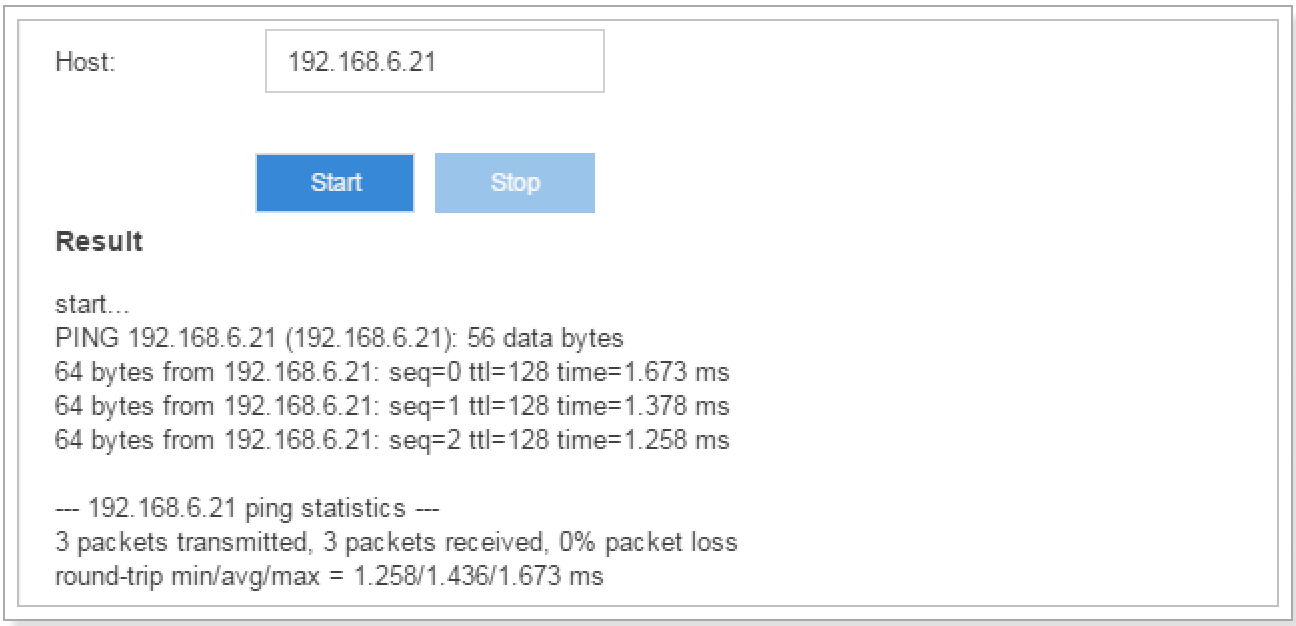
1. Fill in the target IP address and port.
2. Click **Start** to start capturing logs.
3. Click **Stop** to stop capturing.
4. Click **Download** to download the file to your local PC and analyze it.

The output result is in .tar format. Decompress the file and open the .pcap file using Wireshark software.

IP Ping

1. Enter the target IP address or hostname.
2. Click **Start** to start capturing logs.

The output result will display in the window as below.



Host: 192.168.6.21

Result

```
start...
PING 192.168.6.21 (192.168.6.21): 56 data bytes
64 bytes from 192.168.6.21: seq=0 ttl=128 time=1.673 ms
64 bytes from 192.168.6.21: seq=1 ttl=128 time=1.378 ms
64 bytes from 192.168.6.21: seq=2 ttl=128 time=1.258 ms

--- 192.168.6.21 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 1.258/1.436/1.673 ms
```

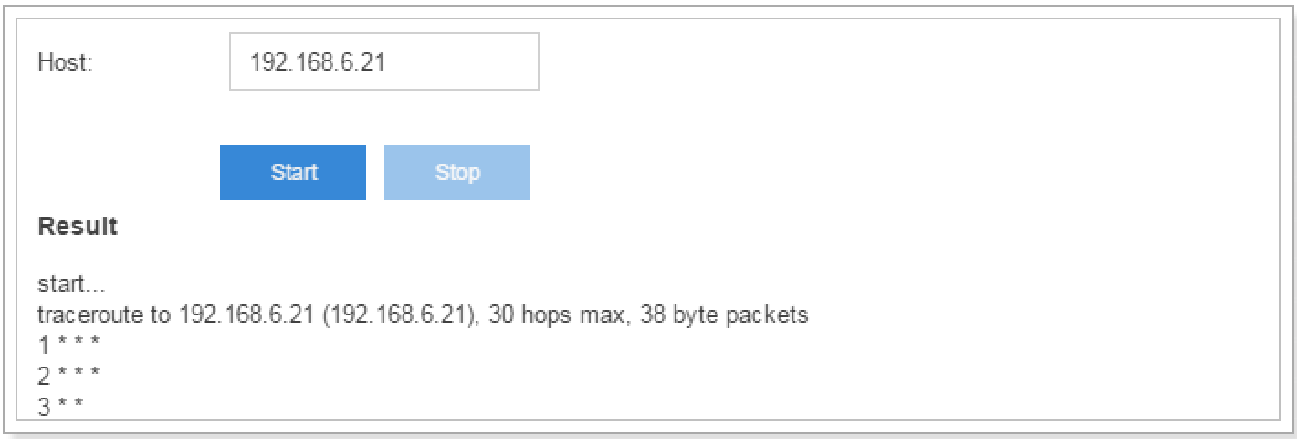
Figure 15-10 IP Ping

Traceroute

1. Enter the target IP address or hostname.

2. Click **Start** to start capturing logs.

The output result will display in the window as below.



Host: 192.168.6.21

```
start...
traceroute to 192.168.6.21 (192.168.6.21), 30 hops max, 38 byte packets
1 * * *
2 * * *
3 * *
```

Figure 15-11 Traceroute