CHAPTER 4

Teams Audio Conferencing and Phone System Management

Balu N Igala*, Vijay Ireddy
[a] Tracy, CA, USA

Microsoft Teams provides different capabilities, such as persistent chat, audio and video calls, conferences (dial-in and client join), and phone systems (inbound/outbound PSTN calls). So far, you have learned how Teams features work, how the components interact, and management aspects. This chapter covers Teams conference management, including audio conferencing (dial-in), Teams Webinars, Teams Premium, and VoIP for internal and external attendees. It also covers Teams Phone System management, including Teams Direct Routing, Operator Connect, Calling Plans, Teams Phone Mobile, E911, and voice routing policies.

The Microsoft Teams Phone System is a cloud-based phone system with advanced features for call control and PBX capabilities. It replaces on-premises PBX systems and provides the following functionalities:

- **Call control:** Allows users to make, receive, and transfer calls to and from landlines and mobile phones on the public switched telephone network (PSTN) right from Teams.
- **Voicemail:** Offers integrated voicemail services with transcription features.
- **Call queues:** Directs incoming calls to the next available attendant or distributes them to a group.

B. N. Ilag et al., *Understanding Microsoft Teams Administration*,
https://doi.org/10.1007/979-8-8688-0014-6_4

- **Auto attendants:** Offers automated systems that answer calls, ask questions, and route the call based on the answers.
- **Call park:** Allows users to put a call on hold and then retrieve the call from another phone.
- **Emergency calling:** Offers support for dialing emergency services.
- **E9-1-1 dialing:** Offers enhanced emergency calling that provides the user's callback number and location to the emergency responders.
- **Caller ID:** Display and control of the caller's phone number.
- **Direct Routing:** Connects Teams to your existing telephony provider to allow the routing of calls via a direct path.
- **Interoperability:** Integrates with third-party systems, such as analog devices and on-premises call centers.

Audio conferencing in Microsoft Teams allows users in a Teams meeting to join over a regular phone line if they're not on a device with Teams installed or if their Internet connection is poor. It provides the following:

- **Dial-in numbers:** It offers a range of numbers, local to multiple countries, that participants can dial to join Teams meetings.
- **Dial-out:** Participants in a meeting can add someone by dialing their number.
- **PIN-protected meetings:** For security, some meetings require a PIN to join via audio conferencing.
- **Dynamic conference IDs:** This provides each meeting with a unique ID, reducing the chance of overlapping or unauthorized access.

After this chapter, you will be able to do the following tasks:

- Plan and manage Teams conferences.
- Use Teams Webinars and Teams Premium
- Plan a Teams Phone System planning.
- Configure and manage Teams Direct Routing
- Configure and manage Microsoft Calling Plan

- Configure and manage Operator Connect
- Configure and manage Teams Phone Mobile
- Configure and manage the call queue and Auto Attendant
- Configure and manage the Teams emergency service
- Manage a phone number and voice routing policy
- Manage a voice routing policy (dial plan, voice routing policy, and PSTN usage)

Planning and Managing Teams Conferences

Let's talk about conferences.

Microsoft Teams Conferences

This section explains how you can collaborate using Teams. You can easily prepare, organize, and follow up by using before and after meeting experiences, such as collaborating before the meeting using chat and Meet Now. Users can be more involved and productive by sharing content from their desktop (Mac and Windows) or mobile devices and adding video to meetings for face-to-face video interactions. Teams meetings work fine with great audio and video quality and reliability when joining from desktops (Windows and Mac), mobile devices, phones, or rooms.

Users can also invite external attendees to join Teams meetings through a web browser with any plug-in. Why do Teams meetings work fine with internal and external participants? The main reason is that Teams is built on a base of the next-generation Skype infrastructure, media services, and Office 365 services, including Exchange, SharePoint, Microsoft Stream, Microsoft Artificial Intelligence service, and Cortana.

Teams also provide an extra layer of engagement before, during, and after meetings. For example, before a meeting, you can have a background conversation in Teams and prepare and discuss content, set up meeting options to manage meeting permissions and settings, and then schedule a Teams meeting. Throughout a meeting, you can use face-to-face video, follow the action, share content, record the session with transcription, use applications integrated with Teams meetings, use live captions, and quickly join

from a Teams room. After a meeting, you can play back the meeting with transcription, share notes, and have a post-meeting chat for collaboration. This makes Teams meetings uniquely reliable and reduces quality complaints drastically.

First, you must understand how to use Teams meetings in your organization effectively.

Organizing Teams Meetings Efficiently

Log in to the Teams client and click Calendar. You will see the day's upcoming meetings when it switches to meeting view. You can switch the calendar to daily, weekly, or monthly views. Figure 4-1 shows the daily and weekly views.

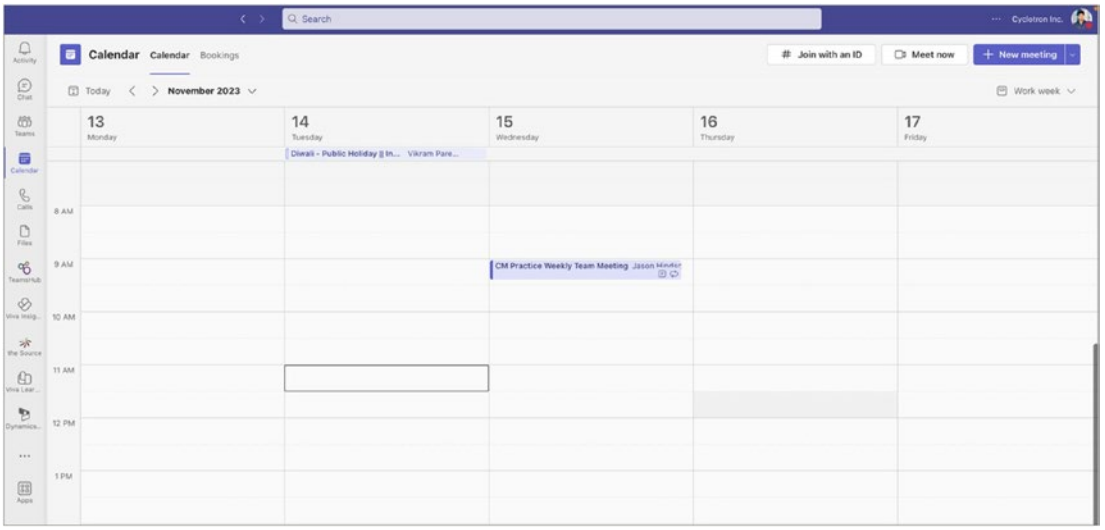

Figure 4-1. *Calendar daily and weekly views*

To schedule a meeting, click New Meeting to open the meeting page.

You can enter a title, location, and start and end times on the meeting schedule page. You can indicate if it is recurring or a one-time meeting and use scheduling assistance to see team members' free/busy information. Here you specify the time zone in which the meeting will be held. You can also select a channel to meet in so all members get invited, or you can choose individual people or a distribution list for meetings. You can add an agenda for the meeting, and other participants can review and edit it before joining the meeting. Once you have added the desired information, click Save to schedule the meeting, as shown in Figure 4-2.

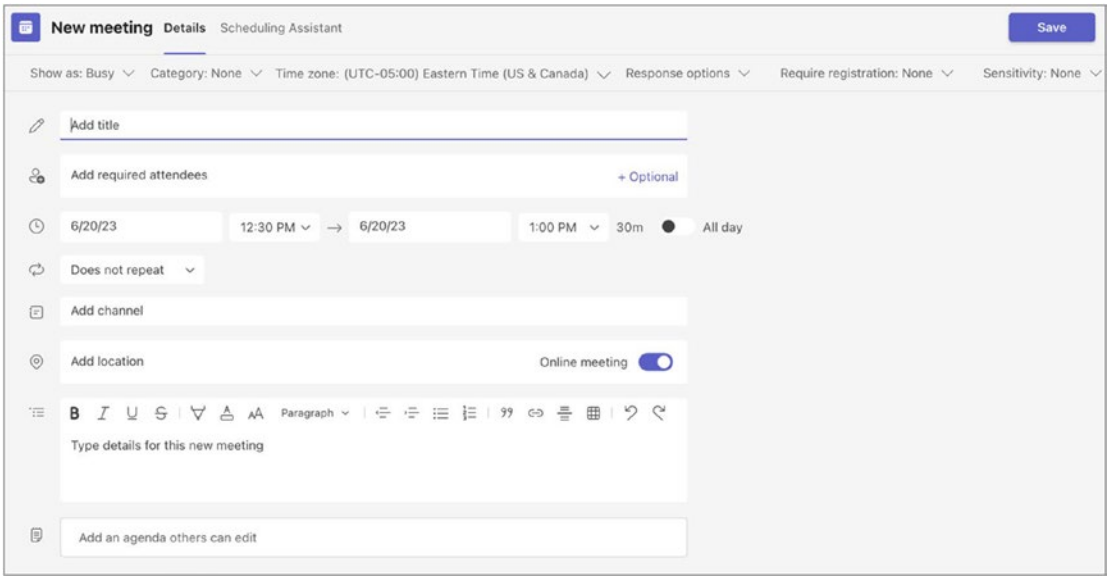

Figure 4-2. *Setting up a new meeting*

At this point, the meeting has been created and shown on the calendar. You can see all the details about the meeting: title, time, and who has scheduled it. You can also see the status of the attendees who have accepted the meeting. This information is not only for the organizer but all attendees.

Once the meeting is scheduled, you can start a chat with all participants before the meeting, where you can discuss the agenda or share any files that attendees should review before the meeting. You can join the meeting in the same conversation by clicking Join, as shown in Figure 4-3.

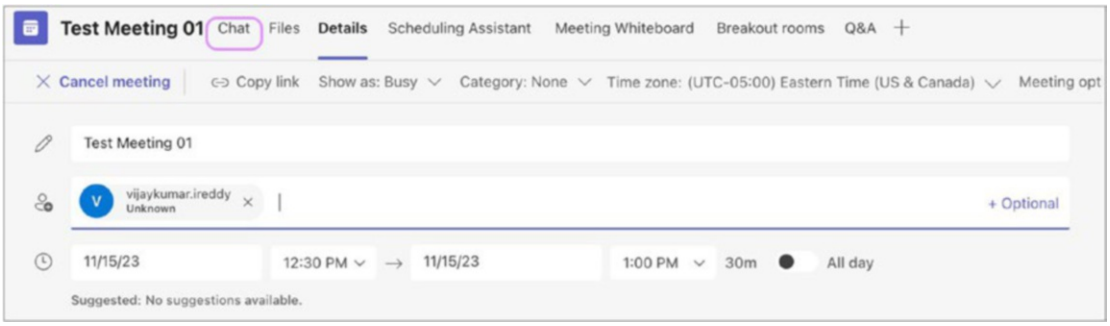

Figure 4-3. *Chat with participants option*

At the top of the screen are several tabs such as Chat, Files, Breakout rooms, Apps, Meeting Whiteboard, and Q&A. Organizers and participants can use these tabs to share files, chat with others, prepare for Q&A, create breakout rooms, and set up polls before the meeting. Meeting organizers can adjust the meeting options before and during the meeting. By default, meeting options include the default organization settings. Depending on the meeting requirements, organizers can change these settings. Please note that this setting will affect only the meeting occurrence/meeting series. To edit the meeting options as an organizer, click the meeting options. Upon clicking, a new window will appear containing the information specified in Figure 4-4.

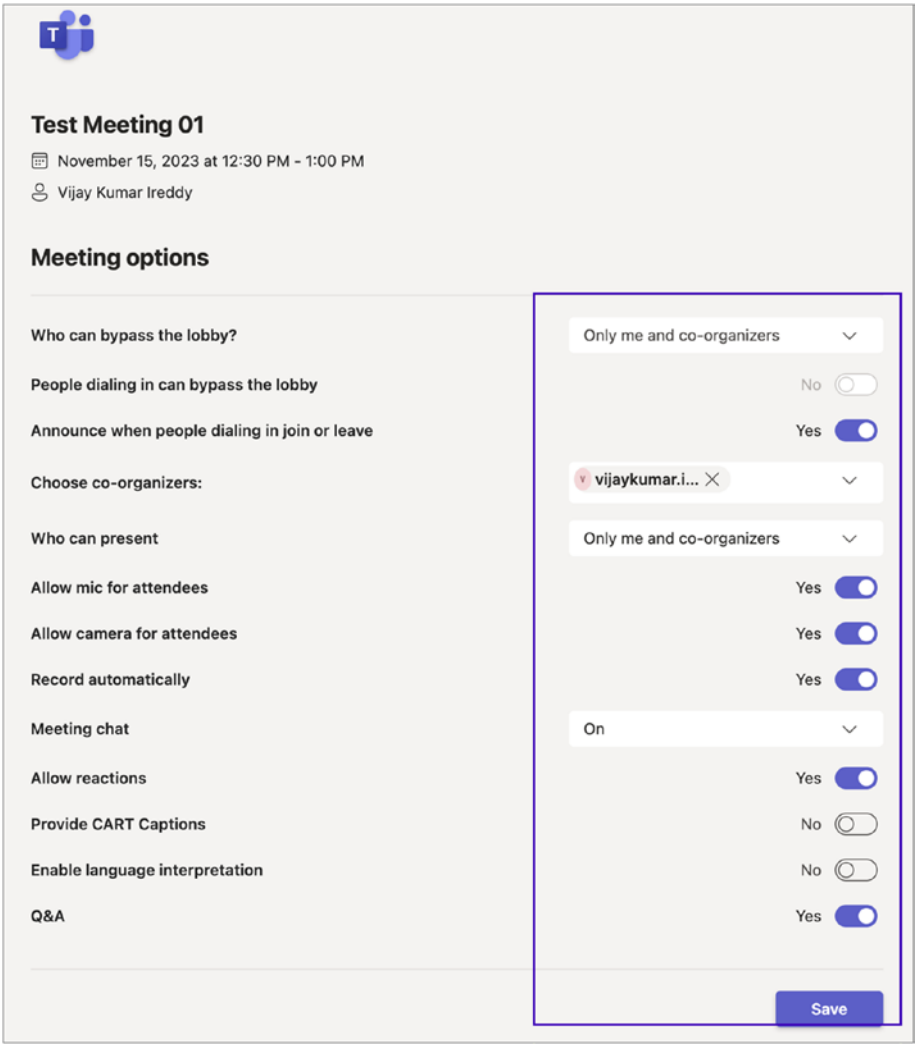

Figure 4-4. *Adjusting the meeting options*

To meet specific needs, organizers can adjust meeting options. For example, in the given meeting example, the organizer wants to include co-organizers, keep all participants in the lobby until allowed into the meeting, and only allow organizers or co-organizers to admit the participants, and the meeting recording is turned on automatically.

You can join the meeting by clicking Join in the Teams client calendar or Outlook Calendar. You can turn on video, view a preview, control audio, and change the audio or video device. Figure 4-5 illustrates joining my test meeting.

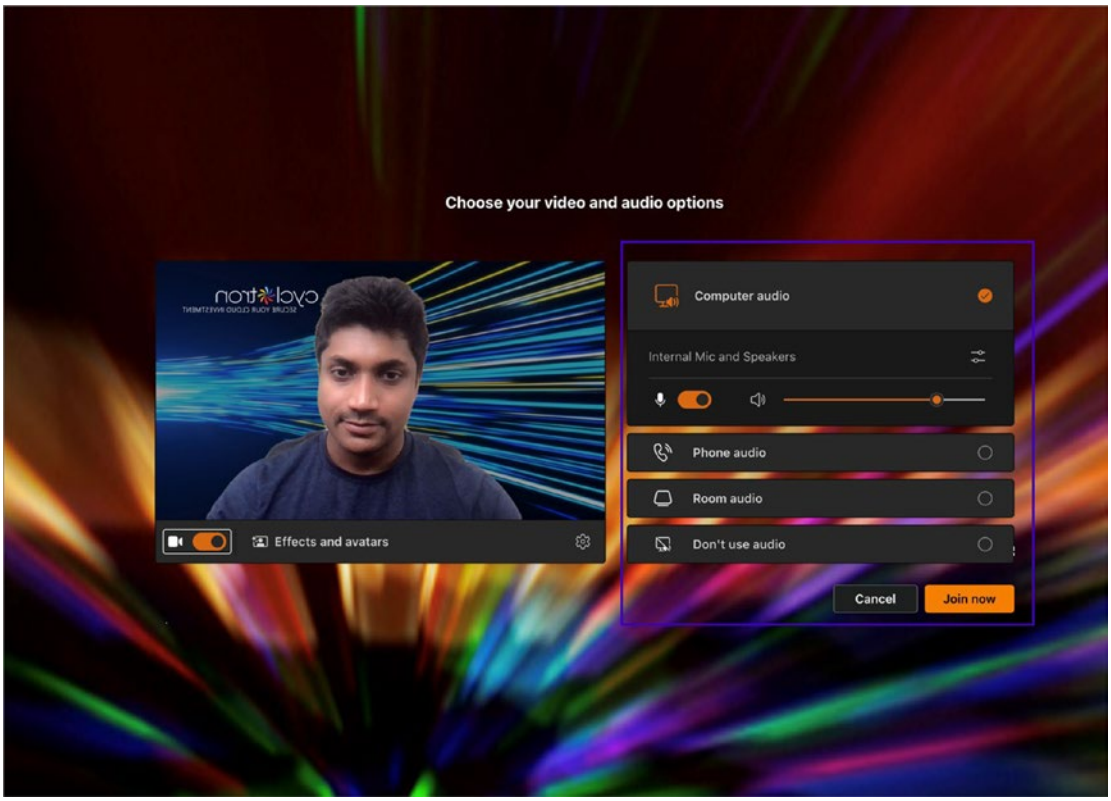

Figure 4-5. *Joining a meeting*

When joining audio in Teams, you have several options to choose from. You can use your computer's default audio setting or select your preferred microphone and speakers. You can also make a Teams call to your phone by entering your phone number (note that this feature requires an Audio Conference License). If there are Teams rooms or certified devices nearby, they will be detected automatically. Lastly, you have the choice not to use any audio at all.

To enable video in your meeting, turn on the video icon and select the Effects and Avatars option. Please note that avatars are currently in public preview. Within the effects options, you can choose from default background effects or upload your custom images. Additionally, Teams offers video enhancement features such as soft focus, brightness adjustment, and mirror image to improve the video quality in low-lighting scenarios.

To use an avatar during your Teams meeting, create one using the Avatar app in the Teams app store. Then, when joining the video, select the Avatar option instead of your video. It's important to note that you can choose only one, either your avatar or your video but not both. For a visual example, refer to Figure 4-6, which shows joining a meeting using an avatar.

Figure 4-6. *Joining a meeting using an avatar*

Tip Teams settings don't have the option to set up default devices to join audio and video for your meetings. However, Teams AI is intuitive and can recognize your preferred method of joining meetings. For instance, if you previously connected multiple meetings via an avatar and room audio, it will suggest using the same way for future meetings.

Once you are ready to join the meeting, click Join to enter the meeting. Once in the meeting, you can use several controls, including turning your camera on or off, muting or unmuting your microphone, sharing a presentation and desktop, and other things. In the upper-right corner, other items manage participants and access chat. Figure 4-7 shows these meeting controls.

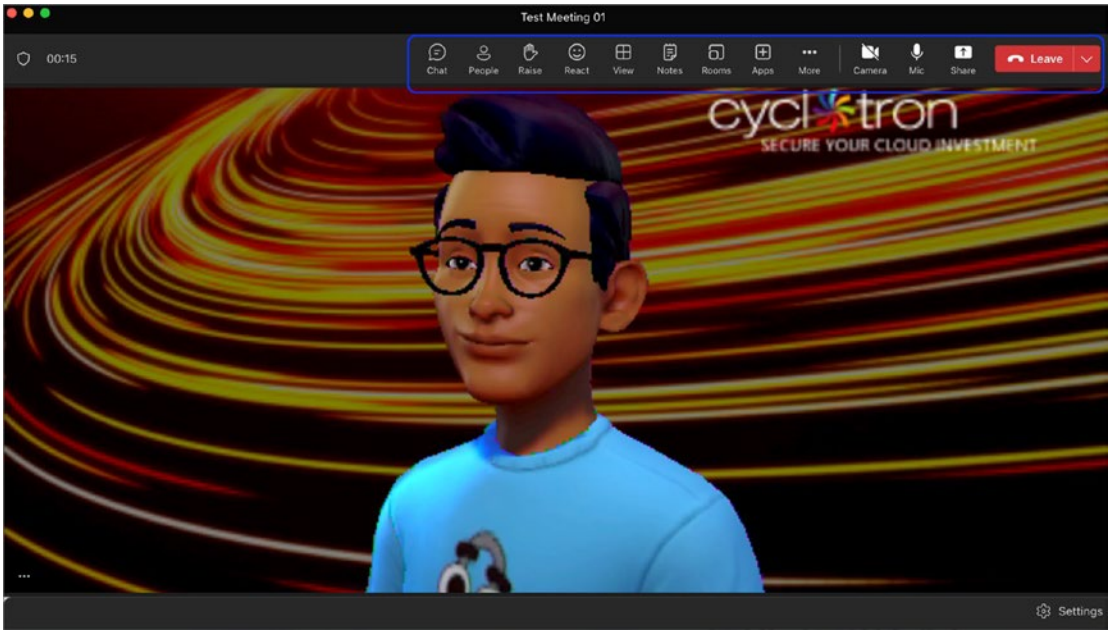

Figure 4-7. *Meeting controls*

During the meeting, you will see several meeting controls. You can use the sharing options to share your screen, window, PowerPoint Live, Excel Live, and whiteboard. Each sharing method has its benefits. If you want to display your entire screen and other desktop activities, choose "share your screen," as it enables seamless sharing of multiple windows. If you share only a single application, consider sharing via "window." Teams meetings offer rich collaboration capabilities through PowerPoint and Excel presentations. PowerPoint Live and Excel Live allow participants to move through the presentation at their own pace. Finally, the whiteboard feature and annotation features enable real-time collaboration among participants.

After a meeting, you can access a recording, any shared presentation files, and a transcript of all the discussions. The recording is stored in the OneDrive of the person who started the recording and can be viewed by all internal meeting participants in Teams. Please note that the recording is available only if the meeting was recorded.

There are two broad meeting types: channel meetings and private meetings. Channel meetings exist within a channel, making them visible to all channel members. Pre- and post-meeting features stay within the channel. You can add nonmembers of a team to the channel meetings, but they will not have access to chat because it is visible to channel members only. A channel meeting can be scheduled from the Teams client calendar view or an existing channel conversation. You can also start an ad hoc meeting from a current channel conversation instead of through a reply. Just create an ad hoc meeting and start.

Private meetings can start from an existing chat conversation with chat participants. They are visible to invited people only, and the pre-meeting and post-meeting experiences are accessible via chat. You can schedule a private meeting with the Teams client or the Outlook Teams add-In.

Teams Meeting Attendee Types

Teams meetings have different attendee types. Depending on your attendee type, you will have different information and options available during meetings.

- **Internal users:** These are organization users with an account in the same tenant organization. For example, my tenant account is `xyz@cyclotron.com`.
- **Guest users:** Guest users are invited to one or many teams in your organization. Guest users will have guest accounts in the same tenant.
- **Federated users:** Federated users are users of a different organization (partner or vendor organization) with federation configured between both organizations that use Teams. For example, `cyclotron.com` and `microsoft.com` are two different organizations that are federated with each other.
- **Anonymous users:** Anonymous users have no account or an account in a tenant without a federation. Usually these types of users join Teams meetings via a web client.

Remember, that attendee type is determined at join time, and you cannot change that. Suppose a federated user forgets to sign in; they will be considered anonymous when joining Teams meetings. If they want to join a meeting as a federated user, they

must sign in first. In that case, they must leave the meeting and rejoin as a federated user. By signing in, it is possible to promote attendees from one attendee type to a different type, such as attendee to the presenter in the meeting.

Meeting Attendees' Experience

Users' experiences will change in a Teams meeting depending on the meeting type and attendee type. For example, beginning with joining a meeting, some users can join a meeting directly, and others might have to wait in the lobby. By default, only internal and guest users can join directly. As a Teams admin, however, you can change the meeting policy to allow everyone to join the meeting directly, irrespective of whether they are internal, guest, or federated users. Anonymous users, however, will not join a meeting directly.

In a meeting, all but anonymous users can mute and remove others and admit users from the lobby to a meeting. Starting a meeting is configurable via policy, and dialing out is also configurable. Only internal users can initiate meeting recordings.

Before and after meetings, internal and guest users can chat in the channel meetings only if they are part of invited teams. Anonymous users cannot see chat, but federated users (tenants in the same region) will see chat after joining the meeting and continue seeing it after it. If federated users are tenants in a different region, they will not see any chats.

Which Teams Clients Can Join a Meeting?

Teams has a number of clients that can participate in a meeting.

- **From desktop client:** You can use a Windows or Mac client, or you can use a web client (Edge, Chrome, or Safari).
- **From mobile:** You can use an Android or iOS Teams app to join a Teams meeting.
- **From a desktop phone:** You can use 3rd Party IP Phone (3PIP) phones and phones optimized for Teams.
- **From a PSTN phone:** You can dial in or out from a Teams meeting.
- **From a Native Teams Device:** You can easily join a meeting with a one-touch join experience on your Teams native IP phone or other Teams native devices.

- **From a room system:** You can join a Teams meeting using Teams room or Surface Hub.
- **Cloud video interop:** You can use third-party CVI solutions like Pexip to integrate with existing room systems.

Teams Licensing for Meetings

Regarding licensing, Teams meetings are included in almost all the Teams licenses. If you want to use Teams audio conferencing, which allows you to dial in and dial out from and to phones, this requires an additional license. Audio conferencing is included in the E5 license or is available as an add-on for E1 and E3 licenses.

A Microsoft Stream license, which provides the ability to record Teams meetings, requires an E1, E2, E3, A1, A3, A5, Microsoft 365 Business, Business Premium, or Business Essential license for both the organizer and the user who initiates the recording.

Note Microsoft is currently providing an add-on Microsoft Teams Audio Conferencing license that includes dial-out capabilities to users in the United States and Canada. These licenses can be assigned to individual users for their audio-conferencing needs. However, it's important to note that dial-out is available only to users in the United States and Canada.

Teams Meeting Delegation

Meeting delegation allows users to schedule a meeting on behalf of other users. To do that, you need to configure a user as a delegate in Outlook and Teams. There are some requirements for delegation. You must have Office 2013 or a newer version and use Exchange Server 2013, Exchange Server 2016, or Exchange Online. In addition, the admin needs to be in the same environment, both on-premises and online. They need to be online in the same tenant for the online environment. A meeting on behalf of another user can be scheduled only with Teams Outlook add-ins.

Recording

To record a Teams meeting, users must have an E1, E3, E5, A1, A3, A5, M365 Business, Business Premium, or Business Essentials license assigned with a Microsoft Streams license.

Finally, the recording user must be enabled for recording and optionally transcription in the meeting policy. This cannot be an anonymous, guest, or federated user in the meetings.

Microsoft Teams Meeting Networking Considerations

Microsoft Teams supports real-time audio and video calls or meetings with optimal call quality. Call quality, however, depends on underlying network quality. Suppose a network is planned well with sufficient bandwidth. In that case, all required communication is allowed through an egress firewall, and the network has no packet loss and latency; teams calls or meetings will work seamlessly with optimal quality. If there is a blockage of Teams traffic with a high packet drop and latency rate, however, the Teams call experience will be poor, and some Teams features will not work as expected.

Where Teams Meetings Are Hosted

Network planning is critical before deploying a Teams meeting workload. To plan for Teams meeting use, you must understand the different components involved. First, the meeting service resides in the Office 365 data center where Teams is deployed. The meeting service mixes and distributes media (audio, video, application, and desktop sharing) for meetings. Each endpoint (internal and external) sends all media to the meeting service, and then each client receives all media they are attending.

In a Teams meeting, Microsoft will be served locally to end users. That means the meeting will be homed in the data center closest to the first user joining. This is a benefit because if you are a multinational organization with users on multiple continents, the Teams meeting is independent of your tenant location, and users will have the meeting in their region. For example, suppose the Cyclotron tenant is provisioned in the United States and the first users join the meeting from Europe. In that case, the meeting will be homed in a European Teams meeting service Office 365 cloud data center. Teams meetings in regions are highly beneficial because they will reduce latency compared to meetings held in a U.S. Microsoft data center. So, Teams meeting is independent of tenant location, and users will always have meetings within their region.

Networking Considerations for Teams Meeting Deployment

You already know that Teams is a cloud-only service, which means the Teams client is registered against a Teams service in the cloud, and Teams meeting attendees have to join the meeting through Teams service in the cloud. Therefore, all Teams signaling and media traffic traverses through the corporate network to the Internet to the Microsoft cloud network. That's why your Teams meeting planning for networking must include these three network segments, as shown in Figure 4-8.

- **Corporate network (on-premises network):** This is where a user resides in the corporate network to send all traffic to the Teams service in Office 365. First, real-time media traverse the local network, where you have complete control. You should configure this to meet the requirements of Microsoft Teams and prioritize traffic accordingly.
- **Interconnect network:** This is the Internet. If you have ExpressRoute deployed, this is an Internet service provider (ISP) connecting the enterprise network to the Microsoft 365 network. You cannot configure or change it because the Internet is unmanaged. However, you can talk to the ISP to optimize peering by reducing hops with the Microsoft Office 365 network or switch to a different ISP.
- **Office 365 global network:** This is a Microsoft-managed, low-latency network optimized for Microsoft Teams.

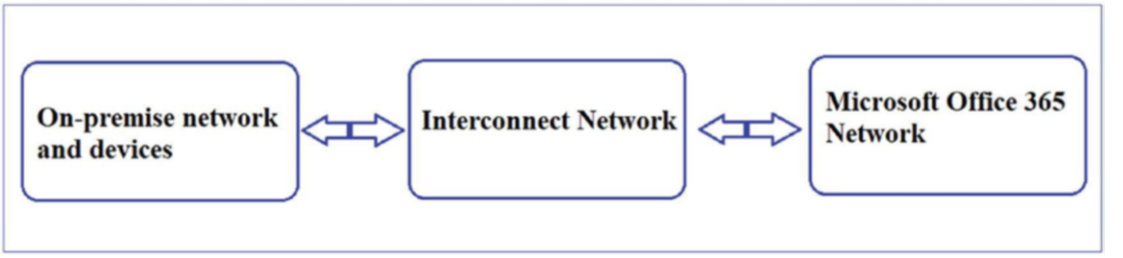

Figure 4-8. *Teams traffic traversing across the networks*

Allowing Teams Inbound and Outbound Traffic Through Firewall Configuration

Most Microsoft Teams connectivity failures or packet drops are related to a firewall. To handle Teams meetings correctly, you as an admin must allow a number of IP subnets, URLs, and FQDNs on your firewall with some ports and protocols. All the IP subnets, URLs, and FQDNs are listed at https://aka.ms/o365ip.

You must also open ports 80 and 443/TCP for all the Teams signaling uses. For media traffic, you must open UDP ports from 3478 to 3481 as preferred and 443/TCP as a fallback. Remember, UDP is always preferred for a better experience than TCP for real-time communications. Ensure the UDP traffic is enabled and avoid proxy servers that might enforce Teams media to TCP traffic.

It is recommended that you bypass Teams traffic from any packet inspection or security stack that might add latency or hold the packet for inspection. If you use VPN connections for remote users, split tunnel the traffic for Microsoft 365 Teams.

Managing a Teams Meeting

Let's look at how to manage a meeting.

Meeting Configuration

In managing a Teams meeting configuration, some global meeting settings apply to all users and all meetings. Meeting policies can be assigned on a per-user basis. By default, all users are assigned with the global policy unless you, an admin, assign a specific policy to be used.

The meeting organizer's policy will be applied to a meeting, so if the organizer has certain rights, all the attendees can use the same feature functionality. Meeting configuration policies can be configured in the Microsoft Teams admin center and by using Windows PowerShell.

Meeting Settings Applied to All Meetings

You can configure several global meeting settings that apply to all users. You can allow or block anonymous participants from meetings, customize meeting invites, and specify network settings, such as QoS marking and customized port ranges.

Meeting Policies Assigned to Users

Meeting policies assigned per user means you can create policies that allow more features to a set of users and restrict some features to specific users per custom requirements. You can configure users to schedule meetings if they can do ad hoc meetings, use Outlook add-ins, or schedule channel or private meetings. The best recommendation is to enable all of these features to provide the maximum opportunity to collaborate, but you should consider your organization's policy.

You can allow features such as transcripts, recording, audio, and video. You can set bandwidth limits and configure contact sharing; for example, whether users share an entire screen, an app only, or this is disabled entirely. You can configure users to allow them to request control for internal users, external users, or both. You can also enable or disable PowerPoint sharing, whiteboards, and shared notes.

You can configure users to schedule and join webinars by allowing meeting registration for better meeting engagement. Additionally, meeting policies allow for customizing recording options, such as enabling recording, setting default expiration time, storage, meeting options, and live captions.

For participants and guests, you can turn on or off the ability of anonymous users to dial out from meetings and start meetings. You can also set lobby settings, such as allowing everyone, everyone in your organization, or everyone in your organization and federated organizations.

Remember that the Global (Org-wide default) policy is created by default, and all the users within the organization will be assigned this meeting policy. As a Teams admin, you can decide if changes must be made to this policy, or you can create one or more custom policies and assign those to users as appropriate.

Creating and Managing Meeting Policy

You can create a new meeting policy or manage the existing meeting policy using the Teams admin center. To create a new meeting policy, follow the steps given next. A meeting policy has different sections: meeting scheduling, meeting join and lobby, meeting engagement, content sharing, recording and transcription, and audio and video.

1. Log in to the Teams admin center. In the left navigation pane, select Meetings. Select Meeting Policies. Click + Add to create a new meeting policy.
2. Once the New Meeting Policy page opens, enter a meaningful name for the new policy and optionally enter a description. In the meeting scheduling section, select whether to turn the following options on or off:
   - **Private meeting scheduling:** Users can schedule private meetings with this setting turned on.
   - **Meet now in private meetings:** This option controls whether users can start an instant private meeting.
   - **Channel meeting scheduling:** Meeting organizers can allow users to schedule channel meetings within channels they belong to with this setting.
   - **Meet now in channel meetings:** This setting enables meeting organizers to allow users to start instant meetings within channels they belong to.
   - **Outlook add-in:** Organizers can schedule private meetings from Outlook by turning on this setting.
   - **Meeting registration:** This option allows organizers to require registration for participants to join a meeting.
   - **Who can register:** This determines who is eligible to register for meetings.
   - **Attendance report:** Organizers can turn attendance reports on or off with this setting.
   - **Who is in the attendance report:** This setting controls whether participants can share their attendance information in the Attendance Report.
   - **Attendance summary:** This option controls whether to show attendance time information, such as join times, leave times, and in-meeting duration, for each meeting participant

Figure 4-9 shows all options in the meeting scheduling section set to On.

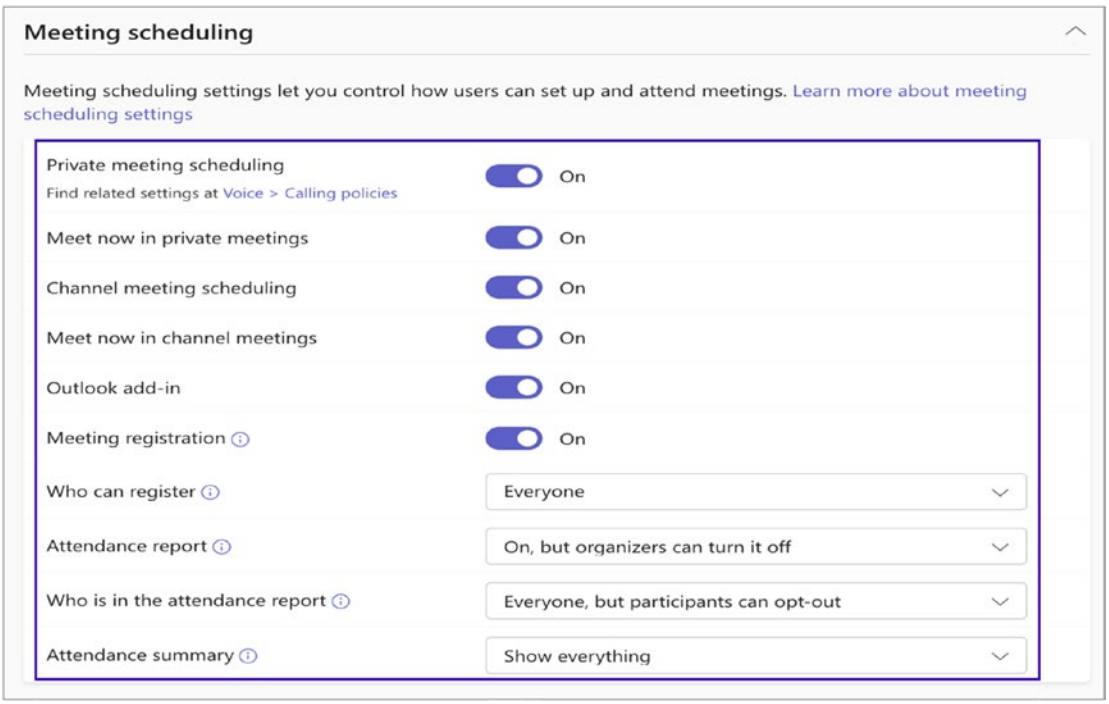

Figure 4-9. *Meeting policy meeting scheduling settings*

For example, Allow Meet Now is a policy applied before starting the meetings and has a per-user model. This policy controls whether the user can start a meeting in a Teams channel without the meeting having been previously scheduled. If you turn this feature on, when a user posts a message in a Teams channel, the user can select Meet Now to initialize an ad hoc meeting in the channel.

3. In the Meeting Join and Lobby section, turn the following options on or off:

   Anonymous users can join a meeting: When this setting is on; anyone can join Teams meetings, including Teams users in other organizations.

Anonymous users and dial-in callers can start a meeting: If you turn on this setting, anonymous users and dial-in users (those who join through a phone call) can start a meeting even if no one else is there.

Who can bypass the lobby: This setting allows you to control who can join a meeting directly and who must wait until they are admitted. This setting controls the default value of who can bypass the lobby in Meeting options; organizers and co-organizers can change this when they set up Teams meetings.

People dialing in can bypass the lobby: Controls whether people who dial in by phone join the meeting directly or wait in the lobby, regardless of who can bypass the lobby setting.

Figure 4-10 shows a summary of the "Meeting join & lobby" settings.

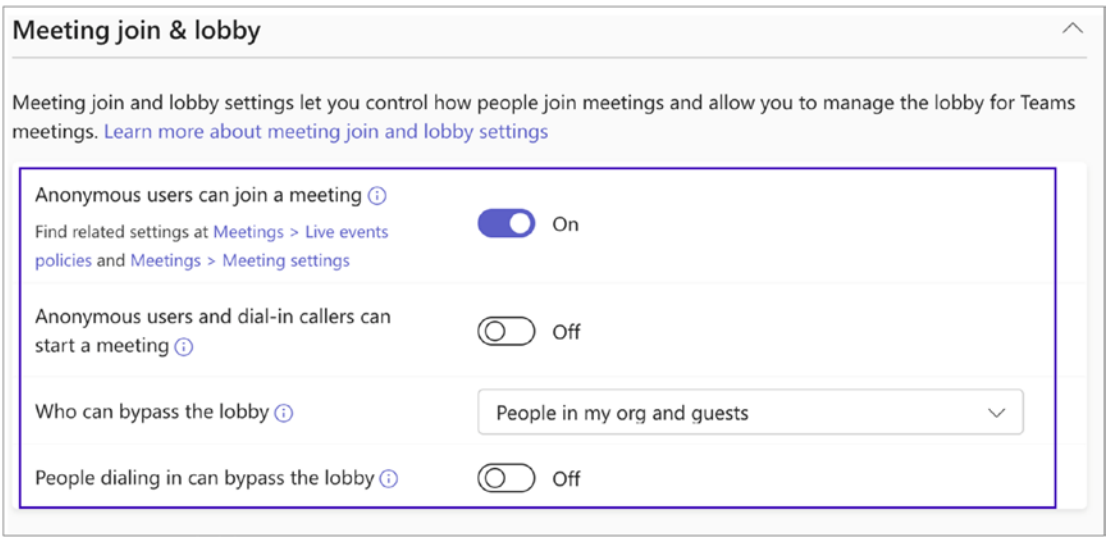

Figure 4-10. *Meeting join & lobby settings*

4. The Meeting Engagement section, shown in Figure 4-11, will help the admin control how people interact with meeting in an organization. The options available are as follows:
Meeting Chat: This feature allows the admin to decide who can participate in the meeting chat.

   Q&A: When turned on, organizers can enable a question-and-answer feature for their meetings.

   Reactions: In Teams meetings, this feature allows users to use live reactions such as Like, Love, Applause, Laugh, and Surprise.

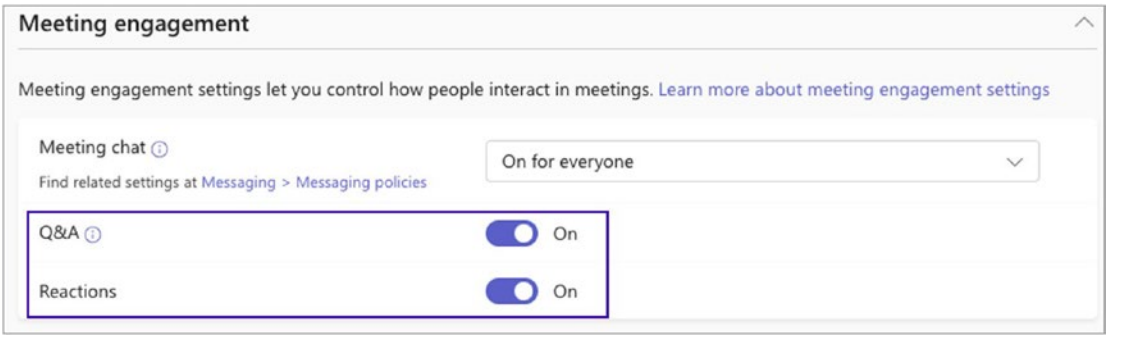

Figure 4-11. *Meeting engagement settings*

5. In the content-sharing section, you can control the sharing of various types of content during team meetings.

   Who can present: This option controls who can be the presenter in the Teams meetings. Options available are everyone, organizers and co-organizers and people in my org, and guests.

Tip To prevent external users from being default presenters, adjust the setting called "People in my organization and guests."

   Screen sharing mode: This controls whether desktop and window sharing is allowed in the user's meeting.

   Participants can give or request control: This setting allows users to choose whether to give control of the shared desktop or window to other participants in the meeting.

External participants can give or request control: You can control whether external participants, anonymous users, and guests can take control of shared screens during Teams meetings. Both organizations must enable this feature for an external participant to take control.

PowerPoint Live: This feature lets the meeting organizer decide if users can share PowerPoint slide decks during the meeting.

Whiteboard: This feature determines if a user can share the whiteboard during a meeting. Participants not part of the organization, such as guests and anonymous users, will follow the same rules inherited from the meeting organizer.

Shared notes: This feature allows attendees to share notes during a meeting. See Figure 4-12.

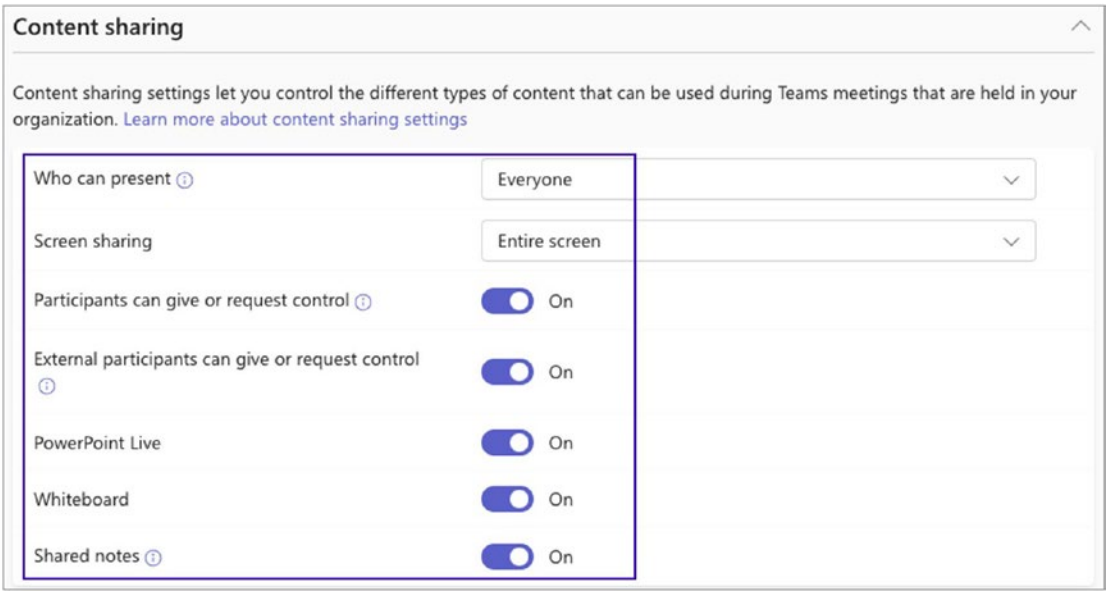

Figure 4-12. *Content sharing settings*

6. The recording and transcription sections allow you to manage the capabilities and features related to recording and transcribing.

   Meeting recording: When turned on, users can record their Teams meetings and group calls.

Note To record a meeting, the organizer and the person who initiated the recording must be permitted to record.

Recordings automatically expire: This feature allows you to set up automatic recording expiration after the number of days set in the default expiration time setting.

Default expiration time: You can set up the default meeting expiration time from 1 to 99999 days. By default, it is set to 120 days within the org-wide policy.

Store recordings outside your country or region: To store meeting recordings outside your country or region, enable the meeting recording and this setting.

Transcription: This setting enables captions and transcription features to be available during the playback of meeting recordings.

Live captions: This per-user policy determines if users want to turn on or turn off live captions during a meeting. See Figure 4-13.

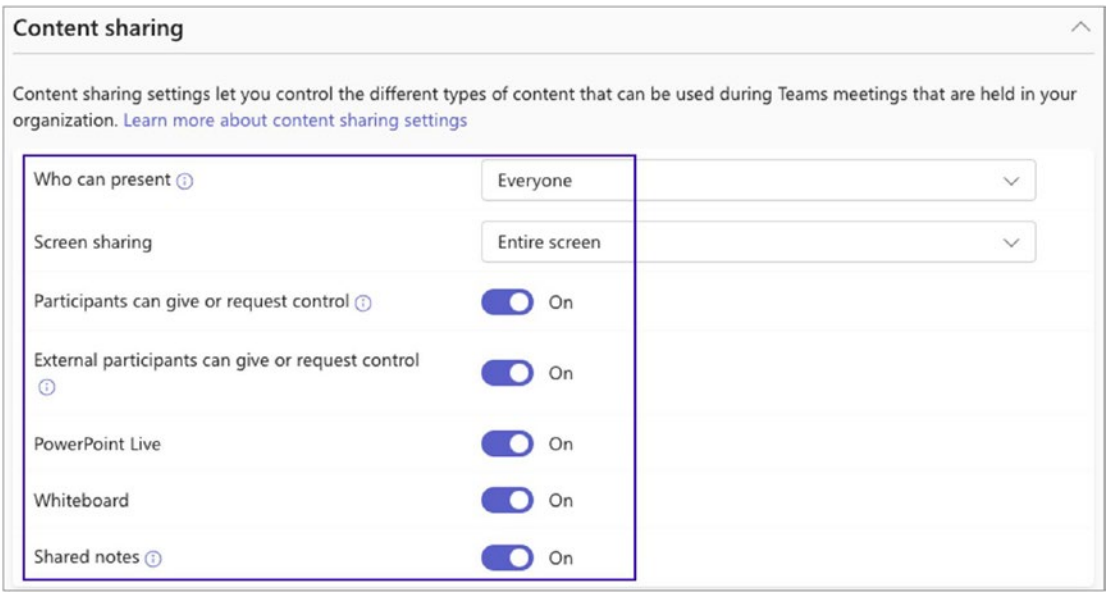

Figure 4-13. *Recording and transcription*

Additional attributes are available for recording and transcription through PowerShell. These attributes include the following:

- Allow cart caption Scheduling
- Channel record download
- Enroll user override
- Live interpretation enabled type
- Meeting invite languages
- Speaker attribute mode:
- Room attribute user override

7. Audio and video settings let you turn on audio and video capabilities within a Teams meeting.

   Mode for IP audio: This feature allows you to control whether you can turn on or off audio (incoming and outgoing) during meetings and group calls.

   Mode for IP video: This feature allows you to control whether you can turn on or off video (incoming and outgoing) during meetings and group calls.

   IP video: This option allows the user to determine if video can be enabled during meetings, one-on-one calls, and group calls. If using Teams on a mobile device, this option controls the ability to share photos and videos during a meeting.

   Local broadcasting: Capture and broadcast audio and video using NDI Technology

   Media bit rate (Kbs): This option controls the quality (media bit rate) of audio, video, and screen sharing during calls and meetings. This is a great option to configure for low-bandwidth sites in your organization.

   Network configuration lookup: If enabled, the roaming policies in the network topology will be verified.

Participants can use video effects: This feature allows them to choose whether to customize their camera feed with video backgrounds and filters.

Live streaming: This allows users to stream their Teams meetings using RTMP. See Figure 4-14.

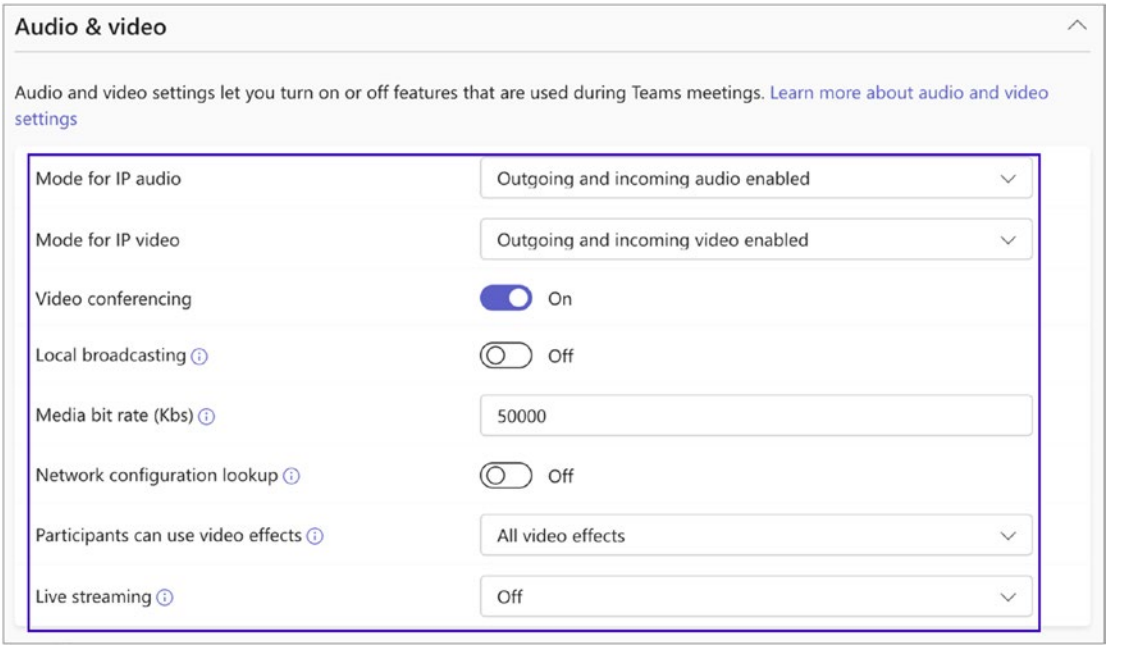

Figure 4-14. *Audio and video settings*

Once you have finished entering your settings, click Save to commit the changes.

Checking Teams Meeting Quality

To check the quality of Teams meetings, there are two tools you can use. The first is Call Quality Dashboard (CQD), which gives aggregated views of call quality and can be used to investigate quality per building, subnet, or any other metric that makes sense in your scenarios. You can use the CQD to proactively identify quality issues by looking at the lowest-quality site and determining how to improve call quality. To access the CQD, log in to the Teams admin center and click Call Quality Dashboard. You should sign in again to the CQD.

Call analytics is the second tool you can use. This allows you to view individual calls and see the quality of a specific call for both one-to-one calls and Teams meetings. Call analytics can be used reactively to troubleshoot individual calls that a user reports as a poor call quality experience. To access call analytics, log in to the Teams admin center and select Users. Find the individual user whose call quality you want to check and then click Call History. Select the individual call to check call quality, as Figure 4-15 shows.

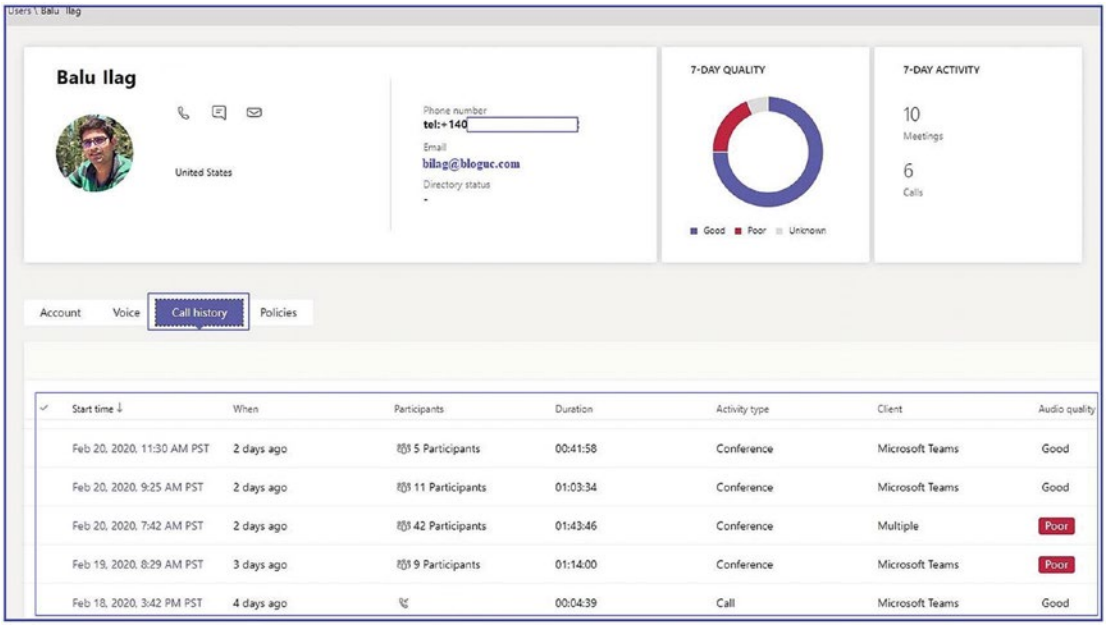

Figure 4-15. *Call analytics*

Microsoft Teams Audio Conferencing

You have already learned how Microsoft Teams meetings work; how Teams provides audio, video, and content sharing through the data network (VoIP); and how the Teams client allows users to join meetings.

This topic covers Teams Audio Conferencing (dial-in), including how Teams Audio Conferencing works, how to acquire a conference bridge, Audio Conferencing licensing, dial-out limits, and more. Teams Audio Conferencing allows attendees to join Teams meetings through dial-in to a Teams conference bridge number with a conference ID through a regular phone (landline or mobile phone). Teams Audio Conferencing is also known as Teams *dial-in conferencing*. For example, users can use Audio Conferencing to attend meetings over a regular phone by dialing into the meeting.

As a Teams admin, you can customize Teams meeting modalities and experiences per your organization's requirements. For example, you can turn certain types of meetings on or off in addition to disabling modalities such as video or screen sharing. Because there is integration between Microsoft 365 tools such as Microsoft Outlook, users can use an add-in to schedule Teams meetings directly from their Outlook calendar.

Based on your organization's needs and requirements, you can configure the appropriate settings for the meetings and conferencing your users will use in Microsoft Teams. Because this communication workspace offers so many options and advantages, it is crucial for you, as a Teams admin, to review and confirm that your environment is configured correctly to provide users the best possible experience.

Before deploying Teams Audio Conferencing across your organization, you should ensure all user locations have Internet access to connect to Microsoft 365 (Internet breakout for each branch and central site is ideal). If it is impossible to have direct Internet connectivity for each branch site, check network quality using the 0365 Connectivity Tool or Microsoft Teams Network Assessment Tool, which shows network quality, including packet loss, jitter, and latency. You will therefore have an idea of users' experience when they use Teams meetings. Additionally, you must check whether your network is ready to deploy Microsoft Teams meetings. Before learning about Teams Audio Conferencing, as a Teams admin, you must know what phone numbers Teams supports.

This topic covers Teams service numbers in detail, including Teams conference numbers and the numbers used for the auto attendant and call queue, including toll and toll-free numbers.

Teams Audio Conferencing Licensing Requirements

To use Teams Audio Conferencing, your organization needs an additional license on top of the Microsoft Teams license. Microsoft 365 Audio Conferencing (Teams Audio Conferencing) licenses are available as part of an Office 365 E5 subscription or as an add-on license to an existing subscription like E1 or E3. Microsoft is offering a free Microsoft Teams Audio Conferencing license that includes dial-out capabilities to users in the United States and Canada. These licenses can be assigned to individual users for their audio conferencing needs. However, it's important to note that dial-out is available only to users in the United States and Canada. Users in other regions must be assigned communication credits to dial out from Teams meetings.

Teams Audio Conferencing Requirements

Teams Audio Conferencing involves the Audio Conferencing licenses, the conference dial-in bridge (phone numbers for dial-in), and communications credits for dialing out from Teams meetings. As part of the Teams Audio Conferencing license, Microsoft provides dedicated dial-in bridge numbers (an admin must acquire the dial-in numbers from Microsoft) and shared conference numbers. Suppose your organization uses a legacy solution like Skype for Business (Lync) On-Premises or Online with enterprise voice and dial-in conferencing with their conference bridge numbers. In that case, the organization might use the existing conference bridge for Teams meetings when upgrading from Skype for Business to Microsoft Teams. Microsoft allows using these service phone numbers by porting them from your current service provider to Microsoft 365. This means you can use Microsoft-provided conference bridge numbers, either dedicated or shared or porting your existing service numbers

As a Teams admin, you must configure a Teams conference bridge number. Conferencing bridge numbers allow users to dial into meetings through a landline or mobile phone. When configuring Teams Audio Conferencing in your Microsoft 365 environment, you will receive conference bridge numbers from Microsoft for an Audio Conferencing bridge (a conferencing bridge can contain one or more phone numbers). These conference bridge numbers are used when the users dial into a Teams meeting (the phone number should be included in every Microsoft Teams meeting invite). When an organization enables the audio conference license, shared audio conference bridge numbers are automatically assigned to their tenant. However, a dedicated conference bridge number (toll or toll-free) is available based on request. As an admin, you can obtain a toll or toll-free conference number from Microsoft by using the Teams admin center or creating a ticket with the PSTN Service desk by going to `https://pstnsd.powerappsportals.com/create-ticket/`.

As a Teams admin, you can continue using the default settings for a conferencing bridge, or you can change the phone numbers (toll and toll-free) and other settings (e.g., the PIN or the languages used). However, you must first decide if you need to add new conferencing bridge numbers, which number should be your default, whether you need to modify the bridge settings, and whether you must port numbers to use with audio conferencing.

Adding Dedicated Conference Bridge Numbers

You must perform the following steps to add a dedicated conference bridge number:

1. Log in to the Teams admin center, and in the left pane, select Meetings. Then select Conference Bridges. On the Conference Bridges page, click + Add.
2. From the + Add drop-down list, select either Toll Number or Toll-Free Number, as shown in Figure 4-16.
3. On the Add Phone Number page, select the phone number you want to add, and then click Apply.

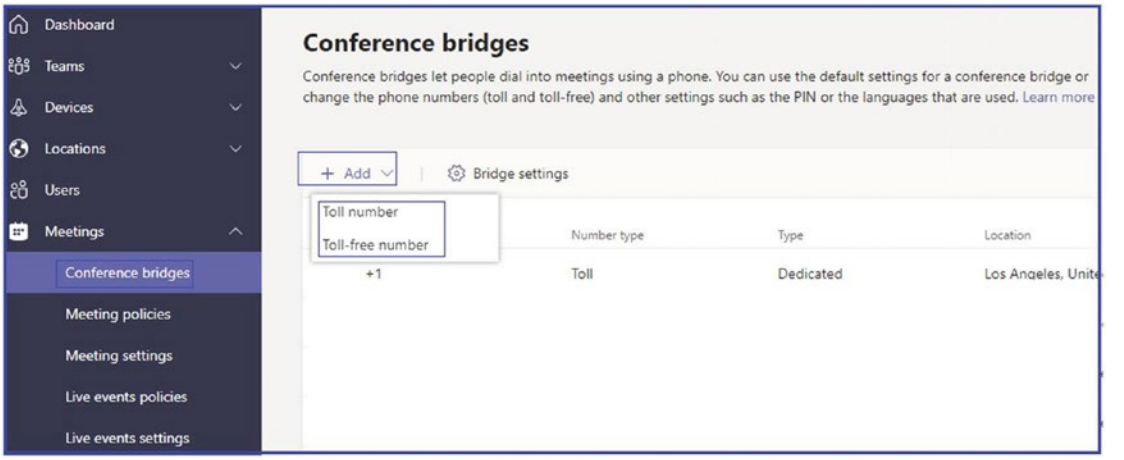

Figure 4-16. *Adding a conference bridge number*

Setting a Default Conference Bridge Number

To configure a default number for your conference bridge, perform this procedure:

1. On the Conference Bridges page, in the main pane that shows all the conference bridge phone numbers, select the phone number you want to configure as your default.
2. Click Set As Default on the menu bar, as shown in Figure 4-17.

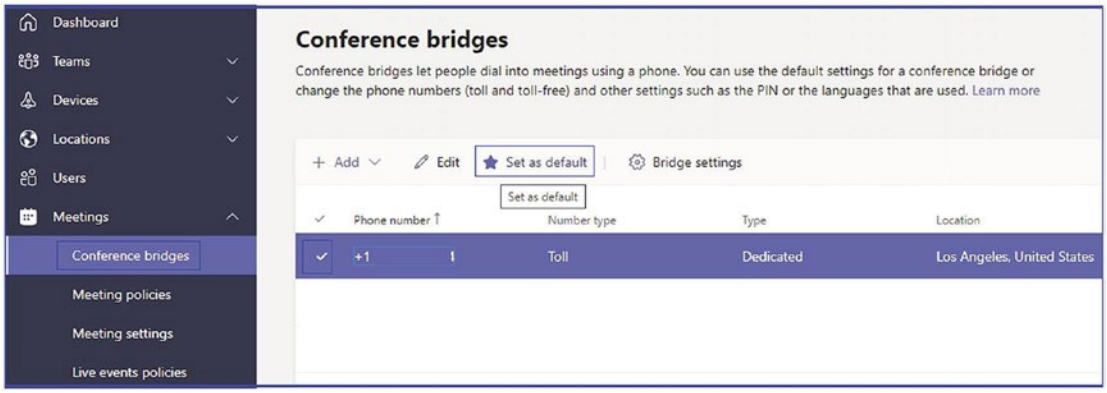

Figure 4-17. *Setting a default conference bridge*

Configuring and Managing Teams Conference Bridge Settings

To configure conference bridge settings, follow these steps:

1. Log in to the Teams admin center and select Meetings. Select Conference Bridges, and click Bridge Settings on the Conference Bridges page.
2. You can set the following options in the Bridge Settings window to configure bridge settings:
    a. **Meeting Entry And Exit Notifications:** You can turn this setting on or off, depending on whether you want users who have already joined the meeting to be notified when someone enters or leaves the meeting. If this setting is on, you can choose from the following options.
    b. **Entry/Exit Announcement Type:** Select one of the following options.
        i. **Names Or Phone Numbers:** When users dial into a meeting, their phone number will be displayed when they join.
        ii. **Tones:** When users dial into a meeting, an audio tone will be played when they join.

c. **PIN Length:** Set the PIN length value between 4 and 12; the default value is 5.

d. **Automatically Send Emails To Users If Their Dial-in Settings Change:** This option should be enabled or disabled.

e. **Mask Phone numbers:** Phone numbers of participants who join a Teams meeting via audio conferencing will be fully displayed to internal participants only. The numbers will be masked so that external participants cannot see them. This setting is enabled by default.

3. Finally, click Apply to confirm the settings, as shown in Figure 4-18.

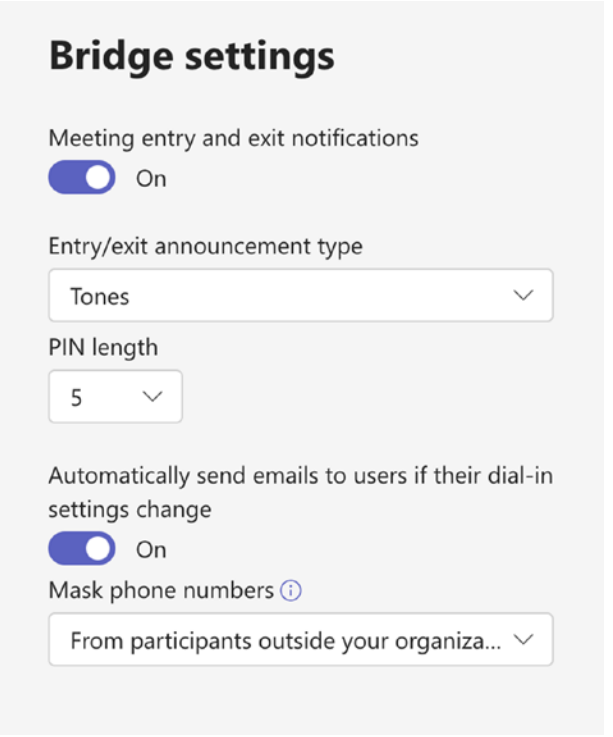

Figure 4-18. *Conference bridge settings*

Setting Up and Managing Communications Credits for Audio Conferencing

Before setting up communications credits, a Teams admin must understand what communications credits are and how they will help. So far, you have learned about Teams meetings and Audio Conferencing, and you know Teams Audio Conferencing allows users to dial out from a meeting to add someone to the Teams meeting. Dialing out from Teams meetings has some limitations, however. Users can dial out from Teams meetings only to certain countries, and the number of minutes is limited. To use Audio Conferencing, each organization has to buy an add-on license to use dial-in and dial-out functionalities in Teams meetings. Limited dial-out minutes are allowed with each Audio Conferencing license subscription.

A Microsoft 365 Audio Conferencing license subscription offers 60 minutes per user per month that can be used to dial out to non-Premium numbers in any of the Zone A countries (Australia, Austria, Belgium, Brazil, Bulgaria, Canada, China, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, India, Ireland, Italy, Japan, Luxembourg, Malaysia, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Puerto Rico, Romania, Russia, Singapore, Slovak Republic, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, United Kingdom, United States). Microsoft considers the number of Audio Conferencing licenses as the *tenant dial-out pool*. The total number of Audio Conferencing licenses multiplied by 60 minutes will be the monthly dial-out minute pool for the organization. For example, the Cyclotron organization has purchased 50 Audio Conferencing subscription licenses. It has 30 users in the United States, 10 in the United Kingdom, and 10 in India. All these Audio Conferencing subscription licenses are assigned to the users. All 50 users share a pool of 50 users × 60 minutes = 3,000 conferencing dial-out minutes per calendar month that can be used to place outbound calls to nonpremium numbers in any of the Zone A countries (refer to `https://docs.microsoft.com/en-us/microsoftteams/audio-conferencing-subscription-dial-out`), regardless of where the meeting organizer is licensed or physically located. For example, as a meeting organizer, Cyclotron User B in India can dial out to any of the Zone A countries up to the minute pool limit (i.e., 3,000 minutes).

Note All dial-out calls exceeding 3,000 minutes per calendar month are billed per minute using communications credits at Microsoft-published rates to that destination.

As an admin, you need to set up communications credits if you would like to use toll-free numbers with Microsoft Teams. Microsoft recommends that you set up communications credits for your Calling Plans (domestic or international) and Audio Conferencing users who need the ability to dial out to any destination. Many countries and regions are included, but some destinations might not be included in the Calling Plan or Audio Conferencing subscriptions. Suppose you don't set up communications credits billing and assign a Communications Credits license to your users. You run out of minutes for your organization (depending on your Calling Plan or Audio Conferencing plan in your country or region). Those users won't be able to make calls or dial out from Audio Conferencing meetings.

Communications credits provide a convenient way to pay for Audio Conferencing and Calling Plan minutes. It ensures users have the ability to add toll-free numbers to use with Audio Conferencing meetings, auto attendants, or call queues. Toll-free calls are billed per minute and require a positive communications credits balance. Dialing out from an Audio Conferencing meeting to add someone else from anywhere in the world requires dial-out credit. Additionally, communications credits get used when users dial any international phone number when they have a Domestic Calling Plan subscription or dial international phone numbers beyond what is included in a Domestic and International Calling Plan subscription. Another important use case for communications credits is dialing out and paying per minute once you have exhausted your monthly minute allotment.

Assigning Communications Credits to a User

You can assign Communications Credits licenses to individual users as an admin by logging in to Microsoft 365 admin center. Navigate to Users. Select Active Users and then select the particular user and enable a Communications Credits license for that user.

Checking Communications Credits Plans and Pricing

Before setting communications credits, you must check the plans and pricing. To do so, log in to the Microsoft 365 admin center (https://portal.office.com/adminportal/home?add=sub&adminportal=1#/catalog) and navigate to the Marketplace and validate the subscription plans.

Setting Up Communications Credits for a Tenant

Next you need to know how to set up communications credits for your organization. To do so, follow this procedure:

1. Log in to the Microsoft Office 365 admin center (https://admin.microsoft.com/Adminportal/Home?) with your work or school account. Click Billing and then select Purchase Services. Scroll down and select Add-Ons.
2. Select Communications Credits. Enter your information on the Communications Credits subscription page, and click Next.
3. In the Add Funds Field, enter the amount you want to add to your account.
4. Microsoft recommends enabling the Auto-Recharge option. It automatically refills your account when the balance falls below your set threshold. If you don't enable this setting, once the funds are used, calling capabilities enabled using communications credits will be disrupted (e.g., inbound toll-free service). Auto-recharge avoids manually adding a communications credits balance each time your balance reaches zero. This feature is selected in the example in Figure 4-19, and $100 in funds has been added for the Cyclotron organization.

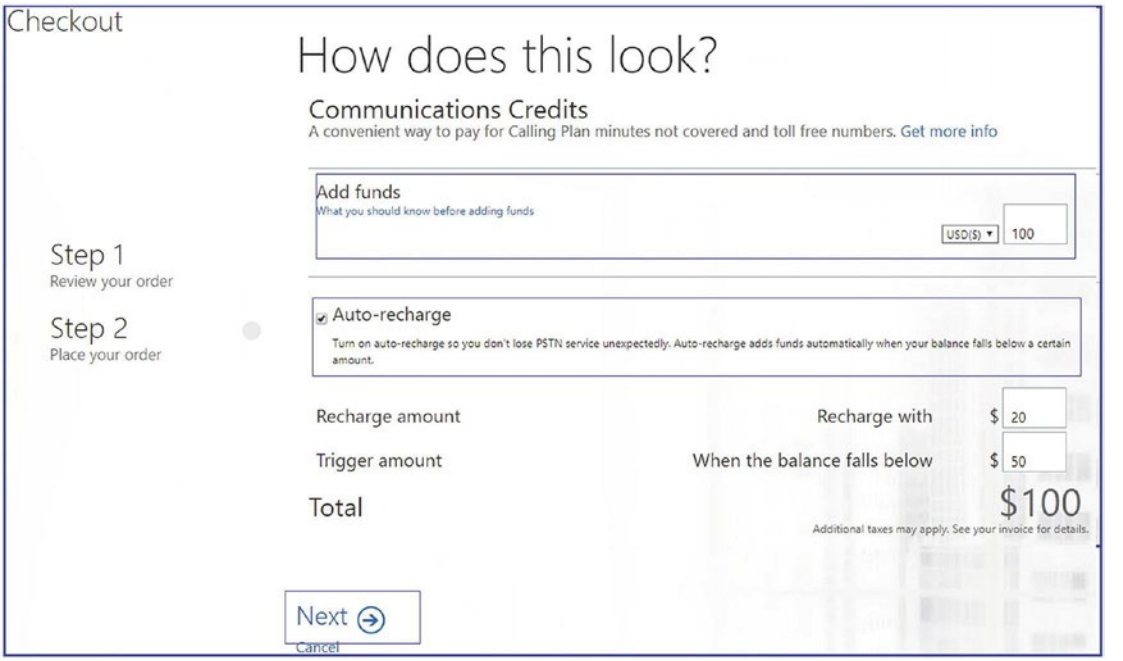

Figure 4-19. *Communications credits*

Note Remember the funds will be applied only to communications credits at Microsoft's published rates when the services are used. Any funds not used within 12 months of the purchase date will expire and be lost, so set the credit level based on your usage.

---

5. Monthly billing for communications credits will be applied only if the allotted funds have been used. To learn how to check your monthly usage, read the next section.
6. Finally, enter your payment information and click Place Order.

Checking a Tenant's PSTN Usage

Every organization will have a different usage rate because usage is dependent on call volume and rates the provider charges. As an admin, you must get this usage data from your current PSTN service provider. For organizations using Skype for Business Online and

Microsoft as a PSTN service provider, you can get usage data by reviewing it in the Microsoft 365 admin center (Analytics and Reports ➤ Usage Reports ➤ PSTN Usage Details).

When setting up communications credits, you must examine your organization's call usage details to determine your needed amounts. You can get call usage information by reviewing the PSTN usage details report. This report lets you export the call data records to Microsoft Excel and create custom reports.

Managing an Individual User's Conference Bridge Number and Language for Teams Meetings

To manage an individual user's conference bridge number, log in to the Teams admin center and navigate to Users. Find the individual user whose conference bridge number you want to check, and then under Account, view the Audio Conferencing settings for the individual, as shown in Figure 4-20.

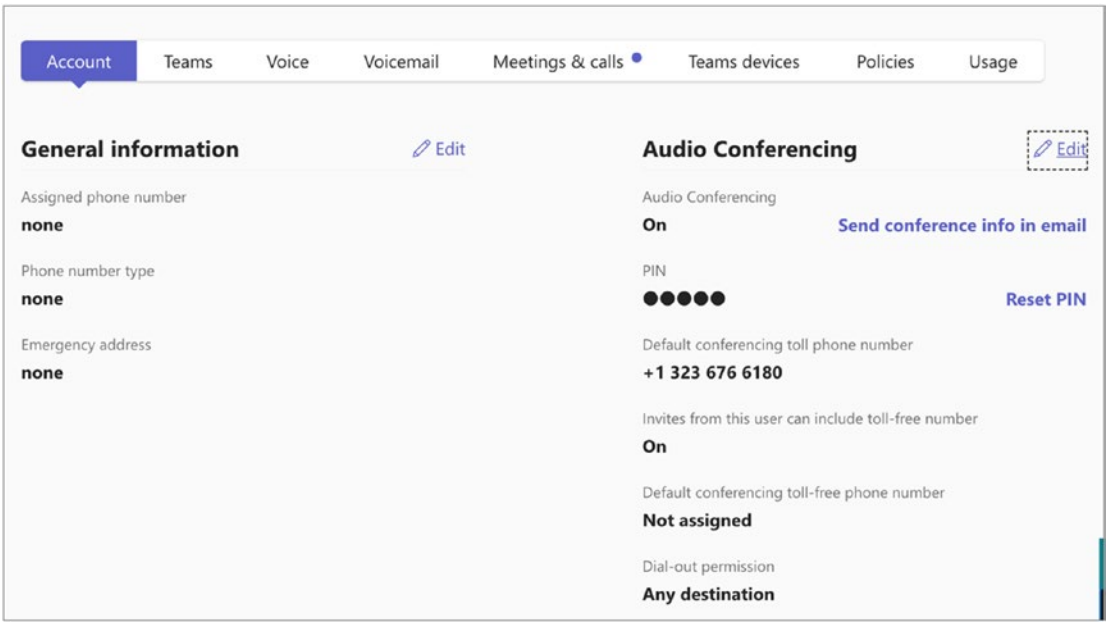

Figure 4-20. *Audio Conferencing settings*

Under Audio Conferencing, click Edit to modify the settings. On the Audio Conference page, turn on Audio Conferencing, modify the Toll Number or Toll-Free Number values, and modify the Dial-Out From Meetings setting if required. Figure 4-21 shows the settings for this example.

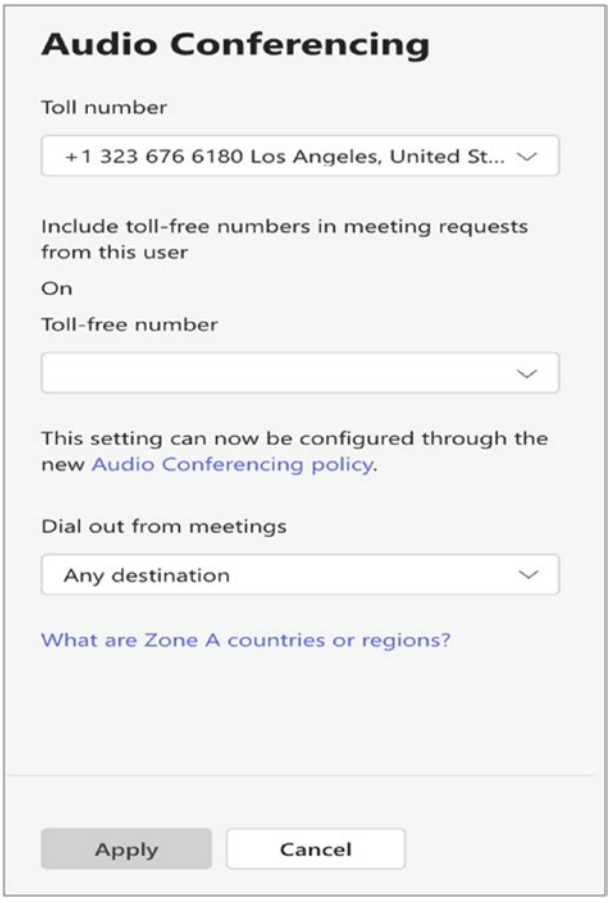

Figure 4-21. *Modifying a conference bridge number for an individual user*

Outbound Calling Restrictions for Audio Conferencing and PSTN Calls

The meeting's dial-out feature is set to "call any destination" by default. However, it's important to note that Audio Conferencing offers free dial-out only to Zone A countries. The organization will be charged pay-per-minute rates for countries outside Zone A based on the specific country. These charges will be deducted from the communication credits. Sometimes, the admin may want to restrict users from dialing out to countries outside of Zone A to prevent unnecessary costs. This can be achieved by changing the user's audio conferencing settings using Windows PowerShell.

```
Grant-CsDialoutPolicy -Identity <username> -PolicyName <policy name>
```

The following table provides an overview of each policy.

PowerShell Cmdlet	Description
`Identity='tag:DialoutCPCandPSTN International'`	A user in the conference can dial out to international and domestic numbers, and this user can also make outbound calls to international and domestic numbers.
`Identity='tag:DialoutCPCDomestic PSTNInternational'`	A user in the conference can dial out only to domestic numbers, and this user can make outbound calls to international and domestic numbers.
`Identity='tag:DialoutCPCDisabled PSTNInternational'`	A user in the conference can't dial out. This user can make outbound calls to international and domestic numbers.
`Identity='tag: DialoutCPC InternationalPSTNDomestic'`	A user in the conference can dial out to international and domestic numbers, and this user can make outbound calls only to domestic PSTN numbers.
`Identity='tag: DialoutCPC InternationalPSTNDisabled'`	A user in the conference can dial out to international and domestic numbers, and this user cannot make any outbound calls to PSTN numbers besides emergency numbers.
`Identity='tag:DialoutCPCand PSTNDomestic'`	A user in the conference can dial out only to domestic numbers, and this user can make outbound calls only to domestic PSTN numbers.
`Identity='tag:DialoutCPCDomestic PSTNDisabled'`	A user in the conference can dial out only to domestic numbers, and this user cannot make any outbound calls to PSTN numbers besides emergency numbers.
`Identity='tag:DialoutCPCDisabled PSTNDomestic'`	A user in the conference can't dial out, and this user can make outbound calls only to domestic PSTN numbers.

(*continued*)

PowerShell Cmdlet	Description
`Identity='tag:DialoutCPCandPSTN Disabled'`	A user in the conference can't dial out, and this user can't make any outbound calls to PSTN numbers besides emergency numbers.
`Identity='tag:DialoutCPCZone APSTNInternational'`	A user in the conference can dial out only to Zone A countries and regions, and this user can make outbound calls to international and domestic numbers.
`Identity='tag:DialoutCPCZone APSTNDomestic'`	A user in the conference can dial out only to Zone A countries and regions, and this user can make outbound calls only to domestic PSTN numbers.
`Identity='tag:DialoutCPCZone APSTNDisabled'`	A user in the conference can dial out only to Zone A countries and regions, and this user can't make any outbound calls to PSTN numbers besides emergency numbers.

For example, if you have a requirement to prevent your users from dialing out to an international PSTN call but allow them for conferencing, assign a dial-out policy with the attribute DialoutCPCandPSTNDomestic. Note that if you assign this policy to U.S. users, they cannot dial out to outside the United States including Canada.

Configuring and Managing Meeting Policies

Teams meeting policies provide a way to permit or restrict features that will be available to users during the meetings and audio conferencing. Before proceeding, it's important to determine whether you want to customize the global meeting policies and/or if you require more than one meeting policy. You must now identify which user groups will be assigned to specific meeting policies. Finally, you must determine whether your organization must purchase and deploy room system devices for your conference rooms.

As a Teams administrator, you are responsible for managing meeting policies, which control the features of meetings scheduled by users within your organization. These policies are created and managed by you and are then assigned to specific users. You can manage meeting policies through the Microsoft Teams admin center or Windows

PowerShell. These policies directly affect the user's meeting experience before, during, and after the meeting ends. There are three different ways in which meeting policies can be applied.

- **Per meeting organizer:** All meeting participants receive the policy of the organizer.
- **Per user:** Only the per-user policy applies to restrict certain features for the organizer or meeting participants.
- **Per organizer and per user:** Certain features are restricted for meeting participants based on their policy and the organizer's policy.

Note The policy named Global (Org-wide default) is created by default, and all the users within the organization will be assigned this meeting policy by default. The company administrators can decide if changes must be made to this policy, or they can decide to create one or more custom policies and assign those to users. You can refer to the previous section to create a new Teams meeting policy.

Teams Meeting Limitations

Administrators need to be aware that Teams meetings have certain limitations. Understanding these limitations allows them to determine if Teams meetings and audio conferencing suit your organization. One limitation is that Teams doesn't include a personal conference ID feature. However, you can use a meeting URL instead, which never expires. Here are some other limitations to keep in mind:

Feature	Maximum Limit
Number of people in a meeting (can chat and call in)	1000, includes GCC, GCCH, and DoD, but not A1 (300).
Number of people in a video or audio call from chat	20.

(*continued*)

Feature	Maximum Limit
Max PowerPoint file size	2 GB.
Meeting recording maximum length	4 hours or 1.5 GB. When this limit is reached, the recording will end and automatically restart.
Breakout room maximum participants in a meeting	300.
Teams meeting limit	30 hours.
Teams URL	Never expire.

Meeting Type	Expiration Time	Each time you start or update a meeting, expiration extends by this much time
Meet now	Start time + 8 hours	N/A
Regular with no end time	Start time + 60 days	60 days
Regular with end time	End time + 60 days	60 days
Recurring with no end time	Start time + 60 days	60 days
Recurring with end time	End time of last occurrence + 60 days	60 days

Type of Meeting	Number of Participants	Registration Supported
Meetings	Up to 20,000* Participants up to 1,000 have fully interactive equal meeting capabilities. Participants over 1,000 up to 20,000 have view-only capabilities	Yes
Webinars	Up to 1,000	Yes
Live events	Up to 20,000	No

Capability	Organizer	Co-organizer	Presenter	Attendee
Speak and share video	Yes	Yes	Yes	Yes
Participate in meeting chat	Yes	Yes	Yes	Yes
Share content	Yes	Yes	Yes	No
Privately view a PowerPoint file shared by someone else	Yes	Yes	Yes	Yes
Take control of someone else's PowerPoint presentation	Yes	Yes	Yes	No
Mute other participants	Yes	Yes	Yes	No
Prevent attendees from unmuting themselves	Yes	Yes	Yes	No
Remove participants	Yes	Yes	Yes	No
Admit people from the lobby	Yes	Yes	Yes	No
Change the roles of other participants	Yes	Yes	Yes	No
Start or stop recording	Yes	Yes	Yes	No
Start or stop live transcription	Yes	Yes	Yes	No
Manage breakout rooms	Yes	Yes	No	No
Change meeting options	Yes	Yes	No	No
Add or remove an app	Yes	Yes	Yes	No
Use an app	Yes	Yes	Yes	Yes
Change app settings	Yes	Yes	Yes	No

Teams Webinars

Teams Webinars is a meeting service available in the Teams meeting suite in addition to Teams Meeting and Teams Live events. This two-way interactive virtual event gives organizers more control over conversations and participants. Currently, webinars can accommodate up to 1,000 attendees, which are popular among training, product demos, customer events, etc. In this section, we will discuss how an admin can set up webinars for an organization, including scheduling a webinar and registering for one. We'll also cover the features of webinars and the licensing requirements.

Features of Webinars

You may be curious about the benefits of using webinars instead of Microsoft Teams meetings and Microsoft Live events, which have similar features. Webinars are particularly useful when you require a blend of Live events and Teams meetings. They provide superior registration capabilities compared to Teams meetings and offer more customizable event options than Teams Live events, including event-based themes and meeting options.

Here are the main features of webinars:

- Schedule webinars for up to 1,000 attendees
- Registration
- Assign co-organizers
- Restrict the webinars to org-wide only
- Limit the day and time when people register
- Adjust meeting options

Licensing

The Teams license provides access to basic webinars and their capabilities mentioned in the previous section, but a Teams Premium license offers additional robust features.

Teams Premium licensing is necessary to utilize the capabilities of Teams Webinars fully. The disparities in webinar features between Teams and Teams Premium are outlined in the "Teams Premium" section later in this chapter. As an administrator, it is essential to understand your organization's needs and acquire Teams Premium licenses accordingly. Teams Premium is an add-on subscription-based license. Additional details on Teams Premium are outlined in the "Teams Premium" section.

Here are some webinar-related features with Teams Premium as of this writing:

> **Set up a green room for webinar presenters:** Presenters can use this feature to join early and make adjustments to audio, video, and content-sharing options. They can also communicate with other organizers and presenters before attendees join.

Create a webinar waiting list: By enabling the waitlist, the registration for a webinar will remain open even after the event has reached its capacity limit set by the organizer. This feature allows additional individuals to register and be automatically placed on the waitlist. As new spots become available, individuals on the waitlist will be notified and allowed to register for the event. Organizers can manually review the registration information and approve or reject each registration.

Limit the day and time when people register: An organizer can create a registration time limit for participants. Once the registration period has ended, users may either be added to a waitlist (if available) or can no longer register.

Manually approving the registrations: As an organizer, you can view all the registered participants and manually approve each one. This feature helps ensure that you have the exact group of attendees you need for the webinar event.

Send reminder emails to the registrants: When you enable this feature, an automated email will be sent to all attendees to remind them about the event. This helps build excitement and keeps everyone updated.

Manage Attendee views: This feature allows the organizer to manage the attendee view for a more streamlined event. The options include enabling attendees to only view the shared screen and participants, all presenters with their presentations, and more.

RTMP-In: The feature RTMP-In enables organizers to create Teams Webinars using an external encoder that users Real-Time Messaging Protocol (RTMP).

Teams Webinars Administration

If you are a Teams administrator, you can modify webinar settings for your organization using specific commands. Webinars are enabled by default, but admins can validate this by connecting to Microsoft Teams PowerShell module running this PowerShell command:

```
Get-CsTeamsEventsPolicy -Identity Global
```

The command returns the information about the Global policy. Under the attributes listed, Allow Webinar will be set to Enabled. To turn off webinars, use the PowerShell command to set Allow Webinar to Disabled.

```
Set-CsTeamsEventsPolicy -Identity Global -AllowWebinars Disabled
```

Currently, the administrator must also ensure that the "Allow registration" option is enabled in the meeting policies. This can be verified through this PowerShell command:

```
Get-CsTeamsEventsPolicy | select identity, AllowRegistration
```

If "Allow registration" is disabled, enable it using the following PowerShell command:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowRegistaration $True
```

As an administrator, you can restrict webinar registration to specific users. By default, registration is open to everyone or the public. However, using the PowerShell command, you can change this setting to only allow internal users and guests:

```
Set-CsTeamsEventsPolicy -Identity Global -EventAccessType
EveryoneInCompanyExcludingGuests
```

To change the settings back to everyone, use the following command:

```
Set-CsTeamsEventsPolicy -Identity Global -EventAccessType Everyone
```

This setting is also available via the Teams meeting policy. Use the following command to modify the changes:

```
Set-CsTeamsMeetingPolicy -Identity Global -Whocanregsiter EveryoneInCompnay
```

To revert to settings for everyone, use the following command:

```
Set-CsTeamsMeetingPolicy -Identity Global -Whocanregsiter Everyone
```

The event registration, RTMP-in, and RTMP-out capabilities are managed using meeting policies discussed in Chapter X and Chapter X.

Teams Webinars Scheduling

Let's look at an example. As an organizer, I plan a webinar to inform my organization about the newest Teams updates and give a brief overview of their features and communication tools. My administrator assigned me a Teams Premium license to take advantage of the webinar features with Teams Premium. I want to schedule the webinar for 30 minutes, limit registration time, add co-organizers, enable a green room for the presenters, and enable Q&A. Let's schedule a Teams webinar based on these requirements.

To schedule a Teams Webinar, go to Teams Calendar and click the down arrow located next to the New Meeting button; from the list of options, select and click Webinar, as shown in Figure 4-22.

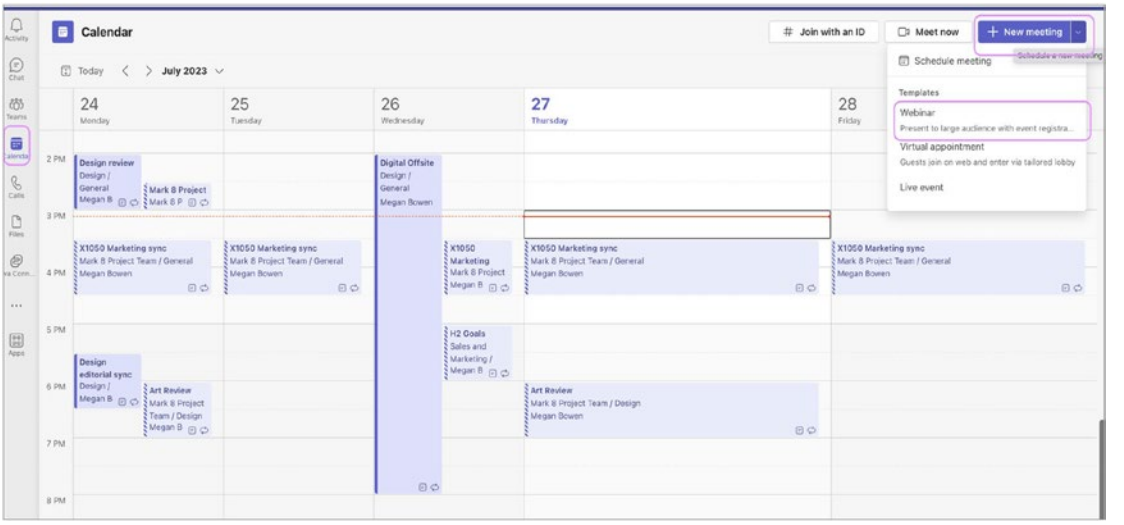

Figure 4-22. *Scheduling a webinar*

On the details page, as shown in Figure 4-23, under the setup section, enter the title, the start and end time of the webinar event, and the description. Next, add your co-organizers and presenters to the meeting. As it is an internal event, choose your organization from the attendee options. At the bottom of the details page, you will find the default meeting options, which you can modify later as the organizer. Click Save and send invites. Please note that the invites will be sent only to the presenter and the organizers, not to your entire organization.

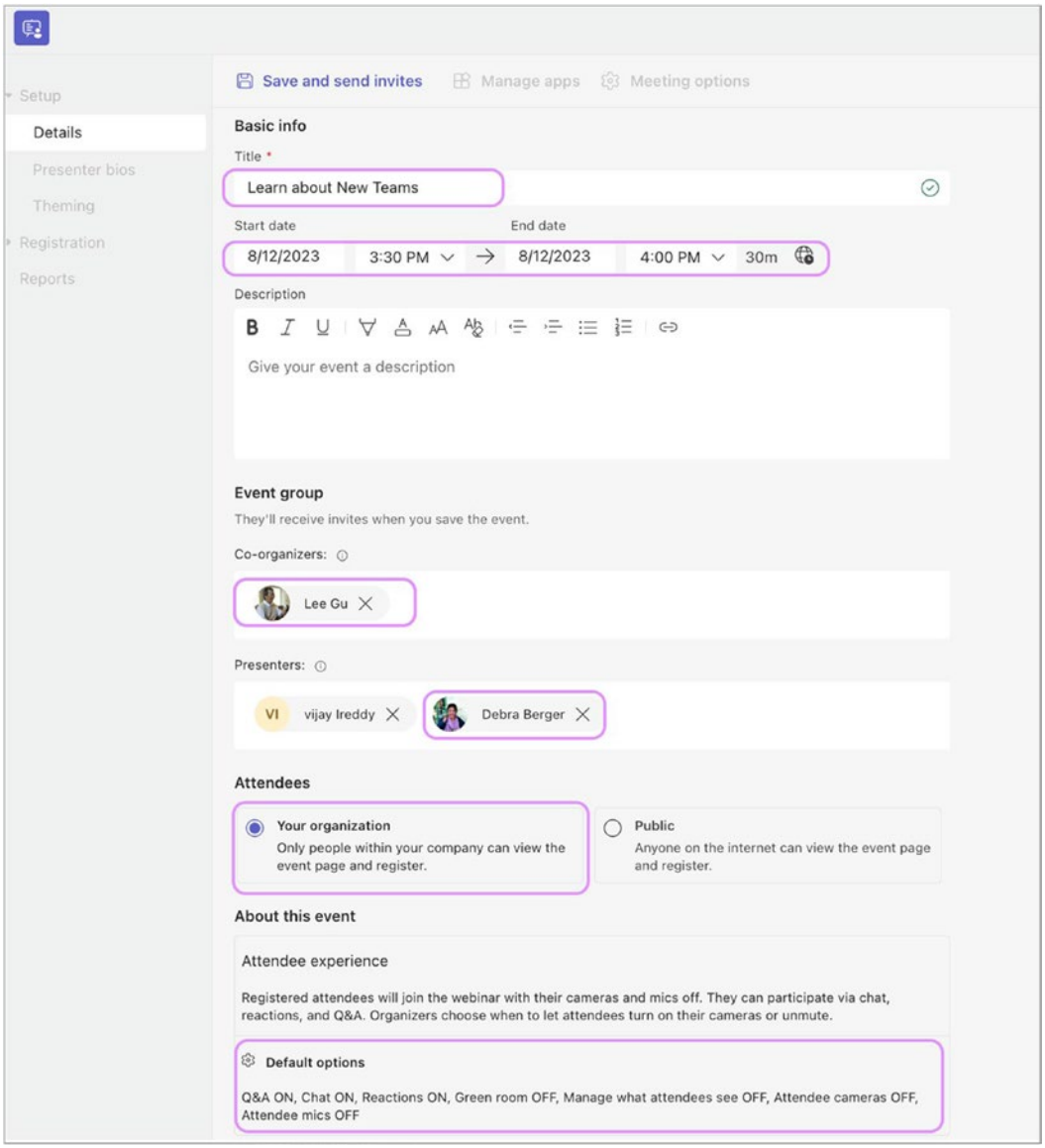

Figure 4-23. *Scheduling a Teams webinar, setup page*

Once the event details are saved, manage apps and meeting options appear on your details screen. As an organizer, I must allow Q&A for all the users and enable a green room as required. These settings can be adjusted in meeting options. As shown in Figure 4-24, click the meeting options, which opens a new browser window with a set of options to adjust. From the list of options, enable Green Room and Q&A and click Save. The detailed meeting options are explained in a later section.

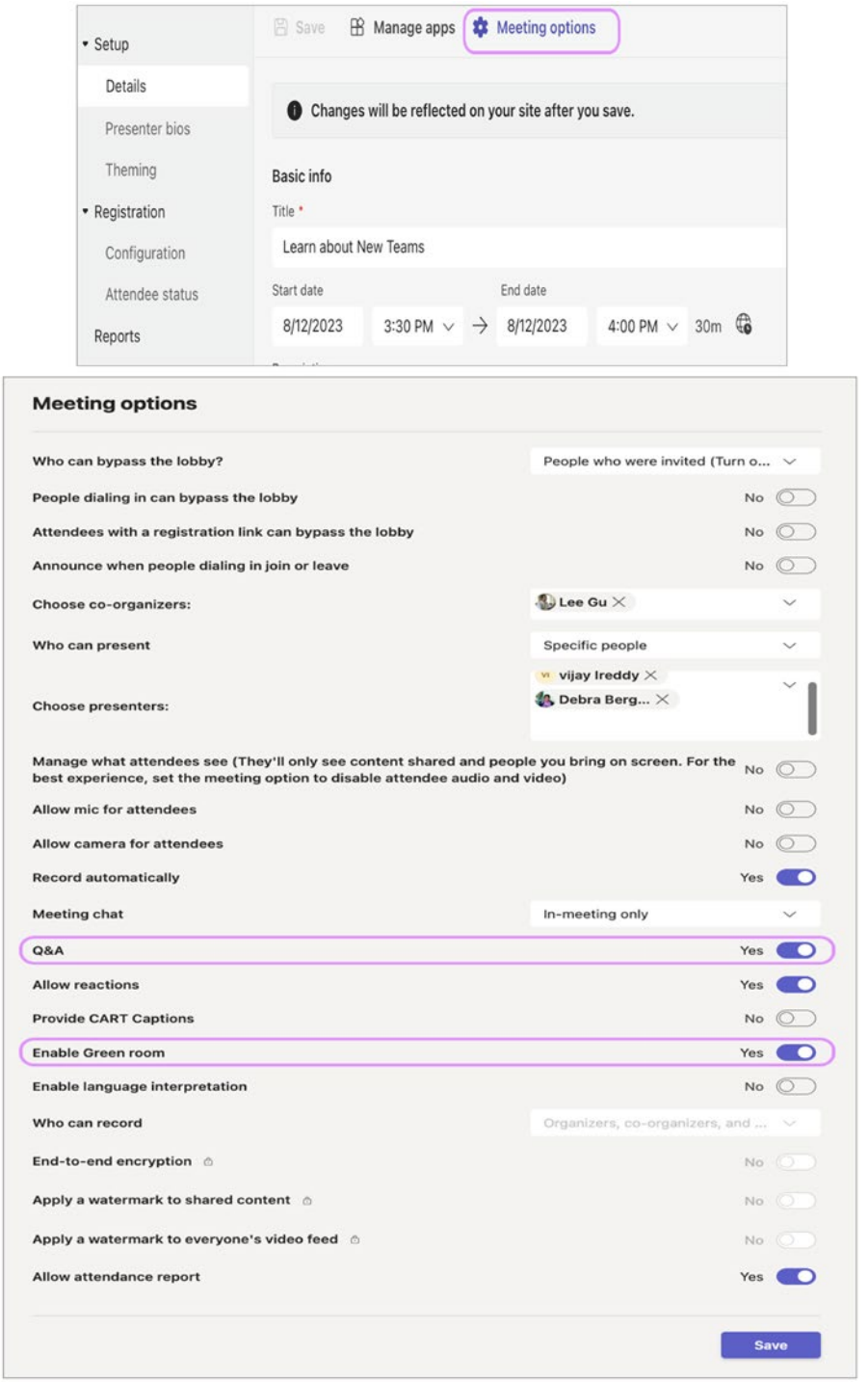

Figure 4-24. *Scheduling a webinar, meeting options*

To update a presenter's bio, return to the setup page and select "Presenter bios." Choose a presenter from the list and click Edit. Add any additional information about the presenter, like bio or photo, and then click Save. For instance, I added more details to a presenter's bio for this event, as shown in Figure 4-25.

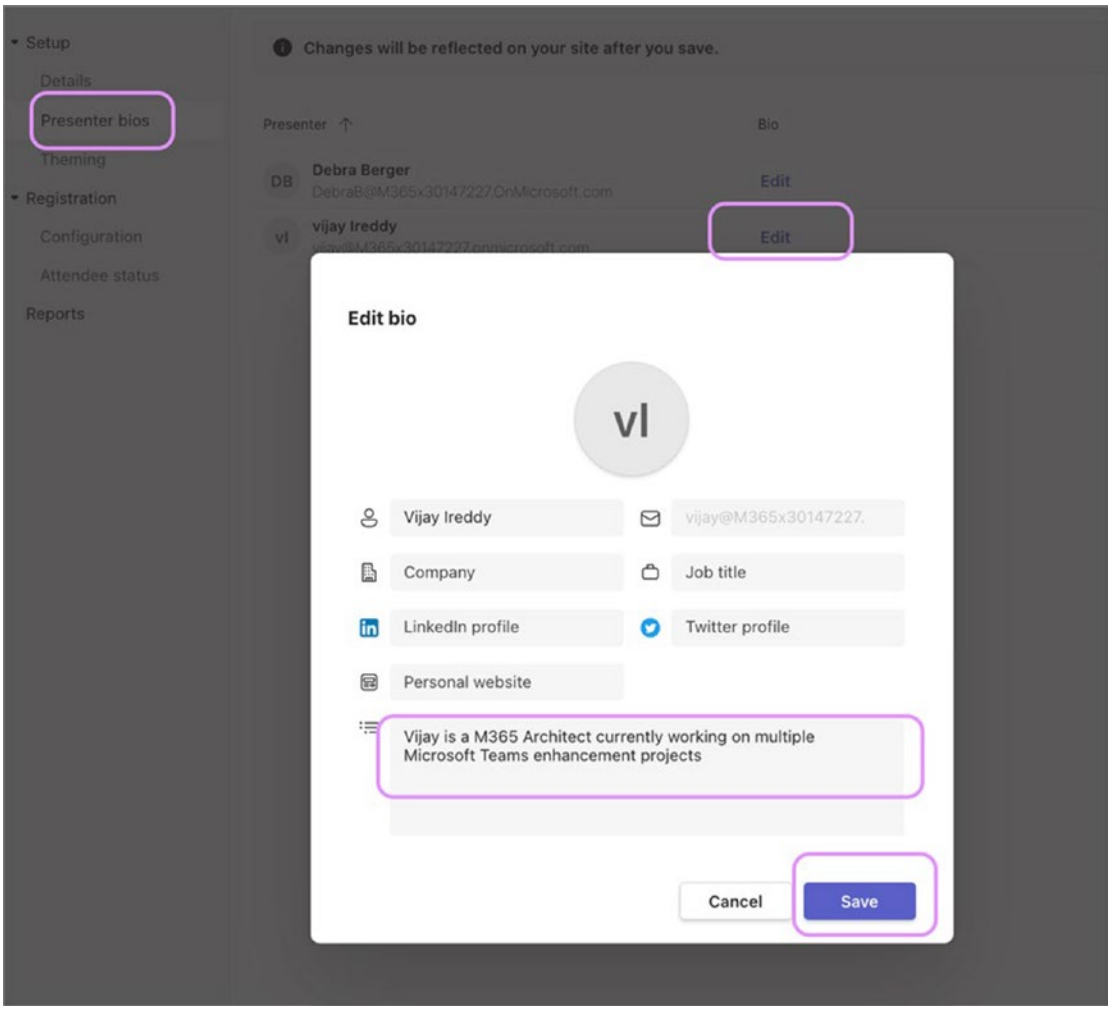

Figure 4-25. *Scheduling a webinar, presenter bio*

Return to the setup section and select Themes. You can choose your organization's banner image and theme color from there. As an organizer, you can customize your banner image, logo, and theme color to personalize the event. The images and theme

colors updated here appear on the registration sites and in the emails sent to the attendees. In my current event, as shown in Figure 4-26, I chose a default theme color, banner image, and logo.

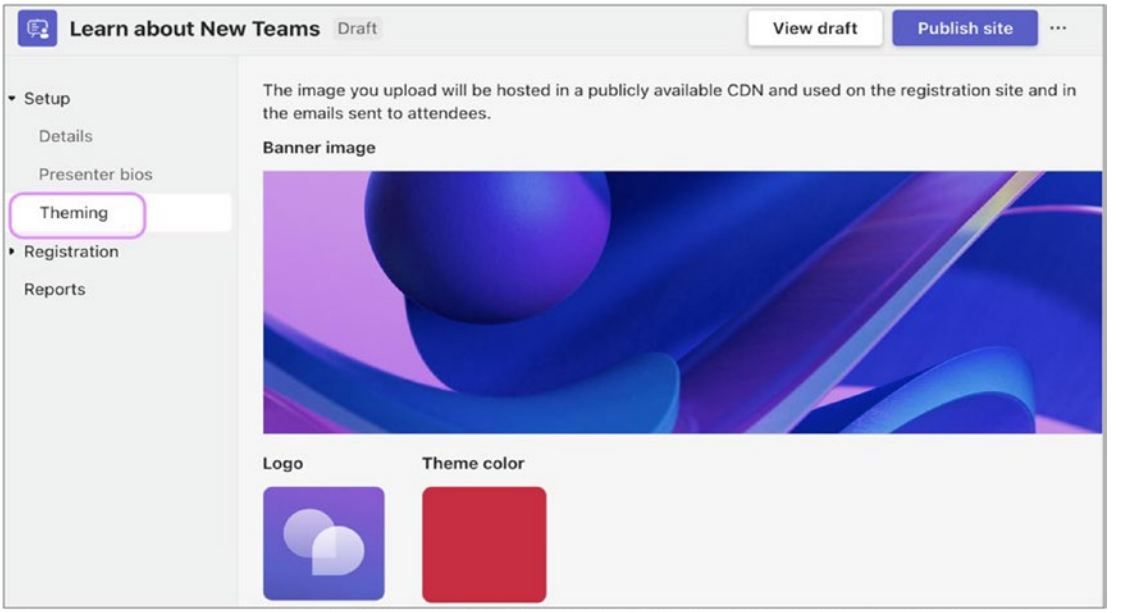

Figure 4-26. *Scheduling a webinar, theming*

Save the themes and click the Registration section. Registration sections contain configuration and attendee status pages.

Teams webinars can host up to 1,000 attendees as of this writing. As an organizer, you can choose the capacity between 1 to 1,000. You can select additional options such as requiring manual approval for all event registrations to manually review each registration and choose to accept or reject, enabling a waitlist for this event, and limiting the registration date. Based on my requirements, I enabled the registration limit for a week, as shown in Figure 4-27.

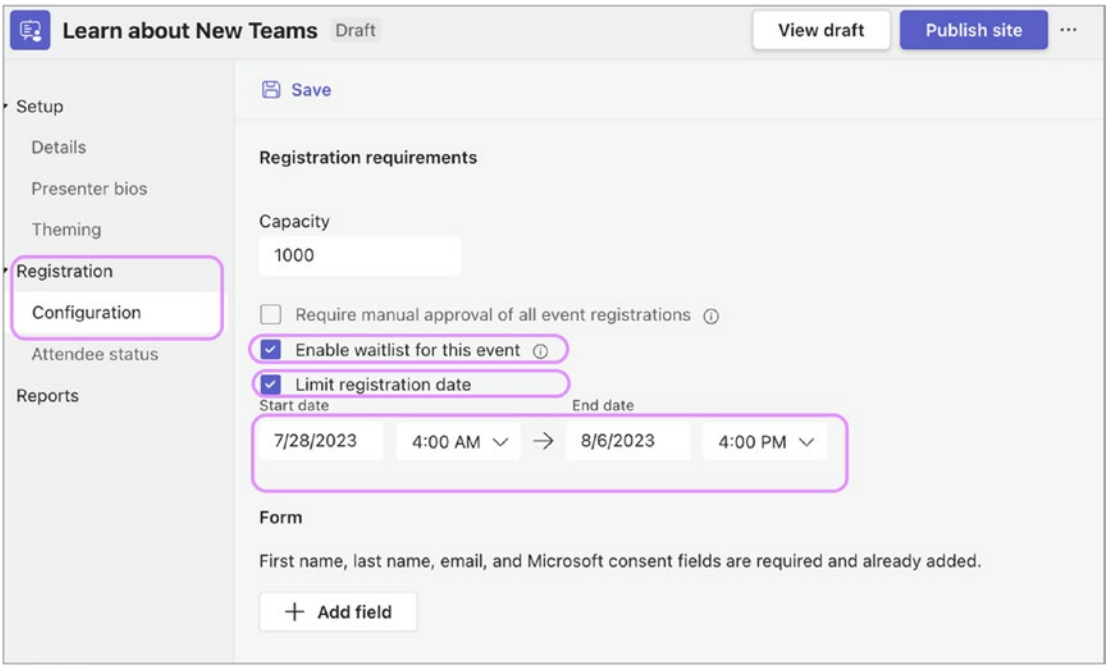

Figure 4-27. *Scheduling a webinar, registration*

The attendance status page displays a roster of users who are either waitlisted, registered, or canceled. You can leave this page for now and come back to it later.

In the reports section, you can find reports related to webinars that can be accessed after the meeting. Typically, the reporting section includes attendance reports, webinar duration, and participant details. Currently, only the organizer has access to these reports.

Validate all the settings and click "Publish site" at the top right. Once the site is published, a sharing link is generated to share the event information with your organization, as shown in Figure 4-28.

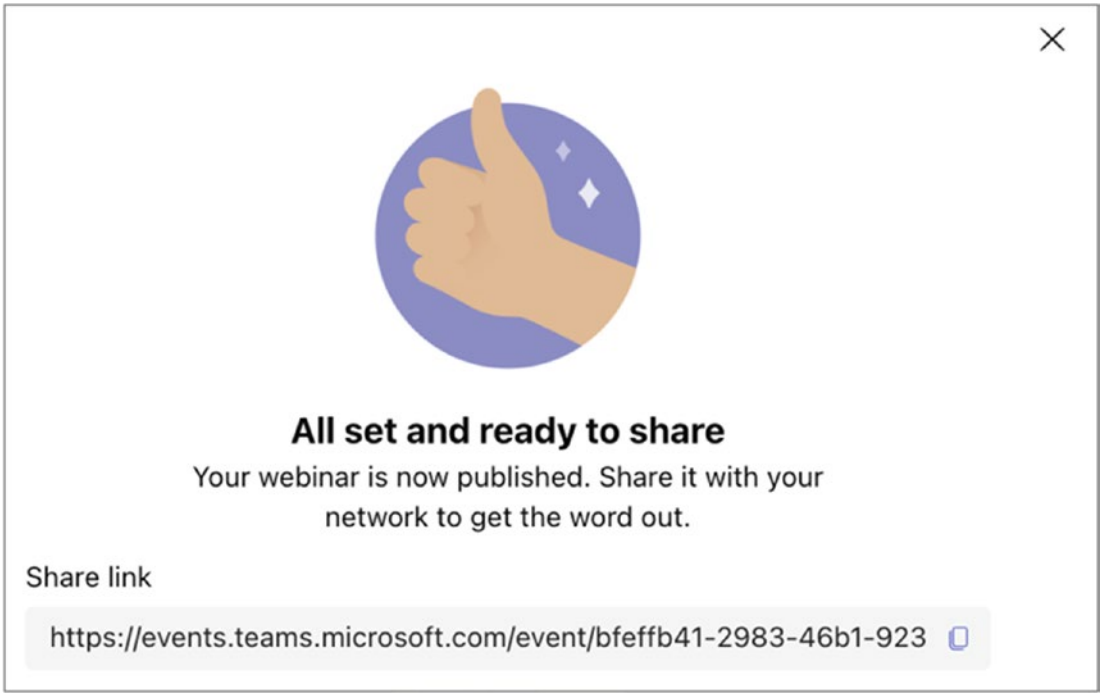

Figure 4-28. *Scheduling a webinar, registration link*

When internal users click the link, they are prompted to sign in with their work account. After successfully signing in, they are directed to a registration site, as shown in Figure 4-29. You can find details about the upcoming event on the website, such as the topic, dates, speakers and bio information, and a registration button. Click the Register button.

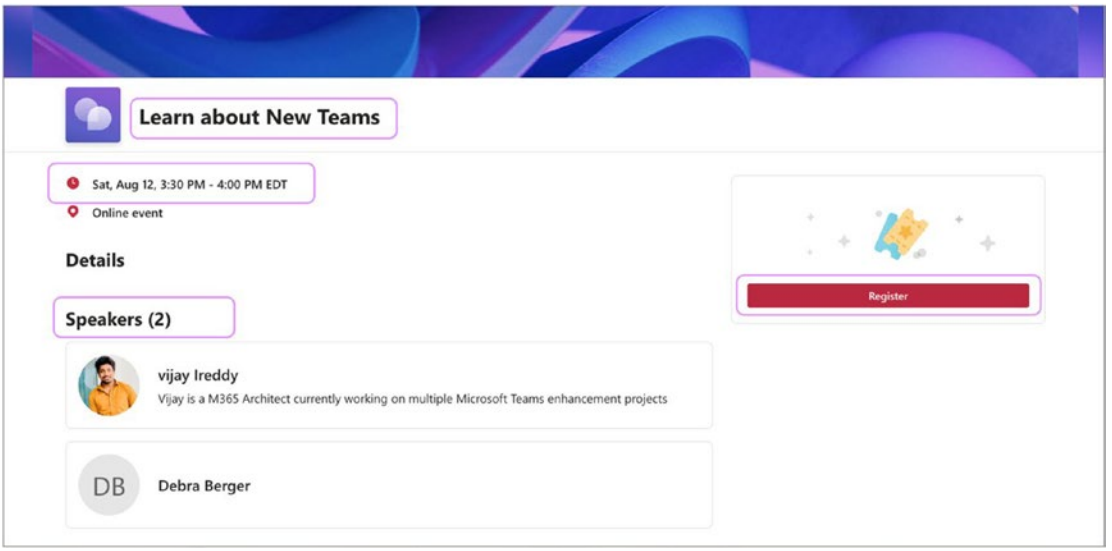

Figure 4-29. *Webinar registration*

If the webinar is public, you are promoted to enter your first name, last name, and email address; if the webinar is internal and you are signed with your M365 account, your information is prefilled. Accept the privacy terms and click Register. Figure 4-30 shows the webinar registration form.

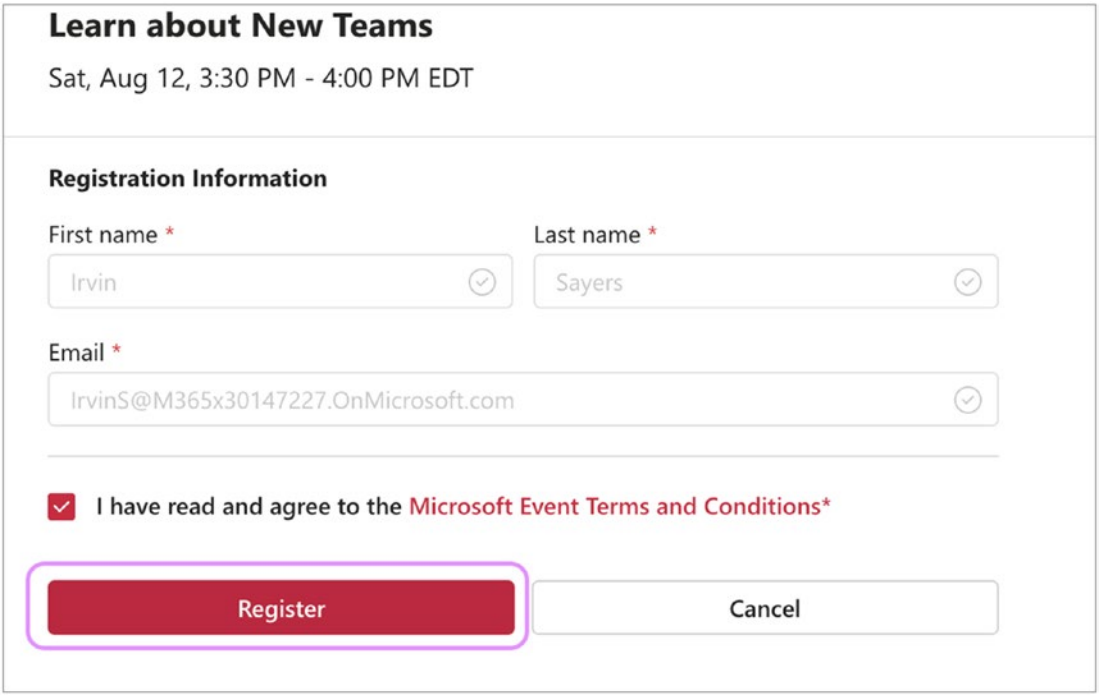

Figure 4-30. *Webinar registration page*

Once the user registers, an email notification with the webinar join-in information is sent to the user's email address, as shown in Figure 4-31. Users can accept the invite in the Teams and Outlook calendars.

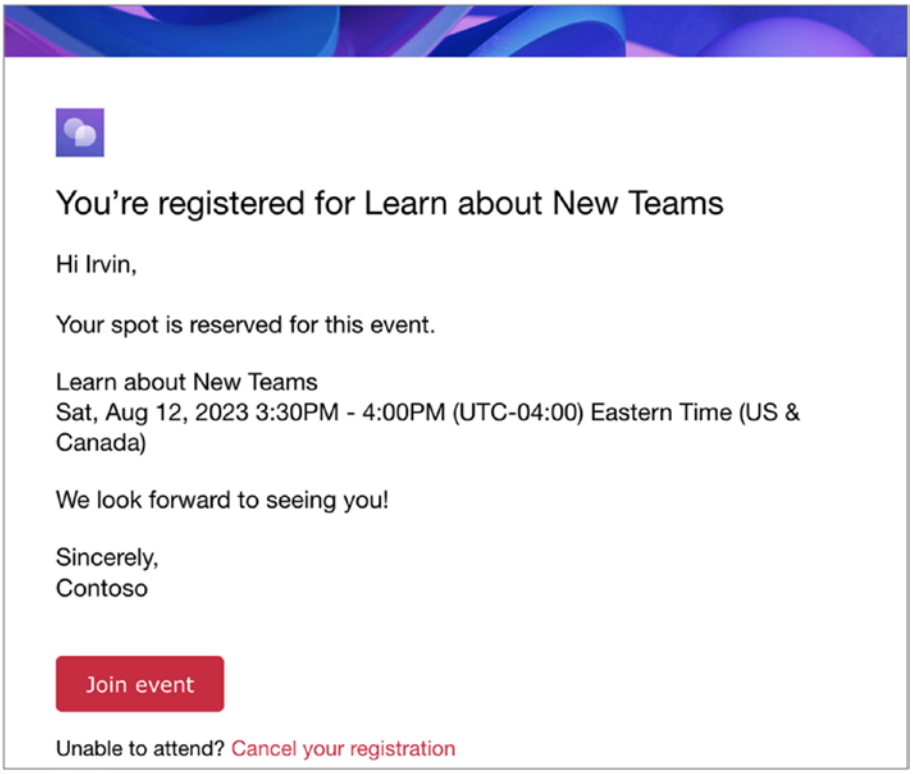

Figure 4-31. *Webinar registration confirmation email*

As an organizer, you can view the list of registered participants by going to the Teams meeting calendar and clicking the scheduled webinar event. Clicking to manage the event opens the scheduling page. To view the list of registered participants, click Registration, then Attendance status, and then Registered, as shown in Figure 4-32.

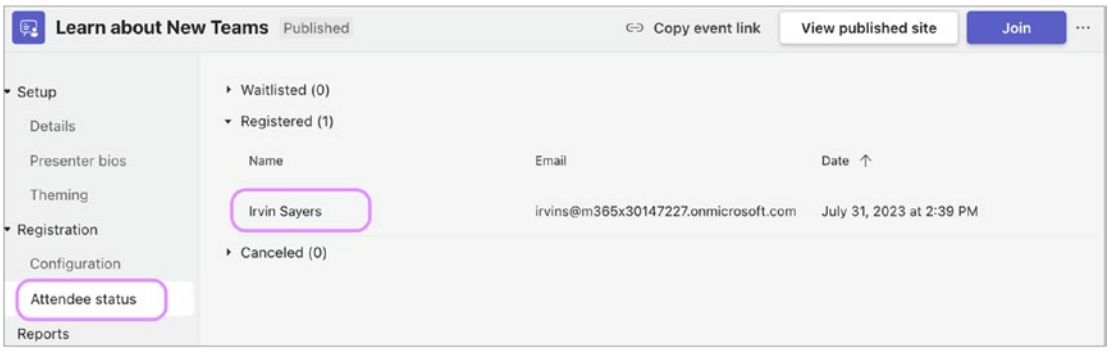

Figure 4-32. *Webinar, attendee registration status*

Presenters can use a green room, a Teams Premium feature, to join a webinar early and adjust audio, video, and content-sharing options. They can also communicate with other organizers and presenters before attendees join. Green rooms are available for the presenters, organizers, and co-organizers. To access the green room for the presenters, ensure the organizer has allowed it in the meeting options for the webinar.

To prepare for a presentation, presenters can use the Join button in their meeting invite to enter the meeting room early and adjust their audio, video, and screen-sharing settings. In the following example, as shown in Figure 4-33, a presenter clicked the meeting link they received when the webinar was scheduled and joined the green room. Once inside, the presenter uploaded a PowerPoint presentation and adjusted their video and background to ensure they were ready to start the webinar. While waiting for the scheduled start time, presenters can interact with attendees using chat and Q&A features and discuss with other presenters and organizers in the green room using audio, video, and screen share.

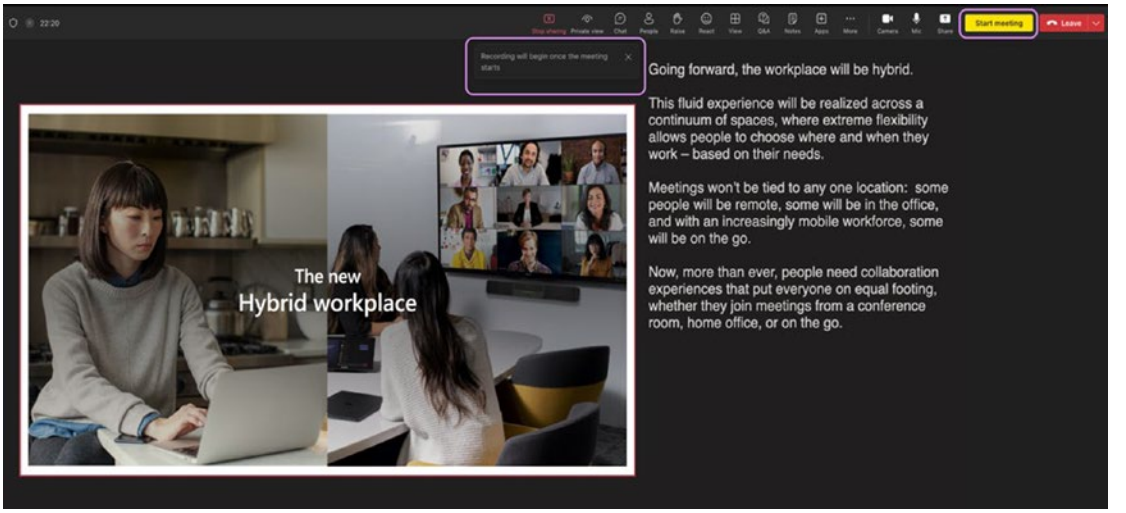

Figure 4-33. *Webinar green room for the presenters*

To start the webinar at the scheduled time, click the "Start meeting" option, as highlighted in Figure 4-33. Once clicked, the recording will begin, and attendees can view the shared screen and the presenter's video.

Meeting Options

Meeting options are available for both Teams meetings and Teams webinars. Additional options become available when an organizer has Teams Premium assigned to them. The following are all the meeting options available. Teams Premium features are indicated by the suffix (P).

- **Sensitivity (P):** Consider using sensitivity labels if your meeting involves sharing confidential information. The details on sensitivity labels are explained in the "Teams Premium" section. The sensitivity labels are preconfigured by the Global admin in the Microsoft Purview Compliance Center. The labels are displayed here for organizers to choose from.
- **Who can bypass the lobby:** If you choose to use the lobby, you and other meeting participants can view a list of people waiting to enter the lobby and decide either to admit or to deny them entry. The Teams administrator configures the default settings for who can bypass the lobby, and Teams meeting organizers can modify these settings.
- **People dialing in can bypass the lobby:** One way to join a Teams meeting is by dialing into the conference bridge, which is explained later in this chapter. To let dial-in users enter the meeting without waiting in the lobby, you can turn on the "People dialing in can bypass the lobby" toggle. The Teams administrator configures the default settings, and the Teams meeting organizers can modify these settings.
- **Announce when people dialing in join or leave:** To receive announcements when people join or leave your meeting via phone (dialing into the conference bridge), toggle on this feature.
- **Choose co-organizers:** To assist in managing a meeting, additional co-organizers may be added. Co-organizers can act as a backup for the organizer to control meeting options and settings. Note that you cannot add an external participant as a co-organizer.

- **Who can present:** With this feature, organizers can assign presenters beforehand or during your meeting to maintain focus and keep things on track. An administrator sets up the default settings, but organizers can modify them if needed. When scheduling a webinar, you can use the option to add presenters. It's important to remember that external participants can be added as presenters in webinars only if the webinar is set to public. However, if these external participants are guests in your organization, they can join, participate, and even present in internal organization webinars.
- **Manage what attendees see (P):** This feature allows the organizer to manage the attendee view for a more streamlined event. The options include enabling attendees to only view the shared screen and participants, all presenters with their presentations, and more**.**
- **Allow mic for attendees:** Turn the "Allow mic for attendees" toggle on or off to change attendee mic permissions.
- **Allow camera for attendees:** Turn the "Allow camera for attendees" toggle on or off to change attendee camera permissions.
- **Record automatically:** To automatically start recording the meeting when a meeting begins, turn on this option. The recording will continue until it's manually stopped, or the meeting ends.
- **Meeting-chat:** By default, all users invited to a meeting can chat before, during, or after the meeting. However, the organizer can choose to limit chat permissions to specific times using this option. This includes during the meeting only or disabling meeting chat altogether.
- **Allow reactions:** During a meeting, attendees can express their emotions by sending live reactions. Turn on "Allow reactions" to allow this feature inside a Teams meeting.
- **Provide CART Captions:** Communication Access Real-Time Translation (CART) is a service that provides instant text translation of speech by trained captioners. By turning on this feature, as a meeting organizer you can provide CART services to the participants

instead of built-in Microsoft Live captions. Please note that a trained captioner is required, and they will need a CART software and CART caption link from the meeting organizer.

- **Enable Greenroom (P):** The green room feature is exclusively available for webinars on Teams Premium. Presenters can use this feature to join a webinar early and adjust audio, video, and content-sharing options. They can also communicate with other organizers and presenters before attendees join. Green rooms are available to presenters, organizers, and co-organizers. Turn on this feature to give green room access to presenters.
- **Enable language interpretation (P):** To have a professional interpreter who can translate the speaker's language into another in real time during your meeting, turn on the "Enable language interpretation" toggle. The professional interpreter will translate the language in real time without disrupting the speaker's original delivery flow. Please note that end-to-end encryption is not available for this feature, and turn off the spatial audio for a more inclusive meeting experience.
- **Q&A:** For active participation during a meeting, you can enable the Q&A feature. This will allow attendees to ask questions, post replies, and even post anonymously.
- **Who can record (P):** When you have a Teams Premium license, you can decide if other internal meeting participants can record the meeting. This feature allows you to choose who is authorized to initiate and manage the recording.
- **End-to-end encryption (P):** Teams Premium offers end-to-end encryption to protect confidential meeting information. Turn this option to encrypt the meeting at the origin and decrypt the data at the destination.
- **Apply a watermark to shared content (P):** This is a Teams Premium feature. When you turn on the "Apply a watermark to shared content" toggle, each meeting participant will see a watermark with their name and email address cast across shared visual content.

- **Allow participants to rename themselves:** To allow participants to modify their display name during a meeting, turn on the "Allow participants to rename themselves" toggle.
- **Allow attendance report:** The attendance reports provide information about the meeting's attendees, such as participants joining and leaving time and the meeting duration. To generate, view, and download attendance reports, turn on the "Allow attendance report" toggle. Please note that only organizers and co-organizers can download the attendance report.
- **Meeting Theme (P):** In Teams Premium, you can use meeting themes to add visuals from your organization, such as logos and brand colors, to your meeting interface. Turn on the Meeting Theme toggle to apply your organization's custom theme for a more personalized, branded meeting experience.

Teams Premium

Due to the global pandemic, meetings and their related tools have become essential for efficient communication among organizations and users. The number of meetings held per day per individual has increased significantly. A survey revealed that organizations have experienced a 252 percent increase in weekly meeting time due to the need to switch through information and solutions, take notes, prepare for meetings, and complete post-meeting work. Organizations have realized that more necessary solutions may be required than meetings such as webinars, virtual appointments, and collaboration tools. As a result of increased security measures, specific confidential meetings require additional precautions to ensure the safety and confidentiality of all participants.

Collaboration and communication became the most needed, and tools like Microsoft Teams helped organizations and users bring them together in a single platform. However, users have struggled to cope with the demanding conditions, resulting in a loss of productivity due to an overload of information from the meetings. By automating and simplifying daily meeting tasks, time spent in meetings can be reduced, and productivity can be increased. To provide advanced meeting capabilities that enable more intelligent, personalized, and secure meetings, Microsoft has

introduced Teams Premium. With Teams Premium, users can focus on what matters most, while AI technology handles the heavy lifting. Teams Premium is an all-in-one integrated solution that supports meetings, webinars, and virtual appointments with advanced protection capabilities for highly sensitive meetings.

Teams Premium Features

Attending meetings is essential to stay informed, but sometimes skipping a meeting can help you focus and be more productive. However, reviewing recordings and transcripts to find relevant information can be time-consuming. Teams Premium can help make meetings more productive by doing the following:

- Automatically generating meeting notes and tasks using AI-powered technology from GPT-3.5 by OpenAI.
- Identifying important moments in a recording such as when a user joined and left the meeting, when a screen is shared, and when a user's name is mentioned.
- Ease navigating through meeting recordings using automatically generated chapters based on the topics.
- Providing live translations for captions in the meeting. If the organizer has Teams Premium, the attendees can use live translations of captions for their meeting, even if they don't have Teams Premium.
- Easily schedule the correct type of meeting with the meeting templates and virtual appointments.
- Create custom brandings in webinars, meetings, and Virtual appointments.
- Create custom together mode scenes for your organization.
- Configure watermarking on participants' videos and shared content to protect meetings and limit who can record.
- Enable end-to-end encryption for online meetings (versus just one-on-one meetings and calls) to help protect the most sensitive conversations.

- Microsoft 365 E5 customers who require the highest level of security can now use their existing Microsoft Purview Information Protection sensitivity labels to apply relevant meeting options automatically.

With your existing M365 subscriptions/0365 subscriptions, you can access the basic virtual appointment experience. Advanced virtual appointments capabilities are available with Teams Premium, which will help you with the following:

- Give customers a personalized experience with pre-appointment SMS reminders, a branded lobby room, and post-appointment follow-ups.
- A dashboard that displays both scheduled and on-demand appointments in one place, with the added feature of chatting with clients before their appointments.
- Gain valuable insights and trends about appointments, such as no-shows and wait times.
- Provide a seamless joining experience for mobile customers without needing users to download the Teams app.

The Teams license offered with M365 and O365 subscriptions provides access to basic webinars and their capabilities, but a Teams Premium license offers additional robust features such as the following:

- Set up a green room for webinar presenters feature to join early and adjust audio, video, and content-sharing options. They can also communicate with other organizers and presenters before attendees join.
- Enable a webinar waiting list to allow additional individuals to register and be automatically placed on the waitlist.
- Limit the day and time when people register.
- Manually approve the registrations to ensure you have the exact group of attendees you need for the webinar event.
- Send reminder emails to the registrants before the webinar.
- Manage attendee views for a more streamlined event.
- Use the RTMP-in feature in webinars.

Availability and Licensing

Teams Premium is available to purchase worldwide through all Microsoft purchasing channels. The tenant must be a commercial, worldwide public sector, EDU, GCC, or nonprofit tenant at general release, and the user must have a 0365/ M365 subscription with Teams to use Teams Premium features.

Teams Premium is a per-user, per-month subscription add-on license that requires each user to have a license assigned to access its functionalities.

Here are a few things to keep in mind regarding current limitations:

- When the meeting organizer has a Teams Premium license, there are some specific meeting and event features that will extend the feature benefit to all meeting attendees. This includes organizational users, guests, and external participants even if they aren't licensed with Teams Premium.
- External participants in virtual appointments don't require a Teams Premium license to benefit from Teams Premium advanced virtual appointments.
- For intelligent recap, all the meeting participants need a Teams Premium license.

Teams Premium for Administrators

Teams Premium features are accessible only through Teams Premium Licensing. As an administrator, you must customize the Teams Premium features to meet your organization's requirements before allowing your users to access them. Once your organization has subscribed to Teams Premium licensing, you can unlock the Teams Premium features. As an administrator, you can then configure the following features.

Using End-To-End Encryption on Meetings Up to 50 Participants

Teams meeting by default have encryption enabled by industry standards. Teams Media traffic is encrypted by Secure RTP, a profile of real-time transport protocol that provides confidentiality and authentication. End-to-end media traffic encryption ensures that the traffic is encrypted at the origin and decrypted at the destination. This ensures that nobody can eavesdrop on real-time conversations, except for the meeting or one-on-one

call or group call participants. Teams offers end-to-end encryption for one-on-one calls and group calls. With Teams Premium, end-to-end encryption is available for meetings with up to 50 participants. As an administrator, you have to enable this feature for your users, By default, end-to-end encryption for meetings is not enabled. You can enable it in the Teams admin center by using an enhanced encryption policy.

As an administrator, you can also control or configure these settings using Microsoft Teams module Powershell commandlets.

```
Set-CsTeamsEnhancedEncryptionPolicy -Identity Global" -MeetingEndToEnd
Encryption DisabledUserOverride
```

You can also use this command to enable end-to-end encryption for one-on-one calls and group calls using the attribute `-CallingEndtoEndEncryptionEnabledType`.

Based on these settings, organizers and co-organizers can turn on end-to-end encryption in the Meeting options for each meeting.

Here are some limitations that administrators and end-user must beware of as of this writing:

- Only audio, video, and video-based screen sharing is end-to-end encrypted. Other features such as apps, avatars, reactions, chat, filters, and Q&A are not end-to-end encrypted.
- During an end-to-end encrypted meeting features including recording, live captions, transcription, together mode, large meetings, large gallery view on desktop, and PSTN are unavailable.
- Desktop clients and mobile clients are supported. Channel meetings can also be end-to-end encrypted. Teams Rooms devices and Surface Hub support is coming soon.
- Other platforms are currently not supported including desktop browser.

Please note that end-to-end meeting encryption can be enforced using meeting templates and sensitivity labels.

Tip Locate the encryption indicator (shield and lock symbol) on your meeting screen to confirm that your meeting is securely encrypted for all the participants. Simply hover over the arrow to view your meeting's unique end-to-end encryption code and ensure that this code is identical for other participants in the meeting.

Adding Watermarks to Meetings

With Teams Premium, users can add watermarks to content shared and participants videos during Teams meetings. However, as an administrator, it's important to note the current limitations of this feature. Currently, watermarks are supported only on Teams desktop clients, Teams mobile clients, and Microsoft Teams Rooms. If you're using any other platform, you will have an audio-only experience when the watermark is used. Watermarks are intended to prevent the unauthorized sharing of confidential information. However, using them during meetings where all participants can directly access the content may not enhance security. Using the combination of watermarks with other Teams Premium protection features like sensitivity labels helps to protect confidential information in meetings. Administrators must also let end users know the limitations of other meeting features when watermarks are turned on. The following meeting features are turned off when watermarks are enabled:

- Meeting recording, including automatic recording and who can record
- Large gallery
- Together mode
- PowerPoint Live
- Whiteboard
- Content from camera

To turn on watermark features from the Teams admin center, follow these steps:

1. Go to Teams Admin Center ➤ Meetings ➤ Meeting Policies.
2. Select the policy to update.

3. To configure the watermark for the attendee video, set Watermark Video to On.
4. To configure the watermark for content shared on the screen, set "Watermark shared content" to On.
5. Use the preview to see how the watermark will look on desktop and mobile devices.
6. Click Save.

You can also turn the watermark on or off by using these PowerShell commands:

```
Set-CsTeamsMeetingPolicy -Identity Global -AllowWatermarkFor
CameraVideo $True
Set-CsTeamsMeetingPolicy -Identity Global -AllowWatermarkFor
ScreenSharing $True
```

Please note that the watermark for meetings can be enforced using meeting templates and sensitivity labels.

Adding Sensitivity Labels

In the previous section, we discussed meeting options. The Teams administrator configures the default settings for meeting options, and the organizer can modify them for each meeting depending upon the meeting requirement. Though this is useful, there are times when the admin needs to ensure that meetings are secured with the admin's configured features, and organizers must keep them the same. With Teams Premium, sensitivity labels can be used to enforce these meeting settings. Microsoft Purview Information Protection offers sensitivity labels that enable you to classify and protect your company's data. Sensitivity labels are usually assigned to documents and emails; in addition to these two, using Teams Premium, sensitivity labels can now be applied to meetings. Sensitive labels protect meeting invites and responses created from Outlook and Teams Calendar and protect Team meetings and chat.

- Meeting organizers can apply sensitivity labels to the Teams meeting invites scheduled in Outlook and Teams. The recipients in your organization will see the sensitivity label.
- All the meeting settings applied to the sensitivity label are enforced when a meeting begins, and internal users can see the labels during the meeting.

The following are meeting settings that you can apply with a sensitivity label:

- Automatically record
- Encryption for meeting video and audio
- Prevent copy of meeting chat
- Prevent or allow copying of chat contents to the clipboard
- Watermark for screen sharing and participants' video
- Who can bypass the lobby
- Who can present
- Who can record

Sensitivity labels can also be applied to Teams meetings using Teams meeting templates. Microsoft recommends configuring and protecting meetings with three tiers of protection. The appropriate level of protection depends on each organization's compliance needs, ranging from no requirements to highly sensitive ones. Microsoft provides basic recommendations for three tiers: baseline protection, sensitive protection, and highly sensitive protection. As an administrator, you can start with these tiers and adjust the configurations to meet the organization's needs. Here are some examples:

Features	Baseline	Sensitive	Highly Sensitive	Highly Sensitive Presentation
Allow camera for attendees	On	On	On	Off
Allow mic for attendees	On	On	On	Off
Apply a watermark to everyone's video feed	Off	Off	On	On
Apply a watermark to shared content	Off	Off	On	On

(*continued*)

Features	Baseline	Sensitive	Highly Sensitive	Highly Sensitive Presentation
End-to-end encryption	Off	Off	On	On
Manage what attendees see	Off	On	On	On
Meeting chat	On	On	In-meeting only	Off
People dialing in can bypass the lobby	Off	Off	Off	Off
Prevent copying chat content to clipboard	Off	Off	On	On
Record meetings automatically	Off	Off	Off	Off
Who can bypass the lobby?	People in my organization, people in trusted domains, and guests	People who were invited	Only me and co-organizers	Only me and co-organizers
Who can present	People in my organization and guests	People in my organization and guests	Only organizers and co-organizers	Only organizers and co-organizers
Who can record	Organizers and presenters	Organizers and co-organizers	Disabled due to watermarking	Disabled due to watermarking

These settings can be managed with a combination of sensitivity labels, meeting templates, and admin settings. Creating a sensitivity label is not covered in this book. Please refer to the following website to learn and configure sensitivity labels for meetings:

https://learn.microsoft.com/en-us/microsoftteams/configure-meetings-three-tiers-protection

Preventing Copying Meeting Chats

If your organization has compliance requirements to prevent copying meeting chats, Teams Premium can make it possible. Administrators can use a sensitivity label to block the copying of chat content. When this label is applied to channel meetings, the label prevents copying chat to the clipboard for all channel chats, even outside channel meetings. For nonchannel meetings, it's enforced only for meetings.

The methods supported to prevent copying chat are as follows:

- Select the text and then right-click and select Copy; or press Ctrl+C.
- Forward messages.
- Share to Outlook.
- Copy link.

Note Copying using developer tools, third-party apps, or screen captures won't be prevented.

Using Organization-Customized Backgrounds

Custom backgrounds are the images that can be applied to the background of a user's video feed in a Teams meeting. As an admin, you can create custom backgrounds based on your organization themes and make them available for your users to use in Teams meeting at any point in time.

To make custom backgrounds available for your Teams Premium licensed users, you must configure a customization policy in the Teams admin center. Figure 4-34 shows the customization policy. To configure it, follow these steps:

1. Go to the Teams admin center, select Meetings and then Customization Policy.
2. Edit an existing policy or create a new policy by clicking Add.
3. Name the customization policy.
4. Turn on "Use background images for my organization."
5. Click Add.

6. Upload a background image.
7. Click Save.

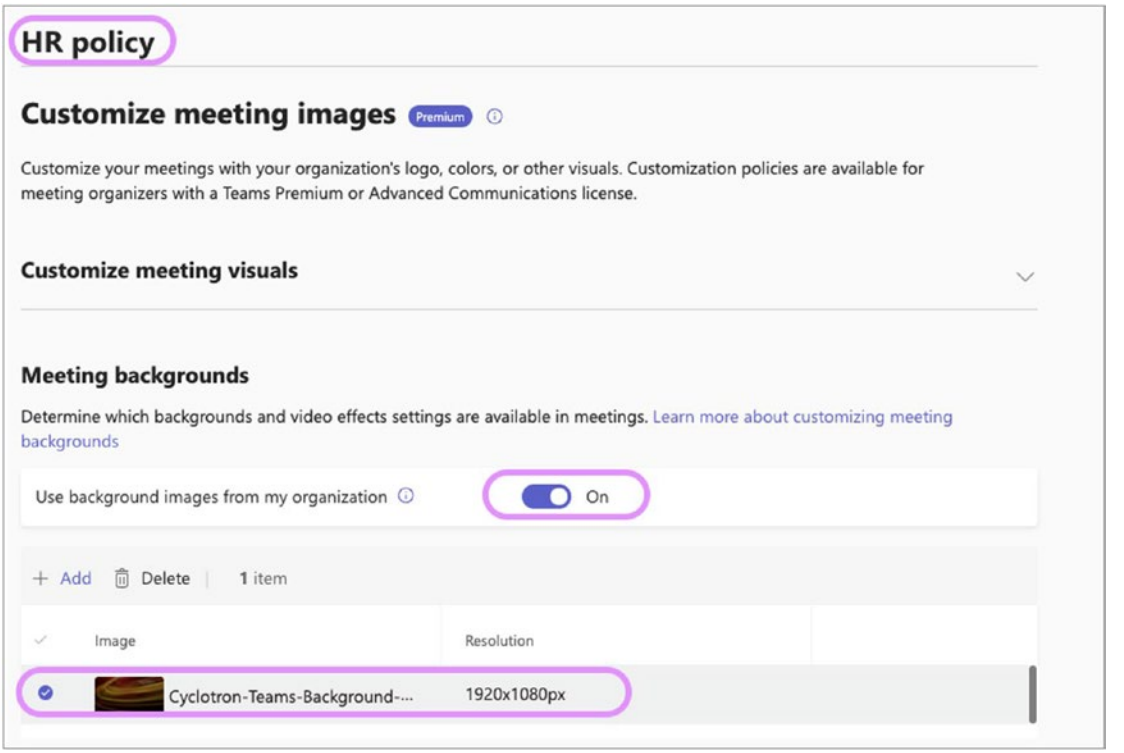

Figure 4-34. *Customization policy*

Here are the current limitations for the uploads:

- PNG and JPEG image formats for their images
- Images with minimum dimensions of 360 pixels × 360 pixels
- Images with maximum dimensions of 3840 pixels × 2160 pixels
- A maximum of 50 custom background images

Using organization-customized Together mode scenes

With Teams Premium, users can create personalized "together mode scenes" through the Teams Developer Portal. Once created, these scenes can be shared as an app within Microsoft Teams. As an administrator, you must permit users to upload custom apps by managing app permission policies. Refer to this link to create custom-together mode scenes for your meetings:

https://learn.microsoft.com/en-us/microsoftteams/platform/apps-in-teams-meetings/teams-together-mode

Using Organization-Customized Meeting Templates

Meeting templates are available with Teams Premium. Using a meeting template, an administrator can customize the meeting options that the meeting organizer controls typically. Meeting templates ensure a consistent meeting experience for users and also ensure compliance by not allowing organizers to change a few settings. Administrators can lock the template option features so that the meeting organizer can't change it and can unlock others so that meeting options can be changed. Figure 4-35 shows the lock settings. Meeting templates can control the following meeting options:

- Allow mic and camera for attendees
- Allow reactions
- Announce when people dialing in join or leave
- Enable watermark for screen share and for video
- End-to-end encryption
- Lobby
- Manage what attendees see
- Meeting chat
- Q&A
- Recording
- Sensitivity label

The "Sensitivity Label" section mentioned that combining meeting templates with sensitivity labels can help enforce meeting protection. It's important to note that if a meeting invitation has a sensitivity label assigned and meeting templates are used, the meeting options enforced by the sensitivity labels will always take priority. Meeting templates are the most effective way to manage meeting options and ensure compliance for organizations without a Microsoft Purview Compliance Center subscription.

To configure meeting templates, follow these steps:

1. Go to the Teams admin center, click Meetings, and click Meeting Templates.
2. By default, you will see a virtual appointment template. Click Add for a new template.
3. Add a name and description for the new template.
4. Configure the template meeting settings based on your organization's needs.
5. Use the Lock icon to lock any meeting settings that organizers cannot change.

Figure 4-35. *Meeting templates- Lock a setting*

6. After validating all the settings, click Save.

Now that the meeting template is created, you must assign it to the users. Meeting templates can be assigned to the users using the meeting template policies. All meeting templates are available in the Global Meeting template policy by default.

Once the policies get synced, users can use these templates to create meetings. The customized meeting templates are available in the Teams calendar. To use a customized meeting template, follow these steps:

1. Go to the Teams application and click the calendar.
2. Click the down arrow located new to "New meeting."
3. Click the template.
4. The template launches with enforced meeting option settings.

Seeing Organization-Customized Branding

With Microsoft Teams Premium, administrators can create personalized meeting themes that showcase their organization's branding, including their logo, images, and theme colors. Meeting themes are assigned in customization policies, and these policies are assigned to the users. To set customization policies, follow these steps:

1. Go to the Teams admin center, select Meetings, and select Customization Policy.
2. Create a new policy by clicking Add.
3. Add a name to the customization policy.
4. Click Add Theme.
5. Upload the image, logo, and choose the theme color.
6. Click Apply.
7. Turn on "Allow organizer to control meeting theme."
8. Click Save.

The following are the locations where the branding can be found:

Themes	Join Launcher	Meeting Pre-Join	Meeting Lobby	Meeting Stage
Logo	No	Yes	Yes	No
Image	No	Yes	Yes	No
Color	Yes	Yes	Yes	Yes

Teams Phone System Planning

Microsoft Teams provides multiple capabilities, such as chat, audio and video calls, meetings, content sharing, phone calls to external numbers, etc. One feature allows you to use the Teams call interface to make outbound phone calls to internal users, and extensions, and connect with the PSTN. The Microsoft Teams technology that allows call control and PBX capabilities is called the Phone System.

The Teams Phone System permits users to place and receive phone calls, transfer calls, and mute or unmute calls. Teams calling provides multiple features, including call answering and initiating (by name and number) with an integrated dial pad, call holding and retrieving, call forwarding and simultaneous ringing, call history, voicemail, and emergency calls. End users can also use different devices to establish calls, including mobile devices, headsets connected to a computer, and IP phones. This section covers the Teams Phone System, including Direct Routing, Calling Plans, phone number management, and phone call routing policies.

Microsoft Teams natively supports audio and video calls and meetings using a VoIP data network without special licensing. Teams with a Phone System license (add-on) enables calls to landlines and mobile phones by connecting the Teams Phone System to the PSTN. Teams Phone System PSTN connectivity can be established in four ways:

- **Teams Direct Routing:** You can connect your existing on-premises PBX infrastructure with the Office 365 Phone System.
- **Teams Calling Plan:** Using the Calling Plan, users can make and receive phone calls directly through Office 365 Phone System as a telephony provider by purchasing a Microsoft Calling Plan (domestic or domestic and international) for Office 365.
- **Teams Operator Connect:** You can use Microsoft Teams to make and receive calls with Teams-certified telephony providers.
- **Teams Phone Mobile:** Microsoft Teams Phone Mobile allows users to use the same phone number for both their mobile service and desk lines/work. Essentially, their SIM-enabled phone number becomes their Teams phone number.

Teams Phone PSTN Call Flow

As an administrator, it's important to understand the signaling and media path for PSTN calls when troubleshooting. Let's examine how signaling and media call flow works when User A from the Cyclotron tenant makes a PSTN outbound local call from the United States by dialing a 10-digit number from their Microsoft Teams client.

In Microsoft Teams, 10-digit calls are converted to E.164 standard by native or user-defined dial plans. The Teams service only recognizes calls in E.164 format, regardless of the digits dialed. The call is routed to the nearest Microsoft Azure front door. The Teams

service performs a reverse number lookup in its database to validate if the number is assigned to a user in the tenant. If not, the Teams service checks if User A has permission to dial out to PSTN numbers. Checkups depend on PSTN connectivity. For Calling Plans, checkups include domestic Calling Plan licenses and dial-out policies. For Operator Connect, checkups include Operator Connect service and dial-out policies. For Teams phone mobile, it validates the Teams Phone Mobile service and dial-out policies. Finally, for Direct Routing, it checks the Online Voice Routing policy and dial-out policies, and if the user is validated to dial outbound, calls are routed to the PSTN carriers.

If you are using the Calling Plans feature, the calls are forwarded to Microsoft's underlying PSTN carrier serving that location. For Operator Connect and Teams Phone Mobile, the calls are sent to the operator's trunk. For Direct Routing, the Teams service checks sends the call to the PSTN gateway associated with the online voice routing policy assigned to User A. Note that the Online voice routing policy must be associated with a PSTN usage that is routable to the PSTN gateway and the session border controller (SBC). The PSTN gateway routes the call to the SBC, and it's forwarded to the PSTN carrier on the defined trunk. The call rings at destination (User B), and User A can hear the early media on their Teams client. Once User B picks up the call, media kicks in.

For Direct Routing, the media flows back through the PSTN network, Direct Routing SBC, Microsoft Phone System, and finally Teams client. For other connectivity models, the media flows through PSTN network, the Microsoft Phone system, and the Teams client. In Direct Routing scenarios, the Teams service bypasses the media when ICE Lite is configured on the SBC. The ICE protocol is used to bypass the media, and User A's Teams client must have direct connectivity with the SBC's external IP address. In such cases, the media flows through the PSTN network, SBC, and the Teams client. When the call is ended by either party (User A or User B), the call termination process follows the reverse path based on the PSTN connectivity models, traversing the same components until the call is fully terminated.

When User A receives an inbound call from User B, the PSTN carriers route the call to the Teams Phone system. In Direct Routing scenarios, calls are sent to SIP trunk/E1/P1 configured on the SBC and routed to the Microsoft Phone system PSTN gateway using the defined trunk in E.164 format. The Teams service performs a reverse number lookup against the database to validate if the number is assigned to any user. If the number is assigned to User A, the call is forwarded to all Teams clients. Like outbound calls, once User A picks up the call, the media kicks in.

For Direct Routing, the media flows back through the PSTN network, Direct Routing SBC, Microsoft Phone System, and finally Teams client. For other connectivity models, the media flows through the PSTN network, the Microsoft Phone system, and the Teams client. In Direct Routing scenarios, when the media bypass is configured, the media flows through the PSTN network, SBC, and Teams client. When the call is ended by either party (User A or User B), the call termination process follows the reverse path based on the PSTN connectivity models, traversing the same components until the call is fully terminated.

Note For PSTN calls, clients use UDP 50000–50019 for media traffic and 1024–65535 for SIP signaling.

Configuring and Managing Teams Direct Routing

Direct Routing allows a Teams admin to connect a supported SBC to Microsoft Phone System to enable voice calling features (PSTN calls). For example, you can configure on-premises PSTN connectivity with an SBC to send and receive phone calls from a user with the Teams client. Direct Routing is the other way to connect to the PSTN, where customers interface existing PSTN services to Teams through on-premises SBCs.

Suppose your organization has an on-premises PSTN connectivity solution, such as the Cyclotron organization using the Ribbon SBC to connect an AT&T SIP trunk. In that case, Direct Routing enables you to connect a supported SBC to the Microsoft Phone System. Direct Routing allows you to use any PSTN trunk with your Microsoft Phone System and configure interoperability between customer-owned telephony equipment, such as a third-party PBX, analog devices, and the Microsoft Phone System.

Figure 4-36 shows on-premises PSTN connectivity using the Direct Routing capability with a Microsoft Teams client.

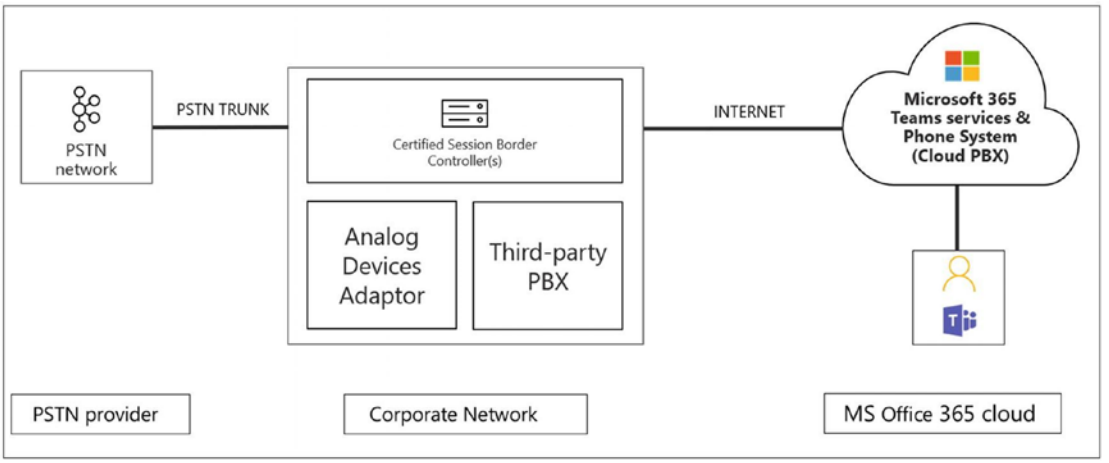

Figure 4-36. *Teams Direct Routing connectivity*

Refer to Chapter 2, which covers Direct Routing requirements, configuring Direct Routing with Windows PowerShell commands, and best practices.

Configuring and Customizing Online PSTN Gateway for Microsoft Teams Direct Routing

One of the main tasks for Teams Phone System Direct Routing configuration is to onboard an on-premises SBC to the Microsoft Teams cloud tenant. To create a new SBC configuration that describes the settings for the peer entity, use the following PowerShell command to create a new Online PSTN gateway:

```
New-CsOnlinePSTNGateway -Fqdn sbc1.cyclotron.com -SipSignallingPort
5061 -MaxConcurrentSessions 100 -Enabled $true
```

This command shows SBC FQDN, SIP signaling port, maximum concurrent sessions, and enabled status; the remaining parameters will stay at their defaults.

When you create an online PSTN gateway, each configuration includes individual settings for an SBC. The SBC configuration setting includes the SIP signaling port, whether media bypass is enabled on this SBC, forward P-Asserted-Identity (PAI), whether the SBC will send SIP options, specifying the limit of maximum concurrent sessions, and much more. One of the important settings that Teams admins can configure for SBC is to set `-Enabled` to `$true` or `$false`. When set to `$false`, the SBC will continue to handle existing calls, but all new calls will be routed to another SBC in a route (if there is one that lasts).

The following is the detailed information for the Teams Direct Routing SBC parameters that can be customized.

-Identity

Every SBC has a unique name that is used for identifying the SBC. When creating a new SBC, the identity is provided through the `-FQDN` parameter. If the parameter is not defined, the identity will be copied from the `-FQDN` parameter, which means that an identity parameter is not mandatory.

For example, this command doesn't define identity but is copied from the Fqdn switch. That means identity is optional.

```
New-CsOnlinePSTNGateway -Fqdn sbc1.cyclotron.com -SipSignallingPort
5061 -MaxConcurrentSessions 100 -Enabled $true
```

-InboundPSTNNumberTranslationRules

While creating an SBC, as an admin you can set the inbound PSTN number translation rules that are applied to PSTN numbers in an inbound direction, as well as in inbound calls coming from carriers to the Teams user.

-InboundTeamsNumberTranslationRules

While creating an SBC, you can set the inbound Teams number translation rules that are applied to Teams numbers (the called numbers) in an inbound direction. This switch gives an ordered list of Teams translation rules that apply to inbound Teams numbers.

-OutboundPSTNNumberTranslationRulesList

While creating an SBC, an admin can set the outbound PSTN number translation rules that are applied to PSTN numbers (the called numbers) in the outbound direction. This switch assigns an ordered list of Teams translation rules that apply to outbound PSTN numbers.

-OutboundTeamsNumberTranslationRulesList

While creating an SBC, you can set the outbound Teams number translation rules applied to Teams numbers (the calling numbers) in the outbound direction. This switch assigns an ordered list of Teams translation rules that apply to outbound Teams numbers.

-SipSignalingPort

This parameter is the listening port used to communicate with Direct Routing services using the Transport Layer Security (TLS) protocol. It must be a value between 1 and 65535. Microsoft recently changed the spelling of this parameter from `SipSignallingPort` to `SipSignalingPort`.

-Fqdn

The fully qualified domain name (FQDN) is the name of the SBC. The online PSTN gateway command has only 63 characters to set the FQDN of an SBC, and it is copied automatically to the identity of the SBC field.

-ForwardCallHistory

This command switch indicates whether call history information will be forwarded to the SBC. If enabled, the Office 365 PSTN Proxy sends two headers: `History-info` and `Referred-By`. The default value for this parameter is `$False`.

-ForwardPAI

If the SBC config setting includes `ForwardPAI` as `True`, then for each outbound to SBC session, the Direct Routing interface (public IP) will report in P-Asserted-Identity fields the TEL URI and SIP address of the user who made a call. This is helpful when you as a Teams admin set the identity of the caller to Anonymous or a general number of the organization; however, for invoicing reasons, the real identity of the user is required, so the PAI setting controls the forward PAI parameter in an online gateway configuration.

For example, the command looks like this:

```
New-CsOnlinePSTNGateway -Fqdn sbc1.cyclotron.com -SipSignallingPort
5061 -MaxConcurrentSessions 100 -ForwardPAI $true -Enabled $true
```

-Enabled

This parameter is used to enable SBC for outbound calls. Also, this setting allows admins to control the SBC state as active or passive. Admins can use this setting to temporarily remove the SBC from service as it is being updated undergoing maintenance.

Note If an admin forgets to set this parameter as true, by default SBC will be created as disabled. The default value is `-Enabled $false`.

Here's an example:

```
New-CsOnlinePSTNGateway -Fqdn sbc1.cyclotron.com -SipSignallingPort
5061 -MaxConcurrentSessions 100 -Enabled $true
```

-ExcludedCodecs

This parameter excludes some codecs when media is being negotiated between the media proxy and the SBC.

-FailoverResponseCodes

Failover response codes are key parameters that have default codes set as (408, 503, and 504). That means you can configure a custom response code or use the default. For example, If Teams Direct Routing receives any 4xx or 6xx SIP error code in response to an outgoing invite, the call is considered completed by default. In the context of an outgoing call from a Teams client to the PSTN number, the call flow will be Teams Client ➤ Direct Routing ➤ SBC ➤ PSTN (telephony network). Setting the SIP codes in this parameter forces Direct Routing, on receiving the specified codes, to try another SBC (if another SBC exists in the voice routing policy of the user).

-FailoverTimeSeconds

This parameter has a default value of 10. Outbound calls not answered by the PSTN gateway within 10 seconds are routed to the next available trunk; if there are no additional trunks, the call is automatically dropped. In an organization with slow

networks and slow gateway responses, that could potentially result in calls being dropped unnecessarily. As an admin, you can decide what failure time should be set for the SBC.

-Force

The `Force` switch specifies whether to remove warning and confirmation messages. It can be useful in scripting to suppress interactive prompts. If the `Force` switch isn't provided in the command, you are prompted for administrative input if required.

-ForwardPai

This switch suggests whether the P-Asserted-Identity (PAI) header will be forwarded along with the call. The PAI header provides a way to verify the identity of the caller. The default value is `$False`. Setting this parameter to `$true` will give the from header anonymously, in accordance with RFC5379 and RFC3325.

-GatewaySiteLbrEnabled

This is another critical setting to enable the SBC to report assigned site location, which is used for location-based routing (LBR). When the SBC has a gateway site and the LBR-enabled parameter is enabled (`$True`), the SBC will report the site name defined by the Teams admin. On an incoming call to a Teams user, the value of the site assigned to the SBC is compared with the value assigned to the user to make a routing decision. The parameter is mandatory for enabling LBR, and the default value for this parameter is `$False`.

-GenerateRingingWhileLocatingUser

This parameter is applicable only for Direct Routing in nonmedia bypass mode. Occasionally inbound calls from the PSTN to Teams clients can take longer than expected to be established. This can happen for a variety of reasons. When this occurs, the caller might not hear anything, the Teams client doesn't ring, and some telecommunications providers might terminate the call. This parameter helps to avoid unexpected silences that can occur in this scenario. Once this parameter is enabled for inbound calls from the PSTN to Teams clients, a unique audio signal is played to the caller to indicate that Teams is in the process of establishing the call.

-MaxConcurrentSessions

The alerting system uses this parameter. When any value is set, the alerting system will generate an alert to the Teams admin when the number of concurrent sessions is 90 percent or higher than this value. If the parameter is not set, alerts are not generated. However, the monitoring system will report the number of concurrent sessions every 24 hours.

-MediaBypass

The media bypass parameter indicates that if the SBC supports media bypass, Teams admins can use it for the SBC. Media bypass is useful for sending media directly to SBC from the Teams client instead of sending media through the Teams service. Media bypass increases call quality, so its use is recommended wherever possible.

-SendSipOptions

This parameter describes if an SBC will or will not send SIP options messages. If disabled, the SBC will be excluded from the Monitoring and Alerting system. Microsoft recommends that you enable SIP options, and the default value is True.

There are additional PowerShell commands to manage online PSTN gateway settings such as `Set-CsOnlinePSTNGateway`, `Get-CsOnlinePSTNGateway`, and `Remove-CsOnlinePSTNGateway`.

Figure 4-37 shows the online PSTN gateway PowerShell command parameters.

```
PS C:\> Get-CsOnlinePSTNGateway -Identity sbc1.bloguc.com


Identity                              : sbc1.bloguc.com
InboundTeamsNumberTranslationRules    : {}
InboundPstnNumberTranslationRules     : {}
OutboundTeamsNumberTranslationRules   : {Remove +, Remove + and Extension}
OutboundPstnNumberTranslationRules    : {EU-Service, EU-Emergency, EU-PrefixAll}
Fqdn                                  : sbc1.bloguc.com
SipSignalingPort                      : 5061
FailoverTimeSeconds                   : 10
ForwardCallHistory                    : False
ForwardPai                            : False
SendSipOptions                        : True
MaxConcurrentSessions                 : 200
Enabled                               : True
MediaBypass                           : False
GatewaySiteId                         :
GatewaySiteLbrEnabled                 : False
FailoverResponseCodes                 : 408,503,504
GenerateRingingWhileLocatingUser      : True
PidfLoSupported                       : False
MediaRelayRoutingLocationOverride     :
ProxySbc                              :
BypassMode                            : None
```

Figure 4-37. *Teams PSTN gateway*

Configuring and Managing Teams Calling Plans

Teams Calling Plan is another way to connect Teams to PSTN using Microsoft as the service provider. Teams provide audio and video calling and meetings using VoIP through the data network, and all these calls and meetings are free. However, making phone calls to external phone numbers or receiving calls from external regular phones to Teams users requires the purchase of a Calling Plan license on top of the Phone System license and Teams license. As an admin, you must know how to purchase and configure Calling Plans for users.

As of this writing, there are two Microsoft Calling Plan options available:

- **Domestic Calling Plan:** Using this plan, Teams licensed users can call out to external phone numbers in the country or region where they are assigned in Office 365.
- **Domestic and International Calling Plan:** Using this plan, Teams licensed users can call out to external phone numbers in the country or region where their Office 365 license is assigned based on the

user's location and to international numbers in supported countries or regions. Currently, Calling Plan is available in 196 countries or regions that you can dial into using an international number.

- **Pay-As-You-Go plan:** With this plan, users can make both domestic and international PSTN calls. Unlimited inbound minutes are included for free, while outbound calls are charged per minute using communication credits. There are two options to choose from:
- **Pay-As-You-Go Calling Plan Zone-1:** For users in the United States and Puerto Rico, Canada, and the United Kingdom.
- **Pay-As-You-Go Calling Plan Zone-2:** For users in Austria, Belgium, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Singapore, Slovakia, Slovenia, South Africa, Spain, Sweden, and Switzerland.

Note

- Zone 1 licenses are not currently available for sale in the United States and Puerto Rico. However, users of United States and Puerto Rico can still obtain them if purchased in another country.
- Zone 2 licenses aren't currently available for sale in the United States and Puerto Rico.
- Mexico has a separate pay-as-you-go plan.

Figure 4-38 shows the Microsoft-provided PSTN and Calling Plan plus Teams Phone System and the Office 365 cloud where corporate and remote users are connected for Teams services and phone calling capabilities.

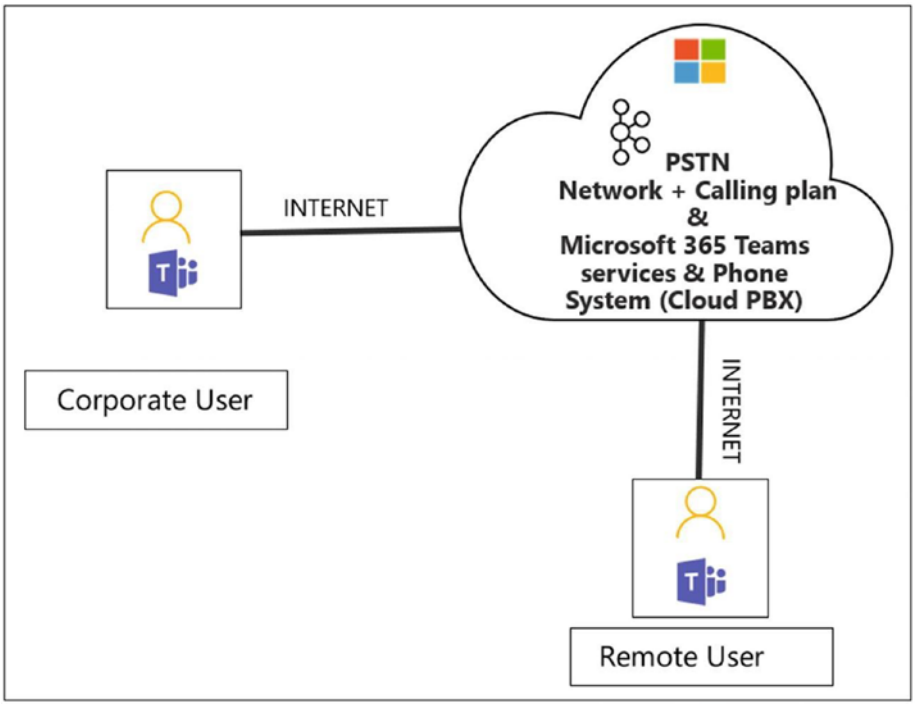

Figure 4-38. *Teams Calling Plan*

Setting Up a Calling Plan

Teams Calling Plan enables Teams users to make and receive phone call. However, as a Teams admin, you must know how to set up the Calling Plan feature. To set up this feature in your Teams environment, perform the following steps:

1. Check to determine whether Calling Plans are available in your country or region before they are purchased. Calling plans can be purchased depending on availability per country or region. Therefore, when planning for your telephony solution, you should verify whether the country or region used in your Office 365 billing location supports Teams Audio Conferencing.

    a. To check if Calling Plans are available in your country or region, visit this site, which shows the countries where Calling Plans are available: https://docs.microsoft.com/en-us/microsoftteams/country-and-region-availability-for-audio-conferencing-and-calling-plans/country-and-region-availability-for-audio-conferencing-and-calling-plans.

2. Purchase and assign licenses. Once you ensure that Calling Plans are available and can be purchased for your country or region, you should buy the Calling Plan licenses and assign them to your users.

   a. To purchase the Calling Plans license, visit https://docs.microsoft.com/en-us/microsoftteams/calling-plans-for-office-365 to get more information.

Note Microsoft Teams Phone System licenses and Calling Plans licenses in Office 365 work together. Before looking for the option to purchase Calling Plans, you must first have the Phone System licenses.

---

3. With a phone number, you can call in and out; hence, you must acquire phone numbers. Teams provides several ways to get phone numbers.

   - **Use the Teams admin center:** This process is used when your country or region supports getting phone numbers through the Teams admin center.
   - **Port existing phone numbers:** This process is used to port your existing phone numbers from the current carrier to the Office 365 Phone System.
   - **Use the request number for port numbers:** This process is used when the Teams admin center in your country or region does not support getting phone numbers.

4. Add emergency addresses and locations for the organization.
5. Assign a phone number and emergency address for the user.

Purchasing a Calling Plan for a Teams Organization

Teams Calling Plan requires making and receiving phone calls on users' Teams client. Also, Teams Phone System licenses and Calling Plan licenses work together, so before purchasing a Calling Plan license, your organization must have Phone System licenses. To purchase Phone System and Calling Plan licenses, follow these steps:

1. Purchase a Phone System add-on license (if you are not using an E5 license). To do so, log in to the Microsoft 365 admin center and select Billing. Select Purchase Services and then Add-on Subscriptions. Click Buy Now.
2. After you have finished buying Phone System licenses, you can buy the Calling Plan by logging in to the Microsoft 365 admin center. Select Billing, select Purchase Services, and then click Add-on Subscriptions. Click Buy Now.

Note Depending on your organization's needs, you can buy and assign different Calling Plans to different users. After you select the calling plan you need, proceed to checkout and purchase it and then you can assign a calling plan to each user in the Microsoft 365 admin center.

Assigning Calling Plans to Users

After acquiring Calling Plan licenses, you as an admin, must assign the Calling Plan license to users using the calling service. To do so, log in to Microsoft 365 admin center and navigate to Users. Select Active Users and then find the user to whom you need to assign a Calling Plan license. Open that user account, select the appropriate license, and click Save Changes. Figure 4-39 shows an account with the Domestic and International Calling Plans assigned.

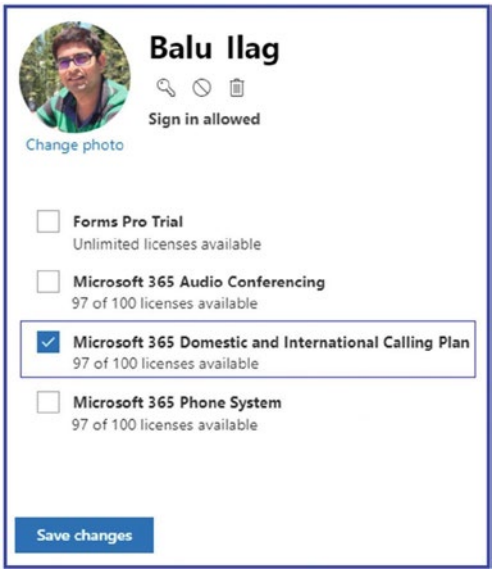

Figure 4-39. *Assigning a calling plan*

Porting a Phone Number to Microsoft

Porting a phone number to Microsoft involves three steps: porting readiness, port scheduling, and number porting.

Porting readiness includes a checklist of activities to ensure readiness for porting. These typically include the following:

- Identify phone numbers to be ported, including subscriber, toll, and toll-free numbers.
- Identify the losing carrier and the billing address associated with these phone numbers.
- Identify a legal representative or authorized user to sign the LOA forms on behalf of your organization.
- If you are porting outside the United States, identify the migration code, fiscal code, etc. These are included in your carrier monthly bills.

- Fill out the LOA Form to request a port schedule. The form is unique to the country of the port request. Ensure you choose the correct country before you schedule a port. LOA forms from Microsft are available at https://learn.microsoft.com/en-us/microsoftteams/manage-phone-numbers.
- Create an emergency address in the Teams admin center. This address is usually the service address associated with your phone number or the location where you plan to service these numbers. Please ensure you enter it accurately, as this address will serve as the emergency address during emergency calls.

Once you confirm that porting readiness is completed, you schedule a port. There are a few things to remember while you are scheduling the port. It is a best practice to schedule porting three weeks in advance as carriers need time to arrange engineers, get approval, or decide if the request is possible. This advance request gives time to manage and resubmit the port request if the carriers reject it. Select a porting time that falls outside of regular business hours to ensure a smooth transition. It would be best if you could schedule it toward the end of the day. In most cases, the Teams admin must assign the phone numbers to the users/call queues/auto attendants. Scheduling outside normal business hours will reduce the end-user impact from making and receiving calls.

To schedule a port, navigate to the Teams admin center, select Phone numbers, and click the port. Choose the country and type of phone number, and hit Next. Enter the Billing Telephony Number setting. The Billing Telephony Number is typically the pilot number for your porting number series/range. You can find this number in the billing summary of your monthly bill. If you have any questions, please get in touch with your losing carrier.

After you enter and click confirm, the system checks with the database and validates the porting availability and the losing carrier. Next, to port your phone numbers, you can either manually enter them separated by commas (,) or upload a CSV file with the numbers prefilled. Click Next and ensure the validation is successful for all the numbers.

Enter the details on the next page like the following:

- Order details
- Port details
- Organization details

- Current service provider details
- Authorized user details
- Service address
- Type of phone number (user usage, service usage)
- Notifications

While entering the authorized user details, you can get the LOA (the LOA is generated based on the details entered in the TAC) sent to the authorized user email for signature or manually upload the LOA. After entering all the details, click Next to upload the LOA if you chose to upload manually. After placing your order, you will receive notifications regarding the status updates, approvals, or rejections to the email address provided during the porting process. If the date and time of the port do not match your order, please contact the PSTN service desk immediately.

You can manually submit porting orders via the PSTN Service Desk. Access it through the Teams admin center; select Phone numbers and create a case. You must prefill the LOA and porting numbers in a CSV file and manually upload them during the port request.

The final stage of number porting is when the losing carrier ports the number to Microsoft. Once the porting order is completed, the notifiers receive an email. The phone number can then be assigned to users or resource accounts in the Teams admin center.

Configuring and Managing Teams Operator Connect

Operator Connect is an additional way to integrate PSTN services into Teams. If your current service provider is part of Microsoft's Certified Operator Connect Program, they can bring PSTN services to Teams using Operator Connect. Operator Connect offers a cost-effective solution for minimizing infrastructure and monthly billing expenses. Instead of billing based on subscriptions, Operator Connect charges your organization based on outbound call usage. This approach helps you save on monthly/annual PSTN bills. Operator Connect might be an effective option if

- You are looking for a cost-saving yet an effective approach.
- Your current service provider is part of the Microsoft Operator Connect program.

- You are looking to bring PSTN services to Teams.
- You don't have Calling Plans available in your region/country.

Figure 4-40 shows a high-level architecture diagram for Operator Connect. The Certified partners connect their SBC as a service (SBCaaS) to Teams. The architecture model utilized direct peering through Microsoft Azure Peering Service, provisioning APIs, and an operator portal for setting up the trunk to Microsoft Teams. This model uses capabilities such as BGP over BFD and end-to-end QoS from the Microsoft Cloud to the operator cloud to strengthen the interconnection. Using the Teams admin center, the initial setup and onboarding are made easier.

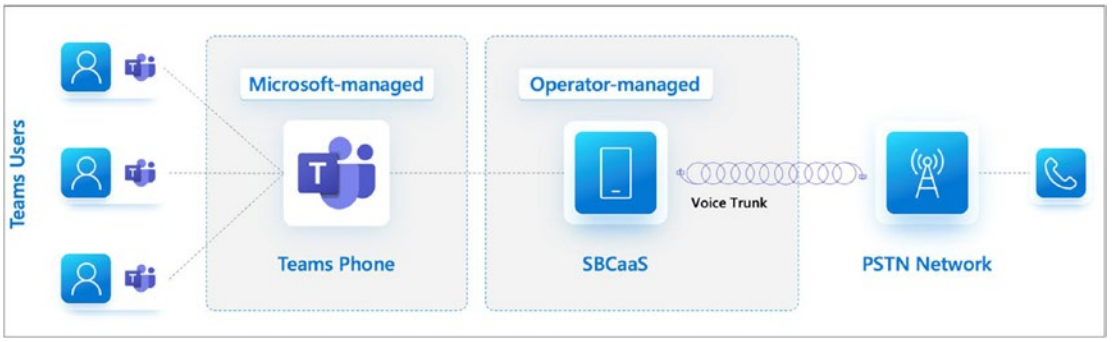

Figure 4-40. *Operator Connect architecture*

Once an operator is onboarded with your tenant, all incoming and outgoing calls will seamlessly go through your Teams to the carrier-managed SBC and then to the PSTN network. This is an all-in-one cloud model; you don't have to manage any infrastructure. This option lets you onboard multiple carriers in a single tenant.

Tip If your organization is comparing the cost estimates of Operator Connect and Calling Plan subscriptions, please consider including taxes. Calling Plan subscriptions already include taxes, whereas Operator Connect partner bill estimates do not.

Plan for Operator Connect

Operator Connect is a popular option when choosing PSTN connectivity models for Teams Phone. However, it's important to perform readiness checks and requirements mapping to ensure it fits your organization correctly. These checks may include the following:

- Validating If your existing carrier is participating in the Operator Connect program to leverage existing contracts
- Whether the Operator Connect model is providing PSTN connectivity to all your devices
- List of operators available in your country or region
- Cost savings with your current model and Operator Connect model

Operator Connect may not be the best option for connectivity and customization if you have a lot of analog device connectivity in your organization. However, most Operator Connect partners offer methods to connect analog devices. Please reach out to specific carriers before making a decision.

Once you decide to go with Operator Connect, be sure to purchase Teams Phone licenses. These licenses are included with E5 subscriptions or can be bought as an add-on with other subscriptions. Teams Phone licenses add a dial pad to the Teams client. Additionally, ensure that all users using Operator Connect are in Teams Only mode, but the entire organization doesn't need to be in Teams Only mode.

Configure Operator Connect

After completing the readiness requirements and choosing an operator, onboard the operator in the Teams admin center.

1. Go to Voice ➤ Operator and choose an operator from the All Operators tab.
2. Under operator settings, select the country you want to enable with your selected operator.
3. Fill in the contact information and provide the company size.
4. Accept the data transfer notice and add your operator and click Save.

Phone Numbers

Once the Operator Connect is enabled, you must choose whether you acquire new phone numbers from your operator or port the existing number. If your existing carrier is the operator connect partner, raise a support ticket with the carrier to move a phone number from your existing trunk to the Operator Connect trunk.

Acquire New Numbers

To acquire new numbers, you must go to your operator's website. Your operator will provide details of the website. Here is a link from Microsoft that lists operator websites: https://cloudpartners.transform.microsoft.com/partner-gtm/operators/directory.

Transfer Your Existing Numbers

To transfer your phone numbers from Calling Plans or your current provider to Operator Connect, you must submit a port order on the operator website with a list of phone numbers and a letter of authorization. After the request is fulfilled, assign the Operator Connect numbers to the users using the following PowerShell command:

```
Set-CsPhoneNumberAssignment -Identity <user> -PhoneNumber <phone number>
-PhoneNumberType OperatorConnect
```

Transferring phone numbers from Direct Routing to Operator Connect can be challenging, depending on whether you manage them on-premises or online. To validate, run the following PowerShell command:

```
Get-CsOnlineUser -Identity <user> | fl RegistrarPool,
OnPremLineURI, LineURI
```

If a user's `OnPremLineUri` attribute contains a phone number, the phone numbers are managed on-premises. The user's phone number must be removed to switch to Operator Connect, requiring scheduled maintenance as the service will be temporarily unavailable.

Here are the steps to assign an Operator Connect number to an on-premises managed Direct Routing user:

1. Set `lineuri` to `Null` in your Skype for Business Server by running the following command:

   ```
   Set-CsUser -Identity <user> -LineURI $null
   ```

2. Allow time for changes to sync and validate in an online directory.

   ```
   Get-CsOnlineUser -Identity <user> | fl RegistrarPool,
   OnPremLineURI, LineURI
   ```

3. After the changes have been replicated, execute the command to remove the phone number from Teams.

   ```
   Remove-CsPhoneNumberAssignment -Identity <user>
   -PhoneNumber <pn> -PhoneNumberType DirectRouting
   ```

4. Unassign the voice routing policy.

   ```
   Grant-CsOnlineVoiceRoutingPolicy -Identity <user>
   -PolicyName $Null
   ```

5. Port or acquire the phone numbers and assign them using this PowerShell command:

   ```
   Set-CsPhoneNumberAssignment -Identity <user>
   -PhoneNumber <phone number> -PhoneNumberType
   OperatorConnect
   ```

Teams Phone Mobile

Teams Phone Mobile is another method for providing PSTN services in Teams. Similar to Operator Connect, a list of telecom vendors or operators participate in the Microsoft Teams Phone Mobile program and are eligible to provide Teams Phone PSTN services using this model.

Unlike the Operator Connect model, the Teams Phone Mobile program allows users to use their SIM-enabled phone number as their Teams phone number. This means that users can access their mobile services and Teams using a single phone number. If your organization aims toward a mobile-driven approach, this PSTN connectivity

option is the right fit. It is especially useful for salespeople to receive and manage phone calls using their SIM-enabled number and to use the same number for SMS and text messages.

Here are the advantages:

- Single number for mobile and Microsoft Teams allowing users to work from any location securely.
- Users can use unified voicemail, seamless transfers, combined call history, and presence across Teams and native mobile devices.
- Recording and retention of voice calls on native mobile devices.

Architecture

The architecture of Teams Phone Mobile mainly consists of Metaswitch Mobile Control Point (MCP) and Teams-certified mobile interworking SBC. MCP is an application that sits on the carrier-grade application server Rhino. It enhances the user experience by integrating Microsoft Teams into the Mobile Operator's call flow. MCP connects to the Operator's IMS core to determine whether the call should be routed to the mobile operator network and directly to the user's native dialer or routed to Microsoft Teams for applying originating and terminating services for calls made from and to end users. MCP queries the Microsoft Teams phone service if a caller or callee is eligible for Teams Phone Mobile services. If the caller or callee is eligible, MCP adds Microsoft Teams Phone services to the call path. If the user isn't eligible, the call does not reach the Microsoft Teams Phone system, and the MCP ensures the call follows its call path.

The Mobile Interworking SBC ensures that it inserts and removes the ISUP signaling information into SIP signaling messages based on whether calls are routed to the Teams Phone System or the mobile operator. Figure 4-41 shows Teams Phone Mobile architecture.

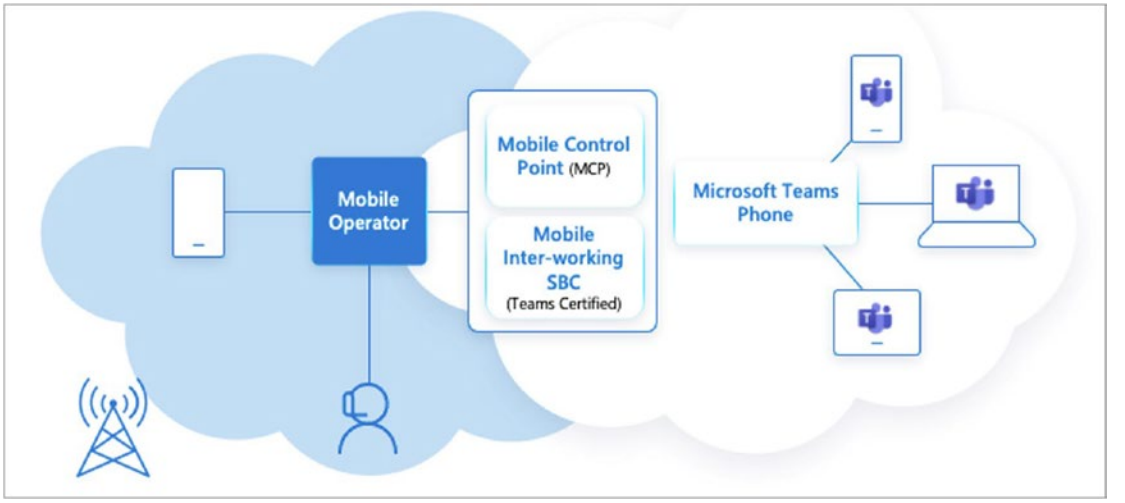

Figure 4-41. *Teams Phone Mobile architecture*

Plan for Teams Phone Mobile

Teams Phone Mobile is a great option for organizations with mobile workforces consisting of frontline workers and sales teams. However, it is essential to validate if Teams Phone is the right method of PSTN connectivity for your organization. The considerations must include the following:

- You want to use a primary company-owned, SIM-enabled mobile number for Teams Phone as a single-number solution.
- Your existing or preferred operator is a participant of the Teams Phone Mobile program.

For users to access Teams Phone Mobile, they need to have the Teams Phone System license and be in Teams-only mode. They also require a Teams Phone Mobile add-on SKU license and an eligible subscription with an operator that supports their SIM-enabled phone numbers for Teams Phone.

Configure Teams Phone Mobile

After completing the readiness requirements and choosing a mobile operator, onboard the operator in the Teams admin center.

1. Go to Voice ➤ Operator and choose an operator from the All Operators tab.
2. Under Operator Settings, select the country you want to enable with your selected operator.
3. Fill in the contact information and provide the company size.
4. Accept the data transfer notice and add your operator and click Save.

Phone Numbers

Once the operator connect is enabled, you must choose whether you acquire new phone numbers from your operator or port the existing number. If you have a company-paid SIM-enabled phone number that you want to add to Teams, contact your operator to confirm your eligibility for the Teams Phone Mobile subscription. Once your operator completes the order, you can assign the numbers to users.

Acquire New Numbers

To acquire new numbers, you must go to your operator's website. Your operator will provide details of the website. Here is a link from Microsoft that lists operator websites: https://cloudpartners.transform.microsoft.com/partner-gtm/operators/directory. Order or acquire SIM-enabled mobile phone numbers with Teams Phone service enabled. After completion, view the list of numbers in the Teams admin center under Voice ➤ Phone numbers.

Transfer Your Existing Numbers

To transfer your phone numbers from Calling Plans, ensure you have eligible Teams Phone Mobile subscription and the Teams Phone Mobile add-on licensee. Contact your operator to port your numbers to Teams Phone Mobile on an eligible wireless voice plan that is SIM-enabled. Once the numbers are ported, the operator will upload the numbers in the Teams admin center. Admins can assign the numbers to users using the following Powershell command:

```
Set-CsPhoneNumberAssignment -Identity <user> -PhoneNumber <phone number>
-PhoneNumberType OCMobile
```

It can be challenging to transfer phone numbers from Direct Routing to Teams Phone Mobile, depending on whether you manage them on-premises or online. To validate, run the following PowerShell command:

```
Get-CsOnlineUser -Identity <user> | fl RegistrarPool,
OnPremLineURI, LineURI
```

If a user's `OnPremLineUri` attribute contains a phone number, the phone numbers are managed on-premises. The user's phone number must be removed to switch to Operator Connect, requiring scheduled maintenance as the service will be temporarily unavailable.

Here are the steps to assign an Operator Connect number to an on-premises managed Direct Routing user:

1. Set `lineuri` to `Null` in your Skype for Business Server by running this command:

   ```
   Set-CsUser -Identity <user> -LineURI $null
   ```

2. Allow time for changes to sync and validate in online directory.

   ```
   Get-CsOnlineUser -Identity <user> | fl RegistrarPool,
   OnPremLineURI, LineURI
   ```

3. After the changes have been replicated, execute the command to remove the phone number from Teams.

   ```
   Remove-CsPhoneNumberAssignment -Identity <user>
   -PhoneNumber <pn> -PhoneNumberType DirectRouting
   ```

4. Unassign the voice routing policy.

   ```
   Grant-CsOnlineVoiceRoutingPolicy -Identity
   <user> -PolicyName $Null
   ```

5. Port or acquire the phone numbers and assign them using this PowerShell command:

   ```
   Set-CsPhoneNumberAssignment -Identity <user>
   -PhoneNumber <phone number> -PhoneNumberType
   OperatorConnect
   ```

Configuring and Managing the Call Queue

Microsoft Teams cloud call queues provide multiple features for calling, including a greeting message, music while individuals are waiting on hold, forwarding calls to call agents in mail-enabled distribution lists and security groups, and setting different parameters such as queue maximum size, timeout, and call handling options.

Teams Phone System call queues, and auto attendants must have at least one associated resource account. Basically, a resource account will need an assigned phone number depending on the proposed usage of the associated call queue or auto attendant. You cannot directly give the phone number to a call queue or auto attendant, so the phone number is assigned to a resource account that is associated with call queue or auto attendant. Therefore, the call queue can be dialed directly or accessed by a selection on an auto attendant, and then all calls in the queue will be sent to agents using one of these techniques.

- With attendant routing, the first call in the queue rings all agents simultaneously.
- With serial routing, the first call in the queue rings all call agents one by one.
- With round-robin, the routing of incoming calls is balanced so that each call agent gets the same number of calls from the queue.
- Only one incoming call notification at a time (for the call at the head of the queue) goes to the call agents.
- After a call agent accepts a call, the next incoming call in the queue will start ringing call agents.

As per Microsoft's new requirements, every resource account utilized with a call queue or auto attendant must be licensed with a Microsoft Teams Phone resource account license, regardless of whether it's assigned a phone number or configured for a nested call queue or nested auto attendant.

Note Call agents who are offline, those who have set their presence to "Do not disturb, "or those who have opted out of the call queue will not receive calls.

Creating a Call Queue

As you learned, a phone number cannot be directly assigned to a call queue; instead, it is assigned to the resource account. That resource account will then be linked to the call queue. That means before creating a call queue, you as a Teams admin must think through the requirements for creating a call queue. The requirements are listed here:

- You must have a resource account created for the call queue.
- When you assign a phone number to a resource account, you can use the free Microsoft Teams Phone Resource Account license.
- Another important requirement is to assign a phone number. Remember that you can assign only toll and toll-free service phone numbers that you got in the Microsoft Teams admin center or port from another service provider to cloud call queues.
- Additionally, communications credits setup in Microsoft 365 is required for toll and toll-free service numbers.
- You can assign multiple resource accounts to call queues, but you cannot assign a single resource account to various call queues.

Follow these steps to create a call queue:

1. Get service numbers from Microsoft or transfer your existing toll or toll-free service numbers before creating your call queues. Once you get the toll or toll-free service phone numbers, they will show up in the Microsoft Teams admin center under Voice ➤ Phone Numbers.
2. Create a resource account. Every call queue must have an associated resource account, which you can associate with the call queue. You should perform the following steps to create a new call queue:
    a. Go to the Microsoft Teams admin center, and select Voice. Select Call Queues, and then click + Add New.
    b. On the Call Queues/Add page, give the call queue a meaningful display name that will be displayed in notifications for incoming calls. Figure 4-42 shows CQ_SipGateway as the queue name.

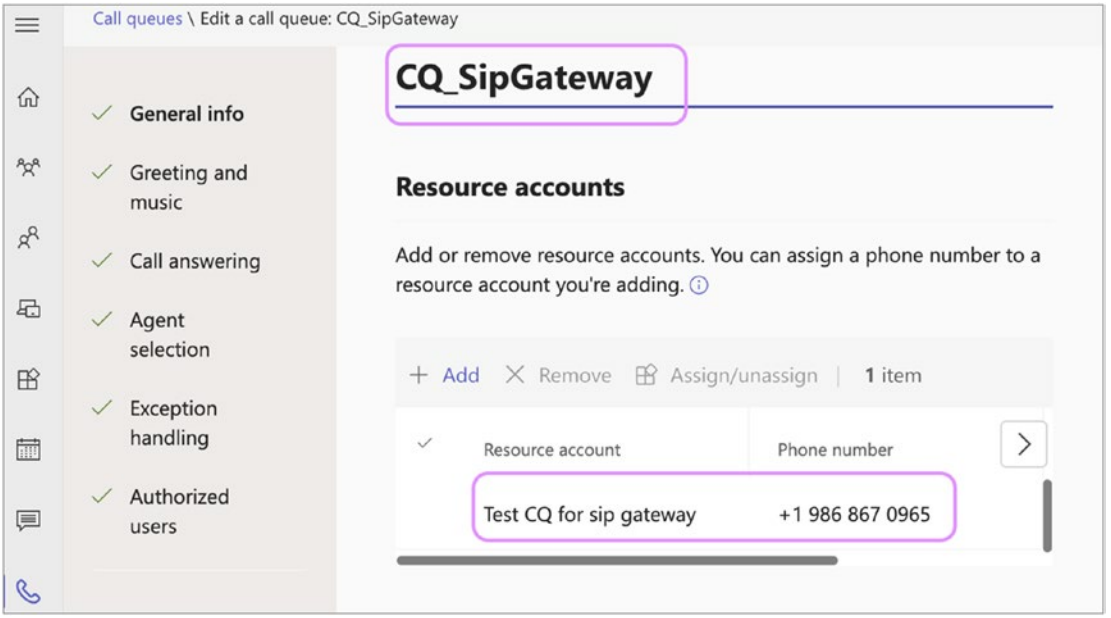

Figure 4-42. *Call queue name and selecting a resource account*

c. Click Add Accounts to select a resource account (it may or may not be associated with a toll or toll-free phone number for the call queue, but each call queue requires an associated resource account). If no resource accounts are listed, you must get service numbers and assign them to a resource account before creating this call queue. In this example, a resource account is created in advance. In Figure 4-43, Test CQ for the sip gateway is assigned with a phone number and assigned to the call queue.

d. To assign a calling ID, click the Add button. This feature allows agents to make outbound calls using either their personal calling ID or the caller ID of a resource account. In this example, we utilize the caller ID of the resource account linked to the call queue. This enables agents to use it as their outbound caller ID.

e. Please choose the preferred language for the agents who will listen to the transcribed voicemail in the call queue. The system will also play prompts to the caller in the selected language. In this example, we choose English (United States). Refer to Figure 4-43 for language selection.

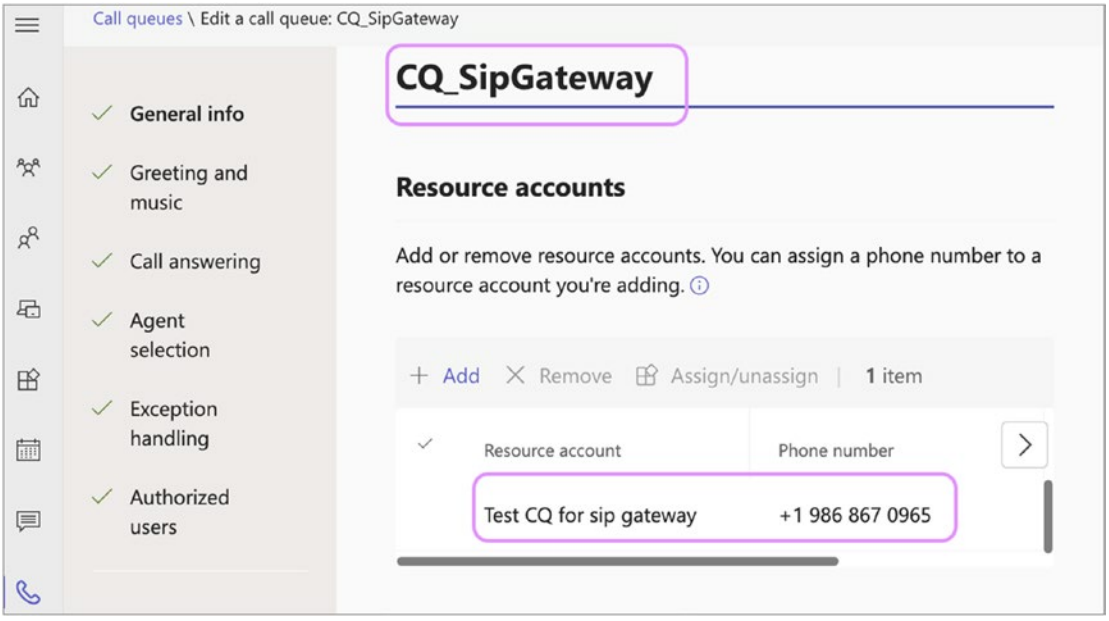

Figure 4-43. *Configuring calling ID and language*

3. Set the greeting and music that will be played while a call is on hold, as shown in Figure 4-44.

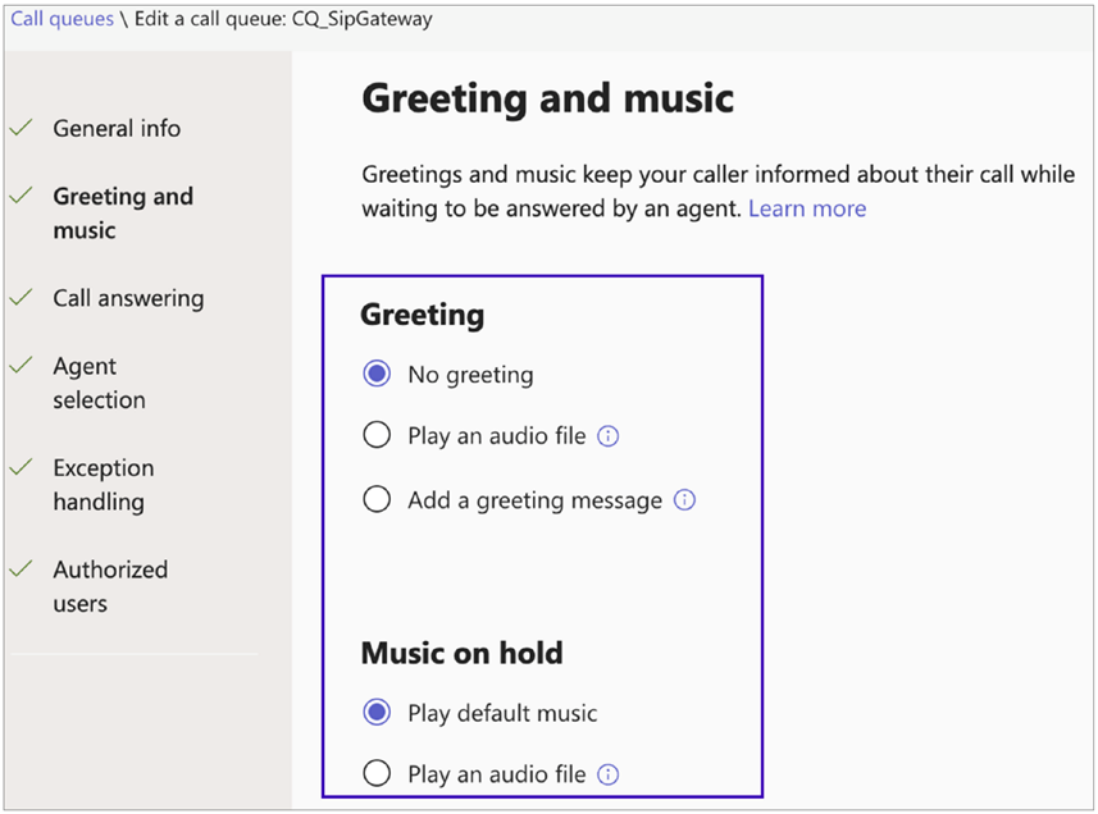

Figure 4-44. *Selecting a greeting and hold music*

4. In the "Call answering" section, add call queue agents and select conference mode.

   a. Select the call answering options. You can select a user agent or group. Up to 200 call agents can belong to an Office 365 group, security group, Teams channel, or distribution list. The example in Figure 4-45 shows Christie Cline as the call agent.

   b. Turn on the conference mode to reduce the time a caller takes to connect with an agent after the call has been accepted. This is useful if all the agents are in Teams-only mode and using Teams-compatible clients.

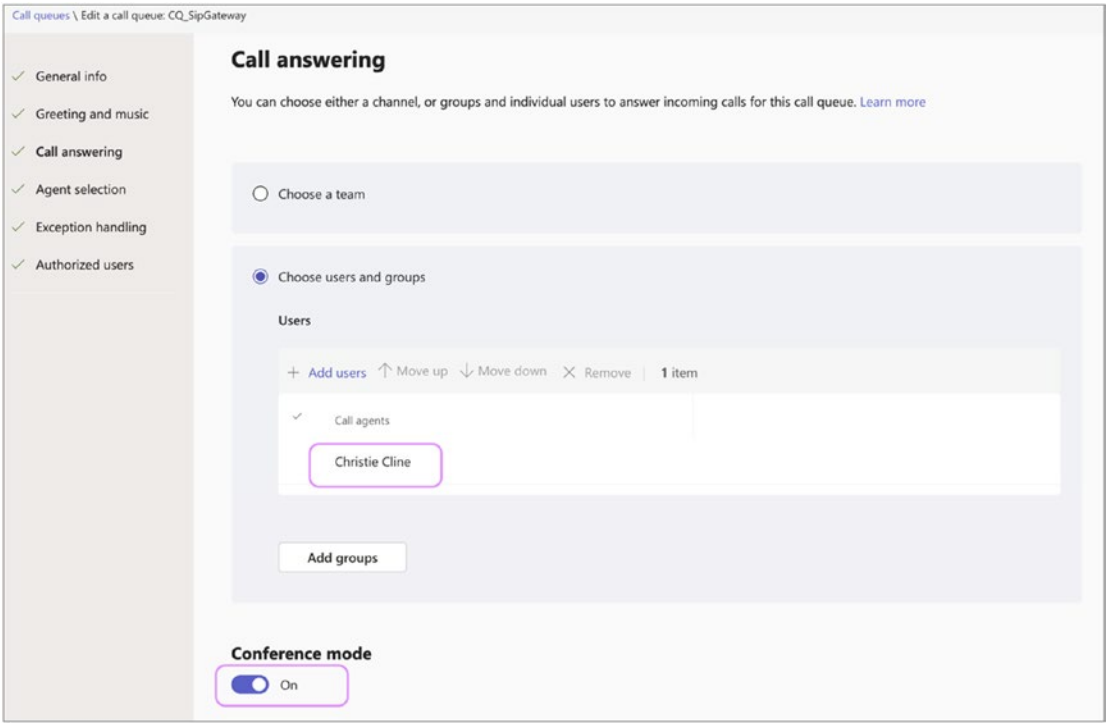

Figure 4-45. *Selecting an agent*

Note The call agents that you select must be online users with a Phone System license and Enterprise Voice enabled, online users with a Calling Plan, or Direct Routing with an On-Premises phone number assigned.

---

5. Select a routing method for your call queue distribution method. You can select from the following options:

   a. **Attendant Routing:** This enables the first call in the queue to ring all call agents simultaneously. The first call agent to pick up the call gets the call.

   b. **Longest Idle:** The call routes to the agent who has been idle for the longest time, based on their presence status displayed as "Available." Agents will receive calls only if their presence status is set to Available.

c. **Serial Routing:** Using this option, an incoming call rings call agents one by one, starting from the beginning of the call agent list (agents cannot be ordered within the call agent list). If an agent dismisses or does not pick up a call, then the call will ring the next agent on the list, trying all agents one by one until it is picked up or times out waiting in the queue.

d. **Round Robin:** This method balances incoming calls routing so that each call agent gets the same number of calls from the queue. Figure 4-46 shows the round-robin method selected. "All agents can opt out of taking calls" is set to On, and the "Call agent alert time" setting is 35 seconds.

e. **Presence-based call routing:** By turning on this setting, Calls are routed depending on the agent's presence status. If the agent is available, they will be added to the routing queue using the previous routing methods. However, if the agent's presence is set to any other status, they will not receive any calls until they change their position to available.

f. **Agents can opt out of taking calls:** Enabling this option allows agents to opt out from a specific call queue if they choose to do so. Agents can adjust these settings within their Teams client.

g. **Agent alert time:** The agent alert time is the duration for which a call rings for an agent before being redirected to another agent. Setting the ringing time to 20 seconds is recommended, as this is the default time for Teams. It is recommended to set the ringing time to 20 seconds, as this is the default ring time for Microsoft Teams.

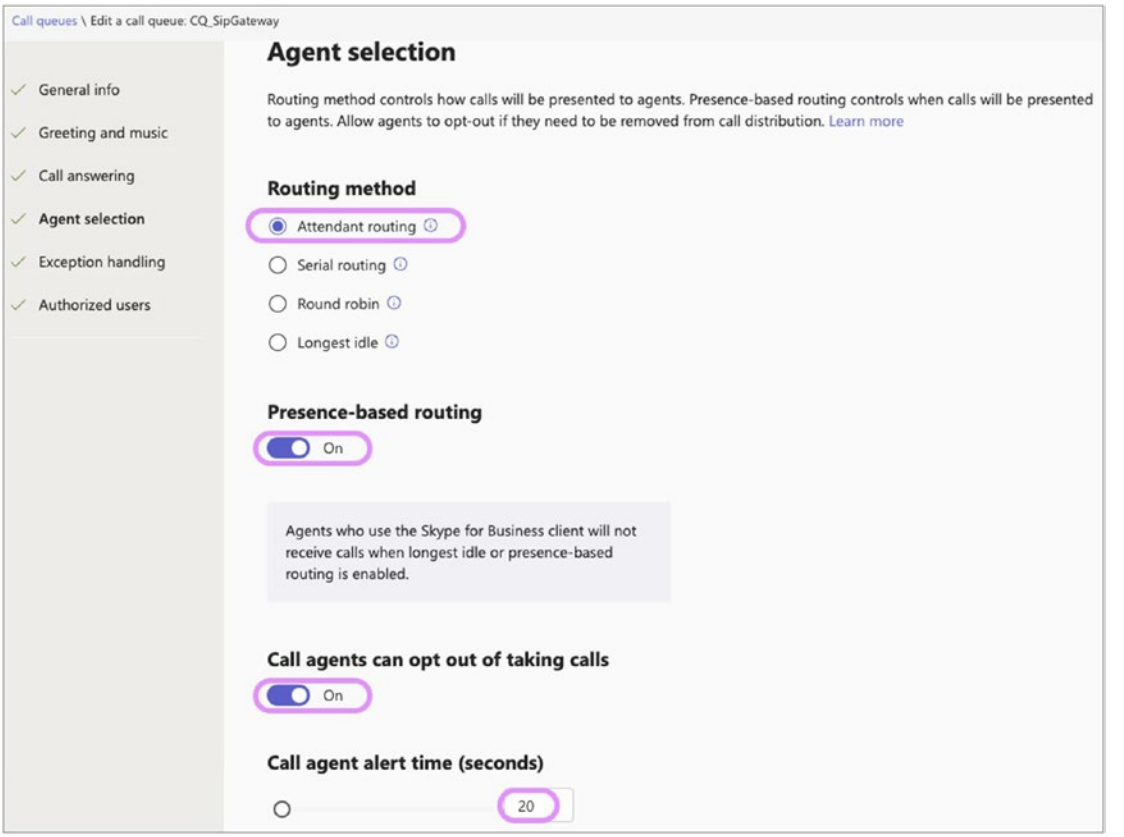

Figure 4-46. *Routing method selection*

6. When it comes to handling exceptions, there are a few settings you can configure. First, you can set Maximum Calls In The Queue. Additionally, you can configure the call timeout and determine how to manage calls when no agents are available in the queue.

   a. **Call Overflow:** Use this setting to set the maximum number of calls that can be in the queue simultaneously (the default is 50, but the value can range from 0 to 200). When the call queue reaches the maximum you have set, you can select what happens to new incoming calls using the following options:

      - **Disconnect:** This option will disconnect the call.

- **Redirect To:** Select one of the following redirect settings using this option:

    1. **Person In Organization:** This selection, shown in Figure 4-47, enables you to select the person to whom the incoming call will be redirected.

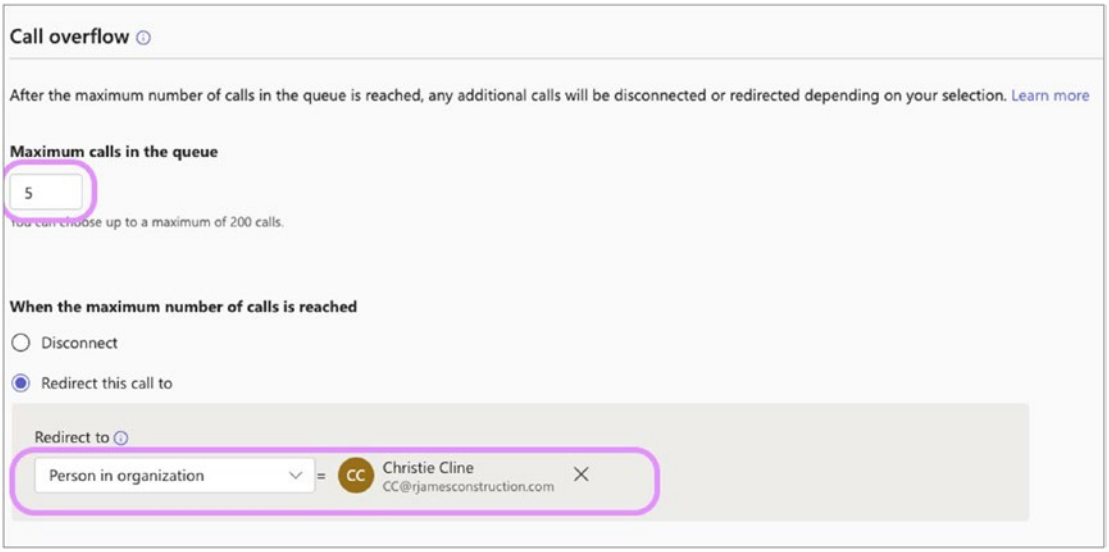

Figure 4-47. *Call overflow handling*

2. **Voice Application:** You must select the name of an existing resource account associated with either a call queue or an auto attendant.
3. **External Phone Number:** If you need to redirect a call to an external phone number, you can do so by assigning the resource account with either a Calling Plan license (if you use Calling Plans) or an Online Voice routing policy (if you use Direct Routing).
4. **Voicemail (Personal):** Use this setting to redirect the call to a user's voicemail.
5. **Voicemail (Shared):** Use this setting to redirect the call to a Microsoft 365 group's voicemail.

b. **Call Timeout:** Using this setting, you can set up the maximum number of minutes that a call can be on hold in the queue before it gets redirected or disconnected. You can specify the value from 0 seconds to 45 minutes. When the call queue reaches the maximum you have set, you can select what happens to new incoming calls using the following options:

- **Disconnect:** This option will disconnect the call.
- **Redirect To:** Select one of the following redirect settings using this option. Refer to Figure 4-48 for call overflow handling.

1. **Person In Organization:** This selection enables you to select the person to whom the incoming call will be redirected.

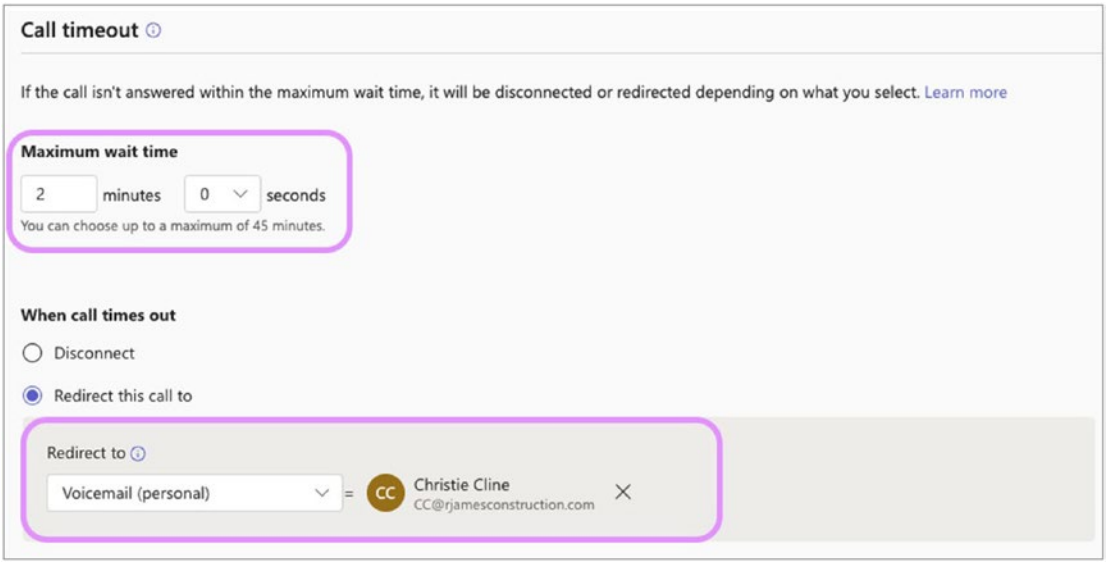

Figure 4-48. *Call overflow handling*

2. **Voice Application:** You must select the name of an existing resource account associated with either a call queue or an auto attendant.

3. **External Phone Number:** If you need to redirect a call to an external phone number, you can do so by assigning the resource account with either a Calling Plan license (if you use Calling Plans) or an Online Voice routing policy (if you use Direct Routing).
4. **Voicemail (Personal):** Use this setting to redirect the call to a user's voicemail.
5. **Voicemail (Shared):** Use this setting to redirect the call to a M365 Group's voicemail.

c. **No Agents Opted/Logged in:** You can use this setting to manage a queue when no agents are logged in or agents are opted out of taking calls from the queue. You can apply this to calls already in the queue and new calls or only the new ones. Configure the call handling under this exception.

- **Queue call:** By selecting this option, the call will remain in the queue.
- **Disconnect:** This option will disconnect the call.
- **Redirect To:** Select one of the following redirect settings using this option:

1. **Person In Organization:** This selection enables you to select the person to whom the incoming call will be redirected.
2. **Voice Application:** You must select the name of an existing resource account associated with either a call queue or an auto attendant.
3. **External Phone Number:** If you need to redirect a call to an external phone number, you can assign the resource account with either a Calling Plan license (if you use Calling Plans) or an Online Voice routing policy (if you use Direct Routing).

4. **Voicemail (Personal):** Use this setting to redirect the call to a user voicemail.

5. **Voicemail (Shared):** Use this setting to redirect the call to a M365 group's voicemail.

7. **Authorized users:** Authorized users are individuals who can manage the call queue settings. Typically, these individuals are supervisors or managers who handle agents. These users must be assigned with Voice application policy to manage the settings. Debra is assigned as an authorized user in the example and added to the HR-Call queue Voice application policy. Debra can manage these settings in the Teams client. See Figure 4-49 and Figure 4-50.

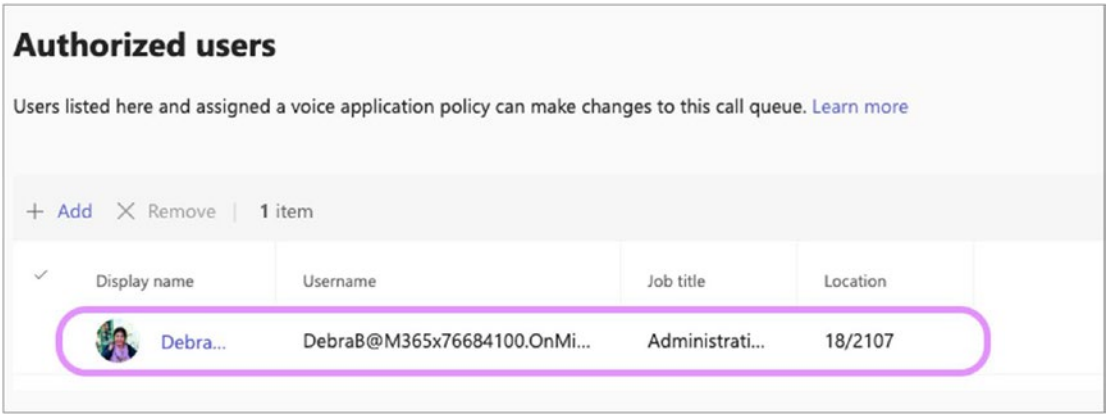

Figure 4-49. *Call queue, authorized users*

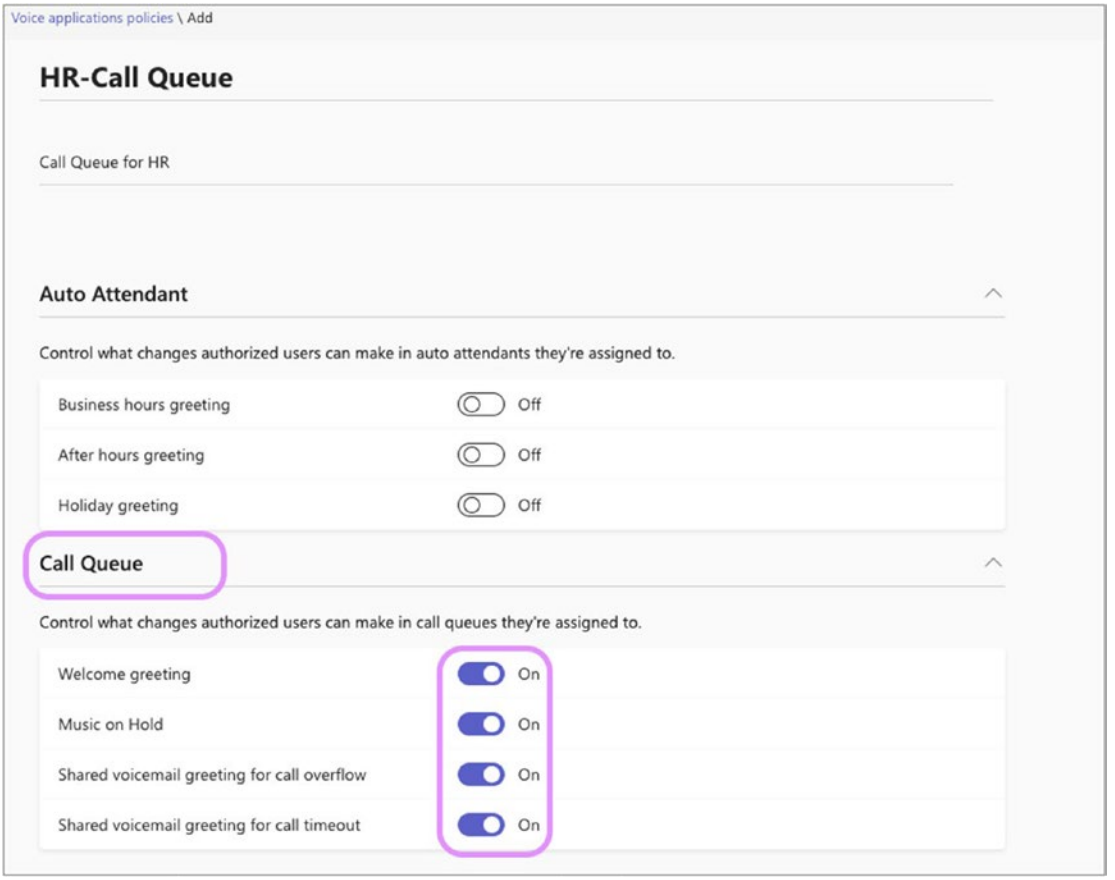

Figure 4-50. *Voice application policy*

8. Verify all the options you selected and then click Save to create the call queue.
9. The call queue might take a while to create. When complete, test the call queue by making a phone call to the resource account service phone number and validate that the call is landing with an agent.

Managing a Call Queue

To manage a call queue, a Teams admin needs to visit the Teams admin center. Log in to the Teams admin center, select Voice, and then select Call Queue. On the Call Queue page, you will see all the call queues listed. You need select the call queue that you want to manage. On the Call Queue page, you can add a new call queue, edit an existing call queue, or delete a call queue (see Figure 4-51).

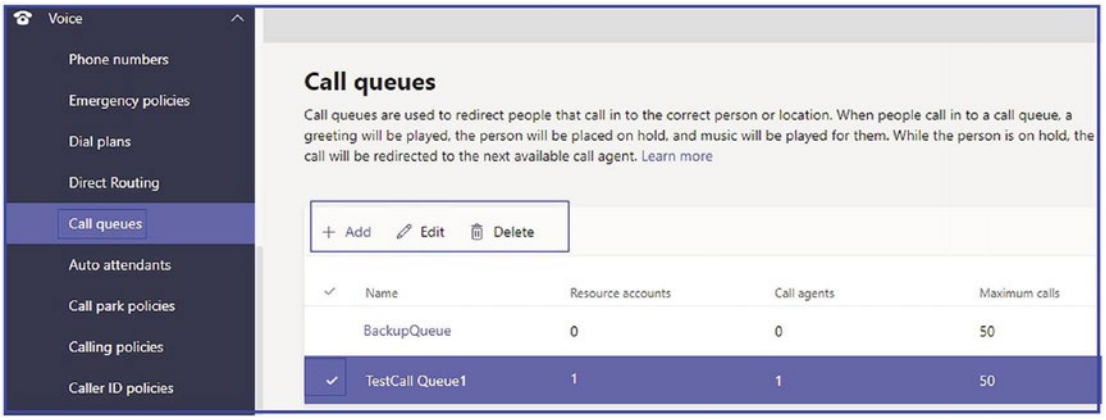

Figure 4-51. *Call queue management options*

You can also manage, create, and set up call queues using Windows PowerShell commands such as `New-CsCallQueue`, `Set-CsCallQueue`, `Get-CsCallQueue`, and `Remove-CsCallQueue`.

Additionally, authorized users can manage the call queues from their Teams desktop client. Please note that they must be added as an authorized user in the call queue and assigned with the voice application policy.

As an administrator, you can validate if a call queue can receive the call by running a diagnostic tool (`https://aka.ms/TeamsCallQueueDiag`).

Managing and Configuring Auto Attendant in Teams

The Teams Phone System provides multiple capabilities, including an auto attendant, which is highly utilized in many customer support organizations. Auto attendants enable external and internal callers to use a menu system to locate and place (or transfer) calls to users or departments in an organization. When people call a number associated with an auto attendant, their options can redirect the call to a user or locate someone else in the organization and then connect to that user.

Microsoft Teams cloud auto attendant features can allow someone to leave a message if a person does not answer the call, and they can provide corporate greetings, custom corporate menus including nested menus (menu inside the menu), and messages that specify business and holiday hours. Auto attendants can also support transferring calls to an operator, other users, call queues, and auto attendants. It also offers a directory search that enables users who call in to search the organization's directory for a name. It also supports multiple languages for prompts, text-to-speech, and speech recognition.

The auto attendant does have some prerequisites before creation.

- An auto attendant must have an associated resource account.
- When assigning a phone number to an auto attendant, you assign it to the resource account associated with that auto attendant; this enables you to have more than one phone number to access an auto attendant.
- A resource account must be assigned with a Microsoft Teams Resource Account license. This license can be acquired for free.
- To get and use toll-free service numbers for your auto attendants, you must set up communications credits.
- A complete auto attendant system usually involves multiple auto attendants and might require only a single assigned phone number for the top-level auto attendant.
- You can assign multiple resource accounts to an auto attendant, but you cannot give a single resource account to multiple auto attendants.

Creating an Auto Attendant with an Existing Resource Account

To create an auto attendant with an existing resource account, follow the procedure in this section. Remember, you cannot directly assign a service phone number to the auto attendant. Assign the number to a resource account associated with the auto attendant.

1. Log in to the Teams admin center and navigate to Voice. Select Auto Attendant and click Add.
2. On the Auto Attendants/Add Auto Attendant page, shown in Figure 4-52, enter a meaningful name and provide the following information:
    - **Operator:** This setting specifies whether a user can request to talk to a person or voice app or if there will be no designated operator. You can refer people to another auto attendant, a call queue, or an enterprise voice-enabled Skype for Business or Teams user.
    - **Time Zone:** This specifies the time zone in which the auto attendant will calculate business hours and holidays.
    - **Language:** This setting specifies the language the system will use.
    - **Enable Voice Input:** This enables voice navigation in the auto attendant menu.

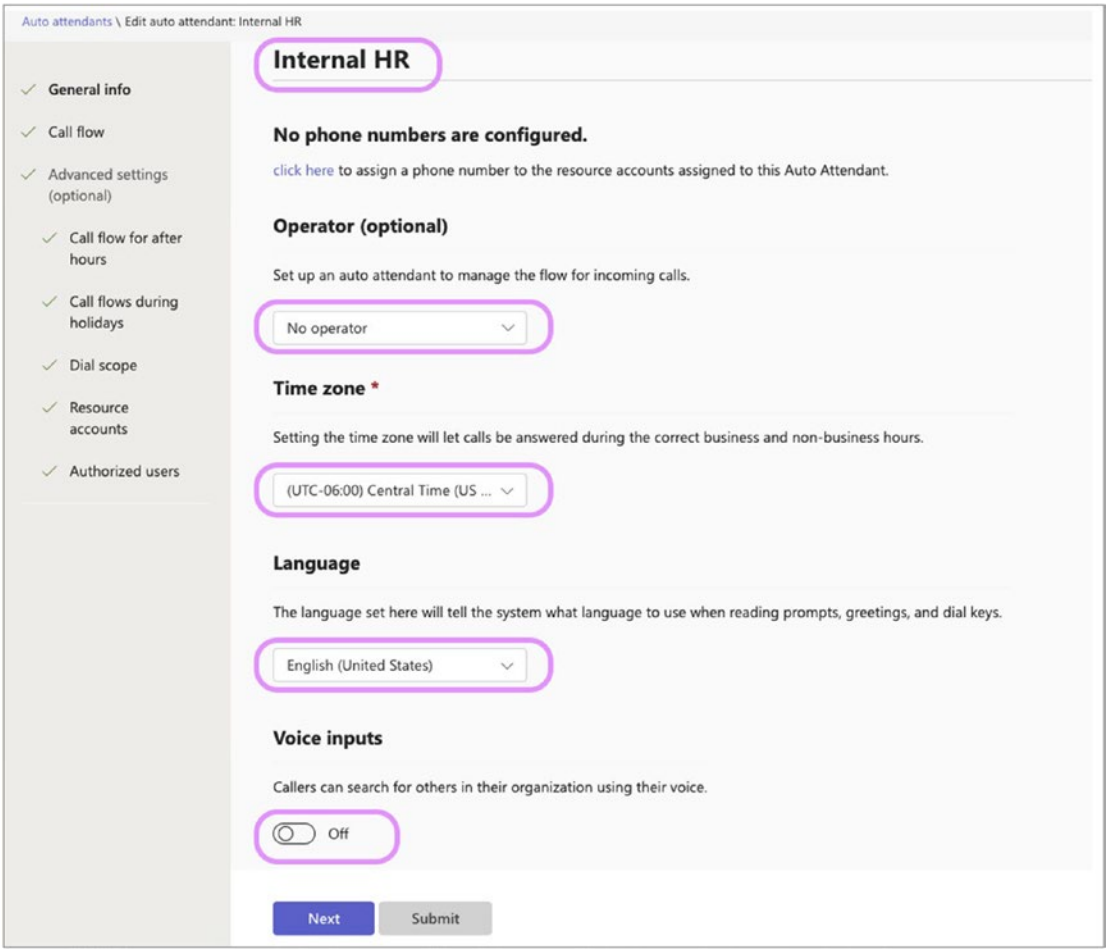

Figure 4-52. *Adding an auto attendant*

3. Click Next. On the page that opens, you are asked to configure the following settings:

    - **First Play A Greeting Message:** You can select No Greeting, Play An Audio File, or Type In A Greeting Message. Figure 4-53 shows an example of a greeting message entered.

Figure 4-53. *Typing in a greeting message*

- **The Route The Call:** You can redirect the call, disconnect the call, or play the menu options, as shown in Figure 4-54. If you play the menu options, you can configure which options are open to the caller and how they can choose among them. Additionally, you can force the caller to listen to the entire menu before selecting a menu option. The caller can use dial keys or voice input to navigate the options, and you can redirect the caller to auto attendants, call queues, or users. You can also allow users to search your directory. The options available for redirection in the menu are as follows:
- **Person In Organization:** This selection enables you to select the person to whom the incoming call will be redirected.
- **Person In Organization:** This selection enables you to select the person to whom the incoming call will be redirected.
- **Operator:** This setting specifies whether a user can request to talk to a person or voice app or if there will be no designated operator. You can refer people to another auto attendant, a call queue, or an enterprise voice-enabled Skype for Business or Teams user.

- **Voice Application:** You must select the name of an existing resource account associated with either a call queue or an auto attendant.
- **External Phone Number:** If you need to redirect a call to an external phone number, you can assign the resource account with either a Calling Plan license (if you use Calling Plans) or an Online Voice routing policy (if you use Direct Routing).
- **Voicemail (Personal):** Use this setting to redirect the call to a user voicemail.
- **Voicemail (Shared):** Use this setting to redirect the call to a M365 group's voicemail.
- **Announcement (Audio):** Use this setting to play an audio file.
- **Announcement (Typed):** Type in the text message to be played as text-to-speech.

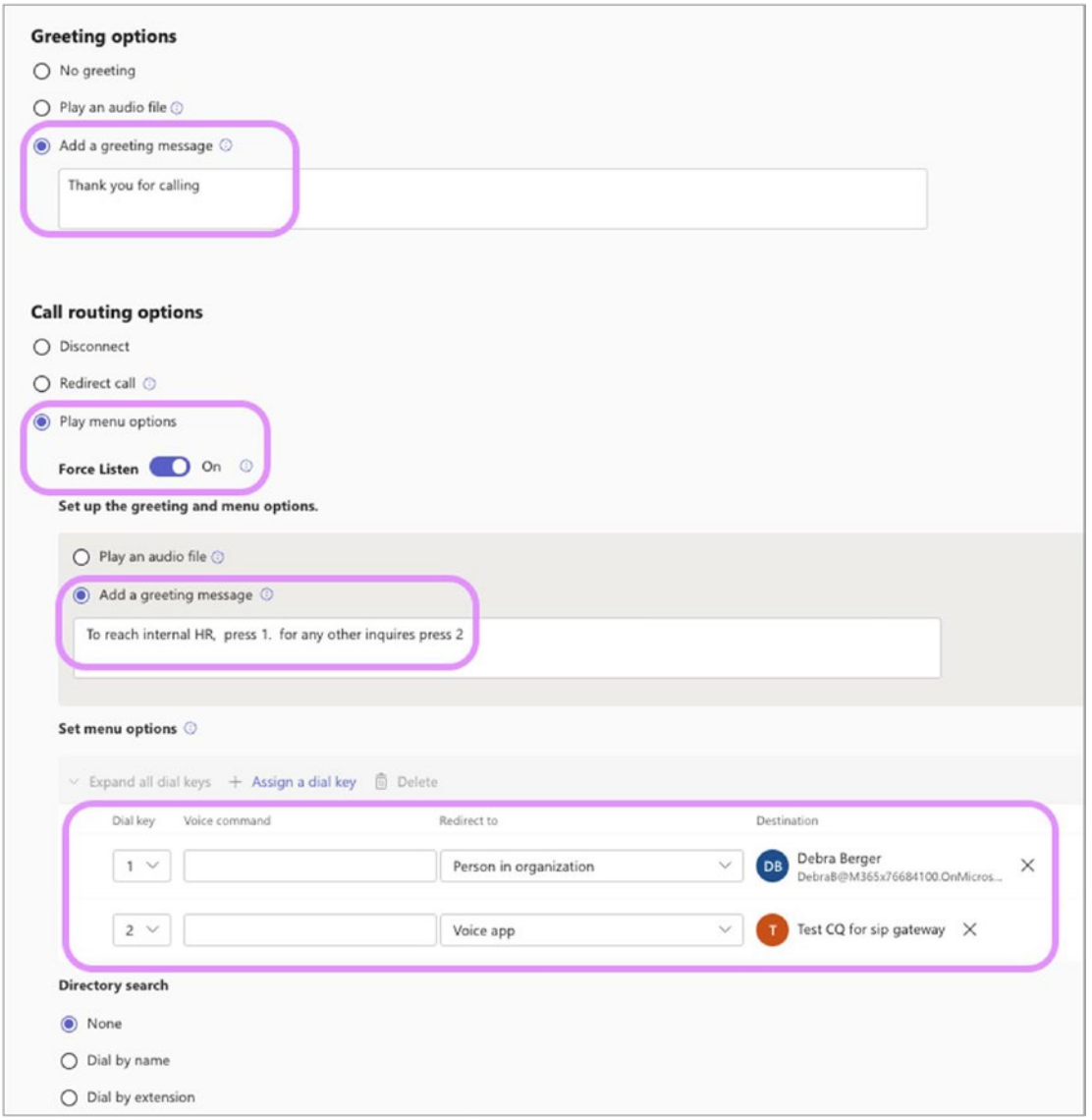

Figure 4-54. *Call routing options*

4. Click Next. On the next page, shown in Figure 4-55, provide the following information:

    a. **Set Business Hours:** Use these settings to specify when the auto attendant will be considered working. If you do not provide business hours, the auto attendant will be set to 24/7 by default.

b. **Set Up After Hours Call Flow:** Select what will happen to the call outside of business hours. If you do not change the default setting, your call will disconnect outside business hours.

c. **First Play A Greeting Message:** Specify a greeting for calls that are received outside of business hours. If you do not change the default setting, your call will not play an outside-of-business-hours greeting.

d. **Call routing options:** After playing the greeting, you have the following options:

    - **Disconnect:** This option will disconnect the call.
    - **Redirect To:** Select one of the following redirect settings using this option.
        - **Person In Organization:** This selection enables you to select the person to whom the incoming call will be redirected.
        - **Voice Application:** You must select the name of an existing resource account associated with either a call queue or an auto attendant.
        - **External Phone Number:** If you need to redirect a call to an external phone number, you can do so by assigning the resource account with either a Calling Plan license (if you use Calling Plans) or an Online Voice routing policy (if you use Direct Routing).
        - **Voicemail (Shared):** Use this setting to redirect the call to a M365 group's voicemail.

- **Play menu options:** With this feature, you can create a menu that allows callers to select their preferred redirect options based on the menu options provided.

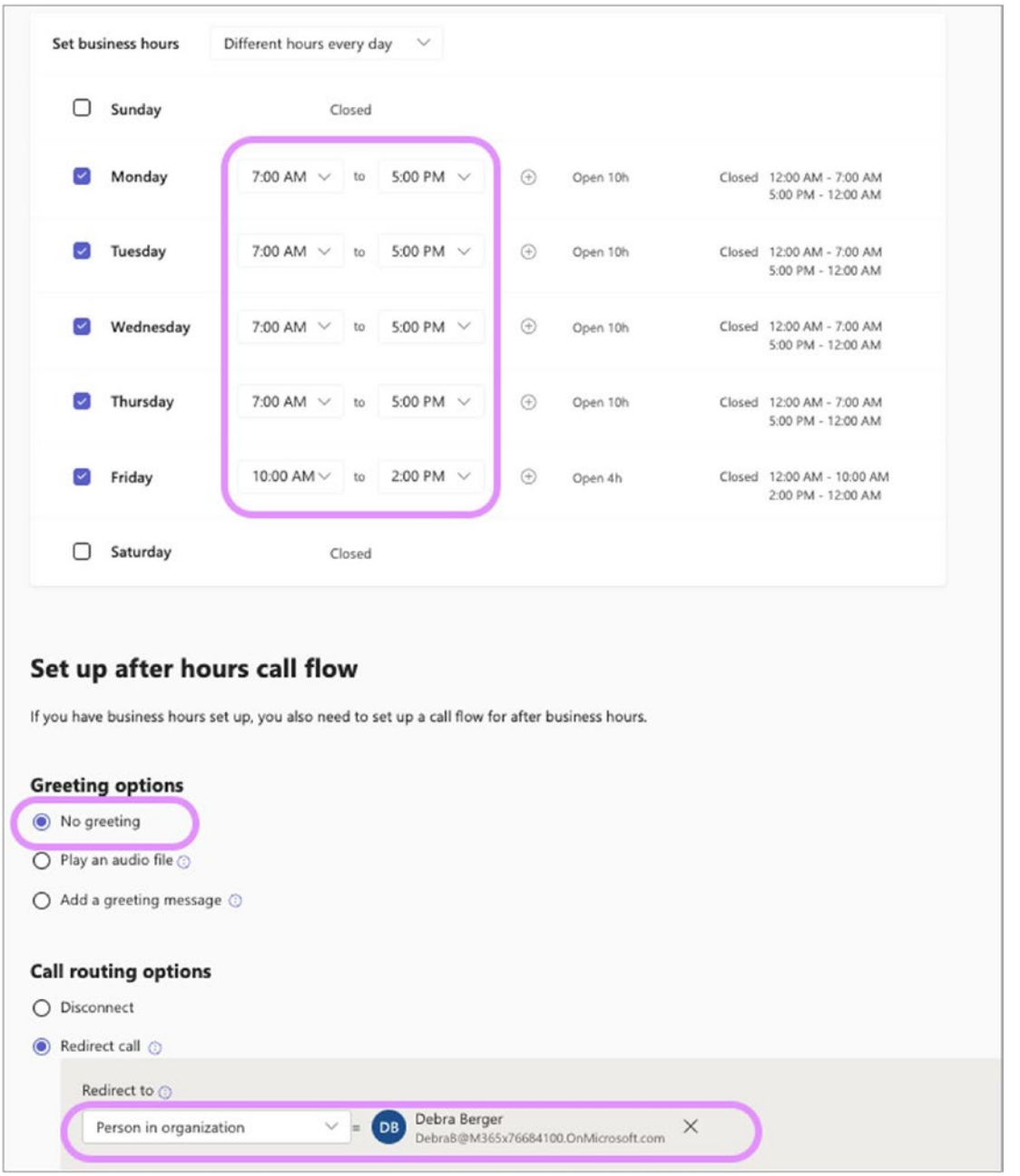

Figure 4-55. *Setting business hours*

5. Click Next. On the next page, you can click + Add to add specific dates as holidays for your auto attendant. Then you will be asked to provide the following information, as shown in Figure 4-56:
   - **Name:** Select the name for the holiday option.
   - **Date:** This is the date for the holiday.
   - **Greeting:** You can elect not to play a greeting and instead play an audio file or use text to speech.
   - **Call routing:** You can decide to disconnect or redirect calls.

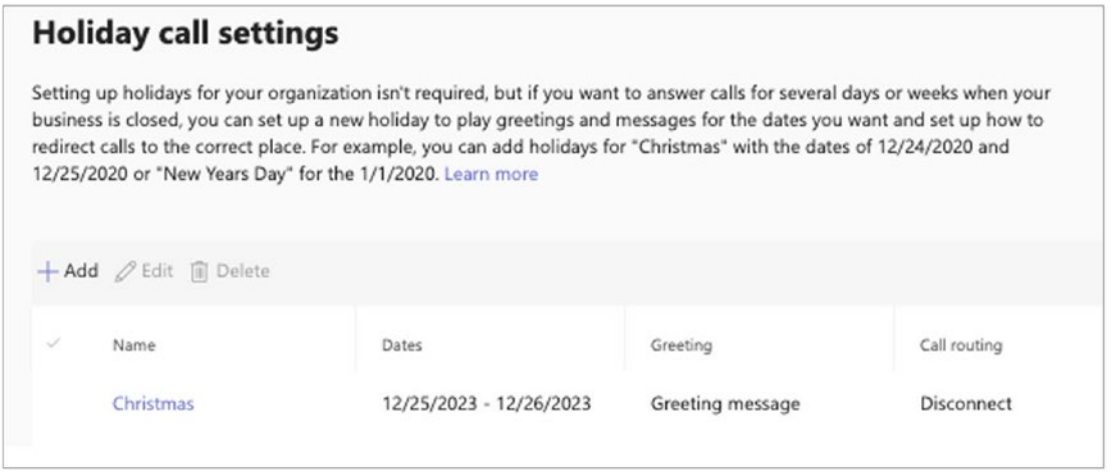

Figure 4-56. *Holiday call settings*

6. Click Save to save the holiday. You can add multiple holidays by repeating steps 5 and 6. You can set up to 50 holidays.
7. Click Next. On the page that opens, you can define the scope of users that is searchable by the caller, as displayed in Figure 4-57.
   - **Include:** Select a group of users or all online users. Online users are all those whose accounts are online or have been added using Azure Directory sync. Custom groups can be security, distribution, and Office 365 Groups.
   - **Exclude:** You can select None or Custom User Group. This will exclude those users from being searchable.

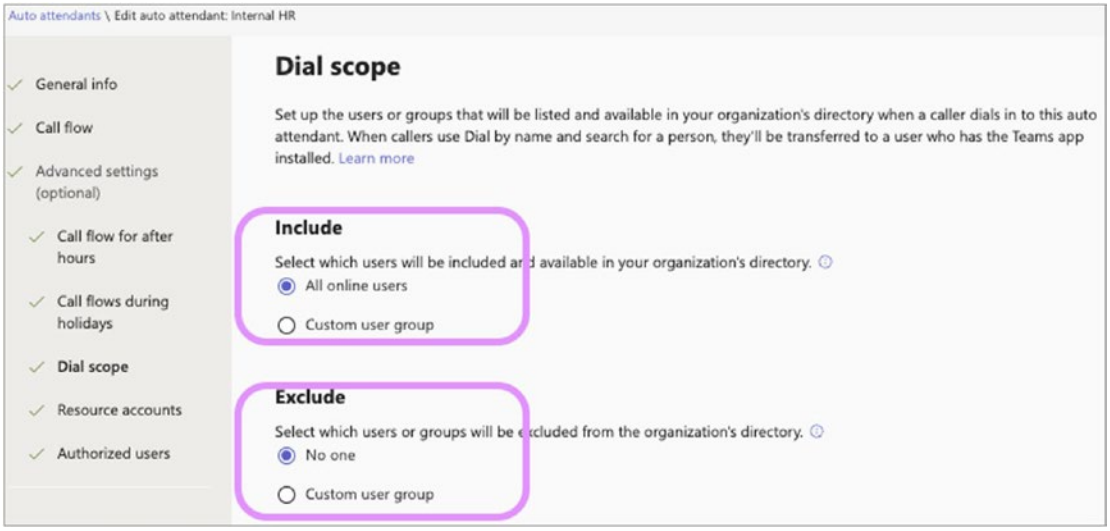

Figure 4-57. *Find people settings*

8. Click Next. On the next page, you will be asked to assign at least one resource account to the auto attendant. Click Add Accounts (see Figure 4-58) and search for the account you already created in the right panel. If you have yet to create an account, you can select Add Resource Account after searching for a nonexisting account name. You can assign a phone number to the resource account.

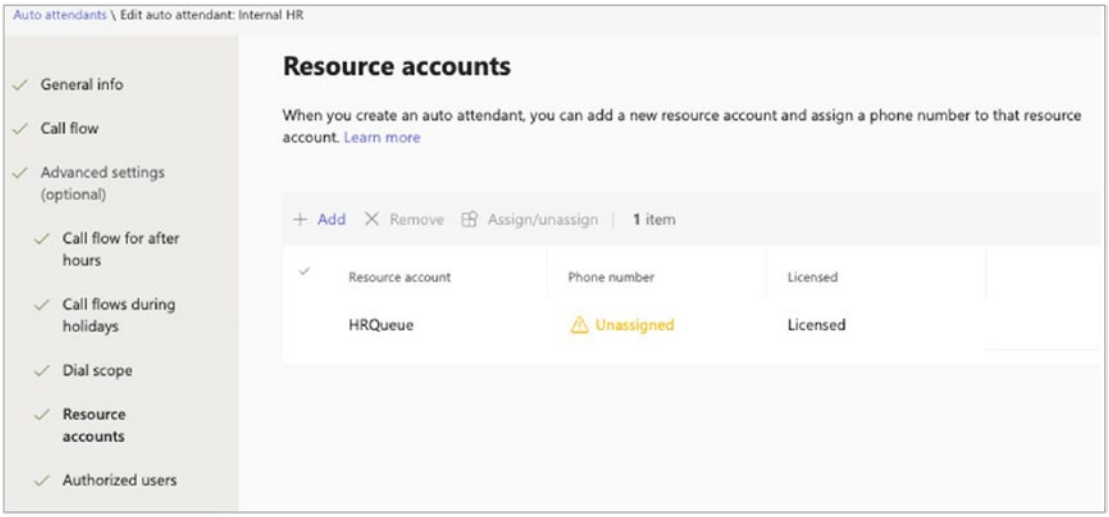

Figure 4-58. *Adding a resource account*

9. Next, add authorized users. Authorized users are a list of individuals who can manage the call queue settings. Typically, these individuals are supervisors or managers who handle agents. These users must be assigned with Voice application policy to manage the settings. Debra is assigned as an authorized user in the example and added to the Voice application policy. Debra can manage these settings in the Teams client. Click Submit to create your auto attendant. See Figure 4-59.

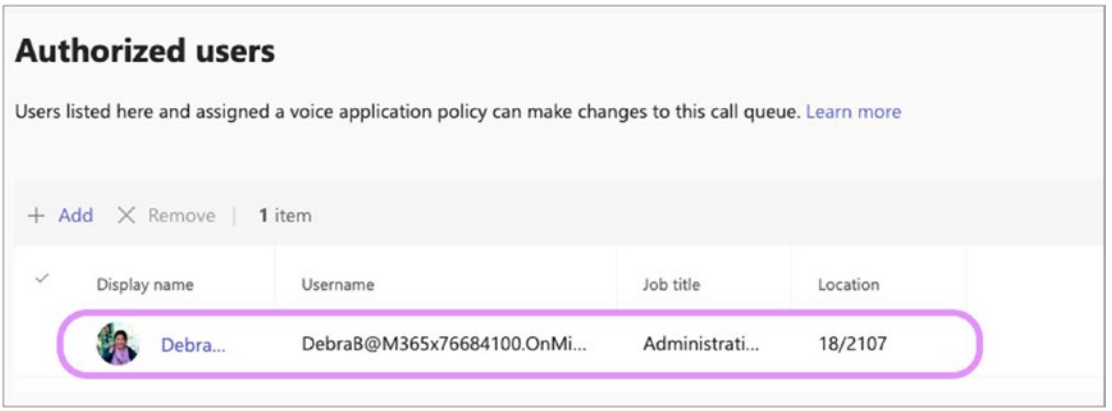

Figure 4-59. *Auto attendants, authorized users*

10. After creating an auto attendant, the next step is to test the auto attendant by calling the resource account phone number that is associated with the auto attendant.

Managing Auto Attendants

As a Teams admin, you must know how to manage auto attendants. To do so, log in to the Teams admin center and navigate to Voice. Select Auto Attendant. On the Auto Attendant page, you will see all auto attendants created in your tenant. You can perform management tasks such as adding new auto attendants, editing existing auto attendants, and deleting auto attendants.

Additionally, authorized users can manage the auto attendants from their Teams desktop client. Please note that they must be added as an authorized user in the auto attendant and assigned to the Voice application policy.

As an administrator, you can validate if an auto attendant is able to receive the call by running a diagnostic tool (https://aka.ms/TeamsAADiag).

Note You cannot call the attendant if you have not assigned a phone number to your resource account.

Assigning Phone Numbers for an Auto Attendant

As a Teams admin, you can assign a Microsoft/Operator connect service number, a Direct Routing number, or a service number ported from on-premises to the resource account that is linked to an auto attendant. As an admin you can port phone numbers from an existing service provider into the Microsoft 365 cloud. There are two processes for porting the phone numbers: automated porting, which is supported for U.S.-based numbers only (Microsoft developed an API with carriers and partners to be able to automate the whole process end-to-end), and Service Desk, which is available for all porting scenarios through support.

You must first get or port your existing toll or toll-free service numbers to assign a service number. Once you get the toll or toll-free service phone numbers, they show up in the Microsoft Teams admin center under Voice ➤ Phone Numbers. You can identify these numbers by looking for the type listed as Service. You can also update the usage for these phone numbers in the Teams admin center if the phone numbers are available with Calling Plans. If you are using Operator Connect, reach out to your Operator Connect provider to update the usage.

Searching for Users

Callers can search by name or extension when searching for users as part of the auto attendant functionality. This functionality is also known as *directory search*.

- **Dial by Name:** This feature enables the people who call your auto attendant to use voice (speech recognition) or their phone keypad (DTMF) to enter a full or partial name to search your company's directory, locate a person, and then have the call transferred to that person.

- **Dial by Extension:** This feature enables callers to use voice (speech recognition) or their phone keypad (DTMF) responses to enter the phone extension of the user they are trying to reach and then have the call transferred to that person.

The users you want to have located and reached using dial by name or dial by extension are not required to have a phone number or have Calling Plans assigned to them. Still, they must have a Phone System license if they are online users or Enterprise Voice enabled for Skype for Business Server users. Dial by name or extension will even be able to find and transfer calls to Microsoft Teams users who are hosted in different countries or regions for multinational organizations. Given the prerequisites involved, you must explicitly enable dial by name and dial by extension in an auto attendant.

Maximum Directory Size

There is no limit in the number of AD users dial by name, and dial by extension can support when a caller searches for a specific person. The maximum name list size that a single auto attendant can support using speech recognition is 80,000 users.

- **With dial by name**, a caller can enter just one part of the name or full names (FirstName + LastName, and LastName + FirstName). There are various formats that can be used when the name is entered. People can use the 0 (zero) key to indicate a space between the first and last name. When the person enters the name, they will be asked to terminate the keypad entry with the pound (#) key; for example, "After you have entered the name of the person you are trying to reach, please press pound." If multiple names are found, a list of names will be displayed, from which the person calling can select the person they are trying to reach.
- **With dial by extension**, the caller needs the full extension number.

People can also search for others in their company using dial by name with name recognition with speech recognition. When you enable speech recognition for an auto attendant, the phone keypad entry is not disabled, which means it can be used at any time (even if speech recognition is enabled on the auto attendant).

Setting Menu Options

Using the Teams admin center, you can assign functions for the 0–9 dial keys in an auto attendant. Different sets of menu options can be created for business hours and after hours, and you can turn dial on or off by name in the menu options. Keys can be mapped to transfer the calls to any of the following:

- An operator.
- Call queue.
- Another auto attendant.
- Microsoft Teams user with a Phone System license that is Enterprise Voice-enabled or has Calling Plans assigned to them. In cloud auto attendants, you can create menu prompts (e.g., "Press 1 for Marketing, Press 2 for Finance") and set up menu options to route calls. Menu prompts can be created either by using text-to-speech or by uploading a recorded audio file. Speech recognition accepts voice commands, but people can also use the phone keypad to navigate the menu.

Configuring and Managing Emergency Calling

The emergency calling service Enhanced 911 (E911) is the official national emergency service number in the United States. Other countries have similar emergency calling services. In the United States, when someone calls 911, the final destination of that call is a Public Safety Answering Point (PSAP) that dispatches first responders. PSAP jurisdictions usually follow local government (city or county) boundaries. E911 determines location information automatically and routes the call to the correct PSAP, and that's how caller gets the help they need.

Basically, an emergency calling service (in this case, E911) permits an emergency operator to identify a caller's location without asking the caller for that information. When a caller is calling from a client using a VoIP network, that information must be obtained based on various factors. Microsoft Teams offers an E911 calling service through Phone System Calling Plan where Microsoft is the service provider, and through Phone System Direct Routing using your existing on-premises PSTN connectivity to a carrier.

This section provides you with the essential information that you as a Teams admin will need to configure an emergency calling service in your environment.

First you need to understand the different terminology used here. First, the emergency address is a civic address containing the physical or street address of a place of business for your organization. For example, the Cyclotron organization's HQ office address is 537 South Tradition Street, Tracy, CA, 95391. Although not an emergency address, a place can also be used. The site is typically used when an office facility contains multiple floors, buildings, office numbers, and so on. A place is associated with an emergency address to give a more exact location within a building.

Note There are differences in how you manage emergency calling depending on whether you are using Microsoft Phone System Calling Plans or Phone System Direct Routing using an SBC connected to the PSTN.

E911 Laws in the United States

All Multi-Line Telephone Systems (MLTS) platforms are required to comply with minimum Enhanced 911 rules set by the Federal Communication Commission. This means that every organization in the United States must comply with federal regulations on Enhanced 911. It is now mandatory for organizations across the United States to comply with both Kari's Law and RAY BAUM's Act, which specify direct dialing, notification, and dispatchable location requirements.

Kari's Law

For every phone that can dial into the public switch network, it is required to be able to dial 911, including softphones. Kari's law mandates that MLTS platforms manufactured, imported, offered for first sale or lease, first sold or leased, or installed after February 16, 2020, must allow users to dial 911 directly without the need to dial a prefix to reach an outside line. Additionally, notification must be provided to front desk, security, and administrative personnel when a 911 call is made, including information about the call's location and the phone number that dialed 911.

Note Kari's law and the commission's rules are forward-looking and do not apply with respect to any MLTS that is manufactured, imported, offered for first sale or lease, first sold or leased, or installed on or before February 16, 2020.

Ray Baum's Act

According to the FCC, all 911 calls must have a "dispatchable location," which means emergency responders should have enough information to locate the person who made the call. Section 506 of Ray Baum's Act defines dispatchable location as this information. The specifics of the dispatchable location will differ depending on where the call is made from, but it may include details. Here's an example:

Street address - 2301 Performance Dr - 4th flr - Room 437/NE Corner

How Is Teams Phone Compliant with These Requirements?

Teams service complies with Kari's law by allowing 911 calls without prefixes or suffixes and without needing to enter the + sign before making the call. Additionally, administrators can configure emergency calling policies to send notifications to the front desk for each location and assign them directly to users or at the network level to dynamically send notifications. To comply with the Raybaums Act, Teams can configure emergency addresses with specific places and locations and assign them to users or networks.

The FCC rules apply to all MTLS systems, including softphones, regardless of their location. This means that even when working remotely, users must provide their accurate location when an emergency call is made from the Teams client. Teams Phone enables users to update their emergency location while working from home, thereby assisting organizations in maintaining compliance with regulations.

How Do Emergency Calls Work for Remote Locations?

Teams Phone enables users to set up emergency addresses while working remotely. Teams use the location services provided by the operating system to suggest an address. The end user can confirm or edit the location or manually enter the address in Teams client.

Once confirmed, the address is saved as the user-confirmed address. Every time the user changes its location, the address is auto-erased. As an administrator, you must enable external lookup mode in the emergency calling policies to allow emergency addresses for the remote location. In the United States, if a user confirms the remote location's address obtained from the operating system or it's edited through autosuggest, the emergency call is routed directly to the PSAP serving the location. If the address is obtained from the operating system and manually edited and confirmed by the user, or if the address is directly edited and confirmed by the user, the call will be redirected to the screening center and transferred to the PSAP. For Canada, calls are screened by the national call center before routing the calls to the nearest PSAP.

How Do Emergency Calls Work with Calling Plans?

Assigning an emergency location to a user when assigned a phone number with a Calling Plan license is mandatory. So, each Calling Plan user is automatically enabled with emergency calling, and the registered address is considered the user's emergency location. It's important to note that the user's emergency address remains the same regardless of whether they change offices or move to different floors within the same building. To address this issue, it's necessary to have a dynamic emergency calling. As an administrator, it's crucial to understand the requirements of your organization and configure your Teams phone to comply with local laws. In the United States, dynamic emergency calling ensures that emergency calls are directed to the nearest public safety answering point without being screened. Here's a breakdown of how emergency calls for Calling Plans are handled based on location:

If a Teams client is located in a tenant-defined dynamic emergency location…	…Route directly to PSAP for users in the…	…United States
If a Teams client is *not* located in a tenant-defined dynamic emergency location…	…Screen call before PSAP routing for users in the….	…United States
If an emergency caller is unable to update their emergency location to the screening center…	…The call will be transferred to the users registered address for users in the…	…United States

(*continued*)

If a Teams client is located in a tenant-defined dynamic emergency location…	…Route directly to PSAP for users in the…	…United States
Regardless of Teams client location…	….Emergency calls are routed directly to the PSAP serving the emergency address associated with the number for users in…	…Canada, Ireland, and the UK
Regardless of Teams client location…	…Emergency calls are routed directly to the PSAP for the local area code of the number for users in the…	…France, Germany, and Spain
Regardless of Teams client location…	…Emergency calls are routed directly to the PSAP for the local area code of the number for users in the…	…Netherlands
Regardless of Teams client location…	…Emergency addresses are configured and routed by the carrier partner for users in…	…Australia
Regardless of Teams client location…	…Emergency calling is not supported for users in…	…Japan

More details are explained in the "Configuring Emergency Calling in Calling Plan Environment" section.

How Do Emergency Calls Work for Operator Connect?

Assigning an emergency location to a user when assigned a phone number with Operator Connect license is mandatory. So, each user is automatically enabled with emergency calling, and the registered address is considered the user's emergency location. When Operator Connect carriers upload phone numbers to your tenant, they will assign each phone number to an emergency location. Depending on the carrier, the emergency address may or may not be altered by the administrator. A dynamic emergency configuration is useful to comply with your location's laws.

For the United States and Canada, dynamic routing is a part of the Operator Connect service. Like Calling Plans, Operator Connect carriers in the United States can route calls based on the current location of Teams clients using dynamic emergency calling instead of the tenant-defined location. For Canada, calls are screened by the national call center before routing the calls to the nearest PSAP. Calls will be routed to the screening center

if the dynamic emergency is not configured. If the screening center cannot determine the actual location of the user, calls will be routed to the nearest PSAP service associated with the registered address. For all the other locations, calls are routed based on the emergency calling network of that country or region.

How Do Emergency Calls Work for Teams Phone Mobile?

Like Operator Connect, each Teams Phone Mobile user is automatically assigned an emergency calling when a phone number is assigned. When Team Phone mobile carriers upload phone numbers to your tenant, they assign each phone number to an emergency location. Depending on the carrier, the emergency address may or may not be altered by the administrator. Dynamic emergency configuration is useful for complying with local laws.

For the United States and Canada, dynamic routing is a part of the Teams Phone Mobile service. Like Calling Plans, Operator Connect carriers in the United States can route calls based on the current location of Teams clients using dynamic emergency calling instead of the tenant-defined location. For Canada, calls are screened by the national call center before routing the calls to the nearest PSAP. Calls will be routed to the screening center if the dynamic emergency is not configured. If the screening center cannot determine the actual location of the user, calls will be routed to the nearest PSAP service associated with the registered address. For all the other locations, calls are routed based on the emergency calling network of that country or region. If a user needs to make an emergency call from their SIM-enabled mobile phone, the operator will use either the geographic coordinates or the cell tower handling the call to determine the user's approximate location.

How Do Emergency Calls Work with Direct Routing?

Emergency calling operates differently than other PSTN connectivity modes when using Direct Routing in Teams. As an administrator, you are responsible for setting up emergency call routing policies that specify the emergency numbers and their associated routing destinations. These policies can be associated with either users or sites. If a site is associated with a policy, that site policy will be used for emergency calls. If no emergency call routing policy has been defined for a user or site, that user cannot make emergency calls. With direct routing, the dynamic emergency configuration is useful for complying with local laws.

When using emergency calling with Direct Routing, it is recommended that you use emergency service responders (ERS) or ELIN applications to route the calls to PSAP. Most of the ERS providers in the United States can route calls based on the current location of Teams clients using dynamic emergency calling instead of the tenant-defined location. For Canada, calls are screened by the national call center before routing the calls to the nearest PSAP. Calls will be routed to the screening center if the dynamic emergency is not configured. If the screening center cannot determine the actual location of the user, calls will be routed to the nearest PSAP service associated with the registered address. For all the other locations, calls are routed based on the emergency calling network of that country or region. ERS providers use Pid-flo values from the SIP invite and parse the location information. Most of the Teams-certified SBCs are integrated with ELIN applications.

As an administrator, if you are using ELIN applications to route emergency calls, you must configure the emergency address and the associated phone numbers and upload them to the ELIN applications. More details are explained in the "Considerations for Emergency Phone System Direct Routing" section.

Configuring an Emergency Location in the Teams Admin Center

Teams emergency calling configuration includes multiple steps. One of the most important steps is to add the emergency location addresses in the Teams admin center. To do so, follow this procedure:

1. Log in to Teams admin center. Navigate to Location and then select Emergency Addresses. Click + Add.
2. Enter the name and a meaningful description for an address, as illustrated in Figure 4-60. Once you are finished, click Save to commit the changes.

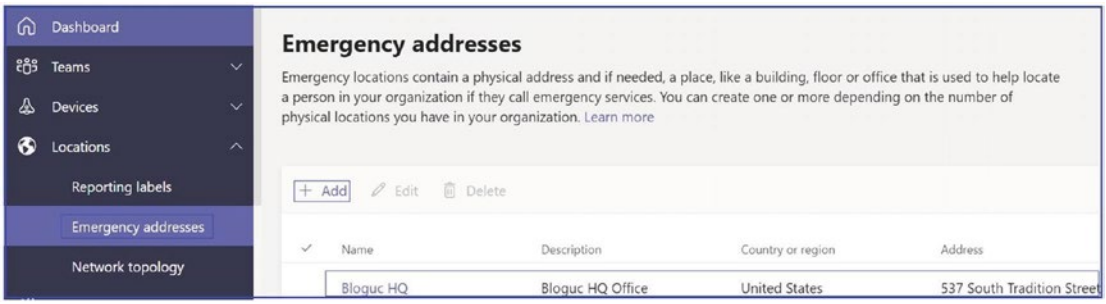

Figure 4-60. *Adding an emergency address*

3. To add more office addresses, repeat steps 1 and 2. Once all the addresses have been added, you will need to validate the status for each one.

Validating Emergency Addresses

After adding the emergency location addresses, the next step is to assign these emergency locations to the user. However, before giving the emergency addresses to an end user or to a network identifier, you as a Teams admin must validate the addresses.

When you enter an emergency address by using the address map search feature in the Microsoft Teams admin center, the address is automatically marked as validated. Remember, you cannot modify a validated emergency address. If the address format changes, you must create a new address with the updated format. After emergency address validation, the address will be marked as validated, and then you can assign this address to an end user account or network identifier. Figure 4-61 shows that the Cyclotron HQ office address has been validated.

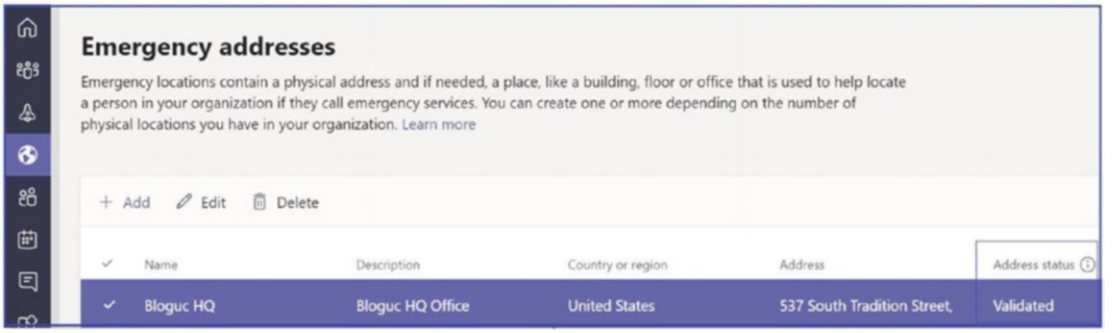

Figure 4-61. *Emergency address status*

Configuring Emergency Calling in a Calling Plan Environment

You must understand multiple considerations before configuring emergency calling, including emergency addresses, dynamic emergency addresses, and emergency call routing.

As a Teams admin, you must understand how emergency calling will work in Phone System Calling Plan scenarios. (For Phone System Calling Plan, Microsoft will provide phone numbers and work as the service provider.) If you are using Calling Plan, then each Calling Plan user (license assigned) will automatically be enabled for emergency

calling and must have a registered emergency address associated with their assigned phone number. Currently, Calling Plan is available in the United States, Canada, and some countries in Europe, the Middle East, and Africa. You can check Calling Plan availability by visiting https://docs.microsoft.com/en-us/microsoftteams/country-and-region-availability-for-audio-conferencing-and-calling-plans/country-and-region-availability-for-audio-conferencing-and-calling-plans.

Note Calling Plan, by default, provides a native emergency call routing service that routes call based on the Teams users' locations. If you want to route Teams users' emergency calls based on their current locations, use dynamic emergency call routing.

Another consideration is using dynamic emergency calling. This feature allows end users to have their location information sent along with the call to emergency services. To use dynamic emergency calling, a Teams admin must define the organization's network topology to identify the location of the client endpoint. For example, Balu usually works from the Tracy office location, so when he makes a call to emergency services, his Tracy office address is sent to the PSAP. Sometimes, however, he works from a Sacramento office location. Suppose he makes a call to emergency services when he is in the Sacramento office. In that case, the dynamic emergency calling service will send his Sacramento office address to the PSAP based on his network identifier that exists on the network.

As of this writing, Microsoft supports dynamic locations for emergency call routing for Calling Plan users in the United States in two scenarios.

- If a Teams client for a U.S. Calling Plan user dynamically acquires an emergency address within the United States, that address is used for emergency routing instead of the registered address, and the call will be automatically routed to the PSAP in the serving area of the address.
- If a Teams client for a U.S. Calling Plan user doesn't dynamically acquire an emergency address within the United States, then the registered emergency address is used to help screen and route

the call. However, the call will be screened to determine if an updated address is required before connecting the caller to the appropriate PSAP.

Emergency call routing to PSAP for Teams Calling Plan is based on factors, such as whether the Teams client dynamically determines the emergency address, whether the emergency address is the registered address associated with the user's phone number, and the emergency calling network of that country.

- If the country is the United States and the Teams client is located at a tenant-defined dynamic emergency location, emergency calls from that client are automatically routed to the PSAP serving that geographic location.
- If a Teams client is not located at a tenant-defined dynamic emergency location, emergency calls from that client are screened by a national call center to determine the caller's location before transferring the call to the PSAP serving that geographic location.
- If an emergency caller is unable to update their emergency location to the screening center, the call will be transferred to the PSAP serving the caller's registered address.

In Canada, Ireland, and the United Kingdom, emergency calls are first screened to determine the user's current location before connecting the call to the appropriate dispatch center. In France, Germany, and Spain, emergency calls are routed directly to the PSAP serving the emergency address associated with the number, regardless of the location of the caller. In the Netherlands, emergency calls are routed directly to the PSAP for the local area code of the number, regardless of the location of the caller. In Australia, emergency addresses are configured and routed by the carrier partner. In Japan, emergency calling is not supported.

Considerations for Emergency Phone System Direct Routing

Microsoft Teams supports emergency calling service through Teams direct routing. Teams allows you to use your existing phone system, including SBC with PSTN connectivity, for inbound and outbound phone calls. As a Teams admin, you must understand how emergency calling works using Direct Routing, and then you can decide

to use Direct Routing for emergency calling. You must define emergency calling policies for Direct Routing users using the `TeamsEmergencyCallRoutingPolicy` PowerShell command to determine emergency numbers and their associated routing destination.

Note The registered emergency locations are not supported for Direct Routing users.

You can allocate a TeamsEmergencyCallRoutingPolicy to a Teams Direct Routing user account, a network site, or both. When a Teams client starts or changes a network connection, Teams performs a lookup of the network site where the client is located. This lookup is based on the following scenarios:

- If a TeamsEmergencyCallRoutingPolicy is associated with the site, then the site policy is used to configure emergency calling.
- If there is no TeamsEmergencyCallRoutingPolicy associated with the site or if the client is connected at an undefined site, then the TeamsEmergencyCallRoutingPolicy associated with the user account is used to configure emergency calling.
- If the Teams client is unable to obtain a TeamsEmergencyCallRoutingPolicy, then the user is not enabled for emergency calling.

You must understand the considerations and the requirements for emergency calling through Direct Routing. In a Teams Direct Routing scenario, the Teams clients for Direct Routing users can acquire a dynamic emergency address, which can be used to dynamically route calls based on the caller's location.

- For emergency call routing in a Teams Direct Routing scenario, the TeamsEmergencyCallRoutingPolicy mentions an online PSTN usage, which should have the appropriate Direct Routing configuration to properly route the emergency calls to the appropriate PSTN gateway(s) using online PSTN routes. As a Teams admin, you should make sure that there is an OnlineVoiceRoute for the emergency dial string.
- The ability to dynamically route emergency calls for Direct Routing users varies depending on the emergency calling network in each

country. Two solutions are available: Emergency Routing Service Providers (ERSPs; U.S. only) and Emergency Location Identification Number (ELIN) gateway applications.

- If you are thinking about using ERSPs, several certified ERSPs can automatically route emergency calls based on the location of the caller.
- If an ERSP is integrated into a Direct Routing deployment, emergency calls with a dynamically acquired location will be automatically routed to the PSAP serving that location.
- Emergency calls without a dynamically acquired location are first screened to determine the current location of the user before connecting the call to the appropriate dispatch center based on the updated location.

Configuring Dynamic Emergency Call Routing Using Direct Routing

Remember that dynamic emergency calling is available through Microsoft Calling Plans and Phone System Direct Routing, and it offers the ability to configure and route emergency calls and notify security personnel based on the current location of the Teams client.

How does dynamic emergency call routing work? For dynamic emergency calling to work, a Teams admin has to define the network topology (adding all user subnets, creating emergency location and assignment, etc.). Based on that network topology configuration, the Teams client provides network connectivity information in a request to the Location Information Service (LIS). The LIS returns a location to the Teams client if there is a match. These location data are transferred back to the client, and then the Teams client includes location data as part of an emergency call. This data is then used by the emergency service provider to determine the appropriate PSAP and to send the call to that PSAP, which lets the PSAP dispatcher find the caller's location to provide the service.

Follow the steps given in the following sections to configure dynamic emergency call routing.

Step 1: Preparation Work

Here is the prep work process:

1. As a Teams admin, you must configure the network settings and the LIS to create a network and emergency location map. Specific to Direct Routing, additional configuration is required for routing emergency calls and possibly for partner connectivity. You must configure connection to an ERSP (in the United States) or configure the SBC for an ELIN application.
2. At startup and periodically afterward or when a network connection is changed, the Teams client sends a location request that contains its network connectivity information to the network settings and the LIS.
3. If there is a network settings site match, emergency calling policies are returned to the Teams client from that site; if there is a LIS match—an emergency location from the network element—the Teams client it is connected to is returned to the Teams client.
4. Once the user using Teams client attempts an emergency call, the emergency location is conveyed to the PSTN, and then for Direct Routing, you must configure the SBC to send emergency calls to the ERSP or configure the SBC ELIN application.

Step 2: Configuring Network Requirements (Sites and Trusted IPs)

Network settings are used to determine the location of a Teams client, and to obtain emergency calling policies and an emergency location dynamically. You can configure network settings according to how your organization wants emergency calling to operate. Network settings include network region, site, subnet, wireless access points, network switch, and trusted IP addresses. Here are the details:

- The network region includes a set of network sites.
- The network site is where your organization has a physical office, such as an office, a set of buildings, or a campus. These sites are defined as a set of IP subnets.

- A network subnet should be associated with a specific network site. A Teams client's location is determined based on the network subnet and the related network site.
- Trusted IP addresses are a collection of the external IP addresses (public-facing IP addresses also known as NAT IPs) of the organization network and are used to determine if the user's endpoint is inside the corporate network.

When Do I Need to Configure Region, Site, Subnet, and Trusted IP Addresses?

The network setting configuration differs based on the Phone System selection. If you are using Calling Plan for a user and require a dynamic configuration of security desk notifications, then you must configure both trusted IP addresses and network sites. If only dynamic locations are required, then you must configure only trusted IP addresses. If neither is required, then configuration of network settings is not required for Calling Plan.

Specific to Direct Routing users, if dynamic enablement of emergency calling or dynamic configuration of security desk notification is required, then you must configure both trusted IP addresses and network sites. If only dynamic locations are required, then you must configure only trusted IP addresses. If neither is required, then configuration of network settings is not required.

Step 3: Configuring Location Information Service, Emergency Policies, and Enabling Users and Sites

Here are the details about step 3.

Configuring Location Information Service (LIS)

LIS is a repository of network sites and subnets. A Teams client gets emergency addresses from the locations associated with different network identifiers, including network subnets and wireless access points (WAPs). As of this writing, an Ethernet switch/port is not supported, but Microsoft plans to support this in the future.

To configure the LIS with network identifiers and emergency locations, you, as a Teams admin can use Windows PowerShell and the commands discussed next.

`Get-CsOnlineLisSubnet` can be used for getting an existing LIS subnet, `Set` allows you to set the LIS subnet, and the `Remove` switch removes the LIS subnet. Similarly, you can use `Get`, `Set`, and `Remove` switches with `-CsOnlineLisPort`, `-CsOnlineLisSwitch`, and `-CsOnlineLisWirelessAccessPoint`.

As an example, the following command shows the subnet 10.10.10.0 set for the LIS with location ID and description.

```
Set-CsOnlineLisSubnet -Subnet 10.10.10.0 -LocationId b983a9ad-1111-455a-
a1c5-3838ec0f5d02 -Description "Subnet 10.10.10.0"
```

Configuring Emergency Policies

As part of an emergency calling service configuration, you need to set two emergency calling policies: Teams emergency call routing policy (TeamsEmergencyCallRoutingPolicy) and Teams emergency calling policy (TeamsEmergencyCallingPolicy). The emergency call routing policies are applied only to Teams Phone System Direct Routing users, not Calling Plan users.

You can create an emergency calling policy and call routing policy using the Teams admin center and Windows PowerShell.

First, to create or manage emergency calling and routing policies using the Teams admin center, log in to the Teams admin center and navigate to Voice. Select Emergency Policies. Once a policy is created, you can assign it to users and network sites. Users can use the Global (Org-wide default) policy or create and give custom policies. Users will automatically be assigned the Global policy unless you create and assign a custom policy.

Note You can edit the settings in the Global policy, but you cannot rename or delete it. For network sites, you create and assign custom policies.

Follow this procedure to create a custom emergency calling policy:

1. Log in to the Teams admin center and navigate to Voice. Select Emergency Policies, and then click the Calling Policies tab. Click Add. Enter a name and description for the policy. The example in Figure 4-62 shows Vijay WFH Policy as the policy name.

2. Turn on "External location lookup mode" to allow your end users to configure their emergency address when working from a network location outside the corporate network.
3. On the same page you can set how you want to notify people in your organization, typically the security desk, when an emergency call is made. To do this, select one of the following options under Notification Mode:
   - **Send Notification Only:** A Teams chat message is sent to the users and groups that you specify.
   - **Conferenced In But Are Muted:** A Teams chat message is sent to the users and groups that you specify, and they can listen (but not participate) in the conversation between the caller and the PSAP operator.
   - **Conferenced In And Are Unmuted:** Using this option, users can participate.

   Suppose you selected the Conferenced In But Are Muted notification mode, in the Dial-Out Number For Notifications box. In that case, you can enter the PSTN phone number of a user or group to call and join the emergency call. For example, enter the number of your organization's security desk (this example uses +12090001111 as the security desk number), who will receive a call when an emergency call is made and can then listen in or participate in the call.
4. Search for and select one or more users or groups, such as your organization's security desk, to notify when an emergency call is made. The example in Figure 4-62 lists Adele Vance. The notification can be sent to email addresses of users, distribution groups, and security groups. A maximum of 50 users can be notified.
5. Set the Emergency service disclaimer to show a banner to remind your end users to confirm their emergency location.

Click Save to commit the changes.

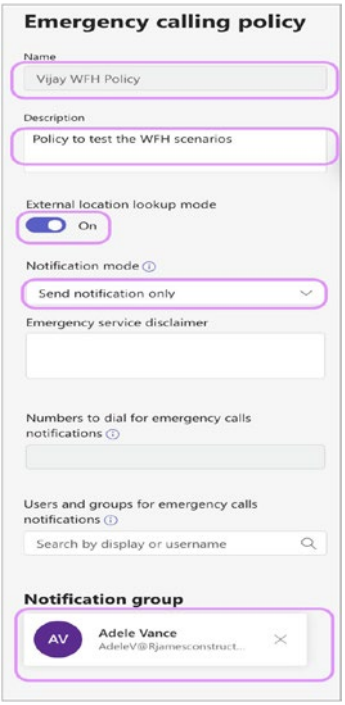

Figure 4-62. *Emergency policies*

You can create a call routing policy by clicking the Call Routing Policies tab.

If you assigned an emergency calling policy to a network site and to a user and if that user is at that network site, the policy assigned to the network site overrides the policy assigned to the user.

You can also use PowerShell to manage emergency call routing and calling policies.

The TeamsEmergencyCallRoutingPolicy is used primarily for routing emergency calls. This policy configures the emergency numbers, masks per number if required, and the PSTN route per number. You can assign this policy to users, to network sites, or to both. (Calling Plan Teams clients are automatically enabled for emergency calling with the emergency numbers from the country based on their Office 365 usage location.) You manage this policy using the `New-`, `Set-`, and `Grant-CsTeamsEmergencyCallRouting` commands. For example, the command shown next first creates a new Teams emergency number object and then creates a Teams emergency call routing policy with this emergency number object.

```
$en =  New-CsTeamsEmergencyNumber -EmergencyDialString "911" -EmergencyDialMask
"911;9911" -OnlinePSTNUsage "Local" -CarrierProfile "Local"

New-CsTeamsEmergencyCallRoutingPolicy -Identity "HQ-Emergency" -Tenant
$tenant -EmergencyNumbers @{add=$en} -AllowEnhancedEmergencyServices:
$true -Description "HQ Emergency Route Policy"
```

Note The OnlinePSTNUsage specified in the first command must previously exist. You can use the `Set-CsOnlinePSTNUsage` command for PSTN usage creation.

The resulting object from the `New-CsTeamsEmergencyNumber` command exists only in memory, so you must apply it to a policy to be used.

`TeamsEmergencyCallingPolicy` is another policy required for emergency calling. It uses Calling Plan and Direct Routing. This policy configures the security desk notification experience during an emergency call. You can set who to notify and how they are notified; for example, automatically notify your organization's security desk and have them listen in on emergency calls. This policy can be assigned to users, network sites, or both. As an admin, you can manage this policy using the `New-`, `Set-`, and `Grant-CsTeamsEmergencyCallingPolicy` commands. For example, the PowerShell command shown here creates a Teams emergency calling policy that has an identity of `Cyclotron-EMS-Policy`, where a notification group and number are specified, as well as the type of notification.

```
New-CsTeamsEmergencyCallingPolicy -Identity Cyclotron-EMS-Policy
-Description "Cyclotron Emergency calling Policy" -NotificationGroup
"alert@cyclotron.com" -NotificationDialOutNumber "+12090001111"
-NotificationMode NotificationOnly -ExternalLocationLookupMode $true
```

Managing Phone Numbers

Let's talk about managing phone numbers.

Acquiring and Managing Teams Service Numbers and User Phone Numbers

Microsoft Teams support service numbers like dial-in conference numbers or auto attendant numbers, as well as user phone numbers like user Teams phone numbers to receive inbound calls and make outbound calls.

- **Teams service** numbers are assigned to services such as Audio Conferencing, auto attendants, and call queues. Service phone numbers, which have a higher concurrent call capacity than user numbers, will vary by country or region and the type of number (whether it is a toll or toll-free number). Admins can acquire service (toll or toll-free) numbers from Microsoft.
- **Teams user phone numbers:** User phone numbers can be assigned to users in the organization for inbound and outbound calling purposes. As an admin, you can acquire Teams user phone numbers from Microsoft or port your existing phone number to Microsoft and use it in Teams Phone System along with Calling Plan.

Getting a Service or Phone Number

An admin can acquire new phone numbers in the Teams admin center. To get a phone number or service number, follow this procedure:

1. Log in to the Teams admin center; then navigate to Voice and click Phone Numbers.
2. On the Phone Numbers page, under Numbers, click + Add for a new phone number request. Enter a name and description.
3. In the Location And Quantity section, enter the following information, as shown in Figure 4-63:
    - **Country Or Region:** Select country or region.
    - **Number Type:** Select the appropriate option that determines whether the phone numbers are designated for users or for services, such as conference bridge, call queue, or auto attendant.

- **Location:** Choose a location for connecting the new phone numbers. If you must create a new location, select Add A Location and enter the required location's data.
- **Area Code:** Select a valid area code for the country and location.
- **Quantity:** Enter the number of phone numbers that you want for your organization.

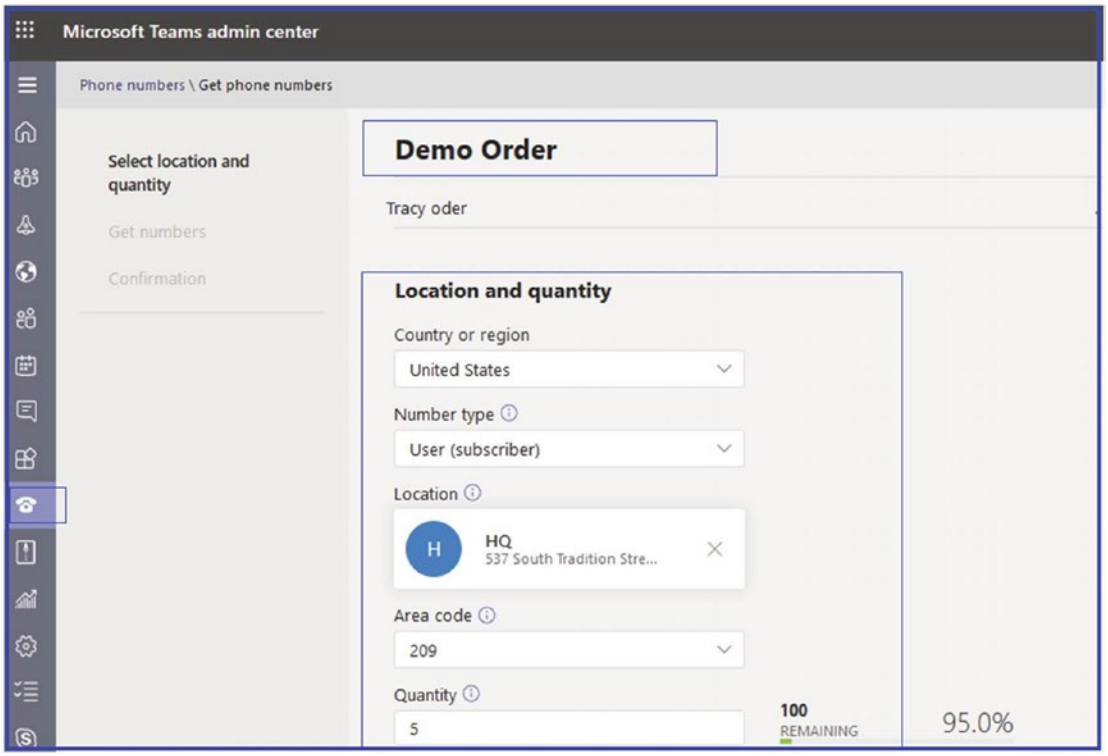

Figure 4-63. *Phone number order*

4. Click Next to continue. Select the phone numbers you want to apply to your tenant on the Get Numbers page.
5. Click Place Order to submit the order.

Note The phone numbers are reserved for only 10 minutes; therefore, if you do not click Place Order, the phone numbers are returned to the pool of numbers, and you have to reorder the phone numbers.

Creating and Managing Voice Routing Policy

As a Teams admin, you must know how to create and manage Teams voice routing policies. Teams Phone System has a routing mechanism that allows a call to be sent to a specific SBC based on the called number pattern plus the particular user who makes the call. SBCs can be designated as active or backup controllers. When the SBC that was configured as active is not available for a specific call route, the call will be routed to a backup SBC.

Voice routing policies are assigned to users, but they are made up of multiple elements, such as PSTN usage, PSTN routes, and the voice routing policy itself. It is a container for PSTN usage, which can be assigned to a user or to multiple users.

- **PSTN usages:** A container for voice routes and PSTN usages, which can be shared in different voice routing policies
- **Voice routes:** A number pattern and set of online PSTN gateways to use for calls where the calling number matches the pattern
- **Online PSTN gateway:** A pointer to an SBC that also stores the configuration that is applied when a call is placed through the SBC, such as forward P-Asserted-Identity (PAI) or Preferred Codecs; can be added to voice routes

Follow these steps to create a voice routing policy:

1. First, create PSTN usage (one or more) for the voice routing policy. Remember that, as of this writing, you cannot create a voice routing policy or PSTN usage or routes using the Teams admin center. You will have to use Windows PowerShell. Before running

the following PowerShell command, however, you must connect to Teams tenant by installing and connecting to the Microsoft Teams module; run the following steps:

```
Install-Module MicrosoftTeams

Connect-MicrosoftTeams
```

2. PSTN usages are the glue that connects a route to the voice routing policy. Use the following command to create PSTN usage for the U.S. East and West regions:

```
Set-CsOnlinePstnUsage -Identity Global -Usage @{Add="US
East and US West"}
```

3. Now create a PSTN route to match the dialed number and use the PSTN gateway. Refer to the following command to create two routes, Tracy 1 and 2, within the U.S. East and West PSTN usages. Remember that the PSTN gateways are already created as part of the Teams Direct Routing configurations.

```
New-CsOnlineVoiceRoute -Identity "Tracy1" -NumberPattern
"^\+1(209|210)

(\d{7})$" -OnlinePstnGatewayList sbc1.cyclotron.com, sbc2.
cyclotron.com -Priority 1 -OnlinePstnUsages "US East and
US West"

New-CsOnlineVoiceRoute -Identity "Tracy2" -NumberPattern
"^\+1(209|210)

(\d{7})$" -OnlinePstnGatewayList sbc3.cyclotron.com, sbc4.
cyclotron.com -Priority 2 -OnlinePstnUsages " US East and
US West"
```

4. The next step is to create a voice routing policy with these created PSTN usages, using these commands:

```
New-CsOnlineVoiceRoutingPolicy "US East and
West" -OnlinePstnUsages "US East and US West"
```

5. Assign the voice routing policy to users. Use this PowerShell command to do so:

   ```
   Grant-CsOnlineVoiceRoutingPolicy -Identity "Balu Ilag"
   -PolicyName "US East and US West"
   ```

   You can verify the voice routing policy assigned to the user by running this PowerShell command:

   ```
   Get-CsOnlineUser "Balu Ilag" | select OnlineVoiceRoutingPolicy
   ```

Tip As an admin, you can create a voice routing policy with multiple PSTN usages. You can use the preceding PowerShell commands and make a script to assign policies to multiple users.

Summary

In this chapter, we delved into the multifaceted capabilities of Microsoft Teams in handling various communication needs, including persistent chat, audio/video calls, conferences (both dial-in and client join), and phone systems for inbound/outbound PSTN calls. Specifically, the chapter elucidated the workings of Teams conference management, encompassing aspects such as audio conferencing (dial-in), Teams Webinars, Teams Premium, VoIP for internal and external attendees, and comprehensive insight into Teams Phone System management.

The Teams Phone System, a cloud-based innovation, stands out as a replacement for traditional on-premises PBX systems, offering advanced functionalities such as call control, voicemail with transcription, call queues, auto attendants, call park, emergency calling features, enhanced E9-1-1 dialing, caller ID display, direct routing, and interoperability with third-party systems. This intricate orchestration of features collectively streamlines and modernizes communication, making Teams a central hub for collaboration and connection in today's dynamic working environment.

References

- https://support.microsoft.com/en-us/office/meeting-options-in-microsoft-teams-53261366-dbd5-45f9-aae9-a70e6354f88e
- https://learn.microsoft.com/en-us/microsoftteams/limits-specifications-teams
- https://learn.microsoft.com/en-us/microsoftteams/meeting-policies-overview
- https://learn.microsoft.com/en-us/microsoftteams/outbound-calling-restriction-policies
- https://learn.microsoft.com/en-us/microsoftteams/set-up-webinars
- https://www.microsoft.com/en-us/microsoft-365/blog/2022/10/12/introducing-microsoft-teams-premium-the-better-way-to-meet/
- https://www.microsoft.com/en-us/microsoft-365/blog/2023/02/01/microsoft-teams-premium-cut-costs-and-add-ai-powered-productivity/
- https://learn.microsoft.com/en-us/microsoftteams/enhanced-teams-experience
- https://learn.microsoft.com/en-us/microsoftteams/configure-meetings-three-tiers-protection
- https://learn.microsoft.com/en-us/microsoftteams/platform/apps-in-teams-meetings/teams-together-mode
- https://learn.microsoft.com/en-us/microsoftteams/operator-connect-plan
- https://cloudpartners.transform.microsoft.com/partner-gtm/operators/directory
- https://learn.microsoft.com/en-us/microsoftteams/operator-connect-mobile-plan

- https://www.metaswitch.com/products/mobile-control-point
- https://learn.microsoft.com/en-us/azure/communications-gateway/mobile-control-point
- https://techcommunity.microsoft.com/t5/azure-for-operators-blog/supporting-operator-connect-mobile/ba-p/3473944
- https://learn.microsoft.com/en-us/microsoftteams/create-a-phone-system-call-queue?tabs=general-info
- https://www.fcc.gov/mlts-911-requirements
- https://www.911.gov/issues/legislation-and-policy/kari-s-law-and-ray-baum-s-act/#:~:text=What%20is%20Kari's%20Law%3F,dialing%20911%20from%20an%20MLTS