

Yealink Teams Phone Setup Guide with Microsoft Configuration Platforms

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 MP52 (E2)/MP54 (E2)/MP56 (E2)/MP58 (E2)/MP55 E2
- Yealink VP59
- Yealink CP965

Users & Licenses

Understand License Types

- ! • The apps or services will be included in the [Microsoft cloud-based suite for Office 365 and Microsoft 365](#). You can go to **Billing > Purchase services** on the [Microsoft 365 admin center](#) to buy licenses.
- The license takes 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	Services or apps you need
Sign in to Teams	Ensure that the selected license (e.g., the Common Area Phone) includes the Microsoft Teams app.

	Apps (6)  Show apps for: All licenses  ☒ Select all ☒ Azure Active Directory Premium P1 Common Area Phone ☒ Exchange Online (Plan 2) Common Area Phone ☒ Microsoft 365 Phone System Common Area Phone ☒ Microsoft Intune Common Area Phone ☒ Microsoft Teams Common Area Phone ☒ Skype for Business Online (Plan 2) Common Area Phone
Common Area Phone	Common Area Phone license Licenses (1)*  ☒ Assign user a product license ☐ Audio Conferencing for non-China users 35 of 35 licenses available ☐ Azure Active Directory Basic The prepaid subscription for this product is no longer active. You need to buy a subscription before you can assign a license. ☐ Business Apps (free) 1 of 6 licenses available ☒ Common Area Phone you're out of licenses. If you turn this on, we'll try to buy an additional license for you.
Calendar feature	Ensure that the selected license (e.g., the Common Area Phone) includes the Exchange Online app.

	Apps (6)  Show apps for: All licenses  ☒ Select all ☒ Azure Active Directory Premium P1 Common Area Phone ☒ Exchange Online (Plan 2) Common Area Phone ☒ Microsoft 365 Phone System Common Area Phone ☒ Microsoft Intune Common Area Phone ☒ Microsoft Teams Common Area Phone ☒ Skype for Business Online (Plan 2) Common Area Phone
Intune (manage device and apply policies on Intune)	Ensure that the selected license (e.g., Microsoft 365 E3) includes the Microsoft Intune app. ☒ Microsoft Defender for Endpoint Plan 1 Microsoft 365 E3 ☒ Microsoft Forms (Plan E3) Microsoft 365 E3 ☒ Microsoft Intune Microsoft 365 E3 ☒ Microsoft Kaizala Pro Microsoft 365 E3
Call queue	Ensure that the selected license (e.g., the Office 365 E5 without Audio Conferencing) includes the Microsoft 365 Phone System app.

	☒ Microsoft 365 Apps for Enterprise Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Communication Compliance Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Defender Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Phone System Office 365 E5 without Audio Conferencing ☒ Microsoft Bookings Office 365 E5 without Audio Conferencing ☒ Microsoft Communications DLP Office 365 E5 without Audio Conferencing  You need follow-up configuration to enable the call queue feature.
Auto Attendant	Ensure that the selected license (e.g., the Office 365 E5 without Audio Conferencing) includes the Microsoft 365 Phone System app. ☒ Microsoft 365 Apps for Enterprise Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Communication Compliance Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Defender Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Phone System Office 365 E5 without Audio Conferencing ☒ Microsoft Bookings Office 365 E5 without Audio Conferencing ☒ Microsoft Communications DLP Office 365 E5 without Audio Conferencing  You need follow-up configuration to enable the call queue feature.
PSTN	1. Microsoft Teams Domestic or Domestic and International Calling Plan

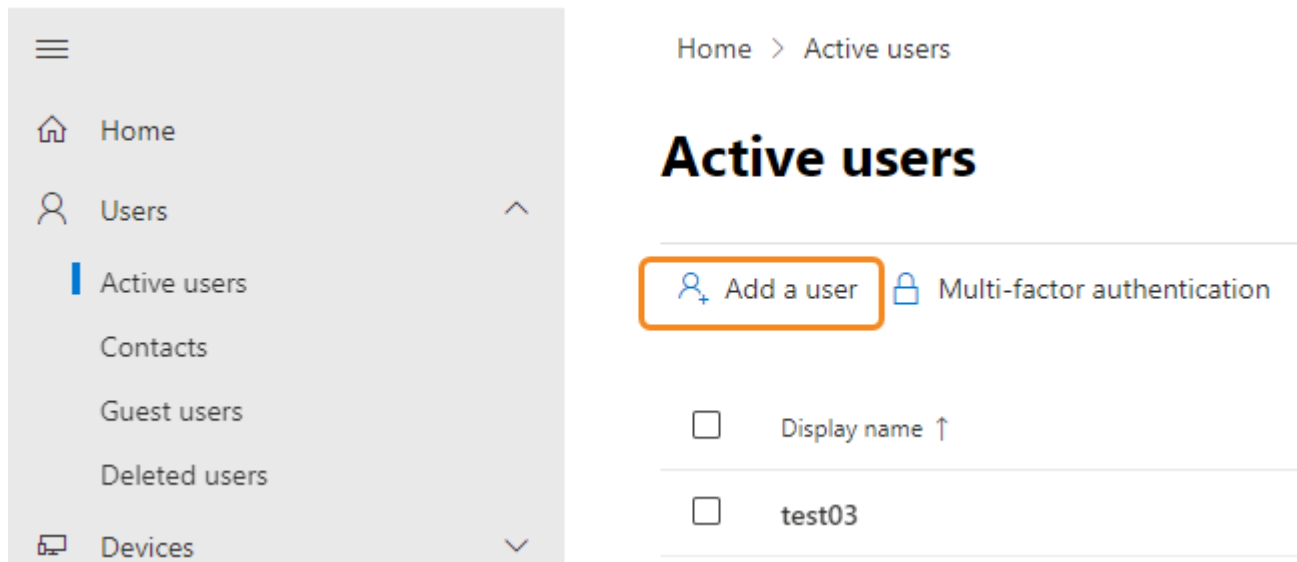
	☐ Microsoft Stream Trial Unlimited licenses available ☒ Microsoft Teams Domestic Calling Plan 0 of 42 licenses available ☐ Microsoft Teams Domestic and International Calling Plan You're out of licenses. If you turn this on, we'll try to buy an additional license for you. ☐ Microsoft Teams Exploratory 3 of 500 licenses available 2. Ensure that the selected license (e.g., the Office 365 E5 without Audio Conferencing) includes the Microsoft 365 Phone System app. ☒ Microsoft 365 Apps for Enterprise Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Communication Compliance Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Defender Office 365 E5 without Audio Conferencing ☒ Microsoft 365 Phone System Office 365 E5 without Audio Conferencing ☒ Microsoft Bookings Office 365 E5 without Audio Conferencing ☒ Microsoft Communications DLP Office 365 E5 without Audio Conferencing ! You need follow-up configuration to set up the PSNT feature.
Whiteboard	Ensure that the selected license (e.g., the Microsoft Teams Room Standard) includes the Microsoft 365 Phone System app.

	Show apps for: All licenses ☒ Select all ☒ Microsoft 365 Audio Conferencing Microsoft Teams Rooms Basic ☒ Microsoft Teams Microsoft Teams Rooms Basic ☒ Whiteboard (Plan 3) Microsoft Teams Rooms Basic
Skype for Business	Ensure that the selected license (e.g., the Office 365 E3) includes the Skype for Business Online (Plan 2) app. ☒ SharePoint (Plan 2) Microsoft 365 E3 ☒ Skype for Business Online (Plan 2) Microsoft 365 E3 ☒ Sway Microsoft 365 E3

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**.



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	Licenses	Apps
Basics Product licenses Optional settings Finish	☐ 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) Unlimited licenses available	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	Back Next

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

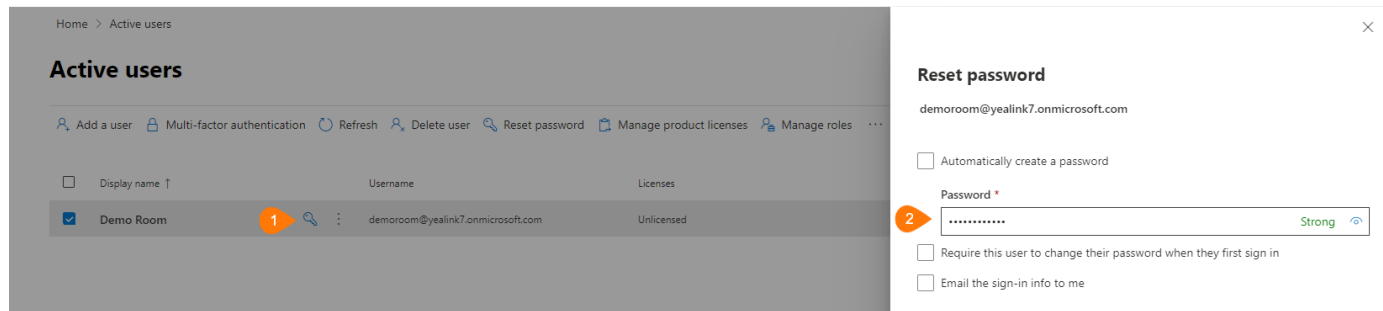
Add a user	Review and finish
Basics Product licenses Optional settings Finish	Assigned Settings Review all the info and settings for this user before you finish adding them. Display and username Monica Zhang test01_@yealink7.onmicrosoft.com Edit Password Type: Auto-generated Edit Product licenses Location: 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 created and click the key to reset the password.

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



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 Introduction

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:

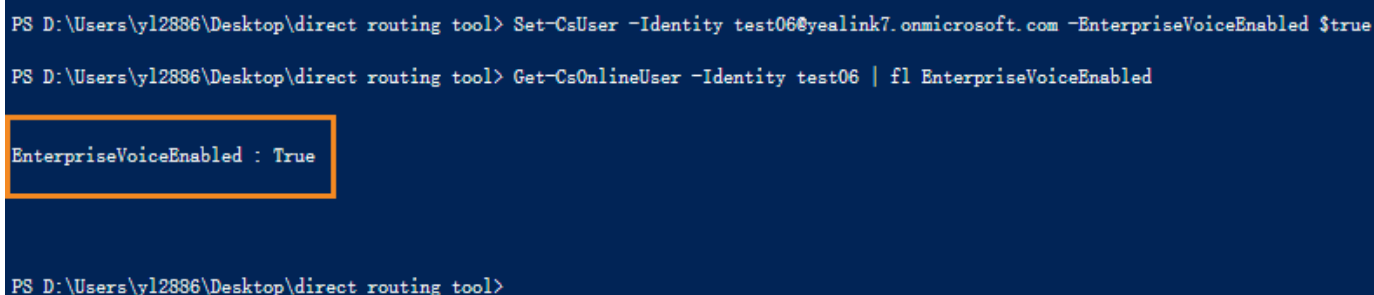
```
Set-CsUser -Identity "<User name>" -EnterpriseVoiceEnabled $true -HostedVoiceMail  
$true  
// change <user name> to the actual user name
```

Example:

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

4. Run the command below to see the status:
5. 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**.

Microsoft Teams admin center

Manage teams

Teams and channels are collections of people, content, and tools used for projects or outcomes within your organization. You can manage all teams and channels, and create new ones. Go to the [Admin center > Groups](#) to manage Microsoft 365 groups. [Learn more](#)

Users summary

3,334 Total users 2,291 Internal users 1,043 Guests

+ Add Edit Archive Delete 10 teams

Name	Standard channels	Private channels	Shared channels	Team members
Browse-Yealink headset support group	1	0	0	8
Yealink TOP Partner Support Program	4	0	0	3
Yealink Technical Support - TD Synnex	1	0	0	8
Yealink MS Hotline Support	1	0	0	19
Comtel & Yealink Technical Support	1	0	0	1
Yealink NZ support	1	0	0	5
Yealink Support	1	0	0	8
Yealink&Franklin Daily Support	1	0	0	7
OHL & Yealink Tech Support	1	0	0	1

Add a new team

Name *
YL technical support

Description
YL technical support

Team owners
Search by display or username

Peter Parker (TEST06)

Privacy
Private

Apply Cancel

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

Microsoft Teams admin center

Manage teams

Teams and channels are collections of people, content, and tools used for projects or outcomes within your organization. You can manage all teams and channels, and create new ones. Go to the [Admin center > Groups](#) to manage Microsoft 365 groups. [Learn more](#)

Users summary

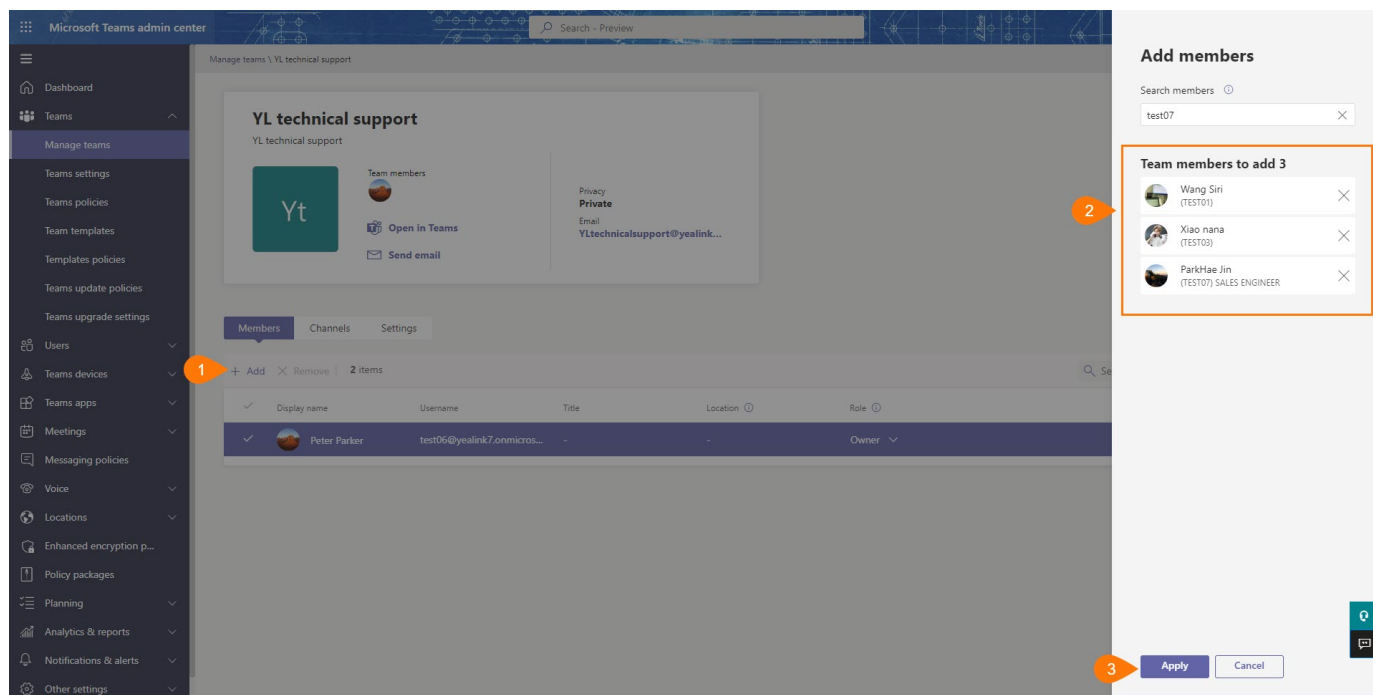
3,334 Total users 2,291 Internal users 1,043 Guests

+ Add Edit Archive Delete 4 teams

Search: technical

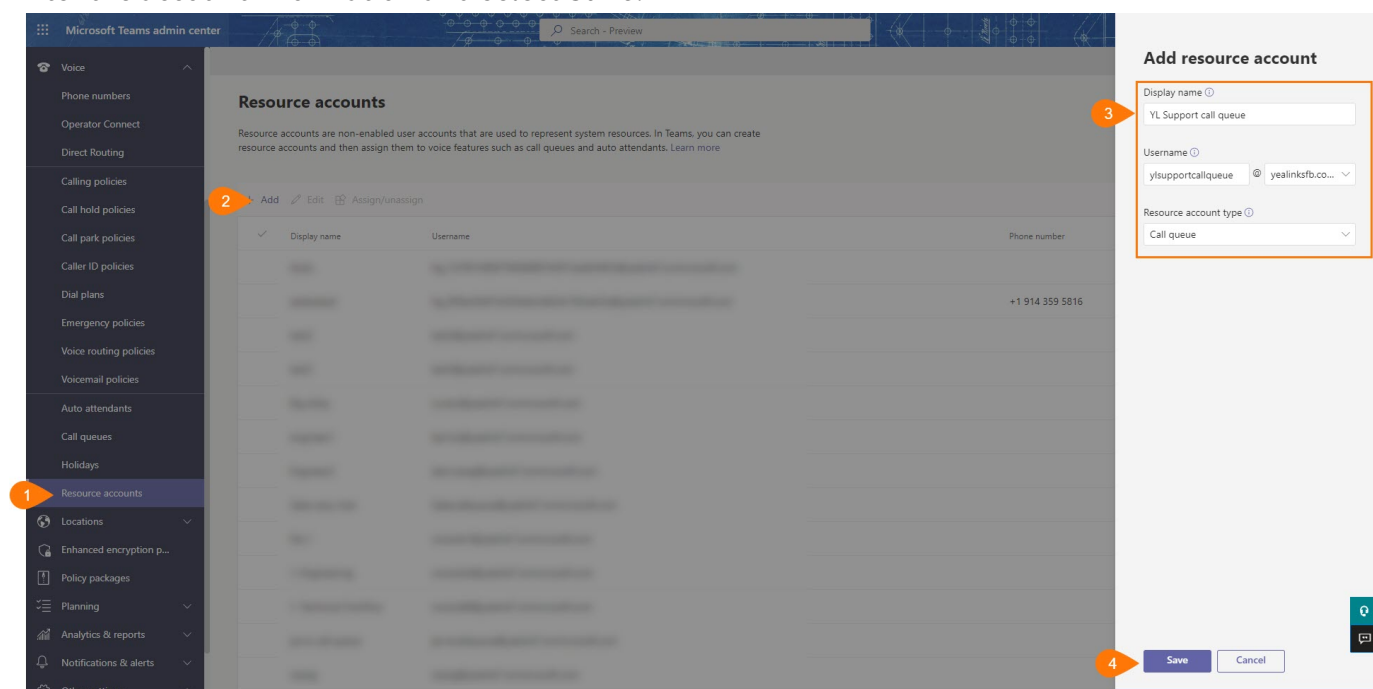
Name	Standard channels	Private channels	Shared channels	Team members	Owners	Guests
YL technical support	1	0	0	1	1	0
Yealink Technical Support - TD Synnex	1	0	0	8	1	2
Comtel & Yealink Technical Support	1	0	0	1	1	0
Asit&Yealink Technical support Team	1	0	0	7	1	1

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

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

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](#).

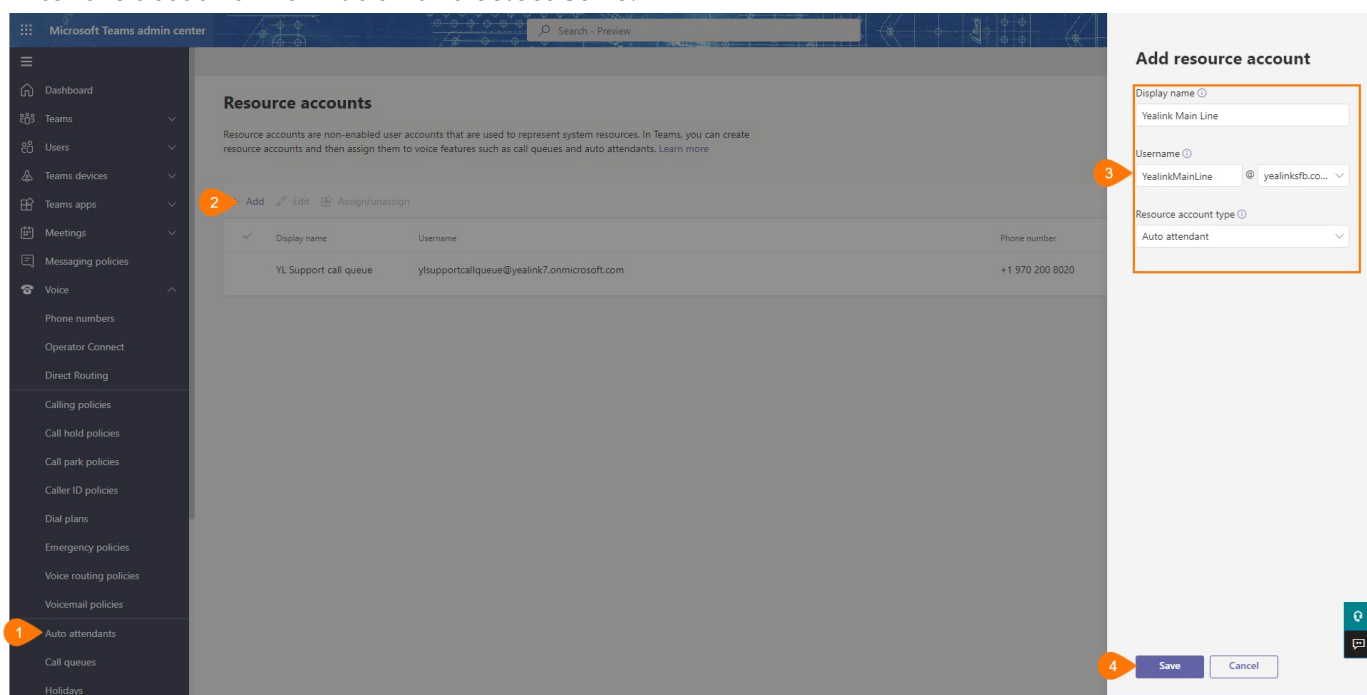
Prerequisites

- 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

General info

Call flow

Advanced settings (optional)

1 Yealink Main Line

Operator (optional)

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

2 Person in organization = 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**.
 - a. 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

✓ General info

Call flow

Advanced settings (optional)

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.

- b. Set the call routing options and click **Next**.

Auto attendants \ Add auto attendant

General info

Call flow

Advanced settings (optional)

1

Call routing options

☐ Disconnect

☐ Redirect call ⓘ

☒ Play menu options

Force Listen ☐ Off ⓘ

Set up the greeting and menu options.

☐ Play an audio file ⓘ

2

☒ 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 X		
1		Voice app	YS Yealink Sales X		
2		Voice app	Y YL Support call queue X		

c. Set the directory search type.

d. 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's business hours.

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

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

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
X

Transcription
Skip voicemail system message [?](#)

☒ On
☐ Off

☐ Play menu options

3

Next

Submit

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

1 Christmas

2 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 = Yealink ×

Transcription ☐ Off Skip voicemail system message ⓘ ☐ Off

☐ Play menu options

5 **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](#)

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

Next Submit

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

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 Add

2

3

4

Submit

Add accounts

Search for resource accounts you want to add.

Search by display or username

Accounts to add (1)

YL Yealink Main Line

Add Cancel

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

1 Calling Plan

Assigned phone number

2 +1 970 200 8021

Assigned to

Your changes must be saved before making more changes.

Select an auto attendant

3 Yealink Main Line

4 **Save** Cancel

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**.

The screenshot shows the Microsoft Teams admin center interface. On the left, the 'Voice' section is expanded, and 'Phone numbers' is selected. The main area displays a table of phone numbers. The first row is selected, showing the number +1 213 458 8107. To the right, a sidebar shows the 'Assign/unassign' configuration for this number. The 'Assigned to' field is set to 'Yealink Amazon offic...' and the 'Emergency location' is set to '405 Hilgard Avenue, Los Angeles CA 90024, US'. The 'Apply' button is highlighted with an orange circle.

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

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:**

- a. Under the **Waiting on activation** tab, click **Add**.
- b. Enter the MAC address, set the location, and click **Save**.

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

6	2	2
MAC addresses or hardware IDs	Verification codes expired	Waiting to sign in

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

1 + Add | Upload | Generate verification code | Edit | Delete | 4 items

ID	ID type	Location	Verification code
02-10-00-04-00-05:999	Hardware ID (analog)	India	--
02-10-00-04-00-05	MAC address	US	--
80-5e-c0-60-3b-e3	MAC address	--	Expired
00-02-91-c6-d3-e8	MAC address	--	Expired

Add MAC addresses or hardware IDs

ID type ① Enter MAC address

2 MAC address 80-5E-C0-DA-A4-52

3 Location Xiamen, China

4 Save Cancel

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

- c. From the **Waiting on activation** tab, select **Upload**.

- d. Download the file template.
- e. Enter the MAC ID and location, and then save the file.
- f. 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**.
2. 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 MAC addresses or hardware IDs
2 Verification codes expired
2 Waiting to sign in

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 hardware ID

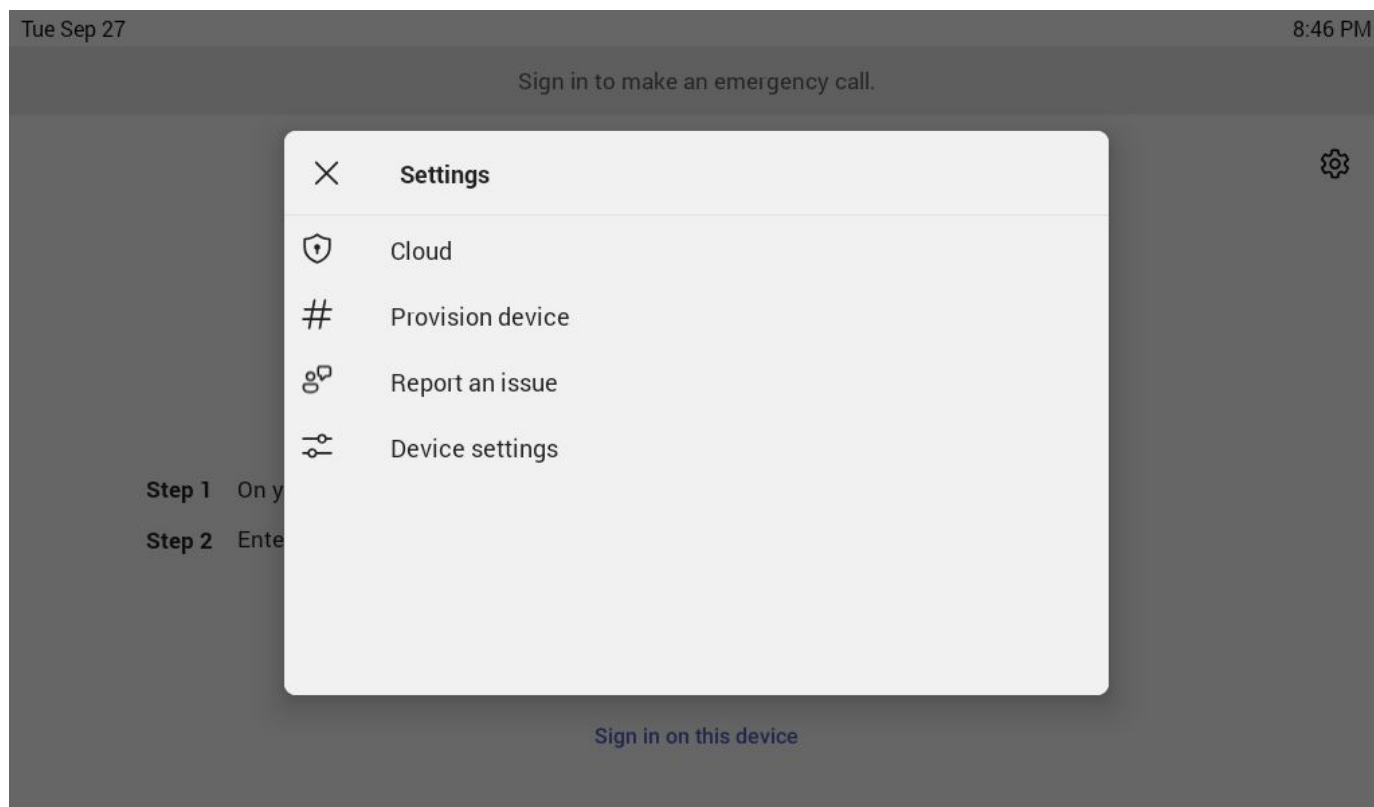
ID	ID type	Location	Verification code
80-5e-c0-da-a4-52	MAC address	Xiamen, China	362671
02-10-00-04-00-05:999	Hardware ID (analog)	India	--
02-10-00-04-00-05	MAC address	US	--
80-5e-c0-60-3b-e3	MAC address	--	Expired
00-02-91-c6-d3-e8	MAC address	--	Expired

4. 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.

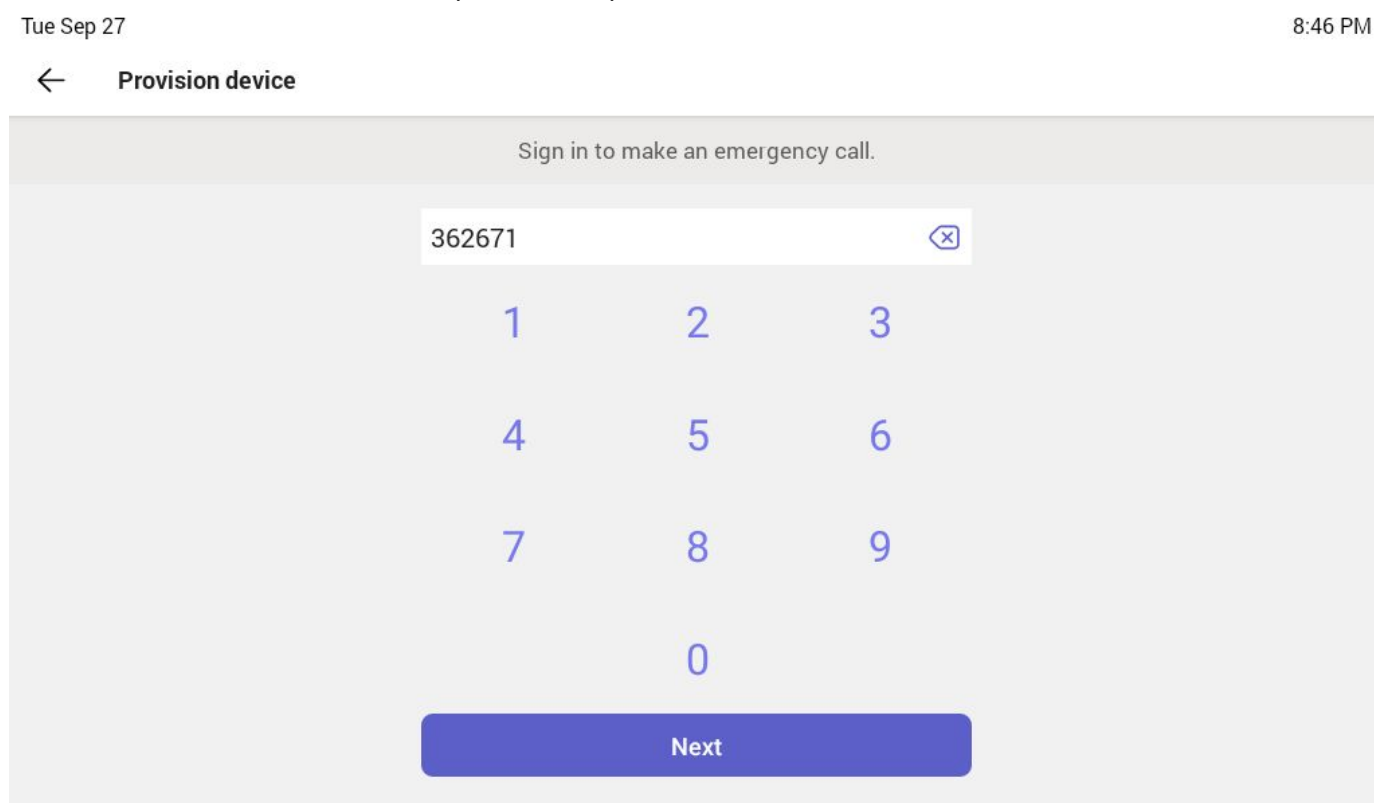
Provision Devices

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.



4. 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.

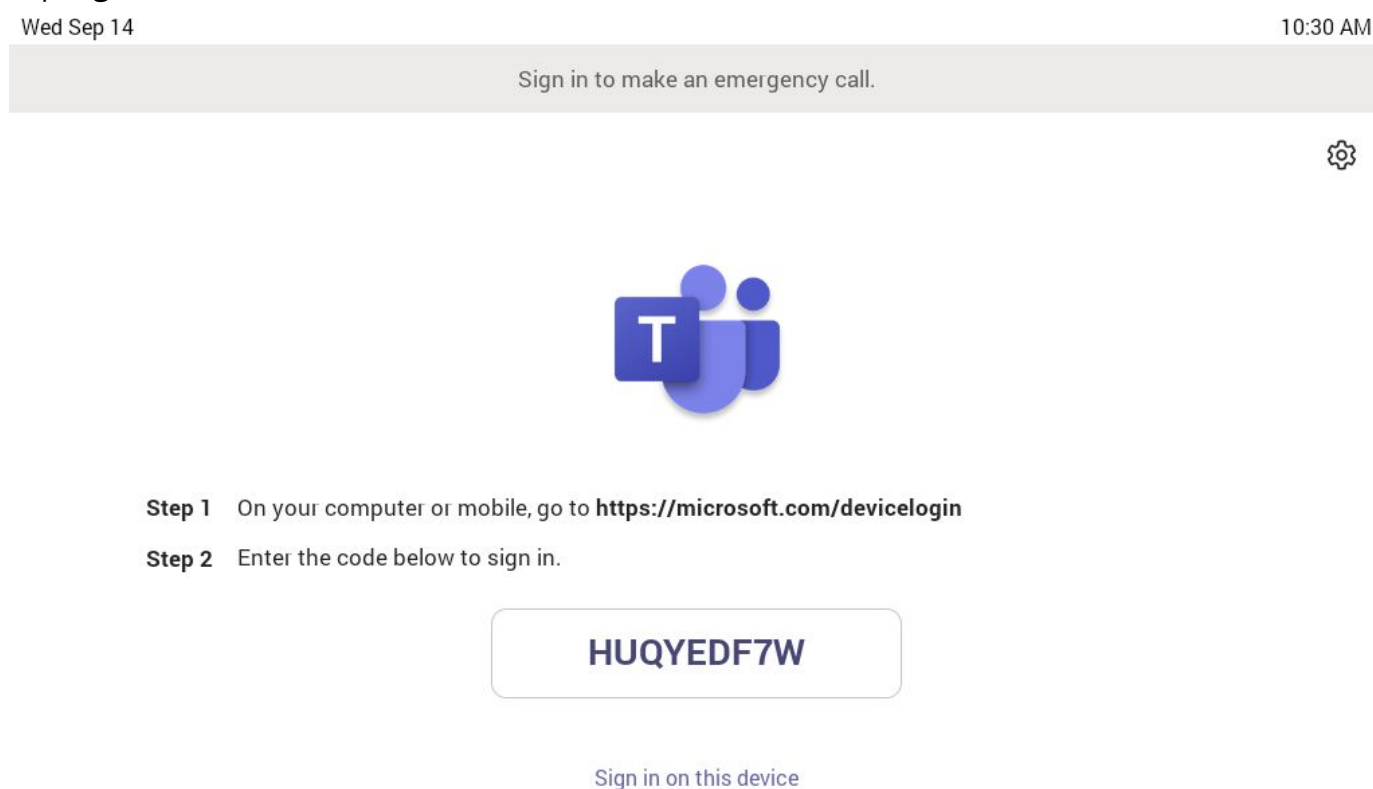
! The following illustrations serves as examples. The actual phone screen you see might be different.

Before you begin

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

On Your Teams Device

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



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

Wed Sep 14

10:33 AM

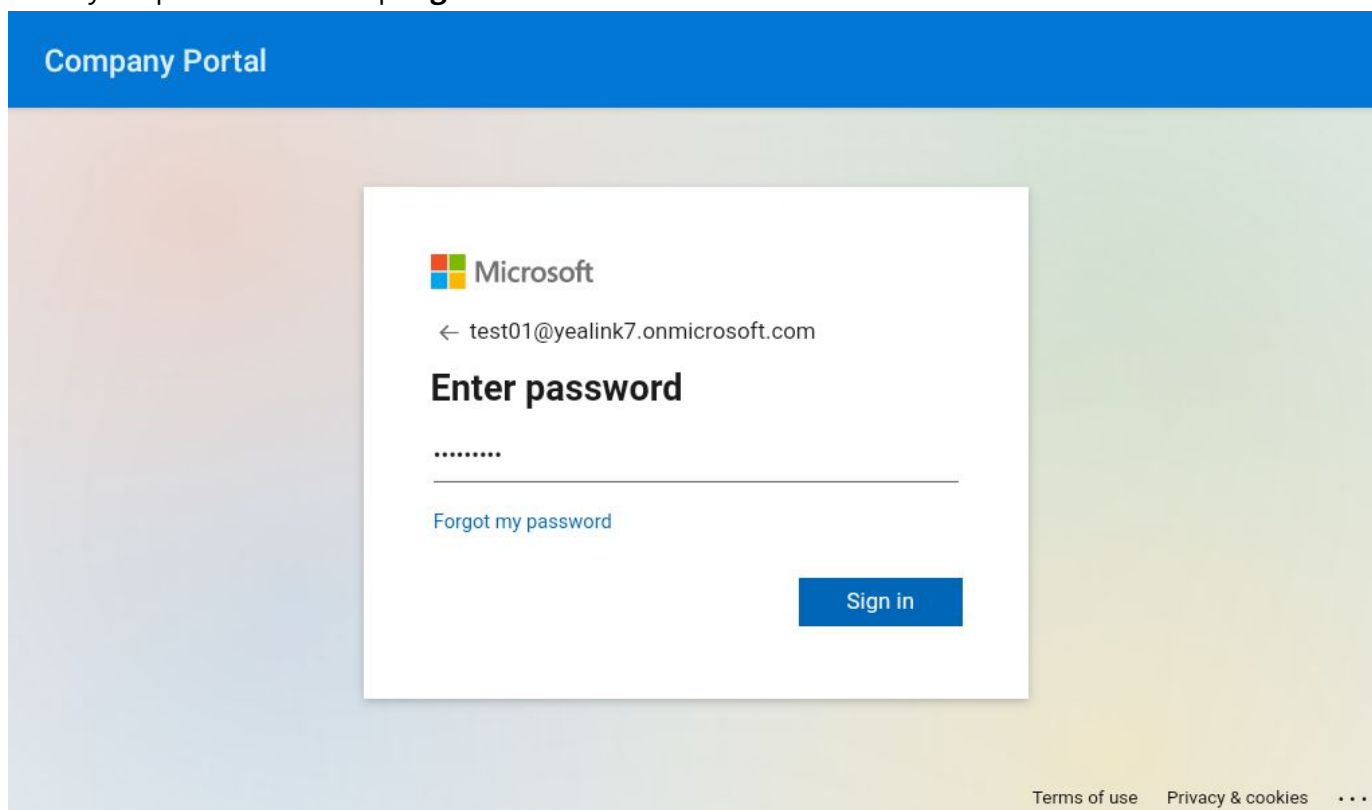


Welcome to Microsoft Teams! A happier place for teams to work together.

**Sign in**

4. 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**.

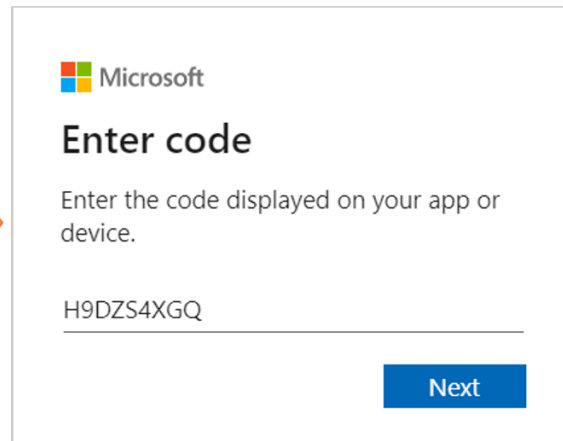
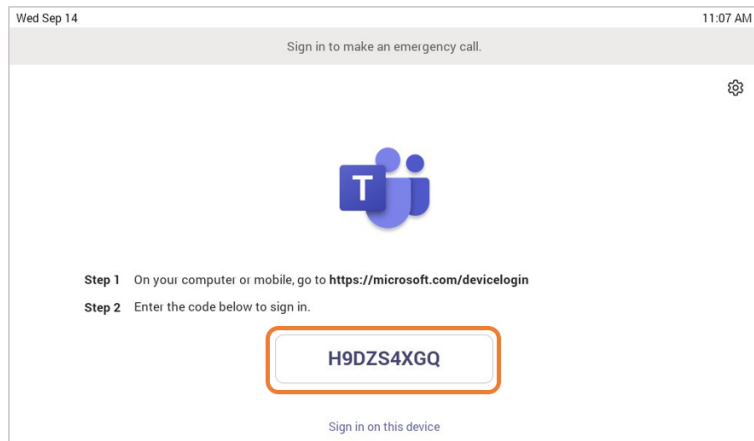


Have meetings and calls with audio, video.

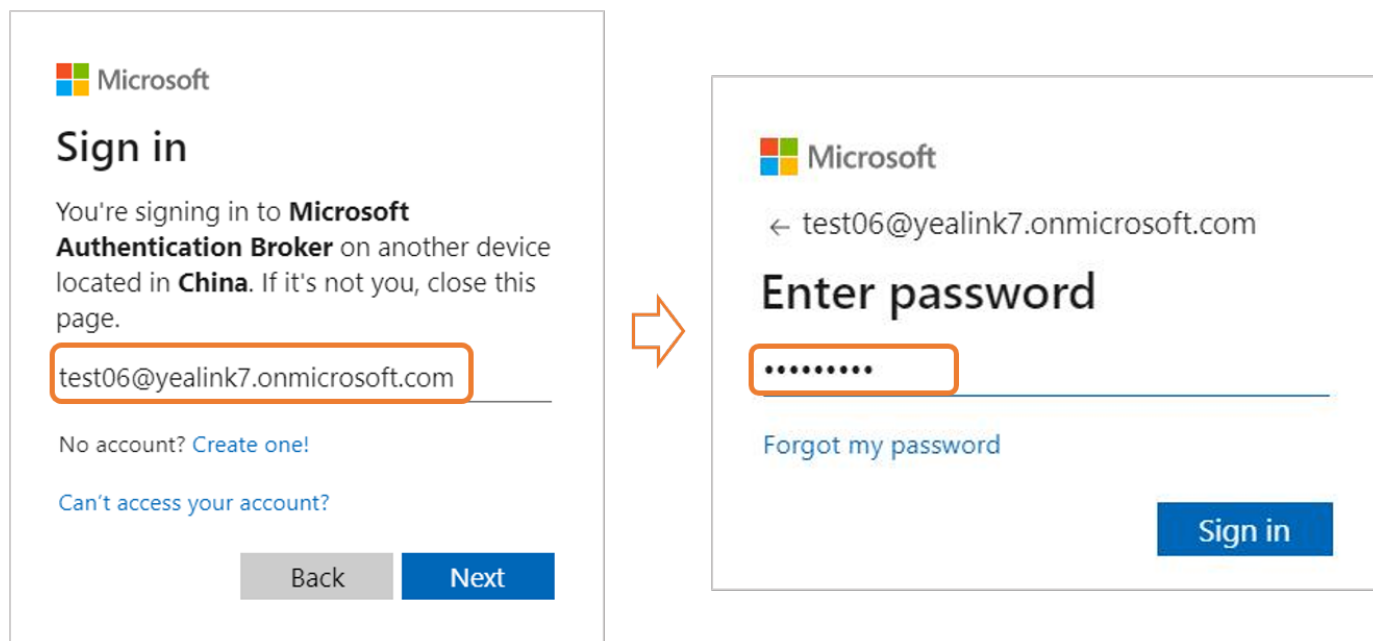
Got it

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.



5. 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

💡 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

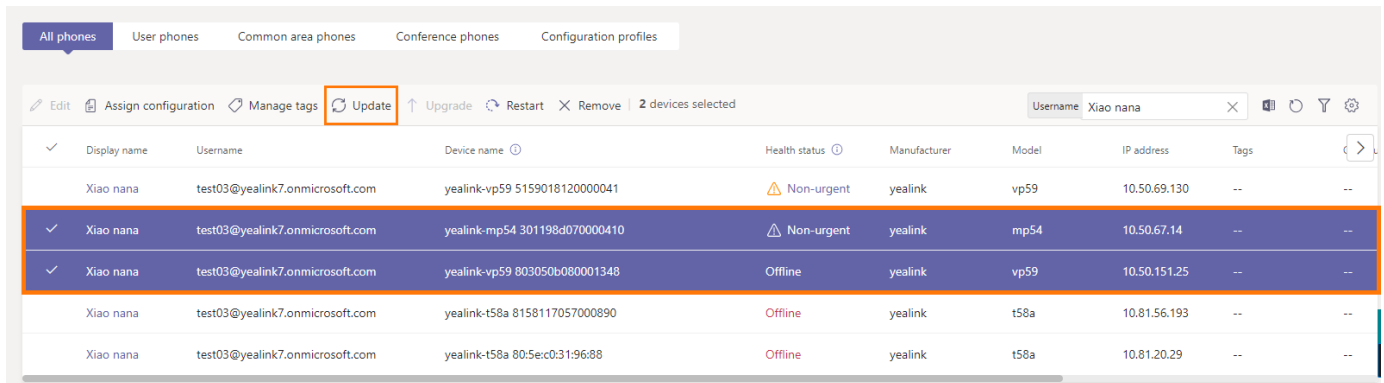
1. Sign in to the [Microsoft Teams admin center](#) as an admin.
2. Go to **Teams Devices > Phones**.
3. Select one or more devices and then select **Update**.

✓	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**.



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

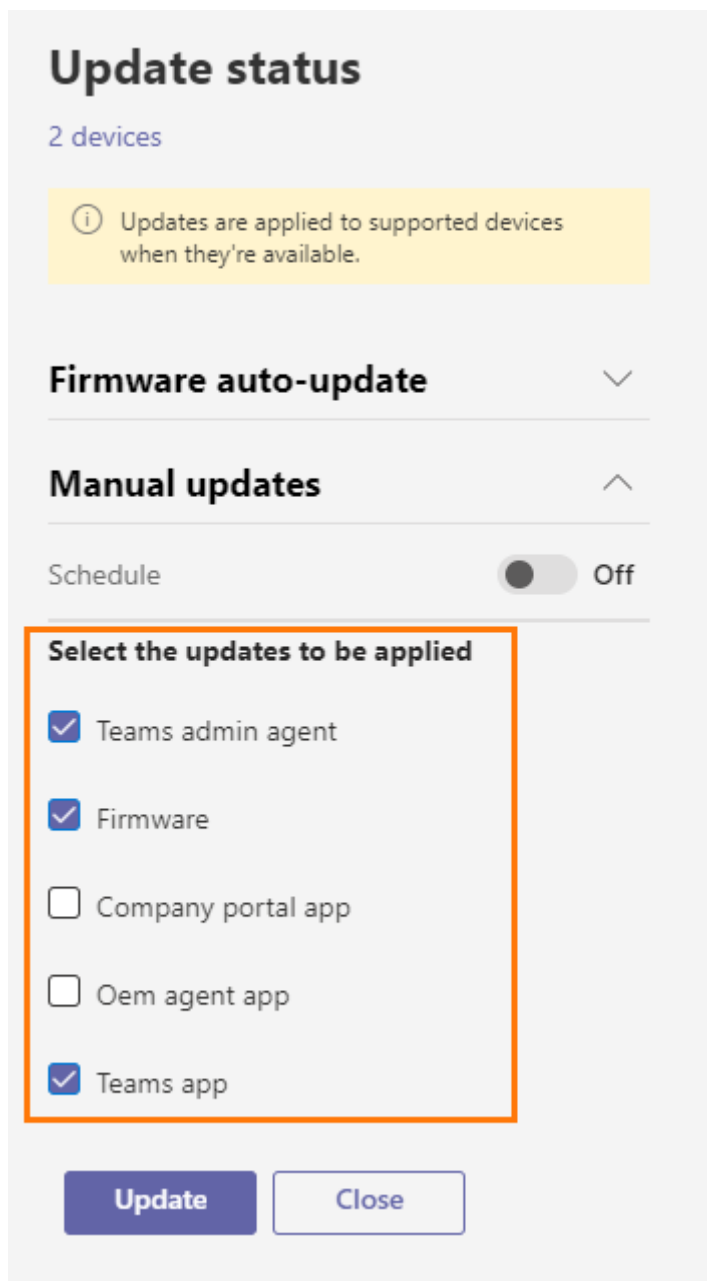
Published on

Aug 29, 2022, 8:30 PM

Update

Close

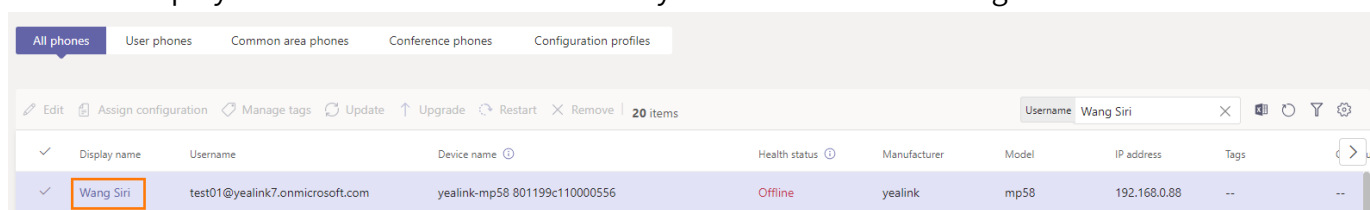
- If you select multiple devices:



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.

6. If the diagnostic log files are available to download, the status will change to "Successful".

✓	Action	Status	Scheduled at	Modified on	Diagnostics file	Initiated by
	DeviceDiagnostics	Successful	-	Sep 19, 2022, 6:59 PM	Download	Peter Parker

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**.

✓	Name	Description	Modified by	Modified on
	hyt-test		Peter Parker	Aug 25, 2022, 3:09 PM
	10.50.70.69		Peter Parker	Aug 30, 2022, 8:41 AM
	Phone lock test		Peter Parker	Aug 22, 2022, 4:17 PM

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.

6. 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**.

All phones User phones Common area phones Conference phones Configuration profiles								
Edit Assign configuration Manage tags Update Upgrade Restart Remove 1 device selected Username: Xiao nana								
✓	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	--

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

6. 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**.
4. 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 in Intune

Generally, the Yealink Teams phone has the pre-installed 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?

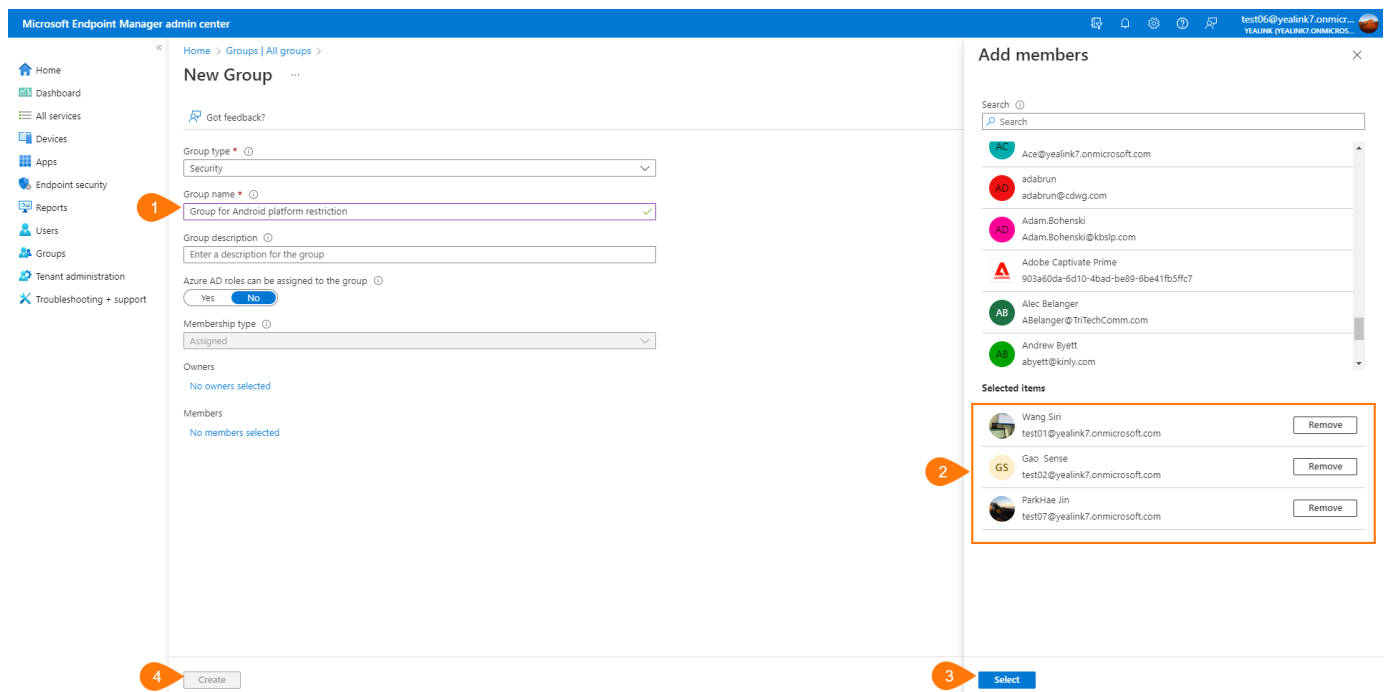
- Device Compliance: Tells you if your device is compliant or not.
- Conditional Access: Determines what to do with these devices depending on their compliant status.

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

Step 1 - Create a Group

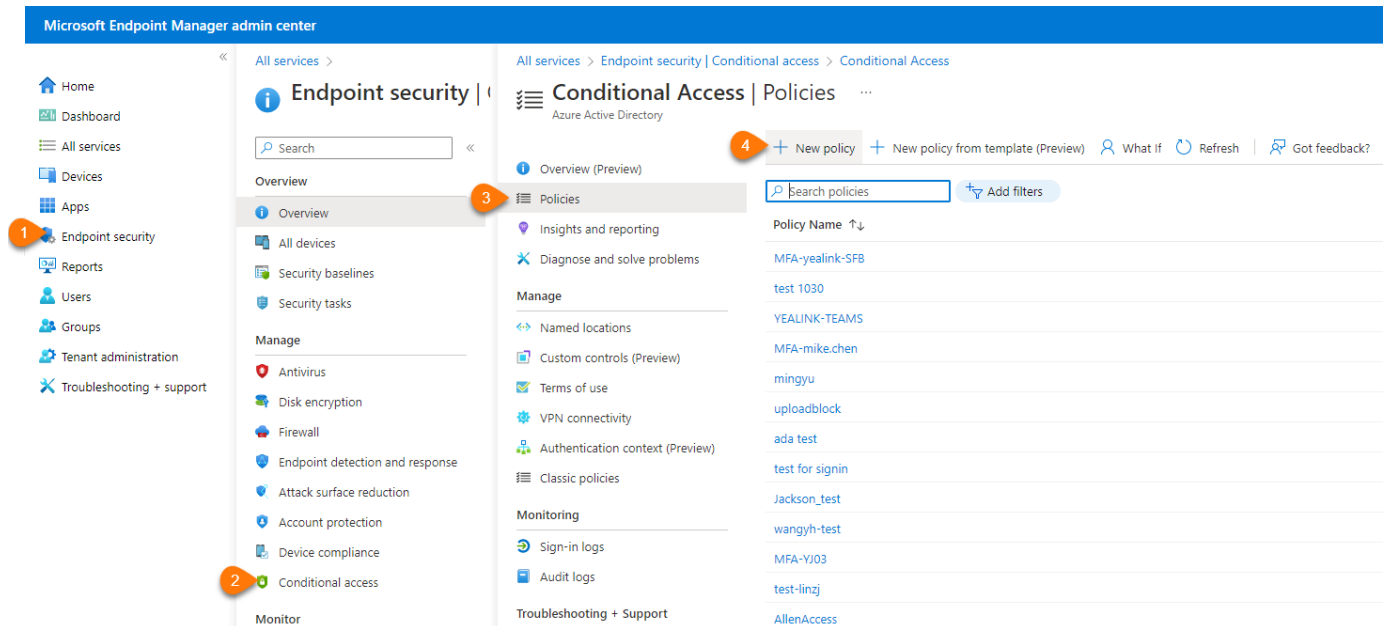
Skip this step if you already have a group that includes the user. Or you can add the user to the existing group.

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

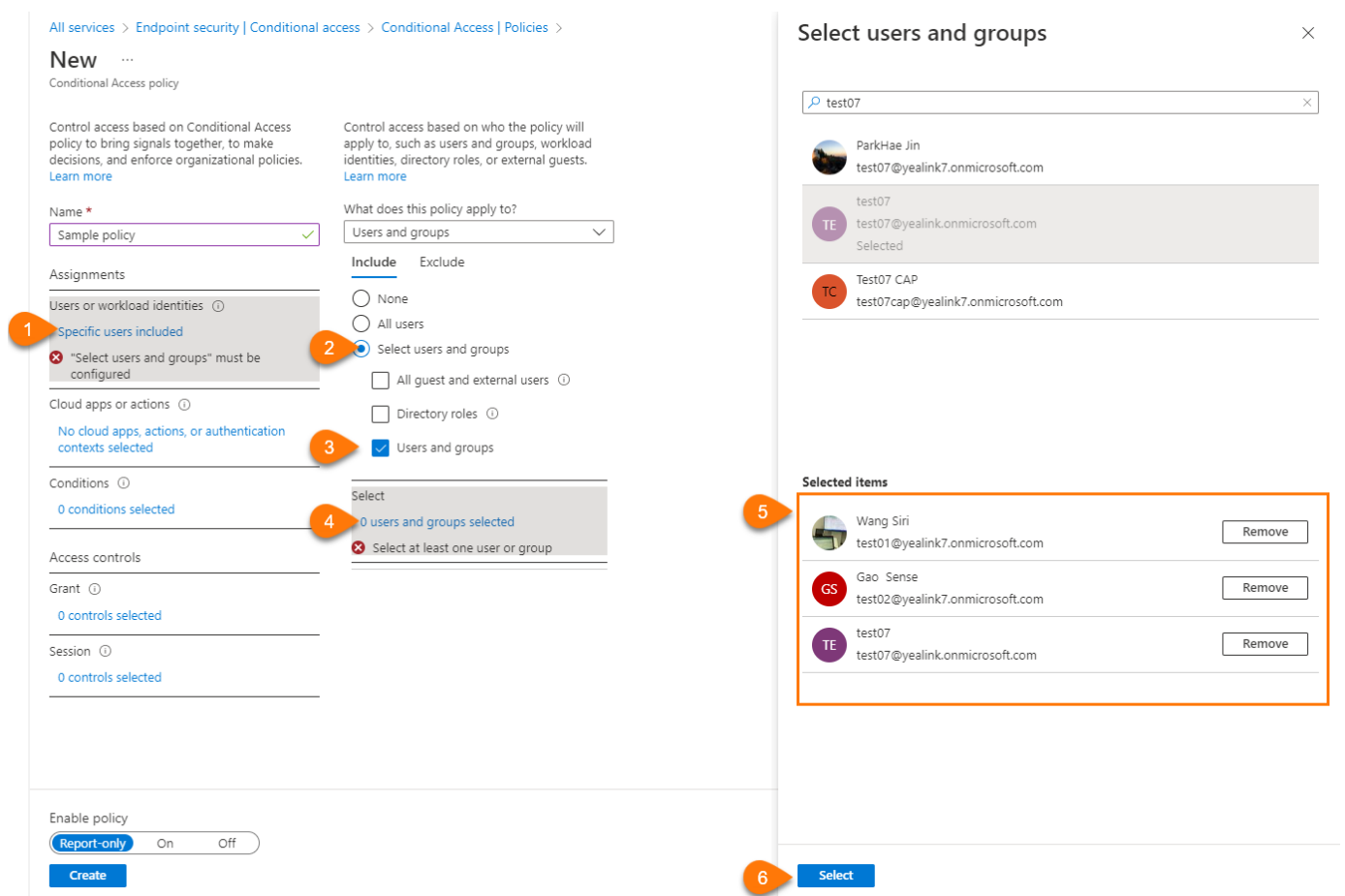
1. Sign in to the [Microsoft Endpoint Manager admin center](#) as an admin.
2. Go to **Endpoint security** > **Conditional access** > **Polices** > **New policy**.



3. Enter the policy name.

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

5. NOTE



- 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.

The screenshot displays the Microsoft Conditional Access policy configuration interface. The main panel shows the 'New' policy setup with fields for Name, Assignments, Cloud apps or actions, Conditions, Access controls, Grant, and Session. A sidebar on the right shows the 'Select' dialog for Cloud apps. Numbered callouts 1 through 5 highlight specific steps: 1. 'No cloud apps, actions, or authentication contexts selected' message; 2. 'Specific users included' link; 3. 'Select' button in the 'Cloud apps or actions' section; 4. 'Microsoft Teams' app in the 'Selected items' list; 5. 'Select' button at the bottom of the 'Select' dialog.

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.

The screenshot shows the 'New' Conditional Access policy configuration page. It includes sections for Name, Assignments, Cloud apps or actions, Conditions, Access controls, Grant, and Session. A 'Device platforms' sidebar is open on the right, showing options to 'Include' or 'Exclude' various device types. Numbered callouts indicate the following steps:

- 1**: Click on the 'Conditions' section.
- 2**: Click on the 'Device platforms' section.
- 3**: Click on the 'Yes' button in the 'Configure' section.
- 4**: Click on the 'Select device platforms' radio button and check the 'Android' checkbox.
- 5**: Click on the 'Done' button.

At the bottom, the 'Enable policy' section shows 'Report-only' selected, with 'On' and 'Off' toggle buttons, and a 'Create' button.

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**.

The screenshot shows the 'New' Conditional Access policy page in the Microsoft Endpoint Manager admin center. The interface includes sections for Name, Assignments, Cloud apps or actions, Conditions, Access controls, and Session. A sidebar on the right titled 'Grant' provides detailed settings for the selected policy. Numbered callouts (1-6) highlight specific steps: 1. Selecting 'Grant' under Access controls; 2. Selecting 'Grant access' in the Grant sidebar; 3. Checking 'Require device to be marked as compliant'; 4. Checking 'Require approved client app'; 5. Selecting 'Require all the selected controls' under 'For multiple controls'; 6. Clicking the 'Select' button at the bottom of the sidebar.

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

- 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**.

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**.

4. 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**.

a. 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 ⓘ	Block Not configured
Rooted devices ⓘ	Block Not configured
Require the device to be at or under the Device Threat Level ⓘ	Secured
Google Play Protect	
Google Play Services is configured ⓘ	Require Not configured
Up-to-date security provider ⓘ	Require Not configured
Threat scan on apps ⓘ	Require Not configured
SafetyNet device attestation ⓘ	Not configured

b. Set the operating system version:

^ Device Properties

Operating System Version

Minimum OS version ⓘ

5.0.0



Maximum OS version ⓘ

9.1.0



c. 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 ⓘ

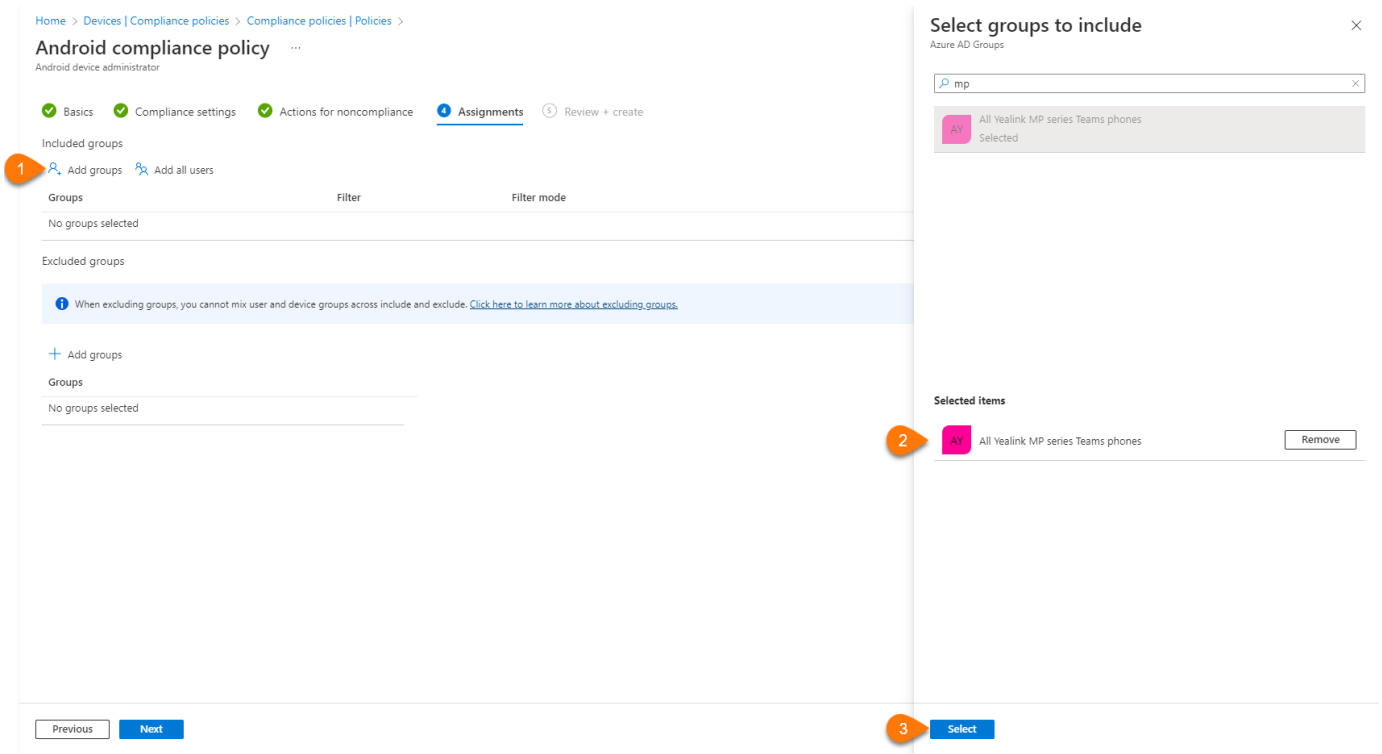
None

Android 9 and earlier or Samsung Knox

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

7. NOTE

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

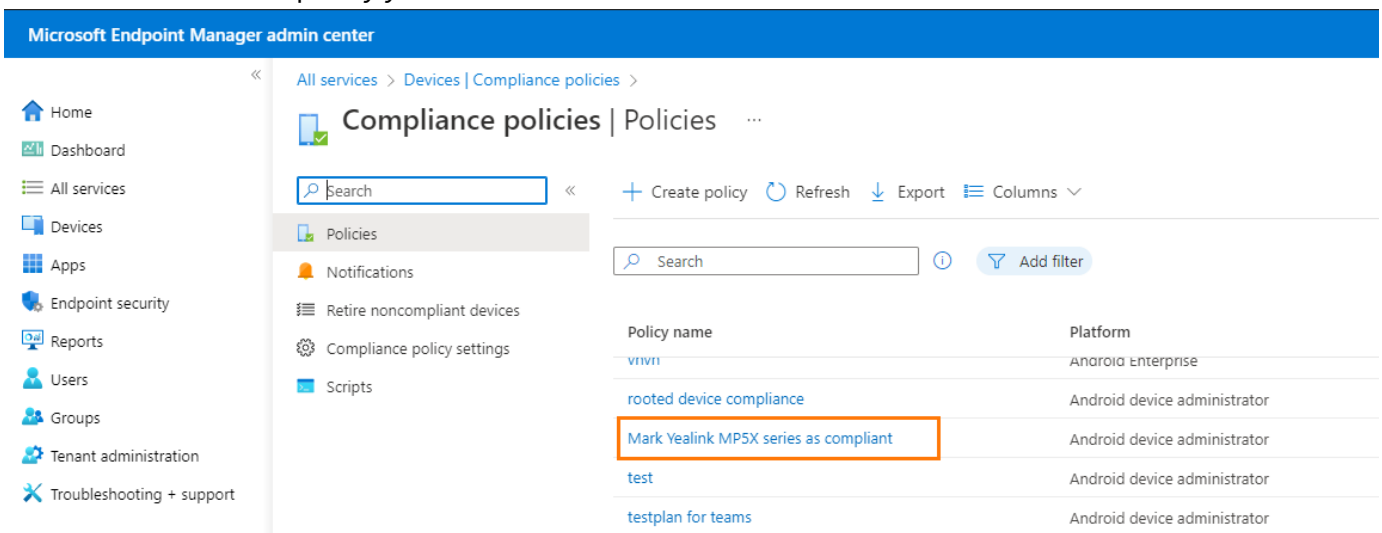


7. Click **Create**.

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.

Dashboard > YeaLink

YeaLink | Sign-in logs

Azure Active Directory

Download Export Data Settings Troubleshoot Refresh Columns

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

Date	Request ID	Correlation ID	Authentication requirement	Status	Continuous access evaluation	Sign-in error code	Failure reason	Additional Details	Troubleshoot Event
9/22/2022, 9:57:23 AM	232f2d4d-c652-4bfe-9...	vcs01 YeaLink	Office 365 Exch	Office 365 Exch	No	50126	Error validating credentials due to invalid username or password.	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.	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.
9/22/2022, 9:57:00 AM	0f46549b-d53a-4ff2-a...	vcs01 YeaLink	Office 365 Exch	Office 365 Exch	No				
9/22/2022, 9:56:59 AM	08bb969f-376a-4409-8...	vcs01 YeaLink	Office 365 Exch	Office 365 Exch	No				
9/22/2022, 9:56:58 AM	1ab86cbd-1d15-4e26-...	vcs01 YeaLink	Office 365 Exch	Office 365 Exch	No				
9/22/2022, 9:56:22 AM	dbffc97b-4dd4-4043-b...	Peter Parker	Azure Portal	Azure Portal	No				
9/22/2022, 9:56:18 AM	b0089bce-04c8-460b-...	ParkHae Jin	Office 365 Exch	Office 365 Exch	No				
9/22/2022, 9:56:15 AM	307eb0ba-f7ce-431d-9...	vcs01 YeaLink	Office 365 Exch	Office 365 Exch	No				
9/22/2022, 9:55:38 AM	6f74519e-f1f6-4782-ae...	Gao Sense	Microsoft Auth	Microsoft Auth	No				
9/22/2022, 9:55:09 AM	cec73cbe-589f-4f92-a...	MIMI Pan	Microsoft Auth	Microsoft Auth	No				
9/22/2022, 9:54:56 AM	3afe47f3-ec85-482a-8...	MIMI Pan	Microsoft Auth	Microsoft Auth	No				
9/22/2022, 9:53:22 AM	69b77fa9-1182-40dd-8...	Peter Parker	Microsoft Auth	Microsoft Auth	No				
9/22/2022, 9:53:19 AM	6df55d07-c45b-449c-a...	Peter Parker	Microsoft Auth	Microsoft Auth	No				
9/22/2022, 9:53:11 AM	65b1827b-7a06-4ade-...	Zoey	Microsoft Team	Microsoft Team	No				
9/22/2022, 9:52:27 AM	d9fe933d-1ad3-45a8-...	Ih12	Microsoft Team	Microsoft Team	No				
9/22/2022, 9:52:00 AM	0f46549b-d53a-4ff2-a...	Wang Siri	Microsoft Auth	Microsoft Auth	No				
9/22/2022, 9:51:41 AM	2f4965ec-3fc8-46d7-b...	Wang Siri	Microsoft Auth	Microsoft Auth	No				
9/22/2022, 9:51:41 AM	12e4727d-cba1-4fbc-b...	Peter Parker	Azure Portal	Azure Portal	No				
9/22/2022, 9:51:34 AM	e6a114c8-cabb-4fc7-b...	Peter Parker	Azure Portal	Azure Portal	No				
9/22/2022, 9:51:24 AM	cea8ee51-e6cd-4bfe-b...	Wang Siri	Microsoft Auth	Microsoft Auth	No				
9/22/2022, 9:51:00 AM	bbd14cd1-06d1-4a91-...	vcs01 YeaLink	Office 365 Exch	Office 365 Exch	No				
9/22/2022, 9:50:22 AM	59931d25-b8d2-4a62-...	Wang Siri	Microsoft Team	Microsoft Team	No				
9/22/2022, 9:50:21 AM	d4d34033-35d5-423e-...	Wang Siri	Microsoft Team	Microsoft Team	No				
9/22/2022, 9:49:42 AM	02d7684f-c40f-46b8-b...	vcs01 YeaLink	Office 365 Exch	Office 365 Exch	No				

Activity Details: Sign-ins

Basic info Location Device info Authentication Details Conditional Access Report-only

User: [Wang Siri](#)

Username: test01@yealink7.onmicrosoft.com

User ID: 53732d9e-d85e-4d40-93cd-6fbaf6f1f3c6

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-f901bc1d605e

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

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