

TG100 VoIP GSM/3G 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: 51.18.0.50

Revised: December 30, 2019

Copyright

Copyright 2006-2019 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 Yeastar Information Technology Co., Ltd. Under the law, reproducing includes translating into another language or format.

Declaration of Conformity



Hereby, 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.

Warranty

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

Yeastar Information Technology Co., Ltd. makes no warranty of any kind with regard to this guide, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Yeastar Information Technology Co., Ltd. shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance or use of this guide.

WEEE Warning



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

Table of Contents

ABOUT THIS GUIDE	9
TG100 GATEWAY OVERVIEW	10
HARDWARE INSTALLATION	12
Package Contents	12
Safety Disclaimers and Installation Warnings	12
Insert/Remove SIM Card	13
Connect Antenna	13
Connect Ethernet Line	13
Connect Power Supply	14
GETTING STARTED	15
Log in Web Interface	15
Web Configuration Panel	16
MANAGE MOBILE MODULE	16
Configure Mobile Module Profile	17
Reboot Mobile Module	17
Enable/Disable Mobile Module	18
Display Caller's Mobile Number	18
Adjust Mobile Module Volume	19
Configure Call Progress Tone	20
Configure the Call Duration of Mobile Trunk	21
Set a Single Call Duration of Mobile Trunk	21
Set a Monthly Talk Plan of Mobile Trunk	21
Set Talk Time Alarm of Mobile Trunk	22
Configure Advanced Settings	23
Unlock the SIM Card	24
CONNECT TG GATEWAY TO YOUR PBX (ACCOUNT MODE)	25

Connect TG Gateway to Your PBX (Account Mode)	25
Set up a Mobile to IP Route (Account Mode)	27
Set up an IP to Mobile Route (Account Mode)	28
CONNECT TG GATEWAY TO YOUR PBX (REGISTER TRUNK)	29
Connect TG Gateway to Your PBX (Register Trunk Mode)	29
Set up a Mobile to IP Route (Register Trunk Mode)	31
Set up an IP to Mobile Route (Register Trunk Mode)	32
CONNECT TG GATEWAY TO YOUR PBX (PEER TRUNK)	33
Connect TG Gateway to Your PBX (Peer Trunk Mode)	34
Set up a Mobile to IP Route (Peer Trunk Mode)	35
Set up an IP to Mobile Route (Peer Trunk Mode)	36
Block Incoming Numbers	37
Block Outgoing Numbers	37
Block both Incoming and Outgoing Numbers	38
Callback	39
Set up Callback for Specific Numbers	39
Set up Callback for All Numbers	40
Add Callback Rules	40
AutoCLIP Route	41
Set up AutoCLIP Route	41
Delete AutoCLIP Records	41
MANAGE MESSAGES	42
Send SMS Messages	42
Manage SMS Contacts	43
Add an SMS Contact	43
Delete an SMS Contact	43
Manage Sent SMS Messages	43

Check the Status of Sent SMS Messages	44
Search Sent SMS Messages	44
Download Searched Results	44
Delete Searched Results	45
Manage Received SMS Messages	45
View Received SMS Messages	45
Reply SMS Messages	45
Search Received SMS Messages	46
Download Searched Results	46
Delete Searched Results	47
SMS to Email	47
Configure Email POP3 Settings	47
Configure SMS to Email Settings	48
Send SMS to Email	48
Email to SMS	49
Configure Email SMTP Settings	49
Configure Email to SMS Settings	50
Send Email to SMS	50
Schedule SMS Clear Tasks	51
Send USSD Messages	52
Send a USSD Message	52
Exit USSD Sessions	52
Enable TG Gateway API	53
Change Password of SMS Center	53
CONFIGURE SYSTEM SETTINGS	54
Change Web Login Password	54
Change Date and Time	54

Upload Custom Prompts	55
Set up System Email	56
Update System Firmware	57
Update Firmware through HTTP Server	57
Upgrade Firmware through TFTP Server	58
Backup and Restore	60
Create a Backup File	60
Upload Backup Files	60
Restore System Configurations	61
Reboot the System	62
Reset the System	62
CONFIGURE SYSTEM NETWORK	63
Change the IP Address of TG Gateway	63
Set up VLAN for the TG Gateway	64
Set up OpenVPN Network	66
Set up DDNS for the TG Gateway	66
Static Route	67
Set up Static Routes	67
CONFIGURE VOIP SETTINGS	68
Group VoIP Trunks	69
Configure SIP Settings	69
Configure SIP General Settings	69
Configure NAT Settings	71
Configure SIP Codec Settings	73
Configure QoS Settings	73
Configure Response Code Settings	74
Configure SIP Advanced Settings	74

Configure IAX Settings.....	76
Configure General Preferences	77
SECURE YOUR GATEWAY	78
Security Center.....	78
Configure Alert Settings	78
Configure IP Attack Alert Settings.....	79
Configure User Lockout Alert Settings	80
Upload Certificate Files	80
Configure Firewall Rules	81
Add a Firewall Rule.....	81
Enable Firewall Function	82
Block Pings through Your TG Gateway	83
Block All Packets and Connections	83
Add an IP Blocklist Rule	83
Delete Blocked IP Address	84
SYSTEM STATUS	84
Check Trunk Status	84
Mobile Trunk Status	85
VoIP Trunk (Account) Status	85
VoIP Trunk (Service Provider) Status	86
Check Network Status	86
Check System Info	86
REPORTS.....	87
Call Logs	87
View Call Logs.....	87
Search Call Logs	88
Download Searched Results	88

Delete Searched Results	89
System Logs.....	89
Trace Hardware Logs	89
Trace Normal Logs.....	90
Trace Debug Logs.....	90
Trace Web Logs	91
Download System Logs.....	91
Delete System Logs.....	91
Capture Ethernet Packet	91

About This Guide

Thanks for choosing Yeastar TG100 VoIP GSM/3G 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 TG100. We begin by assuming that you are interested in TG gateway and familiar with networking and other IT disciplines.

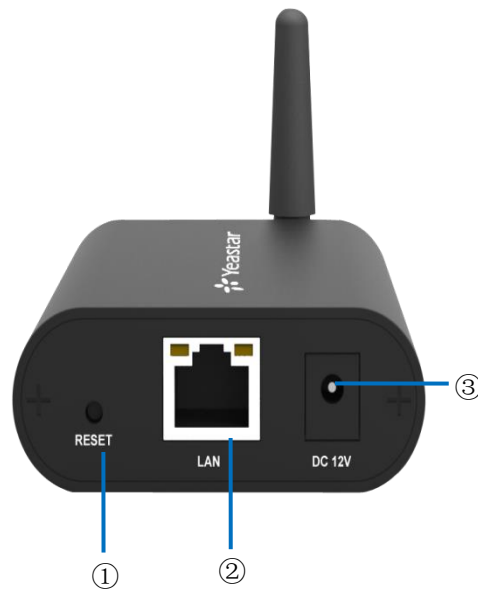
Safety When Working with Electricity



- 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.

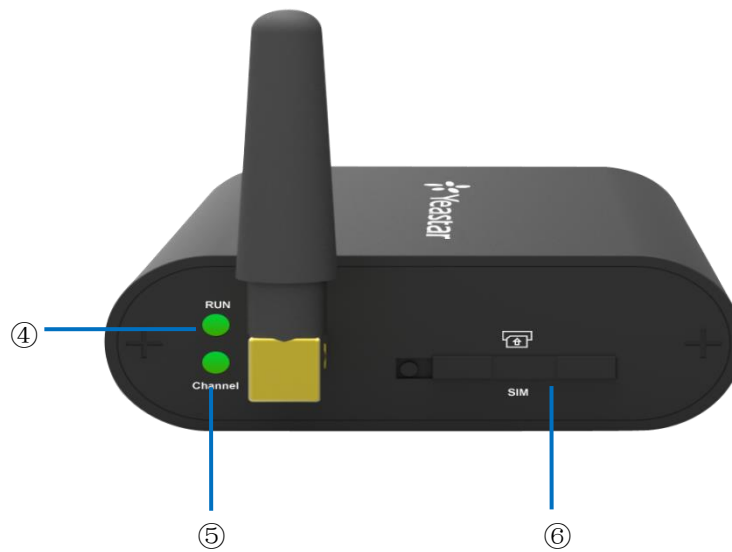
TG100 Gateway Overview

Front Panel



No.	Feature	Description
①	Reset Button	Press and hold for 10 seconds to restore the factory defaults.
②	LAN port	10/100 adaptive RJ45 Ethernet port.
③	Power Inlet	Connect the power supply to the port.

Back Panel



No.	Feature	Description
④	RUN LED	Indicates the system status. <ul style="list-style-type: none">Blinking: The system is working properly.Not Blinking/Off: The system goes wrong.
⑤	Channel LED	Indicates status of the SIM card. <ul style="list-style-type: none">Blinking: The SIM card is in a call or ringing.Static Green: The SIM card is registered.Off: The SIM card is not registered.
⑥	SIM Card Slot	Insert the SIM card to the SIM card slot.

Hardware Installation

- [Package Contents](#)
- [Safety Disclaimers and Installation Warnings](#)
- [Insert/Remove SIM Card](#)
- [Connect Antenna](#)
- [Connect Ethernet Line](#)
- [Connect Power Supply](#)

Package Contents

Item	Unit	QTY	Description
TG100	PC	1	TG100 main box
Power adaptor	PC	1	Power Supply
Warranty card	PC	1	With Serial Number printed for Repair & Return
Antenna (short)	PC	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 adaptor provided with TG100 gateway.
- Make sure that the supply voltage matches the specifications indicated on the front panel of the device.
- To avoid the electric accident, do not open or remove the cover of TG100 when it is working as well as off the power.
- Before cleaning the TG100, cut off the power supply.

Environment

Install the Yeastar TG100 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

Before powering on TG100, open the box and insert the SIM card on the back panel directly.

To remove this card, press the button on the left side, the card will pop directly.

Note:

1. The SIM card should be mini-SIM (2FF).
2. Please cut off the power before installing SIM card. You can also log in Web interface to power this module off separately.

Connect Antenna

TG100 gateway is equipped with antenna connector for the GSM/3G module. The external antenna should be installed vertically always on a site with a good wireless signal. You can follow steps below to connect the antenna.

Procedure

1. Connect the external antenna on a site with a good wireless signal, and rotate the antenna into the antenna connector.
2. Adjust the angle of the antenna.

Connect Ethernet Line

TG100 provides one 10/100M Ethernet port with RJ45 interface and LED indicator. You can follow steps below to connect the Ethernet line.

Procedure

1. Connect one end of Ethernet line into the Ethernet port of TG100 gateway.
2. Connect the other end of the Ethernet line to a hub, switch, router, LAN or WAN.
3. Check the status of the LED indicator.

- Yellow: The port is in 100M mode.
- Dark yellow: The port is in 10M mode.
- Green: The port is properly connected.
- Flashing: Data transmission.

Connect Power Supply

TG100 utilizes the high-performance switch power, which supplies enough voltage and electrical energy.

AC Input: 100~240V

DC Output: 12V, 1A

You can follow steps below to connect power supply.

Procedure

1. Connect one end of the power adapter to the power inlet on the front panel, and plug the other end to the standard electrical wall socket.
2. Check the RUN LED on the back panel. A solid green LED indicates that power is being supplied correctly.

Note:

- Please switch off the power before plugging or unplugging the power adaptor.
- Please disconnect all telecommunication network connectors and cable distribution system connectors before powering off the TG device.

Getting Started

- [Log in Web Interface](#)
- [Web Configuration Panel](#)

Log in Web Interface

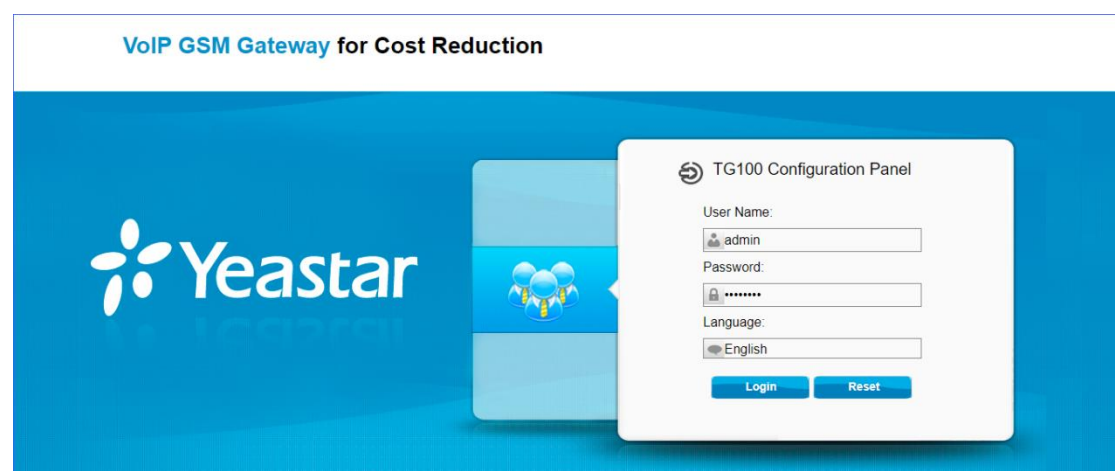
Yeastar TG100 provides web-based configuration interface, you can manage the device by logging in the Web interface. Check the factory defaults below:

- 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, and press **Enter** on your keyboard.
2. Enter your user name and password, and click **Login**.



Web Configuration Panel

There are 4 main sections on the Web Configuration Panel for you to check the TG100's status and configure it.

- **Status:** Check Trunk Status, Network Status, System Info, Call Logs and 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 outbox, etc.
- **Gateway:** Configure the mobile port, VoIP settings, and Routes settings.
- **Logout:** Log out of TG100.

Note:

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


Manage Mobile Module

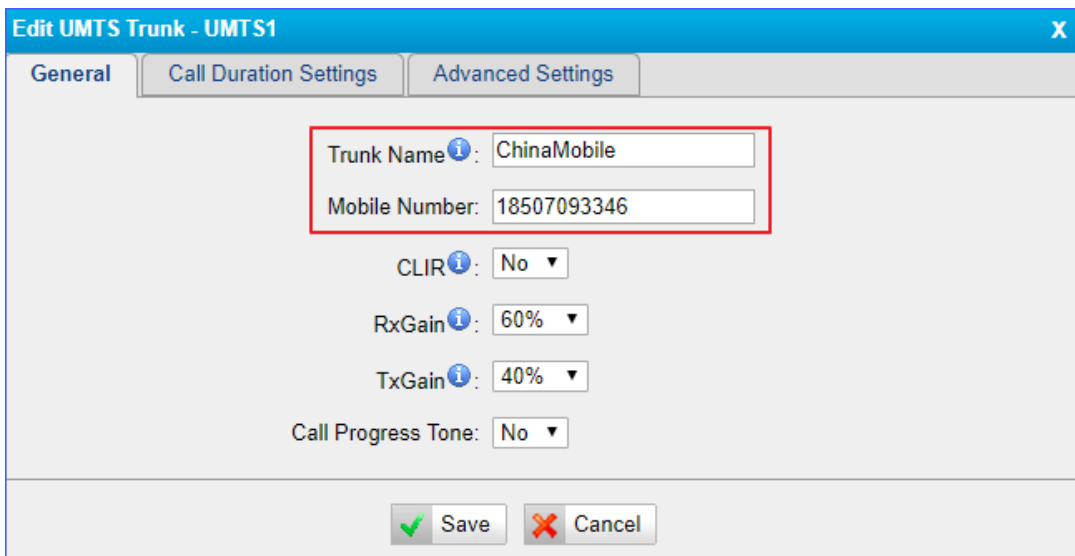
- Configure Mobile Module Profile
- Reboot Mobile Module
- Enable/Disable Mobile Module
- Display Caller's Mobile Number
- Adjust Mobile Module Volume
- Configure Call Progress Tone
- Configure the Call Duration of Mobile Trunk
- Configure Advanced Settings
- Unlock the SIM Card

Configure Mobile Module Profile

You can set a name to the mobile module to help you identify your module on TG100. After inserting a SIM card to a mobile 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**, and click .
2. In the **General** section, enter a name in **Trunk Name** field.
3. Enter the SIM card number in **Mobile Number** field.





Edit UMTS Trunk - UMTS1


General | Call Duration Settings | Advanced Settings

Trunk Name : ChinaMobile



Mobile Number: 18507093346

CLIR : No ▼

RxGain : 60% ▼

TxGain : 40% ▼

Call Progress Tone: No ▼

 Save  Cancel

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

Reboot Mobile Module

You can reboot the mobile module on the web interface.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, and click **Reboot**.

The module starts to reboot.

Port	Trunk Name	Type	Single Call Max Duration	Max. Call Duration(s)	Call Duration(s)	Enable/Disable	Power On/Off	Reboot Module
1	ChinaMobile	UMTS	0	0	0	Disable	Power Off	Reboot 

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

Enable/Disable Mobile Module

By default, mobile module is enabled to make outbound calls. If you don't want to allow the mobile module to make outbound calls, you can disable the module.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, select the module, and click the **Enable**.

Port	Trunk Name	Type	Single Call Max Duration	Max. Call Duration(s)	Call Duration(s)	Enable/Disable	Power On/Off	Reboot Module
1	UMTS1	UMTS	0	0	0	Enable	Power Off	Reboot

- **Disable**: You can make outbound calls through the mobile module.
- **Enable**: You can not make outbound calls through the mobile module.


Display Caller's Mobile Number

If you don't want to display your mobile number on callee's phone, you can enable CLIR feature. By default, CLIR is disabled.

Note:

Contact the SIM carrier to confirm if CLIR feature is supported in advance.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, and click .
2. On the **General** section, select **Yes** or **No** from the drop-down list of CLIR.

Edit UMTS Trunk - UMTS1

General | Call Duration Settings | Advanced Settings

Trunk Name ⓘ: UMTS1

Mobile Number:

CLIR ⓘ: No ▾

RxGain ⓘ: 60% ▾

TxGain ⓘ: 40% ▾


Call Progress Tone: No ▾

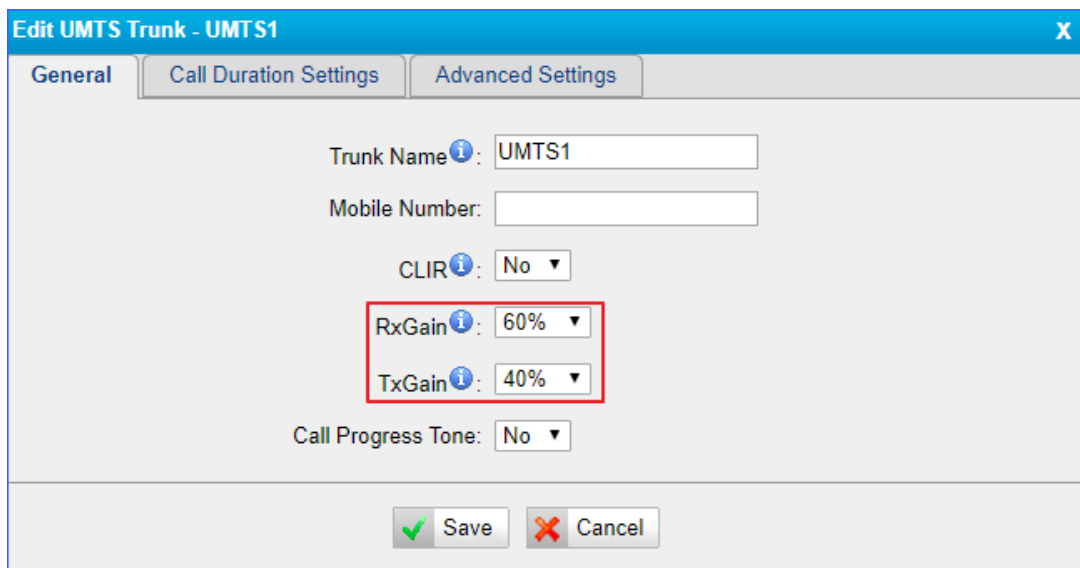
Save Cancel

Adjust Mobile Module Volume

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

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, and click .
2. On the **General** section, change the **RxGain** and **TxGain**.
 - RxGain: The received volume of the module.
 - TxGain: The transmitting volume of the module.



Edit UMTS Trunk - UMTS1

General | Call Duration Settings | Advanced Settings

Trunk Name ⓘ: UMTS1

Mobile Number:

CLIR ⓘ: No ▾

RxGain ⓘ: 60% ▾

TxGain ⓘ: 40% ▾

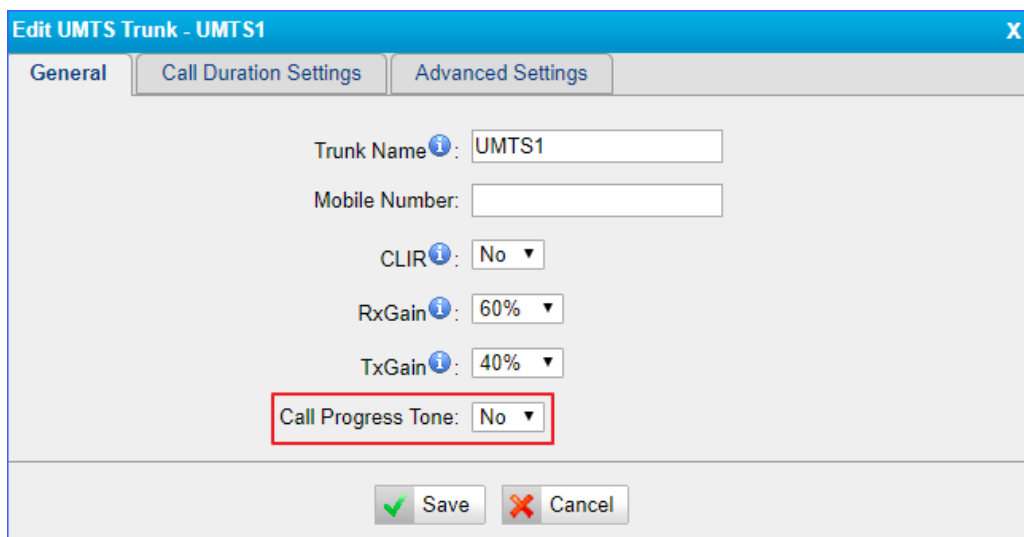
Call Progress Tone: No ▾

Save Cancel

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

Configure Call Progress Tone

When dialing from SIP to GSM/3G, during the trying period at SIM carrier side, it's completely silent in SIP side. You can enable Call Progress Tone to get a virtual ring back tone.



Edit UMTS Trunk - UMTS1

General | Call Duration Settings | Advanced Settings

Trunk Name ⓘ: UMTS1

Mobile Number:

CLIR ⓘ: No ▾


RxGain ⓘ: 60% ▾

TxGain ⓘ: 40% ▾

Call Progress Tone: No ▾

Save Cancel

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, and click .
2. On the **General** section, select **Yes** or **No** from the drop-down list of **Call Progress Tone**.

Configure the Call Duration of Mobile Trunk

You can limit call duration for each call of the 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 on the SIM card earlier.

Set a Single Call Duration of Mobile Trunk

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


Procedure

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

Set a Monthly Talk Plan of Mobile Trunk

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

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, and click .
2. Click the **Call Duration Settings** tab.

3. Set the value of **Round up duration**.
4. Set the value of **Max. Call 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 regularly.
 - a. Set **Enable Clear Stat** to **Yes**.
 - b. Set **Clear Period** to **Day**, **Week** or **Month**.
 - c. Set the **Clear Period Time**.
6. Click **Save** and **Apply Changes**.


The screenshot shows the 'Call Duration Settings' tab. It contains the following fields:

- Single Call Max Duration: 0 min
- Round up duration: 60 s
- Max. Call Duration: 0 s
- Enable Clear Stat: Yes (dropdown)
- Clear Period: Day (dropdown)
- Clear Period Time: 2019 - 12 - 30 00:00 (date and time pickers)

Set Talk Time Alarm of Mobile Trunk

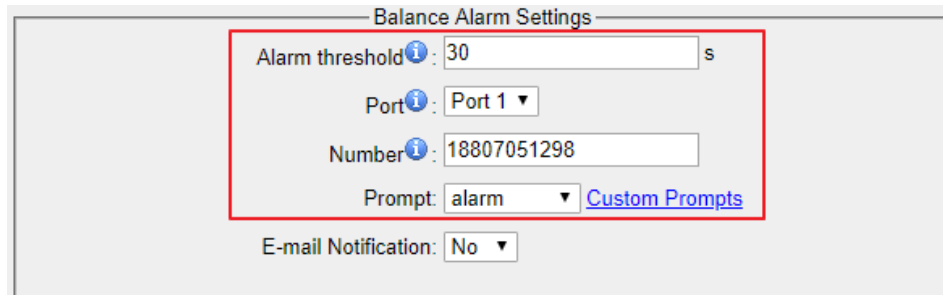
You can set alarm of talk time for the mobile trunk to remind you that the monthly talk time of the mobile trunk is running out.

Procedure

1. Navigate to **Gateway > Mobile List > Mobile List**, and click .
2. Click the **Call Duration Settings** tab.
3. Set the value of **Alarm threshold**.
4. Choose the GSM/3G Port to make alarm calls.

Note: Make sure the port is available to make calls.

5. Set the number to receive the alarm call.
6. Choose an alarm Prompt.

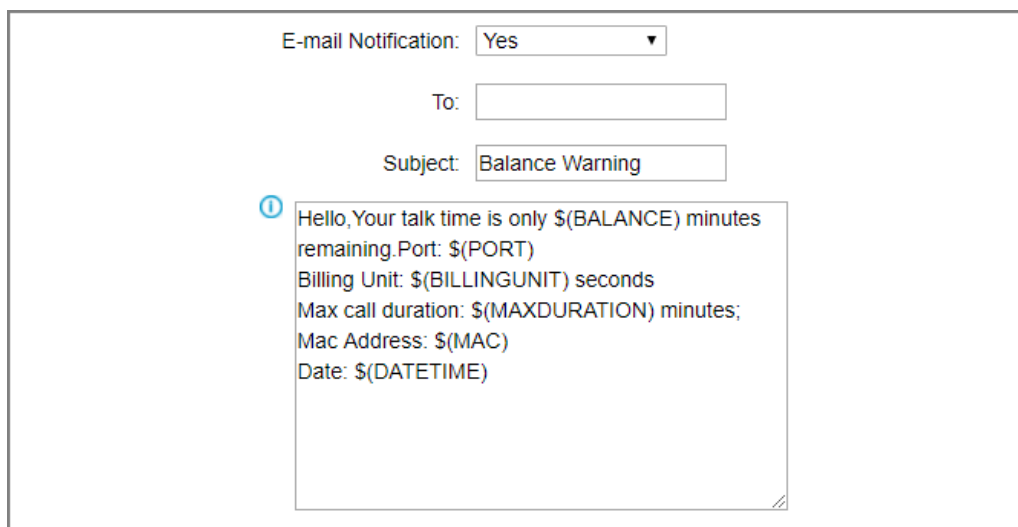


The image shows a 'Balance Alarm Settings' dialog box. A red rectangle highlights the following fields: 'Alarm threshold' (30 s), 'Port' (Port 1), 'Number' (18807051298), and 'Prompt' (alarm). Below the highlighted area is the 'E-mail Notification' field, which is set to 'No'. There is a 'Custom Prompts' link next to the 'Prompt' dropdown.

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

Note:

Make sure SMTP test is successful in “Email settings” page before configuring this feature.



The image shows an 'E-mail Notification' configuration dialog box. The 'E-mail Notification' field is set to 'Yes'. Below it are fields for 'To:' (empty) and 'Subject:' (Balance Warning). A text area contains a sample email body with variables: 'Hello, Your talk time is only \$(BALANCE) minutes remaining. Port: \$(PORT) Billing Unit: \$(BILLINGUNIT) seconds Max call duration: \$(MAXDURATION) minutes; Mac Address: \$(MAC) Date: \$(DATETIME)'.

8. Click **Save** and **Apply Changes**.

Configure Advanced Settings

You can configure advanced settings of the mobile trunk.


Option	Description
IMEI	International Mobile Equipment Identity of this module, it's unchangeable.
IMSI	International Mobile Subscriber Identification of SIM card, it's unchangeable.
SMS Center	The SMS center of this SIM card, TG100 will generate this by default. You can also input the number here for the carrier if it's not the default one.
Carrier	The carrier is connected by default. You can also choose manual mode if this SIM card is supported by several carriers.
Band	The band of this SIM card, you can choose PGSM900, DCS1800, PCS1900, EGSM900/DCS1800, GSM850/PCS1900.

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**, and 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**.

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 to use the same account number and password to register VoIP trunk on your PBX.
 - e. (Optional) Click **Advanced** tab, and configure the advanced settings.

Option	Description
NAT	Network address translation (NAT) is a method of translating the private (not globally unique) address in Internet Protocol (IP) into legal address. NAT is used to limit the number of public IP addresses for security purpose.
Enable SRTP	Secure Real-time Transport Protocol, if it's enabled, the same setting should be enabled on IP phone side.
Qualify	Send check alive packets to IP phones, when it's disabled, TG100 will ignore the reachability and the status of this account will be out of monitoring.
Transport	This will be the transport method used by the account trunk. <ul style="list-style-type: none"> • UDP (default) • TCP • TLS
DTMF Mode	RFC2833, Info, Inband, Auto.
Enable IP Restriction	If this option is enabled, only the allowed IP addresses can register the account number. In this way, VoIP security can be enhanced.

f. Click **Save** and **Apply Changes**.

Add New Account

General Advanced

Trunk Type: Account

Type: SIP

Name: 1000


Account: 1000

Password: UUSccknd1988

Save Cancel

2. Use the VoIP account to register a VoIP trunk on your PBX.
3. Go to **Status > System Status > Trunk Status** to check the account status on

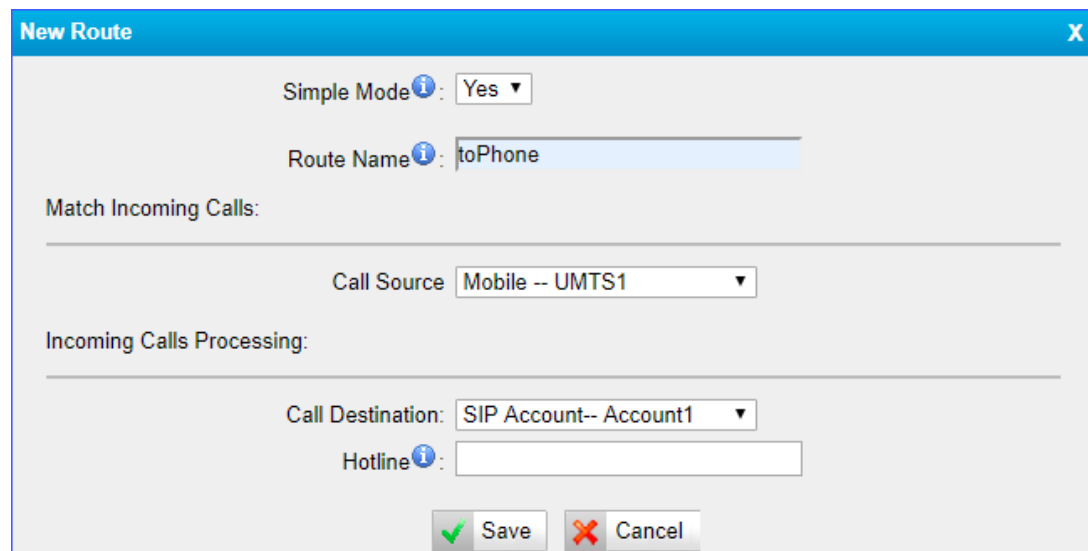
TG gateway.

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 the GSM/3G trunk from **Call Source** field.
5. Choose a SIP account or a trunk group from the **Call Destination** field.



New Route

Simple Mode: Yes

Route Name: toPhone

Match Incoming Calls:

Call Source: Mobile -- UMTS1

Incoming Calls Processing:

Call Destination: SIP Account-- Account1

Hotline:

Save Cancel

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 need a two-stage dial to reach the destination number.

- a. Set **Simple Mode** to **No**.
- b. Set **Two Stage Dial** to **Yes**.

New Route [X]

Simple Mode ⓘ: Yes ▾

Route Name ⓘ: test

Match Incoming Calls:

Call Source: Mobile -- UMTS1 ▾

Incoming Calls Processing:

Call Destination: SIP Account-- Account1 ▾

Hotline ⓘ: 1000

[✓] Save [✗] Cancel

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

When a call reaches the selected GSM/3G 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 or a trunk group from **Call Source** field.
5. Choose the GSM/3G trunk from the **Call Destination** field.

New Route [X]

Simple Mode ⓘ: Yes ▾

Route Name ⓘ: FromS100

Match Incoming Calls:

Call Source: SIP Account-- Account1 ▾

Incoming Calls Processing:

Call Destination: Mobile -- UMTS1 ▾

Hotline:

[✓] Save [✗] Cancel

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

A PBX user can make a call through the selected GSM/3G 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 TG100 web 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 as the PBX extension's protocol.
 - d. Set a **Provider Name**.
 - e. Enter the PBX's IP address or domain in **Hostname/IP** or **Domain** field.
 - 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 to configure the advanced settings.

Option	Description
From User	All outgoing calls from this SIP Trunk will use the From User in From Header of the SIP Invite package. Leave this field blank if not needed.
Online Number	Define the online number for “Skype Connect” and some other SIP service providers. Leave this field blank if not needed.
Maximum Channels	Control the maximum number of simultaneous calls, set as 0 to specify no limit.
Caller ID	Specify the caller ID to use when making outbound calls over this trunk.
Enable SRTP	Define if SRTP is enabled for this trunk, it depends on provider’s configuration.
Qualify	Send check alive packets to the SIP provider.
Enable outbound proxy server	A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI.
Codec	Define the codec for this SIP trunk and its priority.
Transport	<p>This will be the transport method used by the SIP Trunk. This method is given by the SIP trunk provider.</p> <ul style="list-style-type: none"> • UDP • TCP • TLS
DTMF Mode	Set default mode for sending DTMF of this trunk. The default value is rfc2833.
DOD settings	<p>DOD (Direct Outward Dialing) means the caller ID displayed when dialing out.</p> <p>Note: Make sure provider supports this feature before configuring the setting.</p>

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

Add New Trunk

General Advanced

Trunk Type: Trunk

Type: SIP

Provider Name:

Hostname/IP: :5060

Domain:

User Name:

Authorization Name:

Password:

Save Cancel

4. Check the trunk status on TG gateway, go to **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 the GSM/3G trunk from **Call Source** field.
5. Choose a register SIP trunk or a trunk group 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 need a two-stage dial to reach the destination number.

- a. Set **Simple Mode** to **No**.
- b. Set **Two Stage Dial** to **Yes**.

New Route X

Simple Mode : Yes ▾

Route Name : test

Match Incoming Calls:

Call Source Mobile -- UMTS1 ▾

Incoming Calls Processing:

Call Destination: SIP Account-- Account1 ▾

Hotline : 1000

Save Cancel

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

When a call reaches the selected GSM/3G 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 or a trunk group from **Call Source** field.
5. Choose a GSM/3G trunk from **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**.
8. When a PBX user makes a call through the selected GSM/3G 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 TG100 web 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 as your PBX trunk's protocol.
 - d. Set a **Provider Name**.
 - e. Enter the PBX's IP address in **Hostname/IP** field.
 - f. (Optional) Click **Advanced** tab, and configure the advanced settings.

Option	Description
Qualify	Send check alive packets to the SIP provider.
Maximum Channels	Controls the maximum number of simultaneous calls, set 0 to specify no limit
Codec	Define the codec for this SIP trunk and its priority.
Transport	<p>This will be the transport method used by the SIP Trunk. This method is given by the SIP trunk provider.</p> <ul style="list-style-type: none"> ● UDP ● TCP ● TLS
DTMF Mode	Set default mode for sending DTMF of this trunk. The default setting is rfc2833.
DOD settings	<p>DOD (Direct Outward Dialing) means the caller ID displayed when dialing out.</p> <p>Note: Make sure provider supports this feature before</p>

	configuring the setting.
--	--------------------------

g. Click **Save** and **Apply Changes**.

The screenshot shows a window titled "Add Service Provider" with a close button (X) in the top right corner. It has two tabs: "General" and "Advanced". The "General" tab is active. Inside the tab, there are four fields: "Trunk Type" with a dropdown menu showing "Service Provider", "Type" with a dropdown menu showing "SIP", "Provider Name" with an empty text box, and "Hostname/IP" with an empty text box followed by a port field containing "5060". At the bottom of the window are two buttons: "Save" with a green checkmark icon and "Cancel" with a red X icon.

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 indicates 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 the GSM/3G trunk from **Call Source** field.
 5. Choose a service provider trunk or a trunk group 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 need a two-stage dial to reach the destination number.
- a. Set **Simple Mode** to **No**.
 - b. Set **Two Stage Dial** to **Yes**.

New Route

Simple Mode: No

Route Name:

Match Incoming Calls:

Call Source: SIP Account-- Account1

Inbound Caller Pattern:

DID Number:

DID Associated Number:

Enable Callback: No [Callback Settings](#)

Incoming Calls Processing:

Call Destination: Mobile -- UMTS1

Hotline:

Two Stage Dial: Yes

Outbound Dial Pattern:

Strip: 0

Prepend these digits before dialing:

Save Cancel

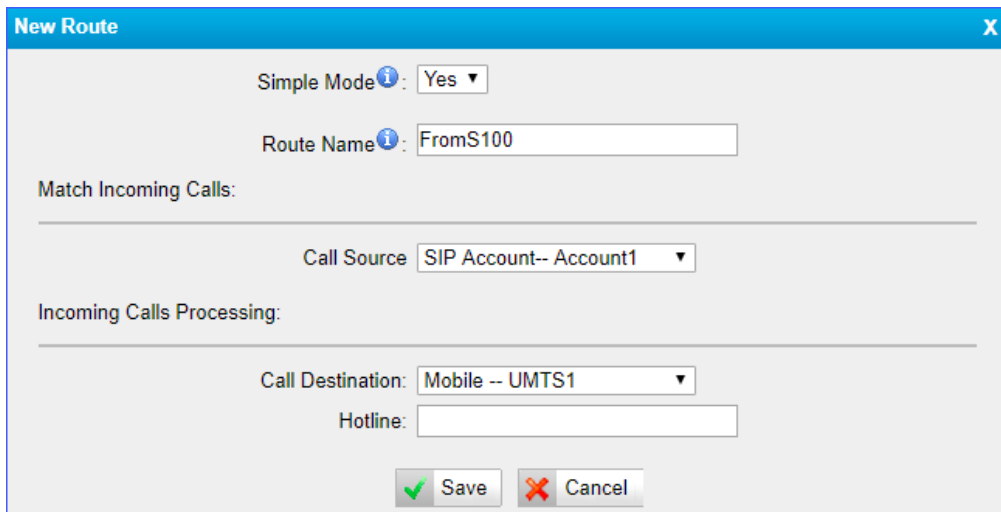
7. Click **Save** and **Apply Changes**.

When a call reaches the selected GSM/3G 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 or a trunk group from **Call Source** field.
5. Choose the GSM/3G trunk from **Call Destination** field.



New Route [X]

Simple Mode ⓘ: Yes ▾

Route Name ⓘ: FromS100

Match Incoming Calls:

Call Source: SIP Account-- Account1 ▾

Incoming Calls Processing:

Call Destination: Mobile -- UMTS1 ▾

Hotline:

[✓] Save [✗] Cancel

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

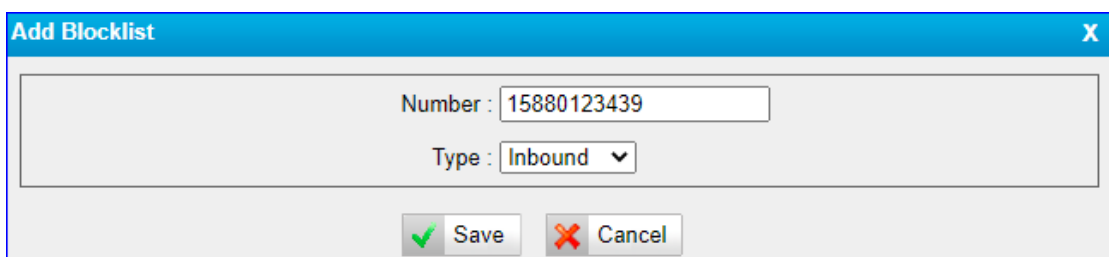
A PBX user can make a call through the selected GSM/3G trunk.

Block Incoming Numbers

You can block the incoming calls from TG gateway to your PBX. When the blocked user calls to the GSM/3G trunk on TG gateway, the system will block the call.

Procedure

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



Add Blocklist [X]

Number: 15880123439

Type: Inbound ▾

[✓] Save [✗] Cancel

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

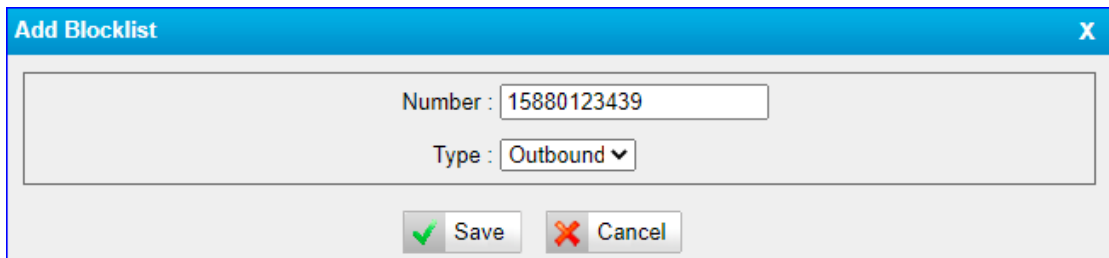
When the number 15880123439 reaches the TG gateway, the call will fail.

Block Outgoing Numbers

You can limit users to call specific numbers through GSM/3G trunk on TG gateway. When users try to call the blocked numbers, the call will fail.

Procedure

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



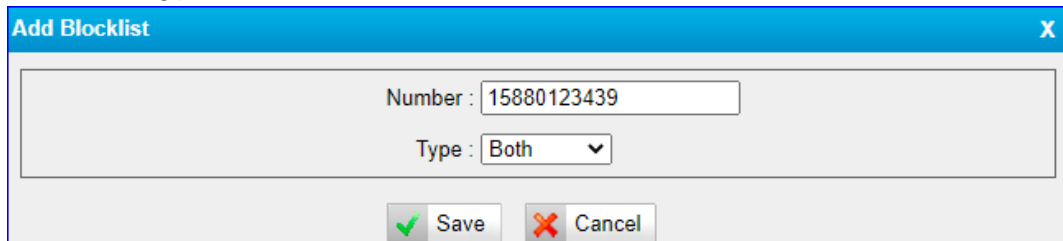
5. Click **Save** and **Apply Changes**.
When PBX user tries to call the number 15880123439 through TG gateway, the call will fail.

Block both Incoming and Outgoing Numbers

You can add a number to the Blocklist. The Blocklisted user can not place calls from TA gateway to your PBX, and extension users on PBX can not place calls to the Blocklisted user through GSM/3G trunk on TG gateway.

Procedure

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



5. Click **Save** and **Apply Changes**.
When PBX user tries to call the number 15880123439 through TG gateway, the call will fail. When the number 15880123439 reaches the TG gateway, the call will also fail.

Callback

Callback feature allows callers to hang up and get called back to TG gateway. Callback feature can reduce the cost for 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. You need to enable Callback on the “Mobile to IP” or “IP to Mobile” setting panel.

Note:

No callback rule is needed if the trunk supports call back with the caller ID directly.

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.
 - a. Set **Simple Mode** to **No**.
 - b. On the **Match Incoming Calls** section, set **Enable Callback** to **Yes**.

Edit Route [X]

Simple Mode ⓘ: No ▼

Route Name ⓘ: default

Match Incoming Calls:

Call Source SIP Account-- Account1 ▼

Inbound Caller Pattern ⓘ:

DID Number ⓘ:

DID Associated Number ⓘ:

Enable Callback: Yes ▼ [Callback Settings](#)

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

Set up Callback for All Numbers

You can enable callback feature for all numbers. When anyone 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. Select 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.
 - a. Set **Simple Mode** to **No**.
 - b. On the **Match Incoming Calls** section, set **Enable Callback** to **Yes**.

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

Add Callback Rules

A callback rule will help you manipulate the numbers to call back from TG gateway. For some GSM/3G carriers, you need to add 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. Select the trunk will be used to call back.
4. Set the callback rule.
 - **Strip:** Define how many digits will be stripped from the front of the callback number before the call is placed.

- **Prepend:** Define how many digits will be added in front of the callback number before the call is placed.

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

AutoCLIP Route

Yeastar TG gateway can automatically record failed outgoing calls 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 **Keep Time**. The system will keep the AutoCLIP records for the configured time.
4. 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. Next time 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 **Delete The Selected**.

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 card on Yeastar TG gateway web 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 “,”.
You can also click **Add Contacts** to add phone numbers to the **Destination** field.
4. Select the GSM/3G port, the system will send SMS messages through the selected port.
5. Enter the message contents in the **Content** field. The max characters is 300. If contents length is longer than 300, the SMS will be cut into 2 pieces at provider side.

6. Click **Send**.

The screenshot shows a web interface titled "General Settings". It contains the following elements:

- Country Code**: A dropdown menu with "China +86" selected.
- Destination**: An empty text input field.
- Select Port**: A dropdown menu.
- Content**: A large text area for entering the message content.
- Add Contacts**: A button with a green plus icon.
- Send**: A button with a green checkmark icon.
- A character count "0/300" is visible at the bottom right of the content area.

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 quick selection 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. You can click **Customized** and enter group name.
Note: Special characters like space are not allowed, you can enter “_” instead.
4. Click **Save** and **Apply Changes**.

Delete an SMS Contact

Procedure

1. Navigate to **SMS > SMS > SMS Contacts**.
2. Select 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 to find your desired SMS message, then check the status.
 - **Successful:** The SMS message is sent successfully.
 - **Failed:** Failed to send SMS message.
 - **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 GSM/3G 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 appear on the page.

Download Searched Results

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

Procedure

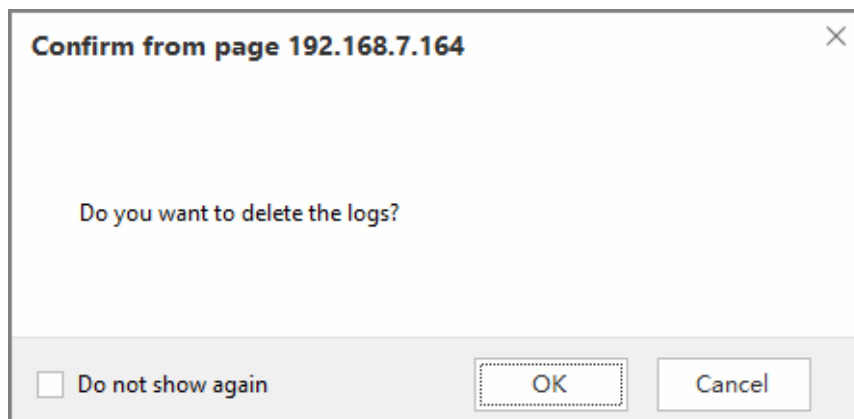
1. Navigate to **SMS > SMS > Outbox**.
2. Click **Download the messages** to download and export the searched SMS messages.

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

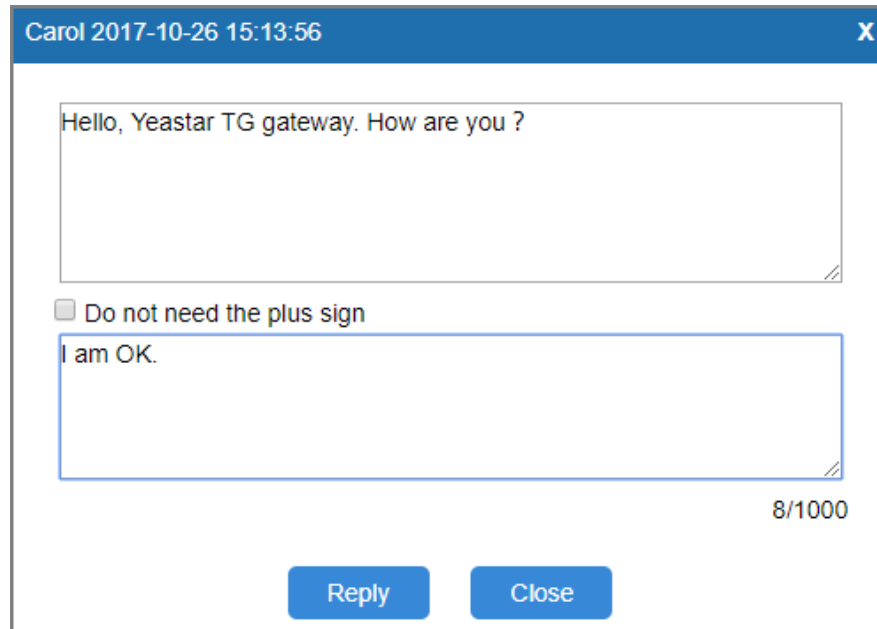
1. Navigate to **SMS > SMS > Inbox**.
2. Choose the desired record, click  to view the detailed messages.

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) Select the checkbox of **Do not need the plus sign** if the destination number doesn't need it.
5. Click **Reply**.



Carol 2017-10-26 15:13:56

Hello, Yeastar TG gateway. How are you ?

☐ Do not need the plus sign

I am OK.

8/1000

Reply Close

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:** Users send SMS messages to which GSM/3G/4G 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

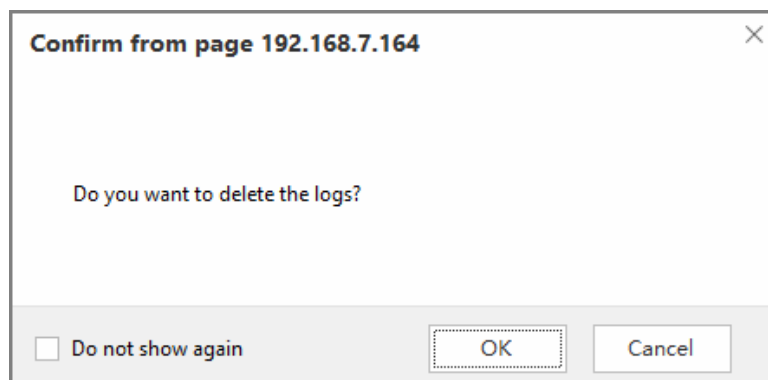
1. Navigate to **SMS > SMS > Inbox**.
2. Click **Download the messages** to download and export the searched SMS messages.

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. Enter the email address in the **Email Address** field.
3. Enter the email password in the **Password** field.

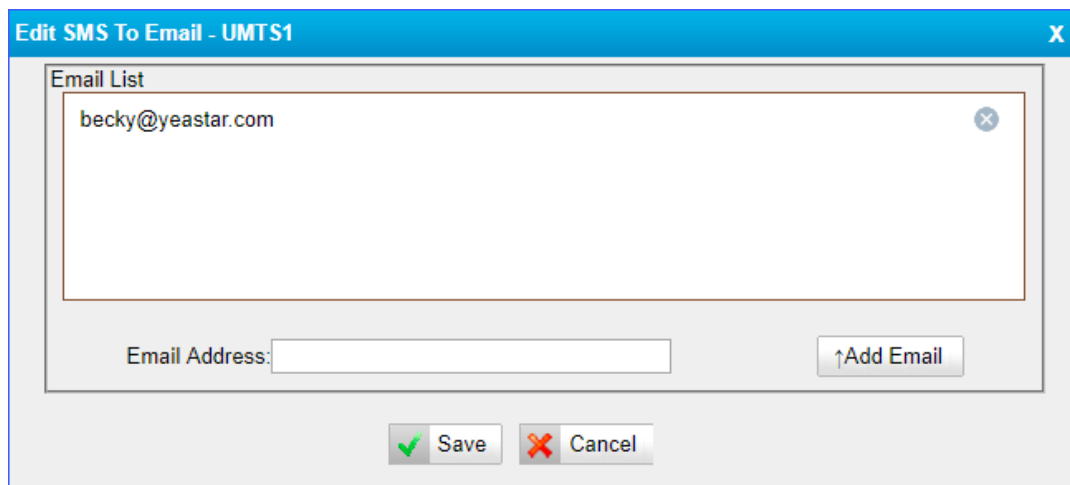
4. Enter the **Receive Server (POP3)** and **Receive Server Port**.
5. Click **Test POP3 Settings** to test if the email settings are correct.
If the web page prompts "Tested successfully", the email settings are correct.
6. Click **Save** and **Apply Changes**.

Configure SMS to Email Settings

Procedure

1. Navigate to **SMS > SMS Settings > Email Settings**.
2. Select the GSM/3G trunk, click  to edit it.
3. Enter an email address, click **Add Email**.

The system will deliver the SMS messages to the added email address.



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 address.

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

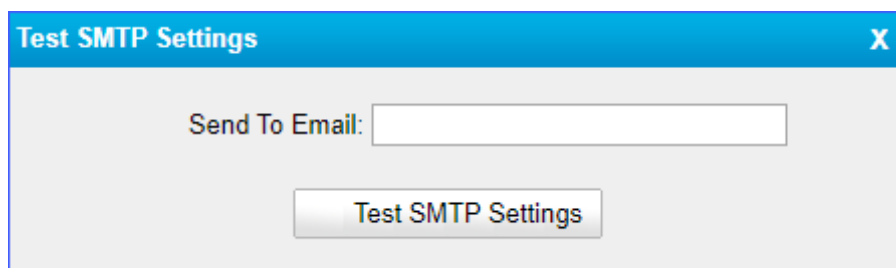
1. Navigate to **SMS > SMS Settings > Email Settings**.
2. Enter a valid email address in the **Email Address** field.
3. Enter the email password in the **Password** field.
4. Enter the **SMTP Server** and **SMTP Server Port** of the email.
5. **(Optional)** Enable SSL/TLS if the email server needs 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 SMTP 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 > Email Settings**.
2. Select the checkbox of **Enable Email To SMS**.
3. **(Optional)** Configure the following settings in the section of **Enable Email to SMS**.
 - **Enable Country Code**: Enable the option if you want to add the country code before the destination phone number, and select a country code from **Country Code**.
 - **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 an email to SMS, you need to send an email to the SMS email address of TG gateway. The system will receive and forward the email to the GSM/3G port, so that the email can be sent 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 no port is specified, the TG gateway will send the SMS by the first available GSM/3G port.

Example: port:3;

- **num:[number]**: Required setting. Enter the destination number.

Example: num:15882025100;

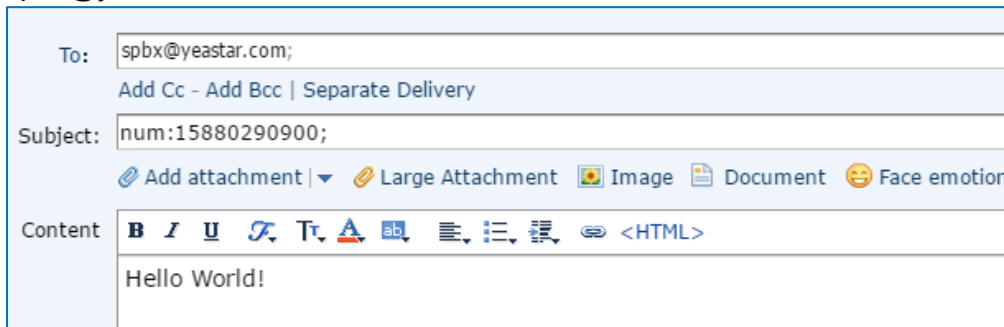
- **code:[code]**: Optional Setting. If you set an access code of Email To SMS, enter the same PIN code in the email subject.

Example: code:125485;

Procedure

1. Log in your email account, and write 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.



The screenshot shows an email composition interface. The 'To' field contains 'spbx@yeastar.com;'. Below it is a link 'Add Cc - Add Bcc | Separate Delivery'. The 'Subject' field contains 'num:15880290900;'. Below the subject field are links for 'Add attachment', 'Large Attachment', 'Image', 'Document', and 'Face emotion'. The 'Content' field has a rich text editor toolbar with icons for bold, italic, underline, link, unlink, text color, background color, bulleted list, numbered list, indent, outdent, and a '<HTML>' link. The text 'Hello World!' is entered in the content field.

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. Set **SMS Clear Enabled** to **Yes**.
 - b. (Optional) Set the **Start Date** and **End Date**. The system will clear the messages periodically during this period.
 - c. Select message **Status**. The system will delete messages of the selected status.
 - d. Set the clear period and clear time.

Outbox	
SMS Clear Enabled:	No
Start Date:	
End Date:	
Status:	All
Clear Period:	Day
Clear Period Time:	2019 - 12 - 25 00 : 00

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

Send USSD Messages

Unstructured Supplementary Service Data (USSD) is sometimes referred to "Quick Codes" or "Feature codes". You can send USSD messages to subscribe services from the GSM/3G carriers.

Send a USSD Message

You can select the GSM/3G port, and send USSD messages to the GSM/3G carrier.

Procedure

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

	Port	USSD Request	USSD Response
<input type="checkbox"/>	3	JQ1457	

Exit USSD Sessions

When you want to subscribe a new service from the GSM/3G carrier, you need to exit the former USSD sessions first.

Procedure

1. Navigate to **SMS > SMS > USSD**.
2. Selected the port.
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

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

Change Password	
Enter Old Password:	<input type="password"/>
Enter New Password:	<input type="password"/>
Retype New Password:	<input type="password"/>

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
- Reset the System

Change Web Login Password

It is highly recommended that you change the system 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 Password	
Enter Old Password:	<input type="password"/>
Enter New Password:	<input type="password"/>
Retype New Password:	<input type="password"/>

Change Date and Time

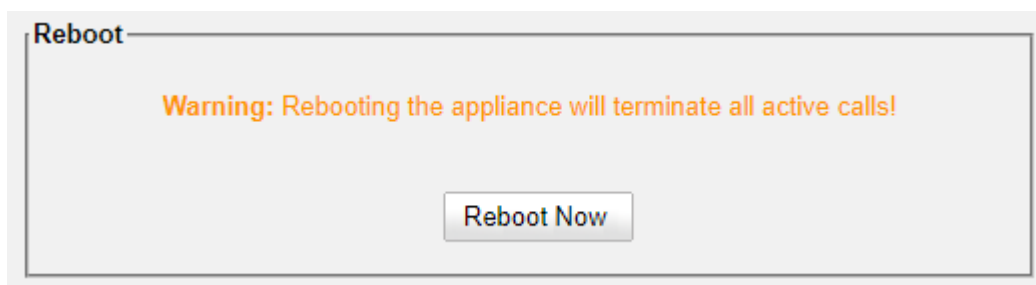
You can adjust the time of TG gateway (including the time zone) to make it consistent with your local time.

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. Select **Automatically Synchronize With An Internet Time Server**, and enter the **NTP Server address**. The system will adjust its internal clock to a central network server.

Note: Make sure the system can access the Internet.

5. You can also select **Set Date & Time Manually** and enter the date and time.
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

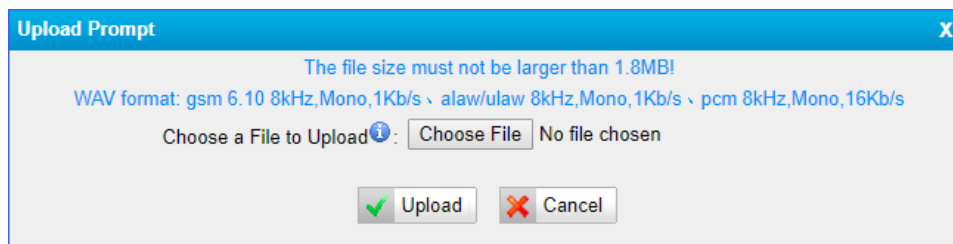
Yeastar TG gateway supports “.WAV”, “.wav”, and “.gsm” audio file. The audio file size must be smaller than 1.8 MB. The supported wav file format:

- pcm 8kHz, 16bit, Mono, 16Kb/s
- alaw/ulaw 8kHz, Mono, 1Kb/s
- gsm 6.10 8kHz, Mono, 1Kb/s

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 uploading 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.

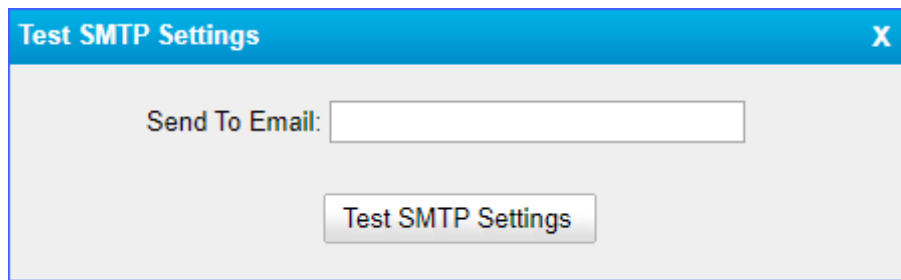
Procedure

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 to 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 SMTP 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.

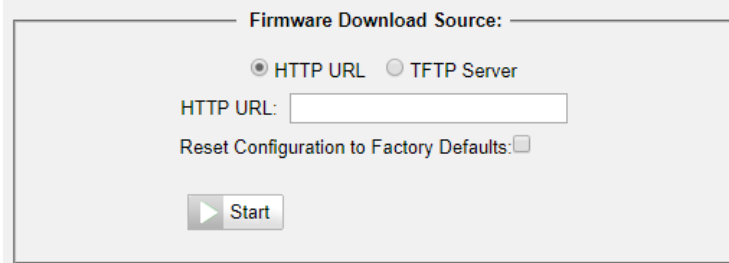
Procedure

1. Navigate to **System > System Preferences > Firmware Update**.
2. Select **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) Select 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.

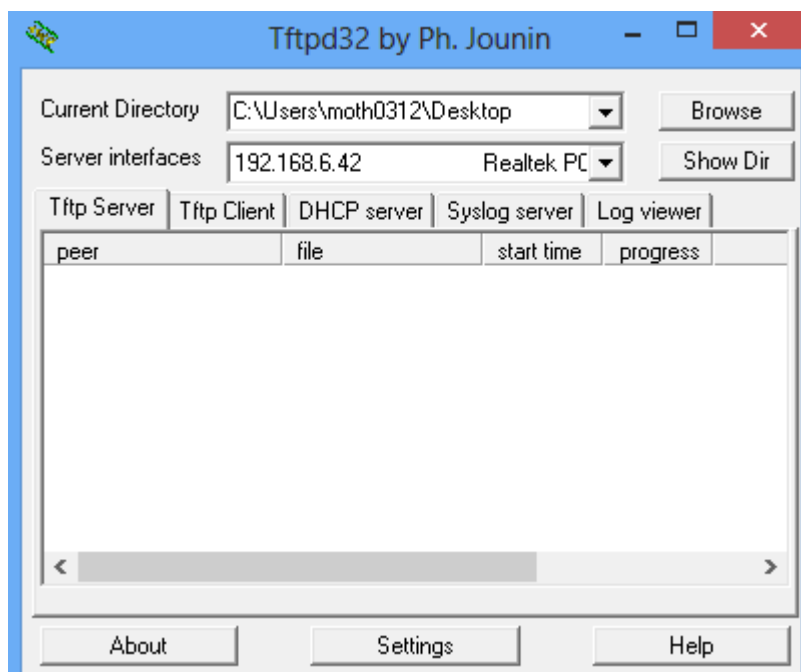


The dialog box is titled "Firmware Download Source:". It contains two radio buttons: "HTTP URL" (selected) and "TFTP Server". Below the radio buttons is a text input field labeled "HTTP URL:". Below the input field is a checkbox labeled "Reset Configuration to Factory Defaults:". At the bottom of the dialog is a "Start" button with a play icon.

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.



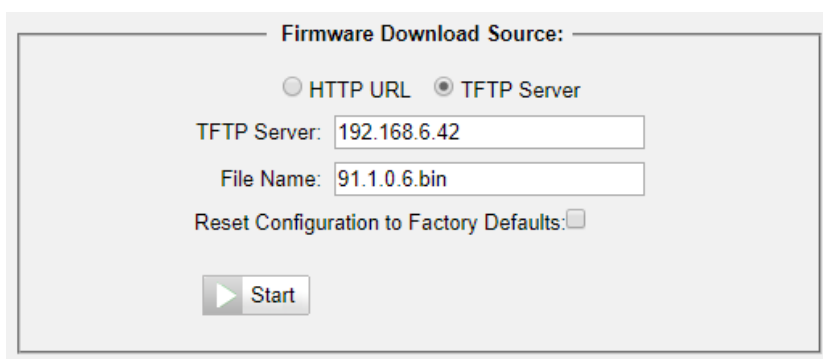
2. Log in TG gateway, navigate to **System > System Preferences > Firmware Update**.

3. Select TFTP Server.
4. Enter the IP address of the TFTP server in **TFTP Server** field.
5. Enter the firmware name 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.



The image shows a software window titled "Firmware Download Source:". Inside the window, there are two radio buttons: "HTTP URL" and "TFTP Server". The "TFTP Server" radio button is selected. Below the radio buttons, there are two text input fields. The first field is labeled "TFTP Server:" and contains the IP address "192.168.6.42". The second field is labeled "File Name:" and contains the filename "91.1.0.6.bin". Below these fields, there is a checkbox labeled "Reset Configuration to Factory Defaults:" which is currently unchecked. At the bottom of the window, there is a button with a play icon and the text "Start".

Backup and Restore

Before resetting TG100 to factory defaults, you can backup up the configurations and restore it using this package.

Note:

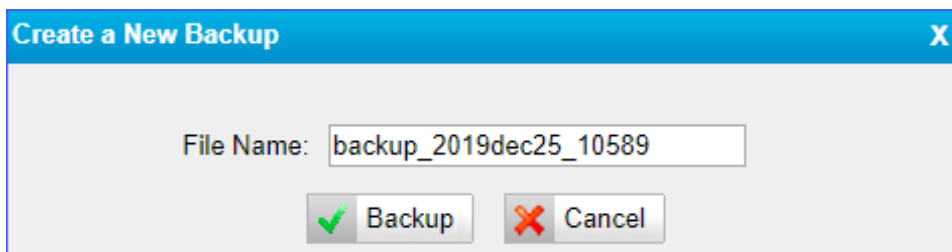
- Only configurations and custom prompts can be backed up.
- When you have updated the firmware version, it's not recommended to restore the old package.

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 **Backup**, 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.

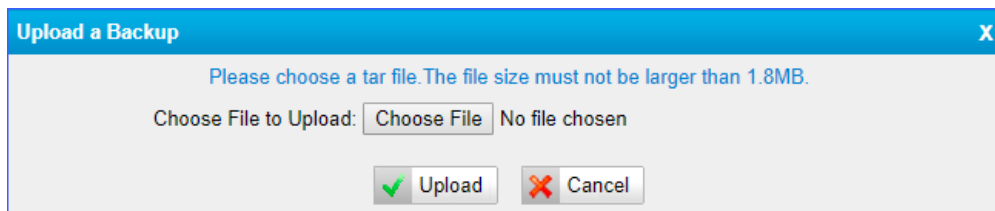
Prerequisite

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.

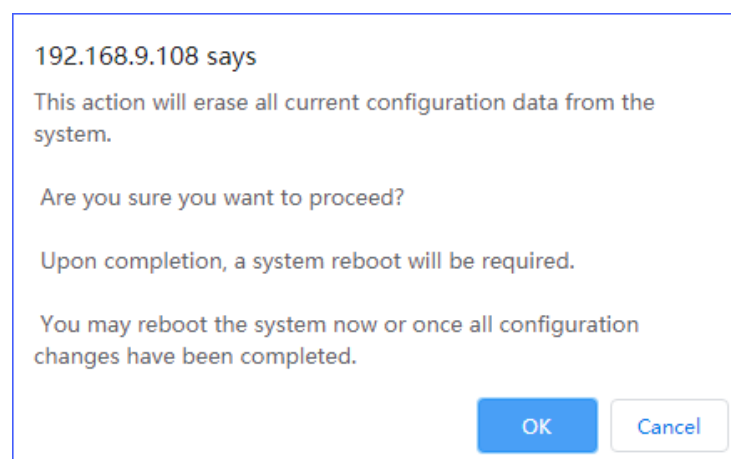


3. Click **Choose File**, and choose a .tar file from your local PC.
4. Click **Upload**.

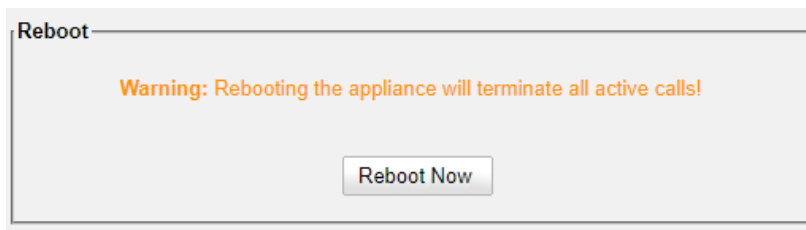
Restore System Configurations

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.



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



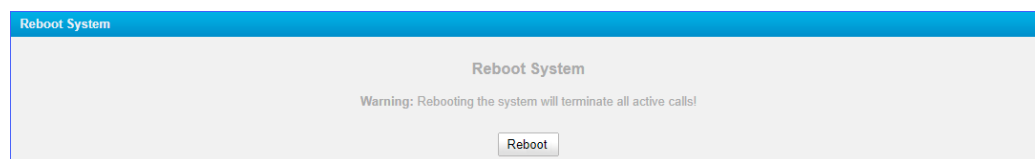
Reboot the System

You can reboot the system on Web interface.

Procedure

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

The system starts to reboot immediately.



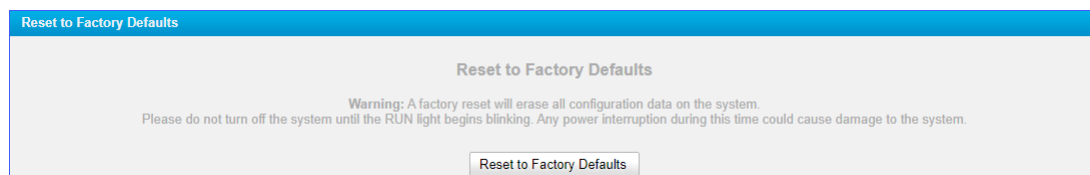
Reset the System

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 interface for the first time with the factory IP address, you can change the network of TG gateway according to your local network.

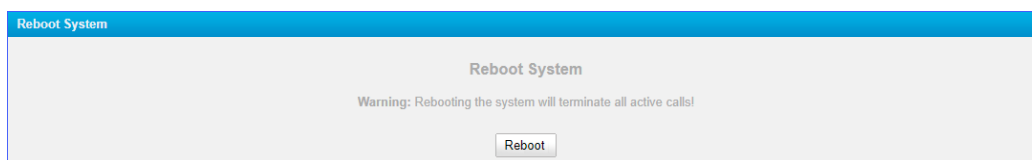
Procedure

1. Navigate to **System > Network Preferences > LAN Settings**.
2. Configure LAN settings.

Option	Description
DHCP	If this option is set to yes, TG100 will act as DHCP client to get an available IP address from your local network. Note: We recommend you to disable DHCP as you need a static IP address to establish steady connection with TG100.
Enable SSH	This is the advanced way to access the device. You can use the software Putty to access the device. In the SSH access, you can do more advanced settings and debug. It's disabled by default. Note: We recommend you to disable this option if not needed.
Port	The default is 8022; you can change it to another one.
Enable FTP	With FTP service, you can connect to TG100 via web browser.
Port	The default is 21; you can change it to another one.
IP Address	Set the IP Address for TG100.

Subnet Mask	Set the subnet mask for TG100.
Gateway	Set the gateway for TG100.
Primary DNS	Set the primary DNS for TG100.
Secondary DNS	Set the secondary DNS for TG100.
IP Address2	Set the second IP Address for TG100.
Subnet Mask2	Set the second subnet mask for TG100.

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



4. 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

A VLAN (Virtual LAN) is a logical local area network (or LAN) that extends beyond a single traditional LAN to a group of LAN segments, given specific configurations. 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 one of the 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 TG100 acts as a VLAN client, you need to set up a 3-layer switch in your local network. Please configure the VLAN information first, then input the details in TG100, so that the packages via TG100 can be added the VLAN label before

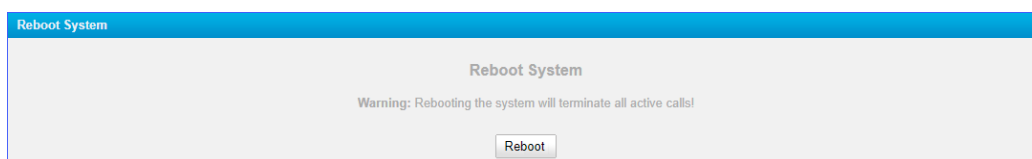
sending to that switch.

Procedure

1. Navigate to **System > Network Preferences > VLAN Settings**.
2. Select a VLAN to enable it.
3. Get the VLAN information from your network administrator and enter the VLAN information on the TG gateway.

Option	Description
NO.1	Enable this option so that you can edit the first VLAN over LAN.
VLAN Number	The VLAN Number is a unique value that you assign to each VLAN on a single device.
VLAN IP Address	Set the IP address for TG100 VLAN over LAN.
VLAN Subnet Mask	Set the subnet mask for TG100 VLAN over LAN.
Default Gateway	Set the default gateway for TG100 VLAN over LAN.
NO.2	Enable this option so that you can edit the second VLAN over LAN.
VLAN Number	The VLAN Number is a unique value that you assign to each VLAN on a single device.
VLAN IP Address	Set the IP address for TG100 VLAN over LAN.
VLAN Subnet Mask	Set the subnet mask for TG100 VLAN over LAN.
Default Gateway	Set the default gateway for TG100 VLAN over LAN.

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 allow users to share information privately between remote locations, or between a remote location and a business' home network. A VPN can provide secure information transport by authenticating users, and encrypting data to prevent unauthorized persons from reading the information transmitted. The VPN can be used to send any kind of network traffic securely. TG100 supports OpenVPN.

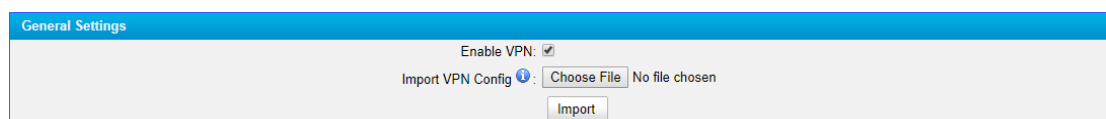
Procedure

1. Navigate to **System > Network Preferences > VPN Settings**, select the checkbox of **Enable VPN**.
2. Click **Choose file**, choose the OpenVPN configuration file from your local PC.

Note:

- Don't configure "user" and "group" in the "config" file. You can get the config package from the OpenVPN provider.
- The configuration file should be a compressed tar file.
- TG100 works as VPN client mode only.

3. Click **Import**.



The screenshot shows the 'General Settings' tab for VPN configuration. It includes a checkbox for 'Enable VPN' which is checked. Below it, there is a section for 'Import VPN Config' with a blue information icon, a 'Choose File' button, and the text 'No file chosen'. At the bottom of this section is an 'Import' button.

Set up DDNS for the TG Gateway

You can set up DDNS for the TG gateway so that users can access the TG gateway by domain name 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:

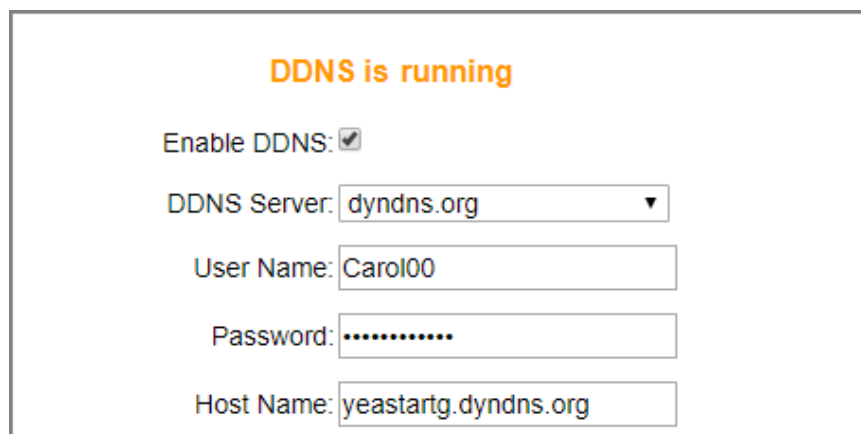
- dyndns.org
- freedns.afraid.org
- www.no-ip.com

- www.zoneedit.com

Procedure

1. Sign up a DDNS account from the supported DDNS providers.
2. Log in TG gateway web interface, navigate to **System > Network Preferences > DDNS Settings**, select 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”.



The screenshot shows a web interface for DDNS settings. At the top, it says "DDNS is running" in orange. Below that, there is a section with the following fields:

- Enable DDNS: ☒
- DDNS Server:
- User Name:
- Password:
- Host Name:

Static Route

In computer networking, a routing table is a data table stored in a router or a networked device that lists the routes to particular network destinations. In some cases, metrics (distances) is associated with those routes. The default gateway priority of TG100 from high to low is VPN/VLAN→LAN port.

Set up Static Routes

Procedure

1. Navigate to **System > Network Preferences > Static Route**.
2. Configure the static route.

- **Destination:** Enter the destination IP address or host that you want to assign a 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 by routing metric. Routing metrics are assigned to routes by routing protocols, which can be used to judge how much a route costs.

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.

Static Route Rules

Destination: 10.10.0.2 Subnet Mask: 255.255.255.255 Gateway: 192.168.7.1 Metric: LAN + Add

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

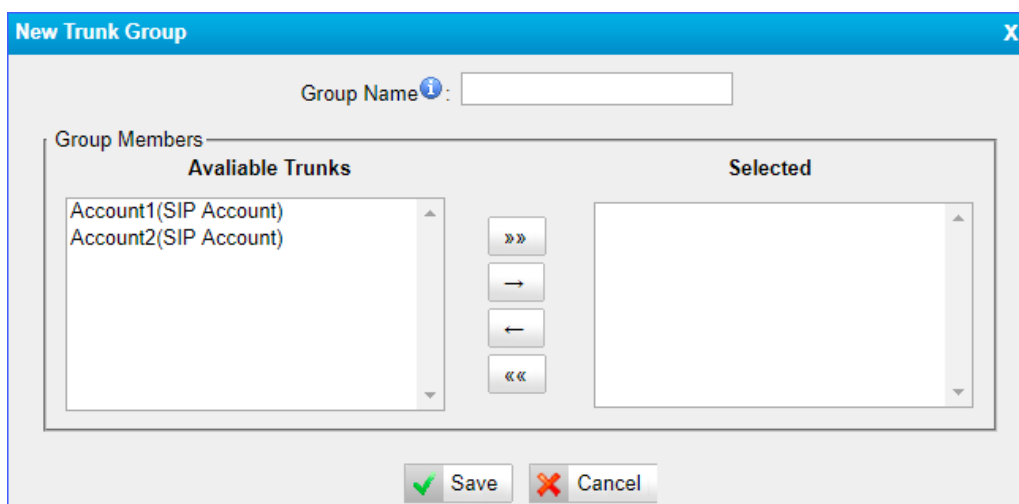
- Group VoIP Trunks
- Configure SIP Settings
- Configure IAX Settings
- Configure General Preferences

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 keep default settings 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**, 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	Whether to verify server's certificate when TG100 works as a TLS client. By default, it is set to "No".
TLS Verify Client	Whether to verify client's certificate when TG100 works as a TLS server. By default, it is set to "No".
TLS Ignore Common Name	Set this parameter to "No", then common name must be the same as IP or domain name.
TLS Client Method	Specify the protocol for outbound TLS connections when TG100 works as TLS client. <ul style="list-style-type: none"> ● tlsv1 ● sslv2 ● 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. The default value is rfc2833. <ul style="list-style-type: none"> ● rfc2833 ● Info ● Inband ● auto
Max Registration/Subscription Time	Maximum duration (in seconds) of a SIP registration. The default value is 3600.
Min Registration/Subscription Time	Minimum duration (in seconds) of a SIP registration. The default value is 60.

Default Incoming/Outgoing Registration Time	The default duration (in seconds) of incoming/outgoing registration. The default value is 120.
Register Attempts	The number of SIP REGISTER messages to send to a SIP Registrar before giving up. The default value is 0, which means no limit.
Register Timeout	Number of seconds to wait for a response from a SIP Registrar before timed out. The default value is 20.
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	Enable this option when your SIP trunk contains more than one IP address.
User Agent	To change the user agent parameter of asterisk. 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 settings on TG gateway.

Navigate to **Gateway > VoIP Settings > SIP Settings > NAT**, 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 used 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 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	<p>Alternatively, you can specify an external host, and the system will perform DNS queries periodically.</p> <p>Note: 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.</p>
External Refresh Interval	If External Host is configured, you can specify how often should TG100 perform a DNS query on this host. The value is specified in seconds.
Local Network Identification	<p>Used to identify the local network using a network number/subnet mask pair when the system is behind a NAT or firewall.</p> <p>Examples are as follows:</p> <p>“192.168.0.0/255.255.0.0”: All RFC 1918 addresses are local networks;</p> <p>“10.0.0.0/255.0.0.0”: Also RFC1918;</p> <p>“172.16.0.0/12”: Another RFC1918 with CIDR notation;</p> <p>“169.254.0.0/255.255.0.0”: Not get the IP address from DHCP server.</p> <p>Please refer to RFC1918 for more information.</p>
NAT Mode	<p>Global NAT configuration for the system.</p> <ul style="list-style-type: none"> ● 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.

	<ul style="list-style-type: none"> ● route = Use NAT but do not include rport in headers.
Allow RTP Re-invite	<p>By default, the system routes media streams from SIP endpoints through itself.</p> <p>If this option is enabled, the system will 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.</p>

Configure SIP Codec Settings

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

Note:

If you want to use codec G729A, we recommend you to buy a license key and input here.

The screenshot shows the 'Codecs' configuration page in the TG100 interface. It features two main sections: 'Available Codecs' and 'Allowed Codecs'. The 'Available Codecs' list includes SPEEX, G722, G726, ADPCM, and G729A. The 'Allowed Codecs' list includes u-law, a-law, and GSM. Between these lists are four buttons: '»»', '→', '←', and '««'. Below the lists is a text input field for 'G.729 License Key' and a note: 'Note: If you would like to use G.729, please enter your license key above.'

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 voice or other media connection will not be delayed or dropped due to interference from other traffic with lower priority.

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.

General	NAT	Codecs	QOS	Response Code	Advanced Settings
<div> <div>Tos SIP: CS3</div> <div>Cos SIP: 3</div> </div> <div> <div>Tos Audio: EF</div> <div>Cos Audio: 5</div> </div>					

Configure Response Code Settings

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

Navigate to **Gateway > VoIP Settings > SIP Settings > Response Code** to configure the response code settings.

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

General	NAT	Codecs	QOS	Response Code	Advanced Settings																								
<p>Gsm-Sip Response Code Configuration</p> <p>Enable Gsm-Sip Response Code: Yes</p> <table> <thead> <tr> <th>GSM Reason</th> <th>SIP Response Code</th> </tr> </thead> <tbody> <tr> <td>Vacant Number</td> <td>404</td> </tr> <tr> <td>Hangup Normal</td> <td>480</td> </tr> <tr> <td>User Busy</td> <td>486</td> </tr> <tr> <td>No Response</td> <td>408</td> </tr> <tr> <td>Rejected</td> <td>403</td> </tr> <tr> <td>Wireless Network Failure</td> <td>503</td> </tr> </tbody> </table> <p>Response Code Switch</p> <table> <thead> <tr> <th>Response Code</th> <th>Response Code After Switching</th> </tr> </thead> <tbody> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> </tbody> </table>						GSM Reason	SIP Response Code	Vacant Number	404	Hangup Normal	480	User Busy	486	No Response	408	Rejected	403	Wireless Network Failure	503	Response Code	Response Code After Switching								
GSM Reason	SIP Response Code																												
Vacant Number	404																												
Hangup Normal	480																												
User Busy	486																												
No Response	408																												
Rejected	403																												
Wireless Network Failure	503																												
Response Code	Response Code After Switching																												

Configure SIP Advanced Settings

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

Check the description of SIP advanced settings as below.

Option	Description
From Field	Where to get the caller ID in SIP packet.

	<ul style="list-style-type: none"> ● From ● Contact ● Remote-Party-ID
To Field	<p>Where to get the DID in SIP packet.</p> <ul style="list-style-type: none"> ● To ● Invite ● Remote-Party-ID
180 Ringing	It is set when the telecom provider needs. Usually it is not needed.
Remote Party ID	Whether send Remote-Party-ID on SIP header. By default, this option is disabled.
Allow Guest	<p>Whether to allow anonymous extension registration. The default value is No.</p> <p>Note: For security reasons, we recommend you to disable this option.</p>
Pedantic	Enable pedantic parameters. The default value is No.
Alwaysauthreject	<p>If enabled, when TG100 rejects “Register” or “Invite” packets, TG100 always responds the packets using “SIP 404 NOT FOUND”.</p> <p>Note: For security reasons, we recommend you to enable this option.</p>
OPTIONS Response 200	<p>No: TG100 will respond a “404 NOT FOUND” SIP packet when receiving an OPTION SIP packet.</p> <p>Yes: TG100 will respond a “200 OK” SIP packet when receiving an OPTION SIP packet.</p>
Session-timers	<p>Enable session-timer mode. The default value is “Accept”.</p> <p>Note: Disable this option if you find call be cut off every 15 minutes.</p>
Session-expires	The max refresh interval.
Session-minse	The min refresh interval, which can not be shorter than 90s.
Session-refresher	<p>Choose session-refresher. The default value is Uas.</p> <ul style="list-style-type: none"> ● Uas ● Uac

Configure IAX Settings

IAX is the Internal Asterisk Exchange protocol, you can connect to TG100 or register IAX trunk to another IAX server. It's supported by the asterisk-based IPPBX.

It is wise to keep the default settings 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**, configure the IAX general settings.

Check the description of IAX settings below.

Option	Description
UDP Port	Port used for IAX2 registrations. The default port is 4569.
Bandwidth	Control which codec will be used. <ul style="list-style-type: none">● Low● Medium● High
Min Registration/Subscription Time	Minimum duration (in seconds) of an IAX2 registration. The default value is 60.
Max Registration/Subscription Time	Maximum duration (in seconds) of an IAX2 registration. The default value is 1200.
Codecs	Enable the codec for IAX communication. <ul style="list-style-type: none">● u-law● a-law● GSM● SPEEX

	<ul style="list-style-type: none">● G726● ADPCM● G729A
--	--

Configure General Preferences

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

Check the description of general preferences settings below.

Option	Description
Ring Timeout	The global timeout value for extensions. By default, the value is 30.
HTTP Bind Port	Port used for HTTP sessions. The default port is 80. Note: If you change the value, please reboot to take effect.
Two Stage Dialing Prompt	Choose the customized two stage dialing prompt. By default, this option is disabled.
Echo cancellation algorithm	Choose the echo cancellation algorithm. <ul style="list-style-type: none">● oslec● aer

Secure Your Gateway

- [Security Center](#)
- [Configure Alert Settings](#)
- [Upload Certificate Files](#)
- [Configure Firewall Rules](#)

Security Center

You can check TG gateway security configurations in “Security Center” page. You can also enter the relevant security settings page rapidly.

Check descriptions of the service port as below.

Option	Description
SIP UDP Port	UDP Port used for SIP registrations. The default port is 5060.
HTTP Bind Port	Port for logging in the web interface. The default port is 80.
SIP TCP Port	TCP Port used for SIP registrations. The default port is 5060.
SIP TLS Port	TLS Port used for SIP registrations. The default port is 5061.
SSH	SSH port is used to access S-Series underlying configurations to debug the system. The default port is 8022. Note: We recommend that you disable SSH if you do not need it.
FTP	With FTP service, you can connect to PBX via web browser. The default port is 21.

Configure Alert Settings


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

Option	Description
PHONE Notification	Whether enable phone notification
Number	Set the phone number to receive alarm notifications.
Port	Choose the GSM/3G port to dial alert call.
Attempts	The attempts to dial a phone number when there is no answer.
Interval	The interval between each attempt to dial the phone number. Must be longer than 3 seconds, the default value is 60 seconds.
Prompt	Users will hear the prompt while receiving the phone notification.

Configure IP Attack Alert Settings

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


Procedure

1. Navigate to **System > Security Center > Alert Settings**, choose **IPATTACK** and click .
2. Configure the **Phone Notification Settings**.
 - a. If you want to enable phone notification, set **Phone Notification** to **Yes**.
 - b. Select the GSM/3G Port to make outbound calls.
 - c. Enter the **Number** to receive call notification. You can set up multiple extensions and outbound phone numbers. Separate phone numbers by “,”.
 - 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. You can set multiple email addresses, and separate them by “,”.
 - 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 **WEBLOGIN** and click .
2. Configure the **Phone Notification Settings**.
 - a. If you want to enable phone notification, set **Phone Notification** to **Yes**.
 - b. Select the GSM/3G **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 **System > Security Center > 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**, set **Type** to **Trusted Certificate**.
- b. Click **Choose File** 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**, set **Type** to **Gateway Certificate**.
- b. Click **Choose File** 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 being attacked.

Important: Back up the system configuration before you start configuring firewall, or you may fail 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 for the rule in the **Description** field.
4. Choose the desired **Protocol**.
5. Enter a port range in **Port** fields. The end port must be equal to or greater than start port. 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, enter 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. X means 0-9 or A-F in hex, the A-F are not case sensitive.

8. Choose the rule **Action**.

- **Accept:** Accept the access from remote hosts.
- **Drop:** Drop the access from remote hosts.
- **Ignore:** Ignore the access.

The screenshot shows a window titled "Add Firewall Rule" with a close button (X) in the top right corner. Inside the window, there are several input fields and a dropdown menu:

- Name:** A text input field.
- Description:** A larger text input area.
- Protocol:** A dropdown menu currently showing "UDP".
- Port:** Two text input fields separated by a colon.
- IP:** Two text input fields separated by a slash.
- MAC Address:** A text input field.
- Action:** A dropdown menu currently showing "Drop".

At the bottom of the window, there are two buttons: "Save" (with a green checkmark icon) and "Cancel" (with a red X icon).

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

Enable Firewall Function

Procedure

1. Navigate to **System > Security Center > Firewall Rules**, select 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**, select 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 fail to access the TG gateway.

Procedure

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

Add an IP Blocklist Rule

The rules in IP Blocklist help the system add the IP address to the Blocklist automatically if the number of the packets sent exceeds the rule you configured.

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

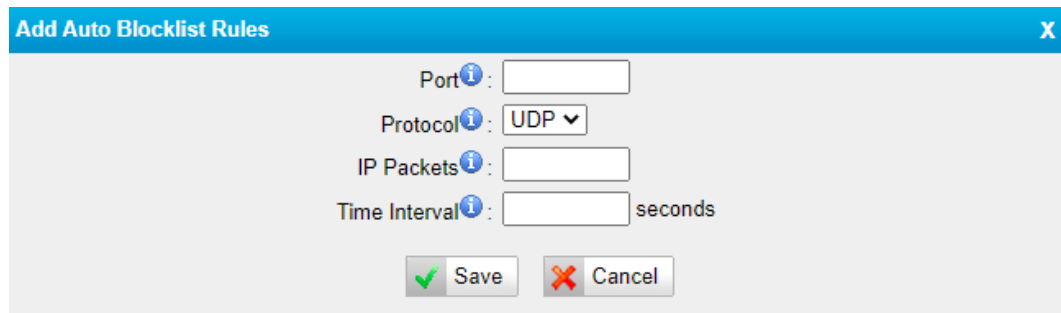
Procedure

1. Navigate to **System > Security Center > IP Blocklist**, click **Add Rule**.
2. Enter the desired port in **Port** field.
3. Choose the **Protocol** of this rule.

4. Specify the number of IP packets allowed 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, which means 90 IP packets are allowed in 60 seconds.

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




The dialog box titled "Add Auto Blocklist Rules" contains the following fields and controls:

- Port:** A text input field.
- Protocol:** A dropdown menu currently showing "UDP".
- IP Packets:** A text input field.
- Time Interval:** A text input field followed by the label "seconds".
- Buttons:** "Save" (with a green checkmark icon) and "Cancel" (with a red X icon).

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 Blocklist**.
2. Choose the desired IP address from **IP Blocklist** 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.

Trunk Status					
Port	Trunk Name	Status	Signal	Carrier	Available Duration
1	UMTS1	Failed	Unregistered Network	--	Unlimited
Status	Trunk Name	Type	User Name	Hostname/IP	Reachability
No VoIP Trunks Defined					
Status	Account		Type		
Registered	20001		SIP		
Unregistered	20002		SIP		

Mobile Trunk Status

Status	Description
Idle	The port is idle
Busy	The port is in use.
Failed	The port has not inserted the SIM Card.

Signal	Description
	No signal
	Poor
	Average
	Good
	Excellent

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.

If you VLAN or OpenVPN are configured, you can also check the status in this page.

Network Status	
LAN	
Hostname :	TG100
MAC Address :	f4:b5:49:04:0b:a0
IP Address :	192.168.9.108
Subnet Mask :	255.255.255.0
Gateway :	192.168.9.1
Primary DNS :	192.168.1.1
Secondary DNS :	

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		
General		
Product Type: TG100		
Hardware Version: V1.10 0000-0000		
Firmware Version: 51.18.0.50		
Uptime: 0:29:37 up 7:36		
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:		
flash:	Used/Total(1K-blocks) 3300/90112	use% 4%
Memory Usage		
Memory Usage:		
Mem:	Used/Total(1K-blocks) 71356/125080	use% 57%

Reports

- [Call Logs](#)
- [System Logs](#)

You can check the detailed call logs and system logs, which is used to debug.

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 > Reports > Call Logs**.
2. Set **View** value, the call log page displays the desired maximum call logs.

The screenshot shows the 'Call Logs' interface. At the top, there are search filters: Start Date (18 Oct 2017), End Date (19 Oct 2017), Caller/Callee, Trunk (All), Duration, Billing Duration, Status (All), and Communication Type (All). A 'Start Searching' button is on the right. Below the filters, there are buttons for 'Download the records' and 'Delete the records'. To the right, it says 'Total: 27' and 'Show: 1-27'. A 'View: 50' dropdown menu is highlighted with a red box. Below this is a table of 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 the trunk which 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 be greater than the value.
- **Billing Duration:** The billing duration. Enter a value to filter the call logs that have billing duration equal to or be greater than the value.
- **Status:** Choose a call status.
- **Communication Type:** Choose a communication type.

Procedure

1. Navigate to **Status > Reports > 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 Logs** page.

Download Searched Results

After searching the desired call logs, you can download and export the call logs to

a .csv file.

Procedure

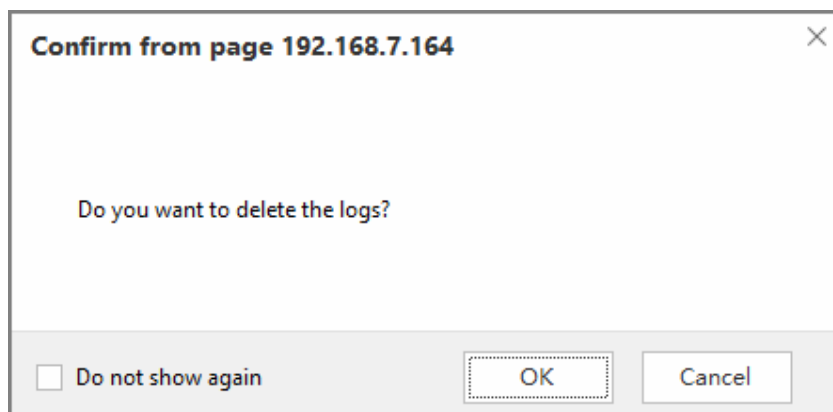
1. Click **Download the records** to download and export the searched call logs.

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 **OK** 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 to store up to 4 hardware log files. When the system generates more than 4 hardware log files, the system will replace the oldest file with a new file.

Procedure

1. Navigate to **Status > Reports > System Logs > Options**.
2. Select 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 to store 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 a new file.

Procedure

1. Navigate to **Status > Reports > System Logs > Options**.
2. Select the checkbox of **Enable Normal Log**.
3. Click **Save** and **Apply Changes**.

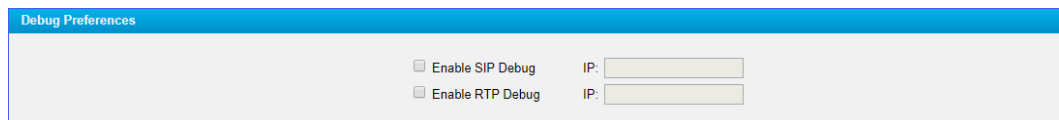
The system will start to trace the normal logs. You can check the normal log file on **System Logs** page.

Trace Debug Logs

The system support to store 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. Select the checkbox of **Enable Debug Log**.
3. **(Optional)** Enable SIP debug and RTP debug, enter the target debug IP address.



Debug Preferences	
<input type="checkbox"/> Enable SIP Debug	IP: <input type="text"/>
<input type="checkbox"/> Enable RTP Debug	IP: <input type="text"/>

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


Procedure

1. Navigate to **Status > Reports > System Logs > Options**.
2. Select 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 interface. You can debug the system efficiently with this tool.

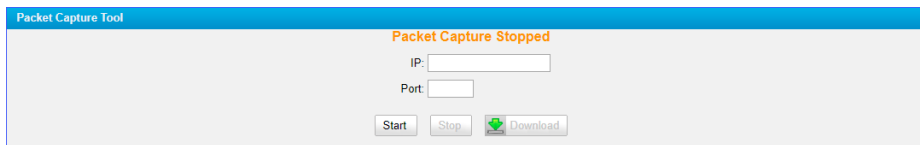
Procedure

1. Navigate to **Status > Reports > System Logs > Packet Capture Tool**.

2. Enter the target IP address.
3. Enter the target port.
4. Click **Start**.

The system will start to capture the Ethernet packet.

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



The screenshot shows a web-based interface for a 'Packet Capture Tool'. At the top, a blue header bar contains the text 'Packet Capture Tool'. Below this, the status 'Packet Capture Stopped' is displayed in orange. There are two input fields: 'IP:' and 'Port:'. At the bottom, there are three buttons: 'Start', 'Stop', and 'Download'. The 'Download' button features a green download icon.

