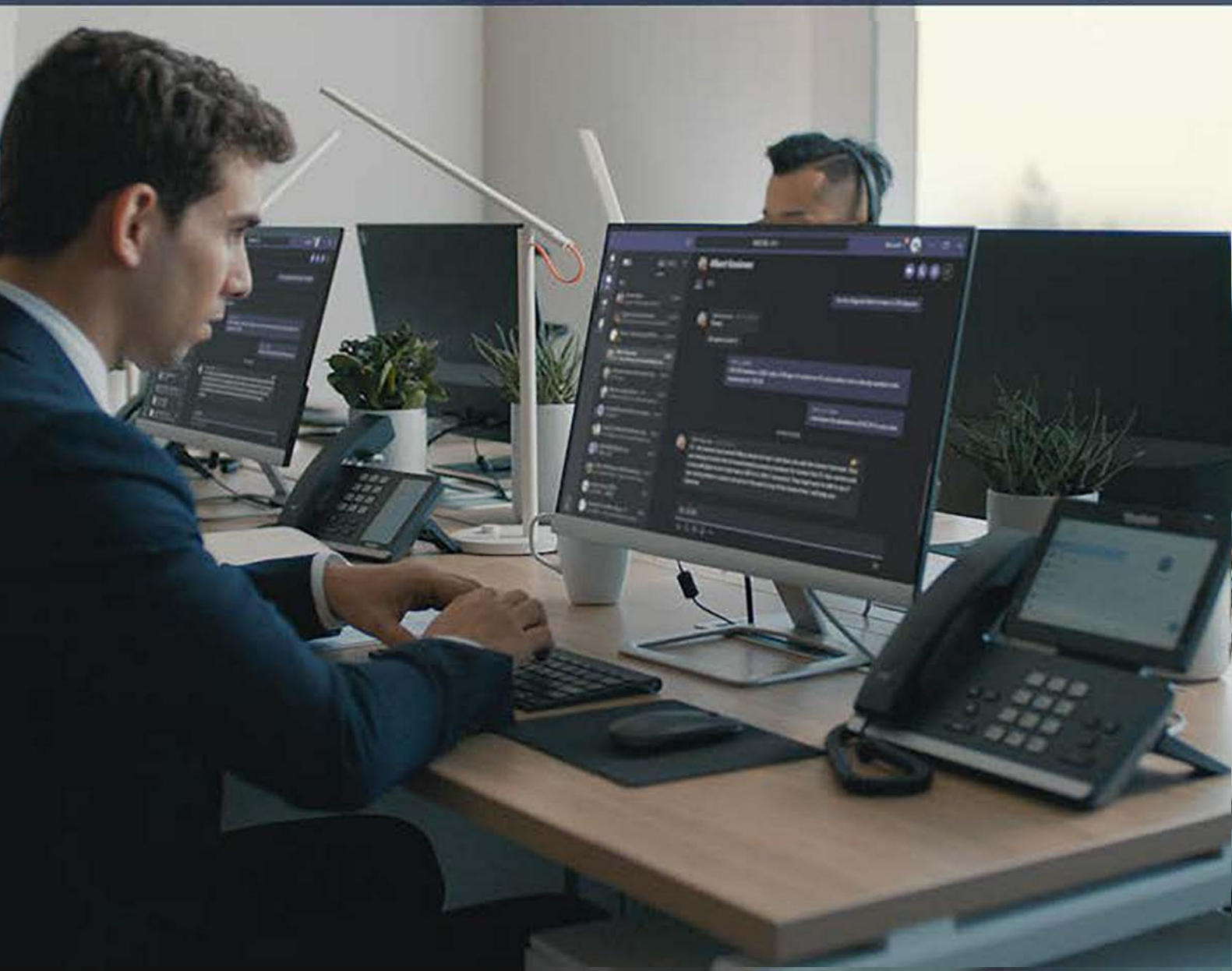




# Teams Phone Setup Guide with Microsoft Configuration Platforms



# Contents

---

## **Contents**

### **About This Guide**

### **Overview of Setting Up Teams Phone**

### **Users & Licenses**

- Understand License Types
- Add Users and Assign Licenses Simultaneously
- Change Account Password

### **Feature Settings**

- Set Up Call Queues
  - Prerequisites
  - Step 1 - Enable Enterprise Voice for Agents
  - Step 2 - Create a Team for the Call Queue Agents
  - Step 3 - Create a Resource Account
  - Step 4 - Assign a License to the Resource Account
  - Step 5 - Create a Call Queue
  - Step 6 - Assign a Call Number to the Resource Account
- Set Up Auto Attendants
  - Prerequisites
  - Step 1 - Create a Resource Account
  - Step 2 - Assign a License to the Resource Account
  - Step 3 - Enable Enterprise Voice
  - Step 4 - Create an Auto Attendant
  - Step 5 - Assign a Call Number to the Resource Account
- Set Up Common Area Phones
  - Prerequisites
  - Step 1 - Create a User Account and Assign Licenses
  - Step 2 - Assign Phone Numbers
  - Step 3 - Sign In

### **Provision Devices on Teams Admin Center**

- Device Firmware Requirements
- Add Device MAC Addresses
- Pre-Configure Devices
- Provision Devices
- Remote Sign In

### **Sign In to Teams Accounts**

- On Your Teams Device
- On a Web Browser

### **Manage Devices on Teams Admin Center**

- Update Devices Remotely
  - Automatic Update
  - Manual Update
- Download Device Logs
- Use Configuration Files
  - Add a Configuration File
  - Assign Configuration File to Devices
- Restart Devices
- Remove Devices from Teams Admin Center

### **Manage Devices on Intune**

- Enroll Devices to Intune
- Manage Device Compliance and Conditional Access

Step 1 - Create a Group

Step 2 - Set Conditional Access

Step 3 - Set Device Compliance

Check the Status of the Compliance Policy

Check the Sign-In Logs

### **Troubleshooting**

Cannot Sign In to Teams Accounts?

Solution 1 - Get the Right User Credentials

Solution 2 - Check the Network Environment

Solution 3 - Upgrade Your Device Firmware to the Latest

Solution 4 - Use Other Accounts to Sign In/Sign in on Other Devices with Your Account

Solution 5 - Reset Your Device

Solution 6 - Check Detailed Reasons on Azure Active Directory Admin Center

Solution 7 - Send the Diagnostic Files to Yealink Support

Cannot Enroll Devices in Intune?

Step 1 - Check the Detailed Reason

Step 2 - Solve the "Device Cap Reached" Issue

Step 3 - Solve the "Device Platform Restriction" Issue

Why Does the Screen Prompt "Rooted Device"?

# About This Guide

---

This guide introduces how to set up Teams phones using the Microsoft configuration platform, including [Teams admin center](#), [Microsoft 365 admin center](#), [Microsoft Endpoint Manager admin center](#), and [Azure Active Directory admin center](#).

Yealink Teams phones include:

- Yealink MP50/MP52/MP54/MP56/MP58
- Yealink VP59
- Yealink CP965

## Overview of Setting Up Teams Phone

---

| Steps | Introduction                                                                                                                                                                                                                                                                                                                                                   |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | <a href="#">Plan the license you need</a><br><a href="#">Create a user account</a><br><a href="#">Assign the corresponding licenses to users.</a>                                                                                                                                                                                                              |
| 2     | Enable following features for the corresponding users: <ul style="list-style-type: none"><li>- <a href="#">Auto attendant</a></li><li>- <a href="#">Call queue</a></li><li>- <a href="#">Common area phone</a></li></ul>                                                                                                                                       |
| 3     | <a href="#">Remotely provision device</a> and <a href="#">remote sign-in</a> on the Teams admin center.                                                                                                                                                                                                                                                        |
| 4     | Sign in to Teams accounts <a href="#">from a Teams phone</a> or <a href="#">a web browser</a> .                                                                                                                                                                                                                                                                |
| 5     | Manage devices on Teams admin center, including: <ul style="list-style-type: none"><li>- <a href="#">Update device firmware and apps</a></li><li>- <a href="#">Download device logs</a></li><li>- <a href="#">Use configuration files</a></li><li>- <a href="#">Restart devices</a></li><li>- <a href="#">Remove devices from Teams admin center</a></li></ul> |
| 6     | <a href="#">Enroll devices on Intune</a><br><a href="#">Manage Device Compliance and Conditional Accesses</a><br><a href="#">Check the compliance status</a><br><a href="#">Check the sign-in logs</a>                                                                                                                                                         |
| 7     | Troubleshooting:<br><a href="#">Teams account sign-in failure</a><br><a href="#">Intune Enrollment failure</a><br><a href="#">Rooted device</a>                                                                                                                                                                                                                |

## Users & Licenses

---

# Understand License Types

Note:

- You can go to **Billing > Purchase services** on the [Microsoft 365 admin center](#) to buy licenses.
- The license takes into effect **10** minutes after your assignment or modification.
- If you need other license types, please see the [Microsoft Teams add-on licenses](#) or contact Microsoft.

| Features you need | Licenses or apps you need                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sign in to Teams  | <p>Ensure that the selected license (e.g., the Common Area Phone) includes the <b>Microsoft Teams</b> app.</p> <div><p>Apps (6) </p><p>Show apps for:</p><div>All licenses </div><p><input checked="" type="checkbox"/> Select all</p><p><input checked="" type="checkbox"/> <b>Azure Active Directory Premium P1</b><br/>Common Area Phone</p><p><input checked="" type="checkbox"/> <b>Exchange Online (Plan 2)</b><br/>Common Area Phone</p><p><input checked="" type="checkbox"/> <b>Microsoft 365 Phone System</b><br/>Common Area Phone</p><p><input checked="" type="checkbox"/> <b>Microsoft Intune</b><br/>Common Area Phone</p><p><input checked="" type="checkbox"/> <b>Microsoft Teams</b><br/>Common Area Phone</p><p><input checked="" type="checkbox"/> <b>Skype for Business Online (Plan 2)</b><br/>Common Area Phone</p></div> |
| Common Area Phone | <p>Common Area Phone license</p> <div><p>Licenses (1)* </p><p><input checked="" type="radio"/> Assign user a product license</p><p><input type="checkbox"/> <b>Audio Conferencing for non-China users</b><br/>35 of 35 licenses available</p><p><input type="checkbox"/> <b>Azure Active Directory Basic</b><br/>The prepaid subscription for this product is no longer active. You need to <a href="#">buy a subscription</a> before you can assign a license.</p><p><input type="checkbox"/> <b>Business Apps (free)</b><br/>1 of 6 licenses available</p><p><input checked="" type="checkbox"/> <b>Common Area Phone</b><br/>You're out of licenses. If you turn this on, we'll try to buy an additional license for you.</p></div>                                                                                                                                                                                          |

| Features you need                                      | Licenses or apps you need                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Calendar feature                                       | <p>Ensure that the selected license (e.g., the Common Area Phone) includes the <b>Exchange Online</b> app.</p> <p>Apps (6) </p> <p>Show apps for:</p> <div data-bbox="534 392 893 425">All licenses</div> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Select all</li> <li><input checked="" type="checkbox"/> <b>Azure Active Directory Premium P1</b><br/>Common Area Phone</li> <li><input checked="" type="checkbox"/> <b>Exchange Online (Plan 2)</b><br/>Common Area Phone</li> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Phone System</b><br/>Common Area Phone</li> <li><input checked="" type="checkbox"/> <b>Microsoft Intune</b><br/>Common Area Phone</li> <li><input checked="" type="checkbox"/> <b>Microsoft Teams</b><br/>Common Area Phone</li> <li><input checked="" type="checkbox"/> <b>Skype for Business Online (Plan 2)</b><br/>Common Area Phone</li> </ul>                                                        |
| Intune<br>(manage device and apply policies on Intune) | <p>Ensure that the selected license (e.g., Microsoft 365 E3) includes the <b>Microsoft Intune</b> app.</p> <div data-bbox="518 896 928 1126"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>Microsoft Defender for Endpoint Plan 1</b><br/>Microsoft 365 E3</li> <li><input checked="" type="checkbox"/> <b>Microsoft Forms (Plan E3)</b><br/>Microsoft 365 E3</li> <li><input checked="" type="checkbox"/> <b>Microsoft Intune</b><br/>Microsoft 365 E3</li> <li><input checked="" type="checkbox"/> <b>Microsoft Kaizala Pro</b><br/>Microsoft 365 E3</li> </ul> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Call queue                                             | <p>Ensure that the selected license (e.g., the Office 365 E5 without Audio Conferencing) includes the <b>Microsoft 365 Phone System</b> app.</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Apps for Enterprise</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Communication Compliance</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Defender</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Phone System</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft Bookings</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft Communications DLP</b><br/>Office 365 E5 without Audio Conferencing</li> </ul> <p>Note: You need <a href="#">follow-up configuration</a> to enable the call queue feature.</p> |

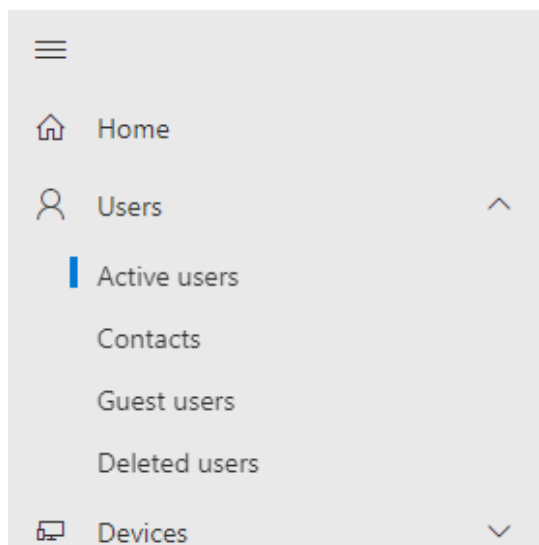
| Features you need | Licenses or apps you need                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto Attendant    | <p>Ensure that the selected license (e.g., the Office 365 E5 without Audio Conferencing) includes the <b>Microsoft 365 Phone System</b> app.</p> <div data-bbox="523 315 920 640"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Apps for Enterprise</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Communication Compliance</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Defender</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Phone System</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft Bookings</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft Communications DLP</b><br/>Office 365 E5 without Audio Conferencing</li> </ul> </div> <p>Note: You need <a href="#">follow-up configuration</a> to enable the call queue feature.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| PSTN              | <p>1. Microsoft Teams Domestic or Domestic and International Calling Plan</p> <div data-bbox="523 763 1013 987"> <ul style="list-style-type: none"> <li><input type="checkbox"/> <b>Microsoft Stream Trial</b><br/>Unlimited licenses available</li> <li><input checked="" type="checkbox"/> <b>Microsoft Teams Domestic Calling Plan</b><br/>0 of 42 licenses available</li> <li><input type="checkbox"/> <b>Microsoft Teams Domestic and International Calling Plan</b><br/>You're out of licenses. If you turn this on, we'll try to buy an additional license for you.</li> <li><input type="checkbox"/> <b>Microsoft Teams Exploratory</b><br/>3 of 500 licenses available</li> </ul> </div> <p>2. Ensure that the selected license (e.g., the Office 365 E5 without Audio Conferencing) includes the <b>Microsoft 365 Phone System</b> app.</p> <div data-bbox="523 1088 874 1402"> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Apps for Enterprise</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Communication Compliance</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Defender</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Phone System</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft Bookings</b><br/>Office 365 E5 without Audio Conferencing</li> <li><input checked="" type="checkbox"/> <b>Microsoft Communications DLP</b><br/>Office 365 E5 without Audio Conferencing</li> </ul> </div> <p>Note: You need follow-up configuration to set up the PSNT feature.</p> |
| Whiteboard        | <p>Ensure that the selected license (e.g., the Microsoft Teams Room Standard) includes the <b>Microsoft 365 Phone System</b> app.</p> <div data-bbox="510 1559 1013 1883"> <p>Show apps for:</p> <div> All licenses </div> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Select all</li> <li><input checked="" type="checkbox"/> <b>Microsoft 365 Audio Conferencing</b><br/>Microsoft Teams Rooms Basic</li> <li><input checked="" type="checkbox"/> <b>Microsoft Teams</b><br/>Microsoft Teams Rooms Basic</li> <li><input checked="" type="checkbox"/> <b>Whiteboard (Plan 3)</b><br/>Microsoft Teams Rooms Basic</li> </ul> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Features you need  | Licenses or apps you need                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Skype for Business | <p>Ensure that the selected license (e.g., the Office 365 E3) includes the <b>Skype for Business Online (Plan 2)</b> app.</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> <b>SharePoint (Plan 2)</b><br/>Microsoft 365 E3</li> <li><input checked="" type="checkbox"/> <b>Skype for Business Online (Plan 2)</b><br/>Microsoft 365 E3</li> <li><input checked="" type="checkbox"/> <b>Sway</b><br/>Microsoft 365 E3</li> </ul> |

## Add Users and Assign Licenses Simultaneously

People on your team need a user account before signing in to Teams phone and using the supported features. After this step, your users have Microsoft 365 licenses, sign-in credentials, and Microsoft 365 mailboxes. You can also assign the corresponding licenses to users.

1. Sign in to the [Microsoft 365 admin center](#) as an administrator.
2. Go to **Users > Active users > Add a user**.



Home > Active users

### Active users

☒ Add a user ☐ Multi-factor authentication

☐ Display name ↑

☐ test03

3. Set the basic information and click **Next**.

## Add a user

- Basics
- Product licenses
- Optional settings
- Finish

## Set up the basics

To get started, fill out some basic information about who you're adding as a user.

First name

Monica

Last name

Zhang

Display name \*

Monica Zhang

Username \*

test01\_

Domains

@ yealink7.onmicrosoft.com

☐ Automatically create a password

Password \*

..... Strong

☐ Require this user to change their password when they first sign in

☐ Send password in email upon completion

Next

4. Assign product licenses and apps for the user and click **Next**.

Add a user

Basics

● Product licenses

○ Optional settings

○ Finish

Licenses

☐ Dynamics 365 Marketing Business Edition  
9999 of 10000 licenses available

☐ Enterprise Mobility + Security E3  
The prepaid subscription for this product is no longer active. You need to [buy a subscription](#) before you can assign a license.

☒ Microsoft 365 Audio Conferencing  
4 of 100 licenses available

☐ Microsoft 365 E3  
86 of 300 licenses available

☐ Microsoft Power Apps Plan 2 Trial  
9990 of 10000 licenses available

☐ Microsoft Power Automate Free  
9557 of 10000 licenses available

☐ Microsoft Stream Trial  
Unlimited licenses available

☒ Microsoft Teams Domestic Calling Plan  
0 of 42 licenses available

☐ Microsoft Teams Domestic and International Calling Plan  
You're out of licenses. If you turn this on, we'll try to buy an additional license for you.

☐ Microsoft Teams Exploratory  
3 of 500 licenses available

☐ Microsoft Teams Rooms Standard  
You're out of licenses. If you turn this on, we'll try to buy an additional license for you.

☐ Office 365 E1  
59 of 215 licenses available

☒ Office 365 E5 without Audio Conferencing  
11 of 135 licenses available

☐ Power BI (free)  
1 unlimited licenses available

Back

Next

Apps

Licenses (3)\*

Apps (55)

Show apps for:

All licenses

☒ Select all

☒ Azure Rights Management  
Office 365 E5 without Audio Conferencing

☒ Common Data Service  
Office 365 E5 without Audio Conferencing

☒ Common Data Service for Teams  
Office 365 E5 without Audio Conferencing

☒ Customer Lockbox  
Office 365 E5 without Audio Conferencing

☒ Data Classification in Microsoft 365  
Office 365 E5 without Audio Conferencing

☒ Exchange Online (Plan 2)  
Office 365 E5 without Audio Conferencing

☒ Graph Connectors Search with Index  
Office 365 E5 without Audio Conferencing

☒ Information Barriers  
Office 365 E5 without Audio Conferencing

☐ Information Protection and Governance Analytics - Premium  
Office 365 E5 without Audio Conferencing  
This app is assigned at the organization level. It can't be assigned per user.

☐ Information Protection and Governance Analytics - Standard  
Office 365 E5 without Audio Conferencing

Back

Next

5. Check the information and click **Finish adding**.

Add a user

✓ Basics

✓ Product licenses

✓ Optional settings

● Finish

Review and finish

Assigned Settings

Review all the info and settings for this user before you finish adding them.

Display and username

Monica Zhang  
test01\_@yealink7.onmicrosoft.com

Edit

Password

Type: Auto-generated

Edit

Product licenses

Location: United States  
Licenses: Microsoft Teams Domestic Calling Plan, Office 365 E5 without Audio Conferencing, Microsoft 365 Audio Conferencing  
Apps: Viva Learning Seeded, Nucleus, Information Protection and Governance Analytics – Standard, 52 more

Edit

Roles (default)

User (no admin center access)

Edit

Profile info

Edit

Back

Finish adding

## Change Account Password

After you create accounts and assign licenses to them, you can set the account password.

1. Sign in to the [Microsoft 365 admin center](#) as an administrator.
2. Expand **Users** and select **Active users**.
3. Find the account you create and click the key to reset the password.

Note:

Leave the **Require this user to change their password when they first sign in** unchecked.

Home > Active users

Active users

Add a user

Multi-factor authentication

Refresh

Delete user

Reset password

Manage product licenses

Manage roles

...

Display name ↑

Username

Licenses

✓ Demo Room

1

...

demoroom@yealink7.onmicrosoft.com

Unlicensed

Reset password

demoroom@yealink7.onmicrosoft.com

☐ Automatically create a password

Password \*

.....

Strong

☐ Require this user to change their password when they first sign in

☐ Email the sign-in info to me

## Feature Settings

You can enable and configure the corresponding features for users. For example, you can [set up a call queue](#) for the support team.

# Set Up Call Queues

Call queues route callers to people in your organization who can help with a particular issue or question. Calls are distributed one at a time to the people (known as agents) in the queue.

## Prerequisites

You need the following resources before creating call queues:

- The members in a call queue must be **Enterprise Voice enabled** users.
- If the members use the Microsoft Teams app for call queue calls, they need to be in **TeamsOnly** mode.
- You have purchased the **Microsoft 365 Phone system** license. See [understand license types](#).

For more detailed information, see the Microsoft doc on [prerequisites of creating call queues](#).

## Step 1 - Enable Enterprise Voice for Agents

Before you create a team for the call queue agents, you need to enable Enterprise Voice for each agent.

### Prerequisite:

You have [downloaded and installed](#) the Teams PowerShell module.

1. Start Windows PowerShell as an administrator.
2. Type the following and press Enter to connect to the Microsoft Teams PowerShell session:

```
Import-Module MicrosoftTeams
$credential = Get-Credential
Connect-MicrosoftTeams -Credential $credential
```

3. Run the command below to assign the `$EnterpriseVoiceEnabled` and `$HostedVoiceMail` properties to the account:

```
Set-CsUser -Identity "<User name>" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true
// change <user name> to the actual user name
```

Example:

```
Set-CsUser -Identity "Perter Parker" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true
```

4. Run the command below to see the status:

If it is true, the Enterprise Voice feature is enabled.

```
Get-CsOnlineUser -Identity "<user name>" | fl EnterpriseVoiceEnabled
```

```
PS D:\Users\yl2886\Desktop\direct routing tool> Set-CsUser -Identity test06@yealink7.onmicrosoft.com -EnterpriseVoiceEnabled $true

PS D:\Users\yl2886\Desktop\direct routing tool> Get-CsOnlineUser -Identity test06 | fl EnterpriseVoiceEnabled

EnterpriseVoiceEnabled : True

PS D:\Users\yl2886\Desktop\direct routing tool>
```

## Step 2 - Create a Team for the Call Queue Agents

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Teams** and select **Manage teams** > **Add**.
3. Enter the team information and click **Apply**.

The screenshot shows the Microsoft Teams admin center interface. On the right, the 'Add a new team' dialog is open. It contains the following information:

- Name:** YL technical support
- Description:** YL technical support
- Team owners:** Peter Parker (TEST06)
- Privacy:** Private

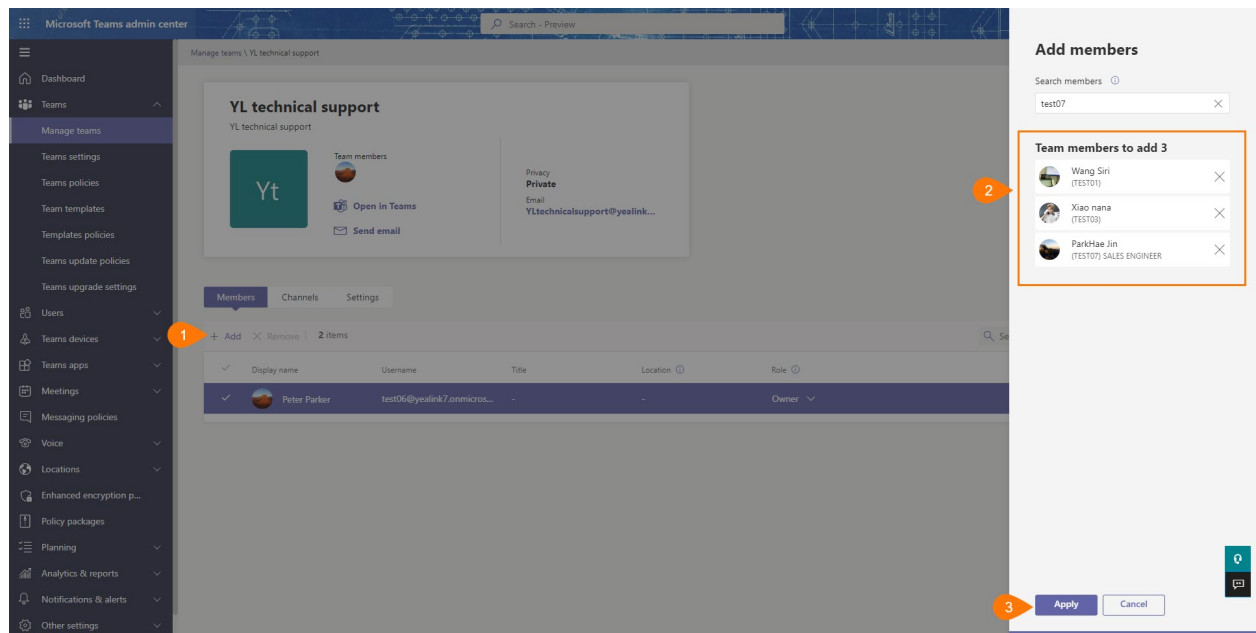
The 'Apply' button at the bottom of the dialog is highlighted with an orange box.

4. Click the name of the created team to view the team's members, channels, and settings.

The screenshot shows the 'Manage teams' page in the Microsoft Teams admin center. A table lists the teams, and the 'YL technical support' team is highlighted with an orange box. The table has the following columns: Name, Standard channels, Private channels, Shared channels, Team members, Owners, and Guests.

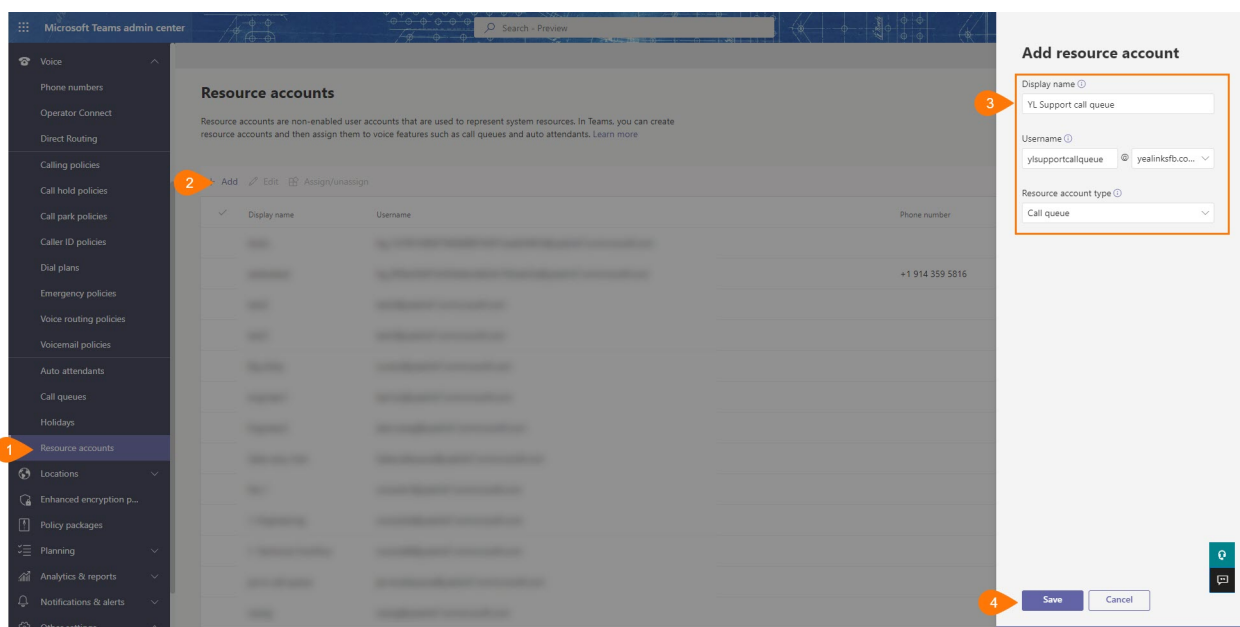
| Name                                 | Standard channels | Private channels | Shared channels | Team members | Owners | Guests |
|--------------------------------------|-------------------|------------------|-----------------|--------------|--------|--------|
| YL technical support                 | 1                 | 0                | 0               | 1            | 1      | 0      |
| Yalink Technical Support - TD Synnex | 1                 | 0                | 0               | 8            | 1      | 2      |
| Comtel & Yalink Technical Support    | 1                 | 0                | 0               | 1            | 1      | 0      |
| Asit&Yalink Technical support Team   | 1                 | 0                | 0               | 7            | 1      | 1      |

5. Under the **Members** tab, click **Add**, add members, and click **Apply**.



## Step 3 - Create a Resource Account

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Voice** and select **Resource accounts**.
3. Select **Add**.
4. Enter the account information and select **Save**.



## Step 4 - Assign a License to the Resource Account

1. Sign in to the [Microsoft 365 admin center](#) as an administrator.
2. Expand **Users** and select **Active users**.
3. Select the resource account to which you want to assign a license. The resource account's user pane will appear.

4. Under the **Licenses and Apps** tab, select **Microsoft 365 Phone System**.
5. Select **Save changes**.

## Step 5 - Create a Call Queue

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Voice** and select **Call queues** > **Add**.
3. Set the general information and click **Next**.

Microsoft Teams admin center

Search - Preview

Call queues \ Add a call queue

**YL Support call queue**

**General info**

Greeting and music

Call answering

Agent selection

Call overflow handling

Call timeout handling

**Resource accounts**

Add or remove resource accounts. You can assign a phone number to a resource account you're adding.

+ Add X Remove 1 item

| ✓ | Resource account      | Phone number |
|---|-----------------------|--------------|
|   | YL Support call queue |              |

**Assign calling ID**

Agents can make outbound calls using the phone numbers on the following resource accounts.

You haven't added any resource accounts yet.

Add

**Language**

This lets you set the language used to transcribe voicemail messages and play system prompts to the caller.

English (United States)

Next

Cancel

4. Set the greeting and music and click **Next**.

Microsoft Teams admin center

Search - Preview

Call queues \ Add a call queue

**Greeting and music**

Greetings and music keep your caller informed about their call while waiting to be answered by an agent. Learn more

**Greeting**

☐ No greeting

☒ Play an audio file

hello.wav

Accepted file formats are MP3, WAV, and WMA. Files must be less than 5 MB.

☐ Add a greeting message

**Music on hold**

☒ Play default music

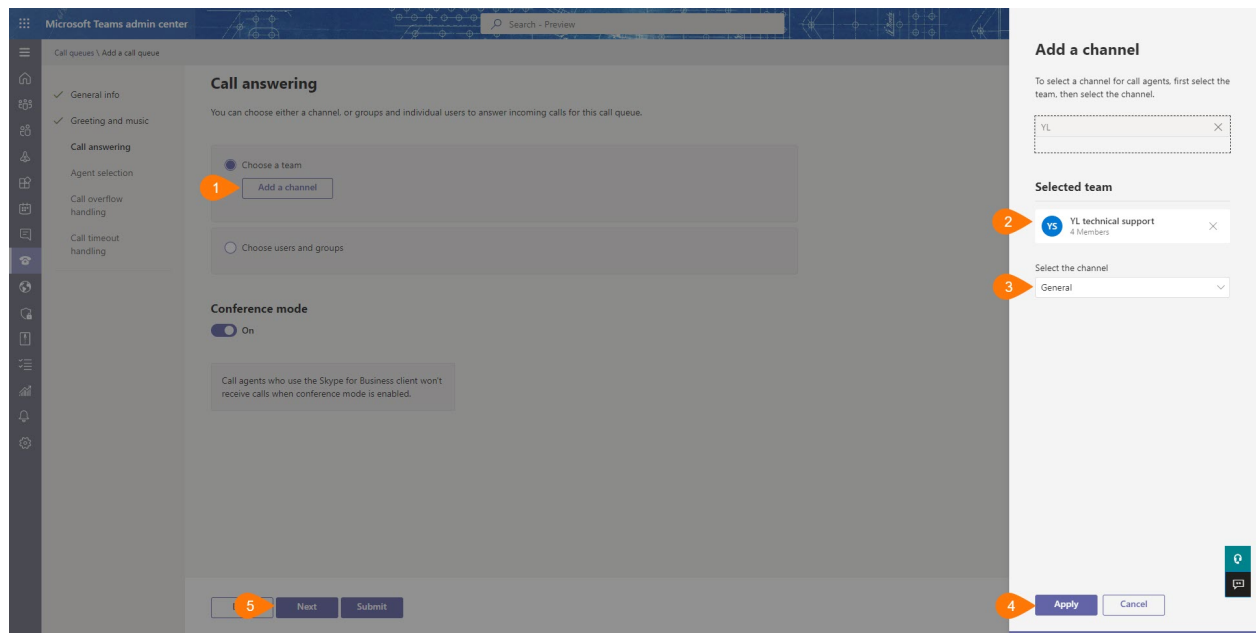
☐ Play an audio file

Next

Submit

Cancel

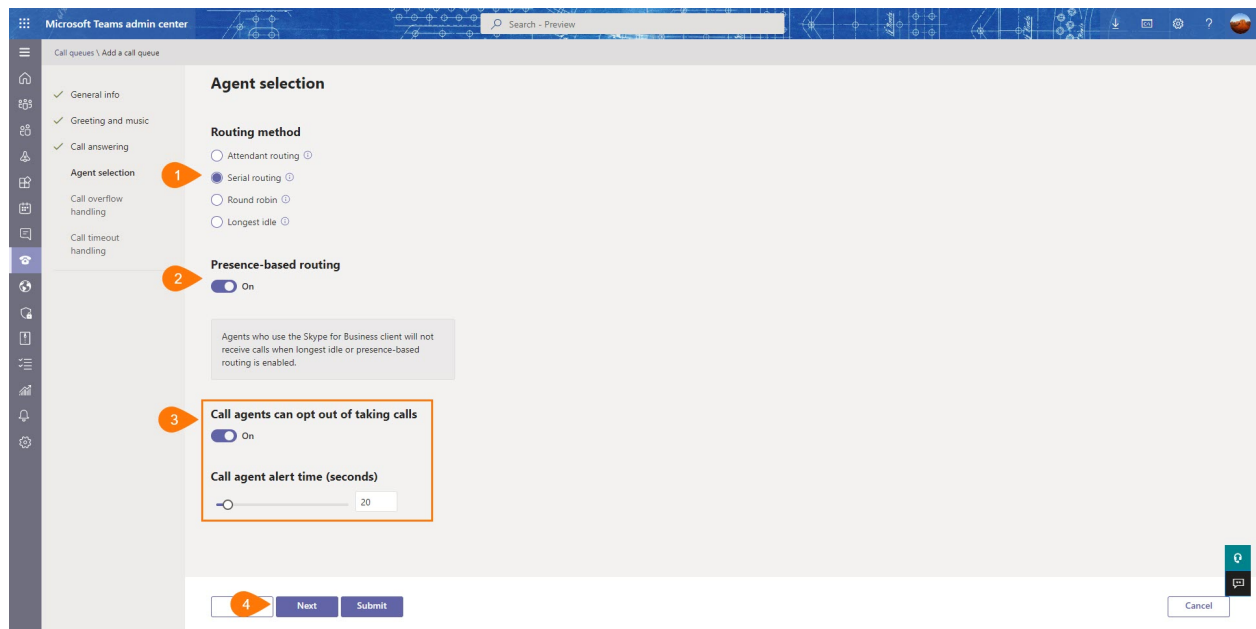
5. Set up call answering and click **Next**.



- **Conference mode**: it reduces the time it takes for a caller to be connected to an agent after the agent accepts the call. For conference mode to work, agents in the call queue must use one of the following clients:

- The latest version of the Microsoft Teams desktop client, Android app, or iOS app
- Microsoft Teams Phone version 1449/1.0.94.2020051601 or later

6. Choose and assign agents and click **Next**.



- **Serial routing**: it brings each agent one by one in the order specified in the **Call agents** list. If an agent dismisses or doesn't pick up a call, the call will ring to the next agent. This will repeat until the call is picked up or times out.
- **Presence-based routing**: call agents whose availability status is set to **Available** can receive the call.
- **Call agents can opt out of taking calls**: call agents can opt out of taking calls or not.
- **Agent alert time**: it specifies how long an agent's phone will ring before the queue redirects the call to the next agent. The recommended alert time is 20 seconds.

7. Set call overflow handling and click **Next**.

8. Set call timeout handling and click **Submit**.

- [Maximum wait time](#): it specifies the maximum time a call can be on hold in the queue before it is redirected or disconnected.

## Step 6 - Assign a Call Number to the Resource Account

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Voice** and select **Resource accounts**.
3. Select the resource account to which you want to assign a number and click **Assign/unassign**.
4. Select the phone number type, a phone number and the call queue you created.
5. Click **Save**.

## Assign/unassign

YL Support call queue

 To see a service number listed here, buy a Phone System or get a Teams Phone Resource Account license and make sure it's not assigned to any other voice services. [Learn more](#)

Phone number type

1

Calling Plan

Assigned phone number

2

+1 970 200 8021

**Assigned to**

 Your changes must be saved before making more changes.

Select a call queue

3

YL support call queue

4

Save

Cancel

## Set Up Auto Attendants

Auto attendants let people call your organization and navigate a menu system to speak to the right department, [call queue](#), person, or operator. You can create auto attendants for your organization with the Microsoft Teams admin center or [PowerShell](#).

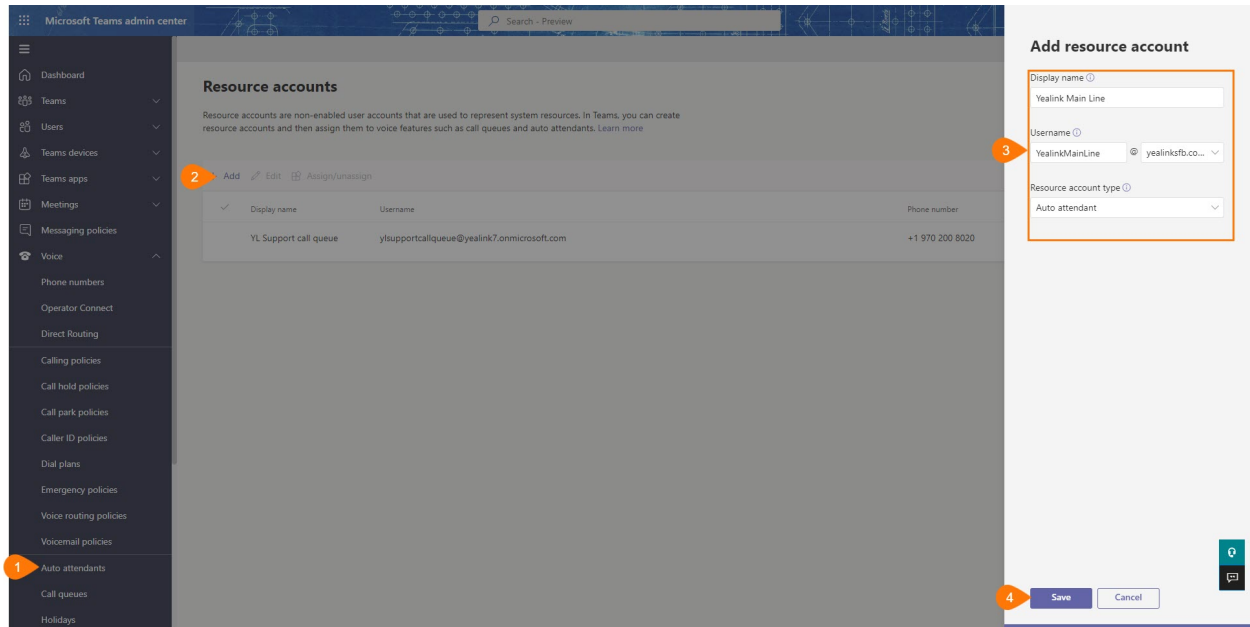
### Prerequisites

- You have purchased the **Microsoft 365 Phone system** license. See [Understand License Types](#).
- The person, operator, or call queue assigned in the auto attendant must be an **Enterprise Voice enabled** user.

For more detailed information, see the Microsoft docs on [prerequisites of creating auto attendants](#).

## Step 1 - Create a Resource Account

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Voice** and select **Resource accounts**.
3. Select **Add**.
4. Enter the account information and select **Save**.



## Step 2 - Assign a License to the Resource Account

1. Sign in to the [Microsoft 365 admin center](#) as an administrator.
2. Expand **Users** and select **Active users**.
3. Select the resource account to which you want to assign a license. The resource account's user pane will appear.
4. Under the **Licenses and Apps** tab, select **Microsoft 365 Phone System**.
5. Select **Save changes**.

## Step 3 - Enable Enterprise Voice

See [Enable Enterprise Voice for Agents](#).

## Step 4 - Create an Auto Attendant

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Voice** and select **Auto attendants** > **Add**.
3. Set the general information and click **Next**.

Microsoft Teams admin center

Auto attendants \ Add auto attendant

**1 Yealink Main Line**

**General info**

Call flow

Advanced settings (optional)

**Operator (optional)**

Set up an auto attendant to manage the flow for incoming calls.

**2** Person in organization PP Peter Parker test06@yealink7.onmicrosoft.com

**Time zone \***

Setting the time zone will let calls be answered during the correct business and non-business hours.

**3** (UTC) Coordinated Universal Time

**Language**

The language set here will tell the system what language to use when reading prompts, greetings, and dial keys.

**4** English (United States)

**5** Voice inputs On

**6** Next Cancel

4. Set the call flow and click **Next**.

1. Set the greeting options. Callers can hear the greeting when they call the number. The system will read the text you set.

Auto attendants \ Add auto attendant

**Call flow**

Set up the calling experience for your organization. Write or record a greeting message, set up call routing, and, in Advanced settings, adjust the call flow based on whether the call is during business hours. [Learn more](#)

**Greeting options**

☐ No greeting

☐ Play an audio file

☒ Add a greeting message

Thanks for calling Yealink.

2. Set the call routing options and click **Next**.

Auto attendants \ Add auto attendant

**Call routing options**

☐ Disconnect

☐ Redirect call

☒ Play menu options

**Force Listen** Off

**Set up the greeting and menu options.**

☐ Play an audio file

☒ Add a greeting message

For Sales, press 1. For support, press 2. To speak to an operator, press 0. You can type or say the name of the person you are trying to reach at any time.

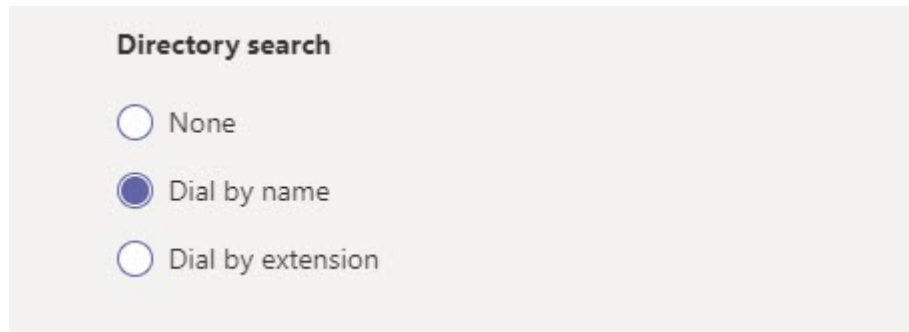
**Set menu options**

**3** + Assign a dial key Delete

| Dial key | Voice command | Redirect to | Destination             | Transcription | Skip voicemail system message |
|----------|---------------|-------------|-------------------------|---------------|-------------------------------|
| 0        | Operator      | Operator    | PP Peter Parker         |               |                               |
| 1        |               | Voice app   | YS Yealink Sales        |               |                               |
| 2        |               | Voice app   | Y YL Support call queue |               |                               |

3. Set the directory search type.

If callers do not know the extension of the internal users, you can enable **Dial by name**. Therefore, callers can say or type the name on the phone keypad.



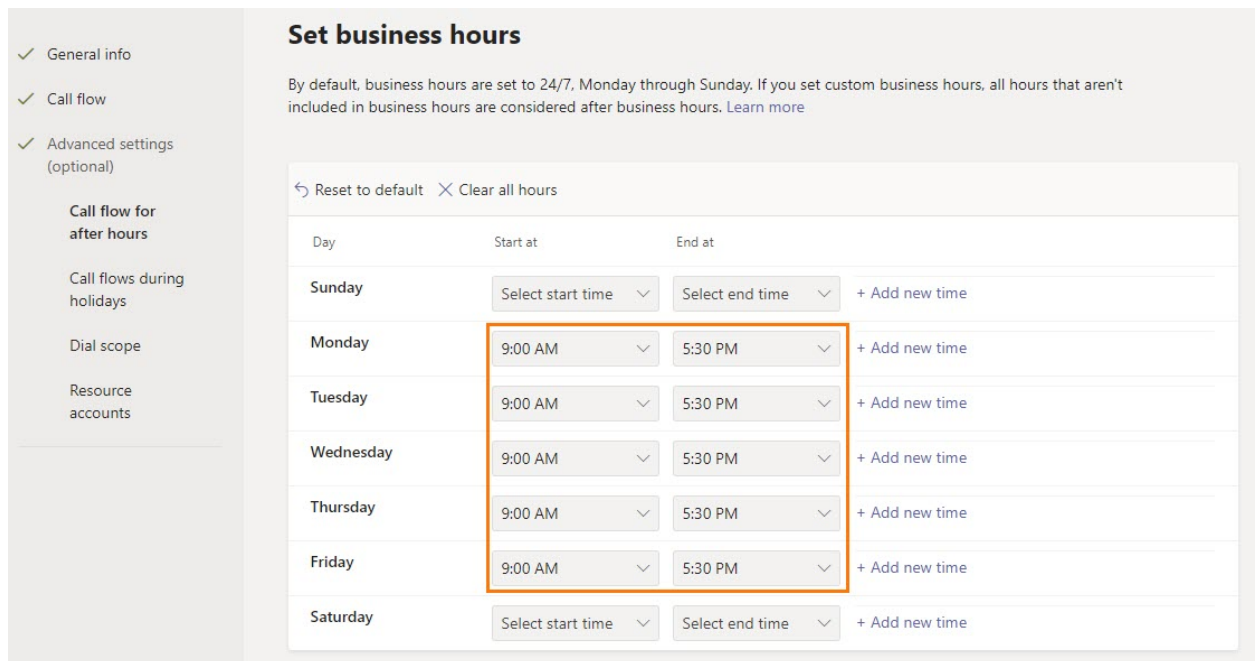
**Directory search**

☐ None

☒ Dial by name

☐ Dial by extension

5. Set your company business hours.



**Set business hours**

By default, business hours are set to 24/7, Monday through Sunday. If you set custom business hours, all hours that aren't included in business hours are considered after business hours. [Learn more](#)

↶ Reset to default   ✕ Clear all hours

| Day       | Start at          | End at          |                |
|-----------|-------------------|-----------------|----------------|
| Sunday    | Select start time | Select end time | + Add new time |
| Monday    | 9:00 AM           | 5:30 PM         | + Add new time |
| Tuesday   | 9:00 AM           | 5:30 PM         | + Add new time |
| Wednesday | 9:00 AM           | 5:30 PM         | + Add new time |
| Thursday  | 9:00 AM           | 5:30 PM         | + Add new time |
| Friday    | 9:00 AM           | 5:30 PM         | + Add new time |
| Saturday  | Select start time | Select end time | + Add new time |

6. Set up after-hours call flow.

General info

Call flow

Advanced settings (optional)

Call flow for after hours

Call flows during holidays

Dial scope

Resource accounts

1

2

3

## Set up after hours call flow

If you have business hours set up, you also need to set up a call flow for after business hours.

### Greeting options

☐ No greeting  
☐ Play an audio file [?](#)  
☒ Add a greeting message [?](#)

Thank you for calling Yealink. Your call is important to us. Please leave your name and number, and we will call you back.

### Call routing options

☐ Disconnect  
☒ Redirect call [?](#)

Redirect to [?](#)

Voicemail = Y Yealink ×

Transcription

☒ On

Skip voicemail system message [?](#)

☐ Off

☐ Play menu options

Back

Next

Submit

7. Click **Add** to add call flows during holidays. If you have not set a holiday, add one first.

General info

Call flow

Advanced settings (optional)

Call flow for after hours

Call flows during holidays

New call flow

Dial scope

Resource accounts

1

2

3

4

5

## Christmas

Holiday

Christmas

### Greeting

☐ No greeting  
☐ Play an audio file [?](#)  
☒ Add a greeting message [?](#)

Thank you for calling Yealink. Our office is closed for the Christmas holiday. Please leave your name and number, and we will call you back.

### Call routing options

☐ Disconnect  
☒ Redirect call [?](#)

Redirect to [?](#)

Voicemail = Y Yealink ×

Transcription

☐ Off

Skip voicemail system message [?](#)

☐ Off

☐ Play menu options

Save

Cancel

8. Set up a dial scope to include or exclude users or groups.

Auto attendants \ Add auto attendant

✓ General info  
✓ Call flow  
✓ Advanced settings (optional)  
✓ Call flow for after hours  
✓ Call flows during holidays  
**Dial scope**  
Resource accounts

### Dial scope

Set up the users or groups that will be listed and available in your organization's directory when a caller dials in to this auto attendant. When callers use Dial by name and search for a person, they'll be transferred to a user who has the Teams app installed. [Learn more](#)

**1** **Include**  
Select which users will be included and available in your organization's directory. ⓘ

☒ All online users  
☐ Custom user group

**Exclude**  
Select which users or groups will be excluded from the organization's directory. ⓘ

☒ No one  
☐ Custom user group

**2**

9. Add a resource account and click **Submit**.

Microsoft Teams admin center

Auto attendants \ Add auto attendant

✓ General info  
✓ Call flow  
✓ Advanced settings (optional)  
✓ Call flow for after hours  
✓ Call flows during holidays  
✓ Dial scope  
**Resource accounts**

### Resource accounts

When you create an auto attendant, you can add a new resource account and assign a phone number to that resource account. [Learn more](#)

You haven't added any resource accounts yet.

**1**

**2** **Add accounts**  
Search for resource accounts you want to add.

Accounts to add (1)

**YL** Yealink Main Line

**3**

**4**

## Step 5 - Assign a Call Number to the Resource Account

1. Sign in to the [Microsoft Teams admin center](#) as an administrator.
2. Expand **Voice** and select **Resource accounts**.
3. Select the resource account to which you want to assign a number and click **Assign/unassign**.
4. Select the phone number type, a phone number and the auto attendant you created.
5. Click **Save**.

## Assign/unassign

Yealink Main Line

 To see a service number listed here, buy a Phone System or get a Teams Phone Resource Account license and make sure it's not assigned to any other voice services. [Learn more](#)

Phone number type



Assigned phone number



**Assigned to**

 Your changes must be saved before making more changes.

Select an auto attendant





## Set Up Common Area Phones

A common area phone is typically placed in an area like a lobby or another area that is available to many people to make a call; for example, a reception area, lobby, or conference phone. Common area phones are signed in with accounts tied to a Common Area Phone license.

## Prerequisites

Make sure you have purchased the **Common Area Phone** license [on Microsoft 365 admin center](#).

## Step 1 - Create a User Account and Assign Licenses

See [Add Users and Assign Licenses Simultaneously](#) to learn how to create a user account and assign the Common Area Phone license.

## Step 2 - Assign Phone Numbers

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Expand **Voice** and select **Phone numbers**.
3. Select a number and click **Edit**.
4. Assign the number to a user and click **Apply**.

**Microsoft Teams admin center**

**Phone numbers**

To set up calling features for users and services in your organization, you can get new numbers or port existing ones from a service provider. You can assign, unassign, and release phone numbers for people or for services, like audio conferencing, auto attendants, or call queues. [Learn more](#)

**Get support for your phone numbers in the Phone Number Service Center**

Create a new case [🔗](#)  
View my existing cases [🔗](#)  
View my existing company cases [🔗](#)

**Numbers** Order history

+ Add | Port | Edit | Release | Change usage | 63 items

| Phone number    | Number provider | Location                     | Available usages            | Licensed usages       | Number type |
|-----------------|-----------------|------------------------------|-----------------------------|-----------------------|-------------|
| +1 213 458 8107 | Microsoft       | Los Angeles, United States   | User, Conference, Voice app | User                  | Geographic  |
| +1 213 458 8108 | Microsoft       | Los Angeles, United States   | User, Conference, Voice app | User                  | Geographic  |
| +1 408 791 0635 | Microsoft       | San Jose, United States      | User, Conference, Voice app | Conference, Voice app | Geographic  |
| +1 646 518 9925 | Microsoft       | New York City, United States | Conference, Voice app       | Conference, Voice app | Geographic  |
| +1 718 650 3667 | Microsoft       | New York City, United States | User, Conference, Voice app | User                  | Geographic  |
| +1 912 446 5506 | Microsoft       | Savannah, United States      | User, Conference, Voice app | User                  | Geographic  |
| +1 912 446 5672 | Microsoft       | Savannah, United States      | User, Conference, Voice app | User                  | Geographic  |

**Assign/unassign**

+1 213 458 8107

**Number usages**  
User

**Number type**  
CallingPlan

**Number features**

**Assigned to**  
Select a person that you want to assign this phone number to

1 **Yealink Amazon offic...**

**Emergency location**  
Select a location within the country or region where emergency services must arrive when a call comes from this phone number.  
If your organization has more than one physical location, it's likely that you'll need more than one emergency location. [Add a new emergency location.](#)

405 Hilgard Avenue, Los Angeles CA 90024, US.

☐ Email user with phone number information

2 **Apply** **Cancel**

## Step 3 - Sign In

Once you create and configure a user account, you can sign in on a phone. You can sign in from one of the following methods:

- [Sign in on the Teams phone](#)
- [Sign in on a web browser](#)
- [Sign in using the Teams admin center](#)

## Provision Devices on Teams Admin Center

You can remotely provision and sign in to a Teams Android device.

## Device Firmware Requirements

Supported device models:

| Device model           | Firmware version     |
|------------------------|----------------------|
| Yealink VP59           | 91.15.0.58 or later  |
| Yealink MP56/MP54/MP58 | 122.15.0.36 or later |
| Yealink T55/T56/T58    | 58.15.0.124 or later |
| Yealink CP960          | 73.15.0.117 or later |
| Yealink CP965          | 143.15.0.7 or later  |

## Add Device MAC Addresses

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Expand **Teams devices** and select **Phones**.
3. Select **Provision new device** from the **Actions** tab.

You can either manually add the MAC address or upload a file to add in batch in the **Provision new devices** window.

- **Manually add a device MAC address:**

1. Under the Waiting on activation tab, click **Add**.
2. Enter the MAC address, set the location, and click **Save**.

The screenshot shows the 'Provision devices' interface in the Microsoft Teams admin center. On the left, a table lists existing devices with columns for ID, ID type, Location, and Verification code. Some devices show 'Expired' status. On the right, a sidebar titled 'Add MAC addresses or hardware IDs' allows adding new devices. It includes fields for 'ID type' (set to 'MAC address'), 'Enter MAC address' (with value '80-5E-C0-DA-A4-52'), and 'Location' (set to 'Xiamen, China'). At the bottom of the sidebar are 'Save' and 'Cancel' buttons. Numbered callouts indicate the workflow: 1. Click 'Add' in the table toolbar; 2. The sidebar opens; 3. Enter details in the sidebar; 4. Click 'Save'.

- **Upload a file to add a device MAC address:**

1. From the **Waiting on activation** tab, select **Upload**.
2. Download the file template.
3. Enter the MAC ID and location, and then save the file.
4. Click **Select a file** and then select **Upload**.

# Pre-Configure Devices

You need a verification code for the devices. The verification code is generated in bulk or at the device level and is valid for 24 hours.

1. From the **Waiting on activation** tab, select an existing MAC ID and click **Generate verification code**.

A password is created for the MAC address and is shown in the **Verification Code** column.

**Provision devices**

Add one or more MAC addresses or hardware IDs for your devices to start provisioning them. When you add your devices, they can be remotely signed in and then deployed in your organization. [Learn more](#)

**Provisioning summary**  
7 2 2  
MAC addresses or hardware IDs Verification codes Waiting to sign in expired

**New device provisioning steps**

1. Manually add or upload a file with new MAC addresses or hardware IDs.
2. Generate a verification code.
3. Export the verification codes for your devices.

Waiting on activation Waiting for sign in

+ Add Upload Generate verification code + Edit Delete 1 item selected Search by MAC address or hardw...

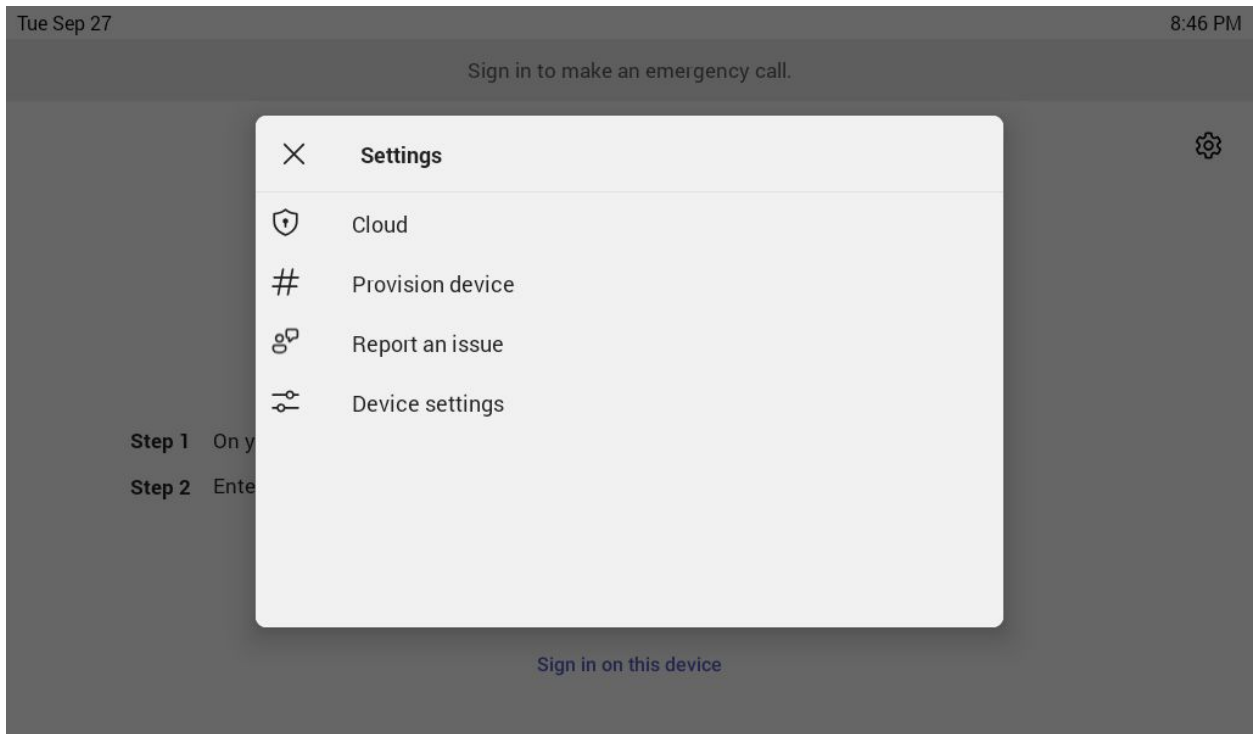
| ID                    | ID type              | Location      | Verification code |
|-----------------------|----------------------|---------------|-------------------|
| 80-5e-c0-d8-a4-52     | MAC address          | Xiamen, China | 362671            |
| 02-10-00-04-00-05:999 | Hardware ID (analog) | India         | --                |
| 02-10-00-04-00-05     | MAC address          | US            | --                |
| 80-5e-c0-d0-3b-e3     | MAC address          | --            | Expired           |
| 00-02-91-c6-d3-e8     | MAC address          | --            | Expired           |

You can also provide the list of MAC IDs and verification codes to the field technicians. You can export the detail directly in a file and share the file with the technician who is doing the actual installation work.

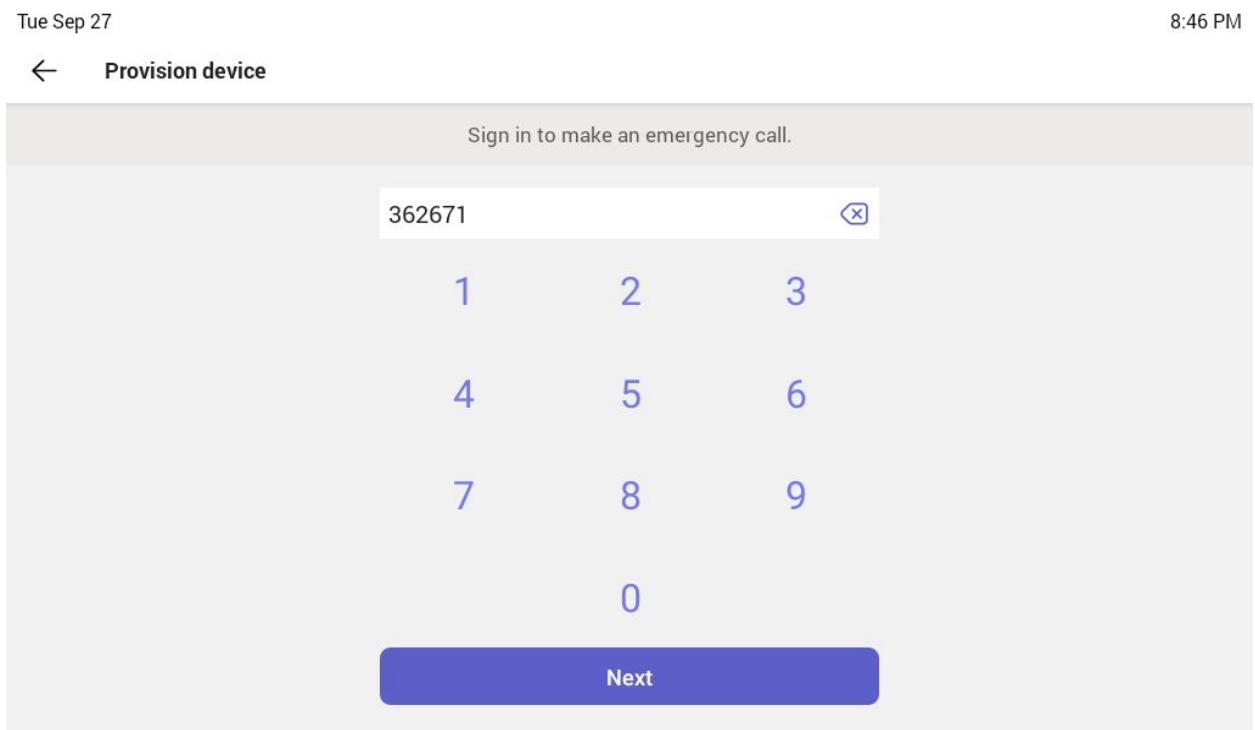
# Provision Devices

When the device is powered on and connected to the network, you can provision the device. These steps are completed on the Teams device.

1. Click the **Settings** icon and select **Provision device** from the **Settings**.



2. Enter the verification code in the provided input field.



Once the device is provisioned successfully, the tenant name appears on the sign-in page.

## Remote Sign In

1. Select a device from the **Waiting for sign in** tab.
2. Follow the instructions in **Sign in a user**, and then select **Close**.

## Sign In to Teams Accounts

After users sign in on Teams devices, administrators can [manage the devices on Teams admin center](#).

You can sign in to your Microsoft Teams account directly on your device or via a web browser.

Note: The following illustrations serves as examples. The actual phone screen you see might be different.

### Before you begin

Contact your system administrator to get your sign-in account.

## On Your Teams Device

1. Tap **Sign in on this device**.

Wed Sep 14

10:30 AM

Sign in to make an emergency call.



**Step 1** On your computer or mobile, go to <https://microsoft.com/devicelogin>

**Step 2** Enter the code below to sign in.

**HUQYEDF7W**

Sign in on this device

2. Enter your user credentials and tap **Sign in**.



Welcome to Microsoft Teams! A happier place for teams to work together.



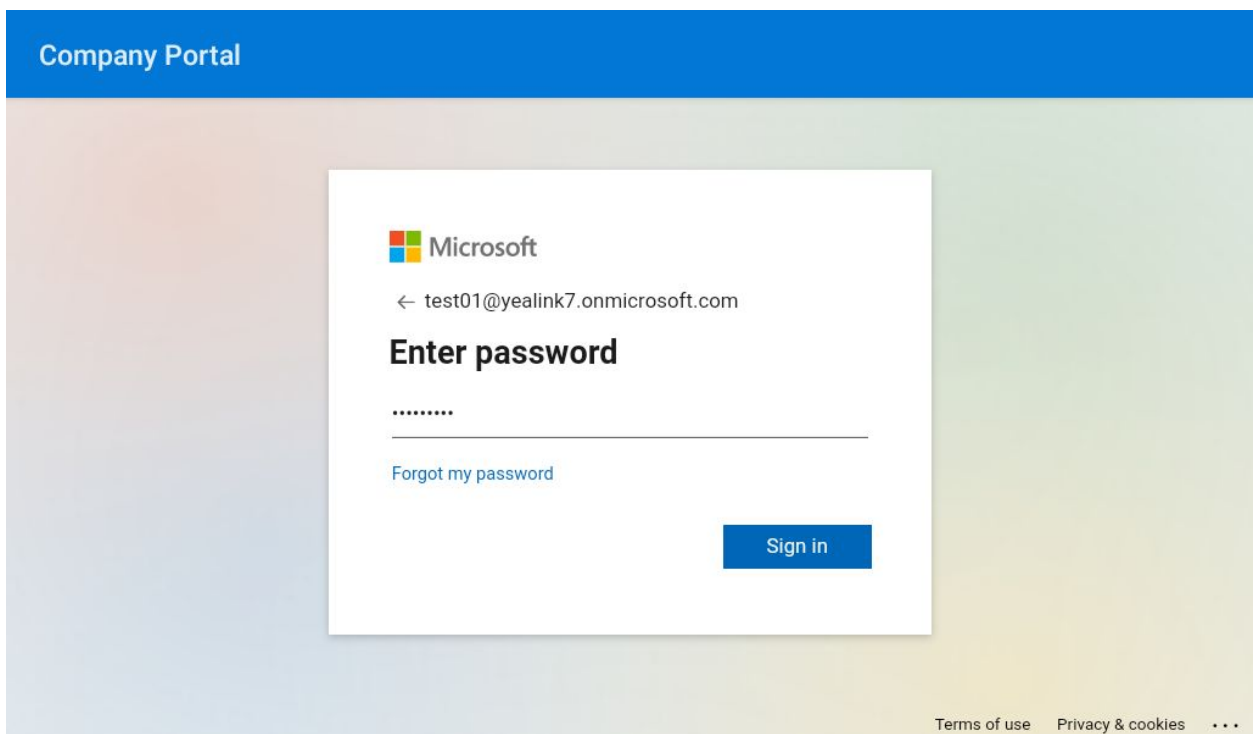
test03@yealink7.onmicrosoft.com

Sign in



You will be connected to the Company Portal automatically.

3. Enter your password and tap **Sign in**.



4. After the device signs in successfully, tap **Got it**.

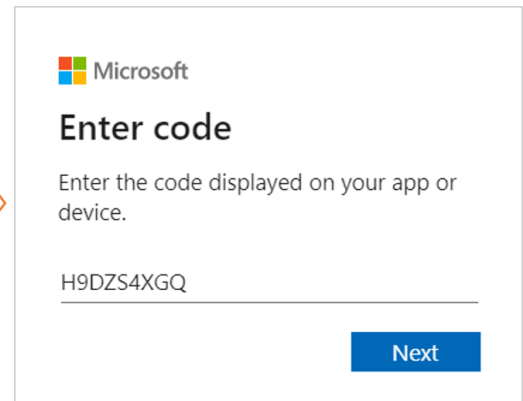
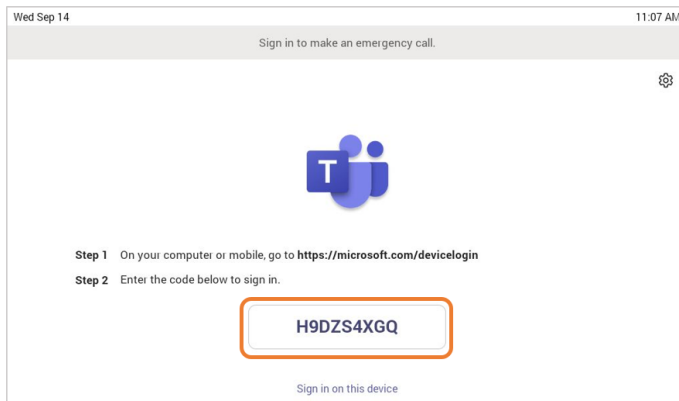


Have meetings and calls with audio, video.

Got it

## On a Web Browser

1. Go to <https://microsoft.com/devicelogin> on your computer or mobile.
2. Enter the code shown on your device and select **Next**.



3. Enter your user credentials or select the desired account to sign in.



Microsoft

## Sign in

You're signing in to **Microsoft Authentication Broker** on another device located in **China**. If it's not you, close this page.

test06@yealink7.onmicrosoft.com

No account? [Create one!](#)

[Can't access your account?](#)

[Back](#) [Next](#)

Microsoft

← test06@yealink7.onmicrosoft.com

## Enter password

.....

[Forgot my password](#)

[Sign in](#)

A confirmation message is displayed after successfully signing in to Microsoft Intune Company Portal.

4. After the device signs in successfully, tap **Got it**.



Have meetings and calls with audio, video.

[Got it](#)

## Manage Devices on Teams Admin Center

After users sign in to Teams accounts on their devices, the devices are connected to the Teams admin center. You can manage them, for example, by updating devices remotely or downloading device logs.

### Update Devices Remotely

With the Microsoft Teams admin center, you can update your Teams phones.

You can update the following for your device on the Teams admin center:

- Teams app and teams admin agent

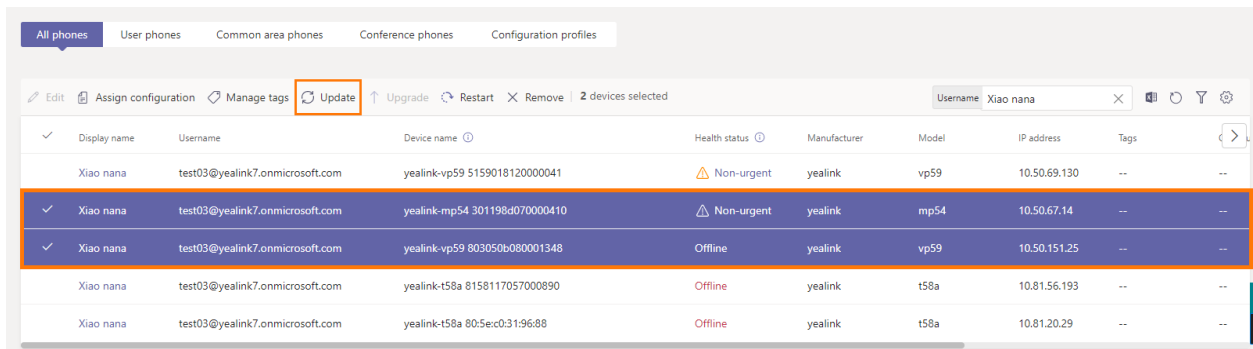
- Company portal app
- OEM agent app
- Device firmware

Note:

You cannot select the desired firmware version to update. If you want to update the device to the desired firmware, you update it from the [web browser](#).

## Automatic Update

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones**.
3. Select one or more devices and then select **Update**.

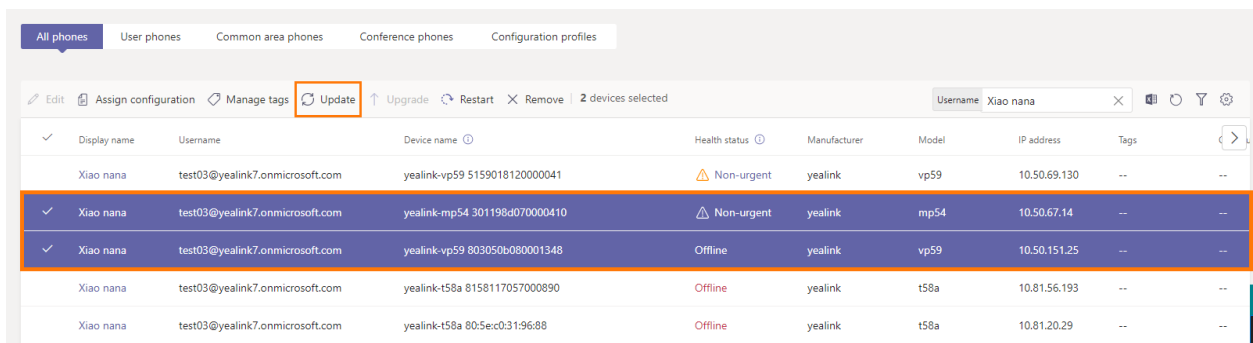


| ✓ | Display name | Username                        | Device name ⓘ                 | Health status ⓘ | Manufacturer | Model | IP address   | Tags |
|---|--------------|---------------------------------|-------------------------------|-----------------|--------------|-------|--------------|------|
|   | Xiao nana    | test03@yealink7.onmicrosoft.com | yealink-vp59 5159018120000041 | ⚠ Non-urgent    | yealink      | vp59  | 10.50.69.130 | --   |
| ✓ | Xiao nana    | test03@yealink7.onmicrosoft.com | yealink-mp54 301198d070000410 | ⚠ Non-urgent    | yealink      | mp54  | 10.50.67.14  | --   |
| ✓ | Xiao nana    | test03@yealink7.onmicrosoft.com | yealink-vp59 803050b080001348 | Offline         | yealink      | vp59  | 10.50.151.25 | --   |
|   | Xiao nana    | test03@yealink7.onmicrosoft.com | yealink-t58a 8158117057000890 | Offline         | yealink      | t58a  | 10.81.56.193 | --   |
|   | Xiao nana    | test03@yealink7.onmicrosoft.com | yealink-t58a 80:5ec0:31:96:88 | Offline         | yealink      | t58a  | 10.81.20.29  | --   |

4. Select one of the following:
  - **As soon as available:** Second-newest device firmware update is applied on the first weekend after the latest update is released.
  - **Defer 30 days:** Second-newest device firmware update is applied 30 days after the latest update is released.
  - **Defer 90 days:** Second-newest device firmware update is applied 90 days after the latest update is released.
5. Select **Update**.

## Manual Update

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Navigate **Teams Devices > Phones**.
3. Select one or more devices and select **Update**.



| ✓ | Display name | Username                        | Device name ⓘ                 | Health status ⓘ | Manufacturer | Model | IP address   | Tags |
|---|--------------|---------------------------------|-------------------------------|-----------------|--------------|-------|--------------|------|
|   | Xiao nana    | test03@yealink7.onmicrosoft.com | yealink-vp59 5159018120000041 | ⚠ Non-urgent    | yealink      | vp59  | 10.50.69.130 | --   |
| ✓ | Xiao nana    | test03@yealink7.onmicrosoft.com | yealink-mp54 301198d070000410 | ⚠ Non-urgent    | yealink      | mp54  | 10.50.67.14  | --   |
| ✓ | Xiao nana    | test03@yealink7.onmicrosoft.com | yealink-vp59 803050b080001348 | Offline         | yealink      | vp59  | 10.50.151.25 | --   |
|   | Xiao nana    | test03@yealink7.onmicrosoft.com | yealink-t58a 8158117057000890 | Offline         | yealink      | t58a  | 10.81.56.193 | --   |
|   | Xiao nana    | test03@yealink7.onmicrosoft.com | yealink-t58a 80:5ec0:31:96:88 | Offline         | yealink      | t58a  | 10.81.20.29  | --   |

4. **Optional:** Select **Schedule** if you want to schedule the update for a future date and time. The updates are applied at the date and time in the timezone selected in **Timezone**.
5. Select the available firmware or apps you want to update and click **Update**.
- If you select a single device:

**Update status**  
yealink-mp54 301198d070000410

**Firmware auto-update** ▾

**Manual updates** ▴

Schedule ☐ Off

Software component  
☒ **Firmware**

Current version  
**122.15.0.80**

New version  
**122.15.0.91**

Published on  
**Jul 29, 2022, 9:20 PM**

---

Software component  
☒ **Teams app**

Current version  
**1449/1.0.94.2022072801**

New version  
**1449/1.0.94.2022082401**

Published on  
**Aug 29, 2022, 8:30 PM**

**Update** **Close**

- If you select multiple devices:

**Update status**  
2 devices

① Updates are applied to supported devices when they're available.

**Firmware auto-update** ▾

**Manual updates** ▴

Schedule ☐ Off

**Select the updates to be applied**

☒ Teams admin agent

☒ Firmware

☐ Company portal app

☐ Oem agent app

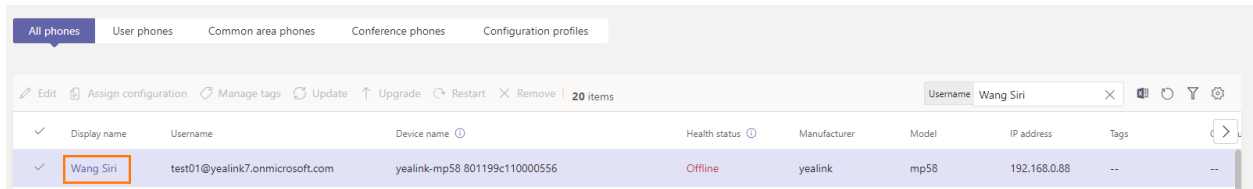
☒ Teams app

**Update** **Close**

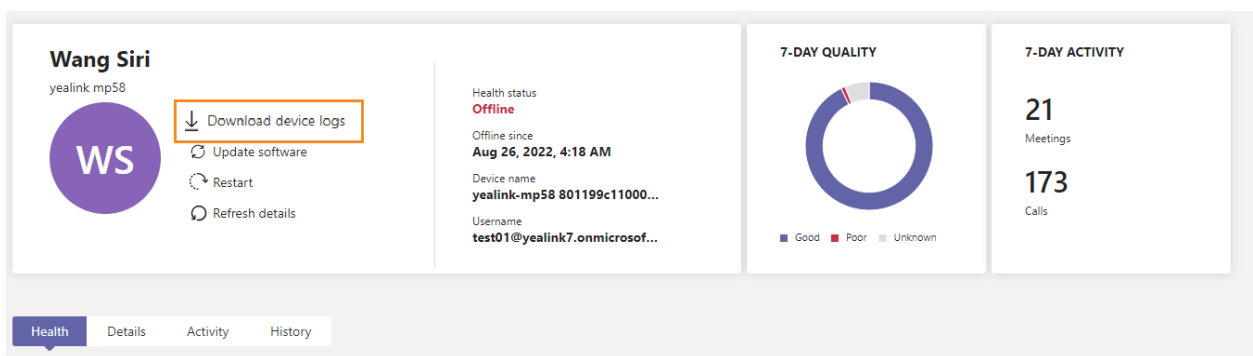
# Download Device Logs

You can download a copy of a device's diagnostic log files if requested to do so by Microsoft support.

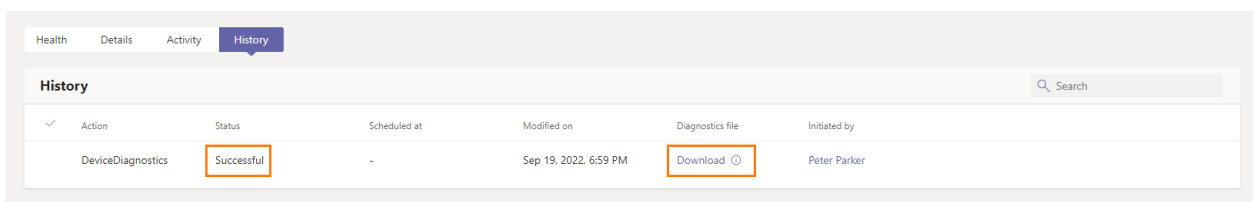
1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones**.
3. Click the display name of the device from which you want to download logs.



4. Select **Download device logs**. It can take several minutes for device logs to become available.



5. Select the **History** tab, then click **Download** to download the log file under the **Diagnostics file** column. If the diagnostic log files are available to download, the status will change to "Successful".

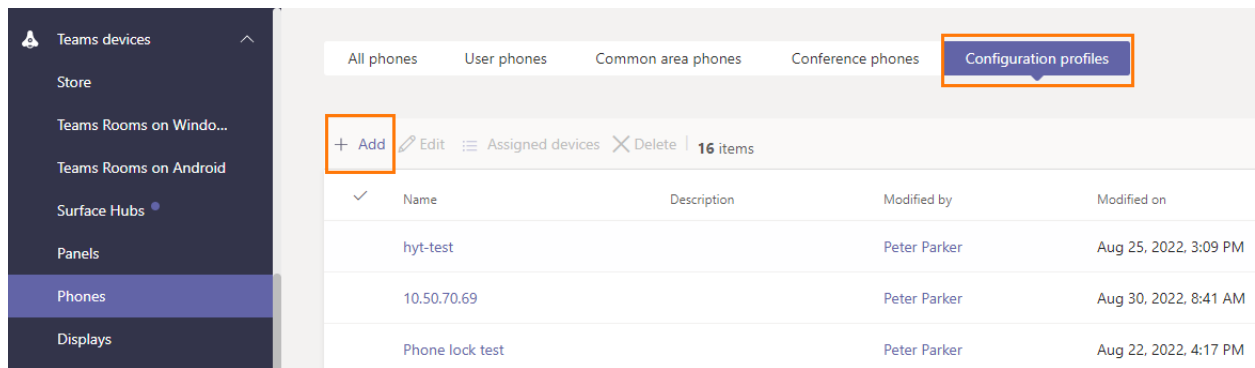


# Use Configuration Files

Use configuration profiles to manage settings and features for different Teams phones in your organization.

## Add a Configuration File

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones > Configuration profiles > Add**.



3. Enter a name for the profile and optionally add a friendly description.
4. Specify the settings you want for the profile, and then click **Save**.

**For Yealink MP series**

MP58, MP56, MP54, CP965

**General**

Device lock ☒ On

Timeout 30 seconds

Device lock PIN 123456

Language Chinese (Simplified, PRC)

Timezone (UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Date format DD/MM/YYYY

Time format 12 Hours (AM/PM)

**Calling settings**

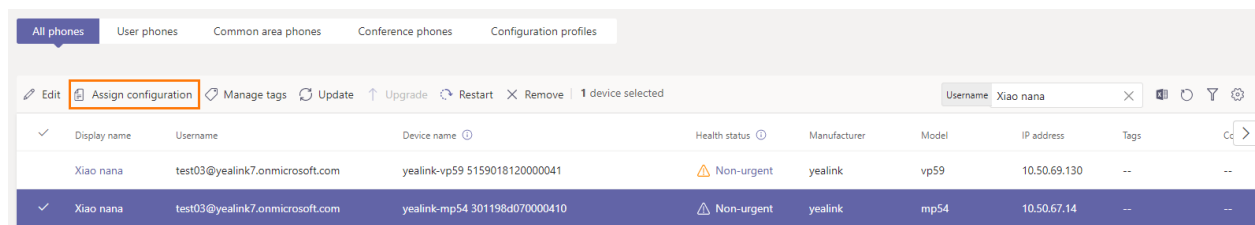
Advanced calling ☐ Off

ⓘ This setting may not be applicable if the device isn't updated.

The newly created configuration profile is displayed in the list of profiles.

## Assign Configuration File to Devices

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones**.
3. Select one or more devices and click **Assign configuration**.



4. Search for a configuration profile to assign to the selected devices and click **Apply**.

**Assign configuration**

Select configuration profile for these devices

For Yealink MP series

**Selected devices (1)**

Y3 yealink-mp54 301198d070000410  
301198d070000410

Apply Cancel

For the devices to which you applied the configuration policy, the **Action** column displays **Config Update** and the **Configuration profile** column displays the configuration profile name.

## Restart Devices

You can directly restart devices on the Teams admin center.

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones**.
3. Select one or more devices, and click **Update**.

The device will restart automatically and immediately.

## Remove Devices from Teams Admin Center

When you remove a device, all the associated data will be removed. Any user or resource accounts must be signed out of any device before it's removed. If this is the only device the account is used for, delete it from the [Microsoft 365 admin center](#).

1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones**.
3. Select one or more devices, and click **Remove**.

## Manage Devices on Intune

### Enroll Devices to Intune

Generally, Yealink Teams phone has pre-installed the Company Portal app.

Therefore, the devices of [Intune-licensed](#) users will be enrolled on Intune automatically when they sign in to Teams account on their devices.

For more information about Microsoft Intune, refer to [Microsoft Intune Documentation](#).

## Manage Device Compliance and Conditional Access

Compliance Policy and Conditional Access are two different features inside of Microsoft Intune. We can use them cooperatively to manage devices and improve device security.

What are Device Compliance and Conditional Access?

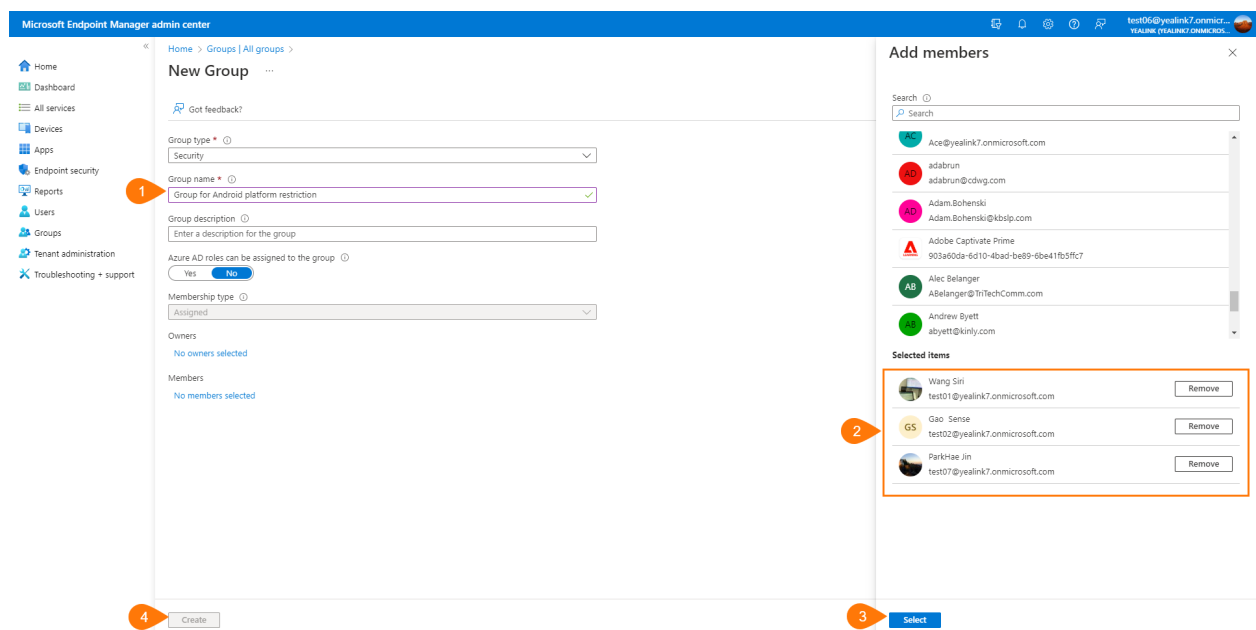
- Device Compliance: Tells you if your device is compliant or not.
- Conditional Access: Determines what to do with these devices depending on their compliant status.

For example, restrict users from enrolling on Intune unless their Android OS versions are later than 9.0.

## Step 1 - Create a Group

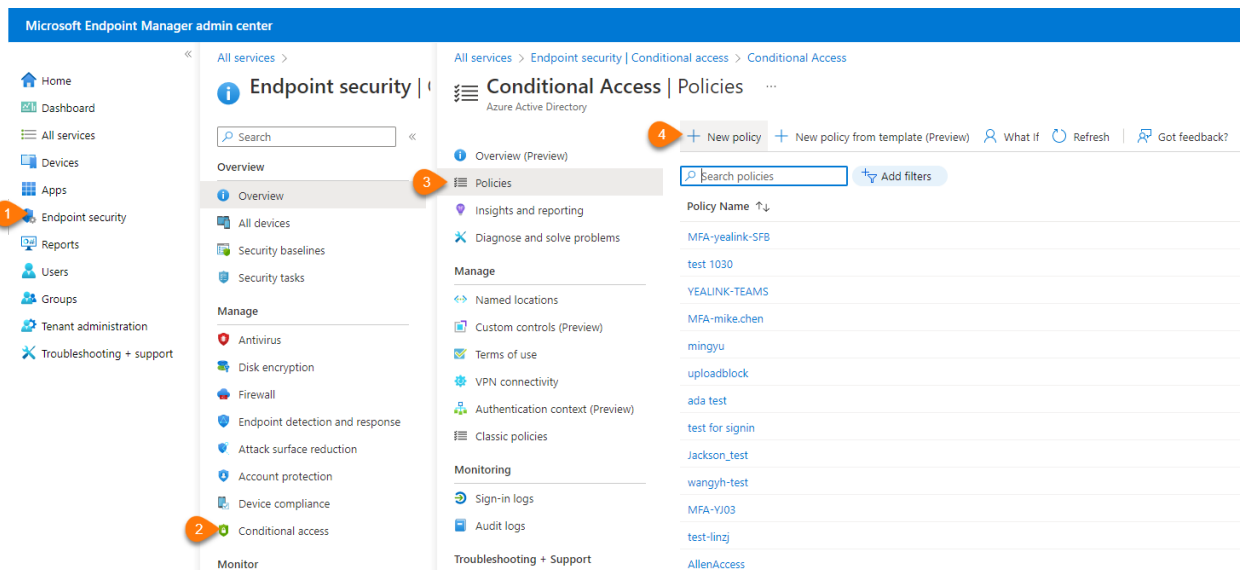
Skip this step if you already have a group that includes the user. Or you can add the user to the existing group.

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Groups** > **New group** to create a group that includes the users whose device platform is restricted.



## Step 2 - Set Conditional Access

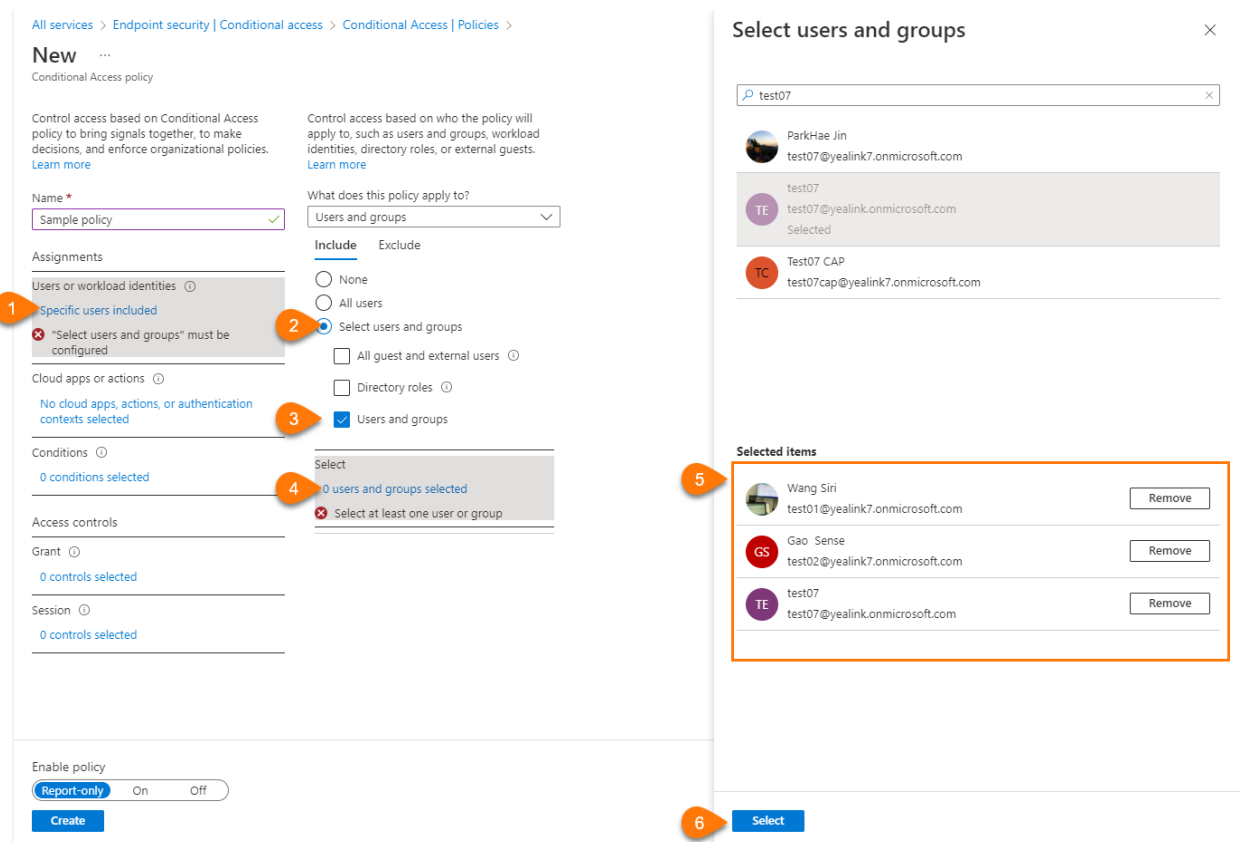
1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Endpoint security** > **Conditional access** > **Polices** > **New policy**.



3. Enter the policy name.

4. Under the **Users or workload identities** field, select the users or groups to which the policy applies.

- Do not select the check box of **All users**. Otherwise, the administrator is locked out.
- Select the users who will use their account to log into Teams phones and do the Intune authentication after you complete setting conditional access and device compliance.
- After you select the users, you can also click **...** > Remove to delete the selected users.



5. Under the **Cloud apps or actions** field, select the desired apps or actions to which this policy applies.

Home > New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  
Sample policy ✓

Assignments

Users or workload identities ⓘ  
Specific users included

Cloud apps or actions ⓘ  
No cloud apps, actions, or authentication contexts selected  
✗ "Select apps" must be configured

Conditions ⓘ  
0 conditions selected

Access controls

Grant ⓘ  
0 controls selected

Session ⓘ  
0 controls selected

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to  
Cloud apps

Include Exclude

☐ None  
☐ All cloud apps  
☒ Select apps

Select  
None  
✗ Select at least one app.

Select

Cloud apps

team

☒ Microsoft Teams  
cc15fd57-2c6c-4117-a88c-83b1d56b4bbe

☐ Teams Device Store  
4b8fd940-29bd-4956-b174-a2d772363942

Selected items

☒ Microsoft Teams  
cc15fd57-2c6c-4117-a88c-83b1d56b4bbe Remove

Enable policy  
Report-only On Off

Create

Select

6. Under the **Conditions** field, set the device platform to which this policy applies.

- If you want to restrict the login location, you can set the Locations under the Conditions tab.
- Select Android as the device platform because the operating system of Teams phone is Android.

Home > New ...  
Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  
Sample policy

Assignments

Users or workload identities ⓘ  
Specific users included

Cloud apps or actions ⓘ  
1 app included

Conditions ⓘ  
0 conditions selected

Access controls

Grant ⓘ  
0 controls selected

Session ⓘ  
0 controls selected

Device platforms ⓘ  
Not configured

Locations ⓘ  
Not configured

Client apps ⓘ  
Not configured

Filter for devices ⓘ  
Not configured

Enable policy  
Report-only On Off

Create

Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure ⓘ  
Yes No

Include Exclude

☐ Any device

☒ Select device platforms

☒ Android

☐ iOS

☐ Windows Phone

☐ Windows

☐ macOS

☐ Linux

Done

7. Under the **Grant** field, select the controls to be enforced.

- You must select the check boxes of **Require device to be marked as compliant** and **Require approved client app**. Therefore, these two rules will be verified when the policy verifies Yealink Teams phones.
- If your company has other restrictions on the controls, for example MFA, you can select the check box of Require multi-factor authentication.

Home >

## New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

Sample policy ✓

Assignments

Users or workload identities ⓘ

[Specific users included](#)

Cloud apps or actions ⓘ

[1 app included](#)

Conditions ⓘ

[1 condition selected](#)

Access controls

Grant ⓘ

1 controls selected

Session ⓘ

0 controls selected

Enable policy

Report-only On Off

Create

## Grant

Control access enforcement to block or grant access. [Learn more](#)

☐ Block access

☒ Grant access

☐ Require multifactor authentication ⓘ

☒ Require device to be marked as compliant ⓘ

⚠ Don't lock yourself out! Make sure that your device is compliant.

☐ Require Hybrid Azure AD joined device ⓘ

☒ Require approved client app ⓘ  
[See list of approved client apps](#)

☐ Require app protection policy ⓘ  
[See list of policy protected client apps](#)

For multiple controls

☒ Require all the selected controls

☐ Require one of the selected controls

Select

8. Enable this policy and click **Create**.

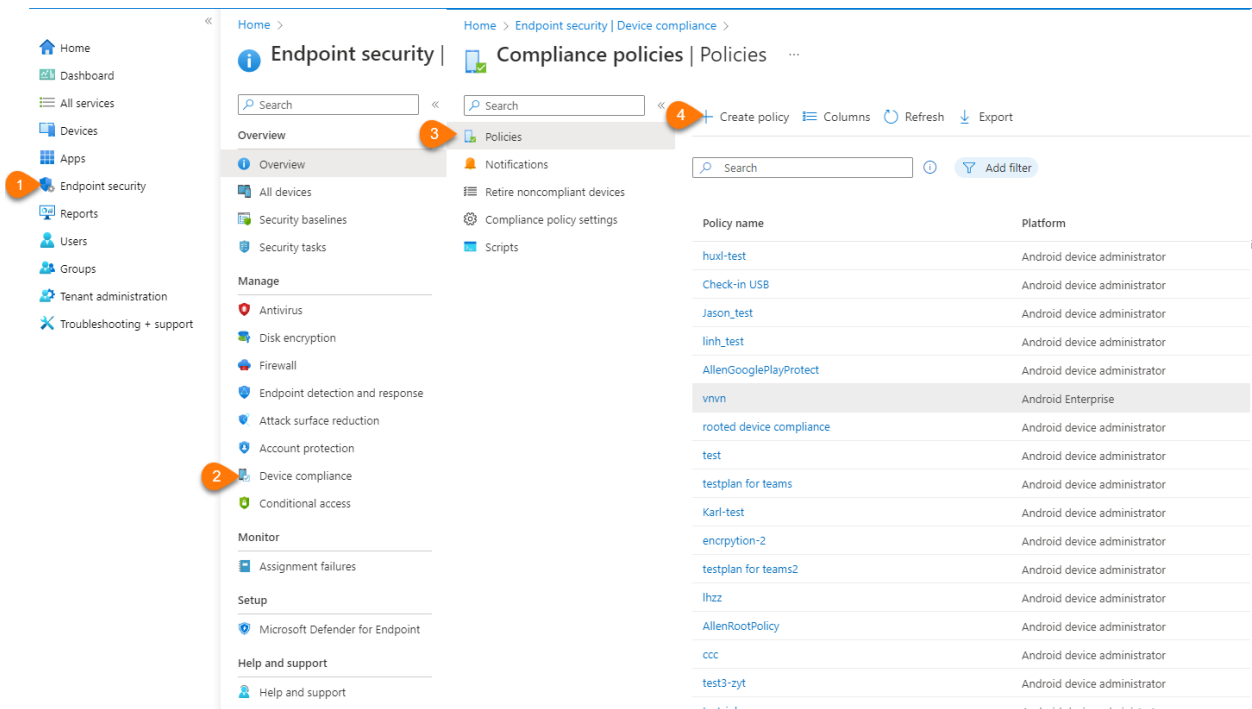
Enable policy

Report-only On Off

Create

## Step 3 - Set Device Compliance

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Endpoint security > Device compliance > Policies > Create policy**.



3. Select a **Platform** for this policy and click **Create**.

You can choose a platform according to your enterprise [enrollment methods for Android devices](#).

4. Under the **Basics** tab, specify a **Name** that helps you identify it later and click **Next**.

5. Under the **Compliance settings** tab, set the following settings and click **Next**.

1. Set the device health:

☒ Basics
 ☒ **2 Compliance settings**
☐ 3 Actions for noncompliance
 ☐ 4 Assignments
 ☐ 5 Review + create

---

☐ Microsoft Defender for Endpoint

---

☒ Device Health

|                                                                |                                                                                                 |
|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| Devices managed with device administrator ⓘ                    | <input type="button" value="Block"/> <input checked="" type="button" value="Not configured"/>   |
| Rooted devices ⓘ                                               | <input checked="" type="button" value="Block"/> <input type="button" value="Not configured"/>   |
| Require the device to be at or under the Device Threat Level ⓘ | <input type="text" value="Secured"/> <input checked="" type="button" value="v"/>                |
| Google Play Protect                                            |                                                                                                 |
| Google Play Services is configured ⓘ                           | <input type="button" value="Require"/> <input checked="" type="button" value="Not configured"/> |
| Up-to-date security provider ⓘ                                 | <input type="button" value="Require"/> <input checked="" type="button" value="Not configured"/> |
| Threat scan on apps ⓘ                                          | <input type="button" value="Require"/> <input checked="" type="button" value="Not configured"/> |
| SafetyNet device attestation ⓘ                                 | <input type="text" value="Not configured"/> <input checked="" type="button" value="v"/>         |

2. Set the operating system version:

#### Device Properties

##### Operating System Version

Minimum OS version ⓘ

5.0.0



Maximum OS version ⓘ

9.1.0



### 3. Set the system security:

#### System Security

##### Encryption

Require encryption of data storage on device. ⓘ

Require

Not configured

##### Device Security

Block apps from unknown sources ⓘ

Block

Not configured

Company Portal app runtime integrity ⓘ

Require

Not configured

Block USB debugging on device ⓘ

Block

Not configured

Minimum security patch level ⓘ

Not configured

Restricted apps ⓘ

Export

App name

App bundle ID

**i** Beginning in October 2020, some settings will not be supported on Android devices that are running Android 10 and later and are not Samsung Knox. These settings are labeled with Android 9 and earlier or Samsung Knox. Click to learn more.

#### All Android devices

These settings work for all Android OS versions and manufacturers.

Maximum minutes of inactivity before password is required ⓘ

Not configured



Require a password to unlock mobile devices ⓘ

Require

Not configured

#### Android 10 and later

These settings work for devices running Android 10 or later.

Password complexity ⓘ

None

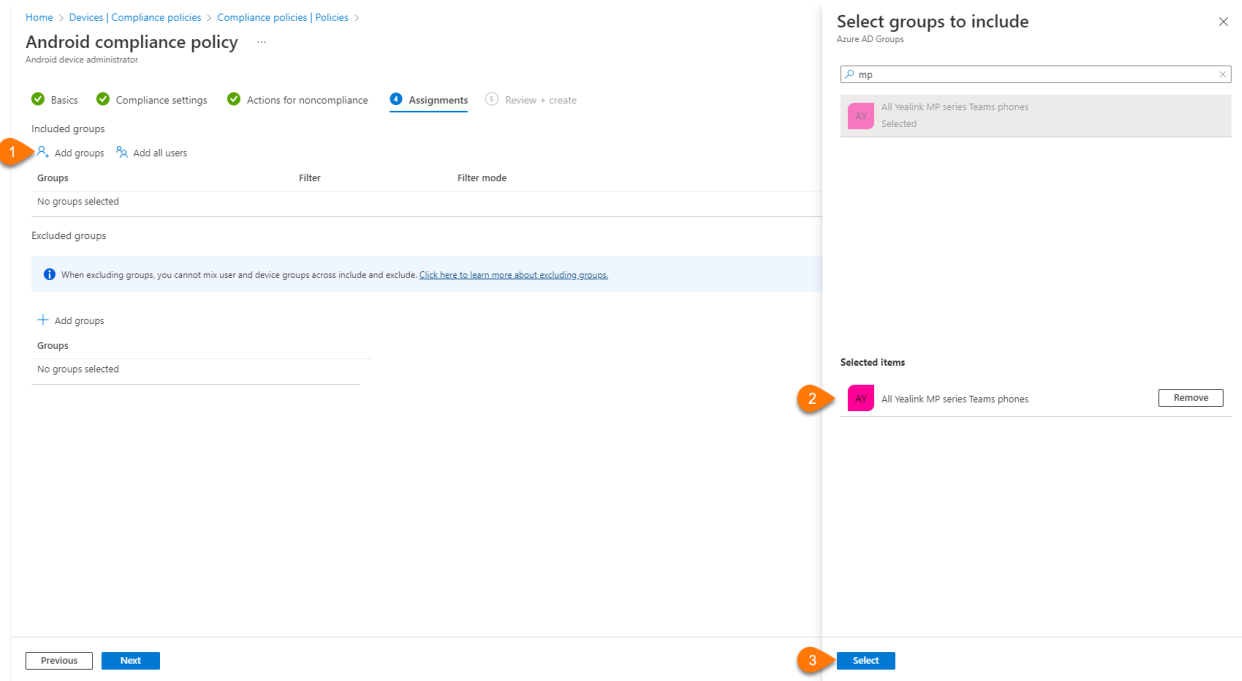


#### Android 9 and earlier or Samsung Knox

- Under the **Assignments** tab, assign this policy to the desired groups to which the users belong and click **Next**.

#### Note:

Do not assign this policy to all users. Otherwise, the administrator is blocked out.

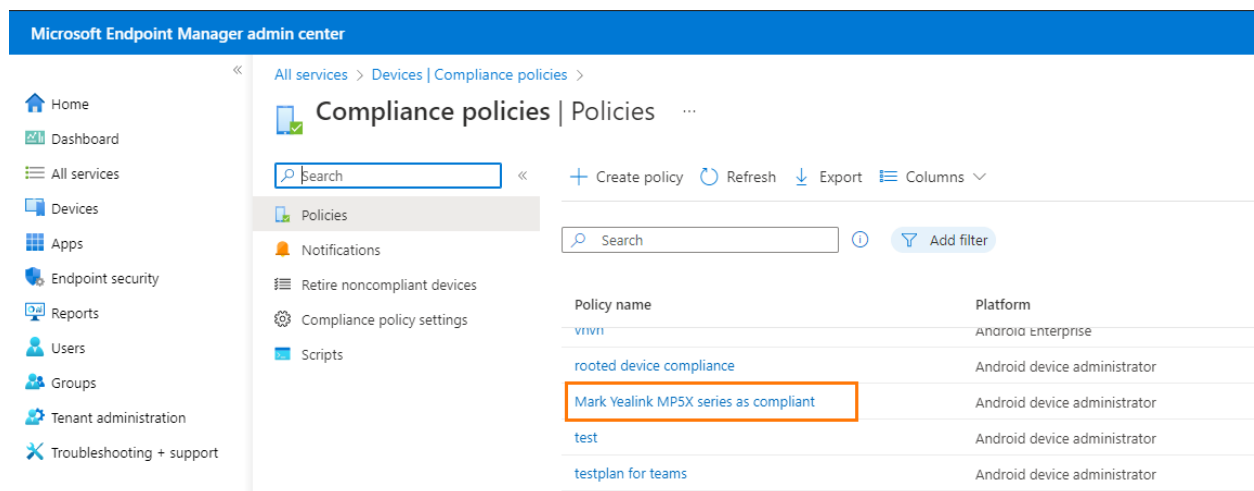


7. Click **Create**.

## Check the Status of the Compliance Policy

After you apply your policy, you can see the device sign-in status.

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Devices > Compliance**.
3. Click the name of the policy you create.



4. Click **Device status** or **User status** to check the corresponding compliance status.

| Search                            | Refresh                         | Export            | Columns             |
|-----------------------------------|---------------------------------|-------------------|---------------------|
| Overview                          | Search                          |                   |                     |
| Manage                            |                                 |                   |                     |
| Properties                        |                                 |                   |                     |
| Monitor                           |                                 |                   |                     |
| Device status                     |                                 |                   |                     |
| User status                       |                                 |                   |                     |
| Per-setting status                |                                 |                   |                     |
| Device                            | User Principal Name             | Compliance status | Last status update  |
| test05_Android_8/16/2022_6:47 ... | None                            | Not evaluated     |                     |
| test01_Android_9/22/2022_1:14 ... | test01@yealink7.onmicrosoft.com | Compliant         | 09/22/2022 09:29 AM |
| test09_Android_9/21/2022_3:18 ... | None                            | Not evaluated     |                     |
| test01_Android_9/8/2022_7:06 AM   | None                            | Not evaluated     |                     |
| test09_Android_8/24/2022_2:07 ... | None                            | Not evaluated     |                     |
| test09_Android_9/21/2022_12:25... | None                            | Not evaluated     |                     |
| test05_Android_9/8/2022_9:11 AM   | None                            | Not evaluated     |                     |
| test09_Android_9/20/2022_12:44... | None                            | Not evaluated     |                     |
| test01_Android_9/20/2022_12:01... | test01@yealink7.onmicrosoft.com | Compliant         | 09/21/2022 02:00 PM |

| Search                          | Refresh      | Export            | Columns             |
|---------------------------------|--------------|-------------------|---------------------|
| Overview                        | Search       |                   |                     |
| Manage                          |              |                   |                     |
| Properties                      |              |                   |                     |
| Monitor                         |              |                   |                     |
| Device status                   |              |                   |                     |
| User status                     |              |                   |                     |
| Per-setting status              |              |                   |                     |
| User Principal Name             | Device count | Compliance status | Last status update  |
| test01@yealink7.onmicrosoft.com | 4            | Compliant         | 09/22/2022 11:43 AM |

## Check the Sign-In Logs

After you apply your policy, you can see the device sign-in status.

1. Sign in to the [Azure Active Directory admin center](#) as an admin.
2. Go to **Azure Active Directory > Monitoring > Sign-in logs**.

Download

Export Data Settings

Troubleshoot

Refresh

Columns

Got feedback?

This view will be soon replaced with a view that includes refresh tokens and application sign-ins. Try out our new sign-ins preview. →

|                       |                          |               |                           |             |                |                          |             |                            |
|-----------------------|--------------------------|---------------|---------------------------|-------------|----------------|--------------------------|-------------|----------------------------|
| 9/22/2022, 9:57:23 AM | 232f2d4d-c652-4bfe-9...  | vcs01 Yealink | Office 365 Exchange O...  | Failure     | 46.101.140.131 | Frankfurt Am Main, He... | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:57:00 AM | 0f46549b-d53a-4ff2-a...  | vcs01 Yealink | Office 365 Exchange O...  | Failure     | 46.101.140.131 | Frankfurt Am Main, He... | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:56:59 AM | 08bba69f-376a-4409-8...  | vcs01 Yealink | Office 365 Exchange O...  | Failure     | 46.101.140.131 | Frankfurt Am Main, He... | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:56:58 AM | 1ab86cbd-1d15-4e26-...   | vcs01 Yealink | Office 365 Exchange O...  | Failure     | 46.101.140.131 | Frankfurt Am Main, He... | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:56:22 AM | dbffc97b-4dd4-4043-b...  | Peter Parker  | Azure Portal              | Success     | 117.28.234.43  | Fuzhou, Fujian, CN       | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:56:18 AM | b0089bce-04c8-460b-...   | ParkHae Jin   | Office 365 Exchange O...  | Success     | 170.114.10.202 | San Jose, California, US | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:56:15 AM | 307eb0ba-f7ce-431d-9...  | vcs01 Yealink | Office 365 Exchange O...  | Failure     | 46.101.140.131 | Frankfurt Am Main, He... | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:55:38 AM | 6f74519e-f1f6-4782-ae... | Gao Sense     | Microsoft Authenticati... | Success     | 117.28.234.43  | Fuzhou, Fujian, CN       | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:55:09 AM | cec73cbe-589f-4f92-a...  | MiMi Pan      | Microsoft Authenticati... | Success     | 117.28.234.43  | Fuzhou, Fujian, CN       | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:54:56 AM | 3afe47f3-ec85-482a-8...  | MiMi Pan      | Microsoft Authenticati... | Failure     | 117.28.234.43  | Fuzhou, Fujian, CN       | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:53:22 AM | 69bf7fa9-1182-40dd-8...  | Peter Parker  | Microsoft Authenticati... | Success     | 117.28.234.43  | Fuzhou, Fujian, CN       | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:53:19 AM | 6df55d07-c45b-449c-a...  | Peter Parker  | Microsoft Authenticati... | Failure     | 117.28.234.43  | Fuzhou, Fujian, CN       | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:53:11 AM | 65b1827b-7a06-4ade-...   | Zoey          | Microsoft Teams Web ...   | Interrupted | 117.28.234.43  | Fuzhou, Fujian, CN       | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:52:27 AM | d9f6933d-1a03-45a8-...   | lh12          | Microsoft Teams           | Success     | 117.28.234.43  | Fuzhou, Fujian, CN       | Not Applied | Single-factor authentic... |
| 9/22/2022, 9:52:00 AM | 0f46549b-d53a-4ff2-a...  | Wang Siri     | Microsoft Authenticati... | Success     | 117.28.234.43  | Fuzhou, Fujian, CN       | Not Applied | Single-factor authentic... |

3. Click the log to see more detailed information. For example, check the sign-in error code to find out why a user failed to sign in.

Dashboard > Yealink

Yealink | Sign-in logs

...

Download

Export Data Settings

Troubleshoot

Refresh

Columns

This view will be soon replaced with a view that includes refresh tokens and application sign-ins.

|                       |                          |               |                 |
|-----------------------|--------------------------|---------------|-----------------|
| 9/22/2022, 9:57:23 AM | 232f2d4d-c652-4bfe-9...  | vcs01 Yealink | Office 365 Exch |
| 9/22/2022, 9:57:00 AM | 0f46549b-d53a-4ff2-a...  | vcs01 Yealink | Office 365 Exch |
| 9/22/2022, 9:56:59 AM | 08bba69f-376a-4409-8...  | vcs01 Yealink | Office 365 Exch |
| 9/22/2022, 9:56:58 AM | 1ab86cbd-1d15-4e26-...   | vcs01 Yealink | Office 365 Exch |
| 9/22/2022, 9:56:22 AM | dbffc97b-4dd4-4043-b...  | Peter Parker  | Azure Portal    |
| 9/22/2022, 9:56:18 AM | b0089bce-04c8-460b-...   | ParkHae Jin   | Office 365 Exch |
| 9/22/2022, 9:56:15 AM | 307eb0ba-f7ce-431d-9...  | vcs01 Yealink | Office 365 Exch |
| 9/22/2022, 9:55:38 AM | 6f74519e-f1f6-4782-ae... | Gao Sense     | Microsoft Auth  |
| 9/22/2022, 9:55:09 AM | cec73cbe-589f-4f92-a...  | MIMI Pan      | Microsoft Auth  |
| 9/22/2022, 9:54:56 AM | 3afe47f3-ec85-482a-8...  | MIMI Pan      | Microsoft Auth  |
| 9/22/2022, 9:53:22 AM | 69b77fa9-1182-40dd-8...  | Peter Parker  | Microsoft Auth  |
| 9/22/2022, 9:53:19 AM | 6df55007-c45b-449c-...   | Peter Parker  | Microsoft Auth  |
| 9/22/2022, 9:53:11 AM | 65b1827b-7a06-4ade-...   | ZoeY          | Microsoft Team  |
| 9/22/2022, 9:52:27 AM | d9fe933d-1ad3-45a8-...   | lh12          | Microsoft Team  |
| 9/22/2022, 9:52:00 AM | 0f46549b-d53a-4ff2-a...  | Wang Siri     | Microsoft Auth  |
| 9/22/2022, 9:51:41 AM | 2f4965ec-3fc8-46d7-b...  | Wang Siri     | Microsoft Auth  |
| 9/22/2022, 9:51:41 AM | 12e4727d-cba1-4fbc-b...  | Peter Parker  | Azure Portal    |
| 9/22/2022, 9:51:34 AM | e6a114c8-cabb-4fc7-b...  | Peter Parker  | Azure Portal    |
| 9/22/2022, 9:51:24 AM | cea8ee51-e6cd-4bfe-b...  | Wang Siri     | Microsoft Auth  |
| 9/22/2022, 9:51:00 AM | bdb14cd1-06d1-4a91-...   | vcs01 Yealink | Office 365 Exch |
| 9/22/2022, 9:50:22 AM | 59931d25-b8d2-4a62-...   | Wang Siri     | Microsoft Team  |
| 9/22/2022, 9:50:21 AM | d4d34033-35d5-423e-...   | Wang Siri     | Microsoft Team  |
| 9/22/2022, 9:49:42 AM | 02d7684f-c40f-46b8-b...  | vcs01 Yealink | Office 365 Exch |

Activity Details: Sign-ins

Basic info

Location

Device info

Authentication Details

Conditional Access

Report-only

Date

9/22/2022, 9:51:41 AM

Request ID

2f4965ec-3fc8-46d7-b664-d29485bc0f01

Correlation ID

83f4775a-471e-41cc-8fd7-66c753c1b2b9

Authentication requirement

Single-factor authentication

Status

Failure

Continuous access evaluation

No

Sign-in error code

50126

Failure reason

Error validating credentials due to invalid username or password.

Additional Details

The user didn't enter the right credentials. It's expected to see some number of these errors in your logs due to users making mistakes.

Troubleshoot Event

Follow these steps:

[Launch the Sign-in Diagnostic.](#)

1. Review the diagnosis and act on suggested fixes.

User

[Wang Siri](#)

Username

test01@yealink7.onmicrosoft.com

User ID

53732d9e-d85e-4d40-93cd-6fbafe1f13c6

Sign-in identifier

test01@yealink7.onmicrosoft.com

User type

Member

Cross tenant access type

None

Application

Microsoft Authentication Broker

Application ID

29d9ed98-a469-4536-ade2-f981bc1d605e

Resource

Device Registration Service

Resource ID

01cb2876-7ebd-4aa4-9cc9-d28bd4d359a9

Resource tenant ID

da574a7f-d308-4fe7-93d7-f055275b863d

Home tenant ID

da574a7f-d308-4fe7-93d7-f055275b863d

For other activity details, see the Microsoft's doc on [Sign-in logs in Azure Active Directory](#).

# Troubleshooting

## Cannot Sign In to Teams Accounts?

**Issue description:**

Users cannot sign in to Teams accounts on their devices.

**Causes & Solution:**

| Causes                 | Solutions                                                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wrong passwords        | <a href="#">Contact admin to get the right user credentials</a>                                                                                                      |
| Unavailable network    | <a href="#">Troubleshoot the network</a>                                                                                                                             |
| Low firmware version   | <a href="#">Upgrade the firmware/software</a>                                                                                                                        |
| Account/hardware issue | <div>- <a href="#">Use other accounts to sign in</a><br/>- <a href="#">Sign in to other devices with your account</a><br/>- <a href="#">Reset your devices</a></div> |
| Other causes           | <a href="#">Check the detailed reason on Azure Active Directory Admin Center</a>                                                                                     |

If the above solution cannot solve the problem, please provide the diagnostic files and contact [Yealink technical support](#).

### Solution 1 - Get the Right User Credentials

If the password is wrong or changed by other persons, you can contact your administrator to get the right user credentials.

**Related topic:**

[Change Account Password](#)

## Solution 2 - Check the Network Environment

1. On the device, click the account avatar.
2. Click **Settings> Device settings> About** to check whether the device has obtained the IP Address.
3. If not, troubleshoot your network setting, and make sure your network environment is available. See [Prepare your organization's network for Microsoft Teams](#).

## Solution 3 - Upgrade Your Device Firmware to the Latest

### Step 1 (1/2): Check the device firmware

1. On the phone, click the account avatar.
2. Click **Settings> Device settings> About** to check whether it is the latest firmware.

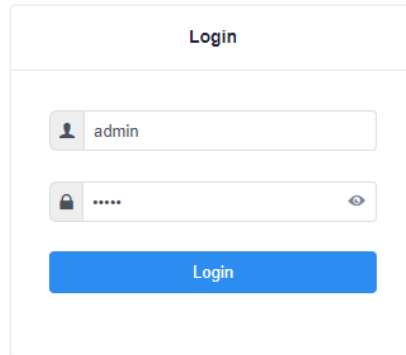
| Product | Latest Firmware Version      |
|---------|------------------------------|
| VP59    | <a href="#">91.15.0.102</a>  |
| MP58    | <a href="#">122.15.0.91</a>  |
| MP56    | <a href="#">122.15.0.91</a>  |
| MP54    | <a href="#">122.15.0.91</a>  |
| MP50    | <a href="#">131.410.0.55</a> |
| CP965   | <a href="#">143.15.0.12</a>  |

3. If it is not the latest, follow the steps below to update it.

### Step 2 (2/2): Update the device firmware

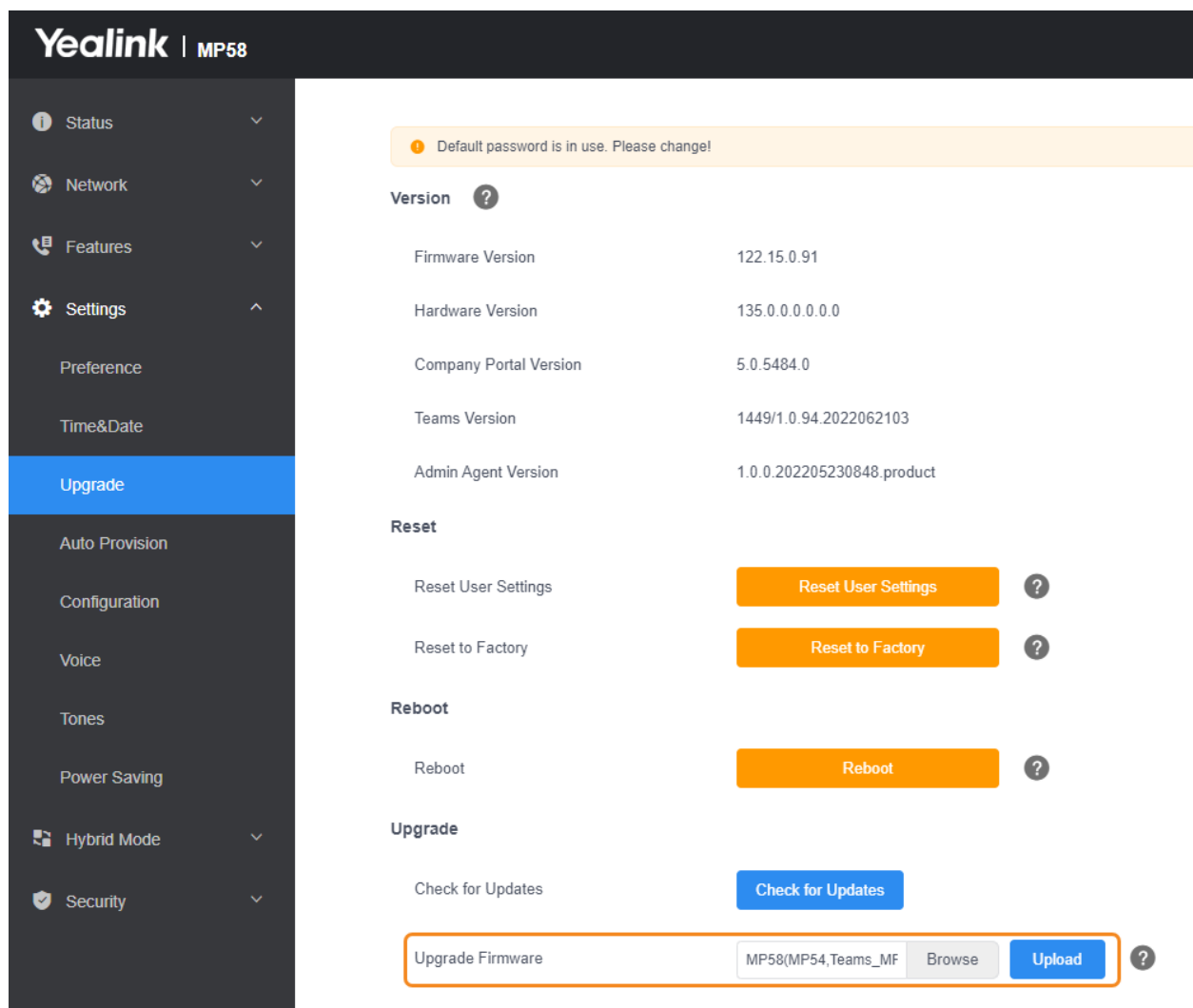
1. Open a web browser and download the latest firmware.
2. Enter the phone IP address in the address bar to access the web user interface.  
If your phone IP address is *10.11.12.13*, enter <http://10.11.12.13> or <https://10.11.12.13>.
3. Enter the admin user name and password (the default user name and password are *admin*).

4. Click **Login**.

A login form with a white background and a thin gray border. At the top, the word "Login" is centered in a small, dark font. Below this, there are two input fields. The first field has a user icon on the left and the text "admin" inside. The second field has a lock icon on the left, five dots in the middle, and an eye icon on the right. Below these fields is a blue button with the word "Login" in white text.

5. Go to **Settings > Upgrade > Upgrade Firmware > Browse**.

6. Select the latest firmware and click **Upload**.



## Solution 4 - Use Other Accounts to Sign In/Sign in on Other Devices with Your Account

If you have [got the right user credentials](#), [checked the network](#), and [upgraded your firmware](#), but you still cannot solve the problem, try the following to check whether your account is available or your device can work well:

- Check your device issue (for example, the device OS version is too low):
  - If your account can sign in on other devices but not yours
  - If other accounts cannot sign in on your devices
- [Check your account issue](#) if your account cannot sign in on both your and other devices.

### Related topics:

- [Sign in on the Teams phone](#)
- [Sign in on a web browser](#)

## Solution 5 - Reset Your Device

Long-press the pound key (#) and the star key (\*) for about 6 seconds when the phone is idle.

## Solution 6 - Check Detailed Reasons on Azure Active Directory Admin Center

1. Sign in to the [Azure Active Directory admin center](#) as an admin.
2. Go to **Azure Active Directory > Monitoring > Sign-in logs**.
3. Add a filter to see the user who failed to sign in.
4. Click the log to see the detailed failure reason, and you can solve the issue with the recommended steps.

For error code 50119, see [cannot enroll devices in Intune?](#).

The screenshot shows the Azure Active Directory Admin Center interface. On the left, the 'Monitoring' section is expanded, and 'Sign-in logs' is selected. The main pane displays a table of sign-in logs. A filter is applied to show only failed sign-ins. One log entry is highlighted, and a detailed view is shown on the right. The detailed view includes the following information:

| Basic info                   | Location                                                                                                                                 | Device info | Authentication Details | Conditional Access | Report-only |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------------------|--------------------|-------------|
| Date                         | 9/28/2022, 9:19:11 PM                                                                                                                    |             |                        |                    |             |
| Request ID                   | 1d8bfb3-e465-4ab8-b22b-9ec9026c7e00                                                                                                      |             |                        |                    |             |
| Correlation ID               | 00d5a875-e269-43b3-a1fd-a077d428baba                                                                                                     |             |                        |                    |             |
| Authentication requirement   | Single-factor authentication                                                                                                             |             |                        |                    |             |
| Status                       | Failure                                                                                                                                  |             |                        |                    |             |
| Continuous access evaluation | No                                                                                                                                       |             |                        |                    |             |
| Sign-in error code           | 50126                                                                                                                                    |             |                        |                    |             |
| Failure reason               | Error validating credentials due to invalid username or password.                                                                        |             |                        |                    |             |
| Additional Details           | The user didn't enter the right credentials. It's expected to see some number of these errors in your logs due to users making mistakes. |             |                        |                    |             |
| Troubleshoot Event           | Follow these steps:<br>Launch the Sign-in Diagnostic.<br>1. Review the diagnosis and act on suggested fixes.                             |             |                        |                    |             |
| User                         | vcso1 Yealink                                                                                                                            |             |                        |                    |             |
| Username                     | vcso1@yealink7.onmicrosoft.com                                                                                                           |             |                        |                    |             |
| User ID                      | a85dec9f-f1d9-45b0-8945-36ef1299e21                                                                                                      |             |                        |                    |             |
| Sign-in identifier           | vcso1@yealink7.onmicrosoft.com                                                                                                           |             |                        |                    |             |
| User type                    | Member                                                                                                                                   |             |                        |                    |             |
| Cross tenant access type     | None                                                                                                                                     |             |                        |                    |             |
| Application                  | Office 365 Exchange Online                                                                                                               |             |                        |                    |             |
| Application ID               | 00000002-0000-0ff1-ce00-000000000000                                                                                                     |             |                        |                    |             |
| Resource                     | Office 365 Exchange Online                                                                                                               |             |                        |                    |             |
| Resource ID                  | 00000002-0000-0ff1-ce00-000000000000                                                                                                     |             |                        |                    |             |
| Resource tenant ID           | da574a7f-d308-4fe7-93d7-f055275b863d                                                                                                     |             |                        |                    |             |
| Home tenant ID               | da574a7f-d308-4fe7-93d7-f055275b863d                                                                                                     |             |                        |                    |             |

## Solution 7 - Send the Diagnostic Files to Yealink Support

1. [Export the device diagnostic files](#).
2. Provide the exact time point when the problem happened.
3. Provide the steps that cause the problem and what solutions you have done.
4. Take a video or photo to show the wrong message or the problem.  
The above information can greatly help us locate and address the problem.
5. Go to [Yealink support website](#) to create a ticket and upload the above information.

## Cannot Enroll Devices in Intune?

### Issue description:

Users failed to enroll devices in Intune.

### Causes:

Microsoft Endpoint Manager admin center might have some restrictions on the device limit, device platform limit, or others.

### Solution:

- [Step 1 - Check the detailed reason](#)

- [Step 2 - Solve the "Device cap reached" issue](#)
- [Step 3 - Solve the "Device platform restriction" issue](#)

## Step 1 - Check the Detailed Reason

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Devices > Monitor > Enrollment failures > Select user**.
3. Search the user that failed to enroll on Intune and click **Select**.

Microsoft Endpoint Manager admin center

Home > Devices | Monitor > Monitor

**Monitor | Enrollment failures**

Search Filter Refresh Export

For a graphical view of enrollment failures see here.

**Select user** **All users**

| Date               | Failure            | OS      | OS version |
|--------------------|--------------------|---------|------------|
| 09/09/22, 9:12 PM  | Device cap reached | Android | 9.0        |
| 09/20/22, 6:42 PM  | Device cap reached | Android | 9.0        |
| 09/14/22, 9:32 PM  | Device cap reached | Android | 11.0       |
| 09/14/22, 9:30 PM  | Device cap reached | Android | 11.0       |
| 09/14/22, 9:28 PM  | Device cap reached | Android | 11.0       |
| 09/14/22, 6:01 PM  | Device cap reached | Android | 9.0        |
| 09/14/22, 10:36 AM | Device cap reached | Android | 9.0        |
| 09/16/22, 3:17 PM  | Device cap reached | Android | 9.0        |
| 09/09/22, 9:23 PM  | Device cap reached | Android | 9.0        |
| 09/09/22, 9:16 PM  | Device cap reached | Android | 9.0        |
| 09/19/22, 8:32 PM  | Device cap reached | Android | 11.0       |
| 09/09/22, 9:09 PM  | Device cap reached | Android | 9.0        |
| 09/19/22, 8:33 PM  | Device cap reached | Android | 11.0       |

**Select user**

Search wang siri

Wang Siri  
test01@yrealink7.onmicrosoft.com  
Selected

**Selected items**

Wang Siri  
test01@yrealink7.onmicrosoft.com

**Select**

4. See the reason and the recommended troubleshooting step.

Microsoft Endpoint Manager admin center

Home > Devices | Monitor > Monitor

**Monitor | Enrollment failures**

Search Filter Refresh Export

For a graphical view of enrollment failures see here.

**Select user** **All users**

| Date               | Failure            | OS      | OS version |
|--------------------|--------------------|---------|------------|
| 09/09/22, 9:12 PM  | Device cap reached | Android | 9.0        |
| 09/20/22, 6:42 PM  | Device cap reached | Android | 9.0        |
| 09/14/22, 9:32 PM  | Device cap reached | Android | 11.0       |
| 09/14/22, 9:30 PM  | Device cap reached | Android | 11.0       |
| 09/14/22, 9:28 PM  | Device cap reached | Android | 11.0       |
| 09/14/22, 6:01 PM  | Device cap reached | Android | 9.0        |
| 09/14/22, 10:36 AM | Device cap reached | Android | 9.0        |
| 09/16/22, 3:17 PM  | Device cap reached | Android | 9.0        |
| 09/09/22, 9:23 PM  | Device cap reached | Android | 9.0        |
| 09/09/22, 9:16 PM  | Device cap reached | Android | 9.0        |
| 09/19/22, 8:32 PM  | Device cap reached | Android | 11.0       |
| 09/09/22, 9:09 PM  | Device cap reached | Android | 9.0        |
| 09/19/22, 8:33 PM  | Device cap reached | Android | 11.0       |

**Enrollment failure**

**Details**  
The user attempted to enroll more devices than maximum allowed.

**Recommended Steps**  
If you do not already allow 15 devices per user, you can increase the Device Limit Restrictions setting. Otherwise, the user must unenroll a device before attempting to enroll another. \n\nIf the user has not reached the maximum number of devices enrolled, check for these issues:  
\n\nMultiple entries for the same device object exist due to multiple enrollment attempts in a short amount of time. These should resolve without further action. \n\nAn entry exists in Intune for a device that no longer communicates with the service. You can delete this device entry.

**Additional Resources**  
[Learn more about device limit restrictions.](#)  
[Learn more about removing devices from Microsoft Intune.](#)

**Device Details**  
Enrollment Start 9/20/2022 6:42:06 PM  
OS Android device administrator  
OS Version 9.0

**Get Support**  
If you can't resolve this issue, [contact support](#) and paste the below Activity ID into the ticket details.  
Activity ID: 255e10d9-6bcc-4e5e-93e9-d6f49d5db9a

## Step 2 - Solve the “Device Cap Reached” Issue

If it is caused by the device cap limit, you can follow the steps below to solve the problem.

If you do not set a device cap:

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Devices > Enroll devices > Enrollment device limit restrictions > Create restrictions**.
3. Set the basic information and click **Next**.

« [All services](#) > [Devices | Enroll devices](#) > [Enroll devices | Enrollment device limit restrictions](#) >

## Create restriction

Device limit restriction

1 Basics 2 Device limit 3 Scope tags 4 Assignments 5 Review + create

Name \* ①  ✓

Description ①

Previous Next 2

4. Set the device limit to 15 and click **Next**.

« All services > Devices | Enroll devices > Enroll devices | Enrollment device limit restrictions >

## Create restriction ...

Device limit restriction

✓ Basics 2 **Device limit** 3 Scope tags 4 Assignments 5 Review + create

Specify the maximum number of devices a user can enroll.

Device limit 1 15

Previous Next 2

5. Assign this restriction to one or several groups and click **Next**.

All services > Devices | Enroll devices > Enroll devices | Enrollment device limit restrictions >

## Create restriction ...

Device limit restriction

✓ Basics ✓ Device limit ✓ Scope tags 4 **Assignments** 5 Review + create

Included groups 1 Add groups

Groups Group Members

No groups selected

### Select groups to include

Azure AD Groups

MP

All Yealink MP series Teams phones  
Selected

Selected items 2 All Yealink MP series Teams phones Remove

Previous Next 4 3 Select

6. Click **Create**.

**If you do not set a device cap or the device cap is less than 15 (max value)**

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Devices > Enroll devices > Enrollment device limit restrictions**.
3. Click a restriction name and click **Properties**.
4. Check whether the device limit is set to 15 (max value) and assigned to a group that includes the user.

[Home](#) > [Devices | Enroll devices](#) > [Enroll devices | Enrollment device limit restrictions](#) > [SMAPLE POLICY-ZYD](#)

## SMAPLE POLICY-ZYD | Properties ...

<<

 Overview

Manage

 **Properties**

**Basics** [Edit](#)

Name

SMAPLE POLICY-ZYD

Description

TEST01\TEST02\TEST07

**Device limit** [Edit](#)

Device limit

15

**Scope tags** [Edit](#)

Default

**Assignments** [Edit](#)

Included groups

All Yealink MP series Teams phones  
SAMPLE GROUP-ZYD

If not, click **Edit** to change them.

**If your existing device restriction cap is set to 15 (the max value), you need to delete some device sign-in logs, as described below:**

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Devices > All devices**.
3. Search the name of the user that failed to sign in.
4. Select **Bulk Device Actions**.

Microsoft Endpoint Manager admin center

Home > Devices

Devices | All devices

Search: wang siri

Refresh Filter Columns Export Bulk Device Actions

Showing 1 to 14 of 14 records

| Device name ↑↓              | Managed by ↑↓ | Ownership ↑↓ | Compliance ↑↓ |
|-----------------------------|---------------|--------------|---------------|
| test01_Android_9/13/2022... | Intune        | Unknown      | Not Evaluated |
| test01_Android_9/20/2022... | Intune        | Personal     | Compliant     |
| test01_Android_9/21/2022... | Intune        | Personal     | Compliant     |
| test01_Android_9/22/2022... | Intune        | Personal     | Not Evaluated |

5. Select the desired device platform, select **Delete** from the action drop-down menu and click **Next**.

Home > Devices | All devices >

## Bulk device action

1 Basics 2 Devices 3 Review + create

OS \* Android (device administrator)

Device action \* Delete

**i** If you delete this device, you will no longer be able to view or manage the device from the Intune portal. The device will no longer be allowed to access your company's corporate resources. Company data may be wiped from the device if the device tries to check-in after it is deleted.

6. Click **Select device to include**, select the devices you want to delete, and click **Next**.

Home > Devices | All devices >

Bulk device action

At least one device must be selected

0 devices selected (100 max)

No devices added

+ Select devices to include

Previous Next

Select devices

wang siri

OS == Android (device administrator) Add filter

|                                   |                                 |                            |
|-----------------------------------|---------------------------------|----------------------------|
| test01_Android_9/13/2022_1:20 PM  | test01@yealink7.onmicrosoft.com | Android (device adminis... |
| test01_Android_9/20/2022_12:01 PM | test01@yealink7.onmicrosoft.com | Android (device adminis... |
| test01_Android_9/21/2022_9:59 AM  | test01@yealink7.onmicrosoft.com | Android (device adminis... |
| test01_Android_9/22/2022_1:14 AM  | test01@yealink7.onmicrosoft.com | Android (device adminis... |
| test01_Android_9/22/2022_1:52 AM  | test01@yealink7.onmicrosoft.com | Android (device adminis... |
| test01_Android_9/6/2022_1:08 PM   | test01@yealink7.onmicrosoft.com | Android (device adminis... |
| test01_Android_9/6/2022_1:34 PM   | test01@yealink7.onmicrosoft.com | Android (device adminis... |
| test01_Android_9/6/2022_2:30 AM   | test01@yealink7.onmicrosoft.com | Android (device adminis... |
| test01_Android_9/7/2022_11:39 AM  | test01@yealink7.onmicrosoft.com | Android (device adminis... |
| test01_Android_9/7/2022_12:33 PM  | test01@yealink7.onmicrosoft.com | Android (device adminis... |

Selected devices

|                                  |                                 |                        |        |
|----------------------------------|---------------------------------|------------------------|--------|
| test01_Android_9/7/2022_12:33 PM | test01@yealink7.onmicrosoft.com | Android (device adm... | Remove |
| test01_Android_9/7/2022_11:39 AM | test01@yealink7.onmicrosoft.com | Android (device adm... | Remove |

Select

7. Click **Create** to delete the selected devices.

## Step 3 - Solve the “Device Platform Restriction” Issue

If it is caused by the device platform limit, you can follow the steps below to solve the problem.

**Before you begin:**

Suppose that you have [created a group](#) and the user who failed to sign in is in the group.

1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Devices > Enroll devices > Enrollment device platform restrictions**.
3. Select the platform you want and click **Create restriction**.
4. Enter the restriction name.
5. Set the platform restrictions.

Microsoft Endpoint Manager admin center

Home > Devices > Enroll devices > Enrollment device platform restrictions >

### Create restriction

Device type restriction

Basics Platform settings Scope tags Assignments Review + create

Specify the platform configuration restrictions that must be met for a device to enroll. Use compliance policies to restrict devices after enrollment. Define versions as major.minor.build. Version restrictions only apply to devices enrolled with the Company Portal. Intune classifies devices as personally-owned by default. Additional action is required to classify devices as corporate-owned. [Learn more](#).

| Type                              | Platform                                    | versions                         | Personally owned                            | Device manufacturer |
|-----------------------------------|---------------------------------------------|----------------------------------|---------------------------------------------|---------------------|
| Android Enterprise (work profile) | <a href="#">Allow</a> <a href="#">Block</a> | Allow min/max range:<br>Min Max  | <a href="#">Allow</a> <a href="#">Block</a> | Manufacturer name   |
| Android device administrator      | <a href="#">Allow</a> <a href="#">Block</a> | Allow min/max range:<br>5.0 11.0 | <a href="#">Allow</a> <a href="#">Block</a> | Manufacturer name   |

Previous Next

6. Assign the restriction to the desired group.

Microsoft Endpoint Manager admin center

Home > Devices > Enroll devices > Enrollment device platform restrictions >

### Create restriction

Device type restriction

Basics Platform settings Scope tags Assignments Review + create

Included groups

Add group

Groups Group Members

No groups selected

Select groups to include

Azure AD Groups

android

AB Android block test

GF Group for Android platform restriction Selected

Wangyh-test-android9-restriction

Selected items

GF Group for Android platform restriction Remove

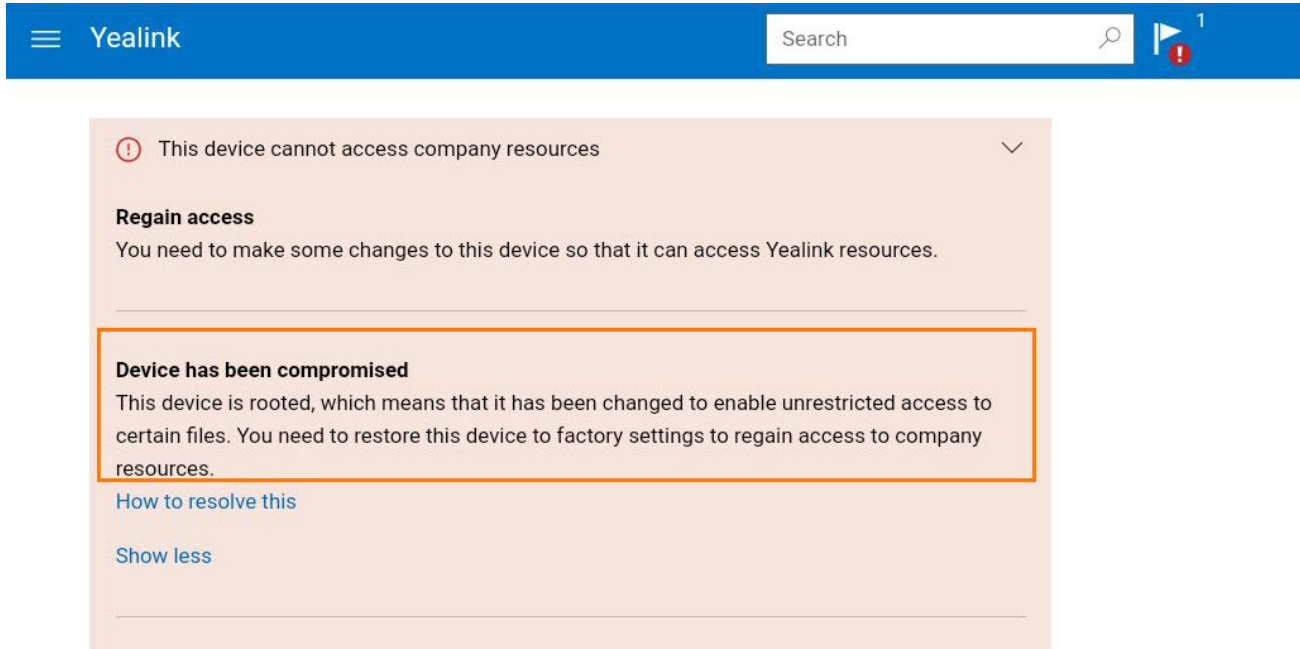
Previous Next Select

7. Click **Next** to preview the settings and click **Create**.

# Why Does the Screen Prompt “Rooted Device”?

## Issue description:

When you enroll devices into Company Portal, the devices are marked as non-compliant, as illustrated in the image below. To solve this issue, please follow the steps below:



## Causes:

Your company has set a compliance policy that blocks rooted devices, and Yealink Teams devices are detected as rooted by Microsoft. Therefore, the device is not compliant with the policy and cannot sign in.

## Solution:

1. See [Upgrade Your Device to the Latest Firmware](#) to upgrade your device firmware.
2. If the issue cannot be solved after upgrading to the latest firmware, please [provide the diagnostic files](#) and contact Yealink technical support.