TG Series GSM VoIP Gateway User 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: 91.1.0.7
Revised: March 1, 2018

Copyright

Copyright 2006-2018 Xiamen Yeastar Information Technology Co., Ltd. **All rights reserved.**
No parts of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, photocopying, recording, or otherwise, for any purpose, without the express written permission of Xiamen Yeastar Information Technology Co., Ltd. Under the law, reproducing includes translating into another language or format.

Declaration of Conformity

Hereby, Xiamen Yeastar Information Technology Co., Ltd. declares that Yeastar TG series gateways are in conformity with the essential requirements and other relevant provisions of the CE, FCC.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.
These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement

- This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.
- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.

Warranty

The information in this document is subject to change without notice.

Xiamen 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. Xiamen 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.

Table of Contents

About This Guide **7**
TG Series Overview **8**
Hardware Specification 8
TG200 Gateway Overview 8
TG400 Gateway Overview 10
TG800 Gateway Overview 11
TG1600 Gateway Overview 13
Hardware Installation **15**
Package Contents 15
Safety Disclaimers and Installation Warnings 15
Insert/Remove SIM Card 16
Desktop Installation 16
Connect Antennas 17
Rack Installation 18
Ground Connection 19
Connect Your Gateway 20
Getting Started **21**
Log in Web User Interface 21
Web Configuration Panel 22
Manage GSM Modules **23**
Configure GSM Module Profile 23
Reboot GSM Modules 24
Enable/Disable GSM Modules 24
Adjust GSM Module Volume 24
Configure the Call Duration of Mobile Trunks 25
Configure Network Type and Band 28
Unlock the SIM Card 29
Configure SIM Card Forwarding and CLIR 29
Group Mobile Trunks 30

Connect TG Gateway to Your PBX (Account Mode) 32
Connect TG Gateway to Your PBX (Account Mode) 32
Set up a Mobile to IP Route (Account Mode) 33
Set up an IP to Mobile Route (Account Mode) 33
Connect TG Gateway to Your PBX (Register Trunk) 35
Connect TG Gateway to Your PBX (Register Trunk Mode) 35
Set up a Mobile to IP Route (Register Trunk Mode) 36
Set up an IP to Mobile Route (Register Trunk Mode) 37
Connect TG Gateway to Your PBX (Peer Trunk) 39
Connect TG Gateway to Your PBX (Peer Trunk Mode) 39
Set up a Mobile to IP Route (Peer Trunk Mode) 40
Set up an IP to Mobile Route (Peer Trunk Mode) 40
Call Control 42
Route Calls Based on Caller ID 42
Route Calls Based on Destination Numbers 42
Block Incoming Numbers 43
Block Outgoing Numbers 43
Callback 44
AutoCLIP Route 46
Manage Messages 47
Send SMS Messages 47
Manage SMS Contacts 48
Manage Sent SMS Messages 48
Manage Received SMS Messages 49
SMS to Email 51
Email to SMS 53
Schedule SMS Clear Tasks 54
Send USSD Messages 55
Enable TG Gateway API 56
Change Password of SMS Center 56
Configure System Settings 58
Change Web Login Password 58

Change Date and Time 58
Upload Custom Prompts 59
Set up System Email 59
Update System Firmware 60
Backup and Restore 62
Reboot the System 64
Schedule Automatic Reboots 64
Reset the System 65
Configure System Network 66
Change the IP Address of TG Gateway 66
Set up VLAN for the TG Gateway 66
Set up OpenVPN Network 67
Set up DDNS for the TG Gateway 68
Static Route 68
Configure VoIP Settings 70
Group VoIP Trunks 70
Configure SIP Settings 70
Configure IAX Settings 75
Configure General Preferences 75
Secure Your Gateway 76
Security Center 76
Configure Alert Settings 76
Upload Certificate Files 77
Configure Firewall Rules 78
System Status 81
Check Trunk Status 81
Check Network Status 82
Check System Info 82
Reports 84
Call Logs 84
System Logs 85

About This Guide

Thanks for choosing Yeastar TG Series GSM gateway.

This guide will help you learn how to operate and manage your TG gateway. In this guide, we describe every detail on the functionality and configuration of the TG series gateway. We begin by assuming that you are interested in TG series gateway and familiar with networking and other IT disciplines.

Products Covered

This guide explains how to configure the following Yeastar TG series gateways:

- NeoGate TG200
- NeoGate TG400
- NeoGate TG800
- NeoGate TG1600

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.

TG Series Overview

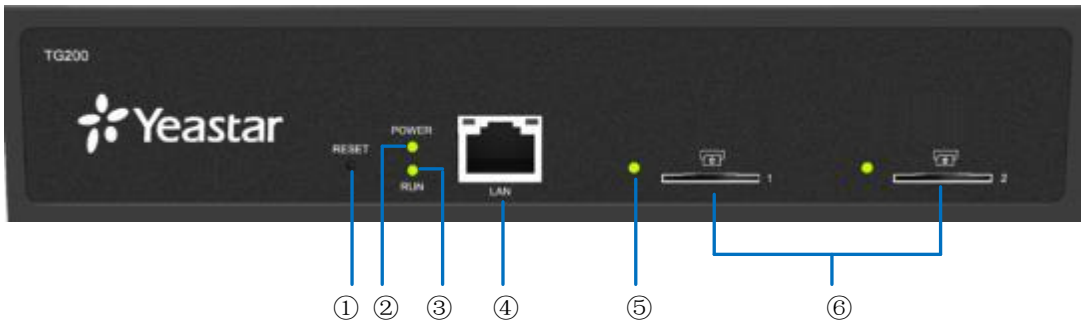
- NeoGate TG200 Gateway Overview
- NeoGate TG400 Gateway Overview
- NeoGate TG800 Gateway Overview
- NeoGate TG1600 Gateway Overview

Hardware Specification

Hardware	TG200	TG400	TG800	TG1600
GSM Channel	2	4	8	16
GSM Frequency	850/900/1800/1900 MHz			
Antenna Splitter (4 in 1)	Support			
Dimensions (L × W × H) (mm)	213 x 160 x 44		340x210x44	440x250x44
Power Supply	AC 100-240V			
Operation Range	0°C to 40°C, 32°F to 104°F			
Humidity	10-90% non-condensing			
Storage Range	-20°C to 65°C, -4°F to 149°F			

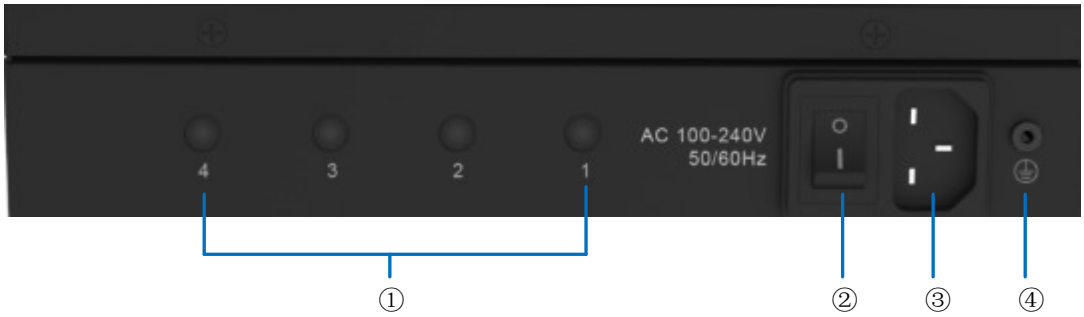
TG200 Gateway Overview

TG200 Gateway Front Panel



No.	Feature	Description
①	Reset Button	Press and hold for 10 seconds to restore the factory defaults
②	Power LED	Indicates the power status. • On: the power is switched on. • Off: the power is switched off.
③	RUN LED	Indicates the system status. • Blinking: the system is working properly. • Static Green/Off: the system goes wrong.
④	LAN Port	10/100 adaptive RJ45 Ethernet port.
⑤	GSM Module LED	Indicates the GSM module status. • Static Green: the module and the inserted SIM card are working properly. • Blinking Slowly: no SIM card is detected or the port is working improperly. • Blinking Quickly: there is an ongoing call on the port. • Off: no module is inserted or the module is damaged.
⑥	SIM Card Slot	Insert the SIM card to the SIM card slot.

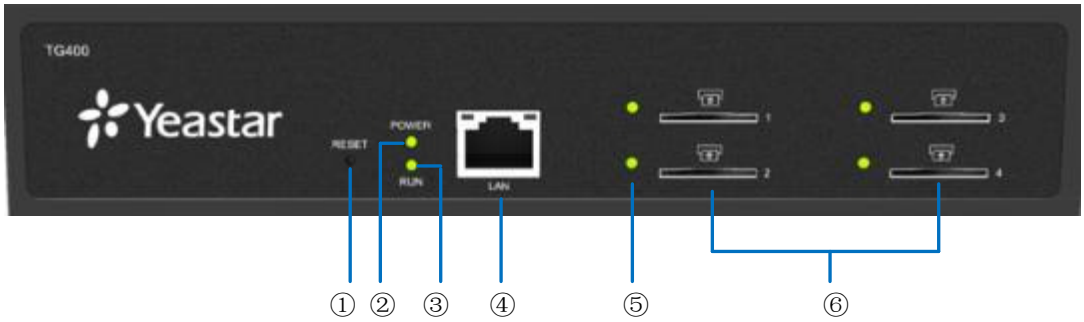
TG200 Gateway Back Panel



No.	Feature	Description
①	Antenna Connector	Connect to GSM Antenna. Port 3 and Port 4 are invalid.
②	Power Switch	Press this button to switch on/off the device.
③	Power Interface	Connect the supplied power supply to the port.
④	Grounding Earth	Protects the personnel and the equipment.

TG400 Gateway Overview

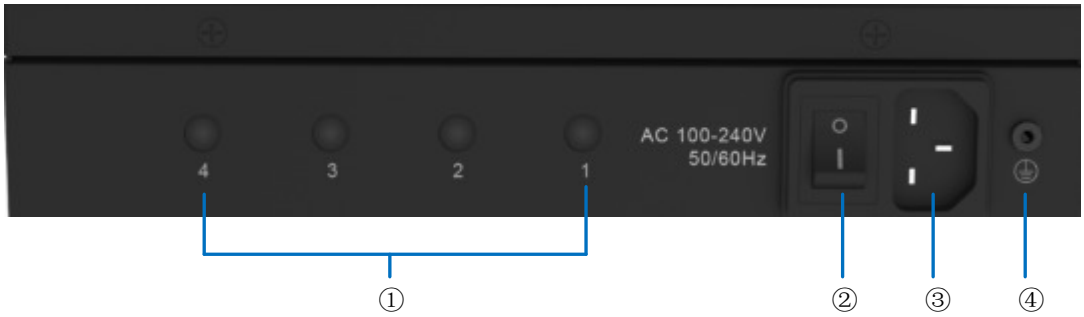
TG400 Gateway Front Panel



No.	Feature	Description
①	Reset Button	Press and hold for 10 seconds to restore the factory defaults
②	Power LED	Indicates the power status. • On: the power is switched on. • Off: the power is switched off.
③	RUN LED	Indicates the system status. • Blinking: the system is working properly. • Static Green/Off: the system goes wrong.

④	LAN Port	10/100 adaptive RJ45 Ethernet port.
⑤	GSM Module LED	Indicates the GSM module status. • Static Green: the module and the inserted SIM card are working properly. • Blinking Slowly: no SIM card is detected or the port is working improperly. • Blinking Quickly: there is an ongoing call on the port. • Off: no module is inserted or the module is damaged.
⑥	SIM Card Slot	Insert the SIM card to the SIM card slot.

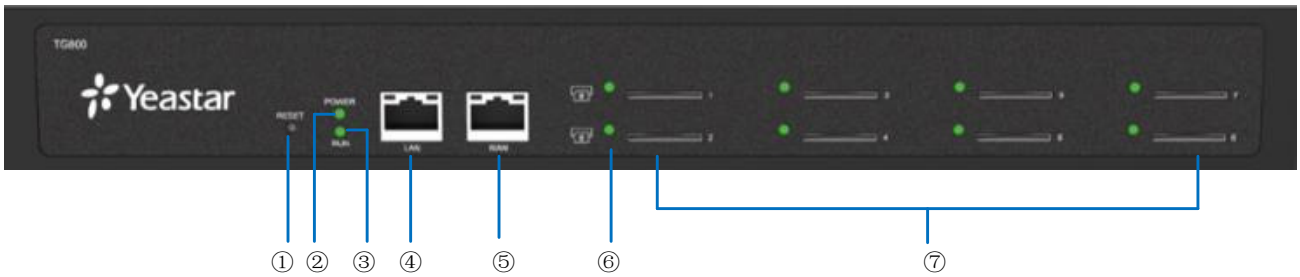
TG400 Gateway Back Panel



No.	Feature	Description
①	Antenna Connector	Connect to GSM Antenna.
②	Power Switch	Press this button to switch on/off the device.
③	Power Interface	Connect the supplied power supply to the port.
④	Grounding Earth	Protects the personnel and the equipment.

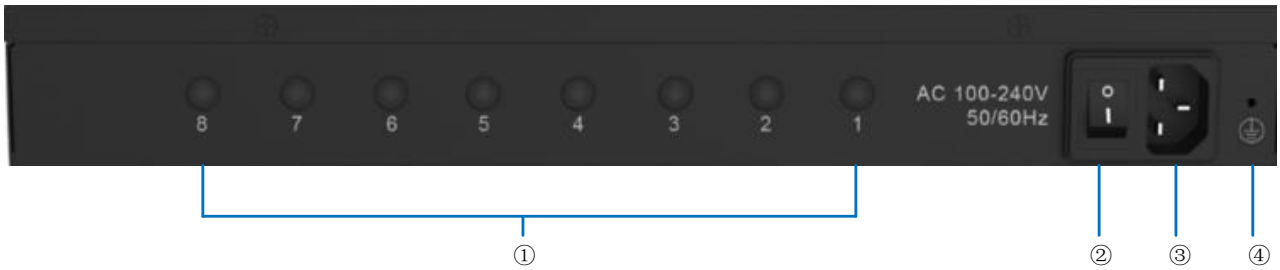
TG800 Gateway Overview

TG800 Gateway Front Panel



No.	Feature	Description
①	Reset Button	Press and hold for 10 seconds to restore the factory defaults
②	Power LED	Indicates the power status. • On: the power is switched on. • Off: the power is switched off.
③	RUN LED	Indicates the system status. • Blinking Green: the system is working properly. • Static Green/Off: the system goes wrong.
④	LAN Port	10/100 adaptive RJ45 Ethernet port.
⑤	WAN Port	10/100 adaptive RJ45 Ethernet port.
⑥	GSM Module LED	Indicates the GSM module status. • Static Green: the module and the inserted SIM card are working properly. • Blinking Slowly: no SIM card is detected or the port is working improperly. • Blinking Quickly: there is an ongoing call on the port. • Off: no module is inserted or the module is damaged.
⑦	SIM Card Slot	Insert the SIM card to the SIM card slot.

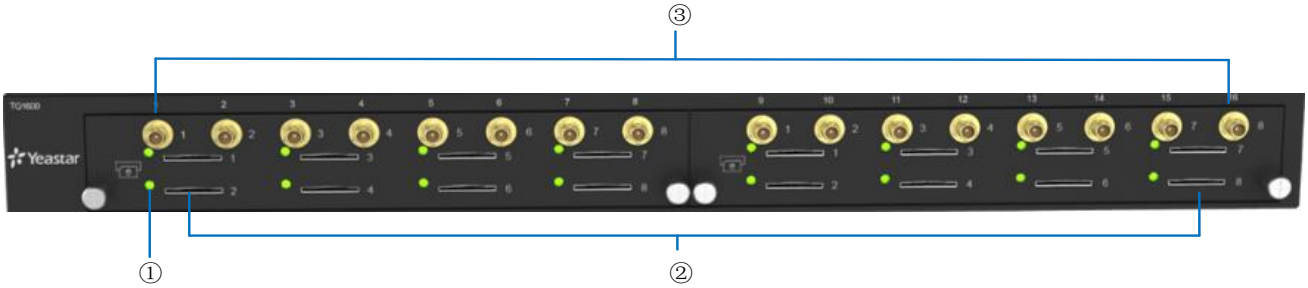
TG800 Gateway Back Panel



No.	Feature	Description
①	Antenna Connector	Connect to GSM Antenna.
②	Power Switch	Press this button to switch on/off the device.
③	Power Interface	Connect the supplied power supply to the port.
④	Grounding Earth	Protects the personnel and the equipment.

TG1600 Gateway Overview

TG1600 Gateway Front Panel



No.	Feature	Description
①	GSM Module LED	Indicates the GSM module status. • Static Green: the module and the inserted SIM card are working properly. • Blinking Slowly: no SIM card is detected or the port is working improperly. • Blinking Quickly: there is an ongoing call on the port. • Off: no module is inserted or the module is damaged.
②	SIM Card Slot	Insert the SIM card to the SIM card slot.
③	Antenna Connector	Connect to GSM Antenna.

TG1600 Gateway Back Panel

No.	Feature	Description
①	Power LED	Indicates the power status. • On: the power is switched on. • Off: the power is switched off.
②	RUN LED	Indicates the system status. • Blinking Green: the system is working properly. • Static Green/Off: the system goes wrong.

③	WAN Port	10/100 adaptive RJ45 Ethernet port.
④	LAN Port	10/100 adaptive RJ45 Ethernet port.
⑤	Reset Button	Press and hold for 10 seconds to restore the factory defaults
⑥	Power Switch	Press this button to switch on/off the device.
⑦	Power Interface	Connect the supplied power supply to the port.
⑧	Grounding Earth	Protects the personnel and the equipment.

Hardware Installation

- Package Contents
- Safety Disclaimers and Installation Warnings
- Insert/Remove SIM Card
- Desktop Installation
- Rack Installation
- Ground Connection
- Connect Your Gateway

Package Contents

Check the package contents before you start to step up the TG gateway.

Item	TG200	TG400	TG800	TG1600
TG Gateway	1	1	1	1
Power cord	1	1	1	1
Warranty card	1	1	1	1
Network cable	1	1	1	1
Antenna	2	4 or 1 Antenna Splitter	8 or 2 Antenna Splitters	16 or 4 Antenna Splitters
Mounting ear	3	3	2	2
Screws	9	9	8	8
Grounding stud and nut	1	1	1	1
Rubber feet	4	4	4	4
Quick Start Guide	1	1	1	1

Safety Disclaimers and Installation Warnings

To avoid unexpected accident, personal injury or device damage, read the safety disclaimers and installation warnings.

Power

- Use only the power cord provided with the Yeastar TG gateway.
- Make sure that the supply voltage matches the specifications indicated on the back panel of the device.
- To avoid the electric accident, do not open or remove the cover of TG gateway when it is working as well as off the power.
- Before cleaning the TG gateway, cut off the power supply.

Environment

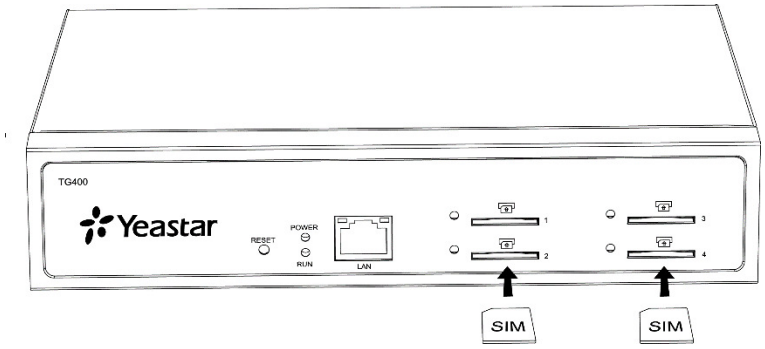
Install the Yeastar TG gateway in a location that is clean, free from vibration, electric shock, and temperature/humidity extremes. The operating temperature should be kept below 104°F (40°C).

Insert/Remove SIM Card

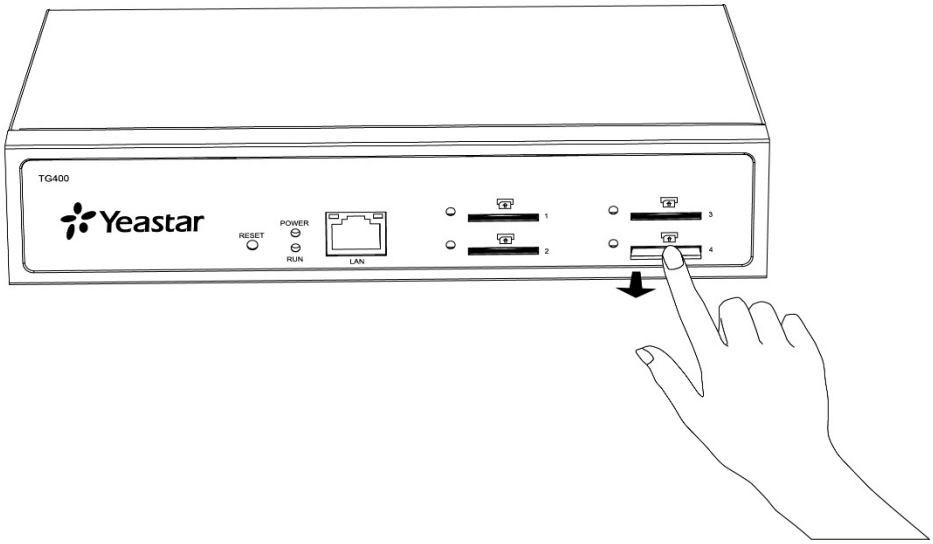
Yeastar TG gateway supports hot plugging of SIM cards. You can insert and remove your SIM cards to the TG gateway directly without powering off the device.

Procedure

1. Insert the SIM card with the angled corner in first and the contact area facing down.



2. Press the SIM card to remove the SIM card.



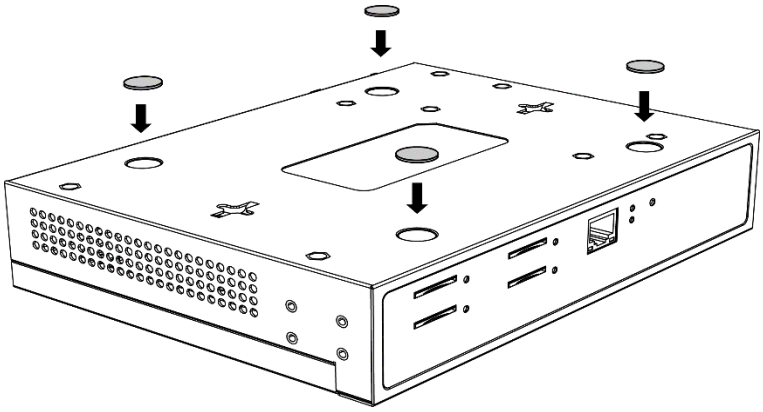
Desktop Installation

WARNING

- Please set 5~10cm gaps around the device for air circulation.
- Please avoid any heavy thing placed on the device.

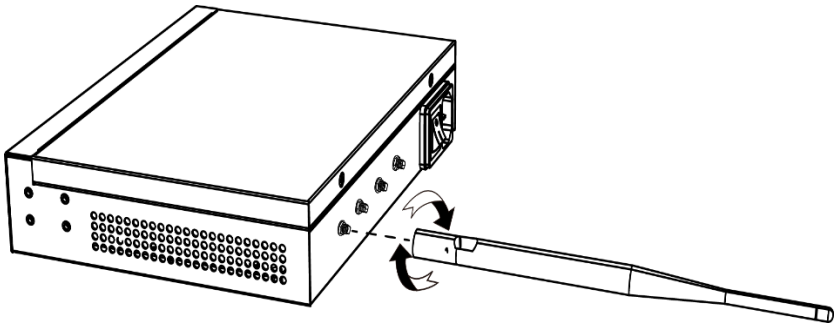
Procedure

1. Place the TG gateway on a steady platform.
2. Remove the adhesive backing paper from the rubber feet.
3. Turn over the device and attach the supplied rubber feet to the recessed areas on the bottom at each corner of the device.

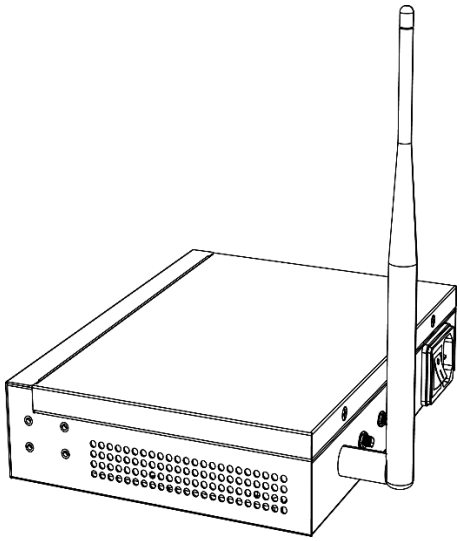


Connect Antennas

1. Connect the external antenna on a site with a good wireless signal. Rotate the antenna into the antenna connector.



2. Adjust the angle of the antenna.



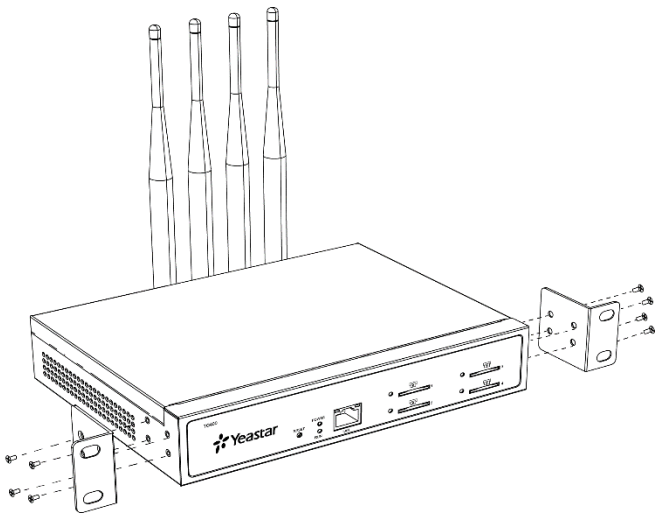
Rack Installation

WARNING

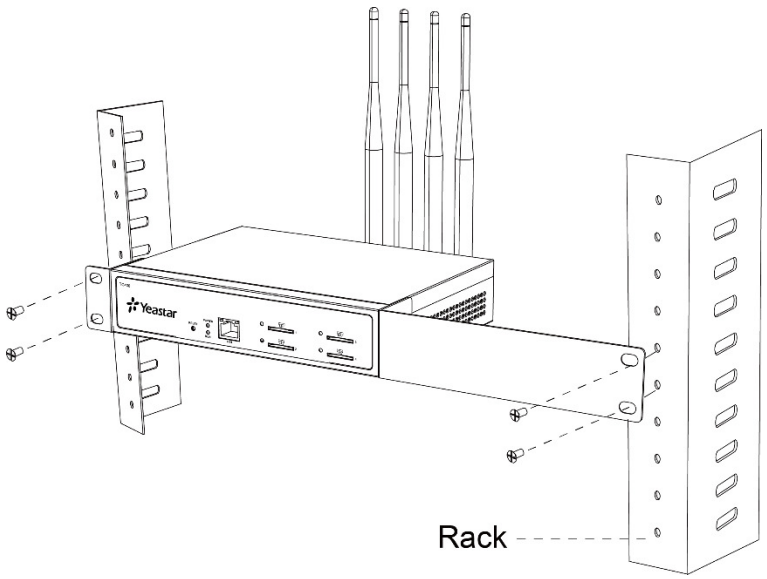
- Be careful not to drop any components. Dropping components may damage them or cause an injury.

Procedure

1. Fix the brackets to the left and right sides of the TG gateway with 4 screws.



2. Place the TG gateway in the 19-inch rack and fix both brackets to the rack with the rack's proprietary mounting equipment.



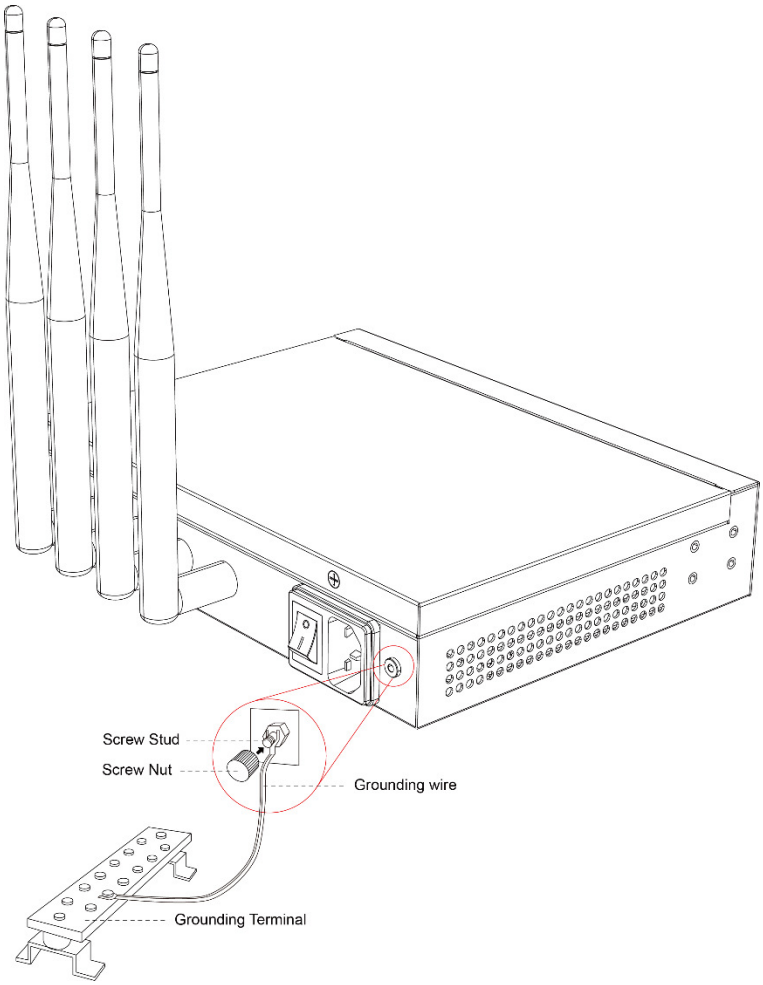
Ground Connection

WARNING

- Proper grounding (connection to ground) is very important to reduce the risk to the user of electrocution or protect the TG gateway from the bad effects of external noise in the case of a lightning strike.
- A permanent connection between ground and the ground terminal of the TG gateway must be made.

Procedure

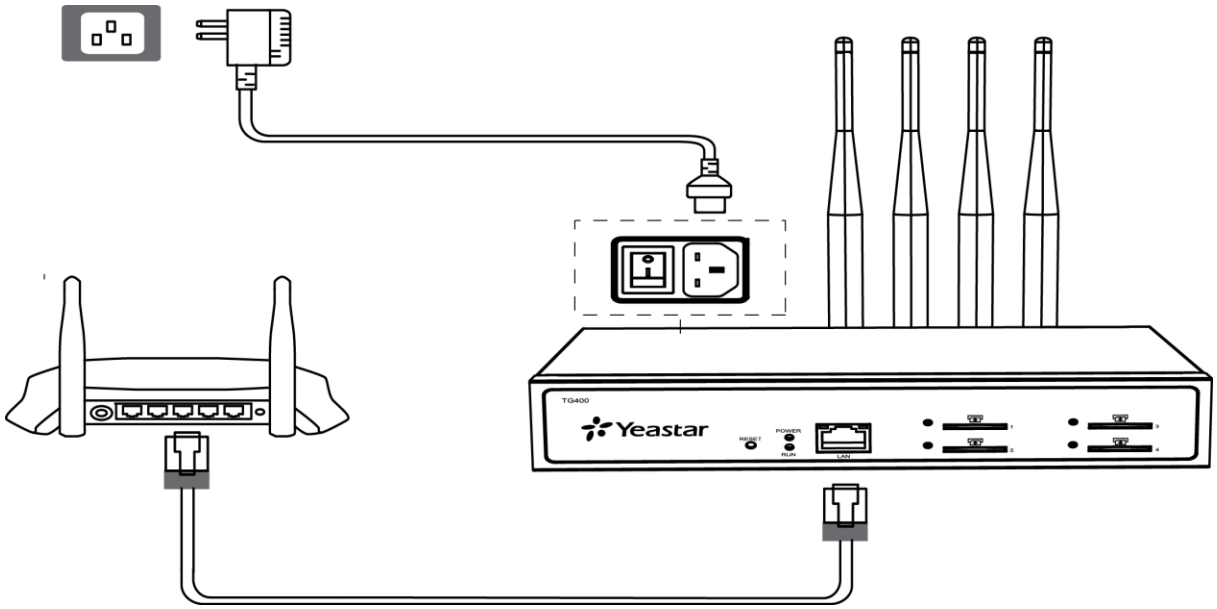
1. Tighten the provided screw stud into the Grounding port on TG gateway.
2. Insert a grounding wire (user supplied).
3. Tighten the provided screw nut.
4. Attach the grounding wire to the grounding terminal.



Connect Your Gateway

Procedure

1. Connect one end of a network cable to the LAN port of TG gateway, and the other end to any port of your company's LAN switch/router.
2. Plug the provided power cord into the power inlet on TG gateway and the other end to a standard electrical wall socket. Wait for the system to boot up till the **RUN** LED starts to blink.



Getting Started

- Log in Web User Interface
- Web Configuration Panel

Log in Web User Interface

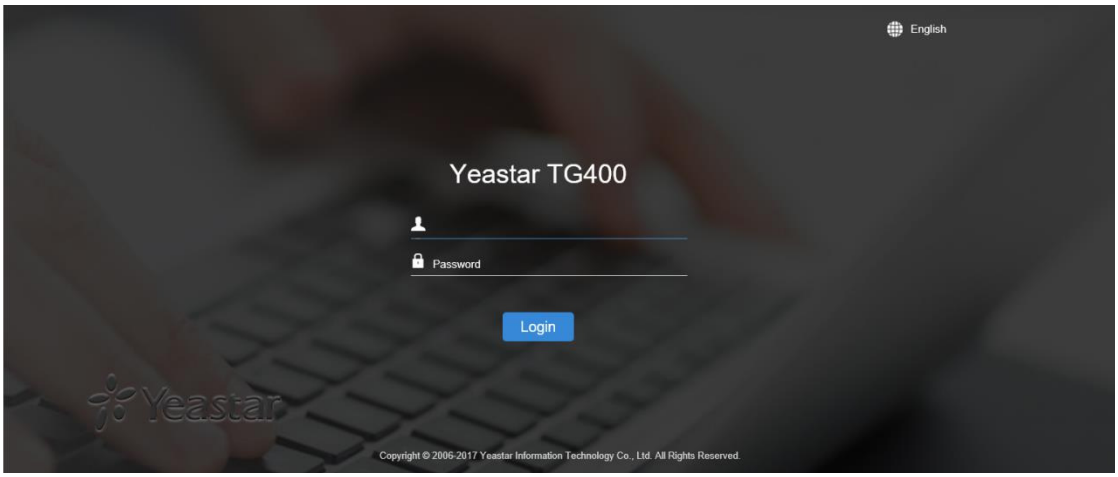
Yeastar TG gateway provides web-based configuration interface, you can manage the device by logging in the Web interface. Check the factory defaults below:

- IP address: http://192.168.5.150
- User Name: admin
- Default Password: password

Procedure

Make sure your computer is connected to the same network as the TG gateway.

1. Start a web browser on your PC, enter the IP address, press **Enter** on your keyboard.
2. Enter your user name and password, click **Login**.



Web Configuration Panel

There are 4 main sections on the Web Configuration Panel for users to check the TG gateway's status and configure it.

- **Status:** Check System Status, Port Status, Trunk Status, Network Status and check call logs, system logs.
- **System:** Configure Network Settings, Security related Settings, System Date and Time, Password, Backup and Restore, etc.
- **SMS:** Send SMS messages and manage the inbox and box, etc.
- **Gateway:** Configure mobile ports, VoIP settings, and Routes settings, etc.
- **Logout:** Log out TG gateway.

Note:
After saving the changes, remember to click the **Apply Changes** on the upper right corner of the Web GUI to make the changes take effect.

Manage GSM Modules

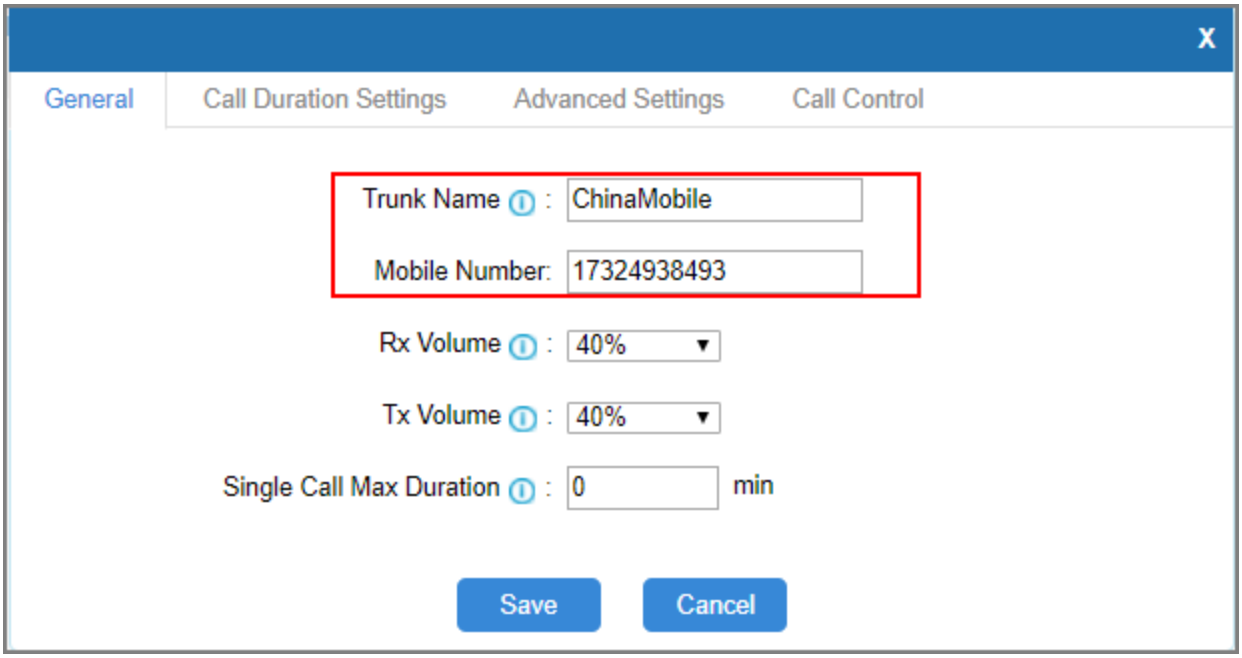
- Configure GSM Module Profile
- Reboot GSM Modules
- Enable/Disable GSM Module
- Adjust GSM Module Volume
- Configure the Call Duration of Mobile Trunks
- Configure Network Mode and Band
- Unlock the SIM Card
- Configure SIM Card Forwarding and CLIR
- Group Mobile Trunks

Configure GSM Module Profile

You can set a name to the GSM module to help you identify your modules on TG gateway. After inserting a SIM card to a GSM module, you can set the module's mobile number as the SIM card number to help you remember the SIM card number.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, select the desired Module, click .
2. In the **General** section, enter a name in **Trunk Name**.
3. Enter the SIM card number in **Mobile Number**.



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

Reboot GSM Modules

You can reboot a specific GSM module on the Web user interface. This action will not affect other GSM modules and can ensure the system is running properly.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, select the desired Module, click **Reboot**. The module starts to reboot.

Port	Trunk Name	Type	Max. Call Duration(min)	Used(min)	Available(min)	Outbound	Reboot Module	
1	ChinaMobile	Mobile	90	0	90	ON	Reboot	
2	Trunk2	Mobile	Unlimited	0	Unlimited	ON	Reboot	
3	Trunk3	Mobile	Unlimited	0	Unlimited	ON	Reboot	
4	Trunk4	Mobile	900	5	895	ON	Reboot	

2. Check the module status on **Status > System Status > Trunk Status**.

Enable/Disable GSM Modules

By default, GSM modules are enabled to make outbound calls. If you want to disallow a GSM module to make outbound calls, you can disable the module.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, select the desired module, click the **Outbound Status**. The outbound status is changed.

Port	Trunk Name	Type	Max. Call Duration(min)	Used(min)	Available(min)	Outbound	Reboot Module	
1	ChinaMobile	Mobile	90	0	90	ON	Reboot	

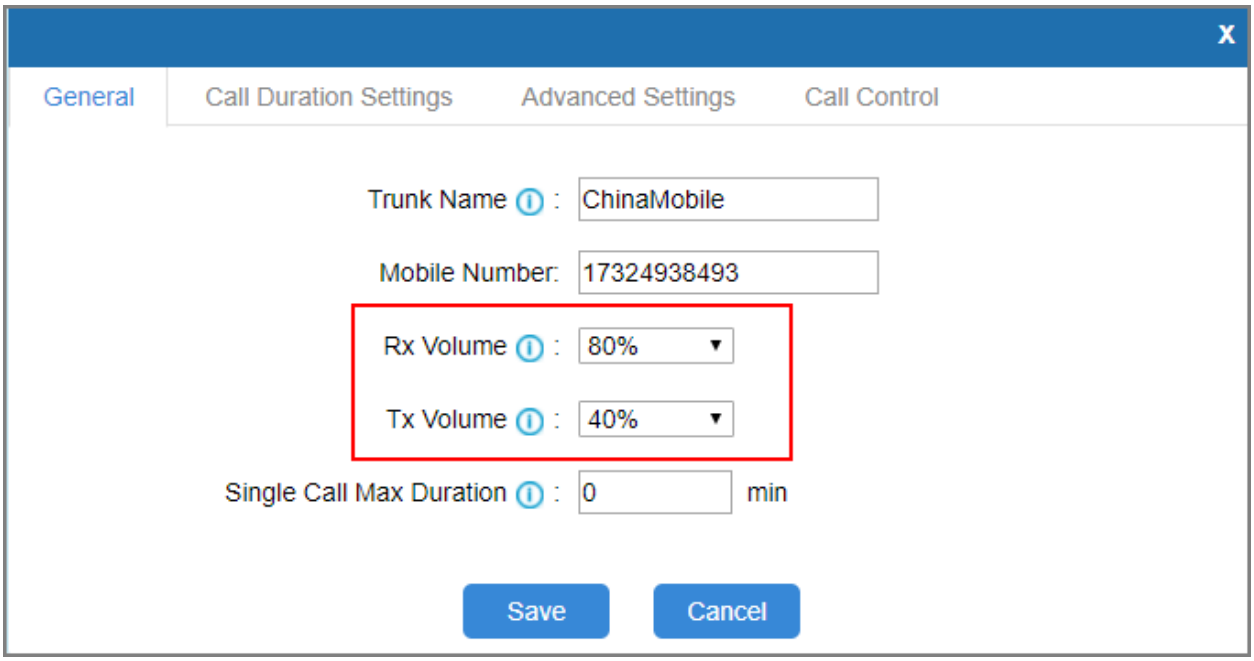
- ON You can make outbound calls through the GSM module.
- OFF You cannot make outbound calls through the GSM module.

Adjust GSM Module Volume

If you find that the call voice is too low or too loud, you can change the relevant GSM module volume.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, select the desired module, click .
2. On the **General** section, change the **Rx Volume** and **Tx Volume**.
   - Rx Volume: the received volume of the module.
   - Tx Volume: the transmitting volume of the module.



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

Configure the Call Duration of Mobile Trunks

You can limit call duration for each call of a mobile trunk or make a monthly talk plan for the mobile trunk.

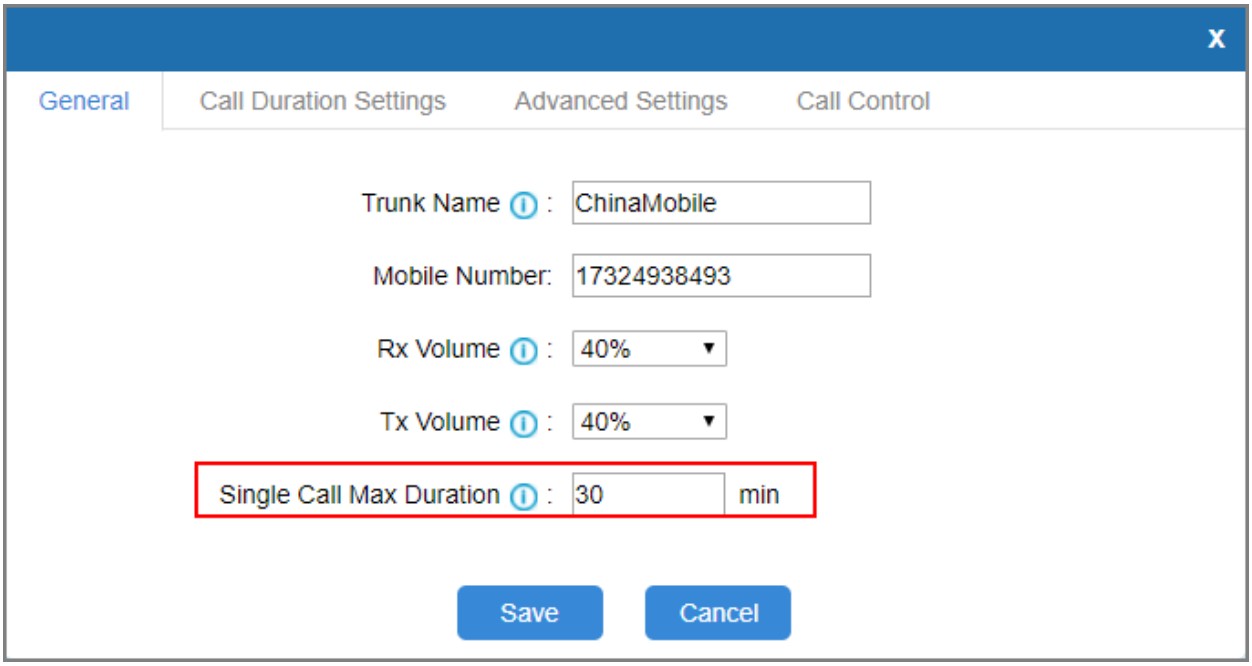
Note: the system starts to count the talk time when the SIM card is installed on the TG gateway. The system doesn't count the talk time that has been used formerly on the SIM card.

Set a Single Call Duration of Mobile Trunk

By default, the system doesn't limit single call duration of mobile trunks. The default value of **Single Call Max Duration** is 0. You can change the value to enable and define the maximum number of minutes called within a single call.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, select the desired module, click .
2. On the **General** section, change the value of **Single Call Max Duration**.



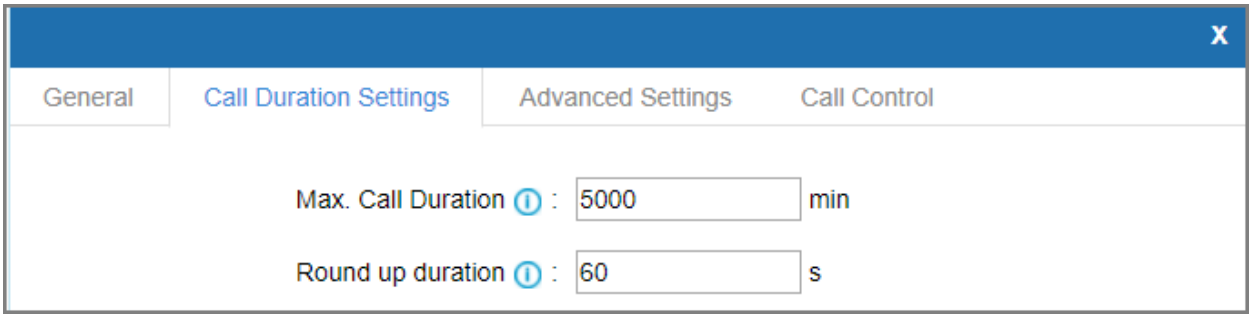
3. Click **Save** and **Apply Changes**.

Set a Monthly Talk Plan of Mobile Trunk

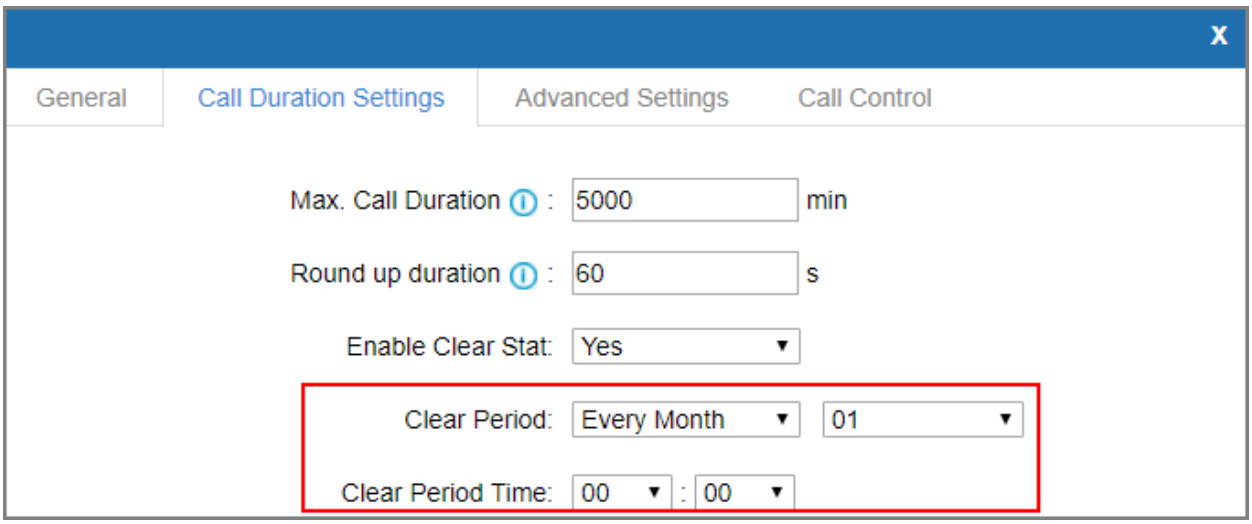
By default, the system doesn't limit monthly talk time of mobile trunks. You can set monthly talk plan for the mobile trunks to count and limit the talk time of outgoing calls on your TG gateway.

Procedure

1. Navigate to **Gateway** > **Mobile List** > **Mobile List**, select the desired module, click .
2. Click the **Call Duration Settings** tab.
3. Set the value of **Max. Call Duration**.
4. Set the value of **Round up duration**.
   For example, the Round up duration is 60 seconds and a call lasts 3 minutes and 15 seconds; the system will count the talk time as 4 minutes.



5. **(Optional)** Enable clear stat and set the clear period and time. The system will clear the call duration data on the TG gateway monthly.
   a. Set **Enable Clear Stat** to **Yes**.
   b. Set **Clear Period** to **Every Month**, and choose the clear day.
   c. Set the **Clear Period** Time.



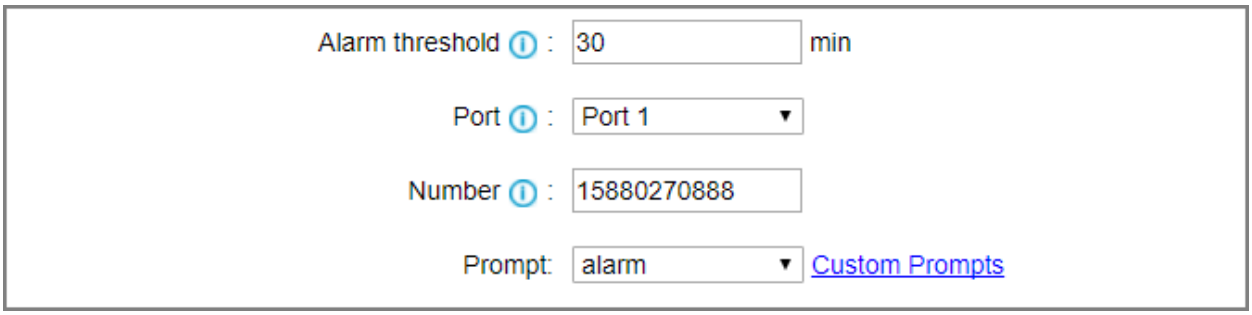
6. Click **Save** and **Apply Changes**.

Set Talk Time Alarm of Mobile Trunks

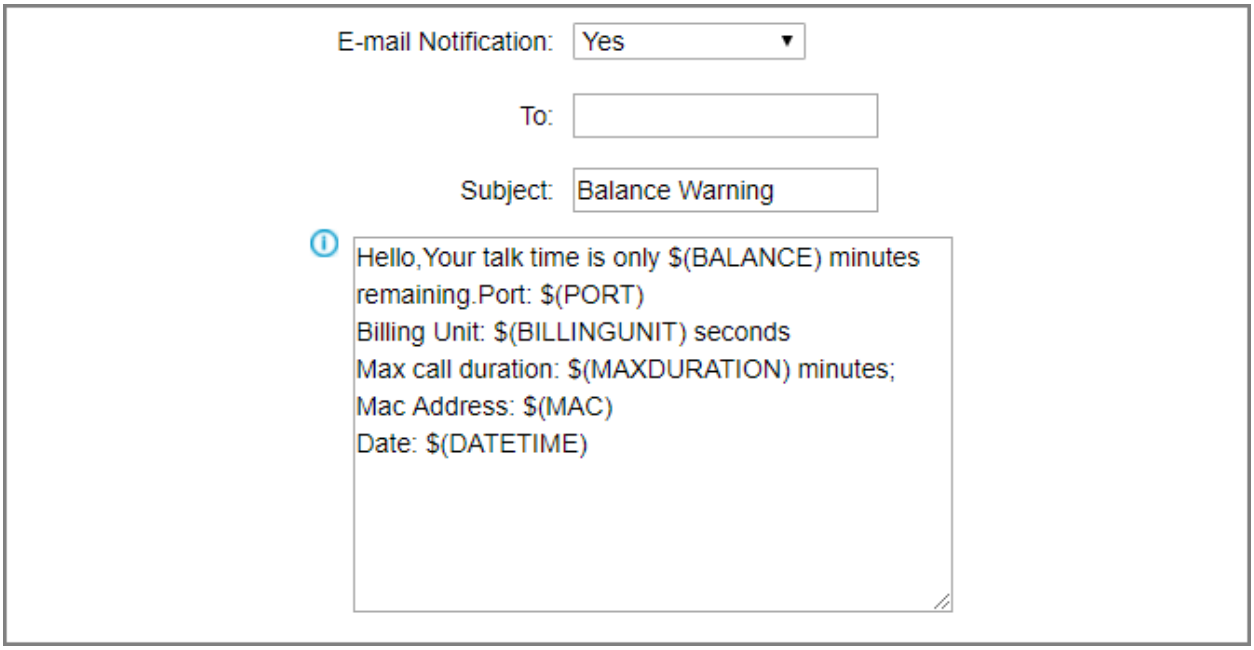
You can set alarm of talk time for mobile trunks to remind you that the monthly talk time of the mobile trunks is running out.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, select the desired module, click .
2. Click the **Call Duration Settings** tab.
3. Set the value of **Alarm threshold**.
4. Choose a GSM **Port** to make alarm calls.
   Note: Make sure the port is available to make calls.
5. Choose an alarm **Prompt**.



6. (**Optional**) Enable E-mail notification and enter the email address to receive alarm e-mail.



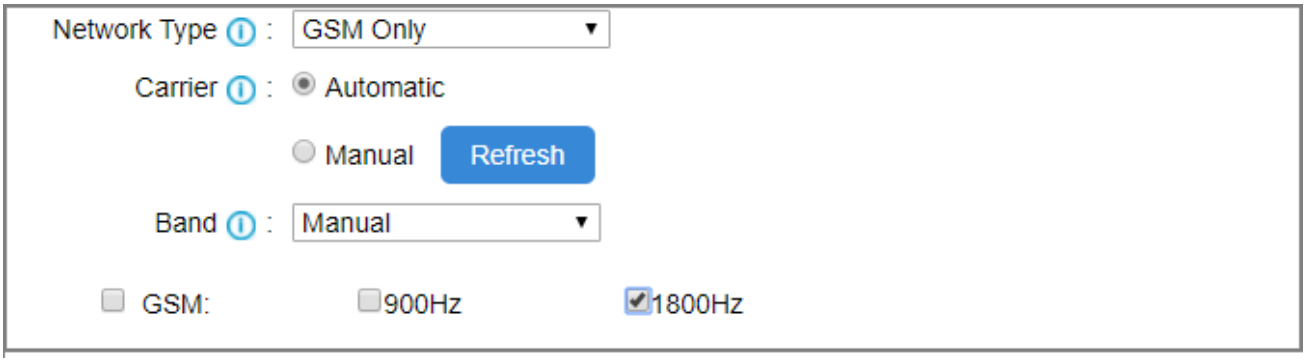
7. Click **Save** and **Apply Changes**.

Configure Network Type and Band

By default, TG gateway identifies the SIM card network type and band automatically. If the network type and band are not suitable for you, you can change the settings manually.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, select the desired module, click .
2. Click the **Advanced Settings** tab.
3. Choose a **Network Type**, the system will use the selected network type to make and receive calls.
4. Set **Band** to **Manual**, and select the desired band.



5. Click **Save** and wait for the web page reloading for about 1 minute, then click **Apply Changes**.

Unlock the SIM Card

If your SIM card has enabled PIN lock, you can unlock the SIM card on TG gateway.
Note: you cannot enable or disable the SIM PIN service on TG gateway.

Procedure

1. Navigate to **Gateway** > **Mobile List** > **Mobile List**, select the desired module, click .
2. Click the **Advanced Settings** tab.
3. Enter your SIM card PIN in the **PIN Code** field.

   Important: if you enter incorrect PIN for 3 times, you need to enter the PUK code to unlock the SIM card. Yeastar TG gateway doesn't support PUK code entering; you can unlock the SIM card with PUK code on your mobile phone.

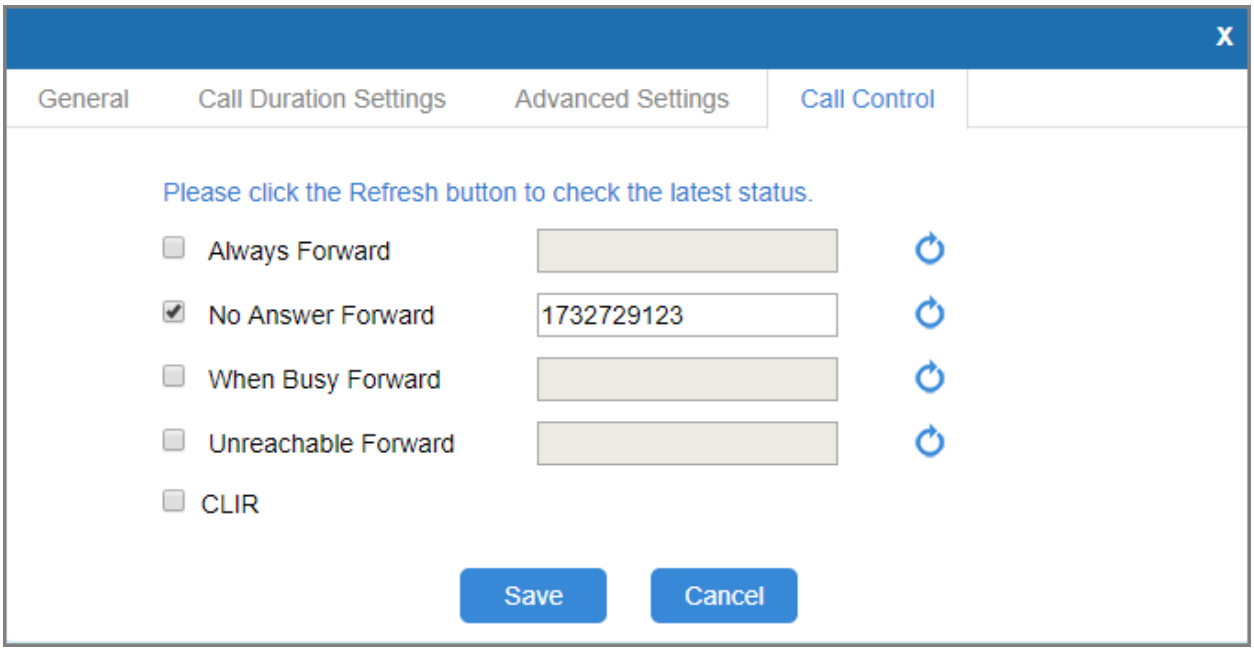
4. Click **Save** and **Apply Changes**.

Configure SIM Card Forwarding and CLIR

You can set call forwarding and CLIR for your SIM cards on Yeastar TG gateway. TG gateway can send service request to the SIM carrier to configure the call forwarding and CLIR settings.
Note: this feature should be supported by your SIM carrier.

Procedure

1. Navigate to **Gateway** > **Mobile List** > **Mobile List**, select the desired module, click .
2. Click the **Call Control** tab.
3. Enable the desired option and enter the number to receive forwarded calls.
4. If you forget the previous settings, click to retrieve the previous settings.



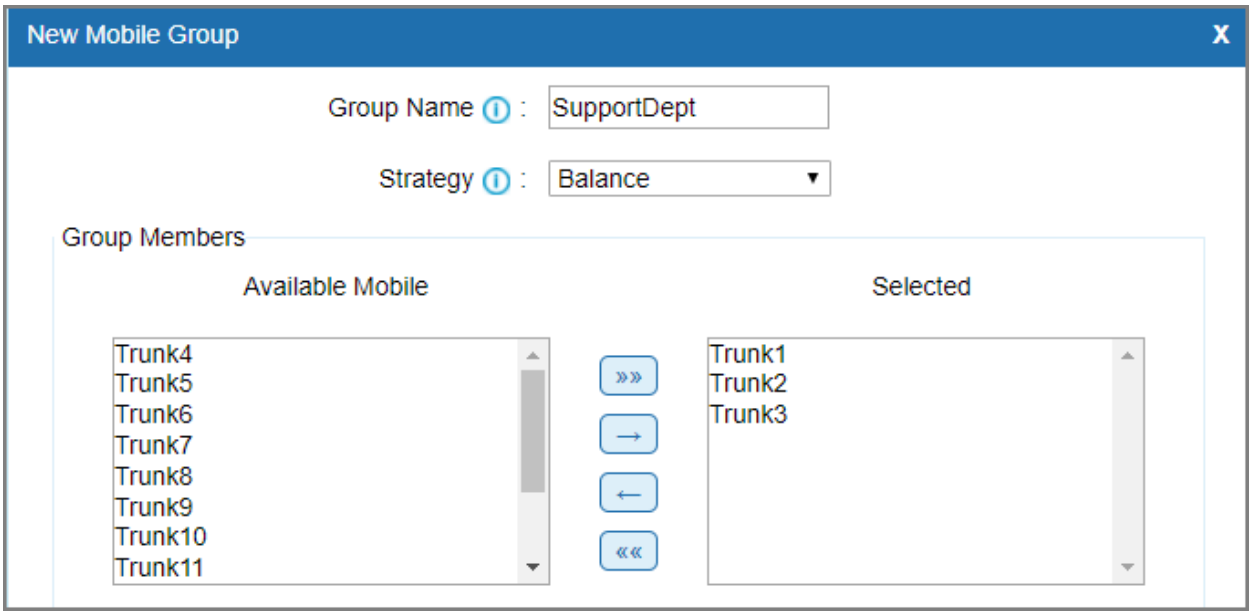
5. Click **Save** and **Apply Changes**.

Group Mobile Trunks

You can manage the mobile trunks efficiently by grouping the trunks. The group of mobile trunks can be selected directly when you are configuring the routes settings.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile Group**, click **Add New Mobile Group**.
2. Enter a name in the **Group Name** field.
3. Select an outgoing **Strategy** for the group of mobile trunks.
   If you apply the mobile group on one **IP to Mobile** route, the system will choose a mobile trunk to make outbound calls using the outgoing strategy.



4. Select desired trunks to the **Selected** box.
5. Click **Save** and **Apply**.

Connect TG Gateway to Your PBX (Account Mode)

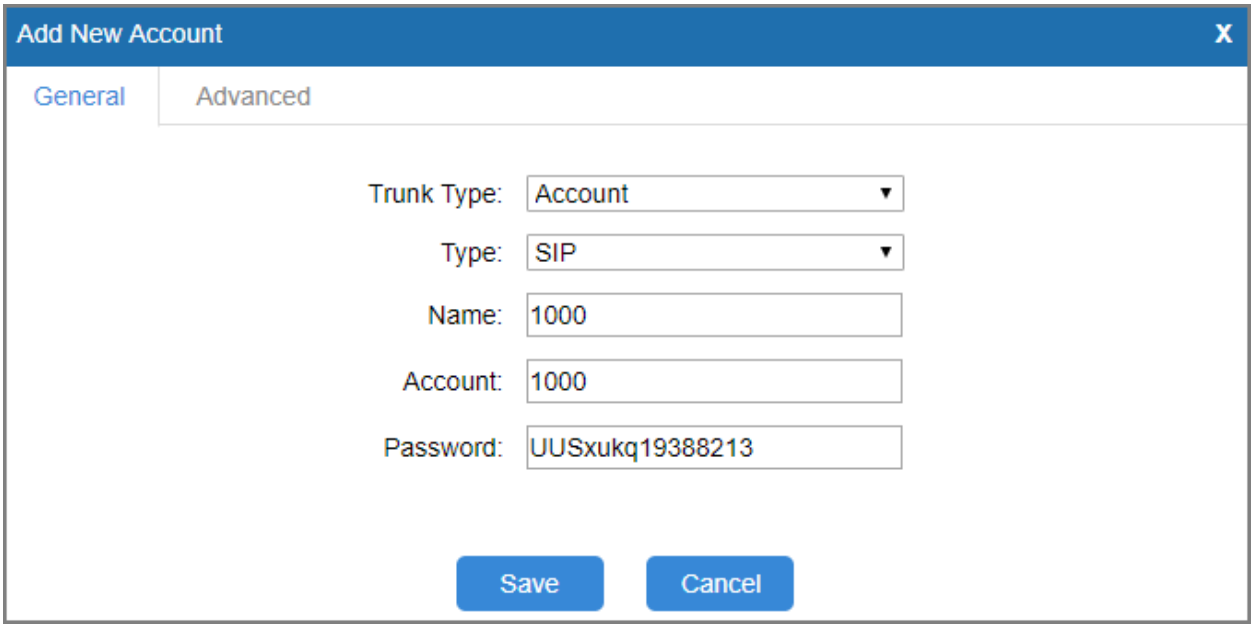
If you choose account mode, you need to create one VoIP account on TG gateway, and configure the following settings

- Connect TG Gateway to Your PBX (Account Mode)
- On your PBX, set up an outbound route for the VoIP trunk
- On your PBX, set up an inbound route for the VoIP trunk
- Set up a Mobile to IP Route (Account Mode)
- Set up an IP to Mobile Route (Account Mode)

Connect TG Gateway to Your PBX (Account Mode)

Procedure

1. Create a VoIP account on TG gateway.
   a. Navigate to **Gateway > VoIP Settings > VoIP Trunk**, click **Add VoIP Trunk**.
   b. Set **Trunk Type** to **Account**.
   c. Choose a protocol from the **Type** field.
   When you use this account to register VoIP trunk, you should choose the same protocol.
   d. Set the account's **Name**, **Account** and **Password**.
   You need use the same account number and password to register VoIP trunk on your PBX.
   e. (**Optional**) Click **Advanced** tab, configure the advanced settings.
   f. Click **Save** and **Apply Changes**.



2. Use the VoIP account to register a VoIP trunk on your PBX.

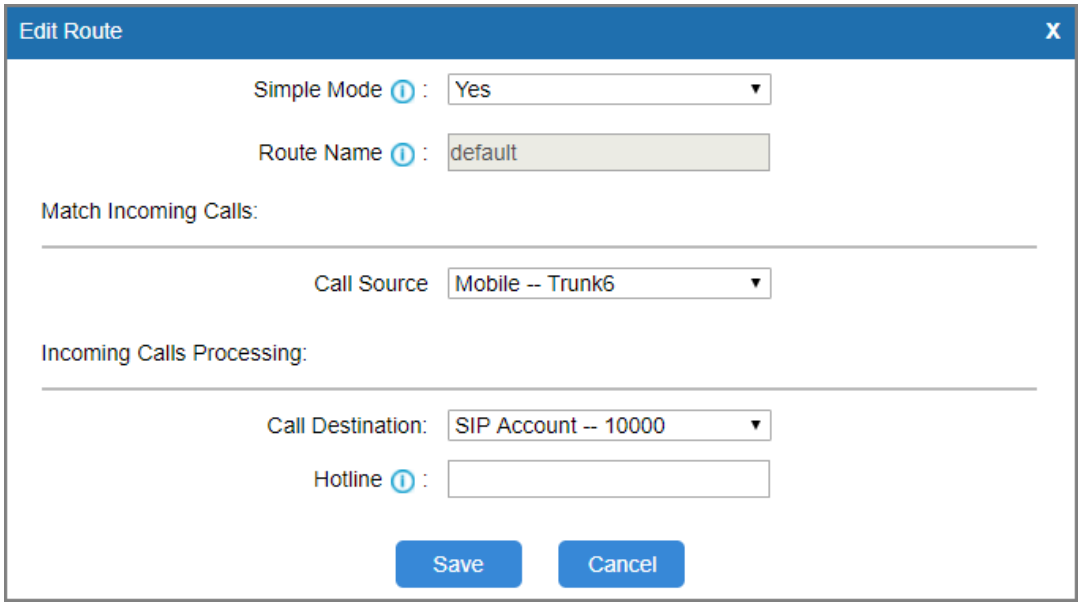
3. Check the account status on TG gateway **Status > System Status > Trunk Status**.

   If the account status shows ✔, then the TG gateway and your PBX are connected.

Set up a Mobile to IP Route (Account Mode)

Procedure

1. Navigate to **Gateway** > **Routes Settings** > **Mobile to IP**.
2. Click **Add Mobile to IP Route**.
3. Enter a name in the **Route Name** field.
4. Choose a GSM trunk or a trunk group from **Call Source** field.
5. Choose a SIP account from the **Call Destination** field.

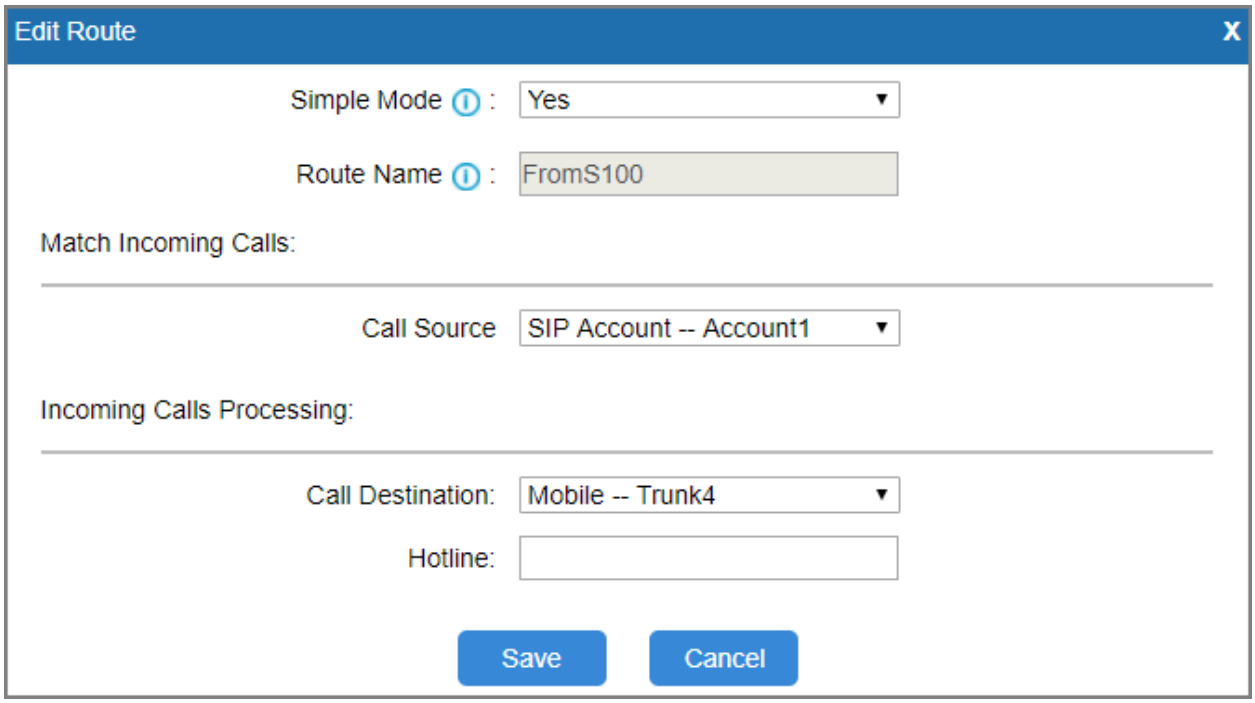


6. Click **Save** and **Apply Changes**
   When a call reaches the selected GSM trunk, the call will be routed to the destination of the PBX's inbound route.

Set up an IP to Mobile Route (Account Mode)

Procedure

1. Navigate to **Gateway** > **Routes Settings** > **IP to Mobile**.
2. Click **Add IP to Mobile Route**.
3. Enter a name in the **Route Name** field.
4. Choose a SIP account from **Call Source** field.
5. Choose a GSM trunk or a trunk group from the **Call Destination** field.



6. Click **Save** and **Apply Changes**
   A PBX user can make a call through the selected GSM trunk.

Connect TG Gateway to Your PBX (Register Trunk)

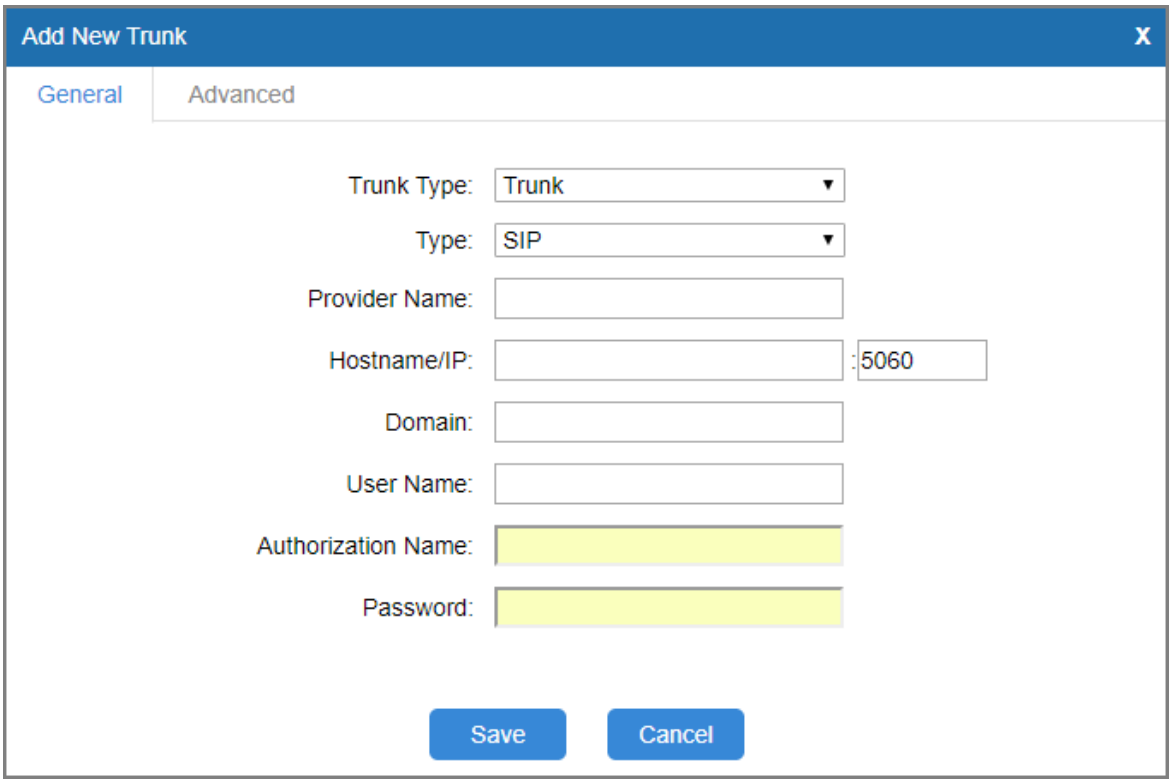
If you choose register trunk mode, you need to create one VoIP account on your PBX, and use the account to register a VoIP trunk on Yeastar TG gateway.

- Connect TG Gateway to Your PBX (Register Trunk Mode)
- Set up a Mobile to IP Route (Register Trunk Mode)
- Set up an IP to Mobile Route (Register Trunk Mode)

Connect TG Gateway to Your PBX (Register Trunk Mode)

Procedure

1. Create one VoIP extension on your PBX.
2. Create a register trunk on TG gateway.
   a. Log in TG web user interface, navigate to **Gateway > VoIP Settings > VoIP Trunk**, click **Add VoIP Trunk**.
   b. Set **Trunk Type** to **Trunk**.
   c. Choose a protocol from the **Type** field. The protocol should be the same with the PBX extension's protocol.
   d. Set a **Provider Name**.
   e. Enter the PBX's IP address or domain in **Domain** and **Hostname/IP** fields.
   f. Enter the PBX extension's number in **User Name** and **Authorization Name** fields.
   g. Enter the PBX extension's password in **Password** field.
   h. (**Optional**) Click **Advanced** tab, configure the advanced settings.
   i. Click **Save** and **Apply Changes**.



3. Check the trunk status on TG gateway **Status > System Status > Trunk Status**.

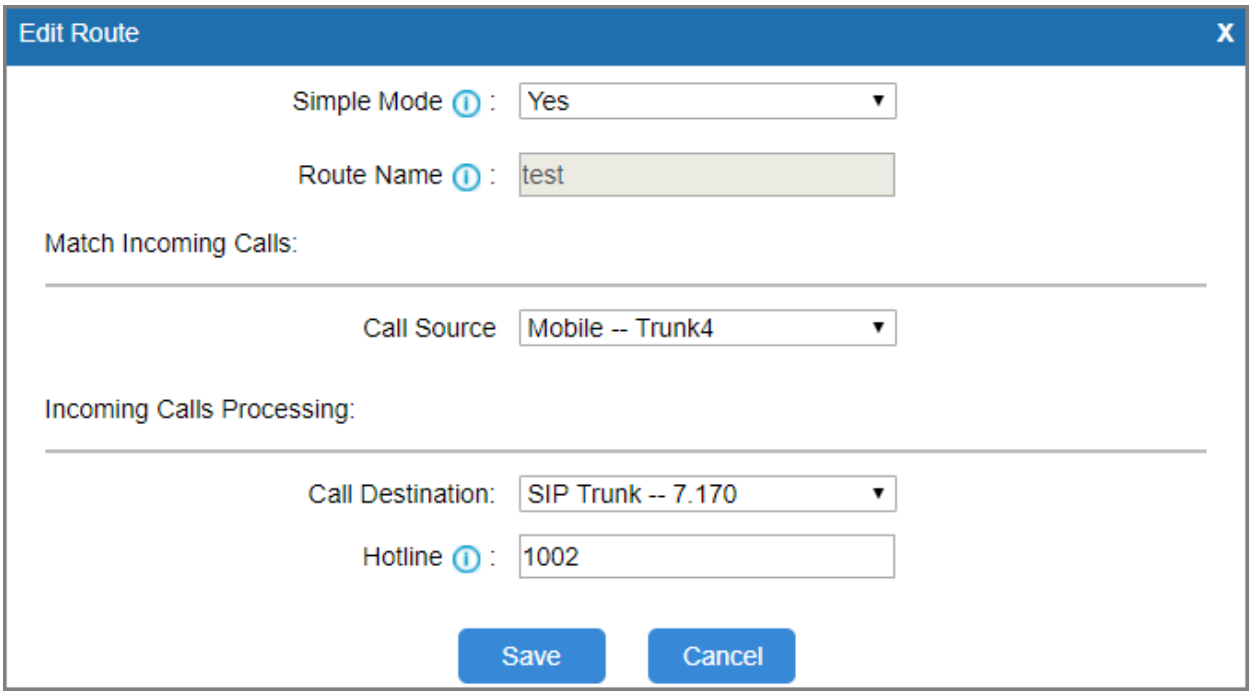
   If the trunk status shows ✓, then the TG gateway and your PBX are connected.

Set up a Mobile to IP Route (Register Trunk Mode)

Procedure

1. Navigate to **Gateway > Routes Settings > Mobile to IP**.
2. Click **Add Mobile to IP Route**.
3. Enter a name in the **Route Name** field.
4. Choose a GSM trunk or a trunk group from **Call Source** field.
5. Choose a register SIP trunk from the **Call Destination** field.
6. **(Optional)** Set the **Hotline** number.
   - If you set hotline to a PBX extension number, the incoming call will be routed to the extension directly.

   Note: if you don't set a hotline number, you will need a two-stage dial to reach the destination number.

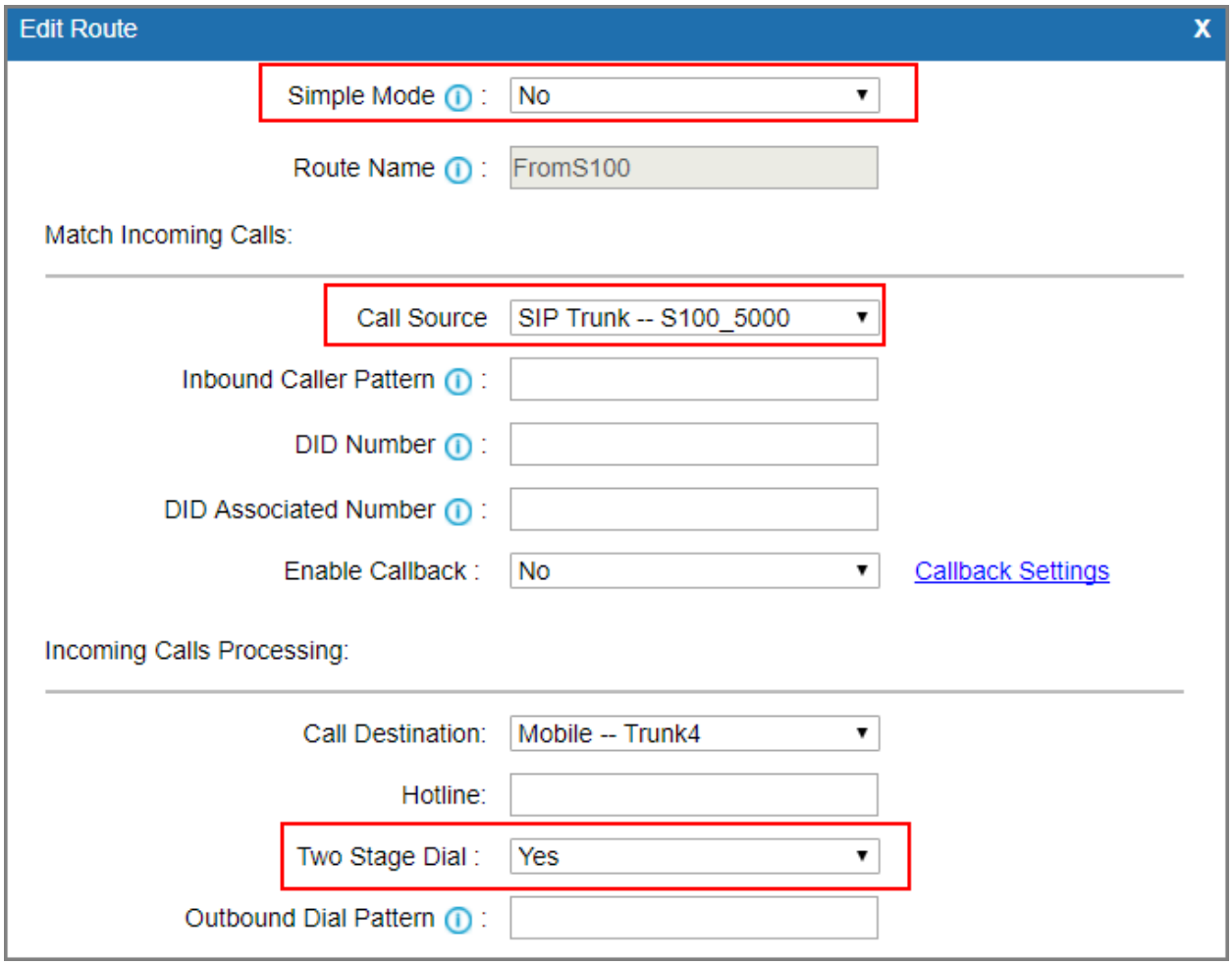


7. Click **Save** and **Apply Changes**
   When a call reaches the selected GSM trunk, the call will be routed to the desired destination.

Set up an IP to Mobile Route (Register Trunk Mode)

Procedure

1. Navigate to **Gateway > Routes Settings > IP to Mobile**.
2. Click **Add IP to Mobile Route**.
3. Enter a name in the **Route Name** field.
4. Choose a register SIP trunk from **Call Source** field.
5. Choose a GSM trunk or a trunk group from the **Call Destination** field.
6. Enable **Two Stage Dial**.
   a. Set **Simple Mode** to **No**.
   b. Set **Two Stage Dial** to **Yes**.



7. Click **Save** and **Apply Changes**

   When a PBX user makes a call through the selected GSM trunk, he/she will hear a dial tone. The PBX user needs to dial the destination number after hearing the dial tone.

Connect TG Gateway to Your PBX (Peer Trunk)

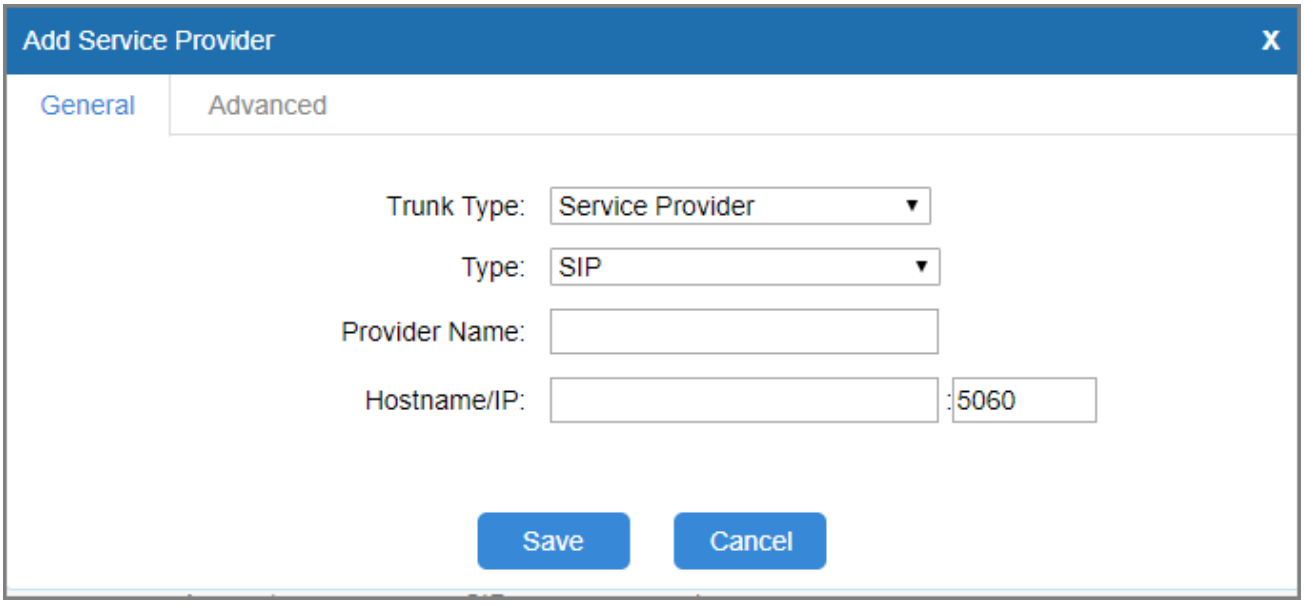
If you choose peer trunk mode, you need to create one peer trunk on TG gateway and configure the following settings:

- On your PBX, create a peer trunk which connects to TG gateway
- On your PBX, set up an outbound route for the peer trunk
- On your PBX, set up an inbound route for the peer trunk
- Connect TG Gateway to Your PBX (Peer Trunk Mode)
- Set up a Mobile to IP Route (Peer Trunk Mode)
- Set up an IP to Mobile Route (Peer Trunk Mode)

Connect TG Gateway to Your PBX (Peer Trunk Mode)

Procedure

1. Create one peer trunk on your PBX.
2. Create a peer trunk on TG gateway.
   a. Log in TG web user interface, navigate to **Gateway > VoIP Settings > VoIP Trunk**, click **Add VoIP Trunk**.
   b. Set **Trunk Type** to **Service Provider**.
   c. Choose a protocol from the **Type** field. The protocol should be the same with your PBX trunk's protocol.
   d. Set a **Provider Name**.
   e. Enter the PBX's IP address or domain in **Domain** and **Hostname/IP** fields.
   f. (Optional) Click **Advanced** tab, configure the advanced settings.
   g. Click **Save** and **Apply Changes**.



3. Check the status of the two peer trunks on both your PBX and the TG gateway.

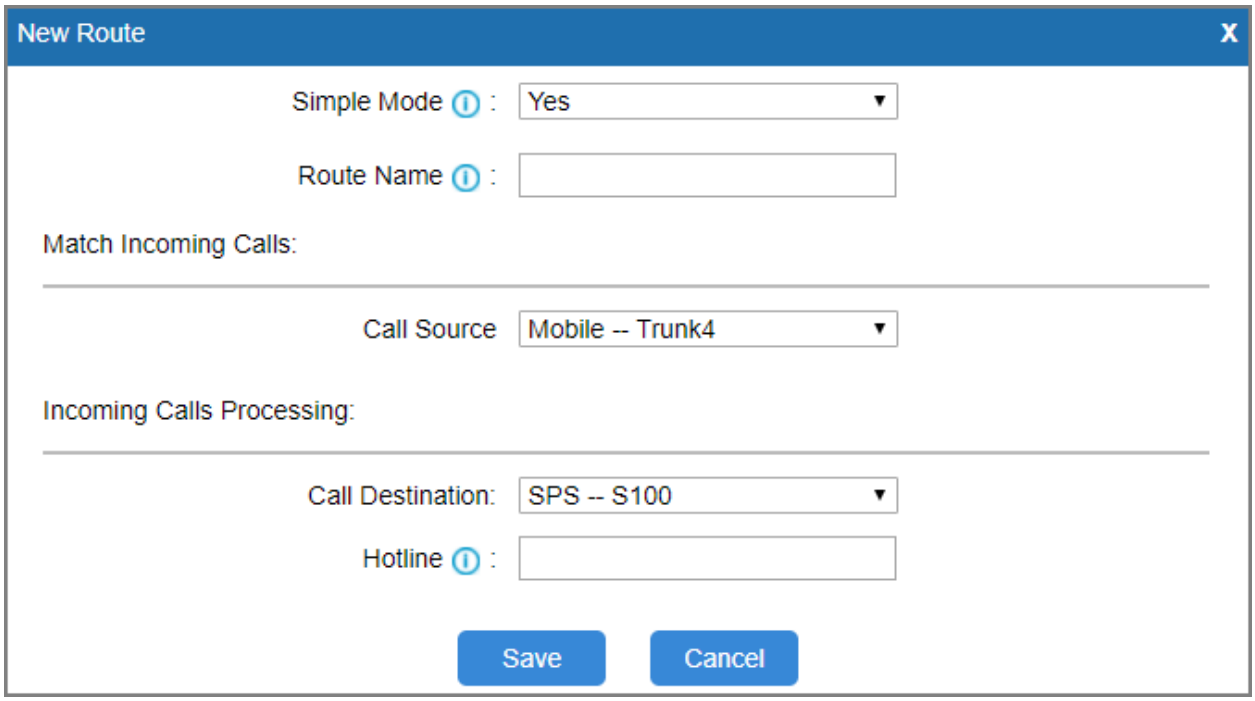
If the status of the two peer trunks both indicate connected, then the TG gateway and your PBX are connected.

Set up a Mobile to IP Route (Peer Trunk Mode)

Procedure

1. Navigate to **Gateway > Routes Settings > Mobile to IP**.
2. Click **Add Mobile to IP Route**.
3. Enter a name in the **Route Name** field.
4. Choose a GSM trunk or a trunk group from **Call Source** field.
5. Choose a service provider trunk from the **Call Destination** field.
6. **(Optional)** Set the **Hotline** number.
   - If you set hotline to a PBX extension number, the incoming call will be routed to the extension directly.
   - If you set the hotline to the DID number of PBX's inbound route, the call will be routed to the destination of the inbound route.

   Note: if you don't set a hotline number, you will need a two-stage dial to reach the destination number.

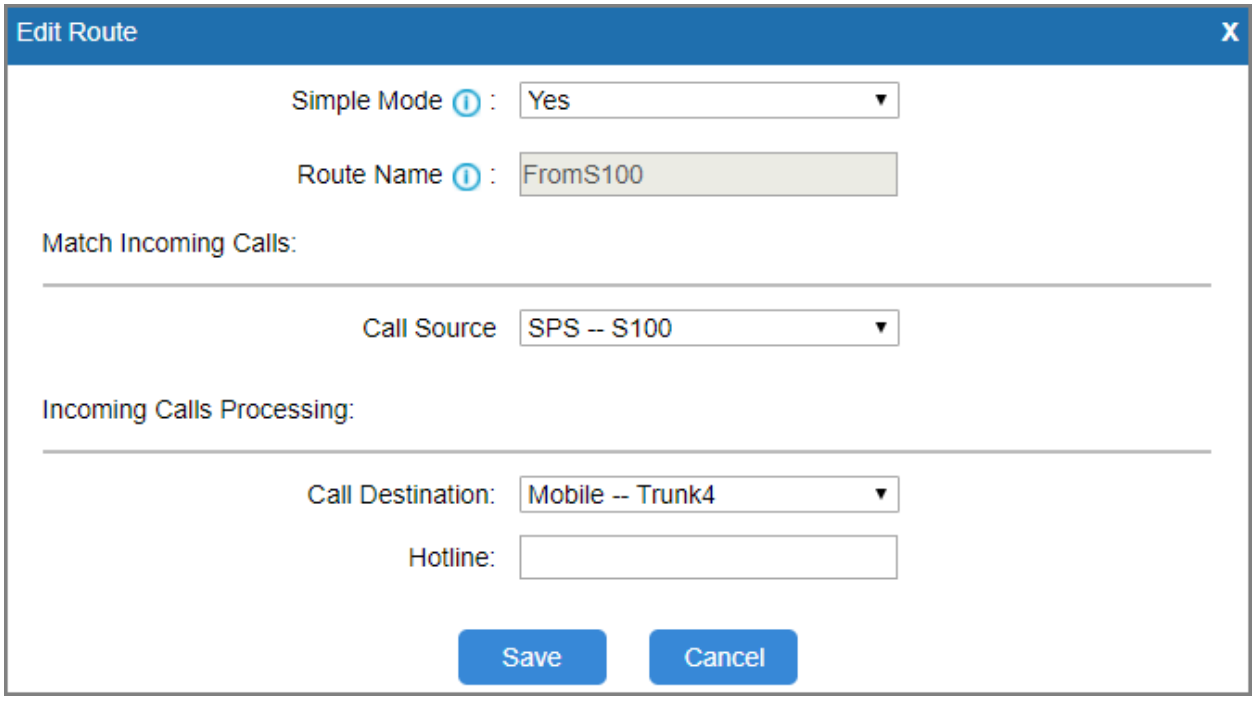


7. Click **Save** and **Apply Changes**.
   When a call reaches the selected GSM trunk, the call will be routed to the desired destination.

Set up an IP to Mobile Route (Peer Trunk Mode)

Procedure

1. Navigate to **Gateway > Routes Settings > IP to Mobile**.
2. Click **Add IP to Mobile Route**.
3. Enter a name in the **Route Name** field.
4. Choose a service provider trunk from **Call Source** field.
5. Choose a GSM trunk or a trunk group from the **Call Destination** field.



6. **Click** Save **and** Apply Changes
   A PBX user can make a call through the selected GSM trunk.

Call Control

- Route Calls Based on Caller ID
- Route Calls on Destination Numbers
- Block Incoming Numbers
- Block Outgoing Numbers
- Callback
- AutoCLIP Route

Route Calls Based on Caller ID

You can set the TG gateway to route calls based on the caller ID number of the person that is calling. If the incoming caller ID doesn't match the route settings, the call will fail.

Procedure

1. Navigate to **Gateway** > **Routes Settings** > **Mobile to IP**.
2. Choose a route, click .
3. Set **Simple Mode** to **No**.
4. Enter a rule on the **Inbound Caller Pattern**.
   Note: leave this field blank to match any or no Caller ID information.
5. Click **Save** and **Apply Changes**.

Route Calls Based on Destination Numbers

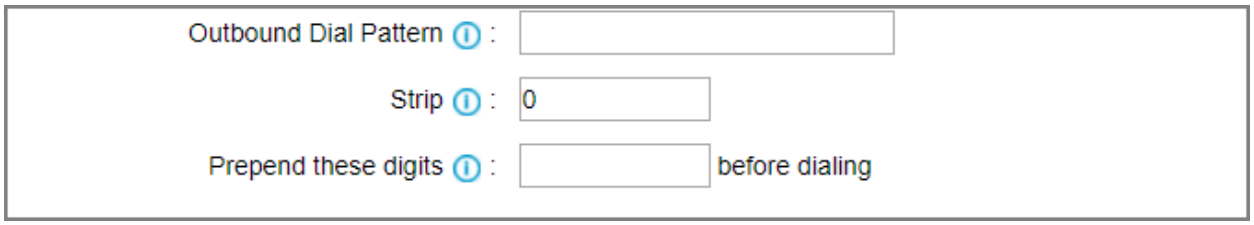
You can set the TG gateway to route calls based on the destination numbers. When the users call in TG gateway and hear a dial tone, they need to do a second dial to reach the desired destination. The TG gateway routes the calls only when the users dial the destination numbers according to the route rule.

Note: this feature would work only when the users get a second stage dial tone.

Procedure

1. Navigate to **Gateway** > **Routes Settings** > **Mobile to IP**.
2. Choose a route, click .
3. Set **Simple Mode** to **No**.
4. Enter a rule on the **Outbound Dial Pattern**.
   Note: leave this field blank to match all dialed numbers.
5. **(Optional)** Set how many digits to strip in **Strip** field.
   The TG gateway will strip the digits from the front of the phone number, and send the rewritten number.

6. **(Optional)** Set which digits to prepend on the dialed numbers in **Prepend these digits** field. The gateway will prepend the digits to the phone number, and send the rewritten number.



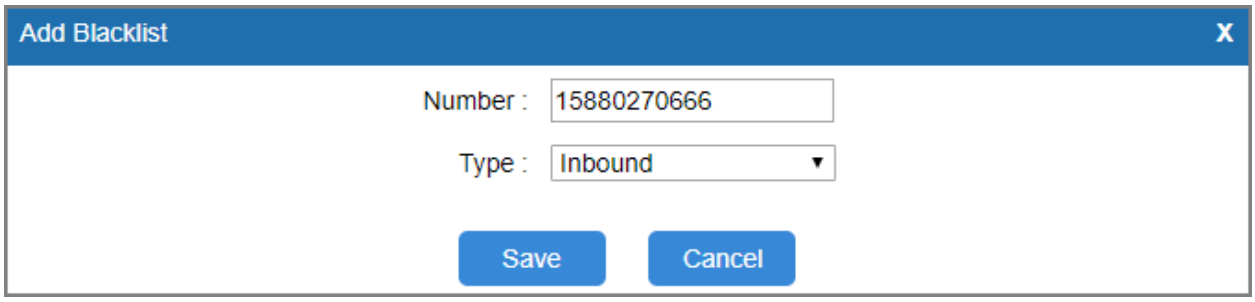
7. Click **Save** and **Apply Changes**.

Block Incoming Numbers

You can block the incoming numbers to call from TG gateway to your PBX. When the blocked user calls to the GSM trunk on TG gateway, the system will block the call.

Procedure

1. Navigate to **Gateway** > **Routes Settings** > **Blacklist**.
2. Click **Add Blacklist**.
3. Enter the desired number.
4. Set the **Type** to **Inbound**.



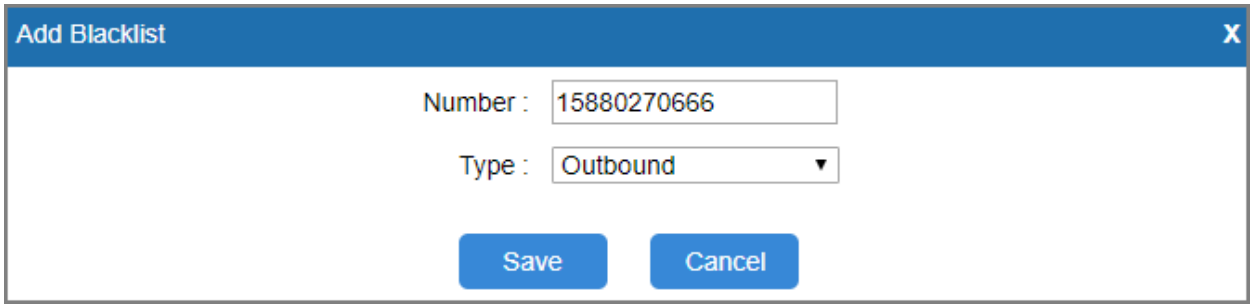
5. Click **Save** and **Apply Changes**.
   When the number 15880270666 reaches the TG gateway, the call will fail.

Block Outgoing Numbers

You can limit users to call specific numbers through GSM trunks on TG gateway. When the users try to call the blocked numbers, the call will fail.

Procedure

1. Navigate to **Gateway** > **Routes Settings** > **Blacklist**.
2. Click **Add Blacklist**.
3. Enter the desired number.
4. Set the **Type** to **Outbound**.



5. Click **Save** and **Apply Changes**.
   When the PBX user tries to call the number 15880270666 through TG gateway, the call will fail.

Callback

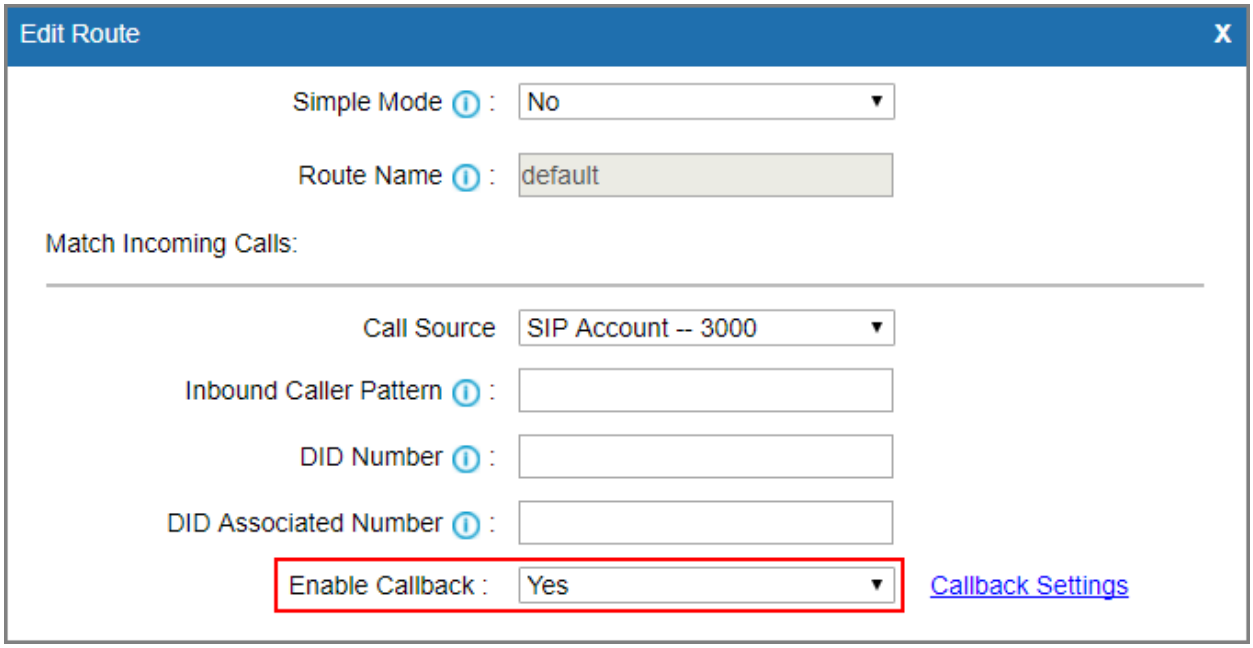
Callback feature allows callers to hang up and get called back to TG gateway. Callback feature could reduce the cost for the users who work out of the office using their own mobile phones.

Set up Callback for Specific Numbers

Callback feature is disabled on the TG gateway by default. The system only calls back the permitted numbers.

Procedure

1. Navigate to **Gateway** > **Routes Settings** > **Callback Settings**.
2. Click **Add Callback Number**.
3. Enter the desired number.
4. Click **Save** and **Apply Changes**.
5. Enable Callback on Mobile to IP route or IP to Mobile route.



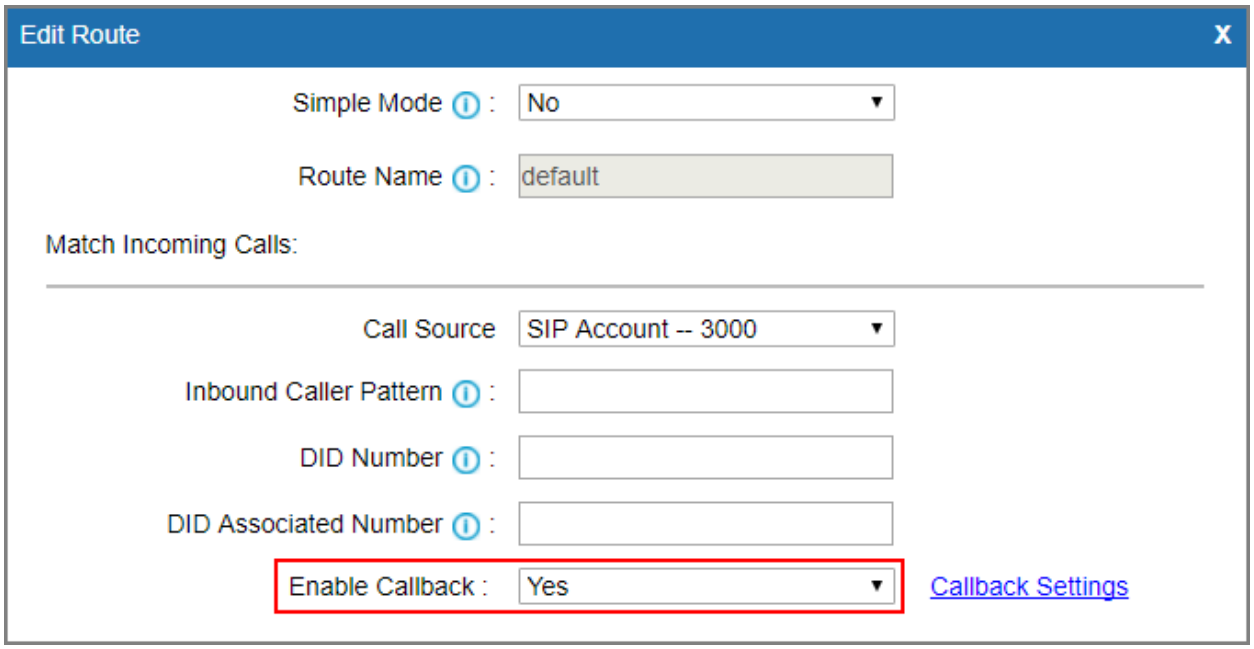
6. Click **Save** and **Apply Changes**.

Set up Callback for All Numbers

You can enable callback feature for all numbers. When any one calls in TG gateway and disconnects the call, the system will call back the user.

Procedure

1. Navigate to **Gateway** > **Routes Settings** > **Callback Settings**.
2. Check the checkbox of **Allow All Numbers**.
3. Click **Save** and **Apply Changes**.
4. Enable Callback on Mobile to IP route or IP to Mobile route.



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

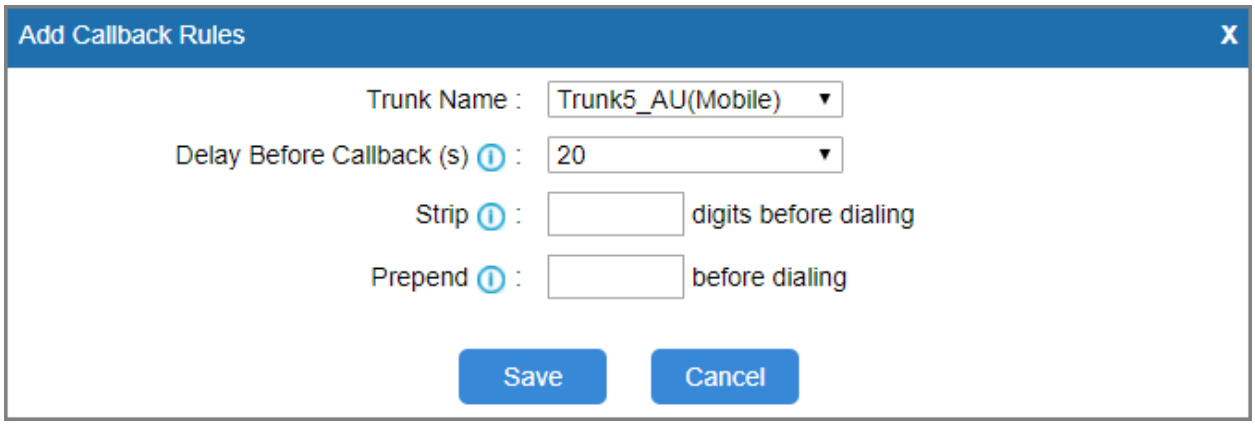
Add Callback Rules

A callback rule will help you to manipulate the numbers call back from TG gateway. For some GSM carriers, you need to add digits or strip digits for the incoming caller ID to ensure that TG gateway can call back to the desired numbers.

Procedure

1. Navigate to **Gateway** > **Routes Settings** > **Callback Settings**.
2. Click **Add Callback Rules**.
3. Choose which trunk will be used to call back.
4. Set the callback rule.
   - **Strip:** define how many digits will be stripped from the call in number before the callback is placed.

- **Prepend:** define digits added before a callback number before the callback is placed.



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

AutoCLIP Route

Yeastar TG gateway can automatically stores records of failed outgoing call to AutoCLIP route table. When the called person calls back, TG gateway will route the call directly to the original caller's extension.

Set up AutoCLIP Route

Procedure

1. Navigate to **Gateway** > **Routes Settings** > **AutoCLIP Settings**.
2. Set **Enable** to **Yes**.
3. **(Optional)** Change the **Record Keep Time**. The system will keep the AutoCLIP records for the configured time.
4. **(Optional)** Change the value of **Digit Match**. Adjust the setting if the incoming caller ID has a prefix "+","0" or others.
5. Click **Save** and **Apply Changes**.

Delete AutoCLIP Records

If you don't want to route the incoming call to the original user, you can delete the AutoCLIP record. The next time, when the called person calls back TG gateway, the call will not be routed to the original user.

Procedure

1. Navigate to **Gateway** > **Routes Settings** > **AutoCLIP Settings**.
2. Select the desired AutoCLIP record, click .

Manage Messages

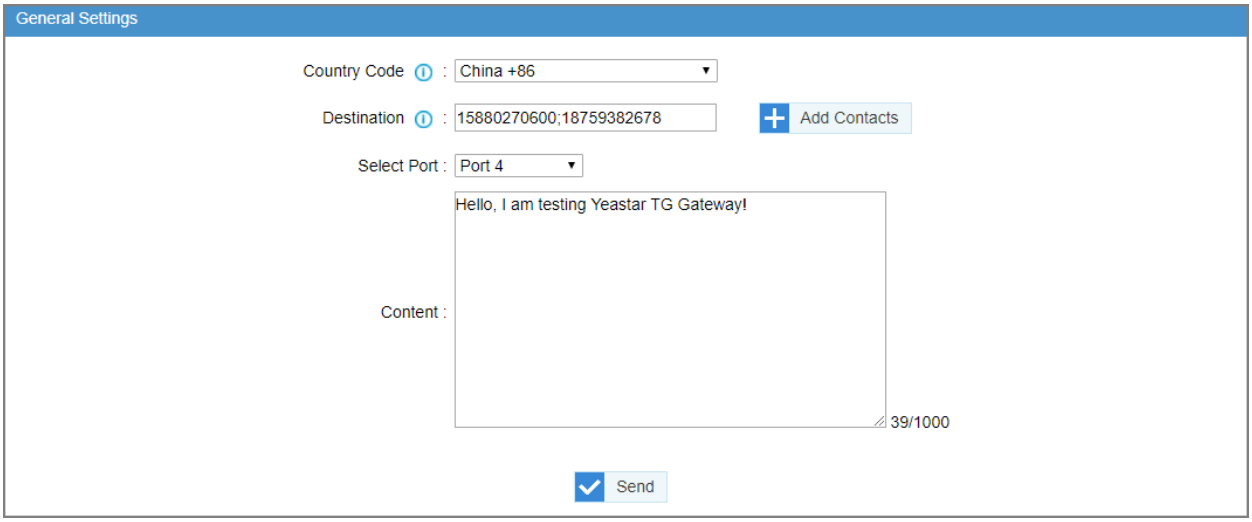
- Send SMS Messages
- Manage SMS Contacts
- Manage Sent SMS Messages
- Manage Received SMS Messages
- SMS to Email
- Email to SMS
- Schedule SMS Clear Tasks
- Send USSD Messages
- Enable TG Gateway API
- Change Password of SMS Center

Send SMS Messages

You can send SMS messages through the installed SIM cards on Yeastar TG gateway Web user interface.

Procedure

1. Navigate to **SMS > SMS > Send SMS**.
2. Choose a **Country Code** for the destination number.
   If you cannot find the desired country code, set **Country Code** to **Custom**, and enter the country code.
3. Enter the destination number in **Destination** field. Separate two phone numbers by a ";".
   You can also click **Add Contacts** to add phone numbers to the **Destination** filed.
4. Choose a GSM port, the system will send the SMS messages through the selected port.
5. Enter the message contents in the **Content** field.
6. Click **Send**.



Manage SMS Contacts

Add an SMS Contact

A contact list allows you to target and text contacts with common interests. Once you have all your contacts created on TG gateway, you can send SMS messages to a single contact or a group or all contacts by directly selecting rather than typing in the numbers manually each time.

Procedure

1. Navigate to **SMS > SMS > SMS Contacts**, click **Add Contact**.
2. Enter the contact name and phone number.
3. **(Optional)** Select a **Group** to add the contact to the group.
4. Click **Save**.

Delete an SMS Contact

Procedure

1. Navigate to **SMS > SMS > SMS Contacts**.
2. Choose a contact and click .

Manage Sent SMS Messages

You can view the status of sent SMS messages, search, download, or delete the sent SMS messages on the TG gateway.

Check the Status of Sent SMS Messages

Procedure

1. Navigate to **SMS > SMS > Outbox**.
2. Search or find your desired SMS message, then check the status.
   - Successful: the SMS message is sent successfully.
   - Failed: the SMS message is not sent successfully.
   - Sending: the system is sending the SMS message.

Search Sent SMS Messages

You can search SMS messages by the following criteria.

- **Date Duration:** choose the Start Date and End Date to filter the call logs.

- **Port:** the system uses which GSM port to send SMS messages.
- **Status:** choose the sent status of the SMS messages.
- **Destination:** enter a destination number.

Procedure

1. Navigate to **SMS > SMS > Outbox**.
2. Set the searching criteria.
3. Click **Start Searching**, the filtered SMS messages appears on the page.

Download Searched Results

After searching the desired SMS messages, you can download and export the records to a .csv file.

Procedure

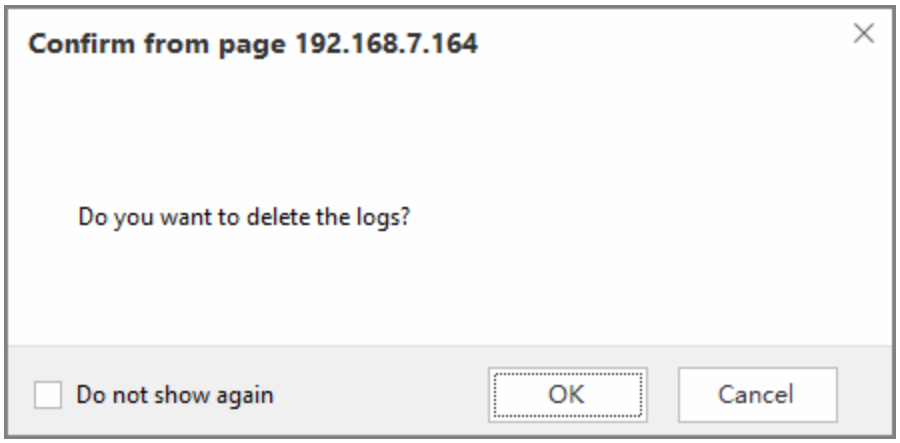
1. Navigate to **SMS > SMS > Outbox**.
2. Click **Download the messages** to download and export the searched SMS messages.

Delete Searched Results

You can search the desired SMS messages, and delete them.

Procedure

1. Navigate to **SMS > SMS > Outbox**.
2. Click **Delete All messages** to delete the searched SMS messages. A popup window appears.



3. Click **Yes** to delete the searched records.

Manage Received SMS Messages

View Received SMS Messages

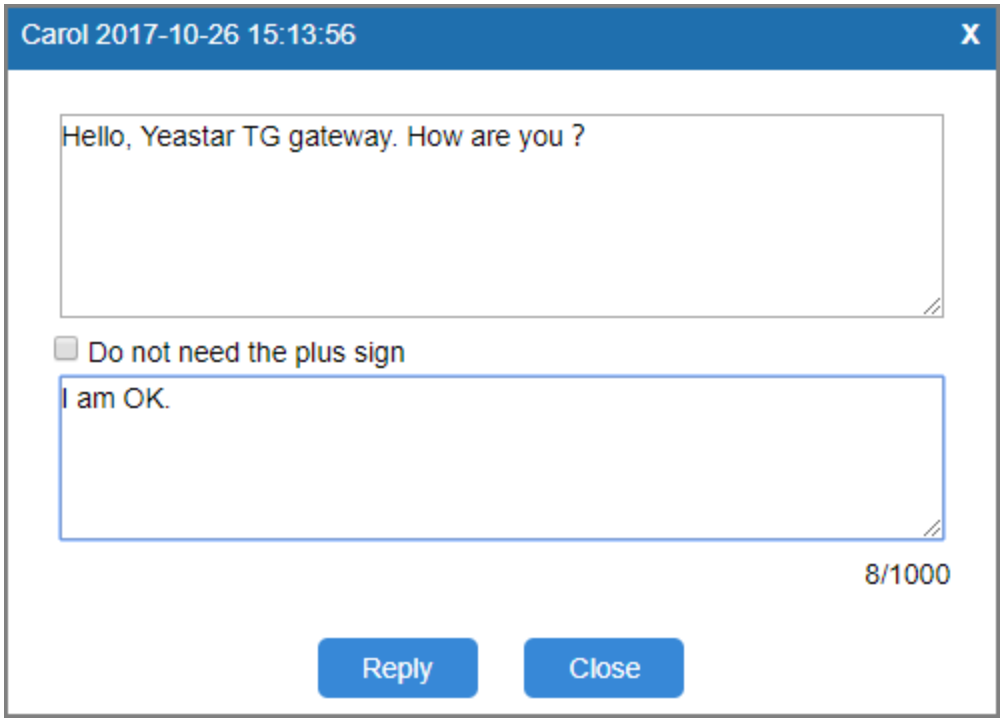
Procedure

1. Navigate to **SMS > SMS > Inbox**.
2. Choose the desired record, click to view the detailed messages.

Reply SMS Messages

Procedure

1. Navigate to **SMS > SMS > Inbox**.
2. Choose the desired record, click .
3. Enter the contents in the box.
4. **(Optional)** Check the checkbox of **Do not need the plus sign** if the destination number doesn't need it.
5. Click **Reply**.



Search Received SMS Messages

You can search SMS messages by the following criteria.

- **Date Duration:** choose the Start Date and End Date to filter the call logs.
- **Port:** the users send SMS messages to which GSM port.
- **Has Read:** choose the read status of the SMS messages.
- **From:** the SMS messages are sent from which number.

Procedure

1. Navigate to **SMS > SMS > Inbox**.
2. Set the searching criteria.
3. Click **Start Searching**, the filtered SMS messages appears on the page.

Download Searched Results

After searching the desired SMS messages, you can download and export the records to a .csv file.

Procedure

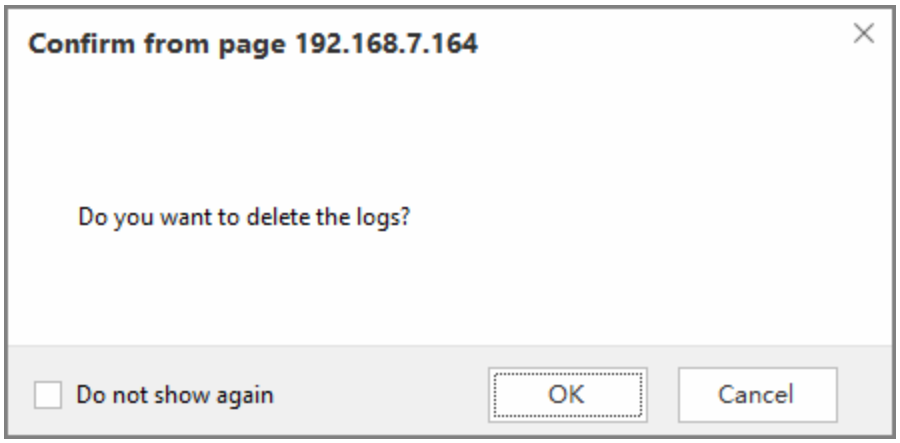
1. Navigate to **SMS > SMS > Inbox**.
2. Click **Download the messages** to download and export the searched SMS messages.

Delete Searched Results

You can search the desired SMS messages, and delete them.

Procedure

1. Navigate to **SMS > SMS > Inbox**.
2. Click **Delete All messages** to delete the searched SMS messages. A popup window appears.



3. Click **Yes** to delete the searched records.

SMS to Email

To send SMS to Email, you need to configure Email POP3 settings and SMS to Email settings.

Configure Email POP3 Settings

Procedure

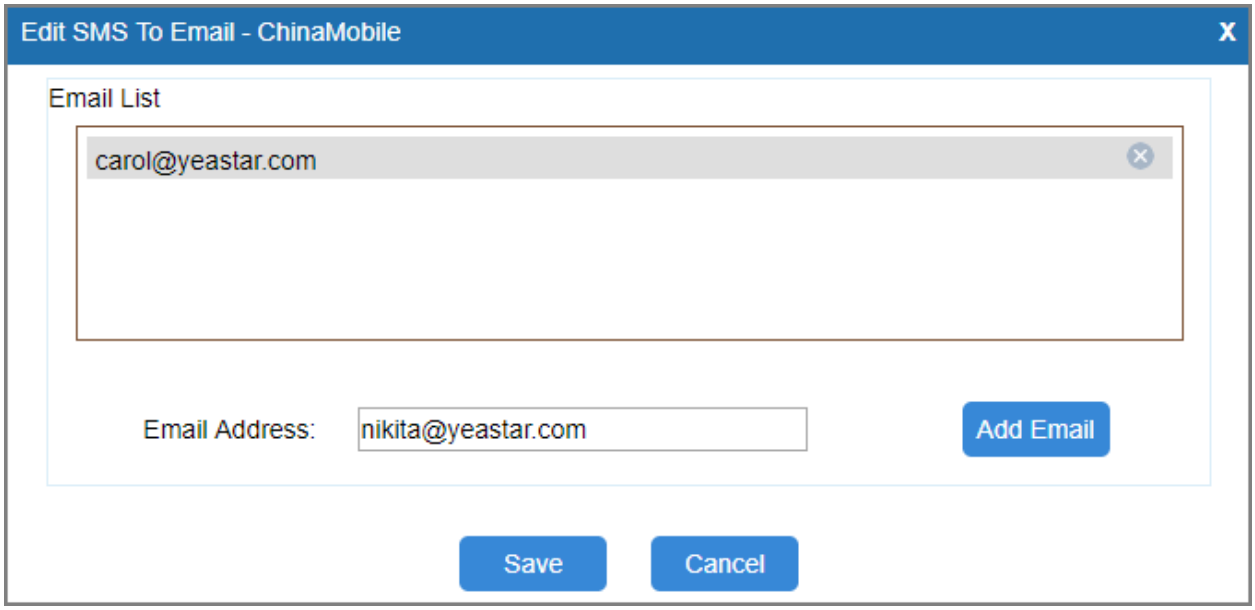
1. Navigate to **SMS > SMS Settings > Email Settings**.

2. Check the checkbox of **Enable SMS To Email**.
3. Enter the email password in the **Password** field.
4. Enter the **POP3 Server** and SMTP **Port** of the email.
5. Click **Test POP3 Settings** to test if the email settings are correct.
   If the web page prompts "Tested successfully", the email settings are correct.
6. Click **Save** and **Apply Changes**.

Configure SMS to Email Settings

Procedure

1. Navigate to **SMS > SMS Settings > Email Settings**.
2. Choose one GSM trunk, click to edit it.
3. Enter an email address, click **Add Email**.
   The system will deliver the SMS messages to the added email addresses.



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

Send SMS to Email

Procedure

1. Create an SMS message on your mobile phone, send the message to the number of SIM card which is installed on TG gateway.

   When the TG gateway receives the message, the gateway will deliver the SMS message to the pre-configured email addresses.

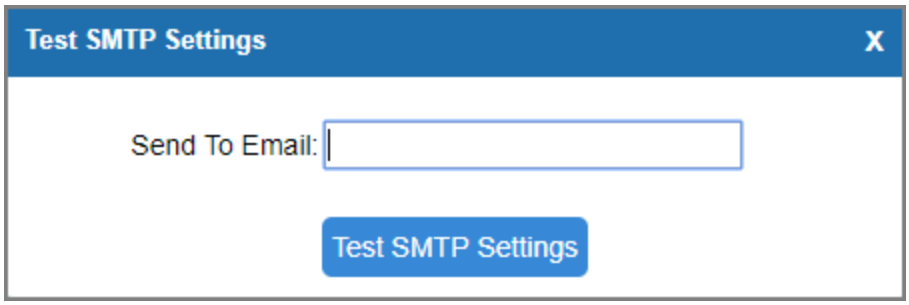
Email to SMS

To send Email to SMS, you need to configure Email SMTP settings and Email to SMS settings.

Configure Email SMTP Settings

Procedure

1. Navigate to **SMS > SMS Settings > Email Settings**.
2. Enter a valid email address in the **Email Address** field.
3. Enter the email password in the **Password** field.
4. Enter the **SMTP Server** and SMTP **Port** of the email.
5. **(Optional)** Enable SSL/TLS if the email server needs SSL/TLS authentication.
   Note: If you use Gmail or Exchange server, enable the SSL/TLS.
6. Test if the email settings are correct.
   a. Click **Test SMTP Settings**.
      The following window appears.



   b. Enter an email address to receive the test email.
   c. Click **Test SMT Settings**.
      The web page will prompt "Tested successfully" if the email settings are correct.
7. Click **Save** and **Apply Changes**.

Configure Email to SMS Settings

Procedure

1. Navigate to **SMS > SMS Settings**.
2. Check the checkbox of **Email To SMS**.
3. **(Optional)** configure the settings in the section of **Email to SMS**.
   - **Enable Country** Code: enable the option if you want to add the country code before the destination phone number.
   - **Receive Email Interval**: set the interval of receiving emails from POP3 server.
   - **Access Code**: set a PIN code to verify emails. The users need to send emails with the correct PIN code.
4. Click **Save** and **Apply Changes**.

Send Email to SMS

To send email to SMS, you need to send an email to the SMS email address of TG gateway. The system will receive the email and forward the email to the GSM port, so that the email can be sent out through SMS to the expected destinations.

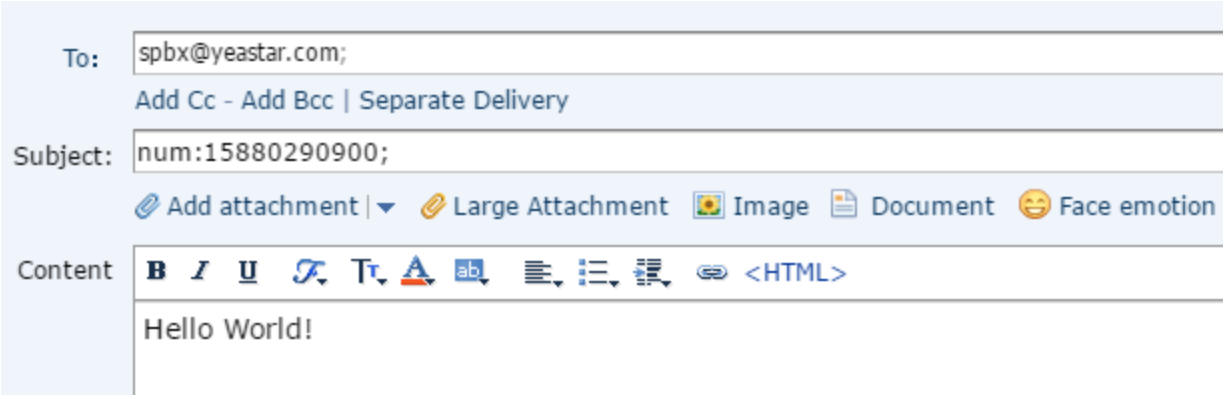
Sending Email to SMS, the format of the email subject is as below:
port:[port];num:[number];code:[code];

Format of the Email Subject

- **port:[port]**: optional setting. If don't specify a port, the TG gateway will send the SMS by the first available GSM port.
  Example: port:3;
- **num:[number]**: required setting. Enter the destination number.
  Example: num:15882025100;
- **code:[code]**: optional Setting. If you set an access code of Email To SMS, enter the same PIN code in the email subject.
  Example: code:125485;

Procedure

1. Log in your email account, compose a new email.
2. Enter the SMS email address of TG gateway as the destination email address.
3. Enter the email subject.
4. Send the email.
   Example: the following figure indicates that the SMS email address is spbx@yeastar.com, and the destination number is 15880290900.

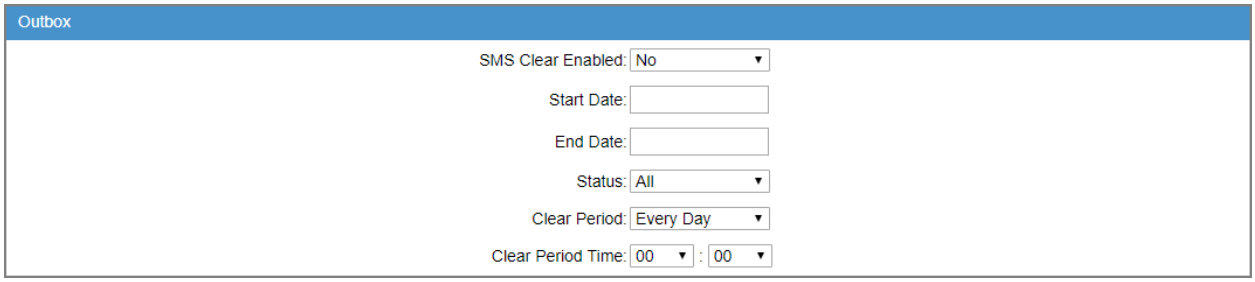


Schedule SMS Clear Tasks

You can schedule clear task for messages in inbox and outbox. The system will clear all the messages in the inbox or outbox periodically.

Procedure

1. Navigate to **SMS > SMS > SMS Clear Settings**.
2. Set clear schedule for inbox or outbox.
   a. Check the checkbox of **SMS Clear Enabled**.
   b. (Optional) Set the Start Date and End Date. The system will clear the messages periodically during this period.
   c. Select the message **Status**. The system will delete the selected messages.
   d. Set the clear period and clear time.



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

Send USSD Messages

Unstructured Supplementary Service Data (USSD) is sometimes referred to as "Quick Codes" or "Feature codes". You can send USSD messages to subscribe services from the GSM carriers.

Send a USSD Message

You can choose a specific GSM port, and send USSD messages to the GSM carrier.

Procedure

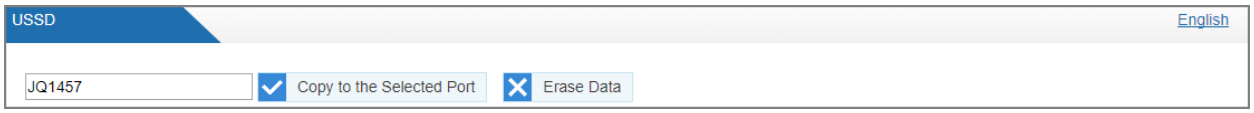
1. Navigate to **SMS > SMS > USSD**.
2. Choose a port, enter the USSD messages in the **USSD Request** field.
3. Click **Send**.

Send USSD Messages in Bulk

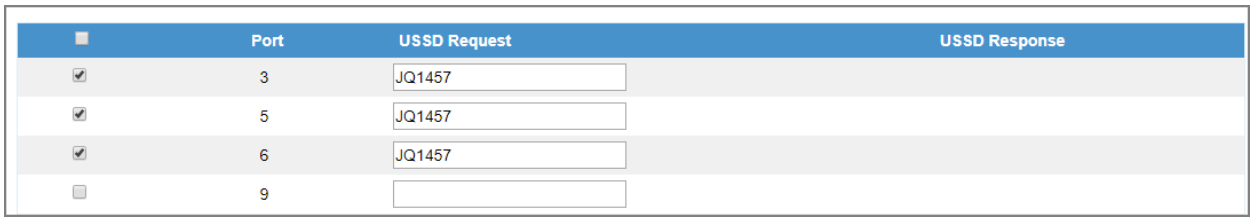
You can send a USSD message for multiple GSM ports in bulk.

Procedure

1. Navigate to **SMS > SMS > USSD**.
2. Selected the desired ports.
3. Enter the USSD message in blank field at the top left.



4. Click **Copy to the Selected Port**.
   The message will apply to the selected ports.



5. Click **Send.**

Exit USSD Sessions

When you want to subscribe a new service from the GSM carrier, you need to exit the former USSD sessions first.

Procedure

1. Navigate to **SMS > SMS > USSD**.
2. Selected the desired ports.
3. Click **Exit USSD Session**.

Enable TG Gateway API

Yeastar TG gateway supports sending and receiving SMS messages with third party software. You need to connect the third party software with TG gateway via API.

Procedure

2. Navigate to **SMS > SMS > API Settings**.
3. Check the checkbox of **Enable API**.
4. Set the **User Name**. The 3rd party software will use the user name to connect to TG gateway.
5. Set the **Password**. The 3rd party software will use the password to connect to TG gateway.
6. **(Optional)** Set the permitted IP addresses. Only the permitted IP addresses can connect to TG gateway via API.
7. Click **Save** and **Apply Changes**.

Change Password of SMS Center

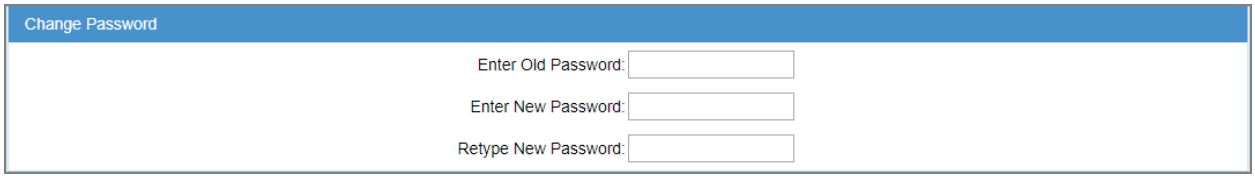
You can provide a Web login account for other users to manage all the SMS related settings. Check the default username and password:

- User Name: sms

- Default password: password

Procedure

1. Navigate to **SMS > SMS > SMS Password**.
2. Enter the old password first.
3. Enter a new password and retype the new password to confirm.
   A strong password is comprised of letters, numbers and characters.
4. Click **Save**, you will be automatically logged out.



Configure System Settings

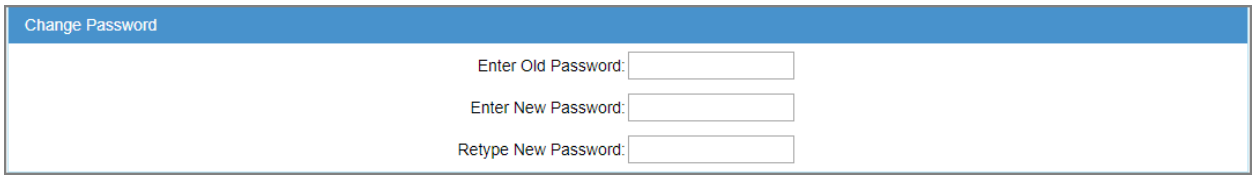
- Change Web Login Password
- Change Date and Time
- Upload Custom Prompts
- Set up System Email
- Update System Firmware
- Backup and Restore
- Reboot the System
- Schedule Automatic Reboots
- Reset the System

Change Web Login Password

It is highly recommended that you change the system's password after first login.

Procedure

1. Navigate to **System** > **System Preferences** > **Password Settings**.
2. Enter the old password first.
3. Enter a new password and retype the new password to confirm.
   A strong password is comprised of letters, numbers and characters.
4. Click **Save**, you will be automatically logged out.

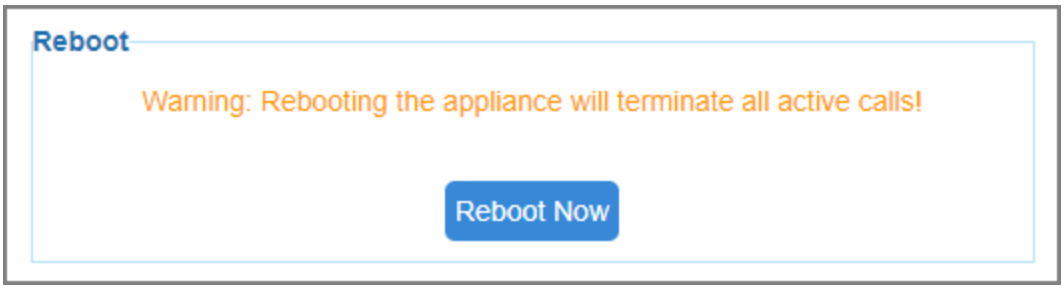


Change Date and Time

You can adjust the time of TG gateway (including the time zone) to make it consistent with your local time.

Procedure

1. Navigate to **System** > **System Preferences** > **Date and Time**.
2. Select your current and correct **Time Zone**.
3. (Optional) Enable the **Daylight Saving Time** if you need it in your place.
4. Check Synchronize with NTP Server, the system will adjust its internal clock to a central network server. If you choose this method, make sure that the system can access the Internet.
5. You can also choose Set up Manually and enter the time with numbers.
6. Click **Save**, a reboot prompt will display on the bottom of the web page.



7. Click **Reboot Now** to reboot the TG gateway.

Upload Custom Prompts

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 and apply it to the place you want to change.

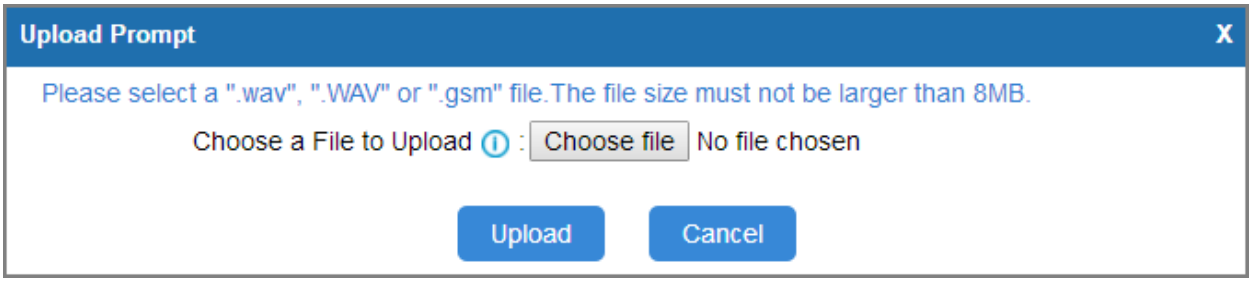
Prerequisite

Yeastar TG gateway supports .WAV, .wav, and .gsm audio file. The audio file size must be smaller than 8 MB. The supported wav file format:

- PCM 8K 16bit ,mono bit rate 128kbps
- law(g.711) 8k 8bit 64kbps
- u-law(g.711) 8k 8bit 64kbps
- gsm 6.10 8k 13kbps

Procedure

1. Navigate to **System** > **System Preferences** > **Custom Prompts**, click **Upload a Prompt**.
   The following window appears.



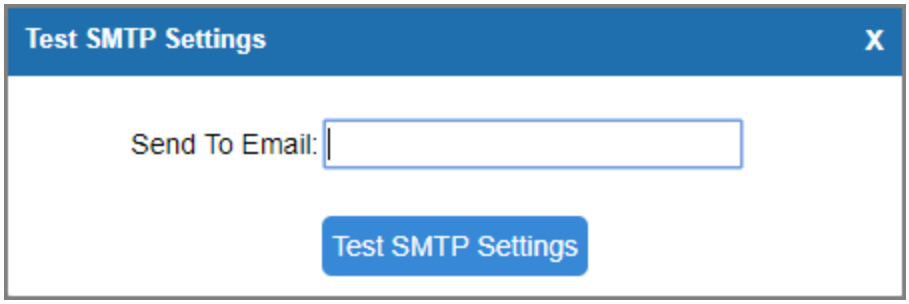
2. Click **Choose File** to choose a file from your local PC.
3. Click **Upload** to start upload the file.
   After uploaded, the file name will be displayed on the **Custom Prompts** page.

Set up System Email

To receive email notifications, you need to set up the system email. The system email is used to send alert event emails.

Procedure

1. Navigate to **System > System Preferences > Email Settings**.
2. Enter a valid email address in the **Email Address** field.
3. Enter the email password in the **Password** field.
4. Enter the **SMTP Server** and SMTP **Port** of the email.
5. (Optional) Enable SSL/TLS if the email server needs SSL/TLS authentication.
   Note: If you use Gmail or Exchange server, you need enable SSL/TLS.
6. Test if the email settings are correct.
   a. Click **Test SMTP Settings**.
      The following window appears.



   b. Enter an email address to receive the test email.
   c. Click Test SMT Settings.
      The web page will prompt "Tested successfully" if the email settings are correct.

Update System Firmware

Update Firmware through HTTP Server

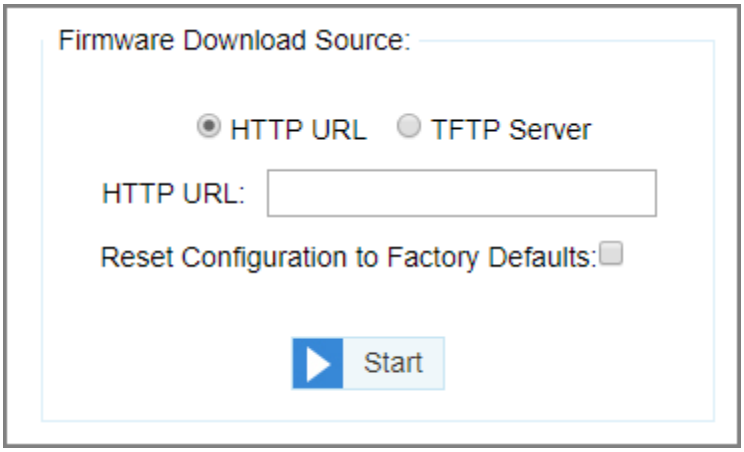
You can get the firmware file download link from Yeastar website and update the firmware through HTTP server.

Important: during the firmware update, don't power off the device, or the system will be damaged.

Procedure

1. Navigate to **System > System Preferences > Firmware Update**.
2. Check the checkbox of **HTTP URL**.
3. Enter the http URL of the desired firmware file.
   Note: the HTTP URL should be a **BIN** file download link.
4. (**Optional**) Check the checkbox of Reset Configuration to Factory Defaults.
   Important: if you choose to reset the system, you will lose all the current system configurations.

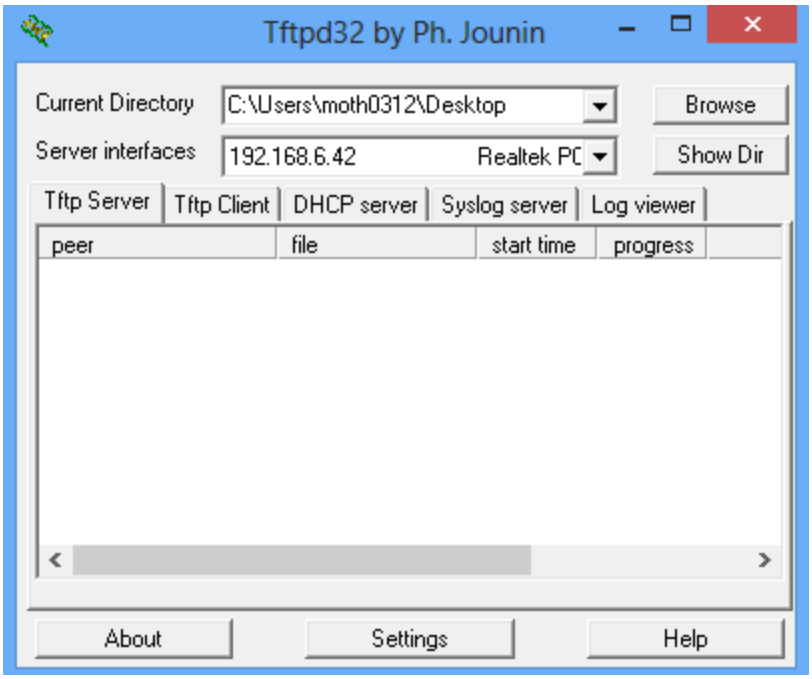
5. Click **Start** to start downloading the file from the HTTP server.
   After downloading the desired firmware file, the system will reboot automatically to take effect.



Upgrade Firmware through TFTP Server

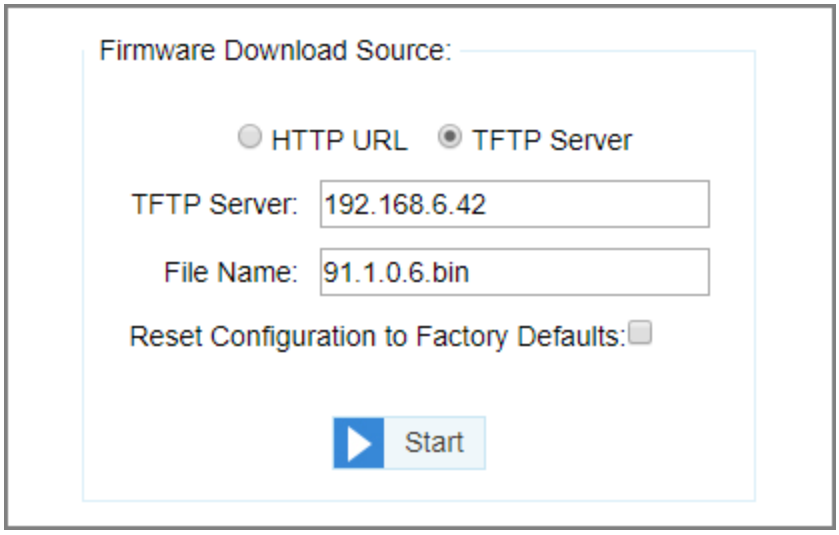
Procedure

1. Set up TFTP server. Below is an example of Tftpd32.
   a. Open Tftpd32.
   b. Click **Browse** to select the firmware file upgraded patch.



2. Log in TG gateway, navigate to **System > System Preferences > Firmware Update**.
3. Check the checkbox of **TFTP Server**.
4. Enter the IP address of the TFTP server in **TFTP Server** field.
5. Enter the name of firmware in **File Name** field.
   Note: The file name should be a BIN file name.

6. Click **Start** to start downloading the file from the TFTP server.
   After downloading the desired firmware file, the system will reboot automatically to take effect.

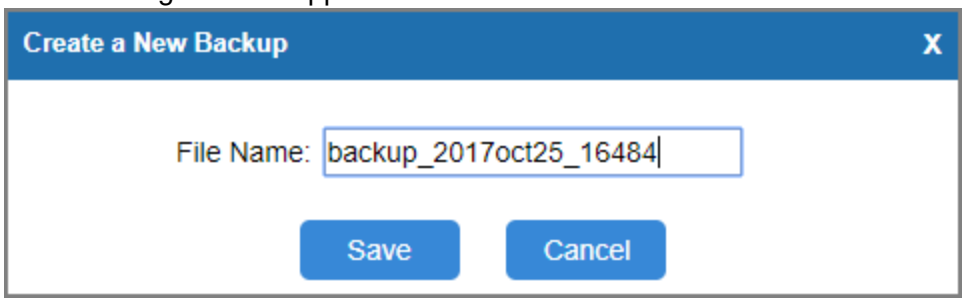


Backup and Restore

Create a Backup File

Procedure

1. Navigate to **System** > **System Preferences** > **Backup and Restore**.
2. Click **Create a New Backup**.
   The following window appears.



3. Set the **File Name**.
4. Click **Save**, all the system configurations are generated in a tar file.
   You can see the backup file on the **Backup and Restore** page.

Upload Backup Files

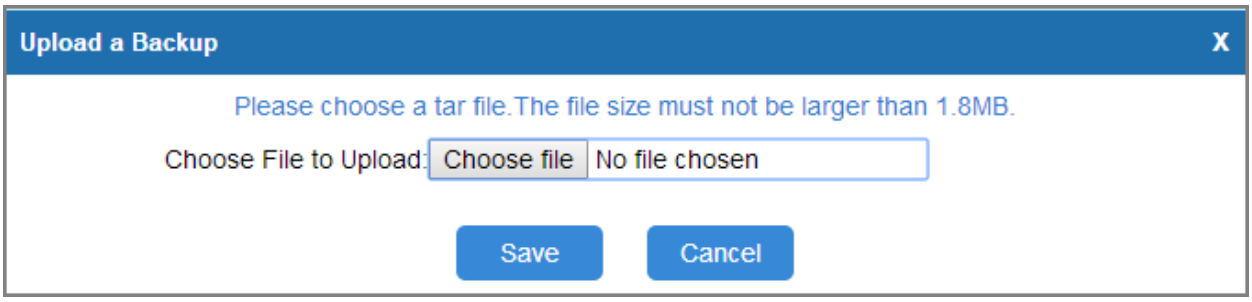
You can upload a backup file from your local PC, and restore the configurations of the backup file.

Prerequisite

The backup file must be a .tar file, and the file size must be smaller than 1.8 MB.

Procedure

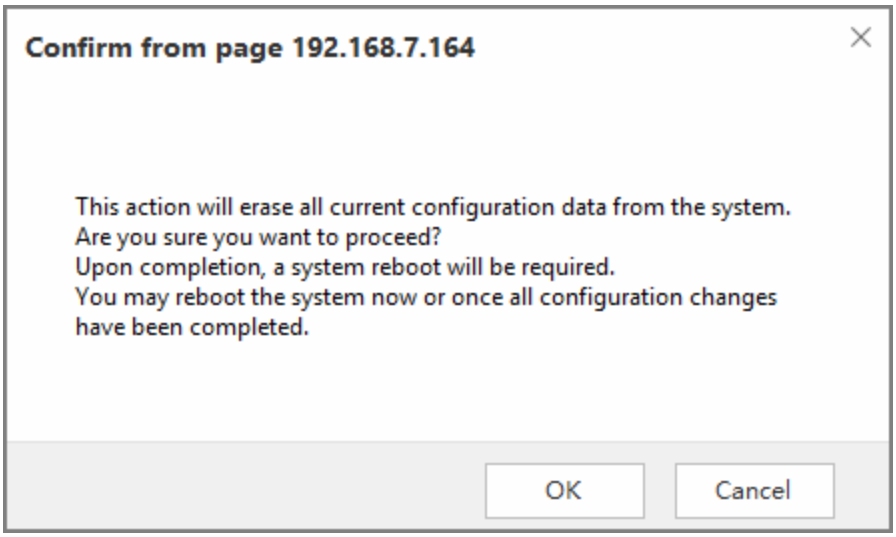
1. Navigate to **System > System Preferences > Backup and Restore**.
2. Click **Upload a Backup**.
   The following window appears.



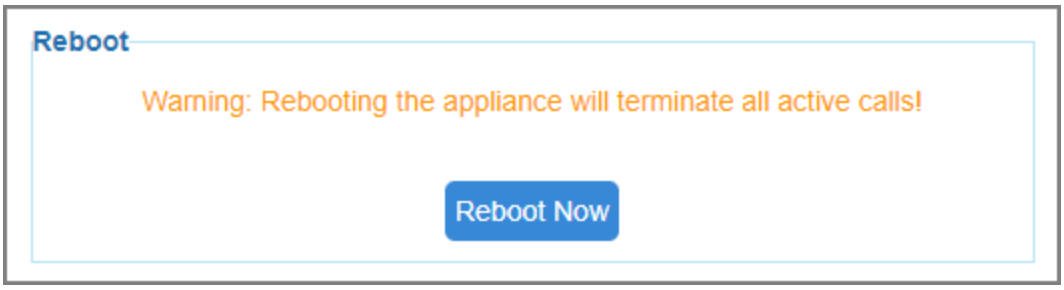
Restore System Configurations

Procedure

1. Navigate to **System > System Preferences > Backup and Restore**.
2. Select a desired backup file, click .
3. Click **OK** to confirm the restore action.



1. Click **Reboot Now** to make the configuration take effect.

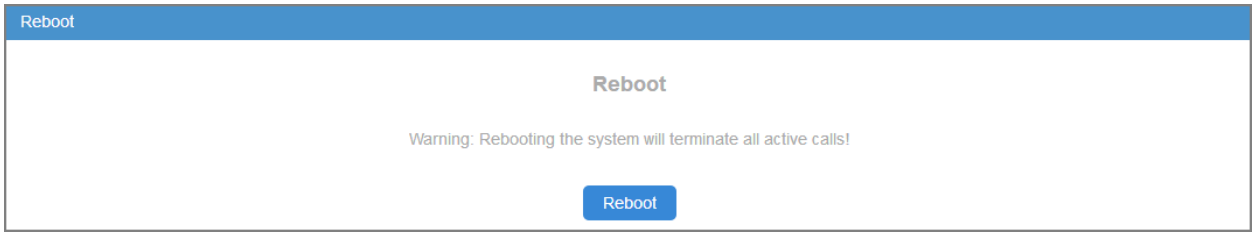


Reboot the System

You can reboot the system on Web user interface.

Procedure

1. Navigate to **System > System Preferences > Reset and Reboot.**
2. Click **Reboot**.
   The system starts to reboot immediately.

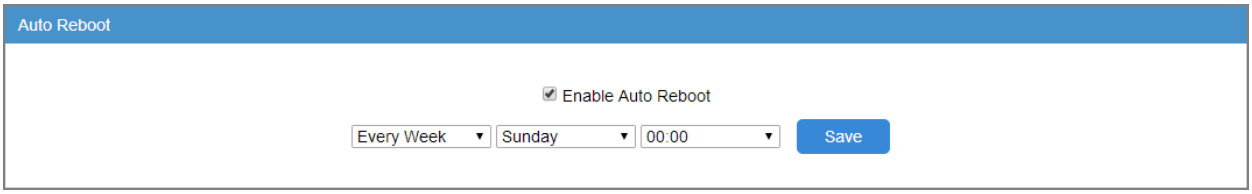


Schedule Automatic Reboots

You can easily schedule an automatic reboots for TG gateway.

Procedure

1. Navigate to **System > System Preferences > Reset and Reboot.**
2. Check the checkbox of **Enable Auto Reboot**.
3. Set the date and time for the automatic reboot.



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

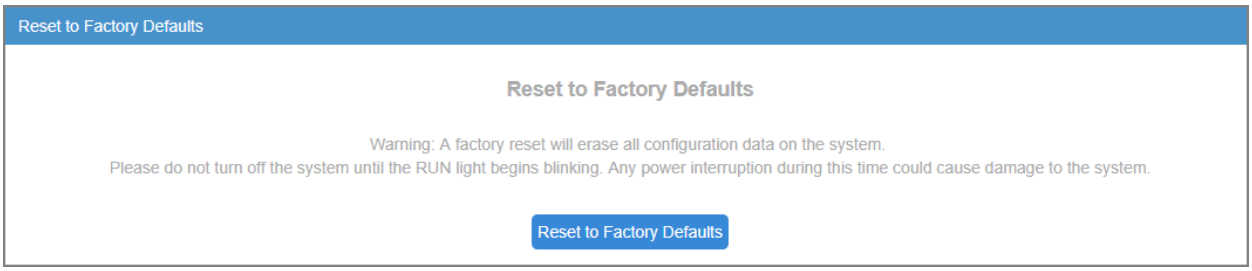
Reset the System

A factory reset will erase all configuration data on the system.

Important: when the system is being reset, don't power off the device, or the system will be damaged.

Procedure

1. Navigate to **System > System Preferences > Reset and Reboot.**
2. Click **Reset to Factory Defaults**.



Configure System Network

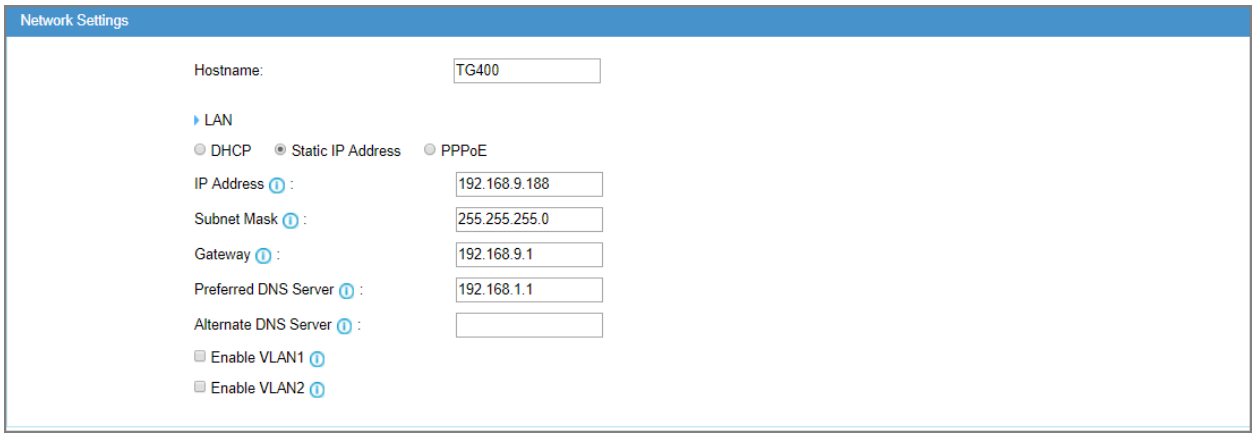
- Change the IP Address of TG Gateway
- Set up VLAN for the TG Gateway
- Set up DDNS for the TG Gateway
- Static Route

Change the IP Address of TG Gateway

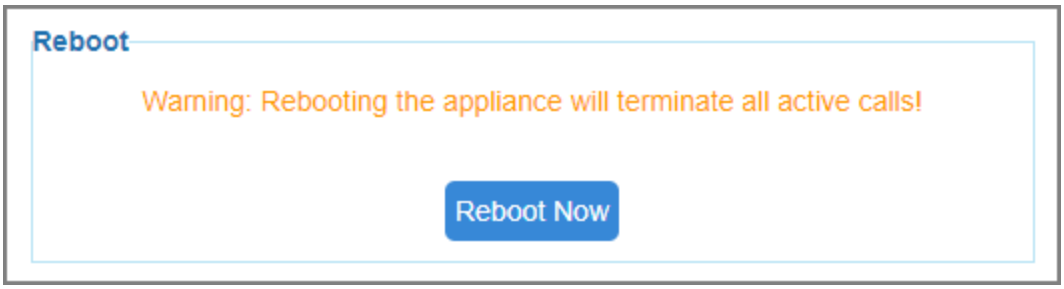
After successfully logging in the Web user interface for the first time with the factory IP address, you can change the network of TG gateway according to your local network.

Procedure

1. Navigate to **System** > **Network Preferences** > **Network Settings** > **LAN**.
2. Choose a network type to **Static IP Address**.
3. Enter the IP address, subnet mask, gateway, DNS server.



4. Click **Save**, a reboot prompt will display on the bottom of the web page.



5. Click **Reboot Now** to reboot the TG gateway.
   After the TG gateway restarts, you can log in the Gateway using the new IP address.

Set up VLAN for the TG Gateway

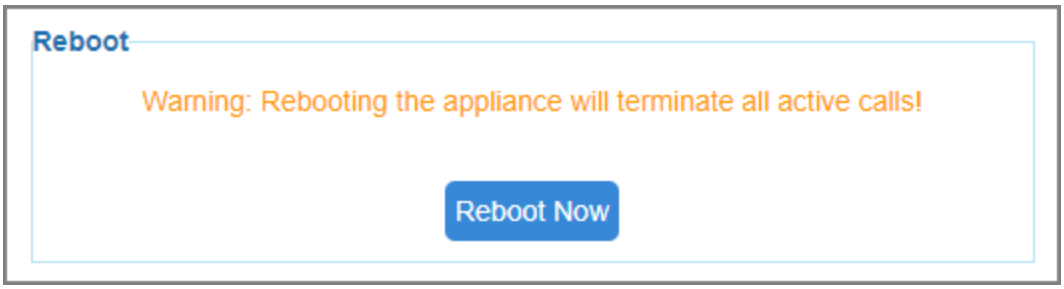
When your local network gets large and has much traffic you need to consider setting up VLAN in your local network. You need to consider using VLAN in any of following situations:

- You have more than 200 devices on your LAN.
- You have a lot of broadcast on your LAN.
- Groups of users need more security or are being slowed down by too many broadcasts.
- Groups of users need to be on the same broadcast domain because they are running the same applications.

Note: Yeastar TG gateway acts as a VLAN client, you need to set up a 3-layer switch in your local network.

Procedure

1. Navigate to **System** > **Network Preferences** > **Network Settings** > **VLAN**.
2. Choose a VLAN to enable it.
3. Get the VLAN information from your network administrator and enter the VLAN information on the TG gateway.
4. Click **Save**, a reboot prompt will display on the bottom of the web page.



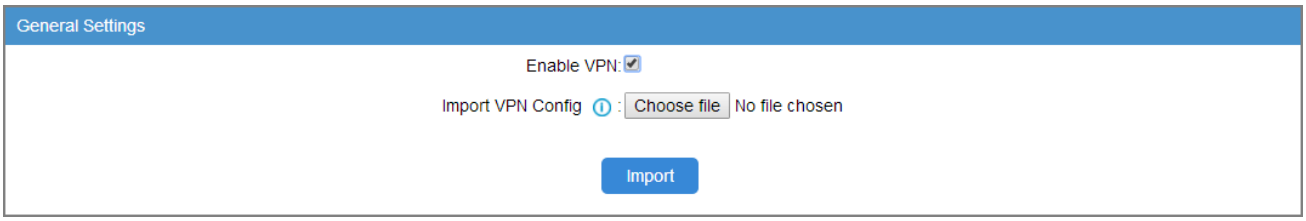
5. Click **Reboot Now** to reboot the TG gateway.

Set up OpenVPN Network

You can set up OpenVPN network for TG gateway to allows users to share information privately between remote locations, or between a remote location and a business' home network.

Procedure

1. Navigate to **System** > **Network Preferences** > **OpenVPN**, check the checkbox of **Enable VPN**.
2. Click **Choose file**, choose the OpenVPN configuration file from your local PC.
   Note: the configuration file should be a compressed tar file.
3. Click **Import**.



4. Check the VPN network status on **Status** > **System Status** > **Network Status**. If the status shows "connected", then the VPN network is available.

Set up DDNS for the TG Gateway

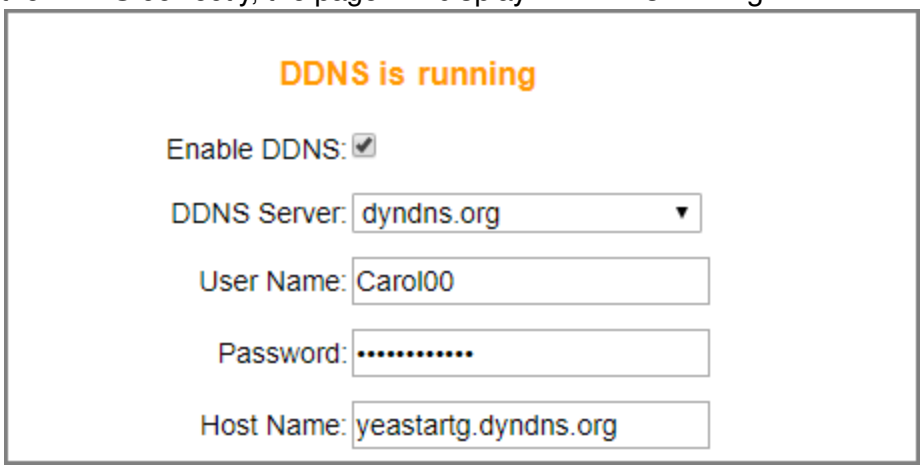
You can set up DDNS for the TG gateway to access the TG gateway using domain names instead of IP address. The DDNS server can change IP address and update your domain information dynamically.

Yeastar TG gateway supports the following DDNS service:

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

Procedure

1. Sign up a DDNS account from the supported DDNS providers.
2. Log in TG gateway user interface, navigate to **System** > **Network Preferences** > **DDNS Settings**, check the checkbox of **Enable DDNS**.
3. Choose the **DDNS Server** of your DDNS account.
4. Enter the DDNS user name, password and host name that you have got from the DDNS server.
5. Click **Save** and **Apply Changes**.
   If you set up the DDNS correctly, the page will display “DDNS is running”.



Static Route

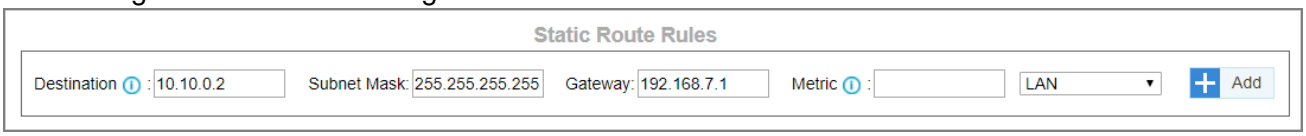
In computer networking a routing table is a data table stored in a router or a networked device that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. Static routes are entries made in a routing table by non-automatic means and which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

Static route on the TG gateway is used to route the connection, packets to particular network destinations, usually a specific gateway.

Set up Static Routes

Procedure

1. Navigate to **Settings** > **System** > **Network Preferences** > **Static Routes**.
2. Configure the static route.
   - **Destination**: enter the destination IP address or IP subnet for the TG gateway to reach using the static route.
   - **Subnet Mask**: enter the subnet mask for the destination address.
   - **Gateway**: enter the gateway address. The TG gateway will reach the destination address via this gateway.
   - **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.
     Note: Leave this field blank if you do not know the information.
   - **Interface**: select the network interface. The TG gateway will reach the destination address using the static route through the selected network interface.



3. Click **Add**, you can see the new created static route on the **Routing Table**.

Routing Table

Destination	Subnet Mask	Gateway	Metric	Interface
default	0.0.0.0	192.168.7.1	0	LAN
10.10.0.2	255.255.255.255	192.168.7.1	0	LAN
192.168.7.0	255.255.255.0	0.0.0.0	0	LAN

Configure VoIP Settings

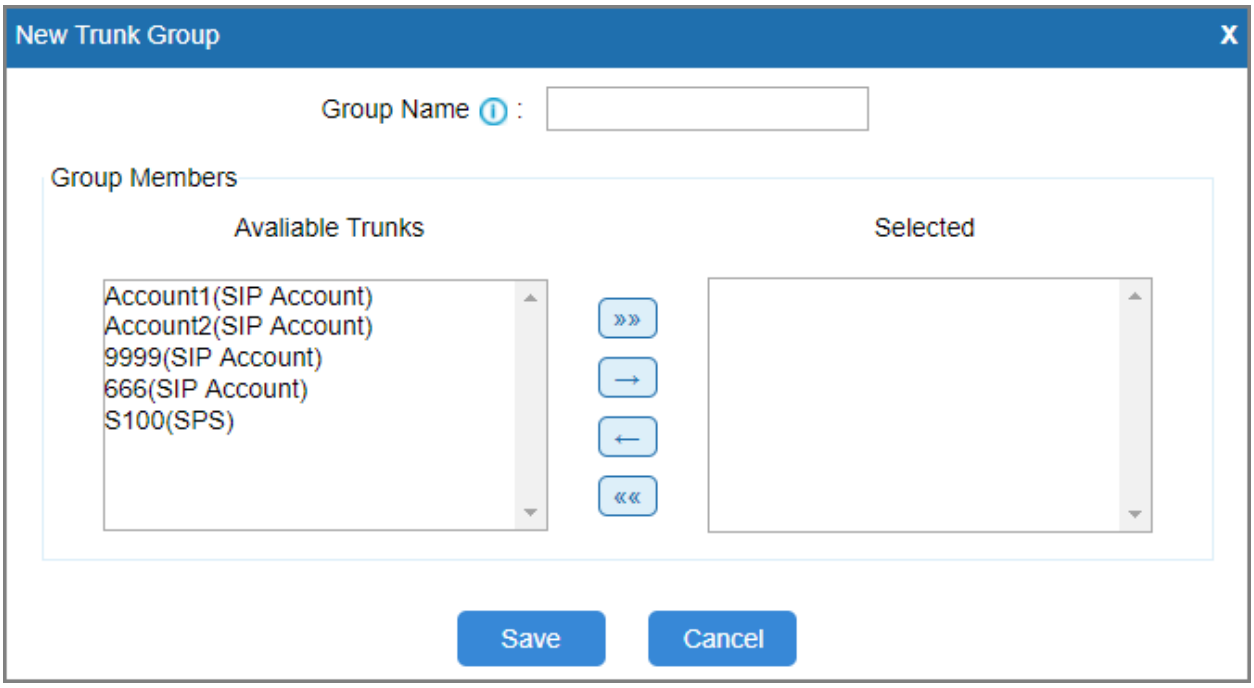
- Group VoIP Trunks
- Configure SIP Settings
- Configure IAX Settings
- Configure General Preferences

Group VoIP Trunks

You can manage the VoIP trunks efficiently by grouping the trunks. The group of VoIP trunks can be selected directly when you are configuring the routes settings.

Procedure

1. Navigate to **Gateway > VoIP Settings > Trunk Group**, click **Add New Trunk Group**.
2. Enter a name in the **Group Name** field.



3. Select desired trunks to the **Selected** box.
4. Click **Save** and **Apply**.

Configure SIP Settings

It is wise to leave the default setting as provided on the system. However, for a few settings, you need to change them to suit your situation.

Configure SIP General Settings

Navigate to **Gateway > VoIP Settings > SIP Settings > General**, to configure the SIP general settings.

Check the description of SIP general settings below.

Option	Description
UDP Port	Port used for SIP registrations, the default is 5060.
TCP Port	Port used for SIP registrations, the default is 5060.
TLS Port	Port used for SIP registrations, the default is 5061.
TLS Verify Server	When using TG gateway as a TLS client, whether or not to verify server's certificate. It is "No" by default.
TLS Verify Client	When using TG gateway as a TLS server, whether or not to verify client's certificate. It is "No" by default.
TLS Ignore Common Name	Set this parameter as "No", then common name must be the same with IP or domain name.
TLS Client Method	When using TG gateway as TLS client, specify the protocol for outbound TLS connections. You can select it as tlsv1, sslv2 or sslv3.
RTP Port Start	Beginning of RTP port range
RTP Port End	End of RTP port range
DTMF Mode	Set default mode for sending DTMF. Default setting: rfc2833
Max Registration/Subscription Time	Maximum duration (in seconds) of a SIP registration. The default is 3600 seconds.
Min Registration/Subscription Time	Minimum duration (in seconds) of a SIP registration. The default is 60 seconds.
Default Incoming/Outgoing Registration Time	The default duration (in seconds) of incoming/outgoing registration.
Register Attempts	The number of SIP REGISTER messages to send to a SIP Registrar before giving up. Default is 0 (no limit)
Register Timeout	Number of seconds to wait for a response from a SIP Registrar before timed out. The default is 20 seconds.
Calling Channel Codec Priority	Once enabled, when dialing out via SIP/SPS trunks, the codec of calling channel will be selected in preference. If not, TG gateway will follow the priority in your SIP/SPS trunks.
DNS SRV Look Up	Please enable this option when your SIP trunk contains more than one IP address.
User Agent	To change the user agent parameter of asterisk . The default is "TG gateway", you can change it if needed. The User Agent will show in SIP packets

Configure NAT Settings

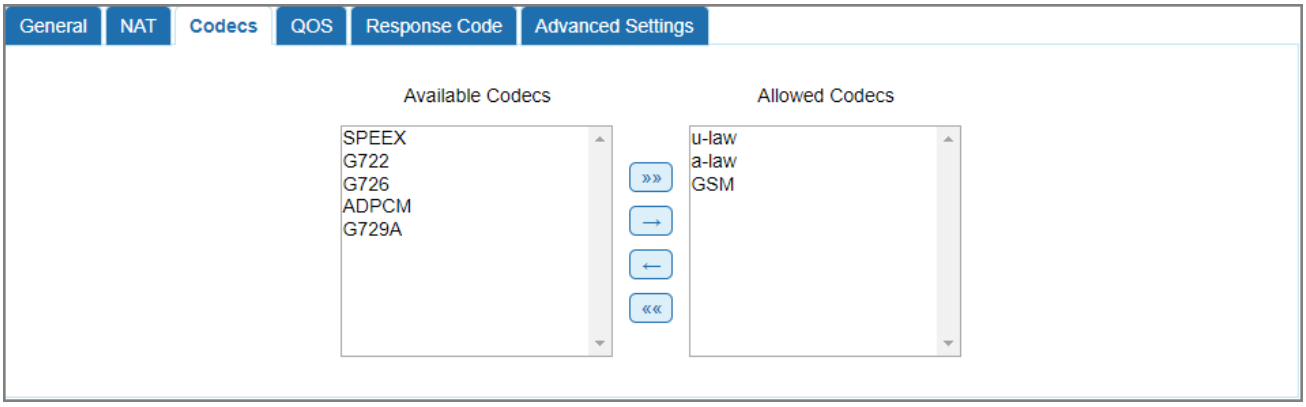
If you want to register the TG VoIP account remotely, you need to configure NAT setting on TG gateway. Navigate to **Gateway > VoIP Settings > SIP Settings > NAT**, to configure the SIP NAT settings.

Check the description of NAT settings below.

Option	Description
Enable STUN	STUN (Simple Traversal of UDP through NATs) is a protocol for assisting devices behind a NAT firewall or router with their packet routing.
STUN Address	The STUN server allows clients to find out their public address, the type of NAT they are behind and the internet side port associated by the NAT with a particular local port. This information is used to set up UDP communication between the client and the VOIP provider and so establish a call.
External IP Address	The IP address that will be associated with outbound SIP messages if the system is in a NAT environment.
External Host	Alternatively, you can specify an external host, and the system will perform DNS queries periodically. This setting is only required when your public IP address is not static. It is recommended that a static public IP address is used with this system. Please contact your ISP for more information.
External Refresh Interval	Used to identify the local network using a network number/subnet mask pair when the system is behind a NAT or firewall. Some examples of this are as follows: “192.168.0.0/255.255.0.0”: All RFC 1918 addresses are local networks; “10.0.0.0/255.0.0.0”: Also RFC1918; “172.16.0.0/12”: Another RFC1918 with CIDR notation; “169.254.0.0/255.255.0.0”: not get the IP address from DHCP server Please refer to RFC1918 for more information.
NAT Mode	Global NAT configuration for the system; the options for this setting are as follows: Yes = Use NAT. Ignore 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.
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.

Configure SIP Codec Settings

Navigate to **Gateway > VoIP Settings > SIP Settings > Codec** to configure the SIP codec settings.

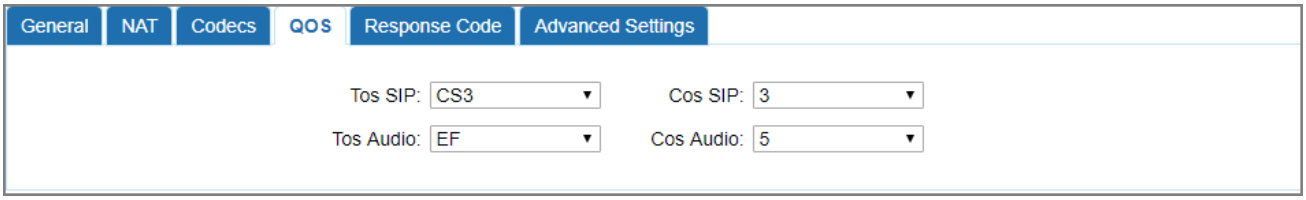


Configure QoS Settings

QoS (Quality of Service) is a major issue in VoIP implementations. You can configure QoS settings 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.

Navigate to **Gateway > VoIP Settings > SIP Settings > QoS** to configure the QoS settings.

Note: we recommend that you configure the QoS in your router or switch instead of TG gateway.

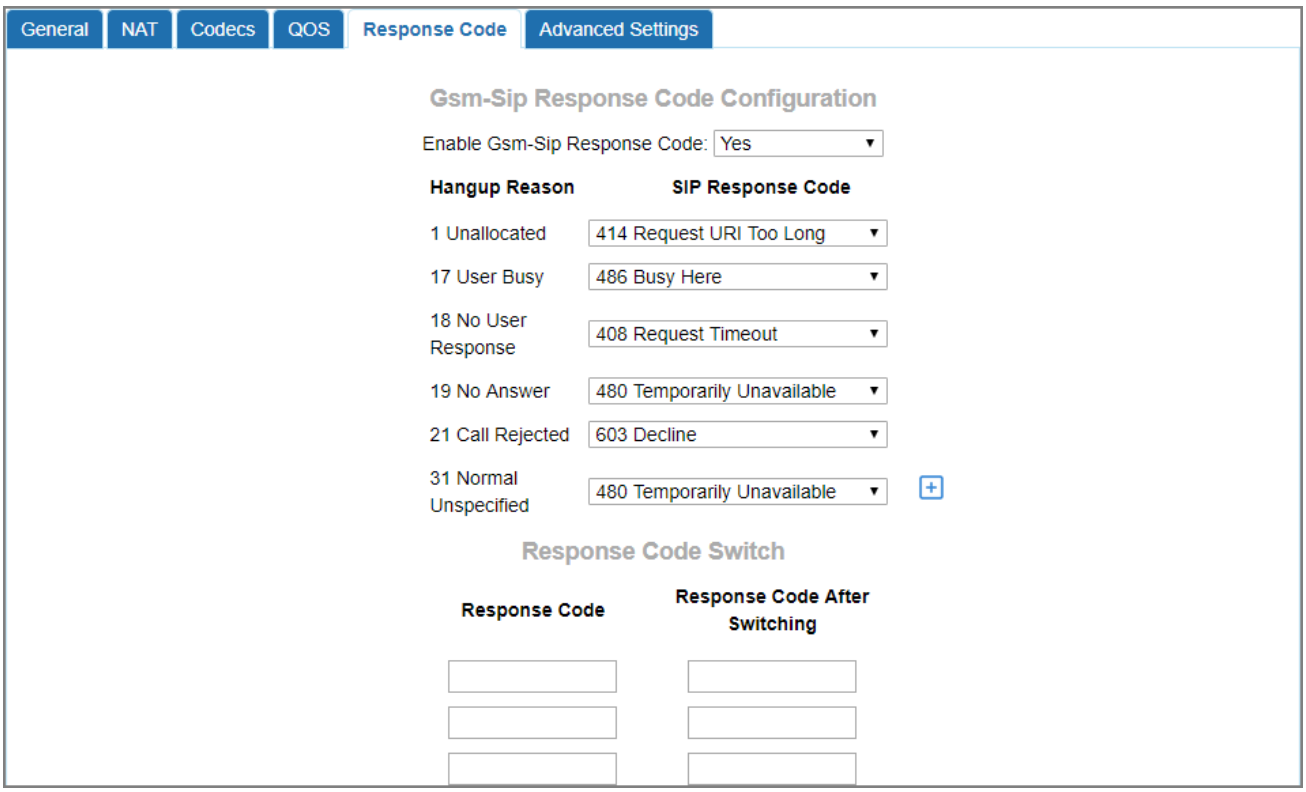


Configure Respond Code Settings

You can change the respond codes from the SIM card carrier before sending the codes to your PBX. After changing the respond codes, the PBX can better understand the exact call status, like busy, no response and others.

Navigate to **Gateway > VoIP Settings > SIP Settings > Respond Code** to configure the respond code settings.

Note: if you are not familiar with the respond codes, contact the PBX administrator and SIM card carrier before you change the settings.



Configure SIP Advanced Settings

Navigate to **Gateway > VoIP Settings > SIP Settings > Advanced Settings**, to configure the SIP advanced settings.

Check the description of SIP advanced settings below.

Option	Description
From Field	Where to get the caller ID in SIP packet
To Field	Where to get the DID in SIP packet
183 Mode	There are two modes Alerted and Immediately. If you choose the Alerted mode, after you make an outbound call, TG will respond a “183 Session Progress” SIP packet. If you choose “Immediately”, TG will respond a “180 ringing” SIP packet
Remote Party ID	Whether send Remote-Party-ID on SIP header. Default is no.
Allow Guest	Whether allow anonymous registration extension. Default: no. It’s recommended to be disabled for security.
Pedantic	Enable pedantic parameter. Default: no.
Always Auth Reject	If enabled, when TG gateway rejects “Register” or “Invite” packets, TG gateway always respond the packets using “SIP 404 NOT FOUND”. It’s recommended to be enabled for security.
OPTIONS Response 200	If you choose “No”, when TG receive an OPTION SIP packet, TG will respond a “404 NOT FOUND” SIP packets. If you choose, TG will respond a “200 OK” SIP packets.

Session-timers	Enable session-timer mode, by default it is “yes”. If you found the call is cut off every 15 minutes , please disable this.
Session-expires	The max refresh interval.
·Session-minse	The min refresh interval, which mustn't be shorter than 90s.
Session-refresher	Choose session-refresher, the default is Uas.

Configure IAX Settings

It is wise to leave the default setting as provided on the system. However, for a few settings, you need to change them to suit your situation.
Navigate to **Gateway > VoIP Settings > IAX Settings** to configure the SIP general settings.

Check the description of IAX settings below.

Option	Description
UDP Port	Port used for IAX2 registrations. The default is 4569.
Bandwidth	Low/medium/high with this option you can control which codec to be used.
Min Registration Time	Minimum duration (in seconds) of an IAX2 registration. The default is 60 seconds
Max Registration Time	Maximum duration (in seconds) of an IAX2 registration. The default is 1200 seconds.
Codecs	Enable the codec you want for IAX communication.

Configure General Preferences

Navigate to **Gateway > VoIP Settings > General Preferences** to configure global settings for the TG gateway.

Check the description of general preferences settings below.

Option	Description
Ring Timeout	The global time out value for extensions, it’s 30 by default.
HTTP Bind Port	Port used for HTTP sessions; the default: 80. If you change this, please reboot to take effect.
Two Stage Dialing Prompt	Choose the customized two stage dialing prompt; it’s disabled by default.

Secure Your Gateway

- Security Center
- Configure Alert Settings
- Upload Certificate Files
- Configure Firewall Rules

Security Center

You can check TG gateway security configuration in “Security Center” page. And also, you can enter the relevant security settings page rapidly.

Check the description of the service port below.

Option	Description
SIP UDP Port	UDP Port used for SIP registrations. The default is 5060.
HTTP Bind Port	Port for login the web. The default port for HTTP is 80.
SSH	SSH port is used to access S-Series underlying configurations to debug the system. The default port is 8022. We recommend that 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.
TCP	TCP Port used for SIP registrations. The default is 5060.
TLS	TLS Port used for SIP registrations. The default is 5061.

Configure Alert Settings

You can set email notification or call notification for system IP attack and Web attack.

Configure IP Attack Alert Settings

When the TG gateway is attacked by an IP address, the system will add the IP to IP Blacklist and send email notification or call notification to the desired users.

Procedure

1. Navigate to **System** > **Security Center** > **Alert Settings**, choose **IP Attack Type** and click .
2. Configure the **Phone Notification Settings**.
   a. If you want to enable phone notification, set **Phone Notification** to **Yes**.
   b. Choose one GSM **Port** to make outbound calls.
   c. Enter the Number to receive call notification.
   d. (**Optional**) Change the alert call attempts, interval, and alert prompt.

3. Configure the **E-mail Notification Settings**.
   a. If you want to enable e-mail notification, set **E-mail Notification** to **Yes**.
   b. In **To** field, enter the email address to receive alert emails.
   c. (**Optional**) Change the e-mail subject and the e-mail template.
4. Click **Save** and **Apply Changes**.

Configure User Lockout Alert Settings

The system will lock the user's IP address after 5 failed web login attempts, and send notification to the desired users.

Procedure

1. Navigate to **System** > **Security Center** > **Alert Settings**, choose **User Lockout Type** and click .
2. Configure the **Phone Notification Settings**.
   a. If you want to enable phone notification, set **Phone Notification** to **Yes**.
   b. Choose one GSM **Port** to make outbound calls.
   c. Enter the Number to receive call notification.
   d. (**Optional**) Change the alert call attempts, interval, and alert prompt.
3. Configure the **E-mail Notification Settings**.
   a. If you want to enable e-mail notification, set **E-mail Notification** to **Yes**.
   b. In **To** field, enter the email address to receive alert emails.
   c. (**Optional**) Change the e-mail subject and the e-mail template.
4. Click **Save** and **Apply Changes**.

Upload Certificate Files

You can create TLS VoIP trunks and accounts on TG gateway. To make the TLS trunks or accounts work, you need to upload certificates to TG gateway.

If you have enabled **TLS Verify Client** (Gateway > VoIP Settings > SIP Settings), you need to upload the TLS certificates on TG gateway.

Procedure

1. Navigate to **Settings** > **System** > **Security** > **Certificates** to upload your certificates.
2. Upload trusted certificate.
   Trusted certificate is a CA certificate. The connected PBX should upload the same certificate.
   a. Click **Upload Certificate**, choose **Type** to **Trusted Certificate**.
   b. Click **Browse** to select the file from your local PC.
   c. Click **Save** to start uploading.
      You can see the certificate appear on **Trusted Certificate** list.
3. Upload gateway certificate.

Gateway certificate is made for the TG gateway.

a. Click **Upload Certificate**, choose **Type** to **Gateway Certificate**.
b. Click **Browse** to select the file from your local PC.
c. Click **Save** to start uploading.
   You can see the certificate appear on **Gateway Certificate** list.

4. Reboot the TG gateway to take effect.

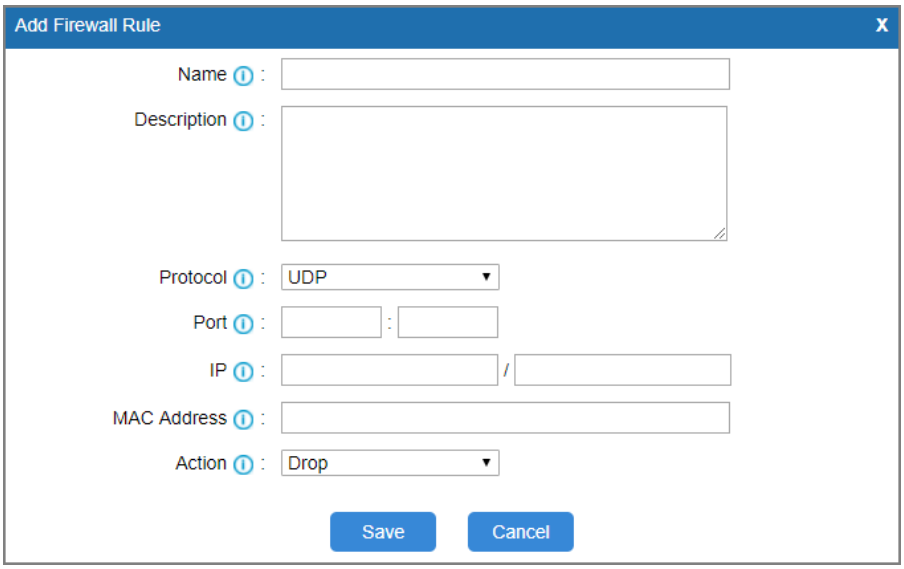
Configure Firewall Rules

You can configure firewall rules for the TG gateway to protect the system from attacking.
Important: back up the system configuration before you start configuring firewall in case you may be unable to log in the system with improper firewall configurations.

Add a Firewall Rule

Procedure

1. Navigate to **System** > **Security Center** > **Firewall Rules**, click **Add Rule**.
2. Set a Name for the rule.
3. (**Optional**) Enter notes in the **Description** field.
4. Choose the desired **Protocol**.
5. Enter a port range in **Port** fields. If you want to set the rule for a specific port, enter the same port value in the two **Port** fields. For example, 5060:5060 stands for port 5060.
6. Enter the IP address and subnet mask in the **IP** field. For example, 192.168.5.0/255.255.255.0.
7. (**Optional**) Enter the MAC address of the target device.
   The format of the MAC address XX:XX:XX:XX:XX:XX.
8. Choose the rule **Action**.
   - **Accept**: accept the access from remote hosts.
   - **Drop**: drop the access from remote hosts.
   - **Ignore**: ignore the access.



9. Click **Save** and **Apply Changes**.

Enable Firewall Function

Procedure

1. Navigate to **System > Security Center > Firewall Rules**, check the checkbox of **Enable Firewall**.
2. Click **Save** and **Apply Changes**.
   The web page will prompt you that the firewall is enabled.

Block Pings through Your TG Gateway

By default, users can use the ping command from other devices to check if the TG gateway is alive. You can block the pings to place your TG gateway in a more secure environment.

Procedure

1. Navigate to **System > Security Center > Firewall Rules**, check the checkbox of **Disable Ping**.
2. Click **Save** and **Apply Changes**.

Block All Packets and Connections

You can add Accept firewall rules for the trusted IP addresses or devices, and block all the other packets and connections.

Important: you must create Accept firewall rules for the HTTP port and SSH port before you block all packets and connections, or you will be unable to access the TG gateway.

Procedure

1. Navigate to **System > Security Center > Firewall Rules**, check the checkbox of **Drop All**.
2. Click **Save** and **Apply Changes**.

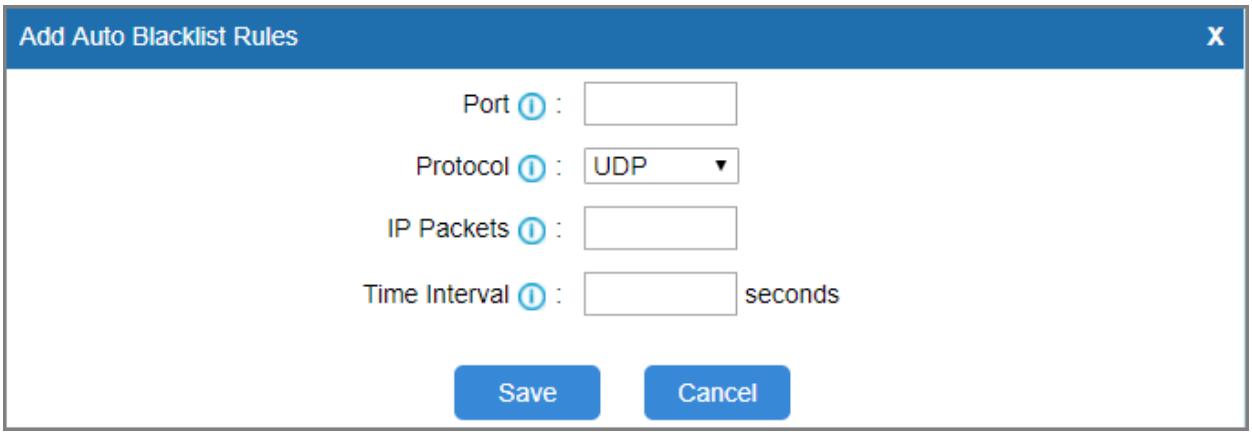
Add an IP Blacklist Rule

The rules in IP Blacklist will help the system to add the IP address to the blacklist automatically if the number of the packets it sends exceeds the rule you configured.

The system has 3 default IP blacklist rules, you can edit them or add a new one.

Procedure

1. Navigate to **System > Security Center > IP Blacklist**, click **Add Rule**.
2. Enter the desired port in Port field.
3. Choose the Protocol of this rule.
4. Enter the allowed IP packets number in the specific time interval in IP Packets field.
5. Enter the time interval to receive IP packets in Time Interval field.
   For example, IP Packets is set to 90, Time Interval is set to 60, and it means 90 IP packets are allowed in 60 seconds.
6. Click **Save** and **Apply Changes**.



Delete Blocked IP Address

You can delete the blocked IP address if the system blocks your trusted IP address.

Procedure

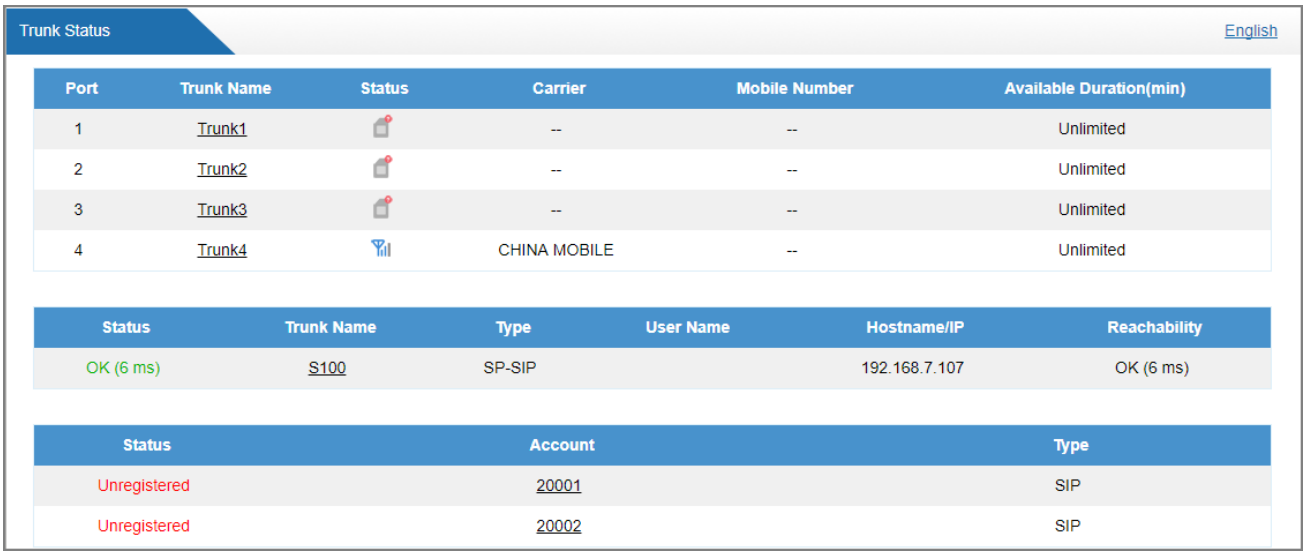
1. Navigate to **System > Security Center > IP Blacklist**.
2. Choose the desired IP address from **IP Blacklist** list, click .

System Status

- Check Trunk Status
- Check Network Status
- Check System Info

Check Trunk Status

Navigate to **Status** > **System Status** > **Trunk Status** to check the mobile trunk status and VoIP trunks status.



Port	Trunk Name	Status	Carrier	Mobile Number	Available Duration(min)
1	Trunk1		--	--	Unlimited
2	Trunk2		--	--	Unlimited
3	Trunk3		--	--	Unlimited
4	Trunk4		CHINA MOBILE	--	Unlimited

Status	Trunk Name	Type	User Name	Hostname/IP	Reachability
OK (6 ms)	S100	SP-SIP		192.168.7.107	OK (6 ms)

Status	Account	Type
Unregistered	20001	SIP
Unregistered	20002	SIP

Mobile Trunk Status

Status	Description
	The trunk is idle, the icon shows the signal strength.
	The trunk is busy.
	The module is powered off.
	No SIM card inserted.
	No signal.
	PIN/PUK Error.
	Mobile network registration failed.

!	Malfunction in module; please examine the relevant module.

VoIP Trunk (Account) Status

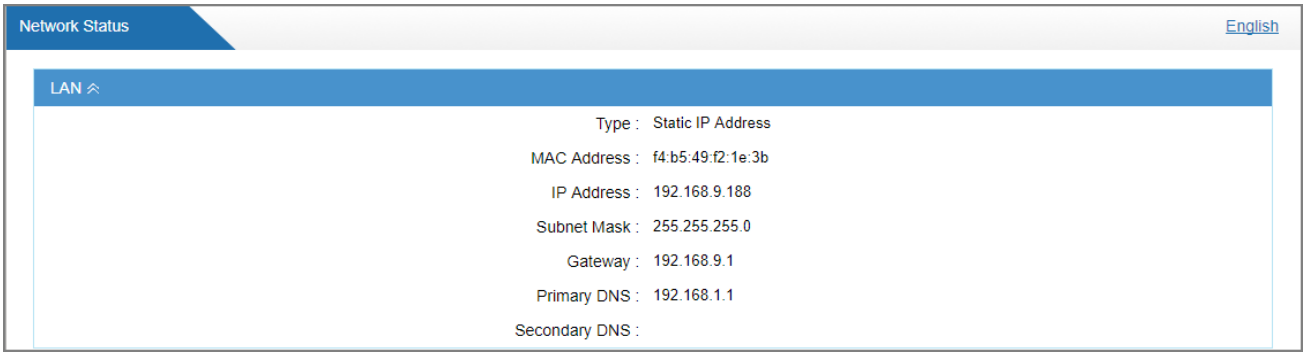
Status	Description
Unregistered	Trunk registration failed
Registered	Successful registration, trunk is ready for use
Request Sent	Registering
Waiting	Waiting for authentication

VoIP Trunk (Service Provider) Status

Status	Description
OK	Successful registration, trunk is ready for use
Unreachable	The trunk is unreachable.
Failed	Trunk registration failed.

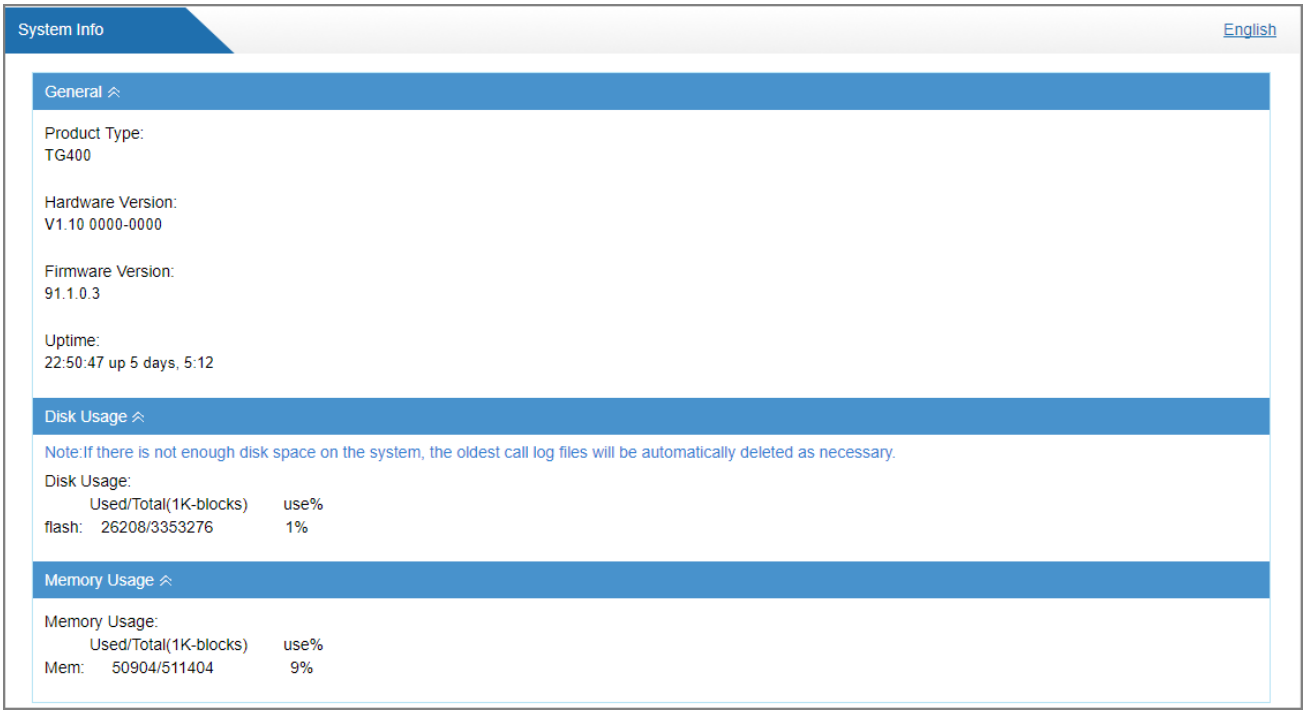
Check Network Status

Navigate to **Status > System Status > Network Status** to check the TG gateway's network information and MAC address.



Check System Info

Navigate to **Status > System Status > System Info** to check the TG gateway's hardware version, firmware version, disk usage, and memory usage.


System Info
English
General
Product Type:
TG400
Hardware Version:
V1.10 0000-0000
Firmware Version:
91.1.0.3
Uptime:
22:50:47 up 5 days, 5:12
Disk Usage
Note:If there is not enough disk space on the system, the oldest call log files will be automatically deleted as necessary.
Disk Usage:
Used/Total(1K-blocks) use%
flash: 26208/3353276 1%
Memory Usage
Memory Usage:
Used/Total(1K-blocks) use%
Mem: 50904/511404 9%

Reports

- Call Logs
- System Logs

Call Logs

You can perform the following operations on the **Call Logs** page.

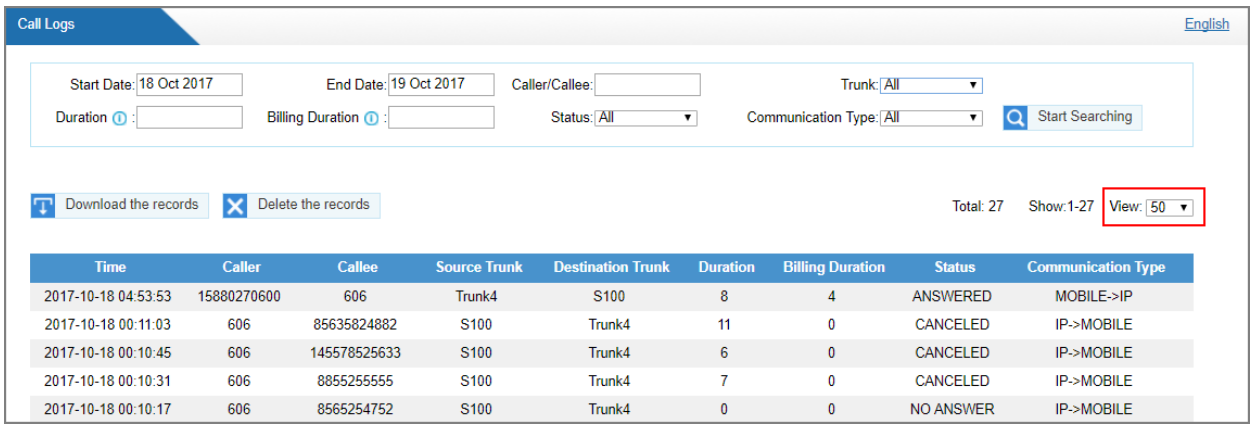
- View call logs
- Search call logs
- Download searched call logs
- Delete searched call logs

View Call Logs

By default, one call log page displays a maximum of 25 records. If you want to view more records on one page, you can change the **View** value.

Procedure

1. Navigate to **Status** > **Report** > **Call Logs**.
2. Set **View** value, the call log page displays the desired maximum call logs.



Time	Caller	Callee	Source Trunk	Destination Trunk	Duration	Billing Duration	Status	Communication Type
2017-10-18 04:53:53	15880270600	606	Trunk4	S100	8	4	ANSWERED	MOBILE->IP
2017-10-18 00:11:03	606	85635824882	S100	Trunk4	11	0	CANCELED	IP->MOBILE
2017-10-18 00:10:45	606	145578525633	S100	Trunk4	6	0	CANCELED	IP->MOBILE
2017-10-18 00:10:31	606	8855255555	S100	Trunk4	7	0	CANCELED	IP->MOBILE
2017-10-18 00:10:17	606	8565254752	S100	Trunk4	0	0	NO ANSWER	IP->MOBILE

Search Call Logs

You can search call logs by the following criteria.

- **Date Duration:** choose the Start Date and End Date to filter the call logs.
- **Caller/Callee:** enter the caller/callee's number to filter the call logs.
- **Trunk:** choose which trunk is used to call out or call in.
- **Duration:** the call duration. Enter a value to filter the call logs that have call duration equal to or greater than the value.

- **Billing Duration:** the billing duration. Enter a value to filter the call logs that have billing duration equal to or greater than the value.
- **Status:** choose a call status.
- **Communication Type:** choose a communication type.

Procedure

1. Navigate to **Status > Report > Call Logs**.
2. Choose **Start Date** and **End Date**.
3. (Optional) Set other searching criteria.
4. Click **Start Searching**, the filtered call logs appears on the **Call Log** page.

Download Searched Results

After searching the desired call logs, you can download and export the call logs to a .csv file.

Procedure

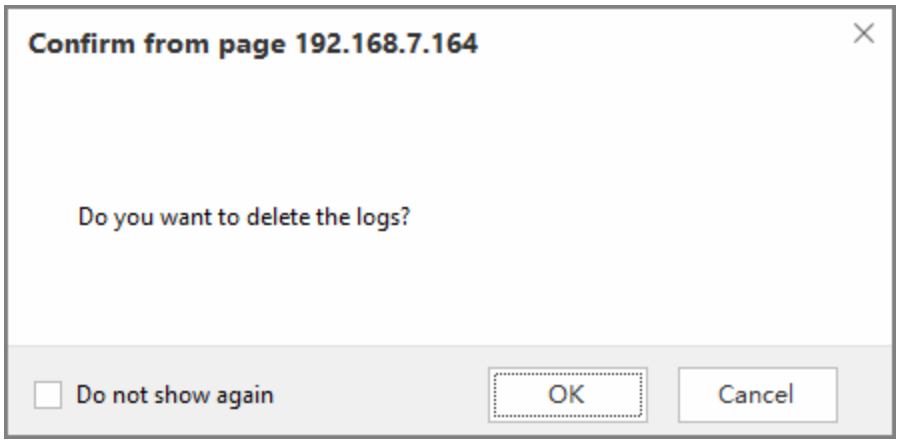
1. Click **Download the records** to download and export the searched call logs.

Delete Searched Results

You can search the desired call logs, and delete them.

Procedure

1. Click **Delete the records** to delete the searched call logs. A popup window appears.



2. Click **Yes** to delete the searched call logs.

System Logs

You can set the system to automatically trace hardware logs, normal logs, debug logs, and web logs.

Trace Hardware Logs

The system supports storing up to 4 hardware log files. When the system generates more than 4 hardware log files, the system will replace the oldest file with the new file.

Procedure

1. Navigate to **Status** > **Reports** > **System Logs** > **Options**.
2. Check the checkbox of **Enable Hardware Log**.
3. Click **Save** and **Apply Changes**.
   The system starts to trace the hardware logs. You can check the hardware log file on **System Logs** page.

Trace Normal Logs

The system supports storing up to 16 normal log files. The maximum size of each log file is 1Mb. When the system generates more than 16 normal log files, the system will replace the oldest file with the new file.

Procedure

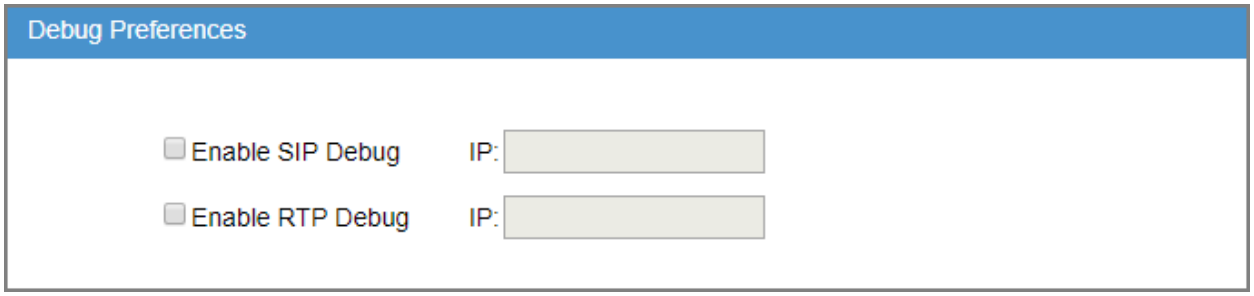
1. Navigate to **Status** > **Reports** > **System Logs** > **Options**.
2. Check the checkbox of **Enable Normal Log**.
3. Click **Save** and **Apply Changes**.
   The system will start to trace the normal logs. You can check the normal log file on **System Logs** page.

Trace Debug Logs

The system supports storing up to 2 debug log files. The maximum size of each log file is 10Mb. The system will delete the debug log files after reboot.

Procedure

1. Navigate to **Status** > **Reports** > **System Logs** > **Options**.
2. Check the checkbox of **Enable Debug Log**.
3. **(Optional)** Enable SIP debug and RTP debug, enter the target debug IP address.



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

The system starts to trace the asterisk debug logs. You can check the debug log file on **System Logs** page.

Trace Web Logs

The system supports storing up to 2 files of web operation logs. The maximum size of each log file is 1Mb. When the system generates more than 2 normal log files, the system will replace the oldest file with the new file.

Procedure

1. Navigate to **Status** > **Reports** > **System Logs** > **Options**.
2. Check the checkbox of **Enable Web Log**.
3. Click **Save** and **Apply Changes**.
   The system will start to trace the web logs. You can check the web log file on **System Logs** page.

Download System Logs

Procedure

1. Navigate to **Status** > **Reports** > **System Logs**.
2. Choose the desired system log file, click .

Delete System Logs

Procedure

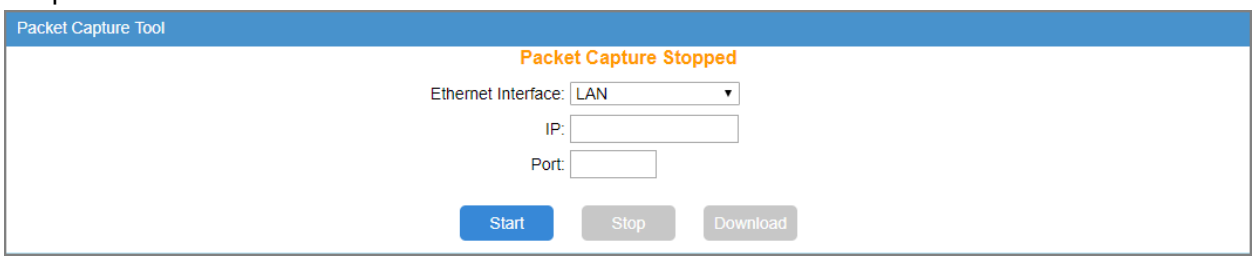
1. Navigate to **Status** > **Reports** > **System Logs**.
2. Choose the desired system log file, click .

Capture Ethernet Packet

Yeastar TG gateway provides an integrated tool to help you capture Ethernet packet on Web user interface. You can debug the system efficiently with this tool.

Procedure

1. Navigate to **Status** > **Reports** > **System Logs** > **Packet Capture Tool**.
2. Choose the target Ethernet Interface.
3. **(Optional)** Enter the target IP address.
4. **(Optional)** Enter the target port.
5. Click **Start**.

The system will start to capture the Ethernet packet.

6. Click **Stop** to stop capturing packet.
7. Click **Download** to download the captured packet to your local PC and use Wireshark to open the packet file.