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:

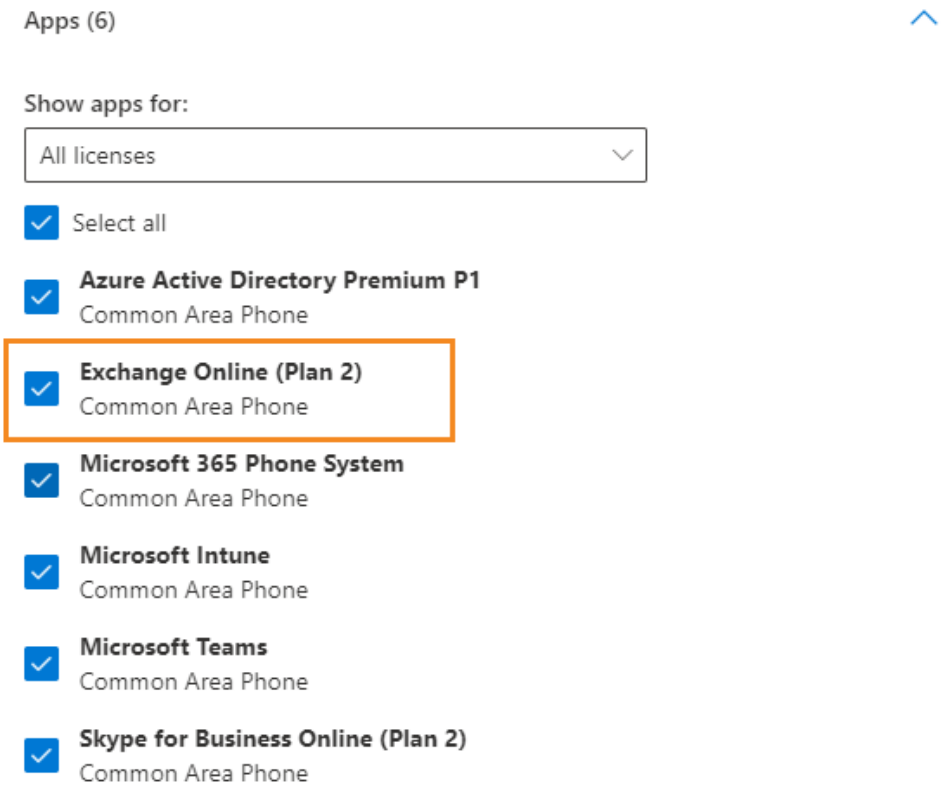
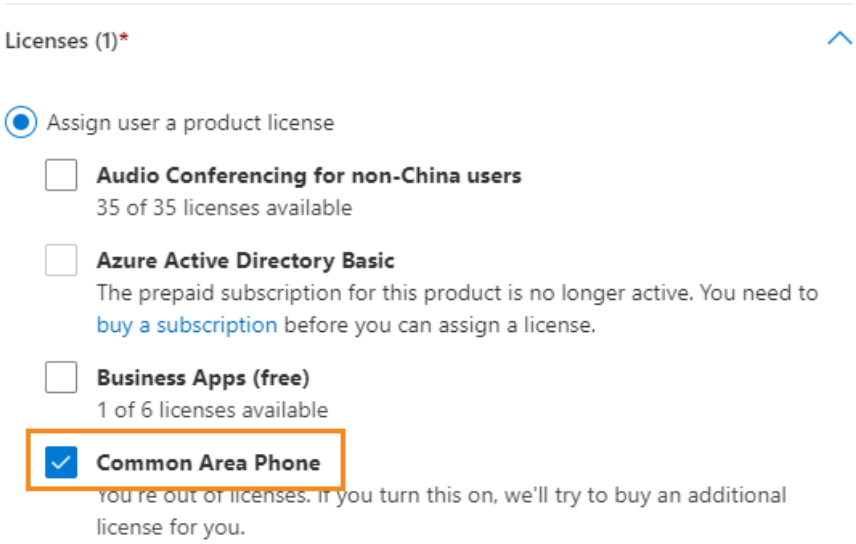
- Yealink MP52 (E2)/MP54 (E2)/MP56 (E2)/MP58 (E2)/MP55 E2
- Yealink VP59
- Yealink CP965

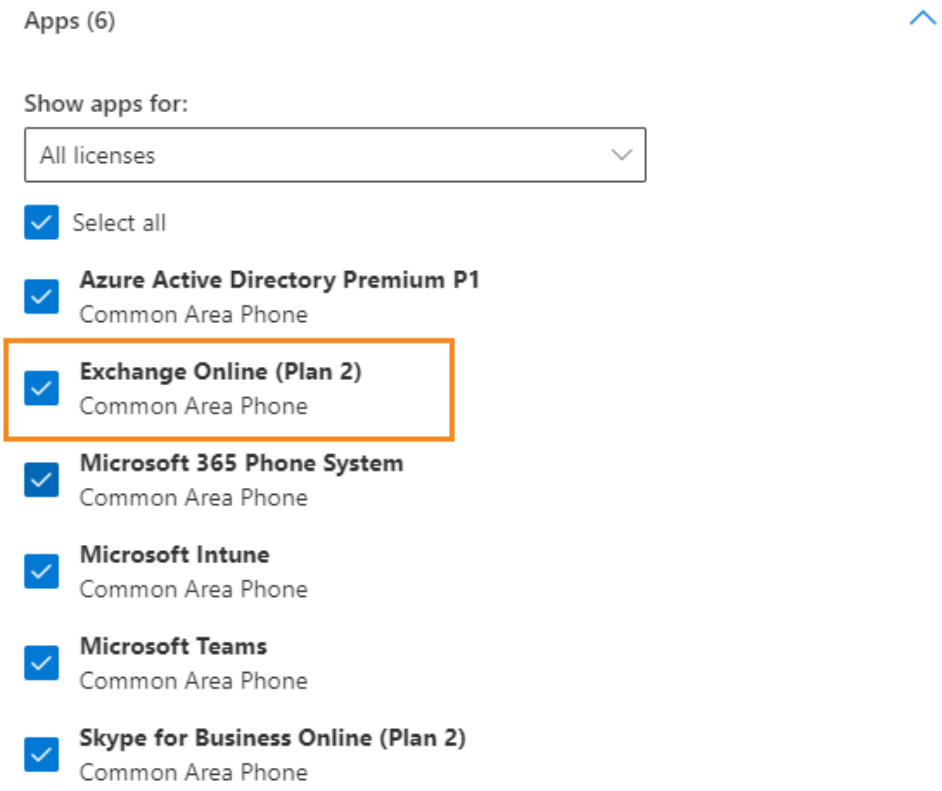
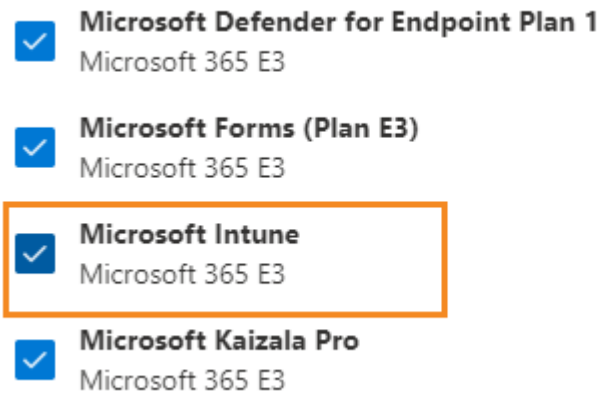
Users & Licenses

Understand License Types

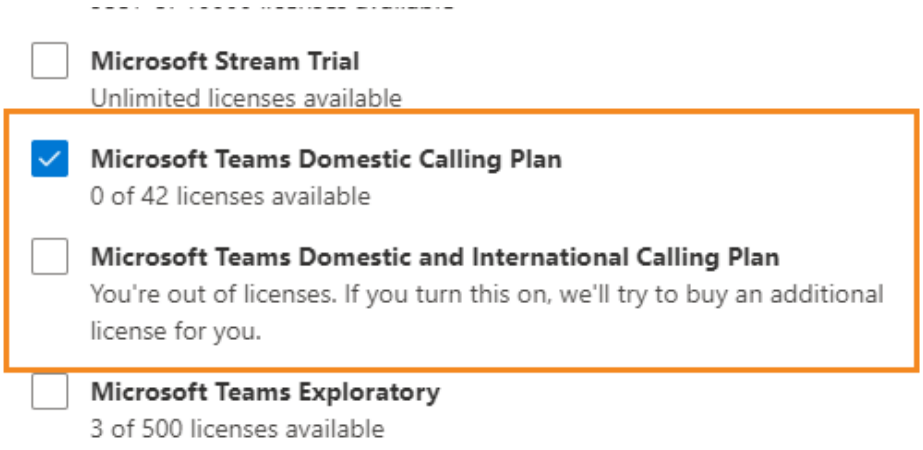
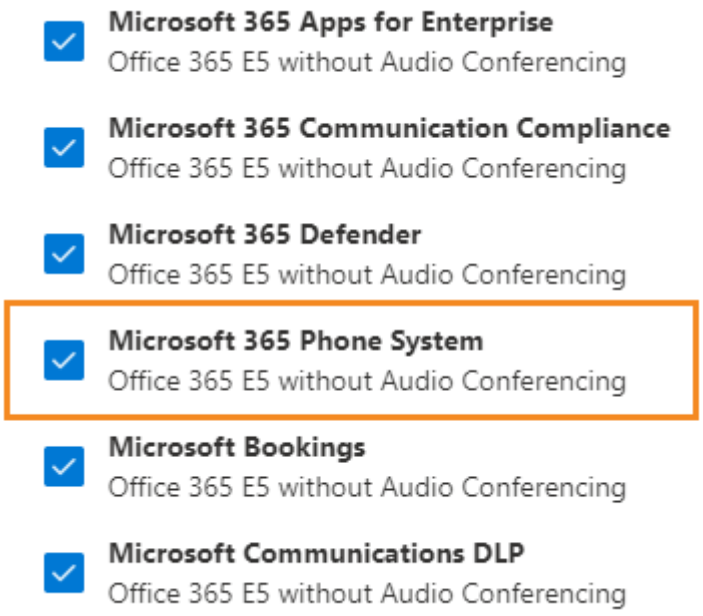
- The apps or services will be included in the Microsoft cloud-based suite for Office 365 and Microsoft 365. You can go to **Billing** > **Purchase services** on the Microsoft 365 admin center to buy licenses.
- The license takes effect **10** minutes after your assignment or modification.
- If you need other license types, please see the Microsoft Teams add-on licenses or contact Microsoft.

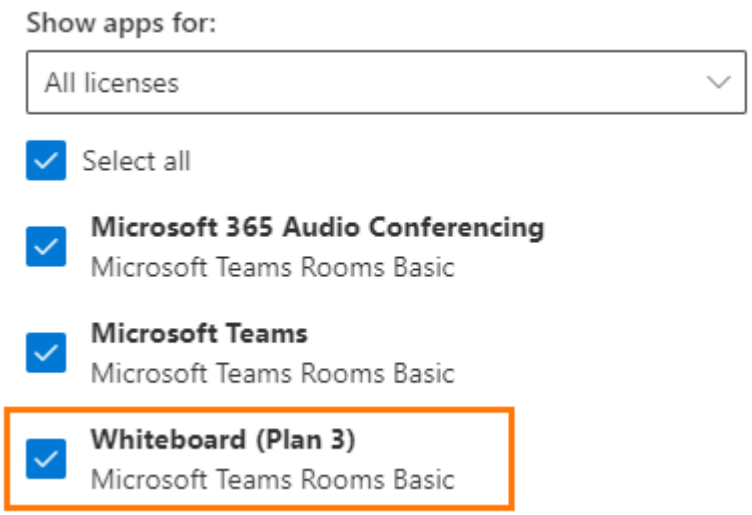
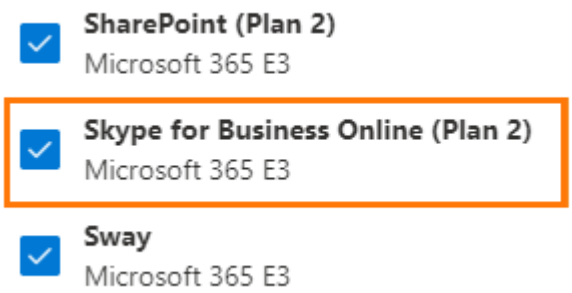
Features you need	Services or apps you need
Sign in to Teams	Ensure that the selected license (e.g., the Common Area Phone) includes the **Microsoft Teams** app.

	
Common Area Phone	Common Area Phone license 
Calendar feature	Ensure that the selected license (e.g., the Common Area Phone) includes the **Exchange Online** app.

	
Intune (manage device and apply policies on Intune)	Ensure that the selected license (e.g., Microsoft 365 E3) includes the **Microsoft Intune** app. 
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

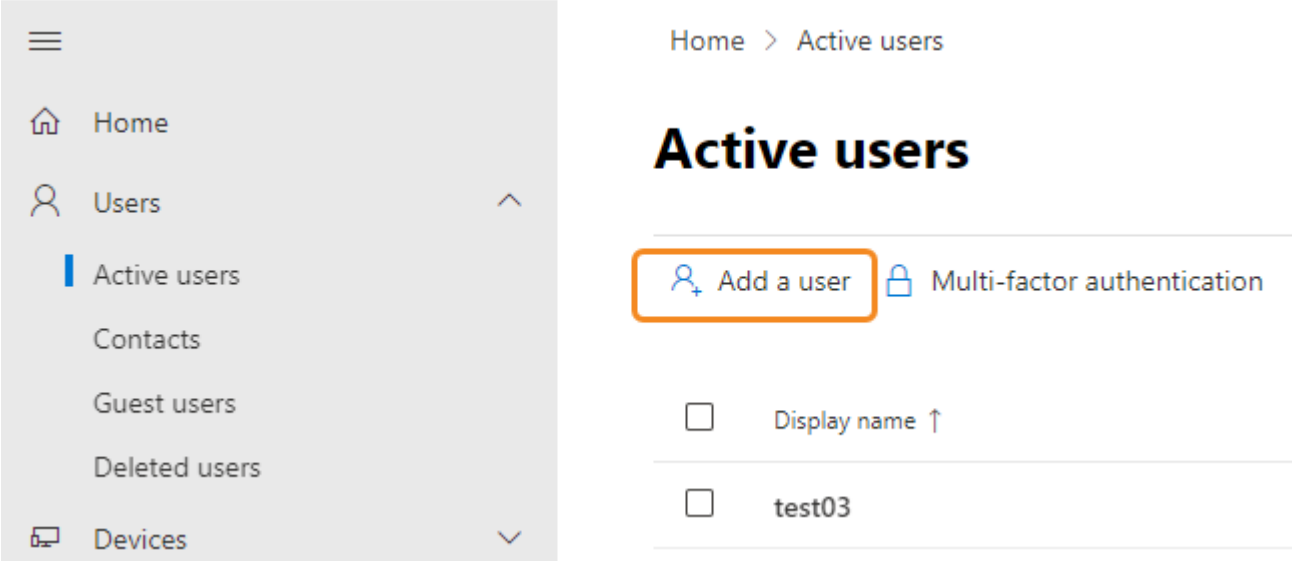
	 2. Ensure that the selected license (e.g., the Office 365 E5 without Audio Conferencing) includes the **Microsoft 365 Phone System** app.  You need follow-up configuration to set up the PSNT feature.
Whiteboard	Ensure that the selected license (e.g., the Microsoft Teams Room Standard) includes the **Microsoft 365 Phone System** app.

	
Skype for Business	Ensure that the selected license (e.g., the Office 365 E3) includes the **Skype for Business Online (Plan 2)** app. 

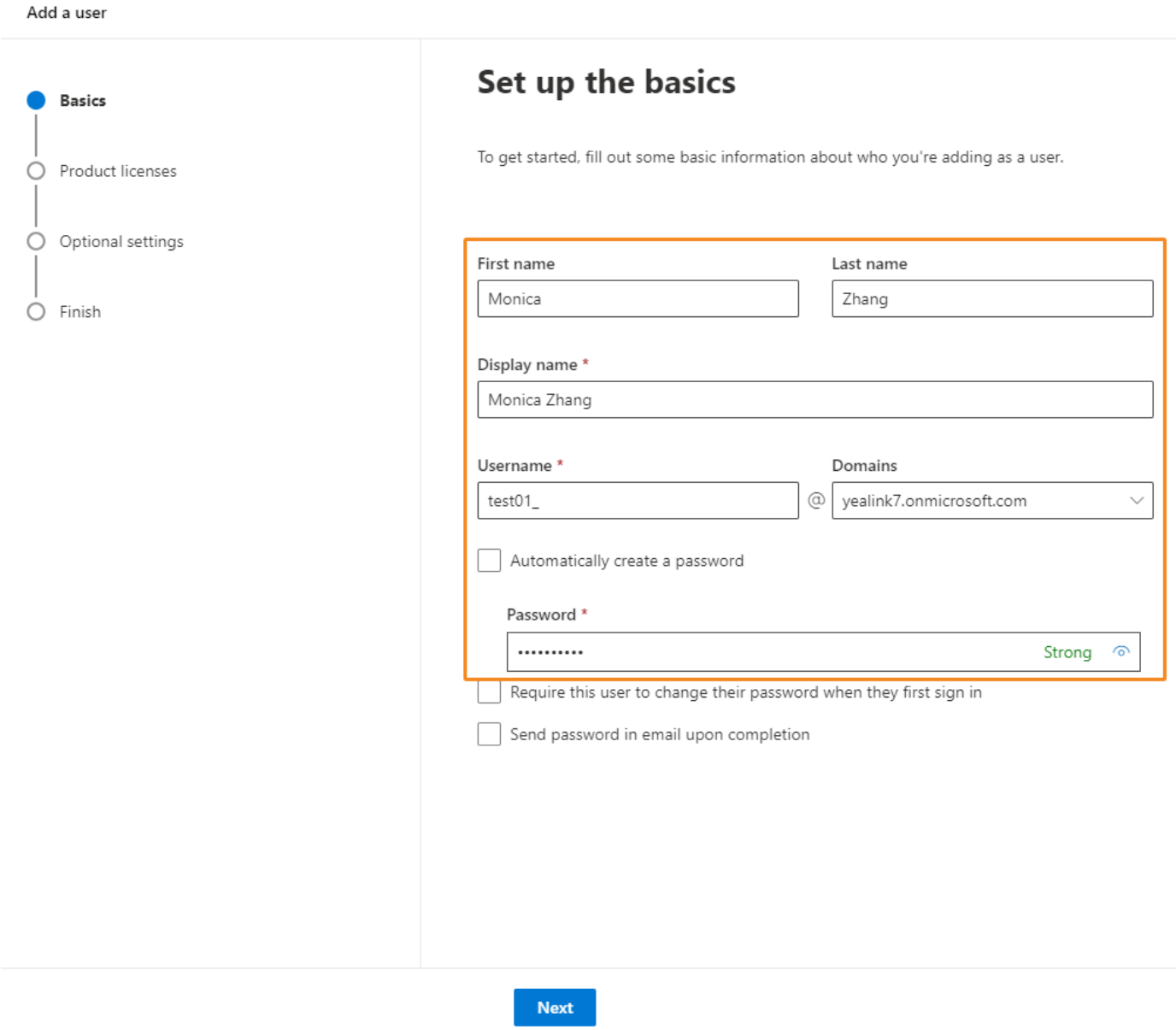
Add Users and Assign Licenses Simultaneously

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.

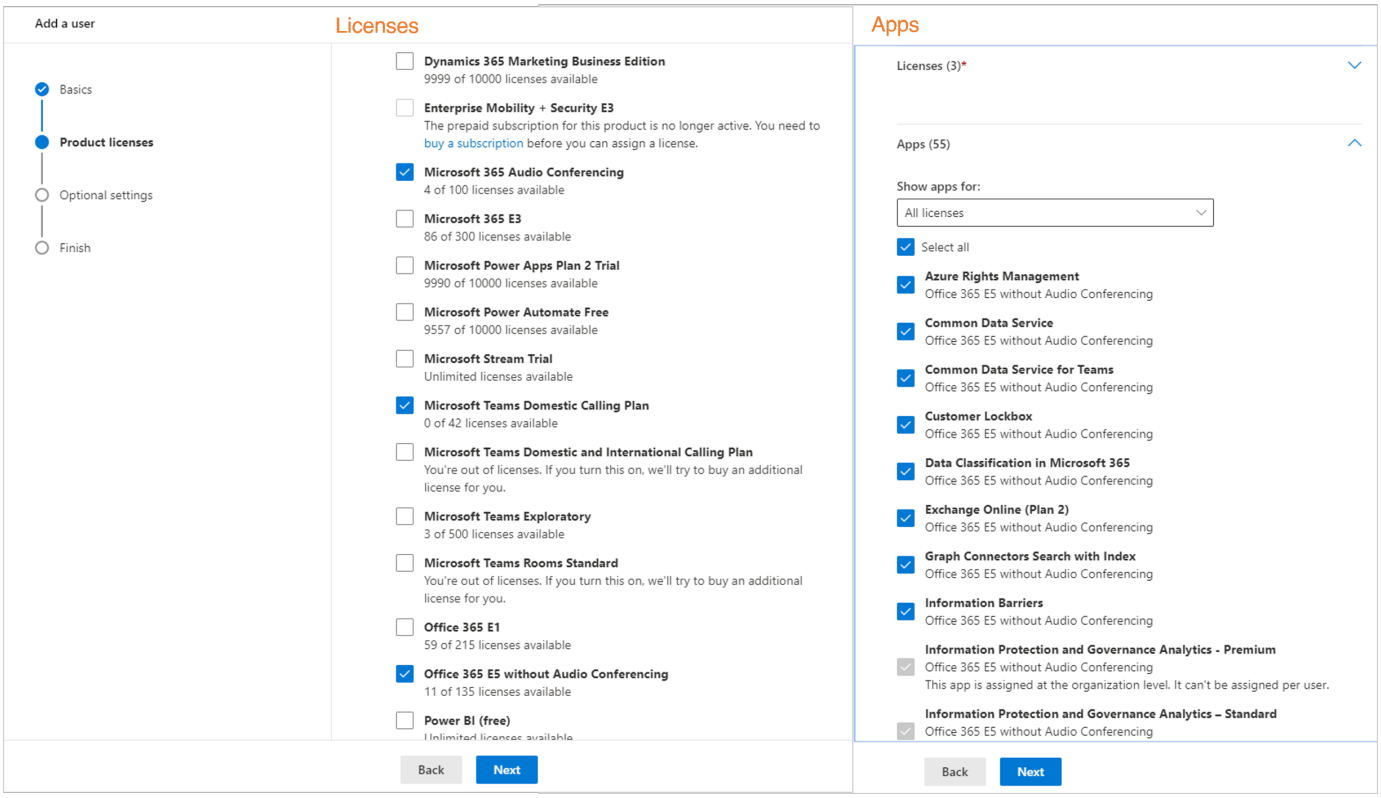
1. Sign in to the Microsoft 365 admin center as an administrator.
2. Go to **Users** > **Active users** > **Add a user**.



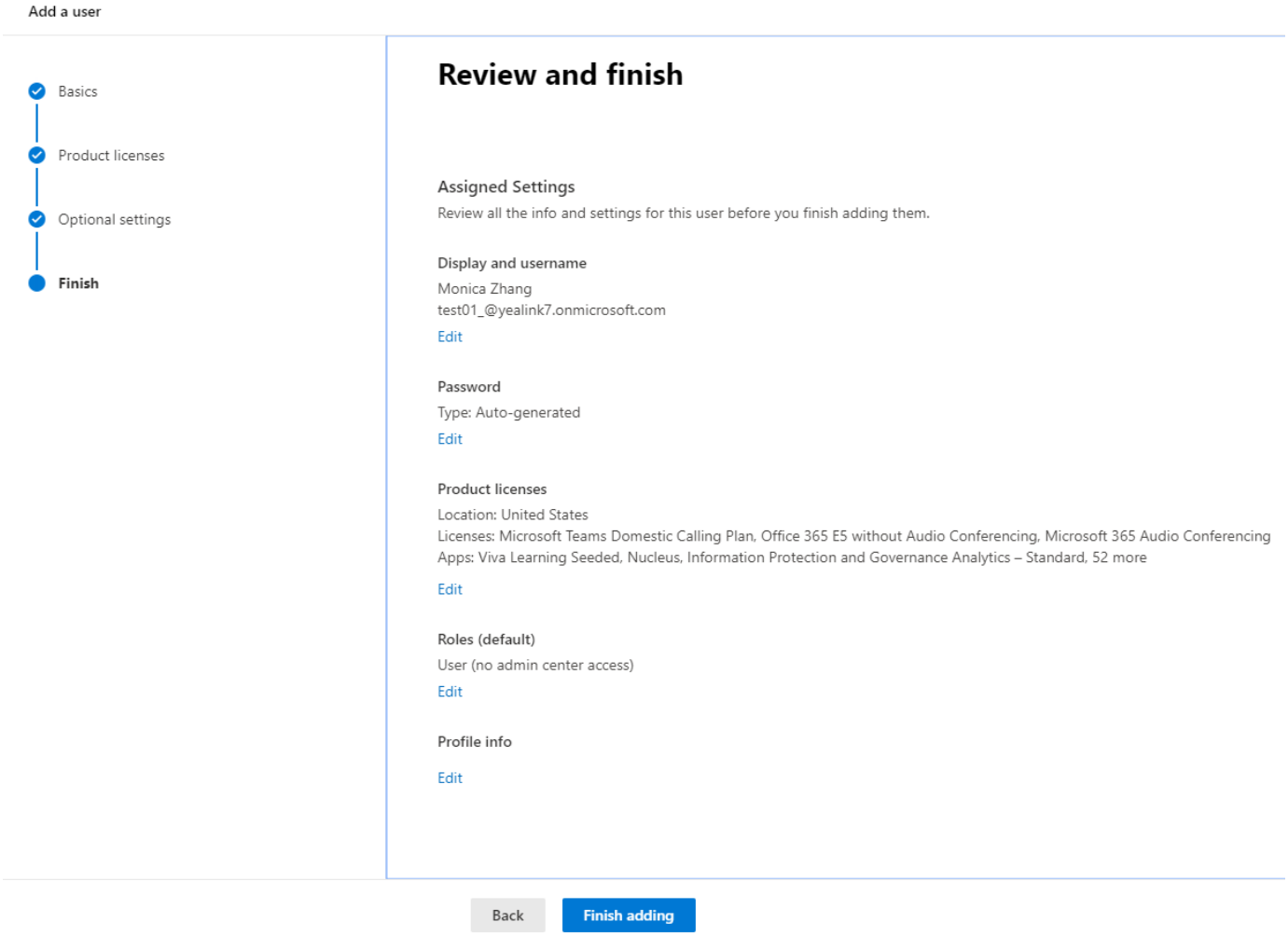
3. Set the basic information and click **Next**.



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



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



Change Account Password

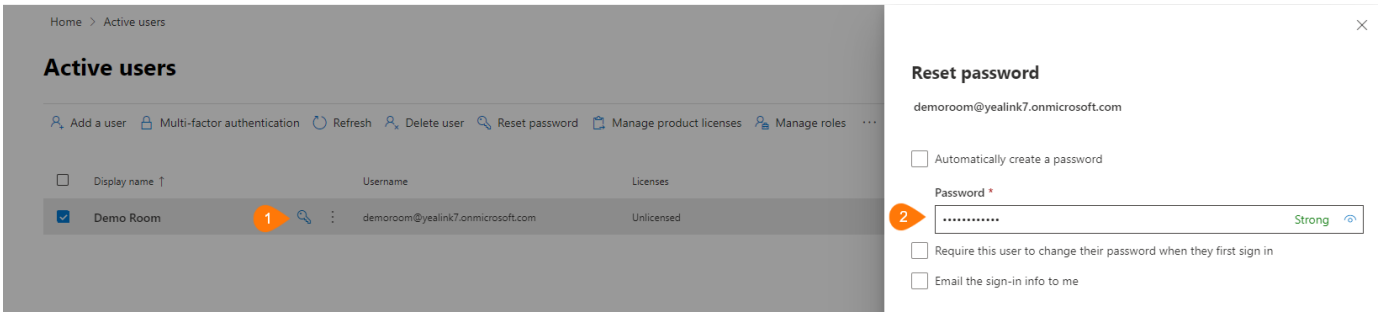
After you create accounts and assign licenses to them, you can set the account password.

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:

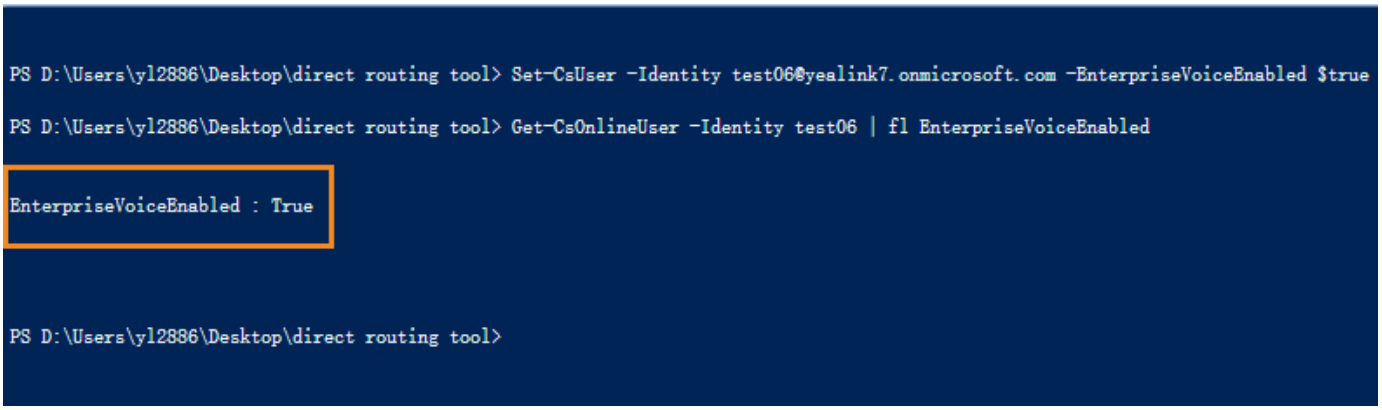
```
Set-CsUser -Identity "<User name>" -EnterpriseVoiceEnabled $true -HostedVoiceMail $true
// change <user name> to the actual user name
```

Example:

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

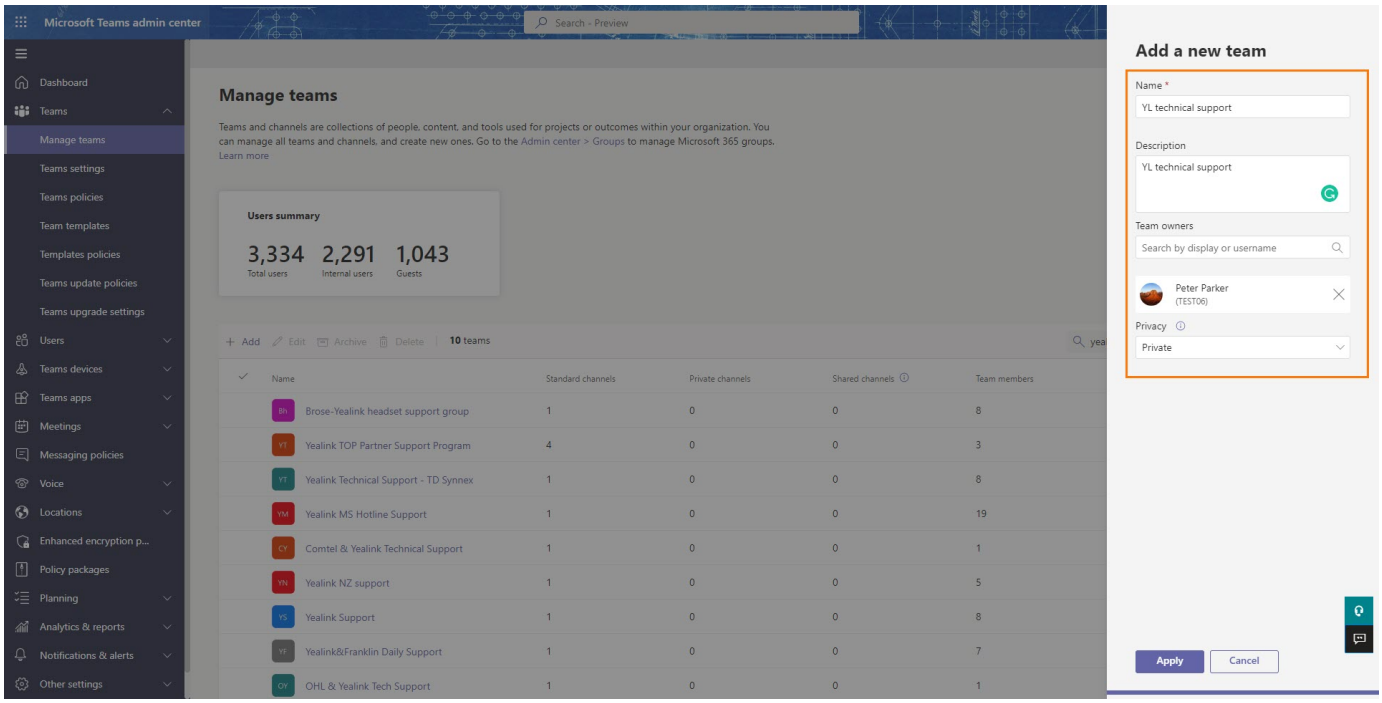
4. Run the command below to see the status:
5. If it is true, the Enterprise Voice feature is enabled.

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

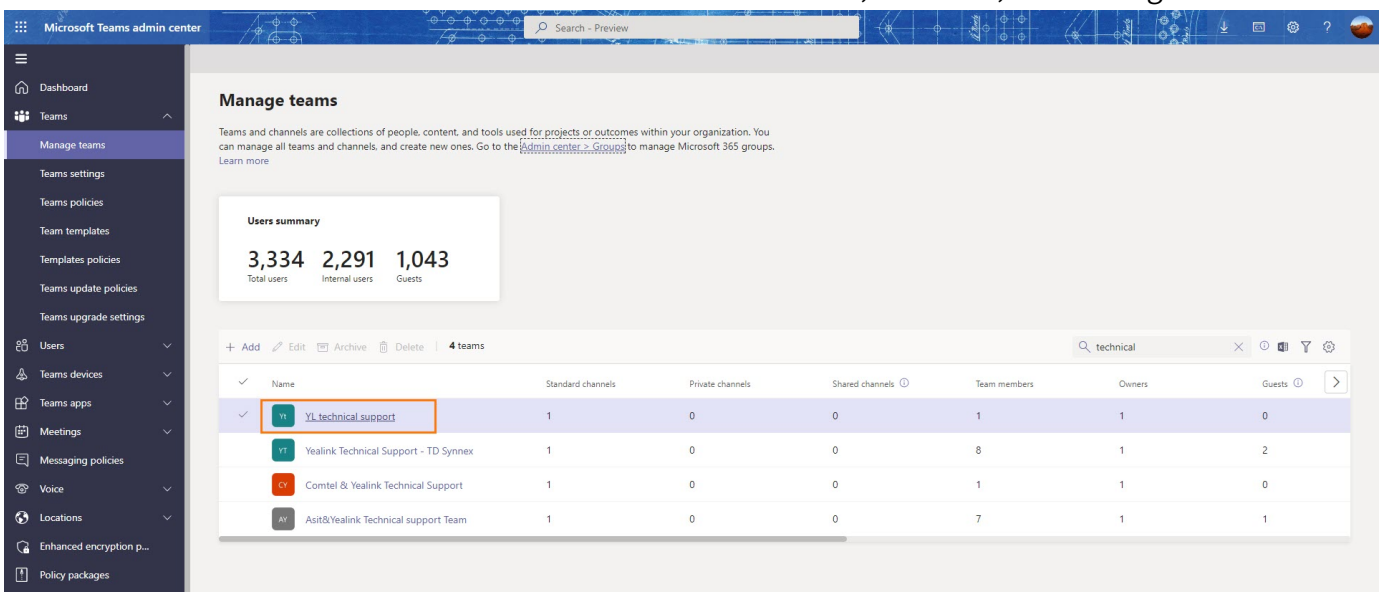


Step 2 - Create a Team for the Call Queue Agents

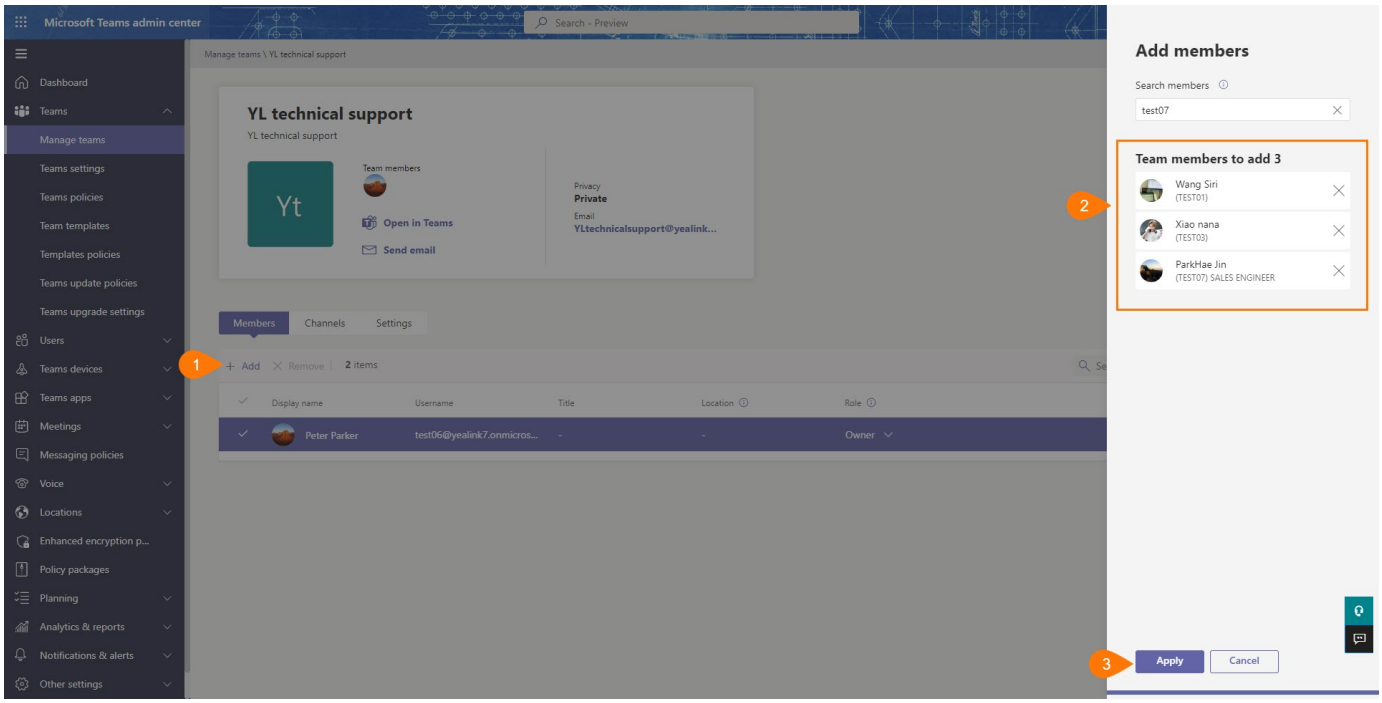
1. Sign in to the Microsoft Teams admin center as an administrator.
2. Expand **Teams** and select **Manage teams** > **Add**.
3. Enter the team information and click **Apply**.



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



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



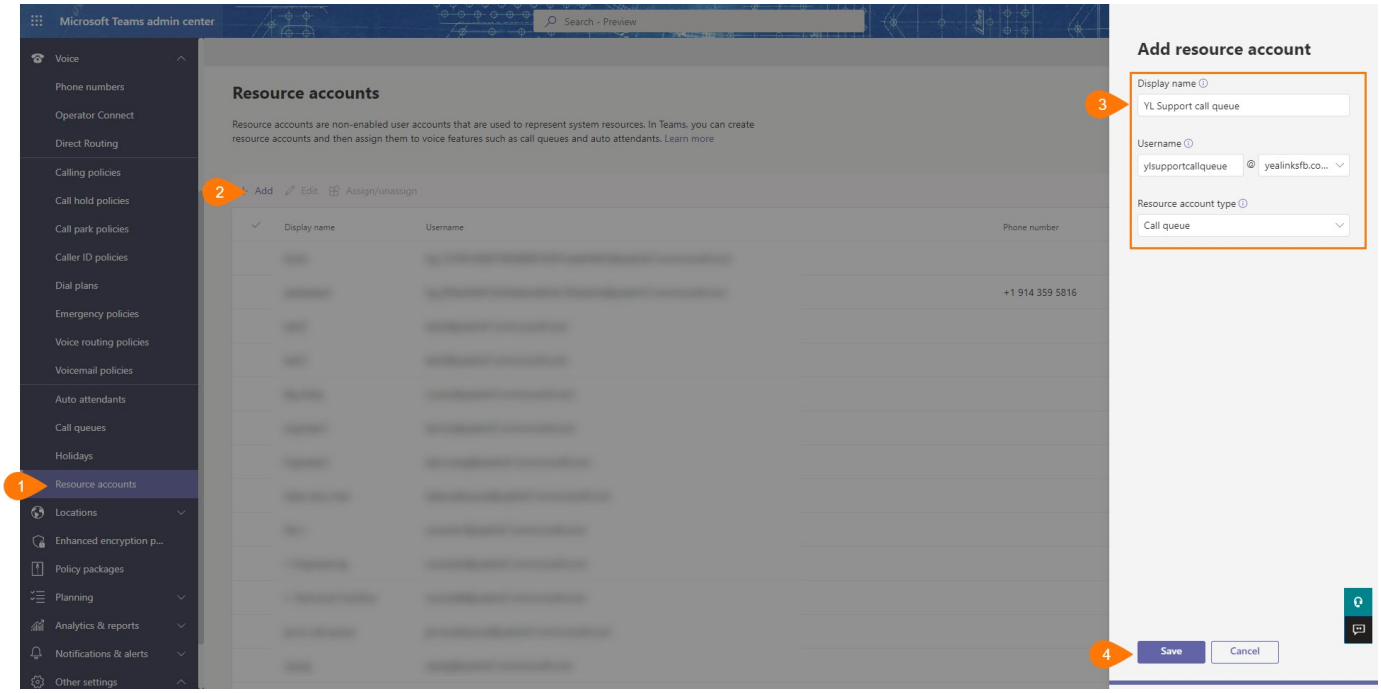
Step 3 - Create a Resource Account

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**.

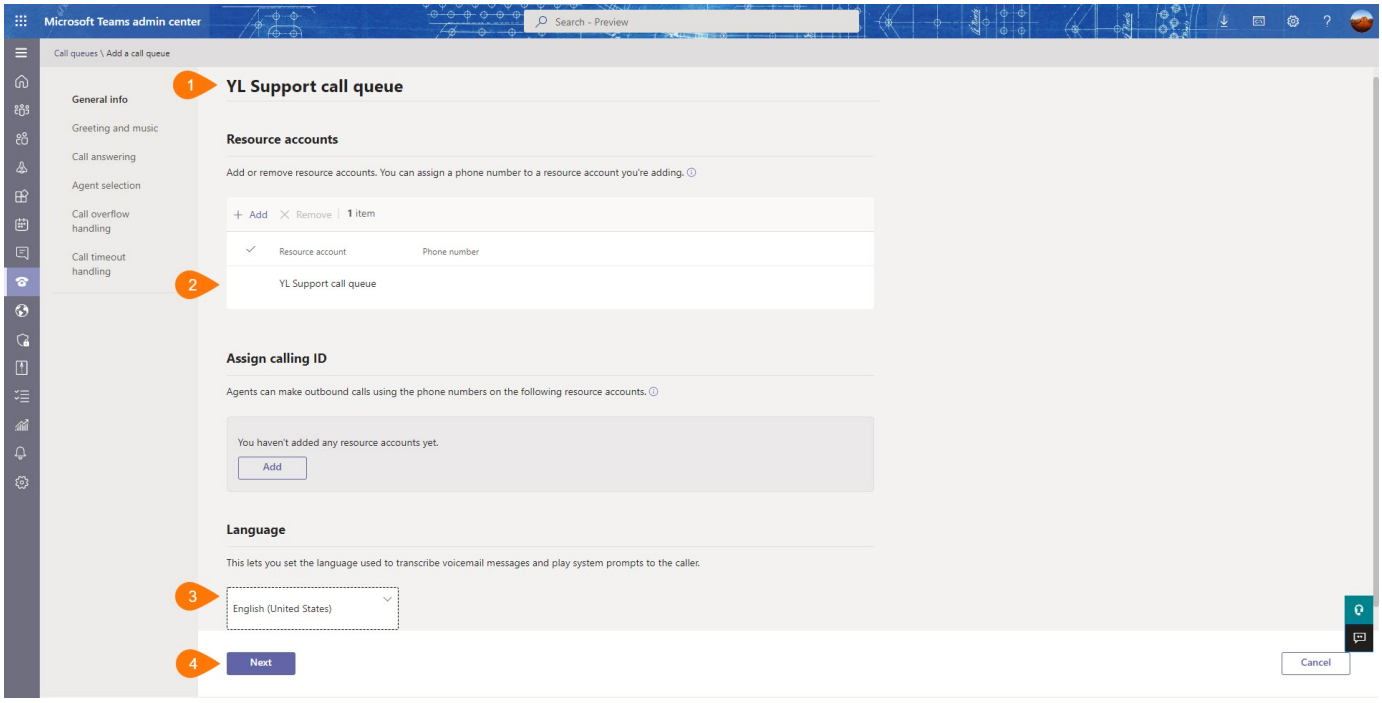
5. Select **Save changes**.

Step 5 - Create a Call Queue

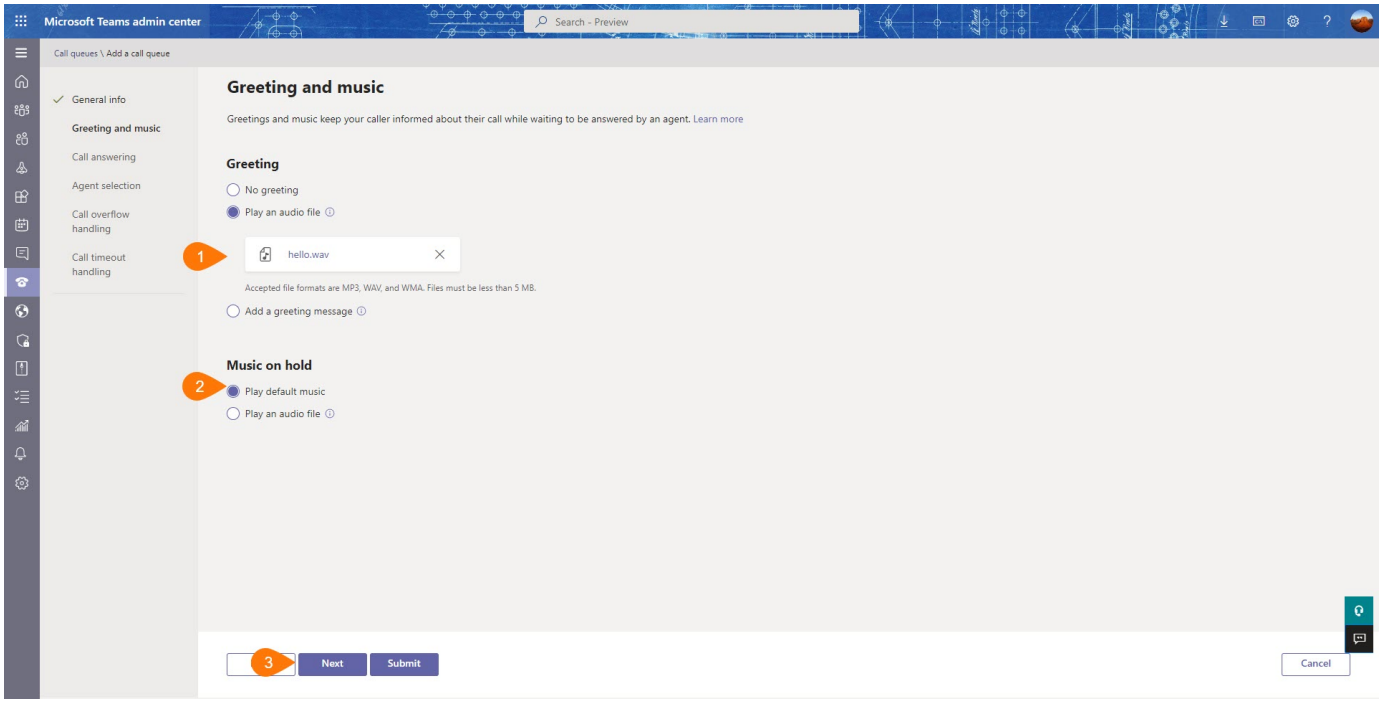
1. Sign in to the Microsoft Teams admin center as an administrator.

2. Expand **Voice** and select **Call queues** > **Add**.

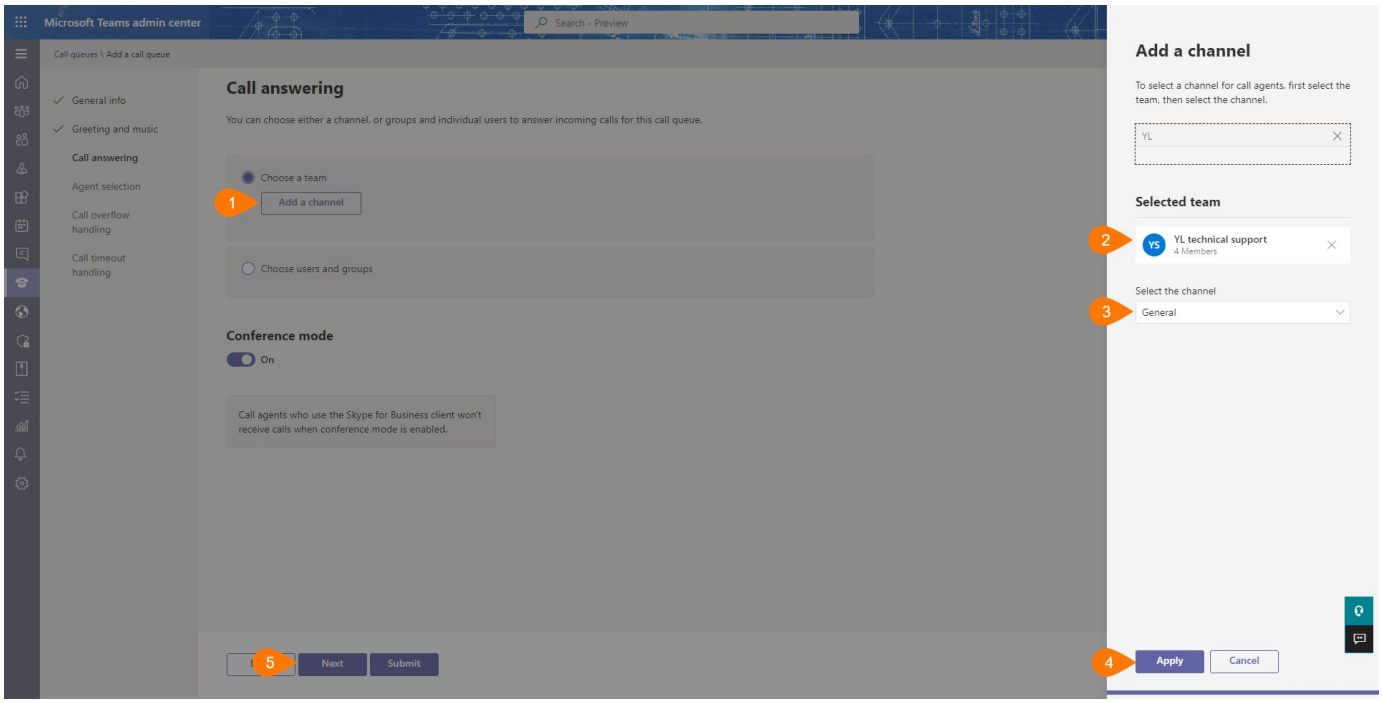
3. Set the general information and click **Next**.



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

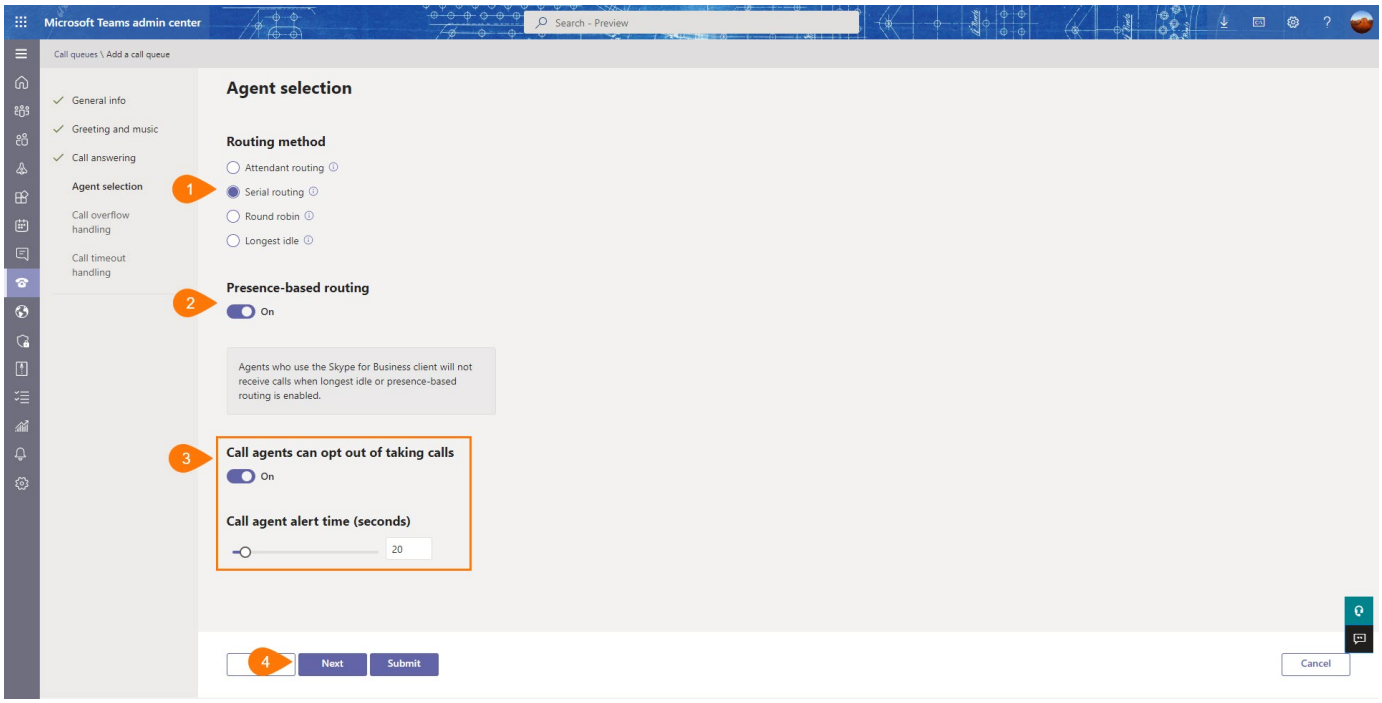


5. Set up call answering and click **Next**.



- 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**.

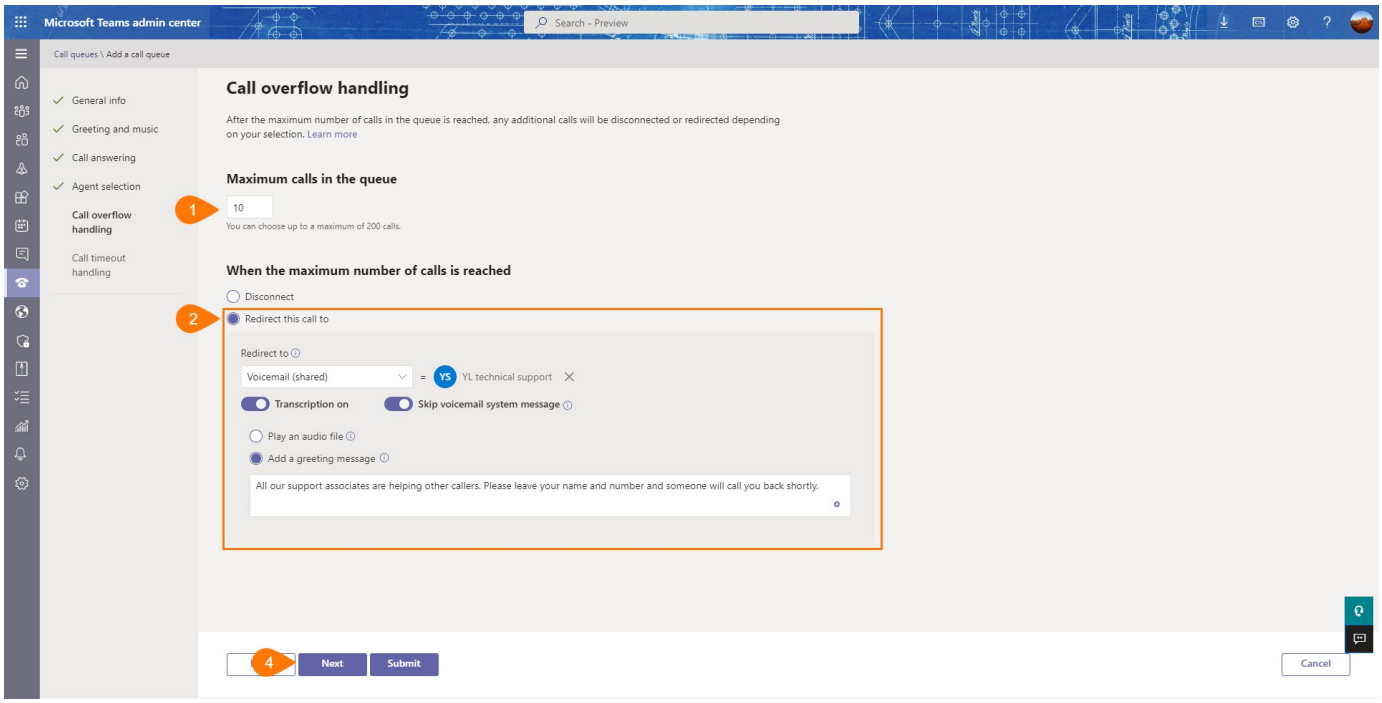


- Serial routing: it brings each agent one by one in the order specified in the **Call agents** list. If an agent dismisses or doesn't pick up a call, the call will ring to the next agent. This will repeat until the call is picked up or times out.
- Presence-based routing: call agents whose availability status is set to **Available** can receive the

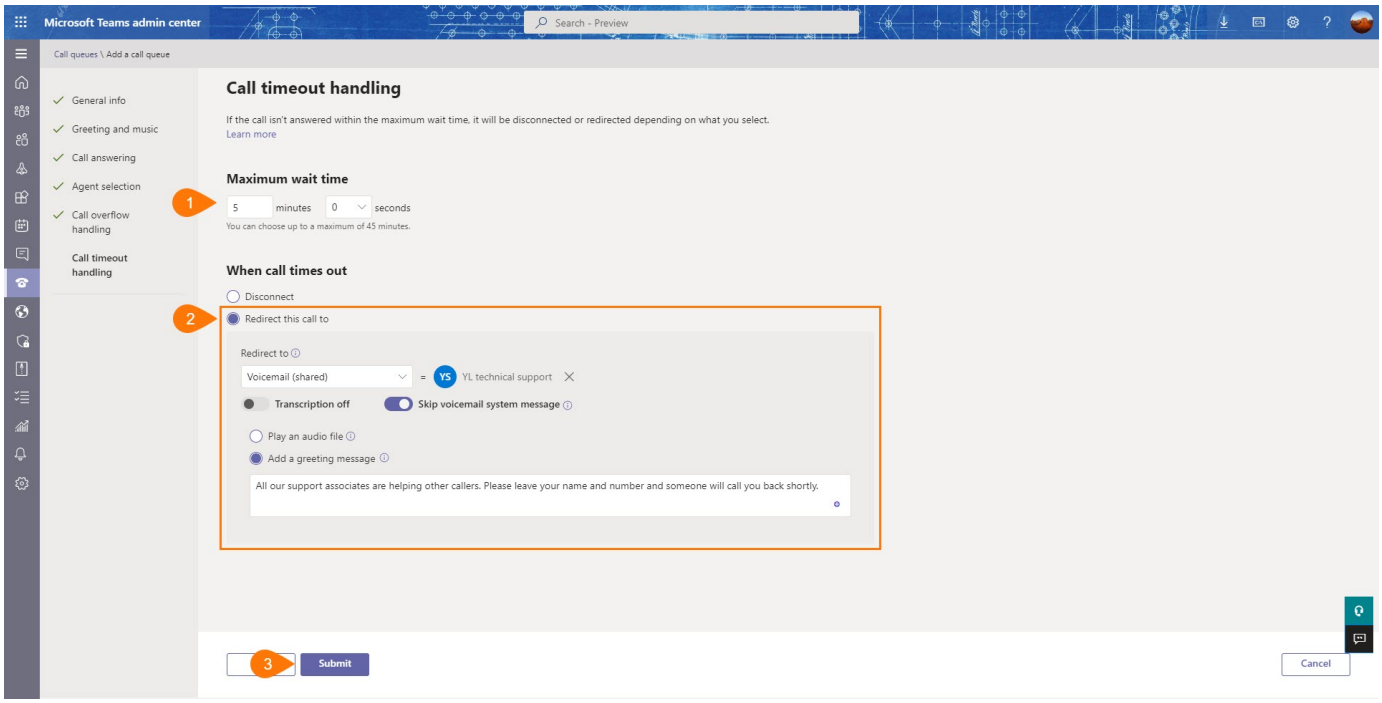
call.

- 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**.



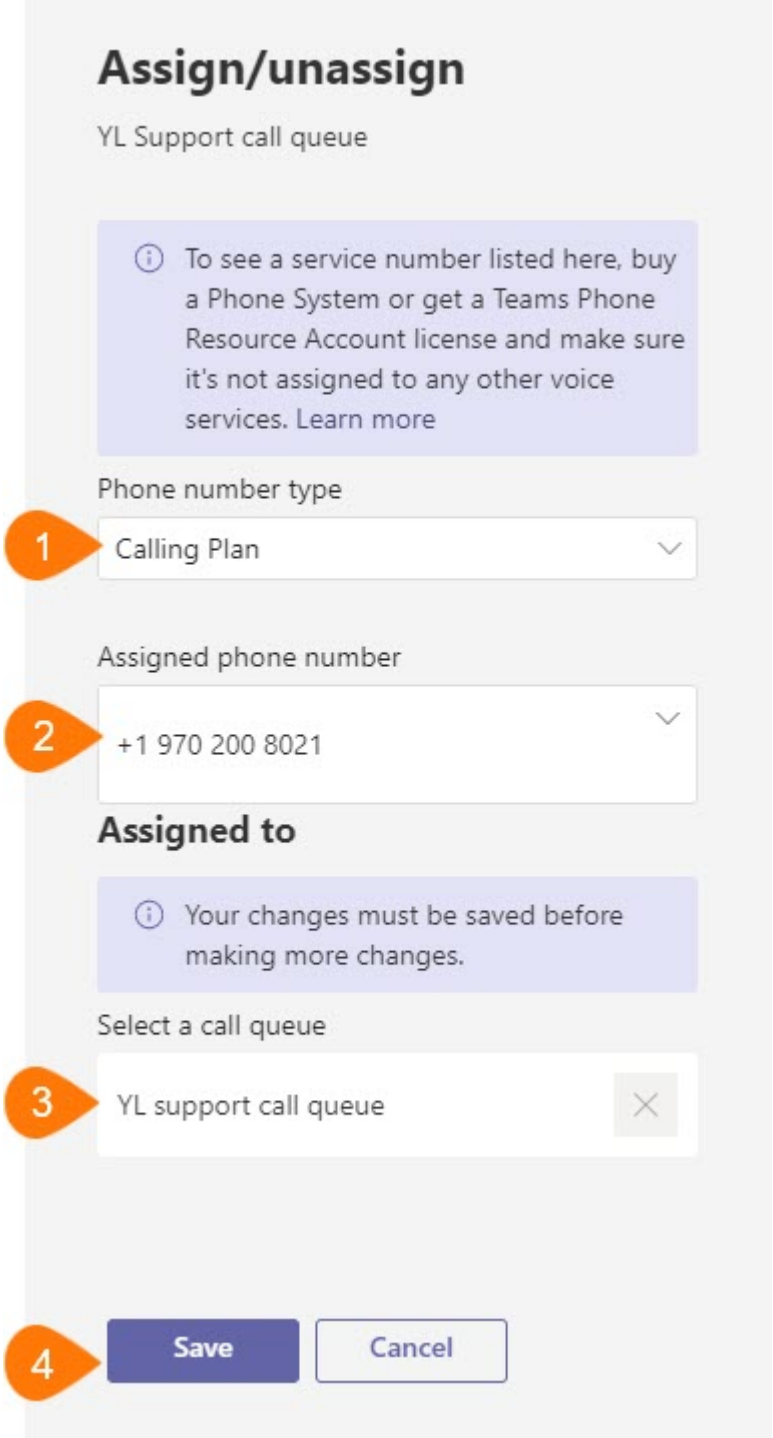
8. Set call timeout handling and click **Submit**.



- 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**.



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.

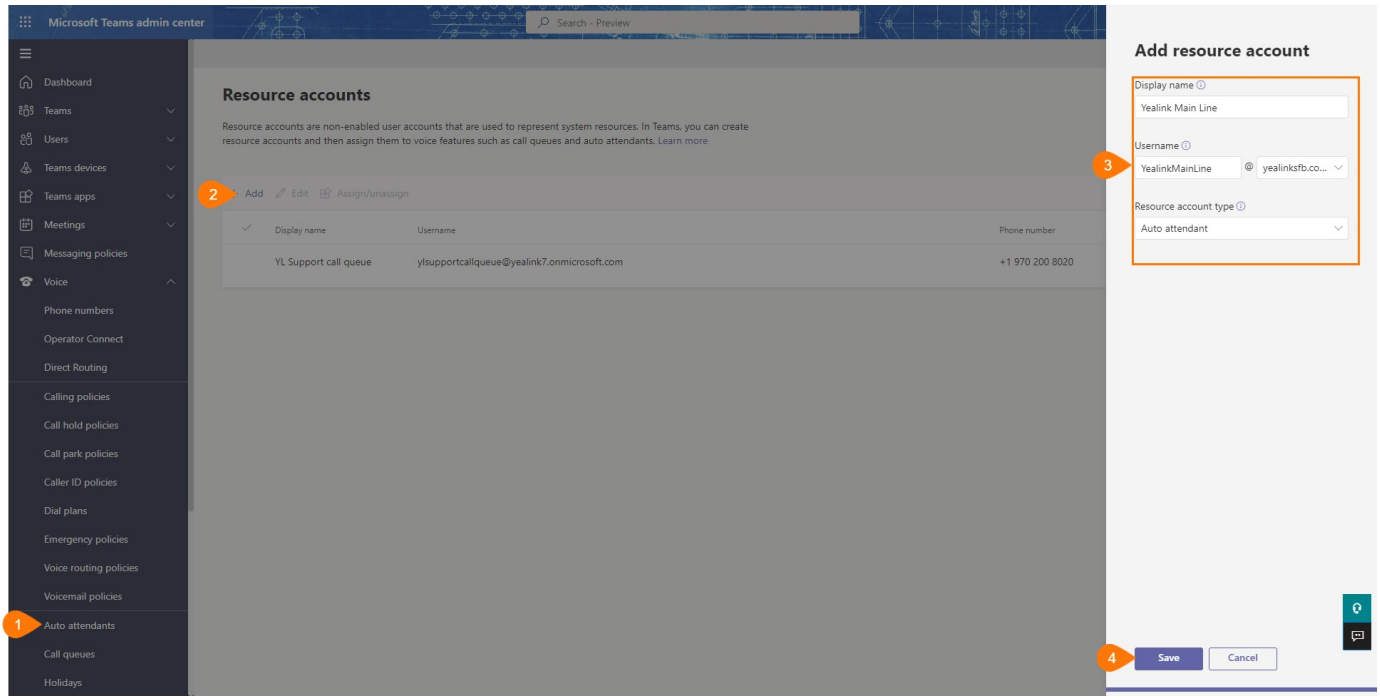
Prerequisites

- 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

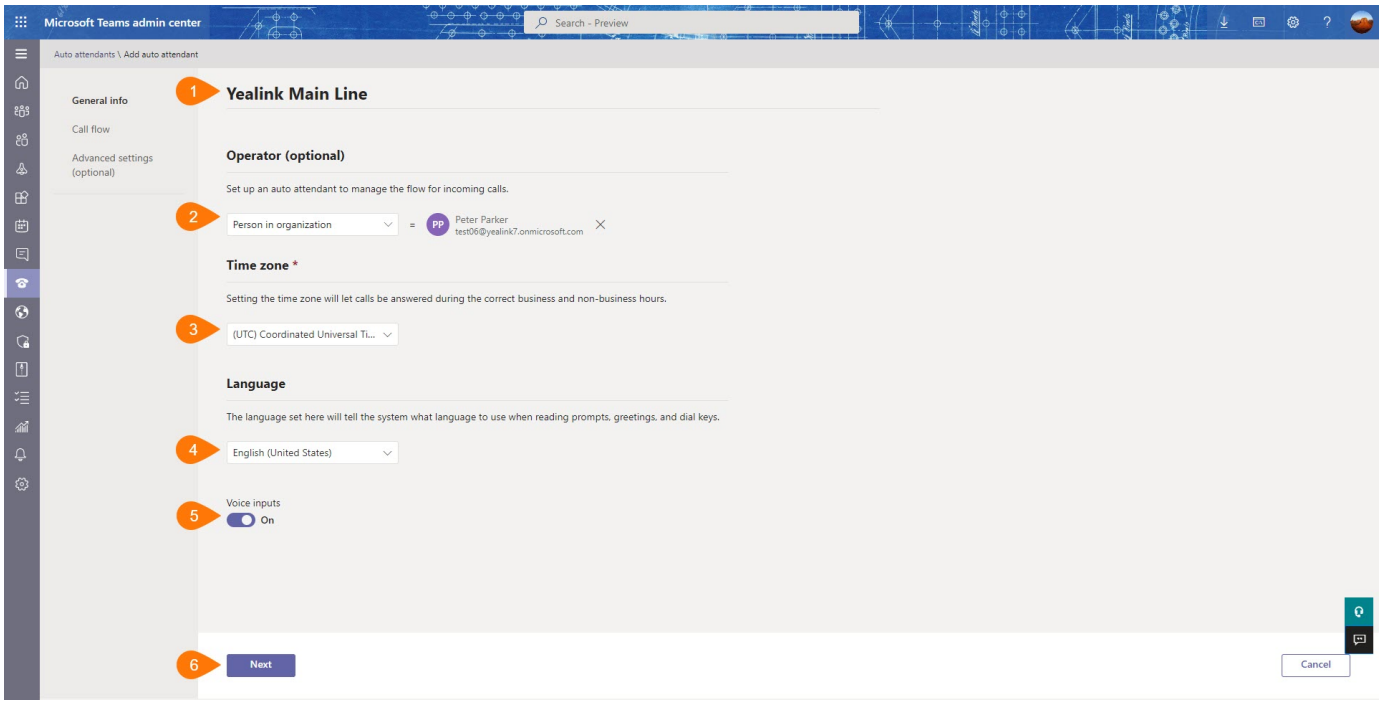
See Enable Enterprise Voice for Agents.

Step 4 - Create an Auto Attendant

1. Sign in to the Microsoft Teams admin center as an administrator.

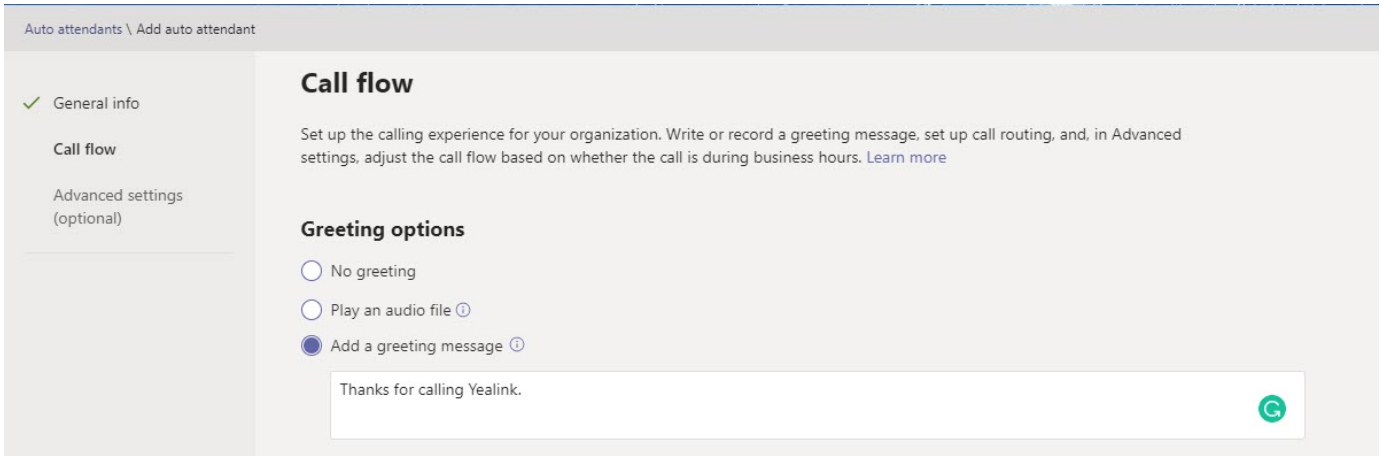
2. Expand **Voice** and select **Auto attendants** > **Add**.

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

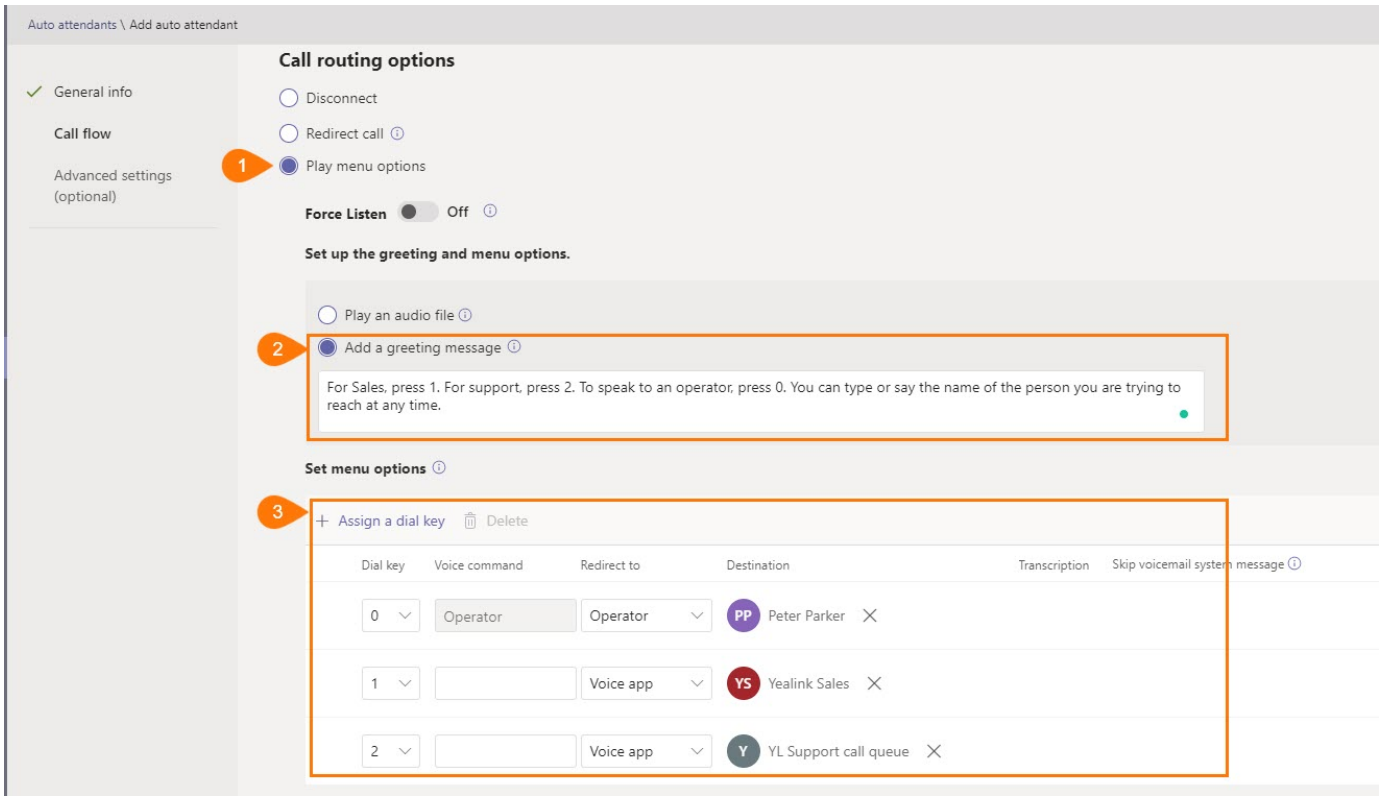


4. Set the call flow and click **Next**.

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



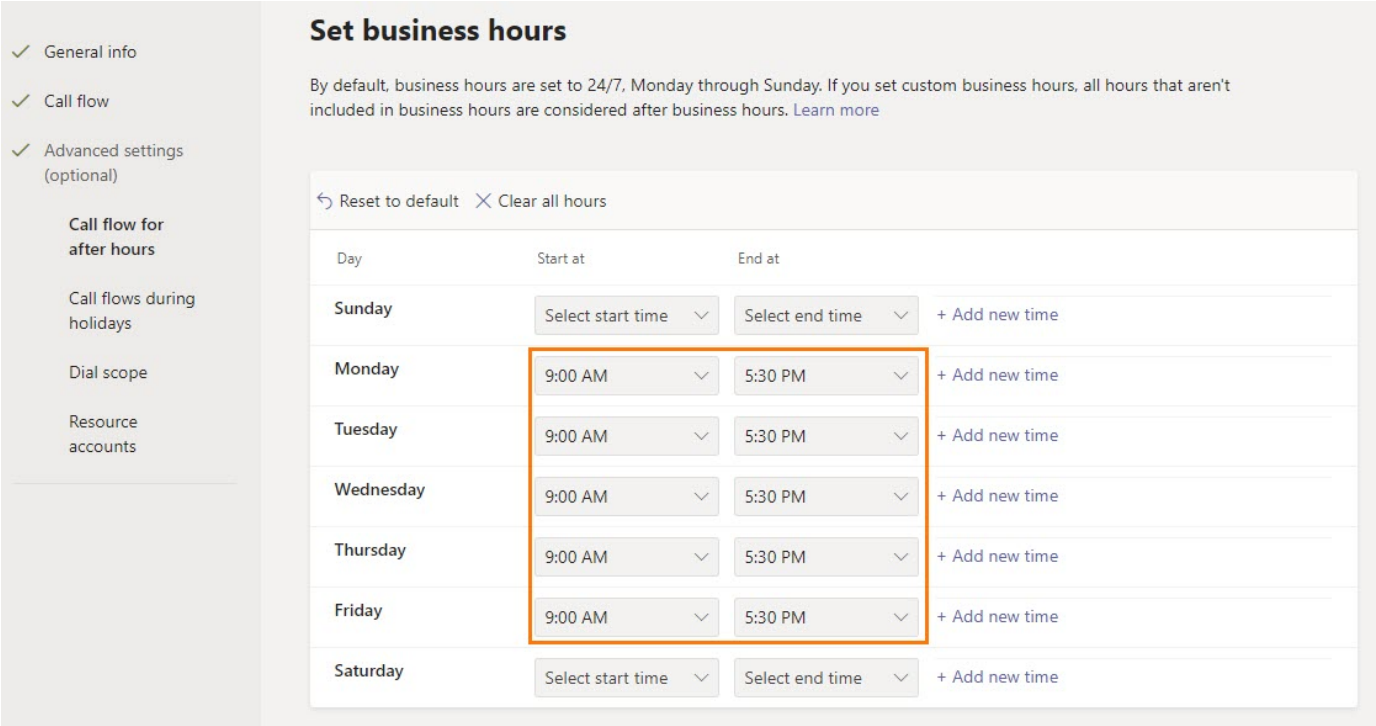
   b. Set the call routing options and click **Next**.



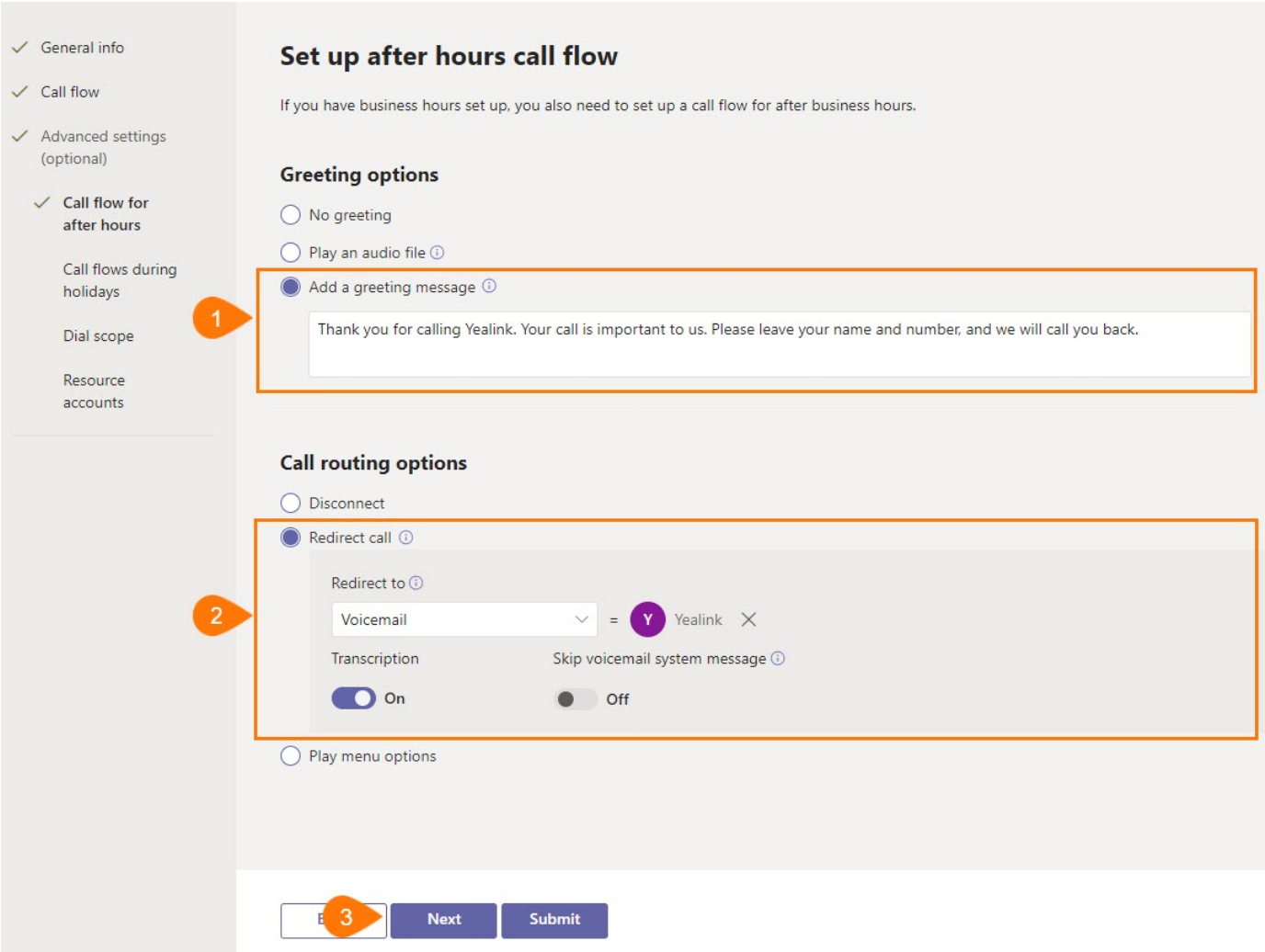
c. Set the directory search type.

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.

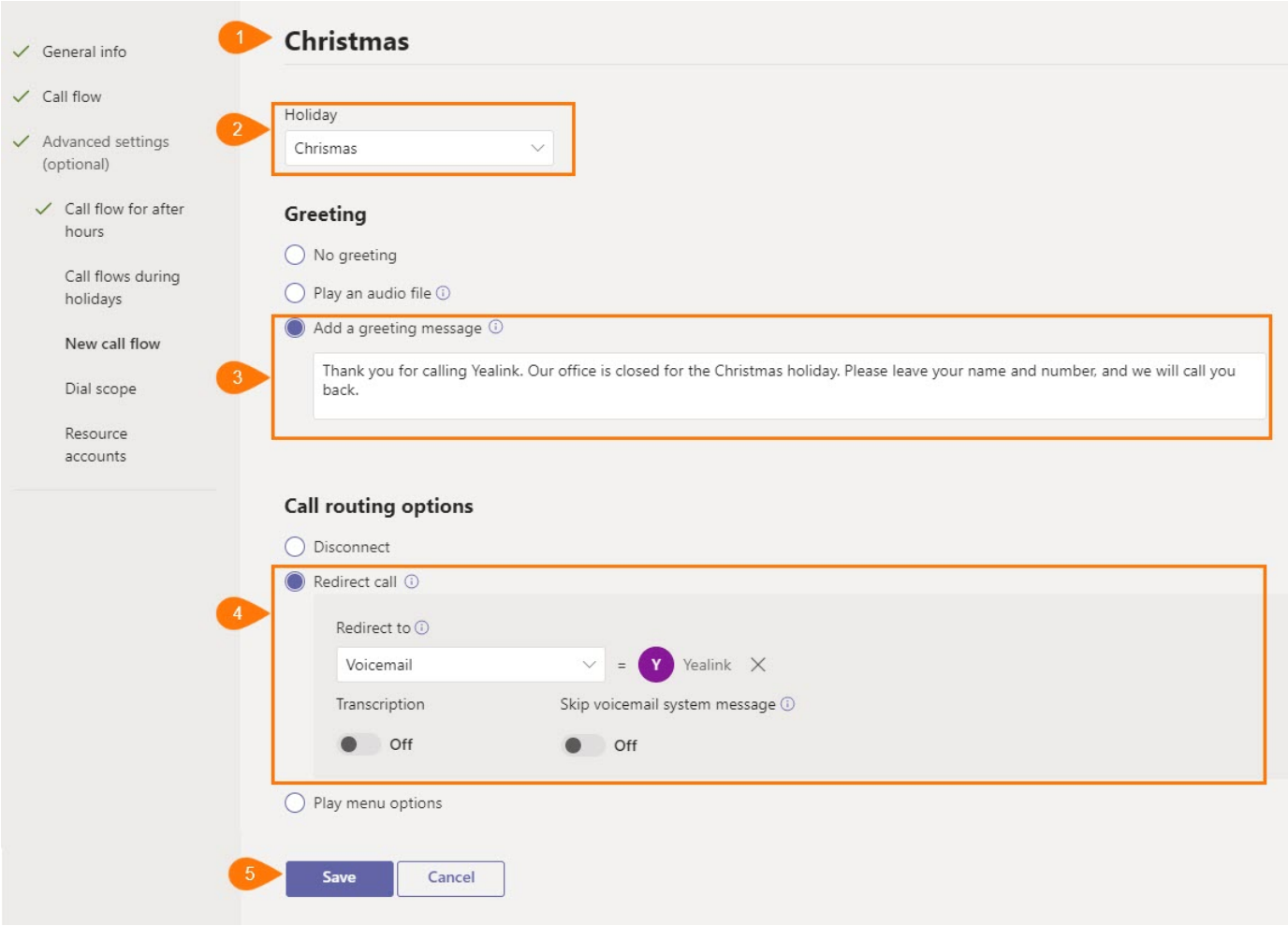
5. Set your company's business hours.



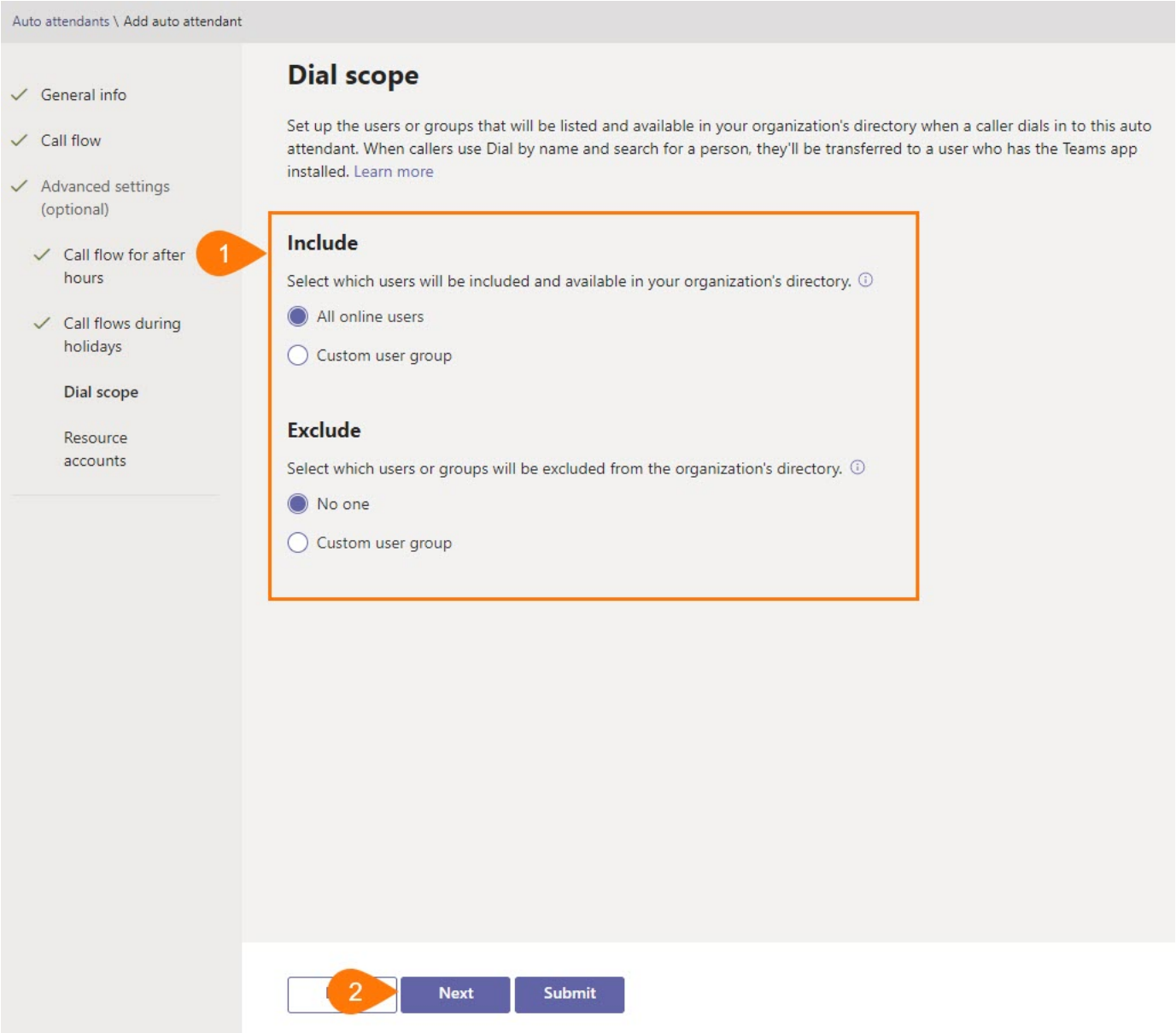
6. Set up after-hours call flow.



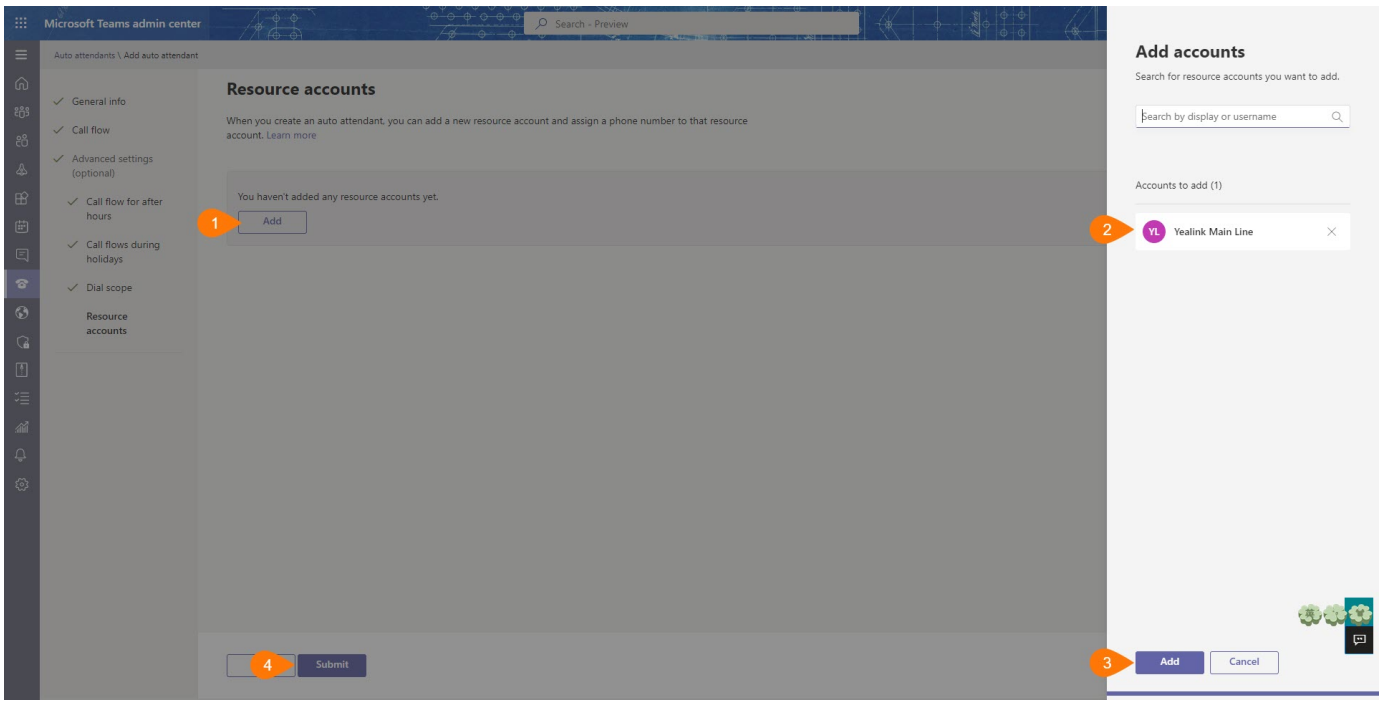
7. Click **Add** to add call flows during holidays. If you have not set a holiday, add one first.



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

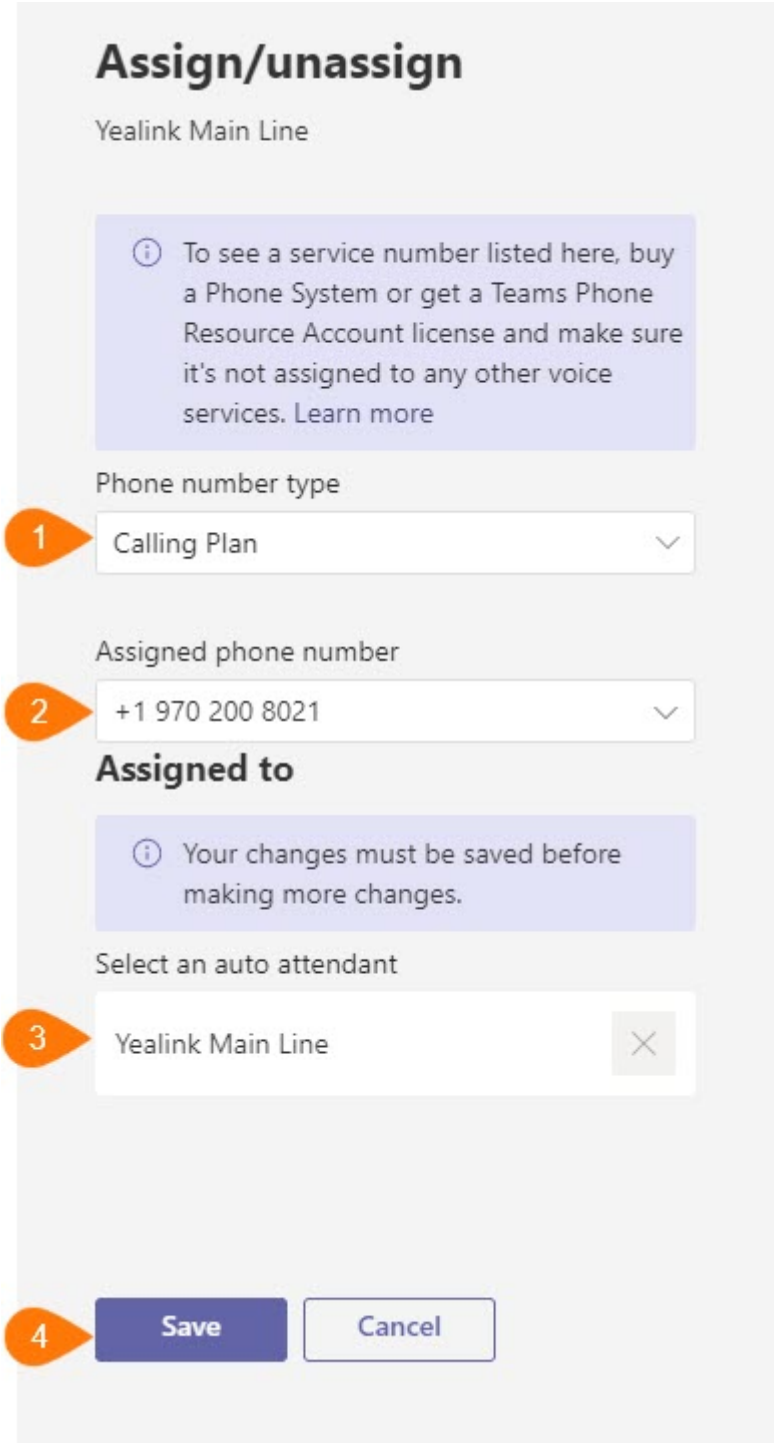


9. Add a resource account and click **Submit**.



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**.



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

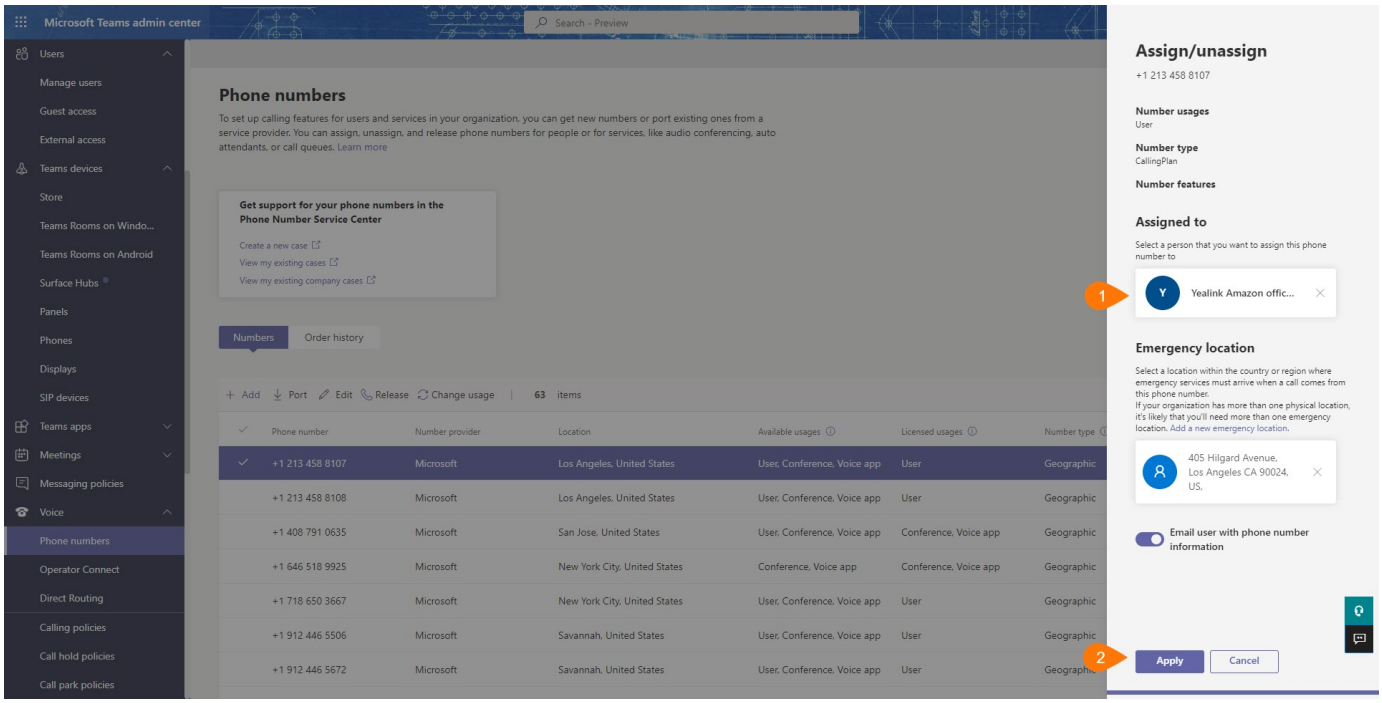
Make sure you have purchased the **Common Area Phone** license on Microsoft 365 admin center.

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**.



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**.

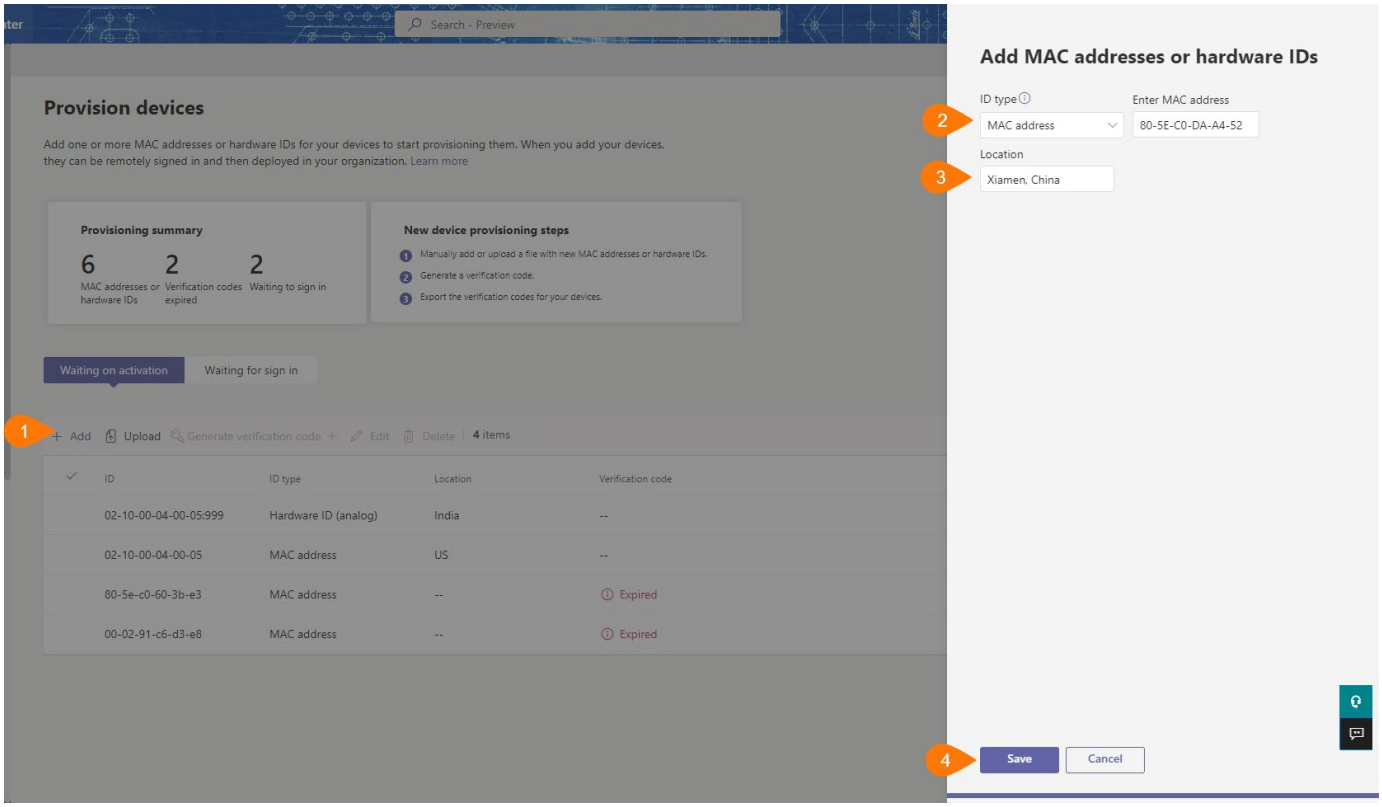
3. Select **Provision new device** from the **Actions** tab.

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**.



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

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

d. Download the file template.

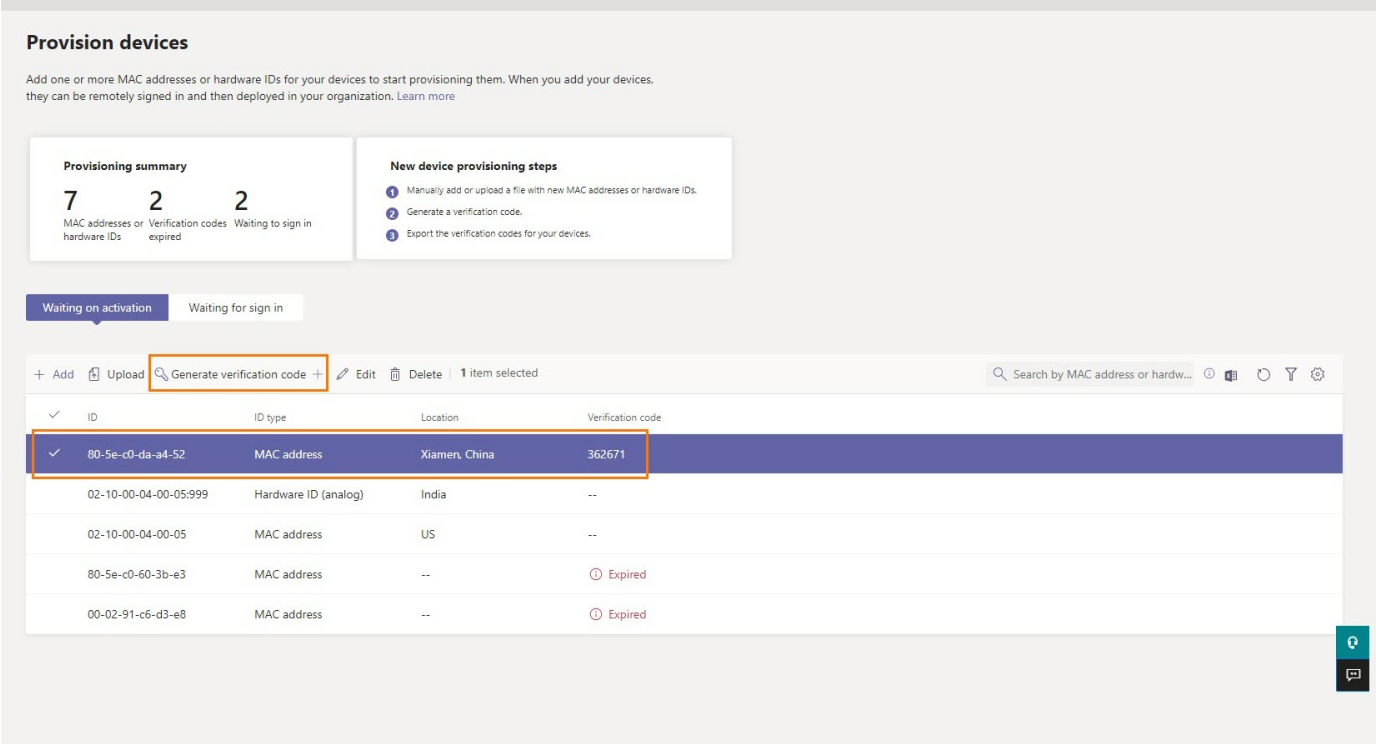
e. Enter the MAC ID and location, and then save the file.

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.

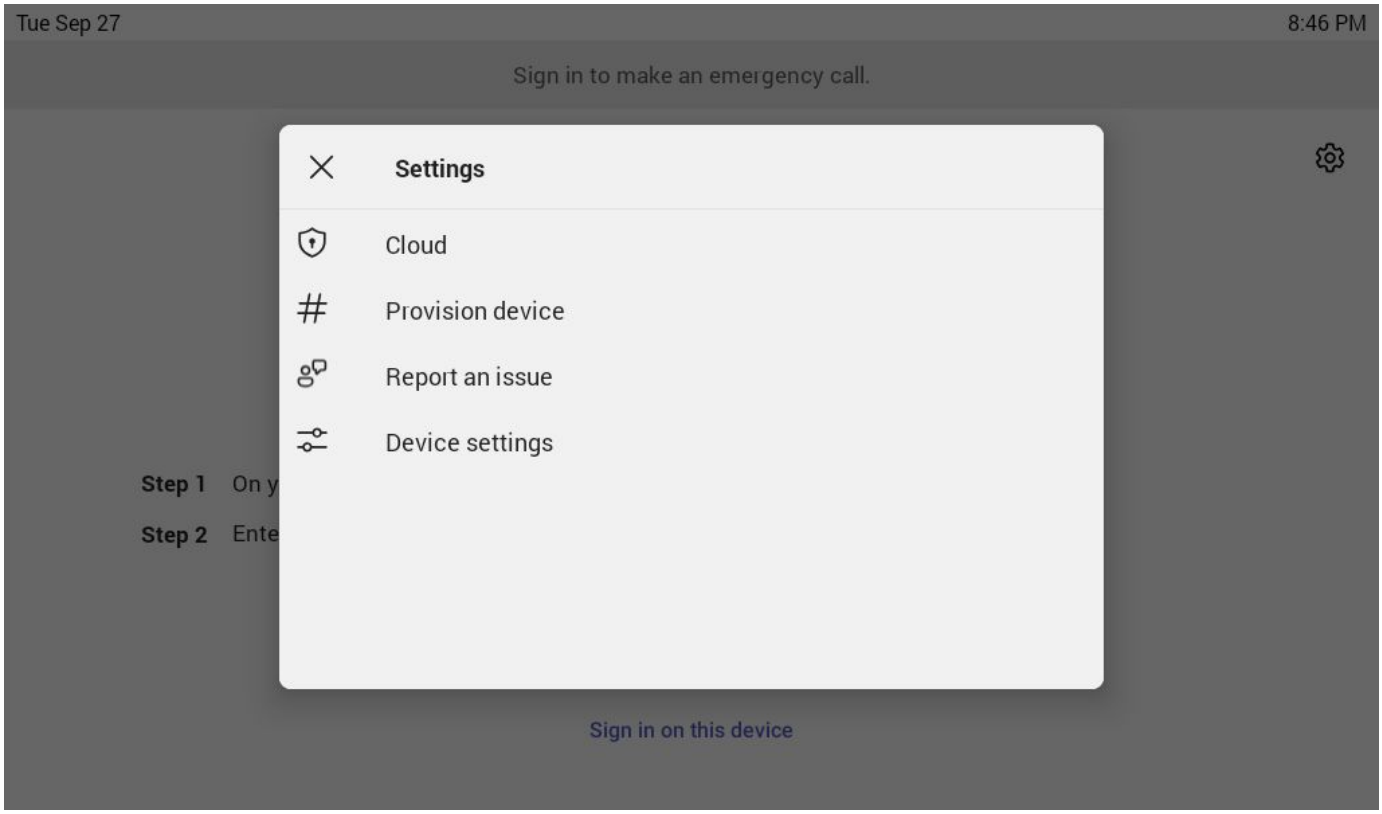


4. You can also provide the list of MAC IDs and verification codes to the field technicians. You can export the detail directly in a file and share the file with the technician who is doing the actual installation work.

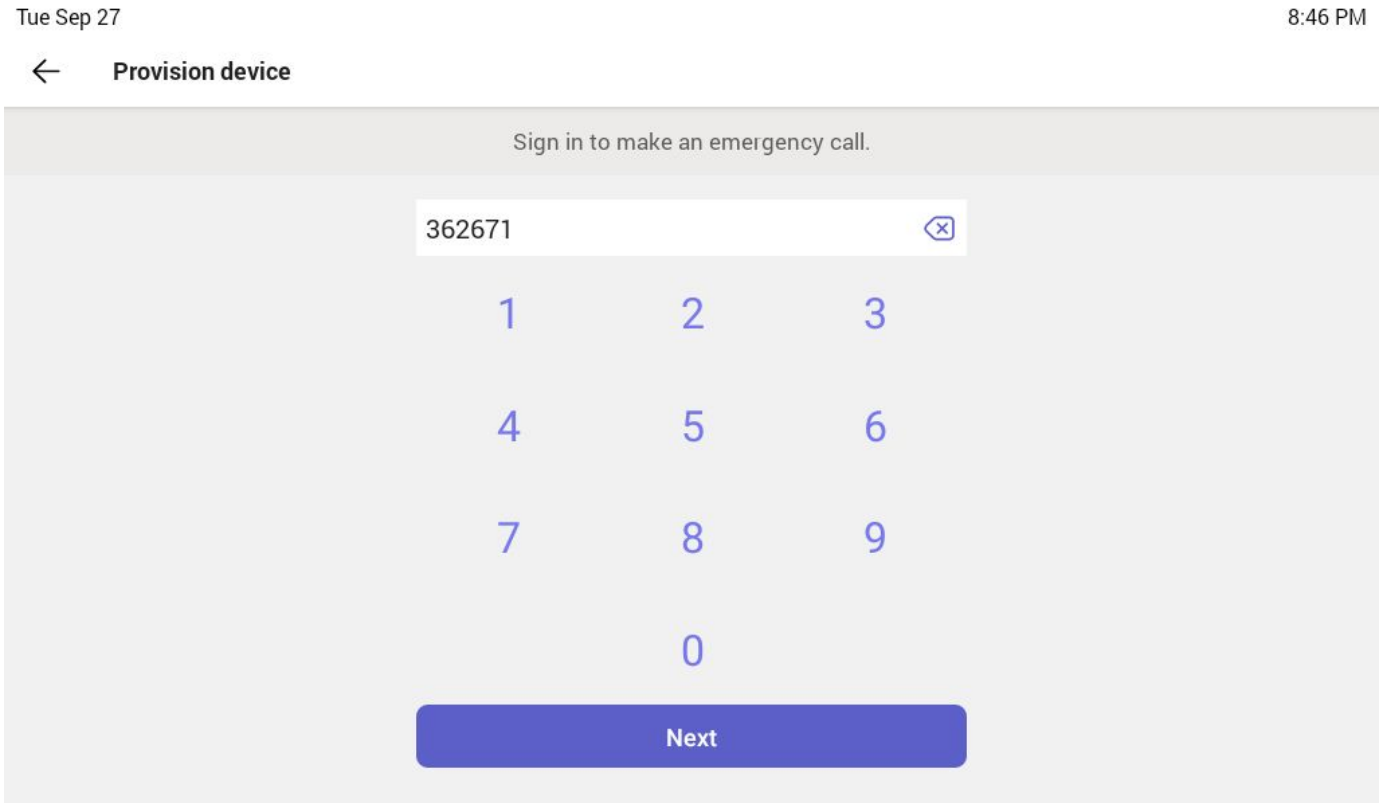
Provision Devices

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.

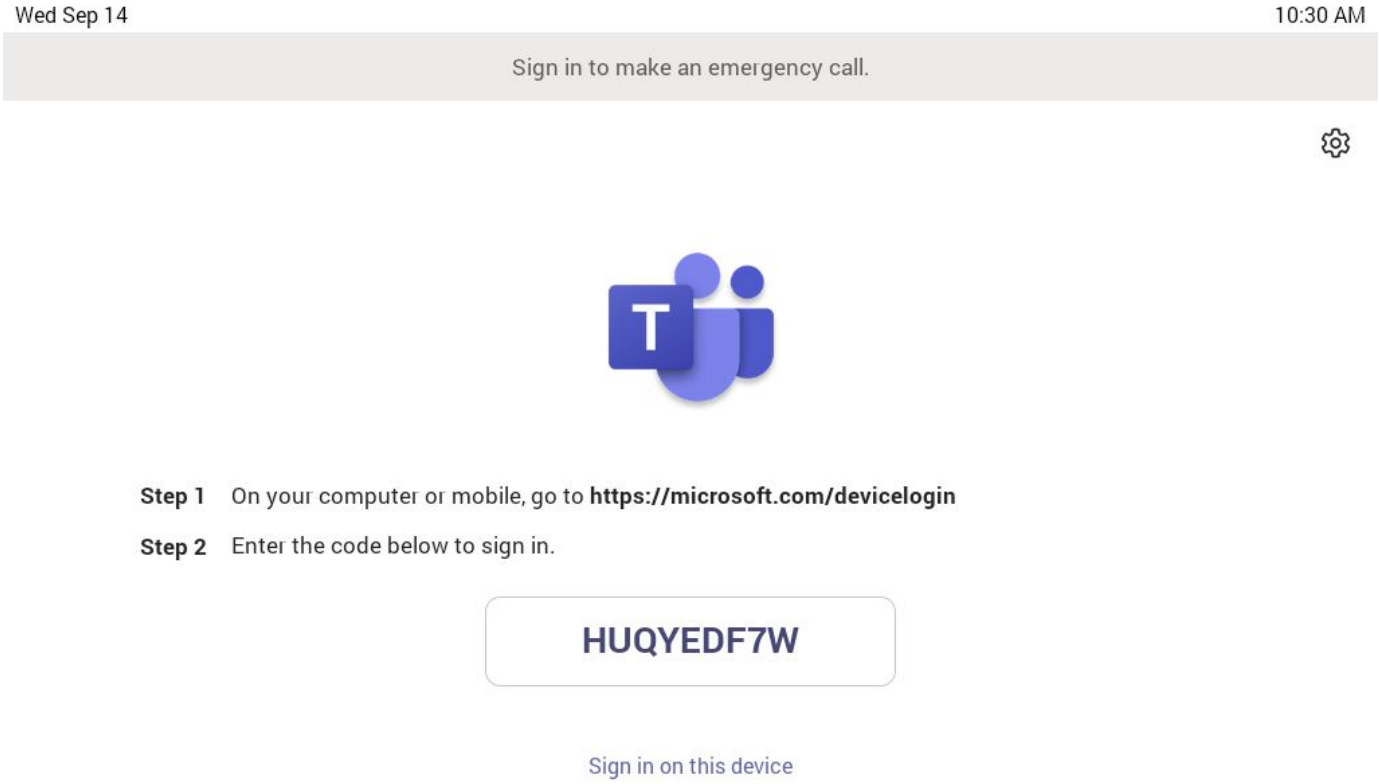
> The following illustrations serves as examples. The actual phone screen you see might be different.

Before you begin

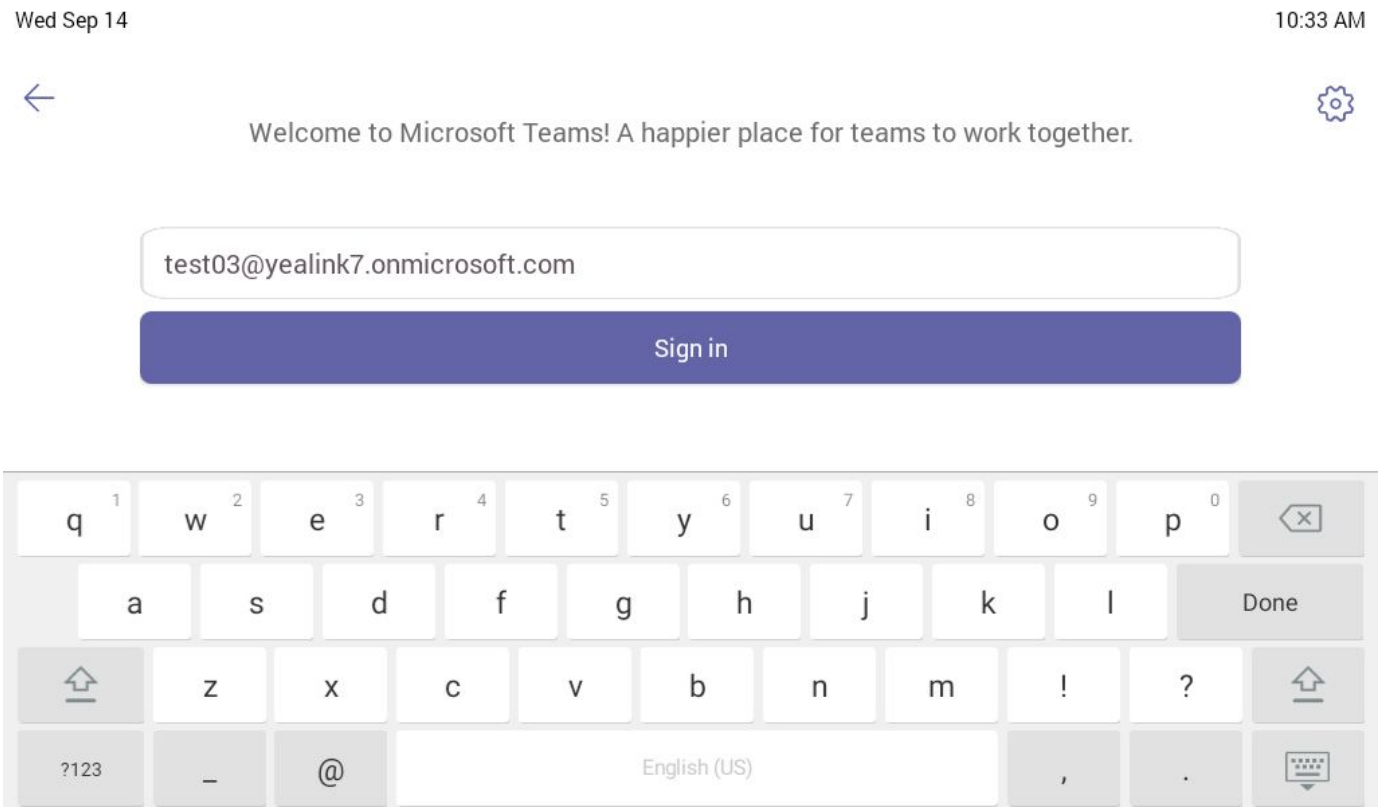
Contact your system administrator to get your sign-in account.

On Your Teams Device

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

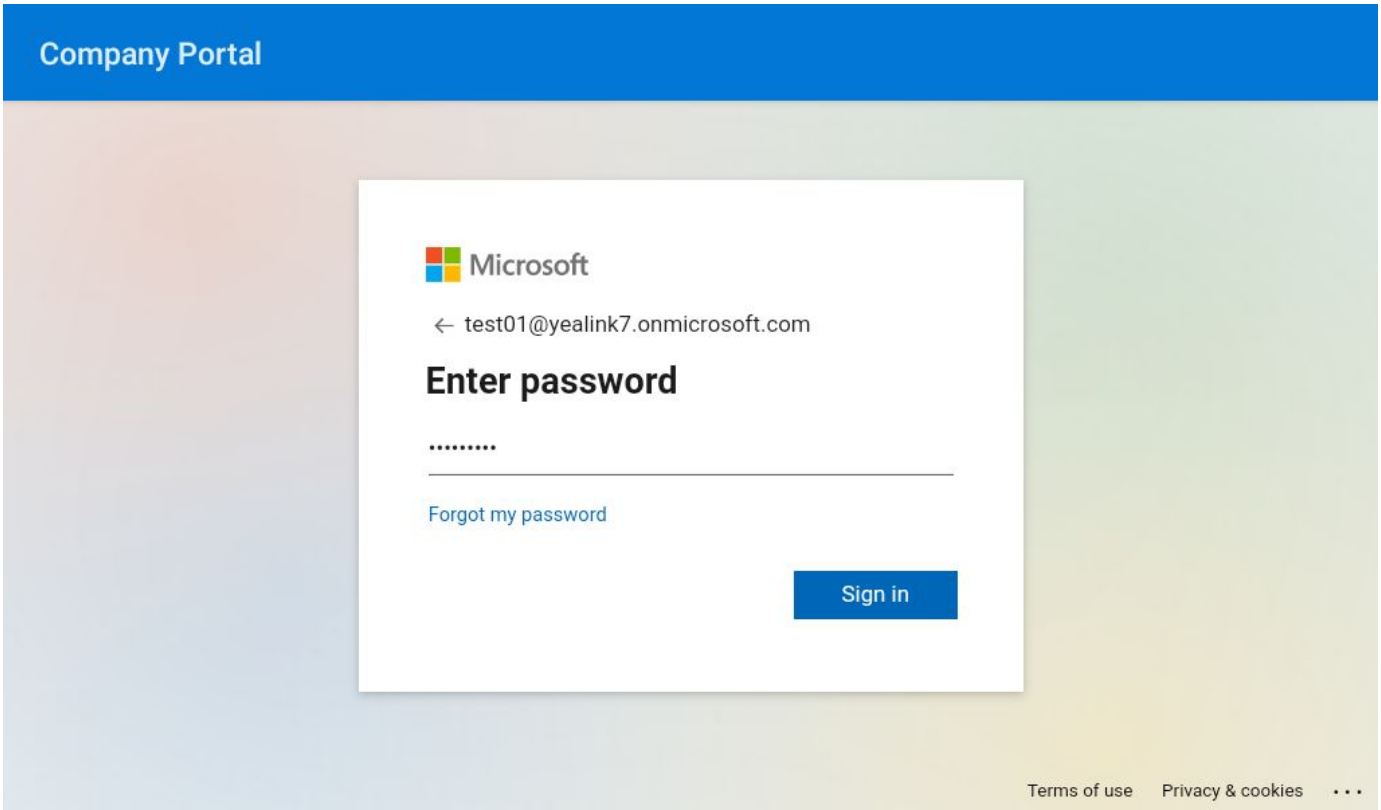


2. Enter your user credentials and tap **Sign in**.

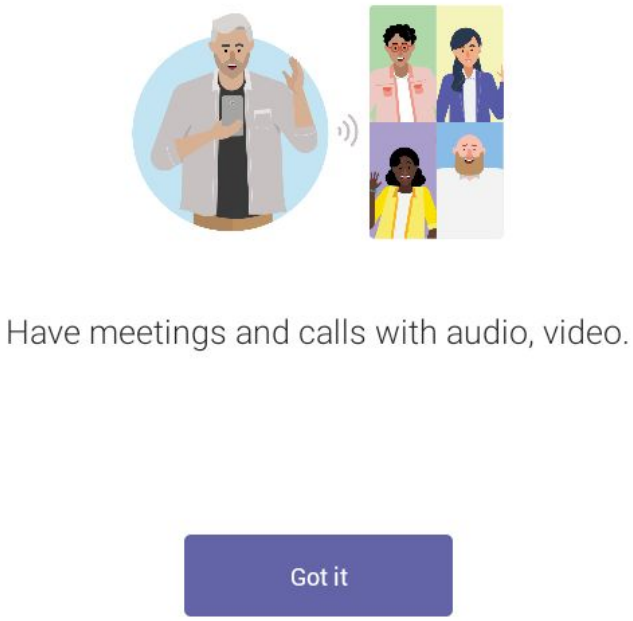


4. You will be connected to the Company Portal automatically.

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



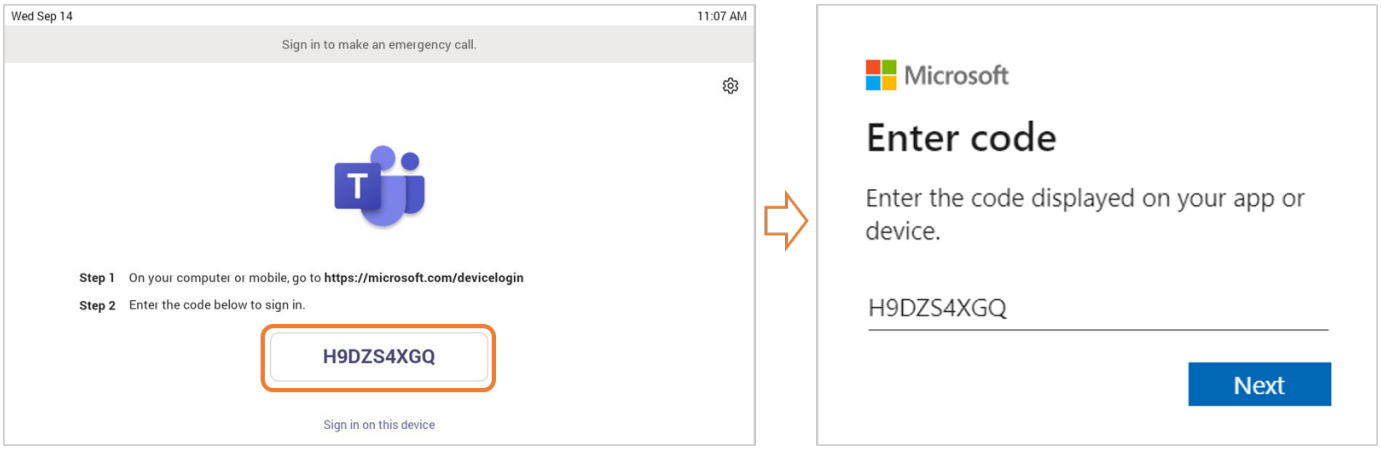
4. After the device signs in successfully, tap **Got it**.



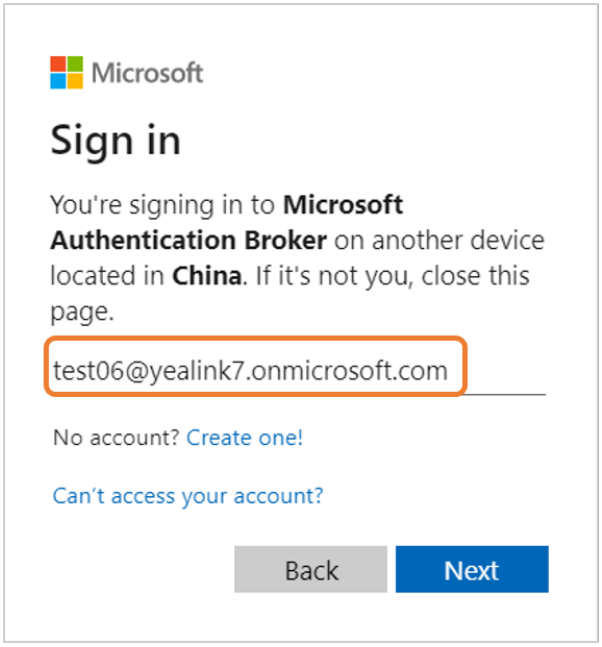
On a Web Browser

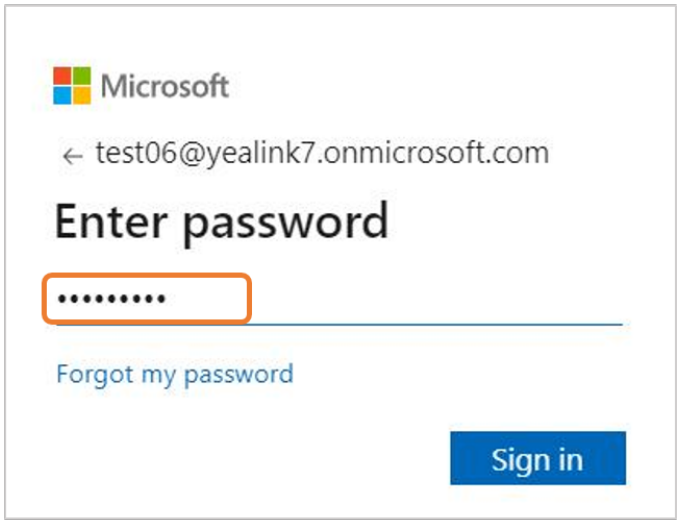
1. Go to https://microsoft.com/devicelogin on your computer or mobile.

2. Enter the code shown on your device and select **Next**.



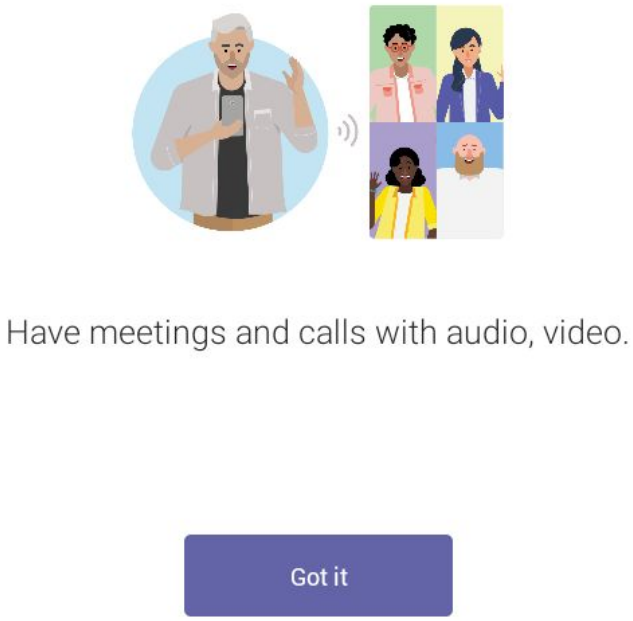
3. Enter your user credentials or select the desired account to sign in.





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**.



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.

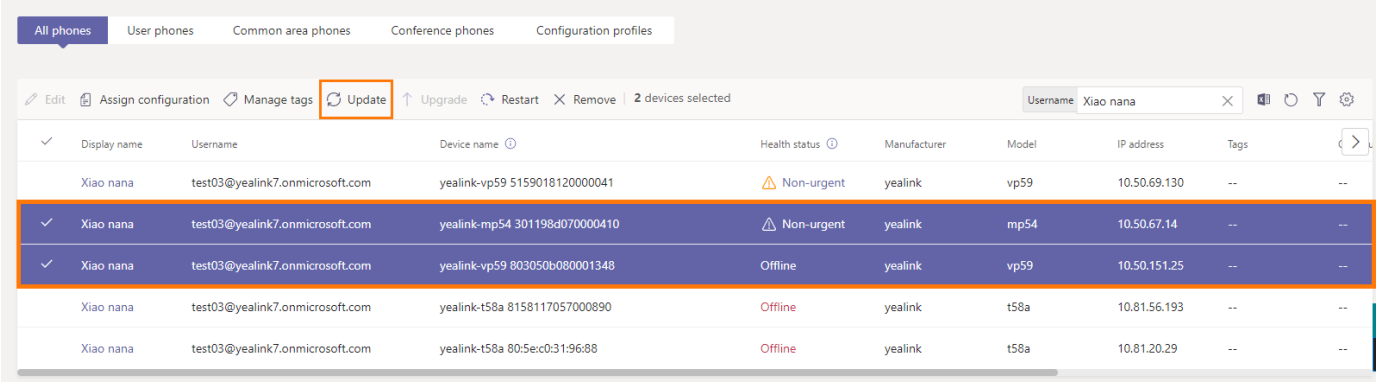
You can update the following for your device on the Teams admin center:

- 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

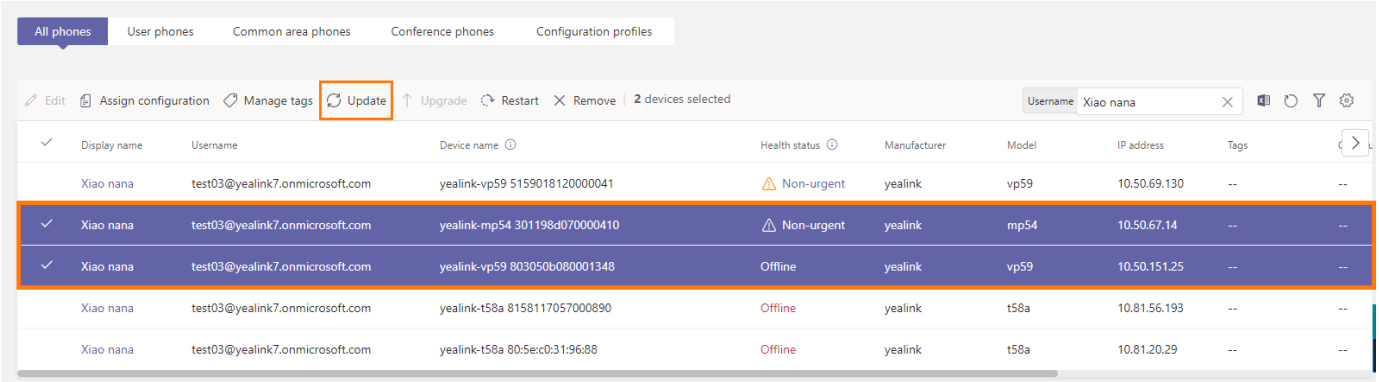
1. Sign in to the Microsoft Teams admin center as an admin.
2. Go to **Teams Devices** > **Phones**.
3. Select one or more devices and then select **Update**.



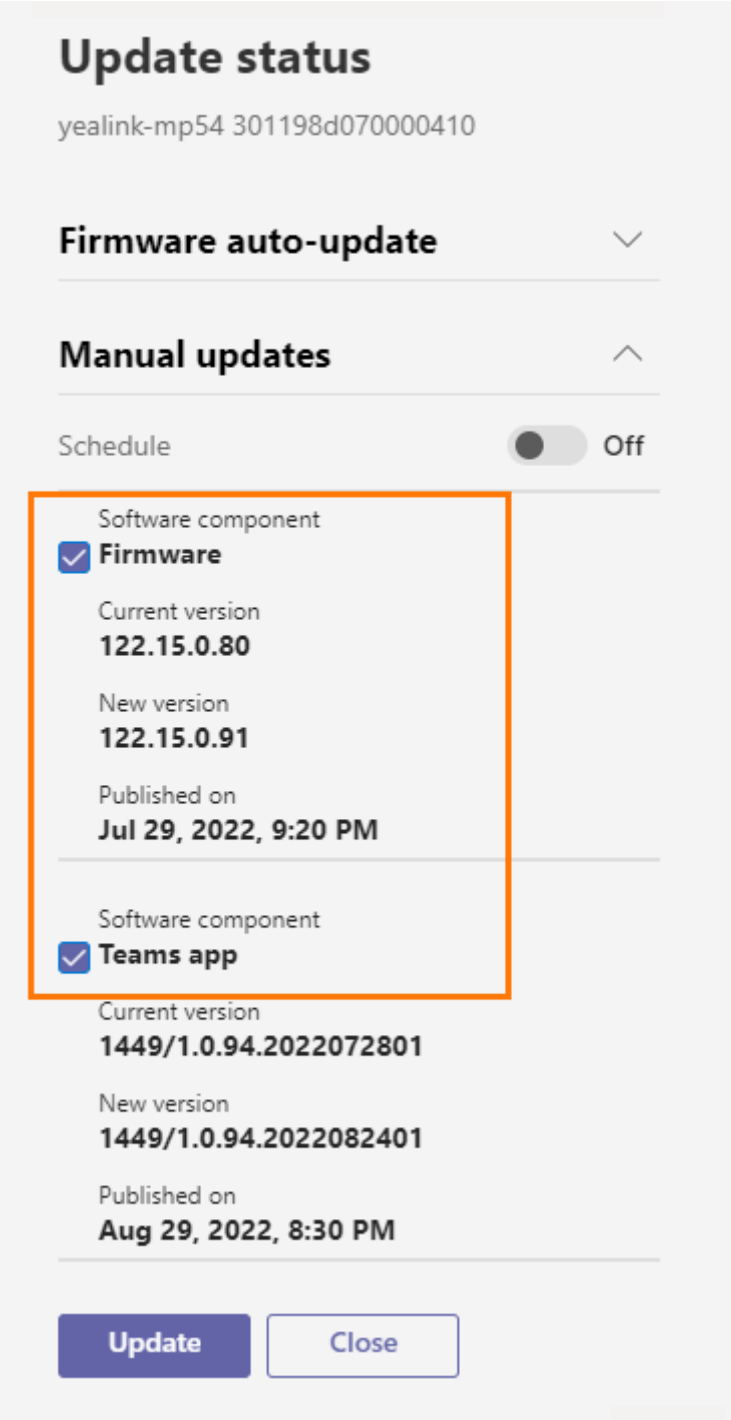
4. Select one of the following:
   - **As soon as available**: Second-newest device firmware update is applied on the first weekend after the latest update is released.
   - **Defer 30 days**: Second-newest device firmware update is applied 30 days after the latest update is released.
   - **Defer 90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

Manual Update

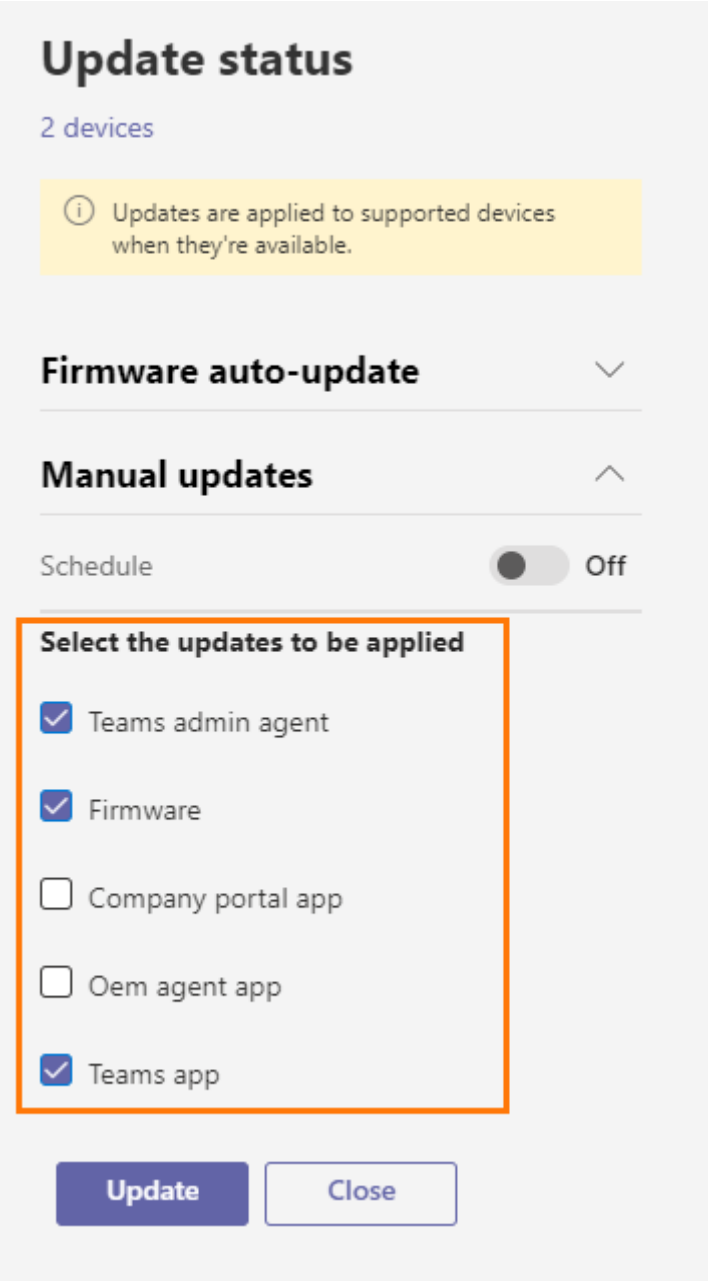
1. Sign in to the Microsoft Teams admin center as an admin.
2. Navigate **Teams Devices** > **Phones**.
3. Select one or more devices and select **Update**.



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:



- If you select multiple devices:



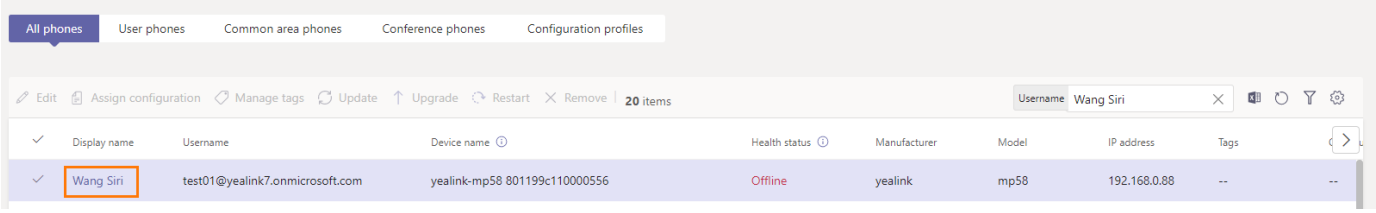
Download Device Logs

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

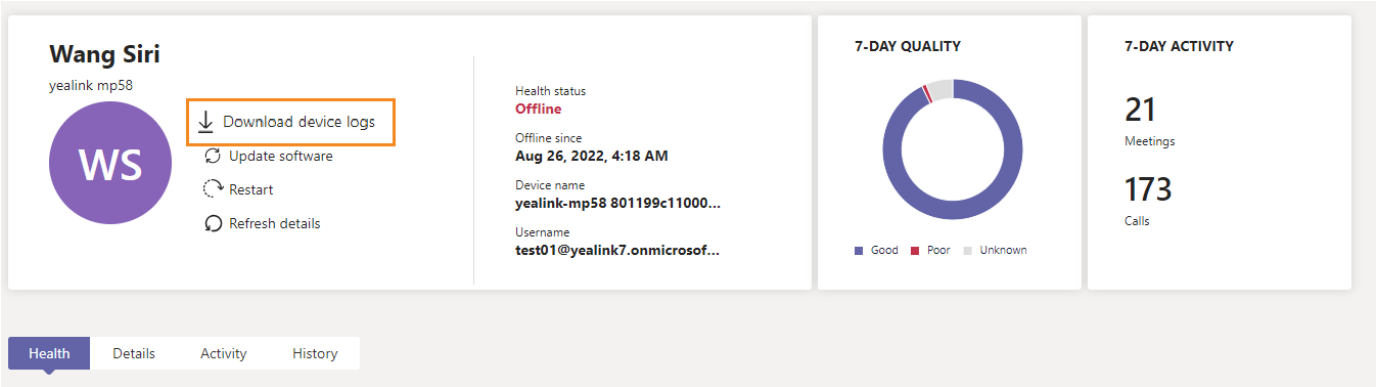
1. Sign in to the Microsoft Teams admin center as an admin.

2. Go to **Teams Devices** > **Phones**.

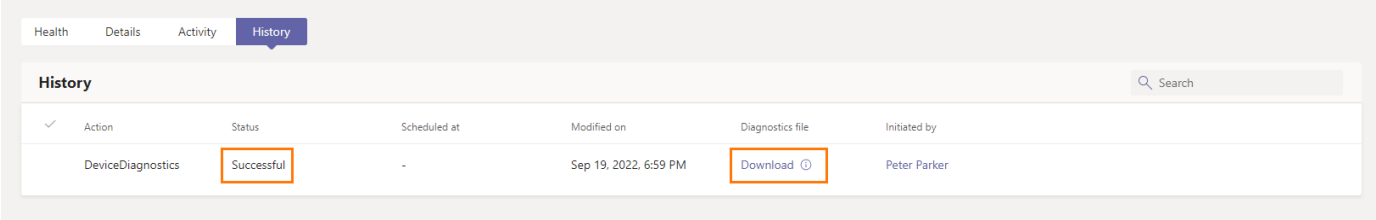
3. Click the display name of the device from which you want to download logs.



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".

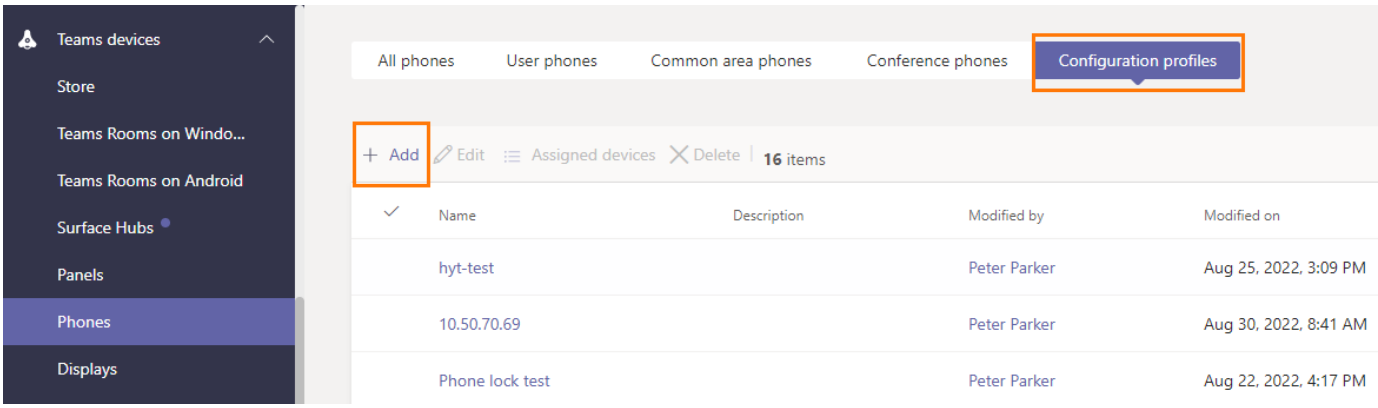


Use Configuration Files

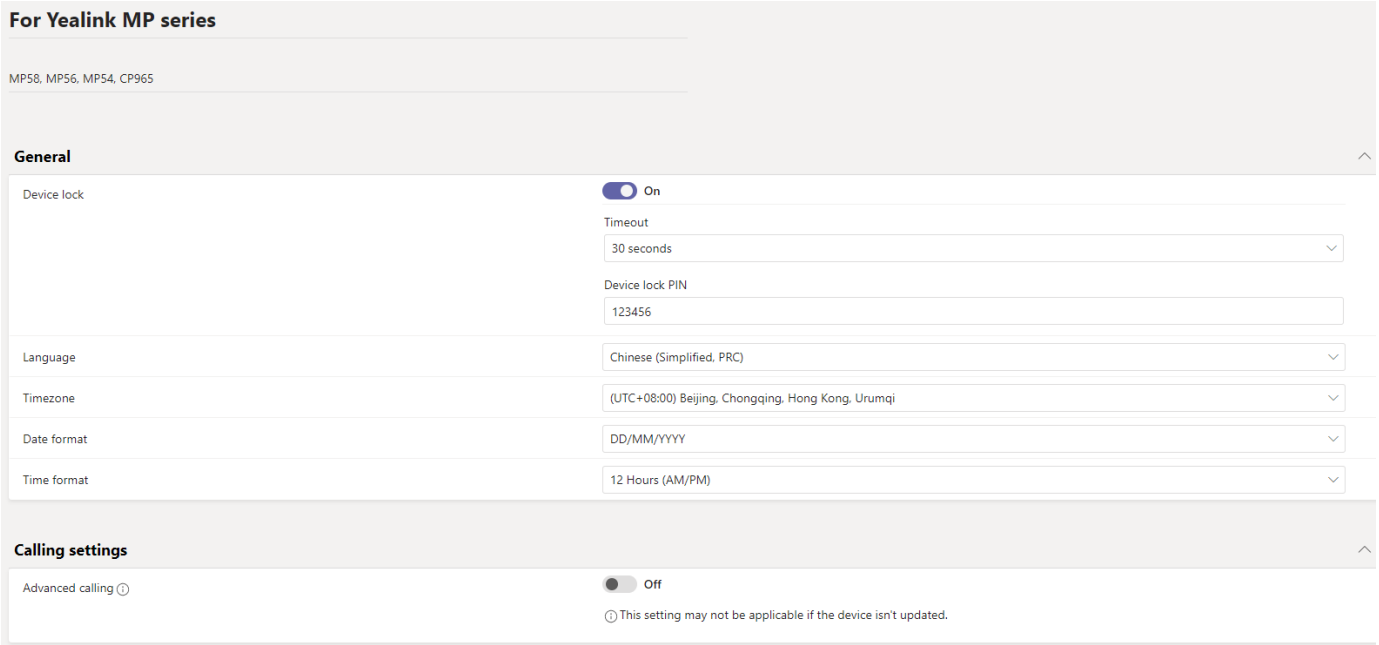
Use configuration profiles to manage settings and features for different Teams phones in your organization.

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**.



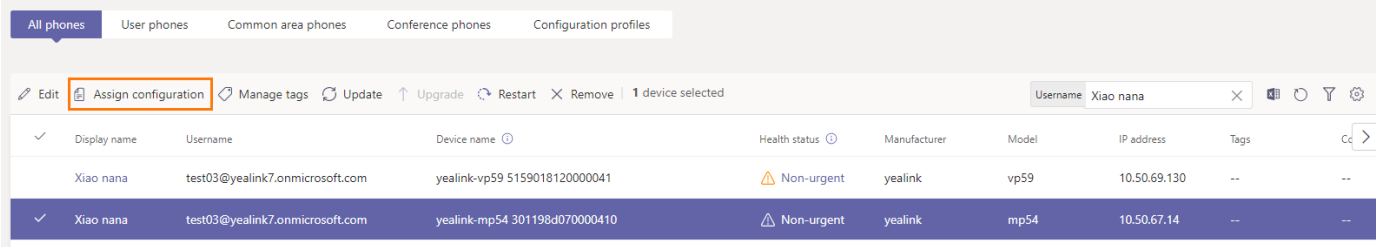
6. The newly created configuration profile is displayed in the list of profiles.

Assign Configuration File to Devices

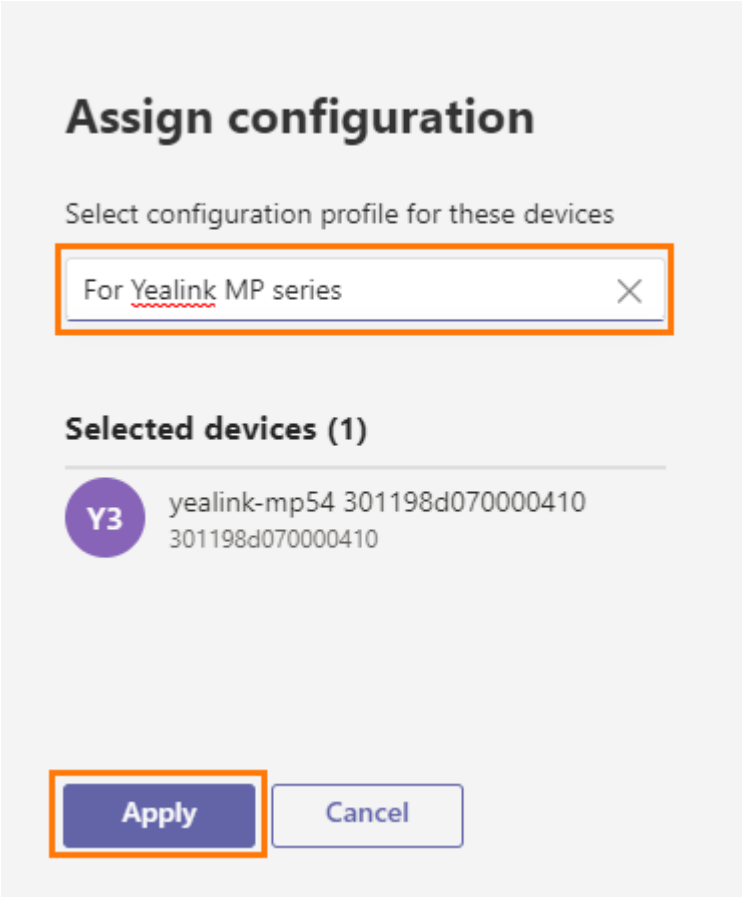
1. Sign in to the Microsoft Teams admin center as an admin.

2. Go to **Teams Devices** > **Phones**.

3. Select one or more devices and click **Assign configuration**.



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



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?

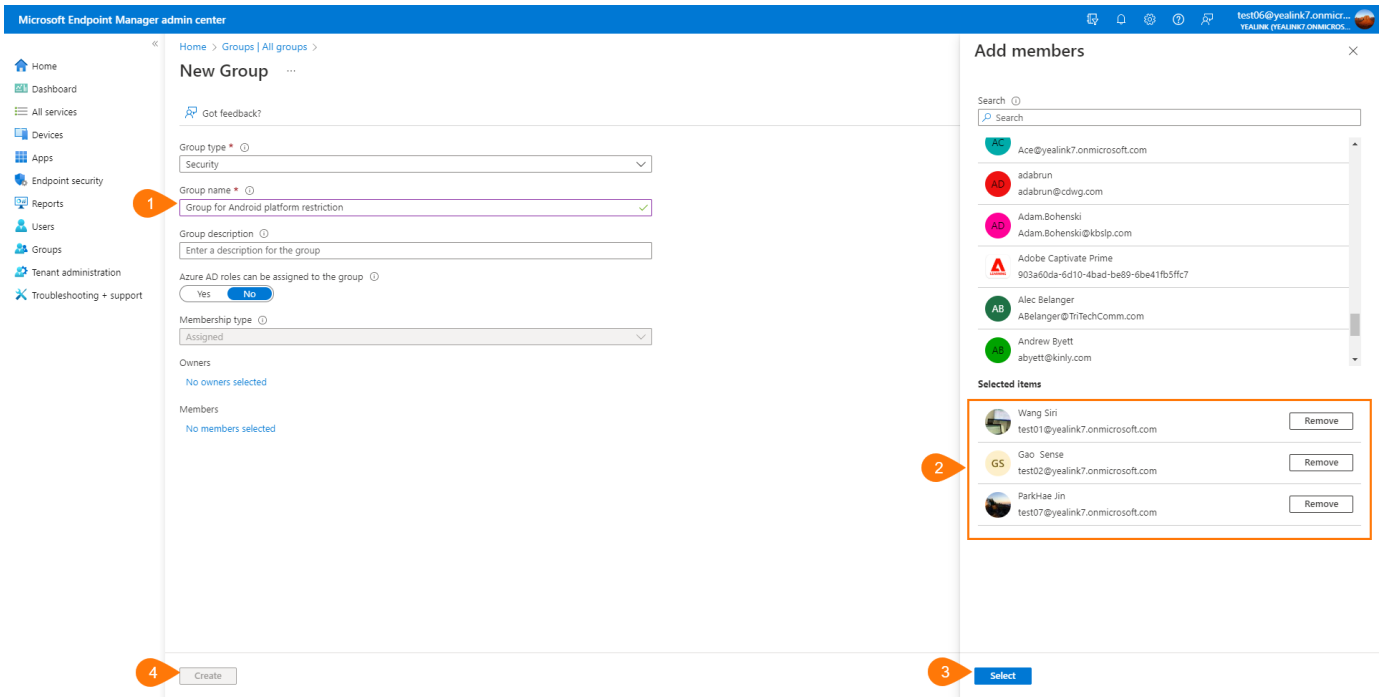
- Device Compliance: Tells you if your device is compliant or not.
- Conditional Access: Determines what to do with these devices depending on their compliant status.

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

Step 1 - Create a Group

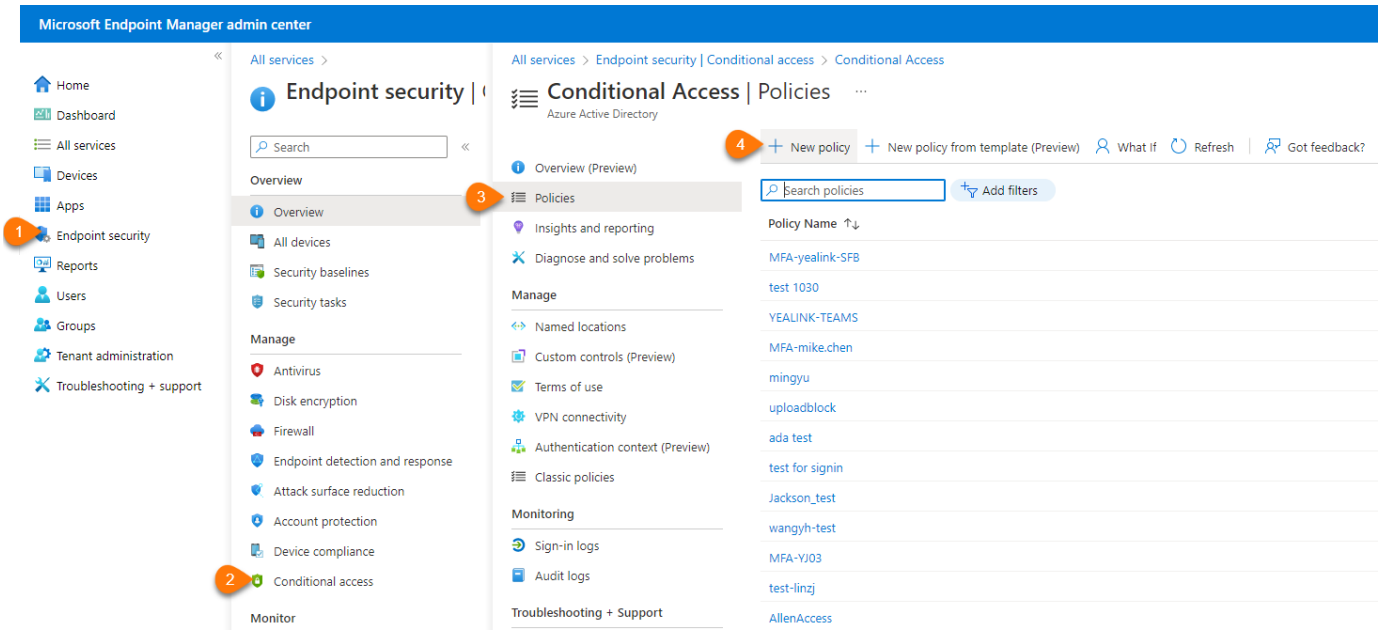
Skip this step if you already have a group that includes the user. Or you can add the user to the existing group.

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.

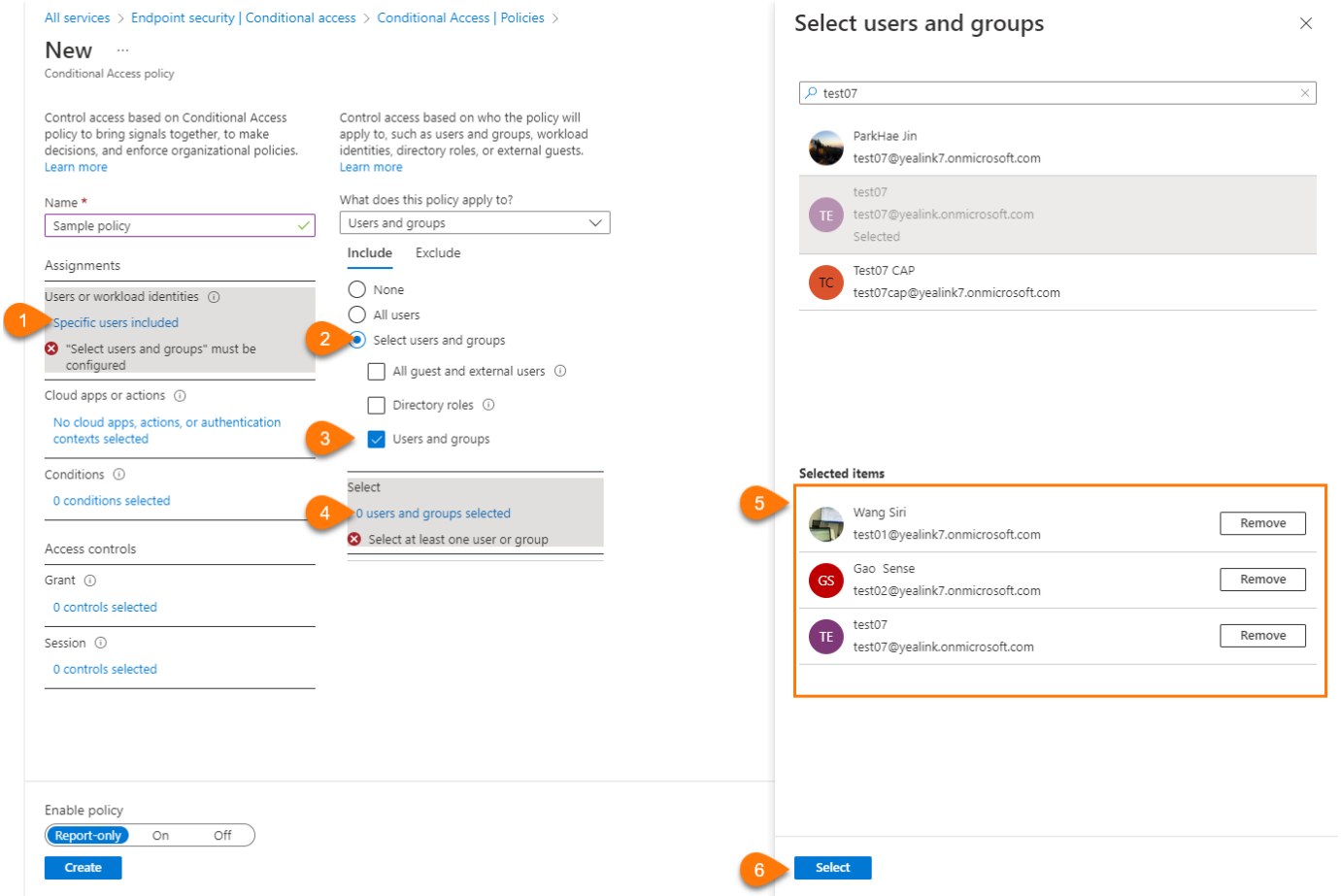


Step 2 - Set Conditional Access

1. Sign in to the Microsoft Endpoint Manager admin center as an admin.
2. Go to **Endpoint security** > **Condional access** > **Polices** > **New policy**.



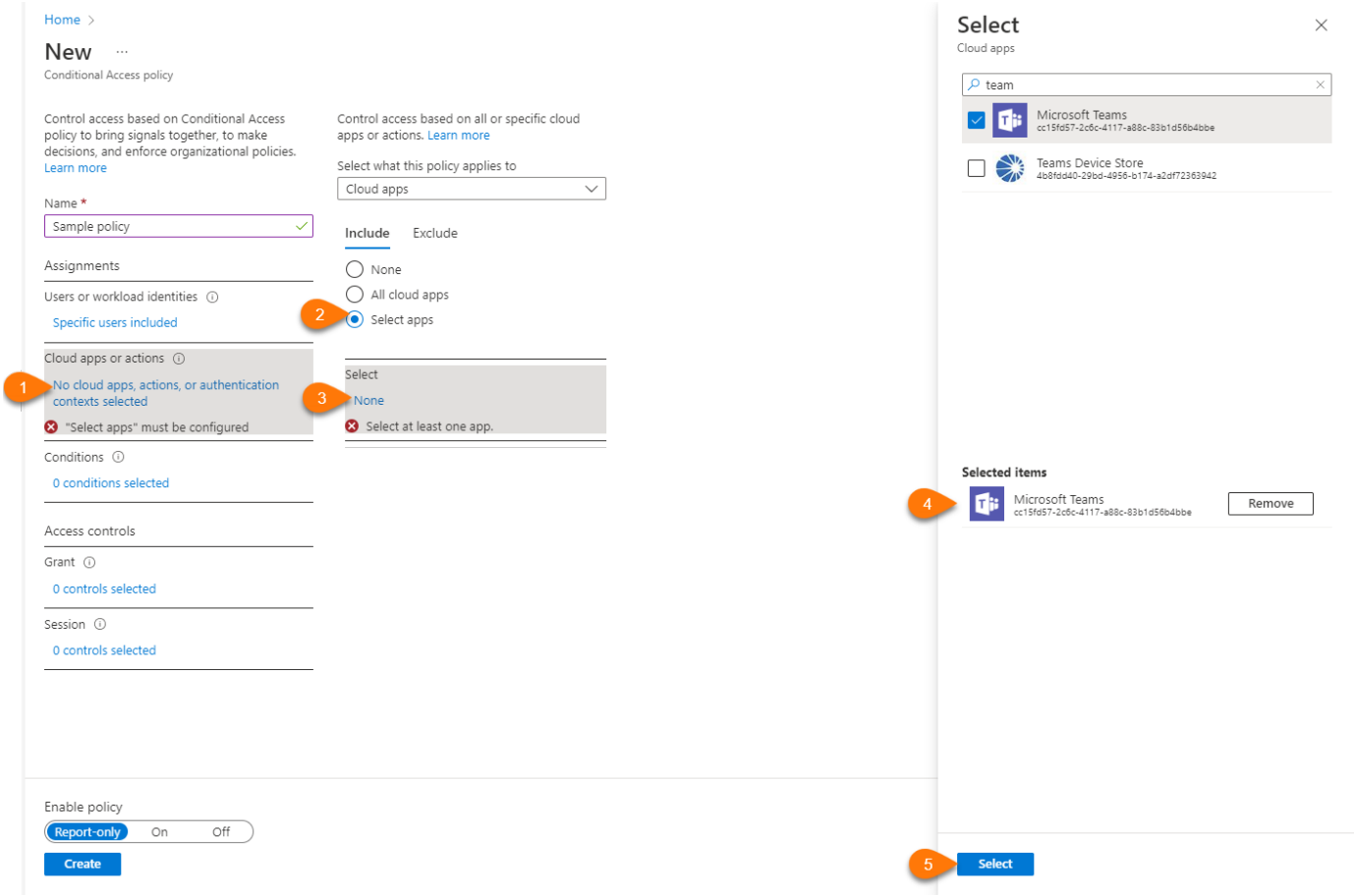
3. Enter the policy name.
4. Under the **Users or workload identities** field, select the users or groups to which the policy applies.
5. **NOTE**



- 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.

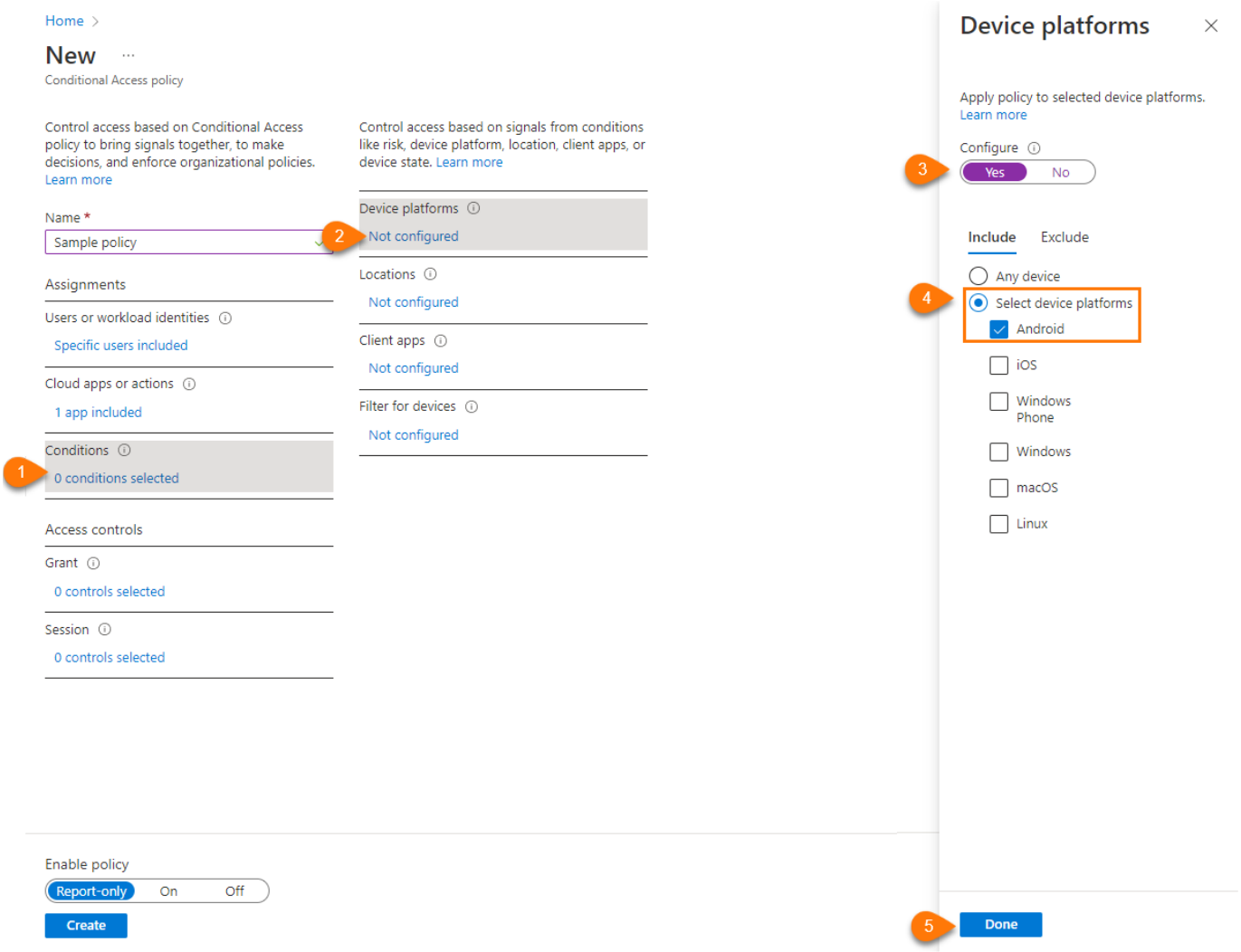
5. Under the **Cloud apps or actions** field, select the desired apps or actions to which this policy applies.



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

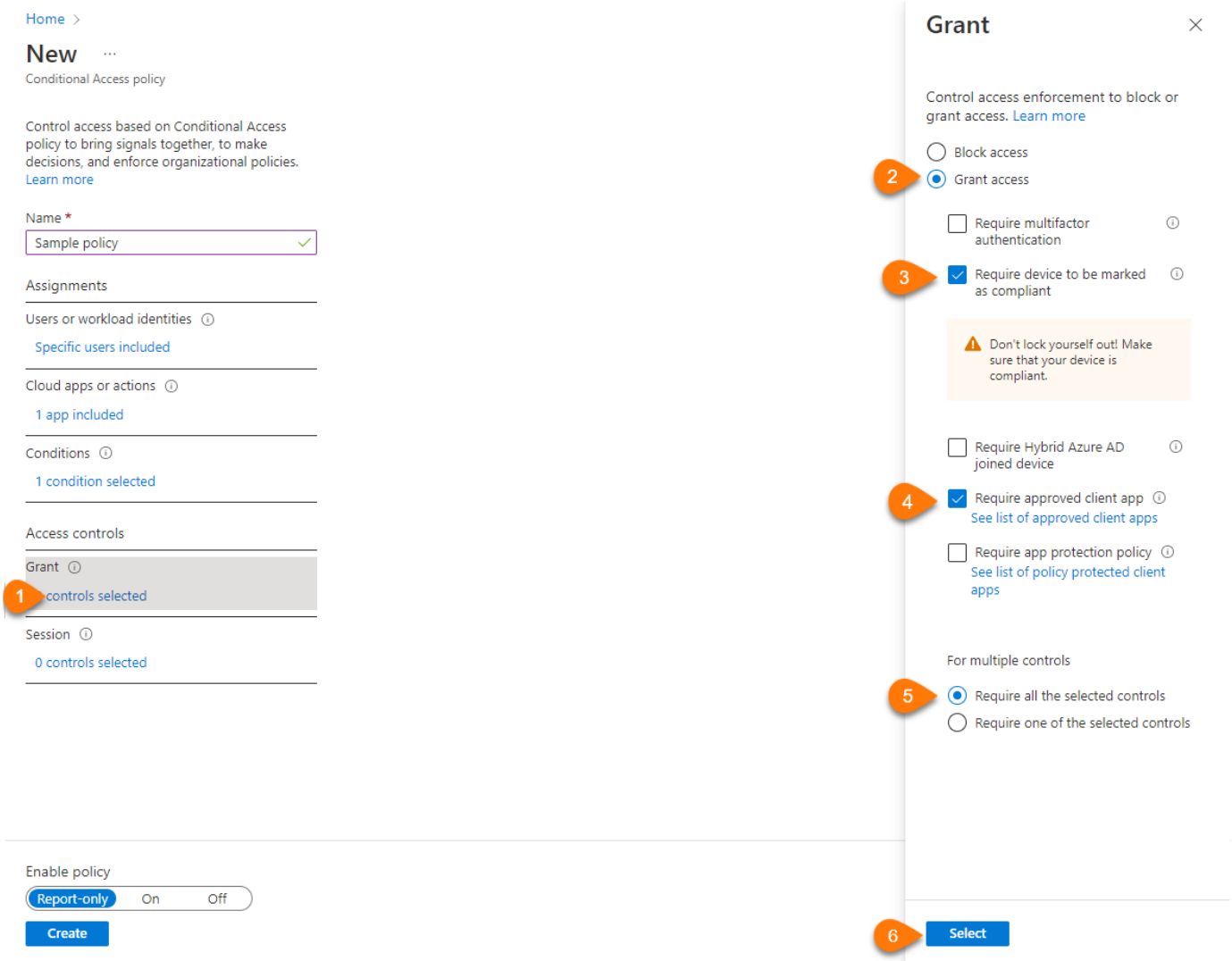
-

- 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.



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**.



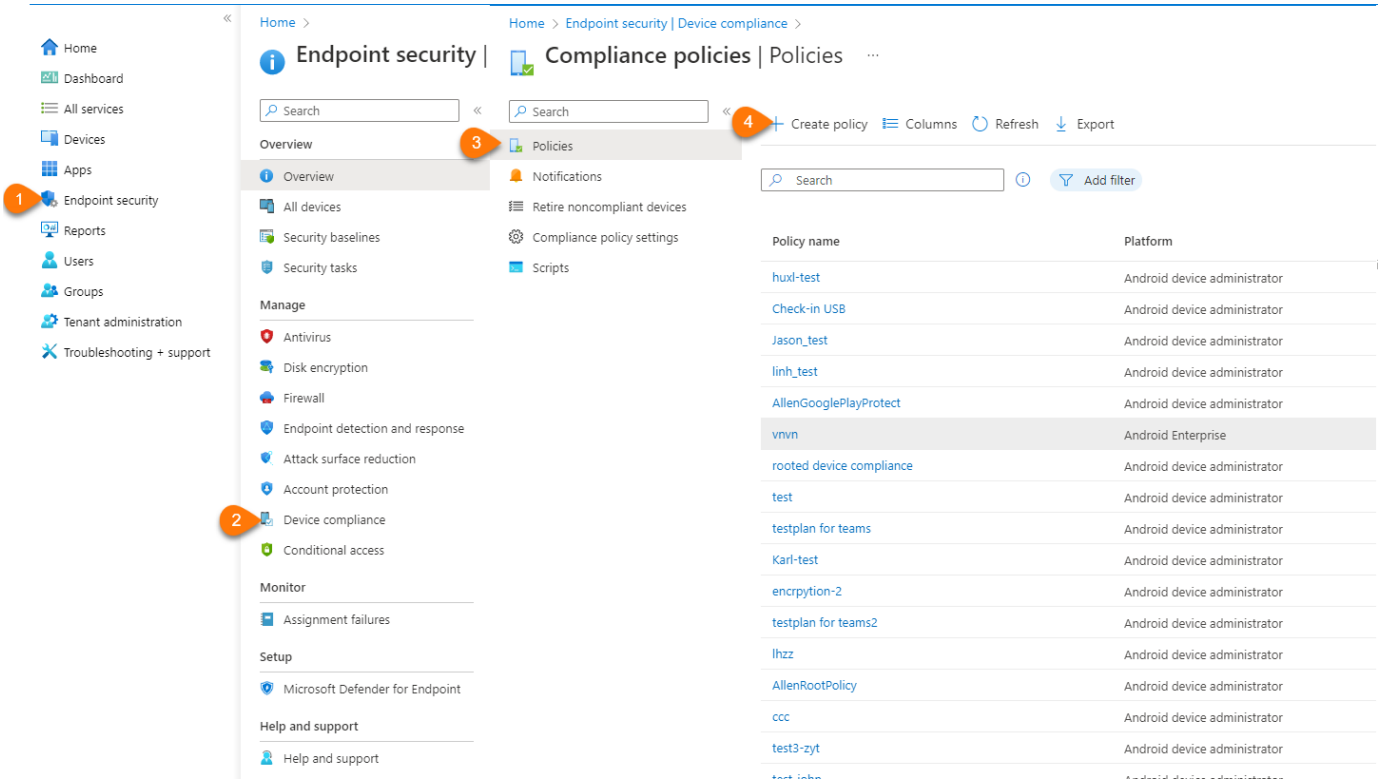
- You must select the check boxes of **Require device to be marked as compliant** and **Require approved client app**. Therefore, these two rules will be verified when the policy verifies Yealink Teams phones.
- If your company has other restrictions on the controls, for example MFA, you can select the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

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

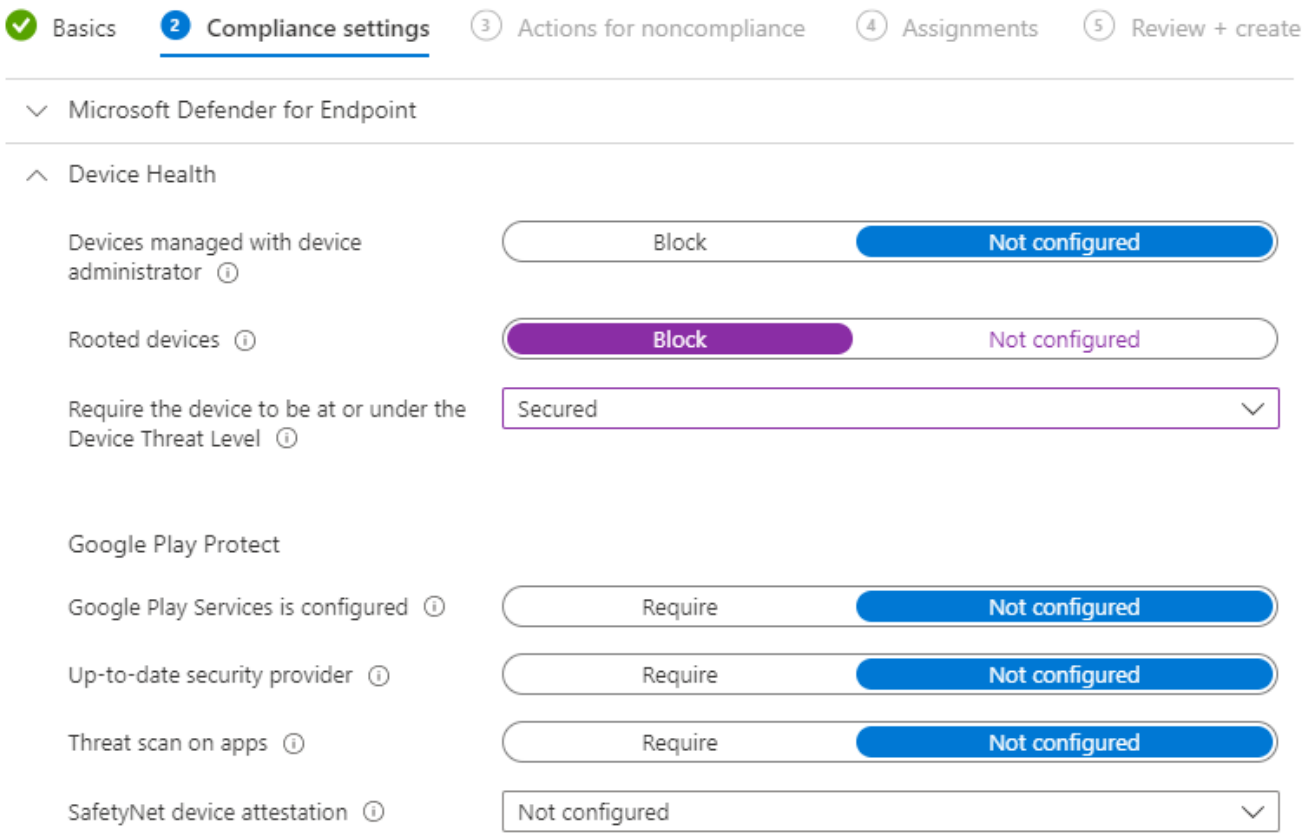
Step 3 - Set Device Compliance

1. Sign in to the Microsoft Endpoint Manager admin center as an admin.

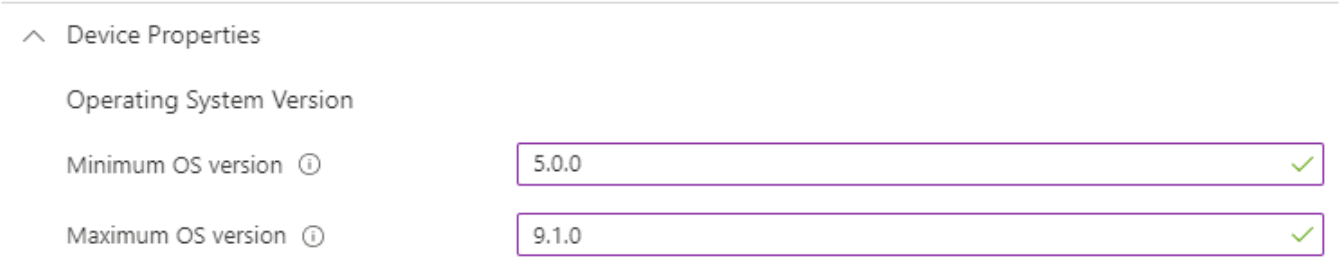
2. Go to **Endpoint security** > **Device compliance** > **Polices** > **Creat policy**.



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:



b. Set the operating system version:



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

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

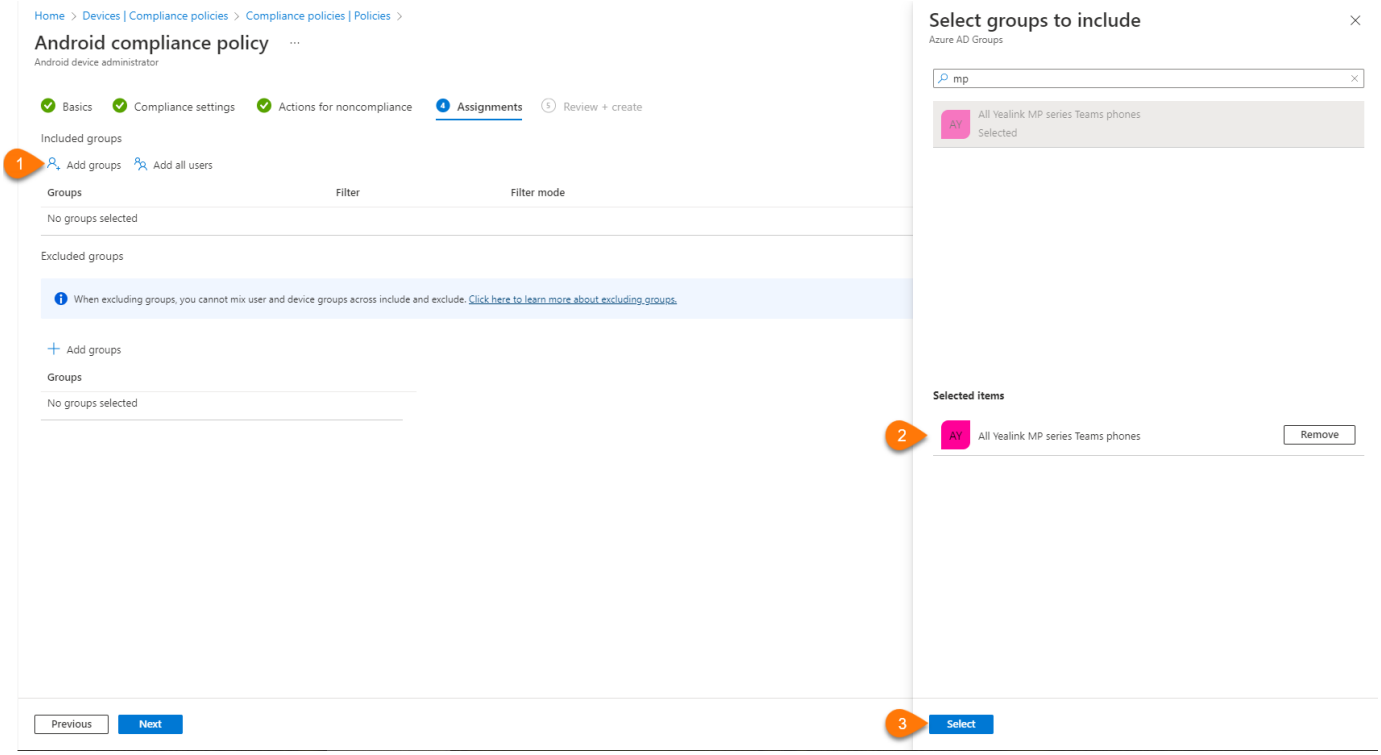
Android 10 and later

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**.

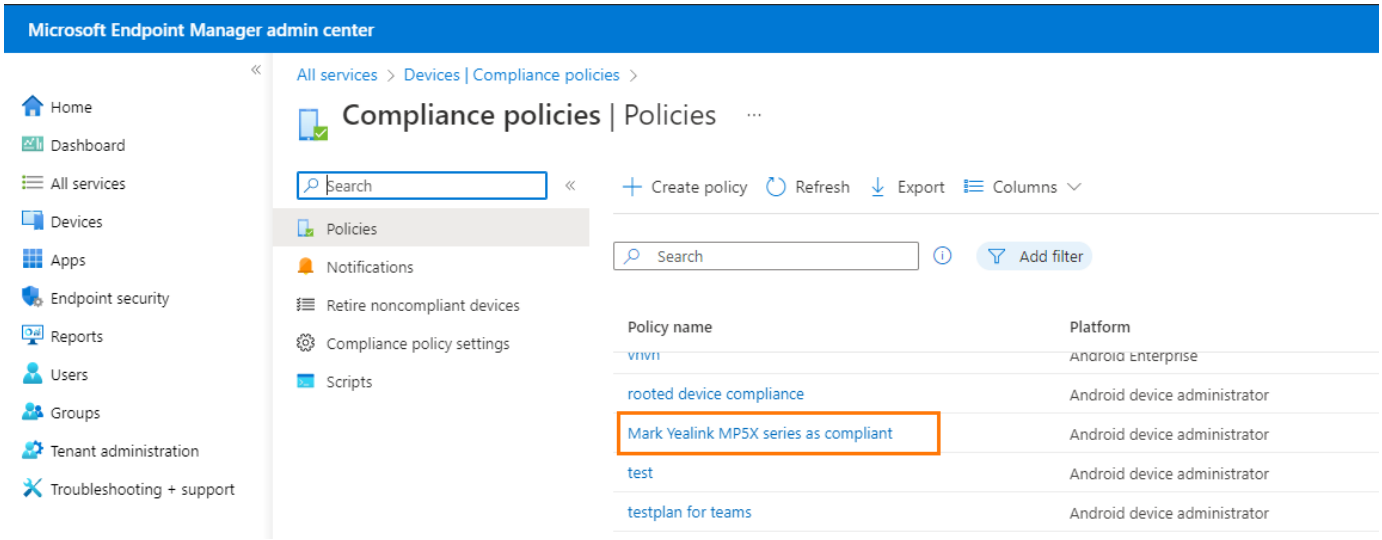
Check the Status of the Compliance Policy

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

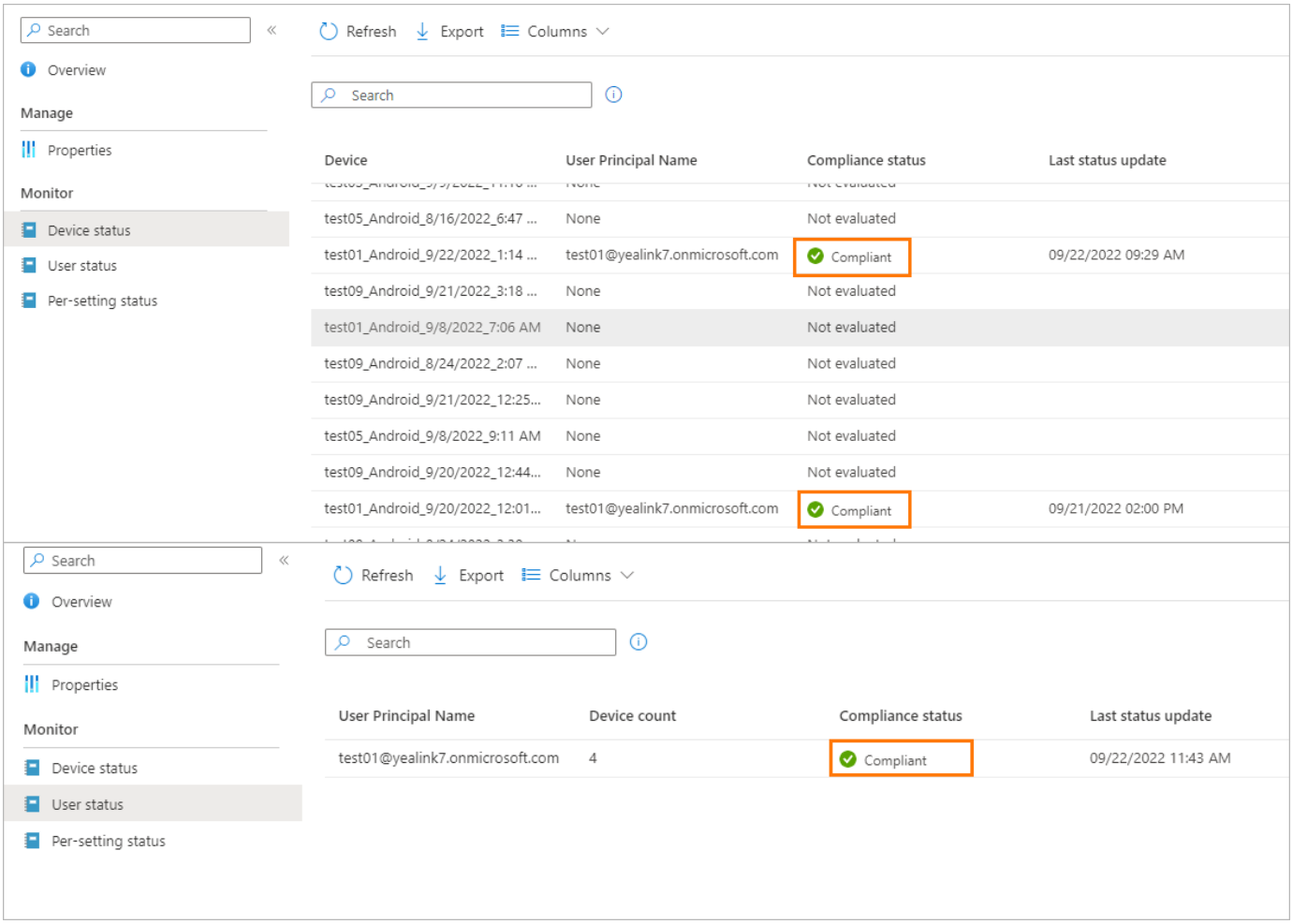
1. Sign in to the Microsoft Endpoint Manager admin center as an admin.

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.

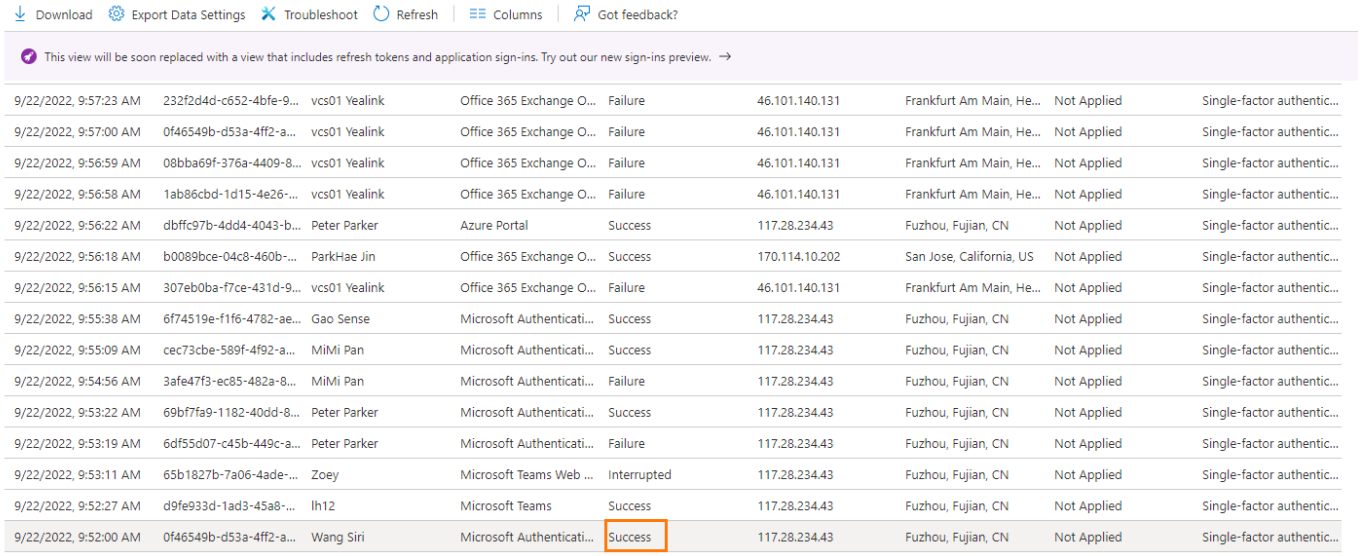


Check the Sign-In Logs

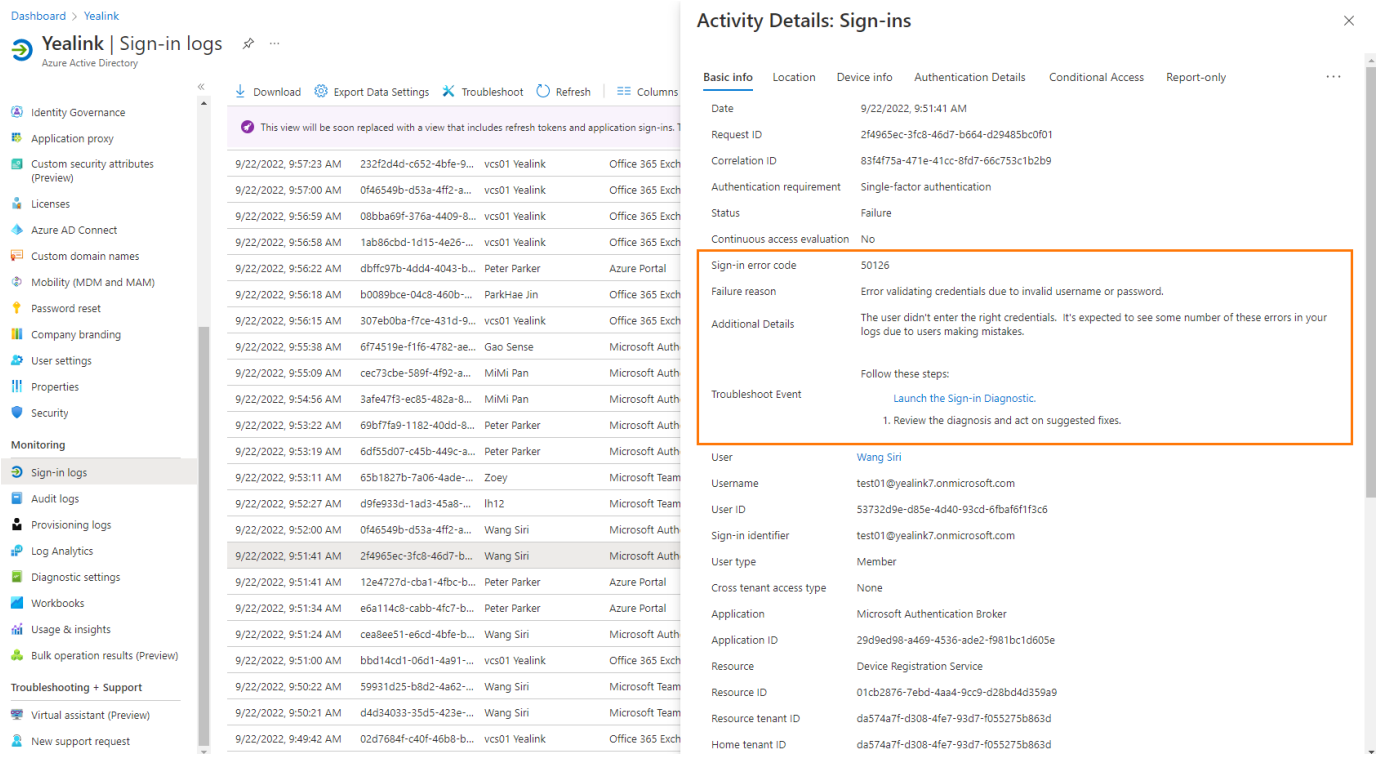
After you apply your policy, you can see the device sign-in status.

1. Sign in to the Azure Active Directory admin center as an admin.

2. Go to **Azure Active Directory** > **Monitoring** > **Sign-in logs**.



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.



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