

Yealink Management Cloud Service for RPS Enterprise Administrator Guide V3.7.0.1

Contents

About This Guide.....	4
Summary of Changes.....	4
Changes for Release 37, Guide Version V3.7.0.1.....	4
Changes for Release 36, Guide Version V3.6.0.30.....	4
Changes for Release 35, Guide Version V3.6.0.20.....	4
Changes for Release 35, Guide Version V3.5.0.10.....	4
Port Requirements.....	5
Logging into/Logging out of YMCS for RPS Enterprise.....	5
Logging into YMCS for RPS Enterprise.....	5
Logging out of YMCS for RPS Enterprise.....	6
Managing Administrator Accounts.....	6
Managing Sub-Administrator Accounts.....	6
Adding Sub-Administrator Accounts.....	6
Resetting the Passwords of the Sub-Administrator Accounts.....	7
Deleting Sub-Administrator Accounts.....	7
Editing the Information of the Administrator Account.....	8
Changing the Login Password.....	8
Forget the Login Password?.....	8
Enabling Login Protection.....	8
Device and Server Overview.....	9
Managing Servers.....	9
Adding Servers.....	10
Editing Servers.....	10
Searching for Servers.....	11
Deleting Servers.....	11
Managing Devices.....	11
Adding Devices.....	11
Importing Devices.....	12
Exporting Devices.....	13
Editing the Device Information.....	13
Resetting Connections of the Devices.....	13
Resetting the Device Connection.....	13
Resetting the Connections of a Batch of the Devices.....	13
Migrating Devices to Another Server.....	14
Checking the Linking Status Between the Device and the Server.....	14

Deleting Devices.....	14
Viewing Operation Logs.....	15
Applying for the AccessKey.....	15
Managing IP Allowlist.....	15
Adding an IP Address to the Allowlist.....	15
Editing the IP Allowlist.....	16
Deleting an IP Address.....	16
Managing the Intercepted Record.....	16
Moving the Blocked IP to the Allowlist.....	16
Resetting the Connections of the Blocked IP.....	17

About This Guide

Yealink Management Cloud Service integrates the RPS function, allowing to add servers and devices on Yealink Management Cloud Service for RPS. After the device is powered on for the first time, the device will be redirected to the server via RPS function.

This guide provides operations for administrators to use Yealink Management Cloud Service for RPS.



Note: If you are an old RPS user, the data on the old RPS platform will be migrated to the RPS management platform.

Summary of Changes

- [Changes for Release 37, Guide Version V3.7.0.1](#)
- [Changes for Release 36, Guide Version V3.6.0.30](#)
- [Changes for Release 35, Guide Version V3.6.0.20](#)
- [Changes for Release 35, Guide Version V3.5.0.10](#)

Changes for Release 37, Guide Version V3.7.0.1

Starting from this version, we apply a new user interface design.

Changes for Release 36, Guide Version V3.6.0.30

The following sections are new for this version:

- [Enabling Login Protection](#)

Major updates have occurred to the following sections:

- [Logging into YMCS for RPS Enterprise](#)

Changes for Release 35, Guide Version V3.6.0.20

The following sections are new for this version:

- [Port Requirements](#)

Changes for Release 35, Guide Version V3.5.0.10

The following sections are new for this version:

- [Managing IP Allowlist](#)
- [Managing the Intercepted Record](#)

Major updates have occurred to the following sections:

- [Managing Devices](#)

Port Requirements

You should open port 443 and 8443 for YMCS for RPS Enterprise. We do not recommend that you modify these ports.

Port	Description
443	It is used for accessing YMCS for RPS Enterprise and reporting the device information to the platform via HTTPS.
8443	It is used for calling the API of YMCS for RPS Enterprise.

Logging into/Logging out of YMCS for RPS Enterprise

- [Logging into YMCS for RPS Enterprise](#)
- [Logging out of YMCS for RPS Enterprise](#)

Logging into YMCS for RPS Enterprise

The accounts on the RPS management platform are created by distributors or resellers, and the login username and password are obtained from the email.

Procedure

1. Enter the device management platform address in the browser address box, and then press Enter.
2. Optional: Select the desired language from the drop-down menu of **Language** in the top-right corner.
3. Enter your username and the password and click **Login**.
4. If you want to enable the login protection feature for dual identify authentication, refer to [Enabling Login Protection](#).

If you enable the login protection of **Email**, the page is shown as below:

Identity Verification

The verification code has been sent to the mailbox bound to the account.

R3MO8Z
(Resend 40)

OK

« Return

If you enable the login protection of **Virtual MFA Device**, the page is shown as below:

Identity Verification

Please open Google Authenticator on your phone to get a 6-digit verification code.

634482

OK

« Return

Logging out of YMCS for RPS Enterprise

If you want to use other accounts to log in, you can log out of the current account. Additionally, if the system has been idle on either page for more than 30 minutes, the system will log out of your account automatically and return to the Login page.

Procedure

Hover your mouse over the company name in the top-right of corner, and then click **Exit**.

You will log out of the current account and return to the Login page.

Managing Administrator Accounts

This chapter provides the basic operations for the administrator account.

- [Managing Sub-Administrator Accounts](#)
- [Editing the Information of the Administrator Account](#)
- [Changing the Login Password](#)
- [Forget the Login Password?](#)
- [Enabling Login Protection](#)

Managing Sub-Administrator Accounts

You can add the sub-administrator account, and assign different data permissions or feature permissions to every sub-administrator account.

- [Adding Sub-Administrator Accounts](#)
- [Resetting the Passwords of the Sub-Administrator Accounts](#)
- [Deleting Sub-Administrator Accounts](#)

Adding Sub-Administrator Accounts

Procedure

1. Click **System Settings > Sub Account Management**.
2. Click **Add**.
3. Enter the corresponding information of the sub-administrator.

Account Info

* Register Email

Contact

Phone Number

4. In the **Account Permission** field, enable the corresponding permission for this account.

Account Permission

Function Permission

☒ All

☒ Device Management

☐ Readonly

☒ Add/Edit Device

☒ Delete

☒ Check Device

☒ Export Device

☒ reset Connection

☐ Server Management

☐ Readonly

☐ Add/Edit Server

5. In the **Data Permission** field, select the corresponding server, so that the server and the device linked to this server can be managed by this account.

Data Permission

☒ 1 selected / ...

Server URL	Number of b...	Server name	Server URL	Number of b...	
Autop	http://10.82...	2	Autop	http://10.82...	2


6. Click **OK**.

Results

The account information will be sent to the sub-administrator's mailbox.

Resetting the Passwords of the Sub-Administrator Accounts

Procedure

1. Click **System Settings > Sub account management**.
2. Click  beside the targeted sub-administrator account.
If you enable SMTP mailbox, the reset password will be sent to the mailbox of sub-administrator.

Deleting Sub-Administrator Accounts

Procedure

1. Click **System Management > Sub Account Management**.
2. Select the desired account.
3. Click **Delete**.
4. Click **OK** according to the prompts.

Editing the Information of the Administrator Account

You can edit the information for your account, for example the contact name, the phone number and the country, so that your distributors or resellers can contact you. The administrator mailbox is used to receive alarms and the account information. If you need to change your registered email, contact your distributor or reseller.

Procedure

1. Hover your mouse over the account avatar in the top-right corner, and then click **Account Settings**.
2. Edit the administrator account in the corresponding field.
3. Click **Confirm**.

Changing the Login Password

To ensure the account security, we recommended that you change the password regularly.

Procedure

1. Hover your mouse over the account avatar in the top-right of corner, and then click **Account Settings**.
2. Click **Edit** beside the password.
3. Enter the current password and enter the new password twice.
4. Click **Confirm**.

Forget the Login Password?

If you forget the password, you can reset it via email.

Procedure

1. Click **Forget Password** on the Login page.
2. Enter the email and the verification code in the corresponding fields.
3. Click **OK**.
4. Click **OK** again according to the prompt.
5. After you receive the email for resetting the password, click the link in 10 minutes to reset the password.

Enabling Login Protection

For single factor authentication, the passwords are easily cracked by brute force. To solve that, YMCS supports multi-factor authentication (MFA), requiring users to pass two authentications before they can log into YMCS.

Procedure

1. Hover your mouse over the account avatar in the top-right corner of the page, and then click **Account Settings**.

2. In the **Login Protection** field, click **Edit**.

Login Protection

☐ Close

☐ Email

☒ Virtual MFA Device

* After the login protection is enabled, identity verification is required when logging in.

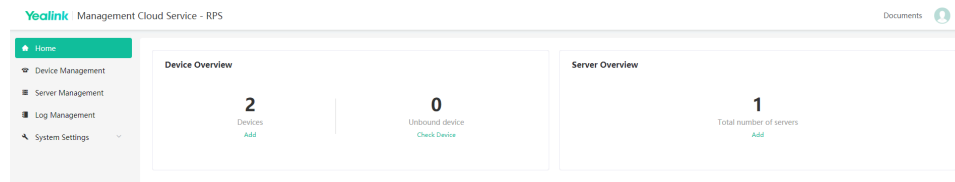
Next step Cancel

3. Select **Virtual MFA Device** or **Email**, complete the operation according to the on-screen prompts.

If the page prompts "Login expired, please log in again", you need to use the new verification method to complete the login.

Device and Server Overview

You can view the total number of devices and servers on the home page of RPS management platform.



Feature	Description
Device overview	<ul style="list-style-type: none"> Displays the total number of devices. Click Add to add devices. Displays the total number of the devices unlinked to the servers. Click Check Device to check linking status between the device and the server.
Server overview	Displays the total number of servers. Click Add to add servers.

Managing Servers

- [Adding Servers](#)
- [Editing Servers](#)
- [Searching for Servers](#)
- [Deleting Servers](#)

Adding Servers

If you want to save your configuration file on use your own server, you can add a server.

Procedure

1. Click **Server Management > Add Server**.
2. Set and save the parameters.

← Add Server

Basic Settings

1 * Server name
Autop
Enter the server name.

* Server URL
http://10.82.24.62/DM-CFG/Phoneautop.cfg
Enter the server URL.

User Name
autop
Enter the server user name and password.

Password

Trusted Certificates

Trusted Certificates File [Click to upload](#)
Only .cer/.pem/.crt/.der file is supported. Maximum size is 5M

Server Certificates

Server Certificate [Click to upload](#)
Only .cer/.pem/.crt/.der file is supported. Maximum size is 5M

Custom Certificates ☒ Close ☐ Enable

2 [Save](#) [Cancel](#)




Note:

- If the device needs to verify the server and requires a custom certificate, upload the trusted certificate.
- If the server needs to verify the device and requires a custom certificate, upload the server certificate.
- If the server requires the device to upload its custom certificate, enable **Custom Certificates**. It is disabled by default and the device will send the default certificate to the server for verification.

Editing Servers

Procedure

1. Click **Server Management**.
2. Click  beside the desired server.
3. Edit and save the parameters.

Searching for Servers

You can search for the server by entering the server name or the URL.

Procedure

1. Click **Server Management**.
2. Enter the server name or the URL in the search box.
3. Click **Search**.

The search results are displayed in the server list.

Deleting Servers

Procedure

1. Click **Server Management**.
2. Select the check boxes of the desired servers and click **Delete**.
3. Click **OK** according to the prompts.

Managing Devices

- [Adding Devices](#)
- [Importing Devices](#)
- [Exporting Devices](#)
- [Editing the Device Information](#)
- [Resetting Connections of the Devices](#)
- [Migrating Devices to Another Server](#)
- [Checking the Linking Status Between the Device and the Server](#)
- [Deleting Devices](#)

Adding Devices

When adding a device, if you select an added server and enter a unique server URL which is different from the URL of the added server, the RPS management platform performs the redirection according to the unique URL you entered. Otherwise, the platform performs the redirection according to the URL of the added server.

Procedure

1. Click **Device Management > Add**.

2. Set and save the parameters.

Add Device

* MAC
805ec0484b91 +
Enter the device MAC.

Server name
Autop
Enter the server name.

Unique Server URL
Please enter : **Optional: you can also associate a server URL with this device. For example, the URL of Yealink RPS server. Note that the unique server has a higher priority than the added server.**

Username
autop
Enter the server username and password.

Password

Remark
T525

Save **Cancel**

If it prompts that other enterprises use the MAC address you entered, check your MAC address or file an appeal to Yealink if necessary.

Importing Devices

If you want to quickly add multiple devices, you can import them in batch. You need to download the template, edit the information in the template and then import the template to YMCS.

Procedure

Click **Device Management > Import**.

Import

Server name: Itspdm
1

Tips: Please download the template and import the data as required **Download template** **2. Download the template and edit the parameter in it.**

Drag the file here or **Click to upload**

device_import_template_en.xls **3. Upload the template.**

4 **Upload** **Cancel**

Note: The file extension must be .xls or .xlsx (Excel format), and the maximum number of imported data cannot exceed 5000

Exporting Devices

You can export a batch of the device information to check the device backup information, or whether the device is sold and so on. If the device is linked to a server, it means the device is sold, otherwise it is not.


Procedure

1. Click **Device Management**.
2. In the top-right corner, click **Export**. The file will be saved in your local system.

Editing the Device Information

You can edit the device information, for example, the server or the unique server URL.

Procedure

1. Click **Device Management**.
2. Click  beside the desired device.
3. Edit and save the parameters.

Resetting Connections of the Devices

On the page of Device Management, you can reset the connection of single device or the connections of batch of the devices.

- [Resetting the Device Connection](#)
- [Resetting the Connections of a Batch of the Devices](#)

Resetting the Device Connection

Procedure

Click **Device Management**, select the desired device, and click **Reset**.

Resetting the Connections of a Batch of the Devices

About this task

If you want to quickly reset the connections of many devices, you can reset them in batch. You need to download the template, add a batch of the devices, and import the template to the device management platform.

Procedure

Click **Device Management** > **Batch Reset**.



Migrating Devices to Another Server

You can migrate a single device or multiple devices to another server at once.

Procedure

1. Click **Device Management**.
2. Select the check boxes of the desired devices.
3. Click **Migrate**.
4. Select the targeted server.
5. Click **Confirm**.

Checking the Linking Status Between the Device and the Server

About this task

You can check the device linking status, which contains the following:

- Bound: the device MAC address belongs to your enterprise and is linked to the server successfully.
- Unbound: the device MAC address belongs to your enterprise but is not linked to the server.
- The device MAC address belongs to other enterprises.
- The query fails: the device does not exist or cannot be found on YMCS.

Procedure

1. Click **Device Management > Check Device**.
2. Enter the device MAC and click **Confirm**.

Results

It shows the result of the device linking status.

If it prompts that other enterprises use the MAC address you entered, check your MAC address or file an appeal to Yealink(<https://ticket.yealink.com/>) if necessary.

Deleting Devices

Procedure

1. Click **Device Management**.
2. Select the desired devices.

3. Click **Delete**.
4. Click **OK** according to the prompts.

Viewing Operation Logs

Any operations on the platform will be recorded in the operation logs. You can view the operation log.

Procedure

1. Click **Log Management**.
2. You can select the start time and the end time, or enter the username/the IP address in the search box, to view the desired operation log.

Applying for the AccessKey

RPS device management platform allows the third parties to call for the API via the accesskey, which you should apply for.

Procedure

1. Click **System Management > API Service**.
2. Click **Acquire**.

Managing IP Allowlist

When the devices send the RPS requests, the server will check the identification of the devices. If the IP of the device is added in the IP allowlist, the server will trust the device.

- [Adding an IP Address to the Allowlist](#)
- [Editing the IP Allowlist](#)
- [Deleting an IP Address](#)

Adding an IP Address to the Allowlist

Procedure

1. Click **System Settings > IP Allowlist > Add**.

2. Enter the IP address and save it.


Add IP allowlist



* IP Address

Editing the IP Allowlist

Procedure

1. Click **System Settings** > **IP Allowlist**.
2. Click  on the right side of the desired item.
3. Edit and save the parameters.

Deleting an IP Address

Procedure

1. Click **System Settings** > **IP Allowlist**.
2. Select the desired item and click **Delete**.
3. Click **OK** to delete.

Managing the Intercepted Record

If the devices fail the identification authentication of the server, the devices will appear in the list of intercept records. You can view and manage the blocked devices on the page of Intercept Record. You can move the blocked devices to the allowlist or reset the connections of the blocked devices. After resetting the connections of the blocked devices, the server will trust the devices once.

- [Moving the Blocked IP to the Allowlist](#)
- [Resetting the Connections of the Blocked IP](#)


Moving the Blocked IP to the Allowlist

On the page of Intercept Record, you can move a single or multiple blocked IP addresses to the allowlist.

Procedure

1. Click **System Settings** → **Intercept Record**.

2. Do one of the following:

- Click  on the right side of the desired device.
- Select the desired devices and click **Add to allowlist**.

3. Click **OK** to add the selected IP address(es) to the allowlist.


Resetting the Connections of the Blocked IP

On the page of Intercept Record, you can reset the connection of a single or multiple blocked IP addresses.

Procedure

1. Click **System Settings**→ **Intercept Record**.

2. Do one of the following:

- Click  on the right side of the desired device.
- Select the desired devices and click **Reset Connection**.

3. Click **OK** to reset the connection.