

Yeastar Remote Management Admin Guide

Version: 1.2.5

Date: 2022-12-16

☎ Support: +86-592-5503301
✉ Support: support@yeastar.com
🌐 <https://www.yeastar.com>

Contents

Remote Management.....	1
Getting Started.....	2
Log in to Yeastar Remote Management.....	2
Modify Your Profile.....	2
Change Login Password.....	3
Dashboard.....	5
Dashboard Overview.....	5
Manage Your Devices.....	8
Add Device by Authentication Code.....	8
Check Device Information.....	10
Set Administrator Privilege of Your Device.....	11
Visit a Device.....	12
Delete a Device.....	13
Add a Device Group.....	14
Manage User Devices.....	16
Set Administrator Privilege of User Device.....	16
Yealink Management Cloud Service.....	17
Set up Quick Access for Yealink Management Cloud Service.....	17
Manage Users.....	19
User Role Permissions.....	19
Add a User.....	19
Manage Users.....	20
Manage Colleagues.....	22
Add a Colleague.....	22
Manage Colleagues.....	23
Expand Capacity of Remote Management.....	24
Expand Capacity of Remote Management.....	24
Email Server.....	25
Set up Email Server.....	25
Network.....	26

Configure an IPv4 Address and an IPv6 Address.....	26
Alarm.....	28
Enable or Disable Alarm.....	28
Enable or Disable 'Alarm to Email'.....	28
Search Alarm Logs.....	29
Acknowledge Alarms.....	30
Maintenance.....	31
Operation Log.....	31
Operation Log.....	31
Search Operation Logs.....	31
Upgrade.....	32
Upload a PBX Firmware File.....	32
Manually Upgrade PBX Firmware.....	32
Schedule Automatic Upgrade for PBX Firmware.....	33
Manage PBX Upgrade Tasks.....	34
Backup and Restore.....	35
Create an On-Demand PBX Backup Task.....	35
Create a Scheduled Backup Task.....	36
Manage PBX Backup Tasks.....	38
Manage PBX Backup Files.....	38
Restore a PBX from a Backup File.....	39
Batch Configuration.....	39
Configuration Template.....	39
Configuration Task.....	41
Hot Standby.....	43
Hot Standby.....	43
Set up Hot Standby.....	44
Primary Server Takes over the System from Secondary Server.....	48
Set Alarm Notification of Hot Standby.....	49
Reference.....	51
Appendix.....	51

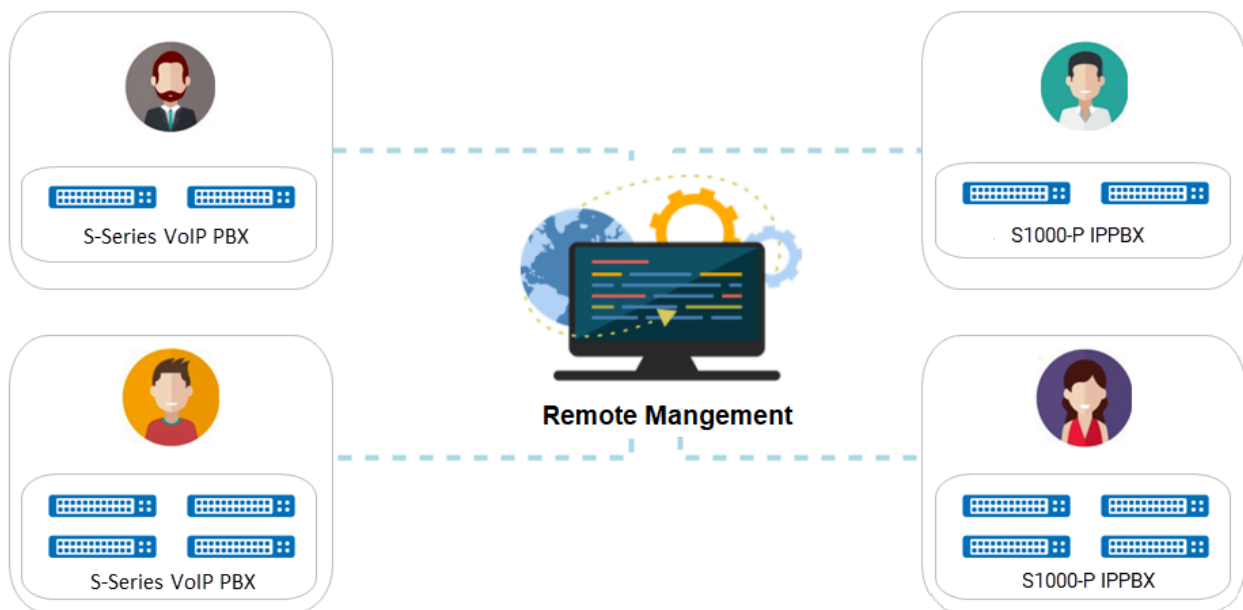
Remote Management

Yeastar Remote Management provides an affordable, low maintenance solution for easily deploying Yeastar VoIP PBX across multiple locations, reducing complexity and providing deep visibility and control.

Compatibility

The following Yeastar products support Remote Management feature:

- Yeastar S-Series VoIP PBX: 30.13.53.34.14 or later.
- Yeastar S1000-P IPPBX: 80.13.53.34.14 or later.



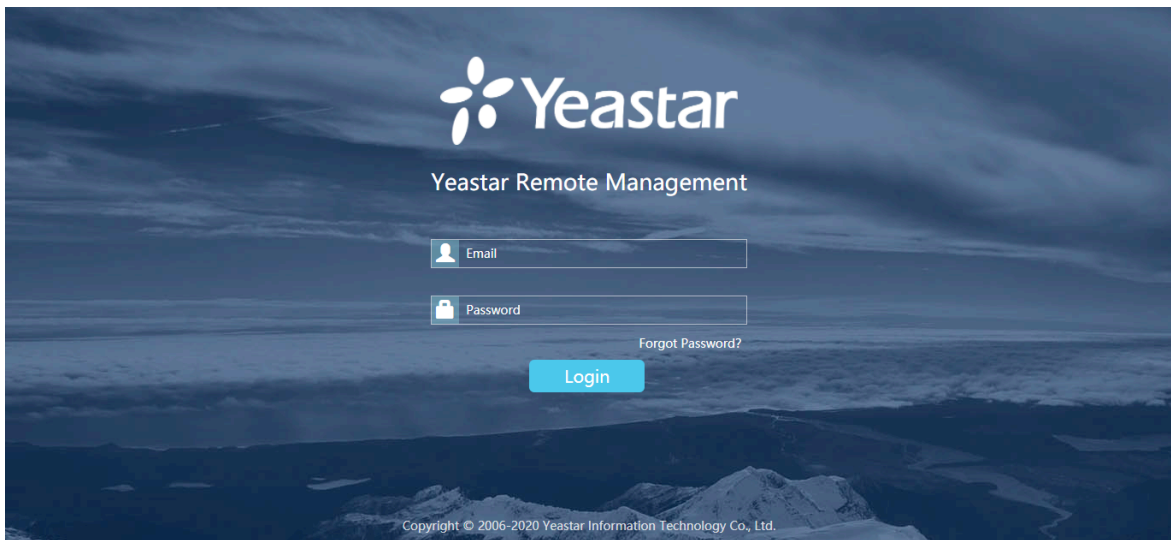
Getting Started

Log in to Yeastar Remote Management

This topic describes how to log in to Yeastar Remote Management.

Procedure

1. Open a web browser, enter the IP address or domain name of your Yeastar Remote Management platform in the address bar.
2. In the Email and Password fields, enter login credentials.



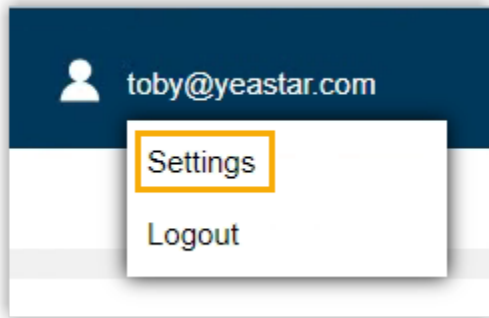
3. Click Login.

Modify Your Profile

This topic describes how to modify your profile.

Procedure

1. At the top-right conner, click your account, then select Settings.



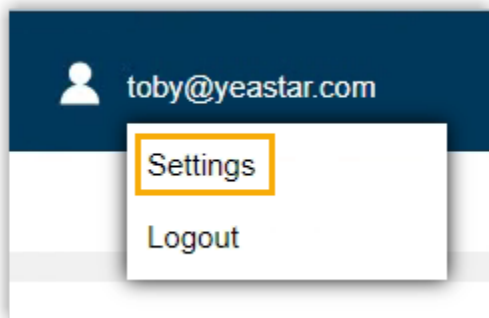
2. In My Information section, view and modify your profile.
 - Name: Enter your name.
 - Email: The email address to log in to Yeastar Remote Management platform.
 - Role: Your role in Yeastar Remote Management platform.
 - Managing/Max Manageable: The number of devices that are under your management, and the total devices that you can manage.
3. Click Save.

Change Login Password

This topic describes how to change login password.

Procedure

1. At the top-right conner, click your account, then select Settings.

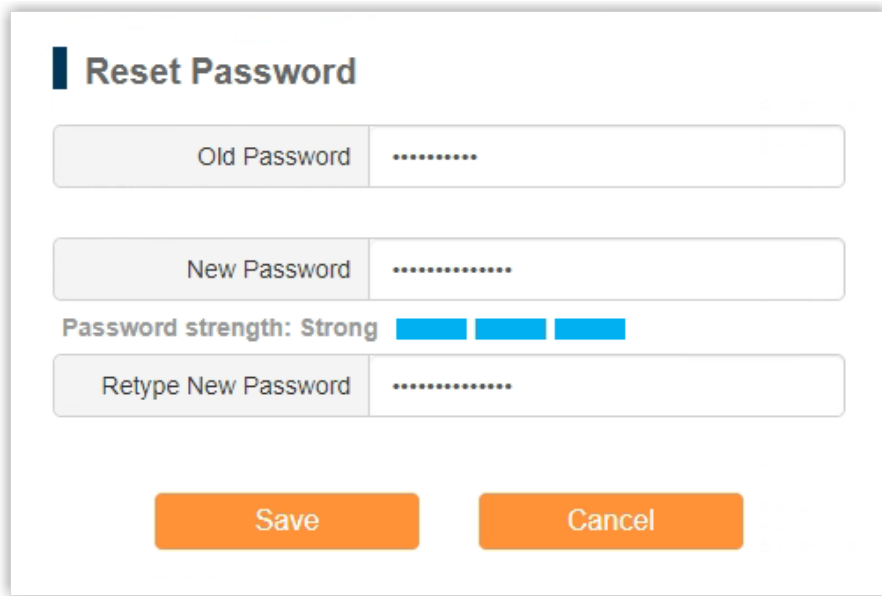


2. Click Security tab.
3. In the Reset Password section, change login password as needed.



Note:

We recommend that you set a strong password with upper cases, lower cases, and digits.



The image shows a 'Reset Password' dialog box. It has a title bar with a blue icon and the text 'Reset Password'. Below the title bar, there are three input fields: 'Old Password', 'New Password', and 'Retype New Password'. Each field has a label on the left and a masked password (dots) on the right. Below the 'New Password' field, there is a 'Password strength' indicator showing 'Strong' with three blue bars. At the bottom of the dialog, there are two orange buttons: 'Save' and 'Cancel'.

Reset Password

Old Password

New Password

Password strength: Strong

Retype New Password

Save Cancel

4. Click Save.

Result

You are automatically logged out of Yeastar Remote Management platform.

What to do next

Use the new password to access Yeastar Remote Management platform again.

Dashboard

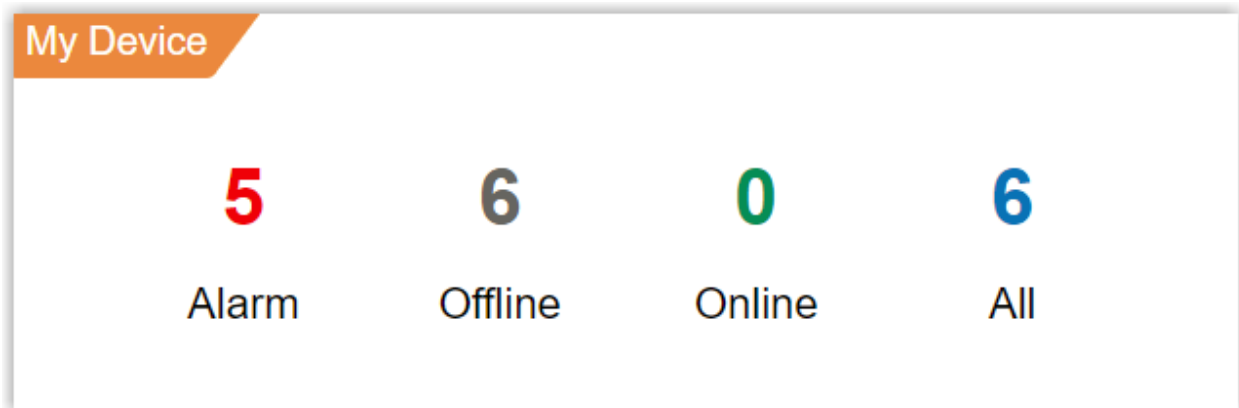
Dashboard Overview

Yeastar Remote Management platform offers you an overview of device status.

My Device

My Device displays the number of devices that are under different status:

- Alarm: The number of abnormal devices.
- Offline: The number of offline devices.
- Online: The number of online devices.
- All: The total number of devices.



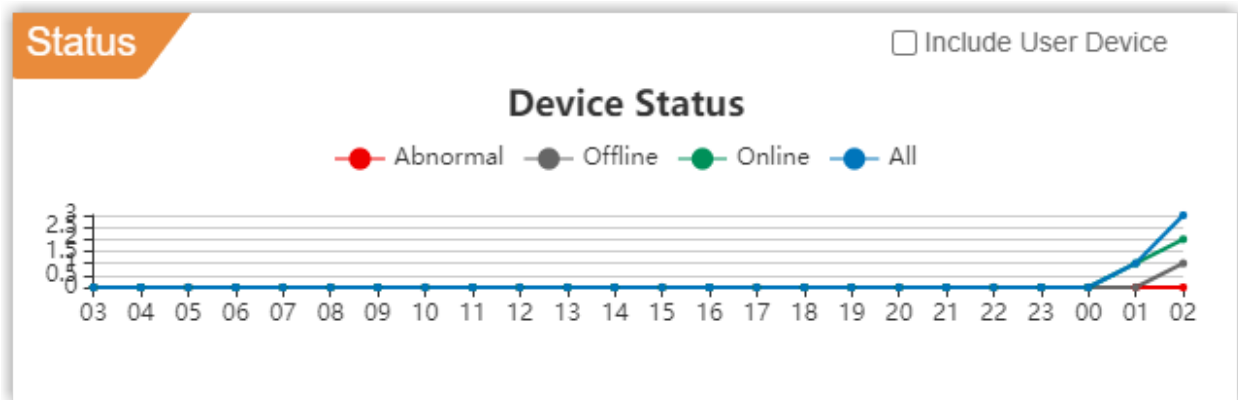
Status

Status displays the number of devices that are under different status by hour.



Note:

If you select the checkbox of Include User Device, the graph displays both your device and your users' device.



- ●: The number of abnormal devices.

If there are major alarms on a device, it would be considered as an abnormal device.

- ●: The number of offline devices.
- ●: The number of online devices.
- ●: The total number of devices.

Recent Alarms

Recent Alarms displays recent alarms for your devices. This page shows at most 10 alarms.

For more information about alarms, go to [Alarm page \(on page 29\)](#).

Recent Alarms

	Alarm Source	Device Na...	Group	Alarm Message	Time
!	System	173	-	Device disconnected. Serial...	2018-03
!	Device	S412	-	VoIP (P2P) Trunk Registrat...	2018-03

Group

Group displays the created device groups, and the number of devices that are under different status.

Group

Group Name	Alarm	Offline	Online	All
Yeastar_S20	0	0	0	0
Yeastar_S50	0	0	0	0

Manage Your Devices

Add Device by Authentication Code

Before you can manage PBX devices on Yeastar Remote Management platform, you need to add PBX devices on the platform.

Procedure

1. Generate an authentication code on Yeastar Remote Management platform.
 - a. Go to Device > My Device, click Add.
 - b. In the pop-up window, configure the following information:



Add Device	
Name	S300
Group	S-Series
<input checked="" type="checkbox"/> Verify Serial Number and MAC address	
Serial Number	
MAC Address	
<div>Add Cancel</div>	

- Name: Enter a name to help you identify the PBX that you want to add.
- Group: Optional. To add the PBX to a specific device group, select a group from the drop-down list.

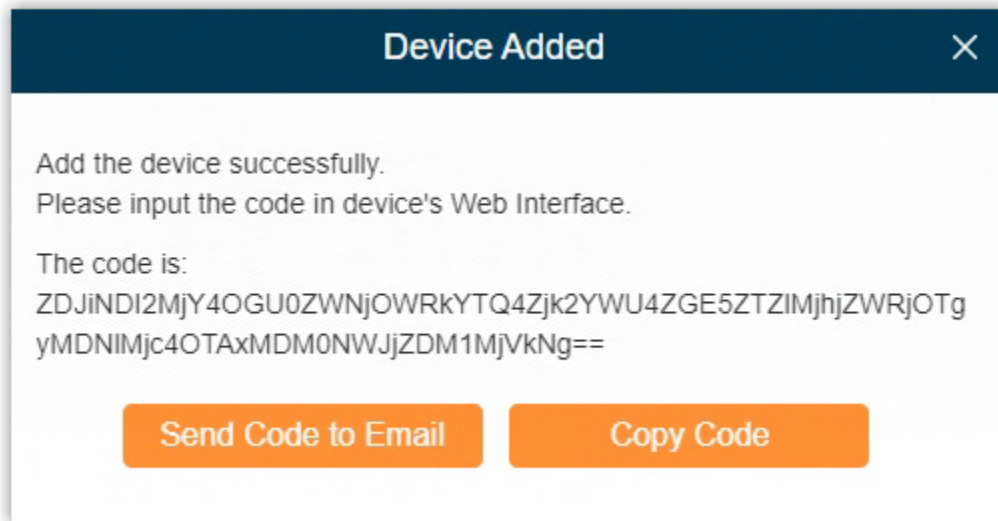
**Tip:**

For more information about group creation, see [Add a Device Group \(on page 14\)](#).

- Verify Serial Number and MAC address: Optional. To generate an authentication code for a specific PBX, select the checkbox, then configure Serial Number and MAC Address.

c. Click Add.

An authentication code is generated. You need to provide PBX administrator with the code, either by clicking Send Code to Email to send the code to a specific email address, or by clicking Copy Code.



2. Connect PBX device to Yeastar Remote Management platform.

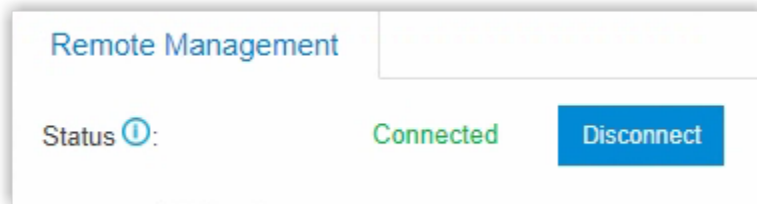
- Log in to the PBX web interface, go to Settings > System > Remote Management.
- Enter the following credentials.

Remote Management	
Status ⓘ:	Disconnected
Authentication Code:	ZDjINDI2MjY4OGU0ZWNjOV
Domain:	2201:c322:1111:2c6a:ffff:ffff:ffff
	Confirm

- Authentication Code: Enter the code that is generated for the PBX on Yeastar Remote Management platform.
 - Domain: Enter the IP address or domain name of Yeastar Remote Management platform.
- c. Click Confirm.

Result

- On the PBX web interface, the status shows "Connected".



- On Yeastar Remote Management platform, device status shows ●.

Status	Device Name	Host Name	Device Group	Serial Number	Model	Expire In	Operation
<input type="checkbox"/> ●	S300	IPPBX	-	202006021441000	Yeastar S300	N/A	

Check Device Information

This topic describes how to check device information.

Procedure

Go to Device > My Device, click beside a desired device.

Result

A pop-up window displays the device information.

Edit Device

Name

S300

Date Registered

2022-09-28 14:00:31

Serial Number

20220928140031

Last Connected

2022-09-28 14:04:17

MAC Address

74:85:40:71:5A:77

Add User

toby@yeastar.com

Model

Yeastar S300

Group

None

Firmware Version

30.14.53.34.75

Uptime

03:06:24

Save

Cancel


Set Administrator Privilege of Your Device

By default, you are the administrator of all the PBX devices under your Yeastar Remote Management account. You can change or add administrator for your device.

Prerequisites

- You have [added at least one user \(on page 19\)](#), and the user meets the following requirements:
 - Account has been activated.
 - The number of manageable devices doesn't reach the limit.
- The desired PBX device was connected earlier or is connected.

Procedure

1. Go to Device > My Device, click  beside a desired device.
2. In the pop-up window, select the checkbox of the desired user, then click Save.

Select Administrator				
<input type="checkbox"/>	Username	Company	Email	Role
<input checked="" type="checkbox"/>	Me		-	-
<input checked="" type="checkbox"/>	Becky		becky@yeastar.com	Distributor
<input type="checkbox"/>	sunmy		sunmy@yeastar.com	Basic

Result

- The device is displayed on User Device page.
- The user can access and manage the device on his or her Yeastar Remote Management platform.


Visit a Device

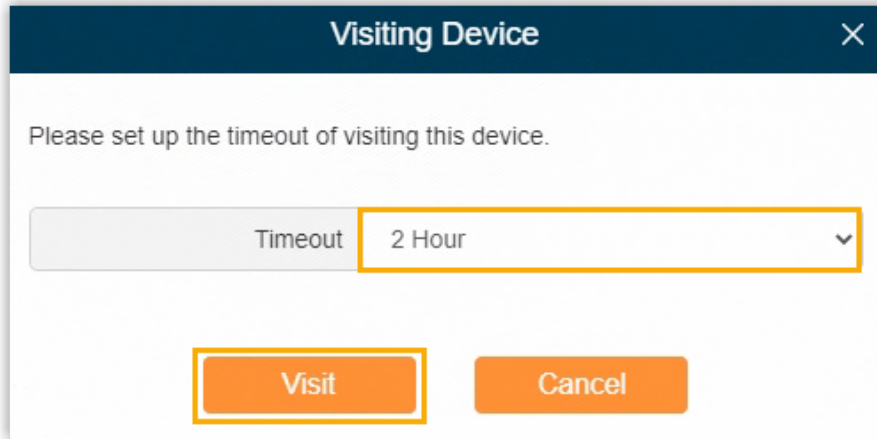
This topic describes how to visit a device.

Prerequisites

At least one PBX device is connected to Yeastar Remote Management platform. (on page 8)

Procedure

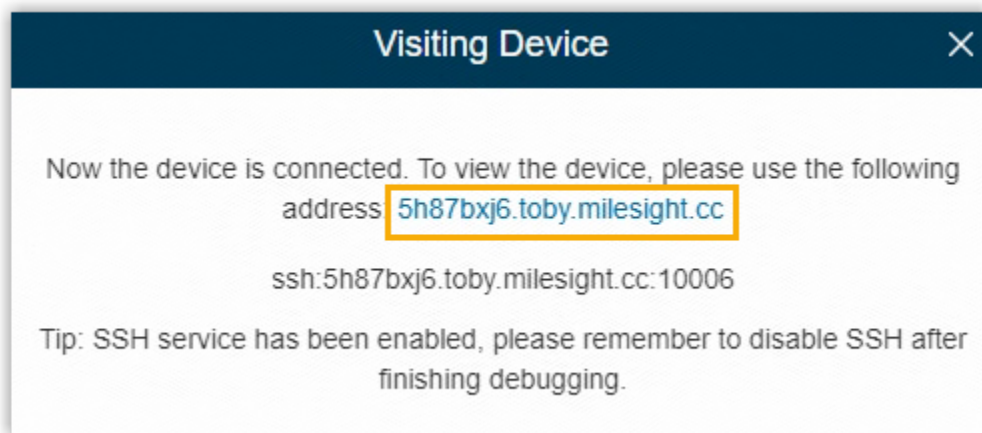
1. Go to Device > My Device, click  beside a desired device.
2. In the pop-up window, set expiration time of a visit link, then click Visit.



The image shows a 'Visiting Device' dialog box with a dark blue header and a close button (X) in the top right corner. The main content area is white and contains the text 'Please set up the timeout of visiting this device.' Below this text is a 'Timeout' label followed by a dropdown menu currently showing '2 Hour'. At the bottom of the dialog are two orange buttons: 'Visit' and 'Cancel'. The 'Visit' button is highlighted with an orange border.

Result

A visit link is displayed on the page.



The image shows the 'Visiting Device' dialog box after the 'Visit' action. The text inside reads: 'Now the device is connected. To view the device, please use the following address' followed by a highlighted blue link '5h87bxj6.toby.milesight.cc'. Below the link is the SSH command 'ssh:5h87bxj6.toby.milesight.cc:10006'. At the bottom, a tip states: 'Tip: SSH service has been enabled, please remember to disable SSH after finishing debugging.'

What to do next


Access the link to visit the device.

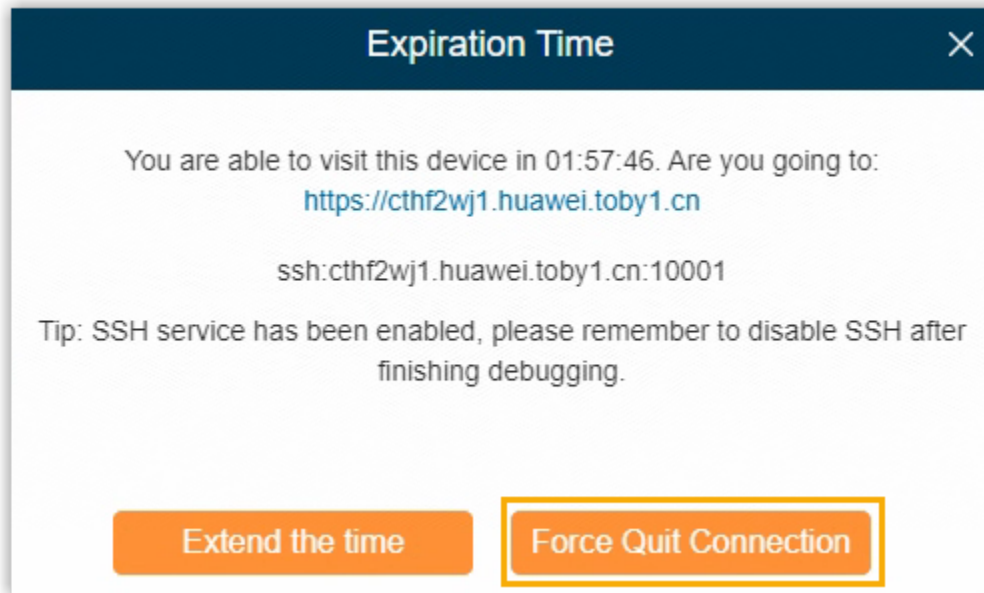
Delete a Device

This topic describes how to delete a device.

Step1. Quit connection to the PBX device


If you have established a valid connection to the desired PBX device, you need to quit the connection first.

1. Go to Device > My Device, click  beside a desired device.
2. In the pop-up window, click Force Quit Connection.



3. In the pop-up dialog box, click Yes.

Step2. Delete the PBX device

1. On My Device list, click  beside the device that you want to delete.
2. In the pop-up dialog box, click Yes.



Note:

If the device is managed by multiple users, it would also be deleted from other users' Remote Management platform.


Add a Device Group

Device Group feature allows you to centrally and efficiently manage multiple devices. This topic describes how to create a device group, and add devices to the group.

Step1. Create a device group

1. Go to Device > Device Group, click Add.
2. In the Group Name field, enter a name to help you identify the device group.
3. Click Add.

Step2. Add devices to the device group

1. On Device Group list, click  beside the desired group.
2. In the pop-up window, click Add.
3. Select the checkboxes of the desired devices, then click Add.
4. Click Save.

Manage User Devices


Set Administrator Privilege of User Device

This topic describes how to add or change administrator of user device.

Prerequisites

- You have [assigned administrator privilege of your device to at least one user \(on page 11\)](#).
- You have [added the desired user \(on page 19\)](#), and the user meets the following requirements:
 - Account has been activated.
 - The number of manageable devices doesn't reach the limit.

Procedure

1. Go to Device > User Device, click  beside a desired device.
2. In the pop-up window, select the checkboxes of the desired users, then click Save.

Select Administrator					✕	
<input type="checkbox"/>	Username	Company	Email	Role		
<input checked="" type="checkbox"/>	Me		-	-		
<input checked="" type="checkbox"/>	Becky		becky@yeastar.com	Distributor		
<input type="checkbox"/>	sunmy		sunmy@yeastar.com	Basic		

Result

The user can access and manage the device on his or her Yeastar Remote Management platform.

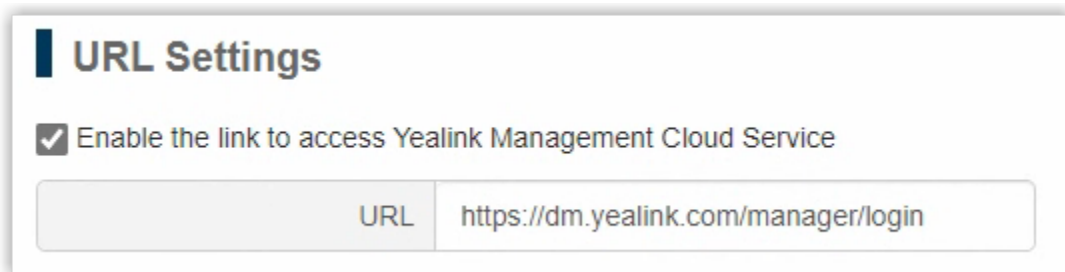
Yealink Management Cloud Service

Set up Quick Access for Yealink Management Cloud Service

For Yeastar partners who also partner with Yealink, they can quickly access Yealink Management Cloud Service (YMCS) from Yeastar Remote Management. This topic describes how to set a URL link, so as to jump to Yealink Management Cloud Service (YMCS) from Yeastar Remote Management.

Procedure

1. Go to Settings > General.
2. In the URL Settings section, do as follows:



The screenshot shows a 'URL Settings' dialog box. It has a title bar with a blue icon and the text 'URL Settings'. Below the title bar, there is a checkbox labeled 'Enable the link to access Yealink Management Cloud Service' which is checked. Below the checkbox, there is a text input field labeled 'URL' containing the text 'https://dm.yealink.com/manager/login'.

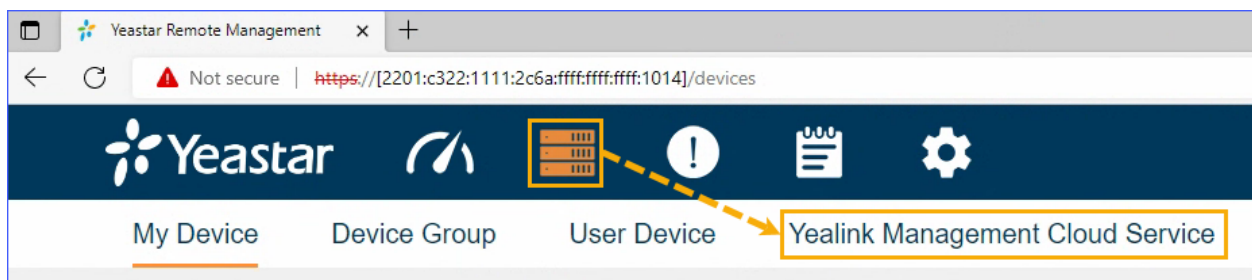
- a. Select the checkbox of Enable the link to access Yealink Management Cloud Service.
 - b. In the URL field, enter the URL.
3. Click Save.

Result

The quick access for Yealink Management Cloud Service is set up.

What to do next

Go to Device page, then click Yealink Management Cloud Service tab.



The URL of Yealink Management Cloud Service is opened in a new tab. Sign in to your account, then you can manage phones on the platform.

Manage Users

User Role Permissions

Yeastar Remote Management platform has built-in user roles with default permissions, which help you define how users can manage devices on the platform.

The permissions for each user role are as follows:

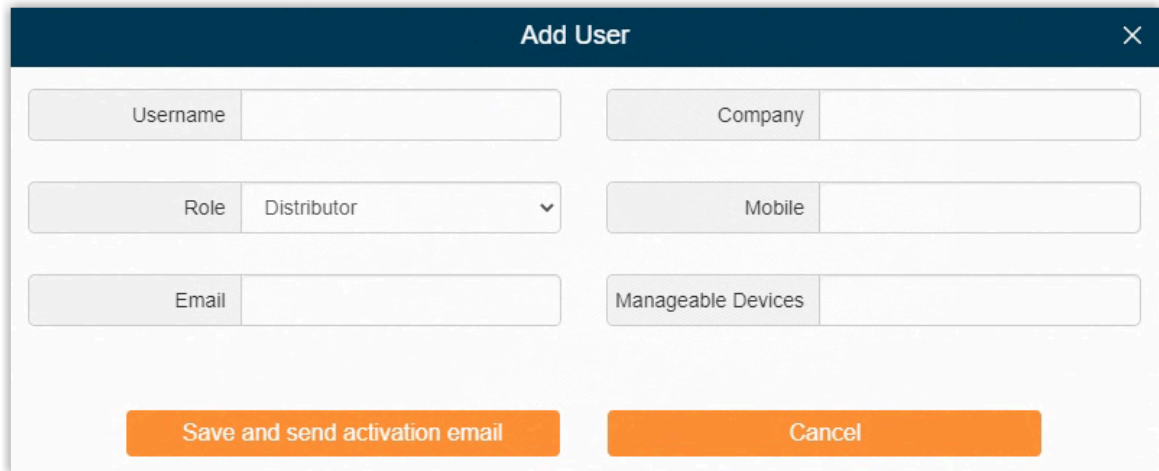
Permission	Distributor	Partner	Basic
Dashboard	√	√	√
Manage My Device	√	√	√
Manage User Device	√	√	×
Alarm Settings	√	√	√
Operation Log	√	√	√
Upgrade	√	√	√
Backup	√	√	√
Batch Configuration	√	√	√
Hot Standby	√	√	√
Create Basic Users	√	√	×
Create Partner Users	√	×	×

Add a User

A user is a sub-administrator of your device, who can access and manage the devices that are assigned by you. This topic describes how to add a user.

Procedure

1. Go to Settings > User, click Add.
2. In the pop-up window, enter user information.



The 'Add User' form is a modal window with a dark blue header containing the title 'Add User' and a close button (X). The form body is white and contains six input fields arranged in two columns. The left column has 'Username', 'Role' (a dropdown menu currently showing 'Distributor'), and 'Email'. The right column has 'Company', 'Mobile', and 'Manageable Devices'. At the bottom of the form are two orange buttons: 'Save and send activation email' on the left and 'Cancel' on the right.

- Username: Enter a user's name.
- Company: Enter the name of the company where the user works.
- Role: Select a role for the user.



Note:

If the user is a Distributor or a Partner, he or she can also create users. The users they create will be displayed on your User list, and you can manage them.

- Mobile: Enter the user's mobile number.
- Email: Enter the user's email address. The system will send an activation email to the email address.
- Manageable Devices: Set how many devices the user can manage on Yeastar Remote Management platform.

3. Click Save and send activation email.

Result

The system sends an activation email to the user.


What to do next


Ask the user to activate his or her account, so that you can give him or her the administrator privilege of a device.


Manage Users


This topic describes how to enable, disable, edit, delete, and export users.

Enable or disable a user


1. Go to Settings > User.
2. To enable a user, do as follows:
 - a. Click  beside a desired user.
 - b. In the pop-up dialog box, click Yes.

The status shows . The user can check device information and status, operate device, and change device settings.

3. To disable a user, do as follows:
 - a. Click  beside a desired user.
 - b. In the pop-up dialog box, click Yes.

The status shows . The user can check device information and status, but can NOT operate device or change device settings.

Edit a user


1. Go to Settings > User, click  beside the desired user.
2. In the pop-up window, change user settings.
3. Click Save and OK.

Delete a user



Important:

- If there's device under the user's management, you can NOT delete the user. To delete the user, you need to transfer device managing authority to another user first.
- User accounts created by the user, if any, will also be deleted.

1. Go to Settings > User, click  beside a desired user.
2. In the pop-up dialog box, click Yes to confirm.

Export user information

1. Go to Settings > User.
2. Click Export.

Information of all the users is exported to a CSV file.

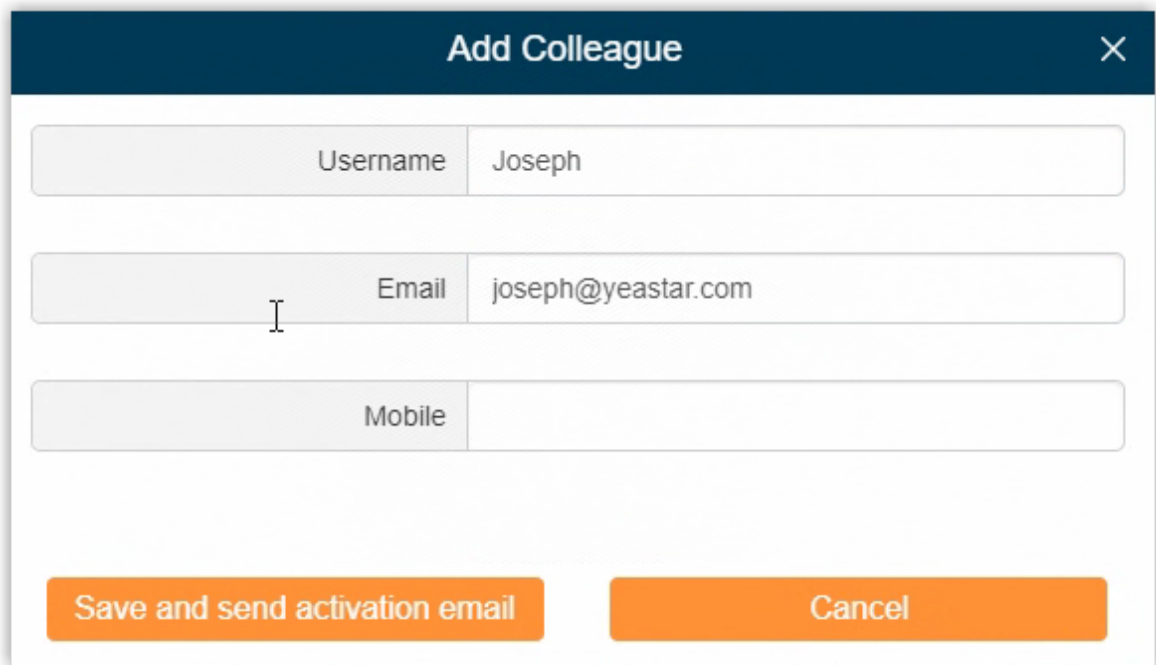
Manage Colleagues

Add a Colleague

A colleague can visit and manage all your devices, and has all of your permissions on Yeastar Remote Management platform except setup of colleague. You can add a colleague to help you manage PBX devices when you are unavailable. This topic describes how to add a colleague.

Procedure

1. Go to Settings > Colleague, click Add.
2. In the pop-up window, enter colleague information.



Add Colleague	
Username	Joseph
Email	joseph@yeastar.com
Mobile	
<div>Save and send activation email Cancel</div>	

- Username: Enter a colleague's name.
 - Email: Enter the colleague's email address.
The system will send an activation email to the email address.
 - Mobile: Enter the colleague's mobile number.
3. Click Save and send activation email.

Result

The system sends an activation email to the colleague's email address. After activating, the colleague will be redirected to login page of Yeastar Remote Management platform.

Manage Colleagues

This topic describes how to edit or delete colleagues.

Edit a colleague

1. Go to Settings > Colleague, click  beside the desired colleague.
2. Edit colleague information.
3. Click Save and OK.

Delete a colleague

1. Go to Settings > Colleague, click  beside the desired colleague.
2. In the pop-up dialog box, click Yes to confirm.

Expand Capacity of Remote Management

Expand Capacity of Remote Management

If you want to expand the number of manageable devices and maintenance time, contact Yeastar to upgrade your license, and then update your license on your Remote Management platform.

Procedure

1. Log in to Yeastar Remote Management, go to Settings > Activation Information.
2. In the Active code field, enter your new license.
3. Click Update.



Important:

Keep the USB Key connected to the server, or the Remote Management will be detected as an abnormal device.

The screenshot shows the Yeastar Remote Management web interface. The top navigation bar includes the Yeastar logo and several icons. Below the navigation bar, there are tabs for General, User, Colleague, Security, Activation Information (which is selected), and Email Server. The main content area is titled 'Active Portal' and displays the following information:

- Status: Activated
- Unique: 065c050df1896a0d4b4e067ab346a300
- Device of numbers: 25
- Maintenance Period: 2020-01-26 to 2020-09-27

Below this information, there is a section for the 'Active code' which contains the value '065c050df1896a0d4b4e067ab346affe'. An orange 'Update' button is located at the bottom of this section, with a mouse cursor pointing at it.

Email Server

Set up Email Server

Email server is used to send emails about account activation, password recovery, and alarm notification. This topic describes how to set up email server.

Procedure

1. Go to Settings > Email Server.
2. Set up email server.
 - Sender Email Address: Enter an available email address.
 - Email Address or Username: Enter the account to log in to the email server.



Note:

Generally, enter the same value as the Sender Email Address. But if the email server provides a unique user name, enter the user name.

- Password: Enter the password to log in to the email server.
 - Outgoing Mail Server (SMTP): Enter the outgoing mail address.
 - Port: Enter the outgoing port.
 - SSL: Enable or disable SSL to secure message sent from the server. If the email sending server requires to authenticate the sender, you need to turn on this option.
 - Enable STARTTLS: If the mail server doesn't support STARTTLS, do not select this option.
3. Test if the email server works.
 - a. Click Test.

If email server is set up successfully, the system prompts "Test Succeed".
 - b. In the pop-up dialog box, click OK.
 - c. Click Submit and OK.

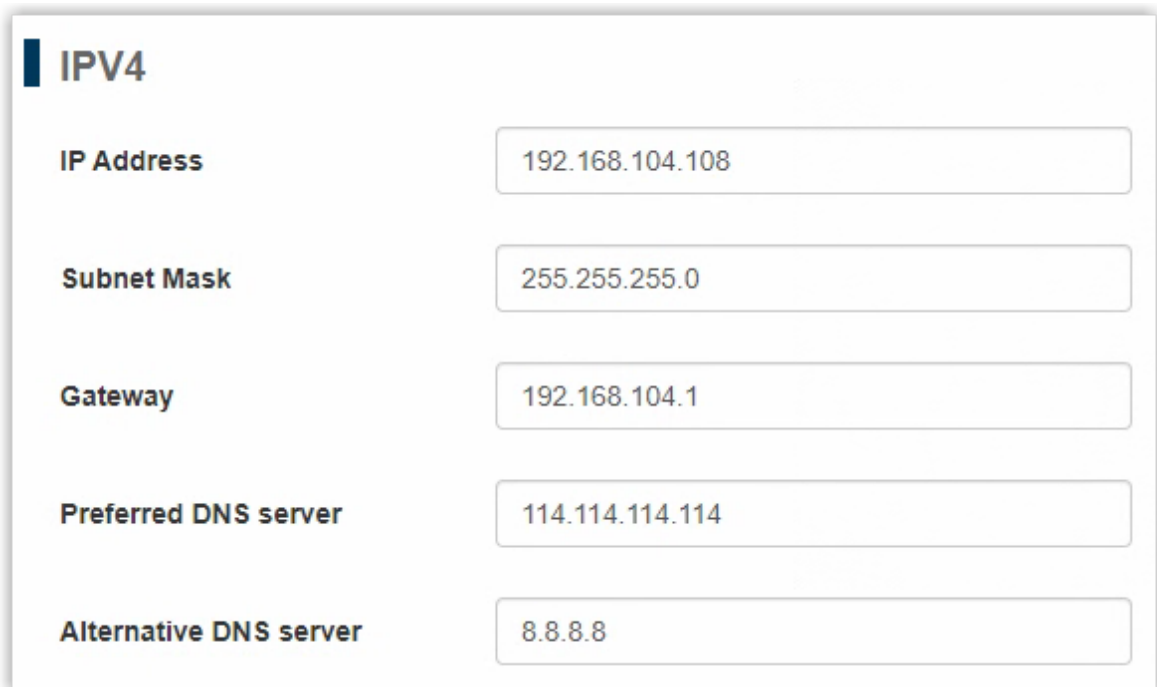
Network

Configure an IPv4 Address and an IPv6 Address

Yeastar Remote Management supports both IPv4 and IPv6 connections. The IP addresses that you have configured when initially setting up Yeastar Remote Management would be synchronized to the network page. You can change or configure the IPv4 address and IPv6 address as needed.

Procedure

1. Go to Settings > Network.
2. If you want to change the IPv4 address, proceed in the IPV4 section:



IPV4	
IP Address	192.168.104.108
Subnet Mask	255.255.255.0
Gateway	192.168.104.1
Preferred DNS server	114.114.114.114
Alternative DNS server	8.8.8.8

- IP Address: Enter an IPv4 address for your Yeastar Remote Management.



Note:

The IP address should be unique and has not been assigned to any other devices in the same network.

- Subnet Mask: Enter the subnet mask.
 - Gateway: Enter the gateway address.
 - Preferred DNS server: Enter the IP address of preferred DNS server.
 - Alternative DNS server: Optional. Enter the IP address of alternative DNS server.
3. If you want to change or configure the IPv6 address, proceed in the IPV6 section.

IPv6

☒ Enable IPv6

IP Address

2201:c322:1111:2c6a:ffff:ffff:1014

IP Prefix Length

64

Gateway

2201:c322:1111:2c6a::

Preferred DNS server

2400:3200::1

Alternative DNS server

- Enable IPv6: Check this option.
- IP Address: Enter an IPv6 address for your Yeastar Remote Management.



Note:

The IP address should be unique and has not been assigned to any other devices in the same network.

- IP Prefix Length: Enter the prefix length of the IPv6 address.
- Gateway: Enter the gateway address.
- Preferred DNS server: Enter the IP address of preferred DNS server.
- Alternative DNS server: Optional. Enter the IP address of alternative DNS server.

4. Click Save.

5. Reboot the system to take effect.

Result


You can access Yeastar Remote Management by IPv4 address or IPv6 address.

Alarm

Enable or Disable Alarm

Alarm feature records key information and keeps you informed when specific events happen to those devices that are under your management. Yeastar Remote Management platform has two alarm levels, major and minor. Major alarms are enabled by default. You can enable or disable alarm for events according to your needs.

Enable alarm for an event


1. Go to Alarm > Alarm Settings.
2. Click  beside a desired event.
When the event occurs, the system will notify you via email.



Note:

Make sure you have [set up email server \(on page 25\)](#), or you can NOT get email notifications when events occur.

Disable alarm for an event

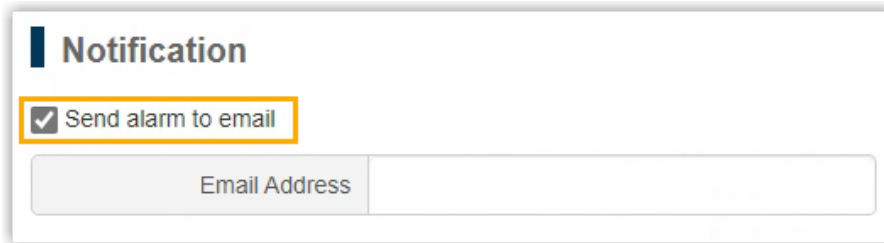
1. Go to Alarm > Alarm Settings.
2. Click  beside a desired event.
When the event occurs, the system will NOT notify you.

Enable or Disable 'Alarm to Email'

Alarm to Email feature helps you get email notifications when specific events happen to PBX devices that are under your management. This topic describes how to enable or disable Alarm to Email feature.

Enable 'Alarm to Email'

1. Go to Settings > General.
2. In the Notification column, select the checkbox of Send alarm to email.



Notification

☒ Send alarm to email

Email Address

3. In the Email Address field, set an email address to receive alarm notifications.
4. Click Save and OK.

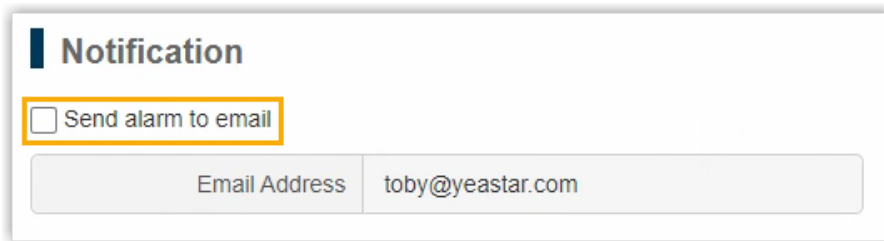


Note:

Make sure you have [set up email server \(on page 25\)](#), or you can NOT get email notifications when events occur.

Disable 'Alarm to Email'

1. Go to Settings > General.
2. In the Notification column, unselect the checkbox of Send alarm to email.



Notification

☐ Send alarm to email

Email Address toby@yeastar.com

3. Click Save and OK.

Search Alarm Logs

This topic describes how to search alarm logs by alarm level, alarm name, specific time, and device serial number.

Procedure

1. Go to Alarm > Alarm List.
2. Set search criteria.
 - Alarm Level: Select an alarm level.
 - Major
 - Minor
 - Alarm Name: Select a specific alarm event.
 - Time: Specify a time period.
 - Serial Number: Enter serial number of a PBX device.
3. Click Search.

Result

The matched alarm logs are displayed on the page.

What to do next

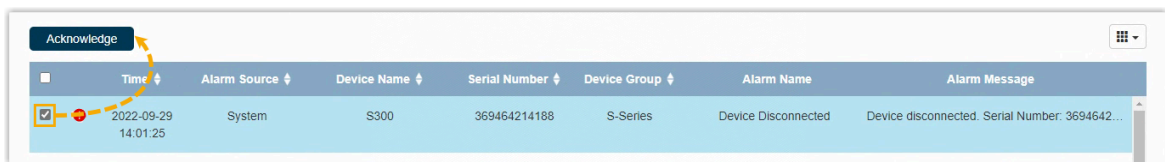
Fix the issue, if any, and then [acknowledge the alarm \(on page 30\)](#).

Acknowledge Alarms

After you check alarm information and fix an issue, you need to acknowledge the alarm, or it remains.

Procedure

1. Go to Alarm > Alarm List.
2. Select the checkbox of the desired alarm, then click Acknowledge.



Result

The alarm is acknowledged. If all the alarms for a PBX device are acknowledged, the device status on My Device page will be changed from ● to ●.

Maintenance

Operation Log

Operation Log

Operation log records operations that are performed on Yeastar Remote Management platform, which helps you monitor and analyze causes of system issues.

Operation log records the following types of logs:

- Login & Logout
- My Device
- Remote Connection
- Device Group
- User Device
- Alarm
- General
- User
- Security
- Batch Configuration
- Upgrade
- Backup
- SMTP
- Hot Standby
- Activation

Search Operation Logs

This topic describes how to search operation logs by log type, IP address, specific time, and device serial number.

Procedure

1. Go to Maintenance > Operation Log.
2. Set search criteria.
 - Log Type: Query all types of operation logs or query logs by a specific type.
 - IP: Enter an IP address. The system will query operations that are performed by device with the IP address.
 - Time: Specify a time period. The system will query logs within the time period.
 - Serial Number: Enter serial number of a PBX device. The system will query logs related with the PBX device.
3. Click Search.

Result

The matched operation logs are displayed on the page.

Upgrade

Upload a PBX Firmware File

Before you create an upgrade task for PBX devices, you need to upload a PBX firmware file. This topic describes how to upload a PBX firmware file.

Procedure

1. Go to Maintenance > Upgrade > Firmware File, click Add.
2. In the pop-up window, click Browse to select a `.bin` file.
3. Optional: Retain the file name, or enter a name in the Filename field.
4. Optional: In the Memo field, add a note to the firmware file.
5. Click Upload.

Result

The firmware file is uploaded and displayed on Firmware File page.

What to do next

[Manually upgrade firmware \(on page 32\)](#) or [schedule an automatic upgrade task \(on page 33\)](#).

Manually Upgrade PBX Firmware

This topic describes how to manually upgrade PBX firmware.

Prerequisites

- You have [added and connected at least one PBX to Yeastar Remote Management platform \(on page 8\)](#).
- You have [uploaded desired firmware file \(on page 32\)](#) to Yeastar Remote Management platform.

Procedure

1. Go to Maintenance > Upgrade > Upgrade, click Add.
2. Configure basic information of the upgrade task.
 - Task Name: Enter a name to help you identify the upgrade task.
 - Memo: Add a note to the upgrade task.

- Firmware File: Select a firmware file from the drop-down list.
 - Firmware Type: The firmware type is automatically matched after you select a firmware file.
 - S-series
 - S1000-P
 - Execution Way: Select Upgrade Now.
3. Add one or more PBXs that you want to upgrade.
 - a. Click Add.
 All connected PBXs compatible with the selected firmware type are displayed on the page.
 - b. Select the checkboxes of the desired devices.
 - c. Click Add.
 4. Click Save.

What to do next

Wait for a few seconds, refresh the Upgrade page, and check status of the upgrade task.

- Not Started: It takes time to connect to and receive response from the desired PBXs, wait a minute and try to refresh the page.
- In Progress: The upgrade task is in progress, which indicates that not all of the PBXs are upgraded completely.
- Completed: The upgrade task is completed, which indicates that all of the PBXs are upgraded.

Schedule Automatic Upgrade for PBX Firmware

This topic describes how to schedule an automatic upgrade task to upgrade PBX at a specific time.

Prerequisites

- You have [added and connected at least one PBX to Yeastar Remote Management platform \(on page 8\)](#).
- You have [uploaded desired firmware file \(on page 32\)](#) to Yeastar Remote Management platform.

Procedure

1. Go to Maintenance > Upgrade > Upgrade, click Add.
2. Configure basic information of the upgrade task.
 - Task Name: Enter a name to help you identify the task.
 - Memo: Add a note to the upgrade task.
 - Firmware File: Select a firmware file from the drop-down list.

- **Firmware Type:** The firmware type is automatically matched after you select a firmware file.
 - S-series
 - S1000-P
 - **Execution Way:** Select Specific Time, and set a time. The selected PBX will be upgraded at the specified time.
3. Add one or more PBXs that you want to upgrade.
 - a. Click Add.

All connected PBXs compatible with the selected firmware type are displayed on the page.
 - b. Select the checkboxes of the desired devices.
 - c. Click Add.
 4. Click Save.

Result

The scheduled upgrade task is created.

What to do next


Check status of the upgrade task.

- **Not Started:** It doesn't come to the scheduled upgrade time.
- **In Progress:** The upgrade task is in progress, which indicates that not all the specified PBXs are upgraded completely.
- **Completed:** The upgrade task is completed, which indicates that all of the specified PBXs are upgraded.


Manage PBX Upgrade Tasks

This topic describes how to edit or delete an upgrade task.

Edit an upgrade task

1. Go to Maintenance > Upgrade, click Upgrade tab.
2. Click  beside the upgrade task that you want to edit.
3. Change task settings.
4. Click Save.

Delete an upgrade task

1. Go to Maintenance > Upgrade, click Upgrade tab.
2. Click  beside the upgrade task that you want to delete.
3. In the pop-up dialog box, click Yes.

Backup and Restore

Create an On-Demand PBX Backup Task

An on-demand backup task helps you back up PBX configurations and data at a time, which saves your time and energy, and improves your work efficiency.

Prerequisites

The PBX that you want to back up is connected to Yeastar Remote Management platform. (on page 8)

Procedure

1. Go to Maintenance > Backup, click Backup.
2. Configure basic information of the backup task.
 - Task Name: Enter a name to help you identify the task.
 - Password: Enter a password to encrypt the backup file.

If set, anyone who wants to restore a PBX from the backup file must enter the password.

- Memo: Add a note to the task.
- Storage Location Type: The location to save backup files.



Note:

Backup files can ONLY be saved on local storage of the corresponding PBX.

- The Backup file will include: Select the configurations and data that will be backed up.
 - System Settings
 - Custom Prompts
 - Call Logs



Note:

To back up call logs, you need to proceed on PBX web interface.

- Execution Way: Set when to perform the one-time backup task.
 - Backup Now: Back up PBX configurations and data as soon as you save the task.
 - Specific time: Back up PBX configurations and data at a specific time. To achieve this, you need to set a time.
- 3. Add one or more PBXs that you want to back up.

- a. Click Add.
All the PBXs that are connected to Yeastar Remote Management platform are displayed on the page.
- b. Select the checkboxes of the desired PBXs.
- c. Click Add.
4. Click Save and OK.

What to do next

Wait for a few seconds, refresh the Backup page, and check status of the backup task.

- Not Started: It takes time to connect to and receive response from the desired PBXs, wait a minute and try to refresh the page.
- In Progress: The backup task is in progress, which indicates that not all of the specified PBX's configurations and data are backed up.
- Completed: The backup task is completed, which indicates that configurations and data of all the specified PBXs are backed up.



Tip:

To check or manage backup files, see [Manage PBX Backup Files \(on page 38\)](#).

Create a Scheduled Backup Task

A scheduled backup task helps you back up PBX configurations and data at a specific time, which saves your time and energy, and improves your work efficiency.

Prerequisites

The PBX that you want to back up is connected to Yeastar Remote Management platform. (on page 8)

Procedure

1. Go to Maintenance > Backup, click Backup Schedule.
2. Configure basic information of the backup task.
 - Task Name: Enter a name to help you identify the task.
 - Password: Enter a password to encrypt the backup file.
If set, anyone who wants to restore a PBX from the backup file must enter the password.
 - Memo: Add a note to the task.
 - Storage Location Type: The location to save backup files.

**Note:**

Backup file can ONLY be saved on local storage of the corresponding PBX.

- The Backup file will include: Select the configurations and data that will be backed up.
 - System Settings
 - Custom Prompts
 - Call Logs

**Note:**

To back up call logs, you need to proceed on PBX web interface.

- Backup Rotation: Set how many backup files are allowed to be stored in local storage of the corresponding PBX.

When the number of backup files reaches the limit, the oldest file will be replaced with the newest.

- Schedule: Set when to perform the backup task.

3. Add one or more PBXs that you want to back up.

a. Click Add.

All the PBXs that are connected to Yeastar Remote Management platform are displayed on the page.

b. Select the checkboxes of the desired PBXs.

c. Click Add.

4. Click Save and OK.

Result

The backup task is created and displayed on Backup list.

What to do next

Check status of the scheduled backup task.

- Not Started: It doesn't come to the backup time.
- In Progress: The scheduled backup task is in progress.
- Scheduled: The scheduled backup task is completed.

**Tip:**


To view and manage backup files, see [Manage PBX Backup Files \(on page 38\)](#).

Manage PBX Backup Tasks

This topic describes how to restart, view, edit, or delete a backup task.

Restart a backup task

In case you want to restart a backup task that was completed earlier, you can restart it as follows.

1. Go to Maintenance > Backup, click  beside a backup task that was completed.
2. Click Save.

The backup task will be re-executed, and the oldest backup file will be replaced with the newest.

View a backup task

1. Go to Maintenance > Backup, click  beside the desired backup task.

Edit a backup task




Note:
You can NOT edit a task that is "In Progress".

1. Go to Maintenance > Backup, click  beside the desired backup task.
2. Change task settings.
3. Click Save and OK.

Delete backup tasks



Note:
You can NOT delete a task that is "In Progress".

1. Go to Maintenance > Backup.
2. To delete a backup task, click  beside the backup task that you want to delete, click Yes.
3. To bulk delete backup tasks, select the checkboxes of the desired backup tasks, click Delete and Yes.

Manage PBX Backup Files

This topic describes how to download or delete the backup file of a specific PBX.

1. Go to Device > My Device, click  beside the desired PBX.


All backup files created on Yeastar Remote Management platform for the PBX are displayed on the page.

2. To download a backup file, click  beside the desired backup file.
3. To delete a backup file, click  beside the desired backup file.


Restore a PBX from a Backup File

This topic describes how to restore a PBX from a backup file.

Procedure

1. Go to Device > My Device, click  beside the desired PBX.
2. In the Select a device drop-down list, select a PBX.

All the PBXs with the same model as the selected PBX are displayed on the drop-down list.

- To restore the PBX to its own backup file, select the device.
 - To restore the PBX to a backup that was created on another PBX, select another PBX.
3. Click  beside the backup file to which you want the PBX to restore.
 4. In the pop-up dialog box, click Yes.

Result

The PBX will be restored from the backup file.

Batch Configuration

Configuration Template

Create a Configuration Template

A configuration template can be used to set certain parameters, and assigned to one or more PBXs at a time, thus saving your energy and time in PBX setup. This topic describes how to obtain a configuration template from a PBX that is connected to Yeastar Remote Management platform.

Background information

Yeastar Remote Management provides a default PBX configuration template, which can be applied to both Yeastar S-Series VoIP PBX and Yeastar S1000-P IPPBX. The default configuration template contains parameters about the following configurations:

- Physical trunk
 - VoIP trunk
 - Extension
 - Inbound Route
 - Outbound Route
 - Time Condition
 - IVR
 - Queue
 - Ring Group
-
- Conference

You can edit the template or create another template according to your needs.

Prerequisites

[The desired PBX is connected to Yeastar Remote Management platform. \(on page 8\)](#)

Procedure

1. Go to Maintenance > Batch Configuration, click Configuration Template tab.
2. Set up a configuration template.
 - a. Click Obtain.
 - b. In the Template Name field, enter a name to help you identify the template.
 - c. In the Memo field, add a note.
 - d. In the Select a Device drop-down list, select a PBX from which you want to obtain a configuration template.
 - e. Click Obtain.

It takes several minutes to obtain a configuration template from the PBX.

Result

The configuration template is displayed on Configuration Template page.

What to do next

[Bulk configure PBXs using a configuration template \(on page 41\)](#) according to your needs.

Manage Configuration Templates


This topic describes how to edit or delete configuration templates.

Edit a configuration template



Note:

You can NOT edit a template that is being applied to PBX devices.


1. Go to Maintenance > Batch Configuration.
2. Under Configuration Template tab, click  beside the configuration template that you want to edit.
3. Change template settings.
4. Click Save and OK.

Delete configuration templates



Note:

You can NOT delete a template that is being applied to PBX devices.

1. Go to Maintenance > Batch Configuration.
2. Under Configuration Template tab, click  beside the configuration template that you want to delete.
3. In the pop-up dialog box, click Yes and OK.

Configuration Task

Bulk Configure PBXs Using a Configuration Template

This topic describes how to bulk configure PBXs using a configuration template.

Prerequisites

[The desired PBXs are connected to Yeastar Remote Management platform. \(on page 8\)](#)

Procedure

1. Go to Maintenance > Batch Configuration.
2. Under Batch Configuration tab, click Add to set up a batch configuration task.
3. Configure basic settings of the task.
 - Task Name: Enter a name to help you identify the task.
 - Memo: Add a note to the task.
 - Configuration Template: Select a template from the drop-down list.

- Default template: The selected PBXs will inherit all parameters in the configuration template.
- {custom_template}: The selected PBXs will inherit all parameters in the configuration template except extensions, which will always be obtained from Default template.

**Note:**

Custom template can ONLY be applied to PBXs of the same model. For example, if you obtain a template from S-Series VoIP PBX, then the template can only be applied to S-Series VoIP PBX.

4. Add one or more PBXs to which the configuration template will be applied.
 - a. Click Add.
 - b. In the pop-up window, select the checkboxes of the desired PBXs.
 - c. Click Add.
5. Click Save.

Result

Configurations of the desired PBXs will be overwritten.

What to do next


Check status of the task.

- Not Started: It takes time to connect to and receive response from the desired PBXs, wait a minute and try to refresh the page.
- In Progress: The task is in progress, which indicates that configuration template has not been applied to all of the PBXs.
- Completed: The task is completed, which indicates that configuration template is applied to all of the PBXs.


Manage Configuration Tasks

This topic describes how to view, edit, and delete configuration tasks.


View configuration tasks

1. Go to Maintenance > Batch Configuration.
2. Under Batch Configuration tab, click  beside the desired configuration task.
Details about the configuration task is displayed in the pop-up window.

Edit configuration tasks

1. Go to Maintenance > Batch Configuration.
2. Under Batch Configuration tab, click  beside the desired configuration task.
3. Change task settings.
4. Click Save.

Delete configuration tasks

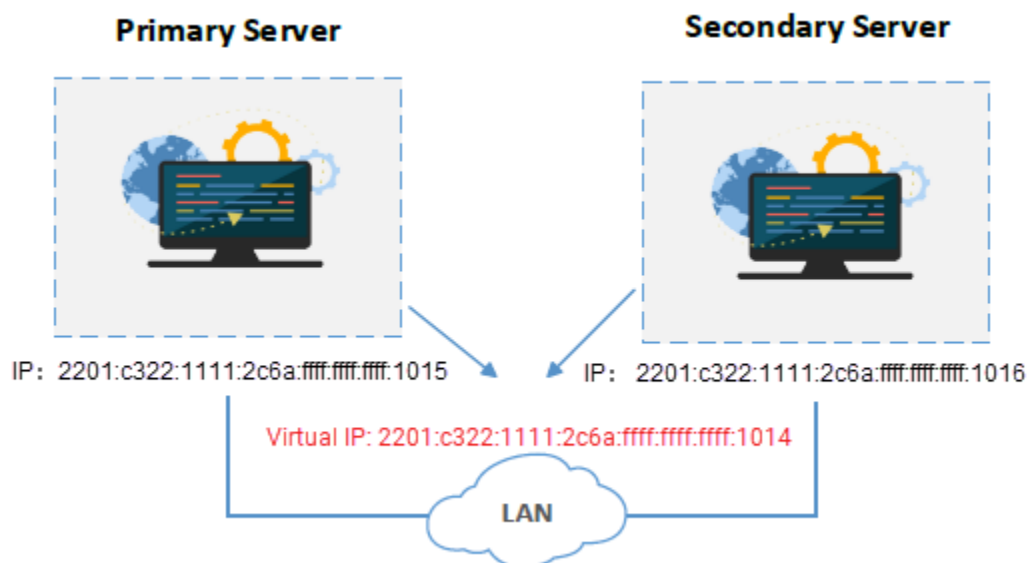
1. Go to Maintenance > Batch Configuration.
2. Under Batch Configuration tab, click  beside the desired configuration task.
3. In the pop-up dialog box, click Yes and OK.

Hot Standby

Hot Standby

The Hot Standby solution provides high system availability and prevents you from unnecessary business loss caused by unexpected server failure.

The solution consists of two Remote Management Servers of the same software, one works in the "active" state and the other works in the "standby" state. The configuration of primary server is synchronized to the secondary server in real time so that both systems contain identical information. When the primary server goes down, the secondary server can automatically and instantly take over.



Set up Hot Standby

This topic describes how to set up hot standby on the primary server and secondary server.

Prerequisites

The primary server and secondary server in the failover pair must meet the following requirements:

- Same software version.
- Same domain name, which is configured in Configuration Wizard when you set up Yeastar Remote Management.
- Same installation environment, both installed on physical machines or both installed on virtual machines.

Step1. Set up hot standby for primary server

1. Log in to Yeastar Remote Management platform, go to Maintenance > Hot Standby.
2. Select the checkbox of Enable Hot standby.
3. Set up the primary server.

- a. In the Mode drop-down list, select Primary.

The Remote Management platform will work as the primary server.

- b. Configure server information.

- Primary Server Hostname: Specify a hostname to help you identify the primary server.
- Secondary Server Hostname: Specify a hostname to help you identify the secondary server.
- Secondary Server IP Address: Enter the IP address of the secondary server.
- Access Code: Enter an access code.



Note:

The two Remote Management Servers must have the same access code to authenticate connection.

- c. Configure virtual IP.

- Virtual IP Address: Enter an available IP address. Virtual IP address is a shared IP for the two Remote Management Servers. The virtual IP always points to the on-site Remote Management Server.
- Subnet Mask / IPv6 Prefix: Enter subnet mask (IPv4) or prefix (IPv6).
- Virtual Gateway: Optional. Enter a gateway address for the virtual IP network.

If left blank, the interactions between the Remote Management Server and the virtual IP network would fail when they are under different network segments.

- **Network Connection Detection:** If all nodes failed to be detected by the secondary server, it means that Internet outage(s) has occurred; both the primary and the secondary server of your Remote Management system have abnormal internet connection. In this case, the Remote Management failover would not work.



Note:

We recommend that you enter the gateway address.

d. Configured advanced settings that will work when the server runs as a standby system.

- **Keep Alive(s):** Define the frequency to send heartbeat keep-alive packets.

The default value is 2 seconds, which means that the standby server sends packets every 2 seconds to detect whether the primary server is alive or not.

- **Dead Time(s):** Define the maximum time interval before the primary server responds to the standby server.

The default value is 120 seconds. If the standby server receives no response after timeout, it takes over automatically.



Note:

Set the Dead Time longer than the server rebooting time, or the standby server will take over when the primary server is rebooting.

e. Click Save.

☒ Enable Hot Standby

Mode Primary

Server Information

Primary Server Hostname Host

Secondary Server Hostname Standby

Secondary Server IP Address 2201:c322:1111:2c6a::1016

Access Code *****

Virtual IP Address

Virtual IP Address 2201:c322:1111:2c6a::1014

Subnet Mask 64

Virtual Gateway 2201:c322:1111:2c6a::

Network Connection Detection 2201:c322:1111:2c6a::

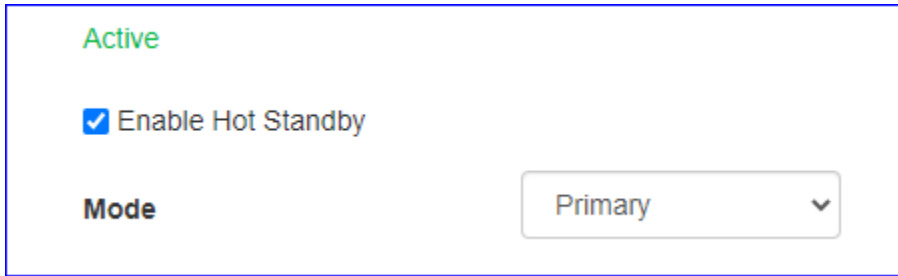
Advanced

Keep Alive(s) 2

Dead Time(s) 120

4. In the pop up dialog box, click Yes to reboot.

When the server boots up, the Remote Management Server works as the primary server.



The screenshot shows a configuration window with a blue border. At the top left, the word 'Active' is displayed in green. Below it, there is a checkbox labeled 'Enable Hot Standby' which is checked with a blue square. At the bottom left, the word 'Mode' is displayed in bold. To the right of 'Mode' is a dropdown menu with 'Primary' selected and a downward arrow icon.

Step2. Set up hot standby for secondary server

1. Log in to another Yeastar Remote Management platform, go to Maintenance > Hot Standby.
2. Select the checkbox of Enable Hot standby.
3. Set up the secondary server.

- a. In the Mode drop-down list, select Secondary.

The Remote Management platform will work as the secondary server.

- b. Configure server information.

- Primary Server Hostname: Specify a [hostname \(on page 44\)](#) to help you identify the primary server.
- Secondary Server Hostname: Specify a [hostname \(on page 44\)](#) to help you identify the secondary server.
- Primary Server IP Address: Enter the IP address of the primary server.
- Access Code: Enter the same access code as that is configured on primary server.

- c. Configure virtual IP.

- Virtual IP Address: Enter the same virtual IP address as that is configured on primary server.
- Subnet Mask / IPv6 Prefix: Enter subnet mask (IPv4) or prefix (IPv6) .
- Virtual Gateway: Enter the same gateway address as that is configured on primary server.
- Network Connection Detection: Enter the same gateway address as that is configured on primary server.

- d. Configured advanced settings that will work when the server runs as a standby system.

- Keep Alive(s): Define the frequency to send heartbeat keep-alive packets.

The default value is 2 seconds, which means that the standby server sends packets every 2 seconds to detect whether the primary server is alive or not.

- Dead Time(s): Define the maximum time interval before the primary server responds to the standby server.

The default value is 120 seconds. If the standby server receives no response after timeout, it takes over automatically.



Note:

Set the Dead Time longer than the server rebooting time, or the standby server will take over when the primary server is rebooting.

e. Click Save.

<input checked="" type="checkbox"/> Enable Hot Standby	
Mode	Secondary
Server Information	
Primary Server Hostname	Host
Secondary Server Hostname	Standby
Primary Server IP Address	2201:c322:1111:2c6a::1015
Access Code	*****
Advanced	
Keep Alive(s)	2
Dead Time(s)	120
Virtual IP Address	
Virtual IP Address	2201:c322:1111:2c6a::1014
Subnet Mask	64
Virtual Gateway	2201:c322:1111:2c6a::
Network Connection Detection	2201:c322:1111:2c6a::

4. In the pop-up dialog box, click Yes to reboot.

When the server boots up, the Remote Management Server works as the secondary server, you can check configurations and data of the primary server on it.



Note:

Any operations on the secondary server would fail. To change server settings, go to the primary server to configure.

Standby	
<input checked="" type="checkbox"/> Enable Hot Standby	
Mode	Secondary

Step3. Test if hot standby works

1. On primary server, [add a device and connect to it \(on page 8\)](#).
2. On secondary server, check if the device is synchronized.

**Note:**

The password setting is synchronized with that of the primary server, so you need to use the same login password as the primary server to log in.

If the device is synchronized, the hot standby works.

Primary Server Takes over the System from Secondary Server

The secondary server automatically and instantly takes over if the primary server goes down. This topic describes how to manually let the primary server take over the Remote Management system from the secondary server.

Prerequisites

- You have repaired the primary server.
- The secondary server has taken over the Remote Management system and is in "Active" status.

The following figure shows the status of the secondary server.

Active

Remote Management Portal Primary Server not detected. Please check if your Primary Server is up and running properly.

☒ Enable Hot Standby

Mode Secondary ▼

Procedure

1. Log in to the web interface of the primary server, go to Maintenance > Hot Standby.
2. Click Fixup.

The primary server starts synchronizing data.

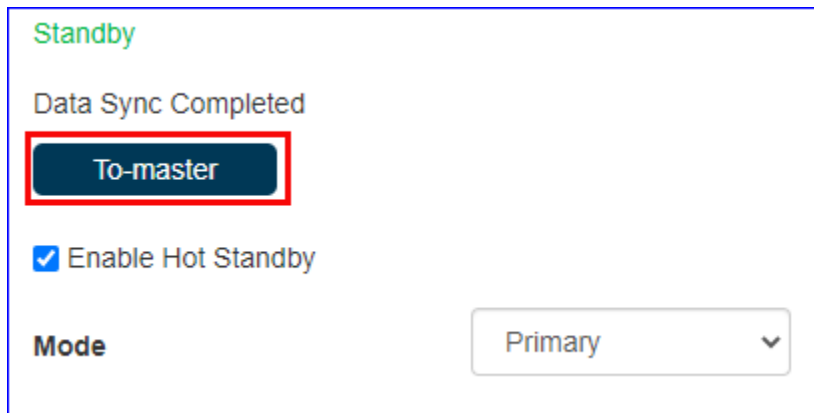
Unknown

Fixup

☒ Enable Hot Standby

Mode Primary ▼

3. After data synchronization completes, click To-master.



Standby

Data Sync Completed

To-master

☒ Enable Hot Standby

Mode Primary

Result

- The primary server takes over the system and status is changed to "Active".
- The secondary server reboots automatically and status is changed to "Standby".

Set Alarm Notification of Hot Standby

This topic describes how to set alarm notification of hot standby.

Background information

To keep informed of hot standby status of Remote Management Server or PBX devices, you can enable alarm notification. If a server or a PBX device is abnormal, you can receive email notification. The supported alarms are as follows:

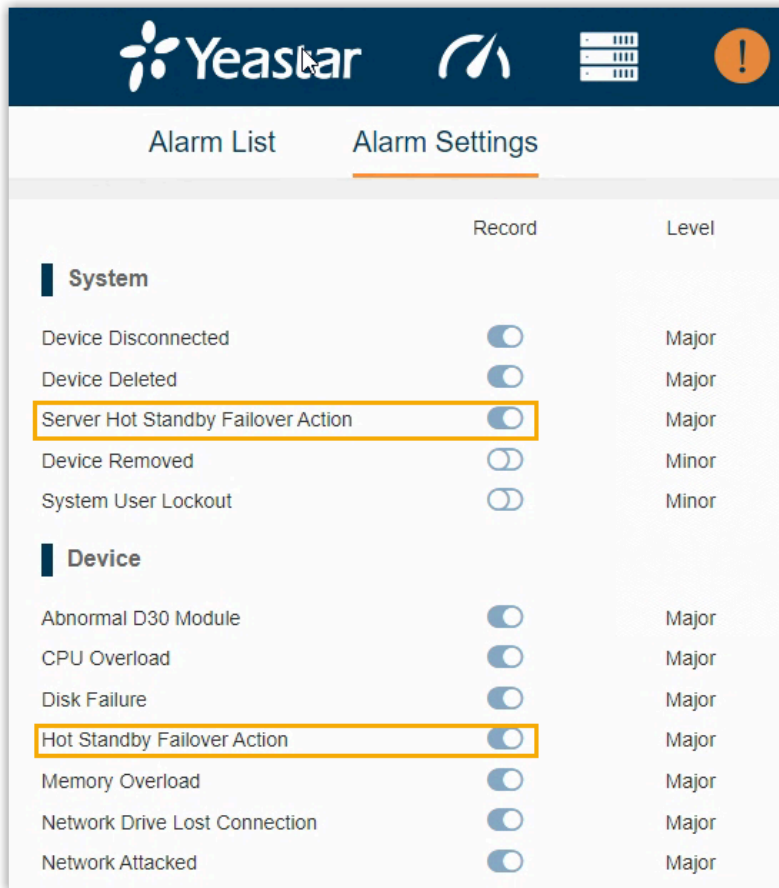
- Server Hot Standby Failover Action: The alarm indicates the failover action of Remote Management Server.
- Hot Standby Failover Action: The alarm indicates the failover action of PBX devices.

Prerequisites

- You have [set up email server \(on page 25\)](#).
- You have [enabled Alarm to Email feature \(on page 28\)](#).

Procedure

1. Go to Alarm > Alarm Settings.
2. Enable notification for the events.



Result

When an alarm occurs, the followings can be achieved:

- The alarm will be recorded in Alarm List.
- A notification email will be sent to your email address.

Reference

Appendix

We provide detailed information about the user name and password, the personal data, the ports, and the communication matrix that are used or collected when you use Remote Management, as well as how to harden security of Remote Management.

For more information, see the following:

- [Appendix 1: User Name & Password, Personal Data, Ports, Communication Matrix](#)
- [Appendix 2: Security Hardening Policy](#)

Yeastar Remote Management Security Hardening Policy

Content

1. Host Security	3
1.1. Upgrade the System to the Latest Version	3
1.1.1. Upgrade Ubuntu from 18.04.5 to 18.04.6	3
1.1.2. Upgrade Dependent Package	3
1.2. Fix Host Vulnerability	4
1.2.1. Nginx	4
1.2.2. PHP	5
1.2.3. Tomcat	5
1.2.4. MySQL	6
1.2.5. Redis	7
1.2.6. OpenSSH	7
1.2.7. Java	8
1.3. Disable debugging tools	9
1.4. SSH Security	9
1.4.1. Disable service accounts login	10
1.4.2. Restrict system accounts login	10
1.4.3. Fail2Ban	11
1.5. Run External Program as Non-root User	12
1.5.1. Nginx service	12
1.5.2. PHP service	12
1.5.3. Tomcat service	12
1.5.4. MySQL service	12
1.5.5. Redis service	13
1.5.6. Stun Server service	13
1.6. File system	13
1.6.1. Modify umask	13
1.6.2. Modify file permission	13
1.7. System parameters	14
1.8. Add Firewall	15
2. Web Security	15
2.1. Update WEB service module	15
2.2. Use TLSv1.3	15
3. Database Security	15
4. Third-party Scanning	15
5. Abatement Measures	15
5.1. Nginx Service	16
5.2. SSH Service	16

1. Host Security

1.1. Upgrade the System to the Latest Version

1.1.1. Upgrade Ubuntu from 18.04.5 to 18.04.6

```
root@huawei-mgt:~# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.6 LTS
Release:        18.04
Codename:       bionic
root@huawei-mgt:~# uname -a
Linux huawei-mgt 4.15.0-197-generic #208-Ubuntu SMP Tue Nov 1 17:23:37 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

1.1.2. Upgrade Dependent Package

```
root@huawei-mgt:~# apt upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@huawei-mgt:~# apt update
Hit:1 http://cn.archive.ubuntu.com/ubuntu bionic InRelease
Get:2 http://cn.archive.ubuntu.com/ubuntu bionic-updates InRelease [88.7 kB]
Get:3 http://cn.archive.ubuntu.com/ubuntu bionic-backports InRelease [83.3 kB]
Get:4 http://cn.archive.ubuntu.com/ubuntu bionic-security InRelease [88.7 kB]
Fetched 261 kB in 3s (89.0 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
All packages are up to date.
root@huawei-mgt:~#
```

1.2. Fix Host Vulnerability

- Upgrade dependent software to the latest version
- Upgrade third-party software to the latest version
- Vulnerability scanner: <https://nvd.nist.gov/vuln/search>

1.2.1. Nginx

- Conclusion: Passed, no vulnerability found (2022.10.25)
- Version 1.22.1
- Validation: nginx -V
- NVD: <https://nvd.nist.gov/products/cpe/search/results?namingFormat=2.3&keyword=nginx+1.22.1>

```
root@huawei-mgt:~# nginx -V
nginx version: nginx/1.22.1
built by gcc 7.5.0 (Ubuntu 7.5.0-3ubuntu1~18.04)
built with OpenSSL 1.1.1k 25 Mar 2021 (running with OpenSSL 1.1.1 11 Sep 2018)
TLS SNI support enabled
configure arguments: --prefix=/usr/share/nginx --with-http_ssl_module --with-pcre=/usr --with-zlib=/usr --with-http_realip_module --with-http_sub_module --with-http_v2_module
```

Q Search Results (Refine Search)

Search Parameters: There are 0 matching records.

- Keyword: nginx 1.22.1
- CPE Status: FINAL
- CPE Naming Format: 2.3

Vendor	Product	Version	Update	Edition	Language
--------	---------	---------	--------	---------	----------

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Twitter Facebook LinkedIn YouTube RSS Email

1.2.2. PHP

- Conclusion: Passed, no vulnerability found (2022.10.25)
- Validation: php --version
- NVD: <https://nvd.nist.gov/products/cpe/search/results?namingFormat=2.3&keyword=php+7.4.33>

```
root@huawei-mgt:~# php --version
PHP 7.4.33 (cli) (built: Dec 11 2022 03:23:03) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
```

PRODUCTS CPE SEARCH

Q Search Results (Refine Search)

Search Parameters: There are 0 matching records.

- Keyword: php 7.4.33
- CPE Status: FINAL
- CPE Naming Format: 2.3

Vendor	Product	Version	Update	Edition	Language
--------	---------	---------	--------	---------	----------

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Twitter Facebook LinkedIn YouTube RSS Email

1.2.3. Tomcat

- Conclusion: Passed, no vulnerability found (2022.10.25)
- Version: 9.0.8
- Validation: tar -xf catalina.jarorg/apache/catalina/util/ServerInfo.class
- NVD: <https://nvd.nist.gov/products/cpe/search/results?namingFormat=2.3&keyword=tomcat+9.0.68>


```
root@huawei-mgt:~# ll /ysdata/server/tomcat
lrwxrwxrwx 1 root root 35 Oct 25 09:24 /ysdata/server/tomcat -> /ysdata/server/apache-tomcat-9.0.68/
```







Search Results (Refine Search)

Search Parameters: There are 0 matching records.

- Keyword: tomcat 9.0.68
- CPE Status: FINAL
- CPE Naming Format: 2.3

Vendor	Product	Version	Update	Edition	Language
--------	---------	---------	--------	---------	----------


NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Fix history:

3.2.4. Apache Tomcat: Low: Apache Tomcat EncryptInterceptor DoS (CVE-2022-29885) (apache-tomcat-cve-2022-29885)

3.2.23. Apache Tomcat: Low: Local Privilege Escalation (CVE-2022-23181) (apache-tomcat-cve-2022-23181)

3.2.24. Apache Tomcat: Low: Apache Tomcat XSS in examples web application (CVE-2022-34305) (apache-tomcat-cve-2022-34305)

1.2.4. MySQL

- Conclusion: Passed, no vulnerability found (2022.10.25)
- Version: 8.0.31
- Validation: mysql --version
- NVD: <https://nvd.nist.gov/products/cpe/search/results?namingFormat=2.3&keyword=mysql+8.0.31>


```
root@huawei-mgt:~# mysql --version
mysql Ver 8.0.31 for Linux on x86_64 (Source distribution)
```







Search Results (Refine Search)

Search Parameters: There are 0 matching records.

- Keyword: mysql 8.0.31
- CPE Status: FINAL
- CPE Naming Format: 2.3

Vendor	Product	Version	Update	Edition	Language
--------	---------	---------	--------	---------	----------


NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Fix history:

Oracle MySQL Vulnerability: CVE-2021-35637 (oracle-mysql-cve-2021-35637)

Oracle MySQL Vulnerability: CVE-2021-35638 (oracle-mysql-cve-2021-35638)

Oracle MySQL Vulnerability: CVE-2022-21253 (oracle-mysql-cve-2022-21253)

Oracle MySQL Vulnerability: CVE-2022-21256 (oracle-mysql-cve-2022-21256)

Oracle MySQL Vulnerability: CVE-2022-21368 (oracle-mysql-cve-2022-21368)

Oracle MySQL Vulnerability: CVE-2021-35610 (oracle-mysql-cve-2021-35610)

Oracle MySQL Vulnerability: CVE-2021-35612 (oracle-mysql-cve-2021-35612)

Oracle MySQL Vulnerability: CVE-2022-21254 (oracle-mysql-cve-2022-21254)

Oracle MySQL Vulnerability: CVE-2022-21265 (oracle-mysql-cve-2022-21265)

Oracle MySQL Vulnerability: CVE-2022-21278 (oracle-mysql-cve-2022-21278)

Oracle MySQL Vulnerability: CVE-2022-21301 (oracle-mysql-cve-2022-21301)

Oracle MySQL Vulnerability: CVE-2022-21351 (oracle-mysql-cve-2022-21351)

Oracle MySQL Vulnerability: CVE-2022-21363 (oracle-mysql-cve-2022-21363)

Oracle MySQL Vulnerability: CVE-2022-21367 (oracle-mysql-cve-2022-21367)

Oracle MySQL Vulnerability: CVE-2022-21378 (oracle-mysql-cve-2022-21378)

Oracle MySQL Vulnerability: CVE-2022-21425 (oracle-mysql-cve-2022-21425)

Oracle MySQL Vulnerability: CVE-2022-21479 (oracle-mysql-cve-2022-21479)

Oracle MySQL Vulnerability: CVE-2021-35602 (oracle-mysql-cve-2021-35602)

... (80)

Oracle MySQL Vulnerability: CVE-2022-21451 (oracle-mysql-cve-2022-21451)

Oracle MySQL Vulnerability: CVE-2022-21460 (oracle-mysql-cve-2022-21460)

1.2.5. Redis

- Conclusion: Passed, no vulnerability found (2022.10.25)
- Version: 6.2.7
- Validation: /ysdata/server/redis/bin/redis-server --version
- NVD: <https://nvd.nist.gov/products/cpe/search/results?namingFormat=2.3&keyword=redis+6.2.7>

```
root@huawei-mgt:~# /ysdata/server/redis/bin/redis-server --version
Redis server v=6.2.7 sha=00000000:0 malloc=jemalloc-5.1.0 bits=64 build=9cbdfdc64cbeef8a
```

1.2.6. OpenSSH

- Conclusion: Passed, no vulnerability passed (2022.10.25)

- Version: 9.0p1
- Validation: /ysdata/server/openssh/sbin/sshd -v

```
root@huawei-mgt:~# /ysdata/server/ssh/sbin/sshd -v
unknown option -- v
OpenSSH_9.0p1, OpenSSL 1.1.1 11 Sep 2018
usage: sshd [-46DdeiqTt] [-C connection_spec] [-c host_cert_file]
           [-E log_file] [-f config_file] [-g login_grace_time]
           [-h host_key_file] [-o option] [-p port] [-u len]
```

Fix history:

```
3.2.5. OpenSSH Vulnerability: CVE-2016-20012 (openbsd-openssh-cve-2016-20012)
3.2.6. OpenSSH Vulnerability: CVE-2020-14145 (openbsd-openssh-cve-2020-14145)
3.2.7. OpenSSH Vulnerability: CVE-2021-41617 (openbsd-openssh-cve-2021-41617)
3.3.1. OpenSSH Vulnerability: CVE-2021-36368 (openbsd-openssh-cve-2021-36368)
```

1.2.7. Java

- Conclusion: Passed, no vulnerability found (2022.12.09)
- Version: 1.8.0_352-b08
- Validation: /ysdata/server/java/bin/java -version

```
root@huawei-mgt:~# /ysdata/server/java/bin/java -version
openjdk version "1.8.0_352"
OpenJDK Runtime Environment (Temurin)(build 1.8.0_352-b08)
OpenJDK 64-Bit Server VM (Temurin)(build 25.352-b08, mixed mode)
```

Fix history:

3.2.6. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21271) (jrevuln-cve-2022-21271)

3.2.7. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21282) (jrevuln-cve-2022-21282)

3.2.8. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21291) (jrevuln-cve-2022-21291)

3.2.9. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21293) (jrevuln-cve-2022-21293)

3.2.10. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21294) (jrevuln-cve-2022-21294)

3.2.11. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21296) (jrevuln-cve-2022-21296)

3.2.12. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21299) (jrevuln-cve-2022-21299)

3.2.13. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21305) (jrevuln-cve-2022-21305)

3.2.14. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21340) (jrevuln-cve-2022-21340)

3.2.15. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21341) (jrevuln-cve-2022-21341)

3.2.16. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21349) (jrevuln-cve-2022-21349)

3.2.17. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21360) (jrevuln-cve-2022-21360)

3.2.18. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21365) (jrevuln-cve-2022-21365)

3.2.19. Java CPU April 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21426) (jrevuln-cve-2022-21426)

3.2.20. Java CPU April 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21434) (jrevuln-cve-2022-21434)

3.2.21. Java CPU April 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21476) (jrevuln-cve-2022-21476)

3.2.22. Java CPU April 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21496) (jrevuln-cve-2022-21496)

3.2.25. Java CPU January 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21248) (jrevuln-cve-2022-21248)

3.2.26. Java CPU April 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21443) (jrevuln-cve-2022-21443)

3.2.27. Java CPU July 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21540) (jre-vulncve-2022-21540)

3.2.28. Java CPU July 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-21541) (jre-vulncve-2022-21541)

3.2.29. Java CPU July 2022 Oracle Java SE, Oracle GraalVM Enterprise Edition vulnerability (CVE-2022-34169) (jre-vulncve-2022-34169)

Spring framework vulnerability:

3.2.30. VMware Spring: CVE-2022-22950: Spring Expression DoS Vulnerability (spring-cve-2022-22950)

1.3. Disable debugging tools

- Disable tcpdump
- Disable strace
- Disable trace
- Disable gdb
- Disable gcc
- Disable netcat
- Disable arthas
- Disable coredump

1.4. SSH Security

- Disable service accounts login
- Restrict system accounts login
- Disable login with blank password
- Disable insecure encryption algorithms
- Set authorization limit
- Disable user environment variables
- Disable X11 forwarding
- Enable fail2ban to limit login attempts

1.4.1. Disable service accounts login

Configuration file: `/etc/passwd`

```
sshd:x:999:999:sshd privsep:/home/sshd:/bin/false
mysql:x:1000:1000::/home/mysql:/sbin/nologin
redis:x:1001:1001::/home/redis:/bin/false
tunnel:x:1002:1002::/home/tunnel:/bin/false
stund:x:1003:1003::/home/stund:/bin/false
_chrony:x:110:113:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
```

1.4.2. Restrict system accounts login

Configuration file: `/etc/ssh/sshd_config`


```
1  # Restrict SSH login to the host
2
3  # Restrict login to specific user groups only
4  AllowGroups tunnel sudo
5
6  # Disable root login
7  PermitRootLogin no
8
9  # Disable login with blank password
10 PermitEmptyPasswords no
11
12 # Enable password authentication
13 PasswordAuthentication yes
14
15 # Disable host-based authentication
16 HostbasedAuthentication no
17
18 # Disable insecure encryption algorithms
19
20 KexAlgorithms -diffie-hellman-group14-sha1
21 HostKeyAlgorithms -ssh-rsa
22 Macs -hmac-sha1*,umac-64*
```

Note: Must allow login of tunnel user group, otherwise the remote tunnel management would not work.

1.4.3. Fail2Ban

```
root@huawei-mgt:~# cat /etc/fail2ban/jail.d/defaults-debian.conf
[sshd]
enabled = true
maxretry = 6
bantime = 10m
root@huawei-mgt:~# systemctl status fail2ban.service
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2022-12-05 04:37:32 EET; 4 days ago
     Docs: man:fail2ban(1)
  Main PID: 1304 (fail2ban-server)
    Tasks: 3 (limit: 2283)
   CGroup: /system.slice/fail2ban.service
           └─1304 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

Dec 05 04:37:31 huawei-mgt systemd[1]: Starting Fail2Ban Service...
Dec 05 04:37:32 huawei-mgt systemd[1]: Started Fail2Ban Service.
Dec 05 04:37:38 huawei-mgt fail2ban-server[1304]: Server ready
```

1.5. Run External Program as Non-root User

External listener of the current host (screenshot: Hot Standby disabled)

```
root@huawei-mgt:~# netstat -nltp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN      1097/systemd-resolv
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      1428/sshd: /ysdata/
tcp        0      0 0.0.0.0:8443           0.0.0.0:*               LISTEN      24264/nginx: master
tcp        0      0 0.0.0.0:443            0.0.0.0:*               LISTEN      24264/nginx: master
tcp        0      0 127.0.0.1:9000         0.0.0.0:*               LISTEN      24209/php-fpm: mast
tcp        0      0 0.0.0.0:3306           0.0.0.0:*               LISTEN      4853/mysqld
tcp        0      0 127.0.0.1:6379         0.0.0.0:*               LISTEN      36083/redis-server
tcp        0      0 0.0.0.0:80             0.0.0.0:*               LISTEN      24264/nginx: master
tcp6       0      0 127.0.0.1:8080         :::*                    LISTEN      24225/java
udp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN      1097/systemd-resolv
udp        0      0 127.0.0.1:323         0.0.0.0:*               LISTEN      1396/chronyd
udp        0      0 172.16.5.98:3478       0.0.0.0:*               LISTEN      5069/stunserver
udp6       0      0 :::1:323              :::*                    LISTEN      1396/chronyd
```

1.5.1. Nginx service

Use child process using fork() system call, and www-data account for external service.

```
root@huawei-mgt:~# ps aux | grep "nginx" | grep -v "grep"
root      24264  0.0  0.0 39656 1128 ?        Ss   Dec05   0:00 nginx: master process /ysdata/server/nginx/sbin/nginx
www-data  24266  0.0  1.5 71168 30340 ?        S    Dec05   0:00 nginx: worker process
```

1.5.2. PHP service

Use internal listener and does not directly provide services for external applications; Use child process using fork() system call, and www-data account for external service.

```
root@huawei-mgt:~# ps aux | grep "php" | grep -v "grep"
root      24209  0.0  0.5 189624 10220 ?        Ss   Dec05   0:11 php-fpm: master process (/ysdata/server/php/etc/php-fpm.conf)
www-data  24215  0.0  0.4 191920 10068 ?        S    Dec05   0:00 php-fpm: pool www
www-data  24216  0.0  0.4 191920 10072 ?        S    Dec05   0:00 php-fpm: pool www
```

1.5.3. Tomcat service

Use internal listener and does not directly provide services for external applications as Tomcat requires some high-privilege execution.

1.5.4. MySQL service

Use child process using fork() system call, and use mysql account to provide services for external applications.

```
root@huawei-mgt:~# ps aux | grep "mysqld" | grep -v "grep"
root      4072  0.0  0.0 4636 1672 ?        S    Dec05   0:00 /bin/sh /ysdata/server/mysql/bin/mysqld_safe --datadir=/ysdata/server/mysql/data --pid-file=/ysdata/se
rver/mysql/data/mysql.pid
mysql     4853  0.2  6.9 988916 139140 ?        Sl   Dec05  14:58 /ysdata/server/mysql/bin/mysqld --basedir=/ysdata/server/mysql --datadir=/ysdata/server/mysql/data --p
login-dir=/ysdata/server/mysql/lib/plugin --user=mysql --log-error=/ysdata/server/mysql/data/mysql-error.log --open-files-limit=65535 --pid-file=/ysdata/server/mysql/da
ta/mysql.pid --socket=/tmp/mysql.sock --port=3306
```

1.5.5. Redis service

Use internal listener and only for internal use.

```
root@huawei-mgt:~# ps aux | grep "redis" | grep -v "grep"
redis    36083  0.0  0.2  61492  5408 ?        Ssl  09:32   0:00 /ysdata/server/redis/bin/redis-server 127.0.0.1:6379
```

1.5.6. Stun Server service

Run with stund account with non-root user privileges.

```
root@huawei-mgt:~# ps aux | grep "stund" | grep -v "grep"
stund    5069  0.0  0.2  33292  5904 ?        Ssl  Dec05   0:00 /ysdata/server/stund/stunserver --configfile /ysdata/server/stund/stun.conf
```

1.6. File system

1.6.1. Modify umask

Add `umask 027` in `/etc/profile` .

```
root@huawei-mgt:~# cat /etc/profile | grep "umask" | grep -v "grep"
umask 0027
```

1.6.2. Modify file permission

Modify file permission to achieve granular permission control.

- Nginx directory access restriction: For the temporary directory, restrict the read and write access to www-data account only; For the rest of the directory, restrict the read and write access to root account.
- PHP directory access restriction: Only www-data can read, write, execute.
- Tomcat directory access restriction: Only www-data can read and write.
- MySQL directory access restriction: Only mysql account can read and write.
- Redis directory access restriction: Only redis account can read and write.

Restrict the read and write capability of mounted disk

```
1  cp -v /usr/share/systemd/tmp.mount /etc/systemd/system/
2  systemctl daemon-reload
3  systemctl --now enable tmp.mount
4
5  # validation method
6  # findmnt /tmp
7  TARGET SOURCE FSTYPE OPTIONS
8  /tmp      tmpfs      tmpfs    rw,nosuid,nodev
9
10
11  echo "tmpfs /dev/shm tmpfs nosuid,nodev,noexec 0 0" >> /etc/fstab
12  mount -o remount,nosuid,nodev,noexec /dev/shm
13
14  # validation method
15  findmnt -n /dev/shm | grep -v noexec
```

1.7. System parameters

- Change kernel parameters

```
1  net.ipv4.conf.all.send_redirects = 0
2  net.ipv4.conf.default.send_redirects = 0
3  net.ipv4.conf.all.send_redirects = 0
4  net.ipv4.conf.default.send_redirects = 0
5  net.ipv4.conf.all.accept_source_route = 0
6  net.ipv4.conf.default.accept_source_route = 0
7  net.ipv4.conf.all.accept_source_route = 0
8  net.ipv4.conf.default.accept_source_route = 0
9  net.ipv4.conf.all.accept_redirects = 0
10 net.ipv4.conf.default.accept_redirects = 0
11 net.ipv6.conf.all.accept_redirects = 0
12 net.ipv6.conf.default.accept_redirects = 0
13 net.ipv4.conf.all.secure_redirects = 0
14 net.ipv4.conf.default.secure_redirects = 0
15 net.ipv4.conf.all.log_martians = 1
16 net.ipv4.conf.default.log_martians = 1
17 net.ipv4.icmp_echo_ignore_broadcasts = 1
18 net.ipv4.icmp_ignore_bogus_error_responses = 1
19 net.ipv4.conf.all.rp_filter = 1
20 net.ipv4.conf.default.rp_filter = 1
21 net.ipv4.tcp_syncookies = 1
```

1.8. Add Firewall

In addition to SSH login protection, also use iptables to strengthen the security.

2. Web Security

Note: For other database security policies, refer to the appendix.

2.1. Update WEB service module

- Upgrade Tomcat service to the latest version
- Fix the vulnerability in Spring framework
- Fix the vulnerability in third-party dependent library

2.2. Use TLSv1.3

- Change NGINX proxy to TLSv1.3, and remove TLSv1.2
- Validation method:

```
1 # SSL probe through another service that has nmap installed
2 nmap --script "ssl-enum-ciphers" 172.16.5.98 -p 443
```

3. Database Security

Upgrade MySQL service to the latest version.

Note: For other database security policies, refer to the appendix.

4. Third-party Scanning

- Upgrade third-party libraries to the latest version
- Upgrade third-party software to the latest versions (Nginx/ Tomcat / PHP / MySQL / Redis)

5. Abatement Measures

Yeastar reserves the right not to be responsible for any security breach, data loss, or unavailability of services caused by incorrect modifications to the following mitigation measures.

Note: For other abasement measures, refer to the appendix.

5.1. Nginx Service

Improved NGINX security in this iteration. If users' web browsers don't support TLS v1.3 protocol, you can downgrade by the following method:

- Configuration file `/ysdata/server/nginx/conf/nginx.conf`

```
1  # Add TLSv1.2
2  ssl_protocols TLSv1.2 TLSv1.3;
```

- Restart NGINX service

```
1  systemctl restart nginx.service
```

5.2. SSH Service

Improved SSH security in this iteration. If users access the system via SSH, or if some users are unable to log in to the system, you can downgrade by the following method:

- Configuration file `/etc/ssh/sshd_config`

```
1  # Modify the users allowed to login
2  AllowGroups tunnel sudo
```

Note: Do not delete the tunnel account as it is necessary to create a remote tunnel. If you specify both AllowUsers and AllowGroups, it may result in login failure.